paloalto TECHDOCS

VM-Series デプロイメント ガイド

Version 10.1



docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

© 2021-2021 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 3, 2021

Table of Contents

VM-Series ファイアウォールについて 15

VM-Series デプロイメント 16
VM-Series の高可用性 18
VM-Series ファイアウォールのアップグレード 20
PAN-OS ソフトウェア バージョンのアップグレード（スタンドアロン版） 20
PAN-OS ソフトウェア バージョンのアップグレード（HA ペア） 23
Panorama を使った PAN-OS ソフトウェア バージョンのアップグレード 29
PAN-OS ソフトウェア バージョンのアップグレード（VM-Series for NSX） 34
VM-Series モデルのアップグレード 39
HA ペアの VM-Series モデルのアップグレード 41
VM-Series ファイアウォールの以前のリリースへのダウングレード 42
VM-Series プラグイン 44
ファイアウォールでの VM-Series プラグインの設定 44
VM-Series プラグインのアップグレード 45
VM-Series ファイアウォールでのジャンボフレームの有効化 48
ハイパーバイザーによって割り当てられた MAC アドレス 50
監視用に公開されるカスタム PAN-OS メトリック 52
VM-Series ファイアウォール上の外部サービスへのアクセスに使用されるインターフェイス 54
PacketMMAPおよびDPDK配信サポート 55
VM-Series での NUMA パフォーマンス最適化の有効化 57
VM-Series ファイアウォールでの ZRAM の有効化 59

VM-Series ファイアウォールのライセンス 61

VM-Series ファイアウォールライセンス 62
ライセンスタイプ 62
フレキシブル vCPU と固定モデルライセンス 63
フレキシブル vCPU と固定モデルのデプロイメント 66
サポート アカウントの作成 67
VM-Series ファイアウォールのシリアル番号と CPU ID フォーマット 68
ライセンス API 69
ライセンス API キーの管理 70
ライセンス API の使用 70
ライセンス API のエラーコード 74

©2023 Palo Alto Networks, Inc.

ライセンス API キーのインストール....75
Panorama ベースのソフトウェアファイアウォールライセンス管理の使用....76
Software NGFW Credits....81
メモリに基づく最大制限....83
クレジットのアクティベート....93
デプロイメントプロファイルの作成....94
デプロイメントプロファイルの管理....96
VM-Series ファイアウォールの登録 (Software NGFW Credit)....97
Panorama のプロビジョニング....100
クレジットの転送....101
ライセンスの非アクティブ化 (Software NGFW Credit)....102
データプレーンコアのカスタマイズ....104
フレキシブル VM-Series ライセンスへの移行....105
VM-Series モデル....110
VM-Series のシステム要件....111
CPU オーバーサブスクリプション....113
VM-50 Lite モード....114
VM-Series モデルのライセンスタイプ....115
VM-Series モデルライセンスのアクティベート....127
VM-Series ファイアウォールの登録....134
VM-Seriesファイアウォールへのデバイス証明書のインストール....137
BYOL ライセンスと PAYG ライセンスの切り替え....141
固定モデル ライセンス間の切り替え....142
ライセンスの非アクティブ化....145
VM-Series ファイアウォールのライセンス バンドルを更新....152
クラウド セキュリティ サービス プロバイダー（CSSP）用ライセンス....154
CSSP ライセンス パッケージの認証コードの取得....154
CSSP 認証コードを使用した VM-Series ファイアウォールの登録....155
登録した VM-Series ファイアウォールに関する顧客情報を追加....156
ESXi サーバーでの VM-Series ファイアウォールのセットアップ....161
VMware vSphere Hypervisor（ESXi）でサポートされているデプロイ....162
ESXi システム上の VM-Series — 要件と制限....163
ESXi システム上の VM-Series — 要件....163
ESXi システム上の VM-Series — 制限....164
VMware vSphere Hypervisor（ESXi）への VM-Series ファイアウォールのインストール....166
VM-Series for ESXi で使用するインターフェイスのプランニング....166

©2023 Palo Alto Networks, Inc.

ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング.....168
ESXi 上の VM-Series の初期設定の実行.....171
VM-Series ファイアウォールにディスクスペースを追加する.....173
ESXi および vCloud Air 上の VM-Series ファイアウォールでの VMware ツールの使用.....174
ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用.....176
ESXi 上での VM-Series CLI を使用した管理インターフェースのスワップ.....177
vCenter 上の VM 監視.....179
VMware vCenter での VM モニタリングについて.....179
VMware vCenter 用 Panorama プラグインのインストール.....180
VMware vCenter 用 Panorama プラグインの設定.....181
ESXi のデプロイメントのトラブルシューティング.....185
基本的なトラブルシューティング.....185
インストールの問題.....185
ライセンスの問題.....187
接続の問題.....188
VM-Series for ESXi のパフォーマンス調整.....190
ESXi 上の NIC ドライバのインストール.....190
ESXi 上の DPDK の有効化.....192
ESXi 上の SR-IOV の有効化.....192
SR-IOV による ESXi VLAN アクセスモードの有効化.....192
ESXi 上の NIC のマルチキュー サポートの有効化.....194
パフォーマンスのためのVNFチューニング.....194

vCloud Air での VM-Series ファイアウォールのセットアップ..... 209

vCloud Air における VM-Series ファイアウォールについて.....210
vCloud Air でサポートされるデプロイメント.....211
vCloud Air での VM-Series ファイアウォールのデプロイ.....212

VMware NSX-T での VM-Series ファイアウォールのセットアップ.....221

VMware NSX-T（North-South）での VM-Series ファイアウォールのセットアップ.....222
VMware NSX-T（North-South）でサポートされている VM-Series ファイアウォールのデプロイメント.....222
NSX-T（North-South）の VM-Series ファイアウォールのセキュリティ ポリシー コンポーネント.....223
NSX-T（North-South）での VM-Series ファイアウォールのデプロイ.....224

©2023 Palo Alto Networks, Inc.

NSX-VからNSX-Tへのセキュリティ ポリシーの拡張 238
NSX-T（East-West）での VM-Series ファイアウォールのセットアップ 241
NSX-T（East-West）での VM-Series ファイアウォールのコンポーネント 241
NSX-T（East-West）での VM-Series ファイアウォール統合 243
VMware NSX-T（East-West）でサポートされている VM-Series ファイアウォールのデプロイメント 245
業務中心のワークフローを使用した VM-Series のデプロイ 246
セキュリティ中心のワークフローを使用した VM-Series のデプロイ 265
Panorama からのサービス定義の削除 298
NSX-T 運用上の VM-Series からのセキュリティ中心デプロイメントへの移行 298
NSX-VからNSX-Tへのセキュリティ ポリシーの拡張 305
NSX-VからNSX-TにVM-Seriesを移動するための定位置移行の使用 307
AWS での VM-Series ファイアウォールのセットアップ 315
AWS での VM-Series ファイアウォールについて 316
AWS EC2 インスタンス タイプ 316
AWS GovCloud における VM-Series ファイアウォール 317
AWS China における VM-Series ファイアウォール 317
AWS Outposts での VM-Series ファイアウォール 317
AWS の用語 318
Amazon ELB で使用する管理インターフェイスのマッピング 321
AWS での VM-Series ファイアウォールのパフォーマンスチューニング 323
AWS でサポートされるデプロイメント 325
AWS での VM-Series ファイアウォールのデプロイ 328
AMI の取得 328
AWS VPC での VM-Series 用プランニングワークシート 334
AWS での VM-Series ファイアウォールの起動 336
AWS Outposts での VM-Series ファイアウォールの起動 345
カスタム Amazon Machine Image（AMI）の作成 354
AWS 上の VM-Series ファイアウォールの EBS ボリュームの暗号化 357
VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ 359
VM-Series ファイアウォールでの CloudWatch モニタリングの有効化 360
VM-SeriesとAWS Gateway Load Balancerの統合 365
VM-SeriesとGateway Load Balancerの手動統合 367
VM-SeriesとAWS Gateway Load Balancerのオートスケーリング 382
AWS における VM-Series ファイアウォールの高可用性設定 399
AWS における HA の概要 399

 ©2023 Palo Alto Networks, Inc.

HA 用の IAM ロール 401
HA リンク 404
ハートビートポーリングおよび Hello メッセージ 405
デバイス優先度およびプリエンプション 405
HA タイマー 405
セカンダリIPを使用したAWS上でのアクティブ/パッシブHA設定 406
インターフェイス移動を使用したAWS上でのアクティブ/パッシブHA設定 413
アクティブ/パッシブ HAをAWSに移行する 417
「ユース ケース：AWS クラウドで EC2 インスタンスを保護する 424
「ユース ケース：ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する 440
ユース ケース：AWS の GlobalProtect ゲートウェイとしての VM-Series ファイアウォール 444
GlobalProtect インフラストラクチャのコンポーネント 445
AWS への GlobalProtect ゲートウェイのデプロイ 445
AWS でのリソースモニタリング 447
Panorama でのAWS プラグインを使った AWS リソースモニタリング 447
Panorama 上の VM モニタリング用 AWS プラグインをセットアップ 447
Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング 461
AWS バージョン 2.0 用 VM-Series Auto Scale テンプレート 463
AWS バージョン 2.1 用 VM-Series オート スケーリングテンプレート 501
AWS-VPC でモニターされる属性の一覧 532
AWS VPCをモニタリングする際に必要な IAM の許可 534

KVM での VM-Series ファイアウォールのセットアップ 535

KVM 上の VM-Series — 要件と前提条件 536
ネットワーク上の VM-Series に接続するためのオプション 538
KVM 上の VM-Series の前提条件 538
KVM でサポートされているデプロイ 544
単一ホストでのトラフィックの保護 544
複数の Linux ホストでのトラフィックの保護 544
KVM への VM-Series ファイアウォールのインストール 546
Virt-Manager を使用した VM-Series ファイアウォールのインストール 546
ISO を使用した VM-Series ファイアウォールのインストール 554
KVM 上での VM-Series CLI を使用した管理インターフェースのスワップ 556
SCSI コントローラの使用の有効化 557

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールでのネットワーク インターフェイスの順序を決定する PCI-ID の確認 558
VM-Series for KVM のパフォーマンス調整 560
Ubuntu 16.04.1 LTS への KVM および Open vSwitch のインストール 560
KVM での Open vSwitch の有効化 561
Open vSwitch と DPDK の統合 561
KVM 上の SR-IOV の有効化 566
SR-IOV による VLAN アクセスモードの有効化 567
KVM 上の NIC のマルチキュー サポートの有効化 568
KVM 上の NUMA ノードへの CPU リソースの分離 569
Intelligent Traffic Offload インテリジェント トラフィック オフロード 571
インテリジェントトラフィックオフロードの要件 572
インテリジェントトラフィックオフロードインターフェース 573
高可用性（HA） 574
BlueField-2 DPU のインストール 576
VM-Series ファイアウォールのインストール 577
仮想関数の有効化 577
BlueField-2 DPU システムの確認 578
BlueField ブートストリームソフトウェアのインストールまたはアップグレード 580
Debian パッケージのインストールまたはアップグレード 581
インテリジェントトラフィックオフロードの実行 582
BlueField-2 DPU のトラブルシューティング 584
PAN-OS のトラブルシューティング 584
参考資料 587

Hyper-V 上での VM-Series ファイアウォールのセットアップ 589

サポートされている Hyper-V のデプロイ 590
単一 Hyper-V ホストのトラフィックの保護 590
複数 Hyper-V ホスト全体のトラフィックの保護 590
Hyper-V のシステム要件 592
Linux 統合サービス 593
Hyper-V 上での VM-Series ファイアウォールのインストール 594
開始する前に 594
Hyper-V 上での VM-Series ファイアウォールのパフォーマンス調整 595
Hyper-V Manager を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング 596
PowerShell を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング 598
VM-Series ファイアウォールの初期設定 599

©2023 Palo Alto Networks, Inc.

Azure での VM-Series ファイアウォールのセットアップ..... 603
Azure における VM-Series ファイアウォールについて..... 604
Azure ネットワークと VM-Series ファイアウォール..... 604
Azure セキュリティ センターの統合..... 605
Azure における VM-Series ファイアウォールのテンプレート..... 607
Azure における VM-Series の最小システム要件..... 609
Azure における VM-Series の高可用性のサポート..... 609
Azure 上の VM-Series のサービス プリンシパル アクセス許可..... 609
Azure でサポートされるデプロイメント..... 613
Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）..... 614
Azure China マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）..... 625
AzureでのPanoramaが統制するデプロイメント..... 632
統制デプロイ環境の準備..... 634
AzureでのVM-Seriesファイアウォールデプロイ環境の統制..... 638
Azure用のカスタムVM-Seriesイメージの作成..... 648
Azure Security Center の推奨事項を使用してワークロードを保護..... 650
Azure Security Center の推奨事項に基づいて VM-Series ファイアウォールをデプロイ..... 650
Azure Security Center から既存の VM-Series ファイアウォールを接続..... 652
Panorama を使用して Azure Security Center にログを転送..... 654
Azure Stack 上に VM-Series ファイアウォールをデプロイ..... 657
VM-Series ファイアウォールでの Azure Application Insights の有効化..... 661
Azureでのモニタリング..... 664
Azure 上のモニタリングについて..... 664
Panorama上のモニタリング用Azureプラグインのセットアップ..... 664
Azure 上で Panorama プラグインを使用して監視される属性..... 672
Azure でのアクティブ/パッシブ HA のセットアップ..... 675
Azure でのアクティブ/パッシブ HA のセットアップ（North-South & East-West トラフィック）..... 676
Azure でのアクティブ/パッシブ HA のセットアップ（East-West トラフィックのみ）..... 690
ARM テンプレートを使用した VM-Series ファイアウォールのデプロイ..... 703
VM-Series and Azure Application Gateway テンプレートのデプロイ..... 707
VM-Series and Azure Application Gateway テンプレート..... 708
VM-Series および Azure Application Gateway テンプレートの使用開始..... 709
Azure での Kubernetes サービスの保護..... 719
Azure Secure Kubernetes Services 用 Panorama プラグインの仕組み..... 719

©2023 Palo Alto Networks, Inc.

AKS クラスタの保護 724

OpenStack での VM-Series ファイアウォールのセットアップ 737

OpenStack での VM-Series のデプロイ 738
基本的なゲートウェイ 738
サービス チェーニングおよびサービス スケーリング 738
VM-Series for OpenStack Solution ソリューションのコンポーネント 740
基本的なゲートウェイ デプロイメント用の Heat テンプレート 742
サービス チェーニングおよびサービス スケーリングでの Heat テンプレートの使用 745
仮想ネットワーク 746
仮想マシン 746
サービス テンプレート 747
サービス インスタンス 748
IPAM 748
サービス ポリシー 749
アラーム 750
基本的なゲートウェイ デプロイメントでの VM-Series ファイアウォールのインストール 752
サービス チェーニングまたはスケーリング用 Heat テンプレートを使用した VM-Series ファイアウォールのインストール 756

Google Cloud Platform 上の VM-Series ファイアウォールのセットアップ 761

>Google Cloud Platform 上の VM-Series ファイアウォールについて 762
>Google Cloud Platform と VM-Series のファイアウォール 762
>VM-Series ファイアウォールの最小システム要件 762
Google Cloud Platform でサポートされているデプロイメント 764
インターネット ゲートウェイ 764
セグメンテーション ゲートウェイ 765
ハイブリッド IPSec VPN 765
Google Public Cloud 上で VM-Series のファイアウォールを設定する準備をする 767
一般的な要件 767
Panorama への VM-Series プラグインのインストール 768
Panorama Plugin for GCPのインストール 769
GCP Marketplaceからのデプロイ準備 769
Google Cloud PlatformへのVM-Seriesファイアウォールのデプロイ 777
Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする 777

©2023 Palo Alto Networks, Inc.

Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ....782
VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ....784
VM-Series ファイアウォールでの Google Stackdriver モニタリングの有効化....785
VM を監視して Google Cloud Platform（GCP）上の VM の変更を追跡する....788
ダイナミックアドレスグループを使用してVPC内のインスタンスを保護する....791
カスタム テンプレートあるいは gcloud CLI を使用して VM-Series ファイアウォールをデプロイ....793
Panorama Plugin for GCPによるVMモニタリング....795
GCP向けPanorama Pluginによる VMモニタリングの設定....795
Google Cloud Platform 上の VM-Series ファイアウォールのオートスケーリング....803
Google Cloud Platform用のオートスケーリングコンポーネント....803
GCPオート スケーリングテンプレートのデプロイ....815
Cisco ENCS ネットワークでの VM-Series ファイアウォールのセットアップ....849
Cisco ENCS デプロイメントの計画....850
Cisco ENCS 用 VM-Series ファイアウォール イメージの準備....852
グラフィカル ユーザー インターフェイスでの qcow2 ファイルの変換....852
コマンド ライン インターフェイスでの qcow2 ファイルの変換....855
Cisco ENCS での VM-Series ファイアウォールのデプロイ....859
Oracle Cloud Infrastructure での VM-Series ファイアウォールのセットアップ....863
OCI シェイプのタイプ....864
OCI でサポートされるデプロイメント....865
OCI への VM-Series ファイアウォールのセットアップ準備....866
Oracle Cloud Marketplace からの VM-Series ファイアウォールのデプロイ....870
OCI でのアクティブ/パッシブ HA の設定....876
Alibaba Cloud での VM-Series ファイアウォールのセットアップ....887
Alibaba Cloud での VM-Series ファイアウォール....888
Alibaba Cloud での VM-Series ファイアウォールの最小システム要件....890
VM-Series ファイアウォールのソフトウェア要件....890

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールで推奨される Alibaba Cloud インスタンス タイプ....890
Alibaba Cloud CLI....891
Alibaba Cloud での VM-Series ファイアウォールのデプロイの準備....892
ライセンスの選択とネットワークの計画....892
Aliyun コマンド ライン インターフェイスを使用するための準備....893
Alibaba Cloud での VM-Series ファイアウォールのデプロイ....894
VPC の作成とネットワークの設定....894
VM-Series ファイアウォールの作成と設定....898
Alibaba Cloud での North-South トラフィックの保護....902
Alibaba Cloud での負荷分散の設定....906

Cisco ACI でのファイアウォールのセットアップ....909

Palo Alto Networks ファイアウォールと Cisco ACI の統合....910
サービス グラフ テンプレート....911
マルチコンテキスト デプロイメント....912
統合のための ACI 環境の準備....913
ネットワーク ポリシー モードでのファイアウォールと Cisco ACI の統合....914
ネットワーク ポリシー モードで East-West トラフィックを保護するファイアウォールのデプロイ....914
ネットワーク ポリシー モードで North-South トラフィックを保護するファイアウォールのデプロイ....932
Cisco ACI でのエンドポイント モニタリング....951
Cisco ACI 用 Panorama プラグインのインストール....952
Cisco ACI プラグインの設定....953
Cisco ACI Dashboard 用 Panorama プラグイン....957

Cisco CSP での VM-Series ファイアウォールのセットアップ....963

Cisco CSP での VM-Series のシステム要件....964
Cisco CSP での VM-Series ファイアウォールのデプロイ....965

Cisco TrustSec のエンドポイント監視....967

Cisco TrustSec 用 Panorama プラグイン....968
一括同期....968
PubSub....969
Cisco TrustSec 用 Panorama プラグインのインストール....970
Cisco TrustSec 用 Panorama プラグインの設定....971
Cisco TrustSec用Panoramaプラグインのトラブルシューティング....980
プラグインのステータスコマンド....980
コマンドのデバッグ....980

©2023 Palo Alto Networks, Inc.

ログのデバッグ....981

Nutanix AHVでのVM-Seriesファイアウォールのセットアップ..... 983

Nutanix での VM モニタリング....984
Nutanix 上の VM モニタリングについて....984
Nutanix 用 Panorama プラグインのインストール....985
Nutanix 用 Panorama プラグインの設定....985

VM-Series ファイアウォールのブートストラップ..... 991

ブートストラップ方法の選択....992
基本設定....993
完全設定....997
VM-Series ファイアウォールのブートストラップ ワークフロー....998
ブートストラップ パッケージ....1000
ブートストラップ パッケージの構造....1000
ブートストラップパッケージの配信....1001
ブートストラップ設定ファイル....1002
init-cfg.txt....1002
bootstrap.xml....1002
Panorama で VM 認証キーを生成....1004
init-cfg.txt ファイルの作成....1006
Init-cfg.txt ファイルのコンポーネント....1007
Init-cfg.txt のサンプル ファイル....1011
Bootstrap.xml ファイルの作成....1014
ブートストラップ用ライセンスの準備....1015
ブートストラップ パッケージの準備....1017
AWS 上での VM-Series ファイアウォールのブートストラップ....1019
Azure 上の VM-Series ファイアウォールのブートストラップ....1023
ESXi における VM-Series ファイアウォールのブートストラップ....1026
ISO を使用した ESXi における VM-Series ファイアウォールのブートストラップ....1026
Block Storage デバイスを使用した ESXi における VM-Series ファイアウォールのブートストラップ....1027
Google Cloud Platform 上の VM-Series ファイアウォールのブートストラップ.. 1029
Hyper-V における VM-Series ファイアウォールのブートストラップ....1031
ISO を使用した Hyper-V での VM-Series ファイアウォールのブート処理....1031
Block Storage デバイスを使用した Hyper-V における VM-Series ファイアウォールのブートストラップ....1032
KVM 上での VM-Series ファイアウォールのブートストラップ....1035

©2023 Palo Alto Networks, Inc.

ISO を使用した KVM における VM-Series ファイアウォールのブートストラップ....1035
Block Storage デバイスを使用した KVM における VM-Series ファイアウォールのブートストラップ....1036
ブートストラップの結果を検証....1038
ブートストラップのエラー....1039

 ©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールについて

Palo Alto NetworksのVM-Series ファイアウォールは、Palo Alto Networks の仮想マシン形式の次世代ファイアウォールです。仮想化環境やクラウド環境で使用するファイアウォールとして位置付けられており、East-West および North-South トラフィックを保護して安全性を確保することができます。

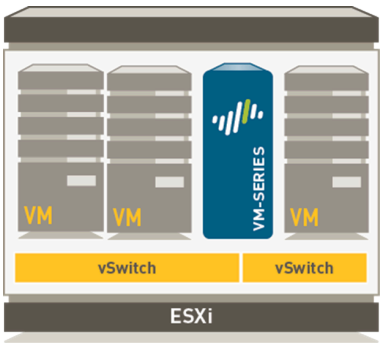
- VM-Series デプロイメント
- VM-Series の高可用性
- VM-Series ファイアウォールのアップグレード
- VM-Series プラグイン
- VM-Series ファイアウォールでのジャンボフレームの有効化
- ハイパーバイザによって割り当てられた MAC アドレス
- 監視用に公開されるカスタム PAN-OS メトリック
- VM-Series ファイアウォール上の外部サービスへのアクセスに使用されるインターフェイス
- PacketMMAPおよびDPDK配信サポート
- VM-Series での NUMA パフォーマンス最適化の有効化
- VM-Series ファイアウォールでの ZRAM の有効化

VM-Series デプロイメント

VM-Series ファイアウォールは、以下のプラットフォームにデプロイできます。

- **VMware vSphere Hypervisor（ESXi）用 VM-SeriesとvCloud Air**

  どの VM-Series モデルも、VMware ESXi にゲスト仮想マシンとしてデプロイできます。仮想フォーム ファクタが必要なクラウドまたはネットワークに最適です。



  詳細は、「ESXi サーバーでの VM-Series ファイアウォールのセットアップ」および「vCloud Air での VM-Series ファイアウォールのセットアップ」を参照してください。

- **VMware NSX-T 上の VM-Series**

  NSX-T 環境内に、VM-100、VM-300、VM-500、または VM-700 をデプロイすることができます。

  詳細は、「VMware NSX-T（North-South）での VM-Series ファイアウォールのセットアップ」を参照してください。

- **Amazon Web Services（AWS）の VM-Series**

  VM-50 を除くすべての VM-Series モデルを AWS クラウドの EC2 インスタンスにデプロイできます。

  詳細は、「AWS での VM-Series ファイアウォールのセットアップ」を参照してください。

- **Google Cloud Platform 用 VM-Series**

  Google Compute Engine インスタンス上の VM-50 および VM-50 を除くすべての VM-Series モデルを AWS クラウドの VM-50 インスタンスにデプロイできます。詳細は、「Google Cloud Platform 上の VM-Series ファイアウォールのセットアップ」を参照してください。

- **Kernel Virtualization Module（KVM）用の VM-Series**

  どの VM-Series モデルも、KVM ハイパーバイザを実行している Linux サーバー上にデプロイできます。詳細は、「KVM での VM-Series ファイアウォールのセットアップ」を参照してください。

- **VM-Series for Microsoft Hyper-V**

  どの VM-Series モデルも、Hyper-V ロールのアドオンを有効にして、あるいはスタンドアロンの Hyper-V 2012 R2 サーバーとともに Windows Server 2012 R2 サーバーにデプロイできます。詳細は、「Hyper-V 上で VM-Series ファイアウォールをセットアップ」を参照してください。

©2023 Palo Alto Networks, Inc.

- **VM-Series for Microsoft Azure**

  VM-50 を除くすべての VM-Series モデルを Azure VNet にデプロイできます。

  詳細は、「Azure の VM-Series ファイアウォールのセットアップ」を参照してください。

©2023 Palo Alto Networks, Inc.

VM-Series の高可用性

高可用性（HA）とは、ネットワーク上の単一障害点を回避するために、2 つのファイアウォールを 1 つのグループに配置して、この 2 つの設定を同期させる設定です。ファイアウォール ピア間のハートビート接続では、ピアがダウンした場合シームレスにフェイルオーバーを実行できます。2 つのデバイス クラスターでファイアウォールを設定すると冗長性が得られるため、ビジネス継続性を確保できます。VM-SeriesファイアウォールでHAを構成する場合、両方のピアを同じタイプのハイパーバイザ上に配置し、同一のハードウェアリソース（CPUコアやネットワークインターフェイスなど）を割り当て、同様のライセンスやサブスクリプション一式を付与する必要があります。Palo Alto Networks ファイアウォールによる HA に関する一般的な情報については、「高可用性」を参照してください。

VM-Seriesファイアウォールでは、セッション同期および設定同期機能で、ステートフルアクティブ/パッシブまたはアクティブ/アクティブ高可用性をサポートします。アクティブ/アクティブ デプロイメントは、一部のプライベート クラウド ハイパーバイザーでのバーチャル ワイヤ デプロイメントとレイヤー 3 デプロイメントでサポートされています。これは、各ファイアウォールが専用のルーティング インスタンスを必要とし、常に両方のファイアウォールから、リアルタイムの完全な冗長性を必要とする場合にのみ推奨されるデプロイメントです。VM-Series ファイアウォールを HA ペアとして設定する方法については、「アクティブ/パッシブ HA の設定」および「アクティブ/アクティブ HA の設定」を参照してください。

Amazon Web Services（AWS）や Azure のようなパブリック クラウドに VM-Series ファイアウォールをデプロイする場合、従来のアクティブ/パッシブ HA 設定を使用できます。「AWS における VM-Series ファイアウォールの高可用性設定」および「Azure でのアクティブ/パッシブ HA のセットアップ」を参照してください。あるいは、プライベート データセンターと比較すると、クラウド インフラストラクチャにおけるリソースまたはリージョンの冗長性の組み込みには本質的な違いがあるので、ネイティブ クラウド サービスを利用して稼働時間を最大化する回復力のあるアーキテクチャを構築する場合には、以下のトピックを参照してください。

- AWS — Amazon ELB を使用した VM-Series ファイアウォールのオート スケーリング。複数のファイアウォールを VPC 内の複数の可用性ゾーンにデプロイします。
- Azure — VM-Series and Azure Application Gateway テンプレートのパラメータ。

サポートされる機能およびリンク	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
アクティブ/パッシブの HA	はい	はい	はい	いいえ	はい	はい	はい	いいえ	はい
アクティブ/アクティブの HA	はい	はい	いいえ	いいえ	いいえ	はい	無し	無し	いいえ

©2023 Palo Alto Networks, Inc.

サポートされる機能およびリンク	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
HA1	はい	はい	はい	いいえ	あり。	はい	はい	はい	はい
HA2—（セッションの同期とキープアライブ）	はい	はい	はい	いいえ	あり。	はい	はい	はい	はい
HA3	はい	はい	無し	無し	無し	あり。	無し	無し	無し

GCP での VM-Series のHA1 および HA2 サポートには、PAN-OS10.0x 以降および VM-Series プラグイン 2.0.5 以降が必要です。

NSX-T（E/W）上の VM-Series の高可用性は、サービス ヘルス チェックと呼ばれる NSX-T の機能を利用して実現しています。この NSX-T 機能により、サービス インスタンスに障害が発生した場合の高可用性をシミュレートすることができます。VM-Series ファイアウォールで設定する場合、VM-Series サービス インスタンスに障害が発生すると、そのファイアウォールに転送されたトラフィックは、クラスタ内の別のファイアウォール インスタンス（サービス クラスタ デプロイの場合）、または他のホスト上のファイアウォール インスタンス（ホスト ベースのデプロイの場合）にリダイレクトされます。NSX-T（E/W）上の VM-Series ファイアウォールの詳細は、「Panorama でのサービス定義の設定」を参照してください。

 ©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのアップグレード

PAN-OS のバージョンまたは VM-Series モデルをアップグレードすることにより、セキュリティ機能やファイアウォールのパフォーマンスを向上する、最新の機能やフィックスを追加することができます。

標準の PAN-OS リリースは、すべての Palo Alto Networks ファイアウォールにインストールすることができます。PAN-OS XFR リリースは VM-Series ファイアウォール専用で、VM-Series ファイアウォール向けの新機能やバグ フィックスが含まれます。VM-Series ファイアウォールに PAN-OS XFR イメージをインストールする場合、インストールしたソフトウェア バージョンよりも前の PAN-OS バージョンでは、その機能やフィックスは利用できません。

XFR イメージには VM-Seriesファイアウォール固有の機能とフィックスが含まれているため、XFR リリースにアップグレードする場合、XFR 固有の機能を保持するために、次回の PAN-OS メジャー リリースの更改まで XFR を利用し続ける必要があります。XFR で利用できるすべてのフィックスと機能は、次の PAN-OS メジャー リリースに取り込まれます。

- PAN-OS ソフトウェア バージョンのアップグレード（スタンドアロン版）
- PAN-OS ソフトウェア バージョンのアップグレード（HA ペア）
- Panorama を使った PAN-OS ソフトウェア バージョンのアップグレード
- PAN-OS ソフトウェア バージョンのアップグレード（VM-Series for NSX）
- VM-Series モデルのアップグレード
- HA ペアの VM-Series モデルのアップグレード
- VM-Series ファイアウォールの以前のリリースへのダウングレード

VM-Series ファイアウォールのインストール手順の詳細は、「VM-Series デプロイメント」を参照してください。

アップグレードの前にご使用のファイアウォール モデルのVM-Series のシステム要件を確認してください。ファイアウォールのメモリが *5.5GB* 未満の場合、ファイアウォールのシステム キャパシティ（セッション、ルール、セキュリティ ゾーン、アドレス オブジェクトなどの数）は、*VM-50 Lite* のキャパシティに制限されます。

PAN-OS ソフトウェア バージョンのアップグレード（スタンドアロン版）

新機能、対処が行われた問題、および既知の問題を確認してから、以下の手順に従って HA 構成ではないファイアウォールのアップグレードを行います。

トラフィックへの影響を避けるために、稼働停止期間中にアップグレードすることを計画してください。ファイアウォールが信頼できる電源に接続されていることを確認してください。アップグレード中に電力が失われると、ファイアウォールを使用できなくなる可能性があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | 十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。

VM-Series システム要件」を参照して、各 VM-Series モデルのリソース要件を確認してください。アップグレード プロセスを続行する前に、追加のハードウェア リソースを割り当てます。追加のハードウェア リソースを割り当てるプロセスはハイパーバイザーによって異なります。

モデルに必要なリソースが VM-Series ファイアウォールにない場合は、デフォルトで VM-50 に関連付けられているキャパシティになります。

STEP 2 | Web インターフェイスから**Device**（デバイス） > **Licenses**（ライセンス）の順に移動し、正しい VM-Series ファイアウォールのライセンスがインストールされていて、そのライセンスがアクティベートされていることを確認します。

VM-Series ファイアウォール スタンドアロン版で**Device**（デバイス） > **Support**（サポート）の順に移動し、サポート ライセンスがアクティベートされていることを確認します。

STEP 3 | 現在の構成ファイルのバックアップを保存します。

ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し**Export named configuration snapshot**（名前付き設定スナップショットのエクスポート）をクリックします。
2. 実行中の設定を含む XML ファイル**running-config.xml** など）を選択し**OK** をクリックして設定ファイルをエクスポートします。
3. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 4 | User-ID を有効にした場合、アップグレード後にファイアウォールは User-ID ソースから再度取得できるように、現在の IP アドレス-ユーザー名間マッピングおよびグループ マッピングをクリアします。ご自分の環境でのマッピングの再取得に必要な時間を推定するには、ファイアウォール上で次の CLI コマンドを実行します。

- IPアドレス - ユーザー名間マッピングの場合:
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- For group mappings:**`show user group-mapping statistics`**

STEP 5 | ファイアウォールで、最新のコンテンツ リリース バージョンが動作していることを確認します。

1. **Device**（デバイス） > **Dynamic Updates**（ダイナミック アップデート）を選択して、どの**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 リリース バージョンが現在インストールされているのかを確認します。

©2023 Palo Alto Networks, Inc.

2. ファイアウォールで最低要件を満たすコンテンツ リリース バージョンが動作していない場合、または最新バージョンの PAN-OS が必要な場合は**Check Now**（今すぐ確認）を選択して、利用可能なアップデートの一覧を入手してください。
3. 目的のコンテンツ リリース バージョンを探して**Download**（ダウンロード）します。

   コンテンツ アップデート ファイルを正常にダウンロードしたら、そのコンテンツ リリース バージョンの Action（アクション）列のリンクが**Download**（ダウンロード）か**Install**（インストール）に変化します。
4. アップデートインストールします。

STEP 6 | VM-Series プラグインをアップグレードします。

1. アップグレード前に最新のリリース ノートを参照し、新しい VM-Series プラグインがご使用の環境に及ぼす影響について確認してください。

   たとえば、新しい VM-Series プラグイン バージョンに AWS の機能だけが含まれているとします。新しい機能を利用するには、AWS の VM-Series ファイアウォール インスタンスでプラグインを更新する必要があります。

   ご使用の環境に適用されないアップグレードはインストールしないでください。
2. VM-Series ファイアウォールにログインし、ダッシュボードでプラグインのバージョンを確認します。
3. **Device**（デバイス） > **Plugins**（プラグイン）を選択し、プラグインのバージョンを確認します**Check Now**（今すぐチェック）を使用して最新の更新があるかどうか確認します。
4. プラグインのバージョンを選択し、Action（アクション）列に**Install**（インストール）をクリックしてプラグインをインストールします。

©2023 Palo Alto Networks, Inc.

STEP 7 | PAN-OS をアップグレードします。

ファイアウォールで管理ポートからインターネットにアクセスできない場合はPalo Alto Networks カスタマー サポート ポータル ポータルからソフトウェアイメージをダウンロードして、ファイアウォールに手動アップロードできます。

1. **Device**（デバイス） > **Software**（ソフトウェア）を選択して**Check Now**（今すぐ確認）をクリックして最新の PAN-OS アップデートを表示します。
2. ターゲットの PAN-OS バージョンを探して**Download**（ダウンロード）します。
3. イメージをダウンロードしたら（手動アップグレードの場合、イメージをアップロードしたら）、イメージを**Install**（インストール）します。
4. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら**Yes**（はい） をクリックします。
   - 再起動を促されなかったら**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し**Reboot Device**（デバイスの再起動）をクリックします。

   この時点で、ファイアウォールは ユーザー *ID* のマッピングをクリアした後、ユーザー *ID* のソースに接続して、マッピングを更新します。
5. ユーザー ID を有効にしている場合、次の CLI コマンドを使って、トラフィックを許可する前にファイアウォールが IP アドレス - ユーザー名およびグループのマッピングを更新していることを確認してください。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**
6. 初めて XFR リリースにアップグレードする場合、この手順を繰り返して対応する XFR リリースにアップグレードしてください。

STEP 8 | ファイアウォールがトラフィックを渡していることを確認します。

Monitor（監視） > **Session Browser**（セッション ブラウザ）を選択して、新しいセッションが表示されていることを確認します。

PAN-OS ソフトウェア バージョンのアップグレード（HA ペア）

高可用性（HA）構成のファイアウォール ペアをアップグレードするには、以下の手順を使用します。この手順は、アクティブ/パッシブ設定とアクティブ/アクティブ設定の両方に適用されます。

高可用性（HA）構成のファイアウォールをアップグレードする際にダウンタイムが発生しないようにするために、一度に 1 つだけ HA ピアをアップデートします。アクティブ/アクティブ ファイアウォールの場合、最初にアップグレードするピアはどちらでも構いません（ただし、分かりやすいように、この手順ではアクティブなセカンダリ ピアを最初にアップグレードしています）。アクティブ/パッシブ ファイアウォールの場合、最初にパッシブ ピアをアップグレードし、アクティブ ピアはサスペンド（フェイルオーバー）し、アクティブ ピアをアップデートし、次にそのピアを稼動状態に戻す（フェイルバック）必要があります。HA ピアのアップグ

©2023 Palo Alto Networks, Inc.

レード中のフェイルオーバーを防止するために、アップグレード作業に進む前にプリエンプションが無効になっていることを確認する必要があります。ペア内の 1 つのピアでのみ、プリエンプションを無効にする必要があります。

トラフィックへの影響を避けるために、稼働停止期間中にアップグレードすることを計画してください。ファイアウォールが信頼できる電源に接続されていることを確認してください。アップグレード中に電力が失われると、ファイアウォールを使用できなくなる可能性があります。

STEP 1 | 十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。

VM-Series システム要件」を参照して、各 VM-Series モデルのリソース要件を確認してください。アップグレード プロセスを続行する前に、追加のハードウェア リソースを割り当てます。追加のハードウェア リソースを割り当てるプロセスはハイパーバイザーによって異なります。

モデルに必要なリソースが VM-Series ファイアウォールにない場合は、デフォルトで VM-50 に関連付けられているキャパシティになります。

STEP 2 | Web インターフェイスから**Device**（デバイス） > **Licenses**（ライセンス）の順に移動し、正しい VM-Series ファイアウォールのライセンスがインストールされていて、そのライセンスがアクティベートされていることを確認します。

VM-Series ファイアウォール スタンドアロン版で**Device**（デバイス） > **Support**（サポート）の順に移動し、サポート ライセンスがアクティベートされていることを確認します。

STEP 3 | 現在の構成ファイルのバックアップを保存します。

ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

ペア内の各ファイアウォールで、これらの手順を実行します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し**Export named configuration snapshot**（名前付き設定スナップショットのエクスポート）をクリックします。
2. 実行中の設定を含む XML ファイル**running-config.xml** など）を選択し**OK** をクリックして設定ファイルをエクスポートします。
3. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 4 | User-ID を有効にした場合、アップグレード後にファイアウォールは User-ID ソースから再度取得できるように、現在の IP アドレス-ユーザー名間マッピングおよびグループ マッ

©2023 Palo Alto Networks, Inc.

ピングをクリアします。ご自分の環境でのマッピングの再取得に必要な時間を推定するには、ファイアウォール上で次の CLI コマンドを実行します。

- IPアドレス - ユーザー名間マッピングの場合:
  - **show user user-id-agent state all**
  - **show user server-monitor state all**
- For group mappings:**show user group-mapping statistics**

STEP 5 | HA ペア内の各ファイアウォールで、最新のコンテンツ リリース バージョンが動作していることを確認します。

PAN-OS 10.1 リリース用にインストールしなければならない最低コンテンツリリースバージョンについてはリリースノート』をご覧ください。アプリケーションおよび脅威のアップデートのベスト プラクティス」に従ってください。

1. 現在インストールされているアップデートを判断するには**Device**（デバイス） > **Dynamic Updates**（ダイナミック アップデート）を選択して、どの**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）をチェックして、現在インストールされているアップデートを判断してください。
2. ファイアウォールで最低限必要なコンテンツ リリース バージョンが動作していない、またはインストールするソフトウェアのバージョンが最新のバージョンを必要としている場合**Check Now**（今すぐ確認）を選択して利用可能なアップデートのリストを取得してください。
3. 目的のコンテンツ リリース バージョンを探して**Download**（ダウンロード）します。

   コンテンツ アップデート ファイルを正常にダウンロードしたら、そのコンテンツ リリース バージョンの Action（アクション）列のリンクが**Download**（ダウンロード）か**Install**（インストール）に変化します。
4. アップデートインストールします。アップデートは両方のピアにインストールする必要があります。

©2023 Palo Alto Networks, Inc.

STEP 6 | VM-Series プラグインをアップグレードします。

1. アップグレード前に最新のリリース ノートを参照し、新しい VM-Series プラグインがご使用の環境に及ぼす影響について確認してください。

   たとえば、新しい VM-Series プラグイン バージョンに AWS の機能だけが含まれているとします。新しい機能を利用するには、AWS の VM-Series ファイアウォール インスタンスでプラグインを更新する必要があります。

   ご使用の環境に適用されないアップグレードはインストールしないでください。

2. VM-Series ファイアウォールにログインし、ダッシュボードでプラグインのバージョンを確認します。
3. **Device**（デバイス） > **Plugins**（プラグイン）を選択し、プラグインのバージョンを確認します**Check Now**（今すぐチェック）を使用して最新の更新があるかどうか確認します。
4. プラグインのバージョンを選択し、Action（アクション）列にあ**Install**（インストール）をクリックしてプラグインをインストールします。

   HA ペアの VM-Series ファイアウォールにプラグインをインストールする際は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態に移行します。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 7 | 各ペアの最初のピアのプリエンプションを無効にします。この設定は、HA ペアの一方のファイアウォールでのみ無効にする必要がありますが、アップグレードを続行する前にコミットが成功していることを確認してください。

1. **Device**（デバイス） > **High Availability**（高可用性）を選択して**Election Settings**（選択設定）を編集します。
2. 有効になっている場合は**Preemptive**（プリエンプティブ）設定を無効（クリア）して**OK** をクリックします。
3. 変更を**Commit**（コミット）します。

STEP 8 | 最初のピアに PAN-OS リリースをインストールします。XFR リリースにアップグレードする場合、XFR リリースに対応するバージョンをインストールします。

アクティブ/パッシブ構成でのダウンタイムを最小限に抑えるために、まずパッシブ ピアをアップグレードします。アクティブ/アクティブ構成の場合は、セカンダリ ピアを最初にアッ

©2023 Palo Alto Networks, Inc.

プグレードします。ベスト プラクティスとして、アクティブ/アクティブ構成を使用している場合、同じメンテナンス期間中に両方のピアをアップグレードすることをお勧めします。

アップグレード前に *HA* が正常に動作しているかどうかをテストしたい場合は、インシデントが発生せずにフェイルオーバーが発生するように、アクティブ/パッシブ構成のアクティブなピアをアップグレードすることを検討してください。

1. 最初のピアで**Device**（デバイス） > **Software**（ソフトウェア）を選択して、最新のアップデートを確認するために**Check Now**（今すぐ確認）をクリックします。
2. ターゲットの PAN-OS バージョンを探して**Download**（ダウンロード）します。

   ファイアウォールで管理ポートからインターネットにアクセスできない場合はPalo Alto Networks サポート ポータル ポータルからソフトウェア イメージをダウンロードして、ファイアウォールに手動アップロードできます。
3. イメージをダウンロードしたら（手動アップグレードの場合、イメージをアップロードしたら）、イメージを**Install**（インストール）します。
4. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら**Yes**（はい） をクリックします。
   - 再起動を促されなかったら**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し**Reboot Device**（デバイスの再起動）を選択します。
5. デバイスの再起動が完了したら**Dashboard**（ダッシュボード）の High Availability（高可用性）ウィジェットを表示して、アップグレードしたデバイスが引き続き HA 構成内でパッシブまたはアクティブなセカンダリ ピアであることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 9 | セカンダリ ピアに PAN-OS リリースをインストールします。XFR リリースにアップグレードする場合、XFR リリースに対応するバージョンをインストールします。

1. （アクティブ/パッシブ構成のみ）HA がアップグレードしたピアにフェイルオーバーするように、アクティブ ピアを一時停止します。
   1. アクティブ ピアで**Device**（デバイス） > **High Availability**（高可用性） > **Operational Commands**（操作コマンド）を選択して**Suspend local device**（ローカル デバイスの一時停止）をクリックします。
   2. **Dashboard**（ダッシュボード）の High Availability（高可用性）ウィジェットを表示して、状態が**Passive**（パッシブ）に変化したことを確認します。
   3. 他のピア上で、ピアがアクティブ化されており、トラフィックを渡していることを確認します**Monitor**（監視） > **Session Browser**（セッション ブラウザ））。
2. セカンダリ ピアで**Device**（デバイス） > **Software**（ソフトウェア）を選択し**Check Now**（今すぐ確認）をクリックして最新のアップデートを確認します。
3. ターゲットの PAN-OS バージョンを探して**Download**（ダウンロード）します。
4. イメージをダウンロードしたら、それ**Install**（インストール）します。
5. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら**Yes**（はい） をクリックします。
   - 再起動を促されなかったら**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し**Reboot Device**（デバイスの再起動）を選択します。
6. （アクティブ/パッシブ構成のみ）アップグレードしたばかりのピアの CLI から、次のコマンドを実行してファイアウォールを再び機能させます。

   ```
   request high-availability state functional
   ```

STEP 10 | PAN-OS XFR のアップグレードのみ）最初のピアとセカンダリ ピアを PAN-OS XFR アップグレードするためにステップ 8ステップ 9を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 11 | 両方のピアが予定通りにトラフィックを渡していることを確認します。

アクティブ/パッシブ構成では、アクティブなピアのみがトラフィックを渡す必要があります。アクティブ/アクティブ構成では、両方のピアがトラフィックを渡す必要があります。

アップグレードが成功したことを確認するには、次の CLI コマンドを実行します:

- アクティブなピアのみ）アクティブ ピアがトラフィックを渡していることを確認するには**show session all** コマンドを実行します。
- セッションの同期状態を確認するには**show high-availability interface ha2** コマンドを実行し、CPU テーブルのハードウェア インターフェイス カウンターが以下のように増加していることを確認します
  - アクティブ/パッシブ構成では、送信済みパケットはアクティブ ピアのみで表示され、パッシブ ピアには受信したパケットのみが表示されます。

    HA2 キープアライブを有効にしている場合、パッシブ ピアのハードウェア インターフェイス カウンターに送信パケットと受信パケットの両方が表示されます。これは、*HA2* キープアライブが双方向で、両方のピアで *HA2* キープアライブ パケットが送信されるためです。
  - アクティブ/アクティブ設定では、両方のピアで受信したパケットと送信したパケットが表示されます。

STEP 12 | アップグレード前にプリエンプションを無効にした場合、ここで有効にします。

1. **Device**（デバイス） > **High Availability**（高可用性）を選択して**Election Settings**（選択設定）を編集します。
2. **Preemptive**（プリエンプティブ）を選択して**OK**をクリックします。
3. 変更を**Commit**（コミット）します。

Panorama を使った PAN-OS ソフトウェア バージョンのアップグレード

次の手順に従い Panorama で管理するファイアウォールをアップグレードします。この手順は、高可用性（HA）設定でデプロイされたスタンド アロン ファイアウォールとファイアウォールに適用されます。

Panorama が直接アップデート サーバーに接続できない場合は、*Panorama* にイメージを手動でダウンロードしてファイアウォールに配信できるように、Panorama がインターネットに接続されていないときのファイアウォールへのアップデートのデプロイ手順に従います。

Panorama からファイアウォールをアップグレードする前に、次のことを行う必要があります：

- Panorama がアップグレードしているものと同じかそれ以降の PAN-OS バージョンを実行していることを確認してください。マネージド ファイアウォールをこのバージョンにアップグレードする前に、Panorama および Log Collectors（ログ コレクタ） を 9.1 にアップグレードする必要があります。また、Log Collectors（ログ コレクタ）を 9.1 にアップグレードする場

©2023 Palo Alto Networks, Inc.

合、ログ インフラの変更のためにすべての Log Collectors を同時にアップグレードする必要があります。

- Panorama を 9.1 にアップグレードする場合、メンテナンス期間を最大 6 時間延長することを予定してください。このリリースには大幅なインフラの変更が含まれており、以前のリリースよりも Panorama のアップグレードに時間がかかります。
- ファイアウォールが信頼できる電源に接続されていることを確認してください。アップグレード中に電力が失われると、ファイアウォールを使用できなくなる可能性があります。

STEP 1 | Panorama のアップグレード後、アップグレードを予定しているファイアウォールに設定をコミットおよびプッシュ配信してください。

STEP 2 | 十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。

「VM-Series システム要件」を参照して、各 VM-Series モデルのリソース要件を確認してください。アップグレード プロセスを続行する前に、追加のハードウェア リソースを割り当てます。追加のハードウェア リソースを割り当てるプロセスはハイパーバイザーによって異なります。

モデルに必要なリソースが VM-Series ファイアウォールにない場合は、デフォルトで VM-50 に関連付けられているキャパシティになります。

STEP 3 | Web インターフェイスから **Device**（デバイス） > **Licenses**（ライセンス）の順に移動し、正しい VM-Series ファイアウォールのライセンスがインストールされていて、そのライセンスがアクティベートされていることを確認します。

VM-Series ファイアウォール スタンドアロン版で、**Device**（デバイス） > **Support**（サポート）の順に移動し、サポート ライセンスがアクティベートされていることを確認します。

STEP 4 | アップグレードする各管理対象ファイアウォールで、現在の設定ファイルのバックアップを保存します。



ファイアウォールは自動的に設定のバックアップを作成しますが、アップグレード前にバックアップを作成して外部に保存しておくことをお勧めします。

1. Panorama Web インターフェイスで、**Panorama** > **Setup**（セットアップ） > **Operations**（操作） を選択し、**Export Panorama and devices config bundle**（**Panorama** および**Device**（デバイス）の設定バンドルのエクスポート） をクリックして、最新の Panorama と各管理アプライアンスの最新の設定バックアップを生成してエクスポートします。
2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 5 | アップグレードするファイアウォールのコンテンツ リリース バージョンを更新します。

PAN-OS 9.1 のリリースに必要な最低コンテンツ リリース バージョンについては、リリースノートをご覧ください。Panorama と管理対象のファイアウォールのコンテンツ更新をデプロ

©2023 Palo Alto Networks, Inc.

イする際は、必ずアプリケーションと脅威更新に関するベストプラクティスに従ってください。

1. **Panorama** > **Device Deployment**（デバイスのデプロイメント） > **Dynamic Updates**（動的更新）を選択して、最新の更新を **Check Now**（今すぐチェック）します。更新が入手可能な場合は、Action（アクション）列に **Download**（ダウンロード）リンクが表示されます。
2. まだインストールしていない場合は、最新のコンテンツ リリース バージョンを **Download**（ダウンロード）します。
3. **Install**（インストール）をクリックし、更新をインストールするファイアウォールを選択してから、**OK** をクリックします。HA ファイアウォールをアップグレードする場合は、両方のピアのコンテンツを更新する必要があります。

STEP 6 | （HA ファイアウォールのアップグレードのみ）HA ペアの一部であるファイアウォールをアップグレードする場合は、プリエンプションを無効にします。各 HA ペアの 1 つのファイアウォールでのみ、この設定を無効にする必要があります。

1. **Device**（デバイス） > **High Availability**（高可用性）を選択して **Election Settings**（選択設定）を編集します。
2. 有効になっている場合は、**Preemptive**（プリエンプティブ）設定を無効（クリア）して、**OK** をクリックします。
3. 変更を **Commit**（コミット）します。アップグレードを続行する前に、コミットが成功していることを確認してください。

STEP 7 | 対象の PAN-OS リリース イメージをダウンロードします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイメント） > **Software**（ソフトウェア）を選択して、最新のリリース バージョンを **Check Now**（今すぐチェック）します。
2. アップグレードするリリース バージョンのファイアウォール固有のファイルを **Download**（ダウンロード）します。アップグレードするファイアウォールのモデル（またはファイアウォール シリーズ）ごとに個別のインストール ファイルをダウンロードする必要があります。

STEP 8 | PAN-OS のソフトウェアの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。

1. アップグレードするファイアウォールモデルに対応するアクション列の **Install**（インストール）をクリックします。
2. ソフトウェア ファイルのデプロイ ダイアログで、アップグレードするすべてのファイアウォールを選択します。ダウンタイムを短縮するには、各 HA ペアで 1 つのピアだ

©2023 Palo Alto Networks, Inc.

けを選択します。アクティブ/パッシブ ペアの場合、パッシブ ピアを選択します。アクティブ/アクティブ ペアの場合は、アクティブ-セカンダリ ピアを選択します。

3. （HA ファイアウォールのアップグレードのみ） **Group HA Peers**（グループ **HA** ピア）が選択されないことを確認してください。
4. **Reboot device after Install**（インストール後にデバイスを再起動）を選択します。
5. アップグレードを開始するには、**OK** をクリックします。
6. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら、**Yes**（はい） をクリックします。
   - 再起動を促されなかったら、**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。
7. ファイアウォールの再起動が完了したら、**Panorama** > **Managed Devices**（管理対象デバイス）を選択し、アップグレードしたファイアウォールのソフトウェア バージョンが 9.1.0 であることを確認します。また、アップグレードしたパッシブ ファイアウォールの HA ステータスがまだパッシブであることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 9 | （HA ファイアウォールのアップグレードのみ）各 HA ペアの 2 番目の HA ピアをアップグレードします。

1. （アクティブ/パッシブ アップグレードのみ）アップグレードする各アクティブ/パッシブペアでアクティブデバイスをサスペンドします。

   1. コンテキストをアクティブなファイアウォールに切り替えます。
   2. **Dashboard**（ダッシュボード）の高可用性ウィジット内で、, verify that **Local**（ローカル）ファイアウォールの状態が **Active**（アクティブ）であり、**Peer**（ピア）が **Passive**（パッシブ）であることを確認します。
   3. **Device**（デバイス） > **High Availability**（高可用性） > **Operational Commands**（操作コマンド） > **Suspend local device**（ローカル **Device**（デバイスのサスペンド）。
   4. **Dashboard**（ダッシュボード）の高可用性ウィジットに戻り、**Local**（ローカル）が **Passive**（パッシブ）に、**Peer**（ピア）が **Active**（アクティブ）に変更したことを確認します。

2. Panorama コンテキストに戻り、**Panorama** > **Device Deployment**（デバイスのデプロイ） > **Software**（ソフトウェア）を選択します。
3. アップグレードする HA ペアのファイアウォール モデルに対応するアクション列の **Install**（インストール）をクリックします。
4. ソフトウェア ファイルのデプロイ ダイアログで、アップグレードするすべてのファイアウォールを選択します。今回は、アップグレードしたばかりの HA ファイアウォールのピアだけを選択します。
5. **Group HA Peers**（グループ **HA** ピア）が選択されないことを確認してください。
6. **Reboot device after Install**（インストール後にデバイスを再起動）を選択します。
7. アップグレードを開始するには、**OK** をクリックします。
8. インストールが正常に完了したら、次のいずれかの方法によって再起動します。

   - 再起動を促されたら、**Yes**（はい） をクリックします。
   - 再起動を促されなかったら、**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。

9. （アクティブ/パッシブ アップグレードのみ）アップグレードしたばかりのピアの CLI から、次のコマンドを実行してファイアウォールを再び機能させます。

   ```
   request high-availability state functional
   ```

STEP 10 | （PAN-OS XFR のアップグレードのみ）最初のピアとセカンダリ ピアを PAN-OS XFR アップグレードするために、ステップ 8～ステップ 9を繰り返します。

STEP 11 | 各管理対象ファイアウォールで実行されているソフトウェアおよびコンテンツ リリース バージョンを確認します。

1. Panorama で、**Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. ファイアウォールを見つけ、表のコンテンツおよびソフトウェアのバージョンを確認します。

   HA ファイアウォールの場合、各ピアの HA ステータスが想定どおりであることを確認することもできます。

©2023 Palo Alto Networks, Inc.

STEP 12 | （HA ファイアウォールのアップデートのみ）アップグレード前に HA ファイアウォールの一方でプリエンプションを無効にした場合は、**Election Settings**（選択設定）（**Device**（デバイス） > **High Availability**（高可用性））を編集し、そのファイアウォールの **Preemptive**（プリエンプティブ）設定を再び有効にして、変更を **Commit**（コミット）します。

PAN-OS ソフトウェア バージョンのアップグレード（VM-Series for NSX）

デプロイ環境に最も適したアップグレード方法を選択します。

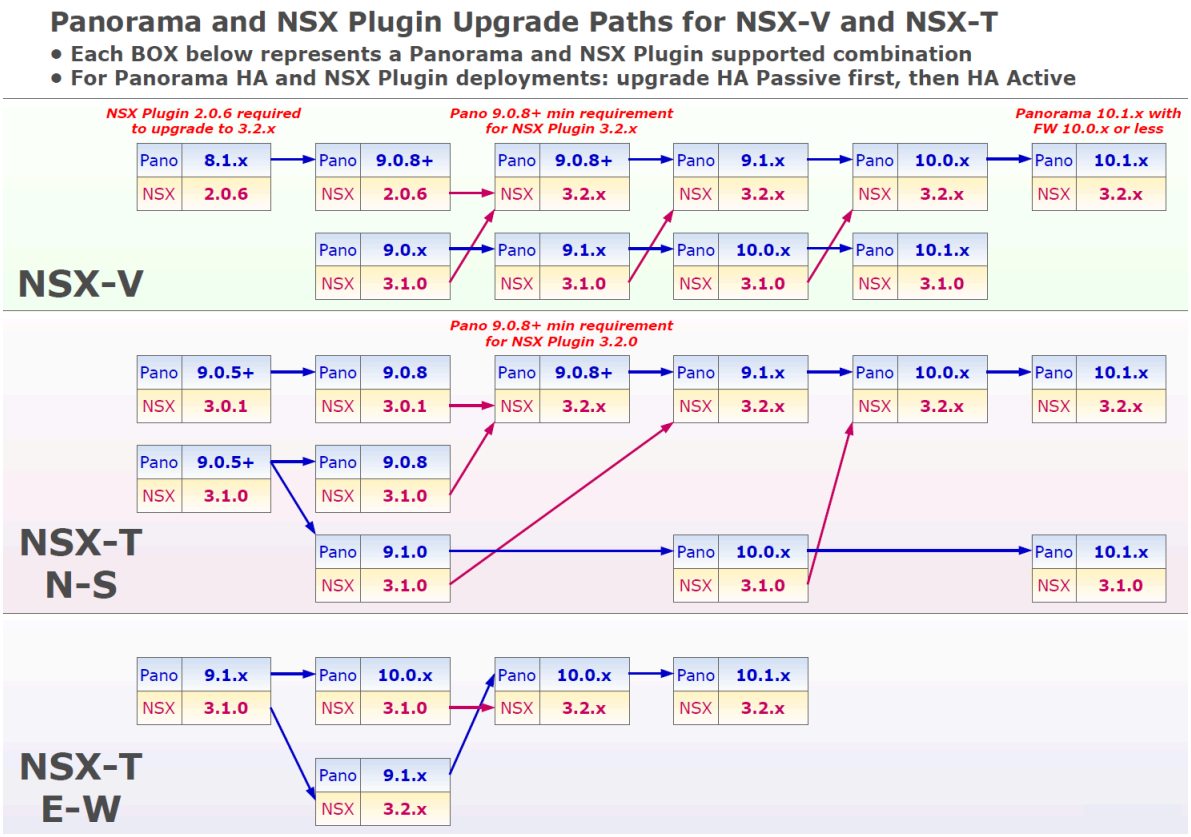
- メンテナンスウィンドウ中に NSX 用の VM-Series をアップグレードする - このオプションを使用して、サービス定義中のOVF URL を変更せずに、メンテナンスウィンドウ中に VM-Series ファイアウォールをアップグレードします。
- トラフィックを中断せずに VM-Series for NSX をアップグレードする - このオプションを使用して、ゲスト VM へのサービスを中断したり、サービス定義の OVF URL を変更したりせずに、VM-Series ファイアウォールをアップグレードします。

次の画像は、現在サポートされているPanoramaとPanorama plugin for VMware NSXの組み合わせ、および正常にアップグレードを行うために必要なアップグレードパスを表しています。

- 下の各ボックスが、サポートされている組み合わせを表しています。
- HAペア内のPanorama plugin for NSXまたはPanoramaをアップグレードする場合、まずパッシブPanoramaピアをアップグレードしてから、次にアクティブHAピアをアップグレードしてください。

VM-Series for VMware NSXデプロイメントをアップグレードする前に、以下の図に示されているアップグレードパスを参照して、ご利用の環境に適したプラグインとPAN-OSの組み合わせに至るまでのアップグレード手順を理解してください。

 ©2023 Palo Alto Networks, Inc.



保守期間中に NSX 用 VM-Series をアップグレード

VM-Series ファイアウォールの NSX エディションの場合は、Panorama を使用してファイアウォールのソフトウェア バージョンをアップグレードします。

STEP 1 | VM-Series for VMware NSXのアップグレードパスを確認します。

STEP 2 | 追加のハードウェア リソースを VM-Series ファイアウォールに割り当てます。

十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。VM-Series システム要件を参照して、各 VM-Series モデルの新しいリソース要件を確認してください。アップグレード プロセスを続行する前に、追加のハードウェア リソースを割り当てます。追加のハードウェア リソースを割り当てる手順は、ハイパーバイザごとに異なります。

STEP 3 | アップグレードする各管理対象ファイアウォールで、現在の設定ファイルのバックアップを保存します。

設定のバックアップはファイアウォールで自動的に作成されますが、アップグレードの前にバックアップを作成して、そのバックアップを外部に保存することをお勧めします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Export Panorama and devices config bundle**（**Panorama** およびデバイスの設定バンドルのエクスポート）をクリックします。このオプションは、Panorama および管理対象デバイス

©2023 Palo Alto Networks, Inc.

の設定バックアップの最新バージョンを手動で生成およびエクスポートする場合に使用します。

2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 4 | リリース ノートを調べ、PAN-OS バージョンで要求されるコンテンツ リリース バージョンを確認します。

アップグレードするファイアウォールで、その PAN-OS バージョンで要求されるコンテンツ リリース バージョンが実行されている必要があります。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Dynamic Updates**（ダイナミック更新）を選択します。
2. 最新の更新があるかどうか確認します。Check Now（今すぐチェック）（ウィンドウの左下）をクリックして最新の更新があるかどうか確認します。Action（アクション）列のリンクは、更新が入手可能かどうかを示します。入手可能なバージョンがある場合は、**Download**（ダウンロード）リンクが表示されます。
3. 選択した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。ダウンロードが正常に完了すると、**Action**（アクション）列のリンクが **Download**（ダウンロード）から **Install**（インストール）に変わります。
4. **Install**（インストール）をクリックし、更新をインストールするデバイスを選択します。インストールが完了すると、**Currently Installed**（現在インストール済み）列にチェック マークが表示されます。

STEP 5 | 選択したファイアウォールにソフトウェア更新をデプロイします。

ファイアウォールが *HA* で設定されている場合は、***Group HA Peers***（***HA*** ピアのグループ化）チェック ボックスをオフにして、*HA* ピアを *1* つずつアップグレードします。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Software**（ソフトウェア）を選択します。
2. 最新の更新があるかどうか確認します。**Check Now**（今すぐチェック）（ウィンドウの左下にある）をクリックして最新の更新があるかどうか確認します。**Action**（アクション）列のリンクは、更新が入手可能かどうかを示します。
3. **File Name**（ファイル名）を確認し、**Download**（ダウンロード）をクリックします。ダウンロードしたソフトウェア バージョンがネットワークにデプロイされたファイアウォール モデルと一致することを確認します。ダウンロードが正常に完了すると、**Action**（アクション）列のリンクが **Download**（ダウンロード）から **Install**（インストール）に変わります。
4. **Install**（インストール）をクリックし、ソフトウェア バージョンをインストールするデバイスを選択します。
5. **Reboot device after install**（インストール後にデバイスを再起動する）をオンにし、**OK** をクリックします。
6. HA で設定されているデバイスがある場合は、**Group HA Peers**（**HA** ピアのグループ化）チェック ボックスをオフにして、HA ピアを 1 つずつアップグレードします。

©2023 Palo Alto Networks, Inc.

STEP 6 | 各管理対象デバイスで実行されているソフトウェアおよびコンテンツ リリース バージョンを確認します。

1. **Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. デバイスを見つけ、表のコンテンツおよびソフトウェアのバージョンを確認します。

トラフィックを中断せずに NSX 用 VM-Series をアップグレード

次の各作業を行い、VMware NSX 環境における VM-Series ファイアウォールの PAN-OS バージョンをアップグレードします。この作業により、VM を別の ESXi ホストに移行することで、トラフィックを妨げることなく PAN-OS をアップグレードできるようになります。

STEP 1 | VM-Series for VMware NSXのアップグレードパスを確認します。

STEP 2 | アップグレードする各管理対象ファイアウォールで、現在の設定ファイルのバックアップを保存します。

設定のバックアップはファイアウォールで自動的に作成されますが、アップグレードの前にバックアップを作成して、そのバックアップを外部に保存することをお勧めします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Export Panorama and devices config bundle**（**Panorama** およびデバイスの設定バンドルのエクスポート）をクリックします。このオプションは、Panorama および管理対象デバイスの設定バックアップの最新バージョンを手動で生成およびエクスポートする場合に使用します。
2. エクスポート ファイルをファイアウォールの外部に保存します。アップグレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 3 | リリース ノートを調べ、PAN-OS バージョンで要求されるコンテンツ リリース バージョンを確認します。

アップグレードするファイアウォールで、その PAN-OS バージョンで要求されるコンテンツ リリース バージョンが実行されている必要があります。

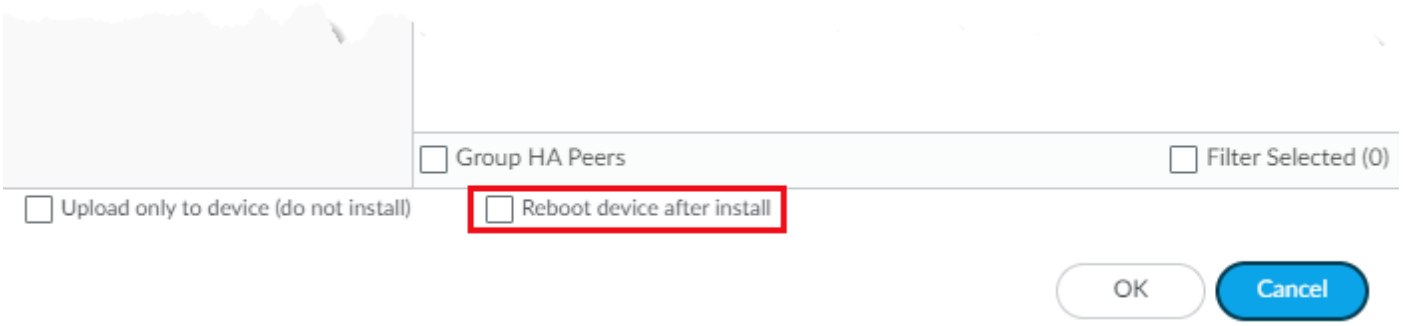
1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Dynamic Updates**（ダイナミック更新）を選択します。
2. 最新の更新があるかどうか確認します。Check Now（今すぐチェック）（ウィンドウの左下）をクリックして最新の更新があるかどうか確認します。Action（アクション）列のリンクは、更新が入手可能かどうかを示します。入手可能なバージョンがある場合は、**Download**（ダウンロード）リンクが表示されます。
3. 選択したバージョンをダウンロードするには、**Download**（ダウンロード）をクリックします。ダウンロードが正常に完了すると、**Action**（アクション）列のリンクが **Download**（ダウンロード）から **Install**（インストール）に変わります。
4. **Install**（インストール）をクリックし、更新をインストールするデバイスを選択します。インストールが完了すると、**Currently Installed**（現在インストール済み）列にチェック マークが表示されます。

©2023 Palo Alto Networks, Inc.

STEP 4 | PAN-OS イメージをクラスター内のすべての VM-Series ファイアウォールにダウンロードします。

1. Panorama にログインします。
2. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Software**（ソフトウェア）を選択します。
3. **Refresh**（更新）をクリックして最新のソフトウェア リリースを表示し、さらに **Release Notes**（リリース ノート）を表示して、リリースにおける変更内容の説明およびソフトウェアをインストールするための移行パスを確認します。
4. **Download**（ダウンロード）をクリックしてソフトウェアを取得し、**Install**（インストール）をクリックします。

   新しいソフトウェアイメージのインストール後は、*VM-Series* ファイアウォールを再起動しないでください。
5. アップグレードする管理対象のデバイスを選択します。
6. **Reboot device after install**（インストール後にデバイスを再起動）のチェックボックスをクリアします。



7. **OK**をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | クラスター内の最初の ESXi ホスト上の VM-Series ファイアウォールをアップグレードします。

1. vCenter にログインします。
2. **Hosts and Clusters**（ホストおよびクラスター）を選択します。
3. ホストを右クリックし、**Maintenance Mode**（メンテナンス モード） > **Enter Maintenance Mode**（メンテナンス モードに切り替え）を選択します。
4. VM-Series ファイアウォールを除き、ホストに接していない VM をすべて移行（自動あるいは手動）します。
5. VM-Series ファイアウォールをパワーオフします。ホストがメンテナンス モードに切り替わる際に自動的にこれが行われるはずです。
6. （任意）アップグレード作業を続行する前に、追加の CPU やメモリを VM-Series ファイアウォールに割り当てます。

   十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。VM-Series モデルを参照して、各 VM-Series モデルの新しいリソース要件を確認してください。
7. ホストを右クリックし、**Maintenance Mode**（メンテナンス モード） > **Exit Maintenance Mode**（メンテナンス モードを終了）を選択します。メンテナンス モードを終了すると、NSX ESX Agent Manager（EAM）が VM-Series ファイアウォールの電源をオンにします。新しい PAN-OS バージョンを持つファイアウォールが再起動します。
8. すべての VM を元のホストに移行（自動あるいは手動）し直します。

STEP 6 | 各 ESXi ホスト上の VM-Series ファイアウォールに対し、この作業を繰り返します。

STEP 7 | 各管理対象デバイスで実行されているソフトウェアおよびコンテンツ リリース バージョンを確認します。

1. **Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. デバイスを見つけ、表のコンテンツおよびソフトウェアのバージョンを確認します。

VM-Series モデルのアップグレード

VM-Series ファイアウォールのライセンス プロセスでは、UUID と CPU ID を使用して VM-Series ファイアウォールの一意のシリアル番号を生成します。そのため、ライセンスを生成するときに、ライセンスは VM-Series ファイアウォールの特定のインスタンスにマッピングされ、変更することはできません。

以下の場合、このセクションの手順を実行します。

- 評価版ライセンスから製品ライセンスに移行する。
- キャパシティの大きいモデルにアップグレードする。VM-100 から VM-300 モデルへのアップグレードなど。

©2023 Palo Alto Networks, Inc.

- キャパシティをアップグレードする。これで、ファイアウォール上の重要なプロセスを再起動します。サービスの中断を最小限に抑えるには、*HA* 設定をお勧めします。*HA* ペアでキャパシティをアップグレードするには、「HA ペアでの VM-Series モデルのアップグレード」を参照してください。
- プライベートクラウドまたはパブリッククラウドのデプロイメントでは、*BYOL* オプションを使用してファイアウォールのライセンスを付与されている場合、インスタンスタイプまたは *VM* タイプを変更する前に VM を非アクティブ化する必要があります。モデルまたはインスタンスをアップグレードすると *UUID* と *CPU ID* が変更されるため、 そのときにライセンスを適用する必要があります。

STEP 1 | 追加のハードウェア リソースを VM-Series ファイアウォールに割り当てます。

キャパシティのアップグレードを開始する前に、新しいキャパシティをサポートできるだけの十分なハードウェア リソースを VM-Series ファイアウォールで使用できることを確認してください。追加のハードウェア リソースを割り当てる手順は、ハイパーバイザごとに異なります。

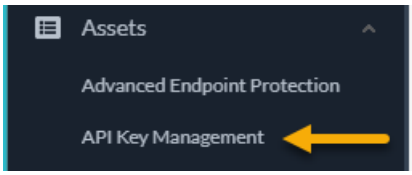
新しい VM-Series モデルのハードウェア要件を確認するには、「VM-Series モデル」を参照してください。

キャパシティのアップグレードでは VM-Series ファイアウォールを再起動する必要はありませんが、ハードウェアの割り当てを変更するために仮想マシンをパワーオフする必要があります。

STEP 2 | ライセンスの API キーをカスタマーサポートポータルから取得します。

1. カスタマー サポート ポータルにログインします。

   必ず、最初のライセンスを登録するために使用したのと同じアカウントを使用してください。
2. 左側のメニューから、アセット > **API** キー管理 を選択します。
3. API キーをコピーします。



STEP 3 | ファイアウォールで CLI を使用し、前の手順でコピーした API キーをインストールします。

```
request license api-key set key <key>
```

STEP 4 | (インターネットにアクセスできる場合) ファイアウォールを有効にして、 デバイス > セットアップ > サービスで サーバー **ID** の更新の確認を行います。

©2023 Palo Alto Networks, Inc.

STEP 5 | 変更を **Commit**（コミット）します。ファイアウォール上に、ローカルに設定したユーザーが存在していることを確認してください。設定がライセンスのない PA-VM オブジェクトの制限を超えている場合、非アクティブ化した後に、Panorama がプッシュしたユーザーは利用できなくなる可能性があります。

STEP 6 | キャパシティをアップグレードします。

Device（デバイス） > **Licenses**（ライセンス） > **Upgrade VM Capacity**（**VM** キャパシティのアップグレード）を選択し、次のいずれかの方法でライセンスおよびサブスクリプションをアクティベートします。

- (インターネット) ライセンスサーバーからライセンス キーを取得 - カスタマー サポートポータルでライセンスをアクティベートした場合は、このオプションを使用します。
- (インターネット) 認証コードを使用 - サポート ポータルで以前にアクティベートされていないライセンスの認証コードを使用して VM-Series キャパシティをアップグレードする場合は、このオプションを使用します。**Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
- (インターネットなし) ライセンスキーの手動アップロード - ファイアウォールとカスタマーサポートポータルとのネットワーク接続が確立されていない場合は、このオプションを使用します。インターネットにアクセスできるコンピュータから CSP にログインし、ライセンスキー ファイルをダウンロードし、ファイアウォールと同じネットワーク内のコンピュータに転送して、ファイアウォールにアップロードします。

STEP 7 | ファイアウォールが正常にライセンス登録されていることを確認します。

Device（デバイス） > **Licenses**（ライセンス）ページで、ライセンスが正常にアクティベートされたことを確認します。

HA ペアの VM-Series モデルのアップグレード

VM-Series ファイアウォールをアップグレードすると、ファイアウォールのキャパシティを増やすことができます。キャパシティは、VM-Series ファイアウォールで最適に処理できるセッション数、ルール数、セキュリティ ゾーン数、アドレス オブジェクト数、IPSec VPN トンネル数、および SSL VPN トンネル数に基づいて定義されます。VM-Series ファイアウォールに新しいキャパシティ ライセンスを適用すると、ファイアウォールにモデル番号とその関連機能が実装されます。

アップグレードする前に、ファイアウォールモデルの VM-Series のシステム要件を確認してください。ファイアウォールのメモリが *5.5GB* 未満の場合、ファイアウォールのキャパシティ（セッション、ルール、セキュリティ ゾーン、アドレス オブジェクトなどの数）は、*VM-50 Lite* のキャパシティに制限されます。

このプロセスは、HA 設定のハードウェアベースのファイアウォールのペアをアップグレードする場合と似ています。キャパシティ アップグレード プロセス中もセッションの同期は継続します（有効にしている場合）。高可用性（HA）構成のファイアウォールをアップグレードする際にダウンタイムが発生しないようにするために、一度に 1 つだけ HA ピアをアップデートします。

©2023 Palo Alto Networks, Inc.

アップグレード プロセス中はファイアウォールの設定を変更しないでください。アップグレード プロセス中は、キャパシティの不一致が検出されると設定の同期が自動的に無効になり、両方の *HA* ピアのキャパシティ ライセンスが一致したときに再度有効になります。

HA ペアのファイアウォールのメジャー ソフトウェア バージョンとキャパシティが異なる場合（バージョン *9.1* と *9.0* など）、両方のデバイスが *HA* サスペンド状態になります。そのため、キャパシティをアップグレードする前に両方のファイアウォールで同じバージョンの *PAN-OS* が実行されていることを確認することをお勧めします。

STEP 1 | パッシブ 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。

手順に従って VM-Series モデルをアップグレードします。

このパッシブ ピアで一部のプロセスが再起動すると、新しい VM-Series モデルがダッシュボードに表示されます。キャパシティがアクティブ ピアと一致しないため、このアップグレードされたピアは機能停止状態になっています。

セッションの同期を有効にしている場合、次のステップに進む前に HA ピアでセッションが同期していることを確認します。セッションの同期状態を確認するには、**`show high-availability interface ha2`** コマンドを実行し、CPU テーブルのハードウェア インターフェイス カウンターが以下のように増加していることを確認します。

- アクティブ/パッシブ設定では、送信済みパケットはアクティブ ピアのみで表示され、パッシブ デバイスには受信したパケットのみが表示されます。

  HA2 キープアライブを有効にしている場合、パッシブ ピアのハードウェア インターフェイス カウンターに送信パケットと受信パケットの両方が表示されます。これは、HA2 キープアライブが双方向で、両方のピアで HA2 キープアライブ パケットが送信されるためです。
- アクティブ/アクティブ設定では、両方のピアで受信したパケットと送信したパケットが表示されます。

STEP 2 | アクティブ 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。

手順に従って VM-Series モデルをアップグレードします。

重要なプロセスが再起動すると、新しい VM-Series モデル名がダッシュボードに表示されます。パッシブ ファイアウォールはアクティブになり、このピア（以前のアクティブ ファイアウォール）が初期状態から移行して HA ペアのパッシブ ピアになります。

VM-Series ファイアウォールの以前のリリースへのダウングレード

次のワークフローを使用して、別の機能リリースにアップグレードする前に実行されていた構成を復元します。アップグレード以降に加えられた変更はすべて失われます。したがって、現在の構成をバックアップして、新しいリリースに戻ったときにそれらの変更を復元できるようにすることが重要です。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールをバージョン *10.0.4* 以降からバージョン *10.0.3* 以前にダウングレードすることはできません。

次の手順を使用して、以前のリリースにダウングレードします。

STEP 1 | 現在の構成ファイルのバックアップを保存します。

設定のバックアップはファイアウォールで自動的に作成されますが、アップグレードの前にバックアップを作成して、そのバックアップを外部に保存することをお勧めします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作) Export named configuration snapshot (名前付き 設定スナップショットのエクスポート)** を選択します。
2. 実行中の設定を含む XML ファイル（**running-config.xml** など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。
3. エクスポート ファイルをファイアウォールの外部に保存します。ダウングレードで問題が発生した場合は、このバックアップを使用して設定を復元することができます。

STEP 2 | 以前の機能リリースイメージをインストールします。

自動保存バージョンは、新しいリリースにアップグレードすると作成されます。

1. 利用可能なイメージについては、**Check Now (今すぐチェック)**（デバイス > ソフトウェア）を確認してください。
2. ダウングレードするイメージを見つけます。イメージをまだダウンロードしていない場合は、**Download**（ダウンロード）します。
3. ダウンロードが完了したら、イメージを **Install**（インストール）します。
4. ダウングレード用の構成ファイルを選択します。これは、デバイスを再起動した後にファイアウォールによってロードされます。ほとんどの場合、現在ダウングレードしているリリースからアップグレードしたときに自動的に保存された構成を選択する必要があります。たとえば、PAN-OS 9.1を実行していて、PAN-OS 9.0.3にダウングレードする場合は、`autosave-9.0.3` を選択します。
5. インストールが正常に完了したら、次のいずれかの方法によって再起動します。
   - 再起動を促されたら、**Yes**（はい） をクリックします。
   - 再起動を促されなかったら、**Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。

©2023 Palo Alto Networks, Inc.

VM-Series プラグイン

VM-Series ファイアウォールには VM-Series プラグインが含まれています。これは、パブリック クラウド プロバイダーまたはプライベート クラウド ハイパーバイザーとの統合のためのビルトイン プラグイン アーキテクチャです。VM-Series プラグインは、PAN-OS とは別に手動でアップグレードできます。これにより Palo Alto Networks® は新機能、フィックス、新しいクラウド プロバイダーやハイパーバイザーとの統合を迅速にリリースできます。

VM-Series プラグインにより、VM-Series ファイアウォールとサポートされているパブリック クラウド プラットフォーム（AWS、GCP、Azure）の間のクラウド特有のやり取りを管理できるようになります。プラグインにより、クラウド監視サービス（AWS CloudWatch など）へのカスタム メトリックの公開、ブートストラップ、ユーザー認証情報の設定、パブリック クラウド環境からの情報のプロビジョニング、PAN-OS 上のクラウド ライブラリまたはエージェントのシームレスな更新を行うことができます。

VM-Series プラグインは、*VM-Series* ファイアウォールとハードウェア ベースのファイアウォールの両方に共通する機能は管理しません。たとえば、*VM Monitoring* は *VM-Series* ファイアウォールとハードウェア ベースのファイアウォールの両方の仮想マシン ワークロードに対してポリシーを一貫して適用できるようにする *PAN-OS* の中心的な機能であるため、*VM-Series* プラグインには含まれていません。

VM-Series プラグインは Panorama プラグインを管理しません。*VM-Series* プラグインと *Panorama* プラグインの違いについては、「VM-Series プラグインと Panorama プラグイン」を参照してください。

VM-Series プラグインは、アップグレードまたはダウングレードが可能な組み込みコンポーネントですが、削除できません。各 PAN-OS リリースには、PAN-OS ソフトウェア バージョンに対応する特定の VM-Series プラグイン バージョンが含まれています。古い PAN-OS ソフトウェア バージョンにダウングレードすると、プラグインもその PAN-OS バージョンと互換性のあるバージョンにダウングレードされます。仮想ファイアウォールで VM-Series プラグインをローカルにアップグレードまたはダウングレードするか、または Panorama から一元的にプラグイン バージョンを管理することができます。

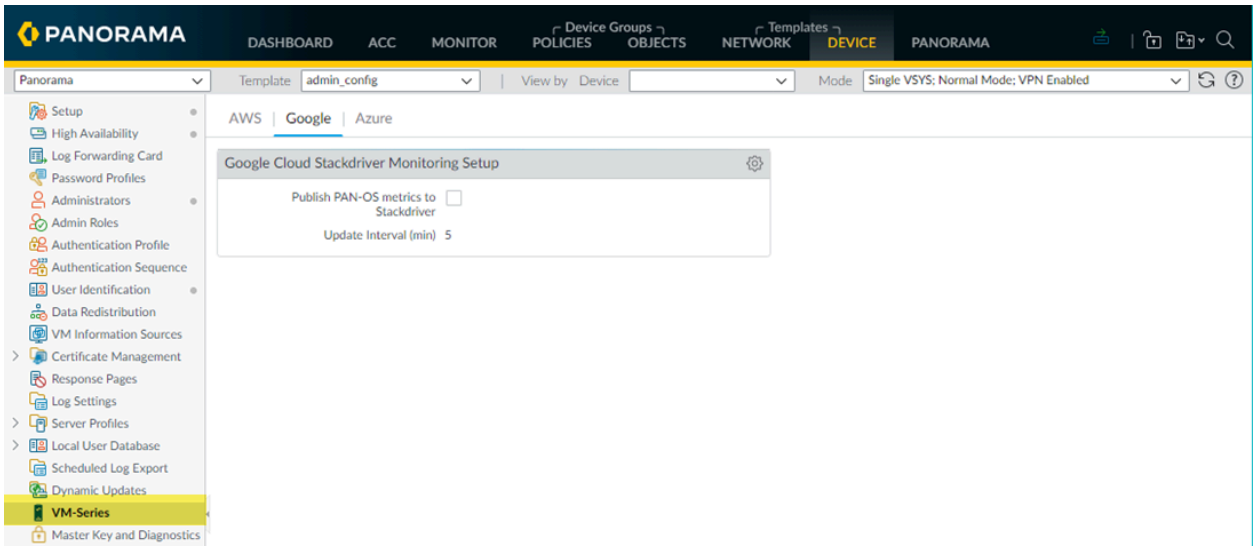
Panorama が VM-Series プラグイン バージョン自体を管理できるようにするか、または管理対象ファイアウォールのクラウド固有メトリックの公開を管理できるようにするには、「Panorama プラグイン」の説明に従って VM-Series プラグインを Panorama にインストールする必要があります。

- ファイアウォールでの VM-Series プラグインの設定
- VM-Series プラグインのアップグレード

ファイアウォールでの VM-Series プラグインの設定

Device（デバイス） > **VM-Series** を選択して、この VM-Series ファイアウォール インスタンスがデプロイされているクラウド プロバイダーのプラグイン統合を設定します。

©2023 Palo Alto Networks, Inc.



パブリック インターフェイス（VMware ESXi など）のないハイパーバイザーまたはクラウドにファイアウォールがデプロイされている場合、タブは VM-Series という名前であり、一般メッセージが表示されます。

VM-Series プラグインのアップグレード

PAN-OS とは別にプラグイン更新がリリースされた場合、（ソフトウェアまたはコンテンツの更新と同様に）VM-Series ファイアウォールまたはブートストラップ ファイルから、プラグイン バージョンを個別にアップグレードできます。

各プラグイン バージョンには PAN-OS 互換性情報と、1 つ以上のクラウド環境を対象とした新機能やバグフィックスが含まれています。

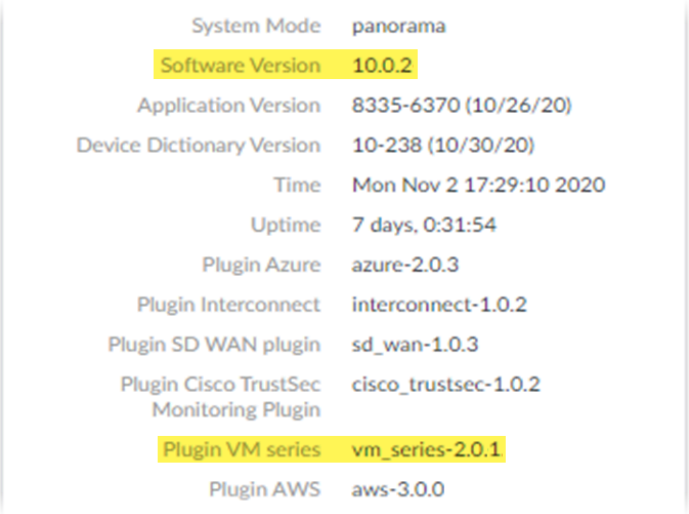
STEP 1 | アップグレード前に最新のリリース ノートを参照し、新しい VM-Series プラグインがご使用の環境に及ぼす影響について確認してください。

たとえば、新しい VM-Series プラグイン バージョンに AWS の機能だけが含まれているとします。新しい機能を利用するには、AWS の VM-Series ファイアウォール インスタンスでプラグインを更新する必要があります。

ご使用の環境に適用されないアップグレードはインストールしないでください。

©2023 Palo Alto Networks, Inc.

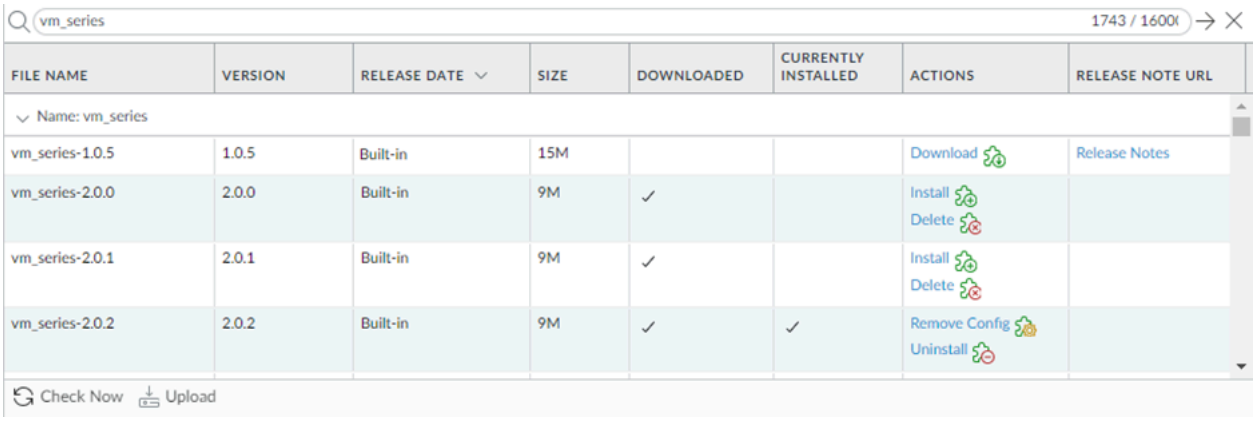
STEP 2 | VM-Series ファイアウォールにログインし、ダッシュボードでプラグインのバージョンを確認します。



STEP 3 | **Panorama** > プラグインを選択し、検索フィールドに **`vm_series`** と入力します。

[今すぐチェック]を選択して、使用可能なバージョンを表示します。

STEP 4 | VM-Series プラグインのバージョンを選択して、ダウンロードをクリックします。

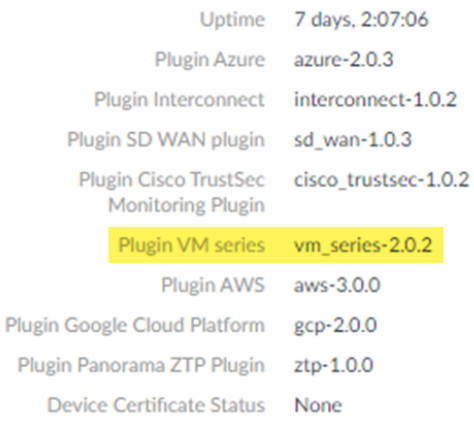


STEP 5 | ダウンロードが完了したら、[アクション]列の[インストール]をクリックします。

プラグインの以前にインストールされているバージョンは、自動的にアンインストールされます。

©2023 Palo Alto Networks, Inc.

STEP 6 | ダッシュボードで、プラグインが正常にアップグレードされたことを確認してください。



©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールでのジャンボフレームの有効化

レイヤー 3 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）はデフォルトで 1500 バイトに設定されています。このサイズはインターフェイスごとに、手動で 512 バイトから 1500 バイトの間で変更することができます。設定項目によっては MTU 値が 1500 バイト以上の Ethernet フレームを必要とするものがあります。これらをジャンボ フレームと呼びます。

ファイアウォールでジャンボ フレームを使用する場合、グローバルレベルでジャンボ フレームを有効化する必要があります。ジャンボ フレームが有効化された場合、すべてのレイヤー 3 インターフェイスのデフォルト MTU サイズは 9192 バイトに設定されます。このデフォルト値は再度 512 バイトから 9216 バイトの間の値に設定し直すができます。

グローバル ジャンボ フレームのサイズを設定すると、その値はインターフェイス設定で個別に MTU 値を設定されない限り、すべてのレイヤー 3 インターフェイスのデフォルト値となります。しかし、これでは一部のインターフェイスのみジャンボ フレームを交換させたい場合に問題となります。こういった場合には、デフォルト値を適用したくないレイヤー 3 インターフェイスすべてにおいて MTU 値を設定していく必要があります。

以下の手順において、ファイアウォールでジャンボ フレームを有効化し、すべてのレイヤー 3 インターフェイスの MTU 値の設定を行い、特定のインターフェイスにおいて個別の値を設定していきます。

複数の *NUMA* ノードでデプロイされた *VM-Series* のファイアウォールインスタンスは、ジャンボフレームサポートが有効になっているときはパケット *MMAP* モードで起動します。複数の *NUMA* ノードでデプロイされた *VM-Series* ファイアウォールインスタンスで *DPDK* を使用するには、ジャンボフレームのサポートを無効にする必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | ジャンボ フレームを有効化し、デフォルトのグローバル MTU 値を設定します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Session**（セッション）を選択し、Session Settings（セッション設定）のセクションを編集します。
2. **Enable Jumbo Frame**（**Jumbo Frame** の有効化）を選択します。
3. **Global MTU**（グローバル **MTU**）用の値を入力します。

   デフォルト値は 9192 です。値の許容範囲は次の通りです:512 - 9216
4. **OK**をクリックします。

   ジャンボ フレームを有効または無効にするには再起動が必要であり、レイヤー 3 インターフェイスが **Global MTU**（グローバル **MTU**）の値を継承するという内容のメッセージが表示されます。
5. **Yes**（はい）をクリックします。

   ジャンボ フレームのサポートが有効化され、この変更を適用するにはデバイスの再起動が必要なことを知らせるメッセージが表示されます。
6. **OK**をクリックします。
7. **Commit**（コミット）をクリックします。

STEP 2 | レイヤー 3 インターフェイス用の MTU 値を設定し、ファイアウォールを再起動します。

インターフェイス用に設定された値はグローバル *MTU* 値よりも優先されます。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス）を選択します。
2. レイヤー 3 **Interface type**（インターフェイス タイプ）のインターフェイスを選択します。
3. **Advanced**（詳細） > **Other Info**（その他の情報）を選択します。
4. **MTU** 用の値を入力します。

   デフォルト値は 9192 です。値の許容範囲は次の通りです:512 - 9216
5. **OK**をクリックします。
6. **Commit**（コミット）をクリックします。
7. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Reboot Device**（デバイスの再起動）を選択します。

©2023 Palo Alto Networks, Inc.

ハイパーバイザーによって割り当てられた MAC アドレス

デフォルトでは、VM-Series ファイアウォールは、ホストまたはハイパーバイザーによって物理インターフェースに割り当てられた MAC アドレスを使用して、レイヤー 3 インターフェースを備えた VM-Series ファイアウォールをデプロイします。これで、ハイパーバイザーが割り当てられたMACアドレスをファイアウォールがARPレスポンス内で使用できるようになります。この機能により、VMware vSwitchのような非学習性スイッチはvSwitchで無差別モードを起動することなく、ファイアウォールのデータプレーンへトラフィックを転送することが可能になります。無差別モードあるいはハイパーバイザーによって割り当てられたMACアドレスのいずれも無効化されている場合、宛先のインターフェイス用MACアドレスとホストにより割り当てられたMACアドレスの不一致を検知した際に、ホストはフレームを落とします。

AWS および *Azure* においてハイパーバイザーが割り当てた *MAC* アドレスの使用を有効または無効にするオプションはありません。どちらのプラットフォームでもデフォルトで有効であり、無効にはできません。

レイヤー 2、バーチャル ワイヤ、またはタップ インターフェイス モードを使用して VM-Series ファイアウォールをデプロイしている場合は、ファイアウォールが接続先されている仮想スイッチで無差別モードを有効にする必要があります。ファイアウォールが通常はゲスト仮想マシンのデフォルト ゲートウェイになっているレイヤー 3 のデプロイ環境でのみ、ハイパーバイザーが割り当てられた MAC アドレスを使用できます。

VM-Series ファイアウォール上で、ハイパーバイザーによって割り当てられた MAC アドレスの機能が有効である場合は、以下の要件に注意してください。

- インターフェイスの **IPv6** アドレス – アクティブ/パッシブ HA 環境（「VM-Seriesの高可用性」参照）において、IPv6 アドレスを使用するレイヤー 3 インターフェイスでは、EUI-64 により生成されたアドレスをインターフェイス識別子（インターフェイス ID）として使用してはなりません。これは、EUI-64 が 48 ビットの MAC アドレスを使用しインターフェイス用の Ipv6 アドレスを抽出しているため、IP アドレスがスタティックではないからです。フェイルオーバーが発生した際に VM-Series ファイアウォールをホストしているハードウェアが変更されると、結果として、HA ピアの IP アドレスも変わってしまい、最終的には HA に障害が発生してしまいます。
- **IP**アドレスのリース - MACアドレスが変更されると、本来のIPアドレスのリースが解除されてしまう可能性があるため、DHCPクライアント、DHCPリレー、およびPPPoEインターフェイスは、IPアドレスを解放する可能性があります。
- **MAC**アドレスと**Gratuitous ARP** - 高可用性設定の中に配置され、ハイパーバイザーによって割り当てられた MAC アドレスを持つVM-Series ファイアウォールは、MACのアドレス指定に関してハードウェアアプライアンスとは異なる挙動を示します。ハードウェアのファイアウォールは、HA ペアのデバイス間において自己生成したフローティング MAC アドレスを使用し、各データプレーンで使用される固有の MAC アドレス（たとえば eth1/1）は、HAの両方のピアがデータプレーンインターフェイスと共通する仮想 MAC アドレスに置き換えられます。HA環境内のVM-Seriesファイアウォールにおいてハイパーバイザーにより割り当てられたMACアドレスの使用を許可した場合、仮想MACアドレスは使用されません。各HAピアの

 ©2023 Palo Alto Networks, Inc.

データプレーンインターフェイスは固有のもので、ハイパーバイザーにより特定されたものです。

各データプレーンインターフェイスは固有のMACアドレスを保有しているため、フェイルオーバー発生時には、周囲のデバイスに新しいMAC/IPアドレスペアを周知するためにも、アクティブとなったVM-Seriesファイアウォールからgratuitous ARPを送る必要があります。このことから、ステートフルフェイルオーバーを有効にするには、ネットワークデバイスは Gratuitous ARP をブロックあるいは無視しないようにする必要があります。必要な場合には必ず、相互ネットワークデバイスの対 ARP ポイズニング機能を無効にしてください。

以下の手順を実行して、ホストまたはハイパーバイザーによって割り当てられたインターフェイス MAC アドレスを VM-Series ファイアウォールで使用できるようにします。

STEP 1 | デバイス > 管理 > セットアップ > 一般設定を選択します。

STEP 2 | 編集アイコンをクリックします。

STEP 3 | [ハイパーバイザー割り当ての **MAC** アドレスの使用]オプションにチェックを付けます。

MACアドレスに変更がある場合、ファイアウォールはこの変更を記録するシステムログを生成し、インターフェイスはgratuitous ARPを生成します。

STEP 4 | **OK** をクリックします。

STEP 5 | ファイアウォールへの変更を**Commit**（コミット）します。ファイアウォールを再起動する必要はありません。

©2023 Palo Alto Networks, Inc.

監視用に公開されるカスタム PAN-OS メトリック

ファイアウォールは、パブリック クラウドの監視システム（AWS®CloudWatch、Azure®Application Insights、Google®Stackdriver など）に次のメトリックをネイティブに公開します：これらのメトリックを使用すると、ファイアウォールのパフォーマンスと使用パターンを評価し、アラームを設定し、 VM-Series ファイアウォールのインスタンスを起動または終了するなどのイベントを自動化するアクションを実行できます。これらのメトリックはファイアウォールのコンテンツ更新を通じて公開されるため、 VM-Series ファイアウォールでこの機能を有効にするために必要なコンテンツリリースのバージョンが最小限であることを確認してください。

メトリック	説明
データプレーン **CPU** 使用率（**%**）	ファイアウォールのデータプレーン CPU 使用率を監視してトラフィック ロードを測定します。
データプレーン パケット バッファ使用率（**%**）	データプレーン バッファの使用状況を監視し、バッファ使用率を測定します。トラフィックが突発的に増加することがある場合は、バッファ利用率を監視することにより、ファイアウォールがデータプレーン バッファを使い果たした結果パケットが破棄されてしまうことを防止できます。
GlobalProtect™ ゲートウェイのアクティブ トンネル	GlobalProtect としてデプロイされたファイアウォールでアクティブな GlobalProtect セッションの数をモニターします。この VM-Series ファイアウォールを VPN ゲートウェイとして使用してリモート ユーザーを保護する場合は、このメトリックを使用します。ご利用のファイアウォールのモデルでサポートされているアクティブなトンネルの最大数をデータシートで確認してください。
GlobalProtect ゲートウェイ トンネル使用率（**%**）	ゲートウェイ上のアクティブな GlobalProtect トンネルを監視し、トンネル利用率を測定します。この VM-Series ファイアウォールを VPN ゲートウェイとして使用してリモート ユーザーを保護する場合は、このメトリックを使用します。
panSessionConnectionsPerSecond	一秒あたりの新規接続確立レートを監視します。
panSessionThroughputKbps	スループット（Kbps）を監視します。
panSessionThroughputPps	一秒あたりのパケット数を監視します。
アクティブなセッション	ファイアウォールでアクティブなセッションの合計数をモニターします。アクティブなセッションとは、ポリシーで

©2023 Palo Alto Networks, Inc.

メトリック	説明
	必要とされる場合に、パケットが検査および転送されるフロー ルックアップ テーブルにあるセッションのことです。
セッション使用率（%）	現在アクティブなTCP、UDP、ICMP、および SSL のセッション、ならびにパケット レート、新しい接続確立レート、およびファイアウォール スループットを監視して、セッション使用率を判断します。
SSL プロキシ使用率（%）	SSL/TLS 復号化のためにクライアントとの SSL 転送プロキシ セッションの割合をモニターします。

これらのメトリックを公開するには、以下を参照してください：

- VM-Series ファイアウォールでの CloudWatch モニタリングの有効化
- VM-Series ファイアウォールでの Azure Application Insights の有効化
- VM-Series ファイアウォールでの Google Stackdriver モニタリングの有効化

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォール上の外部サービスへのアクセスに使用されるインターフェイス

ライセンスおよびソフトウェアとコンテンツの更新を取得し、デプロイ中の仮想マシンを監視するためにカスタム PAN-OS メトリックを公開したり、IP アドレスとタグのマッピングを取得したりするために Palo Alto Networks サーバーにアクセスするには、VM-Series ファイアウォールは、下記の通りです。サポートされている管理インターフェイスの代わりにデータプレーン インターフェイスを使用するには、ファイアウォールがサーバーまたはサービスにアクセスするために使用できるデータプレーン インターフェイスを指定するサービス ルートを設定する必要があります。

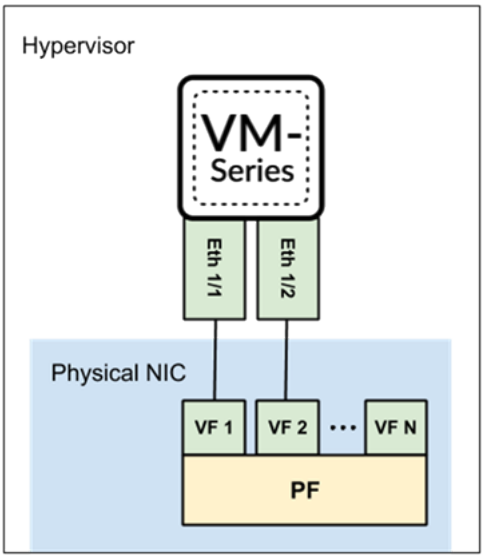
サーバーまたはサービスへのアクセス	VM-Series ファイアウォールで使用されるインターフェイス
ライセンス	管理インターフェイスのみ
ソフトウェア更新	管理インターフェイスまたはサービス ルート
AWS S3 バケット、Azure ストレージ ファイル サービス、Google ストレージ バケットなどのクラウド ストレージの場所からのブートストラップ	インターフェイスがスワップされたときを含む管理インターフェイスのみ *bootstrap.xml* ファイルにライセンスの認証コードが含まれている場合、サービス ルートを使用することはできません。ファイアウォールのライセンスを取得するには、管理インターフェイスを使用する必要があります。
AWS CloudWatch、Azure Application Insights、Google Stackdriver などのクラウド監視サービスに PAN-OS メトリックを公開	インターフェイスがスワップされたときを含む管理インターフェイスのみ
VM 監視	管理インターフェイスまたはサービス ルート

©2023 Palo Alto Networks, Inc.

PacketMMAPおよびDPDK配信サポート

シングルルート I/O 仮想化（SR-IOV）は、VM-Seriesファイアウォール上の仮想機能（VF）ドライバと、ホスト（ハイパーバイザー）上の物理機能（PF）ドライバ間の通信に依存しています。ホストはPFドライバを使用して物理NICと対話し、VM-SeriesファイアウォールはVFドライバを使ってPFドライバと対話します。

次の図は、この概念を簡単に視覚化したものです。



SR-IOV

なぜSR-IOVを使用するのか？SR-IOVは、仮想マシンがNICから直接パケットにアクセスするための高速化テクノロジーです。対照的に、仮想スイッチを使用する際には、ホストがパケットを処理し、仮想スイッチ経由でパケットを送信し、その後仮想マシンがそのパケットを受信します。

互換性マトリックスで、「PacketMMAPドライバのバージョン」には、VM-Seriesファイアウォールのホストのバージョンとネイティブドライバのバージョンの両方が記載されています。たとえば、ホストではi40eで、ファイアウォールではi40e（PCIパススルー用）およびi40evf（SR-IOV用）となっています。

SR-IOVで、i40e PFドライバを使用するNICを考えてみましょう。ホストはNICとi40eドライバを介して通信します。VM-SeriesファイアウォールはそのVFドライバ（i40evf）を使って、ホストのPFドライバと直接通信することができます。これにより、VM-Seriesファイアウォールは直接アクセスが可能になり、パケットの処理速度が向上します。互換性を保つために、ホストPFドライバのバージョンは、ネイティブのPFドライバのバージョンより後のものをインストールしてください。

PCIパススルー

なぜVM-Seriesファイアウォールはネイティブの PFドライバを持っているのでしょうか？「ネットワーク上でVM-Seriesをアタッチするためのオプション」に記載しているように、PCIパススルーを使用する場合、VM-Seriesファイアウォール用にNICが予約されるため、ホスト（また

©2023 Palo Alto Networks, Inc.

はホスト上のその他のゲスト）はNICにアクセスできません。PCIパススルー構成では、VM-Seriesファイアウォールはネイティブのpfドライバを使って直接ホストNICと通信を行います。

ホストにインストールするPFドライバのバージョンを判断するには、「PacketMMAPドライバのバージョン」リストを参照してください。VM-Seriesファイアウォールのネイティブpfドライバよりも上位のバージョンのPFをインストールしてください。

PCIパススルーについては、「ESXi 上の SR-IOV の有効化」および「KVM 上の SR-IOV の有効化」を参照してください。

DPDK

PAN-OSには、DPDK（デフォルト）とMMAPの2種類のパケット処理モードが用意されており、VM-Seriesファイアウォール上にそれぞれのモードに対応するネイティブドライバが存在しています。たとえば、ファイアウォールがDPDKモードの場合、ファイアウォールはバージョンがDPDK i40evfのドライバを使ってホストのi40eドライバと通信します（SR-IOVを使用する場合）。ファイアウォールがパケットMMAPの場合は、別のバージョンのi40evfドライバを使ってホストのi40eドライバと通信します。

ホスト（ハイパーバイザー）上、またはゲスト（VM-Seriesファイアウォール）上でDPDKを有効にすることができます。両方を有効にすると、最良の結果を得られます。

- DPDKによるOVSのコンパイルは、ホスト上でDPDKを有効にする処理の一部です。

  「ホストでの OVS および DPDK の設定」を参照してください。
- VM-Series DPDKはVM-Seriesファイアウォール上のネイティブDPDKドライバを有効にするため、 ホスト上でDPDKを有効にする必要はありませんが、最高のパフォーマンスを確保するために有効にすることをお勧めします。

©2023 Palo Alto Networks, Inc.

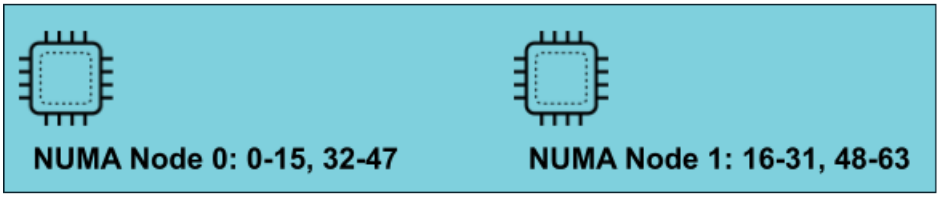
VM-Series での NUMA パフォーマンス最適化の有効化

VM-Series ファイアウォールのパフォーマンスを向上させるために、Non-Uniform Memory Access （NUMA）パフォーマンスの最適化を有効にすることができます。NUMA パフォーマンスの最適化が有効になっている場合、VM-Series ファイアウォールデータプレーンは NUMA ノード 0 に接続された vCPU を使用します。VM-Series ファイアウォールデータプレーンは、NUMA ノード 0 に属する vCPU のみを使用します。VM-Series 管理プレーンはコア 0 を使用し、NUMA ノード 0 の残りの vCPU は VM-Series データプレーンで使用できます。この機能には、PAN-OS 10.1.1 以降および VM-Series プラグイン 2.1.1 以降が必要です。

NUMA パフォーマンスの最適化は、PAN-OS 10.1 ではデフォルトで無効になっています。

2 つの NUMA ノードに 64 コアが組み入れられたデバイスがある場合、NUMA パフォーマンスの最適化を有効にしないと、VM-Series ファイアウォールで使用されるデータプレーン vCPU が異なるノード上にある可能性があり、パフォーマンスに影響します。たとえば、次の例に示すようにシステムが編成されていて、合計 32 個のコアと 24 個のデータプレーンコアを備えた VM-Series ファイアウォールをデプロイするとします。NUMA パフォーマンスの最適化がない場合、VM-Series ファイアウォールは、ノードの場所に関係なくコアを番号順に割り当てるため、ノード 0 でコア 1～15、ノード 1 で 16～24 を使用します。NUMA 最適化を有効にすると、VM-Series はノード 0 のコアのみを使用します。この場合、番号の順序に関係なく、1 から 15 および 33 から 39 になります。データプレーンで使用されていないコアはすべて管理プレーンに割り当てられます。

VM-Series ファイアウォールに割り当てられたコアの数がノード 0 の vCPU の数を超える場合、VM-Series はノード 0 のすべてのコアを使用しますが、他のノードのコアは使用しません。たとえば、VM-Series ファイアウォールに 30 コアを割り当てたが、ノード 0 には 24 コアしかない場合、VM-Series ファイアウォールはノード 0 の 24 コアのみをデータプレーンに使用します。



STEP 1 | VM-Series CLI にログインします。

STEP 2 | 以下のコマンドを実行します。

```
request plugins vm_series numa-perf-optimize enable on
```

以前の NUMA パフォーマンスの最適化：なし

要求された NUMA パフォーマンスの最適化：有効

PA-VM を再起動してください。

©2023 Palo Alto Networks, Inc.

STEP 3 | 再起動が完了したら、VM-Series CLI にログインし、NUMA 最適化が有効になっていることを確認します。

```
show plugins vm_series numa-perf-optimize
```

```
NUMA パフォーマンスの最適化：有効
```

STEP 4 | データプレーンコアの数を確認します。

```
show plugins vm_series dp-cores
```

```
デバイスの現在の DP コア：15 （合計コア：16）
```

STEP 5 | NUMA パフォーマンスの最適化を無効にするには、次のコマンドを使用します。このコマンドでは、VM-Series ファイアウォールを再起動する必要があります。

```
request plugins vm_series numa-perf-optimize enable off
```


©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールでの ZRAM の有効化

VM-Series ファイアウォールでメモリ低下またはメモリ不足の状態が発生した場合は、ZRAM を有効にして、メモリ使用量を改善できます。ZRAM は、compcache（圧縮キャッシュ）とも呼ばれ、圧縮されたブロックデバイスを RAM で作成するための Linux カーネルモジュールです。有効にすると、ZRAM はスワップディスクとして使用され、RAM に常駐するため、スワップの入出力が高速になります。

ZRAM を有効にするには、次の手順を実行します。

STEP 1 | VM-Series CLI にログインします。

STEP 2 | 次の CLI コマンドを使用して、VM の合計メモリを見つけます。

grep pattern “KiB Mem :” mp-log mp-monitor.log

```
KiB Mem :  9202656 total,   566504 free,  3475840 used,  5160312
 buff/cache
KiB Mem :  9202656 total,   497112 free,  3481944 used,  5223600
 buff/cache
KiB Mem :  9202656 total,   511744 free,  3466768 used,  5224144
 buff/cache
KiB Mem :  9202656 total,   511668 free,  3466340 used,  5224648
 buff/cache
KiB Mem :  9202656 total,   512124 free,  3465700 used,  5224832
 buff/cache
KiB Mem :  9202656 total,   511436 free,  3465976 used,  5225244
 buff/cache
KiB Mem :  9202656 total,   510984 free,  3465944 used,  5225728
 buff/cache
```

STEP 3 | 上記の合計メモリを KB から MB に変換します。以下に例を示します。

9202656 / 1024 = 8987 MB

メモリの合計値 (MB) を書き留めます。この値は、次のステップで必要になります。

STEP 4 | 次の 2 つの CLI コマンドを使用して ZRAM を有効にします。

debug software kernelcfg zram-swap enable

debug software kernelcfg zram-swap modify host-mem-threshold <total-memory-in-MB>

STEP 5 | VM-Series ファイアウォールを再起動します。

STEP 6 | ZRAM が有効になっていることを確認します。

debug software kernelcfg zram-swap show config

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのライセンス

VM-Series ファイアウォールは、2 つのライセンスタイプ（BYOL と PayGo）と 2 つの異なるライセンスモデル（デプロイメントプロファイルで指定する柔軟な構成のためのソフトウェア次世代ファイアウォールクレジット（ソフトウェア NGFW）と、固定の VM-Series モデル構成）をサポートします。どちらのモデルも、セキュリティサービスおよびその他の機能のライセンス供与も行います。

認定 CSSP パートナーの方は、「クラウド セキュリティ サービス プロバイダー（CSSP）用ライセンス」で関連情報を確認してください。

サポートアカウントの作成とライセンスの管理の詳細については、次のトピックを参照してください。

- VM-Series ファイアウォールライセンス
- サポート アカウントの作成
- VM-Series ファイアウォールのシリアル番号と CPU ID フォーマット
- ライセンス API
- ライセンス API キーのインストール
- Panorama ベースのソフトウェアファイアウォールライセンス管理の使用
- Software NGFW Credits
- VM-Series モデル
- クラウド セキュリティ サービス プロバイダー（CSSP）用ライセンス

VM-Series ファイアウォールライセンス

この章では、次のライセンス情報を比較します。

- ライセンスタイプ:BYOL と PayGo の比較
- フレキシブル vCPU と固定モデルライセンス:フレキシブル vCPU と固定モデルの比較）
- フレキシブル vCPU と固定モデルのデプロイメント:フレキシブルモデルと固定モデルのデプロイメント手順のサマリー。

ライセンスタイプ

Palo Alto Networks は現在、次の 2 種類のライセンスタイプをサポートしています。Bring Yown License (BYOL) および PAYG (Payas-You-Go、PayGoとも呼ばれる)。

タイプ	説明
BYOL	Software NGFW Credits—すべての PAN-OS リリースを実行している VM-Series ファイアウォールで使用できます。PAN-OS バージョン 10.0.4 以降を実行している VM-Series ファイアウォールは、機能の高度化と柔軟性の強化を実現しています。フレキシブルライセンスのコストは、vCPU の数、有効にしたセキュリティサービス、Panorama をプロビジョニングしてファイアウォールを管理するのかまたはログコレクタとして機能するのかに基づいて決まります。 詳細な説明については、Software NGFW Creditsを参照してください。
BYOL	VM-Series モデルのライセンス - すべての PAN-OS リリースで使用できます。vCPU の数は、選択した VM シリーズモデルに応じて固定されています。 *PAN-OS 10.0.4* 以降で利用可能なフレキシブル *vCPU* は、機能の高度化と *vCPU* 数の増大をサポートします。 キャパシティライセンスのコストは、VM-Series モデル、デバイスメモリ、ストレージコスト、およびサポート資格がベースになります。セキュリティサービスとファイアウォールを管理するための Panorama デプロイは追加コストになります。キャパシティライセンスのタイプは次のとおりです。 • **VM-Series エンタープライズ ライセンス契約（マルチモデル ELA）**：VM-Series ファイアウォールの包括的な 1 年または 3 年間のライセンス契約。個々のライセンスに、Panorama のモデル、セキュリティサービス、サポート資格、およびオプションのデバイス管理ライセンスを組み入れることができます。 マルチモデル ELA はトークンプールを特徴とし、そこからトークンを割り当てて VM-Series ファイアウォールのライセンス処理を行います。（これは ELA に固有のものであり、Software NGFW Credits プールと同じではありません）。 • サポート資格またはセキュリティサービスのバンドル 1 またはバンドル 2 を備えた永続的な VM-Series モデルのキャパシティライセンス。

©2023 Palo Alto Networks, Inc.

タイプ	説明
	• サポート資格と任意選択のセキュリティサービスが付帯する期間ファイアウォールキャパシティライセンス。
PayGo	パブリッククラウドマーケットプレイス (AWS、Azure、GCP など) またはクラウドセキュリティサービスプロバイダー (CSSP) から購入します。ご使用のプロバイダーがサポートする PAN-OS バージョンで使用できます。 9.1.1 より前の PAN-OS バージョンでは、PayGo は VM-Series VM-300 モデルのみをサポートしていました。PAN-OS 9.1.1 以降では、PayGo は固定モデルをサポートできます。VM-100、VM-300、VM-500、VM-700 などの従来の VM モデルがサポートされます。

フレキシブル vCPU と固定モデルライセンス

フレキシブル vCPU ソフトウェア NGFW ライセンスと固定 vCPU VM-Series モデルライセンスの違いは何ですか。それらは、対象物が異なれば請求方法も異なり、それぞれの資金調達法も異なります。次の表に、簡単な比較とそれ以上の詳細へのリンクを示します。

	フレキシブル **vCPU**	**VM-Series** モデル（固定 **vCPU**）
の意味	コストは、vCPU の数と選択したセキュリティサービスに基づきます。 Panorama には、消費する vCPU 以外に費用はかかりません。 再利用可能な Software NGFW credit を購入すると、所定の期間の終了時に失効します。クレジットを有効化した後、クレジットプールに分割することができます。 クレジットを使用するには、クレジットプロファイルを選択し、1 つ以上のデプロイメントプロファイルを作成します。次のような、プラットフォームとしてのファイアウォールコンポーネントの独自の組み合わせを選択します。VM-Series vCPU、セキュリティサービス、管理または専用ログ収集のための仮想 Panorama、およびサポート資格。プロファイルを使用してデプロイされたすべてのファイアウォールは、同じ認証コードでライセンスを付与され、デプロ	コストは、VM-Series モデルのキャパシティライセンス、デバイスメモリ、およびストレージに基づきます。Panorama サービスとセキュリティサービスは別々に購入できます。 • VM-Series エンタープライズ ライセンス契約（マルチモデル ELA）：VM-Series ファイアウォールの包括的な 1 年または 3 年間のライセンス契約。 マルチモデル ELA はトークンプールを特徴とし、そこからトークンを割り当てて VM-Series ファイアウォールのライセンス処理を行います。 • サポート資格またはセキュリティサービスのバンドル 1 またはバンドル 2 を備えた永続的な VM-Series モデルのキャパシティライセンス。 • サポート資格と任意選択のセキュリティサービスが付帯する期間

©2023 Palo Alto Networks, Inc.

	フレキシブル vCPU	VM-Series モデル（固定 vCPU）
	イメントプロファイルから管理できます。	ファイアウォールキャパシティライセンス。
アクティベーション	アクティベーションメールが必要です。アクティベーションと登録は自動的に行われます。	アクティベーションメールと、アクティベーション後に別の登録手順が必要です。
セキュリティサービス	脅威防御、DNS セキュリティ、GlobalProtect、WildFire、URL フィルタリング、SD-WAN、DLP、およびその他のサービスが利用可能になったとき。 デプロイメントプロファイルを作成するときは、セキュリティサービスを任意に組み合わせて選択できます。セキュリティサービスは、プロファイルからいつでも追加または削除できます。	バンドル **1**:脅威防御とプレミアムサポート資格。 バンドル **2**:脅威防御、DNS セキュリティ、GlobalProtect、WildFire、URL フィルタリング、SD-WAN、DLP、およびプレミアムサポート資格。
PAN-OS バージョン	10.0.4 以降を実行しているファイアウォールに対して最大 64 個のフレキシブル vCPU と高度なサービスオプション。	VM-Series モデル（固定 vCPU）は、任意の PAN-OS バージョンで展開できます。
資金調達	プラットフォームとしてのファイアウォールコンポーネントを使用できる再利用可能なクレジット。 クレジットを購入したら、クレジットをアクティベートし、組織の特定のアカウントに関連付ける必要があります。アクティベートされたクレジットは、デプロイメントロファイルの作成で使用するクレジットプールに資金を提供します。 ファイアウォールのデプロイ時には、クレジットが消費されます。ファイアウォールを非アクティブ化すると、クレジットは解放され、後の使用に備えてクレジットプールに戻されます。	• マルチモデル ELA: トークン。 • サポート資格またはセキュリティサービスのバンドル 1 またはバンドル 2 を備えた永続的な VM-Series モデルのキャパシティライセンス。構成は購入時に決定します。新しいライセンスを購入しない限り、設定を変更することはできません。 • サポート資格と任意選択のセキュリティサービスが付帯する期間ファイアウォールキャパシティライセンス。
デプロイメント設定	フレキシブル。デプロイメントプロファイルはいつでも変更できます。プロファイルに加えた変更は、デプロ	VM-Series モデルのキャパシティは変更されませんが、ELA がある場合

©2023 Palo Alto Networks, Inc.

	フレキシブル vCPU	VM-Series モデル（固定 vCPU）
	イメントプロファイル認証コードを共有するすべてのファイアウォールに反映されます。	は、セキュリティサービスを追加できます。 永久ライセンスと期間ライセンスは事前に設定されて前払いされ、変更されることはありません。
デプロイメント	クレジットのアクティベーション後、特定の環境またはユースケース（「NSX 環境の保護」など）のデプロイメントプロファイルを作成し、ファイアウォール vCPU、セキュリティサービス、およびオプションの仮想 Panorama を構成します。デプロイメントプロファイルはいくつでも作成でき、いつでもカスタマイズできます。 Software NGFW creditをアクティベートおよび管理するには、カスタマーサポートポータルのクレジット管理者 (アカウント管理にのみ該当) のロールが必要です。	VM-Series ELA に同意します。VM-Series ファイアウォールをデプロイして設定します。モデルライセンスをアクティベートし、ファイアウォールを登録します。
Panorama	デプロイメントプロファイルを作成するときに、管理用に Panorama を追加するか、あるいはデプロイメントプロファイルを使用するファイアウォールの専用ログコレクタとして追加するかを選択できます。この Panorama は、デプロイメントプロファイルの共有認証コードでデプロイされたファイアウォールを管理できます。	Panorama は別売りです。物理または仮想の Panorama は、ファイアウォール管理またはログ収集に使用できます。
アップグレードまたはダウングレード	VM-Series ファイアウォールまたは Panorama にインターネット接続がある場合、デプロイメントプロファイルに対する変更は、ファイアウォールに自動的に適用されます。 ファイアウォールにインターネット接続がない場合は、ファイアウォールを手動で停止します。[アセット] > [Software NGFW Credit] でデプロイメントプロファイルを変更し、CSP でライセンスキーをダウンロードして	別のモデルに変更するには、ライセンスの変更と再起動が必要です。

©2023 Palo Alto Networks, Inc.

	フレキシブル vCPU	VM-Series モデル（固定 vCPU）
	VM に転送し、CSP からプロファイルを取得し、VM に転送し、VM を再起動してライセンスを適用します。 いずれの場合も、ファイアウォールを再起動する必要はありません。	

フレキシブル vCPU と固定モデルのデプロイメント

次のチェックリストでは、Software NGFW Credit のデプロイメントプロセスと VM-Series モデルのライセンス方法を比較します。

フレキシブル vCPU	固定 vCPU（VM-Series モデル）
1. サポート アカウントの作成. 2. クレジットのアクティベート. 組織は、さまざまなコストセンターを表す多数のアカウントを持つことができます。登録時に、クレジット購入をアカウントに関連付けます。 3. デプロイメントプロファイルの作成. 4. Alibaba, AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、 Hyper-V、KVM、OpenStack に VM-Series ファイアウォールを展開します。Oracle Cloud Infrastructure、vCloud Air、NSX-T、NSX-V。 5. VM-Seriesファイアウォールへのデバイス証明書のインストール (Cortex Data Lake や Auto Focus などのサイトライセンスの場合)。	1. サポート アカウントの作成. 2. VM-Series モデルライセンスのアクティベート. 3. VM-Series ファイアウォールの登録. 4. Alibaba, AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、 Hyper-V、KVM、OpenStack に VM-Series ファイアウォールを展開します。Oracle Cloud Infrastructure、vCloud Air、NSX-T、NSX-V。 5. VM-Seriesファイアウォールへのデバイス証明書のインストール (Cortex Data Lake や Auto Focus などのサイトライセンスの場合)。

©2023 Palo Alto Networks, Inc.

サポート アカウントの作成

カスタマーサポートポータル（CSP）にログインするには、サポートアカウントが必要です。Software NGFW credit をアクティベートおよび管理したり、ソフトウェアアップデートにアクセスしたり、Palo Alto Networks のテクニカルサポートでケースを開いたりするには、ログインする必要があります。さらに、サポートアカウントでは Palo Alto Networks で登録したすべてのアセット（アプライアンス、ライセンス、サブスクリプション）を閲覧および管理することもできます。

現在 AWS からのみ購入可能な従量制ライセンスを除き、すべてのライセンスオプションには、VM-Series ファイアウォールのインストールに必要なソフトウェアパッケージをダウンロードするためのサポートアカウントが必要となります。

既存のサポートアカウントをお持ちの場合は、VM-Series ファイアウォールソフトウェアをダウンロードしてインストールしてから、VM-Series ファイアウォールの登録を続行できます。

STEP 1 | https://support.paloaltonetworks.com/UserAccount/PreRegister にアクセスします。

STEP 2 | サポートアカウントに関連付ける社内電子メールアドレスを入力します。

STEP 3 | 以下のいずれかのオプションを選択し、ユーザー登録フォームに詳細を入力します。

AWS の従量制ライセンスの場合

1. **Register your Amazon Web Services VM-Series Instance**（**Amazon Web Services VM-Series** インスタンスを登録）をクリックします。
2. AWS管理コンソール上で、AWS インスタンス ID、AWS製品コード、ファイアウォールをデプロイした AWS ゾーンの情報を参照します。
3. その他の情報を記入します。

それ以外のライセンスの場合

1. **Register device using Serial Number or Authorization Code**（シリアル ナンバーあるいは認証コードを使用してデバイスを登録）をクリックします。
2. キャパシティ認証コードおよび販売注文番号あるいは顧客IDを入力します。
3. その他の情報を記入します。

STEP 4 | フォームの **Submit**（送信）をクリックします。ユーザーアカウントをアクティベートするためのリンクが添付されたメールが届きます。

アカウントをアクティベートする手順を完了します。アカウントが認証され登録が完了したらサポートポータルへログインできるようになります。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのシリアル番号と CPU ID フォーマット

VM-Series ファイアウォールのインスタンスを起動すると、ファイアウォールの各インスタンスは CPU ID およびファイアウォールのシリアル番号を使用して一意に識別されます。CPU ID の形式およびシリアル番号には、ハイパーバイザに関する情報と VM-Series ファイアウォールの各インスタンスのライセンスの種類が付帯します。

- VM-Series ファイアウォールの従量制ライセンスモデルでは、起動時にファイアウォールがシリアル番号と CPU ID を生成し、これらの詳細を使用してパブリック クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）を行います。
- BYOL モデルを使用して、VM-Series ファイアウォールの固定モデルまたはフレキシブルライセンスを備えた VM-Series ファイアウォールをカスタマーサポートポータル（CSP）で登録します。
  - 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、ファイアウォールの認証コードを適用して、シリアル番号が含まれるライセンス ファイルを生成できます。
  - ファイアウォールがオフラインの場合、CSP を使用して、CPU ID、UUID、認証コードを入力し、シリアル番号が付いたライセンスファイルを生成する必要があります。その後、ファイアウォールにライセンスをインストールできます。

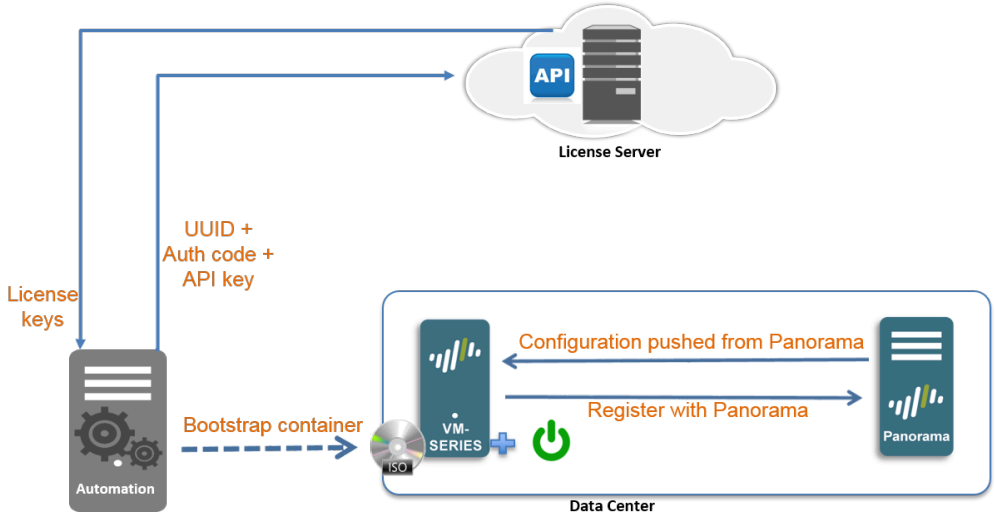
ライセンスタイプ	シリアル番号	CPU ID
BYOL	15 桁、すべて数値 例:0071 **51** 345678909	<Hypervisor>:<ActualCPUID> 例:**ESX**:12345678
PAYG	15 桁、英数字 例:**4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> 例: **AWSMP**:1234567890abcdef0:6kxdw3bbmdeda3o6i1ggqt4km:us-west1

©2023 Palo Alto Networks, Inc.

ライセンス API

ライセンス API を使用して、認証コードの登録、認証コードに添付されたライセンスの取得、ライセンスの更新、または VM-Series ファイアウォール上のすべてのライセンスの非アクティブ化を行います。さらに、ライセンス API を使用すると、インターネットに直接アクセスできず Palo ALto Networks のライセンスサーバーにアクセスできないファイアウォールにライセンスを付与できます。ライセンスを手動で管理することも、カスタムスクリプトまたはオーケストレーションサービスを使用してライセンスを自動化することもできます。

また、オフラインライセンスも含め、ライセンスタスク用の Panorama Software Firewall License プラグインを使用することもできます。プラグインには、*VM-Series* プラグイン *2.0.4* 以降を使用する *Panorama 10.0.0* 以降が必要であり、管理対象の *VM-Series* ファイアウォールは *PAN-OS9.1.0* 以降および *VM-Series* プラグイン *2.0.4* 以降を実行している必要があります。 *Azure* 用の *VM-Series* ファイアウォールには、*VM-Series* プラグイン*2.0.8*が必要です。



モデルベースのライセンスの場合、この API により、認証コードの詳細情報を表示して、認証コードあるいは認証コードバンドル（ファイアウォールの複数のインスタンスをライセンス登録することが可能）に付与された未使用のライセンスの数を確認することもできます。認証コード バンドルにはVM-Seriesモデル、サブスクリプション、さらに一度で簡単に問い合わせられるフォームになっているサポートが含まれています。複数回使用できるこのバンドルは、VM-Seriesファイアウォールをデプロイする際にライセンス登録を行えます。

このAPIを使用できるよう、各サポートアカウントに一意のキーが割り当てられています。各APIクエリはPOSTリクエストであり、ライセンスサーバーへのリクエストを認証するためのAPIキーをリクエストに含める必要があります。認証が終わると、ライセンスサーバーが json 形式（content-type application/json）のレスポンスを返します。

- ライセンス API キーの管理
- ライセンス API の使用
- ライセンス API のエラーコード

©2023 Palo Alto Networks, Inc.

- ライセンス API キーのインストール

ライセンス API キーの管理

ライセンス API を使用するのに必要な API キーを取得するには、サポート ポータルに対するスーパー ユーザー権限がアカウントに必要です。同じキーを使用して、ライセンスをアクティベートおよび非アクティブ化します。

API キーの有効期限は、サポート アカウントの最新サブスクリプションの有効期限と同じ日付です。現行のサブスクリプションを更新し、API キーの有効期限をリセットする必要がある場合は、キーを再生成する（既存のキーが使用されていた場所で既存のキーを新しいキーに置き換える）か、または Palo Alto Networks のサポートに連絡して、既存の API キーの有効期間の延期を依頼できます。

STEP 1 | ライセンス API キーを取得します。

1. スーパー ユーザー権限を持つアカウントで、Palo Alto Networks のサポート ポータルにログインします。
2. アセット > **API** キー管理を選択します。
3. [有効化]をクリックしてキーを表示し、そのキーをコピーして使用します。一度生成したキーは、キーを再生成するか、無効にするまで使用できます。

STEP 2 | API キーを再び生成、あるいは取り消します。

1. 新しい API キーを生成したり、キーの使用を取り消したりできます。
   - **Regenerate**（再び生成）をクリックして新しいキーを生成します。API キーに支障がある可能性がある場合は、新しいキーを生成できます。再生成すると、古いキーが自動的に無効になります。
   - 今後キーを使用しない場合は **Disable**（無効化）を選択します。API キーを無効化すると、キーが返却されます。

ライセンス API の使用

ライセンス API にアクセスするためのベース URI は、https://api.paloaltonetworks.com/api/license です。この URL は、実行するタスク（ライセンスのアクティベーション、ライセンスの無効化、ライセンス使用状況のトラッキングなど）に基づいて変わります。

API リクエストでは必ず HTTP POST メソッドを使用するため、apikey HTTP リクエストヘッダーに API キーを組み入れ、`content-type application/x-www-form-urlencoded` を使った URL エンコード済みフォームのデータとしてリクエストパラメータを渡す必要があります。

API バージョンは任意で、0 または 1 の値を含めることができます。指定する場合は、`version` HTTP リクエスト ヘッダーに含める必要があります。現在の API バージョンは 1 です。バージョンを指定しない場合や、バージョン 0 を指定する場合、リクエストで現在の API バージョンが使用されます。

API レスポンスはすべて json 形式で返されます。

©2023 Palo Alto Networks, Inc.

開始する前に、ライセンス API キーを取得し、ローカルドライブにコピーします。この作業は、以下のタスクを実行する前に行う必要があります。

- ライセンスのアクティベーション
- ライセンスの無効化
- ライセンス使用状況のトラッキング

ライセンスのアクティベーション

ヘッダー：apikey

パラメータ: uuid、cpuid、authCode、memory、serialNumber、vCPU

URL:https://api.paloaltonetworks.com/api/license/activate

パラメータ uuid、cpuid、authCode、および serialNumber は、PAN-OS のバージョンに関係なく、すべての VM-Series ライセンスに適用されます。

オプションのパラメータ memory および vCPU は、フレキシブル vCPU （PAN-OS 10.0.4以降）にのみ適用されます。

- 最初のライセンスアクティベーションでは、API リクエストでパラメータを指定します。以下に例を示します。

```
curl -i -H
 "apikey:a103e3065360acc5e01666fb9335964fcfe668100666db6f3ff43d4544de0###"
--data-urlencode cpuid=AWS:57060500FFFBE###
--data-urlencode uuid=EC2278FF-F0CB-45E2-343B-E97984BAC###
--data-urlencode authCode=D3521###
--data-urlencode vcpu=4
--data-urlencode memory=8388608
https://api.paloaltonetworks.com/api/license/activate
```

- ライセンスキーを保存しなかった場合や、最初のライセンスアクティベーション中にネットワーク接続で問題が発生した場合は、以前にアクティベートしたファイアウォールのライセンスを取得できます。

  API リクエストで、cpuid および uuid を指定するか、またはファイアウォールの serialNumber を指定します。

Curlを使用した初回のライセンス アクティベーション時のリクエストの例：

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F
 --data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-
urlencode authCode=I7115398 https://api.paloaltonetworks.com/api/
license/activate
```

API レスポンスの例：

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureFi--eld":
"Premium","feature_descField":"24 x 7 phone support; advanced
 replacement hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
```


©2023 Palo Alto Networks, Inc.

```
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
"typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2
"vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":null
"mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
"featureField":"Threat Prevention","feature_descField":"Threat
 Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDArj
+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl\n2qJhNq3kwXBDxn181z3nrUOsQd/
eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b\ndZBRH5AQjPoaON7xZ46VMFovOR
+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"",
"errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03T08:18:41",
"startDateField":"5/29/2016","vm_capacityField":null,"uuidField":null,
"cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,
"expirationField":"8/29/2016 12:00:00 AM","PropertyChanged":null}
...<truncated>
```


レスポンスの *feature_Field* は、*keyField* で後に続くキーのタイプを示します。各キーをテキストファイルにコピーし、拡張子を*.key*にして保存します。キーは *json* 形式であるため、改行はありません。パーサーで必要な場合は、必ず改行に変換してください。必ず各キーに適切な名前を付け、ブートストラップ パッケージの */license* フォルダに保存します。たとえば、キーのタイプを含む*authcode*を含めて名前を*I3306691_1pa-vm.key*（キャパシティ ライセンスキー用）、*I3306691_1threat.key*（脅威防御ライセンスキー用）、*I3306691_1wildfire.key*（*WildFire*サブスクリプションのライセンスキー用）にします。

Curl を使用して以前アクティベートしたライセンスを取得する **API** リクエストの例：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 serialNumber=007200006142 https://api/paloaltonetworks.com/api/
license/activate
```

API レスポンスの例：


```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureField":
"Premium","feature_descField":"24 x 7 phone support; advanced
 replacement hardware service","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs
\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","errmsgField":null,
"typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2
"vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":null
```


©2023 Palo Alto Networks, Inc.

```
"mac_countField":null,"drrField":null, "expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP",
"featureField":"Threat Prevention","feature_descField":
"Threat Prevention","keyField":
"NqaXoaFG+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==
\n","auth_codeField":"","errmsgField":null,"typeField":"SUB",
"regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2016","vm_capacityF
:null,"uuidField":null,"cpuidField":null,"mac_baseField":null,
"mac_countField":null,"drrField":null,"expirationField":"8/29/2016
 12:00:00 AM","PropertyChanged":null}
...<truncated>
```


ライセンスの無効化

URL: **https://api.paloaltonetworks.com/api/license/deactivate**

パラメータ：encryptedToken

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無効化するには、ファイアウォールでローカルにライセンス トークン ファイルを作成し、このトークン ファイルを API リクエストで使用する必要があります。ライセンストークンファイルの生成の詳細は、「VM の無効化」または「ライセンスの非アクティブ化 (Software NGFW Credit)」および「CLI を使用して機能ライセンスまたはサブスクリプションを非アクティブ化する」を参照してください。

ヘッダー：apikey

リクエスト： https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

Curl を使用してライセンスを無効化する **API** リクエストの例：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 encryptedtoken@dact_lic.05022016.100036.tok https://
api.paloaltonetworks.com/api/license/deactivate
```

API レスポンスの例：


```
[{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nul
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nul
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nul
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nul
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,"PropertyChanged":nul
{"serialNumField":"007200006150","featureNameField":"","issueDateField":"",
"successField":"Y","errorField":null,"isBundleField":null,
```


 ©2023 Palo Alto Networks, Inc.

```
"PropertyChanged":null}]$
```

ライセンス使用状況のトラッキング

URL: **https://api.paloaltonetworks.com/api/license/get**

パラメータ：authCode

ヘッダー：apikey

リクエスト: https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>

Curl を使用したライセンス使用状況のトラッキングを行う **API** リクエストの例：

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031
 https://api.paloaltonetworks.com/api/license/get
```

API レスポンスの例：

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2016 20:07:16 GMT
Content-Length: 182

{"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":
[{"UUID":"420006BD-113D-081B-F500-2E7811BE80C
9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

ライセンス API のエラーコード

ライセンスサーバーが返すHTTPのエラーコードは次通りです。

- 200 成功
- 400 エラー
- 401 不正な API キー
- 500 サーバー エラー

©2023 Palo Alto Networks, Inc.

ライセンス API キーのインストール

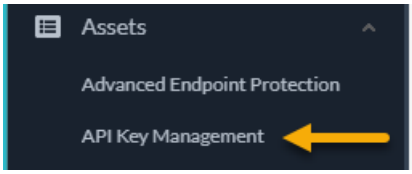
ライセンス API キーは、ライセンスをアクティベート、変更、または非アクティブ化するために使用できます。この手順は、VM-Series ファイアウォールまたは Panorama デプロイメントに適用されます。

カスタマーサポートポータルからライセンス API キーを取得し、CLI を使用してファイアウォールまたは Panorama にキーをインストールするには、スーパーユーザー権限が必要です。

Panorama で、ライセンス API キーをインストールすると、Panorama は自身の管理対象デバイスに API キーをプッシュします。管理対象デバイスに API キーがインストールされている場合、Panorama は新しい API キーで古いキーを上書きします。

STEP 1 | ライセンスの API キーをカスタマーサポートポータルから取得します。

1. カスタマー サポート ポータルにログインします。
2. **Assets**（アセット） > **Licensing API**（ライセンシング **API**）を選択します。
3. API キーをコピーします。



STEP 2 | CLI を使用して、前のステップでコピーした API キーをインストールします。キーをリクエストに貼り付けます。

```
request license api-key set key <key>
```

STEP 3 | (任意) ライセンス無効化 API キーを置き換えるには、次の CLI コマンドを使用して、インストール済みの API キーを削除します。

```
request license api-key delete
```

API キーを削除した場合、ライセンスを非アクティブ化するには、事前に別のライセンスアクティベーション解除キーをインストールする必要があります。

©2023 Palo Alto Networks, Inc.

Panorama ベースのソフトウェアファイアウォールライセンス管理の使用

Panorama ソフトウェアファイアウォールライセンスプラグインを使用すると、Panorama に接続するときに VM-Series ファイアウォールのライセンスを自動的に取得できます。VM-Series ファイアウォールがデプロイメントの境界にあり、Palo Alto Networks ライセンスサーバーに接続できない場合、ソフトウェアファイアウォールライセンスプラグインは、Panorama を使用して VM-Series ファイアウォールのライセンスを取得することにより、ライセンスのアクティベーションプロセスを簡素化します。

さらに、ソフトウェアファイアウォールライセンスプラグインは、クラウドの変更に対処するために自動スケーリングと自動化を使用してファイアウォールをデプロイおよび削除する環境で、VM-Series ファイアウォールのライセンスのアクティベーションと非アクティブ化を簡素化します。

PAYG (従量課金）ライセンスは、このプラグインでの使用はサポートされていません。

ソフトウェアファイアウォールライセンスプラグインを使用して、*VMware NSX* の *VM-Series* ファイアウォールのライセンスを取得しないでください。*VMware NSX* 用の *Panorama* プラグインは、*NSX* および *NSX-T* にデプロイされた *VM-Series* ファイアウォールのライセンスを自動的に取得します

。

また、このプラグインを使用して、*NSX-T* にデプロイされた *VM-Series* ファイアウォールのインスタンスが入っているデバイスグループにデプロイされたファイアウォールのライセンスを取得しないでください。

Panorama ソフトウェアファイアウォールライセンスプラグインをインストールするには、Panorama 10.0.0 以降と VM-Series プラグイン 2.0.4 以降を使用する必要があります。VM-Series ファイアウォールは PAN-OS 9.1.0 以降を実行している必要があります。

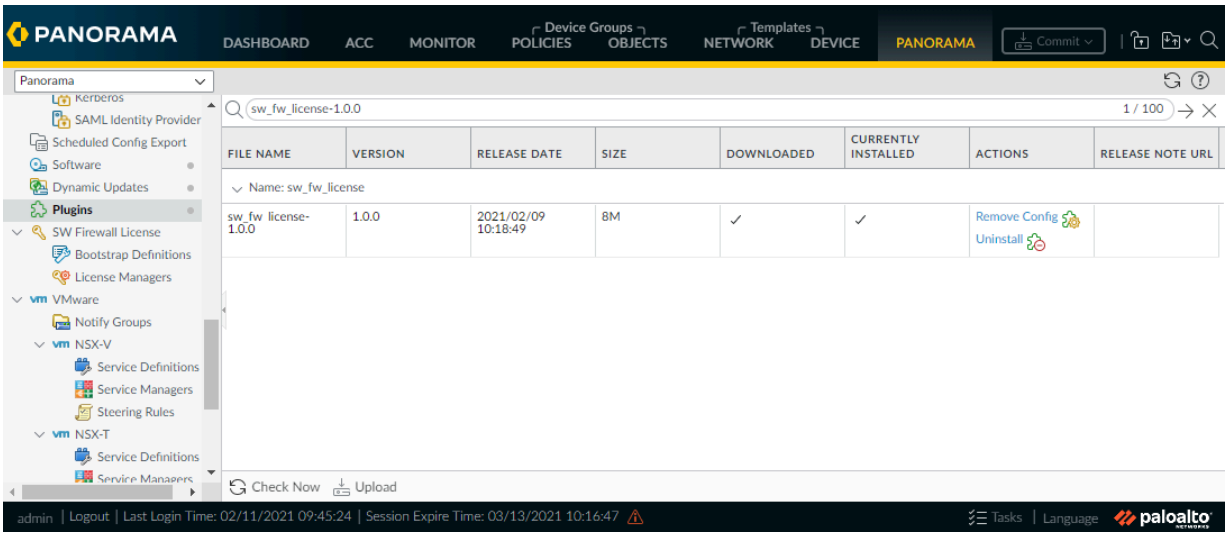
Azure 用の *VM-Series* ファイアウォールには、*VM-Series* プラグイン *2.0.8* 以降が必要です。

©2023 Palo Alto Networks, Inc.

STEP 1 | Panorama 用のソフトウェアファイアウォールライセンスプラグインをインストールします。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Plugins**（プラグイン）を選択します。
3. [今すぐチェック]をクリックして、使用可能なプラグインのリストを取得します。
4. sw_fw_license を検索して、プラグインを見つけます。
5. ソフトウェアライセンスプラグインの[ダウンロード]と[インストール]を選択します。

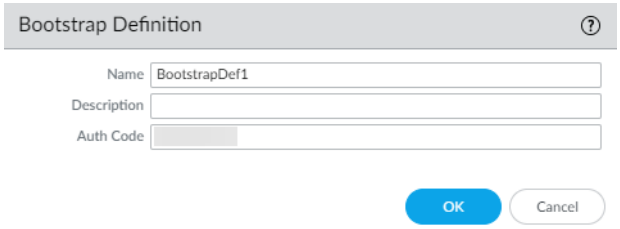
インストールが正常に完了したら、Panorama が更新され、[**Panorama**] タブにソフトウェアライセンスプラグインが表示されます。



©2023 Palo Alto Networks, Inc.

STEP 2 | ブートストラップ定義を構成します。

1. **Panorama** > **SW** ファイアウォールライセンス > ブートストラップの定義を選択します。
2. **[追加]** をクリックします。
3. ブートストラップ定義を識別するためのわかりやすい名前を入力します。
4. （任意）ブートストラップ定義の説明を入力します。
5. Panorama への接続時に VM-Series ファイアウォールのライセンスを取得するために Panorama が使用する認証コードを入力します。
6. **OK** をクリックします。



STEP 3 | ライセンスマネージャーを構成します。

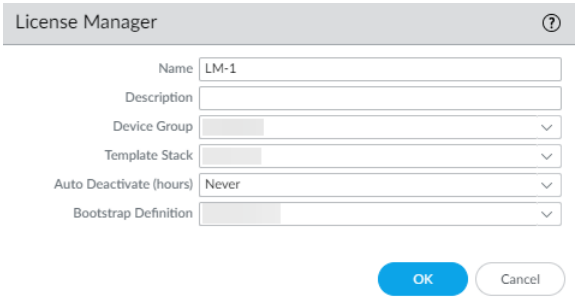
1. **Panorama** > **SW** ファイアウォールライセンス > ライセンスマネージャーを選択します。
2. **[追加]** をクリックします。
3. ライセンスマネージャを識別するためのわかりやすい名前を入力します。
4. （任意）ライセンスマネージャーの説明を入力します。
5. ドロップダウン リストからデバイス グループを選択します。ライセンスマネージャーを使用してブートストラップされた VM-Series ファイアウォールが Panorama に接続すると、指定のデバイスグループ内に配置されます。
6. ドロップダウンからテンプレートスタックを選択します。ライセンスマネージャーを使用してブートストラップされた VM-Series ファイアウォールが Panorama に接続すると、指定のテンプレートスタック内に配置されます。
7. [自動非アクティブ化]フィールドで、接続が切れた VM-Series ファイアウォールのライセンスの非アクティブ化までに Panorama が待機する時間を時間単位で指定します。[しない]を選択すると、Panorama は接続が切れた VM-Series ファイアウォールを非アク

©2023 Palo Alto Networks, Inc.

ティブ化しません。自動非アクティブ化は、デフォルトで[しない]に設定されています。非アクティブ化時間は、時間単位で 1 から 24 までを設定できます。

自動非アクティブ化の間隔がある場合、プラグインは、所定どおりに非アクティブ化するファイアウォールの同じライセンスマネージャーによって管理されている停止した *VM-Series* ファイアウォールのライセンスを非アクティブ化する場合があります。

8. ドロップダウンからブートストラップ定義を選択します。選択したブートストラップ定義は、ライセンスマネージャーに関連付けられた VM-Series ファイアウォールのライセンスを取得するために Panorama が使用する認証コードを指定します。
9. **OK** をクリックします。
10. 変更を **Commit (コミット)** します。



STEP 4 | （任意）VM-Series ファイアウォールをブートストラップするための `init-cfg.txt` ファイルを作成します。ライセンスマネージャーを構成した後、VM-Series ファイアウォールをデプロイするときに、Panorama によって生成されたブートストラップパラメーターをコピーして貼り付けることができます。デプロイメントによっては、表示されるパラメーターが、下の画像に示されているパラメーターのサブセットになる場合があります。たとえば、Panorama アプライアンスがパブリッククラウドにデプロイされている場合、ブートストラップパラメーターには Panorama のパブリック IP アドレスは組み入れられません。その場合、`init-cfg.txt` ファイルにパブリック IP アドレスを手動で入力する必要があります。Panorama は、`init-cfg.txt` で使用するために、常に auth-key と **`plugin-op-commands=panorama-licensing-mode-on`** を生成します。

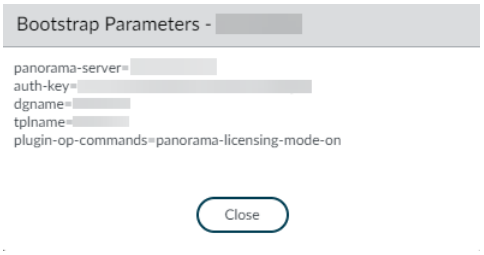
ここに表示される認証キーは Panorama によって生成され、Panorama へのVM-Series ファイアウォール接続を認証するために使用されます。さらに、この認証キーは、Panorama で生成して init-cfg.txt ファイルに追加する VM 認証キーの代わりに使用されます。

ここに表示されている認証キーを *init-cfg.txt* ファイル で使用する場合は、手動で生成された *VM* 認証キーを使用しないでください。

1. **Panorama** > **SW** ファイアウォールライセンス > ライセンスマネージャーを選択します。
2. 特定のライセンスマネージャーのアクション列で、[ブートストラップパラメーターの表示]をクリックします。
3. 表示された情報をコピーしてテキストエディタに貼り付け、ブートストラップ用の `init-cfg.txt` ファイルを作成します。

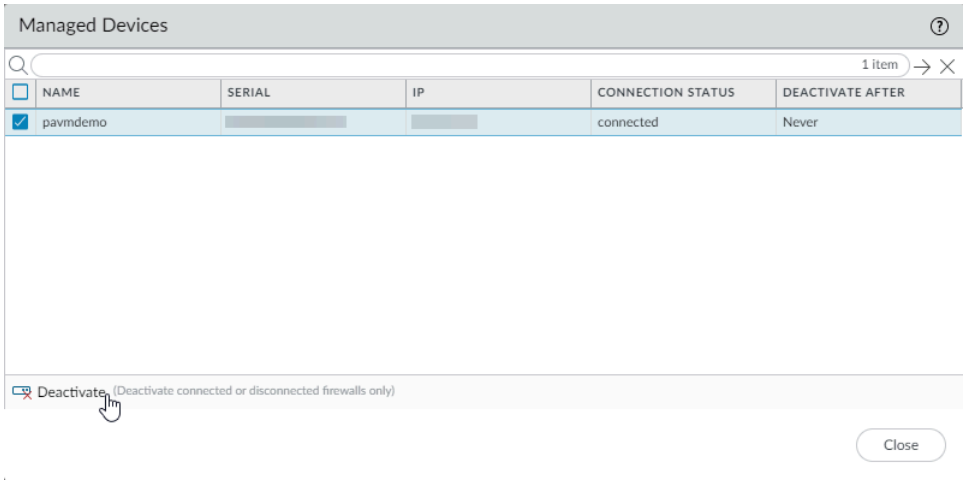
©2023 Palo Alto Networks, Inc.

4. 終了したら、[閉じる]をクリックします。



STEP 5 | （任意）管理対象の VM-Series ファイアウォールを表示して非アクティブ化します。[デバイスの表示]ダイアログから、特定のライセンスマネージャーに関連付けられているデバイスを表示できます。名前、シリアル番号、管理 IP アドレス、接続ステータス、および接続の切れたファイアウォールの非アクティブ化まで Panorama が待機する時間を表示できます。さらに、管理対象 VM-Series ファイアウォールのライセンスを手動で非アクティブ化できます。

1. **Panorama** > **SW** ファイアウォールライセンス > ライセンスマネージャーを選択します。
2. 特定のライセンスマネージャーのアクション列で、[デバイスの表示]をクリックします。
3. 接続中または接続の切れた（ただしまだ非アクティブ化されていない）管理対象 VM-Series ファイアウォールを手動で非アクティブ化するには、リストされている1つ以上の VM-Series ファイアウォールを選択し、[非アクティブ化]をクリックします。



STEP 6 | （任意）接続されたファイアウォールのライセンスを取得するために必要な API 呼び出しを Panorama が完了したことを確認します。

1. Panorama コマンドラインインターフェースにログインします。
2. 以下のコマンドを実行します。

```
show plugins sw_fw_license panorama-api-requests
```


©2023 Palo Alto Networks, Inc.

Software NGFW Credits

Software NGFW Credit は、ソフトウェア NGFW（VM-Series および CN-Series）、クラウド配信セキュリティサービス（CDSS）、またはインターネットアクセスの有無にかかわらずネットワーク（エアギャップネットワークなど）の仮想 Panorama アプライアンスに資金を提供するために使用できます。

デプロイメントプロファイルを作成して、PAN-OS バージョン、ファイアウォールごとの vCPU の数、デプロイメントプロファイルでサポートされるファイアウォールの総数、Panorama 管理またはログ収集、およびセキュリティサービスに基づいて 1 つ以上のファイアウォールを構成します。デプロイメントプロファイルで作成されたすべての VM は、同じ authcode を共有します。

- 固定 vCPU - すべての PAN-OS バージョンと互換性があります。VM-Series モデルおよびセキュリティサービスバンドルに基づいています。モデルまたはサービスオプションを変更するには、新しいライセンスが必要です。
- フレキシブル vCPU - PAN-OS 10.0.4 以降で使用できます。vCPU の数を柔軟に選択でき、セキュリティサービスを柔軟に選択できます。デプロイメントプロファイルを変更して、vCPU の数を追加または減らしたり、新しいサービスを利用可能になったときに追加したり、サービスを削除したりできます。デプロイメントプロファイルの最大 vCPU 数は 64 です。

Software NGFW Credit は期間ベースです。期間は、1 年から 5 年の間の任意の期間に対して定義できます。割り当て済みおよび未割り当てのクレジットはどちらも、合意された期間の終了時に失効します。クレジットプール用に追加のクレジットを購入できますが、有効期限はターゲットプールと同じになります。

ライセンスサーバーへのインターネット接続があり、ファイアウォール、セキュリティサービス、または Panorama デプロイメントの使用を停止した場合、そのリソースに割り当てられたクレジットはクレジットプールに払い戻され、新しいリソースに再割り当てできます。

インターネットに接続していなくて、Palo Alto Networks 更新サーバーに接続できない場合 (エアギャップネットワークにいる場合など)、VM-Series ファイアウォールをユーザーインターフェースまたは Panorama からローカルで管理できます。その後、管理者はカスタマーサポートポータルにログインしてライセンストークンを返却し、資金を再利用できるようにする必要があります。

以下のサポートされるハイパーバイザーの表と、次のデータプレーン上の合計 **vCPU** 数の表を使用して、選択した数の vCPU に必要なハードウェアリソースを割り当てます。

メモリプロファイル	サポートされているハイパーバイザ	最小ハード ドライブ
4.5GB、5.5GB	ESXi、Hyper-V、KVM	32GB（起動時は 60GB）
6.5GB	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB

©2023 Palo Alto Networks, Inc.

メモリプロファイル	サポートされているハイパーバイザ	最小ハード ドライブ
9GB	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB
16GB	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB
56GB	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB

上記のすべてのメモリプロファイルでの最小 vCPU 数は 2 です。4.5GB を選択した場合、Lite モードを有効にできます。Lite モードは、リソースが制限されている環境での代替動作モードです。詳細は、「VM-50 Lite モード」を参照してください。

Lite モードでは、最低 *32GB* のハードドライブ容量が必要です。ただし、*VM-Series* の基本イメージはすべての *vCPU* の組み合わせで共通であるため、*4.5GB* のメモリを搭載した *VM-Series* ファイアウォールのライセンスを取得するまで、*60GB* のハードドライブ領域を割り当てる必要があります。

最高のパフォーマンスを達成するには、必要なすべてのコアを *1* つの *CPU* ソケットで使用できるようにする必要があります。

管理プレーンとデータプレーンに割り当てられる vCPU の配分は、VM-Series ファイアウォールに割り当てられる vCPU の総数によって異なります。メモリプロファイルと vCPU 合計数の特定の組み合わせに自動的に割り当てられるデータプレーン vCPU の数を調べるには、次の表（1～16 個の vCPU と 17～32 個の vCPU）を参照してください。たとえば、メモリプロファイルが 16GB、合計 15 個の vCPU の場合、11 個がデータプレーンに割り当てられ、残りの 4 個が管理プレーンに割り当てられます。

メモリプロファイル	データプレーン上の **vCPU** の合計 **(1～16)**														
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15日**	**16**
4.5GB	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5.5GB	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6.5GB	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2
9GB	1	2	3	3	4	4	4	4	4	4	4	4	4	4	4

©2023 Palo Alto Networks, Inc.

メモリプロファイル	データプレーン上の vCPU の合計 (1～16)														
	2	3	4	5	6	7	8	9	10	11	12	13	14	15日	16
16GB	1	2	3	3	4	5	6	6	7	8	9	9	10	11	12
56GB	1	2	3	3	4	5	6	6	7	8	9	9	10	11	12

メモリプロファイル	データプレーン上の vCPU の合計数 (17～32)															
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
4.5GB	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5.5GB	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6.5GB	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
9GB	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
16GB	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
56GB	12	13	14	15日	15日	16	17	18	18	19	20	21	21	22	23	24

ソフトウェア NGFW タスクに進みます。

- メモリに基づく最大制限
- クレジットのアクティベート
- デプロイメントプロファイルの作成
- デプロイメントプロファイルの管理
- VM-Series ファイアウォールの登録 (Software NGFW Credit)
- Panorama のプロビジョニング
- クレジットの転送
- ライセンスの非アクティブ化 (Software NGFW Credit)
- データプレーンコアのカスタマイズ
- フレキシブル VM-Series ライセンスへの移行

メモリに基づく最大制限

次の表は、単一の VM-Series ファイアウォールのデプロイメントが 4.5、5.5、6.5、9、16、または 56 GB のメモリで構成されたファイアウォール上で作成、保存、管理、または対話できる特定のオブジェクトまたはリソースの最大数を示しています。 これらの制限は、PAN-OS10.0.4以降を実行している VM-Series ファイアウォールのフレキシブルライセンスに適用されます。

©2023 Palo Alto Networks, Inc.

メモリプロファイルと vCPU の総数によって、管理プレーンとデータプレーンに自動的に割り当てられるコアの数が決まります。PAN-OS バージョン 10.0.1 以降を実行している場合は、データプレーンコアの配布のカスタマイズを行うオプションがあります。

SW NGFW ライセンスを使用している場合は、次の 1 つ以上のリソースの要件をサポートするメモリプロファイルを選択できます。

• アドレス割り当て • App-ID • EDL • GlobalProtect クライアント VPN • GlobalProtect クライアントレス VPN • 高可用性（HA）	• インターフェイス • IPSec VPN • L2フォワーディング • マルチキャスト • NAT • オブジェクト (アドレス、サービス)	• ポリシー • QoS • routing • セキュリティプロファイル • セキュリティゾーン数 • セッション数	• SSL復号化 • URL フィルタリング • User-ID • 仮想ルーター • 仮想システム • バーチャル ワイヤー

セッション数

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大セッション (IPv4 または IPv6)	50,000	64,000	250,000	819,200	2,000,000	10,000,000

ポリシー

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
セキュリティ ルール	200	250	1,500	10,000	10,000	20,000
セキュリティ ルール スケジュール	256	256	256	256	256	256
NAT ルール	400	400	3,000	5,000	8,000	15,000
復号化ルール	100	100	1,000	1,000	1,000	2,000
アプリケーション オーバーライド ルール	100	100	1,000	1,000	1,000	2,000
トンネルコンテンツ検査ルール	100	100	100	500	500	2,000
SD-WAN ルール	NA	100	100	100	300	300

©2023 Palo Alto Networks, Inc.

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
ポリシーベース転送ルール	100	100	100	500	500	2,000
キャプティブポータルのルール	10	10	1,000	1,000	1,000	2,000
DoS プロテクションルール	100	100	1,000	1,000	1,000	1,000

セキュリティゾーン数

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大セキュリティ ゾーン	15日	15日	40	40	200	200

オブジェクト (アドレス、サービス)

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
アドレスオブジェクト	2,000	2,500	10,000	10,000	20,000	40,000
アドレスグループ	100	125	1,000	1,000	2,500	4,000
メンバー/アドレス グループ	2,500	2,500	2,500	2,500	2,500	2,500
サービス オブジェクト	1,000	1,000	2,000	2,000	2,000	5,000
サービスグループ	250	250	500	500	250	500
メンバー/サービス グループ	500	500	500	500	500	500
FQDNアドレス オブジェクト	2,000	2,000	2,000	2,000	2,000	2,000
最大 DAG IP アドレス* （システム全体の容量）	1,000	1,000	2,500	200,000	300,000	300,500
IP アドレスごとのタグ	32	32	32	32	32	32

* AppMixト ランザクションを利用して有効にされた App-ID および User-ID 機能で測定されたファイアウォールスループット。

©2023 Palo Alto Networks, Inc.

セキュリティ プロファイル

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
セキュリティ プロファイル	38	38	375	375	750	750

App-ID

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
カスタムApp-IDシグネチャ	6,000	6,000	6,000	6,000	6,000	6,000
共有カスタム App-ID	512	512	512	512	512	512
カスタム App-ID（仮想システム固有）	3,208	1,000	6,416	1,000	6,416	6,416

User-ID

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
IP-User マッピング (管理プレーン)	524,288	524,288	524,288	524,288	524,288	524,288
IP-User マッピング（データプレーン）	64,000	64,000	64,000	64,000	512,000	512,000
ポリシーで使用されるアクティブかつ固有のグループ（LDAP グループ、XML API グループ、および動的ユーザーグループの集合体）*	1,000	1,000	1,000	1,000	10,000	10,000
User-ID エージェントの数	100	100	100	100	100	100
User-ID の監視対象サーバー	100	100	100	100	100	100
ターミナルサーバーエージェント	400	400	400	400	2,000	2,500
ユーザーあたりのタグ*（PAN-OS 9.1 以降）	32	32	32	32	32	32

©2023 Palo Alto Networks, Inc.

* AppMix トランザクションを利用して有効にされた App-ID および User-ID 機能で測定されたファイアウォールスループット。

SSL復号化

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大SSLインバウンド証明書	1,000	1,000	1,000	1,000	1,000	1,000
SSL 証明書キャッシュ (転送プロキシ)	128	128	128	2,000	4,000	8,000
最大同時暗号解読セッション	1,024	1,024	6,400	15,000	50,000	100,000
SSL ポートミラー	はい	あり。	あり。	あり。	あり。	あり。
SSL 復号化ブローカー	無し	いいえ	無し	はい	無し	あり。
サポートされる HSM	はい	あり。	あり。	あり。	あり。	あり。

URL フィルタリング

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
許可リスト、ブロック リスト、カスタム カテゴリの総エントリ	25,000	25,000	25,000	25,000	25,000	100,000
最大カスタム カテゴリ	2,849	2,849	2,849	2,849	2,849	2,849
最大カスタムカテゴリ数 （仮想システム固有）	500	500	500	500	500	500
データプレーンのURLフィルタリングのキャッシュ サイズ	90,000	90,000	90,000	90,000	90,000	250,000
管理プレーンのダイナミック キャッシュ サイズ	100,000	100,000	100,000	100,000	100,000	600,000

EDL

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
カスタムリストの最大数	30	30	30	30	30	30

©2023 Palo Alto Networks, Inc.

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
システムあたりのIPの最大数	50,000	50,000	50,000	50,000	50,000	50,000
システムあたりの DNS ドメインの最大数	50,000	50,000	50,000	5000,000	2,000,000	2,000,00
システムあたりの URL の最大数	50,000	50,000	50,000	100,000	100,000	100,000
最短チェック間隔 （分）	5	5	5	5	5	5

インターフェイス

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
管理 - 帯域外	NA	NA	NA	NA	NA	NA
管理 - 10/100/1000 高可用性	NA	NA	NA	NA	NA	NA
管理 - 40Gbps の高可用性	NA	NA	NA	NA	NA	NA
管理 - 10Gbps の高可用性	NA	NA	NA	NA	NA	NA
トラフィック - 10/100/1000	NA	NA	NA	NA	NA	NA
トラフィック - 100/1000/10000	NA	NA	NA	NA	NA	NA
トラフィック - 1Gbps SFP	NA	NA	NA	NA	NA	NA
トラフィック - 10Gbps SFP +	NA	NA	NA	NA	NA	NA
トラフィック - 40/100Gbps QSFP +/QSFP28	NA	NA	NA	NA	NA	NA
デバイスあたりの802.1qタグ	4,094	4,094	4,094	4,094	4,094	4,094
物理インタフェースあたりの802.1qタグ	4,094	4,094	4,094	4,094	4,094	4,094
最大インターフェイス (論理および物理)	512	512	2,048	2,048	4,096	40,96
最大アグリゲート インターフェイス	NA	NA	NA	NA	NA	NA

©2023 Palo Alto Networks, Inc.

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
SD-WAN 仮想インターフェースの最大数	NA	150	300	500	1,000	1,000

仮想ルーター

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
仮想ルーター	3	3	3	10	20	125

バーチャル ワイヤー

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
バーチャルワイヤー	2	4	12	12	12	12

仮想システム

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
基本仮想システム	1	1	1	1	1	1
最大仮想システム 基本仮想システム容量を超える仮想システム容量に対しては、ライセンスの追加が必要です	NA	NA	NA	NA	NA	NA

routing

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
IPv4 転送テーブルサイズ* (仮想ルーター全体を通して共有されるエントリ)	1,000	2,500	5,000	10,000	32,000	100,000
IPv6 転送テーブルサイズ* (仮想ルーター全体を通して共有されるエントリ)	1,000	1,000	5,000	10,000	32,000	100,000
システムの転送テーブル サイズの合計	1,000	1,000	5,000	10,000	32,000	100,000

©2023 Palo Alto Networks, Inc.

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
32,000	50	50	50	50	50	50
最大ルーティング ピア (プロトコル依存)	500	500	500	500	1,000	1,000
スタティック エントリ - DNS プロキシ	1,024	1,024	1,024	1,024	1,024	1,024
双方向転送検出（BFD）セッション	該当なし	該当なし	128	512	1,024	1,024

* AppMix トランザクションを利用して有効にされた App-ID および User-ID 機能で測定されたファイアウォールスループット。

L2フォワーディング

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
ARPテーブル サイズ/デバイス	1,500	1,500	2,500	10,000	32,000	128,000
IPv6隣接テーブル サイズ	500	500	2,500	10,000	32,000	128,000
MACテーブル サイズ/デバイス	1,500	1,500	2,500	5,000	32,000	128,000
ブロードキャスト ドメインごとの最大ARPエントリ	1,500	1,500	2,500	10,000	32,000	128,000
ブロードキャスト ドメインごとの最大MACエントリ	1,500	1,500	2,500	5,000	32,000	128,000

NAT

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
NATルール総容量	160	400	3,000	5,000	8,000	8,000
最大 NAT ルール (スタティック)* （スタティック NAT ルールをフルキャパシティーに構成するには、他の NAT ルールタイプを使用しない必要があります。）	160	400	3,000	5,000	8,000	8,000

©2023 Palo Alto Networks, Inc.

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大 NAT ルール (DIP)* （DIP NATルールをフルキャパシティーに構成するには、他の NAT ルールタイプを使用しない必要があります。）	160	400	2,000	3,000	8,000	8,000
最大NATルール (DIPP)	160	200	400	800	2,000	2,000
最大変換 IP（DIP）数	16,000	16,000	128,000	128,000	160,000	160,000
最大変換 IP （DIPP）* （DIPP 変換の IP 容量は、DIPP プールのオーバーサブスクリプション値に比例します。ここに示されている容量は、1倍のオーバーサブスクリプション値に基づいています）	200	200	400	800	2,000	2,000
デフォルト DIPP プールオーバーサブスクリプション* （同時セッションでのソース IP とソースポートの再利用）	2	2	2	2	8	8

* AppMix トランザクションを利用して有効にされた App-ID および User-ID 機能で測定されたファイアウォールスループット。

アドレス割り当て

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
DHCPサーバー	3	3	3	10	20	125
DHCP リレー* （最大容量は、DHCP サーバーと DHCP リレーの合計を表します）	500	500	500	500	500	500
最大割り当てアドレス	64,000	64,000	64,000	64,000	64,000	64,000

* AppMix トランザクションを利用して有効にされた App-ID および User-ID 機能で測定されたファイアウォールスループット。

©2023 Palo Alto Networks, Inc.

高可用性（HA）

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
サポートされているデバイス	2	2	2	2	2	2
最大仮想アドレス	32	32	128	32	32	128

QoS

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
QoSポリシー数	100	100	500	1,000	2,000	4,000
QoS をサポートする物理インターフェイス	6	6	6	6	12	12
物理インタフェースごとのクリアテキスト ノード	31	31	31	63	63	63
ポリシーによるDSCP マーキング	はい	あり。	あり。	あり。	あり。	あり。
サポートされるサブインターフェイス	NA	NA	NA	NA	NA	NA

IPSec VPN

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大IKEピア	25	250	1,000	1,000	1,000	2,000
サイト間 （プロキシ ID 使用）	25	250	1,000	2,000	4,000	8,000
SD-WAN IPSec トンネル	NA	250	1,000	1,000	1,000	2,000

GlobalProtect クライアント VPN

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大トンネル数 （SSL、IPSec、および IKE (XAUTH 使用)）	25	250	500	2,000	6,000	12,000

©2023 Palo Alto Networks, Inc.

GlobalProtect クライアントレス VPN

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
最大 SSL トンネル数	40	40	100	400	1,200	2,500

マルチキャスト

機能	4.5 GB	5.5 GB	6.5 GB	9 GB	16 GB	56 GB
複製 (出力インターフェイス)	100	100	100	100	100	100
ルート	500	500	2,000	2,000	4,000	4,000

クレジットのアクティベート

組織内では、それぞれが異なる目的を持つ多くのアカウントを作成できます。アクティベーション中は、デフォルトのクレジットプールごとに 1 つのアカウントのみを選択できます。クレジットプールがアクティブになると、クレジット管理者のロールを付与されたユーザーは、デプロイメントにクレジットを割り当てることができ、他のプールにクレジットを転送することもできます。

既存の CSPア カウントがあり、スーパーユーザーまたは管理者である場合、システムは自動的にクレジット管理者のロールをプロファイルに追加します。既存のアカウントがない場合、CSPは自動的にアカウントを作成し、クレジット管理者のロールをプロファイルに追加します。

あなた（購入者）は、サブスクリプション、クレジットプール ID、サブスクリプションの開始日と終了日、購入したクレジットの数量、およびデフォルトのクレジットプールの説明を詳述した電子メールを受け取ります（VM-Series ファイアウォールライセンスの「デフォルトのクレジットプール」を参照）。

後で参照できるように、このメールを保存してください。

STEP 1 | 電子メールで、[アクティベーションの開始]をクリックして、使用可能なクレジットプールを表示します。

©2023 Palo Alto Networks, Inc.

STEP 2 | アクティベートするクレジットプールを選択します。検索フィールドを使用して、アカウントリストを番号または名前でフィルタリングできます。

複数のクレジットプールを購入した場合（Software NGFW Creditsを参照）、それらは自動的に選択されます。チェックマークは、オンボーディングクレジットのアクティベーションリンクを表します。

認証またはサインインするように求められます。

クレジットプールの選択を解除すると、それらのクレジットをアクティベートするには、電子メールに戻って*[*アクティベーションの開始*]*リンクをクリックする必要があるというリマインダーが表示されます。

STEP 3 | [アクティベーションの開始]を選択します。

STEP 4 | サポートアカウントを選択します（アカウント番号または名前で検索できます）。

STEP 5 | デフォルトのクレジットプールを選択します。

STEP 6 | [デポジットクレジット]を選択します。

デポジットが正常に完了したというメッセージが表示されます。

STEP 7 | (任意）これが初めてのクレジットアクティベーションである場合は、[デプロイメントプロファイルの作成]ダイアログが表示されます。

デプロイメントプロファイルの作成に進んで続行します。

デプロイメントプロファイルの作成

デプロイメントプロファイルを作成するには、カスタマーサポートポータルアカウント（CSP）と、アクティベートされたクレジットプールへのアクセス権が必要です。

開始する前に、デプロイメントプロファイルの構成を使用するファイアウォールの数を見積もります。すべてのファイアウォールを一度にデプロイする必要はありません。

STEP 1 | すでにクレジットプールがある場合は、アカウントにログインし、ダッシュボードからアセット > **Software NGFW Credits** > デプロイメントプロファイルの作成を選択します。

クレジットプールをアクティベートするとすぐに、[デプロイメントプロファイルの作成]フォームが表示されます。

1. VM-Series ファイアウォールタイプを選択します。
2. PAN-OS のバージョンを選択します。
   - 固定モデル（VM-Series モデル）
   - フレキシブル **vCPU** （**PAN-OS 10.0.4**以降）（Software NGFW Credits）
3. **Next**（次へ）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series プロファイル。

1. プロファイル名。

   プロファイルに名前を付けます。

2. ファイアウォールの数。

   十分なクレジットがあると仮定して、このプロファイルがデプロイするファイアウォールの数を入力します。それらをすべて一度にデプロイする必要はありません。

3. ファイアウォールモデル（PAN-OS 10.0.3以下）：

   VM-Series モデルを選択します。

   計画されている **vCPU /**ファイアウォール（PAN-OS 10.0.4以降）。

   ファイアウォールごとの vCPU の数を入力します。

4. サブスクリプションのカスタマイズ。

   ドロップリストからユースケースを選択します。セキュリティサービスを追加または削除できます。

5. （任意）クレジットを使用して **VM** パノラマを有効化します。

   パノラマのユースケース（管理および/またはログコレクター）を選択します。

STEP 3 | （任意）[さらに保護、さらに保存]の後にある疑問符にカーソルを合わせると、クレジットの割り当てが節約にどのように影響するかを確認できます。

STEP 4 | [見積もりコストの計算]をクリックして、クレジットの合計と、デプロイメント前に使用可能なクレジットの数を表示します。

（任意）見積もりの後ろにある疑問符にカーソルを合わせると、各コンポーネントのクレジットの内訳が表示されます。

STEP 5 | [デプロイメントプロファイルの作成]をクリックします。

プロファイルが[現在のデプロイメントプロファイル]タブリストに表示されるまで、数秒待つ必要がある場合があります。割り当てが完了するまでは、[消費/割り当て済みクレジット]列に 0 と[更新の保留中]が表示されます。一番下までスクロールして最後のページに移動し、プロファイルを見つけます。

後でデプロイメントプロファイルを表示するには、親クレジットプールの[詳細]ボタンをクリックし、[現在のデプロイメントプロファイル]タブを選択します。

- 右端にあるプロファイルの認証コードに注意してください。Software NGFW credit 認証コードは D で始まります。
- [消費/割り当て済みクレジット]列には、割り当てが完了するまでは 0 と[更新の保留中]が表示されます。
- [監査証跡]タブには、管理しているクレジットトランザクションとデプロイメントプロファイルが表示されます。このタブでは、時間でプロファイルを検索することもできます。

  検索を使用してプロファイルを見つけ、行を展開して、プロファイルの作成時に指定した構成を表示します。

©2023 Palo Alto Networks, Inc.

デプロイメントプロファイルの管理

デプロイメントプロファイルを作成したら、それを編集、コピー、または削除できます。

- デプロイメントプロファイルの編集
- デプロイメントプロファイルのクローン作成
- デプロイメントプロファイルの削除

デプロイメントプロファイルの編集

STEP 1 | アセット > **Software NGFW Credits**を選択し、プロファイルの作成に使用したクレジットプールの[詳細]ボタンをクリックします。

STEP 2 | [現在のデプロイメントプロファイル]タブを選択します。

STEP 3 | 右端で、縦の省略記号（[その他のオプション]）を選択し、[プロファイルの編集]を選択します。

STEP 4 | 変更を加えて、[デプロイメント プロファイルの更新]を選択します。

STEP 5 | [監査証跡]タブを選択し、検索を使用してプロファイルを見つけます。

検索を使用してプロファイルを見つけ、行を展開して、プロファイルの作成時に指定した構成を表示します。

デプロイメントプロファイルのクローン作成

STEP 1 | アセット > **Software NGFW Credits**を選択し、プロファイルの作成に使用したクレジットプールの[詳細]ボタンをクリックします。

STEP 2 | 右端で、縦の省略記号([その他のオプション])を選択し、[プロファイルのクローン作成]を選択します。

STEP 3 | プロファイル名を変更し、その他の変更を加えて、[デプロイメント プロファイルの作成]を選択します。

STEP 4 | [監査証跡]タブを選択し、検索を使用してプロファイルを見つけます。

行を展開して、複製した構成を表示します。これは、プロファイル名と認証コードが異なる新しい構成です。

デプロイメントプロファイルの削除

デプロイメントプロファイルを削除する前に、ライセンスの非アクティブ化 (Software NGFW Credit)デプロイメントプロファイルを使用してファイアウォールをオンにしてから、VM を非アクティブ化する必要があります。

STEP 1 | アセット > **Software NGFW Credits**を選択し、プロファイルの作成に使用したクレジットプールの[詳細]ボタンをクリックします。

STEP 2 | 右端で、縦の省略記号（[その他のオプション]）を選択し、[削除]を選択します。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールの登録 (Software NGFW Credit)

これらの手順には次のものが必要です。

- IP アドレス、ネットマスク、デフォルトゲートウェイ、および DNS サーバの IP アドレスで構成されたデプロイ済みのファイアウォール。インターネットへの直接アクセスは必要ありません。
- サポートアカウント。まだ作成していない場合は作成してください。

次のいずれかの手順を実行して、デプロイした VM-Series ファイアウォールを登録します。

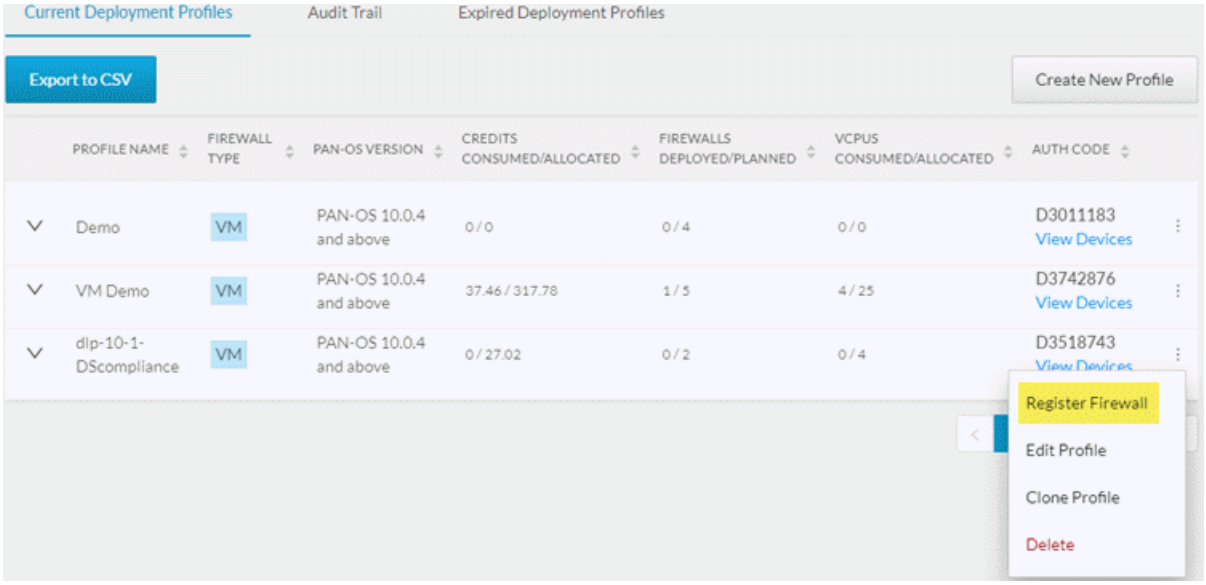
- インターネットへの直接アクセス
- インターネット接続なし

©2023 Palo Alto Networks, Inc.

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は、CSP デプロイメントプロファイルから登録します。登録が成功すると、ライセンスがアクティベートされます。

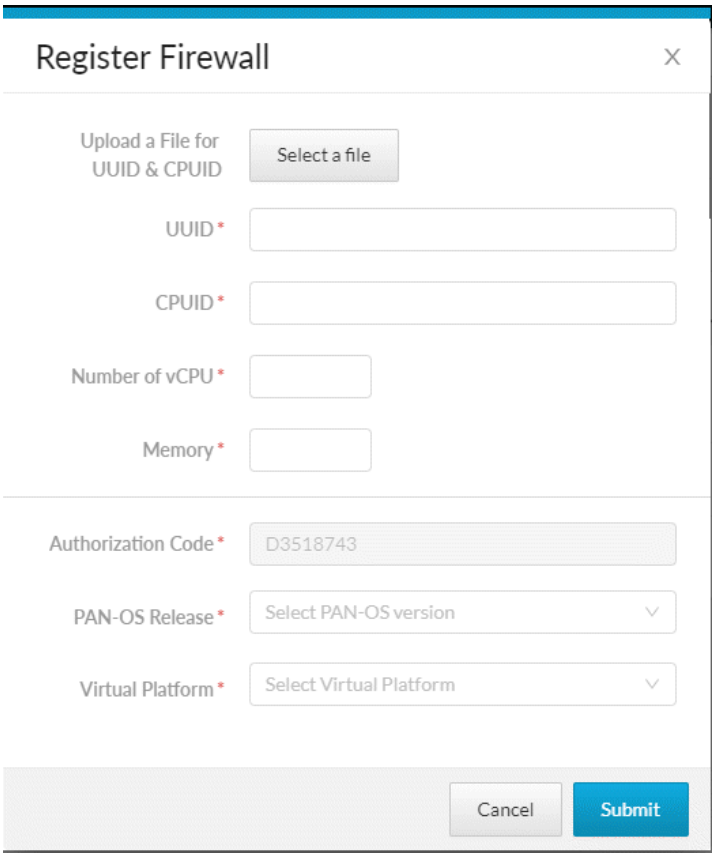
1. ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。
2. アセット > **Software NFGW Credits**を選択します

   クレジットプールを見つけて、[詳細] ボタンをクリックします。
3. [現在のデプロイメントプロファイル] でプロファイルを見つけ、右端の [**AUTH CODE**] 列で縦方向の省略記号 ([その他のオプション]) を選択し、[ファイアウォールの登録] を選択します。



   ファイアウォール登録フォームが開きます。ご自分のファイアウォールの情報を入力し、[サブミット] をクリックします。

©2023 Palo Alto Networks, Inc.



この時点で、ファイアウォールは登録され、ライセンスは自動的にアクティベートされます。このファイアウォールのライセンスがクレジットを消費するようになります。

ファイアウォールが登録され、ライセンスがアクティベートされていることを確認します。

- アセット > **Software NFGW Credits**を選択します
  - 消費されたクレジット、デプロイ済みのファイアウォール、および消費された vCPU は、デプロイメントを反映するように増分するはずです。
  - [認証コード] 列で、[デバイスの表示] リンクをクリックし、デプロイメントのシリアル番号を見つけます。
- アセット > **Software NFGW Credits**を選択します
  - 消費されたクレジット、デプロイ済みのファイアウォール、および消費された vCPU は、デプロイメントを反映するように増分するはずです。
  - [認証コード] 列で、[デバイスの表示] リンクをクリックし、デプロイメントのシリアル番号を見つけます。
- ファイアウォールにログインし、ダッシュボードに有効なシリアル番号が表示され、**PA-VM** ライセンスがデバイス > ライセンスタブに表示されていることを確認します。

©2023 Palo Alto Networks, Inc.

ファイアウォールにインターネット接続がない場合は、手動で登録してください。

この手順により、デバイスがサポートデータベースに追加されます。ファイアウォールはライセンスサーバーに接続できないため、CSP からファイアウォールにライセンスを手動で渡す必要があります。

1. ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。
2. 新しいプロファイルを選択し、縦の省略記号をクリックして、[ファイアウォールの登録]を選択します。
   1. VM とファイアウォールの情報を入力し、[サブミット]を選択します。これにより、ファイアウォールがプロファイルとその認証コードに関連付けられ、シリアル番号が割り当てられます。
   2. [デバイスの表示]をクリックして、関連するデバイスをソフトウェア **NGFW** デバイスで確認します。
   3. [ライセンス]列で、ファイルをホストマシンに安全に転送できる場所にライセンスキーをダウンロードします。
3. ファイアウォールにログインし、デバイス > ライセンスを選択します。

   ウェブ インターフェイス経由でライセンス キーをインストールしなければなりません。ファイアウォールは、*SCP* または *FTP* 経由でのライセンス キーのインストールはサポートしていません。

   - ライセンス キーの手動アップロードリンクをクリックしてライセンス キーを入力します。
   - ダッシュボードに有効なシリアル番号が表示され、**PA-VM** ライセンスが デバイス > ライセンスタブに表示されていることを確認します。

Panorama のプロビジョニング

このオプションは、デプロイメントプロファイルの作成時に Panorama を選択した場合にのみ表示されます。必要に応じて、プロファイルを編集できます。

STEP 1 | アセット > **Software NGFW Credits**を選択し、プロファイルの作成に使用したクレジットプールの[詳細]ボタンをクリックします。

STEP 2 | 右端で、垂直の省略記号（[その他のオプション]）を選択し、[**Panorama** のプロビジョニング]と[プロビジョニング]を選択します。現在のデプロイメントプロファイル用にプロビジョニングされたファイアウォールのリストが表示されます。

これにより、Panorama が作成され、シリアル番号とモデルタイプ PAN-PRA-1000-CP が割り当てられ、Panorama がアセットとして登録されます。プロビジョニングした Panorama は、リスト中の最後の Panorama になります。認証コードは F で始まりますが（したがって、デプロイメントプロファイルと同じではありません）、有効期限はプロファイルのクレジットプールと同じであることに注意してください。

シリアル番号をコピーします。

©2023 Palo Alto Networks, Inc.

STEP 3 | デプロイメントプロファイルから[デバイスの表示]を選択し、[ソフトウェア NGFW デバイス]ページで[**Panorama**]を選択します。これにより、すべての SW NGFW Panorama が表示されます。

コピーしたシリアル番号を使用してシリアル番号で検索します。

アセット > ソフトウェア **NGFW** デバイスを選択し、コピーしたシリアル番号で検索することもできます。

クレジットの転送

カスタマーサポートポータル（CSP）から、同じアカウントのクレジットプール、またはアクセス可能な別のアカウントのクレジットプールにクレジットを転送します。

- 別の CSP アカウント
- このアカウントの別のプール

別の **CSP** アカウント

STEP 1 | CSPア カウントにログインします。

STEP 2 | アセット > **Software NGFW Credits**を選択します。

- ソースクレジットプールを特定し、クレジットプール ID をメモします。
- 宛先クレジットプールを特定し、クレジットプール ID をメモします。

  宛先が別のアカウントにある場合は、左上の[現在のアカウント]ドロップダウンからその宛先を選択し、アセット > **Software NGFW Credit**を選択します。宛先を見つけて、クレジットタイプとクレジットプール ID をメモします。

STEP 3 | ソースクレジットプールに移動し、左下の[クレジットの転送]をクリックします。

STEP 4 | 別の CSP アカウントを選択します。

1. 転送先 - アカウント名を選択します。
2. クレジットタイプとして - クレジットタイプを選択します。このとき、送信元と宛先のタイプは同じである必要があります。
3. クレジットプール **ID** 番号 - クレジットプール ID 番号を選択します。

   選択したタイプのクレジットプールが宛先アカウントにない場合、CSP はクレジットプールを作成するように指示します。
4. 送金金額 - 送金金額を入力します。

STEP 5 | [クレジットの更新]を選択します。

変更を確認するには、少し待つか、画面を更新する必要がある場合があります。

STEP 6 | プールのクレジットトランザクションを表示するには、[詳細]を選択し、[監査証跡]を選択します。

©2023 Palo Alto Networks, Inc.

このアカウントの別のプール

STEP 1 | CSP アカウントにログインします。

STEP 2 | アセット > **Software NGFW Credits**を選択します。

- 宛先クレジットプールを特定し、クレジットプール ID をメモします。
- 指定したタイプの宛先クレジットプールがない場合は、新しいクレジットプールを作成するように求められます。

STEP 3 | ソースクレジットプールに移動し、左下の[クレジットの転送]を選択します。

STEP 4 | [このアカウントの別のプール]を選択します。

1. 新しいクレジットタイプ - クレジットタイプを選択します。このとき、送信元と宛先のタイプは同じである必要があります。
2. クレジットプール **ID** 番号 - クレジットプール ID 番号を選択します。

   選択したタイプのクレジットプールが宛先アカウントにない場合、CSP はクレジットプールを作成するように指示します。
3. 送金金額 - 送金金額を入力します。

STEP 5 | [クレジットの更新]を選択します。

変更を確認するには、少し待つか、画面を更新する必要がある場合があります。

STEP 6 | プールのクレジットトランザクションを表示するには、[詳細]を選択し、[監査証跡]を選択します。

ライセンスの非アクティブ化 (Software NGFW Credit)

ファイアウォール（またはファイアウォールをホストしている VM）を削除する前に、CSP からライセンスを非アクティブ化する必要があります。そうしないと、ライセンスクレジットをクレジットプールに戻すことができません。

ライセンスサーバーにインターネットでアクセスできる場合、CSPのファイアウォールを非アクティブ化すると、ライセンスが自動的に削除され、残りのクレジットがデプロイメントプロファイルに返されます。ライセンスを非アクティブ化した後、ファイアウォールを削除する必要があります。そうしないと、ファイアウォールは引き続きクレジットを消費します。

インターネットにアクセスできない場合は、ファイアウォールからライセンストークンをエクスポートする必要があります。次に、CSPで非アクティブ化を開始し、トークンをアップロード（またはトークンテキストに貼り付け）して非アクティブ化を完了します。

- インターネット アクセス
- インターネット アクセスなし
- インターネットアクセスなし - Panorama管理

©2023 Palo Alto Networks, Inc.

直接インターネットアクセス。

1. アセット > **Software NGFW Credits**を選択し、デプロイメントプロファイルの作成に使用したクレジットプールの[詳細]ボタンをクリックします。
2. デプロイメントプロファイルを見つけ、右端で縦の省略記号（[その他のオプション]）を選択し、[ファイアウォールの非アクティブ化]を選択します。
3. 非アクティブ化するファイアウォールをチェックし、[ファイアウォールの非アクティブ化]を選択します。

インターネットにアクセスできません。

1. ファイアウォール Web インターフェースにログインして、デバイス > ライセンス を選択します。
2. ライセンス管理セクションで **VM** の非アクティブ化を選択します。

   ファイアウォールで非アクティブ化されるライセンス/資格の一覧を確認してください。
3. [手動で完了する]を選択して、非アクティブ化を開始します。

   ライセンストークンのエクスポートリンクをクリックし、トークンファイルをクライアントに保存します。トークンのファイル名は次のようになります。`20150128_1307_dact_lic.01282015.130737.tok`

   この時点で、ファイアウォールでライセンスが非アクティブ化されていますが、クレジットはクレジットプールに戻されていません。
4. トークンファイルを使用して、変更をライセンスサーバーに登録します。

   1. Palo Alto Networks カスタマー サポート Web サイトにログインします。
   2. **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード） > **Deactivate License(s)**（ライセンスの非アクティベート）を選択します。

   [ライセンスの非アクティブ化]フォームで、トークンテキストを貼り付けるか、インターネットにアクセスできるコンピューターにトークンをコピーし、トークンファイルを CSP にアップロードして、ライセンスの削除を完了します。
5. VM の削除

©2023 Palo Alto Networks, Inc.

インターネットアクセスなし — Panorama 管理

1. Panorama Web インターフェイスにログインして、**Panorama** > **Device Deployment**（デバイスのデプロイ） > **Licenses**（ライセンス）の順に選択します。
2. **VM** の非アクティブ化を行い、非アクティブ化する VM-Series ファイアウォールを選択します。
3. [手動で完了する]を選択して、トークンファイルをエクスポートします。
4. [ライセンストークンのエクスポート]リンクをクリックして、トークンファイルを保存します。トークンのファイル名は次のようになります。20150128_1307_dact_lic.01282015.130737.tok

   エクスポートが成功すると、完了メッセージが表示され、ファイアウォールが自動的に再起動します。
5. トークンファイルを使用して、変更をライセンスサーバーに登録します。

   1. Palo Alto Networks カスタマー サポート Web サイトにログインします。
   2. **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード） > **Deactivate License(s)**（ライセンスの非アクティベート）を選択します。

   [ライセンスの非アクティブ化]フォームで、トークンテキストを貼り付けるか、インターネットにアクセスできるコンピューターにトークンをコピーし、トークンファイルを CSP にアップロードして、ライセンスの削除を完了します。
6. (任意) 無効化された VM-Series ファイアウォールを Panorama の管理対象デバイスから削除します。

   非アクティブ化されたファイアウォールを削除する代わりに、別のデバイスグループを作成して割り当てることができます。

   1. **Panorama** > **Managed Devices** (管理対象デバイス)の順に選択します。
   2. 非アクティブ化したファイアウォールを選択し、[削除]をクリックします。

データプレーンコアのカスタマイズ

Software NGFW Creditsで説明したとおり, 、Software NGFW Credit を使用してファイアウォールをデプロイする場合、メモリプロファイルと vCPU の合計数によって、管理プレーンとデータプレーンに自動的に割り当てられるコアの数が決まります。デフォルトの構成は、ほとんどの場合、適切に稼働します。

データプレーンコアのカスタマイズは、次の 2 つの方法でデータプレーンコア数をカスタマイズできるオプション機能です。

- 初期デプロイメント時には、`init-cfg.txt` ファイルブートストラップパラメーター **`plugin-op-commands=set-dp-cores:<#-cores>`**を使用します。「Init-cfg.txt ファイルのコンポーネント」を参照してください。
- デプロイされたファイアウォールから、VM-Series CLI コマンド **`request plugins vm_series dp-cores <#-cores>`** を使用します。この手順を以下に概説します。

©2023 Palo Alto Networks, Inc.

通常、パフォーマンスを向上させるために、データプレーンコアの数を増やします (管理プレーンコアの数が減少します)。データプレーン コアのカスタマイズでは、vCPU の合計数が同じままであるため、デプロイメントプロファイルの変更や追加のクレジットは必要ありません。

- データプレーンコアのカスタマイズは、10.0.4以上の Software NGFW credit プールでライセンス供与された PAN-OS 10.1 以降を実行するファイアウォールでサポートされています。
- データプレーンコアのカスタマイズは、以下の場合はサポートされていません。
  - NSX-T
  - Intelligent Traffic Offload インテリジェント トラフィック オフロード

VM-Series ファイアウォール上のデータプレーン コアをカスタマイズするには、次の手順に従います。

STEP 1 | VM-Series ファイアウォールにログインし、コアの数を表示します。

```
admin@PA-VM(active)>show plugins vm_series dp-cores
Device current DP cores: 13 (Total cores: 18)
```

STEP 2 | データプレーンコアの数を変更します。

少なくとも *1* つの管理プレーン コアが必要です。コアが少なすぎるとパフォーマンスに影響を与えます。

この例では、データプレーンを 14 に増やします。

