PAN-OS Web インターフェイスのヘルプ

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

June 29, 2020

Table of Contents

Web インターフェイスの基本 13

ファイアウォールの概要 14
機能と利点 15
前回のログイン時間およびログイン試行回数 17
当日のメッセージ 18
タスク マネージャ 19
言語 21
アラーム 22
変更のコミット 23
候補設定の保存 27
変更を元に戻す 31
設定のロック 35
Global Find 37
脅威詳細 38
AutoFocus インテリジェンス サマリー 40
設定テーブルのエクスポート 43

ダッシュボード 45

Dashboard Widgets (ダッシュボード ウィジット) 46

ACC 49

ACC の画面紹介 50
ACC のタブ 52
ACC のウィジェット 53
ACC のアクション 55
- タブおよびウィジットの処理 55
- フィルタの処理 – ローカル フィルタおよびグローバル フィルタ 56

監視 59

Monitor > Logs [監視 > ログ] 60
- ログ タイプ 60
- ログ アクション 65

Monitor (監視) > External Logs (外部ログ) 67
Monitor (監視) > Automated Correlation Engine (自動相関エンジン) 68
- [Monitor] > [自動相関エンジン] > [相関オブジェクト] 68
- [Monitor] > [自動相関エンジン] > [相関されたイベント] 69

Monitor > Packet Capture [監視 > パケット キャプチャ] 71
- パケット キャプチャの概要 71
- カスタム パケット キャプチャの構成要素 72
- 脅威パケット キャプチャの有効化 75

Monitor > App Scope [監視 > アプリケーション スコープ] 76
- アプリケーション スコープの概要 76
- アプリケーション スコープのサマリー レポート 77
- アプリケーション スコープの変化モニター レポート 77
- アプリケーション スコープの脅威モニター レポート 78
- アプリケーション スコープの脅威マップ レポート 80
- アプリケーション スコープのネットワーク モニター レポート 80

アプリケーション スコープのトラフィック マップ レポート....81
Monitor > Session Browser [監視 > セッション ブラウザ]....83
Monitor (監視) > Block IP List (ブロック IP リスト) 84
ブロック IP リスト エントリ....84
ブロック IP リスト エントリの表示または削除....85
Monitor > Botnet [監視 > ボットネット]....87
ボットネット レポートの設定....87
ボットネットの設定....88
Monitor (監視) > PDF Reports (PDF レポート) 90
Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レポート > PDF サマリーの管理]....90
Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > ユーザー アクティビティ レポート]....91
Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレポート > Saasアプリケーションの使用状況]....93
Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポート グループ]....95
Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子メール スケジューラ]....96
Monitor > Manage Custom Reports [監視 > カスタム レポートの管理]....98
Monitor > Reports [監視 > レポート]....100

レポートを生成....101
ポリシーのタイプ....102
ポリシールールの移動またはコピー....103
監査コメント アーカイブ....104
監査コメント....104
設定ログ (コミット間) 104
ルール変更....105
ルールの使用状況ヒット数のクエリ....106
ルール ヒット数クエリのデバイス ルールの使用状況....106
Policies > Security [ポリシー > セキュリティ]....108
セキュリティポリシーの概要....108
セキュリティ ポリシー ルールの構成要素....109
ポリシーの作成と管理....118
セキュリティ ポリシー ルールのオーバーライドまたは取り消し....122
アプリケーションおよび使用状況....124
セキュリティポリシー オプティマイザー....127
Policies > NAT [ポリシー > NAT]....129
NAT ポリシーの General (全般) タブ....129
NAT の Original Packet (元のパケット) タブ....130
NAT の Translated Packet (変換済みパケット) タブ....131
NAT の Active/Active HA Binding (アクティブ/アクティブ HA バインド) タブ....134
Policies > QoS [ポリシー > QoS]....136
Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーディング]....140
ポリシー ベース フォワーディングの General (全般) タブ....140
ポリシー ベース フォワーディングの Source (送信元) タブ....141
ポリシー ベース フォワーディングの Destination/Application/Service (宛先/アプリケーション/サービス) タブ....142
ポリシー ベース フォワーディングの Forwarding (転送) タブ....143
Policies > Decryption [ポリシー > 復号化]....145
復号化の General (全般) タブ....145

復号化の Source (送信元) タブ 146
復号化の Destination (宛先) タブ 147
復号化の Service/URL Category (サービス/URL カテゴリ) タブ 148
復号化の Options (オプション) タブ 148
Policies (ポリシー) > Tunnel Inspection (トンネル検査) 150
トンネル検査ポリシーの構成要素 150
Policies > Application Override [ポリシー > アプリケーション オーバーライド] 156
アプリケーション オーバーライドの General (全般) タブ 157
アプリケーション オーバーライドの Source (送信元) タブ 157
アプリケーション オーバーライドの Destination (宛先) タブ 158
アプリケーション オーバーライドの Protocol/Application (プロトコル/アプリケーション) タブ 158
Policies (ポリシー) > Authentication (認証) 160
認証ポリシー ルールの構成要素 160
認証ポリシーの作成と管理 165
Policies > DoS Protection [ポリシー > DoS プロテクション] 167
DoS プロテクションの General (全般) タブ 167
DoS プロテクションの Source (送信元) タブ 168
DoS プロテクションの Destination (宛先) タブ 169
DoS プロテクションの Option/Protection (オプション/防御) タブ 169
Policies > SD-WAN [ポリシー > SD-WAN] 173
SD-WAN General (全般) タブ 173
Source (送信元) タブ 174
Destination (宛先) タブ 175
SD-WAN Application/Service (アプリケーション/サービス) タブ 175
SD-WAN Path Selection (パス選択) タブ 177
SD-WAN Target (ターゲット) タブ 177

Objects 179
オブジェクトの移動、コピー、オーバーライド、取り消し 180
オブジェクトの移動またはコピー 180
オブジェクトのオーバーライド/取り消し 180
Objects > Addresses [オブジェクト > アドレス] 182
Objects > Address Groups [オブジェクト > アドレス グループ] 184
Objects > Regions [オブジェクト > 地域] 186
Objects > Dynamic User Groups [オブジェクト > 動的ユーザー グループ] 187
Objects > Applications [オブジェクト > アプリケーション] 189
アプリケーションの概要 189
アプリケーションでサポートされる操作 193
アプリケーションの定義 196
Objects > Application Groups [オブジェクト > アプリケーション グループ] 201
Objects > Application Filters [オブジェクト > アプリケーションフィルタ] 202
Objects > Services [オブジェクト > サービス] 203
Objects (オブジェクト) > Service Groups (サービス グループ) 205
Objects > Tags [オブジェクト > タグ] 206
タグの作成 206
ルールベースをグループとして表示 208
タグの管理 211
Objects > External Dynamic Lists [オブジェクト > 外部動的リスト] 213
Objects (オブジェクト) > Custom Objects (カスタム オブジェクト) 218
Objects > Custom Objects > Data Patterns [オブジェクト > カスタム オブジェクト > データ パターン] 218

Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> Spyware/Vulnerability（スパイウェア/脆弱性）.....222
Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カテゴリ].....226
Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）.....228
セキュリティ プロファイルのアクション.....228
Objects > Security Profiles > Antivirus [オブジェクト > セキュリティ プロファイル > アンチウイルス].....232
Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Anti-Spyware Profile（アンチスパイウェア プロファイル）.....234
Objects > Security Profiles > Vulnerability Protection [オブジェクト > セキュリティプロファイル > 脆弱性防御].....239
Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング].....243
URL フィルタリングの一般設定.....243
URL フィルタリング カテゴリ.....244
URL フィルタリング設定.....246
ユーザー証明書検出.....248
HTTP ヘッダの挿入.....249
Objects > Security Profiles > File Blocking [オブジェクト > セキュリティ プロファイル > ファイル ブロッキング].....252
Objects > Security Profiles > WildFire Analysis [オブジェクト > セキュリティ プロファイル > WildFire 分析].....254
Objects > Security Profiles > Data Filtering [オブジェクト > セキュリティ プロファイル > データ フィルタリング].....256
Objects > Security Profiles > DoS Protection [オブジェクト > セキュリティ プロファイル > DoS プロテクション].....258
Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション）.....262
Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> SCTP Protection（SCTP プロテクション）.....268
Objects > Security Profile Groups [オブジェクト > セキュリティ プロファイル グループ].....274
Objects > Log Forwarding [オブジェクト > ログ転送].....275
Objects（オブジェクト）> Authentication（認証）.....279
Objects > Decryption Profile [オブジェクト > 復号化プロファイル].....281
復号化プロファイルの一般設定.....281
復号化された SSL トラフィックを制御するための設定.....282
復号化されていないトラフィックを制御するための設定.....288
復号化された SSH トラフィックを制御するための設定.....288
Objects（オブジェクト）> Decryption（復号化）> Forwarding（転送プロファイル）.....290
Objects > SD-WAN Link Management [オブジェクト > SD-WAN リンク管理].....293
Objects > SD-WAN Link Management > Path Quality Profile [オブジェクト > SD-WAN リンク管理 > パス品質プロファイル].....293
Objects (オブジェクト) > SD-WAN Link Management (SD-WANリンク管理) > Traffic Distribution (トラフィック分散).....294
Objects > Schedules [オブジェクト > スケジュール].....296

ネットワーク.....297
[Network] > [インターフェイス].....298
ファイアウォール インターフェイスの概要.....299
ファイアウォール インターフェイスの共通の構成要素.....299

PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素..... 301
タップ インターフェイス..... 301
HA インターフェイス..... 302
バーチャル ワイヤー インターフェイス..... 303
バーチャル ワイヤー サブインターフェイス..... 305
PA-7000 シリーズのレイヤー 2 インターフェイス..... 306
PA-7000 シリーズのレイヤー 2 サブインターフェイス..... 307
PA-7000 シリーズのレイヤー 3 インターフェイス..... 308
レイヤー 3 インターフェイス..... 319
レイヤー 3 サブインターフェイス..... 329
Log Card Interface (ログ カード インターフェイス) 338
ログ カード サブインターフェイス..... 339
復号化ミラー インターフェイス..... 340
Ethernet の集約 (AE) インターフェイス グループ..... 341
Ethernet の集約 (AE) インターフェイス..... 344
Network > Interfaces > VLAN [ネットワーク > インターフェイス > VLAN]..... 350
Network > Interfaces > Loopback [ネットワーク > インターフェイス > ループバック]..... 360
Network > Interfaces > Tunnel [ネットワーク > インターフェイス > トンネル]..... 363
Network > Interfaces > SD-WAN [ネットワーク > インターフェイス > SD-WLAN]..... 366
Network > Zones [ネットワーク > ゾーン] 367
セキュリティ ゾーンの概要..... 367
セキュリティ ゾーンの構成要素..... 367
Network > VLANs [ネットワーク > VLAN]..... 371
Network > Virtual Wires [ネットワーク > バーチャル ワイヤー]..... 372
Network > Virtual Routers [ネットワーク > 仮想ルーター]..... 373
仮想ルーターの一般設定..... 373
静的ルート..... 374
ルート再配信..... 377
RIP..... 378
OSPF..... 381
OSPFv3IPv6..... 386
BGP..... 392
IP マルチキャスト..... 406
ECMP..... 410
仮想ルーターの詳細ランタイム状態..... 412
Network > IPSec Tunnels [ネットワーク > IPSec トンネル]..... 424
IPSec VPN トンネル管理..... 424
IPSec トンネルの [全般] タブ..... 425
IPSec トンネルの Proxy IDs (プロキシ ID) タブ..... 427
ファイアウォールの IPSec トンネル状態..... 428
IPSec トンネルの再起動または更新..... 428
Network (ネットワーク) > GRE Tunnels (GRE トンネル)..... 430
GRE トンネル..... 430
Network > DHCP [ネットワーク > DHCP]..... 432
DHCP の概要..... 432
DHCP アドレス..... 432
DHCP サーバー..... 433
DHCP リレー..... 436
DHCP クライアント..... 437
Network > DNS Proxy [ネットワーク > DNS プロキシ]..... 438
DNS プロキシの概要..... 438
DNS プロキシ設定..... 439
その他の DNS プロキシ アクション..... 441
Network > QoS [ネットワーク > QoS]..... 442

QoS インターフェイス設定 442
QoS インターフェイスの統計情報 444
Network > LLDP [ネットワーク > LLDP] 446
LLDP の概要 446
LLDP の構成要素 446
Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) 449
Network > Network Profiles > GlobalProtect IPSec Crypto [ネットワーク > ネットワーク プロファイル]> GlobalProtect の IPSec 暗号] 449
Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ] 450
Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プロファイル > IPSec 暗号] 456
Network > Network Profiles > IKE Crypto [ネットワーク > ネットワーク プロファイル > IKE 暗号] 458
Network > Network Profiles > Monitor [ネットワーク > ネットワーク プロファイル > 監視] 459
Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理] 459
Network > Network Profiles > Zone Protection [ネットワーク > ネットワークプロファイル > ゾーンプロテクション] 461
Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > QoS 478
Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル] 480
Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル] 481
Network > Network Profiles > SD-WAN [ネットワーク > ネットワーク プロファイル > SD-WAN インターフェイス プロファイル] 483

デバイス 487
Device (デバイス) > Setup (セットアップ) 488
Device > Setup > Management [デバイス > セットアップ > 管理] 489
Device > Setup > Operations [デバイス > セットアップ > 操作] 514
SNMP モニタリングの有効化 521
Device > Setup > HSM [デバイス > セットアップ > HSM] 524
ハードウェア セキュリティ モジュール プロバイダ設定 524
HSM 認証 525
ハードウェア セキュリティ操作 525
ハードウェア セキュリティ モジュール プロバイダ設定および状態 526
ハードウェア セキュリティ モジュール状態 527
Device > Setup > Services [デバイス > セットアップ > サービス] 528
グローバルおよび仮想システムのサービスの設定 528
グローバル サービス設定 529
サービス ルートの設定での IPv4 および IPv6 のサポート 531
宛先サービス ルート 534
Device (デバイス) > Setup (セットアップ) > Interfaces (インターフェイス) 536
Device (デバイス) > Setup (セットアップ) > Telemetry (テレメトリ) 540
Device > Setup > Content-ID [デバイス > セットアップ > Content-ID] 543
Device > Setup > WildFire [デバイス > セットアップ > WildFire] 549
Device > Setup > Session [デバイス > セットアップ > セッション] 553
セッション設定 553
セッション タイムアウト 556
TCP 設定 558

復号化設定:証明書取り消しチェック 560
復号化設定:フォワード プロキシ サーバーの証明書設定 561
VPN セッション設定 562
Device > High Availability [デバイス > 高可用性] 564
HA 設定時の重要事項 564
高可用性の設定 565
Device (デバイス) > Log Forwarding Card (ログ転送カード) 575
Device > Config Audit [デバイス > 設定監査] 577
[Device] > [パスワード プロファイル] 578
ユーザー名とパスワードの要件 578
Device > Administrators [デバイス > 管理者] 580
Device > Admin Roles [デバイス > 管理者ロール] 583
Device > Access Domain [デバイス > アクセス ドメイン] 585
Device > Authentication Profile [デバイス > 認証プロファイル] 586
認証プロファイル 586
SAML Metadata Export from an Authentication Profile (認証プロファイルから SAML メタデータをエクスポートする) 593
Device > Authentication Sequence [デバイス > 認証シーケンス] 595
Device > VM Information Sources [デバイス > VM 情報の送信元] 597
VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソースを有効にするための設定 599
AWS VPC の VM 情報ソースを有効にするための設定 600
Google Compute Engine の VM 情報ソースを有効にするための設定 601
Device (デバイス) > Troubleshooting (トラブルシューティング) 603
Security Policy Match セキュリティポリシー マッチ 603
QoS ポリシー マッチ 605
Authentication Policy Match 認証ポリシー マッチ 606
復号化/SSL ポリシー マッチ 607
NAT ポリシー マッチ 608
ポリシー ベース フォワーディング ポリシー マッチ 609
DoS ポリシー マッチ 610
routing 612
Wildfire をテスト 613
Threat Vault 614
ping 614
トレース ルート 616
ログコレクタの接続性 617
外部ダイナミック リスト 618
更新サーバー 619
クラウド ロギングサービスのステータスをテスト 619
クラウド GP サービスのステータスをテスト 620
Device > Virtual Systems [デバイス > 仮想システム] 621
Device > Shared Gateways [デバイス > 共有ゲートウェイ] 624
Device (デバイス) > Certificate Management (証明書の管理) 625
Device > Certificate Management > Certificates [デバイス > 証明書の管理 > 証明書] 626
ファイアウォールおよび Panorama 証明書の管理 626
信頼できる既定証明機関の管理 631
Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロファイル] 633
Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ] 635
Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル] 637
Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP] 639

Device (デバイス) > Certificate Management (証明書の管理) > SSL Decryption Exclusion (SSL 復号化例外) 642
Device > Response Pages [デバイス > 応答ページ]....645
Device > Log Settings [デバイス > ログ設定]....648
ログの転送先の選択....648
アラーム設定の定義....651
ログのクリア....653
[Device] > [サーバー プロファイル]....654
Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SNMP トラップ]....655
Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]....657
Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]....659
Device (デバイス) > Server Profiles (サーバー プロファイル) > HTTP....661
Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow....664
Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]....666
Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+]....668
Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP]....670
Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]....673
Device (デバイス) > Server Profiles (サーバー プロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ) 674
Device > Server Profiles > DNS [デバイス > サーバー プロファイル > DNS]....678
Device (デバイス) > Server Profiles (サーバー プロファイル) > Multi Factor Authentication (多要素認証) 679
Device > Local User Database > Users [デバイス > ローカル ユーザー データベース > ユーザー]....682
Device > Local User Database > User Groups [デバイス > ローカル ユーザー データベース > ユーザー グループ]....684
Device > Scheduled Log Export [デバイス > スケジュール設定されたログのエクスポート]....685
Device > Software [デバイス > ソフトウェア]....687
Device > Dynamic Updates [デバイス > 動的更新]....689
Device > Licenses [デバイス > ライセンス]....693
Device > Support [デバイス > サポート]....695
Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]....696
マスターキーのデプロイ....697

ユーザー ID....699
Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]....700
Palo Alto Networks User-IDエージェントの設定....700
サーバーの監視....709
ユーザー マッピングのサブネットワークの許可または除外....712
Device (デバイス) > User Identification (User-ID) > Connection Security (接続のセキュリティ) 714
Device > User Identification > User-ID Agents [デバイス > User-ID > User-IDエージェント]....715
User-ID エージェントへのアクセスの設定....715
User-ID エージェントへのアクセスを管理....717
Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (ターミナルサーバー エージェント)....719
Device (デバイス) > User Identification (ユーザー ID) > Group Mapping Settings (グループマッピングの設定) タブ....721

Device > User Identification > Captive Portal Settings [デバイス > User-ID > キャプティブ ポータルの設定]....726

GlobalProtect....731
Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータル]....732
GlobalProtect ポータルの General (全般) タブ....733
GlobalProtect ポータルの Authentication (認証) タブ....734
GlobalProtect ポータルの Portal Agent Data Collection (ポータル データ収集) タブ....737
GlobalProtect ポータルの Agent (エージェント) タブ....737
GlobalProtect ポータルの Clientless VPN (クライアントレス VPN) タブ....760
GlobalProtect ポータルの Satellite (サテライト) タブ....764
Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲートウェイ]....767
GlobalProtect ゲートウェイの General (全般) タブ....767
GlobalProtect ゲートウェイの Authentication (認証) タブ....768
GlobalProtect ゲートウェイの Agent (エージェント) タブ....770
GlobalProtect ゲートウェイの Satellite (サテライト) タブ....781
Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]....785
Network > GlobalProtect > Device Block List [ネットワーク > GlobalProtect > デバイスブロックリスト]....786
Network (ネットワーク) > GlobalProtect > Clientless Apps (クライアントレス アプリケーション) 787
Network (ネットワーク) > GlobalProtect > Clientless App Groups (クライアントレス アプリケーション グループ) 788
Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オブジェクト]....789
HIP オブジェクトの General (全般) タブ....789
HIP オブジェクトの Mobile Device (モバイル デバイス) タブ....791
HIP オブジェクトの Patch Management (パッチ管理) タブ....793
HIP オブジェクトの Firewall (ファイアウォール) タブ....793
HIP オブジェクトの Anti-Malware (アンチマルウェア) タブ....794
HIP オブジェクトの Disk Backup (ディスク バックアップ) タブ....795
HIP オブジェクトの Disk Encryption (ディスク暗号化) タブ....795
HIP オブジェクトの Data Loss Prevention (データ損失防止) 796
HIP オブジェクトの Certificate (証明書) タブ....796
HIP オブジェクトの Custom Checks (カスタム チェック) タブ....797
Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP プロファイル]....798
Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]....800
GlobalProtect アプリ ソフトウェアの管理....800
GlobalProtect アプリのセットアップ....802
GlobalProtect アプリの使用....802

Panorama Web インターフェイス....803
Panorama Web インターフェイスを使用する....804
コンテキスト切り替え....809
Panorama のコミット操作....810
Panorama でのポリシーの定義....819
レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティション....821
Panorama > Setup (セットアップ) > Interfaces (インターフェイス) 823
Panorama > High Availability [Panorama > 高可用性]....826

Panorama > Managed WildFire Clusters (管理対象 WildFire クラスタ) 829
管理対象 WildFire クラスタのタスク.....829
管理対象 WildFire アプライアンスのタスク.....830
管理対象 WildFire の情報.....831
管理対象 WildFire クラスタおよびアプライアンスの管理.....835
Panorama > Administrators [Panorama > 管理者].....846
Panorama > Admin Roles [Panorama > 管理者ロール].....849
Panorama > Access Domains [Panorama > アクセス ドメイン].....851
Panorama > Managed Devices (管理対象デバイス) 853
管理対象ファイアウォールの管理.....853
管理対象ファイアウォールの情報.....854
ファイアウォールのソフトウェアとコンテンツの更新..... 858
ファイアウォールのバックアップ.....859
Panorama > Managed Devices (管理対象デバイス) > Health (健康状態) 860
Detailed Device Health on Panorama (Panorama のデバイス健康状態詳細) 862
Panorama > Templates [Panorama > テンプレート].....866
テンプレート.....866
テンプレート スタック..... 867
Panorama > Templates (テンプレート) > Template Variables (テンプレートの変数) 868
Panorama > Device Groups [Panorama > デバイス グループ]..... 871
Panorama > Managed Collectors [Panorama > 管理対象コレクタ]..... 873
ログ コレクタの情報.....873
ログ コレクタの設定.....874
専用ログ コレクタのソフトウェアの更新.....883
Panorama > Collector Groups [Panorama > コレクタ グループ]..... 885
コレクタ グループの設定..... 885
コレクタグループの情報.....891
Panorama > Plugins (プラグイン) 892
Panorama > VMware NSX..... 893
通知グループの設定..... 893
サービス定義を作成する.....894
NSX Manager へのアクセスの設定.....895
ステアリング ルールの作成.....897
Panorama > Log Ingestion Profile (ログ インジェスト プロファイル) 899
Panorama > Log Settings [Panorama > ログ設定]..... 900
Panorama > Scheduled Config Export [Panorama > スケジュール設定された設定のエクスポート].....902
Panorama > Software [Panorama > ソフトウェア].....904
Panorama ソフトウェア更新の管理.....904
Panorama ソフトウェア更新情報の表示..... 905
Panorama > Device Deployment [Panorama > デバイスのデプロイ]..... 906
ソフトウェアおよびコンテンツ更新の管理.....906
ソフトウェアおよびコンテンツ更新情報の表示..... 909
コンテンツ用動的更新のスケジュール設定.....910
Panorama でコンテンツ バージョンを元に戻す..... 911
ファイアウォールのライセンス管理..... 912

Web インターフェイスの基本

以下のトピックでは、ファイアウォールの概要と、基本的な管理タスクについて説明します。

- ファイアウォールの概要
- 機能と利点
- 前回のログイン時間およびログイン試行回数
- 当日のメッセージ
- タスク マネージャ
- 言語
- アラーム
- 変更のコミット
- 候補設定の保存
- 変更を元に戻す
- 設定のロック
- Global Find
- 脅威詳細
- AutoFocus インテリジェンス サマリー

ファイアウォールの概要

Palo Alto Networks® の次世代ファイアウォールはすべてのトラフィック（アプリケーション、脅威、コンテンツを含む）を検査し、ロケーションやデバイス タイプに関わらずそのトラフィックをユーザーに紐付けます。ユーザー、アプリケーション、コンテンツ（いずれも事業活動に欠かせない要素）はエンタープライズ セキュリティ ポリシーの設定に不可欠な要素になっています。これにより、ビジネス ポリシーに合わせてセキュリティを調整したり、理解・管理しやすいルールを作成することができるようになります。

お客様の組織は当社のセキュリティ オペレーティング プラットフォームの一環である次世代ファイアウォールを使って次のことを実現できます：

- すべてのトラフィック（ポートにかかわらず）を分類化することで、アプリケーション（SaaS アプリケーションを含む）、ユーザー、コンテンツのセキュリティを向上できます。
- ポジティブ エンフォースメント モデルにより、すべての目的のアプリケーションを許可して他をすべてブロックすることで攻撃の入り口を減らせます。
- セキュリティ ポリシーを適用して既知の脆弱性を狙ったエクスプロイト、ウイルス、ランサム攻撃ボット、スパイウェア、ボットネット、APT 攻撃などのその他の未知のマルウェアをブロックできます。
- データおよびアプリケーションをセグメント化し、ゼロ トラストの原則を適用することでデータセンター（仮想化されたデータセンターを含む）を保護できます。
- オンプレミスおよびクラウド環境全体で一貫したセキュリティを適用できます。
- 場所に関係なくユーザやデバイスに、セキュリティ オペレーティング プラットフォームを拡張することにより、安全なモバイル コンピューティングを導入できます。
- 一元的な可視性を実現してネットワーク セキュリティを合理化することでデータを操作可能にし、サイバー攻撃を防ぐことができます。
- 有効な企業の認証情報を不正なウェブサイトに送信すること、攻撃者が盗んだ認証情報を使って横方向に移動することを防ぎ、またネットワーク層に認証ポリシーを適用することでネットワークのセキュリティ侵害を防ぐことで、認証情報を盗もうとする試みを把握・防止します。

© 2019 Palo Alto Networks, Inc.

機能と利点

Palo Alto Networks の次世代ファイアウォールでは、ネットワークへのアクセスを許可されたトラフィックを詳細に制御できます。主な機能と利点は、以下のとおりです。

- アプリケーションベースでのポリシーの適用 (**App-ID™**) – アプリケーション タイプに従ってアクセスを制御すると、プロトコルとポート番号以外の情報にも基づいてアプリケーションが識別されるため、アクセス制御の効果が大幅に向上します。App-ID サービスはリスクの高いアプリケーションをブロックできるだけでなく、ファイル共有など、リスクの高い動作もブロックできます。また、Secure Socket Layer (SSL) プロトコルで暗号化されたトラフィックの暗号を解読して検査できます。
- ユーザー **ID (User-ID™)** – ユーザー ID 機能により管理者は、ネットワーク ゾーンとアドレスの代わりに (またはこれらに加えて)、ユーザーとユーザー グループに基づいてファイアウォール ポリシーを設定および適用できます。ファイアウォールは、Microsoft Active Directory、eDirectory、SunOne、OpenLDAP、および他のほとんどの LDAP ベースのディレクトリ サーバーなど、多くのディレクトリ サーバーと通信して、ユーザーとグループの情報をファイアウォールに提供できます。この情報を使用して、アプリケーションの安全な運用をユーザーまたはグループ単位で定義できます。たとえば管理者は、ある Web ベース アプリケーションの使用を会社内の 1 つの組織に許可し、それ以外の組織に許可しないことができます。また、ユーザーおよびグループに基づいてアプリケーションの特定のコンポーネントをよりきめ細かく制御するように設定することもできます (「User-ID」を参照)。
- 脅威阻止 – ウイルス、ワーム、スパイウェア、およびその他の悪意のあるトラフィックからネットワークを保護する脅威阻止サービスを、アプリケーションとトラフィックの送信元ごとに変えることもできます (「Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル)」を参照)。
- **URL** フィルタリング – アウトバウント接続をフィルタリングして、不適切な Web サイトへのアクセスの阻止もできます (「Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL フィルタリング)」を参照)。
- トラフィックの可視性 – 幅広いレポート、ログ、および通知メカニズムにより、ネットワーク アプリケーション トラフィックとセキュリティ イベントを詳細に観察できます。Web インターフェイスの Application Command Center (ACC) を使用して、トラフィック量が最大のアプリケーションや、セキュリティ リスクが最も高いアプリケーションを特定します (「監視」を参照)。
- 多機能なネットワーキングと速度 – Palo Alto Networks のファイアウォールは、既存のファイアウォールを補完したり、置き換えたりできます。また、どのネットワークにも透過的にインストールでき、スイッチまたはルーティング環境をサポートするように設定できます。マルチギガビットの速度と単一パス アーキテクチャの実現により、ネットワーク遅延にほとんどまたはまったく影響することなく、これらのサービスが提供されます。
- **GlobalProtect** – GlobalProtect™ ソフトウェアは、世界中のどこからでも簡単かつ安全にログインできるようにすることで、現場で使用されるノートパソコンなどのクライアント システムでセキュリティを確保します。
- フェールセーフ機能 – 高可用性 (HA) のサポートにより、ハードウェアやソフトウェアに障害が発生した場合に自動的にフェイルオーバーが実行されます (「Device (デバイス) > Virtual Systems (仮想システム)」を参照)。
- マルウェアの分析とレポート – WildFire™ クラウドベース分析サービスは、ファイアウォールを通過するマルウェアの詳細な分析とレポートを提供します。AutoFocus™ の脅威インテリジェンス サービスとの統合により、組織、業界、グローバル レベルのネットワーク トラフィックに関連するリスクを評価できます。
- **VM-Series** ファイアウォール – VM-Series ファイアウォールは仮想データ センター環境での利用に適した PAN-OS® 仮想インスタンスを提供し、プライベート、パブリック、およびハイブリッドのクラウド コンピューティング環境にとって理想的です。
- 管理および **Panorama** – 各ファイアウォールを直観的な Web インターフェイスまたはコマンドライン インターフェイス (CLI) によって管理できます。また、Palo Alto Networks ファイアウォールの

© 2019 Palo Alto Networks, Inc.

Web インターフェイスと非常によく似た Web インターフェイスを備えた Panorama™ 中央管理システムで、すべてのファイアウォールを一元的に管理することができます。

© 2019 Palo Alto Networks, Inc.

前回のログイン時間およびログイン試行回数

Palo Alto NetworksのファイアウォールやPanoramaの管理者アカウントなど権限付きのアカウントの不正使用を検知して悪用を予防する為、WebインターフェイスとCLI（コマンドラインインターフェイス）には、前回のログイン時間、およびお客様のユーザーネームで行われたログイン試行回数がログイン時に表示されます。これにより、誰かがあなたの管理者認証情報を使用して攻撃しようとしている場合はすぐにそれを知ることができます。

Webインターフェイスへログインすると、前回のログイン日時がウィンドウの左下に表示されます。前回のログイン以降、1回以上ログインに失敗している場合は前回のログイン日時の右側に警告アイコンが表示されます。ログインの試行回数を確認する場合は、警告アイコンにカーソルを合わせるか、**Failed Login Attempts Summary**（ログイン試行回数のサマリー）ウィンドウを開きます（ここには管理者アカウント名、送信元 IP アドレス、ログイン失敗の理由が表示されます）。

自分が行っていないログイン試行が複数回あった場合、ネットワーク管理者の協力のもと、総当たり攻撃を行っているシステムを特定し、ユーザーとホストコンピューターの検証を行い、悪意のある活動を特定して排除します。前回のログイン表示によりアカウントに対する不正アクセスが確認された場合は、直ちにパスワードの変更と設定の検証を行い、設定内容に不審な変更点が無いか確認してください。自分のアカウントを使用してログが削除された、あるいは不正に変更されたかどうか判別が難しい場合は、元の正しい設定に戻してください。

© 2019 Palo Alto Networks, Inc.

当日のメッセージ

管理者が「本日のメッセージ」を設定した場合や、Palo Alto Networks のソフトウェアやコンテンツ リリースに本日のメッセージが組み込まれている場合、ユーザーが Web インターフェイスにログインすると「本日のメッセージ」ダイアログが自動的に表示されます。システムの再起動が迫っている場合など、ユーザーが実行しようとするタスクに影響する、重要な情報を表示します。

1つのページにつき1つのメッセージが表示されます。ダイアログに **Do not show again**（今後は表示しない）というオプションが含まれている場合、以降のログイン時に表示したくないメッセージを非表示にすることができます。

Message of the Day（本日のメッセージ）に少しでも変更が加えられると、前回のログイン時に *Do not show again*（今後は表示しない）を選択した場合でも、次回のセッションで当該のメッセージが表示されます。変更されたメッセージを以降のセッションで表示したくない場合は、再度このオプションを選択する必要があります。

ダイアログページ内を移動する場合、ダイアログの側面に表示されている右向き（▶）と左向き（◀）の矢印をクリックするか、ダイアログ下部に表示されているページセレクター（●○）をクリックします。ダイアログの**Close**[閉じる] を選択した場合は、Webインターフェイスの下部に表示されたメッセージ（✉）をクリックすることで再び開くことができます。

本日のメッセージの設定を行う場合は、**Device**（デバイス）> **Setup**（設定）> **Management**（管理）を開き、バナーとメッセージの設定を編集します。

© 2019 Palo Alto Networks, Inc.

タスク マネージャ

前回ファイアウォールが再起動してから自分や他の管理者、または PAN-OS が開始したタスク（たとえば、手動コミットや自動 FQDN 更新）を表示する場合は、Web インターフェイス下部の **Tasks**（タスク）をクリックします。タスク マネージャでは、以下の表に記載されている各タスクの情報を表示したりアクション実行したりできます。

一部の列はデフォルトでは非表示です。特定の列の表示/非表示の切り替えは、列の見出しにあるドロップダウン リストを開き、*Columns*（列）を選択して、列名を選択（表示）または選択解除（非表示）します。

フィールド/ボタン	の意味
	タスクをフィルタリングするには、いずれかの列の値に基づくテキスト文字列を入力して、Apply Filter（フィルタの適用）（ ）を行います。たとえば、「**edl**」と入力すると、リストがフィルタリングされて EDLFetch（外部動的リストの取得）タスクのみ表示されます。フィルタリングを解除するには、Remove Filter（フィルタの削除）（ ）を行います。
タイプ	タスクのタイプ（ログ要求、ライセンス更新、またはコミットなど）です。タスクに関連する情報（警告など）が長すぎて Messages（メッセージ）列に収まらない場合、Type（タイプ）の値をクリックすると詳細のすべてが表示されます。
ステータス	タスクが、保留中（Queued（キュー追加済み）状態のコミットなど）、進行中（Active（アクティブ）状態のログ要求など）、完了、または失敗かどうかを示します。進行中のコミットの場合、このステータスには進行状況がパーセントで表示されます。
ジョブ ID	タスクを識別するための数字です。CLI でジョブ ID を使用すると、タスクのその他の詳細を確認できます。たとえば、コミット キューにあるコミット タスクの順番を確認するには、以下のように入力します。 `> show jobs id <job-id>` この列はデフォルトでは非表示です。
終了時間	タスクが終了した日時を示します。この列はデフォルトでは非表示です。
開始時間	タスクが開始した日時を示します。コミット タスクの場合、開始時間はコミットがコミット キューに追加された日時を示します。
メッセージ	タスクの詳細を表示します。エントリのメッセージが多すぎる場合、タスクの Type（タイプ）をクリックするとメッセージを表示できます。 コミット タスクの場合、PAN-OS がコミット処理を開始した時間が分かるように、コミットがキューから外された時間がメッセージに含まれます。コミットに対し管理者が入力した説明文を表示する場合は**Commit**

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	Description [コミットの詳細] をクリックします。詳細は、「変更のコミット」を参照してください。
操作	管理者または PAN-OS が開始した保留中のコミットをキャンセルする場合、**x** をクリックします。このボタンを使用できるのは、事前定義済みのロールである、スーパーユーザー、デバイス管理者、仮想システム管理者、Panorama 管理者のいずれかの権限を持つ管理者のみです。
表示	表示するタスクを次から選択します。 • **All Tasks**（すべてのタスク）（デフォルト） • 特定のタイプの **All**（すべて）のタスク（**Jobs**（ジョブ）、**Reports**（レポート）、または **Log Requests**（ログ要求）） • すべての **Running**（実行中）のタスク（進行中） • 特定のタイプのすべての **Running**（実行中）のタスク（**Jobs**（ジョブ）、**Reports**（レポート）、または **Log Requests**（ログ要求）） • （Panorama のみ）2 つ目のドロップダウン リストを使用して、**Panorama**（デフォルト）または特定の管理対象ファイアウォールのタスクを表示できます。
コミットキューのクリア	管理者または PAN-OS が開始した保留中のコミットをすべてキャンセルします。このボタンを使用できるのは、事前定義済みのロールである、スーパーユーザー、デバイス管理者、仮想システム管理者、Panorama 管理者のいずれかの権限を持つ管理者のみです。

© 2019 Palo Alto Networks, Inc.

言語

デフォルトでは、ファイアウォールにログインするために使用されるコンピュータに設定されている言語によって、管理 Web インターフェイスに表示される言語が決まります。言語を手動で変更する場合は**Language**（言語）をクリックし、Web インターフェイスの右下にあるドロップダウンリストから言語を選択し、**OK**をクリックします。Web インターフェイスが更新されると、選択した言語で Web インターフェイスが表示されます。

対応言語：フランス語、日本語、スペイン語、簡体中国語、繁体中国語。

© 2019 Palo Alto Networks, Inc.

アラーム

アラームとはファイアウォールが生成する、特定のイベント タイプ (暗号化や復号化の失敗など) の発生回数が、そのイベント タイプに設定されたしきい値を超えたことを示すメッセージです (「アラーム設定の定義」を参照) 。アラームを生成する際、ファイアウォールはアラームログを作成し、システムアラームダイアログを開き、アラームを表示します。ダイアログを閉じた場合は、Web インターフェイスの下部に表示された **Alarms** (アラーム) ( ) をクリックすることで再び開くことができます。ファイアウォールが特定のアラームのダイアログを自動的に開かないようにする場合は、Unacknowledged Alarms [未承認のアラーム] を選択し、**Acknowledge** [承認] をクリックし、アラームをAcknowledged Alarms [承認済みアラーム] 一覧に移動します。

© 2019 Palo Alto Networks, Inc.

変更のコミット

Web インターフェイスの右上にある **Commit**（コミット）をクリックして、ファイアウォール設定の保留中の変更に対する操作：commit (activate), validate, or preview 管理者や場所に基づいてフィルタリングした保留中の変更をプレビュー、検証、コミットできます。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。

ファイアウォールはコミット作業をキューで処理するので、前回のコミットの進行中に新しいコミットを追加することができます。ファイアウォールは追加順にコミットを実行しますが、FQDN 更新など、ファイアウォールによって開始されるオートコミットを優先します。ただし、管理者が開始したコミットが既にキューの上限まで追加されている場合、ファイアウォールが保留中のコミットの処理を終えるまで待機してから、新しいコミットを開始する必要があります。

コミットをキャンセルする場合や、保留中、実行中、完了済み、あるいは失敗したコミットの詳細を表示する場合は、タスク マネージャを使用します。

Commit（コミット）ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
すべての変更のコミット	管理権限対象のすべての変更をコミットします（デフォルト）。このオプションを選択している場合、ファイアウォールがコミットする設定変更の範囲を手動でフィルタリングできません。代わりに、ログインに使用しているアカウントに割り当てられた管理者ロールによって、コミット スコープが指定されます。 • **Superuser role**（スーパーユーザー ロール）– ファイアウォールはすべての管理者の変更をコミットします。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によって、コミット スコープが異なります（「Device（デバイス）> Admin Roles（管理者ロール）」を参照）。プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれている場合、ファイアウォールはあらゆる管理者が設定した変更をコミットします。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれていない場合、ファイアウォールは本人の変更のみをコミットして、他の管理者の変更はコミットしません。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインをコミット スコープのフィルタリングに自動的に適用します（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理ロールの種類に関係なく、ファイアウォールはアカウントに割り当てられたアクセス ドメインの設定変更のみをコミットします。
指定対象による変更のコミット	ファイアウォールがコミットする設定変更の範囲をフィルタリングします。ログインに使用しているアカウントに割り当てられた管理ロールによって、フィルタリング オプションが決まります。 • **Superuser role**（スーパーユーザー ロール）– 特定の管理者による変更や、特定の場所における変更へとコミット スコープを制限できます。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によって、フィルタリング オプションが異なります（「Device（デバイス）> Admin Roles（管理者ロー

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	ル）」を参照）。プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれている場合、特定の管理者による変更や特定の場所における変更に、コミット スコープを制限できます。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれていない場合、コミット スコープは、本人が特定の場所で加えた変更にしか制限できません。 コミット スコープを以下のようにフィルタリングします。 • **Filter by administrator**（管理者によるフィルタリング）— 他の管理者の変更をコミットできるロールの場合でも、デフォルトでコミット スコープに含まれているのは本人の変更のみです。他の管理者をコミット スコープに追加するには、**<usernames>**（ユーザー名）リンクをクリックして、管理者を選択し、**OK** をクリックします。 • **Filter by location**（場所によるフィルタリング）— 変更の特定の場所を選択して、Include in Commit（コミットに含める）を有効にします。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインに基づいてコミット スコープを自動的にフィルタリングします（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理ロールやフィルタリングの選択に関係なく、コミット スコープにはアカウントに割り当てられたアクセス ドメインの設定変更のみが含まれます。 設定をロードした（Device（デバイス）> Setup（セットアップ）> Operations（操作））後、*Commit All Changes*（すべての変更のコミット）を行ってください。 仮想システムへの変更をコミットする場合、その仮想システムの同じルールベースのルールの追加、削除、位置変更を行ったすべての管理者の変更を含める必要があります。
コミット スコープ	コミットする変更を含む場所を一覧表示します。リストに含まれるのが変更のすべてであるか一部であるかは、複数の要因が影響します。詳細は、「Commit All Changes（すべての変更のコミット）」および「Commit Changes Made By（指定対象による変更のコミット）」に記載されています。場所の種類は以下のとおりです。 • **shared-object**（共有オブジェクト）— 共有の場所で定義されている設定です。 • **policy-and-objects**（ポリシーとオブジェクト）— マルチ仮想システムが存在しないファイアウォールで定義されているポリシー ルールまたはオブジェクトです。 • **device-and-network**（デバイスとネットワーク）— グローバルであり（インターフェイス管理プロファイルなど）、仮想システム専用でないネットワークおよびデバイス設定です。マルチ仮想システムが存在しないファイアウォールのネットワークおよびデバイス設定にも適用されます。 • **<virtual-system>**（仮想システム）— マルチ仮想システムを含むファイアウォールの、ポリシー ルールまたはオブジェクトが定義されて

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	いる仮想システムの名前です。仮想システム専用のネットワークおよびデバイス設定（ゾーンなど）も含まれます。
場所タイプ	この列では保留中の変更の場所が分類されます。 • **Virtual Systems**（仮想システム）— 特定の仮想システムで定義されている設定です。 • **Other Changes**（その他の変更）— 仮想システム専用でない設定です（共有オブジェクトなど）。
コミットに含める （部分的なコミットのみ）	コミットする変更を選択できます。デフォルトでは、**Commit Scope**（コミット スコープ）のすべての変更が選択されています。この列は、特定の管理者に基づく **Commit Changes Made By**（指定対象による変更のコミット）を選択しないと表示されません。 依存関係が、コミットに含める変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更のコミットは、自身の変更も合わせてコミットしない限りできません。
場所タイプ別グループ	**Commit Scope**（コミット スコープ）の設定変更のリストを **Location Type**（場所タイプ）別にグループにします。
プレビューの変更	**Commit Scope**（コミット スコープ）で選択した設定を、実行中の設定と比較できるようにします。プレビュー ウィンドウでは色分けによって詳細が示されます（追加は緑色、変更は黄色、削除は赤色）。 Web インターフェイスのセクションへの変更を一致させる場合、変更前後の **Lines of Context**（コンテキストの行）を表示するようにプレビュー ウィンドウを設定できます。これらは候補のファイルと、比較対象である実行中の設定から取得されます。 プレビュー結果は新しいブラウザ ウィンドウで表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビュー ウィンドウが開かない場合は、ポップアップを許可する手順についてブラウザのドキュメントを参照してください。
変更サマリー	変更をコミットする個別の設定を一覧表示します。**Change Summary**（変更サマリー）のリストでは、各設定の以下の情報が表示されます。 • **Object Name**（オブジェクト名）— ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。 • **Type**（タイプ）— 設定のタイプ（アドレス、セキュリティ ルール、ゾーンなど）です。 • **Location Type**（場所タイプ）— 設定が仮想システムで定義されているかどうかを示します。 • **Location**（場所）— 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列に **Shared**（共有）と表示されます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **Operations**（操作）– 最後のコミット以降、設定に実施された各操作（作成、編集、または削除）を示します。 • **Owner**（オーナー）– 設定に直近の変更を加えた管理者です。 • **Will Be Committed**（コミット予定）– 現在、設定がコミットに含まれているかを示します。 • **Previous Owners**（前回のオーナー）– 直近の変更前に、設定を変更した管理者です。 必要に応じて、**Group By**（グループ化基準）を列名（**Type**（タイプ）など）にできます。 変更リストでオブジェクトを選択し、 **Object Level Difference** (オブジェクトレベルの差)を表示します。
コミットの検証	ファイアウォール設定の構文が正しく、意味が完全かどうかを検証します。出力には、コミットが表示するであろうエラーや警告が含まれます。これにはルール シャドウイングやアプリケーション依存関係の警告があります。検証プロセスを利用すると、エラーを検出、修正してからコミットできます（実行中の設定は変更されません）。固定のコミット ウィンドウがあり、エラーなしでコミットを確実に実行したい場合に便利です。
の意味	他の管理者に変更内容を示すための説明（最大 512 文字）を入力できます。 コミット イベントのシステム ログでは、*512* 文字を超える説明は切り捨てられます。
コミットする	コミットを開始します。他のコミットが保留中の場合は、コミットはコミット キューに追加されます。
コミット状態	コミット中に進行状況を提供し、コミット後に結果を提供します。コミットの結果には、成功または失敗、コミットの変更の詳細、およびコミットの警告が含まれます。以下の警告があります。 • **Commit** (コミット)–一般コミット警告を一覧表示します。 • **App Dependency** (アプリケーションの依存関係)–既存のルールに必要なアプリケーションの依存関係を一覧表示します。 • **Rule Shadow** (ルール シャドウ)–シャドウ ルールを一覧表示します。

© 2019 Palo Alto Networks, Inc.

候補設定の保存

設定候補の新しいスナップショット ファイルを保存するか、既存の設定ファイルを上書きする場合は、ファイアウォールまたは Panorama Web インターフェイスの右上にある **Config**（設定）> **Save Changes**（変更の保存）を選択します。変更内容をコミットする前にファイアウォールまたは Panorama が再起動した場合、保存したスナップショットに設定候補を戻して、前回のコミット後の変更を復元できます。スナップショットに戻すには、**Device**（デバイス）> **Setup**（セットアップ）> **Operations**（操作）で **Load named configuration snapshot**（名前付き設定スナップショットのロード）を選択します。再起動後に設定内容をスナップショットに戻さない場合、候補設定は前回コミットした設定内容（実行中の設定）のまま維持されます。

管理者または場所に基づいて、どの設定の変更を保存するかをフィルタリングできます。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。

ファイアウォールや *Panorama* が再起動しても変更内容が失わないために変更を定期的に保存してください。

変更を候補設定に保存しても、それらの変更は有効にはなりません。有効にするには変更をコミットする必要があります。

Save Changes（変更の保存）ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
Save All Changes（すべての変更の保存）	管理特権対象のすべての変更を保存します（デフォルト）。このオプションを選択している場合、手動ではファイアウォールが保存する設定変更の範囲をフィルタリングできません。代わりに、ログインに使用しているアカウントに割り当てられた管理者ロールによって、保存範囲が指定されます。 • **Superuser role**（スーパーユーザー ロール）– ファイアウォールは管理者全員の変更を保存します。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によって、保存範囲が異なります（「Device（デバイス）> Admin Roles（管理者ロール）」を参照）。プロファイルに **Save For Other Admins**（他の管理者向けの保存）の権限が含まれている場合、ファイアウォールはあらゆる管理者が設定した変更を保存します。管理者ロール プロファイルに **Save For Other Admins**（他の管理者向けの保存）の権限が含まれていない場合、ファイアウォールは本人の変更のみを保存して、他の管理者の変更は保存しません。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインを、保存範囲のフィルタリングに自動的に適用します（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理ロールの種類に関係なく、ファイアウォールはアカウントに割り当てられたアクセス ドメインの設定変更のみを保存します。
Save Changes Made By（指定対象による変更の保存）	ファイアウォールが保存する設定変更の範囲をフィルタリングします。ログインに使用しているアカウントに割り当てられた管理ロールによって、フィルタリング オプションが決まります。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **Superuser role**（スーパーユーザー ロール）— 特定の管理者による変更や、特定の場所における変更へと保存範囲を制限できます。 • **Custom role**（カスタム ロール）— アカウントに割り当てられた管理者ロール プロファイルの権限によって、フィルタリング オプションが異なります（「Device（デバイス）> Admin Roles（管理者ロール）」を参照）。プロファイルに **Save For Other Admins**（他の管理者向けの保存）の権限が含まれている場合、特定の管理者による変更や特定の場所における変更へと、保存範囲を制限できます。管理者ロール プロファイルに **Save For Other Admins**（他の管理者向けの保存）の権限が含まれていない場合、保存範囲は、本人が特定の場所で加えた変更にしか制限できません。 保存範囲を以下のようにフィルタリングします。 • **Filter by administrator**（管理者によるフィルタリング）— 他の管理者の変更を保存できるロールの場合でも、デフォルトで保存範囲に含まれているのは本人の変更のみです。他の管理者を保存するスコープに追加するには、**<usernames>**（ユーザー名）リンクをクリックして、管理者を選択し、**OK** をクリックします。 • **Filter by location**（場所によるフィルタリング）— 特定の場所の変更を選択して、Include in Save（保存に含める）を有効にします。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインに基づいて、保存範囲を自動的にフィルタリングします（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理ロールやフィルタリングの選択に関係なく、保存範囲にはアカウントに割り当てられたアクセス ドメインの設定変更のみが含まれます。
Save Scope（保存範囲）	保存する変更を含む場所を一覧表示します。リストに含まれるのが変更のすべてであるか一部であるかは、複数の要因が影響します。詳細は、「Save All Changes（すべての変更の保存）」および「Save Changes Made By（指定対象による変更の保存）」に記載されています。場所の種類は以下のとおりです。 • **shared-object**（共有オブジェクト）— 共有の場所で定義されている設定です。 • **policy-and-objects**（ポリシーとオブジェクト）—（ファイアウォールのみ）マルチ仮想システムを含まないファイアウォールで定義されているポリシー ルールまたはオブジェクトです。 • **device-and-network**（デバイスとネットワーク）—（ファイアウォールのみ）グローバルであり（インターフェイス管理プロファイルなど）、仮想システム専用でないネットワークおよびデバイス設定です。 • **<virtual-system>**（仮想システム）—（ファイアウォールのみ）マルチ仮想システムを含むファイアウォールの、ポリシー ルールまたはオブジェクトが定義されている仮想システムの名前です。仮想システム専用のネットワークおよびデバイス設定（ゾーンなど）も含まれます。 • **<device-group>**（デバイス グループ）—（Panorama のみ）ポリシー ルールまたはオブジェクトが定義されているデバイス グループの名前です。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **<template>** – （Panorama のみ）設定が定義されているテンプレートまたはテンプレート スタックの名前です。 • **<log-collector-group>** – （Panorama のみ）設定が定義されているコレクタ グループの名前です。 • **<log-collector>** – （Panorama のみ）設定が定義されているログ コレクタの名前です。
場所タイプ	この列では変更が行われた場所が分類されます。 • **Virtual Systems**（仮想システム）– （ファイアウォールのみ）特定の仮想システムで定義されている設定です。 • **Device Groups**（デバイス グループ）– （Panorama のみ）特定のデバイス グループで定義されている設定です。 • **Templates**（テンプレート）– （Panorama のみ）特定のテンプレートまたはテンプレート スタックで定義されている設定です。 • **Collector Groups**（コレクタ グループ）– （Panorama のみ）コレクタ グループ設定固有の設定です。
Include in Save（保存に含める） （一部の保存のみ）	保存する変更を選択できます。デフォルトでは、**Save Scope**（保存範囲）のすべての変更が選択されています。この列は、特定の管理者に基づく **Save Changes Made By**（指定対象による変更の保存）を選択しないと表示されません。 依存関係が、保存に含まれる変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更の保存は、自身の変更も合わせて保存しない限りできません。
場所タイプ別グループ	**Save Scope**（保存範囲）の設定変更のリストを **Location Type**（場所タイプ）別にグループ化します。
プレビューの変更	**Save Scope**（保存範囲）で選択した設定を、実行中の設定と比較できるようにします。プレビュー ウィンドウでは色分けによって詳細が示されます（追加は緑色、変更は黄色、削除は赤色）。 Web インターフェイスのセクションへの変更を一致させる場合、変更前後の **Lines of Context**（コンテキストの行）を表示するようにプレビュー ウィンドウを設定できます。これらは候補のファイルと、比較対象である実行中の設定から取得されます。 プレビュー結果は新しいウィンドウで表示されるので、ブラウザーでポップアップを許可しておく必要があります。プレビューウィンドウが開かない場合はブラウザ設定を参照し、ポップアップブロックの解除を行ってください。
変更サマリー	変更を保存する個別の設定を一覧表示します。**Change Summary**（変更サマリー）のリストでは、各設定の以下の情報が表示されます。 • **Object Name**（オブジェクト名）– ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **Type**（タイプ）— 設定のタイプ（アドレス、セキュリティ ルール、ゾーンなど）です。 • **Location Type**（場所タイプ）— 設定が仮想システムで定義されているかどうかを示します。 • **Location**（場所）— 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列に **Shared**（共有）と表示されます。 • **Operations**（操作）— 最後のコミット以降、設定に実施された各操作（作成、編集、または削除）を示します。 • **Owner**（オーナー）— 設定に直近の変更を加えた管理者です。 • **Will Be Saved**（保存予定）— 保存作業に設定が含まれる予定かどうかを示します。 • **Previous Owners**（前回のオーナー）— 直近の変更前に、設定を変更した管理者です。 必要に応じて、**Group By**（グループ化基準）を列名（**Type**（タイプ）など）にできます。
Save[保存]	選択した変更を、設定スナップショット ファイルに保存します。 • **Save All Changes**（すべての変更の保存）を選択した場合、ファイアウォールはデフォルトの設定スナップショット ファイル（.snapshot.xml）を上書きします。 • **Save Changes Made By**（指定対象による変更の保存）を選択した場合、新しい設定ファイルまたは既存の設定ファイルの **Name**（名前）を指定して、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

変更を元に戻す

前回のコミット以降に候補設定に対して加えた変更を元に戻す場合は、ファイアウォールまたは Panorama Web インターフェイスの右上にある **Config**（設定）> **Revert Changes**（変更を元に戻す）を選択します。変更を元に戻すと、その設定が実行中の設定の値に復元されます。管理者または場所に基づいて、どの設定の変更を元に戻すかをフィルタリングできます。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。

ファイアウォールまたは Panorama が保留中または進行中のすべてのコミットの処理を完了するまで、変更は元に戻せません。元に戻すプロセスを開始すると、ファイアウォールまたは Panorama が自動的に候補と実行中の設定をロックするため、他の管理者は設定を変更したり、変更をコミットしたりできません。元に戻すプロセスが完了すると、ファイアウォールまたは Panorama が自動的にロックを解除します。

Revert Changes（変更を元に戻す）ダイアログには、以下の表に記載されているオプションが表示されます。

フィールド/ボタン	の意味
Revert All Changes（すべての変更を元に戻す）	管理特権対象のすべての変更を元に戻します（デフォルト）。このオプションを選択している場合、手動ではファイアウォールが元に戻す設定変更の範囲をフィルタリングできません。代わりに、ログインに使用しているアカウントに割り当てられた管理者ロールによって、元に戻す範囲が指定されます。 • **Superuser role**（スーパーユーザー ロール）– ファイアウォールは管理者全員の変更を元に戻します。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によって、元に戻す範囲が異なります（「Device（デバイス）> Admin Roles（管理者ロール）」を参照）。プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれている場合、ファイアウォールはあらゆる管理者が設定した変更を元に戻します。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれていない場合、ファイアウォールは本人の変更のみを元に戻して、他の管理者の変更は元に戻しません。 管理者ロール プロファイルでは、コミットの権限が元に戻す権限にも適用されます。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインを、元に戻す範囲のフィルタリングに自動的に適用します（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理者ロールの種類に関係なく、ファイアウォールはアカウントに割り当てられたアクセス ドメインの設定変更のみを元に戻します。
Revert Changes Made By（指定対象に基づいて変更を元に戻す）	ファイアウォールが元に戻す設定変更の範囲をフィルタリングします。ログインに使用しているアカウントに割り当てられた管理ロールによって、フィルタリング オプションが決まります。 • **Superuser role**（スーパーユーザー ロール）– 特定の管理者による変更や、特定の場所における変更へと元に戻す範囲を制限できます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によって、フィルタリング オプションが異なります（「Device（デバイス）> Admin Roles（管理者ロール）」を参照）。プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれている場合、特定の管理者による変更や特定の場所における変更へと、元に戻す範囲を制限できます。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれていない場合、元に戻す範囲は、本人が特定の場所で加えた変更にしか制限できません。 元に戻す範囲を以下のようにフィルタリングします。 • **Filter by administrator**（管理者によるフィルタリング）– 他の管理者の変更を元に戻せるロールの場合でも、デフォルトで元に戻す範囲に含まれているのは本人の変更のみです。元に戻す範囲の指定を他の管理者を追加するには、**<usernames>**（ユーザー名）リンクをクリックして、管理者を選択し、**OK** をクリックします。 • **Filter by location**（場所によるフィルタリング）– 特定の場所の変更を選択して、Include in Revert（元に戻す対象に含める）を有効にします。 アクセス ドメインを実装している場合、ファイアウォールはそれらのドメインに基づいて、元に戻す範囲を自動的にフィルタリングします（「Device（デバイス）> Access Domain（アクセス ドメイン）」を参照）。管理者ロールやフィルタリングの選択に関係なく、元に戻す範囲にはアカウントに割り当てられたアクセス ドメインの設定変更のみが含まれます。
Revert Scope（元に戻す範囲）	元に戻す変更を含む場所を一覧表示します。リストに含まれるのが変更のすべてであるか一部であるかは、複数の要因が影響します。詳細は、「Revert All Changes（すべての変更を元に戻す）」および「Revert Changes Made By（指定対象に基づいて変更を元に戻す）」に記載されています。場所の種類は以下のとおりです。 • **shared-object**（共有オブジェクト）– 共有の場所で定義されている設定です。 • **policy-and-objects**（ポリシーとオブジェクト）–（ファイアウォールのみ）マルチ仮想システムを含まないファイアウォールで定義されているポリシー ルールまたはオブジェクトです。 • **device-and-network**（デバイスとネットワーク）–（ファイアウォールのみ）グローバルであり（インターフェイス管理プロファイルなど）、仮想システム専用でないネットワークおよびデバイス設定です。 • **<virtual-system>**（仮想システム）–（ファイアウォールのみ）マルチ仮想システムを含むファイアウォールの、ポリシー ルールまたはオブジェクトが定義されている仮想システムの名前です。仮想システム専用のネットワークおよびデバイス設定（ゾーンなど）も含まれます。 • **<device-group>**（デバイス グループ）–（Panorama のみ）ポリシー ルールまたはオブジェクトが定義されているデバイス グループの名前です。 • **<template>**（テンプレート）–（Panorama のみ）設定が定義されているテンプレートまたはテンプレート スタックの名前です。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **<log-collector-group>**（ログ コレクタ グループ）– （Panorama のみ）設定が定義されているコレクタ グループの名前です。 • **<log-collector>**（ログ コレクタ）– （Panorama のみ）設定が定義されているログ コレクタの名前です。
場所タイプ	この列では変更が行われた場所が分類されます。 • **Virtual Systems**（仮想システム）– （ファイアウォールのみ）特定の仮想システムで定義されている設定です。 • **Device Group**（デバイス グループ）– （Panorama のみ）特定のデバイス グループで定義されている設定です。 • **Template**（テンプレート）– （Panorama のみ）特定のテンプレートまたはテンプレート スタックで定義されている設定です。 • **Log Collector Group**（ログ コレクタ グループ）– （Panorama のみ）コレクタ グループ設定固有の設定です。 • **Log Collector**（ログ コレクタ）– （Panorama のみ）ログ コレクタ設定固有の設定です。 • **Other Changes**（その他の変更）– 前述の設定エリア（共有オブジェクトなど）に固有でない設定。
Include in Revert（元に戻す対象に含める） （一部を元に戻すのみ）	元に戻す変更を選択できます。デフォルトでは、**Revert Scope**（元に戻す範囲）のすべての変更が選択されています。この列は、特定の管理者に基づく **Revert Changes Made By**（指定対象に基づいて変更を元に戻す）を選択しないと表示されません。 依存関係が、元に戻す対象に含まれる変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更も元に戻さないと、自身の変更を元に戻すことができません。
場所タイプ別グループ	**Revert Scope**（元に戻す範囲）の設定変更を **Location Type**（場所タイプ）別に一覧表示します。
プレビューの変更	**Revert Scope**（元に戻す範囲）で選択した設定を、実行中の設定と比較できるようにします。プレビュー ウィンドウでは色分けによって詳細が示されます（追加は緑色、変更は黄色、削除は赤色）。 Web インターフェイスのセクションへの変更を一致させる場合、変更前後の **Lines of Context**（コンテキストの行）を表示するようにプレビュー ウィンドウを設定できます。これらは候補のファイルと、比較対象である実行中の設定から取得されます。 プレビュー結果は新しいウィンドウで表示されるので、ブラウザーでポップアップを許可しておく必要があります。プレビューウィンドウが開かない場合はブラウザ設定を参照し、ポップアップブロックの解除を行ってください。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
変更サマリー	変更を元に戻す対象の個別の設定を一覧表示します。**Change Summary**（変更サマリー）のリストでは、各設定の以下の情報が表示されます。 • **Object Name**（オブジェクト名）– ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。 • **Type**（タイプ）– 設定のタイプ（アドレス、セキュリティ ルール、ゾーンなど）です。 • **Location Type**（場所タイプ）– 設定が仮想システムで定義されているかどうかを示します。 • **Location**（場所）– 設定が定義されている仮想システムの名前です。仮想システム専用でない設定の場合、列に **Shared**（共有）と表示されます。 • **Operations**（操作）– 最後のコミット以降、設定に実施された各操作（作成、編集、または削除）を示します。 • **Owner**（オーナー）– 設定に直近の変更を加えた管理者です。 • **Will Be Reverted**（元に戻す予定）– 元に戻す作業に設定が含まれる予定がどうかを示します。 • **Previous Owners**（前回のオーナー）– 直近の変更前に、設定を変更した管理者です。 必要に応じて、**Group By**（グループ化基準）を列名（**Type**（タイプ）など）にできます。
元に戻す	選択した変更を元に戻します。

© 2019 Palo Alto Networks, Inc.

設定のロック

同時ログイン セッション中にその他のファイアウォール管理者と設定タスクを調整できるようにするため、Web インターフェイスではapply a configuration or commit lock（設定ロックまたはコミット ロックを適用）し、ロックが解除されるまで、その他の管理者が設定を変更したり変更をコミットしたりできないようにします。

1つ以上のロックが設定されている場合はWebインターフェイスの右上に閉じた南京錠（）が表示され（括弧内にロックの数が表示されます）、開いた南京錠（）が表示されている場合はロックされていないことを示します。どちらの場合も、南京錠をクリックすることでロックのダイアログが表示し、以下のオプションやフィールドを編集することができます。

管理者が候補設定を変更した際に、コミットを自動的にロックするようファイアウォールを設定する場合は、 *Device* > *Setup* > *Management[デバイス* > 設定 > 管理*]* を開いて一般設定を編集し、*Automatically Acquire Commit Lock [コミットロックの自動実施]* を有効化し、*OK*をクリックして *Commit [コミット]* します。

変更を元に戻すと（*Config*（設定）> *Revert Changes*（変更を元に戻す））、ファイアウォールでは候補および実行中設定が自動的にロックされるため、その他の管理者は設定を編集したり変更をコミットしたりできません。元に戻すプロセスの完了後、ファイアウォールではロックが自動的に解除されます。

フィールド/ボタン	の意味
admin	ロックを設定した管理者のユーザー名が表示されます。
場所	1つ以上の仮想システム（vsys）をもつファイアウォールの場合、ロックの範囲は特定のvsysあるいは共有の場所に設定することができます。
タイプ	ロックのタイプには以下のものがあります。 • **Config Lock**[設定ロック] – 他の管理者が候補設定を変更できないようにブロックします。スーパーユーザーまたはロックをセットした管理者のみ解除することができます。 • **Commit Lock**（コミットロック） – 他の管理者が候補設定の変更をコミットすることを阻止します。すべてのロックが解除されるまで、コミットキューは新規のコミットを受け付けません。このロックは、複数の管理者が同時ログインセッションにおいて変更を加え、ある管理者がセッションを完了する前に他の管理者が設定を終えてコミットを実行したような場合に発生する、設定の競合を防ぐためのものです。ロックを設定した管理者が実行したコミットが完了すると、ファイアウォールは自動的にロックを解除します。スーパーユーザーまたはロックをセットした管理者は、手動でそれを解除することもできます。
コメント	最大256文字のコメントを入力できます。他の管理者にロックの理由を知らせる場合に便利です。
次の場所に作成	管理者がロックを設定した日時です。
ログイン状態	ロックを設定した管理者が現在ログイン中かどうかが表示されます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
ロックの設定	ロックを設定する場合は、**Take a Lock** (ロック設定)を開き、**Type** (タイプ)を選択し、**Location** (場所) を指定し（複数の仮想システムをもつファイアウォールのみ）、任意の**Comments** (コメント) を入力し、**OK**をクリックしてから**Close** (閉じる) をクリックします。
ロックの削除	ロックを解除する場合はロックを選択し、**Remove Lock** [ロックを解除]、次に**OK**をクリックし、最後に**Close** [閉じる] をクリックします。

© 2019 Palo Alto Networks, Inc.

Global Find

グローバル検索を使用すると、ファイアウォールまたは Panorama の候補設定に含まれる特定の文字列 (IP アドレス、オブジェクト名、ポリシー名、脅威 ID、ルールの UUID、アプリケーション名など) を検索できます。検索結果はカテゴリ別にグループ化され、Web インターフェイスで設定場所へのリンクが表示されるので、当該文字列が出現する場所、または参照されている場所をすべて簡単に見つけることができます。

グローバル検索を起動するには、Web インターフェイスの右上にある **Search** (検索) アイコン Search をクリックします。グローバル検索はすべての Web インターフェイス ページと場所で使用できます。以下に、検索を上手に行うためのグローバル検索の各種機能を示します。

- マルチ仮想システムが有効になっているファイアウォール上で検索を開始する場合、または管理ロールが定義されている場合は、検索者にアクセス権のあるファイアウォールのエリアの検索結果のみが返されます。Panorama デバイス グループに関しても同様です。管理アクセス権のあるデバイス グループについてのみ、検索結果が表示されます。
- 検索テキストに含まれるスペースは、AND 演算子として処理されます。たとえば、「**`corp policy`**」を検索した場合、検索結果に表示されるには **corp** と **policy** の両方が含まれている必要があります。
- 完全に一致するフレーズを検索するには、フレーズを引用符で囲みます。
- 以前の検索を再実行する場合、Global Find (グローバル検索) をクリックすると、直近 20 件の検索のリストが表示されます。リストの項目をクリックすると、その検索が再実行されます。この検索履歴は、管理者アカウントごとに固有のものです。

グローバル検索は検索可能な各フィールドに対して使用できます。たとえば、セキュリティ ポリシーの場合は、次のフィールドを検索できます。名前、タグ、ゾーン、アドレス、ユーザー、HIP プロファイル、アプリケーション、UUID、およびサービス。検索を実行するには、これらの任意のフィールドの横にあるドロップダウン リストをクリックして、**Global Find** (グローバル検索) をクリックします。たとえば、l3-vlan-trust という名前のゾーンで **Global Find** (グローバル検索) をクリックすると、そのゾーン名で設定全体が検索され、検索結果としてそのゾーンが参照されているすべての場所が返されます。検索結果はカテゴリ別にグループ化され、いずれかの項目にマウス カーソルを移動すると詳細が表示されます。また、項目をクリックすると、その項目の設定ページに移動します。

グローバル検索では、ファイアウォールがユーザーに割り当てる動的コンテンツ (ログ、アドレス範囲、または個別の DHCP アドレス) は検索されません。DHCP の場合、DHCP サーバー属性 (DNS エントリなど) は検索できますが、ユーザーに発行される個々のアドレスは検索できません。別の例は、ユーザーID™機能を有効にしたときにファイアウォールが収集するユーザー名です。この場合、User-ID データベース内に存在するユーザー名またはユーザー グループは、その名前またはグループが設定内に存在する場合 (ポリシー内にユーザー グループ名を定義している場合など) のみ検索可能です。一般に、ファイアウォールが設定に書き込む内容のみ検索できます。

その他の情報をお探しですか？

ファイアウォールまたは Panorama 設定の検索の詳細は、グローバル検索の使用に関するページを参照してください。

© 2019 Palo Alto Networks, Inc.

脅威詳細

- Monitor（監視）> Logs（ログ）> Threat（脅威）
- [ACC] > [脅威アクティビティ]
- Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Anti-Spyware（アンチスパイウェア）/Vulnerability Protection（脆弱性防御）

ファイアウォールが実装する脅威シグネチャ、およびそのシグネチャをトリガーするイベントについては、Threat Details（脅威詳細）ダイアログを参照してください。脅威詳細は次のもののために提供されます。

- ファイアウォールが検出する脅威を記録する脅威ログ（**Monitor**（監視）> **Logs**（ログ）> **Threat**（脅威））
- ネットワークで検出される上位の脅威（**ACC** > **Threat Activity**（脅威アクティビティ））
- 適用を変更または除外する脅威シグネチャ（**Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **Anti-Spyware**（アンチスパイウェア）/**Vulnerability Protection**（脆弱性防御））

脅威シグネチャが見つかり、それについて詳しく調べる必要がある場合は、**Threat Name**（脅威名）または脅威 **ID** にマウスを合わせて、**Exception**（例外）をクリックして脅威詳細を確認します。脅威詳細では、脅威シグネチャがセキュリティ ポリシーの例外として設定されているかどうかを簡単に確認し、特定の脅威に関するThreat Vault の最新情報を検索できます。Palo Alto Networks Threat Vault データベースはファイアウォールと統合されているため、ファイアウォール コンテキストで脅威シグネチャに関する詳細を参照したり、新しいブラウザ ウィンドウで Threat Vault 検索を起動して、ログに記録された脅威を検索したりすることができます。

参照している脅威のタイプに応じて、詳細には、次の表で説明する脅威詳細のすべてまたは一部が組み込まれます。

脅威詳細	の意味
氏名	脅威シグネチャ名。
ID	一意の脅威シグネチャ ID。Threat Vault 検索を新しいブラウザ ウィンドウで開き、Palo Alto Networks の脅威データベースに含まれている、このシグネチャの最新情報を検索するには、**View in Threat Vault**（**Threat Vault** で表示）を選択します。脅威シグネチャの Threat Vault エントリには、シグネチャの更新を含む最初のコンテンツ リリースと最後のコンテンツ リリース、およびシグネチャのサポートに必要となる PAN-OS の最低バージョンなどの詳細が含まれることがあります。
の意味	シグネチャをトリガーする脅威についての情報。
重要度	脅威の重大度。通知、低、中、高、重要のいずれか。
CVE	脅威に関連して、一般に知られているセキュリティの脆弱性。ベンダー固有の ID には一般的に複数の脆弱性が含まれますが、CVE（Common Vulnerabilities and Exposures）識別子は、固有の脆弱性に関する情報を検索するための最も便利な識別子です。
bugtraq id	脅威に関連付けられているバグトラック ID。

© 2019 Palo Alto Networks, Inc.

脅威詳細	の意味
ベンダー ID	脆弱性のベンダー固有識別子。たとえば、MS16-148 は Microsoft の 1 つ以上の脆弱性のベンダー ID であり、APBSB16-39 は Adobe の 1 つ以上の脆弱性のベンダー ID です。
リファレンス	脅威について参考にすることができる調査資料。
プロファイルの免除	デフォルトのシグネチャ アクション以外で、脅威シグネチャに適用するアクションを定義するセキュリティ プロファイル。脅威例外が有効になるのは、除外プロファイルがセキュリティ ポリシー ルールに添付されているときのみです（例外が現在のセキュリティ ルールで使用されているかどうかを確認してください）。
現在のセキュリティ ルールで使用	脅威例外が有効 – この列にチェック マークが付いているということは、ファイアウォールで脅威例外が適用されている（脅威例外を定義する除外プロファイルがセキュリティ ポリシー ルールに添付されている）ということです。 この列にチェック マークが付いていない場合、ファイアウォールでは、推奨デフォルト シグネチャ アクションのみに基づいて脅威に対処しています。
IP アドレスの免除	除外 IP アドレス – 脅威例外をフィルタリングする IP アドレスを追加するか、既存の **Exempt IP Addresses**（除外 **IP** アドレス）を表示できます。関連付けられているセッションに送信元 IP アドレスか宛先 IP アドレスがあり、それが除外 IP アドレスと一致するときに限り、このオプションによって脅威例外が適用されます。その他すべてのセッションでは、デフォルトのシグネチャ アクションに基づいて脅威が対処されます。

脅威詳細を表示できない場合は、次の条件を確認してください。

- ファイアウォールの脅威防御ライセンスが有効である（*Device*（デバイス）> *Licenses*（ライセンス））。
- アンチウイルス、脅威、アプリケーションの最新コンテンツ更新がインストールされている。
- *Threat Vault* アクセスが有効である（*Device*（デバイス）> *Setup*（設定）> *Management*（管理）を選択し、*Logging and Reporting*（ログとレポート）の設定を *Enable Threat Vault Access*（*Threat Vault* アクセスの有効化）に編集する）。
- デフォルトの（またはカスタムの）Antivirus, Anti-Spyware, and Vulnerability Protection security profiles（アンチウイルス、アンチスパイウェア、脆弱性防御のセキュリティ プロファイル）がセキュリティ ポリシーに適用されている。

© 2019 Palo Alto Networks, Inc.

AutoFocus インテリジェンス サマリー

AutoFocus によって集められた脅威インテリジェンスの概要をグラフィカルに表示でき、以下のファイアウォールのアーチファクトの広がりとリスクを評価するのに役立ちます。

- IPアドレス
- URLプロテクションの
- ドメイン
- ユーザー エージェント（データ フィルタリング ログの User Agent（ユーザー エージェント）列で確認できます）
- 脅威名（サブタイプ ウイルスおよび WildFire ウイルスの脅威のみ）
- ファイル名
- SHA-256 ハッシュ（WildFire への送信ログの File Digest（ファイル ダイジェスト）列で確認できます）

AutoFocus Intelligence Summary (AutoFocus インテリジェンス サマリー) ウィンドウを表示するには、まずはアクティブな AutoFocus サブスクリプションを用意して AutoFocus 脅威インテリジェンスを有効化（**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**を選択して AutoFocus 設定を編集）する必要があります。

AutoFocus インテリジェンスを有効化した後、ログあるいは外部動的リストのアーチファクトにカーソルを合わせてドロップダウンリストを開き（ ）、**AutoFocus**をクリックします：

- トラフィック、脅威、URL フィルタリング、WildFire への送信、データ フィルタリング、統合ログ（**Monitor**（監視）> **Logs**（ログ））を表示する。
- 外部動的リスト エントリを表示する。

また、気になる、あるいは疑わしいアーチファクトを詳しく調査するために、ファイアウォールから AutoFocus 検索を起動することもできます。

フィールド/ボタン	の意味
AutoFocus を検索...	アーチファクトに対する AutoFocus 検索を起動する場合にクリックします。
Analysis Information（分析情報）タブ	
セッション数	WildFire がアーチファクトを検出したプライベート セッションの数。プライベートセッションとは、お客様のサポートアカウントに関連付けられたファイアウォールで実行されているセッションを指します。セッション バーにマウス カーソルを移動すると、月あたりのセッション数が表示されます。
サンプル	アーチファクトに関連付けられた組織サンプルおよびグローバル サンプル（ファイルと電子メール リンク）。WildFire 判定（安全、グレイウェア、マルウェア、フィッシング）でグループ化されます。*Global*（グローバル）はすべての WildFire 送信のサンプルを意味します。一方、*organization*（組織）は組織が WildFire に送信するサンプルのみを意味します。 WildFire 判定をクリックすると、範囲（組織またはグローバル）と WildFire 判定でフィルタリングされたアーチファクトの AutoFocus 検索が起動します。
一致するタグ	アーチファクトに一致する AutoFocus タグ。 • プライベート タグ – サポート アカウントに関連付けられた AutoFocus ユーザーにのみ表示されます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• パブリック タグ – すべての AutoFocus ユーザーに表示されます。 • **Unit 42** タグ – 直接的なセキュリティ リスクを引き起こす脅威やキャンペーンを識別します。これらのタグは、Unit 42（Palo Alto Networks 脅威インテリジェンスおよび研究チーム）によって作成されます。 • 情報タグ – コモディティ脅威を識別する Unit 42 タグ。 タグにマウス カーソルを移動すると、そのタグの説明や他のタグの詳細が表示されます。 タグをクリックすると、そのタグの AutoFocus 検索が起動します。 アーティファクトのタグをさらに表示するには、省略記号（...）をクリックしてアーチファクトに対する AutoFocus 検索を起動します。AutoFocus 検索結果の Tags（タグ）列に、アーチファクトに一致するその他のタグが表示されます。
Passive DNS（パッシブ DNS）タブ Passive DNS（パッシブ DNS）タブには、アーチファクトに関連付けられたパッシブ DNS 履歴が表示されます。このタブには、アーチファクトが IP アドレス、ドメイン、または URL の場合の一致情報のみが表示されます。	
要求	DNS 要求を送信したドメイン。ドメインをクリックすると、そのドメインの AutoFocus 検索が起動します。
タイプ	DNS 要求タイプ（A、NS、CNAME など）。
応答	DNS 要求で解決された IP アドレスまたはドメイン。IP アドレスまたはドメインをクリックすると、AutoFocus 検索が起動します。 *Response*（応答）列にプライベート *IP* アドレスは表示されません。
数	要求が作成された回数。
First Seen（最初）	パッシブ DNS 履歴で要求、応答、タイプの組み合わせが最初に出現した日時。
Last Seen（最後に出現した日時）	パッシブ DNS 履歴で要求、応答、タイプの組み合わせが最後に出現した日時。
Matching Hashes（一致するハッシュ）タブ Matching Hashes（一致するハッシュ）タブには、WildFire がアーチファクトを検出した直近のプライベートサンプルが 5 つ表示されます。プライベートサンプルとは、お客様のサポートアカウントに関連付けられたファイアウォールで検出されたサンプルを指します。	
SHA256	サンプルの SHA-256 ハッシュ。ハッシュをクリックすると、そのハッシュの AutoFocus 検索が起動します。
ファイルタイプ	サンプルのファイル タイプ。
作成日	WildFire がサンプルを分析して WildFire 判定を割り当てた日時。
更新日	WildFire がサンプルの WildFire 判定を更新した日時。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
判定	サンプルの WildFire 判定 (安全、グレイウェア、マルウェア、またはフィッシング) 。

© 2019 Palo Alto Networks, Inc.

設定テーブルのエクスポート

管理ユーザーは、ポリシー ルールベース、オブジェクト、管理対象デバイス、インターフェイスのデータを表形式で PDF ファイルまたは CSV ファイルにエクスポートできます。エクスポートされるデータは、Webインターフェイス上で閲覧できるデータです。フィルタリングされたデータの場合、フィルタに一致するデータのみがエクスポートされます。フィルタを適用しない場合、すべてのデータがエクスポートされます。

パスワードなどのすべての機密データは、ワイルドカード (*) 記号で隠されています。

設定テーブルのエクスポートが成功すると、システム ログとダウンロード リンクが生成されます。ダウンロード リンクを使用して、PDF または CSV ファイルをローカルに保存します。ダウンロード リンクを含むウィンドウを閉じると、その特定のエクスポートのダウンロード リンクは使用できなくなります。

表データをエクスポートするには、**PDF/CSV** をクリックして次の項目を設定します。

エクスポート設定	の意味
ファイル名	エクスポートしたデータを識別するために名前 (32 文字以内) を入力します。この名前は、エクスポートにより作成されるダウンロード ファイルの名前になります。
ファイルタイプ	生成するエクスポート出力のタイプを選択します。PDF または CSV 形式のいずれかを選択できます。
Page Size (ページ サイズ)	デフォルトのページ サイズは Letter (レター) (8.5 x 11.0 インチ) です。ページ サイズは変更できません。デフォルトでは、PDF は縦向きに生成され、縦書きの向きに変更されて最大列数に対応します。
の意味 (PDF 専用)	エクスポートに関するコンテキストと追加情報を提供するための説明 (最大 255 文字) を入力します。
Table Data (表データ)	エクスポートする表データを表示します。以前に設定したフィルタリング設定を消去する必要がある場合は、 **Show All Columns** (すべての列を表示) をクリックして、選択したポリシー タイプのすべてのポリシー ルールを表示します。これで、必要に応じて列を追加または削除したりフィルタを適用したりできます。
Show All Columns (すべての列を表示)	すべてのフィルタを削除してすべての表の列を表示します。

設定テーブルのダウンロード リンクを生成するには、**Export** (エクスポート) をクリックします。

© 2019 Palo Alto Networks, Inc.

ダッシュボード

ダッシュボード ウィジェットには、ソフトウェアのバージョン、各インターフェイスの状態、リソース使用率、ログ タイプごとの 10 個までのエントリなど、ファイアウォールや Panorama™ の一般的な情報が表示されます。ログ ウィジェットには、過去 1 時間のエントリが表示されます。

「ダッシュボード ウィジェット」では、ダッシュボードの使用方法、および使用可能なウィジェットについて説明します。

Dashboard Widgets（ダッシュボード ウィジット）

デフォルトでは、**Dashboard**（ダッシュボード）には **3** 列のレイアウトでウィジェットが表示されますが、**2** 列のみを表示するようにダッシュボードをカスタマイズできます。

どのウィジェットを表示し、どのウィジェットを非表示にするのかも決められるため、監視対象のみを表示できます。ウィジェットを表示するには、**Widgets**（ウィジェット）ドロップダウン リストからウィジェットのカテゴリを選択し、ダッシュボードに追加するウィジェットを選択します（名前がグレー表示になっているウィジェットはすでに表示されています）。ウィジェットを非表示にする（表示を停止する）には、ウィジェットを閉じます（ウィジェットのヘッダーの ）。ファイアウォールと Panorama では、ログインしなおしてもウィジェットの表示設定は保存されています（管理者ごとに個別に）。

ダッシュボードのデータが前回いつ更新されたのかは、**Last updated**（最終更新）タイムスタンプで判断します。**Dashboard**（ダッシュボード）全体を手動で更新したり（ダッシュボードの右上の ）、ウィジェットを個別に更新したり（各ウィジェットのヘッダーの ）することができます。**Dashboard**（ダッシュボード）全体の自動更新間隔（分単位）を選択するには、手動ダッシュボード更新オプション（ ）の隣にあるラベルなしのドロップダウンを使用します：自動更新間隔は **1** 分、**2** 分、または **5** 分で設定できます。**Dashboard**（ダッシュボード）全体の自動更新を無効にするには、**Manual**（手動）を選択します。

Dashboard Widgets（ダッシュボード ウィジット）	の意味
アプリケーション ウィジット	
上位のアプリケーション	セッション数が最も多いアプリケーションが表示されます。ブロック サイズでセッションの相対数を示し（マウス カーソルをブロックの上に移動すると数が表示されます）、色でセキュリティのリスクを示します（緑（リスク低）～赤（リスク高））。アプリケーションをクリックして、プロファイルを表示します。
上位のハイリスク アプリケーション	Top Applications（上位アプリケーション）と似ていますが、ここにはセッション数が最も多いハイリスク アプリケーションが表示されます。
ACC リスク ファクタ	過去1週間の間に処理されたネットワーク トラフィックの平均リスクファクタ（1～5）が表示されます。値が大きいほどリスクが大きくなります。
システム ウィジット	
General Information	ファイアウォールあるいは Panorama 名およびモデル、Panorama の CPU および RAM、Panorama のシステムモード、PAN-OS® あるいは Panorama のソフトウェアバージョン、IPv4 および IPv6 管理 IP 情報、シリアル番号、CPU ID および UUID、アプリケーション、脅威、URL フィルタリング定義のバージョン、現在の日次、前回の再起動から経過した時間を表示します。
インターフェイス（ファイアウォールのみ）	各インターフェイスが、有効 (緑)、無効 (赤)、または不明な状態 (グレー) であることを示します。

© 2019 Palo Alto Networks, Inc.

Dashboard Widgets（ダッシュボード ウィジット）	の意味
システム リソース	管理 CPU の使用率、データプレーン使用率、およびセッション数（ファイアウォールまたは Panorama で確立されたセッションの数）が表示されます。
HA	高可用性（HA）を有効にすると、ローカルおよびピア ファイアウォール/Panorama の HA 状態 — 緑（アクティブ）、黄（パッシブ）、黒（その他）— が表示されます。HA の詳細は「Device（デバイス）> Virtual Systems（仮想システム）」または「Panorama > High Availability（高可用性）」を参照してください。
ロック	管理者が設定したロックを表示します。
ログインしている管理者	現在ログインしている各管理者の送信元IPアドレス、セッションタイプ（WebインターフェイスまたはCLI）、およびセッションの開始時刻が表示されます。
ログウィジェット	
脅威ログ	脅威ログには、最新 10 エントリの脅威の ID、アプリケーション、および日時が表示されます。脅威 ID は、マルウェアに関する説明、または URL フィルタリング プロファイルに違反する URL を示します。過去 60 分間のエントリのみが表示されます。
URL フィルタリング ログ	URL フィルタリング ログには、直近 60 分間に生成されたログの説明と日時が表示されます。
データ フィルタリング ログ	データ フィルタリング ログには、直近 60 分間に生成されたログの説明と日時が表示されます。
設定ログ	設定ログには、最新10エントリの管理者ユーザー名、クライアント (WebインターフェイスまたはCLI)、および日時が表示されます。過去 60 分間のエントリのみが表示されます。
システム ログ	システム ログには、最新 10 エントリの説明と日時が表示されます。 「*Config installed*」エントリは、設定の変更が正常にコミットされたことを示します。過去 *60* 分間のエントリのみが表示されます。

© 2019 Palo Alto Networks, Inc.

ACC

アプリケーション コマンド センター (ACC) は、ネットワーク内のアクティビティに関する実用的なインテリジェンスを提供する分析ツールです。ACC は、ファイアウォール ログを使用してネットワーク上のトラフィック トレンドをグラフィカルに表現します。このグラフィカル表現を使用して、データにアクセスし、ネットワークの使用パターン、トラフィック パターン、疑わしいアクティビティ、異常を含め、ネットワーク上のイベント間の関係を視覚化できます。

> ACC の画面紹介
> ACC のタブ
> ACC のウィジェット
> ACC のアクション
> タブおよびウィジットの処理
> フィルタの処理 – ローカル フィルタおよびグローバル フィルタ

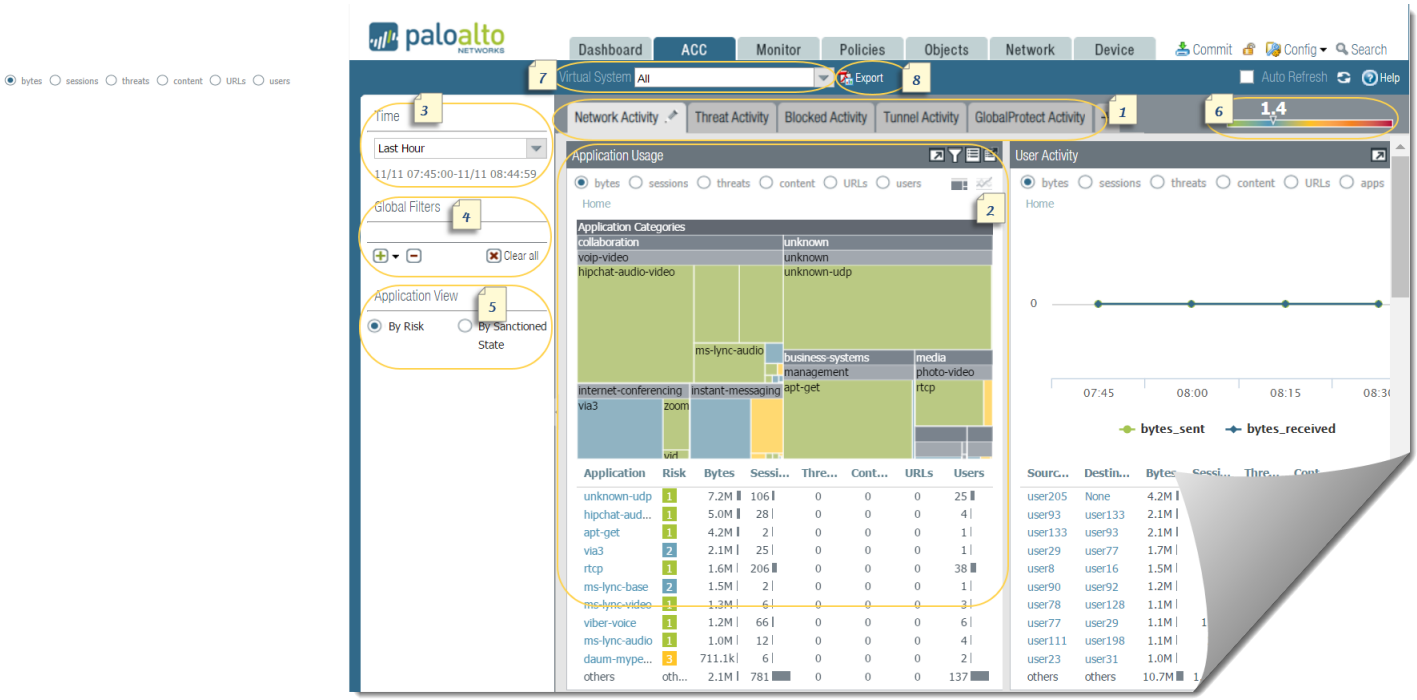
その他の情報をお探しですか？

「アプリケーション コマンド センターの使用」を参照してください。

ACC の画面紹介

以下の表で、ACC タブと各コンポーネントの説明を示します。

ACC の画面紹介



{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}	タブ	ACC には、ネットワーク トラフィック、脅威アクティビティ、ブロックされたアクティビティ、トンネル アクティビティ、GlobalProtect アクティビティ、およびモバイル ネットワーク アクティビティ (GTP セキュリティが有効になっている場合)を表示する事前定義済みのタブが含まれています。各タブの詳細は、「ACC のタブ」を参照してください。
2	ウィジェット	各タブには、タブに関連付けられたイベントとトレンドを最適に表現する、デフォルトのウィジット セットが含まれます。ウィジェットで、バイト数 (入力および出力)、セッション、コンテンツ (ファイルおよびデータ)、URL カテゴリ、アプリケーション、ユーザー、脅威 (有害、安全、グレイウェア、フィッシング)、およびカウントのフィルタを使用してデータを調べることができます。各ウィジェットの詳細は、「ACC のウィジェット」を参照してください。
3	時間	各ウィジットのチャートとグラフにはリアルタイム表示と履歴表示が用意されています。カスタム範囲を選択するか、過去 15 分 ~ 過去 30 日 (または暦日の過去 30 日) 間を選択できます。

© 2019 Palo Alto Networks, Inc.

		データの表示に使用するデフォルトの期間は過去 1 時間です。画面に日付と時間の間隔が表示されます。以下がその例です。 `11/11 10:30:00-01/12 11:29:59`
4	グローバル フィルタ	グローバル フィルタでは、すべてのタブに適用されるフィルタを設定できます。選択されたフィルタがチャートとグラフに適用された後にデータが表示されます。フィルタの使用方法の詳細は、「ACC のアクション」を参照してください。
5	アプリケーションのビュー	アプリケーションのビューでは、ネットワークで使用中の許可されたアプリケーションと不許可のアプリケーション、またはネットワークで使用中のアプリケーションのリスク レベルで ACC ビューをフィルタリングできます。緑色は許可されたアプリケーション、青色は不許可のアプリケーション、黄色は仮想システムまたはデバイス グループごとに許可状態が異なるアプリケーションを示しています。
6	リスク メーター	リスク メーター (1 = 最低 ~ 5 = 最高) は、ネットワーク上の相対的なセキュリティ リスクを示します。リスク メーターではさまざまな要因が使用されます。たとえば、ネットワーク上で確認されたアプリケーションのタイプ、そのアプリケーションに関連付けられるリスク レベル、ブロックされた脅威数によって確認される脅威のアクティビティとマルウェア、侵入されたホスト、マルウェアのホストまたはドメインへのトラフィックがあります。
7	送信元	ファイアウォールと Panorama™ では、表示に使用するデータが異なります。以下のオプションを使用して、ACC のビューを生成するためのデータを選択できます。 仮想システム**(vsys)**:マルチ仮想システムが有効になっているファイアウォールでは、**Virtual System**（仮想システム）ドロップダウンを使用して、ACC の表示にすべての仮想システムを含めるか、選択した仮想システムのみを含めるかを変更できます。 デバイス グループ:Panorama では、**Device Group**（デバイス グループ）ドロップダウンを使用して、ACC の表示にすべてのデバイス グループのデータを含めるか、選択したデバイス グループのデータのみを含めるかを変更できます。 データ送信元:Panoramaでは、表示に**Panorama**を使用するか、**Remote Device Data**（リモートデバイスデータ）を使用するかも変更できます（ファイアウォールデータを管理）。データソースが**Panorama**の場合、特定のデバイスグループに応じて表示をフィルタリングできます。
8	エクスポート	現在のタブに表示されているウィジットを PDF としてエクスポートできます。

© 2019 Palo Alto Networks, Inc.

ACC のタブ

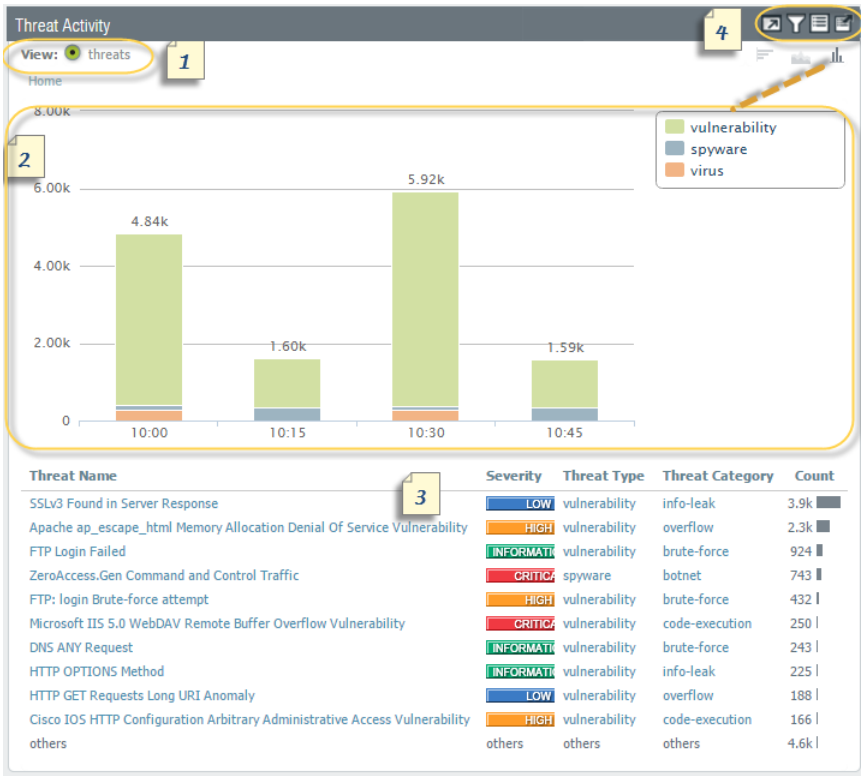
- **Network Activity** (ネットワーク アクティビティ) – ネットワーク上のトラフィックおよびユーザーアクティビティの概要が表示されます。このビューは、使用頻度が上位のアプリケーション、トラフィックを生成した上位のユーザーとそのユーザーがアクセスしたバイト数、コンテンツ、脅威、および URL の詳細、ならびにトラフィックと一致したセキュリティ ポリシー ルールのうち最も多く使用されたセキュリティ ルールに焦点を当てます。また、ネットワーク アクティビティを送信元または宛先のゾーン、領域、または IP アドレス別に表示したり、入力インターフェイスまたは出力インターフェイス別に表示したり、ホスト情報 (ネットワーク上で最もよく使用されたデバイスのオペレーティング システムなど) 別に表示したりできます。
- **Threat Activity** (脅威アクティビティ) – ネットワーク上の脅威の概要が表示されます。このタブは上位の脅威に焦点を当てます。たとえば、脆弱性、スパイウェア、ウイルス、有害なドメインまたは URL にアクセスしているホスト、上位の WildFire 送信 (ファイル タイプ別およびアプリケーション別)、非標準ポートを使用しているアプリケーションです。Compromised Hosts (侵入されたホスト) ウィジットは、すぐれた可視化技術を使用して検出を補完します。これは、correlated events (相関イベント) タブ (Monitor (監視) > Automated Correlation Engine (自動相関エンジン) > Correlated Events (相関イベント) からの情報を使用して、ネットワーク上の侵入されたホストを送信元ユーザーまたは IP アドレスごとに重大度の順番で集約して表示します。
- **Blocked Activity** (ブロックされたアクティビティ) – ネットワークに入ることができなかったトラフィックに焦点を当てます。このタブのウィジェットを使用すると、アプリケーション名、ユーザー名、脅威名、コンテンツ (ファイルとデータ)、およびトラフィックをブロックする拒否アクションの上位セキュリティルールによって拒否されたアクティビティを表示できます。
- **Mobile Network Activity** (モバイル ネットワーク アクティビティ) – セキュリティ ポリシー ルール設定から生成された GTP ログを使用して、ネットワークのモバイル トラフィックが視覚的に表示されます。このビューには、対話形式のカスタマイズ可能な GTP Events (GTP イベント)、Mobile Subscriber Activity (モバイルサブスクライバアクティビティ) および GTP Rejection Cause (GTP 拒否理由) ウィジットが含まれます。これらのウィジットに ACC フィルタを適用してドリルダウンし、必要な情報を分離できます。SCTP Security (SCTP セキュリティ) を有効にすると、このタブのウィジェットは、ファイアウォール上の SCTP イベントの視覚的表現と詳細、および SCTP Association ID (SCTP アソシエーション ID) ごとに送受信されるチャンクの数を表示します。
- **Tunnel Activity** (トンネル アクティビティ) – トンネル検査ポリシーに基づいてファイアウォールで検査されるトンネル トラフィックのアクティビティが表示されます。トンネル ID、モニター タグ、ユーザー、トンネル プロトコル (Generic Routing Encapsulation (GRE)、General Packet Radio Service (GPRS) Tunneling Protocol for User Data (GTP-U)、非暗号化 IPSec など) に基づいて、トンネルの使用状況などの情報が表示されます。
- **GlobalProtect Activity**–GlobalProtect 展開でのユーザー アクティビティの概要を表示します。情報には、ユーザー数とユーザーの接続回数、ユーザーが接続したゲートウェイ、接続の失敗回数と失敗の理由、認証方法の概要と使用された GlobalProtect アプリケーションのバージョン、および隔離されたエンドポイントの数が含まれます。

タブおよびウィジットの処理に記載されている通り、タブおよびウィジェットをカスタマイズすることもできます。

© 2019 Palo Alto Networks, Inc.

ACC のウィジェット

各タブのウィジットを操作できます。フィルタを設定し、表示をドリルダウンしてカスタマイズし、必要な情報に焦点を当てることができます。



各ウィジェットは以下の情報を表示するように構成されています。

{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}	表示、ビュー	バイト、セッション、脅威、カウント、ユーザー、コンテンツ、アプリケーション、URL、有害、安全、グレイウェア、フィッシング、ファイル（名）、データ、プロファイル、オブジェクトでデータをソートできます。使用できるオプションはウィジェットによって異なります。
2	グラフ	グラフ形式の表示オプションとして、ツリーマップ、折れ線グラフ、横棒グラフ、積み上げ領域グラフ、積み上げ棒グラフ、およびマップがあります。使用できるオプションはウィジェットによって異なり、インタラクション操作はグラフ タイプによって異なります。たとえば、非標準ポートを使用するアプリケーションのウィジェットでは、ツリーマップと折れ線グラフのいずれかを選択できます。 表示をドリルダウンするには、グラフをクリックします。クリックしたエリアがフィルタになり、選択対象が拡大し、選択対象のより詳細な情報を表示できます。

© 2019 Palo Alto Networks, Inc.

3	表	グラフの作成に使用されたデータの詳細がグラフの下の表に表示されます。 表内の要素に対して、ローカル フィルタまたはグローバル フィルタをクリックして設定できます。ローカル フィルタを使用した場合、グラフが更新され、表がフィルタでソートされます。 グローバル フィルタを使用した場合、フィルタに固有の情報のみを表示するように ACC 全体の表示が切り替わります。
4	操作	ウィジェットのタイトルバーからは以下の操作を行うことができます。 • **Maximize view**（表示の最大化）– ウィジェットを拡大し、より大きく画面表示をさせることができます。表示を最大化すると、ウィジェットにデフォルトで表示されるトップ 10 アイテムよりも多くの情報を表示できます。 • **Set up local filters**（ローカル フィルタの設定）– フィルタを追加して、ウィジェット内の表示を絞り込むことができます。「フィルタの処理 – ローカル フィルタおよびグローバル フィルタ」を参照してください。 • **Jump to logs**（ログに移動）– ログに直接移動できます（**Monitor**（監視）> **Logs**（ログ）> **<log-type>**（ログタイプ））。ログはグラフ表示に使用されている期間でフィルタされます。 ローカル フィルタとグローバル フィルタを設定した場合、ログ クエリでは期間とフィルタが連結され、設定したフィルタに一致するログのみが表示されます。 • **Export**[エクスポート] – グラフを PDF としてエクスポートできます。

各ウィジェットの詳細は、「ACC の使用」を参照してください。

© 2019 Palo Alto Networks, Inc.

ACC のアクション

ACC 表示のカスタマイズおよび絞り込みを行うには、タブの追加と削除、ウィジットの追加と削除、ローカルおよびグローバル フィルタの設定、ウィジットの操作ができます。

- タブおよびウィジットの処理
- フィルタの処理 – ローカル フィルタおよびグローバル フィルタ

タブおよびウィジットの処理

以下のオプションで、タブとウィジェットの使用およびカスタマイズ方法について説明します。

- カスタムタブの追加
  1. タブリストの横にある追加 ( ) を選択します。
  2. **View Name**[表示名] を追加します。この名前は、タブの名前として使用されます。最大 10 個のカスタム タブを追加できます。

- タブを編集する。

  タブを選択し、タブ名の横にある「編集」をクリックして、タブを編集します。

  例:

  .

- タブをデフォルトとして設定する
  1. タブを編集する。
  2. を選択し、現在のタブをデフォルトとして設定します。ファイアウォールにログインするたびにこのタブが表示されます。

- タブの状態を保存する
  1. タブを編集する。
  2. を選択し、現在のタブの設定をデフォルトとして保存します。

     設定した可能性があるすべてのフィルタを含め、タブの状態が HA ピア全体に同期されます。

- タブをエクスポートする
  1. タブを編集する。
  2. を選択し、現在のタブをエクスポートします。タブがコンピュータに .txt ファイルとしてダウンロードされます。ファイルをダウンロードするには、ポップアップを有効にする必要があります。

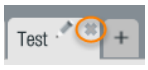
- タブをインポートする
  1. カスタムタブの追加
  2. を選択し、タブをインポートします。
  3. テキスト (.txt) ファイルを参照して選択します。

© 2019 Palo Alto Networks, Inc.

- ビューに含まれているウィジェットを表示する。
  1. ビューを選択して編集 ( ) をクリックします。
  2. **Add Widgets**[ウィジェットの追加] のドロップダウンリストから選択済みのウィジェットを確認します。

- ウィジットまたはウィジット グループを追加する。
  1. 新しいタブを追加するか、事前定義済みのタブを編集します。
  2. **Add Widget**[ウィジェットの追加] から、追加したいウィジェットを選択します。最大12個のウィジェットを選択可能です。
  3. (任意) 2 列レイアウトを作成するには、**Add Widget Group** (ウィジェット グループの追加) を選択します。ウィジェットを 2 列表示画面にドラッグ アンド ドロップできます。ウィジットをレイアウトにドラッグすると、ウィジットをドロップするためのプレースホルダが表示されます。

    ウィジット グループに名前を付けることはできません。

- タブ、ウィジェット、またはウィジェット グループを削除する。
  - カスタム タブを削除するには、タブを選択して削除 () をクリックします。

    事前定義済みのタブを削除することはできません。
  - ウィジェットあるいはウィジェットグループを削除する場合は、タブを編集してから削除 ([X]) をクリックします。削除を取り消すことはできません。

- デフォルト表示をリセットする。

  事前定義済みの表示 (**Blocked Activity**[ブロックされたアクティビティ] 表示など) で、1 つまたは複数のウィジットを削除できます。レイアウトをリセットし、タブに含まれるウィジェットセットをデフォルトに戻す場合、タブを編集してから**Reset View**[ビューのリセット] をクリックします。

フィルタの処理 – ローカル フィルタおよびグローバル フィルタ

詳細情報に焦点を合わせて、ACCに表示する情報を細かく制御する場合はフィルタを使用します。

- **Local Filters**[ローカル フィルタ] - ローカル フィルタは特定のウィジットに適用されます。ローカル フィルタを使用すると、グラフを操作し、表示をカスタマイズできるため、情報を詳細まで掘り下げて、監視する必要がある情報に特定のウィジットでアクセスできます。ローカル フィルタを適用する方法は 2 つあり、グラフまたは表内で属性をクリックする方法と、ウィジェット内で **Set Filter** (フィルタの設定) を選択する方法があります。**Set Filter** (フィルタの設定) により、再起動後も持続するローカル フィルタを設定できます。
- **Global filters**[グローバルフィルタ] - グローバル フィルタはACC全体に適用されます。グローバル フィルタを使用して、自分が最も注目しているデータを中心に表示し、関係のない情報を現在の表示から除外できます。たとえば、特定のユーザーとアプリケーションに関連するすべてのイベントを表示するには、ユーザーの IP アドレスを適用し、アプリケーションを指定して、グローバル フィルタを作成します。これで、そのユーザーとアプリケーションに関連する情報のみを ACC 上のすべてのタブとウィジェットに表示できます。グローバル フィルタはログイン間で持続されません。

  グローバル フィルタは次の 3 つの方法で適用できます。

- **Set a global filter from a table**[表からグローバルフィルタを設定する] - 任意のウィジット内の表から属性を選択し、その属性をグローバルフィルタとして適用します。

© 2019 Palo Alto Networks, Inc.

- **Add a widget filter to a global filter** (グローバル フィルタにウィジェット フィルタを追加する) - 属性にカーソルを合わせ、その右側にある矢印のアイコンをクリックします。これにより、ウィジェットで使用されているローカル フィルタが昇格し、属性がグローバルに適用され、ACC のすべてのタブの表示が更新されます。
- **Define a global filter**[グローバルフィルタを定義する] - ACCの**Global Filters**[グローバル フィルタ] ペインを使用してフィルタを定義します。

- ローカル フィルタを設定する。

  グラフの下の表で、属性をクリックし、その属性をローカル フィルタとして適用することもできます。

  1. ウィジェットを選択し、フィルタ ( ) をクリックします。
  2. 適用したいフィルタを追加 ( ) します。
  3. **Apply**[適用] をクリックします。このフィルタは、再起動後も持続します。

  ウィジットに適用されているローカル フィルタの数がウィジット名の横に示されます。

- 表からグローバル フィルタを設定する。

  表の中の属性にカーソルを合わせ、その右側に表示される矢印をクリックします。

- Global Filters [グローバル フィルタ] ペインを使用して、グローバル フィルタを設定します。

  適用したいフィルタを追加 ( ) します。

- ローカル フィルタをグローバル フィルタにプロモートする。
  1. ウィジット内の任意の表で、属性をクリックします。これにより、属性がローカル フィルタとして設定されます。
  2. フィルタをグローバルフィルタに昇格させる場合は、属性にカーソルを合わせ、その右側にある矢印をクリックします。

- フィルタを削除する。

  削除 ( ) をクリックして、フィルタを削除します。

  - **Global filters**[グローバルフィルタ] - [グローバルフィルタ] ペインにあります。
  - **Local filters**[ローカルフィルタ] - フィルタ ( ) をクリックして、Set Local Filters [ローカルフィルタの設定]ダイアログを表示し、フィルタを選択して削除します。

- すべてのフィルタをクリアする。

  - **Global filters**[グローバルフィルタ] - グローバルフィルタを**Clear All**[すべてクリア]します。
  - **Local filters**[ローカルフィルタ] - ウィジェットを選択し、フィルタ ( ) をクリックします。次に、Set Local Filters [ローカルフィルタの設定] ウィジェットで**Clear All**[すべてクリア] をクリックします。

- フィルタの条件を反転させる。

  属性を選択し、フィルタ条件を反転( )させます。

  - **Global filters**[グローバルフィルタ] - [グローバルフィルタ] ペインにあります。

© 2019 Palo Alto Networks, Inc.

- **Local filters**[ローカルフィルタ] - フィルタ ( ) をクリックして、[ローカルフィルタの設定]ダイアログを表示し、フィルタを追加し、その条件を反転させます。

- 使用中のフィルタを表示する。
  - **Global filters**[グローバルフィルタ] - 適用されているグローバルフィルタの数が [グローバルフィルタ] の下の左ペインに表示されます。
  - **Local filters**[ローカルフィルタ] - ウィジットに適用されているローカルフィルタの数がウィジット名の横に表示されます。フィルタを表示する場合は、**Set Local Filters**[ローカルフィルタの設定] をクリックします。

監視

以下のトピックでは、ネットワーク上のアクティビティをモニターするのに使用できるファイアウォール レポートとログについて説明します。

> Monitor > Logs [監視 > ログ]
> Monitor（監視） > External Logs（外部ログ）
> Monitor（監視） > Automated Correlation Engine（自動相関エンジン）
> Monitor > Packet Capture [監視 > パケット キャプチャ]
> Monitor > App Scope [監視 > アプリケーション スコープ]
> Monitor > Session Browser [監視 > セッション ブラウザ]
> Monitor（監視） > Block IP List（ブロック IP リスト）
> Monitor > Botnet [監視 > ボットネット]
> Monitor（監視） > PDF Reports（PDF レポート）
> Monitor > Manage Custom Reports [監視 > カスタム レポートの管理]
> Monitor > Reports [監視 > レポート]

Monitor > Logs [監視 > ログ]

以下のトピックでは、ログのモニターに関する追加の情報について説明します。

知りたい内容	以下を参照
ログの種類を詳しく知りたい	ログ タイプ
ログのフィルター ログのエクスポート 個別のログエントリの詳細を表示したい ログの表示を変更する	ログ アクション
その他の情報をお探しですか？	ログのモニターと管理

ログ タイプ

- **Monitor (監視) > Logs (ログ)**

ファイアウォールはロールベースの管理権限に基づいて、すべてのログを表示します。閲覧権限のある情報のみが表示されます。これは、表示するログのタイプによって変化します。管理者権限の詳細は、「Device（デバイス）> Admin Roles（管理者ロール）」を参照してください。

ログ タイプ	の意味
トラフィック	各セッションの開始と終了のエントリが表示されます。各エントリには、日時、送信元ゾーン、宛先ゾーン、アドレスおよびポート、アプリケーション名、フローに適用されるセキュリティ ルール名、ルール アクション（**allow**、**deny**、または **drop**）、入力/出力インターフェイス、バイト数、およびセッション終了理由などが記載されます。 [タイプ] 列は、そのエントリがセッションの開始または終了のどちらのエントリなのか、またはセッションが拒否または廃棄されたのかどうかを示します。「drop」は、トラフィックをブロックしたセキュリティ ルールが適用されて「いずれか」のアプリケーションが指定されたことを示し、「deny」はルールが適用されてある特定のアプリケーションが識別されたことを示します。 アプリケーションが識別される前にトラフィックが廃棄された場合 (あるルールにより特定のサービスのトラフィックがすべて廃棄された場合など)、そのアプリケーションは「not-applicable」として表示されます。 トラフィックログを掘り下げ、個別のエントリや分析結果について、より詳細な情報を表示する。 • 詳細 ( ) をクリックすると、セッションに関する詳細な情報 (ICMP エントリを使用して同じ送信元と宛先間の複数のセッショ

© 2019 Palo Alto Networks, Inc.

ログ タイプ	の意味
	ンを集約するかどうかなど) が表示されます (**Count** (繰り返し回数)値は 1 より大きくなります)。 • アクティブな AutoFocus™ ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IP アドレス、ファイル名、URL、ユーザー エージェント、脅威名、またはハッシュの横にカーソルを合わせ、表示されたドロップダウン リスト ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリーを開きます。
脅威	ファイアウォールで生成された各セキュリティ アラームのエントリが表示されます。各エントリには、日時、脅威の名前または URL、送信元および宛先ゾーン、アドレス、ポート、アプリケーション名、フローに適用するセキュリティルール名、およびアラーム アクション (**allow** (許可) または **block** (ブロック)) と重大度が含まれています。 Type (タイプ) の列には、「ウイルス」または「スパイウェア」などの脅威の種類が表示されます。Name (名前) の列には脅威の内容または URL、Category (カテゴリ) の列には脅威のカテゴリ (「keylogger」など) または URL のカテゴリが表示されます。 脅威ログを掘り下げ、個別のエントリや分析結果について、より詳細な情報を表示する。 • 詳細 ( ) をクリックすると、脅威に関する詳細な情報 (そのエントリを使用して同じ送信元と宛先間の同じタイプの複数の脅威を集約するかどうかなど) が表示されます(**Count** (繰り返し回数) 値は 1 より大きくなります)。 • アクティブな AutoFocus ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IPアドレス、ファイル名、URL、ユーザー エージェント、脅威名、またはハッシュの横にカーソルを合わせ、表示されたドロップダウン メニュー ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリー を開きます。 • ローカルパケットキャプチャが有効な場合は、ダウンロード ( ) をクリックして、キャプチャされたパケットを表示します。ローカル パケット キャプチャを有効にするには、**Objects** (オブジェクト) > **Security Profiles** (セキュリティ プロファイル) のサブセクションを参照してください。 • 脅威に関する詳細を表示したり、脅威の除外を脅威ログから直接迅速に設定したりするには、**Name** (名前) 列で脅威名をクリックします。Exempt Profiles (プロファイルの免除) リストには、アンチウイルス、アンチスパイウェア、脆弱性のカスタム防御プロファイルがすべて表示されます。脅威シグネチャの除外を設定するには、セキュリティ プロファイル名の左のチェック ボックスをオンにし、変更を保存します。IP アドレスの除外を追加するには (1 つのシグネチャにつき 100 個までの IP アドレス)、セキュリティ プロファイルを強調表示して、Exempt IP Addresses (IP アドレスの免除) セクションに IP アドレスを追加し、**OK** をクリックして保存します。除外の確認または変更を行うには、関連するセキュリティ プロファイルに移動して **Exceptions** (例外) タブをクリックします。例えば、脅威タイプがvulnerability (脆弱性) である

© 2019 Palo Alto Networks, Inc.

ログ タイプ	の意味
	場合は、**Objects** (オブジェクト) > **Security Profiles** (セキュリティ プロファイル) > **Vulnerability Protection** (脆弱性防御)を選択し、関連するプロファイルをクリックしてから**Exceptions** (例外)タブをクリックします。
URL フィルタリング	Web サイトへのアクセス、およびユーザーが認証情報を Web サイトに送信できるかどうかを制御する URL フィルタのログを表示します。 どの URL カテゴリをブロックまたは許可するのか、どれに認証情報の送信を許可または禁止するのかなど、URL フィルタリング設定を定義するには、Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL フィルタリング) を選択します。URL の HTTP ヘッダー オプションをログに記録することもできます。 アクティブな AutoFocus ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IPアドレス、ファイル名、URL、ユーザー エージェント、脅威名、またはハッシュの横にカーソルを合わせ、表示されたドロップダウン メニュー ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリー を開きます。
WildFire への送信	ファイアウォールが WildFire™ 分析のために転送したファイルおよび電子メール リンクのログを表示します。WildFire はサンプルを分析して分析結果を返すことができ、これにはサンプルに割り当てられた WildFire 判定 (安全、マルウェア、グレイウェア、フィッシング) が含まれます。Action (アクション) 列を参照すると、ファイアウォールがセキュリティ ポリシー ルールに基づいてファイルを許可したかブロックしたかを確認できます。 アクティブな AutoFocus ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IPアドレス、ファイル名、URL、ユーザー エージェント、脅威名、または (File Digest (ファイル ダイジェスト) 列にある) ハッシュの横にカーソルを合わせ、表示されたドロップダウン メニュー ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリー を開きます。
データのフィルタリング	特定のファイルタイプのアップロードまたはダウンロードを防ぐファイアウォールやブロッキングプロファイルに保護されたエリアからの、クレジットカードや社会保障番号などの機密情報の流出を防ぐように設定したデータフィルタリングプロファイルが適用されたセキュリティーポリシーのログを表示します。 ログエントリの詳細情報にアクセスする場合のパスワード保護を設定するには、をクリックします。そこでパスワードを入力して **OK** をクリックします。データ保護パスワードの変更方法または削除方法の手順の詳細は、「Device (デバイス) > Response Pages (応答ページ) 」を参照してください。 各セッションで *1* 回のみ、システムから入力を要求されます。

© 2019 Palo Alto Networks, Inc.

ログ タイプ	の意味
HIP マッチ	GlobalProtect™ ゲートウェイが、エージェントによってレポートされた生 HIP データを定義済み HIP オブジェクトおよび HIP プロファイルと比較するときに特定する、すべての HIP マッチを表示します。その他のログとは異なり、HIP マッチは、セキュリティ ポリシーと一致していないときでもログに記録されます。詳細は、「Network (ネットワーク) > GlobalProtect > Portals (ポータル) 」を参照してください。
GlobalProtect	GlobalProtect 接続ログを表示します。この情報を使用して、GlobalProtect ユーザーとそのクライアント OS バージョンを特定し、接続とパフォーマンスの問題のトラブルシューティングを行い、ユーザーが接続するポータルとゲートウェイを特定します。
IP-Tag	タグが特定の IP アドレスにいつ、どのように適用されたのかという情報を表示します。この情報を使用すれば、特定の IP アドレスがいつ、なぜアドレスグループに配置され、どのポリシールールがそのアドレスに影響を与えるのか判断することができます。ログには Receive Time (受信時間) (セッションの最初および最後のパケットが到達した日時) 、Virtual System (仮想システム)、Source IP-Address (送信元 IP アドレス)、Tag (タグ)、Event (イベント)、Timeout (タイムアウト)、Source Name (送信元名)、Source Type (送信元タイプ) が含まれます。
User-ID™	マッピング情報のソース、User-ID エージェントがマッピングを実行したタイミング、マッピングが期限切れになるまでの残り時間など、IP アドレスとユーザー名のマッピングに関する情報を表示します。この情報を使用すると、User-ID の問題をトラブルシューティングしやすくなります。たとえば、ファイアウォールが誤ったポリシールールをユーザーに適用している場合は、ログを参照して、そのユーザーが正しい IP アドレスにマッピングされているかどうか、およびグループの関連付けが正しいかどうかを検証できます。
GTP	幅広い GTP 属性に関する情報を含むイベントベース ログを表示します。アプリケーション、送信元と宛先のアドレスとタイムスタンプなど、次世代ファイアウォールが識別する TCP/IP 情報に加えて、GTP イベント タイプ、GTP イベント メッセージ タイプ、APN、IMSI、IMEI、エンド ユーザー IP アドレスが含まれます。
トンネル検査	各検査済みトンネル セッションの開始と終了のエントリが表示されます。このログには、受信時間 (セッションの最初と最後のパケットが届いた日時) 、トンネル ID、モニター タグ、セッション ID、トンネル トラフィックに適用されたセキュリティ ルールなどが含まれます。詳細は、「Policies (ポリシー) > Tunnel Inspection (トンネル検査) 」を参照してください。
SCTP	ステートフル検査、プロトコル検証、および SCTP トラフィックのフィルタリングを実行している間に、ファイアウォールによって生成されたログに基づいて、SCTP イベントおよびアソシエーションを表示します。SCTP ログには、SCTP イベント タイプ、チャンク タイプ、SCTP 原因コード、Diameter アプリケーション ID、Diameter コマンド コード、およびチャンクなど、広範囲の SCTP やそのペイ

© 2019 Palo Alto Networks, Inc.

ログ タイプ	の意味
	ロード プロトコル属性に関する情報が含まれています。この SCTP 情報は、送信元および宛先アドレス、送信元および宛先ポート、ルール、タイムスタンプなど、ファイアウォールが識別する一般的な情報に加えて提供されます。詳細は、「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> SCTP Protection（SCTP プロテクション）」を参照してください。
設定	設定変更操作に関するエントリが表示されます。各エントリには、日時、管理者のユーザー名、変更を行ったユーザーのIPアドレス、クライアントのタイプ (WebインターフェイスまたはCLI)、実行されたコマンドのタイプ、コマンドが成功したか失敗したか、設定パス、および変更前後の値が含まれています。
システム<:so>システム	各システム イベントのエントリが表示されます。各エントリには、日時、イベントの重大度、およびイベントの説明が含まれています。
アラーム	アラーム ログは、システムによって生成されたアラームの詳細情報を記録します。このログの情報は、Alarms [アラーム] ウィンドウでも報告されます。「アラーム設定の定義」を参照してください。
authentication	認証ポリシー ルールによってアクセスが制御されているネットワーク リソースに、エンド ユーザーがアクセスしようとしたときに発生する認証イベントに関する情報が表示されます。この情報を使用すると、アクセスの問題をトラブルシューティングしやすくなり、必要に応じて認証ポリシーを調整できるようになります。相関オブジェクトとともに認証ログを使用すると、総当たり攻撃など、ネットワークでの不審なアクティビティを特定することもできます。 必要に応じて、認証タイムアウトをログに記録するように認証ルールを設定できます。これらのタイムアウトは、ユーザーがリソースに対して 1 回だけ認証すれば、その間リソースに何度でもアクセスできるという、その期間に関連します。タイムアウトに関する情報を確認すると、タイムアウトを調整するかどうか、およびその調整方法を判断できます。 システム ログには、*GlobalProtect* に関連する認証イベント、および *Web* インターフェイスへの管理者アクセスに関連する認証イベントが記録されます。
統合	トラフィック、脅威、URLフィルタリング、WildFireへの送信、データフィルタリングログエントリの最新情報を一つの画面で表示します。総合ログビューでは、それぞれのログを個別に検索するかわりに、様々なタイプのログをまとめて検証したりフィルタをかけることができます。または、フィルタ フィールドの左にある矢印をクリックして、**traffic**（トラフィック）、**threat**（脅威）、**url**、**data**（データ）、および（または）**wildfire** を選択することで、表示されるログタイプを指定することができます。 アクティブな AutoFocus ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IPアドレス、ファイル名、URL、ユーザー エージェント、脅威名、またはハッシュの横にカーソルを

© 2019 Palo Alto Networks, Inc.

ログ タイプ	の意味
	合わせ、表示されたドロップダウン メニュー ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリー を開きます。 ファイアウォールはロールベースの管理権限に基づいて、すべてのログを表示します。統合ログを表示する際は、閲覧権限のある情報のみが表示されます。例えば、WildFireへの送信ログを閲覧する権限のない管理者が統合ログを表示した場合は、WildFireへの送信ログは表示されません。管理者権限の詳細は、「Device (デバイス) > Admin Roles (管理者ロール)」を参照してください。 *AutoFocus* 脅威インテリジェンス ポータルで設定された統合ログを使用できます。AutoFocus 検索をセットアップし、*AutoFocus* 検索フィルタを統合ログフィルタ フィールドに直接追加できます。

ログ アクション

以下の表ではログ アクションについて説明します。

操作	の意味

ログのフィルター	各ログページの上部にはフィルタフィールドがあります。フィールドにはIPアドレスや時間範囲などの分析結果を入力し、一致するログエントリを検索することができます。フィールドの右側にあるアイコンから、フィルタの適用、クリア、作成、保存、ロードを行うことができます。
	
	• フィルタの作成:
	  • ログエントリ内の分析結果をクリックし、その分析結果をフィルタに追加します。
	  • **Add**[追加] ( ) をクリックして、新しい検索基準を定義します。それぞれの一致条件について、検索のタイプ (**and**または**or**) を指定する**Connector**[条件式]を選択し、検索を行う**Attribute**[属性]を指定し、検索の範囲を**Operator**[演算子]で定義し、ログエントリから探したい**Value**[値]を選択します。それぞれの一致条件をフィルタフィールドに**Add**[追加]し、入力が終わったらフィールドを**Close**[閉じ]ます。以上が完了したらフィルタを適用 ( ) できます。
	
	  構文エラーを防ぐため、*Value[値]*の文字列が、*has*または*in*などの*Operator[演算子]*を含む場合、文字列を引用符で囲む必要があります。例えば、宛先国のフィルタリングを行い*INDIA*を検索する際に*Value[値]*として***IN***を使う場合は、フィルタを***(dstloc eq "IN")***と入力します。
	
	  (receive_time in last-60-seconds)のログフィルタにより、表示されるログエントリおよびログページを時間とともに増加あるいは減少するように設定することができます。
	
	• フィルタを適用 - 現在のフィルタに一致するログエントリを表示する場合は、フィルタを適用 ( ) をクリックします。

© 2019 Palo Alto Networks, Inc.

操作	の意味
	• フィルタをクリア - フィルタフィールドをクリアする場合は、Clear Filter [フィルタをクリア] ( ) をクリックします。 • フィルタを保存 - フィルタを保存 ( ) を選択し、名前を入力して**OK**をクリックします。 • 保存したフィルタを使用 - 保存したフィルタをフィールドに追加する場合は、Load Filter [フィルタをロード] ( ) をクリックします。
ログのエクスポート	現在のフィルタに一致したすべてのログをCSV形式のレポートにエクスポートする場合は、CSVでエクスポート ( ) をクリックし、**Download file**[ファイルをダウンロード]します。レポートにはデフォルトで最大2,000行のログを含むよう設定されています。CSVレポートの行数制限を変更する場合は、 **Device** (デバイス) > **Setup** (セットアップ) > **Management** (管理) > **Logging and Reporting Settings** (ログとレポートの設定) > **Log Export and Reporting** (ログのエクスポートとレポート) を開き、新しい **Max Rows in CSV Export** (**CSV** エクスポートの最大行数) を入力します。
ポリシー アクションの強調表示	アクションと一致するログ エントリを強調表示する場合に選択します。フィルタリングされたログは、次の色で強調表示されます。 • 緑 – 許可 • 黄 – 継続またはオーバーライド • 赤 – 却下、ドロップ、drop-icmp、st-client、reset-server、reset-both、block-continue、block-override、block-url、drop-all、sinkhole

ログの表示を変更する	ログの表示をカスタマイズするには:
	• 表示ログの自動更新間隔を変更する場合は、ドロップダウンリストから間隔を選択します (**60 seconds**[60 秒]、**30 seconds**[30 秒]、**10 seconds**[10 秒]、または**Manual**[手動])。
	• ページに表示されるログの数と順序を変更する - ログ エントリは、10ページのブロック単位で取得されます。
	  • ページの下部にあるページ送り機能を使用して、ログリスト内を移動します。
	  • ページあたりのログエントリの数を変更するには、各ページのドロップダウンリストから行数を選択します (**20**、**30**、**40**、**50**、**75**、または**100**)。
	  • 結果を昇順または降順でソートするには、**ASC** または **DESC** ドロップダウンリストを使用します。
	• IP アドレスをドメイン名に解決する – **Resolve Hostname** (ホスト名の解決) をオンにすると、外部 IP アドレスがドメイン名に解決されます。
	• ログの表示順を変更する - ログを、受信時間が最新のものから降順で表示する場合は**DESC**[降順]を選択します。ログを、受信時間が一番古いものから昇順で表示する場合は**ASC**[昇順]を選択します。

個別のログエントリの詳細を表示する	各ログ エントリに関する情報を表示するには: • ログの詳細を表示する場合、エントリの詳細 ( ) クリックします。**Adress**[アドレス]ページで、送信元または宛先の IPアドレスから名前へのマッピングを定義している場合、IPアドレスの代わりにそのドメインまたはユーザー名が表示されます。関連付けられている IP アドレスを表示するには、名前の上にカーソルを移動します。 • アクティブな AutoFocus ライセンスが付与されたファイアウォール上で、ログ エントリに含まれる IP アドレス、ファイル名、URL、ユーザー エージェント、脅威名、またはハッシュにカーソルを合わせ、表示されたドロップダウン リスト ( ) をクリックして、その分析結果の AutoFocus インテリジェンス サマリーを開きます。

© 2019 Palo Alto Networks, Inc.

Monitor（監視）> External Logs（外部ログ）

Traps™ Endpoint Security Manager（ESM）から、Panorama™ が管理するログ コレクタに取り込まれたログを表示するには、このページを使用します。Panorama で Traps ESM ログを表示するには、次の手順を実行します。

- Traps ESM サーバーで、Panorama を Syslog サーバーとして設定し、Panorama に転送するためのロギング イベントを選択します。イベントには、セキュリティ関連のイベント、ポリシーの変更、エージェントや ESM サーバーのステータス変更、設定変更などがあります。
- 1 つ以上の管理対象ログ コレクタを備えた、Panorama モードでデプロイされた Panorama で、ログ インジェスト プロファイル（Panorama > Log Ingestion Profile（ログ インジェスト プロファイル））をセットアップし、そのプロファイルを、Traps ESM ログを保存するコレクタ グループ（Panorama > Collector Groups [Panorama > コレクタ グループ]）に接続します。

外部ログはデバイス グループに関連付けられていないため、外部ログは**Device Group**を選択した場合のみ表示される：**All**（すべて）ログはファイアウォールから送信されないためです。

ログ タイプ	の意味
Monitor（監視）> **External Logs**（外部ログ）> **Traps ESM** > **Threat**（脅威）	この脅威イベントには、Traps エージェントにより報告されたすべての防御イベント、通知イベント、暫定イベント、検出後イベントが含まれます。
Monitor（監視）> **External Logs**（外部ログ）> **Traps ESM** > **System**（システム）	ESM サーバー システム イベントには、ESM のステータス、ライセンス、ESM テクニカル サポート ファイル、および WildFire との通信に関連する変更が含まれます。
Monitor（監視）> **External Logs**（外部ログ）> **Traps ESM** > **Policy**（ポリシー）	ポリシー変更イベントには、ルール、保護レベル、コンテンツ更新、ハッシュ制御ログ、および判定への変更が含まれます。
Monitor（監視）> **External Logs**（外部ログ）> **Traps ESM** > **Agent**（エージェント）	エンドポイントで発生するエージェント変更イベントには、コンテンツ更新、ライセンス、ソフトウェア、接続状態、ワンタイムアクション ルール、プロセスとサービス、および検疫済みファイルへの変更が含まれます。
Monitor（監視）> **External Logs**（外部ログ）> **Traps ESM** > **Config**（設定）	ESM 設定変更イベントには、ライセンス、管理ユーザーと管理ロール、プロセス、制限設定、および条件へのシステム規模の変更が含まれます。

Panorama は、エンドポイント上の個々のセキュリティ イベントをネットワーク上のイベントと相関させて、エンドポイントとファイアウォール間の疑わしいまたは悪意のあるアクティビティを追跡できます。Panorama により特定された、相関されたイベントを表示するには、[Monitor] > [自動相関エンジン] > [相関されたイベント]を参照してください。

© 2019 Palo Alto Networks, Inc.

Monitor（監視）> Automated Correlation Engine（自動相関エンジン）

自動相関エンジンは、ネットワーク上のパターンを追跡し、疑わしい動作への拡散を示しているイベントや、有害なアクティブティに達したイベントの相関付けを行います。このエンジンは、個人のセキュリティ アナリストの役割を果たすものであり、ファイアウォール上のさまざまなログ セットに分離されたイベントを調査し、特定のパターンがないかデータをクエリして、点を結んで全体像を作り上げます。これにより、実用的な情報を得ることができます。

相関エンジンは、相関されたイベントを生成する相関オブジェクトを使用します。相関されたイベントによって証拠が照合されます。これにより、関連がないように見えるいくつかのネットワーク イベント間の共通点を追跡できるため、インシデント対応の機会が与えられます。

以下のモデルは自動相関エンジンをサポートします。

- Panorama — M-Series アプライアンスおよびバーチャル アプライアンス
- PA-3200 シリーズ ファイアウォール
- PA-5200 シリーズ ファイアウォール
- PA-7000 シリーズ ファイアウォール

知りたい内容	以下を参照
相関オブジェクトとは何ですか?	[Monitor] > [自動相関エンジン] > [相関オブジェクト]
相関されたイベントとは何ですか? 相関一致での一致の証拠をどこで確認できますか?	[Monitor] > [自動相関エンジン] > [相関されたイベント]
相関一致のグラフィック表示をどのように表示できますか?	ACC で Compromised Hosts（浸入されたホスト）ウィジットを表示してください。
その他の情報をお探しですか？	自動相関エンジンの使用

[Monitor] > [自動相関エンジン] > [相関オブジェクト]

エクスプロイトおよびマルウェアの拡散方法の進歩に対抗するため、相関オブジェクトはファイアウォールでのシグネチャベースのマルウェア検出機能を拡張します。相関オブジェクトは、各種ログ セット全体にわたって疑わしい動作パターンを識別するためのインテリジェンスを提供し、調査に必要な証拠を収集して、イベントにすばやく応答します。

相関オブジェクトは、マッチング パターンや、検索を実行するために使用するデータ ソース、パターン検索の対象期間を指定する定義ファイルです。パターンは、データソースをクエリする Boolean 型の条件構造です。各パターンに重大度およびしきい値が割り当てられます。しきい値は、定義された期間内にパターン マッチが発生する回数です。パターン マッチが発生すると、相関イベントがログに記録されます。

検索を実行するために使用するデータ ソースには、アプリケーション統計、トラフィック、トラフィック サマリー、脅威サマリー、脅威、データ フィルタリング、URL フィルタリングの各ログを含めることができます。たとえば、相関オブジェクトの定義には、感染したホストの証拠やマルウェア パターンの証拠がないかログをクエリするための一連のパターンのほか、トラフィック内でのマルウェアの横方向の移動、URL フィルタリング、および脅威ログのパターンを含めることができます。

© 2019 Palo Alto Networks, Inc.

相関オブジェクトは Palo Alto Networks® により定義され、コンテンツ更新と共にパッケージ化されます。コンテンツ更新を取得するには、有効な脅威防御ライセンスが必要です。

デフォルトでは、すべての相関オブジェクトが有効になっています。オブジェクトを無効化する場合は、オブジェクトを選択して **Disable**[無効化]をクリックします。

相関オブジェクト フィールド	の意味
名前およびタイトル	ラベルは、相関オジェクトで検出するアクティビティのタイプを示します。
ID	一意の番号を使用して相関オブジェクトを識別します。この番号は、6000 番台です。
カテゴリ	ネットワーク、ユーザー、またはホストに与える脅威または損害の種類を要約したもの。
状態	状態は、相関オブジェクトが有効 (アクティブ) か無効 (非アクティブ) かを示します。
の意味	これには、ファイアウォールまたは Panorama でログを分析するための対象となる一致条件を指定します。これは、有害なアクティビティまたはホストの疑わしい動作を識別するために使用する拡散パターンまたは進捗パスを記述するものです。

[Monitor] > [自動相関エンジン] > [相関されたイベント]

相関されたイベントはファイアウォールおよび Panorama での脅威検出機能を拡張し、ネットワーク上のユーザーやホストの疑わしい動作や異常な動作の証拠を収集します。

相関オブジェクトを使用すると、特定の条件または動作を中心にして、複数のログ ソースにわたって共通点を追跡できます。相関オブジェクトに指定した一連の条件がネットワーク上で確認されると、各一致が、相関されたイベントとしてログに記録されます。

相関されたイベントには、以下の表で示されている詳細が含まれます。

項目	の意味
一致時間	相関オブジェクトが一致をトリガーした時間。
更新時間	一致が最後に更新されたタイムスタンプ。
オブジェクト名	一致をトリガーした相関オブジェクトの名前。
送信元アドレス	トラフィックの送信元ユーザーの IP アドレス。
Source User（送信元ユーザー）	ディレクトリ サーバーからのユーザーおよびユーザー グループの情報（User-ID™ が有効な場合）。
重要度	発生した損害の程度に基づいてリスクを分類するレベル。
概要	相関されたイベントに関して収集された証拠を要約する説明。

詳細ログビューを表示する場合は、エントリの詳細（ ）をクリックします。詳細ログ ビューには、一致に関するすべての証拠が含まれます。

© 2019 Palo Alto Networks, Inc.

タブ	の意味
一致情報	**Object Details**[オブジェクトの詳細] - 一致をトリガーした相関オブジェクトに関する情報を提供します。相関オブジェクトの詳細は、「Monitor（監視）> Automated Correlation Engine（自動相関エンジン）> Correlation Objects（相関オブジェクト）」を参照してください。
	Match Details[一致の詳細] - 一致時間、一致の証拠の最終更新時間、イベントの重大度、イベントのサマリーを含む、一致の詳細のサマリー。
Match Evidence [一致の根拠]	このタブには、相関されたイベントを裏付けるすべての証拠が含まれます。セッションごとに収集された証拠に関する詳細情報が表示されます。

Correlated Events（相関イベント）タブでは、情報がグラフィック表示されます。**ACC** > **Threat Activity**（脅威アクティビティ）タブには Compromised Hosts（侵入されたホスト）ウィジットが表示されます。Compromised Hosts [侵入されたホスト] ウィジットでは、表示が送信元ユーザーと IP アドレスによって集約され、重大度でソートされます。

相関されたイベントがログに記録されたときの通知を設定するには、**Device**（デバイス）> **Log Settings**（ログ設定）タブまたは **Panorama** > **Log Settings**（ログ設定）タブに移動します。

© 2019 Palo Alto Networks, Inc.

Monitor > Packet Capture [監視 > パケット キャプチャ]

すべての Palo Alto Networks ファイアウォールにパケット キャプチャ (pcap) 機能が組み込まれており、これを使用して、ファイアウォールのネットワーク インターフェイスを通過するパケットをキャプチャできます。その後、キャプチャしたデータをトラブルシューティングの目的で使用したり、キャプチャしたデータを使用してカスタム アプリケーション シグネチャを作成したりできます。

パケット キャプチャ機能を使用すると *CPU* に大きな負荷がかかるため、ファイアウォールのパフォーマンスが低下する可能性があります。必要な場合にのみ、この機能を使用してください。また、必要なパケットを収集した後は、この機能を必ずオフにしてください。

知りたい内容	以下を参照
ファイアウォールでパケットをキャプチャするために使用できる他の方法は?	パケット キャプチャの概要
カスタム パケット キャプチャを生成するには?	カスタム パケット キャプチャの構成要素
ファイアウォールで脅威が検出されたときにパケット キャプチャを生成するには?	脅威パケット キャプチャの有効化
パケット キャプチャをダウンロードする場所は?	パケット キャプチャの概要
その他の情報をお探しですか ?	
• セキュリティ プロファイルに対して拡張パケット キャプチャを有効にします。	Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]
• パケット キャプチャを使用してカスタム アプリケーション シグネチャを記述します。	カスタム シグネチャを参照してください。
• パケット キャプチャをファイアウォール管理者が表示することを禁止します。	「Web インターフェイス管理者のアクセス権限」を定義します。
• 例を参照	「パケット キャプチャの実行」を参照してください。

パケット キャプチャの概要

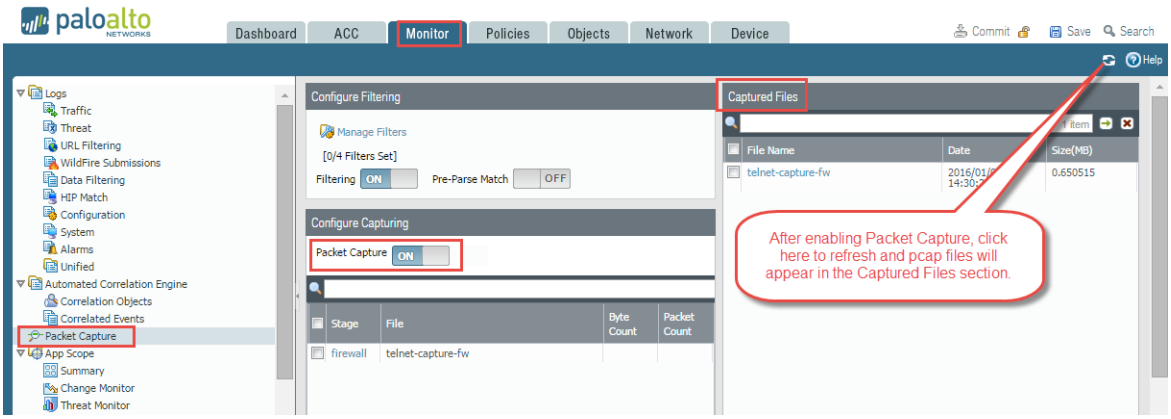
カスタム パケット キャプチャや脅威パケット キャプチャを実行するように Palo Alto Networks ファイアウォールを設定できます。

© 2019 Palo Alto Networks, Inc.

- **Custom Packet Capture**（カスタム パケット キャプチャ）— すべてのトラフィックのパケットをキャプチャしたり、定義したフィルタに基づいてトラフィックのパケットをキャプチャしたりできます。たとえば、特定の送信元および宛先の IP アドレスまたはポートに対するパケットのみをキャプチャするようにファイアウォールを設定できます。これらのパケット キャプチャを使用して、ネットワーク トラフィック関連の問題をトラブルシューティングしたり、アプリケーション属性を収集してカスタム アプリケーション シグネチャを作成したりできます（**Monitor**（監視）> **Packet Capture**（パケット キャプチャ））。ステージ（ドロップ、ファイアウォール、送受信）に基づいてファイル名を定義し、pcap が完了したら、Captured Files（キャプチャされたファイル）セクションで pcap をダウンロードします。
- **Threat Packet Capture**（脅威パケット キャプチャ）— ファイアウォールでウイルス、スパイウェア、または脆弱性が検出された場合にパケットをキャプチャします。この機能は、アンチウイルス、アンチスパイウェア、および脆弱性防御のセキュリティ プロファイルで有効にします。これらのパケット キャプチャによって、脅威を取り巻く状況が提供されるため、攻撃が成功したかどうかを判断したり、攻撃者が使用した方法について詳細を確認したりできます。脅威に対するアクションを許可または通知するように設定する必要があります。これを設定しない場合、脅威がブロックされ、パケットをキャプチャできません。このタイプのパケット キャプチャは、**Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）で設定します。pcap をダウンロード（ ）する場合は、**Monitor**（監視）> **Threat**（脅威）を選択します。

カスタム パケット キャプチャの構成要素

以下の表で、**Monitor**（監視）> **Packet Capture**（パケット キャプチャ）ページの構成要素について説明します。これらを使用して、パケット キャプチャの設定、パケット キャプチャの有効化、パケット キャプチャ ファイルのダウンロードを行います。



カスタム パケット キャプチャの構成要素	設定場所	の意味
フィルタの管理	フィルタリングの設定	カスタム パケット キャプチャを有効にする場合、フィルタを定義して、そのフィルタと一致するパケットのみをキャプチャする必要があります。これにより、pcap 内で必要な情報を容易に見つけることができます。また、ファイアウォールでパケット キャプチャを実行するために必要とされる処理能力を低減できます。 **Add**[追加] をクリックし、新しいフィルタを追加して、以下のフィールドを設定します。 • **ID** — フィルタの ID を入力または選択します。

© 2019 Palo Alto Networks, Inc.

カスタム パケット キャプチャの構成要素	設定場所	の意味
		• **Ingress Interface**[入力インターフェイス] – どの入力インターフェイス上でトラフィックをキャプチャするかを選択します。 • **Source**[送信元] – キャプチャするトラフィックの送信元 IP アドレスを指定します。 • **Destination**[宛先] – キャプチャするトラフィックの宛先 IP アドレスを指定します。 • **Src Port**[送信元ポート] – キャプチャするトラフィックの送信元ポートを指定します。 • **Dest Port**[宛先ポート] – キャプチャするトラフィックの宛先ポートを指定します。 • **Proto**[プロトコル] – フィルタリングするプロトコル番号を指定します (1 ~ 255)。たとえば、ICMP のプロトコル番号は 1 です。 • **Non-IP**[非 IP] – 非 IP トラフィックの処理方法を選択します (すべての IP トラフィックを除外する、すべての IP トラフィックを含める、IP トラフィックのみを含める、または IP フィルタを含めない)。非 IP トラフィックの例として、ブロードキャストや AppleTalk があります。 • **IPv6** – IPv6 パケットをフィルタに入れる場合は、このオプションをオンにします。
フィルタリング	フィルタリングの設定	フィルタの定義が終了したら、**Filtering**[フィルタリング] を**ON**に設定します。フィルタリングが **OFF** の場合、すべてのトラフィックがキャプチャされます。
事前解析一致	フィルタリングの設定	このオプションの目的は、トラブルシューティングを詳細に行うことです。パケットが入力ポートに入ると、いくつかの処理ステップを経て、事前設定されたフィルタと一致するかどうか解析されます。 何らかの障害によって、パケットがフィルタリング段階に到達しない場合があります。たとえば、ルート検索に失敗した場合などに起こります。 **Pre-Parse Match**[事前解析一致] 設定を **ON** に設定すると、システムに入力されるすべてのパケットに対して肯定一致が エミュレートされます。これにより、ファイアウォールはフィルタリング プロセスに到達していないパケットをキャプチャできるようになります。パケットがフィルタリング段階に到達できれば、フィルタ設定に応じて処理され、フィルタリング基準と一致しなければ破棄されます。
パケット キャプチャ	キャプチャの設定	切り替えスイッチをクリックして、パケット キャプチャを **ON** (オン) または **OFF** (オフ) にします。 少なくとも 1 つのキャプチャ ステージを選択する必要があります**Add**[追加] をクリックし、以下を指定します。

© 2019 Palo Alto Networks, Inc.

カスタム パケット キャプチャの構成要素	設定場所	の意味

		• **Stage**[ステージ] – パケットをキャプチャする時点を示します。
		  • **drop** – パケット処理でエラーが生じ、パケットが破棄される時点を指定します。
		  • **firewall** – パケットにセッション一致があるか、セッションの最初のパケットが正常に作成される時点。
		  • **receive**[受信] – データプレーン プロセッサでパケットが受け取られる時点を指定します。
		  • **transmit**[転送] – データプレーン プロセッサでパケットが送信される時点を指定します。
		• **File**[ファイル] – キャプチャ ファイル名を指定します。ファイル名は文字で始める必要があります。また、文字、数字、ピリオド、アンダースコア、またはハイフンを使用できます。
		• **Packet Count**[パケット数] – キャプチャが停止するまでの最大パケット数を指定します。
		• **Byte Count** (バイト数) – キャプチャが停止するまでの最大バイト数を指定します。

キャプチャされたファイル	キャプチャされたファイル	ファイアウォールで以前に生成されたカスタム パケット キャプチャのリストが含まれます。ファイルをクリックすると、ファイルがコンピュータにダウンロードされます。パケットキャプチャを削除する場合は、削除したいものを選択し、**Delete**[削除] します。 • **File Name**[ファイル名] – パケット キャプチャ ファイルのリストが表示されます。ファイル名は、キャプチャ ステージに対して指定したファイル名に基づきます。 • **Date**[日付] – ファイルが生成された日付。 • **Size (MB)**[サイズ (MB)] – キャプチャ ファイルのサイズ。 パケットキャプチャをオンに切り替えて、その後オフに切り替えた後に、リスト上に新しいすべての PCAP ファイルを表示する場合は、更新 ( ) をクリックする必要があります。
すべての設定をクリア	設定	パケット キャプチャをオフにして、すべてのパケット キャプチャ設定をクリアするには、**Clear All Settings**[すべての設定をクリア] をクリックします。 これを行っても、セキュリティ プロファイルに設定されたパケット キャプチャはオフになりません。セキュリティ プロファイルでパケット キャプチャを有効にする方法の

© 2019 Palo Alto Networks, Inc.

カスタム パケット キャプチャの構成要素	設定場所	の意味
		詳細は、「脅威パケット キャプチャの有効化」を参照してください。

脅威パケット キャプチャの有効化

- Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）

ファイアウォールで脅威を検出したときにパケットをキャプチャできるようにするには、セキュリティ プロファイルでパケット キャプチャ オプションを有効にします。

まず、**Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）を選択し、以下の表の説明に従って目的のプロファイルを変更します。

セキュリティ プロファイルのパケット キャプチャ オプション	場所
Antivirus [アンチウイルス]	カスタムのアンチウイルス プロファイルを選択し、**Antivirus**[アンチウイルス] タブで **Packet Capture**[パケットキャプチャ] を選択します。
アンチスパイウェア	カスタムのアンチスパイウェア プロファイルを選択し、**DNS Signatures**[DNS シグネチャ] タブをクリックします。**Packet Capture**[パケット キャプチャ] ドロップダウンリストで **single-packet**または **extended-capture**を選択します。
脆弱性防御	カスタムの脆弱性防御プロファイルを選択し、**Rules**[ルール] タブで、**Add**[追加] をクリックして新しいルールを追加するか、既存のルールを選択します。次に、**Packet Capture**[パケット キャプチャ] ドロップダウンリストで **single-packet** または **extended-capture** を選択します。

アンチスパイウェアおよび脆弱性防御のプロファイルでは、例外時のパケット キャプチャを有効にすることもできます。*Exceptions[例外]* タブをクリックし、シグネチャの*Packet Capture [パケット キャプチャ]* 列でドロップダウンリストをクリックし、*single-packet*または*extended-capture*を選択します。

（任意）キャプチャした（グローバル設定に基づく）パケット数に基づいて脅威パケット キャプチャの長さを定義するには、**Device**（デバイス）> **Setup**（セットアップ）> **Content-ID**を選択し、Content-ID™ Settings（Content-ID™ 設定）セクションで **Extended Packet Capture Length (packets)**（拡張パケット キャプチャ長（パケット））フィールドを変更します（1 ~ 50 の範囲、デフォルトは 5）。

セキュリティ プロファイルでパケット キャプチャを有効にしたら、プロファイルがセキュリティ ルールに含まれていることを確認する必要があります。セキュリティ プロファイルをセキュリティ ルールに追加する方法の詳細は「セキュリティ ポリシーの概要」を参照してください。

セキュリティプロファイルでパケットキャプチャが有効化されている際にファイアウォールが脅威を検出した場合、パケットキャプチャをダウンロード（）あるいはエクスポートすることができます。

© 2019 Palo Alto Networks, Inc.

Monitor > App Scope [監視 > アプリケーション スコープ]

以下のトピックでは、アプリケーション スコープの機能について説明します。

- アプリケーション スコープの概要
- アプリケーション スコープのサマリー レポート
- アプリケーション スコープの変化モニター レポート
- アプリケーション スコープの脅威モニター レポート
- アプリケーション スコープの脅威マップ レポート
- アプリケーション スコープのネットワーク モニター レポート
- アプリケーション スコープのトラフィック マップ レポート

アプリケーション スコープの概要

アプリケーション スコープのレポートには、ネットワークの以下の内容がグラフ表示されます。

- アプリケーション使用状況とユーザー アクティビティの変化
- ネットワーク帯域幅の大部分を占有しているユーザーやアプリケーション
- ネットワークの脅威

アプリケーション スコープのレポートを使用すると、異常な動作や予期しない動作をすばやく見つけて、問題のある動作を特定できます。レポートはそれぞれ、ネットワークに関する動的でユーザーがカスタマイズ可能なウィンドウに表示されます。レポートには、表示するデータや範囲を選択するオプションがあります。Panorama では、表示される情報の**Data Source**[データ ソース]を選択することもできます。デフォルトのデータソース (新しいPanoramaインストールの場合) では、管理対象ファイアウォールによって転送されたログを格納しているPanoramaのローカルデータベースが使用されます。アップグレードの場合、デフォルトのデータソースは**Remote Device Data**[リモートデバイスデータ] (管理対象ファイアウォールのデータ) になります。管理対象ファイアウォールから直接データの集約ビューを取得および表示するには、ソースを **Panorama** から **Remote Device Data** (リモート デバイス データ) に切り替える必要があります。

チャートの線や棒にポインタを置くかクリックすると、ACC に切り替わり、特定のアプリケーション、アプリケーション カテゴリ、ユーザー、またはソースに関する詳しい情報が示されます。

アプリケーション コマンド センターのチャート	の意味
概要	アプリケーション スコープのサマリー レポート
変化モニター	アプリケーション スコープの変化モニター レポート
脅威モニター	アプリケーション スコープの脅威モニター レポート
脅威マップ	アプリケーション スコープの脅威マップ レポート
ネットワーク モニター	アプリケーション スコープのネットワーク モニター レポート
トラフィック マップ	アプリケーション スコープのトラフィック マップ レポート

© 2019 Palo Alto Networks, Inc.

アプリケーション スコープのサマリー レポート

サマリー レポートには、使用量が増加した、減少した、および帯域幅の占有量が多い上位 5 つのアプリケーション、アプリケーション カテゴリ、ユーザー、および送信元のチャートが表示されます。

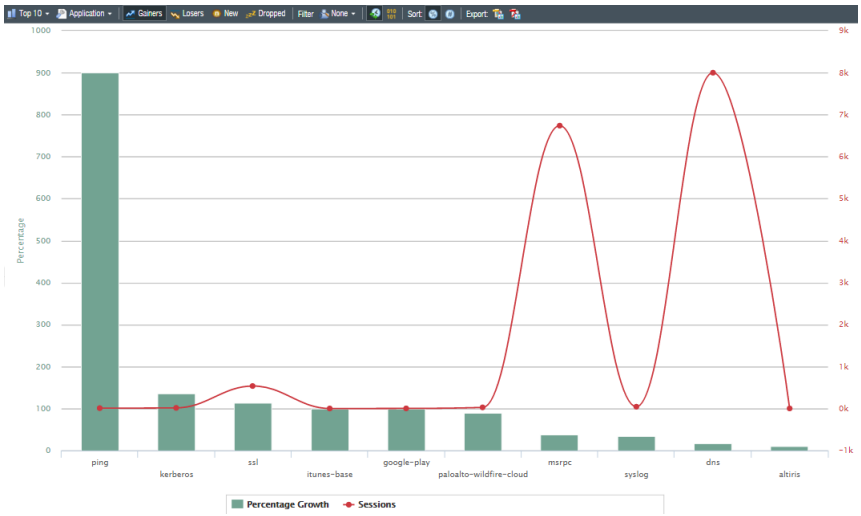
サマリーレポートのチャートをPDF形式でエクスポートする場合は**Export**[エクスポート] (Export:) をクリックします。各チャートが 1 ページの PDF として出力に保存されます。

アプリケーション スコープのサマリー レポート

アプリケーション スコープの変化モニター レポート

変化モニター レポートには、指定した期間の変化が表示されます。たとえば、以下の図は、過去 24 時間と比較して過去 1 時間に使用量が増加した上位のアプリケーションを示しています。上位アプリケーションはセッション数によって決定され、パーセント別にソートされます。

アプリケーション スコープの変化モニター レポート



このレポートには、以下のオプションが表示されます。

© 2019 Palo Alto Networks, Inc.

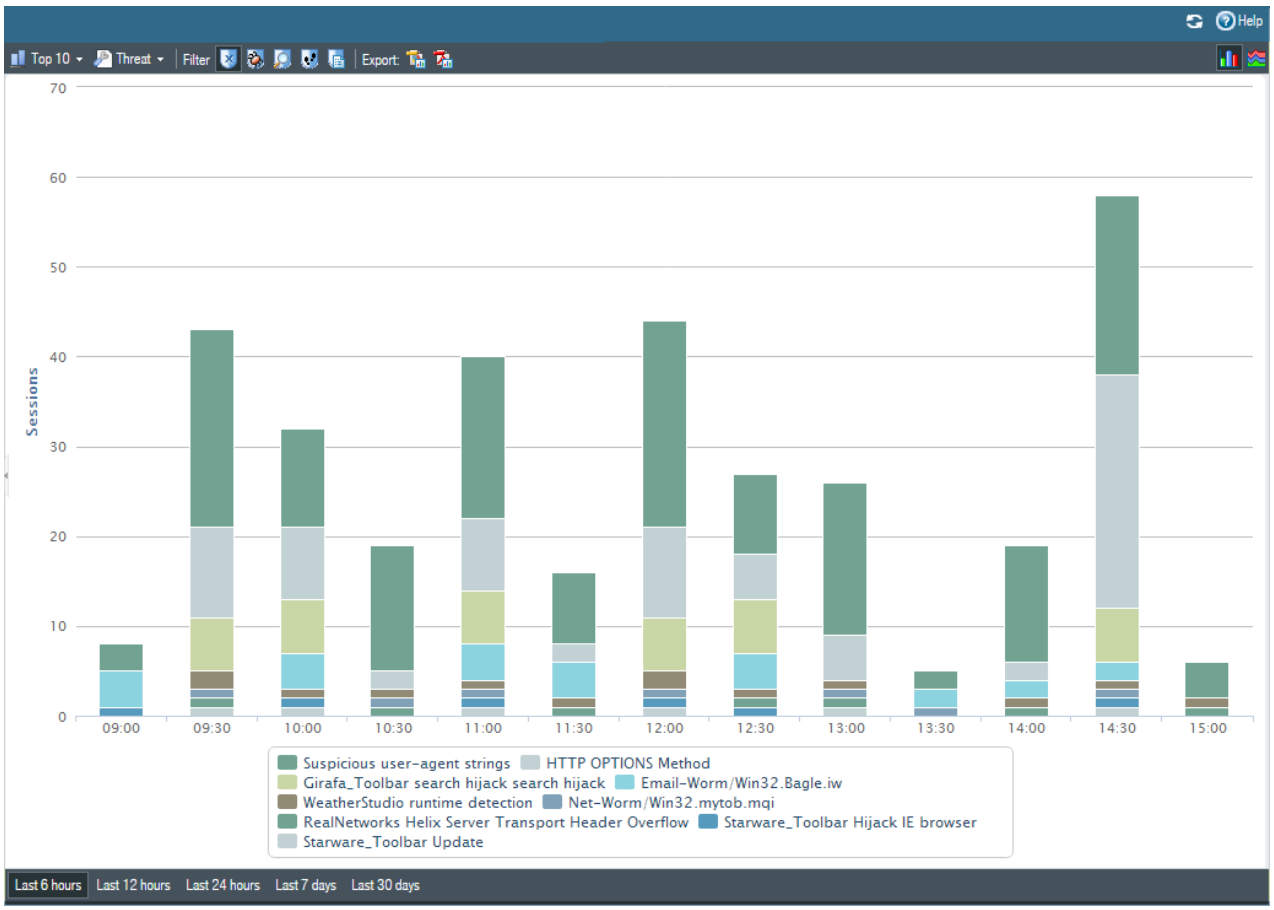
変化モニター レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
Application [アプリケーション]	レポートに含める項目を指定します。Application[アプリケーション]、Application Category[アプリケーションカテゴリ]、Source[送信元]、Destination[宛先]
増加アプリケーション	指定期間を比較し増加した項目を表示します。
利用が減ったアプリケーション	指定期間を比較し減少した項目を表示します。
新規	指定期間を比較しあらたに検出された項目を表示します。
ドロップ	指定期間を比較し検出されなくなった項目を表示します。
フィルタ	フィルタを適用して、選択した項目のみを表示します。None (なし) を選択すると、すべてのエントリが表示されます。
セッション情報やバイト情報を表示します。	セッション情報またはバイト情報のどちらを表示するかを指定します。
ソート	パーセンテージまたは実増加のどちらでエントリをソートするかを指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
下部バー	
比較 (間隔)	変化モニターの比較対象期間を指定します。

アプリケーション スコープの脅威モニター レポート

脅威モニター レポートには、選択した期間にわたって上位を占める脅威の数が表示されます。たとえば、以下の図は、過去 6 時間における上位 10 件の脅威タイプを示しています。

アプリケーション スコープの脅威モニター レポート

© 2019 Palo Alto Networks, Inc.



チャートの下の凡例のように、各タイプの脅威が色分けして示されます。このレポートには、以下のオプションが表示されます。

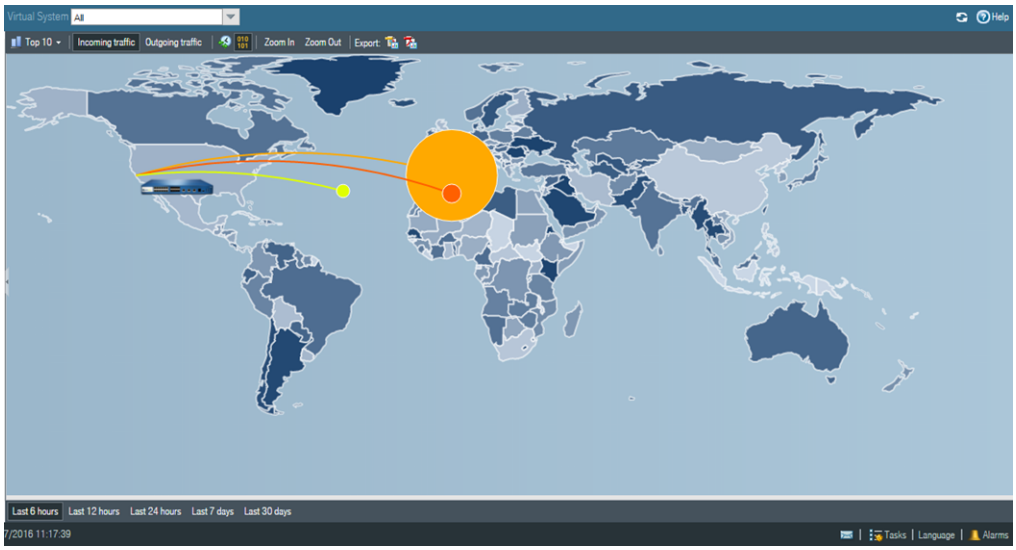
脅威モニター レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
脅威	測定する項目を指定します。Threat[脅威]、Threat Category[脅威カテゴリ]、Source[送信元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した項目のみを表示します。
	情報を表示するグラフ (積み重ね棒グラフまたは積み重ね面グラフ) を指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
下部バー	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	表示対象期間を指定します。

© 2019 Palo Alto Networks, Inc.

アプリケーション スコープの脅威マップ レポート

脅威マップ レポートには、重大度を含めた脅威の地理的ビューが表示されます。

アプリケーション スコープの脅威マップ レポート



チャートの下の凡例のように、各タイプの脅威が色分けして示されます。マップ上の国をクリックし、必要に応じて**Zoom In**[拡大]と**Zoom Out**[縮小]を行います。このレポートには、以下のオプションが表示されます。

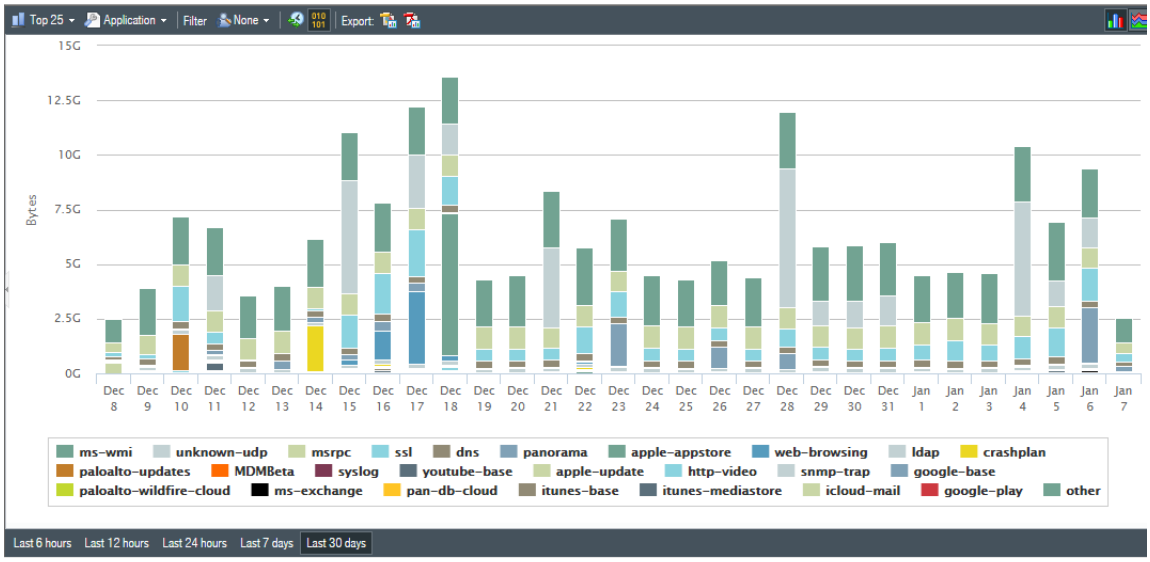
脅威マップ レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
受信した脅威	インバウンド方向 (外部から) の脅威を示します。
送信した脅威	アウトバウンド方向 (外部へ) の脅威を示します。
フィルタ	フィルタを適用して、選択した項目のみを表示します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
下部バー	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	表示対象期間を指定します。

アプリケーション スコープのネットワーク モニター レポート

ネットワーク モニター レポートには、指定した期間にわたって複数のネットワーク アプリケーションによって占有されていた帯域幅が表示されます。図の下の凡例のように、各タイプのネットワーク アプリケーションが色分けして示されます。たとえば、以下の図は、セッション情報に基づく過去 7 日間のアプリケーション帯域幅を示しています。

© 2019 Palo Alto Networks, Inc.

アプリケーション スコープのネットワーク モニター レポート



このレポートには、以下のオプションが表示されます。

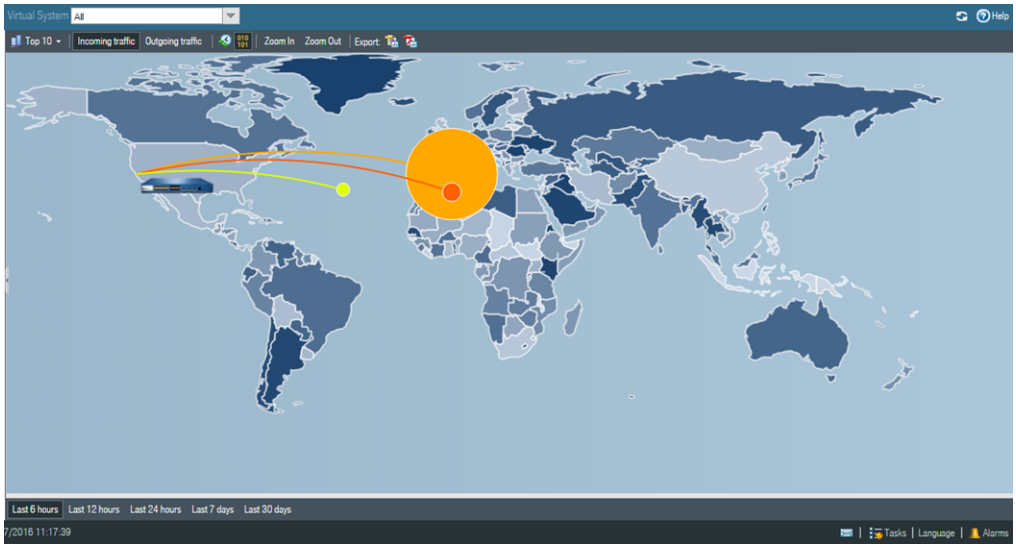
ネットワーク モニター レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
Application [アプリケーション]	レポートに含める項目を指定します。Application[アプリケーション]、Application Category[アプリケーションカテゴリ]、Source[送信元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した項目のみを表示します。**None**[なし] を選択すると、すべてのエントリが表示されます。
セッション情報やバイト情報を表示します。	セッション情報またはバイト情報のどちらを表示するかを指定します。
	情報を表示するグラフ (積み重ね棒グラフまたは積み重ね面グラフ) を指定します。
エクスポート	グラフを .png イメージまたは PDF として エクスポートします。
下部バー	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	変更措置が取られる期間を示します。

アプリケーション スコープのトラフィック マップ レポート

トラフィック マップ レポートには、セッション数またはフロー数に応じて、トラフィック フローの地理的ビューが表示されます。

© 2019 Palo Alto Networks, Inc.

アプリケーション スコープのトラフィック マップ レポート



チャートの下の凡例のように、各タイプのトラフィックが色分けして示されます。このレポートには、以下のオプションが表示されます。

トラフィック マップ レポートのオプション	の意味
上部バー	
トップ 10	上位からいくつの項目を表に表示するかを指定します。
受信トラフィック	受信トラフィックを表示します。
送信トラフィック	送信トラフィックを表示します。
セッション情報やバイト情報を表示します。	セッション情報またはバイト情報のどちらを表示するかを指定します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
下部バー	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days	変更措置が取られる期間を示します。

© 2019 Palo Alto Networks, Inc.

Monitor > Session Browser [監視 > セッションブラウザ]

Monitor > **Session Browser**[監視 > セッションブラウザ]から、ファイアウォール上で現在実行中のセッションの参照とフィルタを行います。このページのフィルタリング オプションの詳細は、「ログ アクション」を参照してください。

© 2019 Palo Alto Networks, Inc.

Monitor（監視）> Block IP List（ブロック IP リスト）

ブロック リストに IP アドレスを配置するようにファイアウォールを設定できます。これには、次を含めいくつかの方法があります。

- **Protect**（保護）に対するアクションを含む DoS プロテクション ポリシー ルールを設定し、そのルールに Classified DoS Protection（分類された DoS プロテクション）プロファイルを適用します。このプロファイルにはブロック期間が含まれます。
- **Block Ip**（ブロック **IP**）に対するアクションを含むルールを使用する Vulnerability Protection（脆弱性防御）プロファイルを使用してセキュリティ ポリシー ルールを設定し、そのルールをゾーンに適用します。

ブロック IP リストは、PA-3200 シリーズ、PA-5200 シリーズ、および PA-7000 シリーズのファイアウォールでサポートされます。

知りたい内容	以下を参照
ブロック IP リストの各フィールドは何を示しますか?	ブロック IP リスト エントリ
ブロック IP リストのエントリをフィルタリング、操作、削除する方法は?	ブロック IP リスト エントリの表示または削除
その他の情報をお探しですか？	アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ 新規セッションのフラッド攻撃に対する Dos プロテクション Monitor Blocked IP Addresses（ブロックされた IP アドレスのモニター）

ブロック IP リスト エントリ

- 監視 > **BlockIPList**

以下の表で、ファイアウォールがブロックしている送信元 IP アドレスのブロック リスト エントリについて説明します。

項目	の意味
ブロック タイム	IP アドレスがブロック IP リストに入った月/日および時:分:秒です。
タイプ	ブロック アクションのタイプです。ハードウェア（hw）またはソフトウェア（sw）のいずれが IP アドレスをブロックしたのかを示します。 脆弱性防御プロファイルを使用する DoS プロテクション ポリシーまたはセキュリティ ポリシーを設定し、送信元 IPv4 アドレスからの接続をブロックするようにすると、それらのパケットが CPU またはパケット バッファ リソースを使用する前に、ハードウェアのトラフィックをファイアウォールが自動的にブロックし

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ます。攻撃トラフィックがハードウェアのブロック容量を超えた場合、ファイアウォールはソフトウェアを使用してトラフィックをブロックします。
送信元 IP アドレス	ファイアウォールがブロックしたパケットの送信元 IP アドレスです。
Ingress ゾーン	ファイアウォールにパケットが入ったインターフェイスに割り当てられたセキュリティ ゾーンです。
残り時間	IP アドレスのブロック IP リスト掲載残り時間 (秒) です。
ブロック ソース	ブロック IP アクションが指定されている、分類された DoS プロテクション プロファイルの名前または脆弱性防御オブジェクト名です。
ブロック済み IP 合計: x/y (z% 使用)	ファイアウォールがサポートしている全体のブロック対象 IP アドレスの数 (y) のうちの、ブロック済み IP アドレスの数 (x)、およびブロック済みの IP アドレスが使用している割合 (z) です。

ブロック IP リスト エントリの表示または削除

ブロック IP リストのエントリを操作して、エントリの詳細情報を表示し、必要に応じてエントリを削除します。

ブロック IP リスト エントリの表示または削除	
特定のブロック IP リスト情報を検索する	列の値を選択すると、**Filters** (フィルタ) フィールドにフィルタが入力され、右矢印をクリックすると、該当の値を持つエントリの検索が開始されます。 フィルタを削除するには、X をクリックします。
現在の画面以外のブロック IP リスト エントリを表示する	**Page** (ページ) フィールドにページ番号を入力するか、一重矢印をクリックして次のページまたは前のページのエントリを表示します。二重矢印をクリックすると、最後のページまたは最初のページのエントリが表示されます。
ブロック IP リスト上の IP アドレスに関する詳細情報を表示する	エントリの Source IP Address (送信元 IP アドレス) をクリックすると、Network Solutions の Who Is にリンクされ、アドレスに関する情報が表示されます。
ブロック IP リスト エントリを削除する	エントリを選択し、**Delete** (削除) をクリックします。 *Web*インターフェイスからサポートされているのはハードウェアエントリの削除のみです。ただし、*CLI* からはハードウェアとソフトウェアの両方のエントリの削除がサポートされています。
ブロック IP リスト全体をクリアする	**Clear All** (すべてクリア) をクリックすると、すべてのエントリが永久に削除されます。つまり、これらのパケットはブロックされなくなります。 *Web*インターフェイスからサポートされているのはハードウェアエントリのブロック *IP* リストのクリアのみです。ただし、ハード

© 2019 Palo Alto Networks, Inc.

ブロック IP リスト エントリの表示または削除	
	ウェアとソフトウェアの両方のエントリのクリアは、*CLI* からサポートされています。

© 2019 Palo Alto Networks, Inc.

Monitor > Botnet [監視 > ボットネット]

ボットネットレポート機能により、ネットワーク内でボットネットに感染した可能性のあるホストを、挙動をもとに特定することができます。レポートには、各ホストのボットネット感染の可能性が1から5の信頼性スコアで表示されます（5は感染の可能性が高いことを示します）。レポートのスケジュールを設定したり、手動でレポートを実行する前に、不審と判定するトラフィックのタイプを設定する必要があります。ボットネット レポート アウトプットの読み方については PAN-OS® 管理者ガイドに記載されています。

- ボットネット レポートの設定
- ボットネットの設定

ボットネット レポートの設定

- Monitor > Botnet > Report Setting [監視 > ボットネット > レポート設定]

ボットネット レポートを生成する前に、ボットネット活動の可能性があるトラフィックを指定する必要があります（「ボットネット レポートの設定」を参照してください）。毎日のレポート作成をスケジューリングする場合や手動で実行する場合は、**Report Setting**[レポート設定]をクリックし、以下のフィールドを入力します。レポートをエクスポートする場合は、レポートを選択し、**Export to PDF**[PDFにエクスポート]、**Export to CSV**[CSVにエクスポート]、あるいは**Export to XML**[XMLにエクスポート]を選択します。

ボットネット レポートの設定	の意味
ランタイムフレームのテスト	レポートの期間を選択します – **Last 24 Hours**（過去 24 時間）（デフォルト）、または **Last Calendar Day**（前日の一日間）
今すぐ実行	今すぐに手動でレポートを生成する場合は**Run Now**[今すぐ実行]をクリックします。レポートはボットネットレポートダイアログの新しいタブで表示されます。
行数	レポートに表示される行数を指定します（デフォルトは100）。
スケジュール設定	毎日自動的にレポートを生成する場合はこのオプションを選択します。デフォルトでは、このオプションが有効化されています。
クエリ ビルダー	（任意）レポートに送信元/宛先 IP アドレス、ユーザー、ゾーンなどの属性別にフィルタをかける場合は、クエリ ビルダーにクエリを **Add**（追加）します。例えば、IPアドレス192.0.2.0から発信されるトラフィックにボットネット活動の可能性がないとわかっている場合は、クエリに`not (addr.src in 192.0.2.0)`を追加し、レポートからそのホストを除外することができます。 • **Connector**[条件式] – 論理結合子 (**and**/**or**) を指定します。**Negate**[除外]を選択した場合、クエリに指定されたホストがレポートから除外されます。 • **Attribute**[属性] - ファイアウォールがボットネット活動を検索するホストのゾーン、アドレス、またはユーザーを指定します。 • **Operator**[演算子] – **Attribute**[属性]を**Value**[値]に関連付ける際の演算子を指定します。 • **Value**[値] – クエリに検出させる値を入力します。

© 2019 Palo Alto Networks, Inc.

ボットネットの設定

- Monitor > Botnet > Configuration [監視 > ボットネット > 設定]

ボットネット活動の可能性があるトラフィックのタイプを指定する場合は、**Botnet**[ボットネット]ページの右側にある**Configuration**[設定]をクリックし、以下のフィールドを入力します。レポートの設定後、手動で実行するか、定期的に実行するようにスケジュール設定を行うことができます（Monitor（監視）> PDF Reports（PDF レポート）> Manage PDF Summary（PDF サマリーの管理）を参照してください）。

デフォルトの *Botnet* レポート設定が最善です。デフォルトの値が誤検出を発生させていると考えられる場合は、*Palo Alto Networks* が値を再評価できるよう、サポートチケットを作成してください。

ボットネットの設定	の意味
HTTP トラフィック	レポートに含まれるHTTPトラフィックのタイプごとの**Count**[カウント数]を**Enable**[有効化]します。ここで設定した**Count**[カウント数]分の各トラフィックイベントが発生すると、レポート上ではそのトラフィックに関係したホストに対し高いスコアが割り当てられます（高いスコアはボットネット感染の可能性が高いことを示します）。イベント数が **Count**（数）より少ない場合、レポートにはより低い確度スコアが表示されるか、（特定のトラフィックタイプでは）ホストのエントリが表示されなくなります。 • **Malware URL visit**[マルウェアURLへのアクセス]（範囲は 2～1000、デフォルトは 5）— マルウェアおよびボットネットの URL のフィルタリングカテゴリに基づき、既知のマルウェア URL に対して通信しているユーザーを特定します。 • **Use of dynamic DNS**[動的DNSの使用]（範囲は 2～1000、デフォルトは 5）- マルウェア、ボットネット通信、またはエクスプロイトキットの可能性がある動的DNSクエリトラフィックを検索します。一般的に、動的DNSドメインはとてもリスクが高いものとされています。多くの場合、マルウェアはIPのブラックリスト入りを免れるために動的DNSを使用しています。このようなトラフィックをブロックするために、URL フィルタリングを使うことも検討してください。 • **Browsing to IP domains**[IPドメインを参照]（範囲は 2～1000、デフォルトは10）— URLではなく、IPドメインを参照するユーザーを特定します。 • **Browsing to recently registered domains**[最近登録されたドメインを参照]（範囲は 2～1000、デフォルトは10）— 過去30日以内に登録されたドメイン名を持つサイトへのトラフィックを検索します。攻撃者、マルウェア、そしてエクスプロイトキットは多くの場合、新しく登録されたドメインを使用しています。 • **Executable files from unknown sites**[不明サイトからの実行可能ファイル]（範囲は 2～1000、デフォルトは10）— 未知のURLサイトから実行形式のファイルをダウンロードされた通信を特定します。多くの感染例には実行ファイルが関係しているため、その他の不審なトラフィックと結びついている場合はホストの調査を優先的に行うことをお勧めします。
不明なアプリケーション	不審かつ不明なTCPまたは不明なUDPアプリケーションに結びついたトラフィックをレポートに含めるかどうかのしきい値を設定します。 • **Sessions Per Hour**[1時間当たりのセッション]（範囲は1～3600、デフォルトは10）- 1時間当たり、指定した回数までのアプリケーションセッションに関わったトラフィックがレポートに加えられます。

© 2019 Palo Alto Networks, Inc.

ボットネットの設定	の意味
	• **Sessions Per Hour**[1時間当たりの宛先の数]（範囲は1～3600、デフォルトは10）- 1時間当たり、指定した数までのアプリケーションの宛先に関わったトラフィックがレポートに加えられます。 • **Minimum Bytes**[最小バイト数]（範囲は1～200、デフォルトは50）- 指定したサイズ以上のアプリケーションペイロードのトラフィックがレポートに加えられます。 • **Maximum Bytes**[最大バイト数]（範囲は1～200、デフォルトは100）- 指定したサイズ以下のアプリケーションペイロードのトラフィックがレポートに加えられます。
IRC	IRCサーバーに関係するトラフィックを含める場合はこのオプションを使用します。

© 2019 Palo Alto Networks, Inc.

Monitor（監視）> PDF Reports（PDF レポート）

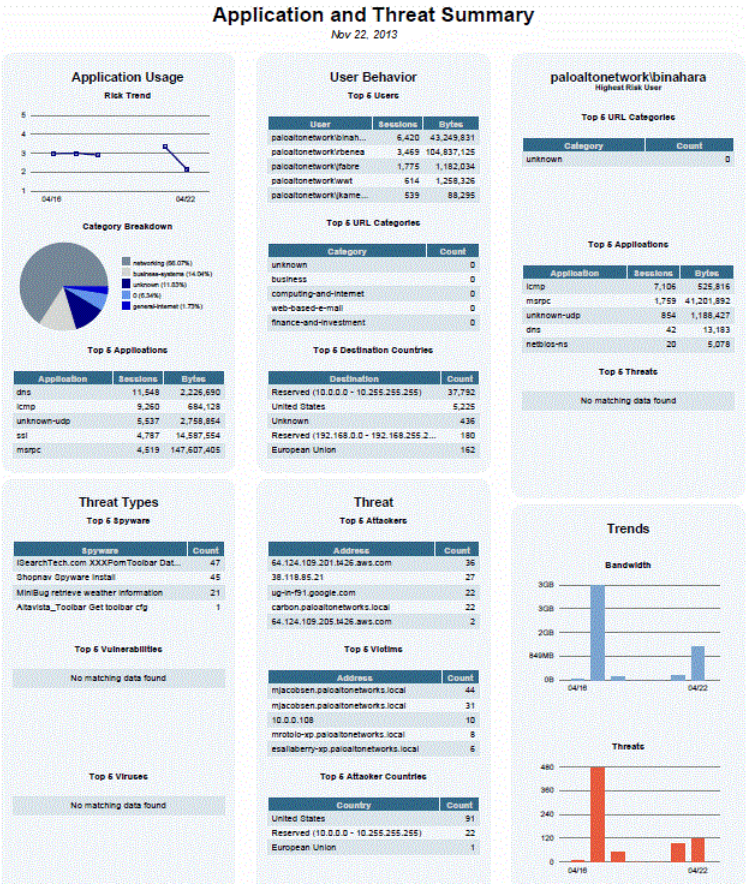
以下のトピックでは、PDF レポートについて説明します。

- Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レポート > PDF サマリーの管理]
- Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > ユーザー アクティビティ レポート]
- Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレポート > Saasアプリケーションの使用状況]
- Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポート グループ]
- Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子メール スケジューラ]

Monitor > PDF Reports > Manage PDF Summary {監視 > PDF レポート > PDF サマリーの管理]

PDF サマリー レポートには、各カテゴリの上位 5 件（上位 50 件ではない）のデータに基づき、既存のレポートから集められた情報が含まれています。このレポートには、別のレポートでは表示されないトレンド チャートも表示されます。

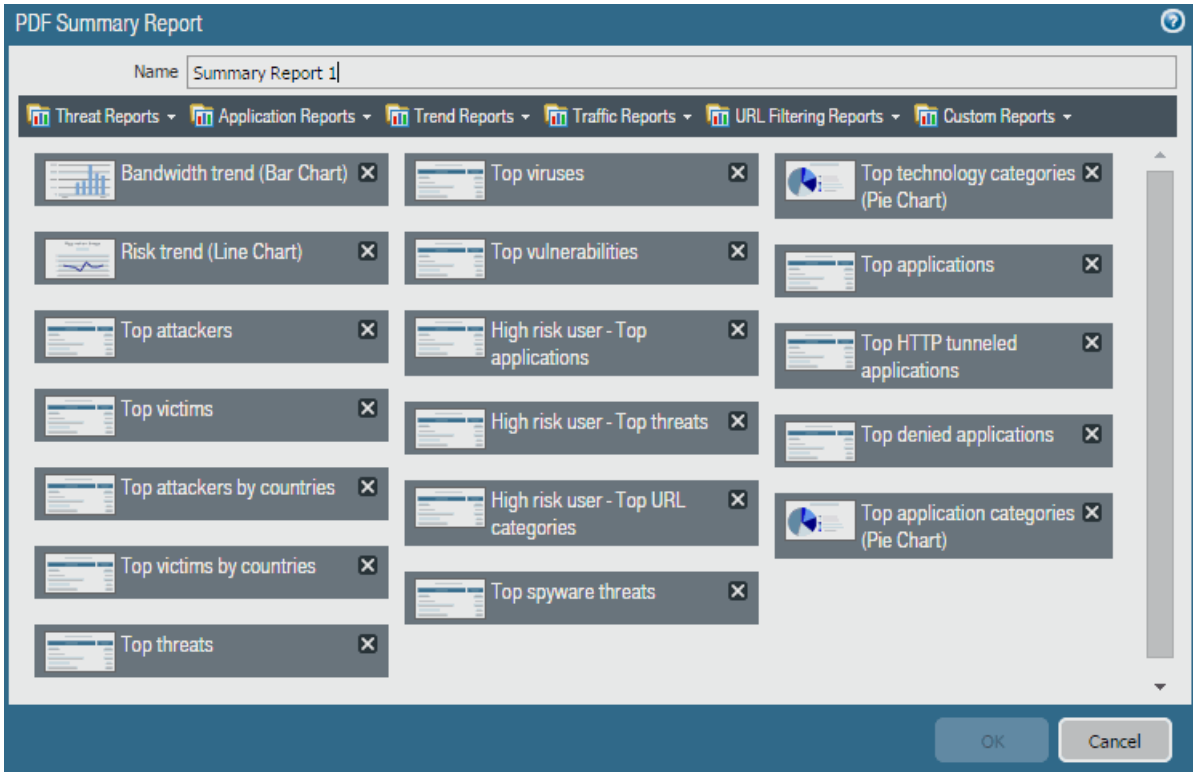
PDF サマリー レポート



© 2019 Palo Alto Networks, Inc.

PDF サマリー レポートを作成するには、**Add** (追加) をクリックします。**PDF Summary Reports** (**PDF** サマリー レポート) ページが開き、使用可能なすべてのレポート項目が表示されます。

PDF レポートの管理



以下のオプションを 1 つ以上使用してレポートを設計します。

- レポートから除外する項目については除外 ([X]) をクリックするか、該当するドロップダウンリストから項目をクリアします。
- 該当するドロップダウンリストから選択することで項目を追加することができます。
- 項目をドラッグアンドドロップして、レポートの別のエリアに移動します。

最大 *18* 個のレポート項目を使用できます。既に *18* 個の項目が含まれている場合は、新たに項目を追加する前に既存の項目を削除する必要があります。

レポートを **Save** (保存) するには、レポート名を入力し、**OK** をクリックします。

PDF レポートを表示するには、 **Monitor (監視)** > **Reports (レポート)**を選択し、 **PDF Summary Report (サマリー レポート)** をクリックしてレポートを選択し、カレンダーの日付をクリックして その日のレポートをダウンロードしてください。

新しい *PDF* サマリー レポートは、そのレポートが実行されるまで表示されません。レポートは毎日午前 *2* 時に自動的に実行されます。

Monitor > PDF Reports > User Activity Report [監視 > PDFレポート > ユーザー アクティビティ レポート]

個々のユーザーまたはユーザー グループのアクティビティの概要を示すレポートを作成するには、このページを使用します。**Add** (追加) をクリックし、以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

ユーザー/グループ アクティビティ レポート設定	の意味
氏名	レポートを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
タイプ	ユーザー アクティビティ レポートの場合:**User**[ユーザー] を選択し、レポートの対象となるユーザーの **Username**[ユーザー名] または **IP address**[IPアドレス]（IPv4 または IPv6）を入力します。
	グループ アクティビティ レポート:**Group**[グループ]を選択し、**Group Name**[グループ名]を入力します。
その他のフィルタ	ユーザー/グループ アクティビティ レポート用のフィルタを作成するには、**Filter Builder**（フィルタ ビルダー）を選択します。
期間	ドロップダウンリストからレポートの期間を選択します。
Include Detailed Browsing	（任意）レポートに詳細なURLログを追加するには、このオプションをオンにします。 詳細な閲覧情報には、選択したユーザーまたはユーザー グループの大量の (何千もの) ログが含まれる可能性があり、その結果、レポートが非常に大きくなる可能性があります。

グループ アクティビティ レポートには、*URL* カテゴリ別ブラウザ サマリーは含まれません。その他すべての情報は、ユーザー アクティビティ レポートとグループ アクティビティ レポートで共通です。

オンデマンドでレポートを実行するには、[今すぐ実行] をクリックします。レポートに表示する行の最大数を変更するには、「ログとレポートの設定」を参照してください。

レポートを保存するには、**OK** をクリックします。次に、レポートの電子メール配信をスケジューリングできます（Monitor（監視）> PDF Reports（PDF レポート）> Email Scheduler（電子メール スケジューラ））。

ログ フィルタの追加

レポートをカスタマイズするには、ユーザー アクティビティ レポートとグループ アクティビティ レポートにログ フィルタを作成します。アプリケーション、アプリケーションの特性などに基づいてアクティビティ レポートをフィルタすることができます。たとえば、認証を取得していない SaaS アプリケーションに興味がある場合は、このアプリケーション特性に基づいてフィルタを作成できます。

ログ フィルタ フィールドの追加	の意味
ログ フィルタ テキスト ボックス	ログに適用するフィルタを書き込みます。複数のフィルタを書き込むことができます。
結合子	追加のフィルタリング オプションを付けてフィルタを追加します。書き込んだフィルタをコネクタに適

© 2019 Palo Alto Networks, Inc.

ログ フィルタ フィールドの追加	の意味
	用しない場合は、**Negate**（除外）ボックスを選択します。
属性	メニューから追加する属性を選択します。
演算子	属性が値と等しいかどうかを選択します。
値	属性の値を設定します。使用可能な場合、可能な値を含むドロップダウン メニューが利用可能になります。

Apply（適用）を選択すると、作成したフィルタをユーザー アクティビティまたはグループ アクティビティ レポートに適用します。

Monitor > PDF Reports > SaaS Application Usage [監視 > PDFレポート > Saasアプリケーションの使用状況]

このページを使用して、ネットワークを通過する SaaS アプリケーションに関連するセキュリティ リスクを要約した SaaS アプリケーション使用状況レポートを生成します。この事前定義済みのレポートは、認可されたアプリケーションと認可されていないアプリケーションの比較を示し、不利なホスティング特性を持つ危険な SaaS アプリケーションを要約し、詳細ページに各カテゴリの最上位のアプリケーションをリストすることにより、アプリケーションのアクティビティをハイライト表示します。この詳細なリスク情報を使用して、ネットワーク上で許可またはブロックしたい SaaS アプリケーションのポリシーを適用することができます。

正確で有益なレポートを生成するには、ネットワーク上で許可されたアプリケーションにタグを付ける必要があります（「Generate the SaaS Application Usage Report（SaaS アプリケーション使用状況レポートの生成）」を参照）。この事前設定タグを持たないアプリケーションは、ファイアウォールおよびPanoramaはネットワーク上で不許可となっているものと判断されます。不許可の SaaS アプリケーションは情報セキュリティの脅威となる可能性があるため、ネットワークで許可されたアプリケーションと不許可のアプリケーションを知っておくことが重要です。不許可のアプリケーションはネットワーク上での動作を許されておらず、脅威に対する脆弱性とプライベート情報あるいは機密情報の漏えいに繋がる可能性があります。

すべてのファイアウォールまたはデバイス グループでアプリケーションに一貫してタグを付けるようにしてください。あるアプリケーションが一方の仮想システム上では許可されたアプリケーションとしてタグ付けされ、もう一方では不許可とされている場合、あるいは *Panorama* では親デバイスグループで不許可とされていて、子デバイスグループでは許可タグが付与されている場合（またはその逆）、*SaaS* アプリケーション使用状況レポートには結果が重複して記載されてしまいます。

ACC で *Application View*（アプリケーションのビュー）を *By Sanctioned State*（許可済み状態別）に設定すると、仮想システムまたはデバイス グループ間で異なる許可済み状態を持つアプリケーションを視覚的に特定できます。緑は許可されたアプリケーション、青は不許可のアプリケーションを示します。黄色のアプリケーションは、異なる仮想システムまたはデバイス グループに異なる許可済み状態があることを示します。

レポートの設定を行う場合は、**Add**[追加] をクリックし、以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

SaaS アプリケーションの使用状況レポートの設定	の意味
氏名	レポートを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
期間	ドロップダウンリストからレポートの期間を選択します。**Last 7 Days**（過去 7 日）、**Last 30 Days**（過去 30 日）、または **Last 90 Days**（過去 90 日）を選択できます。レポートには、現在の日付（レポートが生成された日）のデータが含まれます。
次からログを含める	選択したユーザー グループ、選択したゾーン、あるいはファイアウォールまたは Panorama で設定されているすべてのユーザー グループおよびゾーンのうち、どれを対象としてレポートを生成するかをドロップダウン リストから選択します。 • **For a selected user group**（選択したユーザー グループ）– ファイアウォールまたは Panorama でどの **User Group**（ユーザー グループ）でログをフィルタリングするかを選択します。 • **For a selected zone**（選択したゾーン）– ファイアウォールまたは Panorama でどの **Zone**（ゾーン）でログをフィルタリングするかを選択します。 • **For all user groups and zones**（すべてのユーザー グループとゾーン）– すべてのグループを対象としてレポートを生成したり、表示するユーザー グループ（最大 25 個）を選択したりできます。25 を超えるグループがある場合、ファイアウォールまたは Panorama は上位 25 グループをレポートに表示し、残りのすべてのユーザー グループを Others（その他）グループに含めます。
レポートにユーザー グループ情報を含める （**Selected User Group**（選択したユーザー グループ）に対してレポートを生成するように選択している場合、このオプションを使用できません）	このオプションは、レポートに含めるユーザー グループでログをフィルタリングします。**manage groups**（グループを管理）リンクまたは**manage groups for the selected zone**（選択したゾーンのグループを管理）リンクを選択し、表示するユーザー グループ（最大 25個）を選択します。 選択したゾーンの特定のユーザーグループに関するレポートを生成した場合、選択したどのグループのメンバーでもないユーザーは、Others（その他）と呼ばれるユーザー グループに割り当てられます。
ユーザー グループ	どのユーザー グループを対象としてレポートを生成するかを選択します。このオプションは、**Include logs from**（次からログを含める）ドロップダウン リストで **Selected User Group**（選択したユーザー グループ）を選択した場合にのみ表示されます。
ゾーン	どのゾーンを対象としてレポートを生成するかを選択します。このオプションは、**Include logs from**（次からログを含める）ドロップダウン リストで **Selected Zone**（選択したゾーン）を選択した場合にのみ表示されます。 次に、Include user group information in the report（レポートにユーザー グループ情報を含める）を選択できます。
詳細なアプリケーション カテゴリ情報をレポートに含める	SaaSアプリケーションの使用状況レポートのPDFは2つのパートから構成されています。デフォルトでは両方のパートのレポートが生成されます。レポートの前半（10 ページ分）はレポート対象期間にネットワーク上で使用された SaaS アプリケーションに焦点を当てています。

© 2019 Palo Alto Networks, Inc.

SaaS アプリケーションの使用状況レポートの設定	の意味
	レポートの後半部分（レポート前半に記載された各アプリケーションサブカテゴリのSaaSおよび非SaaSアプリケーションに関する詳細な情報が含まれています）が不要な場合はこのオプションを未選択にしておいてください。レポートの後半部分には、各サブカテゴリの上位のアプリケーション名や、ユーザー、ユーザー グループ、ファイル、転送バイト数、およびこれらのアプリケーションが生み出した脅威に関する情報が含まれています。 詳細情報を含まない場合、レポートは 10 ページ分の長さとなっています。
レポートの最大サブカテゴリを次に制限	SaaS アプリケーション使用状況レポートですべてのアプリケーション サブカテゴリを使用するかどうか、またはサブカテゴリの最大数を 10、15、20、または 25 に制限するかどうかを選択します。 サブカテゴリの最大数を減らした場合、レポートに含める SaaS および SaaS 以外のアプリケーション アクティブティ情報が制限されるため、詳細レポートが短くなります。

必要なときに**Run Now**[今すぐ実行] をクリックしてレポートを生成します。

必要に応じてこのレポートを生成することも、毎日、毎週、または毎月の周期で実行するようにスケジュールすることもできます。レポートをスケジューリングするには、「schedule reports for email delivery（電子メール送信のスケジュール　レポート）」を参照してください。

PA-220 および PA-220R のファイアウォールでは、SaaS アプリケーション使用状況レポートは電子メールの PDF 添付ファイルとして送信されません。かわりに、電子メールにはリンクが記載されており、ウェブブラウザでレポートを開くことができます。

このレポートの詳細については、レポートの管理を参照してください。

Monitor > PDF Reports > Report Groups [監視 > PDF レポート > レポート グループ]

レポート グループを使用すると、レポートのセットを作成できます。システムはそのレポートのセットをまとめ、オプションのタイトル ページとすべての構成レポートが含まれる 1 つの集約された PDF レポートを送信することができます。

レポート グループの設定	の意味
氏名	レポート グループ名を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
タイトル ページ	レポートにタイトルページを追加するには、このオプションをオンにします。
役職	レポート タイトルとして表示される名前を入力します。
レポートの選択 / ウィジェット	グループに含める各レポートを左の列で選択し、右の列に **Add**（追加）します。以下のレポート タイプを選択できます。 • 事前定義済みレポート • カスタム レポート

© 2019 Palo Alto Networks, Inc.

レポート グループの設定	の意味
	• PDF サマリー レポート • CSV • Log View (ログ ビュー) – カスタム レポートを作成するたびに、ファイアウォールは同じ名前の Log View (ログ ビュー) レポートを自動的に作成します。Log View (ログ ビュー) には、カスタム レポートの内容を作成するためにファイアウォールが使用したログが表示されます。ログ ビュー データを含めるには、レポート グループを作成するときに **Custom Reports** (カスタム レポート) を追加し、一致する **Log View** (ログ ビュー) レポートを追加します。レポート グループに対して生成される集約レポートには、カスタム レポート データが表示され、その後にログ データが表示されます。 レポート グループを保存すると、Report Groups (レポート グループ) ページの Widgets (ウィジット) 列に、グループに追加したレポートのリストが表示されます。

レポート グループを使用するには、「Monitor (監視) > PDF Reports (PDF レポート) > Email Scheduler (電子メール スケジューラ)」を参照してください。

Monitor > PDF Reports > Email Scheduler [監視 > PDF レポート > 電子メール スケジューラ]

レポートの電子メール配信をスケジューリングするには、電子メール スケジューラを使用します。この設定を追加する前に、あらかじめレポート グループと電子メール プロファイルを定義しておく必要があります。「Monitor (監視) > PDF Reports (PDF レポート) > Report Groups (レポート グループ)」および「Device (デバイス) > Server Profiles (サーバー プロファイル) > Email (電子メール)」を参照してください。

スケジューリングされたレポートは午前 2 時にレポートの生成処理を開始し、スケジューリングされたすべてのレポートの生成が完了した後、電子メールが転送されます。

電子メール スケジューラ設定	の意味
氏名	スケジュールを識別する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
レポート グループ	スケジューリングするレポート グループ (Monitor (監視) > PDF Reports (PDF レポート) > Report Groups (レポート グループ)) または SaaS アプリケーション使用状況レポート (Monitor (監視) > PDF Reports (PDF レポート) > SaaS Application Usage (SaaS アプリケーション使用状況)) を選択します。
電子メール プロファイル	電子メール設定を定義するプロファイルを選択します。電子メール プロファイルの定義については、「Device (デバイス) > Server Profiles (サーバー プロファイル) > Email (電子メール)」を参照してください。
繰り返し	レポートを生成して送信する頻度 (毎日、毎週月・ 火・ 水・ 木・ 金・ 土・ 日曜日、無効) を選択します。

© 2019 Palo Alto Networks, Inc.

電子メール スケジューラ設定	の意味
電子メール アドレスのオーバーライド	電子メール プロファイルで指定したメール受信者の代わりに使用する別の電子メール アドレスを入力します。
テスト電子メールの送信	クリックすると、**Email Profile**（電子メール プロファイル）で定義した電子メール アドレスにテスト電子メールが送信されます。

© 2019 Palo Alto Networks, Inc.

Monitor > Manage Custom Reports [監視 > カスタム レポートの管理]

カスタム レポートを作成し、必要に応じてまたは定期的に（毎晩）実行できます。事前定義済みのレポートの場合は、**Monitor**（モニター）> **Reports**（レポート）を選択してください。

ファイアウォールがスケジュールされたカスタム レポートを生成した後で、設定を変更して将来の出力を変更すると、そのレポートの過去の結果が無効になる危険があります。スケジュール設定されたレポート設定を変更する必要がある場合は、新しいレポートを作成することをお勧めします。

カスタム レポートを **Add**（追加）して、新しいレポートを作成します。既存のテンプレートに基づいてレポートを作成するには、**Load Template**（テンプレートのロード）を行って、テンプレートを選択します。**Scheduled**（スケジュール設定）された時間ではなく、またはその時間に加えて、レポートを必要なときに生成するには、**Run Now**（今すぐ実行）をクリックします。以下の設定を指定して、レポートを定義します。

カスタム レポートの設定	の意味
氏名	レポートを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	カスタム レポートの説明を入力します。
データベース	レポートのデータ ソースとして使用するデータベースを選択します。
スケジュール設定	レポートを毎晩実行する場合は、このオプションをオンにします。その後、**Monitor**（監視）> **Reports**（レポート）を選択すると、レポートが利用可能になっています。
タイム フレーム	規定の時間枠を選択するか、**Custom**[カスタム] を選択して、日時の範囲を指定します。
ソート基準	ソート オプションを選択して、レポートに含める情報の量などを決定し、レポートの編成を行います。使用可能なオプションは、選択したデータベースによって異なります。
グループ化基準	グループ分けオプションを選択して、レポートに含める情報の量などを決定し、レポートの編成を行います。使用可能なオプションは、選択したデータベースによって異なります。
列	カスタムレポートで使用可能な列を選択し、選択した列に追加（⊞）します。**Up**（上へ）、**Down**（下へ）、**Top**（最上部）、**Bottom**（最下部）を使用して、選択された列の並び替えを行います。必要に応じて、選択済みの列を削除（⊖）することができます。
クエリ ビルダー	レポート クエリを作成するには、以下を指定して、**Add**[追加] をクリックします。クエリが完成するまで、繰り返します。

© 2019 Palo Alto Networks, Inc.

カスタム レポートの設定	の意味
	• **Connector**[条件式] — 追加する式の前に置く結合子（**and/or**）を選択します。 • **Negate**[除外] — クエリを否定（除外）として解釈させるには、このオプションをオンにします。前述の例で、否定のオプションを選択すると、過去 24 時間以内に受け取られていないエントリ、または「untrust」ゾーンから受け取られていないエントリに対する照合が行われます。 • **Attribute**[属性] — データ要素を選択します。使用可能なオプションは、選択したデータベースによって異なります。 • **Operator**[演算子] — 属性が適用されるかどうかを決定する基準を選択します (= など)。使用可能なオプションは、選択したデータベースによって異なります。 • **Value**[値] — 照合する属性値を指定します。

詳細は、「カスタム レポートの生成」を参照してください。

© 2019 Palo Alto Networks, Inc.

Monitor > Reports [監視 > レポート]

このファイアウォールでは、前日、または前の週の指定した日のトラフィック統計情報のさまざまな「上位 50」レポートを作成できます。

レポートを表示するには、ページの右側にあるレポート カテゴリ (Custom Reports (カスタム レポート) など) を展開し、レポート名を選択します。ページの各セクションにレポートが表示されます。各レポートに、選択した期間の情報を表示することができます。

デフォルトでは、ファイアウォールは前日分のすべてのレポートを表示します。他の日付のレポートを表示するには、ページの右下にあるカレンダーでレポートの生成日を選択します。

ファイアウォール以外のシステムでレポートを表示するには、エクスポート オプションを選択します。

- **PDF** にエクスポート
- **CSV** にエクスポート
- **XML** にエクスポート

レポートを生成

以下のトピックでは、ファイアウォール ポリシーのタイプ、ポリシーの移動またはコピー方法、ポリシー設定について説明します。

> ポリシーのタイプ
> ポリシールールの移動またはコピー
> 監査コメント アーカイブ
> ルールの使用状況ヒット数のクエリ
> Policies > Security [ポリシー > セキュリティ]
> Policies > NAT [ポリシー > NAT]
> Policies > QoS [ポリシー > QoS]
> Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーディング]
> Policies > Decryption [ポリシー > 復号化]
> Policies（ポリシー）> Tunnel Inspection（トンネル検査）
> Policies > Application Override [ポリシー > アプリケーション オーバーライド]
> Policies（ポリシー）> Authentication（認証）
> Policies > DoS Protection [ポリシー > DoS プロテクション]
> Policies > SD-WAN [ポリシー > SD-WAN]

ポリシーのタイプ

ポリシーを使用すると、ルールを適用してアクションを自動化し、ファイアウォールの動作を制御できます。ファイアウォールでは、以下のポリシーのタイプがサポートされています。

- 基本セキュリティ ポリシー - アプリケーション、ゾーンとアドレス（送信元と宛先）ごと、および任意でサービス（ポートとプロトコル）ごとにネットワーク セッションをブロックまたは許可します。ゾーンでは、トラフィックを送受信する物理または論理インターフェイスが識別されます。「Policies（ポリシー）> Security（セキュリティ）」を参照してください。
- ネットワーク アドレス変換（NAT）ポリシー - アドレスとポートを変換します。「Policies（ポリシー）> NAT」を参照してください。
- Quality of Services (QoS) ポリシー QoS が有効になっているインターフェイスを通過するトラフィックの処理を分類する方法を決定します。「Policies（ポリシー）> QoS」を参照してください。
- ポリシーベースの転送ポリシー - ルーティング テーブルをオーバーライドして、トラフィックの出力インターフェイスを指定します。「Policies（ポリシー）> Policy Based Forwarding（ポリシーベースの転送）」を参照してください。
- 復号化ポリシー - セキュリティ ポリシーのトラフィック復号化を指定します。ポリシーごとに、復号化するトラフィックの URL のカテゴリを指定できます。SSH 復号は、SSH シェル アクセス以外にも SSH トンネリングを識別して制御するためにも使用されます。「Policies（ポリシー）> Decryption（復号化）」を参照してください。
- トンネル検査ポリシー - トンネリングされたトラフィックにセキュリティ、DoS プロテクション、QoS ポリシーを適用したり、トンネル アクティビティを表示したりします。「Policies（ポリシー）> Tunnel Inspection（トンネル検査）」を参照してください。
- オーバーライド ポリシー - ファイアウォールのアプリケーション定義をオーバーライドします。「Policies（ポリシー）> Application Override（アプリケーション オーバーライド）」を参照してください。
- 認証ポリシー - ネットワーク リソースにアクセスするエンド ユーザーの認証を定義します。「Policies（ポリシー）> Authentication（認証）」を参照してください。
- サービス拒否 (DoS) ポリシー - DoS 攻撃から保護し、一致するルールに対応する保護アクションを実行します。「Policies（ポリシー）> DoS Protection（DoS プロテクション）」を参照してください。
- SD-WAN ポリシーは、リンク パスの正常性が承認され、コンフィグされた正常性メトリックより低下した場合に、送信元と宛先ゾーン間のリンク パス管理を決定します。「Policies (ポリシー) > SD-WAN」を参照してください。

Panorama™ からプッシュされた共有ポリシーは、ファイアウォール Web インターフェイスではオレンジ色で表示されます。これらの共有ポリシーは Panorama でのみ編集できます。ファイアウォールでは編集できません。

ルールベースをグループとして表示（ルールベースで使用されているすべてのタグ グループを表示するため）。多くのルールを持つルールベースではルールベースをグループとして表示し、作成済みのルール階層を維持したまま各グループのタグ、カラーコード、ルール数を表示することで、表示をシンプルにすることができます。

© 2019 Palo Alto Networks, Inc.

ポリシールールの移動またはコピー

ポリシーを移動またはコピーする際には、共有の場所を含め、自分がアクセス許可を与えられている **Destination (宛先)** (ファイアウォール上の仮想システム、またはPanorama上のデバイス グループ) を割り当てることができます。

ポリシー ルールを移動するには、**Policies** (ポリシー) タブでルールを選択し、**Move** (移動) をクリックして、**Move to other vsys** (他の **vsys** に移動) (ファイアウォールのみ) または**Move to different rulebase or device group (他のルールベースあるいはデバイスグループに移動)** (Panorama のみ) を選択し、以下の表の各フィールドを指定して **OK** をクリックします。

ポリシーをコピーする場合は、**Policies**[ポリシー] タブで**Clone**[コピー]をクリックして、以下の表の各フィールドを入力して**OK**をクリックします。

設定の移動/コピー	の意味
選択中のルール	操作対象として選択したポリシルールの名前と現在の場所 (仮想システムまたはデバイスグループ) が表示されます。
宛先	ポリシーまたはオブジェクトの新しい場所として、仮想システム、デバイス グループ、または共有を選択します。デフォルト値は、**Policies**[ポリシー] または **Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] または **Device Group**[デバイス グループ] です。
ルール順序	他のルールに対するルール相対位置を選択します。 • **Move top**[最上部へ] – 他のすべてのルールの前の位置を選択します。 • **Move bottom**[最下部へ] – 他のすべてのルールの後の位置を選択します。 • **Before rule**[事前ルール] – 隣接するドロップダウンリスト リストで直後のルールを選択します。 • **After rule**[事後ルール] – 隣接するドロップダウンリスト リストで直前のルールを選択します。
検証で最初に検出されたエラーに起因するエラーが発生しました	このオプションをオンにすると (デフォルトはオン)、ファイアウォールまたはPanoramaが、最初に検出したエラーを表示し、それ以上エラーをチェックしません。たとえば、移動するポリシー ルールで参照されているオブジェクトが [宛先] に存在しないと、エラーが発生します。このオプションをオフにした場合、ファイアウォールまたはPanoramaは、先に全てのエラーを検出してからそれらを表示します。

© 2019 Palo Alto Networks, Inc.

監査コメント アーカイブ

Audit Comment Archive (監査コメント アーカイブ)を選択し、選択済みのルールの監査コメントの履歴、設定ログ、ルールの変更履歴を表示します。

- 監査コメント
- 設定ログ（コミット間）
- ルール変更

監査コメント

選択したポリシールールの**Audit Comment** (監査コメント)を表示します。フィルターを適用して保存すれば、特定の監査コメントを素早く探し、表示された監査コメントを CSV 形式でエクスポートできます。

項目	の意味
コミット時間	監査コメントがコミットされた時間です。
監査コメント	監査コメントの内容です。
管理者	監査コメントを追加あるいは変更したユーザーです。
設定バージョン	設定のリビジョン番号です。0 は、ポリシールールが初めて作成されて Panorama にコミットされたことを示します。

設定ログ（コミット間）

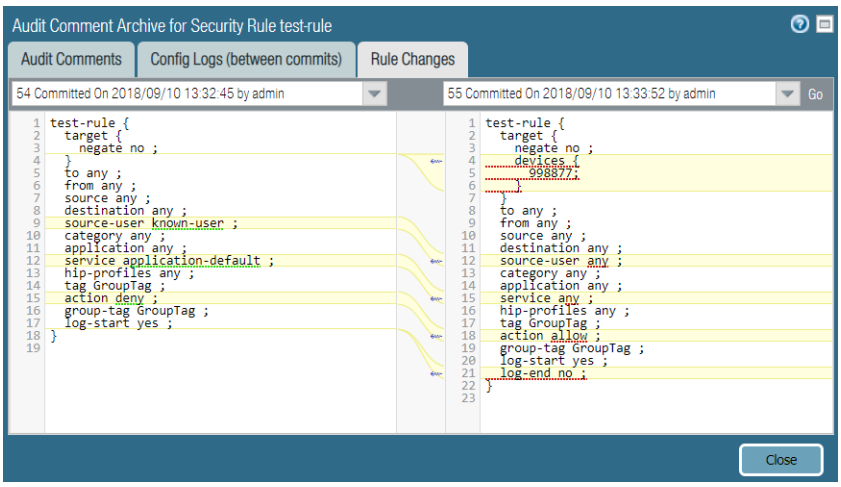
選択済みのポリシールールが各コミットの間に生成した設定ログを表示します。フィルターを適用して保存すれば、特定の設定ログを素早く探し、表示された設定ログを CSV 形式でエクスポートできます。

項目	の意味
時間	監査コメントがコミットされた時間です。
管理者	監査コメントの内容です。
コマンド	実行されたコマンドのタイプです。
変更前	変更が発生する前のルールの情報です。例：ルールの名前を変更した場合、以前の名前が表示されます。
変更後	変更が発生した後のルールの情報です。例：ルールの名前を変更した場合、新しい名前が表示されます。
デバイス名	監査コメントが変更される前のデバイスの名前です。

© 2019 Palo Alto Networks, Inc.

ルール変更

選択済みのポリシールールの構成バージョンを表示・比較し、どのような変更が発生したのか分析できます。比較したいポリシールールの 2 つの構成バージョンをドロップダウンリストで選択します。



© 2019 Palo Alto Networks, Inc.

ルールの使用状況ヒット数のクエリ

- レポートを生成 > ルールの使用状況

ルール使用状況のクエリを使用し、選択したルールベースを特定の期間でフィルタリングします。ルール使用状況のクエリを使用すれば、ポリシー ルールベースを素早くフィルタリングして使用していないルールを特定・削除できるため、攻撃の入り口を減らすことができます。**PDF/CSV**をクリックしてフィルタリングしたルールを PDF あるいは CSV 形式でエクスポートします。Rule Usage Hit Count Query (ルールの使用状況ヒット数のクエリ) を使用するには、**Policy Rule Hit Count** (ポリシールール ヒット数)設定（Device > Setup > Management [デバイス > セットアップ > 管理]）を有効化する必要があります。

デフォルト設定では、ポリシールールベース内のルールの使用状況をクエリする際に**Name** (名前)、**Location** (ロケーション)、**Created** (作成)、**Modified** (編集)、**Rule Usage** (ルールの使用状況)列が表示されます。列をさらに追加し、ポリシールールの詳細情報を確認できます。

タスク	の意味
ヒット数	
期間	選択したルールベースのクエリの対象期間を示します。事前定義済みの期間を選択するか、**Custom** (カスタム)期間を設定します。
使用方法	クエリを行うルールの使用状況を選択します：**Any** (すべて)、**Unused** (未使用)、**Used** (使用済み)、あるいは**Partially Used** (一部使用済み)（Panorama のみ）。
年	（カスタム期間のみ）ポリシー ルールベースのクエリの開始日時を選択します。
過去_日間のルールのリセットを除外	このオプションを使用すれば、特定の期間（日数）中にユーザーが手動でリセットしたルールが除外されます。

ルール ヒット数クエリのデバイス ルールの使用状況

Panorama 管理サーバーでポリシールールのルールの使用状況を閲覧する際、デバイスおよび仮想システムのルールの使用状況を確認できます。**Reset Rule Hit Counter** (ルール ヒット カウンターをリセット)して Hit Count (ヒット数)、First Hit (最初のヒット)、Last Hit (最後のヒット) をリセットします。

PDF/CSVをクリックしてフィルタリングしたルールを PDF あるいは CSV 形式でエクスポートします。

項目	の意味
デバイス グループ	デバイスあるいは仮想システムが属すデバイスグループです。
デバイス名/仮想システム	デバイスグループあるいは仮想システムの名前です。
ヒット数	ポリシールールにマッチしたトラフィックの総数です。
最後のヒット	ポリシールールにトラフィックが最後にマッチした日時です。

© 2019 Palo Alto Networks, Inc.

項目	の意味
最初のヒット	ポリシールールにトラフィックが最初にマッチした日時です。
最後の更新の受信	デバイスから Panorama 管理サーバーに最後にルールの使用状況を受信した時の日時です。
作成日時	ポリシールールが作成された日時です。
変更済	ポリシールールを最後に編集した日時です。ポリシールールが編集されていない場合は列が空になります。
状態	デバイスの接続ステータス：`Connected`（接続済み）あるいは`Disconnected`（切断）。

© 2019 Palo Alto Networks, Inc.

Policies > Security [ポリシー > セキュリティ]

セキュリティ ポリシー ルールは、セキュリティ ゾーンを参照して、アプリケーション、ユーザーまたはユーザー グループ、およびサービス (ポートおよびプロトコル) に基づいて、ネットワーク上のトラフィックを許可、制限、および追跡できるようにします。デフォルトでは、「*rule1*」という名前のセキュリティ ルールがファイアウォールに含まれています。このルールでは、Trust ゾーンから Untrust ゾーンへのトラフィックがすべて許可されています。

知りたい内容	以下を参照
セキュリティ ポリシーとは？	セキュリティポリシーの概要 Panorama については、「ポリシールールの移動またはコピー」を参照してください。
セキュリティ ポリシー ルールを作成する際に使用可能なフィールドは？	セキュリティ ポリシー ルールの構成要素
Web インターフェイスを使用してセキュリティ ポリシー ルールを管理するには？	ポリシーの作成と管理 セキュリティ ポリシー ルールのオーバーライドまたは取り消し アプリケーションおよび使用状況 セキュリティポリシー オプティマイザー
その他の情報をお探しですか？	Security Policy (セキュリティ ポリシー)

セキュリティポリシーの概要

セキュリティ ポリシーを使用すると、ルールを適用し、アクションを実行できます。また、必要に応じて、全般的または個別の指定を行うことができます。ポリシー ルールと受信トラフィックに対し順番に照合されます。トラフィックに一致する最初のルールが適用されるため、固有のルールを全般的ルールよりも先に設定する必要があります。たとえば、他のすべてのトラフィック関連の設定が同じである場合、1 つのアプリケーションに対応するルールがすべてのアプリケーションに対応するルールよりも上に来るようにしなければなりません。

ネットワーク リソースへのアクセス試行時にエンド ユーザーの認証を確実に行うために、ファイアウォールは認証ポリシーを評価してから、セキュリティ ポリシーを評価します。詳細は、「Policies (ポリシー) > Authentication (認証) 」を参照してください。

ユーザー定義のどのルールとも一致しないトラフィックには、デフォルト ルールが適用されます。セキュリティ ルールベースの下部に表示されるデフォルト ルールは、すべてのイントラゾーン (ゾーン内) トラフィックを許可し、すべてのインターゾーン (ゾーン間) トラフィックを拒否するよう事前定義されています。これらのルールは、事前定義済み設定に含まれ、デフォルトで読み取り専用ですが、**Override**[オーバーライド]して、タグ、アクション (許可または拒否)、ログ設定、セキュリティ プロファイルなど、限定された複数の設定を変更することができます。

インターフェイスには、セキュリティ ポリシー ルールを定義する以下のタブが含まれています。

- **General** (全般) — **General** (全般) タブを選択して、セキュリティ ポリシー ルールの名前と説明を設定します。

© 2019 Palo Alto Networks, Inc.

- **Source**[送信元] — **Source**[送信元]タブを選択して、トラフィックの送信元ゾーンまたは送信元アドレスを定義します。
- **User**[ユーザー] — **User**[ユーザー]タブを選択して、個々のユーザーまたはユーザーのグループのポリシーを適用します。ホスト情報プロファイル（HIP）が有効な GlobalProtect™ を使用している場合、GlobalProtect が収集した情報に基づいてポリシーを適用することもできます。たとえば、ユーザーのアクセス レベルを、ファイアウォールにユーザーのローカル設定を通知する HIP によって判別することができます。HIP 情報を使用して、ホストで実行中のセキュリティ プログラム、レジストリ値、およびホストにアンチウイルス ソフトウェアがインストールされているかどうかなど他の多くのチェックを基に、詳細なアクセス制御を行うことができます。
- **Destination**[宛先] — **Destination**[宛先]タブを使用して、トラフィックの宛先ゾーンまたは宛先アドレスを定義します。
- **Application**[アプリケーション] — **Application**[アプリケーション]タブを選択して、アプリケーションまたはアプリケーション グループに基づいて、ポリシーがアクションを実行するように指定します。管理者は、既存の App-ID™ シグネチャを使用し、カスタマイズして、独自のアプリケーションや、既存のアプリケーションの特定の属性を検出することもできます。カスタム アプリケーションは **Objects**（オブジェクト）> **Applications**（アプリケーション）で定義されます。
- **Service/URL Category**（サービス/**URL** カテゴリ） — **Service/URL Category**（サービス/**URL** カテゴリ）タブを選択して、TCP や UDP のポート番号または URL カテゴリをポリシーの一致条件として指定できます。
- **Action**[アクション] — **Action**[アクション]タブから、定義されたポリシー属性に一致するトラフィックに基づいて実行されるアクションを定義します。
- **Usage (**使用状況**)**—**Usage (**使用状況**)**タブを選択すれば、ルールで発見されたアプリケーションのかず、ルールで最後に新しいアプリケーションが発見された時、ヒット数データ、過去 30 日間のトラフィック、ルールが作成された時、最後に編集された時など、ルールの使用状況を確認できます。

セキュリティ ポリシー ルールの構成要素

- Policies > Security [ポリシー > セキュリティ]

以下のセクションでは、個々のセキュリティ ポリシー ルールの構成要素について説明します。セキュリティ ポリシー ルールを作成する際には、以下に示す各オプションを設定できます。

セキュリティ ルールの構成要素	設定場所	の意味
ルール番号	該当なし	ファイアウォールが自動的に各ルールに番号を振り、ルールが移動されると順序が変更されます。特定のフィルタに一致するようにルールをフィルタリングすると、各ルールはルールベース内の全ルールのコンテクストで番号が振られ、評価順に従って並べられます。 Panorama は独立してプレルールおよびポストルールに番号を振ります。Panorama が管理対象ファイアウォールにルールをプッシュすると、付番の際に、ルールベース内のプレルール、ファイアウォールルール、およびポストルールの階層が考慮され、その番号がルールの並びと評価順に反映されます。
氏名	一般条項	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
ルールの種類		ルールがゾーン内、ゾーン間、その両方のどれに適用されるかを指定します。 • **universal**[ユニバーサル] (デフォルト) – 指定された送信元ゾーンおよび宛先ゾーン内の一致するすべてのインターゾーン トラフィックとイントラゾーン トラフィックにルールを適用します。たとえば、送信元ゾーンが A と B で、宛先ゾーンが A と B のユニバーサル ルールを作成するとします。ルールは、ゾーン A 内のすべてのトラフィック、ゾーン B 内のすべてのトラフィック、ゾーン A からゾーン B へのすべてのトラフィック、ゾーン B からゾーン A へのすべてのトラフィックに適用されます。 • **intrazone**[イントラゾーン] – 指定された送信元ゾーン内の一致するすべてのトラフィックにルールを適用します (イントラゾーン ルールには宛先ゾーンを指定できません)。たとえば、送信元ゾーンを A と B に設定するとします。ルールは、ゾーン A 内のすべてのトラフィック、ゾーン B 内のすべてのトラフィックに適用されますが、ゾーン A とゾーン B 間のトラフィックには適用されません。 • **interzone**[インターゾーン] – 指定された送信元ゾーンおよび宛先ゾーン間の一致するすべてのトラフィックにルールを適用します。たとえば、送信元ゾーンを A、B、C、宛先ゾーンを A、B に設定したとします。ルールは、ゾーン A からゾーン B、ゾーン B から ゾーン A、ゾーン C からゾーン A、ゾーン C からゾーン B へのトラフィックには適用されますが、ゾーン A、B、または C 内のトラフィックには適用されません。
の意味		ポリシーの説明を入力します (最大1024 文字)。
tags		ポリシーのタグを指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のルールに「復号」や「復号なし」といった特定の語でタグを付けたり、特定のデータセンターに関するポリシーにその場所の名前を使用したりできます。 デフォルト ルールにタグを追加することもできます。
タグに基づいてルールをグループ化		デフォルト設定は **None** (なし) です。
監査コメント		
監査コメント アーカイブ		

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
設定ログ（コミット間）		
ルール変更		
送信元ゾーン	送信元	送信元ゾーンを **Add**（追加）します（デフォルトは **Any**（すべて））。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
送信元アドレス		送信元アドレス、アドレス グループ、または地域を **Add**（追加）します（デフォルトは **Any (すべて)**）。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**（アドレス）オブジェクト、**Address Group**（アドレスグループ）、または**Regions**（地域）を選択して設定を行います。Objects (オブジェクト)>Addresses (アドレス)およびObjects (オブジェクト)>AddressGroups (アドレスグループ)はそれぞれ、セキュリティポリシー ルールがサポートしているアドレス オブジェクトおよびアドレスグループのタイプを示します。 **Negate** (無効化)オプションを選択すると、指定したアドレスではなく、指定したゾーンからの送信元アドレスにルールが適用されます。
Source User（送信元ユーザー）	感染	このポリシーを適用する送信元ユーザーまたはユーザー グループを**Add**（追加）します： • **any** – ユーザー データに関係なく任意のトラフィックが含まれます。 • **pre-logon**[ログイン前] – GlobalProtect を使用してネットワークに接続しているが、自分のシステムにはログインしていないリモートユーザーが含まれます。GlobalProtect エンドポイントのポータルに Pre-logon（プレログオン）オプションが設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成でき、また、ユーザーが直接ログインしていなくても、そのマシンは完全にログインしているかのようにドメインで認証されます。 • **known-user**（既知のユーザー）– 認証されたすべてのユーザー（ユーザー データがマッピングされた IP アドレス）が含まれます。このオプションは、ドメインの「ドメイン ユーザー」グループに相当します。

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		• **unknown**[未知] – 認証されていないすべてのユーザー (ユーザーにマップされていない IP アドレス) が含まれます。たとえば、**unknown** (未知) はゲスト レベルのアクセスに使用できます。これらのユーザーは、ネットワーク上の IP アドレスを持っていますが、ドメインに認証されず、ファイアウォール上に IP アドレス対ユーザーのマッピング情報がないためです。 • **select**[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1 人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。
送信元 HIP プロファイル	感染	ホスト情報プロファイル (HIP) を**Add (追加)** すると、最新のセキュリティ パッチやアンチウイルス定義がインストールされているかなどエンド ホストのセキュリティ状態に関する情報を収集できます。ポリシーの適用にホスト情報を使用することで、重要なリソースにアクセスするリモート ホストが適切に整備された、セキュリティ標準に準拠した粒度の細かいセキュリティを実現でき、その後に、ネットワーク リソースへのアクセスを許可できます。以下の送信元 HIP プロファイルがサポートされます。 • **any** (任意) – HIP 情報に関係なく任意のエンドポイントが含まれます。 • **select** (選択) – 設定で選択した HIP プロファイルが含まれます。たとえば、1 つの HIP プロファイルや HIP プロファイルのリストを追加したり、手動で HIP プロファイルを追加できます。 • **no-hip** (**HIP** なし) – HIP 情報を必要としません。この設定により、HIP 情報を収集または送信できないサードパーティ クライアントからのアクセスが可能になります。
宛先ゾーン	宛先	宛先ゾーンを **Add** (追加) します (デフォルトは **any** (任意))。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、「Network (ネットワーク) > Zones (ゾーン)」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		イントラゾーン ルールは、送信元と宛先が同じゾーン内にあるトラフィックにのみ一致するため、宛先ゾーンを定義できません。イントラゾーン ルールに一致するゾーンを指定する場合、送信元ゾーンのみを設定する必要があります。
宛先アドレス		宛先アドレス、アドレス グループ、または地域を **Add**（追加）します（デフォルトは **Any** (すべて)）。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**（アドレス）オブジェクトをクリックし、**Address Group**（アドレスグループ）、または**Regions**（地域）を選択してアドレス設定を指定します。Objects (オブジェクト)>Addresses (アドレス)およびObjects (オブジェクト)>AddressGroups (アドレスグループ)はそれぞれ、セキュリティポリシー ルールがサポートしているアドレス オブジェクトおよびアドレスグループのタイプを示します。 **Negate** (無効化)オプションを選択すると、指定したアドレスではなく、指定したゾーン内の宛先アドレスにルールが適用されます。
Application [アプリケーション]	**Application** [アプリケーション]	セキュリティ ポリシー ルールについて、特定のアプリケーションを**Add** (追加)します。アプリケーションに複数の機能がある場合、アプリケーション全体または個別の機能を選択できます。アプリケーション全体を選択した場合、すべての機能が含まれ、将来、機能が追加されるとアプリケーション定義が自動的に更新されます。 セキュリティ ポリシー ルールでアプリケーション グループ、フィルタ、またはコンテナを使用している場合は、Application（アプリケーション）列のオブジェクトの上にマウスを置き、ドロップダウンリストを開いて **Value**（値）を選択すると、オブジェクトの詳細が表示されます。これにより、**Object**[オブジェクト]に移動しなくても、ポリシーからアプリケーションメンバーを直接表示することができます。 常に一つあるいは複数のアプリケーションを指定することで、ネットワーク上で許可したいアプリケーションだけを許可し、攻撃の入り口を減らしてネットワーク トラフィックをしっかり制御できるようにしてください。アプリケーションを*any* (すべて)に設定しないでください。そうするとすべてのアプリケーションのトラフィックが許可され、攻撃の入り口が増えてしまいます。
サービス	サービス/**URL** カテゴリ	特定の TCP または UDP のポート番号に制限したいサービスを選択します。ドロップダウンリスト リストから以下のいずれかを選択します。

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		• **any** - 選択したアプリケーションがすべてのプロトコルやポートで許可または拒否されます。 • **application-default**（アプリケーション-デフォルト）— 選択したアプリケーションが、**Palo Alto Networks®** によって定義されたデフォルトのポートでのみ許可または拒否されます。このオプションは、許可ポリシーに使用することをお勧めします。標準以外のポートやプロトコルで実行されるアプリケーションは、意図的である場合を除き、動作と使用方法が望ましくない可能性があります。このオプションを許可ポリシーに使用することで、そうしたアプリケーションの実行を禁止できます。 このオプションを使用しても、ファイアウォールはすべてのポートのすべてのアプリケーションをチェックしますが、アプリケーションはデフォルトのポート/プロトコルでのみ許可されます。 大抵のアプリケーションの場合は*application-default*を使用し、アプリケーションが標準的でないポートを使用したり、他の悪意のある挙動を生じさせたりしないようにします。アプリケーションのデフォルトのポートが変わると、ファイアウォールが自動的にルールを更新してデフォルトのポートを修正します。内部のカスタム アプリケーションのように標準的でないポートを使用するアプリケーションについては、アプリケーションを修正するか、標準的でないポートを指定するルールを作成し、対象のアプリケーションを必要とするトラフィックにのみルールを適用します。 • **Select**（選択）— 既存のサービスを**Add**（追加）するか、**Service**（サービス）または**Service Group**（サービス グループ）を選択して新しいエントリを指定します。（または Objects（オブジェクト）> Services（サービス）および Objects（オブジェクト）> Service Groups（サービス グループ）を選択します）。
URL カテゴリ		セキュリティ ルールを適用する URL カテゴリを選択します。 • URL カテゴリに関係なくすべてのセッションを許可または拒否するには、**any** を選択します。 • カテゴリを指定するには、ドロップダウンリスト リストから特定のカテゴリ (カスタム カテゴリを含む)を **Add**（追加）します。Objects（オブジェクト）> External Dynamic Lists（外部動的リスト）を選択して、カスタム カテゴリを定義します。
アクション設定	操作	ルールで定義されている属性にマッチするトラフィックに対してファイアウォールが適用する**Action** (アクション)を選択します：

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		• **Allow**（許可）– (デフォルト) 一致するトラフィックを許可します。 • **Deny**（拒否）– 一致するトラフィックをブロックし、拒否されるアプリケーションについて定義されたデフォルトのアクションの拒否を実行します。アプリケーションについてデフォルトで定義されている拒否アクションを表示するには、（**Objects**（オブジェクト）> **Applications**（アプリケーション））でアプリケーションの詳細情報を表示します。 デフォルトの拒否アクションはアプリケーションによって異なるため、ファイアウォールは、あるアプリケーションについては、セッションをブロックしてリセットを送信し、別のアプリケーションについてはセッションを暗黙にドロップするといったアクションを実行します。 • **Drop**[ドロップ] – アプリケーションをサイレントにドロップします。TCP リセットはホストまたはアプリケーションに送信されません。ただし、**Send ICMP Unreachable**（**ICMP** 送信到達不能）を選択した場合を除きます。 • **Reset client**[クライアントのリセット] – クライアント側デバイスに TCP リセットを送信します。 • **Reset server**[サーバーのリセット] – サーバー側デバイスに TCP リセットを送信します。 • **Reset both**[両方のリセット] – クライアント側とサーバー側の両方のデバイスに TCP リセットを送信します。 • **Send ICMP Unreachable**（**ICMP** 送信到達不能）– レイヤー 3 インターフェイスでのみ使用できます。トラフィックのドロップや接続のリセットを行うようにセキュリティ ポリシー ルールを設定すると、トラフィックが宛先ホストに到達しない場合があります。そのような場合は、ドロップされるすべての UDP トラフィックおよび TCP トラフィックについて、トラフィックの送信元 IP アドレスに ICMP 到達不能応答を送信するようにファイアウォールを設定できます。この設定を有効にすると、送信元は正規の手順に従ってセッションをクローズまたはクリアできるため、アプリケーションの処理が中断するのを防ぐことができます。 ファイアウォールに設定されている ICMP 到達不能パケット率を確認するには、（**Device**（デバイス）> **Setup**（セットアップ）> **Session**（セッション））の Session Settings（セッション設定）を表示します。 事前定義済みのインターゾーンおよびイントラゾーン ルールに定義されているデフォルト アクションをオーバーライドする方法については、「セキュリティルールのオーバーライドまたは取り消し」を参照してください。
プロファイル設定	操作	セキュリティ プロファイル ルールと一致するパケットに対してファイアウォールが実行する追加チェックを指定するには、Antivirus（アンチウイルス）、Anti-Spyware（ア

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		ンチスパイウェア）、Vulnerability Protection（脆弱性防御）、URL Filtering（URL フィルタリング）、File Blocking（ファイル ブロッキング）、Data Filtering（データ フィルタリング）、WildFire Analysis（WildFire 分析）、GTP Protection（GTP プロテクション）、および SCTP Protection（SCTP プロテクション）の各プロファイルを選択します。 個々のプロファイルではなくプロファイル グループを指定するには、**Profile Type Group**（プロファイル タイプ グループ）を選択し、**Group Profile**（グループ プロファイル）を選択します。 新しいプロファイルやプロファイル グループを定義するには、該当するプロファイルまたはグループの横にある **New**（新規）をクリックします（「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション）」を参照）。 Security Profiles（セキュリティ プロファイル）（またはプロファイル グループ）をデフォルト ルールに関連付けることもできます。
ログ設定およびその他の設定	操作	ルールに一致するトラフィックのエントリをローカル トラフィック ログに生成するには、以下のオプションを選択します。 • **Log At Session Start**（セッション開始時にログ）（デフォルトではオフ）– セッション開始のトラフィック ログ エントリを生成します。 *ACC でアクティブな GRE トンネルを表示するトンネル セッションやトラブルシューティングが目的でない限り、Log at Session Start (セッション開始時にログ)を有効化しないでください。例えば facebook-base から facebook-chat へ数パケットが生じた後にアプリケーションが変更する場合、セッション終了時のロギングはあまりリソースを消費せずにアプリケーションを正確に識別します。* • **Log At Session End**（セッション終了時にログ）（デフォルトではオン）– セッション開始のトラフィック ログ エントリを生成します。 セッションの開始または終了のエントリがログに記録される場合、*drop []*ドロップおよび *deny [拒否]*のエントリもログに記録されます。 • **Log Forwarding Profile**（ログ転送プロファイル）– ローカル トラフィック ログと脅威ログのエントリをリモートの宛先 (Panorama サーバーや Syslog サーバーなど) に転送す

© 2019 Palo Alto Networks, Inc.

セキュリティ ルールの構成要素	設定場所	の意味
		るには、ドロップダウンリスト リストから **Log Forwarding Profile**（ログ転送プロファイル）を選択します。 脅威ログ エントリの生成は、*Security Profiles*（セキュリティ プロファイル）で定義されます。必要に応じて、*New*（新規）ログ プロファイルを定義します（「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照）。 ログ転送プロファイルを作成・有効化し、専用の外部ストレージデバイスにログを送信します。ファイアウォールのログの保存領域には限界があり、容量が一杯になるとファイアウォールは最も古いログをパージするため、これによってログを保持できます。 デフォルト ルールのログ設定を変更することもできます。以下のオプションを任意に組み合わせて指定します。 • **Schedule**（スケジュール）– ルールを適用する日時を制限するには、ドロップダウン リストからスケジュールを選択します。必要に応じて、**New**（新規）スケジュールを定義します（「復号化された SSL トラフィックを制御するための設定」を参照）。 • **QoS Marking**（**QoS**マーキング）– ルールに一致するパケットの Quality of Services（QoS）の設定を変更するには、**IP DSCP** または **IP Precedence**（**IP**優先度）を選択して、QoS の値を 2 進数形式で入力するか、事前に定義されている値をドロップダウン リストから選択します。QoS の詳細は、「サービス品質」を参照してください。 • **Disable Server Response Inspection**（サーバー レスポンス検査の無効化）–サーバーからクライアントに送信されるパケットの検査を無効にします。このオプションはデフォルトで無効になっています。 セキュリティ状況を最良にするために、*Disable Server Response Inspection*サーバー レスポンス検査の無効化）を有効にしないでください。このオプションを選択すると、ファイアウォールはクライアントからサーバーへのフローのみ検査します。サーバーからクライアントへのフローは検査されないため、トラフィック フローで脅威が存在する場合に一方のフローで特定できなくなります。
基本	ルールの使用状況	• **Rule Created** (ルールの作成時–ルールを作成した日時です。 • **Last Edited** (最終変更)–ルールが最後に編集された日次です。

© 2019 Palo Alto Networks, Inc.

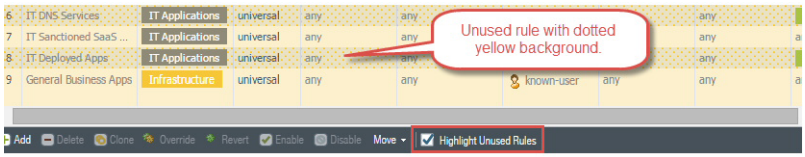
セキュリティ ルールの構成要素	設定場所	の意味
アクティビティ	ルールの使用状況	• **Hit Count** (ヒット数)–トラフィックがルールにマッチ（ヒット）した回数の合計です。 • **First Hit** (最初のヒット)–初めてルールがマッチした時です。 • **Last Hit** (最後のヒット)–最後にルールがマッチした時です。
アプリケーション [applications]	ルールの使用状況	• **Applications Seen** (発見されたアプリケーション)–ルールが許可するアプリケーションの数です。 • **Last App Seen** (最後に発見されたアプリケーション)–ルールで最後の新しいアプリケーション（以前に発見されたことがないアプリケーション）が発見された時から経過した日数です。 • **Compare Applications & Applications Seen** (アプリケーションおよび発見されたアプリケーションを比較)–クリックすると、ルールで設定されているアプリケーションとルールで発見されたアプリケーションを比較できます。このツールを使用すれば、ルールにマッチするアプリケーションを探し、それらをルールに追加することができます。
トラフィック（過去 30 日間）	ルールの使用状況	• **Bytes** (バイト数)–過去 30 日間のルールのトラフィック量（バイト）です。 最も古いルールはトラフィックの累積量が最も多くなりがちであるため、期間を *30* 日より長くするとそのルールがリストの一番上に残り続けるでしょう。そのため、新しいルールに大量のトラフィックがあっても、古いルールの下にリストアップされる可能性があります。

ポリシーの作成と管理

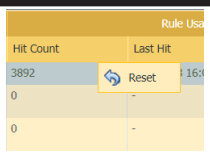
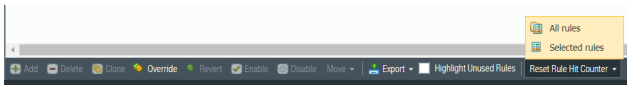
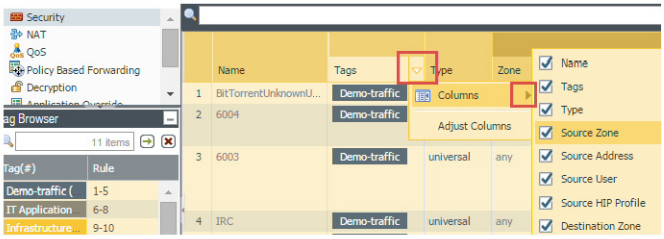
Policies（ポリシー）> **Security**（セキュリティ）ページでは、セキュリティ ポリシーの追加、変更、および管理が可能です。

タスク	の意味
コンテキストの	新しいポリシールールを**Add** (追加)するか、新しいルールのベースとなるルールを選択して**Clone Rule** (ルールをコピー)します。コピーされたルール「rule*n*」が選択したルールの下に挿入されます。*n* は次に使用可能な整数で、これによりルール名が一意になります。コピーの詳細は、「ポリシールールの移動またはコピー」を参照してください。
変更	設定を変更するルールを選択します。 Panorama からプッシュされたルールは、ファイアウォールでは読み取り専用となるため、ローカルでは編集できません。

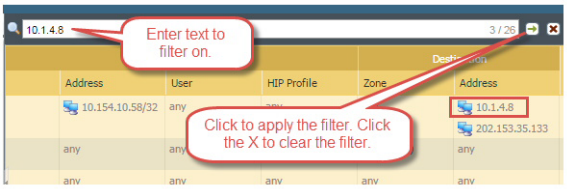
© 2019 Palo Alto Networks, Inc.

タスク	の意味
	Override（オーバーライド）および**Revert**（元に戻す）アクションは、セキュリティ ルールベースの最下部に表示されるデフォルト ルールにのみ適用されます。事前定義ルール、すなわち、すべてのイントラゾーン トラフィックを許可し、すべてのインターゾーン トラフィックを拒否するルールは、ファイアウォールに、ルールベース内の他のどのルールとも一致しないトラフィックの処理方法を指示するものです。これらのルールは事前定義済み設定に含まれるため、**Override** (オーバーライド)して一部のポリシー設定を編集する必要があります。Panorama を使用している場合、デフォルト ルールを **Override**（オーバーライド）して、Device Groups（デバイス グループ）コンテキストまたはShared（共有）コンテキストでファイアウォールにプッシュすることもできます。デフォルト ルールを元に戻すこともできます。これにより、事前定義済み設定や Panorama からプッシュされた設定が復元されます。詳細は「セキュリティ ルールのオーバーライドまたは取り消し」を参照してください。
移動	ルールは、**Policies**（ポリシー）ページに列挙されている順序で、上から下に評価されます。ネットワーク トラフィックに対してルールを評価する順序を変更するには、ルールを選択して、**Move Up** (上へ移動)、**Move Down** (下へ移動)、 **Move Top** (最上部へ移動)、**Move Bottom** (最下部へ移動)、または**Move to a different rulebase or device group** (別のルールベースあるいはデバイスグループに移動)します。詳細は、「ポリシー ルールの移動またはコピー」を参照してください。
UUID のコピー	ルールの UUID をクリップボードにコピーし、設定やログを検索する際に使用できるようにします。
削除します。	既存のルールを選択して**Delete** (削除)します。
有効化/無効化	ルールを無効にするには、選択して **Disable**（無効）にします。無効になっているルールを有効にするには、選択して **Enable**（有効）にします。
ルールの使用状況のモニター	ファイアウォールを前回再起動して以来使用されていないルールを特定したい場合は **Highlight Unused Rules**（未使用のルールをハイライト表示）します。その上で、ルールを**Disable** (無効)にするのか、**Delete** (削除)するのかを判断します。現在使用されていないルールは黄色い網掛けで表示されます。ポリシー ルール ヒット カウントが有効である場合は、Hit Count（ヒット数）データはルールが使用されていないかどうかを判断するために使われます。 各ファイアウォールは、一致のあるルールのトラフィック フラグが維持管理されます。再起動時にデータ プレーンのリセットが発生するとフラグがリセットされるため、このリストを定期的にモニターして、最後のチェック以降にルールに一致があったかどうかを判別してからリストを削除または無効にすることがベストプラクティスになります。 
Reset Rule Hit Counter（ルール ヒット カウ	**Hit Count**（ヒット数）はポリシー ルールの総トラフィック ヒットを追跡します。総トラフィック ヒット数は再起動、アップグレード、データプレーンの再起動後も存続します。特定のルールのヒット カウントをリセットするには、ドロップダウンを展開し、カウントを **Reset**（リセット）します。

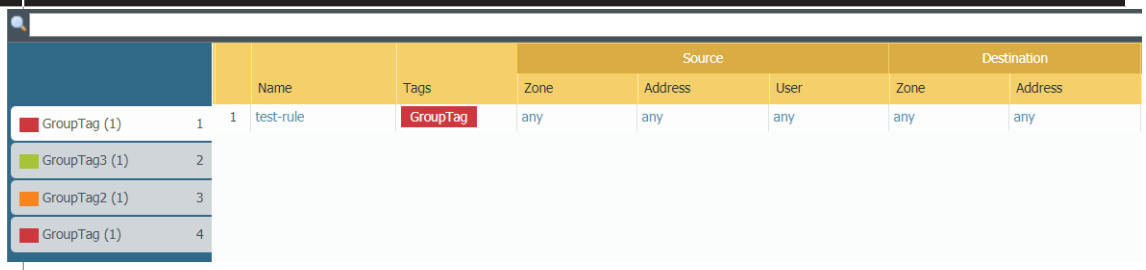
© 2019 Palo Alto Networks, Inc.

タスク	の意味
ンターのリセット）	 あるいは、**Reset Rule Hit Counter** (ルールのヒット カウンターをリセット) (最下部のメニュー) します。ヒット数統計を消去するには、**All Rules** （すべてのルール）を選択するか、指定のルールを選択して **Selected rules** （選択したルール）のヒット数統計のみをリセットします。  最初にヒットしたセキュリティ ポリシーの日付を確認するには、**First Hit** (最初のヒット) を表示します。日付は hh:mm:ss year (時間：分：秒、西暦) の形式で表示されます。この値はリセットできません。 最後にヒットしたセキュリティ ポリシーの日付を確認するには、**Last Hit** (最後のヒット) を表示します。日付は hh:mm:ss year (時間：分：秒、西暦) の形式で表示されます。この値はリセットできません。
列の表示/非表示	**Policies** (ポリシー)のところに表示される各列の表示/非表示を切り替えます。列名を選択すれば表示を切り替えられます。 
フィルタの適用	リストにフィルタを適用するには、**Filter Rules**[フィルタ ルール] ドロップダウンリスト リストから選択します。フィルタを定義するには、項目のドロップダウンリストで**Filter** (フィルタ)を選択します。 デフォルトルールはルールベースフィルタリングの対象外であるため、常にフィルタリング後のルールリストに表示されます。 ポリシーに一致するものとしてログに記録されたネットワーク セッションを表示するには、ルール名のドロップダウンリスト リストで**Log Viewer** (ログ ビューワ)を選択します。 現在の値を表示するには、項目のドロップダウンリストで**Value** (値)を選択します。列メニューから項目を直接編集、フィルタリング、または削除することもできます。たとえば、あるアドレス グループに含まれるアドレスを表示するには、**Address** (アドレス)列内のオブジェクトにカーソルを合わせ、ドロップダウンリストで**Value** (値)を選択します。これにより、**Object**[オブジェクト]タブに移動しなくても、アドレス グループのメンバーおよび対応する IP アドレスを迅速に確認できます。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	オブジェクト名またはIPアドレスをもとに、ポリシー内で使用されているオブジェクトを検索する場合はフィルターを使用します。フィルターの適用後はフィルターに一致した項目のみが表示されます。フィルターは埋め込みオブジェクトに対しても有効です。たとえば、10.1.4.8 でフィルタリングした場合、そのアドレスを含むポリシーのみが表示されます。 
ルールのプレビュー（Panoramaのみ）	**Preview Rules**（ルールのプレビュー）から、ルールを管理対象ファイアウォールにプッシュする前にルールのリストを表示することができます。大量のルールに目を通しやすいように、各ルールベース内でルールの階層がデバイスグループ（および管理対象ファイアウォール）ごとに視覚的に区別されて表示されます。
設定タイトルのエクスポート	最低限の読み取り専用アクセス権を持つ管理ロールは、ポリシー ルールベースを **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などの必要性に応じて具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export（設定バンドルのエクスポート）」を参照してください。
使用されていないルールの強調表示	トラフィックにマッチしないポリシールールを**Rule Usage** (ルールの使用状況)列でハイライト表示します。
グループ	**View Rulebase as Groups** (ルールベースをグループで表示)のボックスにチェックを入れている場合にタグ グループを管理します。次の操作を行えます： • **Move rules in group to different rulebase or device group** (グループ内の結果を別のルールベースあるいはデバイスグループに移動)—選択したタグ グループを別のデバイスグループに移動させます。 • **Change group of all rules** (すべてのルールのグループを変更)—選択したタグ グループ内のルールをルールベース内の別のタグ グループに移動させます。 • **Delete all rules in group** (グループ内のすべてのルールを削除)—選択したタググループ内のすべてのルールを削除します。 • **Clone all rules in group** (グループ内のすべてのルールをコピー)—選択したタググループ内のルールを別のデバイスグループにコピーします。
ルールベースをグループとして表示	**View Rulebase as Groups** (ルールベースをグループとして表示)すれば、**Group Rules by Tag** (タグに基づいてルールをグループ化)で使用しているタグを使ってポリシー ルールベースを表示できます。選択したタグ グループに属すポリシールールが表示されます。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	
ポリシーマッチのテスト	選択したポリシー ルールベースの保護ポリシーのテストを行い、正しいトラフィックが拒否・許可されることを検証します。

セキュリティ ポリシー ルールのオーバーライドまたは取り消し

デフォルトのセキュリティルールである interzone-default と intrazone-default には事前定義済みの設定がありますが、これは、ファイアウォールまたはPanorama上でオーバーライドできます。ファイアウォールがデバイス グループからデフォルト ルールを受信する場合は、デバイス グループ設定もオーバーライドできます。オーバーライドが実行されるファイアウォールまたは仮想システムには、ローカルバージョンのルールが設定情報の中に格納されています。オーバーライド可能な設定は、フルセットの一部です (以下の表にセキュリティ ルールの一部を示します)。デフォルト セキュリティ ルールの詳細は、「Policies（ポリシー）> Security（セキュリティ）」を参照してください。

ルールをオーバーライドするには、ファイアウォールでは **Policies**（ポリシー）> **Security**（セキュリティ）を、Panorama では **Policies**（ポリシー）> **Security**（セキュリティ）> **Default Rules**（デフォルト ルール）を選択します。名前列には、オーバーライド可能なルールの継承アイコン（ ）が表示されます。ルールを選択し、**Override**[オーバーライド] をクリックして、以下の表に示した各設定を編集します。

オーバーライドしたルールを事前定義の設定または Panorama デバイス グループからプッシュされた設定に戻すには、ファイアウォールでは **Policies**（ポリシー）> **Security**（セキュリティ）を、Panorama では **Policies**（ポリシー）> **Security**（セキュリティ）> **Default Rules**（デフォルト ルール）を選択します。

名前列には、オーバーライドされた値を持つルールのオーバーライド アイコン（ ）が表示されます。ルールを選択して、**Revert**[元に戻す] をクリックし、**Yes**[はい] をクリックして操作を確定します。

デフォルト セキュリティ ルールをオーバーライドするフィールド	の意味
General [全般] タブ	
氏名	ルールを識別する **Name**[名前] は読み取り専用であるため、オーバーライドはできません。
ルールの種類	**Rule Type**[ルール タイプ] は読み取り専用であるため、オーバーライドはできません。
の意味	**Description**[説明] は読み取り専用であるため、オーバーライドはできません。
タグ	ドロップダウンリストから**Tags**[タグ]を選択します。

© 2019 Palo Alto Networks, Inc.