```
admin@PA-VM(active)>request plugins vm_series dp-cores 14
Device current DP cores: 14 (Total cores: 18)
```

STEP 3 | VM-Series ファイアウォールを再起動します。

デバイス > セットアップ > 操作を選択し、[デバイスの再起動] をクリックします。

STEP 4 | **show plugins vm_series dp-cores** を使用して、DP コアの数が変更されたことを確認します。

フレキシブル VM-Series ライセンスへの移行

VM-Series ファイアウォールの永続ライセンスまたは ELA ライセンスをフレキシブル VM-Series ファイアウォールライセンス（Software NGFW Credit を使用して資金提供）に移行できます。Panorama から個別のファイアウォールのライセンスを切り替えるか、または複数のファイアウォールのライセンスを一括で切り替えることができます。

©2023 Palo Alto Networks, Inc.

切り替えたいライセンスが、*ELA* または永続ライセンスを備えた *VM-Series* ファイアウォール用である場合は、固定モデルを選択し、フレキシブルライセンスの SW NGFW デプロイメントプロファイルを作成するときに、同じ *VM-Series* モデルと *vCPU* の数を使用する必要があります。 たとえば、現在 *2* つの *vCPU* を搭載した *VM-100* を使用している場合に、デプロイメントプロファイルを作成するには、*[*固定モデル*]*を選択し、*VM-100* を選択して、*2* つの *vCPU* を指定します。容量が同じであれば、新しいサービスを追加できます。

次のいずれかの手順を実行して、ライセンスを移行します。

- インターネットに直接アクセスできるスタンドアロンファイアウォール
- 直接インターネットにアクセスできないスタンドアロンファイアウォール
- インターネットに直接アクセスできる Panorama
- インターネットに直接アクセスできない Panorama
- 移行の確認

インターネットに直接アクセスできるスタンドアロンファイアウォール

このプロセスは、ファイアウォールを通過するトラフィックを中断しません。

STEP 1 | VM-Series ファイアウォール Web インターフェイスにログインします。

STEP 2 | Palo Alto Networks 更新サーバーの設定を確認します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
2. 更新サーバーが `updates.paloaltonetworks.com` に設定されていることを確認します。
3. 更新サーバー **ID** が選択されていることを確認します。

STEP 3 | CSP にログインし、デプロイメントプロファイルの作成を行います。移行するライセンスがELAまたは永久ライセンスの VM-Series ファイアウォール用である場合、固定モデルを選択し、フレキシブルライセンスの SW NGFW デプロイメントプロファイルを作成するときに、同じ VM-Series モデルと vCPU の数を使用する必要があります。

このプロファイルの認証コードを使用します。以下に示されているとおり、フレキシブルファイアウォールライセンスの認証コードは文字 D で始まります。

STEP 4 | **Device** > **Licenses** (デバイス > ライセンス)を選択します。

現在の VM-Series モデルと移行先の VM-Series モデルが異なる場合は、[**VM** 容量のアップグレード]リンクを選択します。

移行の前後で VM-Series モデルが同じである場合は、[認証コードを使用して機能をアクティベートする]リンクを選択します。

STEP 5 | 新しいデプロイメントプロファイルから VM-Series 認証コードを入力します。

©2023 Palo Alto Networks, Inc.

STEP 6 | [**OK**] をクリックしてライセンスのアップグレードを確認します。ファイアウォールは Palo Alto Networks 更新サーバーと通信し、VM-Series モデルに基づいてファイアウォールに必要なトークンを消費します。

STEP 7 | (任意) 移行を確認します。

STEP 8 | デプロイメントの各 VM-Series ファイアウォールでこの作業を繰り返します。

直接インターネットにアクセスできないスタンドアロンファイアウォール

インターネットに直接アクセスせずにファイアウォールでライセンスを移行します。

STEP 1 | 必要に応じて、VM-Series ファイアウォールにライセンス API キーをインストールします。

STEP 2 | CLI を使用して、手動モードを使用し、固定モデルライセンスを非アクティブ化します。

STEP 3 | 手動の手順を使用してファイアウォールから VM を非アクティブ化します。を行い、CSP にログインし、トークンファイルを使用して VM を非アクティブ化します。

STEP 4 | CSP では、古い固定モデルライセンスと同じ VM-Series モデル、vCPU の数、およびセキュリティサブスクリプションを使用してデプロイメントプロファイルの作成を行います。このプロファイルの認証コードを使用します。

STEP 5 | 新しいプロファイルを選択し、縦の省略記号をクリックして、[ファイアウォールの登録]を選択します。

1. VM とファイアウォールの情報を入力し、[サブミット]を選択します。これにより、ファイアウォールがプロファイルとその認証コードに関連付けられ、シリアル番号が割り当てられます。
2. [デバイスの表示]をクリックして、関連するデバイスをソフトウェア **NGFW** デバイスで確認します。
3. [ライセンス]列で、ファイルをホストマシンに安全に転送できる場所にライセンスキーをダウンロードします。

STEP 6 | ファイアウォールでデバイス > ライセンスを選択します。

ウェブ インターフェイス経由でライセンス キーをインストールしなければなりません。ファイアウォールは、*SCP* または *FTP* 経由でのライセンス キーのインストールはサポートしていません。

STEP 7 | ライセンス キーの手動アップロードリンクをクリックしてライセンス キーを入力します。

STEP 8 | ダッシュボードに有効なシリアル番号が表示され、**PA-VM** ライセンスがデバイス > ライセンスタブに表示されていることを確認します。

STEP 9 | (任意) 移行を確認します。

インターネットに直接アクセスできる Panorama

Panorama によって管理されているファイアウォールのライセンスを移行します。

©2023 Palo Alto Networks, Inc.

STEP 1 | **Panorama**、直接インターネットアクセス - Panorama によって管理されているファイアウォールのライセンスを移行します。

STEP 2 | 開始する前に、ファイアウォールにライセンス API キーがインストールされていることを確認してください。

STEP 3 | Panorama Web インターフェイスにログインします。

STEP 4 | ファイアウォールの Palo Alto Networks 更新サーバー設定を確認します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
2. 更新サーバーが `updates.paloaltonetworks.com` に設定されていることを確認します。
3. 更新サーバー **ID** が選択されていることを確認します。

STEP 5 | まだ行っていない場合は、新しいライセンスのデプロイメントプロファイルの作成を行います。このプロファイルは、移行後の Panorama の新しい認証コードを生成するために必要です。

STEP 6 | VM-Series 認証コードを取得します。以下に示すように、フレキシブルライセンスのファイアウォール認証コードは文字 F で始まります。

STEP 7 | 新しい認証コードを適用します。

1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Licenses**（ライセンス）の順に選択して、**Activate**（アクティベーション）をクリックします。
2. VM-Series 認証コードを入力します。
3. フィルターを使用してライセンスを付与する管理対象ファイアウォールを選択します。
4. 各ファイアウォールの **Auth Code**（認証コード）列に認証コードを入力します。
5. ライセンスのアップグレードを確認するために[アクティベート]します。Panorama は Palo Alto Networks の更新サーバーに接続し、選択した VM-Series モデル、vCPU、およびサービスに基づいてファイアウォールに必要なトークンを消費します。

STEP 8 | (任意) 移行を確認します。

インターネットに直接アクセスできない Panorama

インターネットに直接アクセスせずに、Panorama によって管理されている VM-Series ファイアウォールのライセンスを移行します。

STEP 1 | 開始する前に、ファイアウォールにライセンス API キーがインストールされていることを確認してください。

STEP 2 | **Panorama**、インターネットアクセスなし - Panorama によって管理されているファイアウォールのライセンスをオフラインで移行します

©2023 Palo Alto Networks, Inc.

STEP 3 | 手動の手順を使用してPanorama から VM を非アクティブ化します。を行い、CSP にログインし、トークンファイルを使用して VM を非アクティブ化します。

STEP 4 | CSP では、固定モデルライセンスと同じ VM-Series モデル、vCPU の数、セキュリティサブスクリプション、Panorama を使用してデプロイメントプロファイルの作成を行います。このプロファイルの認証コードを使用します。

STEP 5 | 新しいプロファイルを選択し、縦の省略記号をクリックして、[ファイアウォールの登録]を選択します。

1. VM とファイアウォールの情報を入力し、[サブミット]を選択します。これにより、ファイアウォールがプロファイルとその認証コードに関連付けられ、シリアル番号が割り当てられます。
2. [デバイスの表示]をクリックして、関連するデバイスをソフトウェア **NGFW** デバイスで確認します。
3. [ライセンス]列で、ファイルをホストマシンに安全に転送できる場所にライセンスキーをダウンロードします。

STEP 6 | 新しい認証コードを適用します。

1. **Panorama** > デバイスのデプロイメント > ライセンスを選択して、[アクティベート]をクリックします。
2. フィルターを使用してライセンスを付与する管理対象ファイアウォールを選択します。
3. 各ファイアウォールの[認証コード]列に、デプロイメントプロファイルの認証コードを入力します。
4. [アクティベート]をクリックして、ライセンスのアップグレードを確認します。Panorama は Palo Alto Networks の更新サーバーに接続し、選択した VM-Series モデル、vCPU、およびサービスに基づいてファイアウォールに必要なトークンを消費します。

STEP 7 | (任意) 移行を確認します。

移行の確認

ライセンスの移行が正常に完了したことを確認します。

STEP 1 | ライセンス有効期限を調べ、ライセンスの更新が正常に完了したことを確認します。

STEP 2 | デプロイメントプロファイルで有効になっているすべてのサブスクリプションがデバイスに適用されていることを確認します。

STEP 3 | CSP で、割り当てられたクレジットの予想数と、クレジットプールの一致に対して消費されたクレジットを確認します。

STEP 4 | CSP で、関連するトークンまたはライセンスの数が以前の認証コードに戻されていることを確認します。

©2023 Palo Alto Networks, Inc.

VM-Series モデル

VM-Series ファイアウォール
は、VM-50、VM-100、VM-200、VM-300、VM-500、VM-700、VM-1000-HV の各固定 vCPU モデルで利用できます。これらのモデルは、以下で特に明記されていない限り、サポートされているすべてのPAN-OSバージョンで使用できます。VM-Series ファイアウォールのデプロイに使用されるソフトウェア パッケージ（*.xva*、*.ova*、あるいは *.vhdx* ファイル）は、すべてのモデルに共通です。

固定モデルの *ELA* または永久ライセンスを
フレキシブルライセンスに移行して固定モデルを保持することも、ライセンスをフレキシブル *vCPU* ライセンスに置き換えることもできます。ライセンス方法を比較するには、VM-Series ファイアウォールライセンスを参照してください。

- すべてのモデルは VMware ESXi および vCloud Air、KVM、Microsoft Hyper-V、Cisco ACI、Cisco ENCS、および Cisco CSP 上でゲスト仮想マシンとしてデプロイできます。
- パブリッククラウド環境（Amazon Web Services、Azure、Google Cloud Platform、Oracle Cloud Infrastructure、Alibaba Cloud）では、VM-50 を除くすべてのモデルがサポートされています。
- VMware NSX の場合、VM-100、VM-200、VM-300、VM-500、および VM-1000-HV ファイアウォールのみがサポートされます。

VM-Series ファイアウォールにキャパシティ ライセンスを適用すると、ファイアウォールにモデル番号とその関連機能が実装されます。キャパシティは、VM-Series ファイアウォールで最適に処理できるセッション数、ルール数、セキュリティ ゾーン数、アドレス オブジェクト数、IPSec VPN トンネル数、および SSL VPN トンネル数に基づいて定義されます。ネットワーク環境に合ったモデルを購入するためにも、以下の表を使い、各モデルの最大キャパシティやモデル別のキャパシティの違いを把握してください。

model	sessions	セキュリティルール数	ダイナミック IP アドレス数	セキュリティゾーン数	IPSec VPN トンネル数	SSL VPN トンネル数
VM-50IPv6	50,000	• 250 • 200（Lite モード）	1,000	15	• 250 • 25（Lite モード）	• 250 • 25（Lite モード）
VM-100IPv6 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300IPv6	800,000	10,000	100,000	40	2,000	2,000

©2023 Palo Alto Networks, Inc.

model	sessions	セキュリティルール数	ダイナミック IP アドレス数	セキュリティゾーン数	IPSec VPN トンネル数	SSL VPN トンネル数
VM-1000-HV						
VM-500IPv6	2,000,000	10,000	100,000	200	4,000	6,000
VM-700IPv6	10,000,000	20,000	100,000	200	8,000	12,000

SD-WAN機能は、*VM-50*と*VM-100*を除く、すべての*VM-Series*モデルでサポートされています。

VM-Series ファイアウォールをデプロイできるプラットフォームの詳細は、「VM-Series デプロイメント」を参照してください。VM-Series ファイアウォール モデルの詳細は、Palo Alto Networks ファイアウォールの比較ツールを参照してください。VM-Series ファイアウォールについての一般情報を確認することもできます。

- VM-Series のシステム要件
- CPU オーバーサブスクリプション
- VM-50 Lite モード
- VM-Series モデルのライセンスタイプ
- VM-Series モデルライセンスのアクティベート
- VM-Series ファイアウォールの登録
- VM-Seriesファイアウォールへのデバイス証明書のインストール
- BYOL ライセンスと PAYG ライセンスの切り替え
- 固定モデル ライセンス間の切り替え
- ライセンスの非アクティブ化
- VM-Series ファイアウォールのライセンス バンドルを更新

VM-Series のシステム要件

VM-Series ファイアウォールの各インスタンスには、ホスト サーバー上に最小リソースの割り当て（CPU 数、メモリおよびディスク領域）が必要です。次の表を使用して、VM-Series モデルまたはメモリプロファイルに必要なハードウェアリソースを割り当てていることを確認します。

©2023 Palo Alto Networks, Inc.

VM-Series モデル	サポートされているハイパーバイザ	サポートされている vCPU	最小メモリ	GTP が有効状態での最小メモリ	最小ハード ドライブ
VM-50IPv6	ESXi、Hyper-V、KVM	2	• 5.5GB • 4.5GB（Lite モード）	• 6GB • 5GB（Lite モード）	32GB（起動時は 60GB）
VM-100IPv6	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-100) *Azure 上の VM-100 には 4 つの仮想 CPU が必要です。*	2	6.5GB	7.5GB	60GB
VM-300IPv6	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-300)	2、4	9GB*	10GB	60GB
VM-500IPv6	AWS、Azure、Cisco ACI、Cisco CSP、ESXi、Google Cloud Platform、Hyper-V、 KVM、OCI、NSX-T	2、4、8	16GB	20GB	60GB
VM-700IPv6	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	2、4、8、16	56GB	64GB	60GB

* 10.1.X では、ファイアウォールで使用される機能セットまたは機能セットの組み合わせによっては、9 GB では不十分な場合があります。メモリリソースに関連する問題が発生した場合は、一部の機能または機能の組み合わせの追加メモリ要件を満たすために、メモリを 11 GB に増や

©2023 Palo Alto Networks, Inc.

します。または、VM-Series ファイアウォールでの ZRAM の有効化を行ってメモリ使用量を改善することもできます。

VM-50 で Lite モードを有効にすることができます。Lite モードは、リソースが制限されている環境での代替動作モードです。詳細については、VM-50 Lite モードを参照してください。

最高のパフォーマンスを実現するには、必要なすべてのコアを *1* つの *CPU* ソケットで使用できる必要があります。

VM-50 ファイアウォールの動作には、最低 *32GB* のハード ドライブ領域が必要です。ただし、*VM-Series* の基本イメージはすべてのモデルで共通しているため、*VM-50* にライセンスを付与するまでは *60GB* のハード ドライブ領域を割り当てる必要があります。

管理プレーンに割り当てられる vCPU の数とデータプレーンに割り当てられる vCPU の数は、VM-Series ファイアウォールに割り当てられる vCPU の合計数によって異なります。ライセンスで正式にサポートされているよりも多くの vCPU を割り当てると、追加の vCPU が管理プレーンに割り当てられます。

合計 **vCPU** 数	管理プレーンの **vCPU** 数	データプレーンの **vCPU** 数
2	1	1
4	2	2
8	2	6
16	4	12

CPU オーバーサブスクリプション

VM-Series ファイアウォールは、すべてのモデルで CPU オーバーサブスクリプションをサポートしています。CPU オーバーサブスクリプションを使用すると、x86 アーキテクチャ上で稼働しているハイパーバイザーに VM-Series ファイアウォールをより高密度にデプロイできます。割り当てが必要な CPU あたり、2 個（2:1）～ 5 個（5:1）の VM-Series ファイアウォールをデプロイできます。デプロイメントを計画するときは、以下の式を使用して、ハードウェアでサポートされる VM-Series ファイアウォールの数を計算します。

（合計 CPU 数 x オーバーサブスクリプション率）/ファイアウォールあたりの CPU 数 = VM-Series ファイアウォールの総数

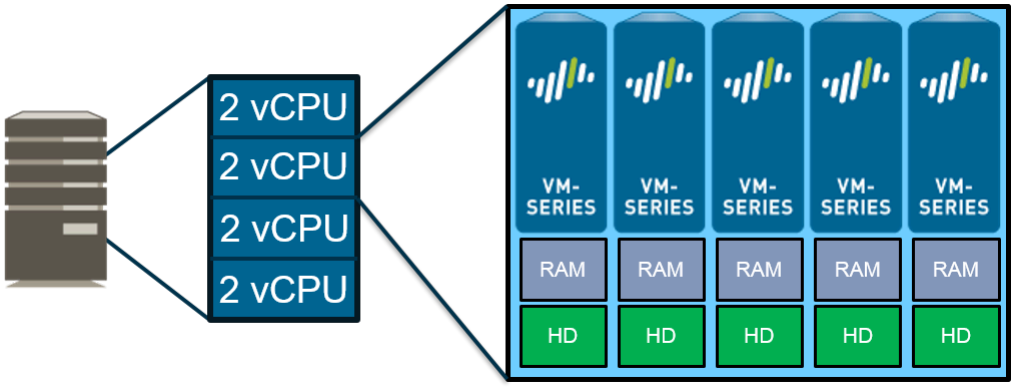
たとえば、比率が 5:1 の場合、ホスト マシンの物理 CPU が 16 個でメモリが 180GB（40 × 4.5GB）以上であれば、VM-50 のインスタンスを最大 40 個サポートできます。各 VM-50 には 2 個の vCPU が必要ですが、vCPU の各ペアに 5 個の VM-50 を関連付けることができます。

（16 個の CPU x 5）/2 = 40 個の VM-50 ファイアウォール

最低限のVM-Series システム要件を満たせば、追加の設定を行わなくても、オーバーサブスクリプションを利用できます。VM-Series ファイアウォールを通常通りデプロイすれば、リソース

©2023 Palo Alto Networks, Inc.

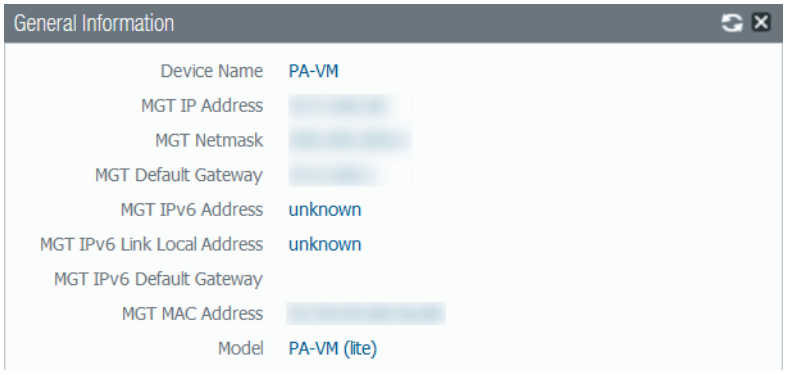
オーバーサブスクリプションが自動的に実行されます。デプロイメントを計画するときは、仮想スイッチなどのその他の機能と、専用のハードウェア リソースが必要なホスト上のゲスト マシンについて検討してください。



VM-50 Lite モード

標準の VM-50 は VM-Series の最小モデルですが、一部の環境で使用可能なリソースよりも多くのリソースを必要とします。VM-50 Lite モードは、ハードウェア リソースが制約されている環境の代替手段です。VM-50 Lite は、標準 VM-50 で必要とされるメモリ 5.5GB ではなく 4.5GB を必要とします。VM-50 Lite は、標準 のVM-50 と同じライセンスを使用しますが、4.5GB の RAM が割り当てられていると Lite モードになります。

- 高可用性環境では、容量不一致の問題が起きないように、*VM-Series* ファイアウォールの両方に *VM-50 Lite* のライセンスが必要です。容量ライセンスの不一致の場合、*VM-50*（非 *Lite*）は容量が大きいとみなされます。 *VM-50 Lite* が機能している間は、*VM-50* は機能しなくなります。
- *VM-50 Lite*はジャンボフレームをサポートしていません。*VM-50*および*VM-50 Lite*は、*WildFire*インライン*ML*をサポートしていません。



 ©2023 Palo Alto Networks, Inc.

VM-Series モデルのライセンスタイプ

VM-Seriesファイアウォールでは、以下のライセンスおよびサブスクリプションが利用可能です。

- **Capacity License**（キャパシティ ライセンス） — VM-Series ファイアウォールは、モデルナンバー（VM-50、VM-100、VM-200、VM300、VM-500、VM-700、または VM-1000-HV）および、ファイアウォール上の関連するキャパシティを有効化する際に、キャパシティ ライセンスと呼ばれるベース ライセンスを必要とします。キャパシティ ライセンスはバンドルに含まれており、永久ライセンスと期間限定ライセンスがあります。
  - **Perpetual License**（永久ライセンス） - ライセンスが付与されたキャパシティにおいてVM-Series ファイアウォールを無期限に使用できる、失効日のないライセンスです。永久ライセンスがお求めいただけるのはVM-Seriesキャパシティライセンスのみです。
  - **Term-Based License**（期間ベースのライセンス） - 期間ベースのライセンスでは、VM-Series ファイアウォールを特定の期間中使用することができます。これには失効日が設定されていて、失効前に更新を促すお知らせが表示されます。キャパシティライセンス、サポート資格、およびサブスクリプションなどで期間ベースのライセンスがご利用いただけます。
- **VM-Series ELA** — 高成長企業の場合、VM-Series エンタープライズ ライセンス契約（VM-Series ELA）は、ファイアウォールのデプロイを高速にするために、無制限の VM-Series ファイアウォールをデプロイできるオプションを BYOL に加えた固定額のライセンス オプションを提供します。ELA には、契約終了時に変更されない 1 年および 3 年の利用規約が伴います。

  VM-Series ELA には次の 2 種類があります。

  - 2018 年 12 月 4 日よりも前に購入された VM-Series ELA は、サポートされているすべてのハイパーバイザーまたはパブリック クラウド環境で、選択した 1 つの VM-Series モデルを含むレガシー VM-Series ELA です。この ELA では VM-Series ファイアウォールの各インスタンスに対し、キャパシティ、サポート、GlobalProtect、PAN-DB URL フィルタリング、脅威防止、および WildFire サブスクリプション用の単一のライセンス認証コードを受け取ります。また、Panorama バーチャル アプライアンスを無制限でデプロイでき、アプライアンスごとに 1000 ファイアウォールのデバイス管理ライセンスが含まれています。

    Palo Alto Networks はこのレガシー VM-Series ELA の廃止を 2019 年 4 月 16 日から開始します。既存のエンタープライズ ライセンスをご利用のお客様には、アカウントがマルチモデル ELA へ移行した時点でサポート担当者から通知が送られます。VM-Series ファイアウォール サブスクリプション契約に基づいてライセンス トークンが配布されます。ファイアウォールの継続運用のために行う必要がある追加の操作はありません。VM-Series ELA ライセンス トークンの管理をご希望の場合は、ELA 管理者を指定する必要があります。ELA 管理者を割り当てることができるのは、Palo Alto Networks カスタマー サポート ポータル（CSP）のスーパー ユーザー ロールのみです。
  - 2018 年 12 月 4 日以降に（新規購入またはレガシー VM-Series ELA の再購入で）購入された VM-Series エンタープライズ ライセンス契約（マルチモデル ELA） は、マルチモデル VM-Series ELA と呼ばれます。この ELA には、VM-Series ファイアウォール ポートフォリオのほとんどのモデルと、GlobalProtect、PAN-DB URL フィルタリング、脅威防止、WildFire サブスクリプション、およびサポート資格が含まれています。ま

©2023 Palo Alto Networks, Inc.

た、Panorama バーチャル アプライアンスを無制限でデプロイでき、アプライアンスごとに 1000 ファイアウォールのデバイス管理ライセンスが含まれています。

パブリック クラウドの VM-Series ファイアウォール ライセンス

VM-Series のファイアウォール ライセンス戦略は、AWS、Azure、Google Cloud Platform で同じです。さまざまなライセンスタイプがあり（「「ライセンス タイプ– VM-Series ファイアウォール」を参照）、独自のライセンスおよび Pay-as-you-go：都度払いライセンス方式を提供する：

- **Bring Your Own License（BYOL）（持ち込みライセンス（BYOL））** - パートナー、販売代理店、あるいは Palo Alto Networks から直接購入可能なライセンスです。BYOLは、個々の容量ライセンス、サポート ライセンス、およびサブスクリプション バンドルをサポートしています。
  - BYOL ライセンスの場合、VM-Seriesファイアウォールのデプロイ後に認証コードを適用する必要があります。
  - BYOL ライセンス バンドルには、ブート ストラップ パッケージに含めることができる 1 つの認証コードがあります（「VM-Series ファイアウォールのブートストラップ」を参照）。バンドルに含まれるすべてのサブスクリプションは、ファイアウォールの起動時にライセンス提供されます。
- **PAYG（pay-as-you-go：都度払い）**–従量制または利用回数制とも呼称されます。PAYG ライセンスはクラウド プロバイダーから購入できます：
  - AWS：AWS Marketplace から購入します。毎時と年間 PAYG オプションをサポートしています。
  - Azure：Azure Marketplace から購入します。毎時 PAYG オプションをサポートします。
  - Google Cloud Platform：Google Cloud Platform Marketplaceから購入します。Google Cloud Platform では、1 分あたりの PAYG オプションがサポートされています。
  - Oracle Cloud Infrastructure:（PAN-OS 10.0.3以降）Oracle Cloud Marketplaceから購入します。

    OCI PAYGライセンスのVM-Seriesは、VM-100をサポートしていません。

  PAYG ライセンス バンドルでは、デプロイすると同時にファイアウォールが使用可能になります（認証コードは送付されません）。クラウド コンソールからファイアウォールを停止または終了すると、PAYG ライセンスは一時停止または終了されます。

  PAYG ライセンスは、インスタンスに割り当てられたハードウェアに基づいて、VM-Series キャパシティ ライセンスを適用します。PAYG インスタンスは、インスタンスで利用できるハードウェア リソースの量をチェックして、利用可能なリソースに対して許可されている最大の VM-Series ファイアウォール キャパシティ ライセンスを適用します。たとえば、インスタンスに 2 つの vCPU と 16GB のメモリがある場合、vCPU の 数に基づいて VM-100 キャパシティ ライセンスが適用されます。ただし、インスタンスに 16 個の vCPU と 16GB のメモリーがある場合は、メモリの量に基づいて VM-500 キャパシティ ライセンスが適用されま

©2023 Palo Alto Networks, Inc.

す。VM-Series モデルのリソース要件の詳細は、「VM-Series のシステム要件」を参照してください。

最初に *PAN-OS 9.1.2* でデプロイされた *PAYG* ファイアウォール インスタンスに対する、*PAN-OS* のダウングレードはサポートされていません。*PAN-OS 9.1.2* より前の *OS* でデプロイされたファイアウォール インターフェイスは、古いバージョンの *PAN-OS* にダウングレードすることができます。

PAYG ライセンスは次のようにバンドルされています：

ライセンス機能	バンドル 1	バンドル 2
VM-Series ファイアウォール容量ライセンス	VM-100、VM-300、VM-500、VM-1000	VM-100、VM-300、VM-500、VM-700
プレミアムサポート	✓	✓
脅威防止（AV、IPS、およびマルウェア防止）	✓	✓
GlobalProtect		✓
PAN-DB URL Filtering		✓
WildFire		✓
DNS セキュリティ		✓

適用した*PAYG* ライセンスの表示に *VM-Series* ファイアウォール *CLI* を使用する場合、***show system info*** コマンドは、***request license info*** コマンドで表示される出力とは異なる値を表示します。*PAN-OS* バージョン *9.1.1* 以前の場合、コマンド ***request license info*** は、適用された *VM-Series* モデルに関係なく、モデルは常に *VM-300* として表示されます。

PAYG ライセンスと BYOL ライセンスを切り替えることはできません。PAYG から BYOL へ移行するには、Palo Alto Networks チャネル パートナーまたは販売代理店に問い合わせて、BYOL ライセンスを購入し、ファイアウォールにライセンスを付与するために使用できる BYOL 認証コードを取得します。ファイアウォールがデプロイされている状態で、ライセンスを切り替える方法については、「BYOL ライセンスと PAYG ライセンスの切り替え」を参照してください。

VM-Series ファイアウォールの評価版を持っていて、同じライセンス タイプ（*BYOL* または *BYOL*）の購入したフル ライセンス版に変更する場合、評価版ライセンスを無効化し、代わりに購入したライセンスをアクティベートできます。手順については、「VM-Series ファイアウォールのアップグレード」を参照してください。

©2023 Palo Alto Networks, Inc.

VM-Series エンタープライズ ライセンス契約（マルチモデル ELA）

VM-Series エンタープライズ ライセンス契約（VM-Series ELA）は 1 年または 3 年の包括的なライセンス契約であり、GlobalProtect、PAN-DB URL フィルタリング、脅威防止、WildFire、および DNS Security サブスクリプションを含めて VM-Series ファイアウォールを購入できるようになります。また、Panorama のサポート資格とデバイス管理ライセンスも含まれています。マルチモデル VM-Series ELA では、1 つの契約で企業のセキュリティ ニーズに応じた VM-Series ファイアウォールのモデルをデプロイできるので、ライセンス管理がシンプルになります。

マルチモデル VM-Series ELA を購入する際には、サブスクリプション期間に渡って必要となるファイアウォールの数を予測します。この予測と、今後の成長に対応する追加の割り当てに基づき、カスタマー サポート ポータル（CSP）のアカウントにライセンス トークン プールが付与されます。このライセンス トークン プールにより、VM-Series ファイアウォールの任意のモデルをデプロイできるようになります。ファイアウォール モデルとデプロイするファイアウォールの数に応じて、使用可能なライセンス トークンのプールから指定の数のトークンが差し引かれます。アカウントから差し引かれるトークンの数は、各ファイアウォール モデルの値に基づいて算出されます。

- VM-50 — 10 トークン
- VM-100 — 25 トークン
- VM-300 — 50 トークン
- VM-500 — 140 トークン
- VM-700 — 300 トークン

VM-Series ELA では、有効期限の最終日に調整が行われることはありません。つまり、デプロイしたファイアウォールの数が予測の数を超えても、遡って請求されることがありません。したがって、柔軟性と説明責任のバランスをとるため、VM-Series ELA の利用条件には、トークンの消費方法と必要時のファイアウォールのデプロイ方法を説明した限定期間と無限定期間が併記されています。詳細については、ELA の契約条件を参照してください。VM-Series ELA でデプロイする VM-Series ファイアウォールには永久ライセンスは含まれていません。したがって、サポート資格を延長し、ファイアウォールのソフトウェア更新とコンテンツ リリース更新に引き続きアクセスするためには、有効期限が切れた時点で契約を更新する必要があります。

CSP で ELA 管理者ロールが付与されている場合は、ライセンス トークンを、独自の CSP アカウントを持ち、異なる部門に所属している他の管理者に移譲するか、または管理者間に分割できます。この共有機能により、社内の他の管理者は、各自の CSP アカウントに使用可能なトークンがある限り、VM-Series ファイアウォールを必要に応じてデプロイできます。ELA トークンを共有するよう他の管理者を招待し、社内のセキュリティ ニーズに対応する VM-Series ファイアウォール モデルをデプロイするには、「VM-Series ELA ライセンス トークンの管理」を参照してください。また、組織内のニーズの変化に基づいてトークンを再配布する場合には、トークンを取り戻して、VM-Series ELA から CSP アカウントを削除することができます。

VM-Series マルチモデル ELA ビデオの視聴

- VM-Series ELA ライセンス トークンの管理
- VM-Series AMI ELA の同意

©2023 Palo Alto Networks, Inc.

VM-Series ELA ライセンス トークンの管理

VM-Series エンタープライズ ライセンス契約（マルチモデル ELA）（VM-Series ELA）により、社内の他の管理者と 1 つの契約を共有できる柔軟性が実現します。ELA をアクティベートするには、Palo Alto Networks カスタマー サポート ポータル（CSP）のスーパー ユーザー ロールが必要です。ELA 認証コードのアクティベーションが完了すると、CSP で ELA 管理者ロールを継承します。

ELA 管理者ロールにより、この契約に含まれるサブスクリプションと、VM-Series ファイアウォールのデプロイに使用できるライセンス トークン プールを管理できます。VM-Series ELA トークンの共有に他の管理者を招待し、各管理者が利用できる VM-Series ファイアウォールのインスタンス数とモデルを設定し、VM-Series ELA から CSP アカウントを削除することができます。各付与対象者は割り当てられている内容に応じて、VM-Series ファイアウォールのデプロイに使用できる特定数のトークンを受け取ります。

追加の購入や付与によって、*CSP* アカウントで使用可能な *VM-Series* ファイアウォールの数が直接増えることはありませんが、*ELA* ライセンス トークンが *VM-Series ELA* トークン プールに追加されます。その後、*ELA* 管理者が特定の *CSP* アカウントに *ELA* ライセンス トークンを割り当てることで、使用可能な *VM-Series* ファイアウォールの数を増やすことができます。

STEP 1 | （レガシー VM-Series ELA をご利用のお客様のみ）トークンを管理する ELA 管理者を指定します。

マルチモデル ELA に移行した既存のエンタープライズ ライセンスのお客様は、VM-Series ELA ライセンス トークンを管理する ELA 管理者を指定する必要があります。変換後に、ファイアウォールを継続的に運用するために必要な操作はありませんが、ELA 管理者が割り当てられるまでは、ファイアウォールをデプロイするためのトークンの（再）割り当ては実行できません。CSP でスーパー ユーザー ロールを持つ管理者だけが ELA 管理者を指定できます。ELA 管理者はトークンを管理し、他の管理者にトークンを付与できます。

1. Palo Alto Networks CSP にログインします。
2. **Members**（メンバー） > **Manage Users**（ユーザーの管理）を選択します。
3. **Actions**（アクション）の下の鉛筆アイコンをクリックして、ELA 管理者ロールを割り当てるユーザーを編集します。
4. **ELA Administrator**（**ELA** 管理者）を選択してからチェック マークをクリックし、選択したユーザーに新しいロールを追加します。
5. ステップ 3 に進みます。

©2023 Palo Alto Networks, Inc.

STEP 2 | ELA 認証コードをアクティベートします。

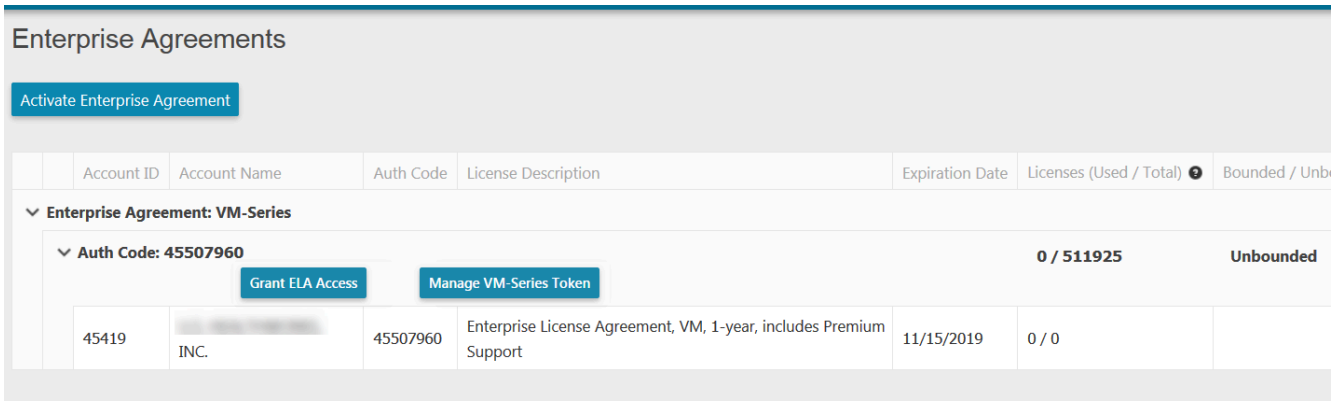
ELA をアクティベートする管理ユーザーは CSP で ELA 管理者ロールとスーパー ユーザー ロールを継承し、トークンの管理と他の管理者へのトークンの付与を実行できます。

1. Palo Alto Networks CSP にログインします。
2. **Assets**（アセット） > **Enterprise Agreements**（エンタープライズ契約） > **Activate Enterprise Agreement**（エンタープライズ契約のアクティベート）を選択します。
3. **Authorization code**（認証コード）を入力し、EULA に **Agree and Submit**（同意して送信）します。

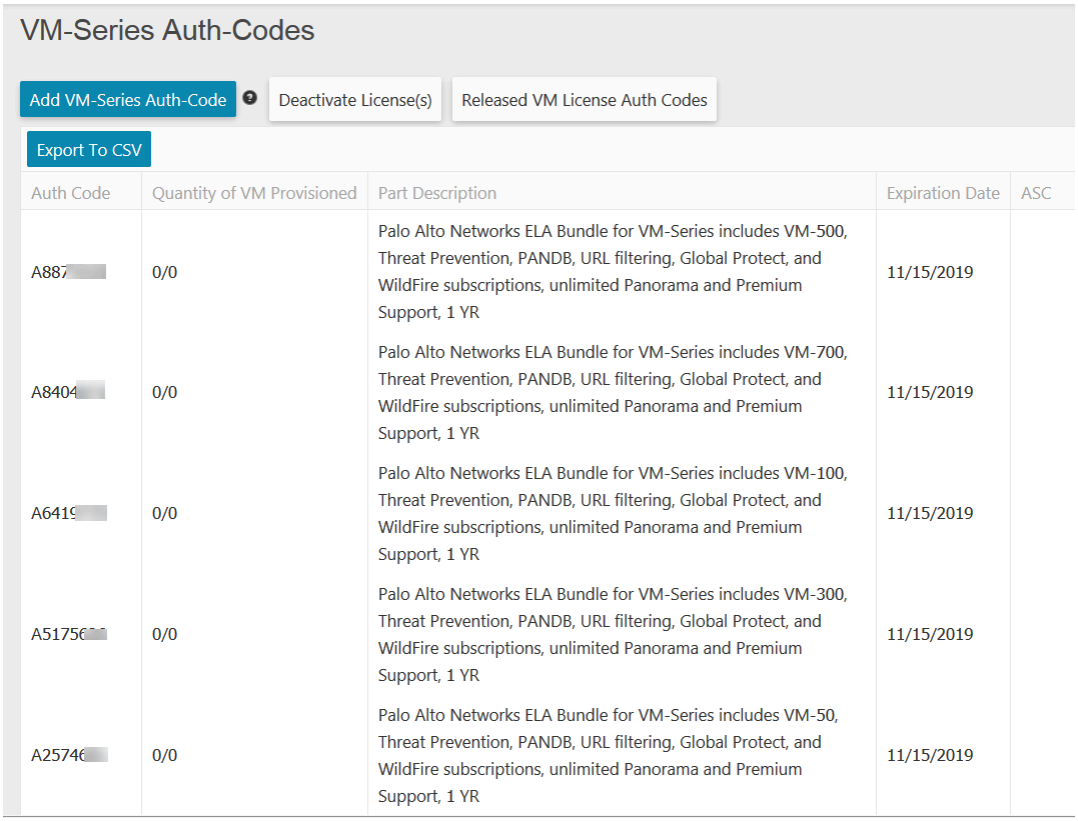
   次の場所から、認証コードがアカウントに登録されていることを確認します:Enterprise Agreements: VM-Series（エンタープライズ契約:VM-Series）。このページには、Auth Code（認証コード）、Account ID（アカウント ID）、Account Name（アカウント名）、License Description（ライセンスの説明）、Expiration Date（有効期

©2023 Palo Alto Networks, Inc.

限）、Licenses (used/total)（ライセンス数（使用済み/合計））、および契約の限定期間と無限定期間にデプロイできる数が表示されます。



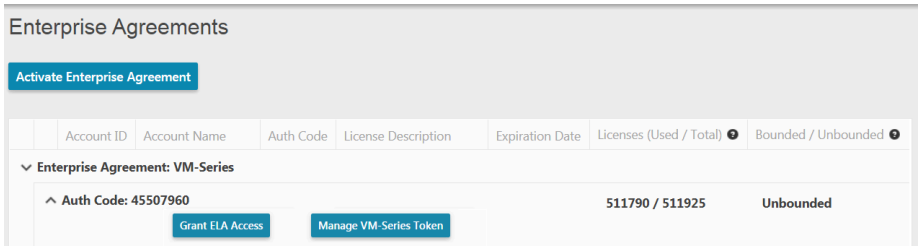
4. **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード）を選択します。各 VM-Series ファイアウォール モデルをデプロイするための認証コードと、ELA に含まれている関連サブスクリプションが表示されます。



©2023 Palo Alto Networks, Inc.

STEP 3 | 社内の他の管理者に ELA アクセス権を付与します。

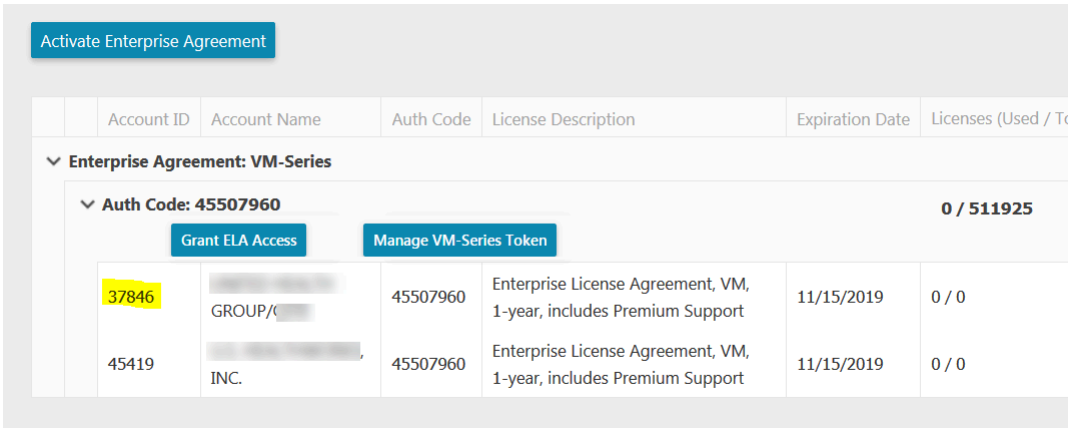
この機能により、VM-Series ELA を社内や部門内の他の管理者と共有でき、これらの管理者が必要に応じて VM-Series ファイアウォールをデプロイできます。ELA 管理者として、CSP でメール アドレスを使用して登録されている他のユーザーにアクセス権を付与できます。



1. **Assets**（アセット） > **Enterprise Agreements**（エンタープライズ契約）で **Grant ELA Access**（**ELA** アクセス権の付与）を選択します。
2. 招待する管理者の **Destination Email**（宛先メール）アドレスを入力します。

   上記で入力する宛先メール アドレスは、CSP でスーパー ユーザー ロールが付与されている登録ユーザーである必要があります。これにより、これらの登録ユーザーはログインして付与を受け入れることができます。メール アドレスが CSP に登録されていない場合、最初に **Members**（メンバー） > **Create New User**（新規ユーザーの作成）でユーザーの新しいアカウントを作成する必要があります。
3. **Notify User**（ユーザーに通知）を選択して、入力したメール アドレス宛ての通知メールをトリガーします。

   受信者は、VM-Series AMI ELA の同意のために CSP にログインする必要があります。受信者が付与を受け入れると、以下のスクリーンショットに示すように **Assets**（アセット） > **Enterprise Agreements**（エンタープライズ契約）でアカウント ID が使用可能になります。



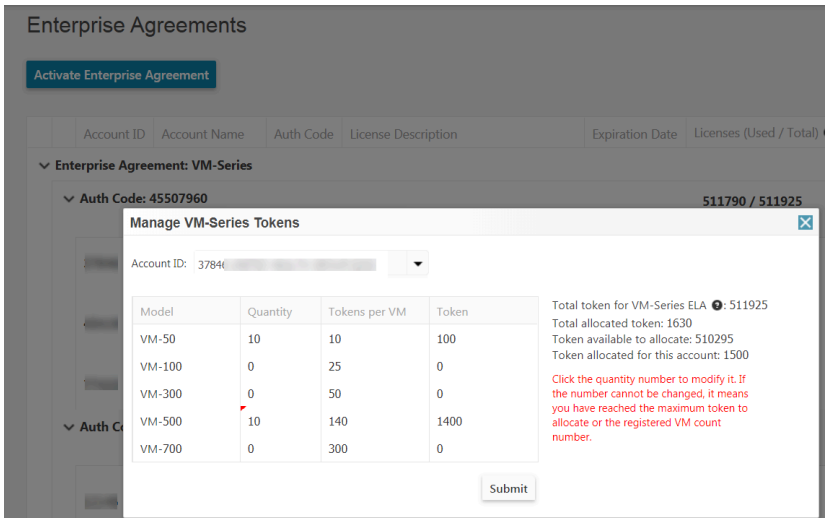
STEP 4 | ファイアウォールをデプロイするためトークンを割り当てます。

1. **Assets**（アセット） > **Enterprise Agreements**（エンタープライズ契約） > **Manage VM-Series Tokens**（**VM-Series** トークンの管理）を選択します。

   アカウント ID ごとに、割り当てるモデル別のファイアウォール数を指定します。ファイアウォールの数とモデルに基づいてトークンの数が自動的に計算され、使用可能に

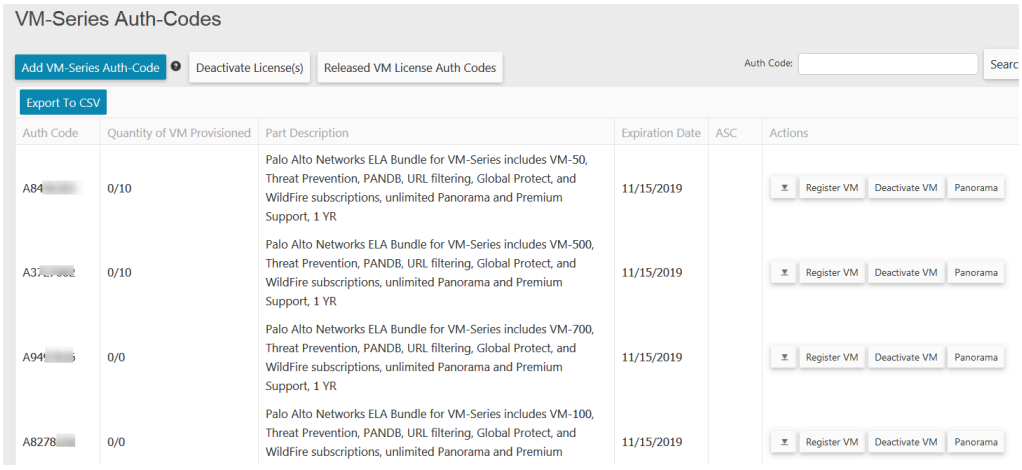
©2023 Palo Alto Networks, Inc.

なります。この例では、VM-50 と VM-500 で、それぞれ 10 個のインスタンスが許可されます。



2. ファイアウォール インスタンスの正確な数がアカウントに保存されていることを確認します。

   Assets（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード）を選択し、割り当てる認証コードを探します。この例に示すアカウントでは、VM-50 と VM-500 で、それぞれ 10 個のインスタンスをプロビジョニングできます。受信者がファイアウォールをデプロイすると、使用可能なすべてのトークンのプールから、特定数のトークンが差し引かれます。プロビジョニングしたファイアウォール インスタンスの数は、割り当てたインスタンスの合計数に対する比率として表示されます。使用可能なトークンがある限り、セキュリティのニーズの拡大に従って、割り当てる数量を増やしたり、異なる VM-Series ファイアウォール モデルへのアクセスを許可するなど、柔軟な対応が可能です。



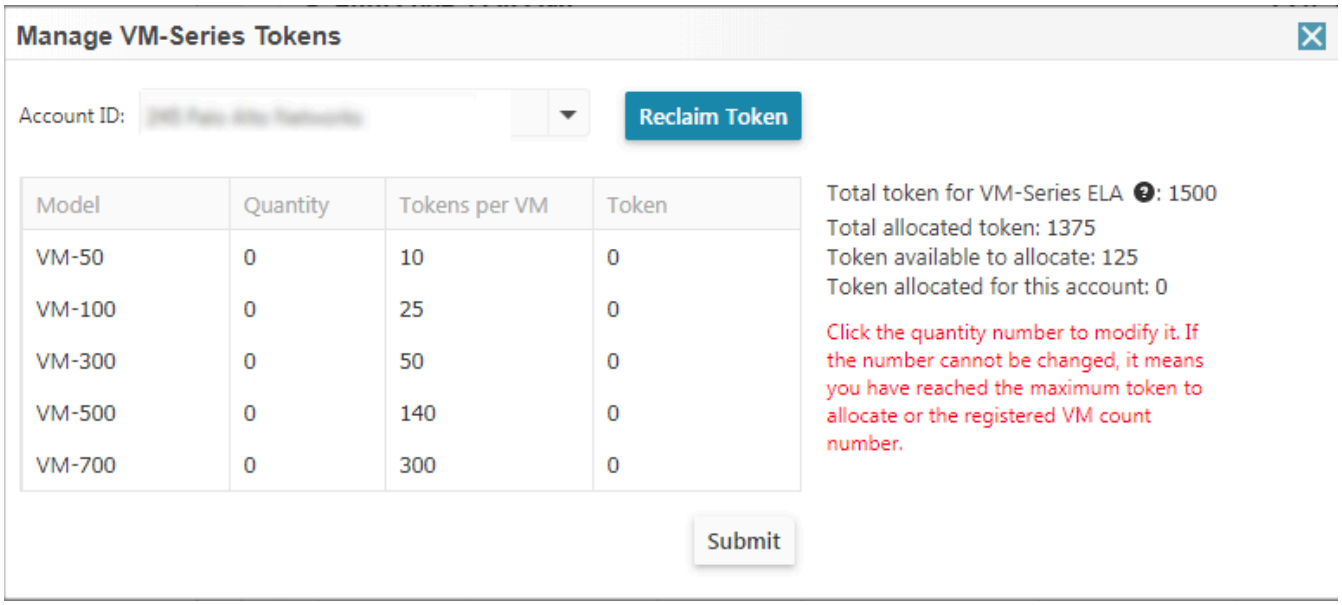
©2023 Palo Alto Networks, Inc.

STEP 5 | トークンを再利用するには VM-Series ELA から CSP アカウントを削除します。

CSP アカウントに割り当てられているトークンの一部を再利用することはできません。トークンを再利用するには、*VM-Series ELA* から *CSP* アカウントを完全に削除し、関連付けられているトークンをすべてトークン プールに再度割り当てます。

1. 削除する CSP アカウントに関連付けられているすべてのトークンが、VM-Series ファイアウォールにより使用されていないことを確認します。削除のためのトークンのプロビジョニングに必要な場合は、VM-Series ファイアウォールを無効化します。
2. **Assets**（アセット） > **Enterprise Agreements**（エンタープライズ契約）**> Manage VM-Series Token**（**VM-Series** トークンの管理）を選択します。

   再利用するトークンのアカウント ID を選択し、**Reclaim Token**（トークンを再利用）をクリックします。トークンが再利用可能になると、削除が正常に完了したことの通知を受信します。



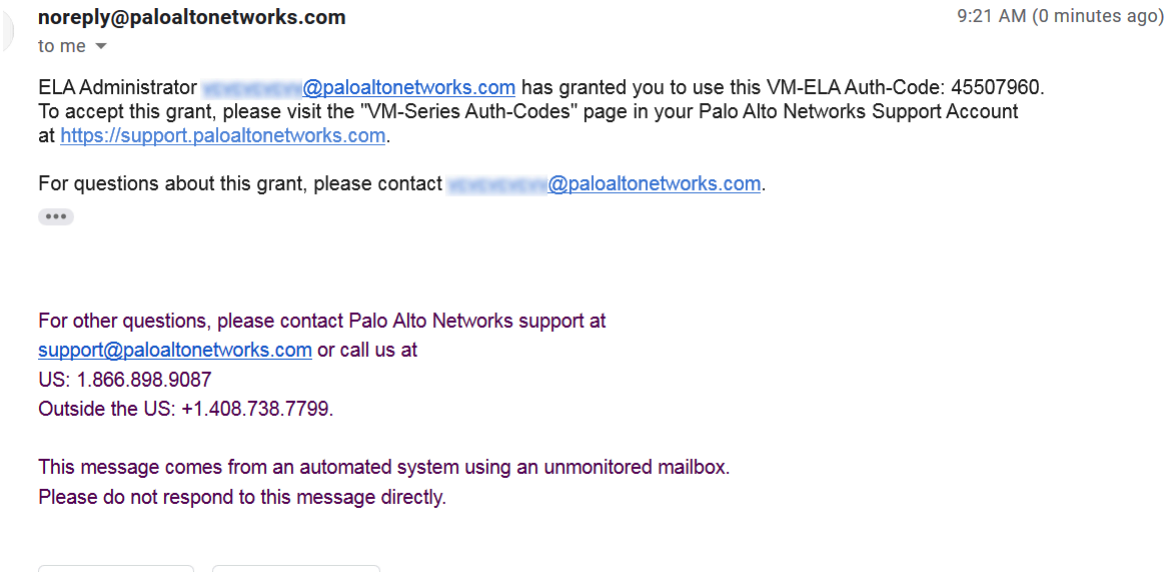
VM-Series AMI ELA の同意

所属する企業が VM-Series ELA を購入している場合、ELA 管理者から契約の共有とライセンス トークン プールの共有に招待されることがあります。これにより、VM-Series ファイアウォールの認証コードにアクセスでき、必要に応じて VM-Series ファイアウォールをデプロイできます。VM-Series ELA へのアクセス権が付与されたら、Palo Alto Networks カスタマー サポート ポータル（CSP）にログインするためのリンクが記載された通知メールを受信します。使用条件に同意する必要があります。ELA の使用条件に同意したら、使用できる VM-Series ファイアウォール モデルとファイアウォールの数を ELA 管理者が割り当てることができるようになります。また、対応する数の VM-Series ELA トークンがアカウントに与えられます。

©2023 Palo Alto Networks, Inc.

STEP 1 | メールの受信ボックスで付与通知を確認してください。

通知には、あなたを VM-Series ELA の共有に招待した ELA 管理者のメール アドレスが記載されています。



STEP 2 | 付与を受け入れます。

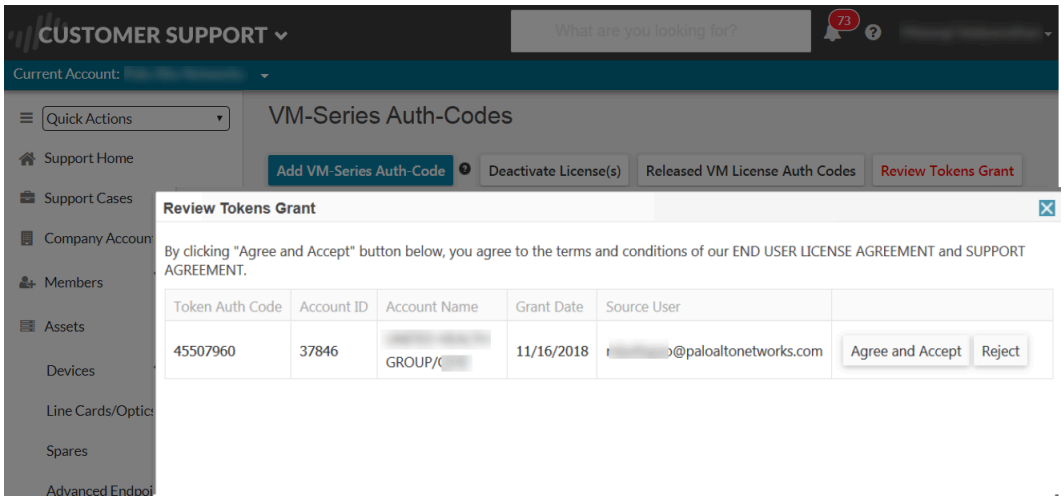
VM-Series ファイアウォールをデプロイできるようにするトークンを ELA 管理者が割り当てるには、その前に、契約条件を確認して EULA とサポート契約に同意する必要があります。

1. Palo Alto CSP にログインします。
2. **VM-Series Auth Codes**（**VM-Series** 認証コード）を選択し、**Review Tokens Grant**（トークンの付与を確認）します。

   付与を受け入れるには、EULA とサポート契約に同意する必要があります。拒否すると、付与を行った ELA 管理者に、付与が拒否されたことを通知するメールが送信されます。付与を受け入れたことを ELA 管理者が確認できるようにしてください。これ

©2023 Palo Alto Networks, Inc.

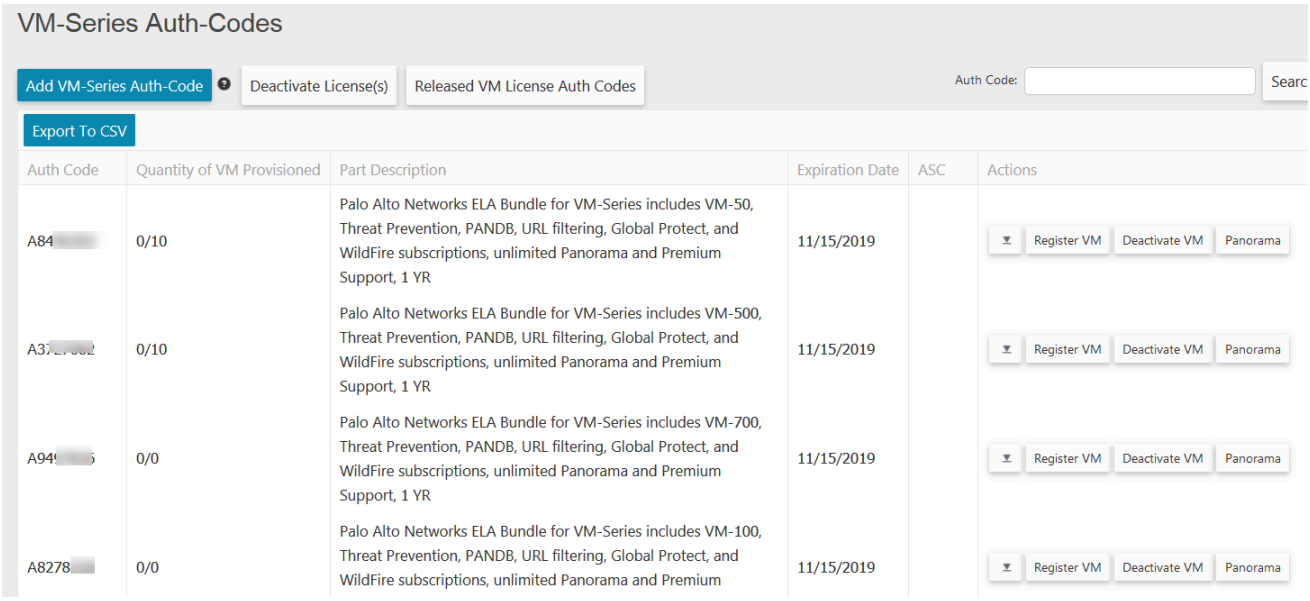
により、ELA 管理者はあなたがデプロイできる VM-Series ファイアウォール モデルとファイアウォールの数を割り当てることができます。



CSP で複数のアカウントに属しており、付与を誤ったアカウントで受け入れた場合は、*ELA* 管理者に対し付与を再送信するように依頼する必要があります。正しいアカウントで付与を受け入れるまでは、認証コードを使用してファイアウォールをプロビジョニングしないでください。

STEP 3 | 割り当てられている VM-Series モデルと数を確認します。

ELA 管理者から、プロビジョニングできる VM-Series ファイアウォール モデルとインスタンス数が割り当てられたら、**Assets**（資産） > **VM-Series Auth Codes**（**VM-Series** 認証コード）を選択して、割り当てられているモデルと各モデルのインスタンス数を確認できます。たとえば、以下のスクリーンショットに示されている付与では、VM-50 と VM-500 それぞれを 10 インスタンスずつデプロイできる認証コードが示されています。



ファイアウォールをデプロイして CSP に登録すると、プロビジョニングされたファイアウォールの数が増加します。**Quantity of VM Provisioned**（プロビジョニングされた **VM** の

©2023 Palo Alto Networks, Inc.

数）には、モデル別にプロビジョニングされた VM の数と使用可能な VM の合計数の比率が表示されます。

VM-Series モデルライセンスのアクティベート

VM-Series ファイアウォールのライセンスをアクティベーションするには、VM-Series ファイアウォールをデプロイして初期設定を完了している必要があります。ファイアウォールをデプロイするには、「VM-Series のデプロイ」を参照してください。

このセクションの手順を、AWS、Azure、Google Public Cloud などのすべての BYOL モデルで使用してください。パブリック クラウドでの従量制のライセンスについては、ライセンスをアクティブ化する必要はありません。「パブリック クラウド用 VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）」の説明に従ってプレミアム サポートをアクティベートしてください。

AWS Marketplace での *VM-Series* ファイアウォールの従量制モデルについては、長短両方の *AWS* インスタンス *ID* のインスタンスがサポートされます。

VM-Series ファイアウォールのライセンスをアクティベーションするまで、ファイアウォールにシリアル番号はなく、データプレーン インターフェイスの MAC アドレスは一意ではありません。また、最小数のセッションのみがサポートされます。ファイアウォールにライセンスが付与されるまで MAC アドレスはユニークではないため、MAC アドレスの重複による問題を避けるためには、複数のライセンス認証されていない VM-Series ファイアウォールを同時に使用しないようにしてください。

ライセンスをアクティベーションしたら、ライセンス サーバーが仮想マシンの UUID と CPU ID を使用して VM-Series ファイアウォールの一意のシリアル番号を生成します。キャパシティ認証コードがシリアル番号とともにライセンスの検証に使用されます。

VM-Series ファイアウォールの ***License***（ライセンス）タブには、すべてのライセンス モデルに対する標準の *VM-300* ライセンス ファイルが表示されます。特定のライセンス モデルに関する情報を探すには、*UI* のシステム情報を参照するか、または *CLI* を使って ***system info*** を表示します。

VM-Series ファイアウォールへのライセンス付与後に *VM-Series* ファイアウォールの削除と再デプロイが必要になった場合は、「ライセンスの無効化」に従ってファイアウォールで必ずライセンスを無効化してください。ライセンスを無効化することにより、テクニカルサポートの力を借りることなく、アクティブなライセンスを*VM-Series*ファイアウォールの新しいインスタンスに移転することが可能です。

- VM-Series ファイアウォール（スタンドアロン版）でのライセンスのアクティベーション
- VMware NSX 用 VM-Series ファイアウォールのライセンスのアクティベーション
- ライセンスのアクティベーションのトラブルシューティング

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォール（スタンドアロン版）でのライセンスのアクティベーション

サブスリプション バンドルによるブートストラップ ワークフローの使用を選択していない場合は、VM-Series ファイアウォールをデプロイして初期設定を行わなければ、VM-Series ファイアウォールでライセンスをアクティベートすることはできません。

- インターネットへの直接アクセス
- インターネット アクセスなし

インターネットへの直接アクセス

ライセンスをアクティベートするには、IPアドレス、ネットマスク、デフォルトゲートウェイ、DNSサーバー、IPアドレスを使用して、ファイアウォールを設定する必要があります。

ファイアウォールで有効な DNS が設定されていて、Palo Alto Networks のライセンス サーバーにアクセスするためのネットワーク接続が確立されていなければなりません。

1. デバイス > ライセンス を選択し、[ライセンスサーバーからライセンスキーを取得する] リンクを選択します。
2. ファイアウォールが更新サーバー（updates.paloaltonetworks.com）に接続され、ライセンスがダウンロードされてから自動的に再起動します。
3. Web インターフェイスにログインし直し、**Dashboard**（ダッシュボード）に有効なシリアル番号が表示されていることを確認します。「**unknown**」と表示されている場合、デバイスはライセンスされていません。
4. **Device**（デバイス） > **Licenses**（ライセンス）で、**PA-VM** ライセンスがデバイスに追加されていることを確認します。

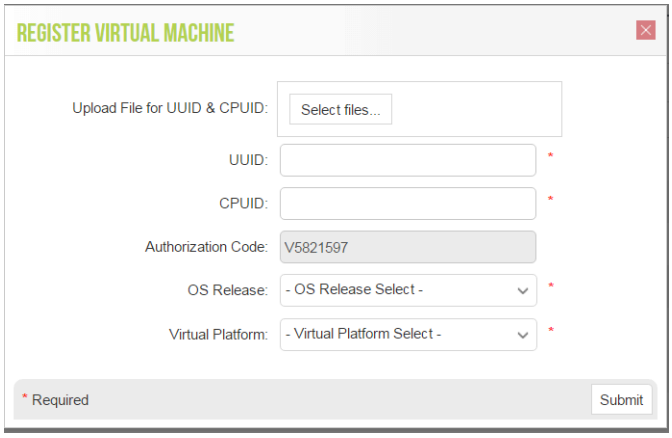
   エラー メッセージが表示された場合は、「ライセンスの有効化に関する問題のトラブルシューティング」に従って問題を解決してください。

インターネット アクセスなし

1. **Device**（デバイス） > **Licenses**（ライセンス）を選択し、**Activate Feature using Auth Code**（認証コードを使用して機能をアクティベート）リンクをクリックします。
2. **Download Authorization File**（認証ファイルのダウンロード）をクリックし、クライアント マシンに **authorizationfile.txt** をダウンロードします。
3. インターネットにアクセスできるコンピュータに **authorizationfile.txt** をコピーし、サポート ポータルにログインします。**My VM-Series Auth-Codes**（自分のVM-Series認証コード）リンクをクリックし、リストから該当する認証コードを選択して **Register VM**（VM登録）リンクをクリックします。
4. **Register Virtual Machine**（仮想マシンの登録）タブで、認証ファイルをアップロードします。ファイアウォールをデプロイした PAN-OS バージョンとハイパーバイザーを選

©2023 Palo Alto Networks, Inc.

択して、登録プロセスを完了します。VM-Series ファイアウォールのシリアル番号がアカウント レコードに関連付けられます。



5. **Assets**（アセット） > **My Devices**（マイデバイス）の順に移動し、登録した VM-Series デバイスを探して **PA-VM** リンクをクリックします。VM-Series ライセンス キーがクライアント マシンにダウンロードされます。
6. VM-Series ファイアウォールの Web インターフェイスにアクセス可能なマシンにライセンス キーをコピーし、**Device**（デバイス） > **Licenses**（ライセンス）の順に移動します。

   ウェブ インターフェイス経由でライセンス キーをインストールしなければなりません。ファイアウォールは、*SCP* または *FTP* 経由でのライセンス キーのインストールはサポートしていません。
7. **Manually Upload License**（ライセンス キーの手動アップロード）リンクをクリックしてライセンス キーを入力します。ファイアウォールでキャパシティ ライセンスがアクティベーションされるときに、自動的に再起動します。
8. デバイスにログインし、**Dashboard**（ダッシュボード）に有効なシリアル番号が表示され、**PA-VM** ライセンスが **Device**（デバイス） > **Licenses**（ライセンス）タブに表示されていることを確認します。

VMware NSX 用 VM-Series ファイアウォールのライセンスのアクティベーション

Panorama では、VMware NSX 用 VM-Series ファイアウォールを一元的に管理することができ、Panorama がインターネットに直接アクセスできる場合はライセンスの有効化プロセスが自動で行われます。Panorama は Palo Alto Networks の更新サーバーに接続してライセンスを取得します。新しい NSX 用 VM-Series ファイアウォールがデプロイされると、Panorama と通信を行ってライセンスを取得します。Panorama がインターネットに接続されていない場合、VM-Series ファイアウォールの各インスタンスを手動でライセンス登録し、ファイアウォールが Panorama に接続できるようにする必要があります。コンポーネントの概要と NSX 用 VM-Series ファイアウォールのデプロイ要件の概要については、「NSX 用 VM-Series ファイアウォールの概要」を参照してください。

この統合ソリューションでは、認証コード（PAN-VM-1000-HV-SUB-BND-NSX2 など）に、脅威防御、URL フィルタリングと WildFire のサブスクリプション、および要求期間のプレミアム サポートが含まれています。

©2023 Palo Alto Networks, Inc.

ライセンスをアクティベーションするには、以下のタスクを完了しておく必要があります。

- 認証コードをサポート アカウントに登録。認証コードを登録しないと、ライセンス サーバーでライセンスの作成に失敗します。
- Panoramaでサービス定義に認証コードを入力。Panorama で**VMWare Service Manager** を選択して **Authorization Code**（認証）を**VMware Service Definition**（**VMware** サービス定義）に追加します。

> 評価版認証コードを購入している場合は、*30* 日か *60* 日の間、*VM-1000-HV* キャパシティ ライセンスで最大 *5* つの *VM-Series* ファイアウォールにライセンスを適用することができます。このソリューションでは、*ESXi* ホストあたり *1* つの *VM-Series* ファイアウォールをデプロイできるため、評価版ライセンスを使用する場合は、*ESXi* クラスタに最大 *5* 台の *ESXi* ホストを含めることができます。

ライセンスを有効化する以下の作業は手動で行います。カスタムスクリプトあるいはオーケストレーション サービスを持っている場合、ライセンス API を使用して VM-Series ファイアウォールのライセンスを取得するプロセスを自動化することができます。

- Panorama からインターネットにアクセスできる場合の NSX 上の VM-Series ファイアウォールでのライセンスのアクティベート
- Panorama からインターネットにアクセスできない場合の NSX 上の VM-Series ファイアウォールでのライセンスのアクティベート
- ライセンスのアクティベーションのトラブルシューティング

Panorama からインターネットにアクセスできる場合の **NSX** 上の **VM-Series** ファイアウォールでのライセンスのアクティベート

Panorama がインターネットにアクセスできる場合は、以下の手順を実行して、NSX 用 VM-Series ファイアウォールを有効化します。

STEP 1 | VM-Seriesファイアウォールが Panorama に接続されていることを確認します。

1. Panorama にログインします。
2. **Panorama** > **Managed Devices**（管理対象のデバイス）を選択し、ファイアウォールが Connected（接続済み）として表示されることを確認します。

STEP 2 | 各ファイアウォールがライセンス登録されていることを確認します。

Panorama > **Device Deployment**（管理対象のデバイス） > **Licenses**（ライセンス）を選択し、Panorama が認証コードを正しく照合し、ライセンスを各ファイアウォールに適用したことを確認します。

ライセンスが表示されない場合は**Refresh**（更新）をクリックします。サブスクリプション ライセンスを取得する VM-Series ファイアウォールを選択し、**OK** をクリックします。

Panorama からインターネットにアクセスできない場合の **NSX** 上の **VM-Series** ファイアウォールでのライセンスのアクティベート

Panorama がインターネットにアクセスできない場合は、以下の手順を実行して、NSX 用 VM-Series ファイアウォールを有効化します。

©2023 Palo Alto Networks, Inc.

STEP 1 | VM-SeriesファイアウォールのCPU IDおよびUUIDを探します。

1. vCenterサーバーからファイアウォールのIPアドレスを取得します。
2. Webインターフェイスにログインして、**Dashboard**（ダッシュボード）を選択します。
3. General Information（一般情報）ウィジェットでファイアウォールの **CPU ID** および **UUID** を取得します。

STEP 2 | 認証コードをアクティベートし、ライセンス キーを生成します。

1. ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。新しいアカウントが必要な場合は「サポート アカウントの作成」を参照してください。
2. **Assets**（アセット） > **VM-Series Auth Codes**（**VM-Series** 認証コード）を選択し、**Add VM-Series Auth Codes**（**VM-Series** 認証コードを追加）をクリックして認証コードを入力します。
3. 先ほど登録した認証コードに対応する行の**Register VM**（**VM** を登録）を選択し、ファイアウォールの CPU ID および UUID を入力して**Submit**（送信）をクリックします。ポータルによってファイアウォールのシリアル番号が生成されます。
4. **Assets**（アセット） > **Devices**（デバイス）を選択し、シリアル番号を探します。
5. Actions（アクション）列のリンクをクリックし、各キーをノートパソコンのローカルにダウンロードします。サブスクリプションのライセンス キーに加え、キャパシティ ライセンスおよびサポート ライセンスキーを取得する必要があります。

STEP 3 | キーをファイアウォールにアップロードします。

1. ファイアウォール インターフェイスにログインします。
2. **Device**（デバイス） > **Licenses**（ライセンス）を選択し、**Manually upload license key**（ライセンス キーを手動でアップロード）を選択します。
3. キーを**Browse**（参照）して選択し、**OK**をクリックしてライセンスをファイアウォールにインストールします。

   キャパシティ ライセンスのキーファイル（*pa-vm.key*）を最初にインストールしてください。キャパシティ ライセンスキーを適用する際、*VM-Series*ファイアウォールが再起動します。再起動にあたり、*Panorama*の管理対象デバイスにファイアウォールを登録するために使用できるシリアル番号がファイアウォールに付与されます。
4. 作業を繰り返して各キーをファイアウォールにインストールします。
5. **Dashboard**（ダッシュボード）を選択し、General Information（一般情報）ウィジェットに**Serial #**（シリアル番号）が表示されることを確認します。

STEP 4 | Panoramaでファイアウォールのシリアル番号を追加します。

Panorama > **Managed Devices**（管理対象のデバイス）を選択し、**Add**（追加）をクリックして、NSX 用 VM-Series ファイアウォールのシリアル番号を入力します。これでファイアウォールがPanoramaに接続して構成およびポリシールールを取得できるようになっているはずです。

©2023 Palo Alto Networks, Inc.

ライセンスのアクティベーションのトラブルシューティング

ライセンスをアクティベートするときによくある問題の一部をこのセクションで紹介します。

十分なメモリがない PA-VM のライセンスを取得すると、次のようなエラーが発生します。

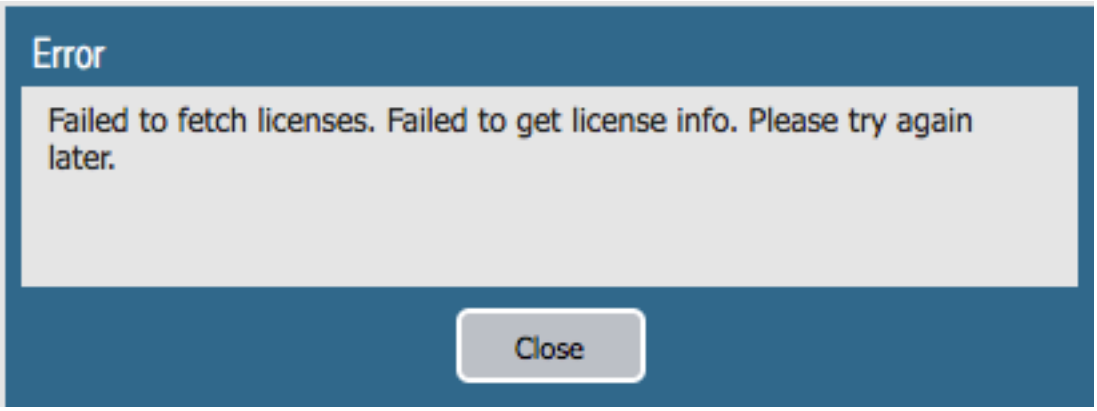
```
Server error : failed key check : Resource check failed.
Memory needed: 6.5GB, allocated memory: 4.8GB
```

この問題を解決するには、ライセンスが必要とする追加のメモリをプロビジョニングし、コマンド**request license fetch** を使用してライセンスを取得します。

他のコマンドを使用すると、次のエラーで失敗します。

```
Server error : failed to fetch license: Cannot apply a provisioning
 license feature to an already provisioned device.
```

次のエラーが表示された場合：「**Failed to fetch licenses**（ライセンスを取得できませんでした）。**Failed to get license info**（ライセンス情報を取得できませんでした）。**Please try again later**（後で再試行してください）」あるいは、一般的な通信エラー メッセージが表示されます。

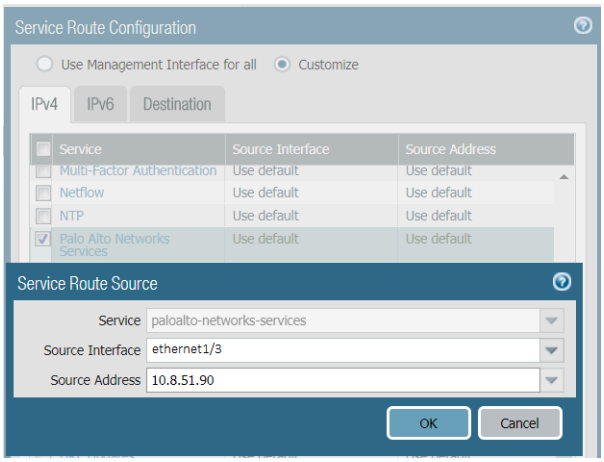


以下を確認してください。

- ファイアウォールがサービス ルートを使用してトラフィックを Palo Alto Networks サーバーにルーティングできるかどうか。デフォルトでは、ファイアウォールは管理インター

©2023 Palo Alto Networks, Inc.

フェイスを使用してサーバーにアクセスします。データプレーン インターフェイスを使用する予定の場合、サービス ルートをセットアップしていることを確認してください。

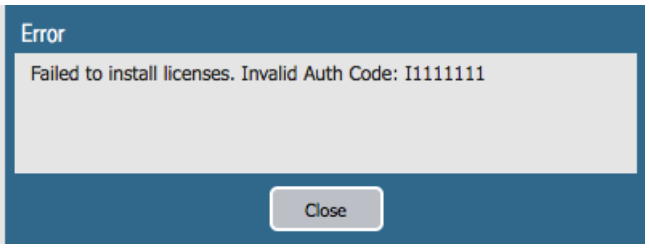


- インターネット経由のルーティングが機能するかどうか。ファイアウォールに SSH で接続し、4.2.2.2 などの公開された IP アドレスに ping します。データプレーン インターフェイスを使用している場合、必ず source オプションを使用してください。例：ping count 3 source 10.0.1.1 host 4.2.2.2。
- DNS が正しくセットアップされているかどうか。ファイアウォールに SSH で接続し、google.com などの DNS 名に ping します。例:

```
warby@warbylan> ping count 3 source 10.0.1.1 host google.com
PING google.com (216.58.195.78) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=1 ttl=55 time=11.6 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=3 ttl=55 time=11.5 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```


©2023 Palo Alto Networks, Inc.

「Invalid Auth Code（認証コードが無効です）」というエラーが表示された場合：



以下を確認してください。

- 認証コードを正しく入力しているかどうか。
- 認証コードをサポート ポータルのアカウントに登録しているかどうか。
- 認証コードが VM-Series ファイアウォールの最大プロビジョニング キャパシティに達していないかどうか。
  - レガシーライセンスの場合は、CSP にログインし、アセット > **VM-Series** 認証コードを選択します。
  - Software NGFW Credit の場合に、デプロイメントプロファイルがわかっているときは、CSP にログインし、アセット > **Software NGFW Credit** を選択し、プロファイルを見つけ、[詳細] をクリックします。

    また、アセット > ソフトウェア **NGFW** デバイス を選択して認証コードで検索することもできます。

VM-Series ファイアウォールの登録

VM-Series ファイアウォールの購入後、VM-Series モデルのキャパシティライセンス認証コード、サポート資格認証コード、および 1 つ以上のサブスクリプションライセンス用認証コードが記載された電子メールが届きます。認証コードを使用するには、Palo Alto Networks カスタマー サポート Web サイトで、そのコードをサポート アカウントに登録する必要があります。VMware が統合された NSX ソリューションの場合、電子メールには、VM-Series モデルの 1 つ以上のインスタンスのキャパシティ ライセンスをバンドルした単一の認証コード、サポート資格、および 1 つ以上のサブスクリプション ライセンスが含まれています。

パブリッククラウド（AWS、Azure、または Google Cloud Platform）の従量制ライセンスには、認証コードがありません。ただし、Palo Alto Networks のプレミアム サポートをアクティベートする際は、サポート アカウントを作成し、Palo Alto Networks カスタマー サポート Web サイトで VM-Series ファイアウォールを登録する必要があります。

サポート アカウントを使用してキャパシティ認証コードあるいはファイアウォールを登録する場合は、このセクションの手順に従ってください。

- VM-Series ファイアウォールの登録 (Software NGFW Credit)
- VM-Series ファイアウォールを登録する（認証コードを使用）
- パブリック クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールを登録する（認証コードを使用）

認証コードを使用して VM-Series ファイアウォールを登録するには、以下の手順を実行します。

STEP 1 | ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。新しいアカウントが必要な場合は「サポート アカウントの作成」を参照してください。

STEP 2 | アセット > **VM-Series** 認証コード > **VM-Series** 認証コードの追加を選択します。

STEP 3 | **Add VM-Series Auth-Codes**（**VM-Series** 認証コードを追加）フィールドに、電子メールで送られてきたキャパシティ認証コードを入力し、一番右のチェックマークをクリックして入力内容を保存します。ページに、サポート アカウントに登録された認証コードのリストが表示されます。

デプロイ済みの VM-Series ファイアウォール数と、各認証コードで現在使用可能なライセンス数を確認できます。すべてのライセンスが使用済みの場合、VM-Series Auth-Codes ページに認証コードは表示されません。デプロイされたすべてのアセットを表示するには、**Assets**（アセット） > **Devices**（デバイス）の順に選択します。

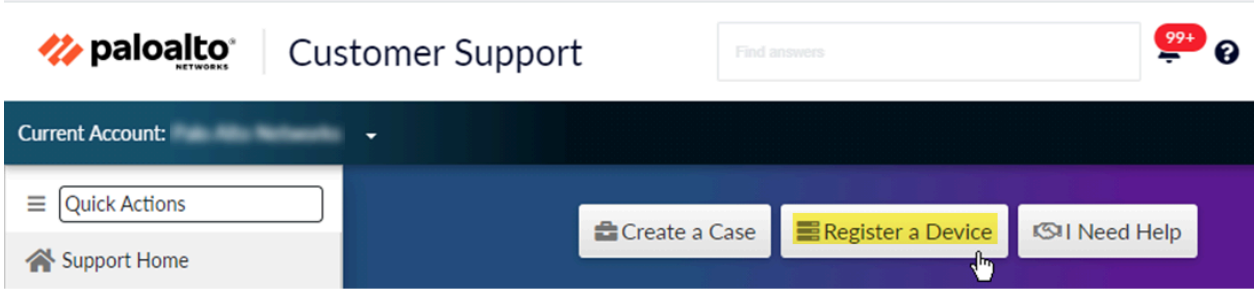
パブリック クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）

Palo Alto Networks カスタマサポートポータル (CSP) で使用量ベースのファイアウォールを登録するには、自動登録または手動登録を使用できます。従量制ベースのファイアウォールの自動登録では、ファイアウォールを起動し、CSP アカウントに関連するサイトライセンス資格にアクセスするとすぐに、シームレスにファイアウォールを登録することができます。詳細はCSPドキュメントを参照してください。

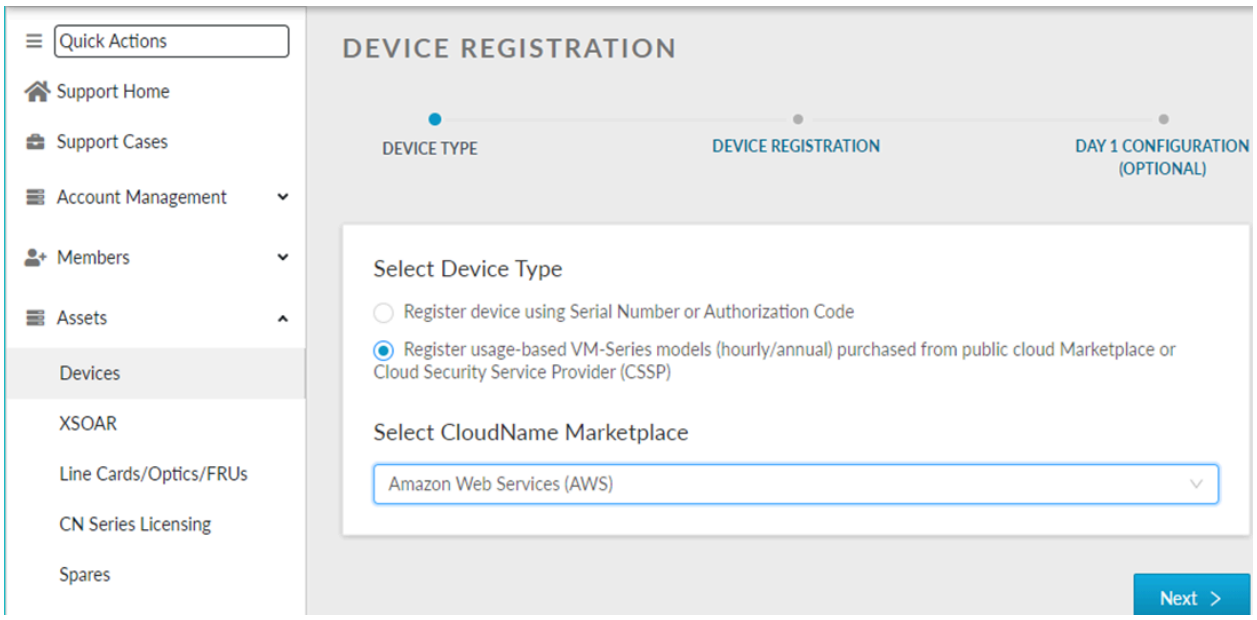
VM-Seriesファイアウォールを手動で登録するには、次の作業を行ってください。手動登録プロセスを開始する前に、VM-Series ファイアウォールにログインし、ダッシュボードに表示されたシリアル番号と CPU ID （UUID はオプション）を書き留めます。

©2023 Palo Alto Networks, Inc.

STEP 1 | Palo Alto Networks カスタマーサポート Web サイトにログインし、[アセット > デバイス > 新しいデバイスの登録] をクリックします。



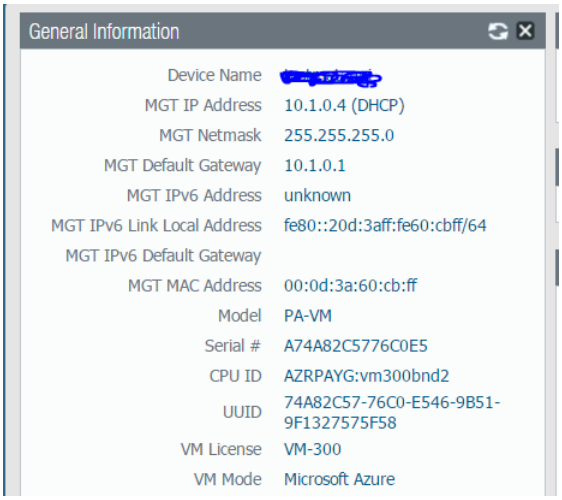
1. パブリッククラウドマーケットプレイスまたはクラウドセキュリティサービスプロバイダー **(CSSP)** から購入した、従量制ベースの **VM-Series** モデル **(**時間単位/年単位**)** を登録するを選択します。
2. クラウドマーケットプレイスのベンダーを選択し、[次へ] をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series ファイアウォールの **Serial #**（シリアル番号）、**CPU ID**、および **UUID** を入力します。

たとえば、VM 上の VM-Series ファイアウォールのダッシュボードには、以下の情報が表示されます。



ファイアウォールをオフラインで使用する場合は、***Offline***（オフライン）チェックボックスを選択し、使用する *PAN-OS* のバージョンを入力します。

STEP 3 | EULA に同意したら、**Agree and Submit**（同意して送信）をクリックし、ファイアウォールを登録します。

STEP 4 | 購入したライセンスの詳細が、CSP のアセットページに表示されていることを確認してください。

VM-Seriesファイアウォールへのデバイス証明書のインストール

ファイアウォールがサイトライセンスの権利を取得して、WildFire、AutoFocus、およびCortex Data Lakeなどのクラウドサービスに安全にアクセスするためには、デバイス証明書が必要になります。VM-Seriesファイアウォールにサイトライセンスを適用するには、ワンタイムパスワードと自動登録PINの2種類の方法があります。各パスワードまたはPINは、カスタマーサポートポータル（CSP）上で生成され、ご自分のPalo Alto Networksサポートアカウント固有のものになります。使用する方法は、ファイアウォールのデプロイに使用するライセンスタイプ、およびPanoramaでファイアウォールを管理するのかどうかによって異なります。

- ワンタイムパスワード—Palo Alto Networksライセンスサーバーにすでに登録しているVM-Seriesファイアウォールの場合、カスタマーサポートポータルでワンタイムパスワードを生成して、それをVM-Seriesファイアウォールに適用する必要があります。この方法は、BYOLまたはELAライセンスを利用する、小規模な管理対象外デプロイ環境内のVM-Seriesファイアウォール、およびPanoramaが管理する手動でデプロイしたVM-Seriesファイアウォールに対して使用します。
- 登録PIN—この方法では、初期スタートアップ時に、VM-Seriesファイアウォールにサイトライセンスを適用することができます。この方法は、ライセンスタイプに関係なく、使用量ベースのライセンス（PAYG）を持つ、起動時のブートストラップ、または任意の種類の自動

©2023 Palo Alto Networks, Inc.

化デプロイを使ってデプロイされたVM-Seriesファイアウォールに対して使用します。自動登録PINにより、CSPを使って使用量ベースのファイアウォールを起動時に自動登録し、サイトライセンスを取得することができます。

NSX-T 上の VM-Series ファイアウォールの場合、サービス定義設定に自動登録 PIN を追加して、初期ブートアップ時にファイアウォールがデバイス証明書を取得するようにすることができます。詳細は、NSX-T（North-South）、および NSX-T（East-West） のサービス定義設定を参照してください。以前にデプロイしたファイアウォールを、デバイス証明書をサポートしているバージョンのPAN-OSにアップグレードする場合、ワンタイムパスワードを使ってそれらのファイアウォールに、個別にデバイス証明書を適用することができます。

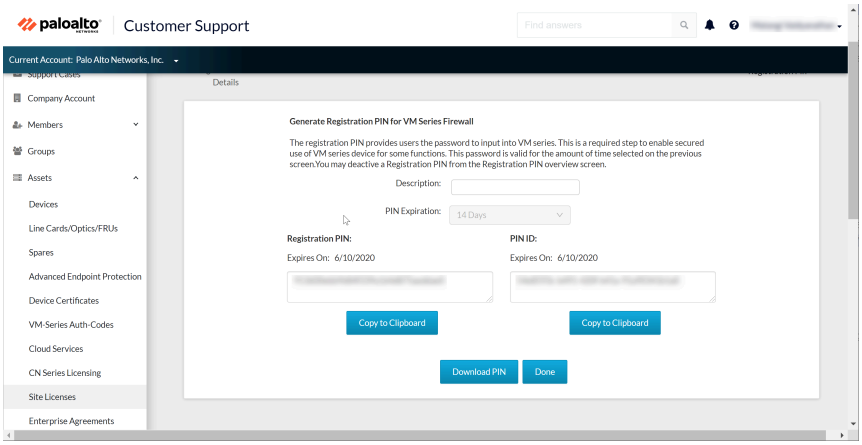
ワンタイムパスワードと自動登録PINは、失効前に使用する必要があります。そうしなかった場合は、CSPに戻って新しいパスワード/PINを生成する必要があります。

起動時に、サイトライセンスを自動的に取得するようにファイアウォールを設定します。

サイトライセンスの権利を取得して、クラウドサービスに安全にアクセスするために、ファイアウォールにはデバイス証明書が必要になります。ファイアウォールの起動時にサイトライセンスを取得するには、ブートストラップパッケージの/licenseフォルダに認証コードを含め、init-cfg.txtファイルに自動登録PIN IDを追加して、それを/configフォルダに配置する必要があります。自動登録PIN IDと値を追加することで、VM-SeriesファイアウォールのPAYGまたは使用量ベースのインスタンスの自動登録も有効になります。

1. カスタマーサポート ポータル（CSP）にログインします。
2. VM-Series登録PINを生成します。

   Assets（アセット） > **Device Certificates**（デバイス証明書） > **Generate Registration PIN**（登録**PIN**の生成）を選択します。PIN IDと値を保存します。PINが失効する前に、忘れずにファイアウォールを起動してください。



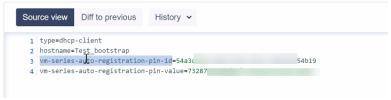
 ©2023 Palo Alto Networks, Inc.

3. 登録PIN IDと値をinit-cfg.txtファイルに追加します。

   必要なパラメータの他に、次のステートメントを含める必要があります:

   ```
   vm-series-auto-registration-pin-id=
   ```

   ```
   vm-series-auto-registration-pin-value=
   ```



4. ファイアウォールにログインして、ファイアウォール上でサイトライセンスを参照できることを確認します。

©2023 Palo Alto Networks, Inc.

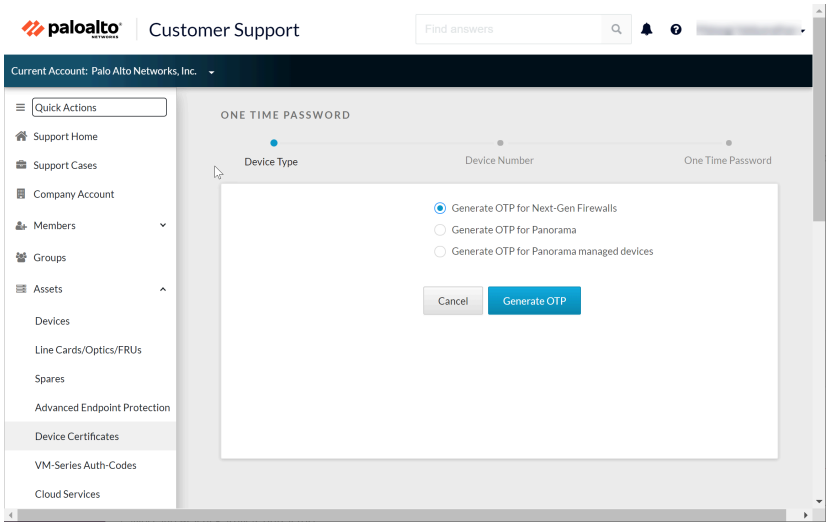
ワンタイムパスワード（OTP）を生成し、ファイアウォールでデバイス証明書を手動で取得します。

サイトライセンスの権利を取得して、クラウドサービスに安全にアクセスするために、ファイアウォールにはこのデバイス証明書が必要になります。

1. カスタマー サポート ポータルにログインします。

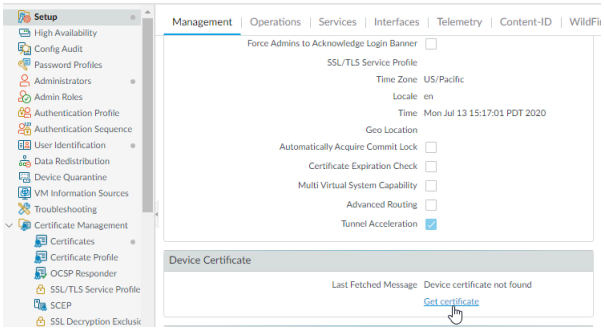
   まだそうしていない場合は、VM-Seriesファイアウォールを登録します。

2. **Assets** > **Device Certificates**（デバイス証明書） > **Generate OTP**（**OTP**の生成）を選択します。



3. リストからファイアウォールを選択して、**Generate OTP**（**OTP**を生成）します。
4. ファイアウォールにログインして、デバイス証明書を取得します。

   Setup（設定） > **Management**（管理） > **Device Certificate**（デバイス証明書）を選択して、**Get Certificate**（証明書の取得）を選択します。



5. デバイス証明書が取得され、ファイアウォール上でサイトライセンスを参照できることを確認します。

VM-Seriesファイアウォールの管理にPanoramaを使用する場合は、「管理対象ファイアウォールへのデバイス証明書のインストール」を参照してください。

©2023 Palo Alto Networks, Inc.

BYOL ライセンスと PAYG ライセンスの切り替え

VM-Series ファイアウォールは、BYOL と PAYG のライセンス オプション間で変換できません。AWS、Azure または Google Cloud Platform で PAYG または BYOL オプションを使用してすでに VM-Series ファイアウォールをデプロイし設定している場合、他方のオプションに切り替えるには、以下の手順に従って設定を保存して既存のファイアウォールにエクスポートし、新しいファイアウォールをデプロイしてから、新しいファイアウォールで設定を復元します。

STEP 1 | 現在の設定ファイルのバックアップを保存し、外部サーバーに保存します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Export named configuration snapshot**（名前付き設定スナップショットのエクスポート）を選択します。
2. 実行中の設定を含む XML ファイル（running-config.xml など）を選択し、**OK** をクリックして設定ファイルをエクスポートします。
3. エクスポート ファイルをファイアウォールの外部に保存します。

STEP 2 | 新しいファイアウォールをデプロイし、必要に応じてライセンスを登録またはアクティベートします。

新しい PAYG インスタンスの場合：

1. AWS、Azure、または Google Cloud Platform マーケットプレイスで、デプロイする PAYG ライセンス バンドルのソフトウェア イメージを選択します。
2. AWS、Azure、または Google パブリック クラウドで新しい VM-Series ファイアウォールをデプロイします。「AWS での VM-Series ファイアウォールのセットアップ」、「Azure での VM-Series ファイアウォールのセットアップ」、または「Google Cloud Platform 上の VM-Series ファイアウォールのセットアップ」を参照してください。
3. パブリック クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）。

新しい BYOL インスタンスの場合：

1. 販売代理店に連絡して BYOL ライセンスを購入し、ファイアウォールをライセンスするために使用できる BYOL 認証コードを入手してください。
2. VM-Series ファイアウォールを登録（認証コードを使用）します。
3. AWS または Azure パブリック クラウドで新しい VM-Series ファイアウォールをデプロイします。「AWS での VM-Series ファイアウォールのセットアップ」、「Azure での VM-Series ファイアウォールのセットアップ」、または「Google Cloud Platform 上の VM-Series ファイアウォールのセットアップ」を参照してください。
4. VM-Series ファイアウォール（スタンドアロン版）でのライセンスのアクティベーションを行います。

STEP 3 | 新しくデプロイしたファイアウォールで、エクスポートした設定を復元します。

1. 新しくデプロイしたファイアウォールの Web インターフェイスにアクセスします。
2. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Import named configuration snapshot**（名前を付けて保存した設定スナップショットをイン

©2023 Palo Alto Networks, Inc.

ポート）をクリックし、外部ホストにある設定ファイルを Browse（参照）して、**OK** をクリックします。

3. **Load named configuration snapshot**（名前を付けて保存した設定スナップショットを読み込む）をクリックし、先ほどインポートした設定ファイルの **Name**（名前）を選択して **OK** をクリックします。
4. **Commit**（コミット）をクリックし、現在アクティブな設定を先ほどインポートしたスナップショットで上書きします。
5. ファイアウォールを削除するか、リプレイスしたファイアウォールでライセンスを無効化する前に、新しいファイアウォールの設定がリプレイスしたファイアウォールに一致することを確認します。

固定モデル ライセンス間の切り替え

BYOL オプションを使用して、現在デプロイされている VM-Series ファイアウォールのライセンスを切り替えることができます。たとえば、ファイアウォールを通過するトラフィックを中断することなく、サブスクリプションバンドルからエンタープライズライセンス契約 (ELA) への移行や、その逆の移行を行うことができます。また、Panorama から個別のファイアウォールまたは複数のファイアウォールのライセンスを同時に切り替えることもできます。

PAYG と *BYOL* の間で *ELA* または永久ライセンスを切り替える場合は、この手順を使用しないでください。詳細は、「BYOL ライセンスと PAYG ライセンスの切り替え」を参照してください。

次のいずれかのライセンス変更のための手順を以下に説明します。

- サブスクリプション バンドル 1 からサブスクリプション バンドル 2
- サブスクリプション バンドル 1 または 2 から ELA
- キャパシティ ライセンスからサブスクリプション バンドルまたは ELA

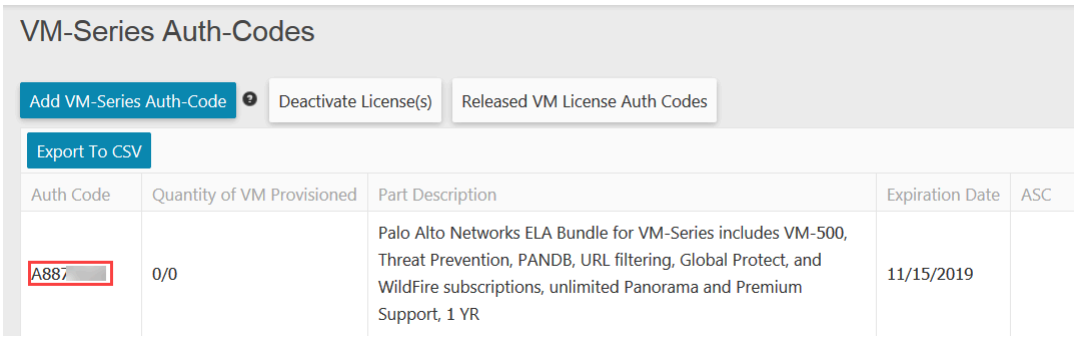
ELA ライセンスに切り替える前に、現在デプロイされている VM-Series ファイアウォールの数をサポートするのに十分な数のトークンを割り当てる必要があります。各 VM-Series モデルに必要なトークンの詳細については、「VM-Series エンタープライズ ライセンス契約（マルチモデル ELA）」を参照してください。

©2023 Palo Alto Networks, Inc.

スタンドアロン ファイアウォールでライセンスを切り替えます。

1. 認証コードを登録します。
   - サブスクリプション バンドルの場合は新しい認証コードを登録します。
   - ELA の場合は ELA 認証コードをアクティベートします。

   > 個々の *VM-Series* ファイアウォールをアクティベートするときには *ELA* 認証コードを使用しないでください。*ELA* の登録後に、*VM-Series* モデル認証コードを使用して個々のファイアウォールをアクティベートします。これらの認証コードは、カスタマー サポート ポータルの ***Assets***（アセット）> ***VM-Series Auth-Codes***（***VM-Series*** 認証コード）で確認できます。
2. VM-Series ファイアウォール Web インターフェイスにログインします。
3. Palo Alto Networks 更新サーバーの設定を確認します。
   1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
   2. **Update Server**（更新サーバー）が updates.paloaltonetworks.com に設定されていることを確認します。
   3. **Update Server Identity**（更新サーバー **ID**）が選択されていることを確認します。
4. VM-Series 認証コードを適用します。ELA のファイアウォール認証コードは、次に示すように文字 A で始まります。



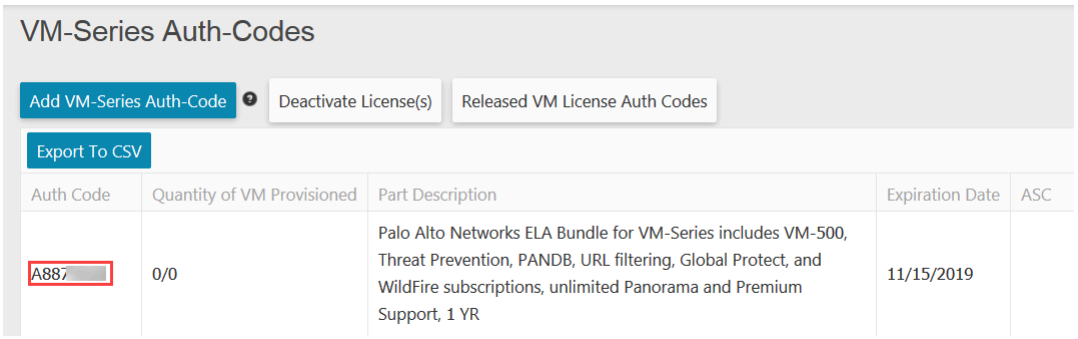
   1. **Device**（デバイス） > **Licenses**（ライセンス）の順に選択し、**Activate feature using authorization code**（認証コードを使用して機能をアクティベート）リンクを選択します。
   2. VM-Series 認証コードを入力します。
   3. **OK** をクリックしてライセンス アップグレードを確認します。ファイアウォールは Palo Alto Networks 更新サーバーと通信し、VM-Series モデルに基づいてファイアウォールに必要なトークンを消費します。
   4. ライセンス有効期限を調べ、ライセンスの更新が正常に完了したことを確認します。
5. デプロイメントの各 VM-Series ファイアウォールでこの作業を繰り返します。

©2023 Palo Alto Networks, Inc.

Panorama を使用して管理対象ファイアウォールのライセンスを切り替えます。

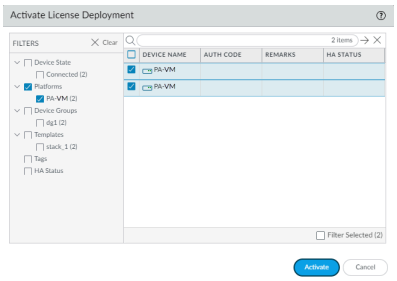
1. 認証コードを登録します。
   - サブスクリプション バンドルの場合は新しい認証コードを登録します。
   - ELA の場合は ELA 認証コードをアクティベートします。

   > 個々の *VM-Series* ファイアウォールをアクティベートするときには *ELA* 認証コードを使用しないでください。*ELA* の登録後に、*VM-Series* モデル認証コードを使用して個々のファイアウォールをアクティベートします。これらの認証コードは、カスタマー サポート ポータルの ***Assets***（アセット）> ***VM-Series Auth-Codes***（***VM-Series*** 認証コード）で確認できます。
2. Panorama Web インターフェイスにログインします。
3. ファイアウォールの Palo Alto Networks 更新サーバー設定を確認します。
   1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
   2. **Update Server**（更新サーバー）が updates.paloaltonetworks.com に設定されていることを確認します。
   3. **Update Server Identity**（更新サーバー **ID**）が選択されていることを確認します。
4. VM-Series 認証コードを適用します。ELA のファイアウォール認証コードは、次に示すように文字 A で始まります。



   1. **Panorama** > **Device Deployment**（デバイスのデプロイ） > **Licenses**（ライセンス）を選択して、**Activate**（アクティベーション）をクリックします。
   2. VM-Series 認証コードを入力します。
   3. フィルターを使用してライセンスを付与する管理対象ファイアウォールを選択します。
   4. 各ファイアウォールの **Auth Code**（認証コード）列に認証コードを入力します。
   5. **Activate**（アクティベーション）をクリックしてライセンス アップグレードを確認します。Panorama は Palo Alto Networks 更新サーバーと通信し、VM-Series モデルに基づいてファイアウォールに必要なトークンを消費します。

©2023 Palo Alto Networks, Inc.



6. ライセンス有効期限を調べ、ライセンスの更新が正常に完了したことを確認します。

ライセンスの非アクティブ化

ライセンスの無効化により、ライセンスの自己管理が可能になります。ファイアウォール（ハードウェア ベースあるいは VM-Series ファイアウォール）に付与された 1 つ以上のライセンスやサブスクリプションを削除したい場合や、VM-Series ファイアウォールを無効化し、アクティブなライセンスやサブスクリプションをすべて解除したい場合、ファイアウォールあるいは Panorama から無効化を行ってください（Palo Alto Networks カスタマー サポート Web サイトでは行わないでください）。

ライセンスを正常に無効化するには、ライセンス無効化 API キーをインストールして、更新サーバーの ID の確認を有効にする必要があります（デフォルトでは有効）。PAN-OS はこの無効化 API キーを使用して、ライセンス サービスのすべての更新を認証します。無効化 API キーは、ファイアウォールとライセンス サーバーが接続されていない場合の手動のライセンス無効化には不要です。

ファイアウォール/Panorama からインターネット接続が可能で、Palo Alto Networks ライセンス サーバーとの通信が可能な場合、ライセンス解除はボタンをクリックするだけで自動的に完了します。ファイアウォール/Panorama にインターネットが接続されていない場合、手動で 2 段階の手順を踏む必要があります。1 段階目の手順では、無効化されたキーの情報を含むライセンス トークン ファイルをファイアウォールあるいは Panorama で生成し、エクスポートを行います。次の手順では、Palo Alto Networks カスタマー サポート Web サイトにログインした状態でトークン ファイルをアップロードし、ファイアウォールのライセンス キーを無効化します。

- CLI を使用して機能ライセンスまたはサブスクリプションを無効化する
- VM の無効化

CLI を使用して機能ライセンスまたはサブスクリプションを無効化する

ファイアウォールにライセンス/サブスクリプションをインストールしていて、ライセンスを別のファイアウォールに割り当て直す必要がある場合、テクニカルサポートの助けを借りなくても、個々のライセンスを非アクティブにして、同じ認証コードを他のファイアウォールで使用することが可能です。この機能は CLI でのみサポートされ、PAN-OS を実行している物理デバイスと仮想デバイスの両方でサポートされます。この手順は通常、固定モデルの永久ライセンスまたは ELA ライセンスで使用されます。

- インターネットアクセス (自動モード)
- インターネットアクセスなし (手動モード)

©2023 Palo Alto Networks, Inc.

インターネットアクセス (自動モード)

STEP 1 | ファイアウォールから CLI にログインします。

STEP 2 | 非アクティブ化する機能のライセンスキーの名前を表示します。

```
request license deactivate key features
```

STEP 3 | ライセンスまたはサブスクリプションを非アクティブ化します。

自動モードを使用して、ライセンスキーを削除します。

```
request license deactivate key features <name> mode auto
```

名前はライセンスキーファイルのフルネームです。以下に例を示します。

```
admin@vmPAN2> request license deactivate key features <name>
```

```
WildFire_License_2015_01_28_I5820573.key mode auto007200002599
WildFire License Success
Successfully removed license keys
```

インターネットアクセスなし (手動モード)

手動モードを使用して、ライセンスキーを削除し、モデルベースライセンスのライセンストークンを生成します。この手順は、ファイアウォールにライセンス API キーがインストールされていることを前提としています。

STEP 1 | ファイアウォールから CLI にログインします。

STEP 2 | 非アクティブ化する機能のライセンスキーの名前を表示します。

```
request license deactivate key features
```

STEP 3 | コマンドラインから手動でライセンスを非アクティブ化します。

```
request license deactivate key features <name> mode manual
```

以下に例を示します。

```
admin@PA-VM> request license deactivate key features
```

```
PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual
Successfully removed license keys
dact_lic.01282015.100502.tok
```

トークンファイルは`dact_lic.timestamp.tok`の形式で、タイムスタンプは`dmmyyyy.hrminsec`の形式で表示されます。

STEP 4 | トークンファイルが生成されたことを確認します。

```
show -token-files
```


©2023 Palo Alto Networks, Inc.

STEP 5 | トークンファイルをエクスポートします。

次のコマンドを 1 行で入力します。

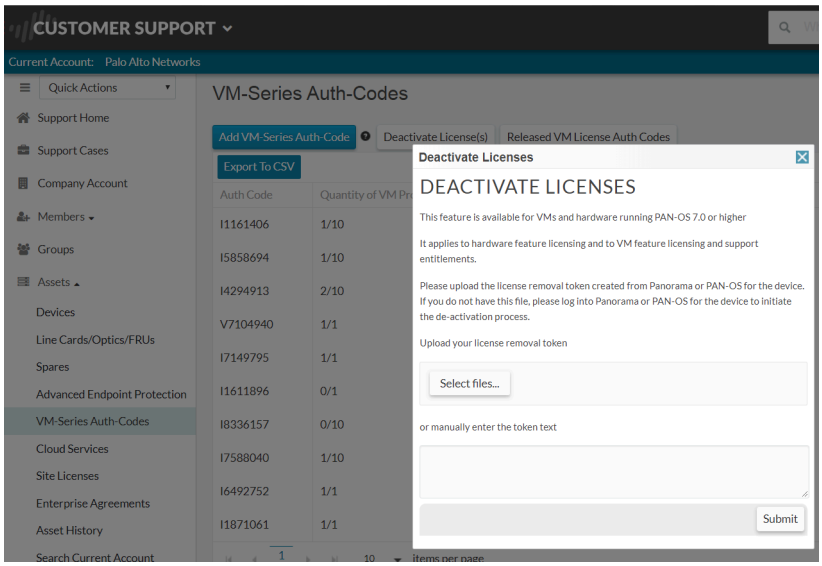
```
scp export license-token-file to <username@serverIP>
from <token_filename>
```

以下に例を示します。

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

STEP 6 | Palo Alto Networks カスタマーサポートポータルにログインします。

1. **Assets**（アセット）タブの **Deactivate License(s)**（ライセンスの無効化）のリンクをクリックします。
2. [アセット > **VM-Series** 認証コード] を選択し、[ライセンスの非アクティブ化] を選択します。
3. トークンファイルをアップロードして、非アクティブ化を完了します。



VM の無効化

VM-Series ファイアウォールの BYOL インスタンスが不要となった場合、Web インターフェース、CLI、または Panorama あるいはファイアウォール上の XML API を使用して、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-Capacity ライセンス、サポート資格）をすべて解放することができます。ライセンスのクレジットはアカウントに返還されるため、VM-Series ファイアウォールの別のインスタンスで同じ認証コードを使用できます。

VM を無効化すると、すべてのライセンス/資格が解除され、VM-Series ファイアウォールはライセンスのない状態になります（ファイアウォールはシリアル ナンバーを失い、最低数のセッションしかサポートできなくなります）。ファイアウォールの設定はそのままの状態で保存されているので、必要に応じてライセンスの再付与を行い、ファイアウォールの機能を完全に復元することも可能です。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールを削除する前に、ライセンスの非アクティブ化を必ず実行してください。ライセンスの非アクティブ化を行う前に *VM-Series* ファイアウォールを削除してしまった場合は、次の *2* つの方法があります。

Panorama で管理されている - *Panorama* からライセンスを非アクティブ化します。

Panorama で管理されていない - Palo Alto Networks カスタマーサポートに連絡してください。

- ファイアウォールから VM を非アクティブ化します。
- Panorama から VM を非アクティブ化します。

ファイアウォールから **VM** を非アクティブ化します。

ファイアウォールから VM ライセンスを非アクティブ化するには、以下の作業を行ってください。

STEP 1 | Web インターフェイスにログインして **Device**（デバイス） > **Licenses**（ライセンス）の順に選択します。

STEP 2 | ライセンス管理セクションで **VM** の非アクティブ化を選択します。

このオプションは VM でのみ表示されます。物理ファイアウォールにはありません。

STEP 3 | ファイアウォールで非アクティブ化されるライセンス/資格の一覧を確認してください。

STEP 4 | VM の無効化を行う場合は以下の方法があります。

- （Palo Alto Networks Licensing サーバーへのインターネットアクセス）[続行]を選択します。

  ファイアウォールを再起動するよう指示され、再起動と同時にライセンスが非アクティブ化されます。
- （インターネットなし）-[手動で完了する]を選択します。

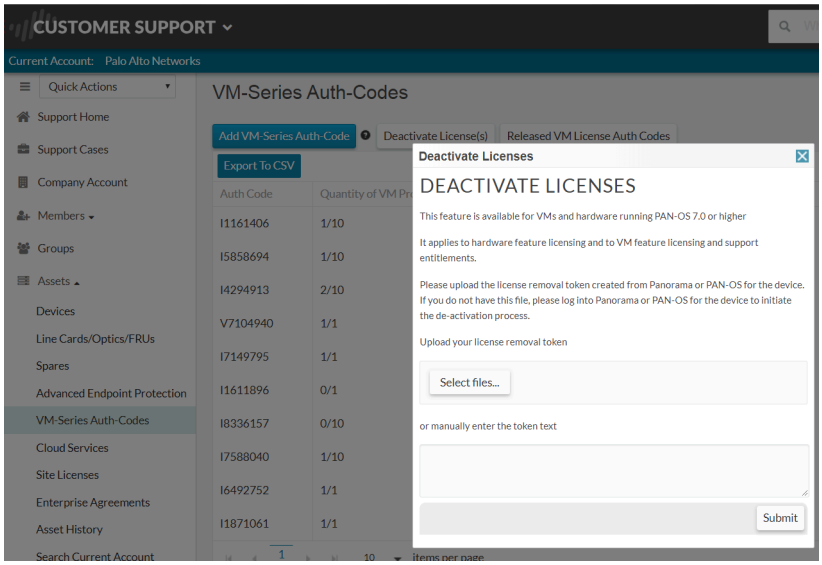
  Export license token（ライセンス トークンのエクスポート）リンクをクリックし、トークン ファイルをローカル コンピュータに保存します。サンプルのトークンファイル名は次のとおりです。20150128_1307_dact_lic.01282015.130737.tok

  ファイアウォールを再起動するよう指示され、再起動と同時にライセンスが非アクティブ化されます。

©2023 Palo Alto Networks, Inc.

STEP 5 | （手動プロセス - インターネットなし）トークンファイルを使用して、変更をライセンスサーバーに登録します。

1. Palo Alto Networks カスタマー サポート Web サイトにログインします。
2. **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード） > **Deactivate License(s)**（ライセンスの非アクティベート）を選択します。
3. Palo Alto Networks カスタマー サポート Web サイトにログインした状態でトークンファイルをアップロードし、無効化作業を完了させます。



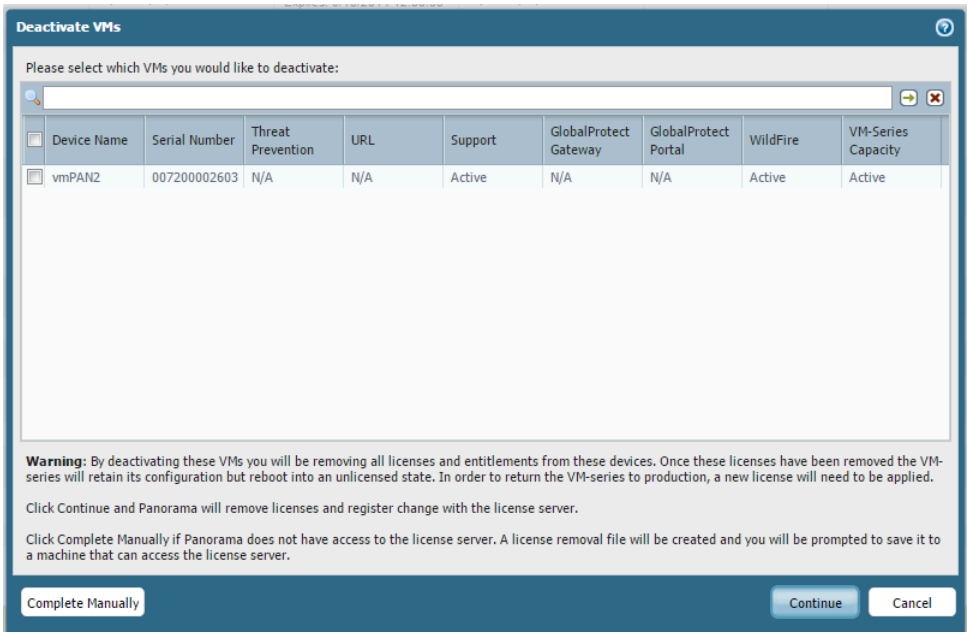
Panorama から **VM** を非アクティブ化します。

Panorama から VM ライセンスを非アクティブ化するには、以下の作業を行ってください。

STEP 1 | Panorama Web インターフェイスにログインして、**Panorama** > **Device Deployment**（デバイスのデプロイ） > **Licenses**（ライセンス）の順に選択します。

©2023 Palo Alto Networks, Inc.

STEP 2 | **Deactivate VMs**（**VM** の無効化）を行い、無効化する VM-Series ファイアウォールを選択します。



STEP 3 | VM の無効化を行う場合は以下の方法があります。

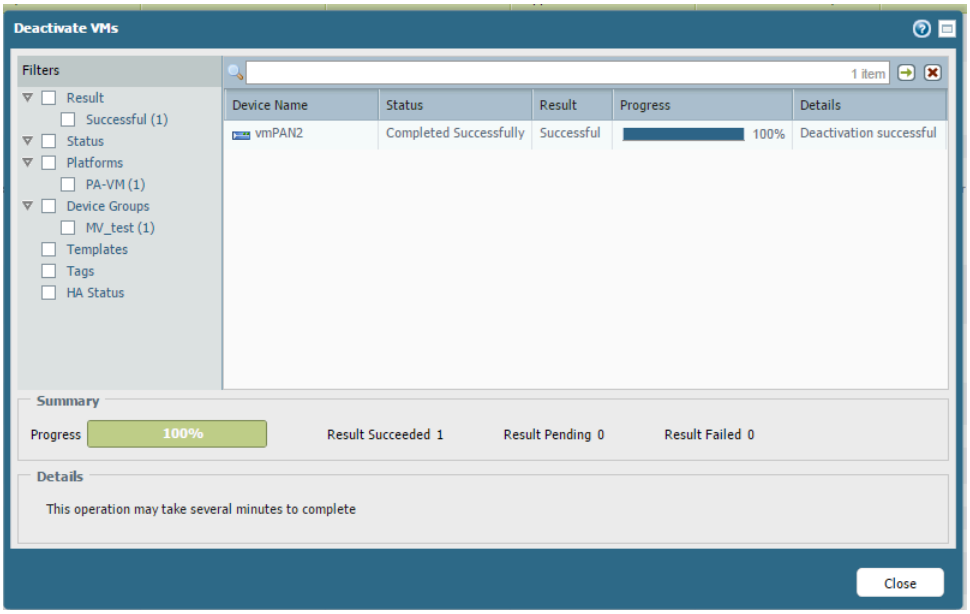
- **Continue**（続行） — Panorama が Palo Alto Networks ライセンス サーバーと直接通信し、変更内容を登録できる場合。ファイアウォールでライセンスが非アクティブ化されたことを確認するには、**Panorama** での更新 > デバイスのデプロイメント > ライセンスを選択します。ファイアウォールは自動的に再起動されます。

©2023 Palo Alto Networks, Inc.

- 手動で完了する - Panorama にインターネットアクセスがない場合、Panorama 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）リンクをクリックし、トークン ファイルをローカル コンピュータに保存します。サンプルのトークンファイル名は次のとおりです。20150128_1307_dact_lic.01282015.130737.tok

  正常完了を知らせるメッセージが画面に表示され、ファイアウォールは自動的に再起動されます。



STEP 4 | （手動プロセスのみ - インターネットなし）トークンファイルを使用して、変更をライセンスサーバーに登録します。

1. Palo Alto Networks カスタマー サポート Web サイトにログインします。
2. **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード） > **Deactivate License(s)**（ライセンスの非アクティベート）を選択します。
3. トークンファイルをアップロードして、非アクティブ化を完了します。

STEP 5 | 無効化された VM-Series ファイアウォールを Panorama の管理対象デバイスから削除します。

1. **Panorama** > **Managed Devices**（管理対象デバイス）を選択します。
2. 管理対象デバイスの一覧から無効化したファイアウォールを選択し、**Delete**（削除）をクリックします。

   ファイアウォールを削除する代わりに、別のデバイスグループを作成し、無効化した *VM-Series* ファイアウォールをこのグループに入れる方法もあります。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのライセンス バンドルを更新

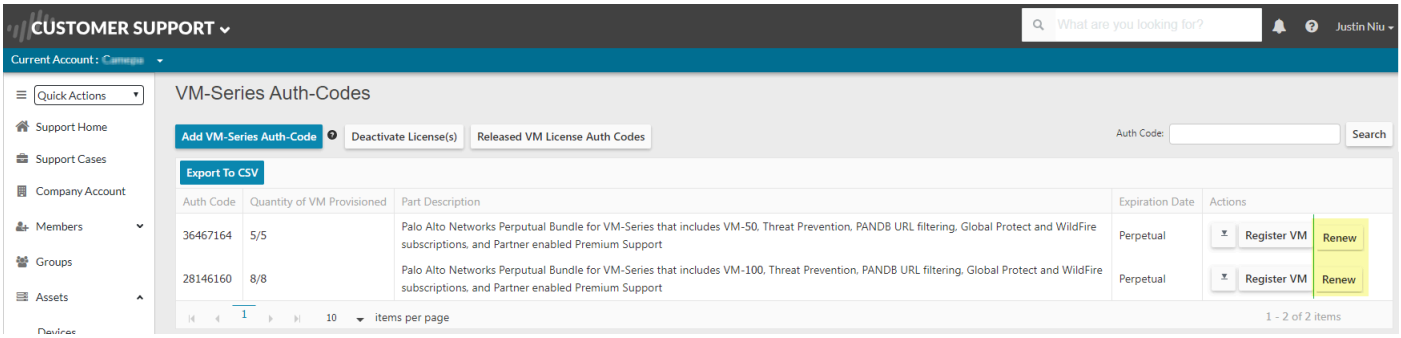
VM-Series ファイアウォールのバンドル ライセンスを更新する必要がある場合は、Palo Alto Networks カスタマーサポート ポータルにログインし、ライセンス数を調整してデプロイメントのニーズに合わせることができます。更新時に使用傾向を確認し、将来のニーズに合わせて次のオプションを選択することができます：

- **Renew**（更新）—すべてのライセンスを現状のまま更新したり、ライセンス数を増やしたり減らしたりできます。必要なライセンス数を減らす場合は、更新対象でないファイアウォールの基本バンドルを入手するよう選択する必要があります。そうしなければ、更新しないそれらのファイアウォールのライセンスを放棄することになります。ライセンス数を増やす場合は、既存の認証コードに追加分が加算されます。
- **Change to Basic Bundle**（基本バンドルに変更）—サブスクリプションを含む VM-Series バンドル 1 あるいはバンドル 2 ライセンスを持っている場合、永続キャパシティ ライセンスおよびサポート資格が含まれる基本バンドルに変更できます。基本バンドルに切り替える際、以前に購入した VM-Series ファイアウォールのモデルは保持されます。現在デプロイされており、既存の認証コードに関連付けられているすべてのファイアウォールは継続的に機能し、サポート資格の期限が更新されます。導入していないファイアウォールがある場合、新規インスタンスをデプロイするために使用できる新しい認証コードを受け取ります。
- **Forfeit**（放棄）—不要になったライセンスを放棄します。更新したくないファイアウォールをデプロイしている場合、更新を止めるインスタンスのシリアル番号を選択する必要があります。現在インストールしているソフトウェアおよびコンテンツ バージョンと共にこれらのファイアウォール インスタンスを継続して使用できますが、サブスクリプションおよびサポート資格は無効になります。プロビジョニングしていない VM-Series ファイアウォールのライセンスを放棄するには、単に放棄する数を選択します。

STEP 1 | ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート ポータルにログインします。

STEP 2 | **Assets**（アセット） > **VM-Series Auth-Codes**（**VM-Series** 認証コード）を選択し、更新する認証コードを探します。

更新可能な認証コードについては、**Renew**（更新）オプションが表示されます。

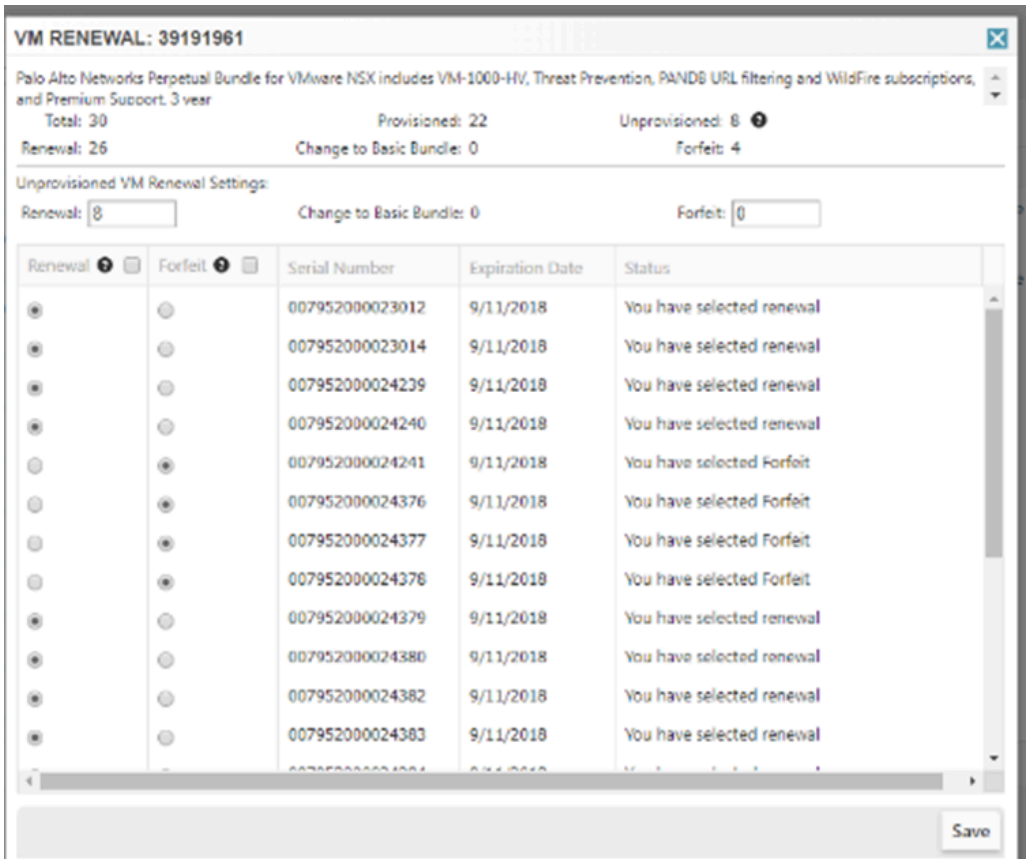


STEP 3 | **Renew**（更新）リンクをクリックし、**Renew**（更新）、**Change to Basic Bundle**（ベーシック バンドルに変更）、あるいは**Forfeit**（放棄）するシリアル番号を選択します。

ファイアウォールをプロビジョニングしていない場合は、行で Serial Number（シリアル番号）に対応するオプションを選択します。ファイアウォール インスタンスをプロビジョニン

©2023 Palo Alto Networks, Inc.

グ解除した場合、**Unprovisioned VM Renewal Settings**（プロビジョニング解除された **VM** の更新の設定）で選択した更新オプションごとに数量を選択します。



STEP 4 | 変更を**Save**（保存）します。

処理を行うために変更が送信されたことを確認する内容が画面に表示されます。変更の送信後に Renew（更新）をもう一度選択すると、各シリアル番号に対するリクエストのステータスが表示されます。更新処理がすでに開始されており、追加のリビジョンを行う必要がある場合は、変更を保存できません。サポートが必要な場合は、更新チーム（renewals@paloaltonetworks.com）までご連絡ください。

©2023 Palo Alto Networks, Inc.

クラウド セキュリティ サービス プロバイダー（CSSP）用ライセンス

Palo Alto Networks CSSP パートナー プログラムにより、サービス プロバイダーは、セキュリティアズアサービスまたはセキュリティアズアホステッドアプリケーションを提供できるようになります。Palo Alto Networks では、クラウド セキュリティ サービス プロバイダー（CSSP）パートナーに、エンタープライズ ユーザーとは異なるライセンス オプションを用意しています。

CSSP パートナーには、サブスクリプションとサポートがバンドルされた VM-Series ファイアウォールで従量制ライセンス モデルを提供しています。CSSP パートナーは、VM-Series モデルで期間ベースのキャパシティ ライセンスと、脅威阻止、URL フィルタリング、AutoFocus、GlobalProtect、および WildFire のサブスクリプション ライセンス、そしてテクニカル サポートやソフトウェア アップデートを利用できるサポート資格を組み合わせて利用することができます。HA 構成でファイアウォールをデプロイする場合は、費用対効果に優れた高可用性オプションを購入できます。

- CSSP ライセンス パッケージの認証コードの取得
- CSSP 認証コードを使用した VM-Series ファイアウォールの登録
- 登録した VM-Series ファイアウォールに関する顧客情報を追加

CSSP ライセンス パッケージの認証コードの取得

CSSP パートナーになるには、Palo Alto Networks CSSP パートナー プログラムに登録する必要があります。CSSP プログラムへの登録方法については、Palo Alto Networks のチャネル ビジネス マネージャーまでお問い合わせください。プログラムに登録された方には、Palo Alto Network のサポート ポータルで、ライセンス パッケージを選択し、ライセンスの利用状況を追跡して、ライセンス資格を適用するためのツールが提供されます。

ライセンス パッケージとは、以下のオプションの組み合わせです。

- 利用期間 – 従量制オプションには、毎時、毎月、1 年間、および 3 年間があります。
- VM-Series ファイアウォール モデル – モデル番号と各モデルに割り当てられたキャパシティであり、VM-100、VM-200、VM-300、および VM-1000-HV があります。
- サブスクリプション バンドル – ベーシック、バンドル 1、およびバンドル 2 の 3 つのオプションがあります。ベーシック オプションにはサブスクリプションは含まれません。バンドル 1 には、IPS、AV、マルウェア阻止を含む脅威阻止ライセンスが含まれます。バンドル 2 には、脅威阻止（IPS、AV、マルウェア阻止を含む）、DNS セキュリティ、GlobalProtect、WildFire、および PAN-DB URL フィルタリング ライセンスが含まれます。
- サポート レベル – プレミアム サポートまたはバックライン サポート。
- 冗長ファイアウォール – オプションとしては、高可用性（HA）と HA なしがあります。冗長ファイアウォールのペアをデプロイしようと計画している場合は、費用対効果に優れたオプションとなります。

©2023 Palo Alto Networks, Inc.

たとえば、PAN-VM-300-SP-PREM-BND1-YU は 1 年間のパッケージあり、プレミアム サポートとサブスクリプション バンドル 1 が付いた VM-300 が含まれます。各パッケージは、最大 10,000 インスタンスの VM-Series ファイアウォールをサポートします。

ライセンス パッケージを選択すると、認証コードが記載された電子メールが届きます。処理の完了まで最大 48 時間かかります。

STEP 1 | ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。新しいアカウントが必要な場合は「サポート アカウントの作成」を参照してください。

STEP 2 | サポート アカウントに登録された認証コードを表示するには、**CSSP** > **Order History**（購入履歴）を選択します。

ファイアウォールのデプロイ時には、各ファイアウォール インスタンスを認証コードで登録しなければなりません。

CSSP 認証コードを使用した VM-Series ファイアウォールの登録

VM-Series ファイアウォールのライセンスをアクティベーションするには、VM-Series ファイアウォールをデプロイして初期設定を完了している必要があります。CSSP パートナーは、ファイアウォールを登録する際に以下のオプションを選択できます。

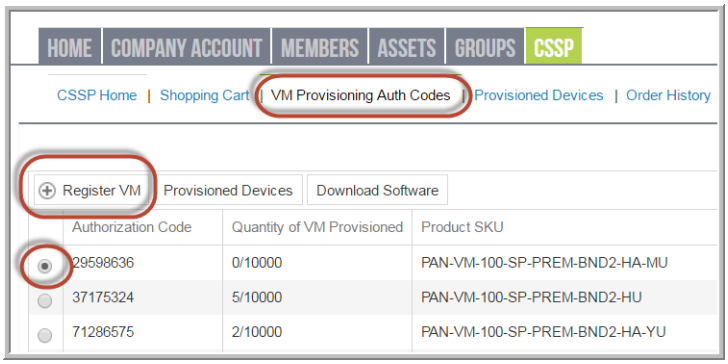
- API – カスタム スクリプトまたはオーケストレーション サービスを利用する場合は、ライセンス API を使用します。このオプションを使用すると、ファイアウォールは、直接インターネットに接続する必要がなくなります。
- Bootstrap（ブートストラップ） – このオプションを使用すると、ファイアウォールが自動的に設定され、最初の起動時にライセンスが供与されます。「VM-Series ファイアウォールのブートストラップ」を参照してください。
- Firewall web interface（ファイアウォールの Web インターフェイス） – ファイアウォールの Web インターフェイスを使用して、VM-Series ファイアウォール（スタンドアロン版）でのライセンスのアクティベーションができます。このワークフローは、インターネットにアクセスできるファイアウォールでも、インターネットにアクセスできないファイアウォールでも有効です。
- Customer Support Portal（カスタマー サポート ポータル） – このオプションを使用すると、以下に示すように、Palo Alto Networks カスタマー サポート ポータルでファイアウォールを手動で登録できます。

STEP 1 | ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。新しいアカウントが必要な場合は「サポート アカウントの作成」を参照してください。

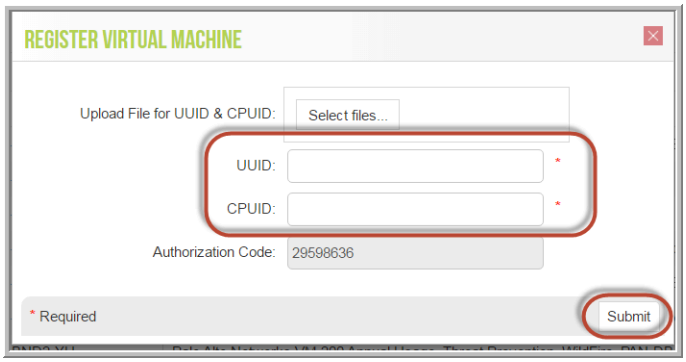
STEP 2 | サポート アカウントに登録された認証コードを表示するには、**CSSP** > **Order History**（購入履歴）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 3 | **CSSP** > **VM Provisioning Auth Codes**（**VM** プロビジョニング認証コード）の順に選択してから、**Authorization Code**（認証コード）を選択し、**Register VM**（**VM** を登録）をクリックします。



STEP 4 | VM インスタンスの **UUID** と **CPUID** を入力し、**Submit**（送信）をクリックします。ポータルによってファイアウォールのシリアル番号が生成されます。



デプロイ済みの *VM-Series* ファイアウォール数と、各認証コードで現在使用可能なライセンス数を確認できます。特定の認証コードで登録されたファイアウォールの総数を表示するには、***CSSP*** > ***VM Provisioning Auth Codes***（***VM*** プロビジョニング認証コード）の順に選択した後、***Authorization Code***（認証コード）を選択し、***Provisioned Devices***（プロビジョニングされたデバイス）をクリックします。

登録した VM-Series ファイアウォールに関する顧客情報を追加

CSSP ライセンスを使用している場合は、ファイアウォールの登録後に、Palo Alto Networks サポート ポータルまたはライセンス API を使用して、VM-Series ファイアウォールのシリアル番号を、ファイアウォールを準備した顧客にリンクさせます。

- 「登録した VM-Series ファイアウォールに関する顧客情報を追加（カスタマー サポート ポータル）」を参照してください。サポート ポータルでは、ユーザー名とパスワードによる認証を行います。
- 「登録した VM-Series ファイアウォールに関する顧客情報を追加（API）」を参照してください。API は、ライセンス API キーを使用して認証を行います。

©2023 Palo Alto Networks, Inc.

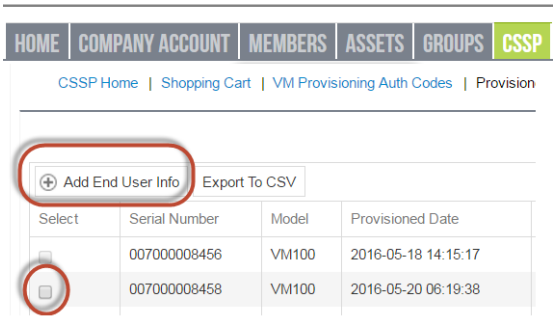
登録した VM-Series ファイアウォールに関する顧客情報を追加（カスタマー サポート ポータル）

カスタマー サポート ポータル経由で登録済みファイアウォールのエンド ユーザー情報を追加するには、以下の手順に従ってください。

STEP 1 | ご自身のアカウント情報を使用してPalo Alto Networks カスタマーサポート Web サイトにログインします。

STEP 2 | **CSSP** > **Provisioned Devices**（プロビジョニング対象デバイス）の順に選択します。

STEP 3 | **Serial Number**（シリアル番号）を選択して **Add End User Info**（エンド ユーザー情報の追加）をクリックします。

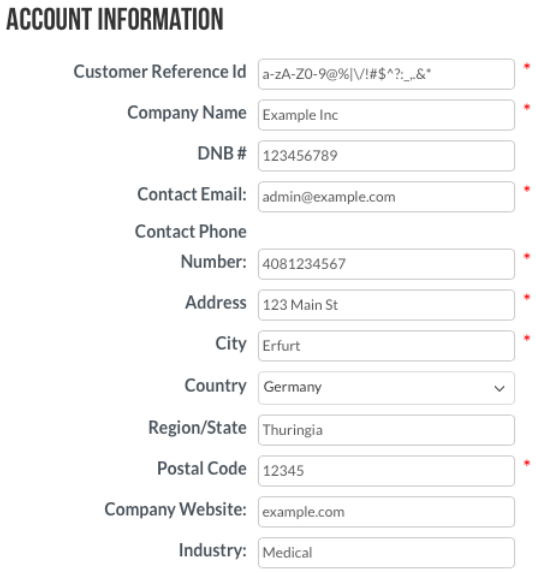


©2023 Palo Alto Networks, Inc.

STEP 4 | ユーザーの**Account Information**（アカウント情報）を次のように入力します。

- Customer Reference Id：Required
- 会社名:Required
- DNB #：Data Universal Numbering System（D-U-N-S）番号
- Contact Email：必須、エンド ユーザーの電子メール アドレス
- Contact Phone Number：エンド ユーザーの電話番号
- アドレス：必須、エンド ユーザーの住所
- 国:必須、ISO の 2 文字の国名コード
- City：必須、エンド ユーザーの居住都市名
- Region/State：必須、米国およびカナダの場合は、ISO の 2 文字の行政区画/属領名コードを入力しなければなりません。他の国の場合は任意の英文字列を入力できます
- Postal Code：必須、エンド ユーザーの郵便番号
- Company Website：エンド ユーザーの Web サイトの URL
- Industry：エンド ユーザーが属する業界のタイプ（ネットワーク、コンサルタント等）

Submit をクリックして情報を保存します。



アカウント情報を追加すると、その顧客に対して登録されているすべてのファイアウォールを見つけられるようになります。***Search Existing End User***（既存のエンド ユーザーの検索）に顧客 *ID* または顧客名を入力してから ***Search***（検索）をクリックすると、その顧客に対してプロビジョニングされているすべてのファイアウォールが検索されます。

登録した VM-Series ファイアウォールに関する顧客情報を追加（API）

https://api.paloaltonetworks.com/api/license/ReportEndUserInfo で API にアクセスできます。

©2023 Palo Alto Networks, Inc.

API リクエストでは HTTP POST メソッドを使用しなければならず、API キーを含み、コンテンツ タイプを JSON として指定する HTTP リクエスト ヘッダーを含めなければなりません。API レスポンスは JSON フォーマットで返されます。

STEP 1 | ライセンス API キーを取得します。

STEP 2 | ReportEndUserInfo API を使用して、CSSP に登録する VM-Series ファイアウォールに関するエンド ユーザー情報を追加します。

URL: **`https://api.paloaltonetworks.com/api/license/ReportEndUserInfo`**

ヘッダー：

- Content-Type：application/json
- apiKey：*API*キー

パラメータ:

- `SerialNumbers`:必須、有効なファイアウォール シリアル番号を 1 つ以上指定してください
- `CustomerReferenceId`:Required
- `CompanyName`:必須、エンドユーザーの勤務先
- `DnBNumber`:Data Universal Numbering System（D-U-N-S）番号
- `PhoneNumber`：エンド ユーザーの電話番号
- `EndUserContactEmail`：必須、エンド ユーザーの電子メール アドレス
- `Address`：必須、エンド ユーザーの住所
- `Country`：必須、ISO の 2 文字の国名コード
- `City`：必須、エンド ユーザーの居住都市名
- `Region/State`：必須、米国およびカナダの場合は、ISO の 2 文字の行政区画/属領名コードを入力しなければなりません。他の国の場合は任意の英文字列を入力できます
- `PostalCode`：必須、エンド ユーザーの郵便番号
- `Industry`：エンド ユーザーが属する業界のタイプ（ネットワーク、コンサルタント等）
- `WebSite`：エンド ユーザーの Web サイトの URL
- `CreatedBy`：この情報を提出するシステムまたは個人

Curl を使用して登録済みの **VM-Series** ファイアウォールにエンド ユーザーの情報を追加するリクエストの例：

```
curl -X POST "http://api.paloaltonetworks.com/api/license/
ReportEndUserInfo" \-H "Content-Type: application/json" \-
H "apikey: your_key_here" \--data-raw '{ "SerialNumbers":
 ["0001A101234"], "CustomerAccountId": 12345, "CompanyName":
 "ExampleInc", "DnBNumber": "123456789", "Address": "123 Main St",
 "City": "Sunnydale", "Region": "CA", "State": "CA", "Country":
 "US", "PostalCode": "12345", "Industry": "Medical", "PhoneNumber":
```


©2023 Palo Alto Networks, Inc.

```
"4081234567", "WebSite": "example.com", "EndUserContactEmail":
"admin@example.com", "CreatedBy": "Jane Doe"}'
```

API レスポンスの例：

```
"{"Message": "End User Information Updated Successfully"}"
```

エラーが発生した場合は、「ライセンス API のエラー コード」を参照してください。

©2023 Palo Alto Networks, Inc.

ESXi サーバーでの VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールは、仮想マシンのパッケージングとデプロイのための標準手法である Open Virtualization Alliance（OVA）フォーマットで配布されます。VMware ESXi を実行可能なすべての x86 デバイスにこのソリューションをインストールできます。

VM-Series ファイアウォールをデプロイするには、vSphere ネットワーク、ESXi ホストのセットアップと設定、仮想マシン ゲストのデプロイメントなど、VMware と vSphere について精通している必要があります。

VM-Series ファイアウォールのデプロイ プロセスを自動化するには、最適な設定とポリシーが含まれた標準テンプレートを作成します。その後 vSphere API と PAN-OS XML API を使用して、ネットワークに新しい VM-Series ファイアウォールをすばやくデプロイできます。

以下の情報については、各トピックを参照してください：

- VMware vSphere Hypervisor（ESXi）でサポートされているデプロイ
- ESXi システム上の VM-Series — 要件と制限
- VMware vSphere Hypervisor（ESXi）への VM-Series ファイアウォールのインストール
- vCenter 上の VM 監視
- ESXi のデプロイメントのトラブルシューティング
- VM-Series for ESXi のパフォーマンス調整

VMware vSphere Hypervisor（ESXi）でサポートされているデプロイ

ESXi サーバーには VM-Series ファイアウォールの 1 つ以上のインスタンスをデプロイできます。ネットワークのどこに VM-Series ファイアウォールをデプロイするかは、トポロジによって異なります。以下のいずれかのオプションを選択します（VMware NSX を使用しない環境の場合）。

- **One VM-Series firewall per ESXi host**（**ESXi** ホストごとに **1** つの **VM-Series** ファイアウォール） — ESXi ホスト上のすべての VM サーバーは、ホストから物理ネットワークに移動するときにファイアウォールを通過します。VM サーバーは、標準仮想スイッチを介してファイアウォールに接続されます。ゲスト サーバーはその他のネットワークには接続できないため、ファイアウォールは ESXi ホストからのすべての発信トラフィック上を監視および制御できます。もう 1 つのバリエーションとして、同じ ESXi ホスト上のサーバー間（East-West トラフィック）を含め、すべてのトラフィックにもファイアウォールを通過させるという方法もあります。
- **One VM-Series firewall per virtual network**（仮想ネットワークごとに **1** つの **VM-Series** ファイアウォール） — すべての仮想ネットワークそれぞれに 1 つの VM-Series ファイアウォールをデプロイします。1 つ以上の ESXi ホストに、内部ネットワークに属する仮想マシンのグループ、外部ネットワークに属するグループ、および DMZ に属するグループが含まれるネットワークを設計している場合、各グループ内のサーバーを保護するように VM-Series ファイアウォールをデプロイできます。グループまたは仮想ネットワークが仮想スイッチやポートグループを他の仮想ネットワークと共有していない場合、ホスト内またはホスト間でその他すべての仮想ネットワークと完全に分離されます。他のネットワークへの物理パスや仮想パスは存在しないため、各仮想ネットワーク上のサーバーはファイアウォールを使用して他のネットワークと通信する必要があります。ファイアウォールは各仮想ネットワークに接続された（標準または分散）仮想スイッチからのすべての発信トラフィック上を監視および制御できます。
- ハイブリッド環境—物理ホストと仮想ホストの両方が使用されます。VM-Series ファイアウォールは、従来の集約場所にある物理的なファイアウォール アプライアンスを置き換えることができます。ハイブリッド環境は、すべてのデバイスに共通のサーバー プラットフォームの利点を実現し、ハードウェアとソフトウェアのアップグレードの依存関係を解除します。

「ESXi システム上の VM-Series — 要件と制限」と「VMware vSphere Hypervisor（ESXi）への VM-Series ファイアウォールのインストール」を続行してください。

©2023 Palo Alto Networks, Inc.

ESXi システム上の VM-Series — 要件と制限

このセクションでは、VMware vSphere Hypervisor（ESXi）上で稼働する VM-Series ファイアウォールの要件と制限を示します。VM-Series ファイアウォールのデプロイ方法については、「VMware vSphere Hypervisor（ESXi）への VM-Series ファイアウォールのインストール」を参照してください。

- ESXi システム上の VM-Series — 要件
- ESXi システム上の VM-Series — 制限

ESXi システム上の VM-Series — 要件

ESXi サーバーには、VM-Series ファイアウォールの複数のインスタンスを作成およびデプロイできます。ファイアウォールの各インスタンスには ESXi サーバーの最小リソース割り当て（CPU 数、メモリおよびディスク領域）が必要であるため、最適なパフォーマンスを得るために以下の仕様に従っていることを確認してください。

VM-Series ファイアウォールは次の要件を満たしていなければなりません。

- ホスト CPU は、仮想化拡張機能を持つ x86 ベースの Intel または AMD CPU でなければなりません。
- サポートしているバージョンの ESXi については、互換性マトリックスを参照してください。vmx バージョンのサポートは、VM-Series ファイアウォールのデプロイに使用する OVA に基づいており、このバージョンを変更することはできません。VM-Series ソフトウェア バージョンのアップグレードまたはダウングレードでは、起動時に有効になった vmx バージョンは変更されません。
- VM-Series モデルの最小ハードウェア要件については、「VM-Series システム要件」を参照してください。
- 2 つ以上のネットワークインターフェイス（vNIC）。1 つは管理インターフェイスの vNIC 専用、もう 1 つはデータ インターフェイス用です。データ トラフィック用の vNIC は 8 つまで追加できます。インターフェイスを追加するには、ESXi サーバーで VLAN Guest Tagging（VGT）を使用するか、ファイアウォール上にサブインターフェイスを構成します。

  デフォルトでは、ハイパーバイザによって割り当てられた MAC アドレスが有効になっています。vSphere は、一意の vNIC MAC アドレスを VM-Series ファイアウォールの各データ プレーン インターフェイスに割り当てます。ハイパーバイザによって割り当てられた MAC アドレスを無効にすると、VM-Series ファイアウォールは独自のプールの MAC アドレスの各インターフェイスを割り当てます。これにより、各インターフェイスの MAC アドレスが異なるため、ファイアウォールのデータプレーン インターフェイスが接続されている仮想スイッチのポート グループで無差別モードを有効にする必要があります。これによりファイアウォールはフレームを受信できます（「ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング」を参照）。無差別モードとハイパーバイザによって割り当てられたMACアドレスのいずれも無効の場合、ファイアウォールはトラフィックを受信しません。これは、vSphere が、フレームの宛先 MAC アドレスと vNIC MAC アドレスが一致しない場合に、仮想マシンにフレームを転送しないための措置です。

©2023 Palo Alto Networks, Inc.

- デフォルトでデータ プレーン開発キット（DPDK）は、ESXi 上の VM-Series ファイアウォールで有効になっています。DPDK の詳細は、「ESXi 上の DPDK の有効化」を参照してください。
- VM-Series ファイアウォールの最高のパフォーマンスを実現するために、VM-Series ファイアウォールをデプロイする前にホストに以下の調整を行うことができます。詳細は、「VM-Series for ESXi のパフォーマンス調整」を参照してください。
  - **DPDK** を有効にします。DPDK を有効にすると、Linux カーネルがバイパスされるため、ホストのパケット処理速度が向上します。代わりに、NIC と対話するときは、ドライバと DPDK ライブラリが使用されます。
  - **SR-IOV** を有効にします。Single Root I/O Virtualization（SR-IOV）を使用すると、1 つのルート ポートの 1 つの PCIe 物理デバイスを、ハイパーバイザやゲストに対して複数の個別の物理デバイスのように見せかけることができます。

    SR-IOV を有効にする物理ポートに vSwitch を設定しないでください。ネットワーク上のホストまたは他の仮想マシンと通信するために、VM-Series ファイアウォールが物理ポートおよび関連する仮想機能（VF）を排他的にそのインターフェイスにアクセスする必要があります。
  - **NIC** のマルチキュー サポートを有効にします。マルチキューにより、vCPU の数に合わせてネットワークのパフォーマンスを高めることができ、複数の TX および RX キューを作成して並列パケット処理を実現できます。

ESXi システム上の VM-Series — 制限

VM-Series ファイアウォールの機能は Palo Alto Networks のハードウェア ファイアウォールと非常によく似ていますが、以下の制限があります。

- ESXiのVM-SeriesではVMwareスナップショット機能を使用しないでください。スナップショットはパフォーマンスに影響を及ぼし、断続的かつ不定のパケットロスを引き起こす可能性があります。VMWareで推奨されるスナップショットの使用方法を参照してください。

  設定のバックアップが必要な場合は Panorama を使用するか、ファイアウォールで **Export named configuration snapshot**（指定した設定のスナップショットをエクスポート）（Device（デバイス） > Set up（設定） > Operations（操作））を使用します。**Export named cinfiguration**（指定した設定のスナップショット）を使用して、ファイアウォールのアクティブな設定内容（`running-config.xml`）がエクスポートされ、任意のネットワークロケーションに保存できるようになります。
- 専用 CPU コアを使用することを推奨します。
- 高可用性（HA）リンクモニタリングは、ESXiのVM-Seriesファイアウォールではサポートされていません。パスモニタリングを有効にして、ターゲットIPアドレスまたはネクスト ホップIPアドレスとの接続を確認します。
- 最大 10 個のポートを設定できます。これは VMware の制限です。1 つのポートは管理トラフィック用として使用され、残りの 9 ポートまではデータ トラフィック用として使用されます。
- vmxnet3 ドライバのみがサポートされています。
- 仮想システムはサポートされません。

©2023 Palo Alto Networks, Inc.

- VM-SeriesファイアウォールのvMotionは、vSphere 6.5、6.7、および7.0でサポートされています（ESXiホストが同種のCPU設定を保有している場合）。vSphere 6.5または6.7にインストールされている状態で、ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用を行うにはPAN-OS 9.1.6以降が必要です。
- レイヤー 2 に接続している ESXi vSwitch ポート グループと VM-Series ファイアウォールの vwire インターフェイスでは偽装送信と無差別モードを有効にする必要があります。
- ESXi 上の VM-Series ファイアウォールで PCI デバイスを使用するには、メモリ マップ I/O（MMIO）を 4GB 以下にする必要があります。サーバーの BIOS で 4GB を超える MMIO を無効にできます。これは ESXi の制限です。
- ESXi 7.0を使用する場合、PCIデバイスパススルーを持つ仮想マシンにVFをアタッチする際に、インターフェイスは表示されません。

©2023 Palo Alto Networks, Inc.

VMware vSphere Hypervisor（ESXi）への VM-Series ファイアウォールのインストール

VM-Series ファイアウォールをインストールするには、Open Virtualization Alliance format（OVA）テンプレートへのアクセス権が必要です。受注完了電子メールで受け取った認証コードを使用し、VM-Seriesファイアウォールを登録して OVA テンプレートをダウンロードします。OVA テンプレートは、3 種類のファイルを含む zip アーカイブです。

- .mf:パッケージ内の個々のファイルの SHA-1 ダイジェストを含む OVF マニフェスト ファイル。
- .ovf:パッケージとそのコンテンツについてのすべてのメタデータが記述されている OVF 記述子ファイル。
- .vmdk:仮想化バージョンのファイアウォールを含む仮想ディスク イメージ ファイル。

ESXi で VM-Series ファイアウォールをインストールおよび設定するには、次のタスクを実行します。

- VM-Series for ESXi で使用するインターフェイスのプランニング
- ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング
- ESXi 上の VM-Series の初期設定の実行
- （任意）VM-Series ファイアウォールにディスク スペースを追加する
- ESXi および vCloud Air 上の VM-Series ファイアウォールでの VMware ツールの使用
- ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用
- ESXi 上での VM-Series CLI を使用した管理インターフェースのスワップ

VM-Series for ESXi で使用するインターフェイスのプランニング

VM-Series ファイアウォールの vNIC とインターフェイスのマッピングを計画することにより、再起動と設定の問題を回避できます。以下の表は、ESXi 上で 10 個の vNIC がすべて有効になっている場合における VMware vNIC と VM-Series インターフェイス間のデフォルト マッピングを示しています。

VMware vNIC	VM-Series インターフェイス
1	Ethernet 1/0（mgmt）
2	Ethernet 1/1（eth1）
3	Ethernet 1/2（eth2）
4	Ethernet 1/3（eth3）
5	Ethernet 1/4（eth4）

©2023 Palo Alto Networks, Inc.

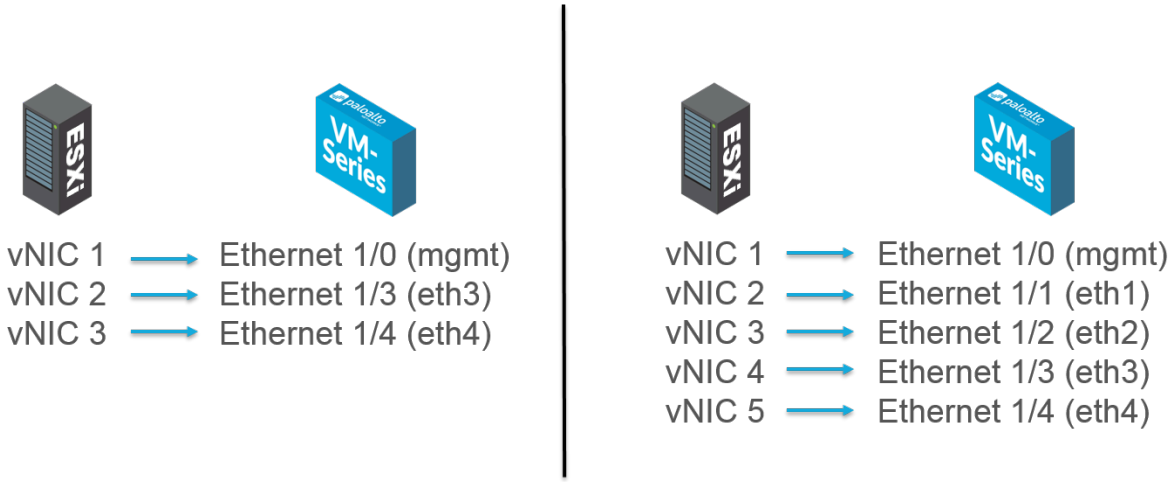
VMware vNIC	VM-Series インターフェイス
6	Ethernet 1/5（eth5）
7	Ethernet 1/6（eth6）
8	Ethernet 1/7（eth7）
9	Ethernet 1/8（eth8）
10	Ethernet 1/9（eth9）

ESXi 上でどの vNIC を追加するかにかかわらず、VM-Series ファイアウォール上のマッピングは同じままです。ファイアウォール上でアクティベートするインターフェイスは必ず ESXi 上で次に使用可能な vNIC を選択します。

次の図では、VM-Series ファイアウォールの eth3 と eth4 が ESXi の vNIC 2 と 3 にペア設定され、eth1 と eth2 はマッピングされていません。

現在のマッピングを維持しながら 2 つのインターフェイスをさらに追加する場合は、vNIC 4 と 5 を有効にしてファイアウォールを再起動します。最後にマッピングされたインターフェイスの後にインターフェイスを追加したため、既存の vNIC マッピングは保持されます。

VM-Series ファイアウォールで eth1 と eth2 を有効にすると、右側に示すようにインターフェイスの順序が変更され、トラフィックに影響するマッピングの不一致が発生します。



前述の例で示した問題を回避するには、以下の作業を行います：

- 初めて ESXi ホストをプロビジョニングする場合は、最初の vNIC 以外の 9 つの vNIC をすべてアクティブにします。VM-Series ファイアウォールをパワーオンする前に 9 個すべての vNIC をプレースホルダとして追加すると、どの VM-Series インターフェイスでも、順序にかかわらず使用できます。

©2023 Palo Alto Networks, Inc.

- すべての vNIC がアクティブである場合、インターフェイスをさらに追加する必要はなくなりました。ESXi 上の各 vNIC ではネットワークの選択が必要であるため、空のポート グループをネットワーク プレースホルダとして作成できます。
- マッピングの不一致を回避するために、VM-Series ファイアウォールの vNIC は除去しないでください。

ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング

VM-Series ファイアウォールを（スタンドアロンの）ESXi サーバー上にデプロイするには、以下の手順を実行します。VM-Series NSX エディションファイアウォールをデプロイする場合は、VMware NSX-T での VM-Series ファイアウォールのセットアップを参照してください。

STEP 1 | OVA ファイルをダウンロードします。

VM-Series ファイアウォールを登録し、OVA ファイルを Palo Alto Networks カスタマー サポート Web サイトから取得してください。

OVA ファイルには基本インストールが含まれています。基本インストールが完了した後は、サポート ポータルから最新の *PAN-OS* バージョンをダウンロードしてインストールする必要があります。これにより、基本イメージが作成された後に実装された、最新の修正を適用できます。手順は、「PAN-OS ソフトウェア バージョンのアップグレード（スタンドアロン版）」を参照してください。

STEP 2 | OVA ファイルをデプロイする前に、VM-Series ファイアウォールで必要になる標準仮想スイッチあるいは分散仮想スイッチをセットアップします。

レイヤー *3* インターフェイスで *VM-Series* ファイアウォールをデプロイする場合、デフォルトでは、ハイパーバイザによって割り当てられた MAC アドレスがファイアウォールで使用されます。ハイパーバイザーが割り当てた *MAC* アドレスを無効化する場合、あるいはレイヤー *2*、バーチャル ワイヤ、またはタップ インターフェイスを伴うファイアウォールをデプロイしている場合は、*VM-Series* ファイアウォールに付与されたすべての仮想スイッチを設定（***Accept***（許可）に設定）し、*promiscuous* モード、*MAC* アドレス変更、*Forged*（偽装）転送の各モードを許可するようにしなければなりません。

VM-Series ファイアウォールのフレームを受信するよう、仮想標準スイッチあるいは仮想分散スイッチを設定します。

仮想標準スイッチ

1. **Home**（ホーム） > **Hosts and Clusters**（ホストおよびクラスター）に移動してホストを選択します。
2. **Configure**（設定）タブをクリックして**Virtual Switches**（仮想スイッチ）を表示します。VM-Series ファイアウォールが連結された仮想スイッチごとに、**Properties**（プロパティ）をクリックします。
3. 仮想スイッチに対応するポート グループをハイライト表示し、**Edit Settings**（設定の編集）をクリックします。vSwitch のプロパティ画面で、**Security**（セキュリティ）タブをク

©2023 Palo Alto Networks, Inc.

リックし、**Promiscuous Mode, MAC Address Changes**（無差別モード、**MAC** アドレス変更）および **Forged Transmits**（偽装送信）を **Accept**（承諾）に設定して、**OK** をクリックします。この変更は、仮想スイッチ上のすべてのポート グループに伝搬されます。

仮想分散スイッチ

1. **Home**（ホーム） > **Networking**（ネットワーキング）を選択します。仮想分散スイッチを選択し、編集する**Distributed Port Group**（分散ポート グループ）をハイライト表示します。
2. **Edit Settings**（設定の編集）をクリックして、**Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、**Promiscuous Mode, MAC Address Changes**（無差別モード、**MAC** アドレス変更）および **Forged Transmits**（偽装送信）を **Accept**（承諾）に設定し、**OK** をクリックします。

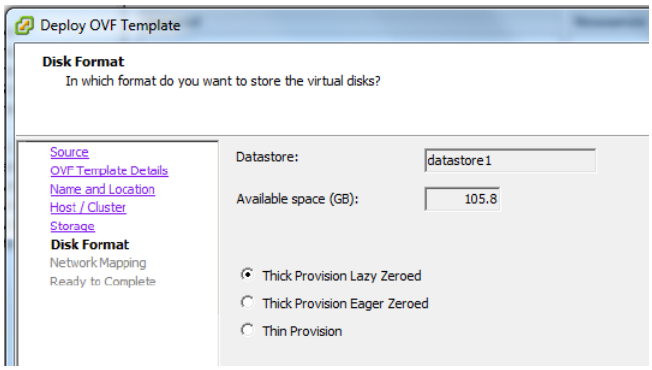
©2023 Palo Alto Networks, Inc.

STEP 3 | OVA をデプロイします。

新規インターフェイスは起動時に検出されるため、*VM-Series* ファイアウォールにインターフェイス（*vNIC*）を追加した場合は、再起動が必要になります。ファイアウォールを再起動する必要性を最小限にするには、初期デプロイ時またはメンテナンス期間中にインターフェイスをアクティブにします。

インストールの進行状況を表示するには、***Recent Tasks***（最近のタスク）リストをモニターします。

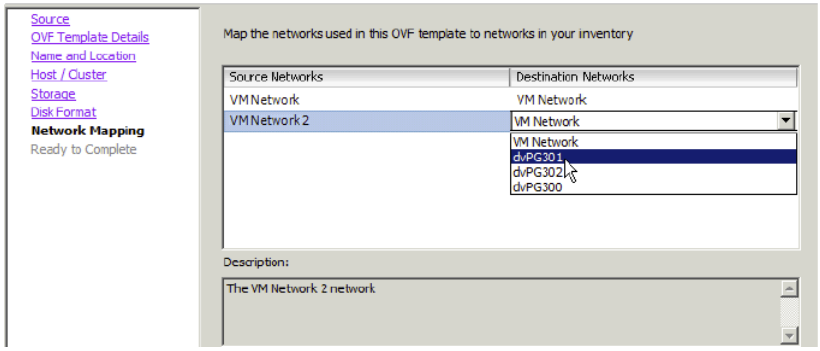
1. vSphere クライアントを使用して vCenter にログインします。必要に応じて、ターゲットの ESXi ホストに直接移動することもできます。
2. vSphere Web クライアントから **Hosts and Clusters**（ホストおよびクラスター）に移動してホストを右クリックし、**Deploy OVF Template**（**OVF** テンプレートのデプロイ）を選択します。
3. 以前にダウンロードした OVA ファイルを参照します。ファイルを選択し、[次へ] をクリックします。テンプレートの詳細を確認して、もう一度 **Next**（次へ）をクリックします。
4. VM-Series ファイアウォール インスタンスに名前を付け、**Inventory Location**（インベントリの場所）ウィンドウでデータ センターとフォルダを選択し、**Next**（次へ）をクリックします。
5. VM-Series ファイアウォールの ESXi ホストを選択し、**Next**（次へ）をクリックします。
6. VM-Series ファイアウォールで使用するデータストアを選択し、**Next**（次へ）をクリックします。
7. データストア プロビジョニングのデフォルト設定をそのままにして、**Next**（次へ）をクリックします。デフォルトは「**Thick Provision Lazy Zeroed**」です。



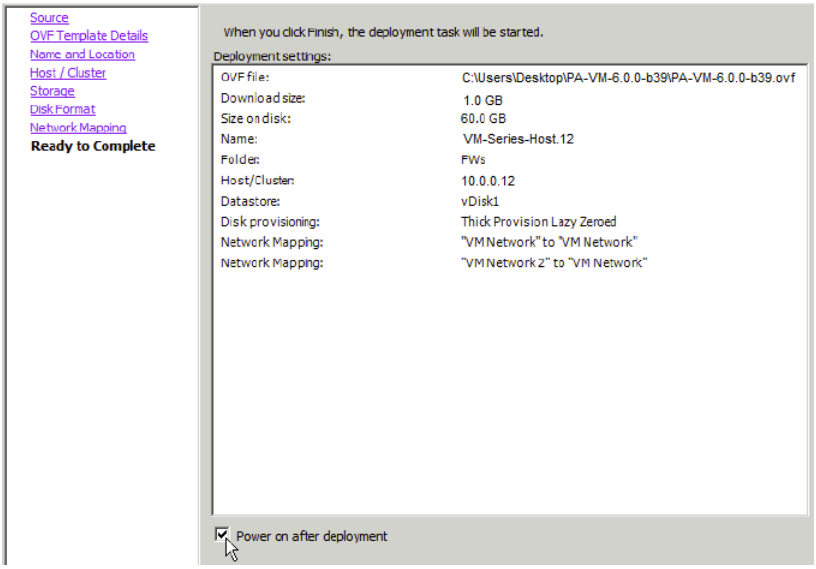
8. 最初に設定された 2 つの vNIC を利用するネットワークを選択します。1 つ目の vNIC は管理インターフェイスで使用され、2 つ目の vNIC は最初のデータ ポートで使用され

 ©2023 Palo Alto Networks, Inc.

ます。**Source Networks**（ソース ネットワーク）が正しい **Destination Networks**（ターゲット ネットワーク）にマップされていることを確認してください。



9. 詳細を確認し、**Power on after deployment**（デプロイ後にパワー オン）を選択し、**Next**（次へ）をクリックします。



10. 導入が完了したら、**Summary**（サマリー）タブをクリックして現在の状態を確認します。

ESXi 上の VM-Series の初期設定の実行

VM-Series ファイアウォールへのネットワーク アクセスを設定するには、ESXi サーバーでバーチャル アプライアンス コンソールを使用します。デフォルトでは、VM-Series ファイアウォールは、DHCP を使用して、管理インターフェイスの IP アドレスを取得しますが、静的 IP アドレスも割り当てることができます。初期設定が完了したら、Web インターフェイスにアクセスし、詳細な設定タスクを実行します。中央管理のために Panorama を使用している場合、Panorama を使用したデバイス管理の詳細は、『Panorama 管理者ガイド』を参照してください。

ブートストラップを使用して ESXi 上の VM-Series ファイアウォールを設定する場合は、「ESXi における VM-Series ファイアウォールのブートストラップ」を参照してください。

ブートストラップの一般的な情報については、「VM-Series ファイアウォールのブートストラップ」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 1 | ネットワーク管理者から必要な情報を入手します。

- MGT ポートの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS サーバーの IP アドレス

STEP 2 | VM-Series ファイアウォールのコンソールにアクセスします。

1. VM-Series ファイアウォール用の ESXi サーバーで **Console**（コンソール）タブを選択するか、VM-Series ファイアウォールを右クリックして**Open Console**（コンソールを開く）を選択します。
2. Enter キーを押して、ログイン画面にアクセスします。
3. デフォルトのユーザー名/パスワード（admin/admin）を入力して、ログインします。
4. 設定モードに切り替えるには、「**configure**」と入力します。

STEP 3 | 管理インターフェイスへのネットワーク アクセス設定を行います。

以下のコマンドを入力します。

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | 変更をコミットし、設定モードを終了します。

「**commit**」と入力します。

「**exit**」と入力します。

STEP 5 | Palo Alto Networks 更新サーバーなど、ファイアウォール管理に必要な外部サービスへのネットワーク アクセスを確認します。

1. 以下の例に示すように、ping ユーティリティを使用して Palo Alto Networks 更新サーバーへのネットワーク接続を検証します。DNS が解決され、レスポンスに更新サーバーの IP アドレスが含まれていることを確認します。更新サーバーは ping リクエストには応答しません。 DNS の解決を確認したら、Ctrl+C キーを押して ping リクエストを停止します。

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes
 of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
```


©2023 Palo Alto Networks, Inc.

2. 次の CLI コマンドを使用して、Palo Alto Networks 更新サーバーからファイアウォールのサポート資格に関する情報を取得します。要求サポートチェック接続がある場合、更新サーバーはファイアウォールのサポート状況に応答します。

STEP 6 | VM-Series ファイアウォールのテストを開始する前に、容量認証コードを適用してライセンスを取得してください。

ライセンスのない VM-Series ファイアウォールは、約 1230 の同時セッションを処理することができます。環境によっては、このセッション制限にすぐに到達し、想定外の結果が出る可能性があります。

VM-Series ファイアウォールにディスクスペースを追加する

VM-Series ファイアウォールは 60GB の仮想ディスクを必要とし、うち 21GB はログ記録に使用されるようにデフォルト設定されています。

- 大規模なデプロイメントを行う場合、Panorama を使用して次世代ファイアウォールからデータを集約し、ネットワーク上の全トラフィックを可視化します。Panorama は一元化されたログとレポートを提供します。
- Panorama を使用しない小規模なデプロイメントでは、仮想ディスクを新しく追加してログ記憶容量を増やすことができます。新しい仮想ディスクは、ログ用に 60GB～2TB のストレージ容量をサポートできます。この作業については後述します。

仮想アプライアンスが仮想ディスクを使用するように設定されている場合、*VM-Series* ファイアウォールはログを保存しなくなります。アプライアンスが仮想ディスクへの接続を失うと、障害期間中のログが損失する可能性があります。必要に応じて、新規作成した仮想ディスクを *RAID* による冗長性が確保されたデータストア上に配置します。*RAID10* では、ロギングを大量に行うアプリケーションで最適な書き込みパフォーマンスが得られます。

STEP 1 | VM-Series ファイアウォールをパワーオフします。

©2023 Palo Alto Networks, Inc.

STEP 2 | ESXi サーバー上で、仮想ディスクをファイアウォールに追加します。

1. ESXi サーバー上の VM-Series ファイアウォールを選択します。
2. **Edit Settings**（設定の編集）をクリックします。
3. **Add**（追加）をクリックして Add Hardware（ハードウェア追加）ウィザードを起動し、オプションの選択を促されたら、以下のオプションを選択します。
   1. ハードウェア タイプに **Hard Disk**（ハード ディスク）を選択します。
   2. **Create a new virtual disk**（新規仮想ディスクを作成）を選択します。
   3. 仮想ディスク タイプに **SCSI** を選択します。
   4. **Thick provisioning**（シック プロビジョニング）ディスク フォーマットを選択します。
   5. 場所フィールドで、**Store with the virtual machine option**（仮想マシン オプションを使用して保存）を選択します。データストアは ESXi サーバーに存在している必要はありません。
   6. 設定が正しいことを確認し、**Finish**（完了）をクリックしてウィザードを終了します。新しいディスクが、バーチャル アプライアンスのデバイス一覧に追加されます。

STEP 3 | ファイアウォールをパワーオンします。

ファイアウォールの電源を入れると、初めて仮想ディスクが初期化されます。初期化処理が完了するまでの時間は、新しい仮想ディスクのサイズによって異なります。

新しい仮想ディスクが初期化され、準備が完了すると、PAN-OS はすべてのログを既存のディスクから新しい仮想ディスクに移動します。新しいログ エントリーは、この新しい仮想ディスクに記録されるようになりました。

PAN-OS は、新しいディスクを記録するシステム ログ エントリーも生成します。

以前に *PAN-OS* ログを保存するために使用されていた仮想ディスクを再利用すると、既存のディスクのすべてのログが上書きされます。

STEP 4 | 新しい仮想ディスクのサイズを確認します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）を選択します。
2. Logging and Reporting Settings（ロギングおよびレポート設定）セクションで、新しいディスク容量が **Log Storage**（ログ ストレージ）に正しく表示されていることを確認します。

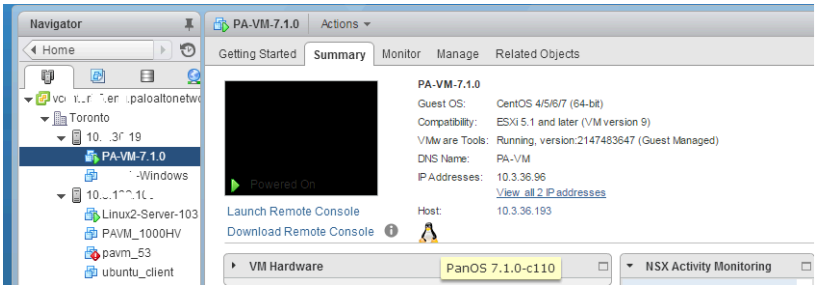
ESXi および vCloud Air 上の VM-Series ファイアウォールでの VMware ツールの使用

VMware Tools ユーティリティは、vCenter Server および vCloud Director からの VM-Series ファイアウォール管理を改善します。VMware Tools は VM-Series ファイアウォールのソフトウェア イメージにバンドルされ、すべてのアップデートは新しい OVF イメージで利用可能になります。vCenter Server または vCloud Director を使用して VMware Tools を手動でインストールまたはアップグレードすることはできません。

©2023 Palo Alto Networks, Inc.

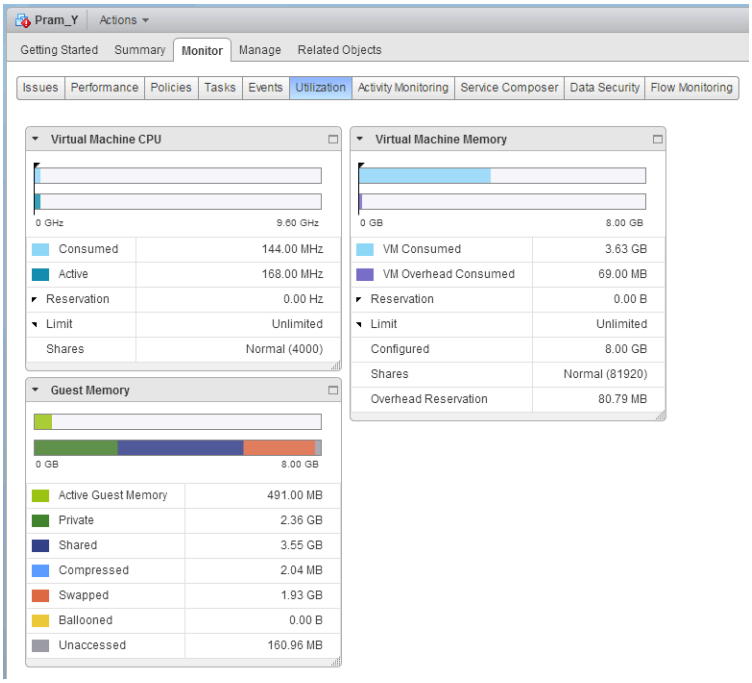
管理インターフェイスで IP アドレス、およびファイアウォールおよび Panorama のソフトウェア バージョンを確認します。

vCenter サーバーの Hosts（ホスト）および Cluster（クラスター）セクションでファイアウォールあるいは Panorama を選択し、管理インターフェイスに割り当てられている IP アドレスおよび現在インストールされているソフトウェア バージョンについての情報を **Summary**（サマリー）タブで確認します。



ハードディスク、メモリ、CPU のリソース使用状況を確認する。この情報を利用して vCenter サーバーのアラームを有効化できます。

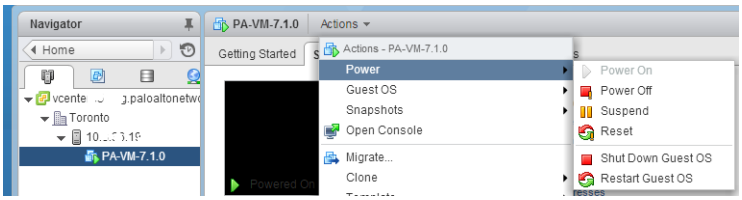
vCenter サーバーの Hosts（ホスト）および Cluster（クラスター）セクションでファイアウォールあるいは Panorama を選択し、ハード ディスク、メモリ、CPU の使用状況についての情報を **Monitor**（監視） > **Utilization**（使用状況）タブで確認します。



 ©2023 Palo Alto Networks, Inc.

vCenter サーバーからファイアウォールおよび Panorama を再起動するか、グレースフル シャットダウンを実行します。

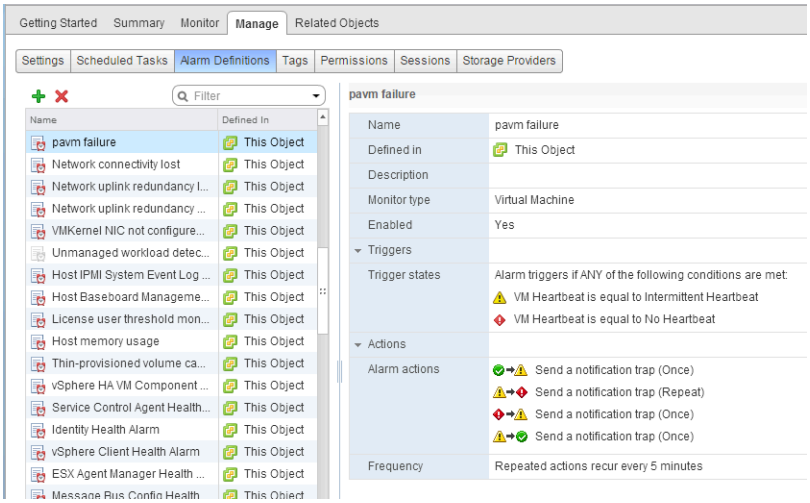
vCenter サーバーの Hosts（ホスト）および Cluster（クラスター）セクションでファイアウォールあるいは Panorama を選択し、**Actions**（アクション） > **Power**（電源）ドロップダウンの順に選択します。



通知を受けたいイベント、あるいは自動アクションを指定したいイベントのアラーム定義を作成します。

アラーム定義を作成する詳細な方法については、VMware ドキュメントをご覧ください。

vCenter サーバーの Hosts（ホスト）および Cluster（クラスター）セクションでファイアウォールあるいは Panorama を選択し、**Manage**（管理） > **Alarm Definitions**（アラーム定義）の順に選択してトリガーを新しく追加し、しきい値に達した際のアクションを指定します。たとえば、一定期間ハートビート通信が無かった場合や、メモリ リソースの使用量が一定のしきい値を超えた場合などです。次のスクリーン ショットは、ファイアウォールあるいは Panorama 上のハートビート モニタリングについての通知を扱う方法を示しています。



ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用

同種のCPU設定を持つESXiホスト間で、vMotionを使ってVMware ESXi上のVM-Seriesファイアウォールを移動する際に、トラフィックフローを維持するためには、vMotion中にPAN-OS CLIを使ってVM-Seriesファイアウォールの内部ハートビートを一時停止する必要があります。ハートビートのモニタリングを一時停止する時間（分）を指定することができます。ハートビートのモニタリングは、最大60分間停止できます。一時停止期間が過ぎた、または強制的に一時停止を中断した場合、ハートビートモニタリングが再開されます。

©2023 Palo Alto Networks, Inc.

VM-SeriesファイアウォールのvMotionは、vSphere 6.5、6.7、および7.0でサポートされています（ESXiホストが同種のCPU設定を保有している場合）。

*vSphere 7.0*以降を実行している場合、*vMotion*の使用時にこれらのコマンドは必要ありません。

STEP 1 | VM-SeriesファイアウォールCLIにログインします。

STEP 2 | 次のコマンドを使って、ハートビートモニタリング一時停止間隔を設定します。一時停止はコマンドを実行すると即座に開始されます。vMotionに予想以上の時間がかかっている場合、新たにより長い間隔でこのコマンドを再実行することができます。この場合も、コマンド実行後即座に一時停止が開始されます。

```
request system heartbeat-pause set interval <一時停止期間（分）>
```

一時停止の残り時間は、次のコマンドで参照することができます。

```
request system heartbeat-pause show interval
```

STEP 3 | （任意）一時停止期間が経過する前にvMotionが完了した場合、期間に0を設定して一時停止を終了することができます。

```
request system heartbeat-pause set interval 0
```

ESXi 上での VM-Series CLI を使用した管理インターフェースのスワップ

デフォルトでは、VM-Series ファイアウォールは最初のインターフェース（eth0）を管理インターフェースとして割り当てます。ただし、デプロイメントによっては、最初のインターフェースをパブリック IP アドレスに事前にマッピングする必要があります。したがって、管理インターフェースを別のインターフェースに割り当てる必要があります。管理インターフェースにパブリック IP アドレスを割り当てることには、セキュリティ上のリスクがあります。

この手順には、VM-Series プラグイン 2.0.7 以降が必要です。

または、ブートストラップ時にInit-cfg.txt ファイルのコンポーネントの一部として管理インターフェースのスワップを有効にすることもできます。

STEP 1 | VM-Series ファイアウォールの CLI にログインし、次のコマンドを入力します。

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 確定してインターフェイスをスワップし、eth1 データプレーン インターフェイスを管理インターフェイスとして使用します。

STEP 3 | ファイアウォールを再起動してスワップを反映させます。以下のコマンドを使用します。

```
request restart system
```

STEP 4 | インターフェイスがスワップされたことを確認します。以下のコマンドを使用します。

```
debug show vm-series interfaces all
```


©2023 Palo Alto Networks, Inc.

```
Phoenix_interface   Base-OS_port   Base-OS_MAC         PCI-ID
       Driver
mgt(interface-swap) eth0   0e:53:96:91:ef:29   0000:00:04.0
  ixgbevf
Ethernet1/1           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0
  ixgbevf
```


©2023 Palo Alto Networks, Inc.

vCenter 上の VM 監視

VMware vCenter 用 Panorama プラグインをインストールし、このプラグインが vCenter 環境でゲストの IP アドレスを取得し、その情報に基づいてダイナミック アドレス グループを使用してポリシーを作成するように設定します。

VMware vCenter 用 *Panorama* プラグインでは、プロキシ サーバーはサポートされていません。

- VMware vCenter での VM モニタリングについて
- VMware vCenter 用 Panorama プラグインのインストール
- VMware vCenter 用 Panorama プラグインの設定

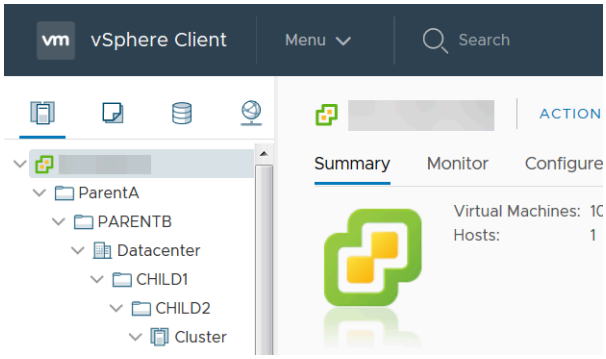
VMware vCenter での VM モニタリングについて

VMware vCenter 用 Panorama プラグインは、ダイナミック アドレス グループを使用して vCenter 環境のポリシーを作成するツールを提供します。ダイナミック アクセス グループを使用して、ゲストの追加または削除などの、環境内の変更に自動的に対応するポリシーを作成できます。VMware vCenter プラグインは vCenter 環境で変更を監視し、変更に関する情報を Panorama と共有します。

このプラグインは、vCenter から受信した情報を処理して Panorama の一連のタグに変換します。これらのタグは、IP アドレスをダイナミック アドレス グループに割り当てるときの一致条件として使用できます。各タグには、VM の上にある階層構造を表すプレフィックスが存在しています。

この例でPanorama の各タグは、以下のプレフィックスで開始しています。各タグには、vCenter 名、データ センター名、およびクラスタ名が含まれています。vCenter 階層構造にフォルダが存在している場合、タグにはフォルダ名が含まれます。タグ内のオブジェクトの順序は、vCenter 階層構造内の順序と一致しています。

vcenter.<vcenter-name>_ParentA_ParentB_Datacenter_CHILD1_CHILD2_Cluster_<tag>



VMware vCenter 用 *Panorama* プラグインでは、*vApps* またはリソース プールに関連付けられているタグはサポートされていません。

Panorama ではタグは次の形式で表示されます。

©2023 Palo Alto Networks, Inc.

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vmname.<vm-name>**—このタグは VM 名に基づいて仮想マシンの IP アドレスをマップします。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>**—このタグはゲスト オペレーティング システムに基づいて、仮想マシンの のIP アドレスをマップします。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>**—このタグはアノテーションに基づいて、仮想マシンの のIP アドレスをマップします。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>**— このタグは、VLAN ID に基づいて仮想マシンの IP アドレスをマップします。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>**—このタグはホスト IP アドレスに基づいて、仮想マシンの のIP アドレスをマップします。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>**—このタグは vCenter で作成されたユーザー定義のタグに基づいて、仮想マシンの のIP アドレスをマップします。

> このプラグインでは *VM* あたり最大 *16* 個のユーザー定義タグがサポートされています。*16* 個を超えるユーザー定義タグは処理されません。

vCenter 用 Panorama プラグインは、128 文字よりも長いタグは処理できません。この文字数には、文字、数字、特殊文字が含まれます。vCenter オブジェクト名内の空白文字は、スラッシュで置換されます。また、Panorama では vCenter VM 名とアノテーションでの非 ASCII 特殊文字、特殊文字 **'<>&"** の使用はサポートされていません。サポートされていない文字を含むタグは破棄されます。

エンドポイントの IP アドレスからタグへのマッピング情報を取得するには、仮想環境の vCenter ごとにモニタリング定義を設定する必要があります。モニタリング定義では、Panorama が vCenter に接続するために必要なユーザー名とパスワードが指定されます。また、デバイス グループと、Panorama がタグをプッシュするファイアウォールを含む対応通知グループも指定されます。モニタリング定義の設定が完了し、VMware vCenter 用 Panorama プラグインがタグを取得したら、DAG を作成し、タグを一致条件として追加できます。

VMware vCenter 用 Panorama プラグインのインストール

vCenter でのエンドポイント モニタリングを開始するため、VMware vCenter 用 Panorama プラグインをダウンロードしてインストールします。

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。HA ペアの Panorama にプラグインをインストールする際は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

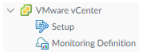
STEP 1 | **Panorama** > **Plugins**（プラグイン）を選択します。

STEP 2 | **Upload**（アップロード）を選択し、**Browse**（参照）をクリックしてプラグイン ファイルを見つけます。

STEP 3 | **OK** をクリックしてアップロードを完了します。

©2023 Palo Alto Networks, Inc.

STEP 4 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。



VMware vCenter 用 Panorama プラグインの設定

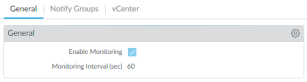
プラグインのインストールが完了したら、以下の手順に従って Panorama と vCenter 間の接続を確立します。

vCenter 環境で仮想マシンをモニタリングするプラグインの場合、VMware ツールがすでにインストールされています。vCenter では VM の IP アドレスを外部から取得できません。これらのアドレスは、VMware ツールでのみ確認できます。さらに、プラグインが vCenter から IP アドレス情報を取得するには、ネイティブの読み取り専用許可が必要です。

STEP 1 | Panorama Web インターフェイスにログインします。

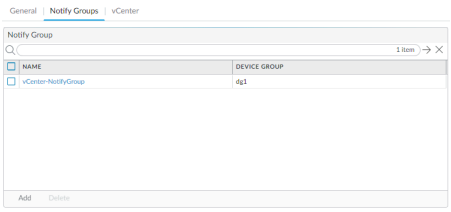
STEP 2 | モニタリングを有効にして、モニタリング間隔を設定します。

1. **Panorama** > **VMware vCenter** > **Setup**（セットアップ） > **General**（全般）を選択します。
2. **Enable Monitoring**（モニタリングの有効化）を選択します。これにより、デプロイメント内のすべての vCenter のモニタリングが有効になります。
3. **Monitoring Interval**（モニタリング間隔）を秒単位で設定します。モニタリング間隔は、Panorama が vCenter から最新のネットワーク情報を取得する頻度です。デフォルト値は 60 秒で、60～84600 秒の範囲で指定できます。



STEP 3 | 通知グループを作成します。

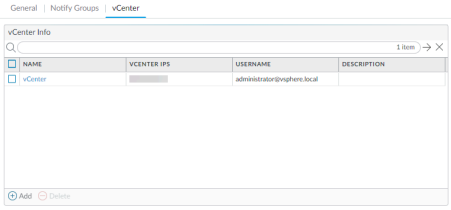
1. **Panorama** > **VMware vCenter** > **Setup**（セットアップ） > **Notify Groups**（通知グループ）を選択します。
2. **Add**（追加）をクリックします。
3. **Name**（名前）に通知グループの分かりやすい名前を入力します。
4. vCenter デプロイメントのデバイス グループを選択します。



©2023 Palo Alto Networks, Inc.

STEP 4 | vCenter 情報を追加します。VMware vCenter 用 Panorama プラグインでは最大 16 個の vCenter インスタンスがサポートされています。

1. **Panorama** > **VMware vCenter** > **Setup**（セットアップ） > **vCenter**を選択します。
2. **Name**（名前）に分かりやすい vCenter 名を入力します。
3. vCenter の IP アドレスまたは FQDN を入力し、該当する場合はポートも入力します。
4. vCenter ユーザー名を入力します。
5. vCenterC パスワードを入力して確認します。
6. **Validate**（検証）をクリックして、Panorama が入力した認証情報を使って vCenter に接続できることを確認します。
7. **OK** をクリックします。



STEP 5 | 最大 16 個のモニタリング定義を設定します。

1 つの vCenter インスタンスは、1 つの Monitoring Definition（モニタリング定義）にのみ割り当てることができます。

1. **Panorama** > **VMware vCenter** > **Monitoring Definition**（モニタリング定義）を選択し、**Add**（追加）をクリックします。
2. この定義を使用する vCenter を識別する**Name**（名前）、および任意で説明を入力します。
3. **vCenter** および **Notify Group**（通知グループ）を選択します。
4. **OK** をクリックします。



STEP 6 | 変更を **Commit (コミット)** します。

©2023 Palo Alto Networks, Inc.

STEP 7 | Panorama 上で VM 情報を閲覧できることを確認し、ダイナミック アドレス グループ用の一致条件を定義します。

一致条件で複数のタグを使用する場合は *OR* 演算子を使用する必要があります。*AND* 演算子を使用すると機能しません。

一部のブラウザ拡張機能が、*Panorama* と *vCenter* の間の *API* コールをブロックすることがあります。これが原因で、*Panorama* は一致条件を受信できなくなります。ブラウザ拡張機能を使用しているときに *Panorama* で一致条件が表示されない場合は、その拡張機能と *Synchronize Dynamic Objects*（動的オブジェクトの同期）を無効にして、*Panorama* に対して使用可能なタグを取り込みます。

STEP 8 | VM のアドレスが DAG に追加されていることを確認します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. DAG の Addresses（アドレス）列で **More**（すべて表示）をクリックします。

   Panorama に、指定した一致条件に基づいて DAG に追加された IPアドレスのリストが表示されます。

STEP 9 | ポリシー内でダイナミック アドレス グループを使用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **[追加]** をクリックし、ポリシーの **[名前]** および **[説明]** を入力します。
3. **Source Zone (送信元ゾーン)** を追加して、トラフィックの送信元となるゾーンを指定します。
4. トラフィックが終端する **Destination Zone (宛先ゾーン)** を追加します。
5. **Destination Address (宛先アドレス)** については、先ほど作成したダイナミック アドレス グループを選択します。
6. トラフィックに対するアクション（**[許可]** または **[拒否]**）を指定し、必要に応じてデフォルト セキュリティ プロファイルをルールに関連付けます。
7. 手順 1～6 を繰り返し、もう 1 つポリシー ルールを作成します。
8. **Commit**（コミット）をクリックします。

STEP 10 | vCenter から動的オブジェクトをいつでも更新できます。更新するには、動的オブジェクトを同期します。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キ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有効化することができます。

1. **Panorama** > **VMware vCenter** > **Monitoring Definition**（モニタリング定義）を選択します。
2. **Synchronize Dynamic Objects**（動的オブジェクトを同期）をクリックします。

STEP 11 | vCenter デプロイメントのファイアウォールが再起動し、Panorama から切断されると、そのファイアウォールが vCenter 用 Panorama プラグインと同期していない状態になり、最新

©2023 Palo Alto Networks, Inc.

情報を受信しなくなります。ファイアウォールが Panorama に再接続したら、Panorama とファイアウォールを手動で同期する必要があります。

1. Panorama CLI にログインします。
2. 以下のコマンドを実行します。

   ```
   admin@Panorama> request plugins vmware_vcenter sync
   ```


©2023 Palo Alto Networks, Inc.

ESXi のデプロイメントのトラブルシューティング

VM-Series ファイアウォールのトラブルシューティング手順の多くは、ハードウェア バージョンの PAN-OS の場合とよく似ています。問題が発生したら、インターフェイス カウンターやシステム ログ ファイルを調べ、必要な場合にはデバッグを使用してキャプチャを作成してください。

以下のセクションでは、いくつかの一般的な問題のトラブルシューティング方法について説明します。

- 基本的なトラブルシューティング
- インストールの問題
- ライセンスの問題
- 接続の問題

基本的なトラブルシューティング



ネットワーク トラブルシューティング ツールの推奨

仮想環境でトラフィックをキャプチャしたり、テスト パケットを挿入したりするために、別々のトラブルシューティング ステーションがあると役立ちます。*tcpdump*、*nmap*、*hping*、*traceroute*、*iperf*、*tcpedit*、*netcat* などの一般的なトラブルシューティング ツールがインストールされた新規 *OS* を最初から作成することも有効です。このマシンは、パワーダウンしてテンプレートに変換することができます。ツールが必要になるたびにトラブルシューティング クライアント（仮想マシン）を問題の仮想スイッチにすばやくデプロイし、それを使用してネットワーク問題を分離することも可能です。テストが完了するとインスタンスは破棄され、テンプレートは次に必要になったときにまた使用されます。

ファイアウォールでのパフォーマンス関連の問題の場合は、まず、そのファイアウォールの Web インターフェイスから **Dashboard** をチェックします。アラートを表示したり、テクニカル サポート（TS）ファイルや Stats Dump ファイルを作成するには、**Device**（デバイス） > **Support**（サポート）の順に移動します。

詳細については、vSphere クライアントで**Home**（ホーム） > **Inventory**（インベントリ） > **VMs and Templates**（仮想マシンおよびテンプレート）の順に移動し、VM-Series ファイアウォールのインスタンスを選択して **Summary**（サマリー）タブをクリックします。**Resources**（リソース）の下で、消費メモリ、CPU、およびストレージの統計情報を確認します。リソース履歴の場合は、**Performance**（パフォーマンス）タブをクリックし、時間経過によるリソース消費量をモニターします。

インストールの問題

- OVA のデプロイに関する問題
- ファイアウォールがメンテナンス モードで起動するのはなぜですか?
- VM-1000-HV 用に基本イメージ ファイルを変更するには?

©2023 Palo Alto Networks, Inc.

OVA のデプロイに関する問題

- VM-Series は、Open Virtualization Alliance（OVA）形式の zip アーカイブとして提供され、3 つのファイルに展開されます。

  OVA イメージのデプロイに問題がある場合は、3 つのファイルが展開され、アクセス可能であることを確認してください。必要に応じて、OVA イメージを再度ダウンロードして解凍します。
- OVA イメージの仮想ディスクは約 1GB です。vSphere クライアントを実行しているコンピュータに存在する必要があります。または、OVA イメージの URL としてアクセス可能である必要があります。
  - vSphere クライアント コンピュータとターゲット ESXi ホスト間のネットワーク接続が、待ち時間と十分な帯域幅を持つことを確認します。接続が不十分な場合は、OVA のデプロイメントに何時間もかかるか、タイムアウトして失敗する可能性があります。

    ESXi ホストと同じネットワーク上のデバイスにイメージをホストする場合は、この問題を最小限に抑えることができます。
  - パス上にあるすべてのファイアウォールは、vSphere から ESXi ホストまでTCPポート 902 および 443 を許可する必要があります。
- ESX 6.5.0a ビルド 4887370 では、ソケットあたり 2 つの CPU コアに制限されます。ソケットあたり 2 つ以上の vCPU を割り当てる VM-300、VM-500、または VM-700 をデプロイする場合は、回避策として、VMware KB：https://kb.vmware.com/s/article/53354 を参照してください。

ファイアウォールがメンテナンス モードで起動するのはなぜですか?

VM-1000-HV ライセンスを購入し、VMware ESXi サーバー上で VM-Series ファイアウォールをスタンドアロン モードでデプロイしている場合、VM-Series ファイアウォールで求められる最小メモリを割り当てる必要があります。

メンテナンス モード中のブートが発生しないようにするには、基本イメージファイルを変更するか（「VM-1000-HV 用に基本イメージ ファイルを変更するには?」参照）、ESXi ホストまたは vCenter サーバーの設定を VM-Series ファイアウォールの電源を入れる前に編集する必要があります。

インターフェイスが「VMXnet3」であることを確認します。インターフェイスの種類を他の形式に設定すると、ファイアウォールはメンテナンス モードで起動します。

VM-1000-HV 用に基本イメージ ファイルを変更するには?

VM-1000-HVライセンスを購入し、VMware ESXiサーバー上でVM-Seriesのファイアウォールをスタンドアロン モードでデプロイしている場合、VM-Seriesファイアウォールの基本イメージファイル（.ovaまたは.xva）で定義される以下の属性を手順に従って変更します。

重要:ここに記載されている値以外の値を変更すると、基本イメージファイルが無効になります。

STEP 1 | 基本イメージ ファイル（7.0.0 など）をメモ帳などのテキスト エディタで開きます。

 ©2023 Palo Alto Networks, Inc.

STEP 2 | 以下に示すように、4096 を探し、割り当てメモリを 5012（5 GB）に変更します。

```
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>4096MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>4</rasd:ResourceType>
        <rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
<Item>
        <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
        <rasd:Description>Memory Size</rasd:Description>
        <rasd:ElementName>5120MB of memory</rasd:ElementName>
        <rasd:InstanceID>2</rasd:InstanceID>
        <rasd:ResourceType>5</rasd:ResourceType>
        <rasd:VirtualQuantity>5120</rasd:VirtualQuantity>
```

STEP 3 | 割り当て仮想 CPU コアの数を 2 から、デプロイに適切な 4 または 8 に変更します。

```
<Item>
        <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
        <rasd:Description>Number of Virtual CPUs</
rasd:Description>
        <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
        <rasd:InstanceID>1</rasd:InstanceID>
        <rasd:ResourceType>3</rasd:ResourceType>
        <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
        <vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket>
      </Item>
<Item>
        <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
        <rasd:Description>Number of Virtual CPUs</
rasd:Description>
        <rasd:ElementName>4 virtual CPU(s)</rasd:ElementName>
        <rasd:InstanceID>1</rasd:InstanceID>
        <rasd:ResourceType>3</rasd:ResourceType>
        <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
        <vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket>
      </Item>
```

または、ファイアウォールをデプロイし、VM-Series ファイアウォールをパワーオンする前に ESXi ホストまたは vCenter サーバーでメモリと CPU の割り当てを直接編集することもできます。

ライセンスの問題

- サポート ライセンスまたは機能ライセンスを適用できないのはなぜですか?
- コピーした VM-Series ファイアウォールに有効なライセンスがないのはなぜですか?
- VM-Series ファイアウォールを移動するとライセンスは無効になりますか?

©2023 Palo Alto Networks, Inc.

サポート ライセンスまたは機能ライセンスを適用できないのはなぜですか?

VM-Series ファイアウォールにキャパシティ認証コードを適用していない可能性があります。サポート ライセンスまたは機能ライセンスのアクティベーション前に、デバイスがシリアル番号を取得できるようにするためにキャパシティ認証コードを適用する必要があります。このシリアル番号は、VM-Series ファイアウォールのその他のライセンスのアクティベーションに必要です。

コピーした VM-Series ファイアウォールに有効なライセンスがないのはなぜですか?

VMware は、VM-Series ファイアウォールを含む各仮想マシンに一意の UUID を割り当てます。そのため、VM-Series ファイアウォールをコピーすると、新しい UUID がそのコピーに割り当てられます。VM-Series ファイアウォールの各インスタンスのシリアル番号とライセンスは UUID に関連付けられているため、ライセンスされた VM-Series ファイアウォールをコピーすると、新しいファイアウォールのライセンスは無効になります。新しくデプロイされたファイアウォールのライセンスをアクティベーションするには、新しい認証コードが必要です。VM-Series ファイアウォールで完全な機能、サポート、およびソフトウェア アップグレードを使用できるようにするには、キャパシティ認証コードおよび新しいサポート ライセンスを適用する必要があります。

VM-Series ファイアウォールを移動するとライセンスは無効になりますか?

ホスト間でVM-Series ファイアウォールを手動で移動する場合は、オプション **This guest was moved**（このゲストは移動しました） を選択してライセンスが無効化されないようにしてください。

接続の問題

- VM-Series ファイアウォールがネットワーク トラフィックを受信しないのはなぜですか?

VM-Series ファイアウォールがネットワーク トラフィックを受信しないのはなぜですか?

VM-Series ファイアウォールで、トラフィック ログ（**Monitor**（監視） > **Logs**（ログ））を確認します。ログが空の場合、以下の CLI コマンドを使用して、VM-Series ファイアウォールのインターフェイスにパケットを表示します。

```
show counter global filter
delta yes
Global counters:
Elapsed time since last sampling: 594.544 seconds
------------------------------------------------------------------------------
Total counters shown: 0
------------------------------------------------------------------------------
```

vSphere 環境では、以下の問題を確認します。

©2023 Palo Alto Networks, Inc.

- ポート グループを確認し、ファイアウォールと仮想マシンが正しいポート グループにあることを確認する

  インターフェイスが正しくマッピングされていることを確認します。

  Network adapter 1 = management

  Network adapter 2= Ethernet1/1

  Network adapter 3= Ethernet1/2

  各仮想マシンの設定で、インターフェイスが正しいポート グループにマッピングされていることを確認します。
- 各ポート グループまたはスイッチ全体で、無差別モードが有効になっているか、ファイアウォールがハイパーバイザによって割り当てられた MAC アドレスに設定されていることを確認します。

  データプレーンの PAN-OS MAC アドレスは vSphere で割り当てられる vNIC MAC アドレスとは異なるため、ハイパーバイザによって割り当てられた MAC アドレスの使用が有効化されていない場合、ポートグループ（または vSwitch 全体）が無差別ポートである必要があります。

  - vSphere で VLAN 設定を確認する

    vSphereポートグループのVLAN設定には2つの意味があります。どのポートグループがLayer 2ドメインを共有するか、そしてアップリンクポートにタグ付け（802.1Q）がされるか否かを決定します。
  - 物理スイッチのポート設定を確認する

    アップリンク ポートを含むポート グループで VLAN ID が指定されている場合、vSphere は 802.1Q を使用してアウトバウンド フレームにタグを付けます。タグは物理スイッチの設定と一致する必要があります。一致しない場合、トラフィックは通過しません。

    分散仮想スイッチ（vDS）を使用している場合、ポート統計を確認します。標準スイッチではポート統計は提供されていません。

©2023 Palo Alto Networks, Inc.

VM-Series for ESXi のパフォーマンス調整

ESXi 用の VM-Series ファイアウォールは、高パフォーマンスのアプライアンスですが、最良の結果を得るには、ハイパーバイザの調整が必要な場合があります。このセクションでは、VM-Series ファイアウォールが最高のパフォーマンスを発揮するためのベスト プラクティスと推奨事項について説明します。パフォーマンスを最大限に引き出すには、ESXi 6.0.0.0 以降が推奨されます。

- ESXi 上の NIC ドライバのインストール
- ESXi 上の DPDK の有効化
- ESXi 上の SR-IOV の有効化
- SR-IOV による ESXi VLAN アクセスモードの有効化
- ESXi 上の NIC のマルチキュー サポートの有効化
- パフォーマンスのためのVNFチューニング

ESXi 上の NIC ドライバのインストール

最高のパフォーマンスを得るには、SR-IOV を Intel 10GB ネットワーク インターフェイスと併用してください。この場合は、各インターフェイスで複数のキューをサポートするために ixgbe 4.4.1 ドライバが必要です。

STEP 1 | ESXi ホスト上のネットワーク インターフェイスのリストを取得します。

1. ESXi ホストの CLI にログインします。
2. 以下のコマンドを使用してネットワーク インターフェイスのリストを取得します。

```
$ esxcli network nic list
```

STEP 2 | 特定のインターフェイスのドライバ バージョンを決定します。

ethtool または **esxcli** を使用して、現在インストールされているドライバのバージョンを決定できます。以下の例では vNIC4 を使用しており、3.21.6 というドライバ バージョンが返されています。

- ethtool—**ethtool -l *<nic-name>***

```
$ ethtool -I vNIC4
driver: ixgbe
version: 3.21.6iov
firmware-version: 0x80000389
bus-info: 0000:04:00.0
```

- esxcli—**esxcli network nic get -n *<nic-name>***

```
$  esxcli network nic get -n vNIC4
   Advertised Auto Negotiation: true
   Advertised Link Modes:
```


©2023 Palo Alto Networks, Inc.

```
Auto Negotiation: true
Cable Type:
Current Message Level: 7
Driver Info:
      Bus Info: 0000:04:00.0
      Driver: ixgbe
      Firmware Version: 0x80000389
      Version: 3.21.6iov
Link Detected: false
Link Status: Down
Name: vNIC4
PHYAddress: 0
Pause Autonegotiate: true
Pause RX: true
Pause TX: true
Supported Ports: FIBRE
Supports Auto Negotiation: true
Supports Pause: true
Supports Wakeon: false
Transceiver: external
Wakeon: None
```

STEP 3 | 新しいドライバをインストールします。

1. VMware の Web サイトから ixgbe 4.4.1 ドライバをダウンロードします。コンテンツをローカル ディレクトリに抽出し、ドライバ用の .zip あるいは .vib ファイルを探します。
2. ESXi ホスト データストア内に新規フォルダを作成します。
3. 抽出したローカルの .zip あるいは .vib ファイルを、ESXi ホスト データストア内の新規フォルダにコピーします。
4. ESXi ホストでメンテナンス モードを有効化します。
5. 次のいずれかのコマンド（.zip ファイルの場合は -d、.vib ファイルの場合は -v）を使用し、新しいドライバをインストールします。

   - **$ esxcli software vib install -d *<path to driver .zip file>***
   - **$ esxcli software vib install -v *<path to driver .vib file>***

   .zip あるいは .vib ファイルの完全パスを指定する必要があります。例:

   ```
   $ esxcli software vib install -d  "/vmfs/volumes/
   Datastore/DirectoryName/DriverName.zip"
   ```

6. VIB インストレーションを確認します。

   ```
   $ esxcli software vib list
   ```

7. ESXi ホストを再起動します。

©2023 Palo Alto Networks, Inc.

ESXi 上の DPDK の有効化

データ プレーン開発キット（DPDK）を利用すると、ネットワークインターフェースカード（NIC）パケットの処理速度が向上するため、VM-Series のパフォーマンスが向上します。VM-Series ファイアウォールでは、ESXi で DPDK はデフォルトで有効になっています。

DPDK の利点を活かすには、「DPDK ドライバーのバージョン」に記載されているいずれかの DPDK ドライバーで、NIC を使用する必要があります。

DPDK を無効にすると、NIC は DPDK の代わりに PacketMMap を使用します。DPDK は、**set system setting dpdk-pkt-io off** コマンドを使用して無効にできます。

ESXiハイパーバイザーサポートと、PAN-OSバージョンごとのPacketMMAPおよびDPDKドライバーサポートについては、互換性マトリックスを参照してください。

ESXi 上の SR-IOV の有効化

Single Root I/O Virtualization（SR-IOV）を使用すると、1 つのルート ポートの 1 つの PCIe 物理デバイスを、ハイパーバイザーやゲストに対して複数の個別の物理デバイスのように見せかけることができます。SR-IOV NIC で仮想機能デバイスを有効にして SR-IOV を有効にし、vCenter でゲスト設定を変更します。

VM-Series for ESXi上のSR-IOVには、PacketMMAPドライバのバージョンに記載されているいずれかのIntel NICドライバが必要です。PAN-OSバージョンごとのSR-IOV と DPDKドライバーのサポートについては、互換性マトリックスを参照してください。

ESXiでSR-IOVを有効にするには、2種類の方法があります。

- **SR-IOV**パススルー—この方法では、SR-IOV NIC上で仮想ファンクションデバイスを有効にして、vCenterでゲスト設定を変更し、SR-IOV VFインターフェイスをアダプタタイプ「SR-IOV passthrough」として追加します。「仮想ファンクションをSR-IOV Passthrough Adapterとして仮想マシンに割り当てる」を参照してください。

  PAN-OS 8.1.2以降で優先されるこの方法では、SR-IOV PFをvSwitchまたはDvSwitchに追加することができます。

- **PCI**アダプタ—PAN-OS 8.0～8.1.1の場合、この方法が必要でした。『8.1デプロイガイド』の「ESXiでのSR-IOVの有効化」から、PCIアダプタのワークフローを参照することができます。

  PCIアダプタを利用する方法には、SR-IOVを有効にする物理ポート上でvSwitchを設定できない制限があります。VM-Series ファイアウォールが、ネットワーク上のホストまたは他の仮想マシンと通信できるように、インターフェイス上の物理ポートおよび関連する仮想ファンクション（VF）への排他的アクセスが必要になります。「vSphere WebクライアントでのPCIデバイスの追加」を参照してください。

SR-IOV による ESXi VLAN アクセスモードの有効化

ESXi 上の VM-Series ファイアウォールは、VLAN アクセスモードで動作して、マルチテナントクラウド/データセンター環境でサービスとしてのセキュリティを提供する仮想ネットワーク機能（VNF）としてデプロイされるユースケースをサポートできます。VLAN アクセスモードでは、各 VNF に各ネットワーク専用の仮想ネットワークインターフェイス（VNI）があり、VLAN タグなしで SR-IOV 仮想機能（VF）との間でパケットを送受信します。 ホストハイパーバイザーの

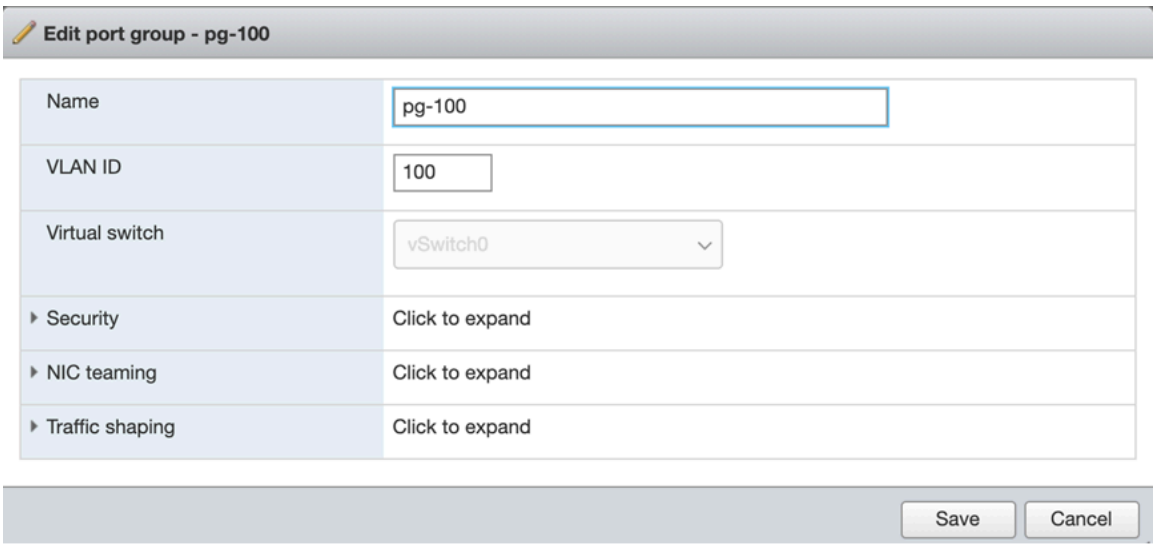
©2023 Palo Alto Networks, Inc.

物理機能と仮想機能でこの機能を有効にする必要があります。次に、VM-Series ファイアウォールで VLAN アクセスモードを有効にすると、ファイアウォールは、すべてのデータプレーンインターフェイスで VLAN タグなしでトラフィックを送受信できます。さらに、QoS ポリシーを構成すると、ファイアウォールはアクセスインターフェイスに QoS を適用し、マルチテナント展開でトラフィックの差別化された処理を提供できます。

デフォルトでは、*ESXi* の *VM-Series* ファイアウォールは *VLAN* トランクモードで稼働します。

STEP 1 | ホストシステムで、VLAN アクセスモードで動作するように物理機能と仮想機能をセットアップします。

1. VMware Host Client インベントリでネットワークをクリックし、ポートグループをクリックします。
2. 編集したいリストで、ポートグループを右クリックし、[設定の編集] を選択します。新しいポートグループの名前を入力します。**VLAN ID**の新しい値を入力します。



VM-Series のファイアウォールで最高のパフォーマンスを得るには、次のことを確認してください。

- *CPU* ピニングを有効にします。
- *IPSec*トンネルを構成している場合は、リプレイ保護を無効にします。

  ファイアウォールの *Web* インターフェースで、ネットワーク > ***IPSec*** トンネル を選択し、*IPSec* トンネルを選択して*[*全般*]*をクリックし、*[*詳細オプションの表示*]*を選択し、 *[*リプレイプロテクションを有効にする*]*をオフにします。

STEP 2 | VM-Series のファイアウォールでCLIにアクセスします。

©2023 Palo Alto Networks, Inc.

STEP 3 | VLANアクセスモードを有効にします。

```
request plugins vm-series vlan-mode access-mode on
```

VLAN アクセスモードを有効 にし、VLAN トランクモードを使用して **request plugins vm-series vlan-mode access-mode off**を入力します。

STEP 4 | ファイアウォールを再起動します。

```
request restart system
```

STEP 5 | VLANモードの設定を確認します。

```
show plugins vm-series vlan-mode
```

ESXi 上の NIC のマルチキュー サポートの有効化

マルチキューにより、vCPU の数に合わせてネットワークのパフォーマンスを高めることができ、複数の TX および RX キューを作成して並列パケット処理を実現できます。マルチキューを有効にするには、.vmx ファイルを変更するか、Advanced Settings（詳細設定）にアクセスします。

STEP 1 | マルチキューを有効にします。

1. .vmx ファイルを開きます。
2. 以下のパラメータを追加します。

```
ethernetX.pnicFeatures = “4”
```

STEP 2 | Receive-Side Scaling（RSS）を有効にします。

1. ESXi ホストで CLI にログインします。
2. 以下のコマンドを実行します。

```
$ vmkload_mod -u ixgbe
$ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

STEP 3 | 最大のパフォーマンスを実現するには、ethernet/vSwitch デバイスごとに追加の CPU スレッドを割り当てます。この場合、ESXi ホストで利用可能なスペアの CPU リソースの量による制限があります。

1. .vmx ファイルを開きます。
2. 以下のパラメータを追加します。

```
ethernetX.ctxPerDev = “1”
```

パフォーマンスのためのVNFチューニング

このトピックは、VM-Seriesデプロイメント用のVNFチューニングに関するガイダンスを提供しています。VM-Seriesデプロイメントのいくつかのパラメータ設定の選択に役立つ参考情報を取

©2023 Palo Alto Networks, Inc.

り上げています。チューニングを行う前に、チューニングパラメータや属性の設定方法を含めて、VM-SeriesファイアウォールをVMware vSphereハイパーバイザーにインストールする手順を理解しておく必要があります。

このガイダンスは、*SD-WAN*、*MSSP*、または*CSSP*などの使用事例を対象にした、ホワイトボックス/グレイボックス環境における*VM-Series*デプロイメントには当てはまらない場合があります。

VM-Seriesは高性能アプライアンスで、プライベートまたはパブリッククラウドにおけるサイズ、ハイパーバイザーのフットプリント、デプロイ場所などに応じて、さまざまなフォームファクタで利用することができます。

グローバルレベルおよびホストレベルの設定の変更は、同じホスト上で動作している他のVMに影響を与えます。さまざまなトレードオフを考慮して、デプロイ環境に最適のパラメータを身長に選択する必要があります。

- ESXiチューニングパラメータ
- ユースケース
- 参考資料

ESXiチューニングパラメータ

VM-Seriesで最高のパフォーマンスを引き出すために、ハードウェア、ハイパーバイザー、およびネットワークI/Oパラメータをチューニングすることができます。

ここに記載しているパラメータは、すべてのデプロイメントモデルに適用されるものではありません。

- BIOS設定
- 物理設定
- 仮想NIC設定
- NUMAとリソースの検討事項

BIOS設定

このセクションは、VM-Seriesファイアウォールのパフォーマンスを強化できる可能性がある、BIOS Power Management（BIOS電源管理）、Hyperthreading（ハイパースレッディング）、およびIntel VT-D設定の推奨事項、およびサンプルのBIOS設定について取り上げています。

- 電源管理
- ハイパースレッディング
- Intel Virtualization Technology for Directed I/O
- サンプルのBIOS設定

電源管理

遅延時間に敏感なアプリケーションの場合、アイドル状態のシステム（各種節電モードのいずれか）が外部イベントに応答する際のパスに、何らかの形式の電源管理機能が遅延時間を増加

©2023 Palo Alto Networks, Inc.

させてしまいます。VMwareはBIOSの電源管理を「static high performance（スタティックハイパフォーマンス）」（OS制御の電源管理なし）に設定し、アクティブな形式の電源管理を無効にすることを推奨しています。Intel Nehalem クラス以降の CPU (Intel Xeon 55xx 以降) を搭載したサーバーには 、C ステートとインテル ターボ・ブーストの 2 つの電源管理オプションがあります。

C-statesを有効にしたまま放置すると、メモリーの遅延時間が増加するため、低遅延時間のワークロードにはお勧めできません。C1Eとして知られている拡張型のC-stateの場合でも、CPUがホルト（アイドル）状態からフルパワー状態に回復するまでの遅延時間が長くなります。VMwareはBIOSでC1Eを無効にして、遅延時間を低減することを推奨しています。

- HPの場合、Power Regulator ModeをStatic High Modeに設定して、QPI Processor、C-state Support、およびC1E Supportを無効にします。
- Dellの場合、Power Management Mode、CPU Power、およびPerformance ManagementをMaximum Performanceに設定します。

他にも検討する必要があるパラメータとして、P-stateがあります。パフォーマンスの観点からは、BIOSのP-state設定を無効にしてください。

Intel Turbo Boostは、時間の経過に伴うパフォーマンスの変動につながる可能性があります。一貫して確実なパフォーマンスを維持するには、Turbo Boostを無効にしてください。

ハイパースレッディング

ハードウェアおよびBIOSがハイパースレッディングをサポートしている場合、ESXiはホスト上で自動的にハイパースレッディングを有効にします。VM-Seriesファイアウォールで最高のパフォーマンスを引き出すために、ESXiホストのハイパースレッディングを無効にしてください。

デプロイ環境がハイパースレッディングの有効化を保証している場合は、VM-Seriesファイアウォールのすべてのリソースが、PCIデバイスにアクセスできる同じNUMA/Socketノードにより予約されていることを確認してください。

一般的には、PA-VMを単一のNUMA VMとして設定してください。詳細については、「NUMAとリソースの検討事項」を参照してください。

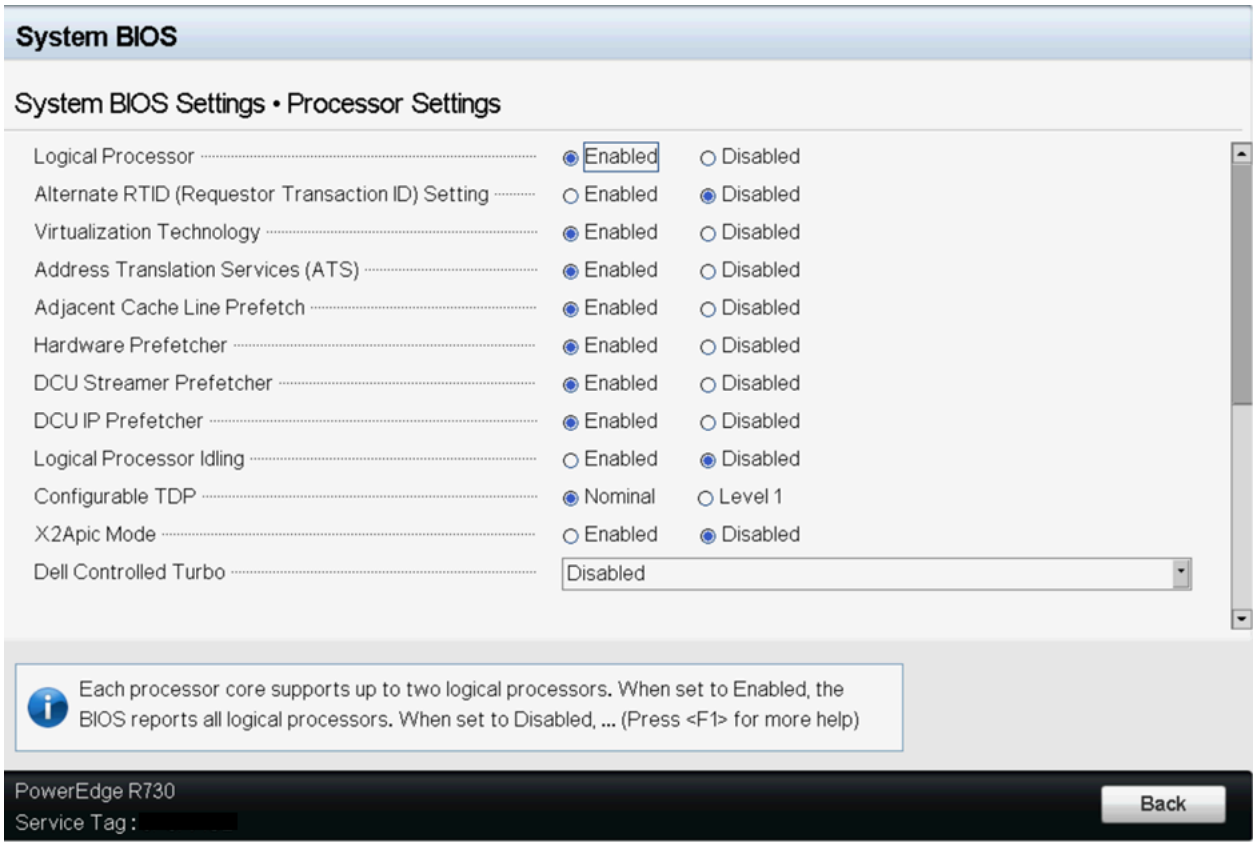
Intel Virtualization Technology for Directed I/O

Intel Virtualization Technology for Directed I/O（Intel VT-D）により、LANカードをゲストシステム専用にして、エミュレートされたLANカードを超えるネットワークパフォーマンスの向上を実現することができます。この機能はBIOSで有効にします。パフォーマンスのためにSR-IOVを活用する場合（推奨）、SRI-OVのBIOS設定を有効にします。

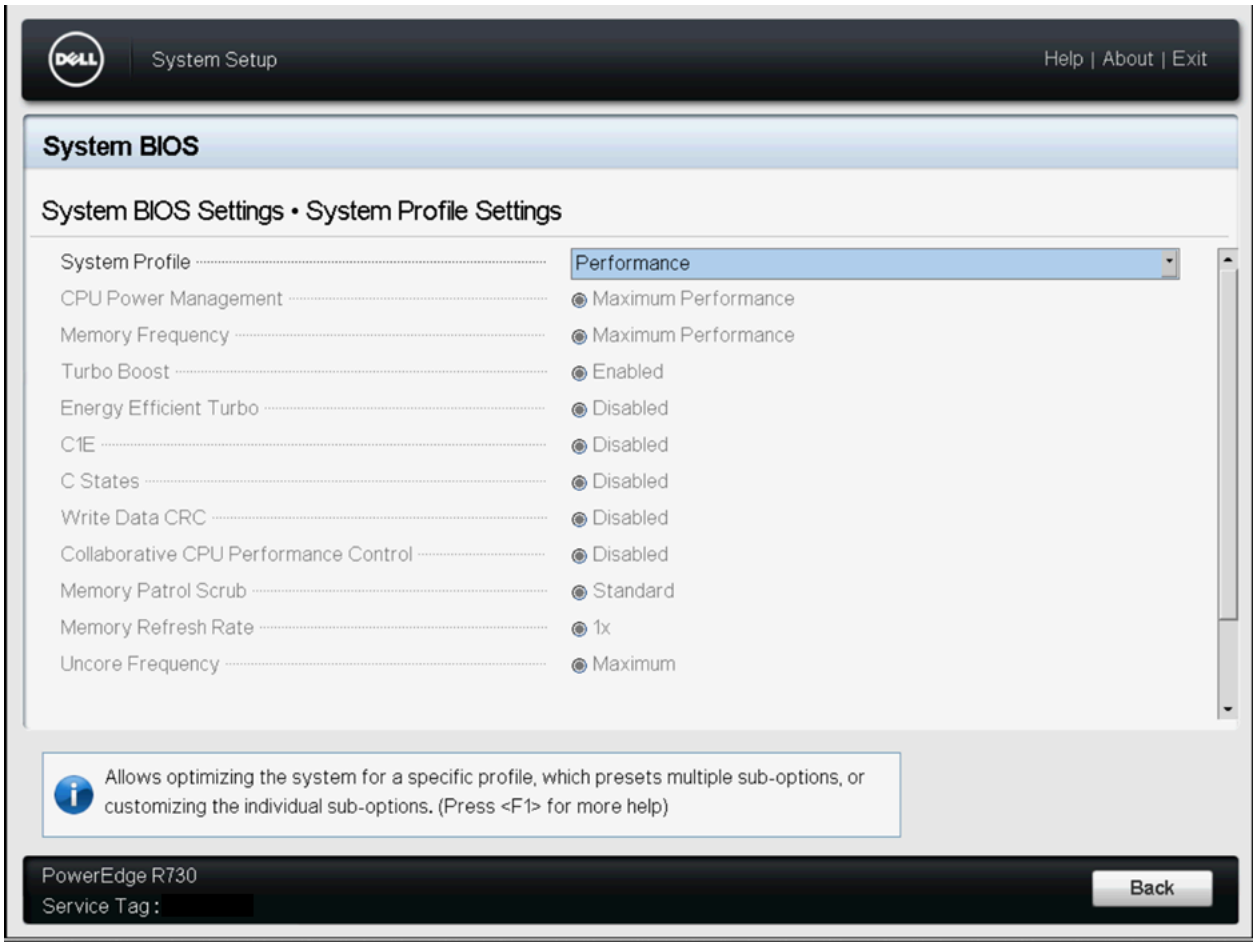
サンプルの**BIOS**設定

Dell BIOS用のシステムプロファイル設定とプロセッサ設定を、次のスクリーンショットに示します。

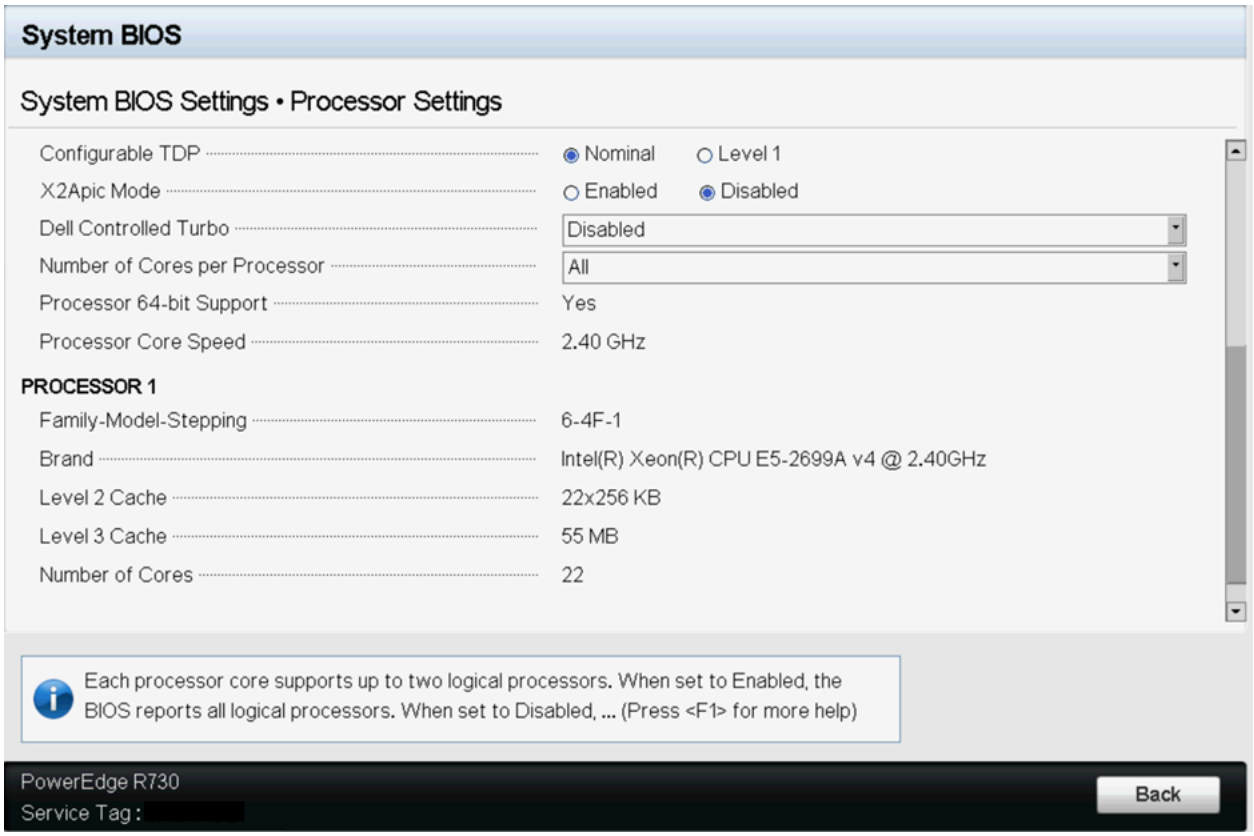
 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.



物理設定

大部分の1GbEまたは10GbEネットワークインターフェイスカード（NIC）は、 () Interrupt Moderation（割り込みモデレーション）またはInterrupt Throttling（割り込みスロットリング）と呼ばれる機能をサポートしています。この機能は、NICからホストへの割り込みをまとめて、ホストが処理に圧倒されて、すべてのCPUサイクルを割り込み処理に費やすことを防止することを目的にしています。ただし、遅延時間に敏感なワークロードの場合、NICが受信パケットまたは正常に回線上に送信されたパケットに対する中断の配布を遅らせている時間は、ワークロードの遅延時間を増やす時間となってしまいます。PA-VMで最高のパフォーマンスを達成するために、Interrupt Moderationを無効にしてください。たとえば、ESXiホスト上の物理NICのInterrupt Moderationを、次のように無効にします:

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0"
```

- 伝送キュー
- キューのペアリング

伝送キュー

ESXiアップリンクpNICレイヤーは、伝送のためにキューに格納されたパケットのソフトウェアTxキューも管理しています。このキューはデフォルトで、500パケットを格納します。ワークロードがI/Oを集中的に消費し、伝送パケットの大規模なバーストが発生する場合、このキューのオーバーフローが発生し、アップリンクレイヤーでパケットが破棄される可能性があります。次のESXiコマンドを使って、Txキューサイズを最大10,000パケットまで増やすことができます:

 ©2023 Palo Alto Networks, Inc.

```
# esxcli system settings advanced set -i 10000 -o /Net/
MaxNetifTxQueueLen
```

物理NICと特定のバージョンのESXiドライバがESXiホスト上で利用されているかどうかに応じて、pNICの伝送リングが小さすぎるためすぐに満杯になり、pNICドライバでパケットが破棄されることがあります。大部分のpNICドライバでは、次のコマンドを使って伝送リングのサイズを増やすことができます:

```
# ethtool -G vmnic0 tx 4096
```

このコマンドは、Txリングサイズを4096エントリに増やします。特定のpNICドライバに設定できる最大サイズ、および現在有効なTxリングサイズは、次のコマンドを使って確認できます:

```
# ethtool -g vmnic0
```

```
Ring parameters for vmnic0:

Pre-set maximums:
RX: 4096
RX Mini: 0
RX Jumbo: 0
TX: 4096
Current hardware settings:
RX: 512
RX Mini: 0
RX Jumbo: 0
TX: 4096
```

キューのペアリング

IntelのixgbeやBroadcomのbnx2xなど、一部のpNICドライバは、「キューのペアリング」もサポートしています。キューのペアリングは、ペアリングされた伝送キューの伝送されたパケットの完了処理も、受信スレッド（NetPoll）が行うことを、ESXiアップリンクレイヤーに示しています。特定の伝送量が多いワークロードの場合、これにより伝送完了処理に遅延が生じて、vNICの伝送リングに他のパケットを伝送するための余地がなくなり、ゲストOS内のvNICドライバがパケットを破棄しなければならなくなる可能性があります。

ESXiホスト上のすべてのpNICのキューペアリングを無効にすると、pNIC伝送完了を処理するための個別のスレッドが作成されます。その結果、完了はタイムリーに処理されて、vNICの伝送リング内に追加のパケットを伝送するための空きスペースを確保できます。

キューのペアリングを無効にするESXiコマンドを次に示します:

```
# esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable
  -i 0
```

これを有効にするためには、ESXiホストを再起動する必要があります。

©2023 Palo Alto Networks, Inc.

*VM-700*で*PCI*パススルーが専用ホスト上で使用されている場合、*NIC/NIC*ドライバのパフォーマンスチューニングは必要ありません。ただし、このデプロイメントモードは一般的ではありません。

仮想**NIC**設定

次のトピックで説明しているように、可能な場合はSR-IOVを使用してより良いパフォーマンスを実現してください。

- SR-IOV
- VMXNET3/vSwitchおよびVirtual Interrupt Coalescing
- Intel x710/x520上でのマルチキューサポートの有効化

SR-IOV

- SR-IOVドライバのモジュールパラメータを変更する場合、ESXiホストを再起動する必要があります。
- ESXiホスト上の物理NICのInterrupt Moderationを、次のように無効にします:

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0“
```

- マルチキューサポートを有効にする場合、ドライバのReceive-Side Scaling（RSS）も有効にする必要があります。
  - RSSを有効にするには、ポートの値を4に設定してください。
  - ポートはカンマ区切り文字列で指定します。

  例:3つのNICにそれぞれ2つのポートを設定。

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m
 ixgbe
  -p RSS=”4,4,4,4,4,4”
```

```
$ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

  例:単一のポートにRSSを設定:

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m
 ixgbe
  -p RSS=”0,4,0,0,0,0”
```

VMXNET3/vSwitchおよび**Virtual Interrupt Coalescing**

デフォルトで、VMXNET3はInterrupt Coalescingアルゴリズムをサポートしています（物理NICがInterrupt Moderationを実装しているのと同じ理由）。ホストシステムへの大量の割り込みの殺到を回避するために、複数のパケットが収集されて、単一の割り込みが生成されます。この処理は、Interrupt Coalescingと呼ばれています。

©2023 Palo Alto Networks, Inc.

Interrupt Coalescenceは、ネットワークインターフェイスが受信するトラフィック量、またはトラフィックを受信した後、ハード割り込みを発行するまでに経過した時間を表しています。即座の割り込み、または頻繁な割り込みは、ハードウェアからの割り込み要求を処理するために、カーネルが実行中のタスクを停止（または「中断」）してしまうため、システムのパフォーマンスが低下してしまいます。割り込みが遅すぎる場合、トラフィックがNICからすぐに出て行かないと、他の多数のトラフィックが到着して、カーネルによる受信待ちのトラフィックが上書きされてしまい、トラフィックが失われてしまう可能性があります。vSphere Web Clientでこの機能を無効にするには、**VM Settings**（**VM**設定） > **Options**（オプション） > **Advanced General**（詳細な全般） > **Configuration Parameters**（設定パラメータ）に移動して、**`ethernetX.coalescingScheme`**のエントリとして値**`disabled`**を追加します。

ホスト上でVirtual Interrupt Coalescingを無効にするには（遅延に敏感なVMだけでなくすべてのVMに影響）、高度なネットワーキングパフォーマンスオプションを設定します。**Configuration**（設定） > **Advanced Settings**（高度な設定） > **Net**に移動して、**`CoalesceDefaultOn`**に**`0`**（無効）を設定します。

Intel x710/x520上でのマルチキューサポートの有効化

ESXi 6.0.0以降と、マルチキューをサポートしているバージョンのixgbeドライバを使用します。互換性マトリックスの、「SR-IOVドライバのバージョン」を参照してください。マルチキューサポートを有効にするには、**`.vmx`**ファイルを変更するか、A**dvanced Settings**（詳細設定）にアクセスします。

```
ethernetX.pnicFeatures = “4”
```

vSwitchが300K PPSを超えられるようにマルチコアアフィニティを設定するには、次のように設定します:

```
ethernetX.pnicFeatures = "4"
ethernetX.ctxPerDev = "1"
```

`ethernetX.ctxPerDev = “1”`の設定は、バイナリフラグのようなものです（有効にするには1を設定）。このバイナリフラグは、ポート **`ethernetX`**からのトラフィックのみを処理するように、CPUスレッドを追加します。これにより、トラフィックスケジューリングのパフォーマンスが改善します。

NUMAとリソースの検討事項

NUMAはNon-Uniform Memory Accessの省略形です。マルチコアプロセッサは葉複雑なデザインとなっています。そのようなシステムのパフォーマンス上の問題に取り組むためには、NUMAsCPUビニングのニュアンスをすべて理解しておく必要があります。確認しておくべき重要な事柄:

- 私達のスレッドが動作しているコアは？（ハイパースレッディングが有効になっている場合は、ハイパースレッディングを確認）
- 私達のvCPUが動作しているコアは？（アフィニティ）
- 物理NICカードがインストールされているNUMAソケットは？

©2023 Palo Alto Networks, Inc.

- メモリーはどこに割り当てられているのか？（NUMA効果）

  任意のソケットで動作しているスレッドは単一の統合されたメモリー空間を参照するため、他のソケットにローカルなメモリーに読み取り/書き込みを行えます。
- メモリーは、ノード上の異なるソケット間で共有されているか？
- ローカルメモリーにアクセスするよりも、異なるソケットのメモリーにアクセスするには、より多くの時間がかかります。

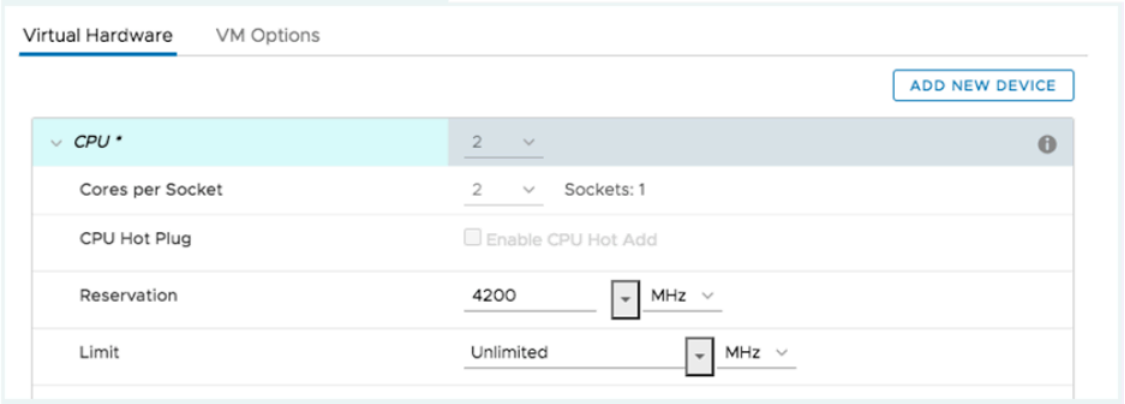
  NUMA効果は、スレッドが他のNUMAドメインにあるメモリーに過度にアクセスしている場合に発生します。NUMA間の問題を防止するために、ソケット0通信とソケット1間のQuick Pathインターコネクト（QPi）を回避するようにしてください。

PA-VMなどの遅延時間に敏感なVMのために、VMwareはESXiホスト上の物理CPU（プロセッサ）数と比べて、vCPUをオーバーコミットしないことをお勧めします。たとえば、ホストにCPUコアが8つある場合、VMのvCPU数を7に制限してください。そうすることで、ESXi VMkernelスケジューラは、他のスケジューリングコンテキスト（他のVMまたはESXiヘルパーワールドからのvCPUなど）と競合しないpCPUにvCPUを配置する機会が増加します。VMに割り当てるvCPU数が、VM内のアクティブなCPUを消費するプロセスまたはスレッド数を超えないようにすることをお勧めします。

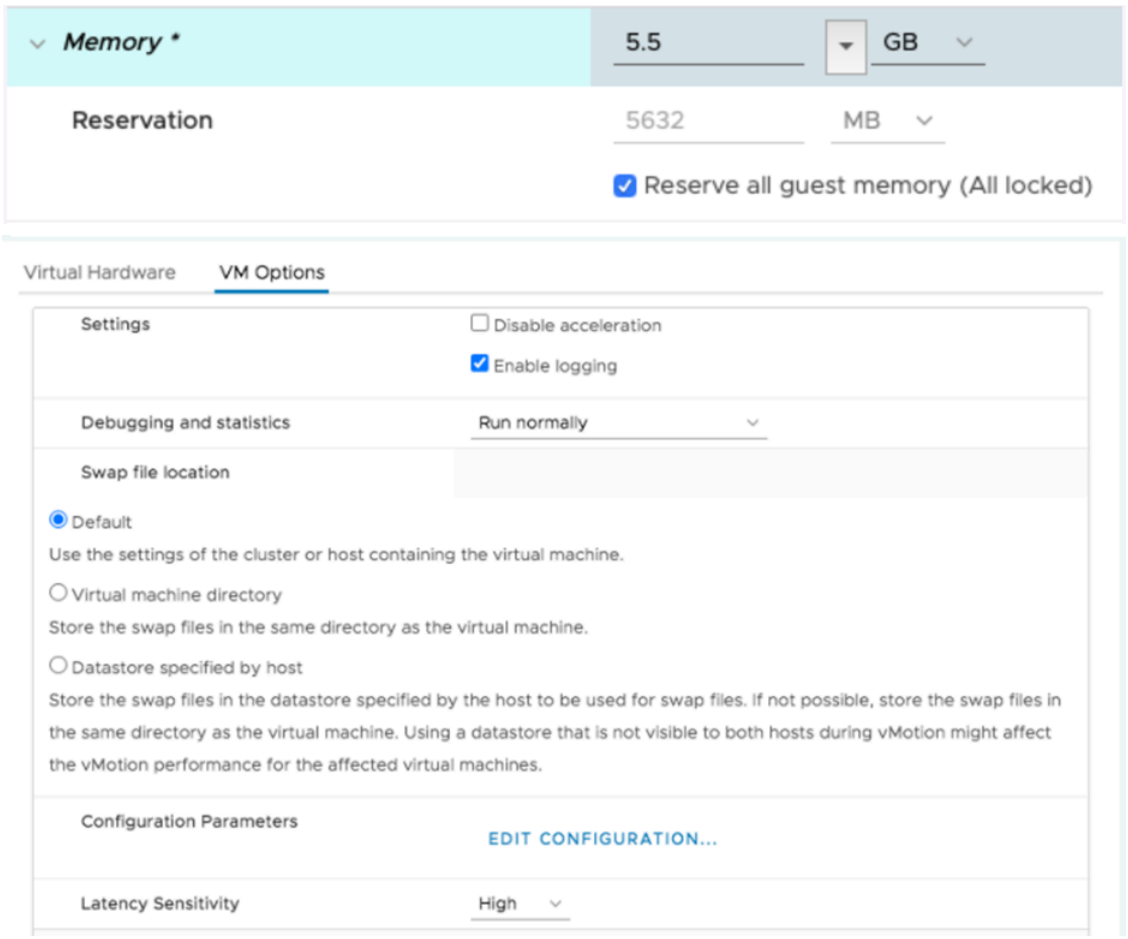
最高のパフォーマンスを実現するために、すべてのvCPUを同じNUMAノード上でスケジュールして、すべてのVMメモリーをそのNUMAノードにアタッチされているローカル物理メモリーから適用し、割り当てるようにしてください。これは、VM設定**numa.nodeAffinity=0, 1, …**を使って変更できます。ここで、0, 1,...はソケット番号を表しています。

VMがCPUリソースに排他的にアクセスできるように、Latency Sensivity（遅延時間感度）をHigh（高）に設定してください。新しい設定を有効にするには、VM CPU予約をmaximum（最大）に設定し、Memory（メモリー）を予約して、CPU limit（CPU制限）をunlimited（無制限）に設定する必要があります。

- 新しいバージョンでは、vSphere Web Clientを使ってVM Latency Sensitivity（VM遅延時間感度）オプションをHigh（高）に設定してください（デフォルトはNormal（標準））。
- 古いバージョンの場合は、**sched.cpu.latencySensitivity**をHigh（高）に設定してください。

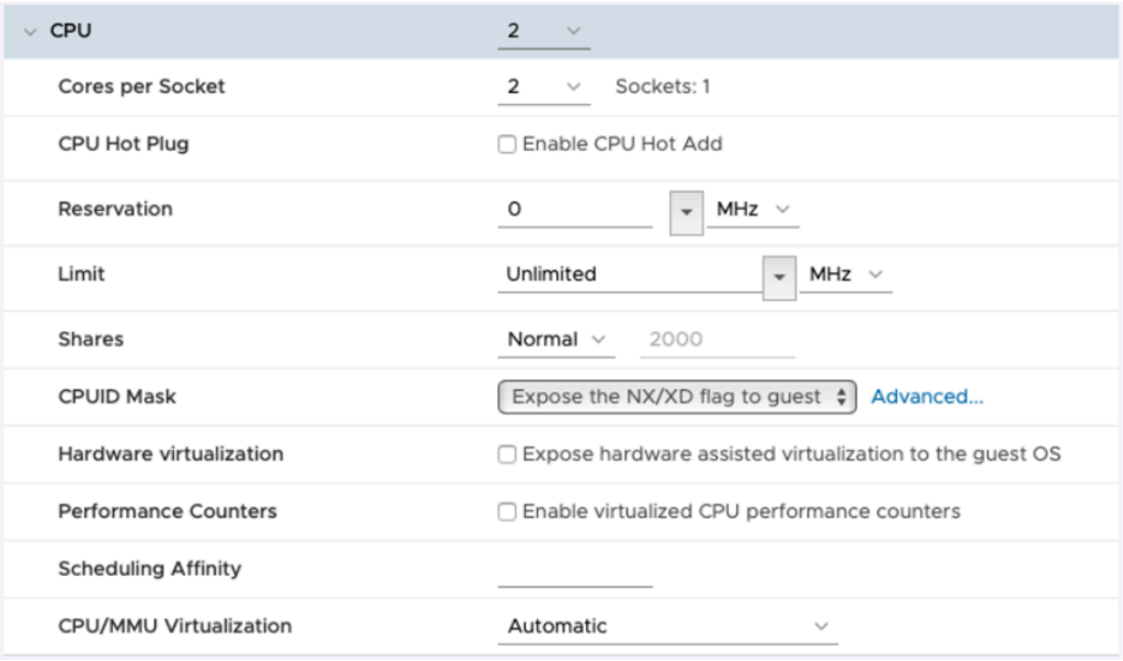


 ©2023 Palo Alto Networks, Inc.



また、VM設定の**Host Affinity**（ホストアフィニティ）を使ってVMのvCPUをホストCPUコアに固定して、別のコアにスケジュールされないようにすることも可能です。Host Affinity（ホストアフィニティ）を使用する際には、NUMAとハイパースレッディングのことを忘れないようにしてください。システムがオーバーコミット状態の場合は、Host Affinity（ホストアフィニティ）を設定しないでください。詳細については、「CPUアフィニティに関する潜在的な問題」を参照してください。

©2023 Palo Alto Networks, Inc.



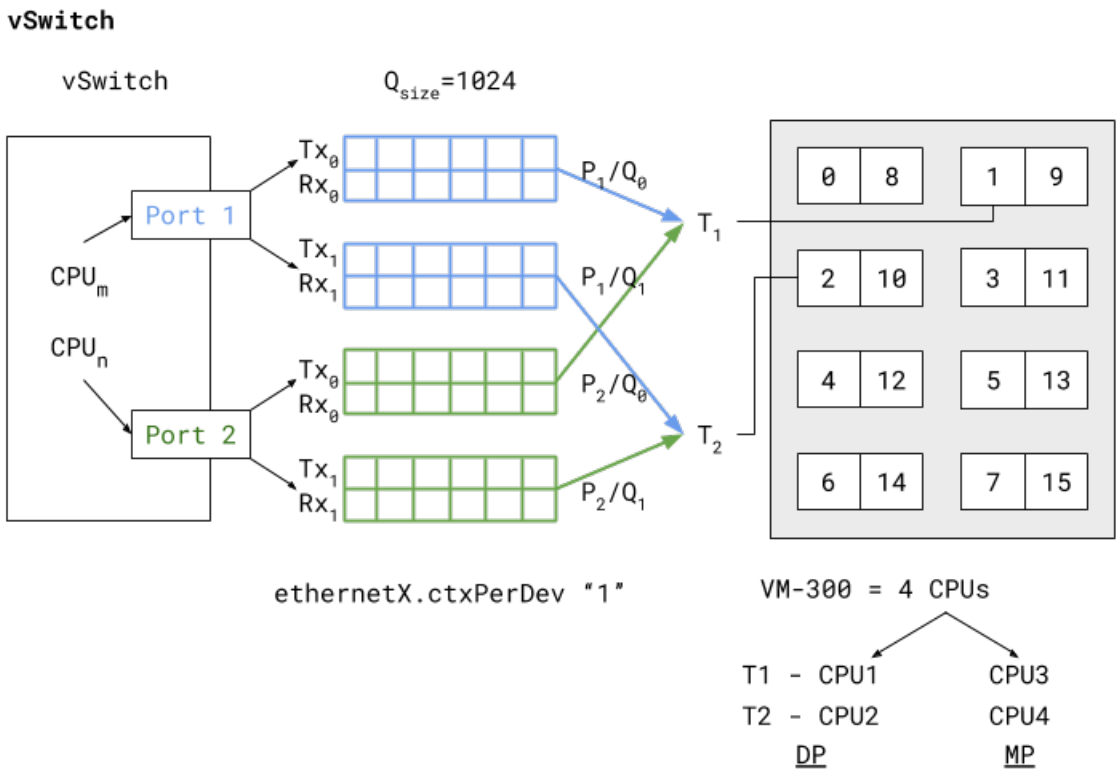
チューニングパラメータを実装したら、esxtopまたはCPUチャートを使って、VMのCPU Ready（%RDY）およびCo Stop（%CSTP）を確認してください。CPUリソースへの排他的アクセスを確実にするために、両方とも0%に近い値でなければなりません。esxtopを使ってNUMAの使用状況を確認して、VMのメモリーリソースがNUMAノード全体に拡散しないようにすることも可能です。詳細は、「esxtop統計情報の解釈」を参照してください。

ユースケース

ユースケース**1: vSwitch**デプロイメント

次の図は、ESXiホスト上へのPA-VMのデプロイメントを表しています。ここで、データポート「Port 1」および「Port 2」は、PA-VMのeth1とeth2にリンクしています。各ポートは2つのキューペア（例:Tx0/Rx0、およびTx1/Rx1）を提供しているか、またはマルチキューが有効になっています。

©2023 Palo Alto Networks, Inc.



複数のキューと送受信されるロードバランシングパケットに対してマルチキューとRSSを有効にすることで、処理パフォーマンスを強化できます。vCPUからポート/キューへのマッピング（この例の場合）の内部ロジックに基づいて、P1/Q0およびP2/Q0に到着する、またはそこから送信されるパケットは、vCPU1上で動作する（固定されている）データプレーンタスクT1により処理されます。データプレーンタスクT2も、上記のvSwitchデプロイメントの図のように、同じような関係で処理が行われます。

2つのデータプレーンタスクはvCPU1およびvCPU2で動作しており、これらのCPUはハイパースレッディングで同じコアを共有しません。つまり、ハイパースレッディングが有効になっていても、ハイパフォーマンスを保つためにタスク割り当てを異なるコアに固定できます。また、これらのデータプレーンタスクvCPUは、NUMAに関係するパフォーマンス上の問題を回避するために、すべて同じNUMAノード（またはソケット）に所属しています。

キューサイズを増やし、ポートとやり取りするトラフィックをスケジュールするポートに、専用のvCPUまたはスレッドを割り当てることで、その他2つのパフォーマンス上のボトルネックに対処することができます。キューサイズ（Qsize）を増やすことで、大量のトラフィックの突然のバーストに対処して、バーストが発生しやすいトラフィックにおけるパケットの破棄を防止することができます。ポートレベルのパケット処理に専用のCPUスレッド（**ethernetX.ctxPerDev = 1**）を追加することで、トラフィックを高い効率で処理することができ、トラフィックのスループットを増やしてラインレートに到達することができます。

PA-VMパケット処理テクニックは、パフォーマンスも決定します。これは、DPDKまたはPacketMMAPに設定できます。DPDKはポーリングモードドライバ（ドライバタイプによる）を使って、キューで受信されたパケットを継続的にポーリングします。これにより、高いスループットパフォーマンスを実現できます。ポーリング期間に影響するのは、パケットにより観測される遅延時間です。ポーリングが継続的に行われる場合（PAN-OS CLIから設定をbusy-poll）、データプレーンタスクのvCPU使用状況は100%になりますが、最高のパフォーマンスを生み出せ

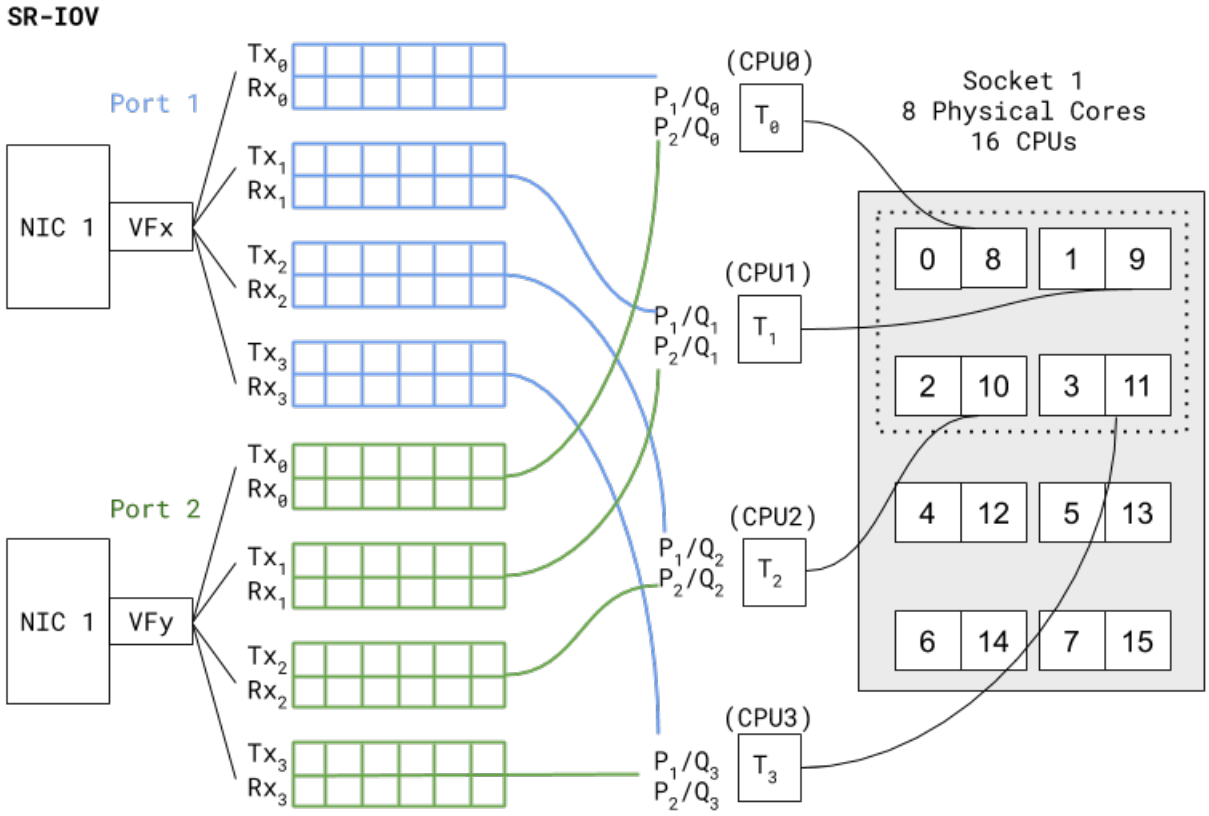
©2023 Palo Alto Networks, Inc.

ます。内部的にソフトウェアは、無駄なCPUリソースの使用を防止するために、ミリ秒レベルのポーリング時間を使用しています。

一方でPacketMMAPはDPDKよりもパフォーマンスは低いですが、任意のネットワークレベルドライバで利用することができます。DPDKの場合、vSwitchドライバはDPDKをサポートしている必要があります。PacketMMAPは、ポートがパケットを受信して、それを受信キューに保管した時に生成される割り込みに対応できます。つまり、各パケットまたはパケットのグループに対して、割り込みが生成され、パケットは処理のために受信キューから取り出されます。そのためパケット処理の遅延時間は低くなりますが、割り込みを毎回処理する必要があり、CPUのオーバーヘッドが高くなるため、スループットが減少します。一般的にPacketMMAPはDPDK（busy poll変更なし）よりもパケット処理の遅延時間が小さくなります。

ユースケース**2**：**SR-IOV**デプロイメント

以下のSR-IOVの図は、vSwitchのユースケースに類似のPAVMデプロイメントを表していますが、SR-IOVモードになっています。



SR-IOVで、互換性のある物理NICポート（Physical Function（物理機能））は、基本的に葉複数のインターフェイス（Virtual Functions（仮想機能））に分割されています。上記の図でNIC1 Port1は、PAVMデータプレーンインターフェイス（例:eth1）の1つとして関連付けられている、VFXと言う名前のVFが存在しています。Port2 VFからPAVM eth2へも、似たような関連付けが作成されています。パケット処理のチェーンは、vSwitch環境内のデプロイメントの処理チェーンと類似しています。唯一の違いは、SR-IOV VFドライバは、PAN-OSで使用されているドライバと互換性がなければならないことにあります。また、内部vSwitch（ホスト内）スイッチングトラフィックがないため、ポートからのトラフィックスケジューリング用の専用のスレッドを設定する必要はありません（つまり、この設定で**ethernetX.ctxPerDev = 1**は不要で

©2023 Palo Alto Networks, Inc.

す）。SR-IOVとDPDKのインターフェイスは、vSwitchのユースケースよりも高いパケット処理パフォーマンスを達成することができます。

参考資料

- データ集中型ワークロードのためのVMware vCloud NFVのチューニング
- vSphereでのTelcoおよび NFVワークロードパフォーマンスチューニングのベストプラクティス
- CPUアフィニティに関する潜在的な問題
- esxtop統計情報の解釈

©2023 Palo Alto Networks, Inc.

vCloud Air での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールは vCloud Director ポータルから vCloud Air ポータルを利用するか、vCloud Air API を使用して、vCloud Air の仮想データ センター（vDC）にデプロイできます。

> vCloud Air における VM-Series ファイアウォールについて
> vCloud Air でサポートされるデプロイメント
> vCloud Air での VM-Series ファイアウォールのデプロイ



vCloud Air における VM-Series ファイアウォールについて

vCloud Director ポータル内の vCloud Air ポータルを利用するか、vCloud Air API を使用して、VM-Series ファイアウォールを VMware vCloud Air 内の仮想データセンター（vDC）に導入することができます。また、既存の Panorama を使用するか、新規のPanoramaをオンプレミスまたはvCloud Air 上に導入することで、すべての物理的ファイアウォールとVM-Series ファイアウォールを中央管理することができます。

vCloud Air 上に VM-Series ファイアウォールを導入する際は以下が必要になります。

- ソフトウェアイメージの ESXi バージョンおよびOpen Virtualization Alliance（OVA）ファイルはPalo Alto Networks カスタマーサポートウェブサイトで入手できます。現在、vCloud Air Marketplaceからは入手できません。

  VM-Seriesファイアウォールを効果的に導入するため、vApp内にファイアウォールのソフトウェアイメージを入れておいてください。vAppとは、単一のオブジェクトとして管理される、事前に設定済みのバーチャルアプライアンス（仮想マシンやオペレーティングシステムイメージ）を入れておくための容器です。たとえば、vAppに多層型アプリケーションやVM-Seriesファイアウォールが含まれている場合、vAppを展開するたびに、vAppと共に展開されるVM-SeriesファイアウォールがWebサーバーとデータベースサーバーを自動的に保護します。
- パートナー、販売代理店、あるいはPalo Alto Networksから直接購入したBring Your Own License（BYOL）モデルのライセンスやサブスクリプション（vCloud AirのVM-Seriesでは、従量制ライセンスはお求めいただけません）。
- vCloud Air のセキュリティ制約上の理由から、vCloud Air における VM-Series ファイアウォールはLayer3インターフェイスとともに導入することをお勧めします。この場合、インターフェイスにおいてハイパーバイザから割り当てられた MAC アドレスを使用できるように設定する必要があります。ハイパーバイザから割り当てられた MAC アドレスを有効化していない場合、vCloud Air の vSwitch は無差別モードや MAC に偽装されたデータ送信をサポートしていないため、VMware vSwitch は VM-Series ファイアウォールのデータプレーンインターフェイスへトラフィックを転送することができません。VM-Series ファイアウォールは、タップインターフェイス、レイヤー 2インターフェイス、またはバーチャルワイヤインターフェイスを使用して導入することはできません。

vCloud Air のVM-Series ファイアウォールはアクティブ/パッシブのHA冗長化構成で導入することができます。ただし、vCloud Air のVM-Series ファイアウォールは、vCloud Air 上でホストされている仮想マシンに対するVMモニタリングの機能をサポートしていません。

vCloud Air について詳しく知りたい場合は、VMware vCloud Airのマニュアルを参照してください。

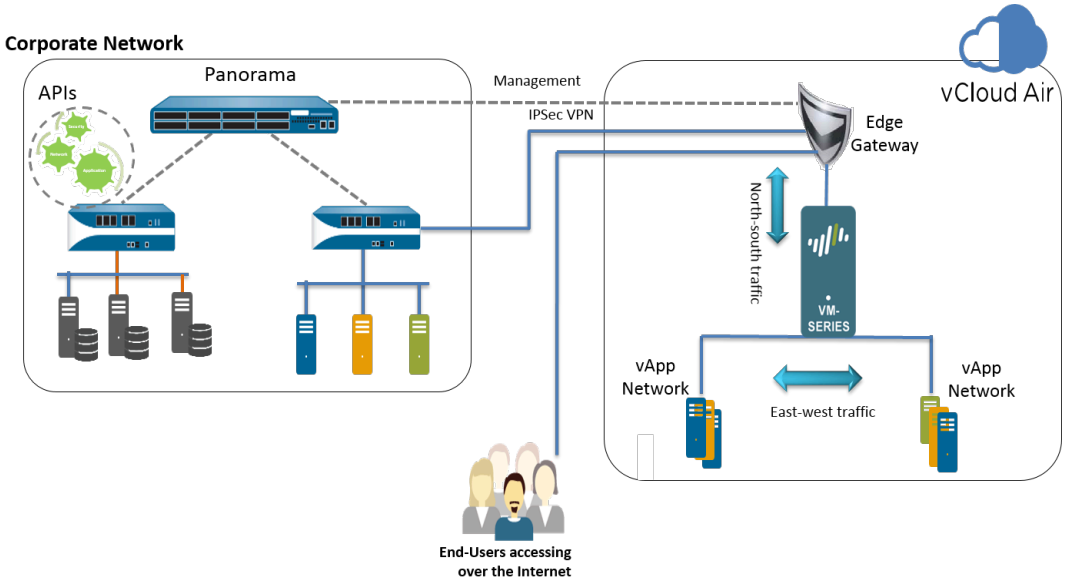
©2023 Palo Alto Networks, Inc.

vCloud Air でサポートされるデプロイメント

アプリケーションを安全に使用し、既知と未知の両方の脅威をブロックし、また、環境の変化への対応をすばやく行うためにも、レイヤー 3 インターフェイスを持つ vCloud Air で、以下のような用途で VM-Series ファイアウォールを導入することができます。

- 仮想データ センターの境界を保護する – VM-Series ファイアウォールを、vCloud Air の隔離ネットワークと経路指定されたネットワークを接続する仮想マシンとして導入します。この導入例では、ファイアウォールが vCloud Air のインフラストラクチャを縦断するすべてのトラフィックを保護します。
- ハイブリッド クラウドを構築する – データ センターとプライベート クラウドを vCloud Air に拡張し、企業ネットワークとデータ センター間の通信に VPN 接続を使用することができます。この導入例において VM-Series ファイアウォールは、トラフィックの暗号化とクラウドへアクセスするユーザーを保護する際に IPSec を使用します。
- **vDC** のアプリケーション サブネット間のトラフィックを保護する – アプリケーションを階層化することでネットワークをセグメント化し、トラフィックを隔離させ、さらに VM-Series ファイアウォールを導入することでサブネットとアプリケーション階層の間の水平方向の脅威から保護し、セキュリティを向上させることができます。

以下の図は、3 つの導入例と Panorama をすべて含んだものです。Panorama は、ポリシー更新の合理化、ポリシーの中央管理、そしてログの記録とレポートの一元化を可能にします。



©2023 Palo Alto Networks, Inc.

vCloud Air での VM-Series ファイアウォールのデプロイ

このセクションに記載されている手順に従い、vCloud Air でオンデマンドあるいは専用 vDC に VM-Series ファイアウォールを導入してください。ここでは、vDC へのトラフィックの出入りに必要なゲートウェイおよび管理トラフィックのルーティングと vDC を通すデータ トラフィックに必要なネットワークの設定を含め、vDC のセットアップが完了していることを前提にしています。

STEP 1 | Palo Alto Networks カスタマー サポート Web サイトから VM-Series の OVA イメージを入手してください（現在、vCloud Air マーケットプレイスからは入手できません）。

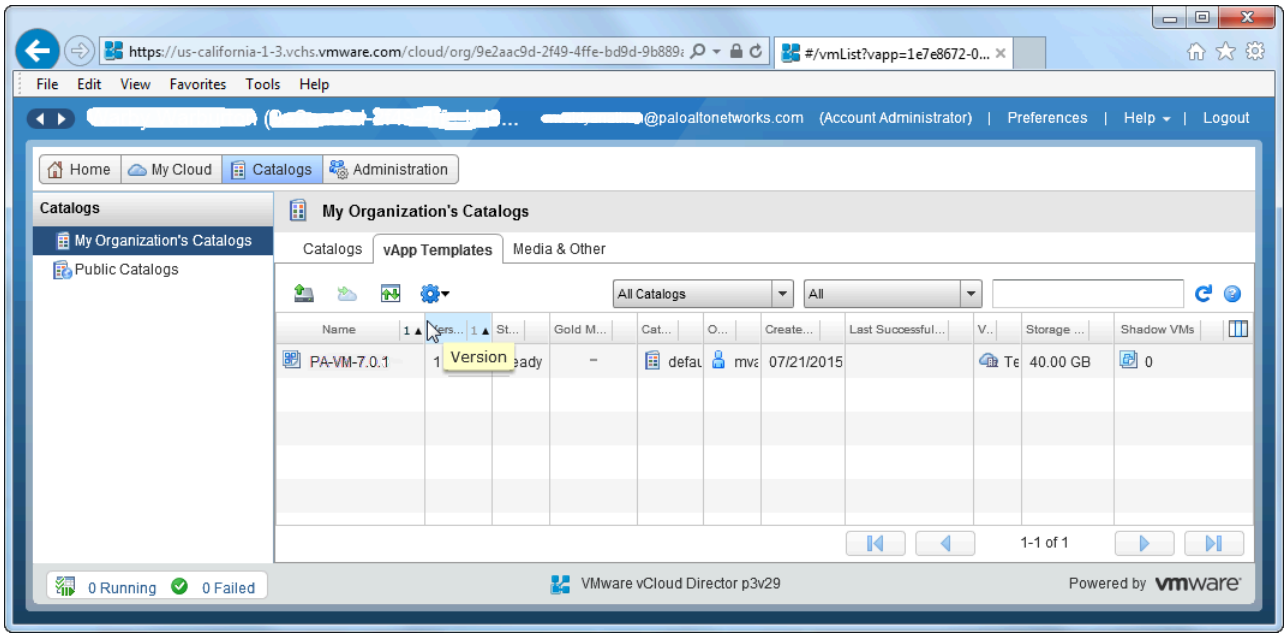
1. www.paloaltonetworks.com/services/support.htmlに移動します。
2. **PAN-OS for VM-Series Base Images** で絞り込みを行い、OVA イメージをダウンロードします。例：PA-VM-ESX-9.1.0.ova

STEP 2 | OVA イメージから Open Virtualization Format（OVF）を抽出し、OVA イメージを vCloud Air カタログへインポートします。

OVA イメージからファイルを抽出する際は、すべてのファイル（.mf、.ovf、.vmdk）を同じディレクトリ内に入れておいてください。

OVAイメージからOVFファイルを抽出する方法については、https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpufにあるVMwareのドキュメントを参照してください。

OVF ファイルのインポートを行う際、VM-Series ファイアウォールのソフトウェア イメージは **My Organization's Catalogs**（組織のカタログ）内にあります。



©2023 Palo Alto Networks, Inc.

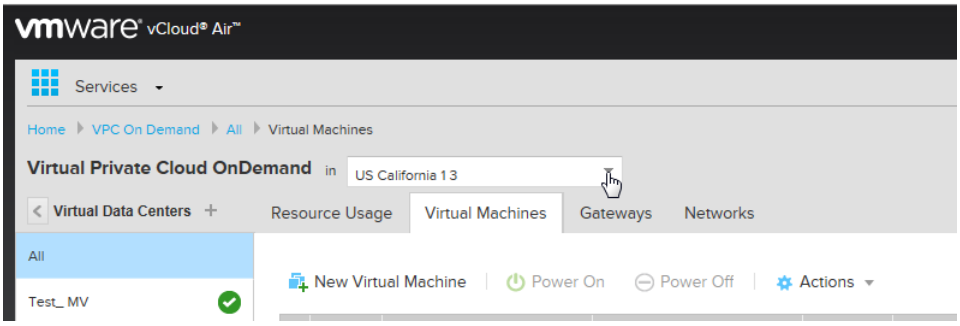
STEP 3 | ワークフローを選択してください。

vApp とは、仮想マシンやオペレーティング システムのイメージを含む、事前に設定済みのバーチャル アプライアンス用のテンプレートを集めたものです。

- VM-Series ファイアウォールを含む新規の vDC と vApp を作成する場合は、ステップ4 へ進んでください。
- vDC をすでにデプロイし、vApp を所持しており、VM-Series ファイアウォールを vApp セキュア トラフィックに追加する場合は、ステップ5へ進んでください。

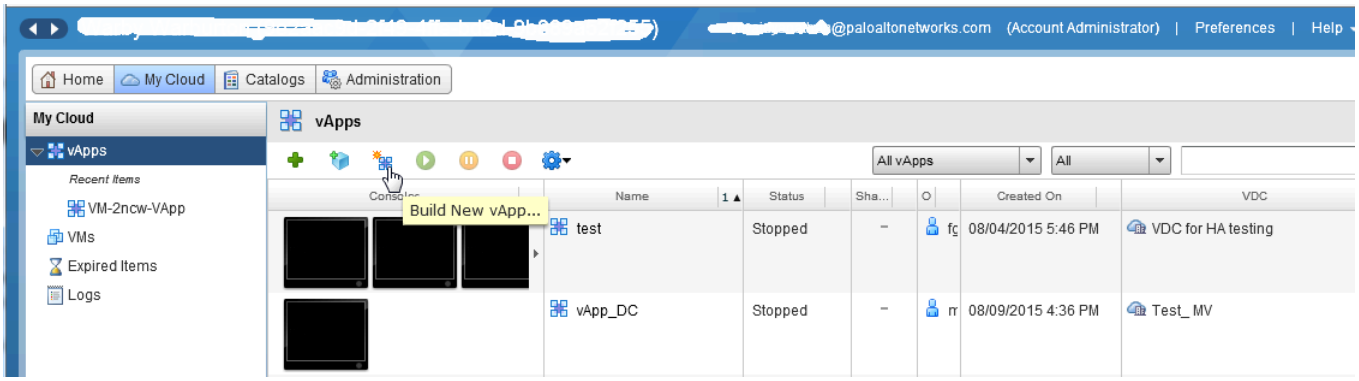
STEP 4 | VM-Series ファイアウォールを含む vDC と vApp を作成します。

1. vCloud Air にログインします。
2. **VPC OnDemand**（**VPC** オンデマンド）を選択し、VM-Series ファイアウォールをデプロイするロケーションを選択してください。



3. **Virtual Data Centers**（仮想データ センター）を選択し、**+** をクリックして新規の仮想データ センターを追加します。
4. vDC を右クリックして、**Manage Catalogs in vCloud Director**（**vCloud Director** のカタログを管理する）を選択します。vCloud Director Web インターフェイスへリダイレクトされます。
5. VM-Series ファイアウォールを含め、1 つ以上の仮想マシンを持つ新規の vApp 作成方法

   1. マイ クラウド > **vApps**を選択し、新規 **vApp** の作成をクリックします。



   2. **Name and Location**（名前とロケーション）を選択し、次に vApp を稼働させる**Virtual Datacenter**（仮想データセンター）を選択します。初期設定ではランタイ

©2023 Palo Alto Networks, Inc.

ムとストレージの **Leases**（リース）は無期限で有効となっており、vApp が自動停止されることはありません。

3. **Add Virtual Machines**（仮想マシンの追加）を実行します。**Look in:**（次を参照する：）ドロップダウンから VM-Series ファイアウォールのイメージを追加する場合は、**My Organization's Catalog**（組織のカタログ）からイメージを選択し、**Add**（追加）をクリックします。**Next**（次へ）をクリックします。
4. **Resources**（リソース）の構成を編集し、仮想マシンが配置された際のストレージポリシーを設定します。VM-Series ファイアウォールは**Standard**（標準）オプションを使用します。
5. **Virtual Machines**（仮想マシン）を設定します。各仮想マシンに名前を付け、それぞれを接続したいネットワークを選択してください。デフォルト ルートのネットワークには NIC 0（管理アクセス用）を接続する必要があります（NIC 1 はデータ トラフィック用）。後で他の NIC を追加することも可能です。
6. 設定を確認し、**Finish** [終了] をクリックします。
7. ステップ6に進みます。

STEP 5 | VM-Series ファイアウォールを vApp に追加します。

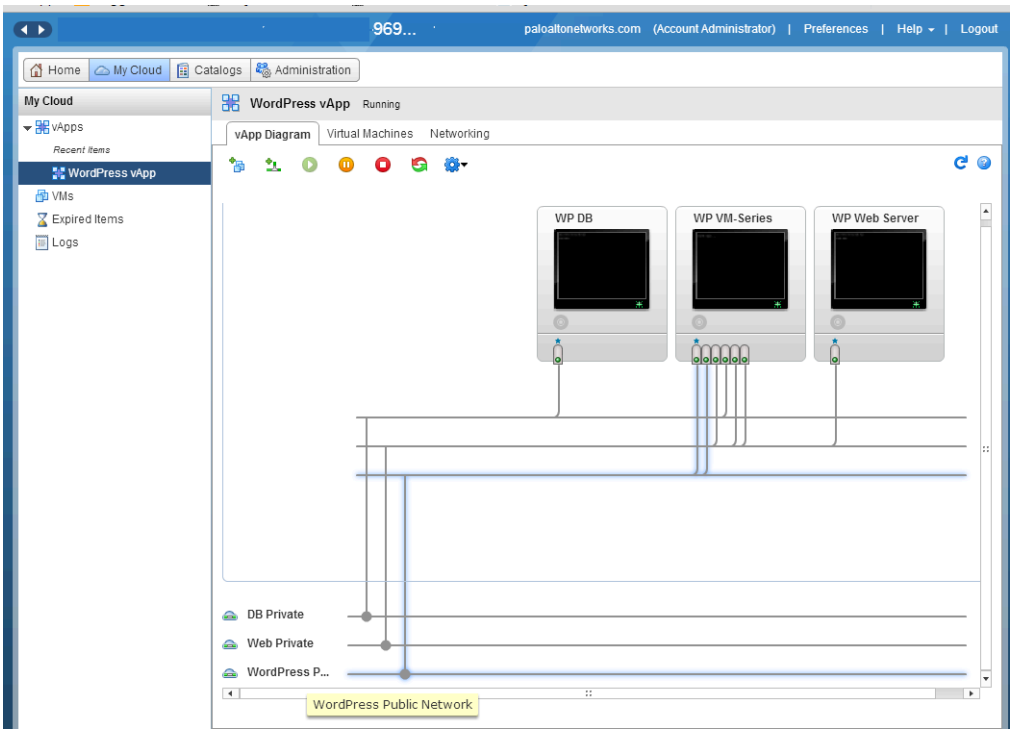
1. vCloud Air にログインします。
2. 左のペインから既存の**Virtual Data Center**（仮想データ センター）を右クリックし、**Manage Catalogs in vCloud Director**（**vCloud Director** のカタログを管理する）を選択します。vCloud Director Web インターフェイスへリダイレクトされます。
3. **My Cloud**（マイ クラウド） > **vApps**を選択し、VM-Series ファイアウォールを組み込む vApp の **Name**（名前）をクリックします。
4. 名前をダブルクリックして vApp を開き、**Virtual Machines**（仮想マシン）を選択し、 ✚ をクリックして仮想マシンを追加します。
   1. **Look in:**（次を参照する：）ドロップダウンで、**My Organization's Catalog**（組織のカタログ）から VM-Series ファイアウォールのイメージを選択し、**Add**（追加）をクリックします。**Next**（次へ）をクリックします。
   2. **Next**（次へ）をクリックして **Configure Resources**（リソースの設定）をスキップします。VM-Series ファイアウォールは **Standard**（標準）設定を使用するため、ストレージ ポリシーを変更する必要はありません。
   3. ファイアウォールの **Name**（名前）を入力し、管理アクセス（**NIC 0**）用にデフォルト ルートのネットワークおよび **IP Mode**（**IP** モード）（スタティックまたは DHCP）を選択します。ステップ6で NIC 1 の設定と NIC の追加を行うことができます。**Next**（次へ）をクリックします。
   4. この vApp に含まれる仮想マシンが使用するゲートウェイ アドレスやネットワーク マスクなど、vApp の vDC への接続方法を確認します。
   5. VM-Seriesファイアウォールを追加済みであることを確認し**Finish** [終了] をクリックします。
   6. ステップ6に進みます。

©2023 Palo Alto Networks, Inc.

STEP 6 | 導入環境に従い、VM-Series ファイアウォールのデータ インターフェイスを隔離または経路指定されたネットワークに接続します。

1. vCloud Director から **My Cloud**（マイ クラウド） > **vApps**の順に選択し、先ほど作成または編集した vApp を選択します。
2. **Virtual Machines**（仮想マシン）を選択し、VM-Series ファイアウォールを選びます。右クリックして **Properties**（プロパティ）を選択します。
3. **Hardware**（ハードウェア）を選択し、NIC のセクションへスクロールして **NIC 1** を選びます。
4. VM-Series ファイアウォールに向けたデータ トラフィックの接続要件に合わせ、データプレーン ネットワーク インターフェイスを vApp ネットワークまたは組織の VDC ネットワークへ追加します。以下の手順を実行し、新しいネットワークを作成します。
   1. ネットワークのドロップダウンから**Add Network**（ネットワーク追加）を選択します。
   2. **Network Type**（ネットワーク タイプ）を選択して名前を付け、**OK** をクリックします。
   3. インターフェイスに新しいネットワークが適用されていることを確認します。
5. ファイアウォールへ複数の NIC を追加する場合は、**Add**（追加）をクリックし、上記のステップ 4 を繰り返します。VM-Series ファイアウォールには、最大で 7 つのデータプレーン インターフェイスを追加することができます。
6. VM-Series ファイアウォールの管理インターフェイスが vDC のデフォルト ルート サブネットに追加され、最低でも 1 つのデータプレーン インターフェイスが経路指定されたネットワークまたは隔離ネットワークに接続されていることを確認してください。
   1. マイ クラウド > **vApps**を選択し、先ほど編集した vApp の 名前をダブルクリックします。
   2. **vApp Diagram**（**vApp** ダイアグラム）からネットワーク接続性を確認します。

©2023 Palo Alto Networks, Inc.

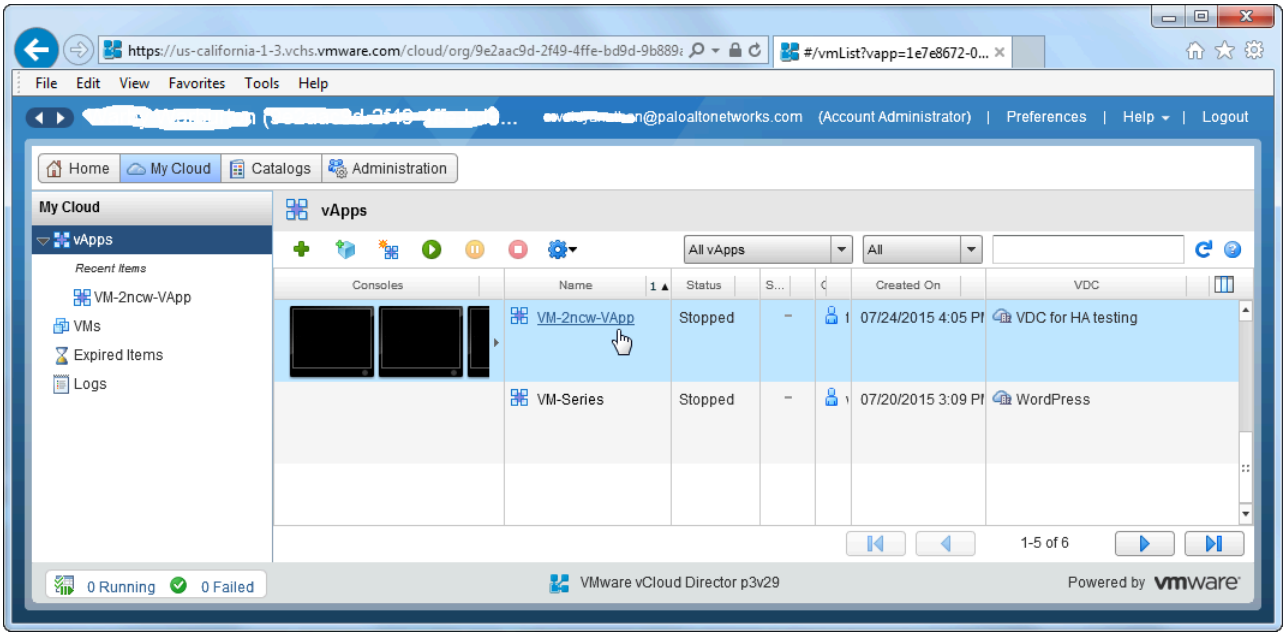


©2023 Palo Alto Networks, Inc.

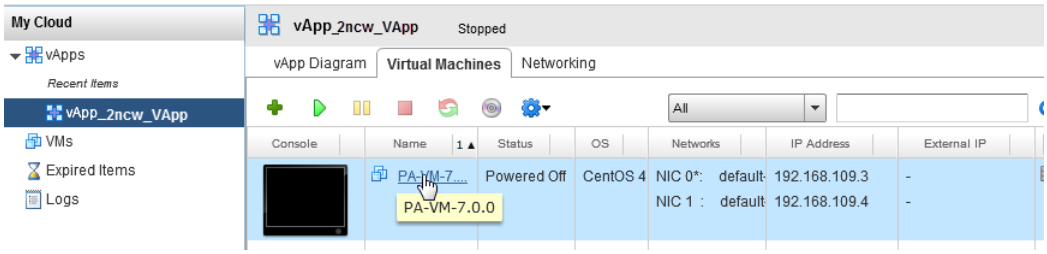
STEP 7 | （任意）VM-Series ファイアウォールに割り当てられたハードウェア リソースを編集します。

ファイアウォールに追加の CPU メモリやハードディスクを割り当てる必要がある場合のみこの手順を行ってください。

1. **My Cloud**（マイ クラウド） > **vApps** を選択し、先ほどデプロイした vApp の **Name**（名前）をダブルクリックします。



2. **Virtual Machine**（仮想マシン）を選択し、VM-Series ファイアウォールの **Name**（名前）をクリックして仮想マシンのプロパティを開きます。



3. VM-Series ファイアウォールに **Hardware**（ハードウェア）リソースを追加します。
   - お使いの VM-Series モデルの vCPU、メモリ、ディスクの最低要件については、「VM-Series システム要件」を参照してください。
   - NIC:管理用に1つ、最大7つのデータプレーンインターフェイス

STEP 8 | VM-Series ファイアウォールをパワー オンします。

STEP 9 | VM-Series ファイアウォール管理インターフェイス用の IP アドレスを設定します。

ESXi 上で VM-Series の初期設定を実行します。

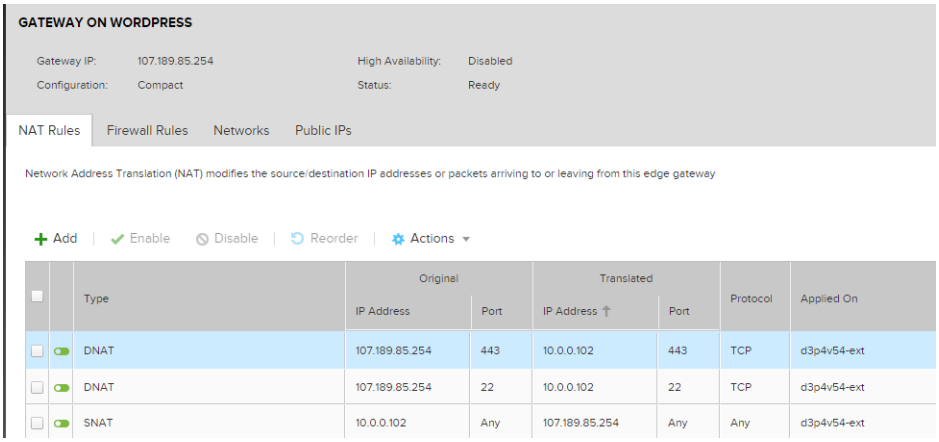
vCloud Air 上の VM-Series ファイアウォールは VMware Tools をサポートしており、ESXi および vCloud Air 上の VM-Series ファイアウォールで VMware Tools を使用し、VM-Series ファイアウォールの管理 IP アドレスを表示できます。

©2023 Palo Alto Networks, Inc.

STEP 10 | VM-Series ファイアウォールのインターネット接続を有効化するため、vCloud Air エッジ ゲートウェイの NAT ルールを定義します。

1. 仮想データセンター > ゲートウェイを選択して、ゲートウェイを選択し、**NAT** ルールをダブルクリックして追加します。
2. DNAT ルールを 2 つ作成します。1 つは SSH アクセス用、もう 1 つは VM-Series ファイアウォールの管理ポートの IP アドレスへの HTTPS アクセス用です。
3. VM-Series ファイアウォールの管理ポートから開始されたすべてのトラフィックに対し、内部ソース IP アドレスを外部 IP アドレス変換する SNAT ルールを作成します。

ファイアウォールのデータプレーン インターフェイスからトラフィックの送受信を行う場合は、*vCloud Air* エッジ ゲートウェイで追加の *DNAT* および *SNAT* ルールを作成する必要があります。



STEP 11 | ファイアウォールの Web インターフェイスにログインします。

この例における Web インターフェイスの URL は https://107.189.85.254 です。

エッジ ゲートウェイの NAT ルールは、外部 IP アドレスおよびポート 107.189.85.254:443 を、それぞれプライベート IP アドレスとポート 10.0.0.102:443 に変換します。

STEP 12 | 認証コードを追加し、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。

ライセンスのアクティベーションを行います。

STEP 13 | ハイパーバイザーによって割り当てられた MAC アドレスを使用するため、VM-Series ファイアウォールの設定を行います。

ハイパーバイザーによって割り当てられた MAC アドレス

©2023 Palo Alto Networks, Inc.

STEP 14 | データプレーン インターフェイスをレイヤー 3 インターフェイスとして設定します。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
2. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type**（インターフェイスタイプ）**:Layer3**
   - **Config**（設定）タブを選択し、インターフェイスをデフォルト ルーターに割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウンから **New Zone**（新規ゾーン）を選択します。新しいゾーン（「untrust」 など）を定義し、**OK** をクリックします。
   - **Ipv4** を選択し、スタティック IP アドレスを割り当てます。
   - **Advanced**（詳細） > **Other Info**（その他の情報）の順に選択し、**Management Profile**（管理プロファイル）ドロップダウンを展開して、**New Management Profile**（新規管理プロファイル）を選択します。
   - プロファイルの **Name**（名前）（「allow_ping」など）を入力し、Permitted Services（許可されたサービス）のリストから Ping を選択して、**OK** をクリックします。
   - インターフェイス設定を保存するには、**OK** をクリックします。
3. インターフェイスを追加する場合は、この操作を繰り返します。
4. **Commit**（コミット）をクリックして変更を保存します。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

paloalto TECHDOCS

VMware NSX-T での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールを VMware NSX-T にデプロイして、North-South および East-West のトラフィックを保護することができます。

> VMware NSX-T（North-South）での VM-Series ファイアウォールのセットアップ
> NSX-T（East-West）での VM-Series ファイアウォールのセットアップ

VMware NSX-T（North-South）での VM-Series ファイアウォールのセットアップ

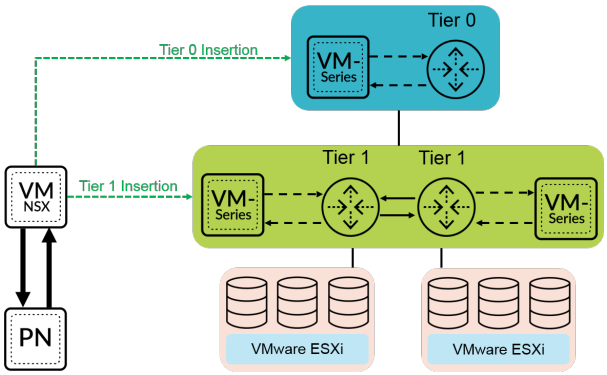
VMware NSX-T の VM-Series ファイアウォールは、Palo Alto 次世代ファイアウォールと Panorama を ESXi ホスト サーバーと統合し、NSX-T Software-Defined Data Center でのすべての North-South トラフィックの包括的な可視化と安全なアプリケーション有効化を提供します。

以下のトピックでは、VMware NSX-T での VM-Series ファイアウォールについて説明します。

- VMware NSX-T（North-South）でサポートされている VM-Series ファイアウォールのデプロイメント
- NSX-T（North-South）の VM-Series ファイアウォールのセキュリティ ポリシー コンポーネント
- NSX-T（North-South）での VM-Series ファイアウォールのデプロイ
- NSX-VからNSX-Tへのセキュリティ ポリシーの拡張

VMware NSX-T（North-South）でサポートされている VM-Series ファイアウォールのデプロイメント

VMware NSX-T Data Center に、1 つ以上の VM-Series ファイアウォール インスタンスをパートナー サービスとしてデプロイできます。North-South トラフィックを保護するため、VM-Series ファイアウォールを Tier-0 または Tier-1 論理ルーターにアタッチします。VM-Series ファイアウォールをスタンドアロン サービス インスタンスとしてデプロイするか、または 2 つのファイアウォールを高可用性（HA）ペアとしてデプロイすることができます。Panorama は、NSX-T Manager と、NSX-T Software-Defined Data Center にデプロイされている VM-Series ファイアウォール間の接続を管理します。



- Tier-0 挿入 — Tier-0 挿入では、論理ネットワークと物理ネットワーク間のトラフィックを処理する Tier-0 論理ルーターに VM-Series ファイアウォールがデプロイされます。Tier-0 挿入で VM-Series ファイアウォールをデプロイすると、NSX-T Manager は Panorama で設定されたデプロイメント情報を使用して、バーチャル ワイヤ モードの Tier-0 論理ルーターにファイアウォールをアタッチします。
- Tier-1 挿入 — Tier-1 挿入では、セグメントへのダウンリンク接続と Tier-0 論理ルーターへのアップリンク接続を提供する Tier-1 論理ルーターに VM-Series ファイアウォールがデプロ

©2023 Palo Alto Networks, Inc.

イされます。NSX-T Manager は、Tier-1 挿入でデプロイされた VM-Series ファイアウォールを、バーチャル ワイヤ モードの Tier-1 論理ルーターにアタッチします。

ファイアウォールのデプロイが完了したら、Tier-0 または Tier-1 ルーターを通過するときにトラフィックを VM-Series ファイアウォールに送信するトラフィック リダイレクト ルールを設定します。Panorama で設定したセキュリティ ポリシー ルールは管理対象 VM-Series ファイアウォールにプッシュされ、ファイアウォールを通過するトラフィックに適用されます。

NSX-T（North-South）の VM-Series ファイアウォールのセキュリティ ポリシー コンポーネント

以下の表は、この Palo Alto Networks と VMware NSX-T の統合ソリューションを構成するコンポーネントを示しています。

VMware コンポーネント	
vCenter/ESXi	vCenter サーバーは、vSphere スイート用の中央管理ツールです。ESXi は、コンピュータの仮想化を実現するためのハイパーバイザーです。 vCenter の互換性については、ご利用のバージョンの NSX-T に応じた、VMware の互換性マトリックスを参照してください。
NSX-T Manager	VMware NSX-T Data Center 2.4.0 以降を、vCenter サーバーにインストールし、登録する必要があります。ESXi クラスタ内の ESXi ホストに VM-Series ファイアウォールをデプロイするには、NSX-T Manager が必要です。

Palo Alto Networks コンポーネント	
PAN-OS	VM-Series の基本イメージ（PA-VM-NST-9.1.zip）は、NSX-T で VM-Series ファイアウォールをデプロイするために必要です。 NSX 用の VM-Series ファイアウォールを ESXi サーバーにデプロイするための最小システム要件は、VM-Series モデルによって決まります。VM-Series モデルの最小ハードウェア要件については、「VM-Series モデル」を参照してください。
Panorama Panorama のバージョンは、管理対象ファイアウォールと同じかそれ以降のバージョンである必要があります。	NSX-T の VM-Series ファイアウォールを使用するには、Panorama 9.1 以降が必要です。 Panorama は、Palo Alto Networks の次世代ファイアウォール用中央管理ツールです。このソリュー

©2023 Palo Alto Networks, Inc.

Palo Alto Networks コンポーネント	
	ションでは、Panorama が NSX-T Manager と連携して、NSX-T 用の VM-Series ファイアウォール上でデプロイ、ライセンスの付与、中央管理（設定やポリシー）を実行します。 Panorama が、NSX-T Manager、VM-Series ファイアウォール、および Palo Alto Networks 更新サーバーにアクセスできる必要があります。 Panorama アプライアンスのデプロイについては、『Panorama 管理者ガイド』を参照してください。
VMware NXS 用 Panorama プラグイン	3.0.0 以降
VM-Series プラグイン	1.0.6 以降
VM-Series ファイアウォール モデル	VM-100、VM-300、VM-500、および VM-700 が NSX-T をサポートします。

NSX-T（North-South）での VM-Series ファイアウォールのデプロイ

VM-Series ファイアウォールのある NSX-T 環境で North-South トラフィックを保護するには、以下のタスクを実行してください。

次の手順は、*NSX-T Manager 3.0*を参照しています。

。

- VMware NSX 用 Panorama プラグインのインストール
- NSX-T Manager と Panorama 間の通信の有効化
- Panorama でのテンプレート スタックとデバイス グループの作成
- Panorama でのサービス定義の設定
- VM-Series ファイアウォールのデプロイ
- VM-Series ファイアウォールへのトラフィックの転送
- NSX-T の VM-Series ファイアウォールへのセキュリティ ポリシーの適用
- ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用

VMware NSX 用 Panorama プラグインのインストール

VMware NSX 用 Panorama プラグインをダウンロードしてインストールします。プラグインをインストールまたはアップグレードする前に、「互換性マトリックス」を参照してください。

©2023 Palo Alto Networks, Inc.

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。Panorama HA ピアにプラグインをインストールする際には、プラグインを最初にパッシブ ピアにインストールしてから、アクティブ ピアにインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 1 | **Panorama** > **Plugins**（プラグイン）を選択します。プラグインをインストールまたはアップグレードする前に、「互換性マトリックス」を参照してください。

STEP 2 | **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。

STEP 3 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 4 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。

NSX-T Manager と Panorama 間の通信の有効化

Panorama と NSX-T Manager 間の通信を有効にするには、以下の手順を実行します。Panorama を最大16台のNSX-T Managerに接続できます。Panorama を複数のNSX-T Managerに接続する場合は、デバイスグループ階層とテンプレートスタックを慎重に計画し、デプロイメントに必要な他のコンポーネントとどのように対話するのかを検討する必要があります。サービス定義は、デバイス グループとテンプレート スタックを参照し、その情報を関連する ESXi クラスターのファイアウォールにプッシュします。

STEP 1 | （任意）Panorama と NSX-V Manager 間の通信のため、Panorama の **Panorama** > **Setup**（セットアップ） > **Services**（サービス） > **Proxy Server**（プロキシ サーバー）で構成されたプロキシ サーバー設定をバイパスします。このコマンドを実行すると、Panorama が NSX-V Manager と直接通信しながら、他のサービスのためにプロキシ通信は維持されます。

1. Panorama CLI にログインします。
2. プロキシ バイパスを有効または無効にするには、以下のコマンドを実行します。

   ```
   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}
   ```

   プロキシ バイパスを有効にする場合は **yes** を選択し、無効にする場合は **no** を選択します。これはデフォルトで**no**が設定されます。

STEP 2 | Panorama Web インターフェイスにログインします。

Web ブラウザから安全な接続（https）を使用し、初期設定時に割り当てられた IP アドレスとパスワードを使用してログインします（https://<*IP address*>）。

©2023 Palo Alto Networks, Inc.

STEP 3 | NSX-T Manager へのアクセスをセットアップします。Panorama を接続するNSX-T Managerごとにこの手順を繰り返します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択し、**Add**（追加）をクリックします。
2. **Name**（名前）に分かりやすい NSX-T Manaer 名を入力します。
3. （任意）NSX-T Managerの説明を追加します。
4. NSX-T Managerにアクセスするための**NSX Manager URL**（NSX-T Manager cluster 仮想 IP アドレスまたは FQDN）を入力します。
5. Panorama が NSX-T Manager への認証を行えるように **NSX Manager Login**（**NSX Manager** ログイン）に認証情報（ユーザー名とパスワード）を入力します。
6. **OK**をクリックします。

NSX-T Manager のログイン用パスワードを変更する場合、必ず *Panorama* 上のパスワードを即座に更新してください。パスワードが間違っていると、*Panorama* および *NSX-T Manager* 間で通信できなくなります。

STEP 4 | 変更を Panorama にコミットします。

Commit (コミット) および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

STEP 5 | Panorama の接続状態を確認します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択します。
2. **Status**（ステータス）列のメッセージを確認します。

   接続が成功すると、状態は **Registered**（登録済み）と表示されます。これは、Panorama と NSX-T Manager が同期していることを示します。

   失敗した状態では、以下のメッセージが表示されます。

   - **No connection**（接続なし）:NSX-T Manager にアクセスできないか、NSX-T Manager へのネットワーク接続を確立できません。
   - **Invalid Credentials**（無効な認証情報）:アクセス認証情報（ユーザー名/パスワード）が正しくありません。
   - **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-T Manager に定義されている設定と異なります。リンクをクリックして失敗の原因を確認してください。たとえば、NSX-T 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-T Manager のサービス定義の検証を行います。Panorama と NSX-T 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。
   - **Connection Disabled**（接続が無効）:Panorama と NSX-T Manager 間の接続が手動で無効にされています。

©2023 Palo Alto Networks, Inc.

Panorama でのテンプレート スタックとデバイス グループの作成

Panorama を使用して NSX-T で VM-Series ファイアウォールを管理するには、ファイアウォールがデバイス グループおよびテンプレート スタックに所属している必要があります。デバイス グループでは、同様のポリシーとオブジェクトが必要なファイアウォールを論理的なユニットとしてグループ化できます。この設定は Panorama の **Objects**（オブジェクト）タブと **Policies**（ポリシー）タブを使用して定義します。テンプレート スタックを使用して、VM-Series ファイアウォールがネットワーク上で動作するのに必要な設定を構成します。この設定は、Panorama の **Device**（デバイス）タブと **Network**（ネットワーク）タブを使用して定義します。NSX-T 設定で使用する各テンプレート スタックにはサービス定義が関連付けられている必要があります。

NSX-T にデプロイされたファイアウォールには、2 つのデフォルト ゾーンとバーチャル ワイヤーモードで設定された 2 つのインターフェイスが存在しています。ethernet1/1 はゾーン **south** の一部で、ethernet1/2 はゾーン **north** の一部です。Panorama からマネージド ファイアウォールにポリシー ルールをプッシュ配信するには、ゾーンを設定する必要があります。インターフェイスが、ファイアウォール上でそれを、Panorama の対応するテンプレート スタックと照合します。

STEP 1 | デバイスグループあるいはデバイスグループの階層を追加します。

1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、**Add**（追加）をクリックします。デバイス グループの階層を作成することもできます。
2. デバイス グループを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット）をクリックした後、**Commit Type**（コミット タイプ）として **Panorama** を選択し、Panorama で実行中の設定に対する変更を保存します。

STEP 2 | テンプレートを追加します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add**（追加）をクリックします。
2. テンプレートを識別するために、一意の **Name**（名前）と **Description**（説明）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

STEP 3 | テンプレート スタックを作成します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add Stack**（スタックの追加）をクリックします。
2. テンプレートを識別するために、一意の **Name**（名前）と **Description**（説明）を入力します。
3. 前に作成したテンプレートを追加するには、**Add**（追加）をクリックします。
4. **OK**をクリックします。
5. **Commit**（コミット） をクリックし、**Commit to Panorama**（**Panorama**に非ミット） を選択して、Panorama で実行中の設定に変更を保存します。

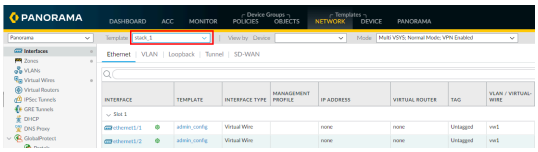
©2023 Palo Alto Networks, Inc.

STEP 4 | バーチャル ワイヤー、インターフェイス、およびゾーンを設定します。下に表示されているドロップダウンから、正しいテンプレートを選択していることを確認してください。作成するオブジェクトは、以下の条件を満たしている必要があります。

デフォルトのバーチャル ワイヤーまたはゾーンの名前を変更する場合、*Panorama*のバーチャル ワイヤーおよびゾーンの名前は、ファイアウォールで使用されている名前と一致している必要があります。

- **ethernet1/1** および **ethernet1/2** を使用します。
- バーチャルワイヤーのオブジェクト名は **vw1** 。
- 最初のゾーン名 **south** 、タイプ **virtual-wire**、そして **ethernet1/1** を含む。
- 2 番目のゾーン名 **north** 、タイプ **virtual-wire**、そして **ethernet1/2** を含む。

デプロイメントの各テンプレートに対して、この作業を繰り返します。



STEP 5 | **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

STEP 6 | テンプレートスタックの DNS および NTP サーバ情報を更新します。デプロイメントでデバイス証明書を使用している場合は、この手順を完了する必要があります。これは、NSX-T 環境にデプロイされたファイアウォールに、デバイス証明書サーバに到達するために必要な正しい DNS 情報があることを確認するために必要です。

1. [テンプレート] ドロップダウンから正しいテンプレートスタックを指定したことを確認します。
2. デバイス > セットアップ > サービスを選択して、[編集]アイコンをクリックします。
3. [サービス] タブで、プライマリ **DNS** サーバーおよびセカンダリ **DNS** サーバーの IP アドレスを入力します。
4. [NTP] タブで、**NTP** サーバーの IP アドレスを入力します。
5. **OK** をクリックします。
6. 変更を Panorama にコミットします。

Panorama でのサービス定義の設定

サービス定義は、NSX-T データ センター環境にインストールされている VM-Series ファイアウォール用の構成を指定しています。サービス定義には、デバイス グループ、テンプレート スタック、および OVF URL を含める必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | 新しいサービス定義を追加します。

*Panorama*で最大*32*のサービス定義を作成できます。

1. **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（サービス定義）を選択します。
2. **Add**（追加）を選択して、新しいサービス定義を作成します。
3. **Name**（名前）に分かりやすいサービス定義名を入力します。
4. （任意）このサービス定義を使用してデプロイされる VM-Series ファイアウォールの機能あるいは目的が分かるような説明を追加します。

STEP 2 | デバイス グループとテンプレート スタックをサービス定義用に割り当てます。

必ずPanorama でのテンプレート スタックとデバイス グループの作成を行うようにしてください。

このソリューションでデプロイされるファイアウォールは、Panorama から集中管理されるため、ファイアウォールが属する **Device Group**（デバイス グループ）と **Template Stack**（テンプレート スタック）を指定する必要があります。このサービス定義を使用してデプロイされるすべてのファイアウォールは、指定したテンプレート スタックおよびデバイスグループに属します。

1. **Device Group**（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あるいはデバイスグループの階層を選択します。
2. **Template**（テンプレート） ドロップダウンでテンプレート スタックを選択します。

あるサービス定義に割り当てられたテンプレート スタックあるいはデバイスグループを他のサービス定義で利用することはできません。

STEP 3 | OVF ファイルの場所を指定します。

zip ファイルをダウンロードして解凍し、.ovf、mf、および .vmdk の各ファイルを抽出して、同じディレクトリに保存します。ovf および vmdk ファイルはファイアウォールの各インスタンスのデプロイに使用されます。

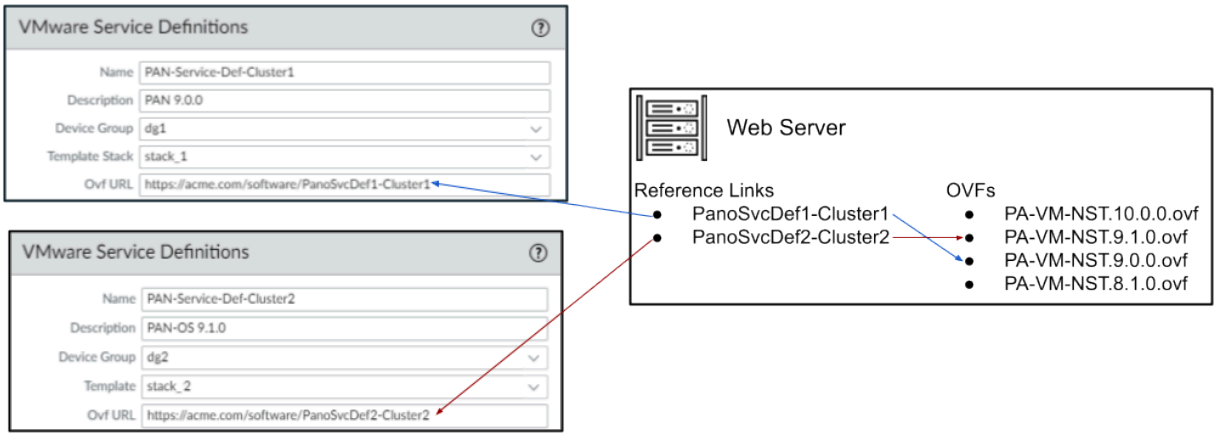
該当するファイル タイプをダウンロードできるように、サーバーのセキュリティ設定を変更する必要がある場合、IISサーバーでMimeタイプ設定を変更したり、Apacheサーバで.htaccessファイルを編集したりします。

VM-Series ファイアウォールの *NSX* サービスのデプロイメントが正常に完了した後は、*Panorama* サービス定義の *OVF* パスを変更しないでください。*VM-Series* ファイアウォールのデプロイメントが正常に完了した後に *OVF* パスを変更すると、*NSX* サービスデプロイメントが失敗した状態になる可能性があります。*NSX-T Manager* でこの問題を解決できますが、これにより、すべての *VM-Series* ファイアウォールが再デプロイされる可能性があります。

デプロイされたファイアウォールに影響を与えることなく、スケーリングしてベースイメージを変更できる OVF パス名を使用することをお勧めします。**https://acme.com/software/PA-VM-NST.9.1.0.ovf** などのパスの代わりに、**https://acme.com/software/PanoSvcDef1-**

©2023 Palo Alto Networks, Inc.

Cluster1.ovf などを使用します。スタティックパス参照を使用すると、OVF パスを変更する必要がなくなります。デプロイメント内の各 Panorama サービス定義 （vSphere クラスター） のパスを作成し、必要に応じて Web サーバー上の PAN-OS ベースイメージ参照を変更することをお勧めします。



OVF URL に、OVF ファイルをホストする Web サーバーの場所を追加します。http および https の両方がサポートされています。

Panoramaには、OVFファイルを取得するために、Webサーバーとのネットワーク接続が必要になります。

同じ ovf バージョンあるいは異なるバージョンをすべてのサービス定義で使用することができます。異なるバージョンの ovf を各サービス定義で使用することにより、異なる ESXi クラスタ内の VM-Series ファイアウォールの PAN-OS のバージョンを変えることができます。

STEP 4 | ファイアウォールの **Insertion Type**（挿入タイプ）として **North South** を選択します。

STEP 5 | NSX ManagerがVM-Seriesファイアウォールをデプロイする時に、自動的にデバイス証明書を取得するには、デバイス証明書を設定します。

新たにデプロイされたVM-Seriesファイアウォールにデバイス証明書を適用するには、このオプションを有効にします。デバイス証明書をサポートするベースイメージOVFを使ってファイアウォールをデプロイする場合にのみ、このオプションを使用してください。Panoramaは、サービス定義の一環として、NSX Managerにデバイス証明書情報をプッ

 ©2023 Palo Alto Networks, Inc.

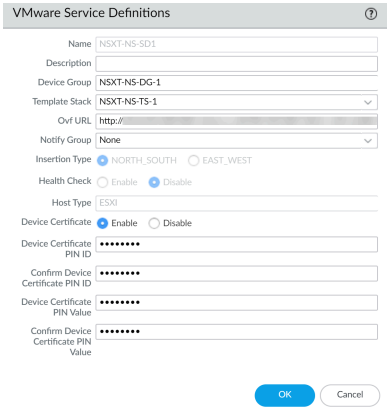
シュ配信します。NSXに新たなファイアウォールがデプロイされた場合、ブートアップ時にファイアウォールにデバイス証明書がインストールされます。

VMware NSX上のVM-Seriesファイアウォールに対するデバイス証明書をサポートしているOVFの一覧については、「Palo Alto Networks互換性マトリックス」を参照してください。

OVF がデバイス証明書をサポートしている場合は、デバイス証明書を使用しているかどうかに関係なく、デバイス証明書を有効にする必要があります。OVFがデバイス証明書をサポートしていない場合は、このオプションを無効にしてください。

1. まだ作業を行っていない場合は、カスタマーサポートポータルにログインして、Registration PINおよびPIN IDを生成します。
2. **Device Certificate**（デバイス証明書）下で、**Enable**（有効）をクリックします。
3. PIN IDをコピーして、それを**Device Certificate PIN ID**（デバイス証明書**PIN ID**）フィールドに入力します。
4. **Confirm Device Certificate PIN ID**（デバイス証明書**PIN ID**の再入力）フィールドに、PIN IDをもう一度入力します。
5. PIN Valueをコピーして、それを**Device Certificate PIN Value**（デバイス証明書**PIN**値）フィールドに入力します。
6. **Confirm Device Certificate PIN Value**（デバイス証明書**PIN**値の再入力）フィールドに、PIN値をもう一度入力します。

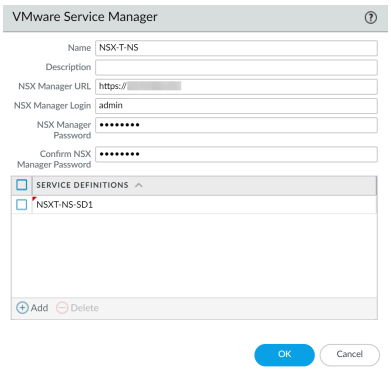
STEP 6 | **OK** をクリックしてサービス定義を保存します。



©2023 Palo Alto Networks, Inc.

STEP 7 | サービス定義をサービス マネージャーにアタッチします。

1. **Panorama** > **VMware** > **NSX-T** > **Service Manager**（サービス マネージャー）を選択し、サービス マネージャー名のリンクをクリックします。
2. Service Definitions（サービス定義）で **Add**（追加）をクリックし、ドロップダウンからサービス定義を選択します。
3. **OK** をクリックします。

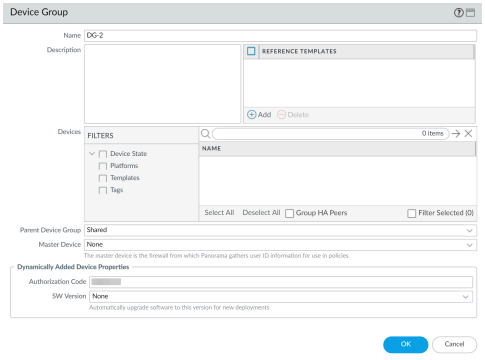


STEP 8 | 認証コードを追加してファイアウォールをライセンス登録します。

1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、作成したサービス定義に関連付けられているデバイス グループを選択します。
2. **Dynamically Added Device Properties**（動的に追加されたデバイス プロパティ）の下で、受注完了電子メールで受け取った認証コードを追加します。任意で **SW Version**（**SW** バージョン）のドロップダウン リストから None（なし）を選択します。

   NSX-T に新しいファイアウォールがデプロイされると、それがデバイス グループに自動的に追加され、指定した認証コードを使ってライセンスが供与され、指定したバージョンの PAN-OS にアップグレードされます。

   サポート ポータルで、デプロイ可能なファイアウォールの総数および認証コードで使用可能なライセンス総数に対する使用済みライセンス数の比率を表示できます。



STEP 9 | **Commit to Panorama**（**Panorama** へのコミット）によってコミットします。

©2023 Palo Alto Networks, Inc.

STEP 10 | NSX-T Manager で、サービス定義が使用可能であることを確認します。

System（システム） > **Service Deployments**（サービスのデプロイ） > **Catalog**（カタログ）を選択します。サービス定義が NSX-T Manager にサービス インスタンスとしてリストアップされます。

VM-Series ファイアウォールのデプロイ

Panorama での設定が完了したら、以下の手順に従って NSX-T データセンターで VM-Series ファイアウォールを起動します。

NSX-T高可用性環境上にVM-Seriesファイアウォールをデプロイする場合、両方のファイアウォールは同じデバイスグループおよびテンプレートスタックにデプロイされます。

STEP 1 | NSX-T Manager にログインします。

STEP 2 | **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Deployment**（デプロイ）を選択します。

STEP 3 | **Partner Service**（パートナー サービス）ドロップダウンから、サービス定義を選択します。

STEP 4 | **Deploy Service**（サービスのデプロイ）をクリックします。

STEP 5 | VM-Seriesファイアウォールの分かりやすい **Service Deployment Name**（サービスデプロイ名）を入力します。

STEP 6 | **Attachment Points**（アタッチメントポイント）下で、tier-0またはtier-1ルーターを選択します。NSX-T Manager により、選択されたルーターに VM-Series ファイアウォールがアタッチされ、このルーターを通過するトラフィックが検査のため VM-Series ファイアウォールにリダイレクトされます。サービス挿入がアタッチされていないルーターを選択する必要があります。

STEP 7 | **Compute Manager**（コンピュート マネージャー）を選択します。コンピュート マネージャーは、データセンターを管理する vCenter サーバーです。

STEP 8 | **Cluster**（クラスター）を選択します。VM-Series ファイアウォールは、Edge Transport ノードを含まない任意のクラスタ上にデプロイできます。

STEP 9 | **Datastore**（データストア）を選択します。

STEP 10 | ネットワーク設定を行います。

1. **Networks**（ネットワーク）列で**Edit Details**（詳細の編集）をクリックします。
2. **Primary Interface Network**（プライマリインターフェイスネットワーク）を選択します。
3. **Primary Interface IP**（プライマリインターフェイス**IP**）を入力します。
4. **Primary Gateway Address**（プライマリゲートウェイアドレス）を入力します。
5. **Primary Subnet Mask**（プライマリサブネットマスク）を入力します。
6. **Save**（保存）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 11 | NSX-T Managerは、選択したPartner Service（パートナーサービス）に基づいて、**Deployment Specification**（デプロイの仕様）および**Deployment Template**（デプロイテンプレート）を記入します。

STEP 12 | **Failure Policy**（障害ポリシー）を Allow（許可）または Block（ブロック）に設定します。障害ポリシーは、ファイアウォールが使用できない場合に VM-Series ファイアウォールに送信されるトラフィックを NSX-T Manager がどのように処理するかを定義します。

STEP 13 | VM-Series ファイアウォールの **Deployment Mode**（デプロイメント モード）として Standalone（スタンドアロン）または High Availability（高可用性）を選択します。エッジノードクラスタが存在しており、High Availability（高可用性）を選択した場合、NSX-T Managerはアクティブなエッジノードにデプロイしたファイアウォールに加えて、スタンバイエッジノードにも追加のVM-Seriesファイアウォールをデプロイします。

STEP 14 | **Save**（保存）をクリックして、VM-Seriesファイアウォールをデプロイします。

VM-Series ファイアウォールへのトラフィックの転送

VM-Series ファイアウォールへトラフィックを転送するには、以下の手順に従います。North-Southトラフィックの場合、リダイレクト ルールはデフォルトでステートレスであり、変更できません。さらに、NSX-Tは、リターン トラフィックに対応する再帰ルールを自動的に作成します。

NSX-T North-South用VM-SeriesファイアウォールをHAモードでデプロイする場合、両方のHAピアに対してトラフィックリダイレクトルールを作成する必要があります。また、まずアクティブピア用のリダイレクトルールを作成してから、次にパッシブピアのルールを作成する必要があります。

再帰ルールは*NSX-T Web*インターフェイスに表示されません。

STEP 1 | NSX-T Manager にログインします。

STEP 2 | **Policy**（ポリシー）モードになっていることを確認します。

STEP 3 | **Security**（セキュリティ） > **North South Security**（ノースサウスセキュリティ） > **Network Introspection**（**N-S**）（ネットワーク診断）を選択します。

STEP 4 | **Add Policy**（ポリシーの追加）をクリックします。

STEP 5 | **Name**（名前）に、分かりやすいポリシー名を入力します。

STEP 6 | **Redirect To**（リダイレクト先）ドロップダウンから、VM-Seriesファイアウォールサービスのインスタンスを選択します。NSX-T Managerが、選択したサービスインスタンスに基づいて、**Applied To**（適用先）フィールドを自動的に入力します。

STEP 7 | 新しく作成したポリシーを選択します。

©2023 Palo Alto Networks, Inc.

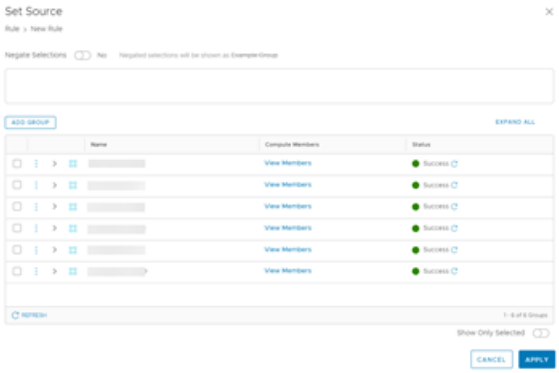
STEP 8 | **Add Rule**（ルールの追加）をクリックします。

NSX-T 環境のアクティブ/スタンバイ *HA* にエッジ ノードがある場合は、各エッジ ノードにリダイレクト ルールを作成する必要があります。*NSX-T*は、フェイルオーバーが発生した場合、スタンバイ ノードにリダイレクト ルールを自動的に適用しません。

STEP 9 | **Name**（名前）フィールドをクリックし、分かりやすいルール名を入力します。

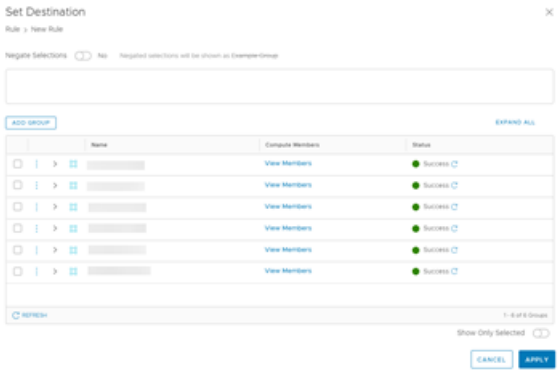
STEP 10 | デフォルトでは、送信元は Any（任意）に設定されます。別の送信元を指定するには以下の手順を実行します。

1. **Source**（ソース）列の編集ボタンをクリックします。
2. ソースとして設定する1つまたは複数のグループを選択するか、またはAdd Group（グループの追加）をクリックして新しいグループを作成します。
3. **Apply**[適用] をクリックします。



STEP 11 | デフォルトでは、宛先は Any（任意）に設定されます。別の宛先を指定するには以下の手順を実行します。

1. **Destination**（宛先）列の編集ボタンをクリックします。
2. 宛先として設定する1つまたは複数のグループを選択するか、またはAdd Group（グループの追加）をクリックして新しいグループを作成します。
3. **Apply**[適用] をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 12 | デフォルトでは、すべてのサービスがファイアウォールにリダイレクトされます。特定のサービスとプロトコルを指定するには以下の手順を実行します。

1. **Services**（サービス）列の編集ボタンをクリックします。
2. サービスとして設定する1つまたは複数のグループを選択するか、またはAdd Service（サービスの追加）をクリックして新しいサービスを作成します。
3. **Apply**[適用] をクリックします。

STEP 13 | トラフィックを VM-Series ファイアウォールに送信するため、**Action**（アクション）のドロップダウン リストから **Redirect**（リダイレクト）を選択します。

STEP 14 | ルールを **Enable**（有効）にします。NSX-T Managerは、作成したリダイレクト ルールを公開し、リターン トラフィック用の再帰ルールを自動的に作成します。再帰ルールはNSX-T Manager Webインターフェイスに表示されません。



STEP 15 | VM-SeriesファイアウォールがHAでデプロイされている場合、パッシブHAピア用に別のルールを作成します。

リターン トラフィックが*VM-Series*ファイアウォールに向けられていない場合は、リターン トラフィックのトラフィック リダイレクト ルールを手動で構成します。

NSX-T の VM-Series ファイアウォールへのセキュリティ ポリシーの適用

VM-Series ファイアウォールをデプロイし、トラフィックをファイアウォールに送信するリダイレクト ルールを作成したので、Panorama を使用して VM-Series ファイアウォールのセキュリティ ポリシー ルールを一元的に管理できます。

STEP 1 | Panorama にログインします。

©2023 Palo Alto Networks, Inc.

STEP 2 | セキュリティ ポリシー ルールを作成する

デフォルトでファイアウォールは、*Bidirectional Forwarding Detection*（*BFD*）（双方向転送検出）を許可するルールを作成します。*BFD*をブロックするルールを作成しないようにしてください。*BFD* がブロックされると、*NSX-T* はファイアウォールが使用できないと認識します。

1. **Policies**（ポリシー） > **Security**（セキュリティ） > **Prerules**（プレルール）を選択します。
2. 「Panorama でのテンプレート スタックとデバイス グループの作成」で、NSX-T での VM-Series ファイアウォール管理のために作成したデバイス グループを選択します。
3. **Add**（追加） をクリックし、ルールの **Name**（名前）と **Description**（説明）を入力します。この例では、セキュリティ ルールが Webフロントエンド サーバーとアプリケーション サーバーの間のすべてのトラフィックを許可しています。
4. **Source Zone**（送信元ゾーン）および**Destination Zone**（宛先ゾーン）を選択します。
5. **Source Address**（送信元アドレス）および **Destination Address**（宛先アドレス）では、アドレス、静的アドレス グループ、または領域を選択または入力します。

   NSX-T の *VM-Series* ファイアウォールでは、*North-South* トラフィックのダイナミック アドレス グループはサポートされていません。
6. 許可する **Application**（アプリケーション）を選択します。この例では、グループ化された特定のアプリケーションの静的グループを含む **Application Group**（アドレス グループ）を作成します。
   1. **Add**（追加）をクリックして、**New Application Group**（新規アプリケーション グループ）を選択します。
   2. **Add**（追加）をクリックし、グループに含めるアプリケーションを選択します。
   3. **OK** をクリックしてアプリケーション グループを作成します。
7. トラフィックについてのアクションを **Allow**（許可） または **Deny**（拒否） に指定し、任意でプロファイルのアンチウイルス、アンチスパイウェア、脆弱性防御のデフォルト セキュリティ プロファイルに関連付けます。
8. **Commit**（コミット）をクリックし、**Commit to Panorama**（**Panorama**にコミット）を選択します。**OK**をクリックします。

STEP 3 | NSX-T の VM-Series ファイアウォールにポリシーを適用します。

1. **Commit**（コミット） > **Push to Devices**（デバイスへのプッシュ） > **Edit Selections**（選択内容の編集）をクリックします。
2. デバイス グループを選択し、**OK** をクリックします。
3. **Force Template Values**（テンプレートの値を適用）を選択します。デフォルトでPanoramaは、ファイアウォール上のオブジェクトを、名前を共有しているPanorama上のオブジェクトで上書きすることはありません。管理対象ファイア

 ©2023 Palo Alto Networks, Inc.

ウォールにポリシーをプッシュするには、Force Template Values（テンプレートの値を適用）を選択する必要があります。

4. テンプレート値を適用することを確認して、**Yes**（はい）をクリックします。
5. **OK**をクリックします。
6. コミットが成功したことを確認します。

STEP 4 | （任意）テンプレートを使用して、DNS サーバー、NTP サーバー、Syslog サーバー、およびログイン バナーなどのネットワーク基本設定およびデバイス設定をプッシュします。

テンプレートの使用については、『Panorama 管理者ガイド』を参照してください。

ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用

VMware NSX-T内に同種のCPU設定を持つESXiホスト間で、vMotionを使ってVM-Seriesファイアウォールを移動する際に、トラフィックフローを維持するためには、vMotion中にPAN-OS CLIを使ってVM-Seriesファイアウォールの内部ハートビートを一時停止する必要があります。ハートビートのモニタリングを一時停止する時間（分）を指定することができます。ハートビートのモニタリングは、最大60分間停止できます。一時停止期間が過ぎた、または強制的に一時停止を中断した場合、ハートビートモニタリングが再開されます。

VM-Seriesファイアウォールのv Motionは、vSphere 6.5、6.7、および7.0でサポートされています（ESXiホストが同種のCPU設定を保有している場合）。

*vSphere 7.0*以降を実行している場合、*vMotion*を使って*VM-Series*ファイアウォールを移動する際に、この手続きは必要ありません。

STEP 1 | VM-SeriesファイアウォールCLIにログインします。

STEP 2 | 次のコマンドを使って、ハートビートモニタリング一時停止間隔を設定します。一時停止はコマンドを実行すると即座に開始されます。vMotionに予想以上の時間がかかっている場合、新たにより長い間隔でこのコマンドを再実行することができます。この場合も、コマンド実行後即座に一時停止が開始されます。

```
request system heartbeat-pause set interval <一時停止期間（分）>
```

一時停止の残り時間は、次のコマンドで参照することができます。

```
request system heartbeat-pause show interval
```

STEP 3 | （任意）一時停止期間が経過する前にvMotionが完了した場合、期間に0を設定して一時停止を終了することができます。

```
request system heartbeat-pause set interval 0
```

NSX-VからNSX-Tへのセキュリティ ポリシーの拡張

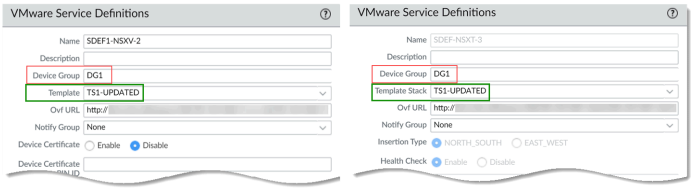
NSX-Vデプロイ環境からNSX-Tデプロイ環境またはNSX-Tデプロイ環境とNSX-Vデプロイ環境の組み合わせに移動する場合、ポリシールールを再度作成することなく、既存のセキュリティポリシーをNSX-VからNSX-Tに拡張することができます。そのためには、既存のデバイスグループを活用して、NSX-VおよびNSX-Tサービス定義間でそれらを共有します。ポリシーをNSX-Tに移行

©2023 Palo Alto Networks, Inc.

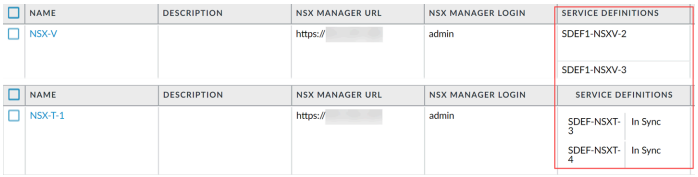
したら、NSX-VでVM-Seriesを使用し続ける、またはNSX-Vデプロイ環境を削除することができます。

STEP 1 | VMware NSX 用 Panorama プラグインのインストール 3.2.0以降。アップグレードする前に、「Panorama Plugin for VMware NSX 3.2.0リリースノートを参照してください。

STEP 2 | デプロイ環境内の各NSX-Vサービス定義に対して、NSX-Tサービス定義を設定します。新しいデバイスグループを作成しないでください。その代わりに、既存のNSX-Vデバイスグループを使用してください。既存のデバイスグループを使用することで、NSX-Vで使われていたのと同じセキュリティポリシールールを、NSX-TにデプロイされたVM-Seriesファイアウォールで利用することができます。特定のゾーンを参照するポリシーがある場合、NSX-Vサービス定義と同じテンプレートスタックを、NSX-Tサービス定義に追加してください。また、デバイスグループが特定のテンプレートを参照している場合は、デバイスグループで参照されているテンプレートを含むテンプレートスタックを選択していることを確認してください。



STEP 3 | NSX-Tサービス管理を設定して、NSX-Tサービス定義をサービスマネージャーに関連付けます。



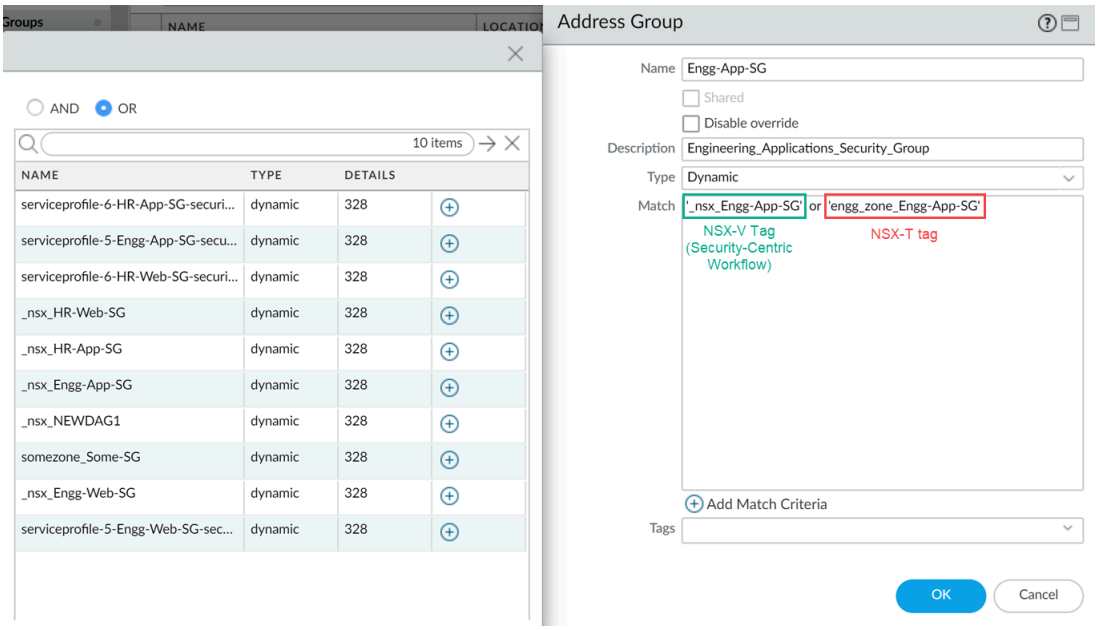
STEP 4 | NSX-T環境を準備して、VM-Seriesファイアウォールをデプロイします。VM-Seriesファイアウォールを起動する前に、セキュリティグループ、サービスチェーン、およびトラフィックリダイレクトポリシーを作成する必要があります。

- NSX-T（North-South）での VM-Series ファイアウォールのデプロイ
- 業務中心のワークフローを使用した VM-Series のデプロイ

©2023 Palo Alto Networks, Inc.

STEP 5 | 既存のダイナミックアドレスグループにNSX-Tタグを追加します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. 既存のNSX-Vダイナミックアドレスグループの名前をクリックします。
3. **Add Match Criteria**（一致条件の追加）をクリックして、NSX-VおよびNSX-Tのタグを表示します。
4. NSX-Tタグを、ダイナミックアドレスグループに追加します。タグ間には、**OR**演算子を使用してください。
5. 必要なタグをすべて追加したら、**OK**をクリックします。
6. 変更を **Commit (コミット)** します。



STEP 6 | NSX-VからNSX-TにVMワークフローが正常に移行された後、NSX-Vの使用を中止する場合は、ダイナミックアドレスグループからNSX-Vタグを削除してください。Panorama plugin for NSXからNSX-V関連の設定がすべて削除されると、NSX-Vタグと対応するIPアドレスの登録がすべて解除され、VM-Seriesファイアウォール設定がNSX-V Managerから削除されます。

©2023 Palo Alto Networks, Inc.

NSX-T（East-West）での VM-Series ファイアウォールのセットアップ

VMware NSX-T の VM-Series ファイアウォールは、Palo Alto 次世代ファイアウォールと Panorama を ESXi ホスト サーバーと統合し、NSX-T Software-Defined Data Center でのすべての East-West トラフィックの包括的な可視化と安全なアプリケーション有効化を提供します。

- NSX-T（East-West）での VM-Series ファイアウォールのコンポーネント
- NSX-T（East-West）での VM-Series ファイアウォール統合
- VMware NSX-T（East-West）でサポートされている VM-Series ファイアウォールのデプロイメント
- 業務中心のワークフローを使用した VM-Series のデプロイ
- セキュリティ中心のワークフローを使用した VM-Series のデプロイ
- Panorama からのサービス定義の削除
- NSX-T 運用上の VM-Series からのセキュリティ中心デプロイメントへの移行
- NSX-VからNSX-Tへのセキュリティ ポリシーの拡張
- NSX-VからNSX-TにVM-Seriesを移動するための定位置移行の使用

NSX-T（East-West）での VM-Series ファイアウォールのコンポーネント

以下の表は、この Palo Alto Networks と VMware NSX-T（East-West） の統合ソリューションを構成するコンポーネントを示しています。

VMware コンポーネント	
vCenter/ESXi	vCenter サーバーは、vSphere スイート用の中央管理ツールです。ESXi は、コンピュータの仮想化を実現するためのハイパーバイザーです。 vCenter の互換性については、ご利用のバージョンの NSX-T に応じた、VMware の互換性マトリックスを参照してください。
NSX-T Manager	VMware NSX-T Data Center 2.5.0 以降を、vCenter サーバーにインストールし、登録する必要があります。ESXi クラスタ内の ESXi ホストに VM-Series ファイアウォールをデプロイするには、NSX-T Manager が必要です。

©2023 Palo Alto Networks, Inc.

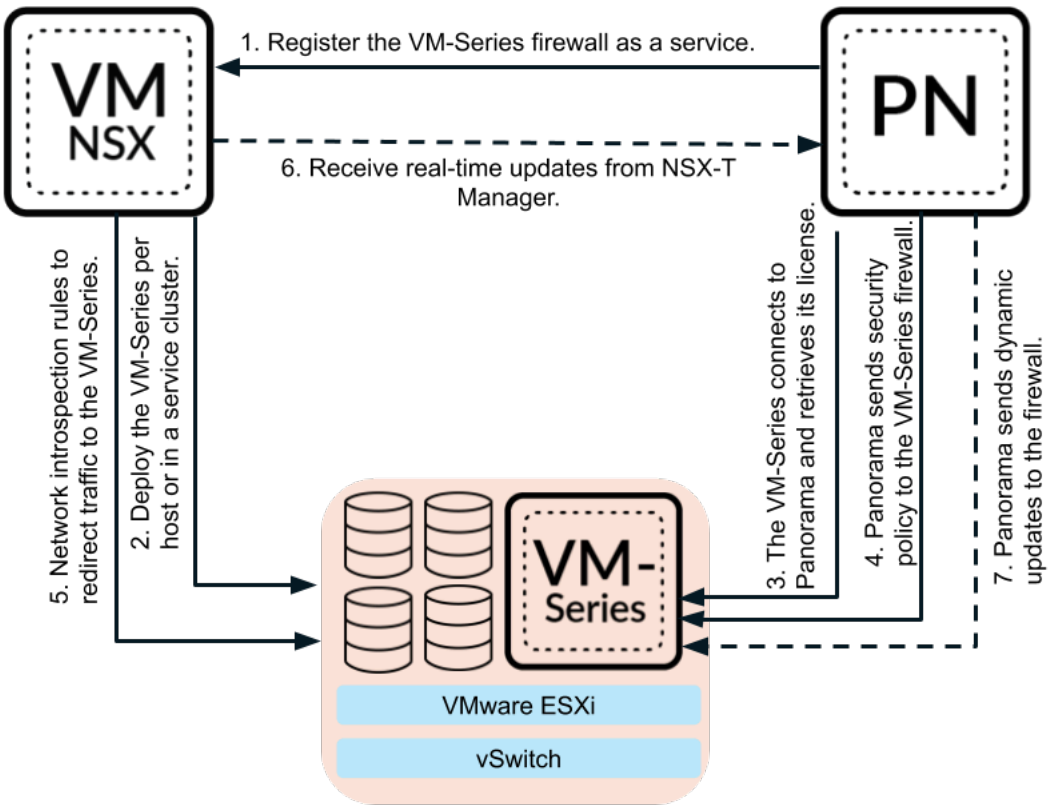
Palo Alto Networks コンポーネント	
PAN-OS	PAN-OS 10.1.x 以降。 VM-Series の基本イメージ（例: PA-VM-NSX-10.1.0.zip）は、NSX-T で VM-Series ファイアウォールをデプロイするのに必要です。 NSX 用の VM-Series ファイアウォールを ESXi サーバーにデプロイするための最小システム要件は、VM-Series モデルによって決まります。VM-Series モデルの最小ハードウェア要件については、「VM-Series モデル」を参照してください。
Panorama Panorama のバージョンは、管理対象ファイアウォールと同じかそれ以降のバージョンである必要があります。	NSX-T の VM-Series ファイアウォールには、10.1.0 が動作しているファイアウォールに対して、Panorama 10.1.0 以降が必要です。 Panorama は、Palo Alto Networks の次世代ファイアウォール用中央管理ツールです。このソリューションでは、Panorama が NSX-T Manager と連携して、NSX-T 用の VM-Series ファイアウォール上でデプロイ、ライセンスの付与、中央管理（設定やポリシー）を実行します。 Panorama が、NSX-T Manager、VM-Series ファイアウォール、および Palo Alto Networks 更新サーバーにアクセスできる必要があります。 Panorama アプライアンスのデプロイについては、「10.1 Panorama 管理者ガイド」を参照してください。
VMware NXS 用 Panorama プラグイン	3.1.0 以降 4.0.0 以降 （セキュリティ中心のワークフローの場合）
VM-Series プラグイン	1.0.8 以降
VM-Series ファイアウォール モデル	VM-100、VM-300、VM-500、および VM-700 が NSX-T をサポートします。

©2023 Palo Alto Networks, Inc.

Palo Alto Networks コンポーネント	
	NSX-T に *VM-Series* ファイアウォールをデプロイする前に、選択したデプロイ モデル（サービス クラスタ または ホスト単位）の *VM-Series* ファイアウォール数をサポートするために十分なハードウェア リソースがあることを確認してください。*VM-700* などの大規模なファイアウォールをデプロイする場合、このことは必須となります。

NSX-T（East-West）での VM-Series ファイアウォール統合

NSX-T Manager、vCenter、Panorama、および VM-Series ファイアウォールは連携して、NSX-T データ センターのセキュリティ上の課題に対処することができます。



©2023 Palo Alto Networks, Inc.

1. **VM-Series** ファイアウォールをサービスとして登録—VMware NSX-T Manager に接続するためにPanorama を使用します。Panorama は NSX-T API を使って NSX-T Manager と通信し、双方向の通信を確立します。Panorama で、Service Manager（サービス マネージャー）の設定を行うには、NSX-T Manager の IP アドレス、ユーザー名、およびパスワードを入力して通信を確立します。

   NSX-T Manager との通信を確立したら、サービス定義を設定します。サービス定義には、VM-Series ファイアウォール ベース イメージの場所、VM-Series ファイアウォールにライセンス供与するために必要な認証コード、およびファイアウォールが所属するデバイス グループとテンプレート スタックが含まれています。

   また、NSX-T Manager はこの接続を使って、NSX-T 環境の変更に関する更新情報を Panorama に送信します。

2. **VM-Series** ファイアウォールをホスト単位またはサービス クラスタ内にデプロイ—NSX-T Manager は、Panorama からプッシュ配信されたサービス定義内の情報を使って、VM-Series ファイアウォールをデプロイします。VM-Series ファイアウォールのデプロイ先（サービス クラスタ内または各 ESXi ホスト）、および NSX-T がVM-Seriesファイアウォールに管理 IP アドレスを提供する方法（DHCP またはスタティック IP）を選択します。ファイアウォールが起動したら、NSX-T Manager の API が、VM-Series ファイアウォールをハイパーバイザーに接続し、vSwitch からのトラフィックを受信できるようになります。

3. **VM-Series** が **Panorama** に接続—次に VM-Series ファイアウォールは、Panorama と接続してライセンスを入手します。Panorama は Palo Alto Networks アップデート サーバーからライセンスを受け取り、それをファイアウォールに送信します。ファイアウォールがライセンスを入手すると、再起動を行いシリアル番号が設定されます。

   > *Panorama* にインターネット接続がない場合、ライセンスを取得してファイアウォールに配信することはできません。その場合、各ファイアウォール個別に、手作業でライセンスを与える必要があります。*VM-Series* ファイアウォールにインターネット接続がない場合、*Panorama* に手動でシリアル番号を追加して、それらを管理対象デバイスとして登録します。そうすることによって、*Panorama* がテンプレート スタック、デバイス グループ、およびその他の設定情報をプッシュ配信できるようになります。詳細は、「VMware NSX 用 VM-Series ファイアウォールのライセンスのアクティベーション」を参照してください。

4. **Panorama** が **VM-Series** ファイアウォールにセキュリティ ポリシーを送信—ファイアウォールが Panorama に再接続したら、サービス定義に設定されているデバイス グループとテンプレート スタックに追加され、適切なセキュリティ ポリシーがファイアウォールにプッシュ配信されます。これで、ファイアウォールによる NSX-T データ センター内のトラフィックの保護準備が完了しました。

5. トラフィックを **VM-Series** ファイアウォールにリダイレクトするイントロスペクション ルールの作成 —NSX-T Manager で、NSX-T データ センター内のトラフィックをリダイレクトする、サービス チェーンとネットワーク インストロペクション ルールを作成します。

6. **NSX-T Manager** からのリアルタイム更新の送信 — NSX-T Manager が仮想環境内の変更に関するリアルタイムの更新情報を Panorama に送信します。これらの更新情報には、VM-Seriesにトラフィックを送信するグループの、グループ メンバーシップや仮想マシンの IP アドレスなどの変更が含まれています。

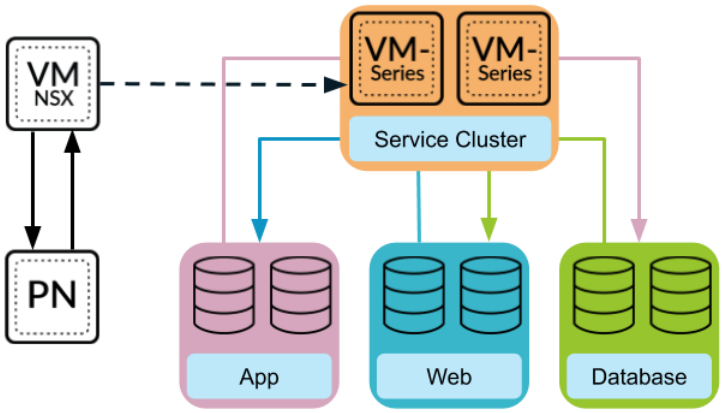
©2023 Palo Alto Networks, Inc.

7. **Panorama** がダイナミック更新を送信—Panorama が NSX-T Manager から更新情報を受信すると、これらの更新情報を管理対象 VM-Series ファイアウォールに送信します。Panorama は、指定した条件に基づいて仮想マシンをダイナミック アドレス グループに配置し、ダイナミック アドレス グループのメンバーシップ情報をファイアウォールにプッシュ配信します。そうすることで、NSX-T データセンター内の仮想マシンからのトラフィックに、適切なセキュリティ ポリシーを適用することができます。

VMware NSX-T（East-West）でサポートされている VM-Series ファイアウォールのデプロイメント

VMware NSX-T Data Center に、1 つ以上の VM-Series ファイアウォール インスタンスをパートナー サービスとしてデプロイして、East-West トラフィックを保護して、マイクロ セグメンテーションを実行することができます。マイクロセグメンテーションを実行する目的で VM-Series ファイアウォールを設定するために、サービス クラスタ内またはホスト単位にファイアウォールをデプロイすることができます。

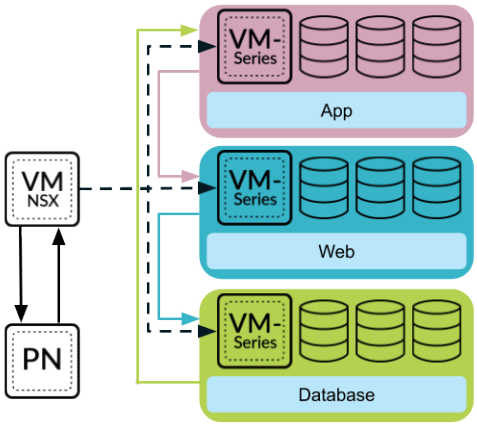
- **Service Cluster**（サービス クラスタ）—クラスタ化されたデプロイ環境では、すべての VM-Series ファイアウォールが単一のクラスタにインストールされます。VM およびグループ間のトラフィックは、宛先に転送される前に、ポリシーの検査、適用のために VM-Series クラスタにリダイレクトされます。クラスタ化されたデプロイ環境を設定する場合、クラスタ内の特定のホストを指定するか、または **Any**（任意）を選択して NSX-T にホストを選択させることができます。



- **Host-Based**（ホスト ベース）—ホスト単位のデプロイ環境の場合、VM-Series ファイアウォールのインスタンスは ESXi クラスタ内の各ホストにインストールされます。同じホスト上のゲスト間のトラフィックはローカル ファイアウォールで検査されるため、検査のために

©2023 Palo Alto Networks, Inc.

ホストから移動する必要はありません。ホストから出て行くトラフィックは、vSwitch に到達する前にファイアウォールが検査を行います。



ファイアウォールのデプロイが完了したら、トラフィックを VM-Series ファイアウォールに送信するトラフィック リダイレクト ルールを設定します。Panorama で設定したセキュリティ ポリシー ルールは管理対象 VM-Series ファイアウォールにプッシュされ、ファイアウォールを通過するトラフィックに適用されます。

VM-Series ファイアウォールを VMwareNSX-T にデプロイするには、業務中心およびセキュリティ中心のデプロイメントの 2 つのワークフローオプションがあります。

- 業務中心 - 業務中心のワークフローでは、デプロイメント手順の一部は Panorama で実行され、残りは NSX-T Manager で実行されます。Panorama では、最初に Panorama と NSX-T Manager 間の通信を有効にし、サービス定義を構成して、VM-Series ファイアウォールを起動する必要があります。次に、NSX-T Manager にログインして、サービスチェーンとステアリングルールを作成して構成を続行する必要があります。VM-Series のデプロイメントを完了するには、Panorama に戻ってセキュリティポリシーを作成する必要があります。
- セキュリティ中心 – セキュリティ中心のワークフローでは、Panorama を単一のガラス板として使用して、セキュリティ操作を制御および管理できます。Panorama からデプロイメントワークフロー全体を完了します。VMware NSX 用の Panorama プラグインは、サービスチェーンとステアリングルールを作成する NSX-TManager に構成をプッシュします。

使いやすいように、NSX-T での VM-Series のデプロイメントに 1 つのデプロイメントワークフローを選択することをお勧めします。ただし、VMware NSX-T 用の VM-Series ファイアウォールは、同じプラグインでの両方のワークフローの使用をサポートします。

業務中心のワークフローを使用した VM-Series のデプロイ

VM-Series ファイアウォールをデプロイして、NSX-T データ センターの North-South トラフィックを保護するには、以下の作業を行います。

- VMware NSX 用 Panorama プラグインのインストール
- NSX-T Manager と Panorama 間の通信の有効化
- Panorama でのテンプレート スタックとデバイス グループの作成
- Panorama でのサービス定義の設定

©2023 Palo Alto Networks, Inc.

- NSX-T（East-West）での VM-Series ファイアウォールの起動
- サービスチェーンの追加
- VM-Series ファイアウォールへのトラフィックの転送
- NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用
- ホスト間でVM-Seriesファイアウォールを移動するためのvMotionの使用

VMware NSX 用 Panorama プラグインのインストール

VMware NSX 用 Panorama プラグインをダウンロードしてインストールします。プラグインをインストールまたはアップグレードする前に、「互換性マトリックス」を参照してください。

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。Panorama HA ピアにプラグインをインストールする際には、プラグインを最初にパッシブ ピアにインストールしてから、アクティブ ピアにインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 1 | **Panorama** > プラグインを選択します。

STEP 2 | **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。

STEP 3 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 4 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。

NSX-T Manager と Panorama 間の通信の有効化

Panorama と NSX-T Manager 間の通信を有効にするには、以下の手順を実行します。Panorama を最大16台のNSX-T Managerに接続できます。Panorama を複数のNSX-T Managerに接続する場合は、デバイスグループ階層とテンプレートスタックを慎重に計画し、デプロイメントに必要な他のコンポーネントとどのように対話するのかを検討する必要があります。サービス定義は、デバイス グループとテンプレート スタックを参照し、その情報を関連する ESXi クラスターのファイアウォールにプッシュします。

STEP 1 | （任意）Panorama と NSX-V Manager 間の通信のため、Panorama の **Panorama** > **Setup**（セットアップ） > **Services**（サービス） > **Proxy Server**（プロキシ サーバー）で構成されたプロキシ サーバー設定をバイパスします。このコマンドを実行すると、Panorama が NSX-V Manager と直接通信しながら、他のサービスのためにプロキシ通信は維持されます。

1. Panorama CLI にログインします。

©2023 Palo Alto Networks, Inc.

2. プロキシ バイパスを有効または無効にするには、以下のコマンドを実行します。

   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}

   プロキシ バイパスを有効にする場合は **yes** を選択し、無効にする場合は **no** を選択します。これはデフォルトで**no**が設定されます。

STEP 2 | Panorama Web インターフェイスにログインします。

Web ブラウザから安全な接続（https）を使用し、初期設定時に割り当てられた IP アドレスとパスワードを使用してログインします（https://<*IP address*>）。

STEP 3 | NSX-T Manager へのアクセスをセットアップします。Panorama を接続するNSX-T Managerごとにこの手順を繰り返します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択し、**Add**（追加）をクリックします。
2. **Name**（名前）に分かりやすい NSX-T Manaer 名を入力します。
3. （任意）NSX-T Managerの説明を追加します。
4. NSX-T Managerにアクセスするための**NSX Manager URL**（NSX-T Manager cluster 仮想 IP アドレスまたは FQDN）を入力します。
5. Panorama が NSX-T Manager への認証を行えるように **NSX Manager Login**（**NSX Manager** ログイン）に認証情報（ユーザー名とパスワード）を入力します。
6. **OK**をクリックします。

NSX-T Manager のログイン用パスワードを変更する場合、必ず *Panorama* 上のパスワードを即座に更新してください。パスワードが間違っていると、*Panorama* および *NSX-T Manager* 間で通信できなくなります。

STEP 4 | 変更を Panorama にコミットします。

Commit (コミット) および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | Panorama の接続状態を確認します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択します。
2. **Status**（ステータス）列のメッセージを確認します。

   接続が成功すると、状態は **Registered**（登録済み）と表示されます。これは、Panorama と NSX-T Manager が同期していることを示します。

   失敗した状態では、以下のメッセージが表示されます。

   - **No connection**（接続なし）:NSX-T Manager にアクセスできないか、NSX-T Manager へのネットワーク接続を確立できません。
   - **Invalid Credentials**（無効な認証情報）:アクセス認証情報（ユーザー名/パスワード）が正しくありません。
   - **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-T Manager に定義されている設定と異なります。リンクをクリックして失敗の原因を確認してください。たとえば、NSX-T 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-T Manager のサービス定義の検証を行います。Panorama と NSX-T 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。
   - **Connection Disabled**（接続が無効）:Panorama と NSX-T Manager 間の接続が手動で無効にされています。

Panorama でのテンプレート スタックとデバイス グループの作成

Panorama を使用して NSX-T 用の VM-Series ファイアウォールを管理するには、ファイアウォールがデバイス グループおよびテンプレート（テンプレート スタックのメンバー）に属している必要があります。デバイス グループでは、同様のポリシーとオブジェクトが必要なファイアウォールを論理的なユニットとしてグループ化できます。この設定は Panorama の **Objects**（オブジェクト）タブと **Policies**（ポリシー）タブを使用して定義します。テンプレート スタックを使用して、VM-Series ファイアウォールがネットワーク上で動作するのに必要な設定を構成してから、関連付けを行います。この設定は、Panorama の **Device**（デバイス）タブと **Network**（ネットワーク）タブを使用して定義します。また、Panorama の NSX-T 設定で使用されるゾーンを持つ各テンプレート スタックは、サービス定義に関連付ける必要があります。最低でも、テンプレート スタック内にゾーンを作成し、NSX-T Manager が VM-Series ファイアウォールにトラフィックをリダイレクトできるようにする必要があります。

Panorama は、NSX-T North-South および NSX-T East-West の両方のデプロイメントを同時にサポートできます。NSX-T North-South および NSX-T East-West に対して、個別のデバイス グループ、テンプレート スタック、およびサービス定義を設定することをお勧めします。

 ©2023 Palo Alto Networks, Inc.

STEP 1 | デバイスグループあるいはデバイスグループの階層を追加します。

1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、**Add**（追加）をクリックします。デバイス グループの階層を作成することもできます。
2. デバイス グループを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット）をクリックした後、**Commit Type**（コミット タイプ）として **Panorama** を選択し、Panorama で実行中の設定に対する変更を保存します。

STEP 2 | テンプレートを追加します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add**（追加）をクリックします。
2. テンプレートを識別するために、一意の **Name**（名前）と **Description**（説明）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

STEP 3 | テンプレート スタックを作成します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add Stack**（スタックの追加）をクリックします。
2. テンプレートを識別するために、一意の **Name**（名前）と **Description**（説明）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット） をクリックし、**Commit to Panorama**（**Panorama**に非ミット） を選択して、Panorama で実行中の設定に変更を保存します。

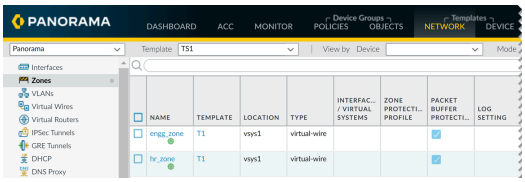
©2023 Palo Alto Networks, Inc.

STEP 4 | 各テンプレートのゾーンを作成します。

各ゾーンは、NSX-T Manager 上でサービス プロファイルにマッピングされます。ゾーンを認可するには、ゾーンがバーチャル ワイヤ タイプであり、かつサービス定義に関連付けられたテンプレートでなければなりません。

各テンプレートにつき最大 32 のゾーンを追加できます。

1. **Network**（ネットワーク） > **Zones**（ゾーン）を選択します。
2. **Template**（テンプレート）のドロップダウン リストから、適切なテンプレートを選択します。
3. **Add**（追加）を選択し、ゾーンの **Name**（名前）を入力します。
4. インターフェイスの **Type**（タイプ）を **Virtual Wire**（バーチャル ワイヤ）に設定します。
5. **OK**をクリックします。
6. ゾーンが正しいテンプレートに追加されていることを確認します。



7. **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

   Panorama により、コミット時に認可されたゾーンごとに、対応するサービス プロファイルが NSX-T Manager 上で作成されます。

STEP 5 | テンプレートスタックの DNS および NTP サーバ情報を更新します。デプロイメントでデバイス証明書を使用している場合は、この手順を完了する必要があります。これは、NSX-T 環境にデプロイされたファイアウォールに、デバイス証明書サーバに到達するために必要な正しい DNS 情報があることを確認するために必要です。

1. [テンプレート] ドロップダウンから正しいテンプレートスタックを指定したことを確認します。
2. デバイス > セットアップ > サービスを選択して、[編集]アイコンをクリックします。
3. [サービス] タブで、プライマリ **DNS** サーバーおよびセカンダリ **DNS** サーバーの IP アドレスを入力します。
4. [NTP] タブで、**NTP** サーバーの IP アドレスを入力します。
5. **OK** をクリックします。
6. 変更を Panorama にコミットします。

Panorama でのサービス定義の設定

サービス定義は、NSX-T データ センター環境にインストールされている VM-Series ファイアウォール用の構成を指定しています。サービス定義には、デバイス グループ、テンプレート スタック、および OVF URL を含める必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | （任意）通知グループを設定します。

仮想環境の変更を通知する必要があるデバイス グループを指定して、通知グループを作成します。指定したデバイス グループに含まれるファイアウォールは、セキュリティ グループとそのグループ内のゲスト VM の IP アドレスのリアルタイム更新を受信します。ファイアウォールは、この更新を使用してポリシーで参照しているダイナミック アドレス グループを構成する最新メンバー リストを決定します。

1. **Panorama** > **VMware** > **Notify Group**（通知グループ）を選択し、**Add**（追加）をクリックします。
2. 通知グループに分かりやすい **Name**（名前）を付けます。
3. 仮想環境の変更を通知する必要があるデバイス グループのボックスをすべて選択します。デバイス グループのチェック ボックスを選択できない場合は、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。
4. **OK**をクリックします。

STEP 2 | 新しいサービス定義を追加します。

*Panorama*で最大*32*のサービス定義を作成できます。

1. **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（サービス定義）を選択します。
2. **Add**（追加）を選択して、新しいサービス定義を作成します。
3. **Name**（名前）に分かりやすいサービス定義名を入力します。
4. （任意）このサービス定義を使用してデプロイされる VM-Series ファイアウォールの機能あるいは目的が分かるような **Description**（説明）を追加します。

STEP 3 | デバイス グループとテンプレート スタックをサービス定義用に割り当てます。

必ずPanorama でのテンプレート スタックとデバイス グループの作成を行うようにしてください。

このソリューションでデプロイされるファイアウォールは、Panorama から集中管理されるため、ファイアウォールが属する **Device Group**（デバイス グループ）と **Template Stack**（テンプレート スタック）を指定する必要があります。このサービス定義を使用してデプロイされるすべてのファイアウォールは、指定したテンプレート スタックおよびデバイスグループに属します。

1. **Device Group**（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あるいはデバイスグループの階層を選択します。
2. **Template**（テンプレート） ドロップダウンでテンプレート スタックを選択します。

   あるサービス定義に割り当てられたテンプレート スタックあるいはデバイスグループを他のサービス定義で利用することはできません。

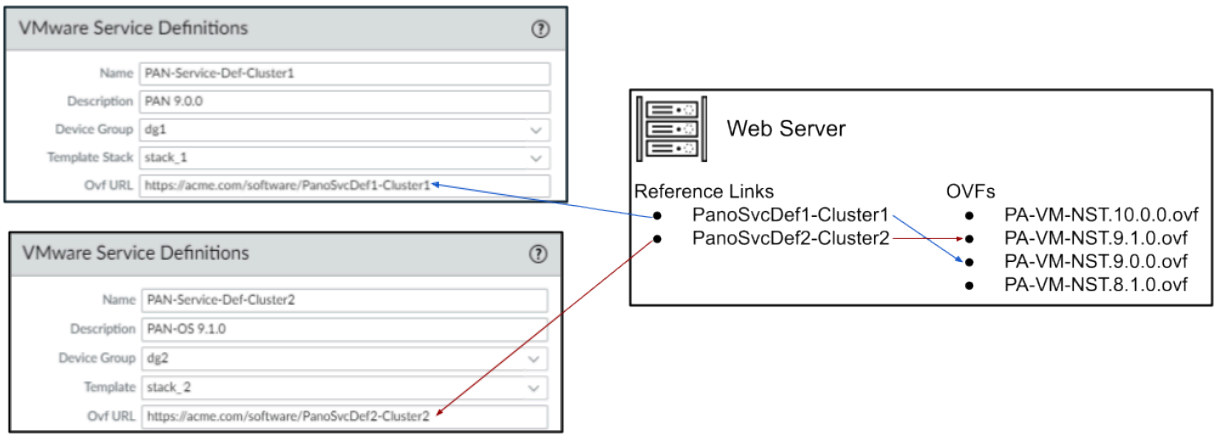
©2023 Palo Alto Networks, Inc.

STEP 4 | OVF ファイルの場所を指定します。

zip ファイルをダウンロードして解凍し、.ovf、mf、および .vmdk の各ファイルを抽出して、同じディレクトリに保存します。ovf および vmdk ファイルはファイアウォールの各インスタンスのデプロイに使用されます。

> *VM-Series* ファイアウォールの *NSX* サービスのデプロイメントが正常に完了した後は、*Panorama* サービス定義の *OVF* パスを変更しないでください。*VM-Series* ファイアウォールのデプロイメントが正常に完了した後に *OVF* パスを変更すると、*NSX* サービスデプロイメントが失敗した状態になる可能性があります。*NSX-T Manager* でこの問題を解決できますが、これにより、すべての *VM-Series* ファイアウォールが再デプロイされる可能性があります。

デプロイされたファイアウォールに影響を与えることなく、スケーリングしてベースイメージを変更できる OVF パス名を使用することをお勧めします。**https://acme.com/software/PA-VM-NST.9.1.0.ovf** などのパスの代わりに、**https://acme.com/software/PanoSvcDef1-Cluster1.ovf** などを使用します。スタティックパス参照を使用すると、OVF パスを変更する必要がなくなります。デプロイメント内の各 Panorama サービス定義 （vSphere クラスター） のパスを作成し、必要に応じて Web サーバー上の PAN-OS ベースイメージ参照を変更することをお勧めします。



OVF URL に、OVF ファイルをホストする Web サーバーの場所を追加します。http および https の両方がサポートされています。

同じ ovf バージョンあるいは異なるバージョンをすべてのサービス定義で使用することができます。異なるバージョンの ovf を各サービス定義で使用することにより、異なる ESXi クラスタ内の VM-Series ファイアウォールの PAN-OS のバージョンを変えることができます。

STEP 5 | （任意）**Notify Group**（通知グループ）を選択します。

STEP 6 | ファイアウォールの **Insertion Type**（挿入タイプ）として **East West** を選択します。

©2023 Palo Alto Networks, Inc.

STEP 7 | （任意）**Enable**（有効）を選択して、**Health Check**（ヘルス チェック）を有効にします。VMware NSX 3.2.0 以降の Panorama プラグインでは、ヘルスチェックはデフォルトで有効になっています。古いバージョンのプラグインでは、ヘルスチェックはデフォルトで無効になっています。サービス ヘルス チェックとも呼ばれる、この NSX-T 機能により、サービス インスタンスに障害が発生した場合の高可用性をシミュレートすることができます。VM-Series ファイアウォールで設定する場合、VM-Series サービス インスタンスに障害が発生すると、そのファイアウォールに転送されたトラフィックは、クラスタ内の別のファイアウォール インスタンス（サービス クラスタ デプロイの場合）、または他のホスト上のファイアウォール インスタンス（ホスト ベースのデプロイの場合）にリダイレクトされます。

> *NSX-T* で *VM-Series* ファイアウォールのコミットとデプロイを行った後は、サービス定義内でヘルス チェックを有効化/無効化することはできません。ヘルス チェック設定の変更をコミットしても、コミット失敗のメッセージが返されます。変更するには、サービス定義を削除した後再作成して、*VM-Series* ファイアウォールを再度デプロイする必要があります。

STEP 8 | NSX ManagerがVM-Seriesファイアウォールをデプロイする時に、自動的にデバイス証明書を取得するには、デバイス証明書を設定します。

新たにデプロイされたVM-Seriesファイアウォールにデバイス証明書を適用するには、このオプションを有効にします。デバイス証明書をサポートするベースイメージOVFを使ってファイアウォールをデプロイする場合にのみ、このオプションを使用してください。Panoramaは、サービス定義の一環として、NSX Managerにデバイス証明書情報をプッシュ配信します。NSXに新たなファイアウォールがデプロイされた場合、ブートアップ時にファイアウォールにデバイス証明書がインストールされます。

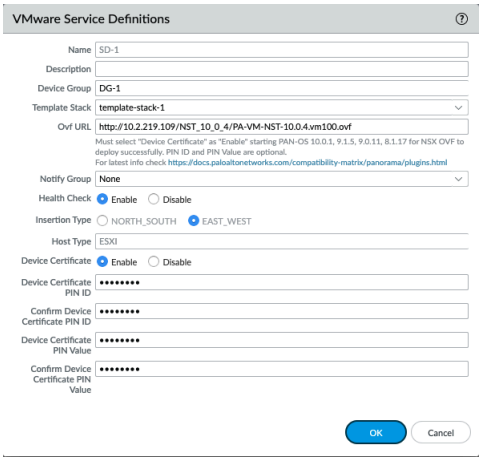
VMware NSX上のVM-Seriesファイアウォールに対するデバイス証明書をサポートしているOVFの一覧については、「Palo Alto Networks互換性マトリックス」を参照してください。

OVF がデバイス証明書をサポートしている場合は、デバイス証明書を使用しているかどうかに関係なく、デバイス証明書を有効にする必要があります。OVFがデバイス証明書をサポートしていない場合は、このオプションを無効にしてください。

1. まだ作業を行っていない場合は、カスタマーサポートポータルにログインして、Registration PINおよびPIN IDを生成します。
2. **Device Certificate**（デバイス証明書）下で、**Enable**（有効）をクリックします。
3. PIN IDをコピーして、それを**Device Certificate PIN ID**（デバイス証明書**PIN ID**）フィールドに入力します。
4. **Confirm Device Certificate PIN ID**（デバイス証明書**PIN ID**の再入力）フィールドに、PIN IDをもう一度入力します。
5. PIN Valueをコピーして、それを**Device Certificate PIN Value**（デバイス証明書**PIN**値）フィールドに入力します。
6. **Confirm Device Certificate PIN Value**（デバイス証明書**PIN**値の再入力）フィールドに、PIN値をもう一度入力します。

©2023 Palo Alto Networks, Inc.

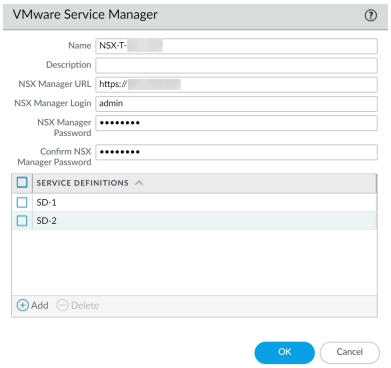
STEP 9 | **OK** をクリックしてサービス定義を保存します。



STEP 10 | サービス定義をサービス マネージャーにアタッチします。

1 つのサービス定義を、複数のサービス マネージャー内で使用することはできません。

1. **Panorama** > **VMware** > **NSX-T** > **Service Manager**（サービス マネージャー）を選択し、サービス マネージャー名のリンクをクリックします。
2. Service Definitions（サービス定義）で **Add**（追加）をクリックし、ドロップダウンからサービス定義を選択します。
3. **OK** をクリックします。



STEP 11 | 認証コードを追加してファイアウォールをライセンス登録します。

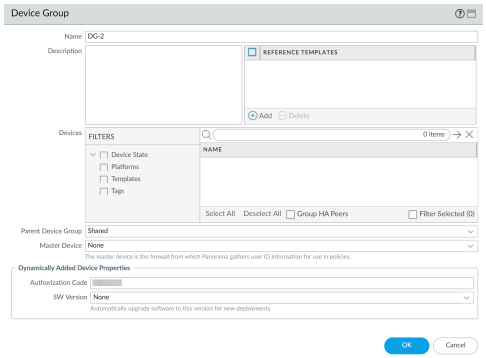
1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、作成したサービス定義に関連付けられているデバイス グループを選択します。
2. **Dynamically Added Device Properties**（動的に追加されたデバイス プロパティ）の下で、受注完了電子メールで受け取った認証コードを追加します。任意で **SW**

©2023 Palo Alto Networks, Inc.

Version（**SW** バージョン）のドロップダウン リストから None（なし）を選択します。

NSX-T に新しいファイアウォールがデプロイされると、それがデバイス グループに自動的に追加され、指定した認証コードを使ってライセンスが供与され、指定したバージョンの PAN-OS にアップグレードされます。

サポート ポータルで、デプロイ可能なファイアウォールの総数および認証コードで使用可能なライセンス総数に対する使用済みライセンス数の比率を表示できます。



STEP 12 | **Commit to Panorama**（**Panorama** へのコミット）によってコミットします。

STEP 13 | NSX-T Manager で、サービス定義が使用可能であることを確認します。

System（システム） > **Service Deployments**（サービスのデプロイ） > **Catalog**（カタログ）を選択します。サービス定義が NSX-T Manager にサービス インスタンスとしてリストアップされます。

NSX-T（East-West）での VM-Series ファイアウォールの起動

VM-Series ファイアウォールを NSX-T 環境のサービスとしてデプロイするには、以下の手順を実行します。**Deployment Specification**（デプロイの仕様）および **Deployment Template**（デプロイ テンプレート） フィールドには、サービス定義の一環として Panorama からプッシュ配信される情報が自動的に記入されます。

Deployment Attributes（デプロイ属性）下の設定は、どれも変更しないでください。これらの値は *Panorama*からインポートされ、それを変更するとデプロイが失敗してしまいます。

STEP 1 | NSX-T Manager にログインします。

STEP 2 | **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Deployment**（デプロイ）を選択します。

STEP 3 | **Partner Service**（パートナー サービス）ドロップダウンから、サービス定義を選択します。

STEP 4 | **Deploy Service**（サービスのデプロイ）をクリックします。

STEP 5 | **Name**（名前）に分かりやすいサービス デプロイ環境名を入力します。

©2023 Palo Alto Networks, Inc.

STEP 6 | **Compute Manager**（vCenter）を選択します。

STEP 7 | **Deployment Type**（デプロイ タイプ）として、**Clustered**（クラスタ）または **Host Based**（ホスト ベース）を選択します。

STEP 8 | **Deployment Type**（デプロイ タイプ）として**Clustered**（クラスタ）を選択した場合、**Clustered Deployment Count**（クラスタ化されたデプロイ数）にクラスタにデプロイする VM-Series ファイアウォール インスタンス数を指定します。

STEP 9 | クラスタ デプロイ環境内で VM-Series を起動する場合、**Host**（ホスト）を選択します。**Host**（ホスト）ドロップダウンから特定のホストを選択するか、または NSX-T Manager にホストを選択させる場合は、**Any**（任意）を選択します。**Per Host**（ホスト単位）のデプロイの場合、このオプションは灰色表示になります。

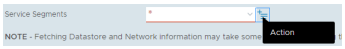
STEP 10 | VM-Series ファイアウォールのリポジトリとして、**Data Store**（データ ストア）を選択します。クラスタ デプロイ環境で、ホストに対して **Any**（任意）を選択した場合は共有データストアを選択します。特定のホストを指定した場合は、ローカル データ ストアを選択します。

STEP 11 | **Networks**（ネットワーク）の設定を行います。

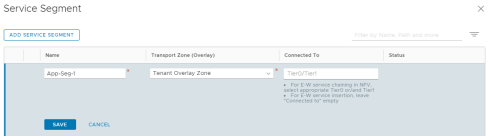
1. Networks（ネットワーク）列で、**Set**（設定）をクリックします。
2. **eth0 - Management Nic** に対して **Network**（ネットワーク）を選択します。
3. **Network Type**（ネットワーク タイプ）として、DHCP または Static IP Pool（スタティック IP プール）を選択します。スタティック IP プールを選択した場合、**IP Pool**（**IP** プール）を選択します。
4. **eth1 - Data-1 Nic** を選択します。
5. **Save**（保存）をクリックします。

STEP 12 | **Service Segment**（サービス セグメント）を設定または選択します。サービス セグメントを設定するには、以下の手順を実行します。

1. **Service Segments**（サービス セグメント）列で、**Action**（アクション）をクリックします。



2. **Add Service Segment**（サービス セグメントの追加）をクリックします。
3. 分かりやすい **Name**（名前）を入力します。
4. **Transport Zone**（**Overlay**）（トランスポート ゾーン（オーバーレイ））を選択します。
5. **Save**（保存）をクリックして、**Close**（閉じる）をクリックします。



STEP 13 | サービスをデプロイする**Cluster**（クラスタ）を選択します。**NSX Configuration**（**NSX** 設定）でクラスタを選択する必要があります。

©2023 Palo Alto Networks, Inc.

STEP 14 | **Save**（保存）をクリックします。

STEP 15 | ファイアウォールのデプロイが正常に完了したことを確認します。

1. **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Service Instances**（サービス インスタンス）を選択します。
2. ファイアウォールが記載されており、**Deployment Status**（デプロイ ステータス）が **Up** になっていることを確認します。

STEP 16 | ファイアウォールが Panorama に接続されていることを確認します。

1. Panoramaにログインします。
2. **Panorama** > **Managed Devices**（管理対象デバイス） > **Summary**を選択します。
3. ファイアウォールが適切なデバイス グループ下に記載されており、**Device State**（デバイス状態）が **Connected**（接続）になっていることを確認します。

サービスチェーンの追加

サービスチェーンは、論理シーケンス内のサービスセットのグループです。トラフィックがサービスチェーンにリダイレクトされた場合、それは設定した順序に応じて各サービスを通過していきます。

STEP 1 | **Security**（セキュリティ） > **Network Introspection Settings**（ネットワーク診断設定） > **Service Chains**（サービスチェーン） > **Add Chain**（チェーンの追加）を選択します。

STEP 2 | サービスチェーンに対する、分かりやすい**Name**（名前）および**Description**（説明）（任意）を入力します。

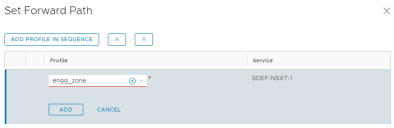
STEP 3 | VM-Seriesファイアウォールのデプロイ時に適用した、**Service Segment**（サービスセグメント）を選択します。

 ©2023 Palo Alto Networks, Inc.

STEP 4 | 転送パスを設定します。サービスチェーンは、サービスプロファイルの論理的なシーケンスです。トラフィックは、転送パスとして指定した順序で、各サービスを通過していきます。

1. **Set Forward Path**（転送パスの設定） > **Add Profile in Sequence**（シーケンスにプロファイルを追加）を選択します。
2. サービスプロファイルを選択します。サービス列は、選択したサービスプロファイルに応じて自動的に記入されます。
3. **[追加]** をクリックします。
4. （任意）NSX-T環境にその他のパートナーサービスプロファイルがある場合、**Add Profile in Sequence**（プロファイルをシーケンスに追加）をクリックして、それらをサービスチェーンに追加します。

   サービス定義あたり、*1*つのサービスプロファイルのみを選択することができます。
5. サービスプロファイルの追加が完了したら、**Save**（保存）をクリックします。



STEP 5 | Reverse Path（逆向きのパス）列で、サービスチェーン内でトラフィックを逆向きに返すには、**Inverse ForwardPath**（転送パスを逆にする）を選択します。

STEP 6 | （任意）他のパートナーサービスプロファイルが選択されている場合、逆向きのパスを設定します。

Forward Path（転送パス）に設定したのと同じ*VM-Series*サービスプロファイルを選択する必要があります。

1. **Set Reverse Path**（逆向きパスの設定） > **Add Profile in Sequence**（シーケンスにプロファイルを追加）を選択します。
2. サービスプロファイルを選択します。サービス列は、選択したサービスプロファイルに応じて自動的に記入されます。
3. **[追加]** をクリックします。
4. （任意）NSX-T環境にその他のサービスプロファイルがある場合、**Add Profile in Sequence**（プロファイルをシーケンスに追加）をクリックして、それらをサービスチェーンに追加します。
5. サービスプロファイルの追加が完了したら、**Save**（保存）をクリックします。

STEP 7 | **Failure Policy**（障害ポリシー）を **Allow**（許可）または**Block**（ブロック）に設定します。これは、サービスプロファイルが失敗した場合に、NSX-Tが実施するアクションを定義しています。

STEP 8 | **Save**（保存）をクリックします。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールへのトラフィックの転送

トラフィック仮想マシンまたは仮想マシンのグループをVM-Seriesファイアウォールに誘導するポリシールールを構成します。

STEP 1 | **Security**（セキュリティ） > **Network Introspection**（**E-W**）（ネットワーク診断） > **Rules**（ルール） > **Add Policy**（ポリシーの追加）を選択します。

STEP 2 | **New Policy**（新しいポリシー） をクリックして、ポリシーにわかりやすい名前を付けます。

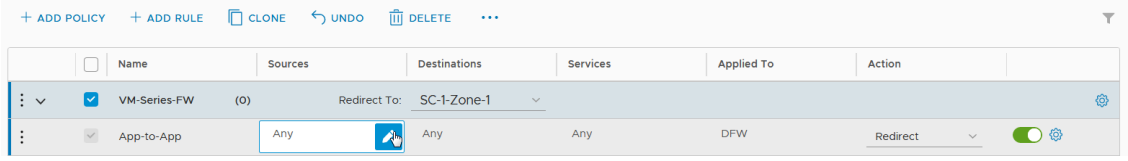
STEP 3 | リダイレクト先 ドロップダウンからサービスチェーンを選択します。

STEP 4 | ポリシーを選択し、**Add Rule**（ルールの追加） をクリックします。

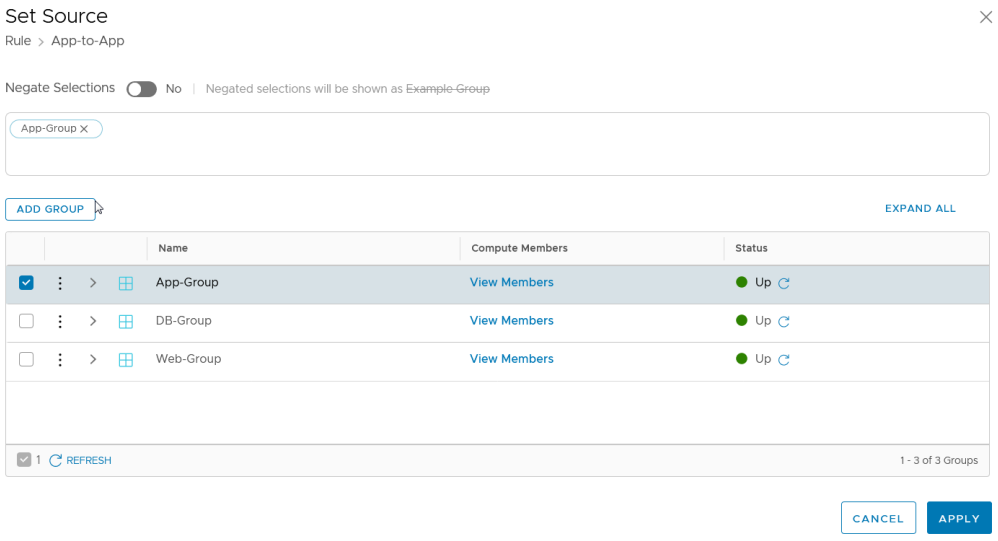
STEP 5 | **New Rule**（新しいルール） をクリックして、ルールにわかりやすい名前を付けます。

STEP 6 | 送信元を選択します。

1. 送信元の列の鉛筆アイコンをクリックして、仮想マシンのソースグループを選択します。



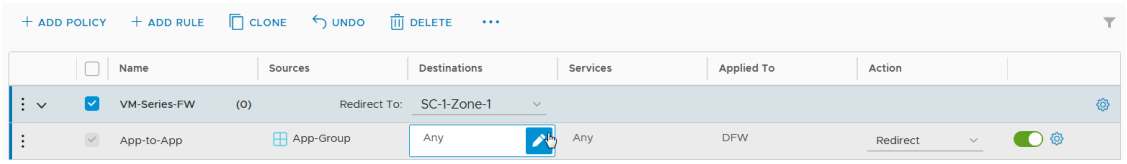
2. 送信元のグループを確認してください。
3. **Apply**[適用] をクリックします。



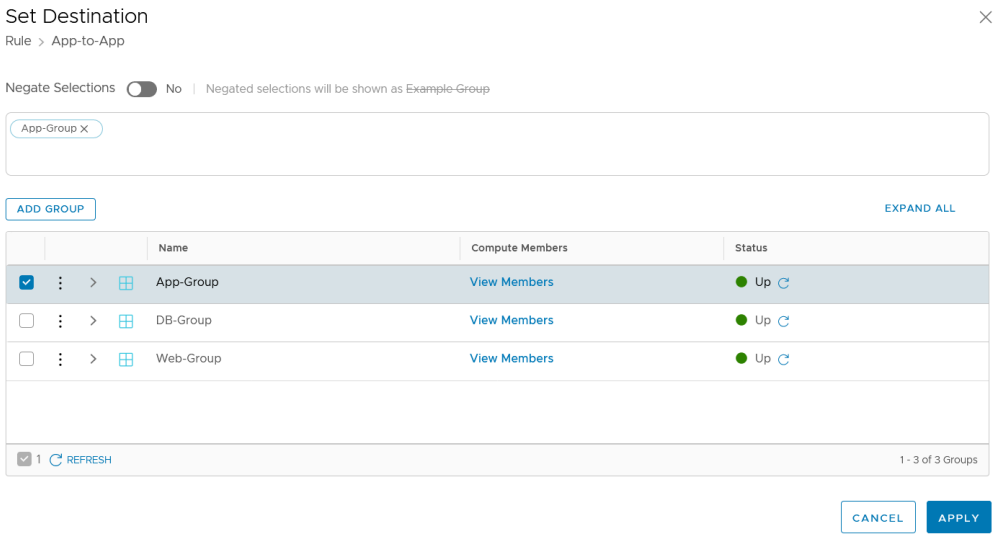
 ©2023 Palo Alto Networks, Inc.

STEP 7 | **Destination**（宛先）を選択します。

1. 宛先の列の鉛筆アイコンをクリックして、仮想マシンのソースグループを選択します。



2. 宛先グループを確認してください。
3. **Apply**[適用] をクリックします。



STEP 8 | （任意）ルールを適用する**Services**（サービス） を選択します。

STEP 9 | 適用先 フィールドで次のいずれかを選択します。

- **DFW** を選択して、論理スイッチに接続されているすべての仮想 NIC にルールを適用します。
- 指定した1つまたは複数のグループのメンバー仮想マシンの仮想 NIC にルールを適用するには、**Groups**（グループ） を選択します。

STEP 10 | アクション—リダイレクト または リダイレクトしない を選択します。

STEP 11 | **Publish**（公開）をクリックします。

STEP 12 | このプロセスを繰り返して、追加のポリシーまたはルールを作成します。

NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用

NSX-T Managerでリダイレクトルールを作成したので、Panorama を使用して VM-Series ファイアウォールのポリシーを一元的に管理できるようになりました。

ポリシーを一元的に管理するには、ダイナミック アドレス グループをセキュリティポリシーの送信元アドレスまたは宛先アドレスとして適用し、ファイアウォールにプッシュします。ファイアウォールは、各セキュリティグループに含まれる仮想マシンの IP アドレスを動的に取得する

©2023 Palo Alto Networks, Inc.

ことができ、指定されたグループにある仮想マシンからのトラフィックまたは仮想マシンへのトラフィックにコンプライアンスを適用します。

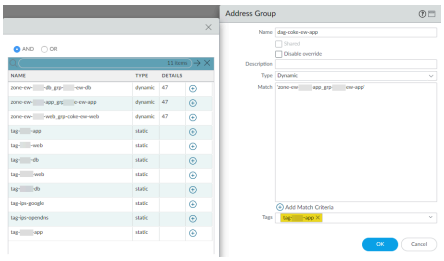
STEP 1 | Panorama にログインします。

STEP 2 | ダイナミック アドレス グループを作成します。

1. **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. NSX-T ファイアウォールで VM-Series 管理のために作成したデバイス グループを **Device Group**（デバイス グループ）から選択します。
3. **Add**（追加）をクリックし、ダイナミック アドレス グループの **Name**（名前）および **Description**（説明）を入力します。
4. **Type**（タイプ）で **Dynamic**（ダイナミック）を選択します。
5. ダイナミック アドレス グループに一致条件を追加します。

   一部のブラウザ拡張機能が、*Panorama* と *NSX-T* の間の *API* コールをブロックすることがあります。これが原因で、*Panorama* は一致条件を受信できなくなります。ブラウザ拡張機能を使用しているときに *Panorama* で一致条件が表示されない場合は、その拡張機能と *Synchronize Dynamic Objects*（動的オブジェクトの同期）を無効にして、*Panorama* に対して使用可能なタグを取り込みます。
6. **Add Match Criteria**（一致条件の追加）をクリックします。
7. **And** 演算子または **Or** 演算子を選択し、セキュリティ グループ名の横にあるプラス（+）アイコンをクリックして、ダイナミック アドレス グループに演算子を追加します。

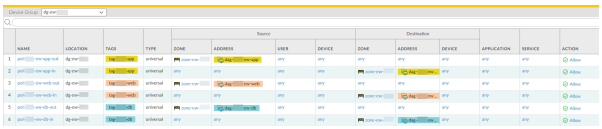
   一致条件のダイアログに表示されるセキュリティ グループは、*NSX-T Manager* で定義したグループから取得されています。ここでは、セキュリティ ポリシーで参照されており、トラフィックが *VM-Series* ファイアウォールにリダイレクトされる グループのみが使用可能です。



8. **OK**をクリックします。
9. 上記の手順を繰り返して、デプロイメントに必要な数のダイナミック アドレス グループを作成します。
10. 変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

STEP 3 | セキュリティ ポリシー ルールを作成する



1. **Policies**（ポリシー） > **Security**（セキュリティ） > **Prerules**（プレルール）を選択します。
2. 「NSX-V Manager 上のサービスとしての VM-Series ファイアウォールの登録」で、NSX-T での VM-Series ファイアウォール管理のために作成したデバイス グループを選択します。
3. **Add**（追加） をクリックし、ルールの **Name**（名前）と **Description**（説明）を入力します。この例では、セキュリティ ルールが Webフロントエンド サーバーとアプリケーション サーバーの間のすべてのトラフィックを許可しています。
4. **Source Zone**（送信元ゾーン）および**Destination Zone**（宛先ゾーン）を選択します。両方の列でゾーン名が同じでなければなりません。
5. **Source Address**（送信元アドレス）および **Destination Address**（宛先アドレス）には、アドレス、アドレス グループ、または領域を選択または入力します。この例では、アドレス グループとして、以前に作成したダイナミック アドレス グループを選択します。
6. 許可する **Application**（アプリケーション）を選択します。この例では、グループ化された特定のアプリケーションの静的グループを含む **Application Group**（アドレス グループ）を作成します。
   1. **Add**（追加）をクリックして、**New Application Group**（新規アプリケーション グループ）を選択します。
   2. **Add**（追加）をクリックし、グループに含めるアプリケーションを選択します。
   3. **OK** をクリックしてアプリケーション グループを作成します。
7. トラフィックについてのアクションを **Allow**（許可） または **Deny**（拒否） に指定し、任意でプロファイルのアンチウイルス、アンチスパイウェア、脆弱性防御のデフォルト セキュリティ プロファイルに関連付けます。
8. 前述のステップを繰り返し、関連するポリシー ルールを作成します。
9. **Commit**（コミット）をクリックし、Commit Typ（コミット タイプ）で **Panorama** を選択します。**OK**をクリックします。

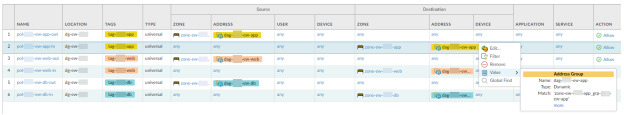
STEP 4 | NSX-T用VM-Seriesファイアウォールにポリシーを適用します。

1. **Commit**（コミット）をクリックし、コミットタイプとして **Device Groups**（デバイス グループ）を選択します。
2. デバイス グループ（この例ではNSX-Tデバイス グループ）を選択し、**OK** をクリックします。
3. コミットが成功したことを確認します。

©2023 Palo Alto Networks, Inc.

STEP 5 | ダイナミック アドレス グループのメンバーが、VM-Series ファイアウォール上に存在することを確認します。

1. Panorama からは、デバイス コンテキストを切り替えてポリシーのプッシュ対象のファイアウォールの Web インターフェイスを起動します。
2. VM-Series ファイアウォールで、**Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、ルールを選択します。
3. アドレス グループのリンクの隣にあるドロップダウンの矢印を選択し、**Inspect**（検査）をクリックします。一致条件が正確であるか確認することもできます。



4. **more**（詳細）リンクをクリックし、登録された IP アドレスのリストが表示されることを確認します。

   このアドレス グループに属し、ここに表示されるすべての IP アドレスについてポリシーが適用されます。

STEP 6 | （任意）テンプレートを使用して、DNS サーバー、NTP サーバー、Syslog サーバー、およびログイン バナーなどのネットワーク基本設定およびデバイス設定をプッシュします。

テンプレートの使用については、『Panorama 管理者ガイド』を参照してください。

STEP 7 | ゾーン プロテクションのプロファイルを作成し、ゾーンに適用します。

ゾーン プロテクション プロファイルは、フラッド、ポートスキャン、ポート スイープやパケット ベースの攻撃に対する防御を行うことができます。これにより、データセンター内の仮想マシン間を移動する同じ層内および異なる層間のトラフィック、およびデータセンター内の仮想マシン（ワークロード）に向かうインターネットからのトラフィックを保護することができます。

1. **Template**（テンプレート）を選択します。
2. **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 プロファイル）を選択し、新規プロファイルの追加と編集を行います。
3. **Network**（ネットワーク） > **Zones**（ゾーン）を選択し、表示された default-zone を選んで、**Zone Protection Profile**（ゾーン プロテクション プロファイル）の中からプロファイルを選択します。

STEP 8 | DoS 防御のプロファイルを作成し、DoS 防御のポリシー ルールに適用します。

1. **Device Group**（デバイスグループ）を選択してください。
2. **Objects**（オブジェクト） > **Security Profiles**（セキュリティ プロファイル） > **DoS Protection**（DoS 防御）を選択し、新規プロファイルの追加と編集を行います。
   - 細かく分類されたプロファイルを作成することで、単一の送信元 IP に適用されるしきい値の設定が可能になります。たとえば、ポリシーに合致したIPアドレスに対して最大セッションレートを設定し、このしきい値がトリガされた際に、当該のIPアドレスをブロックすることができます。

 ©2023 Palo Alto Networks, Inc.

- 集約ポリシーを使用することで、ポリシーに合致するすべてのパケットに対して最大セッションレートを設定することができます。このしきい値は集約された全IPアドレスの新セッションレートに対して適用されます。しきい値がトリガされると、ポリシーに合致するトラフィックすべてに作用します。

3. **Policy**（ポリシー） > **DoS Protection**（**DoS** 防御）から新規の DoS 防御ポリシー ルールを作成し、新しいプロファイルを適用します。

ホスト間で**VM-Series**ファイアウォールを移動するための**vMotion**の使用

VMware NSX-T内に同種のCPU設定を持つESXiホスト間で、vMotionを使ってVM-Seriesファイアウォールを移動する際に、トラフィックフローを維持するためには、vMotion中にPAN-OS CLIを使ってVM-Seriesファイアウォールの内部ハートビートを一時停止する必要があります。ハートビートのモニタリングを一時停止する時間（分）を指定することができます。ハートビートのモニタリングは、最大60分間停止できます。一時停止期間が過ぎた、または強制的に一時停止を中断した場合、ハートビートモニタリングが再開されます。

VM-Seriesファイアウォールのvotionは、vSphere 6.5、6.7、および7.0でサポートされています（ESXiホストが同種のCPU設定を保有している場合）。

*vSphere 7.0*以降を実行している場合、*vMotion*を使って*VM-Series*ファイアウォールを移動する際に、この手続きは必要ありません。

STEP 1 | VM-SeriesファイアウォールCLIにログインします。

STEP 2 | 次のコマンドを使って、ハートビートモニタリング一時停止間隔を設定します。一時停止はコマンドを実行すると即座に開始されます。vMotionに予想以上の時間がかかっている場合、新たにより長い間隔でこのコマンドを再実行することができます。この場合も、コマンド実行後即座に一時停止が開始されます。

```
request system heartbeat-pause set interval <一時停止期間（分）>
```

一時停止の残り時間は、次のコマンドで参照することができます。

```
request system heartbeat-pause show interval
```

STEP 3 | （任意）一時停止期間が経過する前にvMotionが完了した場合、期間に0を設定して一時停止を終了することができます。

```
request system heartbeat-pause set interval 0
```

セキュリティ中心のワークフローを使用した VM-Series のデプロイ

セキュリティ中心のワークフローを使用して、Panorama から NSX-T 用の VM-Series ファイアウォールを制御および管理することができます。サービスチェーンとステアリングルールを作成するために NSX-T Manager にアクセスする必要はありませんが、サービスデプロイメントは NSX-T Manager で作成する必要があります。

- VMware NSX 用 Panorama プラグインのインストール
- NSX-T Manager と Panorama 間の通信の有効化

 ©2023 Palo Alto Networks, Inc.

- Panorama でのテンプレート スタックとデバイス グループの作成
- Panorama でのサービス定義の設定
- NSX-T（East-West）での VM-Series ファイアウォールの起動
- ダイナミック アドレス グループの作成
- セキュリティ ポリシーの作成
- ダイナミックアドレスグループメンバーシップ基準の作成
- ステアリングポリシーの生成
- ステアリングルールの生成

VMware NSX 用 Panorama プラグインのインストール

VMware NSX 用 Panorama プラグインをダウンロードしてインストールします。プラグインをインストールまたはアップグレードする前に、「互換性マトリックス」を参照してください。

セキュリティ中心のデプロイメントワークフローには、*VMware NSX 4.0.0* 用の *Panorama* プラグインが必要です。さらに、*VMware NSX 3.2.x* 用の *Panorama* プラグインからプラグイン *4.0.0* にアップグレードする必要があります

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。Panorama HA ピアにプラグインをインストールする際には、プラグインを最初にパッシブ ピアにインストールしてから、アクティブ ピアにインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 1 | **Panorama** > プラグインを選択します。

STEP 2 | **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。

STEP 3 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 4 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。

NSX-T Manager と Panorama 間の通信の有効化

Panorama と NSX-T Manager 間の通信を有効にするには、以下の手順を実行します。Panorama を最大16台のNSX-T Managerに接続できます。Panorama を複数のNSX-T Managerに接続する場合は、デバイスグループ階層とテンプレートスタックを慎重に計画し、デプロイメントに必要な他のコンポーネントとどのように対話するのかを検討する必要があります。サービス定義は、デバイス グループとテンプレート スタックを参照し、その情報を関連する ESXi クラスターのファイアウォールにプッシュします。

©2023 Palo Alto Networks, Inc.

STEP 1 | （任意）Panorama と NSX-V Manager 間の通信のため、Panorama の **Panorama** > **Setup**（セットアップ） > **Services**（サービス） > **Proxy Server**（プロキシ サーバー）で構成されたプロキシ サーバー設定をバイパスします。

このコマンドを実行すると、Panorama が NSX-V Manager と直接通信しながら、他のサービスのためにプロキシ通信は維持されます。

1. Panorama CLI にログインします。
2. プロキシ バイパスを有効または無効にするには、以下のコマンドを実行します。

   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}

   プロキシ バイパスを有効にする場合は **yes** を選択し、無効にする場合は **no** を選択します。これはデフォルトで**no**が設定されます。

STEP 2 | Panorama Web インターフェイスにログインします。

Web ブラウザから安全な接続（https）を使用し、初期設定時に割り当てられた IP アドレスとパスワードを使用してログインします（https://<*IP address*>）。

STEP 3 | NSX-T Manager へのアクセスをセットアップします。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択し、**Add**（追加）をクリックします。
2. **Name**（名前）に分かりやすい NSX-T Manaer 名を入力します。
3. （任意）NSX-T Managerの説明を追加します。
4. NSX-T Managerにアクセスするための**NSX Manager URL**（NSX-T Manager cluster 仮想 IP アドレスまたは FQDN）を入力します。
5. Panorama が NSX-T Manager への認証を行えるように **NSX Manager Login**（**NSX Manager** ログイン）に認証情報（ユーザー名とパスワード）を入力します。
6. **OK**をクリックします。
7. Panorama を接続するNSX-T Managerごとにこの手順を繰り返します。

NSX-T Manager のログイン用パスワードを変更する場合、必ず *Panorama* 上のパスワードを即座に更新してください。パスワードが間違っていると、*Panorama* および *NSX-T Manager* 間で通信できなくなります。

STEP 4 | 変更を Panorama にコミットします。

Commit (コミット) および **Commit to Panorama (Panorama** へのコミット**)** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | Panorama の接続状態を確認します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択します。
2. **Status**（ステータス）列のメッセージを確認します。

   接続が成功すると、状態は **Registered**（登録済み）と表示されます。これは、Panorama と NSX-T Manager が同期していることを示します。

   失敗した状態では、以下のメッセージが表示されます。

   - **No connection**（接続なし）:NSX-T Manager にアクセスできないか、NSX-T Manager へのネットワーク接続を確立できません。
   - **Invalid Credentials**（無効な認証情報）:アクセス認証情報（ユーザー名/パスワード）が正しくありません。
   - **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-T Manager に定義されている設定と異なります。リンクをクリックして失敗の原因を確認してください。たとえば、NSX-T 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-T Manager のサービス定義の検証を行います。Panorama と NSX-T 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。
   - **Connection Disabled**（接続が無効）:Panorama と NSX-T Manager 間の接続が手動で無効にされています。

Panorama でのテンプレート スタックとデバイス グループの作成

Panorama を使用して NSX-T 用の VM-Series ファイアウォールを管理するには、ファイアウォールがデバイス グループおよびテンプレート（テンプレート スタックのメンバー）に属している必要があります。デバイス グループでは、同様のポリシーとオブジェクトが必要なファイアウォールを論理的なユニットとしてグループ化できます。この設定は Panorama の **Objects**（オブジェクト）タブと **Policies**（ポリシー）タブを使用して定義します。テンプレート スタックを使用して、VM-Series ファイアウォールがネットワーク上で動作するのに必要な設定を構成してから、関連付けを行います。この設定は、Panorama の **Device**（デバイス）タブと **Network**（ネットワーク）タブを使用して定義します。また、Panorama の NSX-T 設定で使用されるゾーンを持つ各テンプレートスタックは、サービス定義に関連付ける必要があります。最低でも、テンプレートスタック内にゾーンを作成し、NSX-T Manager が VM-Series ファイアウォールにトラフィックをリダイレクトできるようにする必要があります。後で、デバイスグループとテンプレートを NSX-T デプロイメントに関連付けて、サービス定義を作成します。

Panorama は、NSX-T North-South および NSX-T East-West の両方のデプロイメントを同時にサポートできます。NSX-T North-South および NSX-T East-West に対して、個別のデバイスグループ、テンプレートスタック、およびサービス定義を設定する必要があります。

 ©2023 Palo Alto Networks, Inc.

STEP 1 | デバイスグループあるいはデバイスグループの階層を追加します。

1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、**Add**（追加）をクリックします。デバイス グループの階層を作成することもできます。
2. デバイス グループを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット）をクリックした後、**Commit Type**（コミット タイプ）として **Panorama** を選択し、Panorama で実行中の設定に対する変更を保存します。

STEP 2 | テンプレートを追加します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add**（追加）をクリックします。
2. テンプレートを識別するために、一意の **Name**（名前）と **Description**（説明）を入力します。
3. **OK**をクリックします。
4. **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

STEP 3 | テンプレートスタックを作成し、新しく作成したテンプレートを追加します。

1. **Panorama** > **Templates**（テンプレート）を選択し、**Add Stack**（スタックの追加）をクリックします。
2. テンプレート スタックを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。
3. [テンプレート] で、[追加] をクリックし、ステップ 2 で作成したテンプレートをドロップダウンから選択します。
4. **OK**をクリックします。
5. **Commit**（コミット） をクリックし、**Commit to Panorama**（**Panorama**に非ミット） を選択して、Panorama で実行中の設定に変更を保存します。

STEP 4 | 各テンプレートのゾーンを作成します。

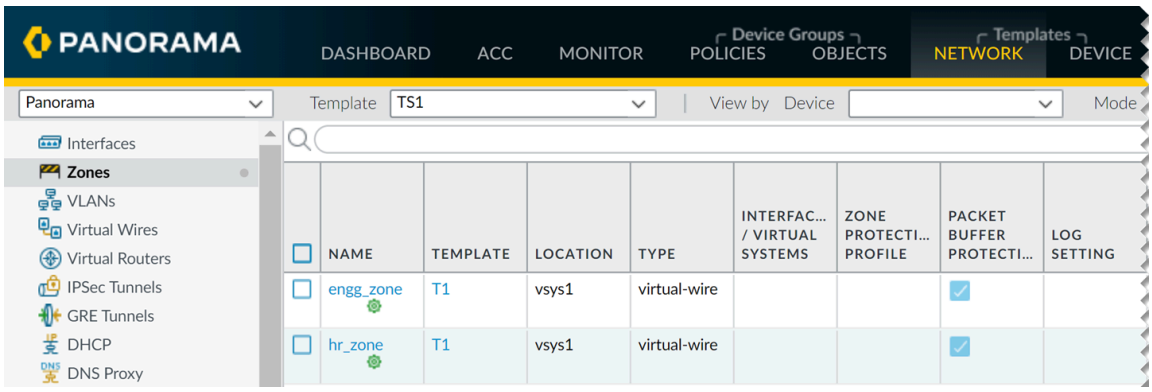
VMware NSX 用の Panorama プラグインは、各ゾーンを NSX-T Manager のサービスプロファイルにマッピングします。認定するには、ゾーンが仮想ワイヤタイプで、サービス定義に関連付けるテンプレートの一部である必要があります。詳細については、Panorama でのサー

 ©2023 Palo Alto Networks, Inc.

ビス定義の設定を参照してください。ほとんどのユースケースでは、1 つのゾーンで十分です。ただし、マルチテナンシーには複数のゾーンを作成する必要があります

各テンプレートにつき最大 32 のゾーンを追加できます。

1. **Network**（ネットワーク） > **Zones**（ゾーン）を選択します。
2. **Template**（テンプレート）のドロップダウン リストから、適切なテンプレートを選択します。
3. **Add**（追加）を選択し、ゾーンの **Name**（名前）を入力します。
4. インターフェイスの **Type**（タイプ）を **Virtual Wire**（バーチャル ワイヤ）に設定します。
5. **OK**をクリックします。
6. ゾーンが正しいテンプレートに追加されていることを確認します。



7. **Commit**（コミット） をクリックし、**Commit Type**（コミット タイプ） として **Panorama** を選択して、Panorama で実行中の設定に変更を保存します。

STEP 5 | テンプレートスタックの DNS および NTP サーバ情報を更新します。デプロイメントでデバイス証明書を使用している場合は、この手順を完了する必要があります。これは、NSX-T 環境にデプロイされたファイアウォールに、デバイス証明書サーバに到達するために必要な正しい DNS 情報があることを確認するために必要です。

1. [テンプレート] ドロップダウンから正しいテンプレートスタックを指定したことを確認します。
2. デバイス > セットアップ > サービスを選択して、[編集]アイコンをクリックします。
3. [サービス] タブで、プライマリ **DNS** サーバーおよびセカンダリ **DNS** サーバーの IP アドレスを入力します。
4. [NTP] タブで、**NTP** サーバーの IP アドレスを入力します。
5. **OK** をクリックします。
6. 変更を Panorama にコミットします。

Panorama でのサービス定義の設定

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。サービス定義には、デバイス グループ、テンプレート スタック、および OVF URL を含める必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | （任意）通知グループを設定します。

仮想環境の変更を通知する必要があるデバイス グループを指定して、通知グループを作成します。指定したデバイス グループに含まれるファイアウォールは、セキュリティ グループとそのグループ内のゲスト VM の IP アドレスのリアルタイム更新を受信します。ファイアウォールは、この更新を使用してポリシーで参照しているダイナミック アドレス グループを構成する最新メンバーリストを決定します。

1. **Panorama** > **VMware** > **Notify Group**（通知グループ）を選択し、**Add**（追加）をクリックします。
2. 通知グループに分かりやすい **Name**（名前）を付けます。
3. 仮想環境の変更を通知する必要があるデバイス グループのボックスをすべて選択します。デバイス グループのチェック ボックスを選択できない場合は、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。
4. **OK**をクリックします。

STEP 2 | 新しいサービス定義を追加します。

*Panorama*で最大*32*のサービス定義を作成できます。

1. **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（サービス定義）を選択します。
2. **Add**（追加）を選択して、新しいサービス定義を作成します。
3. **Name**（名前）に分かりやすいサービス定義名を入力します。
4. （任意）このサービス定義を使用してデプロイされる VM-Series ファイアウォールの機能あるいは目的が分かるような **Description**（説明）を追加します。

STEP 3 | デバイス グループとテンプレート スタックをサービス定義用に割り当てます。

必ずPanorama でのテンプレート スタックとデバイス グループの作成を行うようにしてください。

このソリューションでデプロイされるファイアウォールは、Panorama から集中管理されるため、ファイアウォールが属する **Device Group**（デバイス グループ）と **Template Stack**（テンプレート スタック）を指定する必要があります。このサービス定義を使用してデプロイされるすべてのファイアウォールは、指定したテンプレート スタックおよびデバイスグループに属します。

1. **Device Group**（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あるいはデバイスグループの階層を選択します。
2. **Template**（テンプレート） ドロップダウンでテンプレート スタックを選択します。

   あるサービス定義に割り当てられたテンプレート スタックあるいはデバイスグループを他のサービス定義で利用することはできません。

©2023 Palo Alto Networks, Inc.

STEP 4 | OVF ファイルの場所を指定します。

zip ファイルをダウンロードして解凍し、.ovf、mf、および .vmdk の各ファイルを抽出して、同じディレクトリに保存します。ovf および vmdk ファイルはファイアウォールの各インスタンスのデプロイに使用されます。

VM-Series ファイアウォールの *NSX* サービスのデプロイメントが正常に完了した後は、*Panorama* サービス定義の *OVF* パスを変更しないでください。*VM-Series* ファイアウォールのデプロイメントが正常に完了した後に *OVF* パスを変更すると、*NSX* サービスデプロイメントが失敗した状態になる可能性があります。*NSX-T Manager* でこの問題を解決できますが、これにより、すべての *VM-Series* ファイアウォールが再デプロイされる可能性があります。

OVF URL に、OVF ファイルをホストする Web サーバーの場所を追加します。http および https の両方がサポートされています。

同じ ovf バージョンあるいは異なるバージョンをすべてのサービス定義で使用することができます。異なるバージョンの ovf を各サービス定義で使用することにより、異なる ESXi クラスタ内の VM-Series ファイアウォールの PAN-OS のバージョンを変えることができます。

STEP 5 | （任意）**Notify Group**（通知グループ）を選択します。

STEP 6 | ファイアウォールの **Insertion Type**（挿入タイプ）として **East West** を選択します。

STEP 7 | （任意）**Enable**（有効）を選択して、**Health Check**（ヘルス チェック）を有効にします。

ヘルスチェックはデフォルトで有効になっています。サービス ヘルス チェックとも呼ばれる、この NSX-T 機能により、サービス インスタンスに障害が発生した場合の高可用性をシミュレートすることができます。VM-Series ファイアウォールで設定する場合、VM-Series サービス インスタンスに障害が発生すると、そのファイアウォールに転送されたトラフィックは、クラスタ内の別のファイアウォール インスタンス（サービス クラスタ デプロイの場合）、または他のホスト上のファイアウォール インスタンス（ホスト ベースのデプロイの場合）にリダイレクトされます。

NSX-T で *VM-Series* ファイアウォールのコミットとデプロイを行った後は、サービス定義内でヘルス チェックを有効化/無効化することはできません。ヘルス チェック設定の変更をコミットしても、コミット失敗のメッセージが返されます。変更するには、サービス定義を削除した後再作成して、*VM-Series* ファイアウォールを再度デプロイする必要があります。

STEP 8 | NSX ManagerがVM-Seriesファイアウォールをデプロイする時に、自動的にデバイス証明書を取得するには、デバイス証明書を設定します。

新たにデプロイされたVM-Seriesファイアウォールにデバイス証明書を適用するには、このオプションを有効にします。デバイス証明書をサポートするベースイメージOVFを使ってファイアウォールをデプロイする場合にのみ、このオプションを使用してください。Panoramaは、サービス定義の一環として、NSX Managerにデバイス証明書情報をプッ

 ©2023 Palo Alto Networks, Inc.

シュ配信します。NSXに新たなファイアウォールがデプロイされた場合、ブートアップ時にファイアウォールにデバイス証明書がインストールされます。

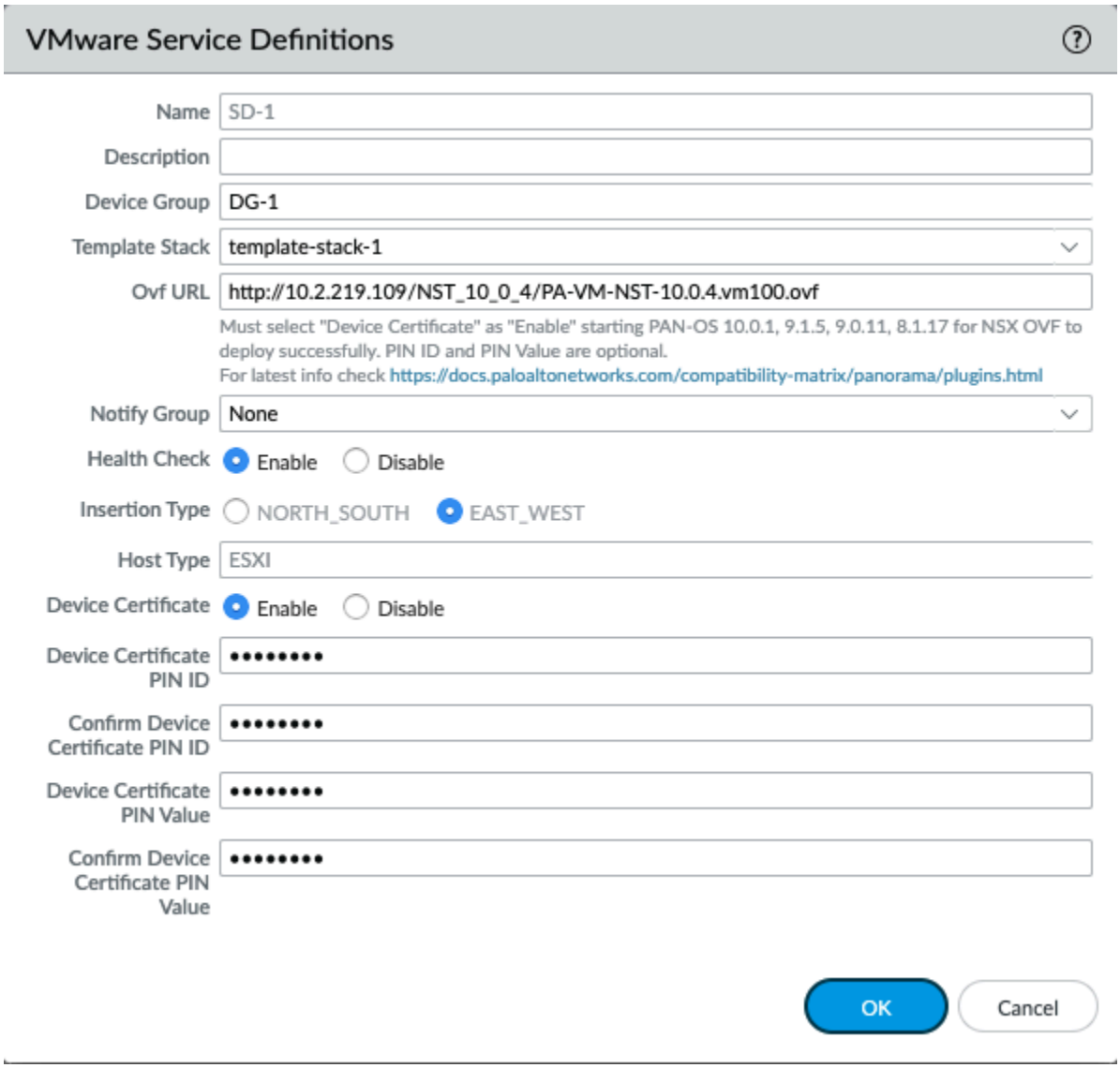
VMware NSX上のVM-Seriesファイアウォールに対するデバイス証明書をサポートしているOVFの一覧については、「Palo Alto Networks互換性マトリックス」を参照してください。

OVF がデバイス証明書をサポートしている場合は、デバイス証明書を使用しているかどうかに関係なく、デバイス証明書を有効にする必要があります。OVFがデバイス証明書をサポートしていない場合は、このオプションを無効にしてください。

1. まだ作業を行っていない場合は、カスタマーサポートポータルにログインして、Registration PINおよびPIN IDを生成します。
2. **Device Certificate**（デバイス証明書）下で、**Enable**（有効）をクリックします。
3. PIN IDをコピーして、それを**Device Certificate PIN ID**（デバイス証明書**PIN ID**）フィールドに入力します。
4. **Confirm Device Certificate PIN ID**（デバイス証明書**PIN ID**の再入力）フィールドに、PIN IDをもう一度入力します。
5. PIN Valueをコピーして、それを**Device Certificate PIN Value**（デバイス証明書**PIN**値）フィールドに入力します。
6. **Confirm Device Certificate PIN Value**（デバイス証明書**PIN**値の再入力）フィールドに、PIN値をもう一度入力します。

©2023 Palo Alto Networks, Inc.

STEP 9 | **OK** をクリックしてサービス定義を保存します。

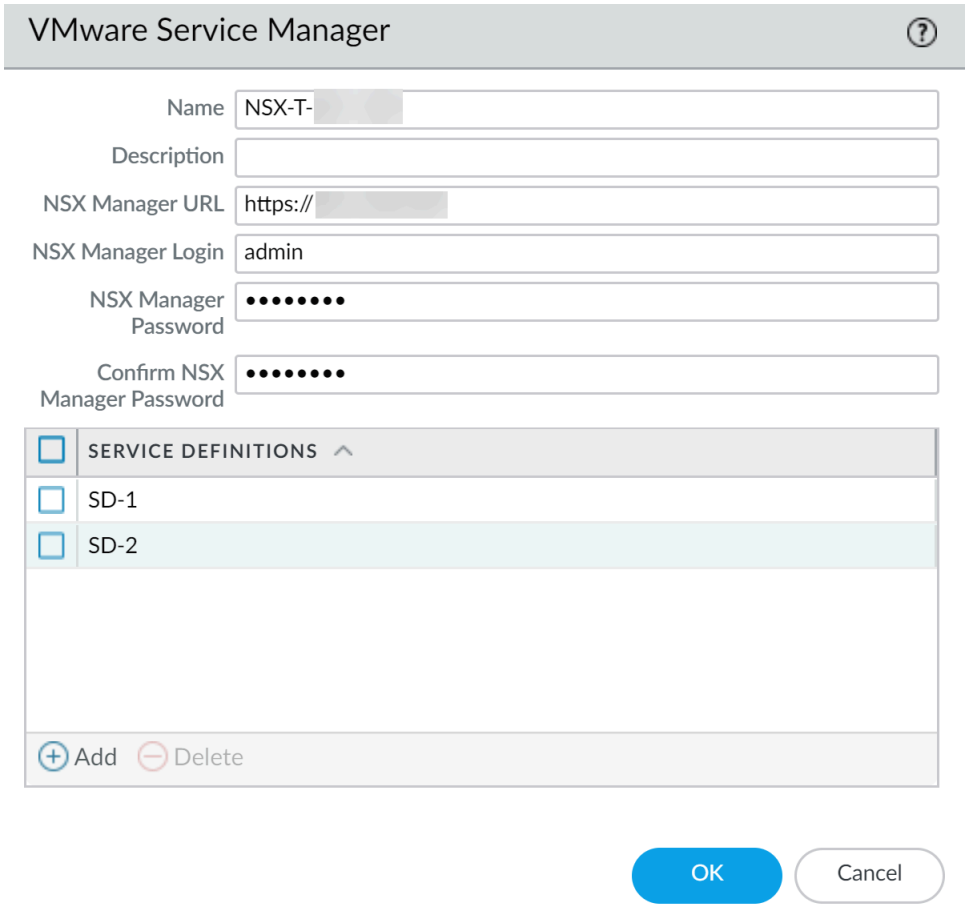


©2023 Palo Alto Networks, Inc.

STEP 10 | サービス定義をサービス マネージャーにアタッチします。

1 つのサービス定義を、複数のサービス マネージャー内で使用することはできません。

1. **Panorama** > **VMware** > **NSX-T** > **Service Manager**（サービス マネージャー）を選択し、サービス マネージャー名のリンクをクリックします。
2. Service Definitions（サービス定義）で **Add**（追加）をクリックし、ドロップダウンからサービス定義を選択します。
3. **OK** をクリックします。



STEP 11 | 認証コードを追加してファイアウォールをライセンス登録します。

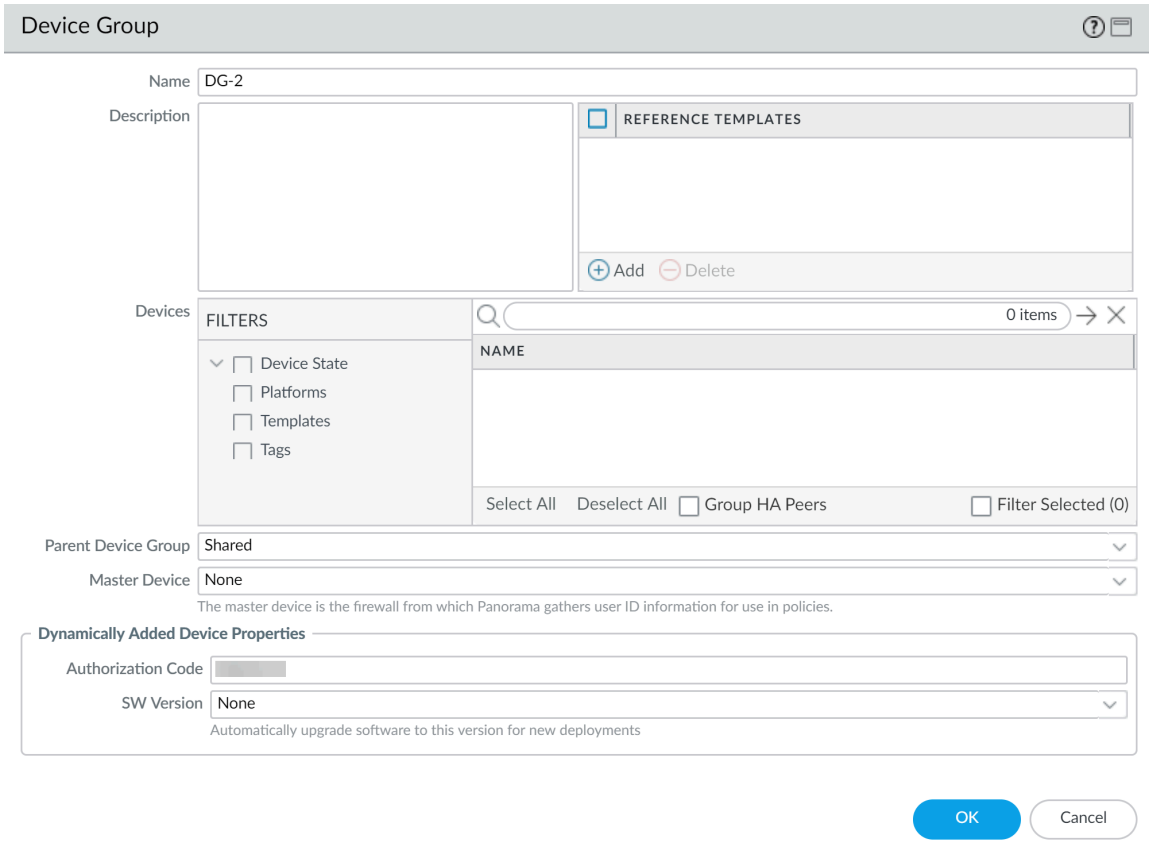
1. **Panorama** > **Device Groups**（デバイス グループ）を選択し、作成したサービス定義に関連付けられているデバイス グループを選択します。
2. **Dynamically Added Device Properties**（動的に追加されたデバイス プロパティ）の下で、受注完了電子メールで受け取った認証コードを追加します。任意で **SW**

©2023 Palo Alto Networks, Inc.

Version（**SW** バージョン）のドロップダウン リストから None（なし）を選択します。

NSX-T に新しいファイアウォールがデプロイされると、それがデバイス グループに自動的に追加され、指定した認証コードを使ってライセンスが供与され、指定したバージョンの PAN-OS にアップグレードされます。

サポート ポータルで、デプロイ可能なファイアウォールの総数および認証コードで使用可能なライセンス総数に対する使用済みライセンス数の比率を表示できます。



STEP 12 | Commit to Panorama（**Panorama** へのコミット）によってコミットします。

©2023 Palo Alto Networks, Inc.

STEP 13 | NSX-T Manager で、サービス定義が使用可能であることを確認します。

System（システム） > **Service Deployments**（サービスのデプロイ） > **Catalog**（カタログ）を選択します。サービス定義が NSX-T Manager にサービス インスタンスとしてリストアップされます。

NSX-T（East-West）での VM-Series ファイアウォールの起動

VM-Series ファイアウォールを NSX-T 環境のサービスとしてデプロイするには、以下の手順を実行します。**Deployment Specification**（デプロイの仕様）および **Deployment Template**（デプロイ テンプレート） フィールドには、サービス定義の一環として Panorama からプッシュ配信される情報が自動的に記入されます。

Deployment Attributes（デプロイ属性）下の設定は、どれも変更しないでください。これらの値は *Panorama*からインポートされ、それを変更するとデプロイが失敗してしまいます。

STEP 1 | NSX-T Manager にログインします。

STEP 2 | **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Deployment**（デプロイ）を選択します。

STEP 3 | **Partner Service**（パートナー サービス）ドロップダウンから、サービス定義を選択します。

STEP 4 | **Deploy Service**（サービスのデプロイ）をクリックします。

STEP 5 | **Name**（名前）に分かりやすいサービス デプロイ環境名を入力します。

STEP 6 | **Compute Manager**（vCenter）を選択します。

STEP 7 | **Deployment Type**（デプロイ タイプ）として、**Clustered**（クラスタ）または **Host Based**（ホスト ベース）を選択します。

STEP 8 | **Deployment Type**（デプロイ タイプ）として**Clustered**（クラスタ）を選択した場合、**Clustered Deployment Count**（クラスタ化されたデプロイ数）にクラスタにデプロイする VM-Series ファイアウォール インスタンス数を指定します。

STEP 9 | クラスタ デプロイ環境内で VM-Series を起動する場合、**Host**（ホスト）を選択します。**Host**（ホスト）ドロップダウンから特定のホストを選択するか、または NSX-T Manager にホストを選択させる場合は、**Any**（任意）を選択します。ホストベースのデプロイメントでは、このオプションはグレー表示されます。

STEP 10 | VM-Series ファイアウォールのリポジトリとして、**Data Store**（データ ストア）を選択します。クラスタ デプロイ環境で、ホストに対して **Any**（任意）を選択した場合は共有データストアを選択します。特定のホストを指定した場合は、ローカル データ ストアを選択します。

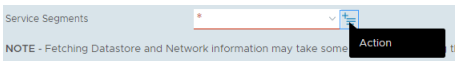
©2023 Palo Alto Networks, Inc.

STEP 11 | **Networks**（ネットワーク）の設定を行います。

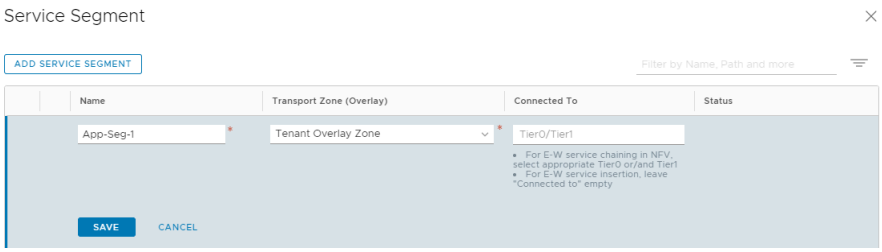
1. Networks（ネットワーク）列で、**Set**（設定）をクリックします。
2. **eth0 - Management Nic** に対して **Network**（ネットワーク）を選択します。
3. **Network Type**（ネットワーク タイプ）として、DHCP または Static IP Pool（スタティック IP プール）を選択します。スタティック IP プールを選択した場合、**IP Pool**（**IP** プール）を選択します。
4. **eth1 - Data-1 Nic** を選択します。
5. 両方のインターフェースがオンになっていることを確認します。
6. **Save**（保存）をクリックします。

STEP 12 | **Service Segment**（サービス セグメント）を設定または選択します。サービス セグメントを設定するには、以下の手順を実行します。

1. **Service Segments**（サービス セグメント）列で、**Action**（アクション）をクリックします。



2. **Add Service Segment**（サービス セグメントの追加）をクリックします。
3. 分かりやすい **Name**（名前）を入力します。
4. **Transport Zone**（**Overlay**）（トランスポート ゾーン（オーバーレイ））を選択します。
5. **Save**（保存）をクリックして、**Close**（閉じる）をクリックします。



STEP 13 | サービスをデプロイする**Cluster**（クラスタ）を選択します。**NSX Configuration**（**NSX** 設定）でクラスタを選択する必要があります。

STEP 14 | **Save**（保存）をクリックします。

STEP 15 | ファイアウォールのデプロイが正常に完了したことを確認します。

1. **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Service Instances**（サービス インスタンス）を選択します。
2. ファイアウォールが記載されており、**Deployment Status**（デプロイ ステータス）が **Up** になっていることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 16 | ファイアウォールが Panorama に接続されていることを確認します。

1. Panoramaにログインします。
2. **Panorama** > **Managed Devices**（管理対象デバイス） > **Summary**を選択します。
3. ファイアウォールが適切なデバイス グループ下に記載されており、**Device State**（デバイス状態）が **Connected**（接続）になっていることを確認します。

ダイナミック アドレス グループの作成

セキュリティ グループは、クラスター内の複数の ESXi ホストのゲストをグループ化する論理コンテナです。適切な条件を満たすダイナミック アドレスグループを作成して変更内容をコミットすると、NSX-V Manager で対応するセキュリティ グループが作成されます。セキュリティ グループの作成は、ゲストの管理や保護を行うために必要です。セキュリティ グループでポリシーの適用を有効にする方法を理解するには、「ダイナミック アドレスグループを使用したポリシー適用」を参照してください。

ダイナミックアドレスグループを NSX-T のセキュリティグループにするには、**‘_nsxt_<dynamic-address-group-name>’** の形式でダイナミックアドレスグループの一致基準を追加する必要があります。一致基準に追加するダイナミックアドレス名は、ダイナミックアドレスグループ名と正確に一致する必要があります。たとえば、アプリケーションと呼ばれるダイナミックアドレスグループには、一致基準 **'_nsxt_Applications'** を含める必要があります。さらに、サービスマネージャの一部であり、コミットされたサービス定義のデバイスグループにダイナミックアドレスグループを含める必要があります。

ダイナミックアドレスグループから作成された各セキュリティグループは、**<service-def-name>_<dynamic-address-group-name>** という形式になります。たとえば、**ServiceDef1_Applications** などです。

作成する各ダイナミックアドレスグループは、*Panorama* で設定された各デバイスグループ全体で固有の名前を持つ必要があります。

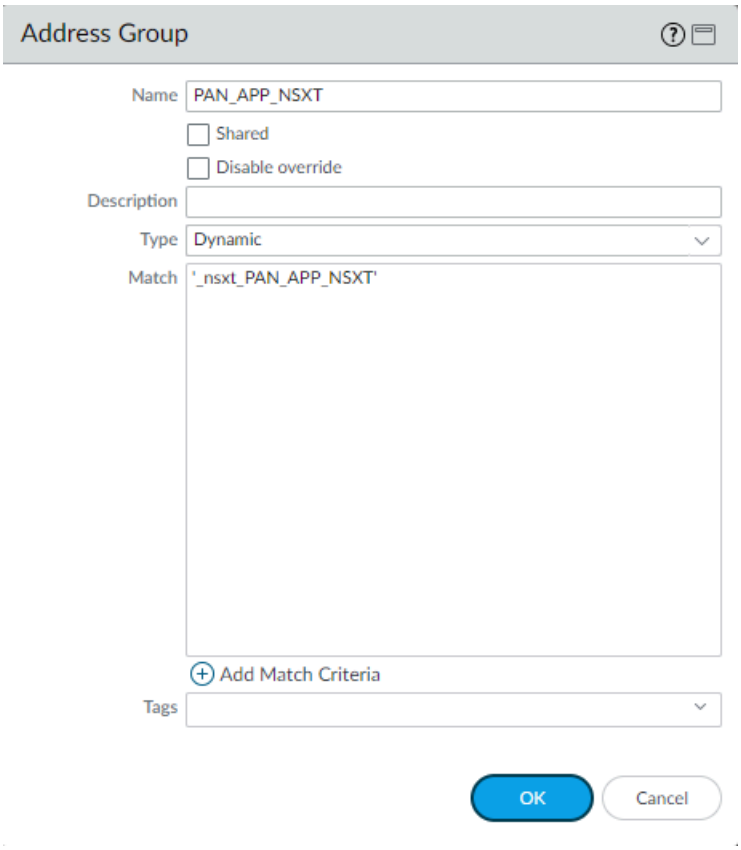
©2023 Palo Alto Networks, Inc.

STEP 1 | デプロイに必要な、各セキュリティ グループのダイナミック アドレス グループを設定します。

1. **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. NSX-V サービス定義に関連付けられているデバイスグループでダイナミックアドレスグループが設定されていることを確認します。
3. **Add**（追加）をクリックし、アドレス グループの **Name**（名前）および **Description**（説明）を入力します。
4. **Type**（タイプ）で **Dynamic**（ダイナミック）を選択します。
5. 一致条件を指定します。

   ダイナミックアドレスグループを *NSX-V Manager* のセキュリティ グループにするには、一致条件の文字列を一重引用符で囲み、*_nsx_* というプレフィックスを付けてアドレスグループの正確な名前を続ける必要があります。たとえば、***'_nsxt_PAN_APP_NSX'*** のようにします。

6. 必要なセキュリティ グループごとにこの操作を繰り返します。



STEP 2 | 変更を **Commit (コミット)** します。

セキュリティ ポリシーの作成

ステアリングポリシーで使用されるステアリングルールを自動生成するために使用されるセキュリティポリシールールを作成します。

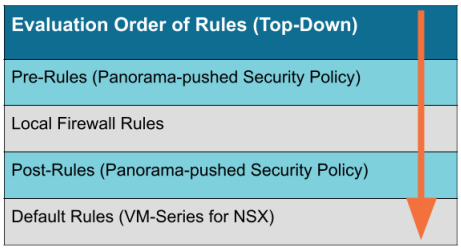
©2023 Palo Alto Networks, Inc.

ステアリングルールの生成を行う場合、プレルール、ポストトルール、またはすべてに基づいてステアリングルールを生成するオプションがあります。[すべて] を選択すると、NSX 用 VMware プラグインは、プレルールとポストルール内の該当するセキュリティごとにステアリングルールを作成します。これにより、不要なステアリングルールが作成され、ルールの管理がより困難になる可能性があります。ステアリングルールをセキュリティルールから簡単に分離できるように、ステアリングルールをポストルールとして作成し、セキュリティルールをプレルールとして作成できます。

Panorama で作成されたセキュリティルールに基づいてステアリングルールを自動生成するには、セキュリティルールが次の基準を満たしている必要があります。

- NSX-T サービス マネージャーに登録されている親または子のデバイスグループに所属する。
- ゾーン内ポリシーであり、1 つのゾーンのみが入っている。
- ルール用に構成されたスタティックアドレスグループ、IP 範囲、またはネットマスクは組み入れられていない。

Panorama で NSX-T ステアリングルールを定義する場所（プレルールベースまたはポストルールベース）を決定するときは、Panorama で作成するセキュリティポリシールールと NSX-T ステアリングルールの数、およびルールがトラフィックに適用される順序を考慮します。プレルールは、ポストルールの前にトラフィックに適用されます。



- プレルール - Panorama プレルールベースを使用して、NSX-T のステアリングルールと VM-Series ファイアウォールセキュリティポリシールールを定義できます。同じルールベースにセキュリティルールとステアリングルールを定義する場合は、ステアリングルールに対するセキュリティルールの順序を考慮する必要があります。ステアリングルールとセキュリティポリシールールの両方を含む大規模なルールベースがある場合、スケーリング時に両方のタイプのルールを管理することが困難になる場合があります。
- ポストルール - インスペクションおよび適用に使用されるセキュリティポリシールールを、NSX-T のステアリングルールの生成に使用されるセキュリティルールから分離すると、大量のルールを使用して展開を拡張するのに役立ちます。ステアリングルールを自動生成すると、プラグインは、指定されたルールベース内の必要な基準を満たすすべてのルールに対してステアリングルールを生成します。したがって、2 つのタイプのルールを分離することで、意図せず無関係なステアリングルールが生成されるのを防ぐことができます。ステアリングルールにはポストルールベースを使用することをお勧めします。特に、大量のセキュリティポリシールールを含むデプロイメントでは使用してください。

セキュリティルールで指定する送信元および宛先のダイナミックアドレスグループ。ステアリングルールを自動生成する場合、ルールが適用される場所（NSX-T 分散ファイアウォールまたはセキュリティグループ）は、セキュリティルールの構成時に指定した送信元と宛先によって異なります。送信元または宛先に [任意] を選択した場合、NSX-T Manager はステアリングルールを分散ファイアウォールに適用します。送信元と宛先にダイナミックアドレスグループを選択した

©2023 Palo Alto Networks, Inc.

場合、ステアリングはそれらのセキュリティグループ内のゲスト仮想マシンに適用されます。ステアリングルールを手動で作成する場合は、ステアリングルールが適用されるセキュリティグループを指定できます。

ステアリングルールの定義に使用されるセキュリティポリシーに、運用中心の展開ワークフローの一部として構成されたダイナミックアドレスグループが含まれていないことを確認してください。含まれている場合、ステアリングルールの送信元と宛先が NSX-T Manager に source-any と destination-any としてプッシュされます。これは、NSX-T 環境のトラフィックに影響を与える可能性があります。

ステアリングルールの自動生成に使用するセキュリティルールを無効にすると、ステアリングルールも無効になります。

- プレルールベースを使用した NSX-T ステアリングルールの定義
- ポストルールベースを使用した NSX-T ステアリングルールの定義
- NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用

プレルールベースを使用した **NSX-T** ステアリングルールの定義

次の手順では、NSX-T ステアリングルールの生成に使用されるセキュリティポリシールールを作成する方法と、Panorama がトラフィックの検査と実施のために VM-Series ファイアウォールにプッシュするセキュリティポリシーを作成する方法について説明します。

NSX-V Manager、VM-Series ファイアウォールおよび Panorama でどのようにルールが機能するかを理解されるまでは、トラフィック リダイレクト ポリシーを適用しないでください。VM-Series ファイアウォール上のデフォルト ポリシーは、*deny all* トラフィックに設定されます。これは、VM-Series ファイアウォールにリダイレクトされるすべてのトラフィックがドロップされることを意味します。

関連するデバイス グループでセキュリティ ポリシー ルールを作成します。セキュリティ ルールごとに Rule Type（ルール タイプ）を Intrazone（イントラゾーン）に設定し、関連付けられたテンプレート スタックで 1 つのゾーンを選択して、ダイナミック アドレス グループを送信元および宛先として選択します。Panorama で適格なセキュリティ ポリシーを作成すると、Panorama でステアリング ルールを生成してコミットするときに、対応するステアリング ルールを NSX-V Manager で作成するのに役立ちます。

STEP 1 | Panorama で **Policies**（ポリシー） > **Security**（セキュリティ） > **Pre Rules**（プレルール）を選択します。

STEP 2 | **Add**（追加）をクリックし、セキュリティ ポリシー ルールの **Name**（名前）と **Description**（説明）を入力します。

STEP 3 | NSX-T サービス定義に関連付けられたデバイスグループで、セキュリティルールを設定していることを確認します。

STEP 4 | Rule Type（ルール タイプ）を **intrazone**（**Devices with PAN-OS 6.1 or later)**（イントラゾーン（**PAN-OS 6.1** 以降を搭載したデバイス））に設定します。

STEP 5 | Source（送信元）タブで、source zone（送信元ゾーン）を、サービス定義に関連付けられているテンプレート スタックからのゾーンに設定します。次に、前に送信元アドレスとし

 ©2023 Palo Alto Networks, Inc.

て作成したダイナミック アドレス グループ（NSX-V セキュリティグループ）を選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを送信元アドレスとして追加しないでください。

STEP 6 | Destination（宛先）タブでは、宛先ゾーンを設定することができません。これは、rule type（ルール タイプ）が intrazone（イントラゾーン）に設定されているためです。次に、前に宛先アドレスとして作成したダイナミック アドレス グループ（NSX-V セキュリティグループ）を選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを宛先アドレスとして追加しないでください。

STEP 7 | **OK**をクリックします。

STEP 8 | 必要なステアリング ルールごとにステップ 1 ～ 7 を繰り返します。

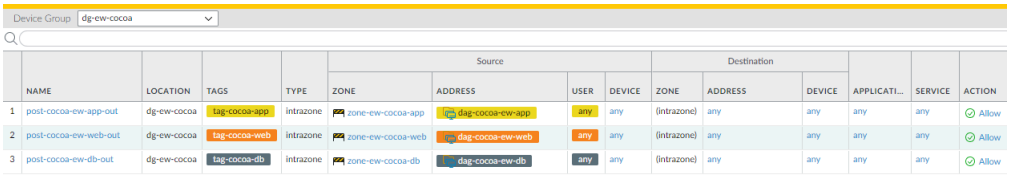
STEP 9 | 変更を **Commit (**コミット**)** します。

STEP 10 | NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用.

ポストルールベースを使用した **NSX-T** ステアリングルールの定義

STEP 1 | セキュリティ ルールを作成します。

1. Panorama で、ポリシー > セキュリティ > ポストルールを選択します。
2. NSX-T サービス定義に関連付けられたデバイスグループで、セキュリティルールを設定していることを確認します。
3. 編集するセキュリティルールの名前をクリックします。
4. Rule Type（ルール タイプ）を **intrazone**（**Devices with PAN-OS 6.1 or later)**（イントラゾーン（**PAN-OS 6.1** 以降を搭載したデバイス））に設定します。
5. Source（送信元）タブで、source zone（送信元ゾーン）を、サービス定義に関連付けられているテンプレート スタックからのゾーンに設定します。次に、前に送信元アドレスとして作成したダイナミック アドレスグループを選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを送信元アドレスとして追加しないでください。
6. Destination（宛先）タブでは、宛先ゾーンを設定することができません。これは、rule type（ルール タイプ）が intrazone（イントラゾーン）に設定されているためです。次に、前に宛先アドレスとして作成したダイナミック アドレスグループを選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを宛先アドレスとして追加しないでください。
7. **OK**をクリックします。
8. 必要なステアリング ルールごとにステップ 1 ～ 7 を繰り返します。



STEP 2 | 変更を Panorama にコミットします。

©2023 Palo Alto Networks, Inc.

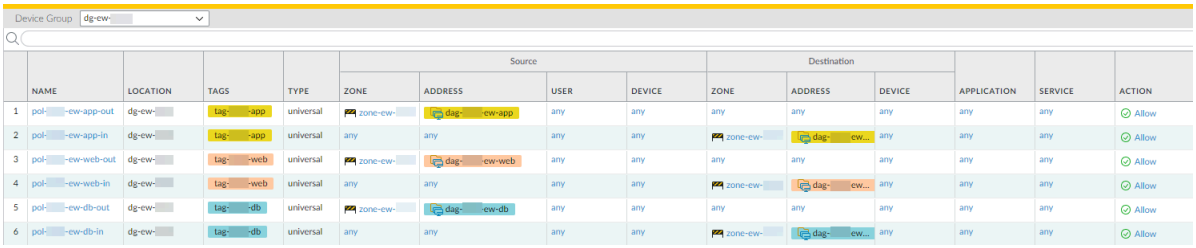
STEP 3 | NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用.

NSX-T（East-West）のVM-Seriesファイアウォールへのセキュリティポリシーの適用

ステアリングルールを定義したので、Panorama を使用して VM-Series ファイアウォールのポリシーを一元管理できます。

ポリシーを一元的に管理するには、ダイナミック アドレス グループをセキュリティポリシーの送信元アドレスまたは宛先アドレスとして適用し、ファイアウォールにプッシュします。ファイアウォールは、各セキュリティグループに含まれる仮想マシンの IP アドレスを動的に取得することができ、指定されたグループにある仮想マシンからのトラフィックまたは仮想マシンへのトラフィックにコンプライアンスを適用します。

STEP 1 | セキュリティ ポリシー ルールを作成する



1. **Policies**（ポリシー） > **Security**（セキュリティ） > **Prerules**（プレルール）を選択します。
2. 「Panorama でのテンプレート スタックとデバイス グループの作成」で、NSX-T での VM-Series ファイアウォール管理のために作成したデバイス グループを選択します。
3. **Add**（追加） をクリックし、ルールの **Name**（名前）と **Description**（説明）を入力します。この例では、セキュリティ ルールが Webフロントエンド サーバーとアプリケーション サーバーの間のすべてのトラフィックを許可しています。
4. **Source Zone**（送信元ゾーン）および**Destination Zone**（宛先ゾーン）を選択します。両方の列でゾーン名が同じでなければなりません。
5. **Source Address**（送信元アドレス）および **Destination Address**（宛先アドレス）には、アドレス、アドレス グループ、または領域を選択または入力します。この例で

©2023 Palo Alto Networks, Inc.

は、アドレス グループとして、以前に作成したダイナミック アドレス グループを選択します。

6. 許可する **Application**（アプリケーション）を選択します。この例では、グループ化された特定のアプリケーションの静的グループを含む **Application Group**（アドレス グループ）を作成します。

   1. **Add**（追加）をクリックして、**New Application Group**（新規アプリケーション グループ）を選択します。
   2. **Add**（追加）をクリックし、グループに含めるアプリケーションを選択します。
   3. **OK** をクリックしてアプリケーション グループを作成します。

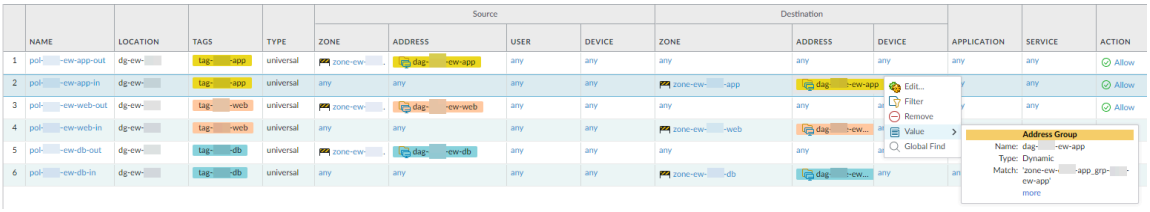
7. トラフィックについてのアクションを **Allow**（許可） または **Deny**（拒否） に指定し、任意でプロファイルのアンチウイルス、アンチスパイウェア、脆弱性防御のデフォルト セキュリティ プロファイルに関連付けます。
8. 前述のステップを繰り返し、関連するポリシー ルールを作成します。
9. **Commit**（コミット）をクリックし、Commit Typ（コミット タイプ）で **Panorama** を選択します。**OK**をクリックします。

STEP 2 | NSX-T用VM-Seriesファイアウォールにポリシーを適用します。

1. **Commit**（コミット）をクリックし、コミットタイプとして **Device Groups**（デバイス グループ）を選択します。
2. デバイス グループ（この例ではNSX-Tデバイス グループ）を選択し、**OK** をクリックします。
3. コミットが成功したことを確認します。

STEP 3 | ダイナミック アドレス グループのメンバーが、VM-Series ファイアウォール上に存在することを確認します。

1. Panorama からは、デバイス コンテキストを切り替えてポリシーのプッシュ対象のファイアウォールの Web インターフェイスを起動します。
2. VM-Series ファイアウォールで、**Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、ルールを選択します。
3. アドレス グループのリンクの隣にあるドロップダウンの矢印を選択し、**Inspect**（検査）をクリックします。一致条件が正確であるか確認することもできます。



4. **more**（詳細）リンクをクリックし、登録された IP アドレスのリストが表示されることを確認します。

   このアドレス グループに属し、ここに表示されるすべての IP アドレスについてポリシーが適用されます。

©2023 Palo Alto Networks, Inc.

STEP 4 | （任意）テンプレートを使用して、DNS サーバー、NTP サーバー、Syslog サーバー、およびログイン バナーなどのネットワーク基本設定およびデバイス設定をプッシュします。

テンプレートの使用については、『Panorama 管理者ガイド』を参照してください。

STEP 5 | ゾーン プロテクションのプロファイルを作成し、ゾーンに適用します。

ゾーン プロテクション プロファイルは、フラッド、ポートスキャン、ポート スイープやパケット ベースの攻撃に対する防御を行うことができます。これにより、データセンター内の仮想マシン間を移動する同じ層内および異なる層間のトラフィック、およびデータセンター内の仮想マシン（ワークロード）に向かうインターネットからのトラフィックを保護することができます。

1. **Template**（テンプレート）を選択します。
2. **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 プロファイル）を選択し、新規プロファイルの追加と編集を行います。
3. **Network**（ネットワーク） > **Zones**（ゾーン）を選択し、表示された default-zone を選んで、**Zone Protection Profile**（ゾーン プロテクション プロファイル）の中からプロファイルを選択します。

STEP 6 | DoS 防御のプロファイルを作成し、DoS 防御のポリシー ルールに適用します。

1. **Device Group**（デバイスグループ）を選択してください。
2. **Objects**（オブジェクト） > **Security Profiles**（セキュリティ プロファイル） > **DoS Protection**（**DoS** 防御）を選択し、新規プロファイルの追加と編集を行います。
   - 細かく分類されたプロファイルを作成することで、単一の送信元 IP に適用されるしきい値の設定が可能になります。たとえば、ポリシーに合致したIPアドレスに対して最大セッションレートを設定し、このしきい値がトリガされた際に、当該のIPアドレスをブロックすることができます。
   - 集約ポリシーを使用することで、ポリシーに合致するすべてのパケットに対して最大セッションレートを設定することができます。このしきい値は集約された全IPアドレスの新セッションレートに対して適用されます。しきい値がトリガされると、ポリシーに合致するトラフィックすべてに作用します。
3. **Policy**（ポリシー） > **DoS Protection**（**DoS** 防御）から新規の DoS 防御ポリシー ルールを作成し、新しいプロファイルを適用します。

ダイナミックアドレスグループメンバーシップ基準の作成

NSX-T では、NSX の Panorama プラグインで、NSX-T セキュリティグループ（ダイナミックアドレスグループ）に属する仮想マシンと IP セットのメンバーシップ基準を構成できます。ダイナミックアドレスグループごとに、サービス定義を指定し、最大 5 つの一致基準を定義する必要があります。各基準は、最大 5 つの一致ルールを備えています。

プラグインでこのメンバーシップ基準を作成し、それを *NSX-TManager* にプッシュします。ただし、これは、デプロイメント内のゲスト仮想マシンに対してメンバーシップ基準を適用しません。タグなどのメンバーシップデータを定義して、*NSX-TManager* のゲスト *VM* に適用する必要があります。

©2023 Palo Alto Networks, Inc.

NSX-T の Panorama プラグインは、仮想マシンまたは IP セットの 2 つのメンバーシップタイプに基づいて、仮想マシンを識別および分類します。各メンバータイプで使用できるキーと演算子を次の表に示します。

メンバータイプ	キー	演算子
IP セット	タグ	Equals
仮想マシン	• タグ • 名前 • OS 名 • コンピュータ名	• Equals • Contains • starts with • ends with • 等しくない（タグキーには適用されません）

メンバーシップ基準の変更は、*Panorama* でのみ行う必要があります。 *NSX-TManager* で変更しないでください。*NSX-T Manager* で変更すると、*VMware NSX* の *Panorama* プラグインはサービス定義を非同期として表示します。非同期ステータスの具体的な理由を確認するには、*[*非同期*]*リンクをクリックする必要があります。メンバーシップ基準の変更が原因である場合は、***[NSX-TConfig-Sync]***をクリックして構成の同期を実行します。

STEP 1 | [**Panorama** > **VMware** > **NSX-T** > メンバーシップ基準 > 追加]を選択します。

少なくとも 1 つのダイナミックアドレスグループを使用してサービス定義のメンバーシップ基準を追加または変更するには、[追加]をクリックする代わりにサービス定義名をクリックします。

STEP 2 | ［名前］から、メンバーシップ基準のサービス定義を選択します。選択したサービス定義は East_West 挿入タイプであり、セキュリティ中心のデプロイメントの一部として使用する必要があります。

STEP 3 | [追加]をクリックして、ダイナミックアドレスグループを指定します。

STEP 4 | ドロップダウンからダイナミックアドレスグループを選択します。ドロップダウンには、指定したサービス定義に関連付けられているダイナミックアドレスグループが一覧表示されます。

プラグイン *UI* は、*Panorama* で構成されたダイナミックおよびスタティックアドレスグループを表示します。メンバーシップ基準を構成するときに、誤ってスタティックアドレスグループを選択しないように注意してください。

STEP 5 | [追加]をクリックして、選択したダイナミックアドレスグループに関連付けられた基準を定義します。

STEP 6 | 基準の分かりやすい名前を入力します。

©2023 Palo Alto Networks, Inc.

STEP 7 | [追加]をクリックしてルールを定義します。

STEP 8 | ルールを定義します。最大 5 つのルールを作成できます。

1. ルールのわかりやすい名前を入力します。
2. メンバータイプ（仮想マシンまたは IP セット）を選択します。
3. キー（タグ、名前、OS 名、コンピューター名）を選択します。
4. 演算子（等しい、含む、で始まる、で終わる、等しくない）を選択します。
5. 値を入力します。

   キーをタグに設定する場合、値はタグになります。プラグインのユーザーインターフェースにはタグが表示されないため、Panorama CLI を使用する必要があります（NSX-T Manager 3.0.0 以降を使用）。

   request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
6. (任意)スコープを入力します。スコープは、キーがタグの場合のみ適用されます。スコープは、NSX-T のオブジェクトタグに適用されるオプションの値です。スコープは NSX-TManager で定義されます。たとえば、オペレーティングシステムに基づいて仮想

 ©2023 Palo Alto Networks, Inc.

マシンにタグを付ける場合、Windows、Linux、および MacOS のタグを作成してから、各タグのスコープを OS に設定できます。

タグとスコープを表示するには、Panorama CLI （NSX-T Manager 3.0.0 以降）を使用します。

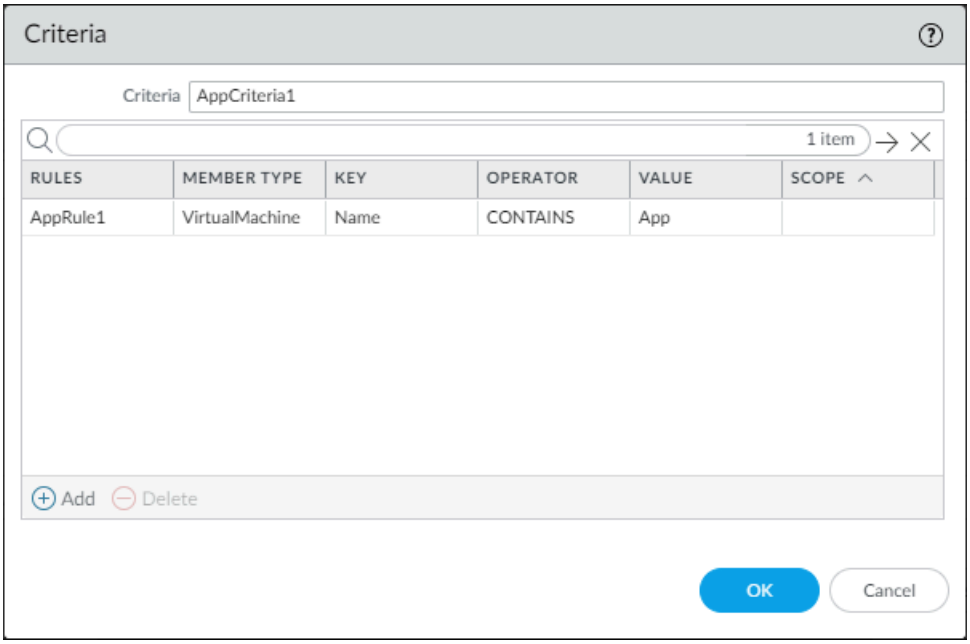
次のコマンドを実行して、タグのリストを表示します。

request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>

次のコマンドを実行して、指定したタグに関連付けられているスコープを表示します。

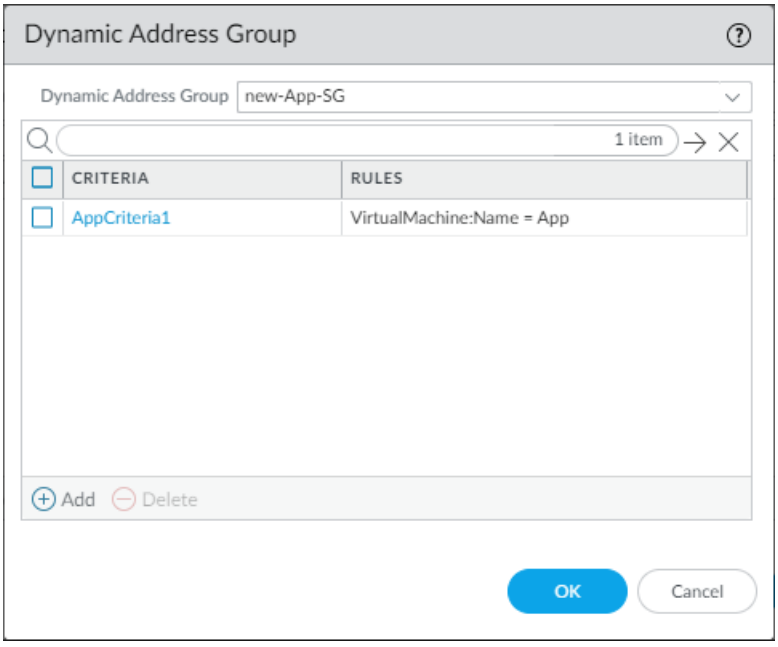
request plugins vmware_nsx nsx_t nsxt-scope tag <tag_value> service-definition <SD-name>

7. **OK** をクリックします。
8. (任意)[追加]をクリックして、追加の（合計で最大 5 つ）ルールを作成します。

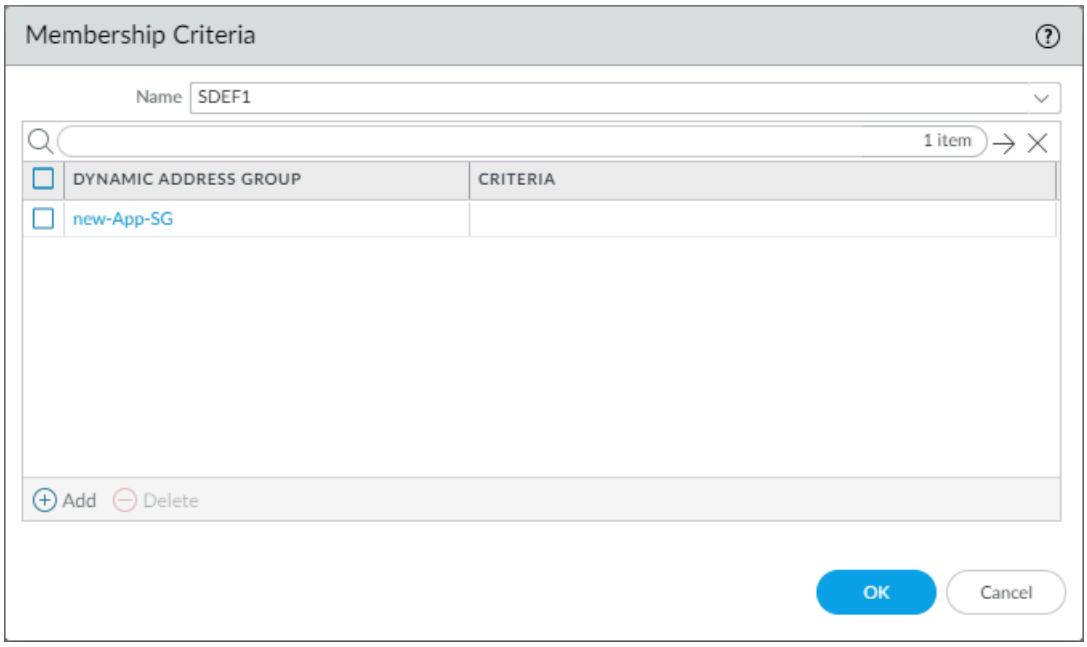


©2023 Palo Alto Networks, Inc.

STEP 9 | [ダイナミックアドレスグループ]ウィンドウで、[**OK**]をクリックして終了するか、あるいは[追加]をクリックして追加の基準（合計 5 つまで）とルールを作成します。



STEP 10 | [メンバーシップ基準]ウィンドウで、[**OK**]をクリックして終了するか、あるいは[追加]をクリックして追加のダイナミックアドレスグループを指定します。



ステアリングポリシーの生成

ステアリングポリシーは、トラフィックがステアリングされるサービスチェーンを定義するために NSX-T によって使用されます。ステアリングポリシーは、手動で作成することも、自動生成することもできます。

©2023 Palo Alto Networks, Inc.

ステアリングポリシーを自動生成すると、VMware NSX-T の Panorama プラグインは、指定された各サービスマネージャーと関連するサービス定義に対するステアリングポリシーを作成します。デフォルトでは、TCP strict は無効になっており、失敗ポリシーは[許可]に設定されています。自動生成されるポリシーは、**auto_<service-def-name>_<zone-name>_steering_policy**の命名形式を使用します。

TCP Strict が有効になっている場合、ファイアウォールは 3 ウェイハンドシェイクの要件を適用します。ファイアウォールがセッションの途中でトラフィックを取得し（たとえば、非対称トラフィックが原因で）、3 ウェイハンドシェイクを検出しない場合、セッションはドロップされます。詳細については、VMware NSX-T のマニュアルを参照してください。

失敗ポリシーには、ファイアウォールがダウンした場合にトラフィックに何が起こるかが定義されます。[許可]を選択すると、トラフィックは宛先への進行を続けます。[ブロック]を選択すると、トラフィックはドロップされます。

さらに、特定のサービスマネージャーを選択する代わりに、すべてのサービスマネージャーを選択するオプションがあります。サービスマネージャのいずれかに操作中心のサービス定義が含まれている場合は、[すべて]を選択することはお勧めしません。プラグインは、操作中心のサービス定義に関連付けられた各ゾーンのステアリングポリシーを作成し、それを NSX-TManager にプッシュします。[すべて]を選択する場合は、ステアリングポリシーを自動生成するときに選択するサービスマネージャーに、セキュリティ中心のサービス定義のみが含まれていることを確認してください。

ステアリングポリシーを自動生成する場合は、ステアリングルールも自動生成する必要があります。また、ステアリングポリシーを手動で作成する場合、ステアリングルールも手動で作成する必要があります。

- ステアリングルールの自動生成
- ステアリングポリシーの手動作成

ステアリングポリシーの変更は、*Panorama* でのみ行う必要があります。 *NSX-TManager* で変更しないでください。*NSX-T Manager* で変更すると、*VMware NSX* の *Panorama* プラグインはサービス定義を非同期として表示します。非同期ステータスの具体的な理由を確認するには、*[非同期]*リンクをクリックする必要があります。ステアリングポリシーの変更が原因である場合は、***[NSX-TConfig-Sync]***をクリックして構成の同期を実行します。

ステアリングルールの自動生成

次の手順を使用して、ステアリングポリシーを自動生成します。

次の手順は、*[すべて]* を選択する代わりに、サービスマネージャーを指定するためのものです。

STEP 1 | **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ポリシーを選択します。

STEP 2 | [自動生成]をクリックします。

 ©2023 Palo Alto Networks, Inc.

STEP 3 | サービスマネージャーの場合は、[選択] を選択します。

特定のサービスマネージャーを選択する代わりに*[すべて]*を選択すると、プラグインは、構成内の各サービスマネージャーに関連付けられた各サービス定義のステアリングポリシーを生成します。さらに、選択したサービスマネージャーにセキュリティ中心のサービス定義が組み入れられていることを確認してください。

STEP 4 | [追加]をクリックして、サービスマネージャーを選択します。

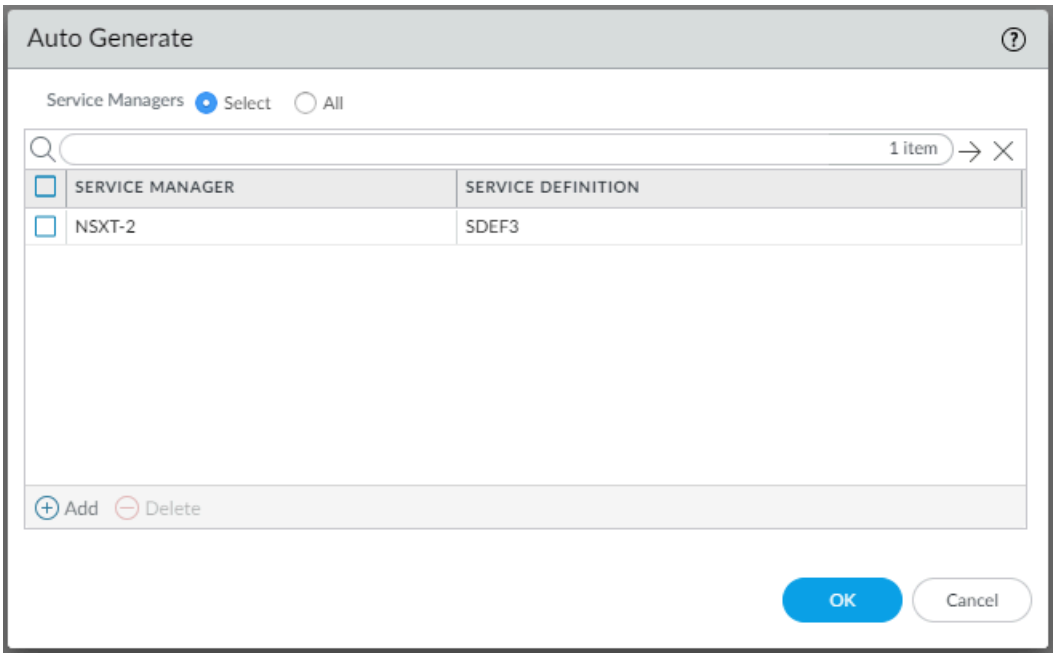
STEP 5 | ドロップダウンからサービスマネージャーを選択します。

STEP 6 | [追加]をクリックして、サービス定義を選択します。

STEP 7 | ドロップダウンからサービス定義を選択します。

STEP 8 | [**OK**]をクリックして、もう一度[**OK**]をクリックします。

STEP 9 | 変更を Panorama にコミットします。



ステアリングポリシーの手動作成

次の手順を使用して、ステアリングポリシーを手動で作成します。

STEP 1 | **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ポリシーを選択します。

STEP 2 | [追加] をクリックします。

STEP 3 | ステアリングポリシーのわかりやすい名前を入力します。

ステアリングポリシー名中にスペースを使用することはできません。

©2023 Palo Alto Networks, Inc.

STEP 4 | ドロップダウンからサービス定義を選択します。

STEP 5 | ドロップダウンからサービスチェーンを選択します。

STEP 6 | （任意）**TCPStrict**を有効にします。このオプションはデフォルトでは無効になっています。

STEP 7 | 失敗ポリシーの許可またはブロックを選択します。[許可]がデフォルトです。

STEP 8 | **OK** をクリックします。

STEP 9 | 変更を Panorama にコミットします。



ステアリングルールの生成

ステアリングルールはステアリングポリシーで定義されます。ルールは、トラフィックの送信元と宛先、イントロスペクションサービス、ルールが適用される NSX-T オブジェクト、およびトラフィックリダイレクトポリシーを定義します。ステアリングルールを手動で作成することも、ステアリングルールを自動的に生成することもできます。

ステアリングルールを生成または作成する前に、ステアリングポリシーを生成または作成する必要があります。

Panorama で作成されたセキュリティルールに基づいてステアリングルールを自動生成するには、セキュリティルールが次の基準を満たしている必要があります。

- NSX-T サービス マネージャーに登録されている親または子のデバイスグループに所属する。
- ゾーン内ポリシーであり、1 つのゾーンのみが入っている。
- ルール用に構成されたスタティックアドレスグループ、IP 範囲、またはネットマスクは組み入れられていない。

自動生成されたステアリングルールは、**auto_<device-group-name>_<device-group-rule-name>**の命名形式を使用します。

デフォルトでは、自動生成されたステアリングルールは、NSX サービスを指定せずに構成されます。さらに、NSX トラフィックの方向は in-out に設定され、ロギングは無効になり、IP プロトコルは ipv4-ipv6 になり、アクションはリダイレクトに設定されます。ルールを自動生成した後、ステアリングを更新してデフォルト値を変更できます。

©2023 Palo Alto Networks, Inc.

さらに、特定のサービスマネージャーを選択する代わりに、すべてのサービスマネージャーを選択するオプションがあります。すべてを選択することはお勧めしません。

ステアリングポリシーを自動生成する場合は、ステアリングルールも自動生成する必要があります。また、ステアリングポリシーを手動で作成する場合は、ステアリングルールも手動で作成する必要があります。

- ステアリングルールの自動生成
- ステアリングルールの手動作成

ステアリングルールの変更は、*Panorama* でのみ行う必要があります。 *NSX-T Manager*で変更しないでください。*NSX-T Manager* で変更すると、*VMware NSX* の *Panorama* プラグインはサービス定義を非同期として表示します。非同期ステータスの具体的な理由を確認するには、*[非同期]*リンクをクリックする必要があります。ステアリングルールの変更が原因である場合は、***[NSX-TConfig-Sync]***をクリックして構成の同期を実行します。

ステアリングルールの自動生成

次の手順を使用して、ステアリングルールを自動生成します。

ステアリングルールを自動生成する場合、ルールが適用される場所（NSX-T 分散ファイアウォールまたはセキュリティグループ）は、セキュリティルールの構成時に指定した送信元と宛先によって異なります。送信元または宛先に [任意] を選択した場合、NSX-TManager はステアリングルールを分散ファイアウォールに適用します。送信元と宛先にダイナミックアドレスグループを選択した場合、ステアリングはそれらのセキュリティグループ内のゲスト仮想マシンに適用されます。

ステアリングルールの[適用先]設定にマップされる送信元アドレスグループと宛先アドレスグループなど、ステアリングルール構成の一部でもあるデバイスグループ構成に変更を加える場合、変更を有効にするには、ステアリングルールを再度自動生成する必要があります。

次の手順は、*[すべて]* を選択する代わりに、サービスマネージャーを指定するためのものです。

STEP 1 | **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ルールを選択します。

STEP 2 | [自動生成]をクリックします。

STEP 3 | ドロップダウンからセキュリティルールのタイプを選択します - すべて、プレルールベースのみ、またはポストルールベースのみ。セキュリティルールは、次の手順で指定されたサービス定義から取得されます。

ステアリングルールを再生成すると、現在のすべてのルールが削除され、選択したルールベースに基づいて新しいルールが作成されます。プレルールベースを使用してステアリングルールを最初に作成し、ポストルールベースを使用してステアリングルールを再生成した場合、ポストルールベースのステアリングルールのみが残ります。

©2023 Palo Alto Networks, Inc.

STEP 4 | [タイプ]で、[選択]を選択します。

STEP 5 | [追加]をクリックして、サービスマネージャーとサービス定義を指定します。

STEP 6 | ドロップダウンからサービスマネージャーを選択します。

STEP 7 | [追加]をクリックして、サービス定義を選択します。

STEP 8 | **OK** をクリックします。

STEP 9 | [**OK**]をクリックして終了するか、または[追加]をクリックして追加のサービスマネージャーとサービス定義を指定します。

STEP 10 | (任意) 自動生成されたルールをクリックして、次のデフォルトオプションを変更します。

ステアリングルールを再生成すると、以前に生成されたステアリングルールに加えた変更はすべて上書きされます。

- NSX-T ロギングを有効にします。
- [追加]をクリックして、Active Directory サーバー、HTTPS、DNS などの**NSX**サービスを指定します。
- ルールを無効にします。ステアリングルールを無効にしても、対応するセキュリティルールが有効になっている場合（デバイスグループ > ポリシー > セキュリティ）、ステアリングルールも有効になります。
- 適用先では、ステアリングルールを適用する場所（**DFW**またはセキュリティグループ）を変更できます。

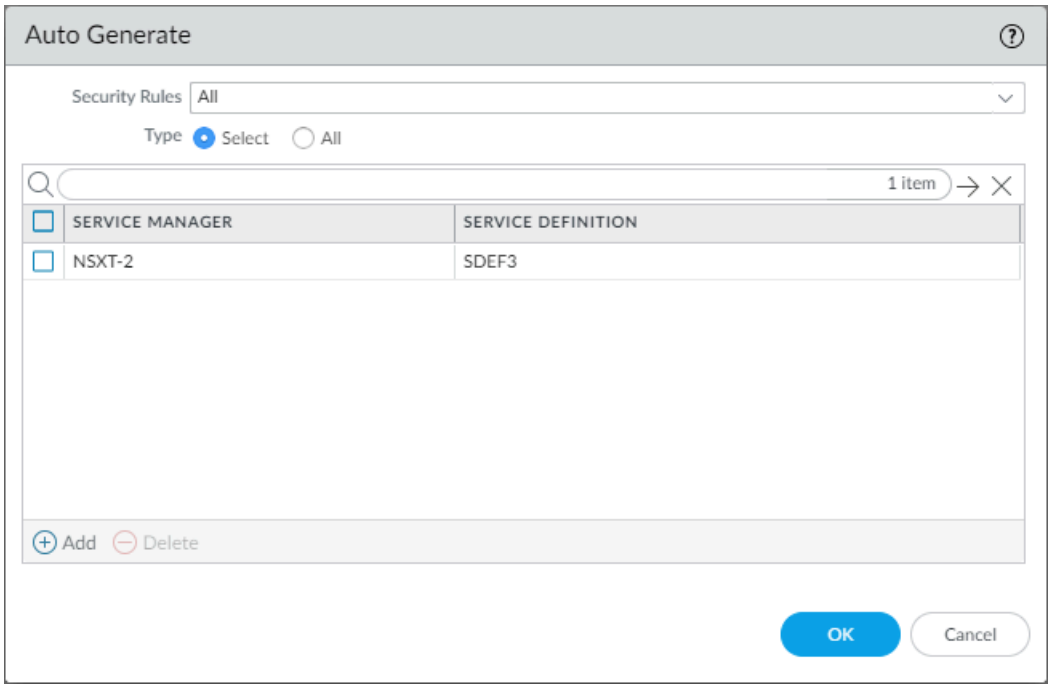
STEP 11 | 不要または誤ったステアリングルールをクリーンアップします。

たとえば、NSX-T ステアリングルールと同じルールベースのセキュリティルールがデバイスグループにく組み入れられている場合、プラグインはそれらの非 NSX-T セキュリティルールに基づいてセキュリティルールを生成します。これらのルールは NSX-T ダイナミックアドレスグループを参照しないため、これらのルールの送信元と宛先は NSX-TManager 内で AnyAny に設定されます。この状態は、NSX-TManager がトラフィックを転送する方法に影響を与える可能性があります。これを回避するには、誤ったステアリングルールを手動で削除する必要があります。

1. 間違ったステアリングルールを選択します。
2. **[削除]** をクリックします。
3. はいをクリックして、削除を確認します。

©2023 Palo Alto Networks, Inc.

STEP 12 | 構成をコミットして、NSX-T Manager にプッシュします。



ステアリングルールの手動作成

次の手順を使用して、ステアリングルールを手動で作成します。

STEP 1 | **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ルールを選択します。

STEP 2 | **[追加]** をクリックします。

STEP 3 | ステアリングルールのわかりやすい名前を入力します。

ステアリングルール名にスペースを使用することはできません。

STEP 4 | ドロップダウンからステアリングポリシーを選択します。

STEP 5 | 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。

STEP 6 | ドロップダウンからセキュリティルールを選択します。

*[セキュリティルール]*ドロップダウンには、サービス定義のすべてのデバイスグループのすべてのセキュリティルールのルールが表示されます。適切なセキュリティルールを選択していることを確認してください。

STEP 7 | アクション(リダイレクト または リダイレクトしない) を選択します。

STEP 8 | (任意) NSX-T ロギングを有効にします。

STEP 9 | **IP** プロトコル(**ipv4-ipv6**、**ipv4**、または **ipv6**）を指定します。

©2023 Palo Alto Networks, Inc.

STEP 10 | **NSX** トラフィックの方向（**in-out**、**in**、または**out**）を指定します。

STEP 11 | （任意）[追加]をクリックして、Active Directory サーバー、HTTPS、DNS などの **NSX** サービスを指定します。

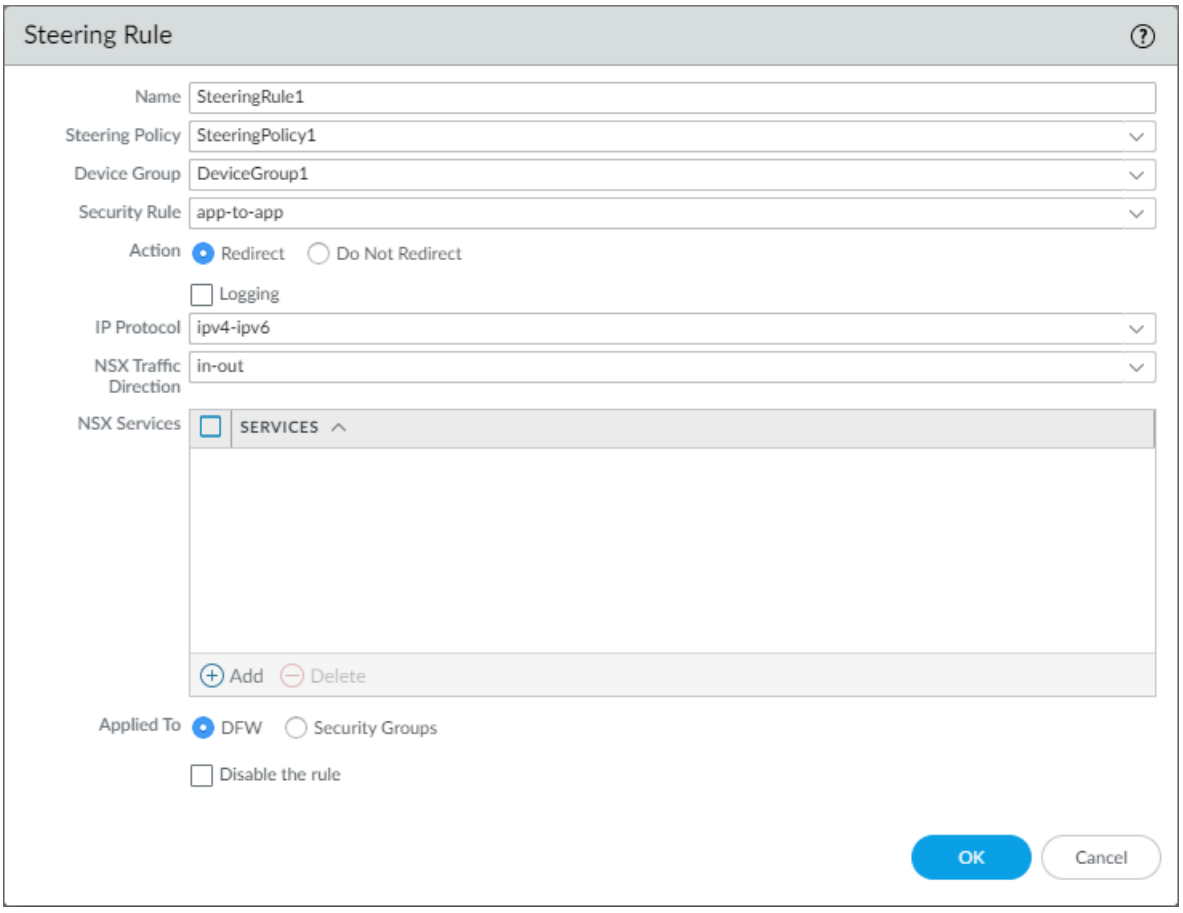
次の *ALG* サービスはサポートされていません。*FTP*、*TFTP*、*ORACLE_TNS*、*SUN_RPC_TCP*、*SUN_RPC_UDP*、*MS_RPC_TCP*、*MS_RPC_UDP*、*NI*

STEP 12 | 適用先は、**DFW**またはセキュリティグループです。1 つ以上のセキュリティグループを選択できます。セキュリティグループは、Panorama で構成されたダイナミックアドレスグループから作成されます。セキュリティグループ名の形式は、**<servicedefinition>_<dynamic-address-group>** となります。DFW を選択すると、セキュリティメンバーシップに関係なく、すべてのゲスト VM にステアリングルールが適用されます。

STEP 13 | (任意)ルールを無効にします。

STEP 14 | **OK** をクリックします。

STEP 15 | 構成をコミットして、NSX-T Manager にプッシュします。



 ©2023 Palo Alto Networks, Inc.

Panorama からのサービス定義の削除

Panorama の NSX-T 設定からサービス定義を削除するには、次の手順を実行します。

STEP 1 | Panorama にログインします。

STEP 2 | セキュリティ中心のデプロイメントの場合は、削除するサービス定義に関連付けられているステアリングルールとステアリングポリシーを削除します。

1. **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ルールを選択します。
2. 削除するステアリングルールを選択します。
3. **[削除]** をクリックします。
4. **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ポリシーを選択します。
5. 削除するステアリングポリシーを選択します。
6. **[削除]** をクリックします。

STEP 3 | 変更を **Commit (コミット)** します。

STEP 4 | 削除するサービス定義に関連付けられている NSX-T にデプロイされている VM-Series ファイアウォールを削除します。

STEP 5 | サービス定義に関連付けられているメンバーシップ条件を削除します。

1. **Panorama** > **VMware** > **NSX-T** > メンバーシップ基準を選択します。
2. 削除する条件を選択します。
3. **[削除]** をクリックします。

STEP 6 | 関連付けられているサービスマネージャからサービス定義のリンクを解除します。

1. **Panorama** > **VMware** > **NSX-T** > **Service Managers**（サービス マネージャー）を選択します。
2. サービス マネージャー名をクリックします。
3. サービス定義を選択します。
4. **[削除]** をクリックします。
5. **OK** をクリックします。

STEP 7 | 変更を Panorama にコミットします。

NSX-T 運用上の VM-Series からのセキュリティ中心デプロイメントへの移行

業務中心の NSX-T デプロイメントをセキュリティ中心の NSX-T 環境に移行するには、次の手順に従います。

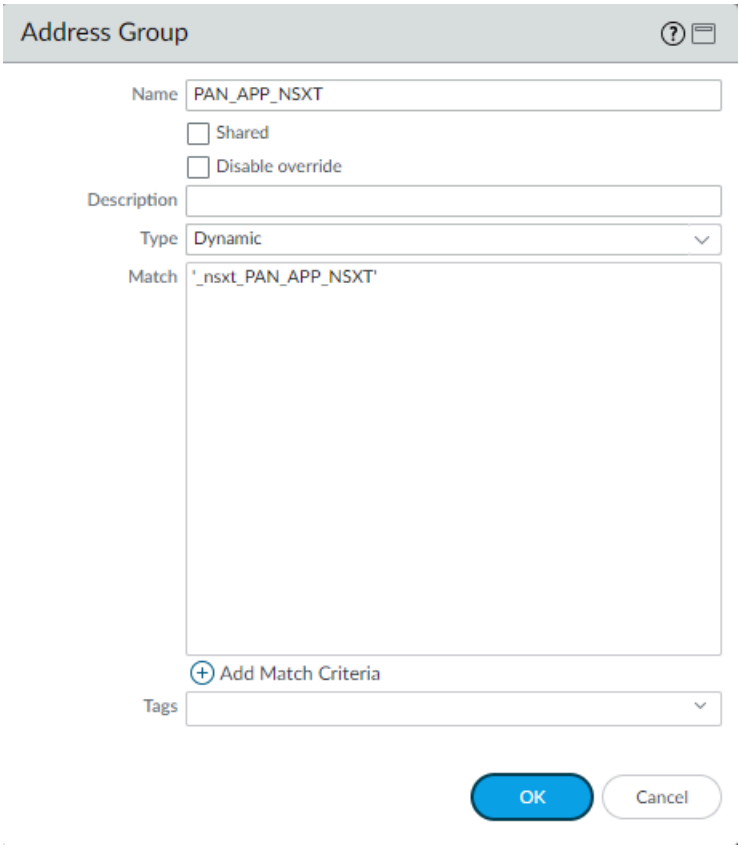
STEP 1 | Panorama にログインします。

©2023 Palo Alto Networks, Inc.

STEP 2 | ダイナミックアドレスグループの一致基準を、セキュリティ中心のデプロイメントに必要な形式に従うように変更します。

1. **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. NSX-V サービス定義に関連付けられているデバイスグループでダイナミックアドレスグループが設定されていることを確認します。
3. 以前に作成した NSX-T ダイナミックアドレスグループの名前をクリックします。
4. 一致条件を編集します。

   ダイナミックアドレスグループを *NSX-V Manager* のセキュリティ グループにするには、一致条件の文字列を一重引用符で囲み、*_nsx_* というプレフィックスを付けてアドレスグループの正確な名前を続ける必要があります。たとえば、***'_nsxt_PAN_APP_NSX'*** のようにします。
5. 必要なセキュリティ グループごとにこの操作を繰り返します。



©2023 Palo Alto Networks, Inc.

STEP 3 | セキュリティルールを NSX-T ステアリングルールとして intrazone に対して設定します。

1. Panorama で **Policies**（ポリシー） > **Security**（セキュリティ） > **Pre Rules**（プレルール）を選択します。
2. NSX-T サービス定義に関連付けられたデバイスグループで、セキュリティルールを設定していることを確認します。
3. **Add**（追加）をクリックし、セキュリティ ポリシー ルールの **Name**（名前）と **Description**（説明）を入力します。
4. Rule Type（ルール タイプ）を **intrazone**（**Devices with PAN-OS 6.1 or later)**（イントラゾーン（**PAN-OS 6.1** 以降を搭載したデバイス））に設定します。
5. Source（送信元）タブで、source zone（送信元ゾーン）を、サービス定義に関連付けられているテンプレート スタックからのゾーンに設定します。次に、前に送信元アドレスとして作成したダイナミック アドレスグループを選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを送信元アドレスとして追加しないでください。
6. Destination（宛先）タブでは、宛先ゾーンを設定することができません。これは、rule type（ルール タイプ）が intrazone（イントラゾーン）に設定されているためです。次に、前に宛先アドレスとして作成したダイナミック アドレスグループを選択します。スタティック アドレス グループ、IP 範囲、ネットマスクを宛先アドレスとして追加しないでください。
7. **OK**をクリックします。
8. 必要なステアリング ルールごとにステップ 1 ～ 7 を繰り返します。
9. 変更を **Commit**（コミット）します。

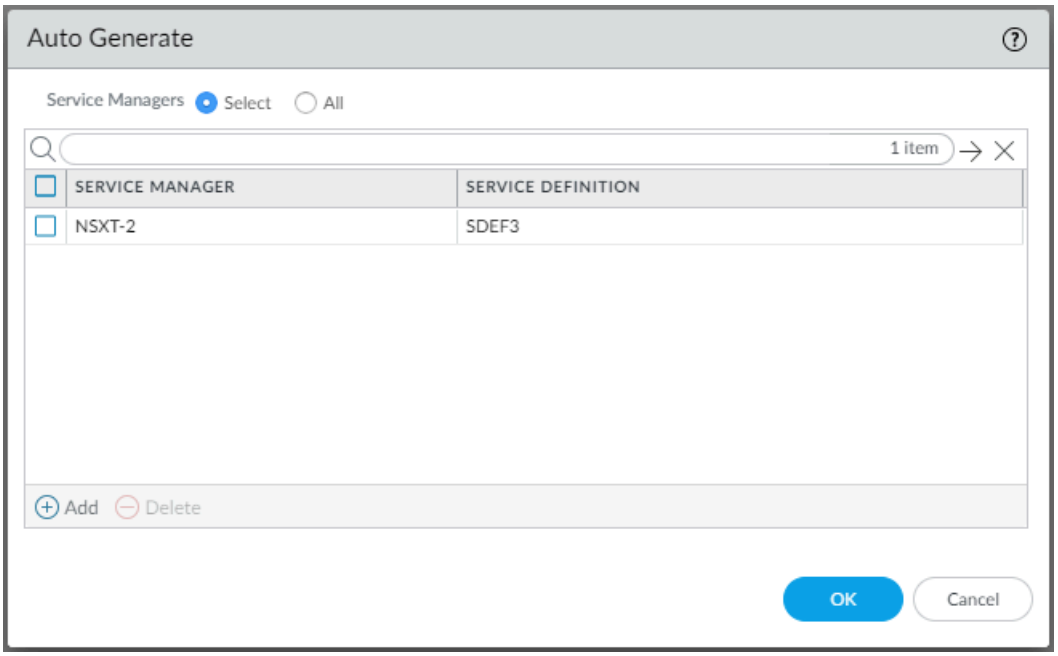
©2023 Palo Alto Networks, Inc.

STEP 4 | 新しいステアリングポリシーを自動生成します。

次の手順は、[すべて] を選択する代わりに、サービスマネージャーを指定するためのものです。

1. **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ポリシーを選択します。
2. [自動生成]をクリックします。
3. サービスマネージャーの場合は、[選択] を選択します。

   特定のサービスマネージャーを選択する代わりに*[すべて]*を選択すると、プラグインは、構成内の各サービスマネージャーに関連付けられた各サービス定義のステアリングポリシーを生成します。
4. [追加]をクリックして、サービスマネージャーを選択します。
5. ドロップダウンからサービスマネージャーを選択します。
6. [追加]をクリックして、サービス定義を選択します。
7. ドロップダウンからサービス定義を選択します。
8. [**OK**]をクリックして、もう一度[**OK**]をクリックします。



9. 変更を **Commit (コミット)** します。

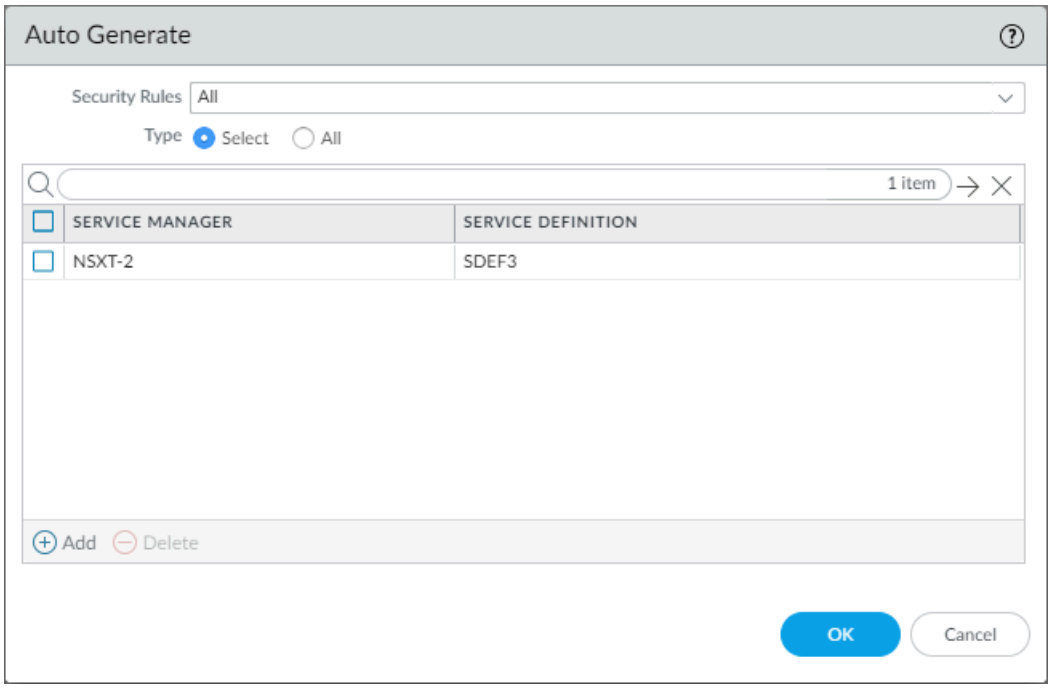
©2023 Palo Alto Networks, Inc.

STEP 5 | 新しいステアリングルールを自動生成します。

ステアリングポリシーを自動生成する場合は、ステアリングルールも自動生成する必要があります。また、ステアリングポリシーを手動で作成する場合は、ステアリングルールも手動で作成する必要があります。

次の手順は、*[すべて]* を選択する代わりに、サービスマネージャーを指定するためのものです。

1. **Panorama** > **VMware** > **NSX-T** > ネットワークイントロスペクション > ルールを選択します。
2. [自動生成]をクリックします。
3. ドロップダウンからセキュリティルールのタイプを選択します - すべて、プレルールベースのみ、またはポストルールベースのみ。セキュリティルールは、次の手順で指定されたサービス定義から取得されます。
4. [タイプ]で、[選択]を選択します。
5. [追加]をクリックして、サービスマネージャーとサービス定義を指定します。
6. ドロップダウンからサービスマネージャーを選択します。
7. [追加]をクリックして、サービス定義を選択します。
8. **OK** をクリックします。
9. [**OK**]をクリックして終了するか、または[追加]をクリックして追加のサービスマネージャーとサービス定義を指定します。
10. (任意) 自動生成されたルールをクリックして、デフォルトオプションを変更します。



STEP 6 | ダイナミックアドレスグループメンバーシップ基準の作成.

STEP 7 | 変更を Panorama にコミットします。

©2023 Palo Alto Networks, Inc.

STEP 8 | NSX-T Manager から業務中心のステアリングルールを削除します。

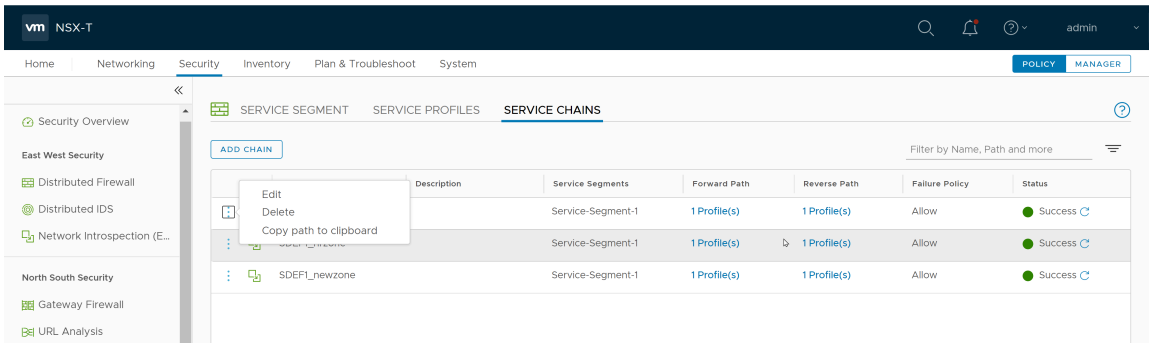
1. NSX-T Manager にログインします。
2. セキュリティ > ネットワークイントロスペクション **(E-W)** > ルールを選択します。
3. 業務中心の各ステアリングルールを選択します。
4. **[削除]** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 9 | NSX-T Manager から業務中心のサービスチェーンを削除します。

1. NSX-T Manager にログインします。
2. セキュリティ > ネットワークイントロスペクション設定 > サービスチェーン を選択します。
3. 垂直の省略記号をクリックします。
4. **[削除]** をクリックします。

©2023 Palo Alto Networks, Inc.



NSX-VからNSX-Tへのセキュリティ ポリシーの拡張

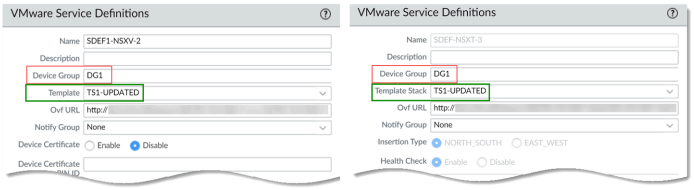
NSX-Vデプロイ環境からNSX-Tデプロイ環境またはNSX-Tデプロイ環境とNSX-Vデプロイ環境の組み合わせに移動する場合、ポリシールールを再度作成することなく、既存のセキュリティポリシーをNSX-VからNSX-Tに拡張することができます。そのためには、既存のデバイスグループを

©2023 Palo Alto Networks, Inc.

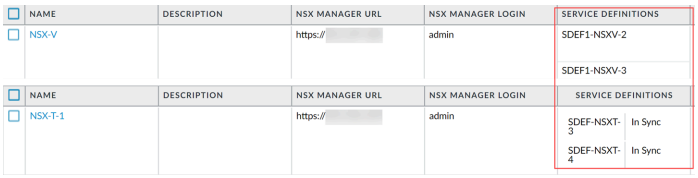
活用して、NSX-VおよびNSX-Tサービス定義間でそれらを共有します。ポリシーをNSX-Tに移行したら、NSX-VでVM-Seriesを使用し続ける、またはNSX-Vデプロイ環境を削除することができます。

STEP 1 | VMware NSX 用 Panorama プラグインのインストール 3.2.0以降。アップグレードする前に、「Panorama Plugin for VMware NSX 3.2.0リリースノートを参照してください。

STEP 2 | デプロイ環境内の各NSX-Vサービス定義に対して、NSX-Tサービス定義を設定します。新しいデバイスグループを作成しないでください。その代わりに、既存のNSX-Vデバイスグループを使用してください。既存のデバイスグループを使用することで、NSX-Vで使われていたのと同じセキュリティポリシールールを、NSX-TにデプロイされたVM-Seriesファイアウォールで利用することができます。特定のゾーンを参照するポリシーがある場合、NSX-Vサービス定義と同じテンプレートスタックを、NSX-Tサービス定義に追加してください。また、デバイスグループが特定のテンプレートを参照している場合は、デバイスグループで参照されているテンプレートを含むテンプレートスタックを選択していることを確認してください。



STEP 3 | NSX-Tサービス管理を設定して、NSX-Tサービス定義をサービスマネージャーに関連付けます。



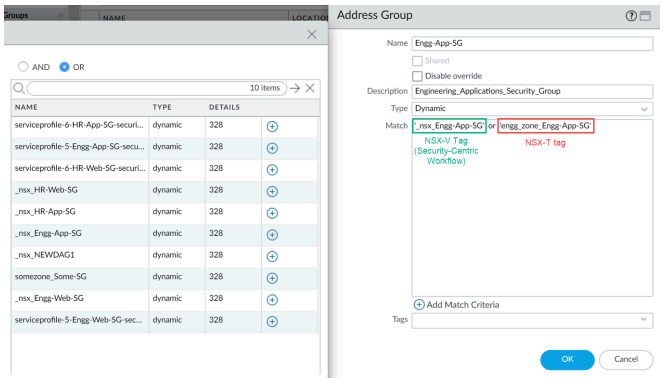
STEP 4 | NSX-T環境を準備して、VM-Seriesファイアウォールをデプロイします。VM-Seriesファイアウォールを起動する前に、セキュリティグループ、サービスチェーン、およびトラフィックリダイレクトポリシーを作成する必要があります。

- NSX-T（North-South）での VM-Series ファイアウォールのデプロイ
- 業務中心のワークフローを使用した VM-Series のデプロイ

©2023 Palo Alto Networks, Inc.

STEP 5 | 既存のダイナミックアドレスグループにNSX-Tタグを追加します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. 既存のNSX-Vダイナミックアドレスグループの名前をクリックします。
3. **Add Match Criteria**（一致条件の追加）をクリックして、NSX-VおよびNSX-Tのタグを表示します。
4. NSX-Tタグを、ダイナミックアドレスグループに追加します。タグ間には、**OR**演算子を使用してください。
5. 必要なタグをすべて追加したら、**OK**をクリックします。
6. 変更を **Commit (コミット)** します。



STEP 6 | NSX-VからNSX-TにVMワークフローが正常に移行された後、NSX-Vの使用を中止する場合は、ダイナミックアドレスグループからNSX-Vタグを削除してください。Panorama plugin for NSXからNSX-V関連の設定がすべて削除されると、NSX-Vタグと対応するIPアドレスの登録がすべて解除され、VM-Seriesファイアウォール設定がNSX-V Managerから削除されます。

NSX-VからNSX-TにVM-Seriesを移動するための定位置移行の使用

NSX-VからNSX-TにVM-Seriesファイアウォール設定を移行するには、次の作業を行ってください。設定を移行することで、Panoramaにすでに設定されているポリシーとダイナミックアドレスグループを再利用することができます。この作業は、VMwareドキュメントで公開されている情報やプロセス、およびPANに固有のステップを参考にしています。

この作業は、オペレーションセントリックのNSX-Vデプロイ環境のみをサポートしています。デプロイメントとは、VM-Series ファイアウォールにトラフィックをリダイレクトするポリシールールが、Panorama ではなく NSX-V Manager で作成されたことを意味しています。

この作業には、*NSX-T Manager 3.1.0*以降が必要になります。

この移行の実施中のセキュリティのダウンタイムを検討することをおすすめします。

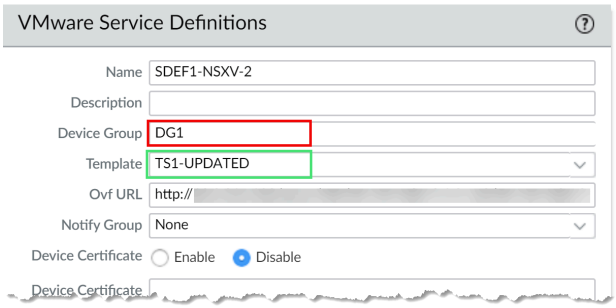
STEP 1 | VMwareが説明しているステップに基づいて、移行するためのNSX-VとNSX-T環境の準備を行います。

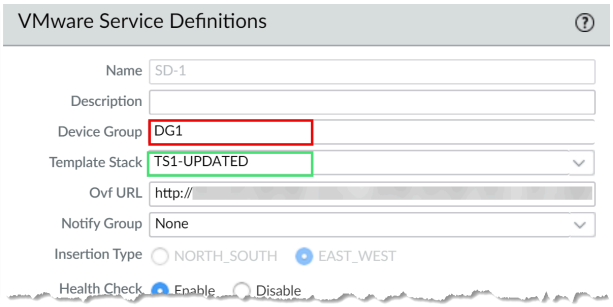
©2023 Palo Alto Networks, Inc.

STEP 2 | VMware NSX 用 Panorama プラグインのインストール 3.2.0以降。アップグレードする前に、「Panorama Plugin for VMware NSX 3.2.0リリースノートを参照してください。

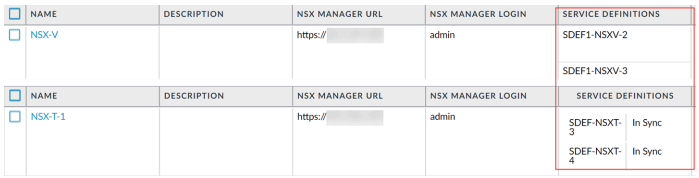
STEP 3 | NSX-T Manager と Panorama 間の通信の有効化.

STEP 4 | デプロイ環境内の各NSX-Vサービス定義に対して、NSX-Tサービス定義を設定します。新しいデバイスグループを作成しないでください。その代わりに、既存のNSX-Vデバイスグループを使用してください。既存のデバイスグループを使用することで、NSX-Vで使われていたのと同じセキュリティポリシールールを、NSX-TにデプロイされたVM-Seriesファイアウォールで利用することができます。特定のゾーンを参照するポリシーがある場合、NSX-Vサービス定義と同じテンプレートスタックを、NSX-Tサービス定義に追加してください。また、デバイスグループが特定のテンプレートを参照している場合は、デバイスグループで参照されているテンプレートを含むテンプレートスタックを選択していることを確認してください。





STEP 5 | NSX-Tサービス管理を設定して、NSX-Tサービス定義をサービスマネージャーに関連付けます。



STEP 6 | NSX-T Managerに、NSX-T設定が存在していることを確認します。

1. NSX-T Manager にログインします。
2. **System**（システム） > **Service Deployments**（サービスのデプロイ） > **Catalog**（カタログ）を選択します。
3. NSX-Tサービス定義が記載されていることを確認します。
4. **Security**（セキュリティ） > **Network Introspection Settings**（ネットワーク診断設定） > **Service Profiles**（サービスプロファイル）を選択します。
5. NSX-Tテンプレートと関連しているゾーンが記載されていることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 7 | まだそうしていない場合は、NSX-T ManagerにCompute Managerを追加します。Registration Status（登録ステータス）およびConnection Status（接続ステータス）がアップ状態であることを確認したら、以下の作業を続行します。

STEP 8 | NSX-V設定をNSX-Tにインポートします。

STEP 9 | NSX-Vから、サービスインスタンスをアンインストールします。



このステップにより、トラフィックが中断されます。

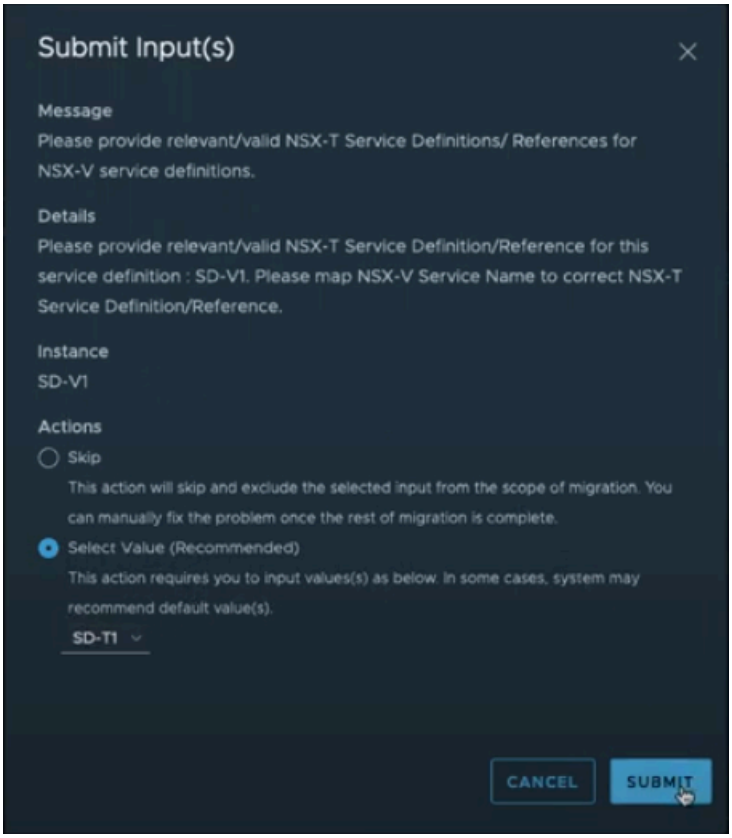
1. vSphereクライアントにログインします。
2. **Installation and Upgrade**（インストールとアップグレード） > **Service Deployment**（サービスデプロイ）を選択します。
3. サービスデプロイを選択します。
4. **[削除]** をクリックします。
5. 確認して、**Delete**（削除）をクリックします。

STEP 10 | NSX-T Manager上で、設定の問題を解決します。設定上の問題を解決している間に、VM-Seriesファイアウォール設定を移行するための特定のアクションを実施する必要がありま

©2023 Palo Alto Networks, Inc.

す。たいていの場合、NSX-T Managerが表示する推奨事項をそのまま受け入れることができます。

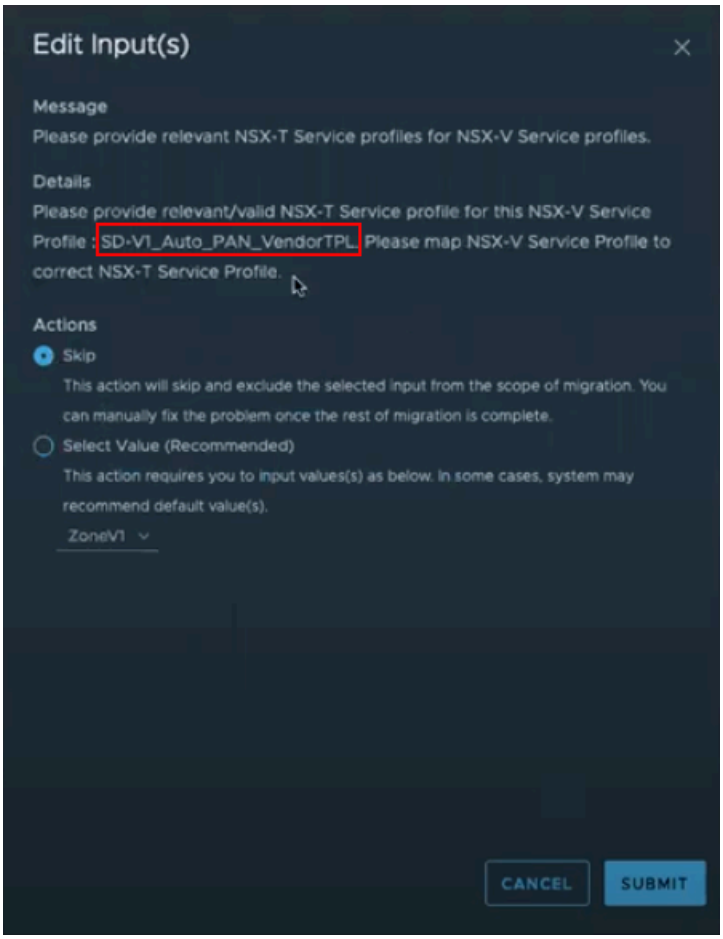
1. サービス挿入設定を解決する場合、NSX-T上のVM-Series用に、以前にPanoramaで設定した正しいサービス定義を選択していることを確認してください。



2. 残りの設定の解決作業を行います。
3. **Migrate Configuration**（設定の移行）に進む前に、サービス挿入のトランスポートゾーンを指定するように問い合わせるメッセージが表示されます。
4. NSX-Vのサービスプロファイルを、NSX-Tの対応するサービスプロファイルにマップします。

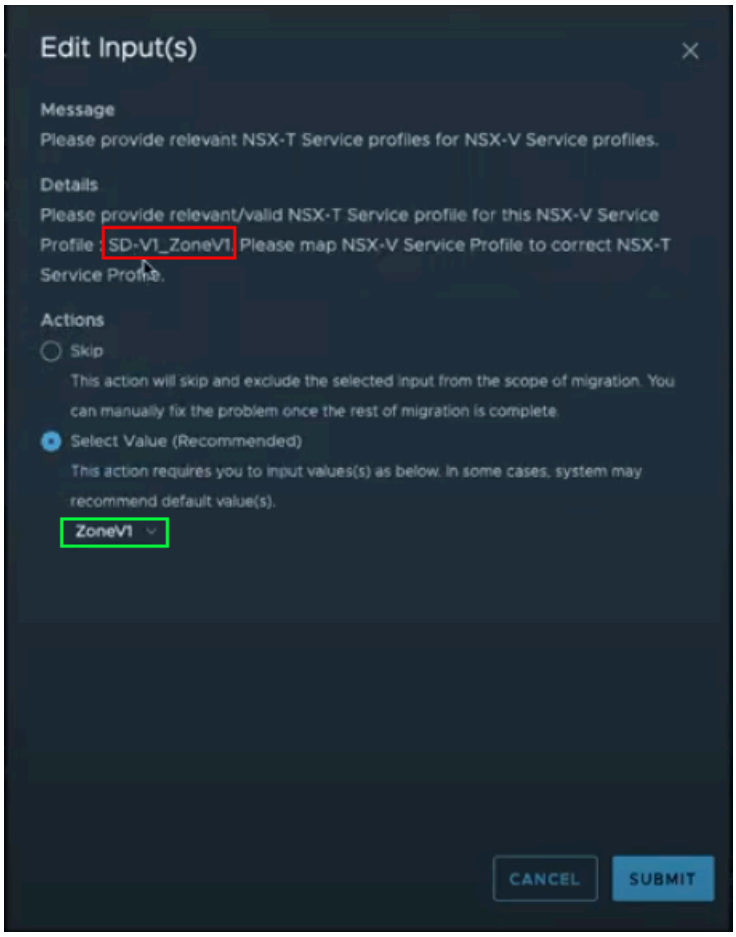
   1. Auto_PAN_VendorTPLはスキップすることができます。

©2023 Palo Alto Networks, Inc.



2. NSX-Tサービスプロファイルを、対応するNSX-Vサービスプロファイルにマップします。

©2023 Palo Alto Networks, Inc.



STEP 11 | 設定を移行します。

STEP 12 | 設定が正常に移行されたことを確認します。

1. **Inventory**（インベントリ） > **Groups**（グループ）を選択して、IPセットとセキュリティグループが存在していることを確認します。セキュリティグループ名をクリックして、正しいIPアドレスがセキュリティグループの一部となっていることを確認することができます。
2. **Security**（セキュリティ） > **Network Introspection Settings**（ネットワーク診断設定） > **Service Segment**（サービスセグメント）を選択して、サービスセグメントが作成されていることを確認します。
3. **Security**（セキュリティ） > **Network Introspection Settings**（ネットワーク診断設定） > **Service Chains**（サービスチェーン）を選択して、サービスチェーンが作成されていることを確認します。Forward Path（フォワードパス）およびReverse Path（リバースパス）のProfiles（プロファイル）リンクをクリックして、サービスプロファイルを参照します。
4. **Security**（セキュリティ） > **Network Introspection**（**E-W**）（ネットワーク診断）を選択して、VM-Seriesファイアウォールのサービスプロファイルにトラフィックを送信する、トラフィックリダイレクトルールが作成されていることを確認します。

STEP 13 | 該当する場合は、エッジを変更、移行します。

©2023 Palo Alto Networks, Inc.

STEP 14 | ホストを設定、移行します。

STEP 15 | 既存のダイナミックアドレスグループにNSX-Tタグを追加します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. 既存のNSX-Vダイナミックアドレスグループの名前をクリックします。
3. **Add Match Criteria**（一致条件の追加）をクリックして、NSX-VおよびNSX-Tのタグを表示します。
4. NSX-Tタグを、ダイナミックアドレスグループに追加します。NSX-Vタグを削除しないことを選択した場合は、タグの間に**OR**演算子を使用してください。
5. 必要なタグをすべて追加したら、**OK**をクリックします。
6. 変更を **Commit (コミット)** します。

STEP 16 | NSX-T（East-West）での VM-Series ファイアウォールの起動.新しいサービスセグメントを作成する必要はありません。移行時に作成されたサービスセグメントを選択してください。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

AWS での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールは、Amazon Web Services（AWS）公開クラウドおよび AWS GovCloud にデプロイできます。その後、EC2 インスタンスにデプロイされているアプリケーションへのアクセスを保護するように設定し、AWS の Virtual Private Cloud（VPC）に配置することができます。

- AWS での VM-Series ファイアウォールについて
- AWS でサポートされるデプロイメント
- AWS での VM-Series ファイアウォールのデプロイ
- VM-SeriesとAWS Gateway Load Balancerの統合
- AWS における VM-Series ファイアウォールの高可用性設定
- ユース ケース：AWS クラウドで EC2 インスタンスを保護する
- ユース ケース：ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する
- ユース ケース：AWS の GlobalProtect ゲートウェイとしての VM-Series ファイアウォール
- AWS 上の VM モニタリング
- Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング
- AWS-VPC でモニターされる属性の一覧

AWS での VM-Series ファイアウォールについて

Amazon Web Service（AWS）はパブリック クラウド サービスの 1 つで、Amazon が管理する共有インフラストラクチャでアプリケーションを実行できます。これらのアプリケーションは、さまざまな AWS リージョンの拡張可能なコンピューティング キャパシティ（EC2 インスタンス）にデプロイすることができ、ユーザーはインターネットを介してそれらのアプリケーションにアクセスできます。

ネットワークの整合性を保ち、EC2 インスタンスを管理しやすくするため、Amazon では Virtual Private Cloud（VPC）を提供しています。VPC は AWS パブリック クラウドから分配され、プライベート ネットワーク領域から CIDR ブロックが割り当てられます（RFC 1918）。VPC 内では、必要に応じてパブリック/プライベート サブネットを振り分け、それらのサブネット内の EC2 インスタンスにアプリケーションをデプロイすることができます。その後、VPC 内のアプリケーションにアクセスできるようにするため、EC2 インスタンスに VM-Series ファイアウォールをデプロイできます。次に、その VM-Series ファイアウォールを、VPC 内の EC2 インスタンスとの間で送受信されるトラフィックを保護するように設定します。

VM-Series ファイアウォールは AWS 公開クラウドあるいはAWS GovCloudのどちらでも使用できます。公開 AWS および AWS GovCloud における VM-Series ファイアウォールは、BYOL（Bring Your Own License：ライセンス持ち込み）モデルおよび時間ベースの PAYG（Pay-As-You-Go：都度払い。AWS Marketplace で利用可能）ライセンス モデルをサポートしています。ライセンスの詳細については、 パブリック クラウド用 VM-Series ファイアウォールのライセンスを参照してください。

- AWS EC2 インスタンス タイプ
- AWS GovCloud における VM-Series ファイアウォール
- AWS China における VM-Series ファイアウォール
- AWS Outposts での VM-Series ファイアウォール
- AWS の用語
- Amazon ELB で使用する管理インターフェイスのマッピング
- AWS での VM-Series ファイアウォールのパフォーマンスチューニング

AWS EC2 インスタンス タイプ

サポートされているインスタンスタイプについては、「EC2インスタンス上のVM-Seriesモデル」を参照してください。

VM-Series ファイアウォールは、「VM-Series のシステム要件」に記載されている最小要件より多くのリソースを持つ AWS インスタンス サイズでもデプロイできます。VM-Series ファイアウォール モデルで最小要件より大きなインスタンス サイズを選択した場合、ファイアウォールは、表に示されている最大数の vCPU コアと最大量のメモリしか使用しませんが、AWS が提供する高速ネットワーク パフォーマンスの利点を活かすことができます。BYOL オプションによりライセンスされている VM-Series ファイアウォールのインスタンス タイプを変更したい場合、ライセンスの有効性を維持するために、インスタンス タイプを切り替える前に VM を非アクティブ化する必要があります。理由については、「VM-Series モデルのアップグレード」を参照してください。

©2023 Palo Alto Networks, Inc.

AWS での VM-Series ファイアウォールのサイジングに関するガイドについては、この記事を参照してください。

AWS GovCloud における VM-Series ファイアウォール

AWS GovCloud は、米国政府機関や顧客の規制あるいはコンプライアンス要件を満たす、AWS の独立した領域のことです。

AWS GovCloud（米国）領域にある政府向けデータや公開データ、およびすべてのカテゴリの CUI（Controlled Unclassified Information）データを含むワークロードの安全性を保つために、VM-Series ファイアウォールは標準的な AWS パブリック クラウドや AWS GovCloud と同様の堅牢なセキュリティ機能を提供します。AWS GovCloud の VM-Series のファイアウォールと標準の AWS パブリック クラウドは、同じ機能をサポートしています。

AWS で VM-Series ファイアウォールをデプロイする方法については、「AWS GovCloud おける AMI」を参照してください。

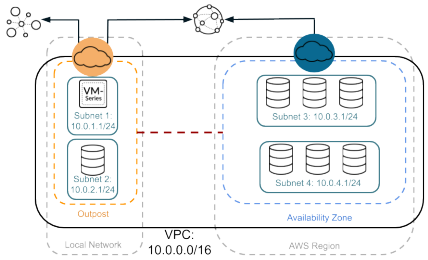
AWS China における VM-Series ファイアウォール

BYOL オプション付きの VM-Series ファイアウォールは、AWS China Marketplaceで利用でき、AWS China（北京）と AWS China（寧夏）リージョンで利用できます。このイメージにアクセスして AWS China の AWS リソースを使用するには、グローバル AWS アカウントとは別に AWS China アカウントを持っている必要があります。

AWS で VM-Series ファイアウォールを起動する前に VM-Series システム要件を確認してください。

AWS Outposts での VM-Series ファイアウォール

AWSクラウドにあるワークロードと同じレベルのセキュリティを、オンプレミスのワークロードに適用するために、オンプレミスロケーションのAWS Outpostsラックに、AWS上のVM-Seriesファイアウォールをインストールすることができます。AWS ージョンのAWS Marketplace BYOL AMIを使用して、VM-Seriesファイアウォールインスタンスを AWS Outpostsサブネット内にデプロイします。



サポート権利をPalo Alto Networksでアクティブ化するために、Palo Alto Networksカスタマーサポート Webサイトでサポートアカウントを作成して、VM-Seriesファイアウォールを登録する方法については、「VM-Series ファイアウォールを登録する（認証コードを使用）」を参照してください。

©2023 Palo Alto Networks, Inc.

AWS の用語

このドキュメントでは、AWS VPC のネットワークや設定に詳しい読者を想定しています。このセクションで使用する用語の背景を理解するために、このドキュメントで言及される AWS の用語（一部の定義は AWS 用語集から直接引用しています）について簡単に説明します。

用語	説明
EC2	Elastic Compute Cloud Amazon のデータセンターで Linux/UNIX インスタンスおよび Windows Server インスタンスを起動および管理するための Web サービス。
AMI	Amazon マシン イメージ AMI は、クラウド内の仮想サーバー インスタンスの起動に必要な情報を提供します。 VM-Series AMI は暗号化されたマシン イメージであり、EC2 インスタンスで VM-Series ファイアウォールをインスタンス化するために必要なオペレーティング システムが組み込まれています。
ELB	Elastic Load Balancing ELBとは、複数のElastic Compute Cloud（EC2）インスタンス全体のトラフィックをルーティングすることによって可用性やスケーラビリティを高めるAmazonウェブサービスのことです。ELBは安全性が疑われるEC2インスタンスを検出し、それが安全な状態に復元されるまでの間、トラフィックを安全なインスタンスへとルーティングします。ELB はネクストホップの負荷分散された EC2 インスタンスのプライマリ インターフェイスにしかトラフィックを送信できません。そのため、AWS で VM-Series ファイアウォールとともに ELB を使用するためには、ファイアウォールがデータプレーン トラフィック用のプライマリ インターフェイスを使用できなくてはなりません。
ENI	Elastic Network Interface EC2 インスタンスにアタッチできる追加のネットワーク インターフェイス。ENI には、プライマリ プライベート IP アドレス、1 つ以上のセカンダリ プライベート IP アドレス、パブリック IP アドレス、Elastic IP アドレス（任意）、MAC アドレス、指定セキュリティ グループでのメンバーシップ、説明、および送信元/宛先チェック フラグなどがあります。
EC2 インスタンスの IP アドレス タイプ	EC2 インスタンスでは、さまざまな種類の IP アドレスを使用できます。 • パブリックIPアドレス:インターネットを介してルーティング可能な IP アドレス。

©2023 Palo Alto Networks, Inc.

用語	説明
	• プライベートIPアドレス:RFC 1918 で定義されているプライベートIPアドレス範囲内のIPアドレス。IP アドレスを手動で割り当てるか、または EC2 インスタンスを起動するサブネットの CIDR ブロックの範囲内で IP アドレスを自動で割り当てるかを選択できます。 Amazon では、すべてのサブネットで最初の 4 つの IP アドレスと最後の 1 つの IP アドレスを IP ネットワーキング用に予約しており、IP アドレスを手動で割り当てる場合にはそれらのアドレスは使用できません。 • Elastic IPアドレス（EIP）:Amazon EC2またはAmazon VPCから割り当てられ、インスタンスで利用可能なスタティックIPアドレス。Elastic IP アドレスは、特定のインスタンスではなく、ユーザーのアカウントに関連付けられます。この IP アドレスは、必要に応じて簡単に割り当て、アタッチ、デタッチ、解放することができるという意味で柔軟性があります。 パブリック サブネットのインスタンスでは、プライベート IP アドレス、パブリック IP アドレス、および Elastic IP アドレス（EIP）を使用でき、プライベート サブネットのインスタンスでは、プライベート IP アドレスおよび任意で EIP を使用できます。
インスタンス タイプ	メモリ、CPU、ストレージ容量、およびインスタンスの 1 時間あたりのコストが規定されている、Amazon が定義した仕様。インスタンスタイプには、標準アプリケーション用に設計されているものと、CPU やメモリの使用量が多いアプリケーション用に設計されているものがあります。
VPC	バーチャル プライベート クラウド 共通のセキュリティと相互接続を共有するインフラストラクチャ、プラットフォーム、およびアプリケーションの各サービスが取り込まれた柔軟性のあるネットワーク。
IGW	Amazon が提供するインターネット ゲートウェイ。 ネットワークをインターネットに接続します。VPC 外部の IP アドレスへのトラフィックをインターネット ゲートウェイにルーティングできます。
IAMロール	IDとアクセス管理 AWS で VM-Series ファイアウォールの高可用性を有効化する際に必要となります。IAMロールはAPIアクションやそのロールを割り当てた後利用可能になるアプリケーションのリソースの定義をします。フェイルオーバーが発生すると、IAMロールは、データプレーンイン

©2023 Palo Alto Networks, Inc.

用語	説明
	ターフェイスのアクティブピアからパッシブピアへの切り替えを求めるAPI要求を確実に行えるよう割り当てを行います。 IAM ロールは VM モニタリングにも必要となります。「AWS-VPC でモニターされる属性の一覧」を参照してください。
サブネット	EC2 インスタンスをアタッチできる VPC の IP アドレス範囲のセグメント。EC2 インスタンスは、セキュリティおよび操作上の必要に応じてサブネットにグループ化されます。 サブネットには、以下の 2 つのタイプがあります。 • プライベートサブネット:このサブネットに含まれる EC2 インスタンスには、インターネットからアクセスできません。 • パブリックサブネット:インターネットゲートウェイがパブリックサブネットにアタッチされ、このサブネットに含まれるEC2インスタンスにインターネットからアクセスできます。
セキュリティグループ	セキュリティグループは ENI にアタッチされます。このグループにより、インターフェイスでインバウンド/アウトバウンド接続の確立が許可される、プロトコル、ポート、および IP アドレス範囲のリストが指定されます。 *AWS VPC* では、セキュリティグループとネットワーク *ACL* によってインバウンド/アウトバウンドのトラフィックが制御されます。このとき、セキュリティグループによって *EC2* インスタンスへのアクセスが規制され、ネットワーク *ACL* によってサブネットへのアクセスが規制されます。*VM-Series* ファイアウォールをデプロイする場合は、セキュリティグループとネットワーク *ACL* でさらに許可グループを設定し、ファイアウォールで *VPC* 内のアプリケーションを安全に有効にできるようにします。
ルート テーブル	ルート テーブルに関連付けられた任意のサブネットから送出されるトラフィックを制御するルーティング ルール個々のサブネットは、1 つのルート テーブルにのみ関連付けることができます。
キーのペア	ID を電子的に証明するために使用するセキュリティ認証情報キー ペアはパブリック キーとプライベート キーで構成されています。VM-Series ファイアウォールの起動時には、キー ペアを生成するか、VM-Series 用の既存のキー ペアを選択する必要があります。プライベート キーは、メンテナンス モードでファイアウォールにアクセスするために必要です。

©2023 Palo Alto Networks, Inc.

用語	説明
CloudWatch	Amazon CloudWatch は、AWS 上で VM-Series ファイアウォールのメトリックを収集して追跡するための監視サービスです。有効な場合、ファイアウォールは AWS API を使用してネイティブ PAN-OS メトリックを CloudWatch に公開します。

Amazon ELB で使用する管理インターフェイスのマッピング

デフォルト設定では、Elastic Network Interface（ENI）eth0 はファイアウォール上の MGT インターフェイスにマッピングし、ENI eth1 はファイアウォール上の ethernet 1/1 にマッピングします。ELB はネクストホップの負荷分散された EC2 インスタンスのプライマリ インターフェイスにしかトラフィックを送信できないため、VM-Series ファイアウォールがデータプレーン トラフィック用のプライマリ インターフェイスを使用できなくてはなりません。

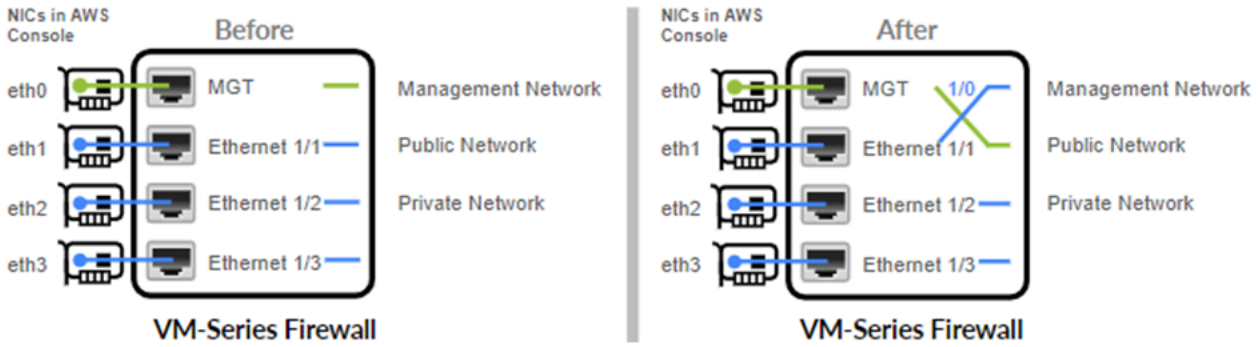
VM-Series ファイアウォールが Amazon ELB サービスの背後にある次のケースでは、ファイアウォールはプライマリ インターフェイス上のデータプレーン トラフィックを受信できます（トポロジー図については「Amazon ELB を使用した VM-Series ファイアウォールのオート スケーリング サービス」を参照してください）。

- VM-Series ファイアウォールは、企業ネットワークに戻る VPN リンクやダイレクト コネクト リンクを使用せずに、直接インターネットに向かうアウトバウンド トラフィックを保護できます。
- VM-Series ファイアウォールは、各ファイアウォールにつきバックエンド サーバー（Web サーバーなど）が 1 つだけある場合にのみ、インターネットに接続するアプリケーションを守ります。VM-Series ファイアウォールと Web サーバーは ELB のバックで同時にリニアにスケーリングできます。

> 現在のところ、ファイアウォールおよびアプリケーション層の *EC2* インスタンスをスケール アウトするために *ELB* サンドイッチタイプのデプロイが必要になるユース ケースでは、管理インターフェイスをスワップしても *ELB* ソリューションをシームレスにデプロイすることはできません。管理インターフェイスをスワップする機能は、*ELB* との統合を部分的にしか解決できません。

ファイアウォールが eth1 ではなく eth0 でデータプレーン トラフィックを送受信できるようにするには、ファイアウォール内で ENI のマッピングをスワップし、以下のように、ENI eth0 が ethernet 1/1 に、ENI eth1 がファイアウォール上の MGT インターフェイスにマッピングされるようにする必要があります。

©2023 Palo Alto Networks, Inc.



可能な場合は、ファイアウォールを構成する前、あるいはポリシー ルールを定義する前に管理インターフェイスをスワップします。

インターフェイスのマッピング方法をスワップすることで、ELB が AWS 内の同じあるいは異なる可用性ゾーンに位置した VM-Series ファイアウォールの安全なインスタンスにトラフィックをルーティングし、キャパシティや耐障害性を高めることができます。

インターフェイス スワップは、VM-Series ファイアウォールが Amazon ELB サービスの背後に位置する場合にのみ必要です。VM-Series ファイアウォールを従来の高可用性セットアップでデプロイする必要がある場合は、このセクションで説明するインターフェイス スワップを設定する必要はありません。「AWS における VM-Series ファイアウォールの高可用性設定」に進んでください。

以下のような方法でインターフェイスをスワップできます。

- **At launch**（起動時） — ファイアウォールを起動するときに、AWS 管理コンソールの **User data**（ユーザー データ）フィールドまたは CLI に **`mgmt-interface-swap=enable`** コマンドを入力するか、ブートストラップ設定に新しい **`mgmt-interface-swap`** 操作コマンドを含めます（AWS 管理コンソールでの操作については、「AWS での VM-Series ファイアウォールの起動」を参照してください）。

©2023 Palo Alto Networks, Inc.

- **After launch**（起動後） – ファイアウォールを起動した後、VM-Series ファイアウォールの CLI を使用して管理インターフェイスをスワップします（**set system setting mgmt-interface-swap enable yes** 操作コマンド）。

  - ファイアウォール上で予期しない挙動が発生するのを防止するために、インターフェイスのスワップ設定を継続的に指定する方法（ブートストラップ設定内、ファイアウォール上の *CLI* から、あるいは *AWS* コンソールの *Amazon EC2 User data*（ユーザー データ）フィールドの使用）を *1* つ選択します。
  - *eth1* インターフェイスの *IP* アドレスを確認するために必要な、*AWS* コンソール（管理コンソールあるいは *CLI*）へのアクセス権限があることを確認してください。さらに、*AWS* セキュリティ グループ ルールによって新しい管理インターフェイスへの接続（*HTTPS* および *SSH*）が許可されていることも確認します。
  - インターフェイスのスワップ前にファイアウォールまたは定義されているポリシー ルールの構成が終了している場合は、*eth0* および *eth1* のいずれかの *IP* アドレスが変更されるとポリシー ルールが影響を受けるかどうか確認してください。

AWS での VM-Series ファイアウォールのパフォーマンスチューニング

次の構成はパフォーマンスに影響します。

- PAN-OS バージョン 9.0.3 以前は、デフォルトで SR-IOV モードを Elastic Network Adapter がサポートする AWS C5 および M5 インスタンスタイプをサポートします。詳細については、Elastic Network Adapter – Amazon EC2用の高性能ネットワークインターフェースを参照してください。
- PAN-OS バージョン 9.0.4 以降では、デフォルトで C5 および M5 インスタンスタイプの DPDK サポートが提供されます。ファイアウォールが DPDK モードの場合、ファイアウォールは DPDK ドライバーを使用します。サポートされているドライバーのリストについては、VM-Series ファイアウォール上の PacketMMAP および PDK ドライバーと公式の DPDK リリースノートを参照してください。
- IETF RFC 8926（Geneve） のカプセル化とスループットの利点と改善点を活用するには、PAN-OS 10.0.2 以降にアップグレードし、VM-Series Integration with AWS Gateway LoadBalancer (AWS ゲートウェイロードバランサーとの VM-Series の統合) を参照してください。

VM-Series CLIを使用して、DPDK 設定を表示するか、またはパックド I/O を有効にします。

ファイアウォールの DPDK 構成の表示

STEP 1 | VM-Series ファイアウォール CLI にログインします。

©2023 Palo Alto Networks, Inc.

STEP 2 | DPDK 構成を表示します。DPDK が有効になっている場合、出力は次のようになります。