デフォルト セキュリティ ルールをオーバーライドするフィールド	の意味
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーにDMZへのインバウンドのタグを付けたり、個々の復号化ポリシーに「復号」または「復号なし」というタグを付けたり、特定のデータセンターに関連付けられたポリシーにその場所の名前を使用したりできます。
Actions [アクション] タブ	
アクション設定	ルールに一致するトラフィックに対して適切な **Action**（アクション）を選択します。 • **Allow**[許可] – (デフォルト) トラフィックを許可します。 • **Deny**[拒否] – トラフィックをブロックし、ファイアウォールが拒否するアプリケーションについて定義されたデフォルトのアクションの拒否を実行します。アプリケーションについてデフォルトで定義されている拒否のアクションを表示するには、**Objects**（オブジェクト）> **Applications**（アプリケーション）でアプリケーションの詳細情報を表示します。 • **Drop**[ドロップ] – アプリケーションをサイレントにドロップします。ホストまたはアプリケーションに、TCP リセット メッセージは送信されません。 • **Reset client**[クライアントのリセット] – クライアント側デバイスに TCP リセット メッセージを送信します。 • **Reset server**[サーバーのリセット] – サーバー側デバイスに TCP リセット メッセージを送信します。 • **Reset both**[両方のリセット] – クライアント側とサーバー側の両方のデバイスに TCP リセット メッセージを送信します。
プロファイル設定	**Profile Type**（プロファイル タイプ） – プロファイルまたはプラットフォーム グループをセキュリティ ルールに割り当てます。 • デフォルトのセキュリティプロファイルによって実行されるチェック動作を指定するには、**Profiles**[プロファイル]を選択して、**Antivirus**[アンチウイルス]、**Vulnerability Protection**[脆弱性防御]、**Anti-Spyware**[アンチスパイウェア]、**URL Filtering**[URLフィルタリング]、**File Blocking**[ファイルブロッキング]、**Data Filtering**[データフィルタリング]、**WildFire Analysis**[WildFire分析]の各プロファイルを選択します。 • 個々のプロファイルではなくプロファイルグループを割り当てるには、**Group**[グループ]を選択し、ドロップダウンリスト リストから **Group Profile**[グループプロファイル]を選択します。 • 新規のプロファイル（Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル））またはプロファイル グループ（Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション））を定義するには、対応するプロファイルまたはグループのドロップダウン リストで **New**（新規）をクリックします。
ログ設定	以下のオプションを任意に組み合わせて指定します。

© 2019 Palo Alto Networks, Inc.

デフォルト セキュリティ ルールをオーバーライドするフィールド	の意味

	• **Log Forwarding**[ログ転送] – ローカル トラフィック ログと脅威ログのエントリをリモートの宛先 (Panorama サーバーや Syslog サーバーなど) に転送するには、ドロップダウンリスト リストから **Log Forwarding**[ログ転送] プロファイルを選択します。セキュリティ プロファイルによって、脅威ログ エントリが生成されるかどうかが決まります。新規の **Log Forwarding** (ログ転送) プロファイルを定義するには、ドロップダウン リストで **Profile** (プロファイル) を選択します (「Objects (オブジェクト) > Log Forwarding (ログ転送) 」を参照)。
	• ルールに一致するトラフィックのエントリをローカル トラフィック ログに生成するには、以下のオプションを選択します。
	  • **Log at Session Start** (セッション開始時にログ) – セッション開始のトラフィック ログ エントリを生成します (デフォルトではオン)。
	  • **Log at Session End** (セッション終了時にログ) – セッション終了のトラフィック ログ エントリを生成します (デフォルトではオフ)。
	  セッション開始またはセッション終了エントリをトラフィック ログに含めるようにファイアウォールを設定した場合は、ドロップ エントリと拒否エントリもトラフィック ログに含められます。

アプリケーションおよび使用状況

- Policies (ポリシー) > Security (セキュリティ) > Policy Optimizer (ポリシー オプティマイザー) > No App Specified (アプリが指定されていません) > Compare (比較) (または、**Apps Seen**(発見されたアプリ)の数字をクリックします)
- Policies (ポリシー) > Security (セキュリティ) > Policy Optimizer (ポリシー オプティマイザー) > Unused Apps (使用していないアプリ) > Compare (比較) (または、**Apps Seen**(発見されたアプリ)の数字をクリックします)
- Policies (ポリシー) > Security (セキュリティ)、**Apps Seen**(発見されたアプリ)の数字をクリックします

また、セキュリティ ポリシー ルールの Usage (使用状況) タブで**Compare Applications & Applications Seen** (アプリケーションおよび発見されたアプリケーションの比較)を行えば、ポート ベースのセキュリティ ポリシー ルールからアプリケーション ベースのセキュリティ ポリシー ルールに移行する際に役立つツールを利用でき、**Applications & Usage** (アプリケーションおよび使用状況)でルールから使用していないアプリケーションを取り除くことができます。

項目	の意味
期間	アプリケーション情報の期間： • **Anytime** (全期間)–ルールを作成してから発見されたアプリケーションを表示します。 • **Past 7 days** (過去 7 日間)–過去 7 日間に発見されたアプリケーションだけを表示します。 • **Past 15 days** (過去 7 日間)–過去15 日間に発見されたアプリケーションだけを表示します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **Past30 days** (過去 **7** 日間)–過去30 日間に発見されたアプリケーションだけを表示します。
ルールのアプリ	対象のルールで設定されている各アプリケーション、あるいはルールで特定のアプリケーションが設定されていない場合は**Any** (すべて)になります。必要に応じてアプリケーションを**Browse** (参照)、**Add** (追加)、**Delete** (削除)でき、そうするとアプリケーションがルールで設定され、Apps on Rule (ルールのアプリ) の隣にある丸で囲まれた数字で数が分かります。この場所でアプリケーションを追加する方法は、セキュリティポリシー ルールの**Application** (アプリケーション)タブでアプリケーションを追加する際と同じです。
発見されたアプリ	ルールにマッチするファイアウォール上で許可され、発見されたすべてのアプリケーションです。Apps Seen (発見されたアプリ) の隣にある丸で囲まれた数字は、対象のルールで発見されたアプリケーションの数を示します。 • **Applications** (アプリケーション)–対象のルールで発見されたアプリケーションです。例えば、ルールが web-browsing トラフィックを許可する場合 (ルールのアプリ) 、web-browsing アプリケーションが多く存在するため、リストに多くのアプリケーションが表示される可能性があります。 • **Subcategory** (サブカテゴリ)–アプリケーションのサブカテゴリです。 • **Risk** (リスク)–アプリケーションのリスク評価です。 • **First Seen** (最初の発見)–ネットワーク上でアプリケーションが初めて発見された日です。 • **First Seen** (最後の発見)–ネットワーク上でアプリケーションが最後に発見された日です。 *First Seen (最初の発見) と Last Seen (最後の発見) の精度は 1 日であるため、ルールを定義した日は First Seen (最初の発見) と Last Seen (最後の発見) が同じ日付になります。* • **Traffic (30 days)** (トラフィック (**30** 日))–過去 30 日間で発見されたトラフィックの量 (バイト) です。 最も古いルールはトラフィックの累積量が最も多くなりがちであるため、期間を長くするとそのルールがリストの一番上に残り続けるでしょう。そのため、新しいルールに大量のトラフィックがあっても、古いルールの下にリストアップされる可能性があります。
発見されたアプリの操作	**Apps Seen** (発見されたアプリ)で行える操作 : • **Create Cloned Rule** (ルールのコピーを作成)–現在のルールをコピーします。ポートベースのルールからアプリケーション ベースのルールに移行する際、初めにポートベースのルールをコピーしてからそのコピーを編集することで、アプリケーション ベースのホワイトリスト ルールを作成します。ポリシーリストでは、コピーしたルールがポートベースのルールの上に挿入されます。必ずこの方法で移行を行い、許可したいトラフィックを誤っ

© 2019 Palo Alto Networks, Inc.

項目	の意味
	て拒否することがないようにしてください。コピーしたルールが必要なアプリケーションを一部許可しない場合、後続のポートベースのルールによってそれらが許可されます。ポートベースのルールを監視して必要に応じて（コピーした）アプリケーションベースのルールを調整します。必要なトラフィックだけをアプリケーション ベースのルールが許可しており、不要なトラフィックだけがフィルタリングされてポートベースのルールの対象になっていることが確実であれば、対象のポートベースのルールを安全に削除できます。 • **Add to This Rule**(ルールに追加)—Apps Seen (発見されたアプリ) のアプリケーションをルールに追加します。アプリケーションをルールに追加すると、**Any** (すべて)のアプリケーションにマッチするように設定されたルール（アプリケーション ベースのルール）が、指定したアプリケーションをホワイトリストに登録するアプリケーション ベースのルールに変わります（新しいアプリケーション ベースのルールがポートベースのルールに取って代わります）。他のすべてのアプリケーション ベースのホワイトリスト ルールと同じように、ルールに追加しないアプリケーションはすべて拒否されます。必ず、許可するアプリケーションをすべて判断し、それらをルールに追加することで、アプリケーションを誤って拒否することがないようにしてください。 • **Add to Existing Rule** (既存のルールに追加)—Apps Seen (発見されたアプリ) から既存のアプリケーションベース (App-ID) のルールにアプリケーションを追加します。これにより、ポートベースのルールから App-ID ベースのルールをコピーし、ポートベースのルールで発見されたアプリケーションを後で App-ID ルールに追加できます。 • **Match Usage** (使用状況にマッチ)—発見されたアプリをすべてルールに移動します（**Match Usage** (使用状況にマッチ)させた後、それらは Apps on Rule (ルールのアプリ) の下にリストアップされます）。リストアップされたすべてのアプリケーションをルールで許可しなければならないということが確実な場合、**Match Usage** (使用状況にマッチ)が非常に便利です。しかし、リストアップされたアプリケーションがすべてネットワーク上で許可するアプリケーションであることを確認する必要があります。ルールで発見されたアプリケーションが多い場合（例えば web-browsing を許可するルール）、ルールをコピーしてアプリケーション ベースのルールに移行する方が良いでしょう。**Match Usage** (使用状況にマッチ)は、よく知られたアプリケーションを伴うシンプルなルールに対して上手く機能します。例えば、ポート 22 用のポートベースのルールが SSH トラフィックしか発見していない（かつ、それしか発見しないはずである）場合、安全に**Match Usage** (使用状況にマッチ)できます。
Clone (コピー) ダイアログ Add to This Rule (このルールに追加) ダイアログ Add Apps to Existing Rule (既存のルールに追加) ダイアログ	**Apps Seen** (発見されたアプリ)からアプリケーションを選択し、関連するアプリケーションを持つ**Create Cloned Rule** (ルールをコピーして作成)あるいは**Add to Rule** (ルールに追加)する場合、ダイアログに次の項目がリストアップされます： • **Name** (名前) (Clone (コピー) と Add Apps to Existing Rule (既存のルールにアプリケーションを追加) ダイアログのみ)。 • Clone (コピー):コピーした新しいルールの名前を入力します。

© 2019 Palo Alto Networks, Inc.

項目	の意味

	• Add Apps to Existing Rule (既存のルールにアプリケーションを追加):アプリケーションを追加するルールをドロップダウンメニューから選択するか、ルールの名前を入力します。
	• **Applications** (アプリケーション) :
	  • コンテナ アプリケーションを追加 (デフォルト):すべてのコンテナ アプリケーション、ルールで発見されたアプリケーション、およびルールで発見されていないコンテナ内のアプリのチェックボックスを選択します。
	  • 発見された特定のアプリケーションを追加:ルールで実際に発見されたアプリケーションのみを選択し、その他の選択をすべて解除します。(コンテナ アプリケーションやその他のアプリケーションを手動で選択できます。)
	• **Application** (アプリケーション):
	  • ルール上で選択されたアプリケーションは、緑色で強調表示されます。
	  • コンテナ アプリが灰色で表示され、その個々のアプリケーションが下にリストアップされます。
	  • ルールで発見されたが、 **Applications & Usage** (アプリケーションおよび使用状況) (通常のテキスト) で選択されていないコンテナ内の個々のアプリケーション。
	  • ルールで発見されていないコンテナ内の個々のアプリケーションです (イタリック体) 。
	  • 日付アプリケーションは、ルールで最後に発見されたものです。
	• **Dependent Applications** (依存アプリケーション):
	  • 選択済みのアプリケーションを実行するためには対象のアプリケーションが必要であるため、アプリケーションの依存関係を追加するチェックボックスがデフォルトで有効になっています。
	  • **Depends On** (依存対象)—選択済みのアプリケーションが依存しているアプリケーションのリストです。選択済みのアプリケーションを実行するためには、これらの依存対象のアプリケーションが必要になります。
	  • **Required By** (被依存)—依存対象のアプリケーションを必要とするアプリケーションをリストアップします (**Depends On** (依存対象)) 。 (依存対象のアプリケーションがさらに他のアプリケーションに依存している場合もあります)
	
	Clone (コピー)、**Add to Rule** (ルールに追加)、および**Add Apps to Existing Rule** (既存のルールにアプリケーションを追加)ダイアログは、アプリケーションが破損していないことを確認する際に役立ち、コピーあるいはルールに追加しようとしているアプリケーションに関連する個々のアプリケーションをこれらのダイアログを使って含めることで、今後もルールを適切に維持できるようになります。

セキュリティポリシー オプティマイザー

- Policies (ポリシー) > Security (セキュリティ) > Policy Optimizer (ポリシー オプティマイザー)

© 2019 Palo Alto Networks, Inc.

Policies (ポリシー) > **Security** (セキュリティ) > **Policy Optimizer** (ポリシー オプティマイザー)には次の内容が表示されます：

- アプリが未指定—アプリケーション ベースのルールに変換するポートベースのルールを識別できるよう、アプリケーションを**any** (すべて)に設定したルール。
- 未使用のアプリ—ルールにマッチしたことがないアプリケーションを含むルール。

項目	の意味
氏名	セキュリティポリシー ルールの名前です。
サービス	セキュリティポリシー ルールに関連するサービスです。
トラフィック（バイト、30 日間）	**Traffic (30 days)** (トラフィック（**30** 日）)—過去 30 日間で発見されたトラフィックの量（バイト）です。 最も古いルールはトラフィックの累積量が最も多くなりがちであるため、期間を長くするとそのルールがリストの一番上に残り続けるでしょう。そのため、新しいルールに大量のトラフィックがあっても、古いルールの下にリストアップされる可能性があります。
許可されるアプリ	ルールが許可するアプリケーションです。**Application** (アプリケーション)ダイアログを開けば、そこでルールのアプリケーションを追加・削除できます。
発見されたアプリ	ルールで発見されたアプリケーションの数です。数をクリックして**Applications & Usage** (アプリケーションおよび使用状況)ダイアログを開くと、ルールで設定されているアプリケーションをルールで発見されたアプリケーションと比較してアプリケーションを編集することができます。
新しいアプリが未発見の日数	最後にルールで新しいアプリケーションが見つかってから経過した日数です。
比較	**Applications & Usage** (アプリケーションおよび使用状況)ダイアログを開くと、ルールで設定されているアプリケーションをルールで発見されたアプリケーションと比較してルールを編集することができます。
最後のヒット	トラフィックがルールに最後にマッチした時です。
最初のヒット	トラフィックがルールに最初にマッチした時です。
変更済	ルールを最後に編集した日時。
作成日時	ルールが作成された日時。

© 2019 Palo Alto Networks, Inc.

Policies > NAT [ポリシー > NAT]

ファイアウォールにレイヤー 3 インターフェイスを定義する場合、ネットワーク アドレス変換 (NAT) ポリシーを設定して、送信元または宛先の IP アドレスやポートに対して、パブリックおよびプライベートの変換を実施するかどうかを指定できます。たとえば、内部 (信頼されている) ゾーンからパブリック (信頼されていない) ゾーンに送信されるトラフィックの送信元プライベート アドレスをパブリック アドレスに変換できます。NAT は、バーチャル ワイヤー インターフェイスでもサポートされています。

NAT ルールは、送信元ゾーンと宛先ゾーン、送信元アドレスと宛先アドレス、およびアプリケーション サービス (HTTP など) に基づいています。セキュリティ ポリシーと同様に、NAT ポリシー ルールと受信トラフィックは順番に照合され、トラフィックに一致する最初のルールが適用されます。

必要に応じて、ローカル ルータに静的 ルートを追加し、パブリック アドレスへのトラフィックをすべてファイアウォールにルーティングします。場合によっては、ファイアウォールの受信インターフェイスに静的 ルートを追加し、プライベート アドレスにトラフィックをルーティングして戻す必要があります。

以下の表に、NAT および NPTv6 (IPv6 ネットワーク間プレフィックス変換) の設定を説明します。

- NAT ポリシーの General (全般) タブ
- NAT の Original Packet (元のパケット) タブ
- NAT の Translated Packet (変換済みパケット) タブ
- NAT の Active/Active HA Binding (アクティブ/アクティブ HA バインド) タブ

その他の情報をお探しですか？

「NAT」を参照してください。

NAT ポリシーの General (全般) タブ

- **Policies** > **NAT** [ポリシー] > **General** (全般)

General[全般]タブを使用して、NATポリシーまたはNPTv6ポリシーの名前とその内容説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。作成するNATポリシーのタイプを選択します。ここで選択したタイプによって、 **Original Packet**[元のパケット]タブおよび**Translated Packet**[変換済みパケット]タブで使用できるフィールドが決まります。

NAT ルール - 一般設定	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを **Add** (追加) して指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。

© 2019 Palo Alto Networks, Inc.

NAT ルール - 一般設定	の意味
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag** (タグ)に基づいてルールをグループ化することができます。
NAT タイプ	変換のタイプを指定します。 • **ipv4** – IPv4 アドレス間の変換に使用します。 • **nat64** – IPv6 と IPv4 間の変換に使用します。 • **nptv6** – IPv6 プレフィックス間の変換に使用します。 1つの NAT ルールで IPv4 と IPv6 のアドレス範囲を組み合わせることはできません。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメントアーカイブ	ポリシールールの以前の**Audit Comments** (監査コメント)を表示します。監査コメントアーカイブは CSV 形式でエクスポートできます。

NAT の Original Packet（元のパケット）タブ

- Policies > NAT > Original Packet [ポリシー > NAT > 元のパケット]

ファイアウォールで変換するパケットの送信元ゾーンと宛先ゾーンを定義するには、**Original Packet**（元のパケット）タブを選択します。必要に応じて、宛先インターフェイスとサービスのタイプを指定することもできます。同じタイプの複数の送信元と宛先ゾーンを設定し、そのルールを特定のネットワークやIPアドレスに適用することができます。

NAT ルール - 元のパケット設定	の意味
送信元ゾーン / 宛先ゾーン	元のパケット (非 NAT) パケットについて、1 つ以上の送信元ゾーンと宛先ゾーンを選択します (デフォルトは **any**)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。 複数のゾーンを特定し、管理の手間を少なくすることができます。たとえば、複数の内部 NAT アドレスが同じ外部 IP アドレスに送信されるように設定できます。
宛先インターフェイス	ファイアウォールが変換するパケットの宛先インターフェイスを指定します。異なるIPアドレスプールを持つ2つのISPにネットワークが接続している場合、宛先インターフェイスを使用することで、IP アドレスを異なった方法で変換できます。
サービス	ファイアウォールが送信元または宛先アドレスを変換する対象となるサービスを指定します。新しいサービス グループを定義するには、Objects（オブジェクト）> Service Groups（サービス グループ）を選択します。

© 2019 Palo Alto Networks, Inc.

NAT ルール - 元のパケット設定	の意味
送信元アドレス / 宛先アドレス	ファイアウォールが変換する送信元アドレスと宛先アドレスの組み合わせを指定します。 NPTv6 では、**Source Address** (送信元アドレス) と **Destination Address** (宛先アドレス) に設定されるプレフィックスを xxxx:xxxx::/yy という形式で指定する必要があります。アドレスにインターフェイス識別子 (ホスト) 部分を定義することはできません。サポートされているプレフィックス長の範囲は /32 ~ /64 です。

NAT の Translated Packet (変換済みパケット) タブ

- Policy (ポリシー) > NAT > Translated Packet (変換済みパケット)

Source Address Translation (送信元アドレス変換) については、**Translated Packet** (変換済みパケット) タブを使用して、送信元に対して実行する変換のタイプ、アドレス、さらに場合によっては送信元の変換先であるポートを決定します。

公開 IP アドレスによるアクセスが必要な内部ホスト用に、宛先アドレス変換を設定することもできます。この場合、**Original Packet** (元のパケット) タブに内部ホストのパブリックな送信元アドレスと宛先アドレスを定義し、**Translated Packet** (変換済みパケット) タブで**Static IP** (静的 **IP**) または **Dynamic IP (with session distribution)** (動的 **IP** (セッション配信付属)) を設定し、**Translated Address** (変換後アドレス) を入力します。次に、公開アドレスがアクセスされると、内部ホストの内部 (宛先) アドレスに変換されます。

NAT ルール - 変換済みパケット設定	の意味
送信元アドレスの変換	変換タイプ (動的または静的 アドレス プール) を選択し、送信元アドレスの変換後の IP アドレスまたはアドレス範囲 (アドレス 1 ~ アドレス 2) を入力します (**Translated Address** (変換後アドレス))。アドレス範囲のサイズは、以下のアドレス プールのタイプによって制限されます。 • **Dynamic IP And Port** (動的 **IP** およびポート) – アドレス選択は、送信元 IP アドレスのハッシュに基づきます。特定の送信元 IP アドレスに対して、ファイアウォールのすべてのセッションで同じ変換後の送信元アドレスが使用されます。動的 IP およびポート (DIPP) の送信元 NAT では、NAT プール内の各 IP アドレスで約 64,000 個の連続するセッションがサポートされます。一部のモデルでは、オーバーサブスクリプションがサポートされます。その場合、1 つの IP で 64,000 個を超える連続するセッションをホストできます。 Palo Alto Networks® DIPP NAT では、使用可能な IP アドレスとポートの数でサポートされる数よりも多くの NAT セッションがサポートされます。オーバーサブスクリプションを使用すると、宛先 IPアドレスが一意の場合、ファイアウォールは IPアドレスとポートの組み合わせを PA-220、PA-820、PA-850、VM-50、VM-300、および VM-1000-HV ファイアウォールで同時に 2 回、PA-5220 ファイアウォールと PA-3200 Series ファイアウォールで同時に 4 回、PA-5250、PA-5260、PA-5280、PA-7050、PA-7080、VM-500、および VM-700 ファイアウォールで 8 回同時に使用できます。 • **Dynamic IP** (動的 **IP**) : 指定した範囲で次に使用可能なアドレスを変換しますが、ポート番号は変更されません。最大32000 個の連続した IP アドレスがサポートされます。動的 IP プールには、複数のサブネットを含めることができるため、内部ネットワーク アドレスを 2 つ以上の別個のパブリック サブネットに変換できます。

© 2019 Palo Alto Networks, Inc.

NAT ルール - 変換済みパケット設定	の意味
	• **Advanced (Dynamic IP/Port Fallback)** (詳細 (動的IP/ポートのフォールバック)) — IP およびポートの変換を実行するほか、プライマリ プールのアドレスを使い切った場合に使用するフォール バック プールを作成するには、このオプションを使用します。**Translated Address** (変換後アドレス) オプションまたは **Interface Address** (インターフェイス アドレス) オプションを使用するとプールのアドレスを定義できます。後者のオプションは IP アドレスを動的に受け取るインターフェイス用です。代替プールを作成するときには、アドレスがプライマリ プールのアドレスと重複しないことを確認します。
送信元アドレスの変換 (続)	• **Static IP**[静的 IP] — 変換に同じアドレスが常に使用され、ポート番号は変更されません。たとえば、送信元の範囲が 192.168.0.1 ~ 192.168.0.10 で、変換の範囲が 10.0.0.1 ~ 10.0.0.10, の場合、アドレス 192.168.0.2 は必ず 10.0.0.2 に変換されます。アドレス範囲は事実上無制限です。 NPTv6 送信元アドレスの変換には、**Static IP** (静的 **IP**) 変換を使用する必要があります。NPTv6 の場合、**Translated Address** (変換後アドレス) 用に設定されたプレフィックスは xxxx:xxxx::/yy の形式でなければならず、アドレスにはインタフェース識別子 (ホスト) 部分を定義することはできません。サポートされているプレフィックス長の範囲は /32 ~ /64 です。 • **None**[なし] — 変換は実行されません。
双方向	(任意) **Static IP (静的 IP)** 送信元アドレス変換で、対応する変換 (NAT または NPTv6) を設定する変換の反対方向にも作成する場合は、双方向変換を有効にします。 双方向変換を有効にする場合は、双方向のトラフィックを制御するセキュリティポリシーが設定されていることを必ず確認しておく必要があります。このようなポリシーが設定されていない場合、双方向変換機能により双方向のパケットが自動的に変換されることになります。
宛先アドレスの変換	ファイアウォールに宛先 NAT を実行させるには、次のオプションを設定します。通常は宛先 NAT を使用して、電子メール サーバーなどの内部サーバーにパブリック ネットワークからアクセスできるようにします。
変換タイプと変換後アドレス	ファイアウォールが宛先アドレスで実行する変換のタイプを選択します。 • **None**[なし] (デフォルト) • **Static IP (静的 IP)**—**Translated Address** (変換後アドレス) を IPアドレスまたは IPアドレスの範囲として、また元の宛先アドレスおよびポート番号が変換される **Translated Port** (変換後ポート) (1 ~ 65535) として入力します。**Translated Port** (変換済みポート) フィールドがブランクの場合、宛先ポートは変更されません。 NPTv6 では、宛先プレフィックス **Translated Address** (変換後アドレス) に設定するプレフィックスを「xxxx:xxxx::/yy」の形式で指定する必要があります。アドレスにインターフェイス識別子 (ホスト) 部分を定義することはできません。サポートされているプレフィックス長の範囲は /32 ~ /64 です。 *NPTv6* では、厳密なプレフィックス変換が行われるため、変換済みポートはサポートされていません。ポート アドレスおよびホスト アドレスのセクションは、変換されずにそのまま転送されます。

© 2019 Palo Alto Networks, Inc.

NAT ルール - 変換済みパケット設定	の意味
	また、*IPv4* の静的 *IP* 変換では *Enable DNS Rewrite (DNS* 書き換えを有効にする*)* こともできます *(*以下で説明します*)*。 • **Dynamic IP (with session distribution)** (動的 **IP** (セッション配信あり)) —Select or enter a **Translated Address** (変換後アドレス) をファイアウォールが選択するFQDN、アドレス オブジェクト、またはアドレスグループである translated address (変換後) を選択または入力します。DNS サーバーが FQDN に複数のアドレスを返す場合、またはアドレスオブジェクトまたはアドレス グループが複数のIPアドレスに変換された場合、ファイアウォールは指定された **Session Distribution Method** (セッション配信方式) を使用してそれらのアドレス間でセッションを配信します。
Session Distribution Method セッション配信方式	destination NAT (宛先NAT - DNAT) 変換を **Dynamic IP (動的IP) (**セッション分散あり**)**になるように選択した場合、宛先変換アドレス (FQDN、アドレス オブジェクト、またはアドレス グループ) が複数のアドレスで解決できます。ファイアウォールがこれらのアドレス間でセッションを分散 (割り当て) する方法を選択して、バランス良くセッションを分散させることができます。 • **Round Robin (**ラウンドロビン**)**— (デフォルト) 新しいセッションをローテーションで IP アドレスに割り当てます。他のいずれかの分散方式を選択しなければならない環境を除き、この方式を使用します。 • **Source IP Hash (**送信元 **IP** ハッシュ**)**—送信元 IP アドレスのハッシュに基づいて新しいセッションを割り当てます。単一の送信元 IP から来るインバウンド トラフィックがある場合は、**Source IP Hash (**送信元 **IP** ハッシュ**)**以外の方式を選択してください。 • **IP Modulo (IP** モジュロ**)**—ファイアウォールはインバウンド パケットの送信元および宛先 IP アドレスを考慮します。ファイアウォールは XOR 操作およびモジュロ操作を実行し、その結果、ファイアウォールが新しいセッションを割り当てる IP アドレスが決まります。 • **IP Hash (IP** ハッシュ**)**—送信元および宛先 IP アドレスのハッシュを使用して新しいセッションを割り当てます。 • **Least Sessions (**最小数のセッション**)**—同時セッションが最も少ない IP アドレスに新しいセッションを割り当てます。短期間のセッションが多くある場合は、 **Least Sessions (**最小数のセッション**)** を使用することでバランス良くセッションを分散させることができます。
Enable DNS Rewrite (DNS 書き換えを有効にする)	PAN-OS 9.0.2 以降の 9.0 リリースでは、宛先 NAT ポリシー ルール タイプが **ipv4** で宛先アドレス変換タイプが **Static IP (**静的 **IP)**の場合、 **Enable DNS Rewrite (DNS** 書き換えを有効にする**)** オプションが利用可能です。宛先 NAT を使用し、ファイアウォールの一方の側で DNS サービスを使用して、ファイアウォールの反対側のクライアントの FQDN を解決する場合は、DNS 書き換えを有効にすることができます。DNS 応答がファイアウォールを通過するとき、ファイアウォールは、DNS 応答が NAT ポリシー ルールで一致する元の宛先アドレスまたは変換済み宛先アドレスを基準にして、DNS 応答の IPアドレスを書き換えます。単一の NATポリシー ルールでは、ファイアウォールがルールに一致するパケットに対して NAT を実行し、 ルールに一致する DNS 応答の IPアドレスに対して NAT を実行します。NAT ルールと相対的に、ファイアウォールが DNS 応答内の IP アドレスに対して NAT を実行する方法を逆または順に指定する必要があります。 • **reverse(**逆**)**—(デフォルト) パケットがルールの変換された宛先アドレスと一致する DNS 応答の場合、ルールが使用する逆変換を使用して DNS 応答を変換します。

© 2019 Palo Alto Networks, Inc.

NAT ルール - 変換済みパケット設定	の意味
	例えば、ルールが 1.1.1.10 を 192.168.1.10 に変換する場合、ファイアウォールは 192.168.1.10 の DNS 応答を 1.1.1.10 に書き換えます。 • **forward(順)**—パケットがルールの元の宛先アドレスと一致する DNS 応答の場合、ルールが使用するのと同じ変換を使用して DNS 応答を変換します。例えば、ルールが 1.1.1.10 を 192.168.1.10 に変換する場合、ファイアウォールは 1.1.1.10 の DNS 応答を 192.168.1.10 に書き換えます。

NAT の Active/Active HA Binding（アクティブ/アクティブ HA バインド）タブ

- Policies > NAT > Active/Active HA Binding [ポリシー > NAT > アクティブ/アクティブHAバインド]

Active/Active HA Binding（アクティブ/アクティブ HA バインド）タブは、ファイアウォールがアクティブ/アクティブの高可用性（HA）設定になっている場合にのみ使用できます。この設定では、（静的または動的 NAT に関係なく）各送信元 NAT ルールをデバイス ID 0 またはデバイス ID 1 にバインドし、各宛先 NAT ルールをデバイス ID **0**、デバイス ID **1**、または **both**（両方）（デバイス ID 0 とデバイス ID 1）、あるいはアクティブ-プライマリのファイアウォールにバインドする必要があります。

以下のように、**Active/Active HA Binding**（アクティブ/アクティブ **HA** バインド）設定を選択し、NAT ルールを HA ファイアウォールにバインドします。

- **0** - NATルールをHAデバイスID 0 のファイアウォールにバインドします。
- **1** - NATルールをHAデバイスID 1 のファイアウォールにバインドします。
- **both**[両方] - NATルールをHAデバイスID 0 のファイアウォールとHAデバイスID 1 のファイアウォールの両方にバインドします。この設定では動的IPや、動的IPおよびポートのNATはサポートされません。
- **primary**[プライマリ] - NATルールをHAアクティブ-プライマリの状態にあるファイアウォールにバインドします。この設定では動的IPや、動的IPおよびポートのNATはサポートされません。

2つのHAピアが固有のNAT IPアドレスプールを持つ場合は、デバイス固有のNATルールを設定することができます。

ファイアウォールが新しいセッションを作成すると、HAバインドはセッションに一致したNATルールを判別します。ルールの照合が行われるためには、バインドにセッションオーナーが含まれている必要があります。NATルールの照合はセッションを作成するファイアウォールが行うものですが、セッションは、セッションオーナーにバインドされたNATルールと照合され、そのうち1つのルールに基づいて変換されます。デバイス固有のルールの場合、ファイアウォールはセッション オーナーに関連付けられていないすべてのNATルールを飛ばして進みます。デバイスID 1 のファイアウォールがセッションオーナーであり、セッションを作成するファイアウォールになる場合を例にとってみましょう。デバイスID 1 は、セッションとNATルールを照合する際に、デバイスID 0 にバインドされたすべてのルールを無視して照合を行います。

片方のピアに障害が発生した場合は、NAT変換を含め、もう一方のピアが、障害が発生したピアのセッション同期用トラフィックの処理を続けます。Palo Alto Networksでは、もう一方のデバイスIDにバインドされたNATルールを重複して作成することをお勧めしています。すなわち、同じ送信元変換アドレスと、同じ宛先変換アドレスを持つ 2 つの NAT ルールが存在し、各ルールがそれぞれのデバイス ID にバインドされます。この設定により、HA ピアは新しいセッションのセットアップ タスクを実行し、自身のデバイス ID にバインドされている NAT ルールで NAT ルールの照合を実行できます。重複する NAT ルールがない場合、機能中のピアは NAT ポリシーの照合を試行しますが、セッションはファイアウォール独自のデバイスに固有のルールと一致しないため、ファイアウォールは自身のデバイス ID にバインドされていないその他の NAT ルールをすべて省略します。

その他の情報をお探しですか？

© 2019 Palo Alto Networks, Inc.

「NAT in Active/Active HA Mode（アクティブ/アクティブ HA モードの NAT）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Policies > QoS [ポリシー > QoS]

QoS ポリシー ルールを追加して、特定の QoS 処理を受け取るトラフィックを定義し、各 QoS ポリシー ルールの QoS クラスを割り当てて、割り当てたクラスのサービスが QoS 対象のインターフェイスから抜け出る際に関連ルールに一致するすべてのトラフィックに適用されるように指定します。

Panoramaからファイアウォールにプッシュされた QoSポリシールールはオレンジ色で表示され、ファイアウォール上からは編集を行うことができません。

また、ファイアウォールの QoS 提供を完全に有効にするために、以下を実行します。

- サービスの各 QoS クラスの帯域幅制限を設定します (Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > QoS を選択して QoS プロファイルを追加または変更)。
- インターフェイス上で QoS を有効にします (Network (ネットワーク) > QoS を選択します)。

QoS のワークフロー、コンセプト、使用例の詳細は、「Quality of Service (サービス品質)」を参照してください。

新しいルールを **Add** (追加) するか、既存のルールをコピーして、以下のフィールドを定義します。

QoS ポリシー ルール設定	
General [全般] タブ	
氏名	ルールの識別に使用する名前 (最大 63 文字) を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	任意の説明を入力します。
タグ	ポリシーにタグを付ける場合、タグを **Add** (追加) して指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復号」と「復号なし」というタグを付けたり、特定のデータ センターに関するポリシーにその場所の名前を使用したりできます。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag (タグ)**に基づいてルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments (監査コメント)**を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。
Source [送信元] タブ	

© 2019 Palo Alto Networks, Inc.

QoS ポリシー ルール設定	
送信元ゾーン	送信元ゾーンを選択します（デフォルトは **any**（任意））。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。
送信元アドレス	IPv4 または IPv6 アドレスの送信元の組み合わせを指定します。識別されたアプリケーションの送信元アドレス情報は、これらのアドレスでオーバーライドされます。特定のアドレスを選択するには、ドロップダウンリストから **select**[選択する] を選択して、以下のいずれかを実行します。 • 使用可能な列で該当するアドレスやアドレスグループの横にあるチェックボックスをオンにし、**Add** (追加) をクリックして選択内容を Selected (選択中の) 列に追加します。 • 名前の最初の数文字を検索フィールドに入力します。入力した文字で始まるすべてのアドレスおよびアドレスグループが一覧表示されます。リスト内の項目を選択するとAvailable [使用可能] 列のオプションが有効化されます。この操作を必要な回数だけ繰り返し、次に **Add**[追加] をクリックします。 • 1 つ以上の IP アドレスを (1 行ごとに 1 つ) 入力します。ネットワーク マスクは指定してもしなくてもかまいません。一般的な形式は以下のとおりです。*<ip_address>/<mask>* • アドレスを削除する場合は、Selected [選択済み] 列より希望のアドレスを選択し、**Delete** [削除] をクリックするか、**any**[すべて] を選択して、すべてのアドレスおよびアドレスグループをクリアします。 このポリシーまたは別のポリシーで使用できる新しいアドレスを追加するには、**New Address**[新規アドレス] をクリックします。新しいアドレス グループを定義するには、Objects（オブジェクト）> Address Groups（アドレス グループ）を選択します。
Source User（送信元ユーザー）	QoS ポリシーが適用される送信元のユーザーおよびグループを指定します。
Negate	このタブで指定した情報に一致しないものに対してポリシーを適用する場合は、このオプションを選択します。
Destination [宛先] タブ	
宛先ゾーン	宛先ゾーンを選択します（デフォルトは **any**（任意））。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。
宛先アドレス	IPv4 または IPv6 アドレスの送信元の組み合わせを指定します。識別されたアプリケーションの送信元アドレス情報は、これらのアドレスでオーバーライドされます。特定のアドレスを選択するには、ドロップダウンリストから **select**[選択する] を選択して、以下のいずれかを実行します。 • 使用可能な列で該当するアドレスやアドレスグループの横にあるチェックボックスをオンにし、**Add** (追加) をクリックして選択内容を Selected (選択中の) 列に追加します。 • 名前の最初の数文字を検索フィールドに入力します。入力した文字で始まるすべてのアドレスおよびアドレスグループが一覧表示されます。リスト

© 2019 Palo Alto Networks, Inc.

QoS ポリシー ルール設定	
	内の項目を選択するとAvailable [使用可能] 列のオプションが有効化されます。この操作を必要な回数だけ繰り返し、次に **Add**[追加] をクリックします。 • 1 つ以上の IP アドレスを (1 行ごとに 1 つ) 入力します。ネットワーク マスクは指定してもしなくてもかまいません。一般的な形式は以下のとおりです。*<ip_address>/<mask>* • アドレスを削除する場合は、Selected [選択済み] 列より希望のアドレスを選択し、**Delete** [削除] をクリックするか、**any**[すべて] を選択して、すべてのアドレスおよびアドレスグループをクリアします。 このポリシーまたは別のポリシーで使用できる新しいアドレスを追加するには、**New Address**[新規アドレス] をクリックします。
Negate	このタブで指定した情報に一致しないものに対してポリシーを適用する場合は、このオプションを選択します。
[アプリケーション] タブ	
Application [アプリケーション]	QoS ルールを適用する特定のアプリケーションを選択します。新しいアプリケーションまたはアプリケーション グループを定義する場合は、**Objects** (オブジェクト) > **Applications** (アプリケーション) を選択します。 アプリケーションに複数の機能がある場合、アプリケーション全体または個別の機能を選択できます。アプリケーション全体を選択した場合、すべての機能が含まれ、将来、機能が追加されるとアプリケーション定義が自動的に更新されます。 QoSルールでアプリケーション グループ、フィルタ、またはコンテナを使用している場合は、Application [アプリケーション] 列のオブジェクトの上にマウスを置き、下向き矢印をクリックして **Value**[値] を選択すると、オブジェクトの詳細が表示されます。これにより、**Objects** (オブジェクト) タブに移動しなくても、ポリシーから直接アプリケーション メンバーを簡単に表示できます。
[サービス/URL カテゴリ] タブ	
サービス	特定の TCP や UDP のポート番号に制限するには、サービスを選択します。ドロップダウンリスト リストから以下のいずれかを選択します。 • **any** - 選択したアプリケーションがすべてのプロトコルやポートで許可または拒否されます。 • **application-default** (アプリケーション-デフォルト) – 選択したアプリケーションが、**Palo Alto Networks** によって定義されたデフォルトのポートでのみ許可または拒否されます。これは、許可ポリシーの推奨オプションです。 • **Select**[選択] - **Add**[追加] をクリックします。既存のサービスを選択するか、**Service**[サービス] または **Service Group**[サービス グループ] を選択して新しいエントリを指定します。
URL カテゴリ	QoS ルールを適用する URL カテゴリを選択します。 • URL カテゴリに関係なくセッションでこの QoS ルールを照合できるようにするには、**Any**[いずれか] を選択します。

© 2019 Palo Alto Networks, Inc.

QoS ポリシー ルール設定	
	• カテゴリを指定するには、**Add**[追加] をクリックし、ドロップダウンリスト リストから特定のカテゴリ (カスタム カテゴリも含む) を選択します。複数のカテゴリを追加できます。カスタム カテゴリの定義の詳細は、「Objects（オブジェクト）> External Dynamic Lists（外部動的リスト）」を参照してください。
DSCP/TOS タブ	
[any]	**Any** [いずれか] (デフォルト) を選択すると、トラフィックに定義された Differentiated Services Code Point（DSCP）値またはIP優先度/Type of Service（ToS）にかかわらず、ポリシーをトラフィックに照合できます。
コードポイント	[コードポイント] を選択すると、トラフィックは、パケットの IP ヘッダーに定義された DSCP 値または ToS 値に基づいて QoS 処理を受信できます。DSCP 値と ToS 値は、トラフィックに要求されるサービス レベル (最優先、ベスト エフォート配信など) を示すために使用されます。コードポイントをQoSポリシーの一致基準として使用すると、セッションは、セッション開始時に検出されたコードポイントに基づいてQoS処理を受信できます。 QoSポリシーにトラフィックを照合させるには、引き続きコードポイントを **Add**[追加] します。 • コードポイント エントリに分かりやすい **Name**[名前] を付けます。 • QoSポリシーの一致条件として使用するコードポイントの **Type**[タイプ] を選択し、特定の **Codepoint**[コードポイント] 値を選択します。**Codepoint Name**[コードポイント名] と **Binary Value**[バイナリ値] を入力することにより、**Custom Codepoint**[カスタムコードポイント] を作成することもできます。
[その他の設定] タブ	
クラス	ルールに割り当てる QoS クラスを選択して、**OK** をクリックします。クラス特性は、QoS プロファイルで定義します。QoS クラスの設定方法の詳細は、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> QoS」を参照してください。
スケジュール	• ポリシーを常時アクティブにしておく場合は**None** [なし] を設定します。 • ドロップダウンリストから**Schedule** [スケジュール]（カレンダーのアイコン）を選択し、単発の時間範囲またはルールがアクティブなあいだ繰り返される時間範囲を設定します。

© 2019 Palo Alto Networks, Inc.

Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーディング]

通常、トラフィックがファイアウォールに到着すると、入力インターフェイスの仮想ルーターが、宛先 IP アドレスに基づいてルートを決定し、それによって出力インターフェイス、および宛先セキュリティゾーンが決まります。ポリシーベースの転送（PBF）ルールを作成して、送信元ゾーン、送信元アドレス、送信元ユーザー、宛先アドレス、宛先アプリケーション、宛先サービスなど、他の情報を指定して、出力インターフェイスを決定することができます。アプリケーションに関連付けられた宛先 IP アドレスおよびポートの最初のセッションは、アプリケーション固有のルールには一致せず、後続の PBF ルール (アプリケーションが指定されない) か、仮想ルーターの転送テーブルに従って転送されます。同じアプリケーションについて、その宛先IPアドレスおよびポートの後続セッションはすべて、アプリケーション固有のルールに一致します。PBF ルールによる転送を確実に行うために、アプリケーション固有のルールを使用しないことをお勧めします。

必要に応じて PBF ルールを使用して、トラフィックが追加の仮想システムを経由するように「VSYS に転送」転送アクションで強制することができます。この場合、宛先仮想システムからファイアウォールの特定の出力インターフェイスを通じてパケットを転送する追加の PBF ルールを定義する必要があります。

以下の表では、ポリシー ベース フォワーディング設定について説明します。

- ポリシー ベース フォワーディングの General（全般）タブ
- ポリシー ベース フォワーディングの Source（送信元）タブ
- ポリシー ベース フォワーディングの Destination/Application/Service（宛先/アプリケーション/サービス）タブ
- ポリシー ベース フォワーディングの Forwarding（転送）タブ

その他の情報をお探しですか？

「Policy-Based Forwarding（ポリシー ベースの転送）」を参照してください。

ポリシー ベース フォワーディングの General（全般）タブ

General[全般]タブを使用してPBFポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングにも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ポリシーの説明を入力します (最大1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを **Add**（追加）して指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに

© 2019 Palo Alto Networks, Inc.

項目	の意味
	「復号」と「復号なし」というタグを付けたり、特定のデータ センターに関するポリシーにその場所の名前を使用したりできます。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag** (タグ)に基づいてルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments** (監査コメント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

ポリシー ベース フォワーディングの Source（送信元）タブ

Source（送信元）タブを選択して、送信元ゾーンまたは送信元アドレスを定義し、送信元から受信するトラフィックに転送ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	送信元ゾーン (デフォルトは any) を選択する場合は、**Add**[追加]をクリックしてドロップダウンリストから選択します。新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。 ポリシーベースの転送では、レイヤー *3* タイプのゾーンのみがサポートされます。
送信元アドレス	**Add**[追加] をクリックして送信元アドレス、アドレス グループ、または地域を追加します (デフォルトは any)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**[アドレス]、**Adress Group**[アドレス グループ]、または**Region**[地域]をクリックして設定を行います。
Source User（送信元ユーザー）	**Add** [追加]をクリックして、ポリシーを適用する送信元ユーザーまたはユーザー グループを選択します。以下の送信元ユーザー タイプがサポートされます。 • **any** – ユーザー データに関係なく任意のトラフィックが含まれます。 • **pre-logon**（ログオン前） – GlobalProtect™ を使用してネットワークに接続しているが、自分のシステムにはログインしていないリモート ユーザーが含まれます。GlobalProtect アプリのポータルに Pre-logon（ログオン前）オプションが設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成でき、また、ユーザーが直接ログインしてい

© 2019 Palo Alto Networks, Inc.

項目	の意味
	なくても、そのマシンは完全にログインしているかのようにドメインで認証されます。 • **known-user**[既知のユーザー] – 認証されたすべてのユーザー (ユーザーデータがマップされた IP) が含まれます。このオプションは、ドメインの「ドメイン ユーザー」グループに相当します。 • **unknown**[未知] – 認証されていないすべてのユーザー (ユーザーにマップされていない IP アドレス) が含まれます。たとえば、unknown はゲストレベルのアクセスに使用できます。これらのユーザーは、ネットワーク上のIPを持っていますが、ドメインに認証されず、ファイアウォール上にIPアドレス対ユーザーのマッピング情報がないためです。 • **select**[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1 人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。

ポリシー ベース フォワーディングの Destination/Application/Service (宛先/アプリケーション/サービス) タブ

Destination/Application/Service[宛先/アプリケーション/サービス]タブを使用して、転送ルールに一致するトラフィックに適用される宛先設定を定義します。

項目	の意味
宛先アドレス	**Add** (追加) をクリックして宛先アドレスあるいはアドレス グループを追加します (デフォルトは any) 。デフォルトでは、ルールは、**any** IP アドレスに適用されます。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address** (アドレス)、**Adress Group** (アドレスグループ)をクリックして設定を行います。
アプリケーション/サービス	PBF ルールを適用する特定のアプリケーションを選択します。新しいアプリケーションを定義する方法については、「アプリケーションの定義」を参照してください。アプリケーション グループを定義する方法については、「Objects (オブジェクト) > Application Groups (アプリケーション グループ) 」を参照してください。 アプリケーション固有のルールを PBF で使用することはお勧めできません。できるかぎり、サービス オブジェクト (プロトコルまたはアプリケーションによって使用されるレイヤー *4* ポート (*TCP* または *UDP*)) を使用してください。 これらのアプリケーションの詳細を表示するには、**Application** (アプリケーション)列のオブジェクトの上にマウスを置き、下矢印をクリックして、**Value** (値)を選択します。これにより、Object (オブジェクト)タブに移動しなくても、ポリシーから直接アプリケーション情報を簡単に表示できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	カスタム アプリケーション、アプリケーション フィルタ、アプリケーション グループは *PBF* ルールで使用できません。

ポリシー ベース フォワーディングの Forwarding（転送）タブ

Forwarding[転送]タブを使用して、転送ポリシーに一致するトラフィックに適用されるアクションおよびネットワーク情報を定義します。トラフィックは、ネクスト ホップ IP アドレスまたは仮想システムに転送することも、ドロップすることもできます。

項目	の意味
操作	以下のいずれかのオプションを選択します。 • **Forward**[転送] – ネクストホップの IP アドレスと出力インターフェイス (指定したネクストホップに到達するためにパケットが通るインターフェイス) を指定します。 • **Forward To VSYS**[VSYSに転送] – ドロップダウンリストから転送先となる仮想システムを選択します。 • **Discard**[破棄] – パケットを廃棄します。 • **No PBF**[PBF なし] – パケットが通るパスを変更しません。このオプションは、ルールに定義された送信元/宛先/アプリケーション/サービスの条件に一致するパケットを除外します。パケットの照合には、PBF の代わりにルーティング テーブルを使用します。ファイアウォールは、ルーティング テーブルを使用して、一致したトラフィックをリダイレクト ポートから除外します。 *Action (アクション) として Forward (転送) あるいは Forward to VSYS (VSYS に転送) を使用し、Monitor (監視) プロファイルをトラフィックに適用できるようにします。（Action (アクション) がトラフィックを転送しない場合は Monitor (監視) プロファイルを適用できません）監視プロファイルは IP アドレスを監視します。対象の IP アドレスへの接続が失敗すると、Monitor (監視) プロファイルがアクションを指定します。*
出口インターフェイス	パケットを特定の出力インターフェイスに向けます。
ネクストホップ	パケットを特定のインターフェイスに向ける場合は、次のいずれかの方法でパケット用のネクストホップを指定します： • **IP Address (IP アドレス)**–IP アドレスを選択し、さらに IPv4 あるいは IPv6 アドレスを使用するアドレス オブジェクトを選択（あるいはアドレス オブジェクトを新たに作成）します。 • **FQDN**–FQDN を選択し、さらに FQDN を使用するアドレス オブジェクトを選択（あるいはアドレス オブジェクトを新たに作成）します。 • **None (なし)**–ネクストホップが存在せず、パケットがドロップされます。
監視	(任意) モニタリングを有効にして、ターゲット **IP Address**[IP アドレス]または**Next Hop**[ネクスト ホップ] IP アドレスとの接続を確認します。**Monitor (監視)** を選択して、IP アドレスが到達不能な場合のアクションを指定した（デフォルトまたはカスタム、**Network (ネットワーク)** > **Network Profiles (ネット**

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ワーク プロファイル) > **Monitor** (監視)) モニタリング **Profile** (プロファイル) を関連付けます。 *Monitor* (監視) プロファイルを設定して監視を有効化し、出力インターフェイスでエラーが発生した場合やルートがダウンした場合に、ファイアウォールがプロファイル内のアクションを実行してサービスの中断を最小化あるいは防止できるようにします。
対称リターンの適用	(非対称ルーティング環境では必須) **Enforce Symmetric Return** (対称リターンの適用) を選択して、**Next Hop Address** (ネクスト ホップ アドレス) リストに IP アドレスを入力します。 対称リターンを有効にすると、リターン トラフィック (たとえば、LAN 上の信頼されたゾーンからインターネットへのトラフィック) が、インターネットからトラフィックが入るときと同じインターフェイスを介して外向きに転送されます。
スケジュール	ルールを適用する日時を制限するには、ドロップダウンリストからスケジュールを選択します。新しいスケジュールを定義する手順については、「復号化された SSL トラフィックのコントロールの設定」を参照してください。

© 2019 Palo Alto Networks, Inc.

Policies > Decryption [ポリシー > 復号化]

トラフィックを復号するようにファイアウォールを設定して、可視化、管理、および詳細なセキュリティを実現できます。復号化ポリシーは、SSL (Secure Sockets Layer) (IMAP(S)、POP3(S)、SMTP(S)、FTP(S)、Secure Shell (SSH) トラフィックなどの SSL カプセル化プロトコルを含む) に適用できます。SSH復号を使用して、許可されていないアプリケーションやコンテンツがセキュアなプロトコルでトンネリングされないようにアウトバウンドおよびインバウンドSSHトラフィックを復号化することができます。

復号化ポリシー ルールを追加して、復号化するトラフィックを定義することができます（URL の分類に基づいたトラフィックの復号化など）。復号化ポリシールールと受信トラフィックは順番に照合されるため、より特定されたルールの方が全般的なルールよりも優先されます。

SSL フォワードプロキシの設定では、信頼された証明書を設定する必要があります。この証明書はユーザーが接続中のサーバーが、ファイアウォールによって信頼された認証局によって著名された証明書を保持している時にユーザーに提示されます。**Device** > **Certificate Management** > **Certificates**[デバイス > 証明書の管理 > 証明書]のページで証明書を作成し、証明書の名前をクリックして、**Forward Trust Certificate**[信頼された証明書の転送] チェックボックスをオンにします。

例えばファイアウォールは証明書のピンニングあるいはクライアント認証を使用するため、ファイアウォールは復号化を技術的に妨げるアプリケーションを復号化しません。

「List of Applications Excluded from SSL Decryption（SSL 復号化除外アプリケーションのリスト）」を参照してください。

以下の表では、復号化ポリシー設定について説明します。

- 復号化の General（全般）タブ
- 復号化の Source（送信元）タブ
- 復号化の Destination（宛先）タブ
- 復号化の Service/URL Category（サービス/URL カテゴリ）タブ
- 復号化の Options（オプション）タブ

その他の情報をお探しですか？

「Decryption（復号化）」を参照してください。

復号化の General（全般）タブ

General[全般]タブを使用して、復号化ポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを **Add**（追加）して指定します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復号」と「復号なし」というタグを付けたり、特定のデータ センターに関するポリシーにその場所の名前を使用したりできます。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag** (タグ)に基づいてルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments** (監査コメント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

復号化の Source（送信元）タブ

Source[送信元]タブを使用して、送信元ゾーンまたは送信元アドレスを定義し、送信元から受信するトラフィックに復号化ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	**Add**[追加] をクリックして送信元ゾーンを選択します (デフォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
送信元アドレス	**Add**[追加] をクリックして送信元アドレス、アドレス グループ、または地域を追加します (デフォルトは any)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**[アドレス]、**Adress Group**[アドレス グループ]、または**Region**[地域]をクリックして設定を行います。**Negate**[上記以外]を選択すると、設定したアドレス以外の任意のアドレスを指定したことになります。
Source User（送信元ユーザー）	**Add** [追加]をクリックして、ポリシーを適用する送信元ユーザーまたはユーザー グループを選択します。以下の送信元ユーザー タイプがサポートされます。 • **any** – ユーザー データに関係なく任意のトラフィックが含まれます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **pre-logon**[ログオン前] – GlobalProtect を使用してネットワークに接続しているが、自分のシステムにはログインしていないリモート ユーザーが含まれます。GlobalProtect アプリのポータルに Pre-logon (ログオン前) オプションが設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成でき、また、ユーザーが直接ログインしていなくても、そのマシンは完全にログインしているかのようにドメインで認証されます。 • **known-user**[既知のユーザー] – 認証されたすべてのユーザー (ユーザーデータがマップされた IP) が含まれます。このオプションは、ドメインの「ドメイン ユーザー」グループに相当します。 • **unknown**[未知] – 認証されていないすべてのユーザー (ユーザーにマップされていない IP アドレス) が含まれます。たとえば、unknown をゲスト レベルのアクセスに対して使用できます。これらのユーザーは、ネットワーク上の IP を持っていますが、ドメインに認証されず、ファイアウォール上に IP 対ユーザーのマッピング情報がないためです。 • **select**[選択] – このウィンドウで選択したユーザーが含まれます。たとえば、1 人のユーザー、個々のユーザーのリスト、グループを追加したり、手動でユーザーを追加する場合があります。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。

復号化の Destination (宛先) タブ

Destination (宛先)タブを使用して、宛先ゾーンまたは宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
宛先ゾーン	**Add**[追加] をクリックして宛先ゾーンを選択します (デフォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、 Network > Zones [ネットワーク > ゾーン] を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
宛先アドレス	**Add**[追加] をクリックして宛先アドレス、アドレス グループ、または地域を追加します (デフォルトは any)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**[アドレス]、**Adress Group**[アドレスグループ]、または**Region**[地域]をクリックして設定を行います。**Negate**[上記以

© 2019 Palo Alto Networks, Inc.

項目	の意味
	外]を選択すると、設定したアドレス以外の任意のアドレスを指定したことになります。

復号化の Service/URL Category（サービス/URL カテゴリ）タブ

Service/URL Category[サービス/URLカテゴリ]タブでは、復号化ポリシーを、TCPポート番号に基づいてトラフィックに、または任意のURLカテゴリ (またはカテゴリリスト) に適用できます。

項目	の意味
サービス	特定の TCP/UDP ポート番号に基づいて、復号化ポリシーをトラフィックに適用します。ドロップダウンリスト リストから以下のいずれかを選択します。 • **any** - 選択したアプリケーションがすべてのプロトコルやポートで許可または拒否されます。 • **application-default**[アプリケーション-デフォルト] – 選択したアプリケーションが、Palo Alto Networks によってアプリケーション用に定義されたデフォルトのポートでのみ復号化 (または復号化を免除) されます。 • **Select**[選択] - **Add**[追加] をクリックします。既存のサービスを選択するか、新規の **Service**[サービス] または **Service Group**[サービス グループ] を指定します。（または Objects > Services [オブジェクト > サービス] および Objects（オブジェクト）> Service Groups（サービス グループ）を選択します）。
URL Category [URL カテゴリ] タブ	復号化ルールを適用する URL カテゴリを選択します。 • URL カテゴリに関係なくすべてのセッションを照合するには、**any** を選択します。 • カテゴリを指定するには、**Add**[追加] をクリックし、ドロップダウンリスト リストから特定のカテゴリ (カスタム カテゴリも含む) を選択します。複数のカテゴリを追加できます。カスタムカテゴリの定義方法に関する詳細を参照してください。

復号化の Options（オプション）タブ

Options[オプション]タブを使用して、一致したトラフィックを復号化するかどうかを決定します。**Decrypt**[復号] が設定されている場合、復号化タイプを指定します。復号化プロファイルを設定または選択して、その他の復号化機能を追加することもできます。

項目	の意味
操作	トラフィックの**decrypt**[復号] または **no-decrypt**[復号なし] を選択します。
タイプ	ドロップダウンリストから復号化するトラフィックのタイプを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **SSL Forward Proxy**[SSL フォワード プロキシ] – ポリシーで外部サーバーへのクライアント トラフィックを復号化するように指定します。 • **SSH Proxy**[SSH プロキシ] – ポリシーで SSH トラフィックを復号化するように指定します。このオプションでは、ssh-tunnel App-ID を指定してポリシーの SSH トンネリングを制御できます。 • **SSL Inbound Inspection**[SSL インバウンド インスペクション] – ポリシーで SSL 着信検証トラフィックを復号化するように指定します。
復号化プロファイル	ポリシールールに復号化プロファイルを適用し、トラフィックの特定の要素のブロックとコントロールを行います。復号化プロファイルの作成については、Objects > Decryption Profile [オブジェクト > 復号化プロファイル]を参照してください。

© 2019 Palo Alto Networks, Inc.

Policies（ポリシー）> Tunnel Inspection（トンネル検査）

以下のクリアテキスト トンネル プロトコルのトラフィック コンテンツを検査するようにファイアウォールを設定できます。

- Generic Routing Encapsulation（GRE）
- General Packet Radio Service（GPRS）Tunneling Protocol for User Data（GTP-U）（GTP をサポートしているファイアウォールでのみサポート）
- 非暗号 IPSec トラフィック（IPSec および転送モードの AH IPSec の NULL 暗号化アルゴリズム）
- 拡張可能な仮想 LAN（VXLAN）

トンネル コンテンツ検査を使用して、これらのタイプのトンネルのトラフィックや、別のクリアテキスト トンネルでネストされたトラフィック（たとえば、GRE トンネル内の Null 暗号化された IPSec）に、セキュリティ、DoS プロテクション、QoS ポリシーを適用できます。

ファイアウォールが検査するパケットのトンネル プロトコルの種類を受信パケット照合時に特定したり、ファイアウォールでのパケットの廃棄または処理の継続の条件を指定したりするトンネル検査ポリシーを作成します。トンネル検査ログとトンネル アクティビティを ACC で表示して、トンネリングされたトラフィックが企業のセキュリティおよび使用ポリシーに沿っていることを確認できます。

ファイアウォールは、イーサネット インターフェイスおよびサブインターフェイス、AE インターフェイス、VLAN インターフェイス、VPN および LSVPN トンネルでのトンネル コンテンツ検査をサポートします。この機能は、レイヤー 3、レイヤー 2、バーチャル ワイヤー、タップ デプロイメントでサポートされています。トンネル コンテンツ検査は、共有ゲートウェイと、仮想システムから仮想システムへの通信で機能します。

知りたい内容	以下を参照
トンネル検査ポリシーを作成する際に使用可能なフィールドは？	トンネル検査ポリシーの構成要素
トンネル検査ログを表示するには？	Log Types and Severity Levels（ログタイプと重大度レベル）
その他の情報をお探しですか？	Tunnel Content Inspection（トンネル コンテンツ検査）

トンネル検査ポリシーの構成要素

トンネル検査ポリシー ルールを追加するには、**Policies**（ポリシー）> **Tunnel Inspection**（トンネル検査）を選択します。ファイアウォールを使用して、クリアテキスト トンネルでネストされたトラフィック（GRE、GTP-U、非暗号化 IPSec、および VXLAN）のコンテンツを検査したり、トンネルコンテンツ検査を活用してこのような種類のトンネルにおけるトラフィックでセキュリティ、DoS プロテクション、QoS ポリシーを適用できます。すべてのファイアウォール モデルは GRE の tunnel content inspection（トンネル コンテンツ検査）および非暗号化 IPSec トンネルをサポートしますが、GTP-U トンネルのトンネル コンテンツ検査をサポートするのは GTP をサポートしているファイアウォールのみです。以下の表で、トンネル検査ポリシーを設定するフィールドについて説明します。

© 2019 Palo Alto Networks, Inc.

トンネル検査ポリシーの構成要素	設定場所	の意味
氏名	一般条項	トンネル検査ポリシーの名前を入力します。最初の文字は英数字で、0 以上の数字、アルファベット文字、アンダースコア、ハイフン、ピリオド、スペースを含めることができます。
の意味		（任意）トンネル検査ポリシーの説明を入力します。
tags		（任意）レポートまたはログのためのタグを入力し、トンネル検査ポリシー対象のパケットを判別できるようにします。
タグに基づいてルールをグループ化		類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag (タグ)**に基づいてルールをグループ化することができます。
監査コメント		ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ		ポリシールールの以前の**Audit Comments (監査コメント)**を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。
送信元ゾーン	送信元	トンネル検査ポリシーを適用するパケットの送信元ゾーンを **Add**（追加）します（デフォルトは **Any**（任意））。
送信元アドレス		（任意）トンネル検査ポリシーを適用するパケットの送信元 IPv4 または IPv6 アドレス、アドレス グループ、または地域アドレス オブジェクトを **Add**（追加）します（デフォルトは **Any**（任意））。
Source User（送信元ユーザー）		（任意）トンネル検査ポリシーを適用するパケットの送信元ユーザーを **Add**（追加）します（デフォルトは **any**（任意））。
Negate		（任意）これらの指定したアドレス以外の任意のアドレスを選択するには、**Negate**（上記以外）を選択します。
宛先ゾーン	宛先	トンネル検査ポリシーを適用するパケットの宛先ゾーンを **Add**（追加）します（デフォルトは **Any**（任意））。
宛先アドレス		（任意）トンネル検査ポリシーを適用するパケットの宛先 IPv4 または IPv6 アドレス、アドレス グループ、または地域アドレス オブジェクトを **Add**（追加）します（デフォルトは **Any**（任意））。
Negate		（任意）これらの指定したアドレス以外の任意のアドレスを選択するには、**Negate**（上記以外）を選択します。

© 2019 Palo Alto Networks, Inc.

トンネル検査ポリシーの構成要素	設定場所	の意味
トンネル プロトコル	検査	ファイアウォールで検査するトンネル プロトコルを **Add**（追加）します。 • **GRE** – ファイアウォールは、トンネルで Generic Route Encapsulation を使用するパケットを検査します。 • **GTP-U** – ファイアウォールは、トンネルで General Packet Radio Service（GPRS）のユーザーデータ用トンネリング プロトコル（GTP-U）を使用するパケットを検査します。 • **Non-encrypted IPSec**（非暗号 **IPSec**）– ファイアウォールは、トンネルで暗号化されていない IPSec（Null 暗号化 IPSec または転送モードの AH IPSec）を使用するパケットを検査します。 • **VXLAN**–ファイアウォールは VXLAN のペイロードを検査し、トンネル内のカプセル化されたコンテンツやアプリケーションを見つけます。 リストからプロトコルを削除するには、プロトコルを選択して **Delete**（削除）します。
最大トンネル検査レベル	**Inspection**（検査）> **Inspect Options**（検査オプション）	ファイアウォールがカプセル化の **One Level**（**1** 段階）（デフォルト）または **Two Levels (Tunnel In Tunnel)**（**2** 段階（トンネル内トンネル））を検査するか指定します。検査は他のレイヤーでのみ行われるため、VXLAN の場合は**One Level (1** レベル**)**を選択します。
最大トンネル検査レベルを超えた場合はパケットをドロップ		（任意）最大トンネル検査レベルの指定値を上回るレベルのカプセル化を含むパケットをドロップします。
トンネル プロトコルが厳密なヘッダーチェックに失敗した場合はパケットをドロップ		（任意）プロトコルの RFC に準拠しないヘッダーを使用しているトンネル プロトコルを含むパケットをドロップします。準拠しないヘッダーは、不審なパケットを示唆します。このオプションにより、ファイアウォールは RFC 2890 に対して GRE ヘッダーを確認します。 *RFC 2890 よりも古い GRE のバージョンを導入しているデバイスで、ファイアウォールが GRE をトンネリングしている場合、このオプションは有効にしないでください。*
トンネル内に不明なプロトコルがある場合はパケットをドロップ		（任意）ファイアウォールが判別できないトンネル内のプロトコルを含むパケットをドロップします。
スキャンされた VXLAN トンネルを送信元に戻す		（任意）このオプションを有効化して、トラフィックを元の VXLAN トンネルのエンドポイント（VTEP）に戻します。例えば、カプセル化されたパケットを送信元の VTEP に戻す場合にこのオプションを使用します。レイヤー 3、

© 2019 Palo Alto Networks, Inc.

トンネル検査ポリシーの構成要素	設定場所	の意味
		レイヤー 3 サブインターフェイス、集約インターフェイス レイヤー 3、VLAN でのみサポートされています。
セキュリティ オプションの有効化	**Inspection**（検査）> **Security Options**（セキュリティ オプション）	（任意）**Enable Security Options**（セキュリティ オプションの有効化）によって、トンネル コンテンツの個別のセキュリティ ポリシー処理用にセキュリティ ゾーンが割り当てられます。内部コンテンツの送信元は、指定した **Tunnel Source Zone**（トンネル送信元ゾーン）に属し、内部コンテンツの宛先は、指定した **Tunnel Destination Zone**（トンネル宛先ゾーン）に属すようになります。 セキュリティ オプションの有効化を行わない場合、デフォルトでは、内部コンテンツの送信元は外部トンネルの送信元と同じゾーンに属し、内部コンテンツの宛先は外部トンネルの宛先と同じゾーンに属します。このため、内部コンテンツの送信元と宛先は、それらの外部トンネルの送信元ゾーンと宛先ゾーンに適用されるセキュリティ ポリシーと同じ管理下に置かれます。
トンネル送信元ゾーン		**Enable Security Options**（セキュリティ オプションの有効化）を実行する場合、 作成したトンネル ゾーンを選択すると、内部コンテンツはポリシー実行の目的でこの送信元ゾーンを使用します。 そうでない場合、デフォルトでは、内部コンテンツの送信元は外部トンネルの送信元と同じゾーンに属し、外部トンネル送信元ゾーンのポリシーも内部コンテンツ送信元ゾーンに適用されます。
トンネル宛先ゾーン		**Enable Security Options**（セキュリティ オプションの有効化）を実行する場合、 作成したトンネル ゾーンを選択すると、内部コンテンツはポリシー実行の目的でこの宛先ゾーンを使用します。 そうでない場合、デフォルトでは、内部コンテンツの宛先は外部トンネルの宛先と同じゾーンに属し、外部トンネル宛先ゾーンのポリシーも内部コンテンツ宛先ゾーンに適用されます。
モニター名	**Inspection (検査) > Monitor Options (監視オプション)** を選択します。	（任意）ログとレポートでトラフィックを監視する目的で、類似するトラフィックをまとめてグループ化するためのモニター名を入力します。
モニター タグ (番号)		（任意）ログとレポート向けに類似するトラフィックをまとめてグループ化するためのタグ番号を入力します（範囲は 1 ~ 16,777,215）。タグ番号はグローバルに定義されます。 このフィールドは、*VXLAN* プロトコルには適用されません。*VXLAN* ログは自動的に *VXLAN* ヘッダーの *VXLAN* ネットワーク識別子（*VNI*）を使用します。

© 2019 Palo Alto Networks, Inc.

トンネル検査ポリシーの構成要素	設定場所	の意味
セッション開始時にログ		（任意）このオプションを選択すると、トンネル検査ポリシーに一致するクリアテキスト トンネル セッションの開始時にログが生成されます。この設定は、セッションに適用されるセキュリティ ポリシー ルールの Log At Session Start（セッション開始時にログ）設定よりも優先されます。 トンネル ログはトラフィック ログとは別に保存されます。外部トンネル セッション（GRE、非暗号化 IPSec、または GTP-U）の情報はトンネル ログに保存され、内部トラフィック フローはトラフィック ログに保存されます。別々に保存することにより、ACC とレポート機能を使用してトンネルのアクティビティ（内部コンテンツのアクティビティと対照）を簡単にレポートできます。 トンネル ログのベストプラクティスは、*Log at Session Start*（セッション開始時にログ）を記録し、*Log at Session End*（セッション終了時にログ）を記録することです。これは、ログを記録するためにトンネルが非常に長寿命になる可能性があるためです。たとえば、*GRE* トンネルはルーターの起動時に起動し、ルーターが再起動されるまで終了しません。セッション開始時にログを選択しないと、*ACC* にアクティブな *GRE* トンネルが存在することはありません。
セッション終了時にログ		（任意）このオプションを選択すると、トンネル検査ポリシーに一致するクリアテキスト トンネル セッションの終了時にログがキャプチャされます。この設定は、セッションに適用されるセキュリティ ポリシー ルールの Log At Session End（セッション終了時にログ）設定よりも優先されます。
ログ転送		（任意）トンネル検査ログを転送する場所を指定するには、ドロップダウンから Log Forwarding（ログの転送）プロファイルを選択します。（この設定は、トラフィック ログに適用されるセキュリティ ポリシール ールの Log Forwarding（ログ転送）設定とは異なります）。
氏名	トンネル **ID** デフォルト設定では、VXLAN ID を設定していない場合にすべてのトラフィックが検査されます。 VXLAN ID を設定している場合、これを一致条件として使用	（任意）最初の文字は英数字で、0 以上の数字、アルファベット文字、アンダースコア、ハイフン、ピリオド、スペースを含めることができる名前。**Name** (名前)はグループ化している VNI を示します。名前は便宜上のものであり、ログ、監視、レポートの要素にはなりません。
VXLAN ID（VNI）		（任意）単一の VNI、コンマ区切りの VNI のリスト、最大 1,600 万件の範囲の VNI（ハイフンを区切り文字として使用）、あるいはこれらを組み合わせて入力します。以下がその例です。

© 2019 Palo Alto Networks, Inc.

トンネル検査ポリシーの構成要素	設定場所	の意味
	してトラフィックの検査を特定の VNI に限定することができます。	1-54,1024,1677011-1677038,94 ポリシー毎の VXLAN ID の上限数は 4,096 件です。設定メモリを保持する場合、可能な限り範囲を使用してください。

© 2019 Palo Alto Networks, Inc.

Policies > Application Override [ポリシー > アプリケーション オーバーライド]

ファイアウォールによるネットワーク トラフィックのアプリケーション分類方法を変更するには、アプリケーション オーバーライド ポリシーを指定します。たとえば、カスタム アプリケーションのいずれかを制御する場合、アプリケーション オーバーライド ポリシー ルールを使用すると、ゾーン、送信元アドレスと宛先アドレス、ポート、およびプロトコルに従って、そのアプリケーションのトラフィックを識別できます。「unknown」として分類されるネットワーク アプリケーションがある場合、そのアプリケーションの新しい定義を作成できます (アプリケーションの定義を参照)。

ファイアウォールが *App-ID* を使用してアプリケーションを特定したり、脅威に対してレイヤー 7 検査を実行したりすることができなくなるため、可能な場合はアプリケーション オーバーライド ポリシーを使用しないでください。内部の専有アプリケーションをサポートする場合、アプリケーション シグネチャを含むカスタム アプリケーションを作成し、ファイアウォールがレイヤー 7 検査を実行してアプリケーション トラフィックの脅威をスキャンできるようにすることが推奨されます。商用アプリケーションが *App-ID* を持っていない場合は、新しい App-ID をリクエストしてください。公開アプリケーション定義 (デフォルトのポートあるいはシグネチャ) が変化し、ファイアウォールがアプリケーションを正しく識別できなくなる場合は、サポートチケットを作成して *Palo Alto Networks* が定義を更新できるようにしてください。その間、ファイアウォールがトラフィックのレイヤー 7 検査を実行し続けられるよう、カスタム アプリケーションを作成します。

セキュリティ ポリシーと同様に、必要に応じて全般的または個別のアプリケーション オーバーライド ポリシーを使用できます。ポリシー ルールと受信トラフィックは順番に照合されるため、より個別のルールの方が全般的なルールよりも上に来るようにする必要があります。

PAN-OS の App-ID エンジンは、ネットワーク トラフィックのアプリケーション特有のコンテンツを識別してトラフィックを分類します。このため、カスタム アプリケーション定義では、単純にポート番号を使用してアプリケーションを識別することができません。アプリケーション定義には、トラフィック (送信元ゾーン、送信元 IP アドレス、宛先ゾーン、および宛先 IP アドレスごとに制限されます) も含まれている必要があります。

アプリケーション オーバーライドを指定するカスタム アプリケーションを作成するには、以下の手順を実行します。

- カスタム アプリケーションを作成します (アプリケーションの定義を参照)。アプリケーションの使用目的がアプリケーション オーバーライド ルールのみである場合、アプリケーションのシグネチャを指定する必要はありません。
- カスタム アプリケーションの起動時に指定されるアプリケーション オーバーライド ポリシーを定義します。通常ポリシーには、カスタム アプリケーションを実行しているサーバーの IP アドレスと、制限された送信元 IP アドレスのセットまたは送信元ゾーンが含まれています。

以下の表を使用して、アプリケーション オーバーライド ルールを設定します。

- アプリケーション オーバーライドの General (全般) タブ
- アプリケーション オーバーライドの Source (送信元) タブ
- アプリケーション オーバーライドの Destination (宛先) タブ
- アプリケーション オーバーライドの Protocol/Application (プロトコル/アプリケーション) タブ

その他の情報をお探しですか？

「Use Application Objects in Policy (ポリシーでのアプリケーション オブジェクトの使用) 」を参照してください。

© 2019 Palo Alto Networks, Inc.

アプリケーション オーバーライドの General（全般）タブ

General[全般] タブを使用して、アプリケーション オーバーライド ポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングにも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを **Add**（追加）して指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復号」と「復号なし」というタグを付けたり、特定のデータ センターに関するポリシーにその場所の名前を使用したりできます。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag (タグ)**に基づいてルールをグループ化することを選択できます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments (監査コメント)**を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

アプリケーション オーバーライドの Source（送信元）タブ

Source[送信元]タブを使用して、送信元ゾーンまたは送信元アドレスを定義し、送信元から受信するトラフィックにアプリケーション オーバーライド ポリシーを適用するように設定します。

項目	の意味
送信元ゾーン	送信元ゾーンを **Add**（追加）します（デフォルトは **any**（任意））。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、 Network > Zones［ネットワーク > ゾーン］を参照してください。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
送信元アドレス	送信元アドレス、アドレス グループ、または地域を **Add** (追加) します (デフォルトは **any** (任意))。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**[アドレス]、**Adress Group**[アドレスグループ]、または**Region**[地域]をクリックして設定を行います。 **Negate**[上記以外]を選択すると、設定したアドレス以外の任意のアドレスを指定したことになります。

アプリケーション オーバーライドの Destination (宛先) タブ

Destination (宛先)タブを使用して、宛先ゾーンまたは宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
宛先ゾーン	**Add**[追加] をクリックして宛先ゾーンを選択します (デフォルトは any)。ゾーンは同じタイプ (Layer 2 [レイヤー 2]、Layer 3 [レイヤー 3]、virtual wire [バーチャル ワイヤー]) である必要があります。新しいゾーンを定義する手順については、 Network > Zones [ネットワーク > ゾーン] を参照してください。 複数のゾーンを使用して管理を簡略化できます。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
宛先アドレス	**Add**[追加] をクリックして宛先アドレス、アドレス グループ、または地域を追加します (デフォルトは any)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address**[アドレス]、**Adress Group**[アドレスグループ]、または**Region**[地域]をクリックして設定を行います。 **Negate**[上記以外]を選択すると、設定したアドレス以外の任意のアドレスを指定したことになります。

アプリケーション オーバーライドの Protocol/Application (プロトコル/アプリケーション) タブ

Protocol/Application[プロトコル/アプリケーション] タブを使用して、プロトコル (TCPまたはUDP)、ポート、アプリケーションを定義して、ポリシーの一致条件にするアプリケーションの属性を詳細に指定できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
PROTOCOL	アプリケーション オーバーライドを許可するプロトコル（**TCP** または **UDP**）を選択します。
ポート	指定した宛先アドレスのポート番号 (0 ~ 65535) またはポート番号の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたはポートの範囲はコンマで区切ります。
Application [アプリケーション]	前述のルール基準に一致するトラフィック フローのオーバーライド アプリケーションを選択します。カスタム アプリケーションをオーバーライドするときに実行される脅威検査はありません。この例外は、脅威検査をサポートする事前に定義されたアプリケーションにオーバーライドする場合です。 新しいアプリケーションを定義する方法については、「Objects（オブジェクト）> Applications（アプリケーション）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Policies（ポリシー） > Authentication（認証）

認証ポリシーを使用すると、エンド ユーザーがネットワーク リソースにアクセスする前に、エンドユーザーの認証を行うことができます。

知りたい内容	以下を参照
認証ルールを作成する際に使用可能なフィールドは？	認証ポリシー ルールの構成要素
Web インターフェイスを使用して認証ポリシーを管理するには？	認証ポリシーの作成と管理 Panorama については、「ポリシールールの移動またはコピー」を参照してください。
その他の情報をお探しですか？	Authentication Policy（認証ポリシー）

認証ポリシー ルールの構成要素

ユーザーがリソースを要求したとき（たとえば、Web ページへのアクセス時）、ファイアウォールが必ず認証ポリシーを評価します。一致するポリシー ルールに基づいて、ファイアウォールは、ログインとパスワード、音声、SMS、プッシュ、またはワンタイム パスワード（OTP）認証のように、異なる要素（タイプ）のチャレンジに対応するようにユーザーに求めます。ユーザーがすべての要素に対応すると、ファイアウォールはセキュリティ ポリシーを評価して（「Policies（ポリシー） > Security（セキュリティ）」を参照）、リソースへのアクセスを許可するかどうかを判断します。

ユーザーが *Web* ベースでないリソース（プリンタなど）に内部またはトンネル モードの GlobalProtect™ ゲートウェイ経由でアクセスする場合、ファイアウォールは認証を求めません。代わりに、接続エラー メッセージが表示されます。これらのリソースにユーザーがアクセスできるようにするには、認証ポータルをセットアップして、接続エラーが表示された場合はポータルにアクセスするようにユーザーに伝えてください。認証ポータルのセットアップについては、御社の *IT* 部門に相談してください。

以下の表で、認証ポリシー ルールの構成要素について説明します。ルールを追加する前に、「認証ポリシーの作成と管理」に記載されている必要条件を満たしてください。

認証ルールの構成要素	設定場所	の意味
ルール番号	該当なし	各ルールは自動的に付番され、ルールを移動すると順番も変更されます。特定のフィルタに一致するルールをフィルタリングすると、**Policies**（ポリシー） > **Authentication**（認証）ページに、各ルールと、ルールベースのルール全体の中で番号が振られ、評価順における順番が一覧表示されます。詳細は、ルールの並びと評価順の説明を参照してください。

© 2019 Palo Alto Networks, Inc.

認証ルールの構成要素	設定場所	の意味
氏名	一般条項	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味		ルールの説明を入力します (最大 1024 文字)。
タグ		ルールのソートおよびフィルタリングのためのタグを選択します（「Objects（オブジェクト）> Tags（タグ）」を参照）。
タグに基づいてルールをグループ化		類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag** (タグ)に基づいてルールをグループ化することができます。
監査コメント		ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ		ポリシールールの以前の**Audit Comments** (監査コメント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。
送信元ゾーン	送信元	ゾーンを **Add**（追加）して、指定したゾーンのインターフェイスからのトラフィックにのみルールを適用します（デフォルトは **any**（任意））。 新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。
送信元アドレス		アドレスまたはアドレス グループを **Add**（追加）して、指定した送信元から発生したトラフィックにのみルールを適用します（デフォルトは **any**（任意））。 **Negate**（上記以外）を選択すると、指定したアドレス以外の任意のアドレスを指定したことになります。 新しいアドレスやアドレス グループを定義する手順については、「Objects（オブジェクト）> Addresses（アドレス）」、および「Objects（オブジェクト）> Address Groups（アドレス グループ）」を参照してください。
Source User（送信元ユーザー）	感染	ルールを適用する送信元ユーザーまたはユーザー グループを選択します。

© 2019 Palo Alto Networks, Inc.

認証ルールの構成要素	設定場所	の意味
		• **any**（任意）– 送信元ユーザーに関係なく任意のトラフィックが含まれます。 • **pre-logon**（ログオン前）– ユーザーはクライアント システムにログインしていないが、ユーザーのクライアント システムは GlobalProtect の pre-logon 機能 でネットワークに接続している状態のリモート ユーザーが含まれます。 • **known-user**（既知のユーザー）– ルールによって認証が呼び出される以前に、ファイアウォールで IP アドレスとユーザー名のマッピングが完了しているすべてのユーザーが含まれます。 • **unknown**（未知）– ファイアウォールで IP アドレスとユーザー名のマッピングが行われていないすべてのユーザーが含まれます。ルールによって認証が呼び出された後、ユーザーが入力したユーザー名に基づいて、ファイアウォールは未知のユーザーのユーザー マッピングを作成します。 • **Select**（対象指定）– Source User（送信元ユーザー）リストに **Add**（追加）したユーザーおよびユーザー グループのみが含まれます。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。
送信元 HIP プロファイル		ホスト情報プロファイル (HIP) を**Add** (追加) すると、最新のセキュリティ パッチやアンチウイルス定義があるかなどのエンド ホストのセキュリティ状態に関する情報を収集できます。詳細や新しい HIP を定義する手順については、「Objects（オブジェクト）> GlobalProtect > HIP Profiles（HIP プロファイル）」を参照してください。
宛先ゾーン	宛先	ゾーンを **Add**（追加）して、指定したゾーンのインターフェイスに向かうトラフィックにのみルールを適用します（デフォルトは **any**（任意））。新しいゾーンを定義する手順については、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。
宛先アドレス		アドレスまたはアドレス グループを **Add**（追加）して、指定した宛先にのみルールを適用します（デフォルトは **any**（任意））。 **Negate**（上記以外）を選択すると、指定したアドレス以外の任意のアドレスを指定したことになります。 新しいアドレスやアドレス グループを定義する手順については、「Objects（オブジェクト）> Addresses（アド

© 2019 Palo Alto Networks, Inc.

認証ルールの構成要素	設定場所	の意味
		レス）」、および「Objects（オブジェクト）> Address Groups（アドレス グループ）」を参照してください。
サービス	サービス/URL カテゴリ	以下のオプションを選択して、特定の TCP および UDP ポート番号のサービスにのみルールを適用します。 • **any**（任意）— すべてのポート、およびプロトコルのサービスを指定します。 • **default**（デフォルト）— Palo Alto Networks が定義するデフォルト ポートのサービスのみを指定します。 • **Select**（対象指定）— サービスまたはサービス グループを **Add**（追加）できるようにします。新しいサービスやサービス グループを作成する手順については、「Objects（オブジェクト）> Services（サービス）」、および「Objects（オブジェクト）> Service Groups（サービス グループ）」を参照してください。 デフォルトでは*service-http*が選択されています。キャプティブポータル用に認証ポリシーを使用する場合は*service-https*も有効化し、ファイアウォールがすべての *Web* トラフィックについてユーザー対 *IP* アドレスのマッピングを必ず学習するようにしてください。
URL カテゴリ		ルールを適用する URL カテゴリを選択します。 • URL カテゴリに関係なくすべてのトラフィックを指定するには、**any**（任意）を選択します。 • カテゴリを **Add**（追加）します。カスタム カテゴリを定義する手順については、「Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> URL Category（URL カテゴリ）」を参照してください。
認証の実施	操作	ファイアウォールがユーザーを認証するために使用する方式（キャプティブ ポータルまたはブラウザ チャレンジなど）と認証プロファイルを指定するための認証の実施オブジェクトを選択します（Objects（オブジェクト）> Authentication（認証））。認証プロファイルは、ユーザーが 1 つのチャレンジに対応するか、多要素認証に対応するかを定義します（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。事前定義済みか、カスタムの認証の実施オブジェクトを選択できます。 ホストやサーバーをキャプティブ ポータル ポリシーから除外しなければならない場合は、*no-captive-portal*を*Authentication Enforcement (*認証の適用*)*として指定している認証プロファイルにそれらを追加します。しかし、ファイアウォールがユーザー対 *IP* アドレスのマッピングを学習する際

© 2019 Palo Alto Networks, Inc.

認証ルールの構成要素	設定場所	の意味
		はキャプティブ ポータル ポリシーが役立つため、可能な限りそれを使用してください。
タイムアウト		ユーザーがリソースに繰り返しアクセスする場合に、ファイアウォールが 1 回だけユーザーに認証を求める間隔を分単位で指定すると（デフォルトは 60）、ユーザーのワークフローの妨げとなる認証チャレンジの頻度を減らすことができます。 **Authentication Enforcement**（認証の実施）オブジェクトで多要素認証を指定する場合、ユーザーは各要素につき認証を 1 回行う必要があります。ファイアウォールはタイムスタンプを記録して、要素の有効期限のタイムアウト時にのみ、チャレンジを再発行します。タイムスタンプを他のファイアウォールに再配信すると、最初にユーザーにアクセスを許可するファイアウォールと、後にそのユーザーのアクセスを制御するファイアウォールが異なる場合も、タイムアウトを適用できます。 *Timeout (タイムアウト)*は、強固なセキュリティ（認証のプロンプトを表示する間隔が短い）とユーザーエクスペリエンス（認証のプロンプトを表示する間隔が長い）の間のトレードオフになります。データセンターなどの重要なシステムやセンシティブな領域へのアクセスが対象である場合、できるだけ頻繁に認証を行うのが最適な選択になるでしょう。ネットワークの境界やユーザーエクスペリエンスが重要なビジネスの場合は、認証の頻度を減らすことが最適な選択になるでしょう。 境界にあるリソースの場合は値を *480* 分（*8* 時間）に設定し、データセンターのリソースや重要なシステムの場合は *60* 分などの小さな値を設定してセキュリティを強化してください。必要に応じて値を監視して調整します。
ログ認証タイムアウト		認証要素に関連付けられているタイムアウトが期限切れになるたびに、ファイアウォールで認証ログを生成する場合は、このオプションを選択します（デフォルトでは無効）。このオプションを有効にすると、アクセス問題のトラブルシューティングに利用できるデータが増えます。相関オブジェクトとともに認証ログを使用して、ネットワーク上の不審なアクティビティを特定できます（総当たり攻撃など）。

© 2019 Palo Alto Networks, Inc.

認証ルールの構成要素	設定場所	の意味
		このオプションを有効にするとログ トラフィックが増えます。
ログ転送		ファイアウォールから Panorama または Syslog サーバーのような外部サービスに認証ログを転送する場合は、ログ転送プロファイルを選択します（「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照）。

認証ポリシーの作成と管理

認証ポリシー ルールの作成と管理を行うには、**Policies**（ポリシー）> **Authentication**（認証）ページを選択します。

タスク	の意味
コンテキストの	次の前提事項を実行してから、認証ポリシー ルールを作成してください。 □ User-ID™ キャプティブ ポータル設定を構成します（「Device（デバイス）> User Identification（User-ID）> Captive Portal Settings（キャプティブ ポータルの設定）」を参照）。ファイアウォールではキャプティブ ポータルが使用されて、認証ルールによって要求される、最初の認証要素が表示されます。Captive Portal（キャプティブ ポータル）では、ファイアウォールは認証 Timeout（タイムアウト）期間に関連付けられたタイム スタンプを記録し、ユーザー マッピングを更新することもできます。 □ ファイアウォールがユーザー認証を行うサービスにアクセスする方法を指定するサーバー プロファイルを設定します（「Device（デバイス）> Server Profiles（サーバー プロファイル）」を参照）。 □ 認証設定を指定する認証プロファイルにサーバー プロファイルを割り当てます（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。 □ 認証方法を指定する認証実施オブジェクトに認証プロファイルを割り当てます（「Objects（オブジェクト）> Authentication（認証）」を参照）。 ルールを作成するには、次のいずれかのステップを実行してから、「認証ポリシー ルールの構成要素」で説明するフィールドに情報を入力します。 • [追加] をクリックします。 • 新しいルールのベースになるルールを選択し、**Clone Rule**（ルールのコピー）をクリックします。ファイアウォールでは、コピーしたルールに <rulename># という名前が付き、選択したルールの下に挿入されます。# は次に使用可能な整数で、これによりルール名が一意になり、コピーしたルール用の新しい UUID が生成されます。詳細は、「ポリシー ルールの移動またはコピー」を参照してください。
変更	ルールを変更するには、ルール名をクリックし、「認証ポリシー ルールの構成要素」で説明するフィールドを編集します。 ファイアウォールがルールを *Panorama* から受信すると、ルールは読み取り専用になります。ルールは *Panorama* のみで編集可能です。
移動	ファイアウォールでは、トラフィックが照合されるとき、ルールが **Policies**（ポリシー）> **Authentication**（認証）ページでリストされている順序で上から下に評価されます。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	評価順序を変更するには、ルールを選択して、**Move Up**（上へ）、**Move Down**（下へ）、**Move Top**（最上部へ）、**Move Bottom**（最下部へ）のうちいずれかを選択します。詳細は、「ポリシー ルールの移動またはコピー」を参照してください。
削除します。	既存のルールを削除するには、ルールを選択して **Delete**（削除）を選択します。
有効化/無効化	ルールを無効化するには、ルールを選択して **Disable**（無効化）を選択します。無効化したルールを再び有効化するには、ルールを選択して **Enable**（有効化）を選択します。
使用されていないルールの強調表示	ファイアウォールの前回再起動時から、トラフィックを照合していないルールを特定する場合は、**Highlight Unused Rules**（未使用のルールをハイライト表示）を選択します。ハイライト表示すると、使用されていないルールを無効化するのか削除するのかを判断できるようになります。このページでは、使用されていないルールは黄色い網掛けでハイライト表示されます。
ルールのプレビュー（Panoramaのみ）	**Preview Rules**（ルールのプレビュー）をクリックして、ルールを管理対象ファイアウォールにプッシュする前にルールのリストを表示することができます。このページでは、各ルールベース内で、デバイス グループ（および管理対象ファイアウォール）ごとにルール階層が視覚的に区別されており、多くのルールに目を通しやすくなっています。

© 2019 Palo Alto Networks, Inc.

Policies > DoS Protection [ポリシー > DoS プロテクション]

DoS プロテクション ポリシーを使用すると、送信元インターフェイス、ゾーン、アドレス、ユーザーや、宛先インターフェイス、ゾーン、ユーザーに一致するパケットの拒否または許可を指定して、個々の重要なリソースを DoS 攻撃から守ることができます。

また、保護アクションを選択し、DoS プロファイルを指定できます。プロファイルにはしきい値（1 秒あたりのセッションまたはパケット数）を設定して、アラームのトリガーや保護アクションのアクティベートを適用したり、割合の上限を指定してそれを超えた場合にすべての新しい接続をドロップしたりできます。これにより、インターフェイス、ゾーン、アドレス、国のセッション数を、セッション総数、送信元 IP アドレスおよび宛先 IP アドレスに基づいて制御できます。たとえば、特定のアドレスまたはアドレス グループと送受信されるトラフィック、特定のユーザーから受信するトラフィック、特定のサービスに使用するトラフィックを制御できます。

ファイアウォールが DoS プロテクション ポリシー ルールを実施した後、ファイアウォールが最も効率的な方法でリソースを使用することをセキュリティ ポリシー ルールが確認します。DoS プロテクション ポリシー ルールがパケットを拒否した場合、そのパケットがセキュリティ ポリシー ルールに到達することはありません。

以下の表では、DoS プロテクション ポリシー設定について記載しています。

- DoS プロテクションの General（全般）タブ
- DoS プロテクションの Source（送信元）タブ
- DoS プロテクションの Destination（宛先）タブ
- DoS プロテクションの Option/Protection（オプション/防御）タブ

その他の情報をお探しですか？

「DoS Protection Profiles（DoS プロテクション プロファイル）」、および「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> DoS Protection（DoS プロテクション）」を参照してください。

DoS プロテクションの General（全般）タブ

- **[Policies]** > **DoS Protection[DoS** プロテクション**]** > **General**（全般）

General（全般）タブを選択して、DoS プロテクション ポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングを行うこともできます。

項目	の意味
氏名	DoS プロテクション ポリシー ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
tags	ポリシーにタグを付ける場合、タグを **Add**（追加）して指定します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。タグは、多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。たとえば、特定のセキュリティ ポリシーに DMZ へのインバウンドのタグを付けたり、復号ポリシーに「復号」や「復号なし」というタグを付けたり、特定のデータ センターに関するポリシーにその場所の名前を使用したりできます。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag (タグ)**に基づいてルールをグループ化することができます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments (監査コメント)**を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

DoS プロテクションの Source（送信元）タブ

Source（送信元）タブを選択して、送信元インターフェイスまたは送信元ゾーン、および必要に応じて送信元アドレスと送信元ユーザーを定義し、受信トラフィックに DoS ポリシー ルールを適用するように設定します。

項目	の意味
タイプ	DoS プロテクション ポリシー ルールを適用する送信元のタイプを選択します。 • **Interface**（インターフェイス） – 指定されたインターフェイスまたはインターフェイス グループから送信されるトラフィックにルールを適用します。 • **Zone**（ゾーン） – 指定されたゾーンのインターフェイスから送信されるトラフィックにルールを適用します。 **Add**（追加）をクリックして、複数のインターフェイスまたはゾーンを選択します。
送信元アドレス	**Any**（すべて）または **Add**（追加）を選択し、DoS プロテクション ポリシー ルールを適用する 1 つ以上の送信元アドレスを指定します。 （任意）指定したアドレス以外の任意のアドレスにルールを適用するには、**Negate**（上記以外）を選択します。
Source User（送信元ユーザー）	DoS プロテクション ポリシー ルールを適用する 1 つ以上の送信元ユーザーを指定します。 • **any**（すべて） – 送信元ユーザーに関係なくパケットが含まれます。 • **pre-logon**（ログイン前） – GlobalProtect を使用してネットワークに接続しており、自分のシステムへのログインはしていないリモート ユーザーからのパケットが含まれます。GlobalProtect アプリのポータルに **pre-logon**（ログオン前）が設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成できるのに加えて、ユーザーが直接ログインしていなくても、ユーザーのマシンは完全にログインしているかのようにドメインで認証されます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **known-user**（既知のユーザー）– 認証されたすべてのユーザー（ユーザー データがマッピングされた IP アドレス）が含まれます。このオプションは、ドメインの「ドメイン ユーザー」グループに相当します。 • **unknown**[未知] – 認証されていないすべてのユーザー (ユーザーにマップされていない IP アドレス) が含まれます。たとえば、**unknown**（未知）はゲスト レベルのアクセスに使用できます。これらのユーザーは、ネットワーク上の IP アドレスを持っていますが、ドメインに認証されず、ファイアウォール上に IP アドレス対ユーザー名のマッピング情報がないためです。 • **Select**（選択）– このウィンドウで指定したユーザーが含まれます。たとえば、1 人のユーザー、個々のユーザーのリスト、あるいはグループを選択したり、手動でユーザーを追加したりできます。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。

DoS プロテクションの Destination（宛先）タブ

Destination（宛先）タブを選択して、宛先ゾーンまたは宛先インターフェイスおよび宛先アドレスを定義し、宛先へのトラフィックにポリシーを適用するように設定します。

項目	の意味
タイプ	DoS プロテクション ポリシー ルールを適用する宛先のタイプを選択します。 • **Interface**（インターフェイス）– 指定されたインターフェイスまたはインターフェイス グループに送信されるパケットにルールを適用します。**Add**（追加）をクリックして、1 つ以上のインターフェイスを選択します。 • **Zone**（ゾーン）– 指定されたゾーンのインターフェイスに送信されるパケットにルールを適用します。**Add**（追加）をクリックして、1 つ以上のゾーンを選択します。
宛先アドレス	**Any**（すべて）または **Add**（追加）を選択し、DoS プロテクション ポリシー ルールを適用する 1 つ以上の宛先アドレスを指定します。 （任意）指定したアドレス以外の任意のアドレスにルールを適用するには、**Negate**（上記以外）を選択します。

DoS プロテクションの Option/Protection（オプション/防御）タブ

Option/Protection（オプション/防御）タブを選択して、DoS プロテクション ポリシー ルールのオプションを設定します。たとえば、ルールを適用するサービスのタイプ、ルールに一致するパケットに対して実行するアクション、一致するトラフィックのログ転送をトリガーするかどうかなどを設定できます。ルールがアクティブになるスケジュールを定義できます。

また、しきい値レートを決定する aggregate（集約）DoS プロテクション プロファイルや classified（分類）DoS プロテクション プロファイルを選択することもできます。このしきい値レートを超えると、ファ

© 2019 Palo Alto Networks, Inc.

イアウォールはアラームのトリガーなどの防御アクションを実行したり、ランダム早期ドロップなどのアクションをアクティベーションしたり、しきい値レートの上限を超えるパケットをドロップしたりします。

項目	の意味
サービス	**Add**（追加）をクリックし、DoS プロテクション ポリシーを適用する 1 つ以上のサービスを選択します。デフォルトは **Any**（すべて）のサービスです。例えば、DoS ポリシーが Web サーバーを保護する場合、HTTP、HTTPS、その他の Web アプリケーション用の適切なサービス ポートを指定します。 重要なサーバーの場合は *DoS* 保護ルールを別途作成し、目標を定めた攻撃を防ぐために使用していないサービス ポートを保護します。
操作	DoS プロテクション ポリシー ルールに一致するパケットに対してファイアウォールが実行するアクションを選択します。 • **Deny**（拒否）– ルールに一致するすべてのパケットをドロップします。 • **Allow**（許可）– ルールに一致するすべてのパケットを許可します。 • **Protect (保護)**–指定した DoS 保護プロファイルで指定されている保護をルールにマッチするパケットに適用します。ルールに一致するパケットは、DoS プロテクション プロファイルのしきい値レートに対してカウントされ、最大レートを超えたときにアラームのトリガー、別のアクションのアクティベーション、パケット ドロップのトリガーが行われます。 *DoS* 保護を適用する目的は *DoS* 攻撃を防ぐことであるため、基本的に*Protect (*保護*)*を使用する必要があります。*Deny (*拒否*)*は *DoS* トラフィックと共に正当なトラフィックをドロップし、また*Allow (*許可*)*は *DoS* 攻撃を防ぐことができません。グループ内で例外を設ける場合のみ、*Deny (*拒否*)*や*Allow (*許可*)*を使用するようにしてください。例えば、グループの大抵のメンバーから来るトラフィックを拒否しつつそのトラフィックの一部だけを許可したり、グループの大抵のメンバーから来るトラフィックを許可しつつそのトラフィックの一部だけを拒否したりすることができます。
スケジュール	DoS プロテクション ポリシー ルールが適用されるスケジュールを指定します。デフォルト設定の **None**（なし）はスケジュールがないことを示し、ポリシーは常に適用されます。 または、スケジュールを選択したり、新しいスケジュールを作成したりして、DoS プロテクション ポリシー ルールが適用されるタイミングを制御します。スケジュールの **Name**（名前）を入力します。マルチ仮想システム ファイアウォールの各仮想システムでこのスケジュールを共有するには、**Shared**（共有）を選択します。**Recurrence**（繰り返し）に **Daily**（毎日）、**Weekly**（毎週）、または **Non-recurring**（**1** 回限り）を選択します。**Start Time**（開始時間）と **End Time**（終了時間）を 24 時間ベースの「時:分」の形式で追加します。
ログ転送	一致するトラフィックの脅威ログ エントリの外部サービス（Syslog サーバー、Panorama など）への転送をトリガーする場合、ログ転送プロファイルを選択するか、**Profile**（プロファイル）をクリックして新しいプロファイルを作成します。 ファイアウォールはルール内のアクションにマッチするトラフィックについてのみ、ログを記録してトラフィックを転送します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	管理を簡単にするために、*DoS* ログを他の脅威ログと分けて、管理者（メールで）およびログ サーバーの両方に直接転送します。
集約（Aggregate）	集約 DoS 保護プロファイルは、DoS 保護ルールで指定されたデバイスの複合グループに適用されるしきい値を設定してそれらのサーバーグループを保護します。例えば、Alarm Rate (アラーム レート) のしきい値を 10,000 CPS にすると、グループ全体に向かう新しい CPS の合計が 10,000 CPS を超えるにファイアウォールがアラーム メッセージを発動させます。 しきい値レートを指定する Aggregate（集約）DoS プロテクション プロファイルを選択します。このしきい値レートに基づいて、受信接続/秒によるアラームのトリガー、アクションのアクティベーション、最大レートの超過が発生します。すべての受信接続（集約）が、Aggregate（集約）DoS プロテクション プロファイルで指定されたしきい値に対してカウントされます。 Aggregate（集約）プロファイル設定が **None**（なし）の場合、集約トラフィックのしきい値設定がないことを意味します。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> DoS Protection（DoS プロテクション）」を参照してください。
分類化（Classified）	分類化 DoS 保護プロファイルは、DoS 保護ルールで指定された個々のデバイスに適用されるしきい値を設定して個々の、あるいは小規模なグループの重要なサーバーを保護します。例えば、Alarm Rate (アラーム レート) のしきい値を 10,000 CPS にすると、ルールで指定された個々のいずれかのサーバーに向かう新しい CPS の合計が 10,000 CPS を超えるにファイアウォールがアラーム メッセージを発動させます。 このオプションを選択し、以下を指定します。 • **Profile**（プロファイル）– このルールに適用する Classified（分類）DoS プロテクション プロファイルを選択します。 • **Address**（アドレス）– **source-ip-only**（送信元 **IP** のみ）、**destination-ip-only**（宛先 **IP** のみ）、**src-dest-ip-both**（送信元 **IP** と宛先 **IP** の両方）のうち、どれに一致したときに受信接続がプロファイルのしきい値に対してカウントされるのかを指定します。 *src-dest-ip-both*カウンターを追跡する場合、ファイアウォールは送信元 *IP* あるいは宛先 *IP* カウンターだけを追跡する場合よりも多くのリソースを消費します。 Classified（分類）DoS プロテクション プロファイルを指定した場合、送信元 IP アドレス、宛先 IP アドレス、または送信元 IP アドレスと宛先 IP アドレスのペアに一致する受信接続のみが、プロファイルで指定したしきい値に対してカウントされます。たとえば、**Max Rate**（最大レート）が 100 cps である Classified（分類）DoS プロテクション プロファイルを指定し、ルールの **Address**（アドレス）設定に **source-ip-only**（送信元 **IP** のみ）を指定できます。この特定の送信元 IP アドレスの接続が 1 秒あたり 100 に制限されます。 ファイアウォールがすべての *IP* アドレスの候補のカウンターを保存することはできないため、インターネットに接続されたゾーン用に*source-ip-only*や*src-dest-ip-both*を使用しないでください。境界のゾーンでは*destination-ip-only*を使用します。 個々の重要なデバイスを保護する場合は*destination-ip-only*を使用します。 インターネットに接続されていないゾーンで疑わしいホストを監視する場合は*source-ip-only*および*Alarm (アラーム)*しきい値を使用します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> DoS Protection（DoS プロテクション）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Policies > SD-WAN [ポリシー > SD-WAN]

アプリケーションと、指定したジッター、レイテンシ–、およびパケット損失率の正常性メトリックを指定するパス品質プロファイルを含む、一致条件を含む SD-WAN ポリシー ルールを作成します。機密性の高い重要なアプリケーションの送信元と宛先の間のパスが低下した場合、SD-WAN ポリシー ルールは、関連付けられたトラフィック分散プロファイルを使用して、アプリケーションの新しい最適なパスを動的に選択します。SD-WAN ポリシー ルールは、Panorama がルールをプッシュする対象デバイスも指定します。

- SD-WAN General (全般) タブ
- Source (送信元) タブ
- Destination (宛先) タブ
- SD-WAN Application/Service (アプリケーション/サービス) タブ
- SD-WAN Path Selection (パス選択) タブ
- (Panorama のみ) SD-WAN Target (ターゲット) タブ

SD-WAN General (全般) タブ

- **Policies (ポリシー) > SD-WAN - > - General (全般)**

General (全般) タブを選択し、 SD-WAN ポリシーの名前と説明を設定します。タグを設定すると、大量のポリシーがある場合に、ポリシーのソートやフィルタリングにも使用できます。

項目	の意味
氏名	ルールを識別する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 63 文字を指定できます。ルール名はファイアウォールおよび Panorama 上で一意でなければなりません。また、デバイス グループとその先祖または子孫デバイス グループ内でも一意でなければなりません。
の意味	ルールの説明を入力します (最大 1024 文字)。
タグ	ポリシーにタグを付ける場合、タグを **Add** (追加) して指定します。 ポリシー タグとは、ポリシーをソートまたはフィルタリングできるキーワードや語句です。多数のポリシーを定義していて、特定のキーワードでタグが付けられたポリシーを表示する場合に役立ちます。例えば、特定の SD-WAN ポリシーに、ルールが適用される特定のハブまたはブランチを特定する一意のタグでタグ付けしたい場合。
タグに基づいてルールをグループ化	類似のポリシールールをグループ化するのに使用するタグを入力します。グループタグを使用すれば、対象のタグに基づいてポリシールール ベースを表示できます。**Tag (タグ)**に基づいてルールをグループ化することを選択できます。
監査コメント	ポリシールールの作成や編集を監査するために使用するコメントを入力します。監査コメントの大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 256 文字を指定できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
監査コメント アーカイブ	ポリシールールの以前の**Audit Comments** (監査コメント)を表示します。監査コメント アーカイブは CSV 形式でエクスポートできます。

Source (送信元) タブ

- **Policies** (ポリシー) - > **SD-WAN** - > **Source** (送信元)

Source (送信元) タブを選択して、SD-WAN ポリシーが適用される着信パケットを定義する送信元ゾーン、送信元アドレス、および送信元ユーザーを定義します。

項目	の意味
送信元ゾーン	送信元ゾーンを指定するには **Add** (追加) を選択して 1 つ以上のゾーンを選択するか **Any** (任意) ゾーンを選択します。 複数のゾーンを指定して管理を簡略化できます。たとえば、異なるゾーンに 3 つのブランチがあり、残りの一致条件とパス選択を 3 つのブランチで同じにする場合、1 つの SD-WAN ルールを作成し、3 つのブランチをカバーする 3 つの送信元ゾーンを指定できます。 *SD-WAN* ポリシー ルールでは、レイヤー *3* タイプのゾーンのみがサポートされます。
送信元アドレス	送信元アドレスを指定するには、送信元アドレスまたは外部ダイナミック リスト (EDL) を**Add** (追加)するか、ドロップダウンから選択するか、**Address** (アドレス) を選択して新しいアドレス オブジェクトを作成します。または、 **Any** (任意)の送信元アドレス (デフォルト) を選択します。
Source User（送信元ユーザー）	特定のユーザーを指定するには、 **Add** (追加) を選択し (タイプは 選択を示します)、ユーザー、ユーザーのリスト、またはユーザーのグループを入力します。または、ユーザーのタイプを選択します。 • 任意–(デフォルト) ユーザー データに関係なく、すべてのユーザーを含めます。 • ログオン前 – GlobalProtect™ を使用してネットワークに接続しているが、自分のシステムにはログインしていないリモートユーザーが含まれます。GlobalProtect アプリのポータルに Pre-logon（ログオン前）オプションが設定されている場合、自分のマシンに現在ログインしていないユーザーは、ユーザー名 pre-logon として識別されます。pre-logon ユーザー用のポリシーを作成でき、また、ユーザーが直接ログインしていなくても、そのマシンは完全にログインしているかのようにドメインで認証されます。 • **known-user**（既知のユーザー） – 認証されたすべてのユーザー（ユーザー データがマッピングされた IP アドレス）が含まれます。このオプションは、ドメインの「ドメイン ユーザー」グループに相当します。 • **unknown**[未知] – 認証されていないすべてのユーザー (ユーザーにマップされていない IP アドレス) が含まれます。例えば、**unknown**(不明) はゲスト レベルのアクセスに使用できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	これらのユーザーは、ネットワーク上の IPアドレスを持っていますが、ドメインに認証されず、ファイアウォール上に IPアドレス対ユーザーのマッピング情報がないためです。 ファイアウォールが *User-ID*™ エージェントではなく、*RADIUS*、*TACACS+*、または *SAML* アイデンティティ プロバイダ サーバーからユーザー情報を収集している場合、ユーザーのリストは表示されません。ユーザー情報を手動で入力する必要があります。

Destination (宛先) タブ

- **Policies (ポリシー) -** > **SD-WAN -** > **Destination (宛先)**

Destination (宛先) タブを選択して、SD-WAN ポリシー ルールが適用されるトラフィックを定義する宛先ゾーンまたは宛先アドレスを定義します。

項目	の意味
宛先ゾーン	宛先ゾーンを**Add** (追加) します (デフォルトは任意)。ゾーンはレイヤー3 である必要があります。新しいゾーンを定義する手順については、「Network (ネットワーク) > Zones (ゾーン)」を参照してください。 複数のゾーンを追加して管理を簡素化します。たとえば、信頼されていない宛先ゾーンが指定されている 3 つの異なる内部ゾーン (マーケティング、販売、広報) がある場合、すべてのケースを対象とした 1 つのルールを作成できます。
宛先アドレス	宛先アドレス、アドレス グループ、External Dynamic Lists (外部ダイナミック リスト - EDL)、または地域を**Add (追加)** します (デフォルトは **Any (任意)**)。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Address (アドレス)**、**Adress Group (アドレスグループ)**をクリックして設定を行います。 **Negate**[上記以外]を選択すると、設定したアドレス以外の任意のアドレスを指定したことになります。

SD-WAN Application/Service (アプリケーション/サービス) タブ

- **Policies (ポリシー) -** > **SD-WAN -** > **Application/Service (アプリケーション / サービス)**

Application/Service (アプリケーション / サービス) タブを選択して、SD-WAN ポリシー ルールを適用するアプリケーションまたはサービスを指定します。

項目	の意味
Path Quality Profile (パス品質プロファイル)	指定したアプリケーションとサービスに適用する最大ジッター、レイテンシ–、およびパケット損失率のしきい値を決定するパス品質プロファイルを選択します。パス品質プロファイルがまだ作成されていない場合は、このタブから 新しい **SD-WAN** パス品質 プロファイルを作成できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
アプリケーション [applications]	SD-WAN ポリシー ルールに特定のアプリケーションを**Add** (追加)するか **Any** (任意)を選択します。アプリケーションに複数の機能がある場合、アプリケーション全体または個別の機能を選択します。アプリケーション全体を選択した場合、すべての機能が含まれ、将来、機能が追加されるとアプリケーション定義が自動的に更新されます。 SD-WAN ポリシー ルールでアプリケーション グループ、フィルタ、またはコンテナを使用している場合は、Application (アプリケーション) 列のオブジェクトの上にマウスを置き、ドロップダウン リストを開いて **Value** (値)を選択すると、オブジェクトの詳細が表示されます。これにより、**Object**[オブジェクト]に移動しなくても、ポリシーからアプリケーションメンバーを直接表示することができます。 レイテンシ#、ジッター、またはパケット損失の影響を受けるビジネスクリティカルなアプリケーションのみを追加します。アプリケーション カテゴリまたはサブカテゴリが広すぎて、アプリケーションごとの制御ができないため、追加しないでください。
サービス	SD-WAN ポリシー ルールに特定のサービスを**Add** (追加) し、これらのサービスからのパケットを許可または拒否するポートを選択します。 • いずれか–選択したサービスがすべてのプロトコルやポートで許可または拒否されます。 • **application-default** (アプリケーションデフォルト)– 選択したサービスが **Palo Alto Networks®** によって定義されたデフォルトのポートでのみ許可または拒否されます。このオプションは 許可アクションを指定するポリシーに使用することをお勧めします。このオプションは、意図的である場合を除き、動作と使用方法が望ましくない可能性があります。このオプションを許可ポリシーに使用することで、そうしたサービスの実行を禁止できます。 このオプションを使用すると、デフォルトのポートのみが *SD-WAN* ポリシーと一致し、アクションが実行されます。セキュリティ ポリシー ルールによっては、デフォルト ポートにない他のサービスが許可される場合がありますが、*SD-WAN* ポリシーと一致せず、*SD-WAN* ポリシー ルールアクションは実行されません。 ほとんどのサービスの場合はアプリケーションデフォルトを使用し、サービスが非標準ポートを使用したり、他の悪意のある動作を生じさせたりしないようにします。サービスのデフォルトのポートが変わると、ファイアウォールが自動的にルールを更新してデフォルトのポートを修正します。内部のカスタム サービスのように標準的でないポートを使用するサービスについては、サービスを修正するか、非標準ポートを指定するルールを作成し、対象のサービスを必要とするトラフィックにのみルールを適用します。 • **Select** （選択）– 既存のサービスを**Add** （追加）するか、**Service** （サービス）または**Service Group** （サービス グループ）を選択し

© 2019 Palo Alto Networks, Inc.

項目	の意味
	て新しいエントリを指定します。（または Objects（オブジェクト）> Services（サービス）および Objects（オブジェクト）> Service Groups（サービス グループ）を選択します）。

SD-WAN Path Selection (パス選択) タブ

- **Policies (ポリシー) - > SD-WAN - > Path Selection (パス選択)**

Path Selection (パス選択) タブを選択して、優先パスのパス正常性メトリックの 1 つが SD-WAN ポリシー ルールのパス品質プロファイルでコンフィグされたしきい値を超えた場合に、ファイアウォールが使用するアプリケーションまたはサービス トラフィックのために新しいパスを選択する方法を制御するトラフィック分散プロファイルを指定します。

項目	の意味
トラフィック分散プロファイル	ドロップダウンからトラフィック分散プロファイルを選択します。これにより、優先パスのパス正常性メトリックの 1 つがルールのパス品質プロファイルで設定されたしきい値を超えたときに、ファイアウォールがアプリケーションまたはサービス トラフィックの代替パスを選択する方法が決定します。

SD-WAN Target (ターゲット) タブ

- **Policies (ポリシー) - > SD-WAN - > Target (ターゲット)**

Target (ターゲット) タブを選択して、Panorama が SD-WAN ポリシー ルールをプッシュする管理対象デバイスを選択します。このタブは、Panorama管理サーバーでのみサポートされています。

項目	の意味
任意 (すべての対象デバイス)	SD-WAN ポリシー ルールを Panorama管理サーバーで管理されているすべてのデバイスにプッシュするには、有効 (チェック) にします。
機器	1. Devices (デバイス) タブの左側で、オプションで1 つ以上のフィルターを選択し、**Name (名前)** セクションの右側に表示されるアイテムをフィルタリングします。 2. **Name (名前)**セクションで、Panorama が SD-WAN ポリシー ルールをプッシュする 1 つ以上のデバイスを選択します。 3. 選択されたデバイスとカウントのみを表示するには **Filter Selected (フィルタ選択済み)** を有効 (チェック) にします。
tags	Tags (タグ) タブで、デバイスに適用された 1 つ以上の**Tags (タグ)** を **Add(追加)** します。Panorama は、指定されたタグでタグ付けされたデバイスに SD-WAN ルールをプッシュします。 *Devices (デバイス) タブまたは Tags (タグ) タブのいずれかを使用して、Panorama がルールをプッ*

© 2019 Palo Alto Networks, Inc.

項目	の意味
	シュする場所を指定できますが、両方を指定することはできません。
これらの指定されたデバイスとタグのみをターゲットに設定する	有効 (チェック) にすると、選択した **Devices** (デバイス) または指定した **Tags** (タグ)のデバイスを除くすべてのデバイスに SD-WAN ポリシー ルールがプッシュされます。

Objects

オブジェクトによりポリシールールの作成、実行スケジュールの設定、そして検索が可能になり、セキュリティプロファイルによりポリシールールで脅威防御を行うことができるようになります。

このセクションでは、セキュリティ プロファイルの設定方法と、ポリシーで使用できるオブジェクトについて説明します。

- Move,Clone,Override,or Revert Objects（オブジェクトの移動、複製、オーバーライド、または元に戻す）
- Objects（オブジェクト）> Addresses（アドレス）
- Objects（オブジェクト）>AddressGroups
- Objects（オブジェクト）> Regions（地域）
- Objects（オブジェクト）> Applications（アプリケーション）
- Objects（オブジェクト）>ApplicationGroups
- Objects（オブジェクト）>ApplicationFilters
- Objects（オブジェクト）> Services（サービス）
- Objects（オブジェクト）>ServiceGroups
- Objects（オブジェクト）> Tags（タグ）
- Objects（オブジェクト）> GlobalProtect > HIP Objects（HIP オブジェクト）
- Objects（オブジェクト）> GlobalProtect > HIP Profiles（HIP プロファイル）
- Objects（オブジェクト）>ExternalDynamic Lists（ExternalDynamic リスト）
- Objects（オブジェクト）>CustomObjects
- Objects（オブジェクト）>SecurityProfiles
- Objects（オブジェクト）>SecurityProfiles > GTP Protection（GTP プロテクション）
- Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> SCTP Protection（SCTP プロテクション）
- Objects（オブジェクト）> ServiceProfile Groups（ServiceProfile グループ）
- Objects（オブジェクト）>LogForwarding
- Objects（オブジェクト）>Authentication（認証）
- （オブジェクト）>DecryptionProfile
- Objects（オブジェクト）> Schedules（スケジュール）

オブジェクトの移動、コピー、オーバーライド、取り消し

既存のオブジェクトを編集する方法については以下のトピックを参照してください。

- オブジェクトの移動またはコピー
- オブジェクトのオーバーライド/取り消し

オブジェクトの移動またはコピー

オブジェクトを移動またはコピーする場合は、Shared（共有）場所を含め、自分がアクセス許可を与えられている **Destination**（宛先）（ファイアウォール上の仮想システム、または Panorama™ 上のデバイスグループ）を割り当てることができます。

オブジェクトルールを移動する場合は、**Objects**[オブジェクト] タブでオブジェクトを選択し、**Move**[移動]をクリックして、**Move to other vsys**[他のvsysに移動]（ファイアウォールのみ）または**Move to other device group**[他のデバイスグループに移動]（Panoramaのみ）を選択し、以下の表の各フィールドを入力して**OK**をクリックします。

オブジェクトをコピーする場合は、**Objects**[オブジェクト] タブで**Clone**[コピー]をクリックして、以下の表の各フィールドを入力して**OK**をクリックします。

設定の移動/コピー	の意味
選択したオブジェクト	操作対象として選択したポリシーまたはオブジェクトの名前と現在の場所 (仮想システムまたはデバイス グループ) が表示されます。
宛先	ポリシーまたはオブジェクトの新しい場所として、仮想システム、デバイス グループ、または共有を選択します。デフォルト値は、**Policies**[ポリシー] または **Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] または **Device Group**[デバイス グループ] です。
検証で最初に検出されたエラーに起因するエラーが発生しました	このオプションをオンにすると（デフォルトはオン）、ファイアウォールまたはPanoramaが、最初に検出したエラーを表示し、それ以上エラーをチェックしません。たとえば、移動するポリシー ルールで参照されているオブジェクトが [宛先] に存在しないと、エラーが発生します。このオプションをオフにした場合、ファイアウォールまたはPanoramaは、先に全てのエラーを検出してからそれらを表示します。

オブジェクトのオーバーライド/取り消し

Panorama では、ツリー階層の中でデバイス グループを 4 段階までネストさせることができます。一番下のレベルのデバイスグループは、連続する上位レベルとして親、祖父母、曾祖父母のデバイス グループを持つことができます。これらをまとめて先祖と呼び、一番下のレベルのデバイスグループはこれらからポリシーとオブジェクトを継承します。一番上のレベルのデバイス グループは、子、孫、曾孫のデバイス グループを持つことができます。これらをまとめて子孫と呼びます。子孫のオブジェクトをオーバーライドして、先祖のオブジェクトとは異なる値を持たせることもできます。このオーバーライド機能はデフォルトで有効になっています。ただし、共有オブジェクトまたはデフォルト (事前設定) オブジェクトをオーバーライドすることはできません。Web インターフェイスでは、値を継承しているオブジェクトには アイコンが、値がオーバーライドされている継承オブジェクトには アイコンが表示されます。

© 2019 Palo Alto Networks, Inc.

- **Override an object**[オブジェクトのオーバーライド] — **Objects**[オブジェクト] タブを選択し、オーバーライドされたオブジェクトの所属先となる子孫 **Device Group**[デバイスグループ] を選択してから、**Override**[オーバーライド] をクリックして設定を編集します。オブジェクトの **Name**[名前] または **Shared**[共有] 設定をオーバーライドすることはできません。
- **Revert an overridden object to its inherited values**[オーバーライドしたオブジェクトの設定値を継承した値に戻す] — **Objects**[オブジェクト] タブを選択し、オーバーライドされたオブジェクトが所属する子孫 **Device Group**[デバイスグループ] を選択してから、当該オブジェクトを選択し、**Revert**[元に戻す] をクリックした後、**Yes**[はい] をクリックして操作を確定します。
- **Disable overrides for an object**[オブジェクトのオーバーライドを無効化] — **Objects**[オブジェクト] タブを選択し、当該オブジェクトが存在する **Device Group**[デバイスグループ] を選択してから、そのオブジェクトの名前をクリックし、**Disable override**[オーバーライドの無効化] チェックボックスをオンにして、**OK** をクリックします。これにより、そのオブジェクトのオーバーライドが、選択した **Device Group**（デバイス グループ）からオブジェクトを継承するすべてのデバイス グループで無効になります。
- **Replace all object overrides across Panorama with the values inherited from the Shared location or ancestor device groups**（**Panorama** 全体のすべてのオブジェクト オーバーライドを共有場所または先祖デバイス グループから継承した値で置換する） — **Panorama** > **Setup**（セットアップ） > **Management**（管理）を選択し、Panorama 設定で **Ancestor Objects Take Precedence**（上位オブジェクトを優先）を選択して、**OK**をクリックします。この後、Panorama およびオーバーライドが含まれるデバイス グループに対してコミットを実行して、継承値をプッシュする必要があります。

© 2019 Palo Alto Networks, Inc.

Objects > Addresses [オブジェクト > アドレス]

アドレスオブジェクトには、IPv4 アドレスまたは IPv6 アドレス (単一の IP アドレス、アドレスの範囲、またはサブネット) 、FQDN、ワイルドカードのアドレス (IPv4 アドレスに続けてスラッシュ、ワイルドカード マスク) のいずれかを含めることができます。アドレス オブジェクトを使用すると、インスタンスごとに手動で各アドレスを追加しなくても、すべてのポリシー ルールベース、フィルター、他のファイアウォール機能の送信元アドレスまたは宛先アドレスと同じアドレスまたはアドレスグループを再利用できます。Web インターフェイスまたは CLI を使用してアドレス オブジェクトを作成します。変更を加えると、オブジェクトが設定の一部になります。

はじめに新規アドレスを**Add** (追加) してから以下の値を指定します。

アドレス オブジェクトの設定	の意味
氏名	このオブジェクトの一部として含めるアドレスを記述する名前 (最大 63 文字) を入力します。この名前は、セキュリティ ポリシールールを定義するときにアドレスのリストに表示されます。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
共有	このアドレス オブジェクトを共有する場合は、以下を含むこのオプションを選択します。 • マルチ **vsys** ファイアウォール上のすべての仮想システム(vsys)–この選択を解除すると、**Objects** (オブジェクト) タブで選択した**Virtual System** (仮想システム) のみに対してアドレスオブジェクトが公開されます。 • **Panorama** 上のすべてのデバイス グループ–この選択を解除すると、**Objects** (オブジェクト) タブで選択した**Device Group** (デバイスグループ) のみに対してアドレスオブジェクトが公開されます。
オーバーライドの無効化 (Panoramaのみ)	このアドレス オブジェクトの設定が、このオブジェクトを継承したデバイス グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトではこの選択はオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
の意味	オブジェクトの説明を入力します (最大1023 文字)。

タイプ	アドレス オブジェクトの型およびエントリを指定します :
	• **IP Netmask (IP** ネットマスク)–以下の形式で IPv4 アドレス、IPv6 アドレスまたは IP アドレス範囲を入力します。Ipv6 アドレスの場合は、ホスト部を指定せずにネットワーク部のみを指定することをお勧めします。以下がその例です。
	  • **192.168.80.150/32**–1 つのアドレスを示します。
	  • **192.168.80.0/24**–192.168.80.0 ~ 192.168.80.255 のすべてのアドレスを示します。
	  • **2001:db8::/32**
	  • **2001:db8:123:1::/64**

© 2019 Palo Alto Networks, Inc.

アドレス オブジェクトの設定	の意味
	• **IP Range (IP 範囲)**—次の形式を使用してアドレスの範囲を入力します。*ip_address–ip_address*（範囲の両端が IPv4 アドレスであるか、または両方が IPv6 アドレスです）。以下がその例です。2001:db8:123:1::1-2001:db8:123:1::22 • **IP Wildcard Mask (IP** ワイルドカード マスク**)**—IPv4 アドレスに続けてスラッシュ、ワイルドカード マスク（0 から始める必要があります）という形式で IP ワイルドカード アドレスを入力します。例：10.182.1.1/0.127.248.0。ワイルドカード マスクのゼロ（0）ビットは、比較対象のビットが、0 がカバーする IP アドレスのビットと一致しなければならないことを示します。マスクの 1 ビットはワイルドカード ビットであり、比較対象のビットが、1 がカバーする IP アドレスのビットと一致する必要がないことを示します。IP アドレスおよびワイルドカード マスクをバイナリに変換します。マッチングの補足：0011 のバイナリ ス二ペットでは、1010 のワイルドカード マスクが 4 つのマッチ（0001、0011、1001、および 1011）をもたらします。 *IP Wildcard Mask* 型のアドレス オブジェクトはセキュリティポリシー ルールでのみ使用できます。 • **FQDN**—ドメイン名を入力します。FQDN はコミット時に最初に解決されます。TTL が最低 FQDN 更新時間以上である場合、FQDN のエントリは後に FQDN の TTL に基づいて更新されます。そうでない場合、FQDN のエントリは Minimum FQDN Refresh Time (最低 FQDN 更新時間) に更新されます。FQDN は、システムの DNS サーバーまたは DNS プロキシ オブジェクト (プロキシが設定されている場合) によって解決されます。
解決	アドレスタイプを選択し、IP アドレスまたは FQDN を入力したら、**Resolve**（解決）をクリックして（ファイアウォールまたは Panorama の DNS 設定に基づいて）関連する FQDN または IP アドレスをそれぞれ表示します。 アドレスオブジェクトを FQDN から IP ネットマスクに変更することができます。FQDN から IP ネットマスクに変更するには、**Resolve**（解決）をクリックして、FQDN が解決する IP アドレスを確認してから、**Use this address**（このアドレスを使用）します。アドレス オブジェクト タイプが IP ネットマスクに動的に変更され、選択した IP アドレスがテキスト フィールドに表示されます。 または、アドレスオブジェクトを IP ネットマスクから FQDN に変更するには、**Resolve**（解決）をクリックして IP ネットマスクが解決する DNS 名を表示し、FQDN を選択して、**Use this FQDN**（この **FQDN** を使用）します。タイプが FQDN に変更され、テキスト フィールドに FQDN が表示されます。
tags	このアドレス オブジェクトに適用するタグを選択または入力します。ここでタグを定義することも、Objects（オブジェクト）> Tags（タグ）タブを使用して新しいタグを作成することもできます。

© 2019 Palo Alto Networks, Inc.

Objects > Address Groups [オブジェクト > アドレス グループ]

セキュリティ ポリシーの作成を簡略化するには、同じセキュリティ設定が必要なアドレスをアドレス グループにまとめます。アドレス グループは、静的または動的にすることができます。

- ダイナミック アドレス グループ:動的アドレスグループには、タグの検索とタグベースのフィルタを使用してメンバーがダイナミックに入力されます。動的アドレス グループは、広範囲に及ぶ仮想インフラストラクチャがあり、仮想マシンの場所/IP アドレスが頻繁に変更される場合に非常に便利です。たとえば、高度なフェイルオーバーで仮想マシンが頻繁にセットアップまたはプロビジョニングされていて、ファイアウォールの設定/ルールを変更せずに新しいマシンとの間で送受信されるトラフィックにポリシーを適用する場合などです。

  ポリシーで動的アドレス グループを使用するには、以下のタスクを実行する必要があります。

  - 動的アドレス グループを定義し、ポリシー ルール内で参照します。
  - ファイアウォールに IP アドレスと対応するタグを通知して、動的アドレス グループのメンバーを構成できるようにします。これを行うには、ファイアウォール上で XML API を使用する外部スクリプトを使用するか、VMware ベースの環境の場合は **Device**（デバイス）> **VM Information Sources**（**VM** 情報の送信元）を選択してファイアウォールの設定を編集します。

  動的アドレス グループには、静的に定義したアドレス オブジェクトも含めることができます。アドレス オブジェクトを作成し、動的アドレス グループに割り当てたものと同じタグを適用すると、その動的アドレス グループには、そのタグに一致するすべての静的オブジェクトと動的オブジェクトが含まれます。そのため、タグを使用して動的オブジェクトと静的オブジェクトの両方を同じ アドレス グループにまとめることができます。
- 動的アドレスオブジェクト:静的アドレスグループには、静的なアドレスオブジェクト、動的アドレスグループ、またはアドレスオブジェクトと動的アドレスグループの両方の組み合わせを含めることができます。

  アドレス オブジェクトを作成するには、**Add**[追加] をクリックし、以下のフィールドを入力します。

アドレス グループ設定	の意味
氏名	アドレス グループを表す名前 (最大 63 文字) を入力します。この名前は、セキュリティ ポリシーを定義するときにアドレスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有	以下に対してアドレスグループを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Virtual System**[仮想システム] のみに対してアドレスグループが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] に対してのみアドレスグループが公開されます。
オーバーライドの無効化（Panoramaのみ）	このアドレス グループ オブジェクトの設定が、このオブジェクトを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでこのオプションはオフになっ

© 2019 Palo Alto Networks, Inc.

アドレス グループ設定	の意味
	ており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
の意味	オブジェクトの説明を入力します (最大1023 文字)。
タイプ	**Static**[静的] または **Dynamic**[動的] を選択します。 動的 アドレス グループを作成するには、一致条件を使用してグループに含めるメンバーをまとめます。**AND** または **OR** 演算子を使用して、**Match**[一致] 条件を定義します。 一致条件に使用する属性のリストを表示するには、送信元/ホストにアクセスして属性を取得できるようにファイアウォールを設定しておく必要があります。設定した情報送信元の各仮想マシンをファイアウォールに登録します。ファイアウォールは、マシンをポーリングして、ファイアウォールの変更なしに *IP* アドレスまたは設定の変更を取得できます。 静的 アドレス グループの場合、**Add**[追加] をクリックし、1 つ以上の**Addresses**[アドレス]を選択します。**Add**[追加] をクリックし、オブジェクトまたはアドレス グループをアドレス グループに追加します。グループには、アドレス オブジェクト、静的と動的の両方のアドレス グループを含めることができます。
tags	このアドレス グループに適用するタグを選択または入力します。タグの詳細は、「Objects（オブジェクト）> Tags（タグ）」を参照してください。

メンバー数およびアドレス	アドレス グループを追加したら、**Objects**（オブジェクト）> **Address Groups**（アドレス グループ）ページの Members Count（メンバー数）列に、グループ内のオブジェクトが動的または静的のどちらの方法で作成されたかが示されます。
	• 静的アドレス グループの場合、アドレス グループのメンバー数を参照できます。
	• タグを使用してメンバーを動的に作成したアドレス グループ、または静的メンバーと動的メンバーの両方を含むアドレス グループの場合、メンバーを参照するには、Address（アドレス）列の **More...**（詳細...）リンクをクリックします。これで、アドレス グループに登録された IP アドレスを参照できます。
	  • Type（タイプ）は、IP アドレスが静的アドレス オブジェクトであるか、動的に登録されるものであるかを示し、IP アドレスを表示します。
	  • Action（アクション）を使用すると、IP アドレスから **Tags**（タグ）を **Unregister**（登録解除）できます。リンクをクリックして、登録元を **Add**（追加）し、登録解除するタグを指定します。

© 2019 Palo Alto Networks, Inc.

Objects > Regions [オブジェクト > 地域]

ファイアウォールでは、特定の国や他の地域に適用されるポリシー ルールを作成できます。地域は、セキュリティ ポリシー、復号化ポリシー、DoS ポリシーの送信元および宛先を指定するときにオプションとして利用できます。セキュリティポリシールールのオプションとして地域を含めるには、国の標準リストから選択するか、このセクションで説明されている地域設定を使用してカスタム地域を定義します。

以下の表では、地域設定について説明します。

地域設定	の意味
氏名	地域を表す名前を選択します。この名前は、セキュリティ ポリシーを定義するときにアドレスのリストに表示されます。
デバイス稼働場所	緯度と経度を指定する場合は、このオプションを選択して値 (xxx.xxxxxx 形式) を指定します。この情報は、App-Scope のトラフィック マップおよび脅威マップに使用されます。「Monitor (監視) > Logs (ログ) 」を参照してください。
addresses	以下のいずれかの形式を使用して IP アドレス、IP アドレス範囲、または地域を識別するサブネットを指定します。 x.x.x.x x.x.x.x-y.y.y.y x.x.x.x/n

© 2019 Palo Alto Networks, Inc.

Objects > Dynamic User Groups [オブジェクト > 動的ユーザー グループ]

動的ユーザー グループを作成するには **Objects**(オブジェクト) > **Dynamic User Groups** (動的ユーザー グループ)、 **Add** (追加) を選択して、以下の設定を構成します。

Dynamic User Group Settings (動的ユーザー グループ設定)	の意味
氏名	動的ユーザー グループを説明する **Name** (名前) を入力します (最大 63 文字)。この名前は、セキュリティ ポリシー ルールを定義するときに送信元ユーザー リストに表示されます。名前は一意で、英数字、スペース、ハイフン、およびアンダースコアのみを使用している必要があります。
の意味	オブジェクトの **Description** (説明) を入力します (最大1,023 文字)。
共有 (Panorama のみ)	動的ユーザー グループの一致条件を Panorama 上のすべてのデバイス グループで使用できるようにする場合は、このオプションを選択します。 *Panorama* は、グループのメンバーをデバイス グループと共有しません。 このオプションをオフにすると、動的ユーザー グループの一致基準は **Objects** (オブジェクト) タブで選択した **Device Group** (デバイス グループ) でのみ使用できます。
オーバーライドを無効にする (Panorama のみ)	管理者が、オブジェクトを継承するデバイス グループのこの動的ユーザー グループの設定をオーバーライドすることを禁止する場合はこのオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
一致	**Add Match Criteria** (条件の追加)から **AND** または **OR** 演算子を使用した動的ユーザー グループのメンバーを定義し、複数のタグを含めます。 *Add Match Criteria* (条件の追加)をすると、既存のタグのみが表示されます。既存のタグを選択するか、新しいタグを作成できます。
tags	(任意) 動的ユーザー グループ オブジェクトに適用する静的オブジェクト タグを選択または入力します。これにより、グループのメンバーではなく、動的ユーザー グループ オブジェクト自体にタグが付けられます。選択したタグを使用すると、一致条件に関係なく関連アイテムをグループ化できます。タグの詳細は、「Objects (オブジェクト) > Tags (タグ)」を参照してください。

動的ユーザー グループを追加すると、グループの次の情報を表示できます。

© 2019 Palo Alto Networks, Inc.

Dynamic User Groups Column (動的ユーザー グループ列)	の意味
場所 (Panorama のみ)	動的ユーザー グループの一致条件が、Panorama のすべてのデバイス グループ (**Shared** (共有)) で使用できるか、選択したデバイス グループで使用できるかを特定します。
Users	動的ユーザー グループのユーザーのリストを表示するには 詳細 を選択します。 • グループに含めるタグをユーザーに追加するには、 **Register Users** (新規ユーザーの登録)から、ユーザーに適用する **Registration Source**(登録ソース) と **Tags** (タグ) を選択します。ユーザーのタグがグループの条件に一致すると、ファイアウォールはユーザーを動的ユーザー グループに追加します。 • (任意) **Timeout** (タイムアウト) を分単位で指定し (デフォルトは 0、範囲は 0 ～ 43,200)、指定した時間が経過したときにユーザーをグループから削除します。 • (任意) **Users** (ユーザー) をグループに **Add** (追加) 、またはグループから **Delete** (削除) します。 • ユーザーからタグを削除してグループのメンバーにならないようにするには、ユーザーを選択し、 **Unregister Users** (ユーザーの登録解除)をしてから **Registration Source** (登録ソース) と **Tags** (タグ)を選択します。 • ユーザーの動的ユーザー グループ リストを確認または変更したら **Close** (終了)をクリックします。

© 2019 Palo Alto Networks, Inc.

Objects > Applications [オブジェクト > アプリケーション]

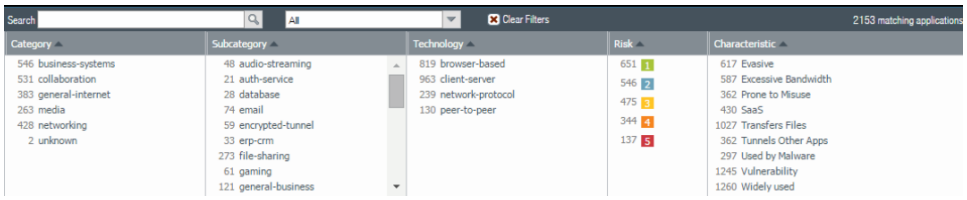
以下のトピックでは、**Applications** (アプリケーション) ページについて説明します。

確認すべき情報	以下を参照
Applications (アプリケーション) ページに表示されるアプリケーションの設定と属性を理解する	アプリケーションの概要 アプリケーションでサポートされる操作
新規アプリケーションを追加するか、既存のアプリケーションを変更する	アプリケーションの定義

アプリケーションの概要

Applications (アプリケーション) ページには、アプリケーションの相対セキュリティ リスク (1 ~ 5) など、各アプリケーション定義のさまざまな属性が表示されます。リスク値は、アプリケーションでファイルを共有できるか、誤用が起こりやすいか、ファイアウォールの回避を試行するか、などの基準に基づいています。値が大きいほどリスクが大きくなります。

ページ上部のアプリケーション ブラウザエリアには、以下のように、表示内容のフィルタに使用できる属性が表示されます。各エントリの左側にある数字は、その属性があるアプリケーションの合計数を表しています。



週次のコンテンツ リリースには、新しいデコーダとシグネチャを開発するためのコンテクストが定期的に含まれています。

以下の表では、アプリケーションの詳細情報について説明します。カスタム アプリケーションおよび Palo Alto® Networks アプリケーションには、これらのフィールドの一部またはすべてが表示されます。

アプリケーションの詳細情報	の意味
氏名	アプリケーションの名前です。
の意味	アプリケーションの説明 (最大 255 文字)。
追加情報	アプリケーションに関する追加情報が掲載されている Web ソース (Wikipedia、Google、および Yahoo!) にリンクします。
標準ポート	アプリケーションがネットワークとの通信に使用するポートです。

© 2019 Palo Alto Networks, Inc.

アプリケーションの詳細情報	の意味
依存	このアプリケーションの実行に必要な他のアプリケーションのリストです。選択したアプリケーションを許可するポリシー ルールを作成する場合は、そのアプリケーションが依存する他のすべてのアプリケーションも許可することを確認する必要があります。
暗黙的に使用	選択したアプリケーションが依存しているものの、暗黙的にサポートされているため、選択したアプリケーションを許可するためにセキュリティ ポリシー ルールに追加する必要のないその他のアプリケーション。
以前の識別	新規の App-ID™、または変更された App-ID について、そのアプリケーションの以前の ID を表します。これにより、アプリケーションの変化に応じてポリシーを変更する必要があるかどうかを査定できます。App-ID を無効にすると、そのアプリケーションに関連付けられたセッションは、そのアプリケーションの以前の ID でポリシーと照合されます。同様に、無効にされた App-ID は、そのアプリケーションの以前の ID でログに記録されます。
アクションの拒否	App-IDは、デフォルトの拒否アクションと共に作成されます。デフォルトの拒否アクションは、アプリケーションが拒否アクションの指定されたセキュリティポリシールールに含まれているときのファイアウォールの応答方法を指定したものです。デフォルトの拒否アクションとして、サイレント ドロップまたは TCP リセットを指定できます。このデフォルトアクションはセキュリティポリシー内でオーバーライドできます。
特徴	
セキュリティを回避する	ファイアウォールを通り抜けるために、ポートやプロトコルを本来の用途とは異なる目的に使用すること。
帯域幅を消費する	通常の使用において 1 Mbps 以上の帯域幅を定常的に消費すること。
乱用されやすい	不正な目的に使用されることが多いこと。また、ユーザーの意図を超えて攻撃されるように容易に設定できてしまうこと。
SaaS	ファイアウォールでは、Software as a Service (SaaS) を次のようなサービスとして分類します。すなわち、ソフトウェアとインフラストラクチャはアプリケーション サービス プロバイダによって所有および管理されているが、ユーザーがデータに対するフル コントロール (データの作成、アクセス、共有、転送の実行権限をどのユーザーに付与するかも含む) を保有しているサービスです。 アプリケーションの特徴という観点から見ると、SaaS アプリケーションと Web サービスは異なります。Web サービスとは、ホストされたアプリケーションであり、ユーザーがデータを所有しないサービス (Pandora など) と、多数の購読者が社交目的で投稿したデータの共有を主要機能とするサービス (LinkedIn、Twitter、Facebook など) があります。
ファイルの転送	ネットワークを介してシステム間でファイルを転送できること。
他のアプリケーションをすり抜けさせる	他のアプリケーションを自分のプロトコル内で転送できること。

© 2019 Palo Alto Networks, Inc.

アプリケーションの詳細情報	の意味
悪意のあるソフトウェアに利用される	アプリケーションがマルウェアに感染した状態で配布されること (マルウェアは、アプリケーションを利用して、伝播、拡散、攻撃、データの不正入手を行うことが知られている)。
既知の脆弱性がある	一般に公表されている脆弱性があること。
広く使われている	ユーザーが 100 万人を超える可能性があること。
他のアプリケーションに対するスキャンを続行	他のアプリケーション シグネチャとの照合を続行するようにファイアウォールに指示します。このオプションをオフにすると、ファイアウォールは、最初にシグネチャが一致した後、アプリケーション シグネチャとの照合を停止します。
SaaS Characteristics SaaS 特性	
情報漏洩	過去 3 年以内に信頼できない情報源に安全な情報を公開した可能性があるアプリケーション。
悪質なサービス利用規約	企業データを危険にさらすおそれのある利用規約が記載されたアプリケーション。
証明書がない	SOC1、SOC2、SSAE16、PCI、HIPAA、FINRAA、またはFEDRAMPなどの業界プログラムまたは証明書に準拠していないアプリケーション。
財政的実行可能性が低い	今後 18〜24 ヶ月以内に中断する可能性のあるアプリケーション。
IP 制限がない	ユーザーアクセスのための IP ベースの制限がないアプリケーション。
分類	
カテゴリ	以下のアプリケーション カテゴリがあります。 • business-system • コラボレーション • 一般インターネット • メディア • networking • 未知
サブカテゴリ	アプリケーションが分類されるサブカテゴリです。カテゴリが異なると、関連付けられるサブカテゴリも異なります。たとえば、collaboration カテゴリのサブカテゴリには、email、file-sharing、instant-messaging、internet-conferencing、social-business、social-networking、voip-video、web-posting があります。一方、business-system カテゴリのサブカテゴリには、auth-service、database、erp-crm、general-business、management、office-programs、software-update、storage-backup があります。
テクノロジ	アプリケーション技術は以下のうちの1つに分類されます。

© 2019 Palo Alto Networks, Inc.

アプリケーションの詳細情報	の意味
	• クライアント/サーバー1 つ以上のクライアントがネットワーク上のサーバーと通信するクライアント/サーバー モデルを使用したアプリケーション。 • ネットワークプロトコル一般に、システム間の通信に使用され、ネットワーク操作を容易にするアプリケーション。大部分の IP プロトコルが含まれます。 • ピアツーピア通信の簡素化を図るため、中央のサーバーを介することなく他のクライアントと直接やり取りして情報を交換するアプリケーション。 • ブラウザベースWeb ブラウザに依存して機能するアプリケーション。
リスク	アプリケーションに割り当てられたリスクです。 この設定をカスタマイズするには、**Customize** (カスタマイズ) リンクをクリックして値 (1 ~ 5) を入力し、**OK** をクリックします。
tags	アプリケーションに割り当てられたタグ。 **Edit Tags (**タグの編集**)** で、アプリケーションのタグを追加または削除します。
オプション	
セッション タイムアウト	非アクティブ状態になってからアプリケーションがタイムアウトするまでの時間 (指定可能範囲は 1 ~ 604800 秒) です。このタイムアウトは、TCP または UDP 以外のプロトコルに適用されます。TCP と UDP は、この表の次の行を参照してください。 この設定をカスタマイズするには、**Customize**[カスタマイズ] リンクをクリックして値を入力し、**OK** をクリックします。
TCP タイムアウト (秒)	TCP アプリケーション フローを停止するタイムアウト (指定可能範囲は 1 ~ 604800 秒) です。 この設定をカスタマイズするには、**Customize**[カスタマイズ] リンクをクリックして値を入力し、**OK** をクリックします。 値 0 は、グローバル セッション タイマー (TCP の場合 3600 秒) が使用されることを示します。
UDP タイムアウト (秒):	UDPアプリケーションフローを停止するタイムアウト (指定可能範囲は1 ~ 604800秒) です。 この設定をカスタマイズするには、**Customize**[カスタマイズ] リンクをクリックして値を入力し、**OK** をクリックします。
TCP Half Closed (秒)	最初の FIN パケットを受信してから、2 つ目の FIN パケットまたは RST パケットを受信するまで、セッションがセッション テーブル内に保持される最大時間 (秒)。タイマーが期限切れになるとセッションが閉じられます (指定可能範囲は 1 ~ 604800 秒)。 デフォルト:このタイマーがアプリケーションレベルで設定されていない場合、グローバル設定が使用されます。

© 2019 Palo Alto Networks, Inc.

アプリケーションの詳細情報	の意味
	この値がアプリケーション レベルで設定されている場合、その値でグローバル **TCP Half Closed**[TCP半閉鎖] 設定がオーバーライドされます。
TCP Time Wait (秒)	2 つ目の FIN パケットまたは RST パケットを受信してから、セッションがセッション テーブル内に保持される最大時間 (秒)。タイマーが期限切れになるとセッションが閉じられます (指定可能範囲は 1 ~ 600 秒)。 デフォルト:このタイマーがアプリケーションレベルで設定されていない場合、グローバル設定が使用されます。 この値がアプリケーション レベルで設定されている場合、その値でグローバル **TCP Time Wait**[TCP待機] 設定がオーバーライドされます。
App-ID 対応	App-ID が有効か無効かを示します。App-IDを無効にすると、そのアプリケーションのトラフィックは、セキュリティポリシーとログの両方で、**Previously Identified As**[以前の識別内容] に指定したApp-IDで処理されます。コンテンツ リリース バージョン 490 の後に追加されたアプリケーションの場合、新規アプリケーションのポリシーへの影響を確認する際にアプリケーションを無効にすることができます。ポリシーをレビューした後、App-ID を **enable**[有効化] することも可能です。以前有効にしたアプリケーションを **disable**[無効化] することもできます。multi-vsys ファイアウォールでは、各仮想システムで App-ID を個別に無効化できます。

ファイアウォールで APP-ID を使用してアプリケーションを識別できない場合、トラフィックは不明 ([unknown-tcp] または [unknown-udp]) として分類されます。この動作は、完全に HTTP をエミュレートするアプリケーションを除き、すべての不明なアプリケーションに適用されます。詳細は、Monitor > Botnet [監視 > ボットネット]を参照してください。

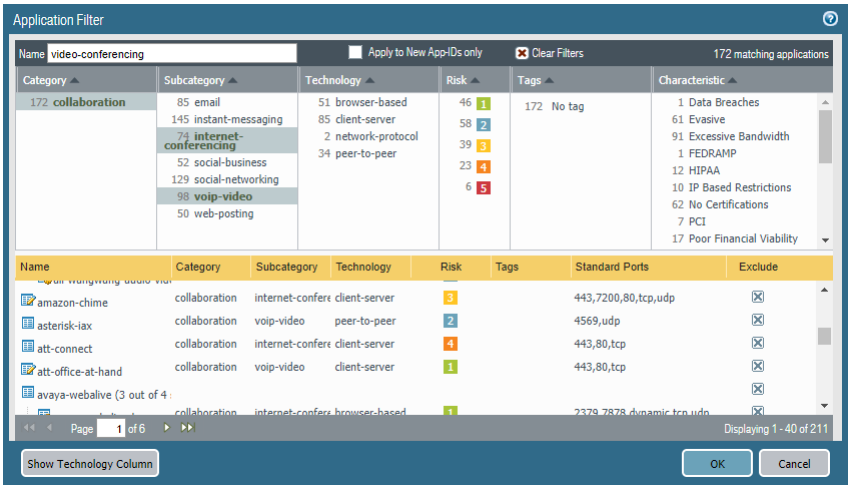
不明なアプリケーションの新しい定義を作成し、その新しいアプリケーション定義のセキュリティ ポリシーを定義できます。さらに、同じセキュリティ設定が必要なアプリケーションをアプリケーション グループにまとめることで、セキュリティ ポリシーの作成を簡略化できます。

アプリケーションでサポートされる操作

必要に応じて、このページで以下の操作を実行できます。

アプリケーションでサポートされる操作	の意味
アプリケーション名による検索	• 特定のアプリケーションを検索する場合は、**Search** (検索) フィールドにアプリケーションの名前または説明を入力して **Enter** キーを押します。ドロップダウンリストには、特定のアプリケーションの検索や絞り込みを行ったり、**All** (すべて) のアプリケーション、**Custom applications** (カスタムアプリケーション)、**Disabled applications** (無効化されたアプリケーション)、または**Tagged applications** (タグ付けされたアプリケーション) を表示することができます。 該当するアプリケーションが表示され、同時にフィルタ列が更新されて、検索条件に一致するアプリケーションの統計値が表示されます。検索は、文字列に部分的に一致します。セキュリティ ポリシーを定義すると、保存したフィルタに一致するすべてのアプリケーションに適用され

© 2019 Palo Alto Networks, Inc.

アプリケーションでサポートされる操作	の意味
	るルールを作成できます。このようなルールは、フィルタに一致するコンテンツの更新によって新しいアプリケーションが追加されると動的に更新されます。 • ページに表示されているアプリケーション属性で絞り込みを行う場合は、フィルタリングの基準として使用する項目をクリックします。たとえば、collaboration カテゴリのみをリストに表示する場合は、**collaboration**（コラボレーション）をクリックすると、そのカテゴリのアプリケーションのみがリストに表示されます。  • その他の列にフィルタを適用するには、列のエントリを選択します。フィルタリングは連続的です。カテゴリ フィルタ、サブカテゴリ フィルタ、テクノロジ フィルタ、リスク フィルタ、特徴フィルタの順に適用されます。たとえば、カテゴリ フィルタ、サブカテゴリ フィルタ、リスク フィルタを適用すると、明示的にテクノロジのフィルタを適用していなくても、自動的にTechnology（テクノロジ）列が制限され、選択したカテゴリとサブ カテゴリに一致するテクノロジのみが表示されます。フィルタを適用するたびに、アプリケーション リストが自動的に更新されます。新しいアプリケーション フィルタを作成する方法については、「Objects（オブジェクト）> Application Filters（アプリケーション フィルタ）」を参照してください。
新しいアプリケーションを追加	新しいアプリケーションを追加する方法については、「アプリケーションの定義」を参照してください。
アプリケーションの詳細を表示、またはカスタマイズする	標準ポート、特性、リスクやその他の情報を含め、アプリケーションの詳細を表示する場合はアプリケーション名のリンクをクリックします。アプリケーション設定の詳細は、「アプリケーションの定義」を参照してください。 アプリケーション名の左にあるアイコンに黄色い鉛筆（ ）が表示されている場合、そのアプリケーションがカスタムアプリケーションであることを示しています。
アプリケーションの無効化	特定の（または複数の）アプリケーションを **Disable** (無効化) すると、アプリケーション シグネチャがトラフィックと照合されなくなります。一致するアプリケーションをブロック、許可、または実施するように定義されたセ

© 2019 Palo Alto Networks, Inc.

アプリケーションでサポートされる操作	の意味
	キュリティ ルールは、アプリケーションを無効にすると、アプリケーション トラフィックに適用されません。新しいコンテンツ リリース バージョンに含まれるアプリケーションは無効にしたほうがよいことがあります。そうしたアプリケーションが一意に識別されると、アプリケーションのポリシーが適用されるかどうかが変わる可能性があるからです。たとえば、新しいコンテンツ バージョンのインストール前の状態では、Web ブラウジング トラフィックとして識別されたアプリケーションがファイアウォールに許可されていたとします。ところがコンテンツの更新をインストールした後、一意に識別されたアプリケーションが、Web ブラウジング トラフィックを許可するセキュリティ ルールに一致しなくなってしまうことがあります。このような場合は、アプリケーションを無効にして、そのアプリケーション シグネチャに一致したトラフィックが引き続き Web ブラウジング トラフィックとして分類され許可されるようにしたほうが適切です。
アプリケーションの有効化	無効化されたアプリケーションを選択して **Enable**（有効化）することにより、設定済みのセキュリティ ポリシーに従ってそのアプリケーションを管理できます。
アプリケーションのインポート	アプリケーションをインポートするには、**Import**[インポート] をクリックします。ファイルを参照して選択し、**Destination**[宛先] ドロップダウンリストからターゲットの仮想システムを選択します。
アプリケーションのエクスポート	アプリケーションをエクスポートする場合は、アプリケーションのオプションを選択して**Export**[エクスポート] をクリックします。プロンプトに従ってファイルを保存します。
アプリケーション設定テーブルのエクスポート	**PDF/CSV** 形式のすべてのアプリケーション上の情報をエクスポートします。Web インターフェイスで表示される列のみエクスポートされます。Export Configuration Table Data（設定バンドルデータのエクスポート）を参照してください。
新しいコンテンツ リリースのインストール後のポリシーへの影響を評価する	コンテンツリリースバージョンのインストール前とインストール後における、アプリケーションに対するポリシーの実施状況を確認する場合は、**Review Policies** (ポリシーの確認)を行います。[ポリシーのプレビュー] ダイアログを使用すると、ダウンロードしたコンテンツ リリース バージョンに含まれている新規アプリケーションによるポリシーへの影響を確認できます。Policy Review（ポリシーのプレビュー）ダイアログでは、既存のセキュリティ ポリシー ルールの保留中のアプリケーション（コンテンツ リリース バージョンでダウンロードされているが、ファイアウォールにインストールされていないアプリケーション）を追加または削除できます。保留中のアプリケーションのポリシーを変更しても、対応するコンテンツ リリース バージョンがインストールされるまで有効になりません。Policy Review（ポリシーのプレビュー）ダイアログは、**Device**（デバイス）> **Dynamic Updates**（動的更新）ページでコンテンツ リリース バージョンをダウンロードおよびインストールする際にも使用できます。
アプリケーションにタグ付けする	SaaSアプリケーションのタグ付け用に**sanctioned**[許可済み] という名前のタグが事前設定されています。SaaSアプリケーションとは、そのアプリケーション特性の詳細において**Saas=yes**と識別されているものを指しますが、許可済みタグはすべてのアプリケーションに使用可能なものです。

© 2019 Palo Alto Networks, Inc.

アプリケーションでサポートされる操作	の意味
	アプリケーションに*sanctioned* (許可)というタグを付け、例えば *SaaS* アプリケーションの利用状況レポートを検証する際やネットワーク上のアプリケーションを評価する際に、許可された *SaaS* アプリケーションのトラフィックと許可されていない *SaaS* アプリケーションのトラフィックとを区別します。 アプリケーションを選択して、**Edit Tags**(タグの編集)をクリックし、ドロップダウンから事前定義済みの**Sanctioned**(許可済み)タグを選択して、ネットワークで明示的に許可するアプリケーションを特定します。また、SaaS アプリケーション使用状況レポートを生成すると（「Monitor（監視）> PDF Reports（PDF レポート）> SaaS Application Usage（Saas アプリケーションの使用状況）」を参照）、ネットワーク上で使用されている許可済みのアプリケーションの統計値と未許可の SaaS アプリケーションの統計値を比較することができます。 アプリケーションを許可済みとタグ付けする場合、以下の制限が課せられます。 • 許可済みのタグは、アプリケーショングループに適用することができません。 • 許可済みのタグは**Shared**[共有] レベルでは適用することができません。デバイスグループあるいは仮想システムにつき1つのアプリケーションのみタグ付けすることができます。 • 許可済みのタグは、facebookコンテナアプリの一部であるfacebookメールなど、コンテナアプリに含まれるアプリケーションには使用することができません。 さらに、**Remove tag**[タグの除去] または**Override tag**[タグのオーバーライド] をすることも可能です。オーバーライドのオプションは、デバイスグループの設定をPanoramaからのプッシュにより継承したファイアウォールのみにおいて使用可能です。

アプリケーションの定義

ポリシーを適用する際にファイアウォールの評価対象とする新しいカスタムアプリケーションを**Add**[追加] する場合は、**Objects**[オブジェクト] > **Applications**[アプリケーション] のページを使用します。

新しいアプリケーション設定	の意味
Configuration [設定] タブ	
氏名	アプリケーション名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときにアプリケーションのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ピリオド、ハイフン、およびアンダースコアのみを使用してください。先頭は文字にする必要があります。
共有	以下に対してアプリケーションを公開する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

新しいアプリケーション設定	の意味
	• multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してアプリケーションが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してアプリケーションが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、このオブジェクトを継承するデバイス グループのこのアプリケーション オブジェクトの設定をオーバーライドすることを防ぐには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
の意味	アプリケーションの一般的な説明を入力します (最大 255 文字)。
カテゴリ	アプリケーションのカテゴリ (**email** や **database** など) を選択します。このカテゴリは、Top Ten Application Categories (トップ 10 のアプリケーション カテゴリ) チャートの生成に使用され、フィルタリングに使用できます (「ACC」を参照)。
サブカテゴリ	アプリケーションのサブカテゴリ (**email** や **database** など) を選択します。このサブカテゴリは、Top Ten Application Categories (トップ 10 のアプリケーション カテゴリ) チャートの生成に使用され、フィルタリングに使用できます (「ACC」を参照)。
テクノロジ	アプリケーションのテクノロジを選択します。
親アプリケーション	このアプリケーションの親アプリケーションを指定します。この設定は、セッションが親アプリケーションとカスタム アプリケーションの両方に一致する場合に適用されます。ただし、カスタム アプリケーションの方が詳細であるためカスタム アプリケーションがレポートされます。
リスク	アプリケーションに関連付けられているリスク レベル (1 = 最低 ~ 5 = 最高) を選択します。
特徴	アプリケーションを危険にさらす可能性のあるアプリケーションの特徴を選択します。各特徴の詳細は「特徴」を参照してください。
Advanced Tab (詳細タブ)	
ポート	アプリケーションで使用するプロトコルが TCP や UDP の場合、**Port**[ポート] を選択してプロトコルとポート番号の組み合わせを 1 つ以上入力します (1 行ごとに 1 エントリ)。一般的な形式は以下のとおりです。 *<protocol>/<port>* ここで、*<port>* は、1 つのポート番号または **dynamic** (動的ポート割り当ての場合) になります。 例 : TCP/dynamic または UDP/32

© 2019 Palo Alto Networks, Inc.

新しいアプリケーション設定	の意味
	セキュリティ ルールのサービス列に**app-default**を使用すると、この設定が適用されます。
IP プロトコル	TCP や UDP 以外の IP プロトコルを指定するには、**IP Protocol**[IP プロトコル] を選択してプロトコル番号 (1 ~ 255) を入力します。
ICMP タイプ	Internet Control Message Protocol バージョン 4 (ICMP) タイプを指定するには、**ICMP Type**[ICMPタイプ] を選択し、タイプの番号を入力します (範囲は 0 ~ 255)。
ICMP6 タイプ	Internet Control Message Protocol バージョン 6 (ICMPv6) タイプを指定するには、**ICMP6 Type**[ICMP6 タイプ] を選択し、タイプの番号を入力します (範囲は 0 ~ 255)。
まったくない	プロトコルに依存しないシグネチャを指定するには、**None**[なし] を選択します。
タイムアウト	アイドル状態のアプリケーションフローが停止するまでの秒数（範囲は0～604800秒）を入力します。0 は、アプリケーションのデフォルトのタイムアウトが使用されることを示します。この値は、すべてのケースで TCP および UDP 以外のプロトコルに使用されます。また、TCP タイムアウトと UDP タイムアウトが指定されていない場合は、TCP と UDP のタイムアウトに使用されます。
TCP タイムアウト	アイドル状態のTCPアプリケーションフローが停止するまでの秒数（範囲は0～604800秒）を入力します。0 は、アプリケーションのデフォルトのタイムアウトが使用されることを示します。
UDP タイムアウト	アイドル状態のUDPアプリケーションフローが停止するまでの秒数（範囲は0～604800秒）を入力します。0 は、アプリケーションのデフォルトのタイムアウトが使用されることを示します。
TCPハーフクローズド	最初のFINを受信してから、2つ目のFINまたはRSTを受信するまでの間、セッションがセッションテーブル内に保持される最大時間を入力します。タイマーが期限切れになるとセッションが閉じられます。 デフォルト:このタイマーがアプリケーションレベルで設定されていない場合、グローバル設定が使用されます（範囲は1～604800秒）。 この値がアプリケーション レベルで設定されている場合、その値でグローバル TCP Half Closed 設定がオーバーライドされます。
TCP待ち時間	2つ目のFINまたはRSTを受信してから、セッションがセッションテーブル内に保持される最大時間を入力します。タイマーが期限切れになるとセッションが閉じられます。 デフォルト:このタイマーがアプリケーションレベルで設定されていない場合、グローバル設定が使用されます（範囲は1～600秒）。 この値がアプリケーション レベルで設定されている場合、その値でグローバル TCP Time Wait 設定がオーバーライドされます。

© 2019 Palo Alto Networks, Inc.

新しいアプリケーション設定	の意味
スキャン	セキュリティプロファイル（ファイルタイプ、データパターン、およびウイルス）に基づいて、許可するスキャンタイプを選択します。
Signatures [シグネチャ] タブ	
★上のセグメントに訳文をまとめました★	**Add**[追加] をクリックして新しいシグネチャを追加し、以下の情報を指定します。 • **Signature Name**[シグネチャ名] – シグネチャの識別に使用する名前を入力します。 • **Comment**[コメント] – 任意で説明を入力します。 • **Ordered Condition Match**[順番が付けられた条件の一致] – シグネチャの条件の定義順序が重要である場合に選択します。 • **Scope**[範囲] – このシグネチャを現在の**Transaction**[トランザクション] のみに適用するか、またはユーザー**Session**[セッション] 全体に適用するかを選択します。 シグネチャの識別条件を指定するこれらの条件は、ファイアウォールがアプリケーションパターンを識別し、トラフィックを制御する場合に使用するシグネチャを生成する際に使用されます。 • **Add AND Condition (AND**条件を追加**)** または **Add OR Condition (OR**条件を追加**)**をクリックして条件を追加します。グループ内に条件を追加するには、グループを選択して **Add Condition**[条件の追加] をクリックします。 • ドロップダウンリストから**Operator**[演算子] を選択します。選択肢には**Pattern Match**[パターンマッチ]、**Greater Than**[超過]、**Less Than**[未満]、および**Equal To**[等しい] があり、それぞれについて以下のオプションを指定します。 （パターン マッチの場合のみ） • **Context**[コンテクスト] – 使用可能なコンテクストから選択します。これらのコンテクストは動的コンテンツアップデートにより更新されます。 • **Pattern**[パターン] – カスタムアプリケーションに適用された、一意のコンテクスト文字列を指定するための正規表現を指定します。 コンテクスト特定のため、パケット キャプチャを実行してください。正規表現のパターンのルールに関する詳細は「パターンのルールの構文」を参照してください。 （Greater Than（超過）、Less Than（未満）の場合） • **Context**[コンテクスト] – 使用可能なコンテクストから選択します。これらのコンテクストは動的コンテンツアップデートにより更新されます。 • **Value**[値] – 一致検索を行う値を指定します（範囲は0～4294967295）。 • **Qualifier and Value** –（任意）修飾子/値のペアを追加します。 （Equal To（等しい）の場合のみ） • **Context**（コンテクスト）– TCP または UDP 宛ての不明な要求や応答（unknown-req-tcp など）、または動的コンテンツ アップデートにより

© 2019 Palo Alto Networks, Inc.

新しいアプリケーション設定	の意味
	入手可能な追加コンテクスト（dnp3-req-func-code など）から選択します。 TCPまたはUDPの不明な要求や応答の場合は、以下を指定します。 • **Position**[位置] – ペイロードの最初の 4 バイトまたは 2 番目の 4 バイトのいずれかを選択します。 • **Mask**[マスク] – 4 バイトの 16 進数値を指定します (たとえば、0xffffff00)。 • **Value**[値] – 4 バイトの 16 進数値を指定します (たとえば、0xaabbccdd)。 他のコンテクストに関しては、そのアプリケーションに関連のある**Value**[値] を指定します。 グループ内で条件を移動するには、条件および **Move Up**[上へ] または **Move Down**[下へ] を選択します。グループを移動するには、グループを選択して **Move Up**[上へ] または **Move Down**[下へ] を選択します。グループ間で条件を移動することはできません。

アプリケーションの使用目的がアプリケーション オーバーライド ルールのみである場合、アプリケーションのシグネチャを指定する必要はありません。

© 2019 Palo Alto Networks, Inc.

Objects > Application Groups [オブジェクト > アプリケーション グループ]

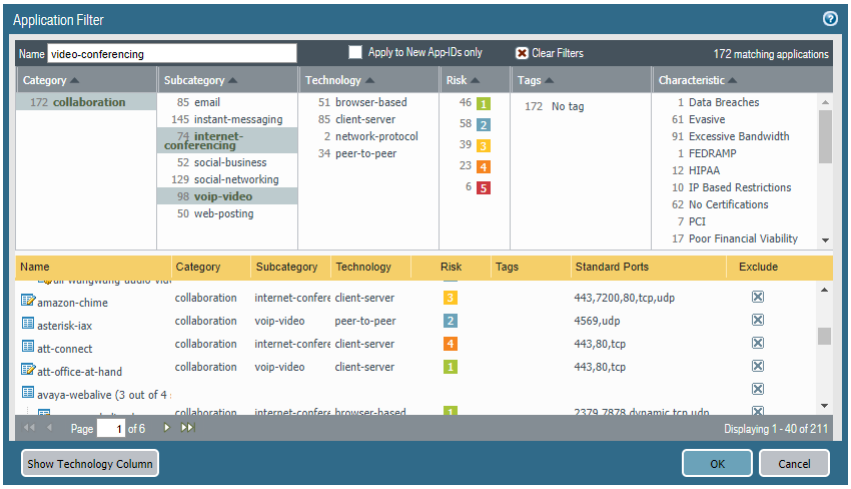
セキュリティ ポリシーの作成を簡略化するには、アプリケーション グループを作成して、同じセキュリティ設定が必要なアプリケーションをまとめることができます (新しいアプリケーションを定義するには、「アプリケーションの定義」を参照してください) 。

新しいアプリケーション グループ設定	の意味
氏名	アプリケーション グループを表す名前 (最大 31 文字) を入力します。この名前は、セキュリティ ポリシーを定義するときにアプリケーションのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有	以下に対してアプリケーショングループを公開する場合は、このオプションを選択します。 multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してアプリケーショングループが公開されます。 Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してアプリケーショングループが公開されます。
オーバーライドの無効化 (Panoramaのみ)	このアプリケーション グループ オブジェクトの設定が、このオブジェクトを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
アプリケーション [applications]	**Add**[追加] をクリックし、このグループに含めるアプリケーション、アプリケーション フィルタ、および他のアプリケーション グループを選択します。

© 2019 Palo Alto Networks, Inc.

Objects > Application Filters [オブジェクト > アプリケーションフィルタ]

アプリケーション フィルタは、繰り返される検索を簡略化するのに役立ちます。アプリケーション フィルタを定義するには、新しいフィルタを **Add**（追加）して、その名前を入力します。ウィンドウの上部で、フィルタリングの基準として使用する項目をクリックします。たとえば、Collaboration [コラボレーション]カテゴリのみをリストに表示するには、**collaboration** をクリックします。



その他の列にフィルタを適用するには、列のエントリを選択します。フィルタリングは連続的で、カテゴリ フィルタ、次にサブカテゴリ フィルタ、テクノロジー フィルタ、リスク フィルタ、タグ、最後に特性フィルタの順に適用されます。

選択したフィルタに応じて、ページに表示されるアプリケーションのリストが自動的に更新されます。

© 2019 Palo Alto Networks, Inc.

Objects > Services [オブジェクト > サービス]

特定のアプリケーションのセキュリティ ポリシーを定義する場合、1 つ以上のサービスを選択して、アプリケーションで使用できるポート番号を制限できます。デフォルトのサービスは、**any** (すべて) で、すべての TCP ポートと UDP ポートが許可されます。HTTP サービスと HTTPS サービスは事前に定義されていますが、他のサービスの定義を追加することができます。一緒に割り当てられることが多いサービスをサービス グループにまとめることで、セキュリティ ポリシーの作成を簡略化できます (「Objects (オブジェクト) > ServiceGroups」を参照) 。

さらに、サービス オブジェクトを使用してサービス ベースのセッション タイムアウトを指定することができます。つまり、同じグループのユーザーまたはグループが同じ TCP または UDP サービスを使用していても、異なるタイムアウトを適用することができます。 アプリケーション ベースのセキュリティ ポリシーをカスタム アプリケーションと共にアプリケーション ベースのセキュリティ ポリシーに適用すると、カスタム アプリケーションのタイムアウトを容易に維持できます。

以下の表では、サービス設定について説明します。

サービス設定	の意味
氏名	サービス名 (最大 **63** 文字) を入力します。この名前は、セキュリティ ポリシーを定義するときにサービスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	サービスの説明を入力します (最大 1023 文字)。
共有	以下に対してサービスオブジェクトを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してサービスオブジェクトが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対してサービスオブジェクトが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、オブジェクトを継承するデバイス グループのこのサービス オブジェクトの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
PROTOCOL	サービスで使用するプロトコル (**TCP** または **UDP**) を選択します。
Destination port	サービスで使用する宛先ポート番号 (0 ~ 65535) またはポート番号の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたはポートの範囲はコンマで区切ります。宛先ポートは必須です。
Source port	サービスで使用する送信元ポート番号 (0 ~ 65535) またはポート番号の範囲 (ポート 1 ~ ポート 2) を入力します。複数のポートまたはポートの範囲はコンマで区切ります。送信元ポートは任意です。

© 2019 Palo Alto Networks, Inc.

サービス設定	の意味
セッション タイムアウト	以下のサービスに対するセッション タイムアウトを定義します。 • **Inherit from application**（アプリケーションから継承）（デフォルト）–サービス ベースのタイムアウトは適用されず、アプリケーションのタイムアウトが適用されます。 • **Override**（オーバーライド）–サービスに対するカスタム セッション タイムアウトを定義します。TCPタイムアウト、TCP ハーフクローズド、および TCP 待機時間フィールドへの値の入力を続行します。
次の設定は、アプリケーション タイムアウトを無効にして、サービスのカスタム セッション タイムアウトを作成する場合にのみ表示されます。	
TCP タイムアウト	データの送信が開始された後に TCP セッションを開いたままにできる最大時間を秒単位で設定します。これが期限切れになるとセッションが閉じます。 範囲は 1 ~ 604800 です。デフォルト値は 3600 秒です。
TCPハーフクローズド	接続の一方の側だけが接続を終了しようとしたときにセッションが開いたままになる最大時間（秒）を設定します。 この設定は次の場合に適用されます。 • ファイアウォールが最初の FIN パケットを受信した後（接続の一方の側がセッションを終了しようとしていることを示す）、第 2 の FIN パケットを受信する前（接続の相手側がセッションを終了していることを示す）、 • RST パケットを受信する前の期間（接続のリセットを示す）。 タイマーが期限切れになるとセッションが閉じます。 範囲は 1 ~ 604800 です。デフォルト値は120 秒です。
TCP 待機時間	セッションを終了するために必要な 2 つの FIN パケットのうちの 2 番目を受信した後、または接続をリセットするために RST パケットを受信した後、セッションが開いたままになる最大時間を、秒単位で設定します。 タイマーが期限切れになるとセッションが閉じます。 範囲は 0 ~600 です。デフォルト値は 15 秒です。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Service Groups（サービス グループ）

セキュリティ ポリシーの作成を簡略化するには、セキュリティ設定が同じであることが多いサービスをサービス グループにまとめます。新しいサービスを定義する方法については、「Objects（オブジェクト）> Services（サービス）」を参照してください。

以下の表では、サービス グループ設定について説明します。

サービス グループ設定	の意味
氏名	サービス グループ名 (最大 63 文字) を入力します。この名前は、セキュリティ ポリシーを定義するときにサービスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有	以下に対してサービスグループを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してサービスグループが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対してサービスグループが公開されます。
オーバーライドの無効化（Panoramaのみ）	管理者が、オブジェクトを継承するデバイス グループのこのサービス グループ オブジェクトの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
サービス	**Add**[追加] をクリックしてグループにサービスを追加します。ドロップダウンリストから選択するか、ドロップダウンリストの下部にある **Service**[サービス] をクリックして設定を指定します。設定の詳細は、Objects（オブジェクト）> Services（サービス）を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects > Tags [オブジェクト > タグ]

タグを使用すると、キーワードまたは語句を使用してオブジェクトをグループ化できます。アドレス オブジェクト、アドレス グループ（静的および動的）、アプリケーション、ゾーン、サービス、サービス グループ、およびポリシー ルールにタグを適用できます。SD-WAN インターフェイス プロファイルを使用して、イーサネット インターフェースにリンク タグを適用することもできます。タグを使用すると、オブジェクトをソートまたはフィルタリングしたり、オブジェクトを色で視覚的に識別したりできます。タグに色を付けると、**Policy** (ポリシー) タブに表示されるオブジェクトに背景色が付けられます。

タグを使ってルールをグループ化するには、事前にそのタグを作成しておく必要があります。タグでグループ化したルールを適用した後、**View Rulebase as Groups** (ルールベースをグループとして表示)し、割り当てられたタグに基づいてポリシー ルールベースが表示されることを確認します。ルールベースをグループとして閲覧する際、ポリシーの順序と優先順位が保持されます。このビューでグループ タグを選択すれば、すべてのルールをタグでグループ化して表示できます。

アプリケーションのタグ付けには**Sanctioned**[許可済み] という事前設定済みのタグを使用可能です（**Objects** > **Applications**[オブジェクト > アプリケーション]）。これらのタグは、正確なMonitor（監視）> PDF Reports（PDF レポート）> SaaS Application Usage（Saas アプリケーションの使用状況）に必要です。

知りたい内容	以下を参照
タグの作成方法	タグの作成
ルールベースをグループとして表示する方法は？	ルールベースをグループとして表示
タグ付けされたルールを検索する。 タグを使用してルールをグループ分けする。 ポリシーで使用されているタグを確認する。 タグをポリシーに適用します。	タグの管理
その他の情報をお探しですか？	「ポリシー」を参照してください。 SD-WAN リンクについては Create a Link Tag (リンク タグの作成) を参照してください。

タグの作成

- **Objects** (オブジェクト) > **Tags** (タグ)

Tags (タグ)を選択し、タグの作成、色の割り当て、タグの削除、名前の変更、コピーができます。各オブジェクトには最大 64 個のタグを付けることができます。オブジェクトに複数のタグがある場合、適用された最初のタグの色が表示されます。

ファイアウォールで、**Tags** (タグ)タブを選択すると、ファイアウォール上でローカルに定義したタグ、または Panorama からファイアウォールにプッシュされたタグが表示されます。Panorama の**Tags** (タグ)タブには、Panorama で定義したタグが表示されます。このタブには、ファイアウォール上に定義された VM 情報の送信元から動的に取得され動的 アドレス グループを形成するタグ、または XML あるいは REST API を使用して定義されたタグは表示されません。

© 2019 Palo Alto Networks, Inc.

新規のタグを作成すると、ファイアウォールまたはPanoramaで現在選択されている仮想システムまたはデバイスグループで、そのタグが自動的に作成されます。

タグ設定	の意味
氏名	一意のタグ名 (最大 127 文字) を入力します。名前では大文字と小文字は区別されません。
共有	以下に対してタグを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects (オブジェクト)** タブで選択した **Virtual System (仮想システム)** のみに対してタグが公開されます。 • Panorama 上の各デバイス グループ。このオプションを無効化 (クリア) すると、**Objects (オブジェクト)** タブで選択した **Device Group (デバイスグループ)** のみに対してタグが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、このタグを継承するデバイス グループのこのタグの設定をオーバーライドすることを防ぐには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このタグを継承するデバイス グループの設定をオーバーライドできます。
カラー	ドロップダウン リストのカラー パレットから、色を選択します (デフォルトは None (なし)) 。
コメント	タグの用途を示すラベルまたは説明を追加します。

- タブの追加:タグを**Add (追加)**して次の各フィールドを入力します：

  Policies[ポリシー] タブでポリシーを作成または編集する際に、新規のタグを作成することもできます。タグは、現在選択されているデバイス グループまたは仮想システムで自動的に作成されます。
- タグの編集:編集、名称変更、あるいは色を割り当てるタグをクリックします。
- タグの削除:**Delete (削除)**をクリックしてタグを選択します。事前定義されたタグを削除することはできません。
- タグの移動またはコピー:タグを移動またはコピーするオプションを使用すると、マルチ仮想システムが有効になっているファイアウォール上の異なるデバイス グループまたは仮想システムにタグをコピーまたは移動できます。

  Move or Clone (移動またはコピー)してタグを選択します。**Destination (宛先)** となる場所 (デバイス グループまたは仮想システム) を選択します。検証プロセスにおいて、エラーの表示を行う前にオブジェクトに含まれるすべてのエラーを検出させたい場合は、**Error out on first detected error in validation (検出中に最初にエラーを検出した時点でエラーを表示)** のオプションを無効化 (クリア) します。デフォルトではこのオプションが有効になっているため、検証プロセスは最初のエラーが検出された時点で停止され、そのエラーのみが表示されます。
- タグをオーバーライドする/元に戻す (Panorama のみ) ：タグの作成時に **Disable override (オーバーライドの無効化)** オプションを選択していない場合は、**Override (オーバーライド)**オプションを使用できます。**Override (オーバーライド)**オプションを使用すると、共有または先祖デバイス グループから継承したタグに割り当てられたカラーをオーバーライドできます。現在のデバイス グループが**Location (場所)**になります。また、**Disable override (オーバーライドを無効化)**して今後のオーバーライドの試みを防ぐこともできます。

  タグに加えた最近の変更を取り消す場合は変更を**Revert (取り消し)**ます。タグを元に戻すと、**Location**[場所] フィールドに、タグの継承元のデバイス グループまたは仮想システムが表示されます。

© 2019 Palo Alto Networks, Inc.

ルールベースをグループとして表示

- **Policies (ポリシー) > <Rulebase Type> (<ルールベース タイプ>)**

View Rulebase as Groups (ルールベースをグループとして表示)すれば、グループ タグを使ってポリシー ルールベースを表示できます。ルールベースをグループとして閲覧する際、ポリシーの順序と優先順位が保持されます。このビューでグループ タグを選択すれば、すべてのルールをタグでグループ化して表示できます。

ルールベースをグループとして表示しながら、**Group** (グループ)をクリックすれば選択したタグ グループ内のすべてのルールを移動、変更、削除、コピーできます。次の表は、ルールベースをグループとして表示する際に利用できるルールの管理オプションを示しています。

オプション	の意味
グループ内の結果を別のルールベースあるいはデバイスグループに移動	選択したルールベースあるいはデバイスグループ内のすべてのポリシールールを別のタグ グループに移動させます。
すべてのルールのグループを変更	選択したタグ グループ内のすべてのルールを別のタグ グループに移動させます。
グループ内のすべてのルールを移動	ルールベース内の選択したタグ グループに含まれるすべてのルールを移動させます。
グループ内のすべてのルールを削除	選択したタグ グループ内のすべてのルールを削除します。
グループ内のすべてのルールをコピー	選択したタグ グループ内のすべてのルールをコピーします。

グループ内の結果を別のルールベースあるいはデバイスグループに移動

ルールベースを整理する必要がある場合、移動したいルールを含んでいるタグ グループを選択して**Move Rules in Group to Different Rulesbase or Device Group** (グループ内のルールを別のルールベースあるいはデバイスグループに移動)し、（個々のルールを個別に移動するのではなく）それらを別のルールベースあるいはデバイスグループに割り当て直します。タグ グループ内のルールを別のデバイスグループに移動する前に、デバイスグループがすでに存在していなくてはなりません（移動中は作成できません）。さらに、タグ グループ内のルールを同じデバイスグループ内の別のルールベースに移動できます。

ルールを別のルールベースあるいはデバイスグループに移動させる場合は次の項目を入力します：

項目	の意味
宛先	ポリシールールを移動させる対象のデバイスグループです。
（Panorama のみ）宛先タイプ	ルールを宛先デバイスグループの**Pre-Rulebase** (プレ ルールベース)あるいは**Post-Rulebase** (ポスト ルールベース)のどちらに移動するのか選択します。
ルール順序	ルールをルールベースのどこに移動するのか選択します。選択肢は以下のとおりです。 • **Move Top** (最上部へ移動)—ルールを宛先デバイスグループのルールベースの一番上に移動します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **Move Bottom** (最下部へ移動)–ルールを宛先デバイスグループのルールベースの最後に移動します。 • **Before Rule** (ルールの前)–ルールを宛先デバイスグループのルールベース内で選択したルールの前に移動します。 • **After Rule** (ルールの後)–ルールを宛先デバイスグループのルールベース内で選択したルールの後に移動します。
検証で最初に検出されたエラーに起因するエラーが発生しました	このボックスにチェックを入れれば、検証中にエラーが発生した場合にエラーを表示する方法を指定できます。チェックを入れた場合、各エラーが個別に表示されます。チェックを入れない場合、各エラーが集約されて単一のエラーとして表示されます。 検証中にエラーが検出されるとルールの移動ジョブが失敗し、宛先デバイスグループにルールが移動されません。

すべてのルールのグループを変更

各ルールを編集するのではなく、**Change Group of All Rules** (すべてのルールのグループを変更)してポリシールールセット全体をあるタグ グループから既存の別のタグ グループに移動させます。新しいタグ グループに移動させる際、タグ グループ ルールのルールの順序が保持されますが、新しいルールを宛先タグ グループ内のルールの前に置くか、後ろに置くかを選択できます。

ルールを別のタグ グループに移動させるには、宛先タグ グループと移動させるルールの配置場所を指定します。

項目	の意味
表示順序の Group (グループ) を選択します	宛先タグ グループを選択します。
最上部へ移動	**Move Top** (最上部へ移動)はルールを宛先タグ グループの一番上に挿入します。
最下部へ	**Move bottom** (最下部へ移動)はルールを宛先タグ グループの一番下に挿入します。

グループ内のすべてのルールを移動

各ルールの順序を個別に変えるのではなく、**Move All Rules in Group** (グループ内のすべてのルールを移動)して選択中のタグ グループ内のすべてのルールをルール階層の上下に移動させます。新しいタグ グループに移動させる際、タグ グループ ルール内の移動されたルールの順序が保持されますが、ルールを宛先タグ グループ内のルールの前に置くか、後ろに置くかを選択できます。

ルールを移動させるには、宛先タグ グループと移動させるルールの配置場所を指定します。

項目	の意味
表示順序の Group (グループ) を選択します	宛先タグ グループを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
最上部へ移動	**Move Top** (最上部へ移動)はルールを宛先タグ グループの前に挿入します。
最下部へ	**Move bottom** (最下部へ移動)はルールを宛先タグ グループの後に挿入します。

グループ内のすべてのルールを削除

Delete All Rules in Group (グループ内のすべてのルールを削除)で選択したタグ グループに関連する使用していない、あるいは不要なルールを削除することで、セキュリティリスクを減らし、ポリシー ルールベースを整理し、ルールの管理を簡単にすることができます。

グループ内のすべてのルールをコピー

タグ グループ内の既存のポリシールールを手作業で作成し直すのではなく、**Clone All Rules in Group** (グループ内のすべてのルールをコピー)すれば、任意のルールベースおよびデバイスグループに含まれる選択済みのタグ グループ内のルールを素早く複製できます。タグ グループ内のルールを別のデバイスグループにコピーする前に、デバイスグループがすでに存在していなくてはなりません（コピー中は作成できません）。さらに、タグ グループ内のルールを同じデバイスグループ内の別のルールベースにコピーできます。

コピーしたルールには、ルール名と次の書式が付与されます：`<Rule Name>-1`.最初にコピーしたルールと同じ場所にルールをコピーし、かつ名前が変化しない場合、名前が付与されます。例えば、`<Rule Name>-2`、`<Rule Name>-3`などです。

ルールをコピーする場合は以下のフィールドを設定します。

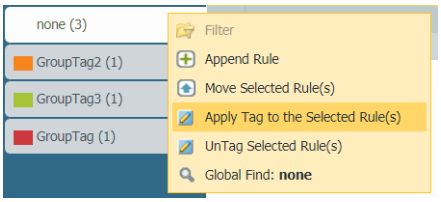
項目	の意味
宛先	コピー対象のポリシールールのターゲット デバイスグループ。
（Panorama のみ）宛先タイプ	ルールを宛先デバイスグループの**Pre-Rulebase** (プレ ルールベース)あるいは**Post-Rulebase** (ポスト ルールベース)のどちらにコピーするのか選択します。
ルール順序	ルールをルールベースのどこにコピーするのか選択します。選択肢は以下のとおりです。 • **Move Top** (最上部へ移動)–コピーしたルールを宛先デバイスグループのルールベースの一番上に挿入します。 • **Move Bottom** (最下部へ移動)–コピーしたルールを宛先デバイスグループのルールベースの最後に挿入します。 • **Before Rule** (ルールの前)–コピーしたルールを宛先デバイスグループのルールベース内で選択したルールの前に挿入します。 • **After Rule** (ルールの後)–コピーしたルールを宛先デバイスグループのルールベース内で選択したルールの後に挿入します。
検証で最初に検出されたエラーに起因するエラーが発生しました	このオプションを選択すれば、検証中にエラーが発生した場合にエラーを表示する方法を指定できます。有効な場合、各エラーが個別に表示されます。無効（クリア）な場合、各エラーが集約されて単一のエラーとして表示されます。 検証中にエラーが検出されるとルールのコピージョブが失敗し、宛先デバイスグループにルールがコピーされません。

© 2019 Palo Alto Networks, Inc.

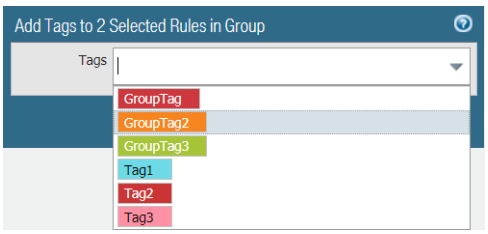
タグの管理

ルールをグループ タグでグループ化した際に実行できるアクションを次の表に示します。

- ルールにタグ付けする。
  1. **View Rules as Groups** (ルールをグループとして表示)を選択します。
  2. 右ペインで一つ以上のルールを選択します。
  3. グループ タグのドロップダウンリストで**Apply Tag to the Selected Rules** (選択中のルールにタグを適用)します。

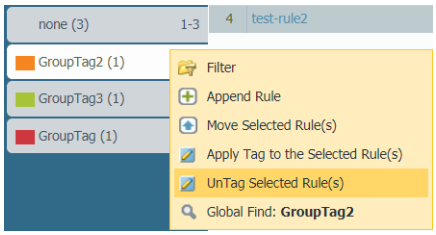


  4. 選択したルールにタグを追加します。



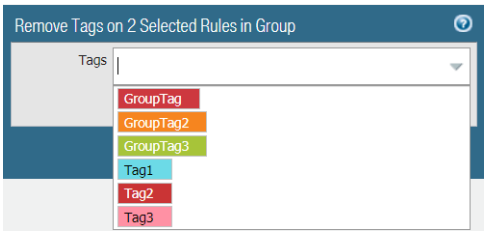
- グループ タグに割り当てられたルールを表示します。
  1. **View Rulebase as Groups** (ルールベースをグループとして表示)してルールが割り当てられているグループ タグを表示します。
  2. 右ペインが更新され、選択したいずれかのタグを含むルールおよびグループ タグが表示されます。
  3. グループ タグを選択し、対象のグループに割り当てられているルールを表示します。グループ タグが割り当てられていないルールは**none** (なし)グループのところにリストアップされます。

- ルールのタグを外す。
  1. **View Rulebase as Groups** (ルールベースをグループとして表示)してルールが割り当てられているグループ タグを表示します。
  2. 右ペインで一つ以上のルールを選択します。
  3. グループ タグのドロップダウンリストで**Apply Tag to the Selected Rules** (選択中のルールにタグを適用)します。



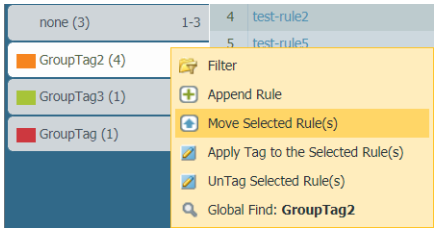
  4. 選択したルールのタグを削除します。さらに、ルールに割り当てられたタグを**Delete All** (すべて削除)することができます。

© 2019 Palo Alto Networks, Inc.



- タグを使用してルールを並べ替える。

  View Rulebase as Groups (ルールベースをグループとして表示)しながら、グループ タグ内のルールを一つ以上選択し、ルール番号にカーソルを合わせてドロップダウンリストで**Move Selected Rule(s)** (選択中のルールを移動)を選択します。選択中のグループ タグに含まれるすべてのルールを移動する場合は、ルールを選択しないでください。



  move rule (ルールの移動) ウィンドウのドロップダウンリスト リストからグループ タグを選択し、ドロップダウンリスト リストで選択したタグの **Move Before** (前に移動) するのか、**Move After** (後に移動) するのかを選択します。

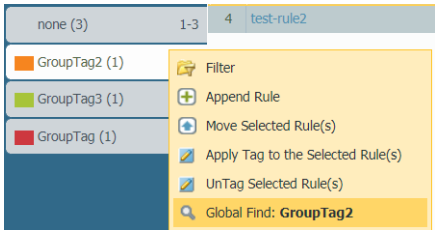
- 選択したタグに適用する新しいルールを追加する。

  View Rulebase as Groups (ルールベースをグループとして表示)しながら、グループ タグにカーソルを合わせてドロップダウンリストで**Append Rule** (ルールを付与)を選択します。

  グループ タグに割り当てられたルールのリストの最後に新しいルールが追加されます。

- グループ タグを検索します。

  View Rulebase as Groups (ルールベースをグループとして表示)しながら、グループ タグにカーソルを合わせてドロップダウンリストで**Global Find** (グローバル検索)を選択します。



- タグ設定バンドルのエクスポート。

  管理ロールは、**PDF/CSV** 形式でオブジェクト構成テーブルをエクスポートし、フィルタを適用して、必要な列だけを含むようにテーブル出力をカスタマイズすることができます。エクスポート ダイアログに表示される列のみがエクスポートされます。Export Configuration Table Data (設定バンドルデータのエクスポート) を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects > External Dynamic Lists [オブジェクト > 外部動的リスト]

外部動的リストは、インポートされた IP アドレス、URL、またはドメイン名のリストに基づくアドレス オブジェクトです。ポリシー ルールでこれらの情報を使用してトラフィックをブロックまたは許可できます。このリストは、ファイアウォールからアクセスできる Web サーバーに保存されたテキスト ファイルでなければなりません。デフォルトでは、ファイアウォールは管理（MGT）インターフェイスを使用してこのリストを取得します。

Palo Alto Networks はアクティブな脅威防止ライセンスを持つユーザーに、組み込み型の悪意のあるホストをブロックするために使用できる動的な IP リストを複数提供しています。このリストは、最新の脅威の調査に基づいて毎日更新されます。

IP アドレス リストをポリシー ルールの送信元および宛先のアドレス オブジェクトとして使用できます。URL リストを URL フィルタリング プロファイル（Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> URL Filtering（URL フィルタリング））で使用したり、セキュリティ ポリシー ルールの一致条件として使用したりできます。ドメイン リストを Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Anti-Spyware Profile（アンチスパイウェア プロファイル）で使用して、指定したドメイン名のシンクホールを実行できます。

すべてのセキュリティ ポリシー ルールの中で一意の送信元を持つ最大 30 個の外部動的リストを各ファイアウォール モデルで使用できます。ファイアウォールでサポートされる、各リスト タイプの最大エントリ数はファイアウォール モデルによって異なります（各外部動的リスト タイプのさまざまなファイアウォール制限を参照してください）。ポリシーで外部動的リストを使用する場合、リストのエントリのみが最大制限にカウントされます。モデルでサポートされる最大エントリ数を超えた場合、ファイアウォールはシステム ログを生成し、制限を超えたエントリをスキップします。ポリシーで現在使用されている IP アドレス、ドメイン、および URL の数と、ファイアウォールでサポートされる合計数を確認するには、**List Capacities**（容量の表示）をクリックしてください（ファイアウォールのみ）。

外部動的リストは評価順に上から下に表示されます。方向ボタン（ページ下部）を使ってリストの順序を変更できます。そうすることで、キャパシティの上限に達する前に EDL で最も重要な項目を確実にコミットできるようになります。

リストをタイプでグループ化している際は *EDL* の順序を変更できません。

外部動的リストをホストするサーバーから最新バージョンの外部動的リストを取得するには、外部動的リストを選択し、**Import Now**（今すぐインポート）します。

Palo Alto Networks の悪意のある *IP* アドレス フィードの設定を削除、コピー、編集することはできません。

新しい外部ダイナミックリストを作成して**Add**（追加）し、以下の表に示す設定を行います。

外部ダイナミックリストの設定	の意味
氏名	外部動的リストを識別する名前（最大32文字）を入力します。この名前は、リストを使用してポリシーを適用するときにこのリストを識別します。
共有	以下に対して外部動的リストを公開する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

外部ダイナミックリストの設定	の意味
	• multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対して外部動的リストが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対して外部動的リストが公開されます。
オーバーライドの無効化（Panoramaのみ）	この外部ダイナミックリスト オブジェクトの設定が、このオブジェクトを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでこのオプションは無効（クリア）になっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
ソース URL のテスト（ファイアウォールのみ）	外部ダイナミックリストをホストするサーバーにファイアウォールが接続できることを確認するには、これをクリックします。 このテストでは、サーバーが正常に認証されたかどうかは確認されません。
Create List（リストの作成）タブ	

タイプ
 	
IP アドレス、URL、およびドメイン名を 1 つのリストに混在させることはできません。それぞれのリストには1つのタイプのエントリのみを含めることができます。
	以下の外部動的リストのタイプから選択してください。
	• **Predefined IP List**（事前定義済み **IP** リスト）– このタイプのリストは、Palo Alto Networks の悪意のある IP アドレス フィードまたは高リスク IP アドレス フィードをリスト エントリのソースとして使用します（アクティブな脅威阻止ライセンスが必要）。
	• **IP List**（**IP** リスト）– 各リストに IPv4 および IPv6 アドレス空間の IP 範囲および IP サブネットを含めることができます。リストには、1行につきIPアドレス、範囲、またはサブネットのうち1つのみが記載されている必要があります。例:
	
	`192.168.80.150/32`
	`2001:db8:123:1::1 or 2001:db8:123:1::/64`
	`192.168.80.0/24 (this indicates all addresses from 192.168.80.0 through 192.168.80.255)`
	`2001:db8:123:1::1 - 2001:db8:123:1::22`
	
	「92.168.20.0/24」、「192.168.20.40-192.168.20.50」など、サブネットや IP アドレス範囲は 1 つの IP アドレス エントリとしてカウントされ、複数の IP アドレスとしてはカウントされません。
	• **Domain List**[ドメインリスト] – それぞれのリストでは1行につき1つまでのドメイン名エントリを持たせることが可能です。例:
	
	`www.p301srv03.paloalonetworks.com`
	`ftp.example.co.uk`
	`test.domain.net`
	
	外部動的リストに含まれるドメインリストについて、ファイアウォールはタイプがスパイウェアかつ重大度が中のカスタムシグネチャのセット

© 2019 Palo Alto Networks, Inc.

外部ダイナミックリストの設定	の意味

	を作成するため、ドメインのカスタムリストをシンクホールにかけることができます。
	• **URL List**[URLリスト] – それぞれのリストでは1行につき1つまでのURLエントリを持たせることが可能です。例:
	`financialtimes.co.in`
	`www.wallaby.au/joey`
	`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`
	`*.example.com/*`
	それぞれのURLリストにつき、デフォルトアクションは許可に設定されています。デフォルト アクションを編集するには、「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> URL Filtering（URL フィルタリング）」を参照してください。

の意味	外部動的リストの説明を入力します（最大255文字）。
送信元	テキスト ファイルが含まれている HTTP または HTTPS URL パスを入力します。例：http://192.0.2.20/myfile.txt。 • 外部ダイナミックリストが事前定義済み IP リストの場合、リスト ソースとして**Palo Alto Networks - High risk IP addresses (**高リスク **IP** アドレス**)**あるいは**Palo Alto Networks - Known malicious IP addresses (**悪意のある既知の **IP** アドレス**)**を選択します。 • 外部動的リストがドメイン リストである場合、**Automatically expand to include subdomains (**自動的に展開してサブドメインを含める**)**がデフォルト設定になります。このオプションにより、PAN-OS が EDL ファイルでリストアップされているドメイン名の低レベル コンポーネントをすべて評価できるようになります。 *EDL* にサブドメインが含まれている場合、展開されたこれらの項目が、アプライアンス モデルの容量に加味されます。サブドメインを手動で定義する場合はこの機能を無効化できます。しかし、リストで明示的に定義していないサブドメインはポリシールールによって評価されません。
証明書プロファイル	外部ダイナミックリストに HTTPS URL が含まれる場合、既存の証明書プロファイルを選択（ファイアウォールおよび Panorama）するか、新しい **Certificate Profile**（証明書プロファイル）を作成（ファイアウォールのみ）して、リストをホストする Web サーバーを認証します。証明書プロファイルの設定方法の詳細は、「Device（デバイス）> Certificate Management（証明書管理）> Certificate Profile（証明書プロファイル）」を参照してください。 デフォルト:なし（証明書プロファイルの無効化） ポリシーを適用するために使用できる外部ダイナミックリストの数を最大化するには、同じソース *URL* を使用する外部ダイナミックリストを、同じ証明書プロファイルを使用して認証します。これにより、このリストは *1* つの外部ダイナミックリストとしてカウントされます。同じソース

© 2019 Palo Alto Networks, Inc.

外部ダイナミックリストの設定	の意味
	URL からの外部ダイナミックリストが、異なる証明書プロファイルを使用している場合、そのリストはそれぞれ一意の外部ダイナミックリストとしてカウントされます。
Client Authentication [クライアントの認証]	基本 HTTP 認証を要求する外部ダイナミックリスト ソースにアクセスするときにファイアウォールで使用するユーザー名とパスワードを追加するには、このオプションを選択します（デフォルトでは無効）。この設定は、外部ダイナミックリストに HTTPS URL が含まれる場合にのみ使用できます。 • **Username**（ユーザー名）– リストにアクセスするための有効なユーザー名を入力します。 • **Password/Confirm Password**（パスワード/パスワード再入力）– ユーザー名のパスワードを入力し、確認します。
アップデートを確認	ファイアウォールがWebサーバーからリストを取得する頻度を指定します。ファイアウォールがリストを取得する間隔は、5分、毎日、毎週、または毎月に設定できます。 **Hourly**（毎時）（デフォルト）、**Five Minute**（5 分）、**Daily**（毎日）、**Weekly**（毎週）、または**Monthly**（毎月）で設定できます。ファイアウォールは、最後のコミットが過去 15 分間以内に行われなかった場合、直ちに設定への変更を自動的にコミットします。 最後の変更が最後の 15 分以内であった場合、最後のコミットの 15 分後にコミットが発生します。リストを参照するポリシールールはすべて更新されるため、ファイアウォールは正常にポリシーを適用することができます。 事前定義済み *IP* リストでは頻度を設定する必要はありません。アクティブな脅威防御ライセンスがあれば、ファイアウォールはコンテンツ更新を動的に受信します。
List Entries and Exceptions（リスト エントリおよび例外）タブ	
リスト エントリ	外部ダイナミックリストのエントリを表示します。 • リスト例外としてエントリを追加する – 最大 100 個のエントリを選択し、送信（ ）をクリックします。 • 項目に関する AutoFocus™ 脅威インテリジェンス サマリーを表示する – エントリにマウス カーソルを移動し、ドロップダウン リストをクリックして、**AutoFocus** をクリックします。項目のサマリーを表示するには、AutoFocus ライセンスを持っており、AutoFocus 脅威インテリジェンスを有効化する必要があります（**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**を選択して**AutoFocus**設定を編集）。 • IP アドレス、ドメイン、または URL が外部ドメインリストに含まれているかどうかを確認する – フィルタ フィールドに値を入力し、フィルタの適用（ ）をクリックします。フィルタをクリア（[X]）すると、完全なリストの表示に戻ります。
手動例外	外部ダイナミックリストの例外を表示します。 • 例外を編集する – 例外をクリックして、変更を加えます。 • 例外を手動で入力する – 新しい例外を手動で **Add**（追加）します。

© 2019 Palo Alto Networks, Inc.

外部ダイナミックリストの設定	の意味
	• 手動例外リストから例外を削除する – 例外を選択して **Delete** (削除) します。 • IP アドレス、ドメイン、または URL が手動例外リストに含まれているかどうかを確認する – フィルタ フィールドに値を入力し、フィルタの適用 (➡) をクリックします。フィルタをクリア ([X]) すると、完全なリストの表示に戻ります。手動例外リストに重複エントリがある場合、外部ダイナミックリストへの変更を保存することはできません。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）

ポリシーに適用して使用する、データパターン、脆弱性とスパイウェアのシグネチャ、およびURLカテゴリをカスタマイズして作成します。

- Objects > Custom Objects > Data Patterns [オブジェクト > カスタム オブジェクト > データ パターン]
- Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> Spyware/Vulnerability（スパイウェア/脆弱性）
- Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カテゴリ]

Objects > Custom Objects > Data Patterns [オブジェクト > カスタム オブジェクト > データ パターン]

以下のトピックでは、データ パターンについて説明します。

確認すべき情報	以下を参照
データ パターンを作成する。	データ パターン設定
正規表現データ パターンの構文の詳細といくつかの例を確認する。	正規表現データ パターンの構文 正規表現データ パターンの例

データ パターン設定

フィルタリング対象とする機密情報のカテゴリを定義する場合は、**Objects**（オブジェクト）> **Custom Objects**（カスタム オブジェクト）> **Data Patterns**（データ パターン）のページを使用します。データ フィルタリング プロファイルの定義の詳細は「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Data Filtering（データ フィルタリング）」を参照してください。

次の 3 種類のデータ パターンを作成し、ファイアウォールで機密情報をスキャンするときに使用できます。

- 事前定義済み – ファイルで社会保障番号とクレジット カード番号をスキャンするには、事前定義済みのデータ パターンを使用します。
- 正規表現 – 正規表現を使用して、カスタム データ パターンを作成します。
- ファイル プロパティ – ファイルで特定のファイル プロパティおよび値をスキャンします。

データ パターン設定	の意味
氏名	データ パターン名（最大 31 文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	データ パターンの説明を入力します (最大 255 文字)。
共有	以下に対してデータパターンを公開する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

データ パターン設定	の意味
	• multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してデータパターンが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対してデータパターンが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、このオブジェクトを継承するデバイス グループのこのデータ パターン オブジェクトの設定をオーバーライドすることを防ぐには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
パターン タイプ	作成するデータ パターンのタイプを以下から選択します。 • 事前定義済みのパターン • 正規表現 • ファイル プロパティ
事前定義済みのパターン	Palo Alto Networks では、クレジット カード番号や社会保障番号など、特定タイプの情報をファイルでスキャンするため、事前定義済みのデータ パターンを提供しています。事前定義済みのパターンに基づいてデータ フィルタリングを設定するには、パターンを **Add** (追加) して以下を選択します。 • **Name** (名前) – 機密データのフィルタリングに使用する、事前定義済みのパターンを選択します。事前定義済みのパターンを選択すると、**Description** (説明) には情報が自動的に入力されます。 • 事前定義済みパターンを検出する **File Type** (ファイル タイプ) を選択します。
正規表現	カスタム データ パターンを **Add** (追加) します。分かりやすい **Name** (名前) をパターンに付けて、データ パターンをスキャンする **File Type** (ファイル タイプ) を設定し、**Data Pattern** (データ パターン) を定義する正規表現を入力します。 正規表現のデータ パターンの構文に関する詳細と例については、以下を参照してください。 • 正規表現データ パターンの構文 • 正規表現データ パターンの例
ファイル プロパティ	ファイル プロパティおよび関連付けられている値をスキャンするデータ パターンを構築します。たとえば、ドキュメントのタイトルに「機密」、「社内」、「秘密」などの語句が含まれる Microsoft Word ドキュメントと PDF をフィルタリングするデータ パターンを **Add** (追加) します。 • **Name** (名前) に分かりやすいデータ パターン名を入力します。 • スキャンする **File Type** (ファイル タイプ) を選択します。 • 特定の値をスキャンする **File Property** (ファイル プロパティ) を選択します。 • スキャンする **Property Value** (プロパティ値) を入力します。

© 2019 Palo Alto Networks, Inc.

正規表現データ パターンの構文

正規表現データ パターンを作成する場合、以下の一般的な要件が適用されます。

- パターンには、値が固定された 7 バイト以上の文字列が含まれている必要があります。7 バイトの内には、ピリオド (.)、アスタリスク (*)、プラス記号 (+)、範囲 ([a-z]) を含められません。
- 値で大文字と小文字を区別する必要がある場合は、可能なすべての文字列のパターンを定義して、用語のすべてのバリエーションに一致させます。例えば、confidential (機密) と指定されたすべての文書に一致させるには、「confidential」、「Confidential」、および「CONFIDENTIAL」を含むパターンを作成する必要があります。

PAN-OS® の正規表現の構文は、従来の正規表現エンジンと似ていますが、それぞれのエンジンはすべて異なります。以下の表に、PAN-OS でサポートされている構文を示します。

パターンのルールの構文	の意味
。	任意の 1 文字に一致します。
不明	直前の文字または表現に 0 ~ 1 回一致します。かっこ内に一般式を含める必要があります。 例:.
*	直前の文字または表現に 0 回以上一致します。かっこ内に一般式を含める必要があります。 例: (abc)*
+	直前の文字または正規表現に 1 回以上一致します。かっこ内に一般式を含める必要があります。 例: (abc)+
|	「または」を指定します。 例: ((bif)|(scr)|(exe)) は、「bif」、「scr」または「exe」に一致します。 代替の従属文字列はかっこ内に含める必要があります。
-	範囲を指定します。 例: [c-z] は、c ~ z の任意の文字列に一致します。
[ ]	指定された任意の文字に一致します。 例: [abz] はa、b、または z に一致します。
^	指定された文字以外の任意の文字に一致します。 例:[^abz] はa、b、またはz以外の任意の文字に一致します。
{ }	最小値と最大値を含む文字列に一致します。 例: {10-20} は、10 ~ 20 バイトの文字列に一致します。固定文字列の前に直接指定する必要があり、ハイフン (–) のみを使用できます。

© 2019 Palo Alto Networks, Inc.

パターンの ルールの構文	の意味
\	上記の任意の文字に対してリテラル一致を実行します。指定した文字の前にバックスラッシュ記号 (\) を付ける必要があります。
&amp	アンパサンド (&) は特殊文字であるため、文字列で & を検索するには、代わりに **&amp**を使用する必要があります。

正規表現データ パターンの例

有効なカスタム パターンの例を以下に示します。

- .*((Confidential)|(CONFIDENTIAL))
  - 任意の場所から「Confidential」または「CONFIDENTIAL」という言葉を検索します。
  - 最初の「.*」は、ストリームの任意の場所を検索することを指定します。
  - デコーダが大文字小文字を区別するかどうかに応じて、上のパターンは「confidential」(すべて小文字) に一致しないことがあります。
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
  - 「Proprietary & Confidential」または「Proprietary and Confidential」を検索します。
  - 「Confidential」の検索よりも詳細な検索です。
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
  - さまざまな形式の単語 draft が後に続く「Press Release」を検索します。これに一致する場合は、プレス リリースの公開準備が整っていないことを示します。
- .*(Trinidad)
  - 「Trinidad」などのプロジェクト コード名を検索します。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> Spyware/Vulnerability（スパイウェア/脆弱性）

ファイアウォールでは、ファイアウォールの脅威エンジンを使用してカスタムのスパイウェア シグネチャと脆弱性シグネチャを作成する機能がサポートされています。スパイウェアのフォンホーム通信や脆弱性の悪用を特定するためのカスタム正規表現パターンを記述できます。作成したスパイウェアと脆弱性のパターンは、カスタム脆弱性プロファイルで使用できます。ファイアウォールは、カスタム定義されたパターンがネットワーク トラフィックに含まれていないか検索し、脆弱性の悪用に対して指定されたアクションを実行します。

週次のコンテンツ リリースには、新しいデコーダとシグネチャを開発するためのコンテクストが定期的に含まれています。

カスタム シグネチャを定義するときに任意で時間属性を含めることができます。これを行うには、攻撃に対してアクションをトリガーする間隔ごとにしきい値を指定します。しきい値に達した場合にのみアクションが実行されます。

アンチスパイウェアプロファイルのシグネチャを定義する場合は、**Custom Spyware Signature**[カスタムスパイウェアシグネチャ] のページを使用します。脆弱性防御プロファイルのシグネチャを定義するには、**Custom Spyware Signature**[カスタム脆弱性シグネチャ] ページを使用します。

カスタムの脆弱性およびスパイウェア シグネチャの設定	の意味
Configuration [設定] タブ	
脅威 ID	その設定で使用する識別子の数値を入力します（スパイウェアシグネチャの範囲は15000～18000、脆弱性シグネチャの範囲は41000～45000）。
氏名	脅威の名前を指定します。
共有	以下に対してカスタムシグネチャを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してカスタムシグネチャが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対してカスタムシグネチャが公開されます。
オーバーライドの無効化（Panoramaのみ）	このシグネチャの設定が、このシグネチャを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでは、この選択は解除されています。つまり、管理者は、

© 2019 Palo Alto Networks, Inc.

カスタムの脆弱性およびスパイウェア シグネチャの設定	の意味
	シグネチャを継承するすべてのデバイス グループで設定をオーバーライドできます。
コメント	任意でコメントを入力します。
重要度	脅威の重大度を示すレベルを割り当てます。
デフォルトのアクション	脅威の条件を満たしたときに実行されるデフォルトのアクションを割り当てます。アクションのリストについては、「セキュリティ プロファイルのアクション」を参照してください。
指示	脅威を評価する方向 (クライアントからサーバー、サーバーからクライアント、その両方) を指定します。
影響を受けるシステム	脅威によって影響を受ける対象 (クライアント、サーバー、そのどちらか、その両方) を指定します。脆弱性シグネチャには適用されますが、スパイウェア シグネチャには適用されません。
CVE	CVE (Common Vulnerability Enumeration) を、追加情報および分析のための外部参照として指定します。
ベンダー	脆弱性のベンダー識別子を、追加情報および分析のための外部参照として指定します。
Bugtraq	Bugtraq (CVE と類似) を、追加情報および分析のための外部参照として指定します。
リファレンス	必要に応じて、追加の分析または情報用にリンクを追加します。この情報は、ユーザーが ACC、ログ、または脆弱性プロファイルから脅威をクリックすると表示されます。
Signatures [シグネチャ] タブ	
標準シグネチャ	**Standard**[標準] を選択し、新しいシグネチャを**Add**[追加] します。以下の情報を指定します。 • **Standard**[標準] – シグネチャの識別に使用する名前を入力します。 • **Comment**[コメント] – 任意で説明を入力します。 • **Ordered Condition Match**[順番が付けられた条件の一致] – シグネチャの条件の定義順序が重要である場合に選択します。 • **Scope**[範囲] – このシグネチャの適用対象 (現在のトランザクションのみ、またはユーザー セッション全体) を選択します。 **Add Or Condition**[Or条件を追加] または **Add And Condition**[And条件を追加] をクリックして条件を追加します。グループ内に条件を追加するには、グループを選択して **Add Condition**[条件の追加] をクリックします。シグネチャに条件を追加して、条件として定義したパラメータが真の場合にトラフィックのシグネチャが生成されるようにします。ドロップダウンリストから**Operator**[演算子] を選択します。演算子によって、カスタム シグネチャがトラフィックと一致するために真である必要がある条件のタイプが決まります。**Less Than**[未

© 2019 Palo Alto Networks, Inc.

カスタムの脆弱性およびスパイウェア シグネチャの設定	の意味

	満]、**Equal To**[等しい]、**Greater Than**[超過]、または **Pattern Match**[パターン マッチ] 演算子を選択します。
	• **Pattern Match**[パターン マッチ] 演算子を選択する際には、以下が真になるように指定すると、シグネチャがトラフィックと一致します。
	  • **Context**[コンテクスト] – 使用可能なコンテクストから選択します。
	  • **Pattern**[パターン] – 正規表現を指定します。正規表現のパターンのルールに関する詳細は「パターンのルールの構文」を参照してください。
	  • **Qualifier and Value**[修飾子と値] – 任意で修飾子/値のペアを追加します。
	  • **Negate**[否定] – **Negate**を選択すると、定義済みのパターンマッチ条件が真でない場合のみ、カスタムシグネチャがトラフィックと一致します。これにより、特定の条件が満たされたとき、カスタム シグネチャがトリガーされないようにできます。
	  Negate 条件だけのカスタム シグネチャを作成することはできません。*Negate* 条件を指定するには、少なくとも *1* つの肯定条件を含める必要があります。また、シグネチャの範囲がセッションに設定されている場合、トラフィックと一致させるには、*Negate* 条件を最後の条件に設定しないようにしてください。
	トラフィックがシグネチャとシグネチャの例外の両方に一致する場合、新しいオプションを使用してシグネチャの生成を無効にすることで、カスタム脆弱性またはスパイウェアシグネチャの例外を定義できます。このオプションを使用すると、通常ならスパイウェアまたは脆弱性攻撃として分類されるネットワーク内の特定のトラフィックを許可できます。その場合、パターンに一致するトラフィックについてのみ、シグネチャが生成されます。パターンには一致するが、パターンの例外にも一致するトラフィックは、シグネチャ生成の対象から除外され、関連するポリシー アクション (ブロックやドロップなど) も実行されません。たとえば、リダイレクトされた URL に対して生成されるシグネチャを定義し、同時に、信頼されたドメインにリダイレクトされた URL についてはシグネチャを生成しないという例外も作成できるようになりました。

	• **Equal To**[等しい]、**Less Than**[未満]、または **Greater Than**[超過] の演算子を選択する場合は、以下が真になるように指定すると、シグネチャがトラフィックと一致します。
	  • **Context**[コンテクスト] – TCP または UDP の未知のリクエストまたは応答から選択します。
	  • **Position**[位置] – ペイロードの最初の 4 バイトまたは 2 番目の 4 バイトのいずれかを選択します。
	  • **Mask**[マスク] – 4 バイトの 16 進数値を指定します (たとえば、0xffffff00)。
	  • **Value**[値] – 4 バイトの 16 進数値を指定します (たとえば、0xaabbccdd)。

組み合わせシグネチャ	**Combination**[組み合わせ] を選択し、以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

カスタムの脆弱性およびスパイウェア シグネチャの設定	の意味
	Combination Signatures[組み合わせシグネチャ] を選択し、シグネチャを定義する条件を以下のように指定します。 • **Add AND Condition**[AND条件を追加] または **Add OR Condition**[OR条件を追加] をクリックして条件を追加します。グループ内に条件を追加するには、グループを選択して **Add Condition**[条件の追加] をクリックします。 • グループ内で条件を移動するには、条件を選択して **Move Up**[上へ] または **Move Down**[下へ] をクリックします。グループを移動するには、グループを選択して **Move Up**[上へ] または **Move Down**[下へ] をクリックします。グループ間で条件を移動することはできません。 **Time Attribute**[時間属性] を選択し、以下の情報を指定します。 • **Number of Hits**[ヒット数] – ポリシーベースのアクションをトリガーするしきい値を、指定した秒数 (1 ~ 3600) のヒット数 (1 ~ 1000) として指定します。 • **Aggregation Criteria**[集約基準] – ヒットの追跡方法 (送信元 IP アドレス、宛先 IP アドレス、または送信元 IP アドレスと宛先 IP アドレスの組み合わせ) を指定します。 • グループ内で条件を移動するには、条件を選択して **Move Up**[上へ] または **Move Down**[下へ] をクリックします。グループを移動するには、グループを選択して **Move Up**[上へ] または **Move Down**[下へ] をクリックします。グループ間で条件を移動することはできません。

© 2019 Palo Alto Networks, Inc.

Objects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カテゴリ]

カスタムURLカテゴリのページを使用してURLのカスタムリストを作成し、URLフィルタリングプロファイルまたはポリシールールの一致条件に使用します。カスタム URL カテゴリでは URL エントリを個別に追加したり、あるいは URL のリストを含むテキストファイルをインポートすることができます。

カスタム カテゴリに追加される *URL* エントリの大文字と小文字は区別されます。

以下の表では、カスタム URL 設定について説明します。

カスタム URL カテゴリ設定	の意味
氏名	カスタム URL カテゴリの識別に使用する名前（最大 31 文字）を入力します。URLフィルタリングポリシーを定義する場合と、ポリシールールのURLカテゴリの一致条件のカテゴリリストにこの名前が表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	URL カテゴリの説明を入力します (最大 255 文字)。
タイプ	カテゴリ タイプを選択します。 • **Category Match** (カテゴリの一致)– **Category Match** (カテゴリの一致)を選択して、指定したすべての URL カテゴリに一致する URL を含む新しいカスタム カテゴリを定義します (URL はリスト内のすべてのカテゴリに一致する必要があります)。2 ～ 4 個のカテゴリを指定します。 • **URL** リスト– **URL** リスト を選択して、カテゴリの URL リストを追加またはインポートします。このカテゴリ タイプには、PAN-OS 9.0 より前に追加された URL も含まれています。
共有	以下に対してURLカテゴリを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。このオプションを無効化（クリア）すると、**Objects** (オブジェクト) タブで選択した **Virtual System** (仮想システム) のみに対してURLカテゴリが公開されます。 • Panorama 上の各デバイス グループ。このオプションを無効化（クリア）すると、**Objects** (オブジェクト) タブで選択した **Device Group** (デバイスグループ) のみに対して URL カテゴリが公開されます。
オーバーライドの無効化（Panoramaのみ）	このカスタム URL オブジェクトの設定が、このオブジェクトを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでこのオプションは無効

© 2019 Palo Alto Networks, Inc.

カスタム URL カテゴリ設定	の意味
	化されており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
サイト	カスタム URL カテゴリのサイトを管理します (追加またはインポートされる各 URL は最大 255 文字です)。 • **Add** (追加)—URL を**Add** (追加)します (一行につきピアは一つのみ) 。各 URL は「www.example.com」の形式で入力できます。また、「*.example.com」など、ワイルドカードを含むこともできます。サポートされる形式に関する詳細な情報についてはObjects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]のブロックリストを参照してください。 • **Import** (インポート) – URL リストが含まれているテキストファイルを参照して**Import** (インポート) します。1行あたり1つのURLのみを入力します。各 URL は「www.example.com」の形式で入力できます。また、「*.example.com」など、ワイルドカードを含むこともできます。サポートされる形式に関する詳細な情報についてはObjects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]のブロックリストを参照してください。 • **Export** (エクスポート)—リストに含まれるカスタム URL エントリを**Export** (エクスポート) (テキストファイルとしてエクスポート) します。 • **Delete** (削除)—エントリを**Delete** (削除)してリストから URL を取り除きます。 *URL* フィルタリングプロファイルで使用したカスタムカテゴリを削除する場合は、アクションを*None* (なし) に設定する必要があります。カテゴリアクションについては、Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）

セキュリティ プロファイルでは、セキュリティ ポリシーで脅威から保護します。それぞれのセキュリティ ポリシー ルールには、1 つ以上のセキュリティ プロファイルを含めることができます。以下のプロファイル タイプを使用できます。

- アンチウイルス プロファイル – ワーム、ウイルス、トロイの木馬から保護したり、スパイウェアのダウンロードをブロックしたりします。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Antivirus（アンチウイルス）」を参照してください。
- アンチスパイウェア プロファイル – 侵入されたホストのスパイウェアから外部指揮統制 (C2) サーバーに対する phone-home 通信またはビーコン通信の試みをブロックします。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Anti-Spyware Profile（アンチスパイウェア プロファイル）」を参照してください。
- 脆弱性防御プロファイル - システムの脆弱性の悪用やシステムへの不正アクセスを防止します。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Vulnerability Protection（脆弱性防御）」を参照してください。
- URL フィルタリング プロファイル – 特定の Web サイトや Web サイト カテゴリ (ショッピングやギャンブルなど) へのユーザーのアクセスを制限します。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> URL Filtering（URL フィルタリング）」を参照してください。
- ファイル ブロッキング プロファイル – 選択したファイル タイプの指定したセッション フロー方向 (インバウンド、アウトバウンド、両方) のトラフィックをブロックします。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> File Blocking（ファイル ブロッキング）」を参照してください。
- WildFire™ 分析プロファイル – WildFire アプライアンスまたは WildFire クラウドでローカルに実行されるファイル分析を指定します。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> WildFire Analysis（WildFire 分析）」を参照してください。
- データ フィルタリング プロファイル – クレジット カード番号や社会保障番号などの機密情報が、保護されたネットワークから漏出するのを防ぎます。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Data Filtering（データ フィルタリング）」を参照してください。
- DoS プロテクション プロファイルは、大量の単一および複数セッション攻撃からファイアウォールを保護するために DoS プロテクション ポリシー ルールで使用されます。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> DoS Protection（DoS プロテクション）」を参照してください。
- GTP プロテクション プロファイルを使用すると、ファイアウォールは GTP トラフィックを検査、検証、およびフィルタリングできます。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション）」を参照してください。

個々のプロファイルの他に、一緒に適用されることが多いプロファイルをまとめて **Objects**（オブジェクト）> **Security Profile Groups**（セキュリティ プロファイル グループ）からセキュリティ プロファイル グループを作成することもできます。

セキュリティ プロファイルのアクション

アクションには、脅威イベントに対するファイアウォールの応答方法を指定します。Palo Alto Networks で定義されている脅威やウイルス シグネチャには、デフォルト アクションが用意されています。デフォルト アクションは通常、**Alert**（アラート）または **Reset Both**（両方のリセット）に設定されています。前者は、通知用に有効にしたオプションを使用して通知されます。後者は、接続の両側をリセットします。ただし、デフォルト アクションは、ファイアウォール上で定義またはオーバーライドできます。アンチウイルス プロファイル、アンチスパイウェア プロファイル、脆弱性防御プロファイル、カスタム スパ

© 2019 Palo Alto Networks, Inc.

イウェア オブジェクト、カスタム脆弱性オブジェクト、または DoS プロテクション プロファイルを定義する際には、以下のアクションを適用できます。

操作	の意味	アンチウイルスプロファイル	アンチスパイウェアプロファイル	脆弱性防御プロファイル	カスタム オブジェクト – スパイウェアと脆弱性	DoSプロテクション プロファイル
Reset Both [デフォルト]	各脅威に対して内部的に指定されているデフォルト アクションが実行されます。 アンチウイルス プロファイルの場合、ウイルス シグネチャのデフォルト アクションが実行されます。	✓	✓	✓	–	ランダム早期ドロップ ランダムソウキドロップ
Allow [許可]	アプリケーション トラフィックが許可されます。 *Allow (許可) アクションは、シグネチャまたはプロファイルに関連するログを生成しません。*	✓	✓	✓	✓	–
Alert [アラート]	各アプリケーション トラフィック フローのアラートが生成されます。アラートは脅威ログに保存されます。	✓	✓	✓	✓	✓ 攻撃量（cps）がプロファイルで設定されたアラームのしきい値に達した場合、アラートが生成されます。

© 2019 Palo Alto Networks, Inc.

操作	の意味	アンチウイルスプロファイル	アンチスパイウェアプロファイル	脆弱性防御プロファイル	カスタム オブジェクト – スパイウェアと脆弱性	DoSプロテクション プロファイル
Drop [ドロップ]	アプリケーション トラフィックが廃棄されます。	✓	✓	✓	✓	–
Reset Client [クライアントのリセット]	TCP の場合、クライアント側の接続がリセットされます。 UDP の場合、接続が廃棄されます。	✓	✓	✓	✓	–
Reset Server [サーバーのリセット]	TCP の場合、サーバー側の接続がリセットされます。 UDP の場合、接続が廃棄されます。	✓	✓	✓	✓	–
Reset Both [両方のリセット]	TCP の場合、クライアント側とサーバー側の両方の接続がリセットされます。 UDP の場合、接続が廃棄されます。	✓	✓	✓	✓	–
Block IP [ブロック IP]	送信元からのトラフィックまたは送信元と宛先のペアからのトラフィックが指定した期間（設定可能）ブロックされます。	–	–	–	–	✓
シンクホール	このアクションでは、悪質なドメインに向けられたDNSクエリをシンクホールIPアドレスに転送します。 このアクションは Palo Alto Networks DNS シグネチャおよびObjects（オブジェクト）> External Dynamic Lists（外部動的リスト）に含まれるカスタム ドメインで使用することができます。	–	–	–	–	–

© 2019 Palo Alto Networks, Inc.

操作	の意味	アンチウイルスプロファイル	アンチスパイウェアプロファイル	脆弱性防御プロファイル	カスタム オブジェクト – スパイウェアと脆弱性	DoSプロテクション プロファイル
ランダム早期ドロップ ランダムソウキドロップ	1 秒あたりの接続数が、DoS プロテクション ルールに適用される DoS プロテクション プロファイルの Activate Rate（アクティベート率）しきい値に達すると、ファイアウォールによってランダムにパケットがドロップされます。	–	–	–	–	✓
SYN Cookie	1 秒あたりの接続数が、DoS プロテクション ルールに適用される DoS プロテクション プロファイルの Activate Rate（アクティベート率）しきい値に達すると、ファイアウォールによって、クライアントからの SYN を認証するための SYN Cookie が生成されます。	–	–	–	–	✓

ポリシー ルールで使用されているプロファイルは削除できません。まず、ポリシー ルールからプロファイルを削除する必要があります。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Antivirus [オブジェクト > セキュリティ プロファイル > アンチウイルス]

Antivirus Profiles[アンチウイルス プロファイル] ページを使用して、定義されたトラフィックに対するファイアウォールのウイルス スキャンのオプションを設定します。ウイルス検査対象のアプリケーションと、ウイルス検出時に実行するアクションを設定します。デフォルトのプロファイルでは、表示されているすべてのプロトコル デコーダがウイルス検査の対象になります。Simple Mail Transport Protocol (SMTP)、Internet Message Access Protocol (IMAP)、および Post Office Protocol Version 3 (POP3) ではアラートが生成され、他のアプリケーションでは検出されたウイルスのタイプに応じてデフォルトのアクション (アラートまたは拒否) が実行されます。次にプロファイルは、特定のゾーンを通過するトラフィックから検査対象のトラフィックを判別するため、セキュリティ ポリシー ルールに適用されます。

カスタマイズしたプロファイルを使用して、信頼されたセキュリティ ゾーン間のトラフィックに対するアンチウイルスの検査を最小限に抑え、インターネットなどの信頼されていないゾーンから受信したトラフィックや、サーバー ファームなどの機密性の高い宛先に送信されるトラフィックの検査を最大化できます。

新しいアンチウイルスプロファイルを追加する場合は、Add (追加) を選択し、以下の設定を行います。

項目	の意味
氏名	プロファイル名 (最大 31 文字) を入力します。この名前は、セキュリティ ポリシーを定義するときにアンチウイルス プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、ピリオド、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有 (Panorama のみ)	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこのアンチウイルス プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
[アンチウイルス] タブ FTP や HTTP など、様々なタイプのトラフィックに対するアクションを指定します。	
パケット キャプチャ	識別されたパケットをキャプチャする場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
デコーダとアクション	ウイルスを検査するトラフィックのタイプごとに、ドロップダウンリストからアクションを選択します。標準のアンチウイルス シグネチャ (Action [アクション]列) と WildFire システムで生成されたシグネチャ (WildFire Action [WildFire アクション] 列) にさまざまなアクションを定義できます。 環境によっては、アンチウイルス シグネチャに長めのソーク時間を必要とするため、このオプションでは、Palo Alto Networks が提供する 2 つのアンチウイルス シグネチャ タイプに異なるアクションを設定できます。たとえば、標準のアンチウイルス シグネチャは、リリースされるまでのソーク時間がより長い (24 時間) のに対し、WildFire シグネチャは脅威が検出されてから 15 分以内に生成されてリリースされます。このため、アクションに block ではなく、WildFire シグネチャに基づく alert を選択する必要が生じることもあります。 デフォルトのアンチウイルス プロファイルをコピーしてすべてのデコーダの *Action (アクション)* および *WildFire Action (WildFire アクション)* を*reset-both*に設定し、そのプロファイルをトラフィックを許可するすべてのセキュリティポリシールールに適用することで、セキュリティを最大限に高めることができます。
アプリケーション例外とアクション	**Applications Exception**[アプリケーション例外] テーブルでは、検査対象外のアプリケーションを定義することができます。たとえば、特定のアプリケーションを除くすべての HTTP トラフィックをブロックするには、そのアプリケーションが例外になるようにアンチウイルス プロファイルを定義します。**Block**[ブロック] は HTTP デコーダに対するアクションで、**Allow**[許可] はアプリケーションの例外です。アプリケーション例外ごとに、脅威の検出時に実行するアクションを選択します。アクションのリストについては、「セキュリティ プロファイルのアクション」を参照してください。 アプリケーションを検索するには、アプリケーション名をテキスト ボックスに入力します。一致するアプリケーションのリストが表示され、選択ができるようになります。 正当なアプリケーションにウイルスが含まれていると誤って判断された場合 (誤検出)、*TAC* を使ってサポートケースを開始し、*Palo Alto Networks* が誤って検出されたウイルスを分析して修正できるようにしてください。問題が解決されたら、プロファイルから例外を削除します。

[ウイルス例外] タブ

Virus Exception (ウイルスの例外)タブを使用して、アンチウイルスプロファイルで無視する脅威のリストを定義します。

見つかったウイルスが実際にはウイルスでないことが定かな場合のみ (誤検出)、ウイルス例外を作成します。誤検出が見つかったと考えられる場合は、*TAC* を使ってサポートケースを開始し、*Palo Alto Networks* が誤って検出されたウイルス シグネチャを分析して修正できるようにしてください。問題が解決されたら、プロファイルからすぐに例外を削除します。

脅威 ID	無視したい特定の脅威を追加する場合は、脅威IDを1つずつ入力し、**Add**[追加] をクリックします。Threat ID は、Threat ログの情報の一部として表示されます。「Monitor (監視) > Logs (ログ)」を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Anti-Spyware Profile（アンチスパイウェア プロファイル）

アンチスパイウェア プロファイルをセキュリティ ポリシー ルールに関連付けることで、ネットワーク上のシステムにインストールされたスパイウェアやコマンドアンドコントロール（C2）マルウェアによって起動された接続を検出できます。セキュリティ ポリシー ルールに割り当てる 2 つの事前定義済みアンチスパイウェア プロファイルのどちらかを選択できます。各プロファイルには、脅威の重大度別に整理された事前定義ルールのセットが用意されています。各脅威シグネチャには、Palo Alto Networks によって指定されたデフォルト アクションが含まれています。

- default — 各シグネチャのデフォルトのアクションを使用します。デフォルトのアクションは、シグネチャの作成時に Palo Alto Networks によって指定されます。
- Strict — strict プロファイルは、重要、高、中の重大度の脅威のシグネチャ ファイルに定義されているアクションをオーバーライドして、**reset-both**アクションに設定します。デフォルト アクションは、低および情報の重大度を持つ脅威とみなされます。
- カスタムのプロファイルを作成することもできます。たとえば、信頼されたセキュリティ ゾーン間のトラフィックのアンチスパイウェア検査における厳重度を軽減して、インターネットから受信したトラフィック、またはサーバー ファームなどの保護資産に送信されるトラフィックの検査の厳重度を最大化するといったことができます。

以下の表では、アンチスパイウェア プロファイル 設定について説明します。

アンチスパイウェア プロファイル設定	の意味
氏名	プロファイル名（最大 31 文字）を入力します。この名前は、セキュリティポリシーを定義するときにアンチスパイウェアプロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、ピリオド、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有（Panorama のみ）	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化（Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこのアンチスパイウェア プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになってお

© 2019 Palo Alto Networks, Inc.

アンチスパイウェア プロファイル設定	の意味
	り、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

Rules（ルール）タブ

アンチスパイウェア ルールでは、カスタム重大度を定義し、任意の脅威（入力したテキストを含む名前を持つ特定の脅威、そしてアドウェアなどの脅威カテゴリ）に対して取るべきアクションを定義することができます。

新しいルールを **Add**（追加）します。または、既存のルールを選択して **Find Matching Signatures**（一致するシグネチャの検索）を選択し、そのルールに基づいて脅威シグネチャをフィルタリングできます。

ルール名	ルール名を指定します。
脅威名	すべてのシグネチャを照合する場合は**any**と入力します。または、シグネチャ名の一部として入力されたテキストを含むすべてのシグネチャを照合するテキストを入力します。
カテゴリ	カテゴリを選択するか、**any (**すべて**)**を選択してすべてのカテゴリにマッチさせます。
操作	各脅威のアクションを選択します。アクションのリストについては、「セキュリティ プロファイルのアクション」を参照してください。 事前定義済みの*strict (*厳格*)*なプロファイルの *Action (*アクション*)* 設定を使用することで、セキュリティを最大化できます。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、このオプションを選択します。 脅威が検出されたときに 1 つのパケットをキャプチャするには、**single-packet**、1 ~ 50 個のパケットをキャプチャするには、**extended-capture** オプションを選択します（デフォルトは 5 パケットです）。extended-capture では、脅威ログを分析するときに脅威についてより詳細なコンテクストを得られます。パケット キャプチャを表示する場合は、**Monitor**（監視）> **Logs**（ログ）> **Threat**（脅威）を選択し、関心のあるログ エントリを見つけて、第 2 列にある緑の下矢印をクリックします。キャプチャするパケットの数を定義するには、**Device**（デバイス）> **Setup**（セットアップ）> **Content-ID** を選択し、Content-ID™ 設定を編集します。 パケット キャプチャは、アクションが **allow (**許可**)** または **alert (**アラート**)** の場合にのみ行われます。**block (**ブロック**)** アクションが設定されている場合、セッションは即座に終了します。 重大度が *critical*（重要）、*high*（高）、*medium*（中）のイベントに対して拡張キャプチャを有効化します。デフォルトの拡張キャプチャの値（*5* パケット）を使用することで、大抵の場合に脅威を分析するための十分な情報を得られます。（パケット キャプチャのトラフィックが多すぎると、パケット キャプチャをドロップするおそれがあります）重大度が高いイベントと比べて情報のキャプチャがそれ程役立たず、低い値のトラフィックが比較的多く発生するため、重大度が *informational (*通知*)* 以

© 2019 Palo Alto Networks, Inc.

アンチスパイウェア プロファイル設定	の意味
	下のイベントに対して拡張キャプチャを有効化しないでください。
重要度	重大度レベル (**critical**[重要]、**high**[高]、**medium**[中]、**low**[低]、または **informational**[通知]) を選択します。
Exceptions [例外] タブ 特定のシグネチャに対するアクションを変更できます。たとえば、特定のシグネチャ セットについてアラートを生成し、他のすべてのシグネチャに一致するすべてのパケットをブロックできます。脅威例外は、通常、誤検出が発生したときに設定します。=脅威例外の管理を容易にするために、脅威例外を **Monitor**（監視）> **Logs**（ログ）> **Threat**（脅威）リストから直接追加できます。新規の脅威から保護されるように、または誤検出に対する新しいシグネチャがインストールされるように、最新のコンテンツ更新を取得してください。	
例外	アクションを割り当てようとしている脅威をそれぞれ**Enable** (有効化) するか、**All** (すべて) を選択してリストにあるすべての脅威に対するアクションを有効化します。このリストは、選択したホスト、カテゴリ、および重大度によって異なります。リストが空の場合、現在の選択に対応する脅威がないことを表します。 IP Address Exemptions (IP アドレスの除外) を使用して、脅威例外をフィルタリングする IP アドレスを追加します。脅威例外に IP アドレスが追加されている場合、そのシグネチャの脅威例外アクションは、例外の IP アドレスにマッチする送信元あるいは宛先 IP アドレスを持つセッションがシグネチャをトリガーした場合にのみ、ルールのアクションをオーバーライドします。シグネチャあたり最大 100 個の IP アドレスを追加できます。このオプションでは、特定の IP アドレスの例外を作成するために新しいポリシー ルールと新しい脆弱性プロファイルを作成する必要はありません。 スパイウェアとして識別されたシグネチャが脅威でないことが確かな場合（誤検出）のみ、例外を作成するようにしてください。誤検出が見つかったと考えられる場合は、*TAC* を使ってサポートケースを開始し、*Palo Alto Networks* が誤って検出されたシグネチャを分析して修正できるようにしてください。問題が解決されたらすぐ、プロファイルから例外を削除します。
DNS Signatures (DNS シグネチャ**)** タブ **DNS Signatures**[DNS シグネチャ] 設定は、ネットワーク上の感染したホストを特定する追加方法です。これらのシグネチャは、マルウェアに関連付けられているホスト名に対する特定の DNS ルックアップを検出します。	
Policies (ポリシー) および Settings (設定) タブ **DNS Signature Policies (DNS** シグネチャ ポリシー**)**では、通常のアンチウイルスシグネチャと同様に、これらのクエリが観察されると許可、アラート、シンクホール、またはブロックするよう、DNS シグネチャ ポリシーソースを設定できます。マルウェアドメインの DNS クエリを実行するホストはボットネットレポートに表示されます。さらに、マルウェアの DNS クエリに対してシンクホールを行う場合は、**DNS Sinkhole Settings (DNS** シンクホール設定**)**内のシンクホール IP を指定できます。	

© 2019 Palo Alto Networks, Inc.

アンチスパイウェア プロファイル設定	の意味
DNS シグネチャ ソース	DNSクエリが発生した場合にアクションを強制的に実施する対象のリストを選択できます。デフォルトの DNS シグネチャ ポリシーのオプションは 2 つあります： • **Palo Alto Networks** コンテンツ **DNS** シグネチャ–動的なコンテンツ更新を通じて更新される、ローカルのダウンロード可能なシグネチャです。 • **Palo Alto Networks DNS** セキュリティ–DNS データのプロアクティブな分析を実行するクラウドベースの DNS セキュリティサービスであり、Palo Alto Networks DNS シグネチャ データベースに対する完全なアクセスを提供します。 このサービスを使用するには、脅威防止ライセンスに加えて *DNS* セキュリティ ライセンスを購入してアクティベートする必要があります。 デフォルト設定では、ローカルでアクセスできる Palo Alto Networks DNS シグネチャ コンテンツの DNS シグネチャはシンクホールされますが、クラウドベースの DNS セキュリティでは許可するように設定されています。DNS セキュリティを使用するシンクホールを有効化したい場合、DNS クエリのアクションをシンクホールに設定する必要があります。シンクホールに使用されるデフォルトのアドレスは Palo Alto Networks のものです（sinkhole.paloaltonetworks.com）。このアドレスは静的ではなく、ファイアウォールや Panorama のコンテンツアップデートを通じて変更される場合があります。 新しいリストを追加する場合は**Add** (追加)し、以前作成済の、タイプがドメインの外部動的リストを選択します。新しいリストを作成する方法については、「Objects（オブジェクト）> External Dynamic Lists（外部動的リスト）」を参照してください。
DNS クエリに対するアクション	既知のマルウェア サイトに対して DNS ルックアップが実行されたときに実行するアクションを選択します。ここでは**alert** (アラート)、**allow** (許可)、**block** (ブロック)、**sinkhole** (シンクホール)を使用できます。Palo Alto Networks DNSシグネチャのデフォルトアクションは**sinkhole** (シンクホール)です。 DNS シンクホール アクションを使用すると、管理者は、ファイアウォールがローカル DNS サーバーよりもインターネット側にある（ファイアウォールが DNS クエリの発行元を認識できない）場合も含め、DNS トラフィックを使用してネットワーク上の感染ホストを特定することができます。脅威防御ライセンスがインストールされていて、セキュリティプロファイルでアンチスパイウェアプロファイルが有効な場合、DNSベースのシグネチャが、マルウェアドメインへの DNS クエリによってトリガーします。ファイアウォールがローカル DNS サーバーよりもインターネット側にある通常のデプロイメントでは、脅威ログは、実際の感染ホストではなくローカル DNS リゾルバをトラフィックの送信元として識別します。マルウェア DNS クエリをシンクホールすると、有害なドメインへのクエリに対する応答を偽装することで、この可視性の問題が解決されます。そのため、悪意のあるドメイン (たとえば、コマンドアンドコントロールなど) への接続を試みるクライアントは、代わりに管理者が指定した IP アドレスへに接続を試みることになります。こうすることで、感染ホストをトラフィック ログ内で容易に特定できます。シンクホール IP への接続を試みるホストはすべて、マルウェアに感染している可能性が高いためです。

© 2019 Palo Alto Networks, Inc.

アンチスパイウェア プロファイル設定	の意味
	ファイアウォールが *DNS* クエリの元の送信者を確認できない際（典型的には、ファイアウォールがローカル *DNS* サーバーのノースにあたる場合）に *DNS* シンクホールを有効化し、感染ホストを識別できるようにします。トラフィックをシンクホールできない場合はブロックしてください。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、任意の送信元に対してこのオプションを選択します。 シンクホールされたトラフィックに対するパケット キャプチャを有効化し、それを分析して感染ホストについての情報を得られるようにしてください。
DNS シンクホールの設定	DNS シグネチャ ソース用のシンクホール アクションを定義した後、シンクホールに使用する IPv4 アドレスおよび（もしくは）IPv6 アドレスを指定します。デフォルトでは、シンクホールのIPアドレスはPalo Alto Networksサーバーに設定されています。こうすることで、トラフィックログを使用し、あるいはシンクホールのIPアドレスでフィルタをかけるカスタムレポートを作成し、感染したクライアントを特定することができます。 以下は、DNS要求がシンクホールに掛けられた場合に発生するイベントの流れです。 感染したクライアント コンピュータ上の有害なソフトウェアが DNS クエリを送信して、インターネット上の有害なホストを解決します。 クライアントの DNS クエリが内部 DNS サーバーに送信され、ファイアウォールの反対側にある公開 DNS サーバーをクエリします。 DNS クエリは、指定した DNS シグネチャ データベース ソース内の DNS エントリと一致するため、シンクホール アクションがクエリに対して実行されます。 感染したクライアントは、そのホストでセッションを開始しようとしますが、代わりに偽装 IP アドレスを使用します。偽装 IP アドレスは、アンチスパイウェア プロファイルの [DNS シグネチャ] タブでシンクホール アクションが選択されたときに定義されたアドレスです。 管理者は、脅威ログに有害な DNS クエリがあるというアラート通知を受け取り、トラフィック ログ内のシンクホール IP アドレスを検索して、シンクホール IP アドレスでセッションを開始しようとしているクライアント IP アドレスを容易に特定できます。

Exceptions [例外] タブ

DNS シグネチャの**Exceptions** (例外)を使用すれば、特定の脅威 ID をポリシーの適用から除外することができます。

ポリシーから除外したい特定の脅威を追加するには、**Threat ID** (脅威 **ID**)を選択あるいは検索して**Enable** (有効化)をクリックします。各エントリがオブジェクトの脅威**ID**、**Name** (名前)、および**FQDN**を提示します。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Vulnerability Protection [オブジェクト > セキュリティプロファイル > 脆弱性防御]

セキュリティ ポリシー ルールでは脆弱性防御プロファイルを指定できます。このプロファイルでは、システムの脆弱性を悪用するバッファ オーバーフローや不正コードの実行などに対する保護レベルを定義します。脆弱性防御機能では、以下の 2 つの事前定義済みプロファイルを使用できます。

- **default** プロファイルでは、default アクションがすべてのクライアントおよびサーバーの重大度が critical、high、medium の脆弱性に適用されます。low および informational の脆弱性防御イベントは検出されません。
- **strict** プロファイルでは、block 応答がすべてのクライアントおよびサーバーの重大度が critical、high、medium のスパイウェア イベントに適用され、default アクションが low および informational の脆弱性防御イベントに使用されます。

カスタマイズしたプロファイルを使用して、信頼されたセキュリティ ゾーン間のトラフィックに対する脆弱性の検査を最小限に抑え、インターネットなどの信頼されていないゾーンから受信したトラフィックや、サーバー ファームなどの機密性の高い宛先に送信されるトラフィックの保護を最大化できます。脆弱性防御プロファイルをセキュリティ ポリシーに適用する方法については、「Policies (ポリシー) > Security (セキュリティ) 」を参照してください。

トラフィックを許可するすべてのセキュリティポリシー ルールに脆弱性保護プロファイルを適用し、バッファオーバーフロー、不正なコードの実行、およびクライアント側およびサーバー側の脆弱性を狙ったその他の攻撃から保護します。

Rules [ルール] 設定では、有効にする一連のシグネチャと、一連のシグネチャのいずれかがトリガーされたときに実行するアクションを指定します。

例外設定では、特定のシグネチャに対するレスポンスを変更できます。たとえば、シグネチャに一致するすべてのパケットをブロックするが選択したシグネチャに一致するパケットはブロックしないでアラートを生成するということが可能です。**Exception**[例外] タブでは、フィルタリング機能がサポートされています。

Vulnerability Protection[脆弱性防御] ページには、一連のデフォルト列が表示されます。列を選択するオプションを使用すれば、その他の情報列を表示できます。列ヘッダーの右側にある矢印をクリックし、Columns [カラム] サブメニューから列を選択します。

以下の表では、脆弱性防御プロファイル設定について説明します。

脆弱性防御プロファイル設定	の意味
氏名	プロファイル名 (最大 31 文字) を入力します。この名前は、セキュリティポリシーを定義するときに脆弱性防御プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、ピリオド、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有 (Panorama のみ)	以下に対してプロファイルを公開する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

脆弱性防御プロファイル設定	の意味
	• multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこの脆弱性防御プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
Rules (ルール) タブ	
ルール名	ルールの識別に使用する名前を指定します。
脅威名	照合するテキスト文字列を指定します。ファイアウォールは、このテキスト文字列のシグネチャ名を検索して一連のシグネチャをルールに適用します。
CVEリスト	指定した CVE に一致する場合にのみシグネチャを適用するには、CVE (Common Vulnerabilities and Exposures) を指定します。 各 CVE の形式は CVE-yyyy-xxxx になります。ここで、yyyy は年、xxxx は一意識別子です。このフィールドで文字列の照合を実行できます。たとえば、2011 年の脆弱性を検索するには「2011」と入力します。
ホスト タイプ	ルールのシグネチャをクライアント側、サーバー側、またはいずれか (**any**) に限定するかどうかを指定します。
重要度	指定した重大度にも一致する場合にのみシグネチャを適用するには、照合する重大度 (**informational**[通知]、**low**[低]、**medium**[中]、**high**[高]、または **critical**[重要]) を選択します。
操作	ルールがトリガーされたときに実行するアクションを選択します。アクションのリストについては、「セキュリティ プロファイルのアクション」を参照してください。 **Default**[デフォルト] アクションは、Palo Alto Networks によって提供された各シグネチャの一部である事前定義のアクションに基づきます。シグネチャのデフォルトのアクションを表示するには、**Objects** (オブジェクト) > **Security Profiles** (セキュリティ プロファイル) > **Vulnerability Protection** (脆弱性防御) を選択し、**Add** (追加) をクリックするか、既存のプロファイルを選択します。**Exceptions** (例外) タブをクリックして **Show all signatures** (すべてのシグネチャの表示) をオンにすると、すべてのシグネチャと関連する **Action** (アクション) のリストが表示されます。 セキュリティを最大限に高めるために、クライアントおよびサーバー両方の *critical* (重要)、*high* (高)、*medium* (中) の重大度を持つイベントに対する *Action* (アクション) を*reset-both*に設定し、*Informational* (通知) および *Low* (低) の重大度を持つ

© 2019 Palo Alto Networks, Inc.

脆弱性防御プロファイル設定	の意味
	イベントに対してデフォルトのアクションを使用してください。
パケット キャプチャ	識別されたパケットをキャプチャする場合は、このオプションを選択します。 脅威が検出されたときに 1 つのパケットをキャプチャするには、**single-packet**、1 ~ 50 個のパケットをキャプチャするには、**extended-capture** オプションを選択します（デフォルトは 5 パケットです）。extended-capture では、脅威ログを分析するときに脅威についてより詳細なコンテクストを得られます。パケット キャプチャを表示する場合は、**Monitor**（監視）> **Logs**（ログ）> **Threat**（脅威）を選択し、関心のあるログ エントリを見つけて、第 2 列にある緑の下矢印をクリックします。キャプチャするパケットの数を定義するには、 **Device**（デバイス）> **Setup**（セットアップ）> **Content-ID** を選択し、Content-ID 設定を編集します。 パケット キャプチャは、アクションが **allow** (許可) または **alert** (アラート) の場合にのみ行われます。**block** (ブロック) アクションが設定されている場合、セッションは即座に終了します。 重大度が *critical* (重要)、*high* (高)、*medium* (中) のイベント用に拡張キャプチャを、重大度が *low* (低) のイベント用に単一パケット キャプチャを有効化します。デフォルトの拡張キャプチャの値（*5* パケット）を使用することで、大抵の場合に脅威を分析するための十分な情報を得られます。（パケット キャプチャのトラフィックが多すぎると、パケット キャプチャをドロップするおそれがあります） 重大度が高いイベントと比べて情報のキャプチャがそれ程役立たず、低い値のトラフィックが比較的多く発生するため、*informationa* (通知) のイベントに対してパケット キャプチャを有効化しないでください。 ログに記録するトラフィックを判断するために使用するロジックと同じものを使用して拡張パケット キャプチャを適用します（ブロックするトラフィックを含め、ログに記録するトラフィックの拡張キャプチャを行います）。
Exceptions [例外] タブ	
脅威	見つかった脅威が実際には脅威でないことが定かな場合のみ（誤検出）、脅威例外を作成します。誤検出が見つかったと考えられる場合は、*TAC* を使ってサポートケースを開始し、*Palo Alto Networks* が誤って検出された脅威を調査できるようにしてください。問題が解決されたら、プロファイルからすぐに例外を削除します。 アクションを割り当てようとしている脅威に対して**Enable**[有効化] をそれぞれ選択するか、**All**[すべて] を選択してリストにあるすべての脅威に対するアクションを有効化します。このリストは、選択したホスト、カテゴリ、および重大度によって異なります。リストが空の場合、現在の選択に対応する脅威がないことを表します。 各ドロップダウンリストからアクションを選択するか、リストの上部にある **Action**[アクション] のドロップダウンリストからアクションを選択してすべて

© 2019 Palo Alto Networks, Inc.