```
> show system setting dpdk-pkt-io on
```

```
Device current Packet IO mode:     DPDK
Device DPDK Packet IO capable:     yes
Device default Packet IO mode:     DPDK
```

DPDK パック I/O の有効化

STEP 1 | VM-Series ファイアウォール CLI にログインします。

STEP 2 | DPDK を有効にします。

```
> set system setting dpdk-pkt-io on
```

STEP 3 | デバイスを再起動します。

ファイアウォールで、デバイス > セットアップ > 操作を選択し、[デバイスの再起動]を選択します。

©2023 Palo Alto Networks, Inc.

AWS でサポートされるデプロイメント

VM-Series ファイアウォールにより、AWS Virtual Private Cloud（VPC）内の EC2 インスタンスとの間で送受信されるインバウンド / アウトバウンド トラフィックが守られます。AWS VPC でサポートされるのは IP ネットワーク（レイヤー 3 ネットワーキング機能）に限られるため、VM-Series ファイアウォールはレイヤー 3 インターフェイスでのみデプロイすることができます。

- VM-Series ファイアウォールをデプロイして、AWS Virtual Private Cloud でホストされる EC2 インスタンスを保護します。

  AWS クラウドでアプリケーションをホストする場合は、VM-Series ファイアウォールを利用して、インターネット経由でそれらのアプリケーションにアクセスするユーザーのアプリケーションを保護し、安全に有効にします。たとえば、以下の図は、インターネット ゲートウェイがアタッチされた Edge サブネットにデプロイされている VM-Series ファイアウォールを示しています。アプリケーションはプライベート サブネットにデプロイされ、インターネットに直接アクセスできません。

  ユーザーがプライベート サブネット内のアプリケーションへのアクセスを要求すると、ファイアウォールはその要求を受け取り、セキュリティ ポリシーを確認し、宛先 NAT を実行してから、その要求を該当するアプリケーションに転送します。リターン パスにおいてファイアウォールは、トラフィックを受信してセキュリティ ポリシーを適用し、送信元 NAT を使用してコンテンツをユーザーに配信します。「ユース ケース：AWS クラウドで EC2 インスタンスを保護する」を参照してください。

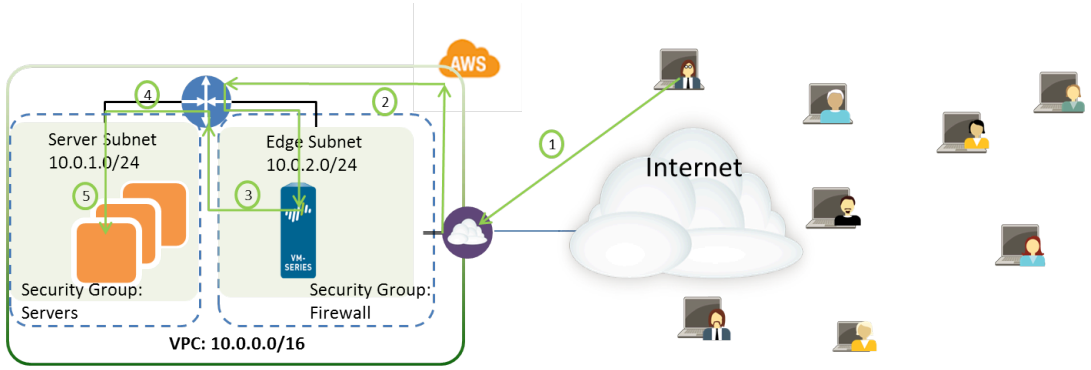


図 **1 : EC2** インスタンス用の **VM-Series**

- 企業ネットワークと AWS Virtual Private Cloud 内の EC2 インスタンスとの間の VPN アクセスのために、VM-Series ファイアウォールをデプロイします。

  企業ネットワークを AWS クラウドにデプロイされたアプリケーションと接続するため、ファイアウォールを IPSec VPN トンネルの終端ポイントとして設定することができます。この VPN トンネルにより、ネットワーク上のユーザーはクラウド内のアプリケーションに保護された状態でアクセスできます。

  中央管理、ネットワーク全域でのポリシーの一貫した適用、および一元的なロギングとレポート作成のために、企業ネットワークに Panorama をデプロイすることもできます。複数 VPC への VPN アクセスをセットアップする必要がある場合は、Panorama を使用することで

 ©2023 Palo Alto Networks, Inc.

地域別にファイアウォールをグループ化し、それらのグループを容易に管理することができます。

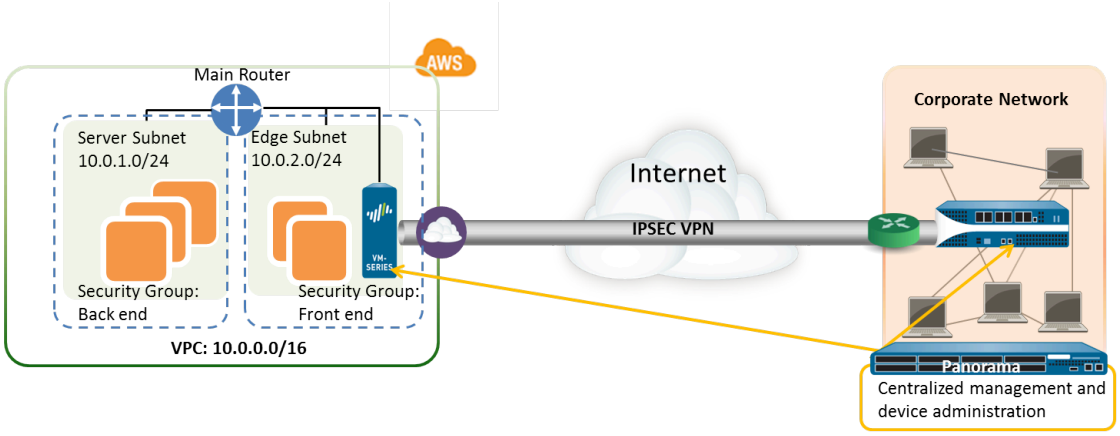


図 **2 : VPN** 接続用の **VM-Series**

- VM-Series ファイアウォールを GlobalProtect ゲートウェイとしてデプロイして、ラップトップを使用するリモート ユーザーのアクセスを保護します。ラップトップ上の GlobalProtect エージェントがゲートウェイに接続すると、そのゲートウェイでは、要求に基づいて企業ネットワークへの VPN 接続をするか、その要求をインターネットにルーティングします。モバイル デバイス（GlobalProtect アプリを使用）でのユーザーのセキュリティ コンプライアンスを適用するため、GlobalProtect ゲートウェイを GlobalProtect Mobile Security Manager と連携させて使用します。GlobalProtect Mobile Security Manager により、企業のアプリケーションとネットワークで使用されるデバイス設定とアカウント情報に基づいて、確実にモバイル デバイスが管理および設定されるようになります。

  上記の各使用例では、アクティブ / パッシブの高可用性（*HA*）ペアで *VM-Series* ファイアウォールをデプロイ可能です。*Ha*環境での *VM-Series* ファイアウォールのセットアップについては、ユース ケース:ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する」を参照してください。

- VM-Series ファイアウォールを Amazon Elastic Load Balancing（ELB）サービスとともにデプロイします。この場合、VM-Series ファイアウォールが Amazon ELB の背後にある次のケースでは、ファイアウォールはプライマリ インターフェイス上のデータプレーン トラフィックを受信できます。

  - VM-Series ファイアウォールは、企業ネットワークに戻る VPN リンクやダイレクト コネクト リンクを使用せずに、直接インターネットに向かうアウトバウンド トラフィックを保護できます。
  - VM-Series ファイアウォールは、各ファイアウォールにつきバックエンド サーバー（Web サーバーなど）が 1 つだけある場合にのみ、インターネットに接続するアプリケーションを守ります。VM-Series ファイアウォールと Web サーバーは ELB のバックで同時にリニアにスケーリングできます。

  Amazon ELB を使用した VM-Series ファイアウォールのオート スケーリング サービスを行うには、GitHub リポジトリに用意されている CloudFormation Template を使用して、インターネット接続されたクラシック ELB と内部クラシック ロード バランサーまたは内部アプ

©2023 Palo Alto Networks, Inc.

リケーション ロード バランサー（内部 ELB）を使用する ELB サンドイッチ トポロジに VM-Series をデプロイします。

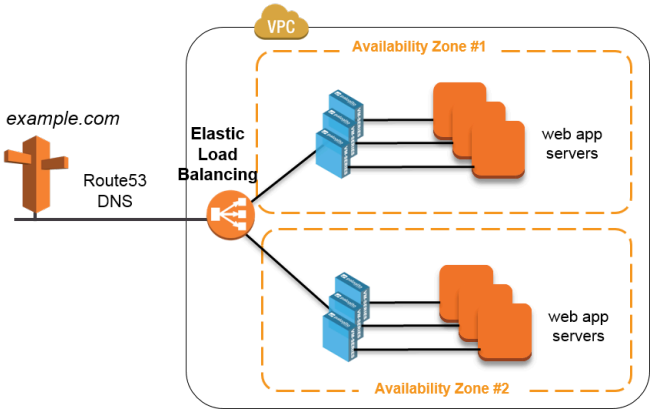


図 **3 : ELB** を使用する **VM-Series**

ファイアウォールが *ELB* の前にある場合は、*eth0* 上のデータプレーン トラフィックを送受信するようファイアウォールを構成することはできません。*VM-Series* ファイアウォールは *Amazon ELB* の後ろに配置する必要があります。

VM-Series ファイアウォールの CLI を使用して管理インターフェイスをスワップするか、ブートストラップで有効にできます。詳細は、「Amazon ELB で使用する管理インターフェイスのマッピング」を参照してください。

ロード バランサー サンドイッチ トポロジをデプロイするには、「Amazon ELB を使用した VM-Series ファイアウォールのオート スケーリング サービス」を参照してください。

Palo Alto Networks の公式サポート ポリシーでカバー対応する上記の *ARM* テンプレートに加えて、*Palo Alto Networks* は Palo Alto Networks の GitHub リポジトリにコミュニティ対応テンプレートを提供しています。これにより、クラウドの自動化および *Azure* のスケールをスムーズに行うことができます。*VPC* 間のトラフィックと、*VPC* とオンプレミス/ハイブリッド クラウド リソース間のトラフィックを保護し、インターネットへのアウトバウンド トラフィックを保護することができるハブおよびサブスクライブ *VPC* デプロイメントについては、AWS Transit VPC を参照してください。

©2023 Palo Alto Networks, Inc.

AWS での VM-Series ファイアウォールのデプロイ

- AMI の取得
- AWS VPC での VM-Series 用プランニングワークシート
- AWS での VM-Series ファイアウォールの起動
- AWS Outposts での VM-Series ファイアウォールの起動
- カスタム Amazon Machine Image（AMI）の作成
- AWS 上の VM-Series ファイアウォールの EBS ボリュームの暗号化
- VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ
- VM-Series ファイアウォールでの CloudWatch モニタリングの有効化

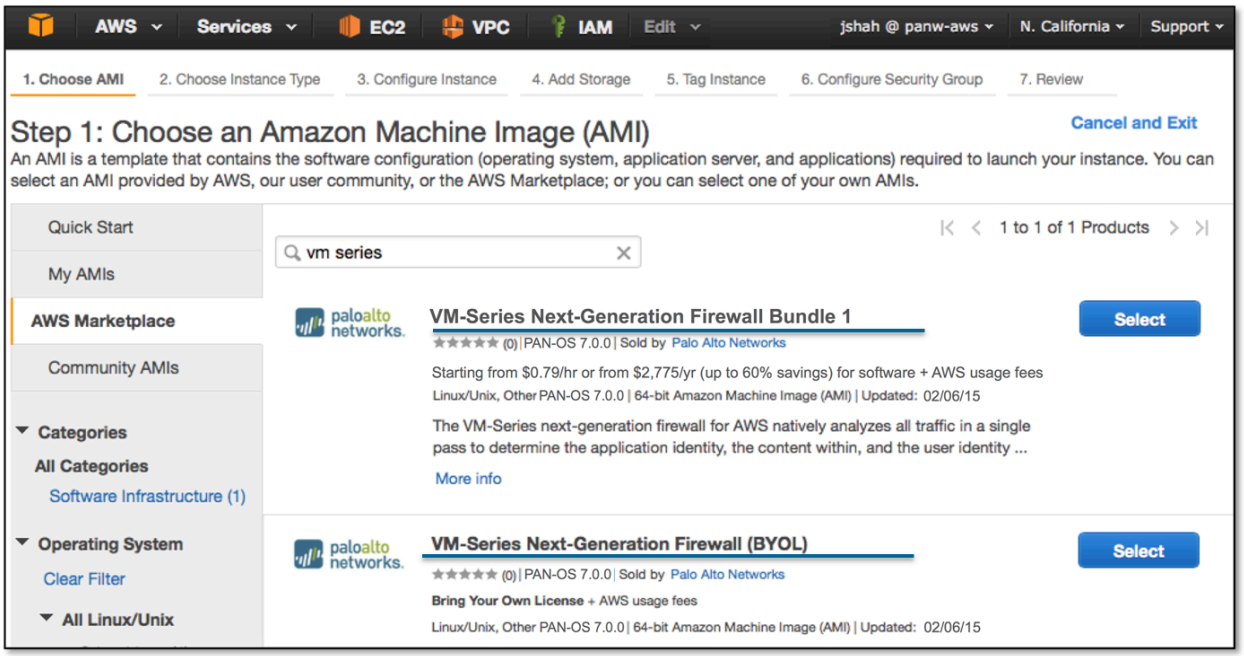
AMI の取得

対象のマーケットプレイスから、AWS 公開クラウドおよび AWS GovCloud の Amazon マシンイメージを取得します。

- AWS 公開クラウドにおける AMI
- AWS GovCloud おける AMI
- VM-Series ファイアウォールの Amazon Machine Image（AMI）ID の取得

AWS 公開クラウドにおける AMI

VM-Series ファイアウォールの AMI は、Bring Your Own License（BYOL）とusage-based（従量制）の 2 種類のライセンスで AWS Marketplace から購入できます。



©2023 Palo Alto Networks, Inc.

BYOL オプションでライセンスを購入する場合は、Palo Alto Networksの セールスエンジニアまたは販売代理店にお問い合わせください。

AWS GovCloud おける AMI

VM-Series ファイアウォールのBring Your Own License（BYOL）モデルおよび従量制のモデルは、AWS GovCloud Marketplace で入手できます。

Marketplace 上で GovCloud アカウントを使用して Palo Alto Networks を検索すれば、VM-Series ファイアウォールの AMI が見つかります。ファイアウォールを起動する前に、サポートされている EC2 インスタンス タイプを確認するようにしてください。詳細については、「AWS での VM-Series ファイアウォールの起動」を参照してください。

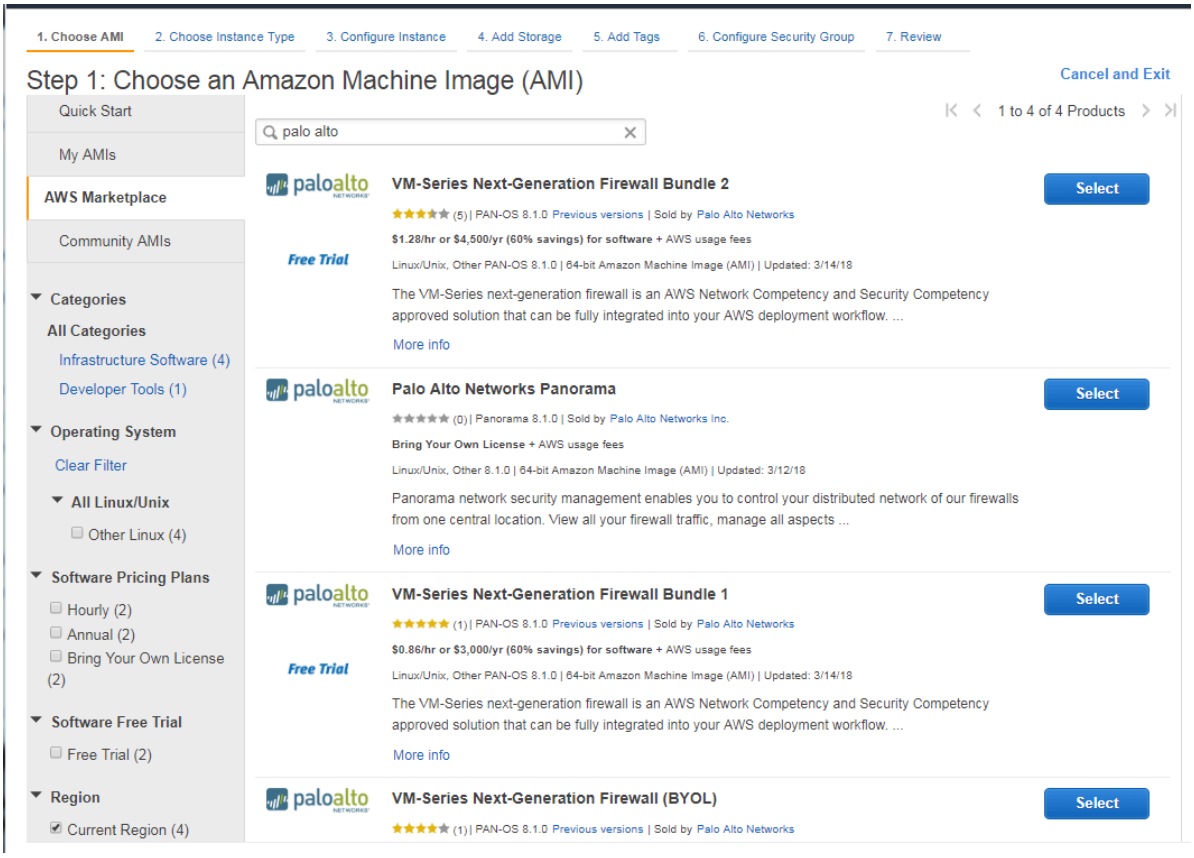


表 **1 : AWS** における **VM-Series** のシステム要件と制限事項の確認

要件	詳細
EC2 インスタンス タイプ	選択した EC2 インスタンス タイプは、VM-Series ファイアウォールの VM-Series のシステム要件を満足しなければなりません。これらの要件を満たさない EC2 インスタンスタイプに VM-Series ファイアウォールをデプロイすると、ファイアウォールはメンテナンス モードで起動します。

©2023 Palo Alto Networks, Inc.

要件	詳細
	AWS で VM モニタリングおよび高可用性をサポートするためには、ファイアウォール管理インターフェイスおよび *AWS API* のエンドポイント（*ec2.us-west-2.amazonaws.com* など）の間にプロキシサーバーがない状態で *VM-Series* ファイアウォールが *AWS API* に直接アクセスできなければなりません。
Amazon Elastic Block Storage（EBS）	VM-Series ファイアウォールでは、ストレージとして Amazon Elastic Block Storage（EBS）ボリュームを使用する必要があります。EBS の最適化により、Amazon EBS の I/O 用に、最適化された設定スタックと追加の専用キャパシティが提供されます。
ネットワーク	AWS でサポートされるのはレイヤー 3 ネットワーキング機能に限られるため、VM-Series ファイアウォールはレイヤー 3 インターフェイスでのみデプロイすることができます。レイヤー 2 インターフェイス、バーチャル ワイヤ、VLAN、およびサブインターフェイスは、AWS VPC にデプロイされている VM-Series ファイアウォールではサポートされていません。
Interface（インターフェイス）	合計で 8 つのインターフェイスをサポートし、管理インターフェイスとして 1 つ、またデータ トラフィック用に最大 7 つの Elastic ネットワーク インターフェイス（ENI）を使用できます。VM-Series ファイアウォールは ENI のホットアタッチをサポートしていないため、ENI の追加または削除を検出するにはファイアウォールを再起動する必要があります。 選択する *EC2* インスタンスタイプにより、有効にできる *ENI* 合計数が決まります。たとえば、*c3.8xlarge* は *8* つの *ENI* をサポートします。
サポート資格とサポート ライセンス	Bring Your Own License モデルの場合、AWS VPC での VM-Series ファイアウォールのインストールに必要な Amazon マシンイメージ（AMI）ファイルを取得するには、サポートアカウントと有効な VM-Series ライセンスが必要です。VM-Series ファイアウォールで必要とされるライセンス（脅威防御、URL フィルタリング、WildFire のキャパシティ ライセンス、サポート ライセンス、およびサブスクリプションなど）は、Palo Alto Networks から購入する必要があります。ライセンスを購入するには、販売代理店にお問い合わせください。「パブリック クラウドの VM-Series ファイアウォール ライセンス」を参照してください。 従量制のライセンスについては時間制や年間契約のモデルがあり、購入するとAWSに直接請求されます。ただし、Palo Alto Networks のサポート資格を登録する必要があります。詳細については、パブリック

©2023 Palo Alto Networks, Inc.

要件	詳細
	クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）を参照してください。

VM-Series ファイアウォールの Amazon Machine Image（AMI）ID の取得

以下の手順に従って、PAN-OS バージョン、ライセンス タイプ、および VM-Series ファイアウォールを起動する AWS リージョンに一致する VM-Series ファイアウォールの AMI ID を見つけます。

STEP 1 | AMI ID の取得に使用するクライアントに AWS CLI をインストールし、AWS 認証情報を使用してログインします。

CLI のインストール手順については、AWS のドキュメントを参照してください。

STEP 2 | 以下の CLI コマンドを使用して AMI-ID を検索します。

```
aws ec2 describe-images --filters "Name=product-code,Values=
 <license-type-value>" Name=name,Values=PA-VM-AWS*
 <PAN-OS-version>*  --region
 <region> --output table --query "Images[*].
{Name:Name,AMI:ImageId,State:State}
```

角かっこ <> で囲まれている値を以下に示す関連情報に置き換える必要があります。

- 各ライセンス タイプには VM-Series プロダクト コードを使用します。値を以下に示します。
  - バンドル 1 –

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - バンドル 2 –

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL–

    ```
    6njl1pau431dv1qxipg63mvah
    ```

- PAN-OSバージョン10.0を使用します。特定の PAN-OS バージョンに複数の機能リリースがある場合は、すべての AMI-ID がリストされます。たとえば 9.0.x の場合、PAN-OS

©2023 Palo Alto Networks, Inc.

バージョン 9.0、9.0.3.xfr、9.0.5.xfr、および 9.0.6 の AMI ID がリストされるので、必要な PAN-OS バージョンの AMI ID を使用できます。

- AWSリージョンの詳細を、https://docs.aws.amazon.com/general/latest/gr/rande.html から取得します。

例:US CaliforniaリージョンのPAN-OS 10.0.0のVM-Seriesバンドル1のAMI-IDを検索するCLIコマンドは次通りです。

```
aws ec2 describe-images --filters "Name=product-code,Values=e9yfvyj3uag5uo5j2hjikv74n" "Name=name,Values=PA-VM-AWS*10.0*"  --region us-west-1 --output json
```

出力は次のようになります。

```
{
    "ProductCodes": [
        {
            "ProductCodeId": "e9yfvyj3uag5uo5j2hjikv74n",
            "ProductCodeType": "marketplace"
        }
    ],
     "VirtualizationType": "hvm",
    "Hypervisor": "xen",
    "ImageOwnerAlias": "aws-marketplace",
    "EnaSupport": true,
    "SriovNetSupport": "simple",
    "ImageId": "ami-06f7a63d7481d0ded",
    "State": "available",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "SnapshotId": "snap-0009036179b39824b",
```


©2023 Palo Alto Networks, Inc.

```
                        "DeleteOnTermination": false,
                        "VolumeType": "gp2",
                        "VolumeSize": 60,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "aws-marketplace/PA-VM-AWS-10.0.0-
f1260463-68e1-4bfb-bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1",
            "RootDeviceType": "ebs",
            "OwnerId": "679593333241",
            "RootDeviceName": "/dev/xvda",
            "CreationDate": "2020-07-20T12:45:22.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "PA-VM-AWS-10.0.0-f1260463-68e1-4bfb-
bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1"
        }
```

表形式で出力することもできます。たとえば、PAN-OS 10.0.2の BYOL イメージの AMI を表示するには、次のようにします。

```
aws ec2 describe-images --filters "Name=product-
code,Values=6njl1pau431dv1qxipg63mvah" "Name=name,Values=PA-VM-
AWS*10.0.2*" --region us-west-1 --output table --query "Images[*].
{Name:Name,AMI:ImageId,State:State}"
```

```
-----------------------------------------------------------------------------
                          DescribeImages
                     |+-----------------------
+----------------------------------------------------------------------------
+-------------+|     AMI     |                   Name
                  |  State  |+-----------------------
+----------------------------------------------------------------------------
+-------------+| ami-037b90bd9b630f594| PA-VM-
AWS-10.0.2-7064e142-2859-40a4-ab62-8b0996b842e9-
ami-07a0e94019f2a2001.4 | available |+-----------------------
```

```
+-------------------------------------------------------------------------------
+-------------+
```

AWS VPC での VM-Series 用プランニングワークシート

デプロイメントを容易にするため、VPC 内のサブネットと、各サブネット内にデプロイする EC2 インスタンスを計画します。開始する前に、以下の表を使用してデプロイに必要なネットワーク情報を照合し、VM-Series ファイアウォールを VPC のトラフィック フローに挿入します。

設定項目	値
VPC CIDR	
セキュリティグループ	
サブネット（パブリック）CIDR	
サブネット（プライベート）CIDR	
サブネット（パブリック）ルート テーブル	
サブネット（プライベート）ルート テーブル	
セキュリティグループ • ファイアウォールへの管理アクセスのルール（eth0/0） • ファイアウォールのデータプレーン インターフェイスへのアクセスのルール • アプリケーション サーバーに割り当てられたインターフェイスへのアクセスのルール	
ELB の後ろにある VM-Series ファイアウォール	
EC2 インスタンス 1（VM-Series ファイアウォール）	サブネット： インスタンス タイプ： 管理インターフェイス IP：

©2023 Palo Alto Networks, Inc.

設定項目	値
EIP は、パブリック サブネットにアタッチされるデータプレーン インターフェイスの場合にのみ必要です。	管理インターフェイス EIP： データプレーン インターフェイス eth1/1 • プライベート IP： • EIP（必要な場合）： • セキュリティ グループ： データプレーン インターフェイス eth1/2 • プライベート IP： • EIP（必要な場合）： • セキュリティ グループ：
EC2 インスタンス 2（保護されるアプリケーション） デプロイされる追加のアプリケーションで、これらの値セットを繰り返し設定します。	サブネット： インスタンス タイプ： 管理インターフェイス IP： デフォルト ゲートウェイ： データプレーン インターフェイス 1 • プライベート IP：
HA の導入要件	VM-Series ファイアウォールを高可用性設定（アクティブ/パッシブ）でデプロイする場合、以下を確認する必要があります。 • IAM ロールを作成し、インスタンスのデプロイ時にそのロールを VM-Series ファイアウォールに割り当てていること。「HA 用の IAM ロール」を参照してください。 • HA ピアを同じ AWS 可用性ゾーンの中にデプロイしていること。 • HA ペアの内のアクティブなファイアウォールは最低で 3 つ（データプレーンインターフェイス 2 つ、管理インターフェイス 1 つ）のENIを保有している必要があります。 HA ペアの内のパッシブなファイアウォールは、管理用 ENI を1 つ、データプレーンインターフェイスとして機能するENIを1 つ保有している必要があります。データプレーンインターフェイスは HA2 インターフェイスとして設定します。

©2023 Palo Alto Networks, Inc.

設定項目	値
	HA ペアの内のパッシブなファイアウォールにはデータプレーンを追加しないでください。フェイルオーバーが発生すると、それまでアクティブであったファイアウォールのデータプレーンインターフェイスが取り外され、アクティブになった（それまでパッシブであった）ファイアウォールに取り付けられます。

AWS での VM-Series ファイアウォールの起動

注文完了電子メールに記載されているキャパシティ認証コードをまだ登録していない場合は、「VM-Series ファイアウォールの登録」を参照してください。登録後以下の手順に従って、Marketplace で公開されている AMI を使用した VM-Series ファイアウォールのデプロイ、または AWS VPC でカスタム Amazon Machine Image（AMI）の作成を次のように行います。

STEP 1 | AWS コンソールにアクセスします。

AWS コンソールにログインし、EC2 Dashboard を選択します。

STEP 2 | ネットワークの必要に応じて VPC をセットアップします。

VM-Series ファイアウォールを既存の VPC で起動する場合でも、新しい VPC を作成する場合でも、VM-Series ファイアウォールは EC2 インスタンスからのトラフィックを受信して、VPC とインターネットとの間でインバウンドおよびアウトバウンド通信を実行できなければなりません。

VPC を作成してアクセスを設定する方法については、AWS VPC のドキュメントを参照してください。

完全なワークフローの例は、「ユース ケース:AWS クラウドで EC2 インスタンスを保護する」を参照してください。

1. 新規 VPC を作成するか、既存の VPC を使用します。AWS のドキュメント「始めましょう」を参照してください。
2. ネットワーク コンポーネントとセキュリティ コンポーネントが適切に定義されていることを確認します。
   - インターネットとの通信を有効化します。デフォルトの VPC にはインターネットゲートウェイが用意されていますので、デフォルトのサブネットで VM-Series ファイアウォールをインストールすれば、インターネットにはアクセスできる状態になっています。
   - サブネットを作成します。サブネットは、EC2 インスタンスを起動できる VPC に割り当てられた IP アドレス範囲のセグメントです。VM-Series ファイアウォールがインターネットにアクセスできるように設定するには、パブリック サブネットに属している必要があります。

©2023 Palo Alto Networks, Inc.

- EC2 インスタンス/サブネットからのインバウンド/アウトバウンド トラフィックを管理するには、必要に応じてセキュリティグループを作成します。
- プライベート サブネットのルート テーブルにルートを追加し、該当する VPC 内のセブネットおよびセキュリティグループ全体に確実にトラフィックをルーティングできるようにします。

3. VM-Series ファイアウォールのペアを HA にデプロイする場合、AWS 上で アクティブ/パッシブ HA を設定するには、HA 用の IAM ロールを定義する必要があります。
4. （任意）ブートストラップによって VM-Series ファイアウォールを設定する場合は、「AWS 上での VM-Series ファイアウォールのブートストラップ」を参照してください。ブートストラップの詳細は、「VM-Series ファイアウォールのブートストラップ」および「ブートストラップ方法の選択」を参照してください。

STEP 3 | VM-Series ファイアウォールを起動します。

*VM-Series*ファイアウォールを起動する際にネットワークインターフェイス（*ENI*）を追加することは可能ですが、この場合、ファイアウォールを再起動した際に、*AWS*は管理インターフェイスに自動的に割り当てられたパブリック*IP*アドレスを放棄します。管理インターフェイスへの接続を確保するためには、ファイアウォールへこれ以上のインターフェイスを追加する前に、管理インターフェイスへ *Elastic IP* アドレスを割り当てる必要があります。

EIPアドレスを保存したい場合、eth 1/1インターフェイスにEIPアドレスを1つ割り当て、このインターフェイスを管理トラフィックとデータトラフィックの両方に使用することも可能です。インターフェイスで許可されるサービスを制限したい場合、あるいはeth 1/1にログイン可能なIPアドレスを制限したい場合はインターフェイスに管理プロファイルを適用してください。

1. EC2 Dashboard で、**Launch Instance**（インスタンスを起動）をクリックします。
2. VM-Series AMI を選択します。AMI の取得方法については、「AMI の取得」を参照してください。
3. EC2 インスタンスで VM-Series ファイアウォールを起動します。

   1. ファイアウォールに必要なリソースを割り当てるための **EC2 instance type**（**EC2** インスタンス タイプ）を選択してから **Next**（次へ）をクリックします。リソースの要件については、「VM-Series のシステム要件」を参照してください。
   2. VPC を選択します。
   3. VM-Series 管理インターフェイスにアタッチするパブリック サブネットを選択します。
   4. **Automatically assign a public IP address**（パブリック**IP**アドレスを自動的に割り当て）を選択します。これにより、VM-Series ファイアウォールの管理インターフェイス用に、公開された IP アドレスを取得することができます。

      後で、管理インターフェイスに Elastic IP アドレスをアタッチできます。インスタンスが終了するとファイアウォールから関連付けが解除されるパブリック IP アドレスとは異なり、Elastic IP アドレスには永続性があり、どこで IP アドレスを参照する場

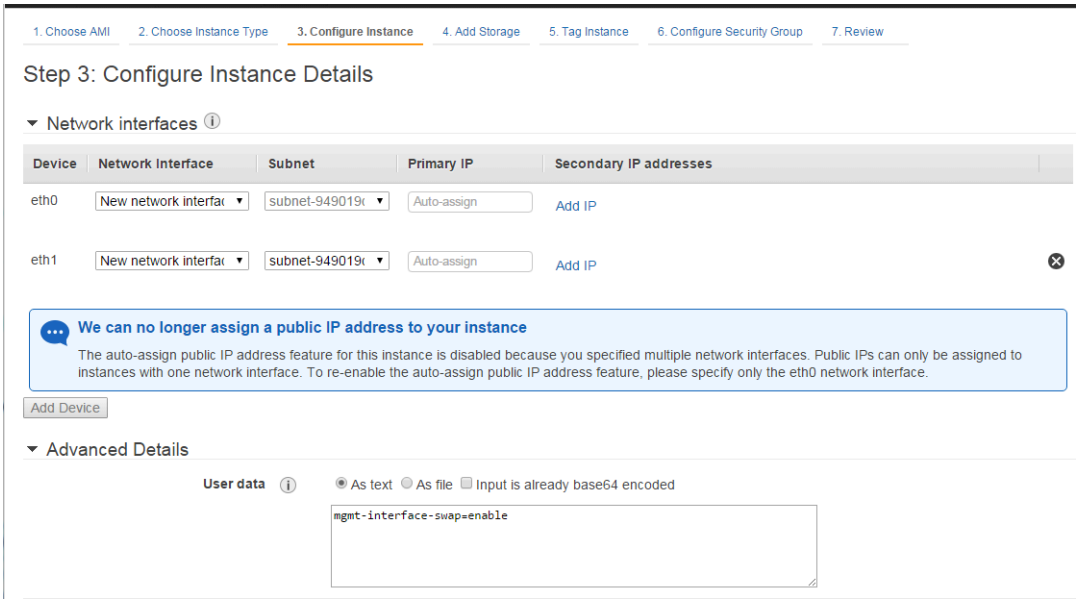
©2023 Palo Alto Networks, Inc.

合も、IP アドレスを再設定することなく VM-Series ファイアウォールの新しい（または代替の）インスタンスに再アタッチできます。

5. **Launch as an EBS-optimized instance**（**EBS**最適化が施されたインスタンスとして起動）を選択します。
6. ファイアウォール上で管理インターフェイスとデータ インターフェイスをスワップできるように、ELB を使用したデプロイメントに新しいネットワーク インターフェイスを追加します。インターフェイスをスワップするには、ENIが2つ以上必要です（eth0およびeth1）。
   - ネットワークインターフェイスの表示を展開し、**Add Device**（デバイスを追加）をクリックしてネットワークインターフェイスをもう一つ追加します。

     VPCにサブネットが一つ以上あり、ローンチ時にENIを追加できることを確認してください。

     ENI が 1 つだけの状態でファイアウォールを起動すると：
     - インターフェイス スワップ コマンドによってファイアウォールがメンテナンス モードになります。
     - *2* つ目の *ENI* を追加したら、ファイアウォールを再起動しなければなりません。
   - Advanced Details（詳細）セクションを展開し、起動中にインターフェイスをスワップするためのテキストとして、**User data**（ユーザーデータ）フィールドに**`mgmt-interface-swap=enable`**と入力します。



Bootstrap Package（ブートストラップパッケージ）–ブートストラップパッケージを使ってファイアウォールをブートストラップする場合、**`mgmt-interface-swap=enable`**の後に区切り文字セミコロンを入力して、次に**`vmseries-bootstrap-aws-s3bucket=<`**バケット名**`>`**を指定することもできます。

User Data（ユーザーデータ）–ユーザーデータでブートストラップを行う場合、**`mgmt-interface-swap=enable`**の後に区切り文字セミコロンを入力し、

©2023 Palo Alto Networks, Inc.

次に「基本設定のユーザーデータとしての入力（パブリッククラウド）」の説明に下がつて追加のキーと値のペアを指定します。

AWS Secret（**AWS**シークレット）—AWSシークレットでブートストラップを行う場合、**`mgmt-interface-swap=enable`**の後に区切り文字セミコロンを入力し、「AWS 上での VM-Series ファイアウォールのブートストラップ」のステップ3の説明に従って、シークレット名をキーと値のペアとして指定します。以下に例を示します。

7. デフォルトの **Storage**（ストレージ）設定を受け入れます。ファイアウォールはボリューム タイプ SSD（gp2）を使用します。

   このキー ペアは、ファイアウォールに初めてアクセスする場合に必要です。また、メンテナンス モードでファイアウォールにアクセスする場合にも必要になります。

8. （任意）タギング。タグを追加して自分のメタデータを作成し、VM-Seriesファイアウォールを識別・グループ化します。たとえば、**Value**（値）に**Name**（名前）タグを追加すれば、このVM-Series ファイアウォールではENIインターフェイスがスワップされているということが分かりやすくなります。
9. 既存の**Security Group**（セキュリティ グループ）を選択するか、または新しく作成します。このセキュリティグループの目的は、ファイアウォールの管理インターフェイスへのアクセスを制限することです。管理インターフェイス用に、最低でもhttpsとsshのアクセスを許可しておいてください。
10. プロンプトが表示されたら、セットアップに適した **SSD** オプションを選択します。
11. **Review and Launch**（確認して起動）を選択します。選択内容が正しいことを確認し、**Launch**（起動）をクリックします。
12. 既存のキー ペアを選択するか、または新しく作成し、キー要求メッセージを受け入れます。
13. プライベート キーをダウンロードして安全な場所に保存します。ファイル拡張子は `.pem` です。このキーは失うと再生成できません。

    VM-Series ファイアウォールの起動には 5 ～ 7 分かかります。進捗状況はEC2ダッシュボードで確認可能です。プロセスが完了すると、EC2 Dashboardの **Instances** [インスタンス] ページに VM-Seriesファイアウォールが表示されます。

©2023 Palo Alto Networks, Inc.

STEP 4 | ファイアウォールの新しい管理者パスワードを設定します。

*VM-Series*ファイアウォールの*CLI*では、一意な管理者用パスワードを設定しなければファイアウォールの*Web*インターフェイスにアクセスできません。*CLI*にログインするには、ファイアウォールをローンチするのに使用した秘密鍵が必要です。

1. パブリック IP アドレスを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH で接続します。CLI にアクセスするには、3で使用または作成した秘密鍵が必要です。

   ELB を使用したデプロイメントをサポートするための *ENI* を追加する場合は、最初に *CLI* にアクセスするための *Elastic IP* アドレスを作成して割り当てなければなりません。6を参照してください。

   SSH アクセス用に PuTTY を使用している場合、「.pem」形式を「.ppk」形式に変換する必要があります。https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.htmlを参照してください。
2. 以下のコマンドを入力してファイアウォールにログインします。

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*
3. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

   configure

   set mgt-config users admin password
4. アクティベートが必要なBYOLを所有している場合、ファイアウォールがPalo Alto Networksライセンスサーバーにできるようにし DNSサーバーのIPアドレスを設定してください。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

   set deviceconfig system dns-setting servers primary *<ip_address>*
5. 以下のコマンドで変更内容をコミットします。

   commit
6. SSH セッションを終了します。

STEP 5 | VM-Series ファイアウォールをシャットダウンします。

1. EC2 Dashboard で、**Instances**（インスタンス）を選択します。
2. リストから VM-Series ファイアウォールを選択し、**Actions**（アクション） > **Stop**（停止）をクリックします。

 ©2023 Palo Alto Networks, Inc.

STEP 6 | Elastic IPアドレス（EIP）を作成し、管理アクセス用ENIに割り当て、VM-Serieファイアウォールを再起動します。

1. **Elastic IPs**（**Elastic IP**）を選択し、**Allocate New Address**（新規アドレスを割り当て）をクリックします。
2. **EC2-VPC** を選択し、**Yes, Allocates**（割り当てる）をクリックします。
3. 新しく割り当てられた EIP を選択し、**Associate Addresss**（関連アドレス）をクリックします。
4. **Network Interface**（ネットワークインターフェイス） 選択し、**Private IP addresss**（プライベート**IP**アドレス）から管理インターフェイスに関連付けられたプライベートIPアドレスを選択し、**Yes, Associates**（関連付けを行う）をクリックします。

STEP 7 | 仮想ネットワーク インターフェイス（1 つまたは複数）を作成して、インターフェイス（1 つまたは複数）を VM-Series ファイアウォールに接続します。仮想ネットワーク インターフェイスは、AWS では Elastic Network Interfaces（ENI）と呼ばれ、ファイアウォール上ではデータプレーン ネットワーク インターフェイスとして機能します。これらのインターフェイスは、ファイアウォールとの間のデータ トラフィックの処理に使用されます。

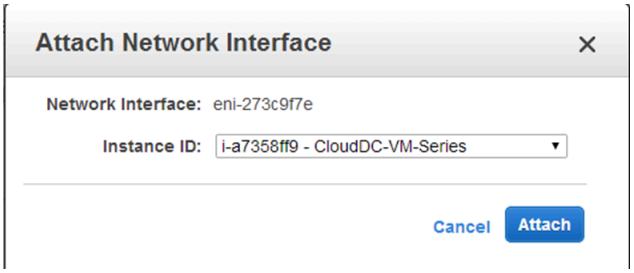
ファイアウォールからのインバウンド/アウトバウンドのトラフィックを許可するENIが最低でも2つ必要となります。VM-Series ファイアウォール上のデータ トラフィックを処理するために 7 個まで ENI を追加できます。EC2 インスタンスタイプをチェックして、サポートされる最大数を確認してください。

1. EC2 Dashboard で **Network Interfacess**（ネットワークインターフェイス）を選択し、**Create Network Interfaces**（ネットワークインターフェイスを作成）をクリックします。
2. 分かりやすいインターフェイス名を入力します。
3. サブネットを選択します。サブネット ID を使用して、正しいサブネットを選択したことを確認します。ENI は、同じサブネット内のインスタンスにのみアタッチできます。
4. インターフェイスに割り当てるアドレスを **Private IPs**（プライベート**IP**）に入力するか、**Auto-assign**（自動割り当て）を選択し、選択されたサブネット内で使用可能な IP アドレスから自動的に IP アドレスを割り当てます。
5. **Security group**（セキュリティ グループ）を選択してネットワーク インターフェイスへのアクセスを制御します。
6. **Yes, Creates**（作成する）をクリックします。



 ©2023 Palo Alto Networks, Inc.

7. VM-Series ファイアウォールに ENI をアタッチするには、上記で作成したインターフェイスを選択し、**Attachs**（アタッチ）をクリックします。



8. **Instance Id**（インスタンス **ID**）で VM-Series ファイアウォールのインスタンス ID を選択し、**Attachs**（アタッチ）をクリックします。
9. 上記の手順を繰り返し、さらに少なくとも 1 つの ENI を作成してファイアウォールにアタッチします。

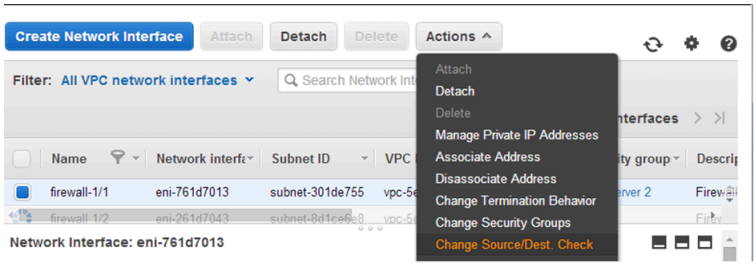
STEP 8 | （従量制のライセンス モデルでは不要）VM-Series ファイアウォール上でライセンスをアクティベートします。

このタスクは、*AWS* 管理コンソールでは実行されません。ライセンスのアクティベーションには、*Palo Alto Networks* サポート ポータルへのアクセスと *VM-Series* ファイアウォールの *Web* インターフェイスが必要です。

「ライセンスのアクティベーション」を参照してください。

STEP 9 | ファイアウォールのデータプレーン ネットワーク インターフェイスごとに送信元/送信先チェックを無効にします。このオプションを無効にすると、ネットワーク インターフェイスに割り当てられた IP アドレス宛てではないネットワーク トラフィックをインターフェイスで処理できるようになります。

1. EC2 Dashboard の **Network Interfacess**（ネットワークインターフェイス）タブで、ネットワーク インターフェイス（eth1/1 など）を選択します。
2. **Action** [アクション] のドロップダウンから、**Change Source/Dest.** を選択します。



3. **Disabled**（無効化）をクリックし、**Save**（保存）をクリックして変更を保存します。
4. ファイアウォールのデータプレーン インターフェイスごとにステップ 1 ～ 3 を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 10 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

設定例については、次の ユース ケースのステップ 14～17を参照してください:AWS クラウドで EC2 インスタンスを保護する」を参照してください。

VPC 内のアプリケーション サーバーで、ファイアウォールのデータプレーン ネットワーク インターフェイスをデフォルトゲートウェイとして定義します。

1. Web ブラウザからの安全な接続（https）を使用し、初期設定時に割り当てた EIP アドレスとパスワードを入力してログインします(https://<Elastic_IP address>)。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。
2. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
3. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「VM_Series_untrust」など）を定義し、**OK** をクリックします。
   - **IPv4** タブで、**Static**（静的）または**DHCP Client**（**DHCP** クライアント）を選択します。

     Static（静的）オプションを使用する場合は、IP セクションで**Add**（追加）をクリックし、インターフェイスの IP アドレスとネットワーク マスクを入力します（例：10.0.0.10/24）。

     この IP アドレスが前に割り当てた ENI の IP アドレスと一致することを確認します。

     DHCP を使用する場合は、**DHCP Clients**（**DHCP** クライアント）を選択します。AWS 管理コンソールで ENI に割り当てたプライベート IP アドレスが自動的に取得されます。
4. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - セキュリティゾーン：VM_Series_trust
   - **IP** アドレス:**Static**（静的）または **DHCP Client**（**DHCP** クライアント）のラジオボタンを選択します。

     スタティックを使用する場合は、IP セクションで**Add**（追加）をクリックし、インターフェイスの IP アドレスとネットワーク マスクを入力します。この IP アドレス

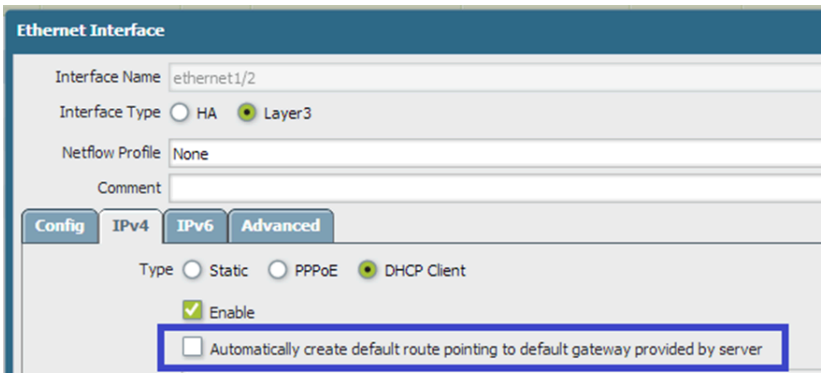
©2023 Palo Alto Networks, Inc.

が、前に割り当てたアタッチされている ENI の IP アドレスと一致することを確認します。

5. **Commit**（コミット）をクリックします。インターフェイスが接続されていることを確認してください。



DHCP を使用する場合は、***Automatically create default route to default gateway provided by server***（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）チェックボックスの選択を解除します。*VPC* のプライベート サブネットにアタッチされているインターフェイスの場合、このオプションを無効にすると、このインターフェイスで処理されるトラフィックが *VPC* のインターネット ゲートウェイに直接流れなくなります。



STEP 11 | VPC でデプロイされているサーバーからのインバウンドおよびアウトバウンド トラフィックを許可する NAT ルールを作成します。

1. ファイアウォールの Web インターフェイスで **Policies**（ポリシー） > **NAT** を選択します。
2. ファイアウォールのデータプレーン ネットワーク インターフェイスから VPC の Web サーバー インターフェイスへのトラフィックを許可する NAT ルールを作成します。
3. Web サーバーからインターネットへのアウトバウンド アクセスを許可する NAT ルールを作成します。

STEP 12 | VPC 内に展開されたサーバーとの間のトラフィックを許可/拒否するセキュリティ ポリシーを作成します。

1. ファイアウォールの Web インターフェイスで **Policies**（ポリシー） > **Security**（セキュリティ） を選択します。
2. **Add**（追加）をクリックし、ゾーンを指定して、ネットワーク経由のトラフィックを制限して監査するために実行するアプリケーションとロギング オプションを指定します。

©2023 Palo Alto Networks, Inc.

STEP 13 | ファイアウォールで変更をコミットします。

Commit（コミット）をクリックします。

STEP 14 | VM-Series ファイアウォールがトラフィックを保護し、NAT ルールが有効であることを確認します。

1. ファイアウォールの Web インターフェイスで **Monitor**（監視） > **Logs**（ログ） > **Traffic**（トラフィック）を選択します。
2. ログを表示し、実装したセキュリティ ポリシーにネットワークを通過するアプリケーションが適合していることを確認します。

AWS Outposts での VM-Series ファイアウォールの起動

VM-Series ファイアウォールを AWS Ouptost にデプロイするには、この手順を実行します。注文完了電子メールに記載されているキャパシティ認証コードをまだ登録していない場合は、「VM-Series ファイアウォールの登録」を参照してください。

STEP 1 | AWS Outposts コンソールにアクセスします。

STEP 2 | AWS Outpost ラックを含むように、VPC を拡張します。

VM-Series ファイアウォールは EC2 インスタンスからのトラフィックを受信して、VPC とインターネットとの間でインバウンドおよびアウトバウンド通信を実行できなければなりません。

Outpost を VPCに接続する手順については、AWS Outpost のドキュメントを参照してください。

1. ネットワーク コンポーネントとセキュリティ コンポーネントが適切に定義されていることを確認します。
   - インターネットとの通信を有効化します。ローカル LAN とインターネットを接続するために、Outpost にはローカル ゲートウェイが必要です。
   - Outpost subnet（Outpost サブネット）を作成します。
   - EC2 インスタンス/サブネットからのインバウンド/アウトバウンド トラフィックを管理するには、必要に応じてセキュリティ グループを作成します。
   - プライベート サブネットのルート テーブルにルートを追加し、該当する VPC 内のセブネットおよびセキュリティ グループ全体に確実にトラフィックをルーティングできるようにします。
2. VM-Series ファイアウォールのペアを HA にデプロイする場合、AWS における VM-Series ファイアウォールの高可用性設定を設定する前にHA 用の IAM ロールを定義する必要があります。
3. （任意）ブートストラップによって VM-Series ファイアウォールを設定する場合は、「AWS 上での VM-Series ファイアウォールのブートストラップ」を参照してください。ブートストラップの詳細は、「VM-Series ファイアウォールのブートストラップ」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 3 | VM-Series ファイアウォールを起動します。

*VM-Series*ファイアウォールを起動する際にネットワークインターフェイス（*ENI*）を追加することは可能ですが、この場合、ファイアウォールを再起動した際に、*AWS*は管理インターフェイスに自動的に割り当てられたパブリック*IP*アドレスを放棄します。管理インターフェイスへの接続を確保するためには、ファイアウォールへこれ以上のインターフェイスを追加する前に、管理インターフェイスへ *Elastic IP* アドレスを割り当てる必要があります。

EIPアドレスを保存したい場合、eth 1/1インターフェイスにEIPアドレスを1つ割り当て、このインターフェイスを管理トラフィックとデータトラフィックの両方に使用することも可能です。インターフェイスで許可されるサービスを制限したい場合、あるいはeth 1/1にログイン可能なIPアドレスを制限したい場合はインターフェイスに管理プロファイルを適用してください。

1. EC2 Dashboard で、**Launch Instance**（インスタンスを起動）をクリックします。
2. VM-Series AMI を選択します。AMI の取得方法については、「AMI の取得」を参照してください。
3. EC2 インスタンスで VM-Series ファイアウォールを起動します。
   1. ファイアウォールに必要なリソースを割り当てるための **EC2 instance type**（**EC2** インスタンス タイプ）を選択してから **Next**（次へ）をクリックします。リソースの要件については、「VM-Series のシステム要件」を参照してください。
   2. VPC を選択します。
   3. Outpost で、VM-Series 管理インターフェイスにアタッチするパブリック サブネットを選択します。
   4. **Automatically assign a public IP address**（パブリック**IP**アドレスを自動的に割り当て）を選択します。これにより、VM-Series ファイアウォールの管理インターフェイス用に、公開された IP アドレスを取得することができます。

      後で、管理インターフェイスに Elastic IP アドレスをアタッチできます。インスタンスが終了するとファイアウォールから関連付けが解除されるパブリック IP アドレスとは異なり、Elastic IP アドレスには永続性があり、どこで IP アドレスを参照する場合も、IP アドレスを再設定することなく VM-Series ファイアウォールの新しい（または代替の）インスタンスに再アタッチできます。
   5. **Launch as an EBS-optimized instance**（**EBS**最適化が施されたインスタンスとして起動）を選択します。
   6. ファイアウォール上で管理インターフェイスとデータ インターフェイスをスワップできるように、ELB を使用したデプロイメントに新しいネットワーク インターフェ

©2023 Palo Alto Networks, Inc.

イスを追加します。インターフェイスをスワップするには、ENIが2つ以上必要です（eth0およびeth1）。

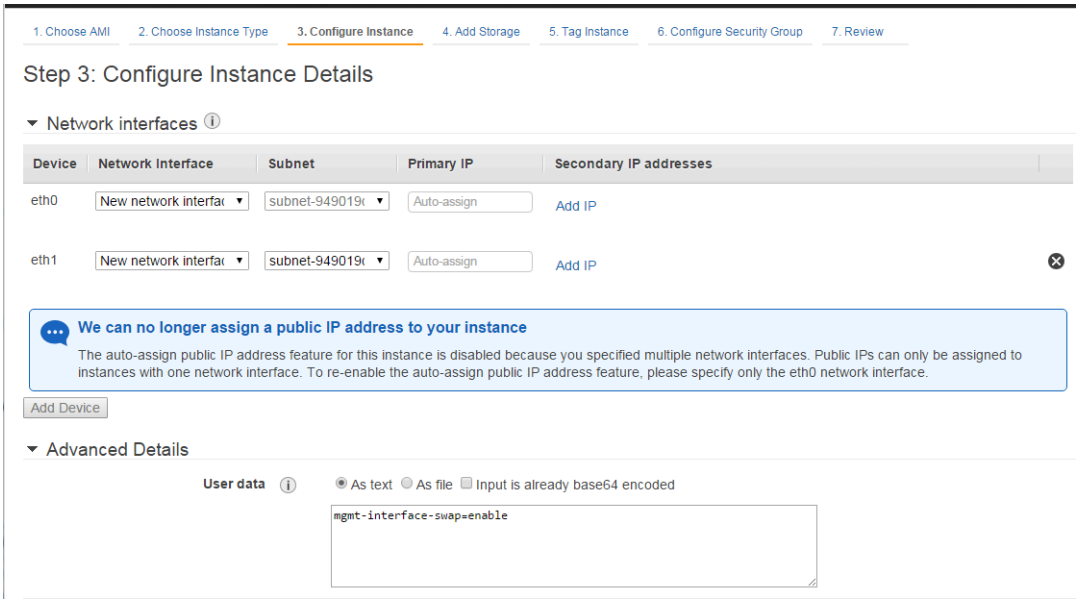
- ネットワークインターフェイスの表示を展開し、**Add Device**（デバイスを追加）をクリックしてネットワークインターフェイスをもう一つ追加します。

  VPCにサブネットが一つ以上あり、ローンチ時にENIを追加できることを確認してください。

  ENI が 1 つだけの状態でファイアウォールを起動すると：
  - インターフェイス スワップ コマンドによってファイアウォールがメンテナンス モードになります。
  - *2 つ目の ENI* を追加したら、ファイアウォールを再起動しなければなりません。

- Advanced Details（詳細）セクションを展開し、起動中にインターフェイスをスワップするためのテキストとして、User（ユーザー）データ フィールドに **`mgmt-interface-swap=enable`** と入力します。

  ファイアウォールをブートストラップする場合は、***`mgmt-interface-swap=enable`***の後に区切り文字のコンマと***`vmseries-bootstrap-aws-s3bucket=<bucketname>`***を入力します。



7. デフォルトの **Storage**（ストレージ）設定を受け入れます。ファイアウォールはボリューム タイプ SSD（gp2）を使用します。

   このキー ペアは、ファイアウォールに初めてアクセスする場合に必要です。また、メンテナンス モードでファイアウォールにアクセスする場合にも必要になります。

8. （任意）タギング。タグを追加して自分のメタデータを作成し、VM-Seriesファイアウォールを識別・グループ化します。たとえば、**Value**（値）に**Name**（名前）タグ

©2023 Palo Alto Networks, Inc.

を追加すれば、このVM-Series ファイアウォールではENIインターフェイスがスワップされているということが分かりやすくなります。

9. 既存の**Security Group**（セキュリティ グループ）を選択するか、または新しく作成します。このセキュリティグループの目的は、ファイアウォールの管理インターフェイスへのアクセスを制限することです。管理インターフェイス用に、最低でもhttpsとsshのアクセスを許可しておいてください。
10. プロンプトが表示されたら、セットアップに適した **SSD** オプションを選択します。
11. **Review and Launch**（確認して起動）を選択します。選択内容が正しいことを確認し、**Launch**（起動）をクリックします。
12. 既存のキー ペアを選択するか、または新しく作成し、キー要求メッセージを受け入れます。
13. プライベート キーをダウンロードして安全な場所に保存します。ファイル拡張子は `.pem` です。このキーは失うと再生成できません。

    VM-Series ファイアウォールの起動には 5 ～ 7 分かかります。進捗状況はEC2ダッシュボードで確認可能です。プロセスが完了すると、EC2 Dashboardの **Instances** [インスタンス] ページに VM-Seriesファイアウォールが表示されます。

STEP 4 | ファイアウォールの新しい管理者パスワードを設定します。

*VM-Series*ファイアウォールの*CLI*では、一意な管理者用パスワードを設定しなければファイアウォールの*Web*インターフェイスにアクセスできません。*CLI*にログインするには、ファイアウォールをローンチするのに使用した秘密鍵が必要です。

1. パブリック IP アドレスを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH で接続します。CLI にアクセスするには、3で使用または作成した秘密鍵が必要です。

   ELB を使用したデプロイメントをサポートするための *ENI* を追加する場合は、最初に *CLI* にアクセスするための *Elastic IP* アドレスを作成して割り当てなければなりません。6を参照してください。

   SSH アクセス用に PuTTY を使用している場合、「.pem」形式を「.ppk」形式に変換する必要があります。https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.htmlを参照してください。
2. 以下のコマンドを入力してファイアウォールにログインします。

   ssh -i <*private_key.pem*> admin@<*public-ip_address*>
3. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

   configure

   set mgt-config users admin password
4. アクティベートが必要なBYOLを所有している場合、ファイアウォールがPalo Alto Networksライセンスサーバーにできるようにに DNSサーバーのIPアドレスを設定してく

©2023 Palo Alto Networks, Inc.

ださい。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

```
set deviceconfig system dns-setting servers primary <ip_address>
```

5. 以下のコマンドで変更内容をコミットします。

```
commit
```

6. SSH セッションを終了します。

STEP 5 | VM-Series ファイアウォールをシャットダウンします。

1. EC2 Dashboard で、**Instances**（インスタンス）を選択します。
2. リストから VM-Series ファイアウォールを選択し、**Actions**（アクション） > **Stop**（停止）をクリックします。

STEP 6 | Elastic IPアドレス（EIP）を作成し、管理アクセス用ENIに割り当て、VM-Serieファイアウォールを再起動します。

1. **Elastic IPs**（**Elastic IP**）を選択し、**Allocate New Address**（新規アドレスを割り当て）をクリックします。
2. **EC2-VPC** を選択し、**Yes, Allocates**（割り当てる）をクリックします。
3. 新しく割り当てられた EIP を選択し、**Associate Addresss**（関連アドレス）をクリックします。
4. **Network Interface**（ネットワークインターフェイス） 選択し、**Private IP addresss**（プライベート**IP**アドレス）から管理インターフェイスに関連付けられたプライベートIPアドレスを選択し、**Yes, Associates**（関連付けを行う）をクリックします。

STEP 7 | 仮想ネットワーク インターフェイス（1 つまたは複数）を作成して、インターフェイス（1 つまたは複数）を VM-Series ファイアウォールに接続します。仮想ネットワーク インターフェイスは、AWS では Elastic Network Interfaces（ENI）と呼ばれ、ファイアウォール上ではデータプレーン ネットワーク インターフェイスとして機能します。これらのインターフェイスは、ファイアウォールとの間のデータ トラフィックの処理に使用されます。

ファイアウォールからのインバウンド/アウトバウンドのトラフィックを許可するENIが最低でも2つ必要となります。VM-Series ファイアウォール上のデータ トラフィックを処理するために 7 個まで ENI を追加できます。EC2 インスタンスタイプをチェックして、サポートされる最大数を確認してください。

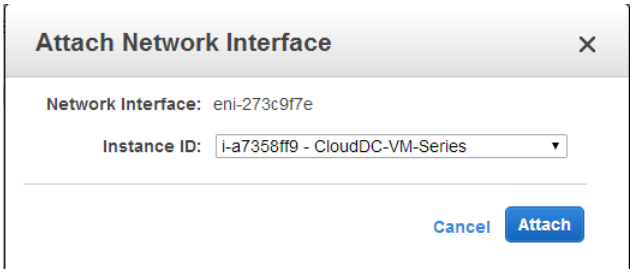
1. EC2 Dashboard で **Network Interfacess**（ネットワークインターフェイス）を選択し、**Create Network Interfaces**（ネットワークインターフェイスを作成）をクリックします。
2. 分かりやすいインターフェイス名を入力します。
3. サブネットを選択します。サブネット ID を使用して、正しいサブネットを選択したことを確認します。ENI は、同じサブネット内のインスタンスにのみアタッチできます。
4. インターフェイスに割り当てるアドレスを **Private IPs**（プライベート**IP**）に入力するか、**Auto-assign**（自動割り当て）を選択し、選択されたサブネット内で使用可能な IP アドレスから自動的に IP アドレスを割り当てます。

©2023 Palo Alto Networks, Inc.

5. **Security group**（セキュリティ グループ）を選択してネットワーク インターフェイスへのアクセスを制御します。
6. **Yes, Creates**（作成する）をクリックします。



7. VM-Series ファイアウォールに ENI をアタッチするには、上記で作成したインターフェイスを選択し、**Attachs**（アタッチ）をクリックします。



8. **Instance Id**（インスタンス **ID**）で VM-Series ファイアウォールのインスタンス ID を選択し、**Attachs**（アタッチ）をクリックします。
9. 上記の手順を繰り返し、さらに少なくとも 1 つの ENI を作成してファイアウォールにアタッチします。

STEP 8 | （従量制のライセンス モデルでは不要）VM-Series ファイアウォール上でライセンスをアクティベートします。

このタスクは、*AWS* 管理コンソールでは実行されません。ライセンスのアクティベーションには、*Palo Alto Networks* サポート ポータルへのアクセスと *VM-Series* ファイアウォールの *Web* インターフェイスが必要です。

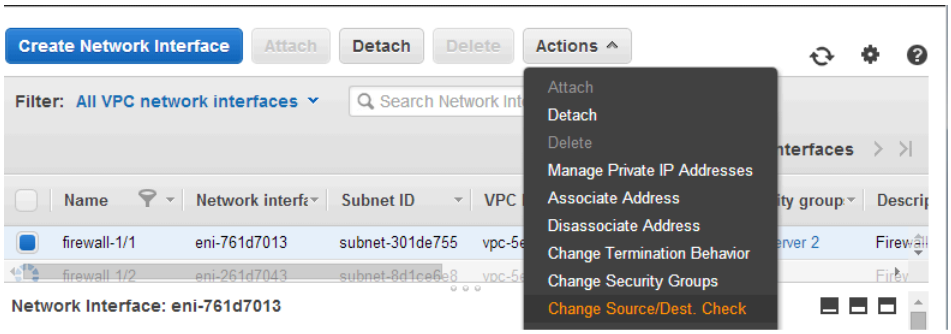
「ライセンスのアクティベーション」を参照してください。

STEP 9 | ファイアウォールのデータプレーン ネットワーク インターフェイスごとに送信元/送信先チェックを無効にします。このオプションを無効にすると、ネットワーク インターフェイスに割り当てられた IP アドレス宛てではないネットワーク トラフィックをインターフェイスで処理できるようになります。

1. EC2 Dashboard の **Network Interfacess**（ネットワークインターフェイス）タブで、ネットワーク インターフェイス（eth1/1 など）を選択します。

©2023 Palo Alto Networks, Inc.

2. **Action** [アクション] のドロップダウンから、**Change Source/Dest.** を選択します。



3. **Disabled**（無効化）をクリックし、**Save**（保存）をクリックして変更を保存します。
4. ファイアウォールのデータプレーン インターフェイスごとにステップ 1 ～ 3 を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 10 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

設定例については、次の ユース ケースのステップ 14～17を参照してください:AWS クラウドで EC2 インスタンスを保護する」を参照してください。

VPC 内のアプリケーション サーバーで、ファイアウォールのデータプレーン ネットワーク インターフェイスをデフォルトゲートウェイとして定義します。

1. Web ブラウザからの安全な接続（https）を使用し、初期設定時に割り当てた EIP アドレスとパスワードを入力してログインします(https://<Elastic_IP address>)。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。
2. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
3. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「VM_Series_untrust」など）を定義し、**OK** をクリックします。
   - **IPv4** タブで、**Static**（静的）または**DHCP Client**（**DHCP** クライアント）を選択します。

     Static（静的）オプションを使用する場合は、IP セクションで**Add**（追加）をクリックし、インターフェイスの IP アドレスとネットワーク マスクを入力します（例：10.0.0.10/24）。

     この IP アドレスが前に割り当てた ENI の IP アドレスと一致することを確認します。

     DHCP を使用する場合は、**DHCP Clients**（**DHCP** クライアント）を選択します。AWS 管理コンソールで ENI に割り当てたプライベート IP アドレスが自動的に取得されます。
4. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - セキュリティゾーン：VM_Series_trust
   - **IP** アドレス:**Static**（静的）または **DHCP Client**（**DHCP** クライアント）のラジオボタンを選択します。

     スタティックを使用する場合は、IP セクションで**Add**（追加）をクリックし、インターフェイスの IP アドレスとネットワーク マスクを入力します。この IP アドレス

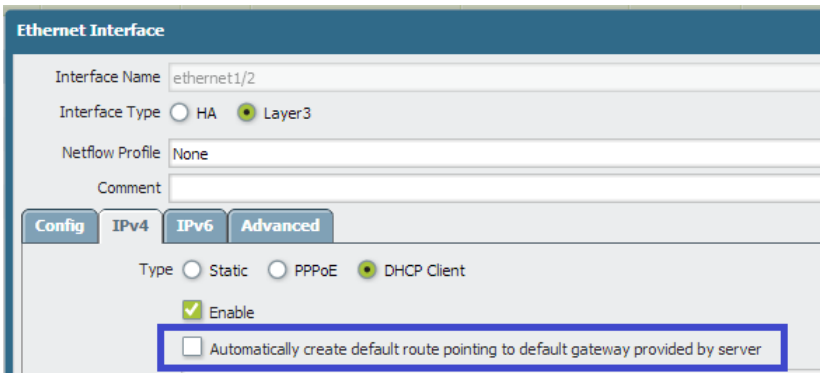
©2023 Palo Alto Networks, Inc.

が、前に割り当てたアタッチされている ENI の IP アドレスと一致することを確認します。

5. **Commit**（コミット）をクリックします。インターフェイスが接続されていることを確認してください。



DHCP を使用する場合は、***Automatically create default route to default gateway provided by server***（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）チェックボックスの選択を解除します。*VPC* のプライベート サブネットにアタッチされているインターフェイスの場合、このオプションを無効にすると、このインターフェイスで処理されるトラフィックが *VPC* のインターネット ゲートウェイに直接流れなくなります。



STEP 11 | VPC でデプロイされているサーバーからのインバウンドおよびアウトバウンド トラフィックを許可する NAT ルールを作成します。

1. ファイアウォールの Web インターフェイスで **Policies**（ポリシー） > **NAT** を選択します。
2. ファイアウォールのデータプレーン ネットワーク インターフェイスから VPC の Web サーバー インターフェイスへのトラフィックを許可する NAT ルールを作成します。
3. Web サーバーからインターネットへのアウトバウンド アクセスを許可する NAT ルールを作成します。

STEP 12 | VPC 内に展開されたサーバーとの間のトラフィックを許可/拒否するセキュリティ ポリシーを作成します。

1. ファイアウォールの Web インターフェイスで **Policies**（ポリシー） > **Security**（セキュリティ） を選択します。
2. **Add**（追加）をクリックし、ゾーンを指定して、ネットワーク経由のトラフィックを制限して監査するために実行するアプリケーションとロギング オプションを指定します。

©2023 Palo Alto Networks, Inc.

STEP 13 | ファイアウォールで変更をコミットします。

Commit（コミット）をクリックします。

STEP 14 | VM-Series ファイアウォールがトラフィックを保護し、NAT ルールが有効であることを確認します。

1. ファイアウォールの Web インターフェイスで **Monitor**（監視） > **Logs**（ログ） > **Traffic**（トラフィック）を選択します。
2. ログを表示し、実装したセキュリティ ポリシーにネットワークを通過するアプリケーションが適合していることを確認します。

カスタム Amazon Machine Image（AMI）の作成

AWS パブリック Marketplace または AWS GovCloud Marketplace に公開された AMI だけを使用するように制限する代わりに、カスタム VM-Series AMI を使用すると、ネットワークで使用する PAN-OS バージョンを含む VM-Series ファイアウォールを柔軟かつ整合性のある方法でデプロイできます。カスタム AMI を使用すると、必要な PAN-OS バージョンのファイアウォールのデプロイにかかる時間を短縮できます。これは、AWS パブリック Marketplace または AWS GovCloud Marketplace で公開されている AMI でファイアウォールをプロビジョンし、使用する資格のある PAN-OS バージョンまたはネットワークで使用する必要のある PAN-OS バージョンへのソフトウェア アップグレードを実行するためにかかる時間が削減されるためです。Auto Scaling VM-Series ファイアウォール CloudFormation テンプレートまたは作成した他のテンプレートでカスタム AMI を使用できるようになります。

BYOL ライセンス、Bundle 1 ライセンス、または Bundle 2 ライセンスでカスタム AMI を作成できます。カスタム AMI を作成するには、ファイアウォールのすべての設定を削除して出荷時デフォルト設定にリセットする必要があります。これにより、このワークフローでは完全に設定された既存のファイアウォールを使用する代わりに、AWS Marketplace からのファイアウォールの新しいインスタンスを起動できます。

BYOL バージョンのファイアウォールを使用してカスタム *AMI* を作成するときには、最初にファイアウォールでライセンスを有効にする必要があります。これにより、ファイアウォールをアップグレードするための *PAN-OS* ソフトウェア更新にアクセスしてダウンロードし、ファイアウォールでライセンスを無効にしてから、ファイアウォールを工場出荷時デフォルト設定にリセットしてカスタム *AMI* を作成できます。ライセンスを無効にしないと、このファイアウォール インスタンスに適用したライセンスを失うことになります。

STEP 1 | Marketplace から VM-Series ファイアウォールを起動します。

「3」を参照してください

STEP 2 | （BYOL のみ）ライセンスを有効にします。

STEP 3 | ソフトウェア更新をインストールし、ファイアウォールを使用する予定の PAN-OS バージョンにアップグレードします。

STEP 4 | （BYOL のみ）ライセンスを無効にします。

©2023 Palo Alto Networks, Inc.

STEP 5 | プライベート データ リセットを実行します。

プライベート データ リセットを実行するとすべてのログが削除され、デフォルト設定が復元されます。

システム ディスクは消去されません。このため、ステップ 4 のコンテンツの更新内容は維持されます。

1. ファイアウォール CLI にアクセスします。
2. すべてのログを削除し、デフォルト設定を復元します。

```
request system private-data-reset
```

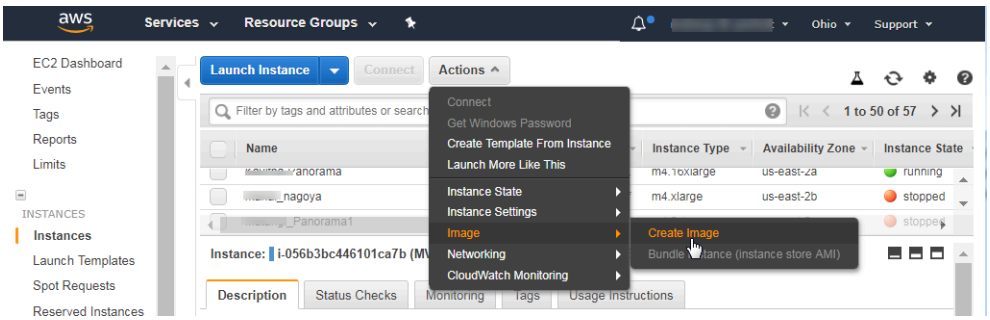
y と入力して確定します。

ファイアウォールが再起動し、デフォルト設定が初期化されます。

©2023 Palo Alto Networks, Inc.

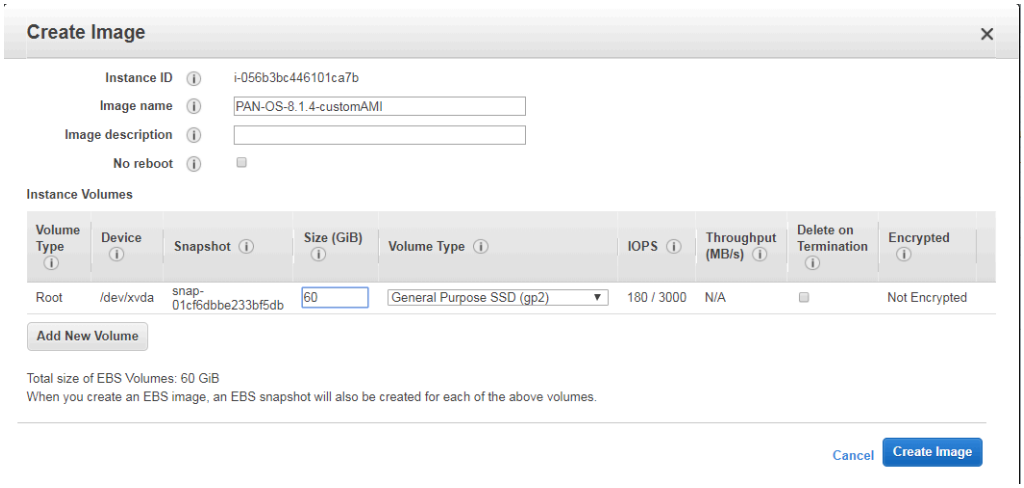
STEP 6 | カスタム AMI を作成します。

1. AWS コンソールにログインし、EC2 Dashboard を選択します。
2. VM-Series ファイアウォールを停止します。
3. VM-Series ファイアウォール インスタンスを選択し、**Image**（イメージ） > **Create Image**（イメージの作成）をクリックします。



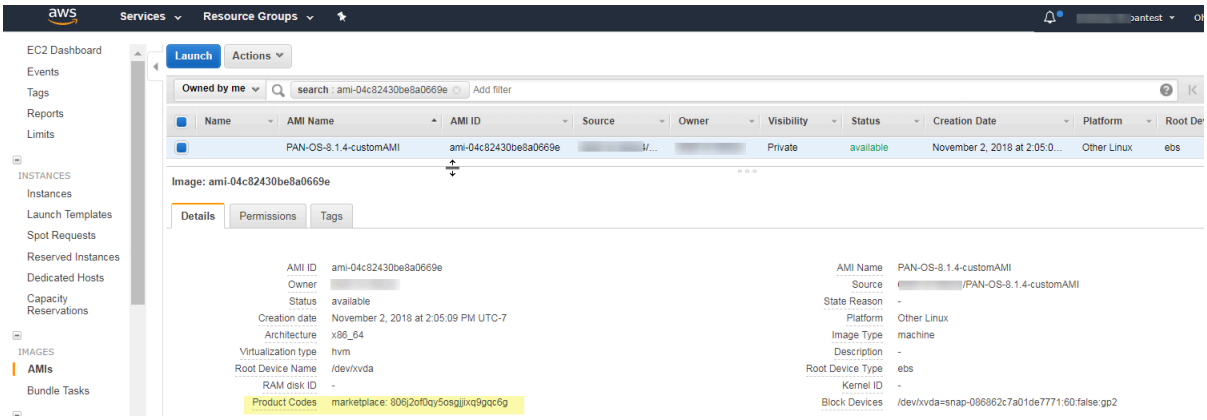
4. カスタム イメージ名を入力し、**Create Image**（イメージの作成）をクリックします。

   ディスク スペースの最小必要容量は 60GB です。



5. カスタム AMI が作成され、正しい製品コードが設定されていることを確認します。
   1. EC2 Dashboard で **AMI**を選択します。
   2. 作成した AMI を選択します。BYOL、Bundle 1、または Bundle 2 のいずれのライセンス オプションで AMI を選択したかどうかに応じて、次のいずれかの製品コードが詳細に表示されます。
      - BYOL—6njl1pau431dv1qxipg63mvah
      - Bundle 1—6kxdw3bbmdeda3o6i1ggqt4km
      - バンドル2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | AWS 上の VM-Series ファイアウォールの EBS ボリュームの暗号化。

Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング デプロイメントで EBS 暗号化とともにカスタム AMI を使用する予定の場合は、AWS アカウントでデフォルトのマスター キーを使用する必要があります。

STEP 8 | ファイアウォールの管理者パスワードを設定します。

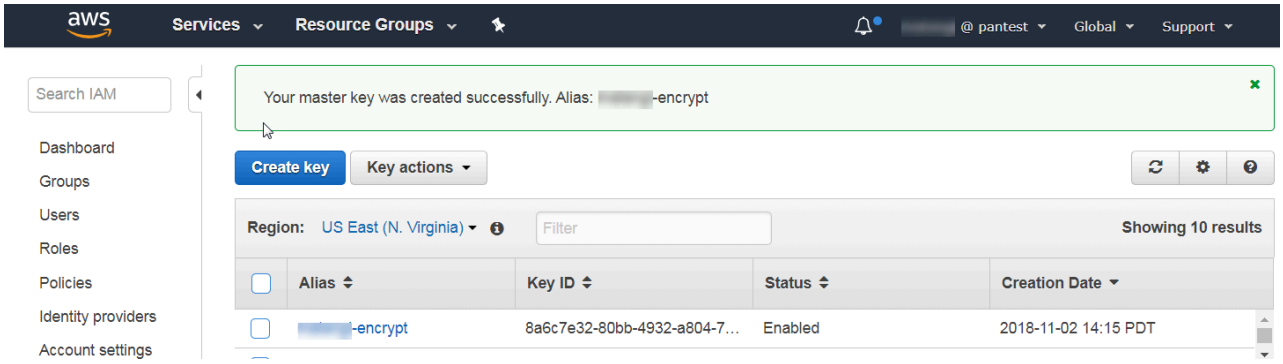
「4」を参照してください

AWS 上の VM-Series ファイアウォールの EBS ボリュームの暗号化

EBS 暗号化は、VM-Series ファイアウォールをデプロイできるすべての AWS EC2 インスタンス タイプ で使用できます。AWS の VM-Series ファイアウォールにデータを安全に保存するには、最初に AWS パブリック Marketplace または GovCloud Marketplace で公開されている AMI のコピーを作成するか、カスタム AMI を使用して、AWS Key Management Service （KMS）のカスタマー マスター キー（CMK）で EBS ボリュームを暗号化します。AWS アカウントのデフォルト マスター キーまたはこれまでに AWS Key Management Service を使用して作成した CMK のいずれかと、データ セキュリティのために KMS が対話する EBS を使用できます。

STEP 1 | AWS で暗号化キーを作成するか、アカウントにデフォルトのマスター キーを使用する場合はこのステップを省略します。

ファイアウォールで EBS ボリュームを暗号化するにはこのキーを使用します。キーがリージョン固有であることに注意してください。

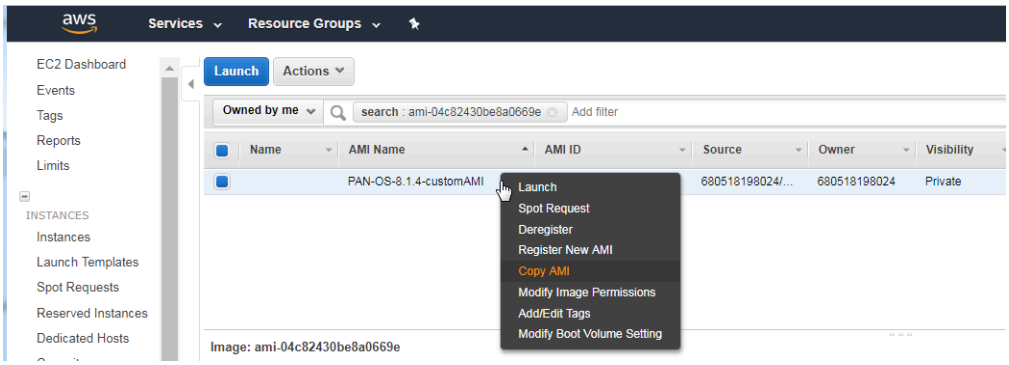


©2023 Palo Alto Networks, Inc.

STEP 2 | このキーを使用して、ファイアウォールで EBS ボリュームを暗号化します。

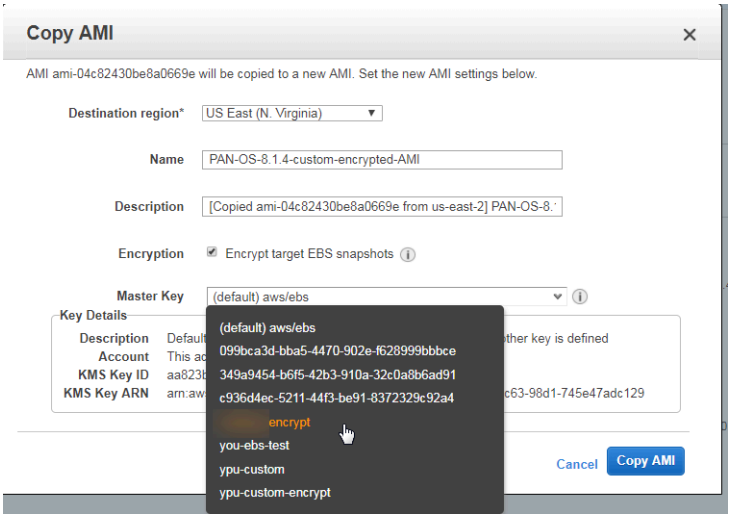
暗号化する AMI のコピーを作成する必要があります。AWS パブリック Marketplace または GovCloud Marketplace で公開されている AMI をコピーするか、カスタム AMI を使用します。（カスタム Amazon Machine Image（AMI）の作成）。

1. EC2 Dashboard で AMI と **Copy AMI**（**AMI** のコピー）を選択します。



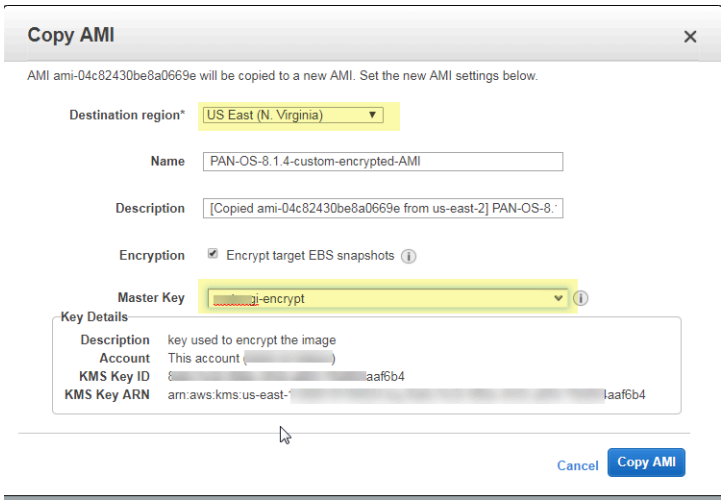
2. AMI の詳細を設定します。

   Encrypt target EBS snapshots（ターゲット **EBS** スナップショットを暗号化する）を必ず選択してください。

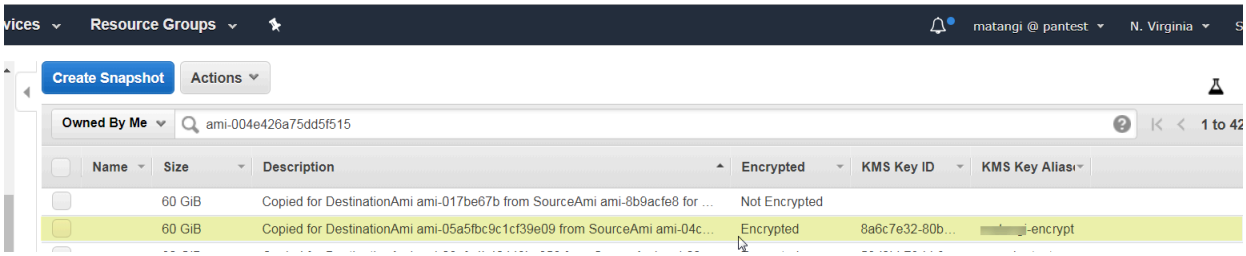


3. 暗号化キーを選択して **Copy AMI**（**AMI** のコピー）を選択し、暗号化 EBS スナップショットを作成します。

©2023 Palo Alto Networks, Inc.



4. **EC2 Dashboard** > **Snapshots**（スナップショット）を選択して、先ほど選択したキーで EBS スナップショットが暗号化されていることを確認します。



VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ

ファイアウォールをデプロイする際に管理インターフェイス（MGT）をデータプレーン インターフェイス（ethernet 1/1）とスワップしなかった場合、ファイアウォールの起動後に CLI を使用し、ファイアウォールがプライマリ インターフェイス上でデータプレーン トラフィックを受信できるようにすることが可能です。

STEP 1 | 「AWS での VM-Series ファイアウォールの起動」のステップ 1 ～ 7 を実行します。

先に進む前に、ファイアウォールに *ENI* が *2* つ（*eth0* および *eth1*）以上あることを確認します。*ENI 1* つだけでファイアウォールを起動する場合、ブート処理時にインターフェイスのスワップ コマンドによってファイアウォールがメンテナンス モードになります。

STEP 2 | EC2 ダッシュボード上で、eth1 インターフェイスの IP アドレスを確認し、AWS セキュリティ グループのルールによって新しい管理インターフェイス（eth1）への接続（HTTPS および SSH）が許可されていることを確認します。

STEP 3 | VM-Series ファイアウォールの CLI にログインし、次のコマンドを入力します。

```
set system setting mgmt-interface-swap enable yes
```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | 確定してインターフェイスをスワップし、eth1 データプレーン インターフェイスを管理インターフェイスとして使用します。

STEP 5 | ファイアウォールを再起動してスワップを反映させます。以下のコマンドを使用します。

```
request restart system
```

STEP 6 | インターフェイスがスワップされたことを確認します。以下のコマンドを使用します。

```
debug show vm-series interfaces all
Phoenix_interface   Base-OS_port   Base-OS_MAC        PCI-ID
       Driver
mgt(interface-swap) eth0   0e:53:96:91:ef:29   0000:00:04.0
  ixgbevf
Ethernet1/1           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0
  ixgbevf
```

VM-Series ファイアウォールでの CloudWatch モニタリングの有効化

AWS の VM-Series ファイアウォールはネイティブ PAN-OS メトリックを AWS CloudWatch に公開でき、これを使用してファイアウォールをモニターできます。これらのメトリックによりパフォーマンスおよび使用パターンを評価し、その評価に基づいて VM-Series ファイアウォールのインスタンスを起動または終了するためのアクションを実行できます。

ファイアウォールは AWS API を使用してメトリックを 名前空間 に発行します。これは、指定された時間間隔でメトリックが収集されるAWS上の場所です。AWS CloudWatchにメトリックを発行するようにファイアウォールを構成すると、メトリックを表示できる2つの名前空間があります。プライマリ名前空間は、名前空間を使用するように構成されたすべてのインスタンスの選択されたメトリックを収集および集約し、セカンダリ名前空間は サフィックス `_dimensions` を使用すると、ホスト名とAWSインスタンスIDメタデータ（または ディメンション）を使用してメトリックをフィルタリングし、個々のVM-Seriesファイアウォールの使用状況とパフォーマンスを可視化できます。

これで、CloudWatch のメトリックをモニターしたり、アラームをトリガーするオート スケーリング ポリシーを作成して、モニターしているメトリックがしきい値に達した場合にファイアウォールの新しいインスタンスを手動でデプロイするためのアクションを実行したりできます。アクションをスケール アウトまたはスケール インするためのアラーム条件の設定のベスト プラクティスについては、『AWS CloudWatch』および『オート スケーリング グループ（ASG）』ドキュメントを参照してください。

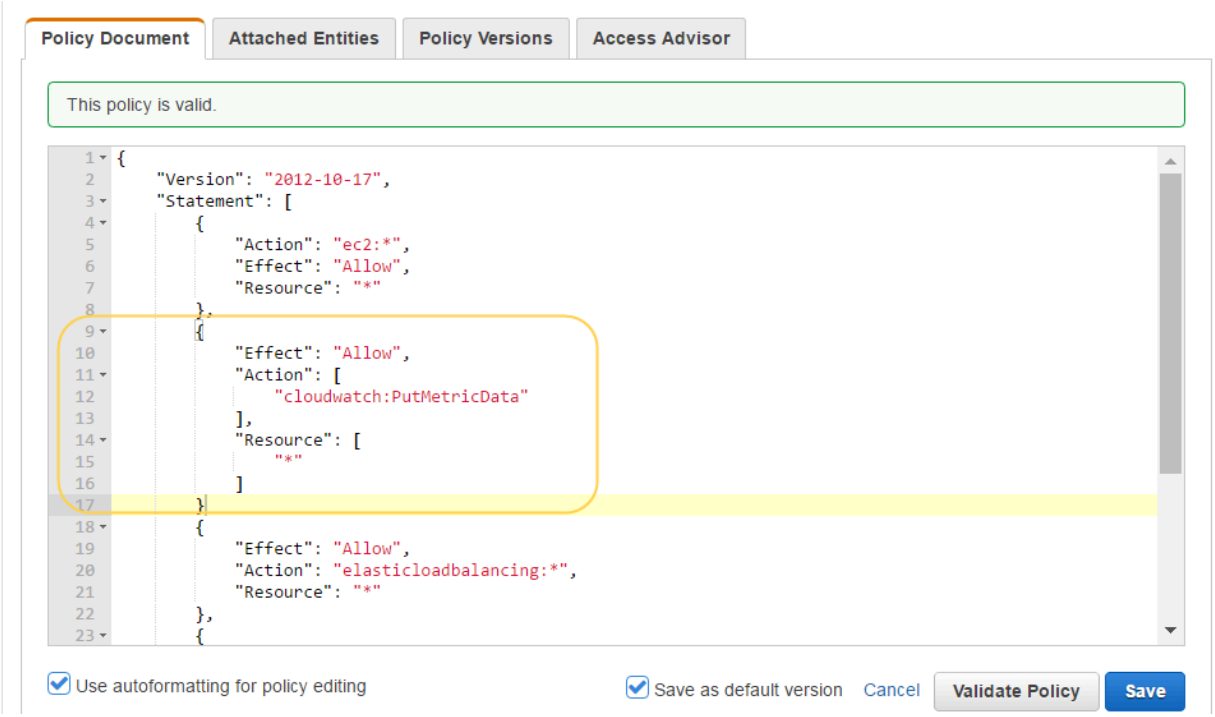
CloudWatch に公開できる PAN-OS メトリックについては、「監視用に公開されるカスタム PAN-OS メトリック」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 1 | AWS で VM-Series ファイアウォールをデプロイするために使用する AWS アイデンティティおよびアクセス管理（IAM）ユーザー ロールの適切な許可を割り当てます。

VM-Series ファイアウォールの新規インスタンスを起動するか AWS の既存の VM-Series ファイアウォールをアップグレードするかに関係なく、インスタンスに関連付けられた IAM ロールには、CloudWatch にメトリックを公開する許可が必要です。

1. AWS コンソールで IAM を選択します。
2. IAM ロールを編集し、以下の許可を付与します。



ここで権限をコピーして貼り付けることができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
             "Action": [
                 "cloudwatch:PutMetricData"
             ],
             "Resource": [
                 "*"
             ]
        }
    ]
}
```


©2023 Palo Alto Networks, Inc.

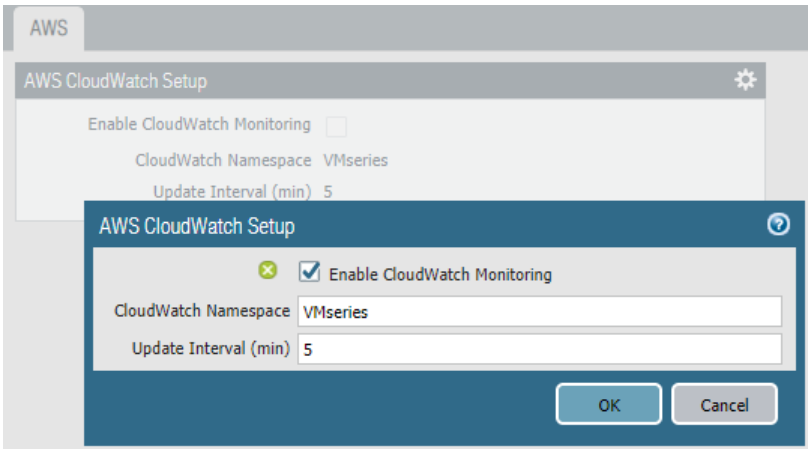
STEP 2 | AWS の VM-Series ファイアウォールで CloudWatch を有効化します。

1. VM-Series ファイアウォールの Web インターフェイスにログインします
2. **Device**（デバイス） > **VM-Series**を選択します。
3. AWS CloudWatch Setup（AWS CloudWatch のセットアップ）で **Edit**（編集）（⚙）をクリックし、**Enable CloudWatch Monitoring**（**CloudWatch** モニタリングを有効にする）を選択します。

   1. ファイアウォールがメトリックを公開できる **CloudWatch Namespace**（**CloudWatch** 名前空間）を入力します。名前空間の先頭に **AWS** は使用できません。

      HA ペアまたは自動スケーリング展開内のすべての VM-Series ファイアウォールの集約メトリックは、上記で入力した名前空間に公開されます。自動的に作成される `_dimensions`サフィックス が付いた名前空間を使用すると、ファイアウォールに接続されたホスト名または AWS インスタンス ID メタデータを使用して、特定のVM-Seriesファイアウォールのメトリックをフィルタリングおよび表示できます。

   2. **Update Interval**（更新間隔）を 1 ～ 60 分の値に設定します。これは、ファイアウォールが CloudWatch にメトリックを公開する頻度です。デフォルトは 5 分です。



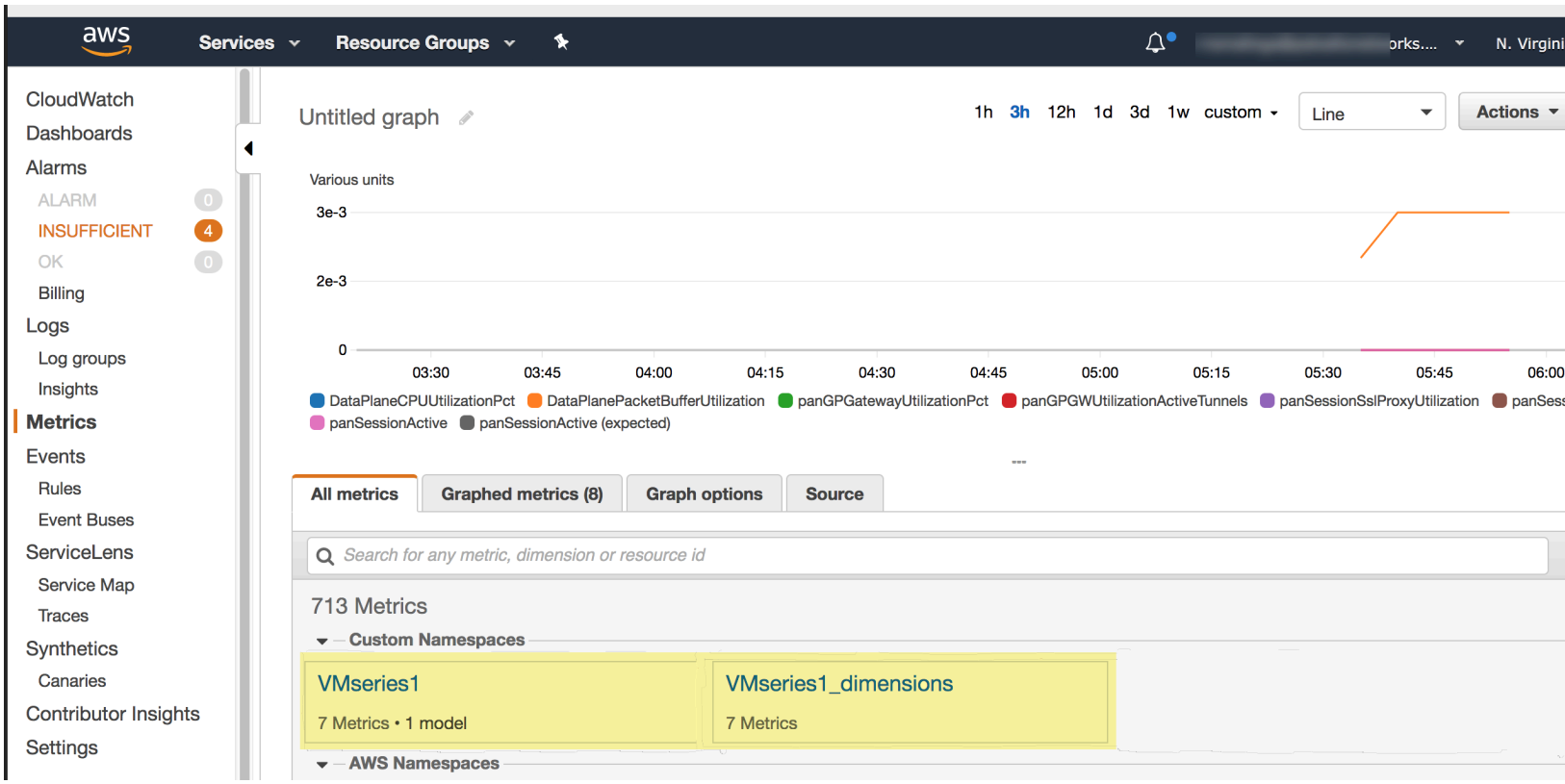
4. 変更を **Commit**（コミット）します。

   ファイアウォールが CloudWatch へのメトリックの公開を開始するまで、PAN-OS メトリックのアラームを設定できません。

©2023 Palo Alto Networks, Inc.

STEP 3 | CloudWatch でメトリックが表示されることを確認します。

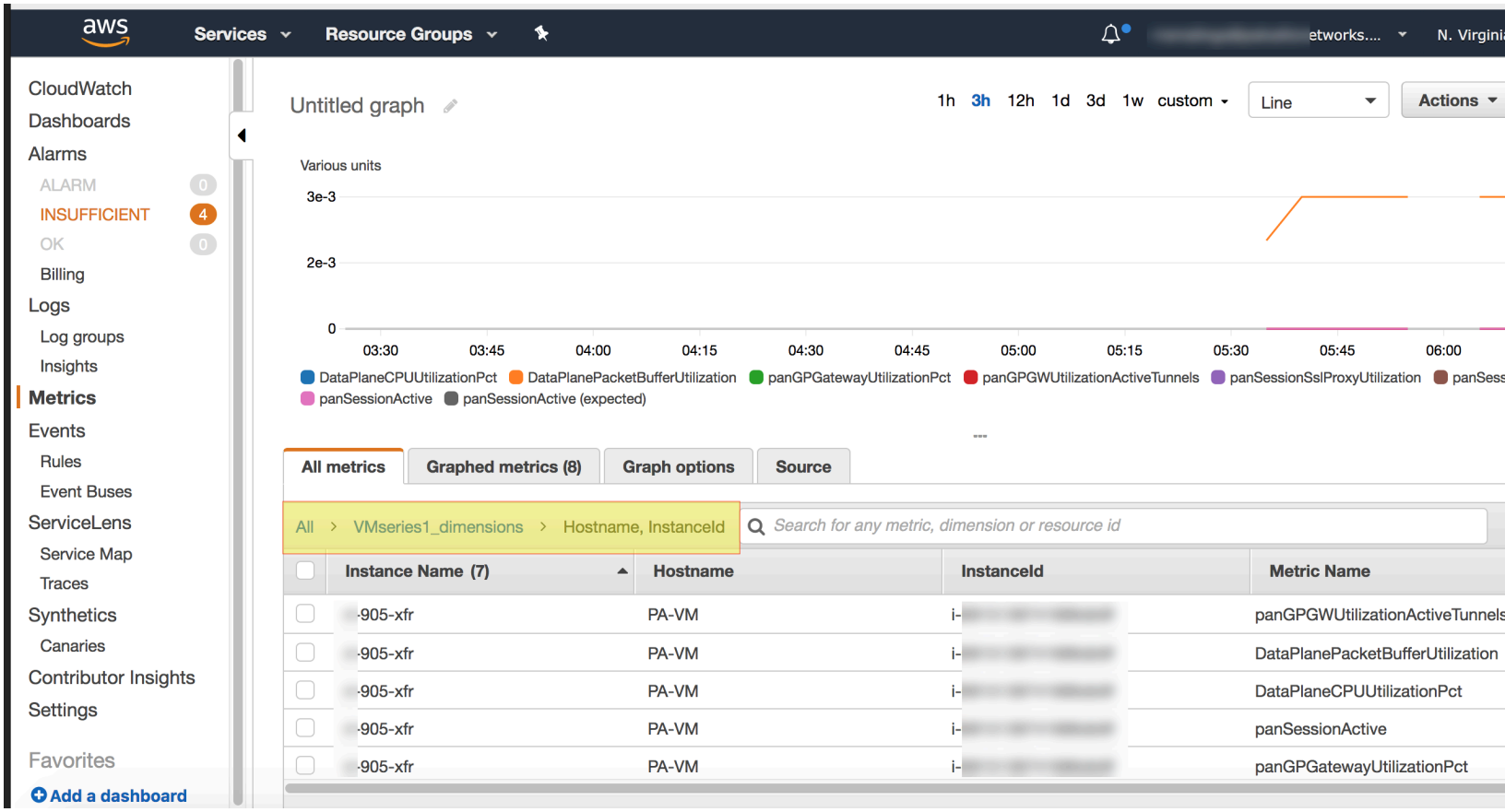
1. AWS コンソールで **CloudWatch** > **Metrics**（メトリック）の順に選択し、カテゴリ別に CloudWatch メトリックを表示します。
2. Custom Metrics（カスタム メトリック）ドロップダウンから、名前空間を選択します。



3. 表示中のリストに PAN-OS メトリックが表示されることを確認します。

   特定のファイアウォールのホスト名または AWS インスタンス ID でフィルタリングするには、`_dimensions`を選択します。

©2023 Palo Alto Networks, Inc.



STEP 4 | CloudWatch で PAN-OS メトリックのアラームおよびアクションを設定します。

http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html にあるAWSドキュメントを参照してください。

ブートストラップ設定のある VM-Series ファイアウォールの場合、サービスが利用できるようになるまでおよそ 7 ～ 9 分かかります。そのため、VM-Series ファイアウォールのオートスケーリングを始動するアラームの設定方法の例をいくつか紹介します。

- リモート ユーザーを保護する GlobalProtect ゲートウェイとして VM-Series ファイアウォールのインスタンスを 2 つデプロイしている場合、GlobalProtect ゲートウェイのアクティブ トンネル メトリックを使用します。アクティブなトンネルの数が 15 分間に 300 を超えた場合のアラームを設定し、VM-Series ファイアウォールの新しいインスタンスを 2 つデプロイできます。これらのインスタンスはブートストラップされ、Global Protect ゲートウェイとして機能するように設定されます。
- AWS のワークロードを保護するためにファイアウォールを使用している場合、セッション使用率メトリックを使用し、リソース使用率に基づいてファイアウォールをスケールインまたはスケール アウトします。セッション使用率メトリックが 15 分間に 60% を上回った場合のアラームを設定し、VM-Series ファイアウォール のインスタンスを 1 つデプロイできます。逆に、セッション使用率が 30 分間に 50% を下回った場合、VM-Series ファイアウォールのインスタンスを終了してください。

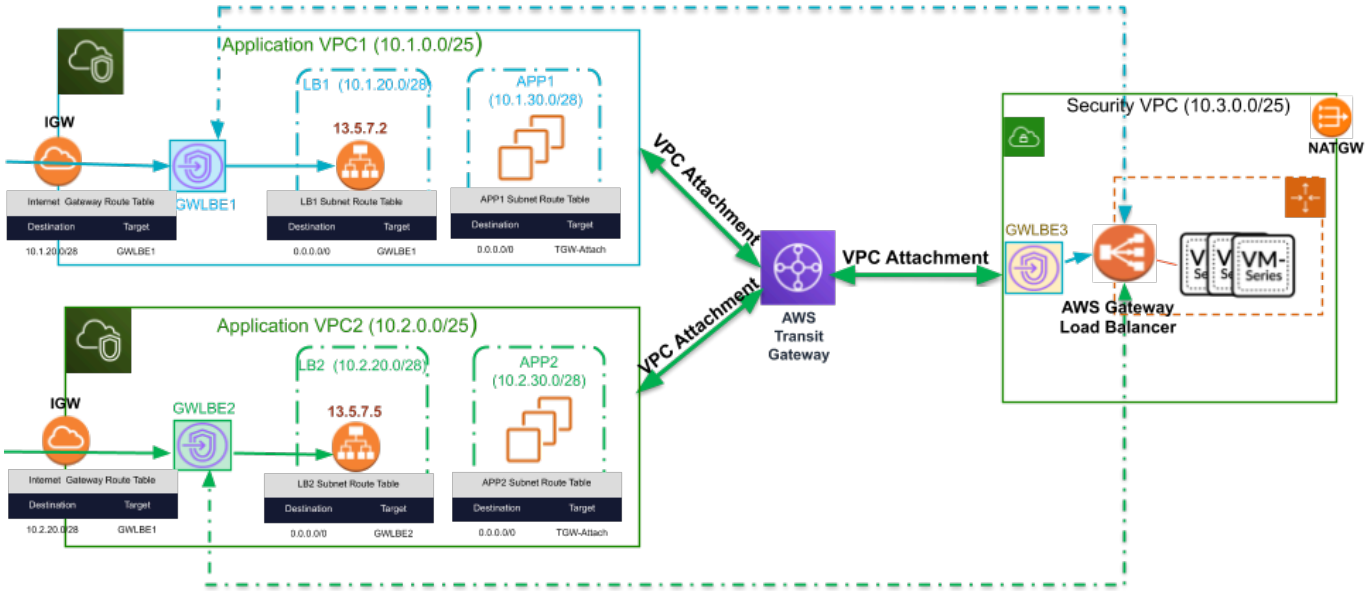
©2023 Palo Alto Networks, Inc.

VM-SeriesとAWS Gateway Load Balancerの統合

AWSゲートウェイロードバランサー（GWLB）は、VM-Seriesファイアウォールのスタックをデプロイして、水平方向にスケーラブルでフォルトトレラントな方法で運用するための、AWSが管理するサービスです。AWS GWLBは、ファイアウォールのスタックとともに、トラフィック検査と脅威防御のためのVPCエンドポイントとして公開することができます。VPCエンドポイント用のゲートウェイロードバランサーエンドポイント（GWLBE）を作成することで、アプリケーションのアウトバウンド、East-West、およびインバウンド トラフィックパスに、オートスケーリングVM-Seriesファイアウォールスタックを手軽に挿入することができます。VM-SeriesファイアウォールとGWLBは、GENEVEカプセル化を使用してトラフィックパケットヘッダーとペイロードをそのまま保持し、アプリケーションへのソースのIDに対する完全な可視性を提供しています。

VM-Series ファイアウォールは、*DHE / ECDHE* 暗号を利用する *TLS1.2* および *TLS1.3* などの、フォワードおよびインバウンドのユースケース用として *GWLB* の背後にデプロイされた場合に復号化をサポートします。

GWLBとVM-Seriesの統合により、AWSトランジットゲートウェイ（TGW）環境がどのように簡素化されるかを、以下の図に示します。トランジットゲートウェイに、集中セキュリティVPCをアタッチします。VM-Seriesファイアウォールのスタック全体に対してトラフィックのスケーリングとロードバランシングを行うために、集中セキュリティVPCにはGWLBが含まれています。



VPCアタッチメント間でルーティングされるトラフィックを、VM-Seriesファイアウォールが検査できるように、VM-Seriesファイアウォールが含まれているセキュリティVPCのトランジットゲートウェイVPCアタッチメント上で、アプライアンスモードを有効にする必要があります。そうすることによって、双方向のトラフィックが対称的にルーティングされます。リクエストおよびレスポンストラフィックの両方が、ファイアウォールVPC内の同じゲートウェイエンドポイントに送信され、GWLBは正しい宛先に送信する前の検査のために、同じVM-Seriesファイアウォールを使用し続けます。

©2023 Palo Alto Networks, Inc.

GWLBとともにデプロイされたVM-Seriesファイアウォールを使って、次の事項を保護できます。

- インバウンドトラフィック—VPC外が起源のトラフィックで、Webサーバーなどのアプリケーションが宛先になっています。VM-Seriesファイアウォールは、AWSセキュリティグループが許可したトラフィック内の、マルウェアや脆弱性がネットワークに潜入することを防止します。
- アウトバウンド トラフィック—アプリケーションVPC内に起源があり、インターネット上の外部リソースが宛先になっているトラフィック。VM-Seriesファイアウォールは、アプリケーションVPC内のワークロードが許可されているサービス（Windows Updateなど）や許可されているURLカテゴリに接続するようにして、機密情報のデータ流出を防止することで、アウトバウンド トラフィックフローを保護します。また、VM-Seriesセキュリティプロファイルは、マルウェアや脆弱性がリターントラフィックに紛れてネットワークに侵入することを防止します。
- East-Westトラフィック—トランジットゲートウェイ環境でEast-Westトラフィックは、2つの異なるアプリケーションVPC内のソースおよび宛先ワークロード間のトラフィックなどの、VPC間トラフィックを表しています。VM-Seriesファイアウォールは、マルウェアの伝搬に対してEast-Westトラフィックフローを保護します。

アプリケーションVPCへのインバウンド トラフィックを保護するために、スポークVPC内にGWLBEエンドポイント（上記の図ではGWLBE1およびGWLBE2）を作成します。次に、エンドポイントおよびファイアウォールを介して、すべてのインバウンドトラフィックをVPCにルーティングするために、スポークVPCのインターネットゲートウェイとサブネットルートテーブルに、ルートルールを追加します。GWLBEがアプリケーションVPCにリダイレクトしたインバウンドトラフィックは、GWLBにリダイレクトされます。次にGWLBは、トラフィックをVM-Seriesターゲットのいずれかにルーティングします。ファイアウォールはトラフィックを検査して、それをGWLBEに送り返します。次にそれが宛先に送信されます。トラフィックは1つのインターフェイスを通じてVM-Seriesファイアウォールに出入りします。

アプリケーションVPCのアウトバウンドトラフィックを保護するために、集中ファイアウォールVPC内にGWLBE（上記の図ではGWLBE3）を作成します。次に、アプリケーションVPC内の、すべてのアウトバウンドトラフィックをトランジットゲートウェイ（TGW）に転送する、ルートルールを使用することができます。TGWには、検査目的で集中セキュリティVPCにすべてのアウトバウンドトラフィックをリダイレクトする、アプリケーションVPCに関連するルートテーブルが存在しています。ファイアウォールがトラフィックを検査して、該当するポリシーを適用したら、トラフィックはGWLBE（GWLBE3）に送り返されて、次にトランジットゲートウェイ（TGW）に転送されます。次に、セキュリティVPCと関連付けられたTGWルートテーブルは、トラフィックを宛先にルーティングします。

アプリケーションVPC間のEast-Westトラフィックを保護するために、集中ファイアウォールVPC内で同じGWLBE（上記の図ではGWLBE3）を使用します。次にアプリケーションVPCおよびトランジットゲートウェイ内のルートルールを使用して、検査のためにトラフィックを集中セキュリティVPCにリダイレクトします。

CloudFormationテンプレート（CFT）、またはTerraformテンプレートを使って、VM-SeriesファイアウォールをGWLBと手動で統合することができます。テンプレートは、Palo Alto Networks GitHubリポジトリから利用することができます。

- VM-SeriesとGateway Load Balancerの手動統合

©2023 Palo Alto Networks, Inc.

- VM-SeriesとAWS Gateway Load Balancerのオートスケーリング

VM-SeriesとGateway Load Balancerの手動統合

VM-SeriesファイアウォールをAWSゲートウェイロードバランサーと手動で統合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。

- VM-SeriesとGateway Load Balancerの設定の有効化
- VM-SeriesとGateway Load Balancerの手動設定
- (任意) VPCエンドポイントとVM-Seriesインターフェイスの関連付け
- (任意) AWS での VM-Series のオーバーレイルーティングの有効化

VM-SeriesとGateway Load Balancerの設定の有効化

VM-SeriesファイアウォールとGWLBを設定する場合、まずGWLBエンドポイントによりファイアウォールにリダイレクトされたトラフィックが適切に処理されるように、VM-Seriesファイアウォールを有効にする必要があります。この機能はVM-SeriesファイアウォールCLI、VM-Seriesブートストラップパッケージ、またはAWSコンソール内のuser-dataフィールドを使って有効にすることができます。

VM-SeriesファイアウォールとGWLBのデプロイの要件を次に示します。

- PAN-OS 10.0.2以降
- VM-Series プラグイン 2.0.2 以降
- ファイアウォールの管理にPanoramaを使用する場合、Panorama 10.0.2以降

GWLBトラフィック検査を有効にして、サブインターフェイスをVPCエンドポイントと関連付けるために表なコマンドを、以下の表に示します。ブートストラップのinit-cfg.txtファイル、またはAWSコンソールのuser-dataフィールドでは、操作コマンドを利用できます。

ブートストラップパラメータ	CLIコマンド	説明
mgmt-interface-swap=enable	set system setting mgmt-interface-swap enable yes このコマンドの内容を反映するには、ファイアウォールを再起動する必要があります。	eth0とeth1をスワップします。eth0がデータインターフェイスになり、eth1が管理インターフェイスになります。
plugin-op-commands=aws-gwlb-inspect:enable	request plugins vm_series aws gwlb inspect enable <yes/no>	GWLBを追加するトラフィックの、VM-Seriesファイアウォールによる処理を有効にします。

©2023 Palo Alto Networks, Inc.

VM-SeriesとGateway Load Balancerの手動設定

AWS上のVM-Seriesファイアウォールを GWLBと手動で設定するには、次の作業を行ってください。

ブートストラップ中にユーザーデータを介して*VPC*エンドポイントをインターフェイスまたはサブインターフェイスに関連付け、*bootstrap.xml*ファイルにインターフェイス設定がない場合、ファイアウォールのブート後にインターフェイスを設定することができます。

STEP 1 | セキュリティVPCを設定します。セキュリティVPCの作成の詳細は、AWSのドキュメントを参照してください。

- 管理インターフェイス用とデータインターフェイス用の2つのサブネットを作成します。
- ファイアウォール管理用とデータ用の2つのセキュリティグループを作成します。
- 管理サブネットセキュリティグループは、管理アクセス用にhttpsとsshを許可する必要があります。
- データVPC内のセキュリティグループが、GENEVE-encapsulatedパケット（UDPポート6081）を許可していることを確認してください。
- デプロイ環境にトランジットゲートウェイと、VPC間を移動するトラフィックが存在している場合、セキュリティVPCアタッチメントでアプライアンスモードを有効にする必要があります。

*VM-Series*ファイアウォールは保護されていないプロトコルによるアクセスを許可していないため、*GWLB*のターゲットグループは、ヘルスチェックに*HTTP*を使用できません。代わりに、*HTTPS*や*TCP*などの他のプロトコルを使用してください。

©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series ファイアウォールを起動します。

1. EC2 Dashboard で、**Launch Instance**（インスタンスを起動）をクリックします。
2. VM-Series AMI を選択します。AMI の取得方法については、「AMI の取得」を参照してください。
3. EC2 インスタンスで VM-Series ファイアウォールを起動します。
   1. ファイアウォールに必要なリソースを割り当てるための **EC2 instance type**（**EC2** インスタンス タイプ）を選択してから **Next**（次へ）をクリックします。リソースの要件については、「VM-Series のシステム要件」を参照してください。
   2. セキュリティVPCを選択します。
   3. eth0にアタッチするデータサブネットを選択します。
   4. **Launch as an EBS-optimized instance**（**EBS**最適化が施されたインスタンスとして起動）を選択します。
   5. インターフェイススワップ後に管理インターフェイスとして動作する、eth1用の他のネットワークインターフェイスを追加します。インターフェイスをスワップするには、ENIが2つ以上必要です（eth0およびeth1）。
      - ネットワークインターフェイスの表示を展開し、**Add Device**（デバイスを追加）をクリックしてネットワークインターフェイスをもう一つ追加します。

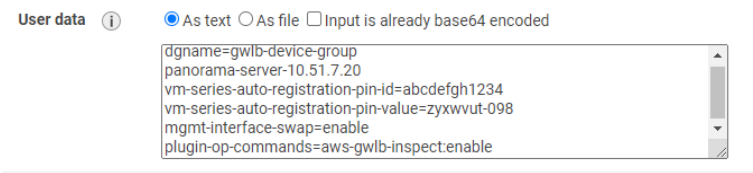
        VPCにサブネットが一つ以上あり、ローンチ時にENIを追加できることを確認してください。

        ENI が *1* つだけの状態でファイアウォールを起動すると：
        - インターフェイス スワップ コマンドによってファイアウォールがメンテナンス モードになります。
        - *2* つ目の *ENI* を追加したら、ファイアウォールを再起動しなければなりません。
      - Advanced Details（詳細）セクションを展開し、**User data**（ユーザーデータ）フィールドに、起動時にインターフェイスをスワップするためのテキストを入力します。

        `mgmt-interface-swap=enable`

        `plugin-op-commands=aws-gwlb-inspect:enable`

        *VM-Series*ファイアウォール上の特定のインターフェイスの*IP*アドレスに、ターゲットタイプを設定した場合、管理インターフェイススワップを有効にする必要はありません。

   6. デフォルトの **Storage**（ストレージ）設定を受け入れます。ファイアウォールはボリューム タイプ SSD（gp2）を使用します。

©2023 Palo Alto Networks, Inc.

7. プロンプトが表示されたら、セットアップに適した **SSD** オプションを選択します。
8. （任意）タギング。タグを追加して自分のメタデータを作成し、VM-Seriesファイアウォールを識別・グループ化します。たとえば、**Value**（値）に**Name**（名前）タグを追加すれば、このVM-Series ファイアウォールではENIインターフェイスがスワップされているということが分かりやすくなります。
9. eth0（データインターフェイス）の、データ**Security Group**（セキュリティグループ）を選択します。UDPポート6081のトラフィックを有効にします。

   ファイアウォールのヘルスチェックを有効にした場合、HTTPを使用することはできません。代わりに、HTTPSやTCPなどの他のプロトコルを使用してください。
10. **Review and Launch**（確認して起動）を選択します。選択内容が正しいことを確認し、**Launch**（起動）をクリックします。
11. 既存のキー ペアを選択するか、または新しく作成し、キー要求メッセージを受け入れます。

    このキー ペアは、ファイアウォールに初めてアクセスする場合に必要です。また、メンテナンス モードでファイアウォールにアクセスする場合にも必要になります。
12. プライベート キーをダウンロードして安全な場所に保存します。ファイル拡張子は `.pem` です。このキーは失うと再生成できません。

    VM-Series ファイアウォールの起動には 5 ～ 7 分かかります。進捗状況はEC2ダッシュボードで確認可能です。プロセスが完了すると、EC2 Dashboardの **Instances** [インスタンス] ページに VM-Seriesファイアウォールが表示されます。

STEP 3 | 管理セキュリティグループをeth1（管理インターフェイス）にアタッチします。sshとhttpsを許可します。詳細は、AWSのマニュアルを参照してください。

STEP 4 | Elastic IPアドレス（EIP）を作成し、ファイアウォールへの管理アクセス（eth1）に使用するENIに割り当てます。

1. **Elastic IPs**（**Elastic IP**）を選択し、**Allocate New Address**（新規アドレスを割り当て）をクリックします。
2. **EC2-VPC** を選択し、**Yes, Allocates**（割り当てる）をクリックします。
3. 新しく割り当てられた EIP を選択し、**Associate Addresss**（関連アドレス）をクリックします。
4. **Network Interface**（ネットワークインターフェイス） 選択し、**Private IP addresss**（プライベート**IP**アドレス）から管理インターフェイスに関連付けられたプライベートIPアドレスを選択し、**Yes, Associates**（関連付けを行う）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | ファイアウォールの新しい管理者パスワードを設定します。

*VM-Series*ファイアウォールの*CLI*では、一意な管理者用パスワードを設定しなければファイアウォールの*Web*インターフェイスにアクセスできません。*CLI*にログインするには、ファイアウォールをローンチするのに使用した秘密鍵が必要です。

1. EIPを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH で接続します。CLI にアクセスするには、先ほど使用または作成した秘密鍵が必要で、ユーザー名**admin**を使用する必要があります。

   SSH アクセス用に PuTTY を使用している場合、「.pem」形式を「.ppk」形式に変換する必要があります。https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.htmlを参照してください。
2. 以下のコマンドを入力してファイアウォールにログインします。

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*
3. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

   configure

   set mgt-config users admin password
4. アクティベートが必要なBYOLを所有している場合、ファイアウォールがPalo Alto Networksライセンスサーバーにできるようにし DNSサーバーのIPアドレスを設定してください。DNSサーバーのIPアドレスを設定する場合は以下のコマンドを実行してください。

   set deviceconfig system dns-setting servers primary *<ip_address>*
5. 以下のコマンドで変更内容をコミットします。

   commit
6. SSH セッションを終了します。

©2023 Palo Alto Networks, Inc.

STEP 6 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

VPC 内のアプリケーション サーバーで、ファイアウォールのデータプレーン ネットワーク インターフェイスをデフォルトゲートウェイとして定義します。

1. Web ブラウザからの安全な接続（https）を使用し、初期設定時に割り当てた EIP アドレスとパスワードを入力してログインします(https://<Elastic_IP address>)。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。
2. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
3. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーンを定義し、**OK** をクリックします。
   - **IPv4** タブで **DHCP Client**（**DHCP** クライアント）を選択します。

     DHCP を使用する場合は、**DHCP Clients**（**DHCP** クライアント）を選択します。AWS 管理コンソールで ENI に割り当てたプライベート IP アドレスが自動的に取得されます。
   - Advanced（高度）タブで、ファイアウォールがヘルスチェックを受け取れるように、管理プロファイルを作成します。
4. **Commit**（コミット）をクリックします。インターフェイスのリンク状態がアップになっていることを確認します 。

STEP 7 | トラフィックを許可/拒否するセキュリティポリシーを作成します。

*GWLB*と統合した場合、*VM-Series*はトラフィックをイントラゾーンとして取り扱うため、デフォルトのイントラゾーンルールがすべてのトラフィックを許可します。ベストプラクティスとして、他のセキュリティポリシールールに一致しないトラフィックに対する拒否アクションを利用して、デフォルトのイントラゾーンルールに優先する設定を行ってください。

1. ファイアウォールの Web インターフェイスで **Policies**（ポリシー） > **Security**（セキュリティ） を選択します。
2. **Add**（追加）をクリックし、セキュリティゾーンを指定して、ネットワーク経由のトラフィックを制限して監査するために実行するアプリケーションとロギング オプションを指定します。

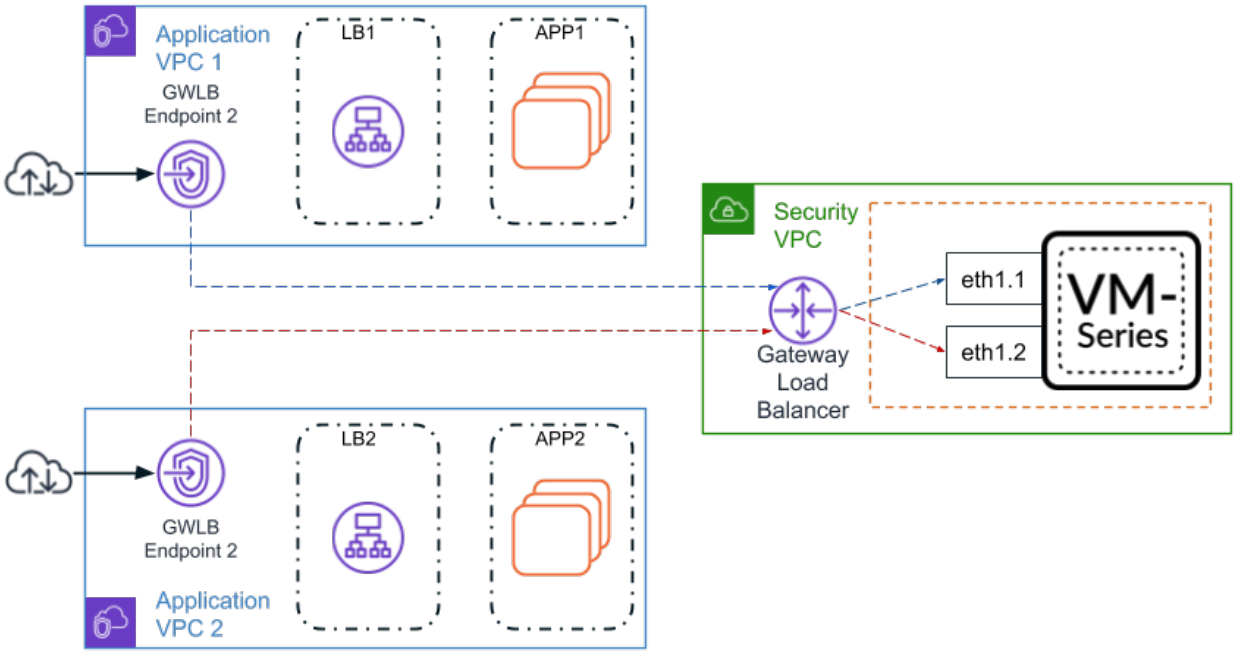
STEP 8 | ファイアウォールへの変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

VPCエンドポイントとVM-Seriesインターフェイスの関連付け

1つまたは複数のVPCエンドポイントを、VM-Seriesファイアウォールの1つのインターフェイスまたはサブインターフェイスと関連付けることができます。単一のVPC内のすべてのエンドポイントを、ファイアウォール上の同じサブインターフェイスに関連付けることで、一貫したポリシーを適用することができます。デプロイ環境に、重複するIPアドレスを持つVPCが存在している場合、異なるVPC内のエンドポイントを異なるサブインターフェイスに関連付けて、差別化したポリシーの施行を行うことができます。

*VPCをインターフェイスまたはサブインターフェイスに関連付けることは、VM-Seriesファイアウォールを*GWLB*と統合する際に必須ではありません。*



インターフェイスを設定し、VPCをファイアウォールインターフェイスに関連付けるには、次の方法を利用できます。

- `bootstrap.xml`ファイル内のインターフェイス設定、および関連するコマンドを、`init-cfg.txt`ファイルまたはAWSユーザーデータの一部として含める。
- ファイアウォールのデプロイが完了した後、手動でインターフェイスを設定して、ファイアウォールCLIを使ってVPCとインターフェイスを関連付ける。

複数のVPCエンドポイントを、VM-Seriesファイアウォール上の単一のインターフェイスに関連付けることができます。ただし、各VPCエンドポイントを個別に関連付ける必要があります。たとえば、VPCエンドポイント1とVPCエンドポイント2を、サブインターフェイスethernet1/1.2に関連付けるには、各VPCエンドポイントに対して個別に関連付け用コマンドを実行する必要があります。

VPCをインターフェイスと関連付けるコマンドを、以下の表に示します。操作コマンドを`init-cfg.txt`ファイルまたはAWSユーザーデータに含めることができます。

©2023 Palo Alto Networks, Inc.

ブートストラップパラメータ	CLIコマンド	説明
plugin-op-commands= aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>	request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>	VPCエンドポイントをファイアウォール上のインターフェイスまたはサブインターフェイスと関連付けます。指定したインターフェイスは、セキュリティゾーンに割り当てられます。
—	request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>	VPCエンドポイントとファイアウォール上のインターフェイスまたはサブインターフェイスとの関連付けを解除します。指定したインターフェイスは、セキュリティゾーンに割り当てられます。
—	show plugins vm_series aws gwlb	GWLBデプロイ環境と関連しているファイアウォールの動作状態を表示します。ファイアウォール設定は表示されません。 たとえば、存在していないインターフェイスへの関連付けを設定した場合、関連付け自体は設定されますが、動作状態の一部とはなりません。そのため、それは表示されません。

ブートストラップinit-cfg.txtファイルまたはAWSユーザーデータを使ってVPC endpointを関連付ける場合、複数のインターフェイスまたはサブインターフェイスを一緒に記述することができます。すべてのコマンドは、単一業にカンマ区切り形式で指定する必要があります。スペースを入れることはできません。次に例を示します。

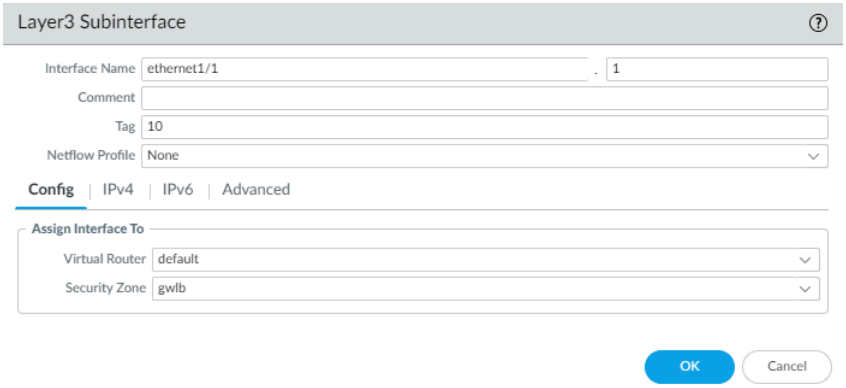
```
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-
vpce:vpce-0913731043b5c0ebc@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-08207ccb4cb23a1de@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-07b66cca88821d6e1@ethernet1/1.2,aws-gwlb-associate-
vpce:vpce-0a9a583fdb928492b@ethernet1/1.3
```

トラフィックを区別するためにサブインターフェイスを使用する場合、各VPCに対するサブインターフェイスを作成し、それをVPCに関連付けます。

©2023 Palo Alto Networks, Inc.

STEP 1 | サブインターフェイスを設定します。

1. ファイアウォール インターフェイスにログインします。
2. **Network**（ネットワーク） > **Interface**（インターフェイス）を選択します。
3. **ethernet1/1**を強調表示して、**Add Subinterface**（サブインターフェイスの追加）をクリックします。
4. 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）を入力します。
5. サブインターフェイスの**VLAN Tag**（**VLAN**タグ）（1～4,094）を入力します。このフィールドは必須ですが、VLANは使用されません。
6. **Virtual Router**（仮想ルーター）を選択します。
7. **Security Zone**（セキュリティ ゾーン）を選択します。
8. **IPv4**タブで、**Type**（タイプ）を**DHCP Client**（**DHCP**クライアント）に設定します。
9. **OK**をクリックします。
10. 各VPCエンドポイントに対して、このコマンドを繰り返します。



STEP 2 | インターフェイスをVPCエンドポイントと関連付けます。

1. ファイアウォール CLI へのログイン
2. 以下のコマンドを実行します。

   request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>

   以下に例を示します。

   request plugins vm_series aws gwlb associate vpc-endpoint vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4

   *VPC*エンドポイント*ID*は、*AWS*コンソールから探すことができます。

3. 各インターフェイスとVPCエンドポイントの関連付けに対して、このコマンドを繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 3 | インターフェイスからVPCエンドポイントへの関連付けを確認します。

```
show plugins vm_series aws gwlb
```

```
GWLB enabled:      True
Overlay Routing:  False
------------------------------------------------------------
VPC endpoint                    Interface
------------------------------------------------------------
vpce-0aeb1a919bd4ae609           ethernet1/1.1
vpce-0294375bfe413f04a           ethernet1/1.2
```

STEP 4 | 必要に応じて、次のコマンドを使ってVPCエンドポイントとインターフェイスの関連付けを解除することができます。

```
request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>
```

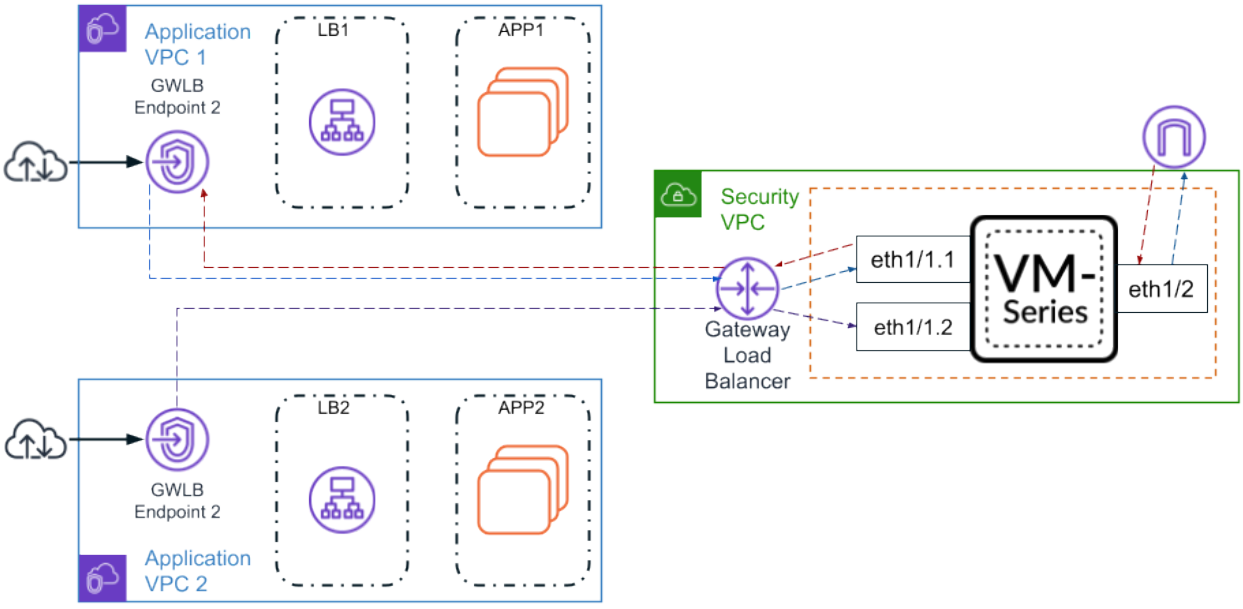
AWS での VM-Series のオーバーレイルーティングの有効化

オーバーレイルーティングには、*PAN-OS 10.0.5* 以降が必要です。

VM-Series ファイアウォール統合でオーバーレイルーティングを使用すると、AWS GWLB で 2 ゾーンポリシーを使用して、AWS 環境から発信される（出る）トラフィックを検査できます。これにより、パケットは、入力したインターフェースとは異なるインターフェースを介して VM-Series ファイアウォールを離れることができます。

オーバーレイルーティングが設定されている場合、ファイアウォールはパケットの内部ヘッダーでレイヤー 3 ルートルックアップを実行できます。宛先が入力インターフェースと同じである場合、パケットは通常どおりに送信されます。セッション内の今後のすべてのパケットは、オーバーレイルーティングが有効になっていないかのように vwire として扱われます。パケットがアウトバウンド宛先に送信される場合、ファイアウォールはパケットのカプセル化を解除し、パケットを IGW または NAT ゲートウェイに転送します。パケットが戻ると、ファイアウォールはカプセル化を再適用します。

©2023 Palo Alto Networks, Inc.



オーバーレイルーティングを有効にするには、次の手順を使用します。

STEP 1 | 開始する前に、信頼インターフェースと非信頼インターフェースに対してそれぞれ異なるサブネットを必ず作成してください。

STEP 2 | VM-SeriesとGateway Load Balancerの手動設定.

STEP 3 | （任意）VPCエンドポイントとVM-Seriesインターフェイスの関連付けを行います。

STEP 4 | オーバーレイルーティング CLI コマンドを使用します。AWS user-data または init-cfg.txt ブートストラップファイルにオーバーレイルーティング op-command を組み入れた場合、この CLI コ マンドは必要ありません。

1. ファイアウォールのコマンドラインインターフェースにログインします。
2. 以下のコマンドを実行します。

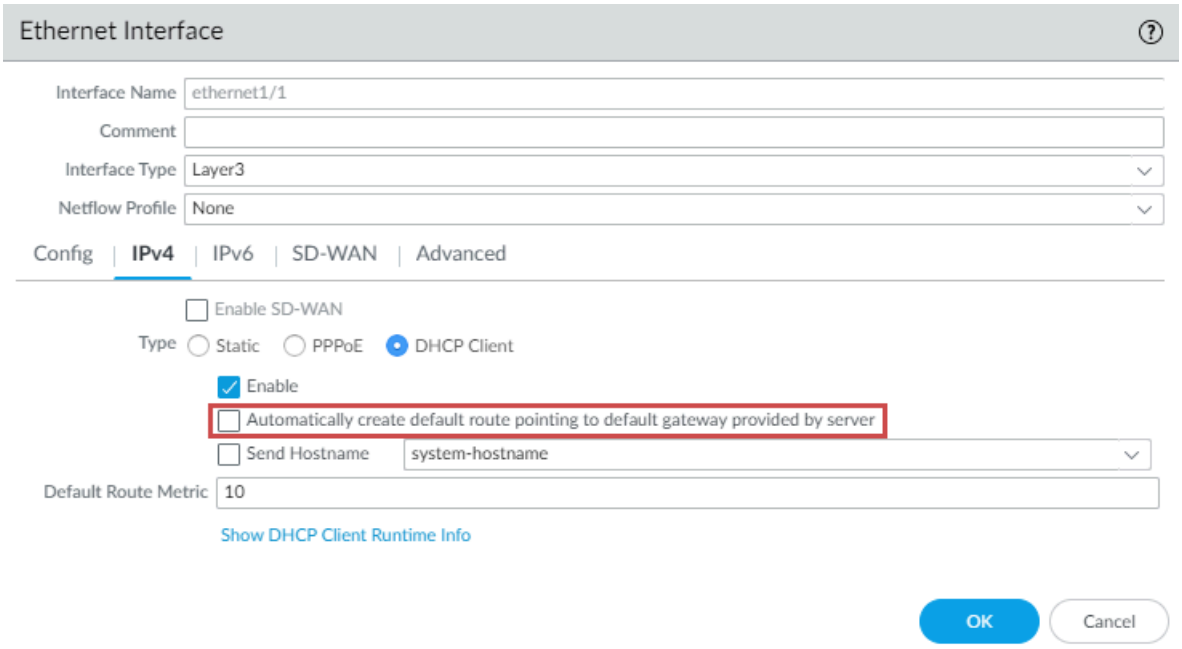
```
request plugins vm_series aws gwlb overlay-routing enable yes
```

STEP 5 | ファイアウォール インターフェイスにログインします。

©2023 Palo Alto Networks, Inc.

STEP 6 | 信頼（入力）インターフェース上の[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すデフォルトルートを自動的に作成する]を無効にしていることを確認します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択します。
2. 信頼インターフェースをクリックしてから、[IPv4] タブをクリックします。
3. [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すデフォルトルートを自動的に作成する]のチェックを外します。
4. ［OK］をクリックします。



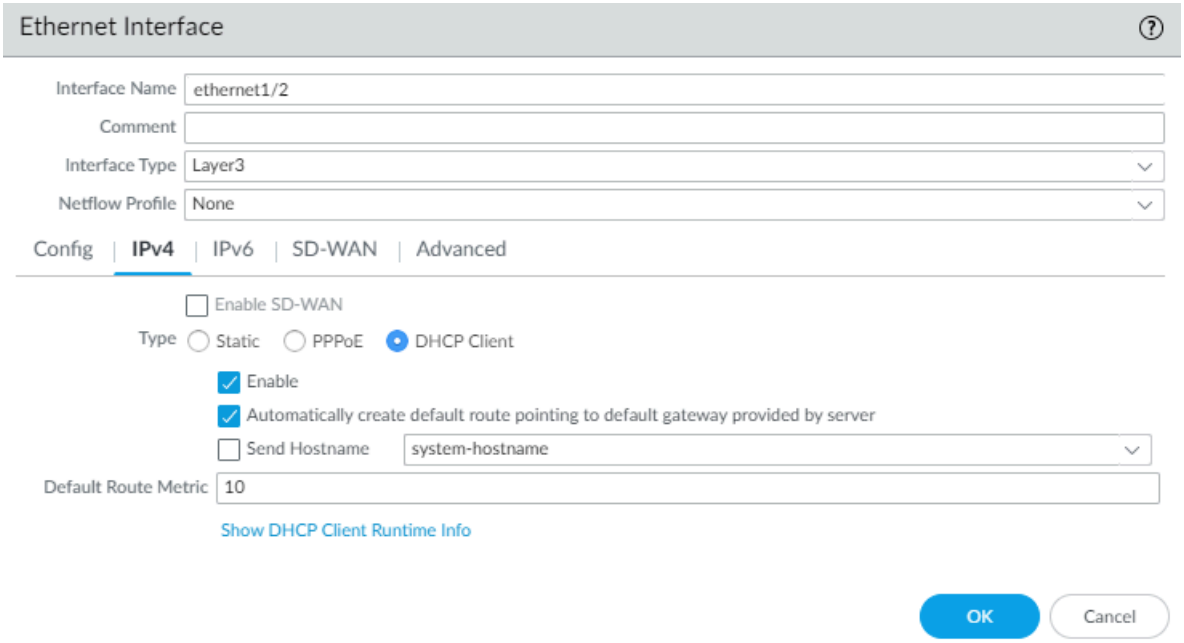
STEP 7 | インターフェースイーサネット 1/2 を設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択します。
2. レイヤー **3** の インターフェースタイプ を選択します。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。このゾーンは、アントラスト

©2023 Palo Alto Networks, Inc.

ゾーンとして機能し、セキュリティ VPC からアウトバウンドトラフィックを送信します。VM-Series-untrust などの新しいゾーンを定義し、[**OK**]をクリックします。

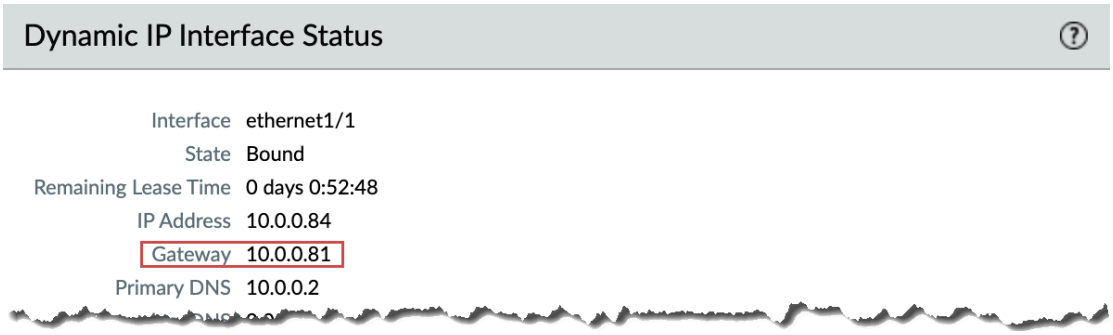
4. **IPv4** タブで **DHCP Client**（**DHCP** クライアント）を選択します。
5. [サーバーによって提供されるデフォルトゲートウェイを指すデフォルトルートを自動的に作成する]を選択します。
6. **OK** をクリックします。



©2023 Palo Alto Networks, Inc.

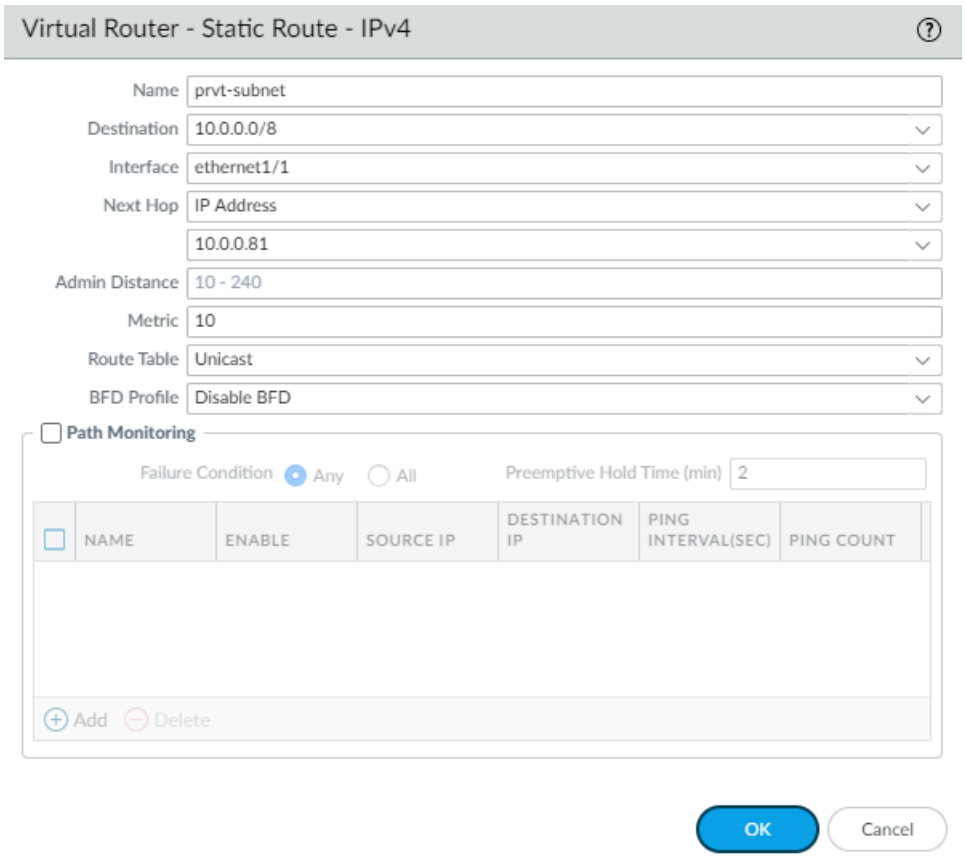
STEP 8 | 仮想ルーターを構成します。

1. ネットワーク > 仮想ルーター > 追加を選択します。
2. 仮想システムの分かりやすい 名前を入力します。
3. [インターフェース]で、イーサネット 1/1 と、イーサネット 1/1 およびイーサネット 1/2 の下のすべてのサブインターフェースを追加します。
4. スタティック ルート > 追加をクリックします。
   1. スタティック ルートのわかりやすい名前を入力します。
   2. 宛先として、アプリケーション VPC サブネットのプライベート IP アドレスを入力します。
   3. [インターフェース]ドロップダウンから信頼（入力）インターフェースを選択します。
   4. [ネクストホップ]で、IP アドレスを選択し、信頼インターフェースのゲートウェイの IP アドレスを入力します。ゲートウェイの IP アドレスは、ネットワーク > インターフェース > イーサネット > 動的 **DHCP** クライアントにあります。



5. **OK** をクリックします。

©2023 Palo Alto Networks, Inc.



5. スタティック ルートがデプロイメント内のすべてのアプリケーション VPC に到達できることを確認します。いくつかの大規模な集約ルート（すべての RFC1918 をカバー）またはアプリケーション VPC 固有のルートを作成できます。サブインターフェースを使用する場合は、サブインターフェースに戻るルーティングをする必要はありません。出力チェックは、一致するサブインターフェイスではなく、一致するインターフェイスのみを検索します。
6. **OK** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 9 | イーサネット 1/2 を出力するトラフィックの NAT ポリシーを作成します。

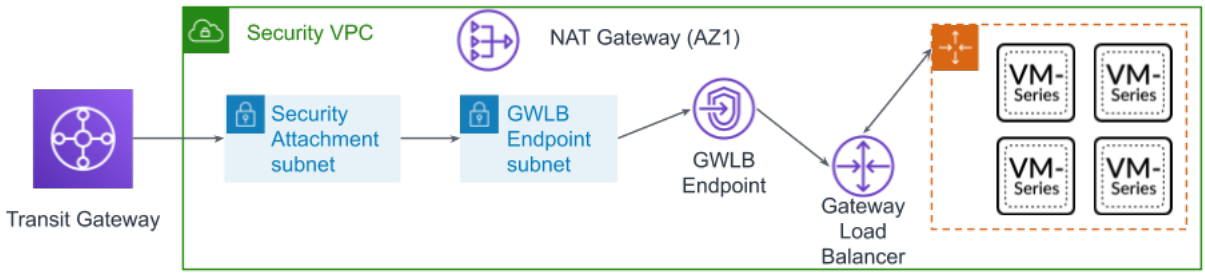
1. ポリシー > **NAT** > 追加を選択します。
2. NAT ポリシー ルールの分かりやすい名前を入力します。
3. [**NAT** タイプ]ドロップダウンから**ipv4**を選択します。
4. [元のパケット]タブで、送信元ゾーンを任意に設定し、宛先ゾーンを信頼できない（出力）ゾーンに設定します。
5. [変換されたパケット]タブで、次のパラメータを設定します。
   - 変換タイプ:ダイナミック IP およびポート
   - アドレスタイプ ：インターフェイス アドレス
   - インターフェイス:ドロップダウンから信頼できない（出力）ポートを選択します。
   - IPアドレス:まったくない
6. **OK** をクリックします。

STEP 10 | 変更を **Commit (コミット)**します。

VM-SeriesとAWS Gateway Load Balancerのオートスケーリング

AWS 用 Palo Alto Networks オートスケーリング テンプレートは、AWS 内にデプロイされたアプリケーションを保護するために、GWLBを使ってVM-Series ファイアウォールの統合と設定を行うために役立ちます。アプリケーション ワークロード リソースの需要の急増に対応できるように、このテンプレートは AWS のスケーラビリティ機能を使用して、AWS 内にデプロイされている VM-Series ファイアウォールを自動的かつ個別にスケーリングします。

これらのテンプレートはコミュニティがサポートしています。



このソリューションは、セキュリティVPCテンプレートとアプリケーションテンプレートを提供しています。セキュリティVPCテンプレートは、VM-Seriesファイアウォールオートスケーリンググループ、GWLB、GWLBE、GWLBEサブネット、セキュリティアタッチメントサブネット、および各アベイラビリティゾーンのNATゲートウェイをデプロイします。CloudFormationテンプレートをPalo Alto Networks GitHubリポジトリからダウンロードします。

AWS GWLBと統合するための、VM-Seriesオートスケーリングテンプレートには、次のビルディングブロックが含まれています。

©2023 Palo Alto Networks, Inc.

構成要素	概要
PANコンポーネント	• 10.0.2以降が動作しているPanorama • PAN-OS 10.0.2以降 • PanoramaにVM-Seriesプラグイン2.0.2以降がインストールされている
ファイアウォール テンプレート （コミュニティでサポートされるテンプレート）	選択したアベイラビリティゾーン（AZ）の数に応じて、`firewall-new-vpc-v3.0.template` は次のものをデプロイします: テンプレートは、最大 *4* つの *AZ* をサポートします。 • Lambda管理用サブネット、トランジットゲートウェイアタッチメント、GWLBエンドポイント、およびNATゲートウェイとTrustサブネット。 • 各サブネットに対するルートテーブル • トランジットゲートウェイアタッチメントとルートテーブル • NATおよびインターネットゲートウェイ • AZあたり1つのVM-Seriesファイアウォールを持つオートスケーリンググループ。 • 各AZに1つのGWLBとGWLBエンドポイント。 ファイアウォールテンプレートのVPC CIDRは、/23より大きくなければなりません。 プロダクション環境にはさまざまなバリエーションが存在しています。これには、サブネット、可用性ゾーン、ルート テーブル、およびセキュリティ グループなどの特定のコンポーネント数が含まれますが、これに限定されるものではありません。`firewall-new-vpc-v3.0.template`は、新しい VPC 内にデプロイする必要があります。 *AWS* 用*VM-Series*オートスケーリングテンプレートは、トランジットゲートウェイまたは*Panorama*をデプロイしません。*firewall-new-vpc-v3.0.template*を起動する前に、トランジットゲートウェイと*Panorama*をデプロイする必要があります。
アプリケーション テンプレート （コミュニティでサポートされるテンプレート）	選択したアベイラビリティゾーン（AZ）の数に応じて、`panw-aws-app-v3.0.template`は次のものをデプロイします: テンプレートは、最大 *4* つの *AZ* をサポートします。 • Lambda用サブネット、トランジットゲートウェイアタッチメント、GWLBエンドポイント、アプリケーションロードバランサー。

©2023 Palo Alto Networks, Inc.

構成要素	概要
	• 各サブネットのルートテーブル、およびインバウンド トラフィックをGWLBエンドポイントに送信するための、インターネットゲートウェイに関連付けられているインバウンドルートテーブル。 • アプリケーションロードバランサー1台 • インターネットゲートウェイ1台 • AZあたり1つのUbuntuインスタンスを持つオートスケーリンググループ。 アプリケーションテンプレートのVPC CIDRは、/23より大きくなければなりません。 アプリケーションテンプレートは、セキュリティテンプレートを検証するための例として使用することを想定しています。
Lambda 関数	AWS Lambda は、堅牢なイベント駆動型の自動化を提供します。複雑なオーケストレーション ソフトウェアは必要ありません。上記の行に記載されているコンポーネントのデプロイに加えて、`firewall-new-vpc-v3.0.template`は次の処理を実行します。 • ファイアウォールの起動時または終了時に、インターフェイス（ENI）を追加または削除する。 • スタックの削除またはインスタンスの終了時に、関連リソースをすべて削除する。 • スケール イン イベント発生時に、Panorama のマネージド デバイスとしてファイアウォールを削除する。 • スケールインイベントの結果、ファイアウォールが終了した場合、ライセンスを非アクティブ化する。 • トランジットゲートウェイを定期的に監視して、新しいアタッチメントやデタッチメントがないかどうかを確認し、必要に応じてセキュリティVPC内のルートテーブルを更新します。
ブートストラップ ファイル GitHub リポジトリで提供されている bootstrap.xml ファイルは、テストと評価のみを目的としています。実稼働デプロ	このソリューションでは、init-cfg.txt ファイルと bootstrap.xml ファイルが必要です。これは、VM-Series ファイアウォールがトラフィック処理用の基本設定を持つようにするためです。 • `init-cfg.txt` ファイルには、ファイアウォールのプライマリ インターフェイス（eth0）でデータプレーン トラフィックを受信できるようにする mgmt-interface-swap 操作コマンドが含まれます。オートスケーリング ソリューションでは、データプレーンと管理インターフェイスをスワップし、GWLBがWebトラフィックをVM-Seriesファイアウォールのオートスケーリング層に転送できるようにする必要があります。 • `bootstrap.xml` ファイルにより、ファイアウォール ネットワーク インターフェイスの基本接続が使用可能になり、テンプレート起動時に入

©2023 Palo Alto Networks, Inc.

構成要素	概要
イメントでは、起動前に bootstrap.xml 内のサンプル認証情報を変更する必要があります。	力されたスタック名に一致する AWS CloudWatch 名前空間にファイアウォールが接続できるようになります。

*AWS*からこれらのテンプレートを削除する必要がある場合、まずアプリケーションテンプレートを先に削除してください。ファイアウォールテンプレートの削除を試みると、削除が失敗してしまいます。

- テンプレートを起動する前に
- ファイアウォールテンプレートの起動
- アプリケーション テンプレートの起動

テンプレートを起動する前に

VM-Seriesファイアウォールのオートスケーリンググループと AWS GWLBを統合するためにテンプレートを起動する前に、次の作業を完了する必要があります。

STEP 1 | 作業を開始する前に、以下のことを確認してください。

- デプロイメントで必要となる数のファイアウォールをサポートしているバンドルの認証コードを取得した。この認証コードを `authcodes` という名前（拡張子なし）のテキスト ファイルに保存し、この `authcodes` ファイルをブートストラップ パッケージの `/license` フォルダに保管する必要があります。
- VM-Series Gateway Load Balancer テンプレートの起動に必要なファイルを GitHub リポジトリからダウンロードした。

©2023 Palo Alto Networks, Inc.

- Transit Gateway（トランジットゲートウェイ）を作成します。このトランジットゲートウェイは、セキュリティおよびアプリケーションVPCを接続します。
  - トランジットゲートウェイIDは、後でテンプレートをデプロイする際に必要になりますので、メモしておいてください。
  - East-Westおよびアウトバウンドトラフィックを保護するために、セキュリティアタッチメントを指す0.0.0.0/0ルートをアプリケーションアタッチメントのルートテーブルに追加する必要があります。
  - **Default route table association**（デフォルトのルートテーブル関連付け）および**Default route table propagation**（デフォルトのルートテーブル伝達）が無効になっていることを確認します。
- ファイアウォールおよびアプリケーションテンプレートの、推奨するVPC CIDRは/23以上です。

ゲートウェイ*GWLB*のターゲットグループは、*VM-Series*のファイアウォールが安全でないプロトコルでのアクセスを許可しないため、ヘルスチェックに*HTTP*を使用できません。代わりに*HTTPS*または*TCP*を使用してください。

STEP 2 | 10.0.2が動作しているPanoramaをデプロイして、次の項目を設定します。

Panoramaは、AWSパブリックIPアドレスを許可する必要があります。VM-Seriesファイアウォールは、テンプレートで作成されたNATゲートウェイの外部IPアドレスを使ってPanoramaにアクセスします。

STEP 3 | PanoramaにVM-Seriesプラグインをダウンロードし、インストールします。

1. **Panorama** > **Plugins**（プラグイン） を選択し、**Check Now**（今すぐチェック） を使用して新しいプラグインパッケージを検索します。VM Series のプラグイン名は `vm_series` です。
2. プラグインのリリースノートを参照して、どのバージョンが有用なアップグレードを提供しているかを判断します。
3. プラグインのバージョンを選択し、Action (アクション) 列にある **Download (**ダウンロード**)** を選択します。
4. Action (アクション) 列の **Install (**インストール**)** をクリックします。インストールが完了すると Panorama から警告が表示されます。
5. プラグインを表示するには、**Device** > **VM-Series (**デバイス **VM-Series)** を選択します。

©2023 Palo Alto Networks, Inc.

STEP 4 | テンプレートを設定します。

1. Panorama Web インターフェイスにログインします。
2. **Panorama** > **Templates**（テンプレート）を選択し、**Add**（追加）をクリックします。
   1. 分かりやすい **Name**（名前）を入力します。
   2. **OK**をクリックします。
3. 仮想ルーターの設定
   1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)**を選択します。。
   2. 先ほど**Template**（テンプレート）ドロップダウンから作成したテンプレートを選択していることを確認します。
   3. **[**追加**]** をクリックします。
   4. 次の形式を使用して仮想ルーターに名前を付けます。VR-<テンプスタック名>。
   5. 仮想ルーターでECMPを有効にします。
   6. **OK**をクリックします。
4. インターフェイスを設定して、ゾーンを作成します。
   1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** を選択して **Add Interface**（インターフェイスの追加） をクリックします。
   2. **Slot 1**（スロット**1**）を選択します。
   3. **Interface Type**（インターフェイス タイプ）を Layer 3（レイヤー 3）に設定します。
   4. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウンから **New Zone**（新規ゾーン）を選択します。Zone [ゾーン] ダイアログの **Name**[名前] で「Internet」などの名前を付けて新しいゾーンを定義し、**OK** をクリックします。
   5. **Virtual Router**（仮想ルーター）ドロップダウンで、先ほど作成した仮想ルーターを選択します。
   6. **IPv4**を選択して、**DHCP Client**（**DHCP**クライアント）をクリックします。
   7. **OK**をクリックします。
5. ヘルスチェックをサポートするために、上記で作成したインターフェースで HTTPS を使用できる管理プロファイル を作成します。
   1. **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**)** の順に選択し、**Add (**追加**)** をクリックします。
   2. インターフェイスが管理トラフィックに対して許可するプロトコルを選択します。**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS**、あるいは**SNMP**のいずれかです。

      これらのプロトコルは平文で送信を行い、安全ではないため ***HTTP*** または ***Telnet*** を有効にしないでください。
6. インターフェイス管理プロファイルをインターフェイスに割り当てます。

©2023 Palo Alto Networks, Inc.

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** を選択し、インターフェイスのタイプ（**Ethernet (イーサネット)**、**VLAN**、**Loopback (ループバック)**、あるいは **Tunnel (トンネル)**）を選択し、さらにインターフェイスを選択します。
2. **Advanced (詳細)** > **Other info (その他の情報)** を選択し、先ほど追加した Interface (インターフェイス) **Management Profile (管理プロファイル)** を選択します。
3. **OK**をクリックします。

7. DNSサーバーとFQDNの更新時間を設定します。
   1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択して、編集アイコンをクリックします。
   2. **Primary DNS Server**（プライマリ**DNS**サーバー）を169.254.169.253に設定します。これは、AWS DNSアドレスです。
   3. **Minimum FQDN Refresh Time**（最低**FQDN**更新時間）を60秒に設定します。
   4. **OK**をクリックします。
8. 変更を **Commit**（コミット）します。次のステップに進む前に、この作業を行う必要があります。
9. 管理者を作成します。
   1. **Device**（デバイス） > **Administrators**（管理者）を選択します。
   2. **Name**（名前）に**pandemo** と入力します。
   3. **Password**（パスワード）に**demopassword**を設定し、**Confirm**（確認）を選択します。
   4. **OK**をクリックします。
10. 変更を **Commit (コミット)** します。

STEP 5 | テンプレート スタックを設定して、テンプレートをテンプレート スタックに追加します。

1. **Panorama** > **Templates**（テンプレート）の順に選択し、**Add Stack**（スタックを追加）します。
2. スタックの識別に使用する一意の **Name**（名前）を入力します。
3. [追加] をクリックして、テンプレートを選択します。
4. **OK** をクリックしてテンプレート スタックを保存します。

©2023 Palo Alto Networks, Inc.

STEP 6 | **Device Group**（デバイスグループ）を作成します。

1. **Panorama** > **Device Groups**（デバイス グループ）の順に選択します。
2. 先ほど**Device Group**（デバイスグループ）ドロップダウンから作成したデバイスグループを選択していることを確認します。
3. **[追加]** をクリックします。
4. 分かりやすい **Name**（名前）を入力します。
5. **OK**をクリックします。
6. すべてのセキュリティプレルールを追加して許可します。
   1. **Policies**（ポリシー） > **Security**（セキュリティ） > **PreRules**（プレルール）を選択し、**Add**（追加）をクリックします。
   2. 分かりやすい **Name**（名前）を入力します。
   3. **Source**（ソース）、**User**（ユーザー）、**Destination**（宛先）、**Application**（アプリケーション）、および**Service/URL Category**（サービス/**URL**カテゴリ）下で、任意の項目を選択します。
   4. **Actions**（アクション）で、**Allow**（許可）を選択します。
   5. **OK**をクリックします。
7. 変更を **Commit (コミット)** します。

STEP 7 | ファイアウォールのライセンスアクティブ化解除APIキーを、Panoramaに追加します。

1. カスタマー サポート ポータルにログインします。
2. **Assets**（アセット） > **Licensing API**（ライセンシング **API**）を選択します。
3. API キーをコピーします。
4. CLI を使用して、前のステップでコピーした API キーをインストールします。

   request license api-key set key *<key>*

STEP 8 | Panoramaをデプロイしたら、AWSのPanoramaセキュリティグループの説明に従って、次のポートを開く必要があります。

- ポート **443**（**HTTPS**）– ファイアウォール テンプレートを初めてデプロイした場合は、HTTPS を開いたままにしておきます。これにより、Lambda が Panorama に接続できます。

  ポート 443 を保護するには、接続を許可する接続元 IP アドレス範囲と、NAT ゲートウェイに割り当てられている EIP を指定します。デプロイ環境内のNATゲートウェイ数は、設定した可用性ゾーン数によって異なります。 () AWS で NAT ゲートウェイの EIP を確認するには、**VPC** > **NAT Gateways**（**NAT** ゲートウェイ）の順に移動します。HTTPS のセキュリティ グループの EIP 情報をメモします。

  また、スタックの削除後にファイアウォールライセンスのリリースをPanoramaに許可するには、ファイアウォールテンプレートをデプロイしたリージョンのCIDR範囲からのトラフィックを許可する必要があります。リージョンのCIDRは、このリンクから探すことができます。

©2023 Palo Alto Networks, Inc.