脆弱性防御プロファイル設定	の意味
	の脅威に同じアクションを適用します。**Show All**[すべてを表示] を選択した場合、すべてのシグネチャが表示されます。そうでない場合は例外となるシグネチャのみが表示されます。 識別されたパケットをキャプチャする場合は、**Packet Capture** (パケット キャプチャ) を選択します。 脆弱性シグネチャ データベースには、総当たり攻撃を表すシグネチャが格納されています。たとえば、Threat ID 40001 は FTP 総当たり攻撃でトリガーされます。総当たり攻撃のシグネチャは、特定の時間のしきい値で条件が発生した場合にトリガーされます。総当たり攻撃のシグネチャのしきい値は事前に設定されています。これは、(**Custom**[カスタム] オプションが選択された状態で) **Vulnerability**[脆弱性] タブの脅威の名前の横にある編集 ( ) をクリックして変更できます。単位時間あたりのヒット数やしきい値の適用先 (送信元、宛先、または送信元と宛先の組み合わせ) を指定できます。 しきい値は、送信元 IP、宛先 IP、または送信元 IP と宛先 IP の組み合わせに適用できます。 デフォルトのアクションが、かっこに囲まれて表示されます。CVE列には、CVE (Common Vulnerabilities and Exposures) の識別子が表示されます。これらは、公開されている情報セキュリティの脆弱性に対応する共通の一意の識別子です。 IP Address Exemptions (IP アドレスの除外) 列をクリックして、脅威例外をフィルタリングする IP アドレスを **Add** (追加) します。脅威例外に IP アドレスを追加する場合、そのシグネチャの脅威例外アクションは、送信元または宛先 IP アドレスのいずれかが例外の IP アドレスに一致するセッションによってシグネチャがトリガーされる場合にのみ、ルールのアクションよりも優先されます。シグネチャあたり最大 100 個の IP アドレスを追加できます。10.1.7.8 や 2001:db8:123:1::1 などのユニキャス IP アドレス (ネットマスクのないアドレス) を入力する必要があります。IP アドレスの除外を追加すると、特定の IP アドレスの例外を作成するために新しいポリシー ルールと新しい脆弱性プロファイルを作成する必要がなくなります。
ベンダー ID	指定したベンダー ID に一致する場合にのみシグネチャを適用するには、ベンダー ID を指定します。 たとえば、Microsoft のベンダー ID の形式は MSyy-xxx になります。ここで、yy は 2 桁の年で、xxx は一意識別子です。たとえば、2009 年の Microsoft を照合するには Search (検索) フィールドに「MS09」と入力します。
カテゴリ	脆弱性のカテゴリに一致する場合にのみシグネチャを適用するには、脆弱性のカテゴリを選択します。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]

URL フィルタリング プロファイルを使用すれば、Web コンテンツへのアクセスを制御できるだけでなく、ユーザーが Web コンテンツとやり取りする方法を制御することもできます。

確認すべき情報	以下を参照
URL カテゴリに基づいて Web サイトへのアクセスを制御する。	URL フィルタリング カテゴリ
企業認証情報の送信を検出して、ユーザーが認証情報を送信できる URL カテゴリを判断します。	ユーザー証明書検出 URL フィルタリング カテゴリ
エンドユーザーが最も厳格なセーフ サーチ設定を使用していない場合に検索結果をブロックします。	URL フィルタリング設定
HTTP ヘッダーのロギングを有効にする。	URL フィルタリング設定
カスタム HTTP ヘッダを使用する Web サイトへのアクセスを制御する。	HTTP ヘッダの挿入
その他の情報をお探しですか？	• URL フィルタリングを設定する方法を詳しく学びます。 • URL カテゴリを使用してクレデンシャル フィッシングを防止します。 • カスタム URL カテゴリを作成する手順については、「Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> URL Category（URL カテゴリ）」を参照してください。 • 適用したい URL のリストをインポートするには、Objects > External Dynamic Lists [オブジェクト > 外部動的リスト]を選択します。

URL フィルタリングの一般設定

以下の表では、一般的な URL フィルタリング設定について説明します。

一般設定	の意味
氏名	プロファイル名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときに URL フィルタリング プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要

© 2019 Palo Alto Networks, Inc.

一般設定	の意味
	があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、このプロファイルを継承するデバイス グループでこの URL フィルタリング プロファイルの設定をオーバーライドすることを禁止するには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

URL フィルタリング カテゴリ

Objects (オブジェクト) > **Security Profiles** (セキュリティ プロファイル) > **URL Filtering** (**URL** フィルタリング) > **Categories** (カテゴリ) を選択して、URL に基づく Website へのアクセスを制御します。

カテゴリ設定	の意味
カテゴリ	Web アクセスおよび使用状況ポリシーを定義できる URL カテゴリとリストを表示します。デフォルトでは、**Site Access** (サイト アクセス) 権限と **User Credential Submission** (ユーザー証明書送信) 権限は、すべてのカテゴリで **Allow** (許可) に設定されます。 URL カテゴリおよびリストは 3 つのドロップダウンリストにグループ化されています： • **Custom URL Categories** (カスタム **URL** カテゴリ)—カスタム URL カテゴリを定義する場合はObjects > Custom Objects > URL Category [オブジェクト > カスタム オブジェクト > URL カテゴリ]を選択します。URL のリストあるいは複数の事前定義済みカテゴリに基づいてカスタム URL カテゴリを決定できます。 • **External Dynamic URL Lists** (外部動的 **URL** リスト)—ファイアウォールが WEB サーバーから得た URL のリストをインポートできるようにする場合はObjects > External Dynamic Lists [オブジェクト > 外部動的リスト]を選択します。 • **Pre-defined Categories** (事前定義済みカテゴリ)—PAN-DB、Palo Alto Networks URL、IP クラウド データベースが定義した URL カテゴリをすべて列挙します。 既知の危険な *URL* カテゴリをすべて*Block* (ブロック) し、以下のようなエクスプロイトの侵入、マルウェアのダウンロード、コマンド アンド コントロール攻撃、データ流出から保護します。 コマンド アンド コントロール、 著作権侵害、ダイ

© 2019 Palo Alto Networks, Inc.

カテゴリ設定	の意味
	ナミック *DNS*、 過激主義、 マルウェア、 フィッシング、 プロキシ回避と匿名プロキシ、 未知、 新規登録ドメイン、 グレイウェア、 パークドメイン。 ブロック ポリシーを段階的に導入する場合は、カテゴリを*continue* (続行)に設定してカスタム応答ページを作成するようにし、ユーザーに利用規約を周知させ、脅威をもたらす可能性があるサイトに訪問しているということを知らせるようにします。適切な期間の後、悪意のある可能性があるこれらのサイトをブロックするポリシーに移行します。
サイト アクセス	URL カテゴリごとに、ユーザーがそのカテゴリの URL にアクセスしようとしたときに実行する操作を選択します。 • **alert**[アラート] – Webサイトへのアクセスを許可しますが、ユーザーがそのURLにアクセスするたびにURLログにアラートが追加されます。 ブロックしないトラフィックのカテゴリに対する *Action* (アクション) として*alert* (アラート)を設定し、アクセスの試みをログに記録し、トラフィックに対する可視性を得られるようにします。 • **allow**[許可] – Webサイトへのアクセスが許可されます。 *allow* (許可)はブロックされないトラフィックをログに記録しないため、アクセスの試みをログに記録し、トラフィックに対する可視性を得たい場合は、トラフィックのカテゴリに対する *Action* (アクション) として*alert* (アラート)を設定してください。 • **block** (ブロック)– Web サイトへのアクセスがブロックされます。URL カテゴリへの Site Access (サイト アクセス) をブロックに設定すると、User Credential Submission (ユーザー証明書送信) 権限も自動的にブロックに設定されます。 • **continue** (続行)–ユーザーに警告ページを表示し、Web サイトにアクセスしないよう促します。その後、ユーザーが警告を無視することにした場合は Web サイトへのアクセスを**Continue** (続行)する選択を行う必要があります。 プロキシ サーバーを使用するように設定されているクライアント マシンでは、続行 (警告) ページは正しく表示されません。 • **override** (オーバーライド) – 応答ページを表示して、有効なパスワードを入力してサイトにアクセスするようにユーザーに要求します。パスワードやその他のオーバーライド設定を行う場合は、**Device** (デバイス) > **Setup** (設定) > **Content ID** (コンテンツ **ID**) を開き、URL 管理者オーバーライド設定を編集します (「Device (デバイス) > Setup (設定) > Content-ID (コンテンツ ID) 」の管理設定の表も参照してください) 。 プロキシ サーバーを使用するように設定されているクライアント マシンでは、オーバーライド ページは正しく表示されません。 • **none** (なし) (カスタムURLカテゴリのみ) – カスタムURLカテゴリを作成してあり、ファイアウォールにURLデータベースベンダーからURLフィルタリングカテゴリを継承させる場合はアクションを**none** (なし) に設定します。アクションを**none** (なし) に設定することで、URLフィルタリングプロファ

© 2019 Palo Alto Networks, Inc.

カテゴリ設定	の意味
	イルに含まれるカスタムカテゴリを無視するような柔軟な設定が可能になり、ポリシールール（セキュリティ、復号化、およびQoS）の一致条件としてカスタムURLカテゴリを使用し、例外を設定したり、異なるアクションを実行させることができます。カスタムURLカテゴリを削除する場合は、そのカスタムカテゴリが使用されているすべてのプロファイルでアクションをnone[なし] に設定する必要があります。カスタム URL カテゴリの詳細は、「Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> URL Category（URL カテゴリ）」を参照してください。
ユーザー証明書送信	URL カテゴリごとに **User Credential Submissions**（ユーザー証明書送信）を選択し、ユーザーが有効な企業認証情報をそのカテゴリの URL に送信することを許可または禁止します。URL カテゴリに基づいてユーザー認証情報の送信を制御する前に、認証情報送信検出を有効にする必要があります（**User Credential Detection**（ユーザー証明書送信）タブを選択）。 **Site Access**（サイト アクセス）をブロックに設定した URL カテゴリでは、ユーザー認証情報送信も自動的にブロックするように設定されます。 • **alert**（アラート）– 認証情報を Web サイトに送信することをユーザーに許可しますが、ユーザーがこのカテゴリのサイトに認証情報を送信するたびに、URL フィルタリング ログを生成します。 • **allow**（許可）（デフォルト）– ユーザーが認証情報を Web サイトに送信することを許可します。 • **block**（ブロック）– ユーザーが認証情報を Web サイトに送信することをブロックします。デフォルトのアンチフィッシング応答ページでは、ユーザー認証情報送信がブロックされます。 • **continue**（続行）– 応答ページを表示し、ユーザーが **Continue** (続行) を選択して認証情報をサイトに送信することを要求します。デフォルトでは、アンチフィッシング続行ページを表示し、認証情報の送信が勧められないサイトにユーザーが認証情報を送信しようとしたとき、ユーザーに警告します。カスタム応答ページを作成してフィッシングの企てについてユーザーに警告するか、その他の Web サイトで有効な企業認証情報を再利用しないようにユーザーを教育するかを選択できます。
URL カテゴリをチェック	クリックして PAN-DB URL フィルタリング データベースにアクセスします。そこでは、URL または IP アドレスを入力してカテゴリ情報を表示できます。
動的 URL フィルタリング（デフォルトで無効） （BrightCloud のみに設定可能）	URL を分類するためのクラウド検索を有効にする場合に選択します。URL の分類にローカル データベースを使用できない場合、このオプションが呼び出されます。 5 秒のタイムアウト中に URL を解決できない場合、応答は「`Not resolved URL`」として表示されます。 *PAN-DB* を使用する場合、このオプションはデフォルトで有効にされており、設定できません。

URL フィルタリング設定

Objects（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **URL Filtering**（**URL** フィルタリング）> **URL Filtering Settings**（**URL** フィルタリング設定）を選択すると、安全な検索設定が適用され、HTTP ヘッダのログが有効になります。

© 2019 Palo Alto Networks, Inc.

URL フィルタリング設定	内容
コンテナ ページのみログを記録 デフォルト:enabled [有効化]	指定したコンテンツタイプに一致するURLのみを記録する場合は、このオプションを選択します。セッション中にファイアウォールはアドバタイズメントやコンテンツ リンクなどのログ関連の Web リンクをログに記録しないため、関連する URL をログに記録しつつ、ロギングおよびメモリの読み込みが削減されます。 送信元の元の *IP* アドレスをマスクするプロキシを使用する場合、HTTP Header Logging (HTTP ヘッダのロギング) *X-Forwarded-For*オプションを有効化し、*Web* ページのリクエストを開始したユーザーの元の *IP* アドレスを保持します。
セーフ サーチ適用の有効化 デフォルト:disabled この機能を使用する場合、URL フィルタリング ライセンスは不要です。	厳密なセーフサーチフィルタリングを適用する場合は、このオプションを選択します。 多くの検索エンジンには、検索クエリ リターン トラフィックでアダルト画像やアダルト動画を除外するセーフ サーチ設定が備わっています。セーフ サーチの適用を有効にする設定を選択すると、ユーザーが最も厳密なセーフ サーチ設定を検索クエリで使用していない場合、ファイアウォールでは検索結果がブロックされます。ファイアウォールでは次の各プロバイダーのセーフ サーチを使用できます。Google、Yahoo、Bing、Yandex、YouTube。これは、ベスト エフォート設定であり、すべての Web サイトで機能することを検索プロバイダが保証しているわけではありません。 セーフ サーチを使用するには、この設定を有効にしてから、URL フィルタリング プロファイルをセキュリティ ポリシー ルールに添付する必要があります。これにより、ファイアウォールは、一致する検索クエリ リターン トラフィックのうち、最も厳密なセーフ サーチ設定を使用していないトラフィックをブロックします。 *Yahoo*アカウントにログイン中に*Yahoo Japan (yahoo.co.jp)* で検索を実行する場合は、検索設定のロックオプションも有効にする必要があります。 ユーザーが他の検索プロバイダを使用してこの機能を迂回しないようにするには、*URL* フィルタリング プロファイルで *search-engines* カテゴリをブロックするように設定してから、*Bing*、*Google*、*Yahoo*、*Yandex*、*YouTube* へのアクセスを許可します。
HTTP ヘッダのロギング	HTTP ヘッダーのロギングを有効にすると、サーバーに送信された HTTP 要求に含まれる属性を表示できます。有効な場合、以下の属性-値ペアの 1 つ以上が URL フィルタリング ログに記録されます。 • ユーザー エージェント – ユーザーが URL へのアクセスに使用する Web ブラウザ。この情報は、HTTP 要求でサーバーに送信されます。たとえば、ユーザー エージェントは Internet Explorer または Firefox である可能性があります。ログ内のユーザー エージェント値は最大 1024 文字をサポートします。 • 参照 – ユーザーを別の Web ページにリンクした Web ページの URL。要求された Web ページにユーザーをリダイレクト (参照) した送信元です。ログ内の参照値は最大 256 文字をサポートします。 • x-forwarded-for – Web ページを要求したユーザーの IP アドレスを保持するヘッダー フィールド オプション。特にネットワーク上にプロキシ サーバーがある場合や、送信元 NAT を実装している場合は、すべての要求がプロキシ

© 2019 Palo Alto Networks, Inc.

URL フィルタリング設定	内容
	サーバーの IP アドレスまたは共通の IP アドレスから送信されているかのようにユーザーの IP アドレスがマスクされてしまうため、これによりユーザーの IP アドレスを識別できて役立ちます。ログ内の x-forwarded-for 値は最大 128 文字をサポートします。

ユーザー証明書検出

Objects（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **URL Filtering**（**URL** フィルタリング）> **User Credential Detection**（ユーザー認証情報検知）を選択すると、ユーザーが認証情報書を送信した際にファイアウォールが検出できるようになります。

ユーザー認証情報検知を設定して *URL* カテゴリで指定されたサイトにのみユーザーが認証情報を送信できるようにし、信頼されていないカテゴリのサイトに認証情報を送信するのを防ぐことで、攻撃の入り口を減らします。ユーザー認証情報の送信のために *URL* フィルタリング プロファイルですべての *URL* カテゴリをブロックする場合は、認証情報をチェックする必要はありません。

ファイアウォールでは、3 つの方法のいずれかが使用されて、Web ページに送信される、有効な認証情報が検出されます。それぞれの方法では User-ID™ が必要であり、これによってファイアウォールは、Web ページに送信されるユーザー名とパスワードを有効な企業認証情報と比較できるようになります。いずれかの方法を選択してから、URL カテゴリに基づいて認証情報のフィッシングを阻止 してください。

ユーザーの認証情報を監視するには、トラフィックを 復号 するようにファイアウォールを設定する必要があります。

ユーザー証明書検出の設定	の意味
IP ユーザー	この認証情報検出方法では、有効なユーザー名の送信がチェックされます。この方法を使用すると、有効な企業ユーザー名を含む認証情報の送信を（付随するパスワードに関係なく）検出できます。ファイアウォールでは、セッションの送信元 IP アドレスにログインしたユーザーにユーザー名が一致することが確認されて、ユーザー名の一致が判断されます。この方法を使用する場合、ファイアウォールは、送信されるユーザー名を IP アドレスとユーザー名のマッピング テーブルと照合します。この方法を使用するには、「Map IP Addresses to Users（IP アドレスとユーザーのマッピング）」で説明されているユーザー マッピング方法のいずれかを使用できます。
グループ マッピング	ファイアウォールは、制限されているサイトにユーザーが送信するユーザー名が有効な企業ユーザー名と一致するかどうかを判断します。これを行うため、ファイアウォールは、送信されるユーザー名をユーザーとグループのマッピング テーブルのユーザー名のリストと照合し、ユーザーが制限されているカテゴリのサイトに企業ユーザー名を送信することを検出します。 この方法では、LDAP グループ メンバーシップに基づいて企業ユーザー名の送信のみがチェックされるため、設定は簡単ですが、誤検出が多くなる傾向があります。この方法を使用するには、グループ マッピングを有効にする 必要があります。

© 2019 Palo Alto Networks, Inc.

ユーザー証明書検出の設定	の意味
Domain Credential（ドメイン証明書）	この認証情報検出方法では、ファイアウォールによって、有効な企業ユーザー名と関連パスワードをチェックできます。ファイアウォールは、ユーザーが送信するユーザー名とパスワードが、同じユーザーの企業ユーザー名とパスワードと一致するかどうかを判断します。 これを行うため、ファイアウォールは、送信される認証情報を有効な企業ユーザー名とパスワードと照合し、送信されるユーザー名が、ログイン ユーザーの IP アドレスに対応することを確認できる必要があります。このモードは Windows ベースの User-ID エージェントのみでサポートされ、User-ID エージェントが読み取り専用ドメイン コントローラ（RODC）にインストールされていて、User-ID 認証情報サービス アドオンが装備されている必要があります。この方法を使用するには、認証ポリシー、キャプティブ ポータル、GlobalProtect™ などのサポート対象ユーザー マッピング方法を使用して、User-ID が IP アドレスをユーザーにマッピングできるようにする必要もあります。 ファイアウォールが有効な企業認証情報の送信のチェックに使用できる方法の詳細、およびフィッシング防御を有効にする手順については、「Prevent Credential Phishing（認証情報フィッシングの防止）」を参照してください。
有効なユーザー名検出済みログ重大度	ファイアウォールが、有効なユーザー名の Web サイトへの送信を検出したことを示すログの重大度を設定します。 このログ重大度は、認証情報送信の権限が、アラート、ブロック、継続のいずれかになっている Web サイトに、有効なユーザー名が送信されるイベントに関連付けられます。認証情報の送信が許可されている Web サイトに、ユーザーが有効なユーザー名を送信することを記録するログの重大度は通知になります。認証情報の送信の許可やブロックを行う URL カテゴリの確認または調整を行うには、**Categories**（カテゴリ）を選択してください。 ログの重大度を *medium* (中) 以上に設定してください。

HTTP ヘッダの挿入

ファイアウォールが HTTP ヘッダとその値を HTTP 要求に挿入して Web アプリケーションへのアクセスを管理できるようにするには、**Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > URL Filtering (URL フィルタリング) > HTTP Header Insertion (HTTP ヘッダ挿入)**を選択します。

ファイアウォールは、*HTTP/1.x* トラフィックのヘッダ挿入のみをサポートします。ファイアウォールは、*HTTP/2* トラフィックのヘッダ挿入をサポートしていません。

定義済みの HTTP ヘッダ挿入タイプに基づいて挿入エントリを作成することも、独自のカスタムタイプを作成することもできます。ヘッダ挿入は通常、カスタム HTTP ヘッダに対して実行されますが、標準 HTTP ヘッダを挿入することもできます。

ヘッダ挿入は、次の場合に発生します。

1. HTTP 要求が、1 つまたは複数の HTTP ヘッダ挿入エントリが設定されたSecurity (セキュリティ) ポリシー ルールと一致する。
2. 指定されたドメインが、HTTP ホスト ヘッダにあるドメインと一致する。
3. アクションは ブロック以外です。

© 2019 Palo Alto Networks, Inc.

ファイアウォールは、*GET*、*POST*、*PUT*、および *HEAD* メソッドに対してのみ *HTTP* ヘッダ挿入を実行できます。

HTTP ヘッダの挿入を有効にし、識別されたヘッダーが要求にない場合、ファイアウォールはヘッダを挿入します。識別されたヘッダが要求にすでに存在する場合、ファイアウォールはヘッダ値を指定した値で上書きします。

挿入エントリを **Add** (追加) 追加するか、既存の挿入エントリを選択して変更します。必要に応じて、挿入項目を選択してから **Delete** (削除) することもできます。

新しい *HTTP* ヘッダ挿入エントリのデフォルトのブロック リスト アクションは *Block* (ブロック) です。別のアクションが必要な場合は、URL フィルタリング カテゴリに進み、適切なアクションを選択します。または、目的のアクションで構成されたプロファイルに挿入エントリを追加します。

HTTP ヘッダの挿入設定	の意味
氏名	HTTP ヘッダ挿入エントリの **Name** (名前) 。
タイプ	作成するエントリの **Type** (タイプ) 。エントリは、事前定義済みまたはカスタムのいずれかです。ファイアウォールはコンテンツ更新を使用して、事前定義済みエントリを入力・管理します。 HTTP ヘッダにユーザー名を含める場合は **Dynamic Fields** (ダイナミック フィールド)を選択します。
ドメイン	ヘッダ挿入は、このリスト内のドメインが HTTP 要求の Host ヘッダと一致すると発生します。 定義済みのエントリを作成する場合、ドメイン リストはコンテンツ更新であり事前定義されています。ほとんどの使用例ではこれで十分ですが、必要に応じてドメインを追加または削除できます。 カスタム エントリを作成するには、少なくとも 1 つのドメインをこのリストに **Add** (追加) します。 各ドメイン名は最大 256 文字まで入力することができ、エントリごとに最大 50 のドメインを識別できます。アスタリスク (*) をワイルドカード文字として使用できます。これは、指定されたドメイン (* .etrade.com など) へのすべての要求に一致します。
ヘッダー	定義済みのエントリを作成する場合、ヘッダ リストはコンテンツ更新により事前作成されます。ほとんどの使用例ではこれで十分ですが、必要に応じてヘッダを追加または削除できます。 カスタム エントリを作成するときは、このリストに 1 つ以上のヘッダ (合計 5 つまで) を追加します。 ヘッダ名には 100 文字まで使用できますが、スペースは使用できません。 ユーザー名を HTTP ヘッダに含める場合は **X-Authenticated-User** を選択してから **Value** (値)を選択するか、新しいヘッダを **Add** (追加) します。
Value (値)	最大 512 文字を使用して **Value** (値) をコンフィグします。ヘッダ値は、指定したドメインの HTTP ヘッダに含める情報によって異なります。例えば、 SaaS アプリケーションへのユーザー アクセスを管理 するには 事前定義済みタイプ を選択するか カスタム エントリを使用します。

© 2019 Palo Alto Networks, Inc.

HTTP ヘッダの挿入設定	の意味
	HTTP ヘッダにユーザ名を含めるには、セキュリティ アプライアンスに要求されるドメインとユーザー名の形式を選択します。 • **(`$domain`)\(`$user`)** • **`WinNT://`(`$domain`)/(`$user`)** または、 **(`$user`)** および **(`$domain`)** ダイナミック トークンを使用してカスタム形式を入力します (**(`$user`)@(`$domain`)** など)。 ファイアウォールは、グループ マッピング プロファイルのプライマリ ユーザー名を使用して、ユーザーとドメインのダイナミック トークンを入力します。 各 ***(`$user`)*** および ***(`$domain`)*** ダイナミック トークンは、値ごとに *1* 回だけ使用します。
ログ	このヘッダ挿入エントリのロギングを有効にするには、**Log** (ログ) を選択します。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > File Blocking [オブジェクト > セキュリティ プロファイル > ファイル ブロッキング]

ファイル ブロッキング プロファイルをセキュリティ ポリシー ルールに割り当てて（Policies（ポリシー）> Security（セキュリティ））、ユーザーが指定のファイル タイプをアップロードまたはダウンロードすることを禁止したり、指定のファイル タイプをアップロードまたはダウンロードしようとしたときにアラートを生成したりできます。

事前定義済みの*strict* (厳格)なプロファイルを適用することで、セキュリティを最大化できます。*strict* (厳格)なプロファイルがブロックするファイル形式を使用する重要なアプリケーションをサポートしなければならない場合は、*strict* (厳格)なプロファイルをコピーして必要なファイル形式の例外だけを適用します。対象のファイル形式を必要とする送信元、宛先、ユーザーだけに例外を許すセキュリティポリシー ルールに、コピーしたプロファイルを適用します。また、*Direction* (方向)を使用して例外をアップロードあるいはダウンロードに制限することもできます。

Windows PE ファイルを一部ブロックしない場合は、未知のファイルをすべて *WildFire* に送信して分析を行ってください。ユーザーアカウントについては *Action* (アクション)を*continue* (続行)に設定し、悪意のある *Web* サイト、メール、ポップアップがユーザーに意図せず悪意のあるファイルをダウンロードさせるドライブバイダウンロード攻撃を防ぎます。自分が開始していないファイル転送を求める *Continue* (続行) プロンプトが表示された場合、危険なダウンロードを行おうとしている可能性があるということをユーザーに周知させてください。

以下の表では、ファイル ブロッキング プロファイル設定について説明します。

ファイル ブロッキング プロファイル設定	の意味
氏名	プロファイル名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときにファイル ブロッキング プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有（Panorama のみ）	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化（Panoramaのみ）	管理者が、プロファイルを継承するデバイス グループのこのファイル ブロッキング プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっ

© 2019 Palo Alto Networks, Inc.

ファイル ブロッキング プロファイル設定	の意味
	ており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

ルール	1 つ以上のルールを定義して、選択したファイル タイプで実行するアクション (存在する場合) を指定します。ルールを追加するには、以下を指定して **Add**[追加] をクリックします。
	• **Name** (名前) – ルール名 (最大 31 文字) を入力します。
	• **Applications**[アプリケーション] – ルールを適用するアプリケーションを選択するか、**any**[すべて] を選択します。
	• **File Types**[ファイルタイプ] – ファイルタイプのフィールドをクリックし、**Add**[追加] をクリックするとサポートされているファイルタイプの一覧が表示されます。プロファイルに追加したいファイルタイプをクリックし、必要に応じファイルタイプを追加します。**Any**[すべて] を選択した場合、設定したアクションがすべてのファイルタイプに対して実行されます。
	• **Direction**[方向] – ファイル転送の方向 (**Upload**、**Download**、または **Both**) を選択します。
	• **Action**[アクション] – 選択したファイル タイプの検出時に実行するアクションを選択します。
	  • **alert**[アラート] – エントリが脅威ログに追加されます。
	  • **continue**[継続] – ダウンロードがリクエストされたことを通知して、続行するかどうかを確認するようにユーザーに求めるメッセージが表示されます。この目的は、認識されないダウンロード (ドライブバイダウンロードとも呼ばれる) の可能性があることをユーザーに警告し、そのダウンロードの続行または停止をユーザーが選択できるようにすることです。
	  continue (続行) アクションを使用してファイル ブロッキング プロファイルを作成する場合、選択できるアプリケーションは **web-browsing** のみです。その他のアプリケーションを選択すると、ユーザーには続行ページのプロンプトが表示されないため、セキュリティ ポリシー ルールに一致するトラフィックはファイアウォールを通過しません。
	  • **block**[ブロック] – ファイルがブロックされます。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > WildFire Analysis [オブジェクト > セキュリティ プロファイル > WildFire 分析]

WildFire 分析プロファイルでは、WildFire アプライアンスまたは WildFire クラウドでローカルに実行される WildFire ファイル分析を指定します。ファイル タイプ、アプリケーション、またはファイルの送信方向 (アップロードまたはダウンロード) に応じて、パブリック クラウドまたはプライベート クラウドにトラフィックを転送するよう指定できます。作成した WildFire分析プロファイルをポリシーに追加することによって (**Policies** > **Security** [ポリシー > セキュリティ])、そのプロファイルの設定をそのポリシーに一致する任意のトラフィック (たとえば、そのポリシーに定義されているURLカテゴリ) に適用できるようになります。

事前定義済みのデフォルト プロファイルを使用し、未知のファイルをすべて WildFire に転送して分析を行います。さらに、WildFire アプライアンスのコンテンツ更新を毎分ダウンロードおよびインストールするよう設定し、常に最新のサポートを得られるようにします。

WildFire 分析プロファイルの設定	
氏名	WildFire 分析プロファイルの分かりやすい名前 (最大 31 文字) を入力します。この名前は、セキュリティ ポリシー ルールを定義する際に選択候補となる WildFire 分析プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	(任意) プロファイル ルールまたはプロファイルの用途の説明です (255 文字まで)。
共有 (Panorama のみ)	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化 (Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこの脆弱性防御プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
ルール	WildFire パブリック クラウドまたは WildFire アプライアンス (プライベート クラウド) にトラフィックを転送して分析するように指定する 1 つ以上のルールを定義します。 • プロファイルに追加する任意のルールの分かりやすい **Name**[名前] (最大 31 文字) を入力します。

© 2019 Palo Alto Networks, Inc.

WildFire 分析プロファイルの設定	

	• **Application**[アプリケーション] を追加して、任意のアプリケーショントラフィックがルールと照合され、指定した分析用の宛先に転送されるようにします。
	• そのルール用の定義済みの分析用の宛先で分析する **File Type**[ファイルタイプ] を選択します。
	
	WildFire プライベート クラウド (*WildFire* アプライアンスによってホストされる) は、*APK*、*Mac OS X*、アーカイブ、および *Linux* ファイルの分析をサポートしていません。
	
	• 送信の **Direction**[方向] に応じてトラフィックにルールを適用します。アップロード トラフィック、ダウンロード トラフィック、またはその両方にルールを適用できます。
	• トラフィックを転送して分析する **Destination**[宛先] を選択します。
	  • ルールと照合されるすべてのトラフィックを WildFire パブリック クラウドに転送して分析する場合は、public-cloud を選択します。
	  • ルールと照合されるすべてのトラフィックを WildFire アプライアンスに転送して分析する場合は、private-cloud を選択します。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Data Filtering [オブジェクト > セキュリティ プロファイル > データ フィルタリング]

データ フィルタリングを使用すると、ファイアウォールはクレジット カード番号、社会保障番号、社内ドキュメントなどの機密情報を検出し、このようなデータが安全なネットワークから漏出するのを防ぐことができます。データ フィルタリングを有効にする前に、Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> Data Patterns（データ パターン）を選択し、フィルタリングするデータのタイプ（社会保障番号や社外秘と記載されたドキュメントのタイトルなど）を定義します。複数のデータ パターン オブジェクトを 1 つのデータ フィルタリング プロファイルに追加できます。セキュリティ ポリシー ルールに割り当てると、ファイアウォールは各データ パターンの許可されたトラフィックをスキャンし、データ フィルタリング プロファイル設定に基づいて一致するトラフィックをブロックします。

データ フィルタリング プロファイル設定	の意味
氏名	プロファイル名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときにログ転送プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有（Panorama のみ）	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化（Panoramaのみ)	管理者が、プロファイルを継承するデバイス グループのこのデータ フィルタリング プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
データ キャプチャ	フィルタによってブロックされたデータを自動的に収集するア場合は、このオプションを選択します。 *Settings (設定) ページの Manage Data Protection (データ保護の管理) にキャプチャしたデータを表示するためのパスワードを指定します。「Device（デバイス）> Setup（セットアップ）> Management（管理）」を参照してください。*

© 2019 Palo Alto Networks, Inc.

データ フィルタリング プロファイル設定	の意味
データ パターン	フィルタリングで使用する既存のデータ パターンを追加するか、**New**（新規）を選択して新しいデータ パターン オブジェクトを設定します（Objects（オブジェクト）> Custom Objects（カスタム オブジェクト）> Data Patterns（データ パターン））。
アプリケーション [applications]	フィルタリング ルールに含めるアプリケーションを指定します。 • 表示されているすべてのアプリケーションにフィルタを適用するには、**any**[すべて] を選択します。これを選択してもすべてのアプリケーションがブロックされるわけではなく、表示されているアプリケーションのみがブロックされます。 • **Add**[追加] をクリックして個々のアプリケーションを指定します。
ファイル タイプ	フィルタリング ルールに含めるファイル タイプを指定します。 • 表示されているすべてのファイル タイプにフィルタを適用するには、**any**[すべて] を選択します。これを選択してもすべてのファイル タイプがブロックされるわけではなく、表示されているファイル タイプのみがブロックされます。 • **Add**[追加] をクリックして個々のファイル タイプを指定します。
指示	フィルタを適用する方向 (アップロード、ダウンロード、または両方) を指定します。
アラートしきい値	アラートをトリガーするまでのファイルのデータ パターン検出回数を指定します。
ブロックしきい値	データ パターンがこの回数以上出現するファイルをブロックします。
ログ重大度	このデータ フィルタリング プロファイル ルールに一致するイベントで記録されるログ重大度を定義します。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > DoS Protection [オブジェクト > セキュリティ プロファイル > DoS プロテクション]

DoS プロテクション プロファイルは、高精度のターゲット指定ができるように設計され、ゾーン プロテクション プロファイルを補強します。DoS プロテクション プロファイルでは、（DoS プロテクション ポリシーで指定した）アラームやアクションをトリガーする 1 秒あたりの新規接続数（CPS）のしきい値レートを指定します。DoS プロテクション プロファイルでは、最大 CPS レートやブロックされた IP アドレスをブロック IP リストに保持する時間も指定します。DoS 保護ポリシールール内で DoS 保護プロファイルを指定し、そこでさらにルールにマッチさせるパケットの条件を指定します。ポリシールールはプロファイルを適用するデバイスを決定します。

DoS 保護プロファイル、および重要な個々のデバイスあるいは小規模のデバイス グループ、特に *WEB* サーバーやデータベースサーバーなどのインターネットに接続されたデバイスを保護するポリシーを作成します。

DoS プロテクション プロファイルを設定できます。集約プロファイル、分類化プロファイル、あるいは各タイプのうち一つを DoS 保護ポリシールールに適用できます。両方のプロファイル タイプを単一のルールに適用すると、ファイアウォールは初めに集約プロファイルを適用してから、必要な場合に分類化プロファイルを適用します。

- 分類化 DoS 保護プロファイルでは、**Classified (分類化)**が**Type (タイプ)**として選択されています。分類化 DoS 保護プロファイルをアクションが**Protect**（保護）の DoS 保護ルールに適用する際、ファイアウォールは、パケットが指定のアドレス タイプ（source-ip-only（宛先 IP のみ）、destination-ip-only（宛先 IP のみ）、src-dest-ip-both（送信元 IP と宛先 IP の両方））に一致した場合にプロファイルの CPS のしきい値に対して接続をカウントします。
- 集約 DoS 保護プロファイルでは、**Aggregate (集約)**が**Type (タイプ)**として選択されています。アクションが**Protect (保護)**である DoS 保護ルールを集約 DoS 保護プロファイルに適用する際、ファイアウォールはルールの条件を満たすすべての接続（ルールで指定されたデバイス グループの合計接続数）をプロファイルの CPS しきい値に対して加味します。

DoS プロテクション プロファイルを DoS プロテクション ポリシーに適用する方法については、「Policies（ポリシー）> DoS Protection（DoS プロテクション）」を参照してください。

マルチ仮想システム（マルチ *vsys*）がある環境で、以下を設定している場合は、

- 仮想システム間の通信が可能な外部ゾーン
- 仮想システムが外部通信に共通インターフェイスおよび *1* つの *IP* アドレスを共有できる共有ゲートウェイ

以下のゾーンおよび *DoS* プロテクション メカニズムが、外部ゾーンで無効になります。

- *SYN cookies*
- *IP* フラグメント
- *ICMPv6*

IP フラグメントと *ICMPv6* 防御を有効にするには、共有ゲートウェイ用のゾーン プロテクション プロファイルを作成します。

共有ゲートウェイで *SYN* フラッドから保護するには、ランダム早期ドロップまたは *SYN Cookie* のいずれかを設定した *SYN* フラッド防御プロファイルを適用できます。外部ゾーンでは、*SYN* フラッド防御にランダム早期ドロップのみを使用できます。

© 2019 Palo Alto Networks, Inc.

DOS プロテクション プロファイルの設定	
氏名	プロファイル名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときにログ転送プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	プロファイルの説明を入力します (最大 255 文字)。
共有（Panorama のみ）	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化（Panoramaのみ）	管理者が、プロファイルを継承するデバイス グループのこの DoS プロテクション プロファイルの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
タイプ	以下のいずれかのプロファイル タイプを選択します。 • **Aggregate**（集約）– プロファイルで設定された DoS のしきい値がルール条件（このルール条件に基づいてプロファイルが適用される）に一致するすべての接続に適用されます。例えば、SYN フラッドの**Alarm Rate (アラーム レート)**のしきい値が 10,000 CPS である集約ルールは、DoS ルールにマッチするすべてのデバイスの合計接続数をカウントします。グループの合計 CPS が 10,000 CPS を超えると、デバイス間でどのように CPS が分散されているかに関わらず、アラームが発生します。 • **Classified**（分類）– プロファイルで設定された DoS のしきい値が、分類条件（送信元 IP アドレス、宛先 IP アドレス、または送信元 IP アドレスと宛先 IP アドレスのペア）を満たす各接続に適用されます。例えば、SYN フラッドの**Alarm Rate (アラーム レート)**のしきい値が 10,000 CPS である分類化ルールはデバイス毎に最大 10,000 CPS を許容し、DoS ルールで指定された任意のデバイスが 10,000 CPS を超えるとアラームを発生させます。
Flood Protection [フラッド防御] タブ	
SYN Flood（SYN フラッド）タブ UDP Flood [UDP フラッド] タブ ICMP Flood [ICMP フラッド] タブ ICMPv6 Flood (ICMPv6 フラッド) タブ	タブに記載されたタイプのフラッド防御を有効化する場合はこのオプションを選択し、以下を指定します。 • **Action**（アクション）–（**SYN Flood**（**SYN** フラッド）のみ）DoS プロテクション ポリシー アクションが **Protect**（保護）で、CPS が **Activate Rate**（アクティベート率）に達した場合にファイアウォールが実行するアクション。以下のいずれかを選択します。 • **Random Early Drop**（ランダム早期ドロップ）– 1 秒あたりの接続数が **Activate Rate**（アクティベート率）しきい値に達すると、ランダムにパケットをドロップします。

© 2019 Palo Alto Networks, Inc.

DOS プロテクション プロファイルの設定	
Other IP Flood (その他の IP フラッド) タブ	• **SYN cookie** – SYN フラッド攻撃中に接続をドロップせずに済むように SYN Cookie を使用して受信確認を生成します。 正当なトラフィックを公正に扱い、しかしファイアウォール リソースを多く消費する *SYN Cookie* から始めます。*CPU* とメモリの使用率を監視し、*SYN Cookie* がリソースを多く消費しすぎている場合は *RED* に切り替えます。ネットワーク（インターネット）の末端で大量の *DoS* 攻撃を防止する専用の *DDoS* 防止デバイスがない場合は、必ず *RED* を使用します。 • **Alarm Rate**（アラーム レート）– DoS アラームを生成するしきい値レート（CPS）を指定します（範囲は 0 ~ 2,000,000 cps、デフォルトは 10,000 cps）。 分類化プロファイルの場合、しきい値をデバイスの平均 CPS レートよりも 15 ~ 20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。集約プロファイルの場合、しきい値をグループの平均 CPS レートよりも 15 ~ 20% 高く設定することがベストプラクティスになります。必要に応じてしきい値を監視して調整します。 • **Activate Rate**（アクティベート率）– DoS 応答が起動されるしきい値レート（cps）を指定します。DoS 応答は、DoS プロテクション プロファイルの **Action**（アクション）フィールドで設定します（Random Early Drop（ランダム早期ドロップ）または SYN cookies）。**Activate Rate**（アクティベート率）の範囲は 0 ~ 2,000,000 cps で、デフォルトは 10,000 cps です。 プロファイルの **Action**（アクション）が **Random Early Drop**（ランダム早期ドロップ）（RED）の場合、1 秒あたりの受信接続数が **Activate Rate**（アクティベート率）しきい値に達すると、RED が発生します。CPS レートを増やすと、アルゴリズムに従って RED レートが増加します。ファイアウォールは、CPS レートが **Max Rate**（最大レート）しきい値に達するまで RED を繰り返します。 分類化プロファイルは CPS の限界を厳密に個々のデバイスに適用します。その限界は保護するデバイスの能力に基づいて決定するため、ユーザーは徐々に CPS をスロットルする必要が無く、**Activate Rate (**アクティベート レート**)**を**Max Rate (**最大レート**)**と同じしきい値に設定することができます。**Max Rate (**最大レート**)**に達する前に個々のサーバーに向かうトラフィックをドロップし始めたい場合のみ、**Activate Rate (**アクティベートレート**)**を**Max Rate (**最大レート**)**より低く設定します。集約プロファイルの場合、しきい値をグループのピーク時 CPS レートよりもほんの少し大きな値に設定します。必要に応じてしきい値を監視して調整します。 • **Max Rate**（最大レート）– ファイアウォールで許容する 1 秒あたりの受信接続数のしきい値を設定します。**Max Rate**（最大レート）しきい値に達すると、ファイアウォールは新しい接続を 100% ドロップします（範囲は 2 ~ 2,000,000 cps、デフォルトは 40,000 cps）。 分類化プロファイルの場合はフラッドが生じないよう、保護しているデバイスの能力に基づいて**Max Rate (**最大レート**)**を決定します。集約プロファイルの場合、**Max Rate (**最大レート**)**をグループの能力の 80 ~ 90% に設定します。必要に応じてしきい値を監視して調整します。

© 2019 Palo Alto Networks, Inc.

DOS プロテクション プロファイルの設定	
	• **Block Duration**（ブロック期間）— 問題のある IP アドレスをブロック IP アドレスに保持し、この IP アドレスの接続をブロックする秒数を指定します。ブロック期間（範囲は 1 ~ 21,600、デフォルトは 300 秒）に到達したパケットは、Alarm Rate（アラーム レート）、Activate Rate（アクティベート率）、または Max Rate（最大レート）しきい値に対してカウントされません。
Resources Protection [リソース保護] タブ	
セッション数	リソース保護を有効化する場合は、このオプションを選択します。
最大同時制限	同時セッションの最大数を指定します。 • **Aggregate**（集約）プロファイル タイプの場合、DoS プロテクション ルール（このルールに基づいて DoS プロテクション プロファイルが適用される）に該当するすべてのトラフィックにこの制限が適用されます。 • **Classified**（分類）プロファイル タイプの場合、分類（送信元 IP、宛先 IP、または送信元 IP と宛先 IP の組み合わせ）に基づいて、DoS プロテクション プロファイルが適用される DoS プロテクション ルールに該当するトラフィックにこの制限が適用されます。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション）

GTP プロテクション プロファイルを使用すると、ファイアウォールは GTP トラフィックを検査できます。このプロファイルを表示するには、Device（デバイス）> Setup（セットアップ）> Management（管理）で GTP セキュリティを有効にする必要があります。

プロファイルのオプションでは、GTP v1-C、GTP v2-C、GTP-U のステートフル検査を有効にしたり、GTPv1-C、GTP v2-C、GTP-U のプロトコル検証を有効にしたり、GTP-U コンテンツ検査を有効にして GTP-U トンネル内のユーザー データをスキャンしたりできます。また、APN、IMSI プレフィックス、RAT に基づいて GTP セッションをフィルタリングしたり、エンドユーザーの IP アドレス スプーフィングを防止してモバイル加入者が超過請求されないように保護したりできます。

GTP 検査プロファイル設定	
GTP 検査	

GTP-C	• ファイアウォールで **GTPv1-C** または **GTPv2-C** あるいはその両方を検索できるようにするには、**Stateful Inspection**（ステートフル検査）を選択します。ステートフル検査を有効にすると、ファイアウォールは送信元 IP、送信元ポート、宛先 IP、宛先ポート、プロトコル、トンネル エンドポイント ID（TEID）を使用して、GTP セッションを追跡します。また、GTP トンネルを確立するために使用される各種 GTP メッセージの順序をチェックして検証します。TEID は GSN トンネル エンドポイントを一意に識別します。アップリンク用のトンネルとダウンリンク用のトンネルは区別され、異なる TEID が使用されます。
	• 有効性チェック エラー時にファイアウォールが実行する **Action**（アクション）（**Block**（ブロック）または**Alert**（アラート））を選択します。アラート アクションでは、トラフィックを許可してログを生成します。ブロック アクションでは、トラフィックを拒否してログを生成します。
	• ファイアウォールがペイロードの GTP ヘッダーおよび情報要素（IE）で実行する必要のある有効性チェックを指定します。ファイアウォールは、上記で選択したブロック アクションまたはアラート アクションを使用してエラーを処理します。以下を検証するようにファイアウォールを設定できます。
	  • **Reserved IE**（予約済み **IE**）— 予約済み IE 値が使用されている GTPv1-C または GTPv2-C メッセージをチェックします。
	  • **Out of Order IE**（順序が不適切な **IE**）（GTPv1-C のみ）— GTPv1-C メッセージの IE の順序が正しいかどうかをチェックします。
	  • **Length of IE**（**IE** の長さ）— IE の長さが無効な GTPv1-C または GTPv2-C メッセージをチェックします。
	  • **Reserved field in header**（ヘッダーの予約済みフィールド）— ヘッダーに無効な値または予約済みの値が使用されている不正な形式のパケットをチェックします。
	  • **Unsupported message type**（サポートされていないメッセージ タイプ）— 未知または不正なメッセージ タイプをチェックします。

© 2019 Palo Alto Networks, Inc.

GTP 検査プロファイル設定	
GTP-U	GTPv1-C または GTPv2-C のステートフル検査を有効にすると、自動的に GTP-U ステートフル検査が有効になります。 GTP-U ペイロードの以下の有効性チェックを指定できます。 • **Reserved IE**（予約済み **IE**）— ペイロードに予約済み IE 値が使用されている GTP-U メッセージをチェックします。 • **Out of order IE**（順序が不適切な **IE**）— GTP-U メッセージの IE の順序が正しいかどうかをチェックします。 • **Length of IE**（**IE** の長さ）— IE の長さが無効なメッセージをチェックします。 • **Reserved field in header**（ヘッダーの予約済みフィールド）— ヘッダーに無効な値または予約済みの値が使用されている不正な形式のパケットをチェックします。 • **Unsupported message type**（サポートされていないメッセージ タイプ）— 未知または不正なメッセージ タイプをチェックします。 また、以下の許可アクション、ブロック アクション、またはアラート アクションを設定できます。 • **End User IP Address Spoofing**（エンド ユーザーの **IP** アドレス スプーフィング）— 加入者ユーザーの機器から送信された GTP-U パケットの送信元 IP アドレスが、トンネルのセットアップ中に変換された、対応する GTP-C メッセージの IP アドレスと同じでない場合にブロックまたはアラートするようにファイアウォールを設定します。 • **GTP-in-GTP** — GTP-in-GTP メッセージの検出時にブロックまたはアラートするようにファイアウォールを設定できます。検出すると、ファイアウォールは重大度が critical（重要）の GTP ログを生成します。 • GTP-U パケット内のユーザー データ ペイロードを検査してポリシーを適用する場合、**GTP-U Content Inspection**（**GTP-U** コンテンツ検査）を有効にします。GTP-U コンテンツを検査すると、GTP-C メッセージから学習した IMSI および IMEI 情報と GTP-U パケットのカプセル化された IP トラフィックを相関できます。
フィルタリング オプション	
RAT フィルタリング	デフォルトでは、すべての無線アクセス テクノロジ（RAT）が許可されます。GTP-C の PDP 作成要求およびセッション作成要求メッセージは、RAT フィルタに基づいてフィルタリングまたは許可されます。モバイル コア ネットワークにアクセスするためにユーザーの機器で使用される以下のリモート アクセス テクノロジ（RAT）に基づいて、許可、ブロック、アラートするかどうかを指定できます。 • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **HSPA** の進化 • **EUTRAN** • 仮想 • **EUTRAN-NB-IoT**

© 2019 Palo Alto Networks, Inc.

GTP 検査プロファイル設定	
IMSI フィルタリング	IMSI（国際モバイル加入者識別番号）は、加入者識別モジュール（SIM）カードでプロビジョニングされた GSM、UMTS、LTE ネットワークの加入者に関連付けられた一意の ID です。 通常、IMSI は 15 桁の数値（8 バイト）で表されますが、これよりも短い場合もあります。IMSI は、以下の 3 つの部分で構成されます。 • 3 桁で構成されるモバイル国コード（MCC）。MCC は、モバイル加入者の居住国を一意に識別します。 • 2 桁（欧州標準）または 3 桁（北米標準）で構成されるモバイル ネットワーク コード（MNC）。MNC は、モバイル加入者のホーム PLMN を識別します。 • PLMN 内のモバイル加入者を識別するモバイル加入者識別番号（MSIN）。 **IMSI Prefix**（**IMSI** プレフィックス）では、MCC と MNC を組み合わせて、特定の GTP からのトラフィックを**allow** (許可)、**block** (ブロック)、あるいは**alert** (アラート)できます。デフォルトでは、すべての IMSI が許可されます。 IMSI または IMSI プレフィックスを手動で入力するか、それらが含まれる csv ファイルをファイアウォールにインポートできます。IMSI には、310* や 240011* などのワイルドカードを含めることができます。 ファイアウォールでは、最大 5000 個の IMSI または IMSI プレフィックスがサポートされています。
APN フィルタリング	アクセス ポイント名（APN）は、ユーザーの機器でインターネットに接続するために必要な GGSN/PGW への参照です。APN は、以下の 2 つの部分で構成されます。 • GGSN/PGW（必要に応じてモバイル ステーションによって要求されるサービス）が接続される外部ネットワークを定義する APN ネットワーク識別子。APN のこの部分は必須です。 • GGSN/PGW がある PLMN GPRS/EPS バックボーンを定義する APN オペレータ識別子。APN のこの部分は任意です。 デフォルトでは、すべての APN が許可されます。APN フィルタでは、APN 値に基づいて GTP トラフィックを許可、ブロック、アラートできます。GTP-C の PDP 作成要求およびセッション作成要求メッセージは、APN フィルタリングに定義されたルールに基づいてフィルタリングまたは許可されます。 APN フィルタリング リストを手動でファイアウォールに追加またはインポートできます。APN の値には、ネットワーク ID またはネットワークのドメイン名（example.com など）、および必要に応じてオペレータ ID を含める必要があります。 APN フィルタリングの場合、ワイルドカード「*」を使用すると、すべての APN を照合できます。「*」と他の文字の組み合わせは、ワイルドカードではサポートされていません。たとえば、「internet.mnc *」は通常の APN として扱われ、internet.mnc で始まるすべてのエントリをフィルタリングしません。 ファイアウォールでは、最大 1000 個の APN フィルタがサポートされています。
GTP Tunnel Limits（GTP トンネル制限）	

© 2019 Palo Alto Networks, Inc.

GTP 検査プロファイル設定	
宛先当たりの許可された最大同時トンネル数	GGSN などの宛先 IP アドレスへの GTP-U トンネルの最大数を制限できます。 範囲:0 ~ 100000000 トンネル。
宛先当たりの最大同時トンネル数でのアラート	ある宛先に対して確立された GTP-U トンネルの最大数に達したときにファイアウォールがアラートをトリガーするしきい値を指定します。設定したトンネル制限に達すると、重大度が high (高) の GTP ログ メッセージが生成されます。
ロギング頻度	設定した GTP トンネル制限を超えたときにファイアウォールがカウントするイベント数。この数を超えるとログが生成されます。この設定を使用して、ログに記録されるメッセージ量を削減できます。 デフォルト:100; 範囲:1-100000000
超過請求の保護	ファイアウォールの Gi/SGi ファイアウォールとして機能する仮想システムを選択します。Gi/SGi ファイアウォールは、PGW/ GGSN から Gi/SGi インターフェイスを通過してインターネットなどの外部 PDN (パケット データ ネットワーク) へ送信されるモバイル加入者の IP トラフィックを検査し、モバイル加入者のインターネット アクセスを保護します。 GGSN がエンド ユーザー IP アドレス プールから以前に使用した IP アドレスをモバイル加入者に割り当てると、超過請求が発生する可能性があります。インターネット上の悪意のあるサーバーが以前の加入者のために開始されたセッションを終了せずにこの IP アドレスにパケットを送信し続けると、このセッションは Gi ファイアウォールで開いたままになります。 (PDP 削除メッセージまたはセッション削除メッセージによって) GTP トンネルが検出されるか、タイムアウトしたときにデータが配信されないようにするために、超過請求保護が有効になっているファイアウォールは、加入者に属しているすべてのセッションをセッション テーブルから削除するように Gi/ SGi ファイアウォールに通知します。GTP セキュリティと SGi/Gi ファイアウォールは同じ物理ファイアウォールに設定する必要がありますが、仮想システムは異なっていても問題ありません。GTP-C イベントに基づいてセッションを削除するには、ファイアウォールにすべての関連するセッション情報が必要です。これが可能なのは、モバイル コア ネットワークで SGi + S11 または S5 インターフェイス (GTPv2) および Gi + Gn インターフェイス (GTPv1) からのトラフィックを管理している場合だけです。
その他のログ設定 デフォルトでは、ファイアウォールは許可された GTP メッセージをログに記録しません。許可された GTP メッセージのロギングは大量のログが生成されるため、トラブルシューティングで必要な場合に選択的に有効化できます。このタブでは、許可されたログ メッセージ以外にもユーザー ロケーション情報のロギングを選択的に有効化できます。	
GTPv1-C の許可されたメッセージ	GTPv1-C のステートフル検査が有効になっている場合、許可された GTPv1-C メッセージのロギングを選択的に有効化できます。これらのメッセージで生成されるログは、必要に応じて問題をトラブルシューティングするのに役立ちます。 デフォルトでは、ファイアウォールは許可されたメッセージをログに記録しません。許可された GTPv1-C メッセージのロギング オプションは、以下のとおりです。

© 2019 Palo Alto Networks, Inc.

GTP 検査プロファイル設定	
	• **Tunnel Management**（トンネル管理）– これらの GTPv1-C メッセージは、SGSN と GGSN などのネットワーク ノードの特定のペア間でカプセル化された IP パケットとシグナル メッセージを送信する GTP-U トンネルの管理に使用されます。これには、PDP コンテキスト作成要求、PDP コンテキスト作成応答、PDP コンテキスト更新要求、PDP コンテキスト更新応答、PDP コンテキスト削除要求、PDP コンテキスト削除応答などのメッセージが含まれます。 • **Path Management**（パス管理）– 通常、これらの GTPv1-C メッセージは、ピアがアライブ状態かどうかを確認するために GSN または無線ネットワーク制御局（RNC）から他の GSN または RNC に送られます。これには、エコー要求/応答などのメッセージが含まれます。 • **Others**（その他）– これらのメッセージには、場所の管理、モビリティの管理、RAN 情報の管理、およびマルチメディア ブロードキャスト マルチキャスト サービス（MBMS）などのメッセージが含まれます。
ユーザー ロケーションを記録	エリア コードやセル ID などのユーザー ロケーション情報を GTP ログに含めることができます。
パケット キャプチャ	GTP イベントをキャプチャできるようになります。
GTPv2-C の許可されたメッセージ	GTPv2-C のステートフル検査が有効になっている場合、許可された GTPv2-C メッセージのロギングを選択的に有効化できます。これらのメッセージで生成されるログは、必要に応じて問題をトラブルシューティングするのに役立ちます。 デフォルトでは、ファイアウォールは許可されたメッセージをログに記録しません。許可された GTPv2-C メッセージのロギング オプションは、以下のとおりです。 • **Tunnel Management**（トンネル管理）– これらの GTPv2-C メッセージは、SGW と PGW などのネットワーク ノードの特定のペア間でカプセル化された IP パケットとシグナル メッセージを送信する GTP-U トンネルの管理に使用されます。これには、以下のメッセージ タイプが含まれます。セッション作成要求、セッション作成応答、ベアラ作成要求、ベアラ作成応答、ベアラ変更要求、ベアラ変更応答、セッション削除要求、セッション削除応答。 • **Path Management**（パス管理）– 通常、これらの GTPv2-C メッセージは、ピアがアライブ状態かどうかを確認するために SGW または PGW などのネットワーク ノードから他の SGW または PGW に送信されます。これには、エコー要求/応答などのメッセージが含まれます。 • **Others**（その他）– これらのメッセージには、モビリティの管理や 3GPP 以外のアクセスに関連するメッセージなどが含まれます。
GTP-U の許可されたメッセージ	GTPv1-C のステートフル検査が有効になっている場合、許可された GTPv1-C メッセージのロギングを選択的に有効化できます。これらのメッセージで生成されるログは、必要に応じて問題をトラブルシューティングするのに役立ちます。 許可された GTP-U メッセージのロギング オプションは、以下のとおりです。 • **Tunnel Management**（トンネル管理）– これらはエラー兆候などの GTP-U シグナル メッセージです。 • **Path Management**（パス管理）– これらの GTP-U メッセージは、ピアがアライブ状態かどうかを確認するためにネットワーク ノード（eNodeB

© 2019 Palo Alto Networks, Inc.

GTP 検査プロファイル設定	
	など）から別のネットワーク ノード（SGW など）に送られます。これには、エコー要求/応答などのメッセージが含まれます。 • **G-PDU** – G-PDU（GTP-U PDU）は、モバイル コア ネットワークのネットワーク ノード内のユーザー データ パケットを送信するために使用され、GTP ヘッダーと T-PDU で構成されます。
新しい GTP-U 当たりのログされた G-PDU パケット	ファイアウォールで GTP-U PDU が検査されていることを確認するには、このオプションを有効にします。ファイアウォールは、新しい GTP-U トンネルごとに指定した数の G-PDU パケットのログを生成します。 デフォルト:1; 範囲:1 ~ 10。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> SCTP Protection（SCTP プロテクション）

ファイアウォールでSCTPチャンクの検証とフィルタリングを行う方法を指定する、Stream Control Transmission Protocol (SCTP)（ストリーム制御伝送プロトコル（SCT`））プロテクション プロファイルを作成します。このプロファイルタイプをセキュリティ プロファイルの下に表示するには、 SCTP セキュリティ（**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **General Settings**（一般設定））を有効にする必要があります。また、マルチホーム環境で SCTP エンドポイントごとの IP アドレス数を制限することもできるほか、ファイアウォールが SCTP イベントを記録するタイミングを指定することもできます。SCTP プロテクション プロファイルを作成したら、ゾーンのセキュリティ ポリシー ルールにプロファイルを適用する必要があります。

SCTP セキュリティをサポートするファイアウォール モデルには、事前定義済みの SCTP プロテクション プロファイル（デフォルト - ss7）がそのまま使用できます。また、default-ss7 プロファイルを新しい SCTP プロテクション プロファイルの基礎として複製できます。**Object**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **SCTP Protection**（**SCTP** プロテクション）を選択し、 **default-ss7**（デフォルト**-ss7**）を選ぶと、この定義済みプロファイルのアラートを引き起こす操作コードが表示されます。

SCTP プロテクション プロファイル設定	
氏名	SCTP プロテクション プロファイルの名前を入力します。
の意味	SCTP プロテクション プロファイルの説明を入力します。
SCTP Inspection SCTP インスペクション	
不明なチャンク	不明なチャンク（RFC3758、RFC4820、RFC4895、RFC4960、RFC5061、または RFC 6525で定義されないチャンク）を含む SCTP を受信する場合のファイアウォールのアクションを選択します: • **allow**（許可）（デフォルト）–パケットに変更を加えないで通過させます。 • **alert**（アラート）–パケットを変更せずに通過させ、SCTP ログを生成させます（これらのログにはログ ストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。 • **block**（ブロック）–パケットを渡す前にチャンクを無効にし、SCTP ログを生成します。
Chunk Flags チャンクフラグ	RFC4960 と矛盾するチャンク フラグを持つ SCTP パケットを受信したときに、ファイアウォールの動作を選択します。 • **allow**（許可）（デフォルト）–パケットに変更を加えないで通過させます。

© 2019 Palo Alto Networks, Inc.

SCTP プロテクション プロファイル設定	
	• **alert**（アラート）–パケットを変更せずに通過させ、SCTP ログを生成させます（これらのログにはログ ストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。 • **block**（ブロック）–パケットをドロップし、SCTP ログを生成します。
Invalid Length 不正な長さ	無効な長さの SCTP チャンクを受信したときに、ファイアウォールの動作を選択します。 • **allow**（許可）（デフォルト）–パケットまたはチャンクに変更を加えないで通過させます。 • **block**（ブロック）–パケットを破棄して SCTP ログを生成します（これらのログにはログ ストレージを割り当てる必要があります。Log Storage (ログ ストレージ) タブを参照してください。
マルチホーミングのIPアドレスの制限数：	ファイアウォールがアラート メッセージを生成する前に、SCTP エンドポイントに設定できる IP アドレスの最大数を入力します（範囲は 1〜8、デフォルトは 4）。 SCTP マルチホーミングは、ピアとの関連付けのために複数の IP アドレスをサポートするエンドポイントの機能です。エンドポイントへの 1 つのパスが失敗すると、SCTP は、そのアソシエーションに提供されている他の宛先 IP アドレスの 1 つを選択します。
ログ設定	許可されたチャンク、アソシエーションの開始と終了、および状態の失敗イベントの SCTP ログを生成する設定の任意の組み合わせを選択します。 • **Log at Association Start** アソシエーション開始時にロギング • **Log at Association End** アソシエーション終了時にロギング • **Log Allowed Association Initialization Chunks** 許可されたアソシエーション初期化チャンクをロギング • **Log Allowed Heartbeat Chunks** 許可されたハートビート チャンクをロギング • **Log Allowed Association Termination Chunks** 許可されたアソシエーション終了チャンクをロギング • **Log All Control Chunks** すべての制御チャンクをロギング • **Log State Failure Events** ログ状態 失敗イベント ファイアウォールが SCTP ログを保存する場合は、SCTP ログ ストレージを割り当てる必要があります（詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。
フィルタリング オプション	
SCTP Filtering SCTP フィルタリング	
氏名	SCTP フィルタの名前を入力します。

© 2019 Palo Alto Networks, Inc.

SCTP プロテクション プロファイル設定	
PPID	SCTP フィルタの PPID を指定します。 • **any**（すべて）–ファイアウォールは、PPID を含むすべての SCTP データ チャンクで指定したアクションを実行します。 • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • 有効な PPID 値（ドロップダウン リストにない値）を入力します。たとえば、H.323 の PPID 値は 13 です。 各 SCTP フィルタで指定できる PPID は 1 つだけですが、SCTP 保護プロファイルに複数の SCTP フィルタを指定できます。
操作	ファイアウォールが指定した PPID を含むデータ チャンクにかかる処理を指定します。 • **allow**（許可）（デフォルト）–チャンクに変更を加えないで通過させます。 • **alert**（アラート）–チャンクを変更せずに通過させ、SCTP ログを生成させます（これらのログにはログ ストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。 • **block**（ブロック）–パケットを渡す前にチャンクを無効にして SCTP ログを生成します（これらのログのログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。
SCTP パケットは、リスト内のフィルタと上から下に一致します。プロファイル用に複数の SCTP フィルタを作成する場合は、SCTP フィルタの順序が異なります。SCTP フィルタリング リストで相対優先度を変更するには、フィルタを 1 つ選択して**Move Up**（上へ）または **Move Down**（下へ）移動します。	
ダイアメーター フィルタリング	
氏名	ダイアメーター フィルタの名前を入力します。
操作	ファイアウォールが実行する、ダイアメーター アプリケーション ID、コマンド コード、および AVP を含むダイアメーター チャンクで実行するアクションを指定します。検査されたチャンクが、指定されたダイアメーター アプリケーション ID と、指定されたダイアメータ コマンド

© 2019 Palo Alto Networks, Inc.

SCTP プロテクション プロファイル設定	
	コードのすべてと、指定されたダイアメータ AVP のいずれかを含む場合は、以下の操作を行います。 • **allow**（許可）（デフォルト）–チャンクに変更を加えないで通過させます。 • **alert**（アラート）–チャンクを変更せずに通過させ、SCTP ログを生成させます（これらのログにはログ ストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。 • **block**（ブロック）–パケットを渡す前にチャンクを無効にして SCTP ログを生成します（これらのログのログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。
ダイアメーター アプリケーション ID	ファイアウォールが指定された処理を行うチャンクの ダイアメーター アプリケーション ID を指定します。 • すべて • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • ダイアメーター基礎アカウンティング • ダイアメーター一般メッセージ • ダイアメーター クレジット制御 また、ダイアメーター アプリケーション ID の数値を入力することもできます（範囲は 0〜4、294,967,295）。ダイアメーター フィルタは、1 つのアプリケーション ID しか持つことができません。
ダイアメーター コマンド コード	ファイアウォールが指定された処理を行うチャンクの ダイアメーター コマンド コード を指定します。**any**（すべて）を選択し、ドロップダウンリストからダイアメーター コマンド コードの 1 つを選択するか、または特定の値を入力します（範囲は0〜16,777,215）。ドロップダウンには、選択したダイアメーター アプリケーション ID に適用されるコマンド コードのみが含まれています。複数のダイアメーター コマンド コードをダイアメーター フィルタに追加することができます。
ダイアメーター AVP	ファイアウォールが指定された処理を行うチャンクのダイアメーター属性値ペア（AVP）コードを指定します。1 つ以上の AVP コードまたは値を入力します（範囲は1〜16,777,215）。
プロファイル用に複数のダイアメーター フィルタを作成する場合は、ダイアメーター フィルタの順序が異なります。ダイアメーター フィルタリング リストで相対優先度を調節するには、フィルタを 1 つ選択して**Move Up**（上へ）または **Move Down**（下へ）移動します。	

© 2019 Palo Alto Networks, Inc.

SCTP プロテクション プロファイル設定	
SS7 Filtering SS7 フィルタリング	
氏名	SS7 フィルタの名前を入力します。
操作	ファイアウォールが指定した SS7 フィルタ要素 を含む SS7 チャンクにかかる処理を指定します。検査されるチャンクが SCCP 発呼者 SSN と指定された SCCP 発呼者 グローバル タイトル (GT) 値および指定された運用コードのいずれかを含む場合 : • **allow** (許可) (デフォルト) –チャンクに変更を加えないで通過させます。 • **alert** (アラート) –チャンクを変更せずに通過させ、SCTP ログを生成させます (これらのログにはログ ストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ : Device (デバイス) > Setup (セットアップ) > Management (管理) を参照してください。 • **block** (ブロック) –パケットを渡す前にチャンクを無効にして SCTP ログを生成します (これらのログのログストレージを割り当てる必要があります。詳細は、Logging and Reporting Settings (ロギングおよびレポート設定) のところにある Log Storage (ログ ストレージ) タブ : Device (デバイス) > Setup (セットアップ) > Management (管理) を参照してください。
SCCP Calling Party SSN SCCP 発呼者 SSN	ファイアウォールが指定された処理を行うチャンクの SCCP 発呼者 SSN を指定します。**any-map** (すべてのマップ) を選択するか、SCCP 発呼者 SSN の 1 つをドロップダウンリストから**Add** (追加) します。 • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **SCCP 管理** SS7フィルタは、SCCP 発呼者 SSNを 1 つしか持つことができません。
SCCP Calling Party GT SCCP 発呼者 GT	ファイアウォールが指定された処理を行うチャンクの SCCP 発呼者 GT 値 を指定します。**Any** (すべて) を選択するか、最大 15 桁の数値を **Add** (追加) します。また、プレフィックスを使用して、SCCP 発呼者 GT 値のグループを入力することもできます。以下がその例です。876534*。複数の SCCP 発呼者 GT値を SS7 フィルタに追加できます。

© 2019 Palo Alto Networks, Inc.

SCTP プロテクション プロファイル設定	
	SCCP 発呼者 SSN のが以下の場合:**INAP** と **SCCP Management**（**SCCP** 管理）では、このオプションは無効になります。
運用コード	ファイアウォールが指定された処理を行うチャンクの運用コード を指定します。 次の SCCP 発呼者 SSNの場合は、**any**（すべて）ドロップダウンリストからすべてまたは運用コードを選択するか、特定の値（範囲は1〜255）を入力します。 • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** SCCP 発呼者 SSN のが以下の場合:**CAP** の場合は、値を入力します（1 ~ 255）。 SCCP 発呼者 SSN のが以下の場合:**INAP** と **SCCP Management**（**SCCP** 管理）では、このオプションは無効になります。 複数の運用 コードを SS7 フィルタに追加することができます。
プロファイル用に複数の SS7 フィルタを作成する場合は、SS7 フィルタの順序が異なります。SS7 フィルタリング リストで相対優先度を調節するには、フィルタを 1 つ選択して**Move Up**（上へ）または **Move Down**（下へ）移動します。	

© 2019 Palo Alto Networks, Inc.

Objects > Security Profile Groups [オブジェクト > セキュリティ プロファイル グループ]

ファイアウォールでは、セキュリティ プロファイルのセットを指定してセキュリティ プロファイル グループを作成する機能がサポートされています。セキュリティ プロファイル グループは、1 つの単位として処理でき、セキュリティ ポリシーに追加できます。たとえば、脅威セキュリティ プロファイル グループを作成して、アンチウイルス、アンチスパイウェア、および脆弱性防御の各プロファイルを追加し、その後、セキュリティ ポリシー ルールを作成してその脅威プロファイルを追加することができます。

同時に割り当てられることが多いアンチウイルス、アンチスパイウェア、脆弱性防御、URL フィルタリング、およびファイル ブロッキングの各プロファイルをプロファイル グループにまとめることで、セキュリティ ポリシーの作成を簡略化できます。

新しいセキュリティ プロファイルを定義するには、**Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）を選択します。

以下の表では、セキュリティプロファイル設定について記載しています。

セキュリティ プロファイル グループ設定	の意味
氏名	プロファイル グループ名（最大 31 文字）を入力します。この名前は、セキュリティ ポリシーを定義するときにプロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有（Panorama のみ）	以下に対してプロファイルグループを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルグループが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した**Device Group**[デバイスグループ] のみに対してプロファイルグループが公開されます。
オーバーライドの無効化（Panoramaのみ）	管理者が、オブジェクトを継承するデバイス グループのこのセキュリティ プロファイル グループ オブジェクトの設定をオーバーライドすることを禁止する場合はこのオプションを選択してください。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
プロファイル	グループに含めるアンチウイルス、アンチスパイウェア、脆弱性防御、URLフィルタリング、およびファイルブロッキングの各プロファイルを選択します。データ フィルタリング プロファイルも、セキュリティ プロファイル グループに含めることができます。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> Data Filtering（データ フィルタリング）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects > Log Forwarding [オブジェクト > ログ転送]

デフォルトでは、ファイアウォールで生成されるログはそのローカル ストレージにのみ存在します。ただし、Panorama™、ログ サービス、または外部サービス（syslog サーバーなど）を使用して、ログ転送情報を定義し、そのプロファイルをセキュリティ、認証、DoS 保護、およびトンネル検査のポリシー ルールに割り当てることにより、ログ情報を集中的に監視できます 。ログ転送プロファイルは、次の Log Types（ログタイプ）の転送先を定義します。データ フィルタリング、GTP、SCTP、脅威、トラフィック、トンネル、URL フィルタリング、および WildFire® 送信ログなど。

コンプライアンス、冗長性、分析の実行、一元的な監視、脅威の挙動のレビュー、長期的なパターンなど、ログを *Panorama* あるいは外部ストレージに転送する理由には様々なものがあります。さらに、ファイアウォールのログの保存容量には限りがあり、保存領域が一杯になったら古いログを削除します。脅威ログおよび *WildFire* ログを必ず転送するようにしてください。

他のログ タイプを転送するには、「Device（デバイス）> Log Settings（ログ設定）」を参照してください。

PA-7000 シリーズのファイアウォールでログを転送したり、ファイルを *WildFire®* に転送するには、まず *PA-7000* シリーズのファイアウォールでLog Card Interface（ログカードインターフェイス）を設定する必要があります。このインターフェイスを設定すると、ファイアウォールは自動的にこのポートを使用します。特別な設定は不要です。*PA-7000* シリーズ ネットワーク処理カード（*NPC*）のいずれかにデータポートをログ カード インターフェイス タイプとして設定し、使用するネットワークがログ サーバと通信できることを確認してください。*WildFire* 転送の場合、ネットワークは *WildFire* クラウドまたは *WildFire* アプライアンス（あるいはその両方）と正常に通信する必要があります。

以下の表で、ログ転送プロファイルの設定について説明します。

ログ転送プロファイルの設定	の意味
氏名	プロファイルを識別する名前を入力します（最大 64 文字）。この名前は、セキュリティ ポリシー ルールを定義するときにログ転送プロファイルのリストに表示されます。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
共有（Panorama のみ）	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • マルチ **vsys** ファイアウォール上のすべての仮想システム**(vsys)**–このオプションを無効（クリア）にすると、プロファイルは **Objects**（オブジェクト）タブで選択した**Virtual System**（仮想システム）のみで利用可能になります。 • **Panorama** 上のすべてのデバイス グループ–このオプションを無効（クリア）にすると、プロファイルは **Objects**（オブジェクト）タブで選択した**Device Group**（デバイスグループ）のみで利用可能になります。
Logging Serviceへの強化されたアプリケーション	Palo Alto Networks クラウドサービス用の強化されたアプリケーション ログは、ロギング サービス サブスクリプションで利用できます。強化されたア

© 2019 Palo Alto Networks, Inc.

ログ転送プロファイルの設定	の意味
ロギングを有効化 (トラフィックおよび URL ログを含む)	プリケーション ロギングにより、Palo Alto Networks クラウドサービス環境で実行されるアプリのネットワーク アクティビティに対する可視性を向上させることを目的としたデータをファイアウォールが収集できるようになります。
オーバーライドの無効化 (Panoramaのみ)	このログ転送プロファイルの設定が、このプロファイルを継承したデバイス グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでこのオプションは無効 (クリア) になっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
の意味	このログ転送プロファイルの目的を説明します。
一致リスト (ラベルなし)	1 つ以上 (最大 64 個) の一致リスト プロファイルを **Add** (追加) し、転送先のほか、ファイアウォールでどのログを送信するかを制御するログ属性ベースのフィルタ、ログに対して実行するアクション (自動タグ付けなど) を指定します。一致リスト プロファイルごとに次の 2 つのフィールド (名前と説明) を入力します。
名前 (一致リスト プロファイル)	一致リスト プロファイルを識別する名前を入力します (最大 31 文字)。
説明 (一致リスト プロファイル)	この一致リスト プロファイルの目的を説明します (最大 1,023 文字)。
ログ タイプ	この一致リストのプロファイルが適用されるログの種類を選択します。認証 (**auth**)、**data** (データ)、**gtp**、**sctp**、**threat** (脅威)、**traffic** (トラフィック)、**tunnel** (トンネル)、**URL**、または **WildFire**。
フィルタ	デフォルトでは、ファイアウォールは、選択された **Log Type** (ログ タイプ) の **All Logs** (すべてのログ) を転送します。ログの一部を転送するには、ドロップダウン リストから既存のフィルタを選択するか、**Filter Builder** (フィルタ ビルダー) を選択して新しいフィルタを追加します。新しいフィルタの各クエリに対して、以下のフィールドを指定して、クエリを **Add** (追加) します。 • **Connector** (条件式) – クエリの結合ロジック (AND/OR) を選択します。ロジックに否定を適用する場合は、**Negate** (否定) を選択します。たとえば、信頼されていないゾーンからのログ転送を防ぐには、**Negate** (上記以外) を選択し、Attribute (属性) として **Zone** (ゾーン)、Operator (演算子) として **equal** (等しい) を選択して、Value (値) 列に信頼されていないゾーンの名前を入力します。 • **Attribute** (属性) – ログの属性を選択します。使用可能な属性は、**Log Type** (ログ タイプ) によって異なります。 • **Operator** (演算子) – 属性を適用するかどうかを決定する基準を選択します (**equal** (等しい) など)。使用可能な基準は、**Log Type** (ログ タイプ) によって異なります。 • **Value**[値] – 照合する属性値を指定します。 フィルタが一致するログを表示またはエクスポートするには、[フィルタリングされたログの表示]を選択します。これにより、**Monitor**タブと同様のオプ

© 2019 Palo Alto Networks, Inc.

ログ転送プロファイルの設定	の意味
	ションが用意されます (**Monitor** (モニタ) > **Logs** (ログ) > **Traffic** (トラフィック)など)。
Panorama Panorama/ロギング サービス	ログ コレクタまたは Panorama 管理サーバーにログを転送する場合、あるいはログをロギング サービスに転送する場合は、**Panorama** を選択します。 このオプションを有効にする場合、configure log forwarding to Panorama (Panorama へのログ転送を設定) する必要があります。 また、ロギング サービスを使用するには、Device (デバイス) > Setup (セットアップ) > Management (管理) でロギング サービスを **Enable** (有効) にする必要があります。
SNMP	ログを SNMP トラップとして転送するには、1 つ以上の SNMP トラップ サーバー プロファイルを **Add** (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > SNMP Trap (SNMP トラップ)」を参照)。
電子メール	ログを電子メール通知として転送するには、1 つ以上の電子メール サーバー プロファイルを **Add** (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > Email (電子メール)」を参照)。
Syslog	ログを Syslog メッセージとして転送するには、1 つ以上の Syslog サーバー プロファイルを **Add** (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > Syslog」を参照)。
HTTP	ログを HTTP 要求として転送するには、1 つ以上の HTTP サーバー プロファイルを **Add** (追加) します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > HTTP」を参照)。
ビルトイン アクション	実行するアクションを **Add** (追加) します。タグ付けと統合という 2 つのタイプを選択できます。 • タグを付ける—ログ エントリ内の送信元または宛先 IP アドレスに対してタグを自動的に追加または削除して、ファイアウォールまたは Panorama の User-ID エージェントあるいはリモートの User-ID エージェントに IP アドレスとタグのマッピングを登録します。これにより、イベントに応答し、セキュリティ ポリシーを動的に適用できます。IP アドレスにタグを付けることができ、ダイナミックアドレス グループを使用してポリシーを動的に適用できることで、可視性が向上し、適切なコンテクストが与えられ、詳細な制御が可能になり、IP アドレスがネットワーク上のどの場所に移動してもセキュリティ ポリシーを一貫して適用できます。 以下の設定を指定します。 • アクションを **Add** (追加) し、そのアクションを説明する名前を入力します。 • タグ付けの対象の IP アドレスを選択します (**Source Address** (送信元アドレス) または **Destination Address** (宛先アドレス))。 ログ エントリに送信元 IP アドレスまたは宛先 IP アドレスを含むすべてのログ タイプに対してアクションを実行できます。相関ログおよび HIP マッチ ログでは、送信元 IP アドレスにのみタグを付けることができます。システム ログおよび設定ログでは、アクションを設定することはできませ

© 2019 Palo Alto Networks, Inc.

ログ転送プロファイルの設定	の意味
	ん。これらのログ タイプのログ エントリに IP アドレスが含まれないためです。 • アクション（**Add Tag**（タグの追加）または **Remove Tag**（タグの除去））を選択します。 • IP アドレスとタグのマッピングを、このファイアウォールまたは Panorama の **Local User-ID**（ローカル **User-ID**）エージェントに登録するか、**Remote User-ID**（リモート **User-ID**）エージェントに登録するかを選択します。 • IP アドレスとタグのマッピングを **Remote User-ID**（リモート **User-ID**）エージェントに登録するには、転送を有効にする HTTP サーバー プロファイルを選択します（Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP）。 • IP 対タグの **Timeout** (タイムアウト)を指定すれば、IP アドレス対タグのマッピングを保持する期間（分）を設定できます。タイムアウトを 0 にすると、IP 対タグのマッピングがタイムアウトしなくなります（範囲は 0 ~ 43200（30 日）、デフォルトは 0）。 タイムアウトを設定できるのは*Add Tag* (タグの追加)アクションだけです。 • ターゲットの送信元または宛先 IP アドレスに対して適用または削除する **Tags**（タグ）を入力または指定します。 • 統合—Azure の VM-Series ファイアウォールでのみ使用可能です。このオプションを使用すると、選択したログを**Azure-Security-Center-Integration** アクションを使用して Azure セキュリティ センターに転送できます。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Authentication（認証）

認証実施オブジェクトでは、ネットワーク リソースにアクセスするエンド ユーザーを認証するために使用する方式とサービスを指定します。オブジェクトを認証ポリシー ルールに割り当てると、認証ポリシー ルールは、トラフィックがルールに一致したときに、該当の認証方式とサービスを呼び出します（Policies（ポリシー）> Authentication（認証）を参照）。

ファイアウォールには、あらかじめ定義された読み取り専用の以下の認証実施オブジェクトがあります。

- **default-browser-challenge**（デフォルト ブラウザ チャレンジ）– ファイアウォールはユーザー認証情報を透過的に取得します。このアクションを選択した場合、キャプティブ ポータルの設定時に Kerberos シングル サインオン（SSO）または NT LAN Manager（NTLM）認証を有効にする必要があります。Kerberos SSO 認証に失敗すると、ファイアウォールは NTLM 認証に戻ります。NTLM を設定していない場合、または NTLM 認証に失敗した場合、ファイアウォールは、事前定義済みの **default-web-form**（デフォルト **Web** フォーム）で指定された認証方式にフォールバックします。
- **default-web-form**（デフォルト **Web** フォーム）– ユーザーを認証するために、ファイアウォールは、キャプティブ ポータルの設定時に指定された証明書プロファイルまたは認証プロファイルを使用します。認証プロファイルを指定した場合、ファイアウォールはプロファイル内のすべての Kerberos SSO 設定を無視し、認証情報を入力するためのキャプティブ ポータル ページをユーザーに表示します。
- **default-no-captive-portal**（デフォルト キャプティブ ポータルなし）– ファイアウォールはユーザーを認証せずにセキュリティ ポリシーを確認します。

カスタムの認証実施オブジェクトを作成する前に以下の操作を行ってください。

- 認証サービスへの接続方法を指定するサーバー プロファイルを設定します（[Device] > [サーバー プロファイル]を参照）。
- Kerberos シングル サインオン パラメータなどの認証設定を指定する認証プロファイルにサーバー プロファイルを割り当てます（Device > Authentication Profile [デバイス > 認証プロファイル]を参照）。

カスタムの認証実施オブジェクトを作成するには、**Add**（追加）をクリックして、以下のフィールドを入力します。

認証強度設定	の意味
氏名	分かりやすい名前（最大 31 文字）を入力し、認証ルールを作成するときにオブジェクトを容易に特定できるようにします。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有（Panorama のみ）	以下に対してオブジェクトを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**（オブジェクト）タブで選択した **Virtual System**（仮想システム）のみに対してオブジェクトが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**（オブジェクト）タブで選択した **Device Group**（デバイス グループ）のみに対してオブジェクトが公開されます。
オーバーライドの無効化（Panoramaのみ）	この認証強度オブジェクトの設定が、このオブジェクトを継承したデバイスグループで管理者によりオーバーライドされることを防止するには、このオプショ

© 2019 Palo Alto Networks, Inc.

認証強度設定	の意味
	ンを選択しますデフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
認証方式	方式を選択します。 • **browser-challenge**（ブラウザ チャレンジ）– ファイアウォールはユーザー認証情報を透過的に取得します。このアクションを選択した場合、選択した **Authentication Profile**（認証プロファイル）で Kerberos SSO を有効にしている必要があります。有効にしていない場合は、キャプティブ ポータルの設定で NTLM を設定している必要があります。Kerberos SSO 認証に失敗すると、ファイアウォールは NTLM 認証に戻ります。NTLM を設定していない場合、または NTLM 認証に失敗した場合、ファイアウォールは **web-form**（**Web** フォーム）認証にフォールバックします。 • **web-form**（**Web** フォーム）– ユーザーを認証するために、ファイアウォールは、キャプティブ ポータルの設定時に指定された証明書プロファイル、または認証実施オブジェクトで選択された **Authentication Profile**（認証プロファイル）を使用します。**Authentication Profile**（認証プロファイル）を選択した場合、ファイアウォールはプロファイル内のすべての Kerberos SSO 設定を無視し、認証情報を入力するためのキャプティブ ポータル ページをユーザーに表示します。 • **no-captive-portal**（キャプティブ ポータルなし）– ファイアウォールはユーザーを認証せずにセキュリティ ポリシーを確認します。
認証プロファイル	ユーザーの身元を確認するために使用するサービスを指定した認証プロファイルを選択します。
メッセージ	ユーザーのトラフィックが認証ルールをトリガーするときに、ユーザーに表示される最初のチャレンジ認証でどのように応答するかの指示を入力します。このメッセージは、**Captive Portal Comfort Page**（キャプティブ ポータル確認ページ）に表示されます。メッセージを入力しない場合、デフォルトの **Captive Portal Comfort Page**（キャプティブ ポータル確認ページ）が表示されます（Device > Response Pages [デバイス > 応答ページ]を参照）。 ファイアウォールは、*Authentication Profile*（認証プロファイル）の *Authentication*（認証）タブ（Device > Authentication Profile [デバイス > 認証プロファイル]を参照）で定義された最初の認証チャレンジ（ファクター）に対してのみ *Captive Portal Comfort Page*（キャプティブ ポータル確認ページ）を表示します。多重認証（*MFA*）チャレンジをプロファイルの *Factors*（ファクター）タブで定義している場合、ファイアウォールは *MFA Login Page*（*MFA* ログイン ページ）を表示します。

© 2019 Palo Alto Networks, Inc.

Objects > Decryption Profile [オブジェクト > 復号化プロファイル]

復号化プロファイルを使用すると、復号化のために指定した SSL および SSH トラフィックの特定の側面、および明示的に復号化から除外したトラフィックをブロックして制御できます。作成した復号化プロファイルは復号化ポリシーに追加できます。この復号化ポリシーに一致するすべてのトラフィックがプロファイル設定を基準に処理されるようになります。

ファイアウォールにはデフォルトの復号化プロファイルが設定されており、新規の復号化ポリシーに自動的に含められます (デフォルトの復号化プロファイルを変更することはできません)。**Add**[追加] をクリックして新規の復号化プロファイルを作成するか、既存のプロファイルを選択し、それを **Clone**[コピー] または変更してください。

確認すべき情報	以下を参照
新しい復号化プロファイルを追加する。 復号化されたトラフィックのポート ミラーリングを有効にする。	復号化プロファイルの一般設定
復号化された SSL トラフィックのブロックと制御を行う。	復号化された SSL トラフィックを制御するための設定
復号化から除外したトラフィック (医療サービスまたは金融サービスとして分類されたトラフィックなど) のブロックと制御を行う。	復号化されていないトラフィックを制御するための設定
復号化された SSL トラフィックのブロックと制御を行う。	復号化された SSH トラフィックを制御するための設定

復号化プロファイルの一般設定

次の表では、復号化プロファイルの一般設定について説明します。

復号化プロファイル — 一般設定	の意味
氏名	プロファイル名 (最大 **31** 文字) を入力します。この名前は、復号化ポリシーを定義するときに復号化プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有 (Panorama のみ)	以下に対してプロファイルを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。

© 2019 Palo Alto Networks, Inc.

復号化プロファイル — 一般設定	の意味
	• Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。
オーバーライドの無効化（Panoramaのみ）	管理者が、このプロファイルを継承するデバイス グループのこの復号化プロファイルの設定をオーバーライドすることを防ぐには、このオプションを選択します。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。
復号化ミラー インターフェイス （AWS の VM-Series ファイアウォール、Azure、NSX エディション、Citrix SDX を除くすべてのモデルをサポートします。）	復号化ポート ミラーリングに使用する **Interface**[インターフェイス] を選択します。 復号化ポート ミラーリングを有効にするには、復号化ポート ミラーライセンスを取得およびインストールして、ファイアウォールを再起動する必要があります。
転送のみ （AWS の VM-Series ファイアウォール、Azure、NSX エディション、Citrix SDX を除くすべてのモデルをサポートします。）	セキュリティポリシーの適用後のみ、復号化されたトラフィックをミラーリングする必要がある場合は、**Forwarded Only**[転送のみ] を選択します。このオプションを指定すると、ファイアウォール内を転送されたトラフィックのみがミラーリングされます。このオプションは、復号化されたトラフィックを他の脅威検出デバイス（DLP デバイスや他の侵入防止システム（IPS）など）に転送する場合に役立ちます。この項目の選択を解除すると（デフォルトではオフ）、ファイアウォールは、インターフェイスへのすべての復号化されたトラフィックをセキュリティポリシー検索の前にミラーリングします。これにより、イベントの再生を行い、脅威を生成するトラフィックやドロップアクションをトリガーするトラフィックを分析することができます。

復号化された SSL トラフィックを制御するための設定

以下の表で、SSL フォワード プロキシまたは SSL インバウンド インスペクションを使用して復号化された SSL トラフィックを制御するための設定について説明します。これらの設定を使用して、外部サーバー証明書の状態、サポートされていない暗号スイートやプロトコル バージョンの使用、復号化を処理するためのシステム リソースの可用性といった基準に基づいて SSL セッションを制限またはブロックできます。

SSL Decryption（SSL 復号化）タブの設定	の意味
SSL FORWARD PROXY (SSL フォワード プロキシ**)** タブ SSL フォワード プロキシを使用して復号化された SSL トラフィックを制限またはブロックするための各種オプションを選択します。	
Server Certificate Validation（サーバー証明書検証） — 復号化された SSL トラフィックのサーバー証明書を制御するオプションを選択できます。	

© 2019 Palo Alto Networks, Inc.

SSL Decryption（SSL 復号化）タブの設定	の意味
期限切れ証明書のセッションをブロック	サーバー証明書の期限が切れている場合、SSL 接続を終了します。これにより、ユーザーは期限切れの証明書を受け入れて SSL セッションを続行することができなくなります。 証明書が失効したセッションをブロックし、安全でないおそれのあるサイトにアクセスできなくします。
発行者が信頼されていないセッションをブロック	サーバー証明書の発行者が信頼されていない場合、SSL 接続を終了します。 発行者を信頼できない場合は中間者攻撃、リプレイ攻撃、その他の攻撃が示唆されるため、発行者を信頼できないセッションをブロックします。
証明書の状態が不明なセッションをブロックします	サーバーが証明書失効状態として「不明」を返す場合に、SSL セッションを終了します。証明書失効状態は、証明書の信頼性が失効しているかどうかを示します。 証明書ステータスが不明であるセッションをブロックし、セキュリティを強化します。しかし、様々な理由で証明書ステータスが不明になることがあるため、これによってセキュリティが厳格になりすぎる可能性があります。未知の証明書ステータスをブロックすることでビジネスに必要なサイトが影響を受ける場合は、証明書ステータスが不明であるセッションをブロックしないでください。
証明書の状態のチェックがタイムアウトしたセッションをブロックします	ファイアウォールが証明書の状態サービスからの応答を待機するよう設定された時間内に証明書の状態を取得できない場合、SSL セッションを終了します。**Certificate Status Timeout**（証明書の有効期限）の値は、証明書プロファイルを作成または変更する際に設定できます（**Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificate Profile**（証明書プロファイル））。 ステータスチェックがタイムアウトする際にセッションをブロックすることは、強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフになります。証明書無効化サーバーの応答が遅い場合は、タイムアウト時のブロックによって有効な証明書を持つサイトがブロックされるおそれがあります。有効な証明書をタイムアウトさせることに不安を感じる場合は、証明書取り消しチェック（CRL）およびオンライン証明書ステータス プロトコル（OCSP）のタイムアウトの値を大きくすることができます。
証明書の延長を制限	動的なサーバー証明書で使用される証明書の拡張を、鍵の用途および拡張鍵の用途に制限します。 他の証明書の拡張が必要でないデプロイ環境で証明書の拡張を制限します。
Append certificate's CN value to SAN extension 証	ファイアウォールが SSL 転送プロキシの復号化の一部としてクライアントに提示する偽装証明書にサブジェクト代替名（SAN）拡張子を追加できるように

© 2019 Palo Alto Networks, Inc.

SSL Decryption（SSL 復号化）タブの設定	の意味
明書のコモンネーム (CN) 値を SAN 拡張項目に追加	します。サーバー証明書に共通名（CN）のみが含まれている場合、ファイアウォールはサーバー証明書 CN に基づいて偽装証明書に SAN 拡張子を追加します。 このオプションは、ブラウザで SAN を使用するためにサーバー証明書が必要で、CN に基づく証明書照合をサポートしない場合に便利です。 エンドユーザーは要求された Web リソースへのアクセスを継続でき、サーバー証明書に CN だけが含まれていてもファイアウォールはセッションの復号化を継続できます。 証明書の *CN* 値を *SAN* 拡張に追加し、リクエストされた *Web* リソースにアクセスしやすくします。
Unsupported Mode Checks（サポートされていないモードのチェック）– サポートされていない SSL アプリケーションを制御するオプションを選択します。	
サポートされていないバージョンのセッションをブロック	PAN-OS が「client hello」メッセージをサポートしていない場合にセッションを終了します。PAN-OS では、SSLv3、TLS1.0、TLS1.1、および TLS1.2 をサポートしています。 サポートされていないバージョンのセッションを常にブロックし、脆弱なプロトコルを使用するサイトにアクセスできなくします。*SSL Protocol Settings (SSL* プロトコル設定*)*タブで最低 *Protocol Version (*プロトコル バージョン*)* を *TLSv1.2* に設定し、脆弱なバージョンのプロトコルを使用するサイトをブロックします。ビジネス上の目的でアクセスする必要があるサイトが脆弱なプロトコルを使用している場合、その脆弱なプロトコルを許可する復号化プロファイルを別途作成し、脆弱なプロトコルを許可しなければならない対象のサイトだけに適用される復号化ポリシー ルールでそれを指定します。
暗号スイートがサポートされていないセッションをブロック	SSL ハンドシェークで暗号スイートが指定されていて、PAN-OS でサポートされていない場合、セッションを終了します。 サポートしない暗号スイートを使用するセッションをブロックします。*SSL Protocol Settings (SSL* プロトコル設定*)*タブで、許可する暗号スイート（暗号化アルゴリズム）を設定します。ユーザーが脆弱な暗号スイートを使用するサイトに接続するのを許可しないでください。
クライアント認証を使用するセッションをブロック	SSL フォワード プロキシ トラフィックのクライアント認証を使用するセッションを終了します。 重要なアプリケーションで必要にならない限り、クライアント認証を伴うセッションをブロックします。そのアプリケーションが必要な場合は、別の復号化プロファイルを作成し、クライアント認証が必要なトラフィックにのみそれを適用しなければなりません。

© 2019 Palo Alto Networks, Inc.

SSL Decryption（SSL 復号化）タブの設定	の意味
Failure Checks（エラー チェック）— 復号化の処理でシステム リソースを使用できない場合に実行するアクションを選択します。	
リソースを使用できない場合にセッションをブロック	復号化を処理するためのシステム リソースが使用できない場合、セッションを終了します。 リソースが利用できない場合にセッションをブロックするかどうかは、強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフになります。リソースが利用できない場合にセッションをブロックしない場合、リソースが影響を受ける際に復号化したいトラフィックをファイアウォールが復号化できなくなります。しかし、リソースが利用できない場合にセッションをブロックすると、普段はアクセスできるサイトが一時的にアクセスできなくなる可能性があるため、ユーザーエクスペリエンスが影響を受けるおそれがあります。
HSM を使用できない場合にセッションをブロック	証明書の署名にハードウェア セキュリティ モジュール (HSM) を使用できない場合は、セッションを終了します。 HSM を利用できない場合にセッションをブロックするかどうかは、HSM が利用できない場合に暗号化されたトラフィックを扱う方法や秘密鍵の取得元など、組織のコンプライアンス規則によって異なります。
クライアント拡張	
ストリップ ALPN	ファイアウォールはデフォルトで HTTP/2 トラフィックを処理・検査します。しかし、ファイアウォールが**Strip ALPN (ALPN** をストリップ**)**するように指定することで、HTTP/2 を無効化できます。このオプションを選択すると、ファイアウォールは ALPN（Application-Layer Protocol Negotiation）TLS 拡張に含まれるすべての値を削除します。 HTTP/2 接続を保護するために ALPN を使用するため、この TLS 拡張用に指定されている値がない場合、ファイアウォールは HTTP/2 トラフィックを HTTP/1.1 にダウングレードするか、それを未知の TCP トラフィックに分類化します。

サポートされていないモードおよび失敗モードについては、セッション情報が *12* 時間キャッシュされます。このため、同じホストとサーバー ペア間の以降のセッションは復号化されません。代わりにこれらのセッションをブロックする場合は、オプションを有効にしてください。

SSL INBOUND INSPECTION (SSL インバウンド インスペクション**)** タブ

SSL インバウンド インスペクションを使用して復号化された SSL トラフィックを制限またはブロックするための各種オプションを選択します。

Unsupported Mode Checks（サポートされていないモードのチェック）— サポートされていないモードが SSL トラフィックで検出された場合にセッションを制御するオプションを選択します。	
サポートされていないバージョンのセッションをブロック	PAN-OS が「client hello」メッセージをサポートしていない場合にセッションを終了します。PAN-OS では、SSLv3、TLS1.0、TLS1.1、および TLS1.2 をサポートしています。

© 2019 Palo Alto Networks, Inc.

SSL Decryption（SSL 復号化）タブの設定	の意味
	サポートされていないバージョンのセッションを常にブロックし、脆弱なプロトコルを使用するサイトにアクセスできなくします。*SSL Protocol Settings (SSL プロトコル設定)*タブで最低 *Protocol Version (プロトコル バージョン)* を *TLSv1.2* に設定し、脆弱なバージョンのプロトコルを使用するサイトをブロックします。ビジネス上の目的でアクセスする必要があるサイトが脆弱なプロトコルを使用している場合、その脆弱なプロトコルを許可する復号化プロファイルを別途作成し、脆弱なプロトコルを許可しなければならない対象のサイトだけに適用される復号化ポリシー ルールでそれを指定します。
暗号スイートがサポートされていないセッションをブロック	暗号スイートが PAN-OS でサポートされていない場合、セッションを終了します。 サポートしない暗号スイートを使用するセッションをブロックします。*SSL Protocol Settings (SSL プロトコル設定)*タブで、許可する暗号スイート（暗号化アルゴリズム）を設定します。ユーザーが脆弱な暗号スイートを使用するサイトに接続するのを許可しないでください。
Failure Checks（エラー チェック）– システム リソースを使用できない場合に実行するアクションを選択します。	
リソースを使用できない場合にセッションをブロック	復号化を処理するためのシステム リソースが使用できない場合、セッションを終了します。 リソースが利用できない場合にセッションをブロックするかどうかは、強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフになります。リソースが利用できない場合にセッションをブロックしない場合、リソースが影響を受ける際に復号化したいトラフィックをファイアウォールが復号化できなくなります。しかし、リソースが利用できない場合にセッションをブロックすると、普段はアクセスできるサイトが一時的にアクセスできなくなる可能性があるため、ユーザーエクスペリエンスが影響を受けるおそれがあります。
HSM を使用できない場合にセッションをブロック	セッション キーの復号化にハードウェア セキュリティ モジュール (HSM) を使用できない場合は、セッションを終了します。 HSM を利用できない場合にセッションをブロックするかどうかは、HSM が利用できない場合に暗号化されたトラフィックを扱う方法や秘密鍵の取得元など、組織のコンプライアンス規則によって異なります。
SSL PROTOCOL SETTINGS (SSL プロトコル設定) タブ SSL セッション トラフィックのプロトコル バージョンと暗号スイートを適用する以下の各設定を選択します。	
プロトコル バージョン	SSL セッションでの最小/最大プロトコル バージョンの使用を強制します。
最小バージョン	SSL 接続の確立に使用できる最小プロトコル バージョンを設定します。

© 2019 Palo Alto Networks, Inc.

SSL Decryption（SSL 復号化）タブの設定	の意味
	Min Version (最低バージョン) を *TLSv1.2* に設定して最大限のセキュリティを提供します。サイトが *TLSv1.2* をサポートしているかどうか確認し、本当に正当なビジネス上の目的がサイトにあるかどうか判断します。*TLSv1.2* をサポートしていないながらアクセスする必要があるサイトについては、サイトがサポートしている最も強固なプロトコル バージョンを指定した復号化プロファイルを別途作成し、脆弱なバージョンの使用を必要なサイトと必要な送信元（ゾーン、アドレス、ユーザー）のみに制限する復号化ポリシー ルールにそれを適用します。
最大バージョン	SSL 接続の確立に使用できる最大プロトコル バージョンを設定します。最大オプションを選択して、最大バージョンを指定しない場合もあります。その場合、選択した最小バージョンと等しいかそれ以降のバージョンがサポートされます。 *Max Version* (最大バージョン) を*Max* (最大)に設定し、プロトコルが改善されたらファイアウォールが自動的にそれをサポートできるようにします。
キー交換アルゴリズム	SSLセッションにおいて、選択したキー交換アルゴリズムの使用を強制します。 3 つのアルゴリズム（**RSA**、**DHE**、**ECDHE**）すべてがデフォルトで有効化されています。**DHE**（Diffie-Hellman）および**ECDHE**（楕円曲線 Diffie-Hellman）は、SSL 転送プロキシあるいはインバウンド インスペクション復号化用のPerfect Forward Secrecy（PFS）を可能にします。
暗号化アルゴリズム	SSL セッションでの選択した暗号化アルゴリズムの使用を適用します。 脆弱な*3DES*や*RC4*暗号化アルゴリズムはサポートしないでください。（*TLSv1.2* を最低プロトコル バージョンとして使用する際、ファイアウォールは自動的にこれら *2* つのアルゴリズムをブロックします）例外を設けて脆弱なプロトコル バージョンをサポートしなければならない場合は、復号化プロファイルの*3DES*および*RC4*のチェックを外します。*3DES*あるいは*RC4*暗号化アルゴリズムを使用するサイトにアクセスしなければならないビジネス上の目的がある場合は、復号化プロファイルを別途作成してそれを対象のサイト用の復号化ポリシー ルールにのみ適用します。
認証アルゴリズム	SSL セッションでの選択した認証アルゴリズムの使用を適用します。 古く脆弱な *MD5* アルゴリズムをグロックします（デフォルト設定ではブロックされます）。*SHA1* 認証を使用する必要なサイトがない場合は、*SHA1* をブロックします。*SHA1* を使用するサイトにアクセスしなければならないビジネス上の目的がある場合は、復号化プロファイルを別途作成してそれを対象のサイト用の復号化ポリシー ルールにのみ適用します。

© 2019 Palo Alto Networks, Inc.

復号化されていないトラフィックを制御するための設定

No Decryption（復号化なし）タブを使用すると、復号化なしアクション（**Policies**（ポリシー）> **Decryption**（復号化）> **Action**（アクション））が設定された復号化ポリシーに一致するトラフィックをブロックする設定を有効にできます。以下のオプションを使用すると、セッションのサーバー証明書を制御できます。ただし、ファイアウォールはセッション トラフィックを復号化および検査しません。

No Decryption（復号化なし）タブの設定	の意味
期限切れ証明書のセッションをブロック	サーバー証明書の期限が切れている場合、SSL 接続を終了します。これにより、ユーザーは期限切れの証明書を受け入れて SSL セッションを続行することができなくなります。 証明書が失効したセッションをブロックし、安全でないおそれのあるサイトにアクセスできなくします。
発行者が信頼されていないセッションをブロック	サーバー証明書の発行者が信頼されていない場合、SSL 接続を終了します。 発行者を信頼できない場合は中間者攻撃、リプレイ攻撃、その他の攻撃が示唆されるため、発行者を信頼できないセッションをブロックします。

復号化された SSH トラフィックを制御するための設定

以下の表に、復号化されたインバウンドおよびアウトバウンド SSH トラフィックを制御するための設定を説明します。これらの設定を使用すると、未サポートのアルゴリズムの使用、SSH エラーの検出、SSH プロキシ復号化を処理するためのリソースの可用性など、さまざまな基準に基づいて、SSH トンネル トラフィックを制限またはブロックできます。

SSH Proxy (SSH プロキシ) タブの設定	の意味
Unsupported Mode Checks（サポートされていないモードのチェック）– サポートされていないモードが SSH トラフィックで検出された場合にセッションを制御するこれらのオプションを使用します。サポートされている SSH バージョンは、SSH バージョン 2 です。	
サポートされていないバージョンのセッションをブロック	「client hello」メッセージが PAN-OS でサポートされていない場合、セッションを終了します。 サポートされていないバージョンのセッションを常にブロックし、脆弱なプロトコルを使用するサイトにアクセスできなくします。*SSL Protocol Settings (SSL プロトコル設定)*タブで最低 *Protocol Version (プロトコル バージョン)* を *TLSv1.2* に設定し、脆弱なバージョンのプロトコルを使用するサイトをブロックします。ビジネス上の目的でアクセスする必要があるサイトが脆弱なプロトコルを使用している場合、その脆弱なプロトコルを許可する復号化プロファイルを別途作成し、脆弱なプロトコルを許可しなければならない対

© 2019 Palo Alto Networks, Inc.

SSH Proxy (SSH プロキシ) タブの設定	の意味
	象のサイトだけに適用される復号化ポリシー ルールでそれを指定します。
アルゴリズムがサポートされていないセッションをブロック	クライアントまたはサーバーで指定されたアルゴリズムが PAN-OS でサポートされていない場合、セッションを終了します。 サポートされていないアルゴリズムを使用するセッションを常にブロックし、脆弱なアルゴリズムを使用するサイトにアクセスできなくします。
Failure Checks (エラー チェック) – SSH アプリケーション エラーが発生した場合、およびシステム リソースを使用できない場合に実行するアクションを選択します。	
SSH エラー時にセッションをブロック	SSH エラーが発生した場合、セッションを終了します。
リソースを使用できない場合にセッションをブロック	復号化を処理するためのシステム リソースが使用できない場合、セッションを終了します。 リソースが利用できない場合にセッションをブロックするかどうかは、強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフになります。リソースが利用できない場合にセッションをブロックしない場合、リソースが影響を受ける際に復号化したいトラフィックをファイアウォールが復号化できなくなります。しかし、リソースが利用できない場合にセッションをブロックすると、普段はアクセスできるサイトが一時的にアクセスできなくなる可能性があるため、ユーザーエクスペリエンスが影響を受けるおそれがあります。

© 2019 Palo Alto Networks, Inc.

Objects（オブジェクト）> Decryption（復号化）> Forwarding（転送プロファイル）

復号転送プロファイルを設定して、ファイアウォールを decryption broker（復号ブローカー）として機能させることができます。復号化ブローカーのファイアウォールは、すでに復号化され検査されているトラフィックをインラインの第三者セキュリティ アプライアンスのセットであるセキュリティ チェーンに転送し、追加の施行を行います。また、ファイアウォールを構成して、セキュリティ チェーンのセッション分散を提供し、セキュリティ チェーン デバイスがオーバーサブスクライブされないようにすることもできます。ファイアウォールがセキュリティ チェーンからトラフィックを受信すると、ファイアウォールはトラフィックを再暗号化し、適切な宛先に転送します。

復号化転送プロファイルを作成して復号化ブローカリングを有効にする前に、次のことを行う必要があります。

- SSL フォワード プロキシ復号化を有効にします。
- セキュリティチェーンへの復号化されたトラフィックの転送（select **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット）の選択、インターフェイスの編集、**Advanced**（詳細）> **Other Info**（その他の情報）の選択、および復号化転送を有効にする）のために、少なくとも 2 つのレイヤー 3 インターフェイスをファイアウォール専用にします。このタスクを繰り返して、第二インターフェイスを復号転送インターフェイスとして有効にします。

これらのタスクを完了したら、復号化転送プロファイルを作成して 2 つのインターフェイスをペアにして、ファイアウォールが復号化されたトラフィックを転送するセキュリティ チェーンの設定を定義します。

サポートされている復号ブローカーとセキュリティー チェーンの開発の詳細と、ファイアウォールを復号ブローカーとして機能させるための完全なワークフローについては、「Decryption Broker（復号ブローカー）」を参照してください。

復号化転送設定	の意味
氏名	プロファイルに分かりやすい名前を付けます。
の意味	プロファイル設定を説明します（オプション）
General [全般] タブ	
Security Chain Type セキュリティ チェーン タイプ	ファイアウォールが復号化されたトラフィックを転送するセキュリティ チェーンのタイプを選択します。 • **Routed (Layer 3)**（ルート化（レイヤー 3））:このタイプのセキュリティ チェーンのデバイスは、レイヤー 3 インターフェイスを使用してセキュリティ チェーン ネットワークに接続します。各インターフェイスには、割り当てられた IP アドレスとサブネット マスクが必要です。セキュリティ チェーン デバイスは、静的ルート（または動的ルーティング）で構成され、インバウンドおよびアウトバウンドのトラフィックをセキュリティ チェーン内の次のデバイスに送信し、ファイアウォールに戻します。 • **Transparent Bridge**（トランスペアレント・ ブリッジ）:トランスペアレント・ ブリッジのセキュリティ チェーン ネットワークでは、すべてのセキュリティ チェーン デバイスに、セキュリティ チェーン ネットワークに接続された 2 つのインターフェイスが設定されています。これら 2 つのデータ プレーン インターフェイスは、トランスペアレント・ ブリッジ モードに

© 2019 Palo Alto Networks, Inc.

復号化転送設定	の意味
	設定されています。 IP アドレス、サブネット マスク、デフォルト ゲートウェイ、またはローカル ルーティング テーブルが割り当てられていません。トランスペアレント・ ブリッジモードのセキュリティ チェーン デバイスは、1 つのインターフェイス上でトラフィックを受信し、次のインラインセキュリティ チェーン デバイスへの途中で他のインターフェイスを出る前に、トラフィックを分析して強制します。
フロー方向	ファイアウォールが、同じ方向（一方向）または反対方向（双方向）で、復号化されたインバウンド セッションとアウトバウンド セッションをセキュリティ チェーンを通じてどのように誘導するかを指定します。選択するフロー方向は、セキュリティ チェーンを構成するデバイスのタイプによって異なります。たとえば、セキュリティ チェーンがセッションの両側を検査できるステートレス デバイスで構成されている場合は、単一方向フローを選択します。
Primary Interface プライマリ インターフェイス	ファイアウォールがトラフィックをセキュリティ チェーンに転送するために使用するプライマリ インターフェイスとセカンダリ インターフェイスを選択します。一緒に、プライマリおよびセカンダリ インターフェイスは、一対の復号転送インターフェイスを形成します。復号転送インターフェイスとして設定したインターフェイスだけが表示されます。
Secondary Interface セカンダリ インターフェイス	
セキュリティ チェーン タブ	
Enable [有効化]	セキュリティ チェーンを有効にします。
氏名	セキュリティ チェーンに分かりやすい名前を付けます。
最初のデバイス	セキュリティ チェーン内の最初のデバイスと最後のデバイスの IPv4 アドレスを選択するか、デバイスを簡単に参照できるように新しいアドレス オブジェクトを定義します。
最後のデバイス	
Session Distribution Method セッション配信方式	複数のルーティング（レイヤー 3）セキュリティ チェーンに転送する場合、ファイアウォールがセキュリティ チェーン間で復号化されたセッションを配信するために使用する方法を選択します。 • **IP Modulo**（**IP** モジュロ）–ファイアウォールは、送信元および宛先 IP アドレスのモジュール ハッシュに基づいてセッションを割り当てます。 • **IP Hashu**（**IP** ハッシュ）–ファイアウォールは、送信元の IP ハッシュと宛先 IP アドレスとポート番号に基づいてセッションを割り当てます。 • **Round Robin**（ラウンドロビン）–ファイアウォールはセキュリティ チェーン間でセッションを均等に割り当てます。 • **Lowest Latency**（最低待機時間）–ファイアウォールは、最小の遅延でセキュリティ チェーンにさらに多くのセッションを割り当てます。この方法を想定通りに機能させるには、待機時間モニタリングと HTTP モニタリング（**Health Monitor**（ヘルス モニター））も有効にする必要があります。
ヘルス モニタ タブ	
ヘルスチェックに失敗した場合	この復号転送プロファイルに関連付けられているすべてのセキュリティチェーンがヘルスチェックに失敗した場合、ファイアウォールを **Bypass Security Chain**（バイパス セキュリティ チェーン）（セッショントラフィックを許可）または **Block Session**（ブロックセッション）に選択します。

© 2019 Palo Alto Networks, Inc.

復号化転送設定	の意味
	つまり、復号プロファイルが複数のセキュリティ チェーンで構成されており、単一のセキュリティ チェーンがヘルスチェックに失敗した場合、ファイアウォールは、**Security Chains**（セキュリティチェーン）タブで指定された方法に基づいて、 すべてのセキュリティ チェーンが失敗した場合にこの設定に基づいてトラフィックを許可します。
ヘルスチェック失敗条件	ヘルス監視の条件が満たされた場合、（**OR Condition**（OR条件））、またはすべての条件が満たされた場合（**AND Condition**（AND条件））、ヘルスチェック失敗をイベントとして定義します。
パス モニタリング 遅延モニタリング HTTP 監視	セキュリティ チェーンが復号されたトラフィックを効果的に処理していないことを識別するために、パス、レイテンシ、または HTTP 監視、あるいはこれらの 3つ の組み合わせを有効にします。有効にする監視の種類ごとに、ヘルスチェックの失敗をトリガする時間とカウントの期間を定義します。 有効化: • デバイスの接続を確認するためのパス監視。 • デバイスの処理速度と効率を確認するレイテンシ監視。 • デバイスの可用性と応答時間を確認する HTTP 監視。

© 2019 Palo Alto Networks, Inc.

Objects > SD-WAN Link Management [オブジェクト > SD-WAN リンク管理]

SD-WAN ポリシー ルールで使用する SD-WAN パス品質プロファイルとトラフィック分散プロファイルを作成します。

- Objects > SD-WAN Link Management > Path Quality Profile [オブジェクト > SD-WAN リンク管理 > パス品質プロファイル]
- Objects > SD-WAN Link Management > Traffic Distribution Profile [オブジェクト > SD-WAN リンク管理 > トラフィック分散プロファイル]

Objects > SD-WAN Link Management > Path Quality Profile [オブジェクト > SD-WAN リンク管理 > パス品質プロファイル]

SD-WAN を使用すると、一意のネットワーク品質要件を持つアプリケーション、アプリケーション フィルタ、アプリケーション グループ、サービス、サービス オブジェクト、およびサービス グループ オブジェクトの各セットのパス品質プロファイルを作成し、SD-WAN ポリシー ルールでそのプロファイルを参照できます。 プロファイルでは、レイテンシー、ジッター、パケットロスの 3 つのパラメータに最大しきい値を設定します。SD-WAN リンクがいずれかのしきい値を超えると、ファイアウォールは、このプロファイルを適用した SD-WAN ルールに一致するパケットに新しい最適パスを選択します。

各パス品質パラメータの感度設定により、プロファイルが適用されるアプリケーションにとってより重要な (推奨される) パラメータをファイアウォールに示すことができます。ファイアウォールは、設定が中または低のパラメータよりも、設定が高のパラメータを重視します。例えば、一部のアプリケーションはジッターやレイテンシーよりもパケット損失の影響を受けやすいため、それらのアプリケーションに関連付けられたプロファイルのパケット損失を高感度に設定すると、ファイアウォールは最初にパケット損失を検査します。

レイテンシー、ジッター、およびパケット損失の感度設定をデフォルト設定 (中) のままにするか、3 つのパラメータすべてを同じ設定にした場合、プロファイルの優先順位はパケット損失、レイテンシー、ジッターとなります。

デフォルトでは、ファイアウォールは200 ミリ秒毎に 最後3つの測定値の平均を取り、レイテンシーおよびジッターを測定し、スライディング ウィンドウ方式でパス品質を測定します。SD-WAN インターフェイス プロファイルを設定するときに、積極的または緩和的なパス モニタリングを選択することにより、この動作を変更できます。

	パス品質プロファイルの設定
名前	パス品質プロファイルの**Name** (名前) を任意の組み合わせで、最大 31 文字の英数字、アンダースコア、ハイフン、スペース、ピリオドを使用して入力します。
レイテンシー (ミリ秒)	**Threshold** (しきい値)–パケットがファイアウォールを出て SD-WAN トンネルの反対側の端に到着し、しきい値を超過する前にそのパケットがファイアウォールに戻るまでの許容ミリ秒数を入力します (範囲は 10 ～ 2,000、デフォルトは 100)。
	Sensitivity (感度)– 高、 中 (デフォルト)、または 低を選択します。

© 2019 Palo Alto Networks, Inc.

	パス品質プロファイルの設定
ジッター (ミリ秒)	**Threshold** (しきい値)—SD-WAN パケットのレイテンシーの平均変動値をミリ秒単位で入力します (範囲は 10 〜 1,000、デフォルトは 100)。デフォルトの 100 ミリ秒のジッターしきい値は、ジッターしきい値を超える前にレイテンシー測定値が平均 100 ミリ秒変動する可能性があることを意味します。
	Sensitivity (感度)— 高、 中 (デフォルト)、または 低を選択します。
Packet Loss (パケット損失率) (%)	**Threshold** (しきい値)—しきい値を超えるまでのリンクのパケット損失率を入力します (範囲は 1 〜 100.0、デフォルトは 1)。
	Sensitivity (感度)— 高、 中 (デフォルト)、または 低を選択します。

Objects (オブジェクト) > SD-WAN Link Management (SD-WANリンク管理) > Traffic Distribution (トラフィック分散)

このトラフィック分散プロファイルでは、セッションの分散と、パスの品質が低下したときにより適切なパスにフェイルオーバーするためにファイアウォールが使用する方法を選択します。ファイアウォールが SD-WAN トラフィックを転送するリンクを決定する際に考慮するリンク タグを追加します。作成した各 SD-WAN ポリシー ルールにトラフィック分散プロファイルを適用します。

	トラフィック分散プロファイル
名前	最大 31 の英数字、ハイフン、スペース、アンダースコア、ピリオドを組み合わせて、トラフィック分散プロファイルの **Name** (名前) を入力します。
Best Available Path (利用できる最適なパス)	コストを考慮せず、アプリケーションが拠点から外への任意のパスを使用できるようにするには **Best Available Path** (利用可能な最適なパス)を選択します。ファイアウォールはトラフィックを分散し、パス品質メトリックに基づいてリスト内のすべてのリンク タグに属するリンクの中からリンクにフェイルオーバーすることで、ユーザーに最高のアプリケーション エクスペリエンスを提供します。
Top Down Priority (トップダウン優先)	最後の手段としてのみ、またはバックアップ リンクとしてのみ使用したいコストの高いリンクや容量の少ないリンクがある場合は、**Top Down Priority** (トップダウン優先) 方式を選択し、それらのリンクを含むタグをこのプロファイルの **Link Tags** (リンク タグ) のリストの最後に配置します。ファイアウォールは最初にリストのトップ リンク タグを使用して、トラフィックをセッションにロードするリンクとフェイルオーバーするリンクを決定します。トップ リンク タグのどのリンクも適していない場合、ファイアウォールはリストの 2 番目のリンク タグからリンクを選択します。2 番目のリンク タグ内のどのリンクも適していない場合、ファイアウォールが適したリンクを見つけるまで、プロセスは必要に応じて続行されます。関連付けられているすべてのリンクが過負荷であり、品質しきい値を満たしているリンクがない場合、ファイアウォールは Best Available Path (利用できる最適なパス) の方法を使用して、トラフィックを転送するリンクを選択します。 アプリケーションのジッター、レイテンシ–、パケットロスが設定されたしきい値を超えると、ファイアウォールはリンク タグのトップダウン リストの先頭からフェイルオーバー先のリンクを探します。
Weighted Session Distribution (重み	ISP および WAN リンクに手動で (ルールに一致する) トラフィックをロードし、電圧低下時にフェイルオーバーを必要としない場合は **Weighted Session Distribution** (重み付

© 2019 Palo Alto Networks, Inc.

	トラフィック分散プロファイル
付きセッション分散)	きセッション分散) を選択します。1つのタグでグループ化されたインターフェイスが取得する新規セッションの静的な割合を適用するときに、リンクの負荷を手動で指定します。例えば、大きな拠点のバックアップや大きなファイルの転送など、レイテンシ–の影響を受けず、リンクの帯域幅容量を多く必要とするアプリケーションには、この方法を選択します。ただし、リンクで電圧低下が発生した場合、ファイアウォールは一致するトラフィックを別のリンクにリダイレクトしません。
Link Tags (リンクタグ)	このプロファイルのために選択したリンク選択プロセス中にファイアウォールに考慮させる リンク タグ を追加します。**Top Down Priority** (トップダウン優先) 方式を選択する場合、タグの順序が重要です。 **Move Up** (上に移動) または **Move Down** (下に移動) でタグの順序を変更できます。
重み	重み付きセッション分散方式を選択する場合は、追加した各リンク タグごとに割合を入力します。割合の合計は 100% でなければなりません。

© 2019 Palo Alto Networks, Inc.

Objects > Schedules [オブジェクト > スケジュール]

デフォルトでは、セキュリティポリシールールが常に有効化されています（毎日かつ常時）。セキュリティ ポリシー ルールを特定の時間に制限するには、スケジュールを定義して該当するポリシーに適用します。スケジュールごとに、固定の日時範囲、あるいは日次または週次の定期スケジュールを指定できます。スケジュールをセキュリティ ポリシーに適用するには、「Policies（ポリシー）> Security（セキュリティ）」を参照してください。

定義したスケジュールでセキュリティ ポリシー ルールが起動されると、適用されたセキュリティ ポリシー ルールは新しいセッションにのみ影響します。既存のセッションはスケジュールされたポリシーの影響を受けません。

スケジュール設定	の意味
氏名	スケジュール名を入力します（最大 31 文字）。この名前は、セキュリティ ポリシーを定義するときにスケジュールのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
共有（Panorama のみ）	以下に対してスケジュールを公開する場合は、このオプションを選択します。 • multi-vsys ファイアウォールの各仮想システム (vsys)。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Virtual System**[仮想システム] のみに対してスケジュールが公開されます。 • Panorama 上の各デバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] のみに対してスケジュールが公開されます。
オーバーライドの無効化（Panoramaのみ）	このスケジュールの設定が、このスケジュールを継承したデバイス　グループで管理者によりオーバーライドされることを防止するには、このオプションを選択します。デフォルトでは、この選択は解除されています。つまり、管理者は、スケジュールを継承するすべてのデバイス グループで設定をオーバーライドできます。
繰り返し	スケジュールのタイプを選択します（**Daily**（毎日）、**Weekly**（毎週）、または **Non-Recurring**（**1** 回限り））。
1 日 1 回	**Add**（追加）をクリックし、**Start Time**（開始時間）と**End Time**（終了時間）を 24 時間形式（HH:MM）で指定します。
週	**Add**（追加）をクリックし、**Day of Week**（曜日）を選択して、**Start Time**（開始時間）と **End Time**（終了時間）を 24 時間形式（HH:MM）で指定します。
1 回限り	**Add**（追加）をクリックし、**Start Date**（開始日）、**Start Time**（開始時間）、**End Date**（終了日）、および **End Time**（終了時間）を指定します。

ネットワーク

以下のトピックでは、ファイアウォールのネットワーク設定について説明します。

- Network > Virtual Wires [ネットワーク > バーチャル ワイヤー]
- [Network] > [インターフェイス]
- Network > Virtual Routers [ネットワーク > 仮想ルーター]
- Network > Zones [ネットワーク > ゾーン]
- Network > VLANs [ネットワーク > VLAN]
- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]
- Network (ネットワーク) > GRE Tunnels (GRE トンネル)
- Network > DHCP [ネットワーク > DHCP]
- Network > DNS Proxy [ネットワーク > DNS プロキシ]
- Network > QoS [ネットワーク > QoS]
- Network > LLDP [ネットワーク > LLDP]
- Network (ネットワーク) > Network Profiles (ネットワーク プロファイル)

[Network] > [インターフェイス]

ファイアウォール インターフェイス (ポート) により、ファイアウォールは、ファイアウォール内の他のインターフェイスや、他のネットワーク デバイスに接続することが可能です。以下のトピックでは、各種インターフェイス タイプとそれらの設定方法について説明します。

確認すべき情報	以下を参照
ファイアウォール インターフェイスとは何ですか？	ファイアウォール インターフェイスの概要
ファイアウォール インターフェイスの知識がありません。ファイアウォール インターフェイスの構成要素は何ですか？	ファイアウォール インターフェイスの共通の構成要素 PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素
ファイアウォール インターフェイスはすでに理解しています。特定のインターフェース タイプの設定情報はどうすれば確認できますか？	**物理インターフェイス (Ethernet)** タップ インターフェイス HA インターフェイス バーチャル ワイヤー インターフェイス バーチャル ワイヤー サブインターフェイス PA-7000 シリーズのレイヤー 2 インターフェイス PA-7000 シリーズのレイヤー 2 サブインターフェイス PA-7000 シリーズのレイヤー 3 インターフェイス レイヤー 3 インターフェイス レイヤー 3 サブインターフェイス Log Card Interface (ログ カード インターフェイス) ログ カード サブインターフェイス 復号化ミラー インターフェイス Ethernet の集約 (AE) インターフェイス グループ Ethernet の集約 (AE) インターフェイス **論理インターフェイス** Network > Interfaces > VLAN [ネットワーク > インターフェイス > VLAN] Network > Interfaces > Loopback [ネットワーク > インターフェイス > ループバック] Network > Interfaces > Tunnel [ネットワーク > インターフェイス > トンネル] Network > Interfaces > SD-WAN [ネットワーク > インターフェイス > SD-WLAN]
その他の情報をお探しですか？	ネットワーク

© 2019 Palo Alto Networks, Inc.

ファイアウォール インターフェイスの概要

ファイアウォール データ ポートのインターフェイス設定により、トラフィックがファイアウォールを出入りできるようになります。Palo Alto Networks® ファイアウォールは、複数のデプロイモードで同時に作動できます。これは、さまざまなデプロイモードをサポートするようにConfigure Interfaces（インターフェイスを設定する）ことができるからです。例えば、バーチャル ワイヤー、レイヤー 2、レイヤー 3、およびタップ モードに対応するようにファイアウォールの Ethernet インターフェイスを設定できます。ファイアウォールでサポートされるインターフェイスを以下に示します。

- **Physical Interfaces (**物理インターフェイス**)**–ファイアウォールは、トラフィックを異なる伝送速度で送受信する 2 種類のメディア (銅線と光ファイバー) をサポートします。イーサネットインターフェイスは、さまざまなタイプとして設定できます。具体的には、タップ、高可用性 (HA)、ログ カード (インターフェイスおよびサブインターフェイス)、復号化ミラー、バーチャル ワイヤー (インターフェイスおよびサブインターフェイス)、レイヤー 2 (インターフェイスおよびサブインターフェイス)、レイヤー 3 (インターフェイスおよびサブインターフェイス)、および Aggregate Ethernet として設定できます。使用可能なインターフェイス タイプおよび伝送速度は、ハードウェア モデルごとに異なります。
- **Logical Interfaces (**論理インターフェス**)**–これらには、仮想ローカル エリア ネットワーク (VLAN) インターフェイス、ループバック インターフェイス、トンネル インターフェイス、および SD-WAN インターフェイスが含まれます。VLAN、SD-WAN またはトンネル インターフェイスを定義する前に、物理インターフェイスをセットアップする必要があります。

ファイアウォール インターフェイスの共通の構成要素

多くのインターフェイスタイプに共通する構成要素を表示し、その設定を行う場合は**Network[**ネットワーク**]** > **Interfaces[** インターフェイス**]**を選択します。

PA-7000 シリーズのファイアウォール インターフェイスを設定する場合、または *Panorama*™ を使用して任意のファイアウォールのインターフェイスを設定する場合、それらに固有または個別の構成要素の説明に関しては Common Building Blocks for PA-7000 Series Firewall Interfaces（PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素）を参照してください。

ファイアウォール インターフェイスの構成要素	の意味
インターフェイス (インターフェイス名)	インターフェイス名は事前に定義されており、変更することはできません。ただし、サブインターフェイス、集約インターフェイス、VLANインターフェイス、ループバック インターフェイス、トンネル インターフェイス、SD-WAN インターフェイスには、数値のサフィックスを付加できます。
インターフェイスタイプ	イーサネット インターフェイス（**Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット））では、以下のインターフェイス タイプを選択できます。 • **Tap** • **HA** • **Decrypt Mirror**（復号化ミラー）(VM-Series NSX、Citrix SDX、AWS、Azure を除くすべてのファイアウォール上でサポート。) • バーチャルワイヤー • レイヤー**2** • レイヤ **3** • **Log Card (**ログカード**)**（PA-7000シリーズのファイアウォールのみ）

© 2019 Palo Alto Networks, Inc.

ファイアウォール インターフェイスの構成要素	の意味
	• **Aggregate Ethernet (AE)**
管理プロファイル	**Management Profile**（管理プロファイル）（**Network**（ネットワーク）> **Interfaces**（インターフェイス）> **<if-config** > **Advanced**（詳細）> **Other Info**（その他の情報））を選択し、このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択します。
リンク ステート	Ethernetインターフェイスの場合、リンク状態は、インターフェイスが現在アクセス可能で、かつネットワークを経由してトラフィックを受信できるかどうかを示します。 • 緑色 - 設定済み、かつ接続中です • 赤色 - 設定済みですが、接続が停止しているか無効です • 灰色 - 設定されていません リンク状態のアイコンの上にポインタを置くと、インターフェイスのリンク速度とデュプレックス設定を示すツール情報が表示されます。
IPアドレス	（任意）Ethernet、VLAN、ループバック、またはトンネルの IPv4 アドレスまたは IPv6 アドレスを設定します。IPv4アドレスの場合は、更にインターフェイスのアドレスモード**Type**[タイプ]を選択できます。**Static**[スタティック]、**DHCP Client**[DHCPクライアント]、または**PPPoE**を選択できます。
仮想ルーター(VR)	インターフェイスに仮想ルーターを割り当てるか、**Virtual Router**（仮想ルーター）をクリックして新しい仮想ルーターを定義します（「Network（ネットワーク）> Virtual Routers（仮想ルーター）」を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
タグ（サブインターフェイスのみ）	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入力します。
VLAN	**Network**（ネットワーク）> **Interfaces**（インターフェイス）> **VLAN** を開き、既存の **VLAN** を変更するか、新しく **Add**（追加）します（Network（ネットワーク）> VLANsを参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているVLANが解除されます。レイヤー 2 インターフェイス間の切り替えを有効にする、または VLAN インターフェイス経由のルーティングを有効にするには、VLAN オブジェクトを設定する必要があります。
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン	新規の定義を行うには、インターフェイスの**Security Zone**（セキュリティ ゾーン）（**Network**（ネットワーク）> **Interfaces**（インターフェイス）> **<if-config** > **Config**（設定））を選択するか、**Zone**（ゾーン）を選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
機能	イーサネットインターフェイスの場合、この列は、以下の機能が有効かどうかを示します。

© 2019 Palo Alto Networks, Inc.

ファイアウォール インターフェイスの構成要素	の意味
	DHCP クライアント DNSプロキシ GlobalProtect™ ゲートウェイ対応 リンク集約制御プロトコル (LACP) リンク レイヤー検出プロトコル (LLDP) NDP モニター Netflow プロファイル QoSプロファイル SD-WAN
コメント	インターフェイスの機能または目的の説明。

PA-7000 シリーズのファイアウォール インターフェイスの共通の構成要素

以下の表は、**Network**[ネットワーク] > **Interfaces**[インターフェイス] > **Ethernet** [イーサネット] ページの構成要素のうち、PA-7000 シリーズのファイアウォール インターフェイスを設定する場合、または Panorama を使用して任意のファイアウォール インターフェイスを設定する場合に固有のまたは個別の構成要素を示しています。インターフェイスを新しく作成する場合は **Add Interface**[インターフェイスの追加] ボタンをクリックし、既存のインターフェイスを編集する場合はその名前 ([Ethernet1/1] など) をクリックします。

PA-7000 シリーズのファイアウォールの場合は、*1* つのデータ ポートで Log Card Interface (ログ カード インターフェイス) を設定する必要があります。

PA-7000 シリーズのファイアウォール インターフェイスの構成要素	の意味
スロット	インターフェイスのスロット番号 (1 ~ 12) を選択します。スロットが複数あるのは、PA-7000 シリーズのファイアウォールのみです。Panorama を使用して他のファイアウォール モデルのインターフェイスを設定する場合は、**Slot 1** (スロット **1**) を選択します。
インターフェイス (インターフェイス名)	選択した**Slot**[スロット]に関連付けられているインターフェイスの名前を選択します。

タップ インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

© 2019 Palo Alto Networks, Inc.

タップ インターフェイスを使用して、ポートのトラフィックをモニターできます。

タップ インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

タップ インターフェイス設定	設定場所	の意味
インターフェイス名	イーサネット インターフェイス	インターフェイス名は事前に定義されており、変更することはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		**Tap**[タップ] を選択します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile**[Netflow プロファイル] をクリックして新しいプロファイルを定義します (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
仮想システム(vsys)	**Ethernet Interface** (イーサネット インターフェイス) > **Config** (設定)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システムを選択するか、**Virtual System**[仮想システム] リンクをクリックして新しいvsysを定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
リンク速度	**Ethernet Interface** (イーサネット インターフェイス) > **Advanced** (詳細)	インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto** を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプレックス		インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート		インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。

HA インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

HA (高可用性) インターフェイスにはそれぞれ固有の機能があります。一方のインターフェイスは設定の同期とハートビート機能を持ち、もう一方のインターフェイスは状態の同期機能を持っています。アク

© 2019 Palo Alto Networks, Inc.

ティブ/アクティブの高可用性が有効になっている場合、ファイアウォールは、3 つ目の HA インターフェイスを使用してパケットを転送できます。

一部の *Palo Alto Networks* ファイアウォールには、*HA* 専用の物理ポートがあります (制御リンク用とデータ リンク用)。専用ポートのないファイアウォールの場合、*HA* に使用するデータ ポートを指定する必要があります。*HA* の詳細は「*Device* (デバイス) > *Virtual Systems* (仮想システム) 」を参照してください。

HA インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

HA インターフェイス設定	の意味
インターフェイス名	インターフェイス名は事前に定義されており、変更することはできません。
コメント	インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ	**HA** を選択します。
リンク速度	インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto** を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプレックス	インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート	インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。

バーチャル ワイヤー インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

バーチャル ワイヤーは論理的に 2 つの Ethernet インターフェイスを結合し、すべてのトラフィック、または選択した VLAN タグを持つトラフィックのみをインターフェイス間で渡すことができます (スイッチングまたはルーティング サービスは使用できません)。また、バーチャル ワイヤー サブインターフェイスを作成し、IP アドレス、IP 範囲、またはサブネットに基づいてトラフィックを分類することもできます。バーチャル ワイヤーでは、隣接ネットワーク デバイスへの変更は必要ありません。バーチャル ワイヤーは、同じ媒体の 2 つの Ethernet インターフェイス (銅線または両方の光ファイバ) を結束するか、カッパーインターフェイスを光ファイバインターフェイスに結束することができます。

バーチャル ワイヤーを設定するには、結束する 2 つのインタフェース (**Network** (ネットワーク) > **Interfaces** (インターフェイス) > **Ethernet**) を決定し、次の表に示すように設定を構成します。

バーチャル ワイヤー用に既存のインターフェイスを使用する場合は、まずそのインターフェイスを、すべての関連付けられたセキュリティ ゾーンから削除します。

© 2019 Palo Alto Networks, Inc.

バーチャル ワイヤー インターフェイス設定	設定場所	の意味
インターフェイス名	イーサネットインターフェイス	インターフェイス名は事前に定義されており、変更することはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		[バーチャル ワイヤー] を選択します。
バーチャルワイヤー	**Ethernet Interface**（イーサネット インターフェイス）> **Config**（設定）	バーチャルワイヤーを選択するか、**Virtual Wire**（バーチャルワイヤー）をクリックして新しいバーチャル ワイヤーを定義します (Network（ネットワーク）> Virtual Wires（バーチャル ワイヤー）を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているバーチャルワイヤーが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システムを選択するか、**Virtual System**[仮想システム] リンクをクリックして新しいvsysを定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
リンク速度	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）	インターフェイスの速度 **auto**（自動）を選択してファイアウォールに自動的に速度を決定させます。バーチャル ワイヤーの両方のインターフェイスは同じ速度である必要があります。
リンクデュプレックス		インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。バーチャル ワイヤーの両方のインターフェイスは同じ転送モードである必要があります。
リンク ステート		インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。
LLDP の有効化	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**	選択すると、インターフェイスでリンク レイヤー検出プロトコル (LLDP) が有効になります。LLDP は、リンク レイヤーで機能し、隣接するデバイスとその機能を検出します。
プロファイル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、**LLDP Profile**（**LLDP** プロファイル）をクリックして新しいプロファイルを作成します（「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> LLDP Profile（LLDP プロファイル）」を参照）。ファイアウォールでグローバルなデフォルト設定を使用するように設定する場合は**None**[なし] を選択します。

© 2019 Palo Alto Networks, Inc.

バーチャル ワイヤー インターフェイス設定	設定場所	の意味
HAパッシブステートを有効にする		LLDP が有効化されている場合、これを選択すると、HA のパッシブ ファイアウォールが LLDP についてそのピアと事前にネゴシエートした後にファイアウォールがアクティブになるように設定されます。 LLDP が有効化されていない場合、これを選択すると、LLDP パケットが HA のパッシブ ファイアウォールを単に通過するように設定されます。

バーチャル ワイヤー サブインターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

バーチャル ワイヤー (vwire) サブインターフェイスでは、VLAN タグまたは VLAN タグと IP 分類子の組み合わせによってトラフィックを分離し、タグの付いたトラフィックを異なるゾーンと仮想システムに割り当ててから、定義された条件に一致するトラフィックのセキュリティ ポリシーを適用できます。

バーチャル ワイヤー インターフェイス を追加するには、そのインターフェイスの行を選択し、**Add Subinterface** (サブインターフェイスの追加) をクリックして、以下の情報を指定します。

バーチャル ワイヤー サブインターフェイス設定	の意味
インターフェイス名	読み取り専用の **Interface Name**[インターフェイス名] フィールドには、選択したvwireインターフェイスの名前が表示されます。サブインターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント	サブインターフェイスの説明 (省略可) を入力します。
タグ	サブインターフェイス用のVLAN Tag[タグ] (0 ~ 4094) を入力します。
Netflowプロファイル	入力サブインターフェイスを通過する単向性のIPトラフィックをNetFlowサーバーにエクスポートする場合は、サーバープロファイルを選択するか、**Netflow Profile**[Netflow プロファイル] をクリックして新しいプロファイルを定義します (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを参照)。**None**[なし] を選択すると、サブインターフェイスから現在の NetFlow サーバー割り当てが削除されます。
IP による分類	**Add**[追加] をクリックし、IP アドレス、IP 範囲、またはサブネットを入力すると、この vwire サブインターフェイスのトラフィックを分類できます。
バーチャルワイヤー	バーチャルワイヤーを選択するか、**Virtual Wire**[バーチャルワイヤー] をクリックして新しいバーチャルワイヤーを定義します (Network > Virtual Wires [ネットワーク > バーチャル ワイヤー]を参照)。**None**[なし] を選択すると、現在サブインターフェイスに割り当てられているバーチャルワイヤーが解除されます。

© 2019 Palo Alto Networks, Inc.

バーチャル ワイヤー サブインターフェイス設定	の意味
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効な場合は、サブインターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン	サブインターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。現在サブインターフェイスに割り当てられているゾーンを解除する場合は**None**[なし] を選択します。

PA-7000 シリーズのレイヤー 2 インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

レイヤー 2インターフェイスを設定する場合は、**Network**[ネットワーク] > **Interfaces**インターフェイス > **Ethernet**イーサネット を開き、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

レイヤー 2 インターフェイス設定	設定場所	の意味
インターフェイス名	イーサネットインターフェイス	インターフェイス名は事前に定義されており、変更することはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		**Layer2**[レイヤー 3] を選択します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile** (**Netflow** プロファイル) をクリックして新しいプロファイルを定義します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow」を参照) 。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
VLAN	**Ethernet Interface** (イーサネット インターフェイス) > **Config** (設定)	レイヤー 2 インターフェイス間の切り替えを有効にする場合、または VLAN インターフェイス経由のルーティングを有効にする場合は、既存の VLAN を選択するか、**VLAN** をクリックして新しい VLAN を定義します (「Network (ネットワーク) > VLAN」を参照) 。**None**[なし] を選択すると、現在インターフェイスに割り当てられているVLANが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システムを選択するか、**Virtual System**[仮想システム] リンクをクリックして新しいvsysを定義します。

© 2019 Palo Alto Networks, Inc.

レイヤー 2 インターフェイス設定	設定場所	の意味
セキュリティゾーン		インターフェイス用の**Security Zone**[セキュリティゾーン]を選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
リンク速度	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）	インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto**[自動] を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプレックス		インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート		インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。
LLDP の有効化	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**	選択すると、インターフェイスでリンク レイヤー検出プロトコル (LLDP) が有効になります。LLDP は、リンク レイヤーで機能し、隣接するデバイスとその機能を検出します。
プロファイル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、**LLDP Profile**（**LLDP** プロファイル）をクリックして新しいプロファイルを作成します（「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> LLDP Profile（LLDP プロファイル）」を参照）。ファイアウォールでグローバルなデフォルト設定を使用するように設定する場合は**None**[なし] を選択します。
HAパッシブステートを有効にする		LLDP が有効化されている場合はこのオプションを選択することで、パッシブなファイアウォールがアクティブに切り替わる前に、もう一方のピアと LLDP の取り決めを行うようになります。

PA-7000 シリーズのレイヤー 2 サブインターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

物理レイヤー 2 インターフェイスとして設定された各 Ethernet ポートについては、ポートで受信するトラフィックに割り当てられる VLAN タグごとに追加の論理レイヤー 2 インターフェイス (サブインターフェイス) を定義できます。レイヤー 2 サブインターフェイス間の切り替えを有効にするには、それらのサブインターフェイスに同じ VLAN オブジェクトを割り当てます。

PA-7000 シリーズ レイヤー 2 インターフェイスを設定するには、その物理インターフェイスの行を選択した後、**Add Subinterface**（サブインターフェイスの追加）をクリックし、以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

レイヤー 2 サブインターフェイス設定	の意味
インターフェイス名	読み取り専用のインターフェイス名の欄には、選択した物理インターフェイスの名前が表示されます。サブインターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント	サブインターフェイスの説明 (省略可) を入力します。
タグ	サブインターフェイス用のVLANTag[タグ] (0 ~ 4094) を入力します。
Netflowプロファイル	入力サブインターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile** (**Netflow** プロファイル) をクリックして新しいプロファイルを定義します (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを参照)。現在サブインターフェイスに割り当てられているNetFlowサーバーを解除する場合は、**None**[なし] を選択します。
VLAN	レイヤー 2 インターフェイス間の切り替えを有効にする場合、または VLAN インターフェイス経由のルーティングを有効にする場合は、VLAN を選択するか、**VLAN** をクリックして新しい VLAN を定義します (「Network (ネットワーク) > VLAN」を参照)。現在サブインターフェイスに割り当てられているVLANを解除する場合は**None**[なし] を選択します。
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効な場合は、サブインターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン	サブインターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。現在サブインターフェイスに割り当てられているゾーンを解除する場合は**None**[なし] を選択します。

PA-7000 シリーズのレイヤー 3 インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

レイヤー 3 インターフェイスを設定するには、インターフェイス (例えば ethernet1/1) を選択して次の情報を指定します。

レイヤー3 インターフェイス設定	設定場所	の意味
インターフェイス名	イーサネットインターフェイス	インターフェイス名は事前に定義されており、変更することはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		[レイヤー 3] を選択します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファ

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		イルを選択するか、**Netflow Profile**（**Netflow** プロファイル）をクリックして新しいプロファイルを定義します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> NetFlow」を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
仮想ルーター(VR)	**Ethernet Interface**（イーサネット インターフェイス）> **Config**（設定）	仮想ルーターを選択するか、**Virtual Router**（仮想ルーター）をクリックして新しい仮想ルーターを定義します（Network（ネットワーク）> Virtual Routers（仮想ルーター）を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
リンク速度	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）	インターフェイス速度を**10**、**100**、**1000**Mbpsのいずれかから選択するか、**auto**[自動] を選択します。
リンクデュプレックス		インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート		インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。
管理プロファイル	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **Other Info**（その他の情報）	このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位（MTU）をバイト数で入力します（576 ~ 9,192、デフォルトは 1,500）。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが送信元にパケットが大きすぎることを示す *ICMP* フラグメント要求メッセージを返します。
TCP MSS の調整		ヘッダーのバイト数に対応できるようにインターフェイスの MTU バイト サイズ以内の値で最大セグメント サイズ（MSS）を調整する場合は選択します。MTUバイトサイズとMSS調整サイズはMSSバイトサイズと等しい値になり、これはIPによって異なります。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		• **IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ)** — 範囲は40～300、デフォルトは40です。 • **IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ)** — 範囲は60～300、デフォルトは60です。 ネットワークを通る**tunnel**[トンネル] のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。 カプセル化によりヘッダーが延長されるので、MSS調整サイズはMPLSヘッダーやVLANタグを持つトンネルトラフィックよりも大きく設定しておくことをお勧めします。
タグのないサブインターフェイス		このレイヤー 3 インターフェイスに属するすべてのサブインターフェイスにタグを付けないように指定します。PAN-OS® は、パケットの宛先に基づいて、タグのないサブインターフェイスを入力インターフェイスとして選択します。宛先がタグのないサブインターフェイスの IP アドレスの場合は、サブインターフェイスにマッピングされます。これは、反対方向のパケットで、送信元アドレスをタグのないサブインターフェイスの IP アドレスに変換する必要があることも示します。この分類メカニズムにより、すべてのマルチキャスト パケットとブロードキャスト パケットが、サブインターフェイスではなく基本インターフェイスに割り当てられます。OSPF (Open Shortest Path First) ではマルチキャストを使用するため、ファイアウォールはタグのないサブインターフェイスで OSPF をサポートしていません。
IPアドレス MAC アドレス	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **ARP Entries**（**ARP** エントリ）	1 つ以上のスタティック ARP（Address Resolution Protocol）エントリを追加するには、**Add**（追加）をクリックし、IP アドレスとそれに関連付けられたハードウェア（MAC）のアドレスを入力します。エントリを削除するには、エントリを選択して **Delete**[削除] をクリックします。静的 ARP エントリによって、指定したアドレスの ARP 処理が減り、中間者攻撃が防止されます。
IPv6 アドレス MAC アドレス	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **ND Entries**（**ND** エントリ）	NDP（Neighbor Discovery Protocol）のネイバー情報を指定するには、**Add**（追加）をクリックし、ネイバーの IP アドレスと MAC アドレスを入力します。
NDP プロキシの有効化	**Ethernet Interface**（イーサネット インター	選択すると、インターフェイスで NDP（Neighbor Discovery Protocol）プロキシが有効になります。ファイアウォールは、このリストの IPv6 アドレスの MAC アドレスを要求する ND パケットに応答します。ファイアウォールはND応答において、これらのア

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
	フェイス）> **Advanced**（詳細）> **NDP Proxy**（NDP プロキシ）	ドレスに宛てられたパケットに応答するプロキシとして機能することを伝えるために、そのインターフェイスのMACアドレスを送信します。 NPTv6 (Network Prefix Translation IPv6) を使用する場合は、**Enable NDP Proxy**[NDP プロキシの有効化] を選択することをお勧めします。 **Enable NDP Proxy**[NDPプロキシの有効化]が選択されている場合、検査文字列を入力し、フィルタの適用（ ）をクリックすることで、膨大なアドレスエントリの絞込を行うことができます。
アドレス		**Add**[追加] をクリックし、1 つ以上の IPv6 アドレス、IP 範囲、IPv6 サブネット、またはファイアウォールが NDP プロキシとして機能するアドレス オブジェクトを入力します。これらのアドレスの 1 つは、NPTv6 の送信元変換のアドレスと同じであることが理想的です。アドレスの順序は問題になりません。 アドレスがサブネットワークの場合、ファイアウォールは、サブネットのすべてのアドレスに対してND応答を送信します。したがって、ファイアウォールのIPv6ネイバーも追加し、**Negate**[除外] を選択し、これらのIPアドレスに応答しないようにファイアウォールに指示することをお勧めします。
Negate		あるアドレスに対して**Negate**[除外] チェック ボックスをオンにすると、NDPプロキシは、そのアドレスを拒否するようになります。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
LLDP の有効化	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**	選択すると、インターフェイスでリンク レイヤー検出プロトコル (LLDP) が有効になります。LLDP は、リンク レイヤーで機能し、隣接するデバイスとその機能を検出します。
LLDPプロファイル		LLDP が有効の場合は、インターフェイスに割り当てる LLDP プロファイルを選択するか、**LLDP Profile**（**LLDP** プロファイル）をクリックして新しいプロファイルを作成します（「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> LLDP Profile（LLDP プロファイル）」を参照）。ファイアウォールでグローバルなデフォルト設定を使用するように設定する場合は**None**[なし] を選択します。
HAパッシブステートを有効にする		LLDP が有効化されている場合はこのオプションを選択することで、パッシブなファイアウォールがアクティブに切り替わる前に、もう一方のピアと LLDP 取り決めを行うことを許可することができます。
タイプ	イーサネット インターフェイス > **IPv4**	IPv4 アドレス タイプをインターフェイスに割り当てる方法を選択します。 • **Static**[静的] — IP アドレスを手動で指定する必要があります。 • **PPPoE** — ファイアウォールがPPPoE（Point-to-Point Protocol over Ethernet）用のインターフェイスを使用します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		• **DHCP Client**[DHCP クライアント] – インターフェイスが DHCP (Dynamic Host Configuration Protocol) クライアントとして機能し、ダイナミックに割り当てられた IP アドレスを受信できます。 アクティブ/アクティブ高可用性 *(HA)* モードのファイアウォールは、*PPPoE* や *DHCP* クライアントをサポートしません。 選択した IP アドレス方式に応じて、タブに表示されるオプションは異なります。
設定	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**	**Settings (設定)**を選択して DDNS フィールドを設定できるようにします。
Enable [有効化]		インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。（DDNS の設定が終わっていない場合は有効化せずに保存し、部分的な設定を保持することができます）
更新間隔（日数）		FQDN にマッピングされた IP アドレスを更新するためにファイアウォールが DDNS サーバーに送信する更新間隔（日数）を入力します（範囲は1～30、デフォルトは 1）。 また、ファイアウォールは*DHCP* サーバーからインターフェイスの新しい *IP* アドレスを受診した際も *DDNS* を更新します。
証明書プロファイル		証明書プロファイルを作成して DDNS サービスを検証します。DDNS サービスは、認証局（CA）が署名した証明書をファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト名（例：host123.domain123.com、or host123）を入力します。DNS がドメイン名として許可している有効な文字を使った構文になっていることを確認する以外、ファイアウォールはホスト名の検証を行いません。
ベンダー		DDNS サービスをこのインターフェイスに提供する DDNS ベンダー（およびバージョン）を選択します。 • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** ファイアウォールが特定の日で失効すると示唆する *DDNS* サービスの古いバージョンを選択する場合、新しいバージョンに移動させます。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		ベンダー名に続く**Name** (名前)および**Value** (値)フィールドは、ベンダー固有のものです。読み取り専用フィールドは、ファイアウォールが DDNS サービスに接続するために使用するパラメーターを示しています。DDNS サービスプロバイダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用するタイムアウトなど、他のフィールドを設定します。
IPv4 タブ - IP		インターフェイスで設定した IPv4 アドレスを追加し、それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー（ベンダー）に登録されています。
IPv6 タブ - IPv6		インターフェイスで設定した IPv6 アドレスを追加し、それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー（ベンダー）に登録されています。
ランタイム情報の表示		DDNS 登録を表示します：DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス（アスタリスク（*）はプライマリ IP アドレスを示します）。トラブルシューティングを目的として、各 DDNS プロバイダーにはホスト名の更新状態を示す独自の返却コードおよび返却日が必要になります。
IPv4 アドレス **Type**[タイプ] = 静的		
ip	イーサネットインターフェイス > **IPv4**	**Add**[追加] をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワーク マスクを指定します。 • CIDR（Classless Inter-Domain Routing）表記法の *ip_address/mask* の形式（例: 192.168.2.0/24）でエントリを入力します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • **Adress**[アドレス] をクリックし、タイプが **IP netmask**[IP ネットマスク] のアドレスオブジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、ファイアウォールが使用する転送情報ベース (FIB) によって決まります。 IP アドレスを削除するには、アドレスを選択して **Delete**[[削除]] をクリックします。
IPv4 アドレス **Type**[タイプ] = **PPPoE**		
Enable [有効化]	イーサネットインターフェイス > **IPv4** > **PPPoE** > イーサネット	PPPoE 終端点用のインターフェイスを有効化する場合に選択します。
username		ポイントツーポイント接続用の Username (ユーザー名) を入力します。
パスワード/再入力パスワード		ユーザー名のパスワードを入力し、確認します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
PPPoE クライアントランタイム情報の表示		（任意）接続を確立するためにファイアウォールがインターネットサービスプロバイダ（ISP）とネゴシエートしたパラメータを表示するダイアログを開きます。表示される具体的な情報は、ISP ごとに異なります。
authentication	イーサネットインターフェイス > **IPv4** > **PPPoE** > **Advanced**	PPPoE通信用の認証プロトコルを選択します。**CHAP** (Challenge-Handshake Authentication Protocol)、**PAP** (Password Authentication Protocol)、またはデフォルトの **Auto**（ファイアウォールがプロトコルを決定）のいずれかから選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロトコルが解除されます。
スタティック アドレス		以下のいずれかの手順を実行して、インターネット サービス プロバイダが割り当てた IP アドレスを指定します (デフォルト値なし)。 • CIDR（Classless Inter-Domain Routing）表記法の *ip_address/mask* の形式（例: 192.168.2.0/24）でエントリを入力します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • **Adress**[アドレス] をクリックし、タイプが **IP netmask**[IP ネットマスク] のアドレスオブジェクトを作成します。 • **None**[なし] を選択すると、インターフェイスから現在のアドレス割り当てが削除されます。
Automatically create default route pointing to peer（ピアを指すデフォルトルートを自動的に作成）		接続時に自動的に PPPoE ピアを指し示すデフォルト ルートを自動的に作成する場合に選択します。
デフォルト ルート メトリック		（任意）ファイアウォールとインターネットサービス プロバイダ間のルートについて、デフォルトルートへの関連付けと、パス選択の際に使用するルートメトリック（優先度）を入力します（範囲は 1 ~ 65,535）。数値が小さいほど優先度が高くなります。
アクセス コンセントレータ		（任意）ファイアウォールが接続するインターネットサービスプロバイダ側のアクセスコンセントレータの名前を入力します（デフォルトなし）。
サービス		（任意）サービス文字列を入力します（デフォルトなし）。
Passive		パッシブ モードを使用する場合に選択します。パッシブ モードでは、PPPoE エンド ポイントはアクセス コンセントレータが最初のフレームを送信するまで待機します。
IPv4 アドレス **Type**[タイプ] = **DHCP**		

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
Enable [有効化]	イーサネット インターフェイス > **IPv4**	インターフェイスの DHCP クライアントを有効化する場合に選択します。
サーバー提供のデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成		DHCP サーバーによって提供されるデフォルト ゲートウェイを指し示すデフォルト ルートを自動的に作成する場合に選択します。
ホスト名の送信		ファイアウォール（DHCP クライアントとして）にインターフェイスのホスト名（Option 12）を DHCP サーバーに送信させる場合に選択します。Send Hostname (ホスト名の送信) を行う場合、デフォルトでファイアウォールのホスト名がホスト名フィールドで選択されます。その名前を送信するか、カスタム ホスト名（大文字および小文字、数字、ピリオド、ハイフン、アンダースコアを含む最長 64 文字）を入力します。
デフォルト ルート メトリック		ファイアウォールと DHCP サーバー間のルートについて、デフォルト ルートに関連付け、パス選択に使用するルートメトリック (優先度) を入力します（任意、範囲は1～65,535、デフォルトなし）。数値が小さいほど優先度が高くなります。
DHCP クライアント ランタイム情報の表示		DHCP のリース状態、ダイナミック IP アドレス割り当て、サブネット マスク、ゲートウェイ、サーバー設定（DNS、NTP、ドメイン、WINS、NIS、POP3、および SMTP）など、DHCP サーバーから受信したすべての設定を表示する場合に選択します。
インターフェースでの IPv6 の有効化	イーサネット インターフェイス > **IPv6**	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID as host portion**[ホスト部分にインターフェイス ID を使用] オプションを選択すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス		**Add**[追加] をクリックして、IPv6 アドレスごとに以下のパラメータを設定します。 • **Address**（アドレス）— IPv6 アドレスとプレフィックス長を入力します（例: 2001:400:f00::1/64）。既存のIPv6アドレスオブジェクトを選択することや、**Address**[アドレス] をクリックしてアドレスオブジェクトを作成することもできます。 • **Enable address on interface**（インターフェイス上のアドレスを有効にする）— インターフェイスの IPv6 アドレスを有効にする場合に選択します。 • **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用）— IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味

		• **Anycast**（エニーキャスト）– 最も近いノードを経由するルーティングを含める場合に選択します。
		• **Send Router Advertisement**（ルーター通知を送信）– このIP アドレスのルーター通知（RA）を有効にする場合に選択します。(インターフェイスのグローバルの **Enable Router Advertisement**[ルーター通知を有効化する] オプションも有効化しておく必要があります)。 RA の詳細は、「ルーター通知を有効にする」を参照してください。
		残りのフィールドは、RA を有効にした場合にのみ適用されます。
		  • **Valid Lifetime**（有効なライフタイム）– ファイアウォールがアドレスを有効とみなす時間（秒）です。有効なライフタイムは、**Preferred Lifetime**（優先ライフタイム）以上でなければなりません（デフォルトは 2,592,000）。
		  • **Preferred Lifetime**（優先ライフタイム）– 有効なアドレスが優先される時間（秒）です。この時間内は、ファイアウォールがこのアドレスを使用してトラフィックを送受信できます。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は **Valid Lifetime**（有効なライフタイム）の期限まで有効です（デフォルトは 604,800）。
		  • **On-link**（オンリンク）– プレフィックス内にアドレスがあるシステムにルーターなしで到達可能である場合に選択します。
		  • **Autonomous**（自律型）– 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。

重複アドレス検出を有効にする	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **Address Resolution**（アドレス解決）	重複アドレス検出（DAD）を有効にする場合に選択し、セクション内の他のフィールドの設定を行います。
DAD 試行回数		ネイバー要請間隔 (**NS Interval (NS 間隔)**) の内にDADを試行する回数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この回数を超えるとネイバーに障害があるとみなされます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到達可能な時間（秒）を指定します（範囲は 1 ~ 36,000、デフォルトは 30）。
NS 間隔 (ネイバー要請間隔)		DADの試行秒数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この秒数を超えると障害があるとみなされます。
NDP モニタリングの有効化		NDP（Neighbor Discovery Protocol）モニタリングを有効にする場合に選択します。有効になっていると、NDP モニター（Features (機能) 列の ）を選択し、ファイアウォールで検出されたネイバーに関する情報（IPv6 アドレス、対応する MAC アドレスおよび User-ID など）を（ベストケース ベースで）表示できます。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
ルーター通知を有効にする	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）	IPv6 インターフェイスでステートレス アドレス自動設定（SLAAC）を行う場合に選択してこのセクション内の他のフィールドを設定します。ルーター通知（RA）メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アドレスごとに RA オプションを設定する場合は、IP アドレス テーブルの **Add**（追加）をクリックしてアドレスを設定します。IP アドレスに RA オプションを設定する場合は、インターフェイスの **Enable Router Advertisement**[ルーター通知を有効にする] オプションを選択する必要があります。
最小間隔 (秒)		ファイアウォールが送信する RA 間の最小間隔（秒）を指定します（範囲は 3 ~ 1,350、デフォルトは 200）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
最大間隔 (秒)		ファイアウォールが送信する RA 間の最大間隔（秒）を指定します（範囲は 4 ~ 1,800、デフォルトは 600）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を指定します（範囲は 1 ~ 255、デフォルトは 64）。ホップ制限を指定しない場合は 0 を入力します。
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を指定します。リンクMTUを指定しない場合は **unspecified** (指定しない) を選択します（範囲は 1,280 ~ 9,192、デフォルトは unspecified）。
到達可能時間 (ミリ秒)		到達可能確認メッセージを受信後ネイバーに到達可能であると想定するためにクライアントが使用する到達可能時間 (ミリ秒) を指定します。到達可能時間を指定しない場合は **unspecified** (指定しない) を選択します（範囲は 0 ~ 3,600,000、デフォルトはunspecified）。
リトランスミッション時間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが待機する時間を決定するリトランスミッション タイマーを指定します。リトランスミッション時間を指定しない場合は **unspecified** (指定しない) を選択します（範囲は 0 ~ 4,294,967,295、デフォルトはunspecified）。
ルーターの有効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェイとして使用する時間を指定します（範囲は 0 ~ 9,000、デフォルトは 1,800）。0 は、ファイアウォールがデフォルト ゲートウェイでは

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		ないことを示します。有効期間が過ぎると、クライアントがそのデフォルト ルーター リストからファイアウォール エントリを削除して、別のルーターをデフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合は、クライアントがこのフィールドを使用して優先ルーターを選択します。セグメントの他のルーターとの比較において、RA が通知するファイアウォール ルーターの優先度を **High**、**Medium** (デフォルト)、**Low** の中から選択します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
整合性チェック	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）（続き）	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システム ログの不一致が記録されます。タイプは **ipv6nd** です。
その他の設定		他のアドレス情報（DNS 関連の設定など）を DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
ルーター通知に DNS 情報を含める	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **DNS Support**（**DNS** サポート）	ファイアウォールがこの IPv6 のイーサネット インターフェイスからの NDP ルーター通知（RA）メッセージで DNS 情報を送信できるようにする場合に選択します。この表の他の DNS Support（DNS サポート）フィールドは、このオプションを選択した場合にのみ表示されます。
SERVER		1 つ以上の再帰 DNS（RDNS）サーバー アドレスを **Add**（追加）し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信できるようにします。RDNS サーバーは、ルート DNS サーバーと権限のある DNS に一連の DNS ルックアップ要求を送信し、最終的に DNS クライアントに IP アドレスを提供します。 ファイアウォールがリストの上から下の順に NDP ルーター通知で受信者に送信する RDNS サーバーを最大 8 個設定できます。その後、受信者は同じ順序でこれらのアドレスを使用します。サーバーの順序を変更するには、サーバーを選択して **Move Up**（上へ）移動したり **Move Down**（下へ）移動したりします。サーバーが必要なくなったら、そのサーバーをリストから **Delete**（削除）します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後に、RDNS サーバーを使用してドメイン名を解決できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。
サフィックス		DNS 検索リスト（DNSSL）の 1 つ以上のドメイン名（サフィックス）を **Add**（追加）および設定します。最大長は255 バイトです。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	設定場所	の意味
		DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に（1 つずつ）追加するドメイン サフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されます。たとえば、DNS クライアントがサフィックスのない「quality」の DNS クエリを送信しようとすると、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスをその名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの DNS クエリの完全修飾ドメイン名は FQDN になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは DNS ルックアップが成功するか（残りのサフィックスは無視されます）、ルーターがリストのすべてのサフィックスを試行するまで DNS サフィックスを試行します。 ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスを使用してファイアウォールを設定します。DNSSL オプションを受信する DNS クライアントは、その非修飾 DNS クエリでサフィックスを使用します。 DNS 検索リストに対して最大 8 個のドメイン名（サフィックス）を設定し、ファイアウォールでそれらを NDP ルーター通知に含めて受信者に送信できます（上から下の順に送信します）。その後、受信者は同じ順序でこれらのアドレスを使用できます。順序を変更するには、サフィックスを選択して **Move Up**（上へ）移動したり **Move Down**（下へ）移動したりします。サフィックスが必要なくなったら、そのサフィックスを **Delete**（削除）します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後に、DNS 検索リストのドメイン名（サフィックス）を使用できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。

レイヤー 3 インターフェイス

- **Network** (ネットワーク) > **Interfaces** (インターフェイス) > **Ethernet** (イーサネット)

トラフィックをルーティングできるイーサネット レイヤー3 インターフェイスをコンフィグします。

レイヤー3 インターフェイス設定	の意味
インターフェイス名	読み取り専用の **Interface Name** (インターフェイス名) は、選択した物理インターフェイスの名前です。
コメント	インターフェイスのユーザーフレンドリーな説明を入力します。
インターフェイスタイプ	[レイヤー 3] を選択します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
Netflow プロファイル	入口インターフェイスを通過する単方向 IP トラフィックを NetFlow サーバーにエクスポートする場合は、既存の NetFlow プロファイルを選択するか、新しい **NetFlow Profile** (プロファイル) (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlowを参照) を作成します 。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
Config Tab (設定タブ)	
仮想ルーター(VR)	仮想ルーターをインターフェイスに割り当てるか、新しい **Virtual Router** (仮想ルーター - **VR**) を定義します (Network (ネットワーク) > Virtual Router (仮想ルーター - VR)を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効になっている場合は、インターフェイスに既存の仮想システム (vsys) を選択するか、新しい **Virtual System** (仮想システム)を定義します。
セキュリティゾーン	インターフェイスの既存のセキュリティ ゾーンを選択するか、新しい **Zone** (ゾーン)を定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
IPv4 Tab (タブ)	
SD-WAN を有効にする	**SD-WAN** を有効にする を選択して、イーサネット インターフェイスの SD-WAN 機能を有効にします。
IPv4 Type (タイプ) = **Static** (スタティック)	
ip	Add (追加) をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IPアドレスとネットワーク マスクを指定します。 • Classless Inter-Domain Routing (CIDR) 表示: *ip_address*/ マスク (192.168.2.0/24)を使用します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • タイプが **IP netmask** (**IP** ネットマスク) のアドレス オブジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、ファイアウォールが使用する転送情報ベース (FIB) によって決まります。 不要になった IP アドレスを **Delete** (削除) します。
Next Hop Gateway (ネクストホップ ゲートウェイ)	**SD-WAN** を有効にするを実行した場合は、Next Hop (ネクスト ホップ) ゲートウェイの IPv4 アドレスを入力します。
IPv4 Type (タイプ) = **PPPoE**、**General Tab** (全般タブ)	
Enable [有効化]	Point-to-Point Protocol Over Ethernet (PPPoE) の終端のインターフェイスをアクティベートするには、**Enable** (有効) を選択します。インターフェイスは、デジタル加入者

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	線 (DSL) モデムはあるが接続を終了する他の PPPoE デバイスがない DSL 環境での接続をサポートする PPPoE 終端ポイントです。
username	ISP がポイントツーポイント接続用に提供したユーザー名を入力します。
パスワードとパスワードの確認	パスワードを入力し、パスワードを確認します。
PPPoE クライアントランタイム情報の表示	PPPoE インターフェイスに関する情報を表示します。
IPv4 Type (タイプ) = PPPoE、Advanced Tab (詳細タブ)	
認証	認証方式を選択します。 • **None (なし)** (デフォルト)– この PPPoE インターフェイスには認証がありません。 • **CHAP**–ファイアウォールは、PPPoE インターフェイスで Challenge Handshake Authentication Protocol (ハンドシェーク認証プロトコルのチャレンジ) –RFC-1994–を使用します。 • **PAP**–ファイアウォールは、PPPoE インターフェイスで Password Authentication Protocol (パスワード認証プロトコル - PAP) を使用します。PAP はユーザー名とパスワードをプレーン テキストで送信するため、CHAP よりも安全性が低くなります。 • **auto (自動)** –ファイアウォールは、PPPoE サーバーと認証方法 (CHAP または PAP) を交渉します。
スタティック アドレス	PPPoE サーバーに希望の IPv4 アドレスを要求します。PPPoE サーバーはそのアドレスまたは別のアドレスを割り当てる場合があります。
ピアを指すデフォルト ルートを自動的に作成	PPPoE サーバーによって提供されるデフォルト ゲートウェイを指し示すデフォルト ルートを自動的に作成する場合はこのオプションを選択します。
デフォルト ルート メトリック	PPPoE 接続のデフォルト ルート メトリック (優先度レベル) を入力します (デフォルトは 10)。数値の低いルートほど、ルート選択時の優先順位が高くなります。例えば、ファイアウォールは、メトリック 10 のルートを使用してから、メトリック 100 のルートを使用します。
アクセス コンセントレータ	ISP からアクセス コンセントレータの名前が提供されている場合は、その名前を入力します。ファイアウォールは、IPS 側のこのアクセス コンセントレータに接続します。これは、0 ～ 255 文字の文字列値です。
サービス	ファイアウォール (PPPoE クライアント) は、PPPoE サーバーに要求されたサービス要求を提供できます。これは、0 ～ 255 文字の文字列値です。
Passive	ファイアウォール (PPPoE クライアント) は、PPPoE サーバーが接続を開始するのを待ちます。これが有効になっていない場合、ファイアウォールは接続を開始します。
IPv4 Tab (タブ)、Type (タイプ) = DHCP Client (クライアント)	

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
Enable [有効化]	インターフェイスがDynamic Address Group (ダイナミック ホスト コンフィグレーション プロトコル - DHCP) クライアントとして機能し、ダイナミックに割り当てられた IPアドレスを受信できるようにします。 高可用性 (*HA*) アクティブ/アクティブ構成のファイアウォールは、*DHCP* クライアントをサポートしません。
サーバー提供のデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成	デフォルト ゲートウェイへのスタティック ルートを作成するようにファイアウォールに指示します。デフォルト ゲートウェイは、クライアントがファイアウォールのルーティング テーブルでルートを維持する必要がない多くの宛先にアクセスしようとしている場合に便利です。
ホスト名の送信	DHCP クライアント インターフェイスにホスト名を割り当て、そのホスト名 (オプション 12) を DHCP サーバーに送信するには、このオプションを選択します。DHCP サーバーは、ホスト名を DNS サーバーに登録できます。その後、DNS サーバーがホスト名から動的 IP アドレスへの解決を自動的に管理できるようになります。外部ホストがホスト名に基づいてインターフェイスを識別できる必要があります。デフォルトの値は **system-hostname** であり、これは > **Device** (デバイス) > **Setup** (セットアップ) > **Management** (管理) > **General Settings** (一般設定) でユーザーが設定するファイアウォールのホスト名です。または、大文字と小文字、数字、ピリオド、ハイフン、下線を含む最大 64 文字でインターフェイスのホスト名を入力することができます。
デフォルト ルート メトリック	ファイアウォールと DHCP サーバー間のルートのデフォルト ルート メトリック (優先順位レベル) を入力します (範囲は 1 ~ 65535、デフォルト メトリックなし)。数値の低いルートほど、ルート選択時の優先順位が高くなります。例えば、ファイアウォールは、メトリック 10 のルートを使用してから、メトリック 100 のルートを使用します。
DHCP クライアント ランタイム情報の表示	DHCP リース ステータス、ダイナミックIP アドレスの割り当て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、SMTP) など、クライアントが DHCP サーバーから継承したすべての設定を表示します。
IPv6 Tab (タブ)	
インターフェースでの IPv6 の有効化	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID	64 ビット拡張一意識別子 (**EUI-64**) を 16 進数形式で入力します (00:26:08:FF:FE:DE:4E:29 など)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID as host portion** (ホスト部分にインターフェイス **ID** を使用) すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス	IPv6 アドレスとプレフィックス長を追加します (2001:400:f00::1/64 など)。または、既存の IPv6 アドレス オブジェクトを選択するか、新しい IPv6 アドレス オブジェクトを作成します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
インターフェイス上のアドレスを有効にする	インターフェイスで IPv6 アドレスを有効にします。
ホスト部分にインターフェイス ID を使用	IPv6 アドレスのホスト部分に **Interface** (インターフェイス) **ID** を使用する場合に選択します。
エニーキャスト	最も近いノードを経由するルーティングを含める場合に選択します。
ルーター通知を送信	この IP アドレスのルーター通知 (RA) を有効にする場合に選択します。(インターフェイスのグローバルの **Enable Router Advertisement**[ルーター通知を有効化する] オプションも有効化しておく必要があります)。 RA の詳細は、この表の「Enable Router Advertisement (ルーター通知を有効にする)」を参照してください。次のフィールドは **Enable Router Advertisement** (ルーター通知を有効にする)場合にのみ適用されます。 • **Valid Lifetime** (有効なライフタイム)–ファイアウォールがアドレスを有効とみなす時間 (秒) です。有効なライフタイムは、**Preferred Lifetime**[優先ライフタイム] 以上でなければなりません。デフォルトは2,592,000 です。 • **Preferred Lifetime** (優先ライフタイム)–有効なアドレスが優先される時間 (秒) です。この時間内は、ファイアウォールがこのアドレスを使用してトラフィックを送受信できます。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は **Valid Lifetime** (有効なライフタイム) の期限まで有効です。デフォルトは 604,800 です。 • **On-link** (オンリンク) – プレフィックス内にアドレスがあるシステムにルーターなしで到達可能である場合に選択します。 • **Autonomous** (自律型) – 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
IPv6 Tab (タブ)、**Address Resolution Tab** (アドレス解決タブ)	
Duplicate Address Detection (重複アドレス検出) を有効にする	重複アドレス検出 (DAD) を有効にする場合に選択し、DAD 試行、到達可能時間(秒)、および NS 間隔をコンフィグします。
DAD 試行回数	ネイバー要請間隔 (**NS Interval** (**NS** 間隔)) の内にDADを試行する回数を指定します (範囲は 1 ~ 10、デフォルトは 1)。この回数を超えるとネイバーに障害があるとみなされます。
Reachable Time (到達可能時間) (秒)	クエリと応答が正常に行われた後引き続きネイバーに到達可能な時間 (秒) を指定します (範囲は 1 ~ 36,000、デフォルトは 30)。
NS 間隔 (秒)	DADの試行秒数を指定します (範囲は 1 ~ 10、デフォルトは 1)。この秒数を超えると障害があるとみなされます。
NDP モニタリングの有効化	NDP (Neighbor Discovery Protocol) モニタリングを有効にする場合に選択します。有効にすると (Features (機能) 列の) **NDP** を選択でき、IPv6 アドレス、対応する

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	MAC アドレス、ユーザー ID などのファイアウォールが検出したネイバーに関する情報を (ベストケース ベースで) 表示できます。
IPv6 Tab (タブ)、Router Advertisement Tab (ルーター通知タブ)	
ルーター通知を有効にする	ネイバー検出を IPv6 インターフェイスで提供するには、このセクションのその他のフィールドを選択して設定します。ルーター通知 (RA) メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アドレスごとに RA オプションを設定する場合は、IP アドレス テーブルの IPv6 アドレスを **Add** (追加) してコンフィグします。IPv6 アドレスに RA オプションを設定する場合は、インターフェイスの **Enable Router Advertisement** (ルーター通知を有効にする) 必要があります。
最小間隔 (秒)	ファイアウォールが送信する RA 間の最小間隔 (秒) を指定します (範囲は 3 ~ 1,350、デフォルトは 200) 。ファイアウォールは、コンフィグした最小値と最大値の間のランダムな間隔で RA を送信します。
最大間隔 (秒)	ファイアウォールが送信する RA 間の最大間隔 (秒) を指定します (範囲は 4 ~ 1,800、デフォルトは 600) 。ファイアウォールは、コンフィグした最小値と最大値の間のランダムな間隔で RA を送信します。
ホップ制限	送信パケットのクライアントに適用するホップ制限を指定する (範囲は 1 〜 255、デフォルトは 64)、 または **unspecified** (未指定)を選択します。これはシステムのデフォルトにマッピングされます。
リンク MTU	クライアントに適用するリンク最大伝送単位 (MTU) を指定する (範囲は 1,280 〜 1,500)、またはデフォルトで **unspecified** (未指定)に指定します。これはシステムのデフォルトにマッピングされます。
到達可能時間 (ミリ秒)	到達可能確認メッセージを受信後ネイバーに到達可能であると想定するためにクライアントが使用する到達可能時間 (ミリ秒) を指定します (範囲は 0 〜 3,600,000) またはデフォルトの **unspecified** (未指定)に指定します。これはシステムのデフォルトにマッピングされます。
リトランスミッション時間 (ミリ秒)	ネイバー要請メッセージを再送信するまでにクライアントが待機する時間 (ミリ秒) を決定するリトランスミッション タイマーを指定します (範囲は 0 〜 4,294,967,295) またはデフォルトの **unspecified** (未指定)に指定します。これはシステムのデフォルトにマッピングされます。
ルーターの有効期間 (秒)	クライアントがファイアウォールをデフォルトゲートウェイとして使用する時間を秒単位で指定します (範囲は 0 ~ 9,000、デフォルトは 1,800) 。0 は、ファイアウォールがデフォルト ゲートウェイではないことを示します。有効期間が過ぎると、クライアントがそのデフォルト ルーター リストからファイアウォール エントリを削除して、別のルーターをデフォルト ゲートウェイとして使用します。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
ルーター設定	ネットワーク セグメントに複数の IPv6 ルーターがある場合は、クライアントがこのフィールドを使用して優先ルーターを選択します。セグメントの他のルーターとの比較において、RA が通知するファイアウォール ルーターの優先度を **High**、**Medium** (デフォルト)、**Low** の中から選択します。
管理された設定	アドレスを DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
その他の設定	他のアドレス情報 (DNS 関連の設定など) を DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
整合性チェック	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システムログの不一致が記録されます。タイプは **ipv6nd** です。
DNS Support Tab (DNSサポート タブ) (Router Advertisement (ルーター通知) タブで Router Advertisement (ルーター通知) を有効にする と利用できます)	
ルーター通知に DNS 情報を含める	ファイアウォールがこの IPv6 イーサネット インターフェイスから NDP ルーター通知で DNS 情報を送信するように選択します。その他の DNS サポート フィールド(Server (サーバー)、Lifetime (ライフタイム)、Suffix (サフィックス)、およびLifetime (ライフタイム) は、このオプションを選択した後にのみ表示されます。
SERVER	1 つ以上の再帰 DNS (RDNS) サーバー アドレスを **Add** (追加) し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信できるようにします。RDNS サーバーは、一連の DNS ルックアップ要求をルート DNS および権威 DNS サーバーに送信し、最終的に IP アドレスを DNS クライアントに提供します。 最大 8 個の RDNS サーバーをコンフィグし、ファイアウォールでそれらを NDP ルーター通知に含めて受信者に送信できます (上から下の順に送信します)。その後、受信者は同じ順序でこれらを使用できます。サーバーの順序を変更するには、サーバーを選択して **Move Up** (上へ) 移動したり **Move Down** (下へ) 移動したりします。サーバーが必要なくなったら、そのサーバーをリストから **Delete** (削除) します。
有効期間	IPv6 DNS クライアントがルーター通知を受信した後で、RDNS サーバーを使用してドメイン名を解決できるようになるまでの最長時間 (秒) を入力します (範囲は**Max Interval (最大間隔) (秒)**から**Max Interval (最大間隔) (秒)**の 2 倍、デフォルトは 1,200)。
サフィックス	DNS 検索リスト (DNSSL) のドメイン名 (サフィックス) を 1 つ以上 **Add** (追加) します。最大長は255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に (1 つずつ) 追加するドメイン サフィックスのリストです。これにより、クエリで完全修飾ドメイン名が使用されます。たとえば、DNS クライアントがサフィックスのない「quality」という名前の DNS クエリを送信しようとすると、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスを名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターのクエリの完全修飾ドメイン名は「quality.company.com」になります。

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは、DNS ルックアップが成功するまで（残りのサフィックスは無視）、またはルーターがリストのすべてのサフィックスを試すまで、DNS サフィックスを使用します。 ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスにより、ファイアウォールを設定します。DNSSL オプションを受信する DNS クライアントは非修飾 DNS クエリでそのサフィックスを使用します。 ファイアウォールがリストの上から下の順に NDP ルーター通知で受信者に送信する DNS 検索リストのドメイン名 (サフィックス) を最大 8 個設定できます。受信者は同じ順序でこれらを使用します。順序を変更するには、サフィックスを選択して **Move Up**（上へ）移動したり **Move Down**（下へ）移動したりします。サフィックスが必要なくなったら、そのサフィックスを **Delete**（削除）します。
有効期間	IPv6 DNS クライアントがルーター通知を受信した後に、DNS 検索リストのドメイン名 (サフィックス) を使用できる最大秒数を入力します (範囲は**Max Interval (最大間隔) (秒)**の値から**Max Interval (最大間隔) (秒)**の 2 倍までで、デフォルトは 1,200 です)。
SD-WAN Tab (タブ)	
SD-WAN インターフェイス ステータス	**IPv4** タブで **SD-WAN** を有効にする を選択すると、ファイアウォールは `SD-WAN` インターフェイス ステータスを表示します。有効。**SD-WAN** を有効にするを実行していない場合、ファイアウォールは SD-WAN ステータスを 無効と表示します。
SD-WAN インターフェイス プロファイル	このイーサネット インターフェiスに適用既存のSD-WAN インターフェイス プロファイルを選択するか、新しい SD-WAN インターフェイス プロファイルを追加します。 *SD-WAN インターフェイス プロファイルを適用する前に、インターフェイスの SD-WAN を有効にする 必要があります。*
Advanced Tab（詳細タブ）	
リンク速度	インターフェイス速度を**10**、**100**、**1000**Mbpsのいずれかから選択するか、**auto**[自動] を選択します。
リンクデュプレックス	インターフェイスの伝送モードをフルデュプレックス、 ハーフデュプレックス、または 自動 交渉のいずれかから選択します。
リンク ステート	インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。
Advanced Tab (詳細タブ)Other Info Tab (その他の情報タブ)	
管理プロファイル	このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義する Management (管理) プロファイルを選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU	このインターフェイスで送信されるパケットの最大転送単位（MTU）をバイト数で入力します（範囲は 576 ~9,192、デフォルトは 1,500）。ファイアウォールの両側

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが送信元にパケットが大きすぎることを示す `ICMP` フラグメント要求メッセージを返します。
TCP MSS の調整	ヘッダーのバイト数に対応できるようにインターフェイスの MTU バイト サイズ以内の値で最大セグメント サイズ（MSS）を調整する場合は選択します。MTUバイトサイズとMSS調整サイズはMSSバイトサイズと等しい値になり、これはIPによって異なります。 • **IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ)** — 範囲は40～300、デフォルトは40です。 • **IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ)** — 範囲は60～300、デフォルトは60です。 ネットワークを通る**tunnel**[トンネル] のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。 カプセル化によりヘッダーが延長されるので、MSS調整サイズはMPLSヘッダーやVLANタグを持つトンネルトラフィックよりも大きく設定しておくと便利です。
タグのないサブインターフェイス	このインターフェイスに対応するサブインターフェイスがタグ付けされていない場合は、このオプションを選択します。
Advanced Tab (詳細タブ)、ARP Entries Tab (エントリ タブ)	
IPアドレス MAC アドレス	1つ以上のスタティックARP（Address Resolution Protocol）エントリを追加する場合は、IPアドレスとそれに関連付けられたハードウェア（メディアアクセス制御、略称MAC）のアドレスを**Add**[追加] します。エントリを削除するには、エントリを選択して **Delete** (削除) します。静的 ARP エントリが ARP プロセシングを減少させます。
Advanced Tab (詳細タブ)、ND Entries Tab (エントリ タブ)	
IPv6 アドレス MAC アドレス	Neighbor Discovery Protocol (ネイバー検出プロトコル - NDP) のネイバー情報を指定する場合は、ネイバーの IPv6 アドレスと MAC アドレスを**Add** (追加) します。
Advanced Tab (詳細タブ)、NDP Proxy Tab (プロキシ タブ)	
NDP プロキシの有効化	インターフェイスで NDP（Neighbor Discovery Protocol）を有効にします。ファイアウォールは、このリストの IPv6 アドレスの MAC アドレスを要求する ND パケットに応答します。ND に対する応答として、ファイアウォールは、そのインターフェイス独自の MAC アドレスを送信します。これにより、ファイアウォールは、リスト内のアドレス宛のパケットを受信するようになります。 NPTv6 (Network Prefix Translation IPv6) を使用する場合は、NDP プロキシを有効にすることをお勧めします。 **Enable NDP Proxy (NDP** プロキシを有効にする**)** を選択すると、フィルタ条件を入力することで膨大な**Address** (アドレス) のエントリを絞り込み、Apply Filter (フィルタの適用 - 灰色の矢印) を実行することができます。
アドレス	1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、またはファイアウォールがNDPプロキシとして機能するアドレスオブジェクトを入力する場合は**Add**（追

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	加) をクリックします。これらのアドレスの 1 つは、NPTv6 の送信元変換のアドレスと同じであることが理想的です。アドレスの順序に影響はありません。 アドレスがサブネットワークの場合、ファイアウォールはサブネット内のすべてのアドレスに対して ND 応答を送信するため、ファイアウォールの IPv6 ネイバーを追加してから、それらのネイバーを **Negate** (除外) し、ファイアウォールがこれらの IPアドレスに応答しないように指示します。
Negate	あるアドレスを **Negate** (除外) し、そのアドレスで NDP プロキシを止めます。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
Advanced Tab (詳細タブ)、LLDP Tab (タブ)	
LLDP の有効化	インターフェイスの Link Layer Discovery Protocol (リンク レイヤー検出プロトコル - LLDP) を有効にします。LLDP はリンクレイヤーで機能し、ネイバーとの間で LLDP データ ユニットを送受信することにより、ネイバー デバイスとその機能を検出します。
LLDPプロファイル	既存の LLDPプロファイルを選択するか、新しい LLDP Profile (LLDPプロファイル)を作成します。プロファイルでは、LLDP モードの設定、Syslog および SNMP 通知の有効化、および LLDP ピアに送信するオプションの TLV (Type-Length-Values) の設定を行えます。
Advanced Tab (詳細タブ)、DDNS Tab (タブ)	
設定	**Settings** (設定)を選択して DDNS フィールドを設定できるようにします。
Enable [有効化]	インターフェイスで DDNS を有効にする—初めに DDNS を有効にしてから設定する必要があります。 (DDNS の設定が終わっていない場合は有効化せずに保存し、部分的な設定を保持することができます)
更新間隔 (日数)	FQDN にマッピングされた IP アドレスを更新するためにファイアウォールが DDNS サーバーに送信する更新間隔(日数) を入力します (範囲は 1 ~ 30、デフォルトは 1)。 また、ファイアウォールは*DHCP* サーバーからインターフェイスの新しい *IP* アドレスを受診した際も *DDNS* を更新します。
証明書プロファイル	証明書プロファイルを作成して DDNS サービスを検証します。DDNS サービスは、認証局 (CA) が署名した証明書をファイアウォールに提供します。
ホスト名	DDNS サーバーに登録されたインターフェイスのホスト名 (host123.domain123.com または host123 など) を入力します。DNS がドメイン名として許可している有効な文字を使った構文になっていることを確認する以外、ファイアウォールはホスト名の検証を行いません。
ベンダー	DDNS サービスをこのインターフェイスに提供する DDNS ベンダー (およびバージョン) を選択します。 • **DuckDNS v1** • **DynDNS v1**

© 2019 Palo Alto Networks, Inc.

レイヤー3 インターフェイス設定	の意味
	• **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** ファイアウォールが特定の日付までに段階的に失効すると示唆する以前のバージョンの *DDNS* サービスを選択した場合は、代わりに新しいバージョンを選択します。 ベンダー名に続く**Name** (名前)および**Value** (値)フィールドは、ベンダー固有のものです。読み取り専用フィールドは、ファイアウォールが DDNS サービスに接続するために使用するパラメーターを示しています。DDNS サービスプロバイダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用するタイムアウトなど、他のフィールドを設定します。
IPv4 Tab (タブ)	インターフェイスで設定した IPv4 アドレスを追加してから、それを選択します。IPv4 アドレスは DDNS プロバイダーが許容している数までしか選択できません。選択されたすべての IP アドレスは DDNS プロバイダー (ベンダー) に登録されています。
IPv6 Tab (タブ)	インターフェイスで設定した IPv6 アドレスを追加してから、それを選択します。IPv6 アドレスは DDNS プロバイダーが許容している数までしか選択できません。選択されたすべての IP アドレスは DDNS プロバイダー (ベンダー) に登録されています。
ランタイム情報の表示	DDNS 登録を表示します：DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス (アスタリスク (*) はプライマリ IP アドレスを示します)。トラブルシューティングを目的として、各 DDNS プロバイダーにはホスト名の更新状態を示す独自の返却コードおよび返却日が必要になります。

レイヤー 3 サブインターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

物理レイヤー 3 インターフェイスとして設定された各 Ethernet ポートについては、追加の論理レイヤー 3 インターフェイス (サブインターフェイス) を定義できます。

PA-7000 シリーズ レイヤー 3 インターフェイスを設定するには、物理インターフェイスを選択した後、**Add Subinterface** (サブインターフェイスを追加) して以下の情報を指定します。

レイヤー 3 サブインターフェイス設定	設定場所	の意味
インターフェイス名	レイヤー **3** サブインターフェイス	読み取り専用の **Interface Name**[インターフェイス名] フィールドには、選択した物理インターフェイスの名前が表示されます。サブインターフェイスを識別する数値サフィックス (1 ~ 9,999) を隣のフィールドに入力します。
コメント		サブインターフェイスの説明 (省略可) を入力します。
タグ		サブインターフェイスの VLAN タグ (1 ~ 4,094) を入力します。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
Netflowプロファイル		入力サブインターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバープロファイルを選択するか、**Netflow Profile**（**Netflow** プロファイル）をクリックして新しいプロファイルを定義します（Device（デバイス）> Server Profiles（サーバー プロファイル）> NetFlowを参照）。現在サブインターフェイスに割り当てられているNetFlowサーバーを解除する場合は、**None**[なし] を選択します。
仮想ルーター(VR)	**LPC Subinterface**（**LPC** サブインターフェイス）> **Config**（設定）	インターフェイスに仮想ルーターを割り当てるか、**Virtual Router**（仮想ルーター）をクリックして新しい仮想ルーターを定義します（「Network（ネットワーク）> Virtual Routers（仮想ルーター）」を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効な場合は、サブインターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン		サブインターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。現在サブインターフェイスに割り当てられているゾーンを解除する場合は**None**[なし] を選択します。
タイプ	**Layer3 Subinterface** > **IPv4**	IPv4 アドレス タイプをサブインターフェイスに割り当てる方法を選択します。 • **Static**[静的] — IP アドレスを手動で指定する必要があります。 • **DHCP Client**[DHCP クライアント] — サブインターフェイスが DHCP (Dynamic Host Configuration Protocol) クライアントとして機能し、ダイナミックに割り当てられた IP アドレスを受信できます。 高可用性（*HA*）アクティブ/アクティブ構成のファイアウォールは、*DHCP* クライアントをサポートしません。 選択した IP アドレス方式に応じて、タブに表示されるオプションは異なります。
ip	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **IPv4**、タイプ = 静的	**Add**（追加）をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワーク マスクを指定します。 • CIDR（Classless Inter-Domain Routing）表記法の *ip_address/mask* の形式（例: 192.168.2.0/24）でエントリを入力します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • タイプが **IP netmask**（**IP** ネットマスク）のアドレス オブジェクトを作成します。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
		インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、システムが使用する転送情報ベース (FIB) によって決まります。 不要になった IP アドレスを **Delete**（削除）します。
Enable [有効化]	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **IPv4**、タイプ = 静的	インターフェイスの DHCP クライアントを有効化する場合に選択します。
サーバー提供のデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成		DHCP サーバーによって提供されるデフォルト ゲートウェイを指し示すデフォルト ルートを自動的に作成する場合に選択します。
ホスト名の送信		ファイアウォール（DHCP クライアントとして）にインターフェイスのホスト名（Option 12）を DHCP サーバーに送信させる場合に選択します。デフォルトで Send Hostname (ホスト名の送信) を行う場合、デフォルトでファイアウォールのホスト名がホスト名フィールドで選択されます。その名前を送信するか、カスタム ホスト名（大文字および小文字、数字、ピリオド、ハイフン、アンダースコアを含む最長 64 文字）を入力します。
デフォルト ルート メトリック		（任意）ファイアウォールとDHCPサーバー間のルートについて、デフォルトルートへの関連付けと、パス選択の際に使用するルートメトリック（優先度）を入力します (範囲は 1 ~ 65535、デフォルトなし)。数値が小さいほど優先度が高くなります。
DHCP クライアント ランタイム情報の表示		DHCPのリース状態、ダイナミックIPアドレス割り当て、サブネットマスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、およびSMTP) など、DHCPサーバーから受信したすべての設定を表示する場合は**Show DHCP Client Runtime Info**[DHCPクライアントのランタイム情報を表示] を選択します。
インターフェースでの IPv6 の有効化	**Layer3 Subinterface** > **IPv6**	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID as host portion**[ホスト部分にインターフェイス ID を使用] オプションを選択すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス		**Add**[追加] をクリックして、IPv6 アドレスごとに以下のパラメータを設定します。 • **Address**（アドレス）– IPv6 アドレスとプレフィックス長を入力します（例: 2001:400:f00::1/64）。既存のIPv6アドレスオブ

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
		ジェクトを選択することや、**Address**[アドレス] をクリックしてアドレスオブジェクトを作成することもできます。 • **Enable address on interface**（インターフェイス上のアドレスを有効にする）— インターフェイスの IPv6 アドレスを有効にする場合に選択します。 • **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用）— IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。 • **Anycast**（エニーキャスト）— 最も近いノードを経由するルーティングを含める場合に選択します。 • **Send Router Advertisement**（ルーター通知を送信）— この IP アドレスのルーター通知（RA）を有効にする場合に選択します。(インターフェイスのグローバルの **Enable Router Advertisement**[ルーター通知を有効化する] オプションも有効化しておく必要があります)。 RA の詳細は、この表の「ルーター通知を有効にする」を参照してください。 残りのフィールドは、RA を有効にした場合にのみ適用されます。 • **Valid Lifetime**（有効なライフタイム）— ファイアウォールがアドレスを有効とみなす時間（秒）です。有効なライフタイムは、**Preferred Lifetime**[優先ライフタイム] 以上でなければなりません。デフォルトは2,592,000 です。 • **Preferred Lifetime**（優先ライフタイム）— 有効なアドレスが優先される時間（秒）です。この時間内は、ファイアウォールがこのアドレスを使用してトラフィックを送受信できます。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は**Valid Lifetime**[有効なライフタイム]の期限まで有効です。デフォルトは 604,800 です。 • **On-link**（オンリンク）— プレフィックス内にアドレスがあるシステムにルーターなしで到達可能である場合に選択します。 • **Autonomous**（自律型）— 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
重複アドレス検出を有効にする	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **IPv6** > **Address Resolution**（アドレス解決）	重複アドレス検出（DAD）を有効にする場合に選択し、セクション内の他のフィールドの設定を行います。
DAD 試行回数		ネイバー要請間隔 (**NS Interval (NS** 間隔**)**) の内にDADを試行する回数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この回数を超えるとネイバーに障害があるとみなされます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到達可能な時間（秒）を指定します（範囲は 1 ~ 36,000、デフォルトは 30）。
NS 間隔 (ネイバー要請間隔)		DADの試行秒数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この秒数を超えると障害があるとみなされます。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
NDP モニタリングの有効化		NDP（Neighbor Discovery Protocol）モニタリングを有効にする場合に選択します。有効にすると、NDP（機能の列の ）を選択して、IPv6 アドレス、対応する MAC アドレス、User-ID など、ファイアウォールが検出したネイバーに関する情報を（ベストケース ベースで）表示できます。
ルーター通知を有効にする	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）	ネイバー検出を IPv6 インターフェイスで提供するには、このセクションのその他のフィールドを選択して設定します。ルーター通知（RA）メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アドレスごとに RA オプションを設定する場合は、IP アドレス テーブルのアドレスを **Add**（追加）して設定します。IP アドレスに RA オプションを設定する場合は、インターフェイスの **Enable Router Advertisement**（ルーター通知を有効にする）必要があります。
最小間隔 (秒)		ファイアウォールが送信する RA 間の最小間隔（秒）を指定します（範囲は 3 ~ 1,350、デフォルトは 200）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
最大間隔 (秒)		ファイアウォールが送信する RA 間の最大間隔（秒）を指定します（範囲は 4 ~ 1,800、デフォルトは 600）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を指定します（範囲は 1 ~ 255、デフォルトは 64）。ホップ制限を指定しない場合は 0 を入力します。
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を指定します。リンクMTUを指定しない場合は **unspecified (指定しない)** を選択します（範囲は 1,280 ~ 9,192、デフォルトは unspecified）。
到達可能時間 (ミリ秒)		到達可能確認メッセージを受信後ネイバーに到達可能であると想定するためにクライアントが使用する到達可能時間 (ミリ秒) を指定します。到達可能時間を指定しない場合は **unspecified (指定しない)** を選択します（範囲は 0 ~ 3,600,000、デフォルトはunspecified）。
リトランスミッション時間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが待機する時間を決定するリトランスミッション タイマーを指定します。リトランスミッション時間を指定しない場合は **unspecified (指定**

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
		しない) を選択します (範囲は 0 ~ 4,294,967,295、デフォルトはunspecified) 。
ルーターの有効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェイとして使用する時間を秒単位で指定します (範囲は 0 ~ 9,000、デフォルトは 1,800) 。0 は、ファイアウォールがデフォルト ゲートウェイではないことを示します。有効期間が過ぎると、クライアントがそのデフォルト ルーター リストからファイアウォール エントリを削除して、別のルーターをデフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合は、クライアントがこのフィールドを使用して優先ルーターを選択します。セグメントの他のルーターとの比較において、RA が通知するファイアウォール ルーターの優先度を **High**、**Medium** (デフォルト)、**Low** の中から選択します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
その他の設定		他のアドレス情報 (DNS 関連の設定など) を DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
整合性チェック	**Layer3 Subinterface** (レイヤー 3 サブインターフェイス) > **IPv6** > **Router Advertisement** (ルーター通知) (続き)	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システム ログの不一致が記録されます。タイプは **ipv6nd** です。 ルー
ルーター通知に DNS 情報を含める	**Layer3 Subinterface** (レイヤー 3 サブインターフェイス) > **IPv6** > **DNS Support** (**DNS** サポート)	この IPv6 Ethernet インターフェイスから NDP ルーター通知によって DNS 情報を送信するファイアウォールのために選択します。この表の他の DNS Support (DNS サポート) フィールドは、このオプションを選択した場合にのみ表示されます。
SERVER		1 つ以上の再帰 DNS (RDNS) サーバー アドレスを **Add** (追加) し、ファイアウォールがこの IPv6 Ethernet インターフェイスから NDP ルーター通知によって送信できるようにします。RDNS サーバーは、一連の DNS ルックアップ要求をルート DNS および権威 DNS サーバーに送信し、最終的に IP アドレスを DNS クライアントに提供します。 最大で 8 個の RDNS サーバーを設定でき、ファイアウォールはこれを NDP ルーター通知によってリストの上から下の順序で受信者へと送信し、受信者は同じ順序でこれを使用します。サーバーの順序を変更するには、サーバーを選択して **Move Up** (上へ) 移動したり **Move Down** (下へ) 移動したりします。サーバーが必要なくなったら、そのサーバーをリストから **Delete** (削除) します。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
有効期間		IPv6 DNS クライアントがルーター通知を受信した後で、RDNS サーバーを使用してドメイン名を解決できるようになるまでの最長時間（秒数）を入力します（範囲は最大間隔（秒）から最大間隔の 2 倍、デフォルトは 1,200）。
サフィックス	**Layer3 Subinterface** (レイヤー3 サブインターフェイス) > **IPv6** > **DNS Support (DNS** サポート) (続き)	DNS 検索リスト（DNSSL）のドメイン名（サフィックス）を 1 つ以上 **Add**（追加）します。最大長は255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に（1 つずつ）追加するドメイン サフィックスのリストです。これにより、クエリで完全修飾ドメイン名が使用されます。たとえば、DNS クライアントがサフィックスのない「quality」という名前の DNS クエリを送信しようとすると、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスを名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターのクエリの完全修飾ドメイン名は「quality.company.com」になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは、DNS ルックアップが成功するまで（残りのサフィックスは無視）、またはルーターがリストのすべてのサフィックスを試すまで、DNS サフィックスを使用します。 ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスにより、ファイアウォールを設定します。DNSSL オプションを受信する DNS クライアントは非修飾 DNS クエリでそのサフィックスを使用します。 最大で 8 個のドメイン名（サフィックス）を DNS 検索リスト オプションに設定でき、ファイアウォールはこれをNDP ルーター通知によってリストの上から下の順序で受信者へと送信し、受信者は同じ順序でこれを使用します。順序を変更するには、サフィックスを選択して **Move Up**（上へ）移動したり **Move Down**（下へ）移動したりします。サフィックスが必要なくなったら、そのサフィックスを **Delete**（削除）します。
有効期間	**Layer3 Subinterface** (レイヤー3 サブインターフェイス) > **IPv6** > **DNS Support (DNS** サポート) (続き)	IPv6 DNS クライアントがルーター通知を受信した後に、DNS 検索リストのドメイン名（サフィックス）を使用できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。
管理プロファイル	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）>	**Management Profile**[管理プロファイル] – このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択しま

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
	Advanced（詳細）> **Other Info**（その他の情報）	す。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位（MTU）をバイト数で入力します（範囲は 576 ~9,192、デフォルトは 1,500）。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが送信元にパケットが大きすぎることを示す *ICMP* フラグメント要求メッセージを返します。
TCP MSS の調整	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **Advanced**（詳細）> **Other Info**（その他の情報）	ヘッダーのバイト数に対応できるようにインターフェイスの MTU バイト サイズ以内の値で最大セグメント サイズ（MSS）を調整する場合は選択します。MTUバイトサイズとMSS調整サイズはMSSバイトサイズと等しい値になり、これはIPによって異なります。 • **IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ)** — 範囲は40 ~ 300、デフォルトは40です。 • **IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ)** — 範囲は60 ~ 300、デフォルトは60です。 ネットワークを通る**tunnel**[トンネル] のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。 カプセル化によりヘッダーが延長されるので、MSS調整サイズはMPLSヘッダーやVLANタグを持つトンネルトラフィックよりも大きく設定しておくと便利です。
IPアドレス MAC アドレス	**Layer3 Subinterface**（レイヤー 3 サブインターフェイス）> **Advanced**（詳細）> **ARP Entries**（ARP エントリ）	1つ以上のスタティックARP（Address Resolution Protocol）エントリを追加する場合は、IPアドレスとそれに関連付けられたハードウェア（メディアアクセス制御、略称MAC）のアドレスを**Add**[追加] します。エントリを削除するには、エントリを選択して **Delete**[削除] をクリックします。静的 ARP エントリが ARP プロセシングを減少させます。
IPv6 アドレス MAC アドレス	**Layer3 Subinterface** > **Advanced** > **ND Entries**	NDP（Neighbor Discovery Protocol）のネイバー情報を指定する場合は、ネイバーのIPアドレスとMACアドレスを**Add**[追加] します。
NDP プロキシの有効化	**Layer3 Subinterface** > **Advanced** > **NDP Proxy**	インターフェイスで NDP（Neighbor Discovery Protocol）を有効にします。ファイアウォールは、このリストの IPv6 アドレスの MAC アドレスを要求する ND パケットに応答します。ND に対する応答として、ファイアウォールは、そのインターフェイス独自の MAC アドレスを送信します。これにより、ファイアウォールは、リスト内のアドレス宛のパケットを受信するようになります。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
		NPTv6 (Network Prefix Translation IPv6) を使用する場合は、NDP プロキシを有効にすることをお勧めします。 **Enable NDP Proxy**[NDPプロキシの有効化] を選択した場合、膨大な**Address**[アドレス] のエントリを絞り込む場合は、フィルタ条件を入力しフィルタの適用アイコン (灰色の矢印) をクリックします。
アドレス		1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、またはファイアウォールがNDPプロキシとして機能するアドレスオブジェクトを入力する場合は**Add**（追加）をクリックします。これらのアドレスの 1 つは、NPTv6 の送信元変換のアドレスと同じであることが理想的です。アドレスの順序は問題になりません。 アドレスがサブネットワークの場合、ファイアウォールは、サブネットのすべてのアドレスに対してND応答を送信します。したがって、ファイアウォールのIPv6ネイバーも追加し、**Negate**[除外] をクリックし、これらのIPアドレスに応答しないようにファイアウォールに指示することをお勧めします。
Negate		あるアドレスを **Negate**（除外）し、そのアドレスで NDP プロキシを止めます。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
設定	**Layer3 Subinterface** > **Advanced** > **DDNS**	**Settings** (設定)を選択して DDNS フィールドを設定できるようにします。
Enable [有効化]		インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。（DDNS の設定が終わっていない場合は有効化せずに保存し、部分的な設定を保持することができます）
更新間隔（日数）	**Layer3 Subinterface** > **Advanced** > **DDNS**	FQDN にマッピングされた IP アドレスを更新するためにファイアウォールが DDNS サーバーに送信する更新間隔（日数）を入力します（範囲は1～30、デフォルトは 1）。 また、ファイアウォールは*DHCP* サーバーからインターフェイスの新しい *IP* アドレスを受診した際も *DDNS* を更新します。
証明書プロファイル		証明書プロファイルを作成して DDNS サービスを検証します。DDNS サービスは、認証局（CA）が署名した証明書をファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト名（例：host123.domain123.com、or host123）を入力します。DNS がドメイン名として許可している有効な文字を使った構文になっていることを確認する以外、ファイアウォールはホスト名の検証を行いません。
ベンダー	**Layer3 Subinterface**	DDNS サービスをこのインターフェイスに提供する DDNS ベンダー（およびバージョン）を選択します。

© 2019 Palo Alto Networks, Inc.

レイヤー 3 サブインターフェイス設定	設定場所	の意味
	> **Advanced** > **DDNS**	• **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** ファイアウォールが特定の日で失効すると示唆する *DDNS* サービスの古いバージョンを選択する場合、新しいバージョンに移動させます。 ベンダー名に続く**Name** (名前)および**Value** (値)フィールドは、ベンダー固有のものです。読み取り専用フィールドは、ファイアウォールが DDNS サービスに接続するために使用するパラメーターを示しています。DDNS サービスプロバイダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用するタイムアウトなど、他のフィールドを設定します。
IPv4 タブ - IP		インターフェイスで設定した IPv4 アドレスを追加してから、それを選択します。IPv4 アドレスは DDNS プロバイダーが許容している数までしか選択できません。選択されたすべての IP アドレスは DDNS プロバイダー (ベンダー) に登録されています。
IPv6 タブ - IPv6		インターフェイスで設定した IPv6 アドレスを追加してから、それを選択します。IPv6 アドレスは DDNS プロバイダーが許容している数までしか選択できません。選択されたすべての IP アドレスは DDNS プロバイダー (ベンダー) に登録されています。
ランタイム情報の表示	**Layer3 Subinterface** > **Advanced** > **DDNS**	DDNS 登録を表示します：DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス (アスタリスク (*) はプライマリ IP アドレスを示します)。トラブルシューティングを目的として、各 DDNS プロバイダーにはホスト名の更新状態を示す独自の返却コードおよび返却日が必要になります。

Log Card Interface (ログ カード インターフェイス)

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

LPC (Log Processing Card) がある PA-7000 シリーズ ファイアウォールでログ転送を設定する場合は、1 つのデータ ポートを **Log Card** (ログ カード) タイプとして設定する必要があります。これは、このファイアウォール モデルのトラフィックおよびロギング機能が管理 (MGT) インターフェイスの機能を超えるためです。ログ カードのデータ ポートは、Syslog、電子メール、SNMP (Simple Network Management Protocol)、Panorama ログ転送、WildFire™ ファイル転送のログ転送を実行します。

ファイアウォールで *Log Card* (ログ カード) タイプに設定できるポートは *1* 個のみです。ログ転送を有効にして *Log Card* (ログ カード) タイプでインターフェイスを設定していないと、変更をコミットしようとしたときにエラーが発生します。

ログ カード インターフェイスを設定するには、設定されていないインターフェイス (Ethernet 1/16 など) を選択し、次の表で説明する設定を構成します。

© 2019 Palo Alto Networks, Inc.

ログ カード インターフェイス設定	設定場所	の意味
スロット	イーサネットインターフェイス	インターフェイスのスロット番号 (1 ~ 12) を選択します。
インターフェイス名		インターフェイス名は事前に定義されており、変更することはできません。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		**Log Card**[ログ カード] を選択します。
IPv4	**Ethernet Interface** > **Log Card Forwarding** [イーサネットインターフェイス ログ カード転送]	ネットワークで IPv4 が使用されている場合は、以下を定義します。 • **IP address**[IP アドレス] – ポートの IPv4 アドレス。 • **Netmask**[ネットマスク] – ポートの IPv4 アドレスのネットワークマスク。 • **Default Gateway**[デフォルトゲートウェイ] – ポートのデフォルトゲートウェイのIPv4アドレス。
IPv6		ネットワークで IPv6 が使用されている場合は、以下を定義します。 • **IP** アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲートウェイの IPv6 アドレス。
リンク速度	**Ethernet Interface** (イーサネット インターフェイス) > **Advanced** (詳細)	インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto** (デフォルト設定) を選択して、接続ごとにファイアウォールに自動的に速度を決定させます。スピード設定が不可のインターフェイスについてはautoのみ設定可能です。 接続速度は最低*1000 Mbps*以上に設定することをおすすめします。
リンクデュプレックス		接続の種類に応じて、インターフェイスの伝送モードをフルデュプレックス (**full**)、ハーフデュプレックス (**half**)、自動ネゴシエート (**auto**) から選択します。デフォルト設定はautoです。
リンク ステート		接続に応じて、インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。デフォルト設定はautoです。

ログ カード サブインターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

Log Card Interface (ログ カード インターフェイス) を追加する場合は、そのインターフェイスの行を選択した後、**Add Subinterface** (サブインターフェイスの追加) をクリックし、以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

ログ カード サブインターフェイス設定	設定場所	の意味
インターフェイス名	**LPC** サブインターフェイス	読み取り専用の**Interface Name**[インターフェイス名] フィールドには、選択したログカードインターフェイスの名前が表示されます。サブインターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
タグ		サブインターフェイス用のVLAN**Tag**[タグ] (0 ~ 4094) を入力します。 使いやすさのため、タグはサブインターフェイス番号と同じにしてください。
仮想システム(vsys)	**LPC Subinterface** (**LPC** サブインターフェイス) > **Config** (設定)	LPC (Log Processing Card) サブインターフェイスの割り当て先の仮想システム (vsys) を選択します。**Virtual Systems**[仮想システム] リンクをクリックして新しいvsysを追加することもできます。LPC サブインターフェイスを vsys に割り当てると、そのインターフェイスは、ログ カードからログ (Syslog、電子メール、SNMP) を転送するすべてのサービスの送信元インターフェイスとして使用されます。
IPv4	**Ethernet Interface** > **Log Card Forwarding** [イーサネットインターフェイス ログカード転送]	ネットワークで IPv4 が使用されている場合は、以下を定義します。 • **IP address**[IP アドレス] – ポートの IPv4 アドレス。 • **Netmask**[ネットマスク] – ポートの IPv4 アドレスのネットワーク マスク。 • **Default Gateway**[デフォルトゲートウェイ] – ポートのデフォルトゲートウェイのIPv4アドレス。
IPv6		ネットワークで IPv6 が使用されている場合は、以下を定義します。 • **IP** アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲートウェイの IPv6 アドレス。

復号化ミラー インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

復号化ポート ミラー機能を使用するには、**Decrypt Mirror**[復号化ミラー] インターフェイス タイプを選択する必要があります。この機能では、ファイアウォールからの復号化されたトラフィックのコピーを作成して、トラフィック収集ツールに送信できます。このツールは、NetWitness や Solera などの生パケット キャプチャを受信してアーカイブや分析を行うことができます。フォレンジックや履歴調査の目的で、または DLP (情報漏洩対策) 機能に包括的なデータ キャプチャを必要とする組織では、この機能が不可欠です。この機能を有効にするには、フリー ライセンスを取得してインストールする必要があります。

© 2019 Palo Alto Networks, Inc.

パブリック クラウド プラットフォーム向け *VM-Series* (*AWS*、*Azure*、*Google Cloud Platform*)、*VMware NSX*、*Citrix SDX* では復号化ポート ミラーリングは使用できません。

復号化ミラー インターフェイスを設定するには、設定されていないインターフェイスの名前 ([Ethernet1/1] など) をクリックし、以下の情報を指定します。

復号化ミラー インターフェイスの設定	の意味
インターフェイス名	インターフェイス名は事前に定義されており、変更することはできません。
コメント	インターフェイスの説明 (省略可) を入力します。
インターフェイス タイプ	**Decrypt Mirror**[復号化ミラー] を選択します。
リンク速度	インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto** を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプレックス	インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート	インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。

Ethernet の集約 (AE) インターフェイス グループ

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

AEインターフェイスグループはIEEE 802.1AXリンク集約をもちい、複数のEthernetインターフェイスを、そのファイアウォールと他のネットワークデバイスまたはファイアウォールへ接続する、一つの仮想インターフェイスにまとめます。AEインターフェイスグループは、組み合わされたインターフェイスの間のロードバランスを行うことでピア同士の帯域幅を増加させます。また、1つのインターフェイスが障害を起こした場合も残りのインターフェイスがトラフィックをサポートするため、冗長性の確保にも役立ちます。

AEインターフェイスグループの設定を行う前に、それが使用するインターフェイスの設定を行う必要があります。特定の集約グループに割り当てたインターフェイスのうち、ハードウェアメディアは異なる場合があります (たとえば、光ファイバと銅線を混在させることもできます) が、帯域幅 (1Gbps、10Gbps、40Gbps、100GBps) とインターフェイスタイプ (HA3、バーチャルワイヤ、レイヤ 2、レイヤ 3 など) は同じでなければなりません。各ファイアウォールにつき最大8個のAEインターフェイスグループを追加することができ、また各グループは最大8個のインターフェイスを持つことができます。

VM-Series モデルを除く *Palo Alto Networks* のすべてのファイアウォールは *AE* インターフェイス グループをサポートしています。

以下のファイアウォール モデルに限り、アクティブ/アクティブの高可用性 (*HA*) 環境におかれた *HA3* (パケット転送) インターフェイスを集約することができます。

- *PA-220*
- *PA-800*シリーズ

© 2019 Palo Alto Networks, Inc.

- *PA-3200シリーズ*
- *PA-5200シリーズ*

AE インターフェイス グループを設定する場合は、**Add Aggregate Group**（集約グループを追加）し、以下の表で説明されている項目を設定してから、インターフェイスをグループに割り当てます（「Ethernet の集約（AE）インターフェイス」を参照）。

集約インターフェイス グループの設定	設定場所	の意味
インターフェイス名	**Ethernet**の集約インターフェイス	読み取り専用の**Interface Name**[インターフェイス名] フィールドには **ae**が設定されています。AE インターフェイス グループを識別する数値サフィックス（1 ~ 8）を隣のフィールドに入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
インターフェイスタイプ		インターフェイス タイプを選択します。このタイプによって、残りの設定要件やオプションが制御されます。 • **HA** – インターフェイスがアクティブ/アクティブ デプロイ環境の 2 つのファイアウォール間の HA3 リンクである場合にのみ選択します。必要に応じて、**Netflow Profile**（**Netflow** プロファイル）を選択し、**LACP** タブの設定を行います（「LACP を有効化」を参照）。 • **Virtual Wire**（バーチャル ワイヤー） – 必要に応じて、**Netflow Profile**（**Netflow** プロファイル）を選択し、「バーチャル ワイヤー設定」の説明に従って **Config**（設定）タブと **Advanced**（詳細）タブを設定します。 • **Layer 2**（レイヤー 2） – 必要に応じて、**Netflow Profile**（**Netflow** プロファイル）を選択し、「レイヤー 2 インターフェイス設定」の説明に従って **Config**（設定）タブと **Advanced**（詳細）タブを設定します。また、必要に応じて **LACP** タブを設定します（「LACP を有効化」を参照）。 • **Layer 3**（レイヤー 3） – 必要に応じて、**Netflow Profile**（**Netflow** プロファイル）を選択し、「レイヤー 3 インターフェイス設定」の説明に従って **Config**（設定）タブ、**IPv4** タブまたは **IPv6** タブ、および **Advanced**（詳細）タブを設定します。また、必要に応じて **LACP** タブを設定します（「LACP を有効化」を参照）。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile**（**Netflow** プロファイル）をクリックして新しいプロファイルを定義します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> NetFlow」を参照）。**None**[なし] を選択すると、現在AEインターフェイスグループに割り当てられているNetFlowサーバーが解除されます。
LACP を有効化	**Aggregate Ethernet Interface**[**Ethernet** の集約インター	AE インターフェイス グループのリンク集約制御プロトコル（LACP）を有効にする場合に選択します。LACP はデフォルトで無効になっています。 LACPを有効化した場合、ファイアウォールとそのLACPピアが直接接続されているかどうかに関わらず、物理リンクレイヤーおよびデータ

© 2019 Palo Alto Networks, Inc.

集約インターフェイス グループの設定	設定場所	の意味
	フェイス] > **LACP [LACP]**	リンクレイヤーにおいてインターフェイス障害が自動的に検知されます。 (LACPを使用しない場合、直接接続されたピア間の物理レイヤーのみにおいてインターフェイス障害が自動的に検出されます。) ホット スペアを設定した場合、LACP により待機中のインターフェイスへ自動フェイルオーバーを行うことが可能になります (「最大ポート」を参照) 。
モード		ファイアウォールの LACP モードを選択します。2つのLACPピアにおいては、一方をアクティブ、もう一方をパッシブにすることをお勧めします。両方ともパッシブの場合は LACP が機能しません。 • **Active**[アクティブ] – ファイアウォールがピア デバイスの LACP の状態 (使用可能または無応答) をアクティブにクエリします。 • **Passive**[パッシブ] (デフォルト) – ファイアウォールがピア デバイスからの LACP 状態のクエリにパッシブに応答します。
トランスミッション率		ファイアウォールがピア デバイスとクエリおよび応答をやりとりする間隔を選択します。 • **Fast**[高速] – 毎秒 • **Slow**[低速] – 30 秒ごと (デフォルトの設定)
高速フェールオーバー		インターフェイスがダウンしたときに、1 秒以内にファイアウォールを動作中のインターフェイスにフェイルオーバーさせたい場合に選択します。それ以外の場合は、標準の IEEE 802.1AX 定義の速度 (3 秒以上) でフェールオーバーが生じます。
システム優先度	**Aggregate Ethernet Interface [Ethernet の集約インターフェイス] > LACP (cont)**	ファイアウォールまたはそのピアが、ポート優先度に応じてもう一方をオーバーライドするかどうかを判断する数字 (以下の **Max Ports**[最大ポート] フィールドの説明を参照)。 数値が小さいほど優先度は高くなります (範囲は *1* ~ *65,535*、デフォルトは *32,768*) 。
最大ポート		任意の時点で LACP 集約グループでアクティブにできるインターフェイスの数 (1 ~ 8)。この値を、グループに割り当てるインターフェイスの数より大きくすることはできません。割り当てられたインターフェイスの数がアクティブなインターフェイスの数を上回ると、ファイアウォールがインターフェースのLACPポート優先度に従って、どのインターフェイスがスタンバイモードかを判断します。LACP ポートの優先度は、グループの個々のインターフェイスを設定する際に設定します (「Ethernet の集約 (AE) インターフェイス」を参照) 。
HAパッシブステートを有効にする		アクティブ/パッシブの高可用性 (HA) 環境にデプロイされたファイアウォールにおいて、フェイルオーバーの実行前にパッシブなピアからアクティブなピアへ LACP を事前にネゴシエートするよう設定する場合に選択します。事前にネゴシエートを実行することで、パッシブなファイアウォールがアクティブに切り替わる際にLACPのネゴシエートを行う必要がなくなるので、フェイルオーバーの作業が高速化されます。

© 2019 Palo Alto Networks, Inc.

集約インターフェイス グループの設定	設定場所	の意味
Same System MAC Address for Active-Passive HA（アクティブ/パッシブ HA に同一システム MAC アドレスを使用する）		これはアクティブ/パッシブの高可用性（HA）環境にデプロイされたファイアウォールにのみ適用されます。アクティブ/アクティブ設定のファイアウォールは一意の MAC アドレスを必要とします。 HAファイアウォールのピアは同じシステム優先度を設定されています。ただし、アクティブ/パッシブ デプロイメントでは、同一の MAC アドレスを割り当てるかどうかにより、それぞれのシステム ID が同じこともあれば、異なることもあります *HA*モードの*LACP*ピアが仮想化されている場合は（ネットワークに*1*つのデバイスとして表示される）、ファイアウォールに同一のシステム*MAC*アドレスを使用すると、フェイルオーバー時の待機時間が最小限に抑えられます。*LACP*ピアが仮想化されていない場合は、ファイアウォールごとに一意の*MAC*アドレスすると、フェイルオーバーの待機時間が最小限に抑えられます。 LACP は、MAC アドレスを使用して、各 LACP ピアのシステム ID を取得します。ファイアウォール ペアおよびピア ペアに同一のシステム優先度の値が設定されている場合は、LACP がシステム ID の値を使用して、ポート優先度に応じてどちらがもう一方をオーバーライドするかを判断します。両方のファイアウォールの MAC アドレスが同じ場合は、両者のシステム ID も同じで、LACP ピアのシステム ID よりも大きいか小さくなります。HA ファイアウォールに一意の MAC アドレスが設定されている場合は、一方のシステム ID は LACP ピアよりも大きく、もう一方は小さいことがあります。後者の場合は、ファイアウォールでフェイルオーバーが発生したときに、LACP ピアとアクティブになるファイアウォール間のポート優先度が切り替わります。
MAC アドレス		**Use Same System MAC Address**[システムと同一のMACアドレスを使用] を有効化した場合は、アクティブ/パッシブの高可用性（HA）ペアのファイアウォールの両方について、システム生成のMACアドレスを選択するか、独自のアドレスを入力します。アドレスがグローバルに一意であることを確認します。

Ethernet の集約（AE）インターフェイス

- Network > Interfaces > Ethernet [ネットワーク > インターフェイス > イーサネット]

Ethernet の集約（AE）インターフェイスを設定する場合は、まず Ethernet の集約（AE）インターフェイス グループを設定して、そのグループに割り当てるインターフェイスの名前をクリックします。特定のグループに割り当てるインターフェイスのうち、ハードウェアメディアは異なる場合があります（たとえば、光ファイバと銅線を混在させることもできます）が、帯域幅とインターフェイスタイプ（レイヤ 3 など）は同じでなければなりません。さらに、インターフェイスのタイプは、AE インターフェイスグループに対して定義されたタイプと同じでなければなりません。ただし、各インターフェイスの設定時にタイプを **Aggregate Ethernet**（**Ethernet** の集約）に変更します。グループに割り当てる各インターフェイスに以下の情報を指定します。

© 2019 Palo Alto Networks, Inc.

AE インターフェイス グループに対するリンク集約制御プロトコル（*LACP*）を有効にした場合は、そのグループのすべてのインターフェイスに対して同じ *Link Speed*（リンク速度）と *Link Duplex*（リンク デュプレックス）を選択します。値が一致していない場合は、コミット操作時に警告が表示され、*PAN-OS* がデフォルトのより高い速度およびフル デュプレックスを設定します。

集約インターフェイス設定	設定場所	の意味
インターフェイス名	**Ethernet**の集約インターフェイス	インターフェイス名は事前に定義されており、変更することはできません。
コメント		（任意）インターフェイスの説明を入力します。
インターフェイスタイプ		**Aggregate Ethernet**[Ethernet の集約] を選択します。
集約グループ		インターフェイスを集約グループに割り当てます。
リンク速度		インターフェイスの速度 (**10**、**100**、または **1000** Mbps) を選択するか、**auto** を選択してファイアウォールに自動的に速度を決定させます。
リンクデュプレックス		インターフェイスの伝送モードを、フル デュプレックス (**full**)、ハーフ デュプレックス (**half**)、オート ネゴシエーション (**auto**) から選択します。
リンク ステート		インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。
LACP ポート優先順位		ファイアウォールがこのフィールドを使用するのは、集約グループのリンク集約制御プロトコル (LACP) が有効になっている場合のみです。割り当てられたインターフェイスの数がアクティブなインターフェイスの数（Max Ports（最大ポート）フィールド）を上回ると、ファイアウォールがインターフェイスの LACP ポート優先度に従って、どのインターフェイスがスタンバイ モードかを判断します。数値が小さいほど優先度は高くなります（範囲は1～65535、デフォルトは32768）。
仮想ルーター(VR)	**Aggregate Ethernet Interface**（**Ethernet** の集約インターフェイス）> **Config**（設定）	Ethernet の集約インターフェイスを割り当てる仮想ルーターを選択します。
セキュリティ ゾーン		Ethernet の集約インターフェイスを割り当てるセキュリティ ゾーンを選択します。
インターフェースでの IPv6 の有効化	**Aggregate Ethernet Interface** > **IPv6**	このインターフェイスの IPv6 を有効にする場合に選択します。
インターフェイス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID**

© 2019 Palo Alto Networks, Inc.

集約インターフェイス設定	設定場所	の意味
		as host portion（ホスト部分にインターフェイス **ID** を使用）すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。

アドレス		IPv6 アドレスを **Add**（追加）し、以下のパラメータを設定します。
		• **Address**[アドレス] – IPv6 アドレスとプレフィックス長を入力します (例: 2001:400:f00::1/64)。既存の IPv6 アドレス オブジェクトを選択することや、**Address**（アドレス）をクリックしてアドレス オブジェクトを作成することもできます。
		• **Enable address on interface**（インターフェイス上のアドレスを有効にする） – インターフェイスの IPv6 アドレスを有効にする場合に選択します。
		• **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用） – IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。
		• **Anycast**（エニーキャスト） – 最も近いノードを経由するルーティングを含める場合に選択します。
		• **Send RA**（**RA** の送信） – この IP アドレスのルーター通知（RA）を有効にする場合に選択します。このオプションを選択する場合、インターフェイスでグローバルに **Enable Router Advertisement**（ルーター通知を有効にする）必要もあります。RA の詳細は、「ルーター通知を有効にする」を参照してください。
		残りのフィールドは、RA を有効にした場合にのみ表示されます。
		  • **Valid Lifetime**（有効なライフタイム） – ファイアウォールがアドレスを有効とみなす時間（秒）です。有効なライフタイムは、**Preferred Lifetime**[優先ライフタイム] 以上でなければなりません。デフォルトは2,592,000 です。
		  • **Preferred Lifetime**（優先ライフタイム） – 有効なアドレスが優先される時間（秒）です。この時間内は、ファイアウォールがこのアドレスを使用してトラフィックを送受信できます。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は **Valid Lifetime**（有効なライフタイム）を超えるまで有効です。デフォルトは 604,800 です。
		  • **On-link**（オンリンク） – 通知されたプレフィックス内に IP アドレスがあるシステムにルーターなしで到達可能な場合に選択します。
		  • **Autonomous**（自律型） – 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。

重複アドレス検出を有効にする	**Aggregate Ethernet Interface**（**Ethernet** の集約インターフェイス）> **IPv6** > **Address**	重複アドレス検出（DAD）を有効にして、**DAD Attempts**（**DAD** 試行回数）の数値を指定できるようにする場合に選択します。
DAD 試行回数		ネイバー要請間隔 (**NS Interval**[NS間隔]) の内にDADを試行する回数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この回数を超えるとネイバーに障害があるとみなされます。

© 2019 Palo Alto Networks, Inc.

集約インターフェイス設定	設定場所	の意味
到達可能時間	**Resolution**（アドレス解決）	クエリと応答が正常に行われた後引き続きネイバーに到達可能な時間（秒）を指定します（範囲は 1 ~ 36,000、デフォルトは 30）。
NS 間隔 (ネイバー要請間隔)		DAD 試行エラーが示されるまでの時間の長さを秒単位で指定します（範囲は 1 ~ 10、デフォルトは 1）。
NDP モニタリングの有効化		Neighbor Discovery Protocol のモニタリングを有効にする場合に選択します。有効になっていると、NDP（Features（機能）列の ）を選択し、ファイアウォールで検出されたネイバーの IPv6 アドレス、対応する MAC アドレスおよび User-ID などの情報を（ベストケースベースで）表示できます。
ルーター通知を有効にする	**Aggregated Ethernet Interface**（**Ethernet** の集約インターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）	IPv6 インターフェイスのネイバー検出を指定して、このセクションの他のフィールドを設定する場合に選択します。ルーター通知（RA）メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アドレスごとに RA オプションを設定する場合は、IP アドレス テーブルのアドレスを **Add**（追加）して設定します。IP アドレスに RA オプションを設定する場合は、インターフェイスの **Enable Router Advertisement**（ルーター通知を有効にする）必要があります。
最小間隔 (秒)		ファイアウォールが送信する RA 間の最小間隔（秒）を指定します（範囲は 3 ~ 1,350、デフォルトは 200）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
最大間隔 (秒)		ファイアウォールが送信する RA 間の最大間隔（秒）を指定します（範囲は 4 ~ 1,800、デフォルトは 600）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を指定します（範囲は 1 ~ 255、デフォルトは64）。ホップ制限を指定しない場合は **0** を入力します。
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を指定します。リンクMTUを指定しない場合は **unspecified**[指定しない] を選択します (範囲は 1280 ~ 9192、デフォルトはunspecified)。
到達可能時間 (ミリ秒)		到達可能確認メッセージを受信後ネイバーに到達可能であると想定するためにクライアントが使用する到達可能時間（ミリ秒）を指定します。到達可能時間を指定しない場合は **unspecified**[指定しない] を選択します (範囲は 0 ~ 3600000、デフォルトはunspecified)。

© 2019 Palo Alto Networks, Inc.

集約インターフェイス設定	設定場所	の意味
リトランスミッション時間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが待機する時間（ミリ秒）を決定するリトランスミッション タイマーを指定します。リトランスミッション時間を指定しない場合は **unspecified**[指定しない] を選択します (範囲は 0 ~ 4294967295、デフォルトはunspecified)。
ルーターの有効期間 (秒)		クライアントがファイアウォールをデフォルト ゲートウェイとして使用する時間（秒）を指定します（範囲は 0 ~ 9,000、デフォルトは 1,800）。0 は、ファイアウォールがデフォルト ゲートウェイではないことを示します。有効期間が過ぎると、クライアントがそのデフォルト ルーター リストからファイアウォール エントリを削除して、別のルーターをデフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合は、クライアントがこのフィールドを使用して優先ルーターを選択します。セグメントの他のルーターとの比較において、RA が通知するファイアウォール ルーターの優先度を **High**、**Medium** (デフォルト)、**Low** の中から選択します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
その他の設定		他のアドレス情報（DNS 関連の設定など）を DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
整合性チェック	**Aggregated Ethernet Interface**（**Ethernet** の集約インターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）（続き）	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システム ログの不一致が記録されます。タイプは **ipv6nd** です。
ルーター通知に DNS 情報を含める	**Aggregated Ethernet Interface**（**Ethernet** の集約インターフェイス）> **IPv6** > **DNS Support**（**DNS** サポート）	ファイアウォールがこの IPv6 の Ethernet の集約インターフェイスからの NDP ルーター通知（RA）メッセージで DNS 情報を送信する場合に選択します。この表の他の DNS Support（DNS サポート）フィールドは、このオプションを選択した場合にのみ表示されます。
SERVER		ファイアウォールがこの IPv6 の Ethernet の集約インターフェイスからの NDP ルーター通知で送信する 1 つ以上の再帰 DNS（RDNS）サーバー アドレスを **Add**（追加）します。RDNS サーバーは、ルート DNS サーバーと権限のある DNS サーバーに一連の DNS ルックアップ要求を送信し、最終的に DNS クライアントに IP アドレスを提供します。 ファイアウォールがリストの上から下の順に NDP ルーター通知で受信者に送信する RDNS サーバーを最大 8 個設定できます。その後、受信者は同じ順序でこれらのアドレスを使用します。サーバーを選択し、**Move Up**（上へ）または **Move Down**（下へ）を選択してサー

© 2019 Palo Alto Networks, Inc.

集約インターフェイス設定	設定場所	の意味
		バーの順序を変更するか、不要になったサーバーを **Delete**（削除）します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後に、RDNS サーバーを使用してドメイン名を解決できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。
サフィックス		DNS 検索リスト（DNSSL）の 1 つ以上のドメイン名（サフィックス）を **Add**（追加）および設定します。サフィックスの最大長は 255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に（1 つずつ）追加するドメイン サフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されます。たとえば、DNS クライアントがサフィックスのない「quality」という名前の DNS クエリを送信しようとすると、ルーターはピリオドと DNS 検索リストの最初の DNS サフィックスを名前に追加して DNS クエリを送信します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの DNS クエリの完全修飾ドメイン名は「quality.company.com」になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは DNS ルックアップが成功するか（残りのサフィックスは無視されます）、ルーターがリストのすべてのサフィックスを試行するまで DNS サフィックスを試行します。 ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスを使用してファイアウォールを設定します。DNSSL オプションを受信する DNS クライアントは、その非修飾 DNS クエリでサフィックスを使用します。 ファイアウォールがリストの上から下の順に NDP ルーター通知で受信者に送信する DNS 検索リストのドメイン名（サフィックス）を最大 8 個設定できます。受信者は同じ順序でこれらを使用します。サフィックスを選択し、**Move Up**（上へ）または **Move Down**（下へ）を選択してサフィックスの順序を変更するか、不要になったサフィックスをリストから **Delete**（削除）します。
有効期間	**Aggregated Ethernet Interface**（**Ethernet** の集約インターフェイス）> **IPv6** > **DNS Support**（**DNS** サポート）（続き）	IPv6 DNS クライアントがルーター通知を受信した後に、DNS 検索リストのドメイン名（サフィックス）を使用できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > VLAN [ネットワーク > インターフェイス > VLAN]

VLAN インターフェイスは、ルーティング情報をレイヤー 3 ネットワーク (IPv4 および IPv6) に提供できます。VLAN インターフェイスには、1 つ以上のレイヤー 2 Ethernet ポート（「PA-7000 シリーズ レイヤー 2 インターフェイス」を参照）を追加できます。

VLAN インターフェイス設定	設定場所	の意味
インターフェイス名	**VLAN** インターフェイス	読み取り専用の **Interface Name**[インターフェイス名] フィールドにはvlanが設定されています。インターフェイスを識別する数値サフィックス（1 ~ 9,999）を隣のフィールドに入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile**（**Netflow** プロファイル）をクリックして新しいプロファイルを定義します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> NetFlow」を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
VLAN	**Ethernet Interface**（イーサネット インターフェイス）> **Config**（設定）	VLAN を選択するか、**VLAN** をクリックして新しい VLAN を定義します（「Network（ネットワーク）> VLANs」を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているVLANが解除されます。
仮想ルーター(VR)		インターフェイスに仮想ルーターを割り当てるか、**Virtual Router**（仮想ルーター）をクリックして新しい仮想ルーターを定義します（「Network（ネットワーク）> Virtual Routers（仮想ルーター）」を参照）。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
管理プロファイル	**Ethernet Interface**（イーサネット インターフェイス）>	**Management Profile**[管理プロファイル] – このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択しま

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
	Advanced（詳細）> **Other Info**（その他の情報）	す。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信されるパケットの最大転送単位（MTU）をバイト数で入力します（範囲は 576 ~ 9,192、デフォルトは 1,500）。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファイアウォールが送信元にパケットが大きすぎることを示す *ICMP* フラグメント要求メッセージを返します。
TCP MSS の調整		ヘッダーのバイト数に対応できるようにインターフェイスの MTU バイト サイズ以内の値で最大セグメント サイズ（MSS）を調整する場合は選択します。MTUバイトサイズとMSS調整サイズはMSSバイトサイズと等しい値になり、これはIPによって異なります。 • **IPv4 MSS Adjustment Size (IPv4 MSS調整サイズ)** — 範囲は40 ~ 300、デフォルトは40です。 • **IPv6 MSS Adjustment Size (IPv6 MSS調整サイズ)** — 範囲は60 ~ 300、デフォルトは60です。 ネットワークを通る**tunnel**[トンネル] のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。 カプセル化によりヘッダーが延長されるので、MSS調整サイズはMPLSヘッダーやVLANタグを持つトンネルトラフィックよりも大きく設定しておくと便利です。
IPアドレス MAC アドレス インターフェイス	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **ARP Entries**（**ARP** エントリ）	1 つ以上のスタティック アドレス解決プロトコル (ARP) エントリを追加するには、**Add**[追加] をクリックし、IP アドレスとそれに関連付けられたハードウェア (メディア アクセス制御、略称 MAC) のアドレスを入力して、ハードウェア アドレスにアクセスできるレイヤー 3 インターフェイスを選択します。エントリを削除するには、エントリを選択して **Delete**[削除] をクリックします。静的 ARP エントリによって、指定したアドレスの ARP 処理が減り、中間者攻撃が防止されます。
IPv6 アドレス MAC アドレス	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **ND Entries**（**ND** エントリ）	NDP（Neighbor Discovery Protocol）のネイバー情報を指定するには、**Add**（追加）をクリックし、ネイバーの IPv6 アドレスと MAC アドレスを入力します。
NDP プロキシの有効化	**Ethernet Interface**（イーサネッ	選択すると、インターフェイスで NDP (Neighbor Discovery Protocol) プロキシが有効になります。ファイアウォールは、このリストの IPv6 アドレスの MAC アドレスを要求する ND パケットに応答します。ND

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
	ト インターフェイス）> **Advanced**（詳細）> **NDP Proxy**（**NDP** プロキシ）	に対する応答として、ファイアウォールは、そのインターフェイス独自の MAC アドレスを送信し、基本的には、これらのアドレス宛のパケットを要求します。 （推奨）NPTv6 (Network Prefix Translation IPv6) を使用する場合は、NDPプロキシを有効化します。 **Enable NDP Proxy**[NDPプロキシの有効化] を選択した場合、フィルタ条件を入力しフィルタを適用（緑色の矢印をクリック）することで、膨大な**Address**[アドレス] のエントリから絞り込みを行うことができます。
アドレス		1つ以上のIPv6アドレス、IP範囲、IPv6サブネット、またはファイアウォールがNDPプロキシとして機能するアドレスオブジェクトを入力する場合は**Add**[追加] をクリックします。これらのアドレスの 1 つは、NPTv6 の送信元変換のアドレスと同じであることが理想的です。アドレスの順序は問題になりません。 アドレスがサブネットワークの場合、ファイアウォールはサブネットのすべてのアドレスに対して ND 応答を送信します。したがって、ファイアウォールの IPv6 ネイバーも追加し、**Negate**（除外）をクリックして、これらの IP アドレスに応答しないようファイアウォールに指示設定することをお勧めします。
Negate		あるアドレスに対して**Negate**[除外] チェック ボックスをオンにすると、NDPプロキシは、そのアドレスを拒否するようになります。Negate は、指定した IP アドレス範囲または IP サブネットの一部に対して実行できます。
設定	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**	Settings (設定) を選択して DDNS フィールドを設定できるようにします。
Enable [有効化]		インターフェースで DDNS を有効化します。初めに DDNS を有効化してから設定を行う必要があります。（DDNS の設定が終わっていない場合は有効化せずに保存し、部分的な設定を保持することができます）
更新間隔（日数）		FQDN にマッピングされた IP アドレスを更新するためにファイアウォールが DDNS サーバーに送信する更新間隔（日数）を入力します（範囲は1～30、デフォルトは 1）。 また、ファイアウォールは*DHCP* サーバーからインターフェイスの新しい *IP* アドレスを受診した際も *DDNS* を更新します。
証明書プロファイル		DDNS サービスを検証するために作成した（あるいは新しく作成する）証明書プロファイルを選択します。DDNS サービスは、認証局（CA）が署名した証明書をファイアウォールに提供します。
ホスト名		DDNS サーバーに登録されたインターフェイスのホスト名（例：host123.domain123.com、or host123）を入力します。DNS がドメイン名として許可している有効な文字を使った構文になっている

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
		ことを確認する以外、ファイアウォールはホスト名の検証を行いません。
ベンダー		DDNS サービスをこのインターフェイスに提供する DDNS ベンダー（およびバージョン番号）を選択します： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** ファイアウォールが特定の日で失効すると示唆する *DDNS* サービスの古いバージョンを選択する場合、新しいバージョンに移動させます。 ベンダー名に続く**Name** (名前)および**Value** (値)フィールドは、ベンダー固有のものです。ファイアウォールが DDNS サービスに接続するために使用するパラメーターを示す読み取り専用フィールドもあります。DDNS サービスプロバイダーが提供するパスワード、DDNS サーバーからの応答がない場合にファイアウォールが使用するタイムアウトなど、他のフィールドを設定します。
IPv4 タブ - IP		インターフェイスで設定した IPv4 アドレスを追加し、それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー（ベンダー）に登録されています。
IPv6 タブ - IPv6	**Ethernet Interface**（イーサネット インターフェイス）> **Advanced**（詳細）> **DDNS**(cont)	インターフェイスで設定した IPv6 アドレスを追加し、それを選択します。選択されたすべての IP アドレスは DDNS プロバイダー（ベンダー）に登録されています。
ランタイム情報の表示		DDNS 登録を表示します：DDNS プロバイダー、解決された FQDN、マッピングされた IPアドレス（アスタリスク（*）はプライマリ IP アドレスを示します）。トラブルシューティングを目的として、各 DDNS プロバイダーにはホスト名の更新状態を示す独自の返却コードおよび返却日が必要になります。
IPv4 アドレスの場合		
タイプ	**Ethernet Interface**（イーサネット インターフェイス）> **IPv4**	IPv4 アドレス タイプをインターフェイスに割り当てる方法を選択します。 • **Static**[静的] – IP アドレスを手動で指定する必要があります。 • **DHCP Client**[DHCP クライアント] – インターフェイスが DHCP (Dynamic Host Configuration Protocol) クライアントとして機能し、ダイナミックに割り当てられた IP アドレスを受信できます。 高可用性（*HA*）アクティブ/アクティブ構成のファイアウォールは、*DHCP* クライアントをサポートしません。

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
		選択した IP アドレス方式に応じて、タブに表示されるオプションは異なります。
• IPv4 アドレス **Type**[タイプ] = 静的		
ip	**Ethernet Interface**（イーサネット インターフェイス）> **IPv4**	**Add**[追加] をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワーク マスクを指定します。 • CIDR（Classless Inter-Domain Routing）表記法の *ip_address/mask* の形式（例: 192.168.2.0/24）でエントリを入力します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • タイプが **IP netmask**（**IP** ネットマスク）のアドレス オブジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、システムが使用する転送情報ベース (FIB) によって決まります。 不要になった IP アドレスを **Delete**（削除）します。
IPv4 アドレス **Type**[タイプ] = **DHCP**		
Enable [有効化]	**Ethernet Interface**（イーサネット インターフェイス）> **IPv4**	インターフェイスの DHCP クライアントを有効化する場合に選択します。
サーバー提供のデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成		DHCP サーバーによって提供されるデフォルト ゲートウェイを指し示すデフォルト ルートを自動的に作成する場合に選択します。
ホスト名の送信		ファイアウォール（DHCP クライアントとして）にインターフェイスのホスト名（Option 12）を DHCP サーバーに送信させる設定を行う場合に選択します。デフォルトで Send Hostname (ホスト名の送信) を行う場合、ファイアウォールのホスト名がホスト名フィールドで選択されます。その名前を送信するか、カスタム ホスト名（大文字および小文字、数字、ピリオド、ハイフン、アンダースコアを含む最長 64 文字）を入力します。
デフォルト ルート メトリック		ファイアウォールと DHCP サーバー間のルートについては、必要に応じてルート メトリック（優先順位レベル）を入力し、それをデフォルト ルートに関連付けて、パスの選択で使用します（範囲は 1 ~ 65,535、デフォルトはなし）。数値が小さいほど優先度が高くなります。
DHCP クライアント ランタイム情報の表示		DHCP のリース状態、ダイナミック IP アドレス割り当て、サブネット マスク、ゲートウェイ、サーバー設定（DNS、NTP、ドメイン、WINS、NIS、POP3、および SMTP）など、DHCP サーバーから受信したすべての設定を表示する場合に選択します。

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
IPv6 アドレスの場合		
インターフェースでの IPv6 の有効化	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6**	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID as host portion**[ホスト部分にインターフェイス ID を使用] オプションを選択すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。

アドレス	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6 (cont)**	**Add**[追加] をクリックして、IPv6 アドレスごとに以下のパラメータを設定します。
		• **Address**[アドレス] — IPv6 アドレスとプレフィックス長を入力します (例: 2001:400:f00::1/64)。既存のIPv6アドレスオブジェクトを選択することや、**Address**[アドレス] をクリックしてアドレスオブジェクトを作成することもできます。
		• **Enable address on interface**（インターフェイス上のアドレスを有効にする）— インターフェイスの IPv6 アドレスを有効にする場合に選択します。
		• **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用）— IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。
		• **Anycast**（エニーキャスト）— 最も近いノードを経由するルーティングを含める場合に選択します。
		• **Send RA**（**RA** の送信）— この IP アドレスのルーター通知（RA）を有効にする場合に選択します。このオプションを選択する場合、インターフェイスでグローバルに **Enable Router Advertisement**（ルーター通知を有効にする）必要もあります。RA の詳細は、「ルーター通知を有効にする」を参照してください。
		残りのフィールドは、RA を有効にした場合にのみ適用されます。
		  • **Valid Lifetime**（有効なライフタイム）— ファイアウォールがアドレスを有効とみなす時間（秒）です。有効なライフタイムは、**Preferred Lifetime**[優先ライフタイム] 以上でなければなりません。デフォルトは2,592,000 です。
		  • **Preferred Lifetime**（優先ライフタイム）— 有効なアドレスが優先される時間（秒）です。この時間内は、ファイアウォールがこのアドレスを使用してトラフィックを送受信できます。優先ライフタイムの期限後は、ファイアウォールがこのアドレスを使用して新しい接続を確立することはできませんが、既存の接続は **Valid Lifetime**（有効なライフタイム）を超えるまで有効です。デフォルトは 604,800 です。
		  • **On-link**（オンリンク）— 通知されたプレフィックス内に IP アドレスがあるシステムにルーターなしで到達可能な場合に選択します。

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
		• **Autonomous**（自律型）– 通知されたプレフィックスとインターフェイス ID を組み合わせて、システムが IP アドレスを独自に作成できる場合に選択します。
重複アドレス検出を有効にする	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **Address Resolution**（アドレス解決）	重複アドレス検出（DAD）を有効にする場合に選択します。これにより **DAD Attempts**（試行回数）を指定できます。
DAD 試行回数		ネイバー要請間隔 (**NS Interval (NS** 間隔)) の内にDADを試行する回数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この回数を超えるとネイバーに障害があるとみなされます。
到達可能時間		クエリと応答が正常に行われた後引き続きネイバーに到達可能な時間（秒）を指定します（範囲は 1 ~ 36,000、デフォルトは 30）。
NS 間隔 (ネイバー要請間隔)		DADの試行秒数を指定します（範囲は 1 ~ 10、デフォルトは 1）。この秒数を超えると障害があるとみなされます。
NDP モニタリングの有効化		Neighbor Discovery Protocol のモニタリングを有効にする場合に選択します。有効になっていると、NDP（Features（機能）列の ）を選択し、ファイアウォールで検出されたネイバーの IPv6 アドレス、対応する MAC アドレスおよび User-ID などの情報を（ベストケースベースで）表示できます。
ルーター通知を有効にする	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6** > **Router Advertisement**（ルーター通知）	IPv6 インターフェイスのネイバー検出を指定して、このセクションの他のフィールドを設定する場合に選択します。ルーター通知（RA）メッセージを受信する IPv6 DNS クライアントは、この情報を使用します。 RA により、ファイアウォールが、スタティックに設定されていない IPv6 ホストのデフォルト ゲートウェイとして機能し、ホストにアドレス設定の IPv6 プレフィックスを提供できます。別の DHCPv6 サーバーをこの機能と併用すると、DNS および他の設定をクライアントに提供できます。 これはインターフェイスのグローバル設定です。IP アドレスごとに RA オプションを設定する場合は、アドレス を IP アドレス テーブルに **Add**（追加）して設定します。IP アドレスに RA オプションを設定する場合は、インターフェイスの **Enable Router Advertisement**（ルーター通知を有効にする）必要があります。
最小間隔 (秒)		ファイアウォールが送信する RA 間の最小間隔（秒）を指定します（範囲は 3 ~ 1,350、デフォルトは 200）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
最大間隔 (秒)		ファイアウォールが送信する RA 間の最大間隔（秒）を指定します（範囲は 4 ~ 1,800、デフォルトは 600）。ファイアウォールは、設定した最小値と最大値の間のランダムな間隔で RA を送信します。
ホップ制限		クライアントに適用する、送信パケットのホップ制限を指定します（範囲は 1 ~ 255、デフォルトは 64）。ホップ制限を指定しない場合は **0** を入力します。

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
リンク MTU		クライアントに適用するリンクの最大転送単位 (MTU) を指定します。リンクMTUを指定しない場合は **unspecified** (指定しない) を選択します (範囲は 1,280 ~ 9,192、デフォルトは unspecified) 。
到達可能時間 (ミリ秒)		到達可能確認メッセージを受信後ネイバーに到達可能であると想定するためにクライアントが使用する到達可能時間 (ミリ秒) を指定します。到達可能時間を指定しない場合は **unspecified** (指定しない) を選択します (範囲は 0 ~ 3,600,000、デフォルトはunspecified) 。
リトランスミッション時間 (ミリ秒)		ネイバー要請メッセージを再送信するまでにクライアントが待機する時間を決定するリトランスミッション タイマーを指定します。リトランスミッション時間を指定しない場合は **unspecified** (指定しない) を選択します (範囲は 0 ~ 4,294,967,295、デフォルトはunspecified) 。
ルーターの有効期間 (秒)		クライアントがファイアウォールをデフォルトゲートウェイとして使用する時間を秒単位で指定します (範囲は 0 ~ 9,000、デフォルトは 1,800) 。0 は、ファイアウォールがデフォルト ゲートウェイではないことを示します。有効期間が過ぎると、クライアントがそのデフォルト ルーター リストからファイアウォール エントリを削除して、別のルーターをデフォルト ゲートウェイとして使用します。
ルーター設定		ネットワーク セグメントに複数の IPv6 ルーターがある場合は、クライアントがこのフィールドを使用して優先ルーターを選択します。セグメントの他のルーターとの比較において、RA が通知するファイアウォール ルーターの優先度を **High**、**Medium** (デフォルト)、**Low** の中から選択します。
管理された設定		アドレスを DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
その他の設定		他のアドレス情報 (DNS 関連の設定など) を DHCPv6 経由で使用できることをクライアントに示す場合に選択します。
整合性チェック	**Ethernet Interface** (イーサネット インターフェイス) > **IPv6** > **Router Advertisement** (ルーター通知)	他のルーターから送信された RA がリンク上で一貫した情報を通知していることをファイアウォールで確認する場合に選択します。ファイアウォールでは、システム ログの不一致が記録されます。タイプは **ipv6nd** です。
ルーター通知に DNS 情報を含める	**Ethernet Interface** (イーサネット インターフェイス) > **IPv6** > **DNS Support** (**DNS** サポート)	ファイアウォールで DNS 情報をこの IPv6 VLAN インターフェイスからの NDP ルーター通知に含めて送信する場合に選択します。この表の他の DNS Support (DNS サポート) フィールドは、このオプションを選択した場合にのみ表示されます。
SERVER		ファイアウォールでこの IPv6 VLAN インターフェイスからの NDP ルーター通知に含めて送信する 1 つ以上の再帰 DNS (RDNS) サーバー アドレスを **Add** (追加) します。RDNS サーバーは、ルート DNS

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
		サーバーと権限のある DNS サーバーに一連の DNS ルックアップ要求を送信し、最終的に DNS クライアントに IP アドレスを提供します。 最大 8 個の RDNS サーバーを設定し、ファイアウォールでそれらを NDP ルーター通知に含めて受信者に送信できます（設定の上から下の順に送信します）。その後、受信者は同じ順序でこれらを使用できます。サーバーの順序を変更するには、サーバーを選択して **Move Up**（上へ）移動したり **Move Down**（下へ）移動したりします。サーバーが必要なくなったら、そのサーバーをリストから **Delete**（削除）します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後に、RDNS サーバーを使用してドメイン名を解決できる最大秒数を入力します（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。
サフィックス		DNS 検索リスト（DNSSL）の 1 つ以上のドメイン名（サフィックス）を **Add**（追加）および設定します。サフィックスの最大長は 255 バイトです。 DNS 検索リストは、DNS クライアント ルーターが DNS クエリに名前を入力する前に非修飾ドメイン名に（1 つずつ）追加するドメインサフィックスのリストです。これにより、DNS クエリで完全修飾ドメイン名が使用されます。たとえば、サフィックスなしの「quality」という名前の DNS クエリを DNS クライアントが送信しようとしています。この場合、ルーターはピリオドと、DNS 検索リストの 1 番目の DNS サフィックスを名前に付加し、DNS クエリを転送します。リストの最初の DNS サフィックスが「company.com」の場合、ルーターの DNS クエリの完全修飾ドメイン名は「quality.company.com」になります。 DNS クエリに失敗すると、ルーターはリストの 2 番目の DNS サフィックスを非修飾名に追加して、新しい DNS クエリを送信します。ルーターは DNS ルックアップが成功するか（残りのサフィックスは無視されます）、ルーターがリストのすべてのサフィックスを試行するまで DNS サフィックスを試行します。 ネイバー検出 DNSSL オプションで DNS クライアント ルーターに提供するサフィックスにより、ファイアウォールを設定します。DNSSL オプションを受信する DNS クライアントは非修飾 DNS クエリでそのサフィックスを使用します。 DNS 検索リストに対して最大 8 個のドメイン名（サフィックス）を設定し、ファイアウォールでそれらを NDP ルーター通知に含めて受信者に送信できます（設定の上から下の順に送信します）。その後、受信者は同じ順序でこれらのアドレスを使用できます。サフィックスを選択し、**Move Up**（上へ）または **Move Down**（下へ）を選択して順序を変更するか、不要になったサフィックスをリストから **Delete**（削除）します。
有効期間		IPv6 DNS クライアントがルーター通知を受信した後に、DNS 検索リストのドメイン名（サフィックス）を使用できる最大秒数を入力しま

© 2019 Palo Alto Networks, Inc.

VLAN インターフェイス設定	設定場所	の意味
		す（範囲は最大間隔（秒）の値からその 2 倍までで、デフォルトは 1,200 です）。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > Loopback [ネットワーク > インターフェイス > ループバック]

以下のフィールドを使用して、ループバック インターフェイスを設定します。

ループバック インターフェイス設定	設定場所	の意味
インターフェイス名	ループバック インターフェイス	読み取り専用の**Interface Name**[インターフェイス名] フィールドには**loopback**が設定されています。インターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile** (**Netflow** プロファイル) をクリックして新しいプロファイルを定義します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow」を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
仮想ルーター(VR)	**Loopback Interface** (ループバック インターフェイス) > **Config** (設定)	インターフェイスに仮想ルーターを割り当てるか、**Virtual Router** (仮想ルーター) をクリックして新しい仮想ルーターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
管理プロファイル	**Ethernet Interface** (イーサネット インターフェイス) > **Advanced** (詳細) > **Other Info** (その他の情報)	**Management Profile**[管理プロファイル] – このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信するパケットの最大転送単位 (MTU) をバイト数で入力します (576 ~ 9,192、デフォルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファ

© 2019 Palo Alto Networks, Inc.

ループバック インターフェイス設定	設定場所	の意味
		イアウォールが送信元にパケットが大きすぎることを示す *ICMP* フラグメント要求メッセージを返します。
TCP MSS の調整		ヘッダーのバイト数に対応できるようにインターフェイスの MTU バイト サイズ以内の値で最大セグメント サイズ (MSS) を調整する場合は選択します。MTUバイトサイズとMSS調整サイズはMSSバイトサイズと等しい値になり、これはIPによって異なります。 • **IPv4 MSS Adjustment Size**[IPv6 MSS調整サイズ] — 範囲は40 ~ 300、デフォルトは40です。 • **IPv6 MSS Adjustment Size**[IPv6 MSS調整サイズ] — 範囲は60 ~ 300、デフォルトは60です。 ネットワークを通る**tunnel**[トンネル] のMSSを小さくする必要がある場合はこれらの設定を行ってください。フラグメント化を行わないパケットのバイト数がMSSよりも大きい場合、この設定を行うことでサイズが調整されるようになります。 カプセル化によりヘッダーが延長されるので、MSS調整サイズはMPLSヘッダーやVLANタグを持つトンネルトラフィックよりも大きく設定しておくと便利です。
IPv4 アドレスの場合		
ip	**Loopback Interface** > **IPv4**	**Add**[追加] をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワーク マスクを指定します。 • /32 のサブネット マスクで IPv4 アドレスを入力します。例: 192.168.2.1/32。/32 サブネット マスクのみがサポートされています。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • **Adress**[アドレス] をクリックし、タイプが **IP netmask**[IP ネットマスク] のアドレスオブジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、システムが使用する転送情報ベース (FIB) によって決まります。 IP アドレスを削除するには、アドレスを選択して **Delete**[[削除]] をクリックします。
IPv6 アドレスの場合		
インターフェースでの IPv6 の有効化	**Loopback Interface** > **IPv6**	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID		64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID**

© 2019 Palo Alto Networks, Inc.

ループバック インターフェイス設定	設定場所	の意味
		as host portion[ホスト部分にインターフェイス ID を使用] オプションを選択すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス		**Add**[追加] をクリックして、IPv6 アドレスごとに以下のパラメータを設定します。 • **Address**[アドレス] – IPv6 アドレスとプレフィックス長を入力します (例: 2001:400:f00::1/64)。既存のIPv6アドレスオブジェクトを選択することや、**Address**[アドレス] をクリックしてアドレスオブジェクトを作成することもできます。 • **Enable address on interface**（インターフェイス上のアドレスを有効にする）– インターフェイスの IPv6 アドレスを有効にする場合に選択します。 • **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用）– IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。 • **Anycast**（エニーキャスト）– 最も近いノードを経由するルーティングを含める場合に選択します。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > Tunnel [ネットワーク > インターフェイス > トンネル]

以下のフィールドを使用して、トンネル インターフェイスを設定します。

トンネル インターフェイス設定	設定場所	の意味
インターフェイス名	トンネルインターフェイス	読み取り専用の**Interface Name**[インターフェイス名] フィールドには**tunnel**が設定されています。インターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント		インターフェイスの説明 (省略可) を入力します。
Netflowプロファイル		入力インターフェイスを通過する単向性の IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、**Netflow Profile** (**Netflow** プロファイル) をクリックして新しいプロファイルを定義します (「Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow」を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
仮想ルーター(VR)	**Ethernet Interface** (イーサネット インターフェイス) > **Config** (設定)	インターフェイスに仮想ルーターを割り当てるか、**Virtual Router** (仮想ルーター) をクリックして新しい仮想ルーターを定義します (「Network (ネットワーク) > Virtual Routers (仮想ルーター)」を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)		ファイアウォールが複数の仮想システムをサポートし、その機能が有効の場合は、インターフェイスの仮想システム (vsys) を選択するか、**Virtual System**[仮想システム] リンクをクリックして新しい vsys を定義します。
セキュリティゾーン		インターフェイス用のセキュリティゾーンを選択するか、**Zone**[ゾーン] をクリックして新しいゾーンを定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。
管理プロファイル	**Ethernet Interface** (イーサネット インターフェイス) > **Advanced** (詳細) > **Other Info** (その他の情報)	**Management Profile**[管理プロファイル] – このインターフェイスを介したファイアウォールの管理に使用できるプロトコル (SSH、Telnet、HTTP など) を定義するプロファイルを選択します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているプロファイルが解除されます。
MTU		このインターフェイスで送信するパケットの最大転送単位 (MTU) をバイト数で入力します (576 ~ 9,192、デフォルトは 1,500)。ファイアウォールの両側のマシンが Path MTU Discovery (PMTUD) を実行し、インターフェイスが MTU を超えるパケットを受信すると、ファ

© 2019 Palo Alto Networks, Inc.

トンネル インターフェイス設定	設定場所	の意味
		イアウォールが送信元にパケットが大きすぎることを示す *ICMP* フラグメント要求メッセージを返します。
IPv4 アドレスの場合		
ip	**Ethernet Interface**（イーサネット インターフェイス）> **IPv4**	**Add**[追加] をクリックし、以下のいずれかの手順を実行して、インターフェイスのスタティック IP アドレスとネットワーク マスクを指定します。 • CIDR（Classless Inter-Domain Routing）表記法の ip_address/mask の形式（例: 192.168.2.0/24）でエントリを入力します。 • タイプが **IP netmask**[IP ネットマスク]の既存のアドレス オブジェクトを選択します。 • **Adress**[アドレス] をクリックし、タイプが **IP netmask**[IP ネットマスク] のアドレスオブジェクトを作成します。 インターフェイスに対して複数の IP アドレスを入力できます。IP アドレスの最大数は、システムが使用する転送情報ベース (FIB) によって決まります。 IP アドレスを削除するには、アドレスを選択して **Delete**[[削除]] をクリックします。
IPv6 アドレスの場合		
インターフェースでの IPv6 の有効化	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6**	このインターフェイスの IPv6 アドレスを有効にする場合に選択します。
インターフェイス ID	**Ethernet Interface**（イーサネット インターフェイス）> **IPv6**	64 ビット拡張一意識別子 (EUI-64) を 16 進数形式で入力します (例: 00:26:08:FF:FE:DE:4E:29)。このフィールドを空白のままにすると、ファイアウォールが、物理インターフェイスの MAC アドレスから生成された EUI-64 を使用します。アドレスの追加時に **Use interface ID as host portion**[ホスト部分にインターフェイス ID を使用] オプションを選択すると、ファイアウォールがそのアドレスのホスト部分にインターフェイス ID を使用します。
アドレス		**Add**[追加] をクリックして、IPv6 アドレスごとに以下のパラメータを設定します。 • **Address**[アドレス] — IPv6 アドレスとプレフィックス長を入力します (例: 2001:400:f00::1/64)。既存のIPv6アドレスオブジェクトを選択することや、**Address**[アドレス] をクリックしてアドレスオブジェクトを作成することもできます。 • **Enable address on interface**（インターフェイス上のアドレスを有効にする）— インターフェイスの IPv6 アドレスを有効にする場合に選択します。 • **Use interface ID as host portion**（ホスト部分にインターフェイス **ID** を使用）— IPv6 アドレスのホスト部分に **Interface ID**（インターフェイス **ID**）を使用する場合に選択します。

© 2019 Palo Alto Networks, Inc.

トンネル インターフェイス設定	設定場所	の意味
		• **Anycast**（エニーキャスト）– 最も近いノードを経由するルーティングを含める場合に選択します。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > SD-WAN [ネットワーク > インターフェイス > SD-WLAN]

仮想 SD-WAN インターフェイスを作成し、同じ宛先の 1 個以上の物理イーサネット インターフェイス メンバーを追加します。

SD-WAN インターフェイス設定	
インターフェイス名	読み取り専用の **Interface Name** (インターフェイス名) フィールドには**sdwan**が設定されています。仮想 SD-WAN インターフェイスを特定する数値サフィックス (1 ~ 9,999) を隣のフィールドに入力します。
コメント	インターネット または 米国西部のハブなど、わかりやすくインターフェイスの説明を入力します。コメントを使用すると、ログやレポートで自動生成された名前を解読するよりも、インターフェイスを特定しやすくなります。
Netflowプロファイル	入口インターフェイスを通過する単方向 IP トラフィックを NetFlow サーバーにエクスポートする場合は、サーバー プロファイルを選択するか、新しい **Netflow Profile** (プロファイル) を定義します (Device (デバイス) > Server Profiles (サーバー プロファイル) > NetFlow を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているNetFlowサーバーが解除されます。
Config Tab (設定タブ)	
仮想ルーター(VR)	仮想ルーターをインターフェイスに割り当てるか、新しい **Virtual Router** (仮想ルーター - **VR**) を定義します (Network (ネットワーク) > Virtual Router (仮想ルーター - VR)を参照)。**None**[なし] を選択すると、現在インターフェイスに割り当てられているルーターが解除されます。
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートし、その機能が有効になっている場合は、インターフェイスに仮想システム(vsys) を選択するか、新しい 仮想システム**(vsys)**を定義します。
セキュリティゾーン	インターフェイスのセキュリティゾーンを選択するか、新しい **Zone** (ゾーン)を定義します。**None**[なし] を選択すると、現在インターフェイスに割り当てられているゾーンが解除されます。ブランチから同じ宛先へのすべてのパスに同じセキュリティ ポリシー ルールが適用されるには、仮想SD-WANインターフェイスおよび仮想SD-WANのすべてのインターフェイス メンバーは、同じセキュリティ ゾーンに配置する必要があります。
Advanced Tab (詳細タブ)	
インターフェイス	この仮想 SD-WAN インターフェイスを構成する レイヤー3 イーサネット インターフェイス (Direct Internet Access [DIA] 用) または仮想 VPN トンネル インターフェイス (ハブ用) を選択します。ファイアウォールの仮想 ルーターは、この仮想 SD-WAN インターフェイスを使用して、SD-WAN トラフィックを DIA あるいはハブの場所にルーティングします。インターフェイスには異なるタグを付けることができます。ただし、複数のインターフェイスを入力する場合は、すべて同じタイプ (VPN トンネルまたは DIA) である必要があります。

© 2019 Palo Alto Networks, Inc.

Network > Zones [ネットワーク > ゾーン]

以下のトピックでは、ネットワークのセキュリティ ゾーンについて説明します。

確認すべき情報	以下を参照
セキュリティーゾーンの目的とは？	セキュリティ ゾーンの概要
セキュリティ ゾーンの設定で使用できるフィールドは?	セキュリティ ゾーンの構成要素
その他の情報をお探しですか？	インターフェイスやゾーンを用いたネットワークのセグメント化

セキュリティ ゾーンの概要

ファイアウォールの物理インターフェイスと仮想インターフェイスをグループ化し、ネットワークの特定のインターフェイスを通過するトラフィックを制御し、ログに記録するためセキュリティ ゾーンを利用します。ファイアウォールのインターフェースでトラフィックの処理を行う場合は、インターフェースをいずれかのセキュリティゾーンに割り当てる必要があります。ゾーンには同じタイプの複数のインターフェイスを割り当てることができますが（タップ、レイヤー 2、またはレイヤー 3 インターフェイスなど）、各インターフェイスは 1 つのゾーンにしか属せません。

ファイアウォールのポリシールールは、セキュリティーゾーンを使用してトラフィックの送信元と宛先を識別します。トラフィックはゾーン内を自由に流れますが、異なるゾーン間において許可するセキュリティ ポリシー ルールが定義されない限り流れません。インターゾーン トラフィックを許可または拒否するには、セキュリティ ポリシー ルールで送信元ゾーンと宛先ゾーン（インターフェイスではない）を参照する必要があります。また、それらのゾーンは同じタイプでなければなりません。たとえば、ある レイヤー 2の ゾーンからのトラフィックのうちセキュリティ ポリシー ルールが許可または拒否できるのは、別のレイヤー 2の ゾーンに向かうもののみです。

セキュリティ ゾーンの構成要素

セキュリティ ゾーンを定義するには、**Add**（追加）をクリックし、以下の情報を指定します。

セキュリティ ゾーン設定	の意味
氏名	ゾーン名（最大31文字）を入力します。この名前は、セキュリティ ポリシーの定義時とインターフェイスの設定時にゾーンのリストに表示されます。名前の大文字と小文字は区別されます。また、仮想ルーター内で一意の名前にする必要があります。文字、数字、スペース、ハイフン、ピリオド、およびアンダースコアのみを使用してください。
場所	このフィールドは、ファイアウォールが複数の仮想システム (vsys) をサポートし、その機能が有効な場合にのみ表示されます。このゾーンが適用されているvsysを選択してください。

© 2019 Palo Alto Networks, Inc.

セキュリティ ゾーン設定	の意味
タイプ	ゾーン タイプ（**Tap**（タップ）、**Virtual Wire**（バーチャル ワイヤー）、**Layer2**（レイヤー 2）、**Layer3**（レイヤー 3）、**External**（外部）、または **Tunnel**（トンネル））を選択し、ゾーンに割り当てられていないそのタイプの **Interfaces**（インターフェイス）をすべて表示します。Layer 2 [レイヤー 2] およびLayer 3 [レイヤー 3] ゾーン タイプでは、該当タイプの イーサネットインターフェイスとサブインターフェイスがすべて表示されます。ゾーンに割り当てたいインターフェイスを**Add**[追加]します。 1つのファイアウォール上の、複数の仮想システム間のトラフィックをコントロールする場合に外部ゾーンを使用します。複数の仮想システムをサポートするファイアウォールで、**Multi Virtual System Capability**[マルチ仮想システム機能] が有効化されている場合のみ表示されます。外部ゾーンの詳細は、「ファイアウォール内に残る VSYS 間トラフィック」を参照してください。 インターフェイスは、1つの仮想システムの1つのゾーンにのみ属することができます。
インターフェイス	このゾーンに1つ以上のインターフェイスを追加します。
ゾーン プロテクション プロファイル	このゾーンからの攻撃にファイアウォールが対応する方法を指定したプロファイルを選択します。新しいプロファイルを作成する手順については、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> Zone Protection（ゾーン プロテクション）」を参照してください。各ゾーンをゾーン プロテクション プロファイルで保護することがベストプラクティスになります。
パケット バッファ保護の有効化	パケット バッファ保護（Device (デバイス) > Setup (セットアップ) > Session (セッション)）をグローバルに設定し、各ゾーンに適用します。ファイアウォールは入力ゾーンのみにパケット バッファ保護を適用します。パケット バッファ保護はデフォルトで無効になっていますが、各ゾーンでパケット バッファ保護を有効化してファイアウォールのバッファを保護することがベストプラクティスになります。
ログ設定	ゾーン プロテクション ログを外部システムに転送するための Log Forwarding（ログ転送）プロファイルを選択します。 デフォルトと指定されたログ転送プロファイルがある場合は、新しいセキュリティ ゾーンを定義するときに、そのプロファイルがこのドロップダウン リストで自動的に選択されます。新しいセキュリティ ゾーンを設定するときに別の Log Forwarding（ログ転送）の選択を続行すると、このデフォルト設定をいつでもオーバーライドできます。新しいログ転送プロファイルを定義または追加する（およびプロファイルをデフォルトに指定してこのドロップダウン リストで自動選択されるようにする）には、**New**（新規）をクリックします（「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照）。 *Panorama* テンプレートのゾーンを設定している場合は、*Log Setting*（ログ設定）ドロップダウン リストに一覧表示されるのは共有されたログ転送プロファイルのみです。共有されていないプロファイルを指定するには、名前を入力する必要があります。
User-IDの有効化	IP アドレスからユーザー名へのマッピング（検出）を行うように User-ID™ を設定した場合は、**Enable User Identification (ユーザー ID を有効化)**してマッピ

© 2019 Palo Alto Networks, Inc.

セキュリティ ゾーン設定	の意味
	ング情報をこのゾーンのトラフィックに適用することがベストプラクティスになります。このオプションを無効にした場合、ゾーン内のトラフィックのユーザーマッピング情報がファイアウォール ログ、レポート、およびポリシーから除外されます。 デフォルト設定では、このオプションを選択した場合、ファイアウォールは、ゾーンのすべてのサブネットワークのトラフィックにユーザーマッピング情報を適用します。情報の適用先をゾーン内の特定のサブネットワークに制限するには、**Include List**[許可リスト]と**Exclude List**[除外リスト]を使用します。 *User-ID* は信頼されたゾーンでのみ有効にしてください。外部の信頼されていないゾーン (インターネットなど) で *User-ID* およびクライアントによるプローブを有効にすると、保護されたネットワークの外にプローブが送信される可能性があります。これにより、*User-ID* エージェントのサービス アカウント名、ドメイン名、暗号化されたパスワード ハッシュの情報が漏洩し、保護されているリソースに攻撃者が不正アクセスできるようになる場合があります。 *User-IDがゾーンに対して検出を実行するのは、User-IDがモニターするネットワーク範囲内にゾーンが含まれる場合に限られます。ゾーンがこの範囲に含まれていない場合、たとえ Enable User Identification[ユーザーIDの有効化]* を選択しても、ファイアウォールはユーザーマッピング情報をゾーンのトラフィックに適用しません。詳細は、「ユーザー マッピングのサブネットワークの許可または除外」を参照してください。
User-ID ACL 許可リスト	デフォルトでは、このリストでサブネットワークを指定しない場合、ファイアウォールは、ログ、レポート、およびポリシーで使用するために、検出したユーザー マッピング情報をゾーンのすべてのトラフィックに適用します。 ユーザー マッピング情報の適用先をゾーン内の特定のサブネットワークに制限するには、サブネットワークごとに **Add**[追加] をクリックし、アドレス (またはアドレス グループ) オブジェクトを選択するか、IP アドレス範囲 (10.1.1.1/24 など) を入力します。**Include List (**許可リスト**)**はホワイトリストであるため、他のすべてのサブネットワークの除外は暗黙的に行われます。**Exclude List (**除外リスト**)**に追加する必要はありません。 **Exclude List**[除外リスト]にエントリを追加するのは、**Include List**[許可リスト]の一部のサブネットワークのユーザー マッピング情報を除外する場合のみです。たとえば、**Include List**[許可リスト]に 10.0.0.0/8 を追加し、**Exclude List**[除外リスト]に 10.2.50.0/22 を追加した場合、ファイアウォールは、10.2.50.0/22 を除く、10.0.0.0/8 のずべてのゾーン サブネットワークのユーザー マッピング情報を許可し、10.0.0.0/8 の外部のすべてのゾーン サブネットワークの情報を除外します。 *User-ID* がモニターするネットワーク範囲に含まれるサブネットワークのみを許可できます。詳細は、「ユーザー マッピングのサブネットワークの許可または除外」を参照してください。
User-ID ACL 除外リスト	**Include List** (許可リスト) の一部のサブネットワークのユーザー マッピング情報を除外するには、アドレス (またはアドレス グループ) オブジェクトを

© 2019 Palo Alto Networks, Inc.

セキュリティ ゾーン設定	の意味
	Add（追加）するか、除外するサブネットワークごとに IP アドレス範囲を入力します。 *Exclude List[*除外リスト*]*にエントリを追加したが、*Include List[*許可リスト*]*にはエントリを追加しない場合、ファイアウォールは、追加したサブネットワークだけではなく、ゾーン内のすべてのサブネットワークのユーザー マッピング情報を除外します。

© 2019 Palo Alto Networks, Inc.

Network > VLANs [ネットワーク > VLAN]

このファイアウォールでは、IEEE 802.1Q 標準に準拠する VLAN がサポートされています。ファイアウォールに定義されたレイヤー 2 インターフェイスをそれぞれ VLAN に関連付けることができます。同じ VLAN を複数のレイヤー 2 インターフェイスに割り当てることができますが、各インターフェイスは 1 つの VLAN にのみ属することができます。

VLAN 設定	の意味
氏名	VLAN 名（最大 31 文字）を入力します。この名前は、インターフェイスを設定するときに VLAN のリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
VLAN インターフェイス	トラフィックを VLAN の外部にルーティングできるようにするには、Network（ネットワーク）> Interfaces（インターフェイス）> VLAN を選択します。
インターフェイス	VLAN のファイアウォール インターフェイスを指定します。
スタティック MAC 設定	MAC アドレスが到達するために経由する必要のあるインターフェイスを指定します。これは、学習したインターフェイス対 MAC のマッピングよりも優先されます。

© 2019 Palo Alto Networks, Inc.

Network > Virtual Wires [ネットワーク > バーチャル ワイヤー]

ファイアウォールで 2 つのバーチャル ワイヤー インターフェイスを指定 (Network (ネットワーク) > Interfaces (インターフェイス) した後にバーチャル ワイヤーを定義するには、**Network** (ネットワーク) > **Virtual Wires** (バーチャル ワイヤー) を選択します。

バーチャル ワイヤー設定	の意味
バーチャル ワイヤー名	バーチャル ワイヤー名 (最大 **31** 文字) を入力します。この名前は、インターフェイスを設定するときにバーチャル ワイヤーのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
インターフェイス	表示されたリストから、バーチャル ワイヤー設定用の イーサネットインターフェイスを 2 つ選択します。リストには、バーチャル ワイヤー インターフェイス タイプで、他のバーチャル ワイヤーに割り当てられていないインターフェイスのみが表示されます。 バーチャル ワイヤー インターフェイスの詳細は、「バーチャル ワイヤー インターフェイス」を参照してください。
タグを許可	バーチャルワイヤーで許可されるトラフィックのタグ番号 (0 ~ 4094) またはタグ番号の範囲 (タグ1 ~ タグ2) を入力します。タグ値 0 (デフォルト) は、タグのないトラフィックを示します。複数のタグまたはタグ範囲はコンマで区切ります。除外されたタグ値を持つトラフィックは廃棄されます。 受信パケットまたは送信パケット上でタグ値が変更されることはありません。 バーチャル ワイヤー サブインターフェイスを使用する場合に **Tag Allowed**[タグを許可] リストを指定すると、リスト内のタグを持つすべてのトラフィックが親バーチャル ワイヤーに分類されます。バーチャル ワイヤー サブインターフェイスでは、親の **Tag Allowed**[タグを許可] リストに存在しないタグを使用する必要があります。
マルチキャスト ファイアウォール設定	セキュリティ ルールをマルチキャスト トラフィックに適用できるようにする場合に選択します。この設定が有効になっていないと、マルチキャスト トラフィックがバーチャル ワイヤー全体に転送されます。
リンク状態パス スルー	リンクのダウン状態が検出されたときにバーチャル ワイヤー ペアのもう一方のインターフェイスをダウンさせる場合に選択します。このオプションを無効化した場合あるいは選択しない場合、接続状況はバーチャルワイヤーを通じて反映されません。

© 2019 Palo Alto Networks, Inc.

Network > Virtual Routers [ネットワーク > 仮想ルーター]

手動で定義したスタティックルートを使用するか、あるいはレイヤー3のルーティングプロトコルに参加することで他のサブネットへのルートを取得する場合は、ファイアウォールに仮想ルーターを設定しておく必要があります。ファイアウォールに定義されたレイヤー 3 インターフェイス、ループバック インターフェイス、および VLAN インターフェイスはそれぞれ、仮想ルーターに関連付けられている必要があります。各インターフェイスは、1つの仮想ルーターにのみ属することができます。

仮想ルーターを定義するには、一般的な設定のほかに、ネットワークで必要とされるスタティック ルートまたはダイナミック ルーティング プロトコルの組み合わせが必要になります。また、ルート再配信やECMPなど、その他の機能を設定することも可能です。

確認すべき情報	以下を参照
仮想ルーターに必要な要素	仮想ルーターの一般設定
設定:	静的ルート ルート再配信 RIP OSPF OSPFv3IPv6 BGP IP マルチキャスト ECMP
仮想ルーターに関する情報を表示する。	仮想ルーターの詳細ランタイム状態
その他の情報をお探しですか？	ネットワーク

仮想ルーターの一般設定

- Network > Virtual Routers > Router Settings > General [ネットワーク > 仮想ルーター > ルーター設定 > 全般]

すべての仮想ルーターでは、以下の表に従ってレイヤー 3 インターフェイスと管理距離のメトリックを割り当てる必要があります。

仮想ルーターの一般設定	の意味
氏名	仮想ルータを表す名前を指定します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。

© 2019 Palo Alto Networks, Inc.

仮想ルーターの一般設定	の意味
インターフェイス	仮想ルーターに含めるインターフェイスを選択します。これにより、仮想ルーターのルーティング テーブルでの発信インターフェイスとして使用することもできます。 インターフェイス タイプを指定する方法については「Network（ネットワーク）> Interfaces（インターフェイス）」を参照してください。 インターフェイスを追加すると、その接続済みルートが自動的に追加されます。
管理上の距離	以下の管理距離を指定します。 • **Static routes**[スタティックルート] - 範囲は10 ~ 240、デフォルトは10です。 • **OSPF Int**[OSPF内部] — 範囲は10 ~ 240、デフォルトは30です。 • **OSPF Ext**[OSPF外部] — 範囲は10 ~ 240、デフォルトは110です。 • **IBGP** - 範囲は10 ~ 240、デフォルトは200です。 • **EBGP** - 範囲は10 ~ 240、デフォルトは20です。 • **RIP** - 範囲は10 ~ 240、デフォルトは120です。

静的ルート

- Network > Virtual Routers > Static Routes [ネットワーク > 仮想ルーター > スタティック ルート]

任意で1つ以上のスタティックルートを入力します。Pv4またはIPv6アドレスを使用してルートを指定する場合は、**IP**または**IPv6** タブをクリックします。通常、ここでデフォルト ルートを設定 (0.0.0.0/0) するために必要になります。デフォルト ルートは、他の方法ではバーチャル ルータのルーティング テーブルに見つからない宛先に適用されます。

スタティック ルートの設定	の意味
氏名	スタティック ルートの識別に使用する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
宛先	CIDR（Classless Inter-Domain Routing）表記法でIPアドレスとネットワークマスクを入力します。*ip_address/mask*（たとえば、IPv4 の場合は 192.168.2.0/24、IPv4 の場合は 2001:db8::/32）。あるいは、タイプが IP ネットマスクのアドレス オブジェクトを作成できます。
インターフェイス	パケットを宛先に転送するインターフェイスを選択するか、ネクストホップ設定を指定するか、その両方を行います。
ネクストホップ	以下のいずれかを選択します。 • **IP Address (IP** アドレス**)**—ネクストホップ ルーターの IP アドレスを入力する、あるいは IP ネットマスク型のアドレス オブジェクトを選択または作成する場合に選択します。IPv4 の場合は /32、IPv6 の場合は /128 のネットマスクがアドレス オブジェクトに求められます。

© 2019 Palo Alto Networks, Inc.

スタティック ルートの設定	の意味
	• **Next VR**[次のVR] – ファイアウォールの仮想ルータをネクストホップとして選択します。これにより、1 つのファイアウォール内の仮想ルーター間で内部的にルーティングできます。 • **FQDN**–ネクストホップを FQDN で識別する場合に選択します。その後、FQDN 型のアドレス オブジェクトを選択するか、FQDN 型のアドレス オブジェクトを新規作成します。 • **Discard**[破棄] – この宛先のトラフィックを廃棄する場合に選択します。 • **None**[なし] – ルートのネクスト ホップが存在しない場合に指定します。
管理距離	スタティックルートの管理距離を指定します（10 ~ 240、デフォルトは10）。
メトリック	スタティック ルートの有効なメトリックを指定します (1 ~ 65535)。
ルート テーブル	どのルート テーブルにファイアウォールがスタティック ルートをインストールするか選択します。 • **Unicast**（ユニキャスト） – ユニキャスト ルート テーブルにルートをインストールします。 • **Multicast**（マルチキャスト） – マルチキャスト ルート テーブルにルートをインストールします。 • **Both**（両方） – ユニキャストとマルチキャストのルート テーブルにルートをインストールします。 • **No Install**（インストールしない） – ルート テーブル（RIB）にルートをインストールしません。ルートが削除されるまで、ファイアウォールは参考のためにスタティック ルートを維持します。
BFDプロファイル	PA-3200 Series、PA-5200 Series、PA-7000 Series、またはVM-Seriesファイアウォールのスタティックルートで双方向フォワーディングの検出 (BFD) を有効化する場合は以下のうちから一つ選択します。 • **default**（デフォルトのBFD設定） • ファイアウォール上で作成したBFDプロファイルです。 • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル] スタティックルートでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）] を選択します。 スタティックルートでBFDを使用する場合: • スタティックルートの両端にあるファイアウォールとピアの両方でBFDセッションがサポートされている必要があります。 • スタティックルートの**Next Hop**[ネクストホップ] のタイプは**IP Address**[IPアドレス]に設定し、有効なIPアドレスを入力する必要があります。 • **Interface**[インターフェイス] の設定を**None**[なし] にすることはできません。DHCPアドレスを使用している場合でも、インターフェイスを選択する必要があります。
パス モニタリング	スタティック ルートでパス モニタリングを有効化する場合に選択します。

© 2019 Palo Alto Networks, Inc.

スタティック ルートの設定	の意味
障害条件	監視対象パスがダウンしていることで、スタティック ルートもダウンしているとファイアウォールが判断する際の条件を選択します。 • **Any**（任意）– スタティック ルートの監視対象宛先いずれかが ICMP 到達不能である場合、ファイアウォールはスタティック ルートを RIB および FIB から削除して、メトリックが次に小さく、同じ宛先に向かうダイナミックまたはスタティック ルートを FIB に追加します。 • **All**（すべて）– スタティック ルートの監視対象宛先がすべて ICMP 到達不能である場合、ファイアウォールはスタティック ルートを RIB および FIB から削除して、メトリックが次に小さく、同じ宛先に向かうダイナミックまたはスタティック ルートを FIB に追加します。 **All**（すべて）を選択すると、たとえば監視対象の 1 つの宛先がメンテナンスのためにオフラインになっていることで、スタティック ルート エラーとなってしまうような可能性を避けられます。
プリエンプティブ ホールド タイム (分)	ダウンしたパス モニターが Up（アップ）状態を維持しなければならない分数を入力します。パス モニターがメンバーである監視対象宛先すべてを評価し、Up（アップ）を維持すると、ファイアウォールはスタティック ルートを RIB に再インストールします。リンクがダウンしたりフラッピングしたりせずにタイマーの期間が過ぎた場合、リンクは安定していると見なされて、パス モニターは Up（アップ）を維持できます。また、ファイアウォールはスタティック ルートを RIB に再度追加できます。 ホールド タイム中にリンクのダウンやフラッピングが発生した場合、パス モニターはエラーとなります。タイマーはダウンしたモニターが Up（アップ）状態に戻ったときに再度開始します。**Preemptive Hold Time**（プリエンプティブ ホールド タイム）が 0 の場合、パス モニターがアップになると即座にファイアウォールがスタティック ルートを RIB に再インストールします。範囲は 0 ~ 1,440、デフォルトは 2 です。
氏名	監視対象宛先の識別に使用する名前を入力します（最大 31 文字）。
Enable [有効化]	スタティック ルートのこの特定の宛先のパス モニタリングを有効化する場合に選択します。ファイアウォールは ICMP Ping をこの宛先に送信します。
送信元IP	監視対象宛先に対する ICMP Ping で送信元としてファイアウォールが使用する IP アドレスを選択します。 • インターフェイスに複数の IP アドレスがある場合は、1 つ選択します。 • インターフェイスを選択した場合、ファイアウォールはデフォルトでインターフェイスに割り当てられている最初の IP アドレスを使用します。 • **DHCP (Use DHCP Client address)**（**DHCP**（**DHCP** クライアントレス アドレスの使用））を選択した場合、ファイアウォールは DHCP がインターフェイスに割り当てたアドレスを使用します。DHCP アドレスを確認するには、 **Network**（ネットワーク）> **Interfaces**（インターフェイス）> **Ethernet**（イーサネット）を選択して、イーサネット インターフェイスの行にある **Dynamic DHCP Client**（動的 **DHCP** クライアント）をクリックします。Dynamic IP Interface Status（動的 IP インターフェイス状態）ウィンドウに IP アドレスが表示されます。
宛先IP	ファイアウォールがパスを監視する対象の、堅牢で安定した IP アドレスまたはアドレス オブジェクトを入力します。監視対象宛先と、スタティック ルー

© 2019 Palo Alto Networks, Inc.

スタティック ルートの設定	の意味
	トの宛先は、同じアドレス ファミリー（IPv4 または IPv6）を使用してください。
Ping Interval (sec)（Ping 間隔（秒））	ファイアウォールがパスを監視する頻度を定める ICMP Ping 間隔を秒数で指定します（監視対象宛先に Ping を送信する頻度。範囲は 1 ~ 60、デフォルトは 3）。
Ping 数	監視対象宛先から ICMP Ping パケットが返ってこない場合に、リンクがダウンしているとファイアウォールが見なすまでの、ICMP Ping パケットの連続数を指定します。**Any**（任意）または **All**（すべて）のエラー条件に基づき、パス モニタリングがエラー状態になると、ファイアウォールはスタティック ルートを RIB から削除します（範囲は 3 ~ 10、デフォルトは 5）。 たとえば、Ping 間隔が 3 秒で、Ping 数 5 個において Ping が存在しない（直近 15 秒間の間、ファイアウォールは Ping を受信していない）場合、パス モニタリングはリンク エラーを検出します。パス モニタリングがエラー状態で、ファイアウォールが 15 秒の後に Ping を受信した場合、リンクの状態はアップと見なされます。**Any**（任意）または **All**（すべて）のエラー条件に基づき、**Any**（任意）または **All**（すべて）の監視対象宛先に対するパス モニタリングの状態はアップと見なすことができます。また、プリエンプティブ ホールド タイムが開始されます。

ルート再配信

- Network > Virtual Router > Redistribution Profiles [ネットワーク > 仮想ルーター > 再配信プロファイル]

再配信プロファイルは、目的のネットワーク動作に応じて、ファイアウォールにおけるフィルタリング、優先順位の設定、アクションの実行を管理します。ルート再配信を使用すると、スタティック ルートと他のプロトコルで取得されたルートを、指定したルーティング プロトコル経由で通知できます。

再配信プロファイルを有効にするには、ルーティング プロトコルに適用する必要があります。再配信ルールがないと、各プロトコルば別個に実行され、それぞれの範囲外では通信しません。再配信プロファイルは、すべてのルーティング プロトコルが設定され、その結果のネットワーク トポロジが確立した後に追加または変更できます。

再配信プロファイルを RIP および OSPF プロトコルに適用するには、エクスポート ルールを定義します。**Redistribution Rules**[ルールの再配信] タブで再配信プロファイルを BGP に適用します。以下の表を参照してください。

再配信プロファイル設定	の意味
氏名	再配信プロファイルを **Add**（追加）して、プロファイル名を入力します。
優先順位	このプロファイルの優先度 (範囲は 1 ~ 255) を入力します。プロファイルは順番に照合されます (優先度の昇順)。
再配信	このウィンドウの設定に基づいてルート再配信を実行するかどうかを選択します。 • **Redist**[再配信あり] — 一致した候補ルートを再配信するには、オンにします。このオプションをオンにした場合、新しいメトリック値を入力します。メトリック値が小さいほど適切なルートになります。

© 2019 Palo Alto Networks, Inc.

再配信プロファイル設定	の意味
	• **No Redist**[再配信なし] — 一致した候補ルートを再配信しない場合、オンにします。
General Filter [一般的なフィルタ] タブ	
タイプ	候補ルートのルートタイプを指定します。
インターフェイス	候補ルートの転送インターフェイスを指定するためのインターフェイスを選択します。
宛先	候補ルートの宛先を指定するには、宛先 IP アドレスまたはサブネット (形式は x.x.x.x または x.x.x.x/n) を入力して **Add**[追加] をクリックします。エントリを削除する場合は、削除 (⊖) をクリックします。
ネクストホップ	候補ルートのゲートウェイを指定するには、ネクストホップを示す IP アドレスまたはサブネット (形式は x.x.x.x または x.x.x.x/n) を入力して **Add**[追加] をクリックします。エントリを削除する場合は、削除 (⊖) をクリックします。
OSPF Filter [OSPF フィルタ] タブ	
パス タイプ	候補OSPFルートのルートタイプを指定します。
エリア	候補 OSPF ルートのエリア識別子を指定します。**OSPF area ID**[OSPFエリアID] (形式は x.x.x.x) を入力し、**Add**[追加] をクリックします。 エントリを削除する場合は、削除 (⊖) をクリックします。
タグ	OSPF タグ値を指定します。数値でタグ値 (1 ~ 255) を入力し、Add [追加] をクリックします。 エントリを削除する場合は、削除 (⊖) をクリックします。
BGP Filter [BGP フィルタ] タブ	
コミュニティ	BGP ルーティング ポリシーのコミュニティを指定します。
拡張コミュニティ	BGP ルーティング ポリシーの拡張コミュニティを指定します。

RIP

- Network > Virtual Routers > RIP [ネットワーク > 仮想ルーター > RIP]

RIP (ルーティング情報プロトコル) の設定には、以下の一般設定が含まれます。

RIP 設定	の意味
Enable [有効化]	RIP を有効化する場合に選択します。
デフォルト ルートの拒否	(推奨) RIP 経由でデフォルト ルートを学習しない場合に選択します。

© 2019 Palo Alto Networks, Inc.

RIP 設定	の意味
BFD	PA-5200 Series、PA-7000 Series、またはVM-Seriesファイアウォールの仮想ルーターでRIP用に双方向フォワーディングの検出（BFD）をグローバルに有効化する場合は、以下のうちから一つ選択します。 • **default**（デフォルトのBFD設定が含まれるプロファイルです） • ファイアウォール上で作成したBFDプロファイルです。 • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル] すべてのRIPインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）]を選択します。シングルRIPのインターフェイスでは、BFDを無効化することができません。

さらに、以下のタブのRIP設定を指定する必要があります。

- **Interfaces**[インターフェイス]:「RIP Interfaces Tab（RIP のインターフェイス タブ）」を参照してください。
- **Timers**[タイマー]:「RIP Timer Tab（RIP タイマー タブ）」を参照してください。
- **Auth Profiles**[認証プロファイル]:「RIP Auth Profiles Tab（RIP の認証プロファイル タブ）」を参照してください。
- **Export Rules**[ルールのエクスポート]:「RIP Export Rules Tab（RIP の エクスポート ルール タブ）」を参照してください。

RIP の Interfaces（インターフェイス）タブ

- Network > Virtual Routers > RIP > Interfaces [ネットワーク > 仮想ルーター > RIP > インターフェイス]

以下のフィールドを使用して RIP インターフェイスを設定します。

RIP – インターフェイス設定	の意味
インターフェイス	RIP プロトコルを実行するインターフェイスを選択します。
Enable [有効化]	これらの設定を有効にするには、オンにします。
通知	デフォルトルートを、指定したメトリック値でRIPピアに通知する場合は、これをオンにします。
メトリック	ルータ通知のメトリック値を指定します。**Advertise**[通知]を可能にした場合のみ、このフィールドが表示されます。
認証プロファイル	プロファイルを選択します。
モード	**normal**[ノーマル]、**passive**[パッシブ]、または **send-only**[送信のみ] を選択します。
BFD	RIPインターフェイスでBFDを有効化する場合は（仮想ルーターのレベルでRIP用のBFDが無効化されていない限り、RIP用のBFD設定をオーバーライドすることになります）、以下のうち一つを選択します。 • **default**（デフォルトのBFD設定が含まれるプロファイルです） • ファイアウォール上で作成したBFDプロファイルです。

© 2019 Palo Alto Networks, Inc.

RIP – インターフェイス設定	の意味
	• 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル] RIPインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）] を選択します。

RIP の Timers（タイマー）タブ

- Network > Virtual Router > RIP > Timers [ネットワーク > 仮想ルーター > RIP > タイマー]

以下の表はRIPのルート更新や失効をコントロールするタイマーをあらわしています。

RIP – タイマー設定	の意味
RIP タイミング	
間隔 (秒)	タイマ間隔を秒単位で指定します。この時間は、他の [RIP Timing] のフィールドで使用されます (範囲は1～60)。
更新間隔	ルート更新通知間の間隔数を入力します (範囲は1 ～ 3600)。
失効の間隔	ルートが最後に更新されてから有効期限が切れるまでの間隔数を入力します (範囲は1 ～ 3600)。
削除間隔	ルートの有効期限が切れてから削除されるまでの間隔数を入力します (範囲は1 ～ 3600)。

RIP の Auth Profiles（認証プロファイル）タブ

- Network > Virtual Router > RIP > Auth Profiles [ネットワーク > 仮想ルーター > RIP > 認証プロファイル]

デフォルト設定では、ファイアウォールはネイバー間のRIPメッセージを認証しません。ネイバー間のRIPメッセージを認証する場合は認証プロファイルを作成し、仮想ルーター上でRIPを実行中のインターフェイスにそれを適用します。以下の表に、**Auth Profiles**[認証プロファイル] タブの設定を示します。

RIP – 認証プロファイル設定	の意味
プロファイル名	RIP メッセージを認証するための認証プロファイル名を入力します。
パスワード タイプ	パスワードのタイプを選択します (Simple [簡易パスワード] または MD5)。 • **Simple**[簡易パスワード] を選択した場合、簡易パスワードを入力して確認します。 • **MD5** を選択した場合は、**Key-ID**[キーID] (0 ～ 255)、**Key**[キー]、および任意の **Preferred**[優先] 状態など、1 つ以上のパスワード エントリを入力します。エントリごとに **Add**[追加] をクリックしてから、**OK** をクリックします。送信メッセージの認証に使用する鍵を指定するには、**Preferred**[優先] オプションを選択します。

© 2019 Palo Alto Networks, Inc.

RIP の Export Rules（エクスポート ルール）タブ

- Network > Virtual Router > RIP > Export Rules [ネットワーク > 仮想ルーター > RIP > ルールのエクスポート]

RIPエクスポートのルールを設定することで、仮想ルーターがピアに送信可能なルートをコントロールすることができます。

RIP – エクスポート ルール設定	の意味
デフォルト ルートの再配信を許可	ファイアウォールからピアにデフォルト ルートを再配信することを許可する場合に選択します。
再配信プロファイル	**Add**[追加]をクリックし、目的のネットワーク動作に基づいて、ルート再配信、フィルタ、優先度、アクションを変更できる再配信プロファイルを選択または追加します。「ルートの再配信」を参照してください。

OSPF

- Network > Virtual Router > OSPF [ネットワーク > 仮想ルーター > OSPF]

OSPF（Open Shortest Path First）プロトコルを設定するには、以下の一般設定を指定する必要があります（任意の BFD は保続）。

OSPF 設定	の意味
Enable [有効化]	OSPF プロトコルを有効化する場合に選択します。
デフォルト ルートの拒否	（推奨）OSPF 経由でデフォルト ルートを学習しない場合に選択します。
ルーターID	この仮想ルーターの OSPF インスタンスに関連付けられているルータ ID を指定します。OSPF プロトコルでは、このルータ ID を使用して OSPF インスタンスを一意に識別します。
BFD	PA-3000 Series、PA-5200 Series、PA-7000 Series、またはVM-Seriesファイアウォールの仮想ルーターで OSPF 用に双方向フォワーディング検出 (BFD) をグローバルに有効化する場合は以下のうちから一つを選択します。 • **default**（デフォルトのBFD設定） • ファイアウォール上で作成したBFDプロファイルです。 • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル] すべてのOSPFインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）]を選択します。シングルOSPFのインターフェイスでは、BFDを無効化することができません。

また、以下のタブで OSPF 設定を指定する必要があります。

- **Areas**[エリア]:「OSPF Areas Tab（OSPF エリア タブ）」を参照してください。
- **Auth Profiles**[認証プロファイル]:「OSPF Auth Profiles Tab（OSPF の認証プロファイル タブ）」を参照してください。

© 2019 Palo Alto Networks, Inc.

- **Export Rules**[ルールのエクスポート]:「OSPF Export Rules Tab（OSPF の エクスポート ルール タブ）」を参照してください。
- **Advanced**[詳細]:「OSPF Advanced Tab（OSPF の詳細タブ）」を参照してください。

OSPF の Areas（エリア）タブ

- Network > Virtual Router > OSPF > Areas [ネットワーク > 仮想ルーター > OSPF > エリア]

以下のフィールドでは、OSPF エリア設定について説明します。

OSPF – エリア設定	の意味
エリア	
エリア ID	OSPF パラメータを適用可能なエリアを設定します。 エリアの識別子を x.x.x.x の形式で入力します。この識別子を受け入れたネイバーのみが同じエリアに属します。
タイプ	以下のいずれかのオプションを選択します。 • **Normal**[通常] — 制限はありません。エリアではすべてのタイプのルートを使用できます。 • **Stub**[スタブ] — エリアからの出口はありません。エリア外にある宛先に到達するには、別のエリアに接続されている境界を通過する必要があります。このオプションを選択した場合、他のエリアからこのタイプの LSA (Link State Advertisement) を受け入れるには **Accept Summary**[サマリーの受け入れ] を選択します。さらに、スタブ エリアへの通知にデフォルト ルート LSA とそれに関連付けられたメトリック値（範囲は 1 ~ 255）を含めるかどうかを指定します。 スタブエリアのエリア ボーダー ルーター (ABR) インターフェイスの **Accept Summary**[サマリーの受け入れ] オプションが無効になっていると、OSPF エリアは Totally Stubby Area (TSA) として動作し、ABR はサマリー LSA を伝搬しません。 • **NSSA** (Not-So-Stubby Area) — エリアから直接外部に出ることができますが、OSPF ルート以外のルートを使用する必要があります。このオプションを選択した場合、このタイプの LSA を受け入れるには **Accept Summary**[サマリーの受け入れ] を選択します。**Advertise Default Route**[デフォルト ルートの通知] を選択して、スタブエリアへの通知にデフォルト ルート LSA とそれに関連付けられたメトリック値 (1 ~ 255) を含めるかどうかを指定します。さらに、デフォルト LSA の通知に使用するルート タイプを選択します。NSSA 経由で学習した外部ルートの他のエリアへの通知を有効にするか、停止する場合は、**External Ranges**[外部範囲] セクションの **Add**[追加] をクリックし、範囲を入力します。
範囲	**Add**[追加] をクリックし、エリア内の LSA 宛先アドレスをサブネットに集約します。サブネットと一致する LSA の通知を有効にするか、停止して、**OK** をクリックします。別の範囲を追加する場合は、この操作を繰り返します。
インターフェイス	エリアに含めるインターフェイスを **Add**（追加）し、以下の情報を入力します。 • **Interface**[インターフェイス] — インターフェイスを選択します。 • **Enable**[有効化] — OSPF インターフェイス設定を有効にします。

© 2019 Palo Alto Networks, Inc.

OSPF – エリア設定	の意味

	• **Passive**（パッシブ） — OSPF インターフェイスで OSPF パケットを送受信しない場合に選択します。このオプションをオンにすると OSPF パケットは送受信されませんが、インターフェイスは LSA データベースに追加されます。
	• **Link type**[リンクタイプ] — このインターフェイスを経由してアクセス可能なすべてのネイバーを、OSPF helloメッセージのマルチキャストによって自動的に検出させる場合は、**Broadcast**[ブロードキャスト] を選択します（Ethernetインターフェイスなど）。自動的にネイバーを検出する場合は、**P2p** (ポイントツーポイント) を選択します。ネイバーを手動で定義する必要がある場合は、**P2mp** (ポイントツーマルチポイント) を選択します。ネイバーを手動で定義できるのは、p2mp モードの場合のみです。
	• **Metric**[メトリック] — このインターフェイスの OSPF メトリックを入力します (0 ~ 65535)。
	• **Priority**[優先順位] — このインターフェイスの OSPF 優先度を入力します (0 ~ 255)。OSPF プロトコルでは、この優先度に基づいて、ルータが指名ルータ (DR) または バックアップ DR (BDR) として選択されます。値が 0 の場合、ルーターが DR または BDR として選択されることはありません。
	• **Auth Profile**[認証プロファイル] — 以前に定義した認証プロファイルを選択します。
	• **BFD** - OSPFピアのインターフェイスで双方向フォワーディングの検知（BFD）を有効化する場合は（仮想ルーターのレベルでOSPF用の**BFD**が無効化されていない限り、OSPF用の**BFD**設定をオーバーライドすることになります）、以下のうち一つを選択します。
	  • **default**（デフォルトのBFD設定）
	  • ファイアウォール上で作成したBFDプロファイルです。
	  • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル]
	  • OSPFピアのインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）] を選択します。
	• **Hello Interval (sec)**[Hello間隔（秒）] — OSPFプロセスが直接接続されているネイバーにHelloパケットを送信する間隔（秒数）です（範囲は0～3600、デフォルトは10）。
	• **Dead Counts**[失敗許容回数] — Hello 間隔の試行回数で、この回数を超えても OSPF がネイバーから Hello パケットを受信しない場合、OSPF はネイバーがダウンしているものとみなします。**Hello Interval**[Hello間隔]に **Dead Counts**[失敗許容回数] を乗じた数が、失敗タイマーの値です（範囲は3～20、デフォルトは4）。
	• **Retransmit Interval (sec) (再送信間隔 (秒))** — OSPFがネイバーからリンク状態通知 (LSA) を待機する秒数で、この時間を過ぎるとOSPFがLSAを再送信します（範囲は0～3600、デフォルトは10）。
	• **Transit Delay (sec) (トランジット遅延（秒）)** — LSA の秒単位の遅延時間です。この時間を過ぎると、インターフェイスから送信されます（範囲は 0 ~ 3600、デフォルトは 1）。

Interface（インターフェイス）（続き）	• **Graceful Restart Hello Delay (sec)**（グレースフル リスタート **Hello** パケット遅延（秒））— アクティブ/パッシブ高可用性が設定されている場合に、OSPF インターフェイスに適用されます。**Graceful Restart Hello Delay (グレースフル リスタート Hello パケット遅延)** は、ファイアウォールが 1 秒間隔でグレース LSA パケットを送信する期間です。この期間は、リスタート中のファイアウォールから Hello パケットが送信されません。リス

© 2019 Palo Alto Networks, Inc.

OSPF – エリア設定	の意味
	タート中は、失敗タイマー（**Hello Interval (Hello 間隔)** に **Dead Counts (失敗許容回数)** を乗じた数）もカウントダウンされます。失敗タイマーの時間が短かすぎる場合は、Hello パケットが遅延したときに、グレースフルリスタート中に隣接がダウンします。そのため、失敗タイマーを **Graceful Restart Hello Delay**（グレースフル リスタート **Hello** パケット遅延）の値の 4 倍以上にすることをお勧めします。たとえば、**Hello Interval**（**Hello** 間隔）が 10 秒で、**Dead Counts**（失敗許容回数）が 4 回の場合、失敗タイマーは 40 秒になります。**Graceful Restart Hello Delay**（グレースフル リスタート **Hello** パケット遅延）が　10 秒に設定されていれば、10 秒遅延しても失敗タイマーの 40 秒以内に十分に収まるため、グレースフル リスタート中に隣接がタイムアウトになることがありません（範囲は 1 ~ 10、デフォルトは 10）。
仮想リンク	バックボーンエリアの接続を維持または拡張するには、仮想リンク設定を指定します。この設定は、エリア境界ルータに対して、バックボーンエリア内 (0.0.0.0) で定義する必要があります。**Add**[追加] をクリックし、バックボーンエリアに含める仮想リンクごとに以下の情報を入力して、**OK** をクリックします。 • **Name**[名前] — 仮想リンクの名前を入力します。 • **Neighbor ID**[ネイバー ID] — 仮想リンクの反対側のルータ (ネイバー) のルータ ID を入力します。 • **Transit Area**[トランジット エリア] — 仮想リンクが物理的に含まれる中継エリアのエリア ID を入力します。 • **Enable**[有効化] — 仮想リンクを有効にするには、オンにします。 • **Timing**[タイミング] — デフォルトのタイミング設定のまま使用することをお勧めします。 • **Auth Profile**[認証プロファイル] — 以前に定義した認証プロファイルを選択します。

OSPF の Auth Profiles（認証プロファイル）タブ

- Network > Virtual Router > OSPF > Auth Profiles [ネットワーク > 仮想ルーター > OSPF > 認証プロファイル]

以下のフィールドでは、OSPF 認証プロファイル設定について説明します。

OSPF – 認証プロファイル設定	の意味
プロファイル名	認証プロファイルの名前を入力します。OSPF メッセージを認証するには、最初に認証プロファイルを定義し、次に **OSPF** タブでそのプロファイルをインターフェイスに適用します。
パスワード タイプ	パスワードのタイプを選択します (Simple [簡易パスワード] または MD5)。 • **Simple**[簡易パスワード] を選択した場合は、パスワードを入力します。 • **MD5** を選択した場合は、**Key-ID**[キーID] (0 ~ 255)、**Key**[キー]、および任意の **Preferred**[優先] 状態など、1 つ以上のパスワード エントリを入力します。エントリごとに **Add**[追加] をクリックしてから、**OK** をクリックしま

© 2019 Palo Alto Networks, Inc.

OSPF – 認証プロファイル設定	の意味
	す。送信メッセージの認証に使用する鍵を指定するには、**Preferred**[優先] オプションを選択します。

OSPF の Export Rules (エクスポート ルール) タブ

- Network > Virtual Router > OSPF > Export Rules [ネットワーク > 仮想ルーター > OSPF > ルールのエクスポート]

以下の表では、OSPF ルートをエクスポートするためのフィールドについて説明します。

OSPF – エクスポート ルール設定	の意味
デフォルト ルートの再配信を許可	OSPF 経由でデフォルト ルートの再配信を許可する場合に選択します。
氏名	再配信プロファイルの名前を選択します。値には IP サブネットまたは有効な再配信プロファイル名を指定する必要があります。
新規パス タイプ	適用するメトリック タイプを選択します。
新規タグ	一致したルート用に 32 ビット値のタグを指定します。
メトリック	(任意) エクスポートされたルートに関連付けられてパス選択に使用されるルート メトリックを指定します (範囲は 1 ~ 65535)。

OSPF の Advanced (詳細) タブ

- Network > Virtual Router > OSPF > Advanced [ネットワーク > 仮想ルーター > OSPF > 詳細]

以下のフィールドでは、RFC 1583 の互換性、OSPF タイマー、およびグレースフル リスタートについて説明します。

OSPF – 詳細設定	の意味
RFC 1583 の互換性	RFC 1583 (OSPF バージョン 2) との互換性を確保する場合に選択します。
タイマー	• **SPF Calculation Delay (sec)**[SPF計算遅延 (秒)] - このタイマーにより、新しいトポロジ情報の受信から、SPF計算を実行するまでの遅延時間を調整することができます。指定する値が低ければそれだけ OSPF の再収束が速くなります。ファイアウォールとピアリングしているルーターは、収束時間の最適化と同様の方法で調整する必要があります。 • **LSA Interval (sec)**[LSA間隔 (秒)] - このオプションは、同一LSA (同一ルーター、同一タイプ、同一 LSA ID) の2つのインスタンスの伝送間の最小時間を指定します。RFC 2328 の MinLSInterval と同等です。低い値を指定すると、トポロジが変更された場合の再収束時間が短縮されます。
グレースフル リスタート	• **Enable Graceful Restart**[グレースフルリスタートを有効化] - この機能が有効なファイアウォールは、ファイアウォールが一時的にダウンして移行が

© 2019 Palo Alto Networks, Inc.

OSPF – 詳細設定	の意味
	実行されている間も、ファイアウォールを経由するルートを引き続き使用するように近隣のルーターに指示します（デフォルトで有効）。 • **Enable Helper Mode**[ヘルパーモードを有効化] - このモードが有効なファイアウォールは、隣接デバイスの再起動中もそのデバイスへの転送を継続します（デフォルトで有効）。 • **Enable Strict LSA Checking**[厳密なLSAチェックを有効化] - トポロジが変更された場合、この機能により、OSPFヘルパーモードが有効なファイアウォールのヘルパーモードが終了します（デフォルトで有効）。 • **Grace Period (sec)**（猶予時間（秒））– 隣接デバイスの再確立中またはルーターの再起動中にピア デバイスがこのファイアウォールに向けた転送を継続する秒数です（範囲は 5 ~ 1,800、デフォルトは 120）。 • **Max Neighbor Restart Time**（ネイバー再起動の最大時間）– ファイアウォールをヘルパー モード ルーターとして使用できる最大猶予時間（秒）です。ピアデバイスのグレースLSAで提供される猶予時間の方が長い場合、ファイアウォールはヘルパーモードになりません（範囲は5 ~ 1800、デフォルトは140）。

OSPFv3IPv6

- Network > Virtual Router > OSPFv3 [ネットワーク > 仮想ルーター > OSPFv3]

OSPFv3（Open Shortest Path First v3）プロトコルを設定するには、以下の表の最初の 3 つの設定を指定する必要があります（BFD は任意）。

OSPFv3設定	の意味
Enable [有効化]	OSPF プロトコルを有効化する場合に選択します。
デフォルト ルートの拒否	OSPF 経由でデフォルト ルートを学習しない場合に選択します。
ルーターID	この仮想ルーターの OSPF インスタンスに関連付けられているルータ ID を指定します。OSPF プロトコルでは、このルータ ID を使用して OSPF インスタンスを一意に識別します。
BFD	PA-3000 Series、PA-5200 Series、PA-7000 Series、および VM-Seriesファイアウォールの仮想ルーターで OSPFv3 用に双方向フォワーディング検出 (BFD) をグローバルに有効化する場合は以下のうちから一つを選択します。 • **default**（デフォルトのBFD設定） • ファイアウォール上で作成したBFDプロファイルです。 • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル] 仮想ルーターのすべての OSPFv3 インターフェイスで BFD を無効化する場合は **None (Disable BFD)**（なし（**BFD** 無効））を選択します。シングル OSPFv3 のインターフェイスでは、BFD を無効化することができません。

さらに、以下のタブで OSPFv3 の設定を指定します。

- **Areas**[エリア]:「OSPFv3 Areas Tab（OSPFv3 エリア タブ）」を参照してください。

© 2019 Palo Alto Networks, Inc.

- **Auth Profiles**[認証プロファイル]:「OSPFv3 Auth Profiles Tab（OSPFv3 の認証プロファイル タブ）」を参照してください。
- **Export Rules**[ルールのエクスポート]:「OSPFv3 Export Rules Tab（OSPFv3 の エクスポート ルール タブ）」を参照してください。
- **Advanced**[詳細]:「OSPFv3 Advanced Tab（OSPFv3 詳細タブ）」を参照してください。

OSPFv3 の Areas（エリア）タブ

- Network > Virtual Router > OSPFv3 > Areas [ネットワーク > 仮想ルーター > OSPFv3 > エリア]

以下のフィールドを使用して、OSPFv3 エリアを設定します。

OSPFv3 – エリア設定	の意味
authentication	この OSPF エリアに指定する認証プロファイルの名前を選択します。
タイプ	以下のいずれかを選択します。 • **Normal**[通常] — 制限はありません。エリアではすべてのタイプのルートを使用できます。 • **Stub**[スタブ] — エリアからの出口はありません。エリア外にある宛先に到達するには、別のエリアに接続されている境界を通過する必要があります。このオプションを選択した場合、他のエリアからこのタイプの LSA (Link State Advertisement) を受け入れるには **Accept Summary**[サマリーの受け入れ] を選択します。さらに、スタブエリアへの通知にデフォルト ルート LSA とそれに関連付けられたメトリック値 (1 ~ 255) を含めるかどうかを指定します。 スタブエリアのエリア ボーダー ルーター (ABR) インターフェイスの **Accept Summary**[サマリーの受け入れ] オプションが無効になっていると、OSPF エリアは Totally Stubby Area (TSA) として動作し、ABR はサマリー LSA を伝搬しません。 • **NSSA** (Not-So-Stubby Area) — エリアから直接外部に出ることができますが、OSPF ルート以外のルートを使用する必要があります。このオプションを選択した場合、このタイプの LSA を受け入れるには **Accept Summary**[サマリーの受け入れ] を選択します。スタブエリアへの通知にデフォルト ルート LSA とそれに関連付けられたメトリック値 (1 ~ 255) を含めるかどうかを指定します。さらに、デフォルト LSA の通知に使用するルート タイプを選択します。NSSA 経由で学習した外部ルートの他のエリアへの通知を有効にするか、停止する場合は、**External Ranges**[外部範囲] セクションの **Add**[追加] をクリックし、範囲を入力します。
範囲	**Add**[追加] をクリックし、エリア内のLSA宛先 IPv6アドレスをサブネットに集約します。サブネットと一致する LSA の通知を有効にするか、停止して、**OK** をクリックします。別の範囲を追加する場合は、この操作を繰り返します。
インターフェイス	**Add**[追加] をクリックし、エリアに含めるインターフェイスごとに以下の情報を入力して、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

OSPFv3 – エリア設定	の意味

	• **Interface**[インターフェイス] — インターフェイスを選択します。
	• **Enable**[有効化] — OSPF インターフェイス設定を有効にします。
	• インスタンス **ID** – OSPFv3 インスタンス ID 番号を入力します。
	• **Passive**（パッシブ） — OSPF インターフェイスで OSPF パケットを送受信しない場合に選択します。このオプションをオンにすると OSPF パケットは送受信されませんが、インターフェイスは LSA データベースに追加されます。
	• **Link type**[リンクタイプ] — このインターフェイスを経由してアクセス可能なすべてのネイバーを、OSPF helloメッセージのマルチキャストによって自動的に検出させる場合は、**Broadcast**[ブロードキャスト] を選択します（Ethernetインターフェイスなど）。自動的にネイバーを検出する場合は、**P2p** (ポイントツーポイント) を選択します。ネイバーを手動で定義する必要がある場合は、**P2mp** (ポイントツーマルチポイント) を選択します。ネイバーを手動で定義できるのは、p2mp モードの場合のみです。
	• **Metric**[メトリック] — このインターフェイスの OSPF メトリックを入力します (0 ~ 65535)。
	• **Priority**[優先順位] — このインターフェイスの OSPF 優先度を入力します (0 ~ 255)。OSPF プロトコルでは、この優先度に基づいて、ルータが指名ルータ (DR) または バックアップ DR (BDR) として選択されます。値が 0 の場合、ルーターが DR または BDR として選択されることはありません。
	• **Auth Profile**[認証プロファイル] — 以前に定義した認証プロファイルを選択します。
	• **BFD** - OSPFv3ピアのインターフェイスで双方向フォワーディングの検知（BFD）を有効化する場合は（仮想ルーターのレベルでOSPFv3用の**BFD**が無効化されていない限り、OSPFv3用の**BFD**設定をオーバーライドすることになります）、以下のうち一つを選択します。
	  • **default**（デフォルトのBFD設定）
	  • ファイアウォール上で作成したBFDプロファイルです。
	  • 新しいBFDプロファイルを作成する場合は**New BFD Profile**[新しいBFDプロファイル]
	  OSPFv3ピアのインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）] を選択します。
	• **Hello Interval (sec)**[Hello間隔（秒）] — OSPFプロセスが直接接続されているネイバーにHelloパケットを送信する間隔（秒数）です（範囲は0～3600、デフォルトは10）。
	• **Dead Counts**[失敗許容回数] — Hello 間隔の試行回数で、この回数を超えても OSPF がネイバーから Hello パケットを受信しない場合、OSPF はネイバーがダウンしているものとみなします。**Hello Interval**[Hello間隔]に **Dead Counts**[失敗許容回数] を乗じた数が、失敗タイマーの値です（範囲は3～20、デフォルトは4）。
	• **Retransmit Interval (sec)** (再送信間隔 (秒)) — OSPFがネイバーからリンク状態通知 (LSA) を待機する秒数で、この時間を過

© 2019 Palo Alto Networks, Inc.

OSPFv3 – エリア設定	の意味
	ぎるとOSPFがLSAを再送信します（範囲は0～3600、デフォルトは10）。 • **Transit Delay (sec)**（トランジット遅延（秒））– ファイアウォールのインターフェイスが LSA の送信を待機させる秒数です（範囲は 0 ～ 3,600、デフォルトは 1）。
インターフェイス（続き）	• **Graceful Restart Hello Delay (sec)**（グレースフル リスタート **Hello** パケット遅延（秒））– アクティブ/パッシブ高可用性が設定されている場合に、OSPF インターフェイスに適用されます。**Graceful Restart Hello Delay (**グレースフル リスタート **Hello** パケット遅延**)** は、ファイアウォールが 1 秒間隔でグレース LSA パケットを送信する期間です。この期間は、リスタート中のファイアウォールから Hello パケットが送信されません。リスタート中は、失敗タイマー（**Hello Interval (Hello** 間隔**)** に **Dead Counts (**失敗許容回数**)** を乗じた数）もカウントダウンされます。失敗タイマーの時間が短かすぎる場合は、Hello パケットが遅延したときに、グレースフル リスタート中に隣接がダウンします。そのため、失敗タイマーを **Graceful Restart Hello Delay**（グレースフル リスタート **Hello** パケット遅延）の値の 4 倍以上にすることをお勧めします。たとえば、**Hello Interval**（**Hello** 間隔）が 10 秒で、**Dead Counts**（失敗許容回数）が 4 回の場合、失敗タイマーは 40 秒になります。**Graceful Restart Hello Delay**（グレースフル リスタート **Hello** パケット遅延）が　10 秒に設定されていれば、10 秒遅延しても失敗タイマーの 40 秒以内に十分に収まるため、グレースフル リスタート中に隣接がタイムアウトになることがありません（範囲は 1 ～ 10、デフォルトは 10）。 • **Neighbors**[ネイバー] – p2pmp インターフェイスの場合、このインターフェイスを介して到達可能なすべてのネイバーに対するネイバー IP アドレスを入力します。
仮想リンク	バックボーンエリアの接続を維持または拡張するには、仮想リンク設定を指定します。この設定は、エリア境界ルータに対して、バックボーンエリア内 (0.0.0.0) で定義する必要があります。**Add**[追加] をクリックし、バックボーンエリアに含める仮想リンクごとに以下の情報を入力して、**OK** をクリックします。 • **Name**[名前] – 仮想リンクの名前を入力します。 • **Instance ID**[インスタンス ID] – OSPFv3 インスタンス ID 番号を入力します。 • **Neighbor ID**[ネイバー ID] – 仮想リンクの反対側のルータ (ネイバー) のルータ ID を入力します。 • **Transit Area**[トランジット エリア] – 仮想リンクが物理的に含まれる中継エリアのエリア ID を入力します。 • **Enable**[有効化] – 仮想リンクを有効にするには、オンにします。 • **Timing**[タイミング] – デフォルトのタイミング設定のまま使用することをお勧めします。 • **Auth Profile**[認証プロファイル] – 以前に定義した認証プロファイルを選択します。

© 2019 Palo Alto Networks, Inc.

OSPFv3 の（認証プロファイル）タブ

- Network > Virtual Router > OSPFv3 > Auth Profiles [ネットワーク > 仮想ルーター > OSPFv3 > 認証プロファイル]

以下のフィールドを使用して、OSPFv3 の認証を設定します。

OSPFv3 – 認証プロファイル設定	の意味
プロファイル名	認証プロファイルの名前を入力します。OSPF メッセージを認証するには、最初に認証プロファイルを定義し、次に **OSPF** タブでそのプロファイルをインターフェイスに適用します。
SPI	リモート ファイアウォールからピアへのパケット トラバーサルのセキュリティ パラメータ インデックス (SPI) を指定します。
PROTOCOL	以下のいずれかのプロトコルを指定します。 • **ESP** — Encapsulating Security Payload プロトコル。 • **AH** — Authentication Header プロトコル。
暗号化アルゴリズム	以下のいずれかを指定します。 • **None**[なし] — 暗号化アルゴリズムは使用されません。 • **SHA1**（デフォルト）— Secure Hash Algorithm 1。 • **SHA256** — Secure Hash Algorithm 2。256 ビット ダイジェストの 4 つのハッシュ関数のセット。 • **SHA384** — Secure Hash Algorithm 2。384 ビット ダイジェストの 4 つのハッシュ関数のセット。 • **SHA512** — Secure Hash Algorithm 2。512 ビット ダイジェストの 4 つのハッシュ関数のセット。 • **MD5** — MD5 メッセージ ダイジェスト アルゴリズム。
キー/再入力キー	認証鍵を入力して確認します。
暗号化 (ESP プロトコルのみ)	以下のいずれかを指定します。 • **3des**（デフォルト）— 56 ビットの 3 つの暗号化鍵を使用する Triple Data Encryption Algorithm（3DES）を適用します。 • **aes-128-cbc** — 128 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard) を適用します。 • **aes-192-cbc** — 192 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard) を適用します。 • **aes-256-cbc** — 256 ビットの暗号化鍵を使用して AES (Advanced Encryption Standard) を適用します。 • **null** — 暗号化は使用されません。
キー/再入力キー	暗号化鍵を入力して確認します。

© 2019 Palo Alto Networks, Inc.

OSPFv3 の Export Rules（エクスポート ルール）タブ

- Network（ネットワーク）> Virtual Router（仮想ルーター）> OSPFv3 > Export Rules（エクスポート ルール）

以下のフィールドを使用して、OSPFv3 ルートをエクスポートします。

OSPFv3 – エクスポート ルール設定	の意味
デフォルト ルートの再配信を許可	OSPF 経由でデフォルト ルートの再配信を許可する場合に選択します。
氏名	再配信プロファイルの名前を選択します。値には IP サブネットまたは有効な再配信プロファイル名を指定する必要があります。
新規パス タイプ	適用するメトリック タイプを選択します。
新規タグ	一致したルート用に 32 ビット値のタグを指定します。
メトリック	（任意）エクスポートされたルートに関連付けられてパス選択に使用されるルート メトリックを指定します (範囲は 1 ~ 65535)。

OSPFv3 の Advanced（詳細）タブ

- Network（ネットワーク）> Virtual Router（仮想ルーター）> OSPFv3 > Advanced（詳細）

以下のフィールドを使用して SPF 計算用トランジット ルーティングを無効にし、OSPFv3 のタイマーとグレースフル リスタートを設定します。

OSPFv3 – 詳細設定	の意味
SPF 計算用トランジット ルーティングを無効にする	このファイアウォールから送信されるルーター LSA に R ビットを設定して、ファイアウォールがアクティブでないことを示す場合に選択します。この状態のファイアウォールはOSPFv3に参加しますが、その他のルーターはトランジットトラフィックを送信しません。この状態でも、ローカルトラフィックは引き続きファイアウォールに転送されます。トラフィックをデバイス周辺に再ルーティングしながらそのファイアウォールにも到達できるため、これはデュアルホームネットワークで保守を行う場合に役立ちます。
タイマー	• **SPF Calculation Delay (sec)**（**SPF** 計算遅延（秒））– これは、新しいトポロジ情報の受信と SPF 計算の情報間で遅延時間を調整できる遅延タイマーです。指定する値が低ければそれだけ OSPF の再収束が速くなります。ファイアウォールとピアリングしているルーターは、収束時間の最適化と同様の方法で調整する必要があります。 • **LSA Interval (sec)**[LSA 間隔 (秒)] – このオプションは、同一 LSA (同一ルーター、同一タイプ、同一 LSA ID) の 2 つのインスタンスの伝送間の最小時間を指定します。RFC 2328 の

© 2019 Palo Alto Networks, Inc.

OSPFv3 – 詳細設定	の意味
	MinLSInterval と同等です。低い値を指定すると、トポロジが変更された場合の再収束時間が短縮されます。
グレースフル リスタート	• **Enable Graceful Restart**[グレースフルリスタートを有効化] - この機能が有効なファイアウォールは、ファイアウォールが一時的にダウンして移行が実行されている間も、ファイアウォールを経由するルートを引き続き使用するように近隣のルーターに指示します（デフォルトで有効）。 • **Enable Helper Mode**[ヘルパーモードを有効化] - このモードが有効なファイアウォールは、隣接デバイスの再起動中もそのデバイスへの転送を継続します（デフォルトで有効）。 • **Enable Strict LSA Checking**[厳密なLSAチェックを有効化] - トポロジが変更された場合、この機能により、OSPFヘルパーモードが有効なファイアウォールのヘルパーモードが終了します（デフォルトで有効）。 • **Grace Period (sec)**（猶予時間（秒））— 隣接デバイスの再確立中またはルーターの再起動中にピア デバイスがこのファイアウォールに向けた転送を継続する秒数です（範囲は 5 ~ 1,800、デフォルトは 120）。 • **Max Neighbor Restart Time**[ネイバー再起動の最大時間] - ファイアウォールをヘルパーモードルーターとして使用できる最大猶予時間（秒）です。ピアデバイスのグレースLSAで提供される猶予時間の方が長い場合、ファイアウォールはヘルパーモードになりません（範囲は5～800、デフォルトは140）。

BGP

- Network > Virtual Router > BGP [ネットワーク > 仮想ルーター > BGP]

Border Gateway Protocol（BGP）では、以下の表の説明に従って BGP の基本設定を指定し、BGP を有効にしてルーター ID と AS 番号を設定する必要があります。また、BGP ピア グループの一部として BGP ピアを設定する必要があります。

ネットワークで必要な場合は、以下のタブで残りの BGP 設定を指定します。

- **General**[一般]:「BGP の General（全般）タブ」を参照してください。
- **Advanced**[詳細]:「BGP の Advanced（詳細）タブ」を参照してください。
- **Peer Group**[ピアグループ]:「BGP の Peer Group（ピア グループ）タブ」を参照してください。
- **Import**[インポート]:「BGP の Import（インポート）および Export（エクスポート）タブ」を参照してください。
- **Export**[エクスポート]:「BGP の Import（インポート）および Export（エクスポート）タブ」を参照してください。
- **Conditional Adv**[条件付き通知]:「BGP の Conditional Adv（条件付き通知）タブ」を参照してください。
- **Aggregate**[集約]:「BGP の Aggregate（集約）タブ」を参照してください。
- **Redist Rules**[ルールの再配信]:「BGP の Redist Rules（再配信ルール）タブ」を参照してください。

BGP の基本設定

仮想ルーターで BGP を使用するには、BGP を有効にしてルーター ID と AS 番号を設定する必要があります。BFD の有効化は任意です。

© 2019 Palo Alto Networks, Inc.

BGP 設定	設定場所	の意味
Enable [有効化]	**BGP**	BGP を有効にする場合に選択します。
ルーターID		仮想ルーターに割り当てる IP アドレスを入力します。
AS 番号		ルーターID に基づいて、仮想ルーターが属する AS の番号を入力します (範囲は 1 ~ 4,294,967,295)。
BFD		PA-5200 Series、PA-7000 Series、またはVM-Seriesファイアウォールの仮想ルーターで、BGP用の双方向フォワーディングの検出（BFD）をグローバルに有効化する場合は、以下のうちから一つを選択します。 • **default**（デフォルトのBFD設定） • ファイアウォールの既存の BFD プロファイル • 新しい **BFD** プロファイルの作成 すべてのBGPインターフェイスでBFDを無効化する場合は**None (Disable BFD)**[なし（BFD無効）]を選択します。シングルBGPのインターフェイスでは、BFDを無効化することができません。 グローバルに *BFD* を有効化あるいは無効化する場合、*BGP* を実行中のすべてのインターフェイスが停止され、*BFD* の機能で再起動されます。これにより、*BGP* トラフィックが中断される可能性があります。よって、*BGP* インターフェイスで *BFD* を有効化する場合は、このような再収斂が実働トラフィックに影響を与えないようなオフピーク時に行うようにしてください。

BGP の General（全般）タブ

- Network > Virtual Router > BGP > General [ネットワーク > 仮想ルーター > BGP > 全般]

以下のフィールドを使用して、BGP の全般設定を指定します。

BGP の全般設定	設定場所	の意味
デフォルトルートの拒否	**BGP** > **General**	BGP ピアから通知されるデフォルト ルートを無視する場合に選択します。
ルートのインストール		グローバル ルーティング テーブルに BGP ルートをインストールする場合に選択します。
MED の集約		ルートの MED (Multi-Exit Discriminator) 値が異なる場合でもルート集約を有効にするには、オンにします。
デフォルトローカル設定		異なるパスで設定を決定するためにファイアウォールで使用できる値を指定します。

© 2019 Palo Alto Networks, Inc.

BGP の全般設定	設定場所	の意味
ASフォーマット		2-byte [2 バイト] (デフォルト) または 4-byte [4 バイト] 形式を選択します。これは、相互運用性のために設定します。
常に MED を比較		別の AS 内のネイバーから受け取ったパスの MED 比較を有効にします。
決定論的 MED 比較		iBGP ピア (同じ AS 内の BGP ピア) から通知されたルートの中からルートを選択するための MED 比較を有効にします。
認証プロファイル		新しい認証プロファイルを **Add** (追加) し、以下の設定を指定します。 • **Profile Name**[プロファイル名] – プロファイルの識別に使用する名前を入力します。 • **Secret/Confirm Secret**[シークレット/再入力 シークレット] – BGP ピア通信に使用するパスフレーズを入力し、確認します。 不要になったプロファイルは削除 (⊖) します。

BGP の Advanced (詳細) タブ

- Network > Virtual Router > BGP > Advanced [ネットワーク > 仮想ルーター > BGP > 詳細]

BGP の詳細設定には、さまざまな機能が含まれます。複数の BGP AS で ECMP を実行できます。(更新パケットのなりすましを防止するために) AS_PATH 属性の最初の AS として各自の AS をリストするように eBGP ピア に要求できます。BGP グレースフル リスタートを設定できます。これは、ルート フラッピング (増減) の影響を最小限に抑えるために BGP の再起動中に転送状態を BGP ピアで保持できるかどうかを示す方法です。AS の BGP ピアリングがフル メッシュにならないように、ルート リフレクタと AS コンフェデレーションを設定できます。ルート ダンペニングを設定して、BGP ネットワークが不安定な場合やルートがフラッピングしている場合に不要なルーターの収束を回避できます。

BGP の詳細設定	設定場所	の意味
ECMP の複数の AS のサポート	**BGP** > **Advanced**	仮想ルーターの ECMP を有効にして、複数の BGP AS で ECMP を実行できるようにする場合に選択します。
EBGP 用の First AS の実施		ファイアウォールは、AS_PATH 属性の最初の AS として eBGP ピアの各自の AS 番号をリストしていない eBGP ピアからの受信更新パケットをドロップします。これにより、隣接する AS 以外の AS から送信されたなりすまし更新パケットや誤った更新パケットが BGP でこれ以上処理されることを回避できます。デフォルトで有効になっています。
グレースフル リスタート		グレースフル リスタート オプションをアクティベーションします。 • **Stale Route Time**[ルート停滞時間] - ルートが膠着状態を持続できる時間を指定します (範囲は1 ~ 3600 秒、デフォルトは120秒)。 • **Local Restart Time**[ローカル再起動時間] - ファイアウォールの再起動にかかる秒数を指定します。この値はピアに通知されます (範囲は1 ~ 3600、デフォルトは120)。

© 2019 Palo Alto Networks, Inc.

BGP の詳細設定	設定場所	の意味
		• **Max Peer Restart Time**[最大ピア再起動時間] - ファイアウォールがピアデバイス再起動時の猶予時間として許容する最大秒数を指定します (範囲は1 ~ 3600 秒、デフォルトは120秒)。
リフレクタ クラスタ ID		リフレクタ クラスタを示す IPv4 識別子を指定します。AS のルート リフレクタ (ルーター) は、学習したルートをそのピアに再通知します。そのため、フル メッシュ接続ですべてのピアがルートを相互に通知する必要はありません。ルート リフレクタにより、設定が簡略化されます。
コンフェデレーション メンバー AS		BGP コンフェデレーション内でのみ表示される AS 番号の識別子 (サブ AS 番号とも呼ばれます) を指定します。BGP コンフェデレーションを使用して AS をサブ AS に分割し、フル メッシュ ピアリングを削減します。
プロファイルのダンペニング	**BGP** > **Advanced (cont)**	ルート ダンペニングは、フラッピングしているルートの通知を停止するかどうかを判断する方法です。ルート ダンペニングにより、ルート フラッピングに起因するルーターの再収束の回数を削減できます。以下の設定があります。 • **Profile Name**[プロファイル名] – プロファイルの識別に使用する名前を入力します。 • **Enable**[有効化] – プロファイルをアクティベーションします。 • **Cutoff**[カットオフ] - ルート停止のしきい値を指定し、この値を超えるとルート通知が停止されるようにします (範囲は0.0 ~ 1000.0、デフォルトは1.25)。 • **Reuse**[再利用] – ルート停止のしきい値を指定します (範囲は 0.0 ~ 1000.0、デフォルトは 5)。この値を下回るとルートは再度使用されます。 • **Max.Max. Hold Time**[最大ホールドタイム] – ルートの不安定度に関係なく、ルートを停止できる時間の最大長を指定します (範囲は 0 ~ 3600 秒、デフォルトは 900 秒)。 • **Decay Half Life Reachable** (到達可能のライフ半減) – ファイアウォールでルートが到達可能とみなされてから、ルートの安定性メトリックを 1/2 にするまでの時間を指定します (範囲は 0 ~ 3600 秒、デフォルトは 300 秒) 。 • **Decay Half Life Unreachable** (到達不能のライフ半減) – ファイアウォールでルートが到達不能とみなされてから、ルートの安定性メトリックを 1/2 にするまでの時間を指定します (範囲は 0 ~ 3600 秒、デフォルトは 300 秒) 。 不要になったプロファイルは削除 (⊖) します。

BGP の Peer Group (ピア グループ) タブ

- Network > Virtual Router > BGP > Peer Group [ネットワーク > 仮想ルーター > BGP > ピア グループ]

BGP ピア グループは、ピア グループのタイプ (例: EBGP) などの設定や、仮想ルーターが更新パケットで送信する AS_PATH リストからプライベート AS 番号を削除するための設定を共有する一連の BGP ピアです。BGP ピア グループにより、同じ設定のピアを複数設定する必要がなくなります。グループに属する BGP ピアを設定するには、1 つ以上の BGP ピア グループを設定する必要があります。

© 2019 Palo Alto Networks, Inc.

BGP ピア グループ設定	設定場所	の意味
氏名	**BGP** > **Peer Group**	ピア グループの識別に使用する名前を入力します。
Enable [有効化]		ピア グループをアクティベーションする場合に選択します。
集約済みコンフェデレーション AS パス		設定した集約済みコンフェデレーション AS へのパスを含める場合に選択します。
Soft Reset with Stored Info（保存した情報を使用したソフト リセット）		ピア設定の更新後にファイアウォールのソフト リセットを実行する場合に選択します。

タイプ		ピアまたはグループのタイプを指定し、関連設定を指定します (この表に後述されている**Import Next Hop** [ネクストホップのインポート] および**Export Next Hop** [ネクストホップのエクスポート] の説明を参照)。
		• **IBGP** — 以下を指定します。
		  • ネクスト ホップのエクスポート
		• **EBGP Confed**[EBGPコンフェデレーション] — 以下を指定します。
		  • ネクスト ホップのエクスポート
		• **IBGP Confed**[IBGPコンフェデレーション] — 以下を指定します。
		  • ネクスト ホップのエクスポート
		• **EBGP** — 以下を指定します。
		  • ネクスト ホップのインポート
		  • ネクスト ホップのエクスポート
		  • **Remove Private AS**（プライベート **AS** の削除）（BGP で AS_PATH 属性からプライベート AS 番号を強制的に削除する場合に選択します）。

ネクスト ホップのインポート		ネクストホップのインポートのオプションを選択します。 • **Original**（オリジナル） — 元のルート通知で提供されたネクスト ホップ アドレスを使用します。 • **Use Peer**（ピアの使用） — ピアの IP アドレスをネクスト ホップ アドレスとして使用します。
ネクスト ホップのエクスポート		ネクストホップのエクスポートのオプションを選択します。 • **Resolve**（解決） — 転送情報ベース（FIB）を使用してネクスト ホップ アドレスを解決します。 • **Original**（オリジナル） — 元のルート通知で提供されたネクスト ホップ アドレスを使用します。 • **Use Self**（自己の使用） — ネクスト ホップ アドレスを仮想ルーターの IP アドレスで置き換えて転送パスに含まれるようにします。

© 2019 Palo Alto Networks, Inc.

BGP ピア グループ設定	設定場所	の意味
プライベート AS の削除		AS_PATH リストからプライベート AS を削除する場合に選択します。
氏名	**BGP** > **Peer Group** > **Peer**	新しい BGP ピアを追加し、識別に使用する名前を入力します。
Enable [有効化]		ピアをアクティベーションするには、オンにします。
ピア AS		ピアの AS を指定します。
MP-BGP 拡張の有効化	**BGP** > **Peer Group**（ピア グループ）> **Peer**（ピア）> **Addressing**（アドレス）	ファイアウォールで RFC 4760 に従って IPv4 および IPv6 の Multiprotocol BGP Address Family Identifier（マルチプロトコル BGP アドレス ファミリー ID）オプションと Subsequent Address Family Identifier（後続のアドレス ファミリー ID）オプションをサポートできるようになります。
アドレス ファミリー タイプ		このピアの BGP セッションでサポートされるアドレス ファミリー（**IPv4** または **IPv6**）を選択します。
後続のアドレス ファミリー		このピアの BGP セッションで使用される後続のアドレス ファミリー プロトコル（**Unicast**（ユニキャスト）または **Multicast**（マルチキャスト））を選択します。
ローカル アドレス – インターフェイス		ファイアウォール インターフェイスを選択します。
ローカル アドレス – IP		ローカル IP アドレスを選択します。
ピア アドレス–タイプおよびアドレス		ピアを識別するアドレスのタイプを選択します： • **IP**–IP を選択し、さらに IP アドレスを使用するアドレス オブジェクトを選択（あるいは IP アドレスを使用するアドレス オブジェクトを新たに作成）します。 • **FQDN**–FQDN を選択し、さらに FQDN を使用するアドレス オブジェクトを選択（あるいは FQDN を使用するアドレス オブジェクトを新たに作成）します。
認証プロファイル	**BGP** > **Peer Group**（ピア グループ）> **Peer**（ピア）> **Connection Options**（接続オプション）	プロファイルを選択するか、ドロップダウンから **New Auth Profile**（新規認証プロファイル）を選択します。プロファイルの**Name**（名前）、**Secret**（シークレット）、**Confirm Secret**（再入力シークレット）を入力します。
キープ アライブ間隔		ピアから受け取ったルートがホールド タイム設定に従って停止されるまでの時間を指定します（範囲は 0 ~ 1,200 秒、デフォルトは 30 秒）。
マルチ ホップ		IP ヘッダーのtime-to-live (Time-To-Live - TTL) 値を設定します。範囲は 0 ~ 255 です。デフォルト値の 0 は、eBGP の1、iBGP の 255 を意味します。

© 2019 Palo Alto Networks, Inc.

BGP ピア グループ設定	設定場所	の意味
オープン遅延時間		ピア TCP 接続を開いてから最初の BGP Open メッセージを送信するまでの遅延時間を指定します (範囲は 0 ~ 240 秒、デフォルトは 0 秒)。
ホールドタイム		ピアからの連続する KEEPALIVE または UPDATE メッセージ間の想定経過時間を指定します。この時間が過ぎるとピア接続が閉じられます (範囲は 3 ~ 3,600 秒、デフォルトは 90 秒)。
アイドル ホールド タイム		アイドル状態で待機する時間を指定します。この時間が経過すると、ピアへの接続が再試行されます (範囲は 1 ~ 3,600 秒、デフォルトは 15 秒)。
受信接続 – リモート ポート		受信ポート番号を指定し、このポートへのトラフィックを **Allow** (許可) します。
送信接続 – ローカル ポート		送信ポート番号を指定し、このポートからのトラフィックを **Allow** (許可) します。
リフレクタ クライアント	**BGP** > **Peer Group** > **Peer** > **Advanced**	リフレクタ クライアントのタイプを選択します (**Non-Client** (非クライアント)、**Client** (クライアント)、**Meshed Client** (メッシュ クライアント) のいずれか)。リフレクタ クライアントから受信したルートは、すべての内部および外部 BGP ピアで共有されます。
ピアリング タイプ		双方向ピアを指定するか、未指定のままにします。
最大プレフィックス		サポートされる IP プレフィックスの最大数を指定します (1 ~ 100,000 または無制限)。
送信側ループ検出の有効化		ファイアウォールで更新でルートを送信する前に FIB のルートの AS_PATH 属性をチェックし、ピア AS 番号が AS_PATH リストにないことを確認できます。リストにある場合、ファイアウォールで削除してループを回避できます。通常、受信側がループ検出を実行しますが、この最適化機能により送信側がループ検出を実行するようになります。
BFD		BGP ピアで双方向フォワーディングの検出 (BFD) を使用する際は (仮想ルーターのレベルで BGP 用の **BFD** が無効化されていない限り、BGP 用の **BFD** 設定をオーバーライドすることになります)、グローバル BGP BFD プロファイルを引き継ぐ場合は既存の BFD プロファイルであるデフォルト プロファイル (デフォルトの BFD 設定) **Inherit-vr-global-setting** を選択し、新しい BFD プロファイルを作成する場合は **New BFD Profile** (新規 **BFD** プロファイル) を選択します。**None (Disable BFD)**[なし (BFD無効)] を選択すると、BGPピアのBFDが無効化されます。 グローバルに*BFD*を有効化あるいは無効化する場合、*BGP*を実行中のすべてのインターフェイスが停止され、*BFD*の機能で再起動されます。これにより、すべての*BGP*トラフィックが中断される可能性があ

© 2019 Palo Alto Networks, Inc.

BGP ピア グループ設定	設定場所	の意味
		ります。インターフェイス上で*BFD*を有効化すると、ファイアウォールがピアとの*BGP*接続を停止し、インターフェイス上で*BFD*のプログラミングを行います。*BGP*接続が停止されたことをピアデバイスが検知すると、実働トラフィックに影響を与える再収斂を行う可能性があります。よって、*BGP*インターフェイスで*BFD*を有効化する場合は、このような再収斂が実働トラフィックに影響を与えないようなオフピーク時におこなうようにしてください。

BGP の *Import*（インポート）および *Export*（エクスポート）タブ

- Network > Virtual Router > BGP > Import[ネットワーク > 仮想ルーター > BGP > インポート]
- Network > Virtual Router > BGP > Export [ネットワーク > 仮想ルーター > BGP > エクスポート]

BGP ルートをインポートまたはエクスポートする新しいインポート ルールまたはエクスポート ルールを **Add**（追加）します。

BGP のインポートおよびエクスポート設定	設定場所	の意味
ルール	**BGP** > **Import**（インポート）または **Export**（エクスポート）> **General**（全般）	ルールの識別に使用する名前を指定します。
Enable [有効化]		ルールをアクティベーションする場合に選択します。
Used By [使用者]		このルールを使用するピア グループを選択します。
AS パスの正規表現	**BGP** > **Import**（インポート）または **Export**（エクスポート）> **Match**（一致）	AS パスをフィルタリングするための正規表現を指定します。
コミュニティの正規表現		コミュニティ文字列をフィルタリングするための正規表現を指定します。
拡張コミュニティの正規表現		拡張コミュニティ文字列をフィルタリングするための正規表現を指定します。
MED		ルートをフィルタリングするための Multi-Exit Discriminator 値を 0 ~ 4、294、967、295 の範囲で指定します。
ルート テーブル		**Import Rule**（インポート ルール）では、一致するルートのインポート先のルート テーブル（ **unicast**, **multicast**, or **both**. ） **Export Rule**（エクスポート ルール）では、一致するルートのエクスポート先のルート テーブル。**unicast**, **multicast**, or **both**.

© 2019 Palo Alto Networks, Inc.

BGP のインポートおよびエクスポート設定	設定場所	の意味
アドレス プレフィックス		ルートをフィルタリングするための IP アドレスまたはプレフィックスを指定します。
ネクストホップ		ルートをフィルタリングするためのネクスト ホップ ルーターまたはサブネットを指定します。
送信元ピア		ルートをフィルタリングするためのピア ルーターを指定します。
操作	**BGP** > **Import**（インポート）または **Export**（エクスポート）> **Action**（アクション）	照合条件を満たしたときに実行するアクション（**Allow**（許可）または **Deny**（拒否））を指定します。
ダンペニング		アクションが **Allow**（許可）の場合のみ、ダンペニング パラメータを指定します。
ローカル設定		アクションが **Allow**（許可）の場合のみ、ローカル優先メトリックを指定します。
MED		アクションが **Allow**（許可）の場合のみ、MED 値を指定します（0 ~ 65,535）。
重み		アクションが **Allow**（許可）の場合のみ、重み値を指定します（0 ~ 65,535）。
ネクストホップ		アクションが **Allow**（許可）の場合のみ、ネクスト ホップ ルーターを指定します。
元		基となるルートのパス タイプを指定します。IGP、EGP、また動作設定が**Allow**[許可]となっている場合のみ、incomplete [不完全] から選択します。
AS パス制限		アクションが **Allow**（許可）の場合のみ、AS パス制限を指定します。
AS パス		AS パスを指定します。動作設定が**Allow**[許可]となっている場合のみ、ASパスに**None** [なし]、**Remove**[削除]、**Prepend**[プリペンド]、**Remove and Prepend**[削除およびプリペンド] のいずれかを指定します。
コミュニティ		コミュニティ オプションを指定します。動作設定が**Allow** [許可] の場合のみ、コミュニティオプションに**None**[なし]、**Remove All**[すべて削除]、**Remove Regex**[正規表現の削除]、**Append**[付加]、**Overwrite**[上書き] のいずれかを指定します。
拡張コミュニティ		コミュニティ オプションを指定します。動作設定が**Allow** [許可] の場合のみ、コミュニティオプションに**None**[なし]、**Remove All**[すべて削除]、**Remove Regex**[正規表現の削除]、**Append**[付加]、**Overwrite**[上書き] のいずれかを指定します。
		不要になったルールは **Delete**（削除）⊖ します。また、必要に応じてルールを **Clone**（コピー）します。ルールを選択して **Move Up**（上

© 2019 Palo Alto Networks, Inc.

BGP のインポートおよびエクスポート設定	設定場所	の意味
		へ）または **Move Down**（下へ）を選択し、順序を変更することもできます。

BGP の Conditional Adv（条件付き通知）タブ

- Network > Virtual Router > BGP > Conditional Adv [ネットワーク > 仮想ルーター > BGP > 条件付き通知]

BGP 条件付き通知では、ピアリングまたは到達の失敗を含め、ローカル BGP ルーティング テーブル（LocRIB）で優先ルートを使用できない場合に通知するルートを制御できます。これは、1 つの AS を別の AS より優先してルートを強制する場合に便利です。たとえば、インターネットに対して複数の ISP を経由するリンクがあり、優先プロバイダへの接続が失われない限り、他のプロバイダではなく優先プロバイダにトラフィックをルーティングする場合に有用です。

条件付き通知では、優先ルート（**Address Prefix**（アドレス プレフィックス））と、優先ルートを識別する他の属性（AS Path Regular Expression（AS パスの正規表現）など）を指定する非存在フィルタを設定します。非存在フィルタと一致するルートがローカル BGP ルーティング テーブルで見つからない場合にのみ、ファイアウォールは通知フィルタで指定された代替ルート（他の非優先プロバイダへのルート）の通知を許可します。

条件付き通知を設定するには、**Conditional Adv**（条件付き通知）タブを選択して、条件付き通知を **Add**（追加）し、以下の表の説明に従って値を設定します。

BGP の条件付き通知設定	設定場所	の意味
Policy [ポリシー]	**BG** > **P** の **Conditional Adv**（条件付き通知）タブ	この条件付き通知ポリシー ルールの名前を指定します。
Enable [有効化]		この条件付き通知ポリシー ルールを有効にする場合に選択します。
Used By [使用者]		この条件付き通知ポリシー ルールを使用するピア グループを **Add**（追加）します。
Non Exist Filter（非存在フィルタ）	**BGP** > **Conditional Adv**（条件付き通知）> **Non Exist Filters**（非存在フィルタ）	優先ルートのプレフィックスを指定するには、このタブを使用します。このタブは、ローカル BGP ルーティング テーブルで使用可能な場合に通知するルートを指定します。プレフィックスが通知され非存在フィルタと一致すると、通知が停止します。 非存在フィルタを **Add**（追加）して、このフィルタの識別に使用する名前を指定します。
Enable [有効化]		非存在フィルタをアクティベーションする場合に選択します。
AS パスの正規表現		AS パスをフィルタリングするための正規表現を指定します。
コミュニティの正規表現		コミュニティ文字列をフィルタリングするための正規表現を指定します。

© 2019 Palo Alto Networks, Inc.

BGP の条件付き通知設定	設定場所	の意味
拡張コミュニティの正規表現		拡張コミュニティ文字列をフィルタリングするための正規表現を指定します。
MED		ルートをフィルタリングするための MED 値を指定します（範囲は 0 ～ 4、294、967、295）。
ルート テーブル		一致するルートが存在するかどうかを確認するためにファイアウォールで検索するルート テーブル（**unicast**（ユニキャスト）、**multicast**（マルチキャスト）、**both**（両方））を指定します。一致するルートがそのルート テーブルに存在しない場合にのみ、ファイアウォールは代替ルートの通知を許可します。
アドレス プレフィックス		優先ルートの正確な Network Layer Reachability Information（NLRI）プレフィックスを **Add**（追加）します。
ネクストホップ		ルートをフィルタリングするためのネクスト ホップ ルーターまたはサブネットを指定します。
送信元ピア		ルートをフィルタリングするためのピア ルーターを指定します。
Advertise Filters（通知フィルタ）	**BGP** > **Conditional Adv**（条件付き通知）> **Advertise Filters**（通知フィルタ）	非存在フィルタのルートがローカル ルーティング テーブルで使用できない場合に通知する、ローカル RIB ルーティング テーブルのルートのプレフィックスを指定するには、このタブを使用します。 通知されるプレフィックスが非存在フィルタと一致しないと、通知が行われます。 通知フィルタを **Add**（追加）して、このフィルタの識別に使用する名前を指定します。
Enable [有効化]		フィルタをアクティベーションする場合に選択します。
AS パスの正規表現		AS パスをフィルタリングするための正規表現を指定します。
コミュニティの正規表現		コミュニティ文字列をフィルタリングするための正規表現を指定します。
拡張コミュニティの正規表現		拡張コミュニティ文字列をフィルタリングするための正規表現を指定します。
MED		ルートをフィルタリングするための MED 値を指定します（範囲は 0 ～ 4、294、967、295）。
ルート テーブル		一致するルートが条件付きで通知される場一致するルートが条件付きで通知される場合にファイアウォールで使用するルート テーブル：**unicast**, **multicast**, or **both**.合にファイアウォールで使用するルート テーブル：

© 2019 Palo Alto Networks, Inc.

BGP の条件付き通知設定	設定場所	の意味
アドレス プレフィックス		優先ルートを使用できない場合に通知するルートの正確な Network Layer Reachability Information（NLRI）プレフィックスを **Add**（追加）します。
ネクストホップ		ルートをフィルタリングするためのネクスト ホップ ルーターまたはサブネットを指定します。
送信元ピア		ルートをフィルタリングするためのピア ルーターを指定します。

BGP の Aggregate（集約）タブ

- Network > Virtual Router > BGP > Aggregate [ネットワーク > 仮想ルーター > BGP > 集約]

ルート集約は、特定のルート（プレフィックス長が長いルート）を 1 つのルート（プレフィックス長が短いルート）にまとめて、ファイアウォールで送信する必要のあるルーティング通知を削減し、ルート テーブルのルートを少なくする操作です。

BGP の集約設定	設定場所	の意味
氏名	**BGP** > の **Aggregate**（集約）タブ	集約ルールの名前を入力します。
プレフィックス		長いプレフィックスを集約するために使用されるサマリー プレフィックス（IP アドレス/プレフィックス長）を入力します。
Enable [有効化]		ルートのこの集約を有効にする場合に選択します。
概要		ルートを要約する場合に選択します。
AS セット		この集約ルールを対象としてファイアウォールで集約ルートの AS パスに一連の AS 番号（AS セット）を含める場合に選択します。AS セットは、集約された個々のルートの元の AS 番号の順不同リストです。
氏名	**BGP** > **Aggregate**（集約）> **Suppress Filters**（停止フィルタ）	一致したルートを停止する属性を定義します。停止フィルタを **Add**（追加）して名前を入力します。
Enable [有効化]		停止フィルタを有効にする場合に選択します。
AS パスの正規表現		集約するルートをフィルタリングするための AS_PATH の正規表現を指定します。たとえば、^5000 は AS 5000 から学習したルートを意味します。
コミュニティの正規表現		集約するルートをフィルタリングするためのコミュニティの正規表現を指定します。たとえば、500:.* は 500:x が含まれるコミュニティに一致します。
拡張コミュニティの正規表現		集約するルートをフィルタリングするための拡張コミュニティの正規表現を指定します。
MED		集約するルートをフィルタリングする MED を指定します。

© 2019 Palo Alto Networks, Inc.

BGP の集約設定	設定場所	の意味
ルート テーブル		停止する（通知しない）集約ルートに使用するルート テーブル（**unicast**（ユニキャスト）、**multicast**（マルチキャスト）、または**both**（両方））を指定します。
アドレス プレフィックス		通知を停止する IP アドレスを入力します。
ネクストホップ		停止する BGP プレフィックスのネクスト ホップ アドレスを入力します。
送信元ピア		（停止する）BGP プレフィックスの受信元ピアの IP アドレスを入力します。
氏名	**BGP** > **Aggregate**（集約）> **Advertise Filters**（通知フィルタ）	フィルタに一致するルートをファイアウォールからピアに通知する通知フィルタの属性を定義します。**Add**（追加）をクリックし、通知フィルタの名前を入力します。
Enable [有効化]		通知フィルタを有効にする場合に選択します。
AS パスの正規表現		通知するルートをフィルタリングするための AS_PATH の正規表現を指定します。
コミュニティの正規表現		通知するルートをフィルタリングするためのコミュニティの正規表現を指定します。
拡張コミュニティの正規表現		通知するルートをフィルタリングするための拡張コミュニティの正規表現を指定します。
MED		通知するルートをフィルタリングするための MED 値を指定します。
ルート テーブル		集約ルートの通知フィルタに使用するルート テーブル（**unicast**（ユニキャスト）、**multicast**（マルチキャスト）、または**both**（両方））を指定します。
アドレス プレフィックス		BGP で通知する IP アドレスを入力します。
ネクストホップ		BGP で通知する IP アドレスのネクスト ホップ アドレスを入力します。
送信元ピア		BGP で通知する、プレフィックスの受信元ピアの IP アドレスを入力します。
	BGP > **Aggregate**（集約）> **Aggregate Route Attributes**（集約ルート属性）	集約ルートの属性を定義します。
ローカル設定		範囲が 0 ~ 4、294、967、295 のローカル設定。
MED		範囲が 0 ~ 4、294、967、295 の Multi Exit Discriminator。
重み		範囲が 0 ~ 65,535 の重み。

© 2019 Palo Alto Networks, Inc.

BGP の集約設定	設定場所	の意味
ネクストホップ		ネクスト ホップ IP アドレス。
元		ルートの元:**igp**、**egp**、または**incomplete**。
AS パス制限		範囲が 1 ~ 255 の AS パス制限。
AS パス		タイプを選択します。**None**（なし）または **Prepend**（プリペンド）。
コミュニティ		タイプを選択します。**None**（なし）、**Remove All**（すべて削除）、**Remove Regex**（正規表現の削除）、**Append**（付加）、**Overwrite**（上書き）。
拡張コミュニティ		タイプを選択します。**None**（なし）、**Remove All**（すべて削除）、**Remove Regex**（正規表現の削除）、**Append**（付加）、**Overwrite**（上書き）。

BGP の Redist Rules（再配信ルール）タブ

- Network > Virtual Router > BGP > Redist Rules [ネットワーク > 仮想ルーター > BGP > ルールの再配信]

以下の表の説明に従って設定を指定し、BGP ルートを再配信するためのルールを作成します。

BGP の再配信ルール設定	設定場所	の意味
デフォルトルートの再配信を許可	**BGP** > の **Redist Rules**（再配信ルール）タブ	ファイアウォールから BGP ピアにデフォルト ルートを再配信することを許可します。
氏名		最初に IP サブネットを **Add**（追加）するか再配信ルールを作成します。
Enable [有効化]		この再配信ルールを有効にする場合に選択します。
ルート テーブル		ルートの再配信先のルート テーブル（**unicast**（ユニキャスト）、**multicast**（マルチキャスト）、または**both**（両方））を指定します。
メトリック		1 ~ 65,535 の範囲でメトリックを入力します。
発信元の設定		再配信されるルートの発信元（**igp**、**egp**、または **incomplete**（不完全）を選択します。**incomplete**（不完全）の値は、接続済みルートを示します。
MED の設定		再配信されるルートの MED を 0 ~ 4、294、967、295 の範囲で入力します。
ローカル設定		再配信されるルートのローカル設定を 0 ~ 4、294、967、295 の範囲で入力します。

© 2019 Palo Alto Networks, Inc.

BGP の再配信ルール設定	設定場所	の意味
AS パス制限の設定		再配信されるルートの AS パス制限を 1 ~ 255 の範囲で入力します。
コミュニティの設定		10 進数または 16 進数、あるいは AS:VAL のフォーマットで 32 ビットの値を選択するか入力します。AS と VAL はそれぞれ 0 から 65,535 までの範囲の値です。最大 10 個のコミュニティを入力します。
拡張コミュニティの設定		16 進数、TYPE:AS:VAL または TYPE:IP:VAL のフォーマットで 64 ビットの値を力します。TYPE は 16 ビット、AS や IP は 16 ビット、VAL は 32 ビットです。最大 5 個の拡張コミュニティを入力します。

IP マルチキャスト

- Network > Virtual Router > Multicast [ネットワーク > 仮想ルーター > マルチキャスト]

マルチキャストプロトコルを設定する場合は、以下の標準設定を指定する必要があります。

マルチキャスト設定	の意味
Enable [有効化]	マルチキャスト ルーティングを有効化する場合に選択します。

さらに、以下のタブの設定を指定する必要があります。

- **Rendezvous Point**[ランデブーポイント]:「Multicast Rendezvous Point Tab (マルチキャストの Rendezvous Point (ランデブー ポイント) タブ)」を参照してください。
- **Interfaces**[インターフェイス]:「Multicast Interfaces Tab (マルチキャストの Interfaces (インターフェイス) タブ)」を参照してください。
- **SPT Threshold**[SPTしきい値]:「Multicast SPT Threshold Tab (マルチキャストの SPT Threshold (SPT しきい値) タブ)」を参照してください。
- **Source Specific Address Space**[送信元固有のアドレススペース]:「Multicast Source Specific Address Tab (マルチキャストの Source Specific Address (送信元固有のアドレス) タブ)」を参照してください。
- **Advanced**[詳細]:「Multicast Advanced Tab (マルチキャストの Advanced (詳細) タブ)」を参照してください。

マルチキャストの *Rendezvous Point* (ランデブー ポイント) タブ

- Network > Virtual Router > Multicast > Rendezvous Point [ネットワーク > 仮想ルーター > ランデブー ポイント]

以下のフィールドを使用して、IP マルチキャストのランデブー ポイントを設定します。

マルチキャスト設定 – ランデブー ポイント	の意味
RP タイプ	この仮想ルーターで実行するランデブー ポイント (RP) のタイプを選択します。静的 RP は、他の PIM ルータで明示的に設定する必要がありますが、候補 RP は自動的に選択されます。

© 2019 Palo Alto Networks, Inc.

マルチキャスト設定 – ランデブー ポイント	の意味

	• **None (なし)** — この仮想ルーターで実行中の RP がない場合に選択します。
	• **Static**[静的] — RP用のスタティックIPアドレスを指定し、ドロップダウンリストから **RP Interface**[RPインターフェイス] および **RP Address**[RPアドレス] のタイプを選択します。このグループ用に選択したRPではなく指定したRPを使用する場合は、**Override learned RP for the same group**[取得した同じグループの RP のオーバーライド] を選択します。
	• **Candidate**[候補] — この仮想ルーターで実行中の RP 候補に以下の情報を指定します。
	  • **RP Interface**[RP インターフェイス] — RP のインターフェイスを選択します。有効なインターフェイス タイプとしてループバック、L3、VLAN、Aggregate Ethernet、トンネルなどがあります。
	  • **RP Address**[RP アドレス] — RP の IP アドレスを選択します。
	  • **Priority**[優先順位] — 候補 RP メッセージの優先度を指定します (デフォルトは 192)。
	  • **Advertisement interval**[通知間隔] — 候補 RP メッセージの通知間隔を指定します。
	• **Group list**[グループ リスト] — **Static**[静的] または **Candidate**[候補] を選択した場合、**Add**[追加] をクリックし、RP の候補となるグループのリストを指定します。

リモート ランデブー ポイント	**Add**[追加] をクリックし、以下を指定します。 • **IP address**[IP アドレス] — RP の IP アドレスを指定します。 • **Override learned RP for the same group** (取得した同じグループの **RP** のオーバーライド) — このグループで選ばれた RP ではなく指定した RP を使用する場合に選択します。 • **Group**[グループ] — 指定したアドレスが RP として機能するグループのリストを指定します。

マルチキャストの *Interfaces* (インターフェイス) タブ

- Network > Virtual Router > Multicast > Interfaces [ネットワーク > 仮想ルーター > マルチキャスト > インターフェイス]

次のフィールドを使用して、IGMP、PIM、およびグループアクセス権設定を共有するマルチキャスト インターフェイスを設定します。

マルチキャスト設定 – インターフェイス	の意味
氏名	インターフェイス グループの識別に使用する名前を入力します。
の意味	任意の説明を入力します。
インターフェイス	インターフェイス グループに属する 1 つ以上のファイアウォール インターフェイスを **Add** (追加) し、マルチキャスト グループのアクセス許可、IGMP 設定、および PIM 設定を共有します。

© 2019 Palo Alto Networks, Inc.

マルチキャスト設定 – インターフェイス	の意味
グループ許可	PIM Any-Source Multicast（ASM）または PIM Source-Specific Multicast（SSM）に参加するマルチキャスト グループを指定します。 • **Any Source**（いずれかの送信元）– **Group**（グループ）インターフェイス グループ内のインターフェイス上のいずれかの送信元からのマルチキャスト トラフィックを受信できるマルチキャストグループを識別する **Name**（名前）を **Add**（追加）します。デフォルトでは、グループは**Any Source**（いずれかの送信元）リストに **Included**（追加済み）です。グループ設定を削除せずにグループを簡単に除外するには、**Included**（追加済み）の選択を解除します。 • **Source Specific**（ソース指定）–インターフェイス グループ内のインターフェイスでマルチキャスト トラフィックが許可されているマルチキャスト **Group**（グループ）と **Source**（送信元）IP アドレスの組の **Name**（名前）を **Add**（追加）します。デフォルトでは、グループと送信元はソース指定のリストに **Included**（追加済み）です。グループとソースのペアを構成を削除せずに簡単に除外するには、 **Included**（追加済み）の選択を解除します。

IGMP	IGMP トラフィックの設定を指定します。マルチ キャスト レシーバ対向インターフェイスの場合は、IGMP を有効にする必要があります。
	• **Enable**（有効化） – IGMP 設定を有効にする場合に選択します。
	• **IGMP Version**[IGMP バージョン] – インターフェイスで実行するバージョン (1、2、または 3) を選択します。
	• **Enforce Router-Alert IP Option**（ルーター アラート **IP** オプションの適用）– IGMPv2 または IGMPv3 の場合にルーター アラート IP オプションを要求するには、このオプションを選択します。IGMPv1 との互換性を確保するには、これを無効にする必要があります。
	• **Robustness**（頑強性） – ネットワーク上のパケット損失を考慮するための整数値を選択します (範囲は 1 ~ 7、デフォルトは 2) 。パケット損失が頻繁に発生する場合は高い値を選択します。
	• **Max Sources**（最大ソース） – このインターフェイス グループで許可する送信元特定メンバシップの最大数を指定します（範囲は 1 ~ 65,535 または **unlimited**（無制限））。
	• **Max Groups**（最大グループ） – このインターフェイス グループで許可するマルチキャスト グループの最大数を指定します（範囲は 1 ~ 65,535 または **unlimited**（無制限））。
	• **Query Configuration** – 以下を指定します。
	  • **Query interval**（クエリ間隔） – 一般的なクエリと受信者からの応答の最大時間を指定します。
	  • **Max Query Response Time**（最大クエリ応答時間） – 一般的なクエリと受信者からの応答間の最大時間を指定します。
	  • **Last Member Query Interval**[最終メンバー照会間隔] – グループまたは送信元特定クエリ メッセージ (グループからの脱退を示すメッセージに応答して送信されたメッセージも含む) 間の間隔を指定します。
	  • **Immediate Leave**（すぐに終了） – 脱退メッセージを受信したときにすぐにグループから脱退させる場合に選択します。

PIM	Protocol Independent Multicast (PIM) 設定を指定します。

© 2019 Palo Alto Networks, Inc.

マルチキャスト設定 – インターフェイス	の意味
	• **Enable**（有効化） — このインターフェイスにおける PIM メッセージの受信や送信を許可する場合に選択します。インターフェイスによるマルチキャスト トラフィックの転送を有効にする必要があります。 • **Assert Interval**（アサート間隔） — PIM 転送者を選択するために、PIM アサート メッセージ間の間隔を指定します。 • **Hello Interval**[Hello 間隔] — PIM hello メッセージ間の間隔を指定します。 • **Join Prune Interval**（プルーン参加間隔）—PIM 参加メッセージ間（および PIM プルーン メッセージ間）の秒数を指定します。デフォルトは60 です。 • **DR Priority**（**DR** 優先順位） — このインターフェイスの指定ルーターの優先順位を指定します。 • **BSR Border**（**BSR** ボーダー） — インターフェイスをブートストラップ境界として使用する場合に選択します。 • **PIM Neighbors**（**PIM** ネイバー） — PIM を使用して通信するネイバーのリストを **Add**（追加）します。

マルチキャストの *SPT Threshold*（*SPT* しきい値）タブ

- Network > Virtual Router > Multicast > SPT Threshold [ネットワーク > 仮想ルーター > SPT しきい値]

最短パスツリー（SPT）しきい値は、仮想ルーターがマルチキャスト グループまたはプレフィックスのマルチキャスト ルーティングを、共有ツリー配信（ランデブー ポイントからの送信元）からソースツリー（最短パスツリーまたは SPT としても知られる）配信に切り替えるポイントを定義します 。マルチキャスト グループまたはプレフィックスの SPT しきい値を **Add**（追加）します。

SPT しきい値	の意味
マルチキャスト グループ/プレフィックス	グループまたはプレフィックスへのスループットがしきい値設定に達したときに、マルチキャスト ルーティングが SPT 配信に切り替わるマルチキャスト アドレスまたはプレフィックスを指定します。
しきい値**(kbps)**	マルチキャストルーティングが対応するマルチキャストグループまたはプレフィックスのSPT配信に切り替えるポイントを指定するには、次の設定を選択します。 • **0**（最初のデータ パケットをオンにする）–（デフォルト）グループまたはプレフィックスのマルチキャスト パケットが到達すると、仮想ルータは SPT ディストリビューションに切り替えます。 • なし（**spt** に切り替えない）–仮想ルータはこのグループまたはプレフィックスにマルチキャスト トラフィックを転送し続けます。 • 任意のインターフェイスおよび任意の期間（範囲は1〜4,294,967,295）で、対応するマルチキャストグループまたはプレフィックスに到達できるマルチキャスト パケットからの合計キロビット数を入力します。スループットがこの数に達すると、仮想ルータは SPT ディストリビューションに切り替わります。

© 2019 Palo Alto Networks, Inc.

マルチキャストの送信元固有のアドレス空白タブ

- Network > Virtual Router > Multicast > Source Specific Address Space [ネットワーク > 仮想ルーター > マルチキャスト > 送信元固有のアドレス スペース]

特定の送信元からのマルチキャスト パケットを受信できるマルチキャスト グループを **Add**（追加）します。これらは、**Multicast**（マルチキャスト）> **Interfaces**（インターフェイス）> **Group Permissions**（グループ権限）タブに指定したのと同じマルチキャスト グループと名前です。

マルチキャスト設定 – 送信元特定アドレス空間	の意味
氏名	ファイアウォールで送信元特定マルチキャスト（SSM）サービスを提供するときの提供先のマルチキャスト グループを識別します。
グループ	特定の送信元からのマルチキャスト パケットを受信できるマルチキャスト グループ アドレスを指定します。
含まれる	マルチキャスト グループを SSM アドレス空間に含める場合に選択します。

マルチキャストの *Advanced*（詳細）タブ

- Network > Virtual Router > Multicast > Advanced [ネットワーク > 仮想ルーター > マルチキャスト > 詳細]

セッション終了後にマルチキャスト ルートがルーティング テーブルに残る時間を設定します。

マルチキャストの詳細設定	の意味
ルートのエイジアウト秒数	セッション終了後にマルチキャストルートがルーティングテーブルに残る秒数を設定することができます（範囲は210～7200、デフォルトは210）。

ECMP

- Network > Virtual Routers > Router Settings > ECMP [ネットワーク > 仮想ルーター > ルーター設定 > ECMP]

ECMP（Equal Cost Multiple Path）処理はネットワーキング機能の一つで、これを使用するとファイアウォールは、同じ宛先に対する等コストのルートを最大 4 つ使用できます。この機能を使用しないときに、同じ宛先に対する等コストのルートが複数ある場合、仮想ルーターは、それらのルートのいずれかをルーティング テーブルから選択し、その転送テーブルに追加します。選択したルートが使用不能でない限り、他のルートは使用しません。仮想ルーターで ECMP 機能を有効にすると、ファイアウォールは、宛先に対する等コストのパスをその転送テーブル内に最大 4 つ持つことができ、以下のことが可能になります。

- 複数の等コスト リンクでの同じ宛先への負荷分散フロー (セッション)。
- 一部のリンクを未使用のままにせず、同じ宛先に対するすべてのリンクで使用可能な帯域幅を利用する。
- リンクに障害が発生した場合、同じ宛先に向かう別の ECMP メンバーにトラフィックを動的に切り替える。ルーティング プロトコルまたは RIB テーブルが代替パス/ルートを選択するのを待つ必要はありません。これにより、リンク障害時のダウン タイムを削減できます。

© 2019 Palo Alto Networks, Inc.

ECMP 負荷分散は、パケット レベルではなく、セッション レベルで実行されます。つまり、ファイアウォールは、パケットを受信するたびではなく、新規セッションの開始時に等コストのパスを選択します。

既存の仮想ルーターで*ECMP*を有効化、無効化、または変更する場合、ルーターはシステムに対し仮想ルーターを再起動させるため、既存のセッションが強制終了される恐れがあります。

仮想ルーターの ECMP を設定するには、仮想ルーターを選択し、**Router Settings**（ルーター設定）で **ECMP** タブを選択した後、説明に従って ECMP 設定を指定します。

確認すべき情報	以下を参照
ECMP を設定する際に使用可能なフィールドは？	ECMP 設定
その他の情報をお探しですか？	ECMP

ECMP 設定

- Network > Virtual Routers > Router Settings > ECMP [ネットワーク > 仮想ルーター > ルーター設定 > ECMP]

以下のフィールドを使用して、ECMP（Equal-Cost Multiple Path）設定を指定します。

ECMP 設定	の意味
Enable [有効化]	ECMP を **Enable**（有効化）します。 既存の仮想ルーターで*ECMP*を有効化、無効化、または変更する場合、ルーターはシステムに対し仮想ルーターを再起動させるため、既存のセッションが強制終了される恐れがあります。
対称リターン	（任意）**Symmetric Return**[対称リターン] を選択すると、関連付けられた入力パケットが到着した際と同じインターフェイスから戻りパケットが出力されます。つまり、ファイアウォールは、ECMP インターフェイスではなく、戻りパケットを送信する入力インターフェイスを使用します。そのため、負荷分散は、**Symmetric Return**[対称リターン] の設定でオーバーライドされます。この動作は、サーバーからクライアントに移動するトラフィックに対してのみ発生します。
最大パス	等コストのパスの最大数を選択します：RIB から FIB にコピーできる、（2、3、または 4）から宛先ネットワークへ。デフォルトは 2です。
メソッド	仮想ルーターで使用するECMP 負荷分散アルゴリズムを以下から 1 つ選択します。ECMP 負荷分散は、パケット レベルではなく、セッション レベルで実行されます。つまり、ファイアウォール (ECMP) は、パケットを受信するたびではなく、新規セッションの開始時に等コストのパスを選択します。 • **IP モジュロ** – デフォルトでは、仮想ルーターは、このオプションを使用してセッションを負荷分散します。このオプションでは、パケット ヘッダー

© 2019 Palo Alto Networks, Inc.

ECMP 設定	の意味

	の送信元および宛先 IP アドレスのハッシュを使用して、使用する ECMP ルートを決定します。
	• **IP Hash**（**IP** ハッシュ）—使用する ECMP ルートを決定する IP ハッシュ方法は 2 通りあります。
	  • **IP Hash**（**IP** ハッシュ）を選択する場合、デフォルトではファイアウォールは送信元 IP アドレスと宛先 IP アドレスのハッシュを使用します。
	  • あるいは、**Use Source Address Only**（送信元アドレスのみ使用）（PAN-OS 8.0.3 とそれ以降のリリースで使用可能）を選択できます。この IP ハッシュ方法は、同じ送信元 IP アドレスに属するすべてのセッションが常に同じパスを使用するようにします。
	  • オプションで、**Use Source/Destination Ports**（ソース/宛先ポートの使用）を選択して、いずれかのハッシュ計算にポートを含めることができます。負荷分散をさらにランダム化するために、**Hash Seed**[ハッシュシード]値 (整数) を入力することもできます。
	• **Weighted Round Robin**[重み付きラウンド ロビン] — このアルゴリズムを使用すると、さまざまなリンクの容量や速度を考慮できます。このアルゴリズムを選択すると、Interface [インターフェイス] ウィンドウが開きます。**Add**[追加] をクリックし、重み付きラウンド ロビン グループに含める**Interface**[インターフェイス]を選択します。インターフェイスごとに、使用する**Weight**[重み]を入力します。**Weight**[重み]は、デフォルトで 100 に設定されています。重みの範囲は 1 ~ 255 です。特定の等コストのパスの重みが大きくなるほど、その等コストのパスが新規セッションで選択される頻度が高くなります。高速のリンクには、低速のリンクよりも大きな重みを与える必要があります。これにより、一層多くの ECMP トラフィックが高速のリンクを通過するようになります。別のインターフェイスと重みを追加するには、**Add**[追加] を再びクリックします。
	• **Balanced Round Robin**[均等ラウンド ロビン] — 受信 ECMP セッションをリンク全体に均等に分散します。

仮想ルーターの詳細ランタイム状態

仮想ルーターのスタティック ルートまたはルーティング プロトコルを設定した後、**Network**（ネットワーク）> **Virtual Routers**（仮想ルーター）を選択し、最後の列の **More Runtime Stats**（ランタイム状態の詳細）を選択すると、仮想ルーターの詳細情報が表示されます。たとえば、ルート テーブル、転送テーブル、設定したルーティング プロトコルとスタティック ルートが表示されます。このウィンドウで提供される仮想ルーターの詳細情報は 1 画面に収まりません。このウィンドウには、以下のタブが表示されます。

- **Routing**[ルーティング]:「Routing Tab（ルーティング タブ）」を参照してください。
- **RIP**:「RIP Tab（RIP タブ）」を参照してください。
- **BGP**:「BGP Tab（BFP タブ）」を参照してください。
- **Multicast**[マルチキャスト]:「Multicast Tab（マルチキャスト タブ）」を参照してください。
- **BFD Summary Information**（**BFD** サマリー情報）:「BFD Summary Information Tab（BFD サマリー情報）」を参照してください。

Routing Tab（ルーティングタブ）

以下の表は、仮想ルーターのルート テーブル、転送テーブル、スタティック ルートのモニタリング テーブルのランタイム統計について示しています。

© 2019 Palo Alto Networks, Inc.

Runtime Stat（ランタイム統計）	の意味
ルート テーブル	
ルート テーブル	ユニキャストまたはマルチキャストのルート テーブルを表示するには、**Unicast**（ユニキャスト）または **Multicast**（マルチキャスト）を選択します。
アドレス ファミリーの表示	テーブルに表示するアドレスのグループの種類を制御するには、**IPv4 Only**（**IPv4** のみ）、**IPv6 Only**（**IPv6** のみ）、または **IPv4 and IPv6**（**IPv4** および **IPv6**）（デフォルト）を選択します。
宛先	仮想ルータが到達できるネットワークの IPv4 アドレスおよびネットマスクまたは IPv6 アドレスおよびプレフィックス長。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレス。ネクストホップが 0.0.0.0 の場合は、デフォルト ルートを表します。
メトリック	ルートのメトリック。ルーティング プロトコルで同一の宛先ネットワークへの複数のルートが存在する場合、メトリック値が最も小さいルートが優先されます。各ルーティング プロトコルは異なるタイプのメトリックを使用します。たとえば、RIP はホップ数を使用します。
重み	ルートの重みです。たとえば、BGP で同一の宛先への複数のルートがある場合、最も重みが大きいルートが優先されます。
flags	• **A?B** – アクティブかつ、BGP 経由で学習したもの • **A C** – アクティブかつ、内部インターフェイスの結果（接続済み）- 宛先 = ネットワーク • **A H** – アクティブかつ、内部インターフェイスの結果（接続済み）- 宛先 = ホストのみ • **A R** – アクティブかつ、RIP 経由で学習したもの • **A S** – アクティブかつ、スタティック • **S** – 非アクティブ（このルートがより高いメトリックを持っているため）かつ、スタティック • **O1** – OSPF 外部タイプ -1 • **O1** – OSPF 外部タイプ -2 • **Oi** – OSPF エリア内 • **Oo** – OSPF エリア間
エイジ	ルーティング テーブルのルート エントリのエイジ。スタティック ルートには、エイジはありません。
インターフェイス	ネクストホップに到達するために使用される仮想ルーターの出力インターフェイス。
レートの	テーブルのランタイム統計を更新する場合にクリックします。
転送テーブル	

© 2019 Palo Alto Networks, Inc.

Runtime Stat（ランタイム統計）	の意味
ファイアウォールは最適なルート（ルート テーブル（*RIB*）から宛先ネットワーク）を選択し、*FIB* に配置します。	
アドレス ファミリーの表示	表示するルート テーブルの種類を制御するには、**IPv4 Only**（**IPv4** のみ）、**IPv6 Only**（**IPv6** のみ）、または **IPv4 and IPv6**（**IPv4** および **IPv6**）（デフォルト）を選択します。
宛先	ルート テーブルから選択された、仮想ルーターが到達できるネットワークの最適な IPv4 アドレスおよびネットマスク、または IPv6 およびプレフィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表します。
flags	• **u** – ルートの状態はアップです。 • **h** – ルートはホストに向かいます。 • **g** – ルートはゲートウェイに向かいます。 • **e** – ファイアウォールは等価コスト マルチパス（ECMP）を使用してこのルートを選択しています。 • * – ルートは、宛先ネットワークに向かう優先パスです。
インターフェイス	ネクスト ホップに到達するために仮想ルーターが使用する出力インターフェイス。
MTU	最大転送単位（MTU）です。この宛先への TCP パケット 1 つあたりでファイアウォールが転送する最大バイト数を示します。
レートの	テーブルのランタイム統計を更新する場合にクリックします。
スタティック ルートのモニタリング	
宛先	仮想ルーターが到達できるネットワークの IPv4 アドレスおよびネットマスクまたは IPv6 アドレスおよびプレフィックス長です。
ネクストホップ	宛先ネットワーク方向のネクスト ホップにあるデバイスの IP アドレス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表します。
メトリック	ルートのメトリック。同一の宛先ネットワークへの複数のスタティック ルートが存在する場合、ファイアウォールはメトリック値が最も小さいルートを優先します。
重み	ルートの重みです。
flags	• **A?B** – アクティブかつ、BGP 経由で学習したもの • **A C** – アクティブかつ、内部インターフェイスの結果（接続済み）- 宛先 = ネットワーク • **A H** – アクティブかつ、内部インターフェイスの結果（接続済み）- 宛先 = ホストのみ • **A R** – アクティブかつ、RIP 経由で学習したもの • **A S** – アクティブかつ、スタティック • **S** – 非アクティブ（このルートがより高いメトリックを持っているため）かつ、スタティック

© 2019 Palo Alto Networks, Inc.

Runtime Stat（ランタイム統計）	の意味
	• **O1** – OSPF 外部タイプ -1 • **O1** – OSPF 外部タイプ -2 • **Oi** – OSPF エリア内 • **Oo** – OSPF エリア間
インターフェイス	ネクストホップに到達するために使用される仮想ルーターの出力インターフェイス。
パス モニタリング (フェール オン)	このスタティック ルートでパス モニタリングが有効である場合、Fail On（フェイル オン）は以下を示します。 • **All**（すべて） – スタティック ルートの監視対象の宛先がすべてダウンしている場合に、ファイアウォールはスタティック ルートがダウンしていると見なして、フェイルオーバーします。 • **Any**（任意） – スタティック ルートの監視対象の宛先いずれかがダウンしている場合に、ファイアウォールはスタティック ルートがダウンしていると見なして、フェイルオーバーします。 スタティック ルートのパス モニタリングが無効である場合、Fail On（フェイル オン）は **Disabled**（無効）を示します。
ステータス	監視対象の宛先への ICMP ping に基づく静的ルートのステータス：静的ルートの**Up**、**Down**、またはパスの監視は **Disabled**（無効）です。
レートの	テーブルのランタイム統計を更新します。

[RIP] タブ

以下の表は、仮想ルーターの RIP のランタイム状態を示しています。

RIP のランタイム状態	の意味
Summary [サマリー]タブ	
間隔（秒）	間隔の秒数です。RIP はこの値（期間）を使用して、更新、失効、削除の間隔を管理します。
更新間隔	仮想ルーターがピアに送信する RIP ルート通知更新の間隔。
失効の間隔	仮想ルーターがピアから受信した最後の更新以降の間隔で、この間隔を超えると、仮想ルーターは、ピアからのルートを使用不可としてマークします。
削除間隔	ルートが使用不可としてマークされた後、更新を受信しなかった場合に、ファイアウォールがルートをルーティング テーブルから削除するまでの間隔です。
Interface [インターフェイス]タブ	
アドレス	RIP が有効な仮想ルーターのインターフェイスの IP アドレス。

© 2019 Palo Alto Networks, Inc.

RIP のランタイム状態	の意味
認証タイプ	認証のタイプ。simple password [簡易パスワード]、MD5、またはnone [なし] があります。
送信許可	チェック マークが付いている場合、このインターフェイスは、RIP パケットの送信が許可されています。
受信許可	チェック マークが付いている場合、このインターフェイスは、RIP パケットの受信が許可されています。
デフォルト ルートの通知	チェック マークが付いている場合、RIP は、デフォルト ルートをピアに通知します。
デフォルト ルート メトリック	デフォルト ルートに割り当てられたメトリック (ホップ数)。メトリック値が低いほど、ルーティング テーブルでの優先度が高くなり、優先パスとして選択されやすくなります。
キー ID	ピアに対して使用される認証キー。
優先	認証の優先キー。
Peer [ピア]タブ	
ピア アドレス	仮想ルーターの RIP インターフェイスに対するピアの IP アドレス。
最終更新	このピアから最終更新を受信した日時。
RIP バージョン	ピアが実行している RIP バージョン。
無効なパケット	このピアから受信した無効なパケット数。ファイアウォールが RIP パケットを解析できない理由として、ルート境界を x バイト超えた、パケット内のルート数が多すぎる、サブネットが不適切、アドレスが無効、認証が失敗した、メモリが不十分などが考えられます。
無効なルーター	このピアから受信した無効なルート数。原因として、ルートが無効、インポートが失敗した、メモリが不十分などが考えられます。

[BGP] タブ

以下の表は、仮想ルーターの BGP のランタイム状態を示しています。

BGP のランタイム状態	の意味
Summary [サマリー]タブ	
ルーター ID	BGP インスタンスに割り当てられたルーター ID。
デフォルト ルートの拒否	Reject Default Route [デフォルト ルートの拒否] オプションが設定されているかどうかを示します。このオプションを設定すると、仮想ルーターは、BGP ピアが通知したデフォルト ルートをすべて無視します。

© 2019 Palo Alto Networks, Inc.

BGP のランタイム状態	の意味
デフォルト ルートの再配信	Allow Redistribute Default Route [デフォルト ルートの再配信を許可] オプションが設定されているかどうかを示します。
ルートのインストール	Install Route [ルートのインストール] オプションが設定されているかどうかを示します。このオプションを設定すると、仮想ルーターは、グローバル ルーティング テーブルに BGP ルートをインストールします。
グレースフル リスタート	Graceful Restart [グレースフル リスタート] が有効かどうかを示します (サポート)。
AS サイズ	選択されている AS フォーマット サイズが 2 バイトと 4 バイトのいずれであるのかを示します。
ローカル AS	仮想ルーターが属する AS の番号。
ローカル メンバー AS	ローカル メンバー AS の番号 (仮想ルーターがコンフェデレーションに含まれている場合にのみ有効)。仮想ルーターがコンフェデレーションに含まれていない場合、このフィールドは 0 です。
クラスタ ID	設定済みの リフレクタ クラスタ ID が表示されます。
デフォルト ローカル設定	仮想ルーターに設定されたデフォルト ローカル設定が表示されます。
常に MED を比較	Always Compare MED [常に MED を比較] オプションが設定されているかどうかを示します。このオプションを設定すると、比較が有効になり、別の AS 内のネイバーから受け取ったルートの中からルートを選択できます。
MED に関係なく集約	Aggregate MED [MED の集約] オプションが設定されているかどうかを示します。このオプションを設定すると、ルートの MED 値が異なる場合でも、ルート集約が有効になります。
決定論的 MED 処理	Deterministic MED [決定論的 MED 比較] オプションが設定されているかどうかを示します。このオプションを設定すると、比較が有効になり、IBGP ピア (同じ AS 内の BGP ピア) から通知されたルートの中からルートを選択できます。
現在の RIB 出力エントリ	RIB 出力テーブルのエントリ数。
ピーク RIB 出力エントリ	任意の一時点で割り当てられた 隣接 RIB 出力ルートのピーク数。
Peer [ピア]タブ	
氏名	ピアの名前。
グループ	このピアが属するピア グループの名前。
ローカル IP	仮想ルーターの BGP インターフェイスの IP アドレス。
ピア IP	ピアの IP アドレス。

© 2019 Palo Alto Networks, Inc.

BGP のランタイム状態	の意味
ピア AS	ピアが属している AS。
パスワード セット	認証が設定されているかどうかが [はい] または [いいえ] で示されます。
ステータス	Active[アクティブ]、Connect[接続]、Established[確立済み]、Idle[待機中]、OpenConfirm、OpenSentなど、ピアの状態を示します。
状態の期間 (秒)	ピアの状態の期間。
Peer Group [ピア グループ] タブ	
グループ名	ピア グループの名前。
タイプ	設定されたピア グループのタイプ (EBGP や IBGP など)。
コンフェデレーションの集約AS	Aggregate Confederation AS [コンフェデレーション AS の集約] オプションが設定されているかどうかが [はい] または [いいえ] で示されます。
ソフト リセット サポート	ピア グループでソフト リセットがサポートされているかどうかが [はい] または [いいえ] で示されます。BGP ピアに対するルーティング ポリシーが変更されると、ルーティング テーブルの更新に影響が及ぶ場合があります。BGP セッションに対しては、ハード リセットよりもソフト リセットが優先されます。これは、ソフト リセットでは、BGP セッションをクリアせずにルーティング テーブルを更新できるからです。
ネクスト ホップ セルフ	このオプションが設定されているかどうかが [はい] または [いいえ] で示されます。
次のホップ サードパーティ	このオプションが設定されているかどうかが [はい] または [いいえ] で示されます。
プライベート AS の削除	更新が送信される前に、プライベート AS 番号が AS_PATH 属性から削除されるかどうかを示します。
Local RIB [ローカルRIB]タブ	
プレフィックス	ローカル RIB (Routing Information Base) のネットワーク プレフィックスおよびサブネット マスク。
フラグ	* は、ルートが最良の BGP ルートとして選択されたことを示します。
ネクストホップ	プレフィックス方向のネクスト ホップの IP アドレス。
ピア	ピアの名前。
重み	プレフィックスに割り当てられた重み属性。ファイアウォールが同じプレフィックスへのルートを複数持っている場合は、重みが最も大きいルートが IP ルーティング テーブルにインストールされます。

© 2019 Palo Alto Networks, Inc.

BGP のランタイム状態	の意味
ローカル設定.	ルートのローカル設定属性。これは、出口が複数ある場合、プレフィックス方向の出口を選択するために使用されます。低いローカル設定よりも高いローカル設定が優先されます。
AS パス	プレフィックス ネットワークへのパス内の AS のリスト。このリストは、BGP 更新で通知されます。
元	プレフィックスの元属性。BGP はどのようにルートについて学習したか。
MED	ルートの MED (Multi-Exit Discriminator) 属性。MED は、ルートのメトリック属性です。これは、ルートを通知する AS によって、外部 AS に提案されます。高い MED よりも低い MED が優先されます。
フラップ数	ルートのフラップの数。
RIB Out [RIBアウト]タブ	
プレフィックス	RIB (Routing Information Base) のネットワーク ルーティング エントリ。
ネクストホップ	プレフィックス方向のネクスト ホップの IP アドレス。
ピア	仮想ルーターがこのルートを通知するピア。
ローカル設定.	プレフィックスにアクセスためのローカル設定属性。これは、出口が複数ある場合、プレフィックス方向の出口を選択するために使用されます。低いローカル設定よりも高いローカル設定が優先されます。
AS パス	プレフィックス ネットワークへのパス内の AS のリスト。
元	プレフィックスの元属性。BGP はどのようにルートについて学習したか。
MED	プレフィックスに対する MED (Multi-Exit Discriminator) 属性。MED は、ルートのメトリック属性です。これは、ルートを通知する AS によって、外部 AS に提案されます。高い MED よりも低い MED が優先されます。
高度なステータス	ルートの通知状態。
集約ステータス	このルートが他のルートと集約されるかどうかを示します。

[マルチキャスト] タブ

以下の表は、仮想ルーターの IP マルチキャストのランタイム状態を示しています。

マルチキャストのランタイム状態	の意味
FIBタブ	

© 2019 Palo Alto Networks, Inc.

マルチキャストのランタイム状態	の意味
グループ	転送情報ベース (FIB) のルートエントリ。仮想ルーターがパケットを転送するマルチキャスト グループ アドレス。
送信元	グループのマルチキャスト パケットの送信元アドレス。
受信インターフェイス	グループのマルチキャスト パケットが到着するインターフェイス。
送信インターフェイス	仮想ルータがグループのマルチキャスト パケットを転送するインターフェイス。
IGMP Interface [IGMPインターフェイス]タブ	
インターフェイス	IGMP が有効になっているインターフェイス。
バージョン	仮想ルータ上で実行する IGMP (Internet Group Management Protocol) のバージョン 1、2、または 3。
クエリ実行者	インターフェイスに接続されたマルチアクセス セグメント上の IGMP クエリ実行者の IP アドレスです。
クエリ実行者のアップ タイム	IGMP クエリ実行者がアップしている秒数です。
クエリ実行者の失効時間	他のクエリ実行者の現行タイマーが期限切れになるまでの残り秒数。
頑強性	IGMP インターフェイスの頑強性
グループ制限	IGMP が同時に処理できるインターフェイス毎の最大グループ数です。
送信元制限	IGMP が同時に処理できるインターフェイス毎の最大ソース数です。
すぐに終了	Immediate Leave [すぐに終了] が設定されているかどうかが [はい] または [いいえ] で示されます。Immediate Leave [すぐに終了] を設定すると、インターフェイスに IGMP グループ固有のクエリを送信せずに、仮想ルーターが転送テーブルからインターフェイスを削除します。
IGMP Membership [IGMPメンバーシップ]タブ	
インターフェイス	グループが所属するインターフェイスの名前。
グループ	インターフェイスが属するマルチキャスト グループのアドレス。
送信元	グループへのマルチキャスト パケットを送信している送信元の IP アドレス。
アップ タイム	メンバーシップがアップしている時間の秒数。
失効時間	メンバーシップが失効するまでの残り時間の秒数です。

© 2019 Palo Alto Networks, Inc.

マルチキャストのランタイム状態	の意味
フィルタ モード	送信元を許可するか除外します。仮想ルーターを設定し、すべてのトラフィックを許可する、この送信元 (許可) からのトラフィックのみを許可する、またはこの送信元 (除外) を除くすべての送信元からのトラフィックを含めるようにします。
有効期限の除外	インターフェイスの除外状態が期限切れになるまでの残り秒数。
V1 ホスト タイマー	インターフェイスに接続された IP サブネットに IGMP バージョン 1 メンバーが存在しないとローカル ルーターが想定するまでの残り時間。
V2 ホスト タイマー	インターフェイスに接続された IP サブネットに IGMP バージョン2 メンバーが存在しないとローカル ルーターが想定するまでの残り時間。
PIM Group Mapping [PIMグループマッピング]タブ	
グループ	ランデブー ポイントにマップされたグループの IP アドレス。
RP	グループのランデブー ポイントの IP アドレス。
元	どこで仮想ルーターが RP について学習したかを示します。
PIM モード	[ASM] または [SSM]。
非アクティブ	グループから RP へのマッピングが非アクティブであるかどうかを示します。
PIMインターフェイスタブ	
インターフェイス	PIM に参加しているインターフェイスの名前。
アドレス	インターフェイスの IP アドレス。
DR	インターフェイスに接続されたマルチアクセス セグメント上の宛先ルーターの IP アドレスです。
送信間隔	設定されている Hello 間隔 (秒)
結合/プルーニング間隔	Join および Prune メッセージ用に設定された間隔 (秒) です。
アサート間隔	アサート メッセージを送信するために仮想ルーター用に設定された PIM アサート間隔 (秒) です。PIM はアサート メカニズムを使用してマルチアクセス ネットワーク用の PIM フォワーダーを選出し始めます。
DR 優先順位	インターフェイスに接続されたマルチアクセス セグメント上の宛先ルーター用に設定された優先順位です。
BSR ボーダー	「はい」または「いいえ」は、インターフェイスがエンタープライズ LAN の境界にあるブートストラップ ルーター (BSR) である仮想ルーターにあるかどうかを示します。
PIM Neighbor [PIMネイバー]タブ	

© 2019 Palo Alto Networks, Inc.

マルチキャストのランタイム状態	の意味
インターフェイス	仮想ルーターのインターフェイスの名前です。
アドレス	インターフェイスから到達可能な PIM ネイバーの IP アドレス。
セカンダリ アドレス	インターフェイスから到達可能な PIM ネイバーのセカンダリ IP アドレス。
アップ タイム	ネイバーがアップしている時間の長さ。
失効時間	仮想ルーターがネイバーから hello パケットを受信していないためにそのネイバーが期限切れになるまでの残り時間の長さ。
生成 ID	ランダムに生成された 32 ビットの値であり、インターフェイス上で PIM フォワーダーが起動あるいは再起動する度（ルーター自体が再起動する場合を含む）に生成され直します。
DR 優先順位	このネイバーからの最後の PIM hello メッセージで仮想ルーターが受信した指定ルーターの優先順位。

BFD Summary Information（BFD サマリー情報）タブ

BFD サマリー情報には、以下のデータが含まれます。

BFD サマリー情報のランタイム状態	の意味
インターフェイス	BFD を実行しているインターフェイス。
PROTOCOL	インターフェイスで BFD を実行しているスタティック ルート（スタティック ルートの IP アドレス ファミリー）またはダイナミック ルーティング プロトコル。
ローカル IP アドレス	BFD を設定したインターフェイスの IP アドレス。
隣接 IP アドレス	BFD ネイバーの IP アドレス。
状態	ローカルおよびリモートBFDピアのBFDの状態:**admin down**（管理者ダウン）、**down**（ダウン）、**init**（初期設定）、または**up**（アップ）。
アップ タイム	BFD のアップタイム（時間、分、秒、ミリ秒）。
ディスクリミネータ (ローカル)	ローカル BFD ピアのディスクリミネータ。ディスクリミネータは、複数の BFD セッションを識別するためにピアで使用されるゼロ以外の一意の値です。
ディスクリミネータ (リモート)	リモート BFD ピアのディスクリミネータ。
エラー	BFD エラーの数。
セッションの詳細	**Details**（詳細）をクリックすると、セッションの BFD 情報（ローカルおよびリモート ネイバーの IP アドレス、最後に受信したリモート診断コード、送信および受信

© 2019 Palo Alto Networks, Inc.

BFD サマリー情報のランタイム状態	の意味
	したコントロール パケットの数、エラーの数、状態の変化を引き起こした最後のパケットに関する情報など) が表示されます。

© 2019 Palo Alto Networks, Inc.

Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

Network > **IPSec Tunnels**[ネットワーク > IPSec トンネル] を使用して、ファイアウォール間の IPSec VPNトンネルを設定および管理します。これは、IKE/IPSec VPN セットアップのフェーズ 2 の部分です。

確認すべき情報	以下を参照
IPSec VPN トンネルを管理する。	IPSec VPN トンネル管理
IPSec トンネルを設定する。	IPSec トンネルの [全般] タブ
	IPSec トンネルの Proxy IDs (プロキシ ID) タブ
IPSec トンネルの状態を表示する。	ファイアウォールの IPSec トンネル状態
IPSec トンネルを再起動または更新する。	IPSec トンネルの再起動または更新
その他の情報をお探しですか？	IPSec トンネルのセットアップ

IPSec VPN トンネル管理

- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

以下の表は、IPSec VPN トンネルの管理方法を示しています。

IPSec VPN トンネルを管理するフィールド	
コンテキストの	新しい IPSec VPN トンネルを **Add** (追加) します。新しいトンネルの設定方法については「IPSec トンネルの General (全般) タブ」を参照してください。
削除します。	不要になったトンネルを **Delete** (削除) します。
Enable [有効化]	無効になっていたトンネルを **Enable** (有効化) します (トンネルはデフォルトで有効化されます)。
無効化	使用しておらず、まだ削除できないトンネルを **Disable** (無効化) します。
PDF/CSV	**PDF/CSV** 形式のすべての IPSec トンネル設定をエクスポートします。フィルタを適用してテーブルの出力をカスタマイズし、必要な列のみを含めることができます。エクスポート ダイアログに表示される列のみがエクスポートされます。Export Configuration Table Data (設定バンドルデータのエクスポート) を参照してください。

© 2019 Palo Alto Networks, Inc.

IPSec トンネルの [全般] タブ

- Network (ネットワーク) > IPSec Tunnels (IPSec トンネル) > General (全般)

IPSec トンネルをセットアップするには、次のフィールドを使用します。

IPSec トンネルの全般設定	の意味
氏名	トンネルを識別する **Name** (名前) を入力します (最大 63 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 このフィールドの制限文字数の 63 文字には、プロキシ ID およびトンネル名が含まれ、コロンで区切られています。
トンネルインターフェイス	既存のトンネル インターフェイスを選択するか、**New Tunnel Interface**[新規トンネル インターフェイス] をクリックします。トンネル インターフェイスの作成の詳細は「Network (ネットワーク) > Interfaces (インターフェイス) > Tunnel (トンネル)」を参照してください。
IPv4 / IPv6	**IPv4** または **IPv6** を選択し、トンネルのエンドポイントの IP アドレス タイプを設定します。
タイプ	自動的に生成されるセキュリティ キーを使用するのか、手動で入力するセキュリティ キーを使用するのかを選択します。**Auto key**[自動キー] を使用することをお勧めします。
自動キー	**Auto Key**[自動キー] を選択する場合、以下の内容を指定します。 • **IKE Gateway** (**IKE** ゲートウェイ) – IKE ゲートウェイの設定の詳細は「Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IKE Gateways (IKE ゲートウェイ)」を参照してください。 • **IPSec Crypto Profile**[IPSec 暗号化プロファイル] – 既存のプロファイルを選択するか、デフォルトのプロファイルを使用します。新しいプロファイルを定義するには、**New** (新規) をクリックし、「Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IPSec Crypto (IPsec 暗号)」の指示に従ってください。 • **Show Advanced Options**[詳細オプションの表示] をクリックすると、残りのフィールドにアクセスできます。 • **Enable Replay Protection** (リプレイ プロテクションを有効にする) – リプレイ攻撃から保護する場合に選択します。 • **Copy TOS Header**[TOS ヘッダーのコピー] – 元の TOS 情報を保持するため、カプセル化されたパケットの内部 IP ヘッダーから外部 IP ヘッダーに TOS (Type of Service) フィールドをコピーします。ECN (Explicit Congestion Notification) フィールドもコピーされます。 • **Add GRE Encapsulation (GRE** カプセル化の追加)–IPSec トンネル内でカプセル化された GRE ヘッダーを追加する場合に選択します。ファイアウォールは他のベンダーのトンネル エンドポイントとの相互運用性を確保するために IPSec ヘッダーの後で GRE ヘッダーを生成します。つまり、GRE トンネルを IPSec トンネルと共有します。 • **Tunnel Monitor** (トンネル モニター) – デバイス管理者にトンネルの障害についてアラートを送信し、別のインターフェイスへの自動フェイルオーバーを実行する場合に選択します。

© 2019 Palo Alto Networks, Inc.

IPSec トンネルの全般設定	の意味
	モニタニングする場合は、トンネル インターフェイスに *IP* アドレスを割り当てる必要があります。 • **Destination IP**[宛先 IP]– トンネルが正常に動作しているかどうかを判別するためにトンネル モニターが使用する、トンネルの反対側の IP アドレスを指定します。 • **Profile**[プロファイル] – トンネルで障害が発生した場合に実行されるアクションを決める、既存のプロファイルを選択します。モニタープロファイルに指定されたアクションが待機/回復の場合、ファイアウォールは、トンネルが機能するようになるまで待機し、ルート テーブルで代替パスを探すことはしません。フェイルオーバー アクションを使用する場合、ファイアウォールはルート テーブルを調べ、宛先に到達するために使用できる代替ルートがないか確認します。詳細は「Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > Monitor (監視)」を参照してください。
手動キー	**Manual Key**[手動キー] を選択する場合、以下の内容を指定します。 • **Local SPI**[ローカル SPI] – ローカル ファイアウォールからピアへのパケット トラバーサルのローカル セキュリティ パラメータ インデックス (SPI) を指定します。SPI は、IPSec トラフィック フローの区別を支援するために IPSec トンネルのヘッダーに追加されている 16 進インデックスです。 • **Interface**[インターフェイス] – トンネルの終端であるインターフェイスを選択します。 • **Local Address**[ローカル アドレス] – トンネルの終端となるローカル インターフェイスの IP アドレスを選択します。 • **Remote SPI**[リモート SPI] – リモート ファイアウォールからピアへのパケット トラバーサルのリモート セキュリティ パラメータ インデックス (SPI) を指定します。 • **Protocol**[プロトコル] – トンネルを経由するトラフィックのプロトコルを選択します (**ESP** または **AH**)。 • **Authentication**[認証] – トンネル アクセスの認証タイプを選択します (**SHA1**、**SHA256**、**SHA384**、**SHA512**、**MD5**、または なし)。 • **Key/Confirm Key**[キー/確認キー] – 認証鍵を入力して確認します。 • **Encryption**[暗号化] – トンネル トラフィックの暗号化オプションを**3des**、**aes-128-cbc**、**aes-192-cbc**、**aes-256-cbc**、**des**、または**null** [暗号化なし] の中から選択します。 • **Key/Confirm Key**[キー/確認キー] – 暗号化鍵を入力して確認します。
GlobalProtectサテライト	**GlobalProtect Satellite**[GlobalProtect サテライト] を選択する場合は、以下の設定項目を指定します。 • **Name**[名前] – トンネルを識別する名前を入力します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 • **Tunnel Interface** (トンネル インターフェイス) – 既存のトンネル インターフェイスを選択するか、New Tunnel Interface (新規トンネル インターフェイス) をクリックします。 • **Portal Address** (ポータル アドレス) – GlobalProtect™ ポータルの IP アドレスを入力します。

© 2019 Palo Alto Networks, Inc.

IPSec トンネルの全般設定	の意味
	• **Interface**（インターフェイス）– ドロップダウン リストから、GlobalProtect ポータルに到達するための出力インターフェイスを選択します。 • **Local IP Address**（ローカル **IP** アドレス）– GlobalProtect ポータルに接続する出力インターフェイスの IP アドレスを入力します。 • 詳細オプション • **Publish all static and connected routes to Gateway**（静的なすべての接続済みルートをゲートウェイに公開）– サテライトが接続されている GlobalProtect ゲートウェイにすべてのルートを公開する場合に選択します。 • **Subnet**[サブネット] – **Add**[追加] をクリックして、サテライトの場所のローカル サブネットを手動で追加します。他のサテライトが同じサブネット情報を使用している場合は、すべてのトラフィックをそのトンネル インターフェイス IP に NAT を行う必要があります。また、この場合はサテライトがルートを共有することはできないため、すべてのルーティングはトンネル IP を介して行われます。 • **External Certificate Authority**（外部認証局）– 外部 CA を使用して証明書を管理する場合に選択します。証明書を生成した後は、それらの証明書をサテライトにインポートし、**Local Certificate**[ローカル証明書] および **Certificate Profile**[証明書プロファイル] の選択が必要になります。

IPSec トンネルの Proxy IDs（プロキシ ID）タブ

- Network（ネットワーク）> IPSec Tunnels（IPSec トンネル）> Proxy IDs（プロキシ ID）

IPSec Tunnel Proxy IDs[IPSecトンネルの プロキシID] は、以下の2つのタブに分かれています。**IPv4** および **IPv6**どちらのタイプもヘルプは同様の内容です。IPv4 と IPv6 の違いは、以下の表の **Local**[ローカル] フィールドと **Remote**[リモート] フィールドに示されています。

IPSec Tunnel Proxy IDs[IPSecトンネルの プロキシID] タブは、IKEv2 のトラフィック セレクタを指定する場合にも使用されます。

プロキシ ID IPv4 および IPv6 の設定	の意味
プロキシ ID	**Add**[追加] をクリックし、プロキシを識別する名前を入力します。 IKEv2 トラフィック セレクタの場合、このフィールドは名前として使用されます。
ローカル	IPv4の場合:x.x.x.x/mask の形式 (たとえば、10.1.2.0/24) でIPアドレスまたはサブネットを入力します。 IPv6:IPアドレスとプレフィックス長を xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length 形式で入力します (つまり、IPv6の規則に従い、たとえば、2001:DB8:0::/48 のように入力します)。 IPv6 アドレッシングでは、すべてのゼロを記述する必要はありません。先行するゼロは省略でき、連続するゼロの 1 つのグループは隣り合う 2 つのコロン (::) で置き換えることができます。

© 2019 Palo Alto Networks, Inc.

プロキシ ID IPv4 および IPv6 の設定	の意味
	IKEv2 トラフィック セレクタの場合、このフィールドは送信元 IP アドレスに変換されます。
リモート	ピアで必要な場合は、以下のようにします。 IPv4 の場合: IP アドレスまたはサブネットを x.x.x.x/mask 形式で入力します (たとえば、10.1.1.0/24 のように入力します)。 IPv6 の場合は、IP アドレスとプレフィックス長を xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix-length 形式で入力します (つまり、IPv6 の規則に従い、たとえば、2001:DB8:55::/48 のように入力します)。 IKEv2 トラフィック セレクタの場合、このフィールドは宛先 IP アドレスに変換されます。
PROTOCOL	ローカルおよびリモート ポートのプロトコルとポート番号を指定します。 **Number** – プロトコル番号 (サードパーティ デバイスとの相互運用性を実現するために使用) を指定します。 • **Any** – TCP や UDP トラフィックを許可します。 • **TCP** – ローカルおよびリモートの TCP ポート番号を指定します。 • **UDP** – ローカルおよびリモートの UDP ポート番号を指定します。 設定された各プロキシ ID は、ファイアウォールの IPSec VPN トンネル容量に影響しません。 このフィールドは、IKEv2 トラフィック セレクタとしても使用されます。

ファイアウォールの IPSec トンネル状態

- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

現在定義されている IPSec VPN トンネルの状態を表示するには、**IPSec Tunnels**[IPSec トンネル] ページを開きます。このページには、以下の状態情報が表示されます。

- Tunnel Status (first status column) (トンネルの状態 (最初の状態列)) – 緑は、IPSec フェーズ 2 セキュリティ アソシエーション (SA) トンネルを表します。赤は、IPSec フェーズ 2 SA が使用できないか、有効期限が切れていることを表します。
- IKE Gateway Status (IKE ゲートウェイの状態) – 緑は、IKE フェーズ 1 SA または IKEv2 IKE SA が有効であることを表します。赤は、IKE フェーズ 1 SA が使用できないか、有効期限が切れていることを表します。
- Tunnel Interface Status (トンネル インターフェイスの状態) – 緑は (トンネル モニターが無効である、またはトンネル モニターの状態がアップでありモニタリング IP アドレスにアクセス可能であるため) トンネル インターフェイスがアップしていることを表します。赤は、トンネル モニターが有効で、リモート トンネル モニタリング IP アドレスがアクセス不可であるために、トンネル インターフェイスがダウンしていることを表します。

IPSec トンネルの再起動または更新

- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

トンネルのステータスを表示する場合は、**Network** (ネットワーク) > **IPSec Tunnels** (**IPSec** トンネル) を開きます。最初の Status (状態) 列には、トンネル情報へのリンクがあります。再起動または更

© 2019 Palo Alto Networks, Inc.

新するトンネルをクリックし、**Tunnel Info**[トンネル情報]を開きます。リストのエントリのいずれかをクリックし、次のいずれかをクリックします。

- **Restart**（再起動）— 選択したトンネルを再起動します。再起動すると、トラフィックのトンネル通過が中断されます。
- **Refresh**（更新）— IPSec SA の現在の状態を表示します。

© 2019 Palo Alto Networks, Inc.

Network (ネットワーク) > GRE Tunnels (GRE トンネル)

GRE (Generic Routing Encapsulation) トンネル プロトコルは、ペイロードのプロトコルをカプセル化するキャリア プロトコルです。GRE パケット自体が転送プロトコル (IPv4 あるいは IPv6) 内でカプセル化されます。GRE トンネルはファイアウォールおよびルーター (あるいは別のファイアウォール) 間のポイントツーポイントの論理リンク内の 2 つのエンドポイントに接続します。Palo Alto Networks のファイアウォールは GRE トンネルのターミネーションをサポートしています。

確認すべき情報	以下を参照
GRE トンネルの構成要素	GRE トンネル
他のベンダーのトンネル エンドポイントとの相互運用性を確保する方法	IPSec トンネルを作成する際、**Add GRE Encapsulation (GRE** カプセル化を追加)を選択します。
その他の情報をお探しですか？	GRE トンネル

GRE トンネル

- Network (ネットワーク) > GRE Tunnels (GRE トンネル)

まずはトンネル インターフェイスを設定します (Network (ネットワーク) > Interfaces (インターフェイス) > Tunnel (トンネル))。次に GRE (generic routing encapsulation) トンネルを追加して次の情報を提供し、作成したトンネル インターフェイスを参照します：

GRE トンネル フィールド	の意味
氏名	GRE トンネルの名前です。
インターフェイス	ローカル GRE トンネル エンドポイント (ソース インターフェイス) (イーサネット インターフェイスあるいはサブインターフェイス)、集約イーサネット (AE) インターフェイス、ループバック インターフェイス、あるいは VLAN インターフェイスとして使用するインターフェイスを選択します。
ローカル アドレス	トンネル インターフェイスのアドレスとして使用するインターフェイスのローカル IP アドレスを選択します。
ピア アドレス	GRE トンネルのもう一方の末端の IP アドレスを入力します。
トンネルインターフェイス	設定したトンネル インターフェイスを選択します。(ルーティングのために、このインターフェイスは

© 2019 Palo Alto Networks, Inc.

GRE トンネル フィールド	の意味
	ネクストホップであるときにトンネルを特定します)
TTL	GRE パケットにカプセル化された IP パケットの TTL を入力します (範囲は 1 ~ 255、デフォルトは 64) 。
ToS ヘッダーのコピー	元の TOS (Type of Service) 情報を保持するため、カプセル化されたパケットの内部 IP ヘッダーから外部 IP ヘッダーに TOS フィールドをコピーする際に選択します。
キープアライブ	GRE トンネルのキープアライブ機能を有効化する場合に選択します (デフォルト設定では無効) 。キープアライブを有効化する場合、デフォルト設定では GRE トンネルがダウンする際は 10 秒間隔で 3 つの応答されないキープアライブ パケット (リトライ) を受け取り、GRE トンネルが復帰する際は 10 秒間隔で 5 つのホールドタイマー間隔を受け取ります。
間隔 (秒)	ローカル側の GRE トンネルがトンネル ピアに送信するキープアライブ パケット間の間隔、キープアライブ パケットが成功した後にファイアウォールがトンネル ピアとの通信を再び確立するまでに各ホールドタイマーが待機する間隔を設定します (範囲は 1 ~ 50、デフォルトは 10) 。
再試行	キープアライブ パケットが返されない際、ファイアウォールがトンネル ピアがダウンしているとみなすまでの間隔を設定します (範囲は 1 ~ 255、デフォルトは 3) 。
ホールドタイム	ファイアウォールがトンネル ピアと再び接続を確立するまでの間、キープアライブ パケットが成功する間隔を設定します (範囲は 1 ~ 64、デフォルトは 5) 。

© 2019 Palo Alto Networks, Inc.

Network > DHCP [ネットワーク > DHCP]

DHCP (Dynamic Host Configuration Protocol) は、TCP/IP およびリンク レイヤーの設定パラメータを提供し、また TCP/IP ネットワーク上で動的に設定されたホストにネットワーク アドレスを提供する標準プロトコルです。Palo Alto Networks ファイアウォールのインターフェイスは、DHCP サーバー、クライアント、またはリレー エージェントとして機能できます。これらの役割を別々のインターフェイスに割り当てることで、ファイアウォールは複数の役割を果たすことができます。

確認すべき情報	以下を参照
DHCP について。	DHCP の概要
DHCP サーバーがアドレスを割り当てる方法。	DHCP アドレス
ファイアウォールで以下の機能のインターフェイスを設定する。	
	DHCP サーバー
	DHCP リレー
	Network > DNS Proxy [ネットワーク > DNS プロキシ]
その他の情報をお探しですか？	DHCP

DHCP の概要

- Network > DHCP [ネットワーク > DHCP]

DHCP では、通信のクライアント-サーバー モデルが使用されます。このモデルにはファイアウォールが担うことのできる、次の3つの役割が含まれています。DHCPクライアント、DHCPサーバー、およびDHCPリレーエージェント。

- DHCPクライアント（ホスト）として機能するファイアウォールは、DHCPサーバーにIPアドレスやその他の設定を要求できます。クライアントファイアウォールのユーザーは、設定の時間と手間を省くことができます。また、DHCPサーバーから継承されるネットワークのアドレス計画やその他のネットワーク リソースおよびオプションを把握する必要もありません。
- DHCPサーバーとして機能するファイアウォールは、クライアントにサービスを提供できます。DHCPのアドレス メカニズムのいずれかを使用することで、管理者は設定時間を節約でき、クライアントでネットワーク接続が不要になったときに、限られた数の IP アドレスを再利用できます。サーバーは、IP アドレスと DHCP オプションを多数のクライアントに配信することもできます。
- DHCPリレーエージェントとして機能するファイアウォールは、ブロードキャストおよびユニキャストDHCPメッセージをリッスンし、それらをDHCPクライアントおよびサーバー間でリレーします。

DHCP は、トランスポート プロトコルとして、User Datagram Protocol（UDP）、RFC 768を使用します。クライアントからサーバーに送信される DHCP メッセージは、ウェルノウン ポート 6（UDP – ブートストラップ プロトコルおよび DHCP）に送信されます。サーバーからクライアントに送信される DHCP メッセージは、ポート 68 に送信されます。

DHCP アドレス

DHCP サーバーからクライアントへの IP アドレスの割り当てまたは送信を行う方法は 3 つあります。

© 2019 Palo Alto Networks, Inc.

- **Automatic allocation**[自動割り当て] — DHCP サーバーは、その **IP Pools**[IP プール] から永久的な IP アドレスをクライアントに割り当てます。ファイアウォールで **Lease**[リース] が **Unlimited**[無制限] として指定されている場合、永久的な割り当てになります。
- **Dynamic allocation**[動的な割り当て] — DHCP サーバーは、リースと呼ばれる最大期間で、アドレスの **IP Pools**[IP プール] の再利用可能な IP アドレスをクライアントに割り当てます。このアドレス割り当て方法は、顧客の IP アドレス数が限られている場合に便利です。この方法では、ネットワークへの一時的なアクセスのみが必要なクライアントに IP アドレスを割り当てることができます。
- **Static allocation**[静的な割り当て] — ネットワーク管理者はクライアントに割り当てる IP アドレスを選択し、DHCP サーバーはその IP アドレスをクライアントに送信します。静的なDHCPの割り当ては恒久的なものです。これを行う場合は、DHCPサーバーを設定し、クライアントファイアウォールの**MAC Address**[MACアドレス] に対応するように **Reserved Address**[予約済みアドレス] を選択します。クライアントが切断 (ログオフ、再起動、停電など) しても、DHCP の割り当てはそのまま保持されます。

  たとえば、LAN 上にプリンタがあり、DNS で LAN のプリンタの名前と IP アドレスが関連付けられているために、その IP アドレスが頻繁に変わらないようにする場合、IP アドレスの静的な割り当てが役立ちます。また、クライアントファイアウォールが何か重要な用途で使用されていて、ファイアウォールがオフになったり、プラグが抜かれたり、再起動したり、停電が発生したりしても、同じIPアドレスを保持する必要がある場合にも便利です。

  Reserved Address[予約済みアドレス] を設定するときは、以下の点に注意してください。

  - これは、**IP Pools**[IP プール] のアドレスです。複数の予約済みアドレスを設定できます。
  - **Reserved Address**[予約済みアドレス] を設定していない場合、サーバーのクライアントは、リースの有効期限が切れたり、再起動したりすると、プールから新しい DHCP の割り当てを受信します（**Lease**[リース] を **Unlimited**[無制限] に設定している場合は除く）。
  - **IP Pools**[IPプール] のすべてのアドレスを **Reserved Address**[予約済みアドレス] として割り当てると、アドレスを要求する次のDHCPクライアントに自由に割り当てることができる動的なアドレスがなくなります。
  - **Reserved Address**[MAC アドレス] を設定せずに **MAC Address**[予約済みアドレス] を設定できます。この場合、DHCPサーバーは、どのファイアウォールにも **Reserved Address**[予約済みアドレス] を割り当てません。プールのいくつかのアドレスを予約し、DHCP を使用せずに FAX やプリンタなどに静的に割り当てることができます。

DHCP サーバー

- Network > DHCP > DHCP Server [ネットワーク > DHCP > DHCP サーバー]

以下のセクションでは、DHCP サーバーの各構成要素について説明します。DHCP サーバーを設定する前に、仮想ルーターおよびゾーンに割り当てられるレイヤー 3 Ethernet またはレイヤー 3 VLAN インターフェイスを設定しておく必要があります。また、DHCP サーバーからクライアントに割り当てるように指定できる、ネットワーク計画の有効な IP アドレス プールを把握している必要もあります。

DHCP サーバーを追加するときは、以下の表に示す設定を行います。

DHCP サーバー設定	設定場所	の意味
インターフェイス	**DHCP** サーバー	DHCP サーバーとして機能するインターフェイスの名前。
モード		**enabled**[有効] モードまたは **auto**[自動] モードを選択します。**Auto**[自動] モードでは、サーバーが有効になりますが、ネットワークで別の DHCP サーバーが検出された場

© 2019 Palo Alto Networks, Inc.

DHCP サーバー設定	設定場所	の意味
		合は無効になります。**disabled**[無効] 設定を指定すると、サーバーが無効になります。
新しい IP を割り当てるときに IP に Ping する	**DHCP Server**（**DHCP** サーバー）> **Lease**	**Ping IP when allocating new IP**[新しい IP を割り当てるときに IP に Ping する] をクリックすると、サーバーは、IP アドレスに ping してから、そのアドレスをクライアントに割り当てます。pingが応答を受信した場合、そのアドレスはすでに別のファイアウォールに使用されているため、割り当てできないということを意味します。サーバーがプールから次のアドレスを割り当てます。このオプションを選択した場合は、表示されている [プローブ IP] 列にチェック マークが付けられます。
リース		リースのタイプを指定します。 • **Unlimited**[無制限] を指定すると、サーバーはIP Pools [IP プール] から動的に IP アドレスを選択し、クライアントに永久的に割り当てます。 • **Timeout**[タイムアウト] により、リースの継続時間が決まります。**Days**[日] および **Hours**[時間] の数値を入力し、必要に応じて **Minutes**[分] の数値を入力します。
IPプール		DHCP サーバーがアドレスを選択する IP アドレスのステートフル プールを指定し、DHCP クライアントに割り当てます。 単一のアドレス、アドレス/<マスクの長さ> (例: 192.168.1.0/24)、またはアドレスの範囲 (例: 192.168.1.10 ~ 192.168.1.20) を入力できます。
予約済みアドレス		必要な場合は、DHCP サーバーで動的に割り当てない IP プール内の IP アドレス (x.x.x.x 形式) を指定します。 **MAC Address**[MACアドレス] (xx:xx:xx:xx:xx:xx 形式) も一緒に指定した場合は、その MACアドレスに関連付けられたファイアウォールがDHCPを通じてIPアドレスを要求した際に、**Reserved Address**[予約済みアドレス] がそのフィアアウォールに割り当てられます。
継承ソース	**DHCP Server**（**DHCP** サーバー）> **Options** オプション	**None**[なし] (デフォルト) を選択するか、各種サーバーの設定を DHCP サーバーに配信するソース DHCP クライアント インターフェイスまたは PPPoE クライアント インターフェイスを選択します。**Inheritance Source**[継承ソース] を指定する場合は、このソースから**inherited**[継承]する以下のオプションを 1 つ以上選択します。 継承ソースを指定する利点の 1 つは、ソース DHCP クライアントのアップストリームであるサーバーから DHCP オプションがすばやく転送されることです。また、継承ソースのオプションが変更されても、クライアントのオプションが常に最新の状態に維持される点も挙げられます。たとえば、継承ソースファイアウォールでNTPサー

© 2019 Palo Alto Networks, Inc.

DHCP サーバー設定	設定場所	の意味
		バー（**Primary NTP**[プライマリNTP]サーバーとして識別されているサーバー）を置き換えると、クライアントは自動的に**Primary NTP**[プライマリNTP]サーバーとして新しいアドレスを継承します。
継承ソース状態のチェック		**Inheritance Source**（継承ソース）を選択した場合、**Check inheritance source status**（継承ソース状態のチェック）をクリックすると、Dynamic IP Interface Status（動的 IP インターフェイス状態）ウィンドウが開き、DHCP クライアントから継承されたオプションが表示されます。
ゲートウェイ	**DHCP Server**（**DHCP** サーバー）> **Options (cont)**オプション	この DHCP サーバーと同じ LAN 上にはないデバイスに到達するために使用するネットワーク ゲートウェイ (ファイアウォールのインターフェイス) の IP アドレスを指定します。
サブネット マスク		**IP Pools**[IP プール] のアドレスに適用するネットワーク マスクを指定します。
オプション		以下のフィールドでドロップダウン リストをクリックし、**None**（なし）または **inherited**（継承済み）を選択するか、そのサービスにアクセスするために DHCP サーバーがクライアントに送信するリモート サーバーの IP アドレスを入力します。**inherited**（継承済み）を選択すると、DHCP サーバーはソース DHCP クライアントから、**Inheritance Source**（継承ソース）として指定された値を継承します。 DHCP サーバーはこれらの設定をクライアントに送信します。 • **Primary DNS**[プライマリ DNS]、**Secondary DNS**[セカンダリ DNS] — 優先および代替 DNS (Domain Name System) サーバーの IP アドレス。 • **Primary WINS**[プライマリ WINS]、**Secondary WINS**[セカンダリ WINS] — 優先および代替 WINS (Windows Internet Naming Service) サーバーの IP アドレス。 • **Primary NIS**[プライマリ NIS]、**Secondary NIS**[セカンダリ NIS] — 優先および代替 NIS (Network Information Service) サーバーの IP アドレス。 • **Primary NTP**[プライマリ NTP]、**Secondary NTP**[セカンダリ NTP] — 使用可能な NTP (Network Time Protocol) サーバーの IP アドレス。 • **POP3 Server**[POP3 サーバー] — POP3 (Post Office Protocol version 3) サーバーの IP アドレス。 • **SMTP Server**[SMTP サーバー] — Simple Mail Transfer Protocol（SMTP）サーバーの IP アドレス。

© 2019 Palo Alto Networks, Inc.

DHCP サーバー設定	設定場所	の意味
		• **DNS Suffix**[DNS サフィックス] – 解決できない非修飾ホスト名が入力されたときにクライアントがローカルで使用するサフィックス。
カスタム DHCP オプション		**Add**[追加] をクリックし、DHCP サーバーからクライアントに送信するカスタム オプションの**Name**[名前]を入力します。 **Option Code**[オプションコード] (範囲は1 ~ 254) を入力します。 **Option Code 43**[オプション コード 43] を入力すると、Vendor Class Identifier (VCI) [ベンダー クラス ID (VCI)] フィールドが表示されます。クライアントのオプション 60 から受信した VCI と比較する一致基準を入力します。ファイアウォールは、クライアントのオプション 60 から受信した VCI を検査し、専用の DHCP サーバー テーブルで一致する VCI を検索し、それに対応する値をオプション 43 のクライアントに返します。VCI 一致基準は、文字列または 16 進値です。16 進値のプレフィックスは「0x」にする必要があります。 **Inherited from DCHP server inheritance source** (**DHCP** サーバーの継承元から継承) を選択すると、サーバーは、そのオプション コードの値を継承元から継承します。ユーザーが **Option Value** (オプション値) を入力する必要はありません。 このオプションの代わりに、以下の方法を使用することもできます。 **Option Type**[オプションタイプ]:**IP Address** (**IP**アドレス)、**ASCII**、または**Hexadecimal** (**16**進数) を選択し、Option Value (オプション値) に使用するデータのタイプを指定します。 **Option Value**[オプション値] で **Add**[追加] をクリックし、カスタム オプションの値を入力します。

DHCP リレー

- Network > DHCP > DHCP Relay [ネットワーク > DHCP > DHCP リレー]

DHCP リレーエージェントとしてファイアウォール インターフェイスを設定する前に、レイヤー 3 Ethernet またはレイヤー 3 VLAN インターフェイスが設定されていることと、インターフェイスが仮想ルーターおよびゾーンに割り当てられていることを確認します。そのインターフェイスでクライアントとサーバー間の DHCP メッセージを渡すことができるようにします。それぞれのインターフェイスは、最大で8つの外部IPv4 DHCPサーバーと8つの外部IPv6 DHCPサーバーへメッセージを転送することができます。クライアントのDHCPDISCOVERメッセージは、設定されたすべてのサーバーに送信され、ファイアウォールは、要求を行ったクライアントに最初に応答したサーバーのDHCPOFFERメッセージをリレーします。

© 2019 Palo Alto Networks, Inc.

DHCP リレー設定	の意味
インターフェイス	DHCP リレー エージェントになるインターフェイスの名前。
IPv4 / IPv6	指定する DHCP サーバーと IP アドレスのタイプを選択します。
DHCP サーバー IP アドレス	DHCP メッセージのリレー先およびリレー元の DHCP サーバーの IP アドレスを入力します。
インターフェイス	DHCP サーバーの IP アドレス プロトコルとして IPv6 を選択し、マルチキャスト アドレスを指定した場合は、出力インターフェイスも指定する必要があります。

DHCP クライアント

- Network > Interfaces > Ethernet > IPv4 [ネットワーク > インターフェイス > イーサネット > IPv4]
- Network > Interfaces > VLAN > IPv4 [ネットワーク > インターフェイス > VLAN > IPv4]

DHCP クライアントとしてファイアウォール インターフェイスを設定する前に、レイヤー 3 Ethernet またはレイヤー 3 VLAN インターフェイスが設定されていることと、インターフェイスが仮想ルーターおよびゾーンに割り当てられていることを確認します。このタスクは、DHCP を使用してファイアウォールのインターフェイスの IPv4 アドレスを要求する必要がある場合に実行します。

DHCP クライアント設定	の意味
タイプ	インターフェイスを DHCP クライアントとして設定する場合は、**DHCP Client**[DHCP クライアント] を選択し、次に**Enable**[有効化] を選びます。
サーバー提供のデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成	ファイアウォールがデフォルト ゲートウェイへのスタティック ルートを作成します。これは、ファイアウォールのルーティング テーブルにルートを保持する必要がないため、クライアントが多数の宛先にアクセスする場合に便利です。
デフォルト ルート メトリック	必要に応じて、ファイアウォールと DHCP サーバー間のルートの **Default Route Metric**[デフォルト ルート メトリック] (優先順位レベル) を入力します。数値の低いルートほど、ルート選択時の優先順位が高くなります。たとえば、メトリックが10のルートは、メトリックが100のルートよりも前に使用されます (範囲は1 ~ 65535、デフォルトはなし) 。
DHCP クライアント ランタイム情報の表示	DHCP のリース状態、ダイナミック IP 割り当て、サブネット マスク、ゲートウェイ、サーバー設定 (DNS、NTP、ドメイン、WINS、NIS、POP3、および SMTP) など、DHCP サーバーから受信したすべての設定が表示されます。

© 2019 Palo Alto Networks, Inc.

Network > DNS Proxy [ネットワーク > DNS プロキシ]

DNS サーバーは、ドメイン名から IP アドレス、および IP アドレスからドメイン名を解決するサービスを実行します。ファイアウォールを DNS プロキシとして設定すると、ファイアウォールはクライアントとサーバー間の中継役として機能します。また、DNS キャッシュからのクエリを解決したり、クエリを別の DNS サーバーに送信したりすることで、DNS サーバーとしても機能します。このページは、ファイアウォールがどのような方法で DNS プロキシとして機能するかを設定する場合に使用します。

知りたい内容	以下を参照
ファイアウォール プロキシ DNS の要求方法。	DNS プロキシの概要
DHCP プロキシの設定方法。	DNS プロキシ設定
スタティック FQDN から IP アドレスへのマッピングの設定方法。	
DNS プロキシの管理方法。	その他の DNS プロキシ アクション
その他の情報をお探しですか？	DNS

DNS プロキシの概要

DNS サーバーとして機能するようにファイアウォールを設定できます。まず、DNS プロキシを作成し、プロキシを適用するインターフェイスを選択します。次に、DNS プロキシ キャッシュにドメイン名が見つからない場合（およびドメイン名がプロキシ ルールに一致しない場合）にファイアウォールが DNS クエリを送信するデフォルトのプライマリおよびセカンダリ DNS サーバーを指定します。

ドメイン名に基づいて DNS クエリを別の DNS サーバーに転送するには、DNS プロキシ ルールを作成します。複数の DNS サーバーを指定すると、DNS クエリを確実にローカライズし、効率を向上させることができます。たとえば、企業の DNS クエリはすべて企業の DNS サーバーに転送し、他のクエリはすべて ISP DNS サーバーに転送できます。

以下のタブを使用して、（デフォルトのプライマリおよびセカンダリ DNS サーバー以外に）DNS プロキシを定義します。

- **Static Entries**（スタティック エントリ）– DNS クエリに対してファイアウォールがキャッシュしてホストに送信する FQDN と IP アドレスのスタティック マッピングを設定できます。
- **DNS Proxy Rules**（**DNS** プロキシ ルール）– ドメイン名と、対応するプライマリおよびセカンダリ DNS サーバーを指定して、ルールに一致するクエリを解決できます。DNS プロキシ キャッシュにドメイン名が見つからない場合、ファイアウォールは、（クエリが到達するインターフェイス上の）DNS プロキシで一致するドメイン名を検索し、その一致結果に基づいてクエリを DNS サーバーに転送します。一致する結果がない場合、ファイアウォールはクエリをデフォルトのプライマリおよびセカンダリ DNS サーバーに送信します。ルールに一致するドメインのキャッシングを有効にできます。
- **Advanced (詳細)**–DNS プロキシ オブジェクトを使用してファイアウォールが生成する DNS/FQDN クエリを解決する場合は、キャッシュ (**Cache (キャッシュ)**を選択) と **Cache EDNS Responses (キャッシュ EDNS 応答)** を有効にする必要があります 。Advanced (詳細) タブでは、TCP クエリと UDP クエリの再試行を制御することもできます。ファイアウォールは、設定されたインターフェイスで TCP ま

© 2019 Palo Alto Networks, Inc.

たは UDP DNS クエリを送信します。DNS クエリの応答が 1 つの UDP パケットに対して長すぎる場合、UDP クエリは TCP に切り替えられます。

DNS プロキシ設定

Add（追加）をクリックし、DNS プロキシとして機能するようにファイアウォールを設定できます。最大 256 個の DNS プロキシをファイアウォールに設定できます。

DNS プロキシ設定	設定場所	の意味
Enable [有効化]	**DNS**プロキシ	この DNS プロキシを有効にする場合に選択します。
氏名		DNS プロキシ オブジェクトの識別に使用する名前を指定します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所		DNS プロキシ オブジェクトの適用先の仮想システムを指定します。 • **Shared**（共有）：プロキシはすべての仮想システムに適用されます。**Shared**[共有] を選択した場合、**Server Profile**[サーバー プロファイル] フィールドは使用できません。代わりに、**Primary**（プライマリ）および **Secondary**（セカンダリ）の DNS サーバー IP アドレスまたはアドレス オブジェクトを入力します。 • この DNS プロキシを使用する仮想システムを選択します。最初に仮想システムを設定する必要があります。**Device**[デバイス] > **Virtual Systems**[仮想システム] に移動し、仮想システムを選択してから、**DNS Proxy**[DNSプロキシ] を選択します。
継承ソース （共有場所のみ）		デフォルトの DNS サーバー設定を継承する送信元を選択します。これは一般的に、ファイアウォールの WAN インターフェイスが DHCP または PPPoE でアドレス指定される支社の導入で使用されます。
継承ソース状態のチェック （共有場所のみ）		DHCP クライアント インターフェイスおよび PPPoE クライアント インターフェイスに現在割り当てられているサーバー設定を確認する場合に選択します。これには、DNS、WINS、NTP、POP3、SMTP、または DNS サフィックスなどが含まれます。
Primary/Secondary （共有場所のみ）		このファイアウォールが（DNS プロキシとして）DNS クエリを送信するデフォルトのプライマリおよびセカンダリ DNS サーバーの IP アドレスを指定します。プライマリ DNS サーバーが見つからないと、ファイアウォールはセカンダリ DNS サーバーを使用します。
サーバ プロファイル		新規 DNS サーバー プロファイルを選択または作成します。仮想システムの場所を [共有] として指定した場合は、このフィールドは表示されません。

© 2019 Palo Alto Networks, Inc.

DNS プロキシ設定	設定場所	の意味
（仮想システムの場所のみ）		
インターフェイス		DNS プロキシとして機能するインターフェイスを **Add**（追加）します。複数のインターフェイスを追加できます。インターフェイスから DNS プロキシを削除する場合は、それを選択して **Delete**（削除）します。 DNS プロキシをサービス ルート機能専用で使用している場合は、インターフェイスは不要です。宛先サービス ルートで送信元 IP アドレスを設定する場合、インターフェイスを持たない DNS プロキシとともに宛先サービス ルートを使用します。そうしない場合、DNS プロキシは、送信元として使用するインターフェイス IP アドレスを選択します（DNS サービス ルートが設定されていない場合）。
氏名	**DNS Proxy[DNS プロキシ] > DNS Proxy Rules [DNS プロキシ ルール]**	CLI 経由でエントリを参照および変更できるようにするには、名前が必要です。
このマッピングによって解決されるドメインのキャッシングをオンにする		このマッピングで解決されるドメインのキャッシングを有効にする場合に選択します。
ドメイン名		ファイアウォールが受信 FQDN を比較する 1 つ以上のドメイン名を **Add**（追加）します。FQDN がルールのいずれかのドメインに一致すると、ファイアウォールはこのプロキシに指定されたプライマリ/セカンダリ DNS サーバーにクエリを転送します。ルールからドメイン名を削除するには、ドメイン名を選択して **Delete**（削除）をクリックします。
DNSサーバ プロファイル （共有場所のみ）		仮想システムの DNS 設定（ファイアウォールがドメイン名のクエリを送信するプライマリおよびセカンダリ DNS サーバーなど）を定義する DNS サーバー プロファイルを選択または追加します。
Primary/Secondary （仮想システムの場所のみ）		ファイアウォールが一致するドメイン名のクエリを送信するときの宛先となるプライマリおよびセカンダリ DNS サーバーのホスト名または IP アドレスを入力します。
氏名	**DNS Proxy（DNS プロキシ）> Static Entries（スタティック エントリ）**	スタティック エントリの名前を入力します。
FQDN		Address（アドレス）フィールドで定義されたスタティック IP アドレスにマッピングするための完全修飾ドメイン名（FQDN）を入力します。
アドレス		このドメインにマッピングする 1 つ以上の IP アドレスを **Add**（追加）します。ファイアウォールがこれらのすべてのアドレスを DNS 応答に含め、クライアントは使用する IP アドレスを選択します。アドレスを削除するには、アドレスを選択して **Delete**[削除] をクリックします。

© 2019 Palo Alto Networks, Inc.

DNS プロキシ設定	設定場所	の意味
TCP クエリ	**DNS Proxy** > **Advanced**	TCP を使用する DNS クエリを有効にする場合に選択します。ファイアウォールでサポートされる同時未解決 TCP DNS 要求の最大数 (**Max Pending Requests** (リクエスト最大保留数)) を指定します (範囲は 64 ~ 256、デフォルトは 64)。
UDP クエリの再試行	**DNS Proxy** > **Advanced**	UDP クエリの再試行の設定を指定します。 • **Interval** (間隔) — 応答を受信しなかった場合に DNS プロキシが別の要求を送信するまでの時間 (秒) (範囲は 1 ~ 30、デフォルトは 2)。 • **Attempts** (試行回数) — DNSP が次の DNS サーバーを試行するまでの最大試行回数 (最初の試行は除く) (範囲は 1 ~ 30、デフォルトは 5)。
Cache	**DNS Proxy** > **Advanced**	ファイアウォールが生成するクエリにこの DNS プロキシ オブジェクトを使用する場合 (つまり、**Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** > **DNS**、または **Device(デバイス)** > **Virtual Systems (仮想システム)** で、virtual system (仮想システム - vsys) と **General (全般)** > **DNS** プロキシを選択) **Cache** を有効にする必要があります。次に、以下を指定します。 • **Enable TTL** (**TTL** の有効化) — ファイアウォールがプロキシ オブジェクトの DNS エントリをキャッシュする時間の長さを制限します。TTL はデフォルトで無効になっています。次に、**Time to Live (sec)** (有効時間 (秒)) を入力します — これはプロキシ オブジェクトのキャッシュされたすべてのエントリが削除されるまでの秒数です。新しい DNS 要求は解決して再度キャッシュする必要があります。範囲は 60 ~ 86,400。デフォルトの TTL はありません。エントリはファイアウォールのキャッシュ メモリがなくなるまで保持されます。 • **Cache EDNS Responses (キャッシュ EDNS 応答)**—ファイアウォールが生成するクエリにこの DNS プロキシ オブジェクトを使用する場合は、DNS (EDNS) 応答のキャッシュ拡張メカニズムを有効にする必要があります。FQDN アドレス オブジェクトのクエリが成功するには、ファイアウォールが DNS 応答をキャッシュできる必要があります。

その他の DNS プロキシ アクション

ファイアウォールをDNSプロキシとして設定した後、**Network**[ネットワーク] > **DNS Proxy [DNS**プロキシ] ページで以下のアクションを実行し、DNSプロキシ設定を管理できます。

- **Modify**[変更] — DNS プロキシを変更するには、DNSプロキシ設定の名前をクリックします。
- **Delete**[削除] — DNS プロキシエントリを選択し、**Delete**[削除] をクリックすると、DNSプロキシ設定が削除されます。
- **Disable**[無効化] — DNSプロキシを無効にするには、DNSプロキシエントリの名前をクリックし、**Enable**[有効化] を選択解除します。無効になっている DNS プロキシを有効にするには、DNS プロキシ エントリの名前をクリックし、**Enable**[有効化] を選択します。

© 2019 Palo Alto Networks, Inc.

Network > QoS [ネットワーク > QoS]

以下のトピックでは、サービス品質（QoS）について説明します。

確認すべき情報	以下を参照
インターフェイスの帯域幅制限を設定し、インターフェイスから出ていくトラフィックの QoS を適用する。	QoS インターフェイス設定
QoS 対応のインターフェイスから出ていくトラフィックをモニターする。	QoS インターフェイスの統計情報
その他の情報をお探しですか？	QoS の詳細なワークフロー、コンセプト、使用例についてはサービス品質を参照してください。
	一致するトラフィックに QoS クラスを割り当てるには、 Policies > QoS [ポリシー > QoS]を選択し、最大 8 つの QoS クラスの帯域幅制限と優先順位を定義するには、 Network（ネットワーク） > Network Profiles（ネットワーク プロファイル） > QoSを選択してください。

QoS インターフェイス設定

インターフェイスの帯域幅制限を設定し、インターフェイスからの出力トラフィックにQoSを適用する場合は、インターフェイス上でQoSを有効にします。QoS インターフェイスを有効にするには、QoS プロファイルをインターフェイスに追加する必要があります。QoS は物理インターフェイスでサポートされますが、ファイアウォール モデルによっては、サブインターフェイスやイーサネットの集約（AE）インターフェイスでもサポートされます。お使いのファイアウォール モデルでサポートされている QoS 機能を確認するには、Palo Alto Networks の製品比較ツールを参照してください。

最初に QoS インターフェイスの **Add**（追加）または編集を行い、次に以下の表に記載されているように設定します。

QoS インターフェイス設定	設定場所	の意味
インターフェイス名	**QoS Interface**（**QoS** インターフェイス）> **Physical Interface**（物理インターフェイス）	QoS を有効にするファイアウォール インターフェイスを選択します。
最大保証帯域　出力側 (Mbps)		このインターフェイスを介してファイアウォールから出力されるトラフィックの最大スループット（Mbps）を入力します。値はデフォルトで 0 で、ファイアウォール制限（PAN-OS 7.1.16 以降のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースでは16,000）を指定します。

© 2019 Palo Alto Networks, Inc.

QoS インターフェイス設定	設定場所	の意味
		Egress Max（最大保証帯域 出力側）は必須フィールドではありませんが、*QoS*インターフェイスのこの値は常に定義しておくことをお勧めします。
このインターフェイスの QoS 機能をオンにする		選択したインターフェイスで QoS を有効にする場合に選択します。
クリア テキスト トンネルインターフェイス	**QoS Interface**（**QoS** インターフェイス）> **Physical Interface**（物理インターフェイス）> **Default Profile**（デフォルト プロファイル）	クリア テキスト トラフィックおよびトンネル トラフィックのデフォルトの QoS プロファイルを選択します。それぞれにデフォルトのプロファイルを指定する必要があります。クリア テキスト トラフィックの場合、デフォルトのプロファイルはすべてのクリア テキスト トラフィックに一括適用されます。トンネル トラフィックの場合、デフォルトのプロファイルは、詳細設定セクションで特定のプロファイルが割り当てられていない各トンネルに個別に適用されます。QoS プロファイルを定義する手順については、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> QoS」を参照してください。
トンネルインターフェイス		
最低保証帯域 出力側 (Mbps)	**QoS Interface** インターフェイス > **Clear Text Traffic** クリア テキスト トラフィック/ **Tunneled Traffic**/トンネル対象トラフィック]	このインターフェイスからのクリア テキストまたはトンネル対象トラフィックに保証される帯域幅を入力します。
最大保証帯域　出力側 (Mbps)		このインターフェイスを介してファイアウォールから出力されるクリア テキストまたはトンネル通過するトラフィックの最大スループット（Mbps）を入力します。値はデフォルトで 0 で、ファイアウォール制限（PAN-OS 7.1.16 以降のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースでは16,000）を指定します。クリア テキストまたはトンネル通過するトラフィックの **Egress Max**（最大保証帯域出力側）は、物理インターフェイスの **Egress Max**（最低保証帯域 出力側）以下でなければなりません。

コンテキストの		• クリアテキストトラフィックの処理内容をより詳細に定義する場合は、**Clear Text Traffic** [クリアテキストトラフィック] タブで **Add** [追加] をクリックします。個々のエントリをクリックして、以下の設定を指定します。
		  • **Name**[名前] — ここでの設定の識別に使用する名前を入力します。
		  • **QoS Profile**[QoS プロファイル] — 指定したインターフェイスとサブネットに適用する QoS プロファイルを選択します。QoS プロファイルを定義する手順については、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> QoS」を参照してください。
		  • **Source Interface**[送信元インターフェイス] — 送信元側のファイアウォール インターフェイスを選択します。
		  • **Source Subnet**[送信元サブネット] — 送信元のサブネットを選択すると、そのサブネットからのトラフィックのみに各設定が適用されます。デフォルト値の **any** [いずれか]をそのまま使用すると、指定したインターフェイスからのすべてのトラフィックに対して各設定が適用されます。

© 2019 Palo Alto Networks, Inc.

QoS インターフェイス設定	設定場所	の意味
		• 特定のトンネルに対するデフォルトプロファイルの割り当てをオーバーライドする場合は、**Tunneled Traffic** [トンネル対象トラフィック] タブで **Add** [追加] をクリックし、以下の設定を指定します。 • **Tunnel Interface**[トンネル インターフェイス] – ファイアウォールのトンネル インターフェイスを選択します。 • **QoS Profile**[QoS プロファイル] – 指定したトンネル インターフェイスに適用する QoS プロファイルを選択します。 たとえば、ファイアウォールに対して 45 Mbps で接続するサイトと T1 で接続するサイトを設定するとします。このとき、T1 サイトには接続が過負荷状態にならないように制限の厳しい QoS 設定を適用する一方で、45 Mbps で接続するサイトにはより柔軟な設定を適用できます。 クリアテキストまたはトンネル対象トラフィックのエントリを削除する場合は、エントリを空白にして**Delete**[削除] をクリックします。 [クリア テキスト] または [トンネル対象トラフィック] セクションが空白のままの場合、[物理インターフェイス] タブの [デフォルト プロファイル] セクションで指定した値が使用されます。

QoS インターフェイスの統計情報

- Network (ネットワーク) > QoS > Statistics (統計)

QoSインターフェイスで、設定済のQoSインターフェイスの帯域幅、セッション、およびアプリケーションの情報を表示する場合は**Statistics** [統計] を選択します。

QoS 統計情報	の意味
帯域幅	選択したノードとクラスの帯域幅チャートがリアルタイムで表示されます。この情報は 2 秒ごとに更新されます。 *QoS* クラスに設定された *Egress Max* (最大保証帯域　出力側) と *Egress Guaranteed* (最低保証帯域　出力側) の制限は、*QoS* 統計情報画面では若干異なる値で表示される場合があります。これは、ハードウェア エンジンが帯域幅の制限とカウンタを集約する方法によって発生する正常動作です。帯域幅の使用率グラフにはリアルタイムの値と数量が表示されるため、運用上の問題はありません。
アプリケーション [applications]	選択した QoS ノードやクラスのアクティブなアプリケーションすべてのリストが表示されます。
送信元ユーザー	選択した QoS ノードやクラスのアクティブな送信元ユーザーすべてのリストが表示されます。
宛先ユーザー	選択した QoS ノードやクラスのアクティブな宛先ユーザーすべてのリストが表示されます。

© 2019 Palo Alto Networks, Inc.

QoS 統計情報	の意味
セキュリティルール数	選択した QoS ノードやクラスに一致し、それを適用するセキュリティ ルールのリストが表示されます。
QoS ルール	選択した QoS ノードやクラスに一致し、それを適用する QoS ルールのリストが表示されます。

© 2019 Palo Alto Networks, Inc.

Network > LLDP [ネットワーク > LLDP]

リンク レイヤー検出プロトコル (LLDP) では、リンク レイヤーの隣接するデバイスとその機能を自動的に検出できます。

確認すべき情報	以下を参照
LLDP について。	LLDP の概要
LLDP を設定する。	LLDP の構成要素
LLDP プロファイルを設定する。	Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]
その他の情報をお探しですか？	LLDP

LLDP の概要

LLDP を使用すると、ファイアウォールは、LLDP データ ユニット (LLDPDU) を含む Ethernet フレームをネイバーとの間で送受信できます。受信デバイスは、情報を MIB に保存します。MIB にアクセスするには、SNMP (Simple Network Management Protocol) を使用します。ネットワーク デバイスは、LLDP によってネットワーク トポロジをマッピングし、接続されているデバイスの機能を学習できます。これによってトラブルシューティングが容易になります。特にそれが顕著なのは、ネットワーク トポロジでファイアウォールが基本的に検出されないようなバーチャル ワイヤーのデプロイにおいてです。

LLDP の構成要素

ファイアウォールでLLDPを有効にする場合は、Edit [編集] をクリックして**Enable**[有効化] をクリックします。デフォルト設定が環境に適していない場合は、以下の表に示す4つの設定を必要に応じて行います。表の残りのエントリは、状態とピアの統計を示しています。

LLDP 設定	設定場所	の意味
送信間隔 (秒)	**LLDP** 一般	LLDPDUが送信される間隔（秒数）を指定します（範囲は1～3600、デフォルトは30）。
送信遅延 (秒)		TLV（Type-Length-Value）要素が変更された後に送信されるLLDP発信の遅延間隔秒数を指定します。多数のネットワーク変更により LLDP 変更の数が急増した場合、またはインターフェイスがフラップした場合は、この遅延により、セグメントが LLDPDU であふれることが防止されます。**Transmit Delay**[送信遅延] の値は、**Transmit Interval**[送信間隔] よりも小さくする必要があります（範囲は1～600、デフォルトは2）。
ホールド タイムの間隔数		TTLホールドタイムの合計を求めるために **Transmit Interval**[送信間隔] で乗算される値を指定します（範囲は1～100、デフォルトは4）。

© 2019 Palo Alto Networks, Inc.

LLDP 設定	設定場所	の意味
		TTL ホールド タイムは、ファイアウォールがピアからの情報を有効であるとして保持する時間の長さです。TTL ホールド タイムの最大値は、乗数値にかかわらず 65535 秒です。
通知間隔		MIBが変更されたときにSyslog およびSNMPトラップ通知が送信される間隔（秒数）を指定します（範囲は1～3600、デフォルトは5）。
スパイグラスフィルタ	**LLDP** 状態 > **Status**	必要に応じて、フィルタ行にデータ値を入力し、灰色の矢印をクリックします。これにより、そのデータ値を含む行のみが表示されます。フィルタをクリアするには、赤色の X をクリックします。
インターフェイス		LLDP プロファイルが割り当てられているインターフェイスの名前。
LLDP		LLDP の状態で、enabled [有効] またはdisabled [無効] のいずれかです。
モード		インターフェイスのLLDPモード:Tx/Rx、Txのみ、またはRxのみです。
プロファイル		インターフェイスに割り当てられたプロファイルの名前。
送信合計		インターフェイスから送信された LLDPDU の数。
ドロップされた送信		エラーが原因でインターフェイスから送信されなかった LLDPDU の数。エラーの例としては、送信する LLDPDU をシステムが作成中に発生した長さのエラーなどがあります。
受信合計		インターフェイスで受信した LLDP フレームの数。
ドロップされた TLV		受信時に破棄された LLDP フレームの数。
エラー		インターフェイスで受信した TLV (Time-Length-Value) 要素のうち、エラーが含まれていたものの数。TLV エラーのタイプとしては、1 つ以上の必須 TLV が欠落している、順序が適切でない、範囲外の情報が含まれている、長さのエラーなどがあります。
認識不可		インターフェイスで受信した TLV のうち、LLDP ローカル エージェントで認識されないものの数。TLV が認識されない原因としては、たとえば、TLV のタイプが予約済みの TLV の範囲内にあることなどが挙げられます。
エージアウト済み		適切な TTL が期限切れになったために受信 MIB から削除された項目の数。
LLDP 統計のクリア		LLDP 統計をすべてクリアする場合に選択します。
スパイグラスフィルタ	**LLDP** ピア > **Peers**	必要に応じて、フィルタ行にデータ値を入力し、灰色の矢印をクリックします。これにより、そのデータ値を含む行のみ

© 2019 Palo Alto Networks, Inc.

LLDP 設定	設定場所	の意味
		が表示されます。フィルタをクリアするには、赤色の X をクリックします。
ローカル インターフェイス		隣接するデバイスを検出したファイアウォール上のインターフェイス。
Remote Chassis ID		ピアのシャーシ ID。MAC アドレスが使用されます。
ポート ID	**LLDP** ピア > **Peers(cont)**	ピアのポート ID。
氏名		ピアの名前。
詳細		**More Info**[詳細情報] をクリックすると、必須および任意のTLVに基づくリモートピアの詳細が表示されます。
シャーシのタイプ		シャーシのタイプは MAC アドレスです。
MAC アドレス		ピアの MAC アドレス。
システム名		ピアの名前。
システムの説明		ピアの説明。
ポートの説明		ピアのポートの説明。
ポートのタイプ		インターフェイス名。
ポート ID		ファイアウォールは、インターフェイスの ifname を使用します。
システムの機能		システムの機能。O はその他、P はリピータ、B はブリッジ、W はワイヤレス LAN、R はルーター、T は電話を表します。
有効になっている機能		ピアで有効になっている機能。
管理アドレス		ピアの管理アドレス。

© 2019 Palo Alto Networks, Inc.

Network（ネットワーク） > Network Profiles（ネットワーク プロファイル）

以下のトピックでは、ネットワーク プロファイルについて説明します。

- Network > Network Profiles > GlobalProtect IPSec Crypto [ネットワーク > ネットワーク プロファイル]> GlobalProtect の IPSec 暗号]
- Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]
- Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プロファイル > IPSec 暗号]
- Network > Network Profiles > IKE Crypto [ネットワーク > ネットワーク プロファイル > IKE 暗号]
- Network > Network Profiles > Monitor [ネットワーク > ネットワーク プロファイル > 監視]
- Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理]
- Network > Network Profiles > Zone Protection [ネットワーク > ネットワークプロファイル > ゾーンプロテクション]
- Network（ネットワーク） > Network Profiles（ネットワーク プロファイル） > QoS
- Network > Network Profiles > LLDP Profile [ネットワーク > ネットワーク プロファイル > LLDP プロファイル]
- Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル]
- Network > Network Profiles > SD-WAN [ネットワーク > ネットワーク プロファイル > SD-WAN インターフェイス プロファイル]

Network > Network Profiles > GlobalProtect IPSec Crypto [ネットワーク > ネットワーク プロファイル]> GlobalProtect の IPSec 暗号]

GlobalProtect IPSec Crypto Profiles[GlobalProtect の IPSec暗号化プロファイル] ページを使用して、GlobalProtect ゲートウェイとクライアント間の VPN トンネルで認証および暗号化を行うためのアルゴリズムを指定します。アルゴリズムを追加する順序は、ファイアウォールがアルゴリズムを適用する順序であり、トンネルのセキュリティとパフォーマンスに影響する場合があります。この順番を変更する場合は、テンプレートを選択して **Move Up**[上へ]または**Move Down**[下へ] をクリックします。

GlobalProtect ゲートウェイとサテライト（ファイアウォール）間の *VPN* トンネルについては、「Network（ネットワーク） > Network Profiles（ネットワーク プロファイル） > IPSec Crypto（IPSec 暗号）」を参照してください。

GlobalProtect の IPSec 暗号化プロファイル設定	
氏名	プロファイルの識別に使用する名前を入力します。名前は大文字小文字を区別し、一意の名前にする必要があります。最大 **31** 文字を使用できます。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
暗号化	**Add**[追加] をクリックし、目的の暗号化アルゴリズムを選択します。セキュリティを最大限に高めるため、降順で順序を以下のように変更します。**aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.

© 2019 Palo Alto Networks, Inc.

GlobalProtect の IPSec 暗号化プロファイル設定	
authentication	**Add**[追加] をクリックし、認証アルゴリズムを選択します。現在のオプションは、**sha1** のみです。

Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]

このページを使用して、ゲートウェイを管理または定義します。このページには、ピア ゲートウェイに対して Internet Key Exchange (IKE) プロトコル ネゴシエーションを実行するために必要な設定情報が含まれています。これは、IKE/IPSec VPN セットアップのフェーズ 1 の部分です。

IKE ゲートウェイを管理、設定、再起動、または更新する方法については、以下を参照してください。

- IKE ゲートウェイ管理
- IKE ゲートウェイの [全般] タブ
- IKE ゲートウェイの Advanced Options (詳細オプション) タブ
- IKE ゲートウェイの再起動または更新

IKE ゲートウェイ管理

- Network > Network Profiles > IKE Gateways [ネットワーク > ネットワーク プロファイル > IKE ゲートウェイ]

以下の表は、IKE ゲートウェイの管理方法を示しています。

IKE ゲートウェイの管理	の意味
コンテキストの	新しい IKE ゲートウェイを作成するには、**Add**[追加] をクリックします。新しいゲートウェイの設定方法は「IKE ゲートウェイの General (全般) タブ」および「IKE ゲートウェイの Advanced Options (詳細オプション) タブ」を参照してください。
削除します。	ゲートウェイを削除するには、ゲートウェイを選択して **Delete**[削除] をクリックします。
Enable [有効化]	無効になっているゲートウェイを有効にするには、ゲートウェイを選択して **Enable**[有効化] をクリックします。デフォルト設定では、ゲートウェイは有効になっています。
無効化	ゲートウェイを無効にするには、ゲートウェイを選択して **Disable**[無効化] をクリックします。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、オブジェクト設定を **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export (設定バンドルのエクスポート) 」を参照してください。

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの [全般] タブ

- Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> IKE Gateways（IKE ゲートウェイ）> General（一般）

以下の表は、 configure an IKE gateway（IKE ゲートウェイの設定）の最初の手順を示しています。IKE は、IKE/IPSec VPN プロセスのフェーズ 1 です。この設定の実行後、「IKE Gateway Advanced Options Tab（IKE ゲートウェイの詳細オプション タブ）」を参照してください。

IKE ゲートウェイの一般設定	の意味
氏名	ゲートウェイを識別する**Name**（名前）を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
バージョン	ゲートウェイにサポートされていて、ピアゲートウェイと必ず使用する必要のあるIKEバージョンを選択します。**IKEv1 only mode**（**IKEv1**限定モード）、**IKEv2 only mode**（**IKEv2**限定モード）、または**IKEv2 preferred mode**（**IKEv2**優先モード）。IKEv2 優先モードでは、ゲートウェイが IKEv2 をネゴシエートします。これは、ピアが IKEv2 もサポートしている場合に使用されます。 それ以外の場合、ゲートウェイは IKEv1 にフォールバックします。
アドレス タイプ	ゲートウェイが使用する IP アドレスのタイプを選択します。**IPv4**あるいは**IPv6**
インターフェイス	VPN トンネルに対する出力ファイアウォール インターフェイスを選択します。
ローカル IP アドレス	トンネルのエンドポイントとなるローカル インターフェイスの IP アドレスを選択または入力します。
ピアIPアドレス タイプ	次のいずれかの設定を選択し、ピアの対応する情報を入力します。 • **Dynamic**（動的）–ピア IP アドレスまたは FQDN 値が不明な場合は、このオプションを選択します。ピア IP アドレス タイプが動的の場合、IKE ゲートウェイ ネゴシエーションを開始するのはピアまでです。 • **IP**–IPv4 アドレスまたは IPv6 アドレス、もしくは IPv4 または IPv6 アドレスであるアドレス オブジェクトとして **Peer Address**（ピア アドレス）を入力します。 • **FQDN**–FQDN または FQDN を使用するアドレス オブジェクトとして **Peer Address**（ピア アドレス） を入力します。 複数の IP アドレスに解決される FQDN または FQDN アドレス オブジェクトを入力すると、ファイアウォールは次のように IKE ゲートウェイのアドレス タイプ（IPv4 または IPv6）と一致するアドレス セットから優先アドレスを選択します。 • IKE セキュリティ アソシエーション（SA）がネゴシエートされていない場合、優先アドレスは最小値のIPアドレスです。 • アドレスが IKE ゲートウェイによって使用され、返されたアドレスのセット内にある場合は、そのアドレスが使用されます（最小であるかどうかにかかわらず）。

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの一般設定	の意味
	• アドレスが IKE ゲートウェイによって使用されているが、返されたアドレスのセットに含まれていない場合は、新しいアドレスが選択されます。 *FQDN* または *FQDN* アドレス オブジェクトを使用すると、ピアが動的 *IP* アドレス変更の対象となる環境での問題が軽減されます（この *IKE* ゲートウェイ ピア アドレスを再設定する必要があります）。
authentication	認証タイプを選択します。ピア ゲートウェイで実行される **Pre-Shared Key**（事前共有鍵）または **Certificate**（証明書）を選択します。選択に応じて「事前共有鍵フィールド」または「証明書フィールド」を参照してください。
事前共有鍵フィールド	
事前共有鍵/ 事前共有鍵の確認	**Pre-Shared Key**（事前共有鍵）を選択した場合は、トンネル間の対称認証に使用される単一のセキュリティ キーを入力します。**Pre-Shared Key**（事前共有鍵）の値は、管理者が最大 255 文字の ASCII または ASCII 以外の文字を使用して作成する文字列です。辞書攻撃で解読されにくいキーを生成します。必要に応じて、事前共有鍵生成プログラムを使用します。
ローカルID	ローカル ゲートウェイのフォーマットと ID を定義します。このフォーマットと ID は、IKEv1 フェーズ 1 SA および IKEv2 SA の両方を確立するために、事前共有鍵とともに使用されます。 以下のタイプから1つを選択し、値を入力します。**FQDN** (ホスト名)、**IP address**（**IP** アドレス）、**KEYID** (HEXのバイナリフォーマットID文字列)、または**User FQDN**（ユーザー**FQDN**）(電子メール アドレス) 値を指定しない場合、ゲートウェイはローカルIPアドレスを **Local Identification**（ローカル **ID**）として使用します。
ピアID	ピア ゲートウェイのタイプと ID を定義します。このタイプと ID は、IKEv1 フェーズ 1 SA および IKEv2 SA の確立時に、事前共有鍵とともに使用されます。 以下のタイプから1つを選択し、値を入力します。**FQDN** (ホスト名)、**IP address**（**IP** アドレス）、**KEYID** (HEXのバイナリフォーマットID文字列)、または**User FQDN**（ユーザー**FQDN**）(電子メール アドレス) 値を指定しない場合、ゲートウェイはピアの IP アドレスを **Local Identification**（ローカル **ID**）として使用します。
証明書フィールド	
ローカル証明書	**Authentication**[認証] のタイプとして **Certificate**[証明書] をドロップダウンリストから選択した場合は、ファイアウォール上にすでに存在する証明書を選択します。 以下の方法で証明書を**Import**[インポート]したり、新しい証明書を**Generate**[生成]したりすることもできます。 **Import**[インポート]:

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの一般設定	の意味

	• **Certificate Name**[証明書名] — インポートする証明書の名前を入力します。
	• **Shared**[共有] — この証明書を複数の仮想システムで共有する場合にクリックします。
	• **Certificate File**[証明書ファイル] — **Browse**[参照] をクリックし、証明書ファイルが配置されている場所に移動します。ファイルを選択して**Open**[開く]をクリックします。
	• **File Format**[ファイル フォーマット] — 以下のいずれかを選択します。
	  • **Base64 Encoded Certificate (PEM)**[Base64 エンコード済み証明書 (PEM)] — 鍵ではなく、証明書が含まれます。クリアテキストです。
	  • **Encrypted Private Key and Certificate (PKCS12)**[暗号化された秘密鍵と証明書 (PKCS12)] — 証明書と鍵の両方が含まれます。
	• **Private key resides on Hardware Security Module**[秘密鍵はハードウェア セキュリティ モジュール上にあります] — ファイアウォールが、鍵が存在する HSM サーバーのクライアントである場合にクリックします。
	• **Import private key**[秘密鍵のインポート] — 証明書ファイルとは別のファイル内にあるために秘密鍵をインポートする必要がある場合にクリックします。
	  • **Key File**[キー ファイル] — キー ファイルを参照し、インポートするキー ファイルに移動します。このエントリは、ファイル フォーマットとして PEM を選択した場合に使用可能です。
	  • **Passphrase**[パスフレーズ]および**Confirm Passphrase**[パスフレーズの確認] — 鍵にアクセスするために入力します。

ローカル証明書名（続き）	**Generate**[生成]する場合 • **Certificate Name**[証明書名] — 作成する証明書の名前を入力します。 • **Common Name**[共通名] — 共通名を入力します。これは、証明書に表記されるIPアドレスまたはFQDNです。 • **Shared**[共有] — この証明書を複数の仮想システムで共有する場合にクリックします。 • **Signed By**[署名者] — Select External Authority (CSR) [外部認証局 (CSR)] を選択するか、ファイアウォールの IP アドレスを入力します。このエントリは、CA である必要があります。 • **Certificate Authority**[認証局] — ファイアウォールがルート CA の場合にクリックします。 • **OCSP Responder**（**OCSP** レスポンダ） — 証明書が有効かどうかを追跡する OCSP を入力します。 • **Algorithm**[アルゴリズム] — 証明書の鍵を生成するために RSA または Elliptic Curve DSA を選択します。 • **Number of Bits**[ビット数] — 鍵のビット数として 512、1024、2048、または 3072 を選択します。 • **Digest**[ダイジェスト] — ハッシュからの文字列を元に戻す方法として、MD5、SHA1、SHA256、SHA384、または SHA512 を選択します。 • **Expiration (days)**[有効期限 (日)] — 証明書が有効である日数を入力します。 • **Certificate Attributes**[証明書の属性]**Type**（タイプ） — 必要に応じて、証明書に追加で含める属性タイプをドロップダウンリストから選択します。 • **Value**[値] — 属性の値を入力します。

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの一般設定	の意味
HTTP 証明書の交換	ハッシュ & URL 方式を使用して証明書の取得場所をピアに通知するには、**HTTP Certificate Exchange**（**HTTP** 証明書の交換）をクリックし、**Certificate URL**（証明書 **URL**）を入力します。Certificate URL（証明書 URL）は、証明書を保存するリモート サーバーの URL です。 ピアもハッシュ & URL をサポートしていることがわかった場合は、SHA1 ハッシュ & URL 交換を通じて証明書が交換されます。 IKE 証明書ペイロードを受信すると、ピアは HTTP URL を参照し、そのサーバーから証明書を取得します。次に、ピアは、証明書ペイロードに指定されたハッシュを使用して、HTTP サーバーからダウンロードした証明書をチェックします。
ローカルID	ローカル ピアが証明書でどのように識別されるかを指定します。以下のタイプから1つを選択し、値を入力します。**Distinguished Name**[識別名]（件名）、**FQDN**（ホスト名）、**IP address**、または**User FQDN**（電子メールアドレス）
ピアID	リモート ピアが証明書でどのように識別されるかを指定します。以下のタイプから1つを選択し、値を入力します。**Distinguished Name**[識別名]（件名）、**FQDN**（ホスト名）、**IP address**、または**User FQDN**（電子メールアドレス）
ピア ID チェック	**Exact**[完全] または **Wildcard**[ワイルドカード] を選択します。この設定は、証明書の検証のために検査されるピア ID に適用されます。たとえば、Peer Identificationがdomain.com に等しい名前で、**Exact**（完全）を選択した場合、IKE ID ペイロードの証明書に指定されたピア IDが mail.domain2.com であったとすると、IKE ネゴシエーションは失敗します。しかし、**Wildcard**（ワイルドカード）を選択した場合、名前文字列のワイルドカードアスタリスク（*）の前にある文字はすべて一致する必要がありますが、* の後の文字は異なっていてもかまいません。
ピア ID と証明書ペイロード ID の不一致を許可する	ピア ID が証明書ペイロードに一致しなくても IKE SA を正常に確立できるように柔軟性を持たせる場合に選択します。
証明書プロファイル	プロファイルを選択するか、新しい**Certificate Profile**（証明書プロファイル）を作成します。このプロファイルにより、ローカル ゲートウェイからピア ゲートウェイへと送信される証明書に適用される証明書オプションが設定されます。「Device（デバイス）> Certificate Management（証明書の管理）> Certificate Profile（証明書プロファイル）」を参照してください。
ピアの拡張鍵使用の厳密な検証を有効にする	鍵の使用方法を厳密に制御する場合に選択します。

IKE ゲートウェイの Advanced Options (詳細オプション) タブ

- Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> IKE Gateways（IKE ゲートウェイ）> Advanced Options（詳細オプション）

パッシブ モードや NAT トラバーサルなどの詳細 IKE ゲートウェイ設定、デッド ピア検出などの IKEv1 設定を構成します。

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの詳細オプション	の意味
パッシブ モードを有効にする	クリックすると、ファイアウォールは IKE 接続に応答するのみで、IKE 接続を開始しなくなります。
NAT トラバーサルを有効にする	クリックすると、IKE および UDP プロトコルで UDP カプセル化が使用され、中間 NAT デバイスを通過できるようになります。 NAT トラバーサルは、IPsec VPN 端点の間にあるデバイスでネットワーク アドレス変換 (NAT) が設定されている場合に有効にします。
IKEv1 タブ	
交換モード	**auto**[自動]、**aggressive**[アグレッシブ]、または **main**[メイン] を選択します。**auto**[自動] モード (デフォルト) の場合、デバイスは、**main**[メイン] モードと **aggressive**[アグレッシブ] モードの両方のネゴシエーション要求を受け入れることができますが、可能なときはいつでもネゴシエーションを開始し、**main**[メイン] モードで鍵交換を行えます。ピア デバイスは同一の鍵交換モードで設定し、最初のデバイスから開始されたネゴシエーション リクエストを受け入れられるようにする必要があります。
IKE 暗号化プロファイル	既存のプロファイルを選択するか、デフォルト プロファイルを維持するか、新しいプロファイルを作成します。IKEv1 と IKEv2 用に選択したプロファイルは異なる場合があります。 IKE 暗号化プロファイルの詳細は「Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IKE Crypto (IKE 暗号)」を参照してください。
フラグメンテーションを有効にする	クリックすると、ローカル ゲートウェイが IKE フラグメント パケットを受信できるようになります。最大フラグメント パケット サイズは 576 バイトです。
Dead Peer Detection	クリックして有効にし、間隔 (2 ~ 100 秒) と、再試行までの遅延時間 (2 ~ 100 秒) を入力します。デッドピア検知 (DPD) は、非アクティブまたは使用不能な IKE ピアを識別します。ピアが使用不能になった場合の失われたリソースの復元に役立ちます。
IKEv2 Tab	
IKE 暗号化プロファイル	既存のプロファイルを選択するか、デフォルト プロファイルを維持するか、新しいプロファイルを作成します。IKEv1 と IKEv2 用に選択したプロファイルは異なる場合があります。 IKE 暗号化プロファイルの詳細は「Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > IKE Crypto (IKE 暗号)」を参照してください。
Cookie の厳密な検証	クリックすると、IKE ゲートウェイで **Strict Cookie Validation**[Cookie の厳密な検証] が有効になります。 • **Strict Cookie Validation**[Cookie の厳密な検証] を有効にすると、IKEv2 Cookieが常に検証されるようになります。イニシエータは、Cookieを含む IKE_SA_INITを送信する必要があります。

© 2019 Palo Alto Networks, Inc.

IKE ゲートウェイの詳細オプション	の意味
	• **Strict Cookie Validation**[Cookieの厳密な検証] を無効にすると (デフォルト設定)、VPNセッションの設定であるグローバルな **Cookie Activation Threshold**[Cookieアクティベーションのしきい値] と照らして、ハーフオープン SA の数が確認されます。ハーフオープン SA の数が **Cookie Activation Threshold**[Cookie アクティベーションのしきい値] を超えた場合、イニシエータは、Cookie を含む IKE_SA_INIT を送信する必要があります。
ライブネス チェック	IKEv2 の **Liveness Check**[ライブネス チェック] は常にオンになっています。すべての IKEv2 パケットは、ライブネス チェックのために使用されます。このボックスをクリックすると、ピアがアイドル状態になって所定の秒数が経過したときに、空の情報パケットが送信されます。範囲:2 ~ 100デフォルト:5. 必要な場合、IKEv2 パケットを送信しようとする側は、ライブネス チェックを最大 10 回試行します (すべての IKEv2 パケットがリトランスミッション設定に影響します)。応答が得られない場合、送信側は IKE_SA と CHILD_SA を閉じて削除します。送信側は、別の IKE_SA_INIT を送信して、もう一度やり直します。

IKE ゲートウェイの再起動または更新

- Network > IPSec Tunnels [ネットワーク > IPSec トンネル]

トンネルのステータスを表示する場合は、**Network**（ネットワーク）> **IPSec Tunnels**（**IPSec** トンネル）を開きます。2番目の状態列には、IKE情報へのリンクがあります。再起動または更新するゲートウェイをクリックします。IKE Info [IKE 情報] ページが開きます。リストのエントリのいずれかをクリックし、次のいずれかをクリックします。

- **Restart**（再起動）— 選択したゲートウェイを再起動します。再起動すると、トラフィックのトンネル通過が中断されます。IKEv1 と IKEv2 の再起動の動作は、以下のように異なります。
  - **IKEv1** — フェーズ 1 SA またはフェーズ 2 SA は、別々に再起動（クリア）でき、その SA のみが影響を受けます。
  - **IKEv2** — IKEv2 SA を再起動すると、子 SA（IPSec トンネル）がすべてクリアされます。

    IKEv2 SA を再起動すると、基礎となる IPSec トンネルもすべてクリアされます。

    IKEv2 SA に関連付けられている IPSec トンネル (子 SA) を再起動しても、その IKEv2 SA には影響が及びません。
- **Refresh**（更新）— IKE SA の現在の状態を表示します。

Network > Network Profiles > IPSec Crypto [ネットワーク > ネットワーク プロファイル > IPSec 暗号]

IPSec SA ネゴシエーション (フェーズ 2) に基づいて、VPN トンネルでの認証および暗号化のプロトコルとアルゴリズムを指定する場合は、 **Network** > **Network Profiles** > **IPSec Crypto**[ネットワーク > ネットワークプロファイル > IPSec暗号化] ページを使用します。

GlobalProtect ゲートウェイとクライアント間の *VPN* トンネルについては、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> GlobalProtect IPSec Crypto（GlobalProtect の IPSec 暗号）」を参照してください。

© 2019 Palo Alto Networks, Inc.

IPSec 暗号化プロファイル設定	の意味
氏名	プロファイルを識別する**Name (名前)**を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
IPSec プロトコル	VPN トンネルを横断するデータを保護するためのプロトコルを選択します。 • **ESP** — Encapsulating Security Payload (ESP) プロトコルは、データの暗号化、ソースの認証、およびデータ整合性の検証を行います。 • **AH** — Authentication Header (AH) プロトコルは、ソースの認証とデータ整合性の検証を行います。 接続の機密性（暗号化）および認証を提供できる*ESP*プロトコルを使用します。
暗号化 (ESP プロトコルのみ)	**Add**[追加] をクリックし、目的の暗号化アルゴリズムを選択します。セキュリティを最大限に高めるため、**Move Up** [上へ]アイコンまたは **Move Down**[下へ]アイコンをクリックし、以下のように順序が降順になるよう変更します。**aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**,（VM-Series ファイアウォールはこのオプションをサポートしていません）、 **aes-128-cbc**, **3des**, および**des.null** (暗号化なし) を選択することもできます。 *AES*暗号化のフォームを使用します。（*DES* および *3DES* は脆弱なアルゴリズムです）
authentication	**Add**[追加] をクリックし、目的の認証アルゴリズムを選択します。セキュリティを最大限に高めるため、項目を選択して**Move Up**[上へ]アイコンまたは**Move Down**[下へ]アイコンをクリックし、以下のように順序が降順になるように変更します。**sha512**, **sha384**, **sha256**, **sha1**, **md5**.**IPSec Protocol**[IPSec プロトコル] が **ESP** の場合は、**none**[なし] (認証なし) を選択することもできます。 *md5*および*sha1*は安全ではないため、*sha256*あるいはそれより強固な認証を使用します。短期間のセッションでは*sha256*を、金融取引のように極めてセキュアな認証が必要なトラフィックでは*sha384*以上を使用します。
DH グループ	IKE（Internet Key Exchange）用のDH（Diffie-Hellman）グループを選択します。**group1**、**group2**、**group5**、**group14**、**group19**、または**group20**。セキュリティを最も強化するには、数値が最も大きいグループを選択します。IKE フェーズ 1 でファイアウォールが作成する鍵を更新しない場合は、**[no-pfs]** (no perfect forward secrecy) を選択します。ファイアウォールは、IPSec セキュリティ アソシエーション (SA) ネゴシエーションで現在の鍵を再利用します。
有効期間	単位を選択し、ネゴシエートされた鍵の有効期間を入力します (デフォルト設定は 1 時間)。

© 2019 Palo Alto Networks, Inc.

IPSec 暗号化プロファイル設定	の意味
ライフサイズ	任意の単位を選択し、鍵が暗号化に使用できるデータ サイズを入力します。

Network > Network Profiles > IKE Crypto [ネットワーク > ネットワーク プロファイル > IKE 暗号]

IKE Crypto Profiles（**IKE** 暗号化プロファイル）ページを使用して、識別、認証、および暗号化のプロトコルとアルゴリズムを指定します（IKEv1 または IKEv2、フェーズ 1）。

アルゴリズムまたはグループのリスト順序を変更する場合は、項目を選択して、**Move Up**[上へ]または**Move Down**[下へ]をクリックします。この順序によって、リモート ピアと設定をネゴシエートするときに最初に選択される設定が決まります。リストの 1 番上にある設定から試行され、成功するまでその下にある設定が順次試行されていきます。

IKE 暗号化プロファイル設定	の意味
氏名	プロファイルの名前を入力します。
DH グループ	DH (Diffie-Hellman) グループの優先度を選択します。**Add**[追加] をクリックしてグループを選択します。**group1**、 **group2** 、 **group5**、 **group14**、**group19**、または **group20**。セキュリティを最大限に高めるため、項目を選択し、**Move Up**[上へ] または **Move Down**[下へ] をクリックして、識別子の数値がより大きいグループがリストの上位に表示されるように移動します。たとえば、**group14** を **group2** よりも上に移動します。
authentication	ハッシュ アルゴリズムの優先度を指定します。**Add**[追加] をクリックしてアルゴリズムを選択します。セキュリティを最大限に高めるため、項目を選択して**Move Up**[上へ]アイコンまたは**Move Down**[下へ]アイコンをクリックし、以下のように順序が降順になるように変更します。**sha512**, **sha384**, **sha256**, **sha1**, **md5**.
暗号化	適切なEncapsulating Security Payload（ESP）認証グループを選択します。**Add**[追加] をクリックしてアルゴリズムを選択します。セキュリティを最大限に高めるため、項目を選択して**Move Up**[上へ]アイコンまたは**Move Down**[下へ]アイコンをクリックし、以下のように順序が降順になるように変更します。**sha512**, **sha384**, **sha256**, **sha1**, **md5**.
キーの有効期間	時間の単位を選択し、ネゴシエートされたIKEフェーズ 1 キーの有効期間（デフォルトは8時間）を選択します。 • IKEv2 — キーの有効期間が切れる前に、SAのキーを再生成する必要があります。そうしないと、有効期限が切れたときに、SAは新しいフェーズ 1 キーネゴシエーションを開始する必要があります。 • IKEv1 — 有効期限が切れないうちに前もってフェーズ 1 キーを再生成することはありません。IKEv1 IPSec SA の有効期限が切れてはじめて、IKEv1 フェーズ 1 キー再生成が起動されます。
IKEv2 多重認証	認証カウントを決定するために、キーの有効期間で乗算される値を指定します (0 ~ 50 の範囲、デフォルト設定は 0)。認証カウントは、ゲートウェイが

© 2019 Palo Alto Networks, Inc.

IKE 暗号化プロファイル設定	の意味
	IKEv2 IKE SA キー再生成を実行できる回数であり、この回数だけ実行した後は、IKEv2 再認証をやり直す必要があります。値として 0 を指定すると、再認証機能が無効になります。

Network > Network Profiles > Monitor [ネットワーク > ネットワーク プロファイル > 監視]

IPSec トンネルをモニターしたり、ポリシーベースの転送 (PBF) ルールのネクストホップ デバイスをモニターしたりするには、モニター プロファイルを使用します。どちらの場合も、モニター プロファイルは、リソース (IPSec トンネルまたはネクストホップ デバイス) が使用できなくなった場合に実行するアクションを指定するために使用されます。モニター プロファイルは任意ですが、サイト間の接続を持続し、PBF ルールを確実に維持するのに非常に効果的です。モニター プロファイルの設定には以下の設定が使用されます。

項目	の意味
氏名	モニター プロファイルの識別に使用する名前を入力します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
操作	トンネルを使用できないときに実行するアクションを指定します。ハートビート喪失の許容発生回数がしきい値に達すると、指定したアクションがファイアウォールによって実行されます。 • **wait-recover** – トンネルが回復するまで待機します。他のアクションは実行しません。パケットは、PBF ルールに従って引き続き送信されます。 • **fail-over** – トラフィックをバックアップ パスにフェイルオーバーします (使用可能な場合)。ファイアウォールはルーティング テーブル検索を使用してこのセッション中のルーティングを判別します。 どちらの場合も、早く回復できるようにファイアウォールによって新しい IPsec 鍵がネゴシエートされます。
間隔	ハートビート間隔 (範囲は2 ~ 10、デフォルトは3) を指定します。
しきい値	ハートビートの喪失回数のしきい値を指定します (範囲は 2 ~ 10、デフォルトは 5) 。この回数を超えると指定したアクションがファイアウォールによって実行されます。

Network > Network Profiles > Interface Mgmt [ネットワーク > ネットワーク プロファイル > インターフェイス管理]

インターフェイス管理プロファイルは、ファイアウォールインターフェイスがアクセスを許容するサービスやIPアドレスを定義することで、ファイアウォールを不正なアクセスから保護します。インターフェイス管理プロファイルは、サブインターフェイスを含めたレイヤー3イーサネットインターフェイス、および理論インターフェイス (集約グループ、VLAN、ループバック、およびトンネルインターフェイス) に

© 2019 Palo Alto Networks, Inc.

割り当てることができます。インターフェイス管理プロファイルを割り当てるには、「Network（ネットワーク）> Interfaces（インターフェイス）」を参照してください。

Telnet、*SSH*、*HTTP*、または *HTTPS* を、インターネットやエンタープライズ セキュリティ境界内の他の信頼されていないゾーンからのアクセスを許可するインターフェイスに接続するインターフェイス管理プロファイルを設定しないでください。これには、*GlobalProtect* ポータルまたはゲートウェイを設定したインターフェイスが含まれます。 *GlobalProtect* は、ポータルまたはゲートウェイへのアクセスを可能にするためのインターフェイス管理プロファイルを必要としません。ファイアウォールと *Panorama* へのアクセスを保護する方法の詳細については、Best Practices for Securing Administrative Access（管理アクセスを保護するためのベストプラクティス）を参照してください。

Telnet、*SSH*、*HTTP*、または *HTTPS* を許可するインターフェイス管理プロファイルを、*GlobalProtect* ポータルまたはゲートウェイを設定したインターフェイスに接続しないでください。これにより、管理インターフェイスがインターネットに公開されるためです。

項目	の意味
氏名	プロファイル名 (最大 **31** 文字) を入力します。この名前は、インターフェイスを設定するときにインターフェイス管理プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
管理サービスの管理	• **Telnet** - ファイアウォールCLIにアクセスする際に使用します。Telnetはプレーンテキストを使用しますが、SSHよりは機密性が劣ります。 インターフェイス上の管理トラフィックには、*Telnet* の代わりに *SSH* を有効化してください。 • **SSH** - ファイアウォールCLIに安全にアクセスする場合に使用します。 • **HTTP** - ファイアウォールウェブインターフェイスにアクセスする際に使用します。HTTPはプレーンテキストを使用しますが、HTTPSよりは機密性が劣ります。 インターフェイス上の管理トラフィックには、*HTTP* の代わりに *HTTPS* を有効化してください。 • **HTTPS** - ファイアウォールウェブインターフェイスに安全にアクセスする場合に使用します。
Network Services（ネットワークサービス）	• **Ping** - 外部サービスとの接続をテストする場合に使用します。例えば、インターフェイスに対してpingを行い、Palo Alto NetworksアップデートサーバーからパロアルトネットワークスPAN-OSソフトウェアやコンテンツのアップデートが受信可能な状態かどうか確認することができます。 • **HTTP OCSP** - ファイアウォールをオンライン証明書状態プロトコル（OCSP）のレスポンダとして設定する場合に使用します。詳細は、「Device（デバイス）> Certificate Management（証明書の管理）> OCSP Responder（OCSP レスポンダ）」を参照してください。 • **SNMP** - SNMPマネージャーからのファイアウォール状態クエリを処理する場合に使用します。詳細は、「SNMP モニタリングの有効化」を参照してください。 • **Response Pages**[応答ページ] - 以下の応答ページを有効化する場合に使用します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **Captive Portal**（キャプティブポータル）- キャプティブ ポータルの応答ページを提供するために使用されるポートは、NTLM の場合はポート 6080、SSL/TLS サーバー プロファイルのないキャプティブ ポータルの場合は 6081、SSL/TLS サーバー プロファイルのキャプティブ ポータルの場合は 6082 です。詳細は、「Device（デバイス）> User Identification（ユーザー ID）> Captive Portal Settings（キャプティブ ポータルの設定）」を参照してください。 • **URL Admin Override**（URL 管理オーバーライド）- 詳細は、「Device（デバイス）> Setup（セットアップ）> Content-ID」を参照してください。 • **User-ID**（ユーザー ID）- ファイアウォール間のユーザー マッピングのRedistribution（再配信）を有効化する場合に使用します。 • **User-ID Syslog Listener-SSL**[User-ID Syslogリスナー-SSL] - PAN-OS統合User-IDエージェントによるSSL経由のsyslogメッセージの回収を許可する場合に使用します。詳細は、「監視対象サーバーに対するアクセスの設定」を参照してください。 • **User-ID Syslog Listener-UDP**[User-ID Syslogリスナー-SSL] - PAN-OS統合User-IDエージェントによるUDP経由のsyslogメッセージの回収を許可する場合に使用します。詳細は、「監視対象サーバーに対するアクセスの設定」を参照してください。
アクセス許可IPアドレス	インターフェイスで許可されるアクセス元の IPv4 または IPv6 アドレスのリストを入力します。

Network > Network Profiles > Zone Protection [ネットワーク > ネットワークプロファイル > ゾーンプロテクション]

ゾーンに適用するゾーン プロテクション プロファイルによって、最も一般的なフラッド、偵察行為、その他のパケットベース攻撃、および IP 以外のプロトコルの使用から保護されます。このプロファイルは、入力ゾーン（トラフィックがファイアウォールに進入するゾーン）における幅広い保護を目的とするもので、特定のエンドホストや特定の宛先ゾーンに進入するトラフィックを阻止するものではありません。ゾーンには 1 つのゾーン プロテクション プロファイルを関連付けることができます。

ゾーン プロテクション プロファイルを各ゾーンに適用し、*IP* フラッド、偵察行為、パケット ベースの攻撃、非 *IP* プロトコルの攻撃を防ぐ保護層を追加します。ファイアウォール上のゾーン プロテクションは、インターネットの境界に位置する専用の *DDoS* デバイスの後に来る *2* つ目の保護層でなければなりません。

ファイアウォールのゾーン プロテクション機能を強化するには、特定のゾーン、インターフェイス、IP アドレス、またはユーザーを対象とした DoS プロテクション ポリシー（Policies（ポリシー）> DoS Protection（DoS プロテクション））を設定します。

ゾーン プロテクションは *1* 秒あたりのパケット数（*pps*）ではなく、*1* 秒あたりの新しい接続数（*cps*）に基づくため、パケットに対するセッション一致がない場合にのみ適用されます。パケットが既存のセッションに一致する場合は、ゾーン プロテクション設定をバイパスします。

© 2019 Palo Alto Networks, Inc.

確認すべき情報	以下を参照
ゾーン プロテクション プロファイルを作成する方法は?	ゾーン プロテクション プロファイルの構成要素 フラッド防御 偵察行為防御 パケット ベースの攻撃保護 プロトコル保護

ゾーン プロテクション プロファイルの構成要素

ゾーン プロテクション プロファイルを作成するには、プロファイルを **Add**（追加）して、名前を付けます。

ゾーン プロテクション プロファイル設定	設定場所	の意味
氏名	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）	プロファイル名（最大 31 文字）を入力します。この名前は、ゾーンを設定するときに Zone Protection（ゾーン プロテクション）プロファイルのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、およびアンダースコアのみを使用してください。
の意味		Zone Protection（ゾーン プロテクション）プロファイルの任意の説明を入力します。

以下のような、ゾーンで必要となる保護のタイプに合わせて設定を組み合わせ、引き続きゾーン プロテクション プロファイルを作成します。

- フラッド防御
- 偵察行為防御
- パケット ベースの攻撃保護
- プロトコル保護

複数の仮想システムがある環境で、以下を有効にしている場合は、

- 仮想システム間の通信が可能な外部ゾーン
- 仮想システムが外部通信に共通インターフェイスおよび *1* つの *IP* アドレスを共有できる共有ゲートウェイ

以下のゾーンおよび *DoS* プロテクション メカニズムが、外部ゾーンで無効になります。

- *SYN cookies*
- *IP* フラグメント
- *ICMPv6*

共有ゲートウェイ用に *IP* フラグメントと *ICMPv6* 防御を有効にするには、共有ゲートウェイ用のゾーン プロテクション プロファイルを個別に作成する必要があります。

© 2019 Palo Alto Networks, Inc.

共有ゲートウェイで *SYN* フラッドから保護するには、ランダム早期ドロップまたは *SYN Cookie* のいずれかを設定した *SYN* フラッド防御プロファイルを適用できます。外部ゾーンでは、*SYN* フラッド防御にランダム早期ドロップのみを使用できます。

フラッド防御

- [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > フラッド防御]

SYN、ICMP、ICMPv6、SCTP INIT、UDP パケットのフラッド防御に加えて、その他のタイプの IP パケットのフラッディングに対する保護を提供するプロファイルを設定します。レートは 1 秒あたりの接続数です。 たとえば、既存のセッションに一致しない受信 SYN パケットは新しい接続と見なされます。

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
SYN	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Flood Protection**（フラッド防御）	SYN フラッドに対する防御を有効にする場合に選択します。

操作		SYN フラッド攻撃に対して実行するアクションを選択します。
		• **Random Early Drop** (ランダム早期ドロップ) – フラッド攻撃を軽減するために SYN パケットを廃棄します。
		  • フローが **Alert**[アラート] 率のしきい値を上回ると、アラームが生成されます。
		  • フローが **Activate**（アクティベート）率のしきい値を上回ると、ファイアウォールはフローを制限するために個々の SYN パケットをランダムに廃棄します。
		  • フローが **Maximum**（最大）率のしきい値を上回ると、すべての受信 SYN パケットを廃棄します。
		• **SYN Cookies**（**SYN Cookie**）– ファイアウォールがプロキシのように動作し、SYN をインターセプト、SYN の宛先であったサーバーの代わりに Cookie を生成して、元の送信元に Cookie 付き SYN-ACK を送信します。送信元が Cookie 付き ACK をファイアウォールに返したときにのみ、ファイアウォールは送信元を有効とみなして、SYN をサーバーに転送します。このアクションをお勧めします。
		SYN Cookie は正当なトラフィックを公正に扱いますが、*RED* よりも多くのファイアウォール リソースを消費します。*SYN Cookie* がリソースを多く消費しすぎている場合は *RED* に切り替えてください。大量の *DoS* 攻撃を防止する専用の *DDoS* 防止デバイスがファイアウォールの前に存在しない場合は、必ず *RED* を使用します。

アラーム レート（接続数/秒）	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Flood**	アラームのトリガーとなる、1 秒あたりにゾーンが受信する SYN パケット数（既存のセッションに一致しない）を入力します。ダッシュボードおよび脅威ログ（Monitor（監視）> Packet Capture（パケット キャプチャ））でアラームを確認できます。範囲は 0 ~ 2000000、デフォルトは 10,000。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
	Protection（フラッド防御）(cont)（続き）	しきい値を平均ゾーン CPS レートよりも 15～20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。
アクティベーション (接続/秒)		ゾーン プロテクション プロファイルで指定したアクションのトリガーとなる、1 秒あたりにゾーンが受信する SYN パケット数（既存のセッションに一致しない）を入力します。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum（最大）率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate（アクティベート）のしきい値を下回ると、SYN パケットの廃棄を停止します。範囲は 1 ～ 2,000,000、デフォルトは 10,000 です。 しきい値をゾーンのピーク時 CPS レートよりもわずかに高く設定して正当なトラフィックのスロットリングを防止し、必要に応じて調整を行うことがベストプラクティスになります。
最大 (接続/秒)		1 秒あたりにゾーンが受信する SYN パケットの最大数（既存のセッションに一致しない）を入力します。最大値を超過した分のパケットは廃棄されます。範囲は 1 ～ 2,000,000、デフォルトは 40,000 です。このしきい値を超えると、CPS レートがしきい値を下回るまで新しい接続がブロックされます。 ファイアウォール リソースを消費する他の機能を加味しつつ、しきい値をファイアウォールの能力の 80～90% に設定することがベストプラクティスになります。
ICMP	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Flood Protection**（フラッド防御）(cont)（続き）	ICMP フラッドに対する防御を有効にする場合に選択します。
アラーム レート（接続数/秒）		攻撃アラームのトリガーとなる、1 秒あたりにゾーンが受信する ICMP エコー要求の数（既存のセッションに一致しない ping）を入力します。範囲は 0 ～ 2000000、デフォルトは 10,000。 しきい値を平均ゾーン CPS レートよりも 15～20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。
アクティベーション (接続/秒)		1 秒あたりにゾーンが受信する ICMP パケット数（既存のセッションに一致しない）を入力します。入力値を超過した分の ICMP パケットは廃棄されます。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum（最大）率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate（アクティベート）のしきい値を下回ると、ICMP パケットの廃棄を停止します。範囲は 1 ～ 2,000,000、デフォルトは 10,000 です。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
		しきい値をゾーンのピーク時 CPS レートよりもわずかに高く設定して正当なトラフィックのスロットリングを防止し、必要に応じて調整を行うことがベストプラクティスになります。
最大 (接続/秒)		1 秒あたりにゾーンが受信する ICMP パケットの最大数 (既存のセッションに一致しない) を入力します。最大値を超過した分のパケットは廃棄されます。範囲は 1 ~ 2,000,000、デフォルトは 40,000 です。 ファイアウォール リソースを消費する他の機能を加味しつつ、しきい値をファイアウォールの能力の 80 ~ 90% に設定することがベストプラクティスになります。
SCTP 初期化	**Network** (ネットワーク) > **Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション) > **Flood Protection** (フラッド防御) (cont) (続き)	開始 (INIT) チャンクを含むストリーム制御伝送プロトコル (SCTP) パケットのフラッドに対する保護を有効にする場合に選択します。INIT チャンクは他のチャンクとバンドルできないので、パケットは SCTP INIT パケットと呼ばれます。
アラーム レート (接続数/秒)		攻撃アラームのトリガーとなる、1 秒あたりにゾーンが受信する SCTP INIT パケット数 (既存のセッションに一致しない) を入力します。範囲は 0 ~ 2,000,000 です。デフォルトのファイアウォール モードごとのパケット数は以下の通りです。 • **PA-5280**—10,000 • **PA-5260**—7,000 • **PA-5250**—5,000 • **PA-5220**—3,000 • **VM-700**—1,000 • **VM-500**—500 • **VM-300**—250 • **VM-100**—200 • **VM-50**—100
アクティベーション (接続/秒)		1 秒あたりにゾーンが受信する SCTP INIT パケット数 (既存のセッションに一致しない) を入力します。入力値を超過した分の SCTP INIT パケットは廃棄されます。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum (最大) 率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate (アクティベート) のしきい値を下回ると、SCTP INIT パケットの廃棄を停止します。範囲は1 ~ 2,000,000 です。ファイアウォール モデルごとのデフォルトは、アラーム レートと同じです。
最大 (接続/秒)	**Network** (ネットワーク) > **Network Profiles** (ネットワーク	1 秒あたりにゾーンが受信する SCTP INIT パケットの最大数 (既存のセッションに一致しない) を入力します。最大値を超過した分のパケットは廃棄されます。範囲は1 ~ 2,000,000

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
	プロファイル) > **Zone Protection** (ゾーン プロテクション) > **Flood Protection** (フラッド防御) (cont) (続き)	です。デフォルトのファイアウォール モードごとのパケット数は以下の通りです。 • **PA-5280**—20,000 • **PA-5260**—14,000 • **PA-5250**—10,000 • **PA-5220**—6,000 • **VM-700**—2,000 • **VM-500**—1,000 • **VM-300**—500 • **VM-100**—400 • **VM-50**—200
UDP	**Network** (ネットワーク) > **Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション) > **Flood Protection** (フラッド防御) (cont) (続き)	UDP フラッドに対する防御を有効にする場合に選択します。
アラーム レート (接続数/秒)		攻撃アラームのトリガーとなる、1 秒あたりにゾーンが受信する UDP パケット数 (既存のセッションに一致しない) を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。 しきい値を平均ゾーン CPS レートよりも 15 ~ 20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。
アクティベーション (接続/秒)		UDP パケットのランダム廃棄のトリガーとなる、1 秒あたりにゾーンが受信する UDP パケット数 (既存のセッションに一致しない) を入力します。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum (最大) 率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate (アクティベート) のしきい値を下回ると、UDP パケットの廃棄を停止します。範囲は 1 ~ 2,000,000、デフォルトは 10,000 です。 しきい値をゾーンのピーク時 CPS レートよりもわずかに高く設定して正当なトラフィックのスロットリングを防止し、必要に応じて調整を行うことがベストプラクティスになります。
最大 (接続/秒)		1 秒あたりにゾーンが受信する UDP パケットの最大数 (既存のセッションに一致しない) を入力します。最大値を超過した分のパケットは廃棄されます。範囲は 1 ~ 2,000,000、デフォルトは 40,000 です。 ファイアウォール リソースを消費する他の機能を加味しつつ、しきい値をファイアウォールの能力の 80 ~ 90% に設定することがベストプラクティスになります。
ICMPv6	**Network** (ネットワーク) > **Network Profiles** (ネットワーク	ICMPv6 フラッドに対する防御を有効にする場合に選択します。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
アラーム レート (接続数/秒)	プロファイル) > **Zone Protection** (ゾーン プロテクション) > **Flood Protection** (フラッド防御) (cont) (続き)	攻撃アラームのトリガーとなる、1 秒あたりにゾーンが受信する ICMPv6 エコー要求の数 (既存のセッションに一致しない ping) を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。 しきい値を平均ゾーン CPS レートよりも 15 ~ 20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。
アクティベーション (接続/秒)		1 秒あたりにゾーンが受信する ICMPv6 パケット数 (既存のセッションに一致しない) を入力します。入力値を超過した分の ICMPv6 パケットは廃棄されます。ファイアウォールはアルゴリズムを使用して、攻撃の割合が Maximum (最大) 率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate (アクティベート) のしきい値を下回ると、ICMPv6 パケットの廃棄を停止します。範囲は 1 ~ 2,000,000、デフォルトは 10,000 です。 しきい値をゾーンのピーク時 CPS レートよりもわずかに高く設定して正当なトラフィックのスロットリングを防止し、必要に応じて調整を行うことがベストプラクティスになります。
最大 (接続/秒)		1 秒あたりにゾーンが受信する ICMPv6 パケットの最大数 (既存のセッションに一致しない) を入力します。最大値を超過した分のパケットは廃棄されます。範囲は 1 ~ 2,000,000、デフォルトは 40,000 です。 ファイアウォール リソースを消費する他の機能を加味しつつ、しきい値をファイアウォールの能力の 80 ~ 90% に設定することがベストプラクティスになります。
その他の **IP**	**Network** (ネットワーク) > **Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション) > **Flood Protection** (フラッド防御) (cont) (続き)	その他の IP (TCP 以外、ICMP 以外、ICMPv6 以外、SCTP 以外、UDP 以外) フラッドに対する防御を有効にする場合に選択します。
アラーム レート (接続数/秒)		攻撃アラームのトリガーとなる、1 秒あたりにゾーンが受信するその他の IP パケット (TCP 以外、ICMP 以外、ICMPv6 以外、SCTP 以外、UDP 以外のパケット) の数 (既存のセッションに一致しない) を入力します。範囲は 0 ~ 2000000、デフォルトは 10,000。 しきい値を平均ゾーン CPS レートよりも 15 ~ 20% 高く設定して通常の変動に対応させ、アラームが多すぎる場合にしきい値を調整するというのがベストプラクティスになります。
アクティベーション (接続/秒)		その他の IP パケットのランダム廃棄のトリガーとなる、1 秒あたりにゾーンが受信するその他の IP パケット (TCP 以外、ICMP 以外、ICMPv6 以外、UDP 以外のパケット) の数 (既存のセッションに一致しない) を入力します。ファ

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – フラッド防御	設定場所	の意味
		イアウォールはアルゴリズムを使用して、攻撃の割合が Maximum（最大）率に到達するまで、攻撃の増加に合わせて廃棄するパケットの数を徐々に増やします。ファイアウォールは、受信する割合が Activate（アクティベート）のしきい値を下回ると、その他の IP パケットの廃棄を停止します。範囲は 1 ~ 2,000,000、デフォルトは 10,000 です。 しきい値をゾーンのピーク時 CPS レートよりもわずかに高く設定して正当なトラフィックのスロットリングを防止し、必要に応じて調整を行うことがベストプラクティスになります。
最大 (接続/秒)		1 秒あたりにゾーンが受信するその他の IP パケット（TCP 以外、ICMP 以外、ICMPv6 以外、UDP 以外のパケット）の最大数（既存のセッションに一致しない）を入力します。最大値を超過した分のパケットは廃棄されます。範囲は 1 ~ 2,000,000、デフォルトは 40,000 です。 ファイアウォール リソースを消費する他の機能を加味しつつ、しきい値をファイアウォールの能力の 80 ~ 90% に設定することがベストプラクティスになります。

偵察行為防御

- Network > Network Profiles > Zone Protection > Reconnaissance Protection [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > 偵察行為防御]

以下の設定で偵察行為防御を定義します。

ゾーン プロテクション プロファイル設定 – 偵察行為防御	設定場所	の意味
TCP ポート スキャン	**Network** [ネットワーク] > **Network Profiles** ネットワーク プロファイル > **Zone Protection**ゾーン プロテクション > **Reconnaissance Protection**（偵察行為防御）	**Enable**[有効化]ではTCPポートスキャンに対する保護を有効化するプロファイルを設定します。
UDP ポート スキャン		**Enable**[有効化]ではUDPポートスキャンに対する保護を有効化するプロファイルを設定します。
ホスト スイープ		**Enable**[有効化]ではホストスイープに対する保護を有効化するプロファイルを設定します。
操作		以下の偵察行為に対してシステムが実行するアクションを指定します。 • **Allow**[許可] – ホストスイープ偵察行為またはポートスキャンを許可します。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – 偵察行為防御	設定場所	の意味
		• **Alert**[アラート] – 指定した時間間隔内でポートスキャンまたはホストスイープがしきい値に達するたびにアラートを生成します（デフォルトのアクションに設定されています）。 • **Block**[ブロック] – 指定した時間間隔が終わるまで、送信元から宛先へ向けた後続のパケットをすべて廃棄します。 • **Block IP**[ブロックIP] - 指定した**Duration**[持続時間]にわたり、後続のパケットをすべて廃棄します（範囲は1～3600、単位は秒数）。**Track By**（追跡区分）により、送信元をブロックするか、あるいは送信元-宛先間トラフィックをブロックするかを選択できます。すなわち、指定した時間間隔あたり単一の送信元から行われた制限回数以上の試みをブロックするか（制限の厳しい設定です）、または、特定の送信元と宛先のペアをもつ試みをブロックします（制限が比較的緩やかな設定です）。 内部で行う脆弱性テスト スキャンを除き、偵察行為スキャンをすべてブロックします。
間隔 (秒)		TCP または UDP ポート スキャンの探知を行う時間間隔（秒）です（範囲は 2 ~ 65,535、デフォルトは 2）。 ホスト スイープの探知を行う時間間隔（秒）です（範囲は 2 ~ 65,535、デフォルトは 10）。
しきい値 (イベント)		アクションをトリガーさせる、指定した時間間隔の間に行われるポートスキャンまたはホストスイープの回数です（範囲は2～65535、デフォルトは100）。 偵察行為の試みをブロックする前に、デフォルトのイベントしきい値を使用していくつかのパケットをログに記録して分析を行います。
送信元アドレスの除外		偵察行為防御のホワイトリスト対象の IP アドレスです。リストは、最大 20 件の IP アドレスまたはネットマスク アドレス オブジェクトをサポートします。 • 名前:除外するアドレスの分かりやすい名前を入力します。 • アドレスタイプ ：ドロップダウン リストから IPv4 または IPv6 を選択します。 • アドレス:ドロップダウン リストからアドレスまたはアドレス オブジェクトを選択するか、手動で入力します。 「ホワイトハット」脆弱性テストを実行する、信頼できる内部グループの *IP* アドレスだけを除外します。

© 2019 Palo Alto Networks, Inc.