- ポート **3978** – ポート 3978 はすべての IP アドレスからのトラフィックを受信できる必要があります。

ファイアウォールテンプレートの起動

このワークフローは、ファイアウォールテンプレートのデプロイ方法について説明しています。

STEP 1 | **init-cfg.txt** ファイルを変更して **/config** フォルダにアップロードした。

Panorama を使用して VM-Series ファイアウォールをブートストラップするため、**init-cfg.txt** ファイルを次のように変更する必要があります。**bootstrap.xml** ファイルは不要です。

さきほどinit-cfg.txtファイルで作成した、デバイスグループとテンプレート名を使用していることを確認してください。

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=
vm-auth-key=
panorama-server=
panorama-server-2=
tplname=
dgname=
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
plugin-op-commands=aws-gwlb-inspect:enable
```

init-cfg.txtファイルには、**plugin-op-commands=aws-gwlb-inspect:enable**を指定している必要があります。これは、VM-SeriesファイアウォールをGWLBと統合する場合に必要になります。

VM-Seriesファイアウォールインスタンスのデプロイ時に、デバイス証明書を自動的にインストールするために、init-cfg.txtファイルにデバイス証明書自動登録PINを追加する必要があります。

STEP 2 | ライセンスの認証コードを ブートストラップパッケージの**/license**フォルダに追加します。

1. テキスト エディタを使用して **authcodes** という名前（拡張子なし）の新しいファイルを作成します。
2. BYOL ライセンスの認証コードをこのファイルに追加し、保存します。認証コードはバンドルを表し、デプロイメントで必要な数のファイアウォールをサポートしていなければなりません。バンドルではなく個別の認証コードを使用すると、ファイアウォールは、ファイルに含まれている最初の認証コードのライセンス キーのみを検索します。

©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォール テンプレート（`panw-aws.zip`）とアプリケーション テンプレート（`app.zip`）の Lambda コードを S3 バケットにアップロードします。ブートストラッピングに使用する S3 バケットを使用できます。

アプリケーション スタックがファイアウォールとは異なるアカウントで管理されている場合は、ファイアウォール テンプレートと同じ AWS リージョンに、アプリケーション アカウントを使用して別の s3 バケットを作成し、`app.zip` をその s3 バケットにコピーします。

STEP 4 | ファイアウォール テンプレートを選択します。

1. AWS 管理コンソールで **CloudFormation** > **Create Stack**（スタックを作成）の順に選択します。
2. **Upload**（アップロード）を選択して、サブデータシートをAmazon S3にアップロードして、ファイアウォールと同じ VPC または別の VPC に、テンプレートが起動するリソースをデプロイします。Open（開く）とNext（次へ）をクリックします。
3. スタック名を指定します。スタック名により、このテンプレートを使用してデプロイされるすべてのリソースを識別できます。

STEP 5 | **Name**（名前）に分かりやすいスタック名を入力します。名前は28文字以下にする必要があります

STEP 6 | VPC のパラメータを設定します。

1. アベイラビリティゾーン数を入力し、アベイラビリティゾーンのドロップダウンから、リージョンを選択します。
2. VM-Series ファイアウォールの AMI ID を検索して入力します。AMI ID が、使用する AWS リージョン、PAN-OS バージョン、および BYOL または PAYG ライセンス オプションと一致していることを確認します。詳細は、「Amazonマシンイメージ IDの取得」を参照してください。
3. ファイアウォールを起動するための EC2 の **Key pair**（キー ペア）を（ドロップダウンリストから）選択します。ファイアウォールにログインするには、このキー ペアの名前と、関連付けられている秘密鍵を入力しなければなりません。
4. デバッグ ログを有効化する場合は、**Enable Debug Log**（デバッグ ログを有効化）で**Yes**（はい）を選択します。デバッグ ログを有効化すると、デプロイメントの問題のトラブルシューティングに役立つ詳細なログが生成されます。これらのログはスタック名を使用して生成され、AWS CloudWatch に保存されます。

デフォルトでは、テンプレートは VM-Series ファイアウォールのスケーリング パラメータとして CPU 利用率を使用します。 カスタム PAN-OS メトリックは、すでに指定してあるスタック名に対応した CloudWatch 名前空間で自動的に公開されます。

STEP 7 | Amazon S3 バケット（1 つまたは複数）の名前を指定します。

1. ブートストラップ パッケージが格納された S3 バケットの名前を入力します。

   ブートストラップ バケットが適切にセットアップされていないか、またはバケット名を正しく入力しないとブートストラップ プロセスが失敗し、ファイアウォールにログインできなくなります。ロード バランサーのヘルス チェックも失敗します。
2. panw-aws.zip ファイルが格納された S3 バケットの名前を入力します。前述したように、ブートストラップと Lambda コードに 1 つの S3 バケットを使用できます。

©2023 Palo Alto Networks, Inc.

STEP 8 | ファイアウォールと Panorama への API アクセスを有効化するキーを指定します。

1. ファイアウォールが API コールを認証するために使用するキーを入力します。デフォルトのキーはサンプル ファイルに基づいており、テストおよび評価にのみ使用してます。本番のデプロイメントでは、API コール専用に別の PAN-OS ログインを作成して、関連するキーを生成しなければなりません。
2. AWS Lambda が Panorama に対して API コールを発行できるようにするための API キーを入力します。本番のデプロイメントでは、API コール専用に別のログインを作成して、関連するキーを生成しなければなりません。

STEP 9 | AWSアカウント番号を追加します。GWLBに接続しているVPCのデプロイに使用した、アカウント番号を指定する必要があります。これらの値はカンマ区切り形式で追加します。テンプレートのデプロイ後に、その他のアカウント番号を追加することができます。

アカウント番号を探すには、AWSコンソールの右上にあるAWSユーザー名をクリックして、**My Security Credentials**（私のセキュリティ認証情報）を選択します。

STEP 10 | トランジットゲートウェイIDを入力します。トランジットゲートウェイは、East-Westおよびアウトバウンド トラフィックを保護するため必要になります。トランジットゲートウェイIDを入力しない場合、テンプレートはインバウンド トラフィックのみをGWLBに統合されたファイアウォールで検査するものと判断します。

STEP 11 | セキュリティVPCのCIDRを入力します。

STEP 12 | テンプレート設定を確認し、テンプレートを起動します。

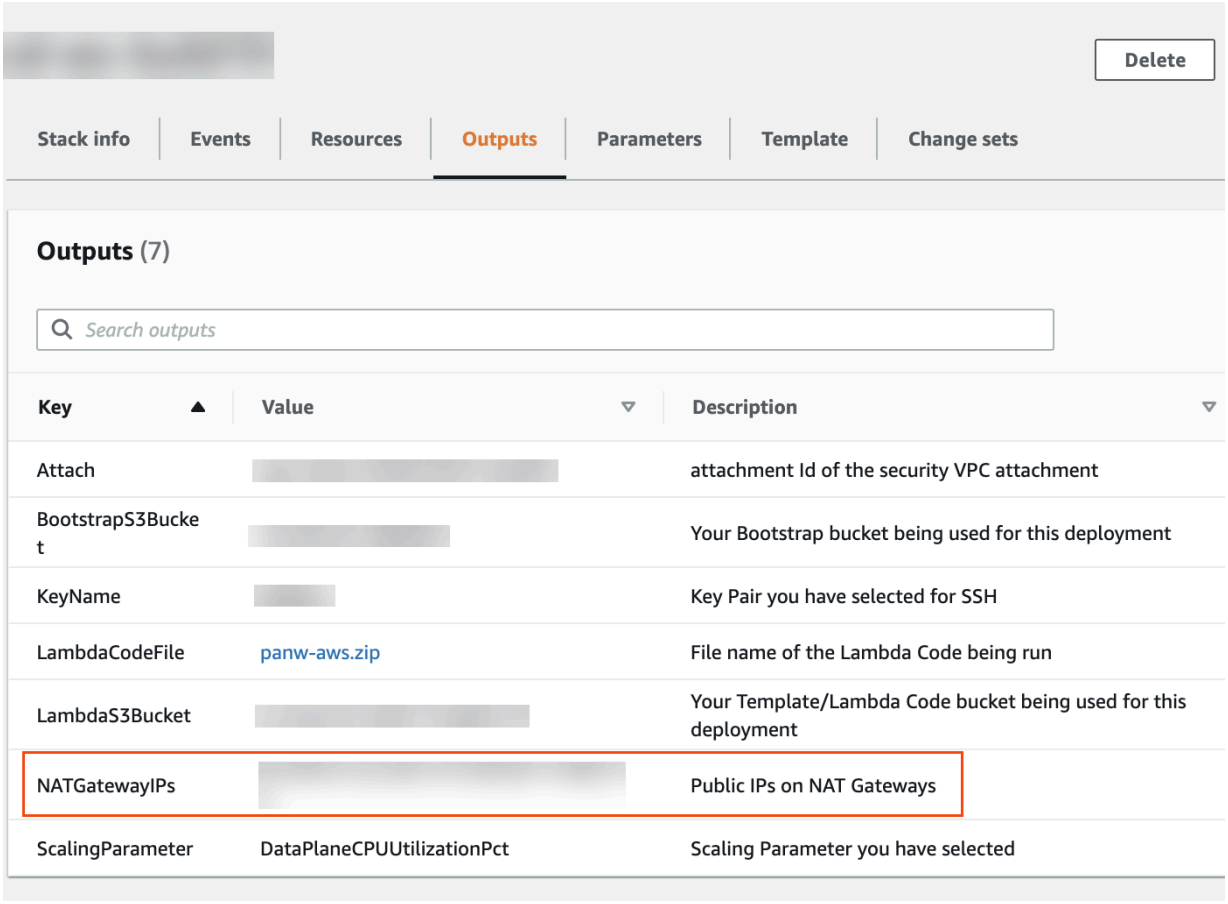
1. **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（このテンプレートによって **AWS CloudFormation** が **IAM** リソースが作成される可能性があることを理解しています）を選択します。
2. **Create**（作成）をクリックしてテンプレートを起動します。CREATE_IN_PROGRESS イベントが表示されます。
3. デプロイメントが成功すると、ステータスが CREATE_COMPLETE に変わります。

STEP 13 | テンプレートが必要なリソースをすべて起動したことを確認します。

STEP 14 | Panorama アプライアンスがデプロイされているセキュリティグループで NAT ゲートウェイの IP アドレスを許可するルールを作成します。これは、ファイアウォールが Panorama

©2023 Palo Alto Networks, Inc.

に接続できるようにするために必要です。NAT ゲートウェイの IP アドレスのリストは、CFT セキュリティスタックの出力にあります。



©2023 Palo Alto Networks, Inc.

1. AWS VPC コンソールにアクセスします。
2. ナビゲーションペインで[セキュリティグループ]を選択します。
3. Panorama がデプロイされているセキュリティを選択します。
4. アクション > 受信ルールの編集 > ルールの追加を選択します。
5. ポート範囲 3978 のカスタム TCP ルールの NAT ゲートウェイ IP アドレスを許可するルールを追加します。
6. [ルールの保存]をクリックします。

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	

アプリケーション テンプレートの起動

アプリケーションテンプレートを起動するには、次の作業を行ってください。

STEP 1 | アプリケーション テンプレートを起動する S3 バケットを作成します。

- クロス アカウント デプロイメントの場合は新しいバケットを作成します。
- アカウントが 1 つの場合は、新しいバケットを作成するか、または以前に作成した S3 バケットを使用できます（すべての処理に 1 つのバケットを使用できます）。

STEP 2 | app.zip ファイルを S3 バケットにアップロードします。

STEP 3 | 起動するアプリケーション起動テンプレートを選択します。

1. AWS 管理コンソールで、**CloudFormation** > **CreateStack** を選択します。
2. Upload a template to Amazon S3（Amazon S3 にテンプレートをアップロード）を選択し、ファイアウォールと同じ VPC または別の VPC に、テンプレートが起動するリソースをデプロイします。**Open**（開く）と**Next**（次へ）をクリックします。
3. スタック名を指定します。スタック名により、このテンプレートを使用してデプロイされるすべてのリソースを識別できます。

STEP 4 | Select list of AZ（可用性ゾーンのリストの選択）で、セットアップがまたがる可用性ゾーン（AZ）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 5 | 分かりやすい **VPC Name**（**VPC**名）を入力します。

STEP 6 | Lambda のパラメータを設定します。

1. app.zip が格納されている S3 バケットの名前を入力します。
2. ZIP ファイルの名前を入力します。

STEP 7 | このテンプレートが起動した、Ubuntu WebサーバーのEC2インスタンスを選択します。

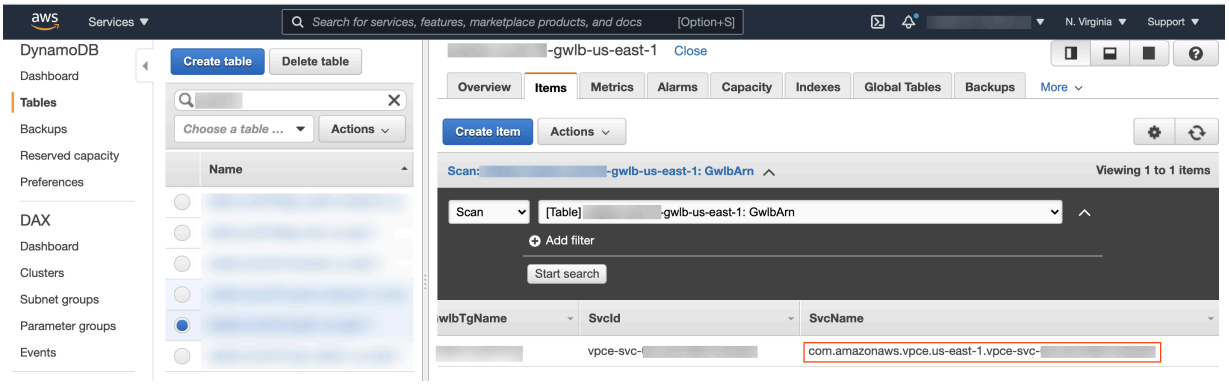
STEP 8 | Amazon EC2キーペアを入力します。

©2023 Palo Alto Networks, Inc.

STEP 9 | セキュリティVPC内のGWLBエンドポイントに対する、サービス設定（Service Name）の名前を入力します。

1. AWSコンソールの**Services**（サービス）ドロップダウンから、**DynamoDB**を選択します。
2. **Tables**（テーブル）を選択して、セキュリティVPCテーブルを探します。テーブル名は <スタック名> -gwlb- <リージョン> になります。例 — cft-deployment-gwlb-us-east-1.
3. Items（アイテム）タブをクリックして、Service Name（サービス名）をコピーします。
4. サービス名をアプリケーションテンプレート構成パラメータに貼り付けます。

©2023 Palo Alto Networks, Inc.



STEP 10 | トランジットゲートウェイIDを入力します。これは、ファイアウォールテンプレートのデプロイ前に作成したのと同じトランジットゲートウェイです。

STEP 11 | テンプレート設定を確認し、テンプレートを起動します。

©2023 Palo Alto Networks, Inc.

STEP 12 | アプリケーションのデプロイが完了したら、トランジットゲートウェイのルートテーブルにルートを追加して、east-westおよびアウトバウンドトラフィックの検査を有効にする必要があります。

1. AWS VPCコンソールにログインします。
2. **Transit Gateway Route Tables**（トランジットゲートウェイルートテーブル）を選択して、トランジットゲートウェイルートテーブルを選択します。このルートテーブルはテンプレートにより作成され、**<アプリケーションスタック名>-<リージョン>-PANWAppAttRt**と呼ばれます。
3. **Routes**（ルート）を選択して、**Create static route**（スタティックルートの作成）をクリックします。
4. **CIDR**フィールドに、0.0.0.0/0と入力します。
5. **Choose attachment**（添付ファイルの選択）ドロップダウンから、VM-Seriesファイアウォール VPC添付ファイルを選択します。
6. **Create static route**（スタティックルートの作成）をクリックします。

STEP 13 | （任意）アプリケーションテンプレートが作成したWebサーバーにアクセスするために、bastionホスト（jump box）を作成します。

1. アプリケーションVPC内に、外部に公開するサブネットを作成します。
2. ご自分のIPアドレスからインターネットゲートウェイへの、このサブネットへのルートを追加します。
3. パブリックIPアドレスを持つパブリックサブネットの、新しいEC2インスタンスを作成します。
4. ご自分のIPアドレスからのSSHを許可する、このEC2インスタンスのセキュリティグループを作成します。

©2023 Palo Alto Networks, Inc.

AWS における VM-Series ファイアウォールの高可用性設定

AWS の VM-Series ファイアウォールはアクティブ/パッシブ HA のみをサポートしています。Amazon Elastic Load Balancing（ELB）でデプロイした場合、 HA はサポートされません（この場合、ELB はフェイルオーバー機能を提供します）。

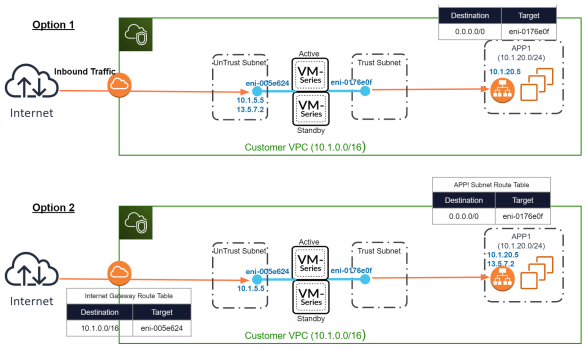
- AWS における HA の概要
- HA 用の IAM ロール
- HA リンク
- ハートビートポーリングおよび Hello メッセージ
- デバイス優先度およびプリエンプション
- HA タイマー
- セカンダリIPを使用したAWS上でのアクティブ/パッシブHA設定
- インターフェイス移動を使用したAWS上でのアクティブ/パッシブHA設定
- アクティブ/パッシブ HAをAWSに移行する

AWS における HA の概要

冗長性を確保するため、アクティブ/パッシブの高可用性（HA）ペアで VM-Series ファイアウォールを AWS にデプロイできます。アクティブ ピアは、まったく同一に構成されているパッシブ ピアと絶え間なく設定とセッション情報を同期させています。2 台のデバイス間のハートビート接続により、アクティブなデバイスがダウンした場合のフェイルオーバーが可能です。AWS上にHA状態のVM-Seriesファイアウォールをデプロイするには、Secondary IP Move（セカンダリIP移動）とDataplane Interface（ENI） Move（データプレーンインターフェイス移動）の2種類のオプションが存在しています。

インターネットに面するアプリケーションへのすべてのトラフィックがファイアウォールを通過するようにするには、2 種類のオプションがあります。VM-Series ファイアウォールの Untrust インターフェイス（上記のイラストの E1/2）上の、アプリケーションのパブリック IP アドレスを設定する、またはAWS 入口ルーティングを設定することができます。AWS 入口ルーティング機能により、ルート テーブルを AWS インターネット ゲートウェイと関連付け、アプリケーション トラフィックを VM-Seriesファイアウォール経由でリダイレクトするルーティング ルールを追加することができます。このリダイレクトにより、アプリケーションのエンドポイントを再設定しないでも、すべてのインターネット トラフィックがファイアウォールを通過します。

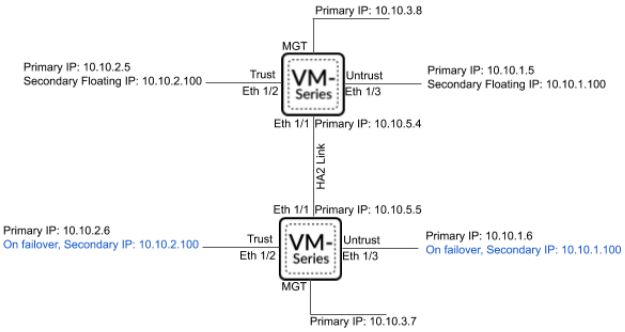
©2023 Palo Alto Networks, Inc.



Secondary IP Move（セカンダリIP移動）

アクティブピアがダウンした場合、パッシブピアがその障害を検出してアクティブに変化します。また、AWSインフラにAPI呼び出しを行い、設定されているセカンダリIPアドレスを、障害が発生したピアのデータプレーンインターフェイスから自己へと移動します。さらに、トラフィックがアクティブなファイアウォールインスタンスに送信されるように、AWSがルートテーブルを更新します。これらの2つの処理により、インバウンド トラフィックとアウトバウンド トラフィックセッションがフェイルオーバー後に復元されます。このオプションにより、DPDKを活用して、VM-Seriesファイアウォールインスタンスのパフォーマンスを改善し、インターフェイス移動HAよりもフェイルオーバー時間を向上しながら、インターフェイス移動が提供するすべての機能をサポートすることができます。

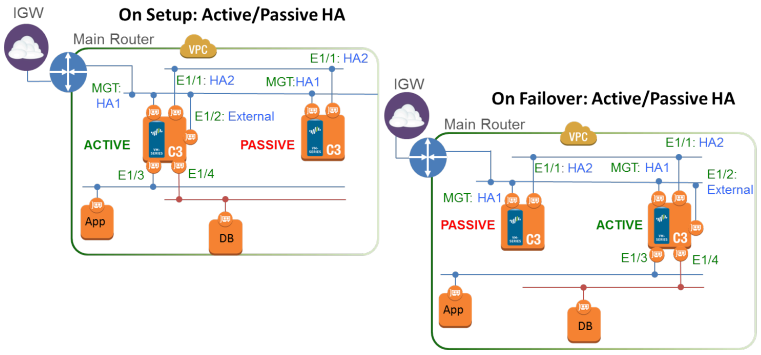
*Secondary IP Move HA*には、*VM-Series*プラグイン*2.0.1*以降が必要です。



Dataplane Interface Move（データプレーンインターフェイス移動）

アクティブピアがダウンした場合、パッシブピアがその障害を検出してアクティブになります。また、AWSインフラにAPI呼び出しを行い、すべてのデータプレーンインターフェイス（ENI）を、障害が発生したピアのデータプレーンインターフェイスから自己へと移動します。

©2023 Palo Alto Networks, Inc.



HA 用の IAM ロール

AWSでは、AWS自身が発行する認証情報を使用して、すべてのAPI要求が暗号化署名されている必要があります。HA ペアとしてデプロイされる VM-Series ファイアウォールの API パーミッションを有効化するには、ポリシーを作成し、そのポリシーをAWS アイデンティティおよびアクセス管理（IAM）サービス内にロールとして加える必要があります。このロールはローンチ時にVM-Seriesファイアウォールに加える必要があります。このポリシーにより、フェイルオーバーが発生した場合に、アクティブなピアからパッシブピアにインターフェイスまたはセカンダリIPアドレスを移動するために必要な、APIアクションを開始するためのアクセス許可がIAMロールに与えられます。

ポリシーを作成する詳細な方法は、AWS ドキュメントの「顧客管理ポリシーの作成」を参照してください。IAM ロールの作成、ロールを割り当てるアカウントやAWSサービスの定義、ロールを割り当てたアプリケーションが使用してよいAPIアクションやリソースの定義の詳細な手順については、AWSドキュメントの IAM Roles for Amazon EC2（Amazon EC2用のIAMロール）を参照してください。

AWS コンソールで設定される IAM ポリシーは、以下のアクションおよびリソースを利用する際は、最低でも許可の取得を必要とします。

*HA*を有効にするには、次の*IAM*アクション、アクセス許可、およびリソースが必要になります。*AWS Cloudwatch* モニタリングを有効にするには、

必要な *IAM* アクションに関するVM-Series ファイアウォールでの CloudWatch モニタリングの有効化を参照してください。

IAMアクション、アクセス許可、またはリソース	概要	インターフェイスの移動	セカンダリIP移動
AttachNetworkInterface	ENIをインスタンスに取り付ける際のアクセス許可。	✓	✓
DescribeNetworkInterfaces	インスタンスにインターフェイスを取り付けるためにENIパラメータを取得する許可。	✓	✓

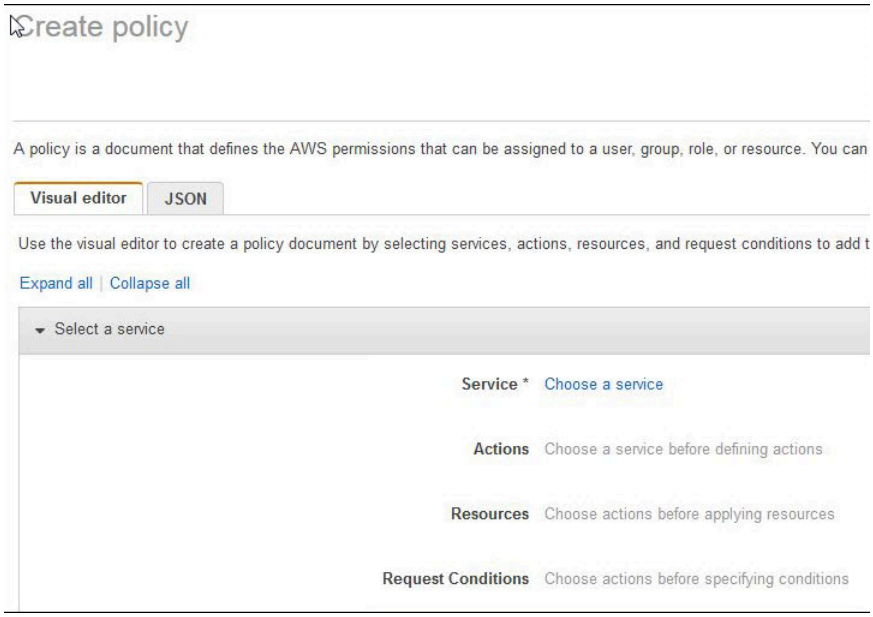
©2023 Palo Alto Networks, Inc.

IAMアクション、アクセス許可、またはリソース	概要	インターフェイスの移動	セカンダリIP移動
DetachNetworkInterface	ENIをEC2インスタンスから取り外す許可。	✓	✓
DescribeInstances	VPC内のEC2インスタンスについて情報を取得するための許可。	✓	✓
AssociateAddress	プライマリIPアドレスに関連するパブリックIPアドレスを、パッシブからアクティブインターフェイスに移動するための許可。		✓
AssignPrivateIpAddresses	セカンダリIPアドレスと関連するパブリックIPアドレスを、パッシブピア上のインターフェイスに割り当てるための許可。		✓
DescribeRouteTables	VM-Seriesファイアウォールインスタンスに関連するすべてのルートテーブルを取得するための許可。		✓
ReplaceRoute	AWSルートテーブルエントリを更新するための許可。		✓
GetPolicyVersion	AWSポリシーバージョン情報を取得するための許可。		✓
GetPolicy	AWSポリシー情報を取得するための許可。		✓
ListAttachedRolePolicies	指定したIAMロールにアタッチされている、すべての管理対象ポリシーのリストを取得するための許可。		✓
ListRolePolicies	指定したIAMロールに埋め込まれている、インラインポリシー名のリストを取得するための許可。		✓
GetRolePolicy	指定したIAMロールに埋め込まれている、特定のインラインポリシーを取得するための許可。		✓

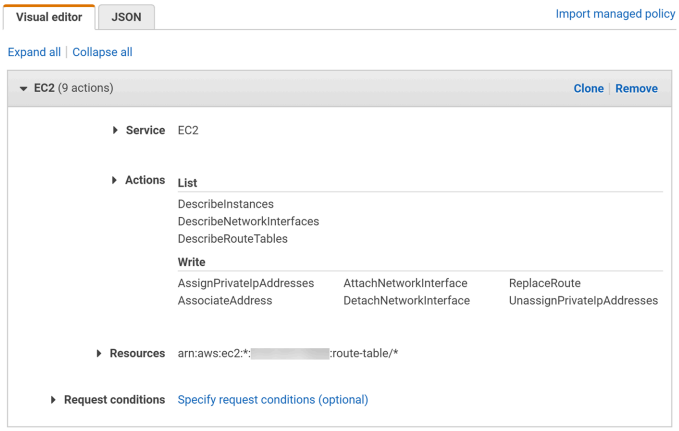
©2023 Palo Alto Networks, Inc.

IAMアクション、アクセス許可、またはリソース	概要	インターフェイスの移動	セカンダリIP移動
policy	IAMポリシーAmazonリソースネーム（ARN）にアクセスするための許可。		✓
role	IAMロールARNにアクセスするための許可。		✓
route-table	ルートテーブルAmazonリソースネーム（ARN）にアクセスして、フェイルオーバー時にそれを更新するための許可。		✓
ワイルドカード（*）	ARNフィールドで、*をワイルドカードとして使用します。	✓	✓

以下のスクリーンショットは、セカンダリIP HA用に、上記のIAMロールのアクセス管理設定を表しています。



 ©2023 Palo Alto Networks, Inc.



インターフェイス移動HA用に最低限必要なアクセス許可:
{"Version":"2012-10-17","Statement":
[{"Sid":"VisualEditor0","Effect":"Allow","Action":
["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstance
"*"}]}

セカンダリIP移動HA用に最低限必要なアクセス許可: {"Version":"2012-10-17","Statement":
[{"Sid":"VisualEditor0","Effect":"Allow","Action":
["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstances","ec2:DescribeNetworkInterfa
“ec2:AssignPrivateIpAddresses”,“ec2:AssociateAddress”,“ec2:DescribeRouteTables”],"Resource": "*"}
{"Sid":"VisualEditor1","Effect":"Allow","Action": "ec2:ReplaceRoute", "Resource": "arn:aws:ec2:*:*:route-
table/*"}]}

HA リンク

HA ペア内のデバイスは、HA リンクを使用してデータを同期し、状態情報を維持します。 AWS では、 VM-Series のファイアウォールは次のポートを使用します：

- **Control Link**（コントロールリンク） - HA1リンクは、Hello、ハートビート、HAの状態、ルーティング用の管理プレーンの同期、User-IDなどの情報交換に使用します。またこのリンクを使用して、アクティブ デバイスまたはパッシブ デバイスの設定変更をピア デバイスと同期します。

  管理ポートはHA1が使用します。クリアテキスト通信には TCP ポート 28769 と 28260、暗号化通信（SSH over TCP）にはポート 28 を使用します。

- **Data Link**（データリンク） - HA2リンクを使用して、セッションの同期、テーブルの転送、IPSec SA、およびARPテーブルをHAペアのデバイス間で同期します。HA2 リンクのデータ フローは（HA2 キープアライブを除き）常に単向性なので、データはアクティブ デバイスからパッシブ デバイスに流れます。

  ethernet1/1はHA2リンクとして割り当てる必要があります。これは、HA内のAWSにVM-Seriesファイアウォールをデプロイするために必要となります。HA データリンクは、IP（プロトコル番号 99）または UDP（ポート 29281）のいずれかを転送ポートとして使用するように設定できます。

AWSのVM-Seriesは、HA1あるいはHA2用のバックアップリンクをサポートしていません。

©2023 Palo Alto Networks, Inc.

ハートビートポーリングおよび Hello メッセージ

ファイアウォールでは、Hello メッセージおよびハートビートを使用して、ピアの応答状態と動作状態を確認します。設定した *Hello* 間隔で Hello メッセージがピアの一方からもう一方へ送信され、デバイスの状態を検証します。ハートビートは、コントロール リンクを介した HA ピアに対する ICMP ping の一種で、ピアがこの ping に応答することで、デバイスの接続および応答状態を証明します。フェイルオーバーをトリガーする HA タイマーの詳細は、「HA タイマー」を参照してください。（VM-Seriesファイアウォール用のHAタイマーは、PA-5200 Seriesファイアウォール用の同等のものと同じものです）

デバイス優先度およびプリエンプション

HA ペアのデバイスにデバイス優先度の値を割り当てることにより、フェイルオーバー発生時にどちらのデバイスにアクティブな役割を持たせて優先的にトラフィックを管理させるかを示すことができます。HA ペアの特定のデバイスを使用してアクティブにトラフィックを保護する必要がある場合、両方のファイアウォールでプリエンプティブ機能を有効にし、各デバイスに優先度の値を割り当てる必要があります。数値の小さい方のデバイス、つまり優先度の高いデバイスがアクティブ デバイスに指定され、ネットワーク上のすべてのトラフィックを管理します。もう一方のデバイスはパッシブ状態となり、アクティブ デバイスと設定情報や状態の情報を同期し、障害が発生した場合のアクティブ状態への移行に備えます。

デフォルトでは、ファイアウォールでプリエンプションが無効になっているため、両方のデバイスで有効にする必要があります。プリエンプティブの動作を有効にすると、優先度の高い（数値の低い方の）ファイアウォールが障害から回復した後に、そのファイアウォールをアクティブ ファイアウォールとして再開させることができます。プリエンプションが発生すると、そのイベントがシステム ログに記録されます。

*AWS*上の*VM-Series*ファイアウォール内の*HA*に対して、プリエンプションはお勧めいたしません。

HA タイマー

高可用性（HA）タイマーは、ファイアウォール障害の検出およびフェイルオーバーのトリガーに使用します。HAタイマーの設定時に煩雑さを軽減するため、以下3種類のプロファイルから選択できます。**Recommended** [推奨]、**Aggressive** [アグレッシブ] および **Advanced** [高度]これらのプロファイルでは、特定のファイアウォール プラットフォームに最適な HA タイマー値が自動入力され、HA の導入速度を高めることができます。

通常のフェイルオーバー タイマー設定には **Recommended**（推奨）プロファイルを使用し、高速なフェイルオーバー タイマー設定には **Aggressive**（アグレッシブ）プロファイルを使用します。**Advanced**（詳細）プロファイルでは、ネットワーク要件に合わせてタイマー値をカスタマイズできます。

©2023 Palo Alto Networks, Inc.

AWS 上の VM-Series の HA タイマー	推奨/アグレッシブプロファイルの初期設定値
プロモーションホールドタイム	2000/500 ms
Hello間隔	8000/8000 ms
ハートビート間隔	2000/1000 ms
最大フラップ数	3/3
プリエンプションホールドタイム	1/1 分
モニター障害時ホールドアップタイム	0/0 ms
追加のマスターホールドアップタイム	500/500 ms

セカンダリIPを使用したAWS上でのアクティブ/パッシブHA設定

新しいVM-Seriesファイアウォールを、セカンダリIPアドレスを持つHAペアとしてデプロイするには、次の作業を行ってください。

STEP 1 | HAペア向けにVM-Seriesファイアウォールをデプロイする前に、以下の事項を確認してください。

- 「VPCプランニングワークシート」を参照して、VM-Seriesファイアウォールに対するVPCの準備が完了していることを確認します。
- Secondary IP Move HAには、VM-Seriesプラグイン2.0.1以降が必要です。
- 両方のHAピアを同じAWSアベイラビリティゾーンの中にデプロイしている。

  VM-Seriesプラグイン2.0.3以降では、HAピアを異なる可用性ゾーンにデプロイすることができます。ただし、HAフェイルオーバーイベント時に、ルートテーブルは更新されますが、セカンダリIPは移動されません。このタイプのデプロイはお勧めしていません。
- IAM ロールを作成し、インスタンスのデプロイ時にそのロールを VM-Series ファイアウォールに割り当てている。
- アクティブおよびパッシブファイアウォールには、それぞれ最低4つのインターフェイス（管理インターフェイス、HA2インターフェイス、Untrustインターフェイス、Trustイン

©2023 Palo Alto Networks, Inc.

ターフェイス）が必要です。また、アクティブファイアウォール上のTrustおよびUntrustインターフェイスには、セカンダリIPアドレスが割り当てられている必要があります。

管理インターフェースは HA1 インターフェースとして使用する必要があります。

- ネットワーク コンポーネントとセキュリティ コンポーネントが適切に定義されていることを確認します。
  - インターネットとの通信を有効化します。デフォルトの VPC にはインターネット ゲートウェイが用意されていますので、デフォルトのサブネットで VM-Series ファイアウォールをインストールすれば、インターネットにはアクセスできる状態になっています。
  - サブネットを作成します。サブネットは、EC2 インスタンスを起動できる VPC に割り当てられた IP アドレス範囲のセグメントです。VM-Series ファイアウォールがインターネットにアクセスできるように設定するには、パブリック サブネットに属している必要があります。
  - ファイアウォールデータインターフェイスを含む、データセキュリティグループを作成します。また、すべてのトラフィック（0.0.0.0/0）を許可するようにセキュリティを設定し、ファイアウォールがセキュリティを採用するようにします。フェイルオーバー時に既存のセッションを維持するために、この作業が必要になります。
  - プライベート サブネットのルート テーブルにルートを追加し、該当する VPC 内のセブネットおよびセキュリティグループ全体に確実にトラフィックをルーティングできるようにします。
- ファイアウォールのブートストラップを行う場合、必要なブートストラップファイルを含むS3バケットを作成します。

©2023 Palo Alto Networks, Inc.

STEP 2 | AWS上にVM-Series ファイアウォールをデプロイします。

1. VM-SeriesファイアウォールにVM-Seriesプラグイン2.0.1以降がインストールされていない場合は、続行する前にプラグインをアップグレードしてください。
2. 各HAピアのHA2インターフェイスとして、ethernet 1/1を設定します。
   1. Amazon EC2コンソールを開きます。
   2. Network Interface（ネットワークインターフェイス）を選択して、次にネットワークインターフェイスを選択します。
   3. **Actions**（アクション） > **Manage IP Addresses**（**IP**アドレスの管理）を選択します。
   4. AWSにIPアドレスを動的に割り当てさせる場合はフィールドを空欄にします。そうでない場合は、VM-Seriesファイアウォールのサブネット範囲内にあるIPアドレスを入力します。
   5. **Yes**（はい）をクリックして、**Update**（更新）を選択します。
   6. アクション > ソース/宛先の変更を選択します。をオンにして [無効化] を選択します。
   7. この作業をセカンダリ（パッシブ）HAピアで繰り返します。
3. 最初の（アクティブ）ピア上のデータプレーンインターフェイスに、セカンダリIPアドレスを追加します。
   1. **Network Interface**（ネットワークインターフェイス）を選択して、次にネットワークインターフェイスを選択します。
   2. **Actions**（アクション） > **Manage IP Addresses**（**IP**アドレスの管理） > **IPv4 Addresses**（**IPv4**アドレス） > **Assign new IP**（新規**IP**の割り当て）を選択します。
   3. AWSにIPアドレスを動的に割り当てさせる場合はフィールドを空欄にします。そうでない場合は、VM-Seriesファイアウォールのサブネット範囲内にあるIPアドレスを入力します。
   4. **Yes**（はい）をクリックして、**Update**（更新）を選択します。
4. セカンダリエラスティック（パブリック）IPアドレスを、アクティブピアのUntrustインターフェイスと関連付けます。
   1. **Elastic IPs**（エラスティック**IP**）を選択し、次に関連付けるエラスティックIPアドレスを選択します。
   2. **Actions**（アクション） > **Associate Elastic IP**（エラスティック**IP**の関連付け）を選択します。
   3. **Resource Type**（リソースタイプ）で、**Network Interface**（ネットワークインターフェイス）を選択します。
   4. エラスティックIPアドレスを関連付けるネットワークインターフェイスを選択します。
   5. **Associate**（関連付け）をクリックします。
5. アウトバウンドトラフィック検査の場合、次のホップをファイアウォールのTrustインターフェイスに設定しているサブネットルートテーブルに、エントリを追加します。
   1. **VPC** > **Route Tables**（ルートテーブル）を選択します。

©2023 Palo Alto Networks, Inc.

2. サブネットルートテーブルを選択します。
3. **Actions**（アクション） > **Edit routes**（ルートの編集） > **Add route**（ルートの追加）を選択します。
4. **Destination**（宛先） CIDRブロックまたはIPアドレスを入力します。
5. **Target**（ターゲット）に、ファイアウォールTrustインターフェイスのネットワークインターフェイスを入力します。
6. **Save routes**（ルートの保存）をクリックします。

6. AWSイングレスルーティングを使用するには、ルートテーブルを作成して、それにインターネットゲートウェイを関連付けます。次に、アクティブファイアウォールのUntrustインターフェイスとして設定されせている次のホップを持つエントリを追加します。
   1. **Route Tables**（ルート テーブル） > **Create Route Table**（ルート テーブルを作成）を選択します。
   2. （任意）ルートテーブル用の、分かりやすい**Name tag**（名前タグ）を入力します。
   3. **Create**（作成）をクリックします。
   4. ルートテーブルをクリックして、**Actions**（アクション） > **Edit edge associations**（エッジ関連付けの編集）を選択します。
   5. **Internet gateways**（インターネットゲートウェイ）を選択して、VPCインターネットゲートウェイを選択します。
   6. **Save**（保存）をクリックします。
   7. ルートテーブルをクリックして、**Actions**（アクション） > **Edit routes**（ルートの編集）を選択します。
   8. **Target**（ターゲット）で、**Network Interface**（ネットワークインターフェイス）を選択して、アクティブファイアウォールのUntrustインターフェイスを選択します。
   9. **Save routes**（ルートの保存）をクリックします。

STEP 3 | ファイアウォール上でインターフェイスを設定します。HA2 データ リンクと、untrust および trust インターフェイス向けに最低 2 つの Layer 3 インターフェイスを設定する必要があります。最初の HA ピアでこのワークフローを完了して、次に 2 番目の HA ピアで手順を繰り返してください

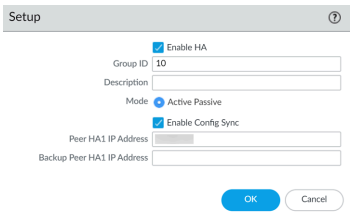
1. ファイアウォール インターフェイスにログインします。
2. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択して、untrust インターフェイスをクリックします。この例で、HA2 インターフェイスは 1/1、trust インターフェイスは ethernet 1/2、untrust インターフェイスは ethernet 1/3 になります。
3. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**HA**

©2023 Palo Alto Networks, Inc.

4. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「trust-zone」 など）を定義し、**OK** をクリックします。
   - **IPv4** タブで **DHCP Client**（**DHCP** クライアント）を選択します。
   - **Enable**（有効化）を選択します。
   - Untrustインターフェイスで、**Automatically create default route pointing to default gateway provided by server**（サーバーが提供する）を選択します。このオプションは、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。
   - ethernet 1/3に対して、この手順を繰り返します。
5. パッシブピアに対して上記の手順を繰り返します。

STEP 4 | HA を有効にします。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General** （全般）を選択します。
2. Setup（セットアップ）の設定を編集します。
3. パッシブ ピアのプライベート IP アドレスを **Peer HA1 IP address**（ピア **HA1 IP** アドレス）フィールドに入力します。
4. **OK** をクリックします。



5. **Election Settings**（選択設定）を編集して、アクティブピアにする特定のファイアウォールを指定します。アクティブファイアウォールの、**Device Priority**（デバイス優先度）の最低値を数値で入力します。両方のファイアウォールのデバイスプロファイル優先順位の値が同じ場合は、HA1 コントロールで最も小さい MAC アドレスのあるファイアウォールがアクティブ ファイアウォールになります。

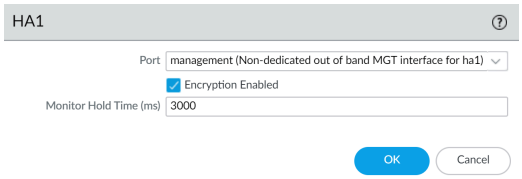
   プリエンプションを使用することはお勧めいたしません。

6. **OK** をクリックします。
7. 変更を **Commit (コミット)** します。
8. パッシブピアに対して上記の手順を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 5 | 管理ポートを使用するためにはコントロールリンク（HA1）を設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Control Link (HA1)（コントロール リンク（HA1））セクションを編集します。



2. （任意）ピア間の HA 通信を保護するには、**Encryption Enabled**（暗号化を有効にする）を選択します。暗号化を有効にする場合は、HAキーをデバイスからエクスポートして、ピア デバイスにインポートします。

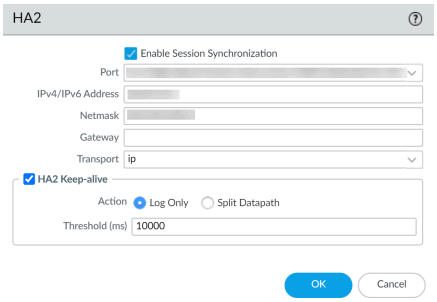
   1. **Device**（デバイス） > **Certificate Management**（証明書管理） > **Certificates**（証明書）を選択します。
   2. **Export HA key**（**HA** 鍵のエクスポート）を選択します。ピア デバイスがアクセスできるネットワーク上の場所に、HA キーを保存します。
   3. ピア デバイスで **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書）を選択します。次に、**Import HA key**（**HA** キーのインポート）を選択し、キーを保存した場所を検索して、そのキーをピア デバイスにインポートします。

STEP 6 | イーサネット 1/1 を使用するためにはデータリンク（HA2）を設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Data Link (HA2)（データ リンク（HA2））セクションを編集します。
2. **Port**（ポート）では ethernet1/1 を選択します。
3. ethernet1/1のIPアドレスを入力します。ここで入力するIPアドレスはEC2ダッシュボードのENIに割り当てられたものと同じものである必要があります。
4. **Netmask**（ネットマスク）を入力します。
5. HA1インターフェイスがそれぞれ別のサブネット上にある場合は、**Gateway**（ゲートウェイ）のIPアドレスを入力します。
6. **Transport**（トランスポート）には **IP** もしくは **UDP**を選択します。第3層トランスポートが必要な場合は**IP**を使用してください（IPプロトコルナンバー 99）。IPオプションで

©2023 Palo Alto Networks, Inc.

の場合と同じように、ファイアウォールにヘッダーのみでなくパケット全体からチェックサムを実行させたい場合は**UDP**を使用してください（UDPポート 29281）。



7. （任意）**HA2 Keep-alive**（**HA2** キープアライブ）パケットの **Threshold**（しきい値）を変更します。初期設定では、ピア間のHA2データリンクをモニタリングするため**HA2 Keep-alive**（**HA2** キープアライブ）が有効化されています。障害が発生し、このしきい値（初期設定は 10000ms です）を超えた場合は、定義されたアクションが実行されます。HA2 キープアライブに障害が発生すると、「critical」レベルのシステムログ メッセージが生成されます。

   HA2 keep-alive（***HA2*** キープアライブ）オプションは、*HA* ペアの両方のデバイス、または一方のデバイスに設定できます。一方のデバイスでこのオプションが有効化されている場合、キープアライブメッセージはそのデバイス単体から送信されます。

STEP 7 | 両方のファイアウォール上で HA の設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のファイアウォールで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブな HA ピアで、**Sync to peer**（ピアに同期）をクリックします。
3. ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **Passive**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。
   - アクティブ ファイアウォール: ローカル ファイアウォールの状態が **Active**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。
4. ファイアウォールのコマンドラインインターフェイスから、次のコマンドを実行します:
   - フェイルオーバーの準備状況を確認するには:

     ```
     show plugins vm_series aws ha state
     ```
   - セカンダリIPマッピングを表示するには:

     ```
     show plugins vm_series aws ha ips
     ```


©2023 Palo Alto Networks, Inc.

インターフェイス移動を使用したAWS上でのアクティブ/パッシブHA設定

インターフェイス移動モードを使ってアクティブ-パッシブHAを設定するには、次の作業を行ってください。

STEP 1 | 前提条件を満たしていることを確認してください。

AWS クラウドの HA に VM-Series ファイアウォールのペアを導入する場合、以下を確認してください。

- Ec2インスタンス上の VM-Series ファイアウォール起動時に作成した IAM ロールを選択します（すでに稼働中のインスタンスにロールを割り当てることはできません）。「HA 用の IAM ロール」を参照してください。

  IAM ロールの作成、ロールの引き継ぎが可能なアカウントまたは AWS サービスの定義、およびロールの引き継ぎ時にアプリケーションが使用できる API アクションおよびリソースの定義の詳細は、「AWS ドキュメント」を参照してください。

- インターフェイス移動HA環境内の、AWS上のVM-Seriesはファイアウォールでは、DPDKはサポートされていません。ファイアウォール上にVM-Seriesプラグイン2.0.1以降が存在している場合、DPDKを無効にする必要があります。

  DPDKを無効にしたら、ファイアウォールを再起動する必要があります。VM-Seriesファイアウォールのデプロイにブートストラップを使用する場合、**op-cmd-dpdk-pkt-io=off**を使ってinit-cfg.txtファイル内のDPDKを無効にすることで、ファイアウォールの再起動を回避することができます。詳細は、「AWS 上での VM-Series ファイアウォールのブートストラップ」を参照してください。

- HA ペアの内のアクティブなファイアウォールは最低で 3 つ（データプレーンインターフェイス 2 つ、管理インターフェイス 1 つ）のENIを保有している必要があります。

  HA ペアの内のパッシブなファイアウォールは、管理用 ENI を1 つ、データプレーンインターフェイスとして機能するENIを1 つ保有している必要があります。データプレーンインターフェイスは HA2 インターフェイスとして設定します。

  > *HA* ペアの内のパッシブなファイアウォールにはデータプレーンを追加しないでください。フェイルオーバーが発生すると、それまでアクティブであったファイアウォールのデータプレーンインターフェイスが取り外され、アクティブになった（それまでパッシブであった）ファイアウォールに取り付けられます。

- HA ピアは AWS の同じ可用性ゾーンに配置されている必要があります。

STEP 2 | AWS で VM-Series ファイアウォールを起動します。

STEP 3 | （VM-Seriesプラグイン2.0.1以降）アクティブおよびパッシブファイアウォール上で、DPDKを無効にします。デフォルトではDPDKが有効になっていますが、インターフェイス移動HAモードはDPDKをサポートしていないため、それを無効にしてPacket MMAPを有効にする必要があります。

1. パッシブファイアウォールCLIにログインします。

©2023 Palo Alto Networks, Inc.

2. 次のコマンドを使ってDPDKを無効にします。このコマンドを実行すると、ファイアウォールが再起動します。

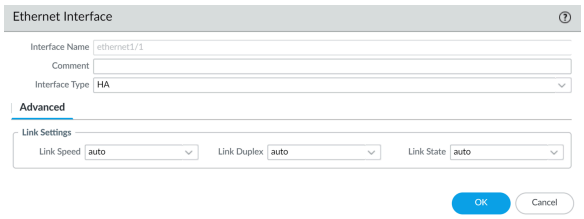
   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 4 | HA を有効にします。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Setup（セットアップ）セクションを編集します。
2. **Enable HA**（**HA** の有効化）を選択します。

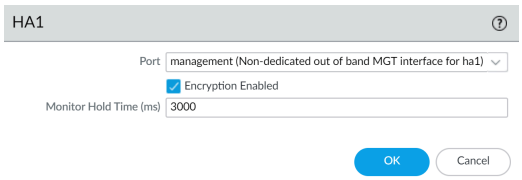
STEP 5 | イーサネット1/1をHAインターフェイスとして設定してください。HA2の通信にはこのインターフェイスを使用する必要があります。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス）を選択します。
2. イーサネット 1/1 が接続されていることを確認してください。
3. イーサネット 1/1 のリンクをクリックし、**Interface Type**（インターフェイス タイプ）を HA に設定します。



STEP 6 | 管理ポートを使用するためにはコントロールリンク（HA1）を設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Control Link (HA1)（コントロール リンク（HA1））セクションを編集します。



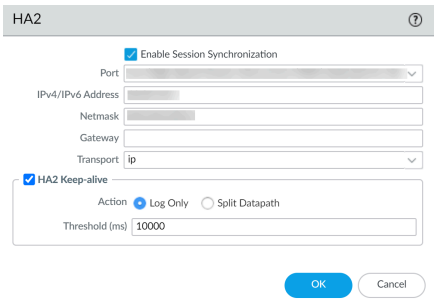
2. （任意）ピア間の HA 通信を保護するには、**Encryption Enabled**（暗号化を有効にする）を選択します。暗号化を有効にする場合は、HAキーをデバイスからエクスポートして、ピア デバイスにインポートします。

   1. **Device**（デバイス） > **Certificate Management**（証明書管理） > **Certificates**（証明書）を選択します。
   2. **Export HA key**（**HA** 鍵のエクスポート）を選択します。ピア デバイスがアクセスできるネットワーク上の場所に、HA キーを保存します。
   3. ピア デバイスで **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書）を選択します。次に、**Import HA key**（**HA** キーのインポート）を選択し、キーを保存した場所を検索して、そのキーをピア デバイスにインポートします。

©2023 Palo Alto Networks, Inc.

STEP 7 | イーサネット 1/1 を使用するためにはデータリンク（HA2）を設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Data Link (HA2)（データ リンク（HA2））セクションを編集します。
2. **Port**（ポート）では ethernet1/1 を選択します。
3. ethernet1/1のIPアドレスを入力します。ここで入力するIPアドレスはEC2ダッシュボードのENIに割り当てられたものと同じものである必要があります。
4. **Netmask**（ネットマスク）を入力します。
5. HA1インターフェイスがそれぞれ別のサブネット上にある場合は、**Gateway**（ゲートウェイ）のIPアドレスを入力します。
6. **Transport**（トランスポート）には **IP** もしくは **UDP**を選択します。第3層トランスポートが必要な場合は**IP**を使用してください（IPプロトコルナンバー 99）。IPオプションでの場合と同じように、ファイアウォールにヘッダーのみでなくパケット全体からチェックサムを実行させたい場合は**UDP**を使用してください（UDPポート 29281）。



7. （任意）**HA2 Keep-alive**（**HA2** キープアライブ）パケットの **Threshold**（しきい値）を変更します。初期設定では、ピア間のHA2データリンクをモニタリングするため**HA2 Keep-alive**（**HA2** キープアライブ）が有効化されています。障害が発生し、このしきい値（初期設定は 10000ms です）を超えた場合は、定義されたアクションが実行されます。HA2 キープアライブに障害が発生すると、「critical」レベルのシステムログ メッセージが生成されます。

> ***HA2 keep-alive***（***HA2*** キープアライブ）オプションは、*HA* ペアの両方のデバイス、または一方のデバイスに設定できます。一方のデバイスでこのオプションが有効化されている場合、キープアライブメッセージはそのデバイス単体から送信されます。

©2023 Palo Alto Networks, Inc.

STEP 8 | デバイス優先順位を設定してプリエンプションを有効にします。

特定のデバイスがアクティブ デバイスに指定されていることを確認する場合には、この設定を使用してください。詳細は、「デバイス優先度およびプリエンプション」を参照してください。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Election Settings（選択設定）セクションを編集します。
2. **Device Priority**（デバイス優先順位）に数値を設定します。優先度を高くするデバイスの数値を小さく設定する必要があります。

   両方のファイアウォールで優先度の値が同じ場合、*HA1* コントロール リンクで *MAC* アドレスが最も小さいファイアウォールがアクティブ デバイスとなります。
3. **Preemptive**（プリエンプティブ）を選択します。

   アクティブ デバイスとパッシブ デバイスの両方でプリエンプティブを有効にする必要があります。
4. フェイルオーバー タイマーを変更します。デフォルトで、HA タイマー プロファイルは、ほとんどの HA デプロイメントに適した **Recommended**（推奨）プロファイルに設定されています。

STEP 9 | （任意）フェイルオーバーがトリガーされるまでのウェイト タイムを変更します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Active/Passive Settings（アクティブ/パッシブ設定）を編集します。
2. **Monitor fail hold up time**（モニター障害時ホールドアップタイム）を 1 ～ 60 分の値に変更します（デフォルト値は 1 分）。ここで指定した時間が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間隔となります。この設定を利用して、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してください。

STEP 10 | HA ピアの IP アドレスを設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Setup（セットアップ）セクションを編集します。
2. ピアの HA1 ポートの IP アドレスを入力します。これは管理インターフェイス（イーサネット 0/0）に割り当てられた IP アドレスであるとともに、もう一方のファイアウォールの HA1 リンクでもあります。
3. **Group Id**（グループ **Id**）ナンバーを**1**ナンバーを 1 から 63 の間で設定します。この値は AWS の VM-Series ファイアウォールでは使用しませんが、空欄にしておくことができません。

STEP 11 | もう一方のピアの設定を行います。

HAピアでステップ3 ～ 9を繰り返します。

 ©2023 Palo Alto Networks, Inc.

STEP 12 | 両方のデバイスで設定が完了したら、アクティブ/パッシブ HA でそれらのデバイスがペアになっていることを確認します。

1. 両方のデバイスで **Dashboard**（ダッシュボード）にアクセスして、**High Availability**（高可用性）ウィジェットを表示します。
2. アクティブ デバイスで、**Sync to peer**（ピアと同期）リンクをクリックします。
3. 下に示すように、デバイスがペアになっていて同期されていることを確認します。
   - パッシブ デバイス:ローカル デバイスの状態が **passive**、設定が **synchronized** と表示されます。
   - アクティブ デバイス:ローカル デバイスの状態が **active**、設定が **synchronized** と表示されます。

STEP 13 | フェイルオーバーが正しく行われていることを確認してください。

1. HAモードを確認します。
   `show plugins vm_series aws ha failover-mode`
2. パケットのIOモードが、パケットMMAPに設定されていることを確認します。
   `show system setting dpdk-pkt-io`
3. HAピアをシャットダウンします。
   1. EC2 Dashboard で、**Instances**（インスタンス）を選択します。
   2. リストから VM-Series ファイアウォールを選択し、**Actions**（アクション） > **Stop**（停止）をクリックします。
4. パッシブピアがアクティブピアのロールを引き継ぎ、アクティブに切り替わったHAピアにデータプレーンインターフェイスが移動されたことを確認してください。

アクティブ/パッシブ HAをAWSに移行する

両方の高可用性モードがサポートされており、デプロイ環境の要件に応じて各モード間で移行することができます。interface-move（インターフェイス移動）モードはDPDKをサポートしていないため、移行を完了する前に、VM-Seriesファイアウォール上でそれを無効にする必要があります。DPDKを無効にする場合、VM-Seriesファイアウォールを再起動する必要があります。それにより、アクティブなファイアウォール上のトラフィックセッションが影響を受けます。

- AWS上のアクティブ/パッシブHAのセカンダリIPモードへの移行
- AWS上のアクティブ/パッシブHAのInterface Move（インターフェイス移動）モードへの移行

AWS上のアクティブ/パッシブHAのセカンダリIPモードへの移行

既存のVM-SeriesファイアウォールHAペアを、interface-move（インターフェイス移動）HAからセカンダリIP HAに移行するには、次の作業を行ってください。

*Secondary IP Move HA*には、*VM-Series*プラグイン*2.0.1*以降が必要です。

STEP 1 | パッシブHAピア上でVM-Series プラグインのアップグレードを行い、次にアクティブピア上で同様に作業を行います。

©2023 Palo Alto Networks, Inc.

STEP 2 | アクティブ ピア上のすべてのデータインターフェイスに対して、セカンダリ IPアドレスを作成します。

1. AWS EC2コンソールにログインします。
2. **Network Interface**（ネットワークインターフェイス）を選択して、次にネットワークインターフェイスを選択します。
3. **Actions**（アクション） > **Manage IP Addresses**（**IP**アドレスの管理） > **IPv4 Addresses**（**IPv4**アドレス） > **Assign new IP**（新規**IP**の割り当て）を選択します。
4. AWSにIPアドレスを動的に割り当てさせる場合はフィールドを空欄にします。そうでない場合は、VM-Seriesファイアウォールのサブネット範囲内にあるIPアドレスを入力します。
5. **Yes**（はい）をクリックして、**Update**（更新）を選択します。

STEP 3 | セカンダリエラスティック（パブリック）IPアドレスを、アクティブピアのUntrustインターフェイスと関連付けます。

1. AWS EC2コンソールにログインします。
2. **Elastic IPs**（エラスティック**IP**）を選択し、次に関連付けるエラスティックIPアドレスを選択します。
3. **Actions**（アクション） > **Associate Elastic IP**（エラスティック**IP**の関連付け）を選択します。
4. **Resource Type**（リソースタイプ）で、**Network Interface**（ネットワークインターフェイス）を選択します。
5. エラスティックIPアドレスを関連付けるネットワークインターフェイスを選択します。
6. **Associate**（関連付け）をクリックします。

STEP 4 | Trustインターフェイスを含むサブネットを指すルートテーブルを作成します。

1. **Route Tables**（ルート テーブル） > **Create Route Table**（ルート テーブルを作成）を選択します。
2. （任意）ルートテーブル用の、分かりやすい**Name tag**（名前タグ）を入力します。
3. **VPC**を選択します。
4. **Create**（作成）をクリックします。
5. **Subnet Associations**（サブネットの関連付け） > **Edit subnet associations**（サブネットの関連付けの編集）を選択します。
6. Trustインターフェイスを含むサブネットの**Associate**（関連付け）チェックボックスを選択します。
7. **Save**（保存）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | セカンダリIP移動HAへの移行に必要な追加のアクションとアクセス許可でIAMロールを更新します。

IAMアクション、アクセス許可、またはリソース	説明
AssociateAddress	プライマリIPアドレスに関連するパブリックIPアドレスを、パッシブからアクティブインターフェイスに移動するための許可。
AssignPrivateIpAddresses	セカンダリIPアドレスおよび関連するパブリックIPアドレスを、パッシブからアクティブインターフェイスに移動するためのアクセス許可。
UnassignPrivateIpAddress	セカンダリIPアドレスと関連するパブリックIPアドレスを、アクティブピア上のインターフェイスから割り当て解除ための許可。
DescribeRouteTables	VM-Seriesファイアウォールインスタンスに関連するすべてのルートテーブルを取得するための許可。
ReplaceRoute	AWSルートテーブルエントリを更新するための許可。
GetPolicyVersion	AWSポリシーバージョン情報を取得するための許可。
GetPolicy	AWSポリシー情報を取得するための許可。
ListAttachedRolePolicies	指定したIAMロールにアタッチされている、すべての管理対象ポリシーのリストを取得するための許可。
ListRolePolicies	指定したIAMロールに埋め込まれている、インラインポリシー名のリストを取得するための許可。
GetRolePolicy	指定したIAMロールに埋め込まれている、特定のインラインポリシーを取得するための許可。
policy	IAMポリシーAmazonリソースネーム（ARN）にアクセスするための許可。
role	IAMロールARNにアクセスするための許可。
route-table	ルートテーブルARNにアクセスするための許可。

©2023 Palo Alto Networks, Inc.

IAMアクション、アクセス許可、またはリソース	説明
ワイルドカード（*）	ARNフィールドで、*をワイルドカードとして使用します。

STEP 6 | アクティブファイアウォールデータインターフェイスと同じサブネット内のパッシブファイアウォールに、新しいインターフェイス（ENI）を作成します。

これらの新しいインターフェイスには、セカンダリ*IP*アドレスを割り当てないでください。

1. Amazon EC2コンソールを開きます。
2. **Network Interfaces**（ネットワークインターフェイス） > **Create Network Interface**（ネットワークインターフェイスの作成） 選択します。
3. 新しいインターフェイスに対する、分かりやすい**Name**（名前）を入力します。
4. **Subnet**（サブネット）で、これらのアクティブファイアウォールのUntrustインターフェイスのサブネットを選択します。
5. **Private IP**（プライベートIP）で、AWSにIPアドレスを動的に割り当てさせる場合はフィールドを空欄にします。そうでない場合は、アクティブファイアウォールのUntrustインターフェイスのサブネット範囲内にあるIPアドレスを入力します。
6. **Security groups**（セキュリティグループ）で、1つまたは複数のセキュリティグループを選択します。
7. **Yes**（はい）および**Create**（作成）を選択します。
8. アクション > ソース/宛先を変更を選択します。をオンにして [無効化] を選択します。
9. これらのステップを、アクティブファイアウォールのTrustインターフェイスのサブネットに対して繰り返します。

STEP 7 | 新しいENIをパッシブファイアウォールインスタンスにアタッチします。セカンダリIP HAを使う方法は、AWSが割り当てるネットワークインターフェイスインデックスに基づいているため、これらのENIをパッシブファイアウォールにアタッチする必要があります。たとえば、アクティブファイアウォールのeth1/2がサブネットAの一部であり、eth1/3がサブネットBの一部である場合、サブネットAの一部であるインターフェイスとサブネットBの一部であるインターフェイスをアタッチする必要があります。この例でAWSは、eth1/2にインデックス値2を、eth1/3にインデックス値3を割り当てています。フェイルオーバーが正常に行われるように、このインデックスを維持する必要があります。

1. 上記で作成されたENIをアタッチするには、作成したUntrustインターフェイスを選択して、**Attach**（アタッチ）をクリックします。
2. パッシブファイアウォールのインスタンスIDを選択し、**Attachs**（アタッチ）をクリックします。
3. Trustインターフェイスに対して、上記のステップを繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 8 | パッシブにログインして、DHCP経由でIPアドレスを取得するようにインターフェイスを設定します。

1. パッシブVM-SeriesファイアウォールWebインターフェイスにログインします。
2. **Network**（ネットワーク） > **Interfaces**（インターフェイス）を選択します。
3. 最初のデータインターフェイスをクリックします。
4. **IPv4**を選択します。
5. **DHCP Client**（**DHCP**クライアント）を選択します。
6. Untrustインターフェイスでのみ、**Automatically create default route pointing to default gateway provided by server**（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）を選択します。
7. ［OK］をクリックします。
8. 各データインターフェイスに対して、この操作を繰り返します。

STEP 9 | データインターフェイスのプライベートIPを参照する、VM-Seriesファイアウォール上にNATポリシーを設定した場合、新たに割り当てたセカンダリIPアドレスを参照するように、それらのポリシーを更新する必要があります。

1. アクティブVM-Series ファイアウォールの Web インターフェイスにアクセスします。
2. **Policies**（ポリシー） > **NAT**を選択します。
3. 変更するNATポリシールールをクリックして、**Translated Packet**（変換されたパケット）を選択します。
4. **Translated Address**（変換されたアドレス）で、Add（追加）をクリックして、AWSで作成されたセカンダリIPアドレスを入力します。
5. プライマリIPアドレスを削除します。
6. **OK**をクリックします。
7. 必要に応じて、これらの手順を繰り返します。
8. 変更を **Commit (コミット)** します。

STEP 10 | セカンダリIP HAフェイルオーバーモードを有効にします。

1. アクティブピア上のVM-Series ファイアウォールにCLIでアクセスします。
2. 以下のコマンドを実行します。

   ```
   request plugins vm_series aws ha failover-mode secondary-ip
   ```

3. 変更をコミットします。
4. 以下のコマンドを実行してHAモードを確認します。

   ```
   show plugins vm_series aws ha failover-mode
   ```

5. パッシブピア上でこのコマンドを繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 11 | 両方のファイアウォール上で HA の設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のファイアウォールで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブな HA ピアで、**Sync to peer**（ピアに同期）をクリックします。
3. ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **Passive**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。
   - アクティブ ファイアウォール: ローカル ファイアウォールの状態が **Active**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。
4. ファイアウォールのコマンドラインインターフェイスから、次のコマンドを実行します:
   - フェイルオーバーの準備状況を確認するには:

     ```
     show plugins vm_series aws ha state
     ```
   - セカンダリIPマッピングを表示するには:

     ```
     show plugins vm_series aws ha ips
     ```

AWS上のアクティブ/パッシブHAのInterface Move（インターフェイス移動）モードへの移行

既存のVM-SeriesファイアウォールHAペアを、セカンダリIP HAからinterface-move（インターフェイス移動）HAに移行するには、次の作業を行ってください。

STEP 1 | パッシブHAピアで、DPDKサポートを無効にします。インターフェイス移動HAモードはDPDKをサポートしていないため、それを無効にしてPacket MMAPを有効にする必要があります。

1. パッシブファイアウォールCLIにログインします。
2. 次のコマンドを使ってDPDKを無効にします。このコマンドを実行すると、ファイアウォールが再起動します。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 2 | アクティブHAピアで、DPDKサポートを無効にします。

1. アクティブファイアウォールにCLIでログインします。
2. 次のコマンドを使ってDPDKを無効にします。このコマンドを実行すると、ファイアウォールが再起動します。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

   ファイアウォールを再起動すると、トラフィックに影響がでます。

©2023 Palo Alto Networks, Inc.

STEP 3 | アクティブピアのHAモードを、セカンダリIPモードからインターフェイス移動モードに変更します。

1. アクティブピア上のVM-Series ファイアウォールにCLIでアクセスします。
2. 以下のコマンドを実行します。

   ```
   request plugins vm_series aws ha failover-mode interface-move
   ```
3. 変更をコミットします。
4. 以下のコマンドを実行してHAモードを確認します。

   ```
   show plugins vm_series aws ha failover-mode
   ```
5. パッシブピア上でこのコマンドを繰り返します。

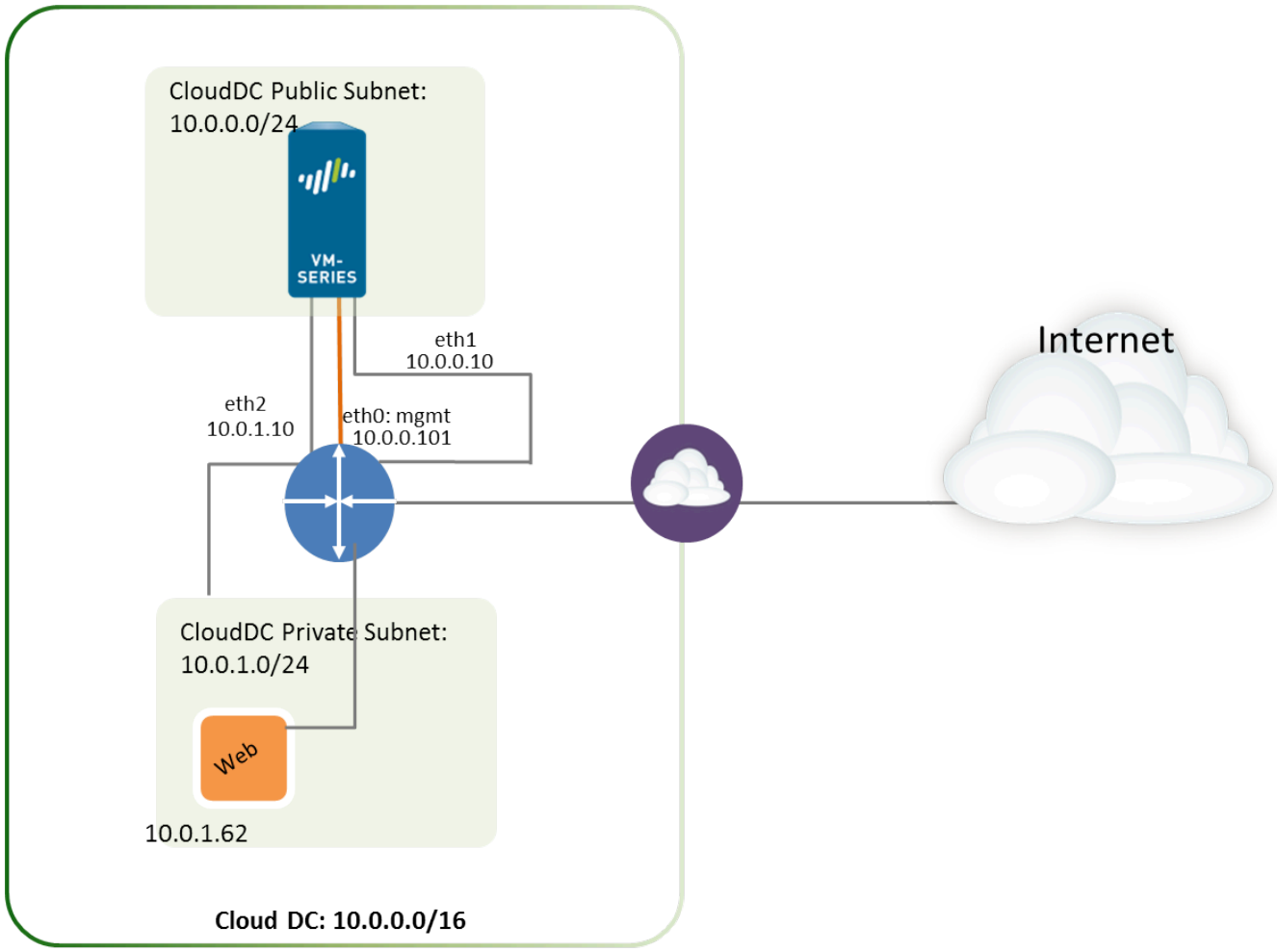
STEP 4 | パッシブファイアウォールインスタンスから、データインターフェイスを削除します。

1. AWS EC2コンソールにログインします。
2. **NetworkInterfaces**（ネットワークインターフェイス）を選択します。
3. パッシブファイアウォールインスタンスのデータインターフェイスを選択して、**Delete**（削除）をクリックします。
4. **Delete Network Interface**（ネットワークインターフェイスの削除）ウィンドウで、**Yes, Delete**（はい、削除します）をクリックします。
5. このプロセスを、パッシブファイアウォールインターフェイス上の各データインターフェイスに対して繰り返します。

©2023 Palo Alto Networks, Inc.

「ユース ケース：AWS クラウドで EC2 インスタンスを保護する

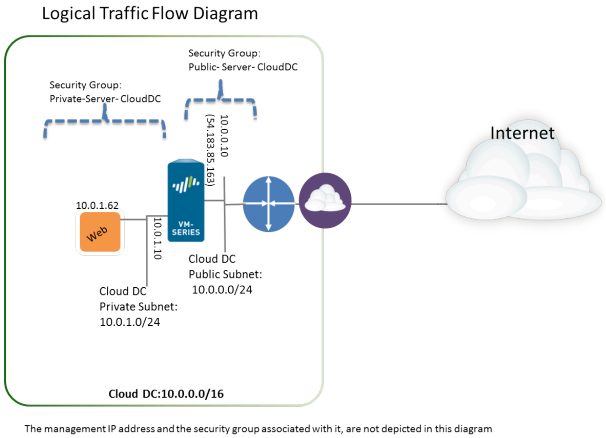
この例では、VPC は、以下の 2 つの /24 サブネットを含む 10.0.0.0/16 ネットワークに展開されています:10.0.0.0/24 および 10.0.1.0/24.VM-Series ファイアウォールは、インターネット ゲートウェイがアタッチされている 10.0.0.0/24 サブネットで起動されます。10.0.1.0/24 サブネットは、VM-Series ファイアウォールによる保護が必要な EC2 インスタンスをホストするプライベート サブネットです。このプライベート サブネット上のサーバーでは、NAT を使用してルーティング可能な IP アドレス（Elastic IP アドレス）でインターネットにアクセスします。AWS VPC での VM-Series 用プランニング ワークシートを使用して、VPC 内の設計を計画します。EC2 インスタンスのサブネット範囲、ネットワーク インターフェイス、および関連付けられた IP アドレスとセキュリティ グループを記録すると、セットアップ プロセスが容易かつ効率的になります。



以下の図は、Web サーバーとの間およびインターネットへのトラフィックの論理フローを表しています。Web サーバーとの間のトラフィックは、プライベート サブネットにアタッチされている VM-Series ファイアウォールのデータ インターフェイスに送信されます。ファイアウォールは、VPC のインターネット ゲートウェイとの間で送受信されるトラフィックにポリシーを

©2023 Palo Alto Networks, Inc.

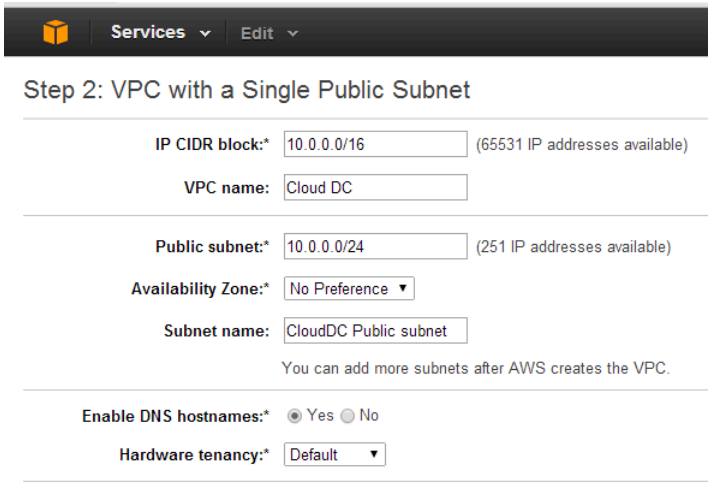
適用して処理します。この図はまた、データ インターフェイスがアタッチされているセキュリティ グループも示しています。



STEP 1 | パブリック サブネットを含む新しい VPC を作成します（または既存の VPC を選択します）。

1. AWS コンソールにログインし、**VPC Dashboard**（**VPC** ダッシュボード）を選択します。
2. 正しい地理上の領域（AWS リージョン）を選択したことを確認します。VPC は現在選択されているリージョンに展開されます。
3. **Start VPC Wizard**（**VPC** ウィザードを起動）を選択し、**VPC with a Single Public Subnet**（単一パブリック サブネットの **VPC**）を選択します。

   この例では、VPC の IP CIDR ブロックは 10.0.0.0/16、VPC 名は Cloud DC、パブリック サブネットは 10.0.0.0/24、サブネット名は Cloud DC Public Subnet です。VPC の作成後、プライベート サブネットを作成します。



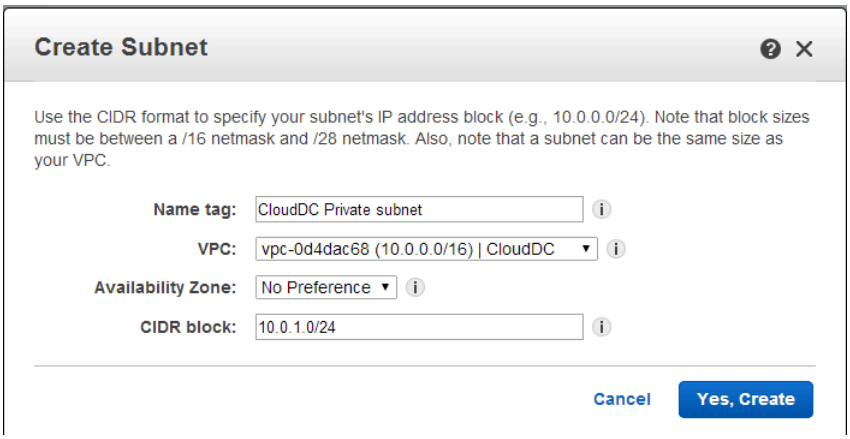
4. **Create VPC**（**VPC** を作成）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 2 | プライベート サブネットを作成します。

Subnets（サブネット）を選択し、**Create a Subnet**（サブネットを作成）をクリックします。情報を入力します。

この例では、サブネットの **Name tag**（名前タグ）は Web/DB Server Subnet です。これは、Cloud Datacenter VPC で作成され、CIDR ブロック 10.0.1.0/24 が割り当てられています。



©2023 Palo Alto Networks, Inc.

STEP 3 | サブネットごとに新しいルート テーブルを作成します。

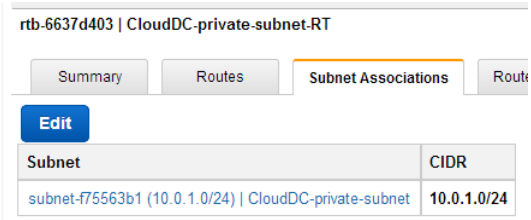
メイン ルート テーブルは *VPC* に自動的に作成されますが、デフォルトのルート テーブルを変更するのではなく、新しいルート テーブルを作成することをお勧めします。

各サブネットからアウトバウンド トラフィックを送信するには、後にこのワークフローで、ルートを各サブネットに関連付けられたルート テーブルに追加します。

1. **Route Tables**（ルート テーブル） > **Create Route Table**（ルート テーブルを作成）を選択します。
2. **Name**（名前）で名前（「CloudDC-public-subnet-RT」など）を追加し、ステップ 1 で作成した VPC を **VPC** で選択して、**Yes, Create**（作成する）をクリックします。
3. ルート テーブルを選択し、**Subnet Associations**（サブネットの関連性）をクリックしてパブリック サブネットを選択します。



4. **Create Route Table**（ルート テーブルを作成）を選択します。
5. **Name**（名前）で名前（「CloudDC-private-subnet-RT」など）を追加し、ステップ 1 で作成した VPC を **VPC** で選択して、**Yes, Create**（作成する）をクリックします。
6. ルート テーブルを選択し、**Subnet Associations**（サブネットの関連性）をクリックしてプライベート サブネットを選択します。



STEP 4 | インバウンド/アウトバウンド インターネット アクセスを VPC 内の EC2 インスタンスに制限するセキュリティ グループを作成します。

デフォルトでは、AWS は、異なるセキュリティ グループに属するインターフェイス間の通信を禁止しています。

Security Groups（セキュリティ グループ）を選択し、**Create Security Group**（セキュリティ グループを作成）ボタンをクリックします。この例では、以下のインバウンド アクセス用ルールを設定した 3 つのセキュリティ グループを作成します。

- CloudDC-Management。VM-Series ファイアウォールの管理インターフェイスに接続できるプロトコルと送信元 IP アドレスを指定します。少なくとも、SSH と HTTPS が必要

 ©2023 Palo Alto Networks, Inc.

です。この例では、このセキュリティ グループにアタッチされているネットワーク インターフェイス上で SSH、ICMP、HTTP、および HTTPS を有効にします。

CloudDC-Management セキュリティ グループには、VM-Series ファイアウォールの管理インターフェイス（eth 0/0）が割り当てられます。

- Public-Server-CloudDC。VPC 内で HTTP、FTP、SSH を介して接続可能な送信元 IP アドレスを指定します。このグループでは、外部ネットワークからファイアウォールへのトラフィックを許可します。

  Public-Server-CloudDC には、VM-Series ファイアウォールのデータプレーン インターフェイス（eth1/1）が割り当てられます。

- Private-Server-CloudDC。アクセスが非常に制限されます。許可するのは、同じサブネット上の他の EC2 インスタンスによる相互または VM-Series ファイアウォールとの通信のみです。

  このセキュリティ グループには、VM-Series ファイアウォールのデータプレーン インターフェイス（eth1/2）とプライベート サブネットの内のアプリケーションがアタッチされます。

  以下のスクリーンショットは、このユース ケースのセキュリティ グループを示しています。

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

STEP 5 | VM-Series ファイアウォールを展開します。

初期起動時には、管理インターフェイスとして機能するプライマリ ネットワーク インターフェイスのみがファイアウォールにアタッチされ、設定されます。データ トラフィックの処理に必要なネットワーク インターフェイスは、ステップ 6 で追加されます。

「AWS での VM-Series ファイアウォールの起動」のステップ 3 を参照してください。

©2023 Palo Alto Networks, Inc.

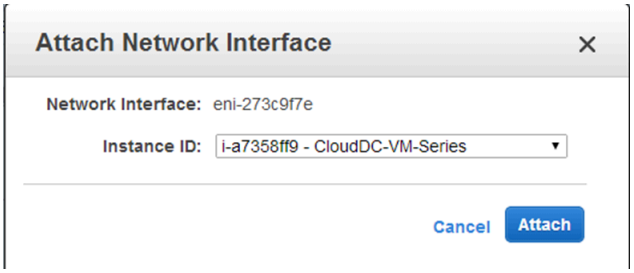
STEP 6 | Elastic Network Interface（ENI）と呼ばれる仮想ネットワーク インターフェイスを作成し、VM-Series ファイアウォールにアタッチします。これらの ENI は、ファイアウォールとの間のデータ トラフィックの処理に使用されます。

1. EC2 Dashboard で **Network Interfacess**（ネットワークインターフェイス）を選択し、**Create Network Interfaces**（ネットワークインターフェイスを作成）をクリックします。
2. 分かりやすいインターフェイス名を入力します。
3. サブネットを選択します。サブネット ID を使用して、正しいサブネットを選択したことを確認します。ENI は、同じサブネット内のインスタンスにのみアタッチできます。
4. インターフェイスに割り当てるアドレスを **Private Ip**（プライベート **IP**）に入力するか、**Auto-assign**（自動割り当て）を選択し、選択されたサブネット内で使用可能な IP アドレスから自動的に IP アドレスを割り当てます。
5. **Security group**（セキュリティ グループ）を選択してネットワーク インターフェイスへのアクセスを制御します。
6. **Yes, Creates**（作成する）をクリックします。

   この例では、以下の設定で 2 つのインターフェイスを作成します。

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - Eth1/1（VM-Series-Untrust）
     - サブネット：10.0.0.0/24
     - プライベート IP：10.0.0.10
     - セキュリティグループ:Public-Server-CloudDC
   - Eth1/2（VM-Series-Trust）
     - サブネット：10.0.1.0/24
     - プライベート IP：10.0.1.10
     - セキュリティグループ:Private-Server-CloudDC
7. VM-Series ファイアウォールに ENI をアタッチするには、上記で作成したインターフェイスを選択し、**Attachs**（アタッチ）をクリックします。



8. **Instance Id**（インスタンス **ID**）で VM-Series ファイアウォールのインスタンス ID を選択し、**Attachs**（アタッチ）をクリックします。

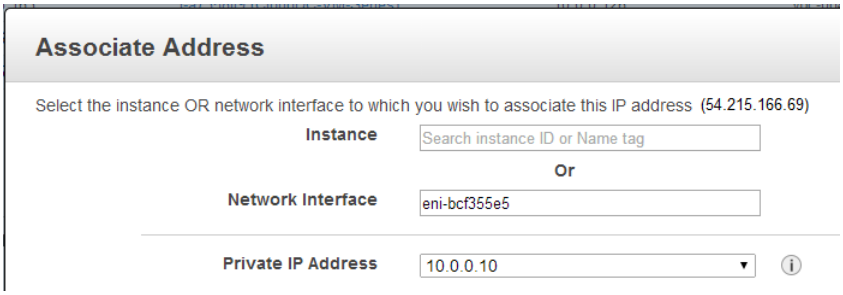
 ©2023 Palo Alto Networks, Inc.

9. ステップ 7 および 8 を繰り返してもう一方のネットワーク インターフェイスをアタッチします。

STEP 7 | Elastic IP アドレスを作成し、インターネットへの直接アクセスが必要なファイアウォールのデータプレーン ネットワーク インターフェイスにアタッチします。

この例では、VM-Series_Untrust が EIP に割り当てられます。インターフェイスに関連付けられた EIP は、プライベート サブネット内の Web サーバー用の公開された IP アドレスです。

1. **Elastic IPs**（**Elastic IP**）を選択し、**Allocate New Address**（新規アドレスを割り当て）をクリックします。
2. **EC2-VPC** を選択し、**Yes, Allocates**（割り当てる）をクリックします。
3. 新しく割り当てられた EIP を選択し、**Associate Addresss**（関連アドレス）をクリックします。
4. **Network Interface**（ネットワーク インターフェイス）でネットワーク インターフェイス、**Private IP address**（プライベート **IP** アドレス）でインターフェイスに関連付けられたプライベート IP アドレスを選択し、**Yes, Associates**（関連付けを行う）をクリックします。



この例では、以下のような設定になります。

Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

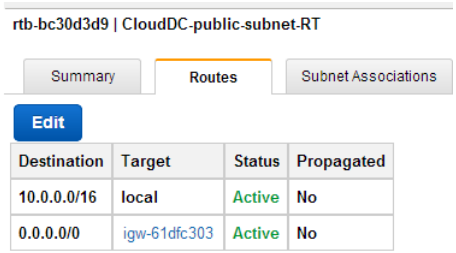
STEP 8 | VM-Series ファイアウォールにアタッチされたネットワーク インターフェイスごとに送信元/送信先チェックを無効にします。この属性を無効にすると、インターフェイスの IP アドレス宛てではないネットワーク トラフィックをインターフェイスで処理できるようになります。

1. **Network Interfaces**（ネットワーク インターフェイス）タブでネットワーク インターフェイスを選択します。
2. **Action** [アクション] のドロップダウンから、**Change Source/Dest.** を選択します。
3. **Disabled**（無効化）をクリックし、**Save**（保存）をクリックして変更を保存します。
4. 追加のネットワーク インターフェイス（この例ではファイアウォール 1/2）について、ステップ 1 ～ 3 を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 9 | （ステップ 3 で）パブリック サブネットに関連付けられたルート テーブルで、VPC のインターネット ゲートウェイにデフォルト ルートを追加します。

1. VPC Dashboard から **Route Tables**（ルート テーブル）を選択し、パブリック サブネットに関連付けられたルート テーブルを見つけます。
2. ルート テーブルを選択し、**Routes**（ルート）を選択して、**Edit**（編集）をクリックします。
3. このサブネットからインターネット ゲートウェイにパケットを転送するルートを追加します。この例では、0.0.0.0/0 は、このサブネットとの間のすべてのトラフィックで、VPC にアタッチされたインターネット ゲートウェイが使用されることを示します。



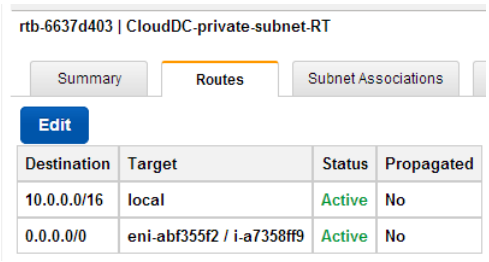
STEP 10 | プライベート サブネットに関連付けられたルート テーブルで、VM-Series ファイアウォールにトラフィックを送信するデフォルト ルートを追加します。

このルートを追加すると、このプライベート サブネットの EC2 インスタンスから VM-Series ファイアウォールへのトラフィックの転送が可能になります。

1. VPC Dashboard から、**Route Tables**（ルート テーブル）を選択し、プライベート サブネットに関連付けられたルート テーブルを見つけます。
2. ルート テーブルを選択し、**Routes**（ルート）を選択して、**Edit**（編集）をクリックします。
3. このサブネットから同じサブネット上にある VM-Series ファイアウォールのネットワーク インターフェイスにパケットを転送するルートを追加します。この例では、0.0.0.0/0 は、このサブネットとの間のすべてのトラフィックで、VM-Series ファイ

©2023 Palo Alto Networks, Inc.

アウォール上の eni-abf355f2（ethernet 1/2、つまり CloudDC-VM-Series-Trust）が使用されることを示します。



プライベート サブネットの *EC2* インスタンスにデプロイされている *Web* サーバーまたはデータベース サーバーごとに、ファイアウォールがサーバーのデフォルト ゲートウェイになるように *VM-Series* ファイアウォールの *IP* アドレスを指すデフォルト ルートを定義する必要があります。

VM-Series ファイアウォールでステップ 11 から 16 を実行します。

STEP 11 | ファイアウォールの新しい管理者パスワードを設定します。

ファイアウォールで *CLI* にアクセスし、デフォルトの管理者パスワードを変更するには、*PuTTY* などの *SSH* ツールが必要です。*SSH* で接続してデフォルト パスワードを変更するまで、*Web* インターフェイスにはアクセスできません。

1. ファイアウォールに設定したパブリック IP アドレスを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH で接続します。

   CLI にアクセスするには、「AWS での VM-Series ファイアウォールの起動」のステップ 3 ～ 12 で使用または作成したプライベート キーが必要になります。
2. 以下のコマンドを入力してファイアウォールにログインします。

   ssh-i *<private_key_name>* admin@*<public-ip_address>*
3. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

   configure
   set mgt-config users admin password
   commit
4. SSH セッションを終了します。

STEP 12 | VM-Series ファイアウォールの Web インターフェイスにアクセスします。

Web ブラウザを開き、管理インターフェイスの EIP を入力します。例：https://54.183.85.163

STEP 13 | VM-Series ファイアウォールでライセンスをアクティベートします。この手順は BYOL ライセンスの場合のみ必要となります（従量制ライセンスは自動的にアクティベートされます）。

「ライセンスのアクティベーション」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 14 | VM-Series ファイアウォールで、ファイアウォールのデータプレーン ネットワーク インターフェイスをレイヤー 3 インターフェイスとして設定します。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
2. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブを選択し、インターフェイスをデフォルト ルーターに割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウンを展開して New Zone（新規ゾーン）を選択します。新しいゾーン（「untrust」など）を定義し、OK をクリックします。
   - IPv4 を選択し、**DHCP Client**（**DHCP** クライアント）を選択します。AWS 管理コンソールでネットワーク インターフェイスに割り当てたプライベート IP アドレスが自動的に取得されます。
   - **Advanced**（詳細） > **Other Info**（その他の情報）タブで、Management Profile（管理プロファイル）ドロップダウンを展開して **New Management Profile**（新規管理プロファイル）を選択します。
   - プロファイルの **Name**（名前）（「allow_ping」など）を入力し、Permitted Services（許可されたサービス）のリストから **Ping** を選択して、**OK** をクリックします。
   - インターフェイス設定を保存するには、**OK** をクリックします。
3. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブを選択し、インターフェイスをデフォルト ルーターに割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「trust」など）を定義し、**OK** をクリックします。
   - **IPv4** を選択し、**DHCP Client**（**DHCP** クライアント）を選択します。
   - **IPv4** タブで、**Automatically create default route to default gateway provided by server**（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）チェック ボックスをオフにします。VPC のプライベート サブネットにアタッチされているインターフェイスの場合、このオプションを無効にすると、この

©2023 Palo Alto Networks, Inc.

インターフェイスで処理されるトラフィックが VPC の IGW に直接流れなくなります。

- **Advanced**（詳細） > **Other Info**（その他の情報）の順に選択し、Management Profile（管理プロファイル）ドロップダウンを展開して、前に作成した allow_ping プロファイルを選択します。
- **OK** をクリックして、インターフェイス設定を保存します。

4. **Commit**（コミット）をクリックして変更を保存します。インターフェイスのリンク状態がアップしていることを確認します 。 リンク状態がアップでない場合は、ファイアウォールを再起動します。

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

STEP 15 | VM-Series ファイアウォールで、VPC 内にデプロイされたアプリケーションとの間のインバウンド/アウトバウンド トラフィックを許可する宛先 NAT ルールと送信元 NAT ルールを作成します。

1. **Policies**（ポリシー） > **NAT**を選択します。
2. ファイアウォールからのトラフィックを Web サーバーに送信する宛先 NAT ルールを作成します。
   1. **Add**（追加）をクリックし、ルールの名前を入力します例：NAT2WebServer。
   2. **Original Packet**（元のパケット）タブで、以下を選択します。
      - **Source Zone**（送信元ゾーン）：untrust（トラフィックの送信元）
      - **Destination Zone**（宛先ゾーン）：untrust（Web サーバーの EIP が関連付けられている、ファイアウォールのデータプレーン インターフェイスのゾーン）
      - **Source Address** [送信元アドレス] :[any]
      - **Destination Address** [宛先アドレス] :10.0.0.10
      - **Translated Packet**（変換済みパケット）タブで、Destination Address Translation（宛先アドレスの変換）チェックボックスをオンにしてか

©2023 Palo Alto Networks, Inc.

ら、**Translated Address**（変換後アドレス）に「10.0.1.62」（Web サーバーのプライベート IP アドレス）と設定します。

3. **OK**をクリックします。

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. Web サーバーからインターネットへのアウトバウンド トラフィックを許可する送信元 NAT ルールを作成します。

1. **Add**（追加）をクリックし、ルールの名前を入力します例：NAT2External。
2. **Original Packet**（元のパケット）タブで、以下を選択します。
   - **Source Zone**（送信元ゾーン）：trust（トラフィックの送信元）
   - **Destination Zone**（宛先ゾーン）：untrust（Web サーバーの EIP が関連付けられている、ファイアウォールのデータプレーン インターフェイスのゾーン）
   - **Source Address** [送信元アドレス] :[any]
   - **Destination Address** [宛先アドレス] :[any]
3. **Translated Packet**（変換済みパケット）タブの Source Address Translation（送信元アドレスの変換）セクションで以下を選択します。
   - **Translation Type** [変換タイプ] :ダイナミック IP およびポート
   - **Address Type** [アドレスタイプ] :変換後アドレス
   - **Translated Address** [変換後アドレス] :10.0.0.10（untrustゾーンのファイアウォールのデータプレーンインターフェイス）
4. **OK**をクリックします。

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
2	NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

4. **Commit**（コミット）をクリックして NAT ポリシーを保存します。

©2023 Palo Alto Networks, Inc.

STEP 16 | VM-Series ファイアウォールで、トラフィックを管理するセキュリティ ポリシーを作成します。

Web サーバーのスタティック *IP* アドレスを入力するのではなく、ダイナミック アドレス グループを使用します。ダイナミック アドレス グループを使用すると、変更に適応するポリシーを自動的に作成できるため、サブネット内で追加の *Web* サーバーを起動したときにポリシーを更新する必要がなくなります。詳細は、「ユースケース:ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する」を参照してください。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。

   この例では、4 つのルールがあります。ファイアウォール トラフィックへの管理アクセスを許可するルール、Web サーバーへのインバウンド トラフィックを許可するルール、Web サーバーへのインターネット アクセスを許可する 3 つ目のルール、最後は、

©2023 Palo Alto Networks, Inc.

事前定義された intrazone-default ルールを変更して、拒否されたすべてのトラフィックがログに記録されるようにするルールです。

2. ファイアウォールへの管理アクセスを許可するルールを作成します。
   1. **Add**（追加）をクリックし、**Name**（名前）にルールの名前を入力します。**Rule Type**（ルール タイプ）が universal であることを確認します。
   2. **Source**（送信元）タブで、**Source Zone**（送信元ゾーン）に untrust を追加します。
   3. **Destination**（宛先）タブで、**Destination Zone**（宛先ゾーン）に trust を追加します。
   4. **Applications**（アプリケーション）タブの **Add**（追加）から、ping と ssh を追加します。
   5. **Actions**（アクション）タブで、**Action**（アクション）を Allow（許可）に設定します。
   6. **OK**をクリックします。

	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
1	AllowManagement	universal	untrust	any	trust	ping ssh	application-default	✓	none	

3. Web サーバーへのインバウンド トラフィックを許可するルールを作成します。
   1. **Add**（追加）をクリックし、**Name**（名前）にルールの名前を入力して、**Rule Type**（ルール タイプ）が universal であることを確認します。
   2. **Source**（送信元）タブで、**Source Zone**（送信元ゾーン）に untrust を追加します。
   3. **Destination**（宛先）タブで、**Destination Zone**（宛先ゾーン）に trust を追加します。
   4. **Applications**（アプリケーション）タブの **Add**（追加）から、web-browsing を追加します。
   5. **Service/URL Category**（サービス/URL カテゴリ）タブで、service（サービス）が application-default に設定されていることを確認します。
   6. **Actions**（アクション）タブで、**Action**（アクション）を Allow（許可）に設定します。
   7. **Actions**（アクション）タブの Profile Settings（プロファイル設定）セクションで、**Profiles**（プロファイル）を選択し、antivirus（アンチウイルス）、anti-

©2023 Palo Alto Networks, Inc.

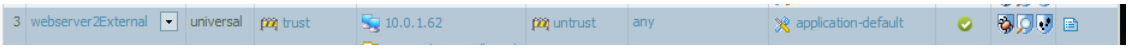
spyware（アンチスパイウェア）、vulnerability protection（脆弱性防御）にデフォルト プロファイルを関連付けます。

8. **OK**をクリックします。



4. Web サーバーへのインターネット アクセスを許可するルールを作成します。

1. **Add**（追加）をクリックし、**Name**（名前）にルールの名前を入力して、Rule Type（ルール タイプ）が universal であることを確認します。
2. **Source**（送信元）タブで、**Source Zone**（送信元ゾーン）に trust を追加します。
3. **Source**（送信元）タブの Source Address（送信元アドレス）セクションで、Web サーバーの IP アドレスである「10.0.1.62」を追加します。
4. **Destination**（宛先）タブで、**Destination Zone**（宛先ゾーン）に untrust を追加します。
5. **Service/URL Category**（サービス/URL カテゴリ）タブで、service（サービス）が **application-default** に設定されていることを確認します。
6. **Actions**（アクション）タブで、**Action**（アクション）を Allow（許可）に設定します。
7. **Actions**（アクション）タブの Profile Settings（プロファイル設定）セクションで、**Profiles**（プロファイル）を選択し、antivirus（アンチウイルス）、anti-spyware（アンチスパイウェア）、vulnerability protection（脆弱性防御）にデフォルト プロファイルを関連付けます。
8. **OK**をクリックします。

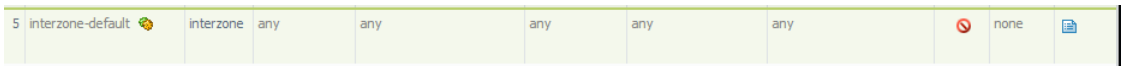


5. 拒否されたすべてのトラフィックをログに記録するように interzone-default ルールを編集します。この事前定義された interzone（ゾーン間）ルールは、異なるゾーン間を移動するトラフィックと一致する他のルールが明示的に定義されていない場合に評価されます。

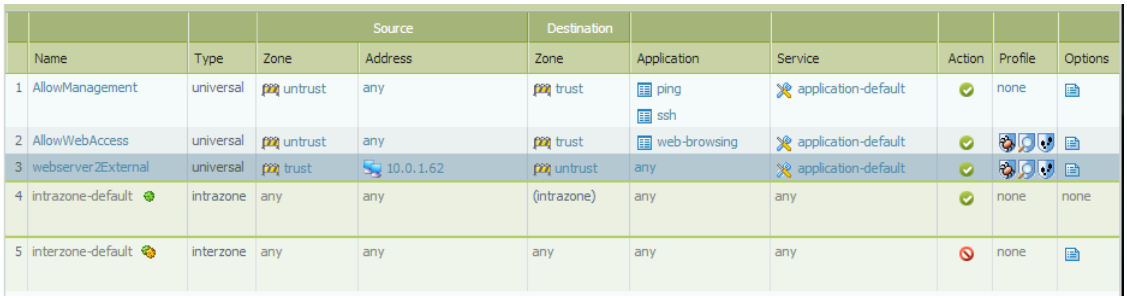
1. **interzone-default** ルールを選択し、**Override**（オーバーライド）をクリックします。
2. **Actions**（アクション）タブで、**Log at session end**（セッション終了時にログ）を選択します。

©2023 Palo Alto Networks, Inc.

3. **OK**をクリックします。



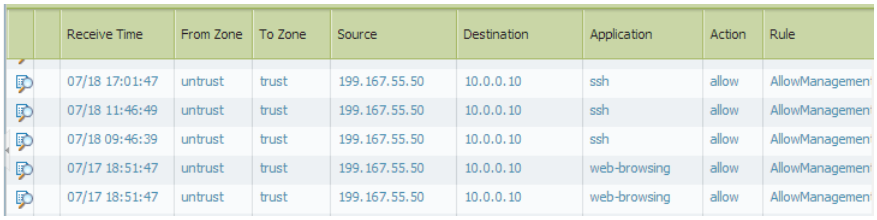
6. ファイアウォールに対して定義した一連のセキュリティ ルールすべてを確認します。
7. **Commit**（コミット）をクリックしてポリシーを保存します。



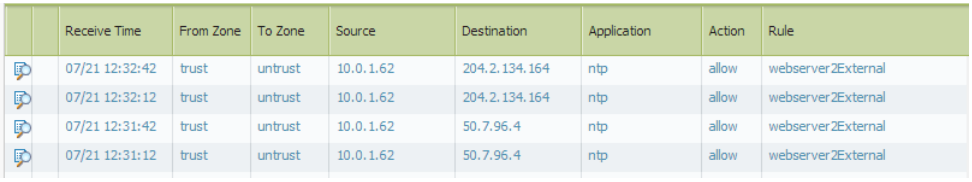
STEP 17 | VM-Series ファイアウォールがトラフィックを保護することを確認します。

1. Web ブラウザを起動し、Web サーバーの IP アドレスを入力します。
2. VM-Series ファイアウォールの Web インターフェイスにログインし、**Monitor**（監視）> **Logs**（ログ） > **Traffic**（トラフィック）の順に選択してセッションのトラフィック ログを表示できることを確認します。

   - Web サーバーへのインバウンド トラフィック（AWS VPC の EC2 インスタンスに到達）



   - Web サーバーからのアウトバウンド トラフィック（AWS VPC の EC2 インスタンス）



VM-Series ファイアウォールがクラウド ゲートウェイとして正常にデプロイされました。

 ©2023 Palo Alto Networks, Inc.

「ユース ケース：ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する

オンデマンドで新しい EC2 インスタンスが起動される AWS-VPC のような動的な環境では、セキュリティ ポリシーの管理負担が煩雑になることがあります。セキュリティ ポリシーでダイナミック アドレス グループを使用すると、俊敏性が向上し、サービスの中断や防御の間隙を阻止できます。

この例では、ファイアウォール上の VM 情報ソースを使って VPC をモニターし、セキュリティ ポリシーでダイナミック アドレス グループを使用して EC2 インスタンスを検出および保護できます。EC2 インスタンスが作成されると、ダイナミック アドレス グループは、グループ メンバーシップに対して定義された条件に一致するすべてのインスタンスの IP アドレスを順に並べ、グループのセキュリティ ポリシーを適用します。この例のセキュリティ ポリシーでは、グループのすべてのメンバーへのインターネット アクセスが許可されます。

ファイアウォール上の *VM* 情報ソースを使用する代わりに、*Panorama* を *VPC* と一元的に通信する単一のポイントとして使用することができます。*AWS Plugin on Panorama* を使用して *IP* アドレス対タグのマッピングを取得し、通知を設定する管理対象のファイアウォールにその情報を登録することができます。このオプションの詳細については、AWS Plugin on Panorama による VM モニタリングを参照してください。

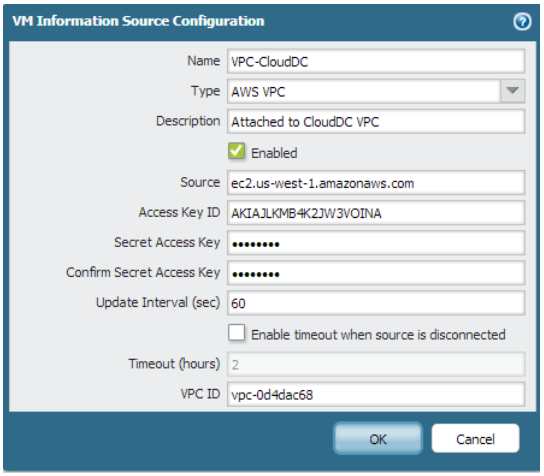
以下のセクションのワークフローでは、すでに AWS VPC が作成され、VM-Series ファイアウォールと一部のアプリケーションが EC2 インスタンスにデプロイされていると想定されています。VM-Series の VPC セットアップ手順は、次を参照してください：「ユース ケース：AWS クラウドで EC2 インスタンスを保護する」。

STEP 1 | VPC をモニターするようにファイアウォールを設定します。

1. **Device**（デバイス） > **VM Information Sources**（**VM** 情報ソース）を選択します。
2. **Add**（追加）をクリックして、以下の情報を入力します。
   1. **Name**（名前）に、モニターする VPC を識別する名前を入力します（「VPC-CloudDC」など）。
   2. **Type**（タイプ）を AWS VPC に設定します。
   3. **Source**（送信元）に VPC の URI を入力します。構文は **ec2.<*your_region*>.amazonaws.com** です
   4. ファイアウォールが AWS サービスへの API コールにデジタル署名するために必要な認証情報を追加します。以下の設定が必要です。
      - **Access Key ID**[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。
      - **Secret Access Key** [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。
   5. （任意）**Update interval**（更新間隔）を 5 ～ 600 秒の値に変更します。デフォルトでは、ファイアウォールは 5 秒ごとにポーリングします。API 呼び出しは毎回 60 秒

©2023 Palo Alto Networks, Inc.

以内にキューに登録され取得されるため、更新の最大所要時間は 60 秒に設定ポーリング間隔を加えた値となります。



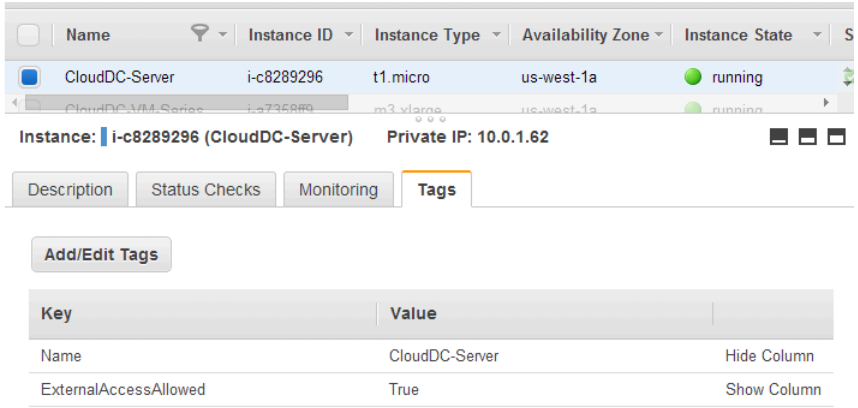
6. **VPC ID** に、AWS 管理コンソールの VPC Dashboard に表示される VPC ID を入力します。
7. **OK** をクリックし、変更を**Commit**（コミット）します。
8. 接続 **Status (**ステータス**)** が connected (接続済み) と表示されていることを確認します。

STEP 2 | VPC の EC2 インスタンスにタグ付けします。

VM-Series ファイアウォールによってモニターできるタグの一覧は、「AWS-VPC でモニターされる属性の一覧」を参照してください。

タグは、名前 - 値ペアです。EC2 インスタンスへのタグ付けは、AWS 管理コンソールの EC2 Dashboard か、AWS API または AWS CLI を使用して行うことができます。

この例では、EC2 Dashboard を使用してタグを追加します。

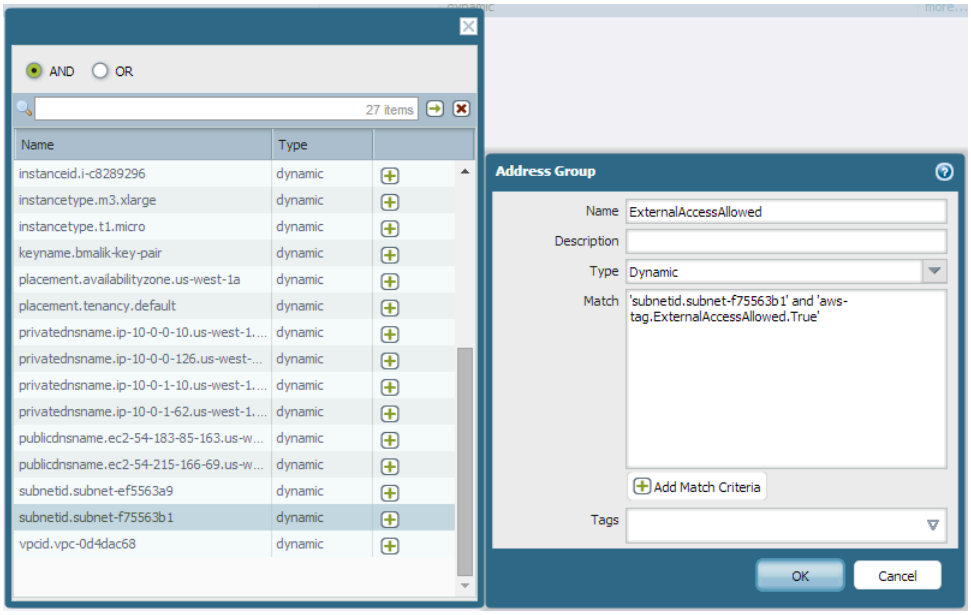


 ©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォール上にダイナミック アドレス グループを作成します。

この機能の概略を把握するために、チュートリアルを参照してください。

1. **Object**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. **Add**（追加）をクリックし、**Name**（名前）にアドレス グループの名前を、**Description**（内容）にアドレス グループの内容を入力します。
3. **Type**（タイプ）で **Dynamic**（ダイナミック）を選択します。
4. 一致条件を指定します。
   1. **Add Match Criteria**（条件の追加）をクリックし、**AND** 演算子を追加します。
   2. 絞り込みまたは照合の基準となる属性を選択します。この例では、作成した ExternalAccessAllowed タグと、VPC のプライベート サブネットのサブネット ID を選択します。



5. **OK**をクリックします。
6. **Commit**（コミット）をクリックします。

 ©2023 Palo Alto Networks, Inc.

STEP 4 | セキュリティ ポリシー内でダイナミック アドレス グループを使用します。

ExternalServerAccess というダイナミック アドレス グループに属する Web サーバーへのインターネット アクセスを許可するルールを作成するには、以下の手順を実行します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Add**（追加）をクリックし、**Name**（名前）にルールの名前を入力して、**Rule Type**（ルール タイプ）が universal であることを確認します。
3. **Source**（送信元）タブで、**Source Zone**（送信元ゾーン）に trust を追加します。
4. **Source**（送信元）タブの Source Address（送信元アドレス）セクションで、**Add**（追加）をクリックして、作成した ExternalServerAccess グループを追加します。
5. **Destination**（宛先）タブで、**Destination Zone**（宛先ゾーン）に untrust を追加します。
6. **Service/URL Category**（サービス/URL カテゴリ）タブで、service（サービス）が **application-default** に設定されていることを確認します。
7. **Actions**（アクション）タブで、**Action**（アクション）を Allow（許可）に設定します。
8. **Actions**（アクション）タブの Profile Settings（プロファイル設定）セクションで、**Profiles**（プロファイル）を選択し、antivirus（アンチウイルス）、anti-spyware（アンチスパイウェア）、vulnerability protection（脆弱性防御）にデフォルト プロファイルを関連付けます。
9. **OK**をクリックします。



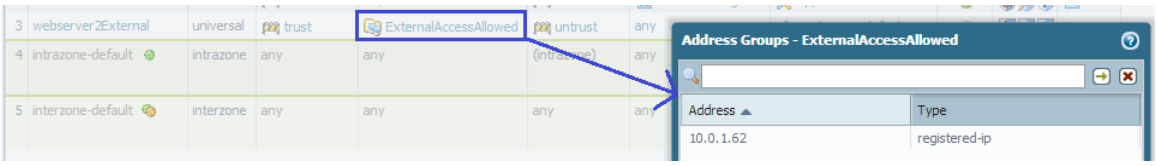
			Source		Destination					
	Name	Type	Zone	Address	Zone	Application	Service	Action	Profile	Options
2	AllowWebAccess	universal	untrust	any	trust	web-browsing	application-default			
3	webserver2External	universal	trust	ExternalAccessAllowed	untrust	any	application-default			

10. **Commit**（コミット）をクリックします。

STEP 5 | ファイアウォール上に、ダイナミック アドレス グループのメンバーが入力されていることを確認します。

このアドレス グループに属し、ここに表示されるすべての IP アドレスについてポリシーが適用されます。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、ルールを選択します。
2. アドレス グループのリンクの隣にあるドロップダウンの矢印を選択し、**Inspect**（検査）をクリックします。一致条件が正確であるか確認することもできます。
3. **more**（詳細）リンクをクリックし、登録された IP アドレスのリストが表示されることを確認します。



 ©2023 Palo Alto Networks, Inc.

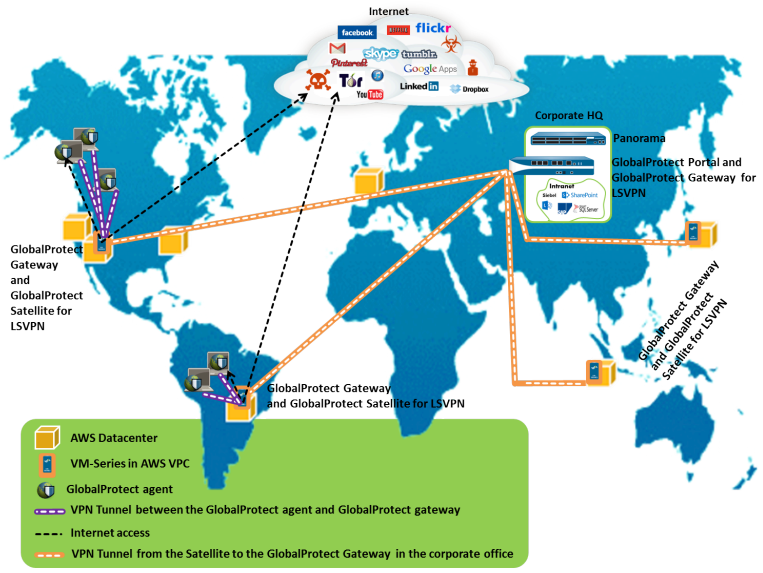
ユース ケース：AWS の GlobalProtect ゲートウェイとしての VM-Series ファイアウォール

モバイルユーザーを脅威や危険なアプリケーションから保護するには、多くの場合、セキュリティおよびITインフラストラクチャの調達とセットアップ、世界各地の帯域幅およびアップタイム要件の確保などが複雑に混ざり合った作業が伴い、しかもすべて予算内で行う必要があります。

AWS で VM-Series ファイアウォールを使用すると、セキュリティと IT 機器とを融合させて実装し、拠点のない地域でモバイル ユーザーが使用するデバイスを一貫して確実に保護することができます。通常、各自のリソースを使用してこのインフラストラクチャをセットアップする場合、コストや IT 機器の負担が生じますが、VM-Series ファイアウォールを AWS クラウドにデプロイすると、このような負担を負うことなく、GlobalProtect™ ゲートウェイを任意の領域にすばやく簡単にデプロイできます。

遅延を最小限に抑えるには、ユーザーに最も近い AWS リージョンを選択して EC2 インスタンスに VM-Series ファイアウォールをデプロイし、ファイアウォールを GlobalProtect ゲートウェイとして設定します。このソリューションでは、AWS クラウド内の GlobalProtect ゲートウェイによりインターネット トラフィックに関するセキュリティ ポリシーが適用されるため、そのトラフィックを企業ネットワークに戻す必要がありません。さらに、企業ネットワーク上にあるリソースにアクセスする場合は、AWS の VM-Series ファイアウォールが LSVPN 機能を利用して、企業ネットワーク上のファイアウォールに戻る IPSec トンネルを確立します。

この分散インフラストラクチャのデプロイメントと中央管理を容易にするには、Panorama を使用して、このソリューションで使用される GlobalProtect コンポーネントを設定します。必要に応じて、ネットワークでモバイル デバイス（スマートフォンやタブレット）を安全に使用できるように、Mobile Device Manager を使用してモバイルデバイスの設定および管理を行います。



- GlobalProtect インフラストラクチャのコンポーネント
- AWS への GlobalProtect ゲートウェイのデプロイ

©2023 Palo Alto Networks, Inc.

GlobalProtect インフラストラクチャのコンポーネント

危険なアプリケーションをブロックし、モバイル ユーザーをマルウェアから保護するには、GlobalProtect ポータル、GlobalProtect ゲートウェイ、GlobalProtect アプリケーションを含む GlobalProtect インフラストラクチャをセットアップする必要があります。さらに、企業のリソースにアクセスするために、AWS の VM-Series ファイアウォールと本社のファイアウォール間に、LSVPN（ハブ アンド スポーク VPN デプロイメント）を使用して IPsec VPN 接続をセットアップする必要があります。

- GlobalProtectエージェント/アプリケーションは、企業のアプリケーションおよびリソースへのアクセスを許可されている各エンドユーザーシステム上にインストールされます。エージェントは、最初にポータルに接続してゲートウェイ上の情報を取得し、最も近い GlobalProtect ゲートウェイへのセキュアな VPN 接続を確立します。エンドユーザー システムとゲートウェイ間の VPN 接続により、データの機密性が確保されます。
- GlobalProtect 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。すべてのエンドユーザー システムは、ポータルから設定情報を受信します。これには、使用可能なゲートウェイ、GlobalProtect ゲートウェイへの接続に必要になる可能性のあるクライアント証明書などの情報が含まれます。このユース ケースでは、GlobalProtect ポータルは、本社にデプロイされたハードウェアベースのファイアウォールです。
- GlobalProtectゲートウェイは、アプリケーション、ユーザー、コンテンツ、デバイス、デバイス状態に基づいてモバイル脅威防御とポリシー適用を行います。このユース ケースでは、AWS の VM-Series ファイアウォールが GlobalProtect ゲートウェイとして機能します。GlobalProtect ゲートウェイは各ユーザー要求をマルウェアやその他の脅威がないかスキャンし、ポリシーで許可されていれば、（LSVPN ゲートウェイへの）IPsecトンネル経由で要求をインターネットまたは企業ネットワークに送信します。
- LSVPN については、GlobalProtectポータル、LSVPN用のGlobalProtectゲートウェイ（ハブ）、およびGlobalProtectサテライト（スポーク）を設定する必要があります。

  このユース ケースでは、事業所のハードウェアベースのファイアウォールが GlobalProtect ポータルおよび LSVPN ゲートウェイとしてデプロイされます。AWS の VM-Series ファイアウォールは、GlobalProtect サテライトとして機能するように設定されます。GlobalProtect サテライトおよびゲートウェイは、ゲートウェイで終端する IPsec トンネルを確立するために設定されます。モバイル ユーザーが企業ネットワーク上のアプリケーションまたはリソースを要求すると、VM-Series ファイアウォールは要求を IPsec トンネル経由でルーティングします。

AWS への GlobalProtect ゲートウェイのデプロイ

モバイル ユーザーを保護するには、AWS での GlobalProtect ゲートウェイのデプロイと設定に加え、この統合ソリューションに必要なその他のコンポーネントをセットアップする必要があります。以下の表で、推奨ワークフローを説明します。

AWS で VM-Series ファイアウォールをデプロイします。

「AWS での VM-Series ファイアウォールのデプロイ」を参照してください。

 ©2023 Palo Alto Networks, Inc.

本社にファイアウォールを設定します。

このユース ケースでは、ファイアウォールは GlobalProtect ポータルおよび LSVPN ゲートウェイとして設定されます。

- GlobalProtect ポータルの設定。
- LSVPN の GlobalProtect ポータルの設定。
- LSVPN サテライトを認証するためのポータルの設定。
- LSVPN の GlobalProtect ゲートウェイの設定。

AWS で VM-Series ファイアウォールを GlobalProtect ゲートウェイおよび LSVPN サテライトとして設定するためのテンプレートを Panorama でセットアップします。

この分散デプロイメントを容易に管理するために、Panorama を使用して AWS でファイアウォールを設定します。

- Panorama でのテンプレートの作成。

次に、以下のリンクを使用してテンプレートの設定を定義します。

- GlobalProtect ゲートウェイとしてのファイアウォールの設定。
- LSVPN に参加するためのサテライトの準備。

Panorama でデバイスグループを作成して、ネットワーク アクセス ポリシーおよびインターネット アクセス ルールを定義し、AWS でファイアウォールに適用します。

「デバイス グループの作成」を参照してください。

AWS で VM-Series ファイアウォールにテンプレートとデバイス グループを適用し、ファイアウォールが正しく設定されていることを確認します。

GlobalProtect クライアント ソフトウェアをデプロイします。

すべてのエンドユーザー システムに、GlobalProtect ゲートウェイに接続するための GlobalProtect エージェントまたはアプリケーションが必要です。

「GlobalProtect クライアント ソフトウェアのデプロイ」を参照してください。

©2023 Palo Alto Networks, Inc.

AWS でのリソースモニタリング

AWS パブリッククラウドでリソースをデプロイあるいは停止する際、AWS 用の Panorama プラグインあるいはファイアウォール上の AWS リソース情報のいずれかを使用し、それらのワークロードに対して一貫した形でセキュリティポリシールールを適用できます。互換性マトリックスで Panorama プラグインのバージョン情報を参照してください。

スケーリングが可能な AWS 用の Panorama プラグインを使えば、AWS パブリック クラウド上で最大 1000 個の AWS VPC を監視できます。このプラグインと共に Panorama をタグの AWS アカウントをポーリングするためのアンカーとして使用してから、メタデータ（IP アドレス対タグのマッピング）をデバイスグループ内の多数のファイアウォールに配信します。Panorama は AWS アカウントと通信して AWS リソース情報を取得するため、クラウド環境に対して行う API コール数を合理化することができます。Panorama および AWS プラグインを使う際、タグの取得とセキュリティポリシーの管理を一元的に行い、ハイブリッドおよびクラウド ネイティブなアーキテクチャに対して一貫した形でポリシーを適用できます。Panorama での AWS プラグインを使った AWS リソースモニタリングを参照してください。

Panorama を持っていないかシンプルなデプロイメントであり、監視する必要がある VPC が 10 件以下である場合、ファイアウォール（ハードウェアあるいは VM-Series ファイアウォール）上の VM 情報ソースを使用して AWS のワークロードを監視できます。ファイアウォールが取得するメタデータをダイナミック アドレス グループ内で使用し、セキュリティ ポリシーでそれらを参照することで、IP アドレスが頻繁に変わったり、スピンアップあるいはダウンしたりする VM ワークロードを保護できます。「ユース ケース：ダイナミックアドレスグループを使用してVPC内の新しいEC2インスタンスを保護する」を参照してください。

Panorama でのAWS プラグインを使った AWS リソースモニタリング

AWS パブリック クラウド内でリソースをデプロイあるいは停止する際、Palo Alto Networks® のファイアウォール上のセキュリティポリシーを同期的に更新し、それらの EC2 インスタンスを保護できる方法が必要になります。Panorama からこの機能を有効化するには、AWS Plugin on Panorama をインストールし、Panorama および AWS VPC 間の API 通信を有効化する必要があります。その後、Panorama が事前定義済みの一連の属性 （あるいはメタデータ要素） を AWS リソースのタグとして収集し、その情報を Palo Alto Networks® のファイアウォールに登録できるようになります。ダイナミック アドレス グループ内でこれらのタグを参照してセキュリティポリシー ルール内の項目にマッチさせる際、AWS アカウント内にデプロイしたすべてのアセットに対して一貫した形でポリシーを適用できます。

- Panorama でのモニタリング用 AWS プラグインのセットアップ
- AWS-VPC でモニターされる属性の一覧

Panorama 上の VM モニタリング用 AWS プラグインをセットアップ

組織が AWS パブリック クラウドにデプロイしたすべての仮想マシンのワークロードを確認するためには、AWS Plugin on Panorama をインストールし、モニタリング定義を構成し

 ©2023 Palo Alto Networks, Inc.

て、Panorama が AWS VPC に認証して対象のワークロードに関する VM 情報を取得できるようにする必要があります。Panorama は実行中の VM の IP アドレス（パブリック IP アドレス、プライマリおよびセカンダリ プライベート IP アドレス）および関連するタグを取得します。Panorama がサポートしているメタデータ要素のリストについては、AWS-VPC でモニターされる属性の一覧を参照してください。

Panorama が属性を取得した後、仮想マシン情報を Panorama からファイアウォールにプッシュするためには、ファイアウォール（ハードウェアあるいは VM-Series）を管理対象のデバイスとして Panorama 上に追加し、ファイアウォールを一つあるいは複数のデバイスグループにグループ化する必要があります。その後、Panorama が AWS から取得する IP アドレス対タグのマッピングを登録するために使用する、通知グループに含まれるデバイスグループはどれで、モニタリング定義内の設定要素がどれなのかを指定できます。

最後に、EC2 インスタンス全体で一貫した形でセキュリティ ポリシーを適用するために、ダイナミック アドレス グループをセットアップし、VM の IP アドレスに向かうトラフィックを許可あるいは拒否するポリシールール内でそれらを参照する必要があります。Panorama 上でダイナミック アドレス グループおよびセキュリティポリシールールを定義し、各ファイアウォールのローカルでダイナミック アドレス グループおよびセキュリティポリシールールを管理する代わりに、それらをファイアウォールにプッシュすることで、Panorama で一元的に行うポリシーおよびオブジェクトの管理や設定を合理化できます。

AWS プラグイン バージョン 2.0 は、AWS パブリック クラウド、AWS GovCloud、および AWS China 上の最大 1000 VPC の EC2 インスタンスの監視に使用します。ただし、AWS China には Panorama をデプロイできないため、IAM ロールはAWS China でのインスタンス プロファイルをサポートしていません。AWS 認証情報を指定する必要があります。

- AWS 上の VM モニタリングのためのチェックリストのプランニング
- Panorama の IAM ロールとアクセス許可
- AWS プラグインのインストールとアップグレード
- VM モニタリング用 AWS プラグインを設定

AWS 上の VM モニタリングのためのチェックリストのプランニング

Panorama が AWS の API とやり取りを行って EC2 インスタンスについての情報を収集できるようにするために、IAM ロールを作成し、AWS への認証に必要な権限、およびVPC 内の EC2 インスタンスにアクセスする権限を付与するポリシーを割り当てる必要があります。Panorama で最大 1000 の VPC を管理するため 100 の IAM ロールを追加できます。

- VPC ID を収集します。
- AWS 上の EC2 インスタンスにタグ付けします。EC2 インスタンスへのタグ付け（名前と値のペアを定義）は、AWS 管理コンソールの EC2 Dashboard か、AWS API または AWS CLI を使用して行うことができます。サポートされている属性のリストについては、AWS-VPC でモニターされる属性の一覧を参照してください。

©2023 Palo Alto Networks, Inc.

- 監視を有効にする VPC 全体で IP アドレスの重複をチェックします。AWS VPC 全体で重複している IP アドレスがある場合、メタデータが追加されるかスワップされるため、ポリシー適用時に予期せぬ動作が発生するおそれがあります。

  重複する *IP* アドレスは *plugin_aws_ret.log* ファイルに書き込まれます。このファイルには、*Panorama* の *CLI* からアクセスできます。

- Panorama および管理対象のファイアウォールの要件を確認してください：
  - 最低システム要件 — Panorama バーチャル アプライアンスあるいはハードウェアベースの Panorama アプライアンス。

Panorama の最低要件				
システム リソース	メモリ	CPU	監視対象 VPC 数	登録されているタグ数
	16GB	4	1〜100	Panorama 9.1 以降と AWS プラグイン v 2.0 では、10,000 件の IP アドレスとそれぞれ 13 件のタグの取得、または 5000 件の IP アドレスとそれぞれ 25 件のタグの取得テストが行われ、それらはデバイス グループに含まれているファイアウォールに正常に登録されました。各 EC2 インスタンスに対する、名前と値を含めたタグの長さは、タグあたり 64 バイトを想定しています。たとえば、EC2 インスタンス名のタグは aws.ec2.tag.Name.prod-web-app-4523-lvss6j になります。
	32 GB	8	100〜500	
	64 GB	16	500〜1000	
Panorama OS バージョン	9.1 以降			
AWS プラグイン バージョン	2.0.0 以降			
ライセンス	ファイアウォールを管理するためのデバイス管理ライセンスおよびアクティブなサポート ライセンス。 次世代ファイアウォールには、有効なサポート ライセンスも必要です。			
EC2 インスタンスでメタデータを取得するためのロールとアクセス許可	「Panorama の IAM ロールとアクセス許可」を参照してください			

©2023 Palo Alto Networks, Inc.

- Panorama 上にファイアウォールをファイアウォールとして追加してデバイスグループを作成し、Panorama が取得した VM 情報をそれらのグループに通知するよう設定できるようにする必要があります。デバイスグループには、VM-Series ファイアウォールやハードウェア ファイアウォール上の仮想システムも含められます。
- Panorama アプライアンスが高可用性構成である場合、両方の Panorama ピアに同じバージョンの AWS プラグインを手作業でインストールする必要があります。また、インスタンス プロファイルを使用している場合は、両方の Panorama ピアに同じインスタンスをアタッチする必要があります。

  ***AWS** プラグインは、アクティブ **Panorama** ピア上でのみ構成します。コミット時に設定はパッシブ **Panorama** ピアと同期されます。**VM** モニタリング用に構成した **AWS** アカウントにポーリングを行うのは、アクティブ **Panorama** ピアだけです。*
- AWS サービスに対する API コールに Panorama がデジタル署名するために必要な認証情報/アクセス許可を設定します。

  各 AWS アカウント内のリソースにアクセスできるようにする長期的な認証情報（アクセス キー ID と秘密アクセス キー）を提供するか、または AWS の Assume Role を設定して同一 AWS アカウントまたはクロスアカウントの定義済み AWS リソースへのアクセスを許可するかを選択できます。Assume Role では、ロール自体を作成する他に、信頼関係を設定して権限を定義する必要があります。これは特に、照会を実行するアカウントに照会対象のアカウントのデータを表示または処理する権限がないクロスアカウント デプロイメントで役立ちます。Panorama プラグインから VPC に対する認証が成功し、タグを取得できるようにするには、すべての AWS サービスに対して AWS Security Token Service（STS）API を使用するように Assume Role を設定する必要があります。また、照会を実行するアカウントのユーザーに、Assume Role を照会してリソース アクセスのための一時的なセキュリティ認証情報を取得するための STS 権限が必要です。AWS 上に Panorama をデプロイしている場合、IAM ロールに対して AWS 認証情報を提供する代わりに、インスタンス プロファイルを使用することができます。インスタンス プロファイルには、Panorama が AWS サービスへの API コールにデジタル署名を行うために必要な、ロール情報と関連する認証情報が含まれています。詳細については、「Panorama の IAM ロールとアクセス許可」を参照してください。

Panorama の IAM ロールとアクセス許可

AWS プラグイン バージョン 2.0 では、IAM ロールまたはインスタンス プロファイルを使って、Panorama による AWS アカウントにデプロイされているリソースの認証とメタデータの取得を可能にすることができます。

- Panorama が AWS にデプロイされていない場合は、2 種類の選択肢があります。監視する AWS アカウントの長期的な IAM 認証情報を提供するか、または AWS の Assume Role を設定して同一 AWS アカウントまたはクロスアカウントの定義済み AWS リソースへのアクセスを許可するかを選択できます。より安全な Assume Role（想定ロール）を使用することをお勧めします。
- AWS に Panorama がデプロイされている場合、前述の 2 種類の選択肢の他に、インスタンス プロファイルを追加して、IAM ロールを EC2 インスタンスに渡すこともできます。同じアカウント内にすべての監視対象リソースと Panorama がある環境でインスタンス プロファイル

©2023 Palo Alto Networks, Inc.

を使用、または Panorama と監視対象リソースが異なる AWS アカウントにデプロイされている環境でクロス アカウント アクセスを行うために、Assume Role（想定ロール）を持つインスタンス プロファイルを使用することができます。インスタンス プロファイルを使用する場合、Panorama に AWS 認証情報を入力しません。

オプション **1:**長期的な認証情報を持つ **IAM** ロール	

必要なロールとアクセス許可	監視対象 VPC/EC2 インスタンスを持つ AWS アカウントの、AWS 認証情報。
	長期認証情報を持つ IAM ロールに関連する最低限の権限（JSON 形式）は次の通りです。
	<pre>{ "Path": "/", "UserName": "panorama_vm_programmatic",
	  "UserId": "AIDAIZXXXXCR5JPII4XYZ",
	  "Arn": "arn:aws:iam::412383210500:user/
	  panorama_vm_programmatic",
	  "CreateDate": "2018-07-06T19:14:31Z",
	  "GroupList": [],
	  "AttachedManagedPolicies":
	  [
	  { "PolicyName": "ReadOnlyAccess",
	  "PolicyArn": "arn:aws:iam::aws:policy/ReadOnlyAcce
	ss"
	  }
	  ]
	},</pre>

Panorama での入力	**Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **IAM Role**（**IAM** ロール）のユーザーに対する、**Access Key ID**（アクセス キー **ID**）および**Secret Access Key**（秘密アクセス キー）を入力します。
オプション **2:Assume Role**（想定ロール）付き **IAM** ロール	
必要なロールとアクセス許可	この方法を利用して同じアカウントまたはクロス アカウント内の VPC を管理できますが、ロールを想定することで通常アクセスできるリソースへのクロス アカウント アクセスを可能にするために使用することをお勧めします。 異なるアカウントからのロールを想定するには、ご利用の AWS アカウントが当該ロールにより信頼されており、信頼ポリシーに信頼できるエンティティとして定義されている必要があります。また、異なるアカウントでロールにアクセスするユーザーには、ロール ARN を指定したセキュア トークン サービス（STS）を持つポリシーが必要です。 監視するアカウント **1** で: • 必要なアクセス許可を持つ IAM ロールを作成します。VM モニタリングの場合、AmazonEC2ReadOnlyAccess が必要です。 • Role ARN（ロールARN）をコピーします。

©2023 Palo Alto Networks, Inc.

	• ユーザーを作成して、アカウント 2 のアカウント ID を、信頼できるエンティティとして追加します。これにより、アカウント 2 がこのロールを使って、アカウント 1 内のリソースにアクセスできるようになります。 アカウント **1** へのアクセスが必要なアカウント **2** で • 次のポリシーを STS アクセス許可付きでアタッチして、ロール ARN をアカウント 1 で作成したものと一致するように変更します。 `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource":"arn:aws:iam::012347211234:role/ PAN-OS-assume-role" } }`
Panorama での入力	• **Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **IAM Role**（**IAM** ロール）で、アカウント 2 のユーザーに対する **Access Key ID**（アクセス キー **ID**）および**Secret Access Key**（秘密アクセス キー）を入力します。 • **Panorama** > **Plugins**（プラグイン） > **AWS** > **Monitoring Definitions**（モニタリング定義）で、監視する AWS アカウント 1 の **Role ARN**（ロール **ARN**）を入力します。
オプション **3:**インスタンス プロファイル	
必要なロールとアクセス許可	AWS 上に EC2 インスタンスとして Panorama がデプロイされている場合のみ *AWS* 管理コンソールを使って *IAM* ロールを作成する場合、ロールと同じ名前でインスタンス プロファイルが自動的に作成されることに注意してください。ロールとインスタンス プロファイルが同じ名前を持っているため、*IAM* ロールを持つ *Panorama*（*EC2* インスタンス）を起動する場合、同名のインスタンス プロファイルがそれに関連付けられます。 Panorama と監視対象リソースがすべて単一の AWS アカウントに存在する場合。 AmazonEC2ReadOnlyAccess を持つ IAM ロールを作成します。
Panorama での入力	**Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **IAM Role**（**IAM** ロール）で、オプションとして **Instance Profile**（インスタンス プロファイル）を選択します。
オプション **4:Assume Role**（想定ロール）を持つインスタンス プロファイル	

©2023 Palo Alto Networks, Inc.

必要なロールとアクセス許可	Panorama と監視対象リソースが複数の異なる AWS アカウントにデプロイされている場合、想定ロールを持つインスタンス プロファイルを使用します。 Panorama HA の場合、両方の Panorama ピアに同じインスタンス プロファイルをアタッチしてください。 **EC2** インスタンスがデプロイされているアカウント **1** で: • IAM ロールを作成します。 • このロールに、Panorama が信頼できるエンティティとしてデプロイされている、AWS アカウント の ID（アカウント 2）を追加します。 • 前述のように、VM モニタリング用に JSON ポリシーをアタッチします。 • ロール ARN をコピーします。このロールは、Panorama が EC2 インスタンスまたは EKS クラスタで、メタデータを取得するために必要です。 **Panorama** をデプロイしたアカウント **2** で: • IAM ロールを作成して、JSON ポリシーをアタッチします（アカウント 1 から取得した STS ポリシーとリソース ARN を利用）。 • 監視する各 AWS アカウントに対して、同じ STS ポリシーをコピーして、ロール ARN を変更します。
Panorama での入力	• **Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **IAM Role**（**IAM** ロール）で、オプションとして **Instance Profile**（インスタンス プロファイル）を選択します。 • **Panorama** > **Plugins**（プラグイン） > **AWS** > **Monitoring Definitions**（モニタリング定義）で、監視する AWS アカウントの **Role ARN**（ロール **ARN**）を入力します。 たとえば、この例の Account 1 です。

AWS プラグインのインストールとアップグレード

AWS 上の EC2 インスタンスのモニタリングを開始するためには、互換性マトリックスを参照して、VM モニタリングをサポートするために必要な AWS 用 Panorama プラグインおよび VM-Series プラグインのバージョンを確認してください。

インストールされている AWS 用 Panorama プラグイン バージョン 1.0.1 をバージョン 2.0.x にアップグレードするには、まずバージョン 2.0.x に必要なバージョンの Panorama と VM-Series プラグインにアップグレードしてから、以下の説明に従ってインストール、アップグレードを実行します。

AWS プラグイン v2.0 をインストールしたら、v1.0 にダウングレードすることはできません。

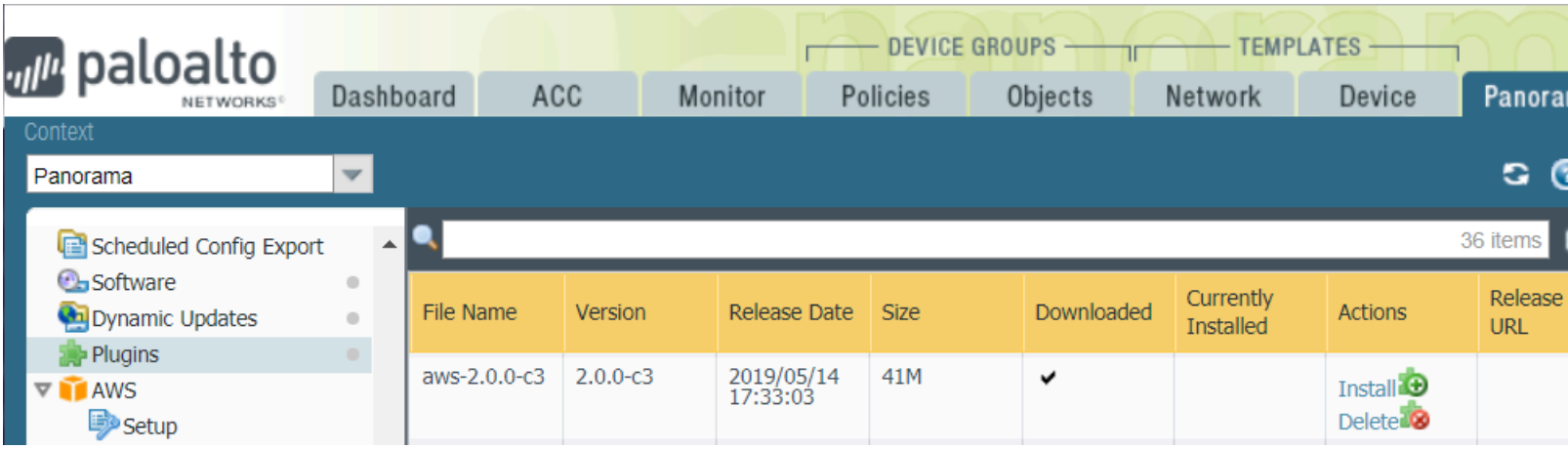
Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール/アップグレード作業を繰り返してください。

©2023 Palo Alto Networks, Inc.

予定されているメンテナンス期間に、プラグインをインストールまたはアンインストールしてください。

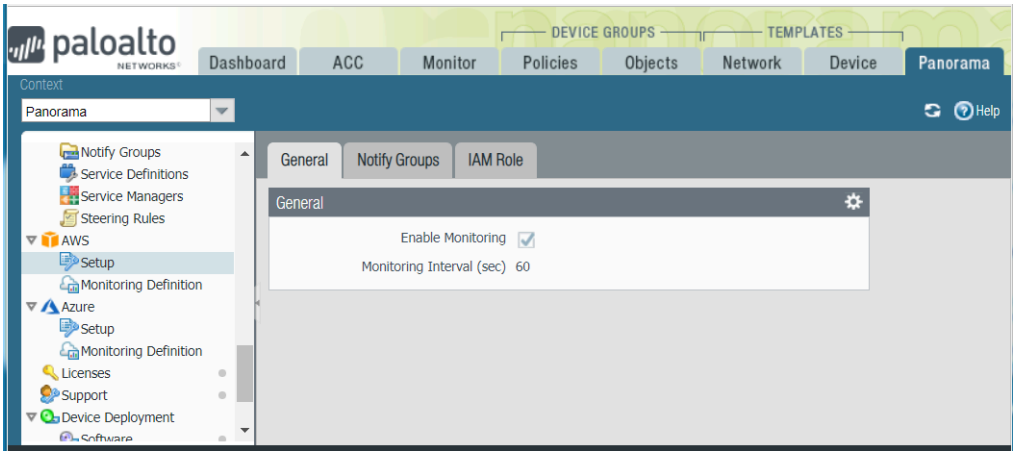
現在クラウド プラットフォームに *Panorama* プラグインがインストールされている場合、別のプラグインをインストール（あるいはアンインストール）する際に、変更をコミットするために *Panorama* の再起動が必要になります。

STEP 1 | Panorama Web インターフェイスにログインし、**Panorama** > **Plugins**（プラグイン）を選択して**Check Now**（今すぐチェック）をクリックし、VM モニタリングをサポートしているバージョンの **AWS**プラグインを入手します。



STEP 2 | **Download and Install**（ダウンロードおよびインストール）を選択し、プラグインをダウンロード、インストールします。

インストールが正常に完了したら Panorama が更新され、**Panorama** > **Plugins**（プラグイン）タブに AWS プラグインが表示されます。



Panorama の ***Dashboard***（ダッシュボード） *General Information*（全般情報）ウィジェットで、インストールされている *AWS* 用 *Panorama* プラグインのバージョンを確認することができます。

©2023 Palo Alto Networks, Inc.

STEP 3 | （HA 状態の Panorama）**Commit**（コミット） > **Commit to Panorama**（**Panorama** にコミット）を選択します。

HA 状態の Panorama の場合、変更内容を Panorama 設定にコミットして、フェイルオーバー時に Panorama ピアにタグが登録されているようにします。

VM モニタリング用 AWS プラグインを設定

AWS パブリック クラウドのデプロイ環境で仮想マシンの監視を始めるためには、AWS プラグインのインストール後、モニタリング定義を作成する必要があります。この定義は、監視する AWS VPC 内の EC2 インスタンスにアクセスする権限を持つ IAM ロール、Panorama が取得した IP アドレス対タグのマッピングのプッシュ先となるファイアウォールを含む通知グループを指定します。ポリシーを適用するためには、その後でダイナミック アドレス グループを作成し、それらをセキュリティポリシー内で参照する必要があります。ダイナミック アドレス グループにより、ファイアウォールが各タグに登録されているパブリックおよびプライベート IP アドレスを取得してから、定義済みのポリシールールに基づいてワークロードを出入りするトラフィックに対してアクセスを許可あるいは拒否できるよう、マッチさせたいタグをフィルタリングすることができます。

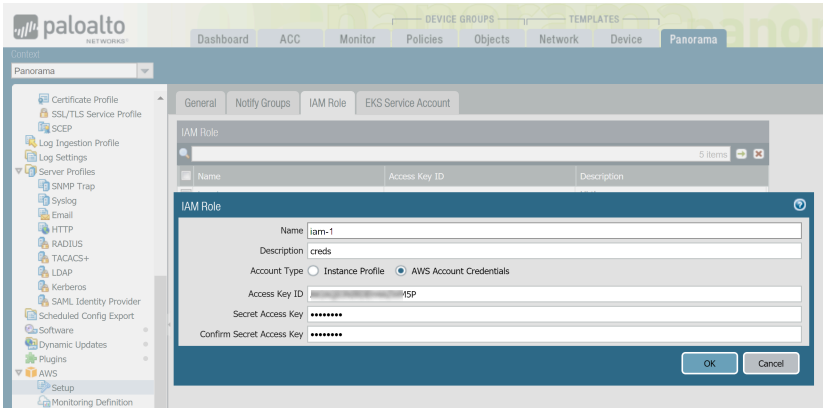
STEP 1 | Panorama Web インターフェイスにログインします。

STEP 2 | 次のオブジェクトをセットアップし、AWS 上の VM モニタリングを有効化します。

- IAM ロールを追加します。

  IAM ロールとは、Panorama が代理で AWS のリソース（EC2 インスタンスとしてデプロイされた仮想マシン）に対してサービス リクエストを行えるよう、アクセスを移譲できるようにするエンティティです。

  1. **Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **IAM Role**（**IAM** ロール） > **Add**（追加）を選択します。

  2. IAM ロールを識別する**Name**（名前）および任意で**Description**（説明）を入力します。
  3. Account Type（アカウント タイプ）を選択—**Instance Profile**（インスタンス プロファイル）または **AWS Account Credentials**（**AWS** アカウント認証情報）を選択します。Panorama が AWS にデプロイされている場合、適切なアクセス許可を持つプロファイル インスタンスを Panorama にアタッチする、または Panorama 上の IAM ロールに関連する認証情報を追加することができます。Panorama が AWS 上にデプロイさ

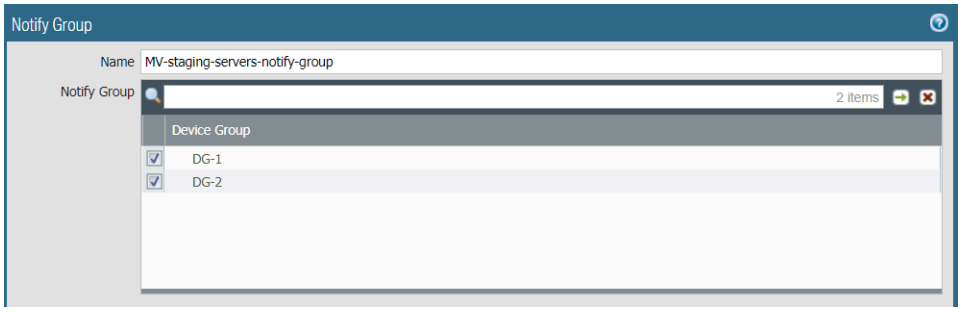
©2023 Palo Alto Networks, Inc.

れていない場合、Panorama でローカルに IAM ロールの認証情報を入力する必要があります。

4. （AWS アカウント認証情報のみ）**Secret Access Key**（秘密アクセスキー）を入力し、確認用に再び入力します。次に **OK** をクリックします。

- 通知グループを追加します。

1. **Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **Notify Groups**（通知グループ） > **Add**（追加）を選択します。



2. Panorama が取得した VM 情報のプッシュ先にするファイアウォールのグループを示す **Name**（名前）を入力します。
3. Panorama が AWS VPC から取得した VM 情報（IP アドレス対タグのマッピング）のプッシュ先にするファイアウォールのグループあるいは仮想システムである**Device Groups**（デバイスグループ）を選択します。ファイアウォールは、更新を使用してポリシーで参照しているダイナミック アドレス グループを構成する最新メンバー リストを決定します。Azure 用の Panorama プラグインを使用している場合、両方の環境のタグと同じファイアウォールや仮想システムをターゲットにすることができます。

   デバイスグループはよくご検討ください。

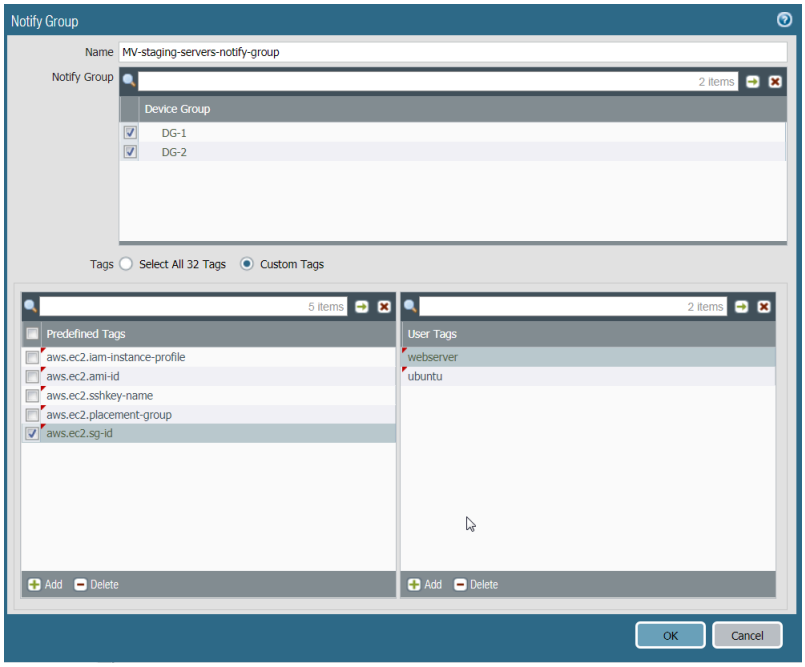
   - モニタリング定義に含められる通知グループは一つだけであるため、通知グループ内の関連するデバイスグループをすべて選択するようにしてください。通知グループに含まれるファイアウォールに *Panorama* がプッシュしたタグを登録解除する場合、モニタリング定義を削除する必要があります。
   - 複数の仮想システムで有効なファイアウォール上のすべての仮想システムにタグを登録するためには、各仮想システムを *Panorama* 上の別のデバイスグループに追加し、デバイスグループを通知グループに割り当てる必要があります。すべての仮想システムを単一のデバイス グループに割り当てる場合、*Panorama* はタグをファイアウォール上の *1* つの仮想システムにのみ登録します。

4. AWS VPC から取得するタグを選択します。

   Select All 32 Tags（32 個のタグをすべて選択）（デフォルト）を使用するか、インスタンスのために取得する **Custom Tags**（カスタム タグ）を選択できます。Custom

©2023 Palo Alto Networks, Inc.

Tags（カスタム タグ）オプションを使用する場合は、使用する事前定義タグとユーザー定義タグをセキュリティ ポリシーの一致条件として **Add**（追加）できます。多数の EC2 インスタンスを監視している場合は、取得するタグの数を減らすと、Panorama の CPU とメモリー容量を効率的に使用できます。ガイドラインについては、「AWS 上の VM モニタリングのためのチェックリストのプランニング」を参照してください。



- プラグイン上で監視が有効化されていることを確認します。Panorama が AWS パブリック クラウドと通信して VM モニタリングを行うために、この設定を有効化する必要があります。

  Enable Monitoring（監視の有効化）チェックボックスは、**Panorama** > **Plugins**（プラグイン） > **AWS** > **Setup**（セットアップ） > **General**（一般）にあります。

STEP 3 | 監視する各 VPC に対して、**Monitoring Definition**（モニタリング定義）を作成します。

新しいモニタリング定義を追加すると、デフォルトで有効になります。

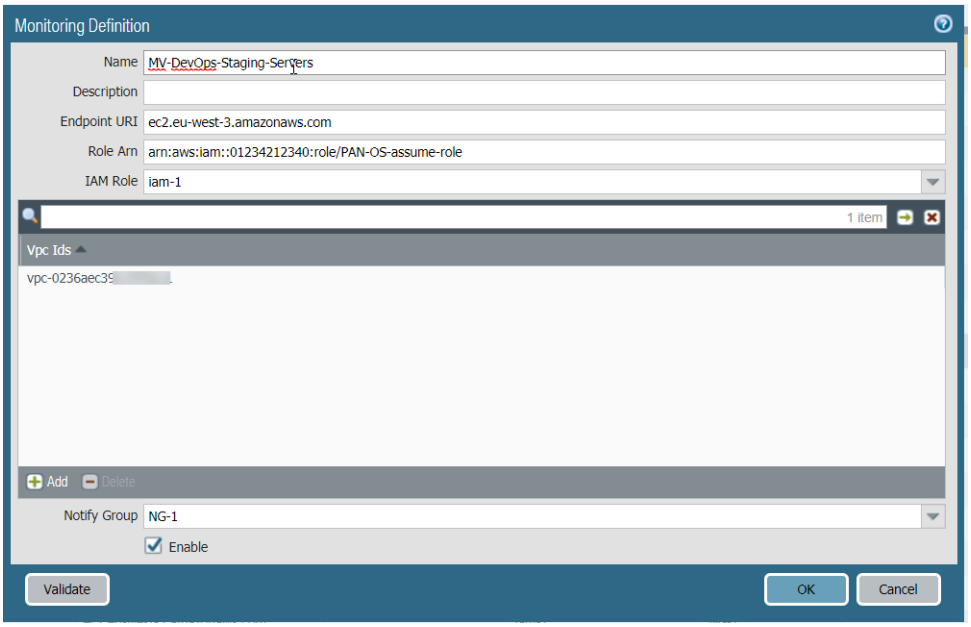
- **Panorama** > **Plugins**（プラグイン） > **AWS** > **Monitoring Definition**（モニタリング定義）を選択し、新しい定義を**Add**（追加）します。
- この定義を使用する AWS VPC を識別する**Name**（名前）、および任意で**Description**（説明）を入力します。
- **Endpoint URI**（エンドポイント **URI**）を入力します。構文は ec2.<your_region>.amazonaws.com です

  AWS China の場合は ec2.<your region>.amazonaws.com.cn です。
- （任意）AWS STS API を使用して同一アカウント内またはクロスアカウントの AWS リソースにアクセスするための権限が含まれている一時認証情報を使用してロールの連鎖

©2023 Palo Alto Networks, Inc.

と IAM ロールをセットアップしている場合は、**Role ARN**（ロール **ARN**）を入力します。ロール ARN は、監視する VPC に所属している必要があります。

- **IAM Role**（**IAM** ロール）を選択し、AWS 管理コンソールの VPC Dashboard（VPC ダッシュボード）から **VPC ID** を **Add**（追加）して、**Notify Group**（グループへ通知）します。



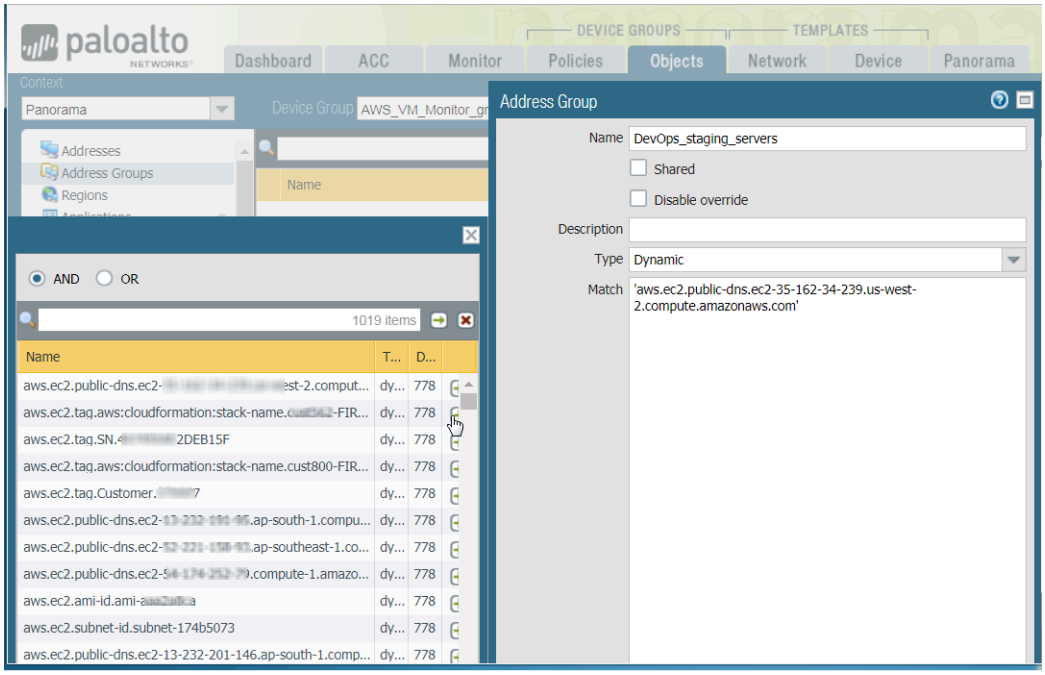
STEP 4 | Panorama 上の変更を**Commit**（コミット）します。

モニタリング定義のステータスが Success（成功）と表示されることを確認します。失敗する場合、AWS VPC ID を正しく入力し、アクセスを検証するための正しいキーおよび ID を指定しているかどうか確認してください。

Validate（検証）をクリックして、*Panorama* が *IAM* ロールとキーを使って認証を行えること、そして上記で入力した *AWS VPC* と通信できることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 5 | Panorama 上で VM 情報を閲覧できることを確認し、ダイナミック アドレス グループ用の一致条件を定義します。



HA フェイルオーバーの際、新たにアクティブになった *Panorama* が *AWS* クラウドに再接続してすべてのモニタリング定義のタグを取得しようと試みます。設定・有効化しているどのモニタリング定義にも *Panorama* が再接続できない場合、*Panorama* は次のシステム ログのメッセージを生成します

```
Unable to process accounts after HA switch-over; user-intervention required.
```

これが発生した場合、*Panorama* にログインしてモニタリング定義を確認し、無効な認証情報を修正したり、無効なアカウントを削除したりする必要があります。*Panorama* が *AWS* クラウドに接続されていなくても、フェイルオーバーの前にすでに取得しているモニタリング定義用のタグはすべて保持され、ファイアウォールはその *IP* アドレスのリストに対してポリシーを適用し続けることができます。*Panorama* は、モニタリング定義を削除する際にのみ、アカウントに関連するすべてのタグを削除します。ベストプラクティスとして、アクション中心のHTTPS 宛先へのログ転送を設定して即座に対応できるようにすることで、この問題を監視できます。

©2023 Palo Alto Networks, Inc.

STEP 6 | トラブルシューティングのために、AWS plugin on Panorama に関連するログがどこにあるかを確認してください。

- 利用可能なすべてのログを表示するには、CLI コマンド **less plugins-log** を使用します。

  plugin_aws_ret.log には、IP アドレスとタグの取得に関連するログが記載されています。

  plugin_aws_proc.log には、登録されている IP アドレスとタグの処理に関連するログが記載されています。

  plugin_aws.log には、AWS プラグイン設定とデーモンに関連するログが記載されています。

モニタリング定義のステータスについては、**show plugins aws vm-mon-status** を使用してください。

```
admin@Panorama> show plugins aws vm-mon-status
Mon-Def Name      VPC           Status  Last Updated Time
 Error Msg
------------------------------------------------------------------------------
MD-Ins-Prof-ARN  vpc-07986b091  Success 2019-12-02T10:24:56.007000
MD-gov           vpc-7ea1cf1a   Success 2019-12-02T10:24:56.008000
MD-IAM-ARN       vpc-025a83c123 Success 2019-12-02T10:24:56.012000
```


©2023 Palo Alto Networks, Inc.

Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング

AWS 用 Palo Alto Networks オートスケーリング テンプレートは、AWS 内にデプロイされたアプリケーションを保護するための、VM-Series ファイアウォールの設定とデプロイを行うために役立ちます。アプリケーション ワークロード リソースの需要の急増に対応できるように、このテンプレートは AWS のスケーラビリティ機能を使用して、AWS 内にデプロイされている VM-Series ファイアウォールを自動的かつ個別にスケーリングします。

- VM-Series の自動化機能には、PAN-OS API とブートストラップ機能（バージョン 2.0 ではブートストラップ ファイルを使用し、バージョン 2.1 では Panorama を使用）などがあります。
- AWS 自動化テクノロジーには、AWS サービス（Lambda、自動スケーリング グループ（ASG）、Elastic Load Balancing（ELB）、S3、SNS など）向けの CloudFormation テンプレートとスクリプトなどがあります。

これらのテンプレートは、Palo Alto Networks GitHub リポジトリ（AWS の VM-Series ファイアウォールのオート スケーリングのためのリポジトリ）から入手できます。

- バージョン 2.0 には、ファイアウォール テンプレートとアプリケーション テンプレートが含まれています。これらのテンプレートとサポート スクリプトは、VM-Series ファイアウォール、内部ファイアウォール、およびアプリケーションを 1 つまたは複数の Virtual Private Cloud（VPC）にデプロイします。

  バージョン 2.0 ではファイアウォール テンプレートがサポートされ、アプリケーション テンプレートはコミュニティでサポートされるようになりました。デプロイメントの詳細については、「AWS 用 VM-Series Auto Scale テンプレート（v2.0）」を参照してください。
- バージョン 2.1 では、1 つの VPC へのデプロイメントがサポートされ、またロード バランサー サンドイッチ トポロジのサポートが追加されました。このトポロジでは、フロントエンド VPC に VM-Seriesファイアウォールをデプロイし、VPC ピアリングまたは AWS PrivateLink で接続されている 1 つ以上のアプリケーション VPC にバックエンド アプリケーションをデプロイできます。

  バージョン 2.1 は、VPC でアプリケーション ロード バランサー（ALB）とネットワーク ロード バランサー（NLB）の両方を実装できます。バージョン 2.1 には、2 種類のファイアウォール テンプレートと 5 種類のアプリケーション テンプレートが用意されています。デプロイメントの詳細については、「AWS バージョン 2.1 用 VM-Series オート スケーリングテンプレート」を参照してください。

既存のテンプレート デプロイメントがある場合、移行手順はありません。

次の表では、各テンプレート バージョンのいくつかの高レベル機能を比較します。

©2023 Palo Alto Networks, Inc.

機能/要件	バージョン 2.0	バージョン2.1
PAN-OS 9.0.1 以降のリリースは Panorama モードで動作する Panorama。 高可用性（*HA*）設定の *Panorama* はサポートされていません。	（任意）Panorama を使用する場合は、VM-Series ファイアウォール VPC とアプリケーション VPC の間で VPC ピアリングを設定する必要があります。ピアリングされたトラフィックはパブリック インターネットを通過します。	（必須）バージョン 2.1 のテンプレートをデプロイします。 *Panorama* では、*VM-Series* ファイアウォールがオート スケーリング用の *PAN-OS* メトリックを公開できるようにするため、*VM-Series* プラグインを手動でインストールする必要があります。
Bootstrapping	S3 バケットの `bootstrap.xml` 設定ファイル。	Panorama の `init-cfg.txt` ファイル。
Palo Alto Networks S3 バケット サンプル	各自の S3 バケットを使用するか、または panw-aws-autoscale-v20-us-west-2 にあるサンプルを使用します。	デプロイメントに各自の S3 バケットを使用します。
シングル VPC または複数の個別 VPC（ハブ アンド スポーク）	はい	あり。
新しい VPC	はい	あり。
既存の VPC（茶色のフィールド）	無し	あり。

©2023 Palo Alto Networks, Inc.

機能/要件	バージョン 2.0	バージョン2.1
VPC あたりの可用性ゾーンの数	2	2-4
外部ロード バランサー	ALB のみ	ALB または NLB
内部ロード バランサー	NLB のみ	ALB または NLB
VM-Series ファイアウォール VPC とバックエンド サーバーへの AWS Private Link 接続。	無し	あり。

テンプレートの詳細については、以下のセクションを参照してください。

- AWS バージョン 2.0 用 VM-Series Auto Scale テンプレート
- AWS バージョン 2.1 用 VM-Series オート スケーリングテンプレート

AWS バージョン 2.0 用 VM-Series Auto Scale テンプレート

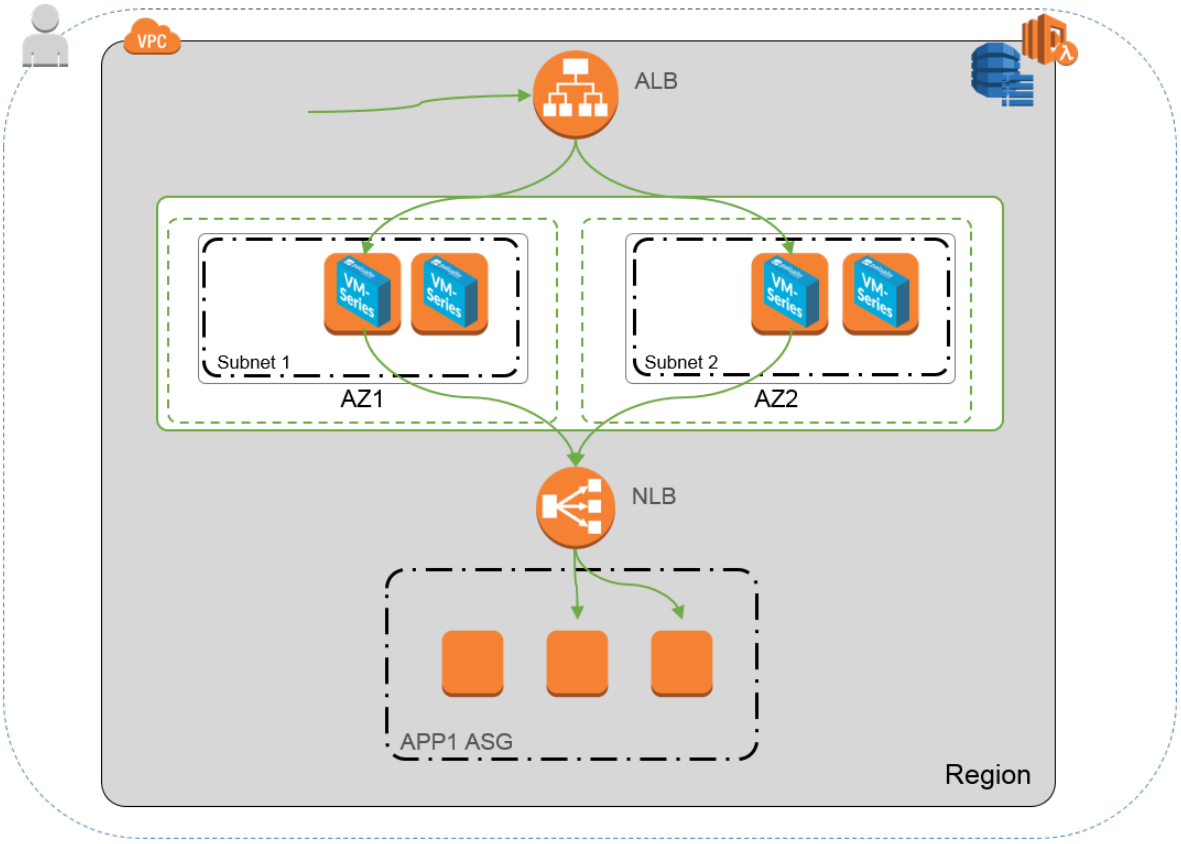
規模が増大したアプリケーションの管理を容易にするため、VM-Series ファイアウォールの Auto Scaling テンプレート バージョン 2.0 は、デプロイメントを簡素化するハブ アンド スポーク アーキテクチャを提供します。このソリューションのバージョンは、単独の AWS アカウント内や複数の AWS アカウントに渡ってシングル VPC とマルチ VPC デプロイメントをサポートする 2 つのテンプレートを提供します。

- ファイアウォール テンプレート – ファイアウォール テンプレートは、アプリケーション ロード バランサー（ALB）と VM-Series ファイアウォールを、2 つの可用性ゾーン（AZ）に渡るオート スケーリング グループ内でデプロイします。このインターネットに接続されているALBは、VPC に入るトラフィックを VM-Series ファイアウォール プール内で分配しま

©2023 Palo Alto Networks, Inc.

す。VM-Series ファイアウォールは、オート スケーリングを可能にするカスタム PAN-OS メトリックを自動的に公開します。

Palo Alto Networks ではファイアウォール テンプレートを公式サポートしており、有効なサポート資格を持っていれば Palo Alto Networks のテクニカル サポートを受けることができます。



次のアプリケーション テンプレートは、上の図に示されているネットワーク ロード バランサーをデプロイします。

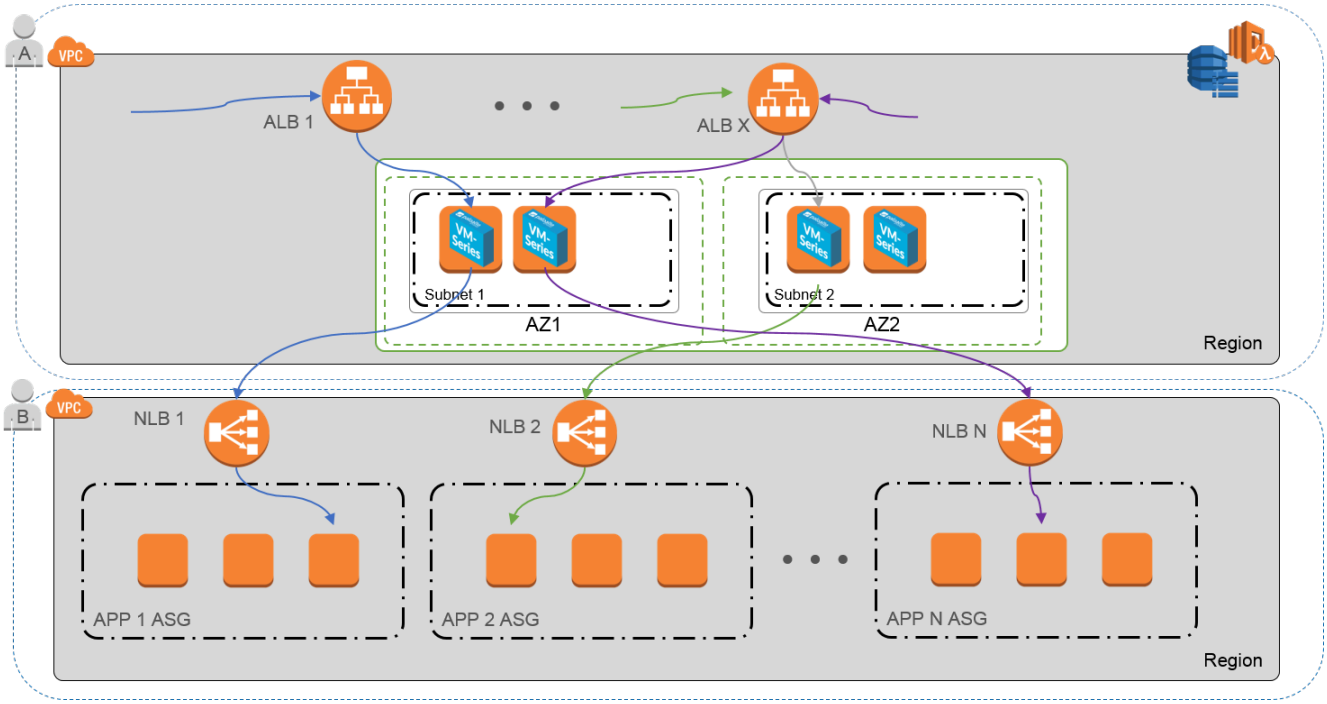
- アプリケーション テンプレート – アプリケーションは、ネットワーク ロード バランサー（NLB）と 1 台の Web サーバーで構成される 1 つのオート スケーリング グループ（ASG）を各 AZ にデプロイします。

  アプリケーション テンプレートは、コミュニティでサポートされます。このテンプレートは、基本的な Web アプリケーションの作成を支援するための例として提供されています。本番環境では、自分で作成したアプリケーション テンプレートを使用するか、もしくは要件に合わせてこのテンプレートをカスタマイズしてください。

これらのテンプレートにより、インターネットに接続されたALBと内部NLBを使用したロード バランサーのサンドイッチ トポロジをデプロイできます。インターネットに接続されたALBは、インターネットからアクセスでき、VPC に入るトラフィックを VM-Series ファイアウォール プール内で分配します。ファイアウォールは、NATポリシーにしたがってトラフィックをNLB（1つまたは複数）に分配し、内部ネットワーク ロード バランサーはトラフィックをWebまたはアプリケーション サーバーのオート スケーリング層に分配します。VM-Series ファイアウォールは、カスタム PAN-OS メトリックを AWS CloudWatch に公開します。CloudWatch サービス

©2023 Palo Alto Networks, Inc.

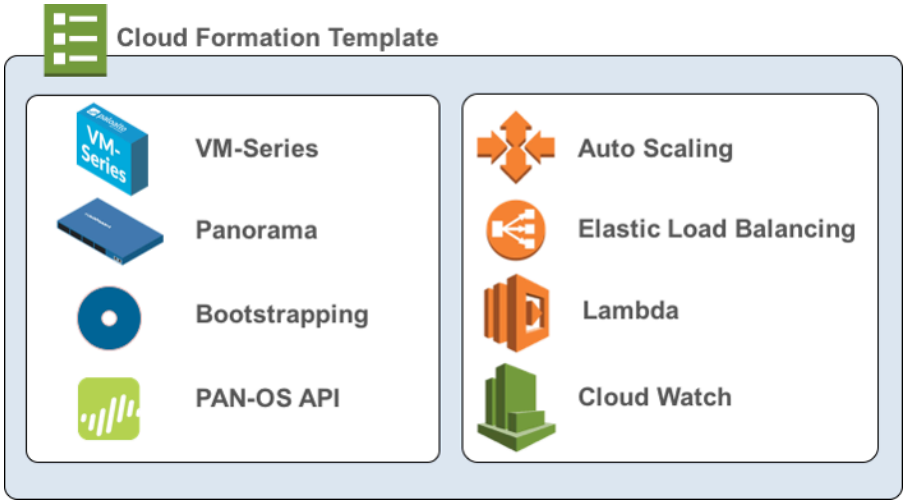
は、VM-Series ファイアウォール上でヘルスとリソース ロードを監視し、その情報を使用して、ファイアウォールの適切なASGでオート スケーリング イベントをトリガします。



- AWS 用 VM-Series Auto Scaling テンプレート（v2.0） で使用されるコンポーネント
- AWS 用 VM-Series Auto Scaling テンプレート（v2.0） でのダイナミック スケーリング
- AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の計画
- 起動前のファイアウォール テンプレートのカスタマイズ（v2.0）
- AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動
- bootstrap.xml ファイル（v2.0）のカスタマイズ
- AWS 用 VM-Series Auto Scaling テンプレート（v2.0）によるスタックの更新
- 管理者アカウントの変更とスタックの更新

©2023 Palo Alto Networks, Inc.

AWS 用 VM-Series Auto Scaling テンプレート（v2.0） で使用されるコンポーネント



AWS 用 VM-Series Auto Scaling テンプレートの構成要素を以下に示します。

構成要素	概要
ファイアウォール テンプレート （Palo Alto Networks が公式にサポートするテンプレート）	`firewall-v2.0.template` では、新しい VPC とサブネット ルート テーブル、AWS NAT ゲートウェイ、2 つの可用性ゾーン（AZ:Availability Zones）、およびこれらの AZ 間でトラフィックをルーティングするために必要なセキュリティ グループがデプロイされます。このバージョン 2.0 テンプレートでは、外部 ALB、および各 AZ 内に VM-Series ファイアウォールを持つ ASG もデプロイされます。 プロダクション環境にはさまざまなバリエーションが存在しています。これには、サブネット、可用性ゾーン、ルート テーブル、およびセキュリティ グループなどの特定のコンポーネント数が含まれますが、これに限定されるものではありません。`firewall-v2.0.template`は、新しい VPC 内にデプロイする必要があります。 *AWS 用 VM-Series Auto Scaling* テンプレートでは、*Panorama* はデプロイされません。*Panorama* は省略可能です。*Panorama* では、ポリシーを簡単に管理したり、情報を一元的に確認したりできます。*Panorama* を使用して、ソリューションでデプロイされる *VM-Series* ファイアウォールを管理する場合、*M-Series* アプライアンス、または企業ネットワーク内のサーバーで *Panorama* バーチャル アプライアンスを使用できます。あるいは、*AWS* 上で *Panorama* 仮想アプライアンスを使用することができます。 このソリューションには、AWS NAT ゲートウェイが含まれています。AWS NAT ゲートウェイは、ファイアウォールがアウトバウン

©2023 Palo Alto Networks, Inc.

構成要素	概要
	ド リクエストを開始して、更新を取得したり、Panorama に接続したり、AWS CloudWatch にメトリックを通知したりするために使用されます。
アプリケーション テンプレート （コミュニティでサポートされるテンプレート）	アプリケーション テンプレートでは、NLB と、Web サーバーを含む ASG が各 AZ にデプロイされます。NLBは各AZに固有のIPアドレスを持っており、ファイアウォールのNATポリシールールは単一のIPアドレスを参照する必要があるため、2つのAZにはそれぞれ1つのASGが存在します。ASG 内のすべてのファイアウォールが同じ設定を使用します。 バージョン 2.0 の Auto Scaling ソリューションには、以下の 2 つのアプリケーション テンプレートが含まれています。 • `panw_aws_nlb-v2.0.template`を利用すると、ファイアウォール テンプレートをデプロイしたのと同じ VPC 内にアプリケーション テンプレート リソースをデプロイできます（同じ AWS アカウント）。 • `panw_aws_nlb_vpcv-2.0.template`では、同じ AWS アカウントまたは複数の AWS アカウントを使って、別々の VPC にアプリケーション テンプレート リソースをデプロイできます。
Lambda 関数	AWS Lambda は、堅牢なイベント駆動型の自動化を提供します。複雑なオーケストレーション ソフトウェアは必要ありません。`firewall-v2.0.template` で AWS Lambda は、Simple Queue Service（SQS）をモニターし、キューに通知される NLB について確認します。Lambda 関数は新しい NLB を検出すると、新しい NAT ポリシー ルールを作成して、ASG 内の VM-Series ファイアウォールに適用します。ファイアウォールは、アプリケーションごとに NAT ポリシー ルールを設定しています。また、ファイアウォールは、（ポートをNLB の IP アドレスにマップする）NAT ポリシー ルールを使用して、アプリケーション Web サーバーの前にある NLB にトラフィックを転送します。 デプロイメントのアプリケーション トラフィックを許可または拒否するセキュリティ ポリシー ルールを作成する必要があります。サンプルの ***bootstrap.xml*** ファイルには、セキュリティ ポリシー ルールは含まれていません。ファイアウォールを一元管理して、セキュリティ ポリシー ルールを簡単に作成するために、*Panorama* を使用する必要があります。 その他の追加機能があります。 • ファイアウォールの起動時または終了時に、インターフェイス（ENI）を追加または削除する。

©2023 Palo Alto Networks, Inc.

構成要素	概要
	• スタックの削除またはインスタンスの終了時に、関連リソースをすべて削除する。 • スケール イン イベント発生時に、Panorama のマネージド デバイスとしてファイアウォールを削除する。 • スケール イン イベントの結果、ファイアウォールが終了した場合、BYOL ライセンスを非アクティブ化する。 Lambda 関数の詳細は、**http://paloaltonetworks-aws-autoscale-2-0.readthedocs.io/en/latest/** を参照してください
ブートストラップ ファイル GitHub リポジトリで提供されている bootstrap.xml ファイルは、テストと評価のみを目的としています。実稼働デプロイメントでは、起動前に bootstrap.xml 内のサンプル認証情報を変更する必要があります。	このソリューションでは、init-cfg.txt ファイルと bootstrap.xml ファイルが必要です。これは、VM-Series ファイアウォールがトラフィック処理用の基本設定を持つようにするためです。 • **`init-cfg.txt`** ファイルには、ファイアウォールのプライマリ インターフェイス（eth0）でデータプレーン トラフィックを受信できるようにする mgmt-interface-swap 操作コマンドが含まれます。Auto Scaling ソリューションでは、データプレーンと管理インターフェイスをスワップし、ALB が Web トラフィックを VM-Series ファイアウォールの Auto Scaling 層に転送できるようにする必要があります。詳細は、「Amazon ELB で使用する管理インターフェイスのマッピング」を参照してください。 • **`bootstrap.xml`** ファイルにより、ファイアウォール ネットワーク インターフェイスの基本接続が使用可能になり、テンプレート起動時に入力されたスタック名に一致する AWS CloudWatch 名前空間にファイアウォールが接続できるようになります。

ソリューションをデプロイするには、「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動」を参照してください。

AWS 用 VM-Series Auto Scaling テンプレート（v2.0 および v2.1）でのダイナミック スケーリングの仕組み

スケール インおよびスケール アウトは、オート スケーリング テンプレート を使用してデプロイされた VM-Series ファイアウォールを使い、カスタム PAN-OS メトリックに基づいて行われます。VM-Series ファイアウォールは、これらのメトリックを Amazon CloudWatch コンソールにネイティブに公開します。スケーリング パラメータとして選択したメトリックに従って、AWS デプロイメント環境のアプリケーション トラフィックを管理して、インスタンスを動的にデプロイおよび終了するための CloudWatch アラームおよびポリシーを定義できます。

ファイアウォールは、5 分ごとに（デフォルト） AWS CloudWatch にメトリックを公開します。定義されている時間間隔で、監視対象メトリックが設定されているしきい値に達すると、CloudWatch はアラームをトリガーしてオート スケーリング イベントを開始します。

オート スケーリング イベントによって新しいファイアウォールのデプロイが行われると、新しいインスタンスは起動時にブートストラップされ、AWS Lambda 関数が NAT ポリシー ルール

©2023 Palo Alto Networks, Inc.

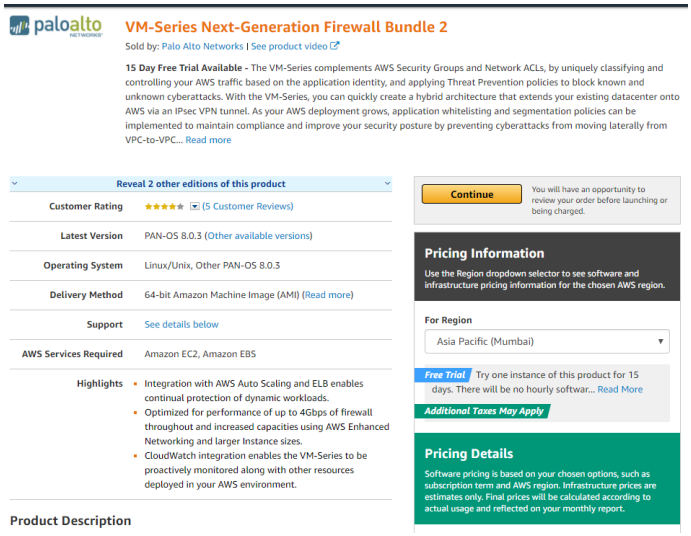
に従ってファイアウォールを設定します。各アプリケーションに対して NAT ポリシー ルールが作成されます。ルールは、デプロイ環境の各ネットワーク ロード バランサーの IP アドレスを参照します。アプリケーション ロード バランサーがリクエストを受け取ると、そのリクエストを、割り当てられている TCP ポート上のファイアウォールに転送します。ファイアウォールはトラフィックを調べてから、対応するネットワーク ロード バランサーにトラフィックを転送します。ネットワーク ロード バランサーは、リクエストをターゲット グループ内の Web サーバーに転送します。

AWS 用 VM-Series Auto Scaling テンプレート（v2.0 および v2.1）の計画

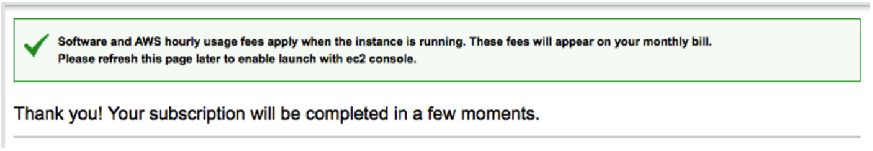
次のチェックリストには、このソリューションを実装するために実行する必要のあるアクションと選択の項目が記載されています。

テンプレート v2.0 および v2.1 用のプランニング チェックリスト	
❑ VM-Series Auto Scaling テンプレートをデプロイするための要件を確認する。	Auto Scaling テンプレートは、AWS Lambda と S3 署名バージョン 2 または 4 を必要とし、サポートされている バージョンの PAN-OS が動作している VM-Series ファイアウォールをデプロイできます。サポートされているリージョンと AMI ID のリストを探し、ファイアウォール テンプレートの入力として提供する必要があります。
❑ IAM ユーザー ロールの適切な許可を割り当てる。	このソリューションを正常に起動するには、VM-Series Auto Scaling テンプレートをデプロイするユーザーに管理者権限または iam-policy.json に記載されている許可が必要です。このファイルから許可をコピーして、新しい IAM ポリシーに貼り付け、ポリシーを新しいまたは既存の IAM ロールにアタッチします。 クロスアカウント デプロイの場合、異なる AWS アカウントにあるリソースにアクセスするには、アプリケーション テンプレートをデプロイするユーザーの IAM ロールにフル SQS アクセス許可と、ファイアウォール テンプレートに属する SQS キューへの書き込みを許可する信頼関係が必要です。
❑ クロスアカウント デプロイに必要な詳細情報を収集する。	ファイアウォール テンプレートとアプリケーション テンプレートが異なるアカウントにあるデプロイの場合、ファイアウォール テンプレート リソースをホストするアカウントが信頼するアカウントになり、アプリケーション テンプレート リソースを保持するもう一方の AWS アカウントが信頼されるアカウントになります。クロスアカウント デプロイのアプリケーション テンプレートを起動するには、以下の情報が必要です。 • アプリケーション テンプレートをデプロイするアカウントのクロスアカウント ロールの Amazon Resource Name（ARN）。 • 信頼するアカウントへのフル SQS アクセスを付与する IAM ロールの作成時に定義した外部 ID。 • アプリケーション テンプレートを起動する各 AWS アカウントの 10 桁のアカウント番号。ファイアウォール テンプレート リ

©2023 Palo Alto Networks, Inc.

テンプレート **v2.0** および **v2.1** 用のプランニング チェックリスト	
	ソースをホストするアカウントは、信頼するアカウントとして機能し、アプリケーション テンプレートのユーザーが必要とするリソースを所有しているため、ファイアウォール リソースにアクセスできる信頼される各アカウントのアカウント番号をリストする必要があります。
❑ Palo Alto Networks サポート ポータルでサポート アカウントの作成を行います（まだ作成していない場合）。	BYOL ライセンスまたは PAYG ライセンスを選択できます。 • BYOL の場合、VM-Series Auto Scaling テンプレートを起動する前に、認証コードを Palo Alto Networks サポート アカウントに登録し、ファイル名とともに認証コードをブートストラップ パッケージの認証コードとして `/license` フォルダに追加する必要があります。詳細は、「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動」または「ファイアウォール テンプレートの起動（v2.1）」を参照してください。 • PAYG の場合、VM-Series ファイアウォールを登録して、サポート資格をアクティベートする必要があります。
❑ （PAYG の場合のみ）エンド ユーザー使用許諾契約（EULA）を確認して同意する。 初めて AWS アカウントで VM-Series ファイアウォールを起動する場合に必要になります。	AWS Marketplace で、Palo Alto Networks を検索し、使用するバンドルを選択します。使用するバンドルの EULA に同意していない場合、VM-Series ファイアウォールのデプロイに失敗します。 • たとえば、**VM-Series Next Generation Firewall Bundle 2**（**VM-Series** 次世代ファイアウォール バンドル **2**）を検索します。 

 ©2023 Palo Alto Networks, Inc.

テンプレート **v2.0** および **v2.1** 用のプランニング チェックリスト	
	• **Continue**（続行）をクリックし、**Manual Launch**（手動起動）を選択します。契約確認して **Accept Software Terms**（ソフトウェア規約に同意）をクリックし、EULA に同意します。  ブラウザを閉じます。
☐ AWS Lambda、Python スクリプト、テンプレートにパブリック S3 バケットとプライベート S3 バケットのどちらを使用するのかを決定する。	Palo Alto Networks は、サポートされているリージョンのリストに記載されているすべての AWS リージョンでパブリック S3 バケットを提供します。これらの S3 バケットには、必要なすべてのテンプレート、AWS Lambda コード、ブートストラップ ファイルが含まれています。 *Palo Alto Networks* では、このソリューションを評価する場合にのみパブリック *S3* バケットのブートストラップ ファイルを使用することを推奨しています。実稼働デプロイの場合、ブートストラップ パッケージのプライベート *S3* バケットを作成する必要があります。 S3 バケットには `panw-aws-autoscale-v20-<region_name>` のように名前を付けます。たとえば、AWS リージョンがオレゴンの場合、バケットは panw-aws-autoscale-v20-us-west-2 のようになります。 プライベート S3 バケットを使用するには、テンプレート、AWS Lambda コード、ブートストラップ ファイルをダウンロードして、プライベート S3 バケットにコピーする必要があります。ファイアウォール テンプレートとアプリケーション テンプレートの両方に必要なすべてのファイルを 1 つの S3 バケットに配置することも、個別の S3 バケットに配置することもできます。

©2023 Palo Alto Networks, Inc.

テンプレート v2.0 および v2.1 用のプランニング チェックリスト

☐ テンプレート、AWS Lambda コード、ブートストラップ ファイルをダウンロードする。	• GitHub リポジトリから、ファイアウォール テンプレート（アプリケーション ロード バランサーと VM-Series ファイアウォール）をデプロイするためのファイルを取得します。
	
	VM-Series Auto Scaling テンプレートのバージョン間でファイルを組み合わせないでください。
	
	• テンプレートと Lambda コード：
	  • panw-aws.zip
	  • firewall-v2.X.template
	• ブートストラップ ファイル：
	  • init-cfg.txt
	  • bootstrap.xml
	
	このソリューションにバンドルされている bootstrap.xml ファイルは、開始をサポートするように設計されており、テストと評価のためにのみ提供されます。実稼働デプロイの場合、起動する前に bootstrap.xml を変更する必要があります。
	• iam-policy：このソリューションを正常に起動するには、VM-Series Auto Scaling テンプレートをデプロイするユーザーに管理者権限またはこのファイルに記載されている許可が必要です。
	
	Palo Alto Networks テクニカル サポートはファイアウォール テンプレートをサポートします。
	• GitHub リポジトリ バージョン 2.0 または 2.1 から、NLB と Web サーバーをデプロイするためのファイルを取得します：
	• テンプレート:
	  • pan_aws_nlb-2.X.template — ファイアウォール テンプレートをデプロイした VPC と同じ VPC（同じ AWS アカウント）内にアプリケーション テンプレート リソースをデプロイするには、このテンプレートを使用します。
	  • pan_aws_nlb_vpc-2.X.template — 異なる VPC にアプリケーション テンプレート リソースをデプロイするには、このテンプレートを使用します。このテンプレートでは、クロスアカウント デプロイをサポートする適切な許可があれば、リソースを同じ AWS アカウント内または異なる AWS アカウントにデプロイできます。
	  • pan_nlb_lambda.template—スケール アウト バックエンド Web サーバーに登録するために、トラフィックを多重化する AWS ネットワーク ロード バランサーを作成します。

©2023 Palo Alto Networks, Inc.

テンプレート **v2.0** および **v2.1** 用のプランニング チェックリスト	
	• Lambda コードと Python スクリプト。
❑ 実稼働環境の bootstrap.xml ファイルをカスタマイズする。	実稼働環境の安全性を確保するには、実稼働デプロイの一意の管理ユーザー名とパスワードを使用して bootstrap.xml ファイルをカスタマイズする必要があります。デフォルトのユーザー名/パスワードは pandemo/demopassword です。また、アプリケーション セキュリティ ニーズに合ったインターフェイス、ゾーン、セキュリティ ポリシー ルールを使用して最適なファイアウォール設定も作成します。
❑ Panorama を使用してロギング、レポート、ファイアウォール管理を一元化するかどうかを決定する。	Panorama は、管理を容易にするためのオプションで、ファイアウォール管理のベスト プラクティスです。このソリューションでデプロイされる VM-Series ファイアウォールのオート スケーリング層を管理する必要はありません。 Panorama を使用する場合は、AWS 上の Panorama バーチャル アプライアンスか、企業ネットワーク内の M-Serie アプライアンスまたは Panorama バーチャル アプライアンスを使用できます。 ***Panorama*** は ***Panorama*** モードで、管理専用モードでなければなりません。 ファイアウォールを Panorama に正常に登録するには、以下の詳細情報を収集する必要があります。 • Panorama の API キー — AWS Lambda で Panorama への API リクエストを行うことができるように、VM-Series Auto Scaling テンプレートを起動するときに API キーを入力する必要があります。実稼働デプロイの場合、API コール専用の個別の管理者アカウントを作成し、関連付けられた API キーを生成することをお勧めします。 • Panorama IP アドレス — 設定（init-cfg.txt）ファイルに IP アドレスを含める必要があります。ファイアウォールは、VPC からこの IP アドレスにアクセスできる必要があります。安全な接続を確保するには、ダイレクト コネクト リンクまたは IPSec トンネルを使用します。 • VM 認証キー — Panorama でファイアウォールを認証して、各ファイアウォールを管理対象デバイスとして追加できるようにします。設定（init-cfg.txt）ファイルにこのキーを含める必要があります。 VM 認証キーは、デプロイの有効期限が切れるまで必要になります。接続リクエストに有効なキーがない場合、VM-Series ファイアウォールを Panorama に登録できません。キーの詳細は、「Panorama で VM 認証キーを生成」を参照してください。

©2023 Palo Alto Networks, Inc.

テンプレート **v2.0** および **v2.1** 用のプランニング チェックリスト	
	• ファイアウォールを割り当てるテンプレート スタック名とデバイス グループ名 – まず、テンプレートを追加してテンプレート スタックに割り当て、Panorama でデバイス グループを作成し、テンプレート スタック名とデバイス グループ名を設定（init-cfg.txt）ファイルに含める必要があります。 コストの削減と *Elastic IP* アドレスの使用のスケーリング制限の緩和のために、ファイアウォールにはパブリック *IP* が設定されません。*Panorama* を使用してファイアウォールを管理しない場合は、*VPC* 内の信頼されないサブネットに接続して *VM-Series* ファイアウォールへの *SSH/HTTPS* アクセスを可能にするジャンプ サーバー（*EIP* アドレスを持つ要塞ホスト）をデプロイしなければなりません。このソリューションには、アウトバウンド リクエストを開始して、更新の取得、*Panorama* への接続、*AWS CloudWatch* へのメトリックの公開を行うためにファイアウォールで使用される *AWS NAT* ゲートウェイがデフォルトで含まれています。
開始する。	AWS 用 VM-Series Auto Scaling テンプレート（v2.0）を起動します

起動前のファイアウォール テンプレートのカスタマイズ（**v2.0** および **v2.1**）

デプロイメント ワークフローを簡素化するため、ファイアウォールでは、テンプレートの起動時に入力する必要があるパラメータの一部が表示されます。テンプレートに含まれる別のオプションを表示してカスタマイズする場合は、AWS 用 VM-Series Auto Scaling テンプレート（v2.0）または（2.1）を起動する前に、メモ帳や Visual Studio Code などのテキスト編集ツールを使用して、お好みの値を指定できます。

AWS 用のオート スケーリング ファイアウォール テンプレートをデプロイする際にカスタマイズできるパラメータは、以下の表で確認してください。このリストのパラメータの変更は、購入していただいたサポート オプションに基づき、Palo Alto Networks の公式サポート ポリシーに含まれます。

パラメータ	概要	デフォルト値
CIDR Block for the VPC（VPC の CIDR ブロック）	VPC に使用する IP アドレス空間。 以下で変更するサブネットは、この *VPC CIDR* ブロックに属する必要があり、なおかつ一意である必要があります。	192.168.0.0/16

©2023 Palo Alto Networks, Inc.

パラメータ	概要	デフォルト値
Management Subnet CIDR Block（管理サブネット CIDR ブロック）	ファイアウォールの管理サブネットの CIDR ブロックをコンマ区切りで列挙したリスト。	192.168.0.0/24, 192.168.10.0/24
Untrust Subnet CIDR Block（信頼されないサブネット CIDR ブロック）	信頼されないサブネットの CIDR ブロックをコンマ区切りで列挙したリスト。	192.168.1.0/24, 192.168.11.0/24
Trust Subnet CIDR Block（信頼されるサブネット CIDR ブロック）	信頼されるサブネットの CIDR ブロックをコンマ区切りで列挙したリスト。	192.168.2.0/24, 192.168.12.0/24
NAT Gateway Subnet CIDR Block（NAT ゲートウェイ サブネット CIDR ブロック）	AWS NAT ゲートウェイの CIDR ブロックをコンマ区切りで列挙したリスト。	192.168.100.0/24, 192.168.101.0/24
Lambda Subnet CIDR Block（Lambda サブネット CIDR ブロック）	Lambda 関数の CIDR ブロックをコンマ区切りで列挙したリスト。	192.168.200.0/24, 192.168.201.0/24
Firewall Instance size（ファイアウォール インスタンス サイズ）	デプロイメントの VM-Series ファイアウォールに必要な AWS インスタンスのタイプとサイズ。	M4.xlarge
Choose your Scaling Parameter（スケーリング パラメータの選択）	テンプレートにより、以下のすべてのメトリックが AWS CloudWatch に公開されます。 • CPU – データプレーン CPU 使用率 • AS – アクティブ セッション	データプレーン CPU 使用率

©2023 Palo Alto Networks, Inc.

パラメータ	概要	デフォルト値
スケーリング パラメータのテンプレートを変更する必要はありません。*AWS* コンソールで AWS CloudWatch アラームを設定することにより、オートスケーリングを始動する *1* つ以上のカスタム *PAN-OS* メトリックを監視できます。	• SU — セッション使用率 • SSPU — SSL プロキシ使用率 • GPU — GlobalProtect ゲートウェイ使用率 • GPAT — GlobalProtect ゲートウェイ使用率アクティブ トンネル • DPB — データプレーン パケット バッファ使用率	
Choose time in seconds for Scaling Period（スケーリング期間の選択（秒））	平均の統計が適用される期間（秒）。60 の倍数を設定する必要があります。	900
Maximum VM-Series Instances（最大 VM-Series インスタンス数）	オート スケーリング グループの VM-Series ファイアウォールの最大数。	3
Minimum VM-Series Instances（最小 VM-Series インスタンス数）	オート スケーリング グループの VM-Series ファイアウォールの最小数。	1
ScaleDown threshold value in percentage/value（スケールダウンしきい値（パーセント/値））	スケールイン イベントがトリガーされる値。	20
ScaleUp threshold value in percentage/value（スケールアップしきい値（パーセント/値））	スケールアウト イベントがトリガーされる値。	80

©2023 Palo Alto Networks, Inc.

AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動

ファイアウォール テンプレートを 1 つの VPC でデプロイして、サンプル アプリケーション テンプレートをファイアウォールと同じ VPC でデプロイするか、または他の VPC でデプロイすることができます。

保護するアプリケーションが別の AWS アカウントに属する場合は、サンプル アプリケーション テンプレートにはクロス アカウント デプロイメントのサポートが含まれます。このソリューションはハブ アンド スポーク アーキテクチャをサポートしているため、ファイアウォール テンプレートを 1 つの AWS アカウントでデプロイし、それをハブとして使用して、同じ、または異なる AWS アカウントに属するアプリケーション（スポーク）を保護することができます。

- VM-Series ファイアウォール テンプレートの起動
- アプリケーション テンプレートの起動
- 複数の内部ロード バランサーをデプロイする場合にのみ必須ですELB サービスへのトラフィックの有効化（v2.0 および v2.1）

VM-Series ファイアウォール テンプレートの起動

このワークフローでは、ファイアウォール テンプレートを使用して、アプリケーション ロード バランサーと VM-Series ファイアウォールをデプロイする方法を説明します。

このファイアウォール テンプレートには、ファイアウォールが更新を取得するためのアウトバウンド リクエストの開始、*Panorama* への接続、および *AWS CloudWatch* へのメトリックの公開に使用する *AWS NAT* ゲートウェイが含まれます。*Panorama* を使用してファイアウォールを管理しない場合は、*VPC* 内の信頼されないサブネットに接続して *VM-Series* ファイアウォールへの *SSH/HTTPS* アクセスを可能にするジャンプ サーバー（*EIP* アドレスを持つ要塞ホスト）をデプロイしなければなりません。このジャンプ サーバーが必要な理由は、*VM-Series* ファイアウォール上の管理インターフェイスがプライベートな *IP* アドレスしか持たないためです。

STEP 1 | AWS 用 VM-Series Auto Scaling テンプレートの計画（v 2.0）」のチェックリストを確認します。

以下の作業が完了していることを確認します。

- PAYG のみ）使用する PAYG バンドルの EULA を確認して同意した。
- For BYOL のみ）認証コードを取得した。この認証コードはブートストラップ パッケージの /license フォルダに格納します。
- VM-Series Auto Scaling テンプレートの起動に必要なファイルをGitHub リポジトリからダウンロードした。

©2023 Palo Alto Networks, Inc.

STEP 2 | init-cfg.txtファイルの変更VM-Seriesファイアウォールインスタンスのデプロイ時にデバイス証明書を自動的にインストールするために、init-cfg.txtファイルにデバイス証明書自動登録PINを追加する必要があります。

vm-series-auto-registration-id=

vm-series-auto-registration-pin-value=

詳細はブートストラップ プロセスとinit-cfg.txt ファイルの説明を参照してください。

Panorama を使用してファイアウォールを管理する場合は、以下の作業を実行します

1. Panorama で VM 認証キーを生成.ファイアウォールから Panorama への接続リクエストには、有効なキーを含めなければなりません。キーの有効期間を 8760 時間（1 年）に設定します。
2. メモ帳などのテキスト エディタで init-cfg.txt ファイルを開きます。フォーマットを変更すると、VM-Series Auto Scaling テンプレートのデプロイに失敗するため、フォーマットは変更しないでください。値と名前のペアとして以下の情報を追加します。
   - プライマリ Panorama の IP アドレスと、任意のセカンダリ Panorama の IP アドレス。入力コマンド：

     panorama-server=

     panorama-server-2=
   - テンプレート スタック名とファイアウォールを割り当てるデバイス グループを指定します。入力コマンド：

     tplname=

     dgname=
   - VM 認証キー。入力コマンド：

     vm-auth-key=
3. AWS 上の VM-Series ファイアウォールで管理インターフェイス（mgmt）とデータプレーン インターフェイス（ethernet 1/1）をスワップするためのコマンドを削除していないことを確認します。たとえば、ファイルにはここに示した名前と値のペアが含まれていなければなりません。

   op-command-modes=mgmt-interface-swap

   vm-auth-key=755036225328715

   panorama-server=10.5.107.20

   panorama-server-2=10.5.107.21

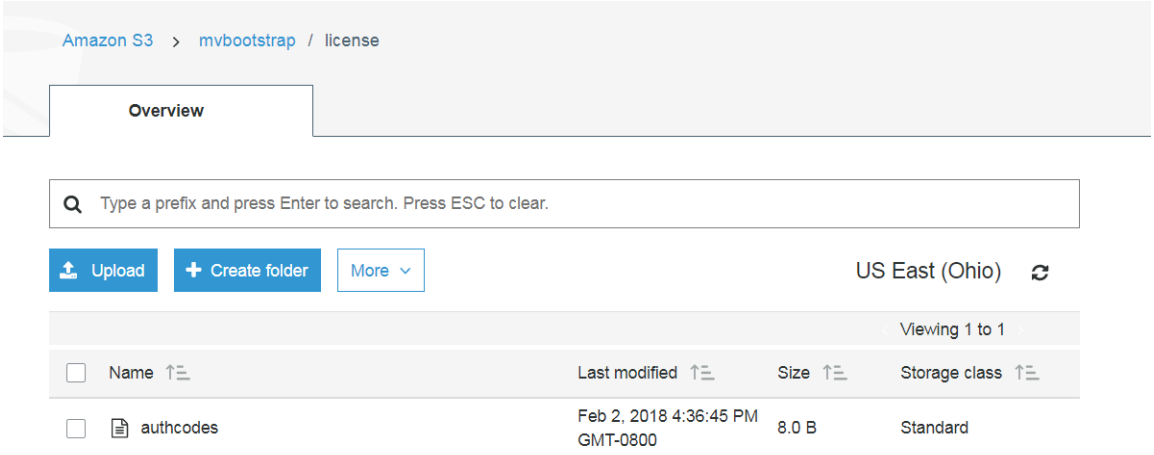
   tplname=FINANCE_TG4

   dgname=finance_dg
4. ファイルを保存して閉じます。

©2023 Palo Alto Networks, Inc.

STEP 3 | BYOL のみ）ライセンスの認証コードを ブートストラップ パッケージの /license フォルダに追加します。詳細は、ブートストラップ パッケージの準備」を参照してください。

1. メモ帳などのテキスト エディタで新しいテキスト（. txt）ファイルを作成します。
2. このファイルに BYOL ライセンスの認証コードを追加し、authcodes（ファイル拡張子なし）でファイルを保存し、「/license」フォルダにアップロードします。認証コードは、デプロイメントで必要な数のファイアウォールをサポートしていなければなりません。ファイアウォールに関連付けられているすべてのライセンス キーをファイアウォールが同時に取り出せるように、個別の認証コードではなく、認証コード バンドルを使用する必要があります。バンドルではなく個別の認証コードを使用すると、ファイアウォールは、ファイルに含まれている最初の認証コードのライセンス キーのみを検索します。



STEP 4 | bootstrap.xml ファイルに定義されている VM-Series ファイアウォール管理者アカウントのデフォルト認証情報を変更します。

VM-Series Auto Scaling テンプレートを本番環境で使用する場合には必須です。

GitHub リポジトリで提供されている bootstrap.xml ファイルは、テストと評価のみを目的としています。本番のデプロイメントではbootstrap.xml ファイル（v2.0）をカスタマイズしてから起動する必要があります。

STEP 5 | 本番環境用の VM-Series Auto Scaling テンプレートを起動するための Amazon Simple Storage（S3）バケットを準備します。

S3 バケットは、テンプレートをデプロイする予定のリージョンと同じリージョンで作成します。パブリック *S3* バケットでホストされるブートストラップ ファイルは、テンプレートを評価しやすくするためにのみ用意されています。

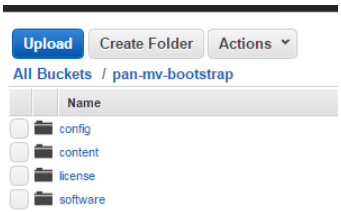
1. ブートストラップ ファイル用に新しい S3 バケットを作成します。
   1. AWS 管理コンソールにログインして S3 コンソールを開きます。
   2. **Create Bucket**（バケットの作成）をクリックします。
   3. **Bucket Name**（バケット名）**Region**（リージョン）を入力し**Create**（作成）をクリックします。バケットは S3 ルート レベルに作成しなければなりません。バケッ

©2023 Palo Alto Networks, Inc.

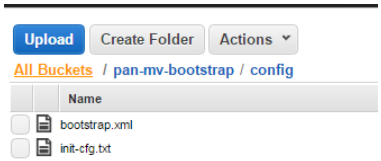
トをネストすると、ブートストラップ ファイルの場所へのパスを指定できないため、ブートストラップは失敗します。

2. ブートストラップ ファイルを S3 バケットにアップロードします。ブートストラップ フォルダは、S3 バケットのルート フォルダに存在しなければなりません。

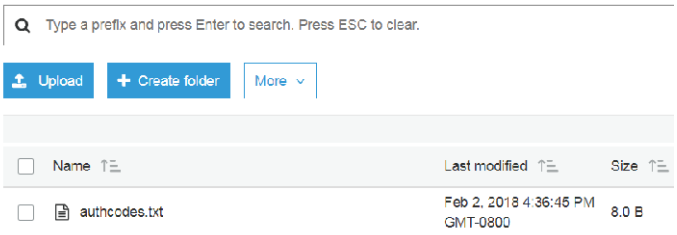
   1. バケット名をクリックし**Create folder**（フォルダを作成）をクリックします。
   2. ブートストラップ用に以下のフォルダ構造を作成します。



   3. リンクをクリックして**config** フォルダを開きます。
   4. **Actions**（アクション） > **Upload**（アップロード）**Add Files**（ファイルを追加）の順に選択し、init-cfg.txt ファイルと bootstrap.xml ファイルを参照して選択してから**Open**（開く）をクリックします。
   5. **Start Upload**（アップロード開始）をクリックして、ファイルを confg フォルダに追加します。このフォルダには、init-cfg.txt と bootstrap.xml の 2 つのファイルのみを格納することができます。



   6. BYOL のみ）リンクをクリックして**license** フォルダを開き、VM-Series ファイアウォールのライセンス認証に必要な認証コードが書き込まれたテキスト ファイルをアップロードします。



3. AWS Lambda コード（panw-aws.zip ファイル）を S3 バケットにアップロードします。この例では、AWS Lambda コードはブートストラップ パッケージと同じ S3 バケットに含まれています。

   1. バケット名をクリックします。
   2. **Add Files**（ファイルを追加）をクリックして panw-aws.zip ファイルを選択してから**Open**（開く）をクリックします。

©2023 Palo Alto Networks, Inc.

3. **Start Upload**（アップロード開始）をクリックして ZIP ファイルを S3 バケットに追加します。

Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
panw-aws.zip	Dec 4, 2017 12:10:50 PM GMT-0800	162.1 KB	Standard

STEP 6 | ファイアウォール テンプレートを選択します。

起動前にファイアウォール テンプレート（v2.0）をカスタマイズする必要がある場合は、この時点でカスタマイズして、カスタマイズ後のテンプレートを選択してください。

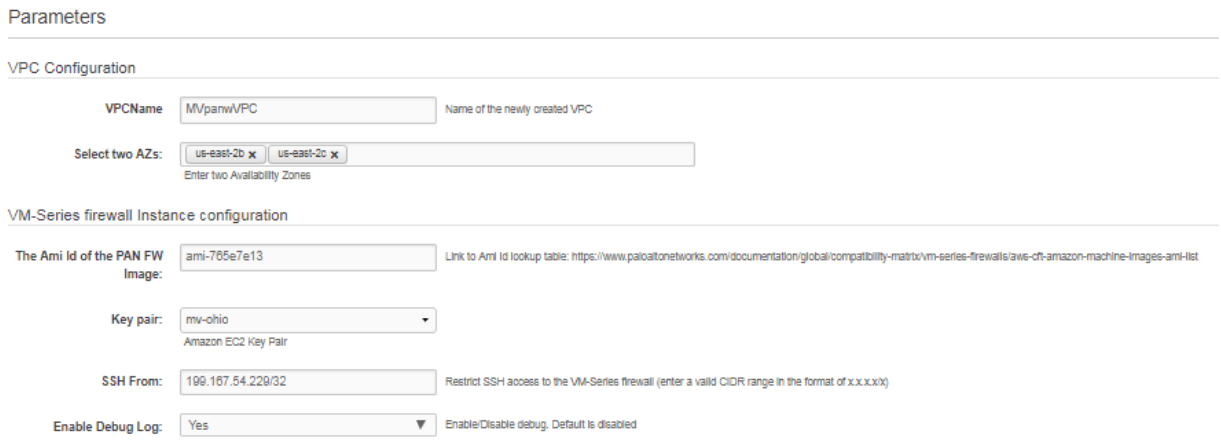
1. AWS 管理コンソールで**CloudFormation** > **Create Stack**（スタックを作成）の順に選択します。
2. **Upload a template to Amazon S3**（**Amazon S3** にテンプレートをアップロード）を選択し、firewall-v2.0.template を選択してから**Open**（開く） と**Next**（次へ）をクリックします。
3. **Stack name**（スタック名）を指定します。スタック名は、このテンプレートがデプロイするすべてのリソースを一意に判別します。

STEP 7 | VPC のパラメータを設定します。

1. **VPC Configuration**（**VPC** の設定）パラメータを以下の用に入力します。
   1. **VPCName**（**VPC** 名）を入力します。
   2. **Select two AZs**（**2** つの可用性ゾーンを選択）で、セットアップがまたがる 2 つの可用性ゾーンを選択します。

©2023 Palo Alto Networks, Inc.

STEP 8 | VM-Series ファイアウォールの設定を選択します。



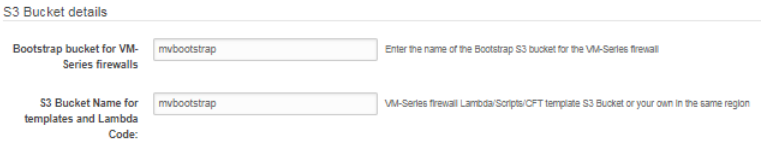
1. VM-Series ファイアウォール用のAMI ID を検索して入力します。AMI ID が、使用する AWS リージョン、PAN-OS バージョン、および BYOL または PAYG ライセンス オプションと一致していることを確認します。
2. ファイアウォールを起動するための EC2 の**Key pair**（キー ペア）を（ドロップダウンから）選択します。ファイアウォールにログインするには、このキー ペアの名前と、関連付けられている秘密鍵を入力しなければなりません。
3. SSH アクセスをファイアウォールの管理インターフェイスに制限します。専用管理 IP アドレスまたはネットワークに対応する CIDR ブロックを供給してください。許可するソース ネットワーク範囲を必要以上には大きくせず、0.0.0.0/0 を許可ソースとして指定しないでください。IP アドレスをテンプレートで指定する前に、その IP アドレスがロックアウトされないことを確認します。
4. デバッグ ログを有効化する場合は**Enable Debug Log**（デバッグ ログを有効化）**Yes**（はい）を選択します。デバッグ ログを有効化すると、デプロイメントの問題のトラブルシューティングに役立つ詳細なログが生成されます。これらのログはスタック名を使用して生成され、AWS CloudWatch に保存されます。

デフォルトでは、テンプレートは VM-Series ファイアウォールのスケーリング パラメータとして CPU 利用率を使用しますカスタム PAN-OS メトリックは、すでに指定してあるスタック名に対応した CloudWatch 名前空間で自動的に公開されます。

©2023 Palo Alto Networks, Inc.

STEP 9 | Amazon S3 バケット（1 つまたは複数）の名前を指定します。

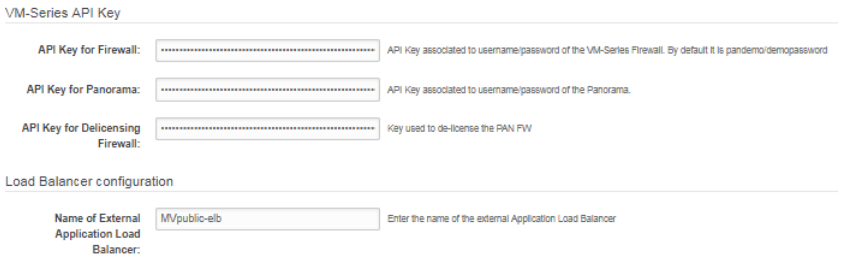
1 つの *S3* バケットをブートストラップ パッケージと *ZIP* ファイルの両方に使用できます。



1. ブートストラップ パッケージが格納された S3 バケットの名前を入力します。

   ブートストラップ バケットが適切にセットアップされていないか、またはバケット名を正しく入力しないとブートストラップ プロセスが失敗し、ファイアウォールにログインできなくなります。ロード バランサーのヘルス チェックも失敗します。
2. panw-aws.zip ファイルが格納された S3 バケットの名前を入力します。

STEP 10 | ファイアウォールと Panorama への API アクセスを有効化するキーを指定します。



1. ファイアウォールが API コールを認証するために使用するキーを入力します。デフォルトのキーはサンプル bootstrap.xml ファイルに基づいており、テストおよび評価にのみ使用してます。本番のデプロイメントでは、API コール専用に別の PAN-OS ログインを作成して、関連するキーを生成しなければなりません。
2. Panorama を一元管理に使用する場合は、AWS Lambda が Panorama に対して API コールを発行できるようにするための API キーを入力します。本番のデプロイメントでは、API コール専用に別のログインを作成して、関連するキーを生成しなければなりません。
3. 自分のアカウントのライセンス無効化 API キーをコピーして貼り付けます。このキーは、スケールイン イベントが発生した場合に、ファイアウォールのライセンスを正常に無効化するのに必要です。このキーの取得方法:

   1. カスタマー サポート ポータルにログインします。
   2. アセット > **API** キー管理] を選択します。
   3. API キーをコピーします。

STEP 11 | アプリケーション ロード バランサー名を入力します。

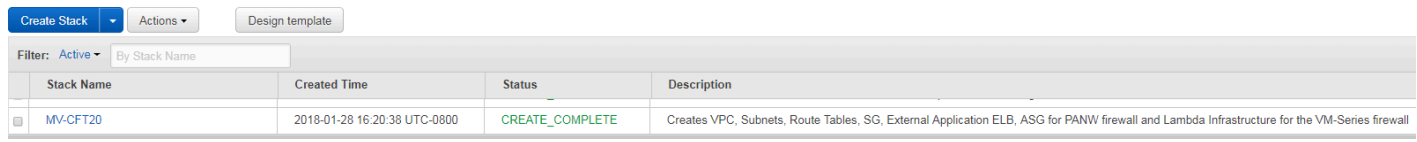
 ©2023 Palo Alto Networks, Inc.

STEP 12 | 任意）VM-Series Auto Scaling テンプレートに関連付けられたリソースを特定するためのタグを適用します。

スタックのリソースを識別して分類するための名前と値のペアを追加します。

STEP 13 | テンプレート設定を確認し、テンプレートを起動します。

1. **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（このテンプレートによって **AWS CloudFormation** が **IAM** リソースが作成される可能性があることを理解しています）を選択します。
2. **Create**（作成）をクリックしてテンプレートを起動します。CREATE_IN_PROGRESS イベントが表示されます。
3. デプロイメントが成功すると、ステータスが CREATE_COMPLETE に変わります。

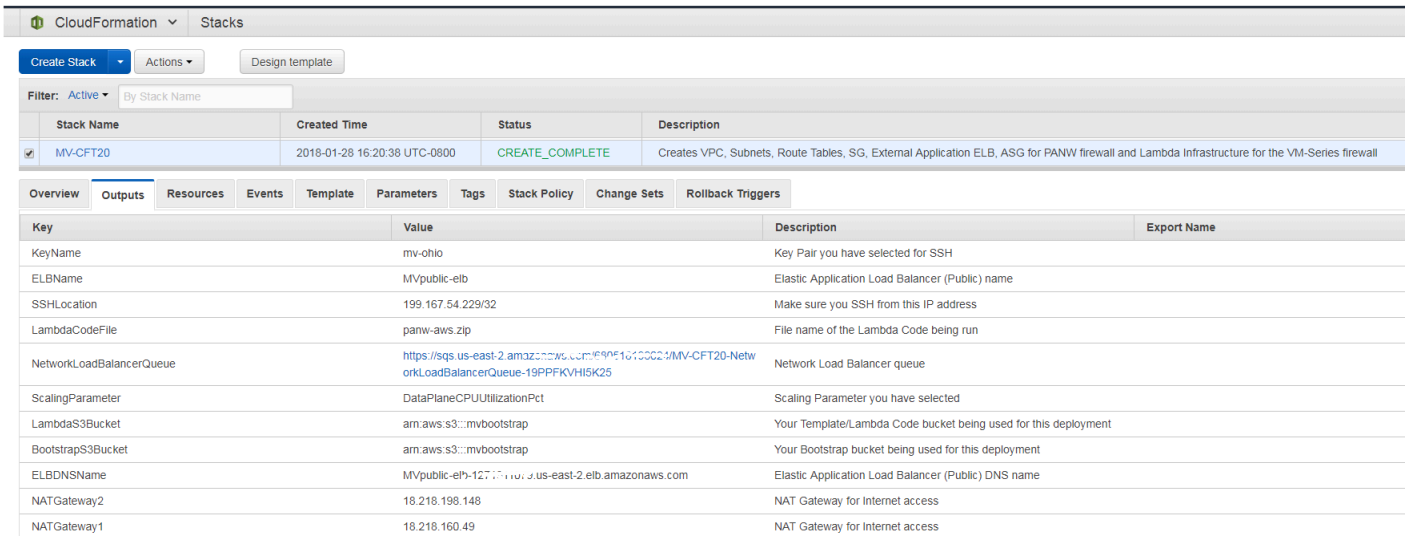


テンプレートをカスタマイズしていなければ、VM-Series Auto Scaling テンプレートは、アプリケーション ロード バランサーの背後に 1 つの VM-Series ファイアウォールを含む ASG を起動します。

©2023 Palo Alto Networks, Inc.

STEP 14 | テンプレートが必要なリソースをすべて起動したことを確認します。

1. AWS 管理コンソールで、リソース リスト出力を表示するスタック名を選択します。



2. EC2 ダッシュボードで**Auto Scaling Groups**（オート スケーリング グループ）を選択します。各可用性ゾーンに、1 つのファイアウォールを持つ 1 つの ASG があることを確認します。ASG 名のプレフィックスにはスタック名が含まれます。
3. VM-Series ファイアウォールにログインします。ジャンプ サーバーをデプロイするか、または Panorama を使用してファイアウォール上の Web インターフェイスにアクセスしなければなりません。

- ファイアウォールが起動してトラフィックを処理できるようになるまで最大で *20* 分ほどかかります。
- テストまたは本番のデプロイメントが終了した後で、料金の発生を中止するには、スタックを完全に削除するしか方法はありません。インスタンスをシャットダウンしたり、*ASG* の最大数を *0* にするだけでは不十分です。

STEP 15 | 以下の情報を保存します。これらの値は、アプリケーション テンプレートのデプロイ時に入力として提供する必要があります。

- 各可用性ゾーンの NAT ゲートウェイの IP アドレス。この IP アドレスは、アプリケーションを別の VPC にデプロイする場合に HTTP アクセスを Web サーバーに制限するのに必要です。この IP アドレスを指定することで、ファイアウォールが別の VPC のアプリケーションへのアクセスを保護し、誰もファイアウォールをバイパスして直接 Web サーバーにアクセスできないようにできます。NAT ゲートウェイ IP アドレスを入力しないと、サンプル アプリケーション テンプレート（panw_aws_nlb_vpc-2.0.template）はテンプレート検証エラーを表示します。IP アドレスはコンマ区切りリストとして入力する必要があります。
- ネットワーク ロード バランサー SQS URL。ファイアウォール スタックの AWS Lambda 関数は、このキューを監視して、デプロイされているネットワーク ロード バランサーについて学習し、VM-Series ファイアウォールがネットワーク ロード バランサーの IP アド

©2023 Palo Alto Networks, Inc.

レスにトラフィックを転送できるようにするための NAT ポリシー ルールを（各アプリケーションに 1 つずつ）ファイアウォール上で作成します。

アプリケーション テンプレートの起動

アプリケーション テンプレートにより、完全なサンドイッチ トポロジーをデプロイでき、オート スケーリング ソリューションを評価できます。このアプリケーション テンプレートは、ファイアウォール テンプレートを使用してデプロイした VM-Series ファイアウォール グループの背後に、ネットワーク ロード バランサーと、Web サーバーのペアをデプロイします。このテンプレートの Web サーバーは、ソフトウェア更新を検索するための直接アウトバウンド アクセス用のパブリック IP アドレスを持ちます。このテンプレートはソリューションの評価に使用し、本番用には自身でテンプレートを作成します。カスタム テンプレートではアプリケーション テンプレートとファイアウォール テンプレートの間の SQS メッセージングを有効化します。

アプリケーション テンプレートを起動する際には、ファイアウォール テンプレートをデプロイしたのと同じ VPC でアプリケーション テンプレートをデプロイするのか（panw_aws_nlb-2.0.template）、あるいは別の VPC でアプリケーション テンプレートをデプロイするのか（panw_aws_nlb_vpc-2.0.template）によって適切なテンプレートを選択してください。別の VPC にデプロイする場合、テンプレートはクロス アカウント デプロイメントのサポートを提供します。クロス アカウント デプロイメントでは、IAM ロールを作成し、信頼する AWS アカウントと信頼される AWS アカウントの間でパーミッションとトラスト リレーションを有効化して、テンプレートの起動時にアカウント情報を入力として指定する必要があります。

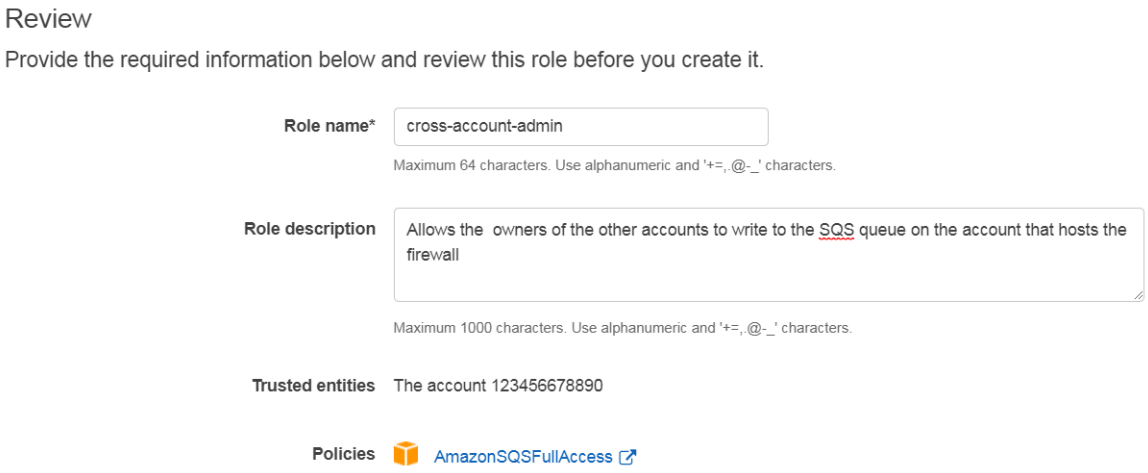
STEP 1 | クロス アカウント デプロイメントでのみ必要）IAM ロールを作成しますAWS のドキュメントを参照してください。

このロールは、異なる AWS アカウントに属するユーザーへのアクセスを許可します。このユーザーは、ファイアウォール テンプレート内で Simple Queue Service（SQS）へのアクセス許可を必要とします。ファイアウォールは、このキューを使用して、デプロイされている各ネットワーク ロード バランサーについて学習し、ネットワーク ロード バランサーの背後にある Web サーバーにトラフィックを転送するための NAT ポリシーを作成します。

- **Account ID**（アカウント **ID**）には、アプリケーション テンプレートをデプロイするアカウントの AWS アカウント ID を入力します。そのアカウント ID を指定することで、ファイアウォール テンプレート リソースをホストするアカウントのリソースへのアクセスが許可されます。
- **Require external ID**（必要な外部 **ID**）を選択し、共有秘密となる値を入力します。外部 ID を指定することで、ユーザーは、リクエストに正しい値が含まれている場合にのみ、ロールを有効とみなすことができます。

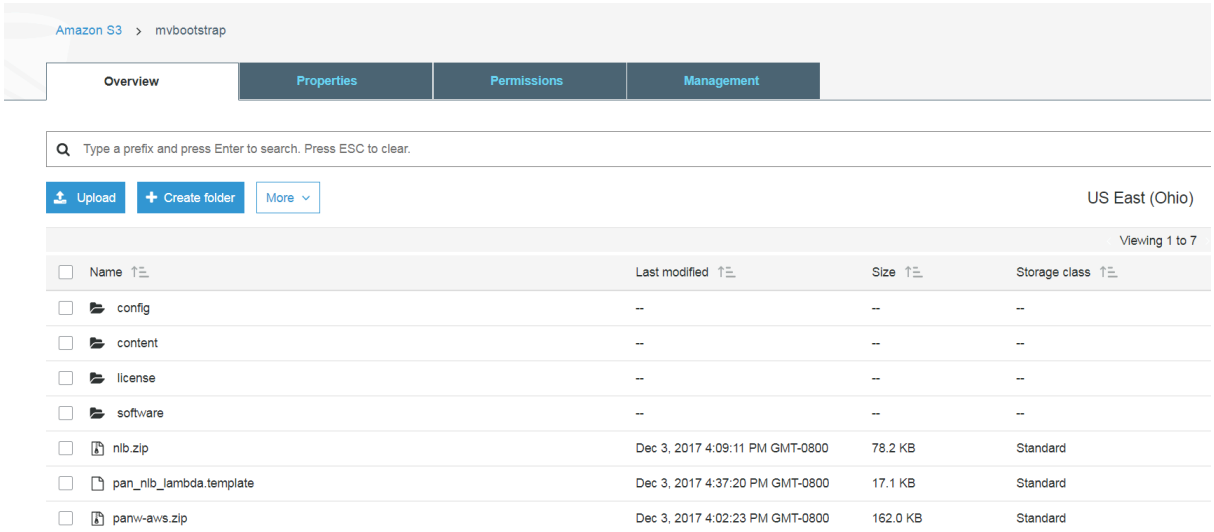
©2023 Palo Alto Networks, Inc.

- **Permissons**（パーミッション）を選択して**Amazon SQS Full Access**（**Amazon SQS** へのフルアクセス）を許可します



STEP 2 | Palo Alto Networks のパブリック S3 バケットを使用するか、またアプリケーション テンプレートを起動するためのプライベート（S3）バケットを準備します。

1. 以下のスクリーンショットに示すように、3 つの .template ファイルを除いたすべてのファイルを格納した ZIP ファイルを nlb.zip という名前でGitHub リポジトリに作成します。
2. 作成してある S3 バケットに ZIP ファイルをアップロードします。



3. nlb.zip ファイルをコピーしたのと同じバケットに pan_nlb_lambda テンプレートをコピーします。

STEP 3 | 起動するアプリケーション テンプレートを選択します。

1. AWS 管理コンソールで**CloudFormation** > **Create Stack**（スタックを作成）の順に選択します。
2. **Upload a template to Amazon S3**（**Amazon S3** にテンプレートをアップロード）を選択し、ファイアウォールと同じ VPC にテンプレートのリソースをデプロイする場合は

©2023 Palo Alto Networks, Inc.

panw_aws_nlb-2.0.template、別の VPC にテンプレートのリソースをデプロイする場合は panw_aws_nlb_vpc-2.0.template を選択しますOpen（開く）Next（次へ）をクリックします。

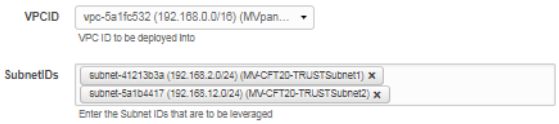
3. **Stack name**（スタック名）を指定します。スタック名により、このテンプレートを使用してデプロイされるすべてのリソースを識別できます。

STEP 4 | VPC とネットワーク ロード バランサーのパラメータを設定します。

1. **Select list of AZ**（可用性ゾーンの選択リスト）で、セットアップがまたがる 2 つの可用性ゾーンを選択します。同じ VPC でデプロイする場合は、ファイアウォール テンプレートに対して選択したのと同じ可用性ゾーンを選択してください。
2. **CIDR Block for VPC**（**VPC** 用の **CIDR** ブロック）を入力します。デフォルトの CIDR は 192.168.0.0/16 です。



3. （panw_aws_nlb-2.0.template を使用して同じ VPC にアプリケーションをデプロイする場合のみ）

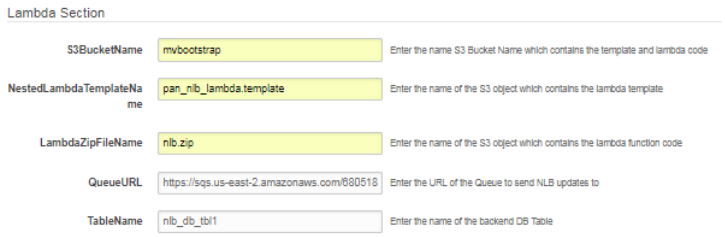


各可用性ゾーンのファイアウォール上の信頼できるサブネットに関連付けられた**VPC ID** と**Subnet IDs**（サブネット **ID**）を選択します。ファイアウォール上の信頼できるサブネットにネットワーク ロード バランサーが接続され、ロード バランサーのサンドイッチ トポロジーが完成します。

4. ネットワーク ロード バランサーの名前を入力します。

 ©2023 Palo Alto Networks, Inc.

STEP 5 | AWS Lambda のパラメータを設定します。



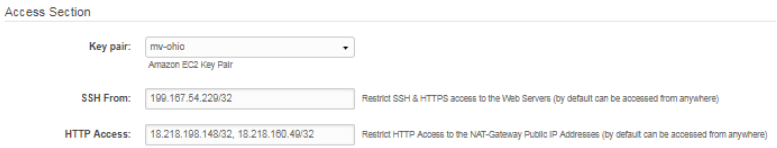
1. nlb.zip と pan_nlb_lambda.template が格納されている S3 バケットの名前を入力します。
2. pan_nlb_lambda.template と ZIP ファイルの名前を入力します。
3. 以前にコピーしてある SQS URL を貼り付けます。
4. 一意の**TableName**（テーブル名）を入力します。このテーブルは、デプロイメントのネットワーク ロード バランサーに関連付けられているアプリケーションのポートと IP アドレスのマッピングを格納します。

   アプリケーション スタックを削除すると、このテーブルも削除されます。したがって、ネットワーク ロード バランサーの複数のインスタンスが同じテーブルに書き込んだ状態でテーブルが削除されると、ファイアウォール上の NAT ルールが適切に機能せず、アプリケーション トラフィックが間違ったポートやネットワーク ロード バランサー転送されることがあります。

STEP 6 | デプロイメントのニーズに合わせて Web サーバーの EC2 インスタンス タイプを修正します。

STEP 7 | Web サーバーを起動するための EC2 の**Key pair**（キー ペア）を（ドロップダウンから）選択します。Web サーバーにログインするには、このキー ペアの名前と、関連付けられている秘密鍵を入力しなければなりません。

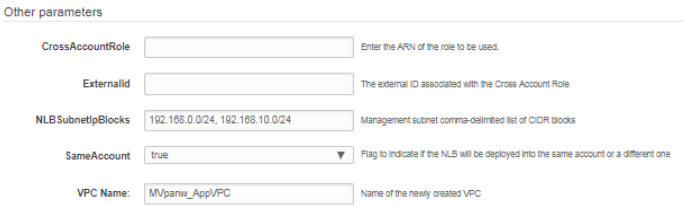
STEP 8 | （panw_aws_nlb-2.0.template を使用している場合のみ）Web サーバーへのアクセスをロックします。



1. **SSH From**（**SSH** の送信元）による Web サーバーへのアクセスを制限します。このリストに含まれる IP アドレスのみが Web サーバーにログインできます。
2. Web サーバーへの HTTP アクセスを制限します。ファイアウォール テンプレートの出力から NAT ゲートウェイのパブリック IP アドレスを入力し、IP アドレスをコンマで区切ってください。NAT ゲートウェイの IP アドレスを入力することで、アプリケーション サーバーへのすべての Web トラフィックが VM-Series ファイアウォールによって保護されることを保証できます。

©2023 Palo Alto Networks, Inc.

STEP 9 | （panw_aws_nlb-2.0.template を使用している場合のみ）別の VPC のアプリケーション テンプレート スタックの起動に必要な、その他のパラメータを設定します。

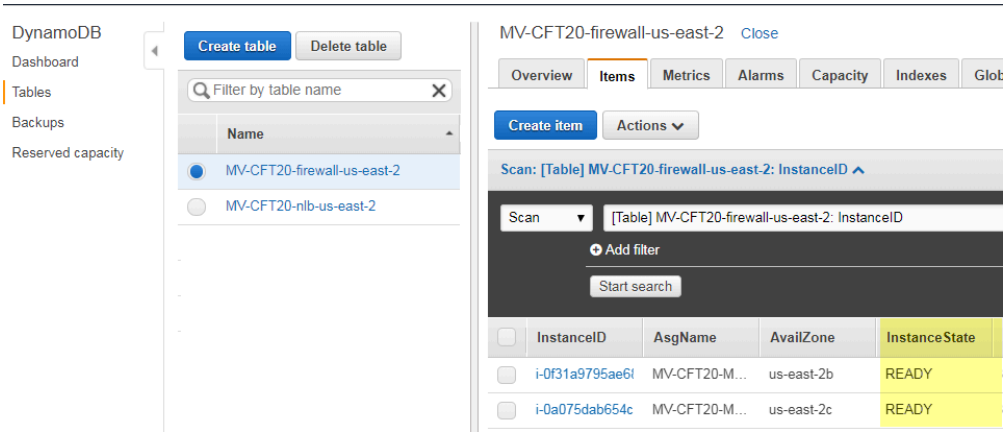


1. このアプリケーション テンプレートをファイアウォール テンプレートと同じ AWS アカウントでデプロイする場合は、SameAccount で**true** を選択し、クロス アカウント ロールと外部 ID は空白のままにしておきます。クロス アカウント デプロイメントを使用する場合は**false** を選択します。

   クロス アカウント デプロイメントの場合は、「（クロス アカウント デプロイメントでのみ必要）IAM ロールを作成します」で定義した**CrossAccountRole** と**ExternalId** に Amazon Resource Number（ARN）を入力します。AWS ドキュメントを参照します。ARN を調べるには、AWS 管理コンソールで**Support**（サポート） > **Support Center**（サポート センター）の順に選択します。
2. アプリケーション テンプレート リソースをデプロイしたい**VPC Name**（**VPC** 名）を入力します。
3. 任意）ネットワーク ロード バランサーの管理サブネットの**NLBSubnetIPBlocks** を変更します。

STEP 10 | テンプレート設定を確認し、テンプレートを起動します。

STEP 11 | ネットワーク ロード バランサーがデプロイ済みで、動作準備が完了していることを確認します。



STEP 12 | アプリケーション ロード バランサーの**DNS** 名を取得して、Web ブラウザに入力します。

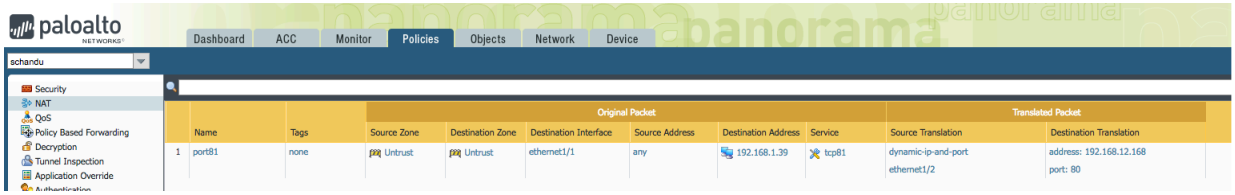
例： http://MVpublic-elb-123456789.us-east-2.elb.amazonaws.com/

Web ページが表示されれば、オート スケーリング テンプレートは正常に起動したことになります。

©2023 Palo Alto Networks, Inc.

STEP 13 | 各ファイアウォールの NAT ポリシー ルールで各ネットワーク ロード バランサーの IP アドレスが指定されていることを確認してください。

アプリケーション テンプレートを使用してネットワーク ロード バランサーの新しいインスタンスと Web サーバーのペアをデプロイすると、ファイアウォールは次のネットワーク ロード バランサー インスタンスに割り当てられているポートについて学習し、新しい NAT ポリシー ルールを作成します。したがって、アプリケーション テンプレートを 3 回起動すると、ファイアウォールはポート 81、82、および 83 に対して合計 3 つの NAT ポリシー ルールを持つことになります。



STEP 14 | アプリケーション テンプレートを複数回起動した場合はELB サービスへのトラフィックを有効化する必要があります。

ELB サービスへのトラフィックの有効化（**v2.0** および **v2.1**）

デプロイメントに 2 つ目以降の内部ロード バランサー（ILB）を追加した場合は、内部ロード バランサー、VM-Series ファイアウォールのオート スケーリング グループ、そして Web サーバーがヘルス ステータスを正しくレポートし、すべての AWS リソースの間でトラフィックが負荷分散されるように、追加の設定が必要です。

v2.0 では *ILB* はネットワーク ロード バランサーとしてのみ動作できます。*v2.1* では *ILB* はアプリケーション ロード バランサーまたはネットワーク ロード バランサーとして動作できます。

STEP 1 | AWS 管理コンソールで、DynamoDB テーブルの各ネットワーク バランサーに割り当てられているポートを確認します。

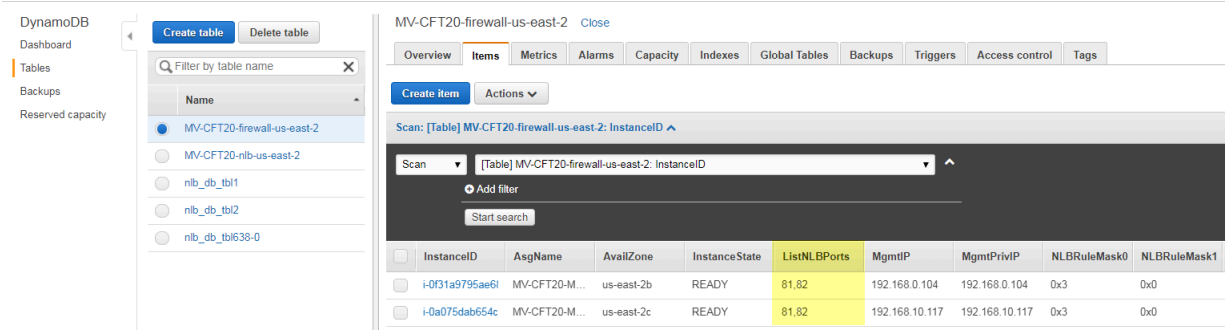
新しい内部ロード バランサーが起動されたら、アプリケーション テンプレートは、テンプレートの起動時に入力として指定された SQS URL に SQS メッセージを送信しなければなりません。ファイアウォール テンプレートの AWS Lambda 関数は、SQS を監視して、ポート マッピングをファイアウォール テンプレートの DynamoDB テーブルに追加します。追加の内部バランサーをデプロイするたびに、割り当てられるポート番号はポート 81 から 1 ずつ増加します。したがって、2 つ目の内部ロード バランサーはポート 82、3 番目はポート 83 を使用します。

1. AWS 管理コンソールで**DynamoDB** サービスを選択します。

©2023 Palo Alto Networks, Inc.

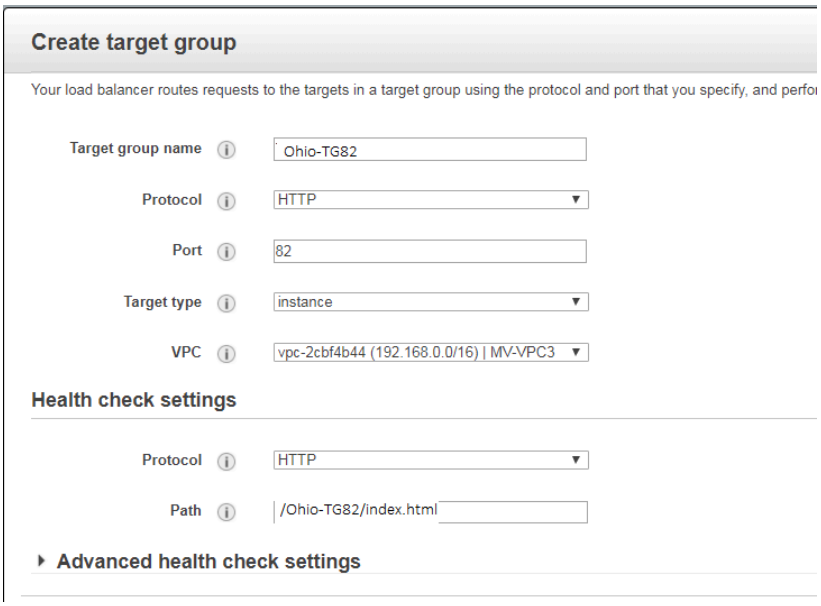
2. **Tables**（テーブル）を選択し、ファイアウォール テンプレートのスタック名と一致するテーブルをクリックします。（例：MV-CFT20-firewall-us-east-2。）

   Items（項目）リストで、ファイアウォール テンプレートに関連付けられている SQS にメッセージを送信している内部ロード バランサーが使用しているポートを確認します。



STEP 2 | ターゲット グループを作成します。内部ロード バランサーは、ターゲット グループのサーバーに対して指定したポートとプロトコルを使用して、登録済みのターゲットにリクエストを送信します。

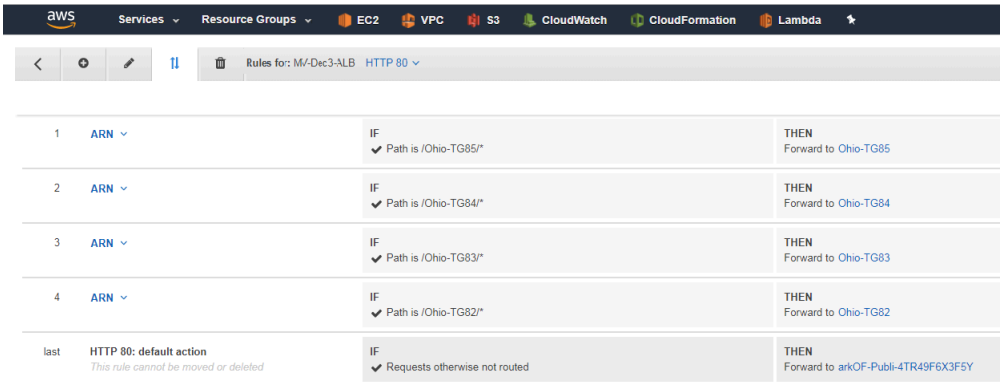
新しいターゲット グループを追加する場合は、DynamoDB テーブルで確認したポート情報を使用します



©2023 Palo Alto Networks, Inc.

STEP 3 | リクエストがターゲット Web サーバーに転送されるように、内部ロード バランサーリスナー ルールを編集します。

1. AWS 管理コンソールの Load Balancing（負荷分散）セクションで**Load Balancers**（ロード バランサー）を選択し、使用しているスタック名と一致する内部ロード バランサーを選択します。
2. **View/edit rules**（ルールを表示/編集）を選択してリスナーのルールを修正します。
3. **Insert rule**（ルールを挿入）を選択して、上記で定義したターゲット グループにトラフィックを転送するためのパス ベースのルートを追加します。



STEP 4 | ターゲット グループを両方の VM-Series ファイアウォール オート スケーリング グループに接続します。

1. Auto Scaling（オート スケーリング）セクション**Auto Scaling Groups**（オート スケーリング グループ）を選択し、スタック名と一致するオート スケーリング グループを選択します。
2. **Details**（詳細） > **Edit**（編集）を選択し**Target Groups**（ターゲット グループ）のドロップダウン リストから新しいターゲット グループを選択します。



STEP 5 | アプリケーション テンプレートによってデプロイされた各 Web サーバーにログインし、ターゲット グループ名で新しいディレクトリを作成して、index.html ファイルをディレク

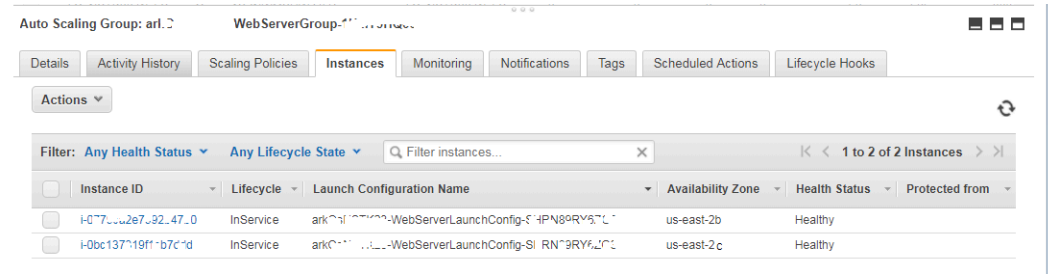
 ©2023 Palo Alto Networks, Inc.

トリにコピーします。index.html ファイルへのパスを設定するまで、この Web サーバーのヘルス チェックは不良ステータスを返します。

```
sudo su
cd/var/www/html
mkdir <target-groupname
cp index.html <target-groupname
```

STEP 6 | Web サーバーのヘルス ステータスを確認します。

Auto Scaling Groups（オート スケーリング グループ）を選択し、アプリケーション スタック名を使用して Web サーバーのオート スケーリング グループを探し、Web サーバーが良好なヘルス ステータスをレポートしていることを確認します



bootstrap.xml ファイル（v2.0）のカスタマイズ

GitHub リポジトリで提供されている bootstrap.xml ファイルでは、ファイアウォール管理者のデフォルトのユーザー名とパスワードが使用されています。実稼働環境に VM-Series Auto Scaling テンプレートをデプロイする前に、最低でも、VM-Series ファイアウォールの管理アカウントに対して、一意のユーザー名とパスワードを作成する必要があります。必要な場合は、ゾーン、ポリシー、ルール、セキュリティ プロファイルを使用してファイアウォールを完全に設定し、ゴールデン設定スナップショットをエクスポートできます。この設定スナップショットは、実稼働環境用の bootstrap.xml ファイルとして使用できます。

実稼働環境で使用する bootstrap.xml ファイルは、以下の 2 つの方法でカスタマイズできます。

- オプション **1**：GitHub リポジトリで提供されているブートストラップ ファイルを使用して AWS 上の VM-Series ファイアウォールを起動します。次に、ファイアウォール設定を変更してエクスポートし、VM-Series Auto Scaling テンプレート用の新しい bootstrap.xml ファイルを作成します。「GitHub ブートストラップ ファイルをシードとして使用」を参照してください。
- オプション **2**：ブートストラップ ファイルを使用せずに AWS 上の新しい VM-Series ファイアウォールを起動します。次に、NAT ポリシー ルールを追加して、VM-Series ファイアウォールでトラフィックが適切に処理されるようにします。その後、設定をエクスポートして、VM-Series Auto Scaling テンプレート用の新しい bootstrap.xml ファイルを作成します。「ブートストラップ ファイルを最初から作成する」を参照してください。

テンプレートのデプロイが完了してから、管理ユーザーの認証情報を変更する必要がある場合、または新しい管理ユーザーを追加してテンプレート スタックを更新する必要がある場合は、「管理アカウントの変更およびスタックの更新」を参照してください。

©2023 Palo Alto Networks, Inc.

ブートストラップ ファイルを最初から作成する

サンプルの bootstrap.xml ファイルを使用せずに、サポートされている PAN OS バージョン（Panorama プラグインの互換性マトリックスを参照）用の AMI を使用して AWS 上で新しい VM-Series ファイアウォールを起動し、設定をエクスポートして、Auto Scalingテンプレートv2.0 VM 用の新しい bootstrap.xml ファイルを作成します。

STEP 1 | VM-Series ファイアウォールを AWS にデプロイし（ブートストラッピングは不要）、パブリック IP アドレスを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH でログインします。ファイアウォールの新しい管理パスワードを設定する必要があります。

STEP 2 | ファイアウォール インターフェイスにログインします。

STEP 3 | （任意）ファイアウォールを設定します。データプレーン インターフェイス、ゾーン、およびポリシー ルールの設定が可能です。

STEP 4 | ファイアウォールへの変更を **Commit**（コミット）します。

STEP 5 | 設定ファイルをエクスポートして、**`bootstrap.xml`** という名前を付けます。（**Device**（デバイス） > **Setup**（セットアップ） > **Operation**（操作） > **Export Named Configuration Snapshot**（名前付き設定スナップショットのエクスポート））。

STEP 6 | bootstrap.xml ファイルを GitHub リポジトリからダウンロードして、テキスト編集ツールで開き、行 353 ～ 356 をコピーします。これらの行には、AWS CloudWatch の名前空間が定義されいます。この名前空間に、ファイアウォールのオート スケーリングに必要なカスタム PAN-OS メトリックが発行されます。

STEP 7 | AWS CloudWatch の情報が含まれるように、前にエクスポートした設定ファイルを編集します。

`</management>` を検索し、`</management>` の後に行 353 ～ 356 をペーストします。

```
352         </management>
353         <aws-cloudwatch>
354           <enabled>yes</enabled>
355           <name>autoscale-default-panw-asg-name</name>
356         </aws-cloudwatch>
357       </setting>
```


©2023 Palo Alto Networks, Inc.

STEP 8 | 管理インターフェイス設定を削除します。

1. **</service>** を検索し、それに続く ip-address、netmask、および default gateway の行を削除します。
2. **</type>** を検索し、それに続く ip-address、netmask、default gateway、および public-key の行を削除します。

```
326         </service>
327         <ip-address>192.168.10.16</ip-address>
328         <netmask>255.255.255.0</netmask>
329         <default-gateway>192.168.10.1</default-gateway>
330         <hostname>PA-VM</hostname>
331       </system>
332       <setting>
333         <config>
334           <rematch>yes</rematch>
335         </config>
336         <management>
337           <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
338           <initcfg>
339             <type>
340               <dhcp-client>
341                 <send-hostname>yes</send-hostname>
342                 <send-client-id>no</send-client-id>
343                 <accept-dhcp-hostname>no</accept-dhcp-hostname>
344                 <accept-dhcp-domain>no</accept-dhcp-domain>
345               </dhcp-client>
346             </type>
347             <ip-address>192.168.10.16</ip-address>
348             <netmask>255.255.255.0</netmask>
349             <default-gateway>192.168.10.1</default-gateway>
350             <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJVEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXlLczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTR
351           </initcfg>
352         </management>
```

STEP 9 | ファイルを保存します。以上で、「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動」に進むことができます。

GitHub ブートストラップ ファイルをシードとして使用

GitHub リポジトリで提供されるブートストラップ ファイルを使用して、AWS Marketplace の AWS で VM-Series ファイアウォールを起動し、実稼働環境のファイアウォール設定を変更します。次に、その設定をエクスポートし、VM-Series Auto Scaling テンプレートで使用できるようになった新しい bootstrap.xml ファイルを作成します。

STEP 1 | ファイアウォールを起動する方法については、「AWS における VM-Series ファイアウォールのブートストラップ」を参照してください。

STEP 2 | VM-Series ファイアウォールの Web インターフェイスにアクセスできるように、Elastic Network Interface（ENI）を追加して、Elastic IP アドレス（EIP）を関連付けます。詳細は、「AWS での VM-Series ファイアウォールの起動」を参照してください。

STEP 3 | EIP アドレスを使用して、ファイアウォールの Web インターフェイスにログインします（ユーザー名とパスワードは admin）。

STEP 4 | 管理者ユーザー アカウントの安全なパスワードを追加します（**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））。

STEP 5 | （任意）実稼働環境を守るようにファイアウォールを設定します。

STEP 6 | ファイアウォールへの変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

STEP 7 | 管理者アカウントの新しい API キーを生成します。この新しいキーを新規ファイルにコピーします。この API キーは、VM-Series Auto Scaling テンプレートを起動するときに入力する必要があります。AWS サービスは API キーを使用してファイアウォールをデプロイし、オート スケーリングのメトリックを公開します。

STEP 8 | 設定ファイルをエクスポートして、**bootstrap.xml** として保存します。（**Device**（デバイス） > **Setup**（セットアップ） > **Operation**（操作） > **Export Named Configuration Snapshot**（名前付き設定スナップショットのエクスポート））。

STEP 9 | テキスト エディタで bootstrap.xml ファイルを開き、管理インターフェイス設定を削除します。

```
        </service>
        <ip-address>192.168.10.16</ip-address>
        <netmask>255.255.255.0</netmask>
        <default-gateway>192.168.10.1</default-gateway>
        <hostname>PA-VM</hostname>
      </system>
      <setting>
        <config>
          <rematch>yes</rematch>
        </config>
        <management>
          <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
          <initcfg>
            <type>
              <dhcp-client>
                <send-hostname>yes</send-hostname>
                <send-client-id>no</send-client-id>
                <accept-dhcp-hostname>no</accept-dhcp-hostname>
                <accept-dhcp-domain>no</accept-dhcp-domain>
              </dhcp-client>
            </type>
            <ip-address>192.168.10.16</ip-address>
            <netmask>255.255.255.0</netmask>
            <default-gateway>192.168.10.1</default-gateway>
            <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJ4d1dEaHFWQ3
            VEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXllczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTRnhZdDdXUlFY
          </initcfg>
        </management>
```

STEP 10 | （PAN-OS 8.0 設定をエクスポートした場合に必要）Palo Alto Networks サーバーを検証する設定が無効になっていることを確認します。`<server-verification>no</server-verification>` を確認します。

STEP 11 | 検証が **yes** になっている場合、**no** に変更します。

STEP 12 | ファイルを保存します。以上で、「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）の起動」に進むことができます。

アプリケーション テンプレートとファイアウォール テンプレート間の SQS メッセージング

firewall-v2.0.template を使用してデプロイされた VM-Series ファイアウォールがトラフィックを検出し、受信トラフィックを自動的に配布するネットワーク ロード バランサーに送信できるように、ファイアウォール テンプレートにはメッセージの Simple Queue Service をモニターする Lambda 関数が含まれています。このメッセージにより、Lambda 関数は新しいネットワーク ロード バランサーの情報を取得し、ファイアウォールで自動的に NAT ポリシー ルールを作成して、トラフィックをネットワーク ロード バランサーの IP アドレスに送信できます。AWS インフラストラクチャ内でトラフィックを正しくルーティングするために、メッセージにはネットワーク ロード バランサーが属する DNS、VPC ID、AZ に関する基本情報を含める必要もあります。

独自のアプリケーション テンプレートを作成している場合、アプリケーション テンプレートをセットアップして、VM-Series Auto Scaling テンプレート バージョン 2.0 内の ファイアウォール テンプレートが使用する SQS URL に、次に示す 2 つのタイプのメッセージを投稿し、環境内で

 ©2023 Palo Alto Networks, Inc.

トラフィックを配布する必要があるネットワーク ロード バランサーの情報を取得する必要があります。

- 新しいネットワーク ロード バランサーが使用できるようになったときにファイアウォールに通知する ADD-NLB メッセージ。
- ネットワーク ロード バランサーが停止し、使用できなくなったときにファイアウォールに通知する DEL-NLB メッセージ。

各メッセージ タイプの以下の例には、サンプルの値が含まれています。これらのメッセージは、デプロイに合う値を使用して変更する必要があります。

ADD-NLB メッセージ

```
msg_add_nlb= { 'MSG-TYPE': 'ADD-NLB', 'AVAIL-ZONES': [{'NLB-
IP':'192.168.2.101', 'ZONE-NAME':'us-east-2a', 'SUBNET-ID':
 'subnet-2a566243'}, {'NLB-IP':'192.168.12.101', 'ZONE-NAME':'us-
east-2b', 'SUBNET-ID': 'subnet-2a566243 '}], 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', 'VPC-ID':
 'vpc-42ba9f2b', 'NLB-NAME': 'publicelb1' }
```

DEL-NLB メッセージ

```
msg_del_nlb= { 'MSG-TYPE': 'DEL-NLB', 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', }
```

Amazon SQS キューにメッセージを送信する方法についての詳細は『AWS ドキュメント』を参照し、アプリケーション テンプレートでのメッセージの作成方法を確認するにはサンプル アプリケーション テンプレート パッケージの **describe_nlb_dns.py** を確認してください。

AWS 用 VM-Series Auto Scaling テンプレート（v2.0）によるスタックの更新

スタックの更新により、VM-Series Auto Scaling テンプレート（firewall-v2.0.template）でデプロイするリソースを変更できます。既存のデプロイメントを削除してソリューションを再デプロイする代わりに、スタックの更新を行って以下のパラメータを変更します。

- ライセンス – BYOL と PAYG の間で切り替えるか、1 つの PAYG バンドルから別の PAYG バンドルへ切り替えます。
- その他のスタック リソース – Amazon マシン イメージ（AMI）ID、AWS インスタンス タイプ、オート スケーリング グループのキー ペアなどの起動設定パラメータを変更します。ファイアウォールの管理者ユーザー アカウントに関連付けられた API キーを更新することもできます。

> *AMI-ID* を変更すると、異なる *PAN-OS* バージョンを使用して *VM-Series* ファイアウォールの新しいインスタンスをデプロイできます。

VM-Series Auto Scaling テンプレートをデプロイすると、オート スケーリング グループと起動設定が自動的に作成されます。起動設定とは、オート スケーリング グループが EC2 インスタンスを起動するために使用するテンプレートで、AMI ID、インスタンス タイプ、オート スケーリング グループのキー ペアなどのパラメータが指定されます。更新済みのパラメータを使用して VM-Series ファイアウォールを起動するには、最初にスタックを更新してから、各 AZ で既存の

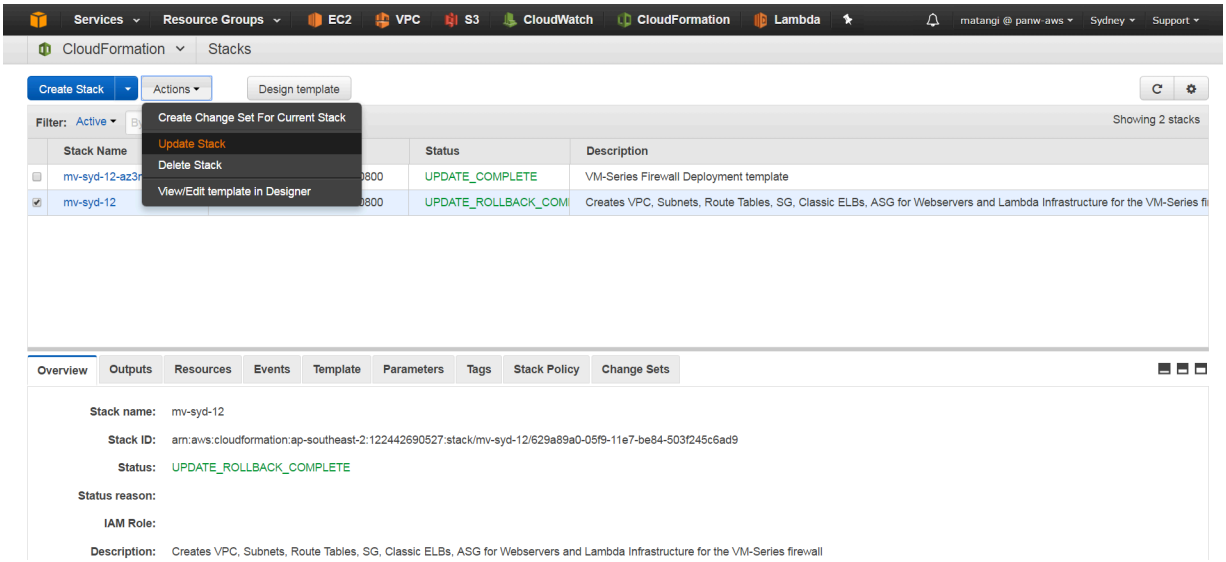
 ©2023 Palo Alto Networks, Inc.

オート スケーリング グループを削除する必要があります。サービスの中断を防ぐには、最初に 1 つの AZ でオート スケーリング グループを削除して、新しいファイアウォール インスタンスが更新済みのスタック パラメータを使用して起動するのを待機します。次に、他の AZ で変更を行う前に、ファイアウォールが更新内容を継承していることを確認します。

重要なアプリケーションの場合は、メンテナンス期間中にスタックの更新を実行してください。

スタックを直接更新することも、変更セットを作成することもできます。このドキュメントで説明しているワークフローでは、手動でスタックの更新を実行します。

STEP 1 | AWS CloudFormation コンソールで、更新する親スタックを選択し、**Actions**（アクション） > **Update Stack**（スタックの更新）の順に選択します。



STEP 2 | 更新するリソースを変更します。

- PAN-OS バージョン — PAN-OS バージョンを変更するには、使用するバージョンの AMI ID を調べ、ID を入力します。
- ライセンス オプション — BYOL から PAYG へ、または PAYG バンドル 1 と 2 の間で切り替えます。

BYOL に切り替える場合、必ず認証コードをブートストラップ パッケージに含めてください（ステップ 3 および 5 を参照）。

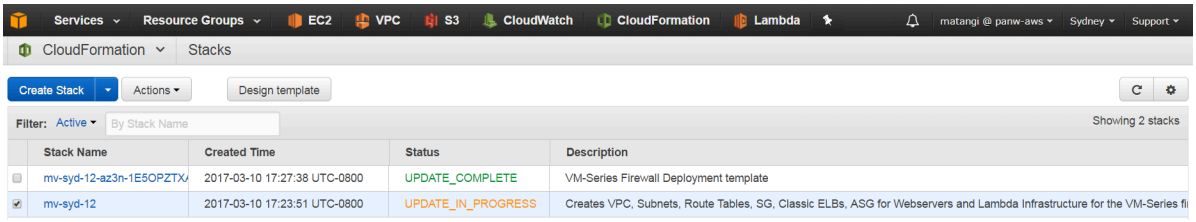
PAYG バンドル バージョン 1 と 2 の間で切り替える場合、VM-Series ファイアウォールの AMI ID を調べます。

- その他のスタック リソース — AMI ID、インスタンス タイプ、セキュリティ グループ、スタック リソースのキー ペア、またはファイアウォールの管理者ユーザー アカウントに関連付けられた API キーを変更できます。

新しい管理者ユーザー アカウントを作成するか、ファイアウォールの既存の管理者の認証情報を変更する場合、そのスタックを更新して更新済みの API キーを使用して新しいファイアウォールをデプロイするには、「管理者アカウントの変更とスタックの更新」のワークフローに従う必要があります。

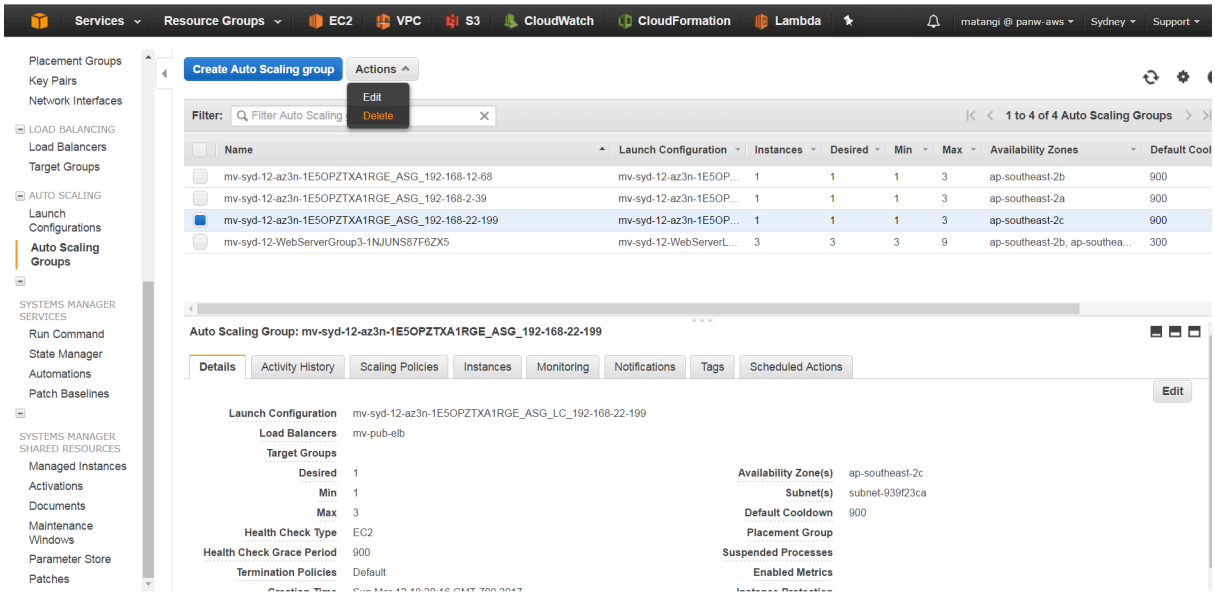
©2023 Palo Alto Networks, Inc.

STEP 3 | 通知に同意して変更内容を確認し、**Update**（更新）をクリックしてスタックの更新を開始します。



STEP 4 | **EC2 dashboard**（**EC2** ダッシュボード） > **Auto Scaling Groups**（オート スケーリング グループ）で、ASG を削除する AZ を選択します。

ASG を削除すると、自動的に新しい ASG の再デプロイのプロセスがトリガーされます。新しい ASG のファイアウォールでは更新済みのスタック設定が使用されます。



STEP 5 | 新しい ASG で VM-Series ファイアウォールを起動するために更新済みのパラメータが使用されていることを確認します。

段階的なロールアウト プロセスを使用して新しい ASG を十分にテストし、ファイアウォールがトラフィックを正しく処理することを確認します。その後、1 時間待ってから次の ASG に移ります。

STEP 6 | ステップ 4 と 5 を繰り返し、他の AZ の ASG を置換します。

管理者アカウントの変更とスタックの更新（v2.0）

テンプレートがすでにデプロイされているときに、VM-Series ファイアウォールの管理アカウントのパスワードを変更したり、新しい管理ユーザー アカウントを作成したりするには、新しい API キーを生成し、管理ユーザー アカウント用のその新しい API キーでテンプレート スタックを更新する必要があります。また、更新した管理ユーザー アカウントで新しいファイアウォール インスタンスを設定するには、ファイアウォール設定をエクスポートし、そのファイルを

©2023 Palo Alto Networks, Inc.

bootstrap.xml に名前変更してから、VM-Series Auto Scaling テンプレートで使用される S3 ブートストラップ フォルダにアップロードする必要があります。

STEP 1 | ファイアウォールの Web インターフェイスにログインし、既存の管理ユーザーの認証情報を変更するか、新しいアカウントを作成します。

STEP 2 | API キーを生成します。

STEP 3 | 現在アクティブな設定をエクスポートして、そのファイル名を bootstrap.xml に変更します。

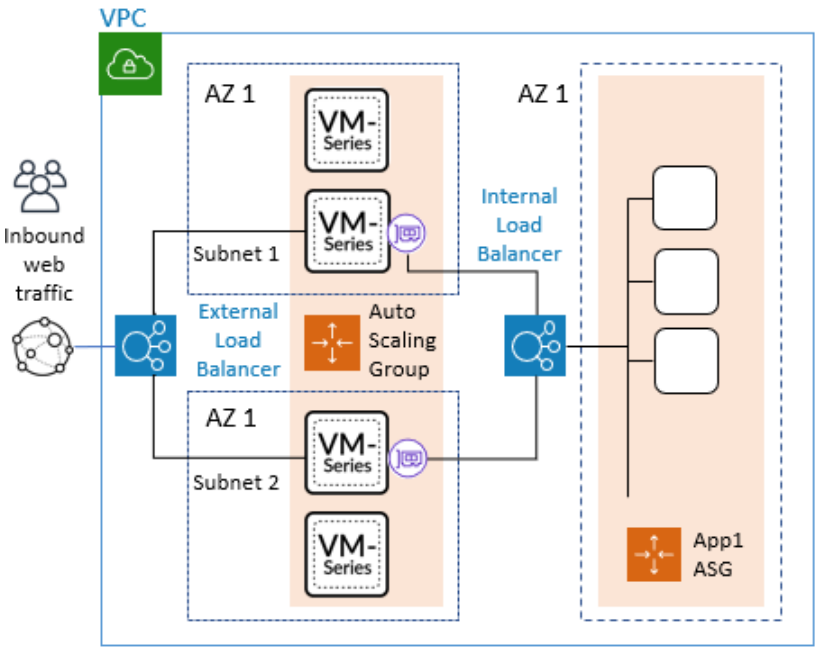
STEP 4 | この bootstrap.xml ファイルを S3 ブートストラップ フォルダにアップロードします（「bootstrap.xml ファイル（v2.0）のカスタマイズ」を参照してください）。

STEP 5 | スタックの API キーを更新し、新しく起動したファイアウォールの管理者アカウントが更新されていることを確認します。

「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）によるスタックの更新」を参照してください。

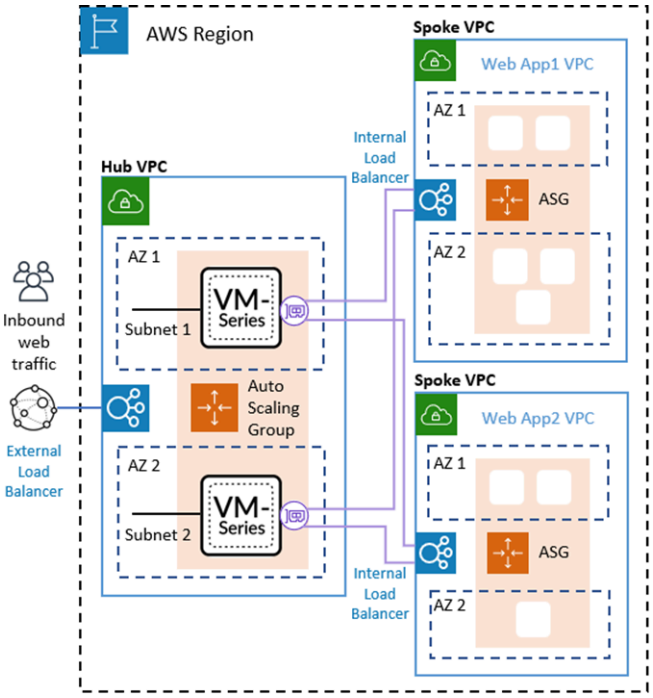
AWS バージョン 2.1 用 VM-Series オート スケーリングテンプレート

VM-Series Auto Scaling テンプレートを使用することで、VM-Series ファイアウォールの 1 つのオート スケーリング グループ（ASG）をデプロイして、インターネットから AWS 上のアプリケーション ワークロードへのインバウンド トラフィックを保護できます。次に示すように、VM-Series ファイアウォール ASG とアプリケーション ワークロードを 1 つの VPC 内にデプロイできます。



©2023 Palo Alto Networks, Inc.

また、次に示すように中央管理 VPC にファイアウォール ASG をデプロイし、同じリージョン内の個別の VPC にアプリケーション ワークロードをデプロイして、ハブ アンド スポーク アーキテクチャを構成できます。



ハブ アンド スポーク アーキテクチャでは、多数のアプリケーション、VPC、またはアカウントを含む AWS デプロイメントへの集中型セキュリティと接続の提供を効率化できます。このアーキテクチャにより俊敏性が向上します。ネットワーク セキュリティ管理者はファイアウォール VPC を管理し、DevOps 管理者またはアプリケーション開発者はアプリケーション VPC を管理できます。

ファイアウォール *VPC* に接続するアプリケーション *VPC* にインターネット ゲートウェイ（*IGW*）がなく、Prisma Public Cloud などの継続的監視およびセキュリティ コンプライアンス サービスを使用していることを確認します。

VPC とインターネットの間のトラフィックを監視して保護するには、1 つまたは複数の AWS アカウントを使用できます。1 つの VPC 内で中央管理型ファイアウォールを使用することで、複数の VPC や複数のアカウントで構成されるデプロイメントのコストを削減できます。

アプリケーション ワークロードを柔軟に保護できるようにするため、バージョン 2.1 では VM-Series ファイアウォール ASG に面した外部ロード バランサーと、アプリケーション ワークロードに面した内部ロード バランサー（ILB）の両方に、アプリケーション ロード バランサーまたはネットワーク ロードバランサーをデプロイできます。

アプリケーション ロード バランサーがアプリケーション ワークロードに面している場合は、VPC ピアリングを使用してファイアウォール VPC をアプリケーション VPC に接続できます。NLB がアプリケーション ワークロードに面している場合は、VPC ピアリングまたは AWS Private Link を使用してファイアウォールとアプリケーション VPC を接続できます。以下にこの要約を示します。

©2023 Palo Alto Networks, Inc.

ファイアウォール VPC LB（外部）	アプリケーション VPC LB（内部）	接続方法
ALB	NLB	AWS Private Link
NLB	NLB	AWS Private Link
NLB	ALB	VPC ピアリング
ALB	ALB	VPC ピアリング

1 つの VPC にデプロイする場合は、上記の表のロード バランサーの組み合わせをすべて使用できます。

グリーンフィールド（新しい VPC とアプリケーション）およびブラウンフィールド（既存の VPC とアプリケーション）の両方のユース ケースでテンプレートをデプロイできます。

テンプレート	新規	既存
ファイアウォール	firewall-new-vpc-v2.1.template panw-aws-same-vpc-v2.1.template	firewall-existing-vpc-v2.1.template panw-aws-same-vpc-v2.1.template
アプリケーション	panw-aws-nlb-new-vpc-v2.1.template panw-aws-alb-new-vpc-v2.1.template	panw-aws-alb-existing-vpc-v2.1.template panw-aws-nlb-existing-vpc-v2.1.template

AWS 用 VM-Series Auto Scaling テンプレート（v2.1）で使用されるコンポーネント

AWS 用 VM-Series Auto Scaling テンプレートの構成要素を以下に示します。

- VM-Series ファイアウォール テンプレート
- アプリケーション テンプレート
- Lambda 関数
- Panorama
- ブートストラップ ファイル

VM-Series ファイアウォール テンプレート

ファイアウォール テンプレートは、2 つ以上の可用性ゾーン（AZ）にまたがるオート スケーリング グループ内に、インターネットに接続する外部ロード バランサーと VM-Series ファイアウォールをデプロイします。外部ロード バランサーは着信 VPC トラフィックを VM-Series ファイアウォール プールに分散します。この外部ロード バランサーとして、アプリケーション ロード バランサー（ALB）またはネットワーク ロード バランサー（NLB）を使用できます。VM-Series ファイアウォールは、オート スケーリングを可能にするカスタム PAN-OS メトリックを自動的に公開します。

©2023 Palo Alto Networks, Inc.

テンプレート	概要
firewall-new-vpc-v2.1.template	新しい VPC の 2 ～ 4 つの可用性ゾーンにファイアウォール スタックをデプロイします。
firewall-existing-vpc-v2.1.template	既存の VPC の 2 ～ 4 つの可用性ゾーンにファイアウォール スタックをデプロイします。 既存の VPC にデプロイするには、以下の情報を入力する必要があります。 • VPC ID • インターネット ゲートウェイ IDこれは既存のゲートウェイです。 • 管理、Untrust、Trust、NAT ゲートウェイ、および Lambda サブネットのサブネット CIDR リスト。テンプレートはこれらのサブネットを作成するときに CIDR を使用します。 新しい ELB を作成することを選択した場合は、テンプレートによりファイアウォール ASG が ELB バックエンド プールに接続されます。既存の ELB を使用する場合は、ファイアウォール ASG を既存のロード バランサー バックエンドに手動で接続する必要があります。

これらのパラメータの詳細については、「起動前のファイアウォール テンプレートのカスタマイズ（v2.0 および v2.1）」を参照してください。

アプリケーション テンプレート

アプリケーション テンプレートでは、内部ロード バランサー（ILB）と、1 台の Web サーバーで構成される 1 つのオート スケーリング グループが、各可用性ゾーン（AZ）にデプロイされます。

テンプレート	概要
panw-aws-same-vpc-v2.1.template	ファイアウォール VPC と同じ VPC にアプリケーションがデプロイされます。ネットワーク ロード バランサーまたはアプリケーション ロード バランサーを選択できます。
panw-aws-alb-new-vpc-v2.1.template	ALB を内部ロード バランサーとして使用し、ファイアウォール VPC とアプリケーション VPC の間で VPC ピアリングを使用して、アプリケーションを新しい VPC にデプロイします。同一アカウント デプロイメントとクロスアカウント デプロイメントの両方がサポートされています。 以下のパラメータを指定する必要があります。

©2023 Palo Alto Networks, Inc.

テンプレート	概要
	• ハブ アカウント ID • VPC ピアリング用のハブ VPC ID • ハブ VPC trust サブネット CIDRこのテンプレートでは、VPC ピアリングの確立後に可用性ゾーンごとに 1 つの CIDR を使用してルート テーブルを作成します。 • StsAssumeRoleARN（SQS アクセスのためのハブ テンプレートからの出力）
panw-aws-nlb-new-vpc-v2.1.template	NLB を内部ロード バランサーとして使用し、ファイアウォール VPC とアプリケーション VPC 間の通信に NLB エンドポイント サービス/インターフェイスを使用して、アプリケーションを新しい VPC にデプロイします。 以下のパラメータを指定する必要があります。 • ハブ アカウント ID • StsAssumeRoleARN（SQS アクセスのためのハブ テンプレートからの出力）
panw-aws-alb-existing-vpc-v2.1.template	ALB を既存のアプリケーション VPC にデプロイします。アプリケーションの VPC ID と既存のサブネット ID を指定する必要があります。 このテンプレートでは、ロード バランサーがアプリケーション VPC にデプロイされ、Lambda リソースが確立されます。ターゲット ワークロードを既存のすべてのロード バランサーからデタッチし、新しいロード バランサーに接続する必要があります。
panw-aws-nlb-existing-vpc-v2.1.template	NLB を既存のアプリケーション VPC にデプロイします。NLB を内部ロード バランサーとして使用し、ファイアウォール VPC とアプリケーション VPC 間の通信に NLB エンドポイント サービス/インターフェイスを使用して、アプリケーションを新しい VPC にデプロイします。

Lambda 関数

AWS Lambda は、堅牢なイベント駆動型の自動化を提供します。複雑なオーケストレーション ソフトウェアは必要ありません。AWS Lambda は、Simple Queue Service（SQS）を監視し、キューに通知されるロード バランサー（ALB または NLB）について確認します。Lambda 関数は新しいロード バランサーを検出すると、新しい NAT ポリシー ルールを作成して、ASG 内の VM-Series ファイアウォールに適用します。ファイアウォールは、アプリケーションごとに NAT

©2023 Palo Alto Networks, Inc.

ポリシー ルールを設定しています。また、ファイアウォールは、（ポートをロード バランサーの IP アドレスにマップする）NAT ポリシー ルールを使用して、アプリケーション Web サーバーの前にあるロード バランサーにトラフィックを転送します。

また Lambda 関数は、Lambda により Panorama のデバイス グループとテンプレート スタックに追加されたすべての設定項目も削除します。これには VM-Series ファイアウォールにプッシュされた NAT ルール、アドレス オブジェクト、スタティック ルートが含まれます。Lambda 関数はライセンス解除も同様に処理します。

Lambda 関数の詳細については、**Palo Alto Networks AWS AutoScale のドキュメント**を参照してください。

Panorama

Auto Scaling v2.1 を設定するには、Panorama モードの Panorama 管理サーバーが必要です。

Panorama 管理サーバーでは、複数の Palo Alto Networks の次世代ファイアウォールを 1 か所から一元的に監視、管理できます。Panorama ではすべてのアプリケーション、ユーザー、およびネットワークを通過する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全体を保護および制御するアプリケーション有効化ポリシーを作成することができます。Panorama について詳しくない場合は、『Panorama 管理者ガイド』を参照してください。

管理対象ファイアウォールは `init-config.txt` ファイルを使用してブートストラップされます。GitHub リポジトリにサンプル ファイルが用意されているので、既存の Panorama にテンプレート スタックとデバイス グループを作成するときには、これらの設定をコピーできます。

Panorama で作成される *untrust* ゾーンと *trust* ゾーンはすべて小文字である必要があります。

Panorama では DHCP を使用してネットワーク インターフェイスを設定する必要があります。

- eth1/1 のみがデフォルト ルート trust ゾーンおよび unrust ゾーンを自動的に作成します。
- セキュリティ ポリシー ゾーンの名前は `untrust` と `trust` です。

  すべてのゾーン名は小文字である必要があります。

- テンプレートにより、管理者アカウント `pandemo` とパスワード `demopassword` が設定されます。
- VR-<*TemplateStackName*> という命名規則に従って仮想ルーターを作成します。仮想ルーターの ECMP タブで ECMP を有効にします。
- Panorama で DNS サーバー アドレスを設定するには、**Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。**Primary DNS Server**（プライマリ **DNS** サーバー）を 169.254.169.253 に、**Secondary DNS Server**（セカンダリ **DNS** サーバー）を 8.8.8.8 に、**FQDN Refresh Time (sec)**（**FQDN** 更新時間（秒））を 60 に設定します。Panorama では、AWS の内部ロード バランサーの FQDN を解決するため、AWS DNS サーバーの IP アドレスが必要となります。FQDN 更新時間は、Panorama が新たに検出された内部ロード バランサーをコミットする間隔です。

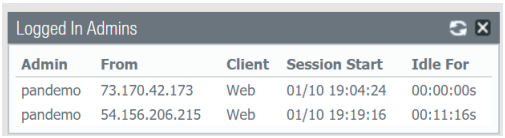
アプリケーション テンプレートの起動後に、Lambda により以下の情報が Panorama に取り込まれます。

©2023 Palo Alto Networks, Inc.

- NAT ポリシー
- アプリケーション テンプレートの LB のアドレス オブジェクト
- 仮想ルーターのスタティック ルート
- Tcp81 サービス オブジェクト

v2.1 ファイアウォール テンプレートには AWS NAT ゲートウェイが含まれます。このゲートウェイは、ファイアウォールが更新の取得、Panorama への接続、および AWS CloudWatch へのメトリックの公開のためにアウトバウンド リクエストを開始するときに使用されます。また、NAT ゲートウェイにはゾーンごとに Elastic IP アドレスがアタッチされています。

AWS 用 Auto Scale テンプレートを使用するには、以下の Panorama リソースが必要です。

Panorama API キー	Panorama API キーは API の認証に必要です。Lambda は API キーを使用してテンプレートとデバイス グループのオプションを自動設定します。API キーを生成するには、「API キーの取得」を参照してください。
Panorama ライセンス無効化キー	このテンプレートでは、Panorama からライセンス キーを無効化するために、「Verify Update Server Identity（更新サーバー ID の確認）」が有効になっていることと、ライセンス無効化 API キーが必要です。ライセンス無効化キーは、「ライセンス API キーのインストール」の説明に従って Palo Alto カスタマー サポート ポータルから入手してください。
Panorama VM-Auth-Key	vm-auth-key は、ブートストラップされたファイアウォールが Panorama に接続し、それぞれのブートストラップ設定を受信できるようにするために必要です。「Panorama で VM 認証キーを生成」を参照してください。
Panorama 管理インターフェイスへのアクセス	• ポート **443**（**HTTPS**）– ファイアウォール テンプレートを初めてデプロイした場合は、HTTPS を開いたままにしておきます。これにより、Lambda が Panorama に接続できます。Panorama で次の接続確認を受け取るまで待ちます。  Logged In Admins Admin / From / Client / Session Start / Idle For pandemo 73.170.42.173 Web 01/10 19:04:24 00:00:00s pandemo 54.156.206.215 Web 01/10 19:19:16 00:11:16s ポート 443 を保護するには、接続を許可する接続元 IP アドレス範囲と、NAT ゲートウェイに割り当てられている EIP を指定します。2 つの NAT ゲートウェイがあり、これらのゲートウェイには EIP が関連付けられています。AWS で NAT ゲートウェイの EIP を確認するには、**VPC** > **NAT Gateways**（**NAT** ゲートウェイ）の順に移動します。HTTPS のセキュリティ グループの EIP 情報をメモします。

©2023 Palo Alto Networks, Inc.

	• ポート **3978** – ポート 3978 はすべての IP アドレスからのトラフィックを受信できる必要があります。

ブートストラップ ファイル

GitHub Auto Scaling リポジトリには **`init-cfg.txt`** ファイルが用意されています。これにより、VM-Series ファイアウォールには以下の操作のための基本設定が含まれます。

- インターフェイス スワップの実行。これにより VM-Series ファイアウォールの **`untrust`** トラフィックは eth0 に AWS ENI を使用します。
- デバイス グループとテンプレートの設定のための Panorama との通信。

Auto Scaling GitHub リポジトリには、最初に使用できる基本設定が用意されています。Auto Scaling ソリューションでは、データプレーン インターフェイスと管理インターフェイスをスワップし、ロード バランサーが Web トラフィックを VM-Series ファイアウォールの Auto Scaling 層に転送できるようにする必要があります。Amazon ELB との管理インターフェイス マッピングの詳細はAmazon ELB で使用する管理インターフェイスのマッピングを参照してください。

AWS 用 VM-Series Auto Scaling テンプレート（v2.1）のデプロイ計画

デプロイを開始する前に、以下のリソースを参照してください。

- テンプレートの機能とアカウントの計画の概要については、「Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング」を参照してください。
- 起動前のファイアウォール テンプレートのカスタマイズ（v2.0 および v2.1）。このトピックに記載されている基本パラメータはすべてのテンプレート バージョンに適用されます。
- AWS 用 VM-Series Auto Scaling テンプレート（v2.0 および v2.1）でのダイナミック スケーリングの仕組み

  これらのコンセプトはすべてのテンプレート バージョンに適用されます。

ファイアウォール テンプレートの起動（v2.1）

ファイアウォール テンプレートとアプリケーション テンプレートを同じ VPC または個別の VPC にデプロイすることを選択できます。

このテンプレートはハブ アンド スポーク アーキテクチャをサポートしています。このアーキテクチャでは、ファイアウォール テンプレートを 1 つの AWS アカウントでデプロイし、それをハブとして使用して、同じ AWS アカウントまたは異なる AWS アカウントに属するアプリケーション（スポーク）を保護できます。

このワークフローでは、ファイアウォール テンプレートを使用して、外部ロード バランサーと VM-Series ファイアウォールをデプロイする方法を説明します。このテンプレートを起動する前に、Panorama で vm-auth-key を設定しておく必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | 「AWS 用 VM-Series Auto Scaling テンプレート（v2.1）のデプロイ計画」および「AWS 用 VM-Series Auto Scaling テンプレート（v2.0 および v2.1）の計画」のチェックリストを確認してください。

以下の作業が完了していることを確認します。

- （PAYG のみ）使用する PAYG バンドルの EULA を確認して同意した。
- （BYOL のみ）デプロイメントで必要となる数のファイアウォールをサポートしているバンドルの認証コードを取得した。この認証コードを `authcodes` という名前（拡張子なし）のテキスト ファイルに保存し、この `authcodes` ファイルをブートストラップ パッケージの `/license` フォルダに保管する必要があります。

  バンドルではなく個別の認証コードを使用すると、ファイアウォールは、ファイルに含まれている最初の認証コードのライセンス キーのみを検索します。

- VM-Series Auto Scaling v2.1 テンプレートの起動に必要なファイルを GitHub リポジトリからダウンロードした。

©2023 Palo Alto Networks, Inc.

STEP 2 | `init-cfg.txt` ファイルを変更して `/config` フォルダにアップロードした。

Panorama を使用して VM-Series ファイアウォールをブートストラップするため、`init-cfg.txt` ファイルを次のように変更する必要があります。`bootstrap.xml` ファイルは不要です。

```
type=dhcp-client
```

```
ip-address=
```

```
default-gateway=
```

```
netmask=
```

```
ipv6-address=
```

```
ipv6-default-gateway=
```

```
hostname=
```

```
vm-auth-key=
```

```
panorama-server=
```

```
panorama-server-2=
```

```
tplname=AWS-tmplspoke1
```

```
dgname=AWS-dgspoke1
```

```
dns-primary=169.254.169.253
```

```
dns-secondary=8.8.8.8
```

```
op-command-modes=mgmt-interface-swap
```

```
dhcp-send-hostname=yes
```


©2023 Palo Alto Networks, Inc.