パケット ベースの攻撃保護

- Network > Network Profiles > Zone Protection > Packet Based Attack Protection [ネットワーク > ネットワーク プロファイル > ゾーン プロテクション > パケット ベースの攻撃保護]

Packet Based Attack protection（パケット ベースの攻撃保護）を設定して、以下のパケット タイプをドロップできます。

- IP ドロップ
- TCP ドロップ
- ICMP ドロップ
- IPv6 Drop[IPv6ドロップ]:
- ICMPv6 ドロップ

IP ドロップ

ゾーンで受信した特定の IP パケットにどう対応するのかをファイアウォールに指示する場合は、以下の設定を行います。

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
スプーフされた IP アドレス	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Packet Based Attack Protection**（パケット ベースの攻撃保護）> **TCP Drop**（**TCP** ドロップ）	入口パケットの送信元 IPアドレスがルーティング可能であり、ルーティング インターフェイスが入口インターフェイスと同じゾーンにあることを確認してください。いずれかの条件が真でない場合は、パケットを破棄します。 なりすまし *IP* アドレスのパケットを内部ゾーンでのみドロップし、必ず入力か所で送信元アドレスがファイアウォールのルーティングテーブルとマッチすることを確認するようにしてください。
厳密な IP アドレス チェック		両方の条件が真であることを確認します。 • 送信元 IPアドレスは、入口インターフェイスのサブネット ブロードキャスト IPアドレスではありません。 • 送信元 IPアドレスは、正確な入口インターフェイスを介してルーティングが可能です。 いずれかの条件が真でない場合は、パケットを破棄します。 共通基準（CC）モードに設定されたファイアウォールについては、破棄されたパケットのログを記録することができます。ファイアウォールの Web インターフェイスで **Device (デバイス)** > **Log Settings (ログ設定)**を選択します。ログの管理のセクションで、**Selective Audit**[選択的監査] を選択し、**Packet Drop Logging**[パケット破棄のログ] を有効化します。
フラグメントされたトラフィック		フラグメント化されたIPパケットの廃棄

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
IP オプションのドロップ		このグループでこの設定を選択することで、ファイアウォールが、これらの IP オプションを含むパケットをドロップできるようにします。
ストリクト ソース ルーティング		Strict Source Routing [ストリクト ソース ルーティング] IP オプションが設定されたパケットを廃棄します。ストリクト ソース ルーティングは、データグラムのソースがルーティング情報を提供し、そのルーティング情報によってゲートウェイまたはホストがデータグラムを送信するオプションです。 ソース ルーティングによって宛先 *IP* アドレスを一致条件として使用するセキュリティポリシールールを攻撃者がバイパスできるようになるため、ストリクト ソース ルーティングを使用するパケットをドロップします。
ルーズ ソース ルーティング		Loose Source Routing [ルーズ ソース ルーティング] IP オプションが設定されたパケットを廃棄します。ルーズ ソース ルーティングは、データグラムのソースがルーティング情報を提供し、ゲートウェイまたはホストが多くの中間ゲートウェイの任意のルートを選択して、ルートの次のアドレスにデータグラムを送信できるオプションです。 ソース ルーティングによって宛先 *IP* アドレスを一致条件として使用するセキュリティポリシールールを攻撃者がバイパスできるようになるため、ルーズ ソース ルーティングを使用するパケットをドロップします。
タイムスタンプ		Timestamp [タイムスタンプ] IP オプションが設定されたパケットを廃棄します。
レコード ルート		Record Route [レコード ルート] IP オプションが設定されたパケットを廃棄します。データグラムにこのオプションが含まれるとき、データグラムをルーティングする各ルーターは独自の IP アドレスをヘッダーに追加し、受信者へのパスを提供します。
セキュリティ		セキュリティ オプションが定義されている場合、パケットを廃棄します。
ストリーム ID		ストリーム ID が定義されている場合、パケットを廃棄します。
未知		クラスと番号が不明な場合、パケットを廃棄します。 未知のパケットを破棄します。
異常な形式		RFC 791、1108、1393、2113 に基づいてクラス、番号、長さの組み合わせに誤りがある場合、パケットを廃棄します。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
		不正な形式のパケットを破棄します。

TCP ドロップ

ゾーンで受信する特定の TCP パケットに対する対応方法をファイアウォールに指示する場合は、以下の設定を行います。

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
重複する TCP セグメントの不一致	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Packet Based Attack Protection**（パケット ベースの攻撃保護）> **TCP Drop**（**TCP** ドロップ）	攻撃者は、重複するけれども異なるデータを利用し接続を構築して、接続の不正な解釈を引き起こすことがあります。攻撃者は、IP スプーフィングとシーケンス番号予測を利用してユーザーの接続をインターセプトし、攻撃者のデータを挿入することがあります。重複の不一致をレポートし、セグメント データが以下のシナリオに一致しない場合にパケットを廃棄するためには、この設定を使用します。 • セグメントが別のセグメント内にある。 • セグメントが別のセグメントの一部と重複する。 • セグメントが別のセグメントを完全に含んでいる。 この保護メカニズムは、シーケンス番号を使用して、TCP データ ストリーム内のどこにパケットが存在するかを判別します。 重複する *TCP* セグメントが一致しないパケットをドロップします。
スプリット ハンドシェイク		一般的な 3 ウェイ ハンドシェークがセッション確立手順で使用されない場合、TCP セッションの確立を防ぎます。許可されないバリエーションの例として、4 ウェイまたは 5 ウェイのスプリット ハンドシェークや同時オープン セッションの確立手順があります。 Palo Alto Networks の次世代ファイアウォールは、**Split Handshake**（スプリット ハンドシェーク）を設定しない場合、スプリット ハンドシェークや同時オープン セッションの確立のためのセッションおよびすべてのレイヤー 7 プロセスを適切に処理します。これをゾーン プロテクション プロファイルに対して設定し、プロファイルをゾーンに適用する場合は、標準的な 3 ウェイ ハンドシェークを使用して、そのゾーンのインターフェイスの TCP セッションを確立する必要があります。バリエーションは許可されません。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
		スプリット ハンドシェイクを伴うパケットをドロップします。
データとの TCP SYN		3 ウェイ ハンドシェーク時の TCP SYN パケットにデータが含まれる場合、TCP セッションの確立を防ぎます。デフォルトで有効になっています。
データとの TCP SYNACK		3 ウェイ ハンドシェーク時の TCP SYN-ACK パケットにデータが含まれる場合、TCP セッションの確立を防ぎます。デフォルトで有効になっています。
非 SYN TCP の拒否		TCPセッションセットアップの最初のパケットがSYNパケットではない場合にパケットを拒否するかどうかを決定します。 • **Global**[グローバル] – CLI で割り当てたシステム全体の設定を使用します。 • はい – 非 SYN TCP を拒否します。 • いいえ – 非 SYN TCP を受け入れます。 非 *SYN TCP* トラフィックを受け入れると、ブロックの発生後にクライアント接続やサーバー接続が設定されていない場合にファイル ブロッキング ポリシーが正常に動作しない可能性があります。 ゾーンでトンネル コンテンツ検査を設定して*Rematch Sessions* (セッションの再マッチング)を有効化する場合、そのゾーンでのみ*Reject Non-SYN TCP (SYN TCP* 以外を拒否)し、トンネル コンテンツ検査ポリシーを有効化あるいは編集することでファイアウォールが既存のトンネル セッションをドロップしないようにします。
非対称パス		同期していないACKまたはウィンドウ外のシーケンス番号を含むパケットを破棄するかバイパスするかを決定します。 • **Global**[グローバル] – CLI で割り当てたシステム全体の設定を使用します。 • **drop**[ドロップ] – 非対称パスを含むパケットをドロップします。 • **bypass**[バイパス] – 非対称パスを含むパケットでスキャンをバイパスします。
TCP オプションの除去		TCP パケットから TCP タイムスタンプまたは TCP Fast Open オプションを除去するかどうかを決定します。
TCP タイムスタンプ	**Network** (ネットワーク) > **Network**	パケットのヘッダーにTCPタイムスタンプがあるかどうかを判断し、ある場合はヘッダーから除去します。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
	Profiles（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Packet Based Attack Protection**（パケット ベースの攻撃保護）> **TCP Drop**（**TCP** ドロップ）	タイムスタンプ *DoS* 攻撃を防止するため、パケットから *TCP* タイムスタンプを取り除きます。
TCP Fast Open		TCP 3 ウェイ ハンドシェーク時の TCP SYN または SYN-ACK パケットから TCP Fast Open オプション（およびある場合はデータ ペイロード）を除去します。 これを選択しない（無効にする）場合、TCP Fast Open オプションは許可されます。これによりデータ配信が含まれるため、接続セットアップのスピードが維持されます。これは、データとの TCP SYN、およびデータとの TCP SYN-ACK とは独立して機能します。デフォルトで無効になっています。
マルチパス TCP (MPTCP) オプション		TCP 拡張である MPTCP は、クライアントから宛先ホストへの接続で同時に複数のパスを使用し、接続を維持できるようにします。デフォルトでは、グローバル MPTCP 設定に基づき、MPTCP サポートは無効です。 このプロファイルに関連するセキュリティ ゾーンの MPTCP 設定を、以下のように確認または調整します。 • **no**（いいえ）– MPTCP サポートを有効にします（MPTCP オプションを除去しない）。 • **yes**（はい）– MPTCP サポートを無効にします（MPTCP オプションを除去する）。これを設定すると、MPTCP には TCP への下位互換性があるため、MPTCP 接続が標準 TCP 接続に変換されます。 • （デフォルト）**global**（グローバル）– グローバル MPTCP 設定に基づいて、MPTCP をサポートします。グローバル MPTCP 設定はデフォルトでは yes（はい）に設定されているため、MPTCP は無効です（MPTCP オプションはパケットから除去されます）。以下の CLI コマンドを使用して、グローバル MPTCP 設定を確認または調整できます。 `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

© 2019 Palo Alto Networks, Inc.

ICMP ドロップ

ゾーンで受信した特定の ICMP パケットをドロップするようにファイアウォールに指示する場合は、以下の設定を選択して有効にします。

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
ICMP ping ID 0	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Packet Based Attack Protection**（パケット ベースの攻撃防御）> **ICMP Drop**（**ICMP** ドロップ）	ICMP pingパケットの識別子の値が0の場合、パケットを廃棄します。
ICMP フラグメント		ICMPフラグメントで構成されるパケットを廃棄します。
ICMP 大型パケット (>1024)		1024バイトを超えるICMPパケットを廃棄します。
エラー メッセージとともに組み込まれている ICMP を破棄		エラーメッセージが組み込まれているICMPパケットを廃棄します。
ICMP TTL 失効エラーを抑制		ICMP TTL の有効期限切れメッセージの送信を停止します。
ICMP フラグメント要求メッセージを抑制		インターフェイスの MTU を超えたパケットに対する ICMP フラグメント要求メッセージの送信を停止し、フラグメントなし（DF）ビットを設定します。この設定により、ファイアウォールの背後のホストで PMTUD プロセスが実行されなくなります。

IPv6 Drop[IPv6ドロップ]:

ゾーンで受信した特定の IPv6 パケットをドロップするようにファイアウォールに指示する場合は、以下の設定を選択して有効にします。

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
タイプ 0 のルーティング ヘッダー	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）	タイプ0のルーティングヘッダーを含むIPv6パケットを廃棄します。タイプ 0 のルーティング ヘッダーについては、『RFC 5095』を参照してください。
IPv4 互換アドレス		RFC 4291 IPv4互換用IPv6アドレスとして定義された IPv6パケットを破棄します。
エニーキャスト送信元アドレス		エニーキャスト送信元アドレスを含むIPv6パケットを廃棄します。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
不要なフラグメントヘッダー	> **Packet Based Attack Protection**（パケット ベースの攻撃保護）> **TCP Drop**（**TCP** ドロップ）	最終フラグメントフラグ（M=0）を含み、オフセットがゼロのIPv6パケットを破棄します。
1280 バイト未満の ICMP の MTU (パケットが大きすぎる)		最大転送単位（MTU）が1,280バイト未満の場合は、パケットが大きすぎるというICMPv6メッセージを含むIPv6パケットを破棄します。
ホップ バイ ホップ拡張		ホップバイホップオプション拡張ヘッダーを含むIPv6パケットを廃棄します。
Routing extension（ルーティング拡張）		ルーティング拡張ヘッダーを含むIPv6パケットを破棄します。ルーティング拡張ヘッダーを含むパケットは、宛先に向かう際に1つ以上の中間ノードを経由します。
宛先の拡張		宛先オプション拡張を含むIPv6パケットを破棄します。宛先オプション拡張には、パケットの宛先のみを対象としたオプションが含まれています。
拡張子ヘッダー内の無効なIPv6オプション		無効なIPv6オプションが拡張ヘッダーに含まれているIPv6パケットを破棄します。
ゼロ以外の予約フィールド		ヘッダーの予約フィールドがゼロに設定されていないIPv6パケットを破棄します。

ICMPv6 ドロップ

ゾーンで受信した特定の ICMPv6 パケットに対して、対応方法をファイアウォールに指示する場合は、以下の設定を選択して有効にします。

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
ICMPv6 宛先に到達不能 - 明示的なセキュリティ ルールの一致が必要です	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾー	メッセージが既存のセッションと関連付けられている場合でも、ICMPv6 宛先到達不能メッセージがセキュリティ ルールと明確に一致している必要があります。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – パケット ベースの攻撃防御	設定場所	の意味
ICMPv6 パケットが大きすぎます - 明示的なセキュリティ ルールの一致が必要です	ン プロテクション) > **Packet Based Attack Protection** (パケット ベースの攻撃防御) > **ICMPv6 Drop** (**ICMPv6** ドロップ)	メッセージが既存のセッションと関連付けられている場合でも、ICMPv6 パケット超過メッセージがセキュリティ ルールと明確に一致している必要があります。
ICMPv6 時間超過 - 明示的なセキュリティ ルールの一致が必要です		メッセージが既存のセッションと関連付けられている場合でも、ICMPv6 の時間超過メッセージがセキュリティ ルールと明確に一致している必要があります。
ICMPv6 パラメータの問題 - 明示的なセキュリティ ルールの一致が必要です		メッセージが既存のセッションと関連付けられている場合でも、ICMPv6 のパラメータ エラー メッセージがセキュリティ ルールと明確に一致している必要があります。
ICMPv6 リダイレクト - 明示的なセキュリティ ルールの一致が必要です		メッセージが既存のセッションと関連付けられている場合でも、ICMPv6 のリダイレクト メッセージがセキュリティ ルールと明確に一致している必要があります。

プロトコル保護

- Network (ネットワーク) > Network Profiles (ネットワーク プロファイル) > Zone Protection (ゾーン プロテクション) > Protocol Protection (プロトコル保護)

ファイアウォールは通常、レイヤー 2 ゾーン間とバーチャル ワイヤー ゾーン間の IP 以外のプロトコルを許可します。プロトコル保護を使用すると、レイヤー 2 VLAN またはバーチャル ワイヤーのセキュリティ ゾーン間あるいはゾーン内において、IP 以外のどのプロトコルを許可するか (包含による)、拒否するか (除外による) を制御できます。IP 以外のプロトコルの例として、AppleTalk、Banyan VINES、Novell、NetBEUI や、Generic Object Oriented Substation Event (GOOSE) などの Supervisory Control and Data Acquisition (SCADA) システムが挙げられます。

ゾーン プロテクション プロファイルでプロトコル保護を設定した後、レイヤー 2 VLAN またはバーチャル ワイヤーの入力セキュリティ ゾーンにプロファイルを適用します。

インターネットに接続されたゾーンでプロトコル保護を有効化し、使用しないプロトコルから来るレイヤー 2 トラフィックがネットワークに侵入しないようにします。

© 2019 Palo Alto Networks, Inc.

ゾーン プロテクション プロファイル設定 – プロトコル保護	設定場所	の意味
ルールの種類	**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Zone Protection**（ゾーン プロテクション）> **Protocol Protection**（プロトコル保護）	プロトコル保護用に作成するリストのタイプを以下のように指定します。 • **Include List**（許可リスト）– このリストのプロトコルのみが許可されます。ただし、IPv4（0x0800）、IPv6（0x86DD）、ARP（0x0806）、VLAN タグ フレーム（0x8100）は許可されます。その他のプロトコルはすべて暗黙的に拒否（ブロック）されます。 • **Exclude List**（除外リスト）– このリストのプロトコルのみが拒否されます。その他のプロトコルはすべて暗黙的に許可されます。IPv4（0x0800）、IPv6（0x86DD）、ARP（0x0806）、VLAN タグ フレーム（0x8100）は除外できません。 許可リストを使用し、使用するレイヤー *2* プロトコルだけをホワイトリストに登録して他のプロトコルをすべて拒否します。これにより、ネットワーク上で使用しないプロトコルを拒否することで攻撃の入り口を減らすことができます。除外リストはリストに含めていないすべてのプロトコルを許可するブラックリストであり、プロトコル保護を設定しない場合、すべてのレイヤー *2* プロトコルが許可されます。
プロトコル名		リストに追加する Ethertype コードに対応するプロトコル名を入力します。ファイアウォールはプロトコル名が Ethertype コードに一致することを確認しませんが、Ethertype コードがプロトコル フィルタを特定します。
Enable [有効化]		リストの Ethertype コードを**Enable**（有効化）します。しかし、テストのためにプロトコルを削除せずに無効にする場合は、無効にしてください。
Ethertype (16 進数)		0x で始まる 16 進数の Ethertype コード（プロトコル）を入力します（範囲は 0x0000 ~ 0xFFFF）。リストには Ethertype を 64 個まで登録できます。 以下に Ethertype コードの参考資料をいくつか示します。 • IEEE の 16 進数 Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> QoS

QoS プロファイルを **Add**（追加）して、最大 8 個のサービスクラスの帯域幅制限および優先順位を定義します。保証帯域幅制限と最大帯域幅制限は、個別のクラスにも、ひとまとめのクラスにも設定することができます。優先順位によって、競合がある場合のトラフィックの処理方法が決まります。

© 2019 Palo Alto Networks, Inc.

ファイアウォールで QoS を完全に提供できるようにするには、以下の手順も必要です。

- QoS 処理を受信するトラフィックを定義します（Policies（ポリシー）> QoS を選択して、QoS ポリシーを追加または変更します）。
- インターフェイス上で QoS を有効にします（Network（ネットワーク）> QoS を選択します）。

QoS の詳細なワークフロー、コンセプト、使用例については、「Quality of Service（サービス品質）」を参照してください。

QoS プロファイル設定	
プロファイル名	プロファイルの識別に使用する名前を入力します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
最大保証帯域　出力側	このインターフェイスを介してファイアウォールから出力されるトラフィックの最大スループット（Mbps）を入力します。値はデフォルトで 0 で、ファイアウォール制限（PAN-OS 7.1.16 以降のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースでは16,000）を指定します。 QoS プロファイルの **Egress Max**（最低保証帯域 出力側）は、QoS が有効になっている物理インターフェイスに定義された **Egress Max**（最低保証帯域 出力側）の値以下でなければなりません。「Network（ネットワーク）> QoS」を参照してください。 *Egress Max*（最大保証帯域出力側）は必須フィールドではありませんが、*QoS* プロファイルのこの値は常に定義しておくことをお勧めします。
最低保証帯域　出力側	このプロファイルで保証する帯域幅 (Mbps) を入力します。出力側の最大保証帯域を超過した場合、ファイアウォールはベストエフォート制でトラフィックを通過させます。
クラス	QoS クラスを **Add**（追加）して、個々の QoS クラスの処理方法を指定します。設定する 1 つ以上のクラスを選択できます。 • **Class**[クラス] – クラスを設定しなくても、QoS ポリシーにクラスを含めることができます。その場合、トラフィックは QoS 全体に対する制限の対象になります。QoS ポリシーに一致していないトラフィックはクラス 4 に割り当てられます。 • **Priority**[優先順位] – クラスに割り当てる優先度を選択します。 　• **real-time** [リアルタイム] 　• **high** 　• **Medium**（中） 　• 低 競合が発生すると、優先順位の低いトラフィックが破棄されます。優先順位 Real-time [リアルタイム]では、固有のキューが使用されます。 • **Egress Max**（最大保証帯域出力側）– このクラスの最大スループット (Mbps) を入力します。値はデフォルトで 0 で、ファイアウォール制限（PAN-OS 7.1.16 以降のリリースでは 60,000 Mbps、PAN-OS 7.1.15 以前のリリースでは16,000）を指定します。QoS クラスの **Egress Max**（最大保証帯域出力側）は、QoS プロファイルに定義された **Egress Max**（最低保証帯域 出力側）以下でなければなりません。

© 2019 Palo Alto Networks, Inc.

QoS プロファイル設定	
	これは必須フィールドではありませんが、*QoS* プロファイルの *Egress Max* (最大保証帯域 出力側) の値を常に定義することをお勧めします。 • **Egress Guaranteed**[最低保証帯域　出力側] – このクラスの保障帯域幅 (Mbps) を入力します。あるクラスに対し割り当てられた保証帯域は、そのクラスのために確保されているわけではなく、未使用の帯域はすべてのクラスで使用可能な状態になっています。しかし、ファイアウォールを通過するトラフィックが出力側の最大保証帯域を超過した場合、ファイアウォールはベストエフォート制でトラフィックを通過させます。

Network > Network Profiles > LLDP Profile　[ネットワーク > ネットワーク プロファイル > LLDP プロファイル]

リンク レイヤー検出プロトコル (LLDP) プロファイルでは、ファイアウォールの LLDP モードの設定、Syslog および SNMP 通知の有効化、および LLDP ピアに送信するオプションの TLV (Type-Length-Values) の設定を行えます。LLDP プロファイルを設定した後、そのプロファイルを 1 つ以上のインターフェイスに割り当てます。

LLDP の設定および監視の方法などについて詳しくは、LLDP をご確認ください。

LLDP プロファイル設定	の意味
氏名	LLDP プロファイルの名前を指定します。
モード	LLDPの動作モードを選択してください。**transmit-receive**[送受信]、**transmit-only**[送信のみ]、または**receive-only**[受信のみ]。
SNMP Syslog 通知	SNMP トラップと Syslog 通知を有効にします。これは、グローバル**Notification Interval**[通知間隔]で実行されます。有効にした場合、ファイアウォールは、**Device** (デバイス) > **Log Settings** (ログ設定) > **System** (システム) > **SNMP Trap Profile** (**SNMP** トラップ プロファイル) および **Syslog Profile** (**Syslog** プロファイル) の設定に従って、SNMP トラップと Syslog イベントの両方を送信します。
ポートの説明	ファイアウォールの ifAlias オブジェクトをPort Description [ポートの説明] の TLV で送信できるようにします。
システム名	ファイアウォールの sysName オブジェクトをSystem Name [システム名] の TLV で送信できるようにします。
システムの説明	ファイアウォールの sysDescr オブジェクトをSystem Description [システムの説明] の TLV で送信できるようにします。
システムの機能	インターフェイスのデプロイメント モード (L3、L2、またはバーチャル ワイヤー) を以下のマッピングによりSystem Capabilities [システムの機能] の TLV で送信できるようにします。 • L3 の場合、ファイアウォールは、ルーター (ビット 6) の機能と他のビット (ビット 1) を通知します。

© 2019 Palo Alto Networks, Inc.

LLDP プロファイル設定	の意味
	• L2 の場合、ファイアウォールは、MAC ブリッジ (ビット 3) の機能と他のビット (ビット 1) を通知します。 • バーチャル ワイヤーの場合、ファイアウォールは、リピーター (ビット 2) の機能と他のビット (ビット 1) を通知します。 SNMP MIB により、インターフェイスで設定された複数の機能が単一エントリに結合されます。
管理アドレス	**Management Address**[管理アドレス]を [管理アドレス] の TLV で送信できるようにします。管理アドレスは 4 つまで入力でき、指定した順に送信されます。順序を変更する場合は、**Move Up**[上へ] または **Move Down**[下へ] をクリックします。
氏名	管理アドレスの名前を指定します。
インターフェイス	IP アドレスが管理アドレスになるインターフェイスを選択します。**None**[なし] を指定した場合は、IPv4またはIPv6を選択する場所の隣のフィールドにIPアドレスを入力できます。
IP の選択肢	**IPv4** または **IPv6** を選択した後、管理アドレスとして送信する IP アドレスを隣のフィールドで選択または入力します。**Management Address**[管理アドレス] の TLV が有効の場合は、1 つ以上の管理アドレスが必要です。管理 IP アドレスを設定しない場合は、送信する管理アドレスとして送信インターフェイスの MAC アドレスが使用されます。

Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル]

双方向フォワーディング検知 (BFD) は、リンク障害の極めて素早い検知を可能にし、さらに別ルートへのフェイルオーバーを早めます。

確認すべき情報	以下を参照
BFDについて	BFD の概要
BFDプロファイルの作成時に入力できるフィールドについて	BFD プロファイルの構成要素
仮想ルーターの BFD ステータスを参照する。	BFD のサマリーと詳細を表示
その他の情報をお探しですか？	BFD の詳細を確認し、設定する。 次の目的で BFD を設定する。 静的ルート BGP OSPF OSPFv3IPv6 RIP

© 2019 Palo Alto Networks, Inc.

BFD の概要

BFDとは、インターフェイス、データリンク、または実際の転送エンジンを含む、2つの転送エンジンの間の双方向パスにおいて発生した障害を検出するプロトコルです。PAN-OS導入環境下では、以下のうち1つのエンジンがファイアウォールのインターフェイスとなり、他方が隣接して設定されたBFDピアとなります。2つのエンジンの間のBFD障害検知は極めて速いため、Helloパケットやハートビートを用いてリンクモニタリングや、頻繁にダイナミックルーティングのヘルスチェックを行った場合よりも素早いフェイルオーバーが可能になります。

BFDが障害を検出した場合、ルーティングプロトコルに対し、ピアに向かうパスを代わりのものに切り替えるよう通知します。BFDがスタティックルート用に設定されている場合、ファイアウォールはRIBおよびFIBのテーブルから障害の発生したルートを除外します。

BFDをサポートしているインターフェイスタイプには、物理イーサネット、AE、VLAN、トンネル（サイト間VPNおよびLSVPN）、およびレイヤー3インターフェイスのサブインターフェイスがあります。それぞれのスタティックルートあるいはダイナミックルーティングプロトコルについて、BFDの有効化または無効化し、デフォルトBFDプロファイルを選択するか、あるいはBFDプロファイルを設定することができます。

BFD プロファイルの構成要素

- Network > Network Profiles > BFD Profile [ネットワーク > ネットワークプロファイル > BFDプロファイル]

デフォルトのBFDプロファイルあるいは作成したBFDプロファイルを適用することで、スタティックルートやダイナミックルーティングプロトコルでBFDを有効化することができます。デフォルトプロファイルではデフォルトのBFD設定を使用しており、これを変更することはできません。BFDプロファイルを新しく**Add**[追加]し、以下の項目を指定することも可能です。

BFDプロファイル設定	の意味
氏名	BFDプロファイルの名前を入力します (最大31文字)。名前の大文字と小文字は区別されます。また、ファイアウォール上で重複していない名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
モード	BFDの動作モード: • **Active**[アクティブ] - BFDがコントロールパケットの送信を開始します（デフォルト）。最低でも1つのBFDピアがアクティブに設定されている必要があります。両方がアクティブでも構いません。 • **Passive**[パッシブ] - BFDはピアからコントロールパケットが送られてくるまで待機し、要求に応じて応答を行います。
希望する最低Tx間隔（ミリ秒）	BFDプロトコルにBFDコントロールパケットを送信させたい間隔の最低値です（ミリ秒単位）。PA-7000 Seriesの最小値は50、PA-3200 Series は 100、VM-Series は 200 です（最大値は 2000、デフォルトは 1000）。 *1つのインターフェイスにおいて複数のプロトコルで異なるBFDプロファイルを使用している場合、BFDプロファイルにはすべて同じDesired Minimum Tx Interval[希望する最低Tx間隔]を設定してください。*

© 2019 Palo Alto Networks, Inc.

BFDプロファイル設定	の意味
最低Rx間隔要件（ミリ秒）	BFDがBFDコントロールパケットを受信できる間隔の最低値です（ミリ秒単位）。PA-7000 Series の最小値は 50、PA-3200 Series は 100、VM-Series は 200 です（最大値は 2000、デフォルトは 1000）。
検知時間乗数値	ローカルシステムはリモートシステムから受信した**Detection Time Multiplier (検知時間乗数)**を同意済みのリモートシステムの送信間隔（**Required Minimum Rx Interval (最低 Rx 間隔要件)**および最後に受信した**Desired Minimum Tx Interval (目標の最低 Tx 間隔)**のうち、いずれか大きい方）で掛けることで検知時間を算出します。検知時間が過ぎるまでに BFD がピアからの BFD コントロールパケットを受信しない場合、障害が発生していることを意味します（範囲は 2～50、デフォルトは 3）。
ホールドタイム（ミリ秒単位）	リンクが確立されてからファイアウォールがBFDコントロールパケットを送信するまでに待機する時間です（ミリ秒単位）。**Hold Time**[待機時間] はBFDアクティブモードのみに適用されます。ファイアウォールが **Hold Time**（ホールドタイム）内に BFD コントロール パケットを受信した場合、それを無視します（範囲は0 ～ 120000、デフォルトは 0）。デフォルトで設定されている0とは、送信**Hold Time**[待機時間] を使用しないということです。リンクが確立すると、ファイアウォールは直ちにBFDコントロールパケットの送受信を行います。
マルチホップの有効化	マルチホップでBFDを有効化します。BGP導入環境にのみ適用されます。
最低Rx TTL値	マルチホップBFDがサポートされている場合に、BFDが受信する最低Time-to-Live値（ホップ数）です。BGP導入環境にのみ適用されます（範囲は1～254、デフォルトなし）。

BFD のサマリーと詳細を表示

- Network > Virtual Routers [ネットワーク > 仮想ルーター]

以下の表で、BFD サマリー情報について説明します。

BFD情報の表示	
BFDサマリーの表示	**Network** > **Virtual Routers**[ネットワーク > 仮想ルーター] を開き、詳細を確認したい仮想ルーターの行で **More Runtime Stats**[ランタイム状態の詳細] をクリックします。**BFD Summary Information**[BFDサマリー情報]のタブを選択します。
BFDの詳細の表示	BFDの詳細を表示したいインターフェイスの行で**details**[詳細] を選択します。

Network > Network Profiles > SD-WAN [ネットワーク > ネットワーク プロファイル > SD-WAN インターフェイス プロファイル]

SD-WAN インターフェイス プロファイルを作成して、リンク タグによって物理リンクをグループ化し、リンクの速度とファイアウォールがそれらのリンクを監視する頻度を制御します。

© 2019 Palo Alto Networks, Inc.

	SD-WAN インターフェイス プロファイル
名前	SD-WAN インターフェイス プロファイルの **Name** (名前) を最大 31 文字の英数字を使用して入力します。名前は英数字で始まる必要があり、文字、数字、アンダースコア (_)、ハイフン (-)、ピリオド (.)、スペースを使用できます。
Link Tag (リンク タグ)	このプロファイルがインターフェイスに割り当てる **Link Tag** (リンク タグ) を選択するか、新しいタグを **Add** (追加) します。リンク タグは、パスの選択およびフェイルオーバー中にファイアウォールが選択する物理リンク (異なる ISP) を束ねます。
の意味	プロファイルのわかりやすい説明を入力します。
リンク タイプ	事前定義済されたリストから物理リンク タイプを選択します (**ADSL/DSL**、**Cable Modem** (ケーブルモデム)、**Ethernet** (イーサネット)、 **Fiber** (ファイバ)、**LTE/3G/4G/5G**、 **MPLS**、**Microwave/Radio** (マイクロ波 / ラジオ波)、**Satellite** (衛星)、**WiFi** 、**Other** (その他))。ファイアウォールは、ファイアウォールへのイーサネット接続としての終端やハンドオフとして任意の CPE デバイスをサポートできます。例えば、Wi-Fi アクセス ポイント、Long-Term Evolution (LTE) モデム、レーザーマイクロ波顧客構内設備 (CPE) はすべて、イーサネット ハンドオフで終端できます。
VPN Data Tunnel Support (VPN データ トンネル サポート)	(PAN-OS 9.1.2 以降の 9.1 リリース) ブランチからハブへのトラフィックとリターントラフィックが、セキュリティを強化するために VPN トンネルを通過するか (デフォルトで有効)、暗号化のオーバーヘッドを回避するために VPN トンネルの外部を通過するかを決定します 。 • 直接インターネット接続またはケーブルモデム、ADSL、その他のインターネット接続などのインターネット ブレイクアウト機能を備えたパブリック リンク タイプでは、 **VPN Data Tunnel Support (VPN** データ トンネル サポート**)** を有効のままにします。 • インターネット ブレークアウト機能を備えないMPLS 、衛星、マイクロ波等のプライベート リンク タイプの場合は、**VPN Data Tunnel Support (VPN** データ トンネル サポート**)** を無効にすることができます。ただし、この場合、トラフィックが VPNトンネル外に送信されるため、トラフィック傍受をされないようにする必要があります。 • 多くのブランチには、ハブに接続しているプライベート MPLS リンクにフェイルオーバーし、ハブからインターネットに到達する必要がある DIA トラフィックがあります。**VPN Data Tunnel Support (VPN** データ トンネル サポート**)** の設定は、プライベート データが VPN トンネルを通過するか、あるいはトンネル外を通過するかを決定し、フェイルオーバー トラフィックはその他の接続を使用します(プライベートデータフローは使用しません) 。ファイアウォールはゾーンを使用して、プライベート MPLS トラフィックからの DIA フェイルオーバー トラフィックをセグメント化します。
Maximum Download (最大ダウンロード) (Mbps)	ISP からの 最大ダウンロード 速度をMbpsで指定します (1 ～100,000 の範囲、デフォルト値はなし)。ISP にリンク速度を問い合わせるか、speedtest.net などのツールを使用してリンクの最大速度をサンプリングし、適切な期間の最大値の平均を取ります。
Maximum Upload (最大アップロード) (Mbps)	ISP からの最大アップロード速度をMbpsで指定します (1 ～ 100,000の範囲、デフォルト値はなし)。ISP にリンク速度を問い合わせるか、speedtest.net などのツールを使用してリンクの最大速度をサンプリングし、適切な期間の最大値の平均を取ります。

© 2019 Palo Alto Networks, Inc.

	SD-WAN インターフェイス プロファイル
パス モニタリング	この SD-WAN インターフェイス プロファイルを適用するインターフェイスをファイアウォールが監視するパス モニタリング モードを選択します。 • **Aggressive (アグレッシブ)** (LTE および衛星を除くすべてのリンク タイプのデフォルト) - ファイアウォールは一定の頻度でプローブ パケットを SD-WAN リンクの反対側に送信します。 *Aggressive (アグレッシブ)* モードは、電圧低下および停電時の高速検出およびフェイルオーバーが必要な場合に使用します。 • **Relaxed (リラックスド)** (LTE およびサテライト リンク タイプのデフォルト)–ファイアウォールはプローブ パケット セットを送信する間隔を数秒 (**Probe Idle Time (プローブ アイドル時間)**) 待機します。これはパス モニタリングの頻度低下を意味します。Probe Idle Time (プローブ アイドル時間) が経過すると、ファイアウォールは設定された **Probe Frequency (プローブ頻度)** で 7 秒間プローブを送信します。 *Relaxed (リラックスド)* モードは、低帯域幅リンクや使用量に応じて課金されるリンク *(LTE等)* を使用している場合、あるいはコストおよび帯域幅の維持と比べて高速検出が重要ではない場合に使用します。
Probe Frequency (プローブ頻度) (秒間)	ファイアウォールがプローブ パケットを SD-WAN リンクの反対側の端に送信する 1 秒あたりの回数であるプローブ頻度を入力します(範囲は 1 ～5、デフォルトは 5)。
Probe Idle Time (プローブ アイドル時間) (秒)	**Relaxed (リラックスド)** パス モニタリングを選択した場合、ファイアウォールがプローブ パケットのセット間で待機する時間である Probe Idle Time (プローブ アイドル時間) (秒) を設定することができます (範囲は 1 ～60、デフォルトは 60)。
Failback Hold Time (フェールバック 保持時間) (秒)	ファイアウォールが回復したリンクが確立されたままになるのをファイアウォールが待機する時間 (秒単位) を入力します。この時間が経過すると、ファイアウォールはフェイルオーバー後にそのリンクを優先リンクとして復元します (20 ～ 120 の範囲、デフォルトは 120)。フェールバック 保持時間は、優先リンクとして回復したリンクの復帰が早過ぎ、すぐに再度失敗することを防ぎます。

© 2019 Palo Alto Networks, Inc.

デバイス

ファイアウォールの基本的なシステム設定と管理タスクのフィールド リファレンスは、以下のセクションを参照してください。

- Device (デバイス) > Setup (セットアップ)
- Device > High Availability [デバイス > 高可用性]
- Device (デバイス) > Log Forwarding Card (ログ転送カード)
- Device > Config Audit [デバイス > 設定監査]
- [Device] > [パスワード プロファイル]
- Device > Administrators [デバイス > 管理者]
- Device > Admin Roles [デバイス > 管理者ロール]
- Device > Access Domain [デバイス > アクセス ドメイン]
- Device > Authentication Profile [デバイス > 認証プロファイル]
- Device > Authentication Sequence [デバイス > 認証シーケンス]
- ユーザー ID
- Device > VM Information Sources [デバイス > VM 情報の送信元]
- Device (デバイス) > Troubleshooting (トラブルシューティング)
- Device > Virtual Systems [デバイス > 仮想システム]
- Device > Shared Gateways [デバイス > 共有ゲートウェイ]
- Device (デバイス) > Certificate Management (証明書の管理)
- Device > Response Pages [デバイス > 応答ページ]
- Device > Log Settings [デバイス > ログ設定]
- [Device] > [サーバー プロファイル]
- Device > Local User Database > Users [デバイス > ローカル ユーザー データベース > ユーザー]
- Device > Local User Database > User Groups [デバイス > ローカル ユーザー データベース > ユーザー グループ]
- Device > Scheduled Log Export [デバイス > スケジュール設定されたログのエクスポート]
- Device > Software [デバイス > ソフトウェア]
- Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]
- Device > Dynamic Updates [デバイス > 動的更新]
- Device > Licenses [デバイス > ライセンス]
- Device > Support [デバイス > サポート]
- Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]

Device（デバイス）> Setup（セットアップ）

- Device > Setup > Management [デバイス > セットアップ > 管理]
- Device > Setup > Operations [デバイス > セットアップ > 操作]
- Device > Setup > HSM [デバイス > セットアップ > HSM]
- Device > Setup > Services [デバイス > セットアップ > サービス]
- Device（デバイス）> Setup（セットアップ）> Interfaces（インターフェイス）
- Device（デバイス）> Setup（セットアップ）> Telemetry（テレメトリ）
- Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]
- Device > Setup > WildFire [デバイス > セットアップ > WildFire]
- Device > Setup > Session [デバイス > セットアップ > セッション]

© 2019 Palo Alto Networks, Inc.

Device > Setup > Management [デバイス > セットアップ > 管理]

- **Device** (デバイス) > **Setup** (セットアップ) > **Management** (管理)を選択します。
- **Panorama** > **Setup** (セットアップ) > **Management** (管理)

管理設定を行うには、ファイアウォールで **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）を選択します。

Panorama テンプレートを使用して管理するファイアウォールを設定するには、Panorama™ で **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）を選択します。Panorama の管理設定を行うには、**Panorama** > **Setup**（セットアップ）> **Management**（管理）を選択します。

以下の管理設定は、記載されていない限り、ファイアウォールと Panorama の両方に適用されます。

- 一般設定
- 認証設定
- ポリシー ルールベース設定
- Panorama設定Device（デバイス）> Setup（セットアップ）> Management（管理）（Panorama に接続するためにファイアウォールで指定する設定）
- Panorama設定Panorama > Setup（セットアップ）> Management（管理）（ファイアウォールに接続するために Panorama で指定する設定）
- ロギングおよびレポート設定
- バナーとメッセージ
- パスワード複雑性設定
- AutoFocus™
- Logging Service

項目	の意味
一般設定	
ホスト名	ホスト名（最大 31 文字）を入力します。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。 値を入力しない場合、PAN-OS® はファイアウォール モデル（PA-5220_2 など）をデフォルトとして使用します。 必要に応じて、DHCP サーバーが提供するホスト名を使用するようにファイアウォールを設定することもできます。「DHCP サーバーが提供するホスト名を使用する（ファイアウォールのみ）」を参照してください。 一意のホスト名を設定し、管理するデバイスを識別しやすくします。
ドメイン	ファイアウォールのネットワーク ドメイン名を入力します (最大 31 文字)。 必要に応じて、DHCP サーバーが提供するドメインを使用するようファイアウォールと Panorama を設定することもできます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	「DHCP サーバーが提供するドメインを使用する（ファイアウォールのみ）」を参照してください。
DHCP サーバーが提供するホスト名を使用する（ファイアウォールのみ）	（管理インターフェイスの IP タイプが DHCP Client（DHCP クライアント）の場合のみ適用されます）管理インターフェイスにDHCPサーバーから受信したドメイン（DNSサフィックス）を使用させる場合はこのオプションを選択します。Hostname（ホスト名）フィールドに指定されている値は、サーバーからのホスト名（有効な場合）で上書きされます。
DHCP サーバーが提供するドメインを使用する（ファイアウォールのみ）	（管理インターフェイスの IP タイプが DHCP Client（DHCP クライアント）の場合のみ適用されます）管理インターフェイスにDHCPサーバーから受信したドメイン（DNSサフィックス）を使用させる場合はこのオプションを選択します。**Domain**（ドメイン）フィールドに指定されている値は、サーバーからのドメインで上書きされます。
ログイン バナー	Webインターフェイスのログインページの**Name** [ユーザー名] および**Password** [パスワード] のフィールドの下に表示するテキスト（最大3,200文字）を入力します。
管理者にログインバナーの承認を強制する	ログインページのログインバナーの上に**I Accept and Acknowledge the Statement Below**（以下の内容を受諾し同意します）という一文を表示し、管理者に選択させるようにする場合はこのオプションを選択してください。管理者はこのメッセージの内容を理解し受諾しない限り**Login**（ログイン）できません。
SSL/TLS Service Profile	既存の SSL/TLS サービス プロファイルを割り当てるか、新しい SSL/TLS サービス プロファイルを作成して、管理インターフェイスで許可される証明書と SSL/TLS プロトコル設定を指定します（「Device（デバイス）> Certificate Management（証明書の管理）> SSL/TLS Service Profile（SSL/TLS サービス プロファイル）」を参照）。ファイアウォールまたは Panorama は、この証明書を使用して、管理（MGT）インターフェイスから、または HTTP/HTTPS 管理トラフィックをサポートするその他のインターフェイスから Web インターフェイスにアクセスする管理者を認証します（「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> Interface Mgmt（インターフェイス管理）」を参照）。**None**（なし）（デフォルト）を選択した場合、ファイアウォールまたは Panorama は事前定義済みの証明書を使用します。 事前定義済みの証明書は便宜上提供されているものです。セキュリティを強化するために、*SSL/TLS* サービス プロファイルを割り当ててください。信頼性を確保するには、クライアント システムの信頼されたルート証明書ストアに含まれる認証局（*CA*）証明書で証明書を署名する必要があります。
タイム ゾーン	ファイアウォールのタイム ゾーンを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
表示言語	ドロップダウンリストから、PDF レポートの言語を選択します。「Monitor（監視）> PDF Reports（PDF レポート）> Manage PDF Summary（PDF サマリーの管理）」を参照してください。 Webインターフェイスに特定の言語設定が設定されている場合でも、PDFレポートにはこの**Locale** [表示言語] の設定で指定した言語が使用されます。
日付	ファイアウォールの日付を設定します。現在の日付 (YYYY/MM/DD 形式) を入力するか、ドロップダウン リストから日付を選択します。 *NTP サーバー (Device (デバイス) > Setup (セットアップ) > Services (サービス))* を定義することもできます。
時間	ファイアウォールの時刻を設定します。現在の時刻を 24 時間形式で入力するか、ドロップダウン リストから時刻を選択します。 *NTP サーバー（Device（デバイス）> Setup（セットアップ）> Services（サービス））*を定義することもできます。
シリアル番号 （Panorama バーチャル アプライアンスのみ）。	Panorama のシリアル番号を入力します。シリアル番号は、Palo Alto Networks® から送信された受注処理電子メールに記載されています。
緯度	ファイアウォールの緯度（-90.0から90.0）を入力します。
経度	ファイアウォールの経度（-180.0から180.0）を入力します。
コミットロックの自動実施	候補設定を変更するときにコミットロックが自動的に適用されるようにするには、このオプションを選択します。詳細は、「変更内容のロック」を参照してください。 *Automatically Acquire Commit Lock (コミット ロックの自動実施)*を有効化し、最初の管理者が変更をコミットするまでの間、他の管理者が設定を変更できないようにします。
証明書有効期限チェック	デバイス内の証明書の有効期限が近づいた時に警告メッセージを作成するようにファイアウォールに指示します。 *Certificate Expiration Check (証明書有効期限チェック)*を有効化し、デバイス内の証明書の有効期限が近づいた時に警告メッセージを作成します。
マルチ仮想システム機能	この機能をサポートするファイアウォールで複数の仮想システムの使用を有効にします（「Device（デバイス）> Virtual Systems（仮想システム）」を参照）。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ファイアウォールでマルチ仮想システムを有効化するには、*640* を超える異なるユーザー グループをファイアウォール ポリシーで参照することはできません。必要に応じて、参照するユーザーグループの数を減らしてください。この後にマルチ仮想システムの有効化と追加を行うと、ポリシーは追加されたマルチ仮想システムごとに*640*個のユーザーグループを参照することができます。
URL フィルタリング データベース （Panorama のみ）	Panoramaで使用するURLフィルタリングベンダーを選択します。**brightcloud** または **paloaltonetworks**（PAN-DB）から選択してください。
ハイパーバイザによって割り当てられた MAC アドレスの使用 （VM-Series ファイアウォールのみ）	PAN-OS カスタム スキーマを使用して MAC アドレスを生成するのではなく、ハイパーバイザによって割り当てられた MAC アドレスを VM-Series ファイアウォールで使用するには、このオプションを選択します。 このオプションを有効にして、インターフェイスに IPv6 アドレスを使用する場合、インターフェイス ID に EUI-64 形式は使用できません。EUI-64 形式では IPv6 アドレスがインターフェイスの MAC アドレスから導出されます。高可用性（HA）アクティブ/パッシブ設定で EUI-64 形式が使用されると、コミット エラーが発生します。
GTP セキュリティ	GPRS トンネリング プロトコル（GTP）トラフィック内の制御プレーン メッセージとユーザー データプレーン メッセージを検査する機能を有効にするには、このオプションを選択します。GTP トラフィックに対してポリシーを適用できるように GTP プロテクション プロファイルを設定するには、「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> GTP Protection（GTP プロテクション）」を参照してください。
SCTP Security SCTP セキュリティ	ストリーム制御伝送プロトコル（SCTP）パケットとチャンクの検査とフィルタリング、および SCTP 開始（INIT）フラッド防御の適用を有効にするには、このオプションを選択します。「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> SCTP Protection（SCTP プロテクション）」を参照してください。SCTP INIT フラッド防御については、「Configure SCTP INIT Flood Protection（SCTP INIT フラッド防御の設定）」を参照してください。
デバイス証明書 (PAN-OS 9.1.3 以降のリリースのみ)	
証明書の取得	クリックして、Palo Alto Networks カスタマー サポート ポータル (CSP)から生成された ワン タイム パスワード (OTP) を入力します。デバイス証明書は、CSP でパノラマを正常に認証し、ゼロタッチプロビジョニング (ZTP) を活用するために必要です。デバイス証明書を正常にインストールすると、以下のように表示されます。 • **Current Device Certificate Status** (現在のデバイス証明書のステータス)–デバイス証明書の現在のステータス (有効、無効、または有効期限切れ)

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **Not Valid Before** (以前は無効)—デバイス証明書がいつ有効になるかを示すタイムスタンプ。 • **Not Valid After** (以降は無効)—デバイス証明書の有効期限が切れ、デバイス証明書が 無効 または 有効期限切れになるときを示すタイムスタンプ。 • **Last Fetched Message** (最後にフェッチされたメッセージ)—デバイス証明書が正常にインストールされた、またはデバイス証明書のインストールに失敗したことを示すメッセージ。 • **Last Fetched Status** (最後にフェッチしたステータス)—デバイス証明書のフェッチのステータス (成功 または 失敗)。 • **Last Fetched Timestamp** (最後にフェッチしたタイムスタンプ)—最後のデバイス証明書のインストール試行のタイムスタンプ。
認証設定	
認証プロファイル	ファイアウォールでローカルに定義されたものではなく、外部サーバーで定義された管理者アカウントを認証するためにファイアウォールで使用する認証プロファイル (またはシーケンス) を選択します (「Device (デバイス) > Authentication Profile (認証プロファイル) 」を参照) 。外部管理者がログインすると、ファイアウォールは認証および承認情報 (管理ロールなど) を外部サーバーに要求します。 外部管理者の認証を有効にするには、認証プロファイルで指定されたサーバー タイプに基づいて追加の手順が必要です。そのサーバータイプは次のとおりです。 • RADIUS • TACACS+ • SAML 管理者は *SAML* を使用して *Web* インターフェイスとの認証を行うことができますが、*CLI* との認証を行うことはできません。 外部管理者の認証を無効にするには、**None** (なし) を選択します。 ローカルで (ファイアウォールで) 定義した管理者アカウントの場合、ファイアウォールは、そのアカウントに割り当てられた認証プロファイルを使用して認証を行います (「Device (デバイス) > Administrators (管理者) 」を参照) 。
証明書プロファイル	ファイアウォールの Web インターフェイスに証明書に基づいてアクセスするよう設定された管理者のクライアント証明書を検証するための証明書プロファイルを選択します。証明書プロファイルの設定手順は、「Device (デバイス) > Certificate Management (証明書の管理) > Certificate Profile (証明書プロファイル) 」を参照してください。 証明書プロファイルを設定し、証明書プロファイルで定義されているルート *CA* 証明書を使って認証を

© 2019 Palo Alto Networks, Inc.

項目	の意味
	行うために管理者のホストマシンが適切な証明書を確実に持っている状態にします。
アイドル タイムアウト	Web インターフェイスまたは CLI 上でアクティビティがない場合に管理者を自動的にログアウトするまでの最大時間（分単位）を入力します（範囲は 0 ~ 1,440、デフォルトは 60）。値 0 は、アクティビティがなくても自動ログアウトはトリガーされないことを意味します。 *Web* インターフェイス ページ（*Dashboard*（ダッシュボード）、システム アラーム ダイアログなど）の手動更新および自動更新で、*Idle Timeout*（アイドル タイムアウト）カウンターがリセットされます。自動更新をサポートするページを使用しているときにファイアウォールのタイムアウトを適用するには、更新間隔を *Manual*（手動）に設定するか、更新間隔をこの *Idle Timeout*（アイドル タイムアウト）よりも大きな値に設定してください。*Auto Refresh*（自動更新）は *ACC* タブで無効にすることもできます。 *Idle Timeout (*アイドル タイムアウト*)*を *10* 分に設定し、管理者がファイアウォールのセッションを開いたままにしている場合に未認証のユーザーがファイアウォールにアクセスするのを防ぎます。
API キーの有効期間	API キーの有効期間（分単位）を入力します（範囲は 0 ~ 525,600、デフォルトは 0）。値を 0 にすると、API キーが失効しなくなります。 以前に生成した API キーをすべて向こうにする場合は**Expire All API Keys (API** キーをすべて失効**)**させます。既存のキーがすべて使用できなくなり、それらの API キーを使って行っている作業をすべて行えなくなるため、このオプションは注意して使用してください。 *API* キーを参照している現在の実装の機能を保ちながらキーを交換できるよう、保守期間中にこの作業を行ってください。
API キーの前回の失効	API キーが最後に失効した時のタイムスタンプを表示します。キーをリセットしたことがない場合、このフィールドは値を持ちません。
最大試行回数	ファイアウォールが許容する、Web インターフェイスおよび CLI への最大ログイン試行回数（0 ~ 10）を入力します。この回数を超えると管理者アカウントがロックアウトされます。値 0 を指定すると、無制限にログインを試行できます。デフォルト値は、通常の運用モードのファイアウォールでは 0、FIPS-CC モードのファイアウォールでは 10 です。ログイン試行回数を制限することで、ファイアウォールを総当たり攻撃から保護できます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	Failed Attempts[最大試行回数] を *0* 以外の値に設定しても、*Lockout Time[ロックアウト時間]* を *0* のままにしておくと、*Failed Attempts[最大試行回数]* は無視され、ユーザーはロックアウトされません。 *Failed Attempts (試行失敗回数)*の値を *5* 以下に設定し、入力ミスに備えてある程度猶予を持たせつつ、悪意のあるシステムがブルート フォースによってファイアウォールにログインしようとするのを防ぎます。
ロックアウト時間	**Failed Attempts** (最大試行回数) の制限に達した後、Web インターフェイスおよび CLI への管理者のアクセスをファイアウォールがロックアウトする時間 (分) を入力します (範囲は 0 ~ 60)。値を 0 (デフォルト) にすると、別の管理者がアカウントのロックを手動で解除するまでロックアウトが適用されます。 *Failed Attempts (試行失敗回数)*を *0* 以外の値にしながら、*Lockout Time (ロックアウト時間)*を *0* のままにしている場合、設定された試行失敗回数に達した後、別の管理者が手動でアカウントをロック解除するまでの間、ユーザーがロックされます。 *Lockout Time (ロックアウト時間)*を *30* 分以上に設定し、攻撃者が続けてログインを試みるのを防ぎます。
ポリシー ルールベース設定	
ポリシーのタグが必須	新しいポリシールールを作成する際に 1 つ以上のタグを求めます。このオプションを有効化する際にすでにポリシールールが存在する場合、対象のルールを後で編集する際に 1 つ以上のタグを追加する必要があります。
ポリシーの説明が必須	新しいポリシールールを作成する際に**Description (説明)**を追加することを求めます。このオプションを有効化する際にすでにポリシールールが存在する場合、対象のルールを後で編集する際に**Description (説明)**を追加する必要があります。
ポリシーにタグあるいは説明がなければコミット失敗	ポリシールールにタグあるいは説明を追加していない場合、強制的にコミットを失敗させます。このオプションを有効化する際にすでにポリシールールが存在する場合、対象のルールを後で編集する際にタグや説明を追加しなければ、コミットが失敗します。 コミットを失敗させる場合、**Require tag on policies (ポリシーのタグが必須)**あるいは**Require description on policies (ポリシーの説明が必須)**を使用する必要があります。
ポリシーの監査コメントが必要	新しいポリシールールを作成する際に**Audit Comment (監査コメント)**を求めます。このオプションを有効化する際にすでにポリシー

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ルールが存在する場合、対象のルールを後で編集する際に**Audit Comment (監査コメント)**を追加する必要があります。
監査コメントの正規表現	監査コメントに必要なコメント書式パラメーターを指定します。
ポリシー ルール ヒット数	ファイアウォールで設定したポリシー ルールとトラフィックの一致頻度を追跡します。有効にすると、各ルールと一致するトラフィックの合計 Hit Count (ヒット数) と、ルールが Created (作成)、Modified (変更)、First Hit (最初にヒット)、Last Hit (最後にヒット) した日時が表示されます。
ポリシーアプリケーションの使用状況	

Panorama設定：Device > Setup > Management [デバイス > セットアップ > 管理]

ファイアウォール、または Panorama のテンプレートに以下の設定を定義します。これらの設定によって、ファイアウォールから Panorama への接続が確立されます。

Panorama の接続設定とオブジェクト共有設定も定義する必要があります。以下を参照してください。（Panorama Settings（Panorama 設定）：Panorama > Setup（セットアップ）> Management（管理））。

ファイアウォールは *Panorama* と認証を行う際、*AES256* により暗号化された *SSL* 接続を使用します。デフォルトでは、*Panorama* とファイアウォールは、事前定義済みの *2,048* ビット証明書を使用して互いに認証を行い、*SSL* 接続を使用して設定管理とログ収集を行います。*Panorama*、ファイアウォール、ログ コレクタ間の *SSL* 接続のセキュリティをさらに強化するには、「保護されたクライアント通信」を参照し、ファイアウォールと *Panorama* またはログ コレクタ間のカスタム証明書を設定してください。

Panorama サーバー	PanoramaサーバーのIPアドレスまたはFQDNを入力してください。Panoramaが高可用性（HA）設定に含まれている場合、2 番目の **Panorama Servers**[Panorama サーバー] フィールドにセカンダリPanoramaサーバーのIPアドレスまたはFQDNを入力します。
Panorama からデータを受信する際のタイムアウト	Panorama から TCP メッセージを受信する際のタイムアウトを入力します（秒単位）（範囲は 1 ~ 240、デフォルトは 240）。
Panorama へデータを送信する際のタイムアウト	Panorama に TCP メッセージを送信する際のタイムアウト（秒単位）を入力します（範囲は 1 ~ 240、デフォルトは 240）。
Panorama に SSL 送信を行う際の再試行カウント	Panorama に Secure Socket Layer（SSL）メッセージを送信する際の許容再試行回数を入力します（範囲は 1 ~ 64、デフォルトは 25）。
自動コミット復旧を有効にする	有効にすると、設定がコミットされてファイアウォールにプッシュされたときや、設定が正常にプッシュされた後に、設定された間隔で、ファイアウォールが Panorama管理サーバへの接続を自動的に検証することができます。 この機能を有効にすると、ファイアウォールが Panorama管理サーバへの接続を確認できない場合、ファイアウォールと Panorama 管理

© 2019 Palo Alto Networks, Inc.

項目	の意味
	は自動的にその設定を以前の実行中の設定に戻して接続を回復します。
Panorama 接続を確認するための試行回数	自動コミット復旧 を有効にすると、ファイアウォールが Panorama管理サーバへの接続をテストする回数を設定します。
再試行の間隔 (秒)	自動コミット回復 を有効にすると、ファイアウォールが Panorama管理サーバへの接続をテストする試行回数の間隔を秒単位で設定します。

保護されたクライアント通信	**Secure Client Communication**（保護されたクライアント通信）を有効にすると、ファイアウォールは（デフォルト証明書の代わりに）設定済みのカスタム証明書を使用して、Panorama またはログ コレクタへの SSL 接続を認証します。
	• **None**（なし）（デフォルト）– デバイス証明書は設定されず、デフォルトの事前定義済みの証明書が使用されます。
	• **Local**（ローカル）– ファイアウォールは、ファイアウォールで生成されたか既存のエンタープライズ PKI サーバーからインポートされたローカルのデバイス証明書および対応する秘密鍵を使用します。
	  • **Certificate**（証明書）– 生成またはインポートしたローカルデバイスの証明書を選択します。この証明書を、（ファイアウォールのシリアル番号のハッシュに基づく）ファイアウォール固有の証明書としたり、Panorama に接続するすべてのファイアウォールで使用する共通のデバイス証明書としたりできます。
	  • **Certificate Profile**（証明書プロファイル）– ドロップダウン リストから証明書プロファイルを選択します。証明書プロファイルは、クライアント証明書を検証するための CA 証明書と、証明書失効状態を確認する方法を定義します。
	• **SCEP** – ファイアウォールは、Simple Certificate Enrollment Protocol（SCEP）サーバーで生成されたデバイス証明書と秘密鍵を使用します。
	  • **SCEP Profile**（**SCEP** プロファイル）– ドロップダウン リストから SCEPProfile を選択します。SCEP プロファイルは、エンタープライズ PKI 内の SCEP サーバーに対してクライアントデバイスを認証するために必要な情報を Panorama に提供します。
	  • **Certificate Profile**（証明書プロファイル）– ドロップダウン リストから CertificateProfile を選択します。証明書プロファイルは、クライアント証明書を検証するための CA 証明書と、証明書失効状態を確認する方法を定義します。

	• **Customize Communication**（カスタマイズ通信）–ファイアウォールは、設定されたカスタム証明書を使用して、選択したデバイスを認証します。 • **Panorama Communication**（**Panorama** 通信）–ファイアウォールは設定されたクライアント証明書を使用して Panorama と通信します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **PAN-DB Communication**（**PAN-DB** 通信）–ファイアウォールは設定されたクライアント証明書を使用して PAN-DB アプライアンスと通信します。 • **WildFire Communication (WildFire** 通信**)**–ファイアウォールは設定されたクライアント証明書を使用して WildFire® アプライアンスと通信します。 • **Log Collector Communication**（ログ コレクタ 通信）–ファイアウォールは設定されたクライアント証明書を使用してログコレクタと通信します。 • **Check Server Identity (**サーバー アイデンティティのチェック**)**–(Panorama と ログ コレクタ通信 のみ) ファイアウォールは、共通名 (CN) をサーバーの IPアドレスまたは FQDN と照合し、サーバーのアイデンティティを確認します。
Panorama ポリシーとオブジェクトを無効/有効にする	このオプションはファイアウォールの**Panorama Settings** [Panorama設定] を編集する場合にのみ表示されます（Panoramaのテンプレートにはありません）。 **Disable Panorama Policy and Objects** [Panorama ポリシーとオブジェクトを無効にする] を選択すると、ファイアウォールに対するデバイスグループのポリシーとオブジェクトの適用が無効になります。デフォルトでは、この操作により、ファイアウォールから伝播されたポリシーとオブジェクトも削除されます。デバイスグループのポリシーとオブジェクトのローカルコピーをファイアウォールで保管する場合は、このオプションをクリックしたときに開くダイアログボックスの**Import Panorama Policy and Objects before disabling** [無効にする前に Panorama ポリシーとオブジェクトをインポート] を選択します。コミットを実行すると、これらのポリシーとオブジェクトはファイアウォール設定の一部となり、Panorama による管理の対象外となります。 通常の操作状況下では、Panorama 管理を無効にすることは不要であるうえに、ファイアウォールのメンテナンスと設定が複雑になりかねません。このオプションは通常、ファイアウォールでデバイス グループの定義とは異なるルールとオブジェクト値が必要な場合に適用されます。たとえば、テストのためにファイアウォールを本番環境からラボ環境に移動する場合などです。 ファイアウォールのポリシーおよびオブジェクト管理を Panorama に戻すには、**Enable Panorama Policy and Objects**[Panorama ポリシーとオブジェクトを有効にする] をクリックします。
デバイスとネットワーク テンプレートを無効/有効にする	このオプションはファイアウォールの**Panorama Settings** [Panorama設定] を編集する場合にのみ表示されます（Panoramaのテンプレートにはありません）。 ファイアウォールに対するテンプレート情報（デバイスとネットワーク設定）の適用が無効化する場合は、**Disable Device and Network Template** [デバイスとネットワークテンプレートを無効にする] を選択します。デフォルトでは、この操作により、ファイアウォールからテンプレート情報も削除されます。テンプレート情報のローカルコピーをファイアウォールで保管する場合は、ボタンをクリックしたときに開いたダイアログボックスの **Import Device and Network Templates before disabling** [無効にする前にデバイスとネッ

© 2019 Palo Alto Networks, Inc.

項目	の意味
	トワーク テンプレートをインポート] のオプションを選択します。コミットを実行すると、テンプレート情報はファイアウォール設定の一部となり、Panorama ではその情報が管理の対象外となります。 通常の操作状況下では、*Panorama* 管理を無効にすることは不要であるうえに、ファイアウォールのメンテナンスと設定が複雑になりかねません。このオプションは通常、ファイアウォールでテンプレートの定義とは異なるデバイスとネットワーク設定値が必要な場合に適用されます。たとえば、テストのためにファイアウォールを本番環境からラボ環境に移動する場合などです。 テンプレートを再度受け入れるようにファイアウォールを設定するには、**Enable Device and Network Templates**[デバイスとネットワーク テンプレートを有効にする] をクリックします。

Panorama設定：Panorama > Setup > Management [Panorama > セットアップ > 管理]

Panorama を使用してファイアウォールを管理する場合、Panorama で以下の設定を行います。これらの設定により、Panorama から管理対象ファイアウォールへの接続に関するタイムアウトおよび SSL メッセージ試行回数と、オブジェクト共有パラメータが決まります。

ファイアウォール、または Panorama のテンプレートにも Panorama 接続設定を定義する必要があります。Panorama Settings（Panorama 設定）：Device（デバイス）> Setup（セットアップ）> Management（管理）を参照してください。

ファイアウォールは *Panorama* と認証を行う際、*AES256* により暗号化された *SSL* 接続を使用します。デフォルトでは、*Panorama* とファイアウォールは、事前定義済みの *2,048* ビット証明書を使用して互いに認証を行い、*SSL* 接続を使用して設定管理とログ収集を行います。これらの *SSL* 接続のセキュリティをさらに強化するには、「Customize Secure Server Communication（保護されたサーバー通信のカスタマイズ）」を参照し、*Panorama* とそのクライアント間のカスタム証明書を設定してください。

デバイスへのデータ受信のタイムアウト	すべての管理対象ファイアウォールから TCP メッセージを受信するときのタイムアウト（秒単位）を入力します（範囲は 1 ~ 240、デフォルトは 240）。
デバイスへのデータ送信のタイムアウト	すべての管理対象ファイアウォールに TCP メッセージを送信するときのタイムアウト（秒単位）を入力します（範囲は 1 ~ 240、デフォルトは 240）。
デバイスに送信される SSL のカウントの再試行	管理対象ファイアウォールに Secure Socket Layer（SSL）メッセージを送信するときの許容再試行回数を入力します（範囲は 1 ~ 64、デフォルトは 25）。
未使用のアドレスとサービス オブジェクトをデバイスと共有	すべてのPanorama共有オブジェクトおよびデバイスグループ固有のオブジェクトを管理対象ファイアウォールで共有するには、このオプションを選択します（デフォルトで有効）。 このオプションを無効にすると、アプライアンスによって Panorama ポリシー内のアドレス、アドレスグループ、サービス、およびサービスグループオブジェクトへの参照がチェックされ、参照されない

© 2019 Palo Alto Networks, Inc.

項目	の意味
	オブジェクトは共有されません。このオプションにより、アプライアンスから管理対象ファイアウォールに必要なオブジェクトのみが送信されるようになり、オブジェクトの総数が削減されます。 デバイス グループ内の特定のデバイスを対象とするポリシー ルールがある場合、そのポリシーで使用されているオブジェクトは、そのデバイス グループで使用されていると見なされます。
上位で定義されたオブジェクトが優先されます	階層内の異なるレベルのデバイス グループに同じタイプと名前のオブジェクトがあり、それらの値が異なる場合、先祖（上位）グループのオブジェクト値が子孫（下位）グループのオブジェクト値よりも優先されることを指定するには、このオプションを選択します（デフォルトでは無効）。つまり、デバイス グループのコミットを実行すると、すべての値が先祖の値でオーバーライドされます。同様に、このオプションでは、共有オブジェクトの値が、デバイス グループ内にある同じタイプと名前のオブジェクトの値をオーバーライドします。 このオプションを選択すると、Find Overridden Objects（オーバーライドされたオブジェクトの検索）リンクが表示されます。
オーバーライドされたオブジェクトの検索	このオプション（Panorama 設定の下部）を選択すると、すべてのシャドー オブジェクトのリストが表示されます。シャドー オブジェクトは、Shared（共有）場所にあるオブジェクトで、デバイス グループ内に同じ名前の、値が異なるオブジェクトがあります。このリンクは、Objects defined in ancestors will take higher precedence（上位で定義されたオブジェクトが優先されます）を指定した場合にのみ表示されます。
グループでのレポートとフィルタリングの有効化	ファイアウォールから受け取ったユーザー名、ユーザー グループ名、およびユーザー名とグループ間のマッピング情報を Panorama でローカルに保存するには、このオプションを選択します（デフォルトでは無効）。このオプションは Panorama のすべてのデバイス グループにグローバルに適用されます。ただし、各デバイス グループのレベルでローカル ストレージを有効にする必要もあります。これを行うには、Master Device（マスター デバイス）を指定し、ファイアウォールをStore users and groups from Master Device（マスター デバイスからのユーザーとグループを保存する）に設定します。
安全な通信設定:Panorama > Setup > Management [Panorama > セットアップ > 管理]	
保護されたサーバー通信のカスタマイズ	• **Custom Certificate Only**（カスタム証明書のみ）– 有効にすると、Panorama は、管理対象のファイアウォールおよびログ コレクタとの認証用のカスタム証明書のみを受け付けます。 • **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）– ドロップダウン リストから SSL/TLS サービス プロファイルを選択します。このプロファイルは、Panorama との通信でファイアウォールが使用できる証明書およびサポートされる SSL/TLS バージョンを定義します。 • **Certificate Profile**（証明書プロファイル）– ドロップダウン リストから証明書プロファイルを選択します。この証明書プロファイルは、証明書失効チェックの動作と、クライアントから提供

© 2019 Palo Alto Networks, Inc.

項目	の意味

	された証明書チェーンの認証に使用できるルート CA を定義します。
	• **Authorization List**（承認リスト）—次のフィールドを使用して新しい承認プロファイルを **Add**（追加）および設定し、Panorama に接続できるクライアント デバイスの承認基準を設定します。Authorization List（承認リスト）は、最大 16 件のプロファイルのエントリをサポートします。
	  • **Identifier**（識別子）—Select **Subject**（サブジェクト）または **Subject Alt**（サブジェクト代替）を選択します。認証識別子としての**Name**（名前）を付けます。
	  • **Type**（タイプ）—**Subject Alt**（サブジェクト代替）の場合。**Name**（名前）が識別子である場合、識別子のタイプとして**IP**、 **hostname**（ホスト名）、または**e-mail**（電子メール）を選択します。**Subject**（サブジェクト）を選択した場合、**common name**（共通名）が識別子タイプになります。
	  • **Value**（値） — 識別子の値を入力します。
	• **Authorize Clients Based on Serial Number**（シリアル番号に基づいてクライアントを承認） —Panorama は、クライアント デバイスをデバイスのシリアル番号のハッシュに基づいて承認します。
	• **Check Authorization List**（承認リストのチェック）—Panorama はクライアント デバイスの ID を認証リストと照合して確認します。デバイスはリストの 1 基準のみと一致するだけで承認されます。一致がない場合、デバイスは承認されません。
	• **Disconnect Wait Time (min)**（切断待機時間（分）） — 管理対象デバイスとの現在の接続を終了するまで Panorama が待機する時間（分単位）。その後、Panorama は、設定済みの「保護されたサーバー通信」設定を使用して、管理対象デバイスとの接続を再度確立します。待機時間は、保護されたサーバー通信の設定がコミットされた後に開始されます。

保護されたクライアント通信	**Secure Client Communication**（保護されたクライアント通信）を使用すると、クライアント Panorama は（デフォルトで事前定義される証明書の代わりに）設定済みのカスタム証明書を使用して、HA ペアの Panorama アプライアンスまたは WildFire アプライアンスへの SSL 接続を認証します。
	• **Predefined**（事前定義済み）（デフォルト）—デバイス証明書は設定されず、デフォルトの事前定義済みの証明書が使用されます。
	• **Local**（ローカル） —Panorama は、ファイアウォールで生成されたか既存のエンタープライズ PKI サーバーからインポートされたローカルのデバイス証明書および対応する秘密鍵を使用します。
	  • **Certificate**（証明書） — ローカルのデバイス証明書を選択します。
	  • **Certificate Profile**（証明書プロファイル） — ドロップダウンリストから証明書プロファイルを選択します。
	• **SCEP** —Panorama は、Simple Certificate Enrollment Protocol（SCEP）サーバーで生成されたデバイス証明書と秘密鍵を使用します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **SCEP Profile**（**SCEP** プロファイル）– ドロップダウン リストから SCEP プロファイルを選択します。 • **Certificate Profile**（証明書プロファイル）– ドロップダウンリストから証明書プロファイルを選択します。 • **Customize Communication**（カスタマイズ通信） • **HA Communication**（**HA** 通信）–Panorama は HA ピアとの HA 通信に設定されたクライアント証明書を使用します。 • **WildFire Communication**（**WildFire** 通信）–Panorama は設定されたクライアント証明書を使用して WildFire アプライアンスと通信します。
ロギングおよびレポート設定 以下を変更するには、このセクションを使用します。 • レポートおよび以下のログ タイプの有効期間およびストレージ割り当て。設定は、高可用性ペア間で同期されます。 • ファイアウォールで生成され、ローカルに保管されているすべてのタイプのログ（「**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）」を参照）。設定は、ファイアウォールのすべての仮想システムに適用されます。 • Panorama モードの M-Series アプライアンスまたは Panorama 仮想アプライアンスがローカルに生成して保存するログ:システム、設定、アプリケーション統計、User-ID™ ログ（**Panorama** > **Setup**（セットアップ）> **Management**（管理）） • レガシー モードの Panorama バーチャル アプライアンスでローカルに生成されたまたはファイアウォールから収集されたすべてのタイプのログ（「**Panorama** > **Setup**（セットアップ）> **Management**（管理）」を参照）。 ファイアウォールから *Panorama* ログ コレクタに送信されるログについては、ストレージ割り当てと有効期間を各コレクタ グループで設定します（「Panorama > Collector Groups（コレクタ グループ）」を参照）。 • ユーザー アクティビティ レポートの計算およびエクスポートの属性 • ファイアウォールまたは Panorama で作成された事前定義済みレポート	
Log Storage (ログストレージ) タブ （Panorama 管理サーバー、および PA-5200 シリーズと PA-7000 シリーズのファイアウォールを除くすべてのファイアウォール モデル） *Logging and Reporting Settings*（ログとレポートの設定）を編集する場合（*Panorama* > *Setup*（セットアップ）> *Management*（管理））、*Panorama* はこのタブを表示し	ログ タイプごとに、次の設定を指定します。 • **Quota**（割り当て）– ハードディスク上に割り当てるログ ストレージの割り当て（パーセント）。**Quota**[割り当て] の値を変更すると、関連付けられたディスクの割り当てが自動的に変更されます。すべての値の合計が 100% を超える場合、メッセージが赤で表示され、設定を保存しようとする場合にエラー メッセージが表示されます。これが発生する場合、合計が 100% の上限を超えないようにパーセンテージを調整します。 *VM-Series* ファイアウォールはデフォルトで*SCTP* ログ ストレージ、*SCTP Summary*（*SCTP* サマリー）、*Hourly SCTP Summary*（*1* 時間ごとの *SCTP* サマリー）、*Daily SCTP Summary*（*1* 日ごとの *SCTP* サマリー）、*Weekly SCTP Summary*（*1* 週間ごとの*SCTP* サマリー）に *0%*の割り当てがあるため、これらのファイアウォールには *SCTP*

© 2019 Palo Alto Networks, Inc.

項目	の意味
ます。*Panorama* テンプレートを使用してファイアウォールの設定を行う場合は（「*Device*（デバイス）> *Setup*（セットアップ）> *Management*（管理））、「Single Disk Storage（シングル ディスク ストレージ）タブおよび Multi Disk Storage（マルチ ディスク ストレージ）タブ」を参照してください。	情報を記録するためのパーセントを割り当てる必要があります。 • **Max Days**（最大日数）– ログの有効期間（日数）（範囲は 1 ~ 2,000）。ファイアウォールまたは Panorama アプライアンスは、指定した期間を超えるログを自動的に削除します。デフォルトでは、有効期間はありません。つまり、ログを無期限に使用できます。 ファイアウォールまたは Panorama アプライアンスは、ログの作成中にログを検証し、有効期間または割り当てサイズを超えているログを削除します。 週次サマリー ログは、ファイアウォールがログを削除する各タイミングの間に有効期限のしきい値に達すると、次の削除の前にしきい値を超える可能性があります。ログ割り当てが最大サイズに達した場合、新しいログエントリは最も古いログエントリを上書きして作成されます。ログ割り当てサイズを小さくする場合、ファイアウォールまたは*Panorama*はその変更をコミットした際に最も古いログを削除します。*HA* アクティブ/パッシブ設定の場合、パッシブ ピアはログを受信しないため、フェイルオーバーが発生してアクティブになるまでログを削除しません。

	• **Core Files**（コア ファイル）– ファイアウォールでシステム プロセスの障害が発生した場合、プロセスの詳細と障害の原因が含まれるコア ファイルが生成されます。コアファイルが大きすぎてデフォルトのコア ファイル保存場所（`/var/cores` パーティション）に入らない場合、**`large-core`** ファイル オプションを有効にして、代替のより大きな保存場所（`/opt/panlogs/cores`）を割り当てることができます。Palo Alto Networks サポートエンジニアは、割り当てられたストレージを必要に応じて増やすことができます。
	`large-core` ファイル オプションを有効または無効にするには、設定モードから次の CLI コマンドを入力した後、設定を コミット します。
	`# set deviceconfig setting management large-core [yes|no]`
	このオプションを無効にすると、コア ファイルは削除されます。
	コア ファイルをエクスポートするには、操作モードから SCP を使用する必要があります。
	`> scp export core-file large-corefile`

© 2019 Palo Alto Networks, Inc.

項目	の意味
	Palo Alto Networks サポート エンジニアのみがコアファイルのコンテンツを解釈できます。 • **Restore Defaults** (デフォルトを復元) – デフォルト値に戻すには、このオプションを選択します。
Session Log Storage (セッション ログ ストレージ) タブおよび **Management Log Storage** (管理ログ ストレージ) タブ (PA-5200 シリーズおよび PA-7000 シリーズのファイアウォールのみ)	PA-5200 シリーズと PA-7000 シリーズのファイアウォールは、管理ログとセッションログを別々のディスクに保存します。ログのセットごとにタブを選択し、Log Storage (ログ保存エリア) タブで説明されている設定を指定します。 • **Session Log Storage** (セッション ログ ストレージ)– **Session Log Quota** (セッション ログ割り当て)を選択し、トラフィック、脅威、URL フィルタリング、HIPマッチ、User-ID、GTP/トンネル、SCTP、認証、および GlobalProtect のログのほか、拡張脅威の PCAP に対して割り当てと有効期間を設定します。 • **Management Log Storage** (管理ログ ストレージ) – システム、設定、およびアプリケーション統計のログのほか、HIP レポート、データ フィルタリング キャプチャ、アプリケーション PCAP、およびデバッグ フィルタ PCAP に対して割り当てと有効期間を設定します。
Single Disk Storage (シングル ディスク ストレージ) タブおよび **Multi Disk Storage** (マルチ ディスク ストレージ) タブ (Panorama テンプレートのみ)	Panorama テンプレートを使用してログ割り当てと有効期間を設定する場合、テンプレートに割り当てられたファイアウォールに基づいて、次のタブの 1 つ、または両方の設定を指定します。 • **PA-5200** シリーズと **PA-7000** シリーズのファイアウォール – **Multi Disk Storage** (マルチ ディスク ストレージ) を選択し、Session Log Storage (セッション ログ ストレージ) タブおよび Management Log Storage (管理ログ ストレージ) タブの設定を指定します。 *PA-5200 Series* ファイアウォールはデフォルトで*SCTP* ログ ストレージ、*SCTP Summary* (*SCTP* サマリー)、*Hourly SCTP Summary* (*1* 時間ごとの *SCTP* サマリー)、*Daily SCTP Summary* (*1* 日ごとの *SCTP* サマリー)、*Weekly SCTP Summary* (*1* 週間ごとの*SCTP* サマリー) に *0%*の割り当てがあるため、これらのファイアウォールには *SCTP* 情報を記録するためのパーセントを割り当てる必要があります。 • その他のファイアウォール モデル – **Single Disk Storage** (シングル ディスク ストレージ) を選択し、**Session Log Quota** (セッション ログ割り当て) を選択して、Log Storage (ログ保存エリア) タブの設定を指定します。
Log Export and Reporting (ログのエクスポートとレポート) タブ	必要に応じて、ログのエクスポートとレポートに関する次の設定を指定します。 • **Number of Versions for Config Audit**[設定監査のバージョン数] – 保存可能な設定監査のバージョン数を入力します (デフォルトは 100)。この数を超えると最も古いバージョンが廃棄されます。保

© 2019 Palo Alto Networks, Inc.

項目	の意味
	存されたバージョンを使用して、設定の変更の監査と比較を行うことができます。 • **Number of Versions for Config Backups** (設定バックアップのバージョン数) – (Panorama のみ) 保存可能な設定バックアップ数を入力します (デフォルトは 100)。この数を超えると最も古い設定バックアップが廃棄されます。 • **Max Rows in CSV Export** (**CSV** エクスポートの最大行数) – トラフィック ログ ビューの **Export to CSV** (**CSV**にエクスポート) で生成される CSV レポートに表示される行の最大数を入力します (範囲は 1 ~ 1,048,576、デフォルトは 65,535)。 • **Max Rows in User Activity Report** (ユーザー アクティビティ レポートの最大行数) – 詳細なユーザー アクティビティ レポートでサポートされる最大行数を入力します (範囲は 1 ~ 1,048,576、デフォルトは 5,000)。
Log Export and Reporting (ログのエクスポートとレポート) タブ (続き)	• **Average Browse Time (sec)** (平均ブラウズ時間 (秒)) – Monitor (監視) > PDF Reports (PDF レポート) > User Activity Report (ユーザー アクティビティ レポート) のブラウズ時間 (秒単位) の計算方法を調整するには、この変数を設定します (範囲は 0 ~ 300、デフォルトは 60)。 計算対象としては、Web 広告やコンテンツ配信ネットワークとして分類されたサイトは無視されます。ブラウズ時間の計算は、URL フィルタリング ログに記録されたコンテナ ページに基づきます。計算に含めるべきではない外部サイトからコンテンツをロードするサイトが多くあるため、コンテナ ページがこの計算の基準として使用されます。コンテナ ページの詳細は、 コンテナ ページを参照してください。平均ブラウズ時間の設定は、管理者が想定するユーザーが Web ページを閲覧する平均時間です。平均ブラウズ時間が経過した後に行われたリクエストは、新しいブラウズ アクティビティと見なされます。計算対象からは、最初のリクエスト時間 (開始時間) から平均ブラウズ時間までの間にロードされる新しい Web ページは無視されます。この動作は、任意の Web ページ内にロードされる外部サイトを除外するために設計されています。例:平均ブラウズ時間が2分に設定されている場合は、ユーザーがWebページを開き、そのページを5分間閲覧しても、そのページのブラウズ時間は2分になります。ユーザーがあるページを閲覧する時間を判断する方法がないため、このような動作が設定されています。 • **Page Load Threshold** (ページ ロードしきい値) (秒)– ページ要素がページにロードされるまでの推定時間を調整できます (秒単位) (範囲は 0 ~ 60、デフォルトは 20)。最初のページのロードからページ ロードしきい値までの間に発生するリクエストは、ページの要素と見なされます。ページ ロードしきい値の範囲外で発生するリクエストは、ページ内のリンクをユーザーがクリックしたものと見なされます。ページ ロードしきい値は、Monitor (監視) > PDF Reports (PDF レポート) > User Activity Report (ユーザー アクティビティ レポート) の計算にも使用されます。 • **Syslog HOSTNAME Format** (**Syslog HOSTNAME** 形式) – syslog メッセージ ヘッダーで FQDN、ホスト名、または IP アドレス (IPv4 または IPv6) を使用するかどうかを選択します。この

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ヘッダーは、メッセージの送信元のファイアウォールまたは Panorama 管理サーバーを識別します。 • **Report Runtime**（レポートの実行時間）– ファイアウォールまたは Panorama アプライアンスで毎日の定期的なレポートの生成を開始する時刻（デフォルトは 2 a.m.）を選択します。 • **Report Expiration Period**（レポートの有効期間）– レポートの有効期間（日単位）を設定します（範囲は 1 ~ 2,000）。デフォルトでは、有効期間はありません。つまり、レポートを無期限に使用できます。ファイアウォールまたは Panorama アプライアンスは、システム時間に基づき、有効期限を過ぎたレポートを毎晩午前 2 時に削除します。
	• **Stop Traffic when LogDb full**（**LogDb** 容量超過時トラフィック転送を停止）–（ファイアウォールのみ、デフォルトでは無効）ログデータベースに空きがない場合にファイアウォール経由のトラフィックを停止する場合は、このオプションを選択します。 • **Enable Threat Vault Access**（**Threat Vault** アクセスの有効化）–（デフォルトでは有効）ファイアウォールは Threat Vault にアクセスし、検出された脅威に関する最新情報を収集できます。この情報は、脅威ログと、ACC に示された上位の脅威アクティビティで利用できます。 • **Enable Log on High DP Load**（**DP** 高負荷時にログを有効にする）–（ファイアウォールのみ、デフォルトでは無効）ファイアウォールのパケット処理の負荷により CPU 使用率が100%に達した場合にシステム ログ エントリを生成することを指定するには、このオプションを選択します。 *Enable Log on High DP Load (DP* 負荷が大きい際にログを有効化*)*すれば、管理者が調査を行って *CPU* 使用率が高くなっている原因を特定できるようになります。 高い *CPU* 負荷により、*CPU* がすべてのパケットを処理するのに十分なサイクルを確保できないため、動作が遅くなる可能性があります。システム ログでこの問題のアラートが通知 *(*ログ エントリが毎分生成*)* されるため、問題の原因を調査できます。 • **Enable High Speed Log Forwarding**（高速ログ転送の有効化）（PA-5200 シリーズおよび PA-7000 シリーズのファイアウォールのみ、デフォルトでは無効）–ログを Panorama に最高 120,000 ログ/秒の割合で転送する場合は、ベスト プラクティスとして、このオプションを選択することをお勧めします。無効にすると、ファイアウォールはログを Panorama に単に最高 80,000 ログ/秒の割合で転送します。 このオプションを有効にした場合、ファイアウォールはログをローカルに保存しません。つまり、ログは **Dashboard**（ダッシュボード）、**ACC**、または **Monitor**（監視）タブに表示されません。また、このオプションを使用するには、Panorama へのログ転送を設定する必要があります。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **Log Collector Status** (ログコレクタのステータス)–ファイアウォールが分散ログ収集アーキテクチャへの接続を成功させ、そこにログを送信しているかどうかを示すステータスを表示します。ファイアウォールがログをロギング サービスにも送信するように設定されている場合は、**Logging Service Status** (ロギング サービスのステータス)を検証します。（ロギング サービス セクション内）。
（Panorama のみ）	• **Buffered Log Forwarding from Device**（デバイスから転送するログのバッファ）–（デフォルトでは有効）Panorama への接続が失われた場合にファイアウォールでそのハード ディスク（ローカル ストレージ）にログ エントリをバッファすることを許可します。Panorama との接続が復元したときに、ファイアウォールはログ エントリを Panorama に転送します。バッファに使用できるディスク領域は、そのファイアウォール モデルのログ ストレージの割り当て、およびロール オーバーを保留しているログの量によって異なります。使用可能な領域がなくなると、新しいイベントをロギングできるように最も古いエントリが削除されます。 *Panorama* への接続がダウンした場合にログが損失するのを防ぐために、*Buffered Log Forwarding from Device* (バッファによるデバイスからのログ転送)を有効化します。 • **Get Only New Logs on Convert to Primary**（プライマリへの変換時に新しいログのみを取得）（デフォルトでは無効）–このオプションは、ログをネットワーク ファイル システム（NFS）に書き込む、レガシーモードの Panorama バーチャル アプライアンスにのみ適用されます。NFS ロギングでは、プライマリ Panorama が NFS にマウントされます。そのため、ファイアウォールはアクティブなプライマリ Panorama のみにログを送信します。このオプションでは、HA フェイルオーバーが発生してセカンダリ Panorama が（プライマリに昇格した後に）NFS へのロギングを再開した場合、新しく生成されたログのみをファイアウォールから Panorama に送信するように設定できます。このオプションを有効にするのは、通常、Panorama への接続が復元されるまで長時間かかったときに、ファイアウォールが大量のバッファ済みログを送信しないようにするためです。 • **Only Active Primary Logs to Local Disk**（アクティブなプライマリログのみをローカル ディスクに保存）（デフォルトでは無効）–このオプションは、レガシーモードの Panorama バーチャル アプライアンスにのみ適用されます。このオプションでは、アクティブな Panorama のみがローカル ディスクにログを保存するように設定できます。
	Pre-Defined Reports（事前定義済みレポート）（デフォルトで有効）– アプリケーション、トラフィック、脅威、URL フィルタリング、ストリーム制御伝送プロトコル（SCTP）の事前定義済みレポートは、ファイアウォールと Panorama で使用できます。SCTP の事前定義済みのレポートは、SCTP セキュリティが **Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **General**

© 2019 Palo Alto Networks, Inc.

項目	の意味
	Settings（一般設定）で有効になった後にファイアウォールとPanorama で使用可能になります。 ファイアウォールは、1時間ごとの結果の生成（および表示用にその結果が集約およびコンパイルされるPanoramaへの送信）にメモリリソースを使用するため、メモリ使用量が減るように、重要ではないレポートを無効にできます。レポートを無効にする場合は、そのレポートのオプションをオフにします。 事前定義済みレポートの生成を全体的に有効または無効にするには、**Select All**（すべて選択）または **Deselect All**（すべての選択を解除）をクリックします。 レポートを無効にする前に、そのレポートがグループ レポートや *PDF* レポートで使用されていないことを確認してください。レポートセットに割り当てられている事前定義済みレポートを無効にした場合、そのレポートセット全体でデータが表示されなくなります。

バナーとメッセージ

Message of the Day（本日のメッセージ）ダイアログですべてのメッセージを表示するには、「本日のメッセージ」を参照してください。

本日のメッセージを設定して *OK* をクリックすると、その後ログインする管理者や、画面の更新を行ったアクティブな管理者に対し、新しいメッセージやアップデートされたメッセージが即座に表示されるようになります（コミットする必要はありません）。これにより他の管理者に対し、間もなく実行予定のコミットを実行前に通知することができます。

当日のメッセージ （チェック ボックス）	管理者が Web インターフェイスへログインする時に「本日のメッセージ」ダイアログを表示させる場合はこのオプションを選択してください。
当日のメッセージ （テキスト入力フィールド）	「本日のメッセージ」ダイアログ用のテキスト（最大3,200文字）を入力してください。
今後は表示しないオプションの有効化	「本日のメッセージ」ダイアログに**Do not show again**（今後は表示しない）オプションを含める場合はこちらを選択してください（デフォルトでは無効）。このオプションを使用すると、以降のログインで管理者に同じメッセージが表示されなくなります。 *Message of the Day [本日のメッセージ]* のテキストを編集した場合、*Do not show again [今後は表示しない]* を選択した管理者にもそのメッセージが表示されます。変更したメッセージを以降のセッションで表示したくない場合、メッセージが再度変更されない限り、管理者はこのオプションを再度選択する必要があります。

© 2019 Palo Alto Networks, Inc.

項目	の意味
役職	「本日のメッセージ」のヘッダーを入力します（デフォルトは`Message of the Day`です）。
背景の色	「本日のメッセージ」ダイアログ用の背景色を選択してください。デフォルト（**None** [なし]）は薄いグレーの背景です。
Icon（アイコン）	「本日のメッセージ」のテキストの上に表示する、事前設定済のアイコンを選択します。 • **None**[なし]（デフォルト） • **Error**（エラー） • **Help**（ヘルプ） • **Information**（情報） • **Warning**（警告）
ヘッダーバナー	ヘッダーバナーに表示するテキストを入力してください（最大3,200文字）。
ヘッダーの色	ヘッダーの背景色を選択します。デフォルト（**None** [なし]）は透明な背景です。
ヘッダーの文字色	ヘッダーテキストの文字色を選択します。デフォルト（**None** [なし]）は黒です。
ヘッダーとフッターに同じバナーを使用する	フッターバナーにヘッダーバナーと同じテキストと配色を割り当てたい場合はこのオプションを選択してください（デフォルトでは有効）。このオプションを有効化すると、フッターバナー用のテキスト入力欄と色のフィールドはグレー表示になります。
フッターバナー	フッターバナーに表示するテキストを入力してください（最大3,200文字）。
フッターの色	フッターの背景色を選択します。デフォルト（**None** [なし]）は透明な背景です。
フッターの文字色	フッターテキストの文字色を選択します。デフォルト（**None** [なし]）は黒です。
パスワード複雑性設定	
enabled [有効化]	ローカル アカウントのパスワードの最小要件を有効にします。この機能を使用すると、定義されたパスワード要件が、ファイアウォールのローカル管理者アカウントで確実に順守されます。 これらのオプションのサブセットを使用したパスワード プロファイルを作成し、設定をオーバーライドしたり、特定のアカウントに適用したりすることもできます。詳細は、「Device（デバイス）> Password Profiles（パスワード プロファイル）」を参照してください。アカウントで使用できる有効な文字の詳細は、「ユーザー名とパスワードの要件」を参照してください。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	パスワードの最大文字数は*31*文字です。*PAN-OS*が許容していない要件を設定しないようにしてください。たとえば、大文字 *10* 個、小文字 *10* 個、数字 *10* 個、特殊文字 *10* 個の要件は、最大文字数の *31* を超えるため、設定しないでください。 高可用性（HA）を設定してある場合は、パスワード複雑性のオプションを設定するときに必ずプライマリ ピアを使用し、変更を加えた後にすぐにコミットしてください。 指定した **Password Hash**（パスワード ハッシュ）の対象のローカル データベース アカウントにパスワード複雑性設定は適用されません（「Device > Local User Database > Users」を参照）。 強固なパスワードを必須にして、ブルートフォースによるネットワーク アクセス攻撃が成功するのを防ぎます。最低文字数を設定し、大文字、小文字、数字、特殊文字をそれぞれ *1* 文字以上求めます。さらに、パスワードで同じ文字を過剰に繰り返したりユーザー名を使用したりするのを防ぎ、パスワードを再利用する頻度を制限し、定期的なパスワードの変更期間を設定することでパスワードを長期間使用し続けられないようにします。パスワード要件が厳格であれば、攻撃者がパスワードをハッキングすることが難しくなります。パスワードの強度を高めるために、必ずパスワード強度のベスト プラクティスに従ってください。
最小文字数	最少のパスワード長を要求します（範囲は 1 ~ 15 文字）。
最少大文字数	最少の大文字数を要求します（範囲は 0 ~ 15 文字）。
最少小文字数	最少の小文字数を要求します（範囲は 0 ~ 15 文字）。
最少数字数	最少の数字の文字数を要求します（範囲は 0 ~ 15 文字）。
最少特殊文字数	最少の特殊文字数（アルファベット以外）を要求します（範囲は 0 ~ 15 文字）。
繰り返し文字のブロック	パスワードで許容される連続重複文字数を指定します（範囲は 2 ~ 15 文字）。 値を 2 に設定すると、パスワードに 2 回連続する同じ文字を含めることはできますが、同じ文字が連続して 3 回以上使用されるパスワードは許可されません。 たとえば、値を「2」に設定する場合、「test11」や「11test11」というパスワードは受け入れられますが、「test111」は数値の「1」が 3 回連続しているため受け入れられません。
ユーザー名を含むパスワードを禁止(逆順を含む)	アカウントユーザー名（またはそれを逆読みにしたもの）をパスワードに使用できないようにする場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
文字が異なる新規パスワード	管理者が自分のパスワードを変更するときに、文字は指定した値によって異なる必要があります。
初回ログイン時にパスワードの変更を要求	管理者がファイアウォールに初めてログインする際にパスワードの変更を求めるプロンプトを表示するには、このオプションを選択します。
パスワードの再使用禁止制限	指定した数に基づいて、以前のパスワードを再使用しないように要求します。たとえば、値を「4」に設定すると、直近の 4 つのパスワードを再使用することができなくなります（範囲は 0 ~ 50）。
パスワード変更期間のブロック（日）	指定した日数が経過するまで、ユーザーはパスワードを変更できません（範囲は 0 ~ 365 日）。
パスワード有効期限（日数）	管理者は、日数（範囲は 0 ~ 365 日）で定期的にパスワードを変更する必要があります。たとえば、値を「90」に設定すると、管理者に 90 日ごとにパスワードの変更を求めるプロンプトが表示されます。 失効の警告を 0 ~ 30 日の範囲で設定して猶予期間を指定することもできます。
失効の警告期間（日数）	**Required Password Change Period**（パスワード有効期限）が設定されている場合は、ユーザーに対してこの**Expiration Warning Period**（失効の警告期間）を使用することで、必要な変更日前に指定された日数（0〜30 の範囲）が残っていない場合に、各ログイン時にパスワードを変更するようプロンプトを表示させることができます。
失効後の管理者ログイン回数（カウント）	必要な変更日の後に、管理者が指定した回数ログインできるようにします（範囲は 0〜3）。たとえば、この値を 3 に設定してアカウントの有効期限が切れた場合、アカウントがロックアウトされる前にパスワードを変更せずに 3 回以上ログインできます。
失効後の猶予期間 (日数)	アカウントが失効しても、管理者はここで指定した期間（日数）はログインできます（範囲は 0 ~ 30 日）。
AutoFocus™	
enabled [有効化]	ファイアウォールとAutoFocusポータルの接続を有効化することで、脅威インテリジェンスデータの取得や、ファイアウォールとAutoFocusを統合的に検索することが可能になります。 AutoFocus に接続されると、ファイアウォールにはトラフィック、脅威、URL フィルタリング、WildFire への送信、およびデータフィルタリングのログエントリに関する AutoFocus データが表示されるようになります（**Monitor**（監視）> **Logs**（ログ））。これらのタイプのログエントリ（IPアドレスやURLなど）から分析結果をクリックし、それに対するAutoFocus調査結果と統計のサマリーを表示することができます。さらにその分析結果に対し、ファイアウォールから直接、拡張AutoFocus検索を行うことができます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ファイアウォールで *AutoFocus* ライセンスが有効かどうか確認してください（*Device*（デバイス）> *Licenses*（ライセンス））。*AutoFocus*ライセンスが表示されない場合、*License Management [*ライセンス管理*]* にあるいずれかのオプションを使用してライセンスをアクティベートしてください。
AutoFocus URL	AutoFocus URLを入力します。 **`https://autofocus.paloaltonetworks.com:10443`**
クエリタイムアウト（秒数）	ファイアウォールが AutoFocus に対し脅威インテリジェンスデータのクエリを行う際の試行継続時間（秒単位）を設定します。AutoFocusポータルが指定した時間内に応答しない場合、ファイアウォールは接続を切断します。

Logging Service

このセクションを使用して、Cortex Data Lake にログを転送するように VM-Series とハードウェアベースのファイアウォールを設定します。以下に説明するオプションを設定するための完全なワークフローは次のとおりです。

- Cortex Data Lake へのLogging (ログ) の開始 (Panorama なし)
- Cortex Data Lake へのLogging (ログ) の開始 (Panorama マネージドファイアウォール用)

*Logging Service (*ログ サービス*)* の名前は、*Cortex Data Lake* に変更されました。ただし、一部のファイアウォール機能とボタンでは、引き続き*Logging Service (*ログ サービス*)* と表示されます。

Logging Service を有効にする	このオプションを選択すると、ファイアウォール (または、Panorama を使用している場合は、選択した **Template (**テンプレート**)**に属するファイアウォール) がログを Cortex Data Lake に転送できるようになります (以前、Cortex Data Lake は Logging Service という名前でした)。 Log Forwarding (ログ転送) を設定する (Objects (オブジェクト) > Log Forwarding (ログ転送)) と、ファイアウォールはログを直接 Cortex Data Lake に転送します。これは、Panorama マネージドファイアウォールの場合でも同じです。
Enable Duplicate Logging (重複ログを有効にする) (Panorama マネージドファイアウォールのみ)	**Enable Duplicate Logging (**重複ログを有効にする**)** により、Cortex Data Lake へのログの送信に加えて、Panorama および分散 Log Collectors (ログ コレクター) へのログの送信が続行されます。 このオプションにより、Cortex Data Lake を評価することができます—有効にすると、選択したテンプレートに属するファイアウォールは、ログのコピーを Cortex Data Lake と Panorama または 分散ログ収集 アーキテクチャの両方に保存します。
Enable Enhanced Application Logging（高度なアプリケーション ロギングの有効化）	**Enable Enhanced Application Logging**（高度なアプリケーション ロギングの有効化）は、ファイアウォールが Palo Alto Networks アプリケーションのネットワーク可視性を高めるデータを収集する場合に実行します。例えば、ネットワークの可視性が向上すると、Palo Alto Networks Cortex XDR アプリは通常のネットワーク アクティビ

© 2019 Palo Alto Networks, Inc.

項目	の意味
	ティのベースラインをより細かく分類して確立し、ファイアウォールが攻撃を示す可能性のある異常な動作を検出できるようになります。 Enhanced Application Logging (高度なアプリケーション ロギング) には、Logging Service (Cortex Data Lake) ライセンスが必要です。ユーザーはこれらのログは閲覧できません。Palo Alto Networks アプリケーションでのみ使用されるように設計されています。
領域	ファイアウォールがログを転送する Cortex Data Lake (Logging Service) インスタンスの地理的リージョンを選択します。Cortex ハブ にログインして、Cortex Data Lake インスタンスが展開されているリージョンを確認します (ハブで、トップ メニュー バーの設定ギアを選択し、 **Manage Apps** (アプリの管理)をクリックします)。
PA-7000 番台および PA-5200 番台のロギング サービスへの接続数	(PA-7000 シリーズ および PA-5200 シリーズ のファイアウォール) ファイアウォールから Cortex Data Lake にログを送信するための接続数を指定します(範囲は 1 ~ 20、デフォルトは 5)。ファイアウォール上で **`request logging-service-forwarding status`** の CLI コマンドを使用し、ファイアウォールおよび Cortex Data Lake 間のアクティブな接続数を確認できます。
Panorama なしのオンボード (Panorama が管理していないファイアウォール用)	Panorama が管理していないファイアウォールに対して、Cortex Data Lake へのログの記録を有効にすることができます。これを行うには、最初に Cortex Data Lake アプリでキーを生成する必要があります。このキーにより、ファイアウォールは Cortex Data Lake を認証して安全に接続できます。キーを生成したら、ここに入力します。次に、ファイアウォールを有効にして、Cortex Data Lake へのログの転送を開始します。
ロギング サービスのステータス	Cortex Data Lake への接続のステータスを表示します。**Show Status** (ステータスを表示)して次のチェックの詳細を表示します： • **License** (ライセンス)—`OK` または `Error` （エラー）であり、ファイアウォールがログを Cortex Data Lake に転送するための有効なライセンスを持っているかどうかを示します。 • **Certificate** (証明書)—`OK` または `Error` （エラー）であり、ファイアウォールが Cortex Data Lake に認証するために必要となる証明書を正常に取得したかどうかを示します。 • **Customer Info** (顧客情報)—`OK` または `Error` （エラー）であり、ファイアウォールが Cortex Data Lake を使用するために必要となる顧客 ID 番号を持っているかどうかを示します。ステータスが`OK`である場合は顧客 ID 番号も表示されます。 • **Device Connectivity** (デバイスの接続性)—ファイアウォールが正常に Cortex Data Lake に接続されたかどうかを示します。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Operations [デバイス > セットアップ > 操作]

以下のタスクを行うことで、Panorama™ およびファイアウォールで実行中の設定と候補設定を管理することができます。Panorama™仮想アプライアンスを使用している場合、このページの設定を使用して、レガシー モードの Panorama仮想アプライアンスのログ ストレージ パーティションを設定することもできます。

候補設定に加えた変更を有効化する場合はその変更をコミットする必要があります。この時点で、変更内容は実行中の設定の一部になります。ベスト プラクティスとして、定期的に候補設定を保存することをお勧めします。

設定ファイル、ログ、レポート、およびその他のファイルを *SCP* サーバーにエクスポートし、それらのファイルを他のファイアウォールや *Panorama M-Series* または仮想アプライアンスにインポートする場合は CLI で Secure Copy (SCP) コマンドを使用することができます。ただし、以下のモデルでは、ログ データベースはエクスポートやインポートを行うには大きすぎるので、ログ データベース全体のエクスポートやインポートはサポートされていません。*PA-7000 Series*ファイアウォール (すべての *PAN-OS®* リリース)、*Panorama 6.0* 以降を実行している *Panorama* 仮想アプライアンス、および *Panorama M-Series* アプライアンス (すべての *Panorama* リリース)。

機能	の意味
設定の管理	
最後に保存された設定に戻します	候補設定のデフォルトのスナップショット (.snapshot.xml) (Web インターフェイスの右上にある**Config** (設定) > **Save Changes** (変更の保存) を選択して作成または上書きするスナップショット) を復元します。 (Panorama のみ) **Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、元に戻す特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
実行中の設定に戻す	現在の実行中の設定が復元されます。この操作によって、前回のコミット以降に候補設定に対してすべての管理者が加えたすべての変更が取り消されます。特定の管理者の変更のみを元に戻すには、「変更を元に戻す」を参照してください。 (Panorama のみ) **Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、元に戻す特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
名前付き設定スナップショットの保存	デフォルトのスナップショット (.snapshot.xml) を上書きしない、候補設定のスナップショットを作成します。スナップショットの **Name** (名前) を入力するか、上書きする既存の名前付きスナップショットを選択します。

© 2019 Palo Alto Networks, Inc.

機能	の意味
	（Panorama のみ）**Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、保存する特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
候補設定の保存	現在の候補設定で候補設定のデフォルトスナップショット（.snapshot.xml）を作成または上書きします。これは、Web インターフェイスの右上にある **Config**（設定）> **Save Changes**（変更の保存）を選択した場合の動作と同じです。特定の管理者の変更のみを保存するには、「候補設定の保存」を参照してください。 （Panorama のみ）**Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、保存する特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
名前付きの設定スナップショットのロード（ファイアウォール） あるいは 名前付きの Panorama 設定スナップショットのロード	現在の候補設定を以下のいずれかで上書きします。 • 名前を付けた候補設定のスナップショット（デフォルトのスナップショットではなく）。 • インポートして名前を付けた実行中の設定。 • 現在実行中の設定。 設定はそのロード先のファイアウォールまたは Panorama に存在する必要があります。 設定の **Name**（名前）を選択し、**Decryption Key**（復号化キー）を入力します。このキーはファイアウォールまたは Panorama のマスター キーです（「Device > Master Key and Diagnostics」を参照）。設定内のすべてのパスワードと秘密鍵を復号化するには、このマスター キーが必要です。インポートした設定をロードする場合、インポート元のファイアウォールまたは Panorama のマスター キーを入力する必要があります。ロード操作が終了すると、設定のロード先のファイアウォールまたは Panorama のマスター キーでパスワードと秘密鍵が再度暗号化されます。 設定に含まれるすべてのルール用に新しい UUID を生成する場合（例えば、設定を別のファイアウォールから読み込むものの、設定を読み込む際に固有のルールを維持したい場合）、スーパーユーザーが**Regenerate Rule UUIDs for selected named configuration** (選択した名前付き設定の ルール **UUID** を再生成)し、すべてのルールに対して新しい UUID を生成する必要があります。 （Panorama のみ）オブジェクト、ポリシー、デバイスグループあるいはテンプレート、あるいはテンプレート設定を指定し、次の項目を選択することで名前付き設定から部分的に設定を読み込みます： • **Load Shared Objects** (共有オブジェクトの読み込み)–すべてのデバイスグループおよびテンプレート設定と共に共有オブジェクトだけを読み込みます。 • **Load Shared Policies** (共有ポリシーの読み込み)–すべてのデバイスグループおよびテンプレート設定と共に共有ポリシーだけを読み込みます。

© 2019 Palo Alto Networks, Inc.

機能	の意味
	• **Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)—読み込むデバイスグループ、テンプレート、あるいはテンプレート スタック設定を指定します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます • **Retain Rule UUIDs** (ルールの **UUID** を保持)—現在アクティブな設定の UUID を保持します。
設定バージョンのロード（ファイアウォール） あるいは Panorama 設定バージョンのロード	ファイアウォールまたは Panorama に保存されている現在実行中の設定の以前のバージョンで現在の候補設定を上書きします。 設定の **Name**（名前）を選択し、**Decryption Key**（復号化キー）を入力します。このキーはファイアウォールまたは Panorama のマスター キーです（「Device > Master Key and Diagnostics」を参照）。設定内のすべてのパスワードと秘密鍵を復号化するには、このマスター キーが必要です。ロード操作が終了すると、マスター キーでパスワードと秘密鍵が再度暗号化されます。 （Panorama のみ）オブジェクト、ポリシー、デバイスグループあるいはテンプレート、あるいはテンプレート設定を指定し、次を選択することで名前付き設定から部分的に設定を読み込みます： • **Load Shared Objects** (共有オブジェクトの読み込み)—すべてのデバイスグループおよびテンプレート設定と共に共有オブジェクトだけを読み込みます。 • **Load Shared Policies** (共有ポリシーの読み込み)—すべてのデバイスグループおよびテンプレート設定と共に共有ポリシーだけを読み込みます。 • **Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)—読み込むデバイスグループ、テンプレート、あるいはテンプレート スタック設定を指定します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます
名前付き設定スナップショットのエクスポート	現在実行中の設定、候補設定のスナップショット、または前回インポートした設定（候補または実行中の設定）をエクスポートします。ファイアウォールは、設定済みの名前が付与されたXMLファイルとして設定をエクスポートします。スナップショットはネットワーク上の任意の場所に保存することができます。 （Panorama のみ）**Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、エクスポートする特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスドメイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
設定バージョンのエクスポート	実行中の**Version**[バージョン] の設定をXMLファイルとしてエクスポートします。 （Panorama のみ）**Select Device Groups & Templates** (デバイスグループおよびテンプレートを選択)を使用し、エクスポートする特定のデバイスグループ、テンプレート、あるいはテンプレート スタック設定を選択します。デバイスグループおよびテンプレート管理者は、自身に割り当てられたアクセスド

© 2019 Palo Alto Networks, Inc.

機能	の意味
	メイン用のデバイスグループ、テンプレート、あるいはテンプレート スタックだけを選択できます。
Panorama およびデバイスの設定バンドルのエクスポート （Panorama のみ）	Panorama 実行中の設定のバックアップと各管理対象ファイアウォールの最新バージョンの生成とエクスポートを行います。設定バンドルを毎日作成して SCP または FTP サーバーにエクスポートするプロセスを自動化するには、「Panorama > Device Deployment（デバイスのデプロイ）」を参照してください。
デバイスの設定バンドルのエクスポートまたはプッシュ （Panorama のみ）	ファイアウォールを選択し、Panorama に保存されているファイアウォール設定に対して以下のいずれかの操作を実行するように求められます。 • ファイアウォールに設定を **Push & Commit**[プッシュ & コミット] する。この操作により、ファイアウォールがクリーニング (ファイアウォールからローカル設定が削除) され、Panorama に保存されているファイアウォール設定がプッシュされます。ファイアウォール設定をインポートしたら、Panorama で管理できるように、このオプションを使用してそのファイアウォールをクリーンアップします。 • 設定をロードせずにファイアウォールに **Export**[エクスポート] する。設定をロードするには、ファイアウォール CLI にアクセスし、設定モード コマンド **load device-state** を実行する必要があります。このコマンドを使用すると、**Push & Commit**[プッシュ & コミット] オプションと同じようにファイアウォールがクリーンアップされます。 これらのオプションは*PAN-OS 6.0.4*以降のリリースを実行中のファイアウォールのみにおいて使用可能です。
デバイス状態のエクスポート （ファイアウォールのみ）	ファイアウォールの状態の情報をバンドルとしてエクスポートします。実行中の設定に加え、状態の情報にはPanoramaからプッシュされたデバイスグループ設定やテンプレート設定が含まれます。ファイアウォールが GlobalProtect™ ポータルの場合、バンドルには証明書情報、ポータルが管理するサテライトの一覧、およびサテライト認証情報が含まれています。ファイアウォールまたはポータルを交換した場合、代替のものに状態のバンドルをインポートすることで、エクスポートしておいた情報を復元することができます。 ファイアウォールの状態のエクスポートを手動で実行するか、スケジュール設定された*XML API*スクリプトを作成し、リモートサーバーにファイルをエクスポートする必要があります。サテライト証明書は頻繁に変更される可能性があるので、この操作を定期的に行う必要があります。 CLI でファイアウォール状態ファイルを作成するには、設定モードで **`save device state`** コマンドを実行します。ファイルには、`device_state_cfg.tgz` という名前が付けられ、`/opt/pancfg/mgmt/device-state` に保存されます。ファイアウォール状態ファイルをエクスポートするための操作コマンドは、**`scp export device-state`** です（**`tftp export device-state`** も使用できます）。 XML あるいは REST API の使用方法の詳細は、『PAN-OS および Panorama API ガイド』を参照してください。

© 2019 Palo Alto Networks, Inc.

機能	の意味
名前付き設定スナップショットのインポート	ネットワーク上から実行中の設定あるいは候補設定をインポートします。**Browse**[参照] をクリックして、インポートする設定ファイルを選択します。
デバイス状態のインポート （ファイアウォールのみ）	**Export device state**（デバイス状態のエクスポート）オプションを選択する場合、ファイアウォールからエクスポートしておいた状態情報のバンドルをインポートします。実行中の設定に加え、状態の情報にはPanoramaからプッシュされたデバイスグループ設定やテンプレート設定が含まれます。ファイアウォールがGlobalProtectポータルの場合、バンドルには、証明書情報、サテライトの一覧、およびサテライト認証情報が含まれています。ファイアウォールまたはポータルを交換した場合、代替のものに状態のバンドルをインポートすることで情報を復元します。
Panorama にデバイス設定をインポート （Panorama のみ）	ファイアウォール設定を Panorama にインポートします。ネットワークおよびデバイス設定を格納するテンプレートが Panorama によって自動的に作成されます。ファイアウォールの仮想システム (vsys) ごとに、ポリシーおよびオブジェクト設定を格納するデバイス グループが Panorama によって自動的に作成されます。デバイス グループは、階層内の Shared（共有）場所の 1 つ下のレベルにありますが、インポートの完了後に別の親デバイス グループに再割り当てすることもできます（「Panorama > VMware NSX」を参照）。 *Panorama* のコンテンツ (アプリケーションおよび脅威データベースなど) のバージョンは、設定のインポート元となるファイアウォール上のバージョンと同じかそれ以上である必要があります。 以下のインポート オプションを設定します。 • **Device**[デバイス] – Panorama が設定をインポートするファイアウォールを選択します。ドロップダウンリストには、Panoramaに接続されていて、かつどのデバイスグループやテンプレートにも割り当てられていないファイアウォールのみが表示されます。個々の vsys ではなく、ファイアウォール全体のみを選択できます。 • **Template Name**[テンプレート名] – インポートしたデバイスおよびネットワーク設定を格納するテンプレートの名前を入力します。マルチ vsys ファイアウォールの場合、このフィールドは空白になります。他のファイアウォールの場合、デフォルト値はファイアウォール名になります。既存のテンプレートの名前を使用することはできません。 • **Device Group Name Prefix**（デバイス グループ名の接頭辞）（マルチ **vsys** ファイアウォールのみ）– 必要に応じて、各デバイス グループ名のプレフィックスとして文字列を追加します。 • **Device Group Name**[デバイス グループ名] – マルチ vsys ファイアウォールの場合、デフォルトで各デバイス グループに vsys 名が設定されます。他のファイアウォールの場合、デフォルト値はファイアウォール名になります。デフォルト名は編集できますが、既存のデバイス グループ名を使用することはできません。 • **Import devices' shared objects into Panorama's shared context**（デバイスの共有オブジェクトを **Panorama** の共有コンテクストにインポート）（デフォルトで有効）–Panorama は、ファイアウォールの Shared（共有）に属するオブジェクトを Panorama の Shared（共有）にインポートします。

© 2019 Palo Alto Networks, Inc.

機能	の意味
	Panorama は、マルチ仮想システムを有効にしていないファイアウォールではすべてのオブジェクトを共有とみなします。このオプションを無効にすると、*Panorama* は、*Shared*（共有）ではなくデバイスグループに共有ファイアウォールオブジェクトをコピーします。この設定には、以下の例外があります。 • 共有ファイアウォール オブジェクトの名前と値が既存の共有 Panorama オブジェクトと同じである場合、インポートではそのファイアウォール オブジェクトは除外されます。 • 共有ファイアウォール オブジェクトの名前または値が共有 Panorama オブジェクトと異なる場合、Panorama はそのファイアウォール オブジェクトを各デバイス グループにインポートします。 • テンプレートにインポートされる設定で共有ファイアウォール オブジェクトを参照している場合、このオプションを選択したかどうかに関係なく、Panoramaはそのオブジェクトを Shared [共有] にインポートします。 • 共有ファイアウォールオブジェクトで、テンプレートにインポートされる設定を参照している場合、このオプションを選択したかどうかに関係なく、Panoramaはそのオブジェクトをデバイスグループにインポートします。 • **Rule Import Location**[ルールのインポート場所] — Panorama がポリシーをプレ ルールとしてインポートするのか、ポスト ルールとしてインポートするのかを選択します。選択内容に関係なく、Panorama はデフォルトのセキュリティ ルール (intrazone-default および interzone-default) をポスト ルールベースにインポートします。 *Panorama* に、インポートするファイアウォール ルールと同じ名前のルールがある場合、*Panorama* には両方のルールが表示されます。ただし、ルール名は一意である必要があるため、*Panorama* でコミットを実行する前にいずれかのルールを削除しないと、コミットに失敗します。
デバイスの操作	
再起動	ファイアウォールまたは Panorama を再起動するには、**Reboot Device**（デバイスの再起動）を実行します。デバイスからログアウトされ、ソフトウェア（PAN-OSまたは Panorama）およびアクティブな設定が再度ロードされます。次に既存のセッションが終了してログが記録され、シャットダウンを実行した管理者の名前のもとでシステムログエントリが作成されます。保存またはコミットされていない設定の変更は失われます（「Device（デバイス）> Setup（セットアップ）> Operations（操作）」を参照）。 *Web* インターフェイスを使用できない場合は、次の運用 *CLI* 操作コマンドを使用します。 `request restart system`
シャットダウン	ファイアウォールや Panorama のグレースフルシャットダウンを実行する場合は、**Shutdown Device**（デバイスのシャットダウン）または**Shutdown**

© 2019 Palo Alto Networks, Inc.

機能	の意味
	Panorama（**Panorama**のシャットダウン）をクリックし、確認のプロンプトが表示された場合に **Yes**（はい）を実行します。保存またはコミットされていない設定の変更は失われます。すべての管理者がログオフされ、以下のプロセスが発生します。 • すべてのログイン セッションがログオフされます。 • インターフェイスが無効になります。 • すべてのシステム プロセスが停止します。 • 既存のセッションが終了し、ログに記録されます。 • シャットダウンを開始した管理者名を示すシステム ログが作成されます。このログ エントリを書き込めない場合は、警告が表示され、システムはシャットダウンしません。 • ディスクドライブが正常にアンマウントされ、ファイアウォールまたは Panorama の電源がオフになります。 ファイアウォールまたは Panorama の電源を入れるには、電源のプラグを抜いてから差し込み直す必要があります。 *Web インターフェイスを使用できない場合は、次の CLI 操作コマンドを使用します。* **`request shutdown system`**
データプレーンの再起動	**Restart Dataplane**（データプレーンの再起動）を実行すると、リブートせずにファイアウォールのデータ機能をリスタートします。このオプションは Panorama または PA-220、PA-800 シリーズのファイアウォール、または VM-Series のファイアウォールでは使用できません。 *Web インターフェイスを使用できない場合は、次の CLI 操作コマンドを使用します。* ***`request restart dataplane`*** PA-7000 シリーズのファイアウォールでは、各 NPC にデータプレーンがあるため、次のコマンドを実行することで、NPC を再起動してこの操作を実行できます。 **`request chassis restart slot`**.
その他	
カスタム ロゴ	**Custom Logo**（カスタム ロゴ）をクリックすると以下の任意の内容をカスタマイズします。 • **Login Screen**（ログイン画面）の背景イメージ • **Main UI**（メイン **UI**）（Web インターフェイス）ヘッダーのイメージ • **PDF Report Title Page**（ **PDF** レポートのタイトル ページ）のイメージ。「Monitor（監視）> PDF Reports（PDF レポート）> Manage PDF Summary（PDF サマリーの管理）」を参照してください。 • **PDF Report Footer**（**PDF** レポート フッター）のイメージ 以前にアップロードした画像（ ）をプレビューまたは削除するには、Upload (<image>) an image file（画像ファイルのアップロード(<image>)）しします。

© 2019 Palo Alto Networks, Inc.

機能	の意味
	デフォルトのロゴに戻るには、エントリを削除して **Commit**（コミット）します。 **Login Screen**（ログイン画面）と **Main UI**（メイン **UI**）では、 表示されるイメージを表示（ ）できます。 必要であれば、ファイアウォールはイメージを収縮させて収まるようにします。PDF レポートの場合、ファイアウォールはイメージを切り取らずに自動的にサイズ変更します。すべてのケースにおいて、プレビューは推奨されるイメージのサイズを表示します。 任意のロゴ イメージの最大サイズは、128KB です。サポートされているファイル タイプは、png、gif、および jpg です。ファイアウォールは、インターレースされたイメージ ファイルや、PDF ファイルの生成を妨げるため、アルファチャンネルを含むイメージ ファイルをサポートしていません。そのイメージの作成者に連絡してアルファチャンネルの削除を依頼するか、使用するグラフィックス ソフトウェアでアルファチャンネル機能を含めずにファイルを保存してください。 PDF レポートの生成方法の詳細は、「Monitor（監視）> PDF Reports（PDF レポート）> Manage PDF Summary（PDF サマリーの管理）」を参照してください。
SNMP のセットアップ	SNMP モニタリングを有効化します。
ストレージパーティションの設定（Panorama のみ）	レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティション。

SNMP モニタリングの有効化

- Device > Setup > Operations [デバイス > セットアップ > 操作]

SNMP (Simple Network Management Protocol) は、ネットワーク上のデバイスをモニターする標準プロトコルです。SNMPマネージャでサポートされているSNMPバージョン（SNMPv2cまたはSNMPv3）を使用するようにファイアウォールを設定する場合は、**Operations** [操作] ページを使用します。ファイアウォールから収集される統計情報を解釈できるように SNMP マネージャにロードする必要のある MIB のリストは『サポートされる MIB』を参照してください。ネットワーク上の SNMP トラップ の宛先と通信するファイアウォールを有効にするサーバー プロファイルを設定するには、「Device（デバイス）> Server Profiles（サーバー プロファイル）> SNMP Trap（SNMP トラップ）」を参照してください。SNMP MIB は、ファイアウォールが生成するすべての SNMP トラップを定義します。SNMP トラップは一意のオブジェクト ID (OID) を識別し、個々のフィールドは変数バインド (varbind) リストとして定義されます。**SNMP Setup**（**SNMP** のセットアップ）をクリックし、以下の設定を指定して SNMP マネージャからの SNMP GET 要求を許可します。

項目	の意味
場所	ファイアウォールの物理的な場所を指定します。ログまたはトラップが生成された場合、この情報により、通知を生成したファイアウォールをSNMPマネージャで識別することができます。
お問い合わせ	ファイアウォールの管理者の名前や電子メール アドレスを入力します。この設定は、標準システム情報の MIB でレポートされます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
イベント固有のトラップ定義を使用	このオプションはデフォルトで選択されており、ファイアウォールは、それぞれのSNMPトラップのイベントタイプに基づいた一意のOIDを使用します。このオプションをオフにすると、すべてのトラップのOIDが同じになります。
バージョン	SNMPバージョンを選択します。**V2c** (デフォルト) または**V3**。この選択内容により、ダイアログに表示される残りのフィールドが決まります。
SNMP V2c の場合	
SNMP コミュニティ名	コミュニティ文字列を入力します。コミュニティ文字列は、SNMP マネージャおよびモニター対象デバイスの SNMP コミュニティを識別し、SNMP GET (統計情報要求) やトラップ メッセージを交換するときにコミュニティ メンバーを相互認証するためのパスワードとして機能します。コミュニティ文字列には最大 127 文字を含めることができます。また、すべての文字を使用でき、大文字と小文字が区別されます。 デフォルトのコミュニティ文字列 *public* は使用しないでください。*SNMP* メッセージにはクリア テキストのコミュニティ文字列が含まれているため、コミュニティ メンバーシップ *(*管理者アクセス*)* を定義するときにネットワークのセキュリティ要件を考慮してください。
SNMP V3 の場合	
名前/表示	1 つ以上のビューのグループをSNMPマネージャのユーザーに割り当てて、ユーザーがファイアウォールから取得できるMIBオブジェクト (統計情報) を制御できます。各ビューは、ペアになっている OID とビット単位のマスクです。OID で MIB を指定し、マスク (16 進数形式) で、その MIB 内 (一致部分を含む) または MIB 外 (一致部分を含まない) でアクセスできるオブジェクトを指定します。 たとえば、**OID** が 1.3.6.1、照合の **Option**[オプション] が **include**[包含]、**Mask**[マスク] が 0xf0 の場合、ユーザーが要求するオブジェクトの OID の最初の 4 つのノード (f = 1111) が 1.3.6.1 に一致している必要があります。オブジェクトの残りのノードは一致している必要はありません。この例の場合、1.3.6.1.2 はマスクに一致しますが、1.4.6.1.2 は一致しません。 ビューのグループごとに **Add**[追加] をクリックし、グループの **Name**[名前] を入力します。次に、グループに **Add**[追加] するビューごとに以下を設定します。 • **View**[表示] – ビューの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン) を含めることができます。 • **OID** – MIB の OID を指定します。 • **Option**[オプション] – MIB に適用する照合ロジックを選択します。 • **Mask**[マスク] – 16 進数形式のマスクを指定します。 すべての管理情報にアクセスできるようにするには、最上位 *OID 1.3.6.1* を使用し、*Mask[*マスク*]* を *0xf0* に設定して、照合の *Option[*オプション*]* を *include[*包含*]* に指定します。
Users	SNMPユーザーアカウントにより、ファイアウォールがトラップを転送するときやSNMPマネージャがファイアウォールの統計情報を取得する際に、認証、プラ

© 2019 Palo Alto Networks, Inc.

項目	の意味
	イバシー、およびアクセス制御を行うことができます。ユーザーごとに、**Add**[追加] をクリックして以下の設定を指定します。 • **Users**[ユーザー] – SNMP ユーザー アカウントを識別するユーザー名を指定します。ファイアウォールで設定するユーザー名は、SNMPマネージャで設定したユーザー名と一致する必要があります。ユーザー名には最大 31 文字を使用できます。 • **View**[表示] – ユーザーにビューのグループを割り当てます。 • **Auth Password**[認証パスワード] – ユーザーの認証パスワードを指定します。ファイアウォールは、トラップの転送時や統計情報要求に応答する際に、このパスワードを使用してSNMPマネージャの認証を受けます。ファイアウォールは、Secure Hash Algorithm（SHA-1 160）を使用してパスワードを暗号化します。パスワードには、8 ~ 256 文字のあらゆる文字を使用できます。 • **Priv Password**[専用パスワード] – ユーザーの専用パスワードを指定します。ファイアウォールは、このパスワードとAdvanced Encryption Standard（AES-128）を使用して、SNMPトラップおよび統計情報要求に対する応答を暗号化します。パスワードには、8 ~ 256 文字のあらゆる文字を使用できます。

© 2019 Palo Alto Networks, Inc.

Device > Setup > HSM [デバイス > セットアップ > HSM]

ハードウェア セキュリティ モジュール（HSM）を設定し、操作を実行し、HSM の状態を表示するには、**Device**（デバイス）> **Setup**（セットアップ）> **HSM** を選択します。

確認すべき情報	以下を参照
ハードウェア セキュリティ モジュール（HSM）の目的と、設定手順の詳細を確認できる場所は?	Secure Keys with a Hardware Security Module（ハードウェア セキュリティ モジュールによるキーの安全確保）
設定:	ハードウェア セキュリティ モジュール プロバイダ設定
	HSM 認証
ハードウェア セキュリティ操作の実行	ハードウェア セキュリティ操作
HSM の状態を表示する方法は?	ハードウェア セキュリティ モジュール プロバイダ設定および状態
	ハードウェア セキュリティ モジュール状態

ハードウェア セキュリティ モジュール プロバイダ設定

ファイアウォールにハードウェアセキュリティモジュール（HSM）を設定する場合は、ハードウェアセキュリティモジュールプロバイダの設定を編集します。

ハードウェア セキュリティ モジュール プロバイダ設定	の意味
プロバイダが設定されました	HSM ベンダーを選択します。 • **None**（なし）（デフォルト）–ファイアウォールはどの HSM にも接続しません。 • **SafeNet Network HSM** • **nCipher nShield Connect** *HSM* サーバー バージョンは、ファイアウォールの HSM client version（HSM クライアント バージョン）と互換性がある必要があります。
モジュール名	HSM のモジュール名を追加します。31 文字以下の任意の ASCII 文字列を指定できます。独立または高可用性の SafeNet HSM 設定を構成する場合は、最大 16 のモジュール名を追加できます。
サーバー アドレス	設定するすべての HSM の IPv4 アドレスを指定します。

© 2019 Palo Alto Networks, Inc.

ハードウェア セキュリティ モジュール プロバイダ設定	の意味
HA （SafeNet Network のみ）	（任意）高可用性設定で SafeNet HSM モジュールを設定する場合はこのオプションを選択します。各 HSM モジュールのモジュール名とサーバー アドレスを設定する必要があります。
自動回復の再試行 （SafeNet Network のみ）	ファイアウォールが HSM への接続の回復を試行する回数を指定します（範囲は 0 ~ 500、デフォルトは 0）。この試行回数に達すると、HSM HA 性設定内の別の HSM にフェイルオーバーします。
高可用性グループ名 （SafeNet Network のみ）	HSM HA グループで使用されるグループ名を指定します。この名前はファイアウォールの内部で使用されます。31 文字以下の任意の ASCII 文字列を指定できます。
ファイルシステムのアドレスの削除 nCipher nShield Connect のみ	nCipher nShield Connect HSM 設定で使用されるリモート ファイル システムの IPv4 アドレスを設定します。

HSM 認証

Setup Hardware Security Module（ハードウェア セキュリティ モジュールのセットアップ）を選択し、以下の設定で HSM に対するファイアウォールの認証を指定します。

HSM モジュール認証	
サーバー名	ドロップダウンリストからHSMサーバー名を選択します。
管理者パスワード	HSM に対するファイアウォールの認証を行う HSM の管理者パスワードを入力します。

ハードウェア セキュリティ操作

Hardware Security Module（ハードウェアセキュリティモジュール）(HSM)または HSM に接続されたファイアウォールで操作を実行するには、**Device**（デバイス）> **Setup**（セットアップ）> **HSM** を選択し、次のハードウェア セキュリティ操作のいずれかを選択します。

ハードウェア セキュリティ操作	
ハードウェア セキュリティ モジュールのセットアップ	HSM を認証するようにファイアウォールを設定します。
詳細情報を表示	HSM サーバー、HSM 高可用性ステータス、および HSM ハードウェアに関する情報を表示します。

© 2019 Palo Alto Networks, Inc.

ハードウェア セキュリティ操作	
Remote Filesystem (リモート ファイルシステム) と同期する (nCipher nShield Connect HSM のみ)	nShield Connect HSM リモート ファイルシステムからファイアウォールにキー データを同期します。
設定のリセット	ファイアウォールへのすべての HSM 接続を削除します。HSM 設定をリセットした後、すべての認証手順を繰り返す必要があります。
HSM Client (クライアント) のバージョンを選択する (SafeNet Network (ネットワーク) HSM のみ)	HSM クライアント (ファイアウォール) 上で実行されているソフトウェアのバージョンを選択できます。HSM サーバー クライアントのバージョンは、ファイアウォールの HSM サーバー バージョンと互換性がある必要があります。クライアント サーバー バージョンの互換性マトリックスについては、HSM ベンダーのドキュメントを参照してください。

ハードウェア セキュリティ モジュール プロバイダ設定および状態

Hardware Security Module Provider (ハードウェア セキュリティ モジュール プロバイダ) セクションには、HSM 設定および HSM の接続状態が表示されます。

ハードウェア セキュリティ モジュール プロバイダの状態	
プロバイダが設定されました	ファイアウォールで設定されている HSM ベンダーを選択します。 • まったくない • **SafeNet Network HSM** • **nCipher nShield Connect**
HA	(SafeNet Network のみ) オンにすると、HSM 高可用性が設定されます。
高可用性グループ名	(SafeNet Network のみ) ファイアウォールに設定される HSM 高可用性のグループ名。
ファイアウォール送信元アドレス	HSM サービスに使用されるポートのアドレス。デフォルトでは、このアドレスには管理ポート アドレスが設定されます。**Device** (デバイス) > **Setup** (セットアップ) > **Services** (サービス) の Services Route Configuration (サービス ルートの設定) を使用して、別のポートを指定できます。
HSM が保護するマスター キー	オンにした場合、HSM でマスター キーが保護されます。
ステータス	ファイアウォールが接続されて HSM に認証されている場合は緑で表示されます。ファイアウォールが認証されていない場合、または HSM へのネットワーク接続がダウンしている場合は赤で表示されます。 HSM 接続の詳細は、「ハードウェア セキュリティ モジュール状態」を参照してください。

© 2019 Palo Alto Networks, Inc.

ハードウェア セキュリティ モジュール状態

Hardware Security Module Status(ハードウェア セキュリティ モジュール状態)には、認証に成功した HSMs に関する以下の情報が含まれます。表示は設定された HSM プロバイダ (SafeNet または nCipher) によって異なります。

ハードウェア セキュリティ モジュール状態	
SafeNet Network HSM	• **Serial Number**（シリアル番号）– HSM パーティションが正常に認証された場合、その HSM パーティションのシリアル番号が表示されます。 • **Partition**（パーティション）– ファイアウォールで割り当てられた HSM のパーティション名。 • **Module State**（モジュール状態）– HSM 接続の現在の動作状態。HSM がこの表に表示されている場合、このフィールドには **Authenticated**（認証済み）と表示されます。
nCipher nShield Connect	• **Name**（名前）– HSM のサーバー名。 • **IP address**（**IP** アドレス）– ファイアウォールで割り当てられた HSM の IP アドレス。 • **Module State**（モジュール状態）– HSM 接続の現在の動作状態。ファイアウォールが HSM に正常に認証された場合、この設定には **Authenticated**（認証済み）と表示されます。認証が失敗した場合は、**Not Authenticated**（認証されていません）と表示されます。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Services [デバイス > セットアップ > サービス]

以下のトピックでは、ファイアウォールにおけるグローバルおよび仮想システムのサービス設定について説明します。

- グローバルおよび仮想システムのサービスの設定
- グローバル サービス設定
- サービス ルートの設定での IPv4 および IPv6 のサポート
- 宛先サービス ルート

グローバルおよび仮想システムのサービスの設定

マルチ仮想システムが有効になっているファイアウォールにおいて、効率的な動作のためにファイアウォールまたはその仮想システムが使用するサービスを設定する際に、それぞれ **Global**（グローバル）タブと **Virtual Systems**（仮想システム）タブを表示する場合は、**Services**（サービス）を選択します。（ファイアウォールが 1 つの仮想システムの場合、またはマルチ仮想システムが無効になっている場合、**Virtual Systems**（仮想システム）タブは表示されません）。

ファイアウォール全体のサービスを設定する場合は、**Global** [グローバル] タブを使用します。これらの設定は、サービスの設定がカスタマイズされていない仮想システムのデフォルト値としても使用されます。

- DNS サーバー、更新サーバー、プロキシ サーバーのそれぞれの宛先 IP アドレスを定義する場合は **Services**（サービス）を編集します。専用の**NTP**タブを使用して、Network Time Protocol設定を編集します。Service（サービス）で使用可能なオプションのフィールドに関する説明については、表 12 を参照してください。
- DNS、電子メール、LDAP、RADIUS、Syslogなどのサービスを提供する際の、ファイアウォールと他のサーバー/デバイス間の通信方法を指定する場合は、**Service Features** [サービス機能] から、**Service Route Configuration** [サービスルートの設定] をクリックします。グローバル サービス ルートを設定するには、以下の 2 つの方法があります。
  - **Use Management Interface for all** [すべてに管理インターフェイスを使用] オプションでは、外部サーバーとのファイアウォールサービス通信はすべて強制的に管理インターフェイス（MGT）を使用して行われます。このオプションを選択する場合、ファイアウォールとサービスを提供するサーバーまたはデバイスとの間の通信を許可するように MGT インターフェイスを設定する必要があります。MGT インターフェイスを設定する場合は、Device（デバイス）> Setup（セットアップ）> Management（管理）を開き、設定を編集します。
  - **Customize**[カスタマイズ] オプションでは、サービスが応答時に宛先インターフェイスおよび宛先 IP アドレスとして使用する、特定の送信元インターフェイスおよび送信元 IP アドレスを設定することで、サービス通信を詳細に制御できます。（たとえば、ファイアウォールと電子メール サーバー間のすべての電子メール通信に使用する特定の送信元 IP/インターフェイスを設定し、Palo Alto Networks サービスには別の送信元 IP/インターフェイスを使用できます）。 同じ設定にカスタマイズする 1 つ以上のサービスを選択し、**Set Selected Service Routes**[選択されたサービス ルートの設定] をクリックします。サービスは表 13 に記載されています。この表では、サービスが **Global**（グローバル）ファイアウォールまたは **Virtual Systems**（仮想システム）用に設定できるかどうか、およびサービスで IPv4/IPv6 の送信元アドレスがサポートされているかどうかがわかります。

Destination[宛先] タブは、カスタマイズ可能な別のグローバル サービス ルート機能です。これは、Service Route Configuration（サービス ルートの設定）ウィンドウに表示されます。「宛先サービス ルート」を参照してください。

1 つの仮想システムのサービス ルートを指定するには、**Virtual Systems**[仮想システム] タブを使用します。場所 (仮想システム) を選択し、**Service Route Configuration**[サービス ルートの設定] をクリックし

© 2019 Palo Alto Networks, Inc.

ます。**Inherit Global Service Route Configuration**（グローバル サービス ルート設定の継承）を選択するか、仮想システムのサービス ルートを **Customize**（カスタマイズ）します。設定をカスタマイズする場合、**IPv4** または **IPv6** を選択します。同じ設定にカスタマイズする 1 つ以上のサービスを選択し、**Set Selected Service Routes**[選択されたサービス ルートの設定] をクリックします。カスタマイズ可能なサービスは、表 13 を参照してください。

共有仮想マシンと特定の仮想システム間の DNS クエリを制御およびリダイレクトするために、DNS プロキシおよび DNS サーバー プロファイルを使用できます。

グローバル サービス設定

- Device > Setup > Services [デバイス > セットアップ > サービス]

共有仮想マシンと特定の仮想システム間の DNS クエリを制御およびリダイレクトするために、DNS プロキシおよび DNS サーバー プロファイルを使用できます。

グローバル サービス設定	の意味
本サービス	
更新サーバー	Palo Alto Networks から更新ファイルをダウンロードするサーバーの IP アドレスまたはホスト名を表します。現在値は、**updates.paloaltonetworks.com** です。テクニカル サポートから指示がない限り、この設定は変更しないでください。
更新サーバー ID の確認	このオプションを有効にすると場合、信頼された機関によって署名された SSL 証明書がソフトウェアまたはコンテンツ パッケージのダウンロード元のサーバーにあるかどうかをファイアウォールまたは Panorama が確認します。これにより、ファイアウォールまたは Panorama サーバーと更新サーバー間の通信に新たなレベルのセキュリティを追加します。 更新サーバーの身元を検証し、信頼できる機関が署名した *SSL* 証明書をサーバーが持っていることを確認します。
DNS 設定	ファイアウォールが FQDN アドレスオブジェクト、ログ、およびファイアウォール管理をサポートするために開始するすべての DNS クエリに対して、DNS サービスのタイプ—**Servers**（サーバー）または **DNS Proxy Object**（**DNS** プロキシ オブジェクト）—を選択します。用意されているオプション: • ドメイン名を解決するプライマリおよびセカンダリ DNS サーバー。 • DNS サーバーを構成する代わりに、ファイアウォール上に DNS プロキシを構成します。DNS プロキシを有効にするには **Cache (キャッシュ)** および **EDNS Cache Responses (EDNS キャッシュ応答)** (**Network (ネットワーク)** > **DNS Proxy (DNS プロキシ)** > **Advanced (詳細)**) を有効にする必要があります。
プライマリDNSサーバー	ファイアウォールからの DNS クエリのプライマリ DNS サーバーの IP アドレスを入力します。たとえば、更新サーバーを検索し、ログの DNS エントリを解決したり、FDQN ベースのアドレス オブジェクトを解決したりする場合などです。
セカンダリ DNS サーバー	（任意）プライマリ サーバーを使用できない場合に使用するセカンダリ DNS サーバーの IP アドレスを入力します。

© 2019 Palo Alto Networks, Inc.

グローバル サービス設定	の意味
最低 FQDN 更新時間（秒単位）	ファイアウォールが DNS から受信する FQDN を更新する頻度の限界を設定します。TTL がこの**Minimum FQDN Refresh Time (最低 FQDN 更新時間)**（秒単位）以上である間、ファイアウォールは FQDN の TTL に基づいて FQDN を更新します。TTL がこの Minimum FQDN Refresh Time (最低 FQDN 更新時間) 未満である場合、ファイアウォールはこの Minimum FQDN Refresh Time (最低 FQDN 更新時間) に基づいて FQDN を更新します（つまり、ファイアウォールはこの設定よりも速い TTL を受け付けません）。ファイアウォールが FQDN を解決する DNS サーバーまたは DNS プロキシ オブジェクトから DNS 応答を受信すると、タイマーが開始されます（範囲は 0 ~ 14,400、デフォルトは 30）。0 に設定すると、ファイアウォールが DNS 内の TTL の値に基づいて FQDN を更新し、最低 FQDN 更新時間を適用しなくなります。 *DNS 内の FQDN の TTL が短く、しかし FQDN の解決が TTL の期間ほど頻繁に変わらず、高速な更新が不要である場合、最低の FQDN Refresh Time (FQDN 更新時間) を設定して不要な FQDN の更新を試みないようにする必要があります。*
古い FQDN エントリのタイムアウト（分）	ネットワークのエラーが発生したり DNS サーバーに到達できなかったりする場合（FQDN が更新を受け取っていない場合）にファイアウォールが古い FQDN 解決を使用し続ける期間（分単位）を指定します（範囲は 0 ~ 10,080、デフォルトは 1,440）。値を 0 にすると、ファイアウォールが古いエントリを使用し続けなくなります。このタイムアウトを過ぎてもまだ DNS サーバーに到達できない場合、FQDN のエントリが解決不能になります（古い解決が削除されます）。 誤ったトラフィックの転送（セキュリティリスクが発生）を許さないよう*FQDN Stale Entry Timeout (古い FQDN エントリのタイムアウト)*の値を十分短くしつつ、かつ意図せずネットワークをダウンさせないよう、トラフィックの継続性を維持できるよう十分長くしてください。
プロキシ サーバーセクション	
SERVER	ファイアウォールがプロキシサーバーを使用して Palo Alto Networks 更新サービスにアクセスする必要がある場合は、プロキシ サーバーの IP アドレスまたはホスト名を入力します。
ポート	プロキシ サーバーのポートを入力します。
感染	プロキシ サーバーにアクセスするときに管理者が入力するユーザー名を入力します。
パスワード/再入力 パスワード	プロキシ サーバーにアクセスするときに管理者が入力するパスワードを入力して確認します。
NTP	
NTP サーバー アドレス	ファイアウォールのクロックを同期するために使用する NTP サーバーの IP アドレスまたはホスト名を入力します。プライマリ サーバーが使用不能になった場合、ファイアウォールのクロック同期に使用するセカンダリ NTP サーバーの IP アドレスまたはホスト名を入力します。(任意)

© 2019 Palo Alto Networks, Inc.

グローバル サービス設定	の意味
	NTP サーバーがすべてのネットワークのファイアウォールのクロックを同期させる際、予定中のジョブが通常通りに実行され、また複数のデバイスが関わる問題の根本原因を特定するためにタイムスタンプを活用できます。プライマリ *NTP* サーバーに到達できない場合に備えてプライマリおよびセカンダリ *NTP* サーバーを設定します。

認証タイプ	NTP サーバーからの日時更新をファイアウォールが認証できるように指定できます。NTP サーバーごとに、ファイアウォールで使用する認証のタイプを選択します。
	• **None**（なし）(デフォルト) – NTP 認証を無効にするにはこのオプションを選択します。
	• **Symmetric Key**（対称キー） – ファイアウォールで対称キー交換（共有秘密）を使用して NTP サーバーからの日時更新を認証するには、このオプションを選択します。Symmetric Key（対称キー）を選択した場合、続けて次の値を指定します。
	  • **Key ID**（キーID） – キーID（1 ~ 65534）を入力します。
	  • **Algorithm**（アルゴリズム）–NTP 認証に使用する MD5 アルゴリズムまたは SHA1 アルゴリズムを選択します。
	  • **Authentication Key/Confirm Authentication Key**（認証キー/再入力 認証キー）– 認証アルゴリズムの認証キーを入力し、確認します。
	• **Autokey**（自動キー） – ファイアウォールで自動キー（公開鍵暗号化）を使用して NTP サーバーからの日時更新を認証するには、このオプションを選択します。
	NTP サーバー認証を有効化し、*NTP* サーバーがクライアントを承認して同期された更新を提供できるようにします。

サービス ルートの設定での IPv4 および IPv6 のサポート

次の表は、グローバル システムと仮想システムの IPv4 と IPv6 でサービス ルート設定がサポートされるかどうかを示しています。

サービス ルートの設定	Global		仮想システム(vsys)	
	IPv4	IPv6	IPv4	IPv6
AutoFocus–AutoFocus™ サーバー。	✓	–	–	–
CRL ステータス – 証明書失効リスト (CRL) サーバー。	✓	✓	–	–
DDNS–動的 DNS サービス。	✓	✓	✓	✓
Panorama によってプッシュされる更新 – Panorama™ からデプロイされるコンテンツ更新とソフトウェア更新。	✓	✓	–	–

© 2019 Palo Alto Networks, Inc.

サービス ルートの設定	Global		仮想システム(vsys)	
	IPv4	IPv6	IPv4	IPv6
DNS—Domain Name System サーバー。 * 仮想システムの場合、DNS は DNS サーバー プロファイルで実行されます。	✓	✓	✓ *	✓ *
外部動的リスト — 外部動的リストの更新。	✓	✓	—	—
電子メール—電子メール サーバー。	✓	✓	✓	✓
HSM—ハードウェア セキュリティ モジュール サーバー。	✓	—	—	✓
HTTP—HTTP 転送。	✓	✓	✓	✓
Kerberos—Kerberos 認証サーバー。	✓	—	✓	✓
LDAP — Lightweight Directory Access Protocol サーバー。	✓	✓	✓	✓
MDM—モバイル デバイス管理サーバー。	✓	✓	—	—
多要素認証 — 多要素認証（MFA）サーバー。	✓	✓	✓	✓
NetFlow — ネットワーク トラフィック統計情報を収集する NetFlow。	✓	✓	✓	✓
NTP—Network Time Protocol サーバー。	✓	✓	—	—
Palo Alto Networks サービス — Palo Alto Networks® およびパブリック WildFire® サーバーからの更新。テレメトリ データを Palo Alto Networks に転送するサービス ルートでもあります。	✓	—	—	—
Panorama—Panorama 管理サーバー。	✓	✓	—	—
Panorama ログ転送 — （PA-5200 シリーズ ファイアウォールのみ）ファイアウォールからログ コレクタへのログ転送。	✓	✓	—	—
プロキシ — ファイアウォールへのプロキシとして機能するサーバー。	✓	✓	—	—
RADIUS — Remote Authentication Dial-in User Service サーバー。	✓	✓	✓	✓

© 2019 Palo Alto Networks, Inc.

サービス ルートの設定	Global		仮想システム(vsys)	
	IPv4	IPv6	IPv4	IPv6
SCEP — クライアント証明書の要求および配信用Simple Certificate Enrollment Protocol。	✓	✓	✓	—
SNMP トラップ — Simple Network Management Protocol トラップ サーバー。	✓	—	✓	—
Syslog — システム メッセージ ログ用のサーバー。	✓	✓	✓	✓
TACACS+ — 認証、認可、課金（AAA）サービスを行う Terminal Access Controller Access-Control System Plus（TACACS+）サーバー。	✓	✓	✓	✓
UID Agent — User-ID エージェント サーバー。	✓	✓	—	✓
URL Updates — Uniform Resource Locator (URL) 更新サーバー。	✓	✓	—	—
す。Device（デバイス）>（情報ソース）.が有効にする **VM** モニター—フィルタを適用してテーブルの出力をカスタマイズし、必要な列のみを含めることができます。 仮想マシンを監視しているパブリッククラウド展開の *VM* シリーズ ファイアウォールは、*MGT* インターフェイスを使用する必要があります。エクスポート ダイアログに表示される列のみがエクスポートされます。	✓	✓	✓	✓
Wildfire Private — プライベート Palo Alto Networks WildFire サーバー。	✓	—	—	—

Global（グローバル）サービス ルートをカスタマイズする場合は、**Service Route Configuration**（サービス ルート設定）を選択し、**IPv4** または **IPv6** タブで、利用可能なサービスのリストからサービスを選択します。複数のサービス ルートを設定して、**Set Selected Service Routes**（選択したサービス ルート）を設定して、複数のサービス ルートを同時に設定することもできます。ドロップダウン リストで**Source Address**（送信元アドレス）の選択内容を制限するには、**Source Interface**（送信元インターフェイス）を選択してから **Source Address**（送信元アドレス）を選択します。**Any**（いずれか）に設定された送信元インターフェイスの場合、使用可能なインターフェイスの中から任意の送信元アドレスを選択できます。Source Address（送信元アドレス）には、選択したインターフェイスに割り当てられている IPv4 または IPv6 アドレスが表示されます。選択した IP アドレスは、サービス トラフィックの送信元になります。ファイアウォールでサービスルートの管理インターフェイスを使用する場合は、**Use default**（デフォルトを使用）できます。 ただし、パケットの宛先IPアドレスが設定された宛先IPアドレスと一致する場合、送信元IPアドレスは宛先に設定された送信元アドレスに設定されます。宛先は各サービスを設定するときに設定されるため、宛先アドレスを定義する必要はありません。たとえば、**Device**（デバイス）>

© 2019 Palo Alto Networks, Inc.

Setup（設定）> **Services**（サービス）で DNS サーバーを定義すると、DNS クエリの宛先が設定されます。サービスに IPv4 と IPv6 の両方のアドレスを指定できます。

Global（グローバル）サービス ルートをカスタマイズするもう1つの方法は、**Service Route Configuration**（サービス ルート設定）選んでから **Destination**（宛先）を選択することです。受信パケットが比較される **Destination**（宛先） IP アドレスを指定します。パケットの宛先アドレスが設定済みの宛先 IP アドレスと一致する場合、送信元 IP アドレスは宛先に設定された送信元アドレスに設定されます。ドロップダウン リストで**Source Address**（送信元アドレス）の選択内容を制限するには、**Source Interface**（送信元インターフェイス）を選択してから **Source Address**（送信元アドレス）を選択します。**Any** [いずれか] に設定された送信元インターフェイスの場合、使用可能なインターフェイスの中から任意の送信元アドレスを選択できます。**MGT** ソース インターフェイスを選択すると、ファイアウォールはサービスルートに MGT インターフェイスを使用します。

Virtual System（仮想システム）のサービス ルートを設定する場合、**Inherit Global Service Route Configuration**（グローバルサービスルート設定の継承）を選択すると、仮想システムのすべてのサービスがグローバルサービスルート設定を継承します。あるいは、**Customize(カスタマイズ)**を選択し、**IPv4** または **IPv6** を選択して、サービスを選択します。また、複数のサービスと **Set Selected Service Routes**（選択したサービス ルートを選択する）を選択することもできます。**Source Interface**[送信元インターフェイス] には、以下の 3 つの選択肢があります。

- **Inherit Global Setting**（グローバル設定の継承） — 選択したサービスがこれらのサービスのグローバル設定を継承します。
- **Any**[いずれか] — 使用可能な任意のインターフェイス (特定の仮想システムのインターフェイス) から送信元アドレスを選択できます。
- ドロップダウン リストからのインターフェイス—**Source Address**（送信元アドレス）のドロップダウンをこのインターフェイスの IP アドレスに制限します。

Source Address[送信元アドレス] の場合、ドロップダウンリストからアドレスを選択します。サービスが選択されている場合、サーバーの応答がこの送信元アドレスに送信されます。

宛先サービス ルート

- Device > Setup > Services > Global [デバイス > セットアップ > サービス > グローバル]

Global（グローバル）タブで、**Service Route Configuration**（サービス ルートの設定）、**Customize**（カスタマイズ）の順にクリックすると、**Destination**（宛先）タブが表示されます。宛先サービス ルートは、(**Virtual Systems**[仮想システム] タブではなく) **Global**[グローバル] タブでしか使用できないため、個々の仮想システムのサービス ルートは、その仮想システムに関連付けられていないルート テーブル エントリをオーバーライドできません。

宛先サービス ルートを使用して、サービスの **Customize**（カスタマイズ）リストでサポートされていない、カスタマイズされたサービスのリダイレクトを追加できます。宛先サービス ルートは、転送情報ベース (FIB) ルート テーブルをオーバーライドするようにルーティングをセットアップする方法です。宛先サービス ルートの設定は、ルート テーブル エントリをオーバーライドします。これらは、サービスに関連している場合もあれば、関連していない場合もあります。

以下のような場合に **Destination**[宛先] タブを使用します。

- サービスにアプリケーション サービス ルートがない場合。
- 1 つの仮想システム内で、複数の仮想ルーター、または仮想ルーターと管理ポートの組み合わせを使用する場合。

宛先サービス ルートの設定	の意味
宛先	**Destination**[宛先] の IP アドレスを入力します。このアドレスと一致する宛先アドレスを持つ着信パケットは、このサービス ルートに指

© 2019 Palo Alto Networks, Inc.

宛先サービス ルートの設定	の意味
	定したSource Address（発信元アドレス）を発信元として使用します。
送信元インターフェイス	Source Address（送信元アドレス）のドロップダウンを制限するには、**Source Interface**（送信元インターフェイス）を選択します。**Any**（すべて）を選択すると、Source Address（送信元アドレス）のドロップダウンですべてのインターフェイス上のすべての IP アドレスを使用できるようになります。**MGT** を選択すると、ファイアウォールはサービスルートに MGT インターフェイスを使用します。
送信元アドレス	サービスルートの **Source Address**（送信元アドレス）を選択します。 このアドレスは宛先から戻ってくるパケットに使用されます。宛先アドレスのサブネットは入力する必要がありません。

© 2019 Palo Alto Networks, Inc.

Device（デバイス）> Setup（セットアップ）> Interfaces（インターフェイス）

このページを使用して、すべてのファイアウォール モデルの管理（MGT）インターフェイスと PA-5200 シリーズ ファイアウォールの補助インターフェイス（AUX-1 および AUX-2）の接続、許可されるサービス、および管理アクセスを設定します。

インターフェイスごとに IP アドレス、ネットマスク（IPv4）、またはプレフィックス長（IPv6）、およびデフォルト ゲートウェイを常に指定することをお勧めします。MGT インターフェイスに関するこれらの設定のいずれか（たとえば、デフォルト ゲートウェイ）を省略した場合、今後の設定変更でファイアウォールにアクセスできるのは、コンソール ポートからのみになります。

M-500 アプライアンス、あるいは *Panorama* バーチャル アプライアンスの *MGT* インターフェイスを設定するには、「Panorama > Setup (セットアップ) > Interfaces (インターフェイス)」を参照してください。

MGT インターフェイスの代わりにループバック インターフェイスを使用してファイアウォールを管理できます（「Network（ネットワーク）> Interfaces（インターフェイス）> Loopback（ループバック）」を参照）。

項目	の意味

タイプ
（MGT インターフェイスのみ）
	以下のうち1つを選択します。
	• **Static**[静的] - **IP Address** [IPアドレス]（IPv4）、**Netmask** [ネットマスク]（IPv4）、**Default Gateway** [デフォルトゲートウェイ] を手動で入力する必要があります。
	• **DHCP Client** [DHCPクライアント] - ファイアウォールがDHCPサーバーを見つけるためにDHCP DiscoverまたはDHCP Requestメッセージを送信できるよう、MGTインターフェイスをDHCPクライアントとして設定します。これに対する応答として、サーバーはMGTインターフェイス用のIPアドレス（IPv4）、ネットマスク（IPv4）、そしてデフォルトゲートウェイを提供します。VM-Seriesファイアウォールでは、MGTインターフェイスのDHCPはデフォルトで無効になっています（AWSおよびAzureのVM-Seriesファイアウォールを除く）。**DHCP Client** [DHCPクライアント] を選択した場合、任意で以下のいずれかまたは両方のクライアントオプションを選択することができます。
	  • **Send Hostname**（ホスト名を送信）- MGT インターフェイスは、そのホスト名を DHCP オプション 12 の一部として DHCP サーバーに送信します。
	  • **Send Client Id**（クライアント **ID** を送信）- MGT インターフェイスは、そのクライアント識別子を DHCP オプション 61 の一部として送信します。
	DHCP Client [DHCPクライアント] を選択した場合、任意で**Show DHCP Client Runtime Info** [DHCPクライアントランタイム情報を表示] をクリックすると動的IPインターフェイスの状態を参照することができます。
	• インターフェイス - MGT インターフェイスを示します。
	• IPアドレス - インターフェイスのIPアドレスです。
	• ネットマスク - どのビットがネットワークまたはサブネットワークで、どのビットがホストであるかを示す、IPアドレスのサブネット マスクです。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• ゲートウェイ - MGTインターフェイスから出て行くトラフィック用のデフォルトゲートウェイ。 • プライマリ/セカンダリNTP - MGTインターフェイスが使用するNTPサーバーのIPアドレスを2つまで表示します。DHCPサーバーがNTPサーバーアドレスを返した場合、ファイアウォールはNTPサーバーアドレスを手動で設定していなかった場合のみそれらを認識します。NTPサーバーアドレスを手動で設定している場合、ファイアウォールがDHCPサーバーから送られてきたアドレスで上書きすることはありません。 • リースタイム - そのDHCP IPアドレスが割り当てられている時間（日/時間/分/秒）を表示します。 • 失効時間 - DHCPリースが無効となる年月日、時間/分/秒およびそのタイムゾーンを表示します。 • DHCP サーバー - MGT インターフェイスの DHCP クライアントに応答する DHCP サーバーの IP アドレスを表示します。 • ドメイン - MGTインターフェイスが属するドメイン名を表示します。 • DNSサーバー - MGTインターフェイスが使用するDNSサーバーのIPアドレスを2つまで表示します。DHCPサーバーがDNSサーバーアドレスを返した場合、ファイアウォールはDNSサーバーアドレスを手動で設定していなかった場合のみそれらを認識します。DNSサーバーアドレスを手動で設定している場合、ファイアウォールがDHCPサーバーから送られてきたアドレスで上書きすることはありません。 必要に応じて、MGT インターフェイスに割り当てられた IP アドレスの DHCP リースを **Renew**（更新）することもできます。完了したら、ウィンドウを**Close** [閉じ] ます。
Aux 1 / Aux 2（補助1/補助2） （PA-5200 シリーズファイアウォールのみ）	補助インターフェイスを有効にするには、以下のいずれかのオプションを選択します。これらのインターフェイスは以下の目的で 10Gbps（SFP+）のスループットを提供します。 • ファイアウォール管理トラフィック – Web インターフェイスおよび CLI にアクセスしてファイアウォールを管理するときに管理者が使用するネットワーク サービス（プロトコル）を有効にする必要があります。 *Web インターフェイスには HTTP ではなく HTTPS を有効にして、CLI には Telnet ではなく SSH を有効にしてください。* • ファイアウォール ピア間の高可用性（HA）同期 – インターフェイスを設定した後、そのインターフェイスを HA の制御リンクとして選択する必要があります（**Device**（デバイス）> **High Availability**（高可用性）> **General**（全般））。 • Panorama へのログ転送 – **Panorama Log Forwarding**（**Panorama** ログ転送）サービスを有効にしてサービス ルートを設定する必要があります（「Device（デバイス）> Setup（セットアップ）> Services（サービス）」を参照）。
IP アドレス (IPv4)	ネットワークで IPv4 を使用する場合、IPv4 アドレスをインターフェイスに割り当てます。または、ループバック インターフェイスの IP アドレスを割り当ててファイアウォールを管理することもできます（「Network（ネットワーク）> Interfaces（インターフェイス）> Loopback（ループバック）」を参照）。デフォルトでは、入力する IP アドレスはログ転送の送信元アドレスです。

© 2019 Palo Alto Networks, Inc.

項目	の意味
ネットマスク (IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワーク マスク (例: 255.255.255.0) を入力する必要もあります。
デフォルト ゲートウェイ	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv4 アドレスを割り当てる必要があります (ゲートウェイはインターフェイスと同じサブネット上にある必要があります)。
IPv6 アドレス/プレフィックス長	ネットワークで IPv6 を使用する場合、IPv6 アドレスをインターフェイスに割り当てます。ネットマスクを示すには、IPv6 プレフィックス長を入力します (例: 2001:400:f00::1/64)。
デフォルト IPv6 ゲートウェイ	IPv6 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv6 アドレスを割り当てる必要があります (ゲートウェイはインターフェイスと同じサブネット上にある必要があります)。
速度	インターフェイスのデータ速度とデュプレックス オプションを設定します。フル デュプレックスまたはハーフ デュプレックスで、10Mbps、100Mbps、1Gbps のいずれかを選択できます。ファイアウォールにインターフェイス速度を決定させるには、デフォルトのオート ネゴシエート設定を使用します。 この設定は、隣接するネットワーク機器のポート設定と一致する必要があります。設定を確実に一致させるには、オート ネゴシエートを選択します (隣接する機器がこのオプションをサポートする場合)。
MTU	このインターフェイスで送信されるパケットの最大転送単位 (MTU) をバイト数で入力します (範囲は 576 ~ 1,500、デフォルトは 1,500)。
管理サービスの管理	• **HTTP** - ファイアウォールの Web インターフェイスにアクセスするには、このサービスを使用します。 *HTTP*はプレーンテキストを使用しますが、*HTTPS*よりは機密性が劣ります。このため、インターフェイス上の管理トラフィックには、*HTTP* の代わりに *HTTPS* を有効化することをお勧めします。 • **Telnet** - ファイアウォールの CLI にアクセスするには、このサービスを使用します。 *Telnet*はプレーンテキストを使用しますが、*SSH*よりは機密性が劣ります。このため、インターフェイス上の管理トラフィックには、*Telnet* の代わりに *SSH* を有効化することをお勧めします。 • **HTTPS** - ファイアウォールの Web インターフェイスに安全にアクセスするには、このサービスを使用します。 • **SSH** - ファイアウォールの CLI に安全にアクセスするには、このサービスを使用します。
Network Services (ネットワーク サービス)	インターフェイスで有効にするサービスを選択します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **HTTP OCSP** - ファイアウォールをオンライン証明書状態プロトコル（OCSP）レスポンダとして設定するには、このサービスを使用します。詳細は、「Device（デバイス）> Certificate Management（証明書の管理）> OCSP Responder（OCSP レスポンダ）」を参照してください。 • **Ping** - 外部サービスとの接続をテストするには、このサービスを使用します。例えば、インターフェイスに対してpingを行い、Palo Alto Networksアップデートサーバーから PAN-OSソフトウェアやコンテンツのアップデートが受信可能な状態かどうか確認することができます。高可用性（HA）配置の場合、HAピアはpingを使用してハートビートのバックアップ情報を交換します。 • **SNMP** - SNMP マネージャーからのファイアウォール統計情報のクエリを処理するには、このサービスを使用します。詳細は、「SNMP モニタリングの有効化」を参照してください。 • **User-ID** - ファイアウォール間のユーザー マッピングの再配信を有効化するには、このサービスを使用します。 • **User-ID Syslog Listener-SSL**（**User-ID Syslog**リスナー**-SSL**）- PAN-OS 統合 User-ID™ エージェントによる SSL 経由の syslog メッセージの収集を有効化するには、このサービスを使用します。詳細は、「監視対象サーバーに対するアクセスの設定」を参照してください。 • **User-ID Syslog Listener-UDP**（**User-ID Syslog**リスナー**-UDP**）- PAN-OS 統合 User-ID エージェントによる UDP 経由の syslog メッセージの収集を有効化するには、このサービスを使用します。詳細は、「監視対象サーバーに対するアクセスの設定」を参照してください。
アクセス許可IPアドレス	管理者がインターフェイスを通じてファイアウォールにアクセスするために使用できる IP アドレスを入力します。空のリスト（デフォルト）は、どの IP アドレスからもアクセスできることを示します。 このリストを空白のままにしないでください。ファイアウォール管理者の *IP* アドレスのみを指定して、不正アクセスを阻止してください。

© 2019 Palo Alto Networks, Inc.

Device（デバイス）> Setup（セットアップ）> Telemetry（テレメトリ）

テレメトリーは、分析用のデータの収集と送信を行うプロセスです。ファイアウォールでテレメトリーを有効にすると、ファイアウォールは、アプリケーション、脅威、デバイスの使用率統計、およびパッシブ DNS に関する情報を含むデータを収集し、Palo Alto Networks に送信します。各テレメトリー参加者が共有するデータからすべての Palo Alto Networks ユーザーがメリットを得ます。テレメトリーはコミュニティ駆動の、脅威を阻止するためのアプローチです。テレメトリーとそのメリットについては詳細をご確認ください。

テレメトリーはオプトイン機能です。ほとんどのテレメトリー データに関して、ユーザーはファイアウォールで収集された情報をプレビューできます。Palo Alto Networks はユーザーのデータを他のお客様またはサードパーティ組織と共有しません。

Device（デバイス）> **Setup**（セットアップ）> **Telemetry**（テレメトリー）を選択し、Palo Alto Networks と共有するテレメトリー データを選択します。Threat Prevention Data（脅威防御データ）およびThreat Prevention Packet Captures（脅威防御パケットキャプチャ）レポートは、ユーザーのネットワーク トラフィックに関して他のテレメトリー レポートよりも詳細な情報を Palo Alto Networks に提供します。

テレメトリー設定	の意味
Report Sample（レポート サンプル）	Report Sample（レポート サンプル）（ ）をクリックすると、XML 形式のレポートが別のタブに表示されます。レポート サンプル内のデータは、レポート サンプルを最初に表示してから 4 時間のファイアウォール アクティビティに基づきます。ファイアウォールは、アプリケーション、脅威防御、URL、および ファイル タイプ識別レポートのレポート サンプルのみを提供します。 1 つのレポートを複数のレポートで構成することができます。 • **Type**（タイプ）– レポートの名前を説明します。 • **Aggregate**（集約）– レポート用にファイアウォールが収集するログ フィールドのリストを表示します（ファイアウォール ログに表示されたときの フィールドの名前については、「Syslog Field Descriptions（Syslog 項目の説明）」を参照）。 • **Values**（値）– レポートで使用する測定単位を示します（たとえば、攻撃国 レポートの値「**count**」は、特定の国に関連付けられた脅威イベントがファイアウォールで検出された回数を意味します）。 レポート用の一致するトラフィックがファイアウォールで検出されなかった場合、レポート サンプルにそのエントリは表示されません。新しいレポート サンプルは、ファイアウォールを再起動した場合にのみ生成されます。
アプリケーション レポート （デフォルトでは無効）	宛先ポートでグループ化された既知のアプリケーション、宛先ポートでグループ化された未知のアプリケーション、および宛先 IP アドレスでグループ化された未知のアプリケーションの数とサイズを共有します。ファイアウォールはこのレポートをトラフィック ログから生成します。 有効にすると、ファイアウォールはアプリケーション レポートを 4 時間おきに送信します。

© 2019 Palo Alto Networks, Inc.

テレメトリー設定	の意味
脅威防御レポート （デフォルトでは無効）	攻撃元の国と宛先ポートごとの脅威数、攻撃者情報のほか、ファイアウォールがこのレポートのデータを収集しているときに脅威イベントによりトリガーされた相関オブジェクトを共有します。 有効にすると、ファイアウォールは脅威防御レポートを 4 時間おきに送信します。
URL レポート （デフォルトでは無効）	マルウェア、フィッシング、動的 DNS、プロキシ回避、疑わしい、待機中、および未知（PAN-DB でまだ分類されていない URL）の PAN-DB URL カテゴリに関して URL フィルタリング ログから生成されたレポートを共有します。ファイアウォールは、URL レポートのデータを収集した時点の PAN-DB 統計も送信します。この統計には、ファイアウォールおよび PAN-DB クラウド上の URL フィルタリング データベースのバージョン、そのデータベース内の URL の数、ファイアウォールで分類した URL の数が含まれます。この統計は、ファイアウォールが URL レポートを送信した時間に基づきます。 有効にすると、ファイアウォールは URL レポートを 4 時間おきに送信します。
ファイル タイプ識別レポート （デフォルトでは無効）	データ フィルタリングとファイル ブロッキングの設定に基づいてファイアウォールで許可またはブロックされたファイルに関するレポートを共有します。 有効にすると、ファイアウォールはファイル タイプ識別レポートを 4 時間おきに送信します。
脅威防御データ （デフォルトでは無効）	Palo Alto Networks で評価しているシグネチャをトリガーした脅威イベントのログを共有します。収集された情報に、攻撃元と被害者の IP アドレスが含まれている場合があります。このオプションを有効にすると、（Palo Alto Networks が現在テストしている）未リリースのシグネチャをバックグラウンドで実行することもできます。このシグネチャはユーザーのセキュリティ ポリシー ルールおよびファイアウォール ログに影響せず、ファイアウォールのパフォーマンスにも影響しません。 有効にすると、ファイアウォールは脅威防御データを 5 分おきに送信します。**Download Threat Prevention Data**（脅威防御データのダウンロード）（ ）をクリックすると、ファイアウォールから Palo Alto Networks に送信された脅威防御データおよび脅威防御パケットキャプチャの最新の 100 フォルダを含む tarball ファイル（.tar.gz）がダウンロードされます。これらの設定を有効にしていない場合、またはこれらの設定を有効にしていてもこのテレメトリー設定の条件に一致する脅威イベントがない場合、ファイアウォールはファイルを生成せず、代わりにエラー メッセージを返します。
脅威防御パケット キャプチャ （デフォルトでは無効）	Palo Alto Networks で評価しているシグネチャをトリガーした脅威イベントからのパケット キャプチャを共有します（脅威パケット キャプチャを取得するようにファイアウォールを有効にしている場合）。収集された情報に、攻撃元と被害者の IP アドレスが含まれている場合があります。 有効にすると、ファイアウォールは脅威防御パケットキャプチャを 5 分おきに送信します。 脅威防御パケット キャプチャを有効にするには、脅威防御データも有効にする必要があります。

© 2019 Palo Alto Networks, Inc.

テレメトリー設定	の意味
Product Usage Statistics（製品使用率統計） （デフォルトでは無効）	失敗したファイアウォール プロセスのバック トレースおよびファイアウォールの状態に関する情報を共有します。バック トレースは、失敗したプロセスの実行履歴の概要を示します。製品使用率統計には、ファイアウォール モデルと PAN-OS に関する詳細、およびファイアウォールにインストールされているコンテンツ リリース バージョンも含まれます。 ファイアウォールから製品使用率統計として送信される情報を表示するには、次の CLI 操作コマンドを入力します。 `show system info` 有効にすると、ファイアウォールは製品使用率統計を 5 分おきに送信します。
パッシブ DNS モニタリング （デフォルトでは無効）	ファイアウォールをパッシブ DNS センサーとして機能させ、分析目的で DNS 情報を Palo Alto Networks に送信できます。パッシブ DNS モニタリングを介して共有するデータは、ドメインと IP アドレス間のマッピングのみで構成されます。Palo Alto Networks の脅威研究チームは、この情報を使用して、PAN-DB URL カテゴリと DNS ベースの C2 シグネチャの正確性、および WildFire マルウェアの検出を向上します。パッシブ DNS モニタリングは、すべてのファイアウォール トラフィックに適用されるグローバル設定です。 有効にすると、ファイアウォールはパッシブ DNS モニタリング データを 1MB ずつ送信します。
すべて選択	すべてのテレメトリー設定を有効にします。
すべての選択を解除	すべてのテレメトリー設定を無効にします。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Content-ID [デバイス > セットアップ > Content-ID]

Content-ID™ タブを使用して、URL フィルタリング、データ保護、およびコンテナ ページの設定を定義します。

Content-ID設定	の意味
URL フィルタリング	
Dynamic URL cache Timeout	**Edit (編集)** をクリックし、タイムアウト値 (時間単位) を入力します。この値はダイナミック URL フィルタリングで使用され、この値により、エントリが URL フィルタリング サービスから返された後にキャッシュに保持される期間が決定します。このオプションは、BrightCloud データベースのみを使用する URL フィルタリングに適用されます。URL フィルタリングの詳細については、 Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]を選択してください。
URL コンティニュー タイムアウト	同一カテゴリの URL に対して Continue (続行) を再度押す前に、ユーザーが **Continue (続行)** アクションに従う間隔を指定します (範囲は 1 ～ 86,400 分、デフォルトは 15)。
URL 管理オーバーライド タイムアウト	ユーザーが **Admin Override (管理オーバーライド)** パスワードを入力してから、ユーザーが同じカテゴリの URL のパスワードを再入力するまでの間隔を指定します (範囲は 1 ～ 86,400 分、デフォルトは15 分)。
カテゴリ検索のクライアント要求を保持	このオプションを有効にすると、ファイアウォールがローカル キャッシュで URL のカテゴリ情報を見つけられない場合に、PAN-DB にクエリを送信するときに Web 要求を保持するように指定できます。 このオプションはデフォルトでは無効になっています。ベスト プラクティスの URL フィルタリング プロファイルの一部として有効にします。
カテゴリ検索タイムアウト (秒)	カテゴリが 未解決であると判断する前に、ファイアウォールが URL のカテゴリの検索を試行する時間を秒単位で指定します (範囲は 1 ～ 60 秒、デフォルトは 2) 。
URL 管理ロックアウト タイムアウト	3 回失敗した後、ユーザーが URL Admin Override (URL 管理オーバーライド) パスワードの使用をロックアウトされる期間を指定します (範囲は 1 ～ 86,400 分、デフォルトは 30 分)。
PAN-DB サーバー (プライベート PAN-DB サーバーに接続する場合に必須)	ネットワーク上のプライベート PAN-DB サーバーの IPv4 アドレス、IPv6 アドレス、または FQDN を指定します。最大 20 エントリを追加できます。 デフォルトでは、ファイアウォールはパブリック PAN-DB クラウドに接続します。プライベート PAN-DB ソリューションは、ファイアウォールがパブリック クラウド内の PAN-DB サーバーに直接アクセスすることを許可しないエンタープライズ向けです。ファイアウォールは、URL データベース、URL

© 2019 Palo Alto Networks, Inc.

Content-ID設定	の意味
	更新、URL 検索で Web ページを分類できるように、この PAN-DB サーバーのリストに含まれるサーバーにアクセスします。
URL 管理オーバーライド	
URL 管理オーバーライドの設定	URL 管理オーバーライド用に構成する 仮想システム ごとに、 **Add** (追加) して、URL フィルタリング プロファイルがページをブロックし、 **Override** (オーバーライド) アクションが指定されている場合に適用される設定を指定します。詳細については、 Objects > Security Profiles > URL Filtering [オブジェクト > セキュリティ プロファイル > URL フィルタリング]を参照してください。 • **Location** (場所)–(マルチvsys ファイアウォールのみ) ドロップダウンから 仮想システム を選択します。 • **Password/Confirm Password** [パスワード/パスワード再入力] – ブロック ページをオーバーライドするためにユーザーが入力する必要があるパスワードを入力します。 • **SSL/TLS Service Profile**[SSL/TLS サービス プロファイル] – 指定したサーバーを介してリダイレクトするときに通信を保護するための証明書および許可された TLS プロトコル バージョンを指定するには、SSL/TLS サービス プロファイルを選択します。詳細は、「Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル]」を参照してください。 • **Mode**[モード] – ブロック ページが透過的に配信されるか (ブロックされた Web サイトから発信したように見える)、指定したサーバーにユーザーをリダイレクトするかを決定します。**Redirect** (リダイレクト)を選択した場合、次に、リダイレクトするための IP アドレスを入力します。 エントリを **Delete** (削除) することもできます。
Content-ID設定	
復号化されたコンテンツの転送を許可	このオプションを有効にすると、ポート ミラーリングまたは解析のために WildFire® にファイルを送信するときに、復号化されたコンテンツを外部サービスに転送するようにファイアウォールを設定することができます。 このオプションを有効化し、復号化されたトラフィック内のすべての未知のファイルを *WildFire* に送信して分析を行います。 マルチ仮想システム (multi-vsys) 機能が有効化されているファイアウォールの場合、このオプションを仮想システムごとに個々に有効にします。**Device** (デバイス) > **Virtual Systems** (仮想システム) を選択し、復号化されたコンテンツの転送を有効にする仮想システムを選択します。このオプションは、仮想システム ダイアログで使用できます。
拡張パケット キャプチャ長	Anti-Spyware (アンチスパイウェア) および Vulnerability Protection (脆弱性防御) プロファイルで拡張キャプチャ オプションが有効になっている場合にキャプチャするパケット数を設定します (範囲は 1 ~ 50、デフォルトは 5) 。
TCP App-ID™ 検査キューを超過するセグメントを転送	このオプションを有効にすると、App-ID キューが 64 セグメントの制限を超えたときに、セグメントが転送され、アプリケーションが `unknown-tcp` として分類されます。このオプションが有効であるか無効であるかに関らず、

© 2019 Palo Alto Networks, Inc.

Content-ID設定	の意味
	このキューを超過したセグメント数を確認するには、以下のグローバル カウンターを使用します: `appid_exceed_queue_limit` ファイアウォールがTCPセグメントを転送しつつも、App-ID検査キューに空きが無いためApp-ID検査が省略されるということを防ぎたい場合はこのオプションを選択してください。 このオプションはデフォルトで無効化されています。最大限のセキュリティを確保するには、このオプションを無効のままにしておく必要があります。 このオプションを無効にすると、*64* を超えるセグメントがキューに追加され *App-ID* の処理を待っている場合、そのストリームで待機時間が増加する場合があります。

TCPコンテンツ検査キューを超過するセグメントを転送	このオプションを有効にすると、TCP セグメントが転送され、TCP コンテンツ検査キューがいっぱいになったときにコンテンツ検査がスキップされます。ファイアウォールはコンテンツエンジンからの応答を待つ間、64個のセグメントをキューに追加することができます。ファイアウォールがセグメントを転送し、コンテンツ検査キューに空きがないためにコンテンツ検査を省略した場合、次のグローバル カウンターの値が増加します。
	
	`ctd_exceed_queue_limit`
	
	ファイアウォールがTCPセグメントを転送しつつも、コンテンツ検査キューに空きが無いためコンテンツ検査が省略されるということを防ぎたい場合はこのオプションを選択してください。このオプションを無効にすると、ファイアウォールはキュー制限を超過したセグメントを破棄し、次のグローバル カウンターの値が増加します。
	
	`ctd_exceed_queue_limit_drop`
	
	これらのグローバルカウンターはTCPおよびUDPの両方のパケットに適用されます。グローバル カウンターを確認した後、設定を変更するように決定した場合は、CLI から次の CLI コマンドを使用して設定を変更できます。
	
	`set deviceconfig setting ctd tcp-bypass-exceed-queue`
	
	このオプションはデフォルトで有効になっていますが、最大限のセキュリティを確保するため、このオプションを無効化することをお勧めします。ただし、ドロップされたトラフィックの *TCP* 再送信が原因で、このオプションを無効にするとパフォーマンスが低下し、一部のアプリケーションで (特に、大量のトラフィックがある状況で) 機能が失われる可能性があります。

© 2019 Palo Alto Networks, Inc.

Content-ID設定	の意味

UDPコンテンツ検査キューを超過するデータグラムを転送	このオプションを有効にすると、UDP データグラムが転送され、UDP コンテンツ検査キューがいっぱいになったときにコンテンツ検査がスキップされます。ファイアウォールはコンテンツ エンジンからの応答を待つ間、64 個のデータグラムをキューに追加することができます。ファイアウォールがデータグラムを転送し、UDP コンテンツ検査キューのオーバーフローのためにコンテンツ検査を省略した場合、次のグローバル カウンターの値が増加します。
	
	`ctd_exceed_queue_limit`
	
	ファイアウォールがデータグラムを転送しつつも、UDPコンテンツ検査キューに空きが無いためコンテンツ検査が省略されるということを防ぎたい場合はこのオプションを選択してください。このオプションが無効化された場合、ファイアウォールは キュー制限を超過したデータグラムを破棄し、次のグローバル カウンターの値を 増加させます。
	
	`ctd_exceed_queue_limit_drop`
	
	これらのグローバルカウンターはTCPおよびUDPの両方のパケットに適用されます。グローバル カウンターを確認した後、設定を変更するように決定した場合は、CLI から次のコマンドを使用して設定を変更できます。
	
	`set deviceconfig setting ctd udp-bypass-exceed-queue`
	
	このオプションはデフォルトで有効になっていますが、最大限のセキュリティを確保するため、このオプションを無効化することをお勧めします。ただし、このオプションを無効化すると、パケットのドロップが原因でパフォーマンスが低下し、一部のアプリケーションで (特に大量のトラフィックがある状況で) 機能が失われる可能性があることに注意してください。

HTTP 部分レスポンスを許可する	この HTTP 部分応答 オプションにより、クライアントはファイルの一部のみを取得することができるようになります。転送の途中経路にある次世代ファイアウォールが悪意のあるファイルの検知と破棄を行った場合、RSTパケットにてTCPセッションを強制終了します。ブラウザにHTTPレンジオプションを実装すると、ファイルの残りの部分を取得するために新しいセッションを開始できるようになります。これにより、最初のセッションに対するコンテクストの欠損を理由にファイアウォールが同じシグネチャをトリガーしてしまうことを防ぐと同時に、ウェブブラウザでファイルを再構築し、悪意のあるファイルを転送することができます。これを防ぐには、必ずこのオプションを無効にしてください。 デフォルトでは、 *HTTP* 部分応答を許可 が有効になっていますが、*Palo Alto Networks* は、最大限のセキュリティを確保するためにこのオプションを無効にすることをお勧めします。このオプションを無効化してもデバイスのパフォーマンスに影響を与えるものではありませんが、*HTTP*ファイル転送中断後の復帰機能が阻害される可能性があります。このオプションを無効化すると、ストリーミング メディア サービス

© 2019 Palo Alto Networks, Inc.

Content-ID設定	の意味
	(Netflix、Microsoft の更新プログラム、*Palo Alto Networks* のコンテンツ更新など*)* にも影響する可能性があります。
リアルタイム シグネチャ検索	
DNS シグネチャ ルックアップのタイムアウト（ms）	ファイアウォールが DNS セキュリティ サービスにクエリを送る期間をミリ秒単位で指定します。指定した期間中にクラウドが応答しない場合、ファイアウォールはリクエストしたクライアントのために関連する DNS 応答をリリースします（範囲は 0 ~ 60,000、デフォルトは 80）。
X-Forwarded-For ヘッダ	
User-ID で X-Forwarded-For ヘッダを使用	このオプションを有効にすると、通常であればクライアントの IP アドレスを隠すプロキシ サーバーとインターネット間にファイアウォールがデプロイされている場合に、User-ID が Web サービスのクライアント要求の X-Forwarded-For（XFF）ヘッダーから IP アドレスを読み取るように指定できます。User-ID は、読み取った IP アドレスを、ポリシーで参照されているユーザー名と照合します。そのため、このポリシーを使用して、関連付けられているユーザーやグループのアクセスを制御してログに記録できます。ヘッダーに複数の IP アドレスが含まれている場合、User-ID は一番左側のエントリを使用します。 場合によって、ヘッダー値が IP アドレスではなく文字列になっていることがあります。文字列がユーザー名と一致し、User-ID がそのユーザー名を IP アドレスにマッピングしている場合、ファイアウォールはそのユーザー名をポリシー内のグループ マッピングの参照で使用します。該当の文字列の IP アドレス マッピングが存在しない場合、ファイアウォールは、送信元ユーザーを **any** または **unknown** に設定しているポリシー ルールを起動します。 URL フィルタリング ログの Source User（送信元ユーザー）フィールドに、一致したユーザー名が表示されます。User-ID が照合を実行できない場合、または IP アドレスに関連付けられたゾーンで User-ID が有効化されていない場合、Source User（送信元ユーザー）フィールドには、プレフィックス **`x-fwd-for`** 付きの XFF IP アドレスが表示されます。 *User-ID の XFF ヘッダーの使用を有効にして、問題を調査する必要があるときに役立つように、元のクライアント IP アドレスがログに表示されるようにします。*
X-Forwarded-For ヘッダの除去	このオプションを有効にすると、ファイアウォールがインターネットとプロキシ サーバー間にデプロイされている場合、Webサービスを要求しているクライアントのIPアドレスが含まれる X-Forwarded-For (XFF) ヘッダーが削除されます。ファイアウォールによって要求を転送する前にヘッダーの値がゼロに設定されるため、転送されるパケットには内部送信元 IP 情報が含まれなくなります。 このオプションを有効にした場合も、ポリシーのユーザー属性では *XFF* ヘッダーの使用は無効になりません。ファイアウォールは、ユーザー属性に使用した後でのみ *XFF* 値をゼロに設定します。

© 2019 Palo Alto Networks, Inc.

Content-ID設定	の意味
	User-ID での *XFF* ヘッダの使用を有効にすると、パケットを転送する前にユーザーを追跡する機能を損なうことなくユーザーのプライバシーを保護するために、*XFF* ヘッダのストリップも有効になります。両方のオプションを有効化することで、元の *IP* アドレスを転送しないことでユーザーのプライバシーを保護しつつ、元のユーザーの *IP* アドレスを追跡してログに記録できるようになります。
コンテンツ ID 機能	
データ保護の管理	クレジットカード番号や社会保障番号など重要な情報を含むログへのアクセスに対し拡張防御を追加します。 **Manage Data Protection** (データ保護の管理) をクリックして、以下のタスクを実行します。 • **Set Password** (パスワードの設定)—まだ設定されていない場合は、新しいパスワードを入力して確認します。 • **Change Password** (パスワードの変更)—以前のパスワードを入力し、新しいパスワードを入力して確認します。 • **Delete Password** (パスワードの削除)—パスワードと保護されていたデータを削除します。
Container Pages	コンテンツ タイプ (たとえば、application/pdf、application/soap+xml、application/xhtml+、text/html、text/plain、text/xml) に基づいてファイアウォールで追跡または記録する URL のタイプを指定するには、これらの設定を使用します。**Location** [場所] のドロップダウンリストから選択した仮想システムごとにコンテナページが設定されます。仮想システム に明示的なコンテナ ページが定義されていない場合、ファイアウォールはデフォルトのコンテンツ タイプを使用します。 **Add** (追加)してコンテンツ タイプを入力するか、既存のコンテンツ タイプを選択します。 仮想システムの新しいコンテンツ タイプを追加すると、コンテンツ タイプのデフォルトのリストがオーバーライドされます。仮想システムに関連付けられているコンテンツ タイプがない場合、コンテンツ タイプのデフォルトのリストが使用されます。

© 2019 Palo Alto Networks, Inc.

Device > Setup > WildFire [デバイス > セットアップ > WildFire]

ファイアウォールと Panorama で WildFire を設定するには、**Device**（デバイス）> **Setup**（セットアップ）> **WildFire** を選択します。WildFire クラウドと WildFire アプライアンスの両方を使用して、ファイル分析を実行できます。レポートされるファイル サイズ制限とセッション情報を設定することもできます。WildFire 設定を入力したら、**WildFire Analysis**（**WildFire** 分析）プロファイル（**Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **WildFire Analysis**（**WildFire** 分析））を作成して、WildFire クラウドまたは WildFire アプライアンスに転送するファイルを指定できます。

復号化されたコンテンツを *WildFire* に転送するには、「Forward Decrypted SSL Traffic for WildFire Analysis（復号化された SSL トラフィックを WildFire Analysis 用に転送する）」を参照してください。

WildFire 設定	の意味
一般設定	
WildFire パブリック クラウド	米国でホストされている WildFire グローバル クラウドに分析用のファイルを送信するには、**`wildfire.paloaltonetworks.com`** と入力します。または、WildFire 地域クラウドに分析用のファイルを送信することもできます。地域クラウドは、ユーザーの場所に応じて、ユーザーが期待するデータ プライバシーに準拠するように設計されています。 リージョナル *WildFire* クラウドにサンプルを転送し、データのプライバシーおよびコンプライアンスに関する現地特有の規則を確実に遵守できるようにします。リージョナル クラウド： • 欧州—***`eu.wildfire.paloaltonetworks.com`*** • 日本—***`jp.wildfire.paloaltonetworks.com`*** • シンガポール—***`sg.wildfire.paloaltonetworks.com`***
WildFire プライベート クラウド	WildFire アプライアンスの IP アドレスまたは FQDN を指定します。 ファイアウォールは、指定されたアプライアンスに分析用のファイルを送信します。 Panorama は脅威 ID を WildFire アプライアンスから収集します。これにより、デバイス グループで設定したアンチスパイウェア プロファイル（DNS シグネチャのみ）とアンチウイルス プロファイルに脅威の例外を追加できます。また、Panorama は WildFire アプライアンスから情報を収集し、PAN-OS 7.0 よりも前のソフトウェア バージョンを実行しているファイアウォールから受信した WildFire Submissions（WildFire への送信）ログで不足しているフィールドを入力できます。
ファイル サイズ制限	WildFire サーバーに転送される最大ファイル サイズを指定します。ファイルのサイズ制限に関するベストプラクティスのすべての推奨事項に関して、上限が大き過ぎてファイアウォールが複数の巨大なゼロデイ ファイルを同時に転送できない場合は、ファイアウォールで利用できるバッファ領域のサイズに基づいて調整を行い、上限を下げてください。バッファ領域が大きい場合は、ファイルサイズの上限をベストプラクティスの推奨事項よりも大きくすることができます。

© 2019 Palo Alto Networks, Inc.

WildFire 設定	の意味
	ファイアウォール リソースに負担をかけない有効な上限の設定として、最初に参考になるのがベストプラクティスの推奨事項です。指定可能な範囲は以下のとおりです。 • **pe**（Portable Executable）- 範囲は 1 ~ 50MB、デフォルトは 16MB です。 *PE ファイルのサイズを 16MB に設定します。* • **apk**（Android アプリケーション）- 範囲は 1 ~ 50MB、デフォルトは 10 MBです。 *APK ファイルのサイズを 10MB に設定します。* • **pdf**（ポータブル ドキュメント フォーマット）– 範囲は 100KB ~ 51,200KB、デフォルトは 3,072KB です。 *PDF ファイルのサイズを 3,072KB に設定します。* • **ms-office**（Microsoft Office）- 範囲は 200KB ~ 51,200KB、デフォルトは 16,384KB です。 *ms-office ファイルのサイズを 16,384KB に設定します。* • **jar**（パッケージ化された Java クラスファイル）- 範囲は 1 ~ 20MB、デフォルトは 5MB です。 *jar ファイルのサイズを 5MB に設定します。* • **flash**（Adobe Flash）- 範囲は 1 ~ 10MB、デフォルトは 5MB です。 フラッシュ ファイルのサイズを *5MB* に設定します。 • **MacOSX**（DMG/MAC-APP/MACH-O PKG ファイル）- 範囲は 1 ~ 50MB、デフォルトは 10MB です。 *MacOSX ファイルのサイズを 1MB に設定します。* • **archive**（RAR と 7z ファイル）- 範囲は 1 ~ 50MB、デフォルトは 50MB です。 アーカイブ ファイルのサイズを *50MB* に設定します。 • **linux**（ELF ファイル）- 範囲は 1 ~ 50MB、デフォルトは 50MB です。 *Linux ファイルのサイズを 50MB に設定します。* • **script (スクリプト)**（JScript、VBScript、PowerShell、Shell Script ファイル）–範囲は 10 ~ 4096KB、デフォルトは 20KB です。

© 2019 Palo Alto Networks, Inc.

WildFire 設定	の意味
	スクリプト ファイルのサイズを *20KB* に設定します。 実行中の*PAN-OS*のバージョンやコンテンツリリースにより、直前の値が変化する可能性があります。有効範囲を表示するには、*Size Limit* (サイズ制限) フィールドをクリックします。使用可能な範囲とデフォルト値がポップアップで表示されます。
安全なファイルのレポート	このオプションを有効にすると (デフォルトでは無効)、WildFire で分析され、安全と判定されたファイルが、**Monitor**[監視] > **WildFire Submissions** [**WildFire** への送信] ログに表示されます。 ファイアウォールでこのオプションが有効な場合でも、WildFire で安全と見なされた電子メール リンクは、処理されるリンクの量が多くなる可能性があるため、ログに記録されません。
レポートのグレイウェアファイル	このオプションを有効にすると (デフォルトでは無効)、WildFire で分析され、グレイウェアと判定されたファイルが、 **Monitor**[監視] > **WildFire Submissions** [**WildFire** への送信] ログに表示されます。 ファイアウォールでこのオプションが有効な場合でも、*WildFire* でグレイウェアと判定された電子メール リンクは、処理されるリンクの量が多くなる可能性があるため、ログに記録されません。 グレイウェア ファイルのレポートを有効化し、セッション情報、ネットワーク アクティビティ、ホスト アクティビティ、および分析に役立つその他の情報をログに記録します。
セッション情報設定	
設定	WildFire サーバーに転送する情報を指定します。デフォルト設定ではすべてが選択されており、次のような脅威イベントを防ぐ対策を行うために統計情報やその他の指標を得られるよう、すべてのセッション情報を転送することがベストプラクティスになります。 • **Source IP**[送信元 IP] – 疑わしいファイルを送信した送信元 IP アドレス。 • **Source Port**[送信元ポート] – 疑わしいファイルを送信した送信元ポート。 • **Destination IP**[宛先 IP] – 疑わしいファイルの宛先 IP アドレス。 • **Destination Port**[宛先ポート] – 疑わしいファイルの宛先ポート。 • **Vsys**[仮想システム] – 見込まれるマルウェアを識別したファイアウォール 仮想システム。 • **Application**[アプリケーション] – ファイルの送信に使用されたユーザー アプリケーション。 • **User**[ユーザー] – ターゲット対象のユーザー名。 • **URL** – 疑わしいファイルに関連付けられた URL。 • **Filename**[ファイル名] – 送信されたファイルの名前。 • **Email sender** [電子メール送信者] – SMTPおよびPOP3トラフィックで悪意のある電子メールリンクが検出されると、WildFireログとWildFireの詳細レポートに送信者名が表示されます。

© 2019 Palo Alto Networks, Inc.

WildFire 設定	の意味
	• **Email recipient** [電子メール受信者] — SMTPおよびPOP3トラフィックで悪意のある電子メールリンクが検出されると、WildFireログとWildFireの詳細レポートに受信者名が表示されます。 • **Email subject** [電子メール件名] — SMTPおよびPOP3トラフィックで悪意のある電子メールリンクが検出されると、WildFireログと WildFireの詳細レポートに電子メールの件名が表示されます。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Session [デバイス > セットアップ > セッション]

Device [デバイス } > **Setup** 設定 > **Session** [セッション] を開き、セッションのエイジアウト時間、復号化証明書設定、およびグローバルなセッション関連の設定 (IPv6トラフィックのファイアウォール設定、ポリシー変更時の既存のセッションへのセキュリティポリシーの再マッチングなど) を設定します。このタブには、以下のセクションがあります。

- セッション設定
- セッション タイムアウト
- TCP 設定
- 復号化設定:証明書取り消しチェック
- 復号化設定:フォワードプロキシサーバーの証明書設定
- VPN セッション設定

セッション設定

以下の表では、セッション設定について説明します。

セッション設定	の意味
セッションの再マッチング	ファイアウォールで、新しく設定されたセキュリティ ポリシーをすでに進行中のセッションに適用するには、**Edit**[編集] をクリックし、**Rematch Sessions**[セッションの再マッチング] を選択します。この機能はデフォルトで有効になっています。この設定が無効な場合、ポリシー変更は、ポリシー変更がコミットされた後に開始されたセッションにのみ適用されます。 たとえば、Telnet を許可する関連ポリシーが設定されているときに Telnet セッションを開始し、その後、Telnet を拒否するポリシー変更をコミットした場合、ファイアウォールは変更されたポリシーを現在のセッションに適用してブロックします。 *Rematch Sessions* (セッションの再マッチング)を有効化し、最新のセキュリティポリシーを現在アクティブなセッションに適用します。
ICMPv6 トークン バケット サイズ	ICMPv6 エラー メッセージの帯域制限に対応するバケット サイズを入力します。トークンバケットサイズは、ICMPv6エラーパケットのバーストをどの程度許容するかを制御するトークンバケットアルゴリズムのパラメータです (範囲は10 ~ 65535パケット、デフォルトは 100)。
ICMPv6 エラー パケット速度	ファイアウォール全体として1秒間に許容されるICMPv6エラーパケットの平均数を入力します (範囲は10 ~ 65535パケット/秒、デフォルトは100パケット/秒) 。この値はすべてのインターフェイスに適用されます。ファイアウォールが ICMPv6 エラー パケット速度に達した場合、ICMPv6 トークン バケットを使用して、ICMPv6 エラー メッセージのスロットリングが有効になります。
IPv6 ファイアウォールの有効化	IPv6のファイアウォール機能を有効化する場合は、**IPv6 Firewalling** [IPv6ファイアウォール設定] の**Edit** [編集] をクリックします。

© 2019 Palo Alto Networks, Inc.

セッション設定	の意味
	IPv6 が有効になっていないと、IPv6 ベースの設定はすべて無視されます。インターフェイスでIPv6が有効化されている場合も、IPv6 が機能するためには **IPv6 Firewalling** [IPv6ファイアウォール設定] 設定も有効にする必要があります。
Jumbo Frame を有効にする グローバル MTU	Ethernet インターフェイスでジャンボ フレームのサポートを有効にする場合に選択します。Jumbo Frame の最大伝送単位（MTU）は 9192 バイトで、特定のモデルで使用できます。 • **Enable Jumbo Frame** [Jumbo Frame を有効にする] をオフにすると、**Global MTU** [グローバルMTU] がデフォルトの1500バイトに設定されます（範囲は576 ~ 1,500）。 • **Enable Jumbo Frame**（**Jumbo Frame** を有効にする）をオンにすると、**Global MTU**（グローバル **MTU**）がデフォルトの 9,192 バイトに設定されます（範囲は 9,192 ~ 9,216 バイト）。 ジャンボ フレームは、通常のパケットと比較して最大 *5* 倍のメモリを消費し、利用可能なパケットバッファの数を *20%* 削減できます。これにより、順不同、アプリケーション識別、およびその他のそのようなパケット処理タスク専用のキューサイズが削減されます。*PAN-OS 8.1* 以降では、ジャンボ フレームのグローバル *MTU* 設定を有効にしてファイアウォールを再起動すると、パケット バッファが再配信されてジャンボ フレームをより効率的に処理します。 ジャンボ フレームが有効で、インターフェイスに具体的な MTU が設定されていない場合、それらのインターフェイスでは自動的にジャンボ フレームのサイズが継承されます。そのため、ジャンボ フレームを有効にする前に、ジャンボ フレームを使用しないインターフェイスがある場合、その MTU を 1500 バイトか別の値に設定する必要があります。インターフェイス (**Network** (ネットワーク) - > **Interfaces** (インターフェイス) - > **Ethernet** (イーサネット)) のMTU を構成するには、PA-7000 シリーズのレイヤー 3 インターフェイスを参照してください。
NAT64 IPv6 最小MTU	IPv6 変換済みトラフィックのグローバル MTU を入力します。デフォルトの 1280 バイトは、IPv6 トラフィックの標準の最小 MTU に基づきます。範囲は 1,280 ~ 9,216 です。
NAT オーバーサブスクリプション率	DIPP NAT オーバーサブスクリプション率を選択します。これは、同じ変換済み IP アドレスとポートのペアを同時に使用できる回数です。オーバーサブスクリプション率を小さくすると、送信元デバイス変換数が少なくなりますが、提供される NAT ルールのキャパシティは大きくなります。 • **Platform Default**（プラットフォームのデフォルト）– オーバーサブスクリプション率の明示的な設定はオフになり、モデルのデフォルトのオーバーサブスクリプション率が適用されます。ファイアウォール モデルのデフォルトの率については、https://www.paloaltonetworks.com/products/product-selection.html を参照してください。 • **1x** – 1 回。オーバーサブスクリプションは行われず、変換後の IP アドレスとポートのペアは、それぞれ一時点に 1 回のみ使用できます。 • **2x** – 2 回。 • **4x** – 4 回。 • **8x** – 8 回。

© 2019 Palo Alto Networks, Inc.

セッション設定	の意味
ICMP 到達不能パケット率/秒	ファイアウォールが 1 秒間に送信できる ICMP 到達不能応答の最大数を定義します。この制限は、IPv4 パケットと IPv6 パケットで共有されます。 デフォルト値は200メッセージ/秒です（範囲は1～65535）。
セッション保持時間自動短縮	アイドル状態のセッションの保持時間短縮を有効にします。 セッション保持時間短縮を有効にして、しきい値（%）と倍率を設定する場合はこのオプションを選択します。 セッション テーブルが **Accelerated Aging Threshold**[セッション保持時間短縮の開始しきい値] (% フル) に達すると、PAN-OS により **Accelerated Aging Scaling Factor**[セッション保持時間短縮倍率] がすべてのセッションのエージング計算に適用されます。デフォルトの短縮倍率は 2 で、保持時間短縮が設定されているアイドル時間の 2 倍の速さで行われます。設定されているアイドル時間を 2 で除算すると、タイムアウト時間が 1/2 に短縮されます。セッションの保持時間短縮を計算するために、PAN-OS では、（そのセッション タイプに）設定されているアイドル時間を短縮倍率で除算して、短縮されたタイムアウトを決定します。 たとえば、短縮倍率が10の場合、通常は3600秒後にタイムアウトするセッションが、10倍速い360秒（1/10の時間）でタイムアウトします。 保持時間短縮のしきい値を設定し、許容できるスケーリング要素を設定することで、セッション テーブルが一杯になり始めた際にセッション テーブルの空きを素早く作ります。
パケット バッファ保護	ベスト プラクティスとして、パケット バッファ保護をグローバルおよび各ゾーンで有効にして、ファイアウォール バッファを DoS 攻撃や攻撃的なセッションや送信元から保護します。このオプションは、システム リソースの不具合や正常なトラフィックが廃棄される原因となる不正なトラフィックや攻撃から、ファイアウォールの受信バッファを保護します。パケット バッファ保護は、問題のあるセッションを特定し、ランダム早期検出 (RED) を防御の最前線として使用し、乱用が続く場合はセッションを破棄するか、問題のある IPアドレスをブロックします。特定の IP アドレスから多量の小さいセッションもしくは急速なセッション作成（またはその両方）をファイアウォールが検出した場合、その IP アドレスをブロックします。 ファイアウォール パケット バッファの使用率のベースラインを計測してファイアウォールの能力を把握し、必ずファイアウォールのサイズが適切であることを確認し、攻撃以外ではバッファ使用率が急増しないようにしてください。 • **Alert (%)**（アラート（%））– このしきい値をパケット バッファの使用率が 10 秒より長い時間超えている場合、ファイアウォールはログ イベントを毎分作成します。パケット バッファ保護がグローバルな範囲で有効になると、ファイアウォールがログ イベントを生成します (範囲は 0% ～ 99%、デフォルトは50%)。値が 0% の場合、ファイアウォールはログ イベントを作成しません。デフォルトのしきい値から始め、必要に応じて値を調整します。 • **Activate (アクティベート) (%)**–このしきい値に到達すると、ファイアウォールは最も危険性の高いセッションの軽減を開始します (範囲は 0% ～ 99%、デフォルトは 50%)。値が 0% の場合、ファイアウォールは RED を適用しません。デフォルトのしきい値から始め、必要に応じて値を調整します。 • **Block Hold Time (ブロック保持時間) (秒)**–セッションが廃棄されるまで、または送信元 IPアドレスがブロックされるまでのセッションの継続時間 (秒単

© 2019 Palo Alto Networks, Inc.

セッション設定	の意味
	位) (範囲は 0 ～ 65,535、デフォルトは 60)。RED により軽減されたセッションをこのタイマーで監視して、設定済みのしきい値を超える使用率のバッファのプッシュが続いているかどうかを確認します。ブロック ホールド タイム経過後も不正な動作が継続する場合、セッションは廃棄されます。値が 0 の場合、ファイアウォールは、パケット バッファ保護に基づくセッション廃棄を実施しません。デフォルトの値から始めてパケット バッファの使用率を監視し、必要に応じて値を調整します。 • **Block Duration (ブロック期間) (秒)**—この時間 (秒) の間、廃棄されたセッションが廃棄されたままになるか、ブロックされた IPアドレスがブロックされたままとなります (範囲は 1 ～ 15,999,999 、デフォルトは 3,600)。IPアドレスを1時間ブロックすることがビジネス条件のペナルティとして厳しすぎる場合を除き、デフォルト値を使用してください。この場合、期間を短縮できます。パケット バッファの使用率を監視し、必要に応じて期間を調整します。 ネットワーク アドレス変換によってパケット バッファの使用率が増加することがあります。これによってバッファの使用率が影響を受ける場合は、ブロック ホールド タイムを短くして個々のセッションを早めにブロックしてブロック期間を減らし、背後の *IP* アドレスから来る他のセッションが不当にペナルティを受けないようにします。
マルチキャストルートの設定バッファ	マルチキャスト ルートの設定バッファを有効化する場合はこのオプションを選択してください (デフォルトでは無効) 。この機能は、対応するマルチキャスト グループにマルチキャスト ルートまたは転送情報ベース (FIB) エントリが存在しない場合、マルチキャスト セッションにおいてファイアウォールが最初のパケットを保存できるようにするものです。デフォルト設定において、ファイアウォールは新しいセッションの最初のマルチキャストパケットのバッファを行わず、代わりに、最初のパケットを使用してマルチキャストルートを確立します。これがマルチキャストトラフィックにおける通常の動作です。コンテンツサーバーがファイアウォールに直接接続され、使用しているカスタムアプリケーションがセッションの最初のパケットが破棄されているケースに対応できない場合にのみ、マルチキャストルートの設定バッファを有効化する必要があります。
マルチキャストルートの設定バッファサイズ	マルチキャスト ルートの設定バッファを有効化した場合は、バッファ サイズを調整し、フローごとのバッファ サイズを指定することが可能です (範囲は 1 ～ 2,000、デフォルトは 1,000) 。 ファイアウォールは最大で5,000パケットをバッファすることができます。

セッション タイムアウト

セッション タイムアウト設定では、ファイアウォール上でセッションが非アクティブになってから PAN-OS がそのセッションを保持する期間を定義します。デフォルトでは、プロトコルのセッション タイムアウト期間が切れると、PAN-OS がセッションを閉じます。破棄セッション タイムアウトは、PAN-OS がセキュリティ ポリシー ルールに基づいてセッションを拒否した後も、セッションが開いたままになる最大時間を定義します。

ファイアウォールでは、特に TCP、UDP、ICMP、および SCTP セッションに対して複数のタイムアウトを定義できます。他のすべてのタイプのセッションには、**Default** (デフォルト) のタイムアウトが適用されます。これらのタイムアウトはすべてグローバルです。つまり、ファイアウォール上にあるそのタイプのすべてのセッションに適用されます。

© 2019 Palo Alto Networks, Inc.

グローバル設定に加え、**Objects**（オブジェクト）> **Applications**（アプリケーション）タブでは個々のアプリケーションのタイムアウトを柔軟に定義できます。そのアプリケーションで使用可能なタイムアウトは、Options [オプション] ウィンドウに表示されます。ファイアウォールは、アプリケーションのタイムアウトを確立済み状態のアプリケーションに適用します。アプリケーションのタイムアウトが設定されると、グローバルな TCP、UDP、または SCTP セッション タイムアウトがオーバーライドされます。

このセクションのオプションを使用して、TCP、UDP、ICMP、および SCTP 固有の、ならびにその他すべてのタイプのセッションのグローバル セッション timeout settings（タイムアウト設定）を定義します。

最適なのはデフォルトの値であり、デフォルトの値を使用することがベストプラクティスになります。ただし、ネットワークのニーズに合わせてこれらの値を変更できます。低すぎる値を設定すると、わずかなネットワーク遅延に反応してファイアウォールとの接続の確立に失敗する可能性があります。高すぎる値を設定すると、エラーの検出が遅れる可能性があります。

Session Timeouts Settings（セッション タイムアウト設定）	の意味
Reset Both [デフォルト]	非 TCP/UDP、非 SCTP、または非 ICMP のセッションが応答なしで開いた状態を維持できる最大秒数です（範囲は 1 ~ 15,999,999、デフォルトは 30）。
デフォルトの破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に非 TCP / UDP / SCTP セッションが開いたままになる最大時間（秒単位）（範囲は1〜15,999,999、デフォルトは 60）。
TCP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に TCP セッションが開いたままになる最大時間（秒単位）（範囲は1〜15,999,999、デフォルトは 90）。
UDP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に UDP セッションが開いたままになる最大時間（秒単位）（範囲は1〜15,999,999、デフォルトは 60）。
ICMP	ICMP セッションが ICMP 応答なしで開いた状態を維持できる最大時間です（範囲は 1 ~ 15,999,999、デフォルトは 6）。
スキャン	ファイアウォールがセッションをクリアし、セッションが使用していたバッファ リソースを回復するまでに、セッションが非アクティブでいられる最長時間 (秒単位)。非アクティブ時間とは、セッションがパケットまたはイベントによって最後に更新されてから経過した時間のことです。(範囲は 5 ~ 30、デフォルトは 10)
TCP	TCP セッションが Established（確立済み）状態になってから（ハンドシェークが完了し、必要に応じてデータ伝送が開始してから）応答なしで開いた状態を維持する最大時間です（範囲は 1 ~ 15,999,999、デフォルトは 3,600）。
TCP ハンドシェーク	SYN-ACK を受信してからそれに続く ACK を送信してセッションを完全に確立するまでの最大秒数です（範囲は 1 ~ 60、デフォルトは 10）。
TCP初期設定	SYN を受信してから SYN-ACK を送信して TCP ハンドシェーク タイマーを開始するまでの最大秒数です（範囲は 1 ~ 60、デフォルトは 5）。
TCPハーフクローズド	1 つ目の FIN を受信してから 2 つ目の FIN または RST を受信するまでの最大秒数です（範囲は 1 ~ 604,800、デフォルトは 120）。

© 2019 Palo Alto Networks, Inc.

Session Timeouts Settings（セッション タイムアウト設定）	の意味
TCP待ち時間	2 つ目の FIN または RST を受信してからの最大秒数です（範囲は 1 ~ 600、デフォルトは 15）。
未検証のRST	検証できない RST（RST が TCP ウィンドウ内にあるが予期しないシーケンス番号が付けられているか、RST が非対称パスから送信されている）を受信してからの最大秒数です（範囲は 1 ~ 600、デフォルトは 30）。
UDP	UDP セッションが UDP 応答なしで開いた状態を維持する最大秒数です（範囲は 1 ~ 1,599,999、デフォルトは 30）。
キャプティブ ポータル	キャプティブ ポータル Web フォームの認証セッションのタイムアウト秒数です（デフォルトは 30、範囲は 1 ~ 1,599,999）。要求されたコンテンツにユーザーがアクセスするには、このフォームに認証資格情報を入力して正常に認証される必要があります。 キャプティブ ポータル Web フォームの認証セッションのタイムアウト秒数です（デフォルトは 30、範囲は 1 ~ 1,599,999）。要求されたコンテンツにユーザーがアクセスするには、このフォームに認証資格情報を入力して正常に認証される必要があります。
SCTP 初期化	ファイアウォールが SCTP アソシエーションの開始を停止する前に、ファイアウォールが INIT ACK チャンクを受信する必要がある SCTP INIT チャンクを受信した最大時間（秒単位）（範囲は1～60、デフォルトは 5）。
SCTP COOKIE	ファイアウォールが SCTP アソシエーションの開始を停止する前に、ファイアウォールがクッキーを使用して COOKIE ECHO チャンクを受信する必要がある状態 COOKIE パラメータの SCTP INIT ACK チャンクを受信した最大時間（秒単位）（デフォルトは 60 ）。
SCTP の破棄	ファイアウォールで設定されたセキュリティ ポリシー ルールに基づき、PAN-OS がセッションを拒否した後に SCTP アソシエーションが開いたままになる最大時間（秒単位）（範囲は1～604,800、デフォルトは 30）。
SCTP	アソシエーションのすべてのセッションがタイムアウトする前に、アソシエーションの SCTP トラフィックなしで経過できる最大時間（秒単位）（範囲は1～604,800、デフォルトは3,600）。
SCTP シャットダウン	ファイアウォールが SHUTDOWN チャンクを無視する前に SHUTDOWN ACK チャンクを受け取るために SCTP SHUTDOWN チャンクが待機した後にファイアウォールが待機する最大時間（秒単位）（範囲は1～600、デフォルトは 30）。

TCP 設定

以下の表では、TCP 設定について説明します。

© 2019 Palo Alto Networks, Inc.

TCP 設定	の意味
TCP順序外キューを超過するセグメントを転送	ファイアウォールがTCP順序外キュー上限（1つのセッションあたり64個）を超えるセグメントを転送するように設定したい場合はこのオプションを選択してください。このオプションを無効化すると、ファイアウォールは順序外キュー上限を超えるセグメントを破棄します。このオプションが有効であることによりファイアウォールが廃棄したセグメント数を確認する場合は、以下の CLI コマンドを実行します。 `show counter global tcp_exceed_flow_seg_limit` このオプションはデフォルトで無効になっており、多くのセキュア デプロイにおいては設定をそのままにしてください。このオプションを無効化すると、順序外セグメントを*64*個以上を受信する特定のストリームで遅延が発生する可能性があります。*TCP* スタックは欠落しているセグメントのリトランスミッションを処理するため、接続が失われることはありません。
タイムスタンプオプションを持たないセグメントを破棄	TCPタイムスタンプにはセグメントの送信日時が記録されているので、ファイアウォールはそのタイムスタンプがセッションに対して有効であるかどうか確認できるので、TCPシーケンス番号のラッピングを防止することができます。TCPタイムスタンプはラウンドトリップ時間の算出にも使用されます。このオプションが有効な場合、ファイアウォールはタイムスタンプが Null のパケットを廃棄します。このオプションが有効であることによりファイアウォールが廃棄したセグメント数を確認する場合は、以下の CLI コマンドを実行します。 `show counter global tcp_invalid_ts_option` このオプションはデフォルトで有効になっており、多くのセキュア デプロイにおいては設定をそのままにしてください。このオプションを有効化するとパフォーマンスが低下するという訳ではありません。ただし、ネットワーク スタックが誤って *Null TCP* タイムスタンプ オプション値でセグメントを生成している場合、このオプションが有効であることで接続の問題が発生する可能性があります。
緊急データフラグ	TCPヘッダーに含まれる緊急ポインター（URGビットフラグ）をファイアウォールに許容させる場合はこのオプションを使用してください。TCPヘッダー内の緊急ポインターは、パケットを即時に処理させる場合に使用され、パケットが緊急ポインターを持つ場合、ファイアウォールはパケットを処理キューから外し、ホストのTCP/IPスタックで迅速に処理を行います。この処理はアウトオブバンド処理と呼ばれます。 緊急ポインターの実装はホストによって異なるため、このオプションを **Clear**（クリア）に設定することで、アウトオブバンド処理を却下し、処理の不画一性を排除できます（デフォルト、および推奨設定）。ペイロード内のアウトオブバンドのバイトはペイロードの一部となり、パケットの緊急処理は行われません。また、**Clear**（クリア）に設定することで、プロトコル スタック内のストリームをパケットの宛先ホストとして、ファイアウォールに確実かつ正確に認識させることができます。このオプションが **Clear**（クリア）に設定されている間

© 2019 Palo Alto Networks, Inc.

TCP 設定	の意味
	にファイアウォールが URG フラグを削除したセグメント数を確認する場合は、以下の CLI コマンドを実行します。 `show counter global tcp_clear_urg` デフォルトでは、このフラグは *Clear*（クリア）に設定されており、多くのセキュア デプロイにおいては設定をそのままにしてください。これはパフォーマンス低下につながるものではありませんが、ごく稀に、*telnet* などのアプリケーションが緊急データ機能を使用しているような場合は *TCP* に影響する可能性があります。このフラグを *Do Not Modify*（編集不可）に設定する場合、ファイアウォールは *TCP* ヘッダーに *URG* ビット フラグを持つパケットを許容し、アウトオブバンド処理が有効化されます（非推奨）。
フラグを持たないセグメントを破棄	フラグを持たない不正なTCPセグメントはコンテンツ検査の回避に使用される場合があります。このオプションが有効な場合（デフォルト）、ファイアウォールは TCP ヘッダーにフラグが設定されていないパケットを廃棄します。このオプションによりファイアウォールが廃棄したセグメント数を確認する場合は、以下の CLI コマンドを実行します。 `show counter global tcp_flag_zero` このオプションはデフォルトで有効になっており、多くのセキュア デプロイにおいては設定をそのままにしてください。このオプションを有効化するとパフォーマンスが低下するという訳ではありません。しかし、*TCP*フラグを持たないセグメントをネットワークスタックが誤って生成している場合、このオプションを設定すると接続に問題が発生する可能性があります。

復号化設定:証明書取り消しチェック

Session [セッション] タブのDecryption Settings [復号化設定] から**Certificate Revocation Checking** [証明書失効チェック] を選択し、以下の表に記載されているパラメータを設定します。

セッション機能:証明書取り消しチェック設定	の意味
有効化:CRL	証明書無効リスト（CRL）方式を使用して証明書の失効状態を検証する場合は、このオプションを選択します。 オンライン証明書状態プロトコル (OCSP) も有効にしている場合、ファイアウォールは最初に OCSP を試行し、OCSP サーバーが使用できない場合は CRL 方式を試行します。 復号化証明書の詳細は「Keys and Certificates for Decryption（復号化のキーと証明書）」を参照してください。

© 2019 Palo Alto Networks, Inc.

セッション機能:証明書取り消しチェック設定	の意味
受信のタイムアウト:CRL	証明書失効状態の検証用に CRL 方式を有効にしている場合、ファイアウォールが CRL サービスからの応答を待つ秒数（1 ~ 60、デフォルトは 5）を指定します。
有効化:OCSP	OCSPを使用して証明書の失効状態を検証する場合は、このオプションを選択します。
受信のタイムアウト:OCSP	証明書失効状態の検証用に OCSP 方式を有効にしている場合、ファイアウォールが OCSP レスポンダからの応答を待つ秒数（1 ~ 60、デフォルトは 5）を指定します。
証明書の状態が不明なセッションをブロックします	OCSPまたはCRLサービスから証明書の失効状態が不明と返された際に、SSL/TLSセッションをブロックする場合は、このオプションを選択してください。その他の場合は、ファイアウォールはセッションを続行します。
証明書の状態のチェックがタイムアウトしたセッションをブロックします	ファイアウォールがCRLまたはOCSP要求のタイムアウトを登録した際に、SSL/TLSセッションをブロックする場合はこのオプションを選択します。その他の場合は、ファイアウォールはセッションを続行します。
証明書の有効期限	ファイアウォールが任意の証明書状態サービスからの応答を待機する秒数（1 ~ 60、デフォルトは 5）を指定します。この期間が終了すると、定義済みのセッション ブロック ロジックが必要に応じて適用されます。**Certificate Status Timeout**[証明書の有効期限] は、以下のように OCSP/CRL の **Receive Timeout**[受信の有効期限] に関連付けられます。 • OCSP および CRL の両方を有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または 2 つの **Receive Timeout**[受信の有効期限] の値の合計のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。 • OCSP のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または OCSP の **Receive Timeout**[受信の有効期限] の値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。 • CRL のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] 値または CRL の **Receive Timeout**[受信の有効期限] 値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。

復号化設定:フォワード プロキシ サーバーの証明書設定

Decryption Settings（復号化設定）（**Session**（セッション） タブ）で、**SSL Forward Proxy Settings**（**SSL** 転送プロキシ設定）を選択し、SSL/TLS Forward Proxy（SSL/TLS 転送プロキシ）復号化のセッションを確立する時の **RSA Key Size**（**RSA** キーのサイズ）または **ECDSA Key Size**（**ECDSA** キーのサイズ）およびファイアウォールがクライアントに対して作動する認証のハッシュ アルゴリズムを設定します。以下の表で、パラメータについて説明します。

© 2019 Palo Alto Networks, Inc.

セッション機能:フォワード プロキシ サーバーの証明書設定	

RSA キーのサイズ	以下のいずれかを選択します。
	• **Defined by destination host**（宛先ホストによる定義）（デフォルト）— 宛先サーバーが使用する鍵に基づいてファイアウォールで証明書を生成する場合は、このオプションを選択します。
	  • 宛先サーバーが RSA 1,024 ビット鍵を使用する場合、ファイアウォールはその鍵のサイズと SHA1 ハッシュ アルゴリズムを使用して証明書を生成します。
	  • 宛先サーバーが 1,024 ビットよりも大きい鍵のサイズを使用する場合（2,048 ビットや 4,096 ビットなど）、ファイアウォールは、2,048 ビット鍵と SHA-256 アルゴリズムを使用する証明書を生成します。
	• **1024** ビット **RSA**（**1024** ビット **RSA**）— 宛先サーバーが使用する鍵のサイズに関係なく、PAN-OS で RSA 1,024 ビット鍵と SHA1 アルゴリズムを使用する証明書を生成する場合は、このオプションを選択します。2013 年 12 月 31 日以降、公開認証局（CA）と一般的なブラウザでは、2048ビット未満のキーを使用するX.509証明書のサポートが制限されています。将来的にブラウザでは、セキュリティの設定に応じて、このような鍵が提示された場合、ユーザーに警告を表示したり、SSL/TLS セッション全体をブロックしたりする可能性があります。
	• **2048** ビット **RSA**（**2048** ビット **RSA**）— 宛先サーバーが使用する鍵のサイズに関係なく、PAN-OS で RSA 2048 ビット鍵と SHA256 アルゴリズムを使用する証明書を生成する場合は、このオプションを選択します。公開 CA と一般的なブラウザでは、2048 ビット鍵よりも強固なセキュリティを提供する 1024 ビット鍵がサポートされています。

ECDSA キーのサイズ	以下のいずれかを選択します。
	• **Defined by destination host**（宛先ホストによる定義）（デフォルト）— 宛先サーバーが使用する鍵に基づいてファイアウォールで証明書を生成する場合は、このオプションを選択します。
	  • 宛先サーバーが ECDSA 256 ビットまたは 384 ビット鍵を使用する場合、ファイアウォールはその鍵のサイズを使用して証明書を生成します。
	  • 宛先サーバーが 384 ビットよりも大きい鍵のサイズを使用する場合、ファイアウォールは、521 ビット鍵を使用する証明書を生成します。
	• **256** ビット **ECDSA**（**256** ビット **ECDSA**）— 宛先サーバーが使用する鍵のサイズに関係なくファイアウォールで ECDSA 256 ビット鍵を使用する証明書を生成する場合は、このオプションを選択します。
	• **384** ビット **ECDSA**（**384** ビット **ECDSA**）— 宛先サーバーが使用する鍵のサイズに関係なくファイアウォールで ECDSA 384 ビット鍵を使用する証明書を生成する場合は、このオプションを選択します。

VPN セッション設定

Session [セッション] を開き、VPN Session Settings [VPNセッション設定] から、VPNセッションを確立するファイアウォールに関連するグローバル設定を指定します。以下の表では、この設定について説明します。

© 2019 Palo Alto Networks, Inc.

VPN セッション設定	の意味
Cookie アクティベーションのしきい値	ファイアウォールごとの IKEv2 ハーフオープン IKE SA の最大許容数を指定します。これを超えると、Cookie の検証がトリガーされます。ハーフオープン IKE SA の数が Cookie アクティベーションのしきい値を超えると、レスポンダが Cookie を要求し、イニシエータは Cookie が含まれる IKE_SA_INIT で応答する必要があります。Cookie の検証に成功すると、別の SA セッションを開始できます。 値を 0 にすると、Cookie の検証が常にオンになります。 グローバル ファイアウォール設定の Cookie Activation Threshold（Cookie アクティベーションのしきい値）は、同様にグローバル設定である Maximum Half Opened SA（ハーフ オープン SA の最大数）（範囲は 0 ~ 65535、デフォルトは 500）未満とする必要があります。
ハーフ オープン SA の最大数	応答を取得せずにイニシエータがファイアウォールに送信できる IKEv2 ハーフオープン IKE SA の最大数を指定します。最大数に達すると、ファイアウォールは新しい IKE_SA_INIT パケットに応答しなくなります（範囲は 1 ~ 65535、デフォルトは 65535）。
キャッシュされた証明書の最大数	ファイアウォールがキャッシュできる、HTTP 経由で取得したピア認証局 (CA) 証明書の最大数を指定します。この値は、IKEv2 ハッシュおよび URL 機能でのみ使用されます（範囲は 1 ~ 4000、デフォルトは 500）。

© 2019 Palo Alto Networks, Inc.

Device > High Availability [デバイス > 高可用性]

- Device > High Availability [デバイス > 高可用性]

冗長性を確保するため、Palo Alto Networks 次世代ファイアウォールを高可用性設定でデプロイします。HAのデプロイには2つの種類があります。

- active/passive (アクティブ/パッシブ) – このデプロイ環境では、アクティブ ピアは 2 つの専用インターフェイスを通じて、設定内容とセッション情報をパッシブ ピアへ継続的に同期させます。アクティブなファイアウォールのハードウェアまたはソフトウェアにおいて障害が発生した場合、サービスを停止させることなく、パッシブなファイアウォールが自動的にアクティブに切り替わります。アクティブ/パッシブのHA導入環境は、バーチャルワイヤー、レイヤー2、またはレイヤー3のすべてのインターフェイスモードでサポートされています。
- active/active (アクティブ/アクティブ) – このデプロイ環境では、両方の HA ピアがアクティブに設定されトラフィックの処理を行います。このような導入環境は非対称的なルーティングを行っている場合や、動的ルーティングプロトコル (OSPF、BGP) に両方のピアをアクティブに保たせたい場合に適しています。アクティブ/アクティブHAは、バーチャルワイヤーモードとレイヤー3モードのみにおいてサポートされます。アクティブ/アクティブの導入環境では、HA1リンクとHA2リンクに加え、専用のHA3リンクが必要です。HA3リンクは、セッションセットアップと非対称トラフィック処理用のパケット転送リンクとして使用されます。

  *HA*ペアでは、両方のピアが同じモデルで同じバージョンの*PAN-OS*およびコンテンツリリースを実行し、同じセットのライセンスを使用している必要があります。

  また、*VM-Series* ファイアウォールの場合、両方のピアが同じハイパーバイザに存在していて、各ピアに同じ数の *CPU* コアが割り当てられている必要があります。
- HA 設定時の重要事項
- 高可用性の設定

HA 設定時の重要事項

- ローカル IP とピア IP に使用するサブネットは、仮想ルーターの他の場所で使用しないでください。
- それぞれのファイアウォールのOSとコンテンツリリースのバージョンは一致している必要があります。一致していない場合はファイアウォールの同期が阻害される恐れがあります。
- HA ポートの LED は、アクティブ ファイアウォールが緑、パッシブ ファイアウォールが黄色になります。
- ローカル ファイアウォールとピア ファイアウォールの設定を比較するには、**Device**[デバイス] タブの **Config Audit**[設定監査] ツールを使用し、左の選択ボックスで対象のローカル設定を、右の選択ボックスでピア設定を選択します。
- Webインターフェイスからファイアウォールを同期する場合は、**Dashboard**[ダッシュボード] のHAウィジェットにある **Push Configuration**[設定をプッシュ] をクリックします。プッシュを行うファイアウォールの設定内容が、ピア ファイアウォールの設定内容に上書きされます。アクティブファイアウォールのCLIからファイアウォールを同期する場合は、コマンド「request high-availability sync-to-remote running-config」を使用します。

  *10*ギガビットの*SFP+* ポートを使用するファイアウォールの高可用性 (*HA*) アクティブ/パッシブ設定では、フェイルオーバーが発生してアクティブファイアウォールがパッシブ状態になる際に、*10*ギガビット*Ethernet*ポートを一度ダウンさせてから再度開通させることでポートが更新されますが、ファイアウォールが再度アクティブになるまで送信機能は有効になりません。隣接するデバイスでソフトウェアをモニターしている場

© 2019 Palo Alto Networks, Inc.

合、ポートがダウンしてから再度開かれているため、ポートのフラッピングが発生していると見なされます。これは、*1* ギガビット *Ethernet* ポートなどの他のポートとは異なる動作です。他のポートでは無効になった場合でも送信は許可されるため、隣接するデバイスでフラッピングは検出されません。

高可用性の設定

HA設定を編集する場合は**Device** [デバイス] > **High Availability** [高可用性] を開き、それぞれの設定グループごとに、以下の表に記載されている情報を指定していきます。

高可用性の設定	の意味
General [全般] タブ	
セットアップ	以下の設定を指定します。 • **Enable HA**[HA の有効化] – 機能をアクティベーションします。 • **Group ID**[グループID] – HAペアの識別に使用する数値 (1 ~ 63) を入力します。このフィールドは複数のHAペアが同じブロードキャストドメインに存在する場合に設定が必須 (かつ一意である必要があります) となります。 • **Description** (内容) – (任意) HA ペアの説明を入力します。 • **Mode**[モード] – HA導入環境のタイプを設定します。**Active Passive** [アクティブ/パッシブ] または**Active Active** [アクティブ/アクティブ] • **Device ID**[デバイスID] – アクティブ/アクティブの設定の場合、デバイスIDを設定し、アクティブ-プライマリのピア (**Device ID**[デバイスID] を**0**に設定) とアクティブ-セカンダリのピア (**Device ID**[デバイスID] を**1**に設定) を設定します。 • **Enable Config Sync**[設定の同期を有効化] – 設定内容をピア間で同期させる場合はこのオプションを選択します。 両方のデバイスが常に同じ設定を持ち、トラフィックを同じように処理できるよう、設定の動機を常に有効にしてください。 • **Peer HA1 IP Address**[ピアHA1のIPアドレス] – ピアファイアウォールのHA1インターフェイスのIPアドレスを入力します。 • **Backup Peer HA1 IP Address** (バックアップ側ピア **HA1** の **IP** アドレス) – ピアのバックアップ制御リンクの IP アドレスを入力します。 バックアップ ピア *HA1* の *IP* アドレスを設定し、プライマリリンクが失敗した場合でもバックアップ リンクが各デバイスを同期させて最新の状態を保てるようにします。
アクティブ/パッシブ設定	• **Passive Link State**[パッシブリンクの状態] – 以下のうち1つを選択し、パッシブなファイアウォールのデータリンクの接続状態を保つかどうかを指定します。このオプションは AWS の VM-Series ファイアウォールでは使用できません。 • **auto**[自動] – 物理的な接続を持つリンクは、物理的には接続しつつも無効化された状態が保たれ、ARP学習やパケット転送には参加しません。接続が再開されるまでの時間が短縮されるので、フェイルオーバー中の収束時に役立ちます。ネットワークループを防ぐため、ファイアウォールにレイヤー2インターフェイスが設定されている場合はこのオプションを選択しないでください。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
	• **shutdown**[シャットダウン] – 強制的にインターフェイス リンクをダウン状態にします。これはデフォルトのオプションです。このオプションでは、ネットワークにループが起きません。 ファイアウォールにレイヤー *2* インターフェイスが設定されていない場合、*Passive Link State (*パッシブリンク状態*)*を*auto (*自動*)*に設定します。 • **Monitor Fail Hold Down Time (min)**[モニター障害時ホールド ダウン タイム (分)] – この値 (1 ~ 60 分) により、ファイアウォールがパッシブになる前に Non-functional 状態で待機する間隔が決まります。このタイマは、リンクまたはパス モニタリングの障害が原因でハートビートおよび hello メッセージが届かない場合に使用します。
選択設定	以下の設定を指定または有効化します。 • **Device Priority**[デバイス優先度] – アクティブ ファイアウォールの識別に使用する優先度の値を入力します。ペアの両方のファイアウォールでプリエンプティブ機能が有効になっている場合、値が低い (優先順位が高い) ファイアウォールがアクティブファイアウォール (範囲は0 ~ 255) になります。 • **Heartbeat Backup**[ハートビートバックアップ] – HAファイアウォールで管理ポートを使用して、ハートビートおよびhelloメッセージのバックアップパスを提供します。管理ポートの IP アドレスは、HA ピアと HA1 制御リンク経由で共有されます。追加の設定は必要ありません。 *HA1* および *HA1* バックアップ リンクに対してインバンド ポートを使用する場合は*Heartbeat Backup (*ハートビート バックアップ*)*を有効化します。*HA1* あるいは *HA1* バックアップ リンクに対して管理ポートを使用する場合は*Heartbeat Backup (*ハートビート バックアップ*)*を有効化しないでください。 • **Preemptive**[プリエンプティブ] – 優先順位の高いファイアウォールが障害から回復した後にアクティブ (アクティブ/パッシブ) あるいはアクティブ-プライマリ (アクティブ/アクティブ) な動作を再開できるようにします。優先度値の高いファイアウォールが障害から回復したときにアクティブまたはアクティブ-プライマリのファイアウォールとしての動作を再開できるようにするには、両方のファイアウォールでプリエンプティブオプションを有効にする必要があります。この設定がオフの場合、優先度の高いファイアウォールが障害から回復した後も、優先度が低いファイアウォールがアクティブあるいはアクティブ-プライマリのまま動作します。 *Preemptive (*プリエンプティブ*)*を有効化するかどうかは、ビジネス要件によって異なります。プライマリ デバイスをアクティブ デバイスにしなければならない場合は*Preemptive (*プリエンプティブ*)*を有効化し、失敗から復帰した後、プライマリ デバイスがセカンダリ デバイスに取って代わるようにします。フェイルオーバーのイベントをできるだけ減らす必要がある場合は*Preemptive (*プリエンプティブ*)*オプションを無効化し、優先順位の高いファイアウォールをプライマリ ファイアウォールにするためにフェイルオーバー後に *HA* ペアが再びフェイルオーバーしないようにします。 • **HA Timer Settings**[HA タイマー設定] – 以下のいずれかの事前設定プロファイルを選択します。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
	• **Recommended**[推奨]:一般的なフェイルオーバータイマー設定で使用します。別の設定が必要であることが確実な場合を除き、**Recommended (推奨)**設定を使用することがベストプラクティスになります。 • **Aggressive**[アグレッシブ]:高速のフェイルオーバータイマー設定で使用します。 プロファイルに含まれる個々のタイマーの事前設定値を表示するには、*Advanced[詳細]* を選択して *Load Recommended[推奨をロード]* または *Load Aggressive[アグレッシブをロード]* をクリックします。お使いのハードウェアモデルの事前設定値が画面に表示されます。 • **Advanced**[詳細]:以下の各タイマーに対して、ネットワーク要件に合わせて値をカスタマイズできます。 • **Promotion Hold Time**[プロモーションホールドタイム] – パッシブピア (アクティブ/パッシブモードの場合) またはアクティブ-セカンダリピア (アクティブ/アクティブモードの場合) が、HAピアとの通信が失われた後でアクティブピアまたはアクティブ-プライマリピアの役割を引き継ぐまでに待機する時間を入力します。このホールド タイムは、ピアの障害宣言が行われた後に開始されます。 • **Hello Interval**[Hello間隔] – もう一方のファイアウォールのHAプログラムが動作していることを確認するための hello パケットの送信間隔をミリ秒単位で入力します (範囲は8,000 ~ 60,000、デフォルトは8,000)。 • **Heartbeat Interval**[ハートビート間隔] – HAピアがICMP pingの形式でハートビートメッセージを交換する頻度を指定します (範囲は1,000 ~ 60,000ミリ秒、デフォルトは1000ミリ秒)。 • **Maximum No. of Flaps**[最大フラップ数] – フラップは、ファイアウォールが前回の非アクティブ状態発生から 15 分以内に再び非アクティブ状態になるとカウントされます。許容する最大フラップ数を指定できます (範囲は0 ~ 16、デフォルトは3)。フラップ数がこの最大数に達するとファイアウォールがサスペンドしたと判断されてパッシブファイアウォールが引き継ぎます。値 0 を指定すると最大数は設定されません (何回フラップが発生してもパッシブ ファイアウォールは引き継がない)。 • **Preemption Hold Time**[プリエンプションホールドタイム] – パッシブピアまたはアクティブ-セカンダリピアがアクティブピアまたはアクティブ-プライマリピアとしての役割を引き継ぐまでに待機する時間を分単位で入力します (範囲は1 ~ 60、デフォルトは1)。
	• **Monitor Fail Hold Up Time (ms)**[モニター障害時ホールド アップ タイム (ミリ秒)] – パス モニターまたはリンク モニターに障害が発生した後にファイアウォールがアクティブのままでいる時間を指定します。隣接するデバイスの偶発的なフラッピングによる HA のフェイルオーバーを回避するためには、この設定をお勧めします (範囲は 0 ~ 60,000 ミリ秒、デフォルトは 0 ミリ秒)。 • **Additional Master Hold Up Time (min)** (追加のマスター ホールド アップ タイム (分)) – この時間間隔は、Monitor Fail Hold Up Time (モニター障害時ホールド アップ タイム) と同じイベントに適用されます (範囲は 0 ~ 60,000 ミリ秒、デフォルトは 500 ミリ秒)。追加の時間間隔は、アクティブ/パッシブモードのアクティブピアとアクティブ/アクティブモードのアクティブなプライマリピアにのみ適用されます。両方のピアで同じリンク/パスモニターの障害が同時に発生した場合にフェイルオーバーを回避するためには、このタイマを設定することをお勧めします。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
コントロール リンク （HA1）/コントロールリンク（HA1 バックアップ）	HA ペアのファイアウォールでは、HA リンク を使用してデータを同期し、状態情報を管理します。専用の制御リンクおよび専用のバックアップ制御リンクを持っているファイアウォールのモデルもあります。例えば、PA-5200 Series ファイアウォールは HA1-A と HA1-B を持っています。この場合、Elections Settings (選出設定) ページで Heartbeat Backup (ハートビート バックアップ) オプションを有効化する必要があります。制御リンク HA リンクに専用 HA1 ポートを使用し、制御リンク (HA バックアップ) にデータ ポートを使用している場合は、Heartbeat Backup (ハートビート バックアップ) オプションを有効にすることをお勧めします。 PA-220ファイアウォールなど専用のHAポートがないファイアウォールの場合は、制御リンクHA接続に管理ポートを設定し、制御リンクHA1バックアップ接続にタイプをHAに設定したデータポートインターフェイスを設定する必要があります。この場合、管理ポートが使用されているため、Heartbeat Backup (ハートビートバックアップ) オプションを有効にする必要はありません。ハートビートバックアップは管理インターフェイス接続を使用して行われるためです。 AWS の VM-Series ファイアウォールでは、管理ポートが HA1 リンクとして使用されます。 *HA制御リンクにデータポートを使用する場合、制御メッセージはデータプレーンから管理プレーンに通信する必要があるため、データプレーンで障害が発生すると、ピア間でHA制御リンク情報を通信することができず、フェイルオーバーが発生します。最善策は専用のHAポートを使用することですが、専用のHAポートがないファイアウォールでは管理ポートを使用します。* プライマリおよびバックアップ HA 制御リンクの以下の設定を指定します。 • **Port**[ポート] – プライマリおよびバックアップの HA1 インターフェイスの HA ポートを選択します。バックアップの設定は任意です。 • **IPv4/IPv6 Address**[IPv4/IPv6 アドレス] – プライマリおよびバックアップの HA1 インターフェイスとなる HA1 インターフェイスの IPv4 または IPv6 アドレスを入力します。バックアップの設定は任意です。 *PA-3200 シリーズのファイアウォールはバックアップ HA1 インターフェイス用の IPv6 アドレスをサポートしていないため、IPv4 アドレスを使用してください。* • **Netmask**（ネットマスク） – プライマリおよびバックアップの HA1 インターフェイスの IP アドレスのネットワーク マスク（たとえば、「255.255.255.0」）を入力します。バックアップの設定は任意です。 • **Gateway**[ゲートウェイ] – プライマリおよびバックアップの HA1 インターフェイスのデフォルト ゲートウェイの IP アドレスを入力します。バックアップの設定は任意です。 • **Link Speed**[リンク速度] –（専用 HAポートをもつモデルのみ）専用のHA1ポートにおけるファイアウォール間の制御リンクの速度を選択します。 • **Link Duplex**[リンクデュプレックス] –（専用HAポートをもつモデルのみ) – 専用のHA1ポートにおけるファイアウォール間の制御リンクのデュプレックスオプションを選択します。 • **Encryption Enabled**[暗号化を有効化] – HAキーをHAピアからエクスポートしてこのファイアウォールにインポートした後で、暗号化を有効にします。さらに、このファイアウォールのHAキーは、一度エクスポートを行いHAピアに

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
	インポートする必要があります。プライマリ HA1 インターフェイスについてこの設定を行います。キーのエクスポートとインポートは証明書ページで行います（「Device（デバイス）> Certificate Management（証明書の管理）> Certificate Profile（証明書プロファイル）」を参照）。 ファイアウォールが直接接続されていない際の暗号化を有効にします（*HA1* 接続はトラフィックを検査、処理、捕捉できるネットワーク デバイスを通過します）。 • **Monitor Hold Time (ms)**（ホールド タイムのモニター（ミリ秒））– 制御リンク障害によるピア障害を宣言するまでにファイアウォールが待機する時間（ミリ秒）を入力します（範囲は 1,000 ~ 60,000 ミリ秒、デフォルトは 3,000 ミリ秒）。このオプションは HA1 ポートの物理リンクの状態をモニターします。

データ リンク (HA2)
 	
HA2 バックアップ リンクが設定されていると、物理リンク障害がある場合は HA2 バックアップ リンクのファイルオーバーが発生します。[HA2 キープアライブ] オプションが有効にされている場合、定義されたしきい値に基づいて HA キープ
	プライマリおよびバックアップ データ リンクの以下の設定を指定します。
	• **Port**[ポート] – HA ポートを選択します。プライマリおよびバックアップの HA2 インターフェイスについてこの設定を行います。バックアップの設定は任意です。
	• **IP Address**[IP アドレス] – プライマリおよびバックアップの HA2 インターフェイスとなる HA インターフェイスの IPv4 または IPv6 アドレスを指定します。バックアップの設定は任意です。
	• **Netmask**[ネットマスク] – プライマリおよびバックアップの HA2 インターフェイスとなる HA インターフェイスのネットワーク マスクを指定します。バックアップの設定は任意です。
	• **Gateway**[ゲートウェイ] – プライマリおよびバックアップの HA2 インターフェイスとなる HA インターフェイスのデフォルト ゲートウェイを指定します。バックアップの設定は任意です。ファイアウォールのHA2 IPアドレスが同じサブネット上にある場合、[ゲートウェイ] フィールドは空白のままにしておく必要があります。
	• **Enable Session Synchronization**[セッション同期を有効にする] - セッション情報をパッシブ ファイアウォールと同期できるようにし、転送オプションを選択します。
	
	セッション同期を有効化し、セカンダリ デバイスがデータプレーン内でセッションを保持し、ファイアウォールが同期済みのセッションにパケットをマッチさせて素早くパケットを転送できるようにします。セッション同期を有効化しない場合はファイアウォールがセッションを再作成しなければならないため、遅延が生じて接続がドロップされるおそれがあります。
	• **Transport**[転送] – 以下のいずれかの転送オプションを選択します。
	  • **Ethernet**[イーサネット] –ファイアウォールが逆並列で接続されているかスイッチを介して接続されている場合に使用します (Ethertype 0x7261)。
	  • **IP**–レイヤー 3 転送が必要な場合に使用します (IP プロトコル番号 99)。
	  • **UDP**–IP オプションでの場合と同じように、チェックサムがヘッダーのみではなくパケット全体に基づいて計算されることを利用するために使用します (UDP ポート 29281)。UDPモードの利点はUDPチェックサムにあり、セッション同期メッセージの整合性を検証することができます。
	• **Link Speed**[リンク速度] – （専用HAポートをもつモデルのみ）専用のHA2ポートにおけるピア間の制御リンクの速度を選択します。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味

アライブ メッセージが失敗すると、フェイルオーバーが発生します。	• **Link Duplex**[リンクデュプレックス] – (専用HAポートをもつモデルのみ) – 専用のHA2ポートにおけるピア間の制御リンクのデュプレックスオプションを選択します。
	  • **HA2 keep-alive (HA2**キープアライブ**)** – HA ピア間のHA2データリンクの健康状態のモニタリングを有効にするために、このオプションを選択することがベストプラクティスになります。このオプションはデフォルトで無効化されていますが、片方、あるいは両方のピアで有効化することができます。有効化した場合、ピアはキープアライブメッセージを使用してHA2接続をモニターし、設定した**Threshold**[しきい値] に従って障害を検知します (デフォルトは10,000ミリ秒) 。HA2キープアライブを有効化した場合、HA2キープアライブ復旧アクションが行われます。**Action**[アクション] を選択します。
	  • **Log Only**[ログのみ] – HA2インターフェイスの障害を、重要イベントとしてシステムログに記録します。アクティブ/パッシブのデプロイ環境の場合、トラフィックを転送するファイアウォールはアクティブなピアのみなので、このオプションを選択してください。パッシブなピアはバックアップ状態にあり、トラフィックを転送していないため、スプリットデータパスは不要です。HA2バックアップリンクを設定していない場合、状態の同期は無効になっています。HA2パスが回復すると、情報ログが生成されます。
	  • **Split Datapath**[スプリットデータパス] – アクティブ/アクティブのHAデプロイ環境の場合はこのオプションを選択し、それぞれのピアに対し、HA2インターフェイスの障害を検知した際はそれぞれのローカルステートとセッションテーブルの所有権を取るよう指示します。HA2の接続が無い場合、状態の同期とセッションの同期は行われません。同期とは、セッションテーブルを個別に管理し、各HAピアからのトラフィックの転送を正常に行えるようにするためのものです。この状態を防ぐために、HA2バックアップリンクを設定してください。
	  • **Threshold (ms)** (しきい値 (ミリ秒)) – 上記のいずれかのアクションがトリガーされる前にキープアライブ メッセージが失敗した期間です (範囲は 5,000 ~ 60,000 ミリ秒、デフォルトは 10,000 ミリ秒) 。

Link and Path Monitoring (リンクおよびパスのモニタリング**)** タブ (AWS の VM-Series ファイアウォールでは使用できません)	
パス モニタリング	以下を指定します。 • **Enabled**[有効] – パスのモニタリングを有効にします。パスのモニタリングをオンにすると、ファイアウォールは指定した宛先 IP アドレスをモニターするために ICMP ping メッセージを送信し、レスポンスがあることを確認します。フェイルオーバー用に他のネットワーク デバイスのモニタリングが必要であったり、リンクのモニタリングのみでは不十分である場合に、バーチャルワイヤー、レイヤー 2、またはレイヤー 3 設定でパスのモニタリングを使用します。 • **Failure Condition**[失敗条件] – モニターしているパス グループの一部またはすべてで応答できない場合にフェイルオーバーを発生させるかどうかを選択します。 パス モニタリングあるいはリンク モニタリングのいずれかを有効化・設定し、パスやリンクがダウンした場合にフェイルオーバーを発生させるようにします。パス モニタリングでは *1* つ以上

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
	のPath Group (パス グループ)を、リンク モニタリングでは 1 つ以上のLink Group (リンク グループ)を設定します。
パス グループ	特定の宛先アドレスをモニターする 1 つ以上のパス グループを定義します。パス グループを追加するには、インターフェイス タイプ (**Virtual Wire**[バーチャル ワイヤー]、**VLAN**、または **Virtual Router**[仮想ルーター]) に対して **Add**[追加] をクリックして、以下を指定します。 • **Name**[名前] – バーチャルワイヤー、VLAN、または仮想ルーターをドロップダウンリストから選択します (ドロップダウンリストには、バーチャルワイヤー、VLAN、または仮想ルーターのどのパスを追加したかに応じて、データが入力されます)。 • **Enabled**[有効] – パス グループを有効にします。 • **Failure Condition** (失敗条件) – 指定した宛先アドレスの一部またはすべてが応答できない場合に、エラーを発生させるかどうかを選択します。 • **Failure Condition**[送信元 IP] –バーチャル ワイヤーおよび VLAN のインターフェイスの場合、ネクストホップ ルータ (宛先 IP アドレス) に送信されるプローブ パケットで使用する送信元 IP アドレスを入力します。ローカル ルータでアドレスをファイアウォールにルーティングできる必要があります。仮想ルーターに関連付けられたパス グループの送信元 IP アドレスは、指定された宛先 IP アドレスの出力インターフェイスとしてルート テーブルに示されているインターネット IP アドレスとして自動的に設定されます。 • **Destination IPs**[宛先 IP] – モニター対象となる 1 つ以上の (コンマ区切りの) 宛先アドレスを入力します。 • **Ping Interval** (**Ping**間隔) – 宛先アドレスに送信される ping 間の間隔を指定します (範囲は 200 ~ 60,000 ミリ秒、デフォルトは 200 ミリ秒)。 • **Ping Count** (**Ping**数) – 障害を宣言するまでに試行する Ping 数を指定します (範囲は 3 ~ 10 回、デフォルトは 10 回)。
リンク モニタリング	以下を指定します。 • **Enabled**[有効] – リンクのモニタリングを有効にします。リンクのモニタリングによって、物理リンクまたは物理リンクのグループに障害が発生した場合にフェイルオーバーのトリガーになります。 • **Failure Condition**[失敗条件] – モニターしているリンク グループの一部またはすべてに障害が発生した場合にフェイルオーバーが発生するかどうかを選択します。 パス モニタリングあるいはリンク モニタリングのいずれかを有効化・設定し、パスやリンクがダウンした場合にフェイルオーバーを発生させるようにします。パス モニタリングでは *1* つ以上のPath Group (パス グループ)を、リンク モニタリングでは *1* つ以上のLink Group (リンク グループ)を設定します。
Link Groups	特定の Ethernet リンクをモニターする 1 つ以上のリンク グループを定義します。リンク グループを追加するには、以下を指定して **Add**[追加] をクリックします。 • **Name**[名前] – リンク グループ名を入力します。 • **Enabled**[有効] – リンク グループを有効にします。 • **Failure Condition** (失敗条件) – 選択したリンクの一部またはすべてに障害が発生した場合にエラーを発生させるかどうかを選択します。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
	• **Interfaces**[インターフェイス] – モニターする 1 つ以上の Ethernet インターフェイスを選択します。
[アクティブ/アクティブ設定] タブ	
パケット転送	ピアによる、セッション設定用およびレイヤー7の検査用（App-ID、コンテンツID、および脅威検査）の、HA3リンクを経由したパケットの転送を**Enable**[有効化] します。
[HA3 インターフェイス]:	アクティブ/アクティブのHAピア間のパケットの転送に使用しようとしているデータインターフェイスを選択します。ここで使用するインターフェイスはタイプを**HA**に設定した専用のレイヤー2インターフェイスである必要があります。 *HA3*リンクに障害が発生した場合、アクティブ-セカンダリピアは機能停止状態に移行します。この状態に移行しないようにするためには、*HA3*リンクとして*2*つ以上の物理インターフェイスをもつリンク集約グループ（*LAG*）インターフェイスを設定します。*HA3*バックアップリンクはファイアウォールでサポートされていません。複数のインターフェイスをもつ集約グループにより、追加の容量とリンクの冗長性を確保し、*HA*ピア間のパケット転送を補助することができます。 HA3 インターフェイスを使用している場合、ファイアウォールとすべての中継ネットワーク デバイスで Jumbo Frame を有効にする必要があります。ジャンボ フレームを有効にする場合は、**Device**（デバイス）> **Setup**（設定）> **Session**（セッション）を選択し、Session Settings（セッション設定）セクションで **Enable Jumbo Frame**（ジャンボ フレームの有効化）オプションを選択します。
VR 同期	HAピアに設定されたすべての仮想ルーターの同期を強制します。 仮想ルーターが動的ルーティングプロトコル用に設定されていない場合はこのオプションを使用します。両方のピアが交換網を介して同じネクストホップルーターに接続されている必要があり、スタティックルーティングのみを使用している必要があります。
QoS 同期	すべての物理インターフェイスの QoS プロファイル選択を同期します。両方のピアのリンク速度が同様で、すべての物理インターフェイスで同じQoSプロファイルが必要な場合には、このオプションを選択します。この設定は、**Network**[ネットワーク] タブの QoS 設定の同期に影響します。QoS ポリシーは、この設定に関係なく同期されます。
仮の保留時間 (秒)	HAがアクティブ/アクティブに設定されたファイアウォールで障害が発生すると、一時的な状態に入ります。暫定的な状態からアクティブ-セカンダリの状態に移行することにより、Tentative Hold Time [暫定的な状態の保留時間] がトリガーされ、ファイアウォールはパケットの処理を開始する前に、この時間中に隣接デバイスへのルーティングを試行してルートテーブルを埋めようとします。このタイマーを使用しない場合、ファイアウォールの回復時にただちにアクティブ-セカンダリ状態になり、必要なルートがないためパケットがブラックホール状態になります（デフォルトは 60 秒）。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味
セッション オーナーの選択	セッションオーナーには、そのセッション内のすべてのレイヤー7検査（App-ID、およびコンテンツID）、およびそのセッション内のすべてのトラフィックログを生成する役割があります。以下のオプションのうち1つを選択し、パケットに対するセッションオーナーの決定方法を指定します。 • **First packet**[最初のパケット] – そのセッションの最初のパケットを受信するファイアウォールをセッションオーナーとして指定する場合はこのオプションを選択します。HA3 全体でトラフィックを最小化し、データプレーン負荷をピアに分散したい場合にベストプラクティスになります。 • **Primary Device**[プライマリデバイス] – アクティブ-プライマリのファイアウォールをすべてのセッションオーナーとして設定したい場合はこのオプションを選択します。この場合、アクティブ-セカンダリのファイアウォールが最初のパケットを受信すると、レイヤー7検査を必要とするすべてのパケットをHA3リンクを経由してアクティブ-プライマリのファイアウォールへ転送します。
セッション セットアップ	セッションセットアップを行うファイアウォールはレイヤー4の処理（アドレスの変換を含む）を通じてレイヤー2を実行し、セッションテーブルエントリを作成します。セッションセットアップは管理プレーンのリソースを消費するため、以下のうち1つのオプションを選択して負荷を分散することができます。 • **Primary Device**[プライマリデバイス] – アクティブ-プライマリのデバイスがすべてのセッションを確立します。 • **IP Modulo**[IPモジュロ] – 送信元IPアドレスのパリティに基づいて、セッションセットアップを分散させます。 • **IP Hash**[IPハッシュ] – よりランダムに分散する必要がある場合は、送信元IPアドレスまたは送信元と宛先のIPアドレス、およびハッシュシード値を使用してセッションセットアップを分散させます。 • **First Packet**[最初のパケット] – ピアがセッションオーナーである場合を含め、最初のパケットを受信したファイアウォールがセッションセットアップを行います。このオプションではHA3リンクを経由するトラフィックが最小限にとどめられ、管理プレーンに負荷がかかるセッションセットアップが、最初のパケットを受信するファイアウォールで必ず行われるようになります。

仮想アドレス	**Add**[追加] をクリックし、**IPv4**または**IPv6**のタブを選択し、再度**Add**[追加] をクリックしてオプションを入力し、使用するHA仮想アドレスのタイプを指定します。フローティングまたはARPロードシェアリングペア内では複数の仮想アドレスのタイプを混在させることもできます。例えば、LANインターフェイスでARPロードシェアリングを使用し、WANインターフェイスではフローティングIPを使用することができます。
	• **Floating**[フローティング] – リンクまたはシステム障害が発生した場合に、HAピア間で移動するIPアドレスを入力します。それぞれのファイアウォールが1つを所有できるよう、2つのフローティングIPアドレスを設定し、優先順位を設定します。どちらかのファイアウォールに障害が発生した場合、フローティングIPアドレスがHAピアに移行されます。
	  • **Device 0 Priority**[デバイス0優先順位] – デバイスIDが0のファイアウォールにフローティングIPアドレスの優先所有権をもたせます。最も低い値をもつファイアウォールの優先順位が最も高くなります。
	  • **Device 1 Priority**[デバイス0優先順位] – デバイスIDが1のファイアウォールにフローティングIPアドレスの優先所有権をもたせます。最も低い値をもつファイアウォールの優先順位が最も高くなります。

© 2019 Palo Alto Networks, Inc.

高可用性の設定	の意味

	• **Failover address if link state is down**[リンク状態がダウンの場合アドレスをフェイルオーバー] – インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
	• **Floating IP bound to the Active-Primary HA device**[フローティングIPをアクティブ-プライマリHAデバイスに固定] – フローティングIPをアクティブ-プライマリピアに固定する場合はこのオプションを選択します。片方のピアに障害が発生し、障害が発生したファイアウォールが復旧して役割がアクティブ-セカンダリのピアに切り替わった後も、トラフィックは継続的に元のアクティブ-プライマリピアに送信されます。
	• **ARP Load Sharing**[ARPロードシェアリング] – HAペアで共有し、ホストのゲートウェイサービスを提供するIPアドレスを入力します。ファイアウォールがホストと同じブロードキャストドメインにある場合にのみ、このオプションを選択する必要があります。**Device Selection Algorithm**[デバイス選択アルゴリズム] を選択します。
	  • **IP Modulo**[IPモジュロ] – ARPリクエスト元IPアドレスのパリティに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
	  • **IP Hash**[IPハッシュ] – ARPリクエスト元IPアドレスのハッシュに基づいて、ARPリクエストに応答するファイアウォールが選択されます。

操作コマンド	
ローカルデバイスをサスペンド （またはローカルデバイスを稼動状態にする）	次の操作モードのCLIコマンドは、ローカルHAピアを一時停止状態にし、ファイアウォールのHA機能を一時的に無効にします。現在アクティブなファイアウォールをサスペンドすると、他のピアが引き継ぎます。 `request high-availability state suspend` サスペンドされたファイアウォールを動作状態に戻す場合は次のCLI操作コマンドを実行します。 **`request high-availability state functional`** フェイルオーバーをテストする場合は、アクティブ（またはアクティブ-プライマリ）ファイアウォールのケーブルを外すか、このリンクをクリックしてアクティブファイアウォールをサスペンドします。

© 2019 Palo Alto Networks, Inc.

Device (デバイス) > Log Forwarding Card (ログ転送カード)

- Device (デバイス) > Log Forwarding Card (ログ転送カード)

ログ転送カード (LFC) は、すべてのデータプレーンのログ (例えばトラフィックや脅威) をファイアウォールから Panorama や Syslog サーバーなどの単一あるいは複数の外部ロギングシステムに転送する、パフォーマンスに優れたログカードです。データプレーンのログはローカルのファイアウォールで利用できなくなったため、管理用 Web インターフェイスから ACC タブが削除され、Monitor (監視)> Logs (ログ) に管理ログ (Configuration (設定)、System (システム)、Alarms (アラーム)) だけが含まれています。

LFC 用のポートを設定する必要があります。ポート 1 は 10Gbps 、ポート 9 は 40Gbps です。ポートは**Device (デバイス) > Log Forwarding Card (ログ転送カード)**で設定します。ファイアウォールはこれらのポートを使用してすべてのデータプレーンのログを Panorama や Syslog サーバーなどの外部システムに転送します。

LFC の要件および各コンポーネントに関する情報については、PA-7000 Series ハードウェア リファレンス ガイドを参照してください。

LFC インターフェイス用に次の表で示している設定を行います。

LFC インターフェイス設定	の意味
氏名	インターフェイス名を入力します。LFC の場合、**lfc1/1**あるいは**lfc1/9**のいずれかを選択する必要があります。
コメント	インターフェイスの説明 (省略可) を入力します。
IPv4	ネットワークで IPv4 が使用されている場合は、以下を定義します。 • **IP address**[IP アドレス] – ポートの IPv4 アドレス。 • **Netmask**[ネットマスク] – ポートの IPv4 アドレスのネットワーク マスク。 • **Default Gateway**[デフォルトゲートウェイ] – ポートのデフォルトゲートウェイのIPv4アドレス。
IPv6	ネットワークで IPv6 が使用されている場合は、以下を定義します。 • **IP** アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲートウェイの IPv6 アドレス。
リンク速度	インターフェイスの速度 (**10000**または**40000**) を選択するか、**auto** (デフォルト設定) を選択して、接続ごとにファイアウォールに自動的に速度を決定させます。利用できるインターフェイス速度は使用するポート (lfc1/1 あるいは lfc1/9) によって異なります。スピード設定が不可のインターフェイスについては**auto**のみ設定可能です。
リンク ステート	接続に応じて、インターフェイスの状態を、有効 (**up**)、無効 (**down**)、自動決定 (**auto**) から選択します。デフォルト設定は**auto**です。
LACP ポート優先順位	ファイアウォールがこのフィールドを使用するのは、集約グループのリンク集約制御プロトコル (LACP) が有効になっている場合のみです。割り当てられたインターフェイスの数がアクティブなインターフェイスの数 (Max Ports (最大ポート)

© 2019 Palo Alto Networks, Inc.

LFC インターフェイス設定	の意味
	フィールド) を上回ると、ファイアウォールがインターフェイスの LACP ポート優先度に従って、どのインターフェイスがスタンバイ モードかを判断します。数値が小さいほど優先度は高くなります (範囲は1 ~ 65535、デフォルトは32768) 。

サブインターフェイスは、マルチ vsys が有効な場合のみ利用できます。LFC サブインターフェイスを設定するには、サブインターフェイスを追加して以下の表に記載されている設定を使用します。

LFC サブインターフェイス設定	の意味
インターフェイス名	読み取り専用の**Interface Name**[インターフェイス名] フィールドには、選択したログカードインターフェイスの名前が表示されます。サブインターフェイスを識別する数値サフィックス (1 ~ 9999) を隣のフィールドに入力します。
コメント	インターフェイスの説明 (省略可) を入力します。
タグ	サブインターフェイス用のVLAN**Tag**[タグ] (0 ~ 4094) を入力します。 使いやすさのため、タグはサブインターフェイス番号と同じにしてください。
仮想システム(vsys)	ログ転送カード (LFC) サブインターフェイスの割り当て先の仮想システム (vsys) を選択します。**Virtual Systems**[仮想システム] リンクをクリックして新しいvsysを追加することもできます。LFC サブインターフェイスを vsys に割り当てると、そのインターフェイスは、ログ カードからログ (Syslog、電子メール、SNMP) を転送するすべてのサービスの送信元インターフェイスとして使用されます。
IPv4	ネットワークで IPv4 が使用されている場合は、以下を定義します。 • **IP address**[IP アドレス] – ポートの IPv4 アドレス。 • **Netmask**[ネットマスク] – ポートの IPv4 アドレスのネットワーク マスク。 • **Default Gateway**[デフォルトゲートウェイ] – ポートのデフォルトゲートウェイのIPv4アドレス。
IPv6	ネットワークで IPv6 が使用されている場合は、以下を定義します。 • **IP** アドレス: ポートの IPv6 アドレス。 • デフォルト ゲートウェイ: ポートのデフォルト ゲートウェイの IPv6 アドレス。

© 2019 Palo Alto Networks, Inc.

Device > Config Audit [デバイス > 設定監査]

設定ファイル同士の差異を確認する場合は **Device** [デバイス] > **Config Audit**[設定監査] を開きます。このページでは設定内容が別々のペインに並べて表示され、内容の差異が行ごとに色づけして表示されます（追加は緑色、変更は黄色、削除は赤色）。

Added	Modified	Deleted

Config Audit Setting（設定監査の設定）	の意味
設定名のドロップダウンリスト（ラベルなし）	比較する2つの設定内容を設定名のドロップダウンリスト（ラベルなし）から選択します（デフォルトは**Running config** [実行中の設定] および**Candidate config** [候補設定] ）。 目的の設定に関連付けられるコミット操作の *Description*（説明）値にある文字列を入力することで、ドロップダウン リストのフィルタリングを行うことができます（「変更のコミット」を参照）。
コンテクストドロップダウン	ハイライト表示されたファイル同士の差異の前後に表示する行数を指定する場合は**Context** [コンテクスト] のドロップダウンリストを使用します。表示する行数を増やすことで、検証結果をWebインターフェイスの設定内容に反映させやすくなります。**Context**（コンテクスト）を **All**（すべて）に設定した場合、結果には設定ファイル全体が含まれます。
Go（実行）	検証を開始する場合は**Go** [実行] をクリックします。
前へ（ << ）および 次へ（ >> ）	連続したバージョンの設定が設定名のドロップダウンリストから選択されるとこれらの矢印が使用可能になります。ドロップダウンリストの1つ前のペアを比較する場合は << を、次の設定ペアを比較する場合は >> をクリックしてください。

© 2019 Palo Alto Networks, Inc.

[Device] > [パスワード プロファイル]

- [Device] > [パスワード プロファイル]
- Panorama > Password Profiles（パスワード プロファイル）

個別のローカル アカウントの基本的なパスワード要件を設定するには、**Device**（デバイス）> **Password Profiles**（パスワード プロファイル）または **Panorama** > **Password Profiles**（パスワード プロファイル）を選択します。パスワード プロファイルは、すべてのローカル アカウントに対して定義された Minimum Password Complexity（パスワード複雑性設定）（**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理））をオーバーライドします。

アカウントにパスワード プロファイルを適用するには、**Device**（デバイス）> **Administrators**（管理者）（ファイアウォールの場合）または **Panorama** > **Administrators**（管理者）（Panoramaの場合）を選択し、アカウントを選択して、**Password Profile**（パスワード プロファイル）を選択します。

ローカル データベース認証を使用する管理者アカウントにパスワード プロフィルを割り当てることはできません（「Device（デバイス）> Local User Database（ローカル ユーザー データベース）> Users（ユーザー）」を参照）。

パスワード プロファイルを作成するには、**Add**（追加）をクリックし、以下の表に従って情報を指定します。

パスワード プロファイル設定	の意味
氏名	パスワード プロファイルを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
パスワード有効期限（日数）	管理者は、日数（範囲は 0 ~ 365 日）で指定された期間ごとに定期的にパスワードを変更する必要があります。たとえば、値を「90」に設定すると、管理者に 90 日ごとにパスワードの変更を求めるプロンプトが表示されます。失効の警告を 0 ~ 30 日の範囲で設定して猶予期間を指定することもできます。
失効の警告期間（日数）	パスワード有効期限を設定した場合は、この設定により、強制パスワード変更日が近づくとユーザーがログインするたびにパスワードの変更を求めるプロンプトを表示することができます（範囲は 0 ~ 30 日）。
失効後の管理者ログイン回数	アカウントが失効した後に、管理者はここで指定した回数だけログインできます。たとえば、値を「3」に設定した場合、アカウントが失効しても、管理者はアカウントがロックアウトされるまで 3 回ログインすることができます（範囲は 0 ~ 3 回）。
失効後の猶予期間 (日数)	アカウントが失効しても、管理者はここで指定した期間（日数）ログインできます（範囲は 0 ~ 30 日）。

ユーザー名とパスワードの要件

PAN-OS および Panorama アカウントのユーザー名とパスワードに使用できる有効な文字を以下の表に示します。

© 2019 Palo Alto Networks, Inc.

アカウントの種類	ユーザー名とパスワードの制限
パスワード文字セット	パスワード フィールドの文字セットには制限がありません。
リモート管理者、SSL-VPN、キャプティブ ポータル	ユーザー名には以下の文字を使用できません。 • バックティック (`) • 山かっこ (< と >) • アンパサンド (&) • アスタリスク (*) • アット記号 (@) • 疑問符 (?) • パイプ (|) • 一重引用符 (') • セミコロン (;) • 二重引用符 (") • ドル記号 ($) • かっこ ('(' と ')') • コロン (':')
ローカル管理者アカウント	ローカル ユーザー名には以下の文字を使用できます。 • 小文字 (a ~ z) • 大文字 (A ~ Z) • 数字 (0 ~ 9) • アンダースコア (_) • ピリオド (.) • ハイフン (-) ログイン名をハイフン (-) で開始することはできません。

© 2019 Palo Alto Networks, Inc.

Device > Administrators [デバイス > 管理者]

ファイアウォールやPanoramaへのアクセス権は管理者アカウントにより制御されます。ファイアウォール管理者には、1 台のファイアウォールか、1 台のファイアウォール上の仮想システムへのフル アクセス権または読み取り専用アクセス権を付与できます。ファイアウォールには、フル アクセス権を持つ **admin** アカウントが事前に定義されています

Panorama 管理者を定義するには「Panorama > Managed Devices (管理対象デバイス) > Summary (サマリー) 」を参照してください。

以下の認証オプションがサポートされています。

- パスワード認証 – 管理者がユーザー名とパスワードを入力してログインします。認証に証明書は不要です。認証プロファイルと併用することや、ローカル データベースの認証に使用することができます。
- クライアント証明書認証 (Web) – この認証方法ではユーザー名とパスワードが不要になり、ファイアウォールへのアクセス認証は証明書のみで行えるようになります。
- 公開鍵認証 (SSH) – 管理者がファイアウォールへのアクセスが必要なマシン上で公開/秘密鍵のペアを生成し、ファイアウォールに公開鍵をアップロードするので、管理者がユーザー名とパスワードを入力しなくても、安全にアクセスできるようになります。

管理者を追加するには、**Add** (追加) をクリックして以下の情報を入力します。

管理者アカウント設定	の意味
氏名	管理者のログイン名 (最大 31 文字) を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。英字、数字、ハイフン、ピリオド、およびアンダースコアのみを使用してください。ログイン名をハイフン (-) で開始することはできません。
認証プロファイル	管理者の認証の認証プロファイルを選択します。この設定は、RADIUS、TACACS+、LDAP、Kerberos、SAML、またはローカル データベース認証に使用できます。詳細は「Device (デバイス) > Authentication Profile (認証プロファイル) 」を参照してください。
クライアント証明書認証のみを使用 (Web)	Webアクセスのクライアント証明書認証を使用する場合は、このオプションを選択します。このオプションを選択すると、ユーザー名とパスワードは不要になり、ファイアウォールへのアクセス認証は証明書のみで行えるようになります。
新しいパスワード 再入力 新しいパスワード	管理者のパスワード (最大 31 文字) を入力し、確認のためにパスワードを再入力します。このパスワードは大文字と小文字を区別します。**Setup** (セットアップ) > **Management** (管理) を選択し、パスワードの最低の長さを適用することもできます。 ファイアウォール管理インターフェイスの安全性を維持するため、管理パスワードを定期的に変更することをお勧めします。管理パスワードには、小文字、大文字、および数字を混在させてください。

© 2019 Palo Alto Networks, Inc.

管理者アカウント設定	の意味
	ファイアウォールのすべての管理者用に、パスワード複雑性設定を構成することもできます。
公開キーの認証 (SSH) の使用	SSH公開キーの認証を使用する場合は、このオプションを選択します。**Import Key**[キーのインポート] をクリックし、公開キー ファイルを参照して選択します。アップロードした鍵は、読み取り専用テキスト エリアに表示されます。 サポート対象の鍵ファイルのフォーマットは、IETF SECSH と OpenSSH です。サポート対象の鍵アルゴリズムは、DSA (1,024 ビット) と RSA (768 ~ 4,096 ビット) です。 公開キー認証に失敗した場合、ファイアウォールは管理者に対しユーザーネームとパスワードを入力するようメッセージを表示します。
管理者タイプ	この管理者にロールを割り当てます。このロールによって、管理者が表示および変更できる内容が決まります。 **Role Based** [ロールベース] を選択した場合、ドロップダウンリストからカスタムロールプロファイルを選択します。詳細は「Device (デバイス) > Admin Roles (管理者ロール)」を参照してください。 **Dynamic** [動的] を選択した場合、以下の事前設定されたロールのいずれかを選択できます。 • **Superuser** (スーパーユーザー) – ファイアウォールに対するフル アクセス権を持ち、新しい管理者アカウントや仮想システムを設定することができます。スーパーユーザー権限を持っていなければ、その他のスーパーユーザー権限を持つ管理者を作成することができません。 • **Superuser** (読み取り専用スーパーユーザー) – ファイアウォールに読み取り専用でアクセスできます。 • **Device administrator** (デバイス管理者) – 新しいアカウントまたは仮想システムの定義を除き、選択したファイアウォールに対するフル アクセス権が与えられます。 • **Device administrator (read-only)** (読み取り専用デバイス管理者) – パスワード プロファイル (アクセス不可) および管理者アカウント (ログイン中のアカウントのみ表示可能) を除き、ファイアウォール設定の全項目に対し読み取りアクセスが許可されます。 • **virtual system (** 仮想システム **- vsys)** 管理者–ファイアウォール上の特定の 仮想システム へのアクセス権を持ち、仮想システムを管理します (マルチ仮想システム機能が有効になっている場合)。仮想システム管理者は、ネットワーク インターフェイス、仮想ルーター、IPSec トンネル、VLAN、仮想ワイヤー、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルにアクセスできません。 • 仮想システム管理者 (読み取り専用)–ファイアウォール上の特定の 仮想システム への読み取り専用アクセス権を持ち、仮想システムを表示します (マルチ仮想システム機能が有効になっている場合)。読み取り専用アクセス権を持つ 仮想システム 管理者

© 2019 Palo Alto Networks, Inc.

管理者アカウント設定	の意味
	は、ネットワーク インターフェイス、仮想ルーター、IPSec トンネル、VLAN、仮想ワイヤー、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルにアクセスできません。
仮想システム(vsys) (仮想システム管理者ロールのみ)	**Add** [追加] をクリックして、管理者が管理できる仮想システムを選択します。
パスワードプロファイル	パスワード プロファイルを選択します (該当する場合)。新しいパスワード プロファイルを作成する方法については、「Device (デバイス) > Password Profiles (パスワード プロファイル)」を参照してください。 管理者用のパスワードプロファイルを作成し、設定した期間が過ぎたら管理者用パスワードが必ず失効するようにします。定期的に管理者用パスワードを変更することで、保存した、あるいは盗まれた認証情報を攻撃者が使用するのを防ぐことができます。

© 2019 Palo Alto Networks, Inc.

Device > Admin Roles [デバイス > 管理者ロール]

管理者ユーザーのアクセス権限や役割を定義する、カスタマイズ可能な管理者ロールプロファイルを定義する場合は **Device** [デバイス] > **Admin Roles**[管理者ロール] を選択します。管理アカウントDevice (デバイス) > Administrators (管理者) を作成する際は、Admin Role profiles or dynamic roles (管理者ロールプロファイルや動的ロール) を割り当てます。

Panorama 管理者用の管理者ロール プロファイルを定義する場合は「Panorama > Managed Devices (管理対象デバイス) > Summary (サマリー) 」を参照してください。

ファイアウォールには一般的な用途で使用可能な3つのロールが事前定義されています。まずスーパーユーザーロールを使用して、ファイアウォールの初期設定および、セキュリティ管理者、監査管理者、および暗号管理者の管理者アカウントを作成します。アカウントを作成し、適切な共通基準管理者ロールを適用したら、それらのアカウントを使用してログインします。連邦情報処理標準 (FIPS) 、または情報セキュリティ国際評価基準 (CC) モードのデフォルトのスーパーユーザー アカウントは「**admin**」で、デフォルトのパスワードは「**paloalto**」に設定されています。標準操作モードでは、「**admin**」のデフォルトのパスワードは「**admin**」 です。事前定義の管理者ロールは、すべてのロールに監査証跡への読み取り専用のアクセス権があるという点を除き、機能が重複しないように作成されています (読み取りと削除のフル アクセス権がある監査管理者は除く)。これらの管理者ロールは変更できず、以下のように定義されています。

- auditadmin — 監査管理者は、ファイアウォールの監査データの定期的な確認を担当する責任者です。
- cryptoadmin — 暗号管理者は、ファイアウォールの安全な接続確立に関連する暗号要素の設定と保守を担当する責任者です。
- securityadmin — セキュリティ管理者は、他の 2 つの管理ロールで対処されない、その他すべての管理タスク (セキュリティ ポリシーの作成など) を担当する責任者です。

管理者ロール プロファイルを追加する場合は、**Add** (追加) をクリックし、次の表で説明する設定を指定します。

カスタムロールを作成し、管理者アクセスを各種の管理者が必要とするものだけに制限します。各種の管理者について、*Web UI*、*XML/REST API*、*Command Line* (コマンドライン)への読み取り専用アクセスを有効化、無効化、あるいは設定します。

Administrator Role Setting (管理者ロール設定)	
氏名	管理者ロールの識別に使用する名前を入力します (最大 31 文字) 。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	(任意) ロールの説明文を入力します (最大 255文字) 。
ロール	管理責任の範囲を選択します。 • **Device** [デバイス] - 1つ以上の仮想システム (vsys) を持つかどうかに関らず、このロールはファイアウォール全体に適用されます。 • 仮想システム—この ロール は、ファイアウォール上の特定の 仮想システム に適用されます (マルチ仮想システム機能が有効になっている場合)。仮想システムに基づく管理者ロール プロファイルは、**Web UI** タブで、ネッ

© 2019 Palo Alto Networks, Inc.

Administrator Role Setting（管理者ロール設定）	
	トワーク インターフェイス、VLAN、仮想ワイヤー、IPSec トンネル、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルにアクセスできません。 管理者アカウントを作成するときは（Device（デバイス）> Administrators（管理者））、仮想システムを選択します。
Web UI	アクセス権限を設定する場合は、特定の Web インターフェイス機能 のアイコンをクリックします。 • **Enable** [有効化] — 選択した機能に読み書きアクセスができます。 • **Read Only** [読み取り専用] — 選択した機能に読み取り専用でアクセスできます。 • **Disable** [無効化] — 選択した機能にアクセスできません。
XML/REST API	特定のXML/REST API 機能のアイコンをクリックして、許可するアクセス権限を設定します (**Enable** (有効) または **Disable** (無効))。

コマンド行	CLIアクセスのロールのタイプを選択します。デフォルトでは **None**（なし）に設定され、CLI へのアクセスは許可されていません。設定の選択肢は Role (ロール) の範囲によって異なります。
	• デバイス
	  • **superuser** (スーパーユーザー) - ファイアウォールに対するフルアクセス権を持ち、新しい管理者アカウントや仮想システムを設定することができます。スーパーユーザー権限を持っていなければ、その他のスーパーユーザー権限を持つ管理者を作成することができません。
	  • **superreader** (スーパーリーダー) — ファイアウォールに読み取り専用でアクセスできます。
	  • **deviceadmin**（デバイス管理者）— 新しいアカウントまたは仮想システムの定義を除き、選択したファイアウォールに対するフル アクセス権が与えられます。
	  • **devicereader**（デバイスリーダー）— パスワード プロファイル（アクセス不可）および管理者アカウント（ログイン中のアカウントのみ表示可能）を除き、ファイアウォール設定の全項目に対し読み取りアクセスが許可されます。
	• 仮想システム(**vsys**)
	  • **vsysadmin**—選択されたファイアウォールの仮想システムにアクセスでき、仮想システムの特定の要素を作成・管理します。**vsysadmin**設定は、ファイアウォール レベルまたはネットワーク レベルの機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPアドレス、IPSec トンネル、VLAN、仮想ワイヤー、仮想ルーター、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルなど) を制御できません。
	  • **vsysreader**—選択されたファイアウォールの仮想システムおよび 仮想システム の特定の要素に対する読み取り専用のアクセスが可能です。**vsysreader** 設定は、ファイアウォール レベルまたはネットワーク レベルの機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPアドレス、IPSec トンネル、VLAN、仮想ワイヤー、仮想ルーター、GRE トンネル、DHCP、DNSプロキシ、QoS、LLDP、またはネットワーク プロファイルなど) にアクセスできません。

© 2019 Palo Alto Networks, Inc.

Device > Access Domain [デバイス > アクセス ドメイン]

- Device > Access Domain [デバイス > アクセス ドメイン]

管理者のアクセスをファイアウォールで特定の仮想システムに制限するには、アクセス ドメインを設定します。ファイアウォールでアクセス ドメインがサポートされるのは、RADIUS、TACACS+、SAML アイデンティティ プロバイダ（IdP）サーバーを使用して、管理者の認証と承認を管理する場合のみです。アクセス ドメインを有効にするには、以下を定義する必要があります。

- 外部認証サーバーのサーバー プロファイル – 「Device（デバイス）> Server Profiles（サーバー プロファイル）> RADIUS」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> TACACS+」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> SAML Identity Provider（SAML アイデンティティ プロバイダ）」を参照してください。
- RADIUS ベンダー固有属性（VSA）、TACACS+ VSA、SAML 属性のいずれか。

管理者がファイアウォールへのログインを試みると、ファイアウォールは管理者のアクセス ドメインを外部サーバーに問い合わせます。外部サーバーは、関連付けられているドメインを返し、ファイアウォールは、アクセス ドメインで指定されている仮想システムに管理者を制限します。ファイアウォールが管理者の認証と承認に外部サーバーを使用しない場合、**Device**（デバイス）> **Access Domain**（アクセス ドメイン）の設定は無視されます。

Panorama では、アクセス ドメインをローカルで管理することや、*RADIUS VSA*、*TACACS+ VSA*、*SAML* 属性を使用して管理することができます（「Panorama > Access Domains（アクセス ドメイン）」を参照）。

アクセス ドメイン設定	の意味
氏名	アクセス ドメインの名前（最大 31 文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、ハイフン、アンダースコア、およびピリオドのみを使用してください。
仮想システム	Available（使用可能）列で仮想システムを選択して **Add**（追加）します。 アクセスドメインは、仮想システムをサポートするファイアウォールのみにおいてサポートされます。

© 2019 Palo Alto Networks, Inc.

Device > Authentication Profile [デバイス > 認証プロファイル]

管理者とエンド ユーザーを認証するための設定を構成するには、このページを使用します。ファイアウォールと Panorama では、ローカル、RADIUS、TACACS+、LDAP、Kerberos、SAML 2.0、多要素認証（MFA）サービスがサポートされます。

認証プロファイルを *1* つ以上作成して外部認証を提供することで、管理を行いやすくなるようにすべての認証リクエストを一か所にまとめ、トラッキングなどのサービスを含む標準的な認証プロセスを使用します。認証が失敗した場合に複数の方式を使う複数の認証プロファイルを作成して優先順位を付け（*Device (デバイス) > Authentication Sequence (認証シーケンス)*）、ローカルのログインアカウントを *1* つ以上作成してすべての外部方式が失敗した場合にフォールバックすることがベストプラクティスになります。

このページを使用して、ファイアウォールまたは Panorama のサービス（Web インターフェイスへの管理アクセスなど）を SAML アイデンティティ プロバイダ（IdP）で登録することもできます。サービスを登録すると、ファイアウォールや Panorama では IdP が使用され、サービスを要求するユーザーを認証できます。サービスを登録するには、SAML メタデータを IdP で入力します。ファイアウォールと Panorama では、サービスに割り当てた認証プロファイルに基づいて SAML メタデータ ファイルが自動的に生成され、このメタデータ ファイルを IdP にエクスポートできるため、登録が簡単です。

- 認証プロファイル
- SAML Metadata Export from an Authentication Profile（認証プロファイルから SAML メタデータをエクスポートする）

認証プロファイル

- Device > Authentication Profile [デバイス > 認証プロファイル]

Device（デバイス）> **Authentication Profile**（認証プロファイル）または **Panorama** > **Authentication Profile**（認証プロファイル）を選択し、認証プロファイルを管理します。新しいプロファイルを作成するには、プロファイルを **Add**（追加）して次のフィールドに情報を入力します。

認証プロファイルを設定したら、*CLI* コマンド「***test authentication***」を使用して、ファイアウォールまたは *Panorama* 管理サーバーがバックエンド認証サーバーと通信できるかどうか、および認証要求が成功しているかどうかを調べます。候補設定でauthentication tests（認証テスト）を実行できるため、コミットする前に設定が正しいかどうかを確認できます。

認証プロファイル設定	の意味
氏名	プロファイルの識別に使用する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、アンダースコア、およびピリオドのみを含む最大 31 文字を指定できます。名前は、他の認証プロファイルや認証シーケンスに対して、現在の **Location**[場所] (ファイアウォールまたは仮想システム) で一意である必要があります。 マルチ仮想システム モードのファイアウォールで、認証プロファイルの *Location*（場所）が仮想システムになっている場合、共有の場所の認証シーケンスと同じ名前を入力しないでください。同様に、プロファイルの *Location*（場所）が *Shared*（共有）になって

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	いる場合、仮想システム シーケンスと同じ名前を入力しないでください。このようなケースでは、同じ名前の認証プロファイルおよびシーケンスをコミットすることはできますが、参照エラーが発生する可能性があります。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location** (場所) を選択することはできません。この値は Shared (共有) (ファイアウォール) または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。

Authentication [認証]タブ

ファイアウォールでは、このタブで設定する認証サービスが起動されてから、Factors (ファクター) タブで追加する多要素認証 (MFA) サービスが起動されます。

ベンダー *API* ではなくて *RADIUS* によってファイアウォールを *MFA* ベンダーと統合する場合は、*MFA* サーバー プロファイルではなくて、そのベンダーの *RADIUS* サーバー プロファイルを設定する必要があります。

タイプ	ユーザーに表示される最初の (時に唯一の) 認証チャレンジを提供するサービスのタイプを選択します。選択内容に応じて、そのサービスに定義する、その他の設定がダイアログに表示されます。オプションは次のとおりです： • **None** (なし) — 認証を使用しません。 • **Local Database** (ローカル データベース) — ファイアウォールのローカル認証データベースを使用します。このオプションは Panorama では使用できません。 • **RADIUS** — RADIUS (Remote Authentication Dial In User Service) サーバーを使用します。 • **TACACS+** — TACACS+ (Terminal Access Controller Access-Control System Plus) サーバーを使用します。 • **LDAP** — LDAP (Lightweight Directory Access Protocol) サーバーを使用します。 • **Kerberos** — Kerberos サーバーを使用します。 • **SAML** — SAML 2.0 (Security Assertion Markup Language 2.0) アイデンティティ プロバイダ (IdP) を使用します。 管理者は *SAML* を使用して、ファイアウォールまたは *Panorama Web* インターフェイスに対して認証できますが、*CLI* に対しては認証できません。
サーバ プロファイル (RADIUS、TACACS +、LDAP、Kerberos のみ)	ドロップダウン リストから認証サーバー プロファイルを選択します。Device (デバイス) > Server Profiles (サーバー プロファイル) > RADIUS、 Device (デバイス) > Server Profiles (サーバー プロファイル) > TACACS +、 Device (デバイス) > Server Profiles (サーバー プロファイル) > LDAP、または Device (デバイス) > Server Profiles (サーバー プロファイル) > Kerberosを参照。

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
IdPサーバープロファイル （SAML のみ）	ドロップダウン リストから SAML アイデンティティ プロバイダのサーバー プロファイルを選択します。Device (デバイス) > Server Profiles (サーバー プロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ)を参照。
RADIUS からユーザー グループを取得 （RADIUS のみ）	RADIUS サーバーに定義されているベンダー固有属性（VSA）からユーザー グループ情報を収集するには、このオプションを選択します。ファイアウォールではこの情報が使用され、認証しているユーザーと許可リストのエントリが照合されます。ポリシーの適用やレポートの生成に、この情報は使用されません。
TACACS+ からユーザー グループを取得 （TACACS+ のみ）	TACACS+ サーバーに定義されているベンダー固有属性（VSA）からユーザー グループ情報を収集するには、このオプションを選択します。ファイアウォールではこの情報が使用され、認証しているユーザーと許可リストのエントリが照合されます。ポリシーの適用やレポートの生成に、この情報は使用されません。
ログイン属性 （LDAP のみ）	ユーザーを一意に識別し、そのユーザーのログイン ID として機能する LDAP ディレクトリ属性を入力します。
パスワード失効の警告 （LDAP のみ）	認証プロファイルが GlobalProtect ユーザー用である場合、パスワードの有効期限が x 日後に切れるという通知メッセージを何日前からユーザーに表示するのか、日数を入力します。デフォルトでは、通知メッセージはパスワードの有効期限の 7 日前から表示されます（範囲は 1 ~ 255 日）。パスワードの期限が切れたユーザーは、VPN にアクセスできなくなります。 pre-logon 接続方式 を使用するように *GlobalProtect* エージェントを設定することも検討してみてください。これにより、パスワードの期限が切れた後でも、ユーザーはドメインに接続してパスワードを変更できます。 ユーザーがパスワードを期限切れにしてしまった場合、管理者は仮のLDAPパスワードを割り当て、ユーザーがVPNにログインできるようにすることもできます。このワークフローでは、ポータル設定の **Cookie authentication for config refresh**[設定更新のためのCookie認証] を **Authentication Modifier**[認証修飾子] に設定することをお勧めしています（このように設定しない場合、仮のパスワードを使用してポータルへの認証を行うことができますが、ゲートウェイログインが失敗してしまい、VPNへのアクセスが行えません）。
署名要求の証明書 （SAML のみ）	アイデンティティ プロバイダ（IdP）に送信する SAML メッセージへの署名のためにファイアウォールで使用する証明書を選択します。このフィールドは、**IdP Server Profile (IdP サーバ プロファイル)**で**Sign SAML Message to IdP (IdP への SAML メッセージの署名)** オプションを有効にする場合に必要です。(Device (デバイス) > Server Profiles (サーバ プロファイル) > SAML Identity Provider (SAML アイデンティティ プロバイダ) を参照)。その他の場合、SAML メッセージに署名するために証明書を選択するかどうかは任意です。 証明書および関連付けられている秘密鍵の生成またはインポートを行うときには、証明書に指定されている鍵の用途の属性により、鍵の使用方法が制御されます。 • 証明書で鍵の用途の属性が明示的にリストされている場合、属性の 1 つはデジタル署名です。デジタル署名はファイアウォールで生成する証明書では使用できません。このような場合は、エンタープライズ認証局（CA）、またはサードパーティ CA から証明書と鍵をインポートする必要があります。

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	• 証明書で鍵の用途の属性が指定されていない場合は、メッセージの署名も含めて、どのような目的にも鍵を使用できます。このような場合は、任意の方法で証明書と鍵を取得 して SAML メッセージに署名できます。 *Palo Alto Networks では、署名証明書を使用して、IdP に送信する SAML メッセージの整合性を確保することをお勧めしています。*
シングルログアウトの有効化 （SAML のみ）	1 つのサービスからログアウトしたユーザーが、すべての認証済みサービスからログアウトできるようにするには、このオプションを選択します。シングル ログアウト（SLO）は、ユーザーが SAML 認証でアクセスしたサービスにのみ適用されます。サービスが組織の外部にあるか組織の内部（ファイアウォール Web インターフェイスなど）にあるかは問いません。このオプションが適用されるのは、**Identity Provider SLO URL**（アイデンティティ プロバイダ **SLO URL**）を IdP サーバー プロファイルで入力した場合のみです。キャプティブ ポータル ユーザーでは SLO を有効にできません。 ユーザーのログアウト後、ファイアウォールでは IP アドレスとユーザーネームのマッピング が自動的に削除されます。
証明書プロファイル （SAML のみ）	ファイアウォールで検証に使用する証明書プロファイルを選択します。 • IdP サーバー プロファイルで指定されている **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）です。IdP ではこの証明書が使用されて、ファイアウォールに対して認証が行われます。認証プロファイル設定を **Commit**（コミット）すると、ファイアウォールでは証明書が検証されます。 • シングル サインオン（SSO）とシングル ログアウト（SLO）の認証のために IdP がファイアウォールに送信する SAML メッセージ。IdP は、IdP サーバー プロファイルで指定されている **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）を使用してメッセージに署名します。 「Device（デバイス）> Certificate Management（証明書の管理）> Certificate Profile（証明書プロファイル）」を参照してください。
ユーザー ドメイン AND ユーザー名修飾子 （SAML を除くすべての認証タイプ）	ファイアウォールでは、認証しているユーザーと許可リストのエントリの照合、および User-ID グループ マッピング に **User Domain**（ユーザー ドメイン）が使用されます。 **Username Modifier**（ユーザー名修飾子）を使用すると、ユーザーがログイン時に入力するドメイン/ユーザー名の文字列を変更できます。ファイアウォールでは、変更された文字列が認証に使用されます。以下のオプションから選択します。 • 未変更のユーザー入力のみを送信するには、**User Domain**（ユーザー ドメイン）を空白（デフォルト）のままにして、**Username Modifier**（ユーザー名修飾子）を変数 **%USERINPUT%**（デフォルト）に設定します。 • ユーザー入力の前にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERDOMAIN%\%USERINPUT%** に設定します。 • ユーザー入力の後にドメインを追加するには、**User Domain**[ユーザー ドメイン] を入力して、**Username Modifier**[ユーザー名修飾子] を **%USERINPUT%@%USERDOMAIN%** に設定します。

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	Username Modifier[ユーザー名修飾子] に *%USERDOMAIN%* 変数が含まれている場合、ユーザーが入力したドメイン文字列は *User Domain[ユーザー ドメイン]* の値に置き換わります。*%USERDOMAIN%* 変数を指定して *User Domain[ユーザードメイン]* を空白のままにすると、ファイアウォールはユーザーが入力したドメイン文字列を削除します。ファイアウォールは、ドメイン名を*User-IDグループマッピング*に適した*NetBIOS*名に解決します。これは親ドメインと子ドメインの両方に適応されます。*User Domain[ユーザー ドメイン]* の修飾子は、自動的に導出される *NetBIOS* 名よりも優先されます。 • ファイアウォールがサーバ プロファイル タイプを使用して、認証シーケンスでユーザー入力のフォーマットをいつどのように変更するかを決定できるようにするには **Username Modifier (ユーザー名修飾子)** として **None**を手動で入力します。このオプションの詳細については、『PAN-OS 管理者ガイド』の認証プロファイルおよびシーケンスの設定を参照してください。
Kerberos レルム （SAML を除くすべての認証タイプ）	ネットワークで Kerberos シングル サインオン (SSO) がサポートされている場合、**Kerberos Realm**[Kerberos レルム] (最大 127 文字) を入力します。これは、ユーザー ログイン名のホスト名部分です。例：ユーザー アカウント名が user@EXAMPLE.LOCAL の場合、レルムは EXAMPLE.LOCAL になります。
Kerberos Keytab（Kerberos キータブ） （SAML を除くすべての認証タイプ）	ネットワークで Kerberos シングルサインオン（SSO）がサポートされている場合、**Import**（インポート）、**Browse**（参照）の順にクリックしてキータブ ファイルを見つけたら **OK** をクリックします。キータブには、SSO認証に必要となる、ファイアウォールのKerberosアカウント情報（プリンシパル名およびハッシュされたパスワード）が含まれています。各認証プロファイルに、1 つのキータブを含めることができます。ファイアウォールは、認証中にまずキータブを使用してSSOを確立しようとします。これに成功した場合、アクセスを試行しているユーザーが許可リストに含まれていれば、認証は即座に成功します。含まれていない場合、認証プロセスは、指定した **Type**（タイプ）の手動認証（ユーザー名/パスワード）にフォールバックします。Type（タイプ）には Kerberos 以外のタイプも指定できます。 ファイアウォールが*FIPS/CC*モードの場合、アルゴリズムは*aes128-cts-hmac-sha1-96*または*aes256-cts-hmac-sha1-96*に設定されている必要があります。それ以外の場合、*des3-cbc-sha1* または *arcfour-hmac* も使用できます。ただし、キータブのアルゴリズムと、*SSO* を有効にするためにチケット発行サービスからクライアントに発行されるサービス チケットのアルゴリズムが一致していない場合、*SSO* プロセスは失敗します。サービス チケットで使用されるアルゴリズムは、*Kerberos* 管理者が決定します。
ユーザー名属性 （SAML のみ）	IdP からのメッセージに含まれる、認証しているユーザーのユーザー名を特定する SAML 属性を入力します（デフォルトは **username**）。**IdP Server Profile**（**IdP** サーバー プロファイル）にユーザー名属性を指定するメタデータが含まれている場合、ファイアウォールでは、このフィールドにそのユーザー名属性が自動的に入力されます。ファイアウォールでは、SAML メッセージから取得されたユーザー名が、認証プロファイルの **Allow List**（許可リスト）のユーザーおよびユーザー グループと照合されます。SAML ログイン時に入力するドメイン/ユーザー名の文字列を変更するようにファイアウォールを設定することはできないため、ログイン

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	ユーザー名は **Allow List**（許可リスト）のエントリと正確に一致する必要があります。必須の SAML 属性はこれのみです。 *SAML* メッセージのサブジェクト フィールドには、ユーザー名が表示されることがあります。ユーザー名属性にユーザー名が表示されない場合、ファイアウォールではサブジェクト フィールドが自動的にチェックされます。
ユーザー グループ属性 （SAML のみ）	IdP からのメッセージで、認証しているユーザーのユーザー グループを特定する SAML 属性を入力します（デフォルトは **usergroup**）。**IdP Server Profile**（**IdP** サーバー プロファイル）にユーザー グループ属性を指定するメタデータが含まれている場合、このフィールドでは、そのユーザー グループ属性が自動的に使用されます。ファイアウォールではグループ情報が使用され、認証しているユーザーと **Allow List**（許可リスト）のエントリが照合されます。ポリシーやレポートに、この情報は使用されません。
管理者ロール属性 （SAML のみ）	IdP からのメッセージで、認証しているユーザーの管理者ロールを特定する SAML 属性を入力します（デフォルトは **admin-role**）。この属性は、エンド ユーザーではなく、ファイアウォール管理者にのみ適用されます。**IdP Server Profile**（**IdP** サーバー プロファイル）に管理者ロール属性を指定するメタデータが含まれている場合、ファイアウォールでは、このフィールドにその管理者ロール属性が自動的に入力されます。ファイアウォールでは、事前定義（ダイナミック）ロールまたは管理者ロール プロファイルが、SAML メッセージから取得したロールと照合され、ロールベースのアクセス制御が適用されます。ロールが 1 つのみの管理者に対して複数の管理者ロールの値が SAML メッセージに含まれる場合は、管理者ロール属性の最初の（左端の）値のみが照合されます。ロールが複数ある管理者の場合は、その属性の複数の値が照合されます。
アクセス ドメイン属性 （SAML のみ）	IdP からのメッセージで、認証しているユーザーのアクセス ドメインを特定する SAML 属性を入力します（デフォルトは **access-domain**）。この属性は、エンド ユーザーではなく、ファイアウォール管理者にのみ適用されます。**IdP Server Profile**（**IdP** サーバー プロファイル）にアクセス ドメイン属性を指定するメタデータが含まれている場合、ファイアウォールでは、このフィールドにそのアクセス ドメイン属性が自動的に入力されます。ファイアウォールでは、ローカルに設定されているアクセス ドメインが、SAML メッセージから取得したアクセス ドメインと照合され、アクセス制御が適用されます。アクセス ドメインが 1 つのみの管理者に対して複数のアクセス ドメインの値が SAML メッセージに含まれる場合は、アクセス ドメイン属性の最初の（左端の）値のみが照合されます。アクセス ドメインが複数ある管理者の場合は、その属性の複数の値が照合されます。
Factors（ファクター）タブ	
追加の認証ファクターの有効化	ユーザーが最初の要素（**Authentication**（認証）タブの **Type**（タイプ）フィールドに指定）に正常に応答した後で、追加の認証ファクター（チャレンジ）をファイアウォールで起動する場合は、このオプションを選択します。 追加の認証ファクタは、認証ポリシーのみを使用するエンドユーザー認証でサポートされます。*GlobalProtect* ポータルとゲートウェイへのリモートユーザー認証、または *PAN-OS* パノラマ *Web* インターフェイスへの管理者認証では、その他のファクターはサポートされていません。追加のファクターを設定することはできますが、これらの使用例に対しては強制されません。ただし、すべて

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	の認証使用例について、*RADIUS* または *SAML* を使用して *MFA* ベンダーと統合することはできます。 多要素認証（MFA）を使用する認証プロファイルを設定したら、認証を実施するオブジェクト（Objects（オブジェクト）> Authentication（認証））にその認証プロファイルを割り当てた後、そのオブジェクトを認証ポリシー ルール（Policies（ポリシー）> Authentication（認証））に割り当て、ネットワーク リソースへのアクセスを制御する必要があります。
度	ユーザーが最初の要素（**Authentication**（認証）タブの **Type**（タイプ）フィールドで指定）に正常に応答した後、ファイアウォールが起動する認証要素ごとに、MFA サーバー プロファイル（Device（デバイス）> ServerProfiles > Multi Factor Authentication（多要素認証））を追加します。ファイアウォールでは、要素を提供する MFA サービスのリストの上から下へと、順に各要素が起動されます。この順番を変更する場合は、サーバー プロファイルを選択して **Move Up**（上へ）または **Move Down**（下へ）をクリックします。指定できる追加要素は 3 つまでです。各 MFA サービスが提供する要素は 1 つです。一部の MFA サービスでは、ユーザーが複数の要素のリストから 1 つの要素を選択できます。ファイアウォールは、ベンダー API によって、これらの MFA サービスと統合します。その他の MFA vendor API integrations（MFA ベンダー API 統合）は、Applications（アプリケーション）または Applications and Threats（アプリケーションと脅威）コンテンツ更新により定期的に追加されます。
Advanced Tab（詳細タブ）	
許可リスト	**Add**（追加）をクリックして **all**（すべて）を選択するか、このプロファイルで認証できる特定のユーザーおよびグループを選択します。ユーザーが認証を行うと、ファイアウォールでは、関連付けられているユーザー名またはグループが、このリストのエントリと照合されます。エントリを追加しないと、ユーザーの認証を行うことができません。 アクセスを行わなければならない正当なビジネス上の理由を持っているユーザーに認証を限定して攻撃の入り口を減らすには、ユーザーあるいはユーザーグループを指定し、*all (すべて)*は使用しないでください。 *[ユーザー ドメイン]* の値を入力した場合、*[許可リスト]* でドメインを指定する必要はありません。たとえば、*User Domain*（ユーザー ドメイン）が ***businessinc*** で、ユーザー ***admin1*** を *Allow List*（許可リスト）に追加する場合、「***`admin1`***」と入力すれば、「***`businessinc\admin1`***」と入力したことになります。ディレクトリサービスにすでに存在するグループを指定するか、*LDAP*フィルタに基づいてカスタムグループを指定できます。
最大試行回数 （SAML を除くすべての認証タイプ）	ファイアウォールで許容されるログイン連続試行回数（0 ~ 10）を入力します。この回数を超えるとユーザーアカウントはロックアウトされます。値 0 を指定すると、無制限にログインを試行できます。デフォルト値は、通常の運用モードのファイアウォールでは 0、FIPS-CC モードのファイアウォールでは 10 です。 *Failed Attempts (試行失敗回数)*の値を *5* 以下に設定し、入力ミスに備えてある程度猶予を持たせつつ、悪意のあるシステムがブルート

© 2019 Palo Alto Networks, Inc.

認証プロファイル設定	の意味
	フォースによってファイアウォールにログインしようとするのを防ぎます。 *Failed Attempts[最大試行回数] を 0 以外の値に設定しても、Lockout Time[ロックアウト時間] を 0 のままにしておくと、Failed Attempts[最大試行回数] は無視され、ユーザーはロックアウトされません。*
ロックアウト時間 （SAML を除くすべての認証タイプ）	ユーザーが **Failed Attempts**（最大試行回数）の数値に達した場合にファイアウォールがユーザー アカウントをロックアウトする時間（範囲は 0 ~ 60 分、デフォルトは 0 分）を入力します。値を 0 にすると、管理者が手動でユーザー アカウントをロック解除するまでロックアウトが適用されます。 *Lockout Time (ロックアウト時間)を 30 分以上に設定し、攻撃者が続けてログインを試みるのを防ぎます。* *Lockout Time[ロックアウト時間] を 0 以外の値に設定しても、Failed Attempts[最大試行回数] を 0 のままにしておくと、Lockout Time[ロックアウト時間] は無視され、ユーザーはロックアウトされません。*

SAML Metadata Export from an Authentication Profile（認証プロファイルから SAML メタデータをエクスポートする）

- Device > Authentication Profile [デバイス > 認証プロファイル]

ファイアウォールや Panorama は、サービスを要求したユーザーを SAML アイデンティティ プロバイダ（IdP）を使用して認証できます。管理者の場合、サービスは Web インターフェイスへのアクセスになることもあります。エンド ユーザーの場合、サービスはネットワーク リソースへのアクセスを可能にするキャプティブ ポータルまたは GlobalProtect になることもあります。サービスの SAML 認証を有効にするには、IdP でそのサービスの特定の情報（SAML メタデータ形式）を入力して、サービスを登録する必要があります。ファイアウォールや Panorama は、サービスに割り当てた認証プロファイルに基づいて SAML メタデータ ファイルを自動生成することで登録を簡略化します。このメタデータ ファイルは IdP にエクスポートできます。メタデータのエクスポートは、IdP の各メタデータ フィールドに値を入力するよりも簡単に行うことができます。

エクスポート ファイルのメタデータの一部は、認証プロファイルに割り当てられた *SAML IdP* サーバー プロファイルから取得されます（Device（デバイス）> Server Profiles（サーバー プロファイル）> SAML Identity Provider（SAML アイデンティティ プロバイダ））。ただし、エクスポート ファイルでは、*SAML IdP* サーバー プロファイルで指定されたメソッドに関係なく、*HTTP* バインディング メソッドとして常に *POST* が指定されます。*IdP* は *POST* メソッドを使用して *SAML* メッセージをファイアウォールまたは *Panorama* に送信します。

認証プロファイルから SAML メタデータをエクスポートするには、Authentication（認証）列の SAML **Metadata**（メタデータ）リンクをクリックし、以下のフィールドを入力します。メタデータ ファイルを IdP にインポートする方法については、IdP のドキュメントを参照してください。

© 2019 Palo Alto Networks, Inc.

SAML メタデータのエクスポート設定	の意味
Commands（コマンド）	SAML メタデータをエクスポートするサービスを選択します。 • **management**（管理）（デフォルト）– Web インターフェイスへの管理者アクセスを提供します。 • **captive-portal**（キャプティブ ポータル）– キャプティブ ポータルを介したネットワーク リソースへのエンド ユーザー アクセスを提供します。 • **global-protect**（**GlobalProtect**）– GlobalProtect を介したネットワーク リソースへのエンド ユーザー アクセスを提供します。 選択内容により、ダイアログに表示されるフィールドが変わります。
[Management（管理）| Captive Portal（キャプティブ ポータル）| GlobalProtect] Auth Profile（認証プロファイル）	メタデータのエクスポート元である認証プロファイルの名前を入力します。デフォルト値は、**Metadata**（メタデータ）リンクをクリックして開いたときのプロファイルです。
Management Choice（管理の選択） （管理のみ）	管理トラフィックで有効にするインターフェイス（MGT インターフェイスなど）を指定するためのオプションを選択します。 • **Interface**（インターフェイス）– ファイアウォールのインターフェイスのリストからインターフェイスを選択します。 • **IP Hostname**（**IP** ホスト名）– インターフェイスの IP アドレスまたはホスト名を入力します。ホスト名を入力する場合、DNS サーバーのアドレス（A）レコードが IP アドレスにマッピングされている必要があります。
[Captive Portal（キャプティブ ポータル）| GlobalProtect] Virtual System（仮想システム） （キャプティブ ポータルまたは GlobalProtect のみ）	キャプティブ ポータル設定または GlobalProtect ポータルを定義する仮想システムを選択します。
IP ホスト名 （キャプティブ ポータルまたは GlobalProtect のみ）	サービスの IP アドレスまたはホスト名を入力します。 • **Captive Portal**（キャプティブ ポータル）– **Redirect Host**（リダイレクト ホスト）の IP アドレスまたはホスト名を入力します（**Device**（デバイス）> **User Identification**（**User-ID**）> **Captive Portal Settings**（キャプティブ ポータルの設定））。 • **GlobalProtect** – GlobalProtect ポータルの **Hostname**（ホスト名）または **IP Address**（**IP** アドレス）を入力します。 ホスト名を入力する場合、DNS サーバーのアドレス（A）レコードが IP アドレスにマッピングされている必要があります。

© 2019 Palo Alto Networks, Inc.

Device > Authentication Sequence [デバイス > 認証シーケンス]

- Device > Authentication Sequence [デバイス > 認証シーケンス]
- Panorama > Authentication Sequence [デバイス > 認証シーケンス]

一部の環境では、ユーザー アカウントが複数のディレクトリ内に存在します（LDAP や RADIUSなど）。認証シーケンスとはログインの際にファイアウォールが使用する一連の認証プロファイルを指します。ファイアウォールは1つのプロファイルで正常にユーザーが認証されるまで、リストの上から下へ順番に、認証、Kerberosシングルサインオン、許可リスト、アカウントロックアウト値を含めたプロファイルをすべて試行し、各ユーザーに適用します。シーケンスのすべてのプロファイルで認証できなかった場合にのみ、ファイアウォールはアクセスを拒否します。認証プロファイルの詳細は「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照してください。

異なる認証方法を使用する複数の認証プロファイルを持つ認証シーケンスを設定します。*2* つ以上の外部認証方式、単一のローカル（内部）方式を設定し、接続の問題で認証が妨げられないようにします。ローカル認証プロファイルをシーケンスの最後のプロファイルにすることで、すべての外部認証が失敗した場合にのみそれを使用するようにします。（外部認証はロギングやトラブルシューティング機能が含まれる専用の、信頼できる一元的な認証サービスを提供します）

認証シーケンス設定	の意味
氏名	シーケンスの識別に使用する名前を入力します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、アンダースコア、およびピリオドのみを含む最大 31 文字を指定できます。名前は、他の認証シーケンスや認証プロファイルに対して、現在の **Location**[場所] (ファイアウォールまたは仮想システム) で一意である必要があります。 複数の仮想システムがあるファイアウォールで、認証シーケンスの *[場所]* が仮想システム *(vsys)* になっている場合、共有の場所の認証プロファイルと同じ名前を入力しないでください。同様に、シーケンスの *Location*（場所）が *Shared*（共有）になっている場合、*vsys* のプロファイルと同じ名前を入力しないでください。このようなケースでは、同じ名前の認証シーケンスおよびプロファイルをコミットすることはできますが、参照エラーが発生する可能性があります。
場所	シーケンスを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。シーケンスを保存すると、その [場所] を変更できなくなります。
ドメインを使用して認証プロファイルを決定します	ファイアウォールで、シーケンスに関連付けられている認証プロファイルの**User Domain**[ユーザードメイン] または **Kerberos Realm**[Kerberosレルム] を使用して、ユーザーがログイン中に入力するドメイン名を照合し、そのプロファイルを使用してユーザーを認証する場合は、このオプションを選択（デフォルト）します。ファイアウォールが照合に使用するユーザー入力は、ユーザー名の前の

© 2019 Palo Alto Networks, Inc.

認証シーケンス設定	の意味
	テキスト（区切り文字は円記号）またはユーザー名の後のテキスト（区切り文字は@）になります。一致が見つからない場合、ファイアウォールはシーケンスの認証プロファイルを上から下へ順に試行します。
認証プロファイル	**Add**[追加] をクリックし、シーケンスに追加する各認証プロファイルのドロップダウンリストから選択します。リストの順番を変更するには、プロファイルを選択して **Move Up**[上へ] または **Move Down**[下へ] をクリックします。プロファイルを削除するには、プロファイルを選択して **Delete**[削除] をクリックします。 多要素認証（*MFA*）サーバー プロファイルまたは *Security Assertion Markup Language*（*SAML*）アイデンティティ プロバイダ サーバー プロファイルを指定する認証プロファイルは追加できません。

© 2019 Palo Alto Networks, Inc.

Device > VM Information Sources [デバイス > VM 情報の送信元]

ここに挙げる送信元（VMware ESXiサーバー、VMware vCenterサーバー、Amazon Web Services Virtual Private Cloud (AWS-VPC)、Google Compute Engine（GCE））にデプロイされた仮想マシン（VM）に対する変更内容をプロアクティブに追跡する場合はこのタブを使用します。

*VM-Series NSX*エディション製品の一部となっている*ESXi*ホストをモニターしており、仮想環境内の変更点を調べる場合は、*VM*情報ソースの代わりに動的アドレスグループを使用してください。*M-Series NSX*エディション製品の場合、*NSX*マネージャは*IP*アドレスの所属する*NSX*セキュリティグループの情報を*Panorama*に提供します。*NSX*マネージャーはサービスプロファイル*ID*を使用して識別を行うので、*NSX*マネージャからの情報には動的アドレスグループにおける一致条件を定義するために必要な情報がすべて含まれています。このため、複数の*NSX*セキュリティグループにまたがって*IP*アドレスが重複している場合にも適切なポリシーを適用することができます。

最大 *32* 個のタグを *IP* アドレスに登録できます。

VM 情報ソースをモニターするには、以下の 2 つの方法があります。

- ファイアウォールは VMware ESXi サーバー、VMware vCenter サーバー、GCE インターフェイス、および AWS-VPCs をモニターし、モニター対象ソースにゲストがプロビジョニングまたは変更された場合は変更内容を取得できます。ファイアウォールまたは複数の仮想システムで設定されたファイアウォール上の仮想システムごとに、最大 10 個のソースを設定できます。

  ファイアウォールが高可用性（HA）構成で設定されている場合、次の条件が適用されます。

  - アクティブ/パッシブ **HA** 設定–アクティブ ファイアウォールのみが VM 情報ソースをモニターします。
  - アクティブ/アクティブセットアップでは、優先度の値が `primary`（プライマリ）のファイアウォールのみが VM 情報ソースをモニターします。

  VM 情報ソースとダイナミック アドレス グループによる同期動作と、仮想環境の変更をモニターする機能についての詳細は、『VM-Series デプロイメント ガイド』を参照してください。
- IP アドレス-ユーザー名のマッピングについては、Windows User ID エージェントまたはファイアウォールに VM 情報ソースを設定して、VMware ESXi サーバーと vCenter サーバーをモニターし、サーバーに設定されたゲストがプロビジョニングまたは変更された場合は変更内容を取得できます。Windows ユーザー ID エージェントは最大 100 個のソースをサポートします。ユーザー ID エージェントは AWS と Google Compute Engine で利用できません。

  モニター対象の *ESXi* または *vCenter Server* の各 *VM* に *VMware Tools* がインストールされていて実行中である必要があります。*VMware Tools* を使用して、各 *VM* に割り当てられた *IP* アドレスとその他の値を収集できます。

モニター対象 VM に割り当てられた値を収集するには、ファイアウォールで以下の表の属性をモニターする必要があります。

VMware ソースでモニターされる属性
• UUID • 氏名 • ゲスト OS • 注釈

© 2019 Palo Alto Networks, Inc.

VMware ソースでモニターされる属性

- VM State — 電源状態は、`poweredOff`、`poweredOn`、`standBy`、`unknown` です。
- バージョン
- ネットワーク —仮想スイッチ名、ポート グループ名、VLAN ID。
- コンテナ名 — vCenter 名、データ センター オブジェクト名、リソース プール名、クラスタ名、ホスト、ホスト IP アドレス。

AWS-VPC でモニターされる属性

- アーキテクチャ
- ゲスト OS
- イメージ ID
- インスタンス ID
- インスタンスの状態
- インスタンス タイプ
- Key Name
- 配置 — テナンシー、グループ名、可用性ゾーン
- プライベート DNS 名
- パブリック DNS 名
- サブネット ID
- Tag (key、value) (インスタンスごとに最大 18 個のタグをサポート)
- VPC ID

Google Compute Engine (GCE) 上でモニタリングする属性

- VM のホスト名
- マシン タイプ
- プロジェクト ID
- プラットフォーム (OS タイプ)
- ステータス
- サブネットワーク
- VPC ネットワーク
- ゾーン

Add (追加) — VM モニタリングの新しいソースを追加するには、**Add** (追加) をクリックし、モニターするソースに応じて詳細を入力します。

- VMware ESXi または vCenter サーバーの場合、「VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソースを有効にするための設定」を参照してください。
- AWS-VPC の場合、「AWS VPC の VM 情報ソースを有効にするための設定」を参照してください。
- Google Compute Engine (GCE) の場合は、Settings to Enable VM Information Sources for Google Compute Engine (Google Compute Engine の VM 情報ソースを有効にするための設定) を参照してください。

Refresh Connected (接続対象の更新) —画面に表示される接続状況を更新します。 これは、ファイアウォールとモニタリング対象のソース間の接続は更新しません。

Delete (削除) —選択した設定済みの VM 情報ソースを削除します。

© 2019 Palo Alto Networks, Inc.

PDF/CSV—VM 情報ソース設定テーブルを PDF またはカンマ区切り値（CSV）ファイルとしてエクスポートします。「Configuration Table Export（設定バンドルのエクスポート）」を参照してください。

VMware ESXi サーバーおよび vCenter サーバーの VM 情報ソースを有効にするための設定

以下の表では、VMware ESXi および vCenter サーバー用に VM 情報の送信元を有効にするために指定する設定について説明します。

Virtual Machine (仮想マシン - VM) のタグを取得するには、ファイアウォールに、*VMware ESXi* および *vCenter* サーバーで読み取り専用アクセス権のあるアカウントが必要です。

VMware ESXi または vCenter サーバーの VM 情報の送信元の有効化設定	
氏名	モニター対象ソースの識別に使用する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
タイプ	モニター対象のホスト/ソースが **ESXi server**[ESXi サーバー]か、**vCenter server**[vCenter サーバー]かを選択します。
の意味	（任意）送信元の場所または機能を識別するラベルを追加します。
ポート	ホスト/ソースのリスニング ポートを指定します。(デフォルト ポートは 443)。
enabled [有効化]	デフォルトでは、ファイアウォールと設定されたソース間の通信は有効になっています。 モニター対象ソースとファイアウォール間の接続状態は、インターフェイスに以下のように表示されます。 • 接続済み • 切断 • 保留。モニター対象ソースが無効になっている場合は、通信状態も黄色で表示されます。 ホストとファイアウォール間の通信を無効にするには、**Enabled** [有効] のオプションをオフにします。
タイムアウト	ホストが応答しない場合、モニター対象送信元への接続を切断するまでの間隔を入力します（範囲は2～10時間、デフォルトは2時間）。 （任意）デフォルト値を変更する場合は、**Enable timeout when the source is disconnected**（送信元切断時のタイムアウトを有効にする）を選択して、値を指定します。指定された制限に達した際、ホストがアクセス不能であるか応答しない場合は、ファイアウォールによって送信元への接続が閉じられます。
送信元	モニターするホスト/ソースの FQDN または IP アドレスを入力します。
username	送信元に対する認証に必要なユーザー名を指定します。

© 2019 Palo Alto Networks, Inc.

VMware ESXi または vCenter サーバーの VM 情報の送信元の有効化設定	
パスワード	パスワードを入力し、確認のために再入力します。
更新間隔	ファイアウォールが送信元から情報を取得する間隔（秒数）を指定します（範囲は 5–600、デフォルトは5）。

AWS VPC の VM 情報ソースを有効にするための設定

以下の表では、AWS VPC 用に VM 情報の送信元を有効にするために指定する設定について説明します。

AWS VPC の VM 情報ソースを有効にするための設定	
氏名	モニター対象ソースの識別に使用する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
タイプ	**AWS VPC** を選択します。
の意味	（任意）送信元の場所または機能を識別するラベルを追加します。
enabled [有効化]	デフォルトでは、ファイアウォールと設定されたソース間の通信は有効になっています。 モニター対象ソースとファイアウォール間の接続状態は、インターフェイスに以下のように表示されます。 • 接続済み • 切断 • 保留。モニター対象ソースが無効になっている場合は、通信状態も黄色で表示されます。 ホストとファイアウォール間の通信を無効にするには、**Enabled** [有効] のオプションをオフにします。
送信元	Virtual Private Cloud が存在する URI を追加します。例: ec2.us-west-1.amazonaws.com 構文は次のとおりです: ec2. <*your_AWS_region*>.amazonaws.com; AWS China の場合：ec2.<AWS_region>.amazonaws.com.cn
アクセス キー ID	AWS アカウントを所有するか、アクセスを許可されているユーザーを一意に識別する英数字のテキスト文字列を入力します。 この情報は、AWS セキュリティ認証情報の一部です。ファイアウォールでは、AWS サービスに対する API コールにデジタル署名するための認証情報 (アクセス キー ID と秘密アクセス キー) が要求されます。
秘密アクセス キー	パスワードを入力し、確認のために再入力します。
更新間隔	ファイアウォールが送信元から情報を取得する間隔（秒数）を指定します（範囲は 60 ~ 1,200、デフォルトは 60）。

© 2019 Palo Alto Networks, Inc.

AWS VPC の VM 情報ソースを有効にするための設定	
タイムアウト	ホストが応答しない場合、モニター対象ソースへの接続を閉じるまでの時間（デフォルトは2時間） （任意）**Enable timeout when the source is disconnected**（送信元切断時のタイムアウトを有効にする）を選択します。指定された制限に達した際、送信元がアクセス不能であるか応答しない場合は、ファイアウォールによって送信元への接続が閉じられます。
VPC ID	モニターする AWS-VPC の ID を入力します (例: vpc-1a2b3c4d)。この VPC 内にデプロイされている EC2 インスタンスのみがモニターされます。 アカウントがデフォルトの VPC を使用するように設定されている場合、デフォルトの VPC ID が AWS アカウント属性の下にリストされます。

Google Compute Engine の VM 情報ソースを有効にするための設定

Device（デバイス）> **VM Information Sources**（**VM** 情報の送信元）> **Add**（追加）

次の表は、Google Cloud Platform で Google Compute Engine インスタンスの VM 情報送信元を有効にするために必要な設定について説明します。Google Compute Engine（GCE）インスタンスの監視を有効にして、特定のプロジェクトの Google Cloud ゾーンで実行中のインスタンスに関するタグ、ラベル、その他のメタデータを取得するために、ファイアウォール（社内の仮想マシンまたは仮想マシン内の Google Cloud）を許可します 。Google Cloud Platform の VM-Series については、「VM-Series デプロイメント ガイド」を参照してください。

Google Compute Engine の VM 情報ソースを有効にするための設定	
氏名	モニター対象ソースの識別に使用する名前を入力します (最大 31 文字)。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
タイプ	**Google Compute Engine** を選択します。
の意味	（任意）送信元の場所または機能を識別するラベルを追加します。
enabled [有効化]	デフォルトでは、ファイアウォールと設定されたソース間の通信は有効になっています。 モニター対象ソースとファイアウォール間の接続状態は、インターフェイスに以下のように表示されます。 • —接続済み • —切断 • —保留中または監視対象のソースが無効です。 設定対象の送信元とファイアウォール間の通信を無効にするには、**Enabled**（有効）のオプションをオフにします。 通信を無効にすると、登録されているすべての IP アドレスとタグが、関連付けられた動的アドレス グループから削除されます。つまり、ポ

© 2019 Palo Alto Networks, Inc.

Google Compute Engine の VM 情報ソースを有効にするための設定	
	リシー ルールは このGoogle Cloud プロジェクトの GCE インスタンスには適用されません。
Service Authentication Type（サービス認証タイプ）	GCE またはサービス アカウントで実行する VM-Series を選択します。 • **VM-Series running on GCE**（**GCE** で実行する **VM-Series**）—VM 監視を有効にするハードウェア ベースまたは VM Series のファイアウォールが Google Cloud Platform 内にデプロイされていない場合は、このオプションを選択します。 • **Service Account**（サービス アカウント）—Google Cloud Platform にデプロイされていないファイアウォールで Google Cloud Engine インスタンスを監視する場合は、このオプションを選択します。このオプションを使用すると、個々のエンドユーザー アカウントを使用せずに、仮想マシンまたはアプリケーションに属する特別な Google アカウントを使用できます。 サービスアカウントには、Google API へのアクセスを許可する IAM ポリシー（**Compute Engine** > **Compute Viewer**特権）が必要で、仮想マシンのメタデータ用に Google Cloud Project内の仮想マシンにクエリを実行できるようにする必要があります。
サービス アカウント認証情報	（サービスアカウントのみ）サービス アカウントの資格情報を含む JSON ファイルをアップロードします。このファイルにより、ファイアウォールはインスタンスに対して認証され、メタデータへのアクセスが許可されます。 Google Cloud コンソール(**IAM & admin**（**IAM** および管理） > **Service Accounts**（サービス アカウント）)にアカウントを作成できます。アカウントを作成し、そのアカウントにキーを追加し、ファイアウォールにアップロードする必要がある JSON ファイルをダウンロードする方法については、Google のドキュメントを参照してください。
プロジェクト ID	監視する Google Cloud Project を一意に識別する英数字の文字列を入力します。
Zone Name（ゾーン名）	ゾーン情報を最大 63 文字の文字列で入力します。例:`us-west1-a`.
更新間隔	ファイアウォールが送信元から情報を取得する間隔（秒数）を指定します（範囲は 60 ~ 1,200、デフォルトは 60）。
タイムアウト	ホストが応答しない場合、モニター対象ソースへの接続を閉じるまでの時間（デフォルトは2時間） （任意）**Enable timeout when the source is disconnected**（送信元切断時のタイムアウトを有効にする）を選択します。指定された制限に達した際、アクセス不能であるか応答しない場合は、ファイアウォールによって送信元への接続が閉じられます。ソースが切断されると、このプロジェクトから登録されたすべての IP アドレスとタグが動的アドレスグループから削除されます。

© 2019 Palo Alto Networks, Inc.

Device (デバイス) > Troubleshooting (トラブルシューティング)

- **Device (デバイス) > Troubleshooting (トラブルシューティング)**
- **Panorama > Managed Devices (管理対象のデバイス) > Troubleshooting (トラブルシューティング)**

デバイスグループあるいはテンプレート設定の変更をコミットする前に、Web インターフェイスから機能をテストし、変更によって現在アクティブな設定に接続性の問題が生じないこと、ポリシーが正しくトラフィックを許可あるいは拒否していることを確認します。

- ポリシーマッチのテスト
  - Security Policy Match セキュリティポリシー マッチ
  - QoS ポリシー マッチ
  - Authentication Policy Match 認証ポリシー マッチ
  - 復号化/SSL ポリシー マッチ
  - NAT ポリシー マッチ
  - ポリシー ベース フォワーディング ポリシー マッチ
  - DoS ポリシー マッチ
- 接続性のテスト
  - routing
  - Wildfire をテスト
  - Threat Vault
  - ping
  - トレース ルート
  - ログコレクタの接続性
  - 外部ダイナミック リスト
  - 更新サーバー
  - クラウド ロギングサービスのステータスをテスト
  - クラウド GP サービスのステータスをテスト

Security Policy Match セキュリティポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(Panorama のみ) デバイスを選択	**Select device/VSYS (デバイス/VSYS を選択)**し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
(Panorama のみ) 選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。

© 2019 Palo Alto Networks, Inc.

項目	の意味
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User（送信元ユーザー）	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0～255 の値になります。
最初の許可ルールに至るまで、ルールのマッチ候補をすべて表示します。	最初にマッチしたルールの結果が得られるまでルールのマッチ候補をすべて表示する場合はこのオプションを有効化します。テスト結果で最初にマッチしたルールだけを返す場合はこれを無効化（クリア）します。
Application [アプリケーション]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィック カテゴリを選択します。
（ファイアウォールのみ）HIP マスクをチェック	ネットワークにアクセスしているエンド デバイスのセキュリティ状態をチェックする場合はこれを選択します。

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	（Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A`（該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected`（デバイスが未接続）–デバイスの接続がドロップされました。
	  • `Shared policy disabled on device`（デバイス上の共有ポリシーが無効）–Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

© 2019 Palo Alto Networks, Inc.

QoS ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User（送信元ユーザー）	トラフィックの送信元であるユーザーを選択します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0 ~ 255 の値になります。
Application [アプリケーション]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィック カテゴリを選択します。
コードポイント タイプ	テストするコードポイント エンコーディングのタイプを選択します。
コードポイント値	コードポイントのエンコードの値を指定します： • **DSCP**—0 ~ 63 • **ToS**—0 ~ 7
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)—トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)—トラフィックを処理しているファイアウォールの名前です

© 2019 Palo Alto Networks, Inc.

項目	の意味

	• Status (ステータス)–テストのステータスを示します：`Success` （成功）あるいは`Failure` （失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` （該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected` （デバイスが未接続）–デバイスの接続がドロップされました。
	  • `Shared policy disabled on device` （デバイス上の共有ポリシーが無効）–Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

Authentication Policy Match 認証ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
カテゴリ	テストするトラフィック カテゴリを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です

© 2019 Palo Alto Networks, Inc.

項目	の意味

	• Status (ステータス)–テストのステータスを示します：`Success` （成功）あるいは`Failure` （失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` （該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected` （デバイスが未接続）–デバイスの接続がドロップされました。
	  • `Shared policy disabled on device` （デバイス上の共有ポリシーが無効）–Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

復号化/SSL ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Application [アプリケーション]	テストするアプリケーション トラフィックを選択します。
カテゴリ	テストするトラフィック カテゴリを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。

© 2019 Palo Alto Networks, Inc.

項目	の意味

	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success` （成功）あるいは`Failure` （失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` （該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected` （デバイスが未接続）–デバイスの接続がドロップされました。

NAT ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Source port	トラフィックの元である特定のポートを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0～255 の値になります。
宛先インターフェイス	トラフィックの宛先であるデバイス上の宛先インターフェイスを入力します。
HA デバイス ID	HA デバイスの ID を入力します： • **0**–プライマリ HA ピア

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• **1**–セカンダリ HA ピア

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	(Panorama のみ) 複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success` (成功) あるいは`Failure` (失敗)。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` (該当なし) –対象のデバイスに対して利用できないテストです。
	  • `Device not connected` (デバイスが未接続) –デバイスの接続がドロップされました。
	  • `Shared policy disabled on device` (デバイス上の共有ポリシーが無効) –Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

ポリシー ベース フォワーディング ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
(Panorama のみ) デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
(Panorama のみ) 選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
インターフェイスから	トラフィックの送信元であるデバイス上のインターフェイスを入力します。
送信元	トラフィックの元である IP アドレスを入力します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User（送信元ユーザー）	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0～255 の値になります。
Application [アプリケーション]	テストするアプリケーション トラフィックを選択します。
HA デバイス ID	HA デバイスの ID： • **0**–プライマリ HA ピア • **1**–セカンダリ HA ピア

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	（Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A`（該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected`（デバイスが未接続）–デバイスの接続がドロップされました。
	  • `Shared policy disabled on device`（デバイス上の共有ポリシーが無効）–Panorama からポリシーをプッシュすることを、デバイス上の Panorama 設定が許可していません。

DoS ポリシー マッチ

項目	の意味
設定をテスト	
テストを選択	実行するポリシーマッチ テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device

© 2019 Palo Alto Networks, Inc.

項目	の意味
	group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
送信者	トラフィックの元であるゾーンを入力します。
受信者	トラフィックの宛先ゾーンを選択します。
インターフェイスから	トラフィックの送信元であるデバイス上のインターフェイスを入力します。
宛先インターフェイス	トラフィックの宛先であるデバイス上の宛先インターフェイスを入力します。
送信元	トラフィックの元である IP アドレスを入力します。
宛先	トラフィックの宛先 IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
Source User（送信元ユーザー）	トラフィックの送信元であるユーザーを入力します。
PROTOCOL	ルーティングに使用する IP プロトコルを入力します。0 ~ 255 の値になります。

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	（Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A`（該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected`（デバイスが未接続）–デバイスの接続がドロップされました。

© 2019 Palo Alto Networks, Inc.

routing

項目	の意味
テストを選択	除外する接続性テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
FiB ルックアップ、Mfib ルックアップ	Lookup (ルックアップ) では次のいずれかを選択します： • **FiB**—アクティブ ルートテーブル内でルートのルックアップを実行します • **Mfib**—アクティブ ルートテーブル内でマルチキャスト ルートのルックアップを実行します
宛先IP	トラフィックの目的地である IP アドレスを入力します。
仮想ルーター(VR)	ルーティングのテストを行う特定の仮想ルーターを指定します。ドロップダウン リストから仮想ルーターを選択します。
ECMP	
送信元IP	トラフィックの送信元である特定の IP アドレスを入力します。
Source port	トラフィックの送信元である特定のポートを入力します。
宛先IP	トラフィックの目的地である特定の IP アドレスを入力します。
Destination port	トラフィックの目的地である特定の宛先ポートを入力します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)—トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)—トラフィックを処理しているファイアウォールの名前です • Status (ステータス)—テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。 • Result (結果)—テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• N/A （該当なし）–対象のデバイスに対して利用できないテストです。 • Device not connected （デバイスが未接続）–デバイスの接続がドロップされました。

Wildfire をテスト

項目	の意味
テストを選択	除外する接続性テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
チャネル	WildFire チャンネルを選択します：**Public**あるいは**Private**.

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	（Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：Success （成功）あるいはFailure （失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • N/A （該当なし）–対象のデバイスに対して利用できないテストです。
	  • Device not connected （デバイスが未接続）–デバイスの接続がドロップされました。

© 2019 Palo Alto Networks, Inc.

Threat Vault

項目	の意味
テストを選択	除外する接続性テストを選択します。
(Panorama のみ) デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
(Panorama のみ) 選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	(Panorama のみ) 複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success` (成功) あるいは `Failure` (失敗)。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` (該当なし) –対象のデバイスに対して利用できないテストです。
	  • `Device not connected` (デバイスが未接続) –デバイスの接続がドロップされました。

ping

この ping のトラブルシューティング テストは、PAN-OS 9.0 以降のリリースを実行するファイアウォールでのみサポートされています。

項目	の意味
テストを選択	除外する接続性テストを選択します。
(Panorama のみ) デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
ルーティングテーブルをバイパス、指定されたインターフェイスを使用	このオプションを有効化すると、ルーティングテーブルをバイパスして指定されたインターフェイスを使用するようになります。設定済みのルーティングテーブルをテストする場合はこのオプションを無効化（クリア）します。
数	送信するリクエストの数を入力します。デフォルトのカウントは 5 です。
エコーリクエスト パケットをフラグメント化しない（IPv4）	テストでエコーリクエスト パケットをフラグメント化しない場合はこのオプションを有効化します。無効化
IPv6 宛先を強制	テストで IPv6 宛先を強制的に使用します。
間隔	リクエスト間の遅延を秒単位で指定します（範囲は 1 ~ 2,000,000,000）。
送信元	エコーリクエストの送信元アドレスを入力します。
アドレスをシンボルで出力しようとしない	テスト結果で IP アドレスを表示し、IP アドレスのホスト名を解決しない場合はこのオプションを有効化します。IP アドレスのホスト名を解決する場合は無効化（クリア）します。
パターン	16 進数のフィル パターンを指定します。
サイズ	リクエスト パケットのサイズをバイト数で入力します（範囲は 0 ~ 65468）。
ToS	IP type-of-service の値を入力します（範囲は 1 ~ 255）。
TTL	ホップの IP time-to-live の値（IPv6 hop-limit の値）を入力します（範囲は 1 ~ 255）。
詳細な出力を表示	テスト結果の詳細な出力を表示します。
ホスト	リモートホストのホスト名およびIPアドレスを入力します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です • Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• Result (結果)—テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます： • N/A （該当なし）—対象のデバイスに対して利用できないテストです。 • Device not connected （デバイスが未接続）—デバイスの接続がドロップされました。

トレース ルート

項目	の意味
テストを選択	除外する接続性テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
IPv4 を使用	選択したデバイスの IPv4 アドレスを使用できるようにします。
IPv6 を使用	選択したデバイスの IPv6 アドレスを使用できるようにします。
最初の TTL	最初のアウトバウンド プローブ パケットで使用する time-to-live を入力します（範囲は 1～255）。
最大 TTL	最大の time-to-live ホップを入力します（範囲は 1～255）。
ポート	プローブで使用するベース ポート番号を入力します。
ToS	IP type-of-service の値を入力します（範囲は 1～255）。
Wait 待機	レスポンスを待機する秒数を入力します（範囲は 1～99,999）。
一時停止	プローブ間で一時停止する時間をミリ秒単位で入力します（範囲は 1～2,000,000,000）。
「don’t fragment」ビットを設定	パスが指定済みの最大トランスミッション ユニット（MTU）をサポートできない際に ICMP パケットを複数のパケットにフラグメント化しない場合はこのオプションを有効化します。
ソケット レベルのデバッグを有効化	このオプションを有効化すると、ソケット レベルでデバッグできるようになります。
ゲートウェイ	最大 8 つのルーズ ソースルート ゲートウェイを指定します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
アドレスをシンボルで出力しようとしない	テスト結果で IP アドレスを表示し、IP アドレスのホスト名を解決しない場合はこのオプションを有効化します。IP アドレスのホスト名を解決する場合は無効化 (クリア) します。
ルーティングテーブルをバイパスしてホストに直接送信	指定済みのルーティングテーブルをバイパスしてホストを直にテストする場合はこのオプションを有効化します。
送信元	アウトバウンド プローブ パケットの送信元アドレスを入力します。
ホスト	リモートホストのホスト名およびIPアドレスを入力します。

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	(Panorama のみ) 複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success` (成功) あるいは`Failure` (失敗)。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A` (該当なし) –対象のデバイスに対して利用できないテストです。
	  • `Device not connected` (デバイスが未接続) –デバイスの接続がドロップされました。

ログコレクタの接続性

項目	の意味
テストを選択	除外する接続性テストを選択します。
(Panorama のみ) デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
(Panorama のみ) 選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。

© 2019 Palo Alto Networks, Inc.

項目	の意味

	（Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。
	• Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • `N/A`（該当なし）–対象のデバイスに対して利用できないテストです。
	  • `Device not connected`（デバイスが未接続）–デバイスの接続がドロップされました。

外部ダイナミック リスト

項目	の意味
テストを選択	除外する接続性テストを選択します。
（Panorama のみ）デバイスを選択	**Select device/VSYS** (デバイス/**VSYS** を選択)し、ポリシーの機能をテストするデバイスおよび仮想システムを指定します。Admin および device group & Template ユーザーには、そのアクセスドメインに基づいてデバイスおよび仮想システムが提示されます。さらに、Panorama 管理サーバーをデバイスとして選択することができます。
（Panorama のみ）選択したデバイス	テスト用に選択したデバイスおよび仮想システムをリストアップします。
URL テスト	接続をテストする URL を指定します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 （Panorama のみ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です • Status (ステータス)–テストのステータスを示します：`Success`（成功）あるいは`Failure`（失敗）。 • Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• N/A （該当なし）—対象のデバイスに対して利用できないテストです。 • Device not connected （デバイスが未接続）—デバイスの接続がドロップされました。

更新サーバー

項目	の意味
テストを選択	除外する接続性テストを選択します。

結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。
	（ Panorama のみ ）複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。
	• Device Group (デバイスグループ)—トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。
	• Firewall (ファイアウォール)—トラフィックを処理しているファイアウォールの名前です
	• Status (ステータス)—テストのステータスを示します：Success （成功）あるいはFailure （失敗）。
	• Result (結果)—テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：
	  • N/A （該当なし）—対象のデバイスに対して利用できないテストです。
	  • Device not connected （デバイスが未接続）—デバイスの接続がドロップされました。

クラウド ロギングサービスのステータスをテスト

クラウド ロギング サービスへの接続ステータスをテストします。このテストは、バージョン 1.3 以降のクラウドサービス プラグインをインストールして実行する Panorama 管理サーバーでのみ利用できます。

項目	の意味
テストを選択	除外する接続性テストを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)—トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	• Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です • Status (ステータス)–テストのステータスを示します：`Success` （成功）あるいは`Failure` （失敗）。 • Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：

クラウド GP サービスのステータスをテスト

GlobalProtect as a Service への接続ステータスをテストします。このテストは、バージョン 1.3 以降のクラウドサービス プラグインをインストールして実行する Panorama 管理サーバーでのみ利用できます。

項目	の意味
テストを選択	除外する接続性テストを選択します。
結果	選択すると、実行したテストの Result Details (結果の詳細) が表示されます。 複数の管理対象のデバイスに対してテストを実行すると、テストされたデバイス毎に次の情報が Results (結果) に表示されます。 • Device Group (デバイスグループ)–トラフィックを処理しているファイアウォールが属すデバイスグループの名前です。 • Firewall (ファイアウォール)–トラフィックを処理しているファイアウォールの名前です • Status (ステータス)–テストのステータスを示します：`Success` （成功）あるいは`Failure` （失敗）。 • Result (結果)–テストの結果を表示します。テストを行えなかった場合は次のいずれかが表示されます：

© 2019 Palo Alto Networks, Inc.

Device > Virtual Systems [デバイス > 仮想システム]

仮想システム (vsys) は、物理ファイアウォール内で個別に管理できる、独立した (仮想) ファイアウォールインスタンスです。各 vsys は、独自のセキュリティ ポリシー、インターフェイス、および管理者による、独立したファイアウォールにすることができます。vsys では、ファイアウォールで提供されるすべてのポリシー、レポート、および可視化機能の管理をセグメント化できます。

たとえば、財務部門に関連付けられているトラフィックのセキュリティ機能をカスタマイズする場合、財務 vsys を定義して、その部門のみに適用するセキュリティ ポリシーを定義できます。ポリシーの管理を最適化するため、個々の vsys へのアクセスを許可する vsys 管理者アカウントを作成し、ファイアウォール全体とネットワーク機能で個別の管理者アカウントを使用できます。こうすることで、財務部門の vsys 管理者が、財務部門のみのセキュリティ ポリシーを管理できます。

ネットワーク機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPアドレス、IPSec トンネルなど) は、ファイアウォール全体とそのすべての仮想システムに関係します。仮想システムの設定 (**Device (デバイス)** > **Virtual Systems (仮想システム)**) は、ファイアウォール レベルおよびネットワーク レベルの機能 (スタティックおよびダイナミック ルーティング、インターフェイスの IPアドレス、IPSec トンネル、VLAN、バーチャル ワイヤ、仮想ルーター、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP、ネットワーク プロファイルなど) を制御しません。各 vsys で、一連の物理および論理ファイアウォール インターフェイス (VLAN、バーチャル ワイヤーなど) とセキュリティ ゾーンを指定できます。各 vsys でルーティングのセグメント化が必要な場合、追加仮想ルーターの作成および割り当てを行い、必要に応じてインターフェイス、VLAN、バーチャル ワイヤーを割り当てる必要があります。

Panorama テンプレートを使用して vsys を定義する場合、1 つの仮想システムをデフォルトとして構成できます。デフォルトの vsys と マルチ仮想システム機能 により、テンプレートのコミット中にファイアウォールが vsys 固有の設定を受け入れるかどうかが決まります。

- マルチ仮想システム機能 が有効になっているファイアウォールは、テンプレートで定義されている vsys に対して vsys 固有の設定を受け入れます。
- マルチ仮想システム機能 が有効になっていないファイアウォールは、デフォルトの vsys に対してのみ vsys 固有の設定を受け入れます。デフォルトの vsys を構成しない場合、これらのファイアウォールは vsys 固有の設定を受け付けません。

PA-3200 シリーズ、*PA-5200* シリーズ、および *PA-7000* シリーズ のファイアウォールでは、マルチ仮想システムがサポートされています。ただし、*PA-3200* シリーズ のファイアウォールでは、マルチ仮想システムを有効化するためのライセンスが必要になります。*PA-220* および *PA-800 Series* ファイアウォールでは、マルチ仮想システムがサポートされていません。

マルチ仮想システムを有効にする前に、以下の点を考慮してください。

- vsys 管理者は、割り当てられた 仮想システム ごとに、セキュリティ ポリシーに必要なすべてのアイテムを作成・管理します。
- ゾーンは、vsys 内のオブジェクトです。ポリシーまたはポリシー オブジェクトを定義する前に、**Policies (ポリシー)** または **Objects (オブジェクト)** タブのドロップダウンから適切な **Virtual System (仮想システム)** を選択します。
- リモートログの宛先 (SNMP、Syslog、および電子メール)、アプリケーション、サービス、およびプロファイルをすべての仮想システム (共有) または1つのvsysで使用できるように設定できます。
- 複数の仮想システムがある場合、単一の vsys を User-ID ハブとして選択し、IP アドレス対ユーザー名のマッピング情報を仮想システム間で共有できます。
- グローバル (ファイアウォールのすべての仮想システム) または vsys 固有のサービス ルートを設定できます (Device (デバイス) > Setup (セットアップ) > Services (サービス))。

© 2019 Palo Alto Networks, Inc.

- vsys の名前変更はローカルのファイアウォールでのみ行うことができます。Panorama では vsys の名前変更はサポートしていません。Panorama で vsys の名前を変更する場合、完全に新規の vsys になるか、新しい vsys 名がファイアウォール上の間違った vsys にマップされます。

vsys を定義する前に、まずはマルチ vsys 機能をファイアウォール上で有効化する必要があります。**Device** (デバイス) > **Setup** (セットアップ) > **Management** (管理)を選択して**General Settings** (一般設定)を編集し、**Multi Virtual System Capability** (マルチ仮想システム機能)を選択してから**OK**をクリックします。これにより、**Device**（デバイス）> **Virtual Systems**（仮想システム）ページが追加されます。そのページを選択して以下の情報を指定し、vsysを**Add** (追加)します。

仮想システム設定	の意味
ID	vsys の識別子を整数で入力します。サポートされる仮想システムの数についての詳細は、ファイアウォール モデルのデータ シートを参照してください。 *Panorama* テンプレートを使用して *vsys* を設定する場合、このフィールドは表示されません。
氏名	vsys の識別に使用する名前（最大 31 文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 *Panorama* テンプレートを使用して *vsys* 設定をプッシュする場合、テンプレートの *vsys* 名はファイアウォールの *vsys* 名と一致している必要があります。
復号化されたコンテンツの転送を許可	ポート ミラーリング時または分析用の WildFire ファイルの送信時に復号化されたコンテンツを仮想システムから外部のサービスに転送できるようにするには、このオプションを選択します。復号ポート ミラーリングも参照してください。
General [全般] タブ	このvsysにDNSプロキシルールを適用する場合は、**DNS Proxy**[DNSプロキシ]オブジェクトを選択します。（Network (ネットワーク) > DNS Proxy (DNS プロキシ)）。 特定の種類のオブジェクトを含める場合は、その種類（インターフェイス、VLAN、バーチャル ワイヤー、仮想ルーター、または識別可能な仮想システム）を選択して、ドロップダウンリストからオブジェクトを選択して**Add** (追加)します。1 つ以上のオブジェクトの種類を追加できます。オブジェクトを削除するには、オブジェクトを選択して **Delete** (削除)します。
[リソース] タブ	この vsys に許可される以下のリソース制限を指定します。各フィールドには、ファイアウォールモデルごとに異なる有効な範囲の値が表示されます。デフォルト設定は 0 です。これは、vsys の制限がファイアウォールモデルの制限と同じであることを意味します。ただし、特定の設定に関する制限は各 vsys には反映されません。例えば、ファイアウォールに 4 つの仮想システムがある場合、各仮想システムには、ファイアウォールごとに許可されている復号化ルールの総数を設定することはできません。すべての仮想システムの復号化ルールの総数がファイアウォールの制限に達すると、それ以上追加することはできません。 • **Sessions Limit**[セッション制限] — セッションの最大数。

© 2019 Palo Alto Networks, Inc.

仮想システム設定	の意味
	show session meter CLI コマンドを使用すると、ファイアウォールがデータ プレーンごとに許可される最大セッション数、仮想システムで使用されている現在のセッション数、および仮想システムあたりのセッション数を表示します。*PA-5200* シリーズおよび *PA-7000* シリーズのファイアウォールでは、仮想システムごとに複数のデータプレーンが存在するため、使用されている現在のセッション数が最大セッション数制限より大きくなることがあります。*PA-5200* シリーズまたは *PA-7000* シリーズのファイアウォールで設定する セッション制限は、データプレーンあたりであり、仮想システムごとに最大値が高くなります。 • **Security Rules (セキュリティルール)** – セキュリティ ルールの最大数。 • **NAT Rules**[NATルール] – NAT ルールの最大数。 • **Decryption Rules**[復号化ルール] – 復号化ルールの最大数。 • **QoS Rules**[QoSルール] – QoS ルールの最大数。 • **Application Override Rules**[アプリケーションオーバーライドルール] – アプリケーションオーバーライドルールの最大数。 • **Policy Based Forwarding Rules (ポリシーベースフォワーディングルール)** – ポリシー ベース フォワーディング (PBF) ルールの最大数。 • **Captive Portal Rules (キャプティブポータルのルール)** – キャプティブポータル（CP）のルールの最大数。 • **DoS Protection Rules (DoS プロテクションルール)** – サービス拒否（DoS）ルールの最大数。 • **Site to Site VPN Tunnels**[サイト間 VPNトンネル] – サイト間VPNトンネルの最大数。 • **Concurrent GlobalProtect Tunnels**[同時GlobalProtectトンネル] – 同時リモートGlobalProtectユーザーの最大数。 • **Inter-Vsys User-ID Data Sharing (vsys 間 User-ID データ共有)**–**Make this vsys a User-ID data hub (この vsys を User-ID データハブにする)**ことでファイアウォール上の他のすべての仮想システムが共有ユーザーマッピング情報にアクセスできるようにするか、**Change hub (ハブを変更)**して新しい vsys を選択し、その vsys を User-ID データハブとして割り当て直します。スーパーユーザーあるいは管理者の権限が必要になります。

© 2019 Palo Alto Networks, Inc.

Device > Shared Gateways [デバイス > 共有ゲートウェイ]

共有ゲートウェイ では、マルチ仮想システムで (通常はインターネット サービス プロバイダなどの共通アップストリーム ネットワークに接続される) 外部通信に 1 つのインターフェイスを共有できます。すべての仮想システムは、1 つの IP アドレスを使用する物理インターフェイスを介して外部と通信します。すべての仮想システムのトラフィックは、共有ゲートウェイを介し、1 つの仮想ルーターを使用してルーティングされます。

共有ゲートウェイではレイヤー 3 インターフェイスを使用するため、レイヤー 3 インターフェイスが少なくとも 1 つ共有ゲートウェイとして設定されている必要があります。仮想システムから共有ゲートウェイを介してファイアウォールを通過する通信には、2 つの仮想システム間の通信と同様のポリシーが必要です。[External vsys] ゾーンで仮想システムのセキュリティ ルールを定義できます。

共有ゲートウェイ設定	の意味
ID	ゲートウェイの識別子 (ファイアウォールでは使用しない)。
氏名	共有ゲートウェイの名前 (最大 31 文字) を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。名前のみが必須です。
DNSプロキシ	(任意) DNSプロキシが設定されている場合、ドメイン名のクエリに使用するDNSサーバーを選択します。
インターフェイス	共有ゲートウェイが使用するインターフェイスを選択します。

© 2019 Palo Alto Networks, Inc.

Device（デバイス） > Certificate Management（証明書の管理）

- Device > Certificate Management > Certificates [デバイス > 証明書の管理 > 証明書]
- Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロファイル]
- Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ]
- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル]
- Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]
- Device（デバイス） > Certificate Management（証明書の管理） > SSL Decryption Exclusion（SSL 復号化例外）

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > Certificates [デバイス > 証明書の管理 > 証明書]

ネットワーク間の通信を安全に行うために、使用する証明書の管理（生成、インポート、更新、削除、および取り消し）を行う場合は、**Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）のページを使用します。ネットワークのHAピア間の通信を保護する高可用性（HA）キーをエクスポートおよびインポートすることもできます。ファイアウォールが信頼する認証局（CA）を表示、有効化、無効化する場合は、 **Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Default Trusted Certificate Authorities**（信頼される既定認証局）のページを使用します。

ファイアウォールおよび *Panorama* での証明書の使用方法の詳細は、証明書の管理 を参照してください。

- ファイアウォールおよび Panorama 証明書の管理
- 信頼できる既定証明機関の管理
- Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロファイル]
- Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ]
- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル]
- Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]
- Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]

ファイアウォールおよび Panorama 証明書の管理

- [Device] > [証明書の管理] > [証明書] > [デバイス証明書]
- [Panorama > 証明書の管理 > 証明書]

ファイアウォールまたは Panorama が Web インターフェイスへのアクセスの保護、SSL 復号、または LSVPN などのタスクに使用する証明書を表示する場合は、**Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）または **Panorama** > **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）のページを開きます。

各証明書の用途の例は以下のとおりです。証明書を生成した後で、証明書の使用方法を定義してください（「デフォルトの信頼できる証明機関の管理」を参照）。

- **Forward Trust**（信頼できる転送）– ファイアウォールは、サーバー証明書に署名を行った認証局（CA）がファイアウォールの CA リストに存在する場合、SSL フォワード プロキシ復号化 時にクライアントへ提示するサーバー証明書のコピーに署名する際にこの証明書を使用します。
- **Forward Untrust**（信頼できない転送）– ファイアウォールは、サーバー証明書に署名を行った CA がファイアウォールの CA リストに存在しない場合、SSL フォワード プロキシ復号化 時にクライアントへ提示するサーバー証明書のコピーに署名する際にこの証明書を使用します。
- **Trusted Root CA**（信頼されたルート**CA**）– ファイアウォールは SSL フォワード プロキシ復号化、GlobalProtect、URL 管理オーバーライド、およびキャプティブ ポータル 用にこの証明書を信頼できる CA として使用します。ファイアウォールには、既存の信頼された認証局が数多く登録されたリストが設定されています。ここでの信頼されたルート認証局証明書とは、お客様の組織が追加

© 2019 Palo Alto Networks, Inc.

した信頼された認証局であり、予めインストールされている信頼された認証局リストに含まれるものではありません。

- **SSL Exclude**（**SSL**除外）— 復号化の例外の設定 を行って SSL/TLS の復号化から特定のサーバーを除外した場合、ファイアウォールはこの証明書を使用します。
- **Certificate for Secure Syslog**（保護された **Syslog** の証明書）— Syslog サーバーに向けた Syslog メッセージでのログ配信 を保護する際、ファイアウォールはこの証明書を使用します。

証明書を生成するには、Generate（生成）をクリックし、以下のフィールドを入力します。

証明書が生成された後で、証明書を管理するためのその他のサポート対象アクションがページに表示されます。

証明書を生成するための設定	の意味
証明書タイプ	証明書を生成するエンティティを選択します。 **Local**（ローカル）— ファイアウォールまたは Panorama で証明書を生成します。 **SCEP** — SCEP（Simple Certificate Enrollment Protocol）サーバーで証明書を生成し、ファイアウォールまたは Panorama に送信します。
証明書名	(Required (必須)) 証明書を特定するための名前を入力します (ファイアウォールでは最大 63 文字、Panorama では最大 31 文字使用できます)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
SCEP プロファイル	（SCEP 証明書のみ）**SCEP Profile**（**SCEP** プロファイル）を選択し、ファイアウォールまたは Panorama が SCEP サーバーと通信する方法を定義して、SCEP 証明書の設定を定義します。詳細は、「Device（デバイス）> Certificate Management（証明書の管理）> SCEP」を参照してください。GlobalProtect ポータルとして動作するファイアウォールを設定してrequest SCEP certificates on demand and automaticallydeploy（必要に応じて SCEP 証明書を要求し、証明書をエンドポイントに自動的にデプロイ）できます。 Generate Certificate（証明書の生成）ダイアログの残りのフィールドは、SCEP 証明書に適用されません。**Certificate Name**（証明書名）と **SCEP Profile**（**SCEP** プロファイル）を指定したら、**Generate**（生成）をクリックします。
共通名（CN）	（必須）証明書に表示されるIPアドレスまたはFQDNを入力します。
共有	複数の仮想システム（vsys）が存在するファイアウォールで、証明書をすべてのvsysで使用できるようにする場合は、**Shared**[共有] を選択します。
署名者	証明書に署名するには、ファイアウォールにインポートした認証局（CA）証明書を使用できます。証明書を自己署名することもでき、その場合はファイアウォールが CA になります。Panorama を使用している場合、Panorama の自己署名証明書の生成に関するオプションがあります。 CA 証明書をインポートした場合、またはファイアウォールで CA 証明書を発行（自己署名）した場合、作成する証明書に署名できる CA がドロップダウンリストに表示されます。

© 2019 Palo Alto Networks, Inc.

証明書を生成するための設定	の意味
	証明書署名要求 (CSR) を生成するには、**External Authority (CSR)**[外部認証局 (CSR)] を選択します。ファイアウォールが証明書とキー ペアを生成したら、CSR をエクスポートして、署名のために CA に送信できます。
認証局	ファイアウォールで証明書を発行する場合、このオプションを選択します。 証明書を認証局としてマークすることで、ファイアウォールでの他の証明書の署名にこの証明書を使用できます。
OCSP レスポンダ	OCSP レスポンダ プロファイルをドロップダウン リストから選択します（「Device（デバイス）> Certificate Management（証明書の管理）> OCSP Responder（OCSP レスポンダ）」を参照）。対応するホスト名が証明書に表示されます。
アルゴリズム	証明書のキー発行アルゴリズムを選択します。**RSA**または**Elliptic Curve DSA**（ECDSA）。 ECDSA で使用される鍵のサイズは RSA アルゴリズムよりも小さいため、SSL/TLS 接続を処理するときのパフォーマンスが向上します。また、ECDSA では、RSA 以上のセキュリティが確保されています。ECDSA は、これをサポートするクライアント ブラウザとオペレーティング システムにお勧めですが、レガシー ブラウザとオペレーティング システムとの互換性のために RSA の選択が求められることがあります。 *PAN-OS 6.1 より前のリリースを実行しているファイアウォールでは、Panorama からプッシュした ECDSA 証明書が削除されます。また、これらのファイアウォールでは、ECDSA 認証局（CA）によって署名された RSA 証明書が無効になります。* ハードウェア セキュリティ モジュール（HSM）を使用して、SSL フォワード プロキシまたはインバウンド インスペクション復号化に使用する ECDSA 秘密鍵を保存することはできません。
ビット数	証明書の鍵長を選択します。 ファイアウォールが FIPS-CC モードで、鍵生成の **Algorithm**（アルゴリズム）が **RSA** の場合、生成される RSA キーは **2048** ビットまたは **3027** ビットである必要があります。**Algorithm**[アルゴリズム] が **Elliptic Curve DSA** の場合、両方の鍵長オプション (**256** と **384**) が機能します。
ダイジェスト	証明書の **Digest**[ダイジェスト] アルゴリズムを選択します。使用可能なオプションは、鍵生成の **Algorithm**[アルゴリズム] によって異なります。 • **RSA** – **MD5**、**SHA1**、**SHA256**、**SHA384**、または **SHA512** • **Elliptic Curve DSA** – **SHA256** または **SHA384** ファイアウォールがFIPS-CCモードに設定され、キー生成の **Algorithm**[アルゴリズム] が **RSA** の場合、**Digest**[ダイジェスト] アルゴリズムとして**SHA256**、**SHA384**、または**SHA512**を選択する必要があります。**Algorithm**[アルゴリズム] が **Elliptic Curve DSA** の場合、両方の **Digest**[ダイジェスト] アルゴリズム (**SHA256** と **SHA384**) が機能します。

© 2019 Palo Alto Networks, Inc.

証明書を生成するための設定	の意味
	TLSv1.2 に依存するファイアウォール サービス（*Web* インターフェイスへの管理者アクセスなど）の要求時に使用するクライアント証明書に、ダイジェスト アルゴリズムとして *SHA512* を含めることはできません。ファイアウォール サービスに *SSL/TLS* サービス プロファイルを設定するときは、クライアント証明書で低いダイジェスト アルゴリズム（*SHA384* など）を使用するか、*Max Version*（最大バージョン）を *TLSv1.1* に制限する必要があります（「Device（デバイス）> Certificate Management（証明書の管理）> SSL/TLS Service Profile（SSL/TLS サービス プロファイル）」を参照）。
有効期限 (日)	証明書が有効な日数（デフォルトは 365）を指定します。 *GlobalProtect* サテライト設定で *Validity Period[有効期間]* を指定すると、このフィールドに入力した値はその値でオーバーライドされます。
証明書の属性	必要に応じて、**Add**[追加] をクリックし、証明書の発行先となるエンティティの識別に使用する追加の **Certificate Attributes**[証明書の属性] を指定します。また、次のような属性を付加することができます。**Country**[国]、**State**[州]、**Locality**[地域]、**Organization**[組織]、**Department**[部門]、および**Email**[電子メール]。更に、以下のうち一つのSubject Alternative [サブジェクトの代替名] フィールドを指定することができます。**Host Name**[ホスト名]（サブジェクト代替名: DNS）、**IP**（サブジェクト代替名: IP）、および**Alt Email**[代替電子メールアドレス]（サブジェクト代替名: email）。 証明書の属性として国を追加するには、*Type[タイプ]* 列から *Country[国]* を選択し、*Value[値]* 列をクリックして *ISO 6366* 国コードを参照します。

ハードウェア セキュリティ モジュール *(HSM)* を設定している場合、秘密鍵はファイアウォールではなく外部 *HSM* ストレージに保存されます。

証明書を管理するためのその他のサポート対象アクション

証明書を生成すると、その詳細がページに表示され、以下のアクションを使用できます。

証明書を管理するためのその他のサポート対象アクション	の意味
削除します。	証明書を選択して **Delete**（削除）します。 ファイアウォールに復号化ポリシーが設定されている場合、用途が*Forward Trust Certificate*（信頼できる証明書を転送）また

© 2019 Palo Alto Networks, Inc.

証明書を管理するためのその他のサポート対象アクション	の意味
	は*Forward Untrust Certificate*（信頼できない証明書を転送）に設定されている証明書を削除することができません。証明書の用途を変更する方法については、「信頼できる既定証明機関の管理」を参照してください。
無効化	無効にする証明書を選択し、**Revoke**[無効化] をクリックします。証明書はただちに「無効化」状態に設定されます。コミットは必要ありません。
更新	証明書が期限切れになった場合、または間もなく期限切れになる場合、対応する証明書を選択して **Renew**[更新] をクリックします。証明書の有効期間 (日数) を設定して **OK** をクリックします。 ファイアウォールが証明書を発行した CA である場合、ファイアウォールはその証明書を、古い証明書と属性が同じでシリアル番号が異なる新しい証明書に置き換えます。 外部認証局（CA）が証明書に署名し、ファイアウォールがオンライン証明書状態プロトコル（OCSP）を使用して証明書の失効状態を検証している場合、ファイアウォールは OCSP レスポンダ情報を使用して証明書の状態を更新します。
インポート	証明書を **Import**（インポート）し、以下のように設定します。 • 証明書を識別する Certificate Name (証明書名) を入力します。 • 証明書ファイルを参照します。**PKCS12**をインポートすると、1 つのファイルに証明書および秘密鍵の両方を含んでいます。**PEM**証明書をインポートした場合、ファイルには証明書のみが含まれています。 各証明書を個別にインポートします。証明書チェーンを選択すると、ファイアウォールはチェーンの先頭の証明書をインポートします。 • 証明書ファイルの**File Format**[ファイル形式] を選択します。 • この証明書の秘密キーの保存にHSMを使用している場合、**Private key resides on Hardware Security Module**[秘密鍵はハードウェアセキュリティモジュール上にあります] を選択します。HSM の詳細は、「Device（デバイス）> Setup（セットアップ）> HSM」を参照してください。 • 必要に応じて **Import private key**（秘密鍵のインポート）を行います（PEM 形式のみ）。証明書の **File Format**（ファイル形式）として **PKCS12** を選択した場合、選択した **Certificate File**（証明書ファイル）にキーが含まれています。**PEM** 形式を選択した場合、暗号化された秘密鍵ファイル（通常のファイル名は *.key）を参照します。両方の形式について、**Passphrase**（パスフレーズ）および **Confirm Passphrase**（パスフレーズ再入力）を入力します。 *FIPS-CC モードの Palo Alto Networks ファイアウォールまたは Panorama サーバーに証明書をインポートする場合、Base64-Encoded Certificate（PEM）として証明書をインポートし、AES で秘密鍵を暗号化する必要があります。また、パスフレーズ ベースの鍵導出方法として SHA1 を使用する必要があります。*

© 2019 Palo Alto Networks, Inc.

証明書を管理するためのその他のサポート対象アクション	の意味
	PKCS12 証明書をインポートするには、（OpenSSL などのツールを使用して）証明書を PEM 形式に変換します。変換中に使用するパスワード フレーズが 6 文字以上であることを確認してください。
エクスポート	エクスポートする証明書を選択して **Export**（エクスポート）をクリックし、**File Format**（ファイル形式）を選択します。 • Encrypted Private Key and Certificate (PKCS12)（暗号化された秘密鍵と証明書（PKCS12））– エクスポートしたファイルには証明書とキーの両方が含まれます。 • Base64 Encoded Certificate (PEM)（Base64 エンコード済み証明書（PEM）– 秘密鍵も必要となる場合は、さらに Export Private Key（秘密鍵のエクスポート）を選択し、Passphrase（パスフレーズ）および Confirm Passphrase（パスフレーズの再入力）を入力します。 • Binary Encoded Certificate (DER) (バイナリエンコード済み証明書（DER）) - キーはエクスポートできず、証明書のみがエクスポート可能です。Export Private Key (秘密鍵のエクスポート) およびパスフレーズのフィールドは使用しないでください。
HA キーのインポート HA キーのエクスポート	HA キーは、両方のファイアウォール ピア間で入れ替える必要があります。つまり、ファイアウォール 1 のキーをエクスポートしてファイアウォール 2 でインポートし、その逆も実行します。 高可用性（HA）の鍵をインポートする場合は、**Import HA Key**[HAキーのインポート] をクリックし、**Browse**[参照] からインポートする鍵ファイルを指定します。 HA の鍵をエクスポートするには、**Export HA Key**[HA キーのエクスポート] をクリックして、ファイルを保存する場所を指定します。
証明書の使用方法の定義	名前列で証明書を選択し、証明書の用途に合ったオプションを選択します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、管理対象の証明書設定のバンドルを **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export（設定バンドルのエクスポート）」を参照してください。

信頼できる既定証明機関の管理

- Trusted Certificate Authorities [デバイス > 証明書の管理 > 証明書 > デフォルトの信頼できる証明機関]

ファイアウォールで信頼する事前に含まれた認証局 (CA) を表示、無効化、またはエクスポートするには、このページを使用します。事前にインストールされた CA のリストには、ファイアウォールがインターネットへの接続を保護するために必要な証明書を発行する最も一般的で信頼できる証明書プロバイダが含まれています。信頼のある各ルート CA に対して、名前、サブジェクト、発行者、有効期限、有効性の状態が表示されます。

中間 CA はファイアウォールと信頼されたルート CA 間の信頼チェーンの一部ではないため、ファイアウォールはデフォルトで中間 CA を信頼しません。ファイアウォールが信頼する中間 CA と組織が必要と

© 2019 Palo Alto Networks, Inc.

する追加の信頼できるエンタープライズ CA（**Device**（デバイス）> **Certificate Management**（証明書管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書））を手動で追加する必要があります。

信頼できる証明機関設定	の意味
Enable [有効化]	CA を無効にした場合は、再び **Enable**（有効化）できます。
無効化	CA を選択して **Disable**（無効化）します。このオプションを使用して、特定の CA のみを信頼したり、ローカル CA のみを信頼してその他すべての CA を無効にしたりすることができます。
エクスポート	CA証明書を選択し、**Export**[エクスポート] します。証明書はオフラインで別のシステムにインポートしたり表示したりできます。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > Certificate Profile [デバイス > 証明書の管理 > 証明書プロファイル]

- **Device** (デバイス) > **Certificate Management** (証明書の管理) > **Certificate Profile** (証明書プロファイル)
- **Panorama** > **Certificate Management** (証明書の管理) > **Certificate Profile** (証明書プロファイル)

証明書プロファイルでは、どの認証局（CA）証明書を使用してクライアント証明書を検証するか、証明書失効状態をどのように検証するか、その状態でどのようにアクセスを制限するかを定義します。キャプティブ ポータル、GlobalProtect、サイト間の IPSec VPN、Dynamic DNS（DDNS）、Web インターフェイスによるファイアウォールおよび Panorama へのアクセスの証明書認証を設定するとき、このプロファイルを選択します。これらの各サービスに別々の証明書プロファイルを設定できます。

証明書プロファイル設定	の意味
氏名	(必須) プロファイルを識別する名前を入力します (ファイアウォールでは最大 63 文字、Panorama では最大 31 文字使用できます)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
ユーザー名フィールド	GlobalProtect がポータルおよびゲートウェイ認証にのみ証明書を使用する場合、PAN-OS ソフトウェアは **Username Field**（ユーザー名フィールド）ドロップダウン リストで選択された証明書フィールドをユーザー名として使用し、それを User-ID サービスの IP アドレスと照合します。 • **Subject** (サブジェクト)—共通名です。 • **Subject Alt**（サブジェクト代替名）—メールまたはプリンシパル名です。 • **None**（なし）— これは通常、GlobalProtect デバイスまたは pre-login 認証に使用されます。
ドメイン	PAN-OS ソフトウェアが User ID を介してユーザーをマッピングできるように、NetBIOS ドメインを入力します。
CA 証明書	（必須）**CA Certificate** (CA証明書) を**Add** (追加)してプロファイルに割り当てます。 必要に応じて、ファイアウォールで Online Certificate Status Protocol（OCSP）を使用して証明書の失効状態を検証する場合は、以下のフィールドを設定して、デフォルトの動作をオーバーライドします。ほとんどのデプロイメントでは、これらのフィールドは適用されません。

© 2019 Palo Alto Networks, Inc.

証明書プロファイル設定	の意味
	• ファイアウォールはデフォルトで証明書の認証機関アクセス（AIA）情報を使って OCSP レスポンダ情報を抽出します。AIA 情報をオーバーライドするには、**Default OCSP URL**（デフォルト **OCSP URL**）（`http://` または `https://` で始まる）を入力します。 • デフォルトでは、ファイアウォールは **CA Certificate**[CA 証明書] フィールドで選択した証明書を使用して、OCSP 応答を検証します。検証に異なる証明書を使用するには、**OCSP Verify CA Certificate**[OCSP 検証 CA 証明書] フィールドでその証明書を選択します。 さらに、証明書の署名に使用したテンプレートを識別する**Template Name (**テンプレート名**)**を入力します。
CRL の使用	証明書無効リスト（CRL）を使用して証明書の失効状態を検証する場合は、このオプションを選択します。
OCSP の使用	OCSPを使用して証明書の失効状態を検証する場合は、このオプションを選択します。 *OCSP* と *CRL* の両方を選択している場合、ファイアウォールはまず *OCSP* を試行します。*OCSP* レスポンダを使用できない場合に限り、*CRL* 方式にフォールバックします。
CRL 受信の有効期限	ファイアウォールが CRL サービスからの応答を待機する期間（1 ~ 60 秒）を指定します。
OCSP 受信の有効期限	ファイアウォールが OCSP レスポンダからの応答を待機する期間（1 ~ 60 秒）を指定します。
証明書の有効期限	ファイアウォールが任意の証明書状態サービスからの応答を待機する期間（1 ~ 60 秒）を指定します。この期間が終了すると、定義したセッション ブロック ロジックが適用されます。
証明書状態が不明な場合にセッションをブロック	OCSPまたはCRLサービスから証明書の失効状態が*unknown [*不明*]* と返された際にファイアウォールでそのセッションをブロックする場合は、このオプションを選択します。その他の場合は、ファイアウォールはセッションを続行します。
タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック	ファイアウォールでOCSPまたはCRL要求のタイムアウトを登録した後にセッションをブロックする場合は、このオプションを選択します。その他の場合は、ファイアウォールはセッションを続行します。
証明書が認証側デバイスに発行されなかった場合セッションをブロック	（GlobalProtect のみ）クライアント証明書の件名のシリアル番号属性が、GlobalProtect アプリケーションがエンドポイントに対してレポートする host ID（ホストID）と一致しない場合にファイアウォールでセッションをブロックする場合は、このオプションを選択します。その他の場合は、ファイアウォールはセッションを許可します。このオプションはGlobalProtect 証明書認証のみに適用されます。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > OCSP Responder [デバイス > 証明書の管理 > OCSP レスポンダ]

証明書の失効状態を検証するための Online Certificate Status Protocol（OCSP）レスポンダ（サーバー）を定義する場合は、**Device**（デバイス）> **Certificate Management**（証明書の管理）> **OCSP Responder**（**OCSP** レスポンダ）のページを開きます。

OCSP を有効にするには、OCSP レスポンダを追加するだけでなく、以下のタスクを実行する必要があります。

- ファイアウォールと OCSP サーバー間の通信を有効にする: **Device**（デバイス）> **Setup**（設定）> **Management**（管理）を選択し、Management Interface Settings（管理インターフェイス設定）セクションから **HTTP OCSP** サービスを選び、**OK** をクリックします。
- ファイアウォールで送信 SSL/TLS トラフィックを復号化する場合に、必要に応じて宛先サーバー証明書の失効状態を検証させる方法: **Device**（デバイス）> **Setup**（設定）> **Sessions**（セッション）を選択し、**Decryption Certificate Revocation Settings**（復号化証明書失効の設定）をクリックし、OCSP セクションで **Enable**（有効化）を選択し、**Receive Timeout**（受信の有効期限）（ファイアウォールが OCSP 応答を待機する期間）を入力して **OK** をクリックします。
- 必要に応じて、OCSP レスポンダとしてファイアウォールを設定するために、OCSP サービスで使用するインターフェイスにインターフェイス管理プロファイルを追加します。最初に、**Network**（ネットワーク）> **Network Profiles**（ネットワーク プロファイル）> **Interface Mgmt**（インターフェイス管理）を選択し、**Add**（追加）をクリックして、**HTTP OCSP** を選択し、**OK** をクリックします。次に、**Network**（ネットワーク）> **Interfaces**（インターフェイス）を選択し、ファイアウォールが OCSP サービスに使用するインターフェイスの名前をクリックし、 **Advanced**（詳細）> **Other info**（その他の情報）を選択し、設定したインターフェイス管理プロファイルを選択して、**OK**、**Commit**（コミット）の順にクリックします。

証明書が取り消された場合に通知を受け取り、適切な作業を行ってポータルおよびゲートウェイへの接続を保護できるよう、*OCSP* レスポンダを有効化します。

OCSP レスポンダ設定	の意味
氏名	レスポンダの識別に使用する名前 (最大 31 文字) を入力します。名前では大文字と小文字を区別します。英字、数字、スペース、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
場所	レスポンダを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、[場所] を選択することはできません。この値は [共有] として事前に定義されています。レスポンダを保存すると、その [場所] を変更できなくなります。
ホスト名	OCSP レスポンダのホスト名 (推奨) または IP アドレスを入力します。PAN-OS はこの値から URL を自動的に導出し、検証する証明書にその URL を追加します。ファイアウォールを OCSP レスポンダとして設定する場合、ホスト名は、ファイアウォールが OCSP サービス

© 2019 Palo Alto Networks, Inc.

OCSP レスポンダ設定	の意味
	に使用するインターフェイスの IP アドレスに解決される必要があります。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル]

- Device > Certificate Management > SSL/TLS Service Profile [デバイス > 証明書の管理 > SSL/TLS サービス プロファイル]
- Panorama > Certificate Management > SSL/TLS Service Profile [Panorama > 証明書の管理 > SSL/TLS サービス プロファイル]

SSL/TLS サービス プロファイルでは、SSL/TLS を使用するファイアウォール サービスまたは Panorama サービス (Web インターフェイスを使用する管理アクセスなど) のサーバー証明書およびプロトコル バージョンまたはバージョンの範囲を指定します。プロトコル バージョンを定義することで、サービスを要求するクライアント システムとの通信の保護に使用できる暗号スイートをプロファイルで制限できます。

ファイアウォール サービスまたは *Panorama* サービスを要求するクライアント システムでは、*SSL/TLS* サービス プロファイルで指定されている証明書を発行した認証局 (*CA*) 証明書を証明書信頼リスト (*CTL*) に含める必要があります。これを含めない場合、ユーザーがサービスを要求したときに証明書エラーが発生します。ほとんどのサードパーティ *CA* 証明書がクライアント ブラウザにデフォルトで表示されます。エンタープライズまたはファイアウォール生成の *CA* 証明書が発行者の場合、その *CA* 証明書をクライアント ブラウザの *CTL* に適用する必要があります。

プロファイルを追加するには、**Add** (追加) をクリックし、以下の表に従ってフィールドを入力します。

SSL/TLS サービス プロファイルの設定	の意味
氏名	プロファイルの識別に使用する名前を入力します (最大 31 文字)。名前では大文字と小文字を区別します。英字、数字、スペース、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
共有	ファイアウォールに複数の仮想システム (vsys) がある場合、このオプションを選択すると、プロファイルをすべての仮想システムで使用できます。デフォルトでは、このオプションはオフになっており、プロファイルは、**Device** (デバイス) タブの **Location** (場所) ドロップダウン リストで選択した vsys でのみ使用できます。
証明書	サーバー証明書を選択、インポート、または生成し、プロファイルに関連付けます (「ファイアウォール証明書および Panorama 証明書の管理」を参照)。 *SSL/TLS* サービスには認証局 *(CA)* 証明書は使用せずに、署名付き証明書のみを使用しでください。
最小バージョン	サービスで使用できる TLS の最も古いバージョン (**Min Version** (最小バージョン)) と最も新しいバージョン (**Max Version** (最大

© 2019 Palo Alto Networks, Inc.

SSL/TLS サービス プロファイルの設定	の意味
最大バージョン	バージョン)) を選択します。**TLSv1.0**、**TLSv1.1**、**TLSv1.2**、または**Max**[最大] (入手可能な最新バージョン) *PAN-OS 8.0* またはそれ以降のリリースで実行する *FIPS/CC* モードのファイアウォールでは、*TLSv1.1*はサポートされている *TLS* バージョンの中で最も古いものです。*TLSv1.0* は選択しないでください。 *TLSv1.2* を使用するファイアウォール サービスを要求する場合、使用するクライアント証明書に *SHA512* をダイジェスト アルゴリズムとして含めることはできません。クライアント証明書でより低いダイジェスト アルゴリズム (*SHA384* など) を使用するか、サービスの*Max Version* (最大バージョン) を *TLSv1.1* に制限する必要があります。 できるだけ強固なバージョンのプロトコルを使用し、ネットワークのセキュリティを最大化します。可能な場合は*Min Version* (最低バージョン)を*TLSv1.2*に、*Max Version* (最大バージョン)を*Max* (最大)にしてください。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > SCEP [デバイス > 証明書の管理 > SCEP]

SCEP (Simple Certificate Enrollment Protocol) は、エンドポイント、ゲートウェイ、サテライトデバイスに対し、個別の証明書を発行するメカニズムを備えています。SCEP 設定を作成する場合は、**Device** (デバイス) > **Certificate Management** (証明書の管理) > **SCEP**を選択します。

SCEP プロファイルの作成方法の詳細については、Deploying Certificates Using SCEP (SCEP を使用する証明書の導入) を参照してください

。

新しい SCEP 設定を始める場合は、**Add** (追加) をクリックし、以下のフィールドに情報を入力します。

SCEP 設定	の意味
氏名	この SCEP 設定に、SCEP_*Example* など、分かりやすい名前を指定します。この名前により、それぞれのSCEPプロファイルと設定プロファイル中に含まれるその他のインスタンスが区別されます。
場所	マルチ仮想システムのあるシステムの場合はプロファイルの場所を選択します。ここで設定する場所はSCEP設定が入手できる場所を示します。
ワン タイム パスワード (チャレンジ)	
SCEPチャレンジ	(任意) SCEP ベースの証明書発行の安全性を高めたい場合は、各回の証明書要求について公開鍵基盤 (PKI) およびポータルとの間に SCEP チャレンジレスポンス機能 (1 回限りのパスワード (OTP)) を設定することができます。 この機能の設定後はバックグラウンドで動作するため、追加の入力が必要になることはありません。 選択するチャレンジ機能により、OTP のソースが決まります。**Fixed** (固定) を選択する場合は、PKI の SCEP サーバーから登録チャレンジ パスワードをコピーし、**Fixed** (固定) に設定したときに表示される、ポータルの **Password** (パスワード) ダイアログにその文字列を入力します。ポータルが証明書を要求するたびに、このパスワードが使用されて PKI で認証されます。**Dynamic** (動的) を選択する場合は、任意のユーザー名およびパスワード (多くの場合は PKI 管理者の認証情報となります) と、ポータルのクライアントがこれらの認証情報を送信する SCEP **Server URL** (サーバー **URL**) を入力します。各回の証明書要求に対し SCEP サーバーが透過的に OTP パスワードを生成する場合、ユーザー名およびパスワードが変更されることはありません。 (各回の証明書要求の後で「The enrollment challenge password is (登録チャレンジ パスワード) 」のフィールドに表示された OTP は画面更新時に変更されます) 。 PKIはそれぞれの新しいパスワードをポータルへ透過的に受け渡し、また、証明書要求に対してそれらのパスワードを使用します。 連邦情報処理標準 (*FIPS*) に準拠するため米国連邦情報処理標準 (*FIPS*) を順守するため、*Dynamic* (動的) を選択し、*HTTPS* を使用する *Server URL* (サーバー *URL*) を指定

© 2019 Palo Alto Networks, Inc.

SCEP 設定	の意味
	し、*SCEP Server SSL Authentication*（*SCEP* サーバー *SSL* 認証）を有効化します。（*FIPS-CC*の実施についてはファイアウォールのログインページおよびファイアウォールのステータスバーに表示されます。）
設定	
サーバー URL	ポータルがリクエストを行い、SCEP サーバーからクライアント証明書を入手する URL を入力します。例: `http://<hostname or IP>/certsrv/mscep/.`
CA-IDENT 名	SCEP サーバーの識別に使用する文字列を入力します。最大で255文字です。

サブジェクト	デバイスおよび任意でユーザーに関する識別情報を含むようにサブジェクトを設定し、証明書署名要求（CSR）でこの情報を SCEP サーバーに提供します。
	エンドポイントのクライアント証明書の要求に使用すると、エンドポイントはデバイスに関する識別情報を送信し、これにはホスト ID 値が含まれます。GUID（Windows）、インターフェイスのMACアドレス（Mac）、Android ID（Androidデバイス）、UDID（iOSデバイス）、あるいはGlobalProtectが割り当てる一意の名前（Chrome）など、ホストIDの値はデバイスの種類によって異なります。サテライト デバイスの証明書の要求に使用するとき、ホスト ID 値はデバイスのシリアル番号になります。
	追加情報を CSR に指定するには、サブジェクト名を入力します。サブジェクトは、*<attribute>=<value>* の形式で識別される名前にして、コモンネーム（CN）キーを含める必要があります。以下がその例です。
	`O=acme,CN=acmescep`
	CN を指定するには、以下の 2 つの方法があります。
	• （推奨）トークンベースの **CN** – サポートされるいずれかのトークン、**$USERNAME**、**$EMAILADDRESS**、**$HOSTID** を入力します。ポータルが必ず特定のユーザー用の証明書をリクエストするよう、ユーザー名あるいはメールアドレスの変数を使用します。デバイスのみに対する証明書をリクエストするには、hostid 変数を指定します。GlobalProtect ポータルがエージェントに SCEP 設定をプッシュするとき、サブジェクト名の CN の部分は、証明書の所有者が持つ実際の値（ユーザー名、hostid、あるいはメール アドレス）に置き換えられます。以下がその例です。
	`O=acme,CN=$HOSTID`
	• **Static CN**[静的CN] – 指定する CN は、SCEP サーバーで発行されるすべての証明書のサブジェクトとして使用されます。以下がその例です。
	`O=acme,CN=acmescep`

© 2019 Palo Alto Networks, Inc.

SCEP 設定	の意味
サブジェクトの代替名タイプ	*Subject Alternative Name (サブジェクトの代替名 - SAN)* タイプには、スタティック エントリを使用します。ファイアウォールは ***$USERNAME***などのダイナミック トークンをサポートしていません。 **None**（なし）以外のタイプを選択した場合は、それぞれの値を入力するためのダイアログが表示されます。 • **RFC 822 Name**（**RFC822** 名）— 証明書のサブジェクトまたはサブジェクト代替名拡張子に電子メールアドレス名を入力します。 • **DNS Name**[DNS名] - 証明書の検証に使用するDNS名を入力します。 • **Uniform Resource Identifier (URI)**[ユニフォームリソース識別子(URI)] - クライアントが証明書を取得するURIリソース名を入力します。
暗号設定	• **Number of Bits**（ビット数）— 証明書のキー用に **Number of Bits**（ビット数）を選択します。ファイアウォールがFIPS-CCモードの場合、生成されるキーは最低でも2048ビット以上である必要があります。（FIPS-CCの実施についてはファイアウォールのログインページおよびファイアウォールのステータスバーに表示されます。） • **Digest**[ダイジェスト] — 証明書の**Digest**[ダイジェスト] アルゴリズムを選択します。**SHA1**、**SHA256**、**SHA384**、または**SHA512**。ファイアウォールがFIPS-CCモードに設定されている場合、**Digest**[ダイジェスト] アルゴリズムとして**SHA256**、**SHA384**、または**SHA512**を選択する必要があります。
デジタル証明書として使用	デジタル署名の検証を行う際に、証明書に含まれる秘密鍵を使用するようにエンドポイントを設定する場合はこのオプションを選択してください。
キーの暗号化に使用	SCEPサーバーが発行する証明書を通して確立されたHTTPS接続を経由して交換されたデータをクライアントのエンドポイントで暗号化する際に、証明書に含まれる秘密鍵を使用するよう設定する場合はこのオプションを選択します。
CA 証明書フィンガープリント	（任意）ポータルが正しい SCEP サーバーに確実に接続されるようにするために、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）を入力します。SCEP サーバー インターフェイスの **Thumbprint**（サムプリント）フィールドからフィンガープリントを入手してください。 SCEP サーバーの管理ユーザー インターフェイスにログインします（「http://<ホスト名または IP>/CertSrv/mscep_admin/」など）。サムプリントをコピーし、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）に入力します。
SCEP サーバー SSL 認証	SSL を有効にするには、SCEP サーバーのルート **CA Certificate**（**CA** 証明書）を選択します。また、必要に応じて**Client Certificate**[クライアント証明書] を選択し、SCEPサーバーとGlobalProtectポータルの間の相互SSL認証を有効にすることも可能です。

© 2019 Palo Alto Networks, Inc.

Device（デバイス）> Certificate Management（証明書の管理）> SSL Decryption Exclusion（SSL 復号化例外）

SSL 復号化例外 を表示して管理します。復号化例外には、事前定義済み例外とカスタム例外の 2 種類があります。

- 事前定義済み例外では、ファイアウォールが復号化するときに中断する可能性があるアプリケーションとサービスを暗号化したまま残すことができます。Palo Alto Networks では、事前定義済み復号化例外を定義し、事前定義済み例外リストの更新と追加を、アプリケーションと脅威のコンテンツ更新の一部として定期的に配信しています。事前定義済み例外はデフォルトで有効ですが、必要に応じてこの例外を無効化できます。
- カスタム復号化例外を作成すると、サーバー トラフィックを復号化から除外できます。対象サーバーからのトラフィックや対象サーバーへのトラフィックはすべて暗号化されたまま残ります。

アプリケーション、送信元、宛先、*URL* カテゴリ、サービスに基づいて、トラフィックを復号化から除外 することもできます。

このページの設定を使用して、復号化例外の変更や追加や、復号化例外を管理を行ってください。

SSL 復号化例外の設定	の意味
復号化例外の変更または追加	
ホスト名	カスタム復号化例外を定義するには、**Hostname**（ホスト名）を入力します。ファイアウォールは、ホスト名を、クライアントから要求された SNI またはサーバー証明書で提示された CN と比較します。ファイアウォールは、定義されたドメインを含む CN をサーバーから提示された場合、セッションを復号化から除外します。 アスタリスク (*) をワイルドカードとして使用することで、ドメインに関連付けられた複数のホスト名の復号化除外を作成できます。アスタリスクは、キャレット (^) が URL カテゴリの例外に対して動作するのと同じように動作し、各アスタリスクは、ホスト名の1つの可変サブドメイン (ラベル) を制御します。これにより、具体的な除外と一般的な除外の両方を作成できます。以下に例を示します。 • mail.*.com は mail.company.com と一致しますが、mail.company.sso.com には一致しません。 • *.company.com は tools.company.com と一致しますが、eng.tools.company.com には一致しません。 • *.*.company.com は eng.tools.company.com と一致しますが、eng.company.com には一致しません。 • *.*.*.company.com は corp.exec.mail.company.com と一致しますが、corp.mail.company.com には一致しません。 • mail.google.* は mail.google.com に一致しますが、mail.google.uk.com には一致しません。 • mail.google.*.* は mail.google.co.uk と一致しますが、mail.google.com には一致しません。

© 2019 Palo Alto Networks, Inc.

SSL 復号化例外の設定	の意味
	例えば、ワイルドカードを使用して video-stats.video.google.com を復号化から除外し、video.google.com を復号化から除外しない場合は、*.*.google.com を除外します。 ホスト名の前にあるアスタリスクのワイルドカードの数に関係なく (ホスト名の前に非ワイルドカード ラベルがない場合)、ホスト名はエントリと一致します。例えば、*.google.com、*.*.google.com、*.*.*.google.com はすべて google.com と一致します。ただし、*.dev.*.google.com は、1 つのラベル (dev) がワイルドカードではないため、google.com と一致しません。 ホスト名は、エントリごとに一意にしてください。事前定義済みエントリをファイアウォールに配信し、それが既存のカスタム エントリと一致する場合は、カスタム エントリが優先されます。 事前定義済み復号化例外のホスト名を編集することはできません。
共有	マルチ仮想システム ファイアウォールのすべての仮想システムで復号化例外を共有するには、**Shared**（共有）を選択します。 事前定義済み復号化例外はデフォルトでは共有されますが、事前定義済みエントリとカスタム エントリの両方を、特定の仮想システムで有効にしたり無効にしたりすることができます。
の意味	（任意）復号化から除外するアプリケーションについて、そのアプリケーションが復号化時に中断する理由などを説明します。
除外	アプリケーションを復号化から除外します。復号化から除外していたアプリケーションの復号化を開始するには、このオプションを無効にします。
復号化例外の管理	
Enable [有効化]	1 つ以上のエントリを **Enable**（有効化）して、復号化から除外します。
無効化	1 つ以上の事前定義済み復号化例外を **Disable**（無効化）します。 復号化例外では、復号化時に中断するアプリケーションが識別されるため、いずれかのエントリを無効にすると、アプリケーションはサポートされなくなります。ファイアウォールがアプリケーションの復号化を試し、そのアプリケーションは中断します。特定の暗号化済みアプリケーションがネットワークに入らないようにする場合は、このオプションを使用できます。
廃止された機能を表示	Palo Alto Networks が復号化例外として定義しなくなった事前定義済みエントリを表示するには、**Show obsoletes**（廃止された機能を表示）します。 廃止されたエントリの詳細: 事前定義済み復号化例外の更新（事前定義済みエントリの削除を含む）は、アプリケーションと脅威のコンテンツ更新の一部としてファイアウォールに配信されます。**Exclude from decryption**（復号化から除外）が有効になっている事前定義済みエントリは、そのエントリを含まなくなったコンテンツ更新をファイアウォールが受信すると、SSL 復号化例外のリストから自動的に削除されます。

© 2019 Palo Alto Networks, Inc.

SSL 復号化例外の設定	の意味
	ただし、**Exclude from decryption**（復号化から除外）が無効になっている事前定義済みエントリは、そのエントリを含まなくなったコンテンツ更新をファイアウォールが受信した後でも SSL 復号化リストに残ります。**Show obsoletes**（廃止された機能を表示）すると、無効となって現在は適用されていない事前定義済みエントリが表示され、必要に応じて手動で削除できるようになります。

© 2019 Palo Alto Networks, Inc.

Device > Response Pages [デバイス > 応答ページ]

カスタム応答ページは、ユーザーが URL にアクセスしようとするときに表示される Web ページです。リクエストされた Web ページまたはファイルの代わりにダウンロードおよび表示されるカスタム HTML メッセージを入力できます。

仮想システムごとに固有のカスタム応答ページを使用できます。以下の表に、ユーザーメッセージをサポートするカスタム応答ページのタイプを示します。

カスタム応答ページのタイプ	の意味
アンチウイルス ブロック ページ	ウイルス感染が原因でアクセスがブロックされたことを示します。
アプリケーション ブロック ページ	アプリケーションがセキュリティ ポリシー ルールでブロックされたためにアクセスがブロックされたことを示します。
キャプティブ ポータル確認ページ	ユーザーがログイン認証情報を入力して、認証ポリシー ルール（「Policies（ポリシー）> Authentication（認証）」を参照）に従ったサービスにアクセスできるよう、ファイアウォールでこのページが表示されます。この認証チャレンジへの応答方法をユーザーに知らせるメッセージを入力します。ファイアウォールは、認証ルール（「Objects（オブジェクト）> Authentication（認証）」を参照）に割り当てられた認証実施オブジェクトで指定された認証プロファイルに基づいて、ユーザーを認証します。 関連する認証実施オブジェクトにメッセージを入力することで、認証ルールごとに固有の認証手順を表示できます。このオブジェクトで定義されたメッセージは、キャプティブ ポータル確認ページで定義されたメッセージをオーバーライドします。
データ フィルタリング ブロック ページ	センシティブな情報が検出されたため、コンテンツがデータ フィルタリング プロファイルと照らし合わされてブロックされます。
ファイル ブロッキング続行ページ	ダウンロードの続行が必要なことを確認するユーザーのためのページです。このオプションは、セキュリティ プロファイルで Continue（続行）機能が有効になっている場合にのみ使用できます。[Objects] > [セキュリティ プロファイル] > [ファイル ブロッキング] の順に選択します。
ファイル ブロッキング ブロック ページ	ファイルへのアクセスがブロックされているためアクセスがブロックされたことを示します。
GlobalProtect アプリケーションのヘルプ ページ	GlobalProtect ユーザー用のカスタム ヘルプページ（GlobalProtect のステータスパネルにある設定メニューからアクセス可能）です。
GlobalProtect ポータルのログイン ページ	GlobalProtect ポータルのウェブページに認証しようとしているユーザー用のログインページです。

© 2019 Palo Alto Networks, Inc.

カスタム応答ページのタイプ	の意味
GlobalProtect ポータルのホームページ	GlobalProtect ポータルのウェブページに正常に認証するユーザー用のホームページです。
GlobalProtect アプリケーションのウェルカム ページ	GlobalProtect に正常に接続するユーザー用のウェルカム ページです。
MFA ログイン ページ	認証ポリシー ルール（「Policies（ポリシー）> Authentication（認証）」を参照）に従ったサービスへのアクセス時にユーザーが多重認証（MFA）チャレンジに応答できるよう、ファイアウォールでこのページが表示されます。この MFA チャレンジへの応答方法をユーザーに知らせるメッセージを入力します。
SAML 認証内部エラー ページ	SAML 認証に失敗したことをユーザーに通知するページ。このページには、ユーザーが認証を再試行するためのリンクが含まれます。
SSL 証明書エラー通知ページ	SSL 証明書が無効になっていることを示す通知です。
SSL 復号オプトアウト ページ	ファイアウォールが検査のためSSLセッションを復号することを表示するユーザー警告ページ
URL フィルタリングおよびカテゴリー致ブロック ページ	URL フィルタリング プロファイルが原因で、または URL カテゴリがセキュリティ ポリシー ルールでブロックされているため、アクセスがブロックされたことを示します。
URL フィルタリングの続行とオーバーライド ページ	ユーザーがブロックをバイパスできるよう一旦ブロックさせておくページです。たとえば、ページが不適切にブロックされていると思われる場合は、**Continue**[続行] をクリックして該当のページに進めます。 オーバーライド ページで、この URL をブロックするポリシーをオーバーライドするには、ユーザーにパスワードの入力が求められます。オーバーライド パスワードの設定手順の詳細は、「URL 管理オーバーライド」セクションを参照してください。
URL フィルタリング セーフ サーチの適用ブロック ページ	**Safe Search Enforcement**（セーフ サーチを適用）オプションが有効になっている URL フィルタリング プロファイルを使用したセキュリティ ポリシー ルールによって、アクセスがブロックされたことを示します。 Bing、Google、Yahoo、Yandex、または YouTube を使用して検索が実行され、ブラウザ、または、検索エンジン アカウント設定でセーフ サーチが厳密（高い）に設定されていない場合、このページが表示されます。このブロック ページで、セーフ サーチ設定を厳密に設定するように指示されます。
アンチフィッシング ブロック ページ	ユーザーが Web ページで企業の有効な認証情報（ユーザー名またはパスワード）を入力しようとしたときに、その Web ページへの認証情報の送信がブロックされている場合、ユーザーにこのページが表示されます。ユーザーは引き続きサイトにアクセスできますが、関連する Web フォームに企業の有効な認証情報を送信することはできません。 認証情報の検出を有効にして、URL カテゴリに基づいて Web ページへの認証情報の送信を制御するには、Objects（オブジェクト）> Security

© 2019 Palo Alto Networks, Inc.

カスタム応答ページのタイプ	の意味
	Profiles（セキュリティ プロファイル）> URL Filtering（URL フィルタリング）を選択します。
アンチフィッシング 続行ページ	このページは、企業の認証情報（ユーザー名とパスワード）を Web サイトに送信することに対してユーザーに警告を表示します。認証情報の送信に対してユーザーに警告を表示することで、企業の認証情報をユーザーが再利用することを阻止できるほか、フィッシングの可能性についてユーザーを教育することができます。ユーザーがサイトに認証情報を送信しようとしたときに、そのサイトに対してユーザー証明書送信権限が **continue**（続行）に設定されている（「Objects（オブジェクト）> Security Profiles（セキュリティ プロファイル）> URL Filtering（URL フィルタリング）」を参照）場合、このページが表示されます。サイトで認証情報を入力するには、ユーザーは **Continue**（続行）を選択する必要があります。

必要に応じて、**Response Pages**[応答ページ] の下で以下の機能を実行できます。

- カスタム HTML 応答ページをインポートするには、変更するページ タイプのリンクをクリックし、import/export [インポート / エクスポート] をクリックします。ページを参照して指定します。インポートが成功したかどうかを示すメッセージが表示されます。インポートを成功させるには、ファイルは必ず HTML 形式にしてください。
- カスタムHTML応答ページをエクスポートするには、該当のページタイプの **Export**[エクスポート] をクリックします。ファイルを開くか、ディスクに保存するかを選択し、常に同じオプションを使用する場合は**Always use the same option**[常に同じオプションを使用] を選択します。
- **Application Block**[アプリケーションブロック] ページや **SSL Decryption Opt-out**[SSL復号化オプトアウト] ページを有効化または無効化する場合は、該当のページタイプの**Enable**[有効化] をクリックします。必要に応じて**Enable**[有効化] を選択、または選択を解除してください。
- 以前にアップロードしたカスタム ページの代わりにデフォルトの応答ページを使用するには、カスタム ブロック ページを削除してコミットします。これで、デフォルトのブロック ページが新しいアクティブ ページに設定されます。

© 2019 Palo Alto Networks, Inc.

Device > Log Settings [デバイス > ログ設定]

アラームの設定、ログのクリア、Panorama、ロギングサービスやその他外部デバイスへのログ転送の有効化を行うには、**Device**（デバイス）> **Log Settings**（ログ設定）を選択します。

- ログの転送先の選択
- アラーム設定の定義
- ログのクリア

ログの転送先の選択

Device（デバイス）> **Log Settings**（ログ設定）

ログ設定ページでは、ログ転送を次のように設定できます。

- **Panorama**、**SNMP** トラップ レシーバ、電子メール サーバー、**Syslog** サーバー、および **HTTP** サーバー—また、ログ エントリの送信元または宛先 IP アドレスに対して、タグを追加または削除できます。システム ログと設定ログ以外のすべてのログ タイプはタグ機能をサポートしています。
- ロギング サービス—ロギング サービスのサブスクリプションがあり、ロギング サービス（Device（デバイス）> Setup（セットアップ）> Management（管理））を有効にしている場合、Panorama/ロギング サービスへのログ転送を設定すると、ファイアウォールはロギング サービスにログを送信します。Panorama はログにアクセスしてログを表示し、レポートを生成するためにログサービスに照会します。
- **Azure Security Center** — Azure Security Center との統合は Azure の VM-Series ファイアウォールでのみ利用できます。
  - Azure Security Center から VM-Series ファイアウォールを起動した場合は、ログ転送プロファイルを含むセキュリティ ポリシー ルールが自動的に有効になります。
  - Azure Marketplace から VM-Series ファイアウォールを起動した場合、またはカスタム Azure テンプレートを使用している場合は、Azure Security Center にシステムログ、ユーザー ID ログ、および HIP 一致ログを転送するために **Azure-Security-Center-Integration** を手動で選択し、他のログ タイプのログ転送プロファイルを使用します（「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照してください）。

Security Center の無料のレイヤーは、*Azure* サブスクリプションで自動的に有効になります。

以下の log types（ログ タイプ）を転送することができます。システム、設定、ユーザー ID、HIP 一致、および相関ログ。各ログ タイプの宛先を指定する場合、一致リスト プロファイルを **Add**（追加）して（最大 64 個）、以下の表に記載されているようにフィールドを設定します。

トラフィック、脅威、*WildFire* への送信、*URL* フィルタリング、データ フィルタリング、トンネル検査、*GTP*、および認証ログを転送する場合、ログ転送プロファイルを設定する必要があります（「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照）。

一致リスト プロファイル設定	の意味
氏名	一致リスト プロファイルを識別する名前を入力します（最大 31 文字）。有効な名前はアルファベット文字で始まる必要があります。名前には、ゼロ、アルファベット文字、下線（_）、ハイフン（-）、ピリオド（.）、またはスペースを使用できます。

© 2019 Palo Alto Networks, Inc.

一致リスト プロファイル設定	の意味
フィルタ	デフォルトでは、一致リスト プロファイルを追加したタイプの **All Logs**（すべてのログ）をファイアウォールは転送します。一部のログを転送するには、ドロップダウン リストを開いて既存のフィルタを選択するか、**Filter Builder**（フィルタ ビルダー）を選択して新しいフィルタを追加します。新しいフィルタの各クエリに対して、以下のフィールドを指定して、クエリを **Add**（追加）します。 • **Connector**（条件式） – クエリの結合ロジック（AND/OR）を選択します。ロジックに否定を適用する場合は、**Negate**（否定）を選択します。たとえば、信頼されていないゾーンからのログ転送を防ぐには、**Negate**（上記以外）を選択し、Attribute（属性）として **Zone**（ゾーン）、Operator（演算子）として **equal**（等しい）を選択して、Value（値）列に信頼されていないゾーンの名前を入力します。 • **Attribute**（属性） – ログの属性を選択します。ログ タイプにより使用できる属性が異なります。 • **Operator**（演算子） – 属性を適用するかどうかを決定する基準を選択します（**equal**（等しい）など）。ログ タイプにより使用できる基準が異なります。 • **Value**[値] – 照合する属性値を指定します。 フィルタが一致するログを表示またはエクスポートするには、**View Filtered Logs**（フィルタリングされたログの表示）を選択します。このタブでは **Monitoring**（モニタリング）タブのページと同じオプションが表示されます（**Monitoring**（モニタリング）> **Logs**（ログ）> **Traffic**（トラフィック）など）。 すべての重大度のログを転送するためのフィルターを設定します（デフォルトのフィルターは*All Logs (*すべてのログ*)*です）。重大度ごとに別々のログ転送方式を作成するには、*Filter (*フィルター*)*で一つ以上の重大度を指定し、*Forward Method (*転送方式*)*を設定してから残りの重大度に対して作業を繰り返します。
の意味	この一致リスト プロファイルの目的を説明します（最大 1,023 文字）。
Panorama/ロギング サービス	ロギング サービス、ログ コレクタまたは Panorama 管理サーバーにログを転送する場合、**Panorama/Logging Service**（**Panorama/**ロギング サービス）を選択します。このオプションを有効にする場合、configure log forwarding to Panorama（Panorama へのログ転送を設定）する必要があります。 相関ログをファイアウォールから*Panorama*へ転送することはできません。*Panorama*は受信したファイアウォールのログに応じて相関ログを生成します。
SNMP	ログを SNMP トラップとして転送するには、1 つ以上の SNMP トラップ サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> SNMP Trap（SNMP トラップ）」を参照）。

© 2019 Palo Alto Networks, Inc.

一致リスト プロファイル設定	の意味
電子メール	ログを電子メール通知として転送するには、1 つ以上の電子メール サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> Email（電子メール）」を参照）。
Syslog	ログを Syslog メッセージとして転送するには、1 つ以上の Syslog サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> Syslog」を参照）。
HTTP	ログを HTTP 要求として転送するには、1 つ以上の HTTP サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP」を参照）。
ビルトイン アクション	ビルトイン アクションには、以下の 2 つのタイプがあります。 • タグ付け—ログ エントリに送信元または宛先 IP アドレスを含むすべてのログ タイプにおいては、必要に応じて以下の設定を編集して、アクションを追加できます。 相関ログと *HIP* マッチ ログの送信元 *IP* アドレスにのみタグ付けできます。システム ログと設定ログでは、ログ エントリに *IP* アドレスが含まれないため、アクションを設定できません。 • アクションを **Add**（追加）し、そのアクションを説明する名前を入力します。 • 自動でタグ付けする IP アドレス（**Source Address**（送信元アドレス）または **Destination Address**（宛先アドレス））を選択します。 • アクション（**Add Tag**（タグの追加）または **Remove Tag**（タグの除去））を選択します。 • IP アドレスとタグのマッピングを、このファイアウォールまたは Panorama の **Local User-ID**（ローカル **User-ID**）エージェントに登録するか、**Remote User-ID**（リモート **User-ID**）エージェントに登録するかを選択します。 • IP アドレスとタグのマッピングを **Remote User-ID**（リモート **User-ID**）エージェントに登録するには、転送を有効にする HTTP サーバー プロファイルを選択します（Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP）。 • IP 対タグの **Timeout (**タイムアウト**)**を指定すれば、IP アドレス対タグのマッピングを保持する期間（分）を設定できます。タイムアウトを 0 にすると、IP 対タグのマッピングがタイムアウトしなくなります（範囲は 0 ~ 43200（30 日）、デフォルトは 0）。 タイムアウトを設定できるのは*Add Tag (*タグの追加*)*アクションだけです。 • ターゲットの送信元または宛先 IP アドレスに対して適用または削除する **Tags**（タグ）を入力または指定します。 • 統合—Azure の VM-Series ファイアウォールでのみ使用可能です。名前を **Add**（追加）し、このアクションを使用して、選択したログを Azure Security Center に転送します。このオプションが表示されない場合

© 2019 Palo Alto Networks, Inc.

一致リスト プロファイル設定	の意味
	は、Azure Security Center で Azure サブスクリプションが有効になっていない可能性があります。

アラーム設定の定義

- Device > Log Settings [デバイス > ログ設定]

CLI および Web インターフェイス用のアラームを設定する場合は、アラーム設定を使用します。以下のイベントに関する通知を設定することができます。

- 指定したしきい値および指定した時間間隔内でセキュリティ ルール (またはルールのグループ) が一致する。
- 暗号化/復号化エラーのしきい値に達する。
- 各ログ タイプのログ データベースの上限に近い。デフォルトでは、空きディスク領域の 90% が使用された場合に通知されるように割り当てが設定されています。アラームを設定すると、ディスクがいっぱいになってログが消去される前に対処できます。

アラームを設定した場合、Web インターフェイス下部の **Alarms** (アラーム) ( ) をクリックして現在のリストを表示することができます。

アラームを追加するには、次の表で説明するアラーム設定を編集します。

アラーム ログの設定	の意味
アラームの有効化	**Enable Alarms** (アラームを有効化) した場合のみ、アラームが表示されます。 アラームを無効にすると、アクションが必要となる重大イベントについて、ファイアウォールによって警告されなくなります。たとえば、マスター キーの期限が近付いていることをアラームよって通知されるとします。キーを変更する前にキーの期限が切れると、ファイアウォールは再起動してメンテナンス モードになり、出荷時の設定へのリセットが必要になります。
CLI アラーム通知の有効化	アラームが発生するたびに CLI アラーム通知を有効にします。
Web アラーム通知の有効化	ウィンドウを開いてユーザー セッションに関するアラーム (ユーザー セッションの発生や承認のタイミングなど) を表示します。
警告アラームの有効化	未承認のアラームが存在する場合、管理者がWebインターフェイスにログインすると管理者のコンピューター上で警告アラーム音が15秒ごとに再生されます。管理者がすべてのアラームを承認するまで、警告音が再生されます。 アラームの表示と承認を行う場合は**Alarms**[アラーム] をクリックしてください。 この機能は、ファイアウォールが FIPS-CC モードに設定されている場合にのみ使用できます。
暗号化/復号化エラー しきい値	アラームが生成されるまでの暗号化/復号化の失敗回数を指定します。

© 2019 Palo Alto Networks, Inc.

アラーム ログの設定	の意味
<ログタイプ> ログ DB	ログのデータベースが指定した最大サイズのパーセンテージに達した場合にアラームを生成します。
セキュリティ違反のしきい値/ セキュリティ違反時間	**Security Violations Time Period**（セキュリティ違反時間）設定で指定した期間（秒数）内に、特定の IP アドレスまたはポートが、**Security Violations Threshold**（セキュリティ違反のしきい値）設定で指定した回数分、拒絶ルールにヒットした場合、アラームが生成されます。
違反のしきい値/ 違反の期間/ セキュリティ ポリシー タグ	**Violations Time Period**[違反の期間] フィールドで指定した期間に一連のルールが **Violations Threshold**[違反のしきい値] フィールドで指定したルール制限違反数に達した場合、アラームが生成されます。セッションが明示的な拒否ポリシーに一致するときに、違反が数えられます。 **Security Policy Tags**[セキュリティ ポリシー タグ] を使用して、ルールの制限しきい値でアラームが生成されるタグを指定します。これらのタグは、セキュリティ ポリシーを定義するときに指定できるようになります。
選択的監査	選択的監査のオプションはファイアウォールがFIPS-CCモードに設定されている場合のみ使用できます。 以下の設定を指定します。 • **FIPS-CC Specific Logging**[FIPS-CC固有のログ] — 情報セキュリティ国際評価基準 (CC) に準拠するために必要な詳細なログ記録が有効になります。 • **Packet Drop Logging**[パケット破棄のログ] - ファイアウォールが破棄したパケットを記録します。 • **Suppress Login Success Logging**[ログイン成功ログの抑制] — ファイアウォールへの管理者ログイン成功のログ記録が停止されます。 • **Suppress Login Failure Logging**[ログイン失敗ログの抑制] — ファイアウォールへの管理者ログイン失敗のログ記録が停止されます。 • **TLS Session Logging**[TLSセッションのログ] - TLSセッション確立のログを記録します。 • **CA (OCSP/CRL) Session Establishment Logging**[CA（OCSP/CRL）セッション確立ログ] - ファイアウォールがオンライン証明書状態プロトコルまたは証明書無効リストのサーバーリクエストを使用して証明書失効状態を確認するよう要求した場合に、ファイアウォールと認証局との間のセッション確立のログを記録します。（デフォルトで無効化されています。） • **IKE Session Establishment Logging**[IKEセッション確立ログ] - ファイアウォール上のVPNゲートウェイがピアと認証を行った場合にIPSec IKEセッションの確立ログを記録します。この場合のピアとは、Palo Alto Networksファイアウォール、あるいはVPN接続の開始と終了に使用される他のセキュリティデバイスが該当します。IKEゲートウェイに固定されたインターフェイスの名前がログに記載されます。IKEゲートウェイ名が設定されている場合はこれも表示されます。このオプションを無効化するとIKEのログイベントの記録がすべて停止されます。（デフォルトで有効化されています。） • **Suppressed Administrators**[抑制された管理者] — リストに記載された管理者による、ファイアウォールの設定変更に関するログ記録を停止します。

© 2019 Palo Alto Networks, Inc.

ログのクリア

- Device > Log Settings [デバイス > ログ設定]

ログ設定のページでログの管理をする際にファイアウォール上のログを削除することができます。クリアするログ タイプをクリックし、**Yes**（はい）をクリックして要求を確定します。

ログおよびレポートを自動的に削除したい場合は、有効期限を設定することができます。詳細は、「Logging and Reporting Settings（ロギングおよびレポート設定」を参照してください。

© 2019 Palo Alto Networks, Inc.

[Device] > [サーバー プロファイル]

以下のトピックでは、ファイアウォール上で設定できるサーバー プロファイル設定について説明します。

- Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SNMP トラップ]
- Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]
- Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]
- Device（デバイス） > Server Profiles（サーバー プロファイル） > HTTP
- Device（デバイス） > Server Profiles（サーバー プロファイル） > NetFlow
- Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]
- Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+]
- Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP]
- Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]
- Device（デバイス） > Server Profiles（サーバー プロファイル） > SAML Identity Provider（SAML アイデンティティ プロバイダ）
- Device > Server Profiles > DNS [デバイス > サーバー プロファイル > DNS]
- Device（デバイス） > Server Profiles（サーバー プロファイル） > Multi Factor Authentication（多要素認証）

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SNMP トラップ]

SNMP (Simple Network Management Protocol) は、ネットワーク上のデバイスをモニターする標準プロトコルです。システム イベントやネットワーク上の脅威に関するアラートを通知するために、モニター対象デバイスから SNMP マネージャ (トラップ サーバー) に SNMP トラップが送信されます。ファイアウォールまたは Panorama から SNMP マネージャにトラップを送信できるようにするサーバー プロファイルを設定するには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **SNMP Trap**（**SNMP** トラップ）を選択するか、**Panorama** > **Server Profiles**（サーバー プロファイル）> **SNMP Trap**（**SNMP** トラップ）を選択します。SNMP GET メッセージ（SNMP マネージャからの統計情報要求）を有効にするには、「SNMPモニタリングの有効化」を参照してください。

サーバー プロファイルを作成したら、SNMP トラップを送信するようにファイアウォールをトリガーするログ タイプを指定する必要があります（「Device（デバイス）> Log Settings（ログ設定）」を参照）。トラップを解釈できるように SNMP マネージャにロードする必要がある MIB のリストについては、「Supported MIBs（サポートされる MIB）」を参照してください。

システム ログの設定またはログのプロファイルで使用されるサーバー プロファイルは削除しないでください。

SNMP トラップ サーバー プロファイルの設定	の意味
氏名	SNMP プロファイルの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
バージョン	SNMPバージョンを選択します。**V2c**（デフォルト）または**V3**。この選択内容により、ダイアログに表示される残りのフィールドが決まります。どちらのバージョンでも、最大 4 つの SNMP マネージャを追加できます。 認証およびその他の機能を提供する *SNMPv3* を使用し、ネットワーク接続が保護された状態を保ちます。
SNMP V2c の場合	
氏名	SNMP マネージャの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン) を含めることができます。

© 2019 Palo Alto Networks, Inc.

SNMP トラップ サーバー プロファイルの設定	の意味
SNMP マネージャ	SNMP マネージャの FQDN または IP アドレスを指定します。
コミュニティ	コミュニティ文字列を入力します。これは、SNMP マネージャおよびモニター対象デバイスの SNMP コミュニティを識別し、トラップの転送時にコミュニティ メンバーを相互認証するためのパスワードとしても機能します。コミュニティ文字列には最大 127 文字を含めることができます。また、すべての文字を使用でき、大文字と小文字が区別されます。 デフォルトのコミュニティ文字列は使用しないでください (コミュニティ文字列を*public (パブリック)*あるいは*private (プライベート)*に設定しないでください) 。複数の *SNMP* サービスを使用する場合に競合が起きないよう、一意のコミュニティ文字列を使用します。*SNMP* メッセージにはクリア テキストのコミュニティ文字列が含まれているため、コミュニティ メンバーシップ *(管理者アクセス)* を定義するときにネットワークのセキュリティ要件を考慮してください。
SNMP V3 の場合	
氏名	SNMP マネージャの名前を指定します。名前には、最大 31 文字 (英数字、ピリオド、アンダースコア、またはハイフン) を含めることができます。
SNMP マネージャ	SNMP マネージャの FQDN または IP アドレスを指定します。
感染	SNMPユーザー アカウントの識別に使用する名前を指定します (最大31文字) 。ファイアウォールで設定するユーザー名は、SNMPマネージャで設定したユーザー名と一致する必要があります。
エンジン ID	ファイアウォールのエンジンIDを指定します。SNMPマネージャとファイアウォールが相互の認証を行う場合、トラップメッセージはこの値を使用して一意にファイアウォールを識別します。このフィールドを空白のままにすると、メッセージではファイアウォールシリアル番号が **EngineID**[エンジンID] として使用されます。値は、16 進数形式 (0x のプレフィックスと、5 ~ 64 バイトの数値を表す 10 ~ 128 文字 (バイトあたり 2 文字)) で入力する必要があります。高可用性 (HA) 設定のファイアウォールの場合、トラップを送信したHAピアをSNMPマネージャが識別できるようにこのフィールドを空白のままにします。空白にしないと、値が同期され、両方のピアで同じ**EngineID**[エンジンID] が使用されます。
認証パスワード	SNMP ユーザーの認証パスワードを指定します。ファイアウォールはこのパスワードを使用して SNMP マネージャの認証を受けます。ファイアウォールは、Secure Hash Algorithm (SHA-1 160) を使用してパスワードを暗号化します。パスワードには、8 ~ 256 文字のあらゆる文字を使用できます。
専用パスワード	SNMP ユーザーの専用パスワードを指定します。ファイアウォールは、このパスワードとAdvanced Encryption Standard (AES-128) を使用して、トラップを暗号化します。パスワードには、8 ~ 256 文字のあらゆる文字を使用できます。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog]

ファイアウォール、Panorama、およびログ コレクタのログを Syslog メッセージとして Syslog サーバーに転送するためのサーバー プロファイルを設定するには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **Syslog** または **Panorama** > **Server Profiles**（サーバー プロファイル）> **Syslog** を選択します。Syslog サーバー プロファイルを定義するには、**Add**（追加）をクリックして、New Syslog Server（新規 Syslog サーバー）の各フィールドを指定します。

- システム、設定、ユーザー *ID*、*HIP* マッチ、および相関ログ用の *Syslog* サーバー プロファイルを選択するには、「Device（デバイス）> Log Settings（ログ設定）」を参照してください。
- トラフィック、脅威、*Wildfire*、*URL* フィルタリング、データ フィルタリング、トンネル検査、認証、および *GTP* ログ用の *Syslog* サーバー プロファイルを選択するには、「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照してください。
- ファイアウォールの、システムまたは設定ログの設定や、ログ転送プロファイルにおいて使用されているサーバープロファイルは削除できません。

Syslog サーバーの設定	の意味
氏名	Syslog プロファイルの名前（最大 31 文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
Servers [サーバー]タブ	
氏名	**Add**（追加）をクリックし、Syslog サーバーの名前（最大 31 文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
SERVER	Syslog サーバーの IP アドレスまたは FQDN を入力してください
転送	Syslog メッセージの転送方法を UDP、TCP、SSL から選択します。 *SSL*を使用し、*Syslog* サーバーに送信するデータを暗号化して保護します。データはクリアテキストの状態で *UDP* あるいは *TCP* を介して送信されるため、途中で読み取ることが可能です。

© 2019 Palo Alto Networks, Inc.

Syslog サーバーの設定	の意味
ポート	Syslog サーバーのポート番号を入力します。UDP の標準ポートは 514、SSL の標準ポートは 6514 で、TCP の場合はポート番号を指定する必要があります。
format	使用するSyslog形式を指定します。BSD（デフォルト）またはIETF。
ファシリティ	Syslog の標準値のいずれかを選択します。Syslog サーバーがfacility [ファシリティ] フィールドを使用してメッセージを管理する方法に対応する値を選択します。Facility（ファシリティ）フィールドの詳細は、RFC 3164（BSD フォーマット）または RFC 5424（IETF フォーマット）を参照してください。
Custom Log Format Tab [カスタム ログ フォーマット] タブ	
ログ タイプ	ログ タイプをクリックして、カスタム ログ形式を指定するためのダイアログ ボックスを開きます。ダイアログ ボックスで、フィールドをクリックしてLog Format [ログ形式] エリアに追加します。その他のテキスト文字列は、Log Format [ログ形式] エリアで直接編集できます。**OK** をクリックして設定を保存します。カスタム ログで使用できる各フィールドの説明を確認してください。 カスタム ログで使用できるフィールドの詳細は、「Device（デバイス）> Server Profiles（サーバー プロファイル）> Email（電子メール）」を参照してください。
エスケープ	エスケープ シーケンスを指定します。**Escaped characters**[エスケープする文字] はスペースなしでエスケープする文字の一覧です。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール]

ログを電子メール通知として転送するためには、サーバ プロファイルを設定し、**Device** (デバイス) > **Server Profiles** (サーバ プロファイル) > **Email** (電子メール) または **Panorama** (パノラマ) > **Server Profiles** (サーバ プロファイル) > **Email** (電子メール) を選択します。電子メール サーバー プロファイルを定義するには、プロファイルを **Add** (追加) し、電子メール通知設定を指定します。

- システム、設定、ユーザー *ID*、*HIP* マッチ、および相関ログ用の *Syslog* サーバー プロファイルを選択するには、「Device (デバイス) > Log Settings (ログ設定)」を参照してください。
- トラフィック、脅威、*Wildfire*、*URL* フィルタリング、データ フィルタリング、トンネル検査、認証、および *GTP* ログ用の *Syslog* サーバー プロファイルを選択するには、「Objects (オブジェクト) > Log Forwarding (ログ転送)」を参照してください。
- 「Monitor (監視) > PDF Reports (PDF レポート) > Email Scheduler (電子メール スケジューラ)」を設定することもできます。
- ファイアウォールの、システムまたは設定ログの設定や、ログ転送プロファイルにおいて使用されているサーバープロファイルは削除できません。

電子メール通知設定	の意味
氏名	サーバー プロファイルの名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location** (場所) を選択することはできません。この値は Shared (共有) (ファイアウォール) または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
Servers [サーバー]タブ	
SERVER	サーバーを識別する名前を入力します (最大 31 文字)。このフィールドは単なるラベルであり、既存の SMTP サーバーのホスト名である必要はありません。
表示名	電子メールの **From**[送信者] フィールドに表示される名前を入力します。
送信者	送信元の電子メール アドレス (security_alert@company.com など) を入力します。
受信者	受信者の電子メール アドレスを入力します。
追加の受信者	別の受信者の電子メール アドレスを入力します (任意)。追加できるのは 1 名の受信者のみです。複数の受信者を追加するには、配布リストの電子メール アドレスを追加します。

© 2019 Palo Alto Networks, Inc.

電子メール通知設定	の意味
ゲートウェイ	電子メールの送信に使用される Simple Mail Transport Protocol (SMTP) サーバーの IP アドレスまたはホスト名を入力します。
Custom Log Format Tab [カスタム ログ フォーマット] タブ	
ログ タイプ	ログ タイプをクリックして、カスタム ログ形式を指定するためのダイアログ ボックスを開きます。ダイアログ ボックスで、フィールドをクリックしてLog Format [ログ形式] エリアに追加します。**OK** をクリックして設定を保存します。
エスケープ	エスケープされた文字を組み込み、エスケープ文字を指定します。

© 2019 Palo Alto Networks, Inc.

Device（デバイス） > Server Profiles（サーバー プロファイル） > HTTP

ログを転送するためのサーバー プロファイルを設定するには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **HTTP** を選択するか、**Panorama** > **Server Profiles**（サーバー プロファイル）> **HTTP** を選択します。ファイアウォールを設定して、ログを HTTP（S）宛先に転送したり、API を公開している任意の HTTP ベースのサービスと統合したりできるほか、HTTP リクエストの URL、HTTP ヘッダー、パラメータ、ペイロードをニーズに合わせて変更できます。また、HTTP サーバー プロファイルを使用して、PAN-OS が統合されている User-ID エージェントを実行しているファイアウォールにアクセスし、ファイアウォールにより生成されたログの送信元または宛先 IP アドレスに 1 つ以上のタグを登録できます。

HTTP サーバー プロファイルを使用してログを転送するための手順:

- システム、設定、ユーザー *ID*、*HIP* マッチ、および相関ログの場合は、「Device（デバイス）> Log Settings（ログ設定）」を参照してください。
- トラフィック、脅威、*Wildfire*、*URL* フィルタリング、データ フィルタリング、トンネル検査、認証、および *GTP* ログの場合は、「Objects（オブジェクト）> Log Forwarding（ログ転送）」を参照してください。

HTTP サーバー プロファイルを使用してログを転送している場合、その *HTTP* サーバー プロファイルを削除できません。ファイアウォールまたは *Panorama* のサーバー プロファイルを削除するには、そのプロファイルへのすべての参照を *Device*（デバイス）> *Log settings*（ログ設定）または *Objects*（オブジェクト）> *Log Forwarding*（ログ転送）のプロファイルから削除する必要があります。

HTTP サーバー プロファイルを定義するには、新しいプロファイルを **Add**（追加）し、以下の表の項目を設定します。

HTTP サーバー設定	の意味
氏名	サーバー プロファイルの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。有効な名前はアルファベット文字で始まる必要があります。名前には、ゼロ、アルファベット文字、下線 (_)、ハイフン (-)、ドット (.)、またはスペースを使用できます。
場所	サーバー プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、**Location**（場所）を変更できなくなります。
Tag Registration（タグ登録）	タグ登録では、ログ エントリ内の送信元または宛先 IP アドレスに対してタグを追加または削除したり、HTTP（S）を使用してファイアウォールの User-ID エージェントにマッピングする IP アドレスとタグを登録したりできます。その後、このタグをフィルタリング基準として使用してグループ メンバーを決定する動的アドレス グループを定義できるほか、タグに基づいてポリシー ルールを IP アドレスに適用できます。

© 2019 Palo Alto Networks, Inc.

HTTP サーバー設定	の意味
	接続の詳細を **Add**（追加）し、ファイアウォールの User-ID エージェントへの HTTP（S）アクセスを有効にします。 Panorama の User-ID エージェントにタグを登録するのにサーバー プロファイルは不要です。また、Windows サーバーで実行されている User-ID エージェントに、HTTP サーバー プロファイルを使用してタグを登録することはできません。
Servers [サーバー]タブ	
氏名	HTTP（S）サーバーを **Add**（追加）し、名前（最大 31 文字）またはリモートの User-ID エージェントを入力します。有効な名前は一意であり、アルファベット文字で始まる必要があります。名前には、ゼロ、アルファベット文字、下線 (_)、ハイフン (-)、ドット (.)、またはスペースを使用できます。 サーバー プロファイルには最大 4 つのサーバーを含めることができます。
アドレス	HTTP(S) サーバーの IP アドレスを入力します。 タグ登録の場合は、User-ID エージェントとして設定されているファイアウォールの IP アドレスを指定します。
PROTOCOL	いずれかのプロトコルを選択します:HTTP または HTTPS。
ポート	サーバー、またはファイアウォールにアクセスするためのポート番号を入力します。デフォルトの HTTP ポートは 80、HTTPS ポートは 443 です。 タグ登録の場合、ファイアウォールは HTTP または HTTPS を使用して、User-ID エージェントとして設定されているファイアウォールの Web サーバーに接続します。
TLS バージョン	サーバーの SSL がサポートしている TLS バージョンを選択します。デフォルトは **1.2** です。
証明書プロファイル	サーバーとの TLS 接続に使用する証明書プロファイルを選択します。 ファイアウォールは、サーバーへの安全な接続を確立する際に、指定された証明書プロファイルを使用してサーバー証明書を検証します。
HTTP 方式	サーバーがサポートする HTTP 方式を選択します。選択できるのは、GET、PUT、POST（デフォルト）、および DELETE です。 User-ID エージェントの場合、GET 方式を使用します。
username	選択した HTTP 方式を実行するためのアクセス権限を持つユーザー名を入力します。 タグをファイアウォールの User-ID エージェントに登録する場合は、スーパーユーザー ロールを持つ管理者のユーザー名である必要があります。
パスワード	サーバー、またはファイアウォールと認証を行うためのパスワードを入力します。
サーバー接続のテスト	サーバーへのネットワーク接続をテストするには、サーバーと **Test Server Connection**（サーバー接続のテスト）を選択します。

© 2019 Palo Alto Networks, Inc.

HTTP サーバー設定	の意味
	このテストでは、User-ID エージェントを実行しているサーバーへの接続はテストされません。
Payload Format (ペイロードの形式) タブ	
ログ タイプ	HTTP 転送で使用できるログ タイプが表示されます。ログ タイプをクリックして、カスタム ログ形式を指定するためのダイアログ ボックスを開きます。
format	デフォルト形式、事前定義済みの形式、またはユーザーが定義したカスタム ペイロード形式のうち、ログ タイプでどの形式を使用するかが表示されます。
事前定義済みの形式	サービスまたはベンダーでログを送信するための形式を選択します。事前定義済みの形式はコンテンツ更新によってプッシュされ、ファイアウォールまたは Panorama に新しいコンテンツ更新がインストールされるたびに変わる可能性があります。
氏名	カスタム ログ形式の名前を入力します。
URI の形式	HTTP(S) を使用してどのリソースにログを送信するかを指定します。 カスタム形式を作成する場合、**URI** は HTTP サービス上のリソースのエンドポイントになります。ファイアウォールは、ユーザーが事前に定義した IP アドレスに URI を付加して、HTTP リクエストの URL を構築します。URI とペイロードの形式が、サードパーティ ベンダーが要求する構文に一致することを確認してください。選択したログ タイプでサポートされる任意の属性を HTTP ヘッダー、パラメータと値のペア、およびリクエスト ペイロード内で使用できます。
HTTP ヘッダー	ヘッダーとそれに対応する値を追加します。
パラメータ	オプションのパラメータと値が含まれます。
ペイロード	外部 Web サーバーへの HTTP メッセージにペイロードとして含めるログ属性を選択します。
テスト ログの送信	外部 Web サーバーがリクエストを正しいペイロード形式で受信することを検証するには、このボタンをクリックします。

© 2019 Palo Alto Networks, Inc.

Device（デバイス） > Server Profiles（サーバー プロファイル） > NetFlow

Palo Alto Networks ファイアウォールは、そのインターフェイス上の IP トラフィックに関する統計を NetFlow フィールドとして NetFlow コレクタにエクスポートできます。NetFlow コレクタは、セキュリティ、管理、アカウント管理、およびトラブルシューティングの目的でネットワーク トラフィックを分析するために使用するサーバーです。すべての Palo Alto Networks ファイアウォールで NetFlow バージョン 9 がサポートされます。このファイアウォールでは、双方向ではなく、一方向の NetFlow のみをサポートします。ファイアウォールでは、インターフェイス上のすべての IP トラフィックに対して NetFlow 処理が実行されます。サンプリング NetFlow はサポートされていません。レイヤー 3、レイヤー 2、Virtualwire、tap、VLAN、ループバック、およびトンネルの各インターフェイスの NetFlow レコードをエクスポートできます。Ethernet の集約インターフェイスでは、集約グループのレコードをエクスポートできますが、グループ内の個々のインターフェイスのレコードをエクスポートできません。ファイアウォールは NetFlow の標準およびエンタープライズ（PAN-OS 固有）テンプレートをサポートします。NetFlow コレクタはこのテンプレートを使用して NetFlow フィールドを解読します。ファイアウォールは、次のエクスポートされたデータのタイプに基づいてテンプレートを選択します。IPv4またはIPv6トラフィック、NATを使用するかどうか、フィールドは標準のものかエンタープライズ固有のものか。

NetFlow エクスポートを設定するには、NetFlow サーバー プロファイルを **Add**（追加）し、エクスポートしたデータを受け取る NetFlow サーバーと、エクスポート パラメータを指定します。インターフェイスにプロファイルを割り当てると（「Network（ネットワーク） > Interfaces（インターフェイス）」を参照）、ファイアウォールは、そのインターフェイス上のすべてのトラフィックの NetFlow データを指定のサーバーにエクスポートします。

Netflow 設定	の意味
氏名	Netflow サーバー プロファイルの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
テンプレート更新レート	ファイアウォールは定期的に各 Netflow テンプレートを更新して、（エクスポートされたデータのタイプが変わった場合は）どのテンプレートを使用するかを再評価し、選択したテンプレートのフィールドに変更があれば適用します。NetFlow コレクタの要件に従って、ファイアウォールが NetFlow テンプレートを更新するレートを **Minutes**（分）（範囲は 1 ~ 3,600、デフォルトは 30）および **Packets**（パケット）（エクスポートされたレコード – 範囲は 1 ~ 600、デフォルトは 20）で指定します。どちらかのしきい値を超えると、ファイアウォールはテンプレートを更新します。必要な更新レートは、NetFlow コレクタに応じて異なります。サーバー プロファイルに複数の NetFlow コレクタを追加する場合、更新レートが最も速いコレクタの値を使用します。
アクティブ タイムアウト	ファイアウォールが各セッションのデータ レコードをエクスポートする頻度（分単位）を指定します（範囲は 1 ~ 60、デフォルトは 5）。NetFlow コレクタがトラフィック統計を更新する頻度に基づいて、頻度を設定します。
PAN-OS フィールド タイプ	Netflow レコードの App-ID および User-ID サービスの PAN-OS 特定フィールドをエクスポートします。

© 2019 Palo Alto Networks, Inc.

Netflow 設定	の意味
Servers（サーバー）	
氏名	サーバーを識別する名前を指定します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
SERVER	サーバーのホスト名または IP アドレスを指定します。プロファイルごとに最大 2 つのサーバーを追加できます。
ポート	サーバー アクセス用のポート番号を指定します（デフォルトは 2055）。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS]

認証プロファイルで参照する Remote Authentication Dial-In User Service（RADIUS）サーバーの設定を行うには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **RADIUS**を選択するか、**Panorama** > **Server Profiles**（サーバー プロファイル）> **RADIUS**を選択します（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。RADIUS を使用し、（GlobalProtect ポータル、またはキャプティブ ポータル経由で）ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォール、または Panorama でローカルに定義されている管理者を認証できるほか、RADIUS サーバーで外部で定義された管理者の認証と承認ができます。

RADIUS サーバー設定	の意味
プロファイル名	サーバー プロファイルを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定するには、このオプションを選択します。複数の仮想システムを持つファイアウォールでは、**Location**[場所] が **Shared**[共有] になっている場合にのみこのオプションが表示されます。
タイムアウト	認証要求がタイムアウトするまでの時間を秒単位で入力します (範囲は1 ~ 120、デフォルトは3)。 *RADIUS サーバー プロファイルを使用してファイアウォールを MFA サービスと統合する場合、この時間を入力して、認証チャレンジに応答できるだけの十分な時間をユーザーに与えます。たとえば、MFA サービスがワンタイム パスワード（OTP）を要求する場合、ユーザーには自分のエンドポイント デバイスで OTP を確認し、MFA ログイン ページに OTP を入力するまでの時間が必要です。*
Authentication Protocol（認証プロトコル）	ファイアウォールで RADIUS サーバーへの接続を保護するために使用する **Authentication Protocol**（認証プロトコル）を選択します。 • **PEAP-MSCHAPv2**– (デフォルト) Microsoft Challenge-Handshake Authentication Protocol (MSCHAPv2) による保護 EAP (PEAP) は、暗号化されたトンネルでユーザー名とパスワードの両方を送信することにより、PAP または CHAP に対するセキュリティを強化します。

© 2019 Palo Alto Networks, Inc.

RADIUS サーバー設定	の意味
	• **PEAP with GTC**（**GTC** 付属の **PEAP**）– 暗号化されたトンネルで 1 回限りのトークンを使用するには、汎用トークン カード（GTC）で保護された EAP（PEAP）を選択します。 • **EAP-TTLS with PAP**（**PAP** 付属の **EAP-TTLS**）– 暗号化されたトンネル内の PAP のプレーンテキスト証明書を転送するには、トンネルを通過する転送レイヤー セキュリティ（TTLS）および PAP で EAP を選択します。 • **CHAP** – RADIUS サーバーが EAP または PAP をサポートしない、またはその用途として構成しない場合、CHAP（Challenge-Handshake Authentication Protocol）を選択します。 • **PAP** – RADIUS サーバーが EAP または CHAP をサポートしない、または RADIUS サーバーを CHAP 用に構成しない場合、Password Authentication Protocol（PAP）を選択します。
有効期限が切れた後にユーザーがパスワードを変更できるようにする	（GlobalProtect 4.1 以降の PEAP-MSCHAPv2）GlobalProtect ユーザーが期限切れのパスワードを変更できるようにするには、このオプションを選択します。
Make Outer Identity Anonymous 外部アイデンティティを匿名化	（PEAP-MSCHAPv2、GTC 付属の PEAP、または PAP 付属の EAP-TTLS）このオプションはデフォルトで有効になっており、サーバーとの認証後にファイアウォールが作成する外部トンネルでユーザーの ID を匿名化します。 一部の *RADIUS* サーバー設定では、匿名の外部 *ID* はサポートされていない可能性があり、オプションをクリアする必要があります。クリアすると、ユーザー名はクリアテキストで送信されます。
証明書プロファイル	（PEAP-MSCHAPv2、GTC 付属の PEAP、または PAP 付属の EAP-TTLS）RADIUS サーバー プロファイルに関連付ける証明書プロファイルを選択または設定します。ファイアウォールはこの Certificate Profile (証明書プロファイル) を使用して RADIUS サーバーの認証を受けます。
再試行	タイムアウト後のリトライ回数を指定します (範囲は 1 ~ 5、デフォルトは 3)。
Servers（サーバー）	適切な順序で各サーバーの情報を設定します。 • **Name**[名前] – サーバーの識別に使用する名前を入力します。 • **RADIUS Server**[RADIUS サーバー] – サーバーの IP アドレスまたは FQDN を入力します。 • **Secret/Confirm Secret**[シークレット/再入力 シークレット] – ファイアウォールと RADIUS サーバー間の接続の検証と暗号化に使用する鍵を入力し、確認します。 • **Port (ポート)** – 認証要求に使用するサーバー ポート (範囲は 1 ~ 65,535、デフォルトは 1812) を入力します。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+]

ファイアウォールまたは Panorama が、Terminal Access Controller Access-Control System Plus（TACACS+）サーバーにどのようにアクセスするかを定義するための設定を行うには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **TACACS+** または **Panorama** > **Server Profiles**（サーバー プロファイル）> **TACACS+** を選択します（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。TACACS+ を使用し、（GlobalProtect ポータル、またはキャプティブ ポータル経由で）ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォールまたは Panorama でローカルに定義されている管理者を認証できるほか、TACACS+ サーバーで外部で定義された管理者の認証と承認ができます。

TACACS+ サーバー設定	の意味
プロファイル名	サーバー プロファイルを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定するには、このオプションを選択します。マルチvsysファイアウォールでは、**Location**[場所] が **Shared**[共有] になっている場合にのみこのオプションが表示されます。
タイムアウト	認証要求がタイムアウトするまでの時間を秒単位で入力します（範囲は1～20、デフォルトは3）。
Authentication Protocol（認証プロトコル）	ファイアウォールで TACACS+ サーバーへの接続を保護するために使用する **Authentication Protocol**（認証プロトコル）を選択します。 • **CHAP** – Challenge-Handshake Authentication Protocol（CHAP）はデフォルトのプロトコルです。PAP よりも安全なため、このプロトコルをお勧めします。 • **PAP** – TACACS+ サーバーが CHAP をサポートしない、または TACACS+ サーバーを CHAP 用に構成しない場合、Password Authentication Protocol（PAP）を選択します。 • **Auto** – ファイアウォールは最初に CHAP を使用して認証を試みます。TACACS+ サーバーが応答しない場合、ファイアウォールは PAP にフォールバックします。
すべての認証に単一接続を使用	すべての認証で同じTCPセッションを使用する場合は、このオプションを選択します。このオプションでは、認証イベントごとに個別の TCP セッションを開始および破棄するために必要な処理を回避できるため、パフォーマンスが向上します。

© 2019 Palo Alto Networks, Inc.

TACACS+ サーバー設定	の意味
Servers (サーバー)	**Add**[追加] をクリックして、TACACS+ サーバーごとに以下の設定を指定します。 • **Name**[名前] — サーバーの識別に使用する名前を入力します。 • **TACACS+ Server**[TACACS+ サーバー] — TACACS+ サーバーの IP アドレスまたは FQDN を入力します。 • **Secret/Confirm Secret**[シークレット/再入力 シークレット] — ファイアウォールとTACACS+サーバー間の接続の検証と暗号化に使用する鍵を入力し、確認します。 • **Port**[ポート] — 認証要求に使用するサーバーのポート (デフォルトは 49) を入力します。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP]

- **[Device]** > [サーバー プロファイル] > **LDAP**
- **Panorama** > **Server Profiles** (サーバー プロファイル) > **LDAP**

認証プロファイルで参照する Lightweight Directory Access Protocol (LDAP) サーバーの設定を行うには、LDAP サーバープロファイルを**Add** (追加)あるいは選択しますDevice (デバイス) > Authentication Profile (認証プロファイル)」を参照)。LDAP を使用し、 (GlobalProtect ポータル、またはキャプティブ ポータル経由で) ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォールまたは Panorama でローカルに定義されている管理者を認証できます。

LDAP サーバー設定	の意味
プロファイル名	プロファイルの識別に使用する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location** (場所) を選択することはできません。この値は Shared (共有) (ファイアウォール) または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定するには、このオプションを選択します。複数の仮想システムを持つファイアウォールでは、**Location**[場所] が **Shared**[共有] になっている場合にのみこのオプションが表示されます。
シリアル番号チェックで子のプロファイルを使用	このオプションを選択し、この LDAP サーバープロファイルが管理対象のエンドポイントからシリアル番号を収集できるようにします。GlobalProtect ポータルおよびゲートウェイがこの情報を使用し、エンドポイントが管理対象 (シリアル番号がアクティブディレクトリに存在) かどうか検証します。
Server List (サーバー リスト)	LDAP サーバーごとにホストの **Name** (名前)、IP アドレスまたは FQDN (**LDAP Server** (**LDAP** サーバー))、および **Port** (ポート) (デフォルトは 389) を**Add** (追加) します。 *LDAP サーバーを 2 つ以上設定して冗長化します。*
タイプ	ドロップダウンリストからサーバータイプを選択します。
ベースDN	ユーザーまたはグループ情報の検索を絞り込むための、ディレクトリ サーバーのルート コンテクストを指定します。
バインド DN	ディレクトリ サーバーのログイン名 (識別名) を指定します。

© 2019 Palo Alto Networks, Inc.

LDAP サーバー設定	の意味
	バインド *DN* アカウントには、*LDAP* ディレクトリを参照する権限が必要です。
パスワード/再入力 パスワード	バインド アカウントのパスワードを指定します。エージェントは暗号化したパスワードを設定ファイルに保存します。
バインドのタイムアウト	ディレクトリ サーバーに接続するときの時間制限（秒）を指定します（範囲は 1 ~ 30、デフォルトは 30）。
検索のタイムアウト	ディレクトリ検索を実行するときの時間制限（秒）を指定します（範囲は 1 ~ 30、デフォルトは 30）。
再試行間隔	システムが LDAP サーバーへの接続試行に失敗してから次に接続を試みるまでの間隔を秒単位で指定します（範囲は 1 ~ 3600、デフォルトは 60）。
SSL/TLS で保護された接続を要求	ファイアウォールで SSL または TLS を使用してディレクトリサーバーと通信する場合は、このオプションを選択します。プロトコルは、サーバー ポートによって異なります。 • 389（デフォルト）– TLS（具体的には、ファイアウォールは、最初のプレーンテキスト接続を TLS にアップグレードする StartTLS 操作を使用します） • 636 – SSL • その他の任意のポート – ファイアウォールはまずTLSの使用しようと試みます。ディレクトリ サーバーで TLS がサポートされていない場合は、SSL にフォールバックします。 セキュリティが向上するためこのオプションを使用することがベストプラクティスであり、デフォルトの状態で選択されています。
SSL セッションのサーバー証明書の確認	SSL/TLS 接続のためにディレクトリ サーバーから提供される証明書をファイアウォールで検証する場合は、このオプションを選択します（デフォルトではオフ）。証明書のについて、ファイアウォールは以下の2点を検証します。 • 証明書が信頼されていて有効であること。ファイアウォールで証明書を信頼するには、そのルート認証局（CA）とすべての中間証明書が **Device**（デバイス）> **Certificate Management**（証明書の管理）> **Certificates**（証明書）> **Device Certificates**（デバイス証明書）の下にある証明書ストアに含まれている必要があります。 • 証明書名は LDAP サーバーのホストの **Name**[名前] と一致していなければなりません。ファイアウォールは、まず証明書の「サブジェクト代替名」属性が一致しているかどうかをチェックし、次に「サブジェクト DN」属性を試行します。証明書でディレクトリ サーバーの FQDN が使用されている場合、**LDAP Server**[LDAP サーバー] フィールドに FQDN を使用しないと、名前の照合に失敗します。 検証に失敗すると、接続できません。この検証を有効にする場合は、**Require SSL/TLS secured connection**[SSL/TLSで保護された接続を要求] を選択する必要があります。

© 2019 Palo Alto Networks, Inc.

LDAP サーバー設定	の意味
	ファイアウォールが *SSL* セッションのサーバー証明書を検証できるようにし、セキュリティを向上させます。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]

ユーザーが Active Directory ドメインコントローラまたは Kerberos V5 準拠の認証サーバーとネイティブに認証できるようにサーバー プロファイルを設定するには、**Device**（デバイス）> **Server Profiles**（サーバー プロファイル）> **Kerberos** を選択するか、**Panorama** > **Server Profiles**（サーバー プロファイル）> **Kerberos**を選択します。Kerberos サーバー プロファイルを設定したら、そのサーバー プロファイルを認証プロファイルに割り当てることができます（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。Kerberos を使用し、（GlobalProtect ポータル、またはキャプティブ ポータル経由で）ネットワーク リソースにアクセスするエンド ユーザー、およびファイアウォール、または Panorama でローカルに定義されている管理者を認証できます。

Kerberos 認証を使用するには、*IPv4* アドレスでバックエンド *Kerberos* サーバーにアクセスできる必要があります。*IPv6* アドレスはサポートされません。

Kerberos サーバー設定	の意味
プロファイル名	サーバーを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定するには、このオプションを選択します。複数の仮想システムを持つファイアウォールでは、**Location**[場所] が **Shared**[共有] になっている場合にのみこのオプションが表示されます。
Servers（サーバー）	Kerberos サーバーごとに、**Add**[追加] をクリックして以下の設定を指定します。 • **Name**[名前] – サーバーの名前を入力します。 • **Kerberos Server**[Kerberos サーバー] – サーバーの IPv4 アドレスまたは FQDN を入力します。 • **Port**（ポート）– サーバーと通信するためのポート（範囲は 1 ~ 65,535、デフォルトは 88）を入力します（任意）。

© 2019 Palo Alto Networks, Inc.

Device（デバイス） > Server Profiles（サーバー プロファイル） > SAML Identity Provider（SAML アイデンティティ プロバイダ）

このページを使用して、Security Assertion Markup Language（SAML）2.0 アイデンティティ プロバイダ（IdP）をファイアウォールまたは Panorama に登録します。ネットワーク リソースへのアクセスを制御する SAML サービス プロバイダとしてファイアウォールまたは Panorama が機能できるようにするには、登録の手順が必要です。管理者およびエンド ユーザーがリソースを要求すると、サービス プロバイダは認証のためにユーザーを IdP にリダイレクトします。エンド ユーザーは、GlobalProtect またはキャプティブ ポータル ユーザーになることができます。管理者をファイアウォールおよび Panorama でローカルで管理できます。また、IdP アイデンティティ ストアで外部で管理することもできます。各ユーザーが 1 つのリソースにログインした後で複数のリソースに自動的にアクセスできるように、SAML シングル サインオン（SSO）を設定できます。また、SAML シングル ログアウト（SLO）を設定することもできます。これを使用すると、各ユーザーは、いずれか 1 つのサービスからログアウトすることで、SSO 対応のすべてのサービスから同時にログアウトできます。

認証シーケンスでは、*SAML IdP* サーバー プロファイルを指定する認証プロファイルがサポートされません。

ほとんどの場合、*SSO* を使用して同じモバイル デバイス上の複数のアプリケーションにアクセスできません。

キャプティブ ポータル ユーザーでは *SLO* を有効にできません。

SAML IdP サーバー プロファイルを作成する最も簡単な方法は、登録情報が含まれるメタデータ ファイルを IdP から **Import**（インポート）することです。インポートした値と共にサーバー プロファイルを保存したら、プロファイルを編集して値を変更できます。IdP からメタデータ ファイルが提供されない場合は、サーバー プロファイルを **Add**（追加）して、情報を手動で入力できます。サーバー プロファイルを作成したら、そのサーバー プロファイルを特定のファイアウォールまたは Panorama サービスの認証プロファイルに割り当てることができます（「Device（デバイス） > Authentication Profile（認証プロファイル）」を参照）。

SAML アイデンティティ プロバイダ サーバー設定	の意味
プロファイル名	サーバーを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	プロファイルを使用できる範囲を選択します。複数の仮想システムがあるファイアウォールの場合、仮想システムを選択するか、**Shared**（共有）（すべての仮想システム）を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。プロファイルを保存すると、その [場所] を変更できなくなります。

© 2019 Palo Alto Networks, Inc.

SAML アイデンティティ プロバイダ サーバー設定	の意味
管理者使用のみ	管理者アカウントでのみ認証にプロファイルを使用できるように指定するには、このオプションを選択します。複数の仮想システムを持つファイアウォールでは、**Location**[場所] が **Shared**[共有] になっている場合にのみこのオプションが表示されます。
アイデンティティ プロバイダ ID	IdP の識別子を入力します。この情報は IdP が提供します。
アイデンティティ プロバイダ証明書	ファイアウォールに送信する SAML メッセージに IdP が署名するために使用する証明書を選択します。IdP がファイアウォールに送信するメッセージの整合性を確保するには、IdP 証明書を選択する必要があります。認証局 (CA) の発行に対して IdP 証明書を検証するには、IdP サーバー プロファイルを参照するいずれかの認証プロファイルで **Certificate Profile** (証明書プロファイル)を指定する必要があります (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参照)。 証明書とそれに関連付けられる秘密鍵を生成、またはインポートする場合、証明書に指定されたキーの使用属性によってキーの使用目的が制御されることに注意してください。証明書で鍵の用途の属性が明示的にリストされている場合、属性の 1 つはデジタル署名です。デジタル署名はファイアウォールで生成する証明書では使用できません。このような場合は、エンタープライズ認証局 (CA) 、またはサードパーティ CA から証明書と鍵をインポートする必要があります。証明書で鍵の用途の属性が指定されていない場合は、メッセージの署名も含めて、どのような目的にも鍵を使用できます。このような場合は、任意の方法で証明書と鍵を取得 して SAML メッセージに署名できます。 IdP 証明書では、以下のアルゴリズムがサポートされます。 • 公開鍵アルゴリズム – RSA (1,024 ビット以上) および ECDSA (すべてのサイズ) 。FIPS/CC モードのファイアウォールでは、RSA (2,048ビット以上) および ECDSA (すべてのサイズ) がサポートされます。 • シグネチャ アルゴリズム – SHA1、SHA256、SHA384、および SHA512。FIPS/CC モードのファイアウォールでは、SHA256、SHA384、および SHA512 がサポートされます。
アイデンティティ プロバイダ SSO URL	IdP から通知されたシングル サインオン (SSO) サービス用の URL を入力します。 メタデータ ファイルをインポートしてサーバー プロファイルを作成する場合、そのファイルに複数の SSO URL が指定されていると、ファイアウォールは、POST またはリダイレクト バインド方式を指定している最初の URL を使用します。 *SAML では HTTP もサポートされますが、HTTPS を使用する URL を使用することを強くお勧めします。*
アイデンティティ プロバイダ SLO URL	IdP から通知されたシングル ログアウト (SLO) サービス用の URL を入力します。 メタデータ ファイルをインポートしてサーバー プロファイルを作成する場合、そのファイルに複数の SLO URL が指定されていると、ファイアウォール

© 2019 Palo Alto Networks, Inc.

SAML アイデンティティ プロバイダ サーバー設定	の意味
	は、POST またはリダイレクト バインド方式を指定している最初の URL を使用します。 *SAML では HTTP もサポートされますが、HTTPS を使用する URL を使用することを強くお勧めします。*
SSO SAML HTTP バインディング	**Identity Provider SSO URL**（アイデンティティ プロバイダ **SSO URL**）に関連付けられている HTTP バインディングを選択します。ファイアウォールはバインドを使用して SAML メッセージを IdP に送信します。オプションは次のとおりです： • **POST** – ファイアウォールは base64 エンコード済みの HTML 形式を使用してメッセージを送信します。 • **Redirect**（リダイレクト）– ファイアウォールは、base64 エンコード済みおよび URL エンコード済みの SSO メッセージを URL パラメータ内で送信します。 *複数の SSO URL を持つ IdP メタデータ ファイルをインポートした場合、ファイアウォールは、POST またはリダイレクト方式を使用する最初の URL のバインドを使用します。ファイアウォールは、他のバインドを使用する URL を無視します。*
SLO SAML HTTP バインディング	**Identity Provider SLO URL**（アイデンティティ プロバイダ **SLO URL**）に関連付けられている HTTP バインディングを選択します。ファイアウォールはバインドを使用して SAML メッセージを IdP に送信します。オプションは次のとおりです： • **POST** – ファイアウォールは base64 エンコード済みの HTML 形式を使用してメッセージを送信します。 • **Redirect**（リダイレクト）– ファイアウォールは、base64 エンコード済みおよび URL エンコード済みの SSO メッセージを URL パラメータ内で送信します。 *複数の SLO URL を持つ IdP メタデータ ファイルをインポートした場合、ファイアウォールは、POST またはリダイレクト方式を使用する最初の URL のバインドを使用します。ファイアウォールは、他のバインドを使用する URL を無視します。*
アイデンティティ プロバイダ メタデータ	このフィールドは、IdP からファイアウォールにアップロードした IdP メタデータ ファイルを **Import**（インポート）した場合にのみ表示されます。このファイルでは、新しい SAML IdP サーバー プロファイルの値と署名証明書を指定します。ファイルを **Browse**（参照）し、Profile Name（プロファイル名）と Maximum Clock Skew（最大クロック スキュー）を指定して、**OK** をクリックすると、プロファイルが作成されます。必要に応じて、プロファイルを編集し、インポートされた値を変更できます。
アイデンティティ プロバイダ証明書の検証	信頼チェーンを検証し、オプションで IdP 署名証明書の失効ステータスを検証するには、このオプションを選択します。 このオプションを有効にするために、認証局 (CA) が IdP の署名証明書を発行する必要があります。IdP の署名証明書を発行した CA を含む証明書プロファイル

© 2019 Palo Alto Networks, Inc.

SAML アイデンティティ プロバイダ サーバー設定	の意味
	を作成する必要があります。認証プロファイルで、IdP 証明書を検証するための SAML サーバ プロファイルおよび証明書プロファイルを選択します (「Device (デバイス) > Authentication Profile (認証プロファイル)」を参照)。 IdP 署名証明書が自己署名証明書である場合、信頼チェーンはありません。 その場合は、このオプションを有効にすることはできません。ファイアウォールは **Validate Identity Provider Certificate** (アイデンティティ プロバイダ証明書の検証) オプションを有効にするかどうかに関係なく、設定するアイデンティティ プロバイダ証明書に対して SAML 応答またはアサーションのシグネチャを常に検証します。IdP が自己署名証明書を提供する場合、PAN-OS 9.1.3 以降の バージョンを使用して、 CVE-2020-2021への影響が軽減していることを確認してください。
IdP への SAML メッセージの署名	IdP に送信するメッセージをファイアウォールで署名することを指定するには、このオプションを選択します。ファイアウォールでは、認証プロファイルで指定した **Certificate for Signing Requests**（署名要求の証明書）が使用されます（「Device（デバイス） > Authentication Profile（認証プロファイル）」を参照）。 署名証明書を使用することで、*IdP* に送信するメッセージの整合性が確保されます。
最大クロック スキュー	ファイアウォールが IdP から受信したメッセージを検証する時点で、IdP とファイアウォールのシステム時間に対して許容される最大時間差を秒単位で入力します（範囲は 1 ~ 900、デフォルトは 60）。時間差がこの値を超える場合、検証（つまり、認証）は失敗します。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > DNS [デバイス > サーバー プロファイル > DNS]

仮想システムの設定を簡略化するために、DNSサーバープロファイルでは、設定されている仮想システム、DNSサーバーの継承ソースまたはプライマリ/セカンダリDNSアドレス、およびDNSサーバーに送信されるパケットで使用する送信元インターフェイスと送信元アドレス（サービスルート）を指定できます。送信元インターフェイスと送信元アドレスは、DNS サーバーからの応答の宛先インターフェイスと宛先アドレスとして使用されます。

DNS サーバー プロファイルは仮想システム専用で、グローバルな共有の場所では使用できません。

DNS サーバー プロファイル設定	の意味
氏名	DNS サーバー プロファイルの名前を付けます。
場所	プロファイルを適用する仮想システムを選択します。
継承ソース	DNS サーバーのアドレスを継承しない場合、**None**[なし] を選択します。継承する場合は、プロファイルが設定を継承する DNS サーバーを指定します。
継承ソース状態のチェック	継承ソースの情報を確認する場合にクリックします。
プライマリ DNS	プライマリDNSサーバーのIPアドレスを指定します。
セカンダリ DNS	セカンダリDNSサーバーのIPアドレスを指定します。
サービスルートIPv4	DNSサーバーに送信されるパケットの送信元がIPv4になるように指定する場合、このオプションを選択します。
送信元インターフェイス	DNS サーバーに送信されるパケットで使用する送信元インターフェイスを指定します。
送信元アドレス	DNS サーバーに送信されるパケットの IPv4 送信元アドレスを指定します。
サービスルートIPv6	DNSサーバーに送信されるパケットの送信元がIPv6になるように指定する場合、このオプションを選択します。
送信元インターフェイス	DNS サーバーに送信されるパケットで使用する送信元インターフェイスを指定します。
送信元アドレス	DNS サーバーに送信されるパケットの IPv6 [送信元アドレス] を指定します。

© 2019 Palo Alto Networks, Inc.

Device（デバイス） > Server Profiles（サーバー プロファイル） > Multi Factor Authentication（多要素認証）

このページを使用して、多重認証（MFA）サーバー プロファイルを設定し、ファイアウォールを MFA サーバーにどのように接続するかを定義します。MFA では、最高機密のリソースを保護できます。この方法では、攻撃者は単一認証要素を侵害して（たとえば、ログイン認証情報を盗んで）ネットワークにアクセスし、ネットワークを横断することはできません。サーバー プロファイルを設定したら、認証を要求するサービスの認証 プロファイルにサーバー プロファイルを割り当てます（「Device（デバイス） > Authentication Profile（認証プロファイル）」を参照）。

次の認証の使用例では、ファイアウォールは RADIUS と SAML を使用する多要素認証（MFA）ベンダーと統合されます。

- GlobalProtect™ ポータルとゲートウェイによるリモート ユーザー認証。
- PAN-OS および Panorama™ Web インターフェイスの管理者認証。
- 認証ポリシーによる認証。

さらに、ファイアウォールは API を使用して MFA vendors（MFA ベンダー）と統合して、エンドユーザ認証のみ（GlobalProtect 認証または管理者認証ではない）の認証ポリシーによる MFA の適用も可能です。

MFA を設定するための完全な手順では、サーバー プロファイルの作成に加えて追加のタスクが必要です。

認証シーケンスでは、*MFA* サーバー プロファイルを指定する認証プロファイルがサポートされません。

ファイアウォールが *RADIUS* を介して *MFA* ベンダーと統合している場合、*RADIUS* サーバー プロファイルを設定します（「Device（デバイス） > Server Profiles（サーバー プロファイル） > RADIUS」を参照）。ファイアウォールは *RADIUS* を介してあらゆる *MFA* ベンダーをサポートします。

MFA サーバー設定	の意味
プロファイル名	サーバーを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	複数の仮想システム（vsys）があるファイアウォールでは、vsys または **Shared**（共有）の場所を選択します。プロファイルを保存すると、その **Location**（場所）を変更できなくなります。
証明書プロファイル	サーバーへの安全な接続をセットアップするときにファイアウォールで MFA サーバー証明書を検証するために使用する認証局（CA）証明書を指定する **Certificate Profile**（証明書プロファイル）を選択します。詳細は、「Device（デバイス） > Certificate Management（証明書の管理） > Certificate Profile（証明書プロファイル）」を参照してください。

© 2019 Palo Alto Networks, Inc.

MFA サーバー設定	の意味

MFA ベンダー/値	MFA ベンダーの **MFA Vendor**（**MFA** ベンダー）を選択し、ベンダー属性ごとに **Value**（値）を入力します。属性はベンダーによって異なります。正しい値については、ベンダーのドキュメントを参照してください。
	• **Duo v2**:
	  • **API Host**（**API** ホスト） – Duo v2 サーバーのホスト名。
	  • **Integration Key**（統合キー）および **Secret Key**（シークレット キー） – ファイアウォールはこれらのキーを使用して Duo v2 サーバーとの認証を行い、サーバーに送信する認証要求に署名します。これらのキーを保護するため、ファイアウォール上のマスター キーによってこれらのキーが自動的に暗号化されます。これにより、これらのキーのプレーンテキスト値はファイアウォール ストレージのどの場所にも表示されなくなります。キーを取得するには、Duo v2 管理者に問い合わせてください。
	  • **Timeout**（タイムアウト） – **API Host**（**API** ホスト）との通信を試みているときにファイアウォールがタイムアウトするまでの時間を秒単位で入力します（範囲は 5 ~ 600、デフォルトは 30）。この間隔は、API ホストとユーザーのエンドポイント デバイスとの間のタイムアウトよりも長くする必要があります。
	  • **Base URI**（ベース **URI**） – 組織が Duo v2 サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシ サーバーの URI（デフォルトは /auth/v2）を入力します。
	• **Okta Adaptive**:
	  • **API Host**（**API** ホスト） – Okta サーバーのホスト名。
	  • **Base URI**（ベース **URI**） – 組織が Okta サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシ サーバーの URI（デフォルトは /api/v1）を入力します。
	  • **Token**（トークン） – ファイアウォールはこのトークンを使用して Okta サーバーとの認証を行い、サーバーに送信する認証要求に署名します。トークンを保護するため、ファイアウォール上のマスター キーによってトークンが自動的に暗号化されます。これにより、トークンのプレーンテキスト値はファイアウォール ストレージのどの場所にも表示されなくなります。トークンを取得するには、Okta 管理者に問い合わせてください。
	  • **Organization**（組織） – **API Host**（**API** ホスト）内の組織のサブドメイン。
	  • **Timeout**（タイムアウト） – **API Host**（**API** ホスト）との通信を試みているときにファイアウォールがタイムアウトするまでの時間を秒単位で入力します（範囲は 5 ~ 600、デフォルトは 30）。この間隔は、API ホストとユーザーのエンドポイント デバイスとの間のタイムアウトよりも長くする必要があります。
	• **PingID**:
	  • **Base URI**（ベース **URI**） – 組織が PingID サーバー用のローカルの認証プロキシ サーバーをホストしている場合、そのプロキシ サーバーの URI（デフォルトは /pingid/rest/4）を入力します。
	  • **Host name**（ホスト名） – PingID サーバーのホスト名を入力します（デフォルトは idpxnyl3m.pingidentity.com）。
	  • **Use Base64 Key**（**Base64** キーを使用）および **Token**（トークン） – ファイアウォールはこのキーとトークンを使用して PingID サーバーとの認証を行い、サーバーに送信する認証要求に署名します。このキーとトークンを保護するため、ファイアウォール上のマスター キーによってこのキーと

© 2019 Palo Alto Networks, Inc.

MFA サーバー設定	の意味
	トークンが自動的に暗号化されます。これにより、このキーとトークンのプレーンテキスト値はファイアウォール ストレージのどの場所にも表示されなくなります。値を取得するには、PingID 管理者に問い合わせてください。 • **PingID Client Organization ID**（**PingID** クライアント組織 **ID**）– 組織の PingID 識別子。 • **Timeout**（タイムアウト）– **Host name**（ホスト名）で指定された PingID サーバーとの通信を試みているときにファイアウォールがタイムアウトするまでの時間を秒単位で入力します（範囲は 5 ~ 600、デフォルトは 30）。この間隔は、PingID サーバーとユーザーのエンドポイント デバイスとの間のタイムアウトよりも長くする必要があります。

© 2019 Palo Alto Networks, Inc.

Device > Local User Database > Users [デバイス > ローカル ユーザー データベース > ユーザー]

ファイアウォールの管理者、キャプティブ ポータルのエンド ユーザー、および GlobalProtect ポータルと GlobalProtect ゲートウェイへの認証を行うエンド ユーザーの認証情報をファイアウォールのローカル データベースに保管するようにセットアップできます。ローカル データベース認証では、外部の認証サービスは不要です。すべてのアカウント管理をファイアウォールで実行します。ローカル データベースを作成し、（オプションで）ユーザーをグループに割り当て（「Device（デバイス）> Local User Database（ローカル ユーザー データベース）> User Groups（ユーザー グループ）」を参照）た後、ローカル データベースに基づいて Device（デバイス）> Authentication Profile（認証プロファイル）を設定できます。

ローカル データベース認証を使用する管理者アカウントに対して、Device（デバイス）> Password Profiles（パスワード プロファイル）を設定することはできません。

ローカル ユーザーをデータベースに **Add**（追加）するには、以下の表の説明に従って設定を行います。

Local User Setting（ローカル ユーザー設定）	の意味
氏名	ユーザーを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	ユーザー アカウントを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。ユーザー アカウントを保存すると、その [場所] を変更できなくなります。
モード	以下のいずれかの認証オプションを指定します。 • **Password**[パスワード] – ユーザーのパスワードを入力および確認します。 • **Password Hash**[パスワード ハッシュ] – ハッシュされたパスワード文字列を入力します。これは、たとえば、既存の UNIX アカウントの認証情報を再利用するときに、プレーンテキストのパスワードがわからず、ハッシュされたパスワードのみを把握している場合に便利です。ファイアウォールは、ハッシュ値の生成に使用するアルゴリズムに関係なく、最大 63 文字の任意の文字列を受け入れます。CLI 操作コマンド **`request password-hash password`** では、ファイアウォールが通常モードの場合は MD5 アルゴリズムが使用され、ファイアウォールが CC/FIPS モードの場合は SHA256 アルゴリズムが使用されます。 ファイアウォールに設定した Minimum Password Complexity（パスワード複雑性設定）パラメータ（*Device*（デバイス）> *Setup*（セットアップ）> *Management*（管理））は、*Password*

© 2019 Palo Alto Networks, Inc.

Local User Setting（ローカル ユーザー設定）	の意味
	Hash（パスワード ハッシュ）を使用するアカウントに適用されません。
Enable [有効化]	ユーザーアカウントをアクティベートする場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

Device > Local User Database > User Groups [デバイス > ローカル ユーザー データベース > ユーザー グループ]

ユーザー グループ情報をローカル データベースに追加するには、**Device**（デバイス）> **Local User Database**（ローカル ユーザー データベース）> **User Groups**（ユーザー グループ）を選択します。

ローカル ユーザー グループ設定	の意味
氏名	グループを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	ユーザー グループを使用できる範囲を選択します。複数の仮想システム (vsys) があるファイアウォールの場合、vsys を選択するか、**Shared**[共有] (すべての仮想システム) を選択します。その他の場合、**Location**（場所）を選択することはできません。この値は Shared（共有）（ファイアウォール）または Panorama として事前に定義されています。ユーザー グループを保存すると、その [場所] を変更できなくなります。
すべてのローカル ユーザー	**Add**[追加] をクリックし、グループに追加するユーザーを選択します。

© 2019 Palo Alto Networks, Inc.

Device > Scheduled Log Export [デバイス > スケジュール設定されたログのエクスポート]

ログのエクスポートをスケジューリングしてログを FTP (File Transfer Protocol: ファイル転送プロトコル) サーバーに CSV 形式で保存したり、SCP (Secure Copy: セキュア コピー) を使用してファイアウォールとリモート ホスト間でデータを安全に転送したりできます。ログのプロファイルには、スケジュールと FTP サーバーの情報が含まれています。たとえば、プロファイルを使用して、毎日 3:00 AM に前日のログを収集して特定の FTP サーバーに保存するように指定できます。

Add[追加] をクリックし、以下の詳細を入力します。

スケジュール設定されたログのエクスポート設定	の意味
氏名	プロファイルの識別に使用する名前を入力します (最大 31 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 プロファイルを作成した後でこの名前を変更することはできません。
の意味	説明 (最大 255 文字) を入力します (任意)。
Enable [有効化]	ログのエクスポートのスケジューリングを有効にする場合は、このオプションを選択します。
ログ タイプ	ログ タイプを選択します (**traffic** (トラフィック)、**threat** (脅威)、**gtp**、**sctp**、**tunnel** (トンネル)、**userid**、**auth**、**url**、**data** (データ)、**hipmatch**、または**wildfire**)。デフォルトはtrafficです。
エクスポートの開始予定時刻 (毎日)	エクスポートを開始する時刻 (hh:mm) を 24 時間形式 (00:00 ~ 23:59) で入力します。
PROTOCOL	ファイアウォールからリモート ホストへのログのエクスポートに使用するプロトコルを選択します。 • **FTP** – このプロトコルは安全ではありません。 • **SCP** – このプロトコルは安全です。残りのフィールドを入力したら、**Test SCP server connection** (**SCP**サーバー接続のテスト) をクリックして、ファイアウォールと SCP サーバー間の接続テストを行い、SCP サーバーのホストキーを検証して受け入れる必要があります。
ホスト名	エクスポートに使用する FTP サーバーのホスト名または IP アドレスを入力します。
ポート	FTP サーバーで使用するポート番号を入力します。デフォルトは 21 です。
path	エクスポートした情報の保存に使用する FTP サーバー上のパスを指定します。
FTP パッシブモードの有効化	エクスポートにパッシブモードを使用する場合は、このオプションを選択します。デフォルトでは、このオプションはオンになっています。

© 2019 Palo Alto Networks, Inc.

スケジュール設定されたログのエクスポート設定	の意味
username	FTP サーバーへのアクセスに使用するユーザー名を入力します。デフォルトはanonymousです。
パスワード/再入力 パスワード	FTP サーバーへのアクセスに使用するパスワードを入力します。ユーザーが anonymous の場合、パスワードは必要ありません。
SCP サーバー接続のテスト （SCP プロトコルのみ）	**Protocol**（プロトコル）を **SCP** に設定した場合、このボタンをクリックしてファイアウォールと SCP サーバー間の接続テストを行い、SCP サーバーのホストキーを検証して受け入れる必要があります。 *Panorama* テンプレートを使用してログのエクスポート スケジュールを設定する場合、テンプレート設定をファイアウォールにコミットした後にこの手順を実行する必要があります。テンプレートのコミットが完了したら、各ファイアウォールにログインし、ログのエクスポート スケジュールを開いて、*Test SCP server connection*（*SCP* サーバー接続のテスト）をクリックします。

© 2019 Palo Alto Networks, Inc.

Device > Software [デバイス > ソフトウェア]

使用可能なソフトウェア リリースの表示、リリースのダウンロードまたはアップロード、リリースのインストール (サポート ライセンスが必要)、ファイアウォールからのソフトウェア イメージの削除、またはリリース ノートの表示を行う場合は **Device** (デバイス) > **Software** (ソフトウェア) を選択します。

ソフトウェアのバージョンをアップグレードまたはダウンロードする前に以下を確認してください。

- 現在のRelease Notes (リリース ノート) を参照し、新機能の説明とリリースのデフォルト動作の変更を表示し、ソフトウェアをアップグレードするための移行パスを表示する。
- PAN-OS® 9.1 New Features Guide (PAN-OS® 9.1 新機能ガイド)のアップグレードとダウングレードの検討事項とアップグレードに関する指示を参照します。
- ファイアウォールの日時設定が現在の日時になっている。PAN-OSソフトウェアはデジタル署名されており、ファイアウォールは新バージョンをインストールする前に署名を確認します。ファイアウォールに現在以外の日付が設定されていると、ファイアウォールはソフトウェア署名の日付が誤って未来になっていると認識し、以下のメッセージを表示します。

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

以下の表に、**Software**[ソフトウェア] ページの使用方法を示します。

ソフトウェア オプション フィールド	の意味
バージョン	Palo Alto Networks 更新サーバーで現在入手可能なソフトウェア バージョンが一覧表示されます。Palo Alto Networks から新しいソフトウェア リリースを入手可能かどうかをチェックするには、**Check Now**[今すぐチェック] をクリックします。ファイアウォールがサービス ルートを使用して更新サーバーに接続し、新しいバージョンをチェックします。適用可能な更新がある場合は、その更新がリストの最上部に表示されます。
サイズ	ソフトウェア イメージのサイズを示します。
リリース日	Palo Alto Networks がリリースを公開した日時を示します。
使用可能	対応するバージョンのソフトウェア イメージがファイアウォールにアップロードまたはダウンロードされていることを示します。
現在インストール済み	対応するバージョンのソフトウェア イメージがアクティベーションされていて、ファイアウォールで現在実行されているかどうかを示します。
操作	対応するソフトウェア イメージで現在実行可能な以下のようなアクションを示します。 • **Download** [ダウンロード] – 対応するソフトウェアバージョンがPalo Alto Networks更新サーバーから入手可能です。入手可能なソフトウェアバージョンを**Download** [ダウンロード] する場合はクリックします。 • **Install** [インストール] – 対応するソフトウェア バージョンがファイアウォールにダウンロード済みまたはアップロード済みです。ソフトウェアを**Install** [インストール] する場合はクリックします。アップグレード プロセスの完了時に再起動が必要です。

© 2019 Palo Alto Networks, Inc.

ソフトウェア オプション フィールド	の意味
	• **Reinstall** [再インストール] - 対応するソフトウェアバージョンが以前インストールされていました。このバージョンを**Reinstall** [再インストール] する場合はクリックします。
リリース ノート	対応するソフトウェア更新のリリース ノートへのリンクが提供されます。このリンクは、Palo Alto Networks 更新サーバーからダウンロードする更新の場合にのみ使用でき、アップロードされた更新では使用できません。
☒	以前にダウンロードまたはアップロードしたソフトウェア イメージをファイアウォールから削除します。アップグレードの必要がない古いリリースの基本イメージのみを削除してください。たとえば、7.0 を実行している場合、ダウングレードする必要がなければ、6.1 の基本イメージを削除できます。
今すぐチェック	Palo Alto Networks から新しいソフトウェア更新を入手可能かどうかをチェックします。
アップロード	ファイアウォールがアクセスできるコンピュータからソフトウェア更新イメージをインポートします。通常、この操作はファイアウォールがインターネットにアクセスできない場合に実行します。Palo Alto Networks 更新サーバーから更新をダウンロードするには、インターネットにアクセスできる必要があります。アップロードを行う場合、インターネットに接続されたコンピュータから Palo Alto Networks の Web サイトにアクセスし、サポート サイト（ソフトウェア アップデート）からソフトウェア イメージをダウンロードし、アップデート内容をコンピュータにダウンロードし、ファイアウォールの **Device**（デバイス）> **Software**（ソフトウェア）を選択してソフトウェア イメージの **Upload**（アップロード）を行います。高可用性 (HA) 設定の場合、**Sync To Peer** [ピアと同期] のオプションを選択し、インポートしたソフトウェアイメージをHAピアにプッシュします。アップロードが完了すると、**Software**（ソフトウェア）ページに、アップロードおよびダウンロードしたソフトウェアと同一の情報（バージョンやサイズなど）と、**Install**（インストール）/**Reinstall**（再インストール）のオプションが表示されます。アップロードしたソフトウェアの場合、**Release Notes** [リリースノート] のオプションは無効化されています。

© 2019 Palo Alto Networks, Inc.

Device > Dynamic Updates [デバイス > 動的更新]

- Device > Dynamic Updates [デバイス > 動的更新]
- Panorama > Dynamic Updates [Panorama > 動的更新]

Palo Alto Networks は動的更新を通じて、新規および更新済みアプリケーション検出、脅威防御、および GlobalProtect データ ファイルが含まれる更新を定期的に公開しています。設定を変更することなく、ファイアウォールはこれらの更新を取得し、それを使ってポリシーを適用できます。アプリケーションおよび一部のアンチウイルス アップデートはサブスクリプションなしで利用できます。その他はお使いのサブスクリプションに紐付いています。

最新の更新ファイルを表示し、各更新ファイルのリリースノートを読み、ダウンロードおよびインストールする更新ファイルを選択できます。以前にインストールした更新のバージョンに戻すこともできます。

動的更新のスケジュールを設定すると、ファイアウォールが新しい更新の有無を確認し、ダウンロードまたはインストールする頻度を定義することができます。特に、アプリケーションや脅威のコンテンツの更新では、脅威の更新の背後に新しいアプリケーションや変更されたアプリケーションの更新を計画するスケジュールを設定できます。 これにより、ファイアウォールに常に最新の脅威防止機能を備えつつ、新規および変更されたアプリケーションがセキュリティ ポリシーにどのように影響するかを評価する時間が長くなります。

Dynamic Updates Options（動的更新オプション）	の意味
バージョン	Palo Alto Networks 更新サーバーで現在入手可能なバージョンが一覧表示されます。Palo Alto Networks から新しいソフトウェア リリースを入手可能かどうかをチェックするには、**Check Now**[今すぐチェック] をクリックします。ファイアウォールがサービス ルートを使用して更新サーバーに接続し、新しいコンテンツ リリース バージョンをチェックします。適用可能な更新がある場合は、その更新がリストの最上部に表示されます。
最終チェック	ファイアウォールが最後に更新サーバーに接続して更新があるかどうかをチェックした日時が表示されます。
スケジュール	更新を取得する頻度をスケジューリングできます。 動的コンテンツアップデートの頻度およびタイミング（**Recurrence**（繰返し）と時間）を設定し、またスケジュール設定されたアップデートの**Download Only**（ダウンロードのみ） 行うか、**Download and Install**（ダウンロードとインストール）を行うかを設定することが可能です。 Antivirus and Applications and Threats（ウイルス対策とアプリケーションと脅威の更新）では、ファイアウォールがインストールする前にコンテンツ更新を利用できる最小時間を設定するオプションがあります。ごくまれに、コンテンツの更新にエラーが発生する可能性があり、このしきい値は、ファイアウォールが指定された時間、利用可能かつ顧客環境で機能しているコンテンツリリースのみをダウンロードすることを保証します。 アプリケーションと脅威のコンテンツの更新では、新規および変更されたアプリケーションでコンテンツの更新に特に適用されるしきい値を設定することもできます。拡張アプリケーションのしきい値は、新しいアプリケーショ

© 2019 Palo Alto Networks, Inc.

Dynamic Updates Options（動的更新オプション）	の意味
	ンや変更されたアプリケーションが導入する変更に基づいてセキュリティ ポリシーを評価し、調整するための時間が長くなります。 *Application and Threat*（アプリケーションと脅威）のコンテンツの更新を常に有効にして、アプリケーションの可用性と最新の脅威の両方を保護する方法については、「アプリケーションと脅威の更新に関するベストプラクティス」を参照してください
ファイル名	ファイル名が一覧表示されます。ファイル名にはコンテンツのバージョン情報が含まれます。
機能	コンテンツ バージョンに含めることができるシグネチャのタイプが一覧表示されます。 アプリケーションおよび脅威コンテンツリリースバージョンの場合、このフィールドには、**Apps, Threats** [アプリケーションおよび脅威] を確認するためのオプションが表示されることがあります。このオプションをクリックすると、ファイアウォールにインストールされた最後のコンテンツ リリース バージョンから使用できるようになった新しいアプリケーション シグネチャが表示されます。**New Applications**（新しいアプリケーション）ダイアログを使用して、新しいアプリケーションを **Enable**（有効化）**/Disable**（無効化）することもできます。一意に識別されるアプリケーションがポリシーに影響を及ぼさないようにするため、コンテンツ リリースに含まれる新しいアプリケーションを無効にする場合があります (未知だったアプリケーションが識別され、以前とは異なって分類されると、コンテンツのインストール前後でアプリケーションの処理が変わる可能性があります)。
タイプ	ダウンロードにフル データベース更新が含まれているか、増分更新が含まれているかを示します。
サイズ	コンテンツ更新パッケージのサイズが表示されます。
リリース日	Palo Alto Networks がコンテンツ リリースを公開した日時。
ダウンロード済み	この列のチェック マークは、対応するコンテンツ リリース バージョンがファイアウォールにダウンロード済みであることを示します。
現在インストール済み	この列のチェック マークは、対応するコンテンツ リリース バージョンがファイアウォールで現在実行されていることを示します。
操作	対応するソフトウェア イメージで現在実行可能な以下のようなアクションを示します。 • **Download**（ダウンロード）– 対応するコンテンツ リリース バージョンを Palo Alto Networks 更新サーバーから入手できます。コンテンツ リリース バージョンをダウンロードするには、**Download**（ダウンロード）をクリックします。ファイアウォールがインターネットに接続できない場合は、インターネットに接続できるコンピュータからCustomer Support Portal（カスタマー サポート ポータル）サイトにアクセスし、**Dynamic Updates**（動的更新）を選択します。必要なコンテンツリリースバージョンを検索して **Download**（ダウンロード）をクリックし

© 2019 Palo Alto Networks, Inc.

Dynamic Updates Options（動的更新オプション）	の意味
	て、ローカル コンピュータに更新パッケージを保存します。次にファイアウォールへソフトウェアイメージを手動で**Upload** [アップロード] します。また、アプリケーションおよび脅威コンテンツ リリース バージョンをダウンロードすると、リリースに含まれる新しいアプリケーション シグネチャの影響を受ける**Review Policies** (ポリシーを確認)するためのオプションが有効になります。 • **Review Policies**（ポリシーの確認）（アプリケーションおよび脅威コンテンツのみ）– コンテンツ リリース バージョンに含まれる新しいアプリケーションによるポリシーへの影響を確認します。コンテンツ更新のインストール前後のアプリケーションの処理を評価するには、このオプションを使用します。Policy Review（ポリシーのレビュー）ダイアログを使用して、保留中のアプリケーション（コンテンツ リリース バージョンでダウンロードされたが、ファイアウォールにインストールされていないアプリケーション）を既存のセキュリティ ポリシーに追加または既存のセキュリティ ポリシーから削除することもできます。保留中のアプリケーションのポリシーを変更しても、その変更は、対応するコンテンツ リリース バージョンがインストールされるまで有効になりません。 • **Review Apps**（アプリのレビュー）（アプリケーションと脅威コンテンツのみ）– ファイアウォールにインストールされた最後のコンテンツ リリース バージョンから使用できるようになった新規および変更済みアプリケーション シグネチャが表示されます。重要なアプリケーションの適用に影響を与える可能性のある変更がコンテンツ更新によって導入された場合、それらのアプリケーションにはポリシー レビューの推奨としてマークされます。Review Policies（ポリシーの確認）をクリックすると、コンテンツの更新が既存のセキュリティ ポリシーにどのように影響するのかを確認したり、アプリケーションのポリシーの影響を確認するまでアプリケーションを無効にすることができます。 • **Install** [インストール] – 対応するコンテンツリリースバージョンがファイアウォールにダウンロード済みです。アップデートを**Install** [インストール] する場合にクリックします。新しいアプリケーションおよび脅威コンテンツ リリース バージョンをインストールすると、**Disable new apps in content update**[コンテンツ更新での新しいアプリケーションの無効化] オプションが表示されます。このオプションにより、最新の脅威に対する保護を有効にしながら、新しいアプリケーション シグネチャの影響のためにポリシーの更新を準備した後でアプリケーションを柔軟に有効にできます（以前に無効にしたアプリケーションを有効にするには、Dynamic Updates（動的更新）ページの **Apps, Threats**（アプリケーションおよび脅威）を選択するか、**Objects**（オブジェクト）> **Applications**（アプリケーション）を選択します）。 • **Revert** [戻す] – 対応するコンテンツリリースバージョンが以前にダウンロードされていて、同じバージョンを再インストールする場合は**Revert** [戻す] をクリックします。
ドキュメント	対応するバージョンのリリース ノートへのリンクが提供されます。
☒	以前にダウンロードしたコンテンツ リリース バージョンをファイアウォールから削除します。
アップロード	ファイアウォールがPalo Alto Networksアップデートサーバーにアクセスできない場合、Palo Alto Networksサポートサイトの動的更新のセクションから動的更新を手動でアップロードすることができます。コンピュータ

© 2019 Palo Alto Networks, Inc.

Dynamic Updates Options（動的更新オプション）	の意味
	にアップデートをダウンロードしたのちに、更新内容をファイアウォールへ**Upload** [アップロード] します。次に **Install From File**（ファイルからインストール）を選択し、ダウンロードしたファイルを選択します。
ファイルからインストール	更新ファイルをファイアウォールへ手動でアップロードしたのちに、このオプションを使用してファイルをインストールします。**Package Type** [パッケージタイプ] のドロップダウンリストからインストールする更新のタイプを選択し（**Application and Threats** [アプリケーションおよび脅威]、**Antivirus** [アンチウイルス]、または**WildFire**）、**OK**をクリック、インストールしたいファイルを選択し、再度**OK**をクリックしインストールを開始します。

© 2019 Palo Alto Networks, Inc.

Device > Licenses [デバイス > ライセンス]

すべてのファイアウォール モデルでライセンスをアクティベートするには、**Device**（デバイス）> **Licenses**（ライセンス）を選択します。Palo Alto Network からサブスクリプションを購入すると、1 つ以上のライセンス キーを有効にするための認証コードが送信されます。

VM-Series ファイアウォールの場合、このページで仮想マシン (VM) を非アクティブにすることもできます。

以下のアクションは、Licenses (ライセンス) ページで実行できます。

- Retrieve license keys from license server（ライセンス サーバーからライセンス キーを取得）サポートポータルでアクティベート済みで、かつ認証コードを必要とする購入済みのサブスクリプションを有効化する場合に選択します。
- Activate feature using authorization code（認証コードを使用した機能のアクティベーション）サポートポータルでアクティベートされておらず、かつ認証コードを必要とする購入済みのサブスクリプションを有効化する場合に選択します。次に、認証コードを入力し、**OK**をクリックします。
- Manually upload license key（ライセンス キーの手動アップロード）:ファイアウォールがライセンス サーバーに接続されておらず、ライセンス キーを手動でアップロードする場合は、ライセンス キー ファイルを https://support.paloaltonetworks.com からダウンロードしてローカルに保存します。Manually upload license key（ライセンス キーの手動アップロード）をクリックし、Browse（参照）をクリックしてファイルを選択し、OK をクリックします。

  *URL*フィルタリングのライセンスを有効化する場合は、ライセンスをインストールし、データベースをダウンロードし、*Activate [アクティベート]* をクリックする必要があります。*URL*フィルタリングに*PAN-DB*を使用している場合、初期シードデータベースを*Download [ダウンロード]* してから *Activate [アクティベート]* をクリックする必要があります。

  *CLI*コマンド ***request url-filtering download paloaltonetworks < region name>*** を実行することもできます。
- **Deactivate VM** [VMのディアクティベート]:このオプションは、永久ライセンスおよび期間ベースのライセンスをサポートするBring Your Own Licenseモデルの VM-Seriesファイアウォールで使用できます。オンデマンドライセンスモデルでは、この機能はサポートされていません。VM-Seriesファイアウォールのインスタンスが必要なくなった場合、**Deactivate VM** [VMのディアクティベート] をクリックします。このオプションを使用すると、すべてのアクティブなライセンス（サブスクリプション ライセンス、VM キャパシティ ライセンス、およびサポート資格）を解放できます。ライセンスのクレジットはアカウントに戻るため、必要に応じて VM-Series ファイアウォールの新しいインスタンスにライセンスを適用できます。ライセンスがディアクティベートされると、VM-Seriesファイアウォールの機能が無効化され、ファイアウォールはライセンスのない状態になります。しかし、設定はそのまま保存されます。
  - VM-Series ファイアウォールがインターネットに直接アクセスできない場合、**Continue Manually**（手動で続行）をクリックします。ファイアウォールは、トークン ファイルを生成します。**Export license token** [ライセンストークンのエクスポート] をクリックし、トークンファイルをローカルコンピュータに保存して、ファイアウォールを再起動します。Palo Alto Networks Support ポータルにログインし、**Assets**（アセット）> **Devices**（デバイス）を選択し、**Deactivate VM**（**VM**のディアクティベート）をクリックして、このトークン ファイルを使用してディアクティベートのプロセスを完了します。
  - **Continue** [続行] をクリックして、VM-Seriesファイアウォールのライセンスをディアクティベートします。ライセンスの非アクティブ化プロセスを完了するには、**Reboot Now**[今すぐ再起動] をクリックします。
  - ディアクティベートを中止してDeactivate VM [VMのディアクティベート] ウィンドウを閉じる場合は**Cancel** [キャンセル] をクリックします。

© 2019 Palo Alto Networks, Inc.

- **Upgrade VM Capacity**（**VM** キャパシティのアップグレード）:このオプションでは、現在ライセンスのある VM-Series ファイアウォールのキャパシティをアップグレードできます。キャパシティをアップグレードしても、アップグレード前に VM-Series ファイアウォールで使用していたすべての設定とサブスクリプションは維持されます。
  - ファイアウォールがライセンス サーバーに接続できる場合は、**Authorization Code**（認証コード）を選択し、Authorization Code（認証コード）フィールドに認証コードを入力し、**Continue**（続行）をクリックして、キャパシティのアップグレードを開始します。
  - ファイアウォールがライセンス サーバーに接続できない場合は、**License Key**（ライセンス キー）を選択し、**Complete Manually**（手動で実行）をクリックしてトークン ファイルを生成し、トークン ファイルをローカル コンピュータに保存します。次にPalo Alto Networks Support ポータルにログインし、 **Assets (アセット)** > **Devices (デバイス)**を選択し、**Deactivate License(s) (ライセンスのディアクティベート)**をクリックして、トークン ファイルを使用します。VM-Series ファイアウォールのライセンス キーをローカル コンピュータにダウンロードし、ライセンス キーをファイアウォールに追加し、**Continue**（続行）をクリックしてキャパシティのアップグレードを完了します。
  - ファイアウォールがライセンス サーバーに接続でき、認証コードがない場合は、**Fetch from license server**（ライセンス サーバーから取得）を選択し、キャパシティのアップグレードを試みる前にライセンス サーバーでファイアウォールのキャパシティ ライセンスをアップグレードします。次に、ライセンス サーバーでライセンスがアップグレードされたことを確認した後、**Continue**（続行）をクリックしてキャパシティのアップグレードを開始します。

© 2019 Palo Alto Networks, Inc.

Device > Support [デバイス > サポート]

- Device > Support [デバイス > サポート]
- Panorama > Support [Panorama > サポート]

サポート関連のオプションを表示する場合は **Device**（デバイス）> **Support**（サポート）または **Panorama** > **Support**（サポート）を選択します。Palo Alto Networks の連絡先、サポートの有効期限、ファイアウォールのシリアル番号に基づいた Palo Alto Networks からの製品およびセキュリティ アラートを表示できます。

必要に応じて、このページで以下の機能を実行します。

- **Support**（サポート）– デバイスのサポート状態に関する情報と、認証コードを使用してサポートをアクティベーションするためのリンクを提供します。
- **Production Alerts/Application and Threat Alerts**（実働アラート/アプリケーションおよび脅威アラート）– これらのアラートは、このページにアクセスしたとき、またはページを更新したときに Palo Alto Networks 更新サーバーから取得されます。実働アラートの詳細、またはアプリケーションおよび脅威アラートの詳細を表示する場合はそのアラート名をクックします。実働アラートは、大規模なリコールが発生した場合またはそのリリースに関する緊急の問題が発生した場合に通知されます。アプリケーションおよび脅威アラートは、重大な脅威が検出されたときに通知されます。
- **Links**（リンク）– デバイスを管理しやすくしたり、サポート連絡先情報にアクセスしたりするための共通のサポート リンクを提供します。
- **Tech Support File**（テクニカル サポート ファイル）– **Generate Tech Support File**（テクニカル サポート ファイルの生成）をクリックして、ファイアウォールで発生している可能性のある問題のトラブルシューティングに対して、サポート チームが使用できるシステム ファイルを生成します。ファイルを生成したら、**Download Tech Support File**[テクニカルサポートファイルのダウンロード] をクリックしてファイルを取得し、そのファイルをPalo Alto Networksサポート部門に送信します。

  ブラウザがダウンロード後に自動的にファイルを開くよう設定している場合はその機能を無効化し、ブラウザでサポートファイルをダウンロードしても開封・抽出を行わないようにする必要があります。
- **Stats Dump File**（**Stats Dump** ファイル）（ファイアウォールのみ）– **Generate Stats Dump File**（**Stats Dump** ファイルの生成）をクリックして、過去 7 日間のネットワーク トラフィックを要約する一連の XML レポートを生成します。レポートが生成されたら、**Download Stats Dump File**[Stats Dumpファイルをダウンロード] することができます。Palo Alto Networks または認定パートナーのシステム エンジニアが、このレポートを使用してセキュリティ ライフサイクル レビュー(SLR) を生成します。SLR は、ネットワークで検出されたものとその関連ビジネスやセキュリティリスクを明らかにし、通常は評価プロセスの一部として使用されます。SLR の詳細は、Palo Alto Networks または認定パートナーのシステム エンジニアにお問い合わせください。
- **Core Files**（コア ファイル）– ファイアウォールでシステム プロセス エラーが発生した場合、プロセスとエラーの理由に関する詳細が記載されたコア ファイルが生成されます。**Download Core Files**（コア ファイルのダウンロード）リンクをクリックして使用可能なコア ファイルのリストを表示し、コア ファイル名をクリックしてダウンロードします。問題解決のサポートを受けるには、ファイルのダウンロード後に Palo Alto Networks サポート ケースにアップロードします。

  コア ファイルの内容は、*Palo Alto Networks* サポート エンジニアのみが解釈できます。

© 2019 Palo Alto Networks, Inc.

Device > Master Key and Diagnostics [デバイス > マスター キーおよび診断]

- **Device (デバイス) > Master Key and Diagnostics (マスター キーおよび診断)**
- **Panorama > Master Key and Diagnostics (マスター キーおよび診断)**

ファイアウォールまたは Panorama ですべてのパスワードと秘密鍵 (CLI にアクセスする管理者を認証するための RSA キーなど) を暗号化するマスター キーを編集します。パスワードとキーを暗号化すると、それらのプレーンテキスト値がファイアウォールまたは Panorama のどの場所にも表示されなくなるため、セキュリティが向上します。

デフォルトのマスター キーを復元するための唯一の方法は、工場出荷時設定へのリセットを実行することです。

デフォルト キーを使用する代わりに新しいマスター キーを設定し、安全な場所にキーを保管して定期的に変更することをお勧めします。プライバシーを強化するには、ハードウェア セキュリティ モジュールを使用してマスター キーを暗号化します (「Device (デバイス) > Setup (セットアップ) > HSM」を参照)。ファイアウォールまたは Panorama 管理サーバーごとに一意のマスター キーを設定した場合、攻撃者は 1 つのアプライアンスのマスター キーを取得しても、他のアプライアンスのパスワードと秘密鍵にアクセスできません。ただし、次の場合は、複数のアプライアンスで同じマスター キーを使用する必要があります。

- 高可用性 (**HA**) 設定 – ファイアウォールまたは Panorama を HA 設定でデプロイする場合、ファイアウォールまたは Panorama 管理サーバーのペアで同じマスター キーを使用します。同じマスター キーを使用しない場合、HA 同期が機能しません。
- **Panorama** からファイアウォールに設定をプッシュする – Panorama を使用して設定を管理対象対象ファイアウォールにプッシュする場合、Panorama と管理対象ファイアウォールで同じマスター キーを使用します。同じマスター キーを使用しない場合、Panorama からのプッシュ操作が失敗します。

マスター キーを設定するには、マスター キーの設定を編集し、以下の表に従って適切な値を入力します。

マスター キーおよび診断の設定	の意味
マスター キー	一意のマスターキーを設定する場合に有効化します。デフォルトのマスターキーを使用する場合は無効化 (クリア) します。
現在のマスター キー	ファイアウォールでのすべての秘密鍵とパスワードの暗号化で現在使用されている鍵を指定します。
新規マスター キー マスター鍵の確認	マスター キーを変更するには、16 文字の文字列を入力して新しいキーを確認します。
ライフ タイム	マスターキーが失効するまでの期間を**Days** (日数) および **Hours** (時間) で指定します。範囲は 1 〜 438,000 日 (50年間) です。 現在のキーが失効する前に新しいマスター キーを設定する必要があります。マスター キーが失効すると、ファイアウォールまたは *Panorama* は自動的にメンテナンス モードで再起動され

© 2019 Palo Alto Networks, Inc.

マスター キーおよび診断の設定	の意味
	ます。この場合、工場出荷時設定へのリセットを実行する必要があります。
リマインダーの時間	マスター キーが失効する前にファイアウォールで失効アラームを生成するまでの **Days**（日数）と **Hours**（時間）を入力します。ファイアウォールは System Alarms（システム アラーム）ダイアログを自動的に開いてアラームを表示します。 失効アラームを表示するには、*Device*（デバイス）> *Log Settings*（ログ設定）を選択し、*Alarm Settings*（アラーム設定）を編集して、*Enable Alarms*（アラームを有効化）します。
HSM に保管	ハードウェア セキュリティ モジュール（HSM）でマスター キーを暗号化する場合にのみ、このオプションを有効にします。DHCP クライアントや PPPoE などのダイナミック インターフェイスで HSM を使用することはできません。 HSM 設定は、HA モードのピア ファイアウォール間では同期されません。したがって、HA ペアの各ピアは異なる HSM ソースに接続できます。Panorama を使用していて両方のピアの設定の同期を維持する必要がある場合、Panorama テンプレートを使用して管理対象ファイアウォールの HSM ソースを設定します。 PA-220 は HSM をサポートしていません。
マスターキーの自動更新	指定した日数および時間数でマスターキーを自動更新する場合に有効化します。無効化（クリア）すると、設定したキーの寿命が過ぎたらマスターキーが失効するようになります。 マスター キーの暗号化を延長する **Days**（日数）と **Hours**（時間数）を指定（範囲は 1 時間 ~ 730 日）することで、**Auto Renew with Same Master Key** (同じマスターキーを自動更新)します。
共通基準	共通基準モードでは、別のオプションを使用して、暗号化アルゴリズム自己テストとソフトウェア整合性自己テストを実行できます。また、この 2 つの自己テストを実行する時刻を指定するためのスケジューラも用意されています。

マスターキーのデプロイ

管理対象のファイアウォール、ログコレクタ、WF-500 アプライアンスの既存のマスターキーを Panorama から直接更新あるいはデプロイします。

項目	の意味
マスターキーのデプロイ	
フィルタ	表示する管理対象デバイスをプラットフォーム、デバイスグループ、テンプレート、タグ、HA ステータス、ソフトウェアバージョンに基づいてフィルタリングします。

© 2019 Palo Alto Networks, Inc.

項目	の意味
デバイス名	管理対象ファイアウォールの名前です。
ソフトウェア バージョン	管理対象デバイスで実行されているソフトウェア バージョンです。
ステータス	管理対象デバイスの接続ステータス (Connected （接続済み）、Disconnected （未接続）、Unknown （不明）) です。
マスターキーのデプロイジョブのステータス	
デバイス名	管理対象ファイアウォールの名前です。
ステータス	マスターキーのデプロイジョブのステータスです。
result	マスターキーのデプロイジョブの結果です。OKあるいはFAIL （失敗）になります。
進捗	マスターキーのデプロイジョブの進捗状況 (%) です。
詳細:	マスターキーのデプロイジョブの詳細です。ジョブが失敗した場合、失敗した理由を示す詳細がここに表示されます。
概要	
進捗	マスターキーのデプロイジョブの進捗状況を示すプログレスバーを表示します。次の情報が表示されます： • **Results Succeeded** (成功した結果)—マスターキーを正常にデプロイできたデバイスの数です。 • **Results Pending** (保留中の結果)—マスターキーのデプロイジョブが現在保留されているデバイスの数です。 • **Results Failed** (失敗した結果)—マスターキーのデプロイジョブが失敗したデバイスの数です。

ユーザー ID

ユーザーID（User-ID™）は、アプリケーション アクティビティおよびポリシーを単純に IP アドレスと結び付ける代わりに、ユーザー名やユーザー グループに結び付け、LDAP等の様々な企業ディレクトリや端末サービスをシームレスに統合する、Palo Alto Networks® の次世代のファイアウォール機能です。User-ID を設定するとアプリケーション コマンド センター（ACC）、アプリケーション スコープ、レポート、およびログのすべてに、ユーザーの IP アドレスに加えユーザー名が含まれるようになります。

> Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]
> Device（デバイス）> User Identification（User-ID）> Connection Security（接続のセキュリティ）
> Device > User Identification > User-ID Agents [デバイス > User-ID > User-IDエージェント]
> Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (ターミナル サーバー エージェント)
> Device > User Identification > Group Mapping Settings [デバイス > User-ID > グループマッピングの設定]
> Device > User Identification > Captive Portal Settings [デバイス > User-ID > キャプティブ ポータルの設定]

その他の情報をお探しですか？

「User-ID」を参照してください。

Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

IP アドレスとユーザー名をマッピングするように、ファイアウォールで実行される PAN-OS 統合 User-ID エージェントを設定します。

確認すべき情報	以下を参照
PAN-OS 統合 User-ID エージェントを設定する。	Palo Alto Networks User-IDエージェントの設定
User-ID エージェントがユーザー マッピング情報用に監視するサーバーへのアクセスを管理する。	サーバーの監視
ファイアウォールが IP アドレスをユーザー名にマッピングする際に含める、あるいは除外するサブネットワークを管理する。	ユーザー マッピングのサブネットワークの許可または除外
その他の情報をお探しですか？	Configure User Mapping Using the PAN-OS IntegratedUser-IDAgent（PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定）。

Palo Alto Networks User-IDエージェントの設定

User-IDエージェントがユーザーマッピングを行う際に使用する方法は、ここでの設定内容に定義されます。

確認すべき情報	以下を参照
クライアントシステム、Windows Remote Management（WinRM）over HTTP あるいは HTTPS のプローブを行ってユーザーマッピング情報のためにサーバーを監視するために、Windows Management Instrumentation（WMI）を使用するよう User-ID エージェントを有効化します。	サーバー監視アカウント
「User-ID エージェントによるユーザー マッピング情報のサーバー ログを監視する」	サーバー モニタリング
ユーザーマッピング情報入手のため、User-IDエージェントがクライアントシステムのプローブを行えるように設定する方法	クライアントのプローブ

© 2019 Palo Alto Networks, Inc.

確認すべき情報	以下を参照
ユーザーがローミングして新しいIPアドレスを取得していても、ファイアウォールが最新のユーザーマッピング情報を保有しているように設定する方法	Cache
キャプティブポータルを通じてマッピングを行うユーザーに対し NT LAN Manager（NTLM）認証を有効化する方法	NTLM認証
ファイアウォールによるユーザーおよびグループのマッピング情報の共有を有効化し、User-IDの管理を簡略化する方法	再配信
ユーザーマッピング情報入手のため、User-IDエージェントがSyslogメッセージの構文解析を行うよう設定する方法	Syslog のフィルタ
マッピング処理から特定のユーザー名を除外するようにUser-IDエージェントを設定する方法	ユーザー リストを無視

サーバー監視アカウント

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **Server Monitor Account (サーバーモニターアカウント)**

クライアントシステム、Windows Remote Management（WinRM）over HTTP あるいは over HTTPS のプローブを行ってユーザーマッピング情報のためにサーバーを監視する際にWindows Management Instrumentation（WMI）を使用するよう PAN-OS 統合 User-ID エージェントを設定する場合は、以下のフィールドを入力します。

また、Windows Remote Management（WinRM）over HTTP あるいは over HTTPS を使用してサーバー監視を認証するよう Kerberos サーバーを設定することで、監視対象サーバーに対するアクセスの設定することもできます。

WMI プローブは、エンドポイントからレポートされたデータを信頼するため、セキュリティの高いネットワークではこの方法を使用して *User-ID* マッピング情報を取得しないことをお勧めします。*Active Directory*（*AD*）セキュリティ イベント ログまたは *Syslog* メッセージを解析するか、*XML API* を使用してマッピング情報を取得するように *User-ID* エージェントを設定する場合、*WMI* プローブを無効にすることをお勧めします。

WMI プローブを使用する場合、信頼されていない外部インターフェイスでは有効にしないでください。エージェントが、ネットワーク外で *User-ID* エージェント サービス アカウントのユーザー名、ドメイン名、パスワード ハッシュなどの機密情報を含む *WMI* プローブを送信してしまうことになります。攻撃者は、この情報を悪用してネットワークに侵入し、さらなるアクセス権を取得する可能性があります。

アクティブディレクトリ認証設定	の意味
ユーザー名	ファイアウォールがWindowsリソースへアクセスする際に使用する、アカウントのドメイン認証情報（**User Name**[ユーザー名] および**Password**[パスワード]）を入力します。アカウントがクライアントコンピュータに対し WMI クエリを行い、Microsoft Exchange サーバー

© 2019 Palo Alto Networks, Inc.