```
dhcp-send-client-id=yes
```

```
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
```

```
vm-series-auto-registration-id=
```

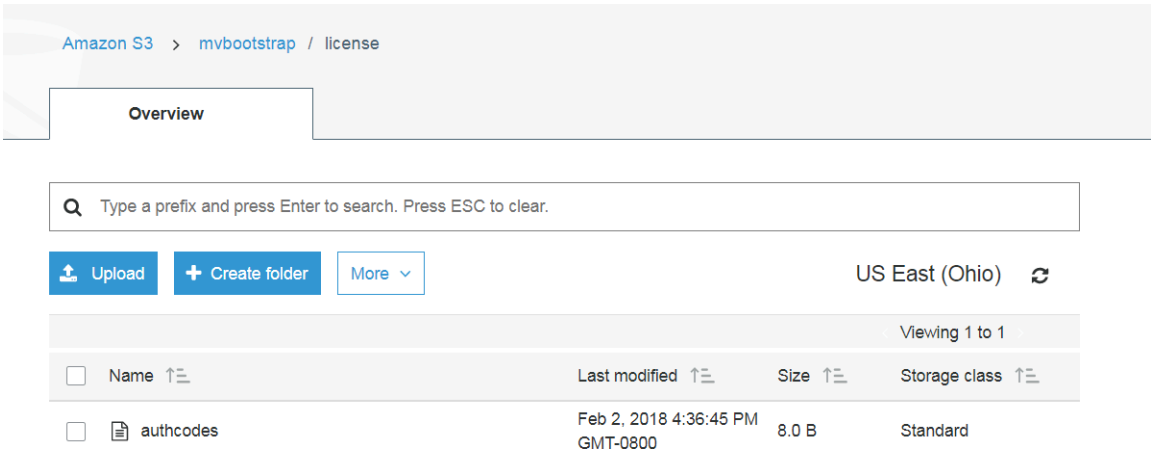
```
vm-series-auto-registration-pin-value=
```

op-command-modes=mgmt-interface-swap が存在していることを確認します。これは、AWS 上の VM-Series ファイアウォールで管理インターフェイス（mgmt）とデータプレーン インターフェイス（ethernet 1/1）をスワップするためのコマンドです。ロード バランサーの DNS 名前解決にかかる時間を短縮するため、AWS DNS サーバーの IP アドレス（169.254.169.253）を使用します。

VM-Seriesファイアウォールインスタンスのデプロイ時に、デバイス証明書を自動的にインストールするために、init-cfg.txtファイルにデバイス証明書自動登録PINを追加する必要があります。

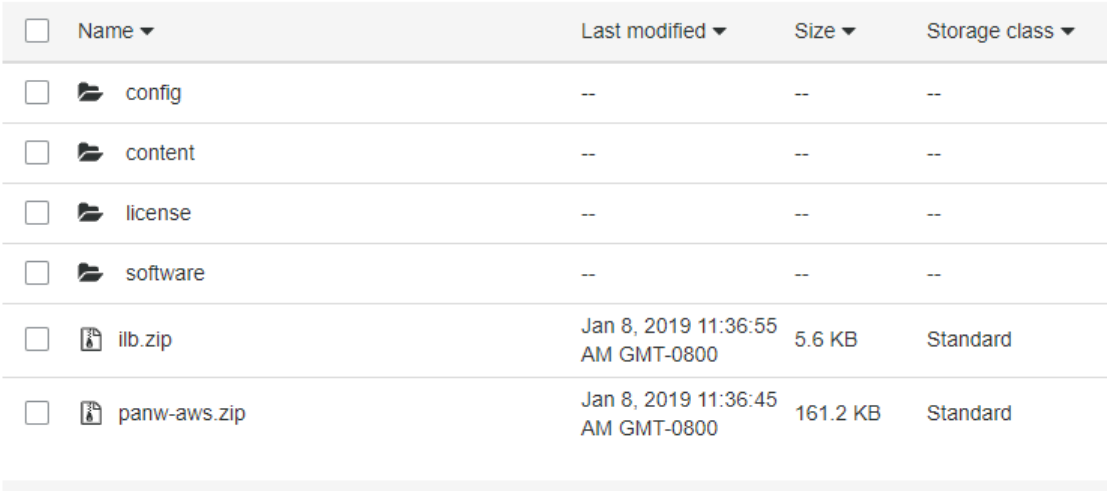
STEP 3 | （BYOL のみ）ライセンスの認証コードをブートストラップ パッケージの **/license** フォルダに追加します。

1. テキスト エディタを使用して **authcodes** という名前（拡張子なし）の新しいファイルを作成します。
2. BYOL ライセンスの認証コードをこのファイルに追加し、保存します。認証コードはバンドルを表し、デプロイメントで必要な数のファイアウォールをサポートしていなければなりません。バンドルではなく個別の認証コードを使用すると、ファイアウォールは、ファイルに含まれている最初の認証コードのライセンス キーのみを検索します。



©2023 Palo Alto Networks, Inc.

STEP 4 | ファイアウォール テンプレート（`panw-aws-zip`）とアプリケーション テンプレート（`ilb.zip`）の Lambda コードを S3 バケットにアップロードします。ブートストラッピングに使用する S3 バケットを使用できます。



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
ilb.zip	Jan 8, 2019 11:36:55 AM GMT-0800	5.6 KB	Standard
panw-aws.zip	Jan 8, 2019 11:36:45 AM GMT-0800	161.2 KB	Standard

アプリケーション スタックがファイアウォールとは異なるアカウントで管理されている場合は、ファイアウォール テンプレートと同じ AWS リージョンに、アプリケーション アカウントを使用して別の s3 バケットを作成し、`ilb.zip` をその s3 バケットにコピーします。

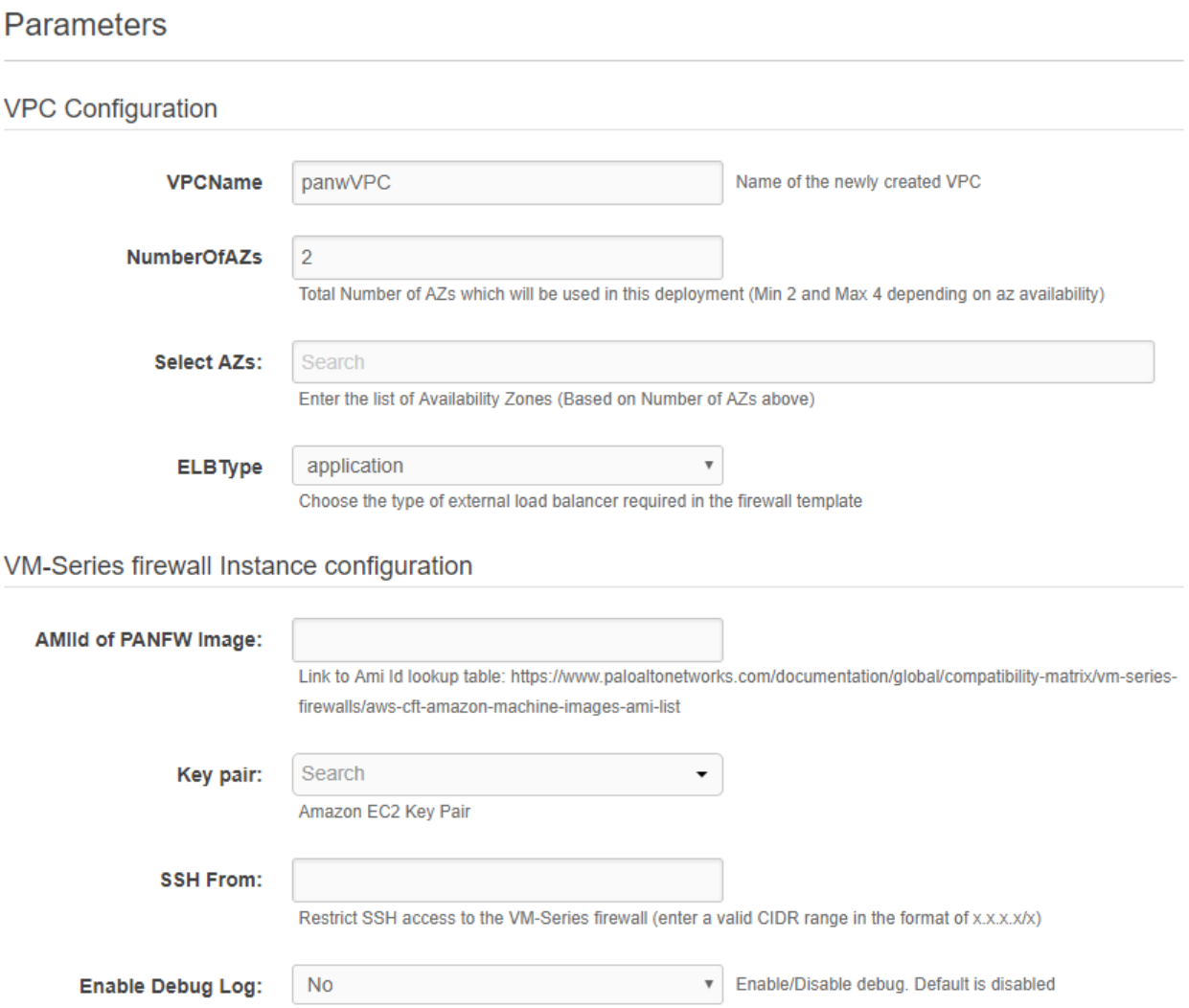
STEP 5 | ファイアウォール テンプレートを選択します。

1. AWS 管理コンソールで **CloudFormation** > **Create Stack**（スタックを作成）の順に選択します。
2. Upload a template to Amazon S3（Amazon S3 にテンプレートをアップロード）を選択し、ファイアウォールと同じ VPC または別の VPC に、テンプレートが起動するリソースをデプロイします。Open（開く）とNext（次へ）をクリックします。
3. スタック名を指定します。スタック名により、このテンプレートを使用してデプロイされるすべてのリソースを識別できます。

©2023 Palo Alto Networks, Inc.

STEP 6 | VPC のパラメータを設定します。

1. 少なくとも 2 つの可用性ゾーンを選択してください。



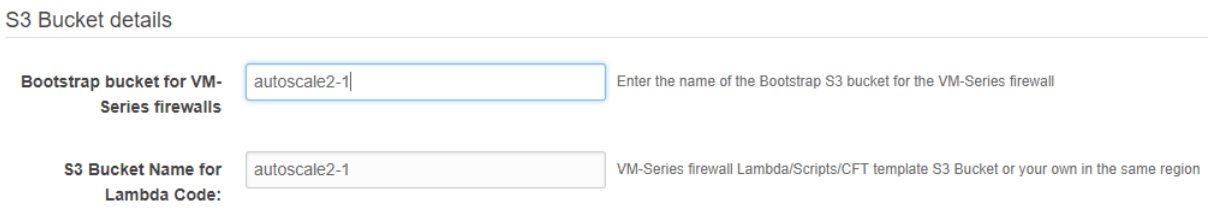
2. VM-Series ファイアウォールの AMI ID を検索して入力します。AMI ID が、使用する AWS リージョン、PAN-OS バージョン、および BYOL または PAYG ライセンス オプションと一致していることを確認します。
3. ファイアウォールを起動するための EC2 の **Key pair**（キー ペア）を（ドロップダウン リストから）選択します。ファイアウォールにログインするには、このキー ペアの名前と、関連付けられている秘密鍵を入力しなければなりません。
4. **SSH from**（**SSH** アクセス元）フィールドでは、ファイアウォールは Panorama により管理され、管理インターフェイスの EIP が割り当てられていません。EIP を割り当てる場合は、接続元の IP 範囲を設定します。
5. デバッグ ログを有効化する場合は、**Enable Debug Log**（デバッグ ログを有効化）で**Yes**（はい）を選択します。デバッグ ログを有効化すると、デプロイメントの間

©2023 Palo Alto Networks, Inc.

題のトラブルシューティングに役立つ詳細なログが生成されます。これらのログはスタック名を使用して生成され、AWS CloudWatch に保存されます。

デフォルトでは、テンプレートは VM-Series ファイアウォールのスケーリング パラメータとして CPU 利用率を使用します。 カスタム PAN-OS メトリックは、すでに指定してあるスタック名に対応した CloudWatch 名前空間で自動的に公開されます。

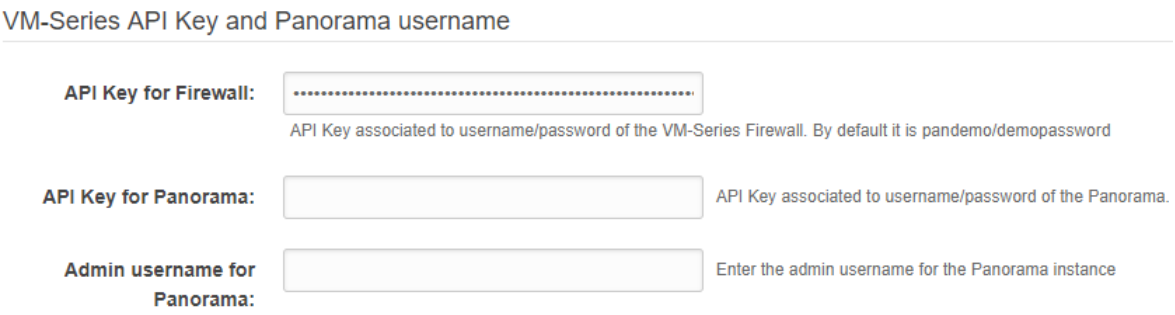
STEP 7 | Amazon S3 バケット（1 つまたは複数）の名前を指定します。



1. ブートストラップ パッケージが格納された S3 バケットの名前を入力します。

   ブートストラップ バケットが適切にセットアップされていないか、またはバケット名を正しく入力しないとブートストラップ プロセスが失敗し、ファイアウォールにログインできなくなります。ロード バランサーのヘルス チェックも失敗します。
2. panw-aws.zip ファイルが格納された S3 バケットの名前を入力します。前述したように、ブートストラップと Lambda コードに 1 つの S3 バケットを使用できます。

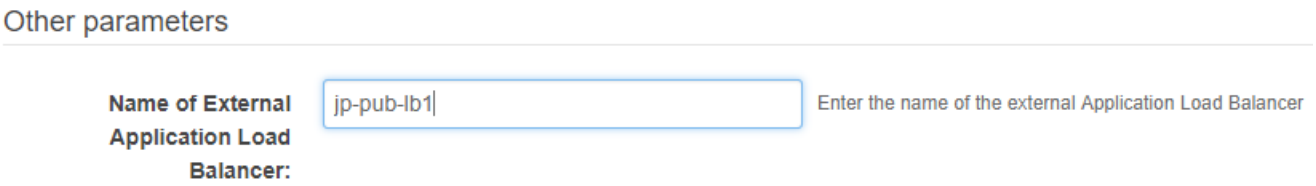
STEP 8 | ファイアウォールと Panorama への API アクセスを有効化するキーを指定します。



1. ファイアウォールが API コールを認証するために使用するキーを入力します。デフォルトのキーはサンプル ファイルに基づいており、テストおよび評価にのみ使用してます。本番のデプロイメントでは、API コール専用に別の PAN-OS ログインを作成して、関連するキーを生成しなければなりません。
2. AWS Lambda が Panorama に対して API コールを発行できるようにするための API キーを入力します。本番のデプロイメントでは、API コール専用に別のログインを作成して、関連するキーを生成しなければなりません。

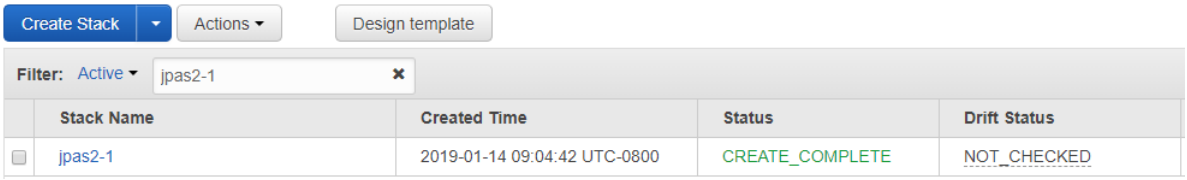
©2023 Palo Alto Networks, Inc.

STEP 9 | アプリケーション ロード バランサー名を入力します。



STEP 10 | テンプレート設定を確認し、テンプレートを起動します。

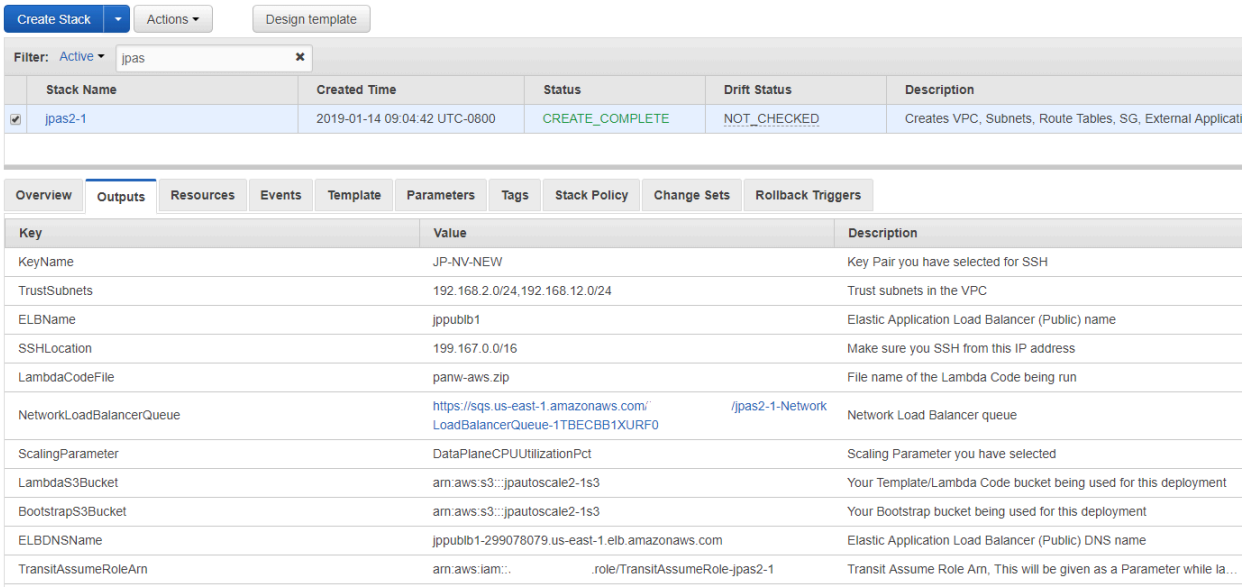
1. **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（このテンプレートによって **AWS CloudFormation** が **IAM** リソースが作成される可能性があることを理解しています）を選択します。
2. **Create**（作成）をクリックしてテンプレートを起動します。CREATE_IN_PROGRESS イベントが表示されます。
3. デプロイメントが成功すると、ステータスが CREATE_COMPLETE に変わります。



©2023 Palo Alto Networks, Inc.

STEP 11 | テンプレートが必要なリソースをすべて起動したことを確認します。

1. EC2 ダッシュボードで、Auto Scaling Groups（オート スケーリング グループ）を選択します。各可用性ゾーンに、VM-Series ファイアウォールの ASG が 1 つあることを確認します。ASG 名のプレフィックスにはスタック名が含まれます。
2. AWS 管理コンソールで、リソース リストの出力を表示するスタック名を選択します。
3. 出力は以下の図のようになります。
   - ネットワーク ロード バランサー キューの名前をメモします。
   - Elastic Load Balancer のパブリック DNS 名をメモします。



ファイアウォールが起動してトラフィックを処理できるようになるまで最大 *20* 分かかります。

テストまたは本番のデプロイメントが終了した後で、料金の発生を中止するには、スタックを完全に削除するしか方法はありません。インスタンスをシャットダウンしたり、*ASG* の最大数を *0* にするだけでは不十分です。

STEP 12 | 以下のファイアウォール テンプレート情報を保存します。これらの値は、アプリケーション テンプレートのデプロイ時に入力として提供する必要があります。

- 各可用性ゾーンの **NAT** ゲートウェイの **IP** アドレス – この IP アドレスは、NAT ゲートウェイの EIP を使用する Lambda が必要に応じて Panorama と通信できるようにするために、HTTPS アクセスを Panorama に制限する際に必要です。
- ネットワーク ロード バランサー **SQS URL** – ファイアウォール スタックの Lambda 関数は、このキューをモニタリングして、デプロイされているネットワーク ロード バランサーについて学習し、Panorama がネットワーク ロード バランサーの IP アドレスにトラフィックを転送できるようにするための NAT ポリシー ルールを（各アプリケーションに 1 つずつ）ファイアウォール上で作成します。

©2023 Palo Alto Networks, Inc.

アプリケーション テンプレートの起動（v2.1）

アプリケーション テンプレートにより、完全なサンドイッチ トポロジをデプロイでき、オートスケーリング ソリューションを評価できます。このアプリケーション テンプレートは、ファイアウォール テンプレートを使用してデプロイした VM-Series ファイアウォール グループの背後に、アプリケーションまたはネットワーク ロード バランサーと、Web サーバーのペアをデプロイします。

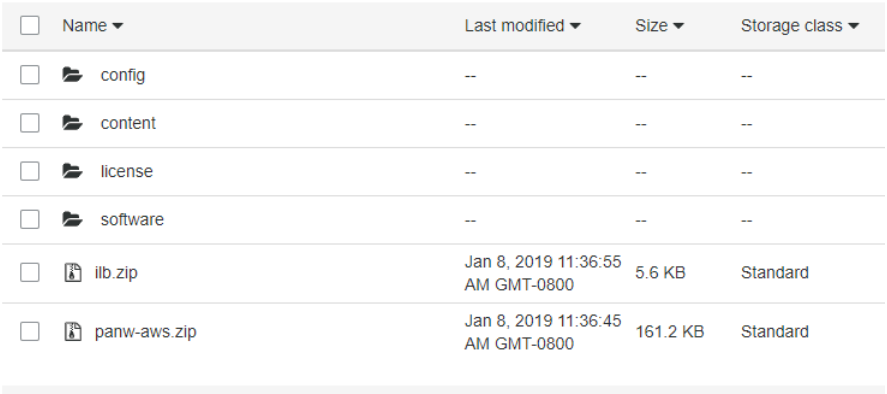
このテンプレートはソリューションの評価に使用しますが、本番用には各自のテンプレートをカスタマイズします。カスタム テンプレートでは、アプリケーション テンプレートとファイアウォール テンプレートの間の SQS メッセージングを有効化します。

アプリケーション テンプレートを起動する際には、ファイアウォール テンプレートをデプロイした VPC でアプリケーション テンプレートをデプロイするのか、あるいは別の VPC でアプリケーション テンプレートをデプロイするのかに応じて適切なテンプレートを選択する必要があります。「ELB サービスへのトラフィックの有効化（v2.0 および v2.1）」を参照してください。

STEP 1 | アプリケーション テンプレートを起動する S3 バケットを作成します。

- クロス アカウント デプロイメントの場合は新しいバケットを作成します。
- アカウントが 1 つの場合は、新しいバケットを作成するか、または以前に作成した S3 バケットを使用できます（すべての処理に 1 つのバケットを使用できます）。

STEP 2 | ilb.zip ファイルを S3 バケットにアップロードします。



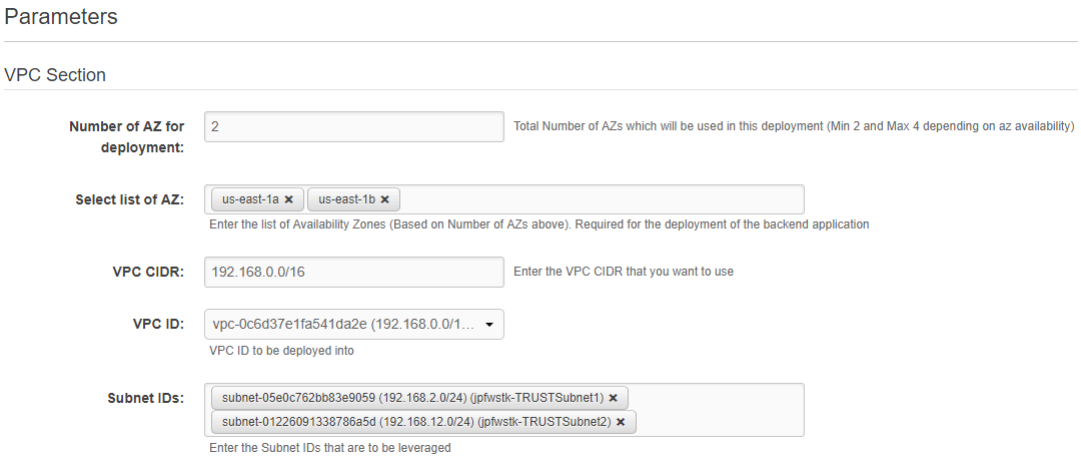
STEP 3 | 起動するアプリケーション起動テンプレートを選択します。

1. AWS 管理コンソールで、**CloudFormation** > **CreateStack** を選択します。
2. Upload a template to Amazon S3（Amazon S3 にテンプレートをアップロード）を選択し、ファイアウォールと同じ VPC または別の VPC に、テンプレートが起動するリソースをデプロイします。**Open**（開く）と**Next**（次へ）をクリックします。
3. スタック名を指定します。スタック名により、このテンプレートを使用してデプロイされるすべてのリソースを識別できます。

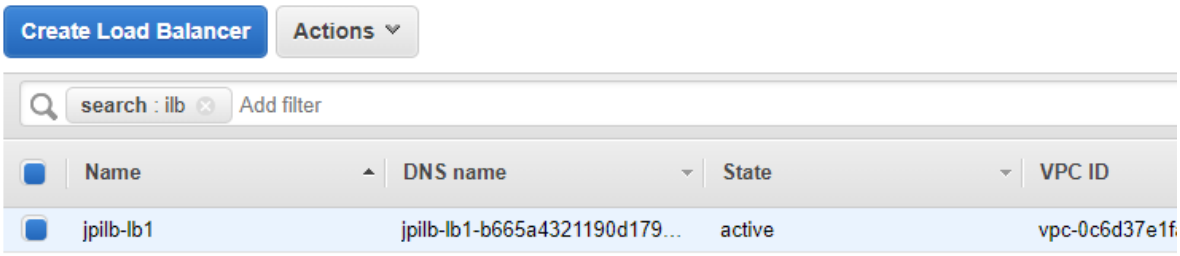
©2023 Palo Alto Networks, Inc.

STEP 4 | VPC とネットワーク ロード バランサーのパラメータを設定します。

1. Select list of AZ（可用性ゾーンの選択リスト）で、セットアップがまたがる 2 つの可用性ゾーンを選択します。同じ VPC でデプロイする場合は、ファイアウォール テンプレートに対して選択したのと同じ可用性ゾーンを選択してください。
2. 新しい VPC にデプロイする場合は、VPC の CIDR ブロックを入力します。デフォルトの CIDR は 192.168.0.0/16 です。
3. 同じ VPC にデプロイする場合は、以前の VPC を選択して Trust サブネットを使用します。

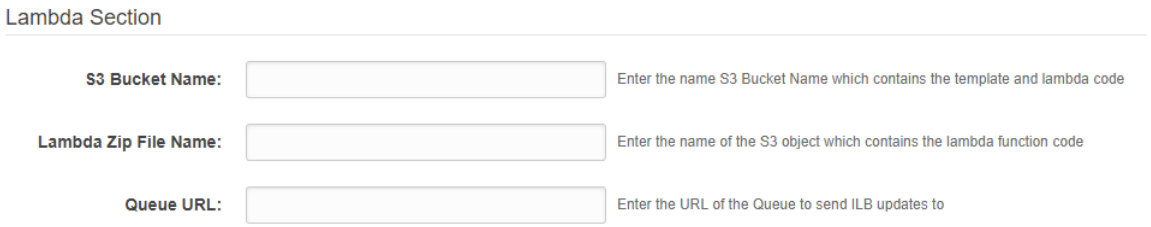


STEP 5 | ロード バランサーのタイプを選択します。



STEP 6 | Lambda のパラメータを設定します。

1. ilb.zip が格納されている S3 バケットの名前を入力します。
2. ZIP ファイルの名前を入力します。
3. 以前にコピーしてある SQS URL を貼り付けます。



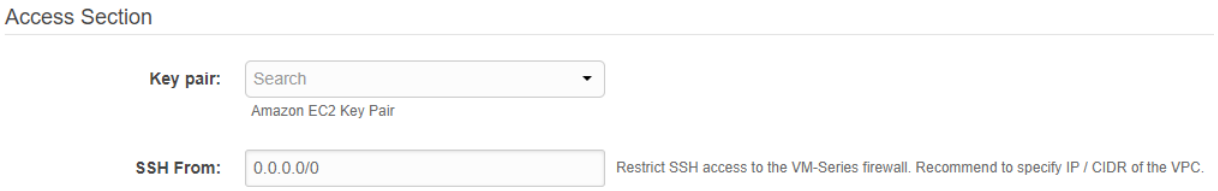
©2023 Palo Alto Networks, Inc.

STEP 7 | ニーズに合わせて Web サーバーの EC2 インスタンス タイプを修正します。



STEP 8 | Web サーバーを起動するための EC2 のキー ペアを（ドロップダウン リストから）選択します。Web サーバーにログインするには、このキー ペアの名前と、関連付けられている秘密鍵を入力しなければなりません。

STEP 9 | 管理アクセス目的でのみサーバーにアクセスするネットワークの IP アドレスを選択します。Web トラフィックは、ファイアウォール テンプレートの起動時にコピーした ELBDNS を通過します。

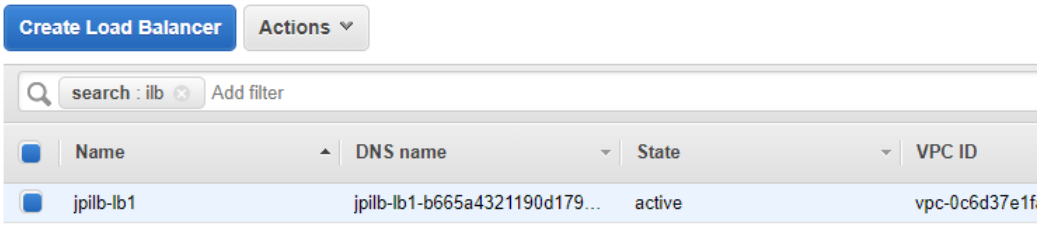


STEP 10 | テンプレート設定を確認し、テンプレートを起動します。

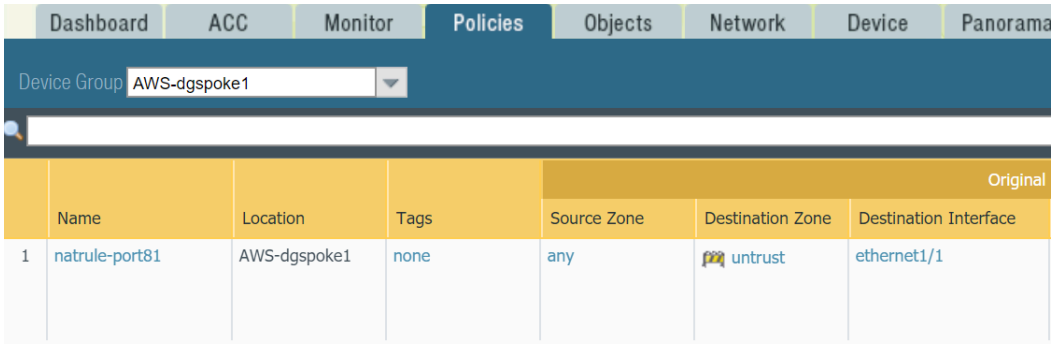
©2023 Palo Alto Networks, Inc.

STEP 11 | アプリケーション テンプレートの起動完了後、Web ページがアクティブになるまで最大 20 分かかることがあります。

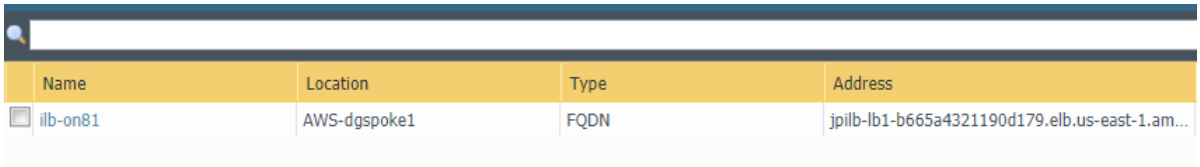
1. アプリケーション テンプレート ロード バランサーがアクティブとしてマークされていることを確認します。



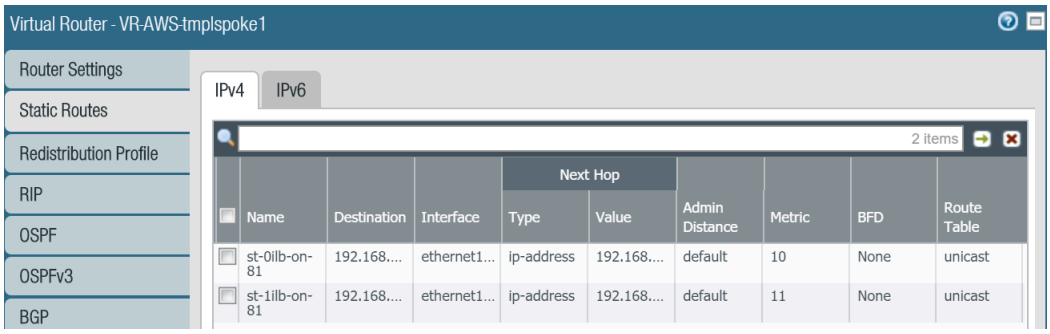
2. Panorama の NAT オブジェクトがデバイス グループに含まれていることを確認します。



3. Panorama のアドレス オブジェクトがデバイス グループに含まれていることを確認します。



4. Panorama の静的ルートがテンプレート スタックに含まれていることを確認します。



STEP 12 | 前に保存したアプリケーション ロード バランサーの DNS 名を取得して、Web ブラウザに入力します。

©2023 Palo Alto Networks, Inc.

STEP 13 | 正常に起動すると、ブラウザには次のような出力が表示されます。



Congratulations, you have successfully launched VM-Series ASG CloudFormation. This file is coming from Webserver Region: us-east-1

StackID: arn:aws:cloudformation:us-east-1: :stack/jpappstk1/1c197cb0-18f4-11e9-b92e-0ab87eb901cc

StackName: jpappstk1

カスタム Amazon Machine Image（v2.1）の作成

AWS パブリック Marketplace または AWS GovCloud Marketplace に公開された AMI だけを使用するように制限する代わりに、カスタム VM-Series AMI を使用すると、ネットワークで使用する PAN-OS バージョンを含む VM-Series ファイアウォールを柔軟かつ整合性のある方法でデプロイできます。カスタム AMI を使用すると、必要な PAN-OS バージョンのファイアウォールのデプロイにかかる時間を短縮できます。これは、AWS パブリック Marketplace または AWS GovCloud Marketplace で公開されている AMI でファイアウォールをプロビジョンし、ネットワークで使用したい PAN-OS バージョンへのソフトウェア アップグレードを実行するためにかかる時間が削減されるためです。Auto Scaling VM-Series ファイアウォール CloudFormation テンプレートまたは作成した他のテンプレートでカスタム API を使用できるようになります。

BYOL ライセンス、Bundle 1 ライセンス、または Bundle 2 ライセンスでカスタム AMI を作成できます。カスタム AMI を作成するには、ファイアウォールのすべての設定を削除してプライベート データ リセットを行う必要があります。これにより、このワークフローでは完全に設定された既存のファイアウォールを使用する代わりに、AWS Marketplace からのファイアウォールの新しいインスタンスを起動できます。

BYOL バージョンのファイアウォールを使用してカスタム AMI を作成するときには、最初にファイアウォールでライセンスを有効にする必要があります。これにより、ファイアウォールをアップグレードするための PAN-OS コンテンツとソフトウェア更新をダウンロードし、ファイアウォールでライセンスを無効にしてから、プライベート データ リセットを実行してカスタム AMI を作成できます。ライセンスを無効にしないと、このファイアウォール インスタンスに適用したライセンスを失うことになります。

STEP 1 | Marketplace から VM-Series ファイアウォールを起動します。

「VM-Series ファイアウォールの起動」を参照してください。

STEP 2 | （BYOL のみ）ライセンスを有効にします。

 ©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォールに最新コンテンツをインストールします。

STEP 4 | （BYOL のみ）ライセンスを無効にします。

STEP 5 | プライベート データ リセットを実行します。

プライベート データ リセットを実行するとすべてのログが削除され、デフォルト設定が復元されます。

システム ディスクは消去されません。このため、ステップ 4 のコンテンツの更新内容は維持されます。

1. ファイアウォール CLI にアクセスします。
2. 設定のコピーをエクスポートします。
3. すべてのログを削除し、デフォルト設定を復元します。

```
request system private-data-reset
```

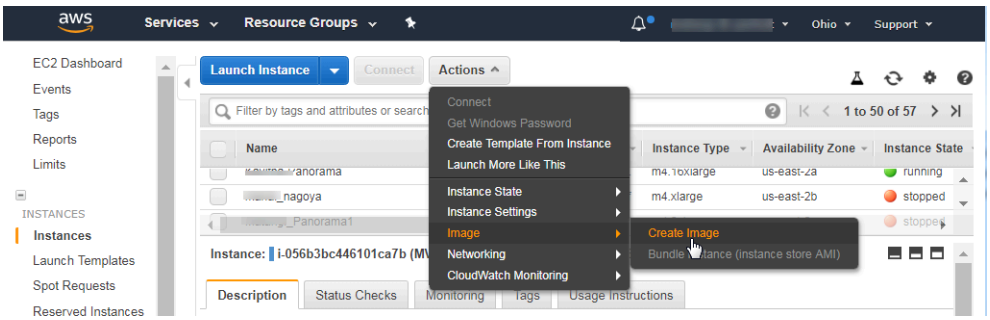
y と入力して確定します。

ファイアウォールが再起動し、デフォルト設定が初期化されます。

©2023 Palo Alto Networks, Inc.

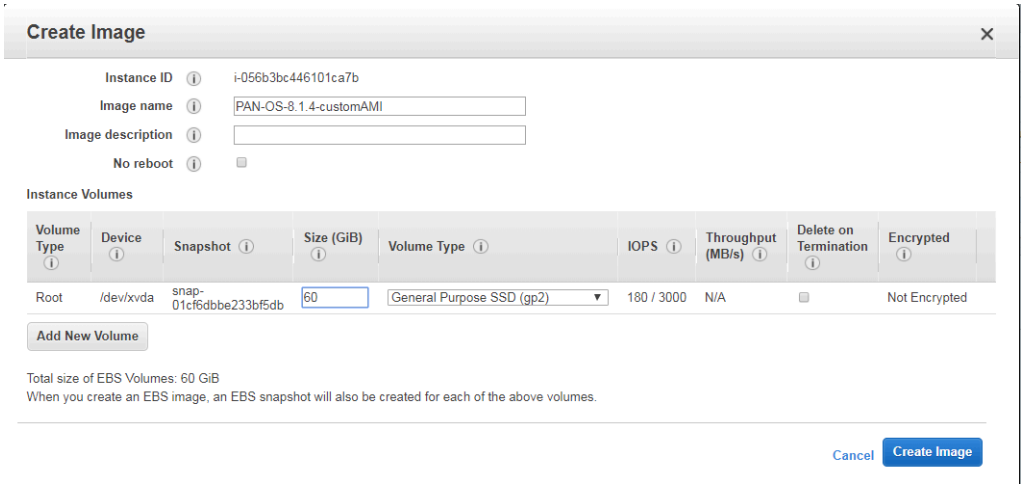
STEP 6 | カスタム AMI を作成します。

1. AWS コンソールにログインし、EC2 Dashboard を選択します。
2. VM-Series ファイアウォールを停止します。
3. VM-Series ファイアウォール インスタンスを選択し、**Image**（イメージ） > **Create Image**（イメージの作成）をクリックします。



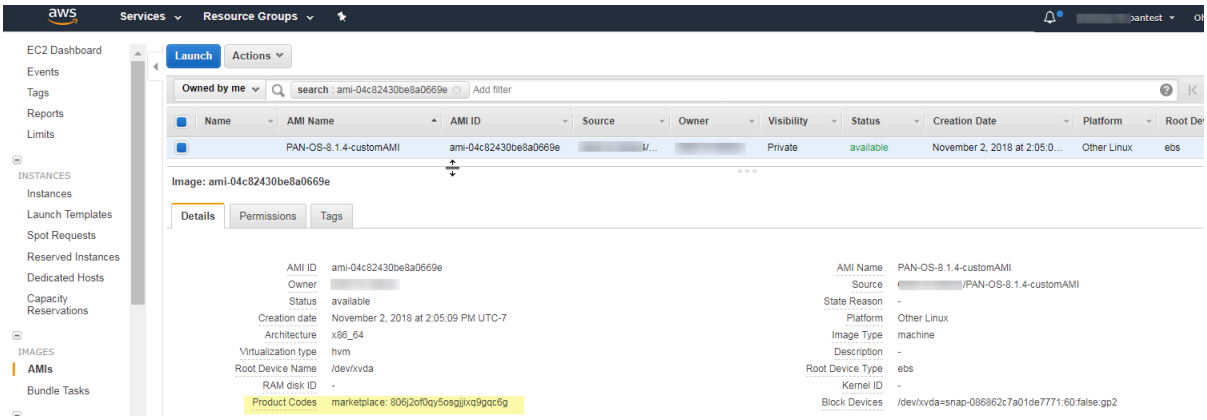
4. カスタム イメージ名を入力し、**Create Image**（イメージの作成）をクリックします。

   ディスク スペースの最小必要容量は 60GB です。



5. カスタム AMI が作成され、正しい製品コードが設定されていることを確認します。
   1. EC2 Dashboard で **AMI**を選択します。
   2. 作成した AMI を選択します。BYOL、Bundle 1、または Bundle 2 のいずれのライセンス オプションで AMI を選択したかどうかに応じて、次のいずれかの製品コードが詳細に表示されます。
      - BYOL—6njl1pau431dv1qxipg63mvah
      - Bundle 1—6kxdw3bbmdeda3o6i1ggqt4km
      - バンドル2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | AWS 上の VM-Series ファイアウォールの EBS ボリュームの暗号化。

Amazon ELB サービスを使用した VM-Series ファイアウォールのオート スケーリング デプロイメントで EBS 暗号化とともにカスタム AMI を使用する予定の場合は、AWS アカウントでデフォルトのマスター キーを使用する必要があります。

VM-Series Auto Scaling テンプレートのクリーンアップ（v2.1）

テンプレートをテスト目的でデプロイした場合は、リソースとコストを節約するためテンプレートを削除します。

STEP 1 | AWS 管理コンソールで **Cloud Formation** > **Create Stack**（スタックを作成）を選択します。

STEP 2 | 以前に起動したファイアウォール テンプレートとアプリケーション テンプレートを見つけ、両方を削除します。

テンプレート スタックの削除の詳細については、What is AWS CloudFormation? を参照してください。

テンプレート スタックを削除しなかった場合、*AWS* からの課金が発生します。

アプリケーション テンプレートとファイアウォール テンプレート間の SQS メッセージング（v2.1）

いずれかのファイアウォール テンプレートを使用してデプロイされた VM-Series ファイアウォールは、トラフィックを検出して、着信トラフィックの自動分配の分配先ロード バランサーへ送信できます。このため、ファイアウォール テンプレートには Simple Queue Service でメッセージを監視する Lambda 関数が含まれています。このメッセージにより、Lambda 関数は新しいロード バランサーの情報を取得し、ファイアウォールで自動的に NAT ポリシー ルールを作成して、トラフィックをロード バランサーの IP アドレスに送信できます。AWS インフラストラクチャ内でトラフィックを正しくルーティングするために、メッセージにはロード バランサーが属する DNS、VPC ID、AZ に関する基本情報を含める必要もあります。

独自のアプリケーション テンプレートを作成している場合、ファイアウォール テンプレートが使用する SQS URL に ADD メッセージと DEL メッセージを投稿し、環境内でトラフィックを分

©2023 Palo Alto Networks, Inc.

配する必要があるロード バランサーの情報を取得するように、アプリケーション テンプレートをセットアップする必要があります。

- 新しいネットワーク ロード バランサーが使用できるようになったときにファイアウォールに通知する ADD-NLB メッセージ。
- ネットワーク ロード バランサーが停止し、使用できなくなったときにファイアウォールに通知する DEL-NLB メッセージ。
- 新しいアプリケーション ロード バランサーが使用できるようになったときにファイアウォールに通知する ADD-ALB メッセージ。
- アプリケーション ロード バランサーが停止し、使用できなくなったときにファイアウォールに通知する DEL-ALB メッセージ。

各メッセージ タイプの以下の例には、サンプルの値が含まれています。これらのメッセージは、デプロイメントに対応した値を使用して変更する必要があります。

ADD-NLB メッセージ

```
msg_add_nlb= {

       "MSG-TYPE": "ADD-NLB",

       "AVAIL-ZONES": [

       {

           "NLB-IP":"192.168.2.101",

           "ZONE-NAME":"us-east-2a",

           "SUBNET-ID": "subnet-2a566243"

       },

       {

           "NLB-IP":"192.168.12.101",

           "ZONE-NAME":"us-east-2b",

           "SUBNET-ID": "subnet-2a566243 "
```


©2023 Palo Alto Networks, Inc.

```
       }

       ],

            "DNS-NAME": "publicelb1-2119989486.us-
east-2.elb.amazonaws.com",

           "VPC-ID": "vpc-42ba9f2b",

           "NLB-NAME": "publicelb1"

}
```

DEL-NLB メッセージ

```
msg_del_nlb= {

 "MSG-TYPE": "DEL-NLB",

 "DNS-NAME": "publicelb1-2119989486.us-east-2.elb.amazonaws.com",

}
```

ADD-ALB

```
{   "AVAIL-ZONES": [

       {

           "SUBNET-CIDR": "172.32.0.0/24",

           "SUBNET-ID": "subnet-0953a3a8e2a8208a9",

           "ZONE-NAME": "us-east-2a"

       },
```


©2023 Palo Alto Networks, Inc.

```
        {
            "SUBNET-CIDR": "172.32.2.0/24",
            "SUBNET-ID": "subnet-0a9602e4fb0d88baa",
            "ZONE-NAME": "us-east-2c"
        },
        {
            "SUBNET-CIDR": "172.32.1.0/24",
            "SUBNET-ID": "subnet-0b31ed16f308b3c4d",
            "ZONE-NAME": "us-east-2b"
        }
    ],
    "VPC-PEERCONN-ID": "pcx-0538bb05dbe2e1b8e",
    "VPC-CIDR": "172.32.0.0/16",
    "ALB-NAME": "appILB-908-0",
    "ALB-ARN":"arn:aws:elasticloadbalancing:us-
east-2:018147215560:loadbalancer/app/appILB-908-0/1997ed20eeb5bcef",
    "VPC-ID": "vpc-0d9234597da6d9147",
    "MSG-TYPE": "ADD-ALB",
```


 ©2023 Palo Alto Networks, Inc.

```
   "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"
```

```
}
```

DEL-ALB メッセージ

```
{
```

```
   "MSG-TYPE": "DEL-ALB",
```

```
   "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"
```

```
}
```

Amazon SQS Queue へのメッセージの送信方法の詳細については、AWS のドキュメントを参照してください。

AWS 用 VM-Series Auto Scaling テンプレート（v2.1）によるスタックの更新

スタックの更新により、VM-Series Auto Scaling テンプレート ファイアウォール テンプレートがデプロイするリソースを変更できます。既存のデプロイメントを削除してソリューションを再デプロイする代わりに、スタックの更新を行って起動設定パラメータを変更します。

AWS インスタンス タイプ、オート スケーリング グループのキー ペア、およびファイアウォールの管理ユーザー アカウントに関連付けられている API キーを変更できます。

デフォルトの通知の変更またはオート スケーリング アラームの作成のためにスタックを更新する必要はありません。「スケーリング パラメータと CloudWatch メトリックの変更（v2.1）」を参照してください。

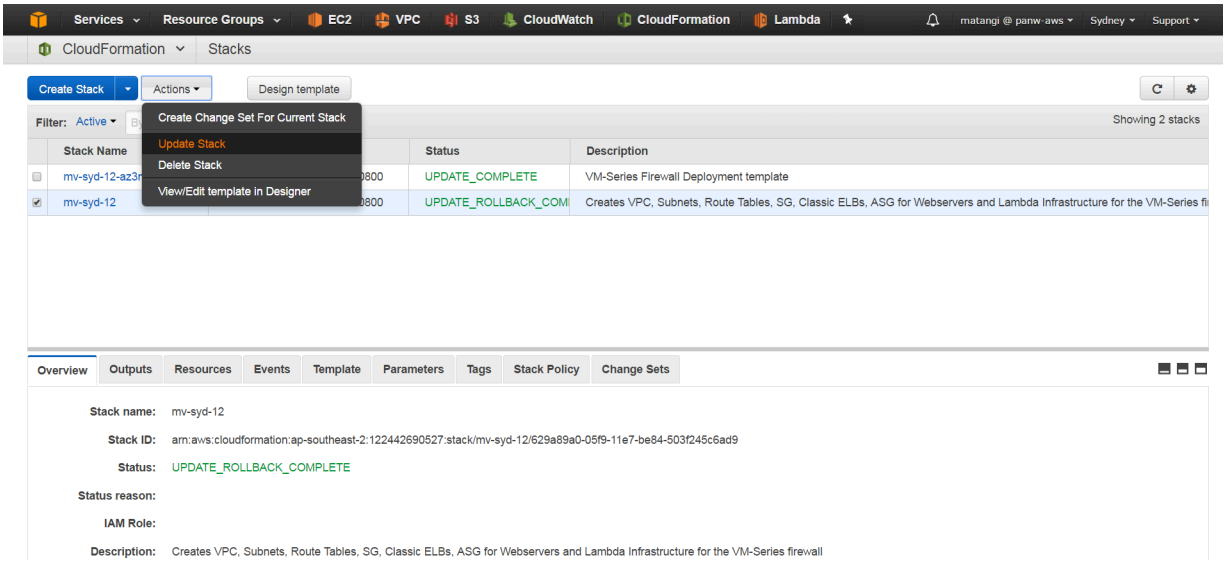
VM-Series Auto Scaling テンプレートをデプロイすると、オート スケーリング グループと起動設定が自動的に作成されます。起動設定は、オート スケーリング グループが EC2 インスタンスを起動するために使用するテンプレートであり、インスタンス タイプ、オート スケーリング グループのキー ペア、およびファイアウォールの管理ユーザー アカウントに関連付けられている API キーなどのパラメータを指定します。

重要なアプリケーションの場合は、メンテナンス期間中にスタックの更新を実行してください。

スタックを直接更新することも、変更セットを作成することもできます。このドキュメントで説明しているワークフローでは、手動でスタックの更新を実行します。

©2023 Palo Alto Networks, Inc.

STEP 1 | AWS CloudFormation コンソールで、更新する親スタックを選択し、**Actions**（アクション） > **Update Stack**（スタックの更新）の順に選択します。

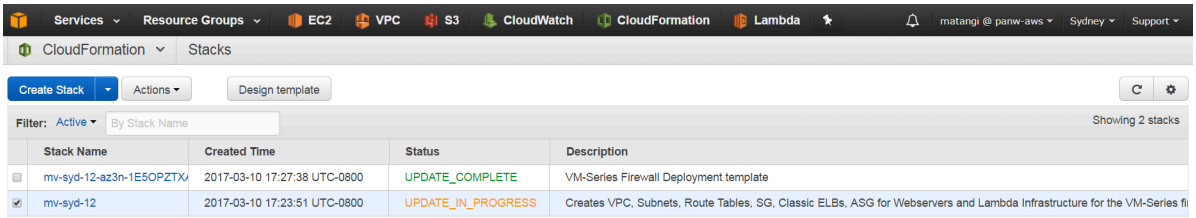


STEP 2 | 更新するリソースを変更します。

インスタンス タイプ、セキュリティ グループ、スタック リソースのキー ペア、またはファイアウォールの管理者ユーザー アカウントに関連付けられた API キーを変更できます。

新しい管理者ユーザー アカウントを作成するか、ファイアウォールの既存の管理者の認証情報を変更する場合、そのスタックを更新して更新済みの API キーを使用して新しいファイアウォールをデプロイするには、「管理アカウントの変更（v2.1）」のワークフローに従う必要があります。

STEP 3 | 通知に同意して変更内容を確認し、**Update**（更新）をクリックしてスタックの更新を開始します。



管理アカウントの変更（v2.1）

テンプレートがすでにデプロイされているときに、VM-Series ファイアウォールの管理アカウントのパスワードを変更したり、新しい管理ユーザー アカウントを作成したりするには、新しい API キーを生成し、管理ユーザー アカウント用のその新しい API キーでテンプレート スタックを更新する必要があります。

STEP 1 | ファイアウォールの Web インターフェイスにログインし、既存の管理ユーザーの認証情報を変更するか、新しいアカウントを作成します。

STEP 2 | API キーを生成します。

 ©2023 Palo Alto Networks, Inc.

STEP 3 | スタックの API キーを更新し、新しく起動したファイアウォールの管理者アカウントが更新されていることを確認します。

「AWS 用 VM-Series Auto Scaling テンプレート（v2.0）によるスタックの更新」を参照してください。

スケーリング パラメータと CloudWatch メトリックの変更（v2.1）

このタスクでは、カスタム PAN-OS メトリックをスケーリング パラメータとして使用してスケール アクションをトリガーする方法を説明します。

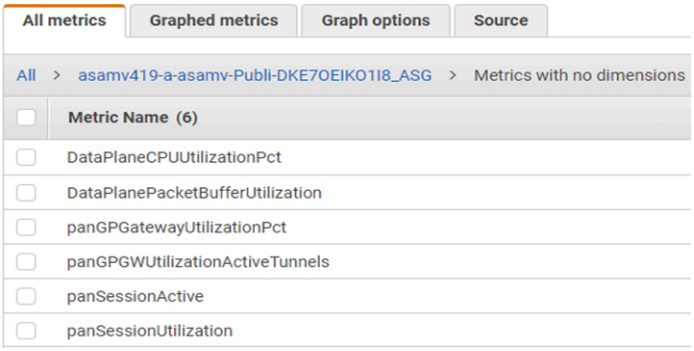
ファイアウォール テンプレートを起動すると、オートスケーリング アクションを定義するときに使用できるスケールイン ポリシーとスケールアウト ポリシーを使用して名前空間が作成されます。ポリシー名には名前空間が次のように含まれています。

- <カスタム名前空間>-scalein - 1 つのインスタンスを削除
- <カスタム名前空間>-scaleout - 1 つのインスタンスを追加

各 PAN-OS メトリックにはデフォルトの通知があります。この通知を削除するか、またはオートスケール アクションに置き換えることができます。メトリックごとに 2 つのアクションを作成します。これは、VM-Series ファイアウォールを追加する時点を決定するアクションと、VM-Series ファイアウォールを削除する時点を決定するアクションです。

STEP 1 | AWS で **Services**（サービス） > **CloudWatch** > **Metrics**（メトリック）を選択します。

STEP 2 | **Custom Namespace**（カスタム名前空間）のリンクを選択し、メトリック リンクを選択して、カスタム PAN-OS メトリックを表示します。



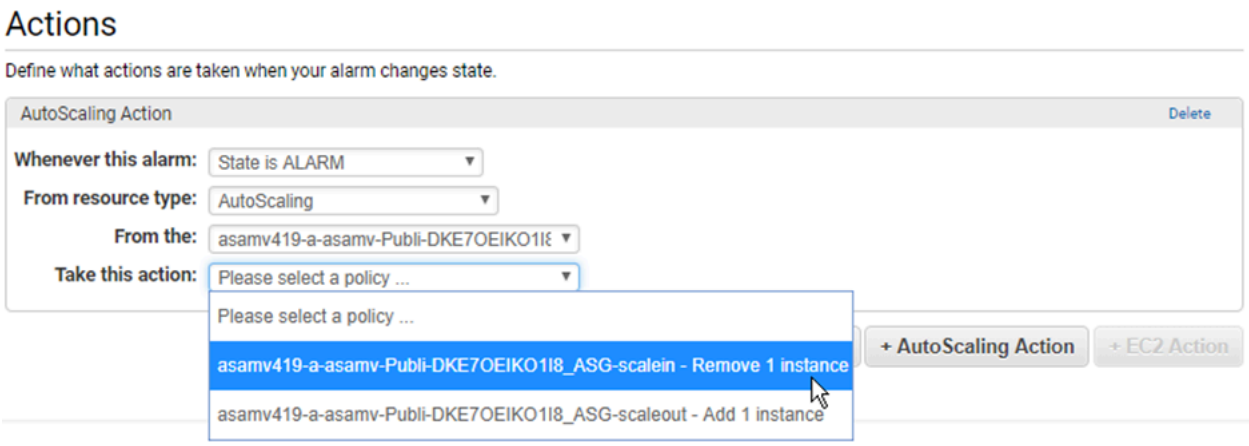
STEP 3 | メトリックを選択するボックスをオンにして、**Graphed metrics**（グラフ化されたメトリック）タブを選択します。

1. **Statistics**（統計）列で統計基準（平均、最小値、最大値など）を選択し、期間を選択します。
2. **Actions**（アクション）列でベル（アラーム作成）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 4 | 設定した期間内に、CPU 使用率が設定した条件に一致または上回ったときにファイアウォールを削除するアラームを定義します。

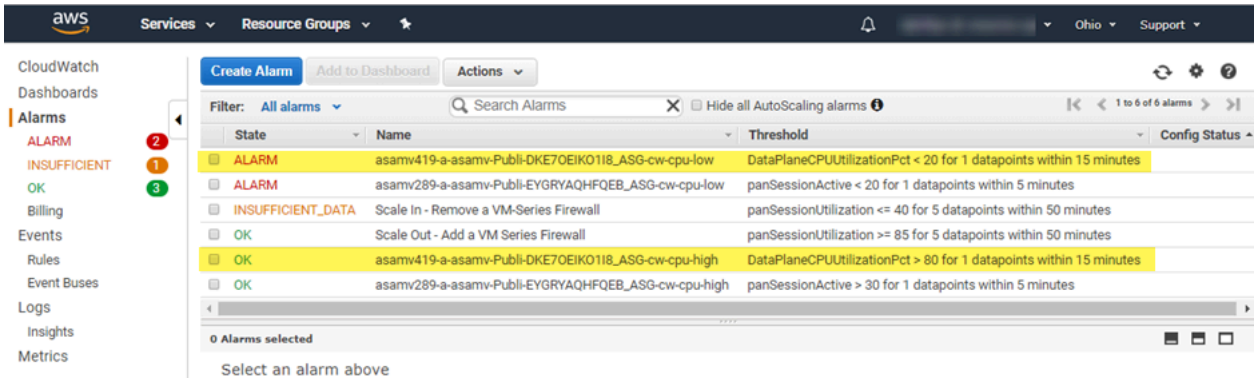
1. **Edit**（編集）を選択して、グラフのタイトルを変更します。
2. **Alarm details**（アラームの詳細）の **Name**（名前）と **Description**（説明）にそれぞれの名前と説明を入力し、演算子を選択し、現行インスタンスを維持する最小値を設定します。最小値を維持できないと、インスタンスが削除されます。
3. **Actions**（アクション）でデフォルトの通知を削除します。
4. **+AutoScaling Action**（+オートスケーリング アクション）を選択します。
   - **From the**（名前空間）リストを使用して名前空間を選択します。
   - **Take this action**（次のアクションを実行する）で、インスタンスを削除するポリシーを選択します。



5. **Create Alarm**（アラームの作成）を選択します。

STEP 5 | CPU 使用率が設定した条件に一致または上回ったときにファイアウォールを追加する 2 番目のアラームを作成します。

STEP 6 | アラームを表示するには、**Services**（サービス） > **CloudWatch** > **Alarms**（アラーム）を選択します。



このウィンドウでアラームを編集するには、編集するアラームの横のボックスをオンにし、**Action**（アクション） > **Edit**（選択）を選択します。

©2023 Palo Alto Networks, Inc.

AWS-VPC でモニターされる属性の一覧

AWS VPC 内で仮想マシンのプロビジョニングあるいは変更を行う際、これらのインスタンスを監視し、ダイナミック アドレス グループで一致条件として使用するタグを取得する方法が 2 つあります。

- **VM** 情報ソース—次世代ファイアウォール上で最大で合計 32 件のタグ（事前定義済みのものが 14、ユーザー定義のキーおよび値のペア（タグ）が 18）を監視できます。
- **AWS Plugin on Panorama**—AWS 用の Panorama プラグインを使用することで、Panorama をパブリック クラウドの AWS VPC に接続し、仮想マシンの IP アドレス対タグのマッピングを取得できます。次に Panorama は、通知用に設定した管理対象の Palo Alto Networks® ファイアウォールに VM 情報を登録します。プラグインを使用すれば、各仮想マシンにつき合計 32 件のタグ（事前定義済みのタグが 11、ユーザー定義のタグが最大 21）を取得できます。

タグ値（名前と値を含む）の最大長は、*116* 文字以下でなければなりません。*Panorama* が *116* 文字を超過しているタグを取得してファイアウォールに登録することはありません。

AWS-VPC でモニターされる属性		ファイアウォール上の **VM** 情報ソース	**AWS Plugin on Panorama**
AMI ID	ImageId.<ImageId string>	はい	はい
Architecture	Architecture.<Architecture string>	はい	いいえ
Availability Zone	AvailabilityZone.<string>	はい	はい
Guest OS	GuestOS.<guest OS name>	はい	いいえ
IAM Instance Profile	Iam-instance-profile.<instanceProfileArn>	いいえ	あり。
インスタンスID	InstanceId.<InstanceId string>	はい	無し
Instance State	InstanceState.<instance state>	はい	無し
インスタンスのタイプ	InstanceType.<instance type>	はい	無し
Key Name	KeyName.<KeyName string>	はい	あり。
Owner ID	Account-number.<OwnerId>	いいえ	はい

©2023 Palo Alto Networks, Inc.

AWS-VPC でモニターされる属性		ファイアウォール上の VM 情報ソース	AWS Plugin on Panorama
この属性値は ENI から取得されます。			
Placement テナント、グループ名	Placement.Tenancy.<string> Placement.GroupName.<string>	はい	あり。
Private DNS Name	PrivateDnsName.<Private DNS Name>	はい	無し
Public DNS Name	PublicDnsName.<Public DNS Name>	はい	あり。
Subnet ID	SubnetID.<subnetID string>	はい	あり。
セキュリティグループ ID	Sg-id.<sg-xxxx>	いいえ	あり。
セキュリティグループ名	Sg-name.<SecurityGroupName>	いいえ	あり。
VPC ID	VpcId.<VpcId string>	はい	あり。
タグ（キー、値）	aws-tag.<key>.<value>	はい、 最大 18 件のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 18 件のタグをファイアウォールで使用できます。	はい、 最大 21 件のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 21 件のタグを Panorama およびファイアウォールで使用できます。

©2023 Palo Alto Networks, Inc.

AWS VPCをモニタリングする際に必要な IAM の許可

VM モニタリングを有効化するには、AWS アクセスキーおよび関連付けられた AWS ログイン認証情報は上記リストの属性に対する許可を取得している必要があります。これらの権限が付与されることで、ファイアウォールはAPI通信を行ったり、AWS VPCの仮想マシンの監視が可能になります。

ユーザーに関連付けられたIAMポリシーは、AmazonEC2ReadOnlyAccessのようなグローバルな読み取り専用アクセスを持っているか、監視を行う属性に対して個別に許可を取得している必要があります。以下の IAM ポリシー例では、AWS VPC のリソースを監視する際の API アクションをリスト化しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeKeyPairs",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs"
            ],
            "Resource": [
                "*"
            ]
}
    ]
}
```


©2023 Palo Alto Networks, Inc.

paloalto TECHDOCS

KVM での VM-Series ファイアウォールのセットアップ

カーネル ベースの仮想マシン（KVM）は、Linux ディストリビューションを実行しているサーバー向けのオープンソースの仮想モジュールです。VM-Series ファイアウォールは、KVM ハイパーバイザを実行している Linux サーバー上にデプロイできます。

このガイドでは、Linux を使用する既存の IT インフラストラクチャが存在しており、Linux および Linux ツールを使用するための基盤があることを前提としています。ここでの説明は、KVM 上に VM-Series ファイアウォールをデプロイする場合にのみ該当するものです。

> KVM 上の VM-Series — 要件と前提条件
> KVM でサポートされているデプロイ
> KVM への VM-Series ファイアウォールのインストール
> VM-Series for KVM のパフォーマンス調整
> Intelligent Traffic Offload インテリジェント トラフィック オフロード

KVM 上の VM-Series — 要件と前提条件

- ネットワーク上の VM-Series に接続するためのオプション
- KVM 上の VM-Series の前提条件

表 **2 : KVM** の **VM-Series** のシステム要件

要件	概要
ハードウェア リソース	VM-Series モデルの最小ハードウェア要件については、「VM-Series システム要件」を参照してください。
ソフトウェア バージョン	互換性マトリックスの、サポートしている KVM ソフトウェアのバージョンを参照してください。
SR-IOV ドライバ	互換性マトリックスの、「PacketMMAP ドライバのバージョン」を参照してください。
DPDK ドライバ	互換性マトリックスの、「DPDK ドライバのバージョン」を参照してください。 KVM上のVM-Seriesで、サポートされているいずれかのNICドライバを使用する場合、デフォルトでDPDKが有効になります。
ネットワーク インターフェイス – ネットワーク インターフェイス カードとソフトウェア ブリッジ	KVM 上の VM-Series では合計 25 個のインターフェイス（1 つの管理インターフェイスと最大 24 個のデータ トラフィック用ネットワーク インターフェイス）をサポートしています。 KVM 上にデプロイされる VM-Series は、Linux ブリッジや Open vSwitch ブリッジといったソフトウェア ベースの仮想スイッチをサポートしています。また、PCI パススルーや SR-IOV 対応アダプタに直接接続することもできます。 PCI パススルーまたは SR-IOV を使用して接続を確立する場合は、SR-IOV または PCI パススルーに使用する物理ポートに vSwitch を構成することはできません。ネットワーク上のホストおよび他の仮想マシンと通信するために、VM-Series ファイアウォールが物理ポートおよび関連する仮想機能（VF）を排他的にそのインターフェイスにアクセスする必要があります。 • Linux ブリッジおよび OVS 上では、e1000 および Virtio ドライバがサポートされています。デフォルトのドライバ rtl8139 はサポートされていません。

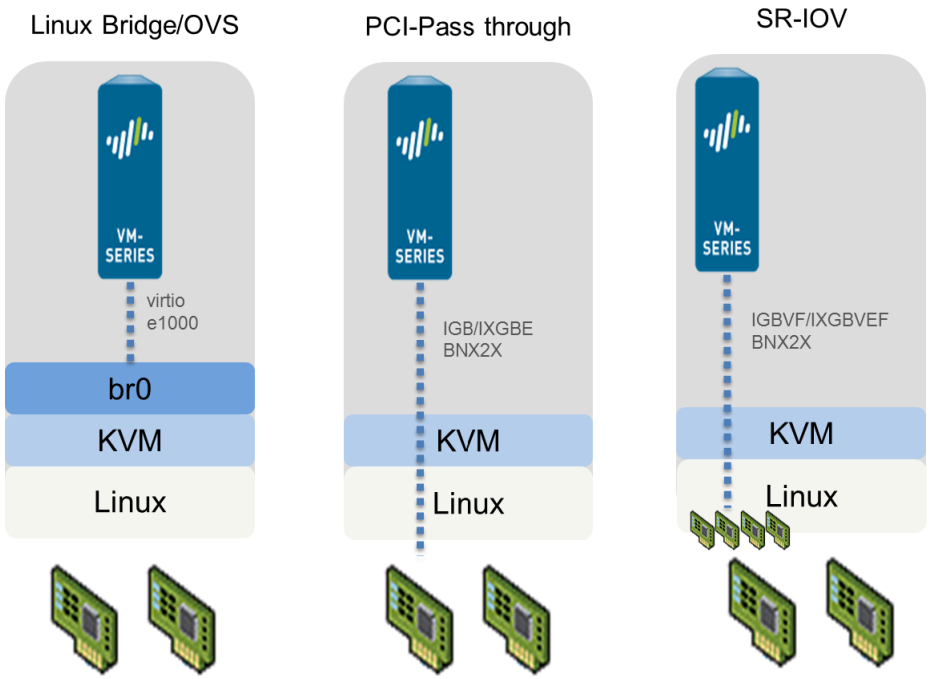
©2023 Palo Alto Networks, Inc.

要件	概要

	• VM-Series ファイアウォールにおける PCI パススルーと SR-IOV のサポートについては、以下のネットワーク カードでテスト済みです。
	  • Intel 82576 ベースの 1G NIC:SR-IOV はすべてのサポート対象 Linux ディストリビューションでサポートされています。PCIパススルー サポート。
	  • Intel 82599 ベースの 10G NIC:SR-IOV はすべてのサポート対象 Linux ディストリビューションでサポートされています。PCIパススルー サポート。
	  • Intel X710 10G NIC：SR-IOV はすべてのサポート対象 Linux ディストリビューションでサポートされています。PCIパススルー サポート
	  • Intel X722 10G NIC：SR-IOV はすべてのサポート対象 Linux ディストリビューションでサポートされています。PCIパススルー サポート
	  • Broadcom 57112 および 578xx ベースの 10G NIC:SR-IOV はすべてのサポート対象 Linux ディストリビューションでサポートされています。PCIパススルーはサポートされません。
	  • Mellanox ConnectX5 10G/25G/50G/100G NIC:SR-IOVは、サポート対象のすべてのLinuxディストリビューションをサポートしています。
	  • 互換性マトリックスの、「PacketMMAPドライバのバージョン」を参照してください。
	
	  *VM-Series* ファイアウォールに割り当てられた *SR-IOV* 対応のインターフェイスは、レイヤー *3* インターフェイスまたは *HA* インターフェイスとして構成する必要があります。

©2023 Palo Alto Networks, Inc.

ネットワーク上の VM-Series に接続するためのオプション



- Linux ブリッジや OVS では、データ トラフィックはソフトウェア ブリッジを介して、同一ホスト上のゲストを接続します。外部と接続する場合、データ トラフィックは、ブリッジの接続先である物理インターフェイスを使用します。
- PCI パススルーでは、データ トラフィックはゲストとその接続先物理インターフェイス間で直接やり取りされます。ゲストに接続されているインターフェイスを、ホストまたはホスト上の他のゲストから使用することはできません。
- SR-IOV では、データ トラフィックはゲストとその接続先仮想機能間で直接やり取りされます。

KVM 上の VM-Series の前提条件

Linux サーバーに VM-Series ファイアウォールをインストールする際には、事前に以下の各セクションの内容を確認してください。

- Linux サーバーの準備
- VM-Series ファイアウォールのデプロイ準備

Linux サーバーの準備

KVMにVM-Seriesファイアウォールをインストールする前に、機能しているLinux環境が存在しており、ネットワークインフラが選択したデプロイ環境が必要とする接続性をサポートしていることを確認してください。

- Linuxサポートの確認
- ネットワークインフラの確認
- Mellanoxソフトウェアツールのインストール

©2023 Palo Alto Networks, Inc.

- KVM上のVM-Seriesファイアウォールの、Mellanox CX5 NIC仮想機能の有効化
- ホスト設定の確認

Linuxサポートの確認

インストールをサポートする適切な環境が存在していることを確認します。

- Linux ディストリビューションのバージョンを確認します。サポートするバージョンについては、互換性マトリックスの「KVM用VM-Series」を参照してください。
- 仮想マシンの作成と管理に必要な KVM ツールとパッケージ（Libvirt など）がインストールおよび設定されていることを確認します。
- SCSI ディスク コントローラを使用して、VM-Series ファイアウォールのデータ格納先ディスクにアクセスする場合は、virsh を使用して virtio-scsi コントローラを VM-Series ファイアウォールに接続する必要があります。コントローラを接続したら、VM-Series ファイアウォールの XML テンプレートを編集して、virtio-scsi コントローラの使用を有効にします。詳細は、「SCSI コントローラの使用の有効化」を参照してください。

  Ubuntu 12.04 上で動作する *KVM* は、*virtio-scsi* コントローラをサポートしていません。

ネットワークインフラの確認

ゲストと VM-Series ファイアウォール間のトラフィック操作、およびインターネット上の外部サーバーと接続するためのネットワーク インフラストラクチャが存在していることを確認します。VM-Series ファイアウォールは、Linux ブリッジ、Open vSwitch、PCI パススルー、または SR-IOV 対応のネットワーク カードを使用して接続できます。

- 使用する各インターフェイスのリンク状態がUPになっていることを確認します。場合によっては、これらのインターフェイスを手動で UP状態にする必要があります。
- Linux ブリッジまたは OVS を使用している場合は、ファイアウォールとのトラフィックの送受信に必要なブリッジが設定済みであることを確認します。ブリッジが設定されていない場合は、ブリッジを作成して、UP 状態になっていることを確認してから、ファイアウォールのインストールを開始します。
- SR-IOVまたはPCIパススルーを使用している場合、すべてのインターフェイスのPCI IDを確認してください。リストを参照する場合は次のコマンドを使用します。

  `Virsh nodedev-list –tree`

  「VM-Series ファイアウォールでのネットワーク インターフェイスの順序を決定する PCI-ID の確認」を参照してください。
- SR-IOVまたはPCIパススルーを使用している場合は、BIOS の仮想化拡張機能（VT-d/IOMMU）が有効になっていることを確認します。たとえば、IOMMU を有効にするには、**`/etc/grub.conf`** に **`intel_iommu=on`** が定義されている必要があります。手順については、システム ベンダーが提供しているドキュメントを参照してください。

©2023 Palo Alto Networks, Inc.

- PCI パススルーを使用している場合は、VM-Series ファイアウォールが接続先のインターフェイスに対して排他的アクセス権を持つようにします。

  排他的アクセスを許可するには、Linuxサーバーから手動でインターフェイスをデタッチする必要があります。

  Virsh nodedev-detach *<pci id of interface>*

  以下に例を示します。

  Virsh nodedev-detach pci_0000_07_10_0

  場合によっては、`/etc/libvirt/qemu.conf`を編集して、`relaxed_acs_check = 1`のコメントを解除する必要があります。

- SR-IOV を使用している場合は、ネットワーク カードが使用する各ポートで仮想機能が有効になっていることを確認します。SR-IOV では、1 つの Ethernet ポート（物理機能）を複数の仮想機能に分割できます。また、1 つのゲストを 1 つ以上の仮想機能にマッピングできます。

  次のように仮想機能を有効にします。

  1. `/etc/modprobe.d/`に新規ファイルを作成します。
  2. viを使ってファイルを編集し、関数を永続的なものにします:

     vim /etc/modprobe.d/igb.conf
  3. 必要な仮想機能の数を有効にします:

     options igb max_vfs=4

     上記の例で、変更内容を保存して Linux サーバーを再起動すると、各インターフェイス（物理インターフェイス）ごとに 4 つの仮想機能が割り当てられます。

  実際にサポートされている仮想機能の数と仮想機能を有効にするための手順の詳細は、ネットワーク ベンダーが提供しているドキュメントを参照してください。

Mellanoxソフトウェアツールのインストール

Mellanox CX5カードを使用している場合、ホスト上にMellanoxソフトウェアツールをインストールしてください。インストールする前に、Linuxサポートとネットワークインフラを確認してください。

STEP 1 | ホストから、次のリンクを使ってご利用のOSのバージョンに適した、Mellanox OpenFabric Enterprise Distribution for Linux（MLNX_OFED）パッケージをダウンロードします:

https://www.mellanox.com/products/infiniband-drivers/linux/mlnx_ofed

STEP 2 | インストールコマンドを実行します。

mlnxofedinstall

前提条件となるすべてのパッケージをインストールしている場合、上記のコマンドですべてのMLNX_OFEDパッケージがインストールされます。ステップ3に進みます。

環境に必要なパッケージが存在していない場合、インストールする必要があるすべてのパッケージが表示されます。パッケージをインストールしたら、インストールコマンドに戻ってステップ3に進んでください。

©2023 Palo Alto Networks, Inc.

STEP 3 | ホストを再起動します。

STEP 4 | Mellanoxソフトウェアツールのステータスを確認します。

```
# mst status
MST modules:
------------------------------------------------------------------
  MST PCI module is not loaded
  MST PCI configuration module loaded

MST devices:
------------------------------------------------------------------
/dev/mst/mt4121_pciconf0     - PCI configuration cycles access.
        domain:bus:dev.fn=0000:3b:00.0 addr.reg=88 data.reg=92
        Chip revision is: 00
```

STEP 5 | PCIリストでMellanoxが更新されていることを確認します:

```
# lspci | grep Mellanox
3b:00.0 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex]
3b:00.1 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex]
```

KVM上のVM-Seriesファイアウォールの、Mellanox CX5 NIC仮想機能の有効化

Mellanox Cx5 NICで仮想機能を有効にする前に、Mellanoxソフトウェアツールをインストールします。

STEP 1 | Mellanoxソフトウェアツール（mst）が開始されていることを確認します。

STEP 2 | 必要な仮想機能の数を有効にします。以下に例を示します。

```
mlxconfig -d /dev/mst/mt4121_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=4
```

上記の例で、変更内容を保存して Linux サーバーを再起動すると、各インターフェイス（物理インターフェイス）ごとに 4 つの仮想機能が割り当てられます。実際にサポートされてい

©2023 Palo Alto Networks, Inc.

る仮想機能の数と仮想機能を有効にするための手順の詳細は、ネットワーク ベンダーが提供しているドキュメントを参照してください。

*Mellanox Cx5 NIC*で初めて仮想機能を有効にした場合、次のエラーメッセージが表示されることがあります:

```
[ 1429.841162] mlx5_core 0000:3b:00.1:
 mlx5_port_module_event:1025:(pid 0): Port module
 event[error]: module 1, Cable error, One or more network
 ports have been powered down due to insufficient/
unadvertised power on the PCIe slot. Please refer to the
 card's user manual for power specifications or contact
 Mellanox support
```

問題を解決するには、*Linux*サーバーで次のコマンドシーケンスを入力します:

```
# mlxconfig -d <dev> set ADVANCED_POWER_SETTINGS=1
# mlxconfig -d <dev> set DISABLE_SLOT_POWER_LIMITER=1
# reboot
```

STEP 3 | 仮想機能のステータスを確認します。

```
# cat  /sys/class/net/enp59s0f1/device/sriov_numvfs
```

（任意）仮想機能が正しく設定されていない場合は（ステータスが0または空）、次のコマンドを実行します:

```
# echo 4 > /sys/class/net/enp59s0f1/device/sriov_numvfs
```

STEP 4 | Mellanoxのそれぞれの物理機能にロードされる仮想機能数が正確に一致するように、PCIデバイスをリスト表示します:

```
# lspci | grep Mellanox
3b:00.0 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex]
3b:00.1 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex]
3b:00.2 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:00.3 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:00.4 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:00.5 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:00.6 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
```


©2023 Palo Alto Networks, Inc.

```
3b:00.7 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:01.0 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
3b:01.1 Ethernet controller: Mellanox Technologies MT28800 Family
 [ConnectX-5 Ex Virtual Function]
```

ホスト設定の確認

VM-Series のパフォーマンスが最大になるようにホストを設定してください。以下の各オプションの設定については、「VM-Series for KVM のパフォーマンス調整」を参照してください。

- **DPDK** を有効にします。DPDK を有効にすると、Linux カーネルがバイパスされるため、ホストのパケット処理速度が向上します。代わりに、NIC と対話するときは、ドライバと DPDK ライブラリが使用されます。DPDK と VM-Series ファイアウォールを一緒に使用するには、Open vSwitch が必要です。
- **SR-IOV** を有効にします。Single Root I/O Virtualization（SR-IOV）を使用すると、1 つのルート ポートの 1 つの PCIe 物理デバイスを、ハイパーバイザやゲストに対して複数の個別の物理デバイスのように見せかけることができます。
- **NIC** のマルチキュー サポートを有効にします。マルチキュー virtio-net を使用すると、vCPU の数に合わせてネットワークのパフォーマンスを高めることができ、複数の TX および RX キューを作成して並列パケット処理を実現できます。
- **NUMA**ノードの**CPU**リソースを分離します。ゲスト VM の CPU リソースを、単一の不均一メモリアクセス（NUMA）ノードに隔離することで、KVM 上の VM-Series のパフォーマンスを向上させることができます。

VM-Series ファイアウォールのデプロイ準備

- Palo Alto Networks カスタマー サポート Web サイトで VM-Series モデルを購入し、認証コードを登録します。「サポート アカウントの作成」および「VM-Series ファイアウォールの登録」を参照してください。
- qcow2 イメージを取得して、Linux サーバー上に保存します。このイメージをフォルダ/var/lib/libvirt/qemu/imagesにコピーすることをお勧めします。

  VM-Series ファイアウォールの複数のインスタンスをデプロイする場合は、qcow2 イメージを必要な数だけコピーします。VM-Series ファイアウォールの各インスタンスは、ファイアウォールのデプロイ時に使用した qcow2 イメージとのリンクを保持しています。データの破損を防ぐため、各イメージが独立しており、また、各イメージがファイアウォールの 1 つのインスタンスで使用されるようにする必要があります。

©2023 Palo Alto Networks, Inc.

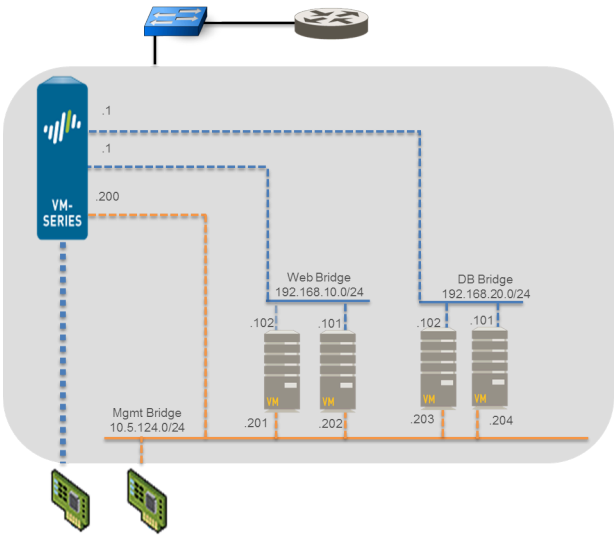
KVM でサポートされているデプロイ

Linux ホストごとに単一の VM-Series ファイアウォールをデプロイする方法と、1 つの Linux ホストに VM-Series ファイアウォールの複数のインスタンスをデプロイする方法があります。VM-Series ファイアウォールは、バーチャル ワイヤ、レイヤー 2、またはレイヤー 3 インターフェイスを使用してデプロイできます。VM-Series ファイアウォールで SR-IOV 対応のインターフェイスを使用する場合、そのインターフェイスは、レイヤー 3 インターフェイスとしてのみ設定可能です。

- 単一ホストでのトラフィックの保護
- 複数の Linux ホストでのトラフィックの保護

単一ホストでのトラフィックの保護

Linux サーバー上のゲスト間の水平トラフィックを保護する場合は、VM-Series ファイアウォールを、バーチャル ワイヤ、レイヤー 2、レイヤー 3 インターフェイスを使用してデプロイできます。下図に、レイヤー 3 インターフェイスを使用したファイアウォールを示します。この例では、ファイアウォールとサーバー上の他のゲストが Linux ブリッジで接続されています。このデプロイでは、Web サーバーとデータベース サーバー間のすべてのトラフィックがファイアウォール経由でルーティングされます。データベース サーバー同士、または Web サーバー同士のトラフィックはブリッジによって処理され、ファイアウォールにはルーティングされません。



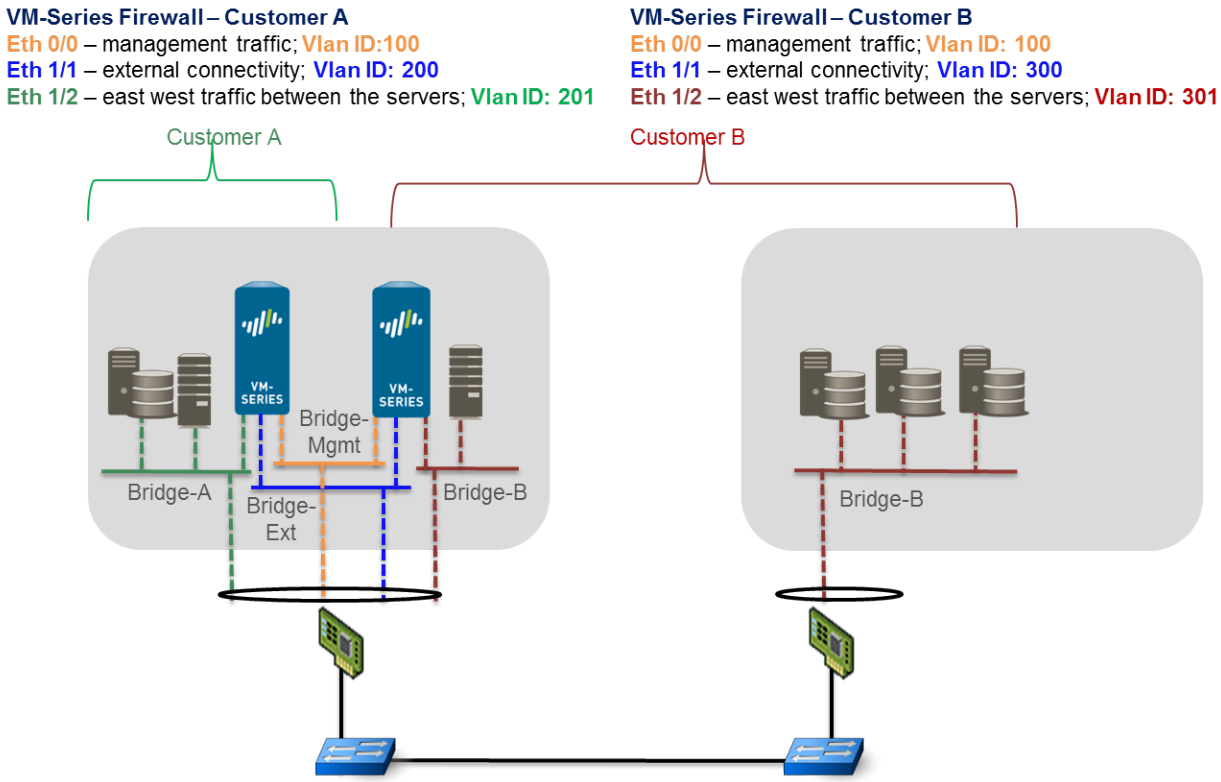
複数の Linux ホストでのトラフィックの保護

各種ワークロードを保護する場合は、1 台の Linux ホスト上に VM-Series ファイアウォールの複数のインスタンスをデプロイできます。たとえば、異なる部門や顧客のトラフィックを分離する必要がある場合は、VLAN タグを使用して

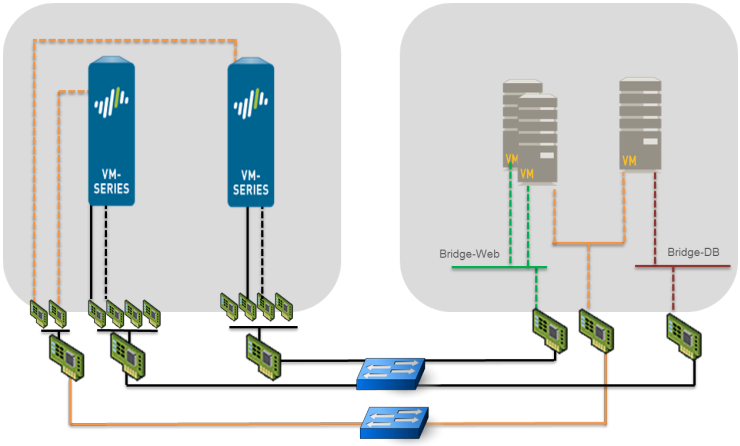
ネットワーク トラフィックを論理的に切り離し、それぞれ適切な VM-Series ファイアウォールにルーティングできます。次の例では、1 台の Linux ホストが、2 つの顧客（顧客 A と顧客 B）の VM-Series ファイアウォールをホストしており、顧客 B のワークロードは 2 台のサーバー

©2023 Palo Alto Networks, Inc.

間に分散しています。トラフィックを切り離して、各顧客用に設定された VM-Series ファイアウォールに向けるために、VLAN を使用しています。



このデプロイ環境の別のバリエーションとして、VM-Series ファイアウォールのペアを高可用性設定でデプロイする方法があります。次の例では、SR-IOV 対応のアダプタを搭載した Linux サーバーに VM-Series ファイアウォールをデプロイしています。SR-IOV では、1 つの Ethernet ポート（物理機能）を複数の仮想機能に分割できます。VM-Series ファイアウォールに接続された各仮想機能は、レイヤー 3 インターフェイスとして構成されます。HA ペアのアクティブなピアは、異なる Linux サーバー上にデプロイされているゲストから自分宛てにルーティングされたトラフィックを保護します。



©2023 Palo Alto Networks, Inc.

KVM への VM-Series ファイアウォールのインストール

KVM の管理に使用する libvirt API には、仮想マシンを作成および管理するためのさまざまなツールが用意されています。KVM 上に VM-Series ファイアウォールをインストールするには、以下のいずれかの方法を使用できます。

- virt-manager — virt-manager 仮想マシン マネージャーを使用して VM-Series をデプロイします。virt-manager には、インストール プロセスを支援する便利なウィザードがあります。
- virsh — KVM コマンドラインを使用して VM-Series をデプロイします。仮想マシン インスタンスを定義する XML ファイルと、ファイアウォールの初期設定を定義するブートストラップ XML ファイルを作成します。次に、ISO イメージを CD-ROM としてマウントし、ファイアウォールをインストールします。
- virt-install — KVM コマンドラインを使用して VM-Series ファイアウォールをデプロイするもう 1 つのオプションです。VM-Series ファイアウォールの定義を作成してインストールするには、このオプションを使用します。

このドキュメントでは、virt-manager と virsh を使用して KVM に VM-Series ファイアウォールをインストールする手順を説明します。

- Virt-Manager を使用した VM-Series ファイアウォールのインストール
- ISO を使用した VM-Series ファイアウォールのインストール
- KVM 上での VM-Series CLI を使用した管理インターフェースのスワップ
- SCSI コントローラの使用の有効化
- VM-Series ファイアウォールでのネットワーク インターフェイスの順序を決定する PCI-ID の確認

Virt-Manager を使用した VM-Series ファイアウォールのインストール

この手順では virt-manager を使用して、RHEL で KVM を実行するサーバーに VM-Series ファイアウォールをインストールします。

- KVM ホスト上の VM-Series ファイアウォールのプロビジョニング
- KVM 上での VM-Series ファイアウォールの初期設定

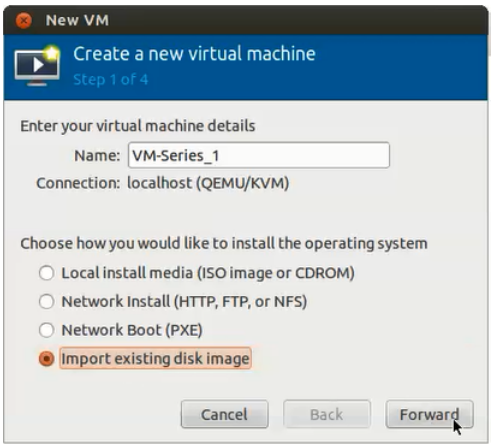
KVM ホスト上の VM-Series ファイアウォールのプロビジョニング

VM-Series ファイアウォールの KVM ホストをプロビジョニングするには、以下の手順を実行します。

©2023 Palo Alto Networks, Inc.

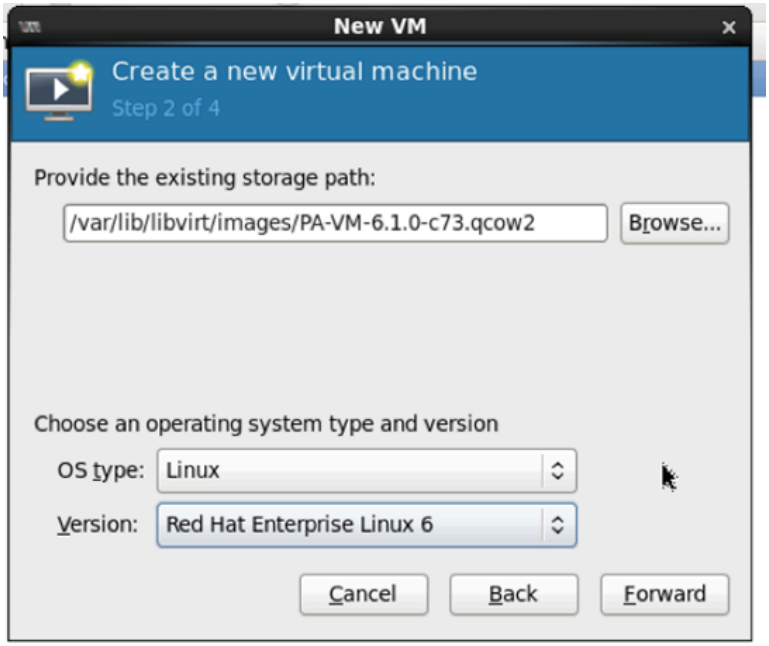
STEP 1 | 新しい仮想マシンを作成し、KVM イメージ用の VM-Series ファイアウォールを virt-mgr に追加します。

1. Virt-manager で、**Create a new virtual machine**（新規仮想マシンを作成）を選択します。
2. VM-Series ファイアウォールの分かりやすい名前を **Name**（名前）に入力します。



3. **Import existing disk image** [既存のディスクイメージをインポート] を選択し、該当のイメージを探し、**OS Type** [OSタイプ] を設定します:Linuxとその**Version** [バージョン] :Red Hat Enterprise Linux 6

   OS Type と *Version* は、*Generic* のままでもかまいません。

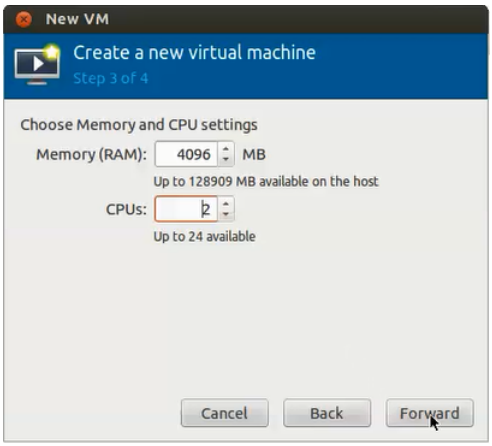


4. データ インターフェイス用のネットワーク アダプタを追加するには、以下の手順を実行します。

©2023 Palo Alto Networks, Inc.

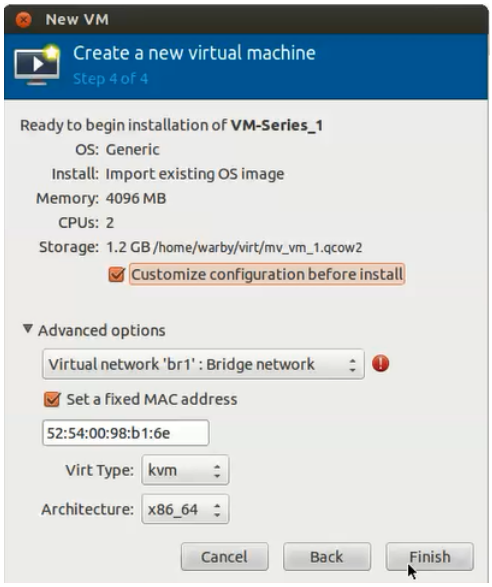
STEP 2 | メモリと CPU の設定を構成します。

1. VM-Series モデルの VM-Series システム要件に基づいて、**Memory**（メモリ）を最小メモリに設定します。
2. VM-Series モデルの VM-Series システム要件に基づいて、**CPU** を最小 CPU 数に設定します。



STEP 3 | 設定のカスタマイズを有効にし、管理インターフェイス ブリッジを選択します。

1. **Customize configuration before install**（インストール前に構成をカスタマイズ）を選択します。
2. Advanced options（詳細オプション）セクションで、管理インターフェイス用のブリッジを選択し、デフォルトの設定をそのまま受け入れます。



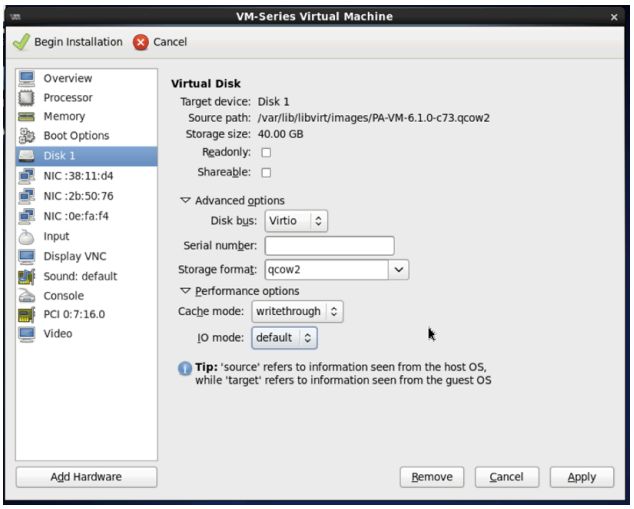
©2023 Palo Alto Networks, Inc.

STEP 4 | 仮想ディスク設定を構成します。

1. **Disk**（ディスク）を選択し、Advanced options（詳細オプション）を展開して、**Storage format**（ストレージ形式）として qcow2、**Disk Bus**（ディスク バス）として Virtio または IDE を選択します（この選択内容はお使いの設定によって異なります）。

   SCSI ディスク バスを使用する場合は、「SCSI コントローラの使用の有効化」を参照してください。

2. Performance options（パフォーマンス オプション）を展開して、**Cache mode**（キャッシュ モード）を **writethrough** に設定します。この設定により、インストール所要時間が短縮され、VM-Series ファイアウォールの実行速度が向上します。



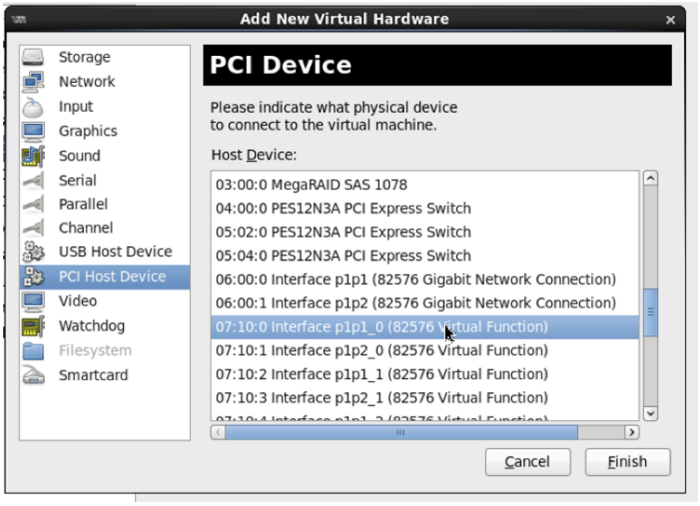
 ©2023 Palo Alto Networks, Inc.

STEP 5 | ネットワーク アダプタを設定します。

1. Linux ブリッジや Open vSwitch などのソフトウェア ブリッジを使用している場合は、**Add Hardware**（ハードウェア追加） > **Network**（ネットワーク）を選択します。
2. **Host Device**（ホスト デバイス）で、ブリッジの名前を入力するか、ドロップダウン リストから選択します。
3. ドライバを指定する場合は、**Device Model**（デバイス モデル）を e-1000 または virtio に設定します。サポートされている仮想マシン タイプはこの 2 つだけです。



4. PCI パススルーまたは SR-IOV 対応デバイスの場合は、**Add Hardware**（ハードウェア追加） > **PCI Host Device**（**PCI** ホスト デバイス）を選択します。

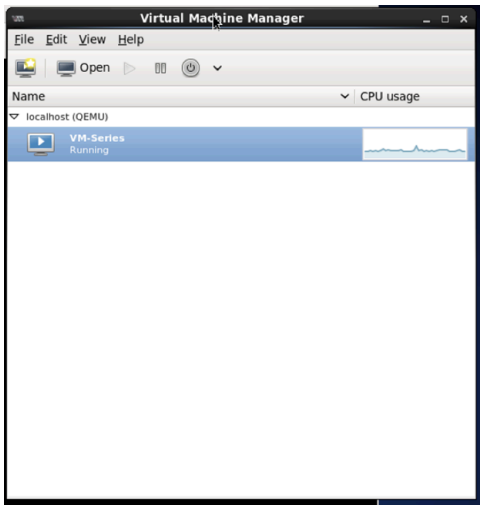


5. **Host Device**（ホスト デバイス）リストで、カードまたは仮想機能のインターフェイスを選択します。
6. **Apply**（適用）または **Finish**（完了）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 6 | **Begin Installation**（インストール開始）  をクリックします。インストールが完了するまで、5 ～ 7 分待ちます。

デフォルトでは、*VM-Series* ファイアウォールの *XML* テンプレートは、*etc/libvirt/qemu* に作成および保存されます。



STEP 7 | （任意）VM-Series ファイアウォールをブートストラップします。

ブートストラップを使用して KVM 上の VM-Series ファイアウォールを設定する場合は、「KVM における VM-Series ファイアウォールのブートストラップ」を参照してください。ブートストラップの詳細は、「VM-Series ファイアウォールのブートストラップ」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 8 | 管理インターフェイスへのネットワーク アクセス設定を行います。

1. コンソールとの接続を開きます。
2. ユーザー名とパスワード（admin/admin）を使用してファイアウォールにログインします。
3. 以下のコマンドを入力して設定モードに切り替えます。

```
configure
```

4. 以下のコマンドを使用して、管理インターフェイスを設定します。

1.
```
set deviceconfig system type static
```

2.
```
set deviceconfig system ip-address <Firewall-IP> netmask
 <netmask> default-gateway <gateway-IP> dns-setting servers
 primary <DNS-IP>
```

<Firewall-IP> は管理インターフェイスに割り当てる IP アドレス、 *<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレスです。

3.
```
commit
```

STEP 9 | ホスト上の各ポートが VM-Series ファイアウォールのどのインターフェイスにマッピングされているのかを確認します。Linux ホスト上のインターフェイスの順序を検証するには、「VM-Series ファイアウォールでのネットワーク インターフェイスの順序を決定する PCI-ID の確認」を参照してください。

トラフィックが正しいインターフェイスによって処理されていることを確認するには、次のコマンドを使用してホスト上のポートと VM-Series ファイアウォール上のポートのマッピングを確認します。

```
admin@PAN-VM> debug show vm-series interfaces all
Phoenix_interface    Base-OS_port       Base-OS_MAC PCI-ID
 mgt                          eth0          52:54:00:d7:91:52
 0000:00:03.0
 Ethernet1/1             eth1          52:54:00:fe:8c:80
 0000:00:06.0
 Ethernet1/2             eth2          0e:c6:6b:b4:72:06
 0000:00:07.0
 Ethernet1/3             eth3          06:1b:a5:7e:a5:78
 0000:00:08.0
 Ethernet1/4             eth4          26:a9:26:54:27:a1
 0000:00:09.0
 Ethernet1/5             eth5          52:54:00:f4:62:13
 0000:00:10.1
```


©2023 Palo Alto Networks, Inc.

STEP 10 | VM-Series ファイアウォールの Web インターフェイスにアクセスして、インターフェイスを設定し、セキュリティ ルールと NAT ルールを定義して、保護する必要のあるアプリケーションを安全に有効化します。

『PAN-OS 管理者ガイド』を参照してください。

KVM 上での VM-Series ファイアウォールの初期設定

VM-Series ファイアウォールへのネットワーク アクセスをセットアップするには、KVM サーバーでバーチャル アプライアンス コンソールを使用します。デフォルトでは、VM-Series ファイアウォールは、DHCP を使用して、管理インターフェイスの IP アドレスを取得します。ただし、スタティック IP アドレスを割り当てることも可能です。初期設定が完了したら、Web インターフェイスにアクセスし、詳細な設定タスクを実行します。中央管理のために Panorama を使用している場合、Panorama を使用したデバイス管理の詳細は、『Panorama 管理者ガイド』を参照してください。

ブートストラップを使用して KVM 上の VM-Series ファイアウォールを設定する場合は、「KVM における VM-Series ファイアウォールのブートストラップ」を参照してください。

ブートストラップの一般的な情報については、「VM-Series ファイアウォールのブートストラップ」を参照してください。

STEP 1 | ネットワーク管理者から必要な情報を入手します。

- MGT ポートの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS サーバーの IP アドレス

STEP 2 | VM-Series ファイアウォールのコンソールにアクセスします。

1. VM-Series ファイアウォール用の KVM サーバーで **Console**（コンソール）タブを選択するか、VM-Series ファイアウォールを右クリックして**Open Console**（コンソールを開く）を選択します。
2. Enter キーを押して、ログイン画面にアクセスします。
3. デフォルトのユーザー名/パスワード（admin/admin）を入力して、ログインします。
4. 設定モードに切り替えるには、「**configure**」と入力します。

STEP 3 | 管理インターフェイスへのネットワーク アクセス設定を行います。

以下のコマンドを入力します。

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```


©2023 Palo Alto Networks, Inc.

STEP 4 | 変更をコミットし、設定モードを終了します。

「**commit**」と入力します。

「**exit**」と入力します。

ISO を使用した VM-Series ファイアウォールのインストール

VM-Series ファイアウォールの XML 定義を手動で作成し、virsh を使用してその定義を ISO としてインポートします。virsh は、仮想マシンのあらゆる側面の管理が可能な極めて強力なツールです。

- ISO ファイルを使用した VM-Series ファイアウォールのデプロイ
- VM-Series ファイアウォールのサンプル XML ファイル

ISO ファイルを使用した VM-Series ファイアウォールのデプロイ

起動時に VM-Series ファイアウォールにスクリプトを渡す必要がある場合は、ISO ファイルを使用して CD-ROM をマウントします。ISO ファイルを使用すると、ファイアウォールの管理ポートの初期設定パラメータが記述されたブートストラップ用 XML ファイルを定義できます。VM-Series ファイアウォールは最初の起動時に、**bootstrap-networkconfig.xml** ファイルをチェックし、そこに定義されている値を使用します。

ブートストラップ ファイルの解析時に *1* つでもエラーが見つかると、*VM-Series* ファイアウォールはそのファイルのすべての設定を拒否し、デフォルト値で起動します。

STEP 1 | XML ファイルを作成し、仮想マシン インスタンスとして定義します。

サンプル ファイルについては、「VM-Series ファイアウォールのサンプル XML ファイル」を参照してください。

以下に、PAN_Firewall_DC1 という名前の VM-Series ファイアウォールの例を示します。

例:

```
user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/
PAN_Firewall_DC1.xml
user-PowerEdge-R510:~/kvm_script$ sudo virsh define/etc/libvirt/
qemu/PAN_Firewall_DC1.xml
Domain PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/
PAN_Firewall_DC1.xml
user-PowerEdge-R510:~/kvm_script$ sudo virsh -q attach-interface
 PAN_Firewall_DC1_bootstp bridge br1 --model=virtio --persistent
user-PowerEdge-R510:~/kvm_script$ virsh list --all
 Id    Name                           State
----------------------------------------------------
 -    PAN_Firewall_DC1_bootstp     shut off
```


©2023 Palo Alto Networks, Inc.

STEP 2 | ブートストラップ用 XML ファイルを作成します。

このファイルに初期設定パラメータを定義して、bootstrap-networkconfig という名前を付けることもできます。

特定のパラメータ、たとえば、*panorama-server-secondary* を除外する必要があるとします。その場合は、その行全体を削除します。*IP* アドレス フィールドを空のままにすると、ファイルの解析に失敗します。

次の例を bootstrap-networkconfig ファイルのテンプレートとして使用してください。bootstrap-networkconfig ファイルには、以下のパラメータのみ含めることができます。

```
<vm-initcfg>
<hostname>VM_ABC_Company</hostname>
<ip-address>10.5.132.162</ip-address>
<netmask>255.255.254.0</netmask>
<default-gateway>10.5.132.1</default-gateway>
<dns-primary>10.44.2.10</dns-primary>
<dns-secondary>8.8.8.8</dns-secondary>
<panorama-server-primary>10.5.133.4</panorama-server-primary>
<panorama-server-secondary>10.5.133.5</panorama-server-secondary>
</vm-initcfg>
```

STEP 3 | ISO ファイルを作成します。この例では、mkisofs を使用します。

ISO ファイルをイメージ ディレクトリ（*/var/lib/libvirt/image*）または *qemu* ディレクトリ（*/etc/libvirt/qemu*）に保存して、ファイアウォールにその *ISO* ファイルに対する読み取りアクセス権があることを確認します。

例:

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -
allow-lowercase -allow-multidot -o <iso-filename> bootstrap-
networkconfig.xml
```

STEP 4 | ISO ファイルを CD-ROM にアタッチします。

例:

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --
mode readonly –persistent\
```

VM-Series ファイアウォールのサンプル XML ファイル

```
<?xml version="1.0"?>
<domain type="kvm">
<name>PAN_Firewall_DC1</name>
<memory>4194304</memory>
<currentMemory>4194304</currentMemory>
<vcpu placement="static">2</vcpu>
```


©2023 Palo Alto Networks, Inc.

```
<os>
<type arch="x86_64">hvm</type>
<boot dev="hd"/>
</os>
<features>
<acpi/>
<apic/>
<pae/>
</features>
<clock offset="utc"/>
<on_poweroff>destroy</on_poweroff>
<on_reboot>restart</on_reboot>
<on_crash>restart</on_crash>
<devices>
<emulator>/usr/libexec/qemu-kvm</emulator>
<disk type="file" device="disk">
<driver type="qcow2" name="qemu"/>
<source file="/var/lib/libvirt/images/panos-kvm.qcow2"/>
<target dev="vda" bus="virtio"/>
</disk>
<controller type="usb" index="0"/>
<controller type="ide" index="0"/>
<controller type="scsi" index="0"/>
<serial type="pty">
<source path="/dev/pts/1"/>
<target port="0"/>
<alias name="serial0"/>
</serial>
<console type="pty" tty="/dev/pts/1">
<source path="/dev/pts/1"/>
<target type="serial" port="0"/>
<alias name="serial0"/>
</console>
<input type="mouse" bus="ps2"/>
<graphics type="vnc" port="5900" autoport="yes"/>
</devices>
</domain>
```

VM-Series ファイアウォールに割り当てられた *vCPU* の数を変更する場合、サンプル *XML* ファイルの以下の行にある *vCPU* の値を ***2*** から ***4*** または ***8*** に変更します。

```
<vcpu placement="static">2</vcpu>
```

KVM 上での VM-Series CLI を使用した管理インターフェースのスワップ

デフォルトでは、VM-Series ファイアウォールは最初のインターフェース（eth0）を管理インターフェースとして割り当てます。ただし、デプロイメントによっては、最初のインターフェースをパブリック IP アドレスに事前にマッピングする必要があります。したがって、管理インターフェースを別のインターフェースに割り当てる必要があります。管理インターフェースにパブリック IP アドレスを割り当てることには、セキュリティ上のリスクがあります。

©2023 Palo Alto Networks, Inc.

または、ブートストラップ時にInit-cfg.txt ファイルのコンポーネントの一部として管理インターフェースのスワップを有効にすることもできます。

STEP 1 | VM-Series ファイアウォールの CLI にログインし、次のコマンドを入力します。

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 確定してインターフェイスをスワップし、eth1 データプレーン インターフェイスを管理インターフェイスとして使用します。

STEP 3 | ファイアウォールを再起動してスワップを反映させます。以下のコマンドを使用します。

```
request restart system
```

STEP 4 | インターフェイスがスワップされたことを確認します。以下のコマンドを使用します。

```
debug show vm-series interfaces all
Phoenix_interface   Base-OS_port   Base-OS_MAC        PCI-ID
       Driver
mgt(interface-swap) eth0   0e:53:96:91:ef:29   0000:00:04.0
  ixgbevf
Ethernet1/1           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0
  ixgbevf
```

SCSI コントローラの使用の有効化

VM-Series ファイアウォールで仮想ディスクへのアクセスにディスク バス タイプとして SCSI を使用する場合は、以下の手順を実行して virtio-scsi コントローラをファイアウォールに接続し、virtio-scsi コントローラの使用を有効にします。

Ubuntu 12.04 上で動作する *KVM* では、*virtio-scsi* コントローラをサポートしていません。*virtio-scsi* コントローラは、*RHEL* または *CentOS* 上で稼働している *VM-Series* ファイアウォール上でのみ有効化できます。

Virt マネージャーは *virtio-scsi* コントローラをサポートしていないため、以下の手順では *virsh* が必要です。

STEP 1 | SCSI コントローラ用の XML ファイルを作成します。以下の例では、virt-scsi.xml という名前の XML ファイルを作成しています。

```
[root@localhost~]# cat /root/virt-scsi.xml
<controller type='scsi' index='0' model='virtio-scsi'>
<address type='pci' domain='0x0000' bus='0x00'
 slot='0x0b'function='0x0'/>
</controller>
```

virtio-scsi コントローラ用のスロットが、他のデバイスと競合していないことを確認します。

STEP 2 | このコントローラを、VM-Series ファイアウォールの XML テンプレートに関連付けます。

©2023 Palo Alto Networks, Inc.

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /
root/virt-scsi.xml
Device attached successfully
```

STEP 3 | ファイアウォールが SCSI コントローラを使用できるようにします。

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/lib/
libvirt/images/PA-VM-6.1.0-c73.qcow2
sda --cache none --persistent
Disk attached successfully
```

STEP 4 | VM-Series ファイアウォールの XML テンプレートを編集します。XML テンプレートでは、ファイアウォールによって使用されるターゲット ディスクとディスク バスを変更する必要があります。

デフォルトでは、*XML* テンプレートは、*etc/libvirt/qemu* に保存されます。

```
<disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='writeback'/>
      <source file='/var/lib/libvirt/images/PA-VM-7.0.0-c73.qcow2'/
>
      <target dev='sda' bus='scsi'/>
      <address type='drive' controller='0' bus='0' target='0'
 unit='0'/>
</disk>
```

VM-Series ファイアウォールでのネットワーク インターフェイスの順序を決定する PCI-ID の確認

VM-Series ファイアウォールとの接続に仮想インターフェイス（Linux/OVS ブリッジ）または PCI デバイス（PCI パススルーまたは SR-IOV 対応アダプタ）のどちらを使用するかに関係なく、VM-Series ファイアウォールはインターフェイスを PCI デバイスとみなします。VM-Series ファイアウォール上でのインターフェイスの割り当ては、PCI-ID に基づいて行われます。PCI-ID とは、バス、デバイスまたはスロット、およびインターフェイスの機能を組み合わせた値です。インターフェイスは、PCI-ID の小さい順に並べられます。つまり、ファイアウォールの管理インターフェイス（eth0）は PCI-ID の最も小さいインターフェイスに割り当てられます。

たとえば、VM-Series ファイアウォールに 4 つのインターフェイス（最初の 3 つは、タイプが virtio または e1000 の仮想インターフェイス、4 つ目は PCI デバイス）を割り当てるとします。各インターフェイスの PCI-ID を確認するには、Linux ホスト上でコマンド **virsh dumpxml $ domain *<name of the VM-Series firewall>*** を入力します。このコマンドにより、VM-Series ファイアウォールに接続されているインターフェイスのリストが表示されます。コマンドの出力で、以下のネットワーク設定を確認します。

```
<interface type='bridge'>
      <mac address='52:54:00:d7:91:52'/>
```


©2023 Palo Alto Networks, Inc.

```
      <source bridge='mgmt-br'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
function='0x0'/>
   </interface>

  <interface type='bridge'>
      <mac address='52:54:00:f4:62:13'/>
      <source bridge='br8'/>
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x10'
function='0x0'/>
   </interface>

  <interface type='bridge'>
      <mac address='52:54:00:fe:8c:80'/>
      <source bridge='br8'/>
      <model type='e1000'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
function='0x0'/>
   </interface>

  <hostdev mode='subsystem' type='pci' managed='yes'>
      <source>
        <address domain='0x0000' bus='0x08' slot='0x10'
function='0x1'/>
      </source>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
function='0x0'/>
   </hostdev>
```

この例では、各インターフェイスの PCI-ID は次のようになっています。

- 最初の仮想インターフェイスの PCI-ID は 00:03:00
- 2 番目の仮想インターフェイスの PCI-ID は 00:10:00
- 3 番目の仮想インターフェイスの PCI-ID は 00:06:00
- 4 番目の仮想インターフェイスの PCI-ID は 00:07:00

したがって、この VM-Series ファイアウォールでは、PCI-ID 00:03:00 を持つインターフェイスが eth0（管理インターフェイス）に、PCI-ID 00:06:00 を持つインターフェイスが eth1（ethernet1/1）に、PCI-ID 00:07:00 を持つインターフェイスが eth2（ethernet1/2）に、PCI-ID 00:10:00 を持つインターフェイスが eth3（ethernet1/3）に、それぞれ割り当てられます。

©2023 Palo Alto Networks, Inc.

VM-Series for KVM のパフォーマンス調整

KVM 用の VM-Series ファイアウォールは、高パフォーマンスのアプライアンスですが、最良の結果を得るには、ハイパーバイザの調整が必要な場合があります。このセクションでは、VM-Series ファイアウォールが最高のパフォーマンスを発揮するためのベスト プラクティスと推奨事項について説明します。

デフォルトでは、KVM は VM ネットワーキング用に Linux ブリッジを使用します。ただし、仮想環境で最高のパフォーマンスを実現するには、専用の I/O インターフェイス（PCI パススルーまたは SR-IOV）が必要です。仮想スイッチが必要な場合は、パフォーマンスが最適化された仮想スイッチ（DPDK を利用する Open vSwitch など）を使用してください。

- Ubuntu 16.04.1 LTS への KVM および Open vSwitch のインストール
- KVM での Open vSwitch の有効化
- Open vSwitch と DPDK の統合
- KVM 上の SR-IOV の有効化
- SR-IOV による VLAN アクセスモードの有効化
- KVM 上の NIC のマルチキュー サポートの有効化
- KVM 上の NUMA ノードへの CPU リソースの分離

Ubuntu 16.04.1 LTS への KVM および Open vSwitch のインストール

インストールを容易にするため、Ubuntu 16.04.1 LTS を KVM ハイパーバイザープラットフォームとして使用することをお勧めします。

STEP 1 | KVM と OVS をインストールします。

1. Ubuntu CLI にログインします。
2. 以下のコマンドを実行します。

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder
 bridge-utils
$ sudo apt-get install openvswitch-switch
```

STEP 2 | 関連パッケージのバージョンを確認して比較します。

以下のコマンドを実行します。

```
$ virsh --version 1.3.1
$ libvirtd --version
libvirtd (libvirt) 1.3.1
$ /usr/bin/qemu-system-x86_64 --version
QEMU emulator version 2.5.0 (Debian
1:2.5+dfsg-5ubuntu10.6), Copyright (c) 2003-2008
Fabrice Bellard
$ ovs-vsctl --version
```


©2023 Palo Alto Networks, Inc.

```
ovs-vsctl (Open vSwitch) 2.5.0
Compiled Mar 10 2016 14:16:49
DB Schema 7.12.1
```

KVM での Open vSwitch の有効化

ゲスト XML 定義のネットワーク設定を変更して OVS を有効にします。

ゲスト XML 定義を以下のように変更します。

```
[...]
    <interface type='bridge'>
       <mac address='52:54:00:fb:00:01'/>
       <source bridge='ovsbr0'/>
       <virtualport type='openvswitch'/>
       <model type='virtio'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
   </interface>
[...]
```

Open vSwitch と DPDK の統合

Open vSwitch（OVS）を DPDK に統合するには、必要なコンポーネントをインストールしてから OVS を設定する必要があります。DPDK は、KVM 用 VM-Series ファイアウォールではデフォルトで有効化されています。

- Ubuntu への QEMU、DPDK、OVS のインストール
- ホストでの OVS および DPDK の設定
- VM-Series ファイアウォール設定ファイルの編集

Ubuntu への QEMU、DPDK、OVS のインストール

OVS で DPDK を有効化する前に、QEMU 2.5.0、DPDK 2.2.0、および OVS 2.5.1 をインストールしなければなりません。以下の手順でコンポーネントをインストールしてください。

STEP 1 | KVM ホスト CLI にログインします。

STEP 2 | 以下のコマンドを実行して QEMU 2.5.0 をインストールします。

```
apt-get install build-essential gcc pkg-config glib-2.0 libglib2.0-
dev libsdl1.2-dev
libaio-dev libcap-dev libattr1-dev libpixman-1-dev
apt-get build-dep qemu
apt-get install qemu-kvm libvirt-bin
wget http://wiki.qemu.org/download/qemu-2.5.0.tar.bz2
tar xjvf qemu-2.5.0.tar.bz2
cd qemu-2.5.0
./configure
make
make install
```


©2023 Palo Alto Networks, Inc.

STEP 3 | dpdk-2.2.0 をインストールします。

1. 以下のコマンドを実行します。

```
wget http://dpdk.org/browse/dpdk/snapshot/dpdk-2.2.0.tar.gz
tar xzvf dpdk-2.2.0.tar.gz
cd dpdk-2.2.0
vi config/common_linuxapp
```

2. CONFIG_RTE_APP_TEST=y は **CONFIG_RTE_APP_TEST=n** に変更してください
3. CONFIG_RTE_BUILD_COMBINE_LIBS=n は **CONFIG_RTE_BUILD_COMBINE_LIBS=y** に変更してください。
4. 以下のコマンドを実行します。

```
vi GNUmakefile
```

5. ROOTDIRS-y := lib drivers app は **ROOTDIRS-y := lib drivers** に変更してください
6. 以下のコマンドを実行します。

```
make install T=x86_64-native-linuxapp-gcc
```

STEP 4 | 以下のコマンドを実行して OVS 2.5.1 をインストールします。

```
wget http://openvswitch.org/releases/openvswitch-2.5.1.tar.gz
tar xzvf openvswitch-2.5.1.tar.gz
cd openvswitch-2.5.1
./configure –with-dpdk=”/root/dpdk-2.2.0/x86_64-native-linuxapp-
gcc/”
make
make install
```

ホストでの OVS および DPDK の設定

OVS と DPDK のサポートに必要なコンポーネントをインストールしたら、OVS と DPDK を使用するようにホストを設定する必要があります。

STEP 1 | KVM ホスト CLI にログインします。

STEP 2 | 既存の OVS-DPDK セットアップを置換または再設定する場合は、以下のコマンドを実行して、以前の設定をリセットします。インターフェイスごとにコマンドを繰り返します。

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | OVS 用の初期 hugepages を設定します。

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```


©2023 Palo Alto Networks, Inc.

STEP 4 | QEMU 用の hugepages をマウントします。

```
mkdir /dev/hugepages
mkdir /dev/hugepages/libvirt
mkdir /dev/hugepages/libvirt/qemu
mount -t hugetlbfs hugetlbfs /dev/hugepages/libvirt/qemu
```

STEP 5 | 現在存在している OVS デーモンがある場合は、以下のコマンドを使用して強制終了します。

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | OVS デーモン用のディレクトリを作成します。

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | 古いディレクトリを消去します。

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | 設定データベースを初期化します。

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
/usr/local/share/openvswitch/vswitch.ovsschema
```

STEP 9 | OVS DB サーバーを作成します。

```
ovsdb-server --remote=punix:/usr/local/var/run/openvswitch/db.sock
 \
--remote=db:Open_vSwitch,Open_vSwitch,manager_options \
--private-key=db:Open_vSwitch,SSL,private_key \
--certificate=db:Open_vSwitch,SSL,certificate \
--bootstrap-ca-cert=db:Open_vSwitch,SSL,ca_cert \
--pidfile --detach
```

STEP 10 | OVS を初期化します。

```
ovs-vsctl --no-wait init
```

STEP 11 | データベース サーバーを起動します。

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```


©2023 Palo Alto Networks, Inc.

STEP 12 | DPDK 用の igb_uio モジュール（ネットワーク デバイス ドライバ）をインストールします。

```
cd ~/dpdk-2.2.0/x86_64-native-linuxapp-gcc/kmod
modprobe uio
insmod igb_uio.ko
cd ~/dpdk-2.2.0/tools/
```

STEP 13 | PCI-ID またはインターフェイス名を使用して、インターフェイスの DPDK を有効にします。

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | OVS デーモンを DPDK モードで起動します。ovs-vswitchd のコア数は変更できます。-c 0x1 を -c 0x3 に変更すると、2 つのコアでこのデーモンを実行できます。

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --
detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/
nr_hugepages
```

STEP 15 | OVS ブリッジを作成して、ポートを接続します。

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
 datapath_type=netdev
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
ovs-vsctl add-br ovs-br1 -- set bridge ovs-br1
 datapath_type=netdev
ovs-vsctl add-port ovs-br1 dpdk1 -- set Interface dpdk1 type=dpdk
```

STEP 16 | OVS 用の DPDK vhost ユーザー ポートを作成します。

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
 type=dpdkvhostuser
ovs-vsctl add-port ovs-br1 vhost-user2 -- set Interface vhost-user2
 type=dpdkvhostuser
```

STEP 17 | ホストが使用する NIC のハードウェア キューの数を設定します。

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | OVS に使用する CPU マスクを設定します。

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```


©2023 Palo Alto Networks, Inc.

STEP 19 | DPDK vhost ユーザー ポートに必要な許可を設定します。以下の例では、読み取り、書き込み、および実行の許可を付与するために 777 が使用されています。

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

VM-Series ファイアウォール設定ファイルの編集

OVS および DPDK をサポートするために、VM-Series ファイアウォールの XML 設定ファイルを編集します。今すぐ XML 設定ファイルにアクセスすることも、VM-Series ファイアウォールをデプロイした後にアクセスすることもできます。ファイアウォールをデプロイした後に実行する場合は、変更を行う前に必ずファイアウォールをシャットダウンしてください。下の値は一例であり、各パラメータの値はお使いの VM-Series モデルによって異なります。

STEP 1 | KVM ホスト CLI にログインします。

STEP 2 | VM-Series ファイアウォールで XML 設定ファイルを編集します。

1. **virsh edit $<*your-vm-series-name*>** を使用して XML 設定ファイルを開きます。
2. HugePage に対応するためのメモリを設定します。ホストにデプロイする VM-Series ファイアウォールのモデルをサポートするために、十分なメモリを指定してください。詳細は、「VM-Series システム要件」を参照してください。

   ```
   <memory unit='KiB'>12582912</memory>
     <currentMemory unit='KiB'>6291456</currentMemory>
     <memoryBacking>
       <hugepages/>
   ```

3. 仮想マシンの必須 CPU フラグを設定します。

   ```
   <cpu mode='host-model'>
   ```

4. 仮想マシンとホスト間でのメモリ共有を有効にします。

   ```
   <numa>
         <cell id='0' cpus='0,2,4,6' memory='6291456' unit='KiB'
    memAccess='shared'/>
         <cell id='1' cpus='1,3,5,7' memory='6291456' unit='KiB'
    memAccess='shared'/>
      </numa>
   ```

5. DPDK vhost ユーザー ポートに VM-Series ファイアウォールのネットワーク インターフェイスを設定します。さらに、ホストによって VM-Series ファイアウォールに指定された virtio 仮想キューの数を設定します。

   ```
   <interface type='vhostuser'>
         <mac address='52:54:00:36:83:70'/>
   ```


©2023 Palo Alto Networks, Inc.

```
      <source type='unix' path='/usr/local/var/run/
openvswitch/vhost-user1' mode='client'/>
<model type='virtio'/>
<driver name='vhost' queues='8'/>
      <address type='pci' domain='0x0000' bus='0x00'
 slot='0x04' function='0x0'/>
    </interface>
    <interface type='vhostuser'>
      <mac address='52:54:00:30:d7:94'/>
      <source type='unix' path='/usr/local/var/run/
openvswitch/vhost-user2' mode='client'/>
<model type='virtio'/>
<driver name='vhost' qeueus='8'>
      <address type='pci' domain='0x0000' bus='0x00'
 slot='0x05' function='0x0'/>
    </interface>
```

KVM 上の SR-IOV の有効化

Single Root I/O Virtualization（SR-IOV）を使用すると、1 つのルート ポートの 1 つの PCIe 物理デバイスを、ハイパーバイザーやゲストに対して複数の個別の物理デバイスのように見せかけることができます。KVM ゲストで SR-IOV を有効にするには、物理 NIC に関連付けられた仮想機能（VF）デバイスのプールを定義して、VF デバイスをプールから PCI ID に自動的に割り当てます。

Intel 10GB ネットワーク インターフェイス（ixgbe ドライバ）を備えた SR-IOV の場合、各 NIC インターフェイスの複数のキューをサポートするために、ドライバ バージョンは 4.2.5 以降である必要があります。PAN-OSバージョンごとのPacketMMAPとDPDKドライバーのサポートについては、互換性マトリックスを参照してください。

STEP 1 | VF のプールのネットワークを定義します。

1. 以下の例のようなテキストを使用して XML ファイルを生成します。お使いのSR-IOVデバイスの物理機能に合わせて、`pf dev`の値を`ethdev`に変更します。

```
<network>
   <name>passthrough</name>
   <forward mode='hostdev' managed='yes'>
     <pf dev='eth3'/>
   </forward>
</network>
```

2. XML ファイルを保存します。
3. 以下のコマンドを実行します。

```
$ virsh net-define <path to network XML file>
$ virsh net-autostart passthrough
$ virsh net-start passthrough
```


©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series のファイアウォールが DPDK モードで確実に起動するようにするには、 KVM ハイパーバイザーのゲスト VM XML 構成を編集して、以下を追加します。

```
<cpu mode='host-passthrough' check='none'/>
```

これにより、CPUフラグが確実に公開されます。

VM で CPU フラグが公開されていることを確認するには：

```
cat /proc/cpuinfo
```

DPDK 18.11 を備えた PAN-OS 10.0 以降の`flags`出力には、`AVX`、または`AES`と`SSE`フラグが必要になります。

STEP 3 | ネットワークを定義して開始してから、ゲスト XML 定義を変更してネットワークを指定します。

```
<interface type='network'>
    <source network='passthrough'>
</interface>
```

ゲストが起動すると、VF は自動的にゲストに割り当てられます。

STEP 4 | ホストにマルチキャスト MAC アドレスを追加します。

SR-IOV が有効であれば、マルチキャスト トラフィックが PF でフィルタリングされます。このフィルタリングにより、OSPF のようなマルチキャストに頼るアプリケーションが失敗するおそれがあります。このフィルタリングを回避するために、マルチキャスト MAC アドレスを次のコマンドを使ってホストに手作業で追加する必要があります。

```
#ip maddress add <multicast-mac> dev <interface-name>
```

SR-IOV による VLAN アクセスモードの有効化

KVM 上の VM-Series ファイアウォールは、VLAN アクセスモードで動作して、マルチテナント クラウド/データセンター環境でサービスとしてのセキュリティを提供する仮想ネットワーク機能（VNF）として展開されるユースケースをサポートできます。VLAN アクセスモードでは、各 VNF に各ネットワーク専用の仮想ネットワークインターフェイス（VNI）があり、VLAN タグなしで SR-IOV 仮想機能（VF）との間でパケットを送受信します。 ホストハイパーバイザーの物理機能と仮想機能でこの機能を有効にする必要があります。次に、VM-Series ファイアウォールで VLAN アクセスモードを有効にすると、ファイアウォールは、すべてのデータプレーンインターフェイスで VLAN タグなしでトラフィックを送受信できます。さらに、QoS ポリシーを構成すると、ファイアウォールはアクセスインターフェイスに QoS を適用し、マルチテナント展開でトラフィックの差別化された処理を提供できます。

デフォルトでは、*KVM* の *VM-Series* ファイアウォールは *VLAN* トランクモードで動作します。

©2023 Palo Alto Networks, Inc.

STEP 1 | ホストシステムで、VLAN アクセスモードで動作するように物理機能と仮想機能をセットアップします。

```
ip link set [inf_name] vf [vf_num] vlan [vlan_id]
```

VM-Series のファイアウォールで最高のパフォーマンスを得るには、次のことを確認してください。

- *CPU* ピニングを有効にします。「KVM 上の NUMA ノードへの CPU リソースの分離」を参照してください。
- *IPSec*トンネルを構成している場合は、リプレイ保護を無効にします。

  ファイアウォールの*Web*インターフェイスで、***Network*** > ***IPSec Tunnels***（***IPSec*** トンネル） を選択し、*IPSec tunnel*を選択して ***General***（全般）をクリックして、***Show Advanced Options***（詳細オプションの表示） を選択し、 ***Enable Replay Protection***（リプレイ プロテクションを有効にする） をオフにします。

STEP 2 | VM-Series のファイアウォールでCLIにアクセスします。

STEP 3 | VLANアクセスモードを有効にします。

```
request plugins vm-series vlan-mode access-mode on
```

VLAN アクセスモードを有効 にし、VLAN トランクモードを使用して **request plugins vm-series vlan-mode access-mode off**を入力します。

STEP 4 | ファイアウォールを再起動します。

```
request restart system
```

STEP 5 | VLANモードの設定を確認します。

```
show plugins vm-series vlan-mode
```

KVM 上の NIC のマルチキュー サポートの有効化

ゲスト XML 定義を変更してマルチキュー virtio-net を有効にします。マルチキュー virtio-net を使用すると、vCPU の数に合わせてネットワークのパフォーマンスを高めることができ、複数の TX および RX キューを作成して並列パケット処理を実現できます。

ゲスト XML 定義を変更します。N の値として 1 ～ 256 の値を挿入し、キューの数を指定します。最適な結果を得るには、キューの数を仮想マシンで設定されたデータプレーン コアの数に一致させます。

```
<interface type='network'>
      <source network='default'/>
      <model type='virtio'/>
      <driver name='vhost' queues='N'/>
```

 ©2023 Palo Alto Networks, Inc.

```
</interface>
```

KVM 上の NUMA ノードへの CPU リソースの分離

ゲスト VM の CPU リソースを、単一の不均一メモリアクセス（NUMA）ノードに隔離することで、KVM 上の VM-Series のパフォーマンスを向上させることができます。KVM 上では、**virsh** を使用して NUMA のトポロジーを確認できます。以下は 2 ノード NUMA システムの例です。

STEP 1 | NUMA トポロジーを表示します。以下の例には 2 つの NUMA ノード（ソケット）があり、それぞれにハイパースレッドが有効化された 4 コア CPU が搭載されています。偶数番号の CPU ID はすべて片方のノードに属し、奇数番号の CPU ID はすべて他方のノードに属します。

```
% virsh capabilities
<…>
  <topology>
    <cells num='2'>
      <cell id='0'>
        <memory unit='KiB'>33027228</memory>
        <pages unit='KiB' size='4'>8256807</pages>
        <pages unit='KiB' size='2048'>0</pages>
        <distances>
          <sibling id='0' value='10'/>
          <sibling id='1' value='20'/>
        </distances>
        <cpus num='8'>
          <cpu id='0' socket_id='1' core_id='0' siblings='0,8'/>
          <cpu id='2' socket_id='1' core_id='1' siblings='2,10'/>
          <cpu id='4' socket_id='1' core_id='2' siblings='4,12'/>
          <cpu id='6' socket_id='1' core_id='3' siblings='6,14'/>
          <cpu id='8' socket_id='1' core_id='0' siblings='0,8'/>
          <cpu id='10' socket_id='1' core_id='1' siblings='2,10'/>
          <cpu id='12' socket_id='1' core_id='2' siblings='4,12'/>
          <cpu id='14' socket_id='1' core_id='3' siblings='6,14'/>
        </cpus>
      </cell>
      <cell id='1'>
        <memory unit='KiB'>32933812</memory>
        <pages unit='KiB' size='4'>8233453</pages>
        <pages unit='KiB' size='2048'>0</pages>
        <distances>
          <sibling id='0' value='20'/>
          <sibling id='1' value='10'/>
        </distances>
        <cpus num='8'>
          <cpu id='1' socket_id='0' core_id='0' siblings='1,9'/>
          <cpu id='3' socket_id='0' core_id='1' siblings='3,11'/>
          <cpu id='5' socket_id='0' core_id='2' siblings='5,13'/>
          <cpu id='7' socket_id='0' core_id='3' siblings='7,15'/>
          <cpu id='9' socket_id='0' core_id='0' siblings='1,9'/>
          <cpu id='11' socket_id='0' core_id='1' siblings='3,11'/>
          <cpu id='13' socket_id='0' core_id='2' siblings='5,13'/>
          <cpu id='15' socket_id='0' core_id='3' siblings='7,15'/>
       </cpus>
```


©2023 Palo Alto Networks, Inc.

```
    </cell>
</cells>
```

STEP 2 | KVM の vCPU を特定の物理 CPU に固定するには、ゲストの xml 定義で **cpuset** 属性を使用します。この例では、8 基の vCPU がすべて最初の NUMA ノードの物理 CPU に固定されています。vCPU を明示的に固定したくない場合は、**cputune** ブロックを省略できます。この場合、すべての vCPU は cpuset で指定された CPU 範囲に固定されますが、明示的な対応付けは行われません。

```
<vcpu cpuset='0,2,4,6,8,10,12,14'>8</vcpu>
<cputune>
  <vcpupin vcpu='0' cpuset='0'/>
  <vcpupin vcpu='1' cpuset='2'/>
  <vcpupin vcpu='2' cpuset='4'/>
  <vcpupin vcpu='3' cpuset='6'/>
  <vcpupin vcpu='4' cpuset='8'/>
  <vcpupin vcpu='5' cpuset='10'/>
  <vcpupin vcpu='6' cpuset='12'/>
  <vcpupin vcpu='7' cpuset='14'/>
</cputune>
```


©2023 Palo Alto Networks, Inc.

Intelligent Traffic Offload インテリジェント トラフィック オフロード

インテリジェントトラフィックオフロードは VM-Series ファイアウォールセキュリティサブスクリプションであり、NVIDIA BlueField-2 DPU で構成すると、VM-Series ファイアウォールの容量スループットが向上します。VM-Series ファイアウォールと BlueField-2DPU は、カーネルバージョン 4.15.0-20 の Ubuntu18.04 を実行している x86 物理ホストにインストールする必要があります。VM-Series ファイアウォールは、バーチャルワイヤモードでデプロイする必要があります。

インテリジェントトラフィックオフロード （ITO）サービスは、フローの最初の数パケットをファイアウォールにルーティングして検査し、フロー内の残りのパケットを検査するかオフロードするかを決定します。この決定は、ポリシーまたはフローを検査できるかどうかに基づいています（たとえば、暗号化されたトラフィックは検査できません）。セキュリティ検査の恩恵を受けることができるフローのみを検査することにより、ファイアウォールの全体的な負荷が大幅に軽減され、セキュリティを犠牲にすることなく VM-Series ファイアウォールのパフォーマンスが向上します。

現在の NVIDIA BlueField-2 DPU のスケーラビリティの制限は次のとおりです。

- セッションテーブルの容量：500,000 セッション
- セッションテーブルの更新率：7000 セッション/秒
- 接続数/秒20,000
- オフロードヘアピンレート： 1500バイトパケットで最大 90 Gbps

BlueField-2 DPU へのオフロードトラフィックが毎秒 7,000 セッションを超える場合、またはオフロードセッションテーブルがいっぱいの場合でも、トラフィックは VM-Series ファイアウォールを通過して検査されます。1 秒あたりのセッション数が 7,000 を下回ると、Bluefield-2 DPU へのインテリジェントトラフィックのオフロードが再開されます。

アクティブ/パッシブの HAは、同じ構成の物理ホストで実行されている VM-Series ファイアウォールでサポートされています。

インテリジェントトラフィックオフロードは、加速エージングセッション設定をサポートしていません。

- インテリジェントトラフィックオフロードの要件
- インテリジェントトラフィックオフロードインターフェース
- 高可用性（HA）
- BlueField-2 DPU のインストール
- VM-Series ファイアウォールのインストール
- BlueField-2 DPU システムの確認
- 仮想関数の有効化
- BlueField ブートストリームソフトウェアのインストールまたはアップグレード

©2023 Palo Alto Networks, Inc.

- Debian パッケージのインストールまたはアップグレード
- インテリジェントトラフィックオフロードの実行
- BlueField-2 DPU のトラブルシューティング
- PAN-OS のトラブルシューティング
- 参考資料

インテリジェントトラフィックオフロードの要件

ITO には、同じ x86 物理ホストに 1 つの VM-Series ファイアウォールと 1 つの BlueField-2 DPU がインストールされている必要があります。VM-Series ファイアウォールのアクティブ/パッシブの高可用性がサポートされています。

ホストごとにデプロイできる ***VM-Series*** ファイアウォールと ***BlueField-2 DPU*** はそれぞれ ***1*** つだけです。

- 2 つの利用可能な 100GB/s ポート（HA の場合は 4 つ）を備えたネットワークスイッチ。

  VLAN を使用する場合は、スイッチが機能していることを確認してください。
- X86 物理ホストハードウェアの要件。
  - 最小 120GB の使用可能な RAM （サーバーの場合は 64GB/VM-Series ファイアウォールの場合は 56GB）
  - 最小 18 個の物理コア
  - PCI-e スロット 3 または 4 に 2 つの 100GB/s ポートが取り付けられた Bluefield-2 SmartNIC MBF2M516A-CEEOT。
  - NVIDIA BlueField イーサネットDPUユーザーガイドで推奨されている、BlueField2 DPU の各ポートごとに認定済み 100GigE SFP。
- X86 ホストソフトウェアの要件。
  - Ubuntu 18.04、カーネルバージョン 4.15.0-20。
  - ブルーフィールドバイナリブートストリームバージョン：5.3-1.0.0.1

    ダウンロードを開始するための、エンドユーザー使用許諾契約への同意。
- VM-Series ファイアウォール用の仮想マシン。
  - PAN-OS 10.1 以降。
  - VM-Series プラグイン 2.1.0 以降。
  - インテリジェントトラフィックオフロードのライセンスを取得するには、10.0.4 以降のソフトウェア NGFW デプロイメントプロファイルを作成します。そこでは、最低 18 個の vCPU とインテリジェントトラフィックオフロードサービスを使用します。プロファイルには、他のセキュリティサービスを組み入れることができます。

    PAN-OS 10.1.1 以降および VM-Series プラグイン 2.1.1 以降を使用して、インテリジェントトラフィックオフロードのライセンスを取得するには、10.0.4 以降のソフトウェア NGFW デプロイメントプロファイルを作成します。ただし、vCPU は 6 つ以上で、イン

 ©2023 Palo Alto Networks, Inc.

テリジェントトラフィックオフロードサービスを使用します。プロファイルには、他のセキュリティサービスを組み入れることができます。

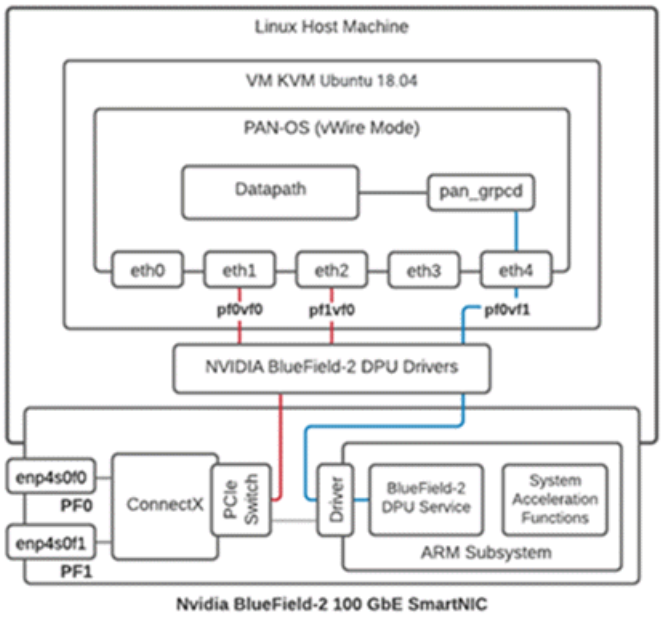
インテリジェントトラフィックオフロードインターフェース

インテリジェントトラフィックオフロードをデプロイすると、次の 3 種類のインターフェースを接続します。

- PAN-OS 仮想インターフェース：
  - eth0： 管理インターフェース
  - eth1、eth2： データプレーン
  - eth3:HA インターフェイス
  - eth4： gRPCインターフェース
- BlueField-2 DPU 物理インターフェース（ホスト OS から作成）。
- BlueField-2 DPU 100GB ポート（ホスト OS から作成）のホスト物理インターフェース。

PAN-OS インターフェースは、物理ホスト上に作成した SR-IOV 仮想関数 （VF） を介して BlueField-2 DPU に接続します（仮想関数の有効化を参照）。

次の図では、2 つの BlueField-2 DPU ポートが物理関数 PF0 および PF1 として示されています。これらの PF は、ホスト側から enp4s0f0 および enp4s0f1 として監視でき、SR-IOV 機能のために複数の VF に分割されます。



- 各 PF の最初の VF は、データポート（eth1：pf0vf0）である必要があります。
- gRPC クライアント/サーバーインターフェース（eth4：pf0v1）の制御チャネルには追加の VF が必要です。

 ©2023 Palo Alto Networks, Inc.

- ホスト側からの VF は次のとおりです。
  - enp4s0f0 は、BlueField-2 DPU では pf0vf0 と pf1vf0 で表され、データに使用されます。
  - enp4s0f1 は pf0vf1 で表され、gRPC 制御トラフィックに使用されます。

高可用性（HA）

アクティブ/パッシブの HA は、物理ホスト上で Vwire モードでデプロイされた VM-Series ファイアウォールのペアに対してサポートされます。

- ファイアウォールは、インテリジェントトラフィックオフロードの要件で指定されているように構成された BlueField-2 DPU を使用して物理ホストにインストールする必要があります。
- HA2 インターフェース（アクティブパケットフローおよびパッシブパケットフローの図を参照）の場合、両方のホストで同じ Mellanox インターフェース（cx-3、cx-4、または cx-5）を使用します。
- （任意）トラフィックスイッチングをサポートするには、ホストが別々の VLAN 上にある必要があります。これにより、「Linux ホスト間のトラフィックの保護」で説明されているように、VLAN タグを使用してプライマリを選択できます。

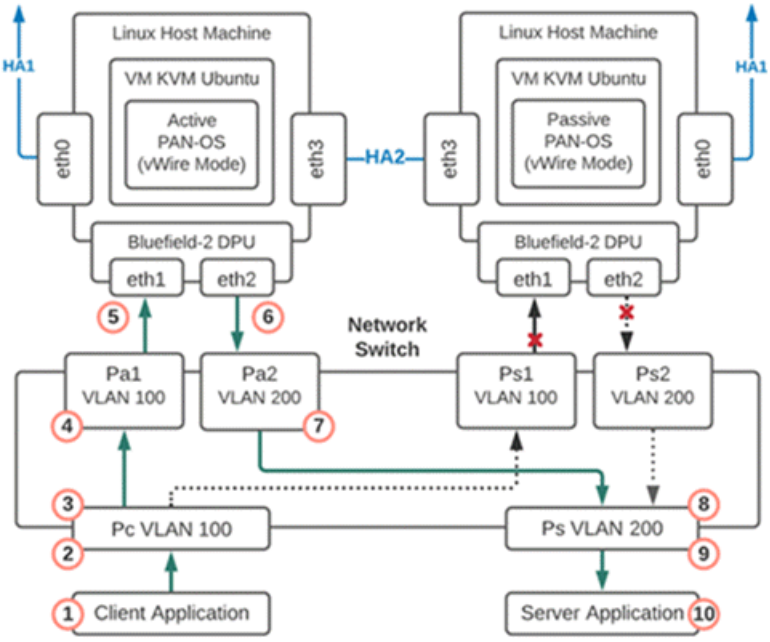
ITO H/A は、VM-Series ファイアウォールの可用性に重点を置いています。各ファイアウォールはセッションテーブルを保守し、各 BlueField-2 DPU はフローテーブルを保守します。HA 構成は、アクティブセッションテーブルを同期し、実行時にパッシブファイアウォールにミラーリングされるようにします。セッションテーブルには、検査が必要なセッションと、オフロードのマークが付けられたセッションの両方が格納されます。

HA は、VM-Series ファイアウォールの NIC 上にある PAN-OS インターフェース eth3 を使用します。Eth3 は、アクティブファイアウォールを選択し、アクティブ/パッシブペアで VM-Series ファイアウォールセッションテーブルを同期します。

アクティブパケットフロー

次の図は、オプションの VLAN 構成を使用する HA 構成のアクティブなパケットフローをたどるステップを示しています。

©2023 Palo Alto Networks, Inc.



1. パケットはクライアントアプリケーションからネットワークスイッチに送信されます。
2. パケットは、VLAN 100 タグをパケットに追加するようにプログラムされたスイッチポートに着信します。
3. ファイアウォールがパッシブモードであるためにポート Ps1 のインターフェースがダウンしているため、タグ付きパケットは、ポート Pa1 にのみ送信できます。
4. パケットがポート Pa1 に到着すると、VLAN 100 がパケットから削除され、パケットはファイアウォール eth1 に配信されます。
5. ファイアウォールは vWire モードで稼働されているため、パケットはファイアウォールによって処理されてから eth2 に送信されます。
6. パケットがポート Pa2 に到着すると、VLAN 200 が追加されます。
7. パケットはポート Pa2 から送出されますが、他の VLAN 200 ポート Ps2 がダウンしているため、ポート Ps への送信のみが可能です。
8. パケットがポート Ps に到着すると、VLAN 200 タグが削除されます。
9. パケットは VLAN タグなしでポート Ps に送信されます
10. パケットはサーバーに配信されます。

フェイルオーバーイベント

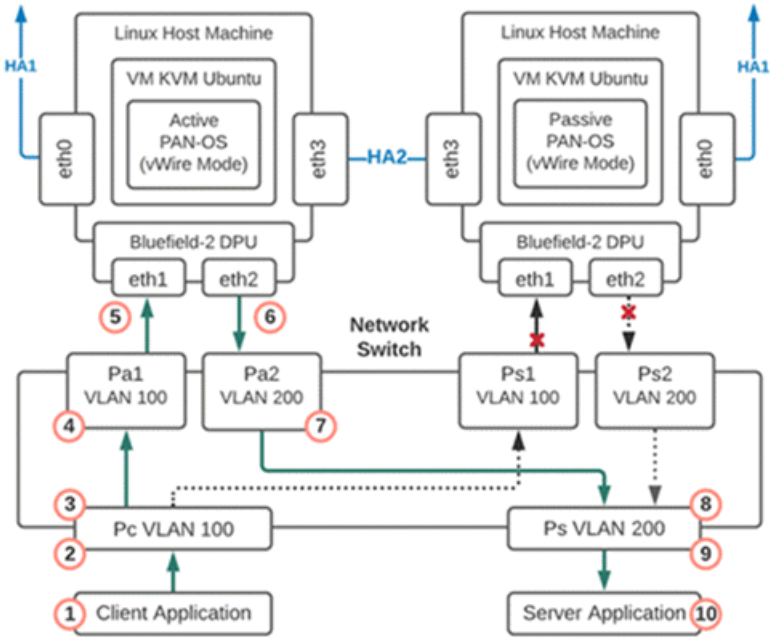
フェイルオーバーイベントは、アクティブな VM-Series ファイアウォールからの通知があったときや、アクティブが応答していないことをパッシブファイアウォールが検出したときに発生します。これが発生すると、ポート Pa1 および Pa2 へのネットワーク接続がダウンし、ポート Ps1 および Ps2 へのネットワーク接続がアクティブになります。

パッシブパケットフロー

VM-Series ファイアウォールがパッシブ状態の場合、パッシブメンバーの BlueField-2 DPU は稼働していますが、フェイルオーバーが発生し、同じ場所に配置された VM-Series ファイアウォー

©2023 Palo Alto Networks, Inc.

ルがアクティブになるまでトラフィックを通過させません。次の図は、オプションの VLAN 構成を使用する HA 構成のパッシブパケットフローをたどるステップを示しています。



1. パケットは、クライアントアプリケーションからネットワークスイッチに送信されます。
2. パケットは、VLAN 100 タグをパケットに追加するようにプログラムされたスイッチポートに着信します。
3. ポート Pa1 のインターフェースがダウンしていて、ファイアウォールがパッシブからアクティブに移行したため、タグ付きパケットは、ポート Ps1 への送信のみが可能です。
4. パケットがポート Ps1 に到着すると、VLAN 100 がパケットから削除され、パケットはファイアウォール eth1 に配信されます。
5. ファイアウォールは vWire モードで稼働されているため、パケットはファイアウォールによって処理されてから eth2 に送信されます。
6. パケットがポート Ps2 に到着すると、VLAN 200 が追加されます。
7. パケットはポート Ps2 から送出されますが、他の VLAN 200 ポート Ps2 がダウンしているため、ポート Ps への送信のみが可能です。
8. パケットがポート Ps に到着すると、VLAN 200 タグが削除されます。
9. パケットは VLAN タグなしでポート Ps に送信されます。
10. パケットはサーバーに配信されます。

BlueField-2 DPU のインストール

VM-Series ファイアウォールをインストールする前に、BlueField-2 DPU を物理ホストにインストールします。BlueField-2 DPU の詳細については、ソフトウェアのドキュメントを参照してください。NVIDIA BLUEFIELD DPU FAMILY SOFTWARE V3.5.0.11563 マニュアル.

1. NVIDIA BlueField イーサネット DPU ユーザーガイドの指示に従って、BlueField-2 DPU をホストマシンにインストールします。

©2023 Palo Alto Networks, Inc.

2. NVIDIA BlueField-2 DPU ソフトウェアクイックスタートガイドの指示に従ってBlueField ドライバーをインストールします。

VM-Series ファイアウォールのインストール

VM-Series ファイアウォールでの KVM の標準インストールでは、PAN-OS がインストールされます。次のセクションのインストール手順に従います。

- KVM 上の VM-Series — 要件と前提条件
- Virt-Manager を使用した VM-Series ファイアウォールのインストールまたはISO を使用した VM-Series ファイアウォールのインストール

仮想関数の有効化

インテリジェントトラフィックオフロードインターフェースの仮想関数（VF）で説明したとおりに、PAN-OS インターフェースを BlueField-2 DPU に接続します。

ポートあたりの仮想関数 VF の最大数は 2 です。データパス用に 2 つと管理インターフェース用に 1 つの合計 3 つが必要です。

STEP 1 | ホストマシンで仮想関数を有効にします。

- デフォルトでは、BlueField-2 DPU はデータパスに最初の VF を使用します。つまりそれは、次の例では enp4s0f0v0 と enp4s0f1v0 です。
- もう 1 つのVFである enp4s0f0v1 は、BlueField-2 カードで実行されているサービスの管理インターフェースに使用されます（VM-Series ファイアウォール管理インターフェースと混同しないでください）。

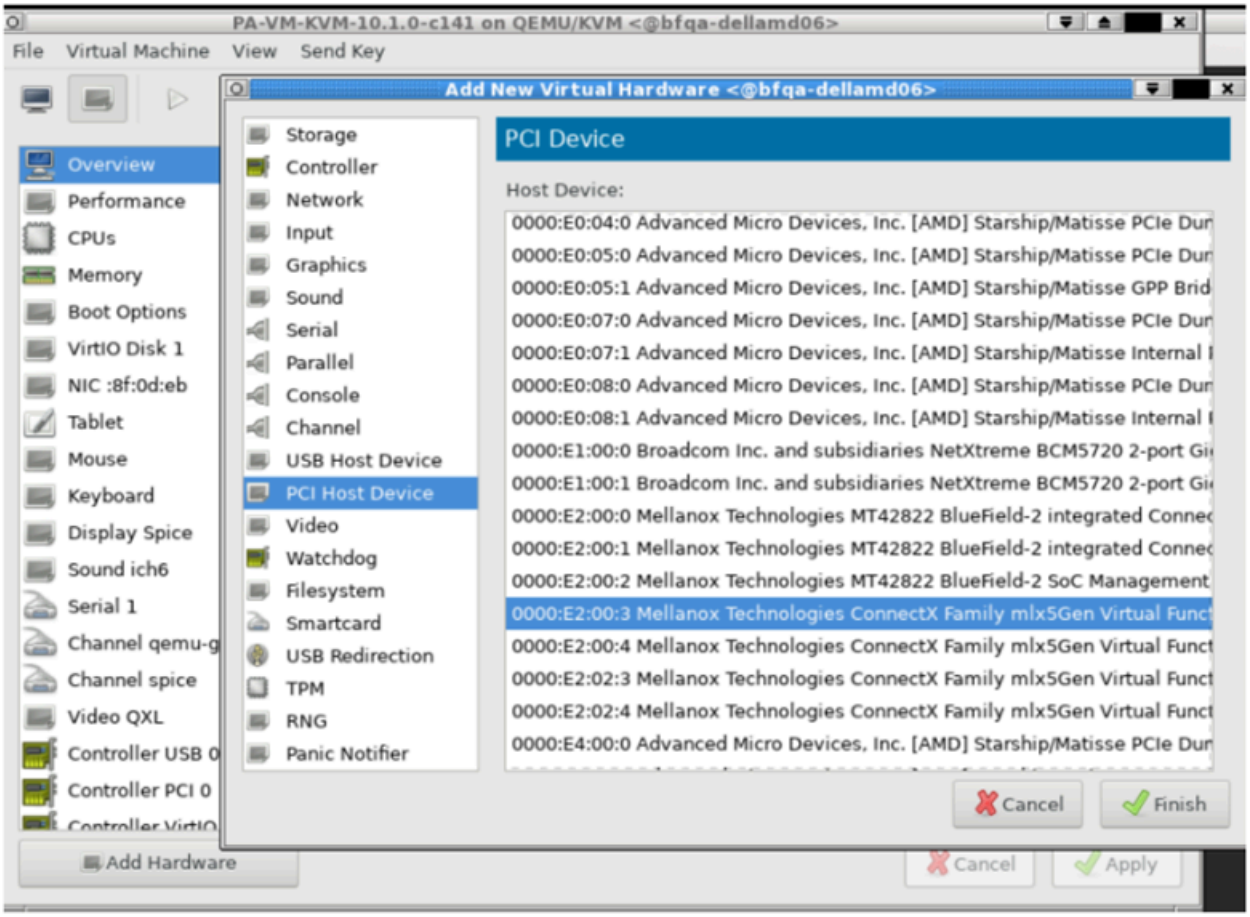
```
$ cat /sys/class/net/enp4s0f0/device/sriov_totalvfs
   8
$ echo 2 > /sys/class/net/enp4s0f0/device/sriov_numvfs
$ cat /sys/class/net/enp4s0f1/device/sriov_totalvfs
   8
$ echo 2 > /sys/class/net/enp4s0f1/device/sriov_numvfs
```


©2023 Palo Alto Networks, Inc.

STEP 2 | KVM ハイパーバイザーから VM-Series ファイアウォールに VF を割り当てます。

VF が VM に割り当てられていない限り、ゲスト PAN-OS は起動しません。

1. VM をシャットダウンします。
2. KVMでは、virt-manager を使用して VF を VM に追加します。
   - [ハードウェアの追加]を選択し、PF1 の VF0 を選択して、[完了]をクリックします。
   - [ハードウェアの追加]を選択し、PF0 の VF0 を選択して、[完了]をクリックします。
   - [ハードウェアの追加]を選択し、PF0 の VF1 を選択して、[完了]をクリックします。



BlueField-2 DPU システムの確認

Rshim ドライバーがホストにインストールされているとき、BlueField-2 DPU は、最初にホストと通信します。Rshim は、tty（minicom からアクセス可能）インターフェースと、tmfifo_net0 と呼ばれるネットワークインターフェースを提供します。tmfifo_net0 インターフェースを使用すると、ホストから BlueField-2 DPU に SSH で接続できます。Rshim ドライバーは x86 ハイパーバイザー OS で稼働しますが、実際、OFED インストールはデフォルトで Rshim ドライバーをインストールします。

©2023 Palo Alto Networks, Inc.

STEP 1 | ホストマシンにログインします。

```
$ ssh user@<host-ip-address>
```

```
$ password:
```

STEP 2 | Rshimド ライバーのホストネットワークインターフェースに IP アドレスがない場合は、IP アドレスを作成する必要があります。

```
$ ip addr add dev tmfifo_net0 192.168.100.1/24
```

STEP 3 | ホストマシンから BlueField-2 DPU サブシステムにログインします。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password: ubuntu
```

これが初めてのログインである場合、システムはデフォルトのパスワードを新しいパスワードに置き換えるように指示します。

STEP 4 | BlueField-2 DPU のデフォルトのパスワードを変更します。

最初のユーザー名を **ubuntu**、パスワードを **ubuntu** としてBlueField-2 DPU にログインします。

ログインすると、新しいパスワードを設定するように求められます。

```
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for ubuntu.
Current password: *****
New password:  *****
Retype new password: *****
passwd: password updated successfully
```

ログアウトして、新しいパスワードでログインします。

STEP 5 | ソフトウェア バージョンを確認します。

```
$ ofed_info -s
```

この場合、次のバージョンまたはそれ以降が返されるはずです。

```
$ MLNX_OFED_LINUX-5.3-0.3.3
```

STEP 6 | Bluefield 2 DPU が正しいモードになっていることを確認します。

正しいモードは、組み込み CPU 機能所有権モードです。モードを確認および構成する手順については、組み込み CPU 機能所有権モードのドキュメントを参照してください。

©2023 Palo Alto Networks, Inc.

BlueField ブートストリームソフトウェアのインストールまたはアップグレード

次の手順に従って、BlueField-2 DPU 用の最新の Bluefield ブートストリーム（BFB） ソフトウェアを使用していることを確認してください。BFB には、BlueField OS と、ドライバーやネットワークインターフェースなどの他のソフトウェアが組み入れられています。

STEP 1 | BFB パッケージを BlueField-2 DPU の物理ホストにダウンロードします。

NVIDIA Web サイトから、DPI ARM コアで実行されている OS 用のドライバーの最新バージョンを入手します。ダウンロードするには、エンドユーザー使用許諾契約に同意する必要があります。

STEP 2 | 物理ホストの Rshim ブート場所から BFB をインストールします。

以下のファイル名（**DOCA** で始まり **.bfb** で終わる文字列）では、スペースが使用されていないことに注意してください。コマンドを 1 行で入力します。

```
$ cat DOCA_v1.0_BlueField_OS_Ubuntu_20.04-5.3-1.0.0.0-3.6.0.11699-1-aarch64.bfb > /dev/rshim0/boot
```

STEP 3 | BlueField-2 DPU にログインします。

BlueField-2 DPU システムの確認で作成した新しいパスワードを使用します。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 4 | BlueField-2 DPU にファームウェアアップグレードを適用します。

次のコマンドを 1 行で入力します。

```
$ sudo /opt/mellanox/mlnx-fw-updater/firmware/mlxfwmanager_sriov_dis_aarch64_41686
```

STEP 5 | システムの電源を入れ直します。

BlueField-2 DPU からログオフし、Linux ホストに戻ります。

```
$ ipmitool chassis power cycle
```

STEP 6 | BlueField-2 DPU にログインします。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```


©2023 Palo Alto Networks, Inc.

STEP 7 | BlueField-2 DPU で opof （オープンオフロード）サービスを開始します。現時点では、opof はスタンドアロンサービスです。

> *opof* を開始する場合、事前に *VF* が存在している必要があります。「仮想関数の有効化」を参照してください。

```
$ opof_setup
$ service opof restart
```

STEP 8 | opof サービスが問題なく実行されていることを確認します。

```
$ service opof status
```

Debian パッケージのインストールまたはアップグレード

Debian パッケージのバージョンが 1.0.4 より前の場合は、アップグレードする必要があります。

STEP 1 | BlueField-2 DPU で、opof パッケージのバージョンを確認します。

```
$ opof -v
```

1.0.4 より前の場合は、アップグレードする必要があります。

STEP 2 | パッケージの NVIDIA リポジトリを追加します。

```
$ cd /etc/apt/sources.list.d
```

各 `wget` コマンドをすべて 1 行で入力します。URL にスペースはありません：

```
wget https://linux.mellanox.com/public/repo/doca/1.0/ubuntu20.04/
doca.list
wget -qO - https://linux.mellanox.com/public/repo/doca/1.0/
ubuntu20.04/aarch64/GPG-KEY-Mellanox.pub | sudo apt-key add -
$ apt update
```

STEP 3 | BlueField-2 DPU で、リポジトリ内の Debian パッケージを確認します。

```
$ apt search opof
```

```
Sorting... Done
Full Text Search... Done
opof/now 1.0.4 arm64 [installed,local]
  Nvidia Firewall Open Offload Daemon
```

STEP 4 | ARM で、古い Debian パッケージをアンインストールします。

```
$ apt remove opof
```

STEP 5 | 新しい Debian パッケージをインストールします。

```
$ apt install opof
```


©2023 Palo Alto Networks, Inc.

STEP 6 | opof サービスをセットアップして再起動します。

```
$ opof_setup
$ service opof restart
```

STEP 7 | opof サービスが問題なく実行されていることを確認します。

```
$ service opof status
```

インテリジェントトラフィックオフロードの実行

このソリューションでは、最高のパフォーマンス/スループットを得るために、インテリジェントトラフィックオフロードソフトウェアへのサブスクリプションと最低 18 個の物理コアが必要です。デフォルトでは、PAN-OS はインテリジェントトラフィックオフロード用に 2 個のコア、管理プロセス用に 4 個のコア、データプレーン処理用に残りの 12 個のコアを割り当てます。

- VM-Series ファイアウォールでのインテリジェントトラフィックオフロードのセットアップ
- BlueField-2 DPU でのインテリジェントトラフィックオフロードサービスのセットアップ
- インテリジェントトラフィックオフロードサービスの開始または再起動
- サービスステータスとヘルスの取得

VM-Series ファイアウォールでのインテリジェントトラフィックオフロードのセットアップ

次の手順に従って、PAN-OS でインテリジェントトラフィックオフロードを有効にします。

STEP 1 | PAN-OS VM を起動します。これは、VM インスタンスがすでに作成されて再起動されていることを前提としています。

```
$ virsh start <vm-name>
```

STEP 2 | SSH を使用して、VM-Series ファイアウォール管理インターフェースにログインします。

```
$ ssh admin@<panos-management-IP-address>
```

```
$ admin@PA-VM>
```

STEP 3 | インテリジェントトラフィックオフロードがインストールされ、ライセンスが付与されていることを確認します。

```
admin@PA-VM> show intelligent-traffic-offload
```

```
Intelligent Traffic Offload:
  Configuration            : Enabled
  Operation Enabled        : True
  Min number packet        : 8
  Min Rate                 : 95
  TCP ageing               : 12-
```


©2023 Palo Alto Networks, Inc.

```
  UDP ageing                : 20
```

構成:有効は、インテリジェントトラフィックオフロードのライセンスが付与されていることを意味します。

操作有効:Trueは、構成済みのデバイスを再起動したことを意味します。

STEP 4 | インテリジェントトラフィックオフロードを有効にします。

次のコマンドを使用して、システムを再起動せずに ITO を有効にします。

admin@PA-VM> **set session offload yes**

set session offload no を使用して、システムをリブートせずに ITO を無効にすることもできます。

STEP 5 | インテリジェントトラフィックオフロードを検証します。

admin@PA-VM> **show session info | match offload**

```
Hardware session offloading:      True
Hardware UDP session offloading:  True
```

グローバルカウンターを表示するには、次のコマンドを使用します。

admin@PA-VM> **show counter global | match flow_offload**

出力の構成と各カウンターの説明の詳細については、セッション数を参照してください。

BlueField-2 DPU でのインテリジェントトラフィックオフロードサービスのセットアップ

このサービスは、VM-Series ファイアウォールでのインテリジェントトラフィックオフロードのセットアップで説明されているように、構築する必要があります。

STEP 1 | ホストマシンから、BlueField-2 DPU コンプレックスにログインします。

$ **ssh ubuntu@192.168.100.2**

```
$ password: ubuntu
$ ubuntu> sudo -i
```

STEP 2 | BlueField-2 DPU OS で予備構成をセットアップします。

root@bf2SmartNIC:~# **opof_setup**

```
[ INFO ] No num of hugepages specified, use 2048
[ INFO ] No gRPC port specified, use pf0vf1
Configure ovs fallback
Configure grpc for pf0vf1
Reserved 2048*2MB hugepages
```


©2023 Palo Alto Networks, Inc.

インテリジェントトラフィックオフロードサービスの開始または再起動

ITO サービスが DPU で実行されている場合、このサービスはおそらく自動的に開始されたものです。ステータスを確認するには、次のコマンドを実行します。

```
$ service opof status
```

opof サービスが実行されていない場合は、次のコマンドを入力してコントローラーを起動します。

```
$ service opof start
```

サービスを再起動するには、次のコマンドを実行します。

```
$ service opof restart
```

サービスステータスとヘルスの取得

opof を使用して、サービスのステータスとヘルスを取得します。各コマンドには、例えば **$ opof -h** のような、独自のコマンドラインヘルプがあります。

- 次のように、セッションをクエリします。

  ```
  $ opof query -i <session_id>
  ```

- 次のように、サービスオフロード統計をクエリします。

  ```
  $ opof stats
  ```

BlueField-2 DPU のトラブルシューティング

次の手順を使用して、システムの電源を入れ直します。

1. システムの電源を入れ直すには、BlueField-2 DPU からログアウトし、Linux ホスト OS に戻ります。

   ```
   $ ipmitool chassis power cycle
   ```

2. 電源を入れ直してもインターフェースが起動しない場合は、BlueField-2 DPU にログインして次のように入力します。

   ```
   $ /sbin/mlnx_bf_configure
   ```

3. ホスト OS に戻り、次のように入力します。

   ```
   $ sudo /etc/init.d/openibd restart
   ```

PAN-OS のトラブルシューティング

トラフィックフローの検証

データトラフィックは、クライアントから生成され、サーバーでセットアップされたインテリジェントトラフィックオフロードを通じて消費されます。IPERF3 テストの実行で説明されているように、IPERF3 を使用してトラフィックを生成できます。トラフィックが開始されると、フローの最初の数パケットが PA-VM に送信され、PA-VM がフローをオフロードする必要があるかどうかを決定します。

©2023 Palo Alto Networks, Inc.

オフロードのフローを識別するには、アプリケーションオーバーライドポリシーを定義する必要があります。TCP フローは、制御パケットに FIN/RST フラグを設定し、それを PA-VM に送信します。PA-VM がフローをオフロードすると決定したら、show session all を使用して、オフロードされたフローを表示します。**show session id <flowID>** を使用して、フローの状態に関する情報を提供します。オフロードされたフローの状態はオフロード：はいです。

フローの後続のパケットがオフロード状態にあり、BlueField-2 DPU を通過している間、フローカウンターは更新されません。フローが完了すると、オフロードサービスはエージングアウトタイマー（CLI から設定された TCP エージング）をトリガーします。タイマーの期限が切れると、サービスは更新されたフロー統計を収集し、VM-Series ファイアウォールに送信します。次に、ファイアウォールはフローセッションカウンターを更新し、**show session id <flowID>** は更新された値を返します。

セッション数

次のコマンドを使用して、セッションカウンターを表示します。

admin@PA-VM > **show counter global | match flow_offload**

各カウンターの出力列は次のとおりです。

カウンター名|値|レート|重大度|カテゴリ|アスペクト|説明。

- 値 - システム起動以降の発生数。
- レート - カウンター変更の頻度。
- 重大度 - 情報、警告、ドロップ。テクニカルサポートに使用されます。
- カテゴリ - フロー（セッションのコンポーネント）。
- アスペクト - フロー全体のオフロード。

カウンター名	の意味
flow_offload_rcv_cpu	セッションがオフロードされた状態中に CPU が受信したパケットの数
flow_offload_session_update	セッションを更新する必要がある回数
flow_offload_session_insert	オフロードデバイスに挿入されたセッションの数
flow_offload_session_delete	オフロードデバイスから削除されたセッションの数
flow_offload_delete_msg_failed	失敗した GRPC への del メッセージの数
flow_offload_add_msg_failed	失敗した GRPC へのセッションメッセージの数
flow_offload_session_verify	オフロードデバイスへの確認メッセージの数
flow_offload_verify_msg_failed	失敗した GRPC への検証メッセージの数
flow_offload_update_session_stat	HW はフローエイジアウトを示します

©2023 Palo Alto Networks, Inc.

カウンター名	の意味
flow_offload_missing_session_stat	統計のセッションが見つかりません
flow_offload_invalid_session	無効なセッション ID をオフロードします
flow_offload_del_session_fail	無効なセッションの削除をオフロードします
flow_offload_add_session_fail	オフロード追加セッションが失敗しました
flow_offload_get_session_fail	Get セッションのオフロードに失敗しました
flow_offload_grpc_fail	grpc 呼び出しのオフロードに失敗しました
flow_offload_active_session	アクティブなオフロードされたセッションの数
flow_offload_aged_session	エージングアウトされたオフロードセッションの数
flow_offload_session	オフロードされたセッションの数

IPERF3 テストの実行

Iperf3 は、データトラフィックテストの実行に対して有効なトラフィックを生成するためのオプションのシンプルなアプリケーションです。サーバーをサービスとして実行するには、**iperf3 -s-D** を使用します。デフォルトでは、アプリケーションは TCP/UDP 宛先ポート 5201 でパケットを待機しますが、ポートは変更できます。

- シングルフロー - シングル iperf3 フローの場合、次のように入力します。

```
iperf3 -c <server-ip-address> -t 60
```

- 複数のフロー - 60 秒間に 20 の同時フローを開始するには、次のように入力します。

```
iperf3 -c <ip of server> -P 20 -t 60
```

インテリジェントトラフィックオフロードの検証

VM-Series ファイアウォールログを使用して、ファイアウォールで実行されている ITO クライアントと BlueField-2 DPU のオフロードサービス間の接続を検証できます。オフロードが成功した場合に予想されるログ出力は次のとおりです。

admin@auto-pavm> **less mp-log pan_grpcd.log**

```
[PD] dec free list 0xe0ff022000
RS LIB INIT in DP!
pan_fec_app_init: fec_data 0xe0feef1088, maxentries 120
[FEC] enc free list 0xe0feef1100, dec free list 0xe0feef10b8
Creating dp grpc ring buf
Initializing dp grpc ring buf
```


©2023 Palo Alto Networks, Inc.

```
Mapping flow data memory
Found offload parameters
Heart beat found 1
Established connection to offload device
```

OPOF のトラブルシューティング

オフロードサービスログを表示して、接続を検証することもできます。

root@linux:~# **service opof status**

```
● opof.service - Nvidia Firewall Intelligent Traffic Offload Daemon
   Loaded: loaded (/etc/systemd/system/opof.service; disabled; vendor
 preset: enabled)
   Active: active (running) since Fri 2021-05-21 18:40:38 UTC; 3h
 48min ago
    Docs: file:/opt/mellanox/opof/README.md
  Process: 163906 ExecStartPre=/usr/sbin/opof_pre_check (code=exited,
 status=0/SUCCESS)
  Main PID: 163922 (nv_opof)
   Tasks: 30 (limit: 19085)
   Memory: 50.7M
   CGroup: /system.slice/opof.service
           └─163922 /usr/sbin/nv_opof -n 1 -a
 0000:03:00.0,representor=[0] -a 0000:03:00.1,representor=[0]
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe PCI
 driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.0 (socket 0)
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL:  Invalid
 NUMA socket, default to 0
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe PCI
 driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.0 (socket 0)
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL:  Invalid
 NUMA socket, default to 0
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe PCI
 driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.1 (socket 0)
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL:  Invalid
 NUMA socket, default to 0
May 21 18:40:38 localhost.localdomain nv_opof[163922]: EAL: Probe PCI
 driver: mlx5_pci (15b3:a2d6) device: 0000:03:00.1 (socket 0)
May 21 18:40:39 localhost.localdomain nv_opof[163922]: EAL: No legacy
 callbacks, legacy socket not created
May 21 18:40:39 localhost.localdomain nv_opof[163922]: EAL: No legacy
 callbacks, legacy socket not created
May 21 18:40:42 localhost.localdomain nv_opof[163922]: Server
 listening on: 169.254.33.51:3443
```

ログは、インテリジェントトラフィックオフロードが IP アドレスをリッスンしているサーバーを介して VM-Series ファイアウォール PA-VM と通信していることを示しており、DPDK パラメーターの他の詳細とともに VF が表示されます。オフロードされる TCP フローの追加からのログも添付されます。

参考資料

- NVIDIABlueField イーサネット DPU ユーザーガイド

©2023 Palo Alto Networks, Inc.

- NVIDIA BLUEFIELD DPUFAMILY ソフトウェア V3.5.0.11563D
- Nvidia DPU インテリジェントトラフィックオフロードデーモン
- OpenOffload gRPC GITHUB
- PAN-OS 管理者ガイド

©2023 Palo Alto Networks, Inc.

Hyper-V 上での VM-Series ファイアウォールのセットアップ

VM-Seriesファイアウォールは、Microsoft Hyper-Vが動作しているサーバー上にデプロイできます。Hyper-Vは、スタンドアロンのハイパーバイザー、またはWindowsサーバー向けのアドオン/ロールです。

- サポートされている Hyper-V のデプロイ
- Hyper-V のシステム要件
- Linux 統合サービス
- Hyper-V 上での VM-Series ファイアウォールのインストール

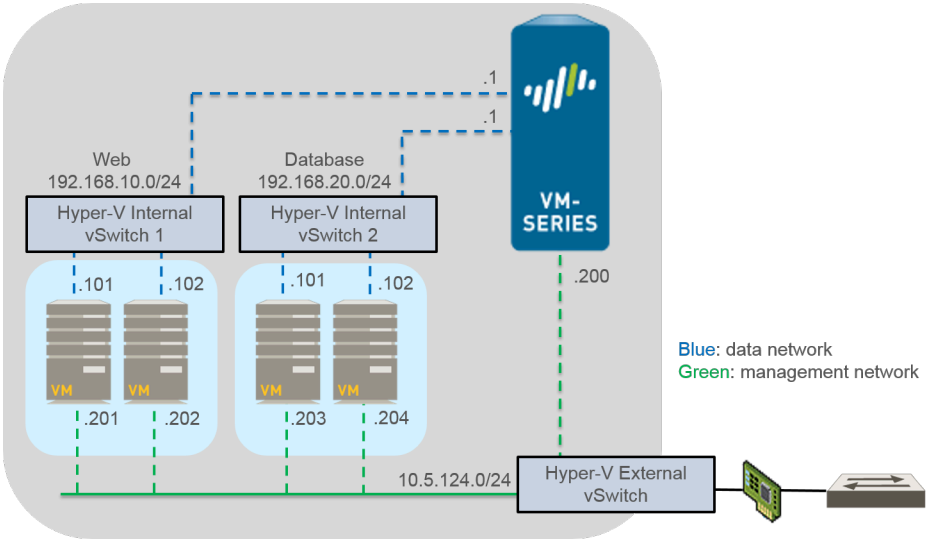
サポートされている Hyper-V のデプロイ

Hyper-Vが動作しているホストには、VM-Series ファイアウォールの 1 つ以上のインスタンスをデプロイできます。どこに VM-Series ファイアウォールをデプロイするかは、ネットワークトポロジによって異なります。VM シリーズはタップ、バーチャル ワイヤ、レイヤー 2 およびレイヤー 3 のインターフェイスのデプロイをサポートしています。

- 単一 Hyper-V ホストのトラフィックの保護
- 複数 Hyper-V ホスト全体のトラフィックの保護

単一 Hyper-V ホストのトラフィックの保護

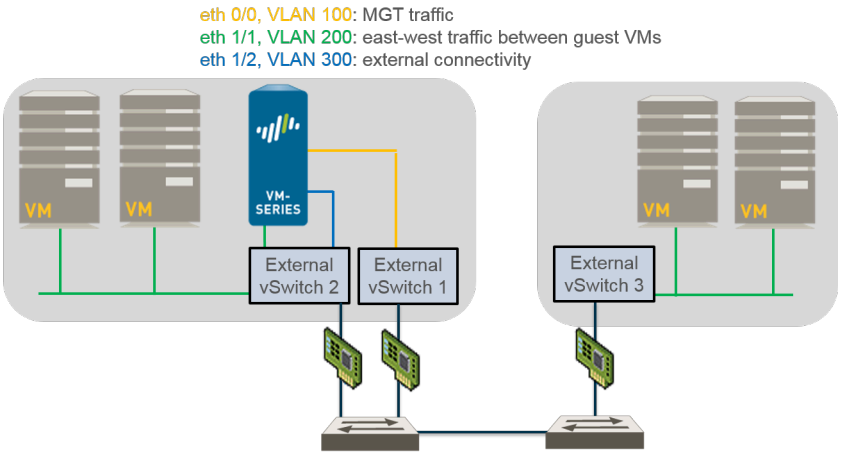
VM-Series ファイアウォールは、他のゲスト VM とともに単一の Hyper-V ホストにデプロイします。以下の例では、VM-Series ファイアウォールにはレイヤー 3 インターフェイスが一つあり、VM-Series および他のゲスト VM が Hyper-V vSwitch によって接続されています。Web サーバーおよびデータベース サーバー間のすべてのトラフィックはファイアウォールを通してルーティングされます。データベース サーバー間のみ、あるいは Web サーバー間のみのトラフィックは外部 vSwitch によって処理され、ファイアウォールを通してルーティングされることはありません。



複数 Hyper-V ホスト全体のトラフィックの保護

VM-Series ファイアウォールをデプロイすれば複数 Hyper-V ホストのトラフィックを保護することができます。以下の例では、VM-Series はレイヤー 2 モードでデプロイされており、ゲスト VM を出入りするトラフィックを保護しています。2 つの Hyper-V ホストに渡って広がる 4 つのゲスト VM 間のトラフィックを単一の VM-Series ファイアウォールが保護します。VLAN タギングは、トラフィックを論理的に隔離してファイアウォールに向かわせるために使用します。さらに、管理トラフィックは固有の外部 vSwitch に配置され、他のすべてのトラフィックから切り離されます。

©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.

Hyper-V のシステム要件

VM-Series では Hyper-V ホストに一定のリソース配分が求められるため、以下にリストアップされている各要件に必ず従い、最適なパフォーマンスを得られるようにしてください。

- ホスト CPU は、仮想化拡張機能を持つ 64 ビット x86 ベースの Intel または AMD の CPU である必要があります。
- VM-Series モデルの最小ハードウェア要件については、「VM-Series システム要件」を参照してください。
- 2 つ以上のネットワーク アダプタ。VM-Series ファイアウォールは合成ネットワーク アダプタをサポートしており、エミュレート ネットワーク アダプタよりも優れたパフォーマンスを発揮します。Hyper-V は最大 8 つの合成ネットワーク アダプタをサポートしています。
- サポートされている Windows Server のバージョンについては、「互換性一覧」を参照してください。

  Hyper-V Server はネイティブの GUI を搭載していないため、すべての構成は PowerShell で行います。しかし、リモート マシン上で実行されている Hyper-V Manager を使用してファイアウォールを管理することができます。Hyper-V ロールのアドオンを使用する場合は、Hyper-V Manager あるいは PowerShell を使ってファイアウォールを管理できます。
- VM-Series ファイアウォールは SR-IOV/PCI パススルーをサポートします。

  DPDK は、Nvidia/Mellanox（Mlx5）SRIOV デバイスでのみサポートされます。SR-IOV を使用するトランクモードはサポートされていません。

©2023 Palo Alto Networks, Inc.

Linux 統合サービス

Linux統合サービス（LIS）は、Hyper-V上のLinuxベースの仮想マシンのパフォーマンスを向上する、ドライバとサービスのパッケージです。VM-Seriesファイアウォールは、ホストと仮想マシン間の統合を改善するために、次のサービスをサポートしています:

- **Graceful Shutdown**（グレースフル シャットダウン） – ゲストにログインすることなく、Hyper-V の管理インターフェイスから VM-Series ファイアウォールのグレースフル シャットダウンを実行できます。
- **Heartbeat to Hyper-V Manager**（**Hyper-V Manager** へのハートビート） – ゲスト VM の稼働状態について、Hyper-V の管理インターフェイスからハートビート モニタリングを行えます。
- **Firewall Management IP Address Visibility**（ファイアウォール管理 **IP** アドレスの可視性） – Hyper-V Manager を使用し、ファイアウォールの管理インターフェイスに割り当てられた IP アドレスを確認できます。

©2023 Palo Alto Networks, Inc.

Hyper-V 上での VM-Series ファイアウォールのインストール

このセクションに記載されている手順に従い、VM-Seriesファイアウォールを Hyper-V ホストにデプロイしてください。VHDX イメージファイルをダウンロードし、VM-Series を Hyper-V ホストにインストールするには、Palo Alto Networks のサポートアカウントおよび有効な VM-Series のライセンスが必要になります。サポート アカウントを使用して、受注完了電子メールで受け取ったキャパシティ認証コードをまだ登録していない場合は、「VM-Series ファイアウォールの登録」を参照してください。登録が完了したら、以下のタスクに進みます。

- 開始する前に
- Hyper-V 上での VM-Series ファイアウォールのパフォーマンス調整
- Hyper-V Manager を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング
- PowerShell を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング
- VM-Series ファイアウォールの初期設定

開始する前に

VM-Series ファイアウォールをインストールして設定する前に、VM-Series ファイアウォールの設定時に必要となる以下の項目について覚えておきましょう。

- 仮想スイッチのタイプ
- MAC アドレスの偽装

仮想スイッチのタイプ

VM-Series をインストールする前に、管理アクセス時に外部に接続する際や、ファイアウォールが保護する仮想マシンを出入りするトラフィックをルーティングする際に必要となる vSwitch を作成しておく必要があります。Hyper-V では 3 つのタイプの vSwitch を作成できます。

- **External vSwitch**（外部 **vSwitch**） – 物理的ネットワークアダプタに連結し、vSwitch が物理ネットワークにアクセスできるようにします。
- **Internal vSwitch**（内部 **vSwitch**） – 仮想マシンおよび Hyper-V ホスト間でトラフィックを通過させます。このタイプの vSwitch は、物理ネットワークに接続できません。
- **Private vSwitch**（プライベート **vSwitch**） – 仮想マシンおよび Hyper-V ホスト間でトラフィックを通過させます。

VM-Series ファイアウォールを管理する際は外部 vSwitch が必要になります。VM-Series ファイアウォールに接続する他の vSwitch については、ネットワーク トポロジーに合わせて任意のタイプのものを使用できます。

MAC アドレスの偽装

レイヤー 3 モードを有効にしたインターフェイスを持つ VM-Series ファイアウォールをデプロイしている場合、ハイパーバイザによって割り当てられた MAC アドレスの使用を有効にし、

©2023 Palo Alto Networks, Inc.

ハイパーバイザおよびファイアウォールが適切にパケットを扱えるようにしてください。または、Hyper-V Manager を使用し、ファイアウォールの各データプレーン インターフェイス用の仮想ネットワーク アダプタにおける MAC アドレスの偽装を有効化します。詳細は、「ハイパーバイザーによって割り当てられた MAC アドレス」を参照してください。

レイヤー 2 モードあるいはバーチャル ワイヤ モードを有効にしたインターフェイスを持つ VM-Series ファイアウォールをデプロイしている場合、ファイアウォールの各データプレーン インターフェイス用の Hyper-V にある仮想ネットワーク アダプタでの MAC アドレスの偽装を有効化します。この設定は、ソース MAC アドレスが外向きのインターフェイスの MAC アドレスと一致しない場合に、VM-Series によって送信されたパケットを仮想ネットワーク アダプタがドロップしないようにするために必要になります。

Hyper-V 上での VM-Series ファイアウォールのパフォーマンス調整

Hyper-V 用の VM-Series ファイアウォールは、高パフォーマンスのアプライアンスですが、最良の結果を得るには、ハイパーバイザの調整が必要な場合があります。このセクションでは、VM-Series ファイアウォールが最高のパフォーマンスを発揮するためのベスト プラクティスと推奨事項について説明します。

- 仮想マシン キューの無効化
- NUMA ノードへの CPU リソースの分離

仮想マシン キューの無効化

Palo Alto Networks では、Hyper-V ホストのすべての NIC の仮想マシン キュー（VMQ）を無効にすることをお勧めします。このオプションは設定ミスの原因になりやすく、有効にするとネットワークのパフォーマンスが低下するおそれがあります。

STEP 1 | Hyper-V Manager にログインして仮想マシンを選択します。

STEP 2 | **Settings**（設定） > **Hardware**（ハードウェア） > **Network Adapter**（ネットワーク アダプタ） > **Hardware Acceleration**（ハードウェア アクセラレーション）を選択します。

STEP 3 | 仮想マシン キューで、**Enable virtual machine queue**（仮想マシン キューの有効化）のチェックを外します。

STEP 4 | **Apply**（適用）をクリックして変更内容を保存し、**OK** をクリックして仮想マシン設定を終了します。

NUMA ノードへの CPU リソースの分離

ゲスト VM の CPU リソースを、単一の不均一メモリアクセス（NUMA）ノードに隔離することで、VM-Series for Hyper-V のパフォーマンスを向上させることができます。VM の NUMA 設定を確認するには、Hyper-V Manager で **Settings**（設定） > **Hardware**（ハードウェア） > **Processor**（プロセッサ） > **NUMA** を選択します。

©2023 Palo Alto Networks, Inc.

Hyper-V Manager を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング

Hyper-V Manager を使用して Hyper-V 上に VM-Series ファイアウォールをデプロイするには、以下の手順を実行します。

STEP 1 | VHDX ファイルをダウンロードします。

VM-Series ファイアウォールを登録し、VHDX ファイルを取得します。

1. https://www.paloaltonetworks.com/services/support にアクセスします。
2. **PAN-OS for VM-Series Base Images** で絞り込みを行い、VHDX ファイルをダウンロードします。例：PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 必要な vSwitch をすべてセットアップします。

vSwitch を作成するには：

1. Hyper-V Manager でホストを選択し、**Action**（アクション） > **Virtual Switch Manager**（仮想スイッチ マネージャー）の順に選択して仮想スイッチ マネージャーのウィンドウを開きます。
2. **Create virtual switch**（仮想スイッチの作成）で vSwitch のタイプ（外部、内部、あるいはプライベート）を選択し、**Create Virtual Switch**（仮想スイッチの作成）をクリックして作成します。

©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォールをインストールします。

1. Hyper-V Manager でホストを選択し、**Action**（アクション） > **New**（新規） > **Virtual Machine**（仮想マシン）を選択します。新規仮想マシン ウィザードで次の設定を行います。
   1. VM-Series ファイアウォールの **Name**（名前）および**Location**（ロケーション）を選択します。VM-Series ファイアウォールは指定されたロケーションに VHDX ファイルを保存します。
   2. **Generation 1**（第一世代）を選択します。これがデフォルトのオプションであり、唯一サポートされているバージョンです。
   3. **Startup Memory**（スタートアップ メモリ）には、VM-Series モデルの VM-Series システム要件に基づいて、メモリを割り当てます。

      動的メモリは有効化しないでください。*VM-Series* ファイアウォールには静的なメモリ割り当てが必要です。

   4. **Networking**（ネットワーキング）を構成します。ファイアウォールの管理インターフェイスに接続する外部 vSwitch を選択します。
   5. **Virtual Hard Disk**（仮想ハードディスク）に接続するには、**Use an existing virtual hard disk**（既存の仮想ハードディスクを使用）を選択し、ダウンロード済みの VHDX ファイルを参照します。
   6. サマリーを確認し、**Finish**（完了）をクリックします。
2. 仮想 CPU をファイアウォールに割り当てます。
   1. 作成した VM を選択し、**Action**（アクション） > **Settings**（設定）に移動します。
   2. **Processor**（プロセッサ）を選択し、VM-Series モデルの VM-Series システム要件に基づいて、最小数の CPU を入力します。
   3. **OK**をクリックします。

STEP 4 | ファイアウォールのデータプレーン インターフェイス用ネットワーク アダプタに少なくとも 1 つ接続します。

1. **Settings**（設定） > **Hardware**（ハードウェア） > **Add Hardware**（ハードウェア追加）を選択し、ネットワーク アダプタの **Hardware type**（ハードウェア タイプ）を選択します。

   レガシー ネットワーク アダプタおよび *SR-IOV* はサポートされていません。選択した場合、*VM-Series* ファイアウォールがメンテナンス モードで起動します。

2. **OK** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 5 | （任意）ハイパーバイザが割り当てた MAC アドレスでレイヤー 3 を使用していない場合、Hyper-V 上の MAC アドレスの偽装を有効化します。

1. データプレーンの仮想ネットワーク アダプタをダブルクリックし、**Advanced Settings**（詳細設定）をクリックします。
2. **Enable MAC address spoofing**（**MAC** アドレスの偽装を有効化）チェックボックスをクリックし、**Apply**（適用）をクリックします。

STEP 6 | ファイアウォールをパワーオンします。

Virtual Machines（仮想マシン）のリストからファイアウォールを選択し、**Action**（アクション） > **Start**（開始）に移動してファイアウォールをパワー オンします。

PowerShell を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング

PowerShell を使用して Hyper-V 上に VM-Series ファイアウォールをデプロイするには、以下の手順を実行します。

STEP 1 | VHDX ファイルをダウンロードします。

VM-Series ファイアウォールを登録し、VHDX ファイルを取得します。

1. https://www.paloaltonetworks.com/services/support にアクセスします。
2. **PAN-OS for VM-Series Base Images** で絞り込みを行い、VHDX ファイルをダウンロードします。例：PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 必要な vSwitch をすべてセットアップします。

以下のコマンドを実行して vSwitch を作成します。vSwitch に名前を付け、スイッチのタイプを選択します。

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | VM-Series ファイアウォールをインストールします。

1. 新しい仮想マシンを作成し、VM-Series モデルの VM-Series システム要件に基づいて、メモリを設定します。

```
> NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -VHDPath
 <file-path-to-vhdx>
```

2. VM-Series モデルの VM-Series システム要件に基づいて、プロセッサ数を設定します。

```
> SET-VMProcessor –VMName <vm-name> –Count 2
```

 ©2023 Palo Alto Networks, Inc.

STEP 4 | ファイアウォールの管理インターフェイス用ネットワーク アダプタに少なくとも 1 つ接続します。

VM の作成時に生成されたデフォルトのネットワーク アダプタを管理 vSwitch に接続します。

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-
adapter-name"> -SwitchName <"management-vswitch">
```

STEP 5 | （任意）ハイパーバイザが割り当てた MAC アドレスでレイヤー 3 を使用していない場合、Hyper-V 上の MAC アドレスの偽装を有効化します。

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-
name"> -MacAddressSpoofing On
```

STEP 6 | ファイアウォールをパワーオンします。

以下に例を示します。

```
> Start-VM -vmname <vm-name>
```

VM-Series ファイアウォールの初期設定

VM-Series ファイアウォールの初期設定を行う方法を説明します。デフォルトでは、VM-Series ファイアウォールは、DHCP を使用して、管理インターフェイスの IP アドレスを取得します。ただし、スタティック IP アドレスを割り当てることも可能です。初期設定が完了したら、Web インターフェイスにアクセスし、詳細な設定タスクを実行します。中央管理のために Panorama を使用している場合、Panorama を使用したデバイス管理の詳細は、『Panorama 管理者ガイド』を参照してください。

ブートストラップを使用して Hyper-V 上の VM-Series ファイアウォールを設定する場合は、「Hyper-V における VM-Series ファイアウォールのブートストラップ」を参照してください。ブートストラップの一般的な情報については、「VM-Series ファイアウォールのブートストラップ」を参照してください。

STEP 1 | ネットワーク管理者から必要な情報を入手します。

- 管理ポート IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS サーバーの IP アドレス

©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series ファイアウォールのコンソールにアクセスします。

1. Hyper-V Manager で VM-Series ファイアウォールを選択し、Actions（アクション）リストの**Connect**（接続）をクリックします。
2. デフォルトのユーザー名およびパスワード、**admin/admin**でファイアウォールにログインします。
3. **configure**コマンドを入力して設定モードに切り替えます。

STEP 3 | 管理インターフェイスへのネットワーク アクセス設定を行います。

以下のコマンドを入力します。

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> netmask <netmask>
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

<Firewall-IP> は管理インターフェイスに割り当てる IP アドレス、 *<netmask>* はサブネットマスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレスです。

STEP 4 | 変更をコミットし、設定モードを終了します。

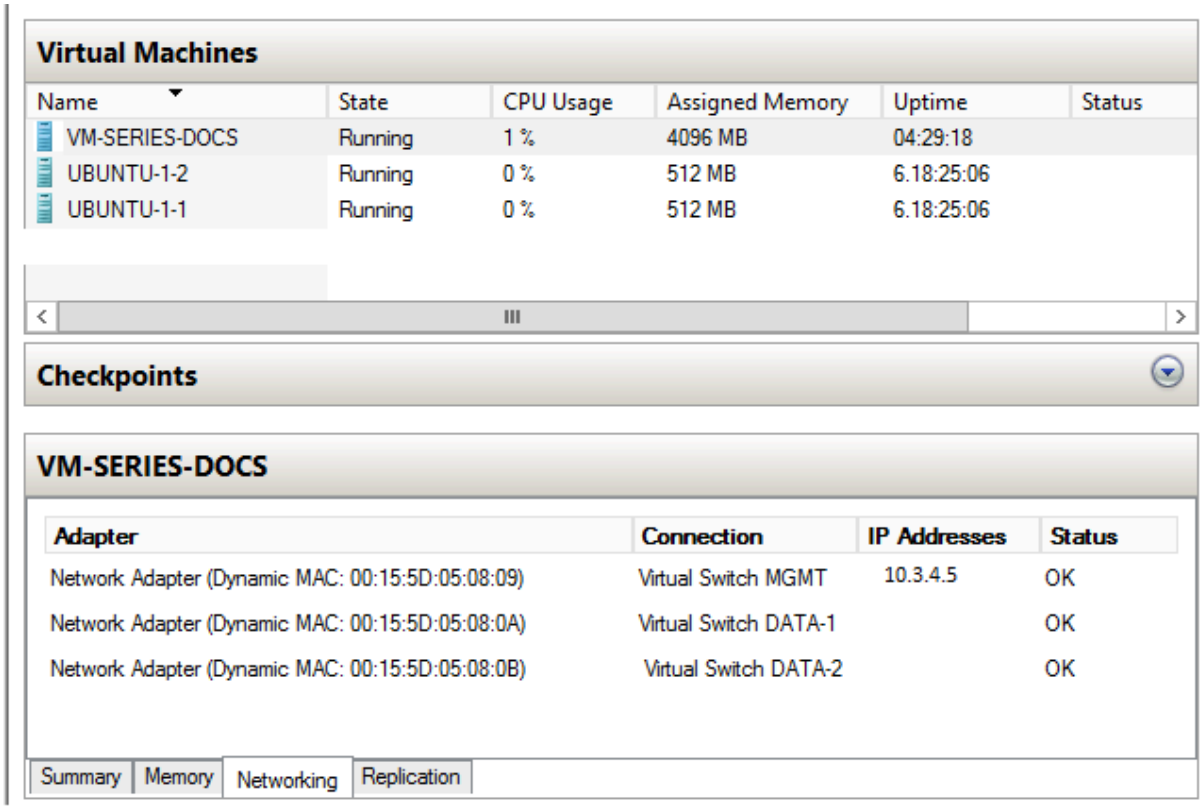
1. 「**commit**」と入力します。
2. 「**exit**」と入力します。

STEP 5 | Hyper-V Manager で管理インターフェイスの IP アドレスを表示できることを確認します。

1. **Virtual Machines**（仮想マシン）のリストで VM-Series ファイアウォールを選択します。
2. **Networking**（ネットワーキング）を選択します。リストの最初に表示されるネットワーク アダプタは、ファイアウォールへの管理アクセスに使用します。リストにある

©2023 Palo Alto Networks, Inc.