アクティブディレクトリ認証設定	の意味
	およびドメイン コントローラの監視を行う際には許可が必要となります。**User Name**[ユーザー名] にはdomain\usernameの構文を使用してください。サーバー認証で Kerberos を使用して監視対象サーバーに対するアクセスの設定を行う場合は、Kerberos のユーザープリンシパル名（UPN）を入力します。
ドメインの DNS 名	監視対象サーバーの DNS 名を入力します。サーバー認証で Kerberos を使用して監視対象サーバーに対するアクセスの設定を行う場合は、Kerberos のレルム ドメインを入力します。 監視対象サーバーに対するアクセスの設定の際に**WinRM-HTTP**を転送プロトコルとして使用している場合はこの設定を行う必要があります。
パスワード/再入力 パスワード	ファイアウォールが Windows リソースへアクセスする際に使用するアカウントのパスワードを入力して確認します。
Kerberosサーバ プロファイル	レルムへのアクセスを制御して WinRM over HTTP あるいは over HTTPS を使用する監視対象サーバーからセキュリティ ログおよびセッション情報を取得する Kerberos サーバー用の Kerberos サーバープロファイルを選択します。

PAN-OS 統合 User-ID エージェントに、サーバーの監視とクライアントのプローブを行わせるよう完全な手順 で設定する場合は、アクティブディレクトリ認証設定の定義の他に、いくつかの追加タスクを行う必要があります。

サーバー モニタリング

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID**エージェントの設定）> **Server Monitor**（サーバーモニタ）

User-ID エージェントがサーバーのセキュリティ イベント ログでログオン イベントを検索して IP アドレスをユーザー名にマッピングできるようにするには、以下の表の説明に従って設定を指定していきます。

*Windows Server*ログ、*Windows Server*セッション、または *eDirectory*サーバーでクエリの負荷が大きい場合は、クエリ間の遅延の観測値が、指定された頻度または間隔を大きく超える可能性があります。

PAN-OS 統合 User-ID エージェントに、サーバーの監視を行わせるよう完全な手順 で設定する場合は、サーバーの監視の設定の他に、いくつかの追加タスクを行う必要があります。

サーバー モニタリング設定	の意味
セキュリティ ログの有効化	Windowsサーバーに対するセキュリティログのモニタリングを有効化する場合はこのオプションを選択します。
サーバーログのモニター頻度（秒）	ファイアウォールが Windows サーバー セキュリティ ログに対しユーザー マッピング情報のクエリを行う頻度を秒単位で指定します（範囲は 1 ~ 3600、デフォルトは 2）。この値は、ファイアウォールが前回のクエリの処理を終了してからファイアウォールが次のクエリを送信するまでの間隔です。

© 2019 Palo Alto Networks, Inc.

サーバー モニタリング設定	の意味
	ログ監視の頻度が少なすぎる場合、最新の *IP* アドレス対ユーザーのマッピングを利用できる可能性があります。ファイアウォールがログを関する頻度が多すぎる場合、ドメイン コントローラ、メモリ、*CPU*、*User-ID* ポリシーの適用に影響を与えるおそれがあります。*2 ~ 30* 秒の範囲の値から始め、パフォーマンスに及ぼす影響、あるいはユーザーマッピングの更新頻度に基づいて値を調整します。
セッションの有効化	監視対象のサーバーにおけるユーザーセッションの監視を有効化する場合はこのオプションを選択してください。ユーザーがサーバーに接続するごとにセッションが作成されます。ファイアウォールはこの情報を使用してユーザーのIPアドレスを特定することができます。 *Enable Session*（セッションの有効化）は行わないでください。この設定では、すべてのユーザー セッションを読み取ることができるように *User-ID* エージェントにサーバー オペレータ権限のある *Active Directory* アカウントが必要です。代わりに、*Syslog* または *XML API* 統合を使用して、（*Windows* オペレーティング システムだけでなく）すべてのデバイス タイプとオペレーティング システムのログインおよびログアウト イベントをキャプチャするソース（ワイヤレス コントローラや *NAC* など）を監視する必要があります。
サーバー セッションの読み取り頻度（秒）	ファイアウォールがWindowsサーバーユーザーセッションに対しユーザーマッピング情報のクエリを行う頻度を秒単位で指定します（範囲は1 ~ 3600、デフォルトは10）。この値は、ファイアウォールが前回のクエリの処理を終了してから次のクエリを開始するまでの間隔です。
Novell eDirectoryクエリ間隔（秒）	ファイアウォールがNovell eDirectoryサーバーに対しユーザーマッピング情報のクエリを行う頻度を秒単位で指定します（範囲は1 ~ 3600、デフォルトは30）。この値は、ファイアウォールが前回のクエリの処理を終了してから次のクエリを開始するまでの間隔です。
Syslog サービス プロファイル	SSL/TLSサービスプロファイルを選択します。このプロファイルには、証明書および許可されているSSL/TLSバージョンが指定されており、User-IDサービスがモニターするファイアウォールと任意のSyslog Sender間の通信に使用されます。詳細は、「Device（デバイス）> Certificate Management（証明書の管理）> SSL/TLS Service Profile（SSL/TLS サービス プロファイル）」および「Syslog Filters（Syslog フィルタ）」を参照してください。**none**[なし] を選択した場合、ファイアウォールは、事前定義された自己署名証明書を使用します。

クライアントのプローブ

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **Client Probing**（クライアントによるプローブ）

© 2019 Palo Alto Networks, Inc.

ユーザー マッピング処理により識別されたそれぞれのクライアント システムに対し、User-ID エージェントが WMI クライアントによるプローブ を行うよう設定することができます。User-IDエージェントは、学習した各IPアドレスを定期的にプローブして、同じユーザーがまだログインしていることを確認します。ユーザー マッピングが存在しない IP アドレスがファイアウォールで発生すると、アドレスがエージェントに送信されてプローブが直ちに行われます。クライアントに対するプローブの設定を変更する場合は、以下のフィールドを編集してください。

セキュリティの高いネットワークでは、クライアントに対するプローブを有効にしないでください。外部の信頼できないインターフェイス上では、クライアントに対するプローブを有効にしないでください。クライアント プロービングは大量のネットワーク トラフィックを生成し、設定を誤るとセキュリティに対する脅威が生じるおそれがあり、またクライアント プロービングを外部の信頼できないゾーンで有効化すると、攻撃者がネットワーク外からプローブを送信することで、*User-ID* サービス アカウント エージェント サービスのアカウント名、ドメイン名、暗号化されたパスワードのハッシュが漏れる可能性があります。代わりに、分離性と信頼性の高いソース（ドメイン コントローラなど）から、*Syslog* や *XML API* との統合を介してユーザー マッピング情報を収集します。この方法には、（*Windows* クライアントだけでなく）すべてのデバイス タイプとオペレーティング システムから安全にユーザー マッピング情報をキャプチャできるという利点もあります。

PAN-OS 統合 *User-ID* エージェントに、クライアントへのプローブを行わせるよう完全な手順 で設定する場合は、クライアントに対するプローブの設定の他に、いくつかの追加タスクを行う必要があります。

NetBIOS プローブは *PAN-OS* 統合 *User-ID* エージェントではサポートされていませんが、Windows ベースの User-ID エージェント ではサポートされています。

クライアントに対するプローブ設定	の意味
プローブの有効化	WMI によるプローブを有効化する場合は、このオプションを選択します。
プローブ間隔（分）	プローブ間隔を分単位で入力します（範囲は1～1440、デフォルトは20）。この値は、ファイアウォールが前回のリクエストの処理を終了してから次のリクエストを開始するまでの間隔です。 大規模な導入環境では、ユーザーマッピング処理により識別された各クライアントをプローブするための時間を確保するため、間隔を適切に設定することが重要です。たとえば、ユーザーが6,000人で間隔が10分の場合は、各クライアントから1秒あたり10回のWMI要求が必要になります。 プローブ リクエストの負荷が大きい場合は、リクエスト間の遅延の観測値が、指定された間隔を大きく超える可能性があります。

Cache

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **NTLM**

ユーザーがローミングして新しい IP アドレスを取得していても、ファイアウォールが最新のユーザー マッピング情報を保有しているようにするため、ユーザー マッピングをファイアウォール キャッシュから削除するタイムアウトを設定します。このタイムアウトは、キャプティブ ポータル以外の方法で

© 2019 Palo Alto Networks, Inc.

学習したユーザー マッピングに適用されます。キャプティブ ポータルで学習したマッピングの場合は、キャプティブ ポータル設定（Device（デバイス）> User Identification（User-ID）> Captive Portal Settings（キャプティブ ポータルの設定）、**Timer**（タイマー）フィールドおよび**Idle Timer**（アイドル タイマー）フィールド）でタイムアウトを設定します。

ドメインが含まれていなくても User-ID ソースから収集したユーザー名を照合するには、ドメインなしで一致するユーザー名を許可するようにファイアウォールを設定します。組織内のユーザー名がドメイン間で重複していない場合にのみ、このオプションを使用してください。

キャッシュ設定	の意味
ユーザー ID タイムアウトを有効にする	ユーザーマッピングエントリに対してタイムアウト値を適用する場合はこのオプションを選択します。そのエントリのタイムアウト値に達した場合、ファイアウォールはそれを削除し、新しくマッピングを行います。これにより、ユーザーがローミングして新しいIPアドレスを取得していても、ファイアウォールには最新のユーザーマッピング情報が保管されるようになります。 このタイムアウトを有効化し、ファイアウォールが最新のユーザー対 *IP* アドレスのマッピングを必ず維持するようにしてください。
User-IDタイムアウト（分）	ユーザー マッピングエントリ用のタイムアウト値を分単位で入力します（範囲は 1 ~ 3,600、デフォルトは 45）。 タイムアウトの値を *DHCP* リースの存続期間の半分、あるいは *Kerberos* チケットの存続期間に設定します。 マッピング情報を再配信するようにファイアウォールを設定すると、各ファイアウォールでは、転送ファイアウォールで設定されているタイムアウトではなく、そのファイアウォールで設定されているタイムアウトに応じて、受信したマッピング エントリが削除されます。
ドメインなしで一致するユーザー名を許可する	ドメインが User-ID 送信元によって提供されない場合、ファイアウォールがユーザーを照合できるようにするには、このオプションを選択します。ユーザーの誤認を防ぐため、ドメイン間でユーザー名が重複していない場合にのみ、このオプションを選択してください。 このオプションを有効にする前に、ファイアウォールが *LDAP* サーバーからグループ マッピングを取得したことを確認します。

*NTLM*認証

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **NTLM**

Windows ユーザーのみを認証する場合、NT LAN Manager（NTLM）を使用できます。クライアント Web 要求が、認証実施オブジェクトによってブラウザ チャレンジが指定される認証ポリシー ルール（「Policies（ポリシー）> Authentication（認証）」を参照）に一致すると、NTLM チャレンジは透過的

© 2019 Palo Alto Networks, Inc.

にクライアントを認証します。その後、ファイアウォールはユーザーマッピング情報をNTLMドメインから収集します。

NTLM認証処理は1つのファイアウォールにつき1つの仮想システムのみにおいて有効化できます（**User Mapping**[ユーザーマッピング] ページの上部にある **Location**[場所] ドロップダウンリストから仮想システムを選択)。

また、必要に応じてファイアウォールをUser-IDエージェントとして他のファイアウォールに追加することで、追加したファイアウォールを使用して他のファイアウォールに対するNTLM認証処理を行うことができます。詳細は「User-ID エージェントへのアクセスの設定」を参照してください。

Windows ベースのユーザー ID エージェントを使用している場合は、エージェントがインストールされたドメイン コントローラに、NTLM 応答が直接転送されます。詳細は、Device（デバイス）> User Identification（User-ID）> Captive Portal Settings（キャプティブ ポータルの設定）の **NTLM Authentication**（**NTLM** 認証）フィールドを参照してください。

NTLM 認証ではなく、Kerberos シングル サインオンを使用するように認証ルールを設定してください。*Kerberos* の方が *NTLM* よりも強力かつ堅牢な認証方法です。また、ドメインに参加するための管理者アカウントがファイアウォールで必要とされません。認証ルールの認証方法に関する設定の詳細は、「Objects（オブジェクト）> Authentication（認証）」を参照してください。

キャプティブ ポータルの設定または Windows ベースの User-ID エージェントを完全な手順で設定する場合は、*NTLM* の有効化の他に、いくつかの追加タスクを行う必要があります。

NTLM 認証処理を設定するには、以下の表の説明に従って設定を指定していきます。

項目	の意味
NTLM 認証処理の有効化	NTLM認証処理を有効化する場合は、このオプションを選択します。
NTLM ドメイン	NTLMドメイン名を入力します。
Admin User Name（管理ユーザー名）（NTLM ドメイン用）	NTLMドメインへのアクセス権を持つ管理者アカウントを入力します。 *Admin User Name[管理ユーザー名]* フィールドにはドメインを含めないでください。含めた場合、ファイアウォールが、そのドメインを参加させることができなくなります。
パスワード/パスワード再入力（NTLM ドメイン用）	NTLMドメインへのアクセス権を持っている管理者アカウントのパスワードを入力します。

再配信

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **NTLM**

認証チャレンジに関連付けられたタイムスタンプとともにユーザー マッピング情報を再配信する User-ID エージェントとして機能するようにファイアウォールまたは仮想システムを設定するには、以下の表の説明に従って設定を指定していきます。のちに、マッピング情報とタイムスタンプを受信するアプライアンス（Panorama など）にこのファイアウォールを接続すると、アプライアンスはこれらのフィールドを使用して、ファイアウォールまたは仮想システムを User-ID エージェントとして識別します。

© 2019 Palo Alto Networks, Inc.

ユーザー マッピング情報と認証タイムスタンプを再配信するようにファイアウォールを完全な手順で設定する場合は、再配信設定の指定の他に、いくつかの追加タスクを行う必要があります。

デフォルトの場合、マルチ仮想システム ファイアウォールは、仮想システム間でユーザー マッピング情報を再配信しませんが、再配信するように設定することもできます。

再配信設定	の意味
コレクタ名	ファイアウォールまたは仮想システムを User-ID エージェントとして識別するコレクタ名（最大 255 文字の英数字）を入力します。
事前共有鍵/事前共有鍵の再入力	ファイアウォールまたは仮想システムを User-ID エージェントとして識別する事前共有鍵（最大 255 文字の英数字）を入力します。

Syslog のフィルタ

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **Syslog Filters**（**Syslogフィルタ**）

User-ID エージェントは、Syslog Parse プロファイルを使用して、エージェントが IP アドレスからユーザー名へのマッピング情報を監視する syslog 送信者から送信された syslog messages（Syslog メッセージ）をフィルタリングします（「Configure Access to Monitored Servers（監視対象サーバーに対するアクセスの設定）」を参照）。各プロファイルでは、次のイベント タイプのいずれかの Syslog メッセージを解析できますが、両方とも解析することはできません。

- 認証（ログイン）イベント –ユーザー マッピングをファイアウォールに追加するために使用します。
- ログアウト イベント – 現行でなくなったユーザー マッピングを削除するために使用します。IP アドレスの割り当てが頻繁に変わる環境では、期限切れのマッピングを削除すると便利です。

Palo Alto Networks では、アプリケーション コンテンツ更新を通じてファイアウォールに事前定義済み Syslog 解析プロファイルを提供しています。ベンダーが新しいフィルタを開発するたびにプロファイルのリストを動的に更新するには、これらの動的コンテンツ アップデートをスケジュールします（「Device（デバイス）> Dynamic Updates（動的更新）」を参照）。事前定義済みプロファイルはどのファイアウォールにでも適用できますが、設定したカスタム プロファイルは、**Device**（デバイス）> **User Identification**（ユーザー **ID**）> **User Mapping**（ユーザー マッピング）で選択した仮想システム（**Location**（場所））にのみ適用されます。

User-ID エージェントが Syslog メッセージを解析するには、Syslog メッセージが次の条件を満たしている必要があります。

- 各メッセージは 1 行の文字列であること。改行（\n）または復帰と改行（\r\n）が行区切りの区切り文字であること。
- 各メッセージの最大サイズは 2,048 バイトであること
- UDP 上で送信されたメッセージは 1 つのパケットに含まれること。SSL 上で送信されたメッセージは複数パケットにまたがることができる。1 つのパケットは複数のメッセージを含むことができる。

カスタム プロファイルを設定する場合は、**Add**（追加）をクリックし、次の表で説明する設定を指定します。この表のフィールドの説明では、次の形式になっている Syslog メッセージのログイン イベントの例を使用します。

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```


© 2019 Palo Alto Networks, Inc.

User-ID エージェントが *Syslog* 送信元のユーザー マッピング情報を解析するように設定する完全な手順 では、*Syslog* 解析プロファイルを作成する他にもさらにタスクが必要です。

項目	の意味
Syslog 解析プロファイル	プロファイルの名前を入力します（英数字最大63文字）。
の意味	プロファイルの説明を入力します (英数字最大255文字)。
タイプ	ユーザー マッピング情報をフィルタリングする解析のタイプを指定します。 • **Regex Identifier**（正規表現識別子）– Syslog メッセージからユーザー マッピング情報の特定と抽出を行うための検索パターンを示す正規表現（regex）を設定する場合は、**Event Regex**（イベント正規表現）、**Username Regex**（ユーザー名正規表現）、および **Address Regex**（アドレス正規表現）を指定します。ファイアウォールは Syslog メッセージ内の認証イベントまたはログアウト イベントを照合し、一致するメッセージ内のユーザー名と IP アドレスを照合する際に正規表現を使用します。 • **Field Identifier**（フィールド識別子）– 認証イベントまたはログアウト イベントで照合を行う文字列を指定し、Syslog メッセージでユーザー マッピング情報を識別する場合は、**Event String**（イベント文字列）、**Username Prefix**（ユーザー名プレフィックス）、**Username Delimiter**（ユーザー名区切り文字）、**Address Prefix**（アドレス プレフィックス）、および **Address Delimiter**（アドレス区切り文字）のフィールドを使用します。 ダイアログの残りのフィールドは、選択内容に従って変わります。次の行の説明に従ってフィールドを設定してください。
イベントの正規表現	成功した認証イベントまたはログアウト イベントを示す正規表現を入力します。この表で使用するメッセージ例の場合、正規表現 **`(authentication\ success)`** によって、文字列 `authentication success` の最初の **`{1}`** インスタンスが抽出されます。スペースの前の円記号は、スペースを特殊文字として扱わないように正規表現エンジンに指示する標準の正規表現エスケープ文字です。
ユーザー名の正規表現	認証成功またはログアウトのメッセージのユーザー名フィールドを識別する正規表現を入力します。この表で使用するメッセージ例の場合、正規表現 **`User:([a-zA-Z0-9\\\._]+)`** は文字列 `User:johndoe_4` に一致し、acme\johndoe1 をユーザー名として抽出します。
アドレスの正規表現	認証成功またはログアウトのメッセージの IP アドレス部分を識別する正規表現を入力します。この表で使用するメッセージ例では、正規表現 **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** は IPv4 アドレス `Source:192.168.0.212` と一致し、192.168.0.212 が IP アドレスとしてユーザー名マッピングに追加されます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
イベントの文字列	認証成功またはログアウトのメッセージを識別するために照合する文字列を入力します。この表で使用するメッセージ例の場合は、文字列 **`authentication success`** を入力します。
ユーザー名のプレフィックス	認証またはログアウトの Syslog メッセージにおいて、ユーザー名フィールドの先頭を識別するために照合する文字列を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。この表で使用するメッセージ例では、`User:` によってユーザー名フィールドの先頭を識別しています。
ユーザー名の区切り文字	認証またはログアウトのメッセージ内のユーザー名フィールドの終了を示すユーザー名の区切り文字を入力します。1 つのスペースを示すには \s（メッセージ例を参照）、タブを示すには \t を使用します。
アドレス プレフィックス	Syslog メッセージで IP アドレス フィールドの先頭を識別するために照合する文字列を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。この表で使用するメッセージ例では、`Source:` によってアドレス フィールドの先頭を識別しています。
アドレスの区切り文字	認証成功またはログアウトのメッセージにおける IP アドレス フィールドの末尾を示すために使用される照合文字列を入力します。たとえば、区切り文字が行区切りであることを示すには、\n を入力します。

ユーザー リストを無視

- **Device**（デバイス）> **User Identification**（**User-ID**）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-IDエージェントの設定**）> **Ignore User List**（ユーザー リストを無視）

除外ユーザー リストでは IP アドレスとユーザーネームのマッピングが不要なアカウントを定義します（キオスク アカウントなど）。リストの設定を行う場合は**Add**[追加] をクリックしてユーザー名を記入します。アスタリスクをワイルドカード文字として使用しte複数のユーザーネームと一致させることが可能ですが、エントリの最後の文字としてのみ使用できます。たとえば、**corpdomain\it-admin*** は **corpdomain** のドメイン内で it-admin から始まるユーザー名をもつすべての管理者と一致します。ユーザーマッピングから除外するエントリを最大5,000個まで追加することができます。

クライアントではなく、ユーザー *ID* エージェントであるファイアウォールの無視ユーザーリストを定義します。クライアントファイアウォールで無視ユーザーリストを定義した場合、リスト内のユーザーは再配布中にマッピングされます。

サーバーの監視

- Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

Microsoft Exchangeサーバー、Active Directory（AD）ドメインコントローラ、Novell eDirectoryサーバー、またはUser-IDエージェントがログインイベントの監視を行っているSyslog送信元などの定義を行う場合は、サーバーモニタリングセクションを使用します。

- 監視対象サーバーに対するアクセスの設定
- 監視対象サーバーに対するアクセスの管理
- ユーザー マッピングのサブネットワークの許可または除外

© 2019 Palo Alto Networks, Inc.

監視対象サーバーに対するアクセスの設定

Server Monitoring（サーバー モニタリング）セクションを使用して、ファイアウォールの監視対象のサーバーを指定するサーバー プロファイルを **Add**（追加）します。

User-ID を監視するサーバーを *2* つ以上設定し、サーバーがダウンしてもファイアウォールが *IP* アドレス対ユーザー名のマッピングを学習できるようにします。

サーバーを監視するように *PAN-OS* 統合 *User-ID* エージェントを完全な手順で設定するには、サーバー プロファイルの作成以外にいくつかの追加タスクを行う必要があります。

サーバー モニタリング設定	の意味
氏名	サーバーの名前を入力します。
の意味	サーバーの説明を入力します。
enabled [有効化]	このサーバーに対するログのモニタリングを有効化する場合はこのオプションを選択します。
タイプ	サーバータイプを選択します。選択内容により、このダイアログに表示されるフィールドが変わります。 • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Syslog Sender**
転送プロトコル（Microsoft アクティブディレクトリおよび Microsoft Exchange のみ）	転送プロトコルを選択します： • **WMI**—（デフォルト）Windows Management Instrumentation（WMI）を使用し、学習した各 IP アドレスを探査して同じユーザーがまだログイン中であることを検証します。 • **Win-RM-HTTP**—Windows Remote Management (WinRM) over HTTP を使用し、サーバー上のセッション情報とセキュリティ ログを監視します。このオプションではサーバー監視アカウント内の Kerberos **Domain's DNS Name (**ドメインの **DNS** 名**)**が必要になります。 • **Win-RM-HTTPS**—Windows Remote Management (WinRM) over HTTPS を使用し、サーバー上のセッション情報とセキュリティ ログを監視します。Kerberos 認証を使用する際に Windows Server でサーバー証明書の検証を求める場合は、必ずグローバル サービス設定で NTP を設定し、証明書プロファイルとして ルート CA を選択（Device (デバイス) > User Identification (ユーザー ID) > Connection Security (接続のセキュリティ)）してください。
ネットワーク アドレス	監視対象サーバーのサーバー IP アドレスまたは FQDN を入力してください。サーバー認証で Kerberos を使用する場合、FQDN を入力する必要があります。このオプションは、**Type**（タイプ）が **Novell eDirectory** の場合にはサポートされていません。
サーバ プロファイル	Novell eDirectory サーバーに接続するための LDAP サーバー プロファイルを選択します（Device（デバイス） > Server Profiles（サーバー プロファイル） > LDAP）。

© 2019 Palo Alto Networks, Inc.

サーバー モニタリング設定	の意味
（Novell eDirectory のみ）	
接続タイプ （Syslog 送信元のみ）	User-ID エージェントが **UDP** ポート（514）と **SSL** ポート（6514）のどちらで Syslog メッセージをリッスンするかを選択します。**SSL** を選択した場合、Enable Server Monitoring（サーバー モニタリングの有効化）で選択した **Syslog Service Profile**（**Syslog** サービス プロファイル）により、Syslog 送信元との接続保護のために許可される SSL/TLS バージョンと、ファイアウォールが使用する証明書が決まります。 *PAN-OS 統合 User-ID エージェントを使用して IP アドレスからユーザー名へのマッピングを行う場合は、セキュリティのために SSL を選択することをお勧めします。UDP を選択する場合、Syslog 送信元とクライアントの両方が保護された専用のネットワーク上にあることを確認し、信頼されていないホストから UDP トラフィックをファイアウォールに送信できないようにしてください。*
フィルタ （Syslog 送信元のみ）	サーバー **Type**（タイプ）が **Syslog Sender**（**Syslog** 送信元）の場合、このサーバーから受信した Syslog メッセージからユーザー名および IP アドレスを抽出する際に使用する Syslog 解析プロファイルを **Add**（追加）します。カスタム プロファイル（「Syslog フィルタの管理」を参照）または事前定義済みプロファイルを追加できます。プロファイルごとに、以下のように **Event Type**（イベント タイプ）を設定します。 • **login**（ログイン）– User-ID エージェントはログイン イベントの Syslog メッセージを解析し、ユーザー マッピングを作成します。 • **logout**（ログアウト）– User-ID エージェントはログアウト イベントの Syslog メッセージを解析し、現行でなくなったユーザー マッピングを削除します。IP アドレスが動的に割り当てられるネットワークでは、自動削除によって、エージェントが各 IP アドレスを現在関連付けられているユーザーに対してのみマッピングするようになるため、ユーザー マッピングの精度が向上します。 *事前定義済みの Syslog 解析プロファイルを追加する場合、名前を確認して、ログインとログアウト イベントのどちらへの一致を意図されているのか判断してください。*
デフォルト ドメイン名 （Syslog 送信元のみ）	（任意）サーバーの **Type**（タイプ）が **Syslog Sender**（**Syslog** 送信者）である場合は、ドメイン名を入力して、現在のドメイン名を Syslog メッセージのユーザー名に上書きするか、Syslog メッセージにドメインが含まれていない場合はユーザー名に追加します。

監視対象サーバーに対するアクセスの管理

User-IDエージェントがユーザーマッピング情報の監視を行っているサーバーへのアクセスを制御する場合はサーバーモニタリングセクションで以下のタスクを行ってください。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
ライセンス情報の表示	それぞれの監視対象のサーバーにおいて、User Mapping (ユーザーマッピング) ページではUser-IDエージェントからサーバーへの接続状況が表示されます。サーバーを**Add**[追加] するとファイアウォールは接続を試みます。接続試行が成功すると、サーバー モニタリング セクションの Status (状態) 列には Connected (接続済み) と表示されます。ファイアウォールから接続できなかった場合、Status (状態列) には `Connection refused` （接続が拒否されました）や `Connection timeout` （接続タイムアウト）などのエラー状態が表示されます。 サーバー モニタリング セクションの他のフィールドの表示内容の詳細は、「監視対象サーバーに対するアクセスの設定」を参照してください。
コンテキストの	監視対象サーバーへのアクセスを設定する場合は、User-ID エージェントにマッピング情報を監視させるサーバーをそれぞれ **Add** (追加) します。
削除します。	ユーザーマッピング処理 (検出) からサーバーを削除したい場合は、そのサーバーを選択し、**Delete**[削除] します。 ヒント：設定内容を消去せずに「検出」からサーバーを削除する場合は、サーバーエントリの編集を行い、**Enabled**[有効化] の選択を解除します。
知っておくべき最も重要な十ヶ条を	Microsoft Active Directoryドメインコントローラは、DNSを使用して自動的に**Discover**[検出] することができます。ファイアウォールは、**Device** (デバイス) > **Setup** (セットアップ) > **Management** (管理) のページにある **General Settings** (一般設定) セクションの **Domain** (ドメイン) フィールドに入力したドメイン名に基づいてドメイン コントローラを検出します。ファイアウォールはドメインコントローラを検出するとサーバーモニタリングリストにエントリを作成するので、それを使用してサーバーを監視対象に追加することができます。 *Discover[検出]* 機能はドメインコントローラのみに使用できます。*Exchange*サーバーや*eDirectory*サーバーには使用できません。

ユーザー マッピングのサブネットワークの許可または除外

- Device > User Identification > User Mapping [デバイス > User-ID > ユーザーマッピング]

IPアドレスからユーザー名へのマッピング (検出) を行う際にUser-IDエージェントが許可/除外するサブネットワークを定義する場合は、「許可/除外ネットワーク」リストを使用します。デフォルト設定において、このリストにサブネットワークを追加していない場合、パブリック IPv4 アドレスをもつクライアント システムで WMI プローブを行う場合を除き、User-ID エージェントはすべてのサブネットワークを対象として User-ID の送信元の検出を試行します。 (パブリック IPv4 アドレスは RFC 1918 および RFC 3927 の範囲外にあるものを指します)

パブリックIPv4アドレスにおけるWMIプローブを有効化する場合は、これらのサブネットワークをリストに追加し、**Discovery**[検出] オプションを**Include**[許可] に設定する必要があります。他のファイアウォールにユーザー マッピング情報を再配信する ようにファイアウォールを構成すると、リストで指定した検出制限が再配信される情報に適用されます。

含有および除外リストを使用し、ファイアウォールがユーザーマッピングを使用するサブネットを定義します。

許可/除外ネットワークリストでは以下のタスクを行うことができます。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
コンテキストの	検出を特定のサブネットワークに制限したい場合は、サブネットワークプロファイルを**Add**[追加] し、以下のフィールドを入力します。 • **Name**[名前] — サブネットワークの識別に使用する名前を入力します。 • **Enabled**[有効] — サーバー監視の際のサブネットワークの許可や除外を有効化する場合はこのオプションを選択します。 • **Discovery**[検出] — User-IDエージェントがサブネットワークを**Include**[許可] するか**Exclude**[除外] するかを選択します。 • **Network Address**[ネットワークアドレス] — サブネットワークのIPアドレスの範囲を入力します。 ユーザー ID エージェントは、すべてを除外という暗黙のルールをリストに適用します。たとえば、**Include**（許可）オプションを指定してサブネットワーク 10.0.0.0/8 を追加すると、User-ID エージェントは、その他すべてのサブネットワークがリストに追加されていない場合もこれらを除外します。**Exclude**[除外] オプションを指定してエントリを追加するのは、明示的に包含したサブネットワークの一部を除外する場合だけです。たとえば、**Include**[包含] オプションを指定して 10.0.0.0/8 を、**Exclude**[除外] オプションを指定して 10.2.50.0/22 を追加すると、ユーザー ID エージェントは、10.0.0.0/8 内のサブネットワークのうち 10.2.50.0/22 を除くすべてを検出し、10.0.0.0/8 外のすべてのサブネットワークを除外します。**Include**[許可] プロファイルを一切追加せずに **Exclude**[除外] プロファイルを追加すると、User-IDエージェントは、追加したサブネットワークだけでなく、すべてのサブネットワークを除外します。
削除します。	リストからサブネットワークを削除する場合は、それを選択して**Delete**[削除] します。 ヒント：設定内容を消去せずに「許可/除外ネットワークリスト」からサブネットワークを削除する場合は、サブネットワークプロファイルの編集を行い、**Enabled**[有効化] の選択を解除します。
カスタム許可/除外ネットワーク	デフォルトでは、ユーザーIDエージェントは、追加された順（上から下）にサブネットワークを評価します。評価順を変更するには、**Custom Include/Exclude Network Sequence**[許可/除外ネットワーク カスタム シーケンス] をクリックします。次に、サブネットワークに対して**Add**[追加]、**Delete**[削除]、**Move Up**[上へ]、**Move Down**[下へ] の各コマンドを実行して、カスタムの評価順を作成します。

© 2019 Palo Alto Networks, Inc.

Device（デバイス）> User Identification（User-ID）> Connection Security（接続のセキュリティ）

User-ID 接続セキュリティ設定の編集（ ）で、ファイアウォールが使用する証明書プロファイルを選択し、Windows User-ID エージェントによって提供された証明書を検証します。ファイアウォールは、選択した証明書プロファイルを使用して User-ID エージェントの ID を検証します。これは、エージェントによって提供されたサーバー証明書を検証することで実現します。

タスク	の意味
User-ID 証明書プロファイル	ドロップダウンから、Windows User-ID エージェントを認証するときに使用する証明書プロファイルを選択するか、New Certificate Profile（新規証明書プロファイル）を選択して新しい証明書プロファイルを作成します。**None**（なし）を選択すると、証明書プロファイルが削除されて、代わりにデフォルトの認証が使用されます。 サーバー認証で Kerberos を使用する際に Windows Server でサーバー証明書の検証を求める監視対象サーバーに対するアクセスの設定場合は、必ずグローバル サービス設定で NTP を設定し、証明書プロファイルとして ルート CA を選択してください。
Remove All（すべて削除）（テンプレート設定のみ）	選択したテンプレートの User-ID 接続セキュリティ設定に割り当てられた証明書プロファイルを削除します。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > User-ID Agents [デバイス > User-ID > User-IDエージェント]

ユーザー名を IP アドレスにマッピングするために User-ID エージェントはさまざまなソース (ディレクトリ サーバーなど) を監視します。エージェントは、ユーザー マッピングをファイアウォール、ログ コレクタ、Panorama に送信します。その後、これらの各アプライアンスは、マッピングを他のファイアウォール、ログ コレクタ、Panorama に転送する再配信ポイントとして機能します。ファイアウォール (**Device** (デバイス) > **User Identification** (**User-ID**) > **User-ID Agents** (**User-ID** エージェント)) または Panorama (**Panorama** > **User Identification** (**User-ID**)) でユーザー マッピングを収集するには、User-ID エージェントや再配信ポイントへの接続を設定する必要があります。

User-ID エージェントまたは再配信ポイントに接続するように専用ログ コレクタを設定するには、User-ID エージェント設定を定義します。*User-ID* エージェントまたは再配信ポイントに接続するようにローカル ログ コレクタを設定することはできません。

ユーザー マッピングを再配信するようにログ コレクタまたは *Panorama* を設定することはできますが、これらのデバイスでは *IP* アドレスをユーザー名にマッピングすることはできません。*Windows* ベースの *User-ID* エージェントと *PAN-OS* 統合 *User-ID* エージェントのみがユーザー マッピングを実行できます。

完全な手順でユーザー マッピングを設定する場合は、*User-ID* エージェントへの接続の設定の他に、いくつかの追加タスクを行う必要があります。

- User-ID エージェントへのアクセスの設定
- User-ID エージェントへのアクセスを管理

User-ID エージェントへのアクセスの設定

各ファイアウォールと Panorama 管理サーバーには、最大 100 個の User-ID エージェントまたは User-ID 再配信ポイント (あるいは両者の組み合わせ) を接続できます。接続を追加するには、**Add** (追加) をクリックし、以下のフィールドを設定します。

User-ID エージェント設定	の意味
氏名	User-ID エージェントまたは再配信ポイントに使用する分かりやすい名前 (最大 31 文字) を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 再配信ポイントとして機能するファイアウォールまたは仮想システムの場合、このフィールドは Collector Name (コレクタ名) フィールドと一致させる必要はありません。
次を使用してエージェントを追加	User-ID エージェントまたは再配信ポイントをファイアウォールが識別する方法を選択します。

© 2019 Palo Alto Networks, Inc.

User-ID エージェント設定	の意味
（ファイアウォールのみ）	• **Serial Number**（シリアル番号）– User-ID マッピングを再配信する Panorama 管理サーバーの場合はこのオプションを選択します。 • **Host and Port**（ホストとポート）– Windows ベースの User-ID エージェント、または User-ID マッピングを再配信するファイアウォール、仮想システム、ログ コレクタの場合はこのオプションを選択します。
シリアル番号（ファイアウォールのみ）	ユーザー マッピングをファイアウォールに再配信する Panorama 管理サーバーを選択します。高可用性（HA）デプロイの場合、アクティブな Panorama（**panorama**）またはパッシブな Panorama（**panorama2**）を選択できます。 ホスト、ポート、その他の接続情報については、ファイアウォールの初期設定時に定義しているため、指定する必要はありません。
ホスト	• **Windows** ベースの **User-ID** エージェント – User-ID エージェントがインストールされている Windows ホストの IP アドレスを入力します。 • ファイアウォール（PAN-OS 統合 User-ID エージェント）– ファイアウォールがユーザー マッピングの送信に使用する MGT インターフェイスまたはサービス ルートの IP アドレスを入力します。MGT インターフェイスの場合は IP アドレスの代わりにホスト名を入力できます。 • ユーザー マッピングを再配信するログ コレクタ – ログ コレクタがユーザー マッピングの送信に使用するインターフェイスのホスト名または IP アドレスを入力します。
ポート	User-ID エージェントが User-ID 要求をリッスンするポート番号を入力します。デフォルトは 5007 ですが、使用可能な任意のポートを指定できます。また、それぞれの User-ID エージェントで異なるポートを使用できます。 以前の一部のバージョンの *User-ID* エージェントでは、デフォルト ポートは *2010* です。
コレクタ名 コレクタの事前共有鍵/コレクタの事前共有鍵の再入力	ファイアウォールまたは仮想システムを User-ID エージェントとして識別する **Collector Name**（コレクタ名）および **Pre-Shared Key**（事前共有鍵）を入力します。ファイアウォールまたは仮想システムでユーザー マッピングを再配信するように設定したときと同じ値を入力します（「Redistribution（再配信）」を参照）。 これらのフィールドで参照するコレクタは *User-ID* エージェントであり、ログ コレクタではありません。また、エージェントがファイアウォールまたは仮想システムである場合にしかフィールドは設定できません。
LDAP プロキシとして使用 （ファイアウォールのみ）	この User-ID エージェントをディレクトリ サーバーを監視するプロキシとして使用し、ユーザー名のグループへのマッピングを行うには、このオプションを選択します。このオプションを使用する場合、ファイアウォールでグループ マッピングを設定する必要があります（Device（デバイス）> User Identification（User-ID）> Group Mapping Settings（グループ マッピング設定））。ファイアウォールはその設定を User-ID エージェントにプッシュして、ユーザー名のグループへのマッピングを実現します。 このオプションは、ファイアウォールがディレクトリサーバーに直接アクセスできないようなデプロイ環境で役立ちます。また、ディレクトリ サーバーで処理するクエリの数が減少することでメリットを享受できるようなデプロイ環境においても役立ちます。そ

© 2019 Palo Alto Networks, Inc.

User-ID エージェント設定	の意味
	れぞれのファイアウォールからサーバーへ直接クエリを送信する必要がなくなり、1 つの User-ID エージェントのキャッシュから、複数のファイアウォールでグループ マッピング情報を受信できるようになります。
NTLM 認証用に使用 （ファイアウォールのみ）	クライアント Web 要求が認証ポリシー ルールに一致する際に NT LAN Manager（NTLM）認証を行うプロキシとしてこの User-ID エージェントを使用する場合は、このオプションを選択します。User-ID エージェントはドメイン コントローラを監視してユーザー マッピング情報を探し、ファイアウォールに情報を転送します。また、このオプションを使用するには、User-ID エージェントで Enable NTLM Authentication（NTLM認証の有効化）を行う必要があります。 このオプションは、ファイアウォールがドメインコントローラに直接アクセスしNTLM認証を行えないようなデプロイ環境で役立ちます。また、ドメイン コントローラで処理する認証要求の数が減少することでメリットを享受できるようなデプロイ環境においても役立ちます。それぞれのファイアウォールからドメイン コントローラへ直接クエリを送信する必要がなくなり、1 つの User-ID エージェントのキャッシュから、複数のファイアウォールでユーザー マッピング情報を受信できるようになります。 *NTLM* 認証ではなく、Kerberos シングル サインオンを使用するように認証ルールを設定してください。*Kerberos* の方が *NTLM* よりも強力かつ堅牢な認証方法です。また、ドメインに参加するための管理者アカウントがファイアウォールで必要とされません。認証ルールの認証方法に関する設定の詳細は、「Objects（オブジェクト）> Authentication（認証）」を参照してください。
enabled [有効化]	ファイアウォールまたは Panorama が User-ID エージェントまたは再配信ポイントと通信できるようにするには、このオプションを選択します。
HIPレポート	このオプションを選択すれば、対象のファイアウォールが User-ID エージェント（GlobalProtect ゲートウェイ、分散ログ収集（DLC）、ファイアウォール、Panorama を含む）として構成されている他のファイアウォールから HIP レポートを受信できるようになります。その後、HIP ベースのポリシーを適用する際にファイアウォールが HIP レポート内のこの情報を使用できるようになります。

User-ID エージェントへのアクセスを管理

ファイアウォールから User-ID エージェントまたは再配信ポイントへの接続を管理する場合は、以下のタスクを実行してください。

タスク	の意味
情報を表示 / 接続対象の更新	**Device**（デバイス）> **User Identification**（**User-ID**）> **User-ID Agents**（**User-ID** エージェント）または **Panorama** > **User Identification**（**User-ID**）を選択し、ファイアウォールまたは Panorama が各 User-ID エージェントまたは再配信ポイントに接続されているかどうかを確認します。Connected [接続済み] 列に緑のアイコンが表示されている場合は正常に接続されていることを示し、黄色いアイコンの場合は接続が無効、赤いアイコンの場合は接続に失敗したことを意味します。初めて状態を参照してから接続状態が変化した可能性がある場合は、**Refresh Connected**（接続対象の更新）をクリックして表示を更新します。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	表示されるその他のフィールドについては、「User-ID エージェントへのアクセスの設定」を参照してください。
コンテキストの	**Add**（追加）してからConfigure Access to User-ID Agents（ユーザー ID エージェントへのアクセスを設定）します。
削除します。	ファイアウォールから User-ID エージェントまたは再配信ポイントへの接続を可能にしている設定内容を削除する場合は、そのエージェントまたは再配信ポイントを **Delete**（削除）します。 設定内容を消去せずに *User-ID* エージェントまたは再配信ポイントへの接続を無効化する場合は、編集を行い、*Enabled*（有効化）オプションの選択を解除します。
カスタム エージェント シーケンス	ファイアウォールに代わって User-ID エージェントによる NT LAN Manager（NTLM）認証 を有効化すると、デフォルト設定として、ファイアウォールはエージェントが追加された順（上から下）に通信を行います（「User-ID エージェントへのアクセスの設定」で **NTLM** 認証用に使用する方法を参照してください）。ファイアウォールがエージェントと通信する順序を変更するには、**Custom Agent Sequence**（カスタム エージェント シーケンス）をクリックして各エージェントを **Add**（追加）し、**Move Up**（上へ）または **Move Down**（下へ）でエージェントを並べ替え、**OK** をクリックします。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、ユーザー ID エージェント設定バンドルを **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export（設定バンドルのエクスポート）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Device (デバイス) > User Identification (ユーザーID) > Terminal Server Agents (ターミナル サーバー エージェント)

同じ IPアドレスを共有する複数のユーザーをサポートしているシステムでは、ターミナル サーバー (TS) エージェントはそれぞれのユーザーにポート レンジを割り当てることで各ユーザーを識別します。ファイアウォールがユーザーおよびユーザー グループに基づいたポリシーを適用できるよう、TS エージェントは、接続されているすべてのファイアウォールに対し、ユーザーに割り当てられたポート レンジを通知します。

すべてのファイアウォール モデルで最大 5,000 個のマルチユーザー システムからユーザー名とポートのマッピング情報を収集できます。ファイアウォールがマッピング情報を収集できる TS エージェントの数は、firewall model (ファイアウォール モデル) によって異なります。

*TS*エージェントへのアクセスを設定する前に、*TS*エージェントのインストールと設定を行う必要があります。ターミナル サーバー ユーザー用のユーザー マッピングを完全な手順で設定する場合は、*TS* エージェントへの接続の設定の他に、いくつかの追加タスクを行う必要があります。

TSエージェントへのアクセスを制御する場合は以下のタスクを実行します。

タスク	の意味
情報を表示 / 接続対象の更新	**Terminal Server Agents** (ターミナル サーバー エージェント) のページにおいて、Connected (接続済) 列にはファイアウォールから TSエージェントへの接続ステータスが表示されます。緑のアイコンが表示されている場合は正常に接続されていることを示し、黄色いアイコンの場合は接続が無効、赤いアイコンの場合は接続に失敗したことを意味します。ページを開いてから接続状態が変化した可能性がある場合は、**Refresh Connected** [接続対象の更新] をクリックして表示を更新します。
コンテキストの	TS エージェントへのアクセスを設定する場合は、エージェントを **Add** (追加) し、以下のフィールドを設定します。 • **Name** (名前) – TS エージェントの識別に使用する名前を入力します (最大31文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 • **Host** (ホスト) – TS エージェントがインストールされているターミナルサーバーの静的 IP アドレスあるいはホスト名を入力します。 • **Port** (ポート) – TS エージェント サービスがファイアウォールと通信する際に使用するポート番号を入力します (デフォルトは 5009)。 • **Alternative IP Addresses** (代替 **IP** アドレス) – TS エージェントがインストールされているターミナル サーバーに、送信トラフィックの送信元 IP アドレスとして表示される可能性がある IP アドレスが複数ある場合、最大 8 個の静的 IP アドレスあるいはホスト名を **Add** (追加) および入力します。 • **Enabled**[有効化] – ファイアウォールがこのTSエージェントと通信できるようにする場合は、このオプションを選択します。
削除します。	TSエージェントへの接続を可能にしている設定内容を削除する場合は、そのエージェントを選択し、**Delete**[削除] をクリックします。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	設定内容を消去せずに *TS* エージェントへの接続を無効化する場合は、エージェントの編集を行い *Enabled*（有効化）オプションの選択を解除します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、デバイス設定バンドルを **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export（設定バンドルのエクスポート）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Device (デバイス) > User Identification (ユーザー ID) > Group Mapping Settings (グループ マッピングの設定) タブ

- **Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループ マッピング設定）

ユーザーとユーザー グループに基づいてセキュリティ ポリシーやレポートを定義する場合は、ディレクトリ サーバーで指定および管理されるグループのリストと対応するメンバーのリストをファイアウォールで取得する必要があります。ファイアウォールは、Microsoft Active Directory（AD）、Novell eDirectory、Sun ONE Directory Server を含む、さまざまな LDAP ディレクトリ サーバーをサポートしています。

各ファイアウォールまたは Panorama がすべてのポリシーで参照できる個別ユーザー グループの数は model（モデル）によって異なります。しかし、モデルに関わらず、グループ マッピング設定を作成する前に LDAP サーバープロファイルを設定する必要があります（Device (デバイス) > Server Profiles (サーバープロファイル) > LDAP）。

ユーザー名をグループにマッピングする完全な手順では、グループ マッピング設定の作成の他に、いくつかの追加タスクを行う必要があります。

必要に応じて以下のフィールドを入力して**Add**（追加）し、グループ マッピング設定を作成します。グループ マッピング設定を削除する場合は、当該のものを選択して **Delete**（削除）します。グループ マッピング設定を削除せずに無効化したい場合は、設定の編集を行い **Enabled**（有効化）オプションの選択を解除します。

グループマッピング設定 – サーバープロファイル	設定場所	の意味
氏名	**Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループ マッピング設定）	グループマッピング情報の識別に使用する名前（最大31文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
サーバ プロファイル	**Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループ マッピング設定）> **Server Profile**（サーバー プロファイル）	このファイアウォールのグループ マッピングに使用する LDAP サーバー プロファイルを選択します。
更新間隔		ファイアウォール ポリシーが使用するグループの更新情報を取得するため、ファイアウォールが LDAP ディレクトリ サーバーと接続を行う間隔を秒数で指定します（範囲は 60 ~ 86,400 秒）。
ユーザー ドメイン		デフォルトでは、**User Domain** (ユーザー ドメイン)は空白になっています。空白のままにすると、ファイアウォールが、Active Directory サーバーのドメイン名を自動的に検出します。この

© 2019 Palo Alto Networks, Inc.

グループマッピング設定 – サーバープロファイル	設定場所	の意味
		フィールドに値を入力した場合、ファイアウォールがLDAPソースから取得したドメイン名はオーバーライドされます。入力値には NetBIOS 名を指定する必要があります。 このフィールドは、*LDAP* ソースから取得したユーザー名とグループ名のみに影響を与えます。ユーザー認証のユーザー名に関連付けられたドメインをオーバーライドするには、そのユーザーに割り当てる認証プロファイルの *User Domain*（ユーザー ドメイン）と *Username Modifier*（ユーザー名修飾子）を設定します（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。
Group Objects（グループ オブジェクト）		• **Search Filter**[検索フィルタ] – LDAPクエリを入力し、取得および追跡の対象とするグループを指定します。 • **Object Class**[オブジェクトクラス] – グループの定義を入力します。デフォルトはobjectClass=groupで、グループ**Search Filter**[検索フィルタ] に一致するディレクトに含まれ、かつobjectClass=groupが設定されているすべてのオブジェクトが取得されます。
User Objects		• **Search Filter**[検索フィルタ] – LDAPクエリを入力し、取得および追跡の対象とするユーザーを指定します。 • **Object Class**[オブジェクトクラス] – ユーザーオブジェクトの定義を入力します。たとえば、Active Directory の場合、objectClass は*user*になります。
enabled [有効化]		グループマッピングにおけるサーバープロファイルを有効化する場合はこのオプションを選択します。
管理対象デバイスのリストを取得		GlobalProtect デプロイメントの場合、このオプションを選択してファイアウォールがディレクトリ サーバー（アクティブディレクトリなど）からシリアル番号を取得できるようにします。そうすることで、GlobalProtect が接続中のエンドポイントのステータスを識別子、エンドポイントのシリアル番号の有無に基づいて HIP ベースのセキュリティ ポリシーを適用できるようになります。

© 2019 Palo Alto Networks, Inc.

グループマッピング設定 – サーバープロファイル	設定場所	の意味
User Attributes ユーザー属性	**Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループマッピングの設定）> **Custom Group**（カスタムグループ）	ユーザーを識別するためにディレクトリ属性を指定します。 • **Primary Username** (プライマリ ユーザー名)–User-ID のソースがユーザー名用に提供する属性を指定します（例えば**`userPrincipalName`**や**`sAMAccountName`**） プライマリ ユーザー名はファイアウォールが他の形式を *User-ID* のソースから取得する場合でも、ファイアウォールがログ、レポート、ポリシー設定でユーザーを識別する手段になります。形式を指定しない場合、ファイアウォールはデフォルトで アクティブディレクトリ には `sAMAccountName` 形式を使用し、*Novell eDirectory* および *Sun ONE Directory Server* には`uid`形式を使用します。 • **E-Mail** (メール)–User-ID のソースがメールアドレス用に提供する属性を指定します。デフォルトは **`mail`** です。 • **Alternate Username 1-3** (代替ユーザー名 **1 ~ 3**)–User-ID のソースが送信できるフォーマットに対応する追加の属性を最大 3 件指定します。 アクティブディレクトリ サーバーを設定する場合、代替ユーザー名 *1* はデフォルトで`userPrincipalName`です。
グループ属性		User-ID のソースがグループを識別するために使用する属性を指定します： • **Group Name** (グループ名)–User-ID のソースがグループ名属性用に使用する属性を指定します。アクティブディレクトリ のデフォルトは`name` で、Novell eDirectory または Sun ONE Directory Server のデフォルトは`cn`です。 • **Group Member** (グループメンバー)–User-ID のソースがグループメンバー用に使用する属性を指定します。デフォルトは `member` です。 • **E-Mail** (メール)–User-ID のソースがメールアドレス用に使用する属性を指定します。デフォルトは `mail` です。

© 2019 Palo Alto Networks, Inc.

グループマッピング設定 – サーバープロファイル	設定場所	の意味
使用可能なグループ 含まれたグループ	**Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループ マッピング設定）> **Group Include List**（許可リストのグループ化）	セキュリティルールの作成時にファイアウォールが表示するグループの数を制限する場合は、これらのフィールドを入力してください。LDAPツリーを探索して、ルールで使用するグループを見つけます。グループを含めるには、グループを選択して Available Groups (利用可能なグループ) リストに追加します（⊞）。グループをリストから削除するには、グループを Included Groups (含めるリスト) で選択して削除します（⊖）。 **Included Groups**（含まれたグループ）リストと **Custom Group**（カスタム グループ）リストの最大合計数は、グループ マッピング設定ごとに 640 エントリです。 ファイアウォールが *LDAP* ディレクトリツリー全体からでなく、必要なグループからのみユーザーグループ マッピングを取得できるよう、必要なグループだけを含めてください。
氏名 LDAP フィルタ	**Device**（デバイス）> **User Identification**（**User-ID**）> **Group Mapping Settings**（グループ マッピング設定）> **Custom Group**（カスタム グループ）	LDAP ディレクトリ内の既存のユーザー グループに一致しないユーザー属性に基づいてファイアウォール ポリシーを設定できるよう、LDAP フィルタに基づいてカスタム グループを作成します。 User-ID サービスは、フィルタに一致するすべての LDAP ディレクトリ ユーザーをカスタム グループにマッピングします。既存のアクティブディレクトリグループドメイン名と同じ識別名（DN）のカスタムグループを作成すると、ファイアウォールは、その名前が参照されるすべての場所（たとえば、ポリシーやログ内）でカスタムグループを使用します。カスタムグループを作成する場合は、以下のフィールドを設定して**Add** (追加)します。 • **Name**[名前] – 現在のファイアウォールまたは仮想システムにおけるグループマッピング設定の中で一意のカスタムグループ名を入力します。 • **LDAP Filter**[LDAPフィルタ] – 最大2,048文字のフィルタを入力します。 *LDAP* 検索を高速化して、*LDAP* ディレクトリ サーバーのパフォーマンスの低下を最小限に抑えるには、索引付きの属性のみをフィルタに使用します。*LDAP* フィルタ

© 2019 Palo Alto Networks, Inc.

グループマッピング設定 – サーバープロファイル	設定場所	の意味
		はファイアウォールで検証されません。 **Included Groups**（含まれたグループ）リストと **Custom Group**（カスタム グループ）リストの合計最大数は 640 エントリです。 カスタム グループを削除するには、グループを選択して **Delete**（削除）します。カスタム グループのコピーを作成する場合は、任意のグループを選択して **Clone**（コピー）してから、必要に応じフィールドを編集します。 カスタム グループを追加またはコピーしたら、変更を *Commit*（コミット）して、新しいカスタム グループをポリシーやオブジェクトで使用できるようにする必要があります。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > Captive Portal Settings [デバイス > User-ID > キャプティブ ポータルの設定]

トラフィックが認証ポリシー ルールに一致するユーザーをファイアウォールで認証するようにキャプティブ ポータル設定を編集 ( ) します。

キャプティブ ポータルで *SSL/TLS* サービス プロファイル (Device (デバイス) > Certificate Management (証明書の管理) > SSL/TLS Service Profile (SSL/TLS サービス プロファイル))、認証プロファイル (Device (デバイス) > Authentication Profile (認証プロファイル))、または証明書プロファイル (Device (デバイス) > Certificate Management (証明書の管理) > Certificate Profile (証明書プロファイル)) を使用する場合、開始前にプロファイルを設定します。キャプティブ ポータルを完全な手順で設定する場合は、これらのプロファイルの設定に加え、いくつかの追加タスクを行う必要があります。

認証ポリシーを適用するには、*Enable Captive Portal* (キャプティブ ポータルの有効化) を行う必要があります (「Policies (ポリシー) > Authentication (認証)」を参照)。

項目	の意味
キャプティブ ポータルの有効化	キャプティブ ポータルを有効化する場合は、このオプションを選択します。
アイドル タイマー (分)	キャプティブ ポータル セッション用のユーザー TTL (time-to-live) を分単位で入力します (範囲は 1 ~ 1,440、デフォルトは 15)。このタイマーは、キャプティブポータルユーザーのアクティビティが発生するたびにリセットされます。ユーザーのアイドル時間が **Idle Timer** (アイドル タイマー) の値を超えると、PAN-OS はキャプティブ ポータル ユーザー マッピングを削除するため、そのユーザーは再びログインを行う必要があります。
タイマー (分)	これは TTL の最大値を分単位で示すもので、キャプティブ ポータル セッションのマッピングが保持される最大の時間となります (範囲は 1 ~ 1,440、デフォルトは 60)。この時間が経過するとPAN-OSはマッピングを削除するので、セッションがまだアクティブな状態であっても、ユーザーは再度認証を行う必要があります。このタイマーは期限切れのマッピングをなくすためのものであり、**Idle Timer** (アイドル タイマー) の値をオーバーライドします。 失効 *Timer* (タイマー) は常に *Idle Timer* (アイドル タイマー) よりも長く設定してください。
SSL/TLS Service Profile	リダイレクト要求をセキュリティ保護するためのファイアウォール サーバー証明書と許可されたプロトコルを指定するには、SSL/TLS サービス プロファイルを選択します (Device (デバイス) > Certificate Management (証明書の管理) > SSL/TLS Service Profile (SSL/TLS サービス プロファイル))。**None** (なし) を選択した場合、ファイアウォールは SSL 接続にローカルのデフォルト証明書を使用します。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	SSL/TLS Service Profile (SSL/TLS サービス プロファイル) でMin Version (最低バージョン)をTLSv1.2に、Max Version (最大バージョン)をMax (最大)に設定し、SSL/TLS プロトコルの脆弱性を最大限に保護します。Max Version (最大バージョン)をMax (最大)に設定することで、より強固なプロトコルが利用できるようになり次第、ファイアウォールが必ず最新のバージョンを使用するようになります。 証明書エラーを表示せずに透過的にユーザーをリダイレクトするには、Web要求のリダイレクト先となるインターフェイスの IPアドレスと一致する証明書に関連付けられたプロファイルを割り当てる必要があります。
認証プロファイル	認証プロファイル（Device（デバイス）> Authentication Profile（認証プロファイル））を選択して、トラフィックが認証ポリシー ルール（Policies（ポリシー）> Authentication（認証））に一致する場合にユーザーを認証できます。ただし、Captive Portal Settings（キャプティブ ポータルの設定）で選択した認証プロファイルは、いずれかのデフォルトの認証実施オブジェクト（Objects（オブジェクト）> Authentication（認証））を参照するルールにのみ適用されます。初期状態ではすべての認証ルールがデフォルトのオブジェクトを参照しているため、これは一般的に PAN-OS 8.0 にアップグレードした直後が適しています。カスタム認証実施オブジェクトを参照するルールの場合、オブジェクトの作成時に認証プロファイルを選択します。
インバウンド認証プロンプト用の GlobalProtect ネットワーク ポート (UDP)	GlobalProtect™ が多要素認証（MFA）ゲートウェイからインバウンド認証プロンプトを受信するために使用するポートを指定します。(range is 1 to 65,536; default is 4,501).多要素認証をサポートするには、GlobalProtect エンドポイントは MFA ゲートウェイからのインバウンド UDP プロンプトを受信および承認する必要があります。GlobalProtect エンドポイントが指定のネットワーク ポートで、信頼できるファイアウォールまたはゲートウェイから UDP メッセージを受信すると、GlobalProtect は認証メッセージを表示します（「Customize the GlobalProtect Agent（GlobalProtect エージェントのカスタマイズ）」を参照）。
モード	認証時にファイアウォールが実行するWeb要求のキャプチャの方法を選択してください。 • **Transparent**（メッセージを表示しない）– ファイアウォールは認証ルールに沿って Web 要求をインターセプトして元の宛先 URL の偽装を行い、HTTP 401 を発行してユーザーに認証を求めるプロンプトを表示します。ただし、ファイアウォールには宛先 URL の実際の証明書がないため、保護されたサイトへのアクセスを試みるユーザーのブラウザには証明書エラーが表示されます。したがって、このモードはレイヤー 2 やバーチャル ワイヤーのデプロイメントなど、絶対に必要な場合にのみ使用してください。 • **Redirect**（リダイレクト）– ファイアウォールは認証ルールに沿って Web 要求をインターセプトして、指定したリダイレクト ホストにリダイレクトします。ファイアウォールは HTTP 302 リダイレクトを使用して、ユーザーに認証を求めるプロンプトを表示します。リダイレクトは優れたエンドユーザーエクスペリエンスを提供するため（**Redirect** (リダイレクト)はタイムアウトが失効した際にリマップしないため、証明書エラーを表示せず、ブラウジングをシームレスにするセッション Cookie を許可します）、**Redirect** (リダイレクト)を使用することがベストプラクティスになります。ただし、レイヤー 3 入力インターフェイスに割り当てられたインターフェイス管理プロファイルで応答ページを有効にする必要があります（詳細は「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> Interface Mgmt（インターフェイス管理）」および「PA-7000 シリーズのレイヤー 3 インターフェイス」を参照）。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	Redirect [リダイレクト] モードのもう1つの利点はセッションCookieを使用できることで、タイムアウトが発生するたびに再度マッピングすることなく、ユーザーが継続して認証済みサイトを閲覧することができます。ある IP アドレスから別の IP アドレス (企業 LAN から無線ネットワークなど) にローミングするユーザーは、セッションが開かれている限り IP アドレスが変化しても再認証する必要がないため、このモードが特に役立ちます。 *Redirect* (リダイレクト) モードは、キャプティブ ポータルで *Kerberos SSO* または *NTLM* 認証を使用する場合に必要です (ブラウザが信頼できるサイトにのみ認証情報を提供するため)。また、キャプティブ ポータルで多要素認証 (*MFA*) を使用する場合も *Redirect* (リダイレクト) モードが必要になります。
セッション Cookie (リダイレクトモードのみ)	• **Enable**[有効化] – セッションCookieを有効にする場合は、このオプションを選択します。 • **Timeout**[タイムアウト] – セッションCookieが**Enable**[有効化] されている場合、このタイマーで設定する値がCookieが有効な時間 (分) となります (範囲は60 ~ 10080、デフォルトは1,440)。 タイムアウトの値を十分短く設定し、ユーザーマッピングの項目が古くならず、かつ単一のセッション中にユーザーにログインを複数回求めないようにすることで優れたユーザーエクスペリエンスを提供できるだけの長さにします。*480* 分 (*8* 時間) 以下の値から始め、必要に応じて値を調整します。 • **Roaming** (ローミング) – セッションがアクティブな間に IP アドレスが変化しても Cookie を保持させたい場合 (エンドポイントが有線ネットワークから無線ネットワークに移動した場合など) は、このオプションを選択します。ユーザーは、Cookieがタイムアウトになった場合またはブラウザを閉じた場合に再認証を行う必要があります。
ホストのリダイレクト (リダイレクトモードのみ)	ファイアウォールがWeb要求をリダイレクトする宛先となるレイヤー3インターフェイスの、IPアドレスに解決されるイントラネットホスト名を指定します。 ユーザーが *Kerberos* シングル サインオン (*SSO*) で認証を行う場合、*Redirect Host* (ホストのリダイレクト) は、Kerberos キータブで指定したホスト名と同じにする必要があります。
証明書プロファイル	証明書プロファイル (Device (デバイス) > Certificate Management (証明書の管理) > Certificate Profile (証明書プロファイル)) を選択して、トラフィックが認証ポリシー ルール (Policies (ポリシー) > Authentication (認証)) に一致する場合にユーザーを認証できます。 この認証タイプの場合、キャプティブ ポータルはユーザーのエンドポイント ブラウザにクライアント証明書の提供を求めるプロンプトを表示します。そのため、クライアント証明書を各ユーザー システムにデプロイする必要があります。さらに、ファイアウォールにクライアント証明書を発行した認証局 (CA) 証明書をインストールして、CA 証明書を証明書プロファイルに割り当てる必要があります。これは、Mac OSおよび Linux エンドポイントで **Transparent** (メッセージを表示しない) 認証を有効にする唯一の認証方法です。

© 2019 Palo Alto Networks, Inc.

項目	の意味
NTLM認証	キャプティブ ポータルが NT LAN Manager（NTLM）認証 用に設定されている場合、ファイアウォールは暗号化されたチャレンジ レスポンス機構を使用して、ユーザーにプロンプトを表示せずにブラウザからユーザーの認証情報を透過的に取得します。 NTLM 認証を呼び出すには、認証ポリシー ルールで **Authentication Method**（認証方式）を **browser-challenge**（ブラウザ チャレンジ）または **default-browser-challenge**（デフォルト ブラウザ チャレンジ）に設定して、**Authentication Enforcement**（認証の実施）オブジェクトを指定する必要があります（Objects（オブジェクト）> Authentication（認証））。オブジェクトで Kerberos シングル サインオン（SSO）が有効になっている **Authentication Profile**（認証プロファイル）を指定した場合、ファイアウォールは NTLM に戻る前に Kerberos 認証を試行します。ブラウザが NTLM を実行できない場合、または NTLM 認証に失敗した場合、ファイアウォールの **Authentication Method**（認証方式）は **web-form**（**Web** フォーム）または **default-web-form**（デフォルト **Web** フォーム）にフォールバックします。 デフォルトでは、Internet ExplorerでNTLMがサポートされています。Firefox および Chrome で NTLM を使用するように設定できますが、NTLM を使用して Windows 以外のエンドポイントを認証することはできません。 キャプティブ ポータルを設定する場合、*NTLM* 認証よりも Kerberos SSO 認証（メッセージを表示しない）を優先してください。*Kerberos* は、*NTLM* よりも強力かつ堅牢な認証方式で、ファイアウォールに管理者アカウントがなくてもドメインに参加できます。 これらのオプションは*Windows*ベースの*User-ID*エージェントにのみ適用されます。*PAN-OS*統合*User-ID*エージェントを使用する場合にドメインに参加するには、ファイアウォールでドメインコントローラの*DNS*名を正常に解決できるようにする必要があります。その後、*PAN-OS* 統合 *User-ID* エージェント設定で NTLM Authentication（NTLM 認証を有効化する）ことで、ドメインへ参加するための認証情報をファイアウォールに提供することができます。*NTLM* は、*Windows Server* バージョン *2003* 以前でのみ使用できます。 Windows ベースの User-ID エージェントで NTLM を使用するように設定するには、以下を指定します。 • **Attempts**[試行回数] — NTLM認証を失敗とみなすまでの試行回数を指定します（範囲は1 ~ 60、デフォルトは1）。 • **Timeout**[タイムアウト] — NTLM認証がタイムアウトするまでの秒数を指定します（範囲は1 ~ 60、デフォルトは2）。 • **Reversion Time**（復帰時間）— エージェントが使用できなくなってから User-ID エージェント（**Device**（デバイス）> **User Identification**（**User-ID**）> **User-ID Agents**（**User-ID** エージェント））の最初に記載されているエージェントに対してファイアウォールが交信を再試行するまでの秒数を指定します（範囲は 60 ~ 3,600、デフォルトは 300）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect

GlobalProtect™ はモバイル ユーザーを管理する完全なインフラストラクチャを提供し、使用しているデバイスや場所にかかわらず、すべてのユーザーの安全なアクセスを可能にします。以下のファイアウォール Web インターフェイス ページでは、GlobalProtect の構成要素を設定および管理できます。

- Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータル]
- Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲートウェイ]
- Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]
- Network > GlobalProtect > Device Block List [ネットワーク > GlobalProtect > デバイスブロックリスト]
- Network (ネットワーク) > GlobalProtect > Clientless Apps (クライアントレス アプリケーション)
- Network (ネットワーク) > GlobalProtect > Clientless App Groups (クライアントレス アプリケーション グループ)
- Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オブジェクト]
- Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP プロファイル]
- Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]

その他の情報をお探しですか？

GlobalProtect インフラストラクチャのセットアップ詳細、ポリシーを適用するためのホスト情報の使用方法、一般的な GlobalProtect のデプロイの設定手順といった GlobalProtect の詳細は「GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)」を参照してください。

Network > GlobalProtect > Portals [ネットワーク > GlobalProtect > ポータル]

GlobalProtect™ ポータルのセットアップと管理を行うには、**Network**（ネットワーク）> **GlobalProtect** > **Portals**（ポータル）を選択します。このポータルは、GlobalProtect インフラストラクチャの管理機能を提供します。GlobalProtect ネットワークに参加するすべてのエンドポイントは、その設定をポータルから受信します。これには、使用可能なゲートウェイの情報や、アプリでゲートウェイへの接続に必要になるクライアント証明書に関する情報が含まれます。ポータルは更に、macOS および Windows エンドポイント用の GlobalProtect アプリ ソフトウェアの動作と配布を制御しています。Linux エンドポイントの場合、サポート サイトからソフトウェアを入手する必要があります。たとえば、モバイルデバイス用の GlobalProtect アプリケーションは、iOS デバイスの場合は Apple App Store を通じて配布され、Android デバイスの場合は Google Play を通じて配布され、Windows Phone および他の Windows UWP デバイスの場合は Microsoft ストアを通じて配布されます。また、Chromebook 用の GlobalProtect アプリケーションは、Chromebook Management Console または Google Play を通じて配布されます。

ポータル設定を追加するには、**Add**[追加] をクリックして GlobalProtect Portal [GlobalProtect ポータル] ダイアログを開きます。

確認すべき情報	以下を参照
GlobalProtectポータル用に設定する必要がある一般設定	GlobalProtect ポータルの General（全般）タブ
ポータル設定に認証プロファイルを割り当てる方法	GlobalProtect ポータルの Authentication (認証) タブ
GlobalProtect アプリケーションがエンドポイントから収集するデータをどうすれば定義できますか？	GlobalProtect ポータルの Portal Agent Data Collection（ポータル データ収集）タブ
設定可能なクライアント認証のオプション	GlobalProtect ポータルの Agent Authentication（エージェント認証）タブ
オペレーティングシステム、ユーザー、および（または）ユーザーグループを指定し、特定のデバイスグループに対して設定を割り当てる方法	GlobalProtect ポータルの Agent Config Selection Criteria（エージェント設定の選択条件）タブ
内部ゲートウェイの設定と優先順位を指定する方法	GlobalProtect ポータルの Agent Internal（エージェント内部）タブ
外部ゲートウェイの設定と優先順位を指定する方法	GlobalProtect ポータルの Agent External（エージェント外部）タブ
異なるタイプのユーザー用に個別のクライアント設定を作成する方法	GlobalProtect ポータルの Agent (エージェント) タブ
GlobalProtect アプリの表示設定と動作設定のうちカスタマイズ可能な項目	GlobalProtect ポータルの Agent App（エージェント アプリケーション）タブ

© 2019 Palo Alto Networks, Inc.

確認すべき情報	以下を参照
HIP データ収集オプションの設定方法	GlobalProtect ポータルの Agent HIP Data Collection (エージェント HIP データ収集) タブ
GlobalProtect アプリをインストールしなくても Web アプリケーションにアクセスできるように GlobalProtect ポータルを設定する方法	GlobalProtect ポータルの Clientless VPN (クライアントレス VPN) タブ
サテライトとして動作するファイアウォールまでVPN接続を延長する方法	GlobalProtect ポータルの Satellite (サテライト) タブ
その他の情報をお探しですか？	ポータルのセットアップ手順の詳細は、『*GlobalProtect Administrator's Guide* (*GlobalProtect* 管理者ガイド) 』の「Configure a GlobalProtect Portal (GlobalProtect ポータルの設定) 」を参照してください。

GlobalProtect ポータルの General (全般) タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Portals** (ポータル) > *<portal-config>* > **General** 全般)

General (全般)タブを選択し、GlobalProtect アプリケーションが GlobalProtect ポータルに接続するために使用するネットワーク設定を定義します。また、必要に応じてGlobalProtectの口グインページを無効化したり、カスタムポータル口グインやヘルプページを指定することができます。カスタム ページを作成およびインポートする方法の詳細は、『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド) 』の「Customize the Portal Login, Welcome, and Help Pages (ポータル ログイン ページ、ウェルカム ページ、ヘルプ ページのカスタマイズ) 」を参照してください。

GlobalProtect ポータルの設定	の意味
氏名	ポータルの名前を入力します (最大 31 文字) 。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場合、**Location**[場所] はGlobalProtectポータルを使用できる仮想システム (vsys) になります。マルチvsysモードに設定されていないファイアウォールの場合、**Location**[場所] は選択できません。ポータルを保存すると、その **Location**[場所] を変更できなくなります。
Network Settings [ネットワーク設定]	
インターフェイス	リモートク エンドポイントおよびファイアウォールからの通信の入り口となるファイアウォールインターフェイスの名前を選択します。 *Telnet*、*SSH*、*HTTP*、または *HTTPS* を許可するインターフェイス管理プロファイルを、*GlobalProtect* ポータルまたはゲートウェイを設定したインターフェイスに接続しないでください。これにより、管理インターフェイスがインターネットに公開されるためです。管理ネットワークへのアクセスを

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの設定	の意味
	保護する方法の詳細については、Best Practices for Securing Administrative Access（管理アクセスを保護するためのベストプラクティス）を参照してください。
IPアドレス	GlobalProtect ポータル Web サービスを実行する IP アドレスを指定します。**IP Address Type**（**IP** アドレス タイプ）を選択して、**IP Address**（**IP** アドレス）を入力します。 • IP アドレス タイプは、**IPv4**（IPv4 トラフィックの場合のみ）、**IPv6**（IPv6 トラフィックの場合のみ）、または **IPv4 and IPv6**（**IPv4** および **IPv6**）です。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。 • IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。 • **IPv4 and IPv6**（**IPv4** および **IPv6**）を選択した場合、それぞれのタイプに適切な IP アドレスを入力します。
Appearance [表示設定]	
ポータルのログイン ページ	（任意）ユーザーがポータルへのアクセスに使用する、カスタムログインページを選択します。**factory-default**[出荷時のデフォルト] ページを選択するか、カスタムページを**Import**[インポート] することができます。デフォルト設定は**None**[なし] です。このページに Web ブラウザからアクセスできないようにする場合、このページを **Disable**（無効化）します。
ポータルのランディング ページ	（任意）ポータルのカスタム ランディング ページを選択します。**factory-default**[出荷時のデフォルト] ページを選択するか、カスタムページを**Import**[インポート] することができます。デフォルト設定は**None**[なし] です。
アプリケーションのヘルプ ページ	（任意）GlobalProtectを使用するユーザーの補助を行うカスタムヘルプページを選択します。**factory-default**[出荷時のデフォルト] ページを選択するか、カスタムページを**Import**[インポート] することができます。出荷時のデフォルト ヘルプ ページは GlobalProtect アプリ ソフトウェアで提供されます。カスタム ヘルプ ページを選択する場合、GlobalProtect ポータルは GlobalProtect ポータル設定を含むヘルプ ページを提供します。デフォルトの **None**（なし）のままにすると、GlobalProtect アプリはページを表示せずにメニューからオプションを削除します。

GlobalProtect ポータルの Authentication (認証) タブ

- **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > *<portal-config>* > **Authentication (認証)**

Authentication (認証)タブを選択し、様々な GlobalProtect™ ポータルの設定を行います：

- ポータルおよびサーバーが認証に使用するSSL/TLSサービスプロファイルです。サービスプロファイルは認証のその他の設定から独立しています。

© 2019 Palo Alto Networks, Inc.

- 第一にユーザーエンドポイントのオペレーティングシステムに、次に任意で設定された認証プロファイルに基づく、固有の認証スキームです。
- （任意）GlobalProtectにおいて、ユーザー認証用に特定の証明書プロファイルを使用できるようにする**Certificate Profile**[証明書プロファイル] です。クライアントが提示する証明書は証明書プロファイルと一致している必要があります（セキュリティスキームの一部としてクライアントの証明書が設定されている場合）。

GlobalProtect ポータルの認証設定	の意味
Server Authentication [サーバー認証]	
SSL/TLS Service Profile	既存のSSL/TLSサービスプロファイルを選択します。このプロファイルでは、管理インターフェイスのトラフィックの安全を確保するために使用する証明書と、使用を許可するプロトコルを指定します。Common Name (CN)（共通名（CN））と、該当する場合はプロファイルに関連付けられている証明書のSubject Alternative Name (SAN)（サブジェクト代替名（SAN））フィールドが、IP アドレスまたは **General**（一般設定）タブで選択した **Interface**（インターフェイス）の FQDN と一致する必要があります。 *GlobalProtect の VPN 設定では、信頼できるサードパーティ CA の証明書または内部のエンタープライズ CA が生成した証明書に関連付けられているプロファイルを使用してください。*
Client Authentication [クライアントの認証]	
氏名	このクライアント認証設定を識別する名前を入力します。（クライアント認証設定は SSL/TLS サービスプロファイルからは独立しています） 複数のクライアント認証設定を作成し、主にオペレーティングシステム毎に違いを付け、さらに固有の認証プロファイル毎に分化させていくことが可能です（同じOSの場合）。例えば、それぞれのオペレーティングシステムごとにクライアント認証設定を追加し、更に同じOSの場合でも固有の認証プロファイルをもつものに対し、異なる設定を付加することが可能です。（これらのプロファイルは、一番細かいものから最も適用範囲が広いものの順に、手動で並べ替えを行う必要があります。）例えば、すべてのユーザーとすべてのOSという設定が最も適用範囲が広いものになります。 GlobalProtect が**pre-logon**（ログオン前）モード（ユーザーがシステムにログオンする前）のアプリに適用する設定、または任意のユーザーに適用する設定を作成することもできます。（Pre-logonでは、ユーザーがGlobalProtect に ログインする前に、GlobalProtectゲートウェイに向けたVPNトンネルを確立します）
OS	エンドポイントのオペレーティング システム（OS）固有のクライアント認証プロファイルを展開する場合は、OS (**Any (任意)**、**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows**、または**WindowsUWP**）を **Add** (追加)します。OSは設定同士を第一に区別するものです。（区別の詳細についてはAuthentication Profile [認証プロファイル]を参照してください） **Browser**[ブラウザ] および**Satellite**[サテライト] の追加オプションでは、特定のシナリオ用の認証プロファイルを指定することができます。GlobalProtect アプリ（Windows および Mac）をダウンロードするWeb ブラウザから、ポータルにアクセスするユーザーを認証する際に使用する認証プロファイルを指定する場合

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの認証設定	の意味
	は、 **Browser** (ブラウザ) を選択します。サテライト (LSVPN) の認証時に使用する認証プロファイルを指定する場合は**Satellite**[サテライト] を選択します。
認証プロファイル	OSによるクライアント認証設定の区別に加え、認証プロファイルを設定することで更に区分していくことが可能です。 (**New Authentication Profile**[新規認証プロファイル]を作成するか、既存のものを選択することができます。) 1つのOSに対し複数の認証オプションを設定したい場合は、複数のクライアント認証プロファイルを作成することができます。 *Gateways[ゲートウェイ] にLSVPNを設定する場合、ここで認証プロファイルを選択しない限り、その設定を保存することができません。また、サテライトの認証にシリアル番号を使用しようとしている場合、ファイアウォールのシリアル番号が見つからない場合や、検証が行えなかったときのために、ポータル認証プロファイルを設定しておく必要があります。* また、 Device > Authentication Profile [デバイス > 認証プロファイル]も参照してください。
Username Label ユーザー名のラベル	GlobalProtect ポータル ログイン用のカスタム ユーザー名ラベルを指定します。たとえば、ユーザー名 (のみ) 、またはメールアドレス**(username@domain)**。
パスワード ラベル	GlobalProtect ポータル ログイン用のカスタム ポータル ラベルを指定します。たとえば、パスワード (トルコ語) またはパスコード (2 重認証、トークンベース認証)
認証メッセージ	ログインに必要な認証情報のタイプをエンドユーザーに伝えるメッセージを入力するか、デフォルトのメッセージのままにしておいてください。メッセージの最大文字数は256文字です。
ユーザー認証情報あるいはクライアント証明書による認証を許可	**No** (いいえ)を選択すると、ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってゲートウェイに認証する必要があります。**Yes** (はい)を選択すると、ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証できるようになります。
証明書プロファイル	
証明書プロファイル	(任意) ユーザーのエンドポイントから受信するクライアント証明書を照合する際にポータルが使用する**Certificate Profile**[証明書プロファイル] 選択します。証明書プロファイルを使用すると、ユーザーはクライアントの証明書がこのプロファイルと一致する場合にのみ認証を行うことができます。 **Allow Authentication with User Credentials OR Client Certificate** (ユーザー認証情報あるいはクライアント証明書による認証を許可)オプションを**No** (いいえ)に設定する場合は**Certificate Profile** (証明書プロファイル)を選択する必要があります。**Allow Authentication with User Credentials OR Client Certificate** (ユーザー認証情報あるいはクライアント証明書による認証を許可)オプションを**Yes** (はい)に設定する場合、**Certificate Profile** (証明書プロファイル)は任意項目です。 証明書プロファイルはOSの種類に依存しません。またこのプロファイルは、認証プロファイルをオーバーライドし、暗号化された Cookie による認証を可能にす

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの認証設定	の意味
	る、Authentication Override（認証のオーバーライド）を有効にした場合もアクティブなままです。

GlobalProtect ポータルの Portal Agent Data Collection（ポータルデータ収集）タブ

Network (ネットワーク) > **GlobalProtect** > **Portals** (ポータル) > **<portal-config>** > **Portal Data Collection** (ポータル データ収集)を選択し、ユーザーがポータルに正常にログインした後に設定選択条件データ内で GlobalProtect アプリケーションがエンドポイントから収集して送信するデータを定義します。

GlobalProtect ポータルのデータ収集設定	の意味
証明書プロファイル	GlobalProtect アプリケーションが送信したマシン証明書にマッチさせるために GlobalProtect ポータルが使用する証明書プロファイルを選択します。
カスタム チェック	アプリで収集するカスタム ホスト情報を定義します。 • **Windows** — 特定のレジストリキーやキー値のチェックを**Add**[追加] します。 • **Mac** — 特定のplistやキー値のチェックを**Add** (追加) します。

GlobalProtect ポータルの Agent (エージェント) タブ

- **Network**（ネットワーク）> **GlobalProtect** > **Portals** > *<portal-config>* > **Agent**（エージェント）

Agent (エージェント)タブを選択してエージェント設定を定義します。GlobalProtectポータルは、まず接続が確立されてからデバイスへ設定を適用します。

ポータルは、信頼されたルート認証局（CA）証明書や中間証明書を自動的に適用するように設定することも可能です。GlobalProtectゲートウェイやGlobalProtectモバイルセキュリティマネージャーが使用しているサーバー証明書をエンドポイントが信頼しない場合、エンドポイントがゲートウェイやモバイルセキュリティマネージャーに向けたHTTPS接続を確立する際にこれらの証明書が必要になります。ポータルはここに指定した証明書を、クライアント設定と共にクライアントへプッシュします。

信頼できるルート認証局証明書を追加する場合は、既存の証明書を**Add**[追加] するか、新しく**Import**[インポート] してください。SSLフォワードプロキシの復号化に必要な信頼できるルート認証局証明書を（表示することなく）クライアントの証明書ストアにインストールする場合は、**Install in Local Root Certificate Store**[ローカルのルート証明書ストアにインストール] を選択します。

GlobalProtect アプリケーションが GlobalProtect ポータルおよびゲートウェイの身元を検証するために使用する、信頼できるルート CA 証明書を指定します。信頼できるルート CA を発行したのと同じ認証局によって署名されていない証明書をポータルあるいはゲートウェイが提示すると、GlobalProtect アプリケーションはそのポータルあるいはゲートウェイと接続を確立できません。

異なるタイプのユーザーごとに異なる設定が必要な場合は、それぞれに対して別個にエージェント設定を作成し、その設定をサポートすることができます。ポータルはその後、ユーザー名/グループ名やクライ

© 2019 Palo Alto Networks, Inc.

アントの OSにより、適用するエージェント設定を判別します。セキュリティルール評価によって、ポータルはリストの先頭から一致する項目を検索します。一致項目を発見すると、ポータルは対応する設定をアプリに配信します。そのため、複数のエージェント設定がある場合、設定を具体的なもの（つまり、特定のユーザーまたは特定のオペレーティングシステム用の設定）から汎用的なものへと並べることが重要です。設定の並び替えには、**Move Up**[上へ] および **Move Down**[下へ] を使用します。必要に応じて新しいエージェント設定を**Add**[追加] してください。ポータルの設定方法とエージェント設定の作成方法の詳細は、『GlobalProtect Administrator's Guide（GlobalProtect 管理者ガイド）』の「GlobalProtect Portals（GlobalProtect ポータル）」を参照してください。新しいエージェント設定を **Add**（追加）するか、既存の設定を変更した場合、**Configs**（設定）ウィンドウが開き、5 つのタブが表示されます。詳細を以下の表に記載します。

- GlobalProtect ポータルの Agent Authentication（エージェント認証）タブ
- GlobalProtect ポータルの Agent Config Selection Criteria（エージェント設定の選択条件）タブ
- GlobalProtect ポータルの Agent Internal（エージェント内部）タブ
- GlobalProtect ポータルの Agent External（エージェント外部）タブ
- GlobalProtect ポータルの Agent App（エージェント アプリケーション）タブ
- GlobalProtect ポータルの Agent HIP Data Collection（エージェント HIP データ収集）タブ

GlobalProtect ポータルの *Agent Authentication*（エージェント認証）タブ

- **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > *<portal-config>* > **Agent (**エージェント**)** > *<agent-config>* > **Authentication (**認証**)**

Authentication (認証**)**タブを選択し、エージェント設定に適用される認証設定を行います。

GlobalProtect ポータルのクライアント認証設定	の意味
Authentication [認証]タブ	
氏名	このクライアント認証の設定に付ける分かりやすい名前を入力してください。
クライアント証明書	（任意）エンドポイントへクライアント証明書を配信する送信元を選択すると、その送信元が証明書をゲートウェイに提示するようになります。相互SSL認証を設定する場合はクライアント証明書が必要となります。 ポータルクライアント設定のpre-logonでSCEPが設定されている場合、ポータルはマシン証明書を生成し、その証明書はゲートウェイの認証や接続に使用するシステム証明書ストアに保存されます。 **SCEP** を通じて PKI が生成した証明書を使用する代わりにファイアウォールの **Local**（ローカル） な証明書を使用する場合は、ファイアウォールに既にアップロード済みの証明書を選択してください。 内部 CA を使用して証明書をエンドポイントに配布する場合、**None(**なし**)** を選択します（デフォルト）。**None**（なし）を選択した場合、ポータルはエンドポイントに対し証明書をプッシュしません。
ユーザー認証情報の保存	アプリ上にユーザー名およびパスワードを保存する場合はYes（はい）を選択し、接続の都度、手動入力あるいはエンド

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのクライアント認証設定	の意味
	ポイントを通じて表示を行わずにパスワードの提供を求める場合はNo（いいえ）を選択します。ユーザーの接続時に、ユーザー名のみを保存しておきたい場合はSave Username Only[ユーザー名のみ保存] を選択してください。生体ログインを許可するにはOnly with User Fingerprint (ユーザーの指紋のみ) を選択します。エンドポイントで生体サインオンが有効になっている場合、指紋スキャンがエンドポイントの信頼できる指紋テンプレートと一致すると、GlobalProtect は保存されたユーザー資格情報を使用します。 認証されていないユーザーが重要なリソースや機密情報にアクセスしやすくなるため、ユーザー認証情報を保存しないでください。ユーザーが *GlobalProtect* に接続する度に認証情報を手動で入力する必要があります。
認証のオーバーライド	
Cookieを生成して認証をオーバーライド	暗号化された、エンドポイント固有のCookieをポータルに生成させる場合はこのオプションを選択します。ユーザーがポータルで認証を行ったのちに、ポータルはこのCookieをエンドポイントに送信します。
認証オーバーライドの Cookie を受け入れる	暗号化された有効な Cookie を使用してエンドポイント認証を行うようポータルを設定する場合はこのオプションを選択してください。有効なCookieをエンドポイントが提示した場合、ポータルはそのポータル自身が暗号化したCookieであることを確認し、復号化を行ってユーザーを認証します。
Cookie 有効期間	Cookieが有効な時間数、日数、あるいは週数を指定します。一般的な有効期間は24時間です。範囲は1～72時間、1～52週間、あるいは1～365日です。Cookieが失効した場合、ユーザーはログイン認証情報を再度入力する必要があり、この入力をうけてポータルは新しいCookieを暗号化してユーザーエンドポイントに送信します。
Cookie を暗号化/復号化する証明書	Cookieの暗号化と復号化に使用する証明書を選択します。 *Cookie*の暗号化および復号化用に、ポータルとゲートウェイで同じ証明書を使用するよう設定されていることを確認してください。（証明書をゲートウェイクライアント設定の一部として設定します。「Network（ネットワーク）> GlobalProtect > Gateways（ゲートウェイ）」を参照してください）
Components that Require Dynamic Passwords (Two-Factor Authentication)（ダイナミック パスワードが必要な構成要素（2 重認証））	

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのクライアント認証設定	の意味
1回限りのパスワード（OTP）などのダイナミックパスワードがGlobalProtectでサポートされるように設定する場合は、ダイナミックパスワードの入力を求めるポータルまたはゲートウェイタイプを指定します。2重認証が有効化されていない環境において、GlobalProtectはログイン認証情報（ADなど）と証明書を用いた通常の認証形式を使用します。 2重認証用のポータルまたはゲートウェイタイプを有効化すると、ユーザーがポータルで1度目の認証を行ったのち、そのポータルまたはゲートウェイは認証情報と2つ目のOTP（あるいはその他のダイナミックパスワード）の提示を求めます。 しかし、認証オーバーライドも同じく有効化している場合、（ユーザーが新しいセッションで認証されると、）認証情報の再入力を行う代わりに、（Cookieの有効期間内に限り、）ユーザーの認証には暗号化されたCookieが使用されます。このため、Cookieが有効である限り、ユーザーは認証の画面表示を行うことなくログインすることが可能になります。Cookieの有効期限を指定する必要があります。	
ポータル	ポータルへの接続にダイナミックパスワードを使用する場合はこのオプションを選択します。
Internal gateways - all（内部ゲートウェイ - すべて）	内部ゲートウェイへの接続にダイナミックパスワードを使用する場合はこのオプションを選択します。
外部ゲートウェイ - 手動のみ	**Manual**[手動] ゲートウェイとして設定されている外部ゲートウェイへの接続にダイナミックパスワードを使用する場合はこのオプションを選択します。
External gateways - auto discovery（外部ゲートウェイ - 自動検出）	アプリが自動検出可能なその他のゲートウェイ（**Manual**（手動）に設定されていないゲートウェイ）への接続にダイナミックパスワードを使用する場合はこのオプションを選択します。

GlobalProtect ポータルの *Agent Config Selection Criteria*（エージェント設定の選択条件）タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Portals** (ポータル) > *<portal-config>* > **Agent** (エージェント) > *<agent-config>* > **Config Selection Criteria** (設定選択条件)

Config Selection Criteria (設定選択条件)タブを選択し、管理対象および管理対象外のエンドポイントが両方あるデプロイ環境でエンドポイントの種類を識別するために使用する一致条件を設定します。ポータルは指定された設定をエンドポイントの種類に基づいてエンドポイントにプッシュできます。

GlobalProtect ポータルの設定選択条件の設定	の意味
User/User Group [ユーザー/ユーザー グループ] タブ	
OS	エンドポイントのオペレーティングシステム（OS）を一つ以上**Add** (追加)し、どのエンドポイントがこの設定を受信するのか指定します。ポータルはエンドポイントのOSを自動的に検知し、そのOS用のクライアント設定を適用します。**Any** (任意)の OS あるいは特定の OS (**Android**、 **Chrome**、 **iOS**、 **IoT**、 **Linux**、 **Mac**、 **Windows**、または **WindowsUWP**) を選択できます。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの設定選択条件の設定	の意味
ユーザー/ユーザー グループ	この設定を適用する特定のユーザーまたはユーザーグループを**Add** (追加) します。 ユーザーグループを選択する前にグループ マッピングを設定する必要があります (*Device* (デバイス) > *User Identification* (*User-ID*) > *Group Mapping Settings* (グループ マッピング設定))。 この設定をすべてのユーザーにデプロイするには、**User/User Group** (ユーザー/ユーザーグループ)のドロップダウンリストで**any** (すべて)を選択します。この設定をプレ ログオンモードの GlobalProtect アプリケーションを使用しているユーザーにのみデプロイする場合は、**User/User Group** (ユーザー/ユーザーグループ)のドロップダウンリストで**pre-logon** (プレ ログオン)を選択します。
デバイス チェック	
マシン アカウントはデバイスのシリアル番号と共に存在	エンドポイントのシリアル番号がアクティブディレクトリに存在するかどうかに応じて一致条件を設定します。
証明書プロファイル	GlobalProtect アプリケーションが送信したマシン証明書にマッチさせるために GlobalProtect ポータルが使用する証明書プロファイルを選択します。
カスタム チェック	
カスタム チェック	マッチさせるカスタム ホスト情報を定義する場合はこのオプションを選択します。
レジストリ キー	Windows エンドポイントに特定のレジストリキーがあるかチェックする場合は、マッチさせる**Registry Key** (レジストリキー)を**Add** (追加)します。指定したレジストリ キーまたはキーの値が欠損しているエンドポイントのみを照合する場合は、**Key does not exist or match the specified value data** (キーが存在しないか、指定した値データと一致しない) のオプションを有効化します。特定の値を照合するには、**Registry Value** (レジストリの値) と **Value Data** (値データ) を入力して**Add** (追加)します。指定された値または値データを明示的に持たないエンドポイントを照合するには、**Negate** (除外)を選択します。
Plist	macOS エンドポイントのプロパティリスト (plist) に特定のエントリがあるかチェックする場合は、**Plist**名を**Add** (追加)します。指定したplistを持たないエンドポイントのみを照合する場合は、**Plist does not exist** (**Plist**が存在しない) オプションを有効

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの設定選択条件の設定	の意味
	化します。plist 内の特定のキー/値ペアによって照合するには、**Key (キー)**と対応する**Value (値)**を**Add (追加)**します。指定されたキーまたは値を明示的に持たないエンドポイントを照合する場合は、**Negate (除外)** を選択します。

GlobalProtect ポータルの *Agent Internal*（エージェント内部）タブ

- **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > *<portal-config>* > **Agent (エージェント)** > *<agent-config>* > **Internal** 内部

Internal (内部)タブを選択し、エージェント設定用の内部ゲートウェイ設定を行います。

GlobalProtect ポータルの内部設定	の意味
内部ホスト検出	
内部ホスト検出	企業ネットワークの内部にいるかどうか、GlobalProtect アプリに判断させる場合はこのオプションを選択します。このオプションは内部ゲートウェイと通信するよう設定されたエンドポイントにのみ適用され、これらのエンドポイントのベストプラクティスになります。 ユーザーがログインを試みた場合、アプリは指定された **IP Address**（**IP**アドレス）に対し、指定された**Hostname**（ホスト名）を使用して内部ホストのリバース DNS 検索を行います。エンドポイントが企業ネットワーク内にある場合、ホストは到達可能なリファレンスポイントとなります。アプリがホストを検出したということは、エンドポイントがネットワーク内にあることを意味しており、アプリは内部ゲートウェイと接続します。アプリが内部ホストの検出に失敗した場合、アプリはネットワーク外にあることを意味しており、アプリは外部ゲートウェイとトンネルを確立します。 • IP アドレス タイプは、**IPv4**（IPv4 トラフィックのみ）、**IPv6**（IPv6 トラフィックのみ）、またはその両方です。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4** と **IPv6** を使用します。これにより IPv4 と IPv6 が同時に動作します。 • IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。 • **IPv4** と **IPv6** を選択した場合、それぞれのタイプに適切な IP アドレスを入力します。
ホスト名	内部ネットワーク内で上記のIPアドレスに解決する**Hostname**[ホスト名] を入力します。
内部ゲートウェイ	
アプリがアクセス要求を行い、さらに、HIP レポートを提供する（GlobalProtect Portals Agent Data Collection	内部ゲートウェイを**Add**[追加] し、以下の情報を指定します。 • **Name**[名前] – ゲートウェイを識別するラベル（最大31文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの内部設定	の意味
Tab（GlobalProtect ポータルのエージェント データ収集）で HIP が有効にされている場合）内部ゲートウェイを指定します。	があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 • **Address**[アドレス] – ゲートウェイ用のファイアウォールインターフェイスのIPアドレスまたはFQDN。ここで指定する値はゲートウェイサーバー証明書の共通名（CN）およびSAN（指定されている場合）と一致させる必要があります。例えば、証明書の生成にFQDNを使用した場合、ここにFQDNを入力する必要があります。 • **Source Address**（送信元アドレス） – エンドポイントの送信元アドレスまたはアドレス プールです。ユーザーが接続すると、GlobalProtect はデバイスの送信元アドレスを認識します。送信元アドレス プールに含まれている IP アドレスの GlobalProtect アプリのみが、このゲートウェイで認証し、HIP レポートを送信できます。 • **DHCP Option 43 Code**（**DHCP** オプション **43** コード）（Windows および Mac のみ） – ゲートウェイ選択用の DHCP サブオプション コードを指します。Specify one or more sub-option codes (in decimal). サブオプション コードを指定します（10 進数）。GlobalProtect アプリは、サブオプション コードで定義された値からゲートウェイ アドレスを読み取ります。

GlobalProtect ポータルの Agent External（エージェント外部）タブ

- **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > *<portal-config>* > **Agent (エージェント)** > *<agent-config>* > **External** エージェント

External (外部)タブを選択し、エージェント設定用の外部ゲートウェイ設定を行います。

GlobalProtect ポータルの外部設定	の意味
Cutoff Time (sec)（カットオフ時間（秒））	最適なゲートウェイを選択する際、使用可能なゲートウェイが応答するまでアプリが待機する時間を秒単位で指定します。以降の接続要求において、アプリはそのカットオフ時間内に応答したゲートウェイとの接続を試行します。値が 0 の場合、アプリは **App**（アプリ）タブの **AppConfigurations**（アプリ設定）にある **TCP Connection Timeout**（**TCP** 接続のタイムアウト）を使用します（範囲は 0 ~ 10、デフォルトは 5）。
外部ゲートウェイ	
企業ネットワーク外からトンネルを確立する場合にアプリが接続を試行する対象となるファイアウォールのリストを指定します。	外部ゲートウェイを**Add**[追加] し、以下の情報を指定します。 • **Name**[名前] – ゲートウェイを識別するラベル（最大31文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。 • アドレス – ゲートウェイが設定されているファイアウォール インターフェイスの IP アドレスまたは FQDN。値は、ゲートウェイ サーバー証明書の CN（および指定されている場合は SAN）と一致させる必要があります。たとえば、証明書の生成に FQDN を使用した場合、ここに FQDN も入力する必要があります。 • **Source Region**（送信元地域） – エンドポイントの送信元地域です。GlobalProtect はユーザーが接続した際にエンドポイントの地域を認

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの外部設定	の意味
	識して、その地域に設定されたゲートウェイに対してのみユーザーの接続を許可します。ゲートウェイの選択では、送信元地域が考慮されてから、ゲートウェイの優先順位が考慮されます。 • **Priority**（優先順位）– アプリが使用するゲートウェイを判別しやすいように値 (**Highest**（最高）、**High**（高）、**Medium**（中）、**Low**（低）、**Lowest**（最低）、**Manual only**（手動のみ）のいずれか) を選択します。**Manual only**（手動のみ）を選択すると、エンドポイントで **Auto Discovery**（自動検出）が有効である場合に GlobalProtect アプリはこのゲートウェイへの接続を試行しません。このアプリは、まず、指定されたすべてのゲートウェイに **Highest**（最高）、**High**（高）、または **Medium**（中）の優先度で接続し、最速で応答するゲートウェイとトンネルを確立します。優先度の高いゲートウェイに到達できない場合、次にアプリは優先度の低い値を持つ追加のゲートウェイに接続します（**Manual only**（手動のみ）のゲートウェイは除く）。 • **Manual**[手動] – ユーザーが手動でゲートウェイを選択（あるいは切り替え）できるようにする場合はこのオプションを選択します。GlobalProtect アプリは、**Manual**（手動）に設定されている外部ゲートウェイであれば、どのゲートウェイにも接続することができます。アプリが他のゲートウェイに接続する場合、既存のトンネルは接続が解除され、新しいトンネルが確立されます。手動ゲートウェイでは、プライマリゲートウェイとは異なる認証方式を使用することもできます。エンドポイントが再起動された場合や、再検出が実行された場合、GlobalProtect エージェントはプライマリゲートウェイに接続します。この機能は、ネットワークの保護されたセグメントにアクセスするために、特定のゲートウェイに一時的に接続する必要があるユーザーグループが存在する場合に役立ちます。
サードパーティ VPN	
サードパーティ VPN	GlobalProtect が対象指定されたサードパーティ VPN クライアントと競合しないよう、GlobalProtect アプリにこれらを無視するように設定する場合は、VPN クライアントの名前を **Add**（追加）します。リストから名前を選択するか、フィールドに名前を入力します。GlobalProtectはここで指定したVPNクライアントのルート設定を無視するようになります。

GlobalProtect ポータルの *Agent App*（エージェント アプリケーション）タブ

- **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > *<portal-config>* > **Agent (**エージェント**)** > *<agent-config>* > **App** アプリ

App (アプリ**)**タブを選択し、ユーザーがシステム上にインストールされた GlobalProtect アプリをどのように操作するかを指定します。作成した各種のGlobalProtectエージェント設定ごとに、異なるアプリ設定を定義できます。

GlobalProtect アプリの設定	の意味
ウェルカム ページ	GlobalProtect に接続したエンドユーザーに対して表示するウェルカムページを選択します。**factory-default**[出荷時のデフォル

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	ト] ページを選択するか、カスタムページを**Import**[インポート] することができます。デフォルト設定は**None**[なし] です。
アプリケーション設定	

接続手段	• **On-demand (Manual user initiated connection)** (オンデマンド (ユーザーによる手動接続)) – ユーザーは GlobalProtect アプリを起動し、当該の GlobalProtect 認証情報を入力する必要があります。このオプションは、主にリモートアクセス接続の場合に使用します。
	• **User-logon (Always On)** (ユーザー ログオン (常時オン)) – ユーザーがエンドポイントにログインすると GlobalProtect アプリはポータルへの接続を自動的に確立します。応答として、ポータルはアプリに適切なエージェント設定を返します。その後、アプリはポータルから受信したエージェント設定に指定されているゲートウェイのうちの 1 つとトンネルを確立します。
	• **Pre-logon** (ログオン前) – これにより、リモートの Windows および Mac ユーザーは常に企業ネットワークに接続された状態になります。また、ユーザーがエンドポイントにログインした際のユーザー ログオン スクリプトとドメイン ポリシーの適用を可能にします。社内と同じようにエンドポイントから企業ネットワークに接続できるため、ユーザーはパスワードの失効時に新しいパスワードでログインしたり、パスワードを忘れた場合にパスワード復元によるサポートを利用したりできます。pre-logon を使用すると、GlobalProtect アプリはユーザーがエンドポイントにログインする前に GlobalProtect ゲートウェイへの VPN トンネルを確立します。エンドポイントはゲートウェイに対し、事前にインストールされたマシン証明書を提示することで認証要求を行います。Windows エンドポイントの場合、その後ゲートウェイは、pre-logon ユーザーからの VPN トンネルを、エンドポイントにログインしたユーザー名に割り当て直します。Mac エンドポイントの場合、アプリが切断を行い、ユーザー用に新しい VPN トンネルを確立します。
	
	pre-logon 接続方式は 2 種類あります。いずれも、同様の pre-logon 機能をユーザーがエンドポイントにログインする前に実施します。ただし、ユーザーがエンドポイントにログインした後は、pre-logon 接続方式によって、GlobalProtect アプリの接続が確立されるタイミングが異なります。
	
	  • **Pre-logon (Always On)** (ログオン前 (常時オン)) – GlobalProtect アプリは、GlobalProtect ゲートウェイへの接続および再接続を自動的に試行します。モバイル デバイスは pre-logon 機能をサポートしていないため、この接続方式が指定された場合、デフォルトは **User-logon (Always On)** (ユーザーログオン (常時オン)) 接続方式となります。
	  • **Pre-logon then On-demand** (**pre-logon** 後オンデマンド) –ユーザーは GlobalProtect アプリを起動してから当該の接続を手動で開始する必要があります。モバイル デバイスは pre-logon 機能をサポートしていないため、こ

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	の接続方式が指定された場合、デフォルトは **On-demand (Manual user initiated connection)**（オンデマンド（ユーザーによる手動接続））接続方式となります。
GlobalProtect アプリ設定の更新間隔 (時間)	GlobalProtect ポータルがアプリの設定を更新する間隔（時間数）を指定します（範囲は 1 ~ 168、デフォルトは 24）。
ユーザーが GlobalProtect アプリを無効化できるようにする	ユーザーによる GlobalProtect アプリの無効化を許可するかどうか、そして無効化を許可する場合は、無効化する際に踏むべき手順を指定します。 • **Allow**（許可）– すべてのユーザーが必要に応じて GlobalProtect アプリを無効化できます。 • **Disallow**（許可しない）– ユーザーは GlobalProtect アプリを無効化することができません。 • **Allow with Comment**（コメント付きで許可）– ユーザーはエンドポイントの GlobalProtect アプリを無効化できますが、その際、無効化する理由を送信する必要があります。 • **Allow with Passcode**（パスコードで許可）– ユーザーはパスコードを入力することで GlobalProtect アプリを無効化できます。このオプションを選択すると、ユーザーは、パスワードと同様に入力時に表示されることがないパスコードの入力と再入力を行う必要があります。一般的に、管理者は予期しない出来事によりユーザーがGlobalProtect VPNを使用してネットワークに接続できなくなる前にユーザーにパスコードを配布しておきます。パスコードは電子メールで送信するか、企業の Web サイトに掲示することで配布することができます。 • **Allow with Ticket**（チケットで許可）– このオプションでは、ユーザーが GlobalProtect を無効化しようとすると、エンドポイントに 16 進数の 8 桁のチケット要求ナンバーを表示するチャレンジレスポンス機構が有効化されます。次にユーザーはファイアウォール管理者またはサポートチームに連絡し（セキュリティ保護のため、電話をお勧めします）、この番号を伝える必要があります。管理者またはサポート担当者は、ファイアウォール（**Network**（ネットワーク）> **GlobalProtect** > **Portals**（ポータル））で、**Generate Ticket**（チケット生成）をクリックし、チケット **Request**（リクエスト）番号を入力して **Ticket**（チケット）番号を取得できます（16 進数の 8 桁）。管理者またはサポート担当はこのチケットナンバーをユーザーに伝え、ユーザーがこれをチャレンジフィールドに入力するとアプリは無効化されます。
ユーザーが GlobalProtectアプリをアンインストールできるようにする	ユーザーが GlobalProtectアプリのアンインストールを許可されているか、許可されている場合は、アプリをアンインストールする前にユーザーが何をする必要があるかを指定します。 • **Allow (許可)**–必要に応じて、すべてのユーザーが GlobalProtectアプリをアンインストールできるようにします。 • **Disallow (許可しない)**–エンドユーザーが GlobalProtectアプリをアンインストールできないようにします。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	• **Allow with Password** (パスワードで許可する)– GlobalProtectアプリをアンインストールするためのパスワードを強制します。このオプションでは、ユーザーがアンインストールを続行する前に、パスワードを入力して確認する必要があります。パスワードは電子メールで送信するか、企業の Web サイトに掲示することで配布することができます。 このオプションでは、コンテンツ リリース バージョン 8196-5685 以降が必要になります。
ユーザーが GlobalProtect アプリをアップグレードできるようにする	エンドユーザーによる GlobalProtect アプリのソフトウエア アップデートの可否、そして許可するよう設定した場合は、アップグレードのタイミング指定の可否を設定します。 • **Disallow**（無効）– ユーザーはアプリのアップグレードを行うことができません。 • **Allow Manually**（手動を許可）– ユーザーは GlobalProtect アプリで **Check Version**（バージョンの確認）を選択することで、アップグレードの確認と実行を手動で行うことができます。 • **Allow with Prompt**（プロンプト付きで許可）（デフォルト）– ファイアウォールで新しいバージョンが起動された場合にプロンプトを表示し、ユーザーは任意のタイミングでアップグレードを行うことができます。 • **Allow Transparently**（メッセージを表示せずに実行）– ポータルで新しいバージョンが使用可能になるとアプリのソフトウェアを自動的にアップグレードします。 • **Internal**（内部）– ポータルで新しいバージョンが使用可能になるとアプリのソフトウエアを自動的にアップグレードしますが、エンドポイントが企業ネットワークに内部接続するまで待機します。これにより、低帯域幅の接続を使用したアップグレードによる遅延を防ぎます。
ユーザーの GlobalProtectアプリからのサインアウトを許可します (Windows、macOS、iOS、Android、Chromeのみ)	ユーザーが、Globalprotectアプリから手動でサインアウトすることを許可するかを指定します。 • **Yes** (はい)(デフォルト)–必要に応じて、すべてのユーザーがGlobalProtectアプリからサインアウトできるようにします。 • **No**（いいえ）– エンド ユーザーは GlobalProtect アプリからサインアウトできません。 このオプションでは、コンテンツ リリース バージョン 8196-5685 以降が必要になります。
Single Sign-On (シングル サインオン - SSO) を使用します (Windows)	シングルサインオン（SSO）を無効化する場合は**No**[いいえ] を選択します。SSO が有効化されている場合、GlobalProtect アプリはユーザーの Windows ログイン認証情報を使用して自動的に認証を行い、GlobalProtect ポータルおよびゲートウェイに接続します。GlobalProtectはサードパーティ認証情報をラップすることができるので、サードパーティの認証情報プロバイダを使用してWindowsログイン認証情報をラップしている場合でも認証と接続を行うことができます。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
Single Sign-On (シングル サインオン - SSO) を使用します (macOS)	シングルサインオン (SSO) を無効化する場合は**No**[いいえ] を選択します。SSO が有効化されている場合 (デフォルト)、GlobalProtect アプリは macOS ログイン認証情報を使用して自動的に認証を行い、GlobalProtect ポータルおよびゲートウェイに接続します。 このオプションでは、コンテンツ リリース バージョン 8196-5685 以降が必要になります。
Clear Single Sign-On Credentials on Logout (ログアウト時にサインオンの認証情報を消去) (Windows のみ)	ユーザーのログアウト後もサインオン認証情報を保存しておく場合は**No**[いいえ] を選択します。ユーザーのログアウト時に消去し、次回ログイン時に再度認証情報の入力を求める場合は**Yes**[はい] (デフォルト) を選択します。
認証の失敗時にはデフォルトの認証を使用	Kerberos認証のみを使用する場合は**No**[いいえ] を選択します。Kerberos 認証が失敗したときにデフォルトの認証方法を使用して認証を再試行する場合は **Yes** (はい) (デフォルト) を選択します。この機能は Mac および Windows エンドポイントでのみサポートされています。
VPN 接続タイムアウトの自動復元	ネットワークの不安定化やエンドポイントの状態の変化によりトンネルが切断されたときに、GlobalProtect アプリが実行する動作を指定するタイムアウト値 (0〜180分) を入力します。デフォルトは 30 です。 • 0—トンネルが切断された後に GlobalProtect がトンネルを再確立しようとしないように、この機能を無効にします。 • 1-180—ここで指定したタイムアウト値を超えない期間、トンネルがダウンした場合、GlobalProtect がトンネル接続を再確立しようとするように、この機能を有効にします。たとえば、タイムアウト値が 30 分の場合、トンネルが 45 分間切断された場合、GlobalProtect はトンネルを再確立しようとしません。ただし、トンネルが 15 分間切断された場合、分数がタイムアウト値を超えていないため、GlobalProtect は再接続を試みます。 *VPN 常時オンが機能しており、タイムアウト値が切れる前にユーザーが外部ネットワークから内部ネットワークに切り替えると、GlobalProtect はネットワーク探索を実行しません。その結果、GlobalProtect は最後の既知の外部ゲートウェイへのトンネルを再確立します。内部ホスト検出をトリガするには、GlobalProtect コンソールからネットワークの再検出を選択する必要があります。*
VPN 再接続を試行するまでの待機時間	**Automatic Restoration of VPN Connection Timeout** (**VPN** 接続タイムアウトの自動復元) を有効にしたときに、最後に接続されたゲートウェイとの接続を再確立する試行の間に、GlobalProtect アプリが待機する時間を秒単位で入力します。ネットワークの状態に応じて、より長い待機時間または短い待機時間を指定します。範囲は 1 ~ 60、デフォルトは 5 です。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	この時間間隔は、SSL VPN トンネルの場合の復元試行の TCP タイムアウトとして使用します。IPSec トンネルの場合は、復元試行の UDP キープアライブ タイムアウトとして使用します。 常時接続モードでは、*GlobalProtect*アプリは、設定された *VPN* 接続の復元試行間の待機時間で無期限に再試行を続けます。ただし、オンデマンドモードの場合、*GlobalProtect*アプリは、 *VPN* 接続の復元試行間の待機時間で設定されたタイムアウトの期間に *1* 回試行し、タイムアウト期間内に成功しない場合は、試行せずに切断状態に切り替えます。
ネットワークアクセスの際に必ずGlobalProtect接続を利用する	すべてのネットワーク トラフィックに GlobalProtect トンネルを通過するように強制する場合は **Yes**（はい）を選択します。ネットワーク アクセスのために GlobalProtect を必要とせず、GlobalProtect が無効または切断されている場合でもユーザーがインターネットにアクセスできる状態の場合は、**No**（いいえ）（デフォルト）を選択します。 トラフィックがブロックされる前にユーザーに指示を出す場合、**Traffic Blocking Notification Message**（トラフィック ブロックの通知メッセージ）を設定し、さらに任意でメッセージを表示するタイミングを指定します（**Traffic Blocking Notification Delay**（トラフィック ブロックの通知の遅延））。 キャプティブポータルへの接続を確立するために必要なトラフィックを許可するには、**Captive Portal Exception Timeout**（キャプティブポータルの例外タイムアウト）を指定します。ユーザーは、タイムアウトの時間が過ぎるまでの間にポータルに認証する必要があります。追加の指示を提供するには、**Captive Portal Detection Message (**キャプティブポータルの検知メッセージ**)**を設定し、任意でメッセージを表示するタイミングを指定します（**Captive Portal Notification Delay (**キャプティブポータルの通知の遅延**)**）。 大抵の場合、デフォルトの選択肢（*No (*いいえ*)*）を使用することになります。*Yes (*はい*)*を選択すると、エンタープライズ内の内部ゲートウェイあるいはエンタープライズ ネットワーク外の外部ゲートウェイにアプリが接続するまで、エンドポイントを出入りするすべてのネットワーク トラフィックがブロックされます。
ネットワーク アクセスのGlobalProtect接続の強制が有効で、GlobalProtect接続が確立されていない場合に、指定されたホスト/ネットワークへのトラフィックを許可する	必要に応じて、ネットワークアクセスに GlobalProtect を適用しても接続が確立されない場合に、アクセスを許可する最大 10 個の IPアドレスまたはネットワーク セグメントを設定できます。複数の値はカンマで区切ります。除外を設定すると、GlobalProtectが切断されているときにユーザーがローカルリソースにアクセスできるようになり、ユーザーエクスペリエンスを向上させることができます。例えば、GlobalProtect が接続されていない場合、 GlobalProtect はリンク ローカル アドレスを除

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	外して、ローカル ネットワーク セグメントまたはブロードキャスト ドメインへのアクセスを許可できます。このオプションでは、コンテンツ リリース バージョン 8196-5685 以降が必要になります。
キャプティブポータルの例外タイムアウト（秒）	ネットワーク アクセスに GlobalProtect を適用する一方で、ユーザーがキャプティブ ポータルに接続するための十分な猶予期間を設定する場合、タイムアウトの秒数を指定します（範囲は 0 ~ 3600）。たとえば、値が 60 の場合、GlobalProtect がキャプティブ ポータルを検出した後 1 分以内に、ユーザーはキャプティブ ポータルにログインする必要があります。値が 0 の場合、GlobalProtect はユーザーがキャプティブ ポータルに接続することを許可せず、即座にアクセスをブロックします。
キャプティブ ポータルの検出時にデフォルトのブラウザで Web ページを自動的に起動する	キャプティブ ポータルの検出時にデフォルトのウェブブラウザを自動的に起動してユーザーがキャプティブ ポータルにシームレスにログインできるようにするには、完全修飾ドメイン名 (FQDN) またはデフォルトのウェブブラウザの起動時にウェブトラフィックを開始する最初の接続試行に使用するウェブサイトの IPアドレス (最大長は 256 文字) を入力します。次に、キャプティブ ポータルはこの Web サイト接続の試行を傍受し、デフォルトの Web ブラウザをキャプティブ ポータルのログイン ページにリダイレクトします。このフィールドが空の場合 (デフォルト)、GlobalProtect はキャプティブ ポータルの検出時にデフォルトの Web ブラウザを自動的に起動しません。
トラフィックブロックの通知遅延（秒）	通知メッセージを表示するタイミングを指定する場合、値に秒数を指定します。ネットワークが到達可能となった後、GlobalProtect は通知を表示するまでのカウントダウンを開始します（範囲は 5 ~ 120、デフォルトは 15）。
Display Traffic Blocking Notification Message（トラフィックブロックの通知メッセージの表示）	GlobalProtect がネットワーク アクセスに必要な場合にメッセージを表示するかどうかを指定します。メッセージを無効化する場合は **No**（いいえ）を選択します。メッセージを有効化する場合は **Yes**（はい）を選択します（GlobalProtect が切断されている状態でネットワークは到達可能であることを検出したときに、GlobalProtect はメッセージを表示します）。
トラフィックブロックの通知メッセージ	GlobalProtect がネットワーク アクセスに必要な場合にユーザーに表示する通知メッセージをカスタマイズします。GlobalProtect が切断されている状態でネットワークは到達可能であることを検出したときに、GlobalProtect はメッセージを表示します。メッセージによって、トラフィックがブロックされている理由を示し、接続する手順を提示できます。以下がその例です。 `To access the network, you much first connect to GlobalProtect.` メッセージは 512 文字以下にしてください。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
ユーザーがトラフィックブロックの通知を無視することを許可	トラフィック ブロック通知を常に表示する場合は **No**（いいえ）を選択します。デフォルトの値は **Yes**（はい）に設定されており、ユーザーは通知を無視できます。
Display Captive Portal Detection Message（キャプティブポータルの検知メッセージの表示）	GlobalProtect がキャプティブ ポータルを検出したときにメッセージを表示するかどうかを指定します。メッセージを表示する場合は **Yes**（はい）を選択します。メッセージを表示しない場合は **No**（いいえ）（デフォルト）を選択します（GlobalProtect がキャプティブ ポータルを検出したとき、GlobalProtect はメッセージを表示しません）。 キャプティブ ポータルの検知メッセージを有効化すると、キャプティブ ポータルの例外タイムアウトの *85* 秒前にメッセージが表示されます。そのため、*Captive Portal Exception Timeout*（キャプティブ ポータルの例外タイムアウト）が *90* 秒以下の場合、メッセージはキャプティブ ポータルが検出された *5* 秒後に表示されます。
キャプティブポータルの検知メッセージ	GlobalProtect がネットワークを検出した場合に、キャプティブポータルに接続するための追加手順をユーザーに表示する通知メッセージをカスタマイズします。以下がその例です。 `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.` メッセージは 512 文字以下にしてください。
Captive Portal Detection Delay (キャプティブ ポータルの検出遅延)	キャプティブ ポータルの検出メッセージを有効にすると、キャプティブ ポータルの検出後、GlobalProtect が検出メッセージを表示するまでの遅延を秒単位で指定できます (範囲は 1 ～ 120、デフォルトは 5)。
クライアントの証明ストアの検索	証明書のタイプ、またはアプリが個人用証明書ストアで検索する証明書を選択します。GlobalProtect アプリは、ポータルやゲートウェイへの認証を行い、GlobalProtect ゲートウェイへのVPNトンネルを確立する際にこの証明書を使用します。 • **User**（ユーザー）– ユーザー アカウントのローカルな証明書を使用して認証を行います。 • **Machine**[マシン] – エンドポイントのローカルな証明書を使用して認証を行います。この証明書はエンドポイントの使用を許可されているすべてのユーザーに適用されます。 • **User and machine**[ユーザーおよびマシン]（デフォルト）– ユーザー証明書およびマシン証明書を使用して認証します。
SCEP 証明書更新期間（日）	SCEPが生成した証明書を失効前に更新するための機能です。ポータルが PKI システムの SCEP サーバーに対し、新しい証明書

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	の要求を証明書失効日の最大何日前に行うかを指定します（範囲は 0 ~ 30、デフォルトは 7）。0を指定すると、ポータルはクライアント設定を更新する際に、クライアント証明書の自動更新を行いません。 アプリが新しい証明書を取得できるようにする場合、ユーザーは更新期間内にログインする必要があります（ユーザーがこの期間内にログインしない場合、ポータルは新しい証明書の要求を行いません）。 例えば、クライアント証明書の有効期間が90日、証明書更新期間が7日だったとします。証明書有効期間の最後7日間のうちにユーザーがログインした場合、ポータルは証明書を生成し、更新されたクライアント設定と共にダウンロードします詳細は「GlobalProtect App Config Refresh Interval (hours)（GlobalProtect アプリ設定の更新間隔（時間））」を参照してください。
クライアント証明向けの拡張キー使用OID	オブジェクト識別子（OID）を指定し、クライアント証明書の拡張キー用途を入力します。この設定では、GlobalProtect が必ずクライアント認証用の証明書のみを選択するようにし、また、以後使用できるように GlobalProtect による証明書の保存を有効化することができます。
スマートカードの取り外し時に接続を維持 （Windows のみ）	クライアント証明書を含むスマート カードをユーザーが取り外したときに接続を維持する場合は **Yes**（はい）を選択します。ユーザーがスマート カードを取り外したときに接続を終了する場合は **No**（いいえ）（デフォルト）を選択します。
Allow Overriding Username from Client Certificate (クライアント証明書からのユーザー名のオーバーライドを許可する)	**No** (いいえ)を選択すると、GlobalProtect にクライアント証明書のユーザー名を使用させ、GlobalProtect がそれを上書きしないようにします (デフォルトで有効)。
詳細ビューの有効化	アプリのユーザーインターフェイスを基本的な最小限のビューに制限する場合は、**No**（いいえ）を選択します。
ユーザーがウェルカムページを終了できるようにする	ユーザーが接続を開始するたびにウェルカム ページを表示する場合は、**No**（いいえ）を選択します。この制約をかけることで、コンプライアンス維持のために組織から求められる利用規約などの重要な情報をユーザーが忘れてしまわないようにすることができます。
ネットワーク オプションの再検出の有効化	ユーザーによる手動ネットワーク再検出を行えないようにする場合は、**No**（いいえ）を選択します。
[ホスト プロファイルの再送信] オプションを有効にする	ユーザーが手動で最新 HIP の再送信をトリガーできないようにする場合は、**No**（いいえ）を選択します。
ポータル アドレスの変更をユーザーに許可する	GlobalProtect アプリの **Home**（ホーム）タブの **Portal**（ポータル）フィールドを無効化する場合は、**No**（いいえ）を選択します。しかしこの場合、ユーザーは接続するポータルを指定できなくなってしまうので、デフォルトポータルアドレス

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	をWindowsレジストリまたはMac plistに入れておく必要があります。 • **Windows registry (Windowsレジストリ)** – `HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup`、キーは`Portal` • **Mac plist**–`/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist`、キーは `Portal` ポータル アドレスの事前デプロイの詳細は、GlobalProtect 管理者ガイドの「Customizable App Settings（カスタマイズ可能なアプリ設定）」を参照してください。
ユーザーが無効なポータルサーバー証明書で続行できるようにする	ポータル証明書が無効なときにアプリがポータルとの接続を確立できないようにする場合は、**No**（いいえ）を選択します。
GlobalProtect アイコンの表示	エンドポイントで GlobalProtect アイコンを非表示にする場合は、**No**（いいえ）を選択します。アイコンが非表示の場合、ユーザーはトラブルシューティングの参照、パスワードの変更、ネットワークの再検出、またはオンデマンド接続の実行などの特定のタスクを行えません。しかし、ユーザーの操作が必要な場合、HIP通知メッセージ、ログインプロンプト、および証明書ダイアログは表示されるようになっています。
ユーザースイッチトンネルの名前変更のタイムアウト（秒） （Windowsのみ）	リモート ユーザーが Microsoft のリモート デスクトップ プロトコル（RDP）を使用してエンドポイントにログインしたのち、GlobalProtect ゲートウェイでの認証状態を保つ秒数を指定します（範囲は0 ~ 600、デフォルトは 0）。リモートユーザーに一定の時間内に認証を求めることで、セキュリティを保つことができます。 新しいユーザーを認証しトンネルをそのユーザー用に切り替えると、ゲートウェイはトンネルの名称を変更します。 0 を指定するとユーザー トンネルの名称は変更されませんが、即座に強制終了されるようになります。この場合、リモートユーザーは新しいトンネルを与えられ、ゲートウェイへの認証の際、制限時間は設けられません（設定済みのTCPタイムアウトを除く）。
Pre-Logon Tunnel Rename Timeout (sec)（pre-logon トンネルの名前変更のタイムアウト（秒））（Windows のみ）	この設定は、エンドポイントをゲートウェイに接続する pre-logon トンネルを GlobalProtect がどのように処理するのかを管理します。 値が -1 の場合、ユーザーがエンドポイントにログインした後、pre-logon トンネルはタイムアウトしません。GlobalProtect はトンネルの名称を変更して、ユーザーに割り当て直します。なお、名称を変更できなかった場合やユーザーが GlobalProtect ゲートウェイにログインしない場合でも、トンネルは持続します。 値が 0 の場合、ユーザーがエンドポイントにログオンしたとき、GlobalProtect は pre-logon トンネルの名称を変更する代わりに、即座に pre-logon トンネルを終了します。この場合、

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	ユーザーに pre-logon トンネル経由での接続を許可するのではなく、GlobalProtect がユーザー用の新しいトンネルを開始します。通常、**Connect Method** (接続方式) を **Pre-logon then On-demand** (**pre-logon** 後オンデマンド) (最初のログオン後に手動による接続開始をユーザーに強制) に設定している場合、この設定が一番便利です。 値が 1 ~ 600 の場合は、ユーザーがエンドポイントにログオンした後、pre-logon トンネルがアクティブ状態で維持される秒数となります。この期間、GlobalProtect は pre-logon トンネルにポリシーを適用します。タイムアウト時間内にユーザーが GlobalProtect ゲートウェイで認証した場合、GlobalProtect はトンネルをユーザーに割り当て直します。タイムアウト時間内にユーザーが GlobalProtect ゲートウェイで認証しなかった場合、GlobalProtect は pre-logon トンネルを終了します。
Preserve Tunnel on User Logoff Timeout (ユーザー ログオフ タイムアウト時にトンネルを保持) (秒)	ユーザーがエンドポイントからログアウトした後に GlobalProtect が既存の VPN トンネルを保持できるようにするには、**Preserve Tunnel on User Logoff Timeout (**ユーザー ログオフ タイムアウト時にトンネルを保持**)** 値を指定します (範囲は 0 ~ 600 秒、デフォルトは 0 秒です)。デフォルト値の 0を受け入れると、GlobalProtect はユーザーのログアウト後のトンネルを保持しません。
システムトレイ通知の表示 (Windowsのみ)	ユーザーからの通知を非表示にする場合は**No**[いいえ] を選択します。システムトレー領域に通知を表示する場合は**Yes**[はい] (デフォルト) を選択します。
Custom Password Expiration Message (カスタムのパスワード有効期限メッセージ) (LDAP 認証のみ)	パスワードの失効が近づいてきた場合に表示するカスタムメッセージを作成します。メッセージの長さは最大200文字までです。
Automatically Use SSL When IPSec Is Unreliable (IPSec が信頼できない場合に SSL を自動的に使用) (時間)	GlobalProtect アプリケーションに **Automatically Use SSL When IPSec Is Unreliable (IPSec** を信頼できない場合に自動的に **SSL** を使用**)** する時間 (時間単位) を指定します (範囲は 0 ~ 168 時間)。このオプションを指定すると、GlobalProtect アプリケーションは指定された期間中、IPSec トンネルを確立しようとしなくなります。このタイマーは、トンネルのキープアライブがタイムアウトしたことで IPSec トンネルがダウンする度に開始されます。 デフォルトの値である 0 を採用すると、アプリが IPSec トンネルを正常に確立できた場合に SSL トンネルを確立するというフォールバックが行われません。IPSec トンネルを確立できない場合にのみ SSL トンネルにフォールバックします。
Connect with SSL Only (SSL 接続のみ)	ユーザーが IPSec ではなく SSL を使用して GlobalProtectゲートウェイに接続する必要があるかを指定します。オプションは次のとおりです： • Yes (はい)—強制的に SSL を使用して、ポータルに設定されているゲートウェイに接続します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	• No (いいえ)–(デフォルト) ゲートウェイで設定されたプロトコルを使用します。 • User can Change (ユーザーが変更可能)–ゲートウェイ設定がいずれかのプロトコルの使用をサポートしている場合、ユーザーは SSL または IPSec の使用を選択できます。 **User can Change (ユーザーが変更可能)**に設定すると、ユーザーは GP アプリで **VPN** のチェックボックスを有効またはオフにできます。安全なアクセスのための最適な接続オプションを可能にするプロトコルを選択するには、**SSL** のみ接続します。
内部のゲートウェイ接続の最大試行回数	GlobalProtect エージェントから内部ゲートウェイに対する接続が失敗した場合に接続を再試行する回数の上限を入力します（範囲は0 ~ 100、デフォルトは 0）。0 の場合、GlobalProtect アプリは接続の再試行を行いません。この値を増やすことで、内部ゲートウェイが最初の接続試行時に一時的にダウンしていた場合や、最初の試行時に到達不能であったものの、設定した試行回数のうちに復旧した場合に、アプリはゲートウェイへ自動的に接続することができます。また、この値を増やすことで、内部ゲートウェイが最新のユーザー情報およびホスト情報を確実に受信できるようになります。
ポータルの接続のタイムアウト（秒）	ポータルへの接続要求に対し応答がなかった場合に、接続要求がタイムアウトするまでの秒数です（範囲は1 ~ 600、デフォルトは 30）。ファイアウォールが 777-4484 より前のアプリケーションおよび脅威のコンテンツ バージョンを実行している場合、デフォルトは 30 です。コンテンツ リリース バージョン 777-4484 で始まる場合、デフォルトは 5 です。
TCP 接続のタイムアウト（秒）	TCP 接続の両端のいずれかからの応答がないために、接続要求がタイムアウトするまでの秒数 (範囲は 1 ~ 600)。ファイアウォールが 777-4484 より前のアプリケーションおよび脅威のコンテンツ バージョンを実行している場合、デフォルトは60 です。コンテンツ リリース バージョン 777-4484 で始まる場合、デフォルトは 5 です。
TCP 受信のタイムアウト（秒）	TCP 要求の応答が一部欠損している場合に、TCP 接続がタイムアウトするまでの秒数です（範囲は1 ~ 600、デフォルトは 30）。
トンネルによって割り当てられた DNS サーバーを使用するすべての FQDN を解決する (Windows のみ)	（GlobalProtect 4.0.3 およびそれ以降のリリース）GlobalProtect トンネルが Windows エンドポイントに接続されている場合の DNS 解決設定を行います。 • **Yes**（はい）（デフォルト）を選択すると、エンドポイントが物理アダプタに設定されている DNS サーバーに DNS クエリを送信するのではなく、Windows エンドポイントがゲートウェイで構成した DNS サーバーとのすべての DNS クエリを解決できるようになります。 • **No**（いいえ）を選択すると、ゲートウェイで構成された DNS サーバーへの最初の照会が解決されない場合、Windows エンドポイントが物理アダプタに設定された DNS サーバーに

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	DNS 照会を送信できるようになります。このオプションは、すべてのアダプタのすべての DNS サーバーを再帰的に照会するネイティブ Windows の動作を保持しますが、一部の DNS 照会を解決するための待機時間が長くなる可能性があります。 GlobalProtect アプリ 4.0.2 およびそれ以前のリリースの DNS 設定を行うには、**Update DNS Settings at Connect**（接続時に **DNS** 設定を更新する）オプションを使用します。
Update DNS Settings at Connect（接続時の DNS 設定の更新） (Windows のみ) (Deprecated (廃止))	（GlobalProtect 4.0.2 およびそれ以前のリリース）GlobalProtect トンネルの DNS サーバー設定を行います。 • **No**（いいえ）（デフォルト）を選択すると、ゲートウェイで構成された DNS サーバーへの最初の照会が解決されない場合、Windows エンドポイントが物理アダプタに設定された DNS サーバーに DNS 照会を送信できるようになります。このオプションは、すべてのアダプタのすべての DNS サーバーを再帰的に照会するネイティブ Windows の動作を保持しますが、一部の DNS 照会を解決するための待機時間が長くなる可能性があります。 • **Yes**（はい）を選択すると、エンドポイントの物理アダプタに設定されている DNS サーバーの代わりに、ゲートウェイで構成した DNS サーバーとのすべての DNS 照会を Windows エンドポイントが解決できるようになります。このオプションを有効にすると、GlobalProtect はゲートウェイの DNS 設定を厳密に適用し、すべての物理アダプタのスタティック設定を上書きします。 この設定を有効にすると（*Yes*（はい））、*GlobalProtect* は以前に保存した *DNS* 設定の復元をさせないために失敗し、その結果、エンドポイントが *DNS* クエリを解決することを防ぎますできなくなります。この機能は廃止され、このシナリオが発生しないように改良された実装に置き換えられています。以前にこの機能を使用していた場合は、*GlobalProtect* アプリ *4.0.3* 以降にアップグレードすることを推奨します。 GlobalProtect アプリ 4.0.3 およびそれ以降のリリースで DNS 設定を行うには、**Resolve All FQDNs Using DNS Servers Assigned by the Tunnel**（トンネルによって割り当てられた **DNS** サーバーを使用するすべての **FQDN** を解決する）オプションを使用します。
Detect Proxy for Each Connection（接続ごとにプロキシを検出） （Windowsのみ）	ポータル接続用のプロキシを自動検出し、以降の接続にそのプロキシを使用する場合は**No**[いいえ] を選択してください。接続のたびにプロキシを自動検出する場合は**Yes**[はい]（デフォルト）を選択してください。
Tunnel Over Proxy をセットアップ（Windows および Mac のみ）	GlobalProtect にプロキシを使用させるか、バイパスさせるか指定します。GlobalProtect にプロキシをバイパスするよう求める場合は**No (いいえ)**を選択します。GlobalProtect にプロキシを使

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
	用するよう求める場合は**Yes (はい)**を選択します。GlobalProtect プロキシの使用に応じて、エンドポイントの OS、トンネル タイプ、ネットワーク トラフィックの挙動が異なります。
Send HIP Report Immediately if Windows Security Center (WSC) State Changes（Windows セキュリティー センター（WSC）の状態が変更された場合に HIP レポートを即座に送信） （Windows のみ）	Windows セキュリティー センター（WSC）の状態が変更された際に、GlobalProtect アプリに HIP データを送信させない場合は **No**（いいえ）を選択してください。WSC の状態が変更された際に即座に HIP データを送信する場合は **Yes**（はい）（デフォルト）を選択します。
Enable Inbound Authentication Prompts from MFA Gateways（MFA ゲートウェイからのインバウンド認証プロンプトの有効化）	多要素認証（MFA）をサポートするには、GlobalProtect エンドポイントはゲートウェイからのインバウンド UDP プロンプトを受信および承認する必要があります。GlobalProtect エンドポイントがプロンプトを受け取り、受信確認できるようにする場合は **Yes**（はい）を選択します。GlobalProtect でゲートウェイからの UDP プロンプトをブロックする場合は **No**（いいえ）（デフォルト）を選択します。
Network Port for Inbound Authentication Prompts (UDP)（インバウンド認証プロンプト用のネットワーク ポート（UDP））	MFA ゲートウェイからのインバウンド認証プロンプトの受け取りに GlobalProtect エンドポイントが使用するポート番号を指定します。デフォルト ポートは 4501 です。ポートを変更するには、1 ~ 65535 の数値を指定します。
Trusted MFA Gateways（信頼された MFA ゲートウェイ）	GlobalProtect エンドポイントが多要素認証において信頼するファイアウォールまたは認証ゲートウェイのリストを指定します。GlobalProtect エンドポイントが指定されたネットワーク ポートで UDP メッセージを受信した場合、UDP プロンプトが信頼されたゲートウェイから来ているときにのみ、GlobalProtect は認証メッセージを表示します。
インバウンド認証メッセージ	追加認証が必要なリソースにユーザーがアクセスしようとしたときに表示する通知メッセージをカスタマイズします。ユーザーが追加認証が必要なリソースにアクセスしようとすると、GlobalProtect はインバウンド認証プロンプトを含む UDP パケットを受信し、このメッセージを表示します。UDP パケットには、Configure Multi-Factor Authentication（多要素認証の設定）時に指定する認証ポータルページの URL も含まれています。GlobalProtect は自動的に URL をメッセージに付加します。以下がその例です。 `You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` メッセージは255文字以下にしてください。
IPv6 優先	GlobalProtect エンドポイントの通信用の優先プロトコルを指定します。優先プロトコルを IPv4 に変更する場合は **No**（いいえ）を選択します。デュアル スタック環境で IPv6 を優先接続にする場合は Yes（はい）（デフォルト）を選択します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
パスワード メッセージを変更	ユーザーが Active Directory (AD) パスワードを変更したときにパスワード ポリシーまたは要件を指定するメッセージをカスタマイズします。以下がその例です。 `Passwords must contain at least one number and one uppercase letter.` 簡体字中国語などの 2 バイトの Unicode 言語の場合、メッセージは 255 文字以下でなければなりません。日本語の場合、メッセージは 128 文字以下にしてください。
起動時にステータスパネルを表示 (Windows のみ)	**Yes (はい)**を選択すると、ユーザーが初めて接続を確立する際に自動的に GlobalProtect のステータスパネルを表示します。**No (いいえ)**を選択すると、ユーザーが初めて接続を確立する際に GlobalProtect のステータスパネルが表示されません。
GlobalProtect アプリの無効化	
パスコード/パスコードの再入力	**Allow User to Disable GlobalProtect App**[ユーザーによるGlobalProtectアプリの無効化] の設定が**Allow with Passcode**[パスコードで許可] の場合、パスコードの入力と再入力を行います。パスコードを記録して安全な場所に保管します。新規のGlobalProtectユーザーに対してパスコードを配布する場合は、電子メールを使用するか、企業ウェブサイトのサポートエリアに掲示する方法があります。 エンドポイントが VPN 接続を確立できず、その機能が使用できない状況であれば、ユーザーはアプリのインターフェイスにこのパスコードを入力して GlobalProtect アプリを無効化し、VPN を使用せずにインターネットへアクセスすることができます。
無効にできる最大回数	ユーザーがファイアウォールへの接続を行う前にGlobalProtectを無効にできる最大回数を指定します。デフォルトの 0 に設定すると、ユーザーは回数の制限を受けることなくアプリを無効化することができます。
タイムアウト満了時間 (分)	GlobalProtect アプリを無効化できる最大の時間を分単位で指定します。ここで指定した時間が経過すると、アプリはファイアウォールへの接続を試みます。デフォルトの0に設定すると、時間の制限を受けることなく無効化することが可能になります。 無効化タイムアウトの値を設定し、ユーザーがアプリを無効化できる期間を制限します。これにより、タイムアウトの期間が過ぎた際に *GlobalProtect* に *VPN* を再び確立させることで、ユーザーおよびユーザーによるリソースへのアクセスを保護することができます。
Uninstall GlobalProtect App (GlobalProtectアプリケーションのアンインストール)	

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリの設定	の意味
パスワード/再入力 パスワード	**Allow User to Uninstall GlobalProtect App** (ユーザーによる **GlobalProtect** アプリのアンインストールを許可する) の設定が **Allow with Password** (パスワードで許可)の場合は、パスワードを入力して確認します。パスワードを記録して安全な場所に保管します。 この設定を使用すると、ユーザーは GlobalProtectアプリケーションをアンインストールできません。設定されている場合、ユーザーは GlobalProtectアプリケーション インターフェイスでこのパスワードを入力して、GlobalProtectアプリケーションをアンインストールする必要があります。
Endpoint Security Managerの設定	
Mobile Security Manager	モバイルデバイス管理（MDM）にGlobalProtect Mobile Security Managerを使用している場合、GP-100アプライアンス上のデバイスチェックイン（登録）インターフェイスのIPアドレスまたはFQDNを入力します。
登録ポート	モバイルエンドポイントが登録のためにGlobalProtect Mobile Security Managerに接続する際に使用するポート番号。Mobile Security Manager はデフォルトでポート 443 をリッスンするように設定されています。 このポート番号のままに設定しておけば、モバイル エンドポイントのユーザーは登録を行う際にクライアント証明書の提示を求められません（使用可能な値は *443*、*7443*、および *8443*）。

GlobalProtect ポータルの *Agent HIP Data Collection*（エージェント *HIP* データ収集）タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Portals** (ポータル) > *<portal-config>* > **Agent** (エージェント) > *<agent-config>* > **HIP Data Collection** (**HIP** データ収集)

HIP Data Collection (**HIP** データ収集)タブを選択し、アプリが HIP レポートでエンドポイントから収集するデータを定義します：

GlobalProtect HIP データ収集設定	の意味
HIP データの収集	アプリに HIP データの収集と送信を行わせたくない場合はこのオプションを解除します。 *GlobalProtect* を有効化し、*HIP* ベースのポリシーを適用するための *HIP* データを収集することで、ファイアウォールがエンドポイントから得た *HIP* データをユーザーが定義して適切なポリシーに適用する *HIP* プロファイルおよび/または *HIP* オブジェクトとマッチできるようにします。

© 2019 Palo Alto Networks, Inc.

GlobalProtect HIP データ収集設定	の意味
Max Wait Time (sec)（最大待機時間（秒））	アプリが HIP データの検索を行う秒数を指定します。この時間が経過すると入手したデータが送信されます（範囲は 10～60、デフォルトは 20）。
証明書プロファイル	GlobalProtect アプリケーションが送信したマシン証明書にマッチさせるために GlobalProtect ポータルが使用する証明書プロファイルを選択します。
カテゴリの除外	アプリによる HIP データ収集の対象外とするホスト情報カテゴリを指定する場合は、**Exclude Categories**（カテゴリの除外）を選択します。HIP収集から除外する**Category**[カテゴリ]（data-loss-preventionなど）を選択します。カテゴリの選択後、特定の Vendor (ベンダー) を **Add**（追加）したのちに、そのベンダーの特定の製品を **Add**（追加）することで、必要に応じて除外内容を詳細に設定することが可能です。各ダイアログの設定を保存する場合は**OK**をクリックします。
カスタム チェック	アプリで収集するカスタムホスト情報を定義する場合は**Custom Checks**（カスタムチェック）を選択します。たとえば、HIPオブジェクト作成対象のVendor [ベンダー] リストやProduct [製品] リストに含まれていない必須アプリケーションがある場合、カスタムチェックを作成して、アプリケーションがインストールされているか（対応するWindowsレジストリキーまたはMac plistキーががあるか）、あるいは実行中か（対応する実行中プロセスがあるかどうか）を判定できます。 • **Windows** — 特定のレジストリキーやキー値のチェックを**Add**[追加] します。 • **Mac** — 特定のplistやキー値のチェックを**Add**[追加] します。 • **Process List**（プロセス リスト） — エンドポイントで実行中かどうかをチェックする対象のプロセスを **Add**（追加）します。たとえば、ソフトウェア アプリケーションが実行しているかどうかを判別するには、実行可能ファイルの名前をプロセス リストに追加します。プロセスは**Windows** タブおよび**Mac**タブのいずれにも追加できます。

GlobalProtect ポータルの Clientless VPN (クライアントレス VPN) タブ

- **Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** > *<portal-config>* > **Clientless VPN (クライアントレス VPN)**

GlobalProtect ポータルを設定して、HTML、HTML5、JavaScript テクノロジを使用する一般的なエンタープライズ Web アプリケーションへの安全なリモート アクセスを提供できるようになりました。ユーザーは GlobalProtect ソフトウェアをインストールすることなく、SSL 対応の Web ブラウザから安全なアクセスを利用できます。これは、パートナーや契約業者をアプリケーションにアクセスできるようにしたり、個人デバイスなどの管理対象外のアセットを安全に利用できるようにしたりしなければならない状況に便利です。この機能を使用する場合、GlobalProtect ポータルからクライアントレス VPN をホストするファイアウォールに GlobalProtect サブスクリプションをインストールする必要があります。以下の表に示すように、**Clientless VPN (クライアントレス VPN)**タブを選択して GlobalProtect Clientless VPN (GlobalProtect クライアントレス VPN) 設定をポータルに設定できます。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのクライアントレス設定	の意味
General [全般] タブ	
クライアントレス VPN	**Clientless VPN**（クライアントレス **VPN**）を選択し、以下のようにクライアントレス VPN セッションの一般的な情報を指定します。
ホスト名	Web アプリケーションのランディング ページをホストする GlobalProtect ポータルの IP アドレスまたは FQDN です。GlobalProtect クライアントレス VPN は、このホスト名でアプリケーション URL を書き直します。 ネットワーク アドレス変換（*NAT*）を使用して *GlobalProtect* ポータルへのアクセスを提供する場合、入力する *IP* アドレスまたは *FQDN* は *GlobalProtect* ポータルの *NAT IP* アドレス（公開 *IP* アドレス）と一致するものであるか、*NAT IP* アドレスに解決できるものである必要があります。
セキュリティゾーン	クライアントレス VPN 設定用のゾーンです。このゾーンで定義されたセキュリティ ルールが、ユーザーがアクセスできるアプリケーションの種類を制御します。
DNSプロキシ	アプリケーション名を解決する DNS サーバーです。**DNS Proxy**（**DNS** プロキシ）サーバーを選択するか、**New DNS Proxy**（新しい **DNS** プロキシ）を設定します（Network（ネットワーク）> DNS Proxy（DNS プロキシ））。
ログイン ライフタイム	クライアントレス SSL VPN セッションの有効期間を、**Minutes**（分）（範囲は 60 ~ 1,440）、または **Hours**（時間）（範囲は 1 ~ 24、デフォルトは 3）の数値で指定します。指定した時間が経過すると、ユーザーは再認証して、新しいクライアントレス VPN セッションを開始しなければなりません。
非アクティビティ タイムアウト	クライアントレス SSL VPN セッションのアイドル状態を許可する期間を、**Minutes**（分）（範囲は 5 ~ 1,440、デフォルトは 30）、または **Hours**（時間）（範囲は 1 ~ 24）の数値で指定します。指定した時間内にユーザーのアクティビティがない場合、ユーザーは再認証して、新しいクライアントレス VPN セッションを開始しなければなりません。
最大ユーザー	同時にポータルにログインさせることができるユーザーの上限です（デフォルトは 10、範囲は 1 以上で上限なし）。ユーザー数の上限に達した場合、以降のクライアントレス VPN ユーザーはポータルにログインできません。
Applications（アプリケーション）タブ	
アプリケーションからユーザーへのマッピング	ユーザーを公開されたアプリケーションに照合する **Applications to User Mapping**（アプリケーションからユーザーへのマッピング）を **Add**（追加）します。このマッピングを通じて、アプリケーションにアクセスするクライアントレス VPNを使用できるユーザーまたはユーザー グループを管理します。アプリケーションおよびアプリケーション グループを定義してから、それらをユーザーにマッピングしてください（Network（ネットワーク）> GlobalProtect > Clientless Apps（クライアントレス アプリケーション）、および Network（ネットワーク）> GlobalProtect > Clientless App Groups（クライアントレス アプリケーション グループ））。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのクライアントレス設定	の意味
	• **Name**（名前）– マッピングの名前を入力します（最大 31 文字）。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。 • **Display application URL address bar** (アプリケーションの **URL** アドレスバーの表示)–ユーザーがアプリのランディング ページに公開されていないアプリを起動するためのアプリケーション URL アドレス バーを表示するには、このオプションを選択します。 有効にすると、ユーザーはページ上の **Application URL**（アプリケーション **URL**）リンクをクリックしてURLを指定できます。
ユーザー/ユーザー グループ	現在のアプリケーション設定の適用対象に個別のユーザーやユーザー グループを **Add**（追加）できます。これらのユーザーは、GlobalProtect クライアントレス VPN を使用して、設定対象のアプリケーションを起動する権限を持ちます。 グループを選択する前にグループ マッピングを設定する必要があります（*Device*（デバイス）> *User Identification*（*User-ID*）> *Group Mapping Settings*（グループ マッピング設定））。 ユーザーやグループだけでなく、これらの設定をユーザーやグループに適用するタイミングを指定できます。 • **any**（すべて）– アプリケーション設定はすべてのユーザーに適用されます（対象ユーザーやユーザー グループを **Add**（追加）する必要はありません）。 • **select**（対象指定）– アプリケーション設定はこのリストに **Add**（追加）したユーザーおよびユーザー グループにのみ適用されます。
アプリケーション [applications]	個別のアプリケーションまたはアプリケーション グループをマッピングに **Add**（追加）できます。設定に追加された **Source Users**（送信元ユーザー）は、GlobalProtect クライアントレス VPN を使用して、追加済みのアプリケーションを起動できます。
Crypto Settings (暗号設定) タブ	
プロトコル バージョン	必要な TLS/SSL バージョンの下限と上限を選択します。TLS バージョンが大きいほど、接続の安全性は高くなります。選択肢には、**SSLv3**、**TLSv1.0**、**TLSv1.1**、**TLSv1.2** が含まれます。
キー交換アルゴリズム	キー交換用のサポート対象アルゴリズム タイプを選択します。選択肢には、**RSA**、Diffie-Hellman（**DHE**）、エフェメラル楕円曲線 Diffie-Hellman（**ECDHE**）が含まれます。
暗号化アルゴリズム	サポート対象の暗号化アルゴリズムを選択します。**AES128** 以上をお勧めします。
認証アルゴリズム	サポート対象の認証アルゴリズムを選択します。選択肢は次の通りです。**MD5**, **SHA1**, **SHA256**, または **SHA384**.**SHA256** 以上をお勧めします。
サーバー証明書の確認	アプリケーションがサーバー証明書を提示したときに発生する可能性がある以下の問題について、対応アクションを有効にします。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのクライアントレス設定	の意味
	• **Block sessions with expired certificate**（証明書が期限切れのセッションをブロック）– サーバー証明書の期限が切れている場合、アプリケーションへのアクセスをブロックします。 • **Block sessions with untrusted issuers**（発行者が信頼されていないセッションをブロック）– サーバー証明書が信頼されていない認証局から発行されたものである場合、アプリケーションへのアクセスをブロックします。 • **Block sessions with unknown certificate status**（証明書の状態が不明なセッションをブロック）– OCSP または CRL サービスが `unknown`（不明）の証明書失効状態を返す場合、アプリケーションへのアクセスをブロックします。 • **Block sessions on certificate status check timeout**（証明書の状態のチェックがタイムアウトしたセッションをブロック）– 証明書の状態のサービスからの応答を受信する前に、証明書の状態のチェックがタイムアウトした場合、アプリケーションへのアクセスをブロックします。
Proxy (プロキシ) タブ	
氏名	GlobalProtect ポータルが公開されたアプリケーションにアクセスするために使用するプロキシサーバーを識別するための、最大 31 文字のラベルです。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
ドメイン	プロキシ サーバーがサービスを提供するドメインを追加します。
プロキシの使用	GlobalProtect ポータルがプロキシ サーバーを使用して公開されているアプリケーションにアクセスできるようにする場合に選択します。
SERVER ポート	プロキシ サーバーのホスト名（または IP アドレス）とポート番号を指定します。
感染 パスワード	プロキシ サーバーへのログインに必要なユーザー名とパスワードを指定します。確認のためにパスワードは再度入力してください。
Advanced Settings (詳細設定) タブ	
除外ドメイン リストのリライト	（任意）**Rewrite Exclude Domain List**（再書き込み除外ドメイン リスト）にドメイン名、ホスト名、またはIP アドレスを **Add**（追加）します。クライアントレス VPN はリバース プロキシとして機能し、公開されているアプリケーションが返すページを変更します。リモート ユーザーがその URL にアクセスすると、要求が GlobalProtect ポータルを通過します。一方、ポータル経由でアクセスする必要のないページがアプリケーションに含まれていることもあります。再書き込みルールから除外し、再書き込みできないようにするドメインを指定してください。 ホストおよびドメイン名では、パスはサポートされません。ホストおよびドメイン名のワイルドカード文字（*）は、名前の最初でのみ使用できます。（*.etrade.com など）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルの Satellite (サテライト) タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Portals** (ポータル) > *<portal-config>* > **Satellite** (サテライト)

サテライトとは、GlobalProtect アプリとして機能して GlobalProtect ゲートウェイへの VPN 接続を確立できるようにする、Palo Alto Networks® ファイアウォール (通常は支社に設置) です。GlobalProtect アプリと同様に、サテライトは、初期設定をポータルから受信します。これには、サテライトがすべての設定済みゲートウェイに接続して VPN 接続を確立できるようにするための証明書と VPN 設定ルーティング情報が含まれます。

支社ファイアウォールにGlobalProtectサテライト設定を定義する前に、WAN接続とのインターフェイスを設定し、セキュリティ ゾーンとポリシーをセットアップして支社LANがインターネットと通信できるようにします。その後、以下の表に示すように、**Satellite (サテライト)**タブを選択してGlobalProtect サテライト設定をポータルに設定できます。

GlobalProtect ポータルのサテライト設定	の意味
一般	• **Name**[名前] – GlobalProtectポータルのサテライト設定につける名前を指定します。 • **Configuration Refresh Interval (hours)**[設定の更新間隔 (時間)] – サテライトデバイスが設定の更新があるかどうかポータルを確認する間隔を指定します (範囲は1 ~ 48時間、デフォルトは24時間) 。
機器	ファイアウォール **Serial Number** (シリアル番号) を使用してサテライトを **Add** (追加) します。ポータルはシリアルナンバーまたはログイン認証情報を使用して接続の要求元を識別することができます。シリアルナンバーを受信できない場合、ポータルはログイン認証情報を要求します。サテライトをファイアウォールシリアルナンバーで識別した場合、サテライトが認証証明書と初期設定を取得するために接続を行う際、ユーザーログイン認証情報を提示する必要はありません。 サテライトがシリアル番号あるいはログイン認証情報を使用して認証を行うと、**Satellite Hostname** (サテライト ホスト名) がポータルに自動的に追加されます。
ユーザー/ユーザー グループの登録	ポータルはシリアル番号を使用して、あるいは使用せずに**Enrollment User/ User Group**[登録ユーザー/登録ユーザーグループ] 設定を使用してサテライトと設定を照合します。シリアル番号が一致しないサテライトは、ユーザー (個人ユーザーまたはグループメンバー) として認証する必要があります。 この設定で制御するユーザーまたはグループを **Add** (追加) します。 設定を特定のグループに制限する場合は、ファイアウォールのグループ マッピングを有効にする必要があります (*Device* (デバイス) > *User Identification* (*User-ID*) > *Group Mapping Settings* (グループ マッピング設定)) 。
ゲートウェイ	**Add**[追加] をクリックして、この設定のサテライトがIPSecトンネルを確立できるゲートウェイのIPアドレスまたはホスト名を入力します。ゲートウェイを設定するインターフェイスの FQDN または IP アドレスを **Gateways**[ゲートウェイ] フィールドに入力します。IP アドレスは、**IPv6**、**IPv4**、またはそれら両方の形で指定できます。デュアル スタック環境で IPv6 接続を指定して優先する場合は、**IPv6 Preferred** (**IPv6** 優先) を選択します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのサテライト設定	の意味
	（任意）設定に複数のゲートウェイを追加している場合、**Routing Priority**（ルーターの優先順位）を使用すると、優先されるゲートウェイをサテライトが選択できます（範囲は 1 ~ 25）。数値が低いほど優先順位が高くなります（使用可能なゲートウェイの場合）。サテライトは、ルーティングメトリックを算出するためにルーティングの優先順位を10倍します。 ゲートウェイによって公開されたルートはスタティック ルートとしてサテライトにインストールされます。スタティックルートのメトリックは、ルーティングの優先順位の*10*倍です。複数のゲートウェイがある場合、必ずルーティングの優先順位も設定して、バックアップゲートウェイによって通知されるルートがプライマリ ゲートウェイによって通知される同じルートよりも高いメトリックになるようにしてください。たとえば、プライマリ ゲートウェイとバックアップ ゲートウェイのルーターの優先順位をそれぞれ *1* と *10* に設定した場合、サテライトは *10* をプライマリ ゲートウェイのメトリックとして使用し、*100* をバックアップ ゲートウェイのメトリックとして使用します。 **Publish all static and connected routes to Gateway**（静的なすべての接続済みルートをゲートウェイに公開）(**Network**（ネットワーク）> **IPSec tunnels**（**IPSec**トンネル）> **<tunnel**（トンネル）> **Advanced**（詳細）—**GlobalProtect Satellite on the <tunnel** > **General**（一般））を選択した場合のみ使用可能）を設定した場合、サテライトはさらにネットワーク情報とルーティング情報をゲートウェイと共有します。
信頼されたルート CA	**Add**[追加] をクリックしてからゲートウェイサーバー証明書を発行するために使用するCA証明書を選択します。サテライトの信頼できるルート CA 証明書は、ポータルのエージェント設定と同時にエンドポイントにプッシュされます。 信頼できるルート *CA* を指定してゲートウェイのサーバー証明書を検証し、*GlobalProtect* ゲートウェイへの安全な *VPN* トンネル接続を確立します。すべてのゲートウェイで同じ発行者を使用してください。 ゲートウェイサーバー証明書の発行の際に使用するルート*CA*証明書がポータル上に存在しない場合、*Import[*インポート*]* または*Generate[*生成*]* が可能です。
クライアント証明書	
ローカル	• **Issuing Certificate**（証明書の発行）— ポータルが使用する証明書を発行するルート CA を選択します。認証が完了するとサテライトに対し証明書が発行されます。必要な証明書がファイアウォールにまだない場合は、**Import**（インポート）または **Generate**（生成）することができます。 証明書がファイアウォールに存在しない場合は、発行証明書を *Import*（インポート）または *Generate*（生成）することができます。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ポータルのサテライト設定	の意味
	• **OCSP Responder**（**OCSP**レスポンダ）– ポータルおよびゲートウェイが提示した証明書の失効状態を検証するためにサテライトが使用する OCSP レスポンダを選択します。ここで **None**（なし）を選択すると、証明書の失効状態の検証に OCSP は使用されません。 証明書が取り消された場合に通知を受け取り、適切な作業を行ってポータルおよびゲートウェイへの接続を保護できるよう、サテライト *OCSP* レスポンダを有効化します。サテライト *OCSP* レスポンダを有効化するには、*Certificate Revocation Checking (*証明書の失効チェック*)* 設定で*CRL*および*OCSP*も有効化する必要があります（*Device (*デバイス*)* > *Setup (*セットアップ*)* > *Session (*セッション*)* > *Decryption Settings (*復号化設定*)*）。 • **Validity Period**（有効期間）（日数）– GlobalProtect サテライト証明書の有効期間を指定します（範囲は 7 ~ 365、デフォルトは 7）。 • **Certificate Renewal Period**（証明書更新期間）（日数）– 証明書有効期間満了の何日前に自動更新を行うかを指定します（範囲は 3 ~ 30、デフォルトは 3）。
SCEP	• **SCEP** – クライアント証明書を生成するための SCEP プロファイルを選択します。プロファイルがドロップダウンリストにない場合、**New**[新規] のプロファイルを作成することができます。 • **Certificate Renewal Period**（証明書更新期間）（日数）– 証明書有効期間満了の何日前に自動更新を行うかを指定します（範囲は 3 ~ 30、デフォルトは 3）。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > Gateways [ネットワーク > GlobalProtect > ゲートウェイ]

GlobalProtect ゲートウェイを設定するには、**Network**（ネットワーク）> **GlobalProtect** > **Gateways**（ゲートウェイ）を選択します。ゲートウェイは GlobalProtect アプリ、または GlobalProtect サテライトに VPN 接続を提供します。

GlobalProtect ゲートウェイのダイアログから新規のゲートウェイ設定を**Add** (追加)するか、既存のゲートウェイ設定を編集する場合はそれを選択します。

確認すべき情報	以下を参照
GlobalProtectゲートウェイ用に設定可能な一般設定	GlobalProtect ゲートウェイの General（全般）タブ
ゲートウェイクライアント認証の設定方法	GlobalProtect ゲートウェイの Authentication（認証）タブ
アプリがゲートウェイと VPN トンネルを確立できるようにトンネルとネットワークを設定する方法	GlobalProtect ゲートウェイの Agent（エージェント）タブ
サテライトがサテライトとして機能するゲートウェイとVPN接続が確立できるようにトンネルとネットワークを設定する方法	GlobalProtect ゲートウェイの Satellite (サテライト) タブ
その他の情報をお探しですか？	ポータルのセットアップ手順の詳細は、『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)』の「Configure GlobalProtect Gateways（GlobalProtect ゲートウェイの設定）」を参照してください。

GlobalProtect ゲートウェイの General（全般）タブ

- **Network**（ネットワーク）> **GlobalProtect** > **Gateways**（ゲートウェイ）> *<gateway-config>* > **General**（全般）

アプリが接続するゲートウェイ インターフェイスを定義し、ゲートウェイがエンドポイントを認証する方法を指定する場合は、**General** (全般)タブを選択します。

GlobalProtect ゲートウェイの一般設定	の意味
氏名	ゲートウェイの名前を入力します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場合、**Location**[場所] はGlobalProtectゲートウェイを使用できる仮想システ

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイの一般設定	の意味
	ム（vsys）になります。マルチ仮想システムモードになっていないファイアウォールの場合、**Location**[場所] フィールドはGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログに表示されません。 ゲートウェイの設定を保存すると、その *Location[場所]* は変更できなくなります。
ネットワーク設定エリア	
インターフェイス	リモートエンドポイント用の入力インターフェイスとして使用するファイアウォールインターフェイスの名前を選択します。（既存のインターフェイスを選択する必要があります） *Telnet*、*SSH*、*HTTP*、または *HTTPS* を許可するインターフェイス管理プロファイルを、*GlobalProtect* ポータルまたはゲートウェイを設定したインターフェイスに接続しないでください。これにより、管理インターフェイスがインターネットに公開されるためです。管理ネットワークへのアクセスを保護する方法の詳細については、Best Practices for Securing Administrative Access（管理アクセスを保護するためのベストプラクティス）を参照してください。
IPアドレス	（任意）ゲートウェイアクセス用のIPアドレスを指定します。**IP Address Type**（**IP** アドレス タイプ）を選択して、**IP Address**（**IP** アドレス）を入力します。 • IP アドレス タイプは、**IPv4**（IPv4 トラフィックのみ）、**IPv6**（IPv6 トラフィックのみ）、または **IPv4 and IPv6**（**IPv4** および **IPv6**）です。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。 IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。**IPv4 and IPv6**（**IPv4** および **IPv6**）を選択した場合、それぞれのタイプに適切なアドレスを入力します。

GlobalProtect ゲートウェイの Authentication（認証）タブ

- **Network**（ネットワーク）> **GlobalProtect** > **Gateways**（ゲートウェイ） > *<gateway-config>* > **Authentication**

SSL/TLSサービスプロファイルを指定し、クライアント認証の詳細を設定する場合は、**Authentication (認証)**を選択します。複数の認証設定を追加することができます。

GlobalProtectゲートウェイの認証設定	
SSL/TLS Service Profile	このGlobalProtectゲートウェイを保護するためのSSL/TLSサービスプロファイルを選択します。サービス プロファイルのコンテンツの詳細については、「Device（デバイス）> Certificate

© 2019 Palo Alto Networks, Inc.

GlobalProtectゲートウェイの認証設定	
	Management（証明書の管理）> SSL/TLS Service Profile（SSL/TLS サービス プロファイル）」を参照してください。
クライアント認証エリア	
氏名	この設定を識別するための一意の名前を入力します。
OS	デフォルトの状態では、この設定がすべてのエンドポイントに適用されます。エンドポイントのリストを OS (**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows**、または **WindowsUWP**)、**Satellite** (サテライト) デバイス、またはサードパーティの IPSec VPN クライアント (**X- Auth**)でさらに詳細に設定することができます。 数ある設定内容は第一にOSにより区別されます。1つのOSに対し複数の設定が必要な場合、認証プロファイルごとに個別の設定を行っていくことが可能です。 設定は、最も詳細なものをリストの一番上に、最も大まかなものを一番下に配置することをお勧めします。
認証プロファイル	ゲートウェイへのアクセスを認証する認証プロファイルまたはシーケンスをドロップダウンリストから選択します。「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照してください。 クライアント認証の場合、必ず 認証プロファイルが *2* 要素認証で *RADIUS* あるいは *SAML* を使用するようにします。*RADIUS* や *SAML* を使用しない場合は、認証プロファイルに加えて証明書プロファイルを設定する必要があります。
Username Label ユーザー名のラベル	GlobalProtect ゲートウェイ ログイン用のカスタム ユーザー名ラベルを指定します。たとえば、ユーザー名（のみ）、またはメールアドレス(**username@domain**)。
パスワード ラベル	GlobalProtect ゲートウェイ ログイン用のカスタム パスワード ラベルを指定します。たとえば、パスワード（トルコ語）またはパスコード（2 重認証、トークンベース認証）
認証メッセージ	このゲートウェイにログインする場合に使用すべき認証情報をエンドユーザに知らせるためのメッセージを入力するか、デフォルトのメッセージのままにしておくことが可能です。メッセージは最大で256文字までです。
ユーザー認証情報あるいはクライアント証明書による認証を許可	**No** (いいえ)を選択すると、ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってゲートウェイに認証する必要があります。**Yes** (はい)を選択すると、ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証できるようになります。

© 2019 Palo Alto Networks, Inc.

GlobalProtectゲートウェイの認証設定	
証明書プロファイル	
証明書プロファイル	（任意）ユーザーのエンドポイントから受信するこれらのクライアント証明書を照合する際にゲートウェイが使用する証明書プロファイルを選択します。証明書プロファイルを使用すると、クライアントの証明書がこのプロファイルと一致する場合にのみゲートウェイがユーザーを認証します。 **Allow Authentication with User Credentials OR Client Certificate (ユーザー認証情報あるいはクライアント証明書による認証を許可)**オプションを**No (いいえ)**に設定する場合は**Certificate Profile (証明書プロファイル)**を選択する必要があります。**Allow Authentication with User Credentials OR Client Certificate (ユーザー認証情報あるいはクライアント証明書による認証を許可)**オプションを**Yes (はい)**に設定する場合、**Certificate Profile (証明書プロファイル)**は任意項目です。 証明書プロファイルはOSの種類に依存しません。

GlobalProtect ゲートウェイの Agent（エージェント）タブ

- **Network**（ネットワーク）> **GlobalProtect** > **Portals** > *<portal-config>* > **Agent**（エージェント）

アプリがゲートウェイと VPN トンネルを確立できるようにするトンネル設定を定義する場合は、**Agent (エージェント)**タブを選択します。さらに、このタブでは VPN のタイムアウト、DNS および WINS のネットワークサービスを指定したり、セキュリティ ポリシー ルールの HIP プロファイルに合致した場合、あるいは合致しなかった場合にエンドユーザーに表示する HIP 通知メッセージを設定できます。

以下のタブでエージェントの設定を行います。

- Tunnel Settings [トンネル設定]タブ
- Client Settings（クライアント設定）タブ
- Client IP Pool（クライアント IP プール）タブ
- Network Services（ネットワーク サービス）タブ
- Connection Settings（接続設定）タブ
- Video Traffic（動画トラフィック）タブ
- HIP Notification（HIP 通知）タブ

Tunnel Settings [トンネル設定]タブ

- **Network (ネットワーク)** > **GlobalProtect** > **Gateways (ゲートウェイ)** > *<gateway-config>* > **Agent (エージェント)** > *<agent-config>* > **Tunnel Settings (トンネル設定)**

Tunnel Settings (トンネル設定)タブを選択してトンネリングを有効化し、トンネルのパラメーターを設定します。

外部ゲートウェイを設定する場合は、トンネルパラメータが必要になります。内部ゲートウェイを設定する場合、トンネルパラメータの設定は必須ではありません。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアントのトンネル モード設定	の意味

トンネル モード	トンネルモードを有効にする場合は、**Tunnel Mode**[トンネルモード] を選択して、以下の設定を指定します。
	• **Tunnel Interface**[トンネルインターフェイス] — ゲートウェイへのアクセス用のトンネルインターフェイスを選択します。
	• **Max User**（最大ユーザー数） — 認証、HIP更新、および GlobalProtect アプリ更新のために同時にゲートウェイにアクセスできるユーザーの最大数を指定します。ユーザーが最大数を超えた場合、ユーザーの最大数に達したことを示すエラーメッセージが表示され、後続のユーザーはアクセスを拒否されます（範囲はプラットフォームによって異なり、フィールドが空の場合に表示されます）。
	• **Enable IPSec**（**IPSec**を有効化） — エンドポイントトラフィックでIPSecモードを使用可能にし、IPSecをプライマリにして、SSL-VPNをフォールバック方式にするには、このオプションを選択します。以下のオプションはIPSecが有効化されるまで使用できません。
	• **GlobalProtect IPSec Crypto**[GlobalProtect の IPSec 暗号] — VPN トンネルの認証および暗号化アルゴリズムを指定する GlobalProtect の IPSec 暗号化プロファイルを選択します。**default**[デフォルト] プロファイルでは、AES-128-CBC暗号化とSHA1認証が使用されます。詳細は、「Network（ネットワーク）> Network Profiles（ネットワーク プロファイル）> GlobalProtect IPSec Crypto（GlobalProtect の IPSec 暗号）」を参照してください。
	• **Enable X-Auth Support**[X-Auth サポートの有効化] — IPSec が有効化されている場合にGlobalProtectゲートウェイのExtended Authentication（X-Auth）サポートを有効にするには、このオプションを選択します。X-Auth サポートにより、X-Auth をサポートするサード パーティ IPSec VPN クライアント (Apple iOS および Android デバイスの IPSec VPN クライアント、Linux の VPNC クライアントなど) は、GlobalProtect ゲートウェイとの VPN トンネルを確立できます。X-Auth オプションにより、VPN クライアントから特定の GlobalProtect ゲートウェイへのリモート アクセスが可能になります。X-Auth アクセスで利用できる GlobalProtect 機能は限定されるため、GlobalProtect アプリケーションを使用することで、GlobalProtect が iOS および Android デバイスに提供するセキュリティ機能セットすべてへのアクセスを簡略化することを検討してください。
	
	X-Auth Support[X-Authサポート] を選択すると**Group Name**[グループ名] および **Group Password**[グループパスワード] のオプションが有効化されます。
	  • グループ名とグループのパスワードが指定されている場合、最初の認証フェーズでは、双方がこの資格証明を使用して認証する必要があります。第2認証フェーズでは有効なユーザー名とパスワードが必要です。認証セクションで設定された認証プロファイルを通じて検証されます。
	  • グループ名とグループ パスワードが定義されていない場合、最初の認証フェーズは、サードパーティ VPN クライアントによって提示された有効な証明書に基づきます。その後この証明書は、認証セクションで設定された証明書プロファイルを通じて検証されます。
	  • デフォルトでは、IPSec トンネルの確立に使用されたキーの有効期限が切れたときに、ユーザーに再認証は要求されません。ユーザーに再認証

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアントのトンネル モード設定	の意味
	を要求する場合は、**Skip Auth on IKE Rekey**[IKEキー再生成での認証をスキップ] の選択を解除します。

Client Settings（クライアント設定）タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Gateways** (ゲートウェイ) > *<gateway-config>* > **Agent** (エージェント) > *<agent-config>* > **Client IP Pool** (クライアント **IP** プール)

GlobalProtect アプリによりゲートウェイとのトンネルを確立する際のエンドポイントの仮想ネットワークアダプタを設定する場合は、**Client Settings** (クライアント設定)タブを開きます。

一部の *Client Settings*（クライアント設定）オプションは、トンネル モードを有効にして、Tunnel Settings（トンネル設定）タブでトンネル インターフェイスを定義した後にのみ使用可能になります。

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
Config Selection Criteria (設定選択条件) タブ	
氏名	クライアント設定の識別に使用する名前（最大31文字）を入力します。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
Source User（送信元ユーザー）	この設定を適用する特定のユーザーまたはユーザーグループを**Add** (追加) します。 ユーザーやユーザー グループを選択する前にグループ マッピングを設定する必要があります（*Device*（デバイス）> *User Identification*（*User-ID*）> *Group Mapping Settings*（グループ マッピング設定））。 この設定をすべてのユーザーにデプロイするには、**Source User** (送信元ユーザー)のドロップダウンリストで**any** (すべて)を選択します。この設定をプレ ログオンモードの GlobalProtect アプリケーションを使用しているユーザーにのみデプロイする場合は、**Source User** (送信元ユーザー)のドロップダウンリストで**pre-logon** (プレ ログオン)を選択します。 ユーザーが*Source User* (送信元ユーザー)、*OS*、および*Source Address* (送信元アドレス)の一致基準にすべてマッチする場合のみ、クライアント設定がデプロイされます。
OS	エンドポイントのオペレーティングシステムに基づいてこの構成を展開するには、次の OS を**Add** (追加) します。**Android**、 **Chrome**、 **iOS**、 **IoT**、 **Linux**、 **Mac**、

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
	Windows、 **WindowsUWP**。また、この値を**Any** (すべて) に設定することで、エンドポイントのオペレーティングシステムに関係なく、ユーザーやユーザーグループごとに設定を適用させることができます。 ユーザーが*Source User* (送信元ユーザー)、*OS*、および*Source Address* (送信元アドレス)の一致基準にすべてマッチする場合のみ、クライアント設定がデプロイされます。
送信元アドレス	ユーザーの場所に基づいてこの設定をデプロイする場合は、送信元の**Region** (地域)あるいはローカル **IP Address** (**IP** アドレス) (IPv4 および IPv6) を**Add** (追加)します。この設定をすべてのユーザーの場所にデプロイする場合、**Region** (地域)や**IP Address** (**IP** アドレス)を指定しないでください。また、この機能は GlobalProtect アプリケーションの古いリリースではサポートされていないため、ユーザーが GlobalProtect アプリケーション 4.0 以前のリリースを実行している場合はこれらのフィールドを空にする必要があります。 接続中のユーザーの場所が*Region* (地域)あるいは*IP Address* (*IP* アドレス)に一致する場合に、*Source Address* (送信元アドレス)のマッチが成功します。 ユーザーが*Source User* (送信元ユーザー)、*OS*、および*Source Address* (送信元アドレス)の一致基準にすべてマッチする場合のみ、クライアント設定がデプロイされます。
Authentication Override (認証オーバーライド) タブ	
認証のオーバーライド	ユーザーが認証プロファイルまたは証明書プロファイルで指定された認証スキームで認証を行ったのちに、ゲートウェイがユーザーの認証を行う際に、保護された、デバイス固有の暗号化されたCookieを使用できるようにします。 • **Generate cookie for authentication override**[認証オーバーライド用Cookieを生成] – Cookieが有効である間、ユーザーがゲートウェイとの認証を行うたびにエージェントはこのCookieを提示します。 • **Cookie Lifetime**[Cookieの有効期間] – Cookieが有効な時間数、日数、あるいは週数を指定します。一般的な有効期間は24時間です。範囲は1 ~ 72時間、1 ~ 52週間、あるいは1 ~ 365日です。Cookieが失効した場合、ユーザーはログイン認証情報を再度入力する必要があり、この入力をうけ、ゲートウェイは新しいCookieを暗号化してユーザーデバイスに送信します。 • **Accept cookie for authentication override**[Cookieによる認証オーバーライドを許可] – ゲートウェイが暗号化されたCookieによる認証を許可するよう設定する場合はこのオプ

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
	ションを選択します。エージェントがCookieを提示すると、ゲートウェイはユーザーを認証する前に、そのCookieが同じゲートウェイ自身が暗号化したものであるかどうかを検証します。 • **Certificate to Encrypt/Decrypt Cookie**[Cookie暗号化/復号化時の証明書] – Cookieの暗号化と復号化を行う際にゲートウェイが使用する証明書を選択します。 *Cookie*の暗号化および復号化用に、ポータルとゲートウェイが共に同じ証明書を使用するよう設定されていることを確認してください。
IP Pools（IP プール）タブ	
認証サーバーからの Framed-IP-Address 属性の取得	GlobalProtectゲートウェイを有効にし、外部認証サーバーを使用して固定IPアドレスを割り当てる場合は、このオプションを選択します。このオプションを有効化した場合、GlobalProtectゲートウェイは、認証サーバーのFramed-IP属性を使用してデバイス接続用のIPアドレスを割り当てます。
認証サーバー IP プール	リモートユーザーに割り当てるIPアドレスのサブネットまたは範囲を**Add**[追加] します。トンネルが確立されると、GlobalProtectゲートウェイは、認証サーバーのFramed-IP-Adress属性を使用してこの範囲のIPアドレスを接続デバイスに割り当てます。IPv4 アドレス（192.168.74.0/24 および 192.168.75.1-192.168.75.100 など）または IPv6 アドレス（2001:aa::1-2001:aa::10 など）を追加できます。 **Retrieve Framed-IP-Address attribute from authentication server**[認証サーバーからのFramed-IP-Adress属性の取得] を有効化している場合にのみ**Authentication Server IP Pool**[認証サーバーIPプール] の設定と有効化が行えるようになります。 認証サーバーの *IP* プールには、すべての同時接続ユーザーをサポートするのに十分な *IP* アドレスが含まれている必要があります。*IP* アドレスは固定的に割り当てられ、ユーザーの接続が切断された後も保持されます。異なるサブネットの複数の範囲を設定し、システムがクライアントの他のインターフェイスと競合しない*IP*アドレスを割り当てられるようにしてください。 ネットワーク内のサーバーおよびルーターは、このIPプールからファイアウォールにトラフィックをルーティングする必要があります。たとえば、ネットワーク192.168.0.0/16では、リモートユーザーは192.168.0.10といったアドレスの割り当てを受けることができます。
IP プール	リモートユーザーに割り当てるIPアドレスの範囲を**Add**[追加] します。トンネルが確立されると、この範囲のアドレスを使用してリモート ユーザーのエンドポイントにインターフェ

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
	イスが作成されます。IPv4 アドレス (192.168.74.0/24 および 192.168.75.1-192.168.75.100 など) または IPv6 アドレス (2001:aa::1-2001:aa::10 など) を追加できます。 競合を回避するには、*IP* プールには、すべての同時接続ユーザーをサポートするのに十分な *IP* アドレスが含まれている必要があります。ゲートウェイでは、クライアントと *IP* アドレスのインデックスが保持されるため、次回接続時に自動的に同じ *IP* アドレスがクライアントに割り当てられます。異なるサブネットの複数の範囲を設定し、システムがクライアントの他のインターフェイスと競合しない*IP*アドレスを割り当てられるようにしてください。 ネットワーク内のサーバーおよびルーターは、このIPプールからファイアウォールにトラフィックをルーティングする必要があります。たとえば、ネットワーク 192.168.0.0/16 では、リモートユーザーに 192.168.0.10 といったアドレスを割り当てることができます。
Split Tunnel (トンネルの分割) タブ	
Access Route (アクセス ルート) タブ	
ローカルネットワークへの直接アクセスなし	Windows および Mac OS システムのローカルネットワークへの直接アクセスを含むスプリットトンネルを無効にする場合は、このオプションを選択します。この機能により、ユーザーがトラフィックをプロキシまたはローカルリソース (ホームプリンタなど) に送信することを防止できます。トンネルが確立されると、すべてのトラフィックはトンネル経由でルーティングされ、ファイアウォールのポリシーが適用されます。
包含	VPN トンネルに含めるルートを **Add** (追加) します。ゲートウェイがこれらのルートをリモート ユーザーのエンドポイントにプッシュして、VPN 接続経由で送信できるユーザー エンドポイントを指定します。 すべてのサブネットあるいはアドレス オブジェクトを含めるには、*0.0.0.0/0* および *::/0* をアクセス ルートとして*Include (*含有*)*します。
除外	VPN トンネルから除外するルートを **Add** (追加) します。これらのルートは、仮想アダプタ (トンネル) ではなく、エンドポイントの物理アダプタ経由で送信されます。 VPN トンネル経由で送信するルートは、トンネルに含めるルート、トンネルから除外するルート、またはその両方の組み合わせの形で定義できます。たとえば、スプリット トンネルを設定し、リモート ユーザーが VPN トンネルを経由せずにインターネットに直接アクセスできるようにすることができます。除外す

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
	るルートは、想定外のトラフィックが除外されることのないように、包含するルートよりも細かく指定してください。 ルートを包含または除外しない場合、すべての要求はトンネル経由でルーティングされます（スプリット トンネルは行われません）。この場合、インターネットの要求はすべてファイアウォールを通過して、ネットワークに出ていきます。この方法により、部外者がユーザーのエンドポイントにアクセスし、そのエンドポイントをブリッジとして利用して社内ネットワークに侵入するのを防ぐことができます。
Domain and Application tab（ドメインとアプリケーション）タブ	
Include Domain（ドメインのインクルード）	ドメインとポートを使用して VPN トンネルに含めるサービス（SaaS）またはパブリック クラウド アプリケーションとしてソフトウェアを追加します（任意）。ゲートウェイがこれらのアプリケーションをリモート ユーザーのエンドポイントにプッシュして、VPN 接続経由で送信できるユーザー エンドポイントを指定します。 各ドメインにポート一覧を設定できます。ポートが設定されていない場合、指定されたドメインのすべてのポートがこのポリシーの対象となります。
Exclude Domain（ドメインを除外する）	ドメインとポートを使用して VPN トンネルから除外するサービス（SaaS）またはパブリック クラウド アプリケーションとしてソフトウェアを追加します（任意）。これらのアプリケーションは、仮想アダプタ（トンネル）ではなく、エンドポイントの物理アダプタで送信されます。 各ドメインにポート一覧を設定できます。ポートが設定されていない場合、指定されたドメインのすべてのポートがこのポリシーの対象となります。 一切のドメインを包含または除外しない場合、すべての要求はトンネル経由でルーティングされます（スプリット トンネルは行われません）。この場合、インターネットの要求はすべてファイアウォールを通過して、ネットワークに出ていきます。この方法により、外部エンドがエンドポイントにアクセスして内部ネットワークにアクセスできなくなる可能性があります。
Include Client Application Process Name（クライアント アプリケーションのプロセス名をインクルード）	アプリケーション プロセス名を使用して VPN トンネルに含めるサービス（SaaS）またはパブリック クラウド アプリケーションとしてソフトウェアを追加します。ゲートウェイがこれらのアプリケーションをリモート ユーザーのエンドポイントにプッシュして、VPN 接続経由で送信できるユーザー エンドポイントを指定します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアント設定およびネットワーク設定	の意味
Exclude Client Application Process Name（クライアント アプリケーションのプロセス名を除外する）	アプリケーション プロセス名を使用して VPN トンネルから除外するサービス（SaaS）またはパブリック クラウド アプリケーションとしてソフトウェアを追加します。これらのアプリケーションは、仮想アダプタ（トンネル）ではなく、エンドポイントの物理アダプタで送信されます。 アプリケーションを包含または除外しない場合、すべての要求はトンネル経由でルーティングされます（スプリット トンネルは行われません）。この場合、インターネットの要求はすべてファイアウォールを通過して、ネットワークに出ていきます。この方法により、外部エンドがエンドポイントにアクセスして内部ネットワークにアクセスできなくなる可能性があります。
[Network Services] タブ	
DNS サーバー	このクライアント設定を持つ GlobalProtect アプリケーションが DNS クエリを送る先となる DNS サーバーの IP アドレスを指定します。各 IP アドレスをコンマで区切れば複数の DNS サーバーを追加できます。
DNS サフィックス	解決できない非修飾ホスト名が入力されたときにエンドポイントがローカルで使用する DNS サフィックスを指定します。カンマで区切って複数の DNS サフィックス（最大 100 個）を入力できます。

Client IP Pool（クライアント IP プール）タブ

- **Network (ネットワーク)** > **GlobalProtect** > **Gateways (ゲートウェイ)** > *<gateway-config>* > **Agent (エージェント)** > *<agent-config>* > **Client IP Pool (クライアント IP プール)**

IPv4 または IPv6 アドレスを GlobalProtect™ ゲートウェイに接続するすべてのエンドポイントに割り当てるために使用されるグローバル IP プールを設定するには、**Client IP Pool (クライアント IP プール)**タブを選択します。

GlobalProtect ゲートウェイ クライアントの IP プール構成設定	の意味
IP プール	リモートユーザーに割り当てる IPv4 または IPv6 アドレスの範囲を**Add**（追加）します。トンネルが確立されると、GlobalProtect ゲートウェイは、そのトンネルを経由してこの範囲の IP アドレスを接続するすべてのエンドポイントに割り当てます。 *IP プールをゲートウェイ レベル（Network（ネットワーク）> GlobalProtect > Gateways（ゲートウェイ）> <gateway-config> > GlobalProtect Gateway Configuration（GlobalProtect ゲートウェイ設定）> Agent（エー*

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアントの IP プール構成設定	の意味
	ジェント) > *Client IP Pool* (クライアント *IP* プール)) で設定する場合は、一切の *IP* プールをクライアント レベル (*Network*ネットワーク) > *GlobalProtect* > *Gateways* (ゲートウェイ) > *<gateway-config>* > *GlobalProtect Gateway ConfigurationGlobalProtect* ゲートウェイ設定) > *Agent* (エージェント) > *Client Settings* (クライアント設定) > *<client-setting>* > *Configs* (構成) > *IP Pools* (*IP* プール)) で設定しないでください。

Network Services (ネットワーク サービス) タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Gateways** (ゲートウェイ) > *<gateway-config>* > **Agent** (エージェント) > *<agent-config>* > **Network Services** (ネットワーク サービス)

GlobalProtect アプリによりゲートウェイとのトンネルを確立する際のエンドポイントの仮想ネットワークアダプタに割り当てられる DNS 設定を行う場合は、**Network Services** (ネットワーク サービス)タブを開きます。

Network Services (ネットワーク サービス) オプションは、トンネル モードを有効にしていて、Tunnel Settings (トンネル設定) タブでトンネル インターフェイスを定義している場合にのみ使用できます。

GlobalProtect ゲートウェイ クライアントのネットワーク サービス設定	の意味
継承ソース	選択された DHCP クライアントまたは PPPoE クライアント インターフェイスから GlobalProtect アプリ設定に、DNS サーバーやその他の設定を配信する継承ソースを選択します。この設定により、DNSサーバーやWINSサーバーなどのすべてのクライアントネットワーク設定は、[継承ソース] で選択されたインターフェイスの設定から継承されます。
継承ソース状態のチェック	クライアントインターフェイスに現在割り当てられているサーバーの設定を参照する場合は、継承ソースをクリックします。
プライマリ DNS セカンダリ DNS	クライアントに DNS を提供するプライマリ サーバーおよびセカンダリ サーバーの IP アドレスを入力します。
プライマリ WINS セカンダリ WINS	エンドポイントに Windows Internet Naming Service (WINS) を提供するプライマリ サーバーおよびセカンダリ サーバーの IP アドレスを入力します。
DNS サフィックスの継承	継承ソースからDNSサフィックスを継承する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアントのネットワーク サービス設定	の意味
DNS サフィックス	解決できない非修飾ホスト名が入力されたときにエンドポイントがローカルで使用するサフィックスを**Add**（追加）します。カンマで区切って複数のサフィックス（最大100個）を入力できます。

Connection Settings（接続設定）タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Gateways** (ゲートウェイ) > *<gateway-config>* > **Agent** (エージェント) > *<agent-config>* > **Connection Settings** (接続設定)

Connection Settings (接続設定)タブを選択し、GlobalProtect™ アプリのタイムアウト設定および認証用 Cookie の使用制限を定義します。

GlobalProtect ゲートウェイ クライアントのトンネルモード接続設定	の意味
Timeout configuration	
ログイン ライフタイム	1 回のゲートウェイ ログイン セッションに許可される日数、時間数、または分数を指定します。
アイドル タイムアウト	未通信状態のセッションが自動的にログアウトされるまでの日数、時間数、または分数を指定します。
アイドル状態での切断	GlobalProtect アプリケーションがトラフィックを VPN トンネル経由でルーティングするのを止めてからエンドポイントがアプリからログアウトするまでに経過する時間（分単位）を指定します。
認証用 Cookie 使用制限	
SSL VPN の自動復元を無効化	このオプションを有効化すると、SSL VPN トンネルの自動復元が行われなくなります。 このオプションを有効化すると、*GlobalProtect* が *Resilient VPN* をサポートしなくなります。
認証用 Cookie 使用制限（VPN トンネルの自動復元あるいは認証のオーバーライド用）	このオプションを有効化すると、次のいずれかの条件に基づいて認証用 Cookie の使用が制限されます： • 認証用 **Cookie** の発効対象である元の送信元 **IP**—認証用 Cookie の使用を、Cookie の元の発効対象であるエンドポイントのパブリックな送信元 IP を持つエンドポイントに制限します。 • 元の送信元 **IP** ネットワーク範囲—認証用 Cookie の使用を、宛先ネットワーク IP アドレス範囲内のパブリックな送信元 IP アドレスを持つエンドポイントに制限します。**Source IPv4 Netmask** (送信元 **IPv4** ネットマスク)を入力して IPv4 アドレスの範囲を指定するか、**Source IPv6 Netmask** (送信元 **IPv6** ネットマスク)を入力して IPv6 アドレスの範囲を指定します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ クライアントのトンネルモード接続設定	の意味
	いずれかのネットマスクを0に設定した場合、指定した IP アドレス タイプでこのオプションが無効になります。例えば、ポータルあるいはゲートウェイがいずれかの IP アドレス タイプ（IPv4 あるいは IPv6）だけをサポートしている、あるいはいずれかの IP アドレス タイプでのみこのオプションを有効化したい場合（ポータルあるいはゲートウェイが IPv4 および IPv6 をサポートしている場合）、ネットマスクを0に設定できます。任意のゲートウェイ設定で一つのネットマスクだけを0に設定できます。両方のネットマスクを同時に0に設定することはできません。 デフォルトの**Source IPv4 Netmask** (送信元 **IPv4** ネットマスク)の値32を採用する場合、Cookie の元の発効対象であるエンドポイントのパブリックな IPv4 アドレスと同じアドレスに認証用 Cookie の使用が制限されます。デフォルトの **Source IPv6 Netmask** (送信元 **IPv6** ネットマスク)の値128を採用する場合、Cookie の元の発効対象であるエンドポイントのパブリックな IPv6 アドレスと同じアドレスに認証用 Cookie の使用が制限されます。

Video Traffic（動画トラフィック）タブ

- **Network** (ネットワーク) > **GlobalProtect** > **Gateways** (ゲートウェイ) > *<gateway-config>* > **Agent** (エージェント) > *<agent-config>* > **Video Traffic** (動画トラフィック)

Video Traffic (動画トラフィック)タブを選択し、VPN トンネルから動画ストリーミングのトラフィックを除外します。

GlobalProtect ゲートウェイ動画トラフィック設定	の意味
トンネルから動画アプリケーションを除外	動画 ストリーミング トラフィックを VPN トンネルから除外できるようにするには、このオプションを選択します。
アプリケーション [applications]	VPN トンネルから除外したい動画ストリーミング アプリケーションを **Add**（追加）または **Browse**（参照）します。 この動画リダイレクトは、次のアプリケーションの動画トラフィック タイプに適用されます。 • Youtube • Dailymotion • Netflix 他の動画ストリーミング アプリケーションでは、次の動画タイプのみをリダイレクトできます。 • MP4 • WebM • MPEG 動画ストリーミング トラフィックは、VPN トンネルからのみ除外できます。動画 ストリーミング アプリケーションを除外しない場合、すべてのリクエストはトンネル経由でルーティングされます（スプリット トンネリングは行わ

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイ動画トラフィック設定	の意味
	れません）。この場合、インターネットの要求はすべてファイアウォールを通過して、ネットワークに出ていきます。この方法により、外部エンドがエンドポイントにアクセスして内部ネットワークにアクセスできなくなる可能性があります。

HIP Notification（HIP 通知）タブ

- **Network (ネットワーク)** > **GlobalProtect** > **Gateways (ゲートウェイ)** > *<gateway-config>* > **Agent (エージェント)** > *<agent-config>* > **HIP Notification (HIP 通知)**

ホスト情報プロファイル（HIP）を含むセキュリティルールが適用された際にエンドユーザーに表示される通知メッセージを定義する場合は**HIP Notification (HIP通知)**タブを開きます。

これらのオプションはHIPプロファイルを作成しセキュリティプロファイルに追加済みの場合のみ使用可能です。

GlobalProtect エージェントの HIP 通知設定	の意味
HIP通知	HIP通知を**Add**[追加] し、オプションを設定します。**Match Message**（一致メッセージ）、**Not Match Message**（不一致メッセージ）のいずれか、あるいは両方の通知を **Enable**（有効化）し、さらに **Show Notification As**（通知の表示方法）を **System Tray Balloon**（システム トレイ バルーン）または **Pop Up Message**（ポップ アップ メッセージ）として表示するかどうかを指定することができます。さらに一致あるいは不一致のメッセージ内容を指定することができます。 これらの設定を使用して、ホストシステムに必須のアプリケーションがインストールされていないことを示す警告メッセージを表示するなど、エンドユーザーにマシンの状態を通知します。Match Message（一致メッセージ）の場合、**Include Mobile App List**（一致したアプリケーションのリストをメッセージに含める）オプションを有効化して、HIP マッチをトリガーしたアプリケーションを表示させることもできます。 *HIP*通知メッセージではリッチ*HTML*形式を使用し、外部の*Web*サイトやリソースへのリンクを含めることができます。 リッチテキスト設定ツールバーのリンク（ ）をクリックして、リンクを追加します。

GlobalProtect ゲートウェイの Satellite (サテライト) タブ

- **Network**（ネットワーク）> **GlobalProtect** > **Gateways**（ゲートウェイ）> *<gateway-config>* > **Satellite (サテライト)**

サテライトとは、GlobalProtect アプリとして機能して GlobalProtectゲートウェイへのVPN接続を確立できるようにする、Palo Alto Networksファイアウォール（通常は支社に設置）です。**Satellite (サテライト)** タブを選択して、ゲートウェイ トンネル設定およびネットワーク設定を定義し、サテライトが VPN 接続を確立できるようにします。また、サテライトが通知するルートを設定することもできます。

- [トンネル設定] タブ

© 2019 Palo Alto Networks, Inc.

- [ネットワーク設定] タブ
- Route Filter (ルート フィルタ) タブ

GlobalProtect ゲートウェイのサテライト設定	の意味
[トンネル設定] タブ	
トンネル設定	**Tunnel Configuration**[トンネル設定] を選択し、ドロップダウンリストから既存の**Tunnel Interface**[トンネルインターフェイス] 、あるいは**New Tunnel Interface**[新規のトンネルインターフェイス] を選択します。詳細は「**Network** (ネットワーク) > **Interfaces** (インターフェイス) > **Tunnel** (トンネル) 」を参照してください。 • **Replay attack detection** (リプレイ攻撃の検出) – リプレイ攻撃から保護します。 *Replay attack detection (*リプレイ攻撃検知)を有効化し、サテライト トンネル設定が有効な場合に *GlobalProtect* サテライトをリプレイ攻撃から保護します。 • **Copy TOS**[TOSのコピー] – 元のTOS (Type of Service) 情報を保持するため、カプセル化されたパケットの内部IPヘッダーから外部IPヘッダーにTOSヘッダーをコピーします。 • **Configuration refresh interval (hours)**[設定の更新間隔 (時間)] – ポータルに設定の更新があるかどうかサテライトデバイスに確認させる間隔を指定します (範囲は1 ~ 48時間、デフォルトは2時間)。
トンネル モニタ	サテライトがゲートウェイトンネル接続をモニターし、接続に失敗した場合にバックアップゲートウェイにフェイルオーバーできるようにする場合は、**Tunnel Monitoring**[トンネルモニタリング] を選択します。 • **Destination Address** (宛先アドレス) – ゲートウェイへの接続があるかどうかを判断するために使用するトンネル モニターの **IPv4** または **IPv6** アドレス (ゲートウェイで保護されるネットワークの IP アドレスなど) を指定します。または、トンネル インターフェイスに IP アドレスを設定した場合はこのフィールドを空白のままにでき、トンネル モニターは代わりにトンネル インターフェイスを使用して接続がアクティブかどうかを判断します。 • **Tunnel Monitor Profile**[トンネル モニター プロファイル] – 別のゲートウェイへの**Failover**[フェイルオーバー]は、LSVPN でサポートされている唯一のトンネル モニタリング プロファイルのタイプです。 *Tunnel Monitoring (*トンネル モニタリング)を有効化してTunnel Monitoring Profile (トンネル モニタリング プロファイル)を設定し、サテライト トンネル設定が有効な場合にフェイルオーバーの動作を制御します。
暗号化プロファイル	**IPSec Crypto Profile**[IPSec暗号化プロファイル] を選択するか、新しいプロファイルを作成します。暗号ファイルにより、VPNトンネルでの識別、認証、および暗号化のためのプロトコルとアルゴリズムが決まります。LSVPNの両方のトンネルエンドポイントが組織内の信頼されるファイアウォールであるので、一般にはESPプロトコル、DH group2、AES 128 CVC暗号化、およびSHA-1認証を使用するデフォルトのプロファイルを使用できます。詳細は「Network (ネットワーク) > Network Profiles (ネットワーク プロファイ

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイのサテライト設定	の意味
	ル) > GlobalProtect IPSec Crypto (GlobalProtect の IPSec 暗号) 」を参照してください。
[ネットワーク設定] タブ	
継承ソース	選択された DHCP クライアントまたは PPPoE クライアント インターフェイスから GlobalProtect サテライト設定に、DNS サーバーやその他の設定を伝搬する継承ソースを選択します。この設定により、DNSサーバーなどのすべてのネットワーク設定は、Inheritance Source [継承ソース] で選択したインターフェイスの設定から継承されます。
プライマリ DNS セカンダリ DNS	サテライトに DNS を提供するプライマリ サーバーおよびセカンダリ サーバーの IP アドレスを入力します。
DNS サフィックス	**Add**[追加] をクリックして、解決できない非修飾ホスト名が入力されたときにサテライトがローカルで使用するサフィックスを入力します。複数のサフィックスをカンマで区切って入力できます。
DNS サフィックスの継承	解決できない非修飾ホスト名が入力されたときに、DNSサフィックスをサテライトに送信してローカルで使用する場合は、このオプションを選択します。
IP プール	このセクションを使用して、VPNトンネルの確立時にサテライトデバイスのトンネルインターフェイスに割り当てるIPアドレスの範囲を**Add**[追加] します。IPv6 または IPv4 アドレスを指定できます。 *IP* プールには、すべての同時接続ユーザーをサポートするのに十分な *IP* アドレスが含まれている必要があります。*IP*アドレスはダイナミックに割り当てられ、サテライトの接続が切断された後は保持されません。異なるサブネットの複数の範囲を設定することにより、システムは、サテライトの他のインターフェイスと競合しない *IP* アドレスをサテライトに割り当てることができます。 ネットワーク内のサーバーおよびルーターは、このIPプールからファイアウォールにトラフィックをルーティングする必要があります。たとえば、ネットワーク 192.168.0.0/16 では、サテライトに 192.168.0.10 といったアドレスを割り当てることができます。 ダイナミック ルーティングを使用している場合、サテライトについて指定した IP アドレスが、ゲートウェイおよびサテライトでトンネル インターフェイスに手動で割り当てた IP アドレスと重複しないようにしてください。
アクセス ルート	**Add**[追加] をクリックして、ルートを以下のように入力します。 • サテライトからのすべてのトラフィックをトンネルを経由してルーティングする場合、このフィールドは空白のままにします。 • 一部のトラフィックのみをゲートウェイ経由でルーティングするには (スプリット トンネルと呼ばれます) 、トンネルする必要のある宛先サブネットを指定します。この場合、サテライトは独自のルーティングテーブルを使用して、指定したアクセスルートの宛先になっていないトラフィックをルーティングします。たとえば、企業ネットワークの宛先になっているト

© 2019 Palo Alto Networks, Inc.

GlobalProtect ゲートウェイのサテライト設定	の意味
	ラフィックのみをトンネルし、ローカルサテライトを使用して安全なインターネットアクセスを可能にすることができます。 • サテライト間のルーティングを有効にするには、各サテライトによって保護されたネットワークのサマリー ルートを入力します。
Route Filter（ルート フィルタ）タブ	
公開されたルートの受け入れ	サテライトによって通知されたルートをゲートウェイのルーティング テーブルに受け入れる場合は、**Accept published routes**（公開されたルートの受け入れ）を有効にします。このオプションを選択しない場合、ゲートウェイはサテライトが通知するルートを受け入れることができません。
許可されたサブネット	サテライトによって通知されるルートの受け入れをさらに制限する場合は、許可するサブネットを **Add**[追加] して、ゲートウェイがルートを受け入れるサブネットを定義します。サテライトによって通知されたサブネットのうち、リストに含まれないものは除外されます。たとえば、LAN 側ですべてのサテライトが、192.168.x.0/24 サブネットで設定されている場合、ゲートウェイでは許可されたルート 192.168.0.0/16 を設定できます。この設定を行うと、ゲートウェイは192.168.0.0/16サブネットにあるサテライトからのみ、ルートを受け入れます。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > MDM [ネットワーク > GlobalProtect > MDM]

Mobile Security Manager を使用してエンド ユーザーのモバイル エンドポイントを管理していて、HIP が有効なポリシーを適用している場合、Mobile Security Manager と通信して管理対象エンドポイントの ＨＩＰ レポートを取得するようにゲートウェイを設定する必要があります。

Mobile Security Manager の MDM 情報を **Add**（追加）して、ゲートウェイで Mobile Security Manager と通信できるようにします。

GlobalProtect MDM 設定	の意味
氏名	Mobile Security Manager の名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
	ファイアウォールがマルチ仮想システムモードに設定されている場合、MDM 設定に Mobile Security Manager を使用可能な仮想システム（vsys）が表示されます。マルチ仮想システムモードに設定されていないファイアウォールの場合、このフィールドは MDM のダイアログに表示されません。Mobile Security Manager を保存すると、その場所を変更できなくなります。
接続設定	
SERVER	ゲートウェイがHIPレポートを取得するために接続する、Mobile Security ManagerのインターフェイスのIPアドレスまたはFQDNを入力します。このインターフェイスへのサービス ルートがあることを確認します。
接続ポート	接続ポートはMobile Security ManagerがHIPレポート要求をリッスンする場所を示します。デフォルトポートは5008です。GlobalProtect Mobile Security Managerはこのポートをリッスンします。サードパーティの Mobile Security Manager を使用する場合、サーバーが HIP レポート要求をリスンするポートの番号を入力します。
クライアント証明書	HTTPS接続を確立する際にゲートウェイがMobile Security Managerに提示するクライアント証明書を選択します。この証明書は、Mobile Security Managerが相互認証を使用するように設定されている場合にのみ必要になります。
信頼されたルート CA	**Add**[追加] をクリックし、HIPレポートを取得するためにゲートウェイが接続するインターフェイスの証明書を発行するために使用されたルートCA証明書を選択します。（このサーバー証明書は Mobile Security Manager のエンドポイント チェックイン インターフェイス用に発効された証明書と異なるものでも構いません。）ルートCA証明書を必ずインポートし、このリストに追加してください。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > Device Block List [ネットワーク > GlobalProtect > デバイスブロックリスト]

GlobalProtect デバイス ブロック リストにエンドポイントを追加するには、**Network**（ネットワーク）> **GlobalProtect** > **Device Block List**（デバイス ブロック リスト）（ファイアウォールのみ）を選択します。リストに追加されたエンドポイントは GlobalProtect VPN 接続を確立することができなくなります。

デバイス ブロック リスト設定	の意味
氏名	デバイスブロックリストの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場合、**Location**[場所] はGlobalProtectゲートウェイを使用できる仮想システム（vsys）になります。マルチ仮想システムモードになっていないファイアウォールの場合、**Location**[場所] フィールドはGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログに表示されません。ゲートウェイの設定を保存すると、その **Location**[場所] は変更できなくなります。
ホストID	エンドポイントを識別できるよう、ホスト名と一意のデバイスIDを組み合わせた一意のIDを入力してください。それぞれのホストIDに対応するホスト名を指定します。
ホスト名	デバイスを識別するホスト名を入力します（最大31文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。

© 2019 Palo Alto Networks, Inc.

Network（ネットワーク） > GlobalProtect > Clientless Apps（クライアントレス アプリケーション）

GlobalProtect クライアントレス VPN を経由してアクセスできるアプリケーションを追加するには、**Network**（ネットワーク） > **GlobalProtect** > **Clientless App**（クライアントレス アプリケーション）を選択します。個々のクライアントレス アプリケーションを追加した後、**Network**（ネットワーク） > **GlobalProtect** > **Clientless App Groups**（クライアントレス アプリケーション グループ）を選択して、アプリケーション グループを定義できます。

GlobalProtect クライアントレス VPN は、HTML、HTML5、および JavaScript テクノロジを使用する一般的なエンタープライズ Web アプリケーションへの安全なリモートアクセスを提供します。ユーザーは GlobalProtect ソフトウェアをインストールすることなく、SSL 対応の Web ブラウザから安全なアクセスを利用できます。これは、パートナーや請負業者によるアプリケーションへのアクセスを有効にする必要がある場合や、管理対象でないアセット（個人用デバイスなど）を安全に有効にする必要がある場合に便利です。

この機能を使用するには、**GlobalProtect** クライアントレス **VPN** の動的更新が必要です。また、GlobalProtect ポータルからクライアントレス VPN をホストしているファイアウォールに GlobalProtect サブスクリプションをインストールする必要があります。

クライアントレス アプリケーション設定	の意味
氏名	アプリケーションの分かりやすい名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
場所	マルチ仮想システムモードになっているファイアウォールの場合、**Location**[場所] はGlobalProtectゲートウェイを使用できる仮想システム（vsys）になります。マルチ仮想システムモードになっていないファイアウォールの場合、**Location**[場所] フィールドはGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログに表示されません。ゲートウェイの設定を保存すると、その **Location**[場所] は変更できなくなります。
アプリケーションのホーム URL	アプリケーションが配置されている URL を入力します（最大 4095 文字）。
アプリケーションの説明	（任意）アプリケーションの説明を入力します（最大 255 文字）。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
アプリケーションのアイコン	（任意）公開するアプリケーション ページでアプリケーションを識別するためのアイコンをアップロードします。アイコンを参照してアップロードすることができます。

© 2019 Palo Alto Networks, Inc.

Network（ネットワーク） > GlobalProtect > Clientless App Groups（クライアントレス アプリケーション グループ）

GlobalProtect クライアントレス VPN を経由してアクセスできるアプリケーションをグループ化するには、**Network**（ネットワーク）> **GlobalProtect** > **Clientless App Groups**（クライアントレス アプリケーション グループ）を選択します。既存のクライアントレス アプリケーションをグループに追加したり、グループの新しいクライアントレス アプリケーションを設定したりできます。複数のアプリケーションを同時に作業する場合にグループは便利です。たとえば、標準の SaaS アプリケーション セット（Workday、JIRA、Bugzilla など）があり、これらをクライアントレス VPN アクセスで設定したいと考える場合があります。

クライアントレス アプリケーション グループ設定	の意味
氏名	アプリケーション グループの分かりやすい名前を入力します（最大 31 文字）。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。
場所	マルチ仮想システムモードになっているファイアウォールの場合、**Location**[場所]はGlobalProtectゲートウェイを使用できる仮想システム（vsys）になります。マルチ仮想システムモードになっていないファイアウォールの場合、**Location**[場所]フィールドはGlobalProtect Gateway [GlobalProtectゲートウェイ] ダイアログに表示されません。ゲートウェイの設定を保存すると、その **Location**[場所] は変更できなくなります。
アプリケーション [applications]	ドロップダウン リストから **Application**（アプリケーション）を **Add**（追加）するか、新しいクライアントレス アプリケーションを設定してグループに追加します。新しいクライアントレス アプリケーションを設定するには、「Network（ネットワーク）> GlobalProtect > Clientless Apps（クライアントレス アプリケーション）」を参照してください。

© 2019 Palo Alto Networks, Inc.

Objects > GlobalProtect > HIP Objects [オブジェクト > GlobalProtect > HIP オブジェクト]

ホスト情報プロファイル（HIP）のオブジェクトを定義するには、**Objects**（オブジェクト）> **GlobalProtect** > **HIP Objects**（**HIP** オブジェクト）を選択します。HIPオブジェクトは、ポリシーを適用する場合に使用する、アプリが送信した生データに対してフィルタをかける際の一致条件を定めるものです。例えば生のホストデータにエンドポイントが所有している数種類のアンチウイルスパッケージに関する情報が含まれる場合に、企業で必要としている特定のアプリに関する情報のみを選別する必要があります。この場合、適用したい特定のアプリケーションに一致するHIPオブジェクトを作成します。

必要なHIPオブジェクトがどれであるか判別する場合は、ホスト情報をどのように使用してポリシーを適用するかを明確化させることをお勧めします。HIPオブジェクト自体は、セキュリティポリシーで使用するHIPプロファイルを作成するための構成要素にすぎないということに注意してください。そのため、オブジェクトをシンプルにし、たとえば、特定のタイプの必須ソフトウェアがあるか、特定のドメインのメンバーか、特定のエンドポイント OS があるかなど、1 つの条件にのみ一致させることが必要になる場合があります。こうすることで、HIPで補完された非常に粒度の細かいポリシーを柔軟に作成することができます。

HIP オブジェクトを作成するには、**Add**[追加] をクリックしてHIP Object [HIP オブジェクト] ダイアログを開きます。各フィールドへの入力内容の説明については、以下の表を参照してください。

- HIP オブジェクトの General（全般）タブ
- HIP オブジェクトの Mobile Device（モバイル デバイス）タブ
- HIP オブジェクトの Patch Management（パッチ管理）タブ
- HIP オブジェクトの Firewall（ファイアウォール）タブ
- HIP オブジェクトの Anti-Malware（アンチマルウェア）タブ
- HIP オブジェクトの Disk Backup（ディスク バックアップ）タブ
- HIP オブジェクトの Disk Encryption（ディスク暗号化）タブ
- HIP オブジェクトの Data Loss Prevention（データ損失防止）
- HIP オブジェクトの Certificate（証明書）タブ
- HIP オブジェクトの Custom Checks（カスタム チェック）タブ

HIP で補完されたセキュリティ ポリシーを作成する方法の詳細は、『*GlobalProtect Administrator's Guide*（*GlobalProtect* 管理者ガイド）』の「Configure HIP-Based Policy Enforcement（HIP ベースのポリシー適用の設定）」を参照してください。

HIP オブジェクトの General（全般）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **General (全般)**

General (全般) タブを選択して、新しい HIP オブジェクトの名前を指定したり、ドメイン、オペレーティング システム、ネットワーク接続のタイプなど、一般的なホスト情報と照合するためのオブジェクトを設定したりします。

HIP オブジェクトの一般設定	の意味
氏名	HIP オブジェクトの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトの一般設定	の意味
共有	**Shared**[共有] を選択した場合、現行のHIPオブジェクトは以下で使用可能になります。 ファイアウォールのすべての仮想システム（vsys）（マルチ仮想システムモードのファイアウォールにログインしている場合）。この選択を解除すると、**Objects**[オブジェクト] タブのドロップダウンリストから選択した **Virtual System**[仮想システム] のみに対してオブジェクトが公開されます。マルチ仮想システムモードに設定されていないファイアウォールの場合、このオプションはHIPオブジェクトのダイアログに表示されません。 Panorama™ のすべてのデバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブのドロップダウンリストから選択した **Device Group**[デバイスグループ] のみに対してオブジェクトが公開されます。 オブジェクトを保存すると、その **Shared**[共有] 設定を変更できなくなります。現在の **Location**（場所）を確認する場合は、 **Objects**（オブジェクト）> **GlobalProtect** > **HIP Objects**（**HIP** オブジェクト）を選択します。
の意味	（任意）説明を入力します。
ホスト情報	ホスト情報を設定する場合のオプションを有効化する場合はこのオプションを選択します。
管理対象	エンドポイントが管理対象かどうかに基づいてフィルタリングします。管理対象のエンドポイントを照合する場合は、**Yes (はい)** を選択します。管理対象以外のエンドポイントを照合する場合は、**No (いいえ)** を選択します。
オーバーライドの無効化（Panoramaのみ)	**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] の子孫デバイス グループのHIPオブジェクトに対するオーバーライドアクセスを制御します。管理者が、継承した値をオーバーライドすることで、オブジェクトのローカルコピーを子孫デバイスグループに作成することを禁止したい場合はこのオプションを選択してください。デフォルトでは、このオプションは解除（オーバーライドが有効化）されています。
ドメイン	ドメイン名による照合を行うには、ドロップダウンリストから演算子を選択して、照合文字列を入力します。
OS	ホストOSによる照合を行う場合は、最初のドロップダウンリストから **Contains**[含む] を選択し、2つ目のドロップダウンリストからベンダーを選択し、3つ目のドロップダウンリストでOSバージョンを選択するか、あるいは**All**[すべて] を選択して、選択したベンダーのすべてのOSバージョンで照合を行うことができます。
クライアント バージョン	特定のバージョン番号による照合を行うには、ドロップダウンリストから演算子を選択して、テキスト ボックスに照合する (または除外する) 文字列を入力します。
ホスト名	特定のホスト名の全体または一部による照合を行うには、ドロップダウンリストから演算子を選択して、テキスト ボックスに照合する (または、選択した演算子によっては除外する) 文字列を入力します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトの一般設定	の意味
ホストID	ホスト ID は、GlobalProtect がホストの識別のために割り当てる、一意の ID です。ホスト ID の値は、デバイス タイプによって異なります。 • **Windows** — レジストリ（HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid）に保存されているマシン GUID • **macOS** — 最初の組み込み物理ネットワーク インターフェイスの MAC アドレス • **Android**—Android ID • **iOS**—UDID • **Linux**—システム DMI テーブルから取得した製品 UUID • **Chrome**— GlobalProtect によって割り当てられた、長さが 32 文字の一意の英数字 特定のホスト ID による照合を行うには、ドロップダウン リストから演算子を選択して、テキスト ボックスに照合する（または、選択した演算子によっては除外する）文字列を入力します。
シリアル番号	エンドポイントのシリアル番号の全体または一部による照合を行うには、ドロップダウンリストから演算子を選択してから、照合文字列を入力します。
ネットワーク	このフィールドを使用して、特定のモバイル デバイス ネットワーク設定によるフィルタリングを有効にします。この一致基準はモバイル デバイスのみに適用されます。 ドロップダウンリストから演算子を選択し、2つ目のドロップダウンリストからフィルタリング基準にするネットワーク接続のタイプを選択します。**Wifi**、**Mobile**[モバイル]、**Ethernet**（**Is Not**[ではない] フィルタの場合のみ選択可能）、または**Unknown**[不明]。ネットワーク タイプを選択したら、指定可能な場合は、追加の照合文字列を入力します。たとえば、モバイル「**Carrier**[通信事業者]」や WiFi「**SSID**」などを指定できます。

HIP オブジェクトの Mobile Device（モバイル デバイス）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **Mobile Device (モバイル デバイス)**

Mobile Device (モバイル デバイス) タブを選択して、GlobalProtect アプリケーションを実行するモバイル デバイスから収集されたデータによる HIP 照合を有効にします。

モバイル デバイスの属性を収集し、*HIP* 実施ポリシーで使用するには、*GlobalProtect* に *MDM* サーバーが必要です。*GlobalProtect* は現在、*AirWatch MDM* サーバーとの *HIP* 統合をサポートしています。

HIP オブジェクトのモバイル デバイス設定	の意味
モバイル デバイス	GlobalProtect アプリが稼動しているモバイル デバイスから収集したホスト データに対するフィルタリングを有効化し、Device（デバイス）、Settings（設定）、および Apps（アプリ）タブを有効化する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトのモバイル デバイス設定	の意味
Device (デバイス) タブ	• **Model**[モデル] — 特定のデバイス モデルによる照合を行うには、ドロップダウンリストから演算子を選択し、照合文字列を入力します。 • **Tag**[タグ] — GlobalProtect Mobile Security Manager に定義されたタグ値による照合を行うには、最初のドロップダウンリストから演算子を選択し、2 つ目のドロップダウンリストからタグを選択します。 • **Phone Number**[電話番号] — デバイスの電話番号の全体または一部による照合を行うには、ドロップダウンリストから演算子を選択し、照合文字列を入力します。 • **IMEI** — IMEI (International Mobile Equipment Identity) による照合を行うには、ドロップダウンリストから演算子を選択し、照合文字列を入力します。
Settings (設定) タブ	• **Passcode**[パスコード] — デバイスにパスコードが設定されているかどうかに基づいてフィルタリングします。パスコードが設定されているデバイスを照合する場合は、**Yes**[はい] を選択します。パスコードが設定されていないデバイスを照合するには、no (いいえ) を選択します。 • **Rooted/Jailbroken**[root 化/jailbreak] — デバイスが root 化または jailbreak されているかどうかに基づいてフィルタリングします。root化またはjailbreakされているデバイスを照合する場合は、**Yes**[はい] を選択します。root化またはjailbreakされていないデバイスを照合する場合は、**No**[いいえ] を選択します。 • **Disk Encryption**[ディスク暗号化] — デバイス データが暗号化されているかどうかに基づいてフィルタリングします。ディスク暗号化が有効なデバイスを照合するには、yes (はい) を選択します。ディスク暗号化が有効ではないデバイスを照合するには、no (いいえ) を選択します。 • **Time Since Last Check-in**[最後のチェックインからの経過時間] — デバイスが最後に MDM にチェックインした日時に基づいてフィルタリングします。ドロップダウンリストから演算子を選択し、チェックイン期間の日数を指定します。たとえば、過去 5 日以内にチェックインされていないデバイスを照合するためのオブジェクトを定義できます。

Apps (アプリ) タブ	• **Apps**[アプリ] — (Androidデバイスのみ) デバイスにインストールされているアプリケーションに基づいて、また、マルウェアに感染したアプリケーションがデバイスにインストールされているかどうかに基づいたフィルタリングを有効にする場合は、このオプションを選択します。
	• **Criteria**[一致条件] タブ
	  • **Has Malware** (マルウェア感染) — マルウェアに感染したアプリがインストールされているデバイスを照合するには、**Yes** (はい) を選択します。マルウェアに感染したアプリがインストールされていないデバイスを照合するには、**No** (いいえ) を選択します。一致条件として **Has Malware** (マルウェア感染) を使用しない場合は、**None** (なし) を選択します。
	• **Include**[含める] タブ
	  • **Package** (パッケージ) — 特定のアプリがインストールされているデバイスを照合するには、アプリを **Add** (追加) して、一意のアプリ名をリバース DNS 形式で入力します。たとえば、com.netflix.mediaclient に続けて、対応するアプリ **Hash** (ハッシュ) を入力します。GlobalProtect アプリはこれを計算し、デバイス HIP レポートで送信します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトの Patch Management（パッチ管理）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **Patch Management (パッチ管理)**

Patch Management (パッチ管理) タブを選択して、GlobalProtect エンドポイントのパッチ状態による HIP 照合を有効にします。

HIP オブジェクトのパッチ管理設定	の意味
パッチ管理	ホストのパッチ管理ステータスに対する照合を有効化し、Criteria (一致条件) およびVendor (ベンダー) タブを有効化する場合はこのオプションを選択します。
Criteria (一致条件) タブ	以下の設定を指定します。 • **Is Installed**[インストール済み] – パッチ管理ソフトウェアがホストにインストールされているかどうかによって照合します。 • **Is Enabled**[有効] – パッチ管理ソフトウェアがホストで有効かどうかによって照合します。**Is Installed**[インストール済み] の選択が解除されている場合、このフィールドは自動的に**none**[なし]に設定され、編集ができなくなります。 • **Severity**（重大度） – 論理演算子のリストから重大度を選択し、指定した重大度値のパッチがホストから欠落しているかどうかを照合します。 GlobalProtect 重大度値と OPSWAT 重大度格付けの間で次のマッピングを使用して、各値の意味を理解してください。 • **0**–低 • **1**–中 • **2**–重要 • **3**–極めて重大 • **Check**[チェック] – エンドポイントのパッチが欠落しているかどうかによって照合します。 • **Patches**[パッチ] – ホストに特定のパッチが適用されているかどうかによって照合します。**Add (追加)**をクリックし、チェックする特定のパッチの KB アーティクル ID を入力します。例えば、Microsoft Office 2010 (KB3128031) 32-Bit Edition の更新をチェックする場合は**3128031**を入力します。
Vendor（ベンダー）タブ	ホスト上で検索して照合する、パッチ管理ソフトウェアや製品の特定のベンダーを定義します。**Add**[追加] をクリックして、ドロップダウンリストから**Vendor**[ベンダー] を選択します。必要に応じて、Add（追加）をクリックして、特定の **Product**（製品）を選択します。**OK** をクリックして設定を保存します。

HIP オブジェクトの Firewall（ファイアウォール）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト) <hip-object>** > *<hip-object>* > **Firewall (ファイアウォール)**

Firewall (ファイアウォール) タブを選択して、GlobalProtect エンドポイントのファイアウォール ソフトウェア状態に基づく HIP 照合を有効にします。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトのファイアウォール設定

ホストのファイアウォールソフトウェア状態による照合を有効化する場合は、**Firewall**[ファイアウォール] を選択します。

- インストール済み — ファイアウォール ソフトウェアがホストにインストールされているかどうかによって照合します。
- **Is Enabled**[有効] — ファイアウォール ソフトウェアがホストで有効かどうかによって照合します。**Is Installed**[インストール済み] の選択が解除されている場合、このフィールドは自動的に**none**[なし]に設定され、編集ができなくなります。
- **Vendor and Product**[ベンダーおよび製品] — ホスト上で検索して照合する特定のファイアウォール ソフトウェア ベンダー/製品を定義します。**Add**[追加] をクリックして、ドロップダウンリストから**Vendor**[ベンダー] を選択します。必要に応じて、**Add**[追加] をクリックして、特定の**Product**[製品]を選択します。**OK** をクリックして設定を保存します。
- **Exclude Vendor**[ベンダーの除外] — 特定のベンダーのソフトウェアがないホストを照合する場合は、このオプションを選択します。

HIP オブジェクトの Anti-Malware（アンチマルウェア）タブ

- **Objects**（オブジェクト）> **GlobalProtect** > **HIP Objects**（**HIP** オブジェクト）> *<hip-object>* > **Anti-Malware (アンチマルウェア)**

Anti-Malware (アンチマルウェア) タブを選択して、GlobalProtect エンドポイントのアンチウイルスあるいはアンチスパイウェア対象範囲に基づく HIP 照合を有効にします。

HIP オブジェクトのアンチマルウェア設定

ホストのアンチウィルスまたはアンチスパイウェア対象範囲に基づいた照合を有効にするには、**Anti-Malware**（アンチマルウェア）を選択します。追加の一致条件を定義します。

- **Is Installed**（インストール済み） — アンチウィルスまたはアンチスパイウェア ソフトウェアがホストにインストールされているかどうかによって照合します。
- **Real Time Protection**（リアルタイム保護）— リアルタイムのアンチウィルスまたはアンチスパイウェア保護がホストで有効かどうかによって照合します。**Is Installed**[インストール済み] の選択が解除されている場合、このフィールドは自動的に**None**[なし]に設定され、編集ができなくなります。
- **Virus Definition Version**[ウイルス定義バージョン] — 指定された日数内にウイルス定義が更新されたかどうか、またはリリースバージョンのどちらに基づいて照合を行うかを指定します。
- **Product Version**（製品バージョン） — アンチウィルスまたはアンチウイルスソフトウェアの特定のバージョンに対して照合を行います。検索するバージョンを指定するには、ドロップダウンリストから演算子を選択して、製品バージョンを表す文字列を入力します。
- 最終スキャン時間 — 最後にアンチウィルスまたはアンチスパイウェア スキャンが実行された時間に基づいて照合を行うかどうかを指定します。ドロップダウンリストから演算子を選択し、照合する**Days**（日）数または**Hours**（時間）数を指定します。
- ベンダーおよび製品 — ホスト上で検索して照合する特定のアンチウィルスまたはアンチスパイウェア ソフトウェア ベンダー/製品を定義します。**Add**（追加）をクリックして、ドロップダウンリストから**Vendor**（ベンダー）を選択します。必要に応じて、**Add**[追加] をクリックして、特定の**Product**[製品]を選択します。**OK** をクリックして設定を保存します。
- **Exclude Vendor**[ベンダーの除外] — 特定のベンダーのソフトウェアがないホストを照合する場合は、このオプションを選択します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトの Disk Backup（ディスク バックアップ）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **Disk Custom Checks (カスタム チェック)**

Disk Backup (ディスク バックアップ) タブを選択して、GlobalProtect エンドポイントのディスク バックアップ状態に基づく HIP 照合を有効にします。

HIP オブジェクトのディスク バックアップ設定
ホストのディスクバックアップ状態による照合を有効にするには、**Disk Backup**[ディスクバックアップ] を選択し、追加の照合条件を以下のように定義します。 • **Is Installed**[インストール済み] — ディスク バックアップ ソフトウェアがホストにインストールされているかどうかによって照合します。 • **Last Backup Time**[最終スキャン時間] — 最後にディスク バックアップが実行された時間に基づいて照合を行うかどうかを指定します。ドロップダウンリストから演算子を選択し、照合する**Days**[日]数または**Hours**[時間]数を指定します。 • **Vendor and Product**[ベンダーおよび製品] — ホスト上で検索して照合する、特定のディスクバックアップ ソフトウェアベンダーまたは製品を定義します。**Add**[追加] をクリックして、ドロップダウンリストから**Vendor**[ベンダー] を選択します。必要に応じて、**Add**[追加] をクリックして、特定の**Product**[製品]を選択します。**OK** をクリックして設定を保存します。 • **Exclude Vendor**[ベンダーの除外] — 特定のベンダーのソフトウェアがないホストを照合する場合は、このオプションを選択します。

HIP オブジェクトの Disk Encryption（ディスク暗号化）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **Disk Encryption (ディスク暗号化)**

Disk Encryption (ディスク暗号化) タブを使用して、GlobalProtect エンドポイントのディスク暗号化状態に基づく HIP 照合を有効にします。

HIP オブジェクトのディスク暗号化設定	の意味
ディスク暗号化	ホストのディスク暗号化状態による照合を有効にする場合は、**Disk Encryption**（ディスク暗号化）を選択します。
基準	以下の設定を指定します。 • **Is Installed**[インストール済み] — ディスク暗号化ソフトウェアがホストにインストールされているかどうかによって照合します。 • **Encrypted Locations**[暗号化された場所] — **Add**[追加] をクリックして、照合時にディスクが暗号化されているかチェックするドライブまたはパスを指定します。 • **Encrypted Locations**[暗号化された場所] — 暗号化されているかどうかをチェックするホスト上の特定の場所を入力します。 • **State**[状態] — 暗号化された場所の状態を照合する方法を指定します。ドロップダウンリストから演算子を選択し、有効な状態 (**full**[フル]、**none**[なし]、**partial**[一部]、**not-available**[使用不可]) を選択します。 **OK** をクリックして設定を保存します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトのディスク暗号化設定	の意味
ベンダー	エンドポイント上で検索して照合する、特定のディスク暗号化ソフトウェアベンダーまたは製品を定義します。**Add**[追加] をクリックして、ドロップダウンリストから**Vendor**[ベンダー] を選択します。必要に応じて、**Add**[追加] をクリックして、特定の**Product**[製品]を選択します。**OK** をクリックして設定を保存し、**Disk Encryption** (ディスク暗号化) タブに戻ります。

HIP オブジェクトの Data Loss Prevention（データ損失防止）

- **Objects** (オブジェクト) > **GlobalProtect** > **HIP Objects** (**HIP** オブジェクト) > *<hip-object>* > **Data Loss Prevention** (データ損失防止)

GlobalProtect エンドポイントがデータ損失防止ソフトウェアを稼働しているか否かに基づいて HIP 照合を設定する場合は、**Data Loss Prevention** (データ損失防止)タブを開きます。

HIP オブジェクトのデータ損失防止設定

ホスト（Windows ホストのみ）のデータ損失防止（DLP）による照合を有効にする場合は、**Data Loss Prevention** (データ損失防止)を選択し、追加の照合条件を以下のように定義します。

- **Is Installed**[インストール済み] – DLP ソフトウェアがホストにインストールされているかどうかによって照合します。
- **Is Enabled**（有効）– DLP ソフトウェアがホストで有効かどうかによって照合します。**Is Installed**[インストール済み] の選択が解除されている場合、このフィールドは自動的に**none**[なし]に設定され、編集ができなくなります。
- **Vendor and Product**[ベンダーおよび製品] – ホスト上で検索して照合する特定の DLP ソフトウェア ベンダー/製品を定義します。**Add**[追加] をクリックして、ドロップダウンリストから**Vendor**[ベンダー] を選択します。必要に応じて、**Add**[追加] をクリックして、特定の**Product**[製品]を選択します。**OK** をクリックして設定を保存します。
- **Exclude Vendor**[ベンダーの除外] – 特定のベンダーのソフトウェアがないホストを照合する場合は、このオプションを選択します。

HIP オブジェクトの Certificate（証明書）タブ

- **Objects**（オブジェクト）> **GlobalProtect** > **HIP Objects**（**HIP** オブジェクト）> *<hip-object>* > **Certificate**（証明書）

Certificate (証明書)タブを選択すれば、証明書プロファイルや他の証明書属性に基づいて HIP マッチを有効化できます。

HIP オブジェクトの証明書設定

Validate Certificate (証明書の検証)を選択すれば、証明書プロファイルおよび証明書属性に基づいてマッチを有効化できます。その後、次のように一致条件を定義します：

- **Certificate Profile** (証明書プロファイル)–HIP レポートで送信されるマシン証明書を検証するために GlobalProtect ゲートウェイが使用する証明書プロファイルを選択します。
- **Certificate Field** (証明書フィールド)–マシン証明書に対してマッチを行うために使用する証明書属性を選択します。

© 2019 Palo Alto Networks, Inc.

HIP オブジェクトの証明書設定
• **Value (値)**—属性の値を設定します。

HIP オブジェクトの Custom Checks（カスタム チェック）タブ

- **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** > *<hip-object>* > **Disk Custom Checks (カスタム チェック)**

Custom Checks (カスタム チェック) タブを選択して、GlobalProtect ポータルに定義されているカスタム チェックに基づく HIP 照合を有効にします。HIP収集にカスタムチェックを追加する方法の詳細は、「Network（ネットワーク）> GlobalProtect > Portals（ポータル）」を参照してください。

HIP オブジェクトのカスタム チェック設定	の意味
カスタム チェック	GlobalProtectポータルに定義されているカスタムチェックによるHIP照合を有効化する場合は、**Custom Checks**[カスタムチェック] を選択します。
プロセス リスト	ホスト システムに特定のプロセスがあるかチェックするには、**Add**[追加] をクリックし、プロセス名を入力します。デフォルトでは、アプリは実行中のプロセスがあるかチェックします。特定のプロセスが実行していないかどうかを確認する場合は、**Running**（実行中）の選択を解除します。プロセスは、オペレーティング システム レベルのプロセスまたはユーザー空間のアプリケーション プロセスとすることができます。
レジストリ キー	Windowsホストに特定のレジストリキーがあるかチェックする場合は、**Add**[追加] をクリックし、照合する **Registry Key**[レジストリキー] を入力します。指定したレジストリ キーまたはキーの値が欠損しているホストのみを照合する場合は、**Key does not exist or match the specified value data**（キーが存在しないか、指定した値データと一致しない）のボックスを選択します。 特定の値を照合するには、**Add**[追加] をクリックし、**Registry Value**[レジストリ値] と **Value Data**[値データ] を入力します。指定された値または値データを明示的に持たないホストを照合するには、**Negate**[除外] を選択します。 **OK** をクリックして設定を保存します。
Plist	Macホストのプロパティリスト（plist）に特定のエントリがあるかチェックする場合は、**Add**[追加] をクリックし、**Plist**名を入力します。指定したplistを持たないホストのみを照合する場合は、**Plist does not exist**[Plistが存在しない] を選択します。 plist 内の特定のキー/値ペアによって照合するには、**Add**[追加] をクリックし、照合する **Key**[キー] と対応する **Value**[値] を入力します。指定されたキーまたは値を明示的に持たないホストを照合する場合は、**Negate**[除外] を選択します。 **OK** をクリックして設定を保存します。

© 2019 Palo Alto Networks, Inc.

Objects > GlobalProtect > HIP Profiles [オブジェクト > GlobalProtect > HIP プロファイル]

HIP が有効化されたセキュリティ ポリシーを設定する場合に使用する HIP プロファイル（モニタリングまたはセキュリティポリシー適用のためにまとめて評価される HIP オブジェクトのコレクション）を作成するには、**Objects**（オブジェクト）> **GlobalProtect** > **HIP Profiles**（**HIP** プロファイル）を選択します。HIPプロファイルを作成する場合は、Booleanロジックを使用し、以前に作成したHIPオブジェクト（と他のHIPプロファイル）を組み合わせることができます。これにより、作成したHIP プロファイルに対してトラフィックフローを評価し、一致か不一致かを判定することができます。一致が見つかった場合、対応するポリシールールが適用されます。一致がなければ、他のポリシー照合条件と同様に、フローは次のルールと照合して評価されます。

HIP プロファイルを作成するには、**Add**[追加] をクリックします。以下の表では、[HIPプロファイル] ダイアログの各フィールドに入力する内容について説明します。HIP で補完されたセキュリティ ポリシーを作成するために GlobalProtect とワークフローをセットアップする方法の詳細は、『*GlobalProtect Administrator's Guide*（*GlobalProtect* 管理者ガイド）』の「Configure HIP-Based Policy Enforcement（HIP ベースのポリシー適用の設定）」を参照してください。

HIP プロファイル設定	の意味
氏名	プロファイルの名前を入力します (最大 **31** 文字)。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
の意味	（任意）説明を入力します。
共有	現在のHIPプロファイルを以下で使用可能にする場合は**Shared**[共有] を選択します。 • ファイアウォールのすべての仮想システム（vsys）（マルチ仮想システムモードのファイアウォールにログインしている場合）。この選択を解除すると、**Objects**[オブジェクト] タブのドロップダウンリストで選択した **Virtual System**[仮想システム] のみに対してプロファイルが公開されます。マルチ仮想システムモードに設定されていないファイアウォールの場合、このオプションはHIPプロファイルのダイアログに表示されません。 • Panorama のすべてのデバイス グループ。この選択を解除すると、**Objects**[オブジェクト] タブのドロップダウンリストで選択した**Device Group**[デバイスグループ] のみに対してプロファイルが公開されます。 プロファイルを保存すると、その **Shared**[共有] 設定を変更できなくなります。現在の **Location**（場所）を確認するには、 **Objects**（オブジェクト）> **GlobalProtect** > **HIP Profiles**（**HIP** プロファイル）を選択します。
オーバーライドの無効化（Panoramaのみ）	このチェック ボックスを使用して、**Objects**[オブジェクト] タブで選択した **Device Group**[デバイスグループ] の子孫デバイスグループのHIPプロファイルへのオーバーライドアクセスを制御します。管理者が、継承した値をオーバーライドすることで、プロファイルのローカルコピーを子孫デバイスグループに作成することを禁止したい場合はこのオプションを選択してください。デフォルトでは、このオプションは解除（オーバーライドが有効化）されています。

© 2019 Palo Alto Networks, Inc.

HIP プロファイル設定	の意味
一致	[条件の追加] をクリックして、[HIP オブジェクト/プロファイル ビルダー] を開きます。 一致条件として使用する最初の HIP オブジェクトまたはプロファイルを選択し、HIP Objects/Profiles Builder (HIP オブジェクト/プロファイル ビルダー) ダイアログの **Match** (一致) テキスト ボックスに追加 (⊞) します。オブジェクトの条件がフローに当てはまらない場合にのみHIPプロファイルでオブジェクトを一致として評価する場合、オブジェクトを追加する前に、**NOT**を選択します。 続けて、作成するプロファイルに必要なだけ一致条件を追加して、追加した条件の間に適切なBoolean演算子 (**AND**または**OR**) を選択します (ここでも必要に応じて**NOT**を使用します)。 複雑なBoolean式を作成する場合は、**Match**[一致] のテキストボックス内の適切な位置に手動でかっこを追加して、HIPプロファイルが意図したロジックを使用して評価されるようにします。たとえば、以下の式は、ホストが FileVault ディスク暗号化 (Mac OSシステム) または TrueCrypt ディスク暗号化 (Windowsシステム) を使用していて、指定されたドメインに属し、Symantec アンチウイルス クライアントをインストールしている場合、そのホストからのトラフィックに HIP プロファイルが一致することを示します。 `((“MacOS” and “FileVault”) or (“Windows” and “TrueCrypt”)) and “Domain” and “SymantecAV”` 新しいHIPプロファイルへのオブジェクトおよびプロファイルの追加が終了したら、**OK**をクリックします。

© 2019 Palo Alto Networks, Inc.

Device > GlobalProtect Client [デバイス > GlobalProtect クライアント]

以下のトピックでは、GlobalProtect アプリのセットアップおよび管理方法について説明します。

確認すべき情報	以下を参照
GlobalProtect ソフトウェアのリリースについての詳細を確認してください。	GlobalProtect エージェントソフトウェアの管理
GlobalProtect ソフトウェアをインストールする。	GlobalProtect エージェントのセットアップ
GlobalProtect ソフトウェアを使用する。	GlobalProtect エージェントの使用
その他の情報をお探しですか？	GlobalProtect クライアント ソフトウェアのセットアップ手順の詳細は、GlobalProtect 管理者ガイドの「GlobalProtect アプリ ソフトウェアのデプロイ」を参照してください。

GlobalProtect アプリ ソフトウェアの管理

ポータルをホストしているファイアウォールに GlobalProtect アプリ ソフトウェアをダウンロードして起動する場合は、**Device**（デバイス）> **GlobalProtect Client**（**GlobalProtect** クライアント）を選択します（ファイアウォールのみ）。以降、ポータルに接続したエンドポイントはアプリ ソフトウェアをダウンロードするようになります。ポータルで指定するエージェント設定では、ポータルがエンドポイントにソフトウェアをプッシュする際の方法とタイミングを定義します。この設定により、アプリが接続した際に自動的にアップグレードが行われるのか、エンドユーザーにアップグレードのプロンプトが表示されるのか、あるいはすべてまたは特定のユーザーに対しアップグレードを禁止するかどうかを決定します。詳細は、「ユーザーによる GlobalProtect アプリのアップグレードを許可」を参照してください。GlobalProtect アプリ ソフトウェアの配布オプションとソフトウェアのデプロイ手順の詳細は、『GlobalProtect Administrator's Guide (GlobalProtect 管理者ガイド)』の「GlobalProtect アプリ ソフトウェアのデプロイ」を参照してください。

GlobalProtect アプリを初めてダウンロードしてインストールする場合、エンドポイントのユーザーは管理者権限でログインする必要があります。その後のアップグレードでは、管理者権限は必要ありません。

GlobalProtect クライアントの設定	の意味
バージョン	このバージョンナンバーは Palo Alto Networks 更新サーバーで入手可能な GlobalProtect アプリ ソフトウェアのバージョンを示しています。Palo Alto Networks から新しいアプリ ソフトウェアリリースを入手可能かどうか確認する場合は、**Check Now**（今すぐチェック）をクリックします。ファイアウォールはサービスルートを使用して更新サーバーに接続し、新しいバージョンの有無をチェックします。適用可能な更新がある場合は、リストの最上部に表示されます。

© 2019 Palo Alto Networks, Inc.

GlobalProtect クライアントの設定	の意味
サイズ	アプリ ソフトウェア バンドルのサイズ。
リリース日	Palo Alto Networks がリリースを公開した日時。
ダウンロード済み	この列にチェック マークがある場合、対応するアプリ ソフトウェア パッケージのバージョンがファイアウォールにダウンロード済みであることを示します。
現在アクティベーション済み	この列にチェック マークがある場合、対応するアプリ ソフトウェア パッケージのバージョンがファイアウォールでアクティブ化済みであり、アプリを接続するとダウンロードできることを示します。一度にアクティブ化できるソフトウェアのバージョンは 1 つのみです。
操作	現在、対応するアプリ ソフトウェア パッケージに対して以下のアクションを実行できることを示します。 • **Download**（ダウンロード） – 対応するアプリ ソフトウェアのバージョンを Palo Alto Networks 更新サーバーから入手可能です。ダウンロードを開始する場合は**Download**[ダウンロード] をクリックします。ファイアウォールがインターネットにアクセスできない場合、インターネットに接続されたコンピュータでカスタマーサポートサイトにアクセスして **Updates** (更新) > **Software Updates** (ソフトウェア更新)を選択し、新しいアプリ ソフトウェア バージョンを検索してローカル コンピュータに**Download**（ダウンロード）します。次にファイアウォールへ アプリ ソフトウェアを手動で**Upload**（アップロード）します。 • **Activate**（アクティベート） – 対応するアプリ ソフトウェア バージョンはファイアウォールにダウンロード済みですが、アプリはまだダウンロードできません。**Activate**（アクティベート）をクリックしてソフトウェアをアクティベートし、アプリをアップグレードできる状態にします。手動でファイアウォールにアップロードしたソフトウェア更新をアクティベートする場合は、**Activate From File**[ファイルからアクティベート] をクリックして、アクティベートするバージョンをドロップダウンリストから選択します（**Currently Activated**[現在アクティベート済み] として表示するには画面の更新が必要になる場合があります）。 • **Reactivate**（再アクティベート） – 対応するアプリ ソフトウェアはアクティベート済みで、クライアントがダウンロードできる状態です。ファイアウォール上で一度にアクティブ化できる GlobalProtect アプリ ソフトウェアのバージョンは1つのみのため、エンドユーザーが現在アクティブなバージョン以外のバージョンにアクセスする必要がある場合、その別のバージョンを**Activate**（アクティベート）して**Currently Active**（アクティベート済み）にする必要があります。
リリース ノート	対応するアプリ バージョンの GlobalProtect リリース ノートへのリンクを提供します。
☒	以前にダウンロードしたアプリ ソフトウェア イメージをファイアウォールから削除します。

© 2019 Palo Alto Networks, Inc.

GlobalProtect アプリのセットアップ

GlobalProtect アプリは、エンドポイントにインストールされ、ポータルとゲートウェイとの GlobalProtect 接続をサポートするアプリケーションです。このアプリは GlobalProtect サービス（PanGP サービス）がサポートします。

ホストのオペレーティング システムで正しいインストール オプション *(32* ビットまたは *64* ビット*)* を選択するようにしてください。*64*ビットのホストにインストールする場合、初期インストールには*64*ビットブラウザと*Java*の組み合わせを使用してください。

アプリをインストールするには、インストーラ ファイルを開いて、画面に表示される指示に従います。

GlobalProtect アプリの使用

GlobalProtect アプリを起動し、GlobalProtect ステータス パネルの設定メニューから **Settings**（設定）を選択すると表示される **GlobalProtect**設定 パネルのタブには、ステータスと設定に関する有用な情報が含まれ、接続の問題のトラブルシューティングに役立つ情報が表示されます。

- 一般タブ—GlobalProtect アカウントに関連付けられているユーザー名とポータルを表示します。このタブからポータルを追加、削除、または変更することもできます。
- **Connection tab**（接続タブ）—GlobalProtect アプリ用に設定されたゲートウェイを表示し、各ゲートウェイに関する次の情報を提供します。
  - Gateway Name（ゲートウェイ名）
  - トンネルのステータス
  - 認証状態
  - 接続タイプ
  - ゲートウェイ IP アドレスまたは FQDN（外部モードでのみ使用可能）

    内部モードの場合、*Connection*（接続）タブには使用可能なゲートウェイ一覧が表示されます。外部モードの場合、*Connection*（接続）タブには接続先のゲートウェイと、ゲートウェイに関する追加の詳細（ゲートウェイの *IP* アドレスや稼働時間など）が表示されます。
- **Host Profile tab**（ホスト プロファイル タブ）—GlobalProtect がホスト情報プロファイル（HIP）を介してセキュリティポリシーを監視および実施するために使用するエンドポイント データを表示します。HIP データをゲートウェイに手動で再送信するには、**Resubmit Host Profile**（ホストプロファイルの再送信）をクリックします。
- **Troubleshooting tab**（トラブルシューティング タブ）— macOS エンドポイントでは、このタブで **Collect Logs**（ログを収集）し、 **Logging Level**（ロギング レベル）を設定できます。Windowsエンドポイントでは、このタブで **Collect Logs**（ログを収集）し、 **Logging Level**（ロギング レベル）を設定し、次の情報を表示してトラブルシューティングを支援します。
  - **Network Configurations**（ネットワーク構成） — 現在のシステム設定を表示します。
  - **Routing Table**[ルーティングテーブル] — GlobalProtect 接続の現在のルート指定方法についての情報を表示します。
  - **Sockets**[ソケット] — 現在アクティブな接続のソケット情報を表示します。
  - **Logs**（ログ） — GlobalProtect アプリとサービスのログを表示することができます。ログ タイプとデバッグ レベルを選択します。**Start**[開始] をクリックするとログが開始し、**Stop**[停止] をクリックするとログが停止します。
- **Notification tab**（通知タブ）—GlobalProtect アプリ上でトリガされる通知の一覧を表示します。特定の通知の詳細を表示するには、通知をダブルクリックします。

Panorama Web インターフェイス

Panorama™ は、Palo Alto Networks® の次世代ファイアウォール製品のための中央管理システムです。Panorama を使用すると、1 つの場所からネットワーク上のすべてのアプリケーション、ユーザー、コンテンツを管理し、ここから得られる情報を使用してネットワークを制御および保護するポリシーを作成することができます。Panorama からポリシーとファイアウォールの中央管理を行うことで、ファイアウォールの分散ネットワークを管理して、運用の効率性を向上させることができます。Panorama は、専用ハードウェア（M-Series）アプライアンス、および VMware バーチャル アプライアンス（ESXi サーバーまたは vCloud Air プラットフォームで稼働）として使用できます。

Panorama Web インターフェイスのビューと設定の大半は、ファイアウォールの Web インターフェイスと同じですが、以下のトピックでは、Panorama、ファイアウォール、ログ コレクタを管理する Panorama Web インターフェイス独自のオプションについて記載します。

- Panorama Web インターフェイスを使用する
- コンテキスト切り替え
- Panorama のコミット操作
- Panorama でのポリシーの定義
- レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティション
- Panorama > Setup（セットアップ）> Interfaces（インターフェイス）
- Panorama > High Availability [Panorama > 高可用性]
- Panorama > Managed WildFire Clusters（管理対象 WildFire クラスタ）
- Panorama > Administrators [Panorama > 管理者]
- Panorama > Admin Roles [Panorama > 管理者ロール]
- Panorama > Access Domains [Panorama > アクセス ドメイン]
- Panorama > Managed Devices（管理対象デバイス）
- Panorama > Managed Devices（管理対象デバイス）> Health（健康状態）
- Panorama > Templates [Panorama > テンプレート]
- Panorama > Device Groups [Panorama > デバイス グループ]
- Panorama > Managed Collectors [Panorama > 管理対象コレクタ]
- Panorama > Collector Groups [Panorama > コレクタ グループ]
- Panorama > Plugins（プラグイン）
- Panorama > VMware NSX
- Panorama > Log Ingestion Profile（ログ インジェスト プロファイル）
- Panorama > Log Settings [Panorama > ログ設定]
- Panorama > Scheduled Config Export [Panorama > スケジュール設定された設定のエクスポート]
- Panorama > Software [Panorama > ソフトウェア]
- Panorama > Device Deployment [Panorama > デバイスのデプロイ]

その他の情報をお探しですか？

中央管理のための Panorama のセットアップや使用の詳細は、『Panorama Administrator's Guide（Panorama 管理者ガイド）』を参照してください。

Panorama Web インターフェイスを使用する

Panorama とファイアウォールの Web インターフェイスの外観は同じです。ただし、Panorama の Webインターフェイスには、Panorama を管理したり、Panorama を使用してファイアウォールやログ コレクタを管理したりするための追加のオプションと Panorama 固有のタブが含まれます。

Panorama のいくつかの Web インターフェイス ページのヘッダーまたはフッターに以下の共通フィールドが表示されます。

Common Field（共通フィールド）	の意味
追加	左側のメニューの上にある **Context**（コンテキスト）ドロップダウン リストを使用して、Panorama の Web インターフェイスとファイアウォールの Web インターフェイスを切り替えることができます（「コンテキスト切り替え」を参照）。
	Dashboard（ダッシュボード）タブと **Monitor**（監視）タブのタブ ヘッダーにある更新（ ）をクリックすると、それらのタブのデータを手動で更新できます。タブ ヘッダーの右側にあるラベルなしのドロップダウン リストを使用して、自動更新間隔を分単位（**1 min**（1 分）、**2 mins**（2 分）、または **5 mins**（5 分））で選択することもできます。自動更新を無効にするには、**Manual**（手動）を選択します。
アクセス ドメイン	アクセス ドメインでは、（**Context**（コンテキスト）ドロップダウン リストを使用して）特定のデバイス グループ、テンプレート、および個々のファイアウォールへのアクセスを定義します。管理者としてログインし、複数のアクセス ドメインが自分のアカウントに割り当てられている場合、**Dashboard**（ダッシュボード）、**ACC**、および **Monitor**（監視）の各タブには、Web インターフェイスのフッターで選択した **Access Domain**（アクセス ドメイン）に関する情報（ログ データなど）のみが表示されます。 アカウントに割り当てられているアクセス ドメインが *1* つのみの場合、*Web* インターフェイスに *Access Domain*（アクセス ドメイン）ドロップダウン リストは表示されません。
デバイス グループ	デバイス グループは、グループとして管理するファイアウォールと仮想システムで構成されます（「Panorama > Device Groups（デバイス グループ）」を参照）。**Dashboard**（ダッシュボード）、**ACC**、および **Monitor**（監視）の各タブには、タブ ヘッダーで選択した **Device Group**（デバイス グループ）に関する情報（ログ データなど）のみが表示されます。**Policies**（ポリシー）タブおよび **Objects**（オブジェクト）タブでは、特定の**Device Group**（デバイス グループ）の設定またはすべてのデバイス グループ（**Shared**（共有）を選択）の設定を指定できます。
テンプレート	テンプレートは、共通のネットワーク設定とデバイス設定を持つファイアウォールのグループであり、テンプレート スタックはテンプレートの組み合わせです（「Panorama > Templates（テンプレート）」を参照）。**Network**（ネットワーク）タブおよび **Device**（デバイス）タブでは、特定の **Template**（テンプレート）またはテンプレート スタックの設定を指定できます。編集できるのは、

© 2019 Palo Alto Networks, Inc.

Common Field（共通フィールド）	の意味
	個々のテンプレート内の設定のみです。そのため、テンプレート スタックを選択した場合、これらのタブ内の設定は読み取り専用で表示されます。
表示基準:デバイス モード	デフォルトでは、**Network**（ネットワーク）タブおよび **Device**（デバイス）タブには、複数の仮想システムと VPN をサポートする、通常の操作モードのファイアウォールで使用できる設定と値が表示されます。ただし、以下のオプションを使用してタブをフィルタリングすることで、編集したいモード固有の設定のみを表示できます。 • **Mode**（モード）ドロップダウン リストで、**Multi VSYS**（マルチ **VSYS**）、**Operational Mode**（操作モード）、および**VPN Mode**（**VPN**モード）オプションを選択または選択解除します。 • 特定のファイアウォールのモード設定を反映するようにすべてのモード オプションを設定するには、**View by**：（閲覧方法：）**Device**（デバイス）ドロップダウン リストでそのファイアウォールを選択します。

Panorama タブには、Panorama とログ コレクタを管理するための以下のページが提供されます。

Panorama ページ	の意味
セットアップ	以下のタスクを実行するには、**Panorama** > **Setup**（セットアップ）を選択します。 • 一般設定（Panorama のホスト名など）と、認証、ログ、レポート、AutoFocus™、バナー、本日のメッセージ、パスワード複雑性に関する設定を指定する。これらの設定は、ファイアウォールで指定する設定（Device（デバイス）> Setup（セットアップ）> Management（管理）を選択）と似ています。 • 設定のバックアップと復元、Panorama の再起動、Panorama のシャット ダウンを行う。これらの操作は、ファイアウォールで実行する操作（Device（デバイス）> Setup（セットアップ）> Operations（操作）を選択）と似ています。 • DNS、NTP、および Palo Alto Networks 更新用サーバーとの接続を定義する。これらの設定は、ファイアウォールで指定する設定（Device（デバイス）> Setup（セットアップ）> Services（サービス）を選択）と似ています。 • Panorama インターフェイス用のネットワーク設定を定義する。Panorama > Setup（セットアップ）> Interfaces（インターフェイス）の順に選択します。 • WildFire™ アプライアンスに関する設定を指定する。これらの設定は、ファイアウォールで指定する設定（Device（デバイス）> Setup（セットアップ）> WildFireを選択）と似ています。 • ハードウェアセキュリティモジュール（HSM）の設定管理これらの設定は、ファイアウォールで指定する設定（Device（デバイス）> Setup（セットアップ）> HSMを選択）と似ています。
HA	一対のPanorama管理サーバーに高可用性（HA）環境を設定します。[Panorama] > [高可用性] の順に選択します。
設定監査	設定ファイル間の差異を確認できます。Device（デバイス）> Config Audit（設定監査）の順に選択します。

© 2019 Palo Alto Networks, Inc.

Panorama ページ	の意味
パスワード プロファイル	Panorama管理者用にパスワードプロファイルを設定することができます。Device（デバイス）> Password Profiles（パスワード プロファイル）の順に選択します。
administrators	Panorama 管理者アカウントを設定できます。Panorama > Administrators（管理者）の順に選択します。 管理者アカウントがロックアウトされている場合、*Administrators*（管理者）ページの *Locked User*（ロックされたユーザー）列にロックが表示されます。このロックをクリックしてアカウントのロックを解除できます。
管理者ロール	Panorama にアクセスする管理者のアクセス権限や役割を制御する管理ロールを定義できます。Panorama > Admin Roles（管理者ロール）の順に選択します。
アクセス ドメイン	デバイス グループ、テンプレート、テンプレート スタック、およびファイアウォールの Webインターフェイスへの管理者アクセスを制御できます。Panorama > Access Domains（アクセス ドメイン）の順に選択します。
認証プロファイル	Panoramaへのアクセスを認証するプロファイルを指定できます。Device（デバイス）> Authentication Profile（認証プロファイル）の順に選択します。
認証シーケンス	Panoramaへのアクセス許可に使用する一連の認証プロファイルを指定できます。Device（デバイス）> Authentication Sequence（認証シーケンス）の順に選択します。
ユーザー ID	User-ID™ エージェントからユーザー マッピング情報を受信するように Panorama を設定できます。[Device] > [ユーザー ID]> [User-ID エージェント] の順に選択します。
管理対象デバイス	ファイアウォールを管理対象デバイスとして Panorama に追加する、ファイアウォールの接続状況とライセンス状態を表示する、ファイアウォールにタグを付ける、ファイアウォールのソフトウェアとコンテンツを更新する、設定のバックアップをロードするなど、ファイアウォールを管理できます。Panorama > Managed Devices（管理対象デバイス）> Summary（サマリー）を選択します。
テンプレート	**Device**（デバイス）タブおよび**Network**（ネットワーク）タブの設定オプションを管理できます。テンプレートとテンプレート スタックを使用すると、同じまたは似た設定を持つ複数のファイアウォールを導入する場合の管理作業を軽減できます。Panorama > Templates（テンプレート）の順に選択します。
デバイスグループ	デバイス グループを設定することで、機能、ネットワーク セグメント、または地理的な場所に基づいてファイアウォールをグループ化できます。デバイス グループには、物理ファイアウォール、仮想ファイアウォール、および仮想システムを含めることができます。 通常、デバイス グループ内のファイアウォールには、類似のポリシー設定が必要です。デバイス グループでは、Panorama の **Policies** [ポリシー]および **Objects** [オブジェクト]タブを使用して、管理対象ファイアウォールのネットワーク全体のポリシーを管理する階層的な手段を実装できます。デバイス グループを最大 4 レベルのツリー階層でネストできます。子孫グループは、先祖グループおよび共有場所のポ

© 2019 Palo Alto Networks, Inc.

Panorama ページ	の意味
	リシーおよびオブジェクトを自動的に継承します。Panorama > Device Groups（デバイス グループ）の順に選択します。
管理対象コレクタ	ログ コレクタを管理できます。Panoramaを使用してログコレクタを設定するため、ログコレクタのことを管理対象コレクタと呼ぶこともあります。管理対象コレクタは、Panorama 管理サーバー（Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンス）にローカルに存在できるほか、専用ログ コレクタ（ログ コレクタ モードの M-Series アプライアンス）とすることができます。[Panorama] > [管理対象コレクタ] の順に選択します。 専用ログ コレクタのソフトウェア更新をインストールすることもできます。 Panorama 管理サーバーを専用ログ コレクタに変換することができます。
コレクタ グループ	コレクタ グループを管理できます。コレクタ グループはログ コレクタを論理的にグループ化するため、設定の適用やファイアウォールの割り当てを一括で行うことができます。Panorama はログをログ コレクタ内のすべてのディスクおよびコレクタ グループ内のすべてのメンバーに均一に分散します。[Panorama] > [コレクタ グループ] の順に選択します。
プラグイン	VMware NSX など、サードパーティ統合用のプラグインを管理できますPanorama > VMware NSX の順に選択します。
VMware NSX	NSX Manager と Panorama 間の通信を有効にすることで、VM-Series ファイアウォールのプロビジョニングを自動化できます。Panorama > VMware NSX の順に選択します。
証明書の管理	証明書、証明書プロファイル、鍵を設定および管理できます。「ファイアウォールおよび Panorama 証明書の管理」を参照してください。
ログ設定	SNMP（Simple Network Management Protocol）トラップ レシーバ、Syslog サーバー、電子メール サーバー、および HTTP サーバーにログを転送できます。[Device] > [ログ設定] の順に選択します。
サーバー プロファイル	Panorama にサービスを提供するさまざまなサーバー タイプのプロファイルを設定できます。以下のいずれかを選択して、特定のサーバー タイプを設定します。 • Device > Server Profiles > Email [デバイス > サーバー プロファイル > 電子メール] • Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP • Device > Server Profiles > SNMP Trap [デバイス > サーバー プロファイル > SNMP トラップ] • Device > Server Profiles > Syslog [デバイス > サーバー プロファイル > Syslog] • Device > Server Profiles > RADIUS [デバイス > サーバー プロファイル > RADIUS] • Device > Server Profiles > TACACS+ [デバイス > サーバー プロファイル > TACACS+] • Device > Server Profiles > LDAP [デバイス > サーバー プロファイル > LDAP] • Device > Server Profiles > Kerberos [デバイス > サーバー プロファイル > Kerberos]

© 2019 Palo Alto Networks, Inc.

Panorama ページ	の意味
	• Device（デバイス）> Server Profiles（サーバー プロファイル）> SAML Identity Provider（SAML アイデンティティ プロバイダ）
スケジュールされた設定のエクスポート	Panorama とファイアウォールの設定を FTP サーバーや Secure Copy（SCP）サーバーに毎日エクスポートできます。Panorama > Scheduled Config Export（スケジュールされた設定のエクスポート）の順に選択します。
software	Panorama ソフトウェアを更新できます。[Panorama] > [ソフトウェア] の順に選択します。
ダイナミック更新	最新のアプリケーション定義や、アンチウイルス シグネチャ（脅威阻止ライセンスが必要）などの新しいセキュリティ上の脅威に関する情報を表示し、新しい定義で Panorama を更新できます。[Device] >[ダイナミック更新] の順に選択します。
support	Palo Alto Networks社の製品およびセキュリティ警告にアクセスできます。Device（デバイス）> Support（サポート）の順に選択します。
デバイスのデプロイ	ファイアウォールやログ コレクタにソフトウェアやコンテンツの更新をデプロイできます。Panorama > Device Deployment（デバイスのデプロイ）の順に選択します。
マスターキーおよび診断	Panoramaで秘密鍵を暗号化するためのマスターキーを指定できます。デフォルトでは、新しいマスター キーを指定しなくても、Panorama は秘密鍵を暗号化形式で保管します。Device（デバイス）> Master Key and Diagnostics（マスター キーおよび診断）の順に選択します。

© 2019 Palo Alto Networks, Inc.

コンテキスト切り替え

各 Panorama Web インターフェイス ページのヘッダーで、左側のメニューの上にある **Context**（コンテキスト）のドロップダウン リストから、Panorama Web インターフェイスとファイアウォール Web インターフェイスを切り替えることができます。ファイアウォールを選択するとWeb インターフェイスが更新され、選択したファイアウォールのすべてのページとオプションが表示されるので、ローカルで管理を行うことができます。ドロップダウン リストには、管理アクセス権のあるファイアウォール（Panorama > Access Domains（アクセス ドメイン）を参照）のうち、Panorama に接続されているファイアウォールのみが表示されます。

フィルタを使用すると、プラットフォーム（モデル）、デバイス グループ、テンプレート、タグ、HA 状態ごとにファイアウォールを検索できます。フィルタ バーにテキスト文字列を入力して、デバイス名ごとに検索することもできます。

高可用性 (HA) モードにあるファイアウォールのアイコンは、HA 状態を示す色付きの背景で表示されます。

© 2019 Palo Alto Networks, Inc.

Panorama のコミット操作

Web インターフェイスの右上にある **Commit**（コミット）をクリックし、Panorama 設定の保留中の変更や、Panorama がファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライアンスにプッシュする変更の操作を選択します。

- **Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）— Panorama 管理サーバーの設定で行った変更をアクティベーションします。また、このアクションでは、デバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライアンスの変更をファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライアンスにプッシュすることなく Panorama 設定にコミットします。Panorama 設定にのみコミットすることで、ファイアウォール、ログ コレクタ、WildFire クラスタおよびアプライアンスでまだアクティベーションの準備ができていない変更を保存できます。

  Panorama 8.0 以降のリリースでは、設定を管理対象デバイスにプッシュすると、実行中の設定（*Panorama* にコミットされた設定）がプッシュされます。*Panorama 7.1* 以前のリリースでは、コミットされていない変更が含まれる候補設定がプッシュされます。そのため、*Panorama 8.0* 以降のリリースでは、最初に変更を *Panorama* にコミットしないと、管理対象デバイスに変更をプッシュできません。
- **Commit**（コミット）> **Push to Devices**（デバイスにプッシュ）— Panorama の実行中の設定をデバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライアンスにプッシュします。
- **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）— すべての設定変更をローカルの Panorama 設定にコミットしてから、Panorama の実行中の設定をデバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタおよびアプライアンスにプッシュします。

保留中の変更を管理者または場所でフィルタリングし、それらの変更のみをコミット、プッシュ、検証、またはプレビューできます。場所は、特定のデバイス グループ、テンプレート、コレクタ グループ、ログ コレクタ、WildFire アプライアンスおよびクラスタ、共有設定、Panorama 管理サーバーになります。

変更をコミットすると、実行中の設定の一部になります。コミットされていない変更は、候補設定の一部になります。Panorama はコミット要求をキューで処理するので、前回のコミットの進行中に新しいコミットを追加することができます。Panorama は追加された順番でコミットを実行しますが、Panorama が追加した自動コミット（FQDN 更新など）を優先的に行います。ただし、管理者が開始したコミットがすでにキューの上限まで追加されている場合、新しいコミットを行う前に、Panorama が保留中のコミットを完了するまで待つ必要があります。タスク マネージャ（Tasks）を使用してコミットのキューをクリアしたり、コミットの詳細を確認することができます。設定変更、コミットプロセス、コミット検証、コミットキューの詳細についてはPanoramaのコミット及び検証作業を参照してください。また、候補設定の保存、変更の取り消し、ローカル設定のインポート、エクスポート、ロードを行うこともできます（Device（デバイス）> Setup（セットアップ）> Operations（操作））。

以下のオプションを使用して、設定変更のコミット、検証、またはプレビューを行うことができます。

フィールド/ボタン	の意味
以下のオプションは、**Commit**（コミット）> **Commit to Panorama**（**Panorama** にコミット）または **Commit**（コミット）> **Commit and Push**（コミットしてプッシュ）を選択して Panorama にコミットする場合に適用されます。	
すべての変更のコミット	管理権限対象のすべての変更をコミットします（デフォルト）。このオプションを選択するときに、Panorama がコミットする設定変更のスコープを手動でフィルタリングすることはできません。代わりに、ロ

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	グインに使用しているアカウントに割り当てられた管理者ロールによって、コミット スコープが指定されます。 • **Superuser role**（スーパーユーザー ロール）– Panorama はすべての管理者の変更をコミットします。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によってコミット スコープが決まります（Panorama > Admin Roles（管理者ロール））。プロファイルに **Commit For Other Admins**（他の管理者のコミット）の権限が含まれている場合、Panorama はすべての管理者が設定した変更をコミットします。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者のコミット）の権限が含まれていない場合、Panorama はその管理者の変更のみをコミットし、他の管理者の変更はコミットしません。 アクセス ドメインを実装している場合、Panorama はそれらのドメインを自動的に適用して、コミット スコープをフィルタリングします（「Panorama > Access Domains（アクセス ドメイン）」を参照）。管理ロールに関係なく、Panorama はアカウントに割り当てられたアクセス ドメインの設定変更のみをコミットします。
指定対象による変更のコミット	Panorama がコミットする設定変更のスコープをフィルタリングします。ログインに使用しているアカウントに割り当てられた管理ロールによって、フィルタリング オプションが決まります。 • **Superuser role**（スーパーユーザー ロール）– 特定の管理者による変更や、特定の場所における変更へとコミット スコープを制限できます。 • **Custom role**（カスタム ロール）– アカウントに割り当てられた管理者ロール プロファイルの権限によってフィルタリング オプションが決まります（Panorama > Admin Roles（管理者ロール））。プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれている場合、特定の管理者による変更や特定の場所における変更に、コミット スコープを制限できます。管理者ロール プロファイルに **Commit For Other Admins**（他の管理者向けのコミット）の権限が含まれていない場合、コミット スコープは、本人が特定の場所で加えた変更にしか制限できません。 コミット スコープを以下のようにフィルタリングします。 • **Filter by administrator**（管理者によるフィルタリング）– 他の管理者の変更をコミットできるロールの場合でも、デフォルトでコミット スコープに含まれているのは本人の変更のみです。他の管理者をコミット スコープに追加するには、*<usernames>*（ユーザー名）リンクをクリックして、管理者を選択し、**OK** をクリックします。 • **Filter by location**（場所によるフィルタリング）– 変更の特定の場所を選択して、Include in Commit（コミットに含める）を有効にします。 アクセス ドメインを実装している場合、Panorama はそれらのドメインに基づいてコミット スコープを自動的にフィルタリングします（「Panorama > Access Domains（アクセス ドメイン）」を参照）。管理ロールやフィルタリングの選択に関係なく、コミット スコープにはアカウントに割り当てられたアクセス ドメインの設定変更のみが含まれます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	設定をロードした（Device（デバイス）> Setup（セットアップ）> Operations（操作））後、*Commit All Changes*（すべての変更のコミット）を行ってください。 デバイス グループへの変更をコミットする場合、そのデバイス グループの同じルールベースのルールを追加、削除、または順序変更を行ったすべての管理者の変更を含める必要があります。
コミット スコープ	コミットする変更を含む場所を一覧表示します。リストに含まれるのが変更のすべてであるか一部であるかは、複数の要因が影響します。詳細は、「Commit All Changes（すべての変更のコミット）」および「Commit Changes Made By（指定対象による変更のコミット）」に記載されています。場所の種類は以下のとおりです。 • **shared-object**（共有オブジェクト）– 共有の場所で定義されている設定です。 • *<device-group>*（デバイス グループ）– ポリシー ルールまたはオブジェクトが定義されているデバイス グループの名前。 • *<template>*（テンプレート）– 設定が定義されているテンプレートまたはテンプレート スタックの名前。 • *<log-collector-group>*（ログ コレクタ グループ）– 設定が定義されているログ コレクタ グループの名前。 • *<log-collector>*（ログ コレクタ）– 設定が定義されているログ コレクタの名前。 • *<wildfire-appliances>* – 設定が定義されている WildFire アプライアンスのシリアル番号。 • *<wildfire-appliance-clusters>* – 設定が定義されている WildFire クラスタの名前。
場所タイプ	この列では保留中の変更の場所が分類されます。 • **Panorama** – Panorama 管理サーバー設定固有の設定。 • **Device Group**（デバイス グループ）– 特定のデバイス グループで定義されている設定。 • **Template**（テンプレート）– 特定のテンプレートまたはテンプレート スタックで定義されている設定。 • **Log Collector Group**（ログ コレクタ グループ）– コレクタ グループ設定固有の設定。 • **Log Collector**（ログ コレクタ）– ログ コレクタ設定固有の設定。 • **WildFire Appliance Clusters**（**WildFire** アプライアンス クラスタ）– WildFire アプライアンス クラスタ設定固有の設定。 • **WildFire Appliances**（**WildFire** アプライアンス）– WildFire アプライアンス固有の設定。 • **Other Changes**（その他の変更）– 前述の設定エリア（共有オブジェクトなど）に固有でない設定。
コミットに含める （部分的なコミットのみ）	コミットする変更を選択できます。デフォルトでは、**Commit Scope**（コミット スコープ）のすべての変更が選択されています。この列は、特定の管理者に基づく **Commit Changes Made By**（指定対象による変更のコミット）を選択しないと表示されません。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	依存関係が、コミットに含める変更に影響する場合があります。たとえば、オブジェクトの追加後に、別の管理者がそのオブジェクトを編集した場合、その別の管理者の変更のコミットは、自身の変更も合わせてコミットしない限りできません。
Group by Type（タイプ別にグループ化）	**Commit Scope**（コミット スコープ）の設定変更のリストを **Location Type**（場所タイプ）別にグループにします。
プレビューの変更	**Commit Scope**（コミット スコープ）で選択した設定を、実行中の設定と比較できるようにします。プレビュー ウィンドウでは色分けによって詳細が示されます（追加は緑色、変更は黄色、削除は赤色）。 Web インターフェイスのセクションへの変更を一致させる場合、変更前後の **Lines of Context**（コンテキストの行）を表示するようにプレビュー ウィンドウを設定できます。これらは候補のファイルと、比較対象である実行中の設定から取得されます。 プレビュー結果は新しいブラウザ ウィンドウで表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビュー ウィンドウが開かない場合は、ポップアップを許可する手順についてブラウザのドキュメントを参照してください。
変更サマリー	変更をコミットする個別の設定を一覧表示します。**Change Summary**（変更サマリー）のリストでは、各設定の以下の情報が表示されます。 • **Object Name**（オブジェクト名）– ポリシー、オブジェクト、ネットワーク設定、またはデバイス設定を識別する名前です。 • **Type**（タイプ）– 設定のタイプ（アドレス、セキュリティ ルール、ゾーンなど）です。 • **Location Type**（場所タイプ）– 設定が定義されている場所（**Device Groups**（デバイス グループ）、**Templates**（テンプレート）、**Collector Groups**（コレクタ グループ）、**WildFire Appliances**（**WildFire** アプライアンス）、または **Wildfire Appliance Clusters**（**WildFire** アプライアンス クラスタ））を示します。 • **Location**（場所）– 設定が定義されているデバイス グループ、テンプレート、コレクタ グループ、WildFire クラスタまたは WildFire アプライアンスの名前。これらの場所で定義されていない設定の列には、**Shared**（共有）が表示されます。 • **Operations**（操作）– 最後のコミット以降、設定に実施された各操作（作成、編集、または削除）を示します。 • **Owner**（オーナー）– 設定に直近の変更を加えた管理者です。 • **Will Be Committed**（コミット対象）– 設定がコミットに含まれるかどうかを示します。 • **Previous Owners**（前回のオーナー）– 直近の変更前に、設定を変更した管理者です。 必要に応じて、**Group By**（グループ化基準）を列名（**Type**（タイプ）など）にできます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
コミットの検証	Panorama 設定の構文が正しく、完全な意味を成しているかどうかを検証します。出力には、コミットが表示するであろうエラーや警告が含まれます。これにはルール シャドウイングやアプリケーション依存関係の警告があります。検証プロセスを利用すると、エラーを検出、修正してからコミットできます (実行中の設定は変更されません)。固定のコミット ウィンドウがあり、エラーなしでコミットを確実に実行したい場合に便利です。
以下のオプションは、**Commit** (コミット) > **Push to Devices** (デバイスにプッシュ) または **Commit** (コミット) > **Commit and Push** (コミットしてプッシュ) を選択して設定変更を管理対象デバイスにプッシュする場合に適用されます。	
スコープのプッシュ	プッシュする変更のある場所を表示します。デフォルトでスコープに含まれる場所は、以下のどのオプションを選択するかによって異なります。 • **Commit** (コミット) > **Commit and Push** (コミットしてプッシュ) – スコープには、Panorama コミットを必要とする変更のあるすべての場所が含まれます。 • **Commit (コミット)** > **Push to Devices (デバイスにプッシュ)** – スコープには、Panorama の実行中の設定と同期していないエンティティ (ファイアウォール、仮想システム、ログ コレクタ、WildFire クラスタ、WildFire アプライアンス) に関連付けられたすべての場所が含まれます (同期状態については、「Panorama > Managed Devices (管理対象デバイス) > Summary (サマリー)」および「Panorama > Managed Collectors (管理対象コレクタ)」を参照)。 どちらを選択しても、Panorama は以下で **Push Scope** (プッシュ スコープ) をフィルタリングします。 • **Administrators** (管理者) – Panorama は、**Commit Scope** (コミット スコープ) と同じフィルタを適用します (「Commit All Changes (すべての変更のコミット)」または「Commit Changes Made By (指定対象による変更のコミット)」を参照)。 • **Access domains** (アクセス ドメイン) – アクセス ドメインを実装している場合、Panorama はそれらのドメインに基づいて **Push Scope** (プッシュ スコープ) を自動的にフィルタリングします (「Panorama > Access Domains (アクセス ドメイン)」を参照)。管理ロールやフィルタリングの選択に関係なく、スコープにはアカウントに割り当てられたアクセス ドメインの設定変更のみが含まれます。 デフォルトの場所を受け入れる代わりに、**Push Scope** (プッシュ スコープ) の選択内容の編集を行うことができます。
場所タイプ	この列では保留中の変更の場所が分類されます。 • **Device Groups** (デバイス グループ) – 特定のデバイス グループで定義されている設定。 • **Templates** (テンプレート) – 特定のテンプレートまたはテンプレート スタックで定義されている設定。 • **Log Collector Groups** (ログ コレクタ グループ) – コレクタ グループ設定固有の設定。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
	• **WildFire Clusters**（**WildFire** クラスタ） — WildFire クラスタ設定固有の設定。 • **WildFire Appliances**（**WildFire** アプライアンス） — WildFire アプライアンス設定固有の設定。
エンティティ	この列には、各デバイス グループまたはテンプレートのプッシュ操作に含まれるファイアウォール（デバイス名またはシリアル番号別）または仮想システム（名前別）が表示されます。 変更をコレクタ グループにプッシュする場合、操作には、グループのメンバーであるすべてのログ コレクタが含まれます（表示されていないログ コレクタも対象となります）。
選択内容の編集	プッシュ操作に含めるエンティティを選択する場合にクリックします。 • デバイス グループとテンプレート • ログ コレクタ グループ • WildFire アプライアンスおよびクラスタ *Panorama* では、まだ *Panorama* 設定にコミットされていない変更をプッシュすることはできません。
デバイス グループとテンプレート	**Edit Selections**（選択内容の編集）を行い、**Device Groups**（デバイス グループ）または **Templates**（テンプレート）を選択して、以下の行のオプションを表示します。
フィルタ	テンプレート、テンプレートスタック、あるいはデバイスグループや関連するファイアウォールやバーチャルシステムのリストから絞り込みを行います。
氏名	プッシュ操作に含めるテンプレート、テンプレート スタック、デバイス グループ、ファイアウォール、あるいは仮想システムを選択します。
最終コミット状態	ファイアウォールおよび仮想システム設定が、テンプレートもしくは Panorama のデバイス グループ設定と同期されているかを示しています。
HA 状態	登録されたファイアウォールの高可用性（HA）状態を示します。 • **Active** [アクティブ] - 正常なトラフィック処理状態 • **Passive** [パッシブ] - 正常なバックアップ状態 • **Initiating** [始動中] - ファイアウォールの起動後最大60秒はこの状態におかれます • **Non-functional** [機能停止中] - エラー状態 • **Suspended** [保留中] - 管理者がファイアウォールをサスペンドしていることを示します • **Tentative** [一時的な状態] - アクティブ/アクティブ環境におけるリンクまたはパスのモニタリングイベント用

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
変更保留中の (Panorama) コミット	選択したファイアウォールおよび仮想システムに変更をプッシュする前に、Panorama コミットが必要か（yes（はい））か否か（no（いいえ））を示します。
Preview Changes（変更のプレビュー）列	**Preview Changes**（変更のプレビュー）を行って、**Push Scope**（プッシュ スコープ）で選択した設定と Panorama の実行中の設定を比較します。Panorama は、**Device Groups**（デバイス グループ）または **Templates**（テンプレート）タブで選択したファイアウォールおよび仮想システムの結果のみが表示されるように出力をフィルタリングします。プレビュー ウィンドウでは色分けによって詳細が示されます（追加は緑色、変更は黄色、削除は赤色）。 プレビュー結果は新しいブラウザ ウィンドウで表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビュー ウィンドウが開かない場合は、ポップアップを許可する手順についてブラウザのドキュメントを参照してください。
すべて選択	リスト中のすべてのエントリを選択します。
すべての選択を解除	リスト中のすべてのエントリの選択を解除します。
すべて展開	テンプレート、テンプレート スタック、またはデバイス グループに割り当てられたファイアウォールおよび仮想システムを表示します。
すべて縮小表示	テンプレート、テンプレートスタック、またはデバイスグループのみを表示します（割り当てられたファイアウォールや仮想システムは表示されません）。
HA ピアのグループ化	高可用性（HA）設定のピアであるファイアウォールをグループ化します。こうすることでリストには、アクティブのファイアウォール（アクティブ/アクティブ設定ではアクティブ-プライマリ）が最初に表示され、パッシブのファイアウォール（アクティブ/アクティブ設定ではアクティブ-セカンダリ）はかっこ内に表示されます。これで、HA モードのファイアウォールを簡単に識別できます。共有ポリシーをプッシュする場合に、個々のピアではなくグループ化されたペアにプッシュできます。 アクティブ/パッシブ環境の*HA*ピアにおいては、設定内容を同時にプッシュできるよう、両方のファイアウォールかそれぞれの仮想システムを同じデバイスグループ、テンプレート、またはテンプレートスタックに入れることも検討してみてください。
検証	選択したファイアウォールおよび仮想システムにプッシュする設定を検証する場合にクリックします。タスク マネージャが自動的に開き、検証の状態が表示されます。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
フィルタが選択されています	特定のファイアウォールもしくは仮想システムを表示したい場合は、それらを選択した状態で **Filter Selected**（選択項目でフィルタ）を選択してください。
候補設定とのマージ	（デフォルトで選択）Panorama からプッシュされた設定変更を、管理者がターゲット ファイアウォール上でローカルに実装した保留中の設定変更とマージします。プッシュ操作により、PAN-OS® がトリガーされて、マージされた変更がコミットされます。この選択を解除すると、ファイアウォールの候補設定がコミットから除かれます。 ファイアウォール管理者にファイアウォール上でローカルに変更をコミットすることを許可していて、*Panorama* から変更をコミットするときにそれらの変更を含めない場合は、このオプションの選択を解除します。 また、Panorama から変更をプッシュする前に、ファイアウォールで設定の監査を行い、ローカルな変更を確認することを推奨します（「Device（デバイス）> Config Audit（設定監査）」を参照）。
デバイスおよびネットワーク テンプレートを含める （Device Groups（デバイス グループ）タブのみ）	（デフォルトで選択）1 回の操作でデバイス グループの変更と関連付けられたテンプレートの変更の両方を選択したファイアウォールおよび仮想システムにプッシュします。これらの変更を個別の操作でプッシュする場合は、このオプションを解除してください。
テンプレートの値を適用	（デフォルトでは無効）すべてのローカル設定をオーバーライドし、選択したファイアウォール上のオブジェクトのうち、テンプレートおよびテンプレート スタックに存在しないか、ローカル設定でオーバーライドされたオブジェクトをすべて削除します。プッシュ操作により、ファイアウォール上の既存の設定がすべて取り消され、ファイアウォールはテンプレートあるいはテンプレート スタックに定義されている設定のみを継承するようになります。 *Force Template Values (*テンプレートの値を適用*)*が有効な設定をプッシュする場合、ファイアウォールのオーバーライドされたすべての値がテンプレートの値で上書きされます。このオプションを使用する前にファイアウォールのオーバーライドされた値をチェックし、コミットによって予期せぬネットワークの障害が発生したり、これらのオーバーライドされた値によって問題が生じたりしないことを確認してください。
ログ コレクタ グループ	**Edit Selections**（選択内容の編集）を行い、プッシュ操作に含める **Log Collector Groups**（ログ コレクタ グループ）を選択します。このタブには、以下のオプションが表示されます。 • **Select All**（すべて選択）– リスト中のすべてのコレクタ グループを選択します。 • **Deselect All**（すべての選択を解除）– リスト中のすべてのコレクタ グループの選択を解除します。

© 2019 Palo Alto Networks, Inc.

フィールド/ボタン	の意味
WildFire アプライアンスおよびクラスタ	**Edit Selections**（選択内容の編集）を行い、**WildFire Appliances and Clusters**（**WildFire** アプライアンスおよびクラスタ）を選択して、以下のオプションを表示します。
フィルタ	WildFire アプライアンスおよびクラスタのリストをフィルタリングします。
氏名	Panorama が変更をプッシュする WildFire アプライアンスおよびクラスタを選択します。
最終コミット状態	WildFire アプライアンスおよびクラスタ設定が Panorama と同期しているかどうかを示します。
選択内容の除外	Push Scope (プッシュ スコープ) に一覧表示されているすべてのファイアウォールを除外します。
デバイス グループのプッシュの検証	Push Scope（プッシュ スコープ）リストでデバイス グループにプッシュする設定を検証します。タスク マネージャが自動的に開き、検証の状態が表示されます。
テンプレートのプッシュの検証	Push Scope（プッシュ スコープ）リストでテンプレートにプッシュする設定を検証します。タスク マネージャが自動的に開き、検証の状態が表示されます。
場所タイプ別グループ	**Location Type**（場所タイプ）を使用して Push Scope（プッシュ スコープ）リストをグループ化する場合に選択します。
以下のオプションは、Panorama 設定をコミットする場合、または変更をデバイスにプッシュする場合に適用されます。	
の意味	他の管理者が変更内容を理解するのに役立つ説明（最大 512 文字）を入力します。 コミット イベントのシステム ログでは、*512* 文字を超える説明は切り捨てられます。
Commit（コミット）/ Push（プッシュ）/Commit and Push（コミットしてプッシュ）	コミットを開始したり、他のコミットが保留中の場合にコミット要求をコミット キューに追加したりします。

© 2019 Palo Alto Networks, Inc.

Panorama でのポリシーの定義

Panorama™ のDevice Groups（デバイス グループ）を使用すると、ファイアウォール ポリシーを一元的に管理できます。Panorama 上に定義されるポリシーは、プレ ルールまたはポスト ルールとして作成されます。プレ ルールとポスト ルールにより、階層的な方法でポリシーを実装できます。

共有コンテクストのプレ ルールとポスト ルールは、共有コンテクストですべての管理対象ファイアウォールの共有ポリシーとして、またはデバイス グループ コンテクストで特定のデバイス グループ用として定義できます。プレ ルールとポスト ルールは Panorama で定義を行った後に管理対象デバイスにプッシュされるため、管理対象ファイアウォールでルールの表示はできますが、編集は Panorama でしか行えません。

- **Pre Rules**[プレ ルール] – ルール順序の先頭に追加され、最初に評価されるルールです。プレルールを使用すれば、組織の利用規約に対する遵守を徹底させることができます。例えば、プレルールによって特定の URL カテゴリへのアクセスをブロックしたり、すべてのユーザーの DNS トラフィックを許可することができます。
- **Post Rules**（ポスト ルール） – ルール順序の末尾に追加され、プレ ルールとファイアウォールでローカルに定義されているルールの後に評価されるルールです。通常、ポスト ルールには、App-ID™、User-ID™、またはサービスに基づいてトラフィックへのアクセスを拒否するルールが含まれます。
- **Default Rules**（デフォルト ルール） – プレ ルール、ポスト ルール、ローカル ファイアウォール ルールのいずれとも一致しないトラフィックをファイアウォールで処理する方法を指定するルールです。これらのルールは、事前定義済みの Panorama 設定の一部です。これらのルールで選択した設定を **Override**（オーバーライド）して編集を有効にするには、「セキュリティ ルールのオーバーライドまたは取り消し」を参照してください。

Preview Rules（ルールのプレビュー）をクリックして、ルールを管理対象ファイアウォールにプッシュする前に、すべてのルールのリストを表示することができます。大量のルールに目を通しやすいように、各ルールベース内でルールの階層がデバイスグループ（および管理対象ファイアウォール）ごとに視覚的に区別されて表示されます。

新しいルールを追加する際、ルールの静的な運用データが表示されます。UUID（Universally Unique Identifier）列にはルールの 36 文字の UUID が表示されます。ファイアウォールはルール毎に UUID を生成します。しかし、ルールを Panorama からプッシュ送信している場合、同じ UUID を持つこれらのルールも Combined Rules Preview (複合ルールのプレビュー) に表示されます。**Created (**作成済み**)**列には、ルールをルールベースに追加した日時が表示されます。さらに、ルールを最後に編集した日時が**Modified (**編集日時**)**列に表示されます。PAN-OS 9.0 にアップグレードする前にポリシールールが作成された場合、**First Hit (**最初のヒット**)**のデータを使用して**Created (**作成**)**日が決定されます。対象のルールで利用できる**First Hit (**最初のヒット**)**のデータがない場合、ファイアウォールあるいは Panorama の管理サーバーが PAN-OS 9.0 にアップグレードされた日時を使用して**Created (**作成**)**日が決定されます。

ルールの追加または編集を Panorama で行うと、対象タブが表示されます。このタブを使用して、ルールが定義されている **Device Group**（デバイス グループ）（または共有の場所）の特定のファイアウォールまたは子孫デバイス グループにルールを適用できます。**Target**（対象）タブでは **Any**（すべて）（デフォルト）を選択でき、ルールはすべてのファイアウォールと子孫デバイス グループに適用されます。特定のファイアウォールまたはデバイス グループを対象にするには、**Any**（すべて）を選択解除してファイアウォールまたはデバイス グループを名前ごとに選択します。特定のファイアウォールまたはデバイス グループを除外するには、**Any**（すべて）を選択解除して、指定のファイアウォールとデバイス グループを名前ごとに選択し、**Target to all but these specified devices**（指定したデバイスを除くすべてを対象にする）を選択します。デバイス グループとファイアウォールのリストが長い場合は、フィルタを適用して、属性（プラットフォームなど）ごとに、または名前と一致する文字列ごとに、エントリを検索できます。

Panorama でルールを正常に追加してプッシュすると、**Rule Usage**（ルールの使用状況）で、ルールがデバイス グループ内のすべてのデバイスで Used（使用）されているか、デバイスグループ内の一部のデバイスによって Partially Used（部分的に使用）されているか、またはデバイスグループ内のデバイスによっ

© 2019 Palo Alto Networks, Inc.

て Unused（使用されていない）かが表示されます。Panorama は、Policy Rule Hit Count（ポリシー ルール ヒット数）（デフォルトで有効）で管理されたファイアウォールに基づいてルールの使用状況を判断します。Panorama コンテクストでは、デバイス グループ全体の共有ポリシー ルールの、ルールの使用状況を表示できます。さらに、コンテクストを個々のデバイス グループに変更し、デバイス グループ内のすべてのデバイスでのポリシー ルールの合計使用状況を表示することもできます。**Preview Rules** (ルールのプレビュー)では、該当のデバイス グループの各ポリシー ルールの **Hit Count** (ヒット数)、**Last Hit** (最後のヒット)、**First Hit** (最初のヒット)が表示されます。総トラフィック ヒット数、および最初と最後のヒットのタイムスタンプは、再起動、アップグレード、およびデータプレーンの再起動イベントを通じて維持されます。「Monitor Policy Rule Usage（ポリシー ルール使用状況のモニター）」を参照してください。

Group Rules by Tag (タグに基づいてルールをグループ化)してタグを適用することでポリシールールのようにグループ化することで、ルールの機能に対する可視性を高め、ルールベース全体にかけてポリシールールを管理しやすくなります。タグに基づいてグループ化されたルールはタグ グループのリストを表示しますが、ルールの優先順位リストを維持します。ルールをタグ グループの最後に追加したり、ルールを別のタグ グループに移動したり、タグ グループ内のルールにタグを追加したり、グループ タグを使ってフィルタリングや検索を行ったりできます。

ポリシールールに対する変更を追跡するには、変更の内容およびルールを作成あるいは編集した理由を示す**Audit Comment** (監査コメント)を追加します。監査コメントを入力し、設定変更をコミットしたら、監査コメントが**Audit Comment Archive** (監査コメント アーカイブ)に保存され、そこで選択したルールの過去の監査コメントをすべて閲覧できるようになります。監査コメントはグローバル検索で検索できます。監査コメント アーカイブは読み取り専用です。

Policies（ポリシー）タブにアクセスできる管理ユーザーは、Webインターフェイスに表示されるポリシー ルールを **PDF/CSV** 形式でエクスポートできます。Export Configuration Table Data（設定バンドル データのエクスポート）を参照してください。

ポリシーを作成するには、各ルールベースの関連するセクションを表示します。

- Policies > Security [ポリシー > セキュリティ]
- Policies > NAT [ポリシー > NAT]
- Policies > QoS [ポリシー > QoS]
- Policies > Policy Based Forwarding [ポリシー > ポリシー ベース フォワーディング]
- Policies > Decryption [ポリシー > 復号化]
- Policies > Application Override [ポリシー > アプリケーション オーバーライド]
- Policies（ポリシー） > Authentication（認証）
- Policies > DoS Protection [ポリシー > DoS プロテクション]
- Policies > SD-WAN [ポリシー > SD-WAN]

© 2019 Palo Alto Networks, Inc.

レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティション

- Panorama > Setup > Operations [Panorama > セットアップ > 操作]

デフォルトでは、レガシー モードの Panorama バーチャル アプライアンスには、すべてのデータ用に 1 つのディスク パーティションがあり、10.89GB がログ ストレージに割り当てられています。ディスク サイズを拡大しても、ログ ストレージ容量は拡大しません。次のオプションを使用して、ログ ストレージ容量を変更してください。

- ネットワーク ファイル システム（**NFS**）– NFS ストレージをマウントするオプションを使用できるのは、レガシー モードになっていて VMware ESXi サーバーで動作する Panorama バーチャル アプライアンスのみです。NFS ストレージをマウントするには、Miscellaneous（その他）セクションで **Storage Partition Setup**（ストレージ パーティションの設定）を選択して **Storage Partition**（ストレージ パーティション）を **NFS V3** に設定し、 Table（表）の説明に従って設定を構成します。NFS Storage Settings（NFS ストレージ設定）。
- デフォルト内部ストレージ – デフォルトの内部ストレージ パーティションに戻します（ESXi サーバーまたは vCloud Air プラットフォームの Panorama で、別の仮想ログ ディスクを以前設定したか、NFS にマウントした場合にのみ該当）。デフォルトの内部ストレージ パーティションに戻すには、Miscellaneous（その他）セクションで **Storage Partition Setup**（ストレージ パーティションの設定）を選択し、**Storage Partition**（ストレージ パーティション）を **Internal**（内部）に設定します。
- 仮想ログ ディスク – VMware ESXi バージョン 5.5 以降で動作している Panorama、または VMware vCloud Air プラットフォームで動作している Panorama では、別の仮想ディスクを追加できます（8TB まで）。ただし、Panorama では元のディスクでデフォルトの 10.89GB ログ ストレージの使用が停止され、既存のログはすべて新しいディスクにコピーされます（ESXi の以前のバージョンでは、2TB までの仮想ディスクのみがサポートされます）。

ストレージ パーティション設定を変更したら、*Panorama* を再起動する必要があります。*Panorama* > *Setup*（セットアップ）> *Operations*（操作）を選択して *Reboot Panorama*（*Panorama* の再起動）を選択してください。

Panorama モードの *Panorama* バーチャル アプライアンスまたは *M-Series* アプライアンスでは、*NFS* ストレージを使用できません。

表 **1 :** 表：**NFS** ストレージ設定

Panorama ストレージ パーティションの設定 - NFS V3	の意味
SERVER	NFSサーバーのFQDNまたはIPアドレスを指定します。
ログ ディレクトリ	ログが保管されるディレクトリの完全パス名を指定します。
PROTOCOL	NFSサーバーとの通信に使用するプロトコル（UDPまたはTCP）を指定します。
ポート	NFSサーバーとの通信に使用するポートを指定します。
読み取りサイズ	NFS が読み取り可能な最大バイト数（範囲は 256 ~ 32,768）を指定します。

© 2019 Palo Alto Networks, Inc.

Panorama ストレージ パーティションの設定 - NFS V3	の意味
書き込みサイズ	NFS が書き込み可能な最大バイト数 (範囲は 256 ~ 32,768) を指定します。
セットアップ時にコピー	Panorama デバイスの起動時に NFS パーティションをマウントし、既存のログをすべてサーバー上の宛先ディレクトリにコピーする場合に選択します。
ロギングパーティションのテスト	NFS パーティションのマウントのテストを実行し、成功メッセージまたは失敗メッセージを確認する場合に選択します。

© 2019 Palo Alto Networks, Inc.

Panorama > Setup（セットアップ）> Interfaces（インターフェイス）

Panorama が使用するインターフェイスを設定する場合に、**Panorama** > **Setup**（セットアップ）> **Interfaces**（インターフェイス）を選択します。これにより、ファイアウォールとログ コレクタの管理、ソフトウェアおよびコンテンツ更新のファイアウォールとログ コレクタへの適用、ファイアウォールからのログ収集、コレクタ グループとの通信ができます。デフォルトでは、Panorama は、ファイアウォールとログ コレクタとのすべての通信に MGT インターフェイスを使用します。

MGT インターフェイスのトラフィックを低減するには、更新の適用、ログ収集、コレクタ グループ通信のための別のインターフェイスを設定します。ログ トラフィックの負荷が高い環境の場合、ログ収集用に複数のインターフェイスを設定できます。また、管理トラフィックのセキュリティを向上するには、*MGT* インターフェイス用に、他のインターフェイスのサブネットよりも秘密性の高い個別のサブネット（*IPv4* ネットマスクまたは *IPv6* プレフィックス長）を定義できます。

使用できるインターフェイスは、Panorama モデルによって異なります。

インターフェイス	最高速度	M-500アプライアンス	Panorama バーチャル アプライアンス
管理（MGT）	1Gbps	✓	✓
イーサネット1（Eth1）	1Gbps	✓	—
イーサネット2（Eth2）	1Gbps	✓	—
イーサネット3（Eth3）	1Gbps	✓	—
イーサネット4（Eth4）	10Gbps	✓	—
イーサネット5（Eth5）	10Gbps	✓	—

インターフェイスを設定するには、インターフェイス名をクリックして、以下の表に記載されているように設定します。

どのような場合でも、*MGT* インターフェイスの *IP* アドレス、ネットマスク（*IPv4* の場合）またはプレフィックス長（*IPv6* の場合）、デフォルト ゲートウェイを指定してください。設定の一部の値が省略された場合（デフォルト ゲートウェイなど）、以降の設定変更ではコンソール ポート経由でしか *Panorama* にアクセスできなくなります。*3* つの設定すべてを指定するまで、他のインターフェイスの設定はコミットできません。

インターフェイス設定	の意味
Eth1/Eth2/Eth3/Eth4/Eth5	インターフェイスを有効にして設定する必要があります。MGT インターフェイスは例外で、これはデフォルトで有効になっています。

© 2019 Palo Alto Networks, Inc.

インターフェイス設定	の意味
Public IP Address (パブリックIPアドレス)	ファイアウォールがプライベートIPアドレス (NAT) に変換されたパブリックIPアドレスを使用して Panorama に接続する場合は、インターフェイスにパブリックIPアドレスを入力します。
IP アドレス (IPv4)	ネットワークで IPv4 を使用する場合、IPv4 アドレスをインターフェイスに割り当てます。
ネットマスク (IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワーク マスク（例: 255.255.255.0）を入力する必要もあります。
デフォルト ゲートウェイ（IPv4）	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv4 アドレスを割り当てる必要があります（ゲートウェイはインターフェイスと同じサブネット上にある必要があります）。
IPv6 アドレス/プレフィックス長	ネットワークで IPv6 を使用する場合、IPv6 アドレスをインターフェイスに割り当てます。ネットマスクを示すには、IPv6 プレフィックス長を入力します（例: 2001:400:f00::1/64）。 *IPv6 アドレスは、プライベート クラウド環境 (ESXi、vCloud Air、KVM、Hyper-V) に展開されたすべての M-Series アプライアンスおよび Panorama バーチャル アプライアンスの MGT インターフェイスでサポートされています。パブリック クラウド環境 (Amazon Web Service (AWS)、AWS GovCloud、Microsoft Azure、および Google Cloud Platform) に展開された Panorama バーチャル アプライアンスの MGT インターフェイスでは、IPv6 アドレスはサポートされていません。*
デフォルト IPv6 ゲートウェイ	IPv6 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv6 アドレスを割り当てる必要があります（ゲートウェイはインターフェイスと同じサブネット上にある必要があります）。 *IPv6 アドレスは、プライベート クラウド環境 (ESXi、vCloud Air、KVM、Hyper-V) に展開されたすべての M-Series アプライアンスおよび Panorama バーチャル アプライアンスの MGT インターフェイスでサポートされています。パブリック クラウド環境 (Amazon Web Service (AWS)、AWS GovCloud、Microsoft Azure、および Google Cloud Platform) に展開された Panorama バーチャル アプライアンスの MGT インターフェイスでは、IPv6 アドレスはサポートされていません。*
速度	インターフェイスの速度を、フル デュプレックスまたはハーフ デュプレックスの 10Mbps、100Mbps、1Gbps、または 10Gbps（Eth4 および Eth5 のみ）に設定します。Panorama にインターフェイス速度を決定させるには、デフォルトのオート ネゴシエート設定を使用します。 この設定は、隣接するネットワーク機器のインターフェイス設定と一致させる必要があります。設定を確実に一致させるには、オート ネゴシエートを選択します（隣接する機器がこのオプションをサポートする場合）。

© 2019 Palo Alto Networks, Inc.

インターフェイス設定	の意味
MTU	このインターフェイスで送信されるパケットの最大転送単位（MTU）をバイト数で入力します（範囲は 576 ~ 1,500、デフォルトは 1,500）。
デバイス管理およびデバイス ログ収集	ファイアウォールとログ コレクタの管理と、それらのログの収集をインターフェイスで有効にします（デフォルトでは MGT インターフェイスで有効）。複数のインターフェイスでこれらの機能の実施を有効にできます。
コレクタ グループ通信	インターフェイスでコレクタ グループ通信を有効にします（デフォルトは MGT インターフェイス）。この機能を実施できるインターフェイスは 1 つのみです。
デバイスのデプロイ	ファイアウォールとログ コレクタに対するソフトウェアおよびコンテンツ更新の適用をインターフェイスで有効にします（デフォルトは MGT インターフェイス）。この機能を実施できるインターフェイスは 1 つのみです。
管理サービスの管理	• **HTTP** — Panorama Web インターフェイスへのアクセスを有効にします。HTTPはプレーンテキストを使用しますが、HTTPSよりは機密性が劣ります。 インターフェイス上の管理トラフィックには、*HTTP* の代わりに *HTTPS* を有効化してください。 • **Telnet** — Panorama CLI へのアクセスを有効にします。Telnetはプレーンテキストを使用しますが、SSHよりは機密性が劣ります。 • **HTTPS** — Panorama Web インターフェイスへの安全なアクセスを有効にします。 インターフェイス上の管理トラフィックには、*Telnet* の代わりに *SSH* を有効化してください。 • **SSH** — Panorama CLI への安全なアクセスを有効にします。
ネットワーク接続性サービス	**Ping** サービスはどのインターフェイスでも使用できます。Panorama インターフェイスと外部サービス間の接続テストに Ping を使用できます。高可用性（HA）配置の場合、HAピアはpingを使用してハートビートのバックアップ情報を交換します。 次のサービスを使用できるのは、MGT インターフェイスのみです。 • **SNMP** — Panorama が SNMP マネージャからの統計クエリを処理できるようにします。詳細は、「SNMP モニタリングの有効化」を参照してください。 • **User-ID** — Panorama が User-ID エージェントから受信したユーザー マッピング情報を再配信できるようにします。
アクセス許可IPアドレス	このインターフェイスの Panorama に管理者がアクセスする際の IP アドレスを入力します。空のリスト（デフォルト）は、どの IP アドレスからもアクセスできることを示します。 このリストを空白のままにしないでください。不正アクセスを防ぐために、*Panorama* 管理者（のみ）の *IP* アドレスを指定します。

© 2019 Palo Alto Networks, Inc.

Panorama > High Availability [Panorama > 高可用性]

Panorama の高可用性 (HA) を有効にするには、以下の表の説明に従って設定を指定します。

Panorama HA 設定	の意味
セットアップ 編集 ( ) をクリックして、以下の設定を行います。	
Enable HA	HA を有効にする場合に選択します。
ピア HA IP アドレス	ピアのMGTインターフェイスのIPアドレスを入力します。
暗号化を有効	MGT インターフェイスが有効になると、HA ピア間の通信が暗号化されます。暗号化を有効化する前に、それぞれのHAピアからHAキーをエクスポートし、もう一方のピアへインポートしてください。**Panorama** > **Certificate Management** (証明書の管理) > **Certificates** (証明書) ページで HA キーをインポートおよびエクスポートします (「ファイアウォールおよび Panorama 証明書の管理」を参照)。 *HA の接続は、暗号化が有効になっている場合は TCP ポート 28 を使用し、暗号化が有効になっていない場合は TCP ポート 28769 を使用します。*
ホールド タイムのモニター (ミリ秒)	制御リンク障害に反応するまでにシステムが待機する時間 (ミリ秒) を入力します (範囲は 1,000 ~ 60,000、デフォルトは 3,000)。
選択設定 編集 ( ) をクリックして、以下の設定を行います。	
優先順位 (Panoramaバーチャル アプライアンスで必要になります)	この設定を行うことで、ファイアウォールのログを主となって受信するピア (プライマリ) が決定されます。HAペアでは、一方のデバイスを**Primary** [プライマリ] として割り当て、もう一方のデバイスを**Secondary** [セカンダリ] として割り当てます。 レガシー モードの Panorama バーチャル アプライアンスのログ ストレージ パーティションを設定する場合、ログ ストレージに内部ディスク (デフォルト) またはネットワーク ファイル システム (NFS) を使用できます。NFSを設定した場合、プライマリの受信ピアのみがファイアウォールのログを受信します。内部ディスク ストレージを設定すると、ファイアウォールはデフォルトでプライマリ ピアとセカンダリ ピアの両方にログを送信しますが、これはロギングおよびレポート設定の **Only Active Primary Logs to Local Disk** (アクティブなプライマリ ログのみをローカル ディスクに保存) を有効にして変更できます。
プリエンプティブ	プライマリ Panorama が障害から回復した後にアクティブな動作を再開できるようにする場合に選択します。無効になっている場合、プライマリ Panorama が障害から回復した後も、セカンダリ Panorama がアクティブのまま動作します。

© 2019 Palo Alto Networks, Inc.

Panorama HA 設定	の意味
HA タイマー設定	ここでの設定内容は、後述のHA選択設定におけるフェイルオーバーの速度を左右します。 • **Recommended** (推奨) — 標準 (デフォルト) のフェイルオーバー タイマーを設定する場合に選択してください。一連の設定数値を表示する場合は**Advanced** [詳細設定] から**Load Recommended** [推奨設定の読込] を選択します。 • **Aggressive** (アグレッシブ) — 高速のフェイルオーバー タイマー設定の場合に選択します。一連の設定数値を表示する場合は**Advanced** [詳細設定] から**Load Agressive** [アグレッシブ設定の読込] を選択します。 • **Advanced** (詳細設定) — 残りの HA 選択設定を表示し、値をカスタマイズする場合に選択します。 以下の設定の **Recommended** (推奨) および **Aggressive** (アグレッシブ) の値を確認してください。
プロモーション ホールド タイム (ミリ秒)	プライマリ ピアがダウンしてからセカンダリ Panorama ピアがその役目を引き継ぐまでに待機する時間をミリ秒単位で入力します (範囲は 0 から 60,000)。推奨 (デフォルト) 値は2000、アグレッシブの場合は500です。
Hello Interval (ms) (Hello 間隔 (ミリ秒)	もう一方のピアが動作していることを確認するための hello パケットの送信間隔をミリ秒単位 (範囲は 8,000 から 60,000) で入力します。推奨 (デフォルト) の場合もアグレッシブの場合も8000に設定されています。
ハートビート間隔 (ミリ秒)	Panorama が HA ピアに ICMP ping を送る間隔をミリ秒単位で指定します (範囲は 1,000 から 60,000)。推奨 (デフォルト) 値は2000、アグレッシブの場合は1000です。
Preemption Hold Time (min) (プリエンプション ホールド タイム (分))	この設定値は**Preemptive** [プリエンプティブ] を設定した場合にのみ適用されます。フェイルオーバーの原因が解決され、パッシブな Panorama ピアがアクティブな状態に復帰する前に待機する時間を分単位で入力します (範囲は 1 から 60)。推奨 (デフォルト) の場合もアグレッシブの場合も1に設定されています。
モニター障害時ホールド アップ タイム (ミリ秒)	パス モニターの障害後、Panorama がパッシブな状態への復帰を試行するまでの待機時間をミリ秒単位で指定します (範囲は 0 から 60,000)。この待機中に障害が発生しても、パッシブピアはアクティブピアを引き継ぐことができません。待機時間を持たせることで、隣接するデバイスの偶発的なフラッピングによるフェイルオーバーを回避することができます。推奨 (デフォルト) の場合もアグレッシブの場合も0に設定されています。
追加のマスター ホールド アップ タイム (ミリ秒)	優先度の高いピアがアクティブ ピアの役割を引き継ぐ前に、パッシブ状態を維持する時間をミリ秒単位で指定します (範囲は 0 から 60,000)。推奨 (デフォルト) 値は7000、アグレッシブの場合は5000です。
パス モニタリング 編集 ( ) をクリックして、HA パス モニタリングの設定を行います。	
enabled [有効化]	パスのモニタリングを有効化する場合に選択します。パスのモニタリングをオンにすると、Panorama は、ICMP pingメッセージを送信してレスポンスがあることを確認することで、指定した宛先IPアドレスをモニターします。

© 2019 Palo Alto Networks, Inc.

Panorama HA 設定	の意味
障害条件	モニターしているパスグループの**Any**[一部]または**All**[すべて]で応答できない場合にフェイルオーバーを発生させるかどうかを選択します。
パス グループ HAパスモニタリング用のパスグループを作成する場合は、**Add**[追加]をクリックし、以下の項目を入力してください。	
氏名	パスグループの名前を指定します。
enabled [有効化]	パス グループを有効にする場合に選択します。
障害条件	指定した宛先アドレスの **Any**（いずれか）または **All**（すべて）が応答できない場合に、エラーを発生させるかどうかを選択します。
Ping 間隔	ICMP エコー メッセージによって宛先 IP アドレスへのパスが有効であることを確認する間隔をミリ秒単位で指定します（範囲は 1,000 ~ 60,000、デフォルトは 5,000）。
Ping 数	障害を宣言するまでの ping 試行回数を指定します（範囲は 3 ~ 10、デフォルトは 3）。
宛先IP	モニターする宛先IPアドレスを1つ以上入力します。複数のアドレスを入力する場合はコンマで区別してください。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed WildFire Clusters（管理対象 WildFire クラスタ）

- Panorama > Managed WildFire Clusters（管理対象 WildFire クラスタ）
- Panorama > Managed WildFire Appliances（管理対象 WildFire アプライアンス）

Panorama M-Series またはバーチャル アプライアンスから、クラスタ内にある WildFire アプライアンスを管理できます。スタンドアロン アプライアンスとして管理することもできます。クラスタの管理（**Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ））とスタンドアロン アプライアンスの管理（**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス））の管理および設定タスクには共通点が多いため、両方について以下のトピックにまとめています。

WildFire アプライアンスを Panorama に追加した後、Web インターフェイスでこれらのアプライアンスをクラスタに追加してクラスタとして管理したり、スタンドアロン アプライアンスとして管理したりします。

- 管理対象 WildFire クラスタのタスク
- 管理対象 WildFire アプライアンスのタスク
- 管理対象 WildFire の情報
- 管理対象 WildFire クラスタおよびアプライアンスの管理

管理対象 WildFire クラスタのタスク

WildFire アプライアンス クラスタの作成と削除は、Panorama から行うことができます。あるクラスタから別のクラスタに設定をインポートする際、設定にかかる時間を節約することもできます。

タスク	の意味
クラスタの作成	必要に応じて **Create Cluster**（クラスタの作成）を行い、新しいクラスタの名前を入力してから **OK** をクリックします。 ローカルで設定し、WildFire アプライアンス ノードを個別に追加して Panorama に追加した既存のクラスタは、WildFire ノードおよびノードのロールとともにリストされます（**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス））。 クラスタ名は有効なサブドメイン名にする必要があり、小文字または数字で始めて、ハイフンを使用できますが、ハイフンをクラスタ名の最初と最後の文字にすることはできず、スペースやその他の文字は使用できません。クラスタ名の最大文字数は 63 文字です。 クラスタを作成したら、管理対象 WildFire アプライアンスをクラスタに追加して Panorama で管理できます。WildFire アプライアンスを Panorama に追加すると、アプライアンスは Panorama に自動的に登録されます。 Panorama には最大 10 個の管理対象 WildFire クラスタを作成でき、各クラスタには 20 個までの WildFire アプライアンス ノードを含めることができます。Panorama では、総計 200 個のスタンドアロン アプライアンスおよびクラスタ ノードを管理できます。
クラスタ設定のインポート	**Import Cluster Config**（クラスタ設定のインポート）により、既存のクラスタ設定をインポートします。クラスタを選択してから **Import Cluster Config**（クラスタ設定のインポート）を行うと、**Controller**（コントローラ）と **Cluster**（クラ

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	スタ）には、選択したクラスタの適切な情報が自動的に入力されます。**Import Cluster Config**（クラスタ設定のインポート）の前にクラスタを選択しない場合は、**Controller**（コントローラ）を選択する必要があり、**Cluster**（クラスタ）には、選択したコントローラ ノードに基づいて自動的に情報が入力されます。 設定をインポートしたら、**Commit to Panorama**（**Panorama** にコミット）により、インポートした候補設定を Panorama の実行中の設定に保存します。
Panorama から削除	WildFire クラスタを Panorama から管理する必要がなくなった場合は、**Remove From Panorama**（**Panorama** から削除）を実行し、**Yes**（はい）を選択してアクションを確定します。クラスタを Panorama の管理から削除した後は、コントローラ ノードからそのクラスタをローカルで管理できます。クラスタをローカルではなくて再び中央管理する場合は、そのクラスタを Panorama アプライアンスにいつでも追加しなおすことができます。
WildFire クラスタ アプライアンスからアプライアンス 通信の暗号化	クラスタ内の WildFire アプライアンス間のデータ通信を暗号化するには、**Secure Cluster Communication**（安全なクラスタ通信）で暗号化を**Enable**（有効）にします。 WildFire は、事前定義された証明書またはカスタム証明書のいずれかを使用してアプライアンス間で通信します。カスタム証明書は、**Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズを構成）し、**Custom Certificate Only**（カスタム証明書のみ）使用されます。 WildFire クラスタが FIPS-CC モードで動作するには、暗号化が必要です。FIPS-CC モードで使用されるカスタム証明書は、FIPS-CC 要件を満たす必要があります。 安全なクラスタ通信を有効にすると、管理対象の WildFire アプライアンスをクラスタに追加できます。新しく追加されたアプライアンスは、安全なクラスタ通信設定を自動的に使用します。

管理対象 WildFire アプライアンスのタスク

Panorama デバイスでは、スタンドアロン WildFire アプライアンスの追加、削除、管理ができます。スタンドアロン アプライアンスを追加したら、WildFire アプライアンス クラスタにクラスタ ノードとして追加したり、個別のスタンドアロン アプライアンスとして管理したりすることができます。

タスク	の意味
アプライアンスの追加	**Add Appliance**（アプライアンスの追加）では、1 つ以上の WildFire アプライアンスを Panorama アプライアンスに追加して中央管理します。各 WildFire アプライアンスのシリアル番号は個別の行（新しい行）に入力します。Panorama では、合計 200 個までの WildFire クラスタ ノードとスタンドアロン WildFire アプライアンスを管理できます。 Panorama で管理する各 WildFire アプライアンスでは、次の WildFire アプライアンス CLI コマンドを使用して、Panorama アプライアンス（Panorama サーバー）、および必要に応じてバックアップ Panorama サーバーの IP アドレスまたは FQDN を設定します。 `set deviceconfig system panorama-server <ip-address | FQDN>`

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	`set deviceconfig system panorama-server-2 <ip-address | FQDN>`
設定のインポート	WildFire アプライアンスと **Import Config**（設定のインポート）を選択し、そのアプライアンスの実行中の設定（のみ）を Panorama にインポートします。 設定をインポートしたら、**Commit to Panorama**（**Panorama** にコミット）により、インポートした候補設定を Panorama の実行中の設定に保存します。
削除	WildFire アプライアンスを Panorama から管理する必要がなくなった場合は、アプライアンスを **Remove**（削除）し、**Yes**（はい）を選択してアクションを確定します。アプライアンスを Panorama の管理から削除した後は、CLI を使用してそのアプライアンスをローカルで管理できます。アプライアンスをローカルではなくて再び中央管理する場合は、必要に応じて、そのアプライアンスを Panorama アプライアンスにいつでも追加しなおすことができます。

管理対象 WildFire の情報

管理対象クラスタごとに次の情報を表示するには、**Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）を選択し（スタンドアロン アプライアンスをこのページから選択して情報を表示することもできます）、スタンドアロン アプライアンスの情報を表示するには、**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス）を選択します。

特筆しない限り、次の表の情報は、WildFire クラスタとスタンドアロン アプライアンスの両方に適用されます。クラスタまたはアプライアンスで以前に設定した情報は事前に入力されます。

管理対象 WildFire の情報	の意味
アプライアンス	アプライアンスの名称。 管理対象 WildFire クラスタ ビューには、クラスタ別に分類されたアプライアンスが表示され、クラスタに追加可能なスタンドアロン アプライアンスが含まれ、シリアル番号（括弧内）とアプライアンス名が含まれます（シリアル番号は名前の一部ではありません）。
シリアル番号 （管理対象 WildFire アプライアンス ビューのみ）	アプライアンスのシリアル番号管理対象 WildFire クラスタ ビューには、アプライアンス名と同じ列にシリアル番号が表示されます（シリアル番号は名前の一部ではありません）。
ソフトウェア バージョン	アプライアンスでインストールされて動作しているソフトウェアのバージョン。
IPアドレス	アプライアンスの IP アドレス。
接続済み	アプライアンスと Panorama の接続状態であり、接続済みまたは切断のいずれかになります。
クラスタ名	アプライアンスがノードとして組み込まれているクラスタの名前。スタンドアロン アプライアンスの場合、ここには何も表示されません。

© 2019 Palo Alto Networks, Inc.

管理対象 WildFire の情報	の意味
分析環境	分析環境 (vm1、vm2、vm3、vm4、vm5) 。各分析環境は、一連のオペレーティング システムとアプリケーションを表します。 • vm-1 では、Windows XP、Adobe Reader 9.3.3、Flash 9、PE、PDF、Office 2003 以前の Office リリースがサポートされます。 • vm-2 では、Windows XP、Adobe Reader 9.4.0、Flash 10n、PE、PDF、Office 2007 以前の Office リリースがサポートされます。 • vm-3 では、Windows XP、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートされます。 • vm-4 では、Windows 7 の 32 ビット、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートされます。 • vm-5 では、Windows 7 の64 ビット、Adobe Reader 11、Flash 11、PE、PDF、Office 2010 以前の Office リリースがサポートされます。
コンテンツ	コンテンツ リリース バージョンのバージョン番号。
ロール	アプライアンスのロール: • **Standalone** (スタンドアロン) – アプライアンスはクラスタ ノードになっていません。 • **Controller** (コントローラ) – アプライアンスはクラスタのコントローラ ノードです。 • **Controller Backup** (コントローラ バックアップ) – アプライアンスはクラスタのコントローラ バックアップ ノードです。 • **Worker** (ワーカー) – アプライアンスは、クラスタのワーカー ノードです。
設定状態	アプライアンスの設定の同期状態。Panorama アプライアンスは WildFire アプライアンスの設定を確認し、アプライアンスの設定と Panorama でそのアプライアンス用に保存されている設定との間で設定の違いをレポートします。 • **In Sync** (同期されています) – アプライアンスの設定は、Panorama で保存されている設定と同期しています。 • **Out of Sync** (同期されていません) – アプライアンスの設定は、Panorama で保存されている設定と同期していません。眼鏡にマウスを合わせると、同期の失敗の原因が表示されます。

クラスタ状態
(管理対象 WildFire クラスタ ページのみ)
	クラスタ状態には、クラスタ ノードごとに次の 3 種類の情報が表示されます。
	• サービス使用可能 (正常な動作状態) :
	  • **wfpc** (WildFire プライベート クラウド) – マルウェア サンプル分析とレポート サービス。
	  • シグネチャ – ローカル シグネチャ生成サービス。
	• 操作の進捗状況 – 操作名に続けてコロン (:) と状態が表示されます。
	  • 操作 – 使用停止、中断、再起動の操作の状態。
	  • 進捗状況 – 操作状態の通知は各操作で同じであり、要求、継続中、拒否、成功、失敗のいずれかになります。
	たとえば、ノードを中断して操作が継続中である場合、クラスタ状態は `suspend:ongoing` と表示されます。ノードを再起動して、操作が要求されたがまだ始まっていない場合、クラスタ状態は `reboot:requested` と表示されます。

© 2019 Palo Alto Networks, Inc.

管理対象 WildFire の情報	の意味
	• エラー条件: クラスタ状態には、次のエラー条件が表示されます。 • クラスタ – `cluster:offline` または `cluster:splitbrain`。 • サービス – `service:suspended` または `service:none`。
最終コミット状態	直近のコミットが成功した場合は `Commit succeeded`。直近のコミットが失敗した場合は `commit failed`。状態を選択して、前回のコミットに関する詳細を表示してください。
Utilization（使用率）> View（表示）	

表示、ビュー	クラスタまたはアプライアンスの使用率統計を **View**（表示）します。個別のアプライアンスのみを表示するか（**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス））、クラスタ統計のみを表示します（**Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ））。
	• **Appliance**（アプライアンス）–（スタンドアロン アプライアンスの表示のみ）アプライアンスのシリアル番号。
	• **Cluster**（クラスタ）–（クラスタの表示のみ）クラスタ名。別のクラスタを選択して表示することもできます。
	• **Duration**（期間）– 統計を収集して表示する期間が表示されます。以下の各期間を選択できます。
	  • **15** 分間
	  • 過去 **1** 時間
	  • 過去 **24** 時間（デフォルト）
	  • 過去 **7** 日
	  • すべて
	Utilization（使用率）の **View**（表示）には 4 つのタブがあり、各タブでは、設定した **Duration**（期間）に基づいて、何が表示されるかが決まります。

General [全般] タブ	**General**（全般）タブには、クラスタまたはアプライアンスの集約済みリソース使用率統計が表示されます。その他のタブには、リソース使用率に関する詳細がファイル タイプ別に表示されます。
	• **Total Disk Usage**（合計ディスク使用率）– クラスタまたはアプライアンスの合計ディスク使用率。
	• **Verdict**（判定）– 判定の **Total**（合計）数、ファイルに割り当てられた各判定タイプの数（**Malware**（マルウェア）、**Grayware**（グレイウェア）、**Benign**（安全））、**Error**（エラー）判定だった判定の数。
	• **Sample Statistics**（サンプル統計）– **Submitted**（送信済み）と **Analyzed**（分析済み）のサンプルの合計数、および分析が **Pending**（保留中）のサンプルの数。
	• **Analysis Environment & System Utilization**（分析環境とシステム使用率）：
	  • **File Type Analyzed**（分析したファイル タイプ）– 分析したファイルのタイプ（**Executable**（実行可能）、**Non-Executable**（実行可能以外）、**Links**（リンク））。
	  • **Virtual Machine Usage**（仮想マシン使用率）– 分析された各ファイル タイプに使用された仮想マシンの数、および各ファイル タイプの分析に使用

© 2019 Palo Alto Networks, Inc.

管理対象 WildFire の情報	の意味
	できる仮想マシンの数。たとえば、実行可能ファイルの場合、VM 使用率は 6/10（使用可能 VM 10 個中の VM 6 個）になることがあります。 • **Files Analyzed**（分析済みファイル数）— 分析された各タイプのファイルの数。

Executable（実行可能）タブ、Non-Executable（実行可能以外）タブ、Links（リンク）タブ	**Executable**（実行可能）、**Non-Executable**（実行可能以外）、**Links**（リンク）には、各ファイル タイプについて同じような情報が表示されます。
	• **Verdict**（判定）— ファイル タイプ別の判定に関する詳細。結果はフィルタリングできます。
	  • 検索ボックス — 検索条件を入力し、判定をフィルタリングします。検索ボックスには、リストのファイル タイプ（項目）の数が表示されます。検索条件を入力したら、フィルタを適用するか（）、フィルタをクリアして（）別の一連の条件を入力します。
	  • **File Type**（ファイル タイプ）— ファイルがタイプ別にリストされます。たとえば、**Executable**（実行可能）タブには .exe と .dll、**Non-Executable**（実行可能以外）タブには、.pdf、.jar、.doc、.ppt、.xls、.docx、.pptx、.xlsx、.rtf、class、.swf、**Links**（リンク）タブには elink ファイル タイプの情報が表示されます。
	  • 各タブでは、**File Type**（ファイル タイプ）ごとに、**Malware**（マルウェア）、**Grayware**（グレイウェア）、**Benign**（安全）の判定の合計数、**Error**（エラー）判定の数、判定の **Total**（合計）数が表示されます。
	• **Sample Statistics**（サンプル統計）— ファイル タイプ別のサンプル分析に関する詳細。
	  • 検索ボックス — **Verdict**（判定）の検索ボックスと同じです。
	  • **File Type**（ファイル タイプ）— **Verdict**（判定）の **File Type**（ファイル タイプ）と同じです。
	  • 各タブでは、**File Type**（ファイル タイプ）ごとに、分析のために **Submitted**（送信済み）となったファイルの合計数、**Analyzed**（分析済み）の合計数、分析が **Pending**（保留中）の数が表示されます。

Firewalls Connected（接続済みファイアウォール）> View（表示）	
表示、ビュー	クラスタまたはアプライアンスに接続しているファイアウォールに関する情報を **View**（表示）します。個別のアプライアンスのみを表示するか（**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス））、クラスタ統計のみを表示します（**Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ））。 • **Appliance**（アプライアンス）—（スタンドアロン アプライアンスの表示のみ）アプライアンスのシリアル番号。 • **Cluster**（クラスタ）—（クラスタの表示のみ）クラスタ名。別のクラスタを選択して表示することもできます。 • **Refresh**（更新）— 表示を更新します。
Registered（登録済み）タブと Submitting Samples（サンプル送信）タブ	**Registered**（登録済み）タブには、クラスタまたはアプライアンスに登録されているファイアウォールに関する情報が、そのファイアウォールがサンプルを送信しているかどうかに関係なく表示されます。

© 2019 Palo Alto Networks, Inc.

管理対象 WildFire の情報	の意味
	Submitting Samples（サンプル送信）タブには、WildFire クラスタまたはアプライアンスにサンプルをアクティブに送信しているファイアウォールに関する情報が表示されます。 これらのタブに表示される情報のタイプ、および情報をフィルタリングする方法は、両方で同じです。 • 検索ボックス – 検索条件を入力し、ファイアウォールのリストをフィルタリングします。検索ボックスには、リストのファイアウォール（項目）の数が表示されます。検索条件を入力したら、フィルタを適用するか（➡）、フィルタをクリアして（✖）別の一連の条件を入力します。 • **S/N** – ファイアウォールのシリアル番号。 • **IP address**（**IP** アドレス）– ファイアウォールの IP アドレス。 • **Model**（モデル）– ファイアウォールのモデル番号。 • **Software Version**（ソフトウェア バージョン）– ファイアウォールでインストールされて動作しているソフトウェアのバージョン。

管理対象 WildFire クラスタおよびアプライアンスの管理

Panorama > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ）を選択し、クラスタを選択して管理するか、WildFire アプライアンスを選択して（**Panorama** > **Managed WildFire Appliances**（管理対象 **WildFire** アプライアンス））スタンドアロン アプライアンスを管理します。**Panorama** > **Managed WildFire Cluster**（管理対象 **WildFire** クラスタ）ビューには、クラスタ ノード（クラスタのメンバーである WildFire アプライアンス）とスタンドアロン アプライアンスがリストされるため、使用可能なアプライアンスをクラスタに追加できます。クラスタではノードを管理するため、クラスタ ノードを選択すると、限定された管理機能のみが提供されます。

特筆しない限り、次の表の設定と説明は、WildFire クラスタと WildFire スタンドアロン アプライアンスの両方に適用されます。クラスタまたはアプライアンスで設定した情報は事前に入力されます。最初に Panorama の情報に変更や追加をコミットしてから、新しい設定をアプライアンスにプッシュする必要があります。

setting	の意味
General [全般] タブ	
氏名	クラスタまたはアプライアンスの **Name**（名前）、またはアプライアンスのシリアル番号。
DNS の有効化 （WildFire クラスタのみ）	クラスタの **Enable DNS**（**DNS** の有効化）を行います。
ファイアウォールの登録先	ファイアウォールを登録するドメイン名。`wfpc.service.`<*cluster-name*>`.`<*domain*> という形式にしてください。たとえば、デフォルトのドメイン名は `wfpc.service.mycluster.paloaltonetworks.com` です。
コンテンツ更新サーバー	**Content Update Server**（コンテンツ更新サーバー）の場所を入力するか、デフォルトの `wildfire.paloaltonetworks.com` を使用し、クラスタまたはアプライアンスが、コンテンツ配信ネットワーク インフラストラクチャで最も近いサーバーからコンテンツ更新を受信するようにします。グローバル クラウド

© 2019 Palo Alto Networks, Inc.

setting	の意味
	に接続すると、ローカルの脅威の分析のみに依存するのではなく、クラウドに接続したすべてのソースからの脅威分析に基づいて、シグネチャと更新にアクセスできるようになります。
サーバー アイデンティティのチェック	証明書の共通名（CN）をサーバーの IP アドレスまたは FQDN と照合し、更新サーバーのアイデンティティを確認するには、**Check Server Identity**（サーバーアイデンティティのチェック）を行います。
WildFire クラウド サーバー	グローバルの **WildFire Cloud Server**（**WildFire** クラウド サーバー）の場所を入力するか、デフォルトの `wildfire.paloaltonetworks.com` を使用し、クラスタまたはアプライアンスが最も近いサーバーに情報を送信できるようにします。情報を送信するかどうか、およびどのような種類の情報をグローバル クラウド（**WildFire Cloud Services**（**WildFire** クラウド サービス））に送信するかは選択できます。
サンプル分析イメージ	クラスタまたはアプライアンスがサンプル分析に使用する VM イメージを選択します（デフォルトは vm-5）。マルウェア テスト ファイル（WildFire API）を取得すると、サンプル分析の結果を確認できます。
WildFire クラウド サービス	クラスタまたはアプライアンスをグローバル WildFire クラウド サーバーに接続すると、**Send Analysis Data**（分析データの送信）、**Send Malicious Samples**（有害サンプルの送信）、**Send Diagnostics**（診断の送信）をグローバル クラウドに対して行うかどうか、または 3 つの組み合わせのいずれかを選択できます。また、グローバルクラウドで **Verdict Lookup**（判定ルックアップ）を実行するかどうかを選択することもできます。グローバル クラウドに情報を送信すると、WildFire ユーザーのコミュニティ全体が利益を得ることになります。共有情報により、すべてのアプライアンスが有害トラフィックを特定して、ネットワークを通過することを防止する能力が高まるためです。
サンプル データ保持	安全、グレイウェア、有害のサンプルを保持する日数。 • **Benign/Grayware**（安全/グレイウェア）サンプル — 範囲は 1 ~ 90、デフォルトは 14 です。 • **Malicious**（有害） サンプル — 最小は 1 で、最大はありません（無期限）です。デフォルトは無期限です。
分析環境サービス	**Environment Networking**（環境ネットワーク）では、仮想マシンがインターネットと通信できるようになります。**Anonymous Networking**（匿名ネットワーク）を選択してネットワーク通信を匿名にすることができますが、**Environment Networking**（環境ネットワーク）を選択してから **Anonymous Networking**（匿名ネットワーク）を有効にする必要があります。 ネットワーク環境が異なると、分析する必要があるドキュメントが多いか、分析する必要がある実行可能ファイルが多いかに応じて、分析負荷のタイプが異なります。優先分析環境を設定すると、環境のニーズに応じて、**Executables**（実行可能ファイル）または **Documents**（ドキュメント）に割り当てるリソースを増やすことができます。**Default**（デフォルト）割り当てでは、**Executables**（実行可能ファイル）と **Documents**（ドキュメント）が均等になります。 使用可能リソースの量は、クラスタに WildFire ノードがいくつあるかによって決まります。

© 2019 Palo Alto Networks, Inc.

setting	の意味
シグネチャ生成	クラスタまたはアプライアンスで、AV、DNS、URL シグネチャまたは 3 つの組み合わせを選択します。
アプライアンス タブ	
ホスト名 （スタンドアロン WildFire アプライアンスのみ）	WildFire アプライアンスのホスト名を入力します。
Panorama サーバー	アプライアンスの IP アドレスか FQDN、またはクラスタを管理しているプライマリ Panorama の IP アドレスか FQDN を入力します。
Panorama サーバー 2	アプライアンスの IP アドレスか FQDN 、またはクラスタを管理しているバックアップ Panorama の IP アドレスか FQDN を入力します。
ドメイン	アプライアンス クラスタまたはアプライアンスのドメイン名を入力します。
プライマリDNSサーバー	プライマリ DNS サーバーの IP アドレスを入力します。
セカンダリ DNS サーバー	セカンダリ DNS サーバーの IP アドレスを入力します。
タイムゾーン	クラスタまたはアプライアンスに使用するタイム ゾーンを選択します。
緯度 （スタンドアロン WildFire アプライアンスのみ）	緯度アプライアンスのホスト名を入力します。
経度 （スタンドアロン WildFire アプライアンスのみ）	経度アプライアンスのホスト名を入力します。
プライマリ NTP サーバー	プライマリ NTP サーバーの IP アドレスを入力し、認証タイプを **None**（なし）（デフォルト）、**Symmetric Key**（対称キー）、**Autokey**（自動キー）のいずれかに設定します。 認証タイプを **Symmetric Key**（対称キー）に設定すると、さらに 4 つのフィールドが表示されます。 • **Key ID**（キー **ID**） – 認証キー ID を入力します。 • **Algorithm**（アルゴリズム） – **SHA1** または **MD5** への認証アルゴリズムを設定します。 • **Authentication Key**（認証キー） – 認証キーを入力します。 • **Confirm Authentication Key**（再入力 認証キー） – 認証キーを確認のためにもう一度入力します。

© 2019 Palo Alto Networks, Inc.

setting	の意味
セカンダリ NTP サーバー	セカンダリ NTP サーバーの IP アドレスを入力し、認証タイプを **None**（なし）（デフォルト）、**Symmetric Key**（対称キー）、**Autokey**（自動キー）のいずれかに設定します。 認証タイプを **Symmetric Key**（対称キー）に設定すると、さらに 4 つのフィールドが表示されます。 • **Key ID**（キー **ID**） – 認証キー ID を入力します。 • **Algorithm**（アルゴリズム） – **SHA1** または **MD5** への認証アルゴリズムを設定します。 • **Authentication Key**（認証キー） – 認証キーを入力します。 • **Confirm Authentication Key**（再入力 認証キー） – 認証キーを確認のためにもう一度入力します。
ログイン バナー	ユーザーがクラスタまたはアプライアンスにログインするときに表示されるバナー メッセージを入力します。
Logging（ログ）タブ（System（システム）タブと Configuration（設定）タブを含む）	
コンテキストの	転送するためのログ転送プロファイルを **Add**（追加）します（**Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ） > *<cluster>* > **Logging**（ロギング） > **System**（システム）または **Panorama** > **Managed WildFire Clusters**（管理対象 **WildFire** クラスタ） > *<cluster>* > **Logging**（ロギング） > **Configuration**（設定））。 • SNMP トラップ レシーバへの SNMP トラップとしてのシステム ログまたは設定ログ • syslog サーバーへの syslog メッセージ • 電子メール サーバーへの電子メール通知 • HTTP サーバーへの HTTP 要求 その他のログ タイプはサポートされません（「Device（デバイス）> Log Settings（ログ設定）」を参照）。 ログ転送プロファイルでは、どのログをどの宛先サーバーに転送するかを指定します。プロファイルごとに以下を設定します。 • **Name**（名前） – ログ設定を識別する名前（最大 31 文字）。英数字と下線のみを使用でき、スペースと特殊文字は使用できません。 • **Filter**（フィルタ） – デフォルトでは、Panorama アプライアンスは、指定されたプロファイルの **All Logs**（すべてのログ）を転送します。一部のログを転送するには、フィルタを選択するか（**severity eq critical**（重大度が重要）、**severity eq high**（重大度が高）、**severity eq informational**（重大度が通知）、**severity eq low**（重大度が低）、**severity eq medium**（重大度が中））、**Filter Builder**（フィルタ ビルダー）を選択して新しいフィルタを作成します。 • **Description**（説明） – 説明（最大 1,023 文字）を入力し、プロファイルの目的について説明します。
Add（追加）> Filter（フィルタ）> Filter Builder（フィルタ ビルダー）	新しいログ フィルタを作成するには、**Filter Builder**（フィルタ ビルダー）を使用します。**Create Filter**（フィルタの作成）を選択してフィルタを作成し、新しいフィルタのクエリごとに次の設定を指定してからクエリを **Add**（追加）します。

© 2019 Palo Alto Networks, Inc.

setting	の意味

	• **Connector**（条件式）— 論理結合子（**and** または **or**）を選択します。**Negate**（上記以外）を選択すると、指定した内容を除外します。たとえば、一部のログ説明の転送を回避するには、属性として **Description**（説明）を選択して演算子として **contains**（含む）を選択し、転送しない説明を識別する値として説明の文字列を入力します。
	• **Attribute**（属性）— ログの属性を選択します。ログ タイプによりオプションが異なります。
	• **Operator**（演算子）— 属性の適用方法を決める基準を選択します（**contains**（含む）など）。ログ タイプによりオプションが異なります。
	• **Value**[値] — 照合する属性値を指定します。
	• **Add**（追加）— 新しいフィルタを追加します。
	
	フィルタで一致するログの表示またはエクスポートを行うには、**View Filtered Logs**（フィルタリングされたログの表示）を選択します。
	
	• 一致するログ エントリを検索するには、検索フィールドに IP アドレスや時間範囲などのアーチファクトを入力します。
	• 次のログを表示する期間を選択します。**Last 15 Minutes**（**15** 分前）、**Last Hour**（**1** 時間前）、**Last 6 Hrs**（**6** 時間前）、**Last 12 Hrs**（**12** 時間前）、**Last 24 Hrs**（**24** 時間前）、**Last 7 Days**（**7** 日前）、**Last 30 Days**（**30** 日前）、または **All**（全て）（デフォルト）。
	• 期間ドロップダウン リストの右にあるオプションを使用し、フィルタの適用、クリア、追加、保存、ロードを行います。
	  • フィルタの適用（ ）— 検索フィールドの条件に一致するログ エントリが表示されます。
	  • フィルタのクリア（ （ — フィルタ フィールドをクリアします。
	  • 新しいフィルタの追加（ ）— 新しい検索条件を定義します（Add Log Filter（ログ フィルタの追加）が表示されますが、これはフィルタの作成と同じです）。
	  • フィルタの保存（ ）— フィルタの名前を入力してから **OK** をクリックします。
	  • 保存したフィルタを使用（ ）— 保存したフィルタをフィルタ フィールドに追加します。
	  • **CSV** にエクスポート（ ）— CSV 形式のレポートにログをエクスポートし、**Download file**（ファイルをダウンロード）します。レポートにはデフォルトで最大2,000行のログを含むよう設定されています。CSV レポートの行数制限を変更する場合は、**Device**（デバイス）> **Setup**（セットアップ）> **Management**（管理）> **Logging and Reporting Settings**（ログとレポートの設定）> **Log Export and Reporting**（ログのエクスポートとレポート）を開き、新しい **Max Rows in CSV Export**（**CSV** エクスポートの最大行数）を入力します。
	
	ページごとに表示されるエントリの数と順序を変更でき、ページの左下にあるページ送り機能を使用してログ リスト内を移動できます。ログ エントリは、10 ページのブロック単位で取得されます。
	
	• ページごと — ドロップダウン リストを使用し、ページごとのログ エントリの数を変更します（**20**、**30**、**40**、**50**、**75**、**100**）。
	• **ASC**（昇順）または **DESC**（降順）— 結果を昇順で（古いログ エントリが先）ソートするには **ASC**（昇順）を選択し、降順で（新しいログ エントリが

© 2019 Palo Alto Networks, Inc.

setting	の意味

	先）ソートするには **DESC**（降順）を選択します。デフォルトは **DESC**（降順）です。
	• **Resolve Hostname**（ホスト名の解決）– 外部 IP アドレスをドメイン名に解決する場合に選択します。
	• **Highlight Policy Actions**（ポリシー アクションの強調表示）– アクションを選択し、アクションと一致するログ エントリを強調表示する場合に選択します。フィルタリングされたログは、次の色で強調表示されます。
	  • 緑 – 許可
	  • 黄 – 継続またはオーバーライド
	  • 赤 – 却下、ドロップ、drop-icmp、st-client、reset-server、reset-both、block-continue、block-override、block-url、drop-all、sinkhole

削除します。	システム ログ リストまたは設定ログ リストから削除するログ転送設定を選択してから **Delete**（削除）します。
認証タブ	
リモート認証リモートニンショウ	アクセスする **Authentication Profile**（認証プロファイル）を選択します。デフォルト設定は**None**[なし] です。選択する認証プロファイルがない場合は、認証プロファイルとシーケンスを設定できます。

ローカル認証	管理者のローカル認証を設定します。
	• **Administrator**（管理者）– Panorama アプライアンスでは管理者レベル ユーザーが 1 つのみであるため、常に **admin** になります。
	• **Mode**（モード）– ローカル認証モード（**Password**（パスワード）または **Password Hash**（パスワード ハッシュ））を設定します。
	  • **Password**（パスワード）– ユーザー パスワードを入力して確認します。
	  • **Password Hash**[パスワード ハッシュ] – ハッシュされたパスワード文字列を入力します。たとえば、既存の UNIX アカウントの認証情報を再利用したいが、プレーンテキストのパスワードがわからず、ハッシュされたパスワードを覚えている場合は、ハッシュされたパスワードが便利です。アプライアンスでは、ハッシュ値の生成に使用されるアルゴリズムに関係なく、63 文字までの任意の文字列を使用できます。ファイアウォールで設定したパスワード複雑性設定のパラメータ（**Panorama** > **Setup**（セットアップ）> **Management**（管理））は、パスワード ハッシュを使用するアカウントに適用されません。

Timeout configuration	クラスタ認証タイムアウトを設定します。 • **Idle Timeout (min)**（アイドル タイムアウト（分））– アイドル タイムアウトを分単位で設定します。何も操作しない時間が、指定したアイドル タイムアウトより長くなると、ユーザーのセッションは終了します。デフォルトは **None**（なし）です（タイムアウトなし）。 • **Failed Attempts**（最大試行回数）– ログイン試行の失敗回数を設定します。これを超えると、ユーザーはシステムからロックアウトされます。デフォルトの最大試行回数は 10 回です。 • **Lockout Time (min)**（ロックアウト時間（分））– ロックアウトされたユーザーが再度ログインするまでに待機する時間を分単位で設定します。デフォルトは 5 分です。

© 2019 Palo Alto Networks, Inc.

setting	の意味
Clustering (クラスタ) タブ (管理対象 WildFire クラスタのみ) および Interface (インターフェイス) タブ (管理対象 WildFire アプライアンスのみ) アプライアンスを Panorama に追加してインターフェイスを管理し、アプライアンスをクラスタに追加してノードのインターフェイスを管理する必要があります。	
アプライアンス (Clustering (クラスタ) タブのみ)	クラスタ ノードを選択し、そのノードの Appliance (アプライアンス) タブと Interfaces (インターフェイス) タブにアクセスします。Appliance (アプライアンス) タブのノード情報は事前に入力され、ホスト名以外は設定できません。Interfaces (インターフェイス) タブにはノードのインターフェイスがリストされます。以下に記載されるように管理するインタフェースを選択します。 • インターフェイス名管理 • インターフェイス名分析環境ネットワーク • インターフェイス名 Etherrnet2 • インターフェイス名 Etherrnet3
インターフェイス名管理	管理インターフェイスは Ethernet0 です。管理インターフェイスの設定を構成するか表示します。 • **Speed and Duplex** (速度とデュプレックス) – **auto-negotiate** (デフォルト)、**10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex**、**1Gbps-full-duplex** のいずれかを選択します。 • **IP Address** (**IP** アドレス) – インターフェイスの IP アドレスを入力します。 • **Netmask** (ネットマスク) – インターフェイスのネットマスクを入力します。 • **Default Gateway** (デフォルト ゲートウェイ) – デフォルト ゲートウェイの IP アドレスを入力します。 • **MTU** – MTU をバイト単位で入力します (範囲は 576 ~ 1,500、デフォルトは 1,500)。 • **Management Services** (管理サービス) – サポートする管理サービスを有効にします。**Ping**、**SSH**、**SNMP** サービスをサポートできます。 プロキシ サーバーを使用してインターネットに接続する場合は、プロキシ設定を構成します。 • **Server** (サーバー) – プロキシ サーバーの IP アドレス。 • **Port** (ポート) – プロキシ サーバーで Panorama デバイス要求を待ち受けるように設定されているポート番号。 • **User** (ユーザー) – プロキシ サーバーで認証用に設定されているユーザー名。 • **Password** (パスワード) および **Confirm Password** (再入力 パスワード) – プロキシ サーバーで認証用に設定されているパスワード • **Clustering Services** (クラスタ サービス) (Clustering (クラスタ) タブのみ) – HA サービスを選択します。 • **HA** – 2 つのコントローラ ノードがクラスタにある場合は、管理インターフェイスを HA インターフェイスとして設定し、管理情報を両方のクラスタ ノードで使用できるようにします。設定しているクラスタ ノードがプライマリ コントローラ ノードである場合は、それを **HA** インターフェイスとしてマークしてください。

© 2019 Palo Alto Networks, Inc.

setting	の意味
	WildFire アプライアンスのイーサネット インターフェイスの使用方法に応じて、プライマリ コントローラ ノードでは HA インターフェイスとして、バックアップ コントローラ ノードでは HA バックアップ インターフェイスとして、Etherent2 または Ethernet3 を設定することもできます。たとえば、Ethernet2 を HA と HA バックアップ インターフェイスとして使用できます。HA と HA バックアップ インターフェイスは、プライマリ コントローラ ノードとバックアップ コントローラ ノードで同じインターフェイス (管理、Ethernet2、Ethernet3) にする必要があります。Ethernet1 を HA/HA バックアップ インターフェイスとして使用することはできません。 • **HA Backup** (**HA** バックアップ) – 設定しているクラスタ ノードがバックアップ コントローラ ノードである場合は、それを **HA Backup** (**HA** バックアップ) インターフェイスとしてマークします。 インターフェイスで許可される IP アドレスを指定します。 • 検索ボックス – 検索条件を入力し、許可される IP アドレスのリストをフィルタリングします。検索ボックスにはリストの IP アドレス (項目) の数が表示されるため、リストの長さが分かるようになっています。検索条件を入力したら、フィルタを適用するか ( ) 、フィルタをクリアして ( ) 別の一連の条件を入力します。 • **Add** (追加) –権限のある IP アドレスを **Add** (追加) します。 • **Delete** (削除) – 管理インターフェイス アクセスから削除する IP アドレスを選択して **Delete** (削除) します。
インターフェイス名分析環境ネットワーク	WildFire アプライアンス クラスタまたはスタンドアロン WildFire アプライアンスの分析環境ネットワーク インターフェイス (Ethernet1、VM インターフェイスとも呼ばれる) の設定を構成します。 • **Speed and Duplex** (速度とデュプレックス) – **auto-negotiate** (デフォルト) 、**10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex**、**1Gbps-full-duplex** のいずれかを設定します。 • **IP Address** (**IP** アドレス) – インターフェイスの IP アドレスを入力します。 • **Netmask** (ネットマスク) – インターフェイスのネットマスクを入力します。 • **Default Gateway** (デフォルト ゲートウェイ) – デフォルト ゲートウェイの IP アドレスを入力します。 • **MTU** – MTU をバイト単位で入力します (範囲は 576 ~ 1,500、デフォルトは 1,500) 。 • **DNS Server** (**DNS** サーバー) – DNS サーバーの IP アドレスを入力します。 • **Link State** (リンク状態) – インターフェイスのリンク状態を **Up** (アップ) または **Down** (ダウン) に設定します。 • 管理サービス – インターフェイスで Ping サービスをサポートする場合は、**Ping** を有効にします。 インターフェイスで許可される IP アドレスを指定します。 • 検索ボックス – 検索条件を入力し、許可される IP アドレスのリストをフィルタリングします。検索ボックスにはリストの IP アドレス (項目) の数が表示されるため、リストの長さが分かるようになっています。検索条件を入力したら、フィルタを適用するか ( ) 、フィルタをクリアして ( ) 別の一連の条件を入力します。

© 2019 Palo Alto Networks, Inc.

setting	の意味
	• **Add**（追加）–権限のある IP アドレスを **Add**（追加）します。 • **Delete**（削除）– 管理インターフェイス アクセスから削除する IP アドレスを選択して **Delete**（削除）します。

インターフェイス名 Etherrnet2
 	
インターフェイス名 Etherrnet3
	Ethernet2 インターフェイスと Ethernet3 インターフェイスには同じパラメータを設定できます。
	
	• **Speed and Duplex**（速度とデュプレックス）– **auto-negotiate**（デフォルト）、**10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex**、**1Gbps-full-duplex** のいずれかを設定します。
	• **IP Address**（**IP** アドレス）– インターフェイスの IP アドレスを入力します。
	• **Netmask**（ネットマスク）– インターフェイスのネットマスクを入力します。
	• **Default Gateway**（デフォルト ゲートウェイ）– デフォルト ゲートウェイの IP アドレスを入力します。
	• **MTU** – MTU をバイト単位で入力します（範囲は 576 ~ 1,500、デフォルトは 1,500）。
	• 管理サービス – インターフェイスで Ping サービスをサポートする場合は、**Ping** を有効にします。
	• **Clustering Services**（クラスタ サービス）– クラスタ サービスを選択します。
	
	  • **HA** – 2 つのコントローラ ノードがクラスタにある場合は、Ethernet2 または Ethernet3 インターフェイスを HA インターフェイスとして設定し、管理情報を両方のクラスタ ノードで使用できるようにします。設定しているクラスタ ノードがプライマリ コントローラ ノードである場合は、それを **HA** インターフェイスとしてマークしてください。
	
	  WildFire アプライアンスのイーサネット インターフェイスの使用方法に応じて、プライマリ コントローラ ノードでは HA インターフェイスとして、バックアップ コントローラ ノードでは HA バックアップ インターフェイスとして、管理インターフェイス（Etherent1）を設定することもできます。HA と HA バックアップ インターフェイスは、プライマリ コントローラ ノードとバックアップ コントローラ ノードで同じインターフェイス（管理、Ethernet2、Ethernet3）にする必要があります。Ethernet1 を HA/HA バックアップ インターフェイスとして使用することはできません。
	  • **HA Backup**（**HA** バックアップ）– 設定しているクラスタ ノードがバックアップ コントローラ ノードである場合は、それを **HA Backup**（**HA** バックアップ）インターフェイスとしてマークします。
	  • **Cluster Management**（クラスタ管理）– クラスタ全体の管理と通信に使用するインターフェイスとして、Ethernet2 または Ethernet3 インターフェイスを設定します。

ロール （Clustering（クラスタ）タブのみ）	クラスタにメンバー アプライアンスがあるとき、アプライアンスのロールは、コントローラ、コントローラ バックアップ、ワーカーのいずれかにすることができます。クラスタのアプライアンスから各ロールに使用する WildFire アプライアンスを変更するには、**Controller**（コントローラ）または **Backup Controller**（バックアップ コントローラ）を選択します。コントローラを変更すると、ロール変更中にデータが失われます。

© 2019 Palo Alto Networks, Inc.

setting	の意味
参照 （Clustering（クラスタ）タブのみ）	**Clustering**（クラスタ）タブには、クラスタの WildFire アプライアンス ノードがリストされます。**Browse**（参照）により、Panorama デバイスがすでに管理しているスタンドアロン WildFire アプライアンスを表示して追加します。 • 検索ボックス – 検索条件を入力し、ノード リストをフィルタリングします。検索ボックスにはリストのアプライアンス（項目）の数が表示されるため、リストの長さが分かるようになっています。検索条件を入力したら、フィルタを適用するか（）、フィルタをクリアして（）別の一連の条件を入力します。 • ノード追加–()ノードをクラスタに追加します。 クラスタに最初に追加する WildFire アプライアンスは、自動的にコントローラ ノードになります。2 番目に追加する WildFire アプライアンスは、自動的にコントローラ バックアップ ノードになります。 最大で 20 個の WildFire アプライアンスをクラスタに追加できます。コントローラ ノードとコントローラ バックアップ ノードを追加したら、その後で追加するすべてのノードはワーカー ノードになります。
削除します。 （Clustering（クラスタ）タブのみ）	1 つ以上のアプライアンスをアプライアンス リストから選択し、クラスタから **Delete**（削除）します。コントローラ ノードを削除できるのは、クラスタに 2 つのコントローラ ノードがある場合のみです。
コントローラの管理 （Clustering（クラスタ）タブのみ）	**Manage Controller**（コントローラの管理）を選択し、クラスタに属す WildFire アプライアンス ノードから **Controller**（コントローラ）と **Controller Backup**（コントローラ バックアップ）を指定します。現在のコントローラ ノードとバックアップ コントローラ ノードはデフォルトで選択されます。バックアップ コントローラ ノードをプライマリ コントローラ ノードと同じノードにすることはできません。
通信タブ	
保護されたサーバー通信のカスタマイズ	• **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）– ドロップダウン リストから SSL/TLS サービス プロファイルを選択します。このプロファイルは、WildFire との通信で接続デバイスが使用する証明書およびサポートされる SSL/TLS バージョンを定義します。 • **Certificate Profile**（証明書プロファイル）– ドロップダウン リストから証明書プロファイルを選択します。この証明書プロファイルは、証明書失効チェックの動作と、クライアントから提供された証明書チェーンの認証に使用できるルート CA を定義します。 • **Custom Certificate Only**（カスタム証明書のみ）– 有効にすると、WildFire は、接続デバイスとの認証用のカスタム証明書のみを受け付けます。 • **Check Authorization List**（承認リストのチェック）– WildFire に接続しているクライアント デバイスを承認リストと照合します。デバイスはリストの 1 項目のみと一致するだけで承認されます。一致がない場合、デバイスは承認されません。 • **Authorization List**（承認リスト）– クライアント デバイスの承認条件を設定するには、**Add**（追加）を選択し、以下のフィールドを入力します。Authorization List（承認リスト）は、最大 16 件のエントリをサポートします。

© 2019 Palo Alto Networks, Inc.

setting	の意味
	• **Identifier**（識別子）—Select **Subject**（サブジェクト）または **Subject Alt**（サブジェクト代替）を選択します。認証識別子としての**Name**（名前）を付けます。 • **Type**（タイプ）—**Subject Alt**（サブジェクト代替）の場合。**Name**（名前）を識別子として選択した場合、識別子のタイプとして**IP**、**hostname**（ホスト名）、または**e-mail**（電子メール）を選択します。**Subject**（サブジェクト）を選択した場合、共通名が識別子タイプになります。 • **Value**（値）— 識別子の値を入力します。

保護されたクライアント通信	**Secure Client Communication**（保護されたクライアント通信）を使用すると、WildFire は（デフォルトで事前定義される証明書の代わりに）設定済みのカスタム証明書を使用して、WildFire アプライアンスへの SSL 接続を認証します。
	• **Predefined**（事前定義済み）—（デフォルト）デバイス証明書は設定されていません。WaveFire はデフォルトの事前定義済み証明書を使用します。
	• **Local**（ローカル）—WildFire は、ファイアウォールで生成されたか既存のエンタープライズ PKI サーバーからインポートされたローカルのデバイス証明書および対応する秘密鍵を使用します。
	  • **Certificate**（証明書）：ローカル デバイス証明書を選択します。
	  • **Certificate Profile**（証明書プロファイル）：ドロップダウン リストから証明書プロファイルを選択します。
	• **SCEP** —WildFire は、Simple Certificate Enrollment Protocol（SCEP）サーバーで生成されたデバイス証明書と秘密鍵を使用します。
	  • **SCEP Profile**（**SCEP** プロファイル）：ドロップダウン リストから SCEP プロファイルを選択します。
	  • **Certificate Profile**（証明書プロファイル）：ドロップダウン リストから証明書プロファイルを選択します。

Secure Cluster Communication 安全なクラスタ通信	**Enable**（有効）を選択すると、WildFire アプライアンス間の通信を暗号化します。デフォルトの証明書では、定義済みの証明書タイプが使用されます。ユーザー定義のカスタム証明書を使用するには、**Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズを構成）し、**Custom Certificate Only**（カスタム証明書のみ）を有効にする必要があります。

© 2019 Palo Alto Networks, Inc.

Panorama > Administrators [Panorama > 管理者]

Panorama > **Administrators**（管理者）を選択し、Panorama 管理者のアカウントを作成および管理します。

スーパーユーザー ロールを持つ管理者として Panorama にログインすると、Locked User（ロックされたユーザー）列のロック アイコンをクリックして他の管理者のアカウントのロックを解除できます。ロックアウトされた管理者は Panorama を操作できません。Panorama は、アカウントに割り当てられた **Authentication Profile**（認証プロファイル）で定義されている、Panorama へのアクセスの連続失敗許容試行回数を超えた管理者をロックアウトします（「Device（デバイス）> Authentication Profile（認証プロファイル）」を参照）。

管理者アカウントを作成するには、**Add**（追加）をクリックし、以下の表の説明に従って設定を指定します。

管理者アカウント設定	の意味
氏名	管理者のログイン ユーザー名（最大 15 文字）を入力します。この名前は、大文字と小文字が区別され、一意でなければならず、文字、数字、ハイフン、アンダースコアのみで構成されます。
認証プロファイル	この管理者を認証する認証プロファイルまたは認証シーケンスを選択します。詳細は、「Device（デバイス）> Authentication Profile（認証プロファイル）」または「Device（デバイス）> Authentication Sequence（認証シーケンス）」を参照してください。
クライアント証明書認証のみを使用（Web）	Web インターフェイス アクセスのクライアント証明書認証を使用する場合に選択します。このオプションを選択すると、ユーザー名（**Name**（名前））とパスワード（**Password**（パスワード））は必要なくなります。
パスワード/再入力 パスワード	管理者のパスワード (最大 15 文字) を入力し、確認のためにパスワードを再入力します。このパスワードは大文字と小文字を区別します。セキュリティを確保するために、管理者がパスワードを定期的に変更することをお勧めします。パスワードには、小文字、大文字、および数字を組み合わせることをお勧めします。パスワードの強度を高めるために、必ずパスワード強度のベスト プラクティスに従ってください。 デバイス グループおよびテンプレートの管理者は **Panorama** > **Administrators**（管理者）にアクセスすることができません。この管理者のローカル パスワードを変更するには、管理者は（Web インターフェイス下部の **Logout**（ログアウト）の横にある）ユーザー名をクリックします。**Panorama** > **Administrators**（管理者）へのアクセス権限を無効化された Panorama ロールを持つ管理者の場合も同様です。 パスワード認証は**Authentication Profile**[認証プロファイル]と併用あるいは順に適用したり、ローカルデータベース認証と併用することができます。 パスワードの有効期限パラメータを設定するには、**Password Profile**（パスワード プロファイル）（「Device（デバイス）> Password Profiles（パスワード プロファイル）」を参照）を選択

© 2019 Palo Alto Networks, Inc.

管理者アカウント設定	の意味
	し、Minimum Password Complexity（パスワード複雑性設定）パラメータ（「Device（デバイス）> Setup（セットアップ）> Management（管理）」を参照）を設定します。ただし、Panorama がローカルで認証する管理者アカウントのみが対象となります。
公開キーの認証 (SSH) の使用	SSH 公開キーの認証を使用する場合に選択します。**Import Key**（キーのインポート）をクリックし、**Browse**（参照）して公開キー ファイルを選択し、**OK** をクリックします。Administrator [管理者] ダイアログの読み取り専用テキスト エリアに、アップロードした鍵が表示されます。 サポート対象の鍵ファイルのフォーマットは、IETF SECSH と OpenSSH です。サポート対象の鍵アルゴリズムは、DSA（1,024 ビット）と RSA（768 ~ 4,096 ビット）です。 公開キーの認証が失敗すると、ログインとパスワード プロンプトが表示されます。
管理者タイプ	タイプの選択によって、管理ロールのオプションが決まります。 • **Dynamic**（動的）– Panorama および管理対象ファイアウォールへのアクセス権を付与するロール。新しい機能が追加されると、Panorama によってダイナミック ロールの定義が自動的に更新されます。ユーザーが手動で更新する必要はありません。 • **Custom Panorama Admin**（カスタム **Panorama** 管理）– 設定可能なロールであり、Panorama 機能に対する読み書きアクセス権または読み取り専用アクセス権を設定できます。また、Panorama 機能に対するアクセス権を一切与えない（アクセス権なし）ように設定することもできます。 • **Device Group and Template Admin**（デバイス グループおよびテンプレート管理）– 設定可能なロールであり、この管理者に対して選択したアクセス ドメインに割り当てたデバイス グループとテンプレートの各機能に対する読み書きアクセス権または読み取り専用アクセス権を設定できます。また、これらの各機能に対するアクセス権を一切与えない（アクセス権なし）ように設定することもできます。

管理者ロール
 	
(ダイナミック管理者タイプ)
	事前に定義されたロールを選択します:
	
	• **Superuser** [スーパーユーザー] – Panoramaとすべてのデバイス グループ、テンプレート、管理対象ファイアウォールに対する読み取り/書き込みのフル アクセス権が付与されます。
	• **Superuser (Read Only)** [スーパーユーザー（読み取り専用）] – Panorama とすべてのデバイス グループ、テンプレート、管理対象ファイアウォールに読み取り専用でアクセスできます。
	• **Panorama administrator** [Panorama 管理者] – Panorama に対するフルアクセス権が付与されます。ただし、以下のアクションを除きます。
	  • Panorama またはファイアウォールの管理者およびロールの作成、変更、削除。
	  • **Device** (デバイス) > **Setup** (セットアップ) > **Operations** (操作)から設定のエクスポート、検証、取り消し、保存、ロード、インポートを行います。

© 2019 Palo Alto Networks, Inc.

管理者アカウント設定	の意味
	• **Panorama**タブから**Scheduled Config Export** [スケジュール設定された設定のエクスポート] 機能を設定する。
プロファイル (カスタムPanorama管理用管理者タイプ)	カスタム Panorama ロールを選択します（「Panorama > Managed Devices（管理対象デバイス）> Summary（サマリー）」を参照）。
管理者ロールに対するアクセス ドメイン (デバイス グループおよびテンプレート管理用管理者タイプ)	アクセス ドメイン（最大 25 個）ごとに管理者に割り当てるには、ドロップダウン リストから **Access Domain**（アクセス ドメイン）を **Add**（追加）します（「Panorama > Access Domains（アクセス ドメイン）」を参照）。次に、隣にある Admin Role（管理者ロール）セルをクリックし、ドロップダウン リストからカスタムの Device Group and Template（デバイス グループとテンプレート）管理者ロールを選択します（「Panorama > Managed Devices（管理対象デバイス）> Summary（サマリー）」を参照）。複数のドメインへのアクセス権を持つ管理者が Panorama にログインすると、Web インターフェイスのフッターに **Access Domain**（アクセス ドメイン）ドロップダウン リストが表示されます。管理者は、割り当てられた任意の **Access Domain**[アクセス ドメイン] を選択し、Panorama に表示する、モニタリングおよび設定データをフィルタリングできます。**Access Domain**[アクセスドメイン]を選択することで、**Context**[コンテクスト]のドロップダウンリストから表示されるファイアウォールも絞り込まれます。 *Radius* サーバーを使用して管理者を認証する場合、管理者のロールとアクセス ドメインを Radius VSA にマッピングする必要があります。*VSA* 文字列の文字数には制限があるため、管理者に対してアクセス ドメインとロールのペアの最大数 *(25)* を構成する場合、各アクセス ドメインと各ロールの名前値を平均で *9* 文字以下とする必要があります。
パスワードプロファイル	**Password Profile**（パスワード プロファイル）を選択します（「Device（デバイス）> Password Profiles（パスワード プロファイル）」を参照）。

© 2019 Palo Alto Networks, Inc.

Panorama > Admin Roles [Panorama > 管理者ロール]

管理者ロールのプロファイルは管理者のアクセス権限や役割を定義する、カスタマイズ可能なロールです。たとえば、管理者に割り当てられたロールにより、生成できるレポート、あるいは管理者が表示または変更できるデバイス グループやテンプレート設定を制御します。

デバイス グループおよびテンプレートの管理者の場合、管理者アカウントに割り当てられた各アクセス ドメインに個別のロールを割り当てることができます（「Panorama > Access Domains（アクセス ドメイン）」を参照）。アクセス ドメインにロールをマッピングすると、管理者が Panorama でアクセスできる情報を非常に詳細に制御できます。たとえば、データ センター内のファイアウォールのすべてのデバイス グループが含まれるアクセス ドメインを設定し、データ センター トラフィックの監視は許可されているが、ファイアウォールの設定は許可されていない管理者にそのアクセス ドメインを割り当てるとします。この場合、すべてのモニタリング権限を有効にするが、デバイス グループ設定へのアクセスは無効にするロールにアクセス ドメインをマッピングします。

管理者ロール プロファイルを作成するには、プロファイルを **Add**（追加）し、以下の表の説明に従って設定を指定します。

Radius サーバーを使用して管理者を認証する場合、管理者のロールとアクセス ドメインを Radius ベンダー固有の属性 (VSA) にマッピングしてください。

Panorama 管理者ロール設定	の意味
氏名	管理者ロールの識別に使用する名前を入力します（最大 31 文字）。この名前は、大文字と小文字が区別され、一意でなければならず、文字、数字、スペース、ハイフン、アンダースコアのみで構成されます。
の意味	（任意）ロールの説明を入力します。
ロール	scope of administrative responsibility（管理責任の範囲）を選択します。**Panorama**またはDevice Group and Template(デバイス グループとテンプレート)
Web UI	Panoramaコンテクスト（**Web UI list (Web UI**リスト**)**）内の特定の機能とファイアウォールコンテクスト（**Context Switch UI list (**コンテクストの切り替え**UI**リスト**)**）で許可されるアクセスのタイプを以下のオプションから指定します。 • **Enable**（許可）（ ）– 読み取りおよび書き込みアクセス • **Read Only**[読み取り専用]（)–読み取りアクセスのみ • **Disable**（無効）（ ）– アクセス不可
XML/REST API (Panoramaロールのみ)	Panoramaと管理対象のファイアウォールについてXML/REST APIアクセスの種類（**Enable (**許可**)**、**Read Only (**読み取り専用**)**、または**Disable (**無効**)**）を選択します。 • **Report (**レポート**)** – ファイアウォールレポートにアクセスできます。 • **Log (**ログ**)** – ファイアウォールログにアクセスできます。 • **Configuration (**設定**)** – Panorama およびファイアウォール設定の取得または変更が許可されます。

© 2019 Palo Alto Networks, Inc.

Panorama 管理者ロール設定	の意味
	• **Operational Requests**（操作要求）— Panorama およびファイアウォール上の操作コマンドの実行が許可されます。 • **Commit**（コミット）— Panorama およびファイアウォール設定のコミットが許可されます。 • **User-ID Agent**（**User-ID** エージェント）— User-ID エージェントにアクセスできます。 • **Export**（エクスポート）— Panorama およびファイアウォールからのファイルのエクスポート（設定、ブロック ページや応答ページ、証明書、キーなど）が許可されます。 • **Import (**インポート**)** — Panorama およびファイアウォールへのファイルのインポート（ソフトウェア更新、コンテンツ更新、ライセンス、設定、証明書、ブロックページ、カスタムログなど）が許可されます。

コマンド行
(Panoramaロールのみ)
	CLI アクセスのロールのタイプを選択します。
	• **None**（なし）— Panorama CLI へのアクセスが無効です（デフォルト）。
	• **superuser**（スーパーユーザー）— **Panorama** へのすべてのアクセスが許可されます。
	• **superreader**（スーパーリーダー）— **Panorama** に対する読み取り専用のアクセス権が与えられます。
	• **panorama-admin**（**Panorama** 管理者）— **Panorama** に対するフル アクセス権が付与されます。ただし、以下のアクションを除きます。
	  • Panoramaの管理者およびロールの作成、変更、削除。
	  • 設定のエクスポート、検証、保存、ロード、インポートを行う。
	  • 設定のエクスポートのスケジュールを設定する。

© 2019 Palo Alto Networks, Inc.

Panorama > Access Domains [Panorama > アクセス ドメイン]

アクセス ドメインでは、特定のデバイス グループ（ポリシーおよびオブジェクトの管理）、テンプレート（ネットワークおよびデバイス設定の管理）、管理対象ファイアウォールの Web インターフェイス（コンテクストの切り替え）に対して、デバイス グループとテンプレートの管理者が与えられているアクセス権限を管理します。最大で 4,000 個のアクセス ドメインを定義してローカルで管理できます。また、RADIUS ベンダー固有属性（VSA）、TACACS+ VSA、または SAML 属性を使用してそれらを管理することもできます。アクセス ドメインを作成するには、ドメインを **Add**（追加）し、以下の表の説明に従って設定を指定します。

アクセス ドメイン設定	の意味
氏名	アクセス ドメインの名前（最大 31 文字）を入力します。この名前は、大文字と小文字が区別され、一意でなければならず、文字、数字、ハイフン、アンダースコアのみで構成されます。
共有オブジェクト	共有場所からこのアクセス ドメイン内のデバイス グループに継承されるオブジェクトに対するアクセス権限を次のうちから 1 つ選択します。権限に関係なく、管理者は共有オブジェクトまたはデフォルト (事前定義済み) オブジェクトをオーバーライドできません。 • **read**[読み取り] — 管理者は共有オブジェクトの表示とコピーができますが、共有オブジェクトに対してその他の操作を実行することはできません。非共有オブジェクトの追加または共有オブジェクトのコピーを行う場合、宛先を、共有ではなく、アクセス ドメイン内のデバイス グループにする必要があります。 • **write**[書き込み] — 管理者は共有オブジェクトに対してすべての操作を実行できます。これがデフォルトの値です。 • **shared-only**[共有のみ] — 管理者はオブジェクトを共有にのみ追加できます。管理者は、共有オブジェクトの表示、編集、および削除もできますが、共有オブジェクトの移動とコピーはできません。これを選択すると、管理者は、非共有オブジェクトに対して表示以外のどの操作も実行できなくなります。
デバイスグループ	特定のデバイスグループに対する読み取り/書き込みアクセスを有効化あるいは無効化します。**Enable All**[すべて有効化]または**Disable All**[すべて無効化]をクリックすることもできます。あるデバイス グループに対して読み書きアクセス権を有効にすると、その子孫のデバイス グループに対して同じアクセス権が自動的に有効になります。子孫のデバイス グループを手動で無効にすると、その最上位の先祖のデバイス グループに対するアクセス権が読み取り専用に自動的に変更されます。デフォルトでは、すべてのデバイス グループに対してアクセス権は無効になっています。 リストに特定のデバイス グループのみを表示する場合、デバイス グループ名を選択し、**Filter Selected**（選択項目でフィルタ）を行います。 共有オブジェクトに対するアクセス権を *shared-only*（共有のみ）に設定した場合、読み書きアクセス権を指定し

© 2019 Palo Alto Networks, Inc.

アクセス ドメイン設定	の意味
	たすべてのデバイス グループに読み取り専用アクセス権が割り当てられます。
テンプレート	割り当てるテンプレートまたはテンプレート スタックごとに、**Add**[追加] をクリックし、ドロップダウンリストからテンプレートまたはテンプレート スタックを選択します。
デバイス コンテクスト （アクセス ドメイン ページのデバイス/仮想システムの列に対応しています）	ローカル設定を行う管理者がコンテクストを切り替えることのできるファイアウォールを選択します。リストに多くのファイアウォールが表示される場合、**Device State**[デバイス状態]、**Platforms**[プラットフォーム]、**Device Groups**[デバイス グループ]、**Templates**[テンプレート]、**Tags**[タグ]、および **HA Status**[HA 状態] でリストをフィルタリングできます。
ログ コレクタ グループ	割り当てるコレクタ グループごとに、ドロップダウンリストからテンプレートまたはテンプレート スタックを選択して**Add** (追加)します。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Devices（管理対象デバイス）

Panorama が管理する Palo Alto Networks ファイアウォールを管理対象のデバイスといいます。Panorama は同じメジャー リリースまたは以前のメジャー リリースを実行しているファイアウォールを管理できますが、より新しいメジャー リリースを実行しているファイアウォールを管理できません。例えば、PAN-OS 9.1 を実行している Panorama は、PAN-OS 9.1 以前のバージョンを実行しているファイアウォールを管理できます。また、Panorama より新しいメンテナンス リリースを実行しているファイアウォールを管理することはお勧めしません。機能が期待どおりに機能しない可能性があります。例えば、Panorama が PAN-OS 9.1.0 を実行している場合、PAN-OS 9.1.1 以降のメンテナンス リリースを実行しているファイアウォールを管理することはお勧めしません。リリース情報の詳細は、PAN-OS 9.1 Release Notes (リリースノート)を参照してください。サポートされている PAN-OS バージョンの詳細は End-of-Life Summary (サポート終了の概要) を参照してください。

- 管理対象ファイアウォールの管理
- 管理対象ファイアウォールの情報
- ファイアウォールのソフトウェアとコンテンツの更新
- ファイアウォールのバックアップ

管理対象ファイアウォールの管理

ファイアウォールでは、以下の管理タスクを実行できます。

タスク	の意味
コンテキストの	ファイアウォールを **Add**（追加）してシリアル番号を 1 行につき 1 つ入力し、管理対象デバイスとして追加します。**Managed Devices**（管理対象デバイス）ウィンドウには、接続の状態、インストールされている更新、初期設定中に設定されたプロパティなど、管理対象ファイアウォールの情報が表示されます。 **Associate Devices** (デバイスの関連付け)ボックスにチェックを入れ、ファイアウォールをデバイスグループあるいはテンプレート スタックと関連付けます。 Panorama 管理サーバーが管理する、複数のファイアウォールを CSV 形式で**Import** (インポート)します。サンプルの CSV ファイルをダウンロードできます。 次に、各ファイアウォールの Panorama 管理サーバーの IP アドレスを入力し（「Device（デバイス）> Setup（セットアップ）> Management（管理）」を参照）、Panorama でファイアウォールを管理できるようにします。 ファイアウォールは*AES-256*により暗号化された*SSL*接続を通じて*Panorama*に登録されます。*Panorama*とファイアウォールはを*2,048*ビット証明書を使用して互いに認証をおこない、*SSL*接続を使用して設定の管理と口グ回収を行います。
再関連付け	選択した一つ以上のファイアウォールを別のデバイスグループあるいはテンプレート スタックに割り当て直します。
削除します。	Panoramaが管理するファイアウォールのリストからファイアウォールを削除する場合は、1つ以上のファイアウォールを選択し、**Delete** (削除)します。

© 2019 Palo Alto Networks, Inc.

タスク	の意味
タグ	1つ以上のファイアウォールを選択し、**Tag**[タグ] をクリックして、最大31文字のテキスト文字列を入力するか、既存のタグを選択します。空白は使用できません。Webインターフェイスに多くのファイアウォールが表示される場所 (ソフトウェアのインストール用のダイアログなど) では、タグを使用してリストをフィルタリングできます。たとえば、「branch office」というタグを追加すると、ネットワーク全体から支店のファイアウォールすべてを検索できます。
インストール	ファイアウォールのソフトウェアおよびコンテンツ更新を**Install** (インストール)します。
HA ピアのグループ化	高可用性 (HA) 設定のピアであるファイアウォールを **Managed Devices** (管理対象デバイス) ページでグループ化する場合は、**Group HA Peers** (**HA** ピアのグループ化) を選択します。この設定により操作の対象がグループ化され、各HAペアの両方のピアに操作を行うか、どちらにも操作を行わないかのいずれかに制限されます。
バックアップの管理	ファイアウォールのバックアップを**Manage** (管理)します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、管理されるファイアウォールのバンドルを **PDF/CSV** としてエクスポートできます。フィルターを適用して、監査などのためのより具体的な表構成出力を作成することができます。Web インターフェイスで表示可能な列のみがエクスポートされます。「Configuration Table Export (設定バンドルのエクスポート) 」を参照してください。
マスターキーのデプロイ	一つ以上のデバイスの新しいマスターキーをデプロイするか、既存のマスターキーを更新します。

管理対象ファイアウォールの情報

Panorama > **Managed Devices** (管理対象デバイス) > **Summary** (サマリ) を選択し、管理対象ファイアウォールごとに以下の情報を表示します。

管理対象ファイアウォールの情報	の意味
デバイス グループ	ファイアウォールがメンバーとなっているデバイス グループの名前が表示されます。デフォルトではこの列は非表示ですが、任意の列ヘッダーのドロップダウンリストを選択し、**Columns** > **Device Group**[列 > デバイス グループ] を選択することでこの列を表示できます。 ファイアウォールグループに応じて、ページにクラスタ内のデバイスが表示されます。各クラスタにヘッダー行があり、デバイスグループ名、割り当てられたファイアウォールの合計数、接続されたファイアウォールの数、階層内のデバイスグループのパスが表示されます。例えば、**Datacenter (2/4 Devices Connected)** (データセンター (接続済みデバイス2/4)) の場合:**Shared** (共有) > **Europe** (欧州) > **Data center** (データ センター) は、 **Data center** (データ センター) というデバイスグループに4つのメンバーファイアウォールが存在し (そのうち2つは接続済み) 、そのデバイスグループは **Europe** (欧州) というデバイスグループの子であることを示します。任意のデバイス グループを折りたたんだり展開したりすることで、そのファイアウォールを非表示にしたり表示したりできます。

© 2019 Palo Alto Networks, Inc.

管理対象ファイアウォールの情報	の意味
デバイス名	ファイアウォールのホスト名またはシリアル番号が表示されます。 VM-Series NSXエディションファイアウォールの場合、ファイアウォール名にはESXiホストのホスト名が付加されます。例えば、PA-VMの場合:Host-NY5105
仮想システム(vsys)	Multiple Virtual Systems [複数の仮想システム] モードになっているファイアウォール上で利用できる仮想システムが一覧表示されます。
モデル	ファイアウォールのモデルを表示します。
tags	各ファイアウォール / 仮想システムに定義されているタグが表示されます。
シリアル番号	ファイアウォールのシリアル番号が表示されます。
操作モード	ファイアウォールの運用モードを選択します。FIPS-CC または 通常になります。
IPアドレス	ファイアウォール/仮想システムのIPアドレスが表示されます。
	IPv4—ファイアウォール/仮想システムの IPv4 アドレスです。
	IPv6—ファイアウォール/仮想システムの IPv6 アドレスです。
Variables 変数	テンプレート固有の変数定義を、テンプレート スタック内のデバイスからコピーするか、既存の変数定義を編集してデバイスの一意の変数を作成して作成します。デバイスがテンプレート スタックに関連付けられていない場合、この列は空になります。デフォルトでは、変数はテンプレート スタックから継承されます。「Create or Edit Variable Definition on a Device（デバイスの変数定義の作成または編集）」を参照してください。
テンプレート	ファイアウォールが属するテンプレートスタックが表示されます。
ステータス	**Device State** [デバイス状態] — Panorama とファイアウォール間の接続の状態が示されます:接続済みまたは切断 VM-Series のファイアウォールには別の 2 つの状態が存在する可能性があります。 • **Deactivated**（停止中）— ファイアウォール上で仮想マシンを直接停止したか、**Deactivate VMs**（**VM** の停止）（**Panorama** > **Device Deployment**（デバイスのデプロイ）> **Licenses**（ライセンス））を選択して仮想マシンが停止し、ファイアウォールのすべてのライセンス/資格が削除されていることを示します。非アクティブ化プロセスによって VM-Series ファイアウォールのシリアル番号が削除されるため、非アクティブ化されたファイアウォールは Panorama から切断されます。 • **Partially deactivated**[部分的に停止] — Panoramaからライセンスの停止プロセスが開始されたが、ファイアウォールがオフラインであ

© 2019 Palo Alto Networks, Inc.

管理対象ファイアウォールの情報	の意味
	り、Panoramaがファイアウォールと通信できないためプロセスがすべて完了していないことを示します。
	HA Status[HAの状態]—ファイアウォールが、以下の状態にあることを示します。 • **Active** [アクティブ] - 正常なトラフィック処理状態 • **Passive** [パッシブ] - 正常なバックアップ状態 • **Initiating** [始動中] - ファイアウォールの起動後最大60秒はこの状態におかれます • **Non-functional** [機能停止中] - エラー状態 • **Suspended** [保留中] - 管理者がファイアウォールをサスペンドしていることを示します • **Tentative** [一時的な状態] - アクティブ/アクティブ環境におけるリンクまたはパスのモニタリングイベント用
	Shared Policy [共有ポリシー] — ファイアウォールのポリシーとオブジェクト設定が Panorama と同期しているかどうかを示します。
	Template [テンプレート] — ファイアウォールのネットワークとデバイス設定がPanoramaと同期しているかどうかを示します。
状態（続き）	**Certificate**（証明書）— 管理対象デバイスのクライアント証明書の状態を示します。 • **Pre-defined**（事前定義済み）— 管理対象デバイスでは、事前定義済み証明書を使用して Panorama で認証しています。 • **Deployed**（デプロイ済み）— カスタム証明書が管理対象デバイスで正常にデプロイされています。 • **Expires in N days N hours**（N 日と N 時間で期限切れ）— 現在インストールされている証明書は、30 日未満で期限切れとなります。 • **Expires in N minutes**（N 分で期限切れ）— 現在インストールされている証明書は、1 日未満で期限切れとなります。 • **Client Identity Check Passed**（クライアント アイデンティティ チェック合格）— 証明書の共通名は、接続中デバイスのシリアル番号と一致します。 • **OCSP Status Unknown**（**OCSP** の状態不明）— Panorama では、OCSP の状態を OCSP レスポンダから取得できません。 • **OCSP Status Unavailable**（**OCSP** の状態使用不可）— Panorama は OCSP レスポンダに接続できません。 • **CRL Status Unknown**（**CRL** の状態不明）— Panorama は CRL データベースから失効状態を取得できません。 • **CRL Status Unavailable**（**CRL** の状態使用不可）— Panorama は CRL データベースに接続できません。
	• **OCSP/CRL Status Unknown**（**OCSP/CRL** の状態不明）— 両方とも有効であるとき、Panorama は OCSP または失効の状態を取得できません。 • **OCSP/CRL Status Unavailable**（**OCSP/CRL** の状態使用不可）— 両方とも有効であるとき、Panorama は OCSP または CRL データベースに接続できません。

© 2019 Palo Alto Networks, Inc.

管理対象ファイアウォールの情報	の意味
	• **Untrusted Issuer**（信頼されていない発行者）– 管理対象デバイスにカスタム証明書がありますが、サーバーはそれを検証していません。 **Last Commit State** [最終コミット状態] – ファイアウォールで最後のコミットが失敗したか、成功したかを示します。
ソフトウェア バージョン | アプリケーションおよび脅威 | アンチウイルス | URL フィルタリング | GlobalProtect™ クライアント | WildFire	ファイアウォールに現在インストールされているソフトウェアとコンテンツのバージョンが表示されます。詳細は、「ファイアウォールのソフトウェアとコンテンツの更新」を参照してください。
バックアップ	PAN-OSはファイアウォール上のコミットを行う際、Panoramaに対し自動的にファイアウォールの設定のバックアップを送信します。設定のバックアップを参照し、必要に応じそれを読み込む場合は**Manage**[管理]をクリックします。詳細は、「ファイアウォールのバックアップ」を参照してください。
最後のマスターキーのプッシュ	Panorama からファイアウォールへのマスターキーのデプロイ ステータスを表示します。
	ステータス–最後に行ったマスターキーのプッシュのステータスを表示します。`Success`（成功）あるいは`Failed`（失敗）のいずれかになります。マスターキーが Panorama からファイアウォールにプッシュされていない場合は`Unknown`（不明）が表示されます。
	タイムスタンプ–Panorama から最後にマスターキーをプッシュした日時を表示します。

デバイス変数定義の作成

デバイスを最初にテンプレート スタックに追加すると、テンプレート スタック内のデバイスからコピーされたデバイス固有の変数定義を作成するか、**Panorama** > **Managed Devices**（管理対象デバイス）> **Summary**（サマリー）を使用してテンプレート変数定義を編集することができます。デフォルトでは、すべての変数定義はテンプレート スタックから継承され、個々のデバイスの変数定義をオーバーライドしたり、削除したりすることはできません。IP アドレス オブジェクトと IP アドレス リテラル（IPネットマスク、IP 範囲、FQDN）を、設定のすべての領域、IKE ゲートウェイ構成（インタフェース）および HA 設定（グループ ID）のインタフェースに置き換えることができます。

デバイス変数定義の作成に関する情報	の意味
テンプレート スタック内の別のデバイスからデバイスの変数定義を複製しますか？	
いいえ	既存の変数定義を表示し、必要に応じて編集します。「Panorama > Templates（テンプレート）> Template Variables（テンプレートの変数）」を参照してください
あり。	ドロップダウン リストで変数定義を複製するデバイスを選択し、複製する特定の変数定義を選択します。

© 2019 Palo Alto Networks, Inc.

ファイアウォールのソフトウェアとコンテンツの更新

管理対象のファイアウォールにソフトウェアまたはコンテンツのアップデートをインストールする場合は、まず**Panorama** > **Device Deployment**（デバイスのデプロイ）のページを開き、アップデートのダウンロードまたはそれをPanoramaへアップロードします。次に、 **Panorama** > **Managed Devices**（管理対象デバイス）ページを選択し、**Install**（インストール）をクリックして、以下のフィールドを設定します。

管理（*MGT*）インターフェイスのトラフィックを削減するには、更新のデプロイのために個別のインターフェイスを使用するように *Panorama* を設定します（「Panorama > Setup（セットアップ）> Interfaces（インターフェイス）」を参照）。

ファイアウォール用ソフトウェア/コンテンツの更新のインストール オプション	の意味
タイプ	インストールする更新のタイプを以下の中から選択します。PAN-OS **Software**[ソフトウェア]、**GlobalProtect Client** software [GlobalProtect クライアントソフトウェア]、**Apps and Threats** signiatures [アプリケーションおよび脅威] のシグネチャ、**Antivirus** signiature [アンチウイルス] シグネチャ、**WildFire**、または**URL Filtering**[URLフィルタリング]
ファイル	更新イメージを選択します。ドロップダウン リストには、**Panorama** > **Device Deployment**（デバイスのデプロイ） ページで Panorama にダウンロードまたはアップロードしたイメージのみが表示されます。
フィルタ	デバイスリストに適用するフィルタを選択します。
機器	イメージをインストールするファイアウォールを選択します。
デバイス名	ファイアウォール名
現在のバージョン	現在ファイアウォールにインストールされている**Type**[タイプ] のファイアウォールの更新バージョンです。
HA 状態	ファイアウォールが、以下の状態にあることを示します。 • **Active** [アクティブ] - 正常なトラフィック処理状態 • **Passive** [パッシブ] - 正常なバックアップ状態 • **Initiating** [始動中] - ファイアウォールの起動後最大60秒はこの状態におかれます • **Non-functional** [機能停止中] - エラー状態 • **Suspended** [保留中] - 管理者がファイアウォールをサスペンドしていることを示します • **Tentative** [一時的な状態] - アクティブ/アクティブ環境におけるリンクまたはパスのモニタリングイベント用
HA ピアのグループ化	高可用性（HA）設定のピアであるファイアウォールをグループ化する場合に選択します。
フィルタが選択されています	デバイスリストに特定のファイアウォールのみを表示する場合、対応するデバイス名を選択し、**Filter Selected**[選択項目でフィルタ]を行います。

© 2019 Palo Alto Networks, Inc.

ファイアウォール用ソフトウェア/コンテンツの更新のインストール オプション	の意味
デバイスにのみアップロード	イメージをファイアウォールにアップロードした際、ファイアウォールを自動的に再起動させない場合に選択します。イメージはファイアウォールを手動で再起動するまでインストールされません。
インストール後にデバイスを再起動（ソフトウェアのみ）	ソフトウェア イメージをアップロードし、インストールする場合に選択します。インストール プロセスによって再起動がトリガーされます。
コンテンツ更新で新しいアプリケーションを無効にする（アプリケーションと脅威のみ）	前回インストールした更新にはない、新しく含まれているアプリケーションを無効化する場合に選択します。これにより最新の脅威を防ぎながらも、ポリシーアップデートを行ったのちに、アプリケーションを有効化していくといった柔軟な対応が可能です。アプリケーションを有効化したい場合、ファイアウォールにログインして、 **Device** [デバイス] > **Dynamic Updates**[動的更新] を開き、機能の列にある**Apps** [アプリ] をクリックして新しいアプリケーションを表示し、有効化したいアプリケーションごとに**Enable/Disable** [有効化/無効化] の設定を選びます。

ファイアウォールのバックアップ

- Panorama > Managed Devices [Panorama > 管理対象デバイス]

Panoramaでは、設定の変更を管理対象ファイアウォールにコミットするたびにその変更内容が自動的にバックアップされます。ファイアウォールのバックアップを管理する場合は **Panorama** > **Managed Devices**（管理対象デバイス）を選択し、ファイアウォールの Backups（バックアップ）列にある **Manage**（管理）をクリックし、以下のいずれかのタスクを行います。

Panoramaデバイスに保存するファイアウォールの設定バックアップ数を設定する場合は、Panorama > Setupセットアップ > Management管理 の順に選択し、[ロギングおよびレポート設定] を編集します。次に、*Log Export and Reporting[ログのエクスポートとレポート]* タブを選択して、 *Number of Versions for Config Backups[設定バックアップのバージョン数]* フィールドに値*(デフォルトは100)*を入力します。

タスク	の意味
保存またはコミットされた設定の詳細を表示する。	バックアップのVersion[バージョン]列で、保存またはされた設定のファイル名またはコミットされた設定のバージョンナンバーをクリックし、関連するXMLファイルの内容を表示します。
保存またはコミットされた設定を設定候補に復元する。	バックアップのAction[動作]列で、**Load**[ロード]と**Commit**[コミット]をクリックします。
保存された設定内容を削除する。	バックアップのAction[動作]列で、Delete[削除]（ ）をクリックします。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Devices（管理対象デバイス） > Health（健康状態）

Panorama™では、管理対象ファイアウォールのハードウェア リソースとパフォーマンスを監視できます。Panorama は、時間推移のパフォーマンス情報（CPU、メモリ、CPS、スループット）、ロギング パフォーマンス、環境情報（ファン、RAID ステータス、電源など）およびコミット、コンテンツのインストール、ソフトウェア アップグレードなどのイベントを一元管理します。ファイアウォールが計算されたベースラインから逸脱すると、Panorama はそれを逸脱デバイスとして報告し、ハードウェアの問題を迅速に特定、診断、解決します。

このページでは次の操作も可能です。

詳細なデバイスヘルスチェックの閲覧。	Panoramaで管理されているデバイスのチェックステータス基準を閲覧する。
HA ピアのグループ化	潜在的な問題を特定し、ハードウェア リソースやパフォーマンスの問題の影響を受けるファイアウォールがあるかどうかを判断するために、どのファイアウォールがグループ化されているかを確認します。
PDF/CSV	最低限の読み取り専用アクセス権を持つ管理ロールは、管理されるファイアウォールのバンドルを **PDF/CSV** 形式でエクスポートできます。フィルターを適用して、監査などで必要なより具体的な表構成出力を作成することができます。Web インターフェイスで表示される列のみエクスポートされます。Export Configuration Table Data（設定バンドルデータのエクスポート）を参照してください。

Panorama > Managed Devices（管理対象デバイス） > *Health*（健康状態）> *All Devices*（全てのデバイス）

このページを使用して、各ファイアウォールについて次の情報を表示します。

ヘルスチェック情報	の意味
デバイス名	ファイアウォールのホスト名またはシリアル番号。 VM-Series NSXエディションファイアウォールの場合、ファイアウォール名にはESXiホストのホスト名が付加されます。例えば、PA-VMの場合:Host-NY5105
モデル	ファイアウォールのモデル。
デバイス	
Throughput (Kbps) スループット (Kb/秒)	キロバイト/秒単位で測定されたデータ スループット（平均5分間）。

© 2019 Palo Alto Networks, Inc.

ヘルスチェック情報	の意味
毎秒コネクション数 (CPS)	ファイアウォールの 1 秒あたりの総接続数 (平均 5 分) 。
セッション	
カウント (セッション)	時間の経過に伴う合計セッション数 (平均 5 分) 。
データ プレーン	
CPU (%)	データ プレーンの総 CPU 使用率。
管理プレーン(MP)	
CPU (%)	管理プレーンの総 CPU 使用率。
MEM (%)	管理プレーンの総メモリ使用率。
ロギング率 (1 秒あたりのログ数)	ファイアウォールがログを Panorama またはログ コレクタに転送する割合 (平均1分) 。
ファン情報	各ファン トレイのファンの有無、現在の状態、RPM、および最後に障害が発生した日付を表示します。ファンの状態は、*A*/*B* で表示されます。*A* は良好な稼働中のファンの数、*B* はファイアウォール上のファンの総数です。仮想ファイアウォールは `N/A` で表示されます。
電源	パワーサプライの有無、現在の状態、最後に障害が発生した日付のタイムスタンプを表示します。パワーサプライの状態は、*A*/*B* で表示されます。*A* は良好な稼働中のパワーサプライの数、*B* はデバイスに付いているパワーサプライの総数です。仮想ファイアウォールは `N/A` で表示されます。
ポート	ファイアウォールで使用されている合計ポート数が表示されます。ポートは、*A*/*B* で表示されます。*A* は良好な稼働中のポートの数、*B* はデバイス上のポートの総数です。

Panorama > *Managed Devices* (管理対象デバイス) > *Health* (健康状態) > *Deviating Devices* (逸脱デバイス)

逸脱デバイス タブには、計算されたベースラインから逸脱しているメトリックを持つデバイスが表示され、その偏差メトリックが赤色で表示されます。ヘルスチェックベースライン測定指標により、7 日間にわたる所定のメトリックヘルスチェックパフォーマンスを平均化し、標準偏差を加算することによって決定されます。

© 2019 Palo Alto Networks, Inc.

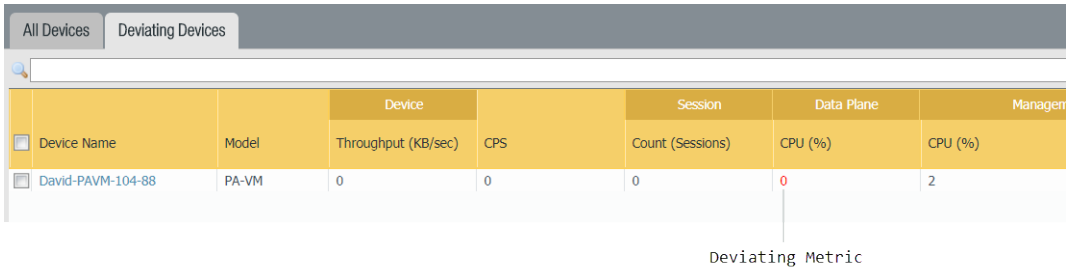


図 1 : 逸脱測定の例

Detailed Device Health on Panorama（Panorama のデバイス健康状態詳細）

All Devices（すべてのデバイス）タブまたは Deviating Devices（逸脱デバイス）タブの Device Name（デバイス名）をクリックすると、個々のファイアウォールの詳細なデバイス健康状態履歴を表示できます。Detailed Device（デバイス詳細）ビューは、時間フィルタを使用して健康状態履歴を提供し、デバイスに関連付けられたメタデータを表示します。デバイスの健康状態情報は、時間軸のデータをグラフで表示できるように、表またはウィジェットとして表示されます。

Manage the Detailed Device View（デバイス詳細ビューの管理）

Detailed Device（デバイス詳細）ビューには、ファイアウォールに関連付けられている説明メタデータとともに詳細なファイアウォールの健康状態情報が表示されます。該当する場合は、ウィジェットの追加オプションについては設定 (⚙) を、ウィジェットを拡大するには最大化パネル (⊡) を設定します。

項目	の意味
操作	
Time Filter（時間フィルタ）	ドロップダウンからデバイス健康状態を表示するには、時間フィルタを選択します。時間フィルタは、**Last 12 hours**（**12** 時間前）、**24 hours**（**24** 時間）、**7 days**（**7** 日）, **15 days**（**15**日）、**30 days**（**30** 日）、または**90 days**（**90**日）から選択できます。
Show Average 平均を表示	すべての時間推移ウィジェットに表示される平均および標準分布を選択します。**None**（なし）、**Last 24 hours**（**24** 時間前）、**7 days**（**7** 日）、または **15 days**（**15** 日）から選択できます。
レートの	表示される情報を最新データに更新します。
Print PDF（PDF で生成）	現在表示中のタブの PDF を生成します。 ダウンロード場所を選択して *PDF* にアクセスするには、ポップアップを有効にする必要があります。
System Information（システム情報）	
System Information（システム情報）	デバイスに関連する以下のメタデータです。IP アドレス、ソフトウェアのバージョン、ウィルス対策ソフトのバージョン、HA 状態、シリアル

© 2019 Palo Alto Networks, Inc.

項目	の意味
	番号、アプリと脅威のバージョン、Wildfire のバージョン、VSYS モード、モデル、およびデバイス モード。

セッション数

Sessions（セッション）タブにはファイアウォールを通過するセッション情報が表示されます。この情報は 6 つのグラフで個別に表示されます。

項目	の意味
スループット	キロビット/秒 (Kbps) 単位で測定されたデータ スループット (平均5分間)。
セッション数	時間の経過に伴う合計セッション数（平均 5 分）。
Connections per Second（接続数/秒）	時間に対するデバイスの合計CPS（平均 5 分）
Packets per Second（毎秒パケット数）	デバイスを通過した 1 秒あたりの合計パケット数（平均 5 分）
Global Session Table Utilization（グローバル セッション テーブル使用率）（PA-7000、PA-5200 アプライアンスのみ）	グローバル セッション テーブルを持つファイアウォール（平均 5 分）に対するグローバル セッション テーブルの時間に対するパーセンテージ。
Session Table Utilization（セッション テーブル使用率）	ファイアウォールの各データプレーンに対するセッション テーブル使用率の時間に対する割合（平均 5 分）を示します。
SSL Decrypted Sessions Info（SSL 復号化処理 セッション数）	時間の経過とともに暗号化された SSL セッションの数を示します（平均5分）。
SSL Proxy Session Utilization（SSL 復号化処理 セッション使用率）	時間経過に伴うプロキシ セッションの利用率を示します（平均 5 分）。

Environments（環境）

Environments（環境）タブには、パワーサプライ、ファン トレイ、ディスクドライブなどのハードウェアの有無、状態、および動作状態が表示されます。このタブには以下のハードウェア ベースのファイアウォールのみ表示されます。

項目	の意味
Fan Status（ファンの状態）	各ファン トレイのファンの有無、現在の状態、RPM、および最後に障害が発生した日付を表示します。ファンの状態は、*A/B* で表示されま

© 2019 Palo Alto Networks, Inc.

項目	の意味
	す。*A* は良好な稼働中のファンの数、*B* はファイアウォール上のファンの総数です。仮想ファイアウォールは N/A で表示されます。
Power Supply（パワー サプライ）	パワーサプライの有無、現在の状態、最後に障害が発生した日付のタイムスタンプを表示します。パワーサプライの状態は、*A*/*B* で表示されます。*A* は良好な稼働中のパワーサプライの数、*B* はデバイスに付いているパワーサプライの総数です。仮想ファイアウォールは N/A で表示されます。
Thermal Status（熱状態）	デバイスの各スロットに関連するすべての熱アラームを表示します。アクティブなアラームがある場合、ファイアウォールは正確な温度と場所に関するより詳しい情報もここに表示されます。
System Disk Status（システム ディスク ステータス）	root、pancfg、panlogs、および panrepo マウントの使用可能、使用中、および使用率を表示します。 システム ディスク ステータスには、RAID が有効になっているファイアウォールのディスク名、サイズ、および RAID ステータスも表示されます。

インターフェイス

（インターフェイス）タブには、ファイアウォール上のすべての物理インターフェイスのステータスと統計情報が表示されます。

項目	の意味
インターフェイス名	インターフェイスの名称。インターフェイスを選択すると、選択したインターフェイスのBit Rate（ビットレート）、Packets per Second（1 秒あたりのパケット数）、Errors（エラー）、およびDrops（ドロップ）のグラフが表示されます。
ステータス	インターフェイスのステータス。Admin Up, Admin Down, Operational Up、または Operational Down。
Bit Rate ビットレート	送受信されたデータのビットレート（bps）を表示します。
Packets per Second（毎秒パケット数）	送受信されたデータの 1 秒あたりのパケット数を表示します。
エラー	送受信されたデータのエラー数を表示します。
Drops（破棄）	送受信されたデータでドロップした接続数を表示します。

ﾛｷﾞﾝｸﾞ

（ロギング）タブには、ファイアウォールを管理するロギング レートと接続が表示されます。

© 2019 Palo Alto Networks, Inc.

項目	の意味
ロギング率	Panorama またはLog Collector（ログ コレクタ）へのデバイス転送ログの 1 分間の平均レートを表示します。
Logging Connections（ロギング接続）	使用可能なすべてのログ転送接続（アクティブまたは非アクティブのステータスを含む）を表示します。
External Log Forwarding（外部ログ転送）	さまざまな種類の外部ログ転送方式の送信、ドロップ、平均転送速度（1 秒あたりのログ数）を表示します。

リソース

（リソース）タブには、ファイアウォールの CPU とメモリの統計情報が表示されます。

項目	の意味
Management Plane Memory（管理プレーンのメモリ）	管理プレーン メモリの時間推移 5 分間平均をパーセントで表示します。
Packet Buffers（パケット バッファ）	パケット バッファ 使用率の時間推移 5 分間平均をパーセントで表示します。複数のデータ プレーン システムでは、このディスプレイには異なる色の異なるデータプレーン、CPU、およびパケット バッファが含まれています。
Packet Descriptors（パケット記述子）	パケット記述子の使用率の時間推移 5 分間平均をパーセントで表示します。複数のデータ プレーン システムでは、このディスプレイには異なる色の異なるデータプレーン、CPU、およびパケット バッファが含まれています。
CPU Management Plane（CPU 管理プレーン）	管理プレーン CPU の時間推移 5 分間平均を表示します。
CPU Data Plane（CPU データ プレーン）	データプレーン CPU の時間あたりの平均 5 分間の平均コア使用率を表示します。複数のデータプレーンを持つシステムでは、表示するデータプレーンを選択できます。
Mounts（ディスク領域使用状況）	デバイス システム ファイル情報を表示します。ディスク領域使用状況のName（名前）、Allocated（割り当て済み）（KB）、Used（使用済み）（KB）、およびAvail（使用可能）（KB）の各領域、およびUtilization（使用）率が表示されます。

HA

（高可用性）タブには、ファイアウォールの HA ステータスとその HA ピアが表示されます。一番上のウィジェットには、デバイスとそのピアの設定とコンテンツのバージョンが表示されます。下のウィジェットには、前の HA フェールオーバーに関する情報と、それに関連する理由（障害が発生したファイアウォールを含む）が表示されます。

© 2019 Palo Alto Networks, Inc.

Panorama > Templates [Panorama > テンプレート]

Device（デバイス）および **Network**（ネットワーク）タブでは、テンプレートまたはテンプレート スタック（テンプレートの組み合わせ）を使用して、類似の設定を必要とする複数のファイアウォールに共通の基本設定を適用できます。Panorama でファイアウォール設定を管理する場合、デバイス グループ とテンプレートの組み合わせを使用します。デバイス グループでは、共有するポリシーおよびオブジェクトを管理し、テンプレートでは、共有するデバイスおよびネットワーク設定を管理します。

テンプレートまたはテンプレート スタック作成用ダイアログで使用できる設定に加えて、**Panorama** > **Templates**（テンプレート）では以下の列が表示されます。

- **Type**[タイプ] - 記載されたエントリが、テンプレートあるいはテンプレートスタックのどちらであるかを示します。
- **Stack**[スタック] - テンプレートスタックに割り当てられたテンプレートを一覧表示します。

操作	以下を参照
テンプレートを追加、コピー、編集、または削除する	テンプレート
テンプレート スタックを追加、コピー、編集、または削除する	テンプレート スタック
その他の情報をお探しですか？	テンプレートおよびテンプレート スタック
	テンプレートおよびテンプレート スタックの管理

テンプレート

Panorama では、最大 1,024 個のテンプレートがサポートされます。以下の表に記載されているように、テンプレートを **Add**（追加）して設定てきます。テンプレートを作成した後、ファイアウォールを管理する前に Configure a Template Stack（テンプレート スタックを設定）し、テンプレートとファイアウォールをテンプレート スタックに追加する必要があります。テンプレートの設定後、Panorama で変更をコミットする必要があります（「Panorama Commit Operations（Panorama のコミット操作）」を参照）。

テンプレートを削除しても、*Panorama* によってファイアウォールにプッシュされた値は削除されません。

テンプレートの設定	の意味
氏名	テンプレート名 (最大 31 文字) を入力します。この名前では、大文字と小文字が区別されます。また、一意のものにしてください。文字、数字、スペース、ハイフン、ピリオド、アンダースコアのみ使用できます。 この名前は、**Device**（デバイス）タブと **Network**（ネットワーク）タブの **Template**（テンプレート）ドロップダウン リストに表示されます。これらのタブで変更した設定は、選択した**Template**[テンプレート]にのみ適用されます。

© 2019 Palo Alto Networks, Inc.

テンプレートの設定	の意味
の意味	テンプレートの説明を入力します。

テンプレート スタック

テンプレート スタックを構成したり、テンプレートをテンプレート スタックに割り当てることができます。ファイアウォールをテンプレート スタックに割り当てると、すべての設定を各テンプレートに個別に追加するのではなく、ファイアウォールに必要な設定をすべてプッシュすることができます。Panorama では、最大 1,024 個のスタックがサポートされます。**Add Stack**（スタックを追加）を利用して新しいテンプレート スタックを作成し、次の表の説明に従って設定を構成できます。テンプレート スタックの設定後、Panorama で変更をコミットする必要があります（「Panorama Commit Operations（Panorama のコミット操作）」を参照）。また、スタックに割り当てられたファイアウォールのネットワークとデバイスの設定を行った場合は、テンプレートコミットを行い、設定をファイアウォールへプッシュする必要があります。

テンプレート スタックを削除したり、テンプレート スタックからファイアウォールを除外したりしても、*Panorama* が以前そのファイアウォールにプッシュした値は削除されません。ただし、テンプレート スタックからファイアウォールを除外すると、*Panorama* は新しい更新をそのファイアウォールにプッシュしなくなります。

テンプレート スタックの設定	の意味
氏名	スタック名 (最大 31 文字) を入力します。この名前は、大文字と小文字が区別され、一意でなければならず、文字から始まり、文字、数字、ハイフン、アンダースコアのみで構成されます。スタック名および割り当てられたテンプレートは、**Device**（デバイス）タブと **Network**（ネットワーク）タブの **Template**（テンプレート）ドロップダウンリストに表示されます。
の意味	スタックの説明を入力します。
テンプレート	スタックに組み込む各テンプレートを **Add**（追加）します（8 個まで）。 テンプレートに設定が重複している場合、割り当てられたファイアウォールに設定をプッシュするときに、リストの上位にあるテンプレートの設定だけが Panorama によってプッシュされます。たとえば、テンプレート_A がリスト内でテンプレート_B よりも上にあり、この 2 つのテンプレートで Ethernet1/1 インターフェイスが定義されているとします。この場合、Panorama は Ethernet1/1 の定義をテンプレート_A からプッシュし、テンプレート_B からはプッシュしません。リスト内のテンプレートの順番を変更するには、テンプレートを選択して **Move Up**（上へ）または **Move Down**（下へ）移動します。 *Panorama* では、スタック内のテンプレートの組み合わせが検証されないため、無効な関係が生じないように plan the order（順番付け）を行ってください。
機器	スタックに追加したいファイアウォールをそれぞれ選択します。 リストに多くのファイアウォールが表示される場合、**Platforms**（プラットフォーム）、**Device Groups**（デバイス グループ）、**Tags**（タグ）、および **HA Status**（HA 状態）でリストをフィルタリングできます。

© 2019 Palo Alto Networks, Inc.

テンプレート スタックの設定	の意味
	モード (*VPN* モード、マルチ *vsys* モード、または操作モード) が一致していない複数のファイアウォールを同じスタックに割り当てることができます。*Panorama* は、モード固有の設定を、そのモードをサポートするファイアウォールにのみプッシュします。
すべて選択	リスト中の全てのファイアウォールを選択します。
すべての選択を解除	リスト中の全てのファイアウォールの選択を解除します。
HA ピアのグループ化	高可用性 (HA) ピアであるファイアウォールをグループ化します。HA に設定されたファイアウォールを簡単に識別できるようになります。テンプレートスタックから設定をプッシュする場合は、個々のファイアウォールではなくグループ化されたペアにプッシュできます。
フィルタが選択されています	特定のファイアウォールのみを表示するには、該当のファイアウォールを選択して、**Filter Selected**[選択項目でフィルタ]を実行します。

Panorama > Templates (テンプレート) > Template Variables (テンプレートの変数)

- テンプレート変数の新規作成
- 既存のテンプレート変数の編集
- デバイスの変数定義の作成または編集

テンプレートやテンプレート スタックの変数 (**Panorama** > **Templates** (テンプレート)) を定義することも、個々のデバイス (**Panorama** > **Managed Devices** (管理対象デバイス) > **Summary** (サマリー)) の既存の変数を編集することもできます。変数は、パノラマを使用してファイアウォール設定を管理するときに、柔軟性と再利便性を提供するテンプレートまたはテンプレート スタックで定義された設定コンポーネントです。変数を使って以下の項目を置き換えることができます。

- 設定のすべての領域における IP アドレス (IP ネットマスク、IP 範囲、および FQDN を含む) 。
- IKE ゲートウェイ設定 (インターフェイス) および HA 設定 (グループ ID) のインターフェイス。

ファイアウォールをテンプレート スタックに追加すると、テンプレートまたはテンプレート スタック用に作成した変数が自動的に継承されます。

テンプレート変数情報	の意味
氏名	変数定義の名称。
テンプレート (デバイスとテンプレート スタック)	変数定義が属するテンプレートの名前を表示します。
タイプ	変数定義のタイプを表示します。 • **IP Netmask** (**IP** ネットマスク) –静的 IP またはネットワーク アドレスを定義します。 • **IP Range** (**IP** 範囲) –IP 範囲を定義します。たとえば、「192.168.1.10-192.168.1.20」と入力します。

© 2019 Palo Alto Networks, Inc.

テンプレート変数情報	の意味
	• **FQDN**–完全修飾ドメイン名を定義します。 • **Group ID**（グループ **ID**）–高可用性グループ ID を定義します。詳細は、「Configuration Guidelines for Active/Passive HA（アクティブ/パッシブ HA の設定ガイドライン）」を参照してください。 • **Interface**（インターフェイス）–ファイアウォール上のファイアウォール インターフェイスを定義します。IKE ゲートウェイ設定にのみ使用可能です。
値	変数定義用に設定された値を表示します。
追加（テンプレートとテンプレート スタック）	新しいテンプレート変数定義を Add (追加) します。
削除します。	既存のテンプレート変数定義を削除します。
コピー	既存のテンプレート変数定義を複製します。
オーバーライド（テンプレートスタックとデバイス）	テンプレートスタックまたはデバイスから継承した既存のテンプレート変数定義をオーバーライドします。変数のタイプまたは名前を変更することはできません。また、デバイス固有の変数をオーバーライドすることはできません。
元に戻す（テンプレート スタックとデバイス）	テンプレートスタックまたはデバイスレベルでオーバーライドされた値をクリアするには 上書きされた変数を元のテンプレート変数定義に戻します。
デバイスのみで使用される値を取得する（デバイスのみ）	選択した変数に、ファイアウォールで使用されている値を入力します。Panorama が値を取得する前に、テンプレートまたはテンプレートのスタック変数を定義してファイアウォールにプッシュする必要があります。ファイアウォールから取得された値は、テンプレートまたはテンプレートスタック変数を **Override**（オーバーライド）上書きして、デバイス固有の変数を作成します。変数定義がファイアウォールにプッシュされていない場合、Panorama はその変数に `Value not found`（値が見つかりません）を返します。

テンプレート変数の新規作成

新しいテンプレート変数定義を**Add**（追加）します。

テンプレート変数定義の新規作成に関する情報	の意味
氏名	変数定義の名称。すべての変数定義名は、ドル記号（「$」）で始まる必要があります。
タイプ	変数定義のタイプを選択します。**IP Netmask**（**IP** ネットマスク）、**IP Range**（**IP** 範囲）、**FQDN**、**Group ID**（グループ **ID**）、または**Interface**（インターフェイス）。
値	変数定義目的の値を入力します。

© 2019 Palo Alto Networks, Inc.

既存のテンプレート変数の編集

テンプレートまたはテンプレートスタックのテンプレート変数定義は、変数を作成した後の任意の時点（**Panorama** > **Templates**（テンプレート））で編集できます。テンプレート変数を**Manage**（管理）して変数を選択し、必要に応じて使用可能な値を編集します。

デバイスの変数定義の作成または編集

Panorama > **Managed Devices**（管理対象デバイス） > **Summary**（サマリー） に移動して、変数定義を作成するか、Panorama テンプレートまたはテンプレート スタックからプッシュされたテンプレート変数を上書きします。テンプレート変数には以下が含まれます。

- 設定のすべての領域における IP アドレス（IP ネットマスク、IP 範囲、または FQDN）。
- IKE ゲートウェイ設定（インターフェイス）または HA 設定（グループ ID）のインターフェイス。

デバイス変数を作成すると、オーバーライドされたデバイス固有の変数を、個別に再作成するのではなく、同じテンプレート スタック内のデバイスからコピーすることができます。デフォルトでは、すべての変数定義はテンプレートまたはテンプレート スタックから継承され、オーバーライドのみ可能です。個々のデバイスの新しい変数定義を削除または作成することはできません。

テンプレートスタック内の既存のデバイスから変数定義をコピーするか、既存のデバイス変数定義を**Edit**（編集）してデバイス変数定義を**Create**（作成）します。

© 2019 Palo Alto Networks, Inc.

Panorama > Device Groups [Panorama > デバイス グループ]

デバイス グループは、1 つのグループとして管理するファイアウォールや仮想システムで構成されます。たとえば、会社内の支店または個々の部門によるグループを管理するファイアウォールなどが考えられます。Panorama はポリシーを適用するときに、これらのグループを 1 つの単位として処理します。ファイアウォールが属することができるデバイス グループは 1 つのみですが、Panorama では仮想システムが個別のエンティティになるため、ファイアウォール内の仮想マシンを異なるデバイス グループに割り当てることができます。

共有の場所に最大 4 レベルのツリー階層でデバイス グループをネストすることで、ファイアウォールのネットワーク全域にわたり、多層的にポリシーを管理することができます。一番下のレベルのデバイスグループは、連続する上位レベルとして親、祖父母、曾祖父母のデバイス グループを持つことができます。これらをまとめて先祖と呼び、一番下のレベルのデバイスグループはこれらからポリシーとオブジェクトを継承します。一番上のレベルのデバイス グループは、子、孫、曾孫のデバイス グループを持つことができます。これらをまとめて子孫と呼びます。 **Panorama** > **Device Groups** (デバイス グループ) を選択すると、Name (名前) 列にこのデバイス グループ階層が表示されます。

デバイス グループの追加、編集、削除を行った場合は、Panorama コミットおよびデバイス グループのコミットを実行します (「Panorama のコミット操作」を参照)。次に、Panorama は設定変更をそのデバイス グループに割り当てられたファイアウォールへプッシュします。Panorama では、最大 1,024 個のデバイス グループがサポートされています。

デバイス グループを設定するには、デバイス グループを **Add** (追加) し、以下の表の説明に従って設定を指定します。

デバイス グループ設定	の意味
氏名	グループを識別する名前を入力します (最大 31 文字)。この名前は、大文字と小文字が区別され、デバイス グループ階層全体で一意でなければならず、文字、数字、スペース、ハイフン、アンダースコアのみで構成されます。
の意味	デバイス グループの説明を入力します。
機器	デバイスグループに追加するファイアウォールをそれぞれ選択します。リストに多くのファイアウォールが表示される場合、**Device State**[デバイス状態]、**Platforms**[プラットフォーム]、**Templates**[テンプレート]、または **Tags**[タグ] でリストをフィルタリングできます。[フィルタ] セクションのかっこの中には、これらの各カテゴリの管理対象ファイアウォールの数が表示されます。 デバイス グループが純粋に組織化を目的とした (つまり、他のデバイス グループが含まれる) ものである場合、そのデバイス グループにファイアウォールを割り当てる必要はありません。
すべて選択	リスト中の全てのファイアウォールと仮想システムを選択します。
すべての選択を解除	リスト中の全てのファイアウォールと仮想システムの選択を解除します。
HA ピアのグループ化	高可用性 (HA) 設定のピアであるファイアウォールをグループ化する場合に選択します。これにより、リストには、アクティブ (アクティブ/アクティブ設定ではアクティ

© 2019 Palo Alto Networks, Inc.

デバイス グループ設定	の意味
	ブ-プライマリ) のファイアウォールが最初に表示されます。パッシブ (アクティブ/アクティブ設定ではアクティブ-セカンダリ) のファイアウォールはかっこ内に表示されます。これで、HA モードのファイアウォールを簡単に識別できます。共有ポリシーをプッシュする場合に、個々のピアではなくグループ化されたペアにプッシュできます。 アクティブ/パッシブ設定の *HA* ピアの場合は、両方のファイアウォールまたはそれらの仮想システムを同じデバイス グループに追加することを検討してください。これにより、両方のピアに設定を同時にプッシュできます。
フィルタが選択されています	特定のファイアウォールもしくは仮想システムを表示したい場合は、それらを選択した状態で**Filter Selected**[選択項目でフィルタ]を実行します。
親デバイス グループ	定義しているデバイスグループを基準として、その真上の階層にあるデバイスグループ (または共有場所) を選択します (デフォルトは**Shared**[共有]) 。
マスターデバイス	ユーザー名とユーザー グループに基づいてポリシー ルールおよびレポートを設定する場合、**Master Device** (マスター デバイス) を選択する必要があります。これは、Panorama がユーザー名、ユーザー グループ名、およびユーザー名とグループのマッピング情報を取得するファイアウォールです。 *Master Device* (マスター デバイス) を変更したり、*None* (なし) に設定したりすると、*Panorama* はそのファイアウォールから受信したすべてのユーザーおよびグループ情報を失います。
Store users and groups from Master Device (マスターデバイスからのユーザーおよびグループを保存)	このオプションは、**Master Device** (マスター デバイス) を選択した場合にのみ表示されます。このオプションを使用すると、Panorama は **Master Device** (マスター デバイス) から受信するユーザー名、ユーザー グループ名、およびユーザー名とグループのマッピング情報をローカルに保存できます。ローカル ストレージを有効にするには、**Panorama** > **Setup** (セットアップ) > **Management** (管理) を選択して Panorama 設定を編集し、 グループでのレポートとフィルタリングの有効化を行う必要もあります。
動的に追加されるデバイス プロパティ — 新しいデバイスがデバイス グループに追加されると、Panorama は指定された認証コードと PAN-OS ソフトウェア バージョンを新しいデバイスに動的に適用します。これは、デバイス グループが Panorama の NSX サービス定義に関連付けられていないと表示されません。	
認証コード	このデバイス グループに追加されたデバイスに適用される認証コードを入力します。
SW バージョン	このデバイス グループに追加されたデバイスに適用されるソフトウェア バージョンを選択します。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Collectors [Panorama > 管理対象コレクタ]

Panorama 管理サーバー（Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンス）は、専用ログ コレクタ（ログ コレクタ モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンス）を管理できます。また、各 Panorama 管理サーバーには、ファイアウォールから直接受信したログを処理するためのローカルの事前定義済みログ コレクタ（名前は default）があります。（レガシー モードの Panorama バーチャル アプライアンスは、専用のログ コレクタを使用せずに、ファイアウォールから直接受信するログを保存します）。

Panorama を使用して専用ログ コレクタを管理する場合は、ログ コレクタを管理対象コレクタとして追加します。

操作	以下を参照
ログ コレクタの情報を表示する	ログ コレクタの情報
ログ コレクタを追加、編集、または削除する	ログ コレクタの設定
ログ コレクタの Panorama ソフトウェアを更新する	専用ログ コレクタのソフトウェアの更新
その他の情報をお探しですか？	ログとレポートの中央管理
	Configure a Managed Collector（管理対象コレクタの設定）

ログ コレクタの情報

Panorama > **Managed Collectors**（管理対象コレクタ）をを選択し、ログ コレクタごとに以下の情報を表示します。その他のパラメータは、ログ コレクタの設定中に設定できます。

ログ コレクタの情報	の意味
コレクタ名	ログコレクタを識別するための固有名です。この名前はログコレクタホスト名として表示されます。
シリアル番号	ログ コレクタとして機能している Panorama アプライアンスのシリアル番号です。ログ コレクタがローカルの場合は、Panorama 管理サーバーのシリアル番号です。
ソフトウェア バージョン	ログコレクタにインストールされているPanoramaソフトウェアのリリースバージョンを示します。
IPアドレス	ログコレクタ用管理インターフェイスのIPアドレスです。
接続済み	ログコレクタとPanoramaの接続状況を示します。

© 2019 Palo Alto Networks, Inc.

ログ コレクタの情報	の意味
設定状態/詳細	ログコレクタの設定がPanoramaと同期されているかどうかを示します。
ランタイムステータス/詳細	コレクタグループ内の他のログコレクタとの接続状況を示します。
ログ再配信状態	特定の操作（ディスクの追加など）を行った場合、ログコレクタはディスクペアにログの再配信を行います。この列は再配信プロセスの完了状態がパーセントで表示されます。
最終コミット状態	ログコレクタ上で行われた前回のコレクタグループコミットが成功したか失敗したかを表示します。
統計	ディスク情報、CPU パフォーマンス、平均ログ数/秒を参照する場合は、ログ コレクタの設定を完了したのちに、**Statistics**（統計）をクリックします。レビュー中のログ範囲をよりよく理解するために、ログコレクタが受信した最も古いログ情報を表示することもできます。 SNMP マネージャを使用して集中管理する場合は、*panLogCollector MIB* でログ統計も参照できます。

ログ コレクタの設定

ログ コレクタを管理するには、**Panorama** > **Managed Collectors**（管理対象コレクタ）を選択します。新しいログ コレクタを管理対象コレクタとして **Add**（追加）するとき、構成する設定は、ログ コレクタの場所、および Panorama を高可用性（HA）設定でデプロイしたかどうかによって異なります。

- 専用ログ コレクタ – ログ コレクタを追加しても、**Interfaces**（インターフェイス）タブは最初からは表示されません。ログ コレクタのシリアル番号（**Collector S/N**（コレクタ シリアル番号））を入力して **OK** をクリックしてから、ログ コレクタを編集してインターフェイス設定を表示する必要があります。
- 孤立（**HA** 以外）またはアクティブ（**HA**）の **Panorama** 管理サーバーにローカルなデフォルト ログ コレクタ – Panorama 管理サーバーのシリアル番号（**Collector S/N**（コレクタ シリアル番号））を入力すると、Collector（コレクタ）ダイアログには、**Disks**（ディスク）設定、**Communication**（通信）設定、および一部の **General**（全般）設定のみが表示されます。ログ コレクタは、その他すべての設定の値を Panorama 管理サーバーの設定から取得します。
- （HA のみ）パッシブ **Panorama** 管理サーバーにローカルなデフォルト ログ コレクタ – Panorama はこのログ コレクタをリモートとして扱うため、専用ログ コレクタを設定する場合と同じように設定する必要があります。

ログ コレクタを設定する完全な手順では、いくつかの追加タスクを行う必要があります。

確認すべき情報	以下を参照
ログ コレクタを特定し、Panorama 管理サーバーおよび外部サービスとの接続を定義する。	ログ コレクタの一般設定

© 2019 Palo Alto Networks, Inc.

確認すべき情報	以下を参照
ログコレクタCLIへのアクセスを設定する。	ログ コレクタの CLI 認証設定
専用ログ コレクタが、管理トラフィック、コレクタ グループ通信、ログ収集に使用するインターフェイスを設定する。	ログ コレクタ インターフェイス設定
ファイアウォールから収集したログを保管するRAIDディスクを設定する。	ログ コレクタの RAID ディスク設定
ログ コレクタがユーザー マッピング情報を User-ID エージェントから受信するように設定する。	User-ID エージェント設定
ログ コレクタが Windows User-ID エージェントで認証するように設定する。	接続のセキュリティ
Panorama、その他のログ コレクタ、ファイアウォールとの通信用にセキュリティ設定を構成する。	通信設定

ログ コレクタの一般設定

- Panorama > Managed Collectors > General [Panorama > 管理対象コレクタ > 一般]

ログ コレクタを識別し、Panorama 管理サーバー、DNS サーバー、NTP サーバーとの接続を定義する場合は、以下の表に記載されている設定を行います。

ログ コレクタの一般設定	の意味
コレクタ シリアル番号	(必須) ログ コレクタとして機能する Panorama アプライアンスのシリアル番号を入力します。ログ コレクタがローカルである場合、Panorama 管理サーバーのシリアル番号を入力します。
コレクタ名	このログ コレクタの識別に使用する名前を入力します (最大 31 文字)。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。 この名前はログコレクタホスト名として表示されます。
保護された Syslog の着信証明書	Traps™ ESM サーバーからログを安全に取り込むために管理対象コレクタが使用しなければならない証明書を選択します。この証明書を着信証明書と呼びます。これは、Panorama/管理対象コレクタが Traps ESM (クライアント) がログを送信する宛先のサーバーであるためです。ログ インジェスト プロファイルの **Transport** (転送) プロトコルが **SSL** である場合、証明書が必要です。

© 2019 Palo Alto Networks, Inc.

ログ コレクタの一般設定	の意味
保護された Syslog の証明書	syslog を外部の Syslog サーバーに安全に転送するための証明書を選択します。証明書の **Certificate for Secure Syslog**（保護された **Syslog** の証明書）オプションが選択されている必要があります（「ファイアウォールおよび Panorama 証明書の管理」を参照）。このログ コレクタが含まれるコレクタ グループに Syslog サーバー プロファイルを割り当てる場合（Panorama > Collector Groups（コレクタ グループ）、**Panorama** > **Collector Groups**（コレクタ グループ）> **Collector Log Forwarding**（コレクタ ログ転送）を参照）、サーバー プロファイルの **Transport**（転送）プロトコルが **SSL** である必要があります（Device（デバイス）> Server Profiles（サーバー プロファイル）> Syslogを参照）。
Panorama サーバー IP	このログコレクタを管理しているPanorama管理サーバーの IPアドレスを指定します。
Panorama サーバー IP 2	Panorama管理サーバーがHA（高可用性）設定でデプロイされている場合、セカンダリピアのIPアドレスを指定します。
ドメイン	ログ コレクタのドメイン名を入力します。
プライマリDNSサーバー	プライマリ DNS サーバーの IP アドレスを入力します。ログ コレクタはこのサーバーを使用して DNS クエリ（Panorama 管理サーバーの検索など）を処理します。
セカンダリ DNS サーバー	（任意）プライマリサーバーを使用できない場合は、使用するセカンダリDNSサーバーのIPアドレスを入力します。
プライマリ NTP サーバー	プライマリ NTP サーバーの IP アドレスまたはホスト名を入力します (存在する場合)。NTP サーバーを使用しない場合は、ログ コレクタの時刻を手動で設定できます。
セカンダリ NTP サーバー	(任意)プライマリサーバーを使用できない場合、使用するセカンダリ NTPサーバーのIPアドレスまたはホスト名を入力します。
タイムゾーン	ログ コレクタのタイムゾーンを選択します。
緯度	ログコレクタの緯度（-90.0から90.0）を入力します。トラフィックおよび脅威マップがアプリケーションスコープ用にこの緯度を使用します。
経度	ログコレクタの経度（-180.0から180.0）を入力します。トラフィックおよび脅威マップがアプリケーションスコープ用にこの経度を使用します。

ログ コレクタの *CLI* 認証設定

- Panorama > Managed Collectors > Authentication [Panorama > 管理対象コレクタ > 認証]

ログコレクタモードのM-Seriesアプライアンス（専用ログコレクタ）にはウェブインターフェイスがなく、CLIのみを持っています。専用ログ コレクタの設定の大部分は、Panorama 管理サーバーを使用して行うことができますが、一部 CLI アクセスを必要とするものもあります。CLI アクセス用の認証設定を行う場合は、次の表で説明する設定を行います。

© 2019 Palo Alto Networks, Inc.

ログ コレクタ認証設定	の意味
Users	常に `admin` と表示され、ログ コレクタでのローカル CLI ログイン名に使用されます。
モード	パスワードの **Mode**（モード）を選択します。 • **Password**（パスワード）– プレーンテキストの **Password**（パスワード）を入力し、**Confirm Password**（再入力 パスワード）にパスワードを再入力します。 • **Password Hash**[パスワード ハッシュ] – ハッシュされたパスワード文字列を入力します。これが便利なのは、たとえば、既存の UNIX アカウントのパスワードを再利用したいが、プレーンテキストのパスワードがわからず、ハッシュされたパスワードしか知らない場合です。Panorama では、ハッシュ値の生成に使用されるアルゴリズムに関係なく、63 文字までの任意の文字列を使用できます。CLI 操作コマンド **`request password-hash password`** *<password>* では、MD5 アルゴリズムが使用されます。変更内容をコミットすると、Panorama はハッシュ値をログ コレクタにプッシュし、管理者パスワードは指定の *password>* になります。
最大試行回数	CLI で許容されるログイン試行回数を入力します（0 ~ 10）。この回数を超えると管理者アカウントはロックされます。値 0 を指定すると、無制限にログインを試行できます。デフォルト値は、通常の運用モードのログ コレクタでは 0、FIPS-CC モードのログ コレクタでは 10 です。ログイン試行回数を制限することにより、総当たり攻撃からログ コレクタを保護しやすくなります。 *Failed Attempts (試行失敗回数) を 0 以外の値にしながら、Lockout Time (ロックアウト時間) を 0 のままにしている場合、別の管理者がロックアウトされた管理者を手動でロック解除するまで、管理者ユーザーは無期限にロックアウトされます。他の管理者が作成されていない場合は、Panorama で Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト時間) の設定を再構成し、構成変更をログ コレクタにプッシュする必要があります。管理者がロックアウトされないようにするには、Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト時間) の両方にデフォルト値の 0 を使用します。*
ロックアウト時間	**Failed Attempts**（最大試行回数）の数値に達してから、ログ コレクタが管理者をロックする時間（分単位）を入力します（範囲は 0 ~ 60、デフォルトは 0）。 *Failed Attempts (試行失敗回数) を 0 以外の値にしながら、Lockout Time (ロックアウト時間) を 0 のままにしている場合、別の管理者がロックアウトされた管理者を手動でロック解除するまで、管理者ユーザーは無期限にロックアウトされます。他の管理者が作成されていない場合は、Panorama で Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト時間) の設定を再構成し、構成変更をログ コレクタにプッシュする必要があります。管理者がロックアウトされないようにするには、Failed Attempts (試行失敗回数) および Lockout Time (ロックアウト時間) の両方にデフォルト値の 0 を使用します。*

ログ コレクタ インターフェイス設定

- Panorama > Managed Collectors（管理対象コレクタ）> Interfaces（インターフェイス）

デフォルトでは、専用ログ コレクタ（ログ コレクタ モードの M-Series アプライアンス）では、管理トラフィック、ログ収集、コレクタ グループ通信に管理（MGT）インターフェイスが使用さ

© 2019 Palo Alto Networks, Inc.

れます。ただし、Palo Alto Networks では、ログ収集とコレクタ グループ通信に個別のインターフェイスを割り当て、MGT インターフェイスのトラフィックを減らすことをお勧めしています。その他のインターフェイスのサブネットよりも秘密性の高い MGT インターフェイスのサブネットを別途定義することで、セキュリティを向上させることができます。個別のインターフェイスを使用するには、まず Panorama 管理サーバーで個別のインターフェイスを設定する必要があります（「Device（デバイス）> Setup（セットアップ）> Management（管理）」を参照）。ログ収集とコレクタ グループ通信に使用できるインターフェイスは、ログ コレクタ アプライアンスのモデルに応じて異なります。例えば、M-500 アプライアンスには次のインターフェイスがあります：Ethernet1（1Gbps）、Ethernet2（1Gbps）、Ethernet3（1Gbps）、Ethernet4（10Gbps）、Ethernet5（10Gbps）

インターフェイスを設定するには、以下の表の説明に従ってリンクを選択して設定を構成します。

MGT インターフェイスの設定を完了するには、*IP* アドレス、ネットマスク（*IPv4* の場合）、プレフィックス長（*IPv6* の場合）のいずれかと、デフォルト ゲートウェイを指定する必要があります。不完全な設定をコミットした場合（デフォルトゲートウェイを省略した場合など）、追って設定を変更する場合はコンソールポート経由でファイアウォールまたは*Panorama*に接続する必要があります。

必ず、完全な *MGT* インターフェイス設定をコミットしてください。*IP* アドレス、ネットマスク（*IPv4* の場合）、プレフィックス長（*IPv6* の場合）のいずれかと、デフォルト ゲートウェイを指定しない場合は、その他のインターフェイスの設定をコミットできません。

ログ コレクタ インターフェイス設定	の意味
Eth1/Eth2/Eth3/Eth4/Eth5	インターフェイスを有効にして設定する必要があります。MGT インターフェイスは例外で、これはデフォルトで有効になっています。
速度とデュプレックス	インターフェイスのデータ速度とデュプレックス オプションを設定します。フル デュプレックスまたはハーフ デュプレックスで、10Mbps、100Mbps、1Gbps、10Gbps（Eth4 と Eth5 のみ）のいずれかを選択できます。ログ コレクタにインターフェイス速度を決定させるには、デフォルトの**auto-negotiate**（オート ネゴシエート）設定を使用します。 この設定は、隣接するネットワーク機器のインターフェイス設定と一致する必要があります。
IP アドレス (IPv4)	ネットワークで IPv4 を使用する場合、IPv4 アドレスをインターフェイスに割り当てます。
ネットマスク (IPv4)	IPv4 アドレスをインターフェイスに割り当てた場合は、ネットワーク マスク（例: 255.255.255.0）を入力する必要もあります。
デフォルト ゲートウェイ（IPv4）	IPv4 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイに IPv4 アドレスを割り当てる必要もあります（ゲートウェイは MGT インターフェイスと同じサブネット上にある必要があります）。
IPv6 アドレス/プレフィックス長	ネットワークで IPv6 を使用する場合、IPv6 アドレスをインターフェイスに割り当てます。ネットマスクを示すには、IPv6 プレフィックス長を入力します（例: 2001:400:f00::1/64）。

© 2019 Palo Alto Networks, Inc.

ログ コレクタ インターフェイス設定	の意味
デフォルト IPv6 ゲートウェイ	IPv6 アドレスをインターフェイスに割り当てた場合は、デフォルト ゲートウェイにも IPv6 アドレスを割り当てる必要があります (ゲートウェイはインターフェイスと同じサブネット上にある必要があります) 。
MTU	このインターフェイスで送信されるパケットの最大転送単位 (MTU) をバイト数で入力します (範囲は 576 ~ 1,500、デフォルトは 1,500) 。
デバイス ログ収集	ファイアウォールからのログ収集のインターフェイスを有効にします。ログ トラフィックが多いデプロイでは、複数のインターフェイスを有効にしてこの機能を実行できます。この機能は、MGT インターフェイスでデフォルトで有効になっています。
コレクタ グループ通信	コレクタ グループ通信のインターフェイスを有効にします。この機能を実行できるインターフェイスは 1 つのみです (デフォルトは MGT インターフェイス) 。
ネットワーク接続性サービス	**Ping** サービスを任意のインターフェイスで使用でき、ログ コレクタ インターフェイスと外部サービスとの間で接続をテストできます。 次のサービスを使用できるのは、MGT インターフェイスのみです。 • **SSH** – Panorama CLI への安全なアクセスを有効にします。 • **SNMP** – 統計クエリを SNMP マネージャーから受信するインターフェイスを有効にします。詳細は、「SNMP モニタリングの有効化」を参照してください。 • **User-ID** – ログ コレクタが User-ID エージェントから受信したユーザー マッピング情報を再配信できるようにします。
アクセス許可IPアドレス	このインターフェイスでログ コレクタにアクセスできるクライアント システムの IP アドレスを入力します。 リストを空にすると (デフォルト) 、すべてのクライアント システムがアクセスできるようになります。 *Palo Alto Networks* では、このリストをブランクにしないことをお勧めしています。*Panorama* 管理者のクライアント システムを指定して、不正アクセスを阻止してください。

ログ コレクタの *RAID* ディスク設定

- Panorama > Managed Collectors > Disks [Panorama > 管理対象コレクタ > ディスク]

M-Series アプライアンスまたは Panorama バーチャル アプライアンスでログ ディスクを設定した後で、ログ コレクタ設定にそれを **Add** (追加) できます。

M-Series アプライアンスは通常、最初の RAID 1 ディスク ペアが A1 と A2 ベイにインストールされた状態で出荷されます。ソフトウェアでは、A1 と A2 ベイのディスク ペアに Disk Pair A (ディスク ペア A) という名前が付いています。残りのベイには順番に、Disk Pair B (ディスク ペア B) 、Disk Pair C (ディスク ペア C) というように名前が付きます。例えばい、M-500 アプライアンスでは、最大 12 個のディスク ペアがサポートされています。同一アプライアンスでは 2TB または 1TB のディスクのペアをインストールできますが、ディスク サイズは各ペアの両方のドライブで同一にする必要があります。

© 2019 Palo Alto Networks, Inc.

Panorama バーチャル アプライアンスでは、ストレージ容量が 24TB の 12 個までの仮想ログ ディスクがサポートされます。

新しいディスクペアを追加すると、ログ コレクタはその既存のログをすべてのディスクに再配信します。この処理には、ログ 1 テラバイトごとに数時間かかる可能性があります。再配信プロセス中は、最大ログ インジェスト率が低くなります。**Panorama** > **Managed Collectors**（管理対象コレクタ）ページの Log Redistribution State（ログ再配信状態）列には、プロセスの完了状況がパーセントで表示されます。

SNMP マネージャを使用して中央監視する場合は、*panLogCollector MIB* でログ統計を参照できます。

User-ID エージェント設定

- Panorama > Managed Collectors（管理対象コレクタ）> User-ID Agents（ユーザー ID エージェント）

専用ログ コレクタでは、最大 100 個の User-ID エージェントからユーザー マッピングを受け取ることができます。エージェントは、ファイアウォールで動作する PAN-OS 統合 User-ID エージェントまたは Windows ベース User-ID エージェントにすることができます。複数の仮想システムがあるファイアウォールでは、各仮想システムが個別の User-ID エージェントとして動作できます。この場合、ログ コレクタは、ファイアウォールまたは Panorama 管理サーバーにユーザー マッピングを再配信できます。

configure user mapping（ユーザー マッピング設定）とnableusermapping redistribution（ユーザー マッピングの再配信）を設定する手順全体では、*User-ID* エージェントの接続以外に、さらにタスクを実行する必要があります。

専用ログ コレクタを設定して User-ID エージェントに接続するには、User-ID エージェントを **Add**（追加）して、次の表で説明する設定を構成します。

User-ID エージェント設定	の意味
氏名	User-ID エージェントの識別に使用する名前（最大 31 文字）を入力します。大文字と小文字を区別し、一意の名前を入力する必要があります。文字、数字、スペース、ハイフン、アンダースコアのみが使用できます。 *User-ID* エージェントとして機能するファイアウォールの場合、このフィールドは Collector Name（コレクタ名）フィールドと一致させる必要はありません。
ホスト	• **Windows** ベースの **User-ID** エージェント – User-ID エージェントがインストールされている Windows ホストの IP アドレスを入力します。 • ファイアウォール（**PAN-OS** 統合 **User-ID** エージェント）– ファイアウォールがユーザー マッピングの再配信に使用するインターフェイスのホスト名または IP アドレスを入力します。
ポート	User-IDエージェントがUser-ID要求をリッスンするポートの番号を入力します。デフォルトはポート 5007 ですが、使用可能な任意のポートを指定可能です。それぞれのUser-IDエージェントでは異なるポートを使用することができます。 一部の旧バージョンの *User-ID* エージェントでは、デフォルトとして *2010* を使用します。

© 2019 Palo Alto Networks, Inc.

User-ID エージェント設定	の意味
コレクタ名	これらのフィールドが参照するコレクタは User-ID エージェントであり、ログ コレクタではありません。このフィールドが適用されるのは、エージェントがファイアウォールまたは仮想システムであり、それがユーザー マッピングをログ コレクタに再配信する場合に限られます。ファイアウォールまたは仮想システムを User-ID エージェントとして識別する **Collector Name**（コレクタ名）および **Pre-Shared Key**（事前共有鍵）を入力します。User-ID エージェントとして動作するようにファイアウォールまたは仮想システムを設定したときと同じ値を入力する必要があります（「Redistribution（再配信）」を参照）。
コレクタの事前共有鍵/コレクタの事前共有鍵の再入力	
enabled [有効化]	ログ コレクタが User-ID エージェントと通信できるようにする場合に選択します。

接続のセキュリティ

- Panorama > Managed Collectors（管理対象コレクタ）> Connection Security（接続のセキュリティ）

Windows User ID エージェントによって提示された証明書を検証するためにログ コレクタが使用する証明書プロファイルを設定します。ログ コレクタは、選択された証明書プロファイルを使用して、User ID エージェントによって提示されたサーバー証明書を検証し、エージェントのアイデンティティを検証します。

タスク	の意味
User-ID 証明書プロファイル	ドロップダウン リストから、Windows User ID エージェントでの認証に使用する証明書プロファイルを選択するか、New Certificate Profile（新規証明書プロファイル）を選択して証明書プロファイルを作成します。証明書プロファイルを削除するには、None（なし）を選択します。

通信設定

- Panorama > Managed Collectors（管理対象コレクタ）> Communication（通信）

ログ コレクタと Panorama、ファイアウォール、他のログ コレクタ間でカスタムの証明書ベースの認証を設定するには、以下の表に記載されているように設定します。

通信設定	の意味
保護されたサーバー通信 — **Secure Server Communication**（保護されたサーバー通信）を有効にすると、ログ コレクタに接続しているクライアント デバイスの識別情報が検証されます。	
SSL/TLS Service Profile	ドロップダウン リストから SSL/TLS サービス プロファイルを選択します。このプロファイルはログ コレクタが提示する証明書を定義し、ログ コレクタとの通信で可能な SSL/TLS バージョンの範囲を指定します。
証明書プロファイル	ドロップダウン リストから証明書プロファイルを選択します。この証明書プロファイルは証明書取り消しチェック動作を定義し、クライアントが提示する証明書チェーンの認証で使用するルート CA を定義します。

© 2019 Palo Alto Networks, Inc.

通信設定	の意味
カスタム証明書のみ	有効化すると、管理対象ファイアウォールとログ コレクタの認証に関して、ログ コレクタはカスタム証明書のみを受け入れます。
シリアル番号に基づいてクライアントを承認	ログ コレクタは、クライアント デバイスのシリアル番号のハッシュに基づいてクライアント デバイスを承認します。
承認リストのチェック	このログ コレクタに接続しているクライアント デバイスまたはデバイス グループを、認証リストに照らして確認します。
切断待機時間（分）	管理対象デバイスとの現行の接続を切断するまでにログ コレクタが待機する時間です。その後、ログ コレクタは指定済みの保護されたサーバー通信設定を使用して、管理対象デバイスとの通信を再構築します。待機時間は、保護されたサーバー通信の設定がコミットされた後に開始されます。
承認リスト	**Authorization List**（承認リスト）— Add（追加）を選択して、以下のフィールドで基準を設定します。 • **Identifier**（識別子）—Select **Subject**（サブジェクト）または **Subject Alt**（サブジェクト代替）を選択します。認証識別子としての**Name**（名前）を付けます。 • **Type**（タイプ）— Subject Alt（サブジェクト代替）の場合。Name（名前）を識別子として選択した場合、識別子のタイプとして **IP**、**hostname**（ホスト名）、または **e-mail**（電子メール）を選択します。Subject（サブジェクト）を選択した場合、識別子のタイプとして共通名が使用されます。 • **Value**（値）— 識別子の値を入力します。
保護されたクライアント通信 — **Secure Client Communication**（保護されたクライアント通信）を有効にすると、Panorama、ファイアウォール、他のログ コレクタとの SSL 通信でのログ コレクタの認証において、特定のクライアント証明書が使用されます。	
証明書タイプ	通信の保護のために使用するデバイス証明書のタイプ（None（なし）、Local（ローカル）、または SCEP）を選択します。
まったくない	**None**（なし）を選択した場合、デバイス証明書は設定されず、保護されたクライアント通信は使用されません。これがデフォルトの選択です。
ローカル	ログ コレクタは、ログ コレクタで生成された、または既存のエンタープライズ PKI サーバーからインポートされた、ローカルのデバイス証明書と、対応する秘密鍵を使用します。
	Certificate（証明書）— ローカルのデバイス証明書を選択します。この証明書は、ファイアウォールに対して一意のものであっても（ログ コレクタのシリアル番号のハッシュに基づく）、Panorama に接続しているすべてのログ コレクタで使用される共通のデバイス証明書であっても構いません。
	Certificate Profile（証明書プロファイル）— ドロップダウン リストから証明書プロファイルを選択します。この証明書プロファイルは、ログ コレクタのサーバー認証の定義に使用します。
SCEP	ログ コレクタは、Simple Certificate Enrollment Protocol（SCEP）サーバーで生成されたデバイス証明書と秘密鍵を使用します。

© 2019 Palo Alto Networks, Inc.

通信設定	の意味
	SCEP Profile（**SCEP** プロファイル）– ドロップダウン リストから SCEP プロファイルを選択します。
	Certificate Profile（証明書プロファイル）– ドロップダウン リストから証明書プロファイルを選択します。この証明書プロファイルは、ログ コレクタのサーバー認証の定義に使用します。
サーバー アイデンティティのチェック	共通名（CN）とサーバーの IP アドレスまたは FQDN の照合によって、クライアント デバイスがサーバーの識別情報を確認します。

専用ログ コレクタのソフトウェアの更新

- Panorama > Managed Collectors [Panorama > 管理対象コレクタ]

専用ログ コレクタにソフトウェア イメージをインストールする場合は、Panorama にイメージをダウンロードまたはアップロードし（「Panorama > Device Deployment（デバイスのデプロイ）」を参照）、**Install**（インストール）をクリックして、以下のフィールドを設定します。

Panorama 管理サーバーのオペレーティング システムはローカルのデフォルト ログ コレクタと共有されるため、ソフトウェア更新を *Panorama* 管理サーバーにインストールすると、両方がアップグレードされます（「Panorama > Software（ソフトウェア）」を参照）。

専用ログ コレクタの場合、*Panorama* > *Device Deployment*（デバイスのデプロイ）> *Software*（ソフトウェア）を選択して、更新をインストールすることもできます（「ソフトウェアおよびコンテンツ更新の管理」を参照）。

管理（*MGT*）インターフェイスのトラフィックを削減するには、更新のデプロイのために個別のインターフェイスを使用するように *Panorama* を設定します（「Panorama > Setup（セットアップ）> Interfaces（インターフェイス）」を参照）。

ログ コレクタへのソフトウェア更新のインストールに関するフィールド	の意味
ファイル	ダウンロードまたはアップロードされたソフトウェアイメージを選択します。
機器	ソフトウェアをインストールするログコレクタを選択します。ダイアログには、それぞれのログコレクタにつき、以下の情報が表示されます。 • **Device Name**（デバイス名）- 専用ログ コレクタの名前です。 • **Current Version**[現在のバージョン] - ログコレクタに現在インストールされているPanoramaソフトウェアのリリースバージョンを示します。 • **HA Status**[HA状況] - ログコレクタの場合、この列は使用しません。専用ログコレクタにおいて高可用性はサポートされていません。
フィルタが選択されています	特定のログコレクタのみを表示する場合は、ログコレクタを選択し、**Filter Selected**[選択項目でフィルタ]を実行します。
Upload only to device (do not Install)（デバイ	ログ コレクタにソフトウェアをアップロードし、自動的に再起動させない場合に選択します。ログ コレクタ CLI にログインして、`request restart system`

© 2019 Palo Alto Networks, Inc.

ログ コレクタへのソフトウェア更新のインストールに関するフィールド	の意味
スにアップロードするだけ（インストールは行わない））	の操作コマンドを実行して手動で再起動を行うまで、イメージはインストールされません。
Reboot device after Install（インストール後にデバイスを再起動）	ソフトウェアのアップロード後に自動的にインストールを行う場合に選択します。インストール処理によりログコレクタは再起動されます。

© 2019 Palo Alto Networks, Inc.

Panorama > Collector Groups [Panorama > コレクタ グループ]

各コレクタ グループには最大 16 個のログ コレクタを割り当てることができ、またそれぞれにはログ転送用のファイアウォールを割り当てることができます。こうすることでPanoramaを使用してログコレクタに対するクエリを行い、集約ログの表示と調査を行うことができます。

事前に定義されているコレクタ グループ（名前はデフォルト）には、*Panorama* 管理サーバー上にローカルに存在する、事前に定義されたログ コレクタを含まれています。

- コレクタ グループの設定
- コレクタグループの情報

コレクタ グループの設定

コレクタグループを設定する場合は、**Add** (追加)をクリックし、以下のパラメータを入力します。

コレクタグループ設定	設定場所	の意味
氏名	**Panorama** > **Collector Groups** コレクタ グループ] > **General**	このコレクタ グループを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
ログストレージ		コレクタ グループが受信するファイアウォール ログのストレージ割り当て合計と使用可能領域を示します。 ストレージ割り当てリンクをクリックして、以下のログタイプのストレージ **Quota(%)**（割り当て（%））と有効期間（**Max Days**（最大日数））を設定します。 • **Detailed Firewall Logs**（詳細なファイアウォール ログ）– トラフィック、脅威、HIP マッチ、動的に登録された IP アドレス（IP タグ）、拡張 PCAP、GTP とトンネル、アプリ統計など、**Device**（デバイス）> **Setup**（セットアップ）> **Logging and Reporting Settings**（ロギングおよびレポート設定）のすべてのログ タイプが含まれます。 • **Summary Firewall Logs**（サマリー ファイアウォール ログ）– トラフィック サマリー、脅威サマリー、URL サマリー、GTP およびトンネル サマリーのように、**Device**（デバイス）> **Setup**（セットアップ）> **Logging and Reporting Settings**（ロギングおよびレポート設定）のすべてのサマリー ログが含まれます。 • **Infrastructure and Audit Logs**（インフラストラクチャおよび監査ログ）– 設定、システム、User-ID、および認証ログが含まれます。

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味
		• **Palo Alto Networks Platform Logs**（**Palo Alto Networks** プラットフォーム ログ）– Traps などの Palo Alto Networks 製品からのログが含まれます。 • **3rd Party External Logs**（サードパーティ外部ログ）– Palo Alto Networks が提供するその他のベンダー統合のログが含まれます。 デフォルトの設定を使用する場合は**Restore Defaults**[デフォルトを復元]をクリックします。
最小保持期間(日)		コレクタグループ内のすべてのログコレクタにおいて、Panoramaがログを保持する最小期間 (1 ~ 2000日)を入力します。現在の日付から最も古いログの日付を引いた値が、定義した最小保持期間よりも小さくなる場合、Panoramaはアラート違反のシステムログを生成します。
コレクター グループのメンバー		このコレクタ グループに含めるログ コレクタを **Add**（追加）します（最大 16 個）。**Panorama** > **Managed Collectors**（管理対象コレクタ）ページで使用可能なログ コレクタを追加できます。特定のコレクタ グループのすべてのログ コレクタが、同じモデルである必要があります（例えば、すべての M-500 アプライアンス、またはすべての Panorama バーチャル アプライアンス）。 ログ コレクタを既存のコレクタ グループに追加すると、*Panorama* はその既存のログをすべてのログ コレクタに再配信します。この処理には、ログ *1* テラバイトごとに数時間かかる可能性があります。再配信プロセス中は、最大ロギング率が低くなります。*Panorama* > *Collector Groups*（コレクタ グループ）ページの *Log Redistribution State*（ログ再配信状態）列には、プロセスの完了状況がパーセントで表示されます。
コレクタ間のログ冗長性の有効化		このオプションを選択した場合、コレクタグループ内の各ログのコピーが2つ作成され、それぞれ異なるログコレクタに保存されます。この冗長性により、いずれかのログコレクタが利用不可になってもログは失われません。すべてのログがコレクタ グループに転送されていることを確認でき、すべてのログ データに関するレポートを実行できます。ログ冗長性を利用できるのは、コレクタ グループに複数のログ コレクタがあり、各ログ コレクタのディスク数が同じ場合のみです。 冗長性を有効にすると、Panorama は既存のログをすべてのログ コレクタに再配信します。この処理には、ログ 1 テラバイトごとに数時間かかる可能性があります。再配信プロセス中は、最大ロギング率が低くなります。**Panorama** > **Collector Groups**（コレクタ グルー

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味
		プ）ページの Log Redistribution State（ログ再配信状態）列には、プロセスの完了状況がパーセントで表示されます。特定のコレクタ グループのすべてのログ コレクタが、同じモデルである必要があります（例えば、すべての M-500 アプライアンス、またはすべての Panorama バーチャル アプライアンス）。 冗長性を有効にすると、作成されるログが多くなるため、この設定には、より大きなストレージ容量が必要です。冗長性を有効にすると、コレクタ グループ内のログ処理トラフィックが 2 倍になり、最大ロギング率が半分になります。各ログ コレクタが、受信する各ログのコピーを配信する必要があるためです。（コレクタ グループの容量が不足すると、古いログが削除されます。）
設定リストのすべてのコレクタに転送		（PA-5200 シリーズおよび PA-7000 シリーズのファイアウォールのみ）設定リストのすべてのログ コレクタにログを送信する場合に選択します。Panorama はラウンドロビン負荷分散を使用して、ログを受信するログ コレクタを適宜選択します。これはデフォルトでは無効です。ログ コレクタが使用不可にならない限り、ファイアウォールはリストの最初のログ コレクタにのみログを送信します（「Devices / Collectors（デバイス/コレクタ）」を参照）。
Secure Inter LC Communication（セキュア インター LC 通信）の有効化	セ	Collector Group（コレクタ グループ）内の Log Collectors（ログ コレクタ）間の相互 SSL 認証にカスタム証明書を使用できるようにします。
場所	**Panorama** > **Collector Groups** コレクタ グループ] > **Monitoring**（モニタリング）	コレクタ グループの場所を指定します。
お問い合わせ		連絡先メールアドレスを設定します（ログコレクタを監視するSNMP管理者の電子メールアドレスなど）。
バージョン		Panorama管理サーバーとの通信に使用するSNMPのバージョンを指定します。**V2cまたはV3** SNMPにより、接続状態、ディスクドライブ統計、ソフトウェアバージョン、平均CPU使用率、平均ログ/秒、ログタイプ別の保存期間など、ログコレクタに関する情報の収集ができるようになります。SNMP 情報は、コレクタ グループごとに利用できます。
SNMPコミュニティ名（V2cのみ）		SNMPマネージャおよびモニター対象デバイス(この場合はログコレクタ)のSNMPコミュニティを識別し、コミュニティメンバーを相互認証するためのパスワードとして機能

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味
		するSNMP Community String [SNMPコミュニティ名] を入力します。 デフォルトのコミュニティ名 *public* は、広く公開されていて安全ではないので使用しないでください。
ビュー（V3のみ）		SNMPビューのグループを**Add**[追加]し、**Views**[ビュー]内でグループ名を入力してください。 各ビューは、オブジェクト識別子（OID）とビット単位のマスクの組み合わせです。OIDで管理対象の情報ベース（MIB）を指定し、16進数形式のマスクを使用して、そのMIB内（一致検索）またはMIB外（不一致検索）でアクセス可能なSNMPオブジェクトを指定します。 グループ内のそれぞれのビューについて、以下の設定を**Add**[追加] します。 • **View**（ビュー）- ビューの名前を指定します。 • **OID** - OIDを指定します。 • **Option**[オプション]（含めるか除外するか）- ビューにOIDを含めるか除外するかを選択して下さい。 • **Mask**[マスク] — OIDに適用するフィルタのマスク値を指定します(0xf0など)。
ユーザー（V3のみ）		それぞれのSNMP用に以下の設定を**Add**[追加] します。 • **Users**[ユーザー] - SNMPマネージャにおけるユーザー認証に使用するユーザー名を入力します。 • **View**（ビュー）- ユーザーが使用できるビューのグループを指定します。 • **Authpwd**（認証パスワード）- SNMP マネージャにおけるユーザー認証に使用するパスワードを入力します（8 文字以上）。パスワードの暗号化でサポートされているのはSecure Hash Algorithm（SHA）のみです。 • **Privpwd**（専用パスワード）- SNMP マネージャに送信する SNMP メッセージを暗号化する際の専用パスワードを入力します（8 文字以上）。Advanced Encryption Standard (AES) のみがサポートされています。
デバイス/コレクタ	**Panorama** > **Collector Groups**（コレクタ グループ）> **Device Log Forwarding**（デバイス ログ転送）	ログ転送設定リストは、どのファイアウォールからどのログ コレクタにログを転送するかを制御します。リストに **Add**（追加）するエントリごとに、Devices（デバイス）リストを **Modify**（変更）してファイアウォールを割り当てて、Collectors（コレクタ）リストにログ コレクタを **Add**（追加）します。 デフォルトでは、リスト エントリで割り当てたファイアウォールは、プライマリ（1 番目の）ログ コレクタにのみ（使用可能である限り）ログを送信します。プライマリ ログ コレクタで障害が発生すると、ファイアウォールは

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味
		セカンダリ ログ コレクタにログを送信します。セカンダリで障害が発生すると、ファイアウォールは第 3 ログ コレクタにログを送信します (以下同様)。この順番を変更する場合は、ログ コレクタを選択して**Move Up**[上へ] ボタンまたは **Move Down**[下へ]をクリックします。 *PA-5200 シリーズと PA-7000 シリーズのファイアウォールのデフォルト ログ転送動作をオーバーライドするには、General (全般) タブの* Forward to all collectors in the preference list (設定リストのすべてのコレクタに転送) を選択します。

システム<:so>システム
設定
HIP マッチ
トラフィック
脅威
WildFire
製品連携
GTP
authentication
User-ID
トンネル
IP-Tag
	Panorama > **Collector Groups** (コレクタ グループ) > **Collector Log Forwarding** (コレクタ ログ転送)	このコレクタ グループから外部サービスに転送するファイアウォール ログのタイプごとに、一致リスト プロファイルを **Add** (追加) します。プロファイルは転送するログと宛先サーバーを指定します。プロファイルごとに以下を設定します。
		
		• **Name** (名前) – 一致リスト プロファイルの識別に使用する名前を入力します (最大 31 文字)。
		• **Filter** (フィルタ) – デフォルトでは、この一致リスト プロファイルが適用されているタイプの **All Logs** (すべてのログ) をファイアウォールは転送します。一部のログを転送するには、既存のフィルタを選択するか、**Filter Builder** (フィルタ ビルダー) を選択して新しいフィルタを追加します。新しいフィルタの各クエリに対して、以下のフィールドを指定して、クエリを **Add** (追加) します。
		
		  • **Connector** (条件式) – 結合子の論理を選択します (and/or)。**Negate** (上記以外) を選択すると、指定した内容を除外します。たとえば、信頼されていないゾーンからのログ転送を防ぐには、**Negate** (上記以外) を選択し、Attribute (属性) として **Zone** (ゾーン)、Operator (演算子) として **equal** (等しい) を選択して、Value (値) 列に信頼されていないゾーンの名前を入力します。
		  • **Attribute** (属性) – ログの属性を選択します。ログ タイプによりオプションが異なります。
		  • **Operator** (演算子) – 属性をどのように適用するかを定める基準を選択します (**equal** (等しい) など)。ログ タイプによりオプションが異なります。
		  • **Value**[値] – 照合する属性値を指定します。
		
		フィルタが一致するログを表示またはエクスポートするには、**View Filtered Logs** (フィルタリングされたログの表示) を選択します。このタブでは **Monitoring** (モニタリング) タブのページと同じオプションが表示されます (**Monitoring** (モニタリング) > **Logs** (ログ) > **Traffic** (トラフィック) など)。

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味

		• **Description**（説明）– この一致リスト プロファイルの主旨に関する説明を最大 1,023 文字で入力します。
		• Destination servers（宛先サーバー）– 各サーバー タイプにサーバー プロファイルを **Add**（追加）します。サーバー プロファイルを設定する手順については、「Device（デバイス）> Server Profiles（サーバー プロファイル）> SNMP Trap（SNMP トラップ）」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> Syslog」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> Email（電子メール）」、または「Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP」を参照してください。
		• Built-in Actions（ビルトイン アクション）– システムおよび設定ログ以外のすべてのログ タイプのアクションを **Add**（追加）できます。
		  • **Action**（アクション）に分かりやすい名前を入力します。
		  • タグ付けする IP アドレス（**Source Address**（送信元アドレス）または **Destination Address**（宛先アドレス））を選択します。相関ログと HIP マッチ ログの送信元 IP アドレスにのみタグ付けできます。
		  • アクション（**Add Tag**（タグの追加）または **Remove Tag**（タグの除去））を選択します。
		  • この Panorama のローカル User-ID エージェントでタグを登録するか、リモート User-ID エージェントでタグを登録するかを選択します。
		  Remote device User-ID Agent（リモート デバイス User-ID エージェント）でタグを登録するには、転送できるようにする HTTP サーバー プロファイルを選択します。
		  • IP 対タグの **Timeout (タイムアウト)**を指定すれば、IP アドレス対タグのマッピングを保持する期間（分）を設定できます。タイムアウトを 0 にすると、IP 対タグのマッピングがタイムアウトしなくなります（範囲は 0 ~ 43200（30 日）、デフォルトは 0）。
		  タイムアウトを設定できるのは*Add Tag (タグの追加)*アクションだけです。
		  • ターゲットの送信元または宛先 IP アドレスに対して適用または削除する **Tags**（タグ）を入力または指定します。

インジェスト プロファイル	**Panorama** > **Collector Groups**（コレクタ グループ）> **Log Ingestion**（ログ インジェスト）	Panorama が Traps ESM サーバーからログを受信できるようにするログ インジェスト プロファイルを **Add**（追加）します。新しいログ インジェスト プロファイルを設定する手順については、「Panorama > Log Ingestion

© 2019 Palo Alto Networks, Inc.

コレクタグループ設定	設定場所	の意味
		Profile（ログ インジェスト プロファイル）」を参照してください。

コレクタグループの情報

Panorama > **Collector Groups** コレクタグループ を選択し、コレクタグループごとに以下の情報を表示します。その他のフィールドは、ログ コレクタの設定が完了した後に設定できます。

コレクタグループの情報	の意味
氏名	コレクタグループを識別するための名前です。
冗長性対応	コレクタグループのログの冗長性が有効化されているかどうかを示します。ログ コレクタの設定を完了または変更した後に、コレクタ グループのログ冗長性を有効にできます。
コレクタ	コレクタグループに割り当てられたログコレクタを示します。
ログ再配信状態	特定の操作（ログ冗長性の有効化など）を行った場合、コレクタグループはログコレクタに対しログの再配信を行います。この列は再配信プロセスの完了状態がパーセントで表示されます。

© 2019 Palo Alto Networks, Inc.

Panorama > Plugins (プラグイン)

- **Panorama** > **Plugins** (プラグイン)
- **Device** (デバイス) > **Plugins** (プラグイン)

Panorama 上のサードパーティ統合をサポートするプラグインをインストール、削除、管理する場合は、**Panorama** > **Plugins** (プラグイン) を選択します。

(VM-Series ファイアウォールでのみ利用可能)**Device** (デバイス) > **Plugins** (プラグイン)を選択し、VM-Series ファイアウォール用のプラグインをインストール、削除、管理します。

プラグイン	の意味
アップロード	ローカル ディレクトリからプラグイン インストール ファイルをアップロードできます。これは、プラグインをインストールするものではありません。インストール ファイルをアップロードすると、インストール リンクがアクティブになります。
ファイル名	プラグイン ファイル名です。 Panorama に**vm_series**プラグインをインストールすると**Device** (デバイス) > **VM-Series**ページが利用可能になり、そこでパブリック クラウド環境 (AWS、Azure、Google) にデプロイされた VM-Series ファイアウォール上のテンプレート設定を管理およびコミットできるようになります。
バージョン	プラグイン バージョン ナンバーです。
プラットフォーム	プラグインがサポートされているモデルです。
リリース日	このプラグイン バージョンのリリース日です。
サイズ	プラグイン ファイル サイズです。
インストール済み	Panorama の各プラグインの現在のインストールの状態を提示します。
操作	• **Install** (インストール) – プラグインの特定のバージョンをインストールします。新しいバージョンのプラグインをインストールすると、以前インストールしたバージョンが上書きされます。 • **Delete** (削除) – 指定されたプラグイン ファイルを削除します。 • **Remove Config** (設定の削除) – このプラグインに関連するすべての設定を削除します。 • **Uninstall** (アンインストール) – プラグインの最新インストールを削除します。Panorama からプラグイン ファイルを削除するものではありません。プラグインをアンインストールした場合、そのプラグインに関連するすべての設定が失われます。関連設定を完全に削除するときにのみ使用します。

© 2019 Palo Alto Networks, Inc.

Panorama > VMware NSX

VM-Series NSXエディションファイアウォールのプロビジョニングを自動化するには、NSX ManagerとPanorama間の通信を有効化する必要があります。PanoramaがVM-SeriesファイアウォールをNSX Manage 上のサービスとして登録すると、NSX Managerには、新しい VM-Seriesファイアウォールをクラスタ内の各ESXiホストに1つ以上のインスタンスをプロビジョニングするために必要な設定が作成されます。

知りたい内容	以下を参照
グループに通知を設定するには？	通知グループの設定
VM-Series NSXエディションファイアウォールの設定を定義するには？	サービス定義を作成する
PanoramaをNSX Managerと通信するように設定するには？	NSX Manager へのアクセスの設定
VM-Series NSX エディション ファイアウォールのステアリング ルールを定義するには？	ステアリング ルールの作成
ダイナミックvSphere環境で、ファイアウォールがポリシーを常に適用しておくよう設定するには？	Objects（オブジェクト）> Address Groups（アドレス グループ）、および Policies（ポリシー）> Security（セキュリティ）を選択します。 Panorama とファイアウォールで仮想環境の変更点を詳しく把握できるようにするには、セキュリティ ポリシーのプレ ルールの送信元および宛先アドレス オブジェクトとして動的アドレス グループを使用します。
その他の情報をお探しですか？	「Set up a VM-Series NSX Edition Firewall（VM-Series NSX エディション ファイアウォールのセットアップ）」を参照してください。

通知グループの設定

- Panorama > Notify Group（通知グループ）

以下の表では、Panorama 通知グループ設定について説明します。

通知グループ設定	の意味
氏名	通知グループの分かりやすい名前を入力します。
Notify Device（通知デバイス）	ネットワークにデプロイされた仮想マシンへの追加または変更について通知を受ける必要があるデバイス グループのボックスをオンにします。 新しい仮想マシンがプロビジョニングされたり、既存のマシンが変更されたりすると、仮想ネットワークに対する変更内容はアップデートとしてPanoramaに配信されます。このように設定された場合、Panoramaは、指定したデバイスグループ内のファイアウォールが動的アドレスグループに登録されたIPアドレスへ

© 2019 Palo Alto Networks, Inc.

通知グループ設定	の意味
	の変更を受信できるように、ポリシールールで参照している動的アドレスオブジェクトの入力と更新を行います。 通知を有効化する場合は、通知を有効化したいすべてのデバイスグループを必ず選択するようにしてください。デバイスグループを選択できない場合は（チェックボックスが表示されない）、そのデバイスグループの階層により自動的に含まれていることを意味します。 この通知プロセスによって、コンテクストが認識され、ネットワーク上のアプリケーション セキュリティが維持されます。たとえば、ハードウェアベースの境界ファイアウォールのグループがあり、新しいアプリケーションまたはWebサーバーがデプロイされた際に通知を受ける必要がある場合、このプロセスは指定されたデバイスグループについてダイナミックアドレスグループの自動更新を開始します。さらに、ダイナミック アドレス オブジェクトを参照するすべてのポリシー ルールには、新しくデプロイまたは変更されたアプリケーションまたはWeb サーバーが自動的に追加され、基準に基づいてセキュアに有効にすることができます。

サービス定義を作成する

- Panorama > VMware NSX > Service Definitions（サービス定義）

サービス定義を使用することで、NSX Manager 上に VM-Series ファイアウォールをパートナー セキュリティ サービスとして登録することができます。Panoramaで32個のサービス定義を作成し、NSX Managerに同期させることができます。

一般的に、ESXiクラスタ内のテナントごとに1つのサービス定義を作成します。それぞれのサービス定義には、ファイアウォールのデプロイに使用するOVF（PAN-OSバージョン）が指定してあり、ESXiクラスタにインストールされているVM-Seriesファイアウォールの設定内容が含まれています。設定内容を指定する場合は、サービス定義に、固有のテンプレート、固有のデバイスグループ、およびそのサービス定義を使用してデプロイされるファイアウォールのライセンス認証コードを含めておく必要があります。デプロイされたファイアウォールは、Panoramaに接続しサービス定義で指定されたデバイスグループ用の設定内容（そのファイアウォールが保護する各テナントや部門のゾーンを含む）とポリシー設定を受信します。

新しいサービス定義を追加する場合は、次の表の説明に従って設定します。

項目	の意味
氏名	NSX Managerに表示したいサービスの名前を入力します。
の意味	(任意) このサービス定義の目的または機能を説明するラベルを入力します。
デバイス グループ	これらのVM-Seriesファイアウォールを割り当てるデバイスグループまたはデバイスグループ階層を選択します。詳細は、「Panorama > VMware NSX」を参照してください。
テンプレート	VM-Seriesファイアウォールを割り当てるテンプレートを選択します。詳細は、「Panorama > Templates（テンプレート）」を参照してください。 サービス定義はそれぞれ固有のテンプレートまたはテンプレートスタックに割り当てる必要があります。

© 2019 Palo Alto Networks, Inc.

項目	の意味
	テンプレートは複数のゾーン（NSX Service Profile Zones for NSX (NSX用のNSXサービスプロファイルゾーン)）を割り当てることが可能です。シングルテナント型のデプロイについては、テンプレートにゾーン（NSX Service Profile Zone）を1つ作成します。マルチテナント型のデプロイについては、それぞれのサブテナントごとにゾーンを作成します。 新規のNSX Service Profile Zoneを作成した場合、そのゾーンはバーチャルワイヤーサブインターフェイスのペアに自動的に割り当てられます。詳細は、「Network（ネットワーク）> Zones（ゾーン）」を参照してください。
VM-Series の OVF URL	NSX Managerが、新しいVM-SeriesファイアウォールをプロビジョニングするためのOVFファイルにアクセスできるURL（IPアドレスまたはホスト名とパス) を入力します。
グループに通知	ドロップダウン リストから通知グループを選択します。

NSX Manager へのアクセスの設定

- Panorama > VMware NSX > Service Managers（サービス マネージャ）

Panorama が NSX Manager と通信できるようにするには、**Add**（追加）をクリックし、以下の表に記載されている設定を行います。

サービス マネージャ	の意味
サービス マネージャ名	VM-Series ファイアウォールをサービスとして識別するための名前を入力します。この名前は、NSX Managerに表示され、VM-Seriesファイアウォールを要求に応じてデプロイするために使用されます。 63 文字以内で指定し、英字、数字、ハイフン、およびアンダースコアのみを使用してください。
の意味	(任意) このサービスの目的または機能を説明するラベルを入力します。
NSX Manager URL	PanoramaがNSX Managerとの接続を確立するために使用するURLを指定します。
NSX Manager ログイン	NSX Manager に設定されている認証情報 (ユーザー名とパスワード) を入力します。Panoramaは、これらの認証情報を使用してNSX Managerとの認証を行います。
NSX Manager パスワード	
NSX Manager パスワードの再入力	
サービス定義	このサービス マネージャに関連するサービス定義を指定します。各サービス マネージャは 32 個までのサービス定義をサポートします。

© 2019 Palo Alto Networks, Inc.

Panorama に変更内容をコミットすると、VMware サービス マネージャのウィンドウに Panorama と NSX Manager の間の接続状態が表示されるようになります。

同期状態	の意味
ステータス	Panorama と NSX Manager 間の接続状態が表示されます。 正常な接続は登録済みとして表示されます - PanoramaとNSX Managerが同期され、VM-SeriesファイアウォールはNSX Manager上のサービスとして登録済みの状態になります。 接続が失敗した場合、以下のようなステータスが表示されます。 • **Connected Error** [接続エラー] - NSX Manager に到達できないか、NSX Manager へのネットワーク接続を確立できません。 • **Not authorized** [認証不可] - アクセス資格情報（ユーザー名/パスワード）が正しくありません。 • **Unregistered** [登録なし] - サービス、サービス マネージャ、またはサービスプロファイルが NSX Managerで使用できないか、削除されています。 • **Out of sync** [同期されていません] - Panorama に定義されている設定が、NSX Manager に定義されている設定と異なります。失敗の原因を表示する場合は**Out of sync** [同期されていません]をクリックします。例えば、NSX Managerのサービス定義のうち、Panoramaで定義された名前と同じものがある可能性があります。このエラーを修正する場合は、エラーメッセージに表示されているサービス定義名を使用して、NSX Managerのサービス定義の検証を行います。PanoramaとNSX Managerの設定内容が同期されるまで、Panoramaに新しいサービス定義を追加することはできません。
動的オブジェクトを同期	**Synchronize Dynamic Objects**[動的オブジェクトを同期] をクリックして、NSX Managerからの動的オブジェクト情報の更新を開始します。動的オブジェクトを同期することで、仮想環境の変更に関するコンテクストを維持できます。また、ポリシールール内で使用される動的アドレスグループを自動的に更新させ、アプリケーションを安全に有効化することができます。 *Panoramaでは、NSX Managerから動的に登録されたIPアドレスのみを表示できます。ファイアウォールに直接登録されたダ動的IPアドレスは表示されません。VM情報ソース（VM-Series NSXエディションファイアウォールではサポートされていません）を使用している場合、または XML APIを使用してIPアドレスをダ動的にファイアウォールに登録している場合に、動的Pアドレスの完全なリスト（Panoramaがプッシュしたものとローカルに登録されたもの）を表示する場合は、各ファイアウォールにログインする必要があります。*
NSX設定の同期化	Panorama で設定されたサービス定義を NSX Manager に同期する場合は **NSX Config-Sync**（**NSX**設定の同期化）を選択します。Panoramaで保留中のコミットがある場合、このオプションは使用できません。 同期が失敗した場合はエラーメッセージの詳細を参照し、エラーがPanoramaとNSX Managerのどちらに起因するものか確認してください。例えば、NSX Managerのルールで参照されているサービス定義をPanorama上で削除した場合、NSX Managerとの同期が失敗します。エラーメッセージに含まれている情報をもとに、エラーの原因と修正が必要な箇所（PanoramaあるいはNSX Manager）を特定します。

© 2019 Palo Alto Networks, Inc.

ステアリング ルールの作成

- Panorama > VMware NSX > Steering Rules（ステアリング ルール）

ステアリング ルールでは、クラスタのどのゲストからのどのトラフィックを VM-Series ファイアウォールに進めるのかを決めます。

項目	の意味
Auto-Generate Steering Rules（ステアリング ルールの自動生成）	次のように設定されているセキュリティ ルールに基づいて、ステアリング ルールを生成します。 • NSX サービス マネージャーで登録されている、親または子のデバイス グループに属す。 • ゾーンが、送信元および宛先と同じである（任意から任意でない）。 • ゾーンが 1 つのみである。 • 静的アドレス グループ、IP 範囲、ネットマスクがポリシーに設定されていない。 デフォルトの場合、Panorama によって生成されるステアリング ルールでは NSX サービスが設定されず、NSX トラフィック ディレクションは inout（両方向）に設定されます。ステアリング ルールが生成されたら、各ステアリング ルールを更新して、NSX トラフィック ディレクションを変更したり、NSX サービスを追加したりすることができます。ステアリング ルールを自動生成すると、Panorama では次のフィールド（Description（内容）と NSX Services（NSX サービス）を除く）に情報が自動的に入力されます。
氏名	NSX Manager に表示したいステアリング ルールの名前を入力します。ステアリング ルールを自動生成すると、各ステアリング ルールにプレフィックス「auto_」が追加され、セキュリティ ポリシー ルール名のスペースは下線（_）で置き換わります。
の意味	(任意) このサービス定義の目的または機能を説明するラベルを入力します。
NSX トラフィック ディレクション	VM-Series ファイアウォールにリダイレクトされるトラフィックの方向を指定します。 • **inout**（両方向）— 両方向のルールを NSX で作成します。送信元と宛先の間を移動する、特定タイプのトラフィックは、VM-Series ファイアウォールにリダイレクトされます。Panorama では、このトラフィック ディレクションが使用されてステアリング ルールが自動生成されます。 • **in**（受信）— 受信ルールを NSX で作成します。宛先から送信元に移動する、特定タイプのトラフィックは、VM-Series ファイアウォールにリダイレクトされます。 • **out**（発信）— 発信ルールを NSX で作成します。送信元から宛先に移動する、特定タイプのトラフィックは、VM-Series ファイアウォールにリダイレクトされます。
NSX サービス	VM-Series ファイアウォールにリダイレクトするアプリケーション（Active Directory サーバー、HTTP、DNS など）トラフィックを選択します。
デバイス グループ	ドロップダウン リストからデバイス グループを選択します。選択したデバイス グループにより、どのセキュリティ ポリシーをステアリング ルールに適用するのかが決まります。デバイス グループは、NSX サービス定義と関連付けられている必要があります。

© 2019 Palo Alto Networks, Inc.

項目	の意味
セキュリティ ポリシー:	自動生成のステアリング ルールのベースになるセキュリティ ポリシー ルール。

© 2019 Palo Alto Networks, Inc.

Panorama > Log Ingestion Profile（ログ インジェスト プロファイル）

ログイン インジェスト プロファイルを使用して、Panorama が外部ソースからログを受信できるようにします。PAN-OS 8.0.0 では、Panorama（Panorama モード）は、Syslog を使用して Traps ESM サーバーからログを取り込むことができる Syslog レシーバとして機能できます。新しい外部ログ ソースのサポートと新しい Traps ESM バージョンの更新は、コンテンツ更新でプッシュされます。

ログ インジェストを有効にするには、Panorama を Traps ESM サーバーの Syslog レシーバとして設定し、Panorama でログ インジェスト プロファイルを定義してログ コレクタ グループに割り当てる必要があります。

新しい外部 Syslog インジェスト プロファイルを追加するには、プロファイルを **Add**（追加）し、以下の表の説明に従って設定を指定します。

項目	の意味
氏名	Syslog インジェスト プロファイルの名前を入力します。最大 255 個のプロファイルを追加できます。
ソース名	ログを送信する外部ソースの名前または IP アドレスを入力します。プロファイル内に最大 4 個のソースを追加できます。
ポート	Panorama がネットワーク経由のアクセスで使用するポートを入力します。Panorama は、このポートを使用して通信やリッスンを行います。 Traps ESM に 23000 ~ 23999 の値を選択します。Panorama と ESM 間の通信を有効にするには、Traps ESM で同じポート番号を設定する必要があります。
転送	TCP、UDP または SSL を選択します。SSL を選択した場合、Panorama > Managed Collectors（管理対象コレクタ）> General（全般）で保護された Syslog 通信の着信証明書を設定する必要があります。
外部ログ タイプ	ドロップダウンからログ タイプを選択します。
バージョン	ドロップダウンからバージョンを選択します。

Monitor（監視）> External Logs（外部ログ）を使用して、Traps ESM サーバーから Panorama に取り込まれたログに関する情報を表示します。

© 2019 Palo Alto Networks, Inc.

Panorama > Log Settings [Panorama > ログ設定]

以下のログ タイプを外部サービスに転送する場合は、**Log Settings**（ログ設定）ページを使用します。

- Panorama 管理サーバー（Panorama モードの M-Series アプライアンスまたは Panorama バーチャル アプライアンス）がローカルに生成するシステム、設定、User-ID、および相関ログ。
- レガシー モードの Panorama バーチャル アプライアンスがローカルに生成、またはファイアウォールから収集するすべてのタイプのログ。

ファイアウォールがログ コレクタに送信するログに関しては、ログ コレクタの設定を完了して外部サービスへの転送を有効にします。

開始前に、外部サービス用にサーバー プロファイルを定義する必要があります（「Device（デバイス）> Server Profiles（サーバー プロファイル）> SNMP Trap（SNMP トラップ）」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> Syslog」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> Email（電子メール）」、「Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP」を参照）。次に、一致リスト プロファイルを **Add**（追加）して、以下の表に記載されているように設定します。

一致リスト プロファイル設定	の意味
氏名	一致リスト プロファイルを識別する名前を入力します（最大 31 文字）。
フィルタ	デフォルトでは、一致リスト プロファイルを追加したタイプの **All Logs**（すべてのログ）を Panorama は転送します。一部のログを転送するには、ドロップダウン リストを開いて既存のフィルタを選択するか、**Filter Builder**（フィルタ ビルダー）を選択して新しいフィルタを追加します。新しいフィルタの各クエリに対して、以下のフィールドを指定して、クエリを **Add**（追加）します。 • **Connector**（条件式）– クエリの結合ロジック（AND/OR）を選択します。ロジックに否定を適用する場合は、**Negate**（否定）を選択します。たとえば、信頼されていないゾーンからのログ転送を防ぐには、**Negate**（上記以外）を選択し、Attribute（属性）として **Zone**（ゾーン）、Operator（演算子）として **equal**（等しい）を選択して、Value（値）列に信頼されていないゾーンの名前を入力します。 • **Attribute**（属性）– ログの属性を選択します。オプションは、ログ タイプによって異なります。 • **Operator**（演算子）– 属性を適用するかどうかを決定する基準を選択します（**equal**（等しい）など）。使用できるオプションは、ログ タイプによって異なります。 • **Value**（値）– クエリが照合する属性値を指定します。 フィルタが一致するログを表示またはエクスポートするには、**View Filtered Logs**（フィルタリングされたログの表示）を選択します。このタブでは **Monitoring**（モニタリング）タブのページと同じオプションが表示されます（**Monitoring**（モニタリング）> **Logs**（ログ）> **Traffic**（トラフィック）など）。

© 2019 Palo Alto Networks, Inc.

一致リスト プロファイル設定	の意味
の意味	この一致リスト プロファイルの主旨に関する説明を最大 1,024 文字で入力します。
SNMP	ログを SNMP トラップとして転送するには、1 つ以上の SNMP トラップ サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> SNMP Trap（SNMP トラップ）」を参照）。
電子メール	ログを電子メール通知として転送するには、1 つ以上の電子メール サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> Email（電子メール）」を参照）。
Syslog	ログを Syslog メッセージとして転送するには、1 つ以上の Syslog サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> Syslog」を参照）。
HTTP	ログを HTTP 要求として転送するには、1 つ以上の HTTP サーバー プロファイルを **Add**（追加）します（「Device（デバイス）> Server Profiles（サーバー プロファイル）> HTTP」を参照）。
ビルトイン アクション	システム ログと設定ログ以外のすべてのログ タイプでアクションを設定できます。 • アクションを **Add**（追加）し、そのアクションを説明する名前を入力します。 • タグ付けする IP アドレス（**Source Address**（送信元アドレス）または **Destination Address**（宛先アドレス））を選択します。 • アクション（**Add Tag**（タグの追加）または **Remove Tag**（タグの除去））を選択します。 • このデバイスのローカル User-ID エージェントにタグを配信するか、リモート User-ID エージェントにタグを配信するかを選択します。 • **Remote device User-ID Agent**（リモート デバイス **User-ID** エージェント）にタグを配信する場合は、転送できるようにする HTTP サーバー プロファイルを選択します。 • IP 対タグの **Timeout** (タイムアウト)を指定すれば、IP アドレス対タグのマッピングを保持する期間（分）を設定できます。タイムアウトを 0 にすると、IP 対タグのマッピングがタイムアウトしなくなります（範囲は 0～43200（30 日）、デフォルトは 0）。 タイムアウトを設定できるのは*Add Tag* (タグの追加)アクションだけです。 • ターゲットの送信元または宛先 IP アドレスに対して適用または削除する **Tags**（タグ）を入力または指定します。相関ログと HIP マッチ ログでは送信元 IP アドレスのみタグ付けできます。

© 2019 Palo Alto Networks, Inc.

Panorama > Scheduled Config Export [Panorama > スケジュール設定された設定のエクスポート]

Panorama およびファイアウォールで実行中のすべての設定のエクスポートをスケジュール設定する場合、エクスポート タスクを **Add**（追加）して、以下の表に記載されているように設定します。

Panorama で高可用性（*HA*）が設定されている場合は、各ピアで以下の手順を実行して、フェイルオーバー後もスケジュール設定されたエクスポートが継続して実行されるようにする必要があります。*Panorama* は、スケジュール設定されたエクスポートを *HA* ピア間で同期しません。

スケジュール設定された設定のエクスポート設定	の意味
氏名	設定のエクスポート ジョブを識別する名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、ハイフン、およびアンダースコアのみを使用してください。
の意味	任意の説明を入力します。
Enable [有効化]	エクスポート ジョブを有効にする場合に選択します。
エクスポートの開始予定時刻 (毎日)	エクスポートを開始する時間を指定します (24 時間形式、HH:MM 形式)。
PROTOCOL	Panoramaからリモートホストへのログのエクスポートに使用するプロトコルを選択します。セキュアコピー（**SCP**）は保護されたプロトコルである一方、**FTP**は保護されていません。
ホスト名	宛先のSCPまたはFTPサーバーの、IPアドレスまたはホスト名を入力してください
ポート	ファイル転送先 FTP サーバーのポート番号を入力します。
path	宛先サーバー上の、エクスポートした設定を保存するフォルダやディレクトリへのパスを指定します。 例えば、設定バンドルが、Panoramaというトップフォルダの中のexported_configというフォルダに保存されている場合、各サーバータイプ用の構文は以下のようになります。 • SCPサーバー://Panorama/exported_config • FTPサーバー://Panorama/exported_config 以下の文字: **.**(ピリオド)、 **+**、 **{** および **}**、 **/**、 **-**、 **_**、 **0-9**、 **a-z**、および **A-Z**。このファイル**Path** (パス)ではスペースはサポートされていません。

© 2019 Palo Alto Networks, Inc.

スケジュール設定された設定のエクスポート設定	の意味
FTP パッシブモードの有効化	FTP パッシブ モードを使用する場合に選択します。
username	送信先での認証に必要なユーザー名を指定します。
パスワード/再入力 パスワード	送信先での認証に必要なパスワードを指定します。 最長 15 文字のパスワードを使用します。ファイアウォールは SCP サーバーに接続しようと試みる際にパスワードを復号化し、復号化されたパスワードは 63 文字以下でなければならないため、パスワードが 15 文字を超えるとテスト SCP 接続にエラーが表示されます。
SCP サーバー接続のテスト	Panorama と SCP ホスト/サーバー間の通信をテストする場合に選択します。 データの安全な転送を有効にするには、SCP サーバーのホスト キーを確認して受け入れる必要があります。ホスト キーを受け入れるまで、接続は確立されません。Panorama で HA が設定されている場合は、各 HA ピアでこの検証を実行し、それぞれが SCP サーバーのホスト キーを受け入れるようにする必要があります。

© 2019 Palo Alto Networks, Inc.

Panorama > Software [Panorama > ソフトウェア]

このページでPanorama管理サーバーにあるPanoramaソフトウェアアップデートを管理します。

- Panorama ソフトウェア更新の管理
- Panorama ソフトウェア更新情報の表示

Panorama ソフトウェア更新の管理

次の表で説明するタスクを実行するには、**Panorama** > **Software**（ソフトウェア）を選択します。

デフォルトでは、ソフトウェアのアップデートが*Panorama*管理サーバーに最大*2*個保存されます。新しいアップデート用の空き領域を確保するために、サーバーは最も古いアップデートを自動的に削除します。Panorama によって保存されるソフトウェア イメージの数を変更して、イメージを手動で削除し、空き領域を確保できます。

バージョンの互換性についてはPanorama用コンテンツとソフトウェアのアップデートをインストールを参照してください。

タスク	の意味
今すぐチェック	Panorama がインターネットに接続されている場合は、**Check Now**（今すぐチェック）をクリックして、最新のアップデート情報を表示することができます（「Panorama ソフトウェア更新情報の表示」を参照してください）。 Panoramaが外部ネットワークに接続されていない場合は、インターネットブラウザを使用してソフトウェアアップデートのサイトから更新情報にアクセスしてください。
アップロード	Panorama がインターネットに接続されていない状態でソフトウェア イメージをアップロードする場合に、インターネット ブラウザを使用してソフトウェア アップデートのサイトにアクセスして必要なリリースを見つけ、Panorama がアクセス可能なコンピューターへソフトウェア イメージをダウンロードする場合は、**Panorama** > **Software**（ソフトウェア）を選択して **Upload**（アップロード）をクリックし、**Browse**（参照）からソフトウェア イメージを選択して **OK** をクリックします。アップロードが完了すると、Available（使用可能）の列に `Uploaded`（アップロード済み）と表示されます。
ダウンロード	Panorama がインターネットに接続されている場合は、必要なリリースを **Download**（ダウンロード）（Action（操作）列）します。ダウンロードが完了すると、使用可能な列に「ダウンロード済み」と表示されます。
インストール	ソフトウェア イメージを **Install**（インストール）（Action（操作）列）します。インストールが完了するとPanorama再起動の際に一度ログアウトが行われます。 *Panorama* システム ファイルの破損を回避するため、*Panorama* では定期的にファイル システムの整合性チェック *(FSCK)* が実行されます。このチェックは、再起動を *8* 回行った後、または前回の*FSCK*から *90* 日経過した後の再起動で実行されます。*FSCK*が進行中であり完了するまでログインできない場合は、*Web*インターフェイスと*SSH*ログイン画面に警告が表示されます。この処理が終了する時間は、ストレージシステ

© 2019 Palo Alto Networks, Inc.

タスク	の意味
	ムのサイズによって異なり、大きなシステムの場合は*Panorama*にログインできるようになるまで数時間かかることもあります。進捗状況を表示するには、*Panorama* へのコンソール アクセスをセットアップします。
リリース ノート	Panorama がインターネットに接続されている場合は、目的のソフトウェア リリースの **Release Notes** (リリース ノート) にアクセスし、リリースの変更、修正、既知の問題、互換性の問題、およびデフォルト動作の変更を確認できます。 Panoramaがインターネットに接続されていない場合は、インターネットブラウザを使用してソフトウェアアップデートのサイトにアクセスし、必要なリリースをダウンロードしてください。
☒	不要になった場合や他のイメージ用に空き容量を確保したい場合に、ソフトウェアイメージを削除することができます。

Panorama ソフトウェア更新情報の表示

Panorama > **Software** (ソフトウェア) を選択し、以下の情報を表示します。Palo Alto Networksの最新情報を表示する場合は**Check Now**[今すぐチェック]をクリックします。

ソフトウェアとコンテンツのアップデート情報	の意味
バージョン	Panoramaのソフトウェアバージョン
サイズ	ソフトウェアイメージのサイズ (メガバイト単位)
リリース日	Palo Alto Networksがアップデートを公開した日時
使用可能	イメージがインストール可能かどうかを示します
現在インストール済み	アップデートのインストールが完了するとチェックマークが表示されます。
操作	イメージに対して実行可能な操作 (**Download**[ダウンロード]、**Install**[インストール]、**Reinstall**[再インストール]) を示します。
リリース ノート	**Release Notes**[リリースノート]をクリックして目的のソフトウェアリリースのリリースノートを参照し、リリースの変更、修正、既知の問題、互換性の問題、およびデフォルト動作の変更を確認します。
☒	不要になった場合やダウンロード/アップロード用に空き容量を確保したい場合に、アップデートを削除することができます。

© 2019 Palo Alto Networks, Inc.

Panorama > Device Deployment [Panorama > デバイスのデプロイ]

Panorama を使用して、ソフトウェアおよびコンテンツ更新を複数のファイアウォールやログ コレクタにデプロイしたり、ファイアウォール ライセンスを管理したりできます。

確認すべき情報	以下を参照
ソフトウェアおよびコンテンツ更新をファイアウォールやログ コレクタにデプロイする。	ソフトウェアおよびコンテンツ更新の管理
インストール済みのソフトウェアおよびコンテンツ更新や、ダウンロードとインストールが可能なソフトウェアおよびコンテンツ更新を確認する。	ソフトウェアおよびコンテンツ更新情報の表示
ファイアウォールやログコレクタの自動アップデートのスケジュールを設定したい	コンテンツ用動的更新のスケジュール設定
1 つまたは複数のファイアウォールのコンテンツ バージョンを Panorama から元に戻します。	Panorama でコンテンツ バージョンを元に戻す
ライセンスを表示、アクティベート、ディアクティベート、更新する。 ファイアウォールライセンスの状態を確認する	ファイアウォールのライセンス管理
その他の情報をお探しですか？	ライセンスの管理と更新

ソフトウェアおよびコンテンツ更新の管理

- Panorama > Device Deployment（デバイスのデプロイ）> Software（ソフトウェア）

Panorama の次のオプションにより、ソフトウェアとコンテンツのアップデートをファイアウォールとログ コレクタにデプロイできます。

管理（*MGT*）インターフェイスのトラフィックを削減するには、更新のデプロイのために個別のインターフェイスを使用するように *Panorama* を設定します（「Panorama > Setup（セットアップ）> Interfaces（インターフェイス）」を参照）。

© 2019 Palo Alto Networks, Inc.

Panorama デバイスのデプロイのオプション	の意味
ダウンロード	インターネットに接続されているPanoramaでソフトウェアまたはコンテンツのアップデートをデプロイしたい場合は、アップデートの**Download**[ダウンロード]を行います。ダウンロードが完了すると、使用可能な列に「ダウンロード済み」と表示されます。ダウンロードが完了すると以下の操作が可能になります。 • PAN-OS/Panorama のソフトウェアやコンテンツのアップデートのインストール。 • GlobalProtect™ アプリまたは SSL VPN クライアント ソフトウェア アップデートの Activate（有効化）。
アップグレード	BrightCloud URLフィルタリングコンテンツのアップグレードが入手可能な場合は**Upgrade**[アップグレード]をクリックします。アップグレードが正常に行われたら、アップデートをファイアウォールにインストールします。
インストール	PAN-OS ソフトウェア、Panorama ソフトウェア、コンテンツ アップデートをダウンロードまたはアップロードしたら、Action（操作）列の **Install**（インストール）をクリックし、以下のように選択します。 • **Devices**[デバイス] - アップデートを適用するファイアウォールまたはログコレクタを選択します。リストが長すぎる場合はフィルタを使用します。高可用性（HA）ピアであるファイアウォールをグループ化する場合は、**Group HA Peers**[HAピアのグループ化]を選択します。HA に設定されたファイアウォールを簡単に識別できるようになります。特定のファイアウォールまたはログコレクタのみを表示する場合は、表示したいものを選択して**Filter Selected**[選択項目でフィルタ]を実行します。 • **Upload only to device**（デバイスにアップロードのみ行う）（ソフトウェアのみ）– ソフトウェアをアップロードするが、自動インストールを行いたくない場合に選択します。この場合は手動でソフトウェアをインストールする必要があります。 • **Reboot device after install**（インストール後にデバイスを再起動）（ソフトウェアのみ）– インストール プロセスで自動的にファイアウォールまたはログ コレクタを再起動する場合に選択します。再起動するまでインストールは完了しません。 • **Disable new apps in content update**（コンテンツ アップデート時に新しいアプリケーションを無効にする）（アプリケーションと脅威のみ）– 前回インストールしたアップデート内容と比較して、今回のアップデートに新しく含まれているアプリケーションを無効化する場合はこのオプションを選択します。これにより最新の脅威を防ぎながらも、ポリシーアップデートを行ったのちに、アプリケーションを有効化していくといった柔軟な対応が可能です。アプリケーションを有効化したい場合、ファイアウォールにログインして、 **Device** [デバイス] > **Dynamic Updates**[動的更新] を開き、機能の列にある**Apps** [アプリ] をクリックして新しいアプリケーションを表示し、有効化したいアプリケーションごとに**Enable/Disable** [有効化/無効化] の設定を選びます。 *Panorama* > *Managed Devices*（管理対象デバイス）を選択してファイアウォール ソフトウェアとコンテンツのアップデートをインストールするか、*Panorama* > *Managed Collectors*（管理対象コントローラ）を選択して専用ログ コレクタのソフトウェア アップデートをインストールすることもできます。
アクティベート	GlobalProtect アプリ ソフトウェアのアップデートをダウンロードまたはアップロードしたら、Action（操作）列の **Activate**（アクティベート）をクリックし、以下のようにオプションを選択します。

© 2019 Palo Alto Networks, Inc.

Panorama デバイスのデプロイのオプション	の意味
	• **Devices**[デバイス] - アップデートをアクティベートするファイアウォールを選択します。リストが長すぎる場合はフィルタを使用します。高可用性（HA）ピアであるファイアウォールをグループ化する場合は、**Group HA Peers**[HAピアのグループ化]を選択します。HA に設定されたファイアウォールを簡単に識別できるようになります。特定のファイアウォールのみを表示するには、該当のファイアウォールを選択して、**Filter Selected**[選択項目でフィルタ]を実行します。 • **Upload only to device**（デバイスにアップロードのみ行う）– PAN-OS にアップロードしたイメージを自動的にアクティベートしたくない場合に選択します。ファイアウォールにログインし、アクティベートする必要があります。
リリース ノート	**Release Notes**[リリースノート]をクリックして目的のソフトウェアリリースのリリースノートを参照し、リリースの変更、修正、既知の問題、互換性の問題、およびデフォルト動作の変更を確認します。
ドキュメント	希望のコンテンツリリースに関するリリースノートを参照したい場合は**Documentation**[ドキュメント]をクリックします。
☒	ソフトウェアやコンテンツアップデートが不要になった場合や、ダウンロード/アップロード用に空き容量を確保したい場合に、これらを削除することができます。
今すぐチェック	**Check Now**（今すぐチェック）し、ソフトウェアとコンテンツのアップデートの情報を表示します。
アップロード	Panorama がインターネットに未接続の状態でソフトウェアやコンテンツ アップデートをデプロイしたい場合は、ソフトウェア アップデートまたは動的更新のサイトからコンピュータへアップデートをダウンロードし、アップデートのタイプに対応した **Panorama** > **Device Deployment**（デバイスのデプロイ）ページを選択して、**Upload**（アップロード）をクリックし、アップデートの **Type**（タイプ）を選び（コンテンツのアップデートのみ）、アップロードされたファイルを選択し、**OK** をクリックします。タイプに基づき、以下の手順に従って更新のインストールまたはアクティベーションを行います。 • **PAN-OS or Panorama software**[PAN-OSまたはPanoramaソフトウェア] - アップロードが完了すると、Available[使用可能]の列にUploaded[アップロード済み]と表示されます。アップロードが完了したら、ソフトウェア アップデートをインストールします。 • **GlobalProtect Client or SSL VPN Client software**（**GlobalProtect** クライアントまたは **SSL VPN** クライアント ソフトウェア）– ファイルからアクティベートします。 • **Dynamic updates**（動的更新）– ファイルからインストールします。
ファイルからインストール	コンテンツ アップデートのアップロード後、**Install from File**（ファイルからインストール）をクリックしてコンテンツの **Type**（タイプ）を選択し、アップデートのファイル名を選び、さらにファイアウォールまたはログ コレクタを選択します。
ファイルからアクティベーション	GlobalProtect アプリ ソフトウェアのアップデートのアップロード後、**Activate from File**（ファイルからアクティベート）をクリックし、アップデートのファイル名を選び、ファイアウォールを選択します。
スケジュール	コンテンツ用動的更新をスケジュールする場合に選択します。

© 2019 Palo Alto Networks, Inc.

ソフトウェアおよびコンテンツ更新情報の表示

- Panorama > Device Deployment（デバイスのデプロイ）> Software（ソフトウェア）

Panorama > **Device Deployment**（デバイスのデプロイ）> **Software**（ソフトウェア）を選択し、現在インストールされている、または、ダウンロードやインストールが可能な PAN-OS ソフトウェア、**GlobalProtect** クライアント ソフトウェア、動的更新（コンテンツ）を表示します。**Dynamic Updates**[動的更新]のページでは情報がコンテンツタイプ（アンチウイルス、アプリケーションと脅威、URLフィルタリング、およびWildFire）によって整列され、最後に更新情報を確認した日時が表示されています。Palo Alto Networksのソフトウェアやコンテンツの最新情報を表示する場合は**Check Now**[今すぐチェック]をクリックします。

ソフトウェアとコンテンツのアップデート情報	
バージョン	ソフトウェアまたはコンテンツアップデートのバージョン
ファイル名	アップデートファイルの名前
プラットフォーム	アップデートが指定されたファイアウォールまたはログ コレクタ モデル。数字はハードウェア ファイアウォール モデル（たとえば、`7000` は PA-7000 シリーズ ファイアウォールを指します）を、`vm` は VM-Series ファイアウォールであることを示し、`m` は M-Series アプライアンスであることを示します。
機能	（コンテンツのみ）コンテンツバージョンに含まれている可能性があるシグネチャタイプの一覧が表示されます。
タイプ	（コンテンツのみ）ダウンロードにフルデータベースアップデートが含まれているか、増分更新が含まれているかを示します。
サイズ	アップデートファイルのサイズ
リリース日	Palo Alto Networksがアップデートを公開した日時
使用可能	（PAN-OSまたはPanoramaソフトウェアのみ）アップデートがダウンロード済みまたはアップロード済みであることを示します。
ダウンロード済み	（SSL VPNクライアントソフトウェア、GlobalProtectクライアントソフトウェア、またはコンテンツのみ）チェックマークはアップデートがダウンロード済みであることを示します。
操作	アップデートに対して実行可能な操作を示しています。ダウンロード、アップグレード、インストール、アクティベーション。
ドキュメント	（コンテンツのみ）希望するコンテンツリリースに関するリリースノートへのリンクが提供されます。
リリース ノート	（ソフトウェアのみ）希望するソフトウェアリリースに関するリリースノートへのリンクが提供されます。
☒	アップデートが不要になった場合や、ダウンロード/アップロード用に空き容量を確保したい場合に、これを削除することができます。

© 2019 Palo Alto Networks, Inc.

コンテンツ用動的更新のスケジュール設定

- Panorama > Device Deployment > Dynamic Updates [Panorama > デバイスのデプロイ > 動的更新]

更新の定期的な自動ダウンロードおよびインストールを設定する場合は、**Schedules**（スケジュール）をクリックし、**Add**（追加）を選び、以下の表に記載されているように設定します。

動的更新のスケジュール設定	
氏名	スケジュール設定するジョブを識別するための名前を入力します（最大 31 文字）。この名前は、大文字と小文字が区別され、一意でなければならず、文字、数字、ハイフン、アンダースコアのみで構成されます。
disabled	スケジュール設定したジョブを無効化する場合に選択します。
タイプ	スケジュールを設定したいコンテンツのタイプを選択します。**App**[アプリケーション]、**App and Threat**[アプリケーションと脅威]、**Antivirus**[アンチウイルス]、**WildFire**、または**URL Database**[URLデータベース]。
繰り返し	Panorama が更新サーバーにチェックインする間隔を選択します。繰り返しオプションは、更新のタイプによって異なります。
時間	**Daily**[毎日] 更新の場合、24 時間形式で **Time**[時刻] を選択します。 **Weekly**[毎週] 更新の場合、**Day**[曜日] と、24 時間形式で**Time**[時刻] を選択します。
コンテンツ更新での新しいアプリケーションの無効化	更新の **Type**（タイプ）を **App**（アプリケーション）または **App and Threat**（アプリケーションと脅威）に設定し、**Action**（アクション）を **Download and Install**（ダウンロードとインストール）に設定している場合のみ、コンテンツ更新での新しいアプリケーションを無効化できます。 前回インストールした更新にはない、新しく含まれているアプリケーションを無効化する場合に選択します。これにより最新の脅威を防ぎながらも、ポリシーアップデートを行ったのちに、アプリケーションを有効化していくといった柔軟な対応が可能です。アプリケーションを有効化する場合、ファイアウォールにログインして、 **Device**（デバイス）> **Dynamic Updates**（動的更新）を開き、Features（機能）列にある**Apps**（アプリ）をクリックして新しいアプリケーションを表示し、有効化するアプリケーションごとに**Enable/Disable**（有効化/無効化）の設定をクリックします。
操作	• **Download Only**[ダウンロードのみ] - Panoramaは定期的にアップデートをダウンロードします。ファイアウォールおよびログ コレクタには、更新を手動で「インストール」する必要があります。 • **Download and Install**[ダウンロードおよびインストール] - Panoramaは定期的にアップデートをダウンロードし、自動的にインストールを行います。
機器	**Devices**[デバイス]を選び、定期的なコンテンツアップデートを受信させるファイアウォールを選択します。
ログ コレクタ	**Log Collectors**[ログコレクタ]を選び、定期的なコンテンツアップデートを受信させる管理対象コレクタを選択します。

© 2019 Palo Alto Networks, Inc.

Panorama でコンテンツ バージョンを元に戻す

- Panorama > Device Deployment > Dynamic Updates [Panorama > デバイスのデプロイ > 動的更新]

1 つまたは複数のファイアウォールへのアプリケーション、アプリケーションと脅威、アンチウィルス、WildFire、WildFire のコンテンツアップデートを、以前にインストールした Panorama のコンテンツ バージョンから、すばやく **Revert Content**（コンテンツを元に戻す）ことができます。元に戻すコンテンツ バージョンは、現在ファイアウォールにインストールされているバージョンより古いバージョンである必要があります。コンテンツを元に戻す操作は、Panorama 8.1 を実行することで利用できます。ファイアウォール上のコンテンツは、元に戻す機能がファイアウォール上でローカルで使用可能な限り、元に戻すことができます。

項目	の意味
フィルタ	コンテンツを元に戻したいデバイスにフィルタを適用します。次のフィルタを使用できます。 • デバイス状態 • プラットフォーム • デバイスグループ • テンプレート • tags • HA 状態 • ソフトウェアのバージョン (PAN-OS) • 現在のコンテンツのバージョン
機器	元に戻すデバイスを 1 つ以上選択します。次のデバイス情報を表示します。 • デバイス名–ファイアウォールの名前です。 • 現在のバージョン–デバイスにインストールされている現在のコンテンツ バージョンです。コンテンツ バージョンがインストールされていない場合、列に 0 が表示されます。 • 以前のバージョン（コンテンツ）–PAN 8.1 以降を実行しているファイアウォールに以前にインストールされたコンテンツ バージョンです。コンテンツ バージョンが以前にインストールされていない場合、またはファイアウォールが 8.1 より前の PAN-OS バージョンを実行している場合は、列は空白になります • ソフトウェアのバージョン–デバイスにインストールされている現在の PAN-OS バージョンです。 • HA ステータス– HA ペアの場合の HA ステータスを表示します。デバイスが HA ペアにない場合、列は空白になります。
グループ HA ペア	HA ピアをグループ化するにはこのボックスにチェックを入れます。

元に戻すデバイスを選択したら、**OK** をクリックします。

© 2019 Palo Alto Networks, Inc.

ファイアウォールのライセンス管理

- Panorama > Device Deployment > Licenses [Panorama > デバイスのデプロイ > ライセンス]

Panorama > **Device Deployment**（デバイスのデプロイ）> **Licenses**（ライセンス）を開き、以下のタスクを行ってください。

- インターネットに直接接続されていないファイアウォールのライセンスを更新します。Refresh（更新）をクリックしてください。
- ファイアウォールのライセンスをアクティベートします。ファイアウォールのライセンスをアクティベートする場合、**Actibvate**（アクティベート）をクリックし、ファイアウォールを選択し、認証コードの列で Palo Alto Networks がファイアウォール用に配布した認証コードを入力します。
- VM-Series ファイアウォールにインストールされたすべてのライセンスやサブスクリプション/資格をディアクティベートします。**Deactivate VMs**（**VM**のディアクティベート）をクリックし、ファイアウォールを選択し（一覧には PAN-OS 7.0 以上のリリースを実行しているファイアウォールのみが表示されます）、次のうちいずれかをクリックします。
  - **Continue**[続行] - ライセンスをディアクティベートして、変更をライセンス サーバーに自動的に登録します。ライセンスのクレジットがアカウントに戻されて、ライセンスが再利用可能になります。
  - **Complete Manually**[手動で実行] - トークンファイルを生成します。Panorama からインターネットに直接アクセスできない場合、これを使用します。ディアクティベートの操作を完了する為には、サポートポータルにログインし、**Assets** (アセット)を選択し、**Deactivate License(s)** (ライセンスのディアクティベート)をクリックしてトークンファイルをアップロードし、**Submit** (送信)をクリックする必要があります。その後、ディアクティベート プロセスを完了します。

管理対象ファイアウォールの現在のライセンス状態を表示することもできます。ファイアウォールがインターネットに直接接続されている場合、Panorama はライセンス サーバーに毎日自動的にチェックインを行い、ライセンスの延長や更新を取得し、それらをファイアウォールにプッシュします。チェックインは午前1時から2時の間に行われるようハードコードされており、この時間を変更することはできません。

ファイアウォールのライセンス情報	
デバイス	ファイアウォール名
仮想システム(vsys)	ファイアウォールが複数の仮想システムをサポートする かしない かを示します。
脅威防御	ライセンスが有効 、無効 、または期限切れ（有効期限日も表示されます）であることを示します。
URLプロテクションの	
support	
GlobalProtectゲートウェイ	
GlobalProtectポータル	
WildFire	
VM-Series 容量	これがVM-Seriesファイアウォールであるか、 否か を示します。