他のアダプタはファイアウォールのデータプレーン インターフェイスとして使用されます。



STEP 6 | Palo Alto Networks 更新サーバーなど、ファイアウォール管理に必要な外部サービスへのネットワーク アクセスを確認します。

1. 以下の例に示すように、ping ユーティリティを使用して Palo Alto Networks 更新サーバーへのネットワーク接続を検証します。DNS が解決され、レスポンスに更新サーバーの IP アドレスが含まれていることを確認します。更新サーバーは ping リクエストには応答しません。

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes
 of data.
From 192.168.1.1 icmp_seq=1 Destination Host Unreachable
From 192.168.1.1 icmp_seq=2 Destination Host Unreachable
From 192.168.1.1 icmp_seq=3 Destination Host Unreachable
From 192.168.1.1 icmp_seq=4 Destination Host Unreachable
```

DNS の解決を確認したら、*Ctrl+C* キーを押して *ping* リクエストを停止します。

©2023 Palo Alto Networks, Inc.

2. 以下の CLI コマンドを実行して、Palo Alto Networks 更新サーバーからファイアウォールのサポート資格に関する情報を取得します。

```
request support
check
```

接続されている場合、更新サーバーはファイアウォールのサポート ステータスを伴うレスポンスを返します。

STEP 7 | （任意）VM-Series のジャンボ フレーム構成が Hyper-V でサポートされている最大 MTU を超えていないことを確認します。

ジャンボフレームが有効な場合、VM-Series はデフォルトで 9216 バイトの MTU を持ちます。しかし、Hyper-V ホストの物理ネットワーク アダプタでサポートされている最大 MTU サイズは、ネットワーク アダプタの能力に応じて 9000 あるいは 9014 になります。構成した MTU を Hyper-V で確認するには：

1. Windows Server 2012 R2 で **Control Panel**（コントロール パネル）を開き、**Network and Internet**（ネットワークとインターネット） > **Network and Sharing Center**（ネットワークと共有センター） > **View network status and tasks**（ネットワーク状態とタスクを表示）を開きます。
2. リストでネットワーク アダプタあるいは仮想スイッチをクリックします。
3. **Properties**（プロパティ）をクリックします。
4. **Configure**（設定）をクリックします。
5. Advanced（詳細）タブのリストから**Jumbo Packet**（ジャンボ パケット）を選択します。
6. Value（値）のドロップダウン メニューで 9000 あるいは 9014 を選択します。
7. **OK**をクリックします。

Hyper-V のジャンボ フレームを有効化した場合、VM-Series ファイアウォールでジャンボ フレームを有効化し、Hyper-V ホストで設定されている値と同じになるように MTU サイズを設定してください。

STEP 8 | VM-Series ファイアウォールの Web インターフェイスにアクセスして、インターフェイスを設定し、セキュリティ ルールと NAT ルールを定義して、保護する必要のあるアプリケーションを安全に有効化します。

『PAN-OS 管理者ガイド』を参照してください。

©2023 Palo Alto Networks, Inc.

Azure での VM-Series ファイアウォールのセットアップ

Azure で VM-Series ファイアウォールを使用すると、Azure マーケットプレイス内の仮想マシンとして、Palo Alto Networks の次世代ファイアウォールのセキュリティ機能が利用できるようになります。VM-Series ファイアウォールは仮想マシンのワークロードおよびデータを確実に保護するセキュリティ機能の一式を提供します。ファイアウォールによって実現できる機能は、セキュリティグループ、Web アプリケーション ファイアウォール、ネイティブのポートベースのファイアウォールのようなネイティブのセキュリティ機能とは異なります。

Azure では、VM-Series ファイアウォールは BYOL（bring your own license：ライセンス持ち込み）モデルあるいは時間ベースの PAYG（pay-as-you-go：都度払い）モデルで利用できます。Microsoft Azure により、ファイアウォールをデプロイしてクラウド上の仮想ネットワーク内のワークロードを保護できるようになるため、公開クラウド ソリューションをデプロイしたり、業務 IT インフラを拡張してハイブリッド ソリューションを作成することが可能になります。

- Azure における VM-Series ファイアウォールについて
- Azure でサポートされるデプロイメント
- Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）
- Azure China マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）
- AzureでのPanoramaが統制するデプロイメント
- Azure用のカスタムVM-Seriesイメージの作成
- Azure Security Center の推奨事項を使用してワークロードを保護
- Azure Stack 上に VM-Series ファイアウォールをデプロイ
- VM-Series ファイアウォールでの Azure Application Insights の有効化
- Azure 上の VM 監視
- Azure でのアクティブ/パッシブ HA のセットアップ
- ARM テンプレートを使用した VM-Series ファイアウォールのデプロイ
- VM-Series and Azure Application Gateway テンプレートのデプロイ
- Azure での Kubernetes サービスの保護

Azure における VM-Series ファイアウォールについて

Azure における VM-Series ファイアウォールは、リソースマネージャーのデプロイモードを使用して仮想ネットワーク（VNet）内にデプロイしなければなりません。VM-Series ファイアウォールは、標準の Azure パブリック クラウド、Azure China、Azure Government（DoD Impact Level 5 データのセキュリティ要件および FedRAMP High 標準に準拠する Azure Government の DoD を含む）にデプロイできます。

マーケットプレイスの Azure パブリック クラウド、Azure Government、および Azure DoD リージョン向け VM-Series ファイアウォールは、BYOL（Bring Your Own License: ライセンス持ち込み）モデルあるいは時間ベースの PAYG（Pay-As-You-Go: 従量課金）オプションの両方に対応しています。ライセンスの詳細については、「VM-Series ファイアウォールのライセンス タイプ」を参照してください。また、VM-Series ファイアウォールをデプロイできるサポートされている Azure リージョンのリストを参照してください。

Azure China の場合、VM-Series ファイアウォールは BYOL オプションのみをサポートします。作業の流れについては、Azure China マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）を参照してください。

また、Azure Stack（組織のデータセンター内で Azure サービスを利用できるようにする Microsoft 社のプライベート クラウド）上で VM-Series ファイアウォールをデプロイすることもできます。Azure Stack を使用すれば、ハイブリッド クラウド ソリューションを構築し、パブリックな Azure デプロイ環境をオンプレミスの Azure Stack セットアップ環境と統合できます。VM-Series ファイアウォール BYOL は Azure Marketplace からダウンロードし、Azure Stack 上のテナントで利用できるようにすることが可能です。方法については、「Azure Stack 上で VM-Series ファイアウォールをデプロイする」を参照してください。

- Azure ネットワークと VM-Series ファイアウォール
- Azure セキュリティ センターの統合
- Azure における VM-Series ファイアウォールのテンプレート
- Azure における VM-Series の最小システム要件
- Azure における VM-Series の高可用性のサポート

Azure ネットワークと VM-Series ファイアウォール

AzureのVNetインフラは、仮想マシンがなくても各サブネットにネットワークインターフェイスを与えることができます。このアーキテクチャにはVNet内のすべての仮想マシンに直接接続する内部ルートテーブル（システムルートと呼ばれる）が含まれているため、サブネット内のトラフィックは自動的に仮想マシンに送られます。VNet外の宛先IPアドレスについては、トラフィックは設定に応じてデフォルトの内部ゲートウェイあるいはVPNゲートウェイに送られます。VM-Seriesファイアウォールを通してトラフィックをルーティングするには、サブネットを離れるトラフィック用のネクストホップを指定するユーザー定義のルート（UDR）を作成する必要があります。このルートは、他のサブネット宛てのトラフィックがシステムルートを使用して他のサブネット内の仮想マシンに直接アクセスするのではなく、VM-Series ファイアウォールに向かうよう強制します。たとえば、ウェブ層およびデータベース層がある 2 層式アプリケーションでは、トラフィックがウェブサブネットから VM-Series ファイアウォールを経由して、DB サブネットに向かうように UDR をセットアップします。

©2023 Palo Alto Networks, Inc.

Azure では、*UDR* はサブネットを離れるトラフィックに対してのみ使用できます。トラフィックがインターネットからサブネットに入ってくる方法を指定したり、トラフィックをサブネット内で仮想マシンへとルーティングするユーザー定義のルートを作成することはできません。*UDR* を使用すると、アウトバウンド トラフィックを *VM-Series* ファイアウォールのインターフェイスに向けることができ、ファイアウォールが常にインターネットへのトラフィックを確実に確保できるようになります。

Microsoft Azure の詳細についてはhttps://azure.microsoft.com/en-us/documentation/をご覧ください。

Azure マーケットプレイスで利用できる VM-Series ファイアウォールをデプロイするためのソリューション テンプレートにはネットワークインターフェイスが 3 つあります。Azure でのアクティブ/パッシブ HA のセットアップには、HA2 リンクのインターフェイスを追加する必要があります。テンプレートをカスタマイズするには、GitHub リポジトリで利用できる ARM テンプレートを使用します。

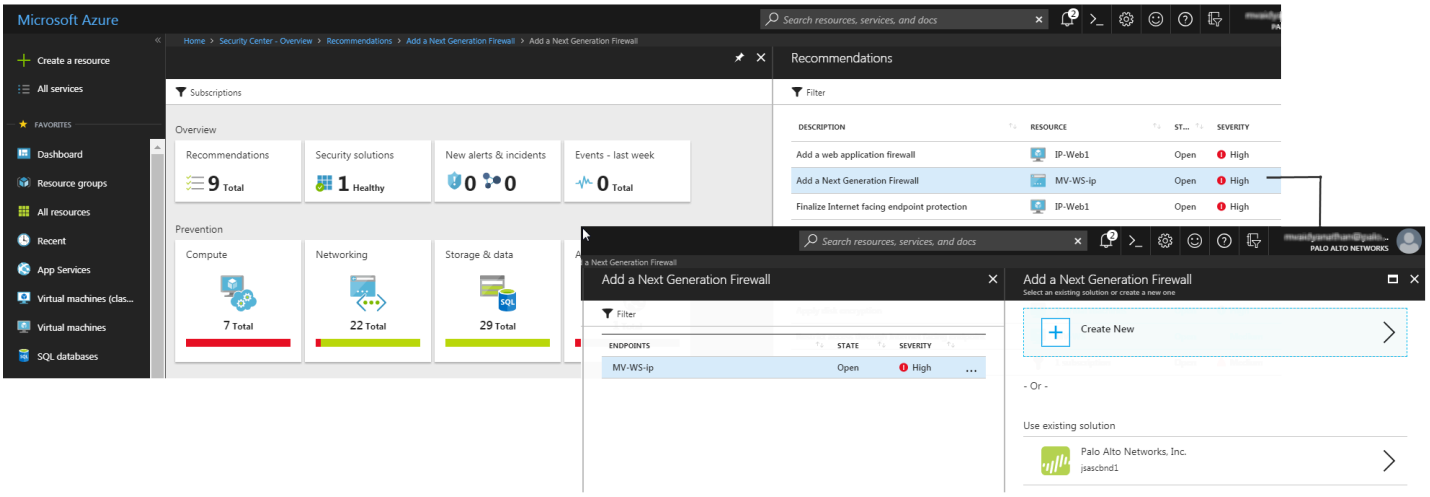
Azure セキュリティ センターの統合

Microsoft は、パートナー セキュリティ ソリューション用の Azure Security Center サポートを廃止して、それに代わる Azure Sentinel を提供しました。

VM-Series ファイアウォールは Azure Security Center と統合されており、Azure のワークロードのセキュリティの状況を監視し警告する統一されたビューを提供します。Azure Security Center では、Azure ワークロードを脅威から守り、パブリック クラウドでビジネスと知的財産を保護する際のギャップを緩和するパートナー セキュリティ ソリューションとして、VM-Series ファイアウォールを利用できます。この統合を有効にし、ログをセキュリティ アラートとして Azure Security Center ダッシュボードに直接表示するために、Azure の VM-Series ファイアウォールはログ転送プロファイルを含みます。

はじめに、ご利用の Azure サブスクリプションで Azure Security Center を有効にする必要があります。この統合を有効にする方法は 2 通りあります。

- **Azure Security Center** のダッシュボードの推奨事項に基づいて **VM-Series** ファイアウォールをデプロイします。



©2023 Palo Alto Networks, Inc.

Azure Security Center のダッシュボードが、インターネットにさらされているワークロードを保護するために VM-Series ファイアウォールをデプロイするよう推奨している場合、ファイアウォールを新しいリソースグループあるいは既存の空のリソースグループにのみデプロイできます。これは現在、既存のリソースグループ内に複数の NIC アプライアンスをデプロイすることを Azure が制限しているためです。そのため、VM-Series ファイアウォールをデプロイした後、保護する必要があるトラフィックのパスに含まれるよう、手作業で設定を行う必要があります。

Azure Security Center からファイアウォールを導入すると、ファイアウォールは、管理、外部フェイス（内部）（内部）、内部フェーシング（Trust）の 3 つのネットワーク インターフェイスと、Trust サブネットからすべての発信トラフィックを送信するユーザー定義ルート（UDR）ファイアウォールの Trust インターフェイスに渡すことで、インターネットに接続されたトラフィックが常にファイアウォールによって検査されるようにします。デフォルト設定には、セキュリティ ポリシー ルールの 2 つの例が含まれています。 アウトバウンド デフォルトルールでは、アプリケーションのデフォルト ポート上の Trust ゾーンから Untrust ゾーンへのすべてのトラフィックが許可され、インバウンド デフォルトルールでは、デフォルトのアンチウイルス、アンチスパイウェア、および脆弱性保護のセキュリティ プロファイルを使用してトラフィックを検査した後、すべての Untrust ゾーンから Trust ゾーンへの Web ブラウジング トラフィックが有効になります。また、ファイアウォールは、インバウンド ルールまたはアウトバウンド ルールで傍受されたすべてのファイルを、分析するために WildFire パブリック クラウドに転送します。両ルールには、著作権侵害、ダイナミック DNS、エクストリミズム、マルウェア、フィッシング、および未知の URL カテゴリへのすべてのトラフィックをブロックする URL フィルタリング プロファイルが含まれます。これらのセキュリティ プロファイルに加えて、セキュリティ ポリシー ルールは両方ともセッション終了時にログに記録され、セキュリティ通知として脅威ログおよび WildFire への送信ログを Azure Security Center ダッシュボードに転送することができます。

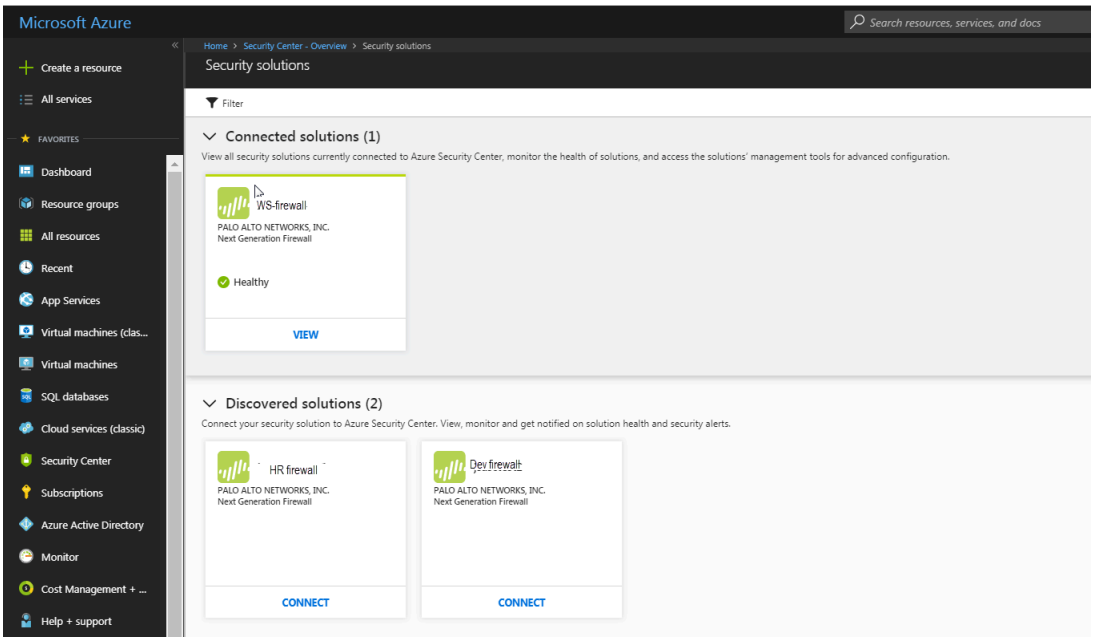
この統合を実際に使用し、保護するワークロードとして同じリソースグループ内でAzure Security Center の推奨事項に基づいて VM-Series ファイアウォールをデプロイを行うために、インターネットにさらされているパブリック IP アドレスを持つワークロードを準備することができます。Azure Security Center はセキュリティリスクを検出すると、次世代ファイアウォールをデプロイすることを推奨します。その後、後でワークロードを追加できる新しいリソースグループ内で VM-Series ファイアウォールをデプロイできるようになります。推奨事項を出すために準備したワークロードをその後で削除する必要があります。

- ワークロードを保護するためにすでにデプロイしている **VM-Series** ファイアウォールを選択します。Azure Security Center の Standard サービス階層を持っている場合、Azure CLI、PowerShell、あるいは ARM テンプレートでカスタマイズされたデプロイを使用して、あるいは Azure Marketplace からデプロイしたすべての既存の VM-Series ファイアウォールを検出・表示します。Azure サブスクリプション内のファイアウォールは、Azure Security

©2023 Palo Alto Networks, Inc.

Center のダッシュボード上の Security Solutions（セキュリティ ソリューション）のところでグループ化されます。

Microsoft Azure の Free サービス階層サブスクリプションは、既存のファイアウォールの検出をサポートしていません。



Azure Security Center から既存の VM-Series ファイアウォールを接続を行うには、Linux 仮想マシンをセットアップして Syslog 転送を設定し、ファイアウォール ログを Common Event Format のアラートとして Azure Security Center に転送する必要があります。追加の設定を行うことで、すべての Azure アセットを監視できる単一のガラス ビューのペインを有効化できます。

大量のログを *Azure Security Center* に転送すると、追加のサブスクリプション コストが発生する可能性があります。

Azure における VM-Series ファイアウォールのテンプレート

Azure ではテンプレートを使用して VM-Series ファイアウォールをデプロイできます。Palo Alto Networks は、ソリューション テンプレートと ARM テンプレートという 2 種類のテンプレートを提供しています。

- **Solution Templates in the Azure Marketplace（Azure** マーケットプレイスにあるソリューション テンプレート） — Azure マーケットプレイスで利用できるソリューション テンプレートを使用すれば、Azure ポータルを使って VM-Series ファイアウォールをデプロイできます。既存のリソース グループおよびストレージ アカウントを使用（あるいは新規作成）し、Azure China を除くすべてのリージョンで、以下のようなデフォルト設定の VM-Series ファイアウォールをデプロイできます。
  - VNet CIDR 10.8.0.0/16：CIDRは異なるプライベートIPアドレスの範囲に変えることができます。

©2023 Palo Alto Networks, Inc.

- 3つのサブネット– 10.8.0.0/24（management）、10.8.1.0/24（untrust）、10.8.2.0/24（trust）
- 3 つのネットワークインターフェイス。各サブネットにつき 1 つ。VNet CIDRをカスタマイズする場合、変更に合わせてサブネットの範囲がマッピングされます。

ソリューション テンプレートを使用する方法については、「Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）」を参照してください。Azure China については、「Azure China マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）」を参照してください。

- **ARM Templates in the GitHub Repository**（**GitHub** リポジトリにある **ARM** テンプレート）– マーケットプレイス ベースのデプロイに加え、Palo Alto Networks が GitHub リポジトリ内で提供している Azure リソース マネージャーのテンプレートを使用すれば、Azure に VM-Series ファイアウォールをデプロイするプロセスが簡単になります。
  - ARM テンプレートを使用して VM-Series ファイアウォールをデプロイ – 基本的な ARM テンプレートには 2 つの JSON ファイル（Template ファイルおよび Parameters ファイル）が含まれており、単一の操作で VNet 内にすべてのリソースをデプロイし、準備を行えます。これらのテンプレートは、無保証のベスト エフォート サポート ポリシーで提供されます。

    *Palo Alto Networks*が提供しているすべてのイメージファイルを探すために*Azure CLI*を使用する場合、次の情報を使ってコマンド（*show vm-image list*）を実行する必要があります。
    - *Publisher: paloaltonetworks*
    - *Offer: vmseries-flex*
    - *SKU*：*byol*、*bundle1*、*bundle 2*
    - バージョン：*10.0.0*、または最新のバージョン
  - VM-Series and Azure Application Gateway テンプレートをデプロイし、外部と内部の Azure Load Balancer（VM-Series と Azure Application Gateway）のペア間で 2 つの VM-Series ファイアウォールを使用して、インターネットに接続された Web アプリケーションを保護するスケールアウト セキュリティ アーキテクチャをサポートします。このテンプレートは、現在 Azure China では使用できません。
  - ARM テンプレートは、VM-Series ファイアウォールを既存のリソース グループにデプロイするときに使用します。たとえばAzure でのアクティブ/パッシブ HA のセットアップを行う場合などです。

Palo Alto Networks の公式サポート ポリシーでカバー対応する上記の ARM テンプレートに加えて、Palo Alto Networks は Palo Alto Networks の GitHub リポジトリにコミュニティサポートテンプレートを提供しています。これにより、クラウドの自動化および Azure のスケールをスムーズに行うことができます。

©2023 Palo Alto Networks, Inc.

Azure における VM-Series の最小システム要件

VM-Series ファイアウォールは Azure リソース マネージャー（ARM）モードでデプロイしなければなりません。クラシック モード（サービス管理ベースのデプロイ）はサポートされていません。Azure における VM-Series ファイアウォールは次の要件を満たしていなければなりません。

- 次のタイプの Azure Linux VM - サポートされているモデル。

  上記のタイプには、Accelerated Networking（SR-IOV）のサポートが含まれています。
- VM-Series ファイアウォールのデプロイに必要なメモリ、ディスク、および CPU コアについては、「VM-Series システム要件」を参照してください。

  ロギング用に 40 GB から 8TB のディスク領域を追加できます。VM-Series ファイアウォールは、使用可能な場合には Azure マネージド ディスクを使用します。一部のインスタンス タイプでは、Azure が提供する一時ディスクを使用しません。
- 最大 8 つのネットワーク インターフェイス（NIC）。管理アクセス用に 1 つのプライマリ インターフェイス、データ トラフィック用に最大 7 つのインターフェイスが必要です。

  各サブネットについて仮想マシンがネットワーク インターフェイスを必要としないため、Azure ではネットワーク インターフェイス 3 つ（1 つは管理トラフィック用、2 つはデータプレーン トラフィック用）だけで VM-Series ファイアウォールをセットアップできます。ファイアウォール上でゾーンベースのポリシー ルールを作成するには、1 つのデータプレーン インターフェイスを ***trust*** ゾーンに、もう 1 つを ***untrust*** ゾーンに割り当てられるよう、データプレーン インターフェイスが 2 つ以上必要になります。HA デプロイメントでは、HA ピア間の HA2 リンク用に別のインターフェイスが必要です。

  Azure VNet はレイヤー 3 のネットワークであるため、Azure における VM-Series ファイアウォールはレイヤー 3 インターフェイスのみをサポートしています。

Azure における VM-Series の高可用性のサポート

可用性を確保するため、セッション同期が設定されている従来の構成でAzure でのアクティブ/パッシブ HA のセットアップを行うか、または Azure Application Gateway や Azure Load Balancer などのクラウドネイティブのロード バランサーを使用するスケール アウト アーキテクチャを使用して、ファイアウォールの安全なインスタンス全体にトラフィックを分散します。詳細は、「VM-Series と Azure Application Gateway テンプレートのデプロイ」を参照してください。

Azure 上の VM-Series のサービス プリンシパル アクセス許可

PanoramaがAzure APIと通信してワークロードの情報を収集できるようにするには、Azureアクティブディレクトリアプリケーション、およびAzure ADで認証を受け、サブスクリプション内のリソースにアクセスするために必要なアクセス許可を持つサービスプリンシパルを作成する必要があります。

Active Directory アプリケーションとサービスプリンシパルを作成するには、ポータルを使用して、リソースにアクセスできる Azure AD アプリケーションとサービスプリンシパルを作成する方法に示された手順に従ってください。アプリケーションの生成プロセスには、「アプリケー

©2023 Palo Alto Networks, Inc.

ションをロールに割り当てる」およびIAMロール「reader」をアプリケーションに割り当てるステップが存在しています。

ADアプリケーションを作成、登録するために必要な権限を持っていない場合は、Azure ADあるいはサブスクリプションの管理者にサービスプリンシパルの作成を依頼してください。

アプリケーションを登録後、これらの値を記録してください。後ほどPanorama plugin for Azureで使用します。

- アプリケーションID
- 秘密鍵（秘密鍵の作成時に記録してください。ページから移動すると、秘密鍵は参照できなくなります）。
- テナントID

許可

次の表には、最低限必要なビルトインロール、およびロールをカスタマイズする場合のきめ細かいアクセス許可について記載しています。

目的	許可
Azure High Availability（高可用性）	「Azure でのアクティブ/パッシブ HA のセットアップ」を参照してください。
Azure Application Insights VM-Series ファイアウォールでの Azure Application Insights の有効化	**“Microsoft.Authorization/*/read”,** **“Microsoft.Network/networkInterfaces/*”,** **“Microsoft.Network/networkSecurityGroups/*”,** **“Microsoft.Network/virtualNetworks/*”,** **“Microsoft.Compute/virtualMachines/read”**
Azure Monitoring（Azureモニタリング） Panorama上のモニタリング用Azureプラグインのセットアップ	サービスプリンシパル用に最低でも「閲覧者」のロールが必要です。代わりに、次のカスタム要件を追加することができます: **“Microsoft.Compute/virtualMachines/read”,** **“Microsoft.Network/networkInterfaces/read”,** **“Microsoft.Network/virtualNetworks/read”,** **“Microsoft.Network/locations/serviceTags/read”** **"Microsoft.Network/loadBalancers/read",** **"Microsoft.Network/publicIPAddresses/read"** **"Microsoft.Resources/subscriptions/resourcegroups/read",**
Panoramaが統制するデプロイ環境。	**“Microsoft.Resources/subscriptions/resourcegroups/*”,**

©2023 Palo Alto Networks, Inc.

目的	許可
カスタムロールの作成とActive Directoryとの関連付け	**“Microsoft.Resources/deployments/write”,** **“Microsoft.Resources/deployments/operationStatuses/read”,** **“Microsoft.Resources/deployments/read”,** **“Microsoft.Resources/deployments/delete”**
	"Microsoft.Network/publicIPPrefixes/write", **"Microsoft.Network/publicIPPrefixes/read",** **"Microsoft.Network/publicIPPrefixes/delete",** **"Microsoft.Network/publicIPAddresses/write",** **"Microsoft.Network/publicIPAddresses/read",** **"Microsoft.Network/publicIPAddresses/delete",** **"Microsoft.Network/publicIPAddresses/join/action",**
	"Microsoft.Network/natGateways/write", **"Microsoft.Network/natGateways/read",** **"Microsoft.Network/natGateways/delete",** **"Microsoft.Network/natGateways/join/action",**
	"Microsoft.Network/virtualNetworks/read", **"Microsoft.Network/virtualNetworks/write",** **"Microsoft.Network/virtualNetworks/delete",** **"Microsoft.Network/virtualNetworks/subnets/write",** **"Microsoft.Network/virtualNetworks/subnets/read",** **"Microsoft.Network/virtualNetworks/subnets/delete",** **"Microsoft.Network/virtualNetworks/subnets/join/action",**
	"Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read",
	"Microsoft.Network/networkSecurityGroups/write", **"Microsoft.Network/networkSecurityGroups/read",**

©2023 Palo Alto Networks, Inc.

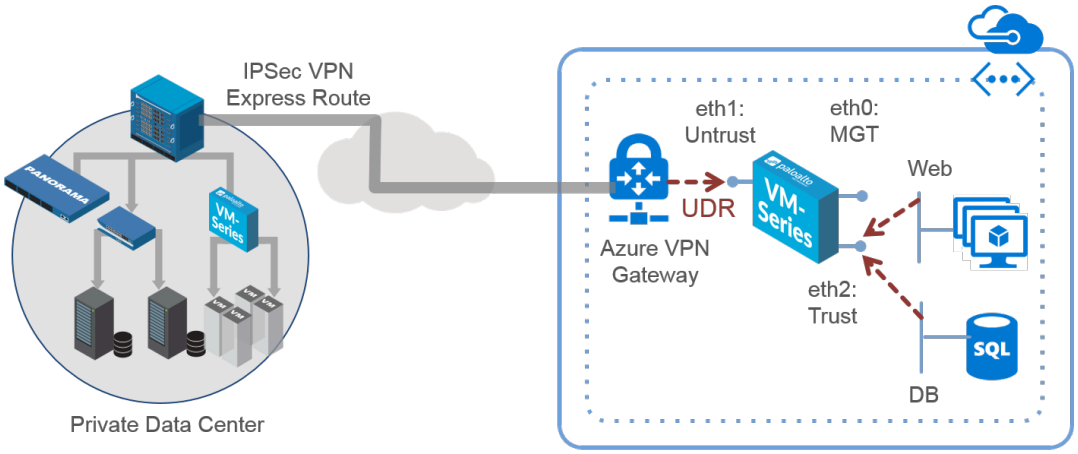
目的	許可
	"Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Network/networkSecurityGroups/join/action",
	"Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/action", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
	"Microsoft.Network/locations/serviceTags/read",
	"Microsoft.Network/applicationGateways/read", "Microsoft.Network/networkInterfaces/read",
	"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Compute/virtualMachineScaleSets/read", "Microsoft.Compute/virtualMachineScaleSets/delete", "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
	"Microsoft.Compute/virtualMachines/read",
	"Microsoft.Compute/images/read",
	"Microsoft.insights/components/write", "Microsoft.insights/components/read", "Microsoft.insights/components/delete",
	"Microsoft.insights/autoscalesettings/write"

©2023 Palo Alto Networks, Inc.

Azure でサポートされるデプロイメント

Azure で VM-Series ファイアウォールを使用し、次のような状況でネットワーク ユーザーを保護します。

- ハイブリッドおよび **VNet** から **VNet** へ – Azure における VM-Series ファイアウォールにより、IPSec および ExpressRoute を使用して安全に物理的データ センター/プライベート クラウドを Azure へと拡張することができます。データ センターをより安全に改善するためには、ネットワークをセグメント化し、ワークロードを個々の VNet に分散すれば、IPSec トンネルおよびアプリケーションを許可するポリシーを使用して、VNet 間のトラフィックの流れを安全に保護することができます。



- **Inter-Subnet**（インターサブネット） – VM-Series ファイアウォールを Vnet 内のサーバー手前に配置することで、複数層から成るアーキテクチャの各アプリケーション間のインターサブネット トラフィックの水平方向の脅威から保護できます。
- **Gateway**（ゲートウェイ） – VM-Series ファイアウォールは Vnet ゲートウェイとして配置することで、Azure 仮想ネットワーク（VNet）内のインターネット接続を利用するデプロイを保護できます。VM-Series ファイアウォールは Vnet 内のサーバーに向かうトラフィックを保護し、さらに複数層から成るアーキテクチャの各アプリケーション間のインターサブネット トラフィックに対して水平方向の脅威から保護します。
- **GlobalProtect** – Azure インフラストラクチャを使用して迅速かつ簡単に VM-Series ファイアウォールを GlobalProtect™ としてデプロイし、ロケーションにかかわらず、ゲートウェイのセキュリティ ポリシーをリモート ユーザーおよびデバイスへと拡張できます。

Azure Marketplace（ソリューションテンプレート）からのVM-Seriesファイアウォールのデプロイ、AzureスタックへのVM-Seriesファイアウォールのデプロイ、またはAzureでのVM-Seriesファイアウォールデプロイ環境の統制を行うことができます。

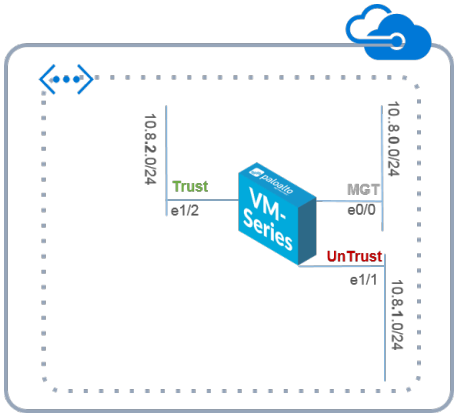
また、ファイアウォールのデプロイに使用できる、Azure上のVM-Seriesファイアウォールテンプレートを確認することもできます。

ブートストラップの情報については、Azure 上の VM-Series ファイアウォールのブートストラップを参照してください。

©2023 Palo Alto Networks, Inc.

Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）

Azure® Marketplace および Azure Government Marketplace で利用できる、VM-Series ファイアウォール用のソリューション テンプレートをデプロイする方法を説明します。GitHub リポジトリで利用できるカスタマイズ可能な Azure Resource Manager (ARM) テンプレートを使用するには、ARM テンプレートを使用して VM-Series ファイアウォールをデプロイ」を参照してください。



STEP 1 | Azure アカウントをセットアップします。

1. Microsoft® アカウントを所有していない場合は作成してください。
2. Microsoft アカウントの認証情報を使用して Azure ポータル**`https://portal.azure.com`**あるい**`https://portal.azure.us`**）にログインします。

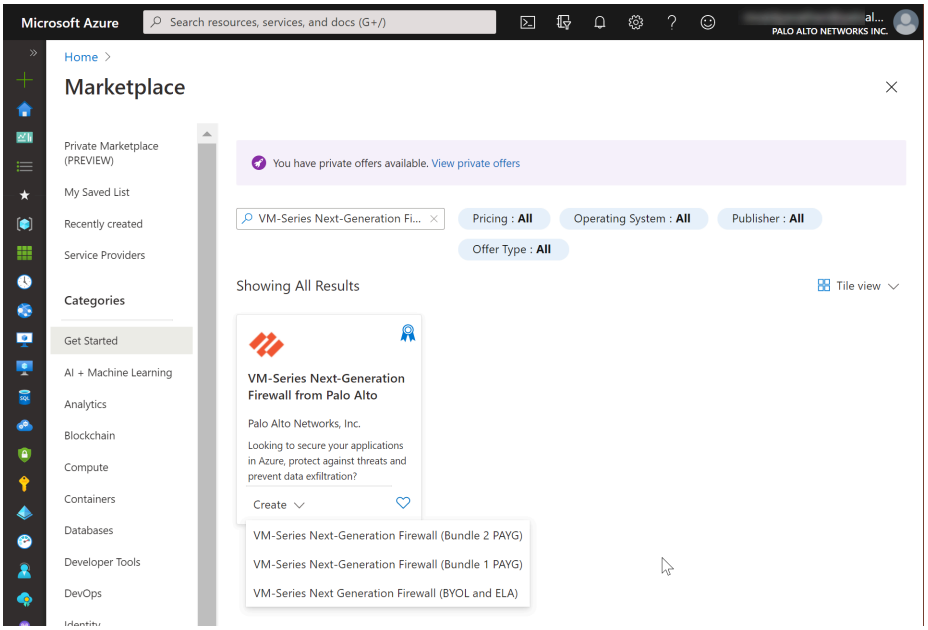
> トライアル版を使用している場合、サポート リクエスト***Help + Support***（ヘルプ + サポート） > ***New Support Request***（新規サポート リクエスト））を開き、割り当てられている仮想マシン コアの量を増やす必要がある場合があります。

STEP 2 | Azure マーケットプレイスで VM-Series のソリューション テンプレートを探します。

1. **Marketplace**（マーケットプレイス） > **Virtual Machines**（仮想マシン）を選択します。
2. Palo AltoNetworks® を検索すると、VM-Series ファイアウォールの製品リストが表示されます。BYOL（bring your own license：ライセンス持ち込み）と PAYG（pay-as-you-

©2023 Palo Alto Networks, Inc.

go：都度払い）モデルの違いについては「パブリック クラウドの VM-Series ファイアウォール ライセンス」を参照してください。



3. オファリングを選択し、新しい VM-Series ファイアウォールを**Create**（作成）します。

©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォールをデプロイします。

1. ファイアウォールの基本設定を行います。

   1. 自分の Azure**Subscription**（サブスクリプション）を選択します。
   2. 新しいリソース グループを作成するか、空の既存のリソース グループを選択します。リソース グループは、このデプロイ用の VM-Series ファイアウォールに関連するすべてのリソースを取り込みます。

      Azure では、複数のネットワーク インターフェイス コントローラ（*NIC*）を有効にするマーケットプレイス ソリューション用に既存のリソース グループを選択するオプションが削除されました。ファイアウォールを既存のリソース グループにデプロイするにはGitHub リポジトリの *ARM* テンプレートを使用するか、独自のカスタム *ARM* テンプレートを使用します。

   3. ファイアウォールをデプロイしようとしているAzurリージョンを選択します。
   4. ファイアウォールの管理者の**Username**（ユーザー名）を入力します。
   5. 認証タイプを選択—Password（パスワード）またはSSH Public Key（SSH公開鍵）。

      *FIPS-CC*操作モードでファイアウォールを使用する場合、*SSH*キー認証を有効にする必要があります。ユーザー名とパスワードを使用して*VM-Series*ファイアウォールをデプロイすることはできますが、操作モードを*FIPS-CC*に変更すると、そのユーザー名とパスワードを使用して認証できなくなります。*FIPS-CC*モード へのリセット後、*SSH* キーを使用してログインする必要があります。その後、ファイアウォール *Web*インターフェースに後でログインするために使用できるユーザー名とパスワードを設定できます。*SSH*キー作成の詳細についてはAzureのドキュメントを参照してください。

   6. ファイアウォールへの管理者アクセスを保護するため**Password**（パスワード）（31 文字まで）を入力するか**SSH public key**（**SSH** 公開鍵）をコピー & ペーストします。

2. ネットワーキングを構成します。

   1. 既存の Azure Virtual Network（VNet）を選択するか新規作成し、VNet の IP アドレス空間を入力します。デフォルトのクラスレス ドメイン間ルーティング（CIDR）IP アドレスは 10.8.0.0/16 です。
   2. ネットワーク インターフェイスのサブネットを設定します。

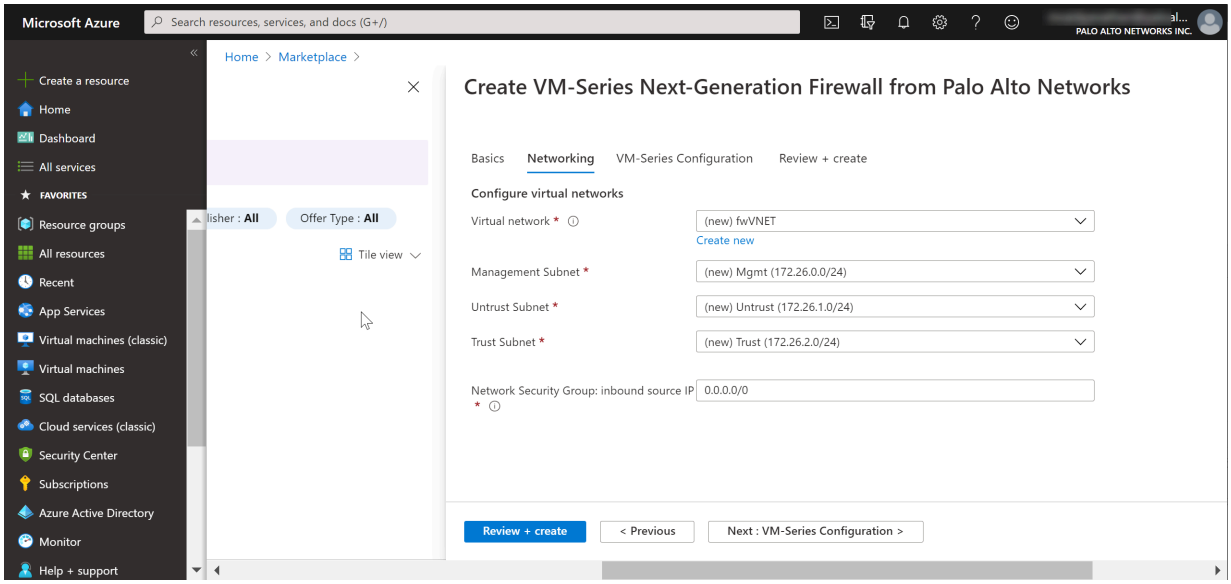
      デフォルトのサブネットを使用する場合は、設定を確認する必要があります。既存の VNet を使用している場合、3 つのサブネットをセットアップしているはずです（それぞれ管理インターフェイス用、trust インターフェイス用、untrust インターフェイス用）。VNet を新規作成する場合、各サブネットのプレフィックスを確認または変更してください。デフォルトのサブネットは、管理サブネットでは 10.8.0.0/24、untrust サブネットでは 10.8.1.0/24、trust サブネットでは 10.8.2.0/24 です。

   3. VNet にアクセスできるソース IP アドレスまたは IP 範囲（CIDR ブロックを含む）を入力します**Network Security Group: inbound source IP**（ネットワーク セキュリ

©2023 Palo Alto Networks, Inc.

ティ グループ：インバウンド ソース **IP**）を有効にすると、Azure VNet へのインバウンド アクセスを制限できます。

ファイアウォールへのアクセスを制限します。専用管理 *IP* アドレスまたはネットワークに対応する *CIDR* ブロックを供給してください。許可するソース ネットワーク範囲を必要以上には大きくせず、*0.0.0.0/0* を許可ソースとして指定しないでください。*IP* アドレスをテンプレートで指定する前に、その *IP* アドレスがロックアウトされないことを確認します。



3. ファイアウォールへの管理アクセスを定義します。

1. デフォルトの変数（(new) fwMgmtPublicIP）を使用し**Public IP address**（パブリック **IP** アドレス）をファイアウォールの管理インターフェイス`eth0`）に割り当てます。

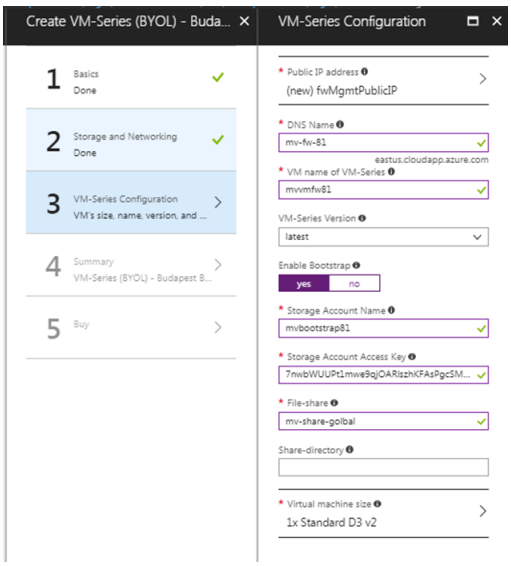
   Azure 高速ネットワークは、管理インターフェイスではサポートされていません。

2. DNS 名を使用してファイアウォールにアクセスするためのプレフィックスを入力します。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、入力したプ

©2023 Palo Alto Networks, Inc.

レフィックスと画面に表示されるプレフィックスを組み合わせる必要があります。例:**<*yourname*<*your-region*.cloudapp.azure.com**

3. 最新の**VM-Series Version**（**VM-Series** バージョン）を選択します。
4. リソースグループ内の VM-Series ファイアウォールを識別するための表示名を入力します。



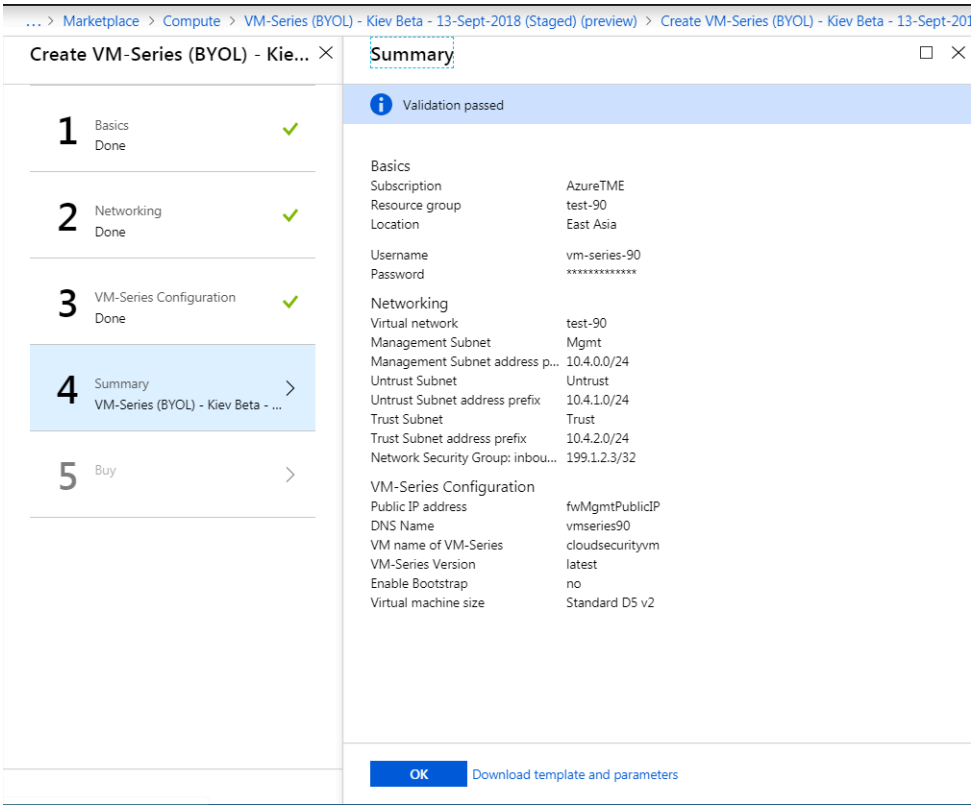
4. 起動時にファイアウォールを設定するための情報を追加します「Azure 上の VM-Series ファイアウォールのブートストラップ」を参照してください。
   1. **yes**（はい）を選択して**Enable Bootstrap**（ブートストラップを有効にする）を選択してください。
   2. ブートストラップ パッケージを保持する**Storage Account Name**（ストレージ アカウント名）を入力します。
   3. **Storage Account Access Key**（ストレージ アカウントのアクセスキー）を入力します。このファイアウォールはストレージ アカウントを認証し、その中に保存されているファイルにアクセスするには、このアクセスキーが必要です。
   4. ブートストラップに必要なファイルをアップロードした**File share name**（ファイル共有名）を追加します。ストレージ アカウントは、ファイアウォールをデプロイ中

©2023 Palo Alto Networks, Inc.

のリージョンと同じリージョン内にある必要があり、ブートストラップ用の正しいフォルダ構造を持っている必要があります。

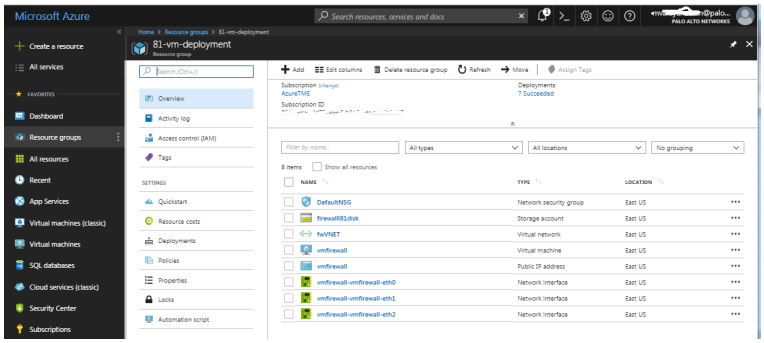
5. 必要に応じて Azure 仮想マシンの層およびサイズを選択します**Change size**（サイズの変更）リンクを使用して、サポートされているインターフェイス タイプを確認しAzure での VM-Series の最小システム要件を確認します。

5. サマリーを確認し**OK**をクリックします。次に、利用規約およびプライバシー ポリシーに同意した後**Create**（作成）してファイアウォールを起動します。



6. VM-Series ファイアウォールが正常にデプロイされたことを確認します。

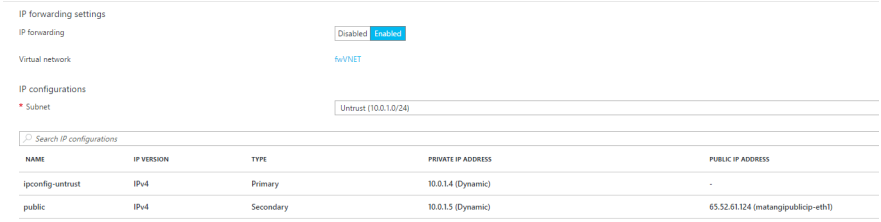
1. **Dashboard**（ダッシュボード） > **Resource Groups**（リソース グループ）を選択し、リソース グループを選択します。
2. リソース グループを選択し、どのリソースが正常にデプロイされたかの詳細について**Overview**（概要）を参照してください。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Series ファイアウォールの untrust インターフェイスのパブリック IP アドレスをアタッチします。パブリック IP アドレスを新規作成する場合、Microsoft が所有する IP アドレスのブロックから取得することになるため、特定のアドレスを選択することはできません。インターフェイスに割り当てられるパブリック IP アドレスの最大数は、Azure サブスクリプションに基づきます。

1. Azure ポータルで、パブリック IP アドレス**eth1** インターフェイス等）を追加するネットワーク インターフェイスを選択します。
2. **IP Configurations**（**IP** 設定） > **Add**（追加）を選択し、パブリック IP アドレスについて**Enabled**（有効化）を選択します。パブリック IP アドレスを新規作成するか、使用可能なアドレスを選択します。
3. インターフェイスに関連付けられた セカンダリ IP アドレスを表示できることを確認します。

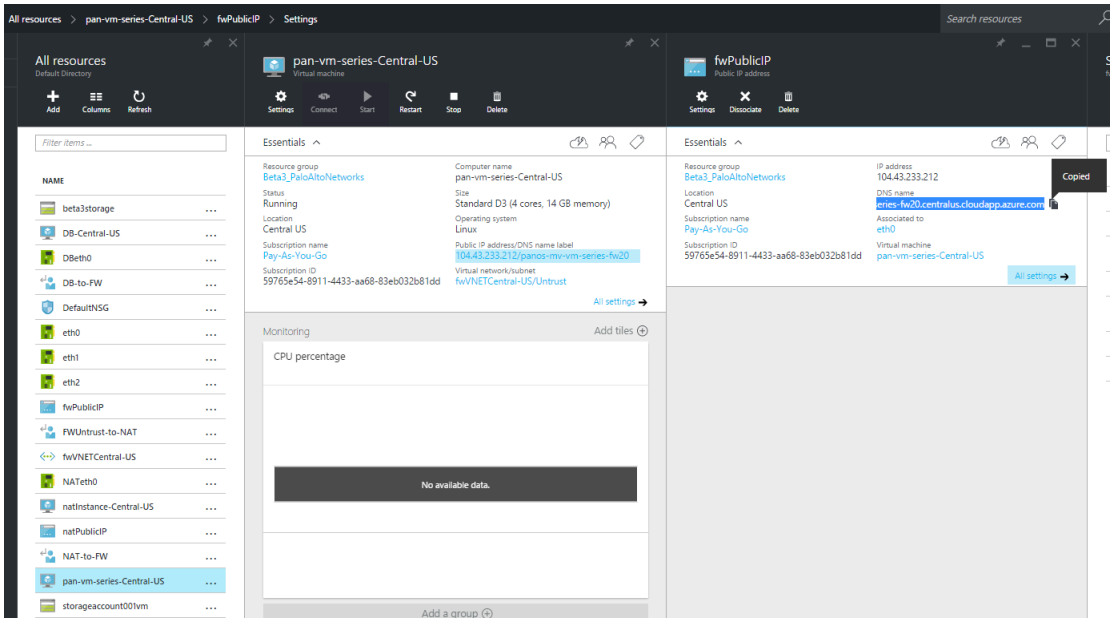


セカンダリ *IP* アドレスをネットワーク インターフェイスにアタッチした場合、*VM-Series* ファイアウォールはインターフェイスに割り当てられたプライベート *IP* アドレスを自動的に取得しません。*VM-Series* ファイアウォールの *Web* インターフェイスを使用してプライベート *IP* アドレスを手動で設定する必要があります。データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 5 | ファイアウォールの Web インターフェイスにログインします。

1. Azure ポータル**All Resources**（すべてのリソース）で VM-Series ファイアウォールを選択し、そのファイアウォールの完全 DNS 名を確認します。



1. Web ブラウザから安全な（https）接続を使用し、その DNS 名を使用してファイアウォールにログインします。
2. Parameters ファイルで定義した ユーザー名パスワードを入力します。証明書の警告が表示されますが問題ありません。Web ページを続行してください。

©2023 Palo Alto Networks, Inc.

STEP 6 | VM-Series ファイアウォールでライセンスをアクティベートします。

BYOL バージョンの場合

1. サポート アカウントを作成します。
2. VM-Series ファイアウォールを登録（認証コードを使用）します。
3. ファイアウォールの Web インターフェイスで**Device**（デバイス） > **Licenses**（ライセンス）を選択し**Activate feature using authentication code**（認証コードを使用して機能をアクティベート）を選択します。
4. サポート ポータルで登録したキャパシティ認証コード*auth-code*）を入力します。ファイアウォールが更新サーバー`updates.paloaltonetworks.com`）に接続され、ライセンスがダウンロードされてから自動的に再起動します。
5. 再度 Web インターフェイスにログインし**Dashboard**（ダッシュボード）で次の項目を確認します。
   - **Serial#**（シリアル番号）に表示されている有効なシリアル番号。

     `Unknown` と表示されている場合、ファイアウォールはライセンスされていません。ファイアウォール上のトラフィック ログを確認するには、有効なキャパシティ ライセンスをインストールする必要があります。
   - **VM Mode**（**VM** モード）に Microsoft Azure と表示されます。

PAYG バージョンの場合

1. サポート アカウントを作成します。
2. パブリック クラウドの VM-Series ファイアウォールの従量制モデルを登録する（認証コード不使用）。

STEP 7 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

1 つのサーバーで異なる IP アドレスおよび SSL 証明書を使用して複数の Web サイトまたはサービスをホストしている場合、VM-Series ファイアウォール インターフェイスで複数の IP アドレスを設定する必要がある場合もあります。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
2. **ethernet 1/1**をクリックし、以下のように設定します。
   - **Interface Type**（インターフェイス タイプ）を**Layer3**（レイヤー **3**）（デフォルト）に設定します。
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - また**Config**（設定）タブで**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して**New Zone**（新規ゾーン）を選択します**UnTrust** という新しいゾーンを定義し**OK** をクリックします。
   - インターフェイスに IP アドレスを 1 つだけ割り当てる場合は**IPv4** タブで**DHCP Client**（**DHCP** クライアント）を選択します。ファイアウォールは、ARM テンプレートに割り当てられたプライベート IP アドレスを自動的に取得します。複数の IP アドレスを割り当てる予定であれば**Static**（静的）を選択して、Azure ポータルのイ

©2023 Palo Alto Networks, Inc.

ンターフェイスに割り当てられるプライマリおよびセカンダリの IP アドレスを手動で入力します。

- このインターフェイスによって処理されるトラフィックが VNet のデフォルトゲートウェイに直接流れないように**Automatically create default route to default gateway provided by server**（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）を無効にします（クリアする）。

3. **ethernet 1/2**をクリックし、以下のように設定します。
   - **Interface Type**（インターフェイス タイプ）を**Layer3**（レイヤー 3）（デフォルト）に設定します。
   - **Security Zone**（セキュリティ ゾーン）を**Trust** に設定します。
   - **IP address**（**IP** アドレス）**DHCP Client**（**DHCP** クライアント）または**Static**（静的）を設定します。
   - このインターフェイスによって処理されるトラフィックが VNet のデフォルトゲートウェイに直接流れないように**Automatically create default route to default gateway provided by server**（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）を無効にします（クリアする）。
4. 変更を**Commit**（コミット）して、インターフェイスのリンク状態が「up」であることを確認します。
5. ファイアウォールがルーティングする必要があるすべてのネットワークについて、VM-Series ファイアウォールの仮想ルーター上でスタティックルートを追加します。

   たとえば、ファイアウォールが保護するサーバーの宛先サブネットにデフォルト ルートを追加するには：
   - **Network**（ネットワーク） > **Virtual Router**（仮想ルーター） > **default**（デフォルト） > を選択します。
   - **Static Routes**（静的ルート） > **IPv4**を選択し、宛先サーバーのネクストホップ IP アドレスを追加します。すべてのトラフィック（インターフェイス ethernet1/1 から 0.0.0.0/0 に向かう）のネクストホップ IP アドレスを x.x.x.1 に設定できます。

STEP 8 | 特定のデプロイのファイアウォールを設定します。

- ゲートウェイ—UnTrust ゾーンの前にサードパーティ製のロードバランサーをデプロイします。
- ハイブリッドおよび **VNet** 間— UnTrust ゾーンの前に Azure VPN ゲートウェイあるいは NAT 仮想マシンをデプロイします。
- サブネット間 — VM-Series ファイアウォールで、Trust インターフェイスに接続されているサブネットに基づいてトラフィックを許可するためのイントラゾーン セキュリティ ポリシー ルールを追加します。
- **GlobalProtect™**—NAT 仮想マシンを UnTrust ゾーンの前にデプロイします。

©2023 Palo Alto Networks, Inc.

STEP 9 | トラフィックを VM-Series ファイアウォールに転送します。

1. VM-Series ファイアウォールが Azure リソース グループ内のすべてのトラフィックを保護できるように、ファイアウォールでスタティック ルートを設定します。
2. VM-Series ファイアウォールのインターフェイスを経由してすべてのトラフィックを転送するために、ユーザー定義のルートを設定します。詳細は、Azure ドキュメントのUDR に関するセクションを参照してください。

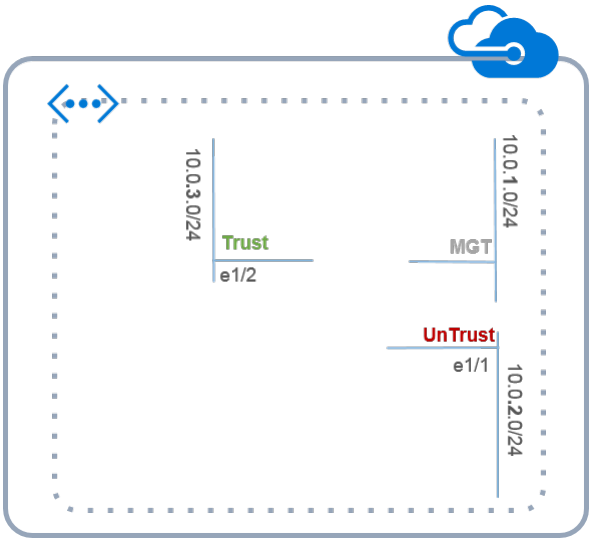
   内部サブネット上のユーザー定義のルートは、すべてのトラフィックを Trust インターフェイスを通して送信する必要があります。インターネットからのすべてのトラフィックを UnTrust 側にあるユーザー定義のルートは、VM-Series ファイアウォール上の UnTrust インターフェイスを通して送ります。Azure クラウドを使用する企業ネットワークに接続するハイブリッド デプロイ環境の場合、Azure VPN ゲートウェイを介して、あるいは Azure Application Gateway または Azure Load Balancer からインターネット トラフィックが来る場合があります。

STEP 10 | PAN-OS® メトリックを Azure Application Insights に公開する方法については、「VM-Series ファイアウォールでの Azure Application Insights の有効化」を参照してください。

©2023 Palo Alto Networks, Inc.

Azure China マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）

Azure China マーケットプレイスで利用できる、VM-Series ファイアウォール用のソリューション テンプレートをデプロイする方法をご説明します。Azure China マーケットプレイスは、BYOL モデルの VM-Series ファイアウォールのみをサポートしています。ファイアウォールは、空の既存のリソース グループまたは新しいリソース グループにデプロイできます。テンプレートのデフォルトの VNet は 10.0.0.0/16 で、デプロイする VM-Series ファイアウォールには 3 つのネットワーク インターフェイスがあります。下で示しているように、1 つは管理インターフェイス、2 つはデータプレーン インターフェイスです。GitHub リポジトリで利用できるカスタマイズ可能な ARM テンプレートを使用するには、「ARM テンプレートを使用して VM-Series ファイアウォールをデプロイ」を参照してください。



STEP 1 | Azure アカウントをセットアップします。

1. Microsoft アカウントを作成します。
2. Microsoft アカウントの認証情報を使用して Azure ポータル（**`https://portal.azure.com`**）にログインします。

   トライアル版を使用している場合、サポート リクエスト（***Help + Support***（ヘルプ + サポート） > ***New Support Request***（新規サポート リクエスト））を開き、割り当てられている仮想マシン コアの量を増やす必要がある場合があります。

©2023 Palo Alto Networks, Inc.

STEP 2 | Azure マーケットプレイスで VM-Series のソリューション テンプレートを探します。

1. Azure China マーケットプレイス（https://market.azure.cn）で Palo Alto Networks を検索します。VM-Series ファイアウォールのさまざまな PAN-OS バージョンのオファーが表示されます。



2. オファーを選択して、**Immediate deployment of**（即座にデプロイ）をクリックします。

STEP 3 | ファイアウォールをデプロイします。

1. 自分の Azure **Subscription**（サブスクリプション）を選択します。
2. リソース グループを選択し、このデプロイ用の VM-Series ファイアウォールに関連するすべてのリソースを取り込みます。

> *VM-Series* ファイアウォールは、新しいリソース グループまたは空の既存のリソース グループにデプロイできます。ファイアウォールを他のリソースがある既存のリソース グループにデプロイするには、GitHub リポジトリの *ARM* テンプレートを使用するか、独自のカスタム *ARM* テンプレートを使用します。既存のリソースが、*ARM* テンプレートで指定するパラメータ値に一致することを確認してください。

1. 新しいリソース グループを作成する場合、リソース グループの名前を入力し、ファイアウォールをデプロイする Azure China 領域を選択します。
2. 既存のリソース グループを選択する場合、このリソースの Azure China 領域を選択し、完全なデプロイを選択します。

3. ファイアウォールの基本設定を行います。

1. 既存のストレージ アカウント名を入力するか、新規作成します。
2. ファイアウォールの vhd mage をコピーして保存する blob ストレージ コンテナの名前を入力します。
3. ファイアウォールの管理インターフェイス（eth0）のパブリック IP アドレスにアクセスするための DNS 名を入力します。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、入力したプレフィックスをサフィックスと組み合わせる必要

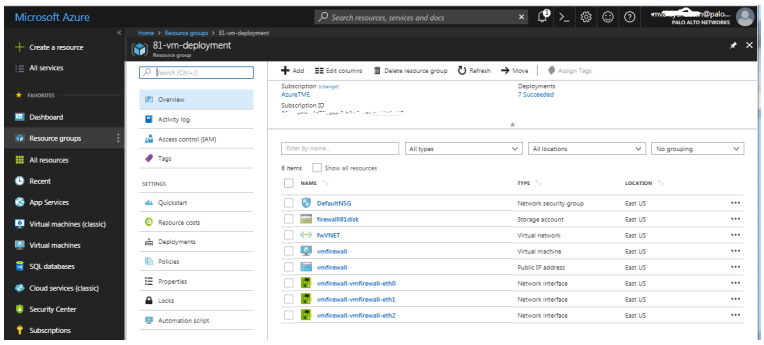
©2023 Palo Alto Networks, Inc.

があります。たとえば、<yourDNSname><china_region>.cloudapp.azure.com のようになります。

4. ファイアウォールの管理者の **Username**（ユーザー名）を入力します。
5. ファイアウォールへの管理者アクセスを保護するための **Password**（パスワード）を入力します。
6. 必要に応じて Azure 仮想マシンの層およびサイズを選択します。「Azure における VM-Series の最小システム要件」を参照してください。
7. **VmName** を入力します。これは、リソース グループ内の VM-Series ファイアウォールを識別するための表示名です。
8. **PublicIPAddressName** を使用して、リソース グループ内のファイアウォール管理インターフェイスにラベルを付けます。Microsoft Azure では、定義した DNS 名とこの名前がバインドされるため、パブリック インターネットからファイアウォールの管理インターフェイスにアクセスできます。
9. VNet を識別する **VirtualNetworkName** を入力します。VNet のデフォルトの IP **Address Prefix**（アドレス プレフィックス）は 10.0.0.0/16 です。これは、IP アドレスのニーズに合わせて変更できます。
10. ネットワーク インターフェイスのサブネットを設定します。既存の VNet を使用している場合、3 つのサブネットを定義しているはずです（それぞれ管理インターフェイス用、trust インターフェイス用、untrust インターフェイス用）。VNet を新規作成する場合、各サブネットのプレフィックスを確認または変更してください。デフォルトのサブネットは 10.0.1.0/24、10.0.2.0/24、10.0.3.0/24 です。必要に応じて、これらのサブネットを管理インターフェイス、trust インターフェイス、untrust インターフェイスに割り当てることができます。

4. 概要を確認し、利用規約およびプライバシー ポリシーに同意した後、**Immediate deployment**（即座にデプロイ）をクリックしてファイアウォールをデプロイします。デプロイには 20 分かかる可能性もあり、このページのリンクを使用して進捗状況を確認できます。
5. VM-Series ファイアウォールが正常にデプロイされたことを確認します。

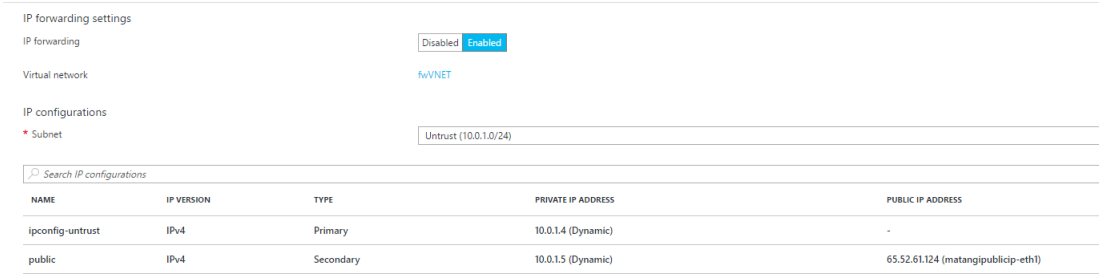
1. Microsoft アカウントの認証情報を使用して、Azure China ポータル（https://portal.azure.cn）にログインします。
2. **Dashboard**（ダッシュボード） > **Resource Groups**（リソース グループ）の順に選択し、リソース グループを選択します。
3. 詳細な状態については、**All Settings**（すべての設定） > **Deployments**（デプロイ） > **Deployment History**（デプロイ履歴）を選択します。



©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Series ファイアウォールの untrust インターフェイスのパブリック IP アドレスをアタッチします。これにより、パブリック インターネットからインターフェイスにアクセスでき、インターネットに接続されるアプリケーションまたはサービスの場合に便利です。

1. Azure ポータルで、パブリック IP アドレスを追加するネットワーク インターフェイスを選択します。たとえば、eth1 インターフェイスなどです。
2. **IP Configurations**（**IP** 設定） > **Add**（追加）を選択し、パブリック IP アドレスについて **Enabled**（有効化）を選択します。パブリック IP アドレスを新規作成するか、使用可能なアドレスを選択します。
3. インターフェイスに関連付けられた セカンダリ IP アドレスを表示できることを確認します。



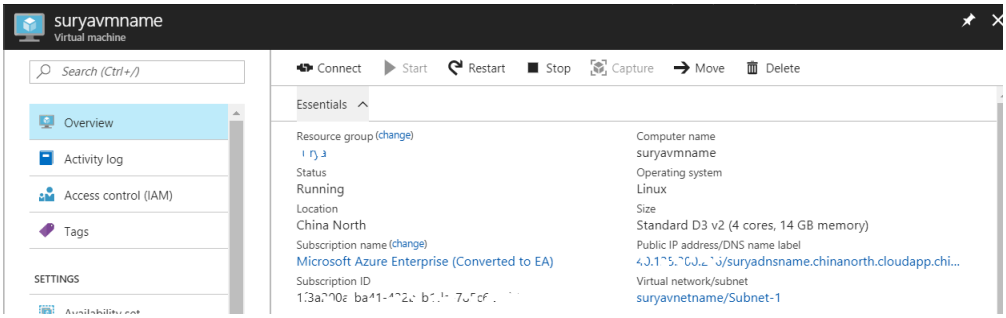
セカンダリ *IP* アドレスをネットワーク インターフェイスにアタッチした場合、*VM-Series* ファイアウォールはインターフェイスに割り当てられたプライベート *IP* アドレスを自動的に取得しません。*VM-Series* ファイアウォールの *Web* インターフェイスを使用してプライベート *IP* アドレスを手動で設定する必要があります。「データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定」を参照してください。

Azure の VM-Series ファイアウォールの各インターフェイスには動的（デフォルト）または静的なプライベート IP アドレス、複数のパブリック IP アドレス（静的または動的）が関連付けられています。インターフェイスに割り当てられるパブリック IP アドレスの最大数は、Azure サブスクリプションに基づきます。パブリック IP アドレスを新規作成する場合、Microsoft が所有する IP アドレスのブロックから取得することになるため、特定のアドレスを選択することはできません。

©2023 Palo Alto Networks, Inc.

STEP 5 | ファイアウォールの Web インターフェイスにログインします。

1. Azure ポータルの**All Resources**（すべてのリソース）で VM-Series ファイアウォールを選択し、そのファイアウォールの完全 DNS 名を確認します。



2. Web ブラウザから安全な接続（https）を使用し、その DNS 名を使用してファイアウォールにログインします。
3. 以前に定義したユーザー名/パスワードを入力します。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。

STEP 6 | VM-Series ファイアウォールでライセンスをアクティベートします。

1. サポート アカウントを作成します。
2. VM-Series ファイアウォールを登録（認証コードを使用）します。
3. ファイアウォールの Web インターフェイスで **Device**（デバイス） > **Licenses**（ライセンス）を選択し、**Activate feature using authentication code**（認証コードを使用して機能をアクティベート）を選択します。
4. サポート ポータルで登録したキャパシティ認証コードを入力します。ファイアウォールが更新サーバー（updates.paloaltonetworks.com）に接続され、ライセンスがダウンロードされてから自動的に再起動します。
5. 再度 Web インターフェイスにログインし、**Dashboard**（ダッシュボード）で次の項目を確認します。
   - **Serial#**（シリアル番号）に表示されている有効なシリアル番号。

     Unknown（不明）と表示されている場合、デバイスはライセンスされていません。ファイアウォール上のトラフィック ログを確認するには、有効なキャパシティ ライセンスをインストールする必要があります。
   - **VM Mode**（**VM** モード）に Microsoft Azure と表示されます。

©2023 Palo Alto Networks, Inc.

STEP 7 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

1 つのサーバーで異なる IP アドレスおよび SSL 証明書を使用して複数の Web サイトまたはサービスをホストしている場合、VM-Series ファイアウォール インターフェイスで複数の IP アドレスを設定する必要がある場合もあります。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
2. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :Layer3（デフォルト）
   - Config（設定）タブで、インターフェイスをデフォルト ルーターに割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウンを展開して New Zone（新規ゾーン）を選択します。UnTrust という新しいゾーンを定義し、OK をクリックします。
   - **IPv4** タブで、インターフェイスで 1 つの IP アドレスのみを割り当てる予定であれば、**DHCP Client**（**DHCP** クライアント）を選択します。ARM テンプレートで割り当てられているプライベート IP アドレスが自動的に取得されます。複数の IP アドレスを割り当てる予定であれば、**Static**（静的）を選択して、Azure ポータルのインターフェイスに割り当てられるプライマリおよびセカンダリの IP アドレスを手動で入力します。
   - **Automatically create default route to default gateway provided by server**（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）チェックボックスをオフにします。このオプションを無効にすると、このインターフェイスで処理されるトラフィックが VNet のデフォルト ゲートウェイに直接流れなくなります。
3. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type**（インターフェイス タイプ）を Layer3（デフォルト）に設定します。
   - **Security Zone** [セキュリティゾーン]:Trust
   - **IP** アドレス:**DHCP Client**（**DHCP** クライアント）または **Static**（静的）を選択します。
   - **Automatically create default route to default gateway provided by server**（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）チェックボックスをオフにします。このオプションを無効にすると、このインターフェイスで処理されるトラフィックが VNet のデフォルト ゲートウェイに直接流れなくなります。
4. **Commit**（コミット）をクリックします。インターフェイスのリンク状態が「up」であることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 8 | 特定のデプロイのファイアウォールを設定します。

- ゲートウェイ — UnTrust ゾーンの前にサードパーティ製のロード バランサーをデプロイします。
- ハイブリッドおよび VNet 間 — UnTrust ゾーンの前に Azure VPN ゲートウェイあるいは NAT 仮想マシンをデプロイします。
- サブネット間 — VM-Series ファイアウォールで、イントラゾーンのセキュリティ ポリシー ルールを追加してその Trust インターフェイスにアタッチされたサブネットに基づいてトラフィックを許可します。
- GlobalProtect — UnTrust ゾーンの前に NAT 仮想マシンをデプロイします。

STEP 9 | トラフィックを VM-Series ファイアウォールに転送します。

1. VM-Series ファイアウォールが Azure リソース グループ内のすべてのトラフィックを保護できるように、ファイアウォールでスタティック ルートを設定します。
2. VM-Series ファイアウォールのインターフェイスを経由してすべてのトラフィックを転送するために UDR を設定します。詳細は、Azure ドキュメントの UDR に関するセクションを参照してください。

   内部サブネット上の UDR がすべてのトラフィックを Trust インターフェイスを通して送信する必要があります。インターネットからのすべてのトラフィックを UnTrust 側にある UDR が VM-Series ファイアウォール上の UnTrust インターフェイスを通して送ります。Azure クラウドを使用する企業ネットワークに接続するハイブリッド デプロイ環境の場合、Azure VPN ゲートウェイを介して、あるいは Azure Application Gateway または Azure Load Balancer からインターネット トラフィックが来る場合があります。

©2023 Palo Alto Networks, Inc.

AzureでのPanoramaが統制するデプロイメント

Panorama plugin for Azureは、Azureクラウド内のセキュリティ体制を集中的にデプロイ、設定、監視します。ファイルを管理するためのセキュリティポリシーを有効にするため、Azureネットワーク内のVM-Seriesデプロイを統制しています。プラグインは、Azure ARMデプロイとAzure Monitorページをリンクして、VM-Seriesファイアウォールのデプロイステータス、使用状況、およびパフォーマンスなどの情報を提供しています。

Azureで、葉プラグインはロードバランサー、サブネット、およびNATゲートウェイや、VM-Seriesファイアウォールオートスケーリングセットなどの、Azureリソースのデプロイ環境を統制します。Panoramaで、プラグインは自動的にPanoramaデバイスグループ、テンプレートスタック、およびNATポリシーを設定します。Azureリソースからタグを読み込んで、ファイアウォールのグループに対してタグベースのポリシーを有効にします。

Panorama プラグインは、Azure 環境の 1 つ以上のリージョンでのデプロイメントをオーケストレーションできます。デプロイメント環境は、保護する必要があるトラフィックに応じて、Hub スタックまたはインバウンドスタック、またはその両方から成り立つことが可能です。

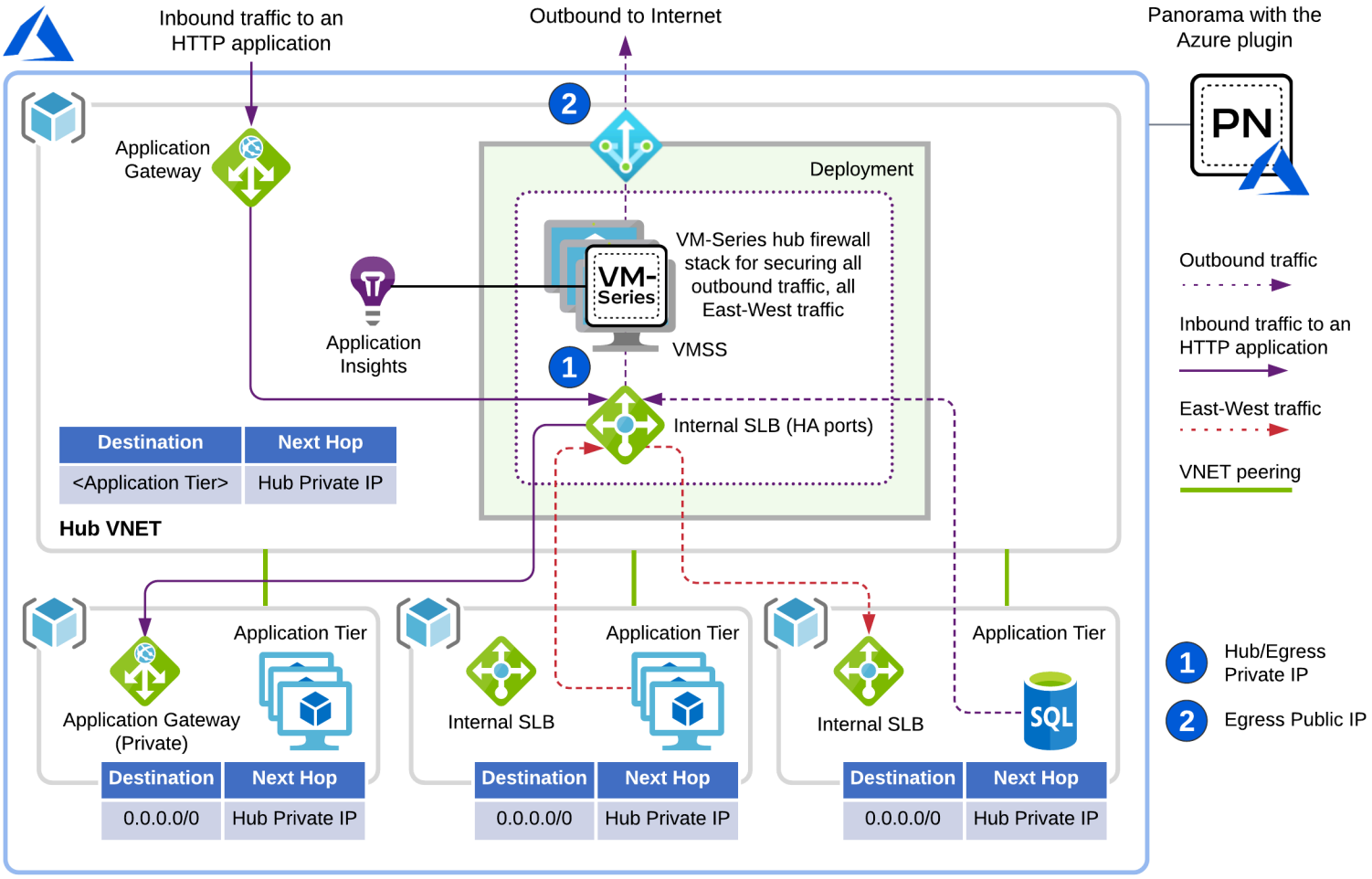
- *Hub*ファイアウォールスタックは、アプリケーションワークロード間のアウトバウンド トラフィックとEast-Westトラフィックを保護します。
- インバウンドファイアウォールスタックは、パブリックに面しているアプリケーションとやり取りされるトラフィックを保護します。

各スタック内のファイアウォール数を設定することができます。デプロイ環境内のファイアウォールの静的な量、またはスケーリングに使用するVMSSの範囲を設定することができます。デプロイ環境内のスタックは両方とも、VM-SeriesファイアウォールのVMSSを作成し、それぞれ最大25件のファイアウォールまで拡張することができます。

Hubスタック

Hubスタックを使用し、Azure Internal Standard Load Balancer（HAポート付き）を活用して、一連のファイアウォールにまたがってスケーリングとロードバランシングを行います。標準のロードバランサーのプライベート IP アドレス （**2**、次の図の「Hub/出口プライベート IP」）を使用して、検査と脅威防御のためにトラフィックをファイアウォールにルーティングできます。Hub スタックは、アプリケーションのアウトバウンドおよび East-West トラフィックを保護します。

©2023 Palo Alto Networks, Inc.



アウトバウンドトラフィックとEast-Westトラフィックを保護するために、アプリケーションVNETのルートルールを追加して、検査のためにトラフィックをHubスタックにリダイレクトします。

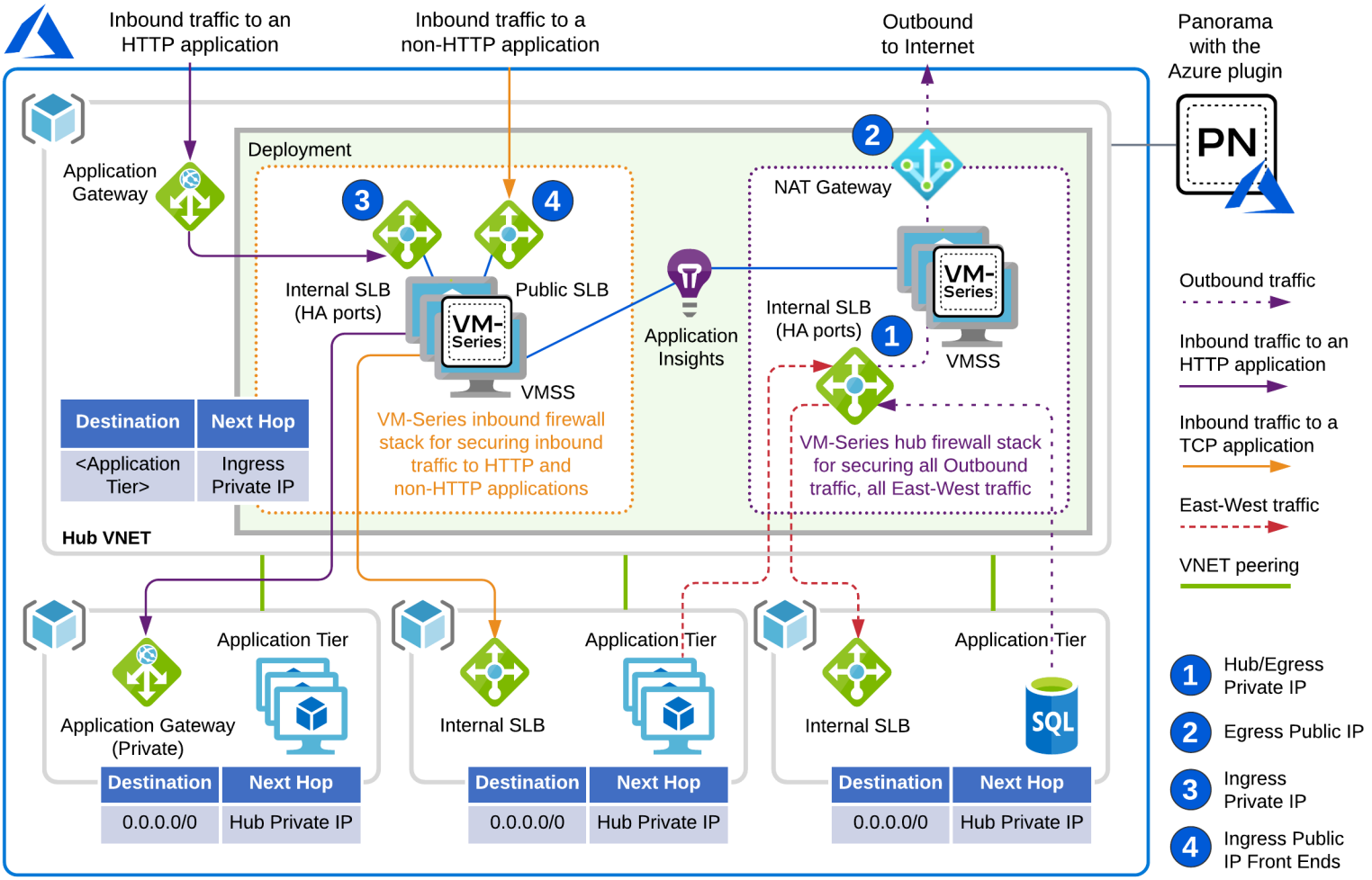
Inbound Stack（インバウンドスタック）

インバウンドファイアウォールスタックは、個別にスケーリングを行い、アプリケーションのインバウンドトラフィックに対して可視性とセキュリティを追加します。

インバウンド HTTP トラフィックを保護するために、アプリケーションゲートウェイのサブネットルートテーブルに UDR を追加して、すべてのトラフィックをインバウンドスタックにルーティングします（**3**、次の図の入口プライベートIP）。HTTP 以外のインバウンド トラフィックを保護するために、Panorama プラグインを使って、アプリケーションエンドポイントのフロントエンドエントリを作成します（**4**、次の図の入口パブリック IP フロントエンド）。検査を有効にするために、PanoramaプラグインはAzure Public Standard Load Balancer（Azureパブリック標準ロードバランサー）上でロードバランサールールを、ファイアウォール上でNATルールを自動的に作成します。

HTTP/HTTPSインバウンド トラフィックのみが存在している場合は、インバウンドスタックを放置して、そのトラフィックを単純にHubスタックで保護することができます。

©2023 Palo Alto Networks, Inc.



統制デプロイ環境の準備およびAzureでのVM-Seriesファイアウォールデプロイ環境の統制を参照してください。

統制デプロイ環境の準備

AzureでVM-Seriesファイアウォールを統制するには、次の作業を行ってください。

- 設定の前提条件
- 統制のアクセス許可
- カスタムロールの作成とActive Directoryとの関連付け
- Azure Directoryドメイン名の検索

設定の前提条件

PanoramaとAzureで次の基本作業を行ってください。

©2023 Palo Alto Networks, Inc.

- Azure
  - プラグインのAPI呼び出しを有効にするために、サービスプリンシパルを作成する。
  - VM-SeriesファイアウォールTransit VNet専用のCIDRブロックをプランニングする。プラグインはこのCIDRブロックを管理して、それを使って初期のファイアウォールVNetのデプロイを行い、将来的に新しいテンプレートスタックへのアップグレードを実施します。

    最低のCIDR範囲は/22です。
- Panorama
  - Panoramaで有効なライセンスAPIキーを設定していることを確認する。そうすることで、オートスケーリングのスケールインイベント時に、ライセンスの解除を管理できるようになります。「ライセンス無効化 API キーのインストール」を参照してください。
  - Application Insight設定をテンプレートスタックに追加するために、Panoramaに最新バージョンのVM-Seriesプラグインをインストールする。
- 認定された Azure リージョン

  Panorama オーケストレーションのデプロイメントは、VM-Series ファイアウォールをサポートするすべてのリージョンでサポートされています。次のリージョンが認定されています。リストにないリージョンにデプロイして問題が発生した場合は、サポートに連絡してください。
  - 米国西部
  - 米国西部 2
  - 北中部米国
  - 米国東部
  - 米国東部 2
  - 西ヨーロッパ
  - ドイツ西中部
  - アラブ首長国連邦北
  - 西インド
  - Australia Southeast（オーストラリア南東部）

デプロイをプランニングする際には、現在Panorama Plugin for Azureバージョン2.xを実行している場合、現在のバージョンへのアップグレードは許可されていないことに注意してください。また、現在のバージョンをインストールした後は、バージョン2.xのプラグインにダウングレードすることはできません。詳細は、互換性マトリックスのPanorama Plugin for Azureを参照してください。

統制のアクセス許可

これは、Template Deployerロールのアクセス許可を持つサンプルJSONファイルです。**AssignableScopes**セクションには、デプロイ先のサブスクリプション、および保護するVM-SeriesファイアウォールVNetとピアリングされたアプリケーションVNETを含む各サブスクリプションを含めて、クエリを行う必要があるすべての関連するサブスクリプションが含まれています。

©2023 Palo Alto Networks, Inc.

```
{
    "Name": "Template Deployment",
    "IsCustom": true,
    "Description": "Manage template deployments.",
    "Actions": [
        "Microsoft.Resources/subscriptions/resourcegroups/*",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Network/publicIPPrefixes/write",
        "Microsoft.Network/publicIPPrefixes/read",
        "Microsoft.Network/publicIPPrefixes/delete",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/natGateways/write",
        "Microsoft.Network/natGateways/read",
        "Microsoft.Network/natGateways/delete",
        "Microsoft.Network/natGateways/join/action",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/write",
        "Microsoft.Network/virtualNetworks/delete",
        "Microsoft.Network/virtualNetworks/subnets/write",
        "Microsoft.Network/virtualNetworks/subnets/read",
        "Microsoft.Network/virtualNetworks/subnets/delete",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/
read",
        "Microsoft.Network/networkSecurityGroups/write",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/delete",
        "Microsoft.Network/loadBalancers/probes/join/action",
        "Microsoft.Network/loadBalancers/backendAddressPools/join/
action",
        "Microsoft.Network/loadBalancers/frontendIPConfigurations/
read",
        "Microsoft.Network/locations/serviceTags/read",
        "Microsoft.Network/applicationGateways/read",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Compute/virtualMachineScaleSets/write",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/delete",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/
read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/images/read",
        "Microsoft.insights/components/write",
        "Microsoft.insights/components/read",
        "Microsoft.insights/components/delete",
        "Microsoft.insights/autoscalesettings/write"
```


©2023 Palo Alto Networks, Inc.

```
    ]
     "NotActions": [
    ],
     "AssignableScopes": [
        "/subscriptions/{deployment-subscription}",
        "/subscriptions/{app1-subscription}",
        "/subscriptions/{app2-subscription}",
        .
        .
        .
    ]
}
```

カスタムロールの作成とActive Directoryとの関連付け

STEP 1 | AzureでActive Directoryを作成するには、Azure Active Directoryに移動して、左側の**App Registrations**（アプリケーション登録）をクリックします。プラグインが必要なアクセス許可を使ってカスタムロールを作成します。

JSONの例を以下に示します。

1. **add**（追加）をクリックして、名前を指定します。上記のJSONファイルから作成したロールを選択し、「Assign access to（アクセスの割当先）」をActive Directoryユーザーのままにして、次に最初のステップで作成したActive Directoryを選択してSave（保存）をクリックします。
2. タイプを選択します。

   Redirect URI（リダイレクトURI）下は何も変更しないでください。

STEP 2 | プラグインが必要なアクセス許可を使ってカスタムロールを作成します。

「関連ドキュメント」を参照してください。

1. Azure CLIにログインします。

   ```
   az login
   ```

2. 統制のアクセス許可内のファイルから、カスタムロールを作成します。

   ```
   az role definition create --role-definition <role-json-file>
   ```


©2023 Palo Alto Networks, Inc.

STEP 3 | ロールを、ステップ1で作成したActive Directoryに関連付けます。コンソールまたはCLIを使用できます。

You must repeat this step in every subscription defined in the 統制のアクセス許可のカスタムロールの***assignableScope***セクションに定義されている各サブスクリプションに対して、この手順を繰り返す必要があります。

コンソール

1. Azureポータルで、**Subscriptions**（サブスクリプション）に移動して目的のサブスクリプションを選択します。
2. 左側から、**Access Control（IAM）**（アクセス制御）を選択した後、上部のバーから**Role Assignments**（ロール割り当て）を選択します。
3. **Add**（追加）を選択して、**add role assignment**（ロール割り当ての追加）を選択します。
   - ステップ3で作成したロールを選択して、「Assign access to（アクセスの割当先）」はActive Directoryユーザーのままにします。
   - ステップ1で作成したActive Directoryを選択して、**Save**（保存）をクリックします。

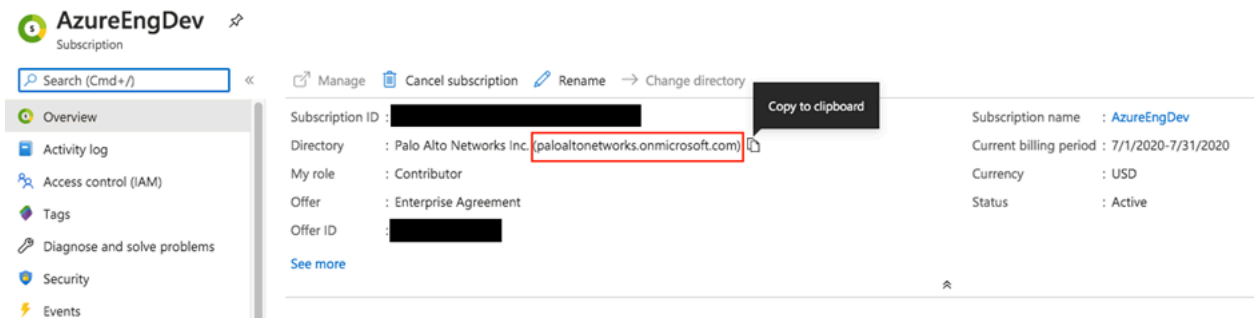
CLI:

次のコマンドで**<role-name>**は、前の例「テンプレートのデプロイ」のサンプルJSONファイルにある名前を表しています。

```
az ad sp create-for-rbac --name <name-of-service-principal>
--role <role-name>
--output json
```

Azure Directoryドメイン名の検索

AzureデプロイおよびAzureポータル内のApplication Insightsインスタンスへのリンクを提供するために、以下のようにサブスクリプションのディレクトリドメインを識別する必要があります。



AzureでのVM-Seriesファイアウォールデプロイ環境の統制

最大10件の統制されたデプロイ環境を作成することができます。さらに、オーケストレーションされた各デプロイメントは、最大 100 のフロントエンドアプリケーションをサポートします。

©2023 Palo Alto Networks, Inc.

*Azure China*および*Azure Government*はサポートされていません。

©2023 Palo Alto Networks, Inc.

STEP 1 | サービス プリンシパルを作成します。

作成したサービスプリンシパル認証情報をオンボーディングして、デプロイ環境を統制するために必要なAPI呼び出しを行うための、Panoramaプラグインアクセス許可を与えます。

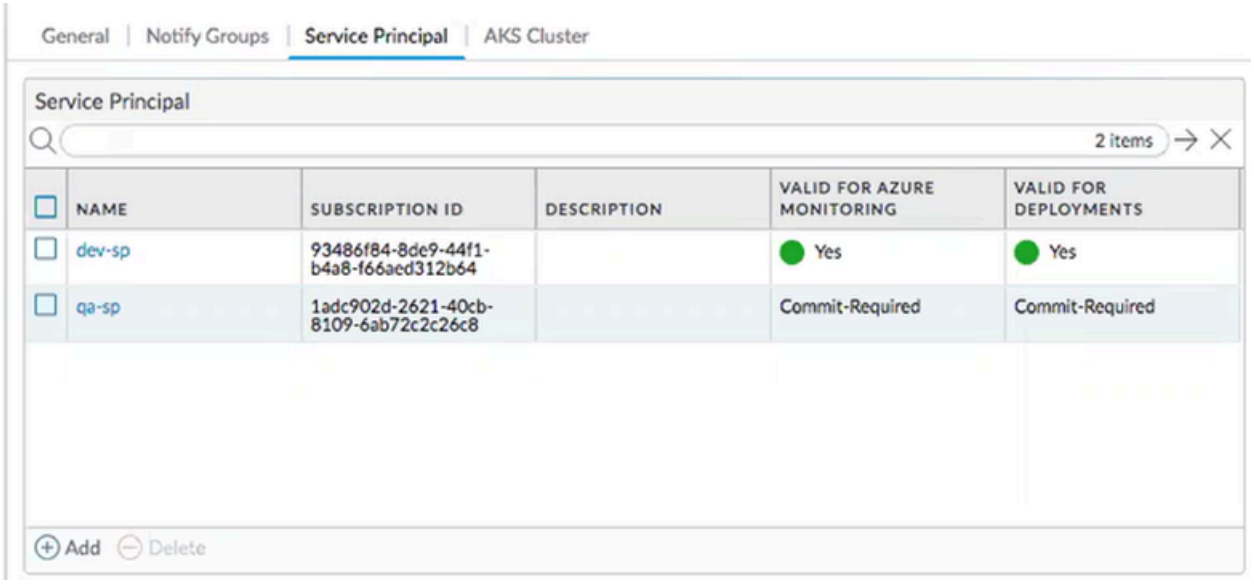
1. **Setup**（セットアップ） > **Service Principal**（サービスプリンシパル） > **Add**（追加）を選択します。
2. サービスアカウントを識別する**Name**（名前）および任意で**Description**（説明）を入力します。
3. 監視する Azure サブスクリプションの**Subscription ID**（サブスクリプション **ID**）を入力します。

   Azure ポータルにログインしてこのサブスクリプション ID を取得する必要があります。
4. **Client ID**（クライアント**ID**）を入力します。クライアント ID は、Azure Active Directory アプリケーションに関連付けられているアプリケーション ID です。
5. **Client Secret**（クライアント シークレット）を入力し、確認用に再び入力します。
6. **Tenant ID**（テナント **ID**）を入力します。

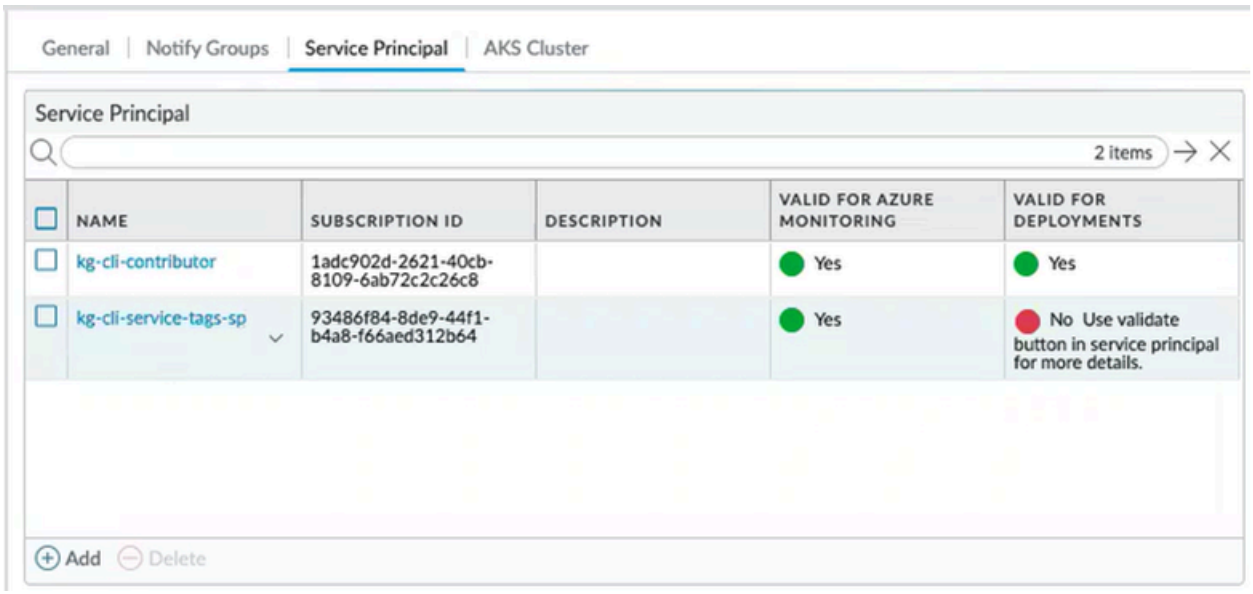
   テナント ID は、アクティブディレクトリ アプリケーションをセットアップする際に保存したディレクトリ ID です。
7. **Validate**（検証）をクリックし、入力したキーおよび ID が有効であり、Panorama が API を使用して Azure サブスクリプション と通信できることを確認します。

   検証には最大で1分ほどかかります。進捗状況を確認するために、ページを更新することができます。
8. サービスプリンシパルが有効だった場合、変更内容をコミットします。

   コミットすることにより、デプロイ環境の設定時に、サービスプリンシパルを利用できるようになります。



 ©2023 Palo Alto Networks, Inc.



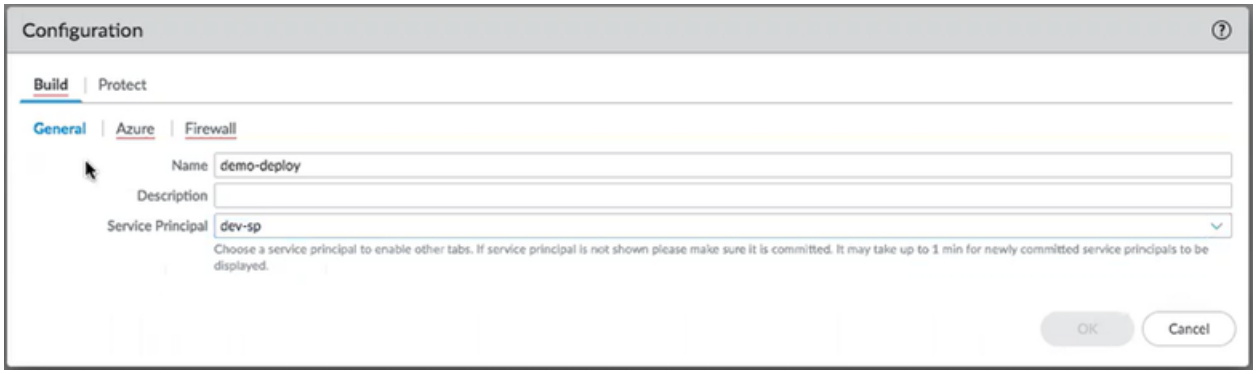
©2023 Palo Alto Networks, Inc.

STEP 2 | Azureデプロイ環境を設定します。

1. **Deployments**（デプロイ）を選択して、設定を**Add**（追加）します。
2. **Build**（ビルド） > **General**（全般）を選択します。
   - **Name**（名前）および必要に応じて**Description**（説明）を入力します。
   - ドロップダウンリストから、サービスプリンシパルを選択します。

     Azureタブを有効にするために、有効なサービスプリンシパルを選択する必要があります。

     目的のサービスプリンシパルが見つからない場合、ステップ1に戻ってサービスプリンシパルが有効なもので、コミットされていることを確認してください。



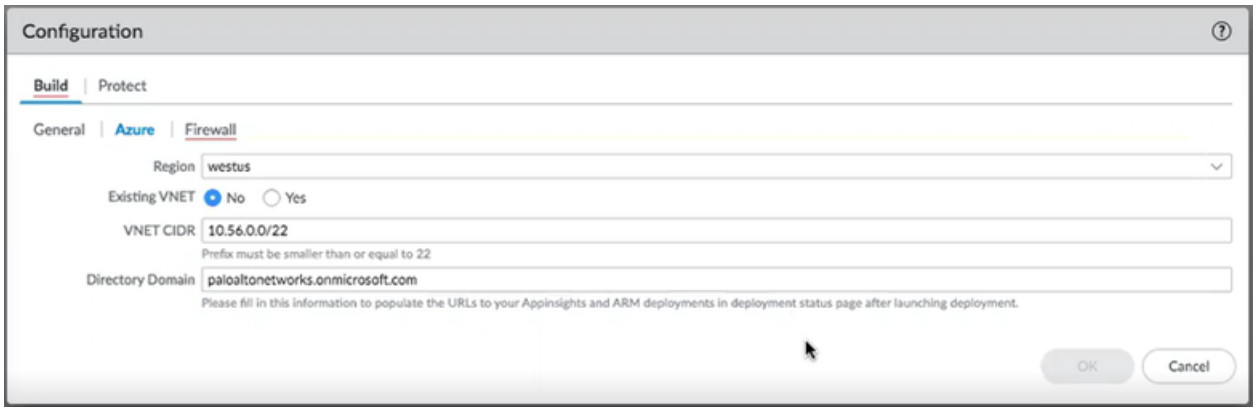
3. **Build**（ビルド） > **Azure**タブで、リージョンを選択します。

   ドロップダウンリストは動的なもので、Palo Alto NetworksのVM-Series次世代ファイアウォールイメージを持つすべてのリージョンが表示されます。

   - **Existing VNET**（既存の**VNET**）。
     - 新しいVNETを作成する場合は、**No**（いいえ）を選択します。

       プラグインはVNET CIDRおよびDirectory Domain（ディレクトリドメイン）を使って、VNETを作成します。
     - 既存のVNETを指定する場合は、**Yes**（はい）を選択します。
   - **VNET CIDR**—CIDR範囲を入力します。プレフィックスは、/22以下でなければなりません。例:192.168.0.0/22。
   - **Directory Domain**（ディレクトリドメイン）—「Azure Directoryドメイン名の検索」を参照してください。この文字列は、サブスクリプション内のすべてのリソースに対するURLの一部で、プラグインがデプロイ環境にリンクするために役立ちます。

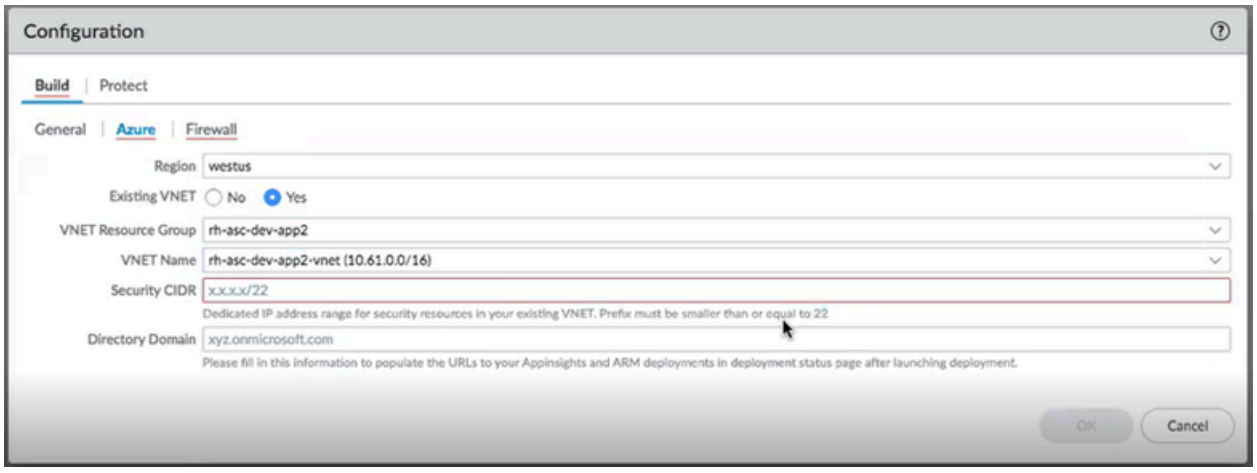
©2023 Palo Alto Networks, Inc.



Yes（はい）を選択した場合、プラグインがVNET Resource Group（VNETリソースグループ）、VNET Name（VNET名）、Security CIDR（セキュリティCIDR）、およびDirectory Domain（ディレクトリドメイン）を問い合わせます。

- **VNET Resource Group**（**VNET**リソースグループ）—選択したリージョン内のすべてのリソースグループのリストから選択してください。
- **VNET Name**（**VNET**名）—選択したリソースグループ内のVNETのリストから選択します。
- **Security CIDR**（セキュリティ**CIDR**）—CIDR範囲を入力します。プレフィックスは、/22以下でなければなりません。例:192.168.0.0/22。
- **Directory Domain**（ディレクトリドメイン）—「Azure Directoryドメイン名の検索」を参照してください。この文字列は、サブスクリプション内のすべてのリソースに対するURLの一部で、プラグインがデプロイ環境にリンクするために役立ちます。

VNET Resource Group（VNETリソースグループ）およびVNET Name（VNET名）は、プラグインが既存のVNETを探すために役立ちます。プラグインがデプロイしたものはすべて、プラグインが管理するリソースグループに配置されます。



STEP 3 | デプロイ環境のVM-Seriesファイアウォールスタックを設定します。

アウトバウンド/East-Westトラフィックを保護するために、Hubスタックをデプロイすることができます。インバウンドトラフィックを保護するために、インバウンドスタックをデプロ

©2023 Palo Alto Networks, Inc.

イすることができます。すべてのトラフィックフローを保護する必要がある場合は、両方のスタックをデプロイすることも可能です。

どちらのスタックも、設定パラメータは同じです。

- **License Type**（ライセンスタイプ）—BYOL、Bundle 1、またはBundle 2を選択します。
- **License Authcode**（ライセンス認証コード）—（BYOLのみ）。Welcome（歓迎）の手紙に記載されている認証コードを入力します。
- **VM Size**（**VM**サイズ）
  - ドロップダウンリストには、入力した認証コードと相関があるVMサイズが表示されます。
  - Bundle1またはBundle2—任意のVMサイズを選択します。

Existing Device Group（既存のデバイスグループ）—デバイスグループは、両方のスタックおよびデプロイ環境に対して一意でなければなりません。つまり、各デプロイ環境内の各スタックに対して、個別の専用デバイスグループが必要になります。

No（いいえ）を選択した場合、プラグインがデバイスグループを作成します。

Yes（はい）を選択した場合、ドロップダウンリストから既存のデバイスグループを選択してください。

- **Min Firewalls**（最低ファイアウォール数）—VMSSに対して1～25の範囲の値。
- **Max Firewalls**（最大ファイアウォール数）—VMSSに対して1～25の範囲の値。

STEP 4 | **Build**（ビルド） > **Firewall**（ファイアウォール） > **Basic**（基本）を選択して、両方のスタックに共通の情報を設定します。

Image Type（イメージタイプ）では、**Marketplace Image**（**Marketplace**イメージ）または**Custom Image**（カスタムイメージ）を選択します。

- **Image Resource Group**（イメージリソースグループ）—（カスタムイメージのみ）カスタムイメージを含むリソースグループを選択します。カスタムイメージの場合、リストにはステップ2.bで選択したリージョンからのイメージを含む、すべてのリソースグループが表示されます。
- **Image**（イメージ）—（カスタムイメージのみ）ドロップダウン リストには、選択したリソースグループ内のすべてのイメージが表示されます。
- **Software Version**（ソフトウェアバージョン）—（Marketplaceイメージ）有効なソフトウェアバージョンのみが表示されます。PAN-OSの最低バージョンについては、「互換性マトリックス」を参照してください。
- **Username**（ユーザー名）—作成したファイアウォールの管理ユーザー名。名前は、VM-Seriesファイアウォールと Azureの両方で有効なものでなければなりません。「VM作成時のユーザー名の要件は？」を参照してください。
- **Password**（パスワード）—作成したファイアウォールの管理者パスワード。パスワードは、VM-Seriesファイアウォールと Azureの両方の、文字および長さの要件（31文字）を

©2023 Palo Alto Networks, Inc.

満たしている必要があります。「VM作成時のパスワードの要件は？」を参照してください。

- **Confirm Password**（パスワードの再入力）—パスワードを再入力します。
- **Primary Panorama IP**（プライマリ**Panorama IP**）—ブートアップ時にファイアウォールが、Panoramaと接続するために使用する、Panorama IPアドレスを指定します。ドロップダウンリストに表示されるパブリックまたはプライベートIPアドレスから選択するか、またはPanorama IPアドレスを入力します。
- **Secondary Panorama IP**（）—（PanoramaがHAセットアップを行っている場合のみ。）ブートアップ時にファイアウォールが、Panoramaと接続するために使用する、セカンダリPanorama IPを指定します。ドロップダウン リストから選択するか、または正しいIPを入力してください。
- **Configure Device Certificate PIN**（デバイス証明書**PIN**を設定）。これらの値を暗号化されているため、各値を入力して、それを確認する必要があります。
  - **Device Certificate PIN ID**（デバイス証明書**PIN ID**）—デバイス証明書ID。
  - **Confirm Device Certificate PIN ID**（デバイス証明書**PIN ID**の再入力）
  - **Device Certificate PIN Value**（デバイス証明書**PIN**値）—証明書のPIN値。
  - **Confirm Device Certificate PIN Value**（デバイス証明書**PIN**値の再入力）

STEP 5 | **Build**（ビルド） > **Firewall**ファイアウォール > **Advanced**高度を選択し、必要に応じてデフォルト値を指定します。

デフォルト値を編集するには、**Advanced**（高度）を選択します。

- **Autoscaling Metric**（オートスケーリング測定基準）—デフォルトはData Plane CPU Util Percent（データプレーンCPU使用状況割合）です。
- **Scale In Threshold**（スケールインしきい値）—デフォルトを使用するか、またはスケールインしきい値を定義します。
- **Scale Out Threshold**（スケールアウトしきい値）—デフォルトを使用するか、またはスケールアウトしきい値を定義します。
- **Jumbo Frame**（ジャンボフレーム）—デフォルトでは無効になっています。

OK をクリックし、変更をコミットします。**Deploy**（デプロイ）ボタンが表示されるまでページを更新して、その後**Deploy**（デプロイ）をクリックしてデプロイを開始します。デプロイを開始すると、情報が**Deployments**（デプロイ）ページに表示されます。

デプロイが完了するまでに、約*15*～*20*分ほどかかります。

©2023 Palo Alto Networks, Inc.

STEP 6 | デプロイステータスを表示するには、**Azure** > **Deployments**（デプロイ）を選択します。

- Resource Group（リソースグループ）列には、プラグインが作成したリソースグループが表示されます。
- ファイアウォールの管理インターフェイスは、Firewall Access IP（ファイアウォールアクセスIP）を使ってPanoramaに接続します。Panoramaが設定の必要なしで接続できるように、このアドレスをホワイトリストに設定する必要があります。

  パブリッククラウドに *Panorama* をデプロイしている場合は、ファイアウォールアクセス *IP* を *Panorama* セキュリティグループに必ず追加してください。

  「Panorama用に使用されているポート」を参照して、トラフィックを許可するために開く必要があるポートを判断してください。
- 各スタックの詳細については、デプロイメントの詳細列のリンクを開いてください。
  - **Hub** スタック – デプロイメントからの出口トラフィックと、ファイアウォールからの管理トラフィックの NAT ゲートウェイは同じなので、Hub スタックパブリック IP は、デプロイメントサマリーのファイアウォールアクセス IP と一致します。

    すべてのアウトバウンドおよび East-West トラフィックは、検査のために出口プライベート **IP** にルーティングする必要があります。UDRを設定している場合、このアドレスにトラフィックを送信することができます。
  - インバウンドスタック – プライベート IP は、ファイアウォールに面している Azure 内部ロードバランサーのアドレスです。UDRを設定している場合、このアドレスにトラフィックを送信することができます。
- デプロイ情報とAzureのApplication Insights（アプリケーションの知見）を参照するには、リンクを使用してください。
- デプロイの詳細には、Success（成功）、Warning（警告）、およびFailure（失敗）などのメッセージが表示されます

STEP 7 | バックエンドTCP/UDPアプリケーション向けのインバウンド保護を設定します。

インバウンドファイアウォールスタックに面しているパブリックロードバランサーは、任意のバックエンドUDPまたはTCPアプリケーションのエントリーポイントになります。バック

 ©2023 Palo Alto Networks, Inc.

エンドアプリケーションにルーティングするために、プラグインが必要なロードバランサーおよびファイアウォール設定を管理できるように、次の設定を追加します。

1. **Azure** > **Deployments**（デプロイ）を選択して、デプロイ環境を選択します。
2. **Protect**（保護）タブを選択して、**Add**（追加）をクリックします。
3. アプリケーションの**Name**（名前）を指定して、**Protocol**（プロトコル）を選択します。

   保護の詳細を入力します:

   - **Frontend IP Type**（フロントエンド**IP**タイプ）—New Public IP（新しいパブリックIP）、Existing Frontend（既存のフロントエンド）、およびExisting Public IP（既存のパブリックIP）のいずれかを選択します。

     Existing Frontend（既存のフロントエンド）を選択した場合、**Frontend Name**（フロントエンド名）には、ロードバランサー上の既知のすべてのフロントエンドが表示されます。
   - **Resource Group**（リソースグループ）—（既存のパブリックIPのみ）ドロップダウンリストから、目的のフロントエンドIPアドレスが存在しているリソースグループを選択します。
   - IP Name（IP名）—（既存のパブリックIPのみ）IPをロードバランサーのフロントエンドにマップして、NATルールを作成するために使用します。
   - **Frontend Port**（フロントエンドポート）—パブリックロードバランサーでトラフィックを受信するように設定された、フロントエンドポートを追加します。
   - **Backend IP**（バックエンド**IP**）—バックエンドアプリケーションのIPアドレスを追加します。
   - **Backend Port**（バックエンドポート）—バックエンドアプリケーションがトラフィックを受信する予定のポートを追加します。

   OKをクリックします。
4. **Commit**（コミット）を選択して、ロードバランサーの設定を追加して、ファイアウォールにそれをプッシュ配信します。

©2023 Palo Alto Networks, Inc.

Azure用のカスタムVM-Seriesイメージの作成

後ほどAzureデプロイ環境で利用するために、カスタムVM-Seriesファイアウォールイメージを作成することができます。カスタムイメージにより、目的のバージョンのPAN-OSを使ってVM-Seriesファイアウォールを柔軟かつ一貫してデプロイすることができます。Azure Marketplaceから利用できるイメージのみに制限されることはありません。また、カスタムイメージに最新のコンテンツやウィルス対策のアップデートを含めることができます。

カスタムイメージを作成する場合、VHDを作成する前に、ユーザー設定、ユーザー、プラグイン設定など、すべてのプライベートデータを削除する必要があります。また、カスタムイメージを準備、作成するために、次の作業を行ってください。

カスタムイメージの作成に使われた*VM-Series*ファイアウォールが、プレミアムディスクタイプを使ってデプロイされている場合、カスタムイメージを使ってデプロイする*VM-Series*ファイアウォールは、同じプレミアムディスクタイプを使ってデプロイする必要があります。ただし、標準ディスクタイプを利用してデプロイされたファイアウォールを使ってイメージを作成した場合は、標準またはプレミアムのディスクタイプを使ってデプロイすることができます。

STEP 1 | Azureにログインします。

STEP 2 | Azure MarketplaceからVM-Seriesファイアウォールをデプロイします。

STEP 3 | （BYOLライセンスのみ）ライセンスをアクティブ化します。

STEP 4 | PAN-OS 10.0.3へのVM-Series ファイアウォールのアップグレードを行います。PAN-OS 10.0.3にアップグレードすると、VM-Seriesプラグインも2.0.3にアップグレードされます。

STEP 5 | Azure Marketplaceテンプレートに指定したユーザー名とパスワードを使って、SSH経由でVM-Seriesファイアウォールコマンドラインインターフェイスにアクセスします。

STEP 6 | VM-Seriesファイアウォールが、正しいPAN-OS、VM-Seriesプラグイン、コンテンツ、およびウィルス対策のバージョンを保有していることを確認します。

```
show system info
```

STEP 7 | （BYOLライセンスのみ）ライセンスを無効化します。

STEP 8 | VM-Seriesファイアウォール上でプライベートデータのリセットを実行します。このコマンドでは、ファイアウォールを再起動する必要があります。続行する前に、VM-Seriesファイアウォールが完全にリブートするまで待機する必要があります。リブートには、5～7分ほどかかることがあります。

```
request system private-data-reset
```


©2023 Palo Alto Networks, Inc.

STEP 9 | VM-Seriesインスタンスから、新しいVHDイメージを作成します。

1. Azure CLIにログインします。
2. 正しいサブスクリプションを使用していることを確認します。

   ```
   az account set --subscription <subscription-id>
   ```
3. VMを一般化して複数のデプロイに対してイメージを作成できるようにして、新しいVHDを作成するには次のコマンドを実行します。

   ```
   az vm deallocate --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az vm generalize --resource-group <myResourceGroup> --name
   <myVM>
   ```

STEP 10 | カスタムイメージから、新しいVM-Seriesファイアウォールを作成します。

```
az image create --resource-group <myResourceGroup> --name <myImage>
--source <resource-id-of-VM>
```

STEP 11 | カスタムイメージを使ってVM-Seriesファイアウォールをデプロイしたら、デプロイ環境を確認します。

1. 以前に使用した認証情報を使ってファイアウォールにログインする必要があります。
2. 正常にログインしたら、ファイアウォールが正しいバージョンのPAN-OSを実行しており、正しいコンテンツおよびウィルス対策のバージョンを保有していることを確認します。

   ```
   show system info
   ```

STEP 12 | （任意）カスタムイメージを他のリージョンにコピーします。

```
az image copy –source-resource-group <source-rg> –source-object-name
<pa-vm-image-name> –target-location <target-region> –target-resource-
group <destination-rg>
```

 ©2023 Palo Alto Networks, Inc.

Azure Security Center の推奨事項を使用してワークロードを保護

Microsoft は、パートナー セキュリティ ソリューション用の Azure Security Center サポートを廃止して、それに代わる Azure Sentinel を提供しました。

Azure Security Center が有効な Azure サブスクリプション内に新しいワークロードをデプロイする際、Azure Security Center により、これらのワークロードを 2 つの方法で保護できます。1 つ目の方法では、Azure Security Center が VM-Series ファイアウォールの新規インスタンスをデプロイしてインターネットに接続するアプリケーションのワークロードを保護することを推奨します。もう一つの方法では、Azure サブスクリプション内にデプロイした VM-Series ファイアウォール（パートナー セキュリティ ソリューション）を Azure Security Center が検出した後、追加の設定を行い、VM-Series ファイアウォールを Azure Security Center に接続してダッシュボードのアラートを表示できるようにする必要があります。統合および各ワークロードの利点と欠点の詳細については、Azure Security Center の統合を参照してください。

- Azure Security Center の推奨事項に基づいて VM-Series ファイアウォールをデプロイ
- Azure Security Center から既存の VM-Series ファイアウォールを接続

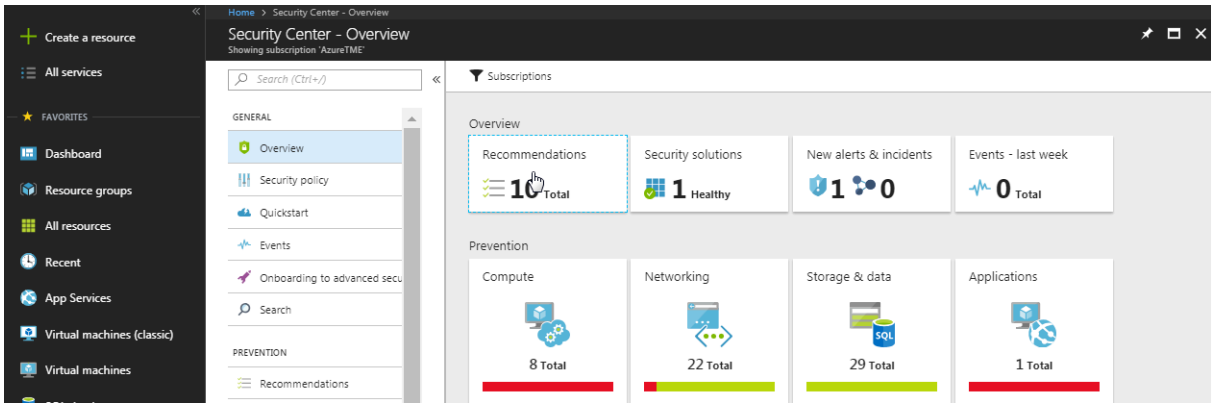
Azure Security Center の推奨事項に基づいて VM-Series ファイアウォールをデプロイ

Azure Security Center は Azure リソースをスキャンし、次世代ファイアウォールを必要とするワークロードを保護するための推奨事項を提示します。推奨事項がダッシュボードに表示された後、Azure Marketplace から VM-Series ファイアウォールの新規インスタンスをデプロイするか、Azure CLI、PowerShell、あるいは ARM テンプレートを使用できます。Azure CLI、PowerShell、あるいは ARM テンプレートを使用してカスタマイズされたデプロイメントを利用するメリットは、保護する必要があるワークロードと同じリソースグループ内に VM-Series ファイアウォールをデプロイできることです。Azure で Azure Marketplace を使用して VM-Series ファイアウォールをデプロイする際、ファイアウォールは新規リソースグループあるいは空のリソースグループにのみデプロイできます。そのため、マーケットプレイスのデプロイメントでは、保護するワークロードから来るトラフィックをその後で確実に別のリソースグループ内のファイアウォールへと向ける必要があります。

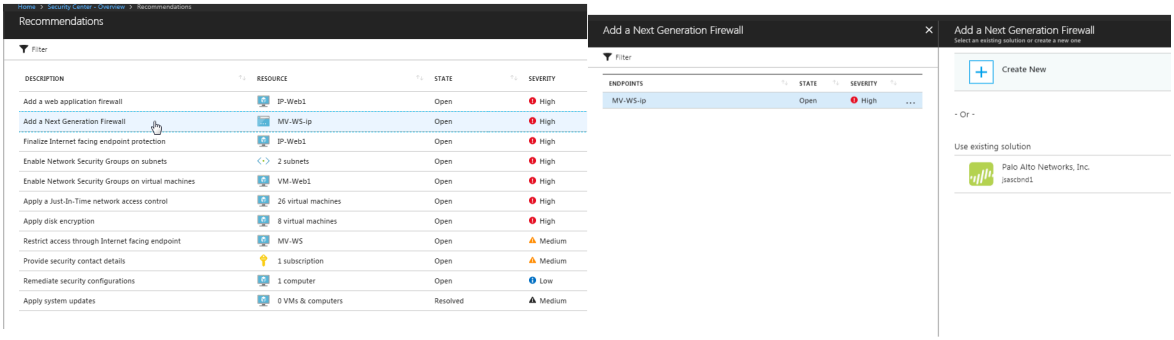
STEP 1 | Azure ポータルにログインし、Security Center のダッシュボードにアクセスします。

©2023 Palo Alto Networks, Inc.

STEP 2 | **Recommendations**（推奨）を選択します。



STEP 3 | **Add a Next Generation Firewall**（次世代ファイアウォールの追加）を選択し、さらに保護するワークロードを選択します。



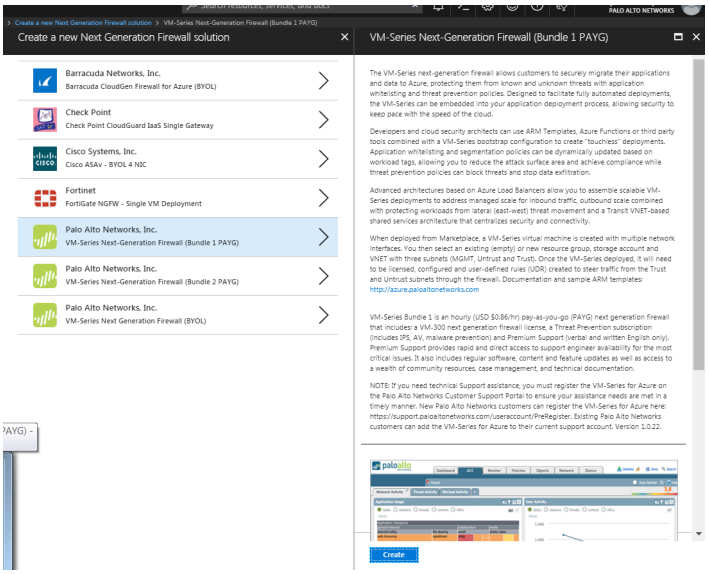
STEP 4 | VM-Series ファイアウォールの新規インスタンスをデプロイするのか、VM-Series ファイアウォールの既存のインスタンスを使用するのか選択します。

このワークフローを使用するには、インターネットにさらされたパブリック IP アドレスを持つワークロードを準備し、新しいリソースグループ内に VM-Series ファイアウォールのイン

©2023 Palo Alto Networks, Inc.

スタンスをデプロイします。その後、準備したワークロードを削除し、VM-Series ファイアウォールをデプロイしたリソースグループ内に本番用のワークロードをデプロイします。

- **Create New**（新規作成）する場合は、Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューション テンプレート）を参照してください。
- **Use existing solution**（既存のソリューションを使用）するには、以前にデプロイした VM-Series ファイアウォールを選択します。



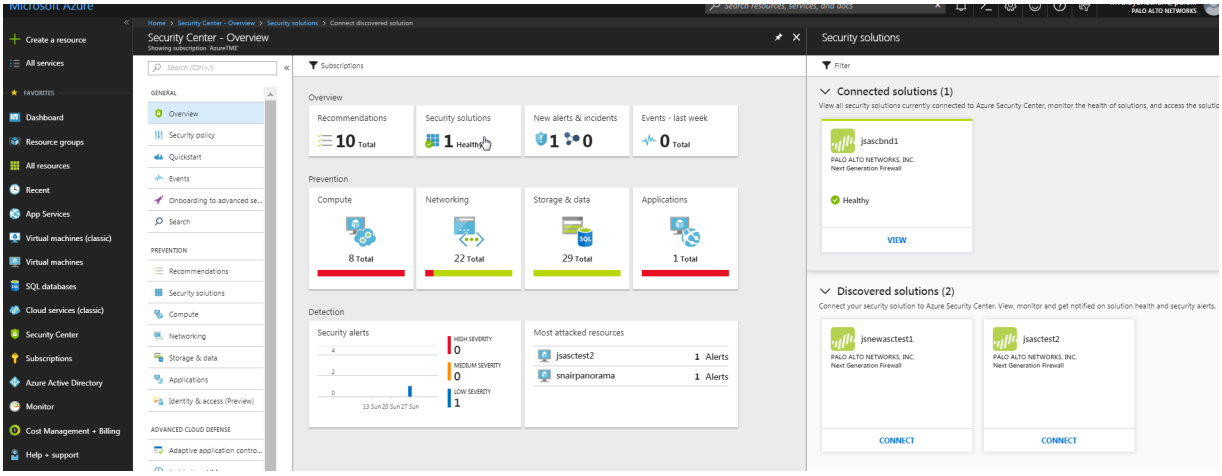
Azure Security Center から既存の VM-Series ファイアウォールを接続

Azure サブスクリプション内に VM-Series ファイアウォールがデプロイされたことを Azure Security Center が検出すると、そのファイアウォールがセキュリティ ソリューションとして表示されます。その後、Syslog 経由で Common Event Format（CEF）を使用して VM-Series ファイアウォールを Security Center に接続し、Security Center のダッシュボードでファイアウォールログをアラートとして表示できるようになります。

STEP 1 | Azure ポータルにログインし、Security Center のダッシュボードにアクセスします。

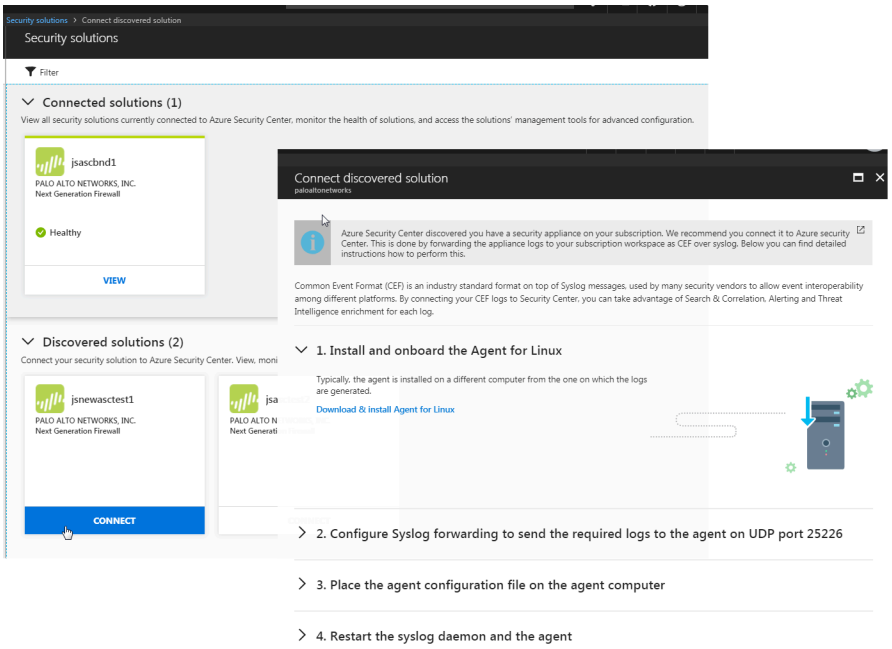
©2023 Palo Alto Networks, Inc.

STEP 2 | セキュリティ ソリューションを選択し、この Azure サブスクリプションの範囲で入手できる VM-Series ファイアウォールをすべて表示します。



STEP 3 | 見つかったソリューションの表示を展開し、保護したいワークロードと同じリソースグループに属す VM-Series ファイアウォールのインスタンスを選択し、**Connect**（接続）をクリックします。

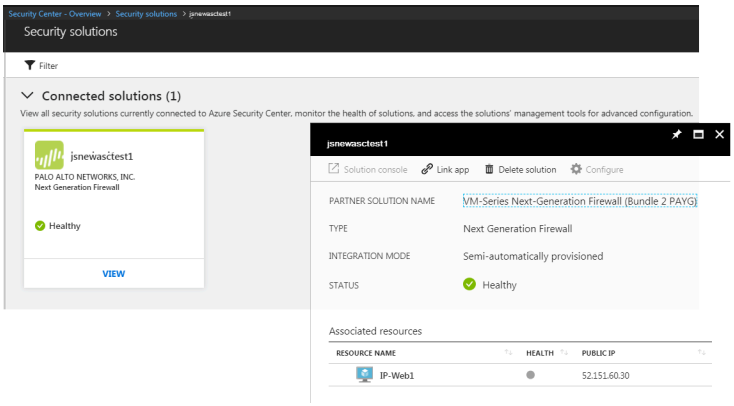
Security Center のダッシュボードでアラートとしてファイアウォール ログを表示するには、画面に表示される 4 ステップの作業を行う必要があります。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Series ファイアウォールが Security Center に正常に接続すると、Connected（接続済み）のソリューション一覧に VM-Series ファイアウォールが表示されます。

View（表示）をクリックし、保護する必要があるワークロードをファイアウォールが保護していることを確認します。



Panorama を使用して Azure Security Center にログを転送

Panorama を使用してファイアウォールを管理する場合は、テンプレートとデバイス グループを使用してファイアウォール ログを Azure Security Center に転送できます。デフォルトの Azure Security Center のログ転送プロファイルでは、ファイアウォールが生成した低、中、高、重要の重大度を持つ脅威および WildFire 送信ログが、Azure Security Center のダッシュボードにセキュリティ アラートとして表示されます。アラートをより効率的に集中化および優先順位付けできるように、重要なログ フィルターを設定して、関心のあるログのみを転送するか、重要度の高い重大度ログと重大度の高い重大度ログのみを転送できます。また、アプリケーションとセキュリティのニーズに基づいて、いくつかのセキュリティ ポリシー ルールにログ転送プロファイルを選択的にアタッチすることもできます。

Panorama からの Azure Security Center の統合を有効にするには、次の作業を行います。

STEP 1 | Panorama でファイアウォールを管理対象デバイスとして追加します。

STEP 2 | Panorama で、Azure Security Center にログを転送するファイアウォールにログ転送設定をプッシュするためのテンプレートと デバイス グループの作成を行います。

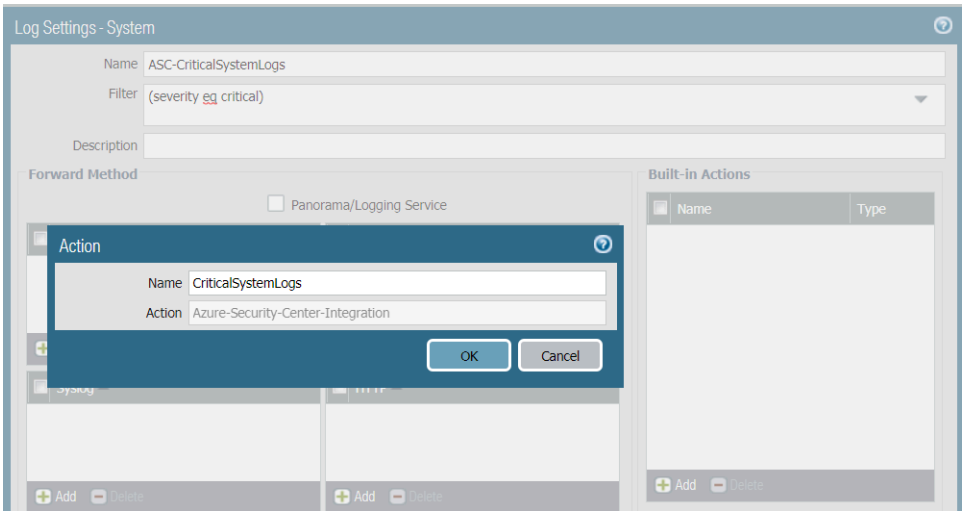
©2023 Palo Alto Networks, Inc.

STEP 3 | ロギング サービスに転送するログ タイプを指定します。

転送を有効にする方法は、ログ タイプによって異なります。ポリシー一致に基づいて生成されたログでは、デバイス グループ内でログ転送プロファイルを使用し、テンプレート内でログ設定を使用する他のログ タイプではログ転送プロファイルを使用します。

1. システム、設定、ユーザー ID、および HIP マッチ ログの転送を設定します。

   1. **Device**（デバイス） > **Log Settings**（ログ設定）を選択します。
   2. ロギング サービスにログを転送するファイアウォールを含む**Template**（テンプレート）を選択します。
   3. ログ サービスに転送する各ログ タイプに対して、一致リスト フィルターを **Add**（追加）します。**Name**（名前）を付け、さらに任意で **Filter**（フィルター）を定義します。
   4. ビルトイン アクションを **Add**（追加）し、**Name**（名前）を入力します。Azure-Security-Center-Integration アクションが自動的に選択されます。**OK** をクリックします。

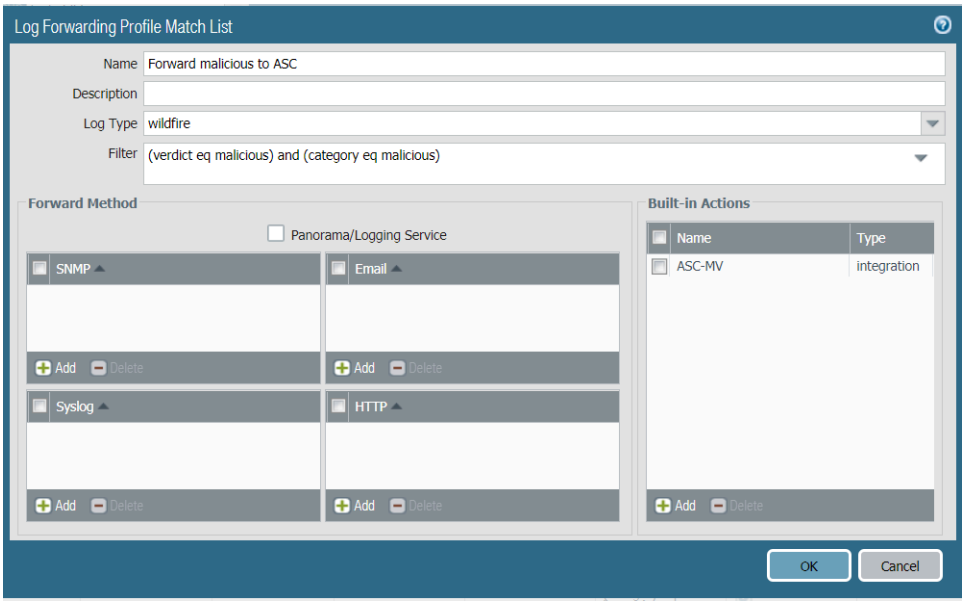
   5. **OK** をクリックします。

2. 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、認証ログなど、ポリシーの一致が発生したときに生成されるその他すべてのログ タイプの転送を設定します。これらのログを転送するには、ログを転送する各ポリシー ルールにログ転送プロファイルを作成してアタッチする必要があります。

   1. プロファイルを **Add**（追加）するには、**Device Group**（デバイス グループ）を選択してから、**Objects**（オブジェクト） > **Log Forwarding**（ログ転送）を選びます。ログ転送プロファイル一致リストで、転送する各ログ タイプを追加します。

©2023 Palo Alto Networks, Inc.

2. デバイス グループ内のファイアウォールがログを Azure Security Center に転送できるようにするには、ビルトイン アクションで **Add**（追加）を選択します。



3. 作成したばかりのデバイスグループに標準セキュリティ ポリシー ルールを作成し、**Actions**（操作）を選択して、ログを Azure Security Center に転送するために作成したログ転送プロファイルを添付します。ファイアウォールにインターフェイスとゾーンと基本的なセキュリティポリシーが用意されるまでは、トラフィックは通過せず、セキュリティ ポリシー ルールに一致するトラフィックのみがログに記録されます（デフォルト）。
4. 作成する各ルールごとに、**Actions**（操作）を選択して、 ファイアウォールがログを Azure Security Center に転送できるようにするログ転送プロファイルを選択します。

STEP 4 | 変更内容を Panorama にコミットして、作成したテンプレートとデバイス グループにプッシュします。

STEP 5 | ファイアウォール ログが Azure Security Center に転送されていることを確認します。

1. Azure ポータルにログインし、**Azure Security Center** を選択します。
2. Azure Securoty Center ダッシュボードでファイアウォール ログがセキュリティ アラートとして表示されていることを確認します。

©2023 Palo Alto Networks, Inc.

Azure Stack 上に VM-Series ファイアウォールをデプロイ

VM-Series ファイアウォールを Azure Stack 上にデプロイし、多層構造アーキテクチャにおけるアプリケーション間のインターサブネット トラフィック、および Azure Stack デプロイ環境においてサーバーから出るアウトバウンド トラフィックを保護できます。Azure Stack デプロイ環境においてサーバーに向かうインバウンドトラフィックを保護するゲートウェイとして VM-Series ファイアウォールを使用する場合、インバウンドトラフィックを受信してファイアウォールへと転送するファイアウォールの前に NAT アプライアンスをデプロイする必要があります。Azure Stack では VM-Series ファイアウォールなどの仮想マシンの非プライマリ インターフェイスにパブリック IP アドレスを割り当てられないため、NAT アプライアンスが必要になります。

Azure Stack 上の *VM-Series* ファイアウォールは、ブートストラップ、*Azure Application Insights*、*Azure Security Center* の統合をサポートしていません。

パブリックな Azure の場合と異なり、VM-Series ファイアウォールを Azure Stack にデプロイするためのソリューション テンプレートはありません。そのため、ARM テンプレートを使用して VM-Series ファイアウォールをデプロイする必要があります。GitHub 上でコミュニティによってサポートされているサンプル ARM テンプレートを最初に使用してから、本番用の独自の ARM テンプレートを作成できます。

STEP 1 | Azure から AzureStack に マーケットプレイスの項目をダウンロードします。

VM-Series ファイアウォールを Azure Stack 上へデプロイするには、8.1以降のPAN-OS イメージ の BYOL へアクセスできなくてはなりません。コネクテッドなデプロイ環境では、Azure Marketplace から Azure Stack に直接イメージをダウンロードできます。

STEP 2 | Azure Stack ポータルにアクセスします。

Azure Stack の運用者（サービスプロバイダーあるいは組織の管理者）が、ポータルにアクセスするための正しい URL を提供する必要があります。

STEP 3 | VM-Series ファイアウォールを展開します。

VM-Series ファイアウォール用のソリューション テンプレートは、Azure Stack では利用できません。そのため、前のステップでダウンロードしたイメージを ARM テンプレート内で参照し、VM-Series ファイアウォールをデプロイする必要があります。まずは、GitHub のコミュニティによってサポートされているポリシーの元で入手できるサンプル ARM テンプレートをデプロイできます。

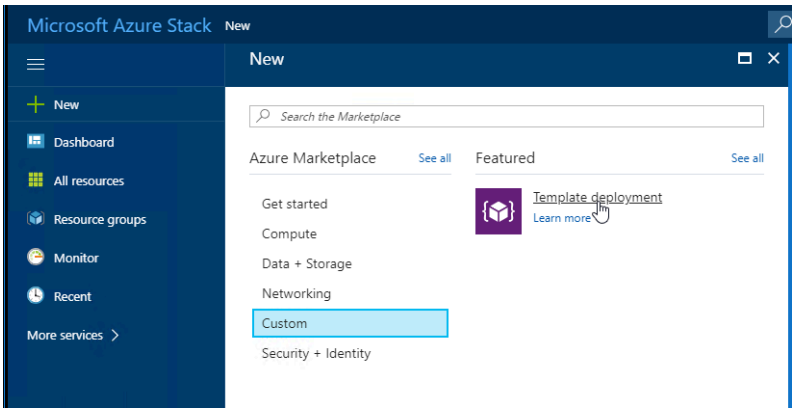
1. サンプルのAzure Stack GitHub テンプレートを入手します。
   - azurestackdeploy.json を選択してコンテンツを表示します。
   - Raw（生データ）をクリックして JSON ファイルのコンテンツをコピーします。
2. サンプルの GitHub テンプレートをデプロイします。

   ファイアウォールは、空の既存のリソース グループまたは新しいリソース グループにデプロイできます。テンプレート内のデフォルト VNet は 192.168.0.0/16 で、デ

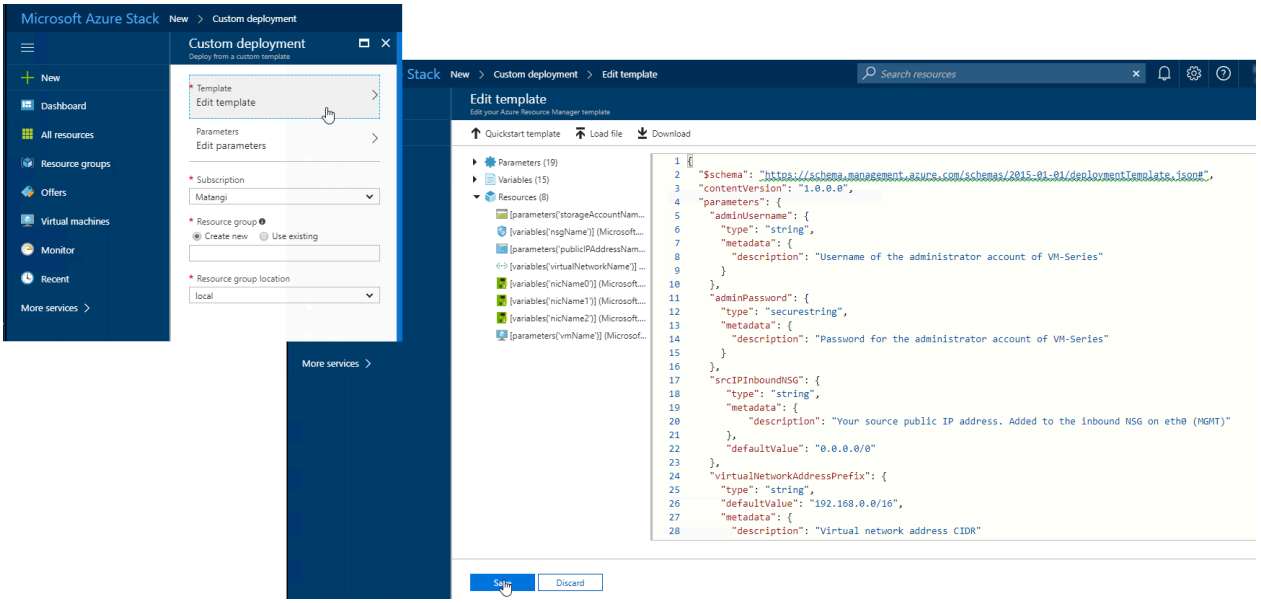
©2023 Palo Alto Networks, Inc.

プロイする VM-Series ファイアウォールには 3 つのネットワーク インターフェイスがあります（1 つは 192.168.0.0/24 サブネット上の管理インターフェイス、2 つは 192.168.1.0/24 および 192.168.2.0/24 サブネット上のデータプレーン インターフェイス）。これらのサブネットは、ニーズに合わせてカスタマイズできます。

- Azure Stack ポータルにログインします。
- **New**（新規） > **Custom**（カスタム） > **Template deployment**（テンプレート デプロイメント）を選択します。

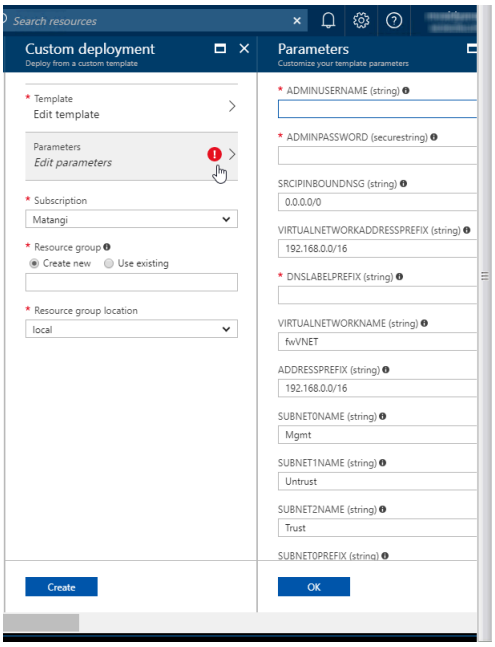


- **Edit template**（テンプレートを編集）し、テンプレート内の既存のコンテンツをすべて削除し、以前にコピーした JSON テンプレートのコンテンツを貼り付けて**Save**（保存）します。

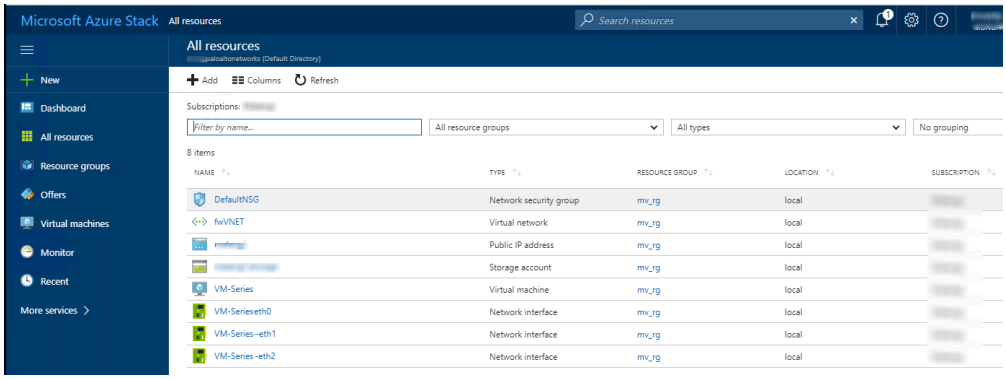


 ©2023 Palo Alto Networks, Inc.

- **Edit parameters**（パラメータを編集）し、必要なパラメータの値を入力し、必要に応じてデフォルトの値を変更して**OK**をクリックします。



- 使用したい**Subscription**（サブスクリプション）を選択してから**OK**をクリックします。
- 既存の空の**Resource Group**（リソースグループ）を選択するか、新しいものを作成して**OK**をクリックします。
- **Create**（作成）をクリックします。ダッシュボードの新しいタイルに、テンプレートのデプロイの進捗状況が表示されます。



STEP 4 | 次のステップ：

1. ファイアウォールの Web インターフェイスにログインします。

   Web ブラウザから安全な接続（https）を使用し、その DNS 名を使用してファイアウォールにログインします。以前に定義したユーザー名/パスワードを入力します。証

©2023 Palo Alto Networks, Inc.

明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。

2. VM-Series ファイアウォールでライセンスをアクティベートします。

   1. サポート アカウントを作成し、VM-Series ファイアウォールを登録（認証コードを使用）します。
   2. ファイアウォールの Web インターフェイスで **Device**（デバイス） > **Licenses**（ライセンス）を選択し、**Activate feature using authentication code**（認証コードを使用して機能をアクティベート）を選択します。
   3. サポート ポータルで登録したキャパシティ認証コードを入力します。ファイアウォールが更新サーバー（updates.paloaltonetworks.com）に接続され、ライセンスがダウンロードされてから自動的に再起動します。
   4. **Dashboard**（ダッシュボード）で Web インターフェイスにログインし直し、有効な**Serial#**（シリアル番号）が表示されることを確認します。

      VM Mode（**VM** モード）に Microsoft Azure と表示されます。

      Unknown（不明）と表示されている場合、デバイスはライセンスされていません。ファイアウォール上のトラフィック ログを確認するには、有効なキャパシティ ライセンスをインストールする必要があります。

STEP 5 | 7

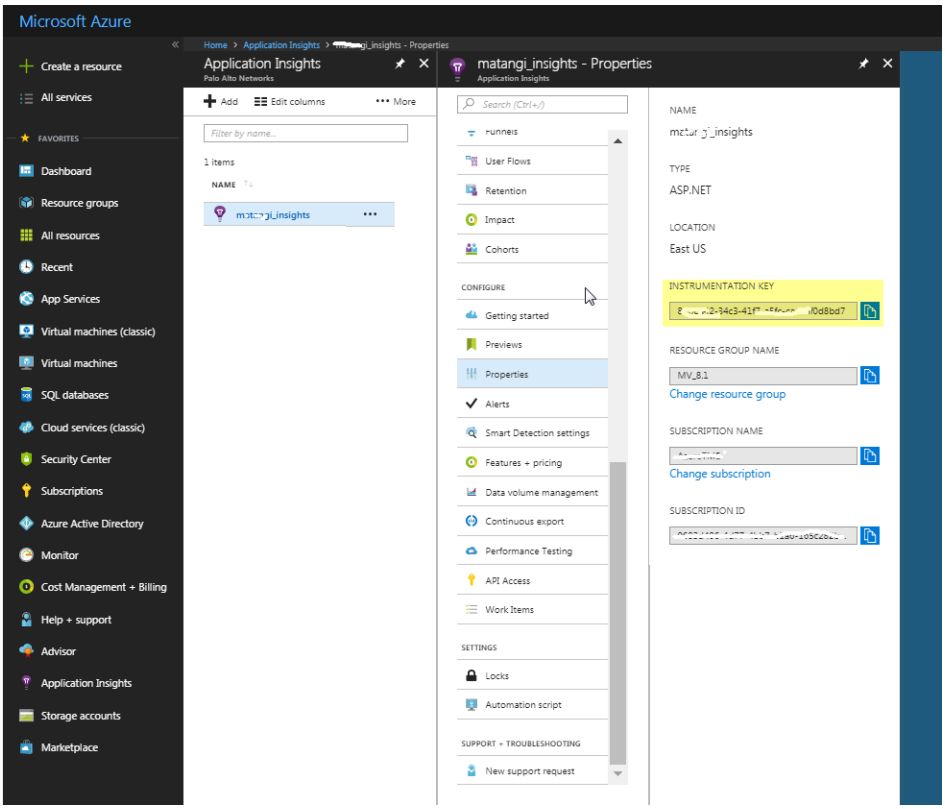
©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールでの Azure Application Insights の有効化

Azure 上の VM-Series ファイアウォールは、Azure ポータルから直接ファイアウォールを監視するために使用できる、Azure Application Insights にネイティブにカスタム PAN-OS メトリックを公開できます。これらのメトリックを使用すると、アラームを設定したり、VM-Series ファイアウォールのインスタンスの起動や終了などのイベントを自動化するためのアクションを実行するためのパフォーマンスや使用パターンを評価できます。利用可能なメトリックの説明については、「監視用に公開されるカスタム PAN-OS メトリック」を参照してください。

STEP 1 | Azure ポータルで、ファイアウォールを監視するための Application Insights インスタンスを作成して、**Configure**（設定） > **Properties**（プロパティ）から **Instrumentation Key**（インストルメンテーション キー）をコピーします。

ファイアウォールは、Application Insights インスタンスを認証し、そのインスタンスに対してメトリックを公開するために、このキーを必要とします。必要なアクセス許可については、「Azure 上の VM-Series のサービス プリンシパル アクセス許可」を参照してください。

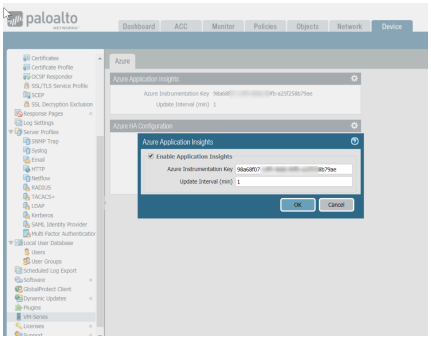


 ©2023 Palo Alto Networks, Inc.

STEP 2 | ファイアウォールがメトリックを Application Insight インスタンスに公開できるようにします。

1. Azure 上の VM-Series ファイアウォールにログインします。
2. **Device**（デバイス） > **VM-Series** > **Azure**を選択します。
3. **Azure Application Insights** を編集して、以前にコピーしたインストルメンテーションキーを入力してください。

   デフォルトのメトリック公開間隔は 5 分です。これは 1～60 分の範囲で変更することができます。



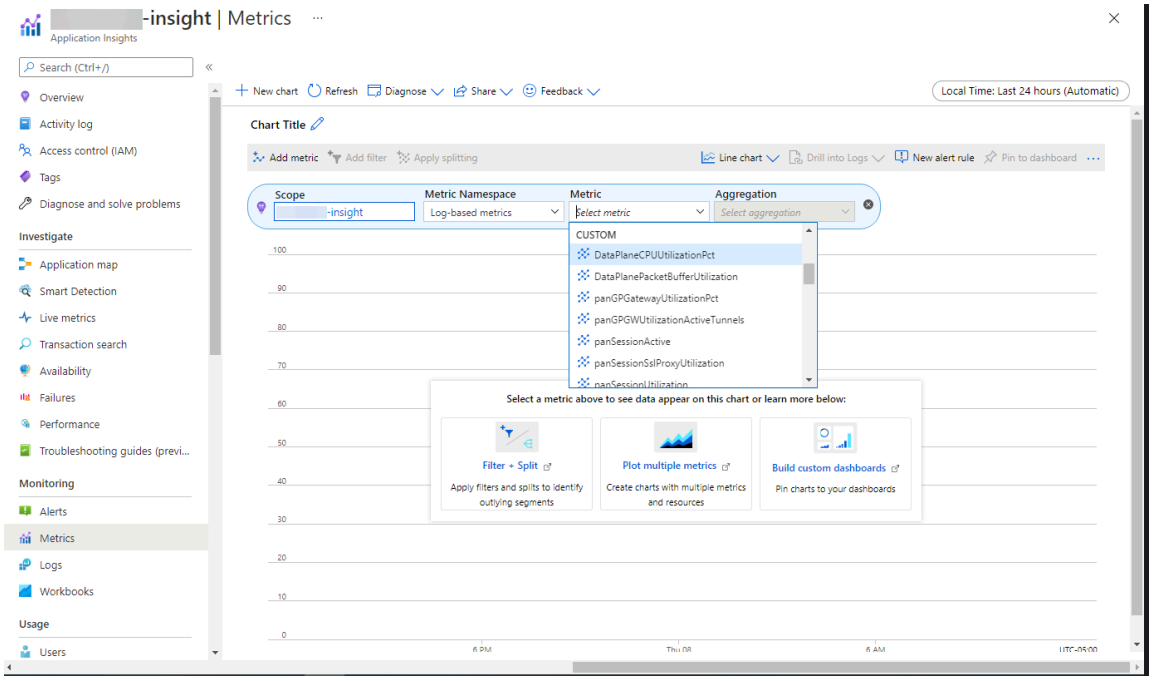
4. 変更を **Commit**（コミット）します。

   ファイアウォールは、システム ログを生成して、Azure Application Insights への認証の成功または失敗を記録します。

©2023 Palo Alto Networks, Inc.

STEP 3 | Azure Application Insights ダッシュボードでメトリックを表示できることを確認します。

1. PAN-OS カスタムメトリックを表示するには、Azure ポータルで Application Insights インスタンスを選択し、モニタリング > メトリックを選択します。



2. トレンドを監視し、アラートをトリガーするメトリックを選択します。Application Insight のメトリックの詳細については、Microsoft Azure のドキュメントを参照してください。

 ©2023 Palo Alto Networks, Inc.

Azureでのモニタリング

Microsoft® Azure® 上の VM 監視により、セキュリティ ポリシー ルールを動的に更新して、Azure サブスクリプション内にデプロイされたすべてのアセットにセキュリティ ポリシーを一貫して適用することができます。この機能を有効化するには、Panorama plugin for Azureをインストールし、Panorama および Azure サブスクリプション間の API 通信を有効化する必要があります。その後、Panoramaがすべてのアセットの IP アドレスとタグのマッピングを収集し、Azureリソース情報をPalo Alto Networks®ファイアウォールにプッシュあるいは配信できるようになります。

- Azure 上のモニタリングについて
- Panorama上のモニタリング用Azureプラグインのセットアップ
- Azure 上で Panorama プラグインを使用して監視される属性

Azure 上のモニタリングについて

Azure パブリック クラウドで仮想マシンをデプロイあるいは停止する際、Azure 用の Panorama プラグインを使用し、それらのワークロードに対して一貫した形でセキュリティポリシールールを適用できます。

スケーリングが可能な Azure 用の Panorama プラグインを使えば、Azure パブリック クラウド上で最大 100 件のAzure サブスクリプションを監視できます。このプラグインと共に Panorama をタグのサブスクリプションをポーリングするためのアンカーとして使用してから、メタデータ（IP アドレス対タグのマッピング）をデバイスグループ内の多くのファイアウォールに配信します。PanoramaはAzureサブスクリプションと通信してAzureリソース情報を取得するため、クラウド環境に対して行う API コール数を合理化することができます。ファイアウォールのローカルでセキュリティポリシーを定義することもできますが、Panorama およびプラグインを使用することで、セキュリティポリシーの管理を一元的に行い、ハイブリッドおよびクラウド ネイティブなアーキテクチャに対して一貫した形でポリシーを適用できるようになります。

互換性マトリックスの Panorama プラグインのバージョン情報を参照してください。

Panorama上のモニタリング用Azureプラグインのセットアップ

組織がAzureクラウドにデプロイしたすべてのワークロードを確認するためには、Azure Plugin on Panoramaをインストールし、モニタリング定義を構成して、PanoramaがAzureサブスクリプションに認証して対象の Azure ワークロードに関する情報を取得できるようにする必要があります。Panoramaは、Azureリソースのプライマリプライベート IPアドレスおよび関連するタグを取得します。Panorama がサポートしているメタデータ要素のリストについては、Azure 上で Panorama プラグインを使用して監視される属性を参照してください。

Panorama が属性を取得した後、リソース情報を Panorama からファイアウォールにプッシュするためには、ファイアウォール（ハードウェアあるいは VM-Series）を管理対象のデバイスとして Panorama 上に追加し、ファイアウォールを一つあるいは複数のデバイスグループにグループ化する必要があります。その後、Panorama が Azure から取得する IP アドレス対タグのマッピングを登録するために使用する、通知グループに含まれるデバイスグループはどれで、モニタリング定義内の設定要素がどれなのかを指定できます。

©2023 Palo Alto Networks, Inc.

最後に、Azureのワークロード全体で一貫した形でセキュリティポリシーを適用するために、ダイナミックアドレスグループをセットアップし、AzureリソースのIPアドレスに向かうトラフィックを許可あるいは拒否するポリシールール内でそれらを参照する必要があります。Panorama 上でダイナミック アドレス グループおよびセキュリティポリシールールを定義し、各ファイアウォールのローカルでダイナミック アドレス グループおよびセキュリティポリシールールを管理する代わりに、それらをファイアウォールにプッシュすることで、Panoramaで一元的に行うポリシーおよびオブジェクトの管理や設定を合理化できます。

*Azure*プラグインは、*Azure*パブリッククラウド上の*Azure*リソースの監視に使用します。*Azure Government*または*Azure China*はサポートされていません。

- Azure プラグインを使用する VM モニタリングのためのチェックリストのプランニング
- Azure プラグインのインストール
- モニタリング用Azureプラグインの設定

Azureプラグインを使用するモニタリングのチェックリストのプランニング

- アクティブディレクトリ アプリケーションおよびサービス プリンシパルをセットアップして API アクセスを有効化します。Panorama が Azure API と通信してワークロードの情報を収集できるようにするには、Azure アクティブディレクトリのサービス プリンシパルを作成する必要があります。このサービス プリンシパルは、Azure AD に認証してサブスクリプション内のリソースにアクセスするために必要な権限を持っています。

  このセットアップを完了させるには、Azure AD テナントを使ってアプリケーションを登録する権限、アプリケーションをサブスクリプション内のロールに適用する権限が必要になります。必要な権限を持っていない場合は、Azure AD あるいはサブスクリプションの管理者に閲覧者の IAM ロールまたは「Azure 上の VM-Series のサービス プリンシパル アクセス許可」に記載されているカスタム アクセス許可を持つサービス プリンシパルを作成してもらってください。
- サービス プリンシパル全体を通じてサブスクリプション ID が一意であることを確認します。Panorama では、単一のサービス プリンシパルのみを使用して Azure サブスクリプションを監視できます。100 件のサービス プリンシパル リソースと共に最大 100 件の Azure サブスクリプションを監視できます。
- Panorama 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あるいは仮想システムに最大 8000 件の IP アドレス対タグのマッピングをプッシュできます。Panorama および管理対象のファイアウォールの要件を確認してください：
  - 最低システム要件（互換性マトリックスの Panorama プラグインの情報を参照）：

    Panorama 仮想アプライアンス、またはPanorama 8.1.3 以降が動作するハードウェア ベースの Panorama アプライアンス、および管理対象ファイアウォールに対するアクティブなサポート ライセンスとデバイス管理ライセンス。

    PAN-OS 8.0 または 8.1 が動作している、ライセンスを持つ次世代ファイアウォール。
  - Panorama上にファイアウォールを管理対象デバイスとして追加してデバイスグループを作成し、Panoramaが取得した情報をそれらのグループに通知するよう設定できるようにす

 ©2023 Palo Alto Networks, Inc.

る必要があります。デバイスグループには、VM-Series ファイアウォールやハードウェアファイアウォール上の仮想システムも含められます。

- Panorama プラグインが取得、登録できるタグ数を以下に示します。

  PAN-OS 8.1.3 以下が動作するファイアウォールを管理している 8.1.3 以降が動作している Panoramaで、デバイス グループ内に含まれているファイアウォールまたは仮想システムは、7000 件の IP アドレスと、それぞれ 10 件のタグ、または 6500 件の IP アドレスと、それぞれ 15 件のタグを保有することができます。

  PAN-OS 8.0.x が動作しているファイアウォールを管理している Panorama 8.1.3 以降の場合、2500 件の IP アドレスと、それぞれ 10 件のタグを保有できます。

  - Panorama アプライアンスが高可用性構成である場合、両方の Panorama ピアに同じバージョンの Azure プラグインを手作業でインストールする必要があります。

    Azure プラグインは、アクティブ *Panorama* ピア上でのみ構成します。コミット時に設定はパッシブ *Panorama* ピアと同期されます。モニタリング用に構成した*Azure*サブスクリプションにポーリングを行うのは、アクティブ*Panorama*ピアだけです。

Azure プラグインのインストール

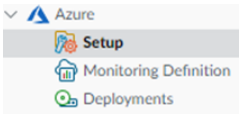
Azure上でモニタリングを始めるにあたり、Azure Plugin on Panoramaをダウンロードおよびインストールする必要があります。Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。

すでに *Panorama* プラグインをインストールしている場合、別のプラグインをインストール（あるいはアンインストール）する際に、変更をコミットするために *Panorama* の再起動が必要になります。そのため、再起動を行えるよう、予定されている保守期間中に追加のプラグインのインストールを行ってください。

STEP 1 | Panorama Web インターフェイスにログインし、**Panorama** > **Plugins**（プラグイン）を選択して**Check Now**（今すぐチェック）をクリックし、利用できるプラグインのリストを入手します。

STEP 2 | **Download**（ダウンロード）を選択してプラグインを**Install**（インストール）します。

インストールが正常に完了したら Panorama が更新され、**Panorama**タブに Azure プラグインが表示されます。



STEP 3 | Panorama を再起動します。

Panorama > **Setup**（セットアップ） > **Operations**（操作） > **Reboot Panorama**（**Panorama** の再起動）を選択します。

 ©2023 Palo Alto Networks, Inc.

モニタリング用Azureプラグインの設定

Azureパブリッククラウドのデプロイ環境でリソースの監視を始めるためには、Azure プラグインのインストール後、モニタリング定義を作成する必要があります。この定義は、監視する Azure サブスクリプション内のリソースにアクセスする権限を持つサービス プリンシパル、Panorama が取得した IP アドレス対タグのマッピングのプッシュ先となるファイアウォールを含む通知グループを指定します。ポリシーを適用するためには、その後でダイナミック アドレス グループを作成し、それらをセキュリティポリシー内で参照する必要があります。ダイナミック アドレス グループにより、ファイアウォールがタグ用に登録されているプライマリ プライベート IP アドレスを取得してから、定義済みのポリシールールに基づいてワークロードを出入りするトラフィックに対してアクセスを許可あるいは拒否できるよう、マッチさせたいタグをフィルタリングすることができます。

STEP 1 | Panorama Web インターフェイスにログインします。

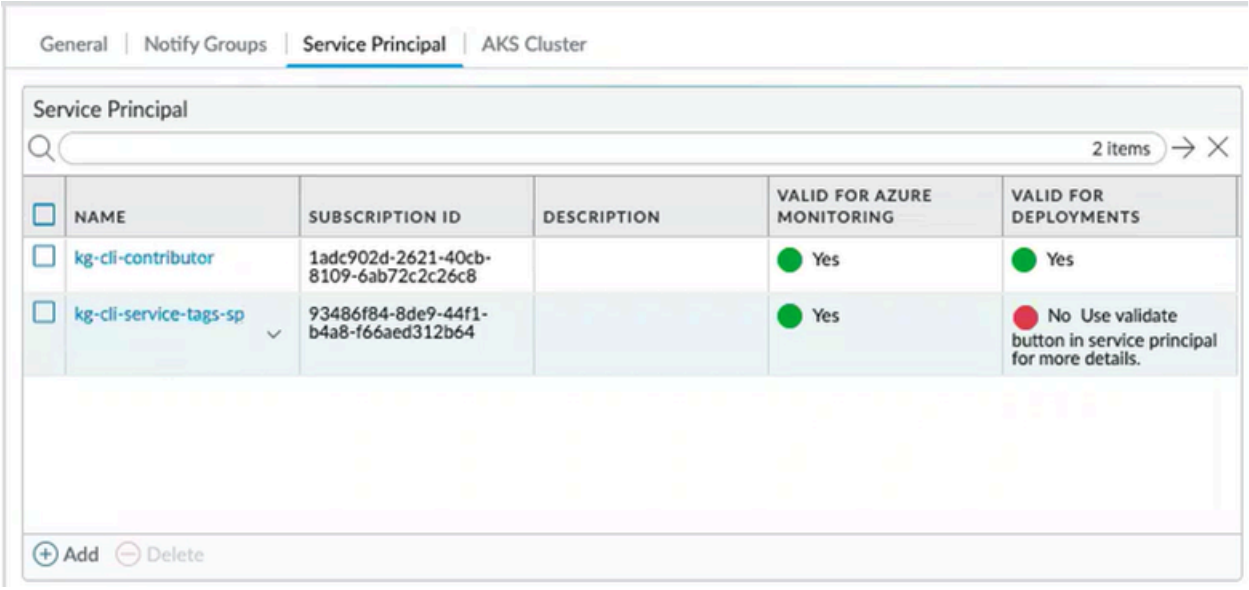
©2023 Palo Alto Networks, Inc.

STEP 2 | 次のオブジェクトをセットアップし、Azure上のモニタリングを有効化します。

- サービス プリンシパルを追加します。

  サービス プリンシパルは、Azure ポータルで作成したサービス アカウントです。Azure AD に付与されるこのアカウントは、Azure サブスクリプション内のリソースにアクセスして管理できる制限付きの権限を持っています。

  1. **Panorama** > **Plugins**（プラグイン） > **Azure** > **Setup**（セットアップ） > **Service Principal**（サービス プリンシパル） > **Add**（追加）を選択します。

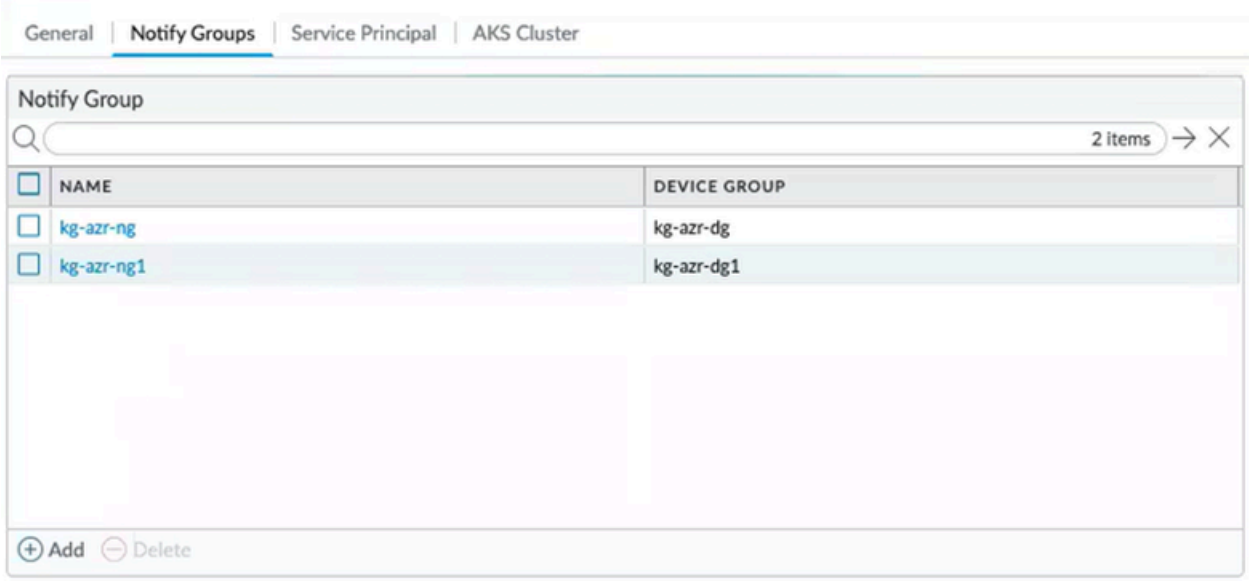


  2. サービス アカウントを識別する**Name**（名前）および任意で**Description**（説明）を入力します。
  3. 監視する Azure サブスクリプションの**Subscription ID**（サブスクリプション **ID**）を入力します。Azure ポータルにログインしてこのサブスクリプション ID を取得する必要があります。
  4. **Client Secret**（クライアント シークレット）を入力し、確認用に再び入力します。
  5. **Tenant ID**（テナント **ID**）を入力します。テナント ID は、アクティブディレクトリ アプリケーションをセットアップする際に保存したディレクトリ ID です。
  6. **Validate**（検証）をクリックし、入力したキーおよび ID が有効であり、Panorama が API を使用して Azure サブスクリプション と通信できることを確認します。

- 通知グループを追加します。

  1. **Panorama** > **Plugins**（プラグイン） > **Azure** > **Setup**（セットアップ） > **Notify Groups**（通知グループ） > **Add**（追加）を選択します。

©2023 Palo Alto Networks, Inc.



2. Panoramaが取得した情報のプッシュ先にするファイアウォールのグループを識別する**Name**（名前）、および任意で**Description**（説明）を入力します。
3. PanoramaがAzureサブスクリプションから取得した情報（IPアドレス対タグのマッピング）のプッシュ先にするファイアウォールのグループあるいは仮想システムである**Device Groups**（デバイスグループ）を選択します。ファイアウォールは、更新を使用してポリシーで参照しているダイナミック アドレス グループを構成する最新メンバー リストを決定します。

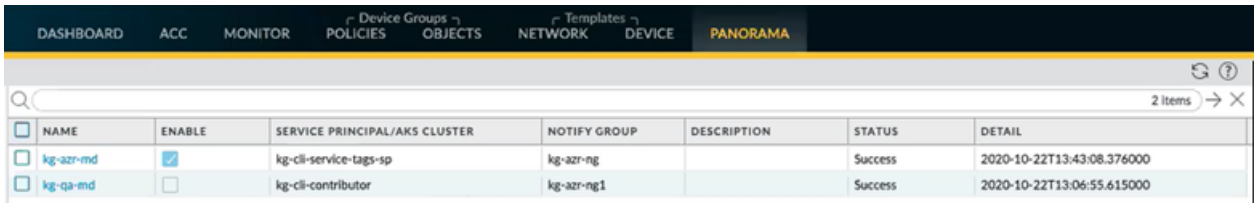
   デバイスグループはよくご検討ください。

   - モニタリング定義に含められる通知グループは一つだけであるため、通知グループ内の関連するデバイスグループをすべて選択するようにしてください。通知グループに含まれるファイアウォールに Panorama がプッシュしたタグを登録解除する場合、モニタリング定義を削除する必要があります。
   - 複数の仮想システムで有効なファイアウォール上のすべての仮想システムにタグを登録するためには、各仮想システムを Panorama 上の別のデバイスグループに追加し、デバイスグループを通知グループに割り当てる必要があります。すべての仮想システムを単一のデバイスグループに割り当てる場合、Panorama はタグを単一の仮想システムにのみ登録します。
4. プラグイン上で監視が有効化されていることを確認します。PanoramaがAzureパブリッククラウドと通信してモニタリングを行うために、この設定を有効化する必要があります。

   Enable Monitoring（監視の有効化）チェックボックスは、**Panorama** > **Plugins**（プラグイン） > **Azure** > **Setup**（セットアップ） > **General**（一般）にあります。

©2023 Palo Alto Networks, Inc.

STEP 3 | **Monitoring Definition**（モニタリング定義）を作成します。



新しいモニタリング定義を追加すると、デフォルトで有効になります。

- **Panorama** > **Plugins**（プラグイン） > **Azure** > **Monitoring Definition**（モニタリング定義）を選択し、新しい定義を **Add**（追加）します。
- この定義を使用する Azure サブスクリプションを識別する**Name**（名前）、および任意で**Description**（説明）を入力します。
- **IService Principal**（サービス プリンシパル）および**Notify Group**（通知グループ）を選択します。

  ワークロードの情報を収集するための API コールのヘッダーで使用する Azure Bearer Token を生成するために、Panorama にはサービス プリンシパル設定で指定するキーおよび ID が必要になります。

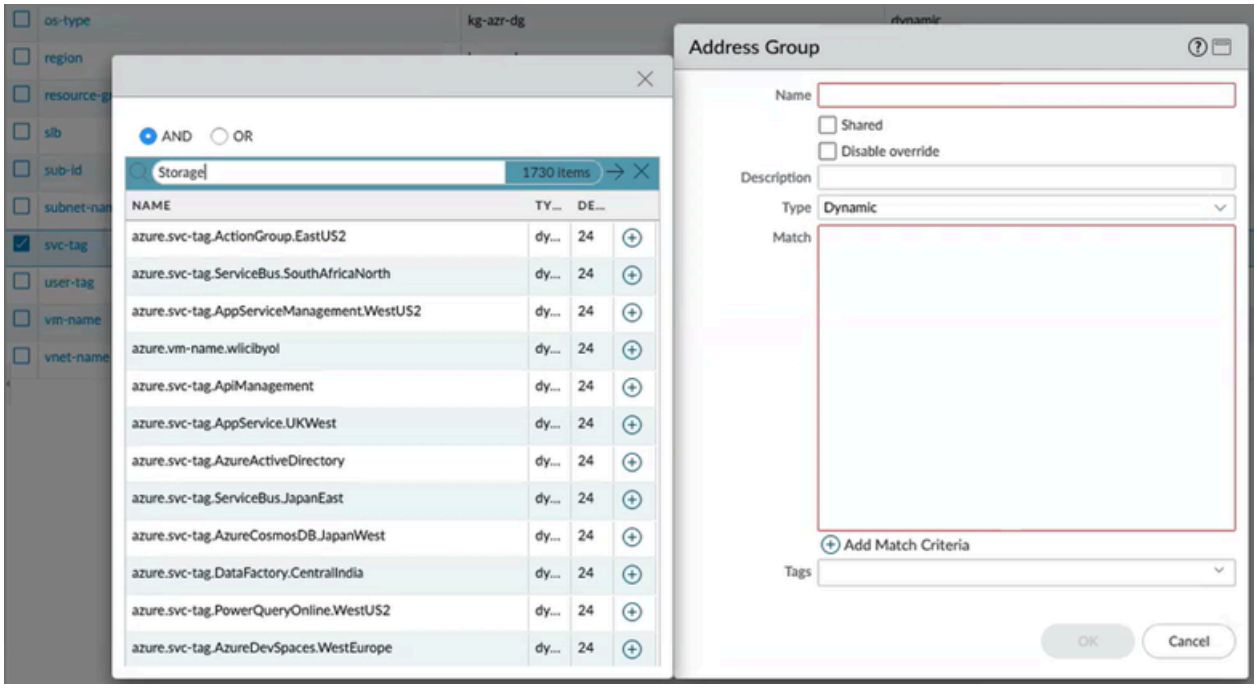
STEP 4 | Panorama 上の変更を**Commit**（コミット）します。

モニタリング定義のステータスが Success（成功）と表示されることを確認します。失敗する場合、Azure サブスクリプション ID を正しく入力し、サービス プリンシパル用の正しいキーおよび ID を指定しているかどうか確認してください。

©2023 Palo Alto Networks, Inc.

STEP 5 | Panoramaで情報を閲覧できることを確認し、ダイナミックアドレスグループ用の一致条件を定義します。

一部のブラウザ拡張機能が、*Panorama* と *Azure* の間の *API* コールをブロックすることがあります。これが原因で、*Panorama* は一致条件を受信できなくなります。ブラウザ拡張機能を使用しているときに *Panorama* で一致条件が表示されない場合は、その拡張機能と *Synchronize Dynamic Objects*（動的オブジェクトの同期）を無効にして、*Panorama* に対して使用可能なタグを取り込みます。



©2023 Palo Alto Networks, Inc.

HA フェイルオーバーの際、新たにアクティブになった *Panorama* が *Azure* クラウドに再接続してすべてのモニタリング定義のタグを取得しようと試みます。単一のモニタリング定義に再接続する際にもエラーが発生する場合、*Panorama* はシステム ログのメッセージを生成します。

```
Unable to process subscriptions after HA switch-over;
 user-intervention required.
```

このエラーが発生する場合は *Panorama* にログインし、無効なサブスクリプションを削除したり有効な認証情報を指定したりするなどして問題を解決し、変更をコミットし、*Panorama* が再接続してすべてのモニタリング定義を取得できるようにする必要があります。*Panorama* が *Azure* クラウドに接続されていない状態でも、ファイアウォールはフェイルオーバー前に取得していたすべてのタグのリストを保持しており、その *IP* アドレスのリストに対して継続してポリシーを適用できます。*Panorama* は、モニタリング定義を削除する際にのみ、サブスクリプションに関連するすべてのタグを削除します。ベストプラクティスとして、アクション中心のHTTPS 宛先へのログ転送を設定して即座に対応できるようにすることで、この問題を監視します。

Azure 上で Panorama プラグインを使用して監視される属性

Azure 用の Panorama プラグインを使用する際、Panorama は Microsoft® Azure® デプロイメントの仮想マシン上で、次の一連のメタデータ要素または属性を収集します。各VMにつき合計32件のタグ（事前定義済みのタグが11、ユーザー定義のタグが最大21）を取得できます。

タグの最大文字数は *127* 文字です。*Panorama* が *127* 文字を超過しているタグを取得してファイアウォールに登録することはありません。また、タグに「{」や「"」などの、非*ASCII*特殊文字を使用することはできません。

次の属性は、すべてのバージョンのAzure用Panoramaプラグインで監視されます。

仮想マシン

VM 監視	例
VM 名	azure-tag.vm-name.web_server1
Network Security Group Name（ネットワーク セキュリティ グループ名）	azure-tag.nsg-name.myNSG
OS Type（OSタイプ）	azure-tag.os-type.Linux
OS パブリッシャー	azure-tag.os-publisher.Canonical

©2023 Palo Alto Networks, Inc.

VM 監視	例
OS オファー	azure-tag.os-offer.UbuntuServer
OS SKU	azure-tag.os-sku.14.04.5-LTS
サブネット	azure-tag.subnet.webtier
VNet	azure-tag.vnet.untrustnet
Azure リージョン	azure-tag.region.east-us
リソース グループ名	azure-tag.resource-group.myResourceGroup
サブスクリプション**ID**	azure.sub-id.93486f84-8de9-44f1-b4a8-f66aed312b64
ユーザー定義のタグ 最大 21 件のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 21 件のタグを Panorama およびファイアウォールで使用できます。	azure-tag.mytag.value

ロードバランサー

Azureバージョン3.0以降のPanoramaプラグインは、各アプリケーションゲートウェイおよび標準のロードバランサーに対するタグをサポートしています（パブリックIPアドレスとプライベートIPアドレスの両方）。各ロードバランサーには、リソースグループ、ロードバランサー名、およびリージョンに対する事前定義タグが用意されています。また、ロードバランシングに固有のユーザー定義タグを、最高21件までサポートしています。

ロードバランサーのタグ	例
ロードバランサー	azure.<type>.myLoadBalancer
Azure リージョン	azure-tag.region.east-us
リソース グループ名	azure-tag.resource-group.myResourceGroup
ユーザー定義のタグ 最大 21 件のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 21 件のタグを Panorama	azure-tag.mytag.value

©2023 Palo Alto Networks, Inc.

ロードバランサーのタグ	例
およびファイアウォールで使用できます。	

Subnet/VNET

Azureバージョン3.0以降上のPanoramaプラグインは、サブスクリプション内の各サブネットおよびVNETに対するタグをサポートしています。各サブネットタグとVNETタグは、完全なIP CIDR範囲と関連付けられているので、個別のIPアドレスの代わりにCIDR範囲に基づいてポリシーを作成することができます。プラグインはサブスクリプション内の各サブネットおよびVNETをクエリして、そのタグを作成します。

サブネットおよび**VNET**タグ	例
サブネット名	azure.subnet-name.web
VNET名	azure.vnet-name.myvnet

サービスタグのモニタリング

Azureバージョン3.0のPanoramaプラグインは、サービスタグをサポートしています。

Azureサービスタグを利用すると、使用するAzureサービスのみにネットワークアクセスを制限できるため、Azure仮想マシンとAzure仮想ネットワークのセキュリティを簡素化できます。サービスタグは、特定のAzureサービスのIPアドレスプレフィックスのグループを表しています。たとえば、すべてのストレージIPアドレスを表すタグを利用できます。

プラグインは毎日APIコールを行って（UTCで午前5:00）、Azureポータルからすべてのサービスタグを取得し、ペイロードを解析してIPとサービスのマッピングを作成し、それをプラグインデータベースに保管します。マッピングはconfigdに渡され、次にPanorama上に送られます。APIコールによるサービス情報の取得が失敗した場合は、**service_tags_public.json**の内容からIPとサービスのマッピングが作成されます。プラグインのログは、IPとサービスのマッピングの期限（日次取得またはJSONファイル）を報告します。

また、プラグインの新しいインストールに対するサービスタグの更新、イベントのコミット、および定義の追加/削除のモニタリングも行います。

IPとサービスのマッピング例を以下に示します。

```
Service Name: AppServiceManagementazure.svc-tag.<service-name>
Example:
    azure.svc-tag.AppServiceManagement.WestUS2
Public IP CIDRs:
    13.166.40.0/26
    54.179.89.0/18
```


©2023 Palo Alto Networks, Inc.

Azure でのアクティブ/パッシブ HA のセットアップ

アクティブ/パッシブ高可用性（HA）構成の Azure で VM-Series ファイアウォールのペアを設定できます。Azure 上の HA の場合、Azure リソース グループ内に両方のファイアウォール HA ピアをデプロイして、両方の HA ピア上に同じバージョンの VM-Series プラグイン をインストールする必要があります。

- Azure でのアクティブ/パッシブ HA のセットアップ（North-South & East-West トラフィック）—Azure インフラにインターネットに対応するアプリケーションをデプロイしており、north-south トラフィックを保護する必要がある場合、フェイルオーバー時にトラフィックを保護するためにフローティング IP アドレスが必要になります。外部との接続性を有効にするこのフローティング IP アドレスは、常にアクティブなピアにアタッチされます。フェイルオーバー時には、IP アドレスがデタッチされ、新たにアクティブになったピアに IP アドレスがアタッチされる処理が、数分間で行われます。
- Azure でのアクティブ/パッシブ HA のセットアップ（East-West トラフィックのみ）—アプリケーションのアクセスおよびセキュリティ要件が Azure インフラ内に含まれており、east-west トラフィックのみを保護する必要がある場合は、フローティング IP アドレスは必要ありません。代わりに、HA 実装はフェイルオーバー時間を短縮するために、Azure ルーティング テーブルの UDR を自動的に再設定します。

Azure の VM-Series ファイアウォールで HA を有効にするには、次の表にリストされているアクセス許可が付帯する Azure ActiveDirectory アプリケーションとサービスプリンシパルを作成する必要があります。

Azure HA タイプ	許可	ロールの範囲

セカンダリ IP 移動 HA	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action"`
	次の許可は、いずれかのデータインターフェースにパブリック IP アドレスを割り当てた場合にのみ必要です。標準の SKU インターフェースをお勧めします。
	`"Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/`
		• VM がデプロイされている仮想ネットワーク
		• 2 つの VM-Series ファイアウォール
		• 両方の VM-Series ファイアウォールの NIC
		• Network Security Group（ネットワーク セキュリティ グループ）
		• VM-Series ファイアウォールのパブリック IP アドレス

©2023 Palo Alto Networks, Inc.

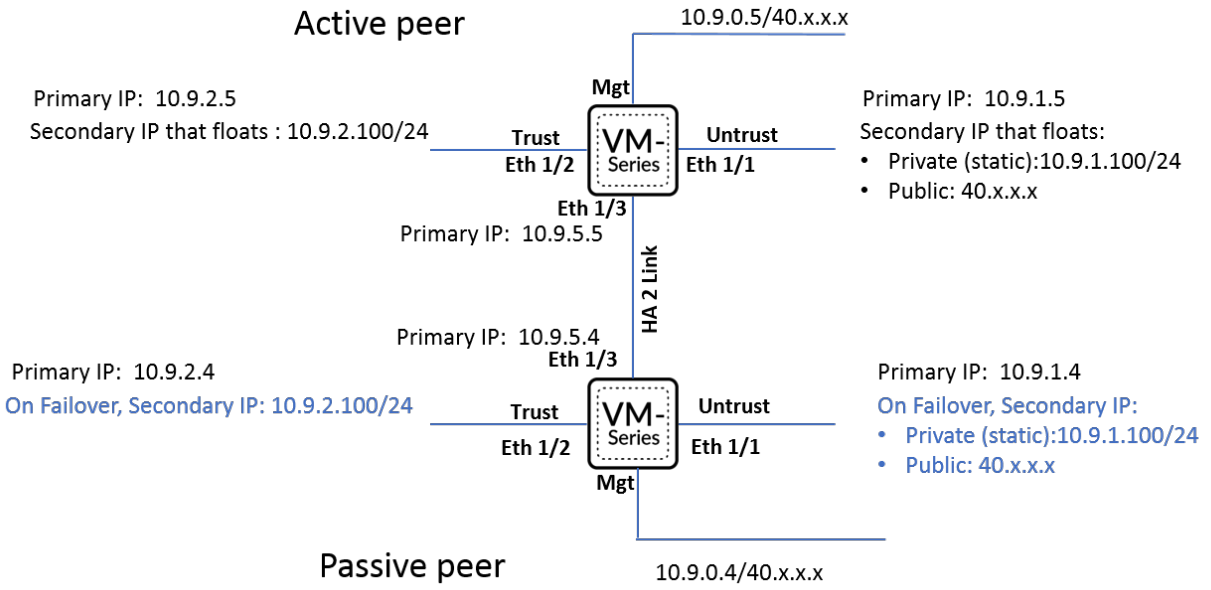
Azure HA タイプ	許可	ロールの範囲
	read""Microsift.Network/publicIPAddresses/write"	
UDR HA	"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/routeTables/*""Microsift.Network/networkInterfaces/*"	• 2 つの VM-Series ファイアウォール • 両方の VM-Series ファイアウォールの NIC • UDR に関連付けられたルートテーブル
セカンダリ IP 移動と UDR	"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/routeTables/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action" 次の許可は、いずれかのデータインターフェースにパブリック IP アドレスを割り当てた場合にのみ必要です。標準の SKU インターフェースをお勧めします。 "Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/read""Microsift.Network/publicIPAddresses/write"	• VM がデプロイされている仮想ネットワーク • 2 つの VM-Series ファイアウォール • 両方の VM-Series ファイアウォールの NIC • Network Security Group（ネットワークセキュリティ グループ） • VM-Series ファイアウォールのパブリック IP アドレス • UDR に関連付けられたルートテーブル

Azure でのアクティブ/パッシブ HA のセットアップ（North-South & East-West トラフィック）

Azure インフラ内でアプリケーションへの north-south トラフィックを保護したい場合は、あるピアから別のピアに素早く切り替えられるフローティング IP アドレスを使って、このワークフローを実行します。Azure でファイアウォールのプライマリ インターフェイスに関連付けられている IP アドレスは移動できないため、フローティング IP アドレスとして機能できるセカンダリ IP アドレスを割り当てる必要があります。アクティブ ファイアウォールがダウンすると、フローティング IP アドレスはアクティブ ファイアウォールからパッシブ ファイアウォールに

©2023 Palo Alto Networks, Inc.

移動します。これによってパッシブ ファイアウォールがアクティブ ピアになるとすぐに、トラフィックをスムーズに保護できます。フローティング IP アドレスの他に、HA ピアにはデータを同期し状態情報を維持するために HA リンク（コントロール リンク（HA1）とデータ リンク（HA2））も必要です。



- HA を有効にするためのファイアウォールのセットアップ
- Azure での VM-Series ファイアウォールのアクティブ/パッシブ HA の設定

HA を有効にするためのファイアウォールのセットアップ

Azure で VM-Series ファイアウォールで HA を設定するため、以下の詳細情報を収集します。

Active Directory アプリケーションとサービス プリンシパルを設定して、プログラムによる API アクセスを有効にします。

- ファイアウォールが Azure API を操作できるようにするには、Azure Active Directory サービス プリンシパルを作成する必要があります。サービス プリンシパルには、Azure AD に対する認証と、サブスクリプション内のリソースへのアクセスに必要な権限が含まれています。このセットアップを行うには、アプリケーションを Azure AD テナントに登録し、サブスクリプションのロールにアプリケーションを割り当てるための権限が必要です。必要な権限を持っていない場合は、Azure AD あるいはサブスクリプションの管理者にサービス プリンシパルの作成を依頼してください。必要な許可については、上の表を参照してください。後でこのワークフローで使用する以下の詳細情報をコピーします。
  - クライアント **ID** – Active Directory に関連付けられているアプリケーション ID （Azure ポータルのホーム > **Azure Active Directory** > アプリの登録をクリックし、アプリケーションを選択して ID をコピーします）。

©2023 Palo Alto Networks, Inc.

- テナント **ID** — Active Directory に関連付けられているディレクトリ ID （Azure ポータルのホーム > **Azure Active Directory** > プロパティ > ディレクトリ **ID**をクリックし、アプリケーションを選択して ID をコピーします）。

- **Azure** サブスクリプション **ID**— ファイアウォールをデプロイした Azure サブスクリプション。Azure ポータルにログインしてこのサブスクリプション ID を取得する必要があります。
- リソース グループ名— HA ピアとして設定するファイアウォールをデプロイしたリソース グループの名前。両方のファイアウォールが同じリソース グループに含まれている必要があります。
- 秘密鍵 - Active Directory アプリケーションに関連付けられている認証キー （Azure ポータルでホーム > **Azure Active Directory** > 証明書とシークレットをクリックし、[クライアントシークレット]の下の[値]をコピーします。秘密鍵がない場合は、最初に秘密鍵を作成してから、値をコピーします）。アプリケーションとしてログインするには、キーの値とアプリケーション ID の両方を指定する必要があります。

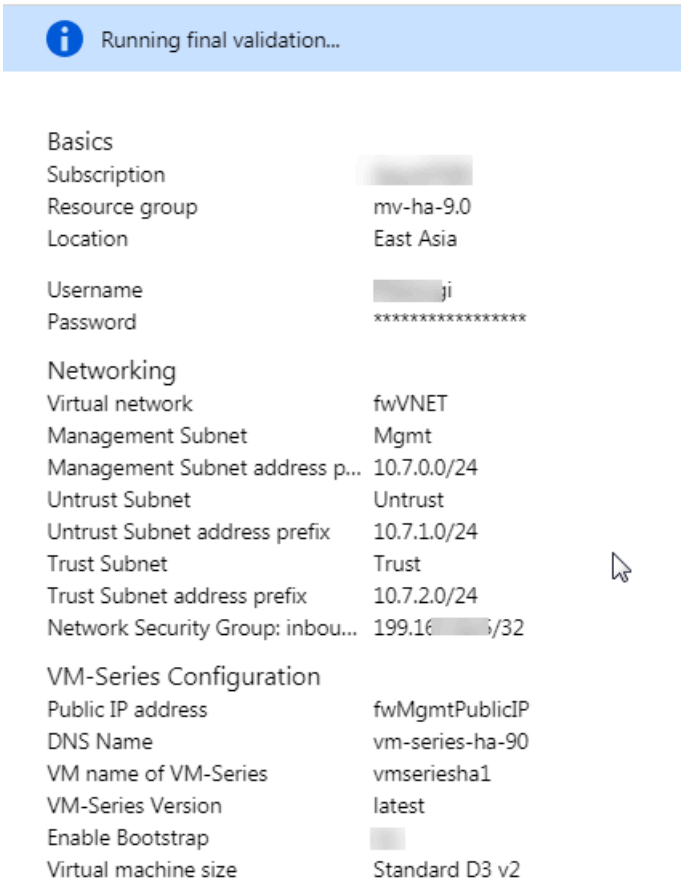
VM-Series ファイアウォールを同一の Azure リソース グループにデプロイするために必要なテンプレートの入手先を確認します。

HA 設定では、両方の HA ピアが同一の Azure リソース グループに属している必要があります。Azure Marketplace からファイアウォールの最初のインスタンスをデプロイする場合、2 番目のファイアウォール インスタンスを既存のリソース グループにデプロイするときには、カスタム ARM テンプレートまたは Palo Alto Networks のサンプル GitHub テンプレートを使用する必要があります。カスタム テンプレートまたは Palo Alto Networks のサンプル テンプ

©2023 Palo Alto Networks, Inc.

レートが必要となるのは、Azure では空ではないリソース グループにファイアウォールをデプロイする操作がサポートされていないためです。

最初のファイアウォール インスタンスのデプロイメント情報をコピーします。以下に例を示します。



上記のスクリーンショットに示されている **VM-Series** ファイアウォールの **VM** 名を、ファイアウォールの Web インターフェイスのホスト名と一致させます。**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）で同じ名前を追加する必要があります。これは、ファイアウォールのホスト名がフェイルオーバーのトリガーに使用されるためです。

Azure での VM-Serie ファイアウォールのネットワーク インターフェイス設定について計画します。

HA をセットアップするには、両方の HA ピアを同一の Azure リソース グループ内にデプロイし、両方のファイアウォールのネットワーク インターフェイスの数が同一である必要があります。各 HA ピアには少なくとも次の 4 つのネットワーク インターフェイスが必要です。

- 管理インターフェイス（**eth0**）— プライマリ インターフェイスに関連付けられているプライベートおよびパブリック IP アドレス。パブリック IP アドレスにより、ファイアウォールの Web インターフェイスにアクセスでき、SSH アクセスが可能になります。

  アクティブ/パッシブ HA ピア間のコントロール リンク通信のための HA1 ピア IP アドレスとして、管理インターフェイスでプライベート IP アドレスを使用できます。専用の

 ©2023 Palo Alto Networks, Inc.

HA1 インターフェイスが必要な場合は、各ファイアウォールにネットワーク インターフェイスを追加でアタッチする必要があります。つまりこの場合は各ファイアウォールに 5 つのインターフェイスが必要です。

- **Untrust** インターフェイス（**eth1/1**）— /32 ネットマスク付きのプライマリ プライベート IP アドレスと、プライベート IP アドレス（任意のネットマスク）およびパブリック IP アドレスの両方を使用するセカンダリ IP 設定。

  フェイルオーバー発生時には、パッシブ ピアがアクティブ状態に移行すると、セカンダリ IP 設定に関連付けられているパブリック IP アドレスが、以前のアクティブ ピアからデタッチされ、現在アクティブな HA ピアにアタッチされます。
- **Trust** インターフェイス（**eth1/2**）— プライマリおよびセカンダリ プライベート IP アドレス。フェイルオーバー発生時には、パッシブ ピアがアクティブ状態に移行すると、セカンダリ プライベート IP アドレスが以前のアクティブ ピアからデタッチされ、現在アクティブな HA ピアにアタッチされます。
- **HA2**（**eth 1/3**）— プライマリ プライベート IP アドレス。HA2 インターフェイスは、HA ピアがセッションを同期し、テーブル、IPSec セキュリティ アソシエーション、ARP テーブルを転送するときに使用するデータ リンクです。

インターフェイス	アクティブ ファイアウォール ピア	パッシブ ファイアウォール ピア	概要
Trust	セカンダリ IP アドレス	—	アクティブ ピアの trust インターフェイスには、フェイルオーバー発生時にもう一方のピアに移動できるセカンダリ IP 設定が必要です。trust インターフェイスのこのセカンダリ IP 設定は、インターフェイスが保護するサーバーのネットマスク付きプライベート IP アドレスである必要があります。フェイルオーバー発生時には、VM-Series プラグインが Azure API を呼び出し、このセカンダリ プライベート IP アドレスをアクティブ ピアからデタッチし、パッシブ ピアにアタッチします。現在のアクティブ ピアにこの IP アドレスをアタッチすることで、ファイアウォールは untrust インターフェイスのフローティング IP でトラフィックを受信し、trust インターフェイスのフローティング IP、そしてワークロードにトラフィックを送信できるようになります。
Untrust	セカンダリ IP アドレス	—	ファイアウォールの untrust インターフェイスでは、untrust サブネットの静的 IP アドレスとネットマスクを含むセカンダリ IP 設定と、インターネット経由でバックエンド サーバーまたはワークロードに接続するためのパブリック IP アドレスが必要です。フェイルオーバー発生時には、VM-Series プラグインが Azure API を呼び出

©2023 Palo Alto Networks, Inc.

インターフェイス	アクティブ ファイアウォール ピア	パッシブ ファイアウォール ピア	概要
			し、このセカンダリ IP 設定をアクティブ ピアからデタッチし、パッシブ ピアがアクティブ状態になる前にパッシブ ピアにアタッチします。このセカンダリ IP 設定のフローティング プロセスにより、現在アクティブなファイアウォールが引き続き、ワークロード宛てのインバウンド トラフィックを処理できます。
HA2	Azure 管理コンソールから NIC をファイアウォールに追加します。	Azure 管理コンソールから NIC をファイアウォールに追加します。	アクティブ ピアとパッシブ ピアで、セッションの同期を可能にする専用 HA2 リンクを追加します。 HA1 のデフォルト インターフェイスは管理インターフェイスであり、ファイアウォールにインターフェイスを追加する代わりにこの管理インターフェイスを使用できます。HA2 リンク経由でのデータ フローを有効にするには、Azure ポータルでネットワーク インターフェイスを追加し、ファイアウォールで HA2 用にこのインターフェイスを設定する必要があります。

Azure での VM-Series ファイアウォールのアクティブ/パッシブ HA の設定

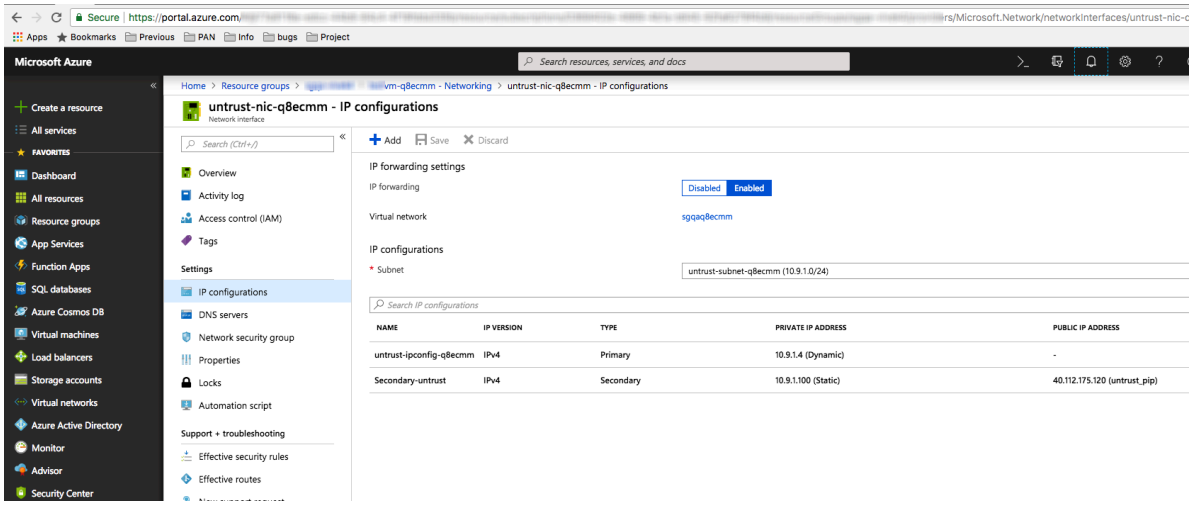
このワークフローでは、Azure Marketplace の VM-Series ファイアウォール ソリューション テンプレートを使用して VM-Series ファイアウォールの最初のインスタンスをデプロイし、サンプル GitHub テンプレートを使用して 2 番目のインスタンスをデプロイします。

HA 設定での *VM-Series* ファイアウォールのセットアップに必要な *Active Directory* アプリケーションに関連付けられている認証キー（クライアント シークレット）は、ファイアウォールと *Panorama* では *VM-Series* プラグイン バージョン *1.0.4* を使用して暗号化されています。このキーは *VM-Series* プラグイン バージョン *1.0.4* で暗号化されているので、ファイアウォールを *Panorama* から一元的に管理するには、同じバージョンのプラグインを *Panorama* と管理対象 *VM-Series* ファイアウォールにインストールする必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | Solution テンプレートを使用して VM-Series ファイアウォールをデプロイし、ネットワークインターフェイスを HA に合わせてセットアップする必要があります。

1. セカンダリ IP 設定をファイアウォールの untrust インターフェイスに追加します。



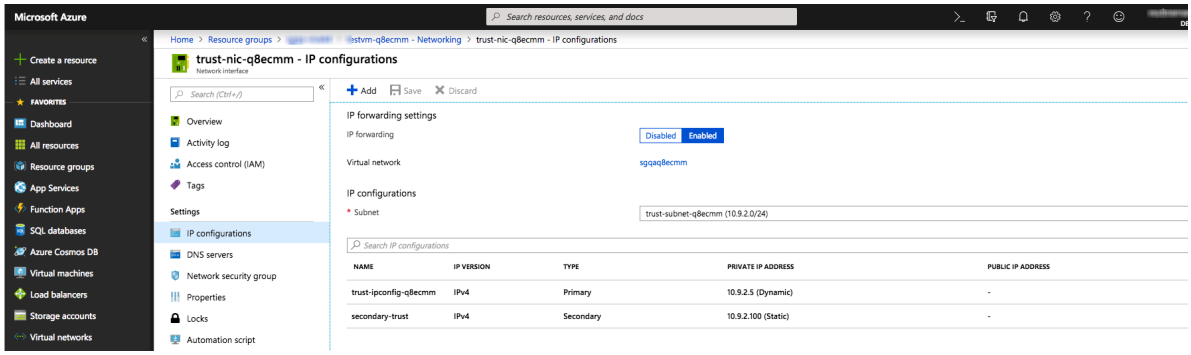
アクティブ ピアとして指定するファイアウォールに、セカンダリ IP 設定（プライベート IP アドレス（ネットマスク）とパブリック IP アドレス）をアタッチする必要があります。セカンダリ IP 設定は常にアクティブ HA ピアにとどまり、フェイルオーバーの発生時には別のピアに移動します。

このワークフローでは、このファイアウォールがアクティブ ピアとして指定されます。アクティブ HA ピアのデバイス優先度の数値は小さくなります。デバイス優先度は、ファイ

©2023 Palo Alto Networks, Inc.

アウォールの HA 設定で設定されます。この値は、ファイアウォールがアクティブ ピアの役割を想定する優先度を示します。

2. セカンダリ IP 設定をファイアウォールの trust インターフェイスに追加します。



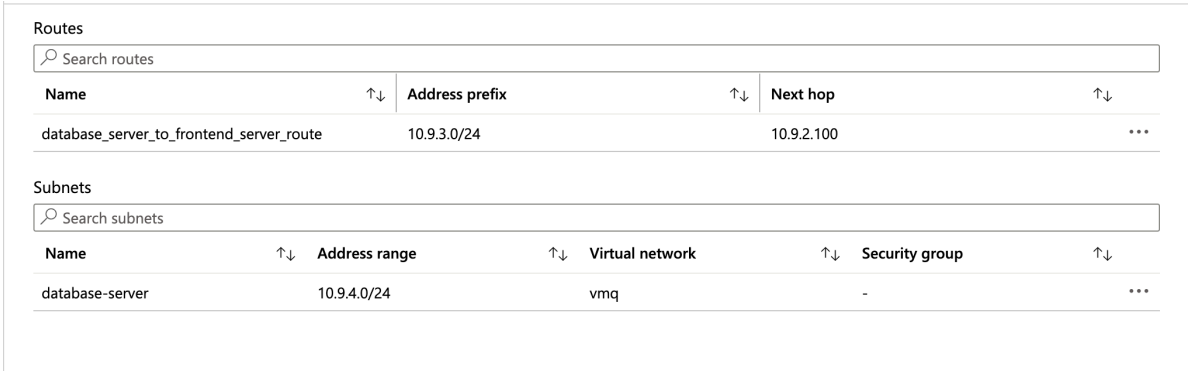
trust インターフェイスのセカンダリ IP 設定には、静的プライベート IP アドレスだけが必要です。この IP アドレスは、フェイルオーバー発生時にアクティブ ファイアウォールからパッシブ ファイアウォールに移動するので、トラフィックは untrust インターフェイス

©2023 Palo Alto Networks, Inc.

から trust インターフェイス、trust インターフェイスからファイアウォールで保護されている宛先サブネットへと流れます。

3. ファイアウォール HA ピア間の HA2 通信のためにネットワーク インターフェイスをアタッチします。
   1. 仮想ネットワーク内でサブネットを追加します。
   2. ネットワーク インターフェイスを作成し、ファイアウォールにアタッチします。
4. Azure にルート テーブルを設定します。

   次のホップは、ここに記載しているフローティング IP アドレスを指す必要があります。



 ©2023 Palo Alto Networks, Inc.

Routes

Search routes

Name	Address prefix	Next hop
frontend_Server_to_Database_Server_route	10.9.4.0/24	10.9.1.100

Subnets

Search subnets

Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

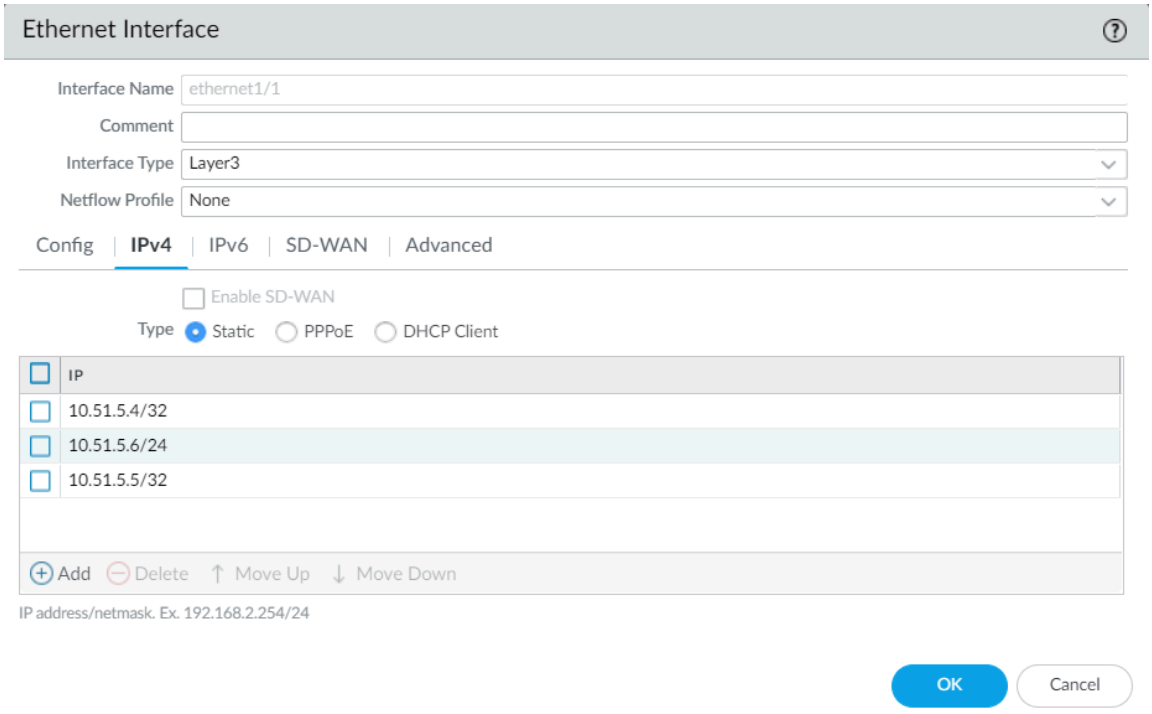
©2023 Palo Alto Networks, Inc.

STEP 2 | ファイアウォール上でインターフェイスを設定します。

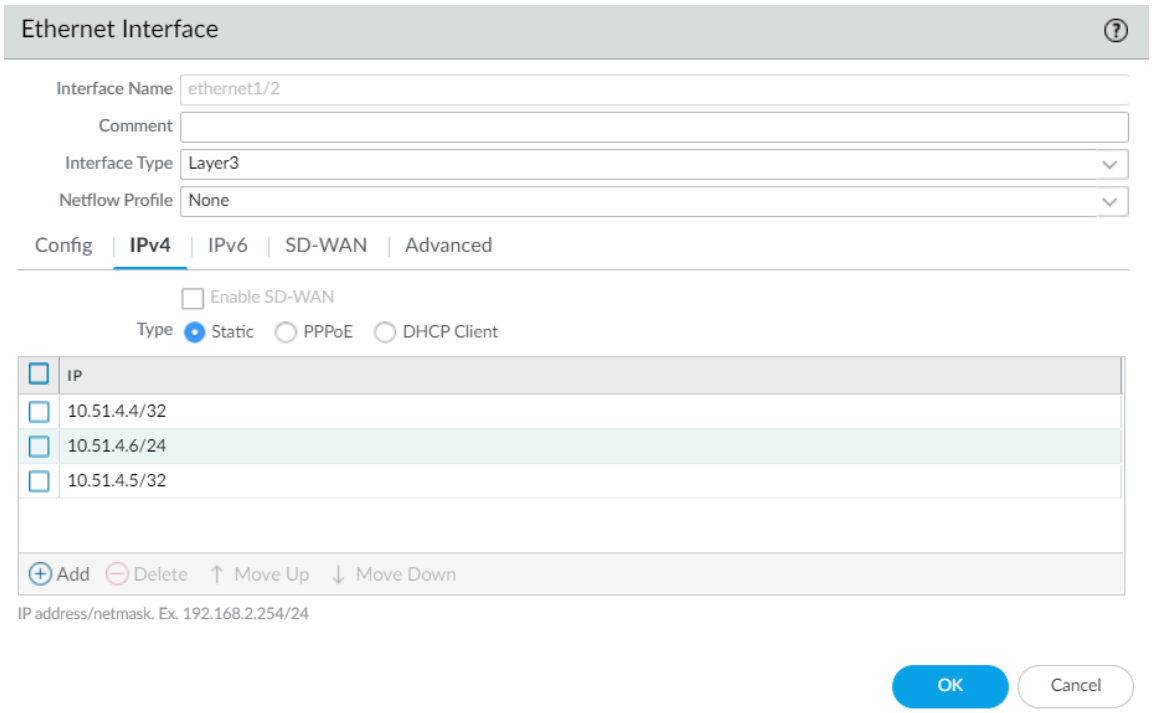
パッシブ HA ピアのデプロイとセットアップを行う前に、アクティブ HA ピアで次の手順を実行します。

1. ファイアウォール インターフェイスにログインします。
2. ethernet 1/1 を untrust インターフェイスとして設定し、ethernet 1/2 を trust インターフェイスとして設定します。

   Network（ネットワーク） > **Interfaces**（インターフェイス）を選択して次のように設定します。



©2023 Palo Alto Networks, Inc.



3. ethernet 1/3 を HA インターフェイスとして設定します。

   HA2 リンクをセットアップするため、インターフェイスを選択して **Interface Type**（インターフェイス タイプ）を **HA** に設定します。リンク速度とデュプレックスを auto に設定します。



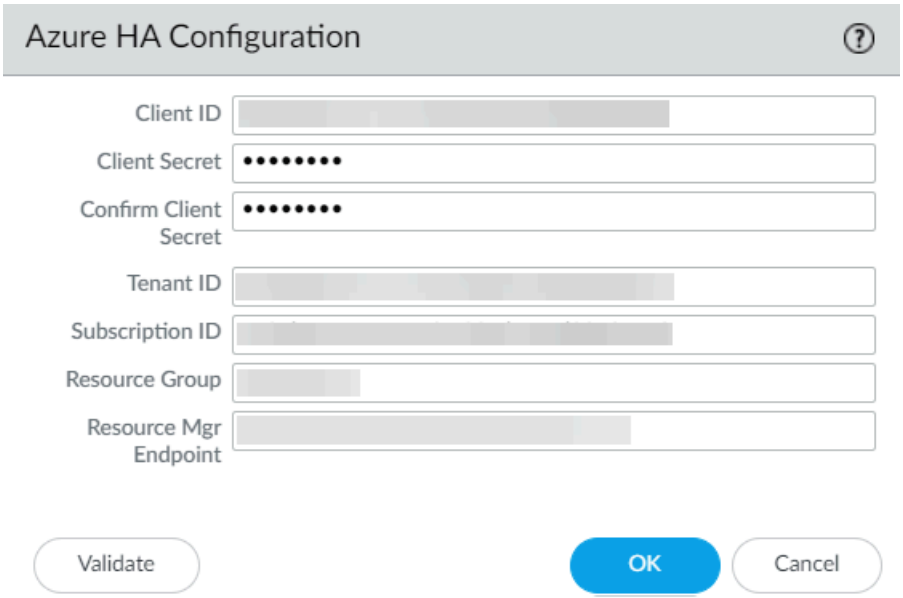
©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォールをデプロイした Azure リソース グループに対する認証を実行するように VM-Series プラグインを設定します。

VM-Series プラグインで Azure HA 設定をセットアップします。

クライアント シークレットを暗号化するには、VM-Series プラグイン バージョン 1.0.4 以降を使用します。Panorama を使用してファイアウォールを管理する場合は、VM-Series プラグイン バージョン 1.0.4 以降をインストールする必要があります。

1. **Device**（デバイス） > **VM-Series** を選択して、ファイアウォール プラグインと Azure リソース間のプログラムによるアクセスを有効にします。



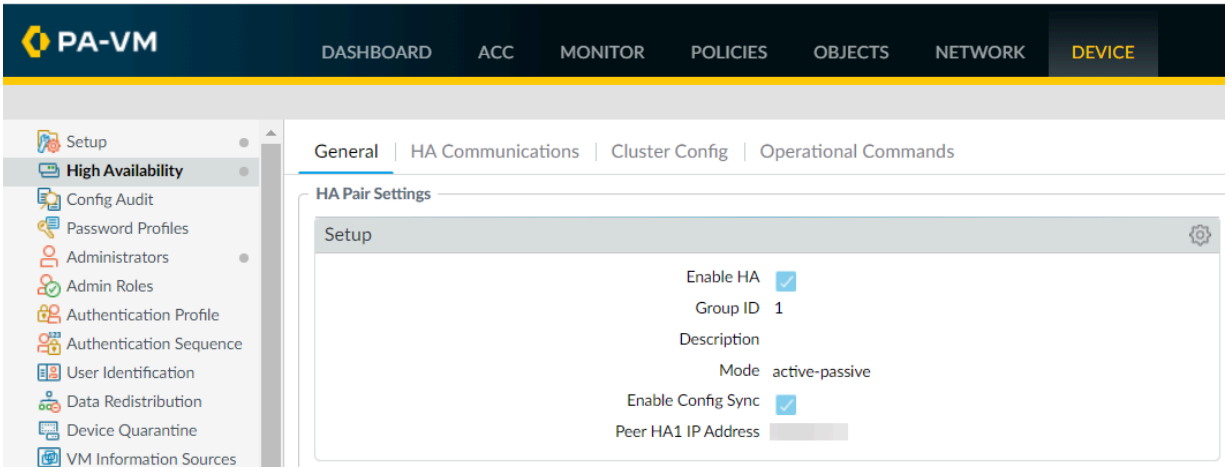
2. **Client ID**（クライアント **ID**）を入力します。クライアント ID は、Azure Active Directory アプリケーションに関連付けられているアプリケーション ID です。
3. **Client Secret**（クライアント シークレット）を入力し、確認用に再び入力します。
4. **Tenant ID**（テナント **ID**）を入力します。テナント ID は、アクティブディレクトリ アプリケーションをセットアップする際に保存したディレクトリ ID です。
5. 監視する Azure サブスクリプションの**Subscription ID**（サブスクリプション **ID**）を入力します。
6. リソースグループ名を入力します。
7. （Azure Stack デプロイメントの場合のみ） リソースマネージャーエンドポイントURLを入力します。

   このフィールドは、*VM-Series* プラグイン *2.1.2* 以降で使用できます。

8. **Validate**（検証）をクリックし、入力したキーおよび ID が有効であり、VM-Series プラグインが API を使用して Azure リソースと通信できることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 4 | HA を有効にします。



1. **Device**（デバイス） > **Setup**（セットアップ） > **HA** を選択します。
2. パッシブ ピアのプライベート IP アドレスとして **Peer HA1 IP address**（ピア **HA1 IP** アドレス）を入力します。
3. （任意）コントロール リンク（HA1）を編集します。コントロール リンクに管理インターフェイスを使用する予定がなく、インターフェイス（ethernet 1/4 など）を追加している場合は、このセクションを編集して、そのインターフェイスを HA1 通信に使用するインターフェイスとして選択します。
4. データ リンク（HA2）を編集し、**Port**（ポート）として ethernet 1/3 を使用するように設定し、このピアの IP アドレスと、サブネットの **Gateway**（ゲートウェイ） IP アドレスを追加します。

STEP 5 | 変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

STEP 6 | 同じ Azure リソース グループ内でパッシブ HA ピアをセットアップします。

1. ファイアウォールの 2 番目のインスタンスをデプロイします。
   - GitHub からカスタム テンプレートおよびパラメータ ファイルをダウンロードします。
   - Azure ポータルにログインします。
   - カスタム テンプレートを検索し、**Deploy from a custom template**（カスタム テンプレートからのデプロイ）を選択します。
   - **Build your own template in the editor**（エディタで専用のテンプレートを作成） > **Load file**（ファイルの読み込み）を選択します。
   - ダウンロードした **azuredeploy.json** を選択して **Save**（保存）を選択します。
   - 入力が完了したら、利用規約に同意して **Purchase**（購入）します。

     入力内容（Azure サブスクリプション、リソース グループの名前、リソース グループの場所、ファイアウォールをデプロイする既存の VNet の名前、VNet CIDR、サブネット名、サブネット CIDR）が、すでにデプロイされているファイアウォール インスタンスと一致していることを確認し、管理サブネット、trust サブネット、untrust サブネットの IP アドレスを開始します。
2. ステップ 1 とステップ 2 を繰り返して、インターフェイスをセットアップし、ファイアウォールをパッシブ HA ピアとして設定します。
3. ステップ 3 を省略し、「HA の有効化（ステップ 5）」の手順を完了します。ステップ 4 で、このパッシブ HA ピアに合わせて IP アドレスを変更します。

STEP 7 | 両方のファイアウォールの設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のデバイスで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブ ファイアウォールで、**Sync to peer** （ピアと同期）リンクをクリックします。
3. 次のように、ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **passive**、**Running Config** （行コンフィグ）が **synchronized** と表示されます。
   - アクティブ ファイアウォールローカル ファイアウォールの状態が **active**、**Running Config**（実行コンフィグ）が **synchronized** と表示されます。
4. パッシブ ピアで VM-Serie プラグインの設定が同期されていることを確認します。

   Device（デバイス） > **VM-Series** を選択し、パッシブ ピアで設定を省略した Azure HA 構成が表示されていることを確認します。

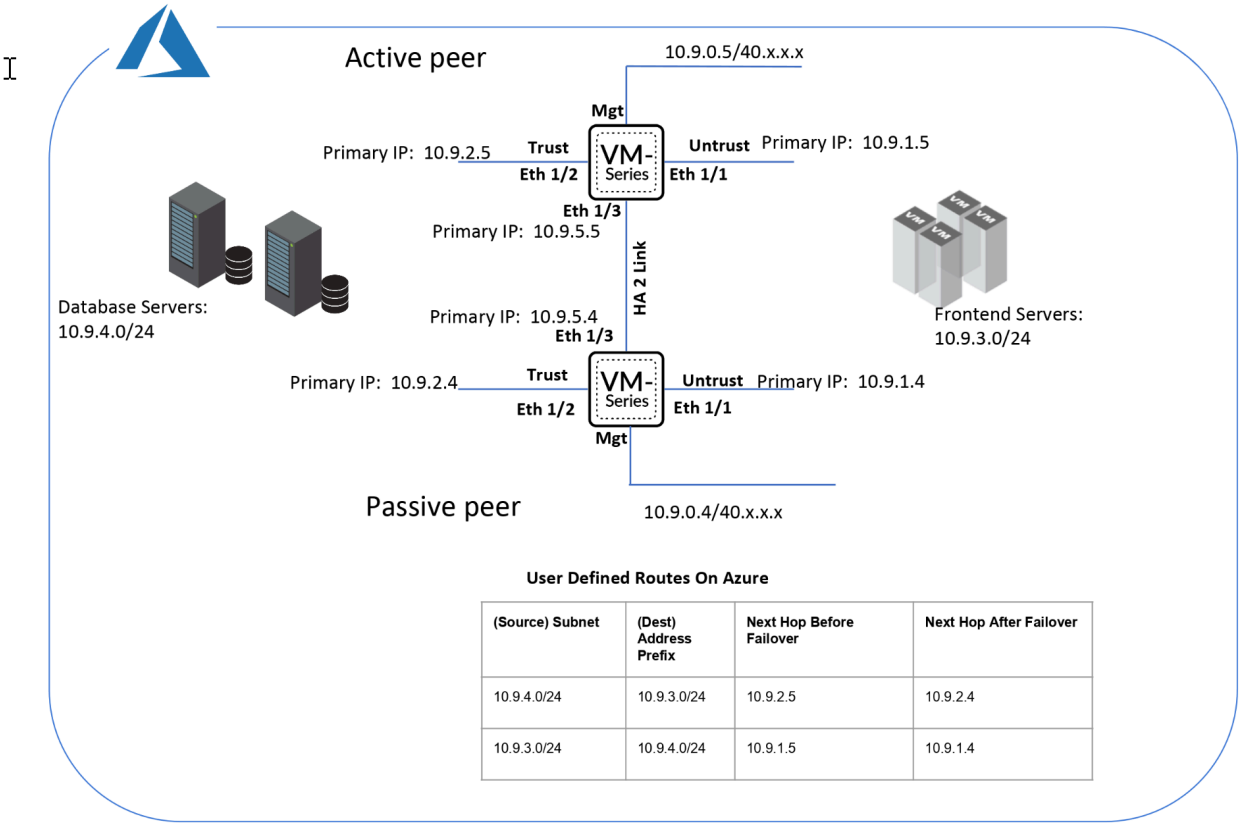
Azure でのアクティブ/パッシブ HA のセットアップ（East-West トラフィックのみ）

Azure インフラ内にすべてのリソースを展開し、Azure VNet への north south トラフィックにセキュリティを適用する必要がない場合、フローティング IP アドレスなしでアクティブ/パッ

 ©2023 Palo Alto Networks, Inc.

シブ高可用性（HA）構成内に VM-Series ファイアウォールのペアをデプロイすることができます。HA ピアにはデータを同期し状態情報を維持するために、引き続き HA リンク（コントロール リンク（HA1）とデータ リンク（HA2））も必要です。

VM-Series プラグイン バージョン 1.0.9 以降を使用して、2 つのファイアウォール HA ピアの両方を同じ Azure リソース グループ内にデプロイする必要があります。



User Defined Routes On Azure

(Source) Subnet	(Dest) Address Prefix	Next Hop Before Failover	Next Hop After Failover
10.9.4.0/24	10.9.3.0/24	10.9.2.5	10.9.2.4
10.9.3.0/24	10.9.4.0/24	10.9.1.5	10.9.1.4

- HA を有効にするためのファイアウォールのセットアップ
- Azure での VM-Series ファイアウォールのアクティブ/パッシブ HA の設定

HA を有効にするためのファイアウォールのセットアップ

Azure で VM-Series ファイアウォールで HA を設定するため、以下の詳細情報を収集します。

Active Directory アプリケーションとサービス プリンシパルを設定して、プログラムによる API アクセスを有効にします。

- ファイアウォールが Azure API を操作できるようにするには、Azure Active Directory サービス プリンシパルを作成する必要があります。サービス プリンシパルには、Azure AD に対する認証と、サブスクリプション内のリソースへのアクセスに必要な権限が含まれてい

©2023 Palo Alto Networks, Inc.

ます。このセットアップを行うには、アプリケーションを Azure AD テナントに登録し、サブスクリプションのロールにアプリケーションを割り当てるための権限が必要です。必要な権限を持っていない場合は、Azure AD あるいはサブスクリプションの管理者にサービス プリンシパルの作成を依頼してください。必要な許可については、上の表を参照してください。後でこのワークフローで使用する以下の詳細情報をコピーします。

- クライアント **ID** – Active Directory に関連付けられているアプリケーション ID （Azure ポータルのホーム > **Azure Active Directory** > アプリの登録をクリックし、アプリケーションを選択して ID をコピーします）。
- テナント **ID** – Active Directory に関連付けられているディレクトリ ID （Azure ポータルのホーム > **Azure Active Directory** > プロパティ > ディレクトリ **ID**をクリックし、アプリケーションを選択して ID をコピーします）。
- **Azure** サブスクリプション **ID**– ファイアウォールをデプロイした Azure サブスクリプション。Azure ポータルにログインしてこのサブスクリプション ID を取得する必要があります。
- リソース グループ名– HA ピアとして設定するファイアウォールをデプロイしたリソース グループの名前。両方のファイアウォールが同じリソース グループに含まれている必要があります。
- 秘密鍵 - Active Directory アプリケーションに関連付けられている認証キー （Azure ポータルでホーム > **Azure Active Directory** > 証明書とシークレットをクリックし、[クライアントシークレット]の下の[値]をコピーします。秘密鍵がない場合は、最初に秘密鍵を作成してから、値をコピーします）。アプリケーションとしてログインするには、キーの値とアプリケーション ID の両方を指定する必要があります。

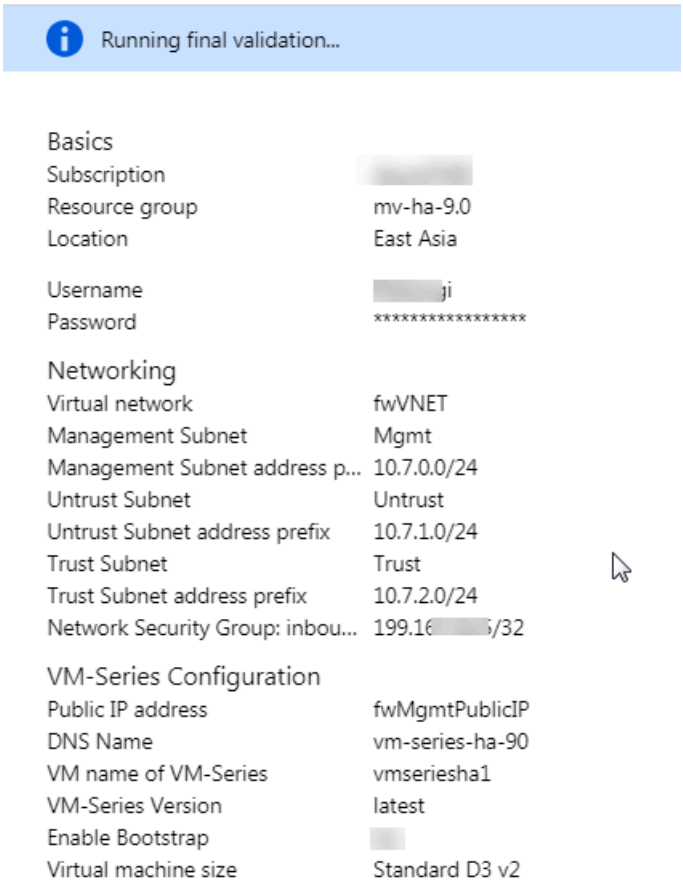
VM-Series ファイアウォールを同一の Azure リソース グループにデプロイするために必要なテンプレートの入手先を確認します。

HA 設定では、両方の HA ピアが同一の Azure リソース グループに属している必要があります。Azure Marketplace からファイアウォールの最初のインスタンスをデプロイする場合、2 番目のファイアウォール インスタンスを既存のリソース グループにデプロイするときには、カスタム ARM テンプレートまたは Palo Alto Networks のサンプル GitHub テンプレートを使用する必要があります。カスタム テンプレートまたは Palo Alto Networks のサンプル テンプ

 ©2023 Palo Alto Networks, Inc.

レートが必要となるのは、Azure では空ではないリソース グループにファイアウォールをデプロイする操作がサポートされていないためです。

最初のファイアウォール インスタンスのデプロイメント情報をコピーします。以下に例を示します。



上記のスクリーンショットに示されている **VM-Series** ファイアウォールの **VM** 名を、ファイアウォールの Web インターフェイスのホスト名と一致させます。**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）で同じ名前を追加する必要があります。これは、ファイアウォールのホスト名がフェイルオーバーのトリガーに使用されるためです。

Azure での VM-Serie ファイアウォールのネットワーク インターフェイス設定について計画します。

HA をセットアップするには、両方の HA ピアを同一の Azure リソース グループ内にデプロイし、両方のファイアウォールのネットワーク インターフェイスの数が同一である必要があります。各 HA ピアには少なくとも次の 4 つのネットワーク インターフェイスが必要です。

- 管理インターフェイス（**eth0**）— プライマリ インターフェイスに関連付けられているプライベートおよびパブリック IP アドレス。パブリック IP アドレスにより、ファイアウォールの Web インターフェイスにアクセスでき、SSH アクセスが可能になります。

  アクティブ/パッシブ HA ピア間のコントロール リンク通信のための HA1 ピア IP アドレスとして、管理インターフェイスでプライベート IP アドレスを使用できます。専用の

 ©2023 Palo Alto Networks, Inc.

HA1 インターフェイスが必要な場合は、各ファイアウォールにネットワーク インターフェイスを追加でアタッチする必要があります。つまりこの場合は各ファイアウォールに 5 つのインターフェイスが必要です。

- **Untrust** インターフェイス（**eth1/1**）– ネットマスクが /32 のプライマリ プライベート IP アドレス。

  フェイルオーバー時、パッシブ ピアがアクティブ状態に遷移すると、VM-Series プラグインは自動的にトラフィックを、パッシブ ピアのプライマリ プライベート アドレスに送信します。Azure UDR によりトラフィック フローが有効になります。
- **Trust** インターフェイス（**eth1/2**）– プライマリ プライベート IP アドレス。フェイルオーバー時、パッシブ ピアがアクティブ状態に遷移すると、VM-Series プラグインは自動的にトラフィックを、パッシブ ピアのプライマリ プライベート アドレスに送信します。
- **HA2**（**eth 1/3**）– プライマリ プライベート IP アドレス。HA2 インターフェイスは、HA ピアがセッションを同期し、テーブル、IPSec セキュリティ アソシエーション、ARP テーブルを転送するときに使用するデータ リンクです。

インターフェイス	アクティブ ファイアウォール ピア	パッシブ ファイアウォール ピア	概要
HA2	Azure 管理コンソールから NIC をファイアウォールに追加します。	Azure 管理コンソールから NIC をファイアウォールに追加します。	アクティブ ピアとパッシブ ピアで、セッションの同期を可能にする専用 HA2 リンクを追加します。 HA1 のデフォルト インターフェイスは管理インターフェイスであり、ファイアウォールにインターフェイスを追加する代わりにこの管理インターフェイスを使用できます。HA2 リンク経由でのデータ フローを有効にするには、Azure ポータルでネットワーク インターフェイスを追加し、ファイアウォールで HA2 用にこのインターフェイスを設定する必要があります。

©2023 Palo Alto Networks, Inc.

Azure での VM-Series ファイアウォールのアクティブ/パッシブ HA の設定

このワークフローでは、Azure Marketplace の VM-Series ファイアウォール ソリューション テンプレートを使用して VM-Series ファイアウォールの最初のインスタンスをデプロイし、サンプル GitHub テンプレートを使用して 2 番目のインスタンスをデプロイします。

HA 設定での *VM-Series* ファイアウォールのセットアップに必要な *Active Directory* アプリケーションに関連付けられている認証キー（クライアント シークレット）は、ファイアウォールと *Panorama* では *VM-Series* プラグイン バージョン *1.0.9* を使用して暗号化されています。このキーは *VM-Series* プラグイン バージョン *1.0.9* で暗号化されているので、ファイアウォールを *Panorama* から一元的に管理するには、同じバージョンのプラグインを *Panorama* と管理対象 *VM-Series* ファイアウォールにインストールする必要があります。

STEP 1 | Solution テンプレートを使用して VM-Series ファイアウォールをデプロイし、ネットワーク インターフェイスを HA に合わせてセットアップする必要があります。

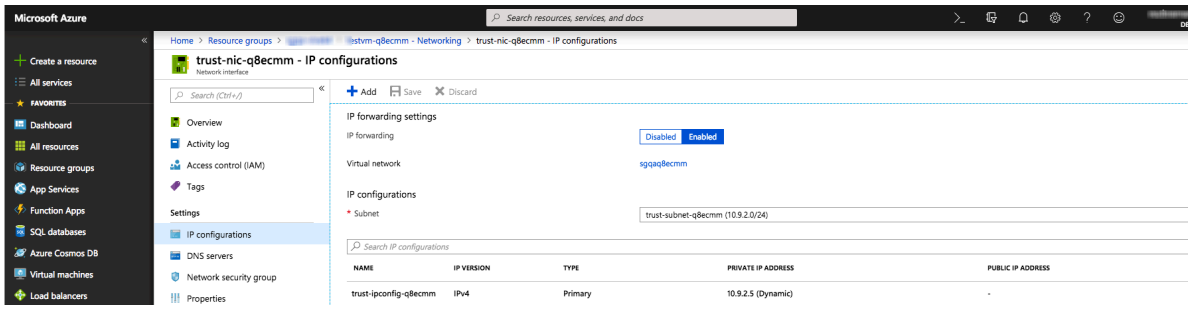
Azure VNet 内の east west トラフィックを保護するためには、trust ファイアウォール インターフェイスと untrust ファイアウォール インターフェイスのプライマリ IP アドレスのみが必要になります。フェイルオーバーが発生すると、UDR が変化し、ルートがアクティブ状態に遷移したピアのプライマリ IP アドレスを指すようになります。

1. プライマリ IP 設定を、アクティブなファイアウォール ピアの trust インターフェイスに追加します。

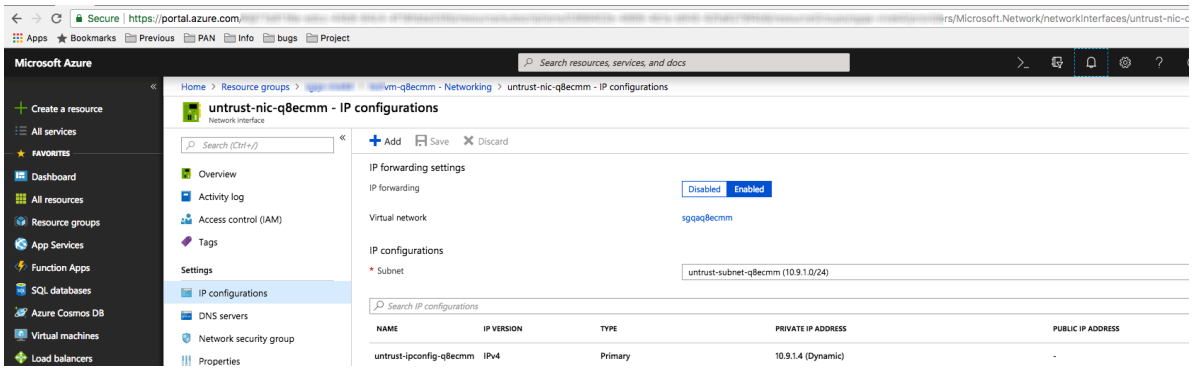
   このワークフローでは、このファイアウォールがアクティブ ピアとして指定されます。アクティブ HA ピアのデバイス優先度の数値は小さくなります。デバイス優先度は、ファイ

©2023 Palo Alto Networks, Inc.

アウォールの HA 設定で設定されます。この値は、ファイアウォールがアクティブ ピアの役割を想定する優先度を示します。



2. プライマリ IP 設定を、アクティブなファイアウォール ピアの untrust インターフェイスに追加します。

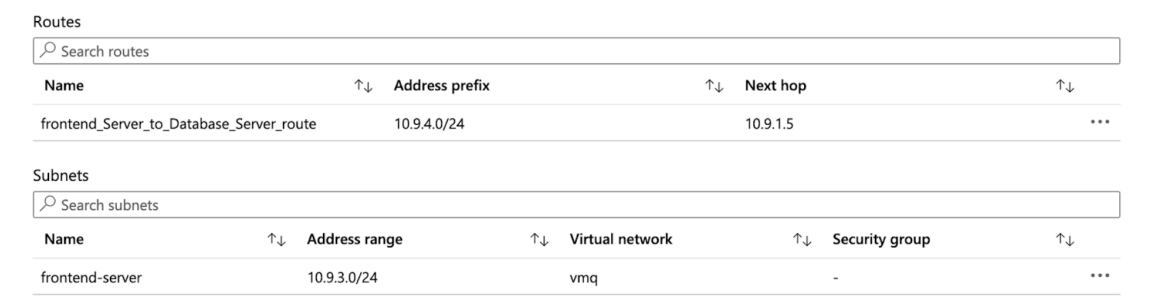


 ©2023 Palo Alto Networks, Inc.

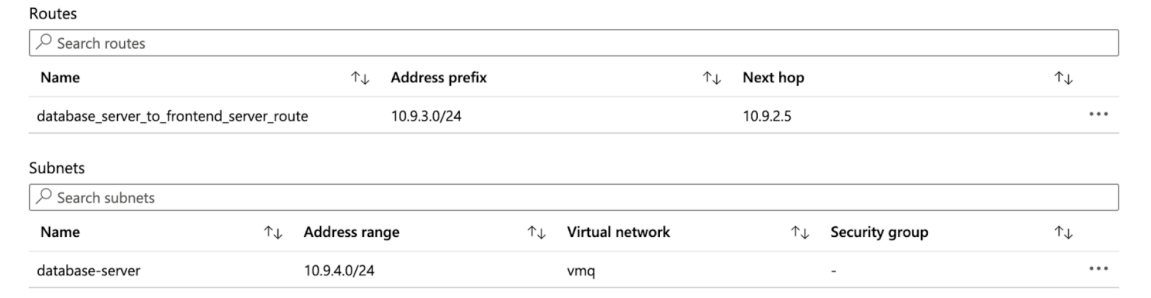
3. ファイアウォール HA ピア間の HA2 通信のためにネットワーク インターフェイスをアタッチします。
   1. 仮想ネットワーク内でサブネットを追加します。
   2. ネットワーク インターフェイスを作成し、ファイアウォールにアタッチします。
4. Azure にルート テーブルを設定します。

   アクティブなファイアウォール ピアの、trust および untrust インターフェイスの、プライマリ IP アドレスの次のホップへのルートを作成します。

Example with Frontend Server to Database Server Route :



Example with Database Server to Frontend Server route:



フェイルオーバー後、データベース サーバからフロントエンド サーバーへのルートの次のホップが、10.9.2.5 から 10.9.2.4 に変化します。同様に、フロントエンド サーバーからデータベース サーバーへのルートの次のホップが、10.9.1.5 から 10.9.1.4 に変化します。

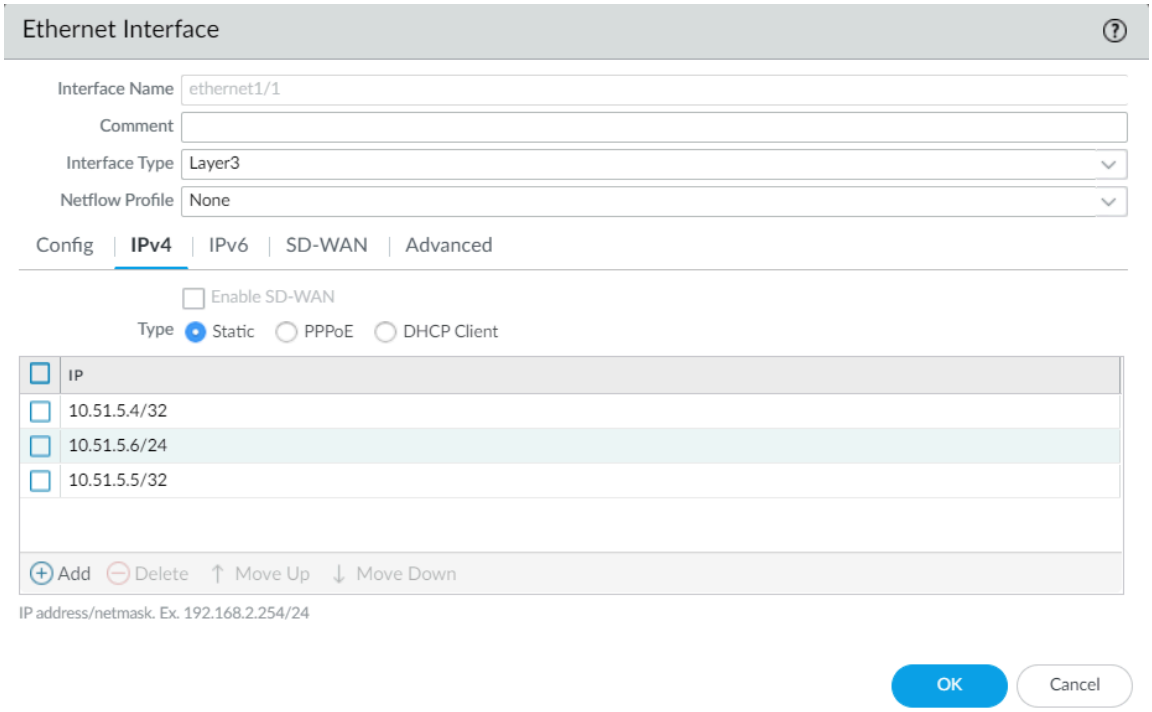
©2023 Palo Alto Networks, Inc.

STEP 2 | ファイアウォール上でインターフェイスを設定します。

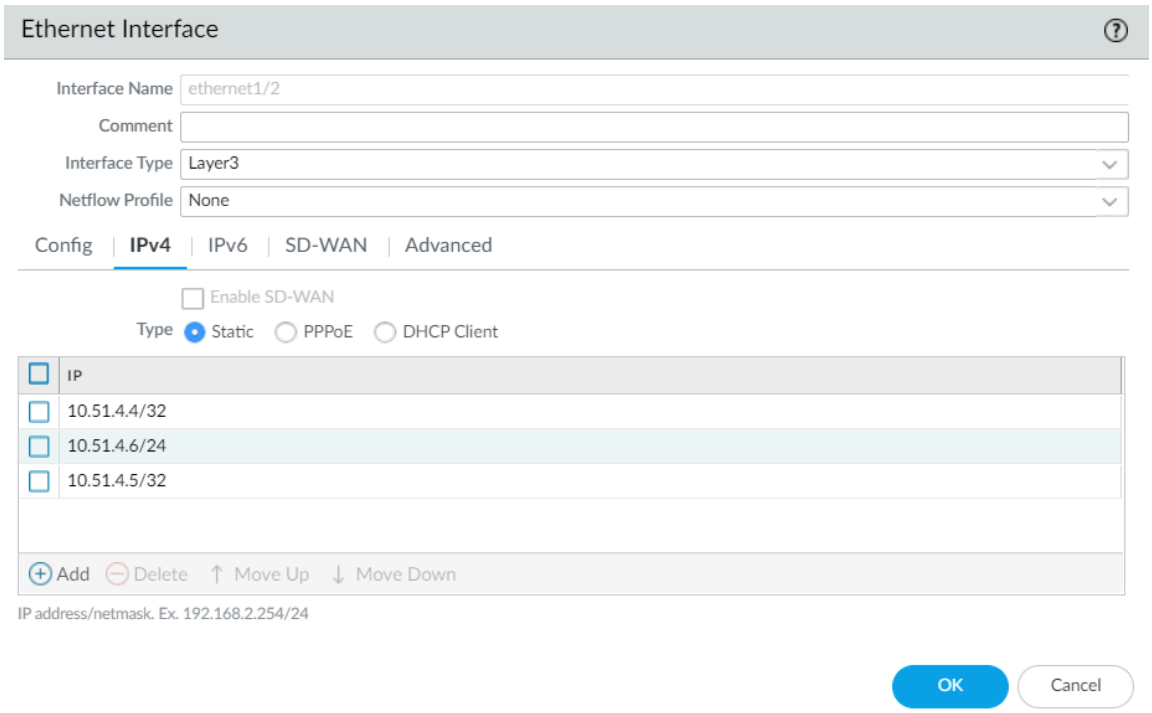
パッシブ HA ピアのデプロイとセットアップを行う前に、アクティブ HA ピアで次の手順を実行します。

1. ファイアウォール インターフェイスにログインします。
2. ethernet 1/1 を untrust インターフェイスとして設定し、ethernet 1/2 を untrust インターフェイスとして設定します。

   Network（ネットワーク） > **Interfaces**（インターフェイス）を選択して次のように設定します。



©2023 Palo Alto Networks, Inc.



3. ethernet 1/3 を HA インターフェイスとして設定します。

   HA2 リンクをセットアップするため、インターフェイスを選択して **Interface Type**（インターフェイス タイプ）を **HA** に設定します。リンク速度とデュプレックスを auto に設定します。



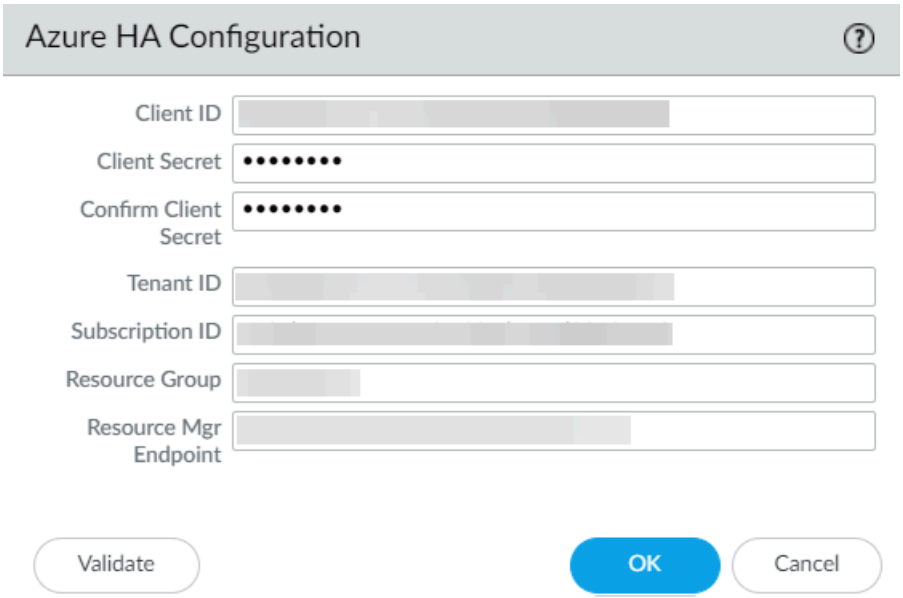
 ©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォールをデプロイした Azure リソース グループに対する認証を実行するように VM-Series プラグインを設定します。

VM-Series プラグインで Azure HA 設定をセットアップします。

クライアント シークレットを暗号化するには、VM-Series プラグイン バージョン 1.0.4 以降を使用します。Panorama を使用してファイアウォールを管理する場合は、VM-Series プラグイン バージョン 1.0.4 以降をインストールする必要があります。

1. **Device**（デバイス） > **VM-Series** を選択して、ファイアウォール プラグインと Azure リソース間のプログラムによるアクセスを有効にします。



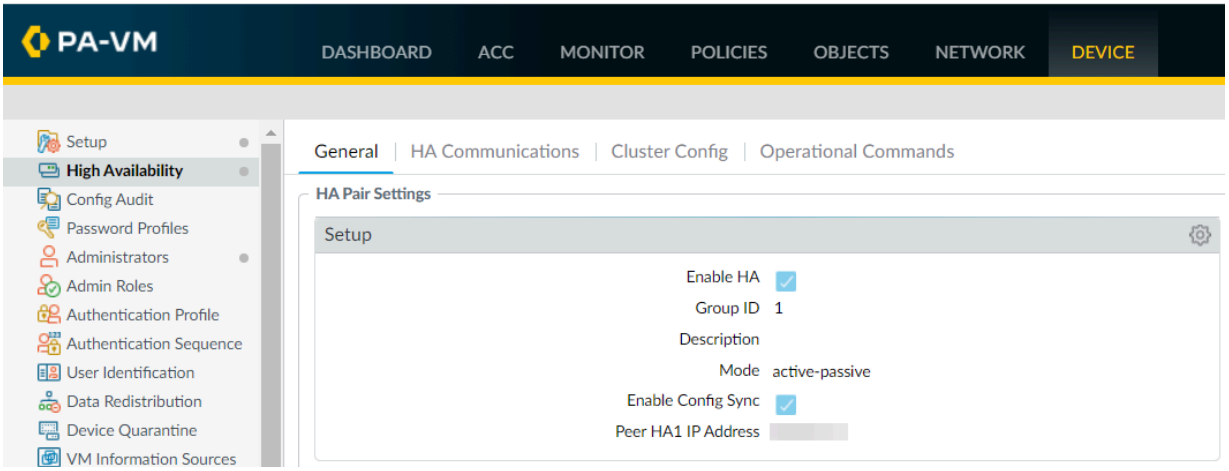
2. **Client ID**（クライアント **ID**）を入力します。クライアント ID は、Azure Active Directory アプリケーションに関連付けられているアプリケーション ID です。
3. **Client Secret**（クライアント シークレット）を入力し、確認用に再び入力します。
4. **Tenant ID**（テナント **ID**）を入力します。テナント ID は、アクティブディレクトリ アプリケーションをセットアップする際に保存したディレクトリ ID です。
5. 監視する Azure サブスクリプションの**Subscription ID**（サブスクリプション **ID**）を入力します。
6. リソースグループ名を入力します。
7. （Azure Stack デプロイメントの場合のみ） リソースマネージャーエンドポイントURLを入力します。

   このフィールドは、*VM-Series* プラグイン *2.1.2* 以降で使用できます。

8. **Validate**（検証）をクリックし、入力したキーおよび ID が有効であり、VM-Series プラグインが API を使用して Azure リソースと通信できることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 4 | HA を有効にします。



1. **Device**（デバイス） > **Setup**（セットアップ） > **HA** を選択します。
2. パッシブ ピアのプライベート IP アドレスとして **Peer HA1 IP address**（ピア **HA1 IP** アドレス）を入力します。
3. （任意）コントロール リンク（HA1）を編集します。コントロール リンクに管理インターフェイスを使用する予定がなく、インターフェイス（ethernet 1/4 など）を追加している場合は、このセクションを編集して、そのインターフェイスを HA1 通信に使用するインターフェイスとして選択します。
4. データ リンク（HA2）を編集し、**Port**（ポート）として ethernet 1/3 を使用するように設定し、このピアの IP アドレスと、サブネットの **Gateway**（ゲートウェイ） IP アドレスを追加します。

STEP 5 | 変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

STEP 6 | 同じ Azure リソース グループ内でパッシブ HA ピアをセットアップします。

1. ファイアウォールの 2 番目のインスタンスをデプロイします。
   - GitHub からカスタム テンプレートおよびパラメータ ファイルをダウンロードします。
   - Azure ポータルにログインします。
   - カスタム テンプレートを検索し、**Deploy from a custom template**（カスタム テンプレートからのデプロイ）を選択します。
   - **Build your own template in the editor**（エディタで専用のテンプレートを作成） > **Load file**（ファイルの読み込み）を選択します。
   - ダウンロードした **azuredeploy.json** を選択して **Save**（保存）を選択します。
   - 入力が完了したら、利用規約に同意して **Purchase**（購入）します。

     入力内容（Azure サブスクリプション、リソース グループの名前、リソース グループの場所、ファイアウォールをデプロイする既存の VNet の名前、VNet CIDR、サブネット名、サブネット CIDR）が、すでにデプロイされているファイアウォール インスタンスと一致していることを確認し、管理サブネット、trust サブネット、untrust サブネットの IP アドレスを開始します。
2. ステップ 1 とステップ 2 を繰り返して、インターフェイスをセットアップし、ファイアウォールをパッシブ HA ピアとして設定します。
3. ステップ 3 を省略し、「HA の有効化（ステップ 5）」の手順を完了します。ステップ 4 で、このパッシブ HA ピアに合わせて IP アドレスを変更します。

STEP 7 | 両方のファイアウォールの設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のデバイスで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブ ファイアウォールで、**Sync to peer** （ピアと同期）リンクをクリックします。
3. 次のように、ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **passive**、**Running Config** （行コンフィグ）が **synchronized** と表示されます。
   - アクティブ ファイアウォールローカル ファイアウォールの状態が **active**、**Running Config**（実行コンフィグ）が **synchronized** と表示されます。
4. パッシブ ピアで VM-Serie プラグインの設定が同期されていることを確認します。

   Device（デバイス） > **VM-Series** を選択し、パッシブ ピアで設定を省略した Azure HA 構成が表示されていることを確認します。

©2023 Palo Alto Networks, Inc.

ARM テンプレートを使用した VM-Series ファイアウォールのデプロイ

Palo Alto Networks はマーケットプレイス ベースのデプロイに加えて、サンプル ARM テンプレートをホストしている GitHub リポジトリを提供しており、ダウンロードしたら必要に応じてカスタマイズすることもできます。ARM テンプレートとは、ネットワーク インターフェイス、完全な仮想マシン、さらには複数の仮想マシンを伴うアプリケーション スタック全体といった個々のリソースで必要となる各リソースを記述した JSON ファイルです。

ARM テンプレートは上級者向けであり、Palo Alto Networks はコミュニティがサポートしているポリシーの元で ARM テンプレートを提供しています。ARM テンプレートの情報については、ARM テンプレートについての Microsoft ドキュメントをご覧ください。

必要なすべてのリソースを簡単にデプロイできるよう、2 層式のサンプル テンプレート（https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample）には次の 2 つの JSON ファイルが含まれています。

- **Template** ファイル — azureDeploy.json は、リソース グループ内のすべてのコンポーネントをデプロイするメインのリソースファイルです。
- **Parameters** ファイル — azureDeploy.parameters.json は、VNet 内で VM-Series ファイアウォールを正常にデプロイするために必要となる各パラメータが含まれたファイルです。これには、仮想マシンの層およびサイズ、ファイアウォールのユーザー名およびパスワード、ファイアウォール用のストレージ コンテナの名前といった詳細データが含まれています。このファイルは Azure VNet のデプロイ環境に合わせてカスタマイズできます。

ファイアウォールをインターネットに接続されたアプリケーションのゲートウェイとしてデプロイできるように、テンプレートでは VM-Series ファイアウォール、データベース サーバー、Web サーバーがプロビジョニングされます。VNet はルーティングできないプライベートな IP アドレス空間 192.168.0.0/16 を使用します。172.16.0.0/12 あるいは 10.0.0.0/8 を使用するようテンプレートに変更を加えることもできます。

また、ARM テンプレートは必要なユーザー定義のルールおよび IP 転送フラグも提供し、VM-Series ファイアウォールが Azure リソース グループを保護できるようにします。テンプレートに含まれている 5 つのサブネット（Trust、Untrust、Web、DB、NAT）については、5 つのルート テーブル（トラフィックを VM-Series ファイアウォールおよび NAT 仮想マシンにルーティングするためのユーザー定義のルールを持つ各サブネットに 1 つずつ）があります。

テンプレートに含まれている 4 つのサブネット（Trust、Untrust、Web、DB）については、4 つのルート テーブル（トラフィックを VM-Series ファイアウォールにルーティングするためのユーザー定義のルールを持つ各サブネットに 1 つずつ）があります。

©2023 Palo Alto Networks, Inc.

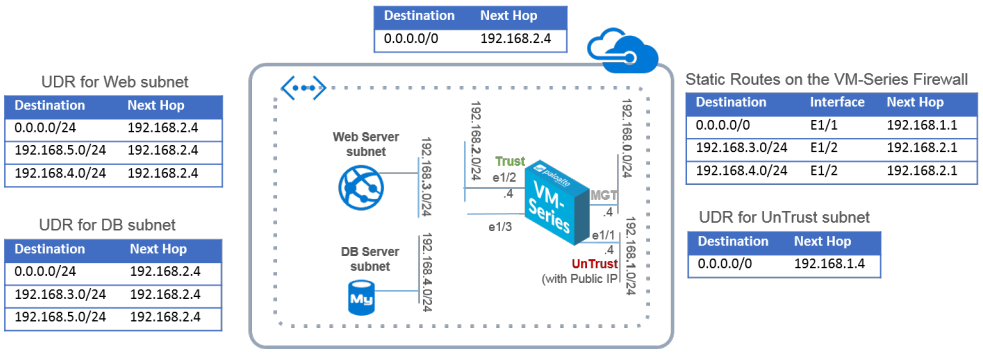


図 **4 : ARM** テンプレートを使用した **VM-Series** ファイアウォールのデプロイ

STEP 1 | GitHub リポジトリから 2 層式のサンプル ARM テンプレートをダウンロードします。

ファイルをローカルクライアントにダウンロード、保存します: https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample

STEP 2 | Azure でリソース グループを作成します。

1. **azurelogin**コマンドを実行してAzure CLIにログインします。

   Azure Government または Azure China で CLI にアクセスする方法の詳細は、CLI のインストールに関する Azure ドキュメントを参照してください。
2. 次のコマンドを実行してリソース マネージャー モードに切り替えます: **azureconfig mode arm**
3. リソース グループを作成します。

STEP 3 | ARM テンプレートをデプロイします。

1. テキスト エディタで Parameters ファイルを開き、デプロイ環境に合わせて値を変更します。

   Azure China で、*VM-Series* ファイアウォールをデプロイするために必要な *VHD* イメージをホストするストレージ アカウントのパスを編集する必要があります。テンプレート ファイルの変数セクションで、***userImageNameURI*** というパラメータを見つけ、その値を *VHD* イメージを保存した場所に置き換えます。
2. 作成したリソース グループにテンプレートをデプロイします。

```
azure group create -v -n “<YourResourceGroupName>”

-l “<YourAzureLocation>” -d “<GiveASmallDeploymentLabel>”

-f azureDeploy.json -e azureDeploy.parameters.json
```


©2023 Palo Alto Networks, Inc.

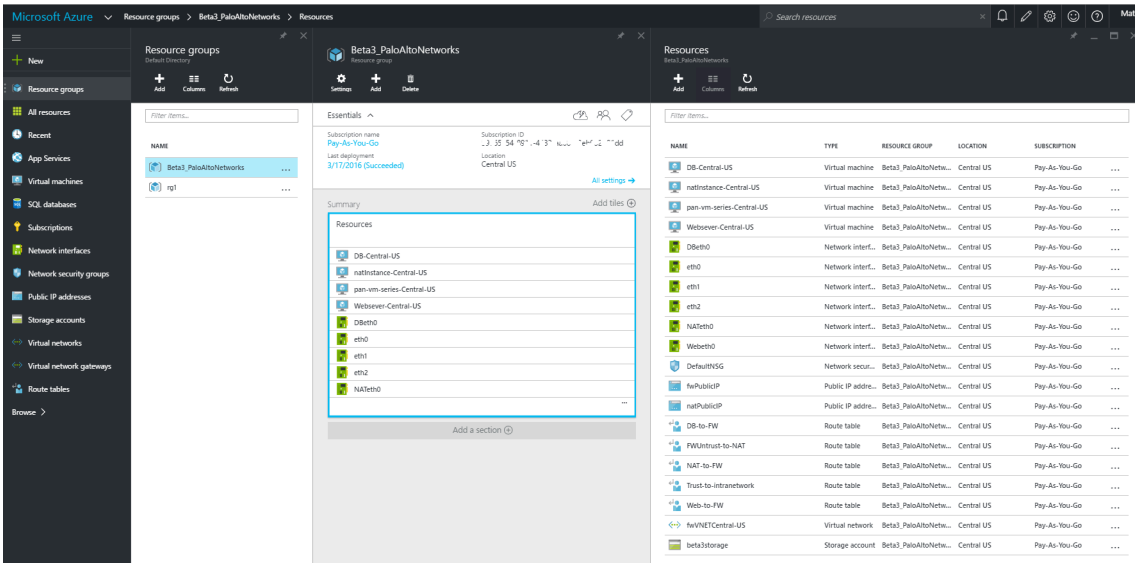
3. Azure CLI からデプロイの進行状況/ステータスを確認します。

```
azure group deployment show "<YourResourceGroupName>"


“<YourDeploymentLabel>“
```

テンプレートが正常にデプロイされた場合: `ProvisioningStateis Running`。

`ProvisioningStateis Failed` が表示された場合は、*Azure* ポータルの ***Resource Group***（リソース グループ）**>** ***Events***（イベント）にてエラーを確認してください。フィルタリングして直近 *1* 時間のイベントのみ表示し、最近のイベントを選択し、データを吟味してエラーを見つけます。

4. VM-Series ファイアウォールが正常にデプロイされたことを確認します。
   1. **Dashboard**（ダッシュボード） > **Resource Groups**（リソース グループ）を選択し、リソース グループを選択します。
   2. 詳細な状態については、**All Settings**（すべての設定） > **Deployments**（デプロイ） > **Deployment History**（デプロイ履歴）を選択します。



ARM テンプレート内の定義に従い、*VNet* 内のアドレス空間はプレフィックス *192.168* を使用します。

5. パブリック IP アドレスをファイアウォールの untrust インターフェイスにアタッチします。

©2023 Palo Alto Networks, Inc.

STEP 4 | ファイアウォールを VNet ゲートウェイとして構成し、インターネット接続を利用するデプロイを保護します。

1. ファイアウォールの管理インターフェイスの IP アドレスにログインします。
2. データプレーン ネットワーク インターフェイスをファイアウォールのレイヤー 3 インターフェイスとして設定します（**Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**）。
3. ファイアウォール上の仮想ルーターに静的ルールを追加します。この例でファイアウォールを介してトラフィックをルーティングするには、ファイアウォール上にスタティック ルートが 3 つ必要です（**Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）でルーターを選択して **Static Routes**（静的 ルート）をクリック）。
   1. すべてのアウトバウンド トラフィックを UnTrust ゾーン、ethernet1/1 を介して 192.168.1.1 にある Azure ルーターへとルーティングします。
   2. Web サーバーのサブネットに向かうすべてのインバウンド トラフィックを Trust ゾーン、ethernet1/2 を介して 192.168.2.1 にある Azure ルーターへとルーティングします。
   3. データベース サーバーのサブネットに向かうすべてのインバウンド トラフィックを Trust ゾーン、ethernet1/2 を介して 192.168.2.1 にある Azure ルーターへとルーティングします。
4. セキュリティ ポリシー ルールを作成（**Policies**（ポリシー） > **Security**（セキュリティ））し、ファイアウォールでインバウンドおよびアウトバウンド トラフィックを許可します。また、Web サーバーのサブネットからデータベース サーバーのサブネットに向かうトラフィック、およびその逆向きのトラフィックをセキュリティ ポリシー ルールに許可させる必要もあります。
5. ファイアウォールへの変更を **Commit**（コミット）します。
6. VM-Series ファイアウォールがトラフィックを保護することを確認します（**Monitor**（監視） > **Logs**（ログ） > **Traffic**（トラフィック））。

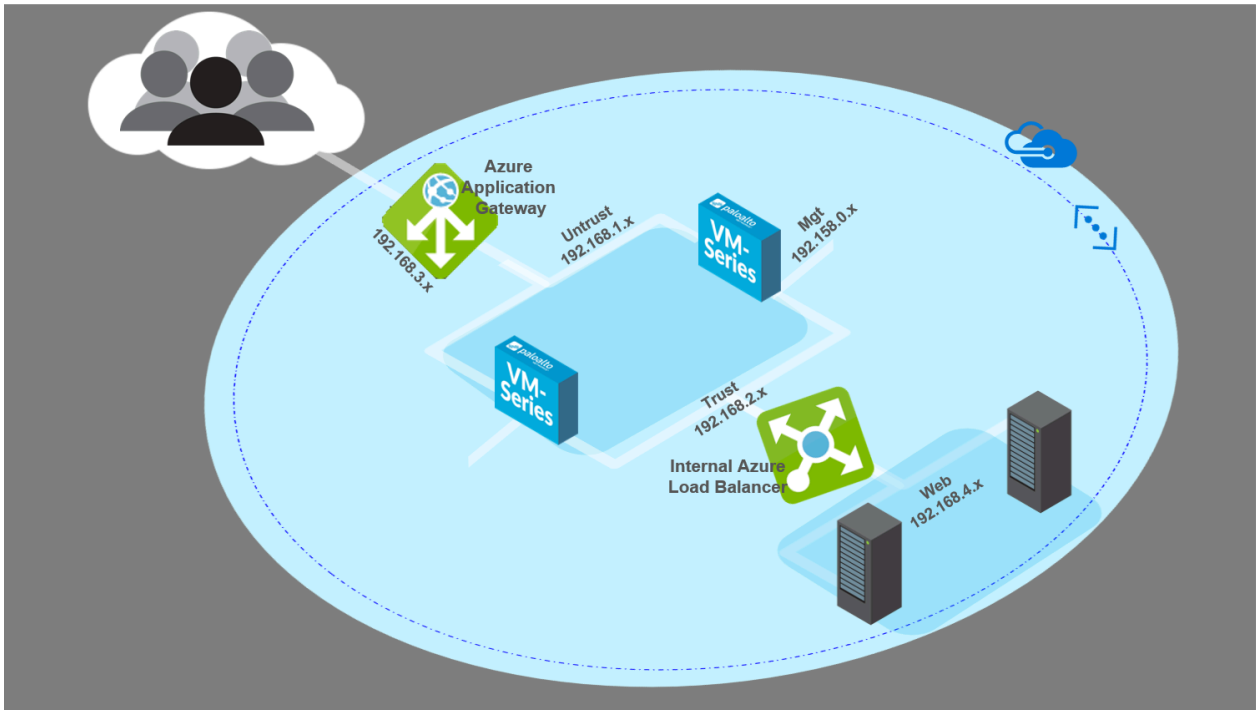
©2023 Palo Alto Networks, Inc.

VM-Series and Azure Application Gateway テンプレートのデプロイ

VM-Series and Azure Application Gateway テンプレートは、Microsoft Azure（現在、Azure China では使用できません）でのインターネットに接続されたデプロイの Web ワークロードを保護する目的で、VM-Series ファイアウォールをデプロイするために使用できるスターター キットです。

このテンプレートでは、（内部と外部の）Azure Load Balancer のペア間で 2 つの VM-Series ファイアウォールをデプロイします。外部ロード バランサーは Azure Application Gateway です。これはインターネットに接続されたゲートウェイとしても機能する HTTP（Layer 7）ロード バランサーであり、トラフィックを受信し、VM-Series ファイアウォール経由で内部ロード バランサーに配布します。内部ロード バランサーは Web サーバーのペアに面した Azure Load Balancer（Layer 4）です。このテンプレートは、BYOL および Azure マーケットプレイス バージョンの VM-Series ファイアウォールをサポートしています。

Web ワークロードでの要求が増大し、Web サーバー層の容量を増やした場合は、追加の VM-Series ファイアウォールを手動でデプロイして Web サーバー層を保護することができます。

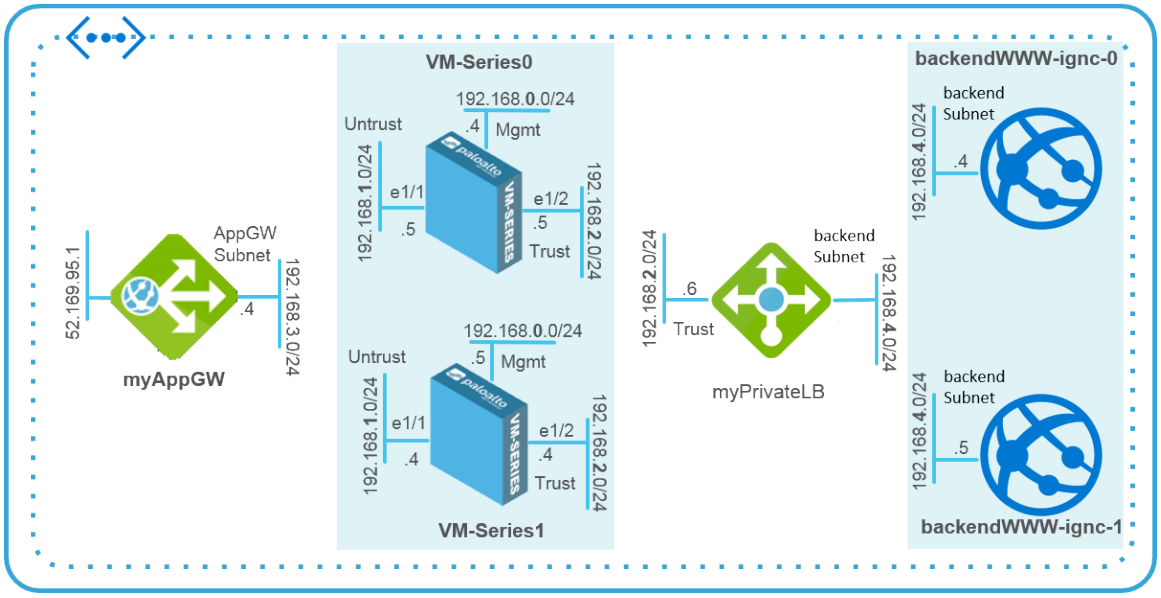


- VM-Series and Azure Application Gateway テンプレート
- VM-Series および Azure Application Gateway テンプレートの使用開始

©2023 Palo Alto Networks, Inc.

VM-Series and Azure Application Gateway テンプレート

VM-Series and Azure Application Gateway テンプレートは、Azure Application Gateway（レイヤー 7 ロード バランサー）と Azure（レイヤー 4）ロード バランサーを起動します。アプリケーション ゲートウェイとロード バランサーの間では、高可用性セットの VM-Series ファイアウォールのペアと、別の高可用性セットの Ubuntu 上で Apache2 が動作しているサンプル Web サーバーのペアがネストされます。高可用性セットは、予定されているシステム停止と予期せぬシステム停止の両方からシステムを保護します。以下のトポロジー図に、テンプレートでデプロイされるリソースを示します。



新規または既存のストレージ アカウントとリソース グループを使用して、Azure ロケーション内にあるこのソリューション用のすべてのリソースをデプロイできます。リソース グループ名とストレージ アカウント名のデフォルトはありませんので、必ず名前を入力してください。新規の VNet を作成するか、既存の VNet を使用できますが、テンプレートは CIDR ブロック 192.168.0.0/16 を使用して *vnet-FW* という名前のデフォルト VNet を作成し、5 つのサブネット（192.168.1.0/24 ～ 192.168.5.0/24）を割り当てて、Azure Application Gateway、VM-Series ファイアウォール、Azure Load Balancer、および Web サーバーをデプロイします。各 VM-Series ファイアウォールは 3 つのネットワーク インターフェイスでデプロイされ、管理サブネット（192.168.0.0/24）には ethernet0/1、アントラスト サブネット（192.168.1.0/24）には ethernet1/1、そしてトラスト サブネット（192.168.2.0/24）には ethernet1/2 が配置されます。

テンプレートは、ポート 80,443、および 22 上の任意のソース IP アドレスからのインバウンド トラフィックを許可するネットワーク セキュリティ グループ（NSG）を作成します。また、VM-Series ファイアウォールのペアと Web サーバーのペアをそれぞれの高可用性セットにデプロイし、計画された、あるいは予期せぬメンテナンス期間中にそれぞれ最低 1 つのインスタンスが利用できるようにします。各高可用性セットは、3 つのデフォルト ドメインと 5 つのアップデート ドメインを使用します。

Azure Application Gateway はリバース プロキシ サービスとして機能し、クライアント接続を終端して、リクエストをバックエンド Web サーバーに転送します。Azure Application Gateway は HTTP リスナーと共にセットアップされ、デフォルトのヘルス プローブを使用して VM-Series

©2023 Palo Alto Networks, Inc.

ファイアウォールの IP アドレス（ethernet1/1）の状態が良好でトラフィックを受信できることをテストします。

テンプレートはオート スケーリング ソリューションは提供しないため、自分でキャパシティ ニーズを計画して、環境でのテンプレートの適用を行うために必要なリソースをデプロイする必要があります。

VM-Series ファイアウォールは、Web サーバーに向けられた Web トラフィックを受信して保護するようには設定されていません。したがって、VM-Series ファイアウォールからデフォルトのルーターにトラフィックを送信するためのスタティック ルートでファイアウォールを設定し、トラフィックをロード バランサーの IP アドレスに戻すための送信先 NAT ポリシーとセキュリティ ポリシー ルールを設定しなければなりません。NAT ポリシー ルールは、ファイアウォールが Azure Application Gateway 上の HTTP リスナーからの応答をヘルス プローブに戻すためにも必要です。基本的なファイアウォール設定を支援するため、GitHub リポジトリには *appgw-sample.xml* というサンプル設定ファイルが用意されており、このファイルから作業を開始することができます。

VM-Series および Azure Application Gateway テンプレートの使用開始

VM-Series & Azure Application Gateway テンプレートでは、Azure China を除き、Microsoft Azure でインターネットに接続されたデプロイの Web ワークロードをデプロイして保護するために必要なすべてのリソースが起動されます。このセクションでは、テンプレートをデプロイし、Web サーバーに向かうトラフィックをルーティングして保護するためにファイアウォールを設定し、このテンプレートがデプロイのニーズに対応するために提供する機能およびリソースを拡張する方法についての詳細を説明します。

- Azure へのテンプレートのデプロイ
- VM-Series and Azure Application Gateway テンプレートのパラメータ
- サンプルの設定ファイル
- テンプレートの適用

Azure へのテンプレートのデプロイ

Azure にテンプレートをデプロイするには、以下の手順を実行します。

©2023 Palo Alto Networks, Inc.

STEP 1 | テンプレートをデプロイします。

現在、*Azure China* でのデプロイには使用できません。

1. https://github.com/PaloAltoNetworks/azure-applicationgateway からテンプレートにアクセスします。
2. **Deploy to Azure**（**Azure** にデプロイ）をクリックします。
3. テンプレートをデプロイするために詳細を入力します。各パラメータの説明およびデフォルト値（存在する場合）については、「VM-Series and Azure Application Gateway テンプレートのパラメータ」を参照してください。

   少なくとも、**Azure Subscription**（**Azure** サブスクリプション）、**Resource Group**（リソース グループ）、**Location**（ロケーション）、**Storage Account Name**（ストレージ アカウント名）、および VM-Series ファイアウォールの管理者アカウントの

©2023 Palo Alto Networks, Inc.

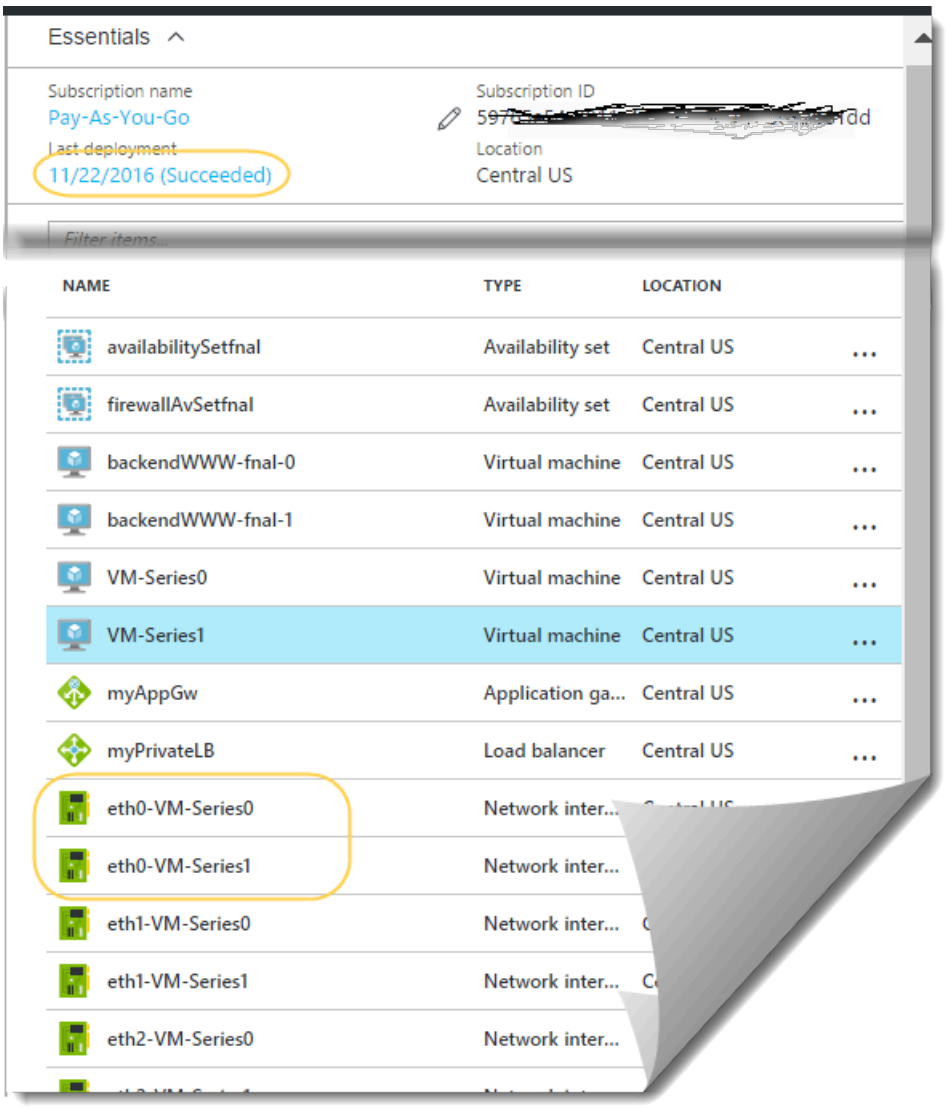
Username/password（ユーザー名/パスワード）または **SSH Key**（**SSH** キー）を入力する必要があります。

4. **Purchase**（購入）をクリックして契約条件に同意し、リソースをデプロイします。

   検証エラーが発生した場合、クリックして詳細を確認し、エラーを修正してください。

5. Azure ポータルで、VM-Series ファイアウォールを含むテンプレート リソースが正常にデプロイされたことを確認します。

   1. **Dashboard**（ダッシュボード） > **Resource Groups**（リソース グループ）を選択し、リソース グループを選択します。
   2. **Overview**（概要）を選択し、デプロイしたすべてのリソースを確認します。デプロイのステータスが **Succeeded**（成功）と表示されているはずです。



3. VM-Series ファイアウォールの管理インターフェイスにアクセスするために、**eth0-VM-Series0** および **eth0-VM-Series1** に割り当てられたパブリック IP アドレスまたは DNS 名を書き留めます。

©2023 Palo Alto Networks, Inc.

STEP 2 | ファイアウォールにログインします。

1. Web ブラウザから安全な接続（https）を使用し、eth0-VM-Series0 の IP アドレスまたはファイアウォールの DNS 名にログインします。
2. Parameters ファイルで定義した ユーザー名/パスワードを入力します。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。

STEP 3 | VM-Series ファイアウォールを設定します。

ファイアウォールを手動で設定することも、GitHub リポジトリに用意されているサンプルの設定ファイルをインポートして各自のセキュリティのニーズに合わせてカスタマイズすることもできます。

- ファイアウォールを手動で設定する – 少なくとも以下を行う必要があります。

1. データプレーン ネットワーク インターフェイスをファイアウォールのレイヤー 3 インターフェイスとして設定します（**Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**）。
2. ファイアウォール上の仮想ルーターに静的ルールを追加します。この静的ルールによって、ファイアウォールの untrust インターフェイス IP アドレスを ethernet1/1 に向かうトラフィックのネクストホップ アドレスとして指定します（**Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）で、ルーターを選択して **Static Routes**（静的ルート）をクリックします）。
3. セキュリティ ポリシー ルールを作成（**Policies**（ポリシー） > **Security**（セキュリティ））し、ファイアウォールでインバウンドおよびアウトバウンド トラフィックを許可します。
4. NAT ポリシーを追加します（**Policies**（ポリシー） > **NAT**）。ファイアウォールで宛先 NAT ルールおよび送信元 NAT ルールを作成し、トラフィックを Web サーバーに送信して、リクエストを開始したクライアントに戻す必要があります。

   宛先 NAT ルールはファイアウォールの untrust インターフェイスに到達するすべてのトラフィックに適用されます。このルールは、パケットの宛先 IP アドレスを内部ロード バランサーの IP アドレスに変換して、すべてのトラフィックが内部ロード バランサーに向けられ、バックエンド Web サーバーに向けられるようにするために必要です。

   送信元 NAT ルールは、バックエンド Web サーバーから発信され、ファイアウォールの untrust インターフェイスに向かうすべてのトラフィックに適用されます。このルールにより、送信元アドレスをファイアウォールの trust インターフェイスの IP アドレスに変換します。
5. 変更を **Commit**（コミット）します。
   - サンプルの設定ファイルのインポート
6. サンプルの設定ファイルをローカル クライアントにダウンロードして保存します。
7. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択し、**Import named configuration snapshot**（名前を付けて保存した設定スナップショットをイン

©2023 Palo Alto Networks, Inc.

ポート）をクリックして、ローカルに保存したサンプルの設定ファイルを **Browse**（参照）し、**OK** をクリックします。

8. **Load named configuration snapshot**（名前を付けて保存した設定スナップショットを読み込む）をクリックし、先ほどインポートしたサンプルの設定ファイルの **Name**（名前）を選択して **OK** をクリックします。
9. 使用した CIDR ブロックからの IP アドレスに一致するように、アドレス オブジェクトの IP アドレスおよびスタティック ルートを変更します。eth1-VM-Series0 および eth1-VM-Series1 のプライベート IP アドレスを使用するようアドレス オブジェクトを更新します。
10. 重要 |新しい管理者ユーザー アカウントを作成します。**Device**（デバイス） > **Administrators**（管理者）の順に選択し、新しいアカウントを **Add**（追加）します。
11. **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）の General Settings（全般設定）ウィジェットで **Hostname**（ホスト名）を変更します。
12. 変更内容を **Commit**（コミット）し、ログアウトします。このコミットにより、現在アクティブな設定がサンプルの設定ファイルと先ほど行った更新で上書きされます。コミット時に、テンプレートをデプロイするときに指定したホスト名と管理者ユーザー アカウントが上書きされます。以後、新しい管理者ユーザー アカウントとパスワードを使用してログインする必要があります。
    - ファイアウォールにログインする – 作成した認証情報を使用し、サンプルの設定ファイルの一部としてインポートした pandemo 管理者アカウントを削除します。

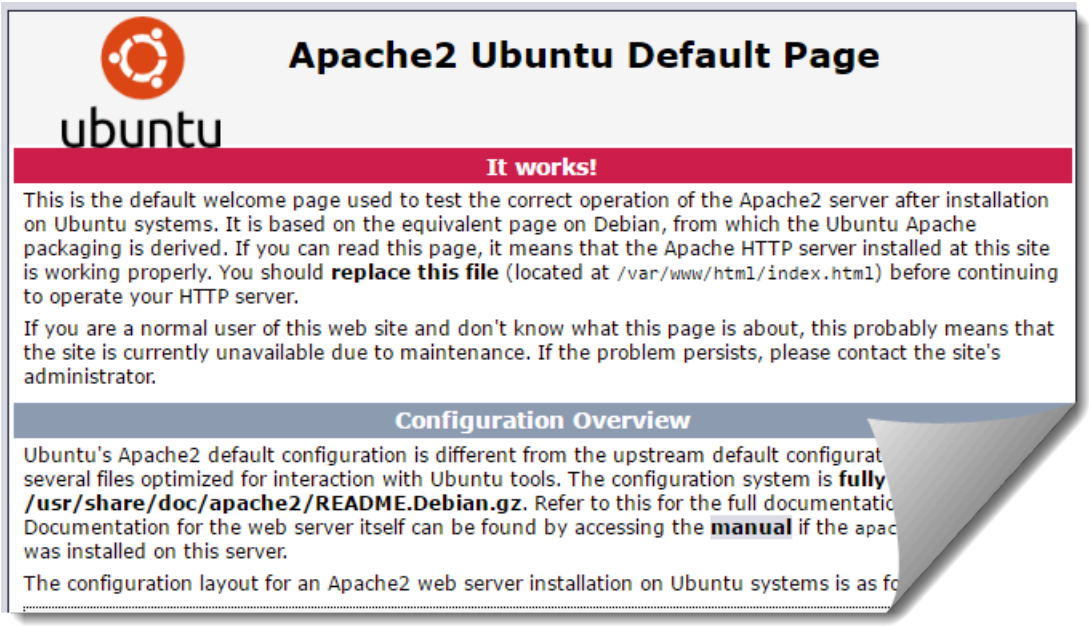
STEP 4 | ログインしてその他の VM-Series ファイアウォールのインスタンスを設定します。

「VM-Series ファイアウォールを設定します」の手順を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 5 | ファイアウォールが正しく設定されたことを確認します。

Web ブラウザから、http を使用してアプリ ゲートウェイの IP アドレスまたは DNS 名にアクセスします。デフォルトの Apache 2 Ubuntu Web ページが表示されるはずです。



サンプル設定のファイアウォールを使用した場合、ファイアウォールにログインし、**Monitor**（監視） > **Logs**（ログ） > **Traffic**（トラフィック）で始まるセッションで生成されたトラフィック ログを表示します。

VM-Series and Azure Application Gateway テンプレートのパラメータ

必須パラメータと任意のパラメータ、およびデフォルト値がある場合はそれらを下表に示します。

パラメータ	概要
Resource group（リソース グループ）	新規のリソース グループを作成するか、または既存のリソース グループを指定します（デフォルトなし）。
サブスクリプション	テンプレートでデプロイするリソースのコストをカバーするために使用する Azure サブスクリプションのタイプ。
場所	テンプレートをデプロイする Azure ロケーションを選択します（デフォルトなし）。
Network Security Group（ネットワーク セキュリティ グループ）	
Network Security Group Name（ネットワーク	ネットワーク セキュリティ グループは、VM-Series ファイアウォールと Web サーバーにアクセスできるソース IP アドレスを制限します。

©2023 Palo Alto Networks, Inc.

パラメータ	概要
セキュリティ グループ名）	デフォルト: nsg-mgmt
Network Security Group Inbound Src IP（ネットワーク セキュリティ グループ インバウンド ソース IP）	テンプレートによってデプロイされる VM の管理ポートにログインできるソース IP アドレスです。 デフォルト値の 0.0.0.0/0 は、どの IP アドレスからでもファイアウォールの管理ポートにログインできることを意味します。
ストレージアカウント	
Storage Account Name（ストレージ アカウント名）	新規のストレージ アカウントを作成するか、または既存のストレージ アカウントを指定します（デフォルトなし）。名前はグローバルに一意でなければなりません。
Storage Account Type（ストレージ アカウント タイプ）	標準およびプレミアム ストレージのいずれかと、データ複製ニーズをローカル冗長性、ジオ冗長性、およびリード アクセス ジオメトリ冗長性から選択します。 デフォルトはローカル冗長ストレージ（LRS）です。その他に、標準 GRS、プレミアム LRS、および標準 RAGRS があります。
VNet	
仮想ネットワーク	新規の VNet を作成するか、または既存の VNet を指定します。 VNet のデフォルト名は vnet-FW です。
Virtual Network Address Prefix（仮想ネットワーク アドレス プレフィックス）	192.168.0.0/16
Azure Application Gateway	
App Gateway Name（アプリケーション ゲート名）	myAppGw
App Gateway DNS Name（アプリケーション ゲート DNS 名）	グローバルに一意な Azure Application Gateway の DNS 名を入力します。
App Gateway Subnet Name and Prefix（アプリケーション ゲートウェ	デフォルトのサブネット名は AppGWSubnet、サブネット プレフィックスは 192.168.3.0/24 です。

©2023 Palo Alto Networks, Inc.

パラメータ	概要
イ サブネット名および プレフィックス）	
Azure Load Balancer および Web サーバー	
Internal Load Balancer Name（内部ロード バランサー名）	myPrivateLB
Internal Load Balancer Name and Prefix（内部ロード バランサー サブネット名およびプレフィックス）	デフォルトの名前は backendSubnet、サブネットプレフィックスは 192.168.4.0/24 です。
Backend Vm Size（バックエンド VM サイズ）	デフォルト サイズは標準層 D1 Azure VM です。テンプレート内のドロップダウンでは、バックエンド Web サーバー用の他の Azure VM オプションを見ることができます。
ファイアウォール	
Firewall Model（ファイアウォール モデル）	BYOL または PAYG から選択します（バンドル 1 またはバンドル 2 で、各バンドルには VM-300 とサブスクリプション セットが含まれます）。
Firewall Vm Name and Size（ファイアウォール VM 名およびサイズ）	ファイアウォールのデフォルト名は VM-Series、デフォルト サイズは標準層 D3 Azure VM です。 テンプレート内のドロップダウンでは、VM-Series ファイアウォール用の他の Azure VM オプションを見ることができます。
Mgmt Subnet Name and Prefix（管理サブネット名およびプレフィックス）	このソリューションでデプロイされている M-Series ファイアウォールと Web サーバーの管理サブネットです。 デフォルトの名前は Mgmt、サブネット プレフィックスは 192.168.0.0/24 です。
Mgmt Public IP Address Name（管理パブリック IP アドレス名）	各ファイアウォール上の管理インターフェイスにアクセスするためのホスト名を入力します。名前はグローバルに一意でなければなりません。
Trusted Subnet Name and Prefix（信頼できるサブネット名とプレフィックス）	VM-Series ファイアウォール上の eth1/1 が接続されるサブネットで、このサブネットは VM-Series ファイアウォールを Azure Application Gateway に接続します。ファイアウォールは、Web サーバーに向けられた Web トラフィックを eth1/1 で受信します。

©2023 Palo Alto Networks, Inc.

パラメータ	概要
	デフォルトの名前は Trust、サブネット プレフィックスは 192.168.2.0/24 です。
Untrusted Subnet Name（信頼されないサブネット名）	VM-Series ファイアウォール上の eth1/2 が接続されるサブネットです。ファイアウォールは、リターンおよびアウトバウンド Web トラフィックをこのインターフェイスで受信します。 デフォルトの名前は Untrust、サブネット プレフィックスは 192.168.1.0/24 です。名前はグローバルに一意でなければなりません。
ユーザー名	VM-Series ファイアウォールおよび Web サーバーの管理者アカウントのユーザー名を入力します。
Authentication Type（認証タイプ）	パスワードによる認証または SSH 公開鍵のどちらかを使用できます（デフォルトなし）。

サンプルの設定ファイル

作業を簡単に開始できるようにするために、GitHub リポジトリには、*appgw-sample.xml* という名前のサンプル設定ファイルが含まれています。このファイルには、以下のルール/オブジェクトが入っています。

- アドレス オブジェクト – **firewall-untrust-IP** と **internal-load-balancer-IP** の 2 つのアドレス オブジェクトです。これらのオブジェクトは、セットアップで IP アドレスを一致させるために変更する必要があります。また、Azure ポータルで eth1-VM-Series0 と eth1-VM-Series1 に割り当てられたプライベート IP アドレスを使用するには、これらのアドレス オブジェクトを変更する必要があります。
- スタティック ルート – ファイアウォールのデフォルトの仮想ルーターには、192.168.1.1 へのスタティック ルートがあります。デフォルトのテンプレートの値を使用する場合は、この IP アドレスが正確なアドレスとなります。信頼できないサブネット CIDR を変更した場合は、セットアップに一致するように IP アドレスを更新する必要があります。送信元がバックエンド Web サーバーで、宛先がアプリケーション ゲートウェイであるすべてのトラフィックは、この IP アドレスを次のホップとして使用して、ファイアウォール上の Untrust インターフェイスにパケットを配信します。
- **NAT** ポリシー ルール – NAT ポリシー ルールにより、宛先 NAT と送信元 NAT が有効になります。
  - 宛先 NAT ルールの対象は、ファイアウォール上の Untrust インターフェイス（ethernet1/2）、つまり firewall-untrust-IP アドレス オブジェクトに到着するすべてのトラフィックです。このルールにより、パケットの宛先 IP アドレスが内部ロード バランサーの IP アドレスに変換されます。そのため、すべてのトラフィックが内部ロード バランサーに送信され、その結果、バックエンド Web サーバーに送信されます。
  - 送信元 NAT ルールの対象は、送信元がバックエンド Web サーバーで、宛先がファイアウォール上の信頼できないネットワーク インターフェイスであるすべてのトラフィックで

©2023 Palo Alto Networks, Inc.

す。このルールにより、送信元アドレスが、ファイアウォール（ethernet1/2）上の Trust インターフェイスの IP アドレスに変換されます。

- セキュリティ ポリシー ルール — サンプル設定ファイルでは、2 つのセキュリティ ポリシー ルールが定義されています。最初のルールでは、すべてのインバウンド Web ブラウジング トラフィックが許可され、ファイアウォールのセッション開始時にログが生成されます。2 番目のルールでは、それ以外のすべてのトラフィックがブロックされ、ファイアウォールのセッション開始時および終了時にログが生成されます。これらのログを使用して、このデプロイメントの Web サーバーへのすべてのトラフィックをモニターできます。
- 管理ユーザーの認証情報 — サンプル設定ファイルには、ファイアウォールにログインするためのユーザー名とパスワードが含まれています。このユーザー名とパスワードは、pandemo/demopassword に設定されています。サンプル設定をインポートしたら、パスワードを変更して強力なカスタム パスワードを設定するか、または新しい管理者アカウントを作成して pandemo アカウントを削除する必要があります。

テンプレートの適用

キャパシティのニーズが増大したら、ニーズを分析して、デプロイ シナリオのテンプレートを拡張できます。計画されたキャパシティ ニーズに合わせてスターター テンプレートを拡張する方法をいくつか説明します。

- Azure Application Gateway の後方に追加の VM-Series ファイアウォールをデプロイします。同じ可用性セットに追加の VM-Series ファイアウォールを手動でインストールするか、または新しい可用性セットを実行して、追加の VM-Series ファイアウォールを手動でデプロイすることができます。
- GitHub リポジトリのサンプル設定ファイルで定義されている基本設定を拡張して VM-Series ファイアウォールを設定します。
- Azure Application Gateway で HTTPS 負荷分散（SSL オフロード）を有効にします。詳細については Azure のドキュメントを参照してください。
- テンプレートに含まれているサンプル Web サーバーを追加または置換します。

©2023 Palo Alto Networks, Inc.

Azure での Kubernetes サービスの保護

Azure Kubernetes サービスを保護するには、まず Panorama 用 Azure プラグインをインストールして、Azure の Azure での Kubernetes サービスの保護 デプロイメントを設定する必要があります。Panorama 用 Azure プラグインはタグ ベースの VM モニタリングとAzure での Kubernetes サービスの保護 をサポートしており、Azure Kubernetes Services（AKS）クラスタのインバウンド トラフィックの保護、および AKS クラスタからのアウトバウンド トラフィックの監視を行います。Panorama統制のデプロイメントにより、Azure のオート スケーリング メトリックとスケール イン、スケール アウトしきい値を活用して、アプリケーション ワークロード リソースの需要の急増や急減を管理し、VM-Series ファイアウォールを個別にスケーリングすることができます。

AKSクラスタのインバウンド トラフィックを保護するために、最初に実施する必要があります。Panorama統制デプロイメントはAzure での Kubernetes サービスの保護 と連係してネットワークとリソースに関する情報を収集し、Azure での Kubernetes サービスの保護 デプロイメントに対するVM-Seriesファイアウォールのオートスケーリング層を作成します。AKS クラスタを保護するために必要な、OS、プラグイン、およびテンプレート バージョンを確認するには、Palo Alto Networks 互換性マトリックスを参照してください。

Palo Alto Networks は、新しい Azure VNet 内に Azure Kubernetes Service（AKS）クラスタをデプロイするための、AKS テンプレートを提供しています。Azure plugin on Panorama は、Azure Kubernetes クラスタの監視、「内部ロード バランサー」として指定したサービスの活用、およびダイナミック アドレス グループで使用できるタグの作成などを行うための、通信をセットアップするために役立ちます。Panorama のダイナミック アドレス グループを活用して、AKS クラスタ上で動作しているサービスにルーティングされるインバウンド トラフィックに、セキュリティ ポリシーを適用することができます。

- Azure Secure Kubernetes Services 用 Panorama プラグインの仕組み
- AKS クラスタの保護

Azure Secure Kubernetes Services 用 Panorama プラグインの仕組み

VM-Series のファイアウォールを使用して、Azure Kubernetes Service（AKS）クラスタのインバウンド トラフィックを保護することができます。VM-Series のファイアウォールは、ロードバランサー（Azure Load Balancer）によって公開されたサービスのみを保護できます。アウトバウンド トラフィックは監視のみ可能です。

この章では、Azure Plugin for PanoramaをAKSクラスタに接続できるようにするさまざまなコンポーネントについて説明します。

- 要件
- AKS クラスタを保護するためのサンプルのハブ アンド スポーク トポロジ
- User Defined Widgets（ユーザー定義ウィジェット）
- Secure Cluster Communication （安全なクラスタ通信）
- Kubernetes ラベルを使用したダイナミック アドレス グループ

©2023 Palo Alto Networks, Inc.

要件

このソリューションには、以下のものが必要になります。最低システム要件について、互換性マトリックスの Panorama プラグインの情報を参照してください。

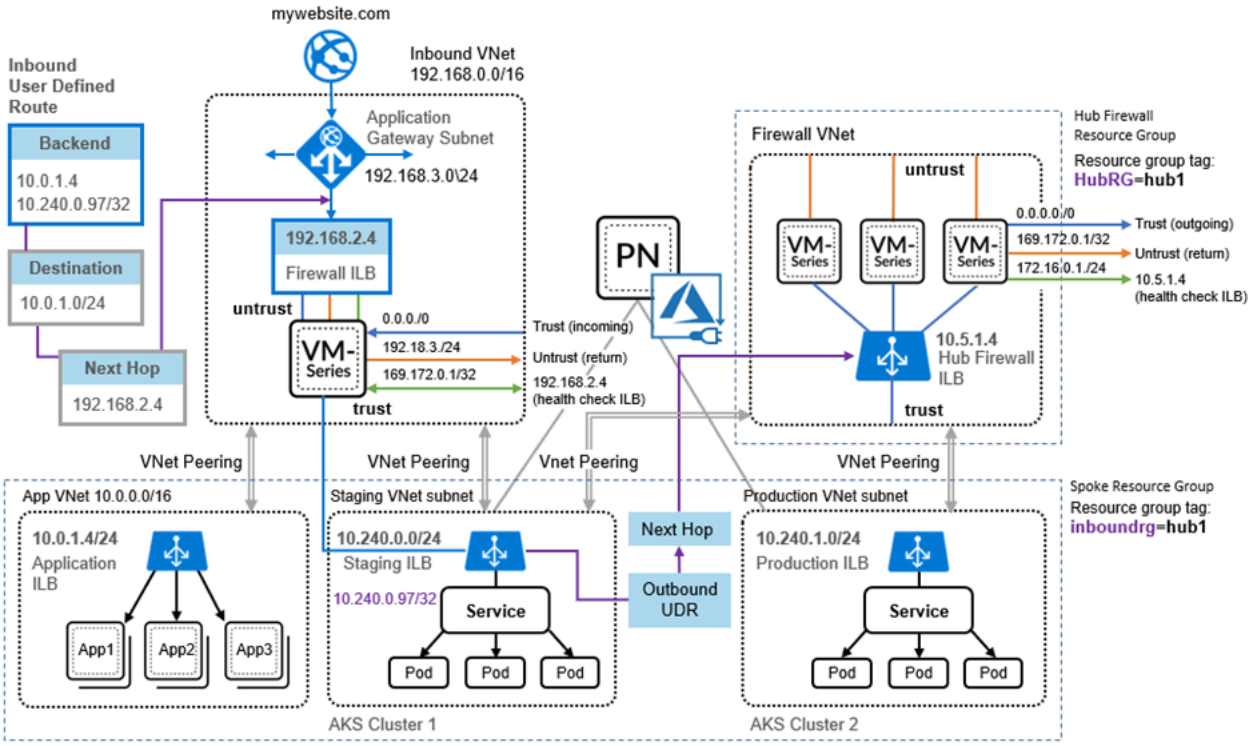
- VM-Series ファイアウォール
- Panorama ー Panorama バージョンは、ご使用の VM-Series PAN-OS バージョン以上でなければなりません。
- Azure 用 Panorama プラグイン
- Panoramaが統制するデプロイ環境。
- Azure AKS template version 1.0.このテンプレートはAKS クラスタを作成します。

  クラスタで AKS の高度なネットワーク（CNI）を有効にする必要があります。

  AKSのデプロイメントでは、ハブアンドスポーク VNet の VNet ピアリングを構成するために高度なネットワークが必要です（AKS クラスタを保護するためのサンプルのハブ アンド スポーク トポロジ)を参照）。

AKS クラスタを保護するためのサンプルのハブ アンド スポーク トポロジ

Azure AKS クラスタのインバウンド トラフィックを保護する、自動スケール デプロイメントのサンプルを以下の図に示します。一部のコンポーネントを確認してみましょう。



- オート スケーリング インフラストラクチャ– Azure オート スケーリング テンプレートは、メッセージング インフラストラクチャと基本的なハブ アンド スポーク アーキテクチャを作成します。
- **AKS** クラスタ– Palo Alto Networks AKSテンプレートは、新しい VNet に AKS クラスタを作成します。スポーク リソース グループの名前を指定すると、Panorama 用 Azure オート ス

©2023 Palo Alto Networks, Inc.

ケーリング プラグインが検出できるように、テンプレートはスポーク リソース グループ名で VNet と AKS クラスタにタグを設定します。Panorama 用 Azure プラグインは、AKSクラスタサービスについて学習するよう、ステージング ILB でサービス IP アドレスのクエリを実行します。

AKS クラスタに関連付けることができるスポーク ファイアウォール スケール セットは*1*つだけです。 単一の *AKS* クラスタで複数のサービスを公開する場合は、それらを同じスポークで保護する必要があります。

リソースグループごとに、サブネットベースのアドレスグループを作成します。たとえば、上の図では、*10.240.0.0 / 24*（*AKS Cluster 1*）のアドレスグループを作成します。

- **VNet** ピアリング—同じリージョン内の他の VNet と通信するには、VNET ピアリング を手動で構成する必要があります。

  クロス リージョン ピアリングはサポートされていません。

  他の自動化ツールを使用して、*AKS* クラスタをデプロイできます。既存の *VNet*（ハブ ファイアウォール *VNet* など）にデプロイする場合は、インバウンドおよびアウトバウンドのハブ アンド スポークのリソースグループへの *VNet* ピアリングを手動で構成し、*VNet*および*AKS*クラスタにリソースグループ名を手動でタグ付けする必要があります。

- ユーザー定義のルートとルール—ユーザー定義のルートとルールを手動で構成する必要があります（User Defined Widgets（ユーザー定義ウィジェット）を参照）。上の図では、UDR ルールに従って、受信トラフィックを検査のためにファイアウォール ILB にリダイレクトできます。AKS クラスタを出るアウトバウンド トラフィックは、Azure ユーザー定義ルーティング（UDR）ルールを使用してハブ ファイアウォール ILB にリダイレクトされます。このソリューションでは、Kubernetes オーケストレーションがそのまま機能するためのデフォルトポリシーとして「すべて許可」を想定していますが、ポリシーを適用するには、許可リストまたは拒否リストを使用して、アウトバウンド トラフィックを許可または拒否できます。

User Defined Widgets（ユーザー定義ウィジェット）

インバウンド または アウトバウンド トラフィックを管理するには、ユーザー定義のルーティングとルーティングルールを手動で作成する必要があります。

インバウンド

上の図では、アプリケーション ゲートウェイからのインバウンド トラフィックがバックエンドプールに送られ、UDR ルールに基づいてファイアウォール ILB にリダイレクトされます。たとえば、VNet サブネットを指す UDR を作成して、Kubernetes サービスのトラフィックがファイアウォール ILB を指すようにします。

アウトバウンド

ハブ ファイアウォール セットでは、保護される AKS クラスタごとに、クラスタ サブネット CIDR の静的ルートを作成する必要があります。ネクストホップはハブ VNet の信頼されたサブネットのゲートウェイアドレスです。

©2023 Palo Alto Networks, Inc.

AKS クラスタのすべてのアウトバウンド トラフィックは、単一の UDR ルールで設定されたハブ ファイアウォールに送信されます。

Secure Cluster Communication（安全なクラスタ通信）

Azure用の Panorama プラグインは、特定の AKS クラスタのAKS コントローラー ノードとのみ通信できます。アウトバウンド AKS トラフィックの場合、ネクストホップはハブ ファイアウォール ILB です。アウトバウンド トラフィックが監視されるため、すべてのトラフィックを許可する必要があります。次のトピックでは、接続の確立に役立つ一般的な方法を強調しています。ネットワークとサブネットを計画するときは、これらを覚えておいてください。

- AKS クラスタ認証を作成
- アドレス グループを使用してトラフィックを識別する
- トップ レベル ポリシーにサブネット アドレス グループを追加する
- ワークロードと AKS クラスタ VNet がピアリングされている場合のアプリケーションの中断を防止

AKS クラスタ認証を作成

Panorma 用のAzureプラグインで AKS クラスタを接続するときは、シークレット認証トークンを入力する必要があります。Kubernetes コマンドを使用して、次の手順を実行します。

STEP 1 | ClusterRoleを作成します。

STEP 2 | ClusterRoleBinding を作成します。

1. ClusterRoleBinding の `.yaml` ファイルを作成します。たとえば `crb.yaml` という名前のテキスト ファイルを作成します。

```
apiVersion: rbac.authorization.k8s.io
kind: ClusterRoleBinding
metadata:
  name: default-view
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: view
subjects:
- kind: ServiceAccount
name: default
namespace: default
```

2. Azure Cloud Shell を使用して `crb.yaml` でロール バインディングを適用します。

   kubectl apply -f crb.yaml

3. 作成したサービス アカウントを確認します。

   kubectl get serviceaccounts

©2023 Palo Alto Networks, Inc.

STEP 3 | サービス アカウント認証情報を `.json` ファイルに保存します。

1. ローカル マシンで、認証情報を保存するディレクトリに移動します。
2. kubectl コマンドを使用してトークンを作成します。

   ```
   MY_SA_TOKEN=‘kubectl get serviceaccounts default -o
   jsonpath=’{.secrets[0].name}’‘
   ```
3. トークン名を確認します。

   ```
   $ echo $MY_SA_TOKEN
   ```
4. 認証情報を表示します。

   ```
   kubectl get secret $MY_SA_TOKEN -o json
   ```

Panorama 用のAzureプラグインで AKS クラスタを接続するときは、ステップ 3.dを参照してください。

アドレス グループを使用してトラフィックを識別する

監視対象のアウトバウンド トラフィックの細分性を作成するには、AKS クラスタ VNet サブネット専用のアドレスグループを作成します（たとえば、上の図の10.240.0.97/32）。次に、すべて許可 を使用する代わりに、着信トラフィックまたは戻りトラフィックを許可するルールを記述できます。

アドレス グループを作成する場合は、AKS コントローラーとワーカーノード間の通信を維持するように注意してください。「トップ レベル ポリシーにサブネット アドレス グループを追加する」を参照してください。

通信が中断されると、アプリケーション トラフィックが失われたり、アプリケーションのデプロイメントに問題が発生したりする可能性があります。

トップ レベル ポリシーにサブネット アドレス グループを追加する

接続を維持するには、アドレス グループが Panorama のトップレベルポリシーの一部である必要があります。クラスタ アドレス グループを構成するか、クラスタ をブートストラップしてクラスタ アドレス グループを構成できます。

VNet ピアリングまたは User Defined Widgets（ユーザー定義ウィジェット） を構成する前に、アドレス グループをトップ レベル ポリシーに追加します。

ワークロードと **AKS** クラスタ **VNet** がピアリングされている場合のアプリケーションの中断を防止

AKS クラスタが別々の VNet で実行される VM ワークロードと共存し、VNet がワークロードスポーク（受信）とハブ（送信）の両方とピアリングされている場合、ワークロードと AKS トラフィックを区別するためにアドレス グループを作成する必要があります。 上記のように、アドレス グループをトップ レベル ポリシーに追加します。

Kubernetes ラベルを使用したダイナミック アドレス グループ

AKS クラスタ リソースを監視する場合、Azure プラグインはAKS サービスの次の IP タグを自動的に生成します。

 ©2023 Palo Alto Networks, Inc.

```
aks.<aks cluster name>.<aks service name>
```

ノード、ポッド、またはその他のリソースのタグは生成されません。

AKS サービスにラベルがある場合、タグは次のようになります（ラベルごとに1つ）。

```
aks.<aks cluster name>.svc.<label>.<value>
```

クラスタ に labelSelector タグが定義されている場合、プラグインは次の IP タグを生成します。

```
aks_<labelSelector>.<aks cluster name>.<aks service name>
```

AKS クラスタの保護

Panorama が Azure Kubernetes Services（AKS）クラスタ内のロード バランサーに接続するには、AKS クラスタとの接続を確立するために、Azure plugin on Panorama を有効にする必要があります。その後、Panorama が設定オブジェクトとポリシー ルールを管理対象ファイアウォールにプッシュできるように、ファイアウォールが属しているテンプレートとデバイス グループを設定する必要があります。

- 開始する前に
- テンプレートを使用した AKS クラスタのデプロイ
- Panorama 用 Azure プラグインでの AKS クラスタの接続
- VNet ピアリングのセットアップ
- ファイアウォール ILB へのトラフィックのリダイレクト
- ポリシー関連 AKS サービスの適用
- AKS サービスのデプロイと保護

開始する前に

AKS を保護するには、まず GitHub で利用できるAzure Auto Scaling（Azure オート スケーリング）ソリューションをデプロイする必要があります。

Kubernetes クラスタ内でサービスとして動作している Web アプリケーションを保護するには、VNets、サブネット、および UDR のプランニングを行う必要があります。VM-Series ファイアウォールと Panorama は、Kubernetes サービスのセキュリティと視認性を提供しています。

- 「Azure Secure Kubernetes Services 用 Panorama プラグインの仕組み」を確認してください。
- Palo Alto Networks の AKS テンプレートを使用するには、AKS の高度なネットワーク が必要です。

©2023 Palo Alto Networks, Inc.

- AKS クラスタをデプロイする前に、AKS サブネットを設計してください。「AKS クラスタを保護するためのサンプルのハブ アンド スポーク トポロジ」および「Secure Cluster Communication （安全なクラスタ通信）」を確認してください。
  - テンプレートは、サンプルとして単一の AKS クラスタ（サービス）を作成します。VNet、VNet のサブネット、およびサービスの CIDR 範囲を指定する必要があります。CIDR 範囲は重複しないようにしてください。
  - 要件に合わせてサブネットのサイズを調整します。パフォーマンスに影響するため、無駄に大きな範囲を指定しないようにしてください。
  - 「User Defined Widgets（ユーザー定義ウィジェット）」を参照してください。大きなサブネット固有のルートではなく、特定の UDR ルートを指定してください。
- VNet のピアリング方法をプランニングします。AKS クラスタのピアリングを行う場合は、「Secure Cluster Communication （安全なクラスタ通信）」を忘れずに読むようにしてください。
- トラフィックを識別する手段について検討してください。
  - アウトバウンド AKS トラフィックでアドレス グループを使用する場合は、「トップ レベル ポリシーにサブネット アドレス グループを追加する」を参照してください。
  - 名前空間で一意ではないサービス名またはタグがある場合は、一意の結果が得られるようにラベル セレクタを使ってタグと名前空間をフィルタリングします。

テンプレートを使用した AKS クラスタのデプロイ

Azure AKS テンプレートは、新しい VNet 内のクラスタをプロビジョニングするサンプルです。

STEP 1 | GitHub で PaloAltoNetworks/azure-aks に移動して、リポジトリからビルド パッケージを探してください。

STEP 2 | ビルド パッケージを解凍します。自己のデプロイに合わせて `azuredeploy.json` および `parameters.json` ファイルを編集して保存します。

STEP 3 | 次の Azure CLI コマンドを実行して、テンプレートをデプロイします。

```
az group deployment validate --resource-group RG_NAME
--template-file azuredeploy.json
--parameters @parameters.json
```

```
az group deployment create --name DEPLOYMENT_NAME
--resource-group RG_NAME
--template-file azuredeploy.json
--parameters @parameters.json
```


©2023 Palo Alto Networks, Inc.

STEP 4 | AKS クラスタにアプリケーションまたはサービスをデプロイします。

1. タイプがロード バランサーになるようにサービス YAML ファイルに注釈を付け、それに service.beta.kubernetes.io/azure-load-balancer-internal: "true" と注釈を付けます。以下に例を示します。

```
 apiVersion: v1
   kind: Service
 metadata:
  name: azure-vote-front
  labels:
    service: "azure-vote-front"
    tier: "stagingapp"
  annotations:
    service.beta.kubernetes.io/azure-load-balancer-internal:
"true"
 spec:
  type: LoadBalancer
ports:
- port: 80
selector:
 app: azure-vote-front
```

2. まだ作業を行っていない場合は、続行する前にAKS クラスタ認証を作成します。
3. AKS クラスタにサービスをデプロイします。

   たとえば、kubectl 経由でアプリケーションをデプロイすることができます。

   kubectl apply -f myapplication.yaml

   たとえば、https://github.com/Azure-Samples/azure-voting-app-redis/blob/master/azure-vote-all-in-one-redis.yaml を参照してください。
4. デプロイ サービスのサービス IP を取得するには、kubectl を使用します。

```
kubectl get services -o wide
```

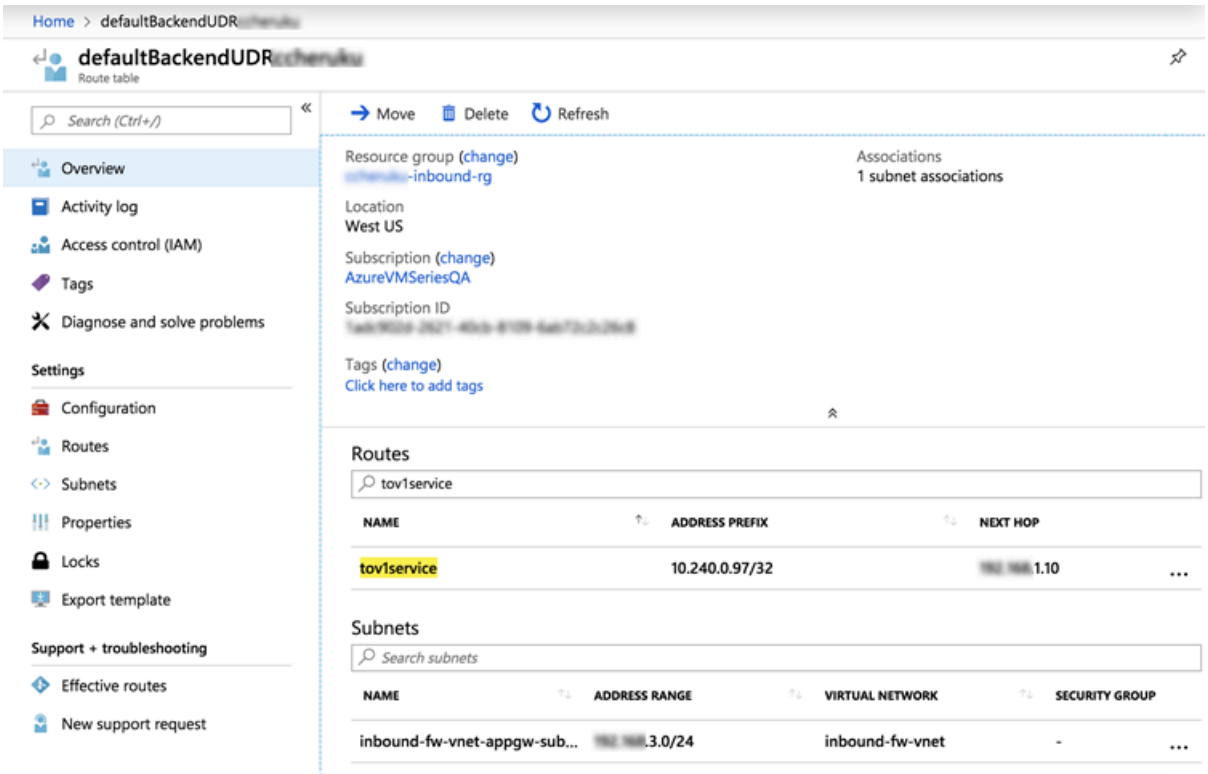
```
NAME               TYPE           CLUSTER-IP     EXTERNAL-IP   PORT(S)          AGE     SELECTOR
azure-vote-back    ClusterIP      10.0.77.21     <none>        6379/TCP         2d23h   app=azure-vote-back
azure-vote-front   LoadBalancer   10.0.18.189    10.240.0.97   80:31937/TCP     2d23h   app=azure-vote-front
kubernetes         ClusterIP      10.0.0.1       <none>        443/TCP          2d23h   <none>
```

   ステップ a に従って、EXTERNAL-IP 列で、10.240.0.97 は ILB 用です。Azure でユーザー定義のルートを作成するには、サービス IP を使用します。

©2023 Palo Alto Networks, Inc.

STEP 5 | サービスが Application Gateway の背後にあるファイアウォール ILB を指すように、UDR ルールを作成します。

Azure でインバウンド スポーク リソース グループに移動し、ルート テーブルを表示して、宛先サービス IP に基づく新しいルートを追加します。次の画面で、tov1service **ADDRESS PREFIX** 列の値はサービス IP です。



Panorama 用 Azure プラグインでの AKS クラスタの接続

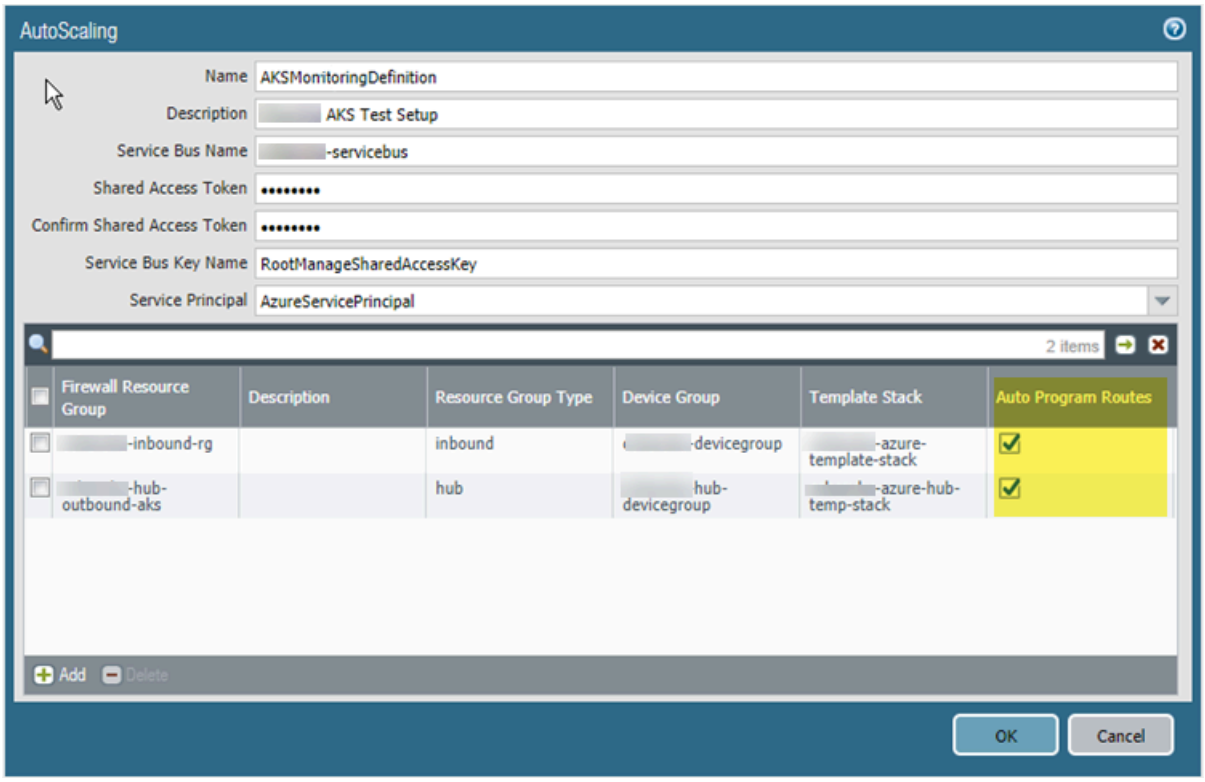
この作業は、Panoramaが統制するデプロイを行っており、テンプレート、テンプレートスタック、デバイスグループを作成していることを前提にしています。

各フォームの記入方法の詳細は、Panorama のオンライン ヘルプを参照してください。

STEP 1 | デプロイの設定時に作成したモニタリング定義を参照するには、**Panorama** > **Azure** > **Deployments**（デプロイ）を選択します。以下のように、**Auto Program Routes**（ルートの

©2023 Palo Alto Networks, Inc.

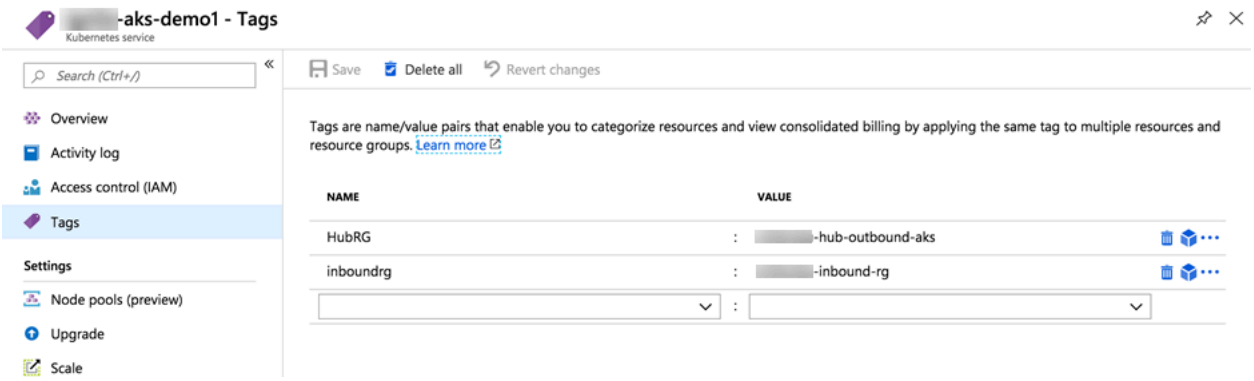
自動プログラミング）を有効にすると、ファイアウォール ルートがプログラミングされます。



©2023 Palo Alto Networks, Inc.

STEP 2 | AKS で、リソース グループにタグを設定します。タグは名前と値のペアです。

1. **Home**（ホーム） > **Resource groups**（リソース グループ）を選択して、リソース グループを選択します。
2. **Tags**（タグ）を選択して、名前と値のペアを定義します。次のように、タグ名は inboundgrouprg および HubRG でなければなりません:
   - inboundgrouprg—スポーク リソース グループ名
   - HubRG—Hub リソース グループ名



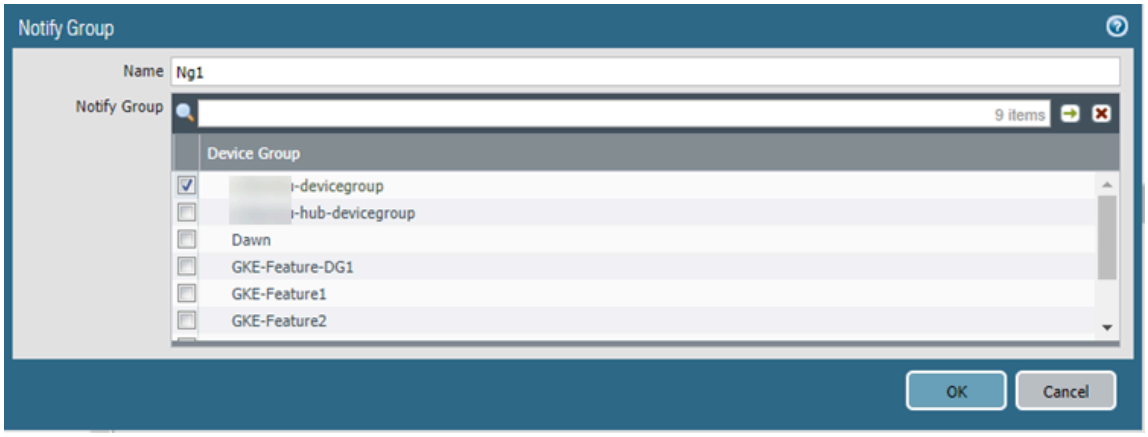
テンプレートは、スポーク リソース グループの名前をパラメータとして取得し、Panorama plugin for Azureが検出できるように、スポーク リソース グループ名で VNet および AKS クラスタにタグを設定します。

テンプレートはリソースを、個別の *VNet* にデプロイします。*AKS* クラスタとサービスを、スポーク ファイアウォール セットと同じ *VNet* 内に手動でデプロイした場合、スポーク リソース グループ名に対して手動でタグを作成する必要があります。

©2023 Palo Alto Networks, Inc.

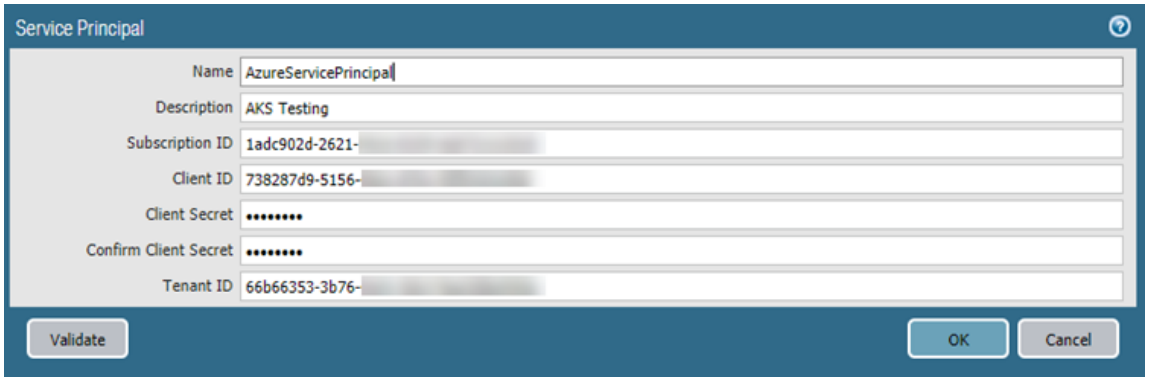
STEP 3 | Panoramaで、**Panorama** > **Azure** > **Setup**（セットアップ）の順に選択します。

1. **General**（全般）タブで、モニタリングを有効にします。
2. **Notify Groups**（通知グループ）タブで、通知するデバイス グループを**Add**（追加）します。



3. **Service Principal**（サービス プリンシパル）タブで、サービス プリンシパルを**Add**（追加）、**Validate**（検証）します。

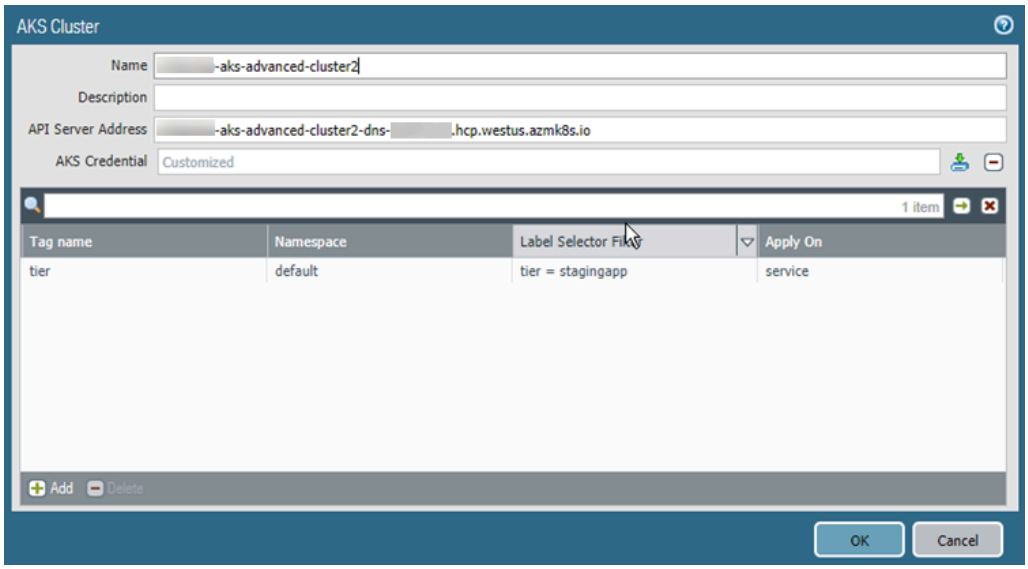
   統制デプロイ環境用に作成したサービスプリンシパルを使用してください。



4. **AKS Cluster**（**AKS** クラスタ）タブで、AKS クラスタを**Add**（追加）します。
   - AKS クラスタの名前を正確に入力してください。
   - API サーバーのアドレスを入力します。Azure でアドレスを検索するには、AKS サービスを表示して、Overview（概要）を選択します。
   - AKS 認証情報の JSON ファイルをアップロードします（「AKS クラスタ認証を作成」を参照）。
5. 残りのフィールドを記入して、1 つまたは複数のタグを **Add**（追加）します。

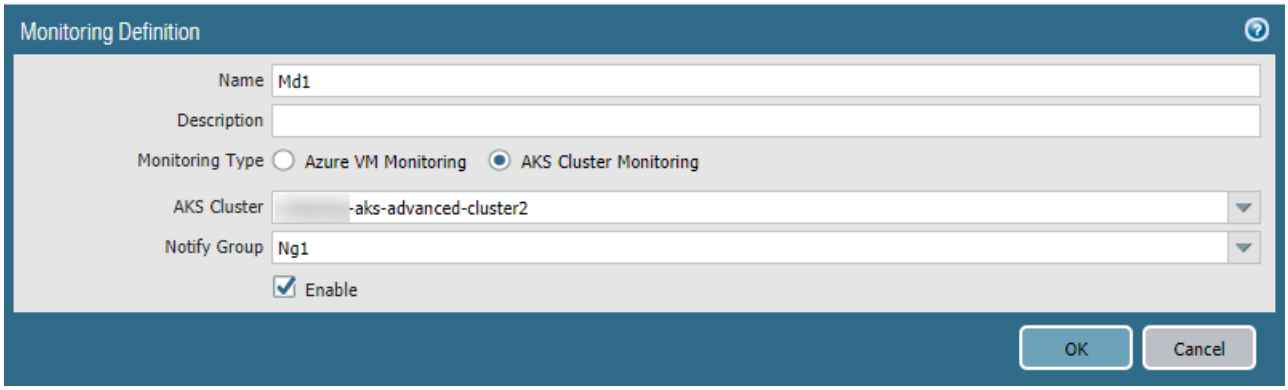
   名前空間で一意ではないサービス名またはタグがある場合は、一意の結果が得られるようにラベル セレクタを使ってタグと名前空間をフィルタリングします。

©2023 Palo Alto Networks, Inc.



STEP 4 | **Panorama** > **Azure** > **Monitoring Definition**（モニタリング定義）を選択します。

1. モニタリング定義を追加します。
2. 名前と説明を入力して、**AKS Cluster Monitoring**（**AKS** クラスタ モニタリング）を選択します。
3. **AKS Cluster**（**AKS** クラスタ）および **Notify Group**（通知グループ）を選択し、**Enable**（有効）を選択して、**OK**をクリックします。



VNet ピアリングのセットアップ

トラフィックの識別にアドレス グループを使用する場合、ピアリングを設定する前に、トップレベルの Panorama ポリシーにサブネット アドレス グループを追加するようにしてください。

AKS クラスタのデプロイ後、Inbound VNet からクラスタへ、およびクラスタからファイアウォール VNet への VNet Peering（VNet のピアリング）を設定します。

ファイアウォール ILB へのトラフィックのリダイレクト

トラフィックを特定の ILB にリダイレクトするには、ユーザー定義のルート（UDR）とルーティング ルールを手動で作成する必要があります。例として、「Azure Secure Kubernetes Services 用

©2023 Palo Alto Networks, Inc.

Panorama プラグインの仕組み」がインバウンド UDR をどのように表しているのかを参照してください。

STEP 1 | Web トラフィックを適切なバックエンド プールにリダイレクトするルーティング ルールを作成します。

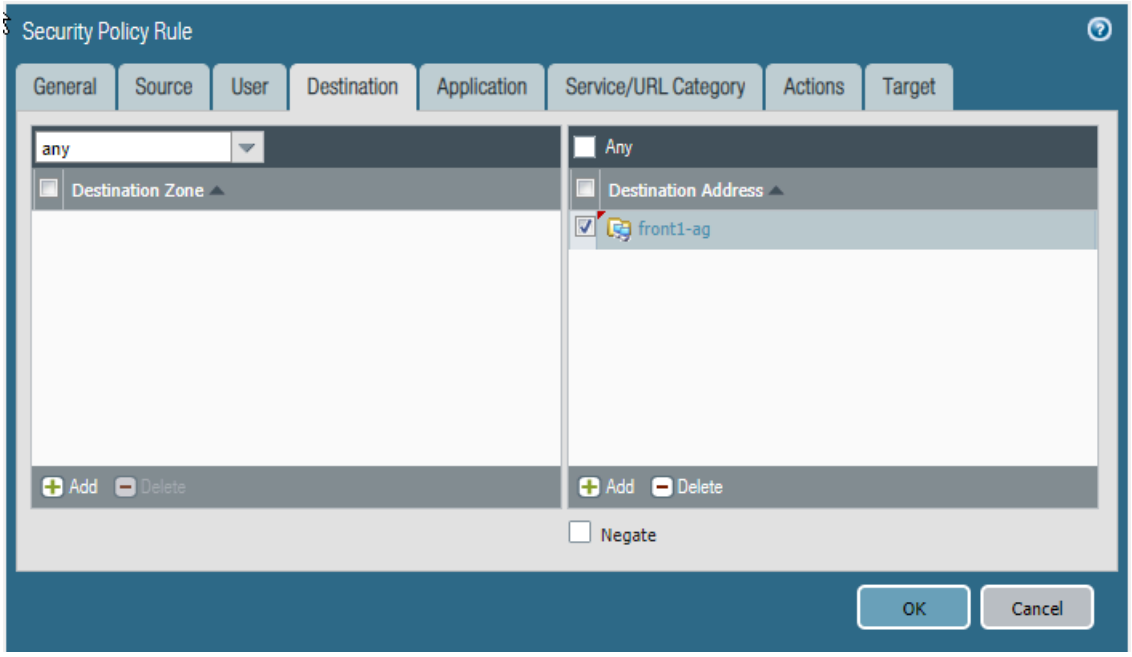
STEP 2 | サービス CIDR のルートを追加して、次のホップをスポーク ファイアウォール リソース グループからのインバウンド ファイアウォール ロード バランサーにするには、アプリケーション ゲートウェイ サブネットの UDR ルールを更新します。

ポリシー関連 AKS サービスの適用

STEP 1 | Panorama で、Policies（ポリシー）を選択します。

STEP 2 | **Device Group**（デバイス グループ）リストで、AKS サービス用のデバイス グループを選択します。

STEP 3 | セキュリティポリシー ルールを**Add**（追加）します。フォームを記入して、**Destination**（宛先）タブで宛先アドレスまたはアドレス グループを**Add**（追加）します。



AKS サービスのデプロイと保護

ここでは、VM-Series ファイアウォールと Panorama 用 Azure プラグインを使って、Kubernetes サービスへのインバウンド トラフィックとアウトバウンド トラフィックを保護する方法の概要を説明していきます。

©2023 Palo Alto Networks, Inc.

STEP 1 | アプリケーション デプロイ 環境で、アプリケーション用の YAML ファイルを作成するか、または既存のファイルを使用してください。サンプルのアプリケーション YAML ファイルを次に示します:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      containers:
      - name: azure-vote-back
        image: redis
        resources:
          requests:
            cpu: 100m
            memory: 128Mi
          limits:
            cpu: 250m
            memory: 256Mi
        ports:
        - containerPort: 6379
          name: redis
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-back
  labels:
    service: backend
spec:
  ports:
  - port: 6379
  selector:
    app: azure-vote-back
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-front
spec:
  replicas: 5
  selector:
    matchLabels:
      app: azure-vote-front
  template:
    metadata:
```

 ©2023 Palo Alto Networks, Inc.

```
      labels:
        app: azure-vote-front
    spec:
      containers:
      - name: azure-vote-front
        image: microsoft/azure-vote-front:v1
        resources:
          requests:
            cpu: 100m
            memory: 128Mi
          limits:
            cpu: 250m
            memory: 256Mi
        ports:
        - containerPort: 80
        env:
        - name: REDIS
          value: "azure-vote-back"
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
  labels:
    service: "azure-vote-front"
    type: "production"
    providesecurity: "yes"
    a: "value"
    b: "value"
    c: "value"
    tier: "stagingapp"
  annotations:
    service.beta.kubernetes.io/azure-load-balancer-internal: "true"
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: azure-vote-front
```

STEP 2 | Kubernetes サービスにラベルを設定するために、YAML ファイルを編集します。

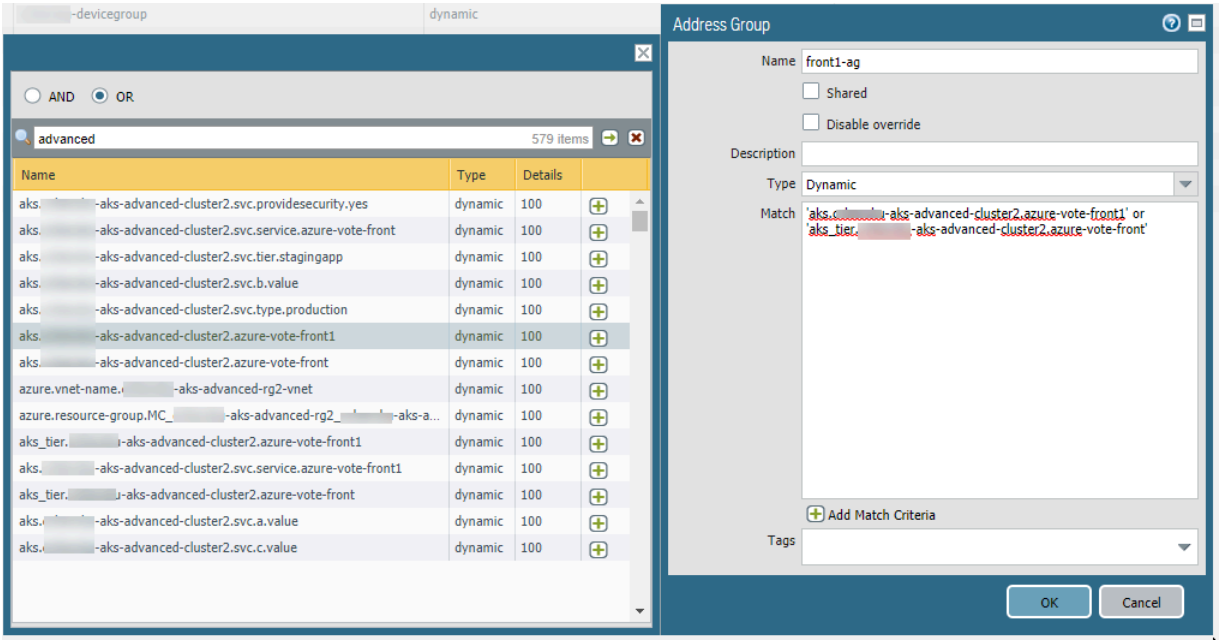
ラベルにより、AKS 用 Panorama プラグインを使ってクラスタに接続する際に、対応するタグと IP のマッピングが作成されます。たとえば、上記のサンプルファイルで、サービス メタデータ内のアプリケーション ラベルに注目してください。これは、**azure-vote-back** および **azure-vote-front** となっています。

STEP 3 | AKS クラスタで、YAML ファイルを適用します。

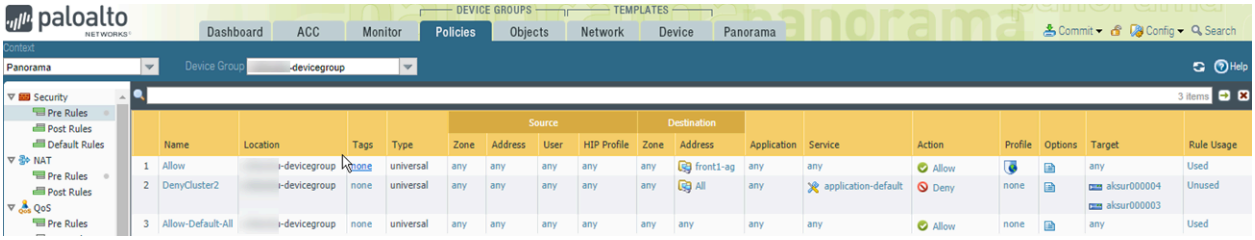
©2023 Palo Alto Networks, Inc.

STEP 4 | Panorama で、リソース グループ タグを使ってアドレス グループを作成します。

1. **Objects**（オブジェクト）タブで、**Device Group**（デバイス グループ）リストからデバイス グループを選択します。
2. **Address Groups**（アドレス グループ）を選択して、アドレス グループを**Add**（追加）します。
   1. 名前を指定して、**Dynamic**（ダイナミック）タイプを選択します。
   2. アドレスを**Add**（追加）します。追加により、検出されたアドレスを記載したウィンドウが表示されます。リストの生成には、数分ほどかかることがあります。
   3. Match Criteria（一致条件）に対して、1 つまたは複数のアドレスを選択できます。条件の相互関係を示す AND または OR を選択します。
   4. 多数のアドレスが表示された場合は、検索ボックスに文字列を入力して、出力のフィルタリングを行います。以下の図を参照してください。
   5. アドレス リストで、+ をクリックして、アドレス グループ一致条件にアドレスを含めます。
   6. 一致条件の指定が完了したら、**OK**をクリックします。



STEP 5 | アドレス グループを使ってポリシーを表示します。



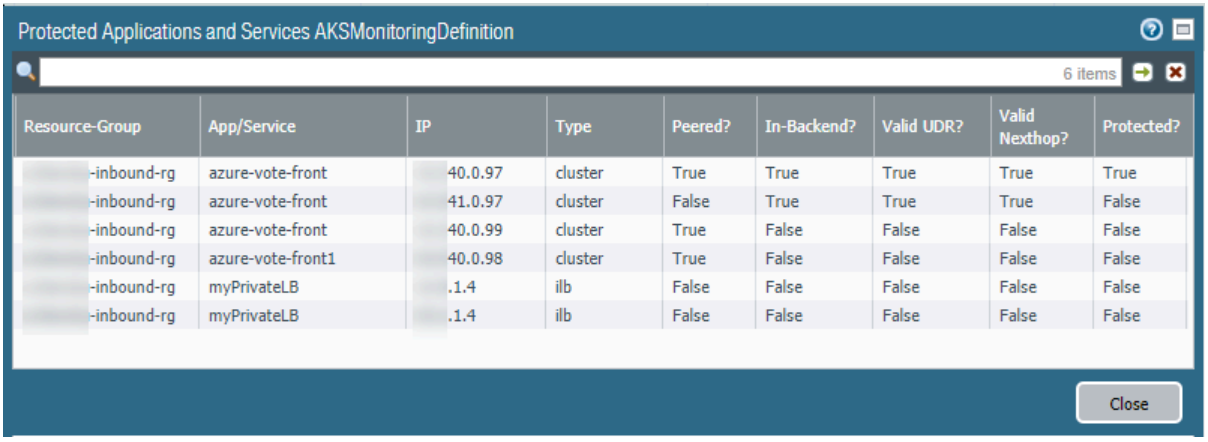
©2023 Palo Alto Networks, Inc.

STEP 6 | 保護された AKS サービスを表示します。

Panorama > **Azure** > **Deployments**（デプロイメント）でモニタリング定義を表示して、Action（アクション）列で**Protected Applications and Services**（保護されたアプリケーションとサービス）リンクを選択します。

Protected?（保護）列には、リソース グループのセキュリティ ステータスの要約が表示されます。このウィンドウの表示が完了するまでに、数分ほどかかることがあります。多数のリソース グループが存在している場合は、検索ボックスに文字列を入力して、出力のフィルタリングを行ってください。

出力は、Azure リソース グループの設定に基づいています。デバイス グループまたはテンプレート スタック メンバーシップにはクエリを行いません。



Resource-Group	App/Service	IP	Type	Peered?	In-Backend?	Valid UDR?	Valid Nexthop?	Protected?
-inbound-rg	azure-vote-front	40.0.97	cluster	True	True	True	True	True
-inbound-rg	azure-vote-front	41.0.97	cluster	False	True	True	True	False
-inbound-rg	azure-vote-front	40.0.99	cluster	True	False	False	False	False
-inbound-rg	azure-vote-front1	40.0.98	cluster	True	False	False	False	False
-inbound-rg	myPrivateLB	.1.4	ilb	False	False	False	False	False
-inbound-rg	myPrivateLB	.1.4	ilb	False	False	False	False	False

©2023 Palo Alto Networks, Inc.

OpenStack での VM-Series ファイアウォールのセットアップ

OpenStack 用 VM-Series ファイアウォールを使用すれば、ネットワーク セキュリティ、パフォーマンス、可視性を実現しながらアプリケーションを安全に配信できます。

- OpenStack 用 VM-Series ファイアウォール
- VM-Series for OpenStack Solution ソリューションのコンポーネント
- 基本的なゲートウェイ デプロイメント用の Heat テンプレート
- サービス チェーニングおよびサービス スケーリングでの Heat テンプレートの使用
- 基本的なゲートウェイ デプロイメントでの VM-Series ファイアウォールのインストール
- サービス チェーニングまたはスケーリング用 Heat テンプレートを使用した VM-Series ファイアウォールのインストール

OpenStack での VM-Series のデプロイ

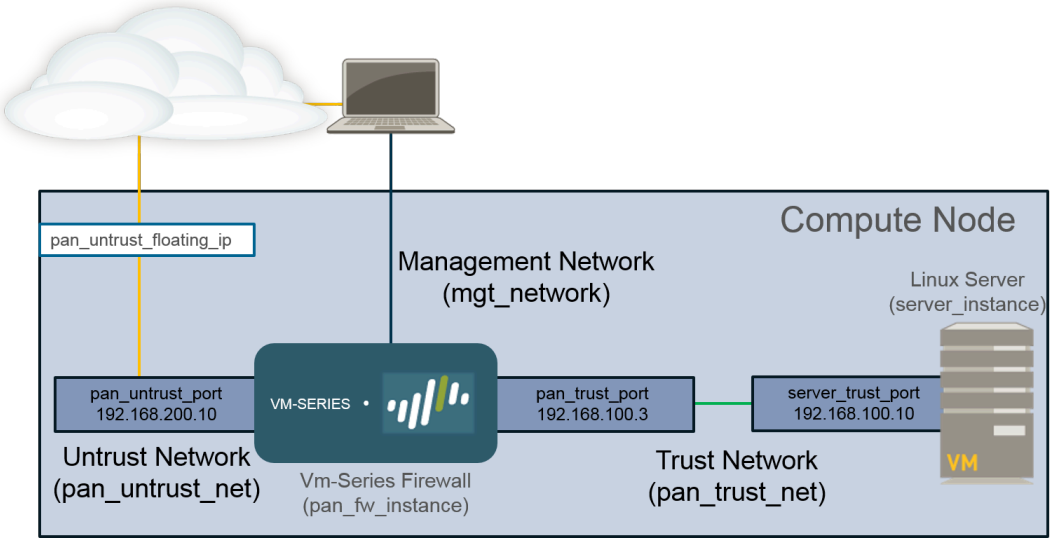
Palo Alto Networks から提供される Heat オーケストレーション テンプレートでは、サービス チェイニングを使用して、またはサービス スケーリングを動的に使用して VM-Series ファイアウォールを個別にデプロイできます。

- 基本的なゲートウェイ
- サービス チェーニングおよびサービス スケーリング

基本的なゲートウェイ

OpenStack の VM-Series ファイアウォールを使用すると、OpenStack 環境の計算ノード上で稼働する KVM ハイパーバイザに VM-Series ファイアウォールをデプロイできます。このソリューションでは、Heat オーケストレーション テンプレートとブートストラッピングを使用して、VM-Series ファイアウォールと Linux サーバーがデプロイされます。VM-Series ファイアウォールは、サーバーを出入りするトラフィックを検査して、デプロイされている Linux サーバーを保護します。サンプルのブートストラップ ファイルを使用すると、VM-Series ファイアウォールは、基本設定で起動して、トラフィックを処理します。

これらの Heat テンプレート ファイルとブートストラップ ファイルを併用することで、VM-Series ファイアウォールと Linux サーバーの 2 台の仮想マシンが、以下に示すようなネットワーク設定で作成されます。



サービス チェーニングおよびサービス スケーリング

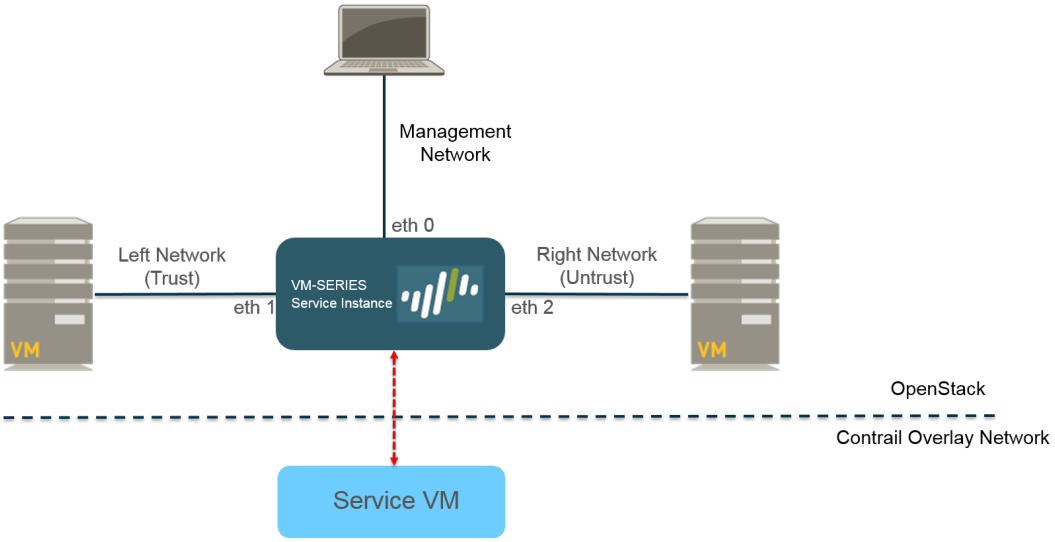
OpenStack Queens では、サービスチェーンやサービススケーリングによる *VM-Series* ファイアウォールのデプロイはサポートされていません。

サービス チェーニングは、OpenStack 環境に VM-Series ファイアウォールをサービス インスタンスとしてデプロイする Contrail の機能です。サービス チェーンは、ファイアウォールや

©2023 Palo Alto Networks, Inc.

ロード バランサーなどの一連のサービス仮想マシンのことを指します。サービス チェーン内の各仮想マシンは、サービス インスタンスと呼ばれます。サービス スケーリングを使用すると、VM-Series ファイアウォールの追加のインスタンスを動的にデプロイできます。OpenStack は、Ceilometer が収集した CPU 使用率や受信バイト/秒のメトリックを使用して、VM-Series ファイアウォールの追加のインスタンスのデプロイやシャットダウンを行い、現在のネットワーク ニーズに応えます。

OpenStack ソリューションの VM-Series ファイアウォールは、Heat オーケストレーション テンプレートを利用して、サービス チェーニングやサービス スケーリングに必要なコンポーネントの設定とデプロイを行います。Palo Alto Networks が提供する Heat テンプレートから、サービス テンプレート、サービス インスタンス、および（VM-Series ファイアウォールにトラフィックを転送するための）サービス ポリシーが作成されます。これにより、2 台の Linux サーバーがデプロイされ、それらの間に VM-Series ファイアウォール サービス インスタンスがデプロイされます。



 ©2023 Palo Alto Networks, Inc.

VM-Series for OpenStack Solution ソリューションのコンポーネント

OpenStack 環境の VM-Series ファイアウォールは、以下のコンポーネントを使用してテストされています。

コンポーネント	概要
software	サポートしているソフトウェアのバージョンについては、「互換性マトリックス」を参照してください。
VM-Series ハードウェア リソース	VM-Series モデルの最小ハードウェア要件については、「VM-Series システム要件」を参照してください。 OpenStack では、計算インスタンスの CPU、メモリ、およびストレージ容量をフレーバーで定義します。Heat テンプレートをセットアップするときは、VM-Series モデルのハードウェア要件を満たすか、それを上回る計算フレーバーを選択します。
Fuel Master	Fuel は、OpenStack 用の Web UI ドリブン デプロイメントおよび管理ツールです。
OpenStack コントローラ	このノードは、API やスケジューリングなどの共有 OpenStack サービスの大部分を実行します。また、Horizon UI は、このノード上で動作します。
OpenStack 計算	OpenStack デプロイメントでは、計算ノードに仮想マシンと VM-Series ファイアウォールが含まれています。VM-Series を収容する計算ノードは、以下の基準を満たす必要があります。 • インスタンス タイプ OS::Nova::Server • 3 つ以上のインターフェイスの設定が可能 • VM-Series qcow2 イメージに対応 • 計算フレーバー パラメータに対応 ***VM-Series*** ファイアウォールでは、ネストされた仮想化がサポートされません。そのため、ベアメタル サーバーに ***OpenStack*** 計算ノードをインストールします。
Contrail コントローラ	Contrail コントローラ ノードは、仮想化ネットワークの管理、制御、および分析に使用される Software Defined Networking コントローラです。計算ノードとゲートウェイ ノードにルーティング情報を送信します。

©2023 Palo Alto Networks, Inc.

コンポーネント	概要
	また、Contrail コントローラは、サービス チェーニングとサービス スケーリングに必要なサポートを提供します。
Contrail ゲートウェイ	Contrail ゲートウェイ ノードは、仮想ネットワークから外部ネットワークへの IP 接続を仲介します。仮想マシンを始点とする MPLS over GRE トンネルは、ゲートウェイ ノードで終端します。このノードで、パケットはカプセル化解除され、IP ネットワークの宛先に送信されます。
Ceilometer（OpenStack テレメトリー）	OpenStack 用の VM-Series ファイアウォールの場合、Ceilometer は、サービス スケーリングの CPU 使用率をモニターします。CPU 使用率が所定のしきい値に達すると、VM-Series ファイアウォールの新しいサービス インスタンスがデプロイまたはシャットダウンされます。
Heat オーケストレーション テンプレート ファイル	Palo Alto Networks では、VM-Series ファイアウォールをデプロイするためのサンプルの Heat テンプレートを提供しています。このテンプレートは、メイン テンプレートと環境テンプレートから構成されます。このファイルから 1 つの管理インターフェイスと 2 つのデータ インターフェイスを備えた 1 つの VM-Series インスタンスがインスタンス化されます。 基本的なゲートウェイ デプロイメントでは、テンプレートから 1 つのインターフェイスを備えた Linux サーバーがインスタンス化されます。サーバーのインターフェイスは、テンプレートで作成されたプライベート ネットワークに接続されます。 サービス チェーニング デプロイメントまたはサービス スケーリング デプロイメントでは、テンプレートから 2 つの Linux サーバーがインスタンス化されます。そのうちの 1 つのサーバーは、ファイアウォールの各データ インターフェイスに接続されます。
VM-Series ファイアウォールのブートストラップ ファイル	VM-Series ファイアウォールのブートストラップ ファイルは、init-cfg.txt ファイル、bootstrap.xml ファイル、および VM-Series 認証コードから構成されます。Palo Alto Networks では、Heat テンプレート ファイルとともに、サンプルの init-cfg.txt ファイルと bootstrap.xml ファイルを提供しています。VM-Series ファイアウォールの使用許諾を得て、サブスクリプションをアクティベートするには、所有する認証コードを入力する必要があります。VM-Series のブートストラップ ファイルの詳細は、「VM-Series ファイアウォールのブートストラップ」を参照してください。

©2023 Palo Alto Networks, Inc.

基本的なゲートウェイ デプロイメント用の Heat テンプレート

Heat テンプレート ファイルには、以下の 4 つのファイルが含まれています。これらのファイルを使用して、OpenStack の KVM 上にある VM-Series ファイアウォールを起動できます。VM-Series ファイアウォールと Linux サーバーをデプロイするには、これら 4 つのファイルがすべて必要です。

- **pan_basic_gw.yaml** – 計算ノード上の VM-Series ファイアウォールと Linux サーバーをサポートするために作成される、インターフェイスや IP アドレスなどのリソースを定義します。
- **pan_basic_gw_env.yaml**–この環境ファイルは、VM-SeriesファイアウォールとLinuxサーバーが存在している環境を定義しています。pan_basic_gw.yamlファイル内の多くのパラメータが、VM-SeriesやLinuxサーバーのフレーバーなどの、このファイルに定義されているパラメータを参照しています。
- **init-cfg.txt** – ファイアウォールの管理インターフェイスで DHCP を有効にするための操作コマンドが含まれます。
- **bootstrap.xml** – VM-Series ファイアウォールの基本設定が記述されています。bootstrap.xml ファイルでは、データ インターフェイスと IP アドレスが設定されます。これらの値は、pan_basic_gw.yaml ファイル内の対応する値に一致している必要があります。

  また、bootstrap.xml ファイルには、untrust2trust という名前の NAT ルールが含まれています。このルールにより、サーバー上の信頼できるポートが VM-Series ファイアウォール上の信頼できないポートに変換されます。

ブートストラップ ファイルを OpenStack に渡すには、ファイルの取り込み（パーソナリティ ファイル）、またはユーザー データの、2 種類のオプションがあります。

OpenStack Queens 以降、ファイルの取り込みはサポートされていません。ユーザー データを使用する必要があります。

以下の表は、pan_basic_gw.yaml テンプレート ファイルによって作成されるリソースを示しています。該当する場合は、デフォルト値が記載されています。

リソース	説明
pan_fw_instance	1 つの管理インターフェイスと 2 つのデータ インターフェイスを備えた VM-Series ファイアウォール。
server_instance	単一のインターフェイスを備えた 1 台の Linux サーバー。
pan_trust_net	ファイアウォール上の信頼できるインターフェイスとサーバー上の信頼できるインターフェイスが接続されている内部ネットワークへの接続。

©2023 Palo Alto Networks, Inc.

リソース	説明
pan_trust_subnet	ファイアウォール上の信頼できるインターフェイスに接続されており（pan_trust_net）、CIDR の値が 192.168.100.0/24 であるサブネット。
pan_untrust_net	ファイアウォール上の信頼できないポートが接続されている信頼できないネットワーク。
pan_untrust_subnet	ファイアウォール上の信頼できないインターフェイスに接続されており（pan_untrust_net）、CIDR の値が 192.168.200.0/24 であるサブネット。
allow_ssh_https_icmp_secgrou	ポート 22 および 443 上の TCP と ICMP トラフィックを許可するセキュリティ グループ。
pan_untrust_port	レイヤー 3 モードでデプロイされた VM-Series ファイアウォール上の信頼できないポート。Heat テンプレートには、このポートに対するデフォルト IP アドレスの 192.168.200.10 が記述されています。 Heat テンプレートでこの IP アドレスを変更する場合は、bootstrap.xml ファイルでもこの IP アドレスを変更する必要があります。
pan_untrust_floating_ip	public_network から割り当てられたフローティング IP アドレス。
pan_untrust_floating_ip_assoc	これにより、pan_untrust_floating_ip が pan_untrust_port に割り当てられます。
pan_trust_port	VM-Series ファイアウォール レイヤー 3 モードの信頼できるポート。
server_trust_port	Linux サーバー レイヤー 3 モードの信頼できるポート。Heat テンプレートには、このポートに対するデフォルト IP アドレスの 192.168.100.10 が記述されています。 Heat テンプレートでこの IP アドレスを変更する場合は、bootstrap.xml ファイルでもこの IP アドレスを変更する必要があります。

pan_basic_gw.yaml ファイルは、pan_basic_gw_env.yaml を参照して、VM-Series ファイアウォールと Linux サーバーのデプロイに必要なリソースを作成するために必要となる多くの値を取得します。Heat テンプレート環境ファイルには、以下のパラメータが含まれています。

©2023 Palo Alto Networks, Inc.

パラメータ	概要
mgmt_network	VM-Series ファイアウォールの管理インターフェイスは、このパラメータで指定されたネットワークに接続されます。このテンプレートでは、管理ネットワークは作成されません。そのため、Heat テンプレートをデプロイする前に、管理ネットワークを作成する必要があります。デフォルト値は mgmt_ext_net です。
public_network	OpenStack クラスターとその中の仮想マシンが外部ネットワークまたはパブリック ネットワークと通信するために使用するアドレス。パブリック ネットワークは、パブリック エンドポイントに仮想 IP アドレスを提供します。このアドレスは、OpenStack サービス API に接続する際に使用されます。このテンプレートでは、パブリック ネットワークは作成されません。そのため、Heat テンプレートをデプロイする前に、パブリック ネットワークを作成する必要があります。デフォルト値は public_net です。
pan_image	このパラメータでは、VM-Series ファイアウォールをデプロイする際に Heat テンプレートで使用される VM-Series 基本イメージを指定します。デフォルト値は pa-vm-7.1.4 です。
pan_flavor	このパラメータでは、VM-Series ファイアウォールに割り当てるハードウェア リソースを定義します。デフォルト値は m1.medium です。この値は、「KVM での VM-Series ファイアウォールのセットアップ」の章に記載されているKVM 上の VM-Series のシステム要件を満たします。
server_image	このパラメータにより、Linux サーバーに対して使用するイメージが Heat テンプレートに指示されます。デフォルト値は Ubuntu-14.04 です。
server_flavor	このパラメータでは、Linux サーバーに割り当てるハードウェア リソースを定義します。デフォルト値は m1.small です。
server_key	サーバー キーは、SSH 経由で Linux サーバーにアクセスする際に使用されます。デフォルト値は server_key です。この値を変更するには、環境ファイルに新しいサーバー キーを入力してください。

©2023 Palo Alto Networks, Inc.

サービス チェーニングおよびサービス スケーリングでの Heat テンプレートの使用

OpenStack Queens では、サービスチェーンやサービススケーリングによる *VM-Series* ファイアウォールのデプロイはサポートされていません。

Heat テンプレート環境ファイルは、サービス チェーニングまたはサービス スケーリングによってデプロイする VM-Series ファイアウォール インスタンス特有のパラメータを定義します。環境ファイルで定義されるパラメータは、以下のセクションに分割されています。サービス チェーニング用の Heat テンプレートには vwire と L3 という 2 つのバージョンがあります。サービス スケーリング用の Heat テンプレートは 1 つだけです。

サービス チェーニングでは、Heat テンプレート ファイルと 2 つのブートストラップ ファイルを使用して、VM-Series ファイアウォール サービス インスタンスと左右のネットワークで合計 2 台の Linux サーバーを起動する必要があります。

- テンプレート ファイル — このテンプレートは、VM-Series ファイアウォールと 2 台の Linux サーバーをサポートするために作成されるリソース（インターフェイスや IP アドレスなど）を定義します。
  - vwire デプロイメント用のファイルは service_chaining_template_vm.yaml です。
  - L3 デプロイメント用のファイルは service_chaining_template_L3.yaml です。
  - サービス スケーリング デプロイメント用のファイルは service_scaling_template.yaml です。
- 環境ファイル—この環境ファイルは、VM-SeriesファイアウォールとLinuxサーバーが存在している環境を定義しています。このテンプレート内の多くのパラメータが、VM-Seriesのフレーバーや Linuxサーバー名などの、このファイルに定義されているパラメータを参照しています。
  - vwire デプロイメント用のファイルは service_chaining_env_vm.yaml です。
  - L3 デプロイメント用のファイルは service_chaining_env_L3.yamlです。
  - サービス スケーリング デプロイメント用のファイルは service_scaling_env.yaml です。
- **service_instance.yaml** — （サービス スケーリングのみ）ネストされた Heat テンプレートであり、サービス インスタンスをデプロイするために Service_Scaling_template.yaml によって参照されます。イベントのスケーリングに使用するサービス インスタンスをデプロイするために必要な情報を提供します。
- **init-cfg.txt** — VM-Series ファイアウォールをブートストラップするのに必要な最小限の情報を提供します。提供されている init-cfg.txt には、ファイアウォール管理インターフェイス上で DHCP を有効にするための操作コマンドのみが含まれています。
- **<file_name>_bootstrap.xml** — VM-Series ファイアウォールの基本設定を提供します。bootstrap.xml ファイルはデータ インターフェイスを設定します。これらの値は、Heat テンプレート ファイルの対応する値と一致します。

©2023 Palo Alto Networks, Inc.

init-cfg.txt および bootstrap.xml ファイルの詳細は、「ブートストラップ設定ファイル」を参照してください。

環境ファイルのパラメータを以下の表に示します。

- 仮想ネットワーク
- 仮想マシン
- サービス テンプレート
- サービス インスタンス
- IPAM
- サービス ポリシー
- アラーム

仮想ネットワーク

Heat テンプレート環境ファイルの仮想ネットワーク設定パラメータにより、Heat テンプレートによってデプロイされる VM-Series ファイアウォールと 2 台の Linux サーバーを接続する仮想ネットワークが定義されます。

仮想ネットワーク（**VN** 設定）	
management_network	VM-Series ファイアウォールの管理インターフェイスは、このパラメータで指定されたネットワークに接続されます。
left_vn または left_network	左側の仮想ネットワークの名前。
right_vn または right_network	右側の仮想ネットワークの名前。
left_vn_fqdn	左側の仮想ネットワークの完全修飾ドメイン名。
right_vn_fqdn	右側の仮想ネットワークの完全修飾ドメイン名。
route_target	ルート ターゲット設定が外部ゲートウェイと同じになるように、この値を編集してください。

仮想マシン

仮想マシンのパラメータでは、左側および右側の Linux サーバーを定義します。ポート タプルの名前はここで定義され、Heat テンプレートによって参照されます。Contrail の場合、ポート タプルとは、同じ仮想マシンに接続されている仮想ネットワーク インターフェイスの順序付きセットのことです。ポート タプルにより、ポートを作成し、サービス インスタンスの作成時にその情報を渡すことができます。Heat テンプレートは、左側のポート、右側のポート、および管理ポートを作成して、ポート タプルに追加します。この後、ポート タプルは、サービス インスタンスにリンクされます。Heat テンプレートを使用してサービス インスタンスを起動する

 ©2023 Palo Alto Networks, Inc.

と、ポート タプルにより、OpenStack にデプロイされている仮想マシンに対してサービス仮想マシンがマッピングされます。

仮想マシン（VM 設定）	
flavor	左側および右側の仮想マシンのフレーバー。デフォルト値は m1.small です。
left_vm_image、right_vm_image または image	左側および右側の仮想マシンのソフトウェア イメージの名前。アップロードしたイメージのファイル名と同じになるように、この値を変更してください。 デフォルト値は TestVM です。これは、OpenStack で提供されるデフォルト イメージです。
svm_name	VM-Series ファイアウォールに適用される名前。
left_vm_name および right_vm_name	左側および右側の仮想マシンの名前。
port_tuple_name	2 台の Linux サーバーと 1 台の VM-Series ファイアウォールで使用されるポート タプルの名前。
server_key	サーバー キーは、SSH 経由で仮想マシンにアクセスする際に使用されます。デフォルト値は server_key です。この値を変更するには、環境ファイルに新しいサーバー キーを入力してください。

サービス テンプレート

サービス テンプレートでは、サービス インスタンス、たとえば、ソフトウェア イメージ、仮想マシン フレーバー、サービス タイプ、インターフェイスなどのパラメータを定義します。サービス テンプレートは、ドメインの範囲内で設定され、指定されたドメイン内のすべてのプロジェクト上で使用できます。

サービス テンプレート（ST 設定）	
S_Tmp_name	サービス テンプレートの名前。
S_Tmp_version	サービス テンプレートのバージョン。デフォルト値は 2 です。ポート タプルをサポートするためにサービス テンプレートのバージョン 2 が必要であるため、このパラメータは変更しないでください。
S_Tmp_service_mode	サービス モードは、VM-Series ファイアウォール サービス インスタンスが使用するネットワーク モードです。L3 ネットワーク テンプレートの場合、デフォルト値は in-network です。バーチャル ワイヤ テンプレートの場合、デフォルト値は transparent です。

 ©2023 Palo Alto Networks, Inc.

サービス テンプレート（ST 設定）	
S_Tmp_service_type	テンプレートによってデプロイされるサービスのタイプ。デフォルト値は firewall です。VM-Series ファイアウォールをデプロイするときは、デフォルト値を変更しないでください。
S_Tmp_image_name	このパラメータでは、VM-Series ファイアウォールをデプロイする際に Heat テンプレートで使用される VM-Series 基本イメージを指定します。OpenStack 環境にアップロードする VM-Series ファイアウォール イメージの名前と同じになるように、このパラメータを編集してください。
S_Tmp_flavor	このパラメータでは、VM-Series ファイアウォールに割り当てるハードウェア リソースを定義します。デフォルト値は m1.large です。
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	このパラメータでは、管理インターフェイス、左側のインターフェイス、および右側のインターフェイスのインターフェイス タイプを定義します。
domain	このサービス テンプレートが関連付けられるドメイン。デフォルト値は default-domain です。

サービス インスタンス

Heat テンプレート環境ファイルのサービス インスタンス部分には、Heat テンプレートとサービス テンプレートによってデプロイされる個々のインスタンスの名前が記述されています。

サービス インスタンス（SI 設定）	
S_Ins_name	サービス インスタンス名。これは、Contrail の VM-Series ファイアウォール インスタンスの名前です。
S_Ins_fq_name	サービス インスタンスの完全修飾名。

IPAM

IP アドレス管理（IPAM）は、サービス インスタンスのインターフェイスの IP アドレス情報を提供します。ご使用の環境に応じて以下のパラメータを変更します。

IPAM（IPAM 設定）	
NetIPam_ip_prefix_mgmt	VM-Series ファイアウォールの管理インターフェイスの IP プレフィックス。デフォルト値は 172.2.0.0 です。

©2023 Palo Alto Networks, Inc.

IPAM（IPAM 設定）	
NetIPam_ip_prefix_len_mgmt	VM-Series ファイアウォールの管理インターフェイスの IP プレフィックス長。デフォルト値は /24 です。
NetIPam_ip_prefix_left	VM-Series ファイアウォールの左側のインターフェイスの IP プレフィックス。デフォルト値は10.10.1.0です。
NetIPam_ip_prefix_len_left	VM-Series ファイアウォールの左側のインターフェイスの IP プレフィックス長。デフォルト値は /24 です。
NetIPam_ip_prefix_right	VM-Series ファイアウォールの右側のインターフェイスの IP プレフィックス。デフォルト値は10.10.2.0です。
NetIPam_ip_prefix_len_right	VM-Series ファイアウォールの右側のインターフェイスの IP プレフィックス長。デフォルト値は /24 です。
NetIPam_addr_from_start_true	このパラメータは、上記のサブネット上の VM に IP アドレスを割り当てる方法を決定します。true の場合は、新しい VM が次に使用可能な IP アドレスを取得します。false の場合は、新しい VM に IP アドレスが無作為に割り当てられます。デフォルト値は true です。

サービス ポリシー

サービス ポリシーでは、左側および右側の仮想マシン間で渡されるトラフィックを VM-Series ファイアウォール サービスに向かわせるトラフィック リダイレクト ルールおよびポリシーを定義します。

サービス ポリシー（ポリシー設定）	
policy_name	VM-Series ファイアウォールを経由するようにトラフィックをリダイレクトする Contrail のサービス ポリシーの名前。L3 テンプレートの場合、デフォルト値は PAN_SVM_policy-L3 です。バーチャル ワイヤ テンプレートの場合、デフォルト値は PAN_SVM_policy-vw です。
policy_fq_name	サービス ポリシーの完全修飾名。
simple_action	VM-Series ファイアウォール サービス インスタンスに向かうトラフィックに対して Contrail が適用するデフォルト アクション。VM-Series ファイアウォールでは独自のセキュリティ ポリシーがトラフィックに適用されるため、デフォルト値は pass です。
protocol	VM-Series ファイアウォールに渡すことが Contrail によって許可されるプロトコル。デフォルト値は any です。

©2023 Palo Alto Networks, Inc.

サービス ポリシー（ポリシー設定）	
src_port_end and src_port_start	このパラメータは、ポリシー ルールに関連付ける必要のある送信元ポートを指定する場合に使用します。ポートは、1 つだけ入力することも、コンマで区切って複数入力することも、<port>-<port> 形式を使用して範囲で入力することもできます。 提供されている Heat テンプレートの場合、デフォルト値は任意の送信元ポートを意味する -1 です。
direction	このパラメータでは、VM-Series ファイアウォールに渡すことが Contrail によって許可されるトラフィックの方向を定義します。デフォルト値は<>、つまり双方向トラフィックです。
dst_port_end and dst_port_start	このパラメータは、ポリシー ルールに関連付ける必要のある宛先ポートを指定する場合に使用します。ポートは、1 つだけ入力することも、コンマで区切って複数入力することも、<port>-<port> 形式を使用して範囲で入力することもできます。 提供されている Heat テンプレートの場合、デフォルト値は任意の宛先ポートを意味する -1 です。

アラーム

アラーム パラメータは、サービス スケーリングで使用され、サービス チェーニング環境ファイルには含まれていません。このパラメータで定義したしきい値は、スケーリングの実行タイミングを決定するために Contrail で使用されます。この一連のパラメータは、サービス スケーリング Heat テンプレートでのみ使用されます。

cooldown パラメータで設定されているデフォルト時間は、ファイアウォールに十分な起動時間を与えることを目的としています。cooldown 値を変更する場合は、それぞれの新しいファイアウォール インスタンスが起動できるだけの時間を残してください。

アラーム	
meter_name	追加の VM-Series ファイアウォールをデプロイしたり、停止したりするタイミングを決定するために Ceilometer によってモニターされ、Contrail によって使用されるメトリック。Heat テンプレートでは、サービス スケーリングのメトリックとして、CPU 使用率またはバイト/秒が使用されます。
cooldown_initial	最初のサービス インスタンスが起動されてから追加のサービス インスタンスが起動されるまでに Contrail が待機する時間。デフォルト値は 1200 秒です。

©2023 Palo Alto Networks, Inc.

アラーム	
cooldown_scaleup	最初のスケール アップ サービス インスタンスが起動された後に Contrail が待機する追加のサービス インスタンスの起動間隔。デフォルト値は 1200 秒です。
cooldown_scaledown	最初のスケール アップ サービス インスタンスがシャットダウンされた後に Contrail が待機する追加のサービス インスタンスのシャットダウン間隔。デフォルト値は 1200 秒です。
period_high	この期間に渡って平均 CPU 負荷が高いことが確認されると、アラームがトリガーされます。デフォルト値は300秒です。
period_low	この期間に渡って平均 CPU 負荷が低いことが確認されると、アラームがトリガーされます。デフォルト値は300秒です。
threshold_high	スケールアップ イベントを起動する前に Contrail が参照する CPU 使用率の値（パーセンテージまたはバイト/秒）。デフォルト値は、CPU 使用率 40%、または 2800 バイト/秒です。
threshold_low	スケールダウン イベントを起動する前に Contrail が参照する CPU 使用率の値（パーセンテージまたはバイト/秒）。デフォルト値は、CPU 使用率 20%、または 12000 バイト/秒です。

©2023 Palo Alto Networks, Inc.

基本的なゲートウェイ デプロイメントでの VM-Series ファイアウォールのインストール

以下のステップを実行して、VM-Series ファイアウォールを OpenStack にデプロイするために必要な Heat テンプレート、ブートストラップ ファイル、およびソフトウェア イメージを準備します。ファイルの準備ができたら、VM-Series ファイアウォールと Linux サーバーをデプロイします。

STEP 1 | Heat テンプレートとブートストラップ ファイルをダウンロードします。

Heat テンプレートとブートストラップ ファイルを GitHub リポジトリからダウンロードします。

STEP 2 | VM-Series ベース イメージをダウンロードします。

1. Palo Alto Networks カスタマー サポート ポータルにログインします。
2. **Software Updates**（ソフトウェアの更新）を選択し、**Filter By**（絞り込み）ドロップダウンから **PAN-OS for VM-Series KVM Base Images** を選択します。
3. VM-Series の KVM **qcow2** ファイルをダウンロードします。

STEP 3 | Ubuntu 14.04 をダウンロードして OpenStack コントローラにイメージをアップロードします。

Heat テンプレートでは、Linux サーバーを起動するための Ubuntu イメージが必要です。

1. Ubuntu 14.04 をダウンロードします。
2. Horizon UI にログインします。
3. **Project**（プロジェクト） > **Compute**（計算） > **Images**（イメージ） > **Create Image**（イメージを作成）を選択します。
4. Ubuntu 14.04 のイメージ名を pan_basic_gw_env.yaml ファイルのパラメータに合わせて変更します。
5. イメージ ソースを **Image File**（イメージ ファイル）に変更します。
6. **Choose File**（ファイルを選択） をクリックして、Ubuntu イメージ ファイルの場所まで移動します。
7. フォームを Ubuntu イメージのファイル フォーマットに併せて変更します。
8. **Create Image**（イメージを作成）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Series for KVM のベース イメージを OpenStack コントローラにアップロードします。

1. Horizon UI にログインします。
2. **Project**（プロジェクト） > **Compute**（計算） > **Images**（イメージ） > **Create Image**（イメージを作成）を選択します。
3. ご利用の Heat テンプレートに画像名と一致するように画像に**Name**（名前）を付けます。
4. イメージ ソースを **Image File**（イメージ ファイル）に変更します。
5. **Choose File**（ファイルを選択）をクリックして、VM-Series イメージ ファイルの場所まで移動します。
6. フォーマットを **QCOW2-QEMU Emulator**（**QCOW2-QEMU** エミュレータ）に設定します。
7. **Create Image**（イメージを作成）をクリックします。

STEP 5 | ブートストラップ ファイルをアップロードします。ブートストラップ ファイルを OpenStack に渡すには、ファイルの取り込み（パーソナリティ ファイル）、またはユーザー データの、2 種類のオプションがあります。ユーザー データを使ってブートストラップ ファイルを渡す場合、ファイルを tar ボール（.tgz ファイル）に入れて、その tar ボールを base64 でエンコードします。

OpenStack Queens 以降、ファイルの取り込みはサポートされていません。ユーザー データを使用する必要があります。

- ファイルの取り込みを行う場合、init-cfg.txt、bootstrap.xml、および VM-Series 認証コードは、OpenStack コントローラまたは OpenStack コントローラがアクセスできる Web サーバーにアップロードします。
- **--user-data** メソッドを使用してブートストラップ パッケージを config-drive に渡す場合は、次のコマンドで tar ボールを作成して、tar ボール（.tgz ファイル）を base64 でエンコードします:

```
tar -cvzf <file-name>.tgz config/
ライセンスソフトウェアコンテンツ
base64 -i <in-file> -o <outfile>
```

STEP 6 | ブートストラップ ファイルと認証コードを指定するように pan_basic_gw.yaml テンプレートを編集します。

- パーソナリティ ファイルを使用している場合、personality 下のファイルの保存場所へのパスまたは Web サーバー アドレスを指定します。使用していない行のコメントを解除します。

```
  pan_fw_instance:
    type: OS::Nova::Server
    properties:
      image: { get_param: pan_image }
      flavor: { get_param: pan_flavor }
      networks:
```

 ©2023 Palo Alto Networks, Inc.

```
        - network: { get_param: mgmt_network }
        - port: { get_resource: pan_untrust_port }
        - port: { get_resource: pan_trust_port }
      user_data_format: RAW
      config_drive: true
      personality:
        /config/init-cfg.txt: {get_file: "/opt/pan_bs/init-
cfg.txt"}
#        /config/init-cfg.txt: { get_file: "http://
web_server_name_ip/pan_bs/init-cfg.txt" }
        /config/bootstrap.xml: {get_file: "/opt/pan_bs/
bootstrap.xml"}
#        /config/bootstrap.xml: { get_file: "http://
web_server_name_ip/pan_bs/bootstrap.xml" }
        /license/authcodes: {get_file: "/opt/pan_bs/authcodes"}
#        /license/authcodes: {get_file: "http://
web_server_name_ip/pan_bs/authcodes"}
```

- ユーザー データを使用している場合、user_data 下のファイルの保存場所へのパスまたは Web サーバー アドレスを指定します。複数持っている場合

```
pan_fw_instance:
    type: OS::Nova::Server
    properties:
      image: { get_param: pan_image }
      flavor: { get_param: pan_flavor }
      networks:
        - port: { get_resource: mgmt_port }
        - port: { get_resource: pan_untrust_port }
        - port: { get_resource: pan_trust_port }
      user_data_format: RAW
      config_drive: true
      user_data:
#        get_file: http://10.0.2.100/pub/repository/panos/images/
openstack/userdata/boot.tgz
        get_file: /home/stack/newhot/bootfiles.tgz
```

STEP 7 | pan_basic_gw_env.yaml テンプレート環境ファイルを環境に合わせて編集します。管理およびパブリック ネットワーク値が OpenStack 環境で作成した値と一致することを確認します。pan_image に、VM-Series ベース イメージ ファイルに割り当てた名前を設定します。ここでサーバー キーを変更することもできます。

```
root@node-2:~# cat basic_gateway/pan_basic_gw_env.yaml
parameters:
  mgmt_network: mgmt_ext_net
  public_network: public_net
  pan_image: pa-vm-image
  pan_flavor: m1.medium
  server_image: Ubuntu-14.04
  server_flavor: m1.small
  server_key: server_key
```

 ©2023 Palo Alto Networks, Inc.

STEP 8 | Heat テンプレートをデプロイします。

1. **source openrc** コマンドを実行します。
2. **heat stack-create <*stack-name*> -f <*template*> -e ./<*env-template*>**コマンドを実行します

```
root@node-2:~# heat stack-create stack1 -f pan_basic_gw.yaml -e pan_basic_gw_env.yaml
+--------------------------------------+------------+--------------------+----------------------+--------------+
| id                                   | stack_name | stack_status       | creation_time        | updated_time |
+--------------------------------------+------------+--------------------+----------------------+--------------+
| ebe40f9d-2781-4bb2-b246-f15c761f9045 |   stack1   | CREATE_IN_PROGRESS | 2017-01-25T13:36:59 | None         |
+--------------------------------------+------------+--------------------+----------------------+--------------+
```

STEP 9 | VM-Series ファイアウォールが適切にデプロイされたことを確認します。

スタックの作成ステータスは以下のコマンドで確認できます。

- **heat stack-list** でスタックのステータスを確認します。
- **heat event-list** でスタックの作成中に発生したイベントのリストを表示します。
- **heat stack-show** でスタックの詳細を表示します。

STEP 10 | VM-Series ファイアウォールが Linux サーバーにアクセスするトラフィックを両方向で検査することを確認します。

1. ファイアウォールにログインします。
2. **Monitor**（モニター） > **Logs**（ログ） > **Traffic**（トラフィック）を選択して、SSH セッションを表示します。

©2023 Palo Alto Networks, Inc.

サービス チェーニングまたはスケーリング用 Heat テンプレートを使用した VM-Series ファイアウォールのインストール

以下のステップを実行して、VM-Series ファイアウォールをデプロイするために必要な Heat テンプレート、ブートストラップ ファイル、およびソフトウェア イメージを準備します。ファイルの準備ができたら、VM-Series ファイアウォール サービスと 2 台の Linux サーバーをデプロイします。

OpenStack Queens では、サービスチェーンやサービススケーリングによる *VM-Series* ファイアウォールのデプロイはサポートされていません。

STEP 1 | Heat テンプレートとブートストラップ ファイルをダウンロードします。

Heat テンプレートとブートストラップ ファイルを GitHub リポジトリからダウンロードします。

STEP 2 | VM-Series ベース イメージをダウンロードします。

1. Palo Alto Networks カスタマー サポート ポータルにログインします。
2. **Software Updates**（ソフトウェアの更新）を選択し、**Filter By**（絞り込み）ドロップダウンから **PAN-OS for VM-Series KVM Base Images** を選択します。
3. VM-Series の KVM **qcow2** ファイルをダウンロードします。

STEP 3 | Ubuntu 14.04 をダウンロードして OpenStack コントローラにイメージをアップロードします。

サービス チェーニングを使用する場合は、OpenStack で提供されているデフォルトのイメージ（TestVM）を使用できます。TestVM を使用する場合はこのステップはスキップしてください。サービス スケーリングを使用する場合は Ubuntu イメージが必要です。

1. Ubuntu 14.04 をダウンロードします。
2. Horizon UI にログインします。
3. **Project**（プロジェクト） > **Compute**（計算） > **Images**（イメージ） > **Create Image**（イメージを作成）を選択します。
4. Ubuntu 14.04 のイメージ名を pan_basic_gw_env.yaml ファイルのパラメータに合わせて変更します。
5. イメージ ソースを **Image File**（イメージ ファイル）に変更します。
6. **Choose File**（ファイルを選択） をクリックして、Ubuntu イメージ ファイルの場所まで移動します。
7. フォームを Ubuntu イメージのファイル フォーマットに併せて変更します。
8. **Create Image**（イメージを作成）をクリックします。

Ubuntu イメージを使用する場合にはサーバー キーが必要です。サーバー キーが環境ファイルに追加されていることを確認します。

©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Series for KVM のベース イメージを OpenStack コントローラにアップロードします。

1. Horizon UI にログインします。
2. **Project**（プロジェクト） > **Compute**（計算） > **Images**（イメージ） > **Create Image**（イメージを作成）を選択します。
3. ご利用の Heat テンプレートに画像名と一致するように画像に**Name**（名前）を付けます。
4. イメージ ソースを **Image File**（イメージ ファイル）に変更します。
5. **Choose File**（ファイルを選択）をクリックして、VM-Series イメージ ファイルの場所まで移動します。
6. フォーマットを **QCOW2-QEMU Emulator**（**QCOW2-QEMU** エミュレータ）に設定します。
7. **Create Image**（イメージを作成）をクリックします。

STEP 5 | ブートストラップ ファイルをアップロードします。ファイルは、ここで説明するフォルダ構造にアップロードしなければなりません。Heat テンプレートは、このフォルダ構造を使用してブートストラップ ファイルを探します。

1. OpenStack コントローラにログインします。
2. 以下のフォルダ構造を作成します。

   /root/bootstrap/config/

   /root/bootstrap/license/
3. SCP または FTP を使用して init-cfg.txt および bootstrap.xml ファイルを config フォルダに追加し、VM-Series 認証コードを license フォルダに追加します。

STEP 6 | テンプレート環境ファイルを環境に合わせて編集します。環境ファイルのイメージ名が、ファイルをアップロードした際に付けたファイル名と一致することを確認します。

```
parameters:
# VN config
  management_network: 'mgmt_net'
  left_vn: 'left_net'
  right_vn: 'right_net'
  left_vn_fqdn: 'default-domain:admin:left_net'
  right_vn_fqdn: 'default-domain:admin:right_net'
  route_target: "target:64512:20000"
# VM config
  flavor: 'm1.small'
  left_vm_image: 'TestVM'
  right_vm_image: 'TestVM'
  svm_name: 'PAN_SVM_L3'
  left_vm_name: 'Left_VM_L3'
  right_vm_name: 'Right_VM_L3'
  port_tuple_name: 'port_tuple_L3'
#ST Config
  S_Tmp_name: PAN_SVM_template_L3
  S_Tmp_version: 2
  S_Tmp_service_mode: 'in-network'
  S_Tmp_service_type: 'firewall'
```

 ©2023 Palo Alto Networks, Inc.

```
  S_Tmp_image_name: 'PA-VM-8.0.0'
  S_Tmp_flavor: 'm1.large'
  S_Tmp_interface_type_mgmt: 'management'
  S_Tmp_interface_type_left: 'left'
  S_Tmp_interface_type_right: 'right'
  domain: 'default-domain'
# SI Config
  S_Ins_name: PAN_SVM_Instance_L3
  S_Ins_fq_name: 'default-domain:admin:PAN_SVM_Instance_L3'
#IPAM Config
  NetIPam_ip_prefix_mgmt: '172.2.0.0'
  NetIPam_ip_prefix_len_mgmt: 24
  NetIPam_ip_prefix_left: '10.10.1.0'
  NetIPam_ip_prefix_len_left: 24
  NetIPam_ip_prefix_right: '10.10.2.0'
  NetIPam_ip_prefix_len_right: 24
  NetIPam_addr_from_start_true: true
#Policy Config
  policy_name: 'PAN_SVM_policy-L3'
  policy_fq_name: 'default-domain:admin:PAN_SVM_policy-L3'
  simple_action: 'pass'
  protocol: 'any'
  src_port_end: -1
  src_port_start: -1
  direction: '< >'
  dst_port_end: -1
  dst_port_start: -1
```

STEP 7 | ブートストラップ ファイルと認証コードを指定するようにテンプレート ファイルを編集します。パーソナリティで、ファイルの保存場所へのパスを指定します。使用していない行のコメントを解除します。

```
Pan_Svm_instance:
    type: OS::Nova::Server
    depends_on: [ mgmt_InstanceIp, left_InstanceIp,
 right_InstanceIp ]
    properties:
      name: {get_param: svm_name }
      image: { get_param:  S_Tmp_image_name }
      flavor: { get_param: S_Tmp_flavor }
      networks:
        - port: { get_resource: mgmt_VirtualMachineInterface }
        - port: { get_resource: left_VirtualMachineInterface }
        - port: { get_resource: right_VirtualMachineInterface }
      user_data_format: RAW
      config_drive: true
      personality:
        /config/init-cfg.txt: {get_file: "/root/bootstrap/config/
init-cfg.txt"}
#        /config/init-cfg.txt: { get_file: "http://10.4.1.21/
op_test/config/init-cfg.txt" }
        /config/bootstrap.xml: {get_file: "/root/bootstrap/config/
Service_Chaining_bootstrap_L3.xml"}
#        /config/bootstrap.xml: { get_file: "http://10.4.1.21/
op_test/config/Service_Chaining_bootstrap_L3.xml" }
```

 ©2023 Palo Alto Networks, Inc.

```
#        /license/authcodes: {get_file: "/root/bootstrap/license/
authcodes"}
#        /license/authcodes: {get_file: "http://10.4.1.21/op_test/
license/authcodes"}
```

STEP 8 | Heat テンプレート ファイルをアップロードします。

1. OpenStack コントローラにログインします。
2. SCP または FTP を使用して、Heat テンプレート ファイルと環境ファイルを追加します。

STEP 9 | Heat テンプレートをデプロイします。

1. **source openrc** コマンドを実行します。
2. **heat stack-create *<stack-name>* -f *<template>* -e ./*<env-template>***コマンドを実行します

STEP 10 | VM-Series ファイアウォールが適切にデプロイされたことを確認します。

スタックの作成ステータスは以下のコマンドで確認できます。

- **heat stack-list** でスタックのステータスを確認します。
- **heat event-list** でスタックの作成中に発生したイベントのリストを表示します。
- **heat stack-show** でスタックの詳細を表示します。

STEP 11 | VM-Series ファイアウォールが Linux サーバー間のトラフィックを両方向で検査することを確認します。

1. ファイアウォールにログインします。
2. **Monitor**（モニター） > **Logs**（ログ） > **Traffic**（トラフィック）を選択して、SSH セッションを表示します。

©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

paloalto TECHDOCS

Google Cloud Platform 上の VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールは Google Cloud Platform 上の Google Compute Engine インスタンスにデプロイできます。

> Google Cloud Platform でサポートされているデプロイメント
> Google Public Cloud 上で VM-Series のファイアウォールを設定する準備をする
> Google Cloud PlatformへのVM-Seriesファイアウォールのデプロイ
> Panorama Plugin for GCPによるVMモニタリング
> Google Cloud Platform 上の VM-Series ファイアウォールのオートスケーリング

>Google Cloud Platform 上の VM-Series ファイアウォールについて

>VM-Series のファイアウォールは、次世代型ファイアウォール機能を Google® Cloud Platform（GCP™）に提供します。

>パフォーマンスを最大限に発揮するために、GCP 上の VM-Series ファイアウォールは高速パケット処理を提供し、VM-Series ファイアウォール ライセンスと Google Cloud Platform 仮想マシン（VM）サイズの特定の組み合わせに基づいてネットワーク パフォーマンスを向上させるデータプレーン開発キット（DPDK）ライブラリをサポートしています。

- >Google Cloud Platform と VM-Series のファイアウォール
- >VM-Series ファイアウォールの最小システム要件

>Google Cloud Platform と VM-Series のファイアウォール

>VM-Series のファイアウォールと Google Cloud Platform（GCP）を統合することにより、VM-Series ファイアウォールを Google Compute Engine インスタンス上で動作する仮想マシン（VM）としてデプロイできますGoogle Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする>の際、このプロセスが簡略化されます。

>VM-Series ファイアウォールのデプロイ後は次のオプションのサービスを設定できます：

- >VM-Series ファイアウォールでの Google Stackdriver Monitoring の有効化– ファイアウォールから、PAN-OS メトリックを Google Stackdriver サービスにプッシュします。
- >VM をモニタリングして Google Cloud Platform 上の VM の変更を追跡する– インスタンスを含む特定の GCP ゾーンを監視する VM 情報ソースを設定します。監視対象の VM メタデータには、事前定義済み GCP のプロパティ（プロジェクト ID など）、ラベルやネットワーク タグなどのユーザー定義プロパティが含まれます。

>VM-Series ファイアウォールの最小システム要件

>パブリック クラウド用 VM-Series ファイアウォールのライセンスを選択し、ライセンス方式として bring-your-own-license（BYOL）あるいは pay-as-you-go（PAYG）のいずれかを選択する必要があります。Google Compute Engine インスタンスに VM-Series ファイアウォールをデプロイするには、お使いのライセンスの>VM-Series システム要件 をサポートするマシンタイプを選択する必要があります。

>各ライセンスの事前定義され>標準マシンタイプの最小限の推奨事項については、以下の表を参照してください。リソース要件が VM-Series ファイアウォール ライセンスと互換性がある場合は、パフォーマンスの高いマシン タイプを選択するか、独自の>カスタム マシン タイプを作成することができます。

>単一の Google Compute Engine インスタンスで最大 8 つ>ネットワーク インターフェイスをサポートします。インターフェイスを 8 つ設定する場合は、n1-standard-8 またはそれ以上のマシン タイプを選択します。

>

©2023 Palo Alto Networks, Inc.

>容量	>BYOL	>バンドル 1 および 2		
		>PAYG	>マーケットプレース	>推奨される事前定義のマシン タイプ
>VM-100 ファイアウォール	✓ >	>	>	>n1-standard-4
>VM-200 ファイアウォール	✓ >	>	>	
>VM-300 ファイアウォール	✓ >	✓ >	✓ >	
>VM-1000-HV ファイアウォール	✓ >	>	>	
>VM-500 ファイアウォール	✓ >	>	>	>n1-standard-8
>VM-700 ファイアウォール	✓ >	>	>	>n1-standard-16

©2023 Palo Alto Networks, Inc.

Google Cloud Platform でサポートされているデプロイメント

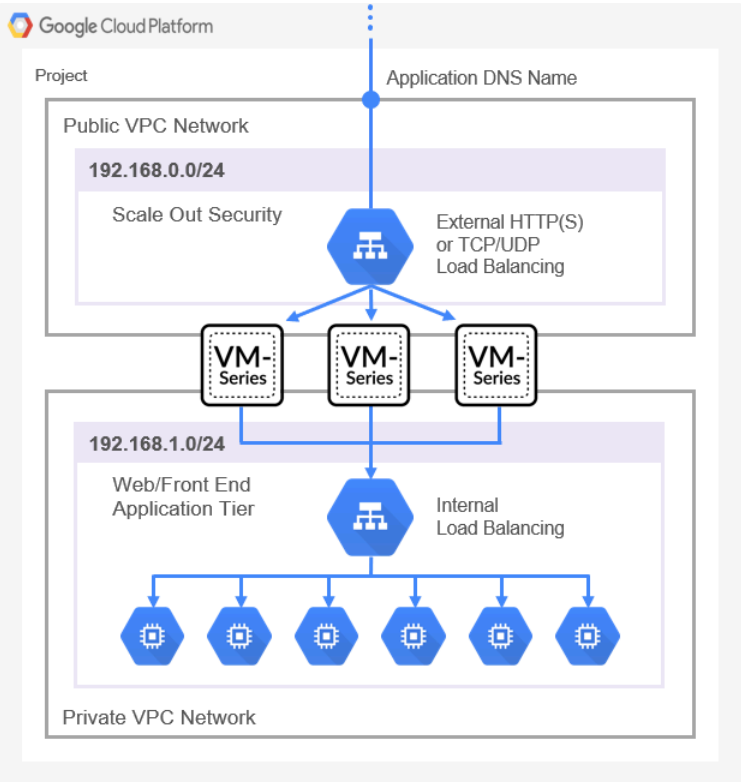
仮想プライベート クラウド（VPC）上のネットワーク内の Google® Compute Engine インスタンスに VM-Series ファイアウォールをデプロイ可能です。以下のデプロイメントのタイプがあります：

- インターネット ゲートウェイ
- セグメンテーション ゲートウェイ
- ハイブリッド IPSec VPN

インターネット ゲートウェイ

VM-Series ファイアウォールは、既知の未知の脅威からアプリケーションを保護するために、インターネット間の North/South トラフィックを保護します。Google プロジェクトは最大 5 つの VPC ネットワークを持つことができます。インターネット ゲートウェイの典型的な例については、Google の構成の例を参照してください。

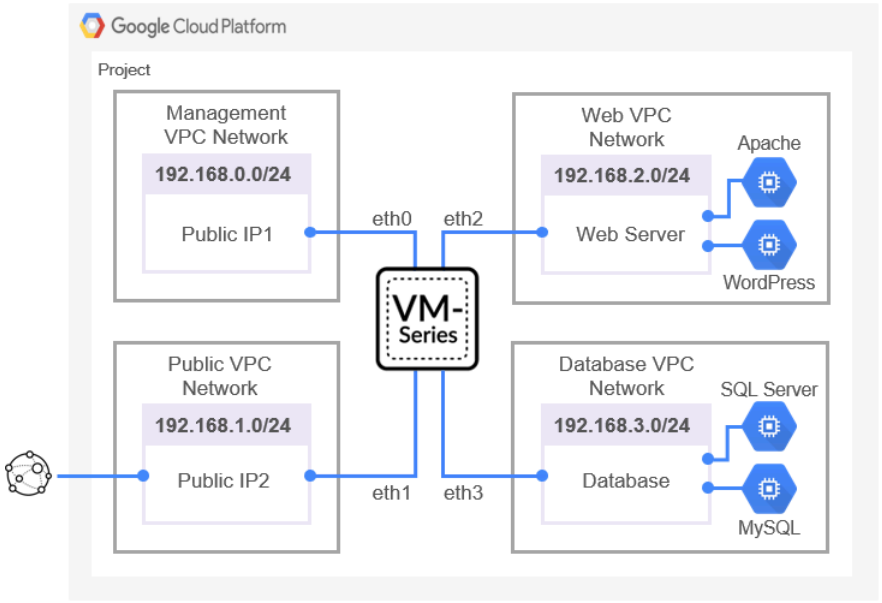
パブリック クラウド環境では、より大規模で高性能な VM ではなく、スケールアウト アーキテクチャ（以下の図を参照）を使用するのが一般的です。このアーキテクチャ（サンドイッチデプロイメントとも呼ばれる）では、単一障害点が回避され、必要に応じてファイアウォールを追加または削除できます。



©2023 Palo Alto Networks, Inc.

セグメンテーション ゲートウェイ

セグメンテーション ゲートウェイは、データ保護のコンプライアンスとアプリケーションへのアクセスを確保するために、仮想プライベート クラウド（VPC）間の East/West トラフィックを保護します。次の図は、North/South および East/West の両方のトラフィックを保護するファイアウォールを示しています。

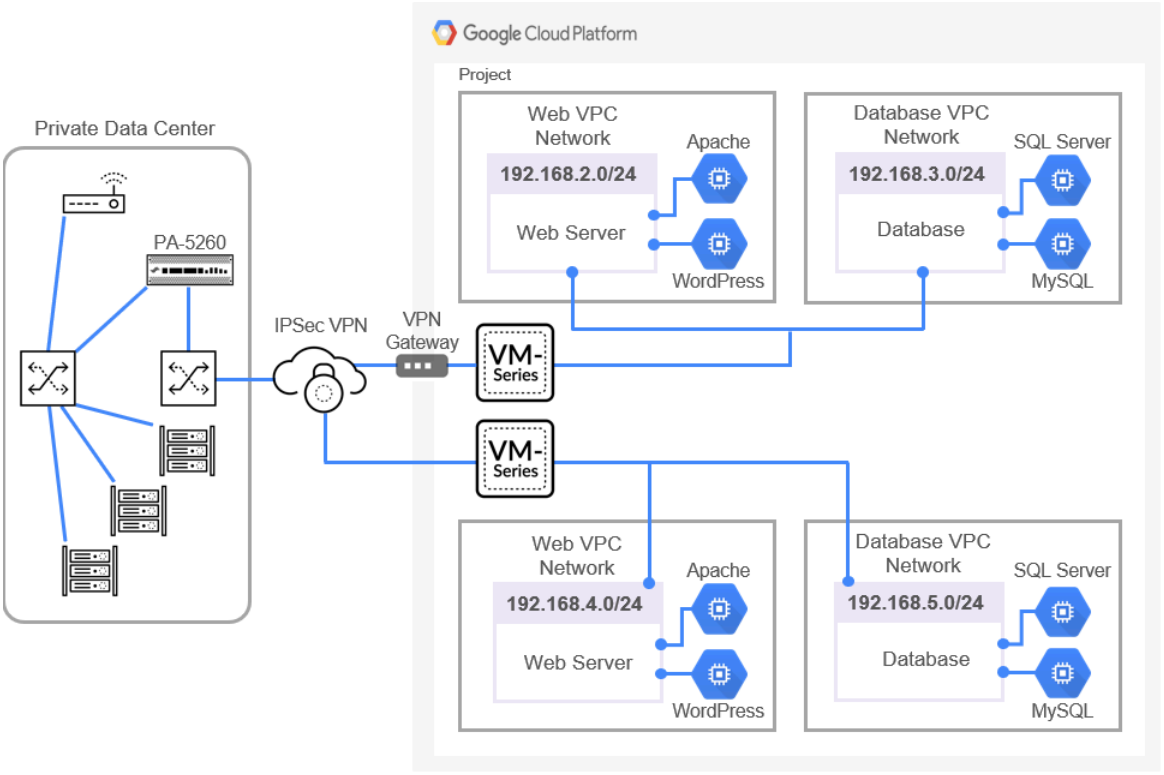


ハイブリッド IPSec VPN

VM-Series のファイアウォールは IPSec VPN 終端ポイントとして機能し、Google Cloud Platform（GCP）にホストされているアプリケーションとの間で安全な通信を可能にします。

次の図のデプロイメントでは、オンプレミス ネットワークから GCP にデプロイされた VM-Series ファイアウォールと、オンプレミス ネットワークから Google Cloud VPN ゲートウェイへの IPSec 接続へのサイトツーサイト VPN を示します。

©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.

Google Public Cloud 上で VM-Series のファイアウォールを設定する準備をする

Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイするを行うためのプロセスには、準備作業が必要です。

Google Marketplaceを使ってデプロイを行う場合、事前にプロジェクト ネットワークおよびサブネットワークを作成し、VM-Series ファイアウォールのインスタンスに対するネットワークおよび IP アドレスの割り当てを計画する必要があります。デプロイ時、既存のネットワークおよびサブネットワークから選択を行う必要があります。

デプロイメントを計画するときは、次のトピックを参照してください。

- 一般的な要件
- Panorama への VM-Series プラグインのインストール
- Panorama Plugin for GCPのインストール
- GCP Marketplaceからのデプロイ準備

一般的な要件

このチェックリストのコンポーネントは、直接またはPanoramaを使って管理するVM-Seriesファイアウォールのデプロイに共通のものです。Stackdriverモニタリング、VMモニタリング、オートスケーリング、またはKubernetesデプロイ環境の保護などの、サービス用のPanoramaプラグインには、追加の要件が存在しています。

互換性マトリックスから、パブリッククラウドに関するPanoramaプラグインの情報を常に確認するようにしてください。このリリースには次のソフトウェアが必要になります。

- **GCP**アカウント—リンクしているメールアドレスを持つ GCP ユーザーアカウントを持ち、そのメールアドレスのユーザー名およびパスワードを知っておく必要があります。
- **Google Cloud SDK**—まだそうしていない場合は、Google Cloud SDKをインストールします。これには、Google Cloud API、gcloud、およびその他のコマンドラインツールが含まれています。コマンドラインインターフェイスを使って、ファイアウォールテンプレートやその他のテンプレートをデプロイすることができます。
- **GCP**の**VM-Series**ファイアウォール上の**PAN-OS**—PAN-OSバージョンが動作するVM-Seriesファイアウォールは、Google Marketplaceから利用することができます。
  - **VM-Series**ファイアウォール—Panoramaから管理するVM-Seriesファイアウォールは、Google MarketplaceからのPalo Alto Networksイメージを使って、Google Cloud Platformにデプロイする必要があります。ファイアウォールは、「>VM-Series ファイアウォールの最小システム要件」を満たしている必要があります。
  - **VM-Series**ライセンス—VM-Seriesにライセンスを供与して、シリアル番号を取得する必要があります。VM-Seriesファイアウォールを Panoramaの管理対象デバイスとして追加するには、シリアル番号が必要になります。VM-Seriesファイアウォールのデプロイに Panorama plugin for GCPを使用している場合は、BYOL認証コードを指定する必要があ

©2023 Palo Alto Networks, Inc.

ります。サービスの課金はGoogle Marketplaceが取り扱いますが、デプロイするファイアウォールはPalo Alto Networksのライセンスサーバーと直接やり取りを行います。

- ファイアウォール上に**VM-Series**プラグイン—PAN-OS 9.0以降が動作しているVM-Seriesファイアウォールには、VM-Seriesプラグインが含まれています。このプラグインは、パブリックおよびプライベートクラウドの統合を管理します。互換性マトリックスに記載されているように、VM-Seriesプラグインには各リリースのPAN-OSに対応する最低バージョンが存在しています。

  PAN-OSのメジャーアップグレードがあった場合、VM-Seriesプラグインのバージョンは自動的にアップグレードされます。マイナーリリースの場合、VM-Seriesプラグインのアップグレードはご自分の判断で行ってください。アップグレードは手動で行います。「Panorama への VM-Series プラグインのインストール」を参照してください。

- 管理モードで動作する**Panorama**—管理対象ファイアウォールと同じまたはそれ以降のバージョンのPAN-OSが動作している、Panorama物理/仮想アプライアンス。仮想インスタンスは、GCPにデプロイする必要はありません。
  - ライセンスされたバージョンのPanoramaが必要です。
  - Panoramaには、管理、デプロイするVMがあるVPCへのネットワークアクセスが必要になります。
  - GCPにデプロイされているVMを管理する場合、またはオートスケーリングなどの機能を設定する場合、Panorama plugin for GCPサポートの要件を満たすために、PAN-OSおよびVM-Seriesプラグインのバージョンがパブリッククラウドの要件を満たしている必要があります。
  - Panorama上のVM-Seriesプラグイン。「Panorama への VM-Series プラグインのインストール」を参照してください
- **Panorama plugin for GCP**バージョン**2.0.0**—GCPプラグインは、VMモニタリングまたはオートスケーリングテンプレートを使ってデプロイされたファイアウォールの、ライセンス供与、ブートストラップ、および設定を行うために必要な操作を管理します。GCPプラグインはVMモニタリングまたはオートスケーリングテンプレートとともに、Panoramaテンプレートのテンプレートスタック、およびデバイスグループを使用して、管理対象VM-Seriesファイアウォールにトラフィックを送信するNATルールをプログラムします。

  「Panorama Plugin for GCPのインストール」を参照してください。

Panorama への VM-Series プラグインのインストール

Panoramaで、互換性マトリックスのパブリッククラウドに関するテーブルに記載されているように、設定するGCP機能をサポートしているバージョンのVM-Seriesプラグインをインストール、またはアップグレードします。

初期インストールVM-Seriesプラグインは Panoramaのオプションなので、最初にインストールする際にはサポートポータルからVM-Seriesプラグインをダウンロードして、次に**Panorama** > **Device Deployment**（デバイスのデプロイ） > **Plugins**（プラグイン）に移動して、アップロードとインストールを行う必要があります。

Upgrade（アップグレード）—**Panorama** > **Device Deployment**（デバイスのデプロイ） > **Plugins**（プラグイン）に移動して、**Check Now**（今すぐ確認）をクリックします。互換性マトリックスのパブリッククラウドの要件を満たしているバージョンをインストールします。

 ©2023 Palo Alto Networks, Inc.

Panorama Plugin for GCPのインストール

Panoramaを使って、Palo Alto Networksテンプレートで作成されたVMモニタリングまたはオートスケーリングデプロイ環境を管理したい場合は、Panorama plugin for GCPが必要です。Panoramaで、互換性マトリックスのパブリッククラウドに関するテーブルに記載されているように、設定するGCP機能をサポートしているバージョンのプラグインをインストールします。

*Panorama Plugin for GCP*をバージョン*1.0.0*からバージョン*2.0.x*にアップグレードすることはできません。バージョン*1.0.0*をインストールしている場合は、それを削除してから*2.0.x*をインストールしてください。

STEP 1 | インストールされているPanoramaを確認します。

Panoramaで、PAN-OSのバージョンがGCPオートスケーリングをサポートするための要件を満たしていることを確認します。

STEP 2 | Panorama plugin for GCP v1.0を削除します。

Panorama plugin v1.0がインストールされている場合は、それを削除する必要があります。

STEP 3 | Panorama plugin for GCPをインストールします。

Panorama > **Plugins**（プラグイン）を選択して、検索バーに**gcp**と入力します。設定する機能をサポートしているバージョンのプラグインをインストールします（パブリッククラウドの互換性マトリックステーブルを参照）。

インストール後は、Panoramaダッシュボードの**General Information**（全般情報）リストから、プラグインを参照することができます。**Panorama** > **GoogleCloud Platform**を表示すると、[セットアップ]、[モニタリング定義]、および[オートスケール]インターフェースが表示されます。

STEP 4 | （任意）Panoramaアプライアンスが高可用性構成である場合、両方のPanoramaピアに同じバージョンのGoogleプラグインを手作業でインストールする必要があります。

*Google*プラグインは、アクティブ*Panorama*ピア上にのみ設定します。コミット時に設定はパッシブ *Panorama* ピアと同期されます。*VM*モニタリング用に設定した*Google VM*にポーリングを行うのは、アクティブ*Panorama*ピアだけです。

GCP Marketplaceからのデプロイ準備

Google Marketplaceを使ってGoogle Compute Engine（GCE）インスタンスにファイアウォールをデプロイする前に、これらの要件を確認して適切なアカウントと権限を持っていることを確認してください。

- 一般的なアカウントおよびアクセス許可
- 利用可能なGoogleリソース
- Googleの認証方式
- SSH キーペア

©2023 Palo Alto Networks, Inc.

一般的なアカウントおよびアクセス許可

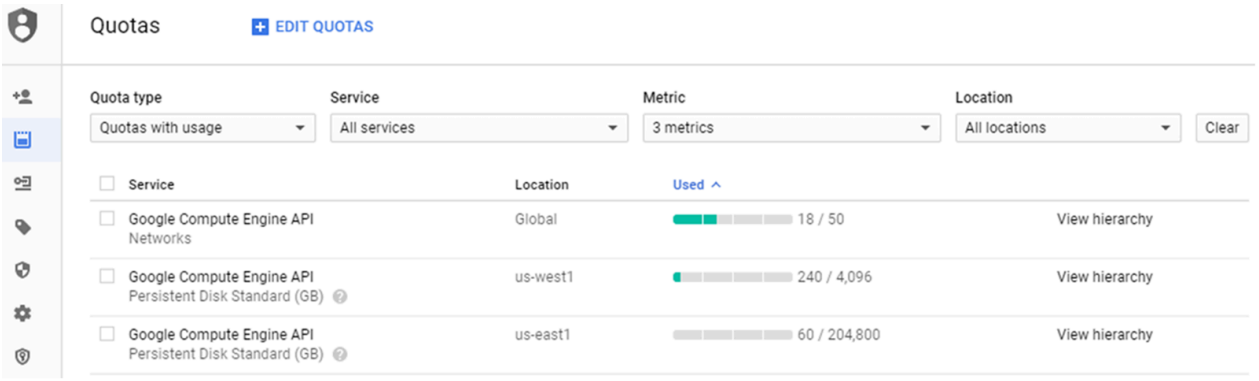
- 自分自身、および自身が許可するすべてのユーザーが、VM-Series ファイアウォールに接続するための次の最低限のロールあるいは同等の Identity and Access Management（IAM）権限を持っている必要があります。
  - **Compute Viewer** —Compute Viewerにより、コンピューティングエンジンのリソースを取得し、それらのリソースに格納されたデータを読み取ることができなくてもリストすることができます。
  - ストレージ オブジェクト ビューワー— 同じプロジェクト内の Google ストレージ バケットを使用してブートストラップすることができます。

  必要以上の権限を持つIAM 権限あるいは事前定義済みのロールを組織内のユーザーが持っているかもしれません。*VM-Series* ファイアウォールのアクセスを適切に制限するようにしてください。

  「Googleの認証方式」で説明しているように、サービスアカウントでアクセスを制限することもできます。
- モニタリング メトリック ライター— Stackdriver に対して要求されます。

利用可能なGoogleリソース

プロジェクトには、 VM-Series ファイアウォールを Google Compute Engine のインスタンスとしてデプロイするのに十分なリソースが必要です。GCP Marketplaceソリューションをデプロイする場合は、ソリューションがファイアウォールに加えて他の VM もデプロイするかどうか判断してください。Google Cloud Consoleで、[**IAM** と **admin** > **Quotas**]を選択して、プロジェクトのリソースクォータと、消費されたネットワークとディスク容量を確認します。リソースを消費し尽くしている場合は、Google 社に連絡して組織の割り当てを増やしてもらうことが可能です。



Googleの認証方式

GCP は、インスタンスに接続するための複数の方法をサポートしています。サービス アカウントあるいは SSH キーペアを使って認証できます。

1. サービス アカウント—サービス アカウントはエンドユーザーではなく、アプリケーションやVMに適用されます。これらは、プログラムやスクリプトを使用するとき、またはgcloudコマンド ラインからファイアウォールにアクセスするときに、アクセスを制御するために一般的に使用されます。Google サービス アカウントを認証インスタンスまたはアプリケーショ

©2023 Palo Alto Networks, Inc.

ンに使用している場合は、そのアカウントの電子メール アドレスを知っている必要があります。サービス アカウント キーの作成と管理を参照してください。

別のプロジェクトから、またはコマンドラインからなど、プロジェクト外から VM-Series ファイアウォールに接続したい場合は、サービス アカウントを使用する必要があります。たとえば、物理的な次世代ファイアウォールが VM-Series ファイアウォールを監視できるようにする場合、VM-Series ファイアウォールのサービス アカウント情報を JSON ファイルに保存する必要があります。接続を構成する際、物理的ファイアウォール内でファイルをアップロードします。

1. **IAM & Admin** > **Service accounts**（サービスアカウント）を選択して、**+Create Service Account**（サービスアカウントの作成）を選択します。

   サービスアカウント名と説明を入力して、**Create**（作成）をクリックします。
2. ドロップダウンメニューからロールタイプを選択し、右側から適切なアクセスレベルを選択します。

   たとえば、Project > Editorを選択します。サービスアカウントに対して複数のロールを選択できます。終了したら、**Continue**（続行）をクリックします。
3. 特定のユーザーに、このサービスアカウントにアクセスするためのアクセス許可を与えます。前のステップのロールにアクセスためのアクセス許可を与えるには、右側の**Permissions**（アクセス許可）列からメンバーを選択します。

2. **SSH**キー—Marketplaceから VM-Series ファイアウォールをデプロイする場合、Google Compute Engine インスタンスのメタデータ用に、単一の Open SSH キーを RSA 形式で提示する必要があります。

   VM-Series ファイアウォールは、デプロイ時にキーを一つだけ許可します。

   「SSH キーペア」の説明のように、デプロイ時に公開鍵をMarketplaceのデプロイメント内に貼り付けます。デプロイ後、秘密鍵を使って SSH でファイアウォールに接続し、管理者アカウントを設定します。ユーザーを追加する方法については、ファイアウォール管理者の管理を参照してください。

さまざまな方法で認証できます:

- インスタンスのサービスアカウントを作成する—特定のインスタンスまたはインスタンスグループに対するサービスアカウントを作成して、特定のアクセス許可を与えることができます。このアクセス許可は、その後ユーザーに与えられます。
- プロジェクトのフォルトのサービスアカウントを使用する—Google Cloud Platform（GCP™）コンソールを使用している場合、メールアドレスを使ってログインし、プロジェクト管理者

©2023 Palo Alto Networks, Inc.

からアカウントに割り当てられた権限あるいはロールに基づいてGCEインスタンスにアクセスできます。

Google Cloud Consoleまたはgcloudコマンドライン ツールを使用して作成されたすべてのGoogle Compute Engineインスタンスには、名前が電子メールアドレス形式のデフォルトのサービス アカウントがあります。

```
<project-number>-compute@developer.gserviceaccount.com
```

ファイアウォール インスタンスのサービス アカウント名を表示するには、インスタンスの詳細を表示し、下部にスクロールします（Compute Engine のデフォルトのサービス アカウントを参照）。

デフォルトのサービスアカウントは、VM-Seriesファイアウォールと同じプロジェクト内のVMの認証を管理できます。アクセススコープを使用すると、ファイアウォールはGoogle Cloudプロジェクトの VMのAPI呼び出しを開始できます。

- **IAM 権限および Google API** を使用—Google SDK API とgcloud を使用する場合は、API を呼び出して認証する必要があります。
  - コマンドラインからファイアウォールを管理する場合や、ファイアウォールを設定するスクリプトを実行したい場合は、通常、Google SDK を使用します。
  - 接続する仮想マシンにGoogle APIを必要とするアプリケーションを含むカスタム イメージがない限り、Google APIにアクセスする必要はありません。

SSH キーペア

Google MarketplaceからVM-Seriesファイアウォールをデプロイする場合、VM-Seriesファイアウォールの認証を受けるためにSSHキーペアが必要になります。

キー生成のドキュメントに従ってキーペアを作成します。公開鍵ファイルは編集しないでください。編集により、不正な文字が追加されるおそれがあります。

VM-Series ファイアウォールは、GCE インスタンスとは異なる方法で認証を管理します。デプロイ後は、まず**admin**（管理）ユーザーとしてログインします。VM-Seriesファイアウォールのデフォルトユーザー名は、1回のみ受け付けられます。正常にログインした後、VM-Series Web インターフェイスに使用する管理者のユーザー名およびパスワードを設定します（「Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする」を参照）。

Google MarketplaceデプロイメントインターフェイスのSSH key（SSHキー）フィールドには、次のプレースホルダが表示されます：

```
admin:ssh-rsa your-SSH-key
```

admin は、ファイアウォールに初めてログインする際に必要となる VM-Series ファイアウォールの管理者ユーザーの名前です。Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイするを行う場合、**admin:**プレフィックスをMarketplaceフィールドに追加します。

公開鍵の全部を提示しない場合、あるいはキーを Marketplace **SSH key**（**SSH** キー）フィールドに貼り付ける際に不正な文字がキーに含まれている場合、VM-Series ファイアウォールにログインできません。初めて SSH で VM-Series ファイアウォールに接続する際、公開鍵がファイアウォールに転送されます。

©2023 Palo Alto Networks, Inc.

公開鍵が壊れている場合は、デプロイメントを削除してやり直す必要があります。すべてのネットワークおよびサブネットワークが保持されますが、ファイアウォール ルールを再び作成する必要があります。

STEP 1 | SSH キーを探すに記載されている通り、SSH キーペアを作成し、お使いのオペレーティングシステムのデフォルトの場所に SSH キーペアを保存します。

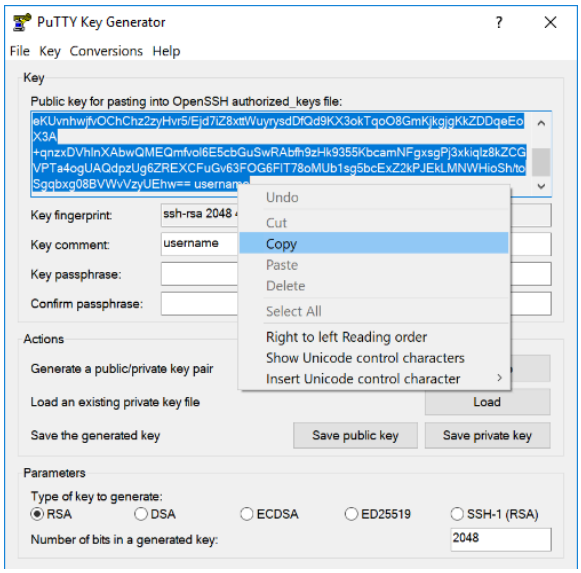
- **Linux**または**MacOS**—`ssh-keygen`を使って .sshディレクトリにキーペアを作成します。
- **Windows**—PuTTYgen を使ってキー ペアを作成します。

  Key comment（キーのコメント）フィールドは VM-Series ファイアウォールに影響しません。デフォルトのもの（キーの作成日）を残しても、キー ペアの名前を覚えやすくなるコメントを入力してもかまいません。**Save private key**（秘密鍵の保存）ボタンを使って秘密鍵を .ssh ディレクトリに保存します。

STEP 2 | 公開鍵の全体を選択します。

- **Linux**または**MacOS**—テキストエディタで公開鍵を開いて公開鍵をコピーします。
- **Windows**—PuTTY Key Generator を使用して公開鍵を表示する必要があります。PuTTYgenを起動して**Load**（読み込み）をクリックし、.sshディレクトリに保存した秘密鍵を参照します。

  PuTTYgen で下にスクロールしながらキーの全体を選択していることを確認し、右クリックして Copy（コピー）を選択します。



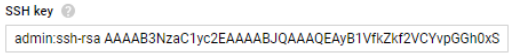
 ©2023 Palo Alto Networks, Inc.

STEP 3 | 下記の説明に従って、SSHキーフィールドに公開鍵を入力します。

1. Marketplace **SSH key**（**SSH** キー）フィールドでプレースホルダおよび次のタイプを削除します：

   admin:

   コロンの後に余分なスペースがないことを確認してください。
2. カーソルを**admin:**の後に挿入して**Paste as plain text**（プレーンテキストとして貼り付け）を選択します。以下に示すように、キーは1行で指定する必要があります。

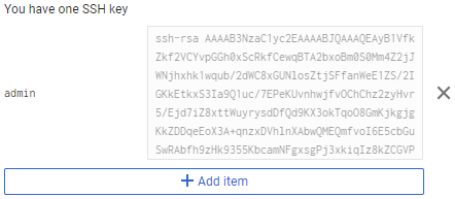
3. カーソルをキーの最後に移動してスペースを追加して、次に**admin**と入力します。

   SSH key（**SSH**キー）フィールドの最終的な内容は、次のようになります:

   admin:ssh-rsa [KEY] **admin**

STEP 4 | キーを確認します。

デプロイ後、ファイアウォールにログインしようと試みる前に、管理インスタンスを表示して、改行や余分なスペースなどがないかどうか、キーをチェックします：



キー全体が1行に指定されており、その形式が**admin:ssh-rsa** [KEY] **admin**のようになっている場合、これで作業は完了です。

STEP 5 | （任意）何か問題がある場合は、キーを交換する必要があります。

1. **X**をクリックしてキーを削除してから、**+ Add item**（項目の追加）をクリックします。
2. ステップ3に記載されているように、キーを入力します。ここで、**SSH** キーフィールドに以下が表示されるはずです。

   admin:ssh-rsa [KEY] **admin**
3. **Save**（保存）をクリックして更新されたデプロイメントをデプロイします。
4. キーを再確認します。

仮想プライベート クラウド（VPC）ネットワークの計画

Google Marketplaceからデプロイする前に、VPCネットワーク（ネットワークと呼称される）、サブネットワーク（サブネットとも呼称される）、Googleファイアウォールのルールの計画を立てます。Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイするを開始する前に、ネットワークとサブネットワークを作成する必要があります。

Marketplace デプロイメント ページには、デプロイ開始時に存在したネットワークおよびサブネットワークだけが表示されます。ネットワークが不足している場合、デプロイメントを閉じてネットワークを作成してからやり直す必要があります。

 ©2023 Palo Alto Networks, Inc.

- **VPC**ネットワーク—各VM-Seriesファイアウォールネットワークインターフェイス専用のカスタムネットワークを作成する必要があります。
  - VM-Series ファイアウォールのライセンスに基づき、必要なネットワーク インターフェイス数を決定するために、「パブリック クラウドの VM-Series ファイアウォール ライセンス」を参照してください。VM-Series ファイアウォールをローンチするために必要となる、少なくとも 3 つの VPC ネットワークとサブネットを設定します。
  - GCP プロジェクトには、事前設定済みの設定とファイアウォール ルールを備えたデフォルトのネットワークがあります。このデフォルトのネットワークを使用しない場合は削除することができます。
  - デフォルト設定では、単一のプロジェクトに最大 5 つのネットワークがあります。GCP 管理者は、プロジェクト用の追加のネットワークをリクエストできます。
  - 管理インターフェイスに接続するためには、アクセスを許可する GCP ファイアウォール ルールを作成する必要があります。**Enable GCP Firewall rule for connections to Management interface**（管理インターフェイスへの接続に使用する **GCP** ファイアウォール ルールを有効化）する選択を行い、**Source IP in GCP Firewall rule for connections to Management Interface**（管理インターフェイスへの接続に使用する **GCP** ファイアウォール ルール内の送信元 **IP**）用の CIDR ブロックを指定すれば、デプロイ中にこれを行えます。

    保護したいインスタンスをネットワークに必ずすべて含めてください。

- サブネットワーク—コンピューティング エンジンのインスタンスは、1 つのインスタンスで最大 8 つのレイヤー 3 インターフェイスをサポートできます。Management、Trust、および Untrust インターフェイスは 3 つのインターフェイスを消費します。また、最大 5 つの追加データプレーン インターフェイスを作成できます。通常、データプレーン インターフェイスがアプリケーションのネットワークを代表します。
- **IP**アドレス—インターフェイスサブネットワークを作成する際にIPアドレス範囲を指定し、サブネットワークをデプロイするときに外部アドレスを有効にするオプションがあります。
  - ネットワーク サブネットを作成するときは、IP アドレスの範囲を指定する必要があります。この範囲を内部ネットワークで使用するため、他のサブネットとオーバーラップさせることはできません。
  - デプロイ時に、ネットワーク インターフェイスの作成時に外部 IP アドレスを有効にすることができます。デフォルト設定では、単一のエフェメラルなIP アドレスが与えられます。デプロイ中に予約済みの静的 IP アドレスを指定することはできませんが、デプロイ後にエフェメラルなアドレスを静的 IP アドレスへと昇格することができます（エフェメラルな外部 IP アドレスを指定を参照）。

ネットワーク インターフェイスの計画

Google Cloud Platform Marketplace からデプロイする場合、デフォルトの VM-Series のファイアウォールのデプロイメントには、管理プレーン インターフェイス、ならびに Untrust および Trust データプレーン インターフェイスの 3 つのインターフェイスがあります。VM 上の利用可能なコンピューティング リソースに応じて、追加のデータプレーン インスタンスを定義できます。 詳細は、「パブリック クラウドの VM-Series ファイアウォール ライセンス」を参照してください。

©2023 Palo Alto Networks, Inc.

デプロイ中にこれらのインターフェイスに名前を付けられます。

インターフェイスの順序

Marketplaceでデプロイする場合、ネットワーク インターフェイスの順序は事前に定義されます。管理インターフェイスは eth0、Untrust to eth1、および Trust to eth2 にマップされます。負荷分散のために管理インターフェイスをスワップする必要がある場合、管理インターフェイスを eth0 にマッピングし、Untrusted インターフェイスを eth1 にマッピングする必要があるため、Marketplace はこの順序を使用します。

管理インターフェイス

追加する最初のネットワーク インターフェイスはファイアウォールの eth0 にマップされ、これには IP 転送を有効にするオプションが含まれます。このネットワークインターフェイスを使って VM-Series ファイアウォールを管理できます。通常、このインターフェイスは外部 IP アドレスを一つ持ちます。

外部 *IP* アドレスは、パブリック サブネットにアタッチされるデータプレーン インターフェイスの場合にのみ必要です。作成時に、一時的な *IP* アドレスを受け取ってから、デプロイ後にそれを静的 *IP* アドレスに昇格することができます（一時的な外部 IP アドレスの昇格を参照）。

データプレーン インターフェイス（**Untrust**、**Trust**）

Marketplace からデプロイする際、インターフェイスを追加する順序は事前に決められています。

- 管理インターフェイスの後に Untrust インターフェイスを設定します。この順序は、信頼されていないインターフェイスが eth1 にマッピングされていることを示します。Untrust インターフェイスは通常、パブリック サブネットに接続され、外部 IP アドレスを有します。

  外部 *IP* アドレスは、パブリック サブネットにアタッチされるデータプレーン インターフェイスの場合にのみ必要です。作成時に、「一時的な外部 IP アドレスの昇格」で説明したように、一時的な *IP* アドレスを受け取り、それを静的 *IP* アドレスに昇格することができます。

- Trust インターフェイスは、Untrust インターフェイスの次に来て、eth2 にマップされている必要があります。Trust ネットワークには、外部 IP アドレスがないことが多いです。Trust インターフェイスの後で、任意のデータプレーン インターフェイスを追加できます。

追加のデータプレーン インターフェイス

WEB サーバー、データベース、ネットワーク内のその他のアプリケーションなど、保護する必要があるアプリケーションのインターフェイスを計画します。ファイアウォールを起動するのに必要となる 3 つのインターフェイスに加え、最大 5 つの追加のデータプレーン インターフェイスを作成できます。保護するアプリケーションが、VM-Series ファイアウォールに接続するネットワーク内にあることを確認してください。

©2023 Palo Alto Networks, Inc.

Google Cloud PlatformへのVM-Seriesファイアウォールのデプロイ

GCP Marketplaceテンプレートを使ってVM-Seriesファイアウォールをデプロイするには、ファイアウォール上の各インターフェイスに対して、まずVPCネットワークを作成する必要があります。Google Marketplaceからファイアウォールをデプロイした後、GCP VPC設定内で機能するように、ファイアウォールにログインして設定を調整することができます。モニタリングを有効にして、リソース管理の改善に役立つ測定基準を収集したり、アプリケーション環境の変更に自動的に適合するセキュリティポリシールールを作成したりすることもできます。

- Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする
- Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ
- VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ
- VM-Series ファイアウォールでの Google Stackdriver モニタリングの有効化
- VM を監視して Google Cloud Platform（GCP）上の VM の変更を追跡する
- ダイナミックアドレスグループを使用してVPC内のインスタンスを保護する
- カスタム テンプレートあるいは gcloud CLI を使用して VM-Series ファイアウォールをデプロイ

Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする

Google® Cloud Platform Marketplaceを使用し、固定 vCPU キャパシティ ライセンスの VM-Series ファイアウォールをデプロイできます(VM-Series モデル)。パブリック クラウド から利用できるライセンスイメージは次のとおりです。

- VM-Series 次世代ファイアウォール バンドル 1
- VM-Series 次世代ファイアウォール バンドル 2
- VM-Series 次世代ファイアウォール（BYOL）

これらのライセンス オプションの詳細については、Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイするを参照してください。

Marketplace は、最小限の管理インターフェイスと 2 つのデータプレーン インターフェイス（Trust および UnTrust）を備えた VM-Series ファイアウォールのインスタンスをデプロイします。仮想プライベート クラウド（VPC）内に最大 5 つの Google Compute Engine インスタンス用の追加のデータプレーン インターフェイスを追加できます。

VM-Series ファイアウォールをデプロイする前に、組織内でプロジェクトを作成または選択し、「VPC ネットワーク計画」と「ネットワークインターフェイスの計画」記載の指示に従ってファイアウォールに接続するネットワークとサブネットを作成する必要があります 。

同じ VPC ネットワークに複数のネットワーク インターフェイスを接続することはできません。作成するすべてのインターフェイスには、少なくとも 1 つのサブネットを持つ専用ネットワー

©2023 Palo Alto Networks, Inc.

クが必要です。ネットワークに追加のデータプレーン インスタンスが含まれていることを確認してください。

STEP 1 | ブートストラップ方法の選択.

STEP 2 | マーケットプレイスで VM-Series ファイアウォールのリスティングを探します。

1. Google Cloud Console にログインします。
2. Products and Services（製品とサービス）メニューで、**Marketplace**（マーケットプレイス）を選択します。
3. **VM-Series** を検索します。
4. VM-Series ファイアウォール ライセンスのオプションを 1 つ選択します。

STEP 3 | **Launch on Compute Engine**（**Compute Engine** の起動）クリックします。

STEP 4 | インスタンスに名前を付け、リソースを選択します。

1. **Deployment Name**（デプロイ名）を入力します（この名前は Deployment Manager で表示されます）。名前は固有のものである必要があり、プロジェクト内の他のデプロイと競合することはできません。
2. **Zone**（ゾーン）を選択します。サポートされている一連のゾーンのリージョンおよびゾーンを参照してください。
3. ご利用のライセンス VM-Series システム要件およびGoogle Cloud Platform 上の VM-Series ファイアウォールの最小システム要件に従い **Machine Type**（マシン タイプ）を選択します。

STEP 5 | インスタンスのメタデータを指定します。

Bootstrap Bucket（ブートストラップ バケット）および**Interface Swap**（インターフェイスのスワップ）オプションは、VM-Series ファイアウォールが初めて起動する際の初期設定に影響します。

1. **Bootstrap Bucket**（ブートストラップ バケット）（任意）–ブートストラップファイルを使う予定である場合は、ストレージバケットの名前、またはブートストラップ パッケージを含んでいる、ストレージバケット内のフォルダへのパスを入力します。ストレージバケットにアクセスするためのアクセス許可が必要です。以下に例を示します。

   vmseries-bootstrap-gce-storagebucket=<<バケット名**>>**

   or

   vmseries-bootstrap-gce-storagebucket=<バケット名**/**ディレクトリ名**>**

   カスタムメタデータを使ってブートストラップすることを選択した場合、ステップ6に進んでください。
2. **Interface Swap**（インターフェイスのスワップ）（任意）–デプロイ時に管理インターフェイス（eth0）と最初のデータプレーン インターフェイス（eth1）をスワップします。インターフェイスのスワップは、Google Cloud Platform HTTP（S）ロード バランシングの内側に VM-Series ファイアウォールをデプロイする場合にのみ必要です。詳細

©2023 Palo Alto Networks, Inc.

については、「Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ」参照してください。

3. **SSH key**（**SSH** キー）—SSH キーペアからパブリック キーを貼り付けます。SSH キーペアで対象の OS の指示に従い、キーを作成、コピーして貼り付けます。Windows ユーザーは PuTTY でキーを表示し、ユーザーインターフェイスからコピーして マーケットプレイス デプロイメントに貼り付ける必要があります。

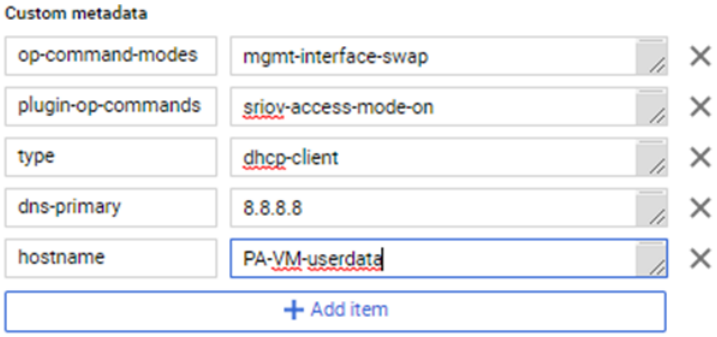
   キーの書式が正しくない場合、*VM-Series* ファイアウォールがログインを拒否します。デプロイメントを削除してやり直す必要があります。

4. **More**（その他）をクリックして他のメタデータ オプションを表示します。**blockProjectKeys**および**enableSerialConsole**のオプションはインスタンスのプロパティです。デプロイが正常に完了した後、このメタデータの値を変更できます。

   - **blockProjectKeys** （任意）—プロジェクト キーをブロックする場合、指定した SSH 公開鍵のみを使用してインスタンスにアクセスできます。
   - **enableSerialConsole** （任意）—シリアル コンソールと対話することで、インスタンスの作成を監視し、インタラクティブなデバッグ タスクを実行できます。

STEP 6 | カスタムメタデータを指定します。

カスタムメタデータを使ってブートストラップすることを選択した場合、ステップ5で追加しなかったキーと値のペアを追加します。キー/値のペアの一覧については、「Init-cfg.txt ファイルのコンポーネント」を参照してください。以下に例を示します。



STEP 7 | ブート ディスクを設定します。

1. **Boot disk type**（起動ディスクのタイプ）—SSD 永続ディスクあるいは標準的な永続ディスクのいずれかを選択します。「ストレージのオプション」を参照してください。
2. **Boot disk size**（起動ディスクのサイズ）—最大サイズは 60GB です。後でディスク サイズを編集できますが、そのためには VM を停止する必要があります。

STEP 8 | 管理インターフェイスを設定します。

1. **Management VPC Network name**（管理 **VPC** ネットワーク名）—既存のネットワークを選択します
2. **Management Subnet name**（管理サブネット名）—既存のサブネットを選択します。
3. **Enable External IP for Management interface**（管理インターフェイス用の外部 **IP** を有効化）（任意）—このオプションを有効にすると、VM-Series ファイアウォール管理イ

©2023 Palo Alto Networks, Inc.

ンターフェイスに割り当てられた IP アドレスを使用して、SSH で VM-Series ファイアウォール Web インターフェイスにアクセスできます。

4. **Enable GCP Firewall rule for connections to Management interface**（管理インターフェイスへの接続に使用する **GCP** ファイアウォール ルールを有効化）（任意）—このオプションは、指定する外部の送信元 IP アドレス用に GCP ファイアウォール許可ルールを自動的に作成します。
5. **Source IP in GCP Firewall rule for connections to Management Interface**（管理インターフェイスへの接続に使用する **GCP** ファイアウォール ルール内の送信元 **IP**）—**Enable GCP Firewall rule for connections to Management interface**（管理インターフェイスへの接続に使用する **GCP** ファイアウォール ルールを有効化）する場合は、送信元 IP アドレスあるいは CIDR ブロックを入力します。
   - 0.0.0.0/0 は使用しないでください。専用管理 IP アドレスまたはネットワークに対応する IP アドレスあるいは CIDR ブロックを指定してください。ソース ネットワークの範囲を必要以上に大きくしないでください。
   - アドレスをチェックし、自分自身をロックアウトしていないことを確認します。

STEP 9 | Untrust データプレーン インターフェイスを設定します。

1. **Untrust VPC Network name**（信頼しない **VPC** ネットワーク名）—既存のネットワークを選択します。
2. **Untrust Subnet name**（信頼しないサブネット名）—既存のサブネットを選択します。
3. **Enable External IP for Untrust**（**Untrust** の外部 **IP** を有効化）—GCP を有効化し、外部 IP アドレスとして機能するエフェメラルなIP アドレスを指定します。

STEP 10 | Trust データプレーン インターフェイスを設定します。

1. **Trust VPC Network name**（信頼する **VPC** ネットワーク名）—既存のネットワークを選択します。
2. **Trust Subnet name**（信頼するサブネット名）—既存のネットワークを選択します。
3. **Enable External IP for Trust**（**Trust** の外部 **IP** を有効化）—GCP を有効化し、外部 IP アドレスとして機能するエフェメラルなIP アドレスを指定します。

©2023 Palo Alto Networks, Inc.

STEP 11 | その他のインターフェイスを設定します。追加するデータプレーン インターフェイスの数を入力する必要があります（デフォルトは 0（なし））。デプロイメント ページには、番号 4～8 の追加のデータプレーン 5 つに使用するフィールドが常に表示されます。

1. **Additional Dataplane interfaces**（追加のデータプレーン インターフェイス）—追加のデータプレーン インスタンスの数を入力します。

   この数が *0*（デフォルト）である場合、インターフェイス フィールドで指定していても、番号 *4*～*8* のデータプレーンは無視されます。たとえば *2* を指定してから *3* つのインターフェイスの情報を入力すると、最初の *2* つだけが作成されます。

2. **Additional Dataplane # VPC name**（追加のデータプレーン **[**番号**]** VPC 名）—既存のネットワークを選択します。
3. **Dataplane # Subnet name**（データプレーン **[**番号**]** サブネット名）—存在するサブネットを選択します。
4. **Enable External IP for dataplane # interface**（データプレーン **[**番号**]** インターフェイスの外部 **IP** を有効化）—GCP を有効化し、外部 IP アドレスとして機能するエフェメラルなIP アドレスを指定します。

STEP 12 | インスタンスを**Deploy**（デプロイ）します。

STEP 13 | Google Cloud Deployment Managerを使ってデプロイメントを閲覧・管理します。

STEP 14 | CLI を使用して、ファイアウォールの管理者パスワードを変更します。

1. コマンドラインから VM-Series ファイアウォールにログインします。お使いの SSH ツールで管理インターフェイスの外部 IP に接続し、秘密鍵へのパスを指定します。

   Windows ユーザー：PuTTY を使って VM-Series ファイアウォールに接続し、コマンドラインの指示を出します。秘密鍵へのパスを指定するために、**Connection**（接続） > **SSH** > **Auth**（認証）を選択します。**Private key file for authentication**（認証用の秘密鍵ファイル）：**Browse**（参照）をクリックして秘密鍵を選択します。

2. 設定モードに切り替えます。

   ```
   VMfirewall> configure
   ```

3. 以下のコマンドを入力します。

   ```
   VMfirewall# set mgt-config users admin password
   ```

4. 管理者の新しいパスワードを入力して確認します。
5. 新しいパスワードをコミットします。

   ```
   VMfirewall# commit
   ```

6. コマンド モードに戻ります。

   ```
   VMfirewall# exit
   ```

7. （任意）インターフェイスのスワップ用にブートストラップ ファイルを使用した場合、次のコマンドを使ってインターフェイス マッピングを表示します：

   ```
   VMfirewall> debug show vm-series interfaces all
   ```


©2023 Palo Alto Networks, Inc.

STEP 15 | VM-Series のファイアウォール Web インターフェイスにアクセスします。

1. ブラウザで、管理インターフェイスの IP アドレスへのセキュアな（https）接続を作成します。

   ネットワーク エラーが発生する場合は、接続を許可する GCP ファイアウォール ルールがあることを確認してください。
2. プロンプトが表示されたら、CLI から指定したユーザー名（admin）と管理者用パスワードを入力します。
3. （任意）ブート処理を行った場合、ブート処理の完了を検証します。

   問題が発生した場合は、VM-Series ファイアウォールのログ情報を検索してください。**Monitor**（監視） > **System**（システム）を選択して手動検索フィールドに **`description contains 'bootstrap'`** と入力し、ブート処理が完了したことを示す結果のメッセージを探してください。

物理ファイアウォールの場合と同様に、ファイアウォールにログインした後、管理者を追加してインターフェイス、ゾーン、NAT ルール、およびポリシー ルールを作成できます。

Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ

内部負荷分散は、次ホップの負荷分散された Google Compute Engine インスタンスのプライマリ インターフェイスにのみトラフィックを送信できるため、VM-Series ファイアウォールはデータプレーン トラフィックに eth0 を使用できる必要があります。

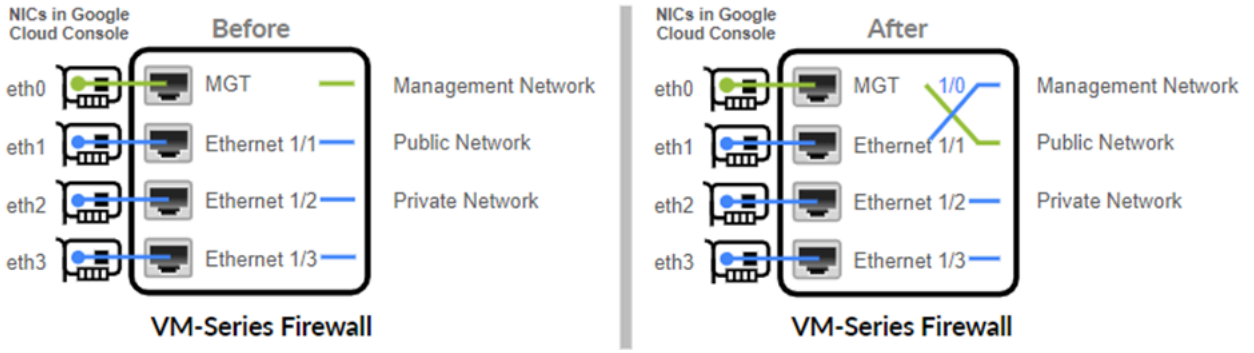
VM-Series のファイアウォールが Google Cloud Platform の内部負荷分散インターフェイスの背後にある場合、ファイアウォールは eth0 でデータプレーン トラフィックを受信できます。

- VM-Series ファイアウォールは、企業ネットワークへの VPN リンクまたは直接接続リンクを必要とせずに、トラフィックをインターネットに直接送信します。
- VM-Series ファイアウォールは、各ファイアウォールにつきバックエンド サーバー（Web サーバーなど）が 1 つだけある場合にのみ、インターネットに接続するアプリケーションを守ります。VM-Series のファイアウォールと Web サーバーは、Google の内部負荷分散アドレスの後ろで、ペアで線形に拡張できます。

ファイアウォールが eth1 ではなく eth0 でデータプレーン トラフィックを送受信できるようにするには、eth0 が ethernet 1/1 にマッピングされるように、eth1 がファイアウォール上の 内部負荷分散ネットワーク インターフェイスのマッピングをスワップできるようにする必要があります。

可能な場合、ファイアウォールを構成する前、およびポリシー ルールを定義する前に管理インターフェイスのマッピングをスワップします。

©2023 Palo Alto Networks, Inc.



インターフェイスのマッピング方法をスワップすることで、Google Cloud Platform は、同じゾーンまたは異なるゾーンにある VM-Series ファイアウォールの正常なインスタンスにトラフィックを配信し、ルーティングすることができます。

管理インターフェイスをスワップする

インターフェイスをスワップする、または作成後にファイアウォールを設定することができます。

作成時– VM-Series ファイアウォールをデプロイするとき、2 通りでインターフェイスのスワップを有効化できます。

- Google Cloud Console – インスタンスの作成フォームで、**Metadata**（メタデータ）フィールドでキーと値のペアを入力します。ここでは、**mgmt-interface-swap** がキーであり、**enable** が値です。
- 「Google Cloud Platform 上の VM-Series ファイアウォールのブートストラップ」で説明されている通りに、ブートストラップ ファイル –ブートストラップ設定に **mgmt-interface-swap** コマンドを含めたブートストラップファイルを作成します。インスタンスの作成フォームで、**Metadata**（メタデータ）フィールドにキーと値のペアを入力して、ブートストラップオプションを有効にします。

VM-Series ファイアウォールから–ファイアウォールにログインして、VM-Series ファイアウォール CLI を使用した管理インターフェイスをスワップします。運用モードでは、次のコマンドを発行します。

```
set system setting mgmt-interface-swap enable yes
```


©2023 Palo Alto Networks, Inc.

- インターフェイス スワップの設定を指定する方法として、ブートストラップ設定ファイル、ファイアウォール *CLI*、*Google Compute Engine* インスタンスの***Metadata***（メタデータ）フィールド（*Google Cloud Console* からアクセス）を選択します。*1* つの方法を使用すると、ファイアウォールで予測可能な動作を保証できます。

  Google Cloud Console では、*eth0* と *eth1* をスワップしたかどうかは確認できません。スワップ後、負荷分散が *eth0* で、ファイアウォール管理インターフェイスが *eth1* であるため、*Google Cloud Platform* の負荷分散を適切に設定し、*1* つ以上の *VM-Series* ファイアウォールへの負荷分散を保護するセキュリティ ポリシー ルールを作成できます。
- スワップ前に *VM-Series* ファイアウォールの構成が終了している場合は、*eth0* および *eth1* のいずれかの *IP* アドレスが変更されるとポリシー ルールが影響を受けるかどうか確認してください。

VM-Series ファイアウォール CLI を使用した管理インターフェイスのスワップ

このタスクは、アーキテクチャで *VM-Series* のファイアウォールを *Google Cloud Platform* の内部ロード バランサーの背後に配置する場合にのみ必要です。

ファイアウォールのデプロイ時にメタデータを指定して管理インターフェイス（MGT）をデータプレーン インターフェイスとスワップしなかった場合は、CLI を使用してファイアウォールがプライマリ インターフェイスでデータプレーン トラフィックを受信できるようにすることができます。

STEP 1 | Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする。

先に進む前に、ファイアウォールにネットワーク インターフェイスが *2* つ（*eth0* および *eth1*）以上あることを確認します。*1* つのインターフェイスだけでファイアウォールを起動する場合、ブート処理時にインターフェイスのスワップ コマンドによってファイアウォールがメンテナンス モードになります。

STEP 2 | Google Cloud Console で、VM インスタンスの詳細を表示して、eth1 インターフェイスのネットワーク インターフェイスの IP アドレスを確認し、セキュリティ ルールによって新しい管理インターフェイス（eth1）への接続（HTTPS および SSH）が許可されていることを確認します。

STEP 3 | VM-Series ファイアウォールの CLI にログインし、次のコマンドを入力します。

```
set system setting mgmt-interface-swap enable yes
```

コマンド ライン インターフェイスからデフォルトのマッピングを表示することができます。出力は以下に似たものになります：

```
> debug show vm-series interfaces all
Interface_name  Base-OS_port
  mgt              eth0
  Ethernet1/1      eth1
```


©2023 Palo Alto Networks, Inc.

```
Ethernet1/2      eth2
```

STEP 4 | 確定してインターフェイスをスワップします（eth1 データプレーン インターフェイスを管理インターフェイスとして使用）。

STEP 5 | ファイアウォールを再起動してスワップを反映させます：

```
request restart system
```

STEP 6 | インターフェイスがスワップされたことを確認します：

```
debug show vm-series interfaces all
```

VM-Series ファイアウォールでの Google Stackdriver モニタリングの有効化

Google® Compute Engine インスタンス上の VM-Series ファイアウォールは、カスタム PAN-OS メトリックを Google Stackdriver に公開できます。これらのメトリックを使用してパフォーマンスと使用パターンを評価し、ファイアウォール リソースを適切に管理できるようになります。

- Google Stackdriver 権限
- Google Stackdriver を有効にする

Google Stackdriver 権限

認証要件は、デフォルトのサービス アカウントを使用して認証できるかどうか、または Google API を使用して認証する必要があるかどうかによって異なります。

以下の2つの方法で認証できます：

- **VM-Series** ファイアウォールのインスタンス用にデフォルトのサービス アカウントを使用—Google Cloud Platform（GCP™）コンソールを使用している場合、メールアドレスを使ってログインし、プロジェクト管理者からアカウントに割り当てられた権限あるいはロールに基づいてインスタンスにアクセスできます。
- **IAM** 権限および **Google API** を使用—Google SDK API とgcloud を使用する場合は、API を呼び出して認証する必要があります。コマンドラインからファイアウォールを管理する場合や、ファイアウォールを設定するスクリプトを実行したい場合は、通常、Google SDK を使用します。

Google Cloud Console または gcloud コマンドライン ツールを使用して作成されたすべての Google Compute Engine インスタンスには、名前が電子メールアドレス形式のデフォルトのサービス アカウントがあります。

```
<project-number>-compute@developer.gserviceaccount.com
```

ファイアウォール インスタンスのサービス アカウント名を表示するには、インスタンスの詳細を表示し、下部にスクロールします（Compute Engine のデフォルトのサービス アカウントを参照）。

©2023 Palo Alto Networks, Inc.

デフォルトのサービス アカウントは、VM-Series ファイアウォールと同じプロジェクト内の VM を監視するための認証を管理できます。

- アクセス スコープを使用すると、ファイアウォールは Google Cloud プロジェクトの VM を監視する API 呼び出しを開始できます。
- 監視対象の仮想マシンに Google API を必要とするアプリケーションを含むカスタム イメージがない限り、Google API にアクセスする必要はありません。

物理的なファイアウォール、または別のプロジェクトの VM-Series ファイアウォールからの監視を設定する場合は、Google API を使用して認証する必要があります。前提条件は 2 つあります：

- Google API がインストールされていること。
- アカウントに Monitoring Metric Writer および Stackdriver Account Viewer のロールがなければなりません。

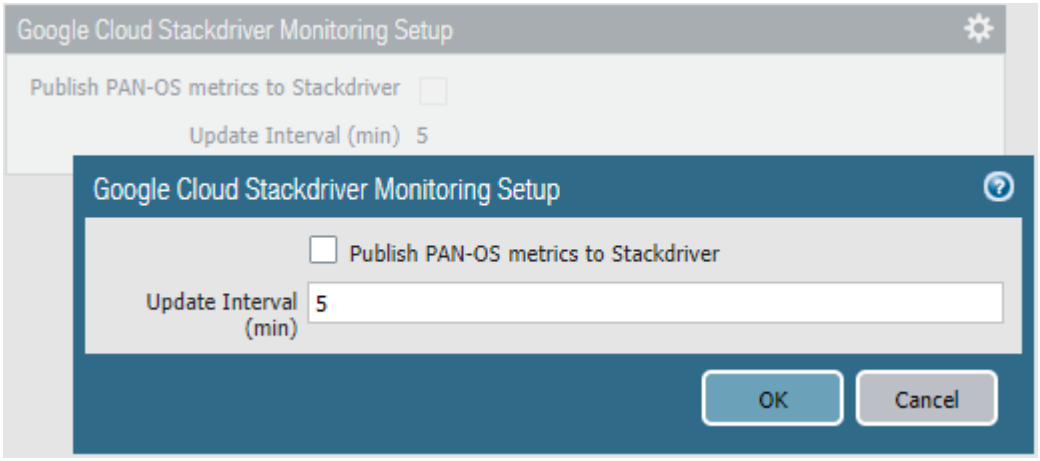
Google Stackdriver を有効にする

Google Stackdriver に公開できる PAN-OS メトリックについては、「監視用に公開されるカスタム PAN-OS メトリック」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 1 | Google Compute Engine インスタンスの VM-Series のファイアウォールから Stackdriver に PAN-OS メトリックをプッシュします。

1. VM-Series ファイアウォールの Web インターフェイスにログインします。
2. **Device**（デバイス） > **VM-Series**を選択します。Google Cloud Stackdriver の監視設定のところで、**Edit**（編集）（⚙）をクリックします。
   1. **Publish PAN-OS metrics to Stackdriver**（**PAN-OS** のメトリックを **Stackdriver** にパブリッシュ）のチェックボックスをオンにします。



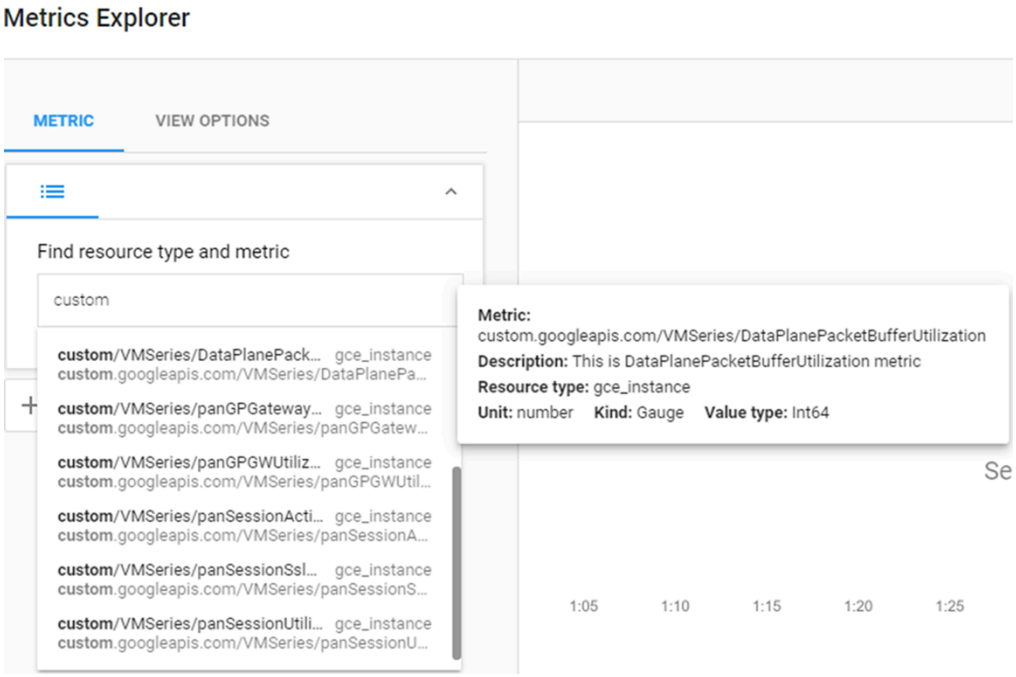
   2. **Update Interval**（更新間隔）を設定します（範囲は 1 ～ 60 分、デフォルトは 5）。これは、ファイアウォールが Stackdriver にメトリックを公開する頻度です。
   3. **OK**をクリックします。
3. 変更を **Commit (コミット)** します。

   PAN-OS メトリックのアラームを設定する前に、ファイアウォールが Stackdriver にメトリックを公開するまで待機します。

©2023 Palo Alto Networks, Inc.

STEP 2 | Stackdriver でメトリックが表示されることを確認します。

1. Google Cloud Console で、**Products and Services**（製品とサービス） > **Monitoring**（監視）を選択します。
2. Stackdriver で、**Resources**（リソース） > **Metrics Explorer**（**Metrics Explorer**）を選択します。
3. Find resource type and metric（リソース タイプとメトリックの検索）セクションで、検索フィールドに**`custom`**と入力して PAN-OS メトリックをフィルタリングします。



STEP 3 | Stackdriver で PAN-OS メトリックのアラートおよびアクションを設定します。監視のQuickstart for Google Compute Engine のクイックスタート、および Stackdriver の アラート発信の説明を参照してください。

VM を監視して Google Cloud Platform（GCP）上の VM の変更を追跡する

PAN-OS 9.0（仮想または物理）を実行するファイアウォールを有効にすると、Google Compute Engine インスタンスにデプロイされたアプリケーションのワークロードを監視できます。VM 監視では、VM-Series ファイアウォールのメタデータ要素または属性の定義済みセットを監視できますPAN-OS 9.1 管理者ガイドクラウド プラットフォームの仮想マシンで監視される属性を参照してください。

Google VPC 内の仮想マシンの追加、移動、削除を認識することで、アプリケーション環境の変更に自動的に適応するセキュリティ ポリシー ルールを作成できます。仮想マシンをデプロイまたは移動すると、ファイアウォールは属性（またはメタデータ要素）を収集します。このメタデータは、ポリシー一致およびダイナミック アドレス グループの定義に使用できます「ダイナミック アドレス グループを使用した VPC 内のインスタンスのセキュア化」を参照）。

©2023 Palo Alto Networks, Inc.

各ファイアウォール、または複数の仮想システムが可能なファイアウォール上の各仮想システムには、最大 10 個の VM 情報ソースを設定できます。Panorama テンプレートを使用して情報ソースをプッシュすることもできます。

VM モニタリングを実行するためには、IAM ロール Monitoring Metric Writer（監視メトリックライター）が必要です。

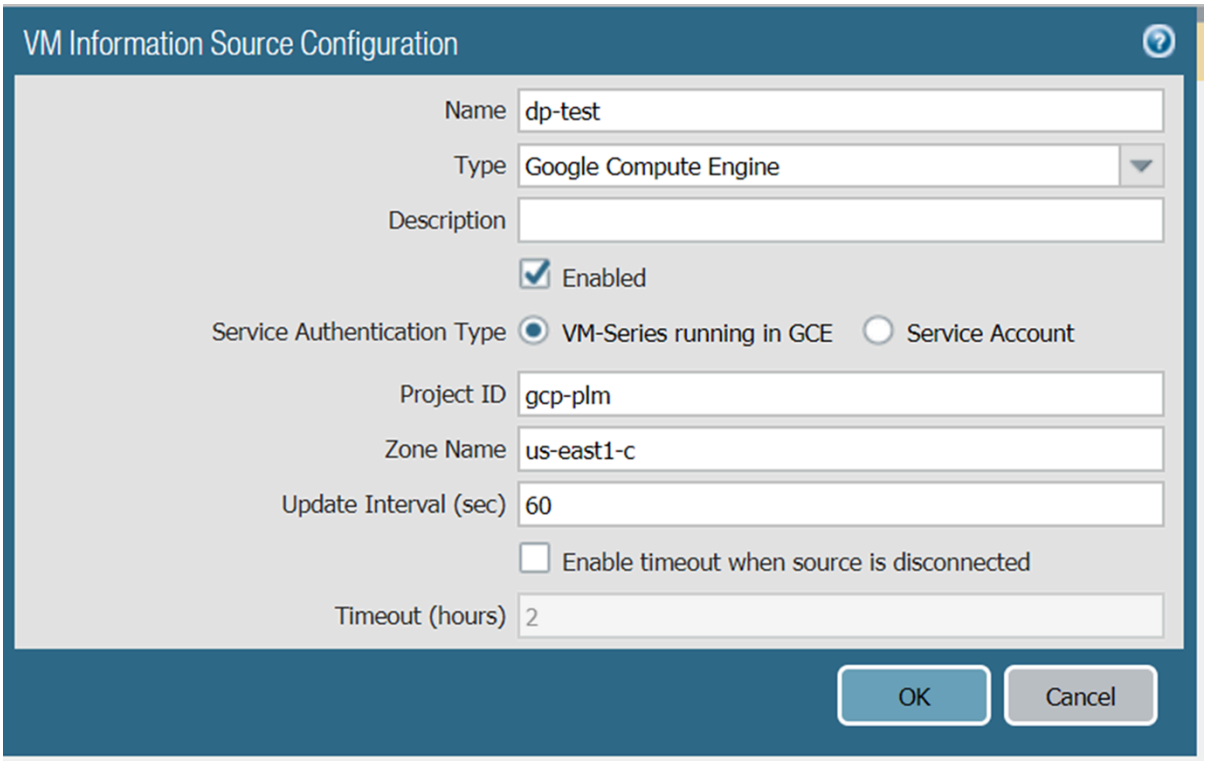
STEP 1 | デプロイしたファイアウォールにログインします。

STEP 2 | VM 監視を有効化します。

1. **Device**（デバイス） > **VM Information Sources**（**VM** 情報ソース）を選択します。
2. VM 情報ソース**Add**（追加）して次の情報を入力します：
   - **Name**（名前）に、モニターするインスタンスを識別する名前を指定します。
   - Google Compute Engine の**Type**（タイプ）を選択します。
   - **Enabled**（有効）を選択します。
   - **Service Authentication Type**（サービス認証タイプ）を選択します。
     - **VM-Series running in GCE**（**GCE** で動作する **VM-Series**）を選択すると、インスタンスの作成時に生成されるデフォルトのサービス アカウントで認証されます。これはインスタンスのメタデータの一部です。
     - 現在のプロジェクト外のファイアウォールから監視したい場合は**Service Account**（サービス アカウント）を選択しますサービス アカウントの認証情報を JSON 形式でアップロードする必要があります「サービス アカウント キーの作成と管理」を参照してください。
   - 任意**Update interval**（更新間隔）を 5 ～ 600 秒の値に変更します。デフォルトでは、ファイアウォールは 5 秒ごとにポーリングします。API 呼び出しは毎回 60 秒ご

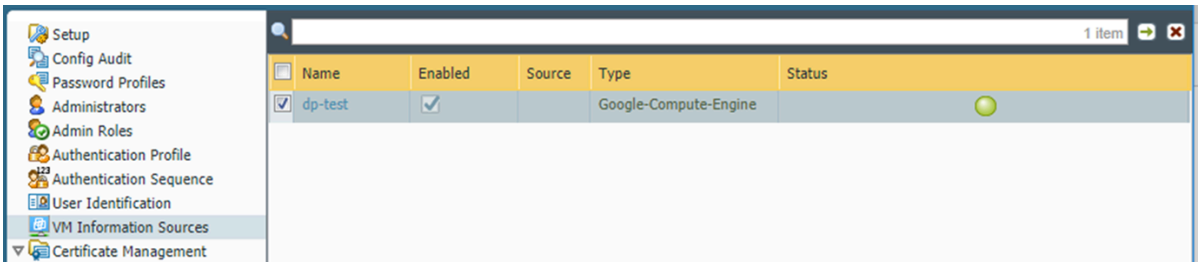
©2023 Palo Alto Networks, Inc.

とにキューに登録され取得されます。更新の最大所要時間は 60 秒に設定ポーリング間隔を加えた値となります。



- 任意）タイムアウトまでの時間数を変更するには**Enable timeout when the source is disconnected**（ソースとの接続解除時のタイムアウトを有効化）にチェックを入れ、監視対象のソースとの接続が閉じられるまでのTimeout（タイムアウト）（時間）を入力します（範囲は 2～10、デフォルトは 2）。

  ファイアウォールがホストにアクセスできず、指定された限界に達すると、ファイアウォールはソースへの接続を閉じます。
- **OK** をクリックし、変更を**Commit**（コミット）します。



STEP 3 | 接続状態を確認します。

接続状態が保留または切断の場合は、送信元が動作しており、ファイアウォールが送信元にアクセスできることを確認します。モニター対象送信元ソースとの通信に管理（MGT）ポート以外のポートを使用する場合は、サービス ルートを変更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）を選択し**Service Route Configuration**（サービス ルート設定）をクリックして**VM Monitor**（VM 監視） サービスの**Source Interface**（ソース インターフェイス）を変更します）。

©2023 Palo Alto Networks, Inc.

ダイナミックアドレスグループを使用してVPC内のインスタンスを保護する

オンデマンドで新しいインスタンスが起動される Google® Cloud Platform（GCP™）のような動的な環境では、セキュリティ ポリシーの管理負担が煩雑になることがあります。ポリシーでダイナミック アドレス グループを使用すると、俊敏性が向上し、サービスの中断や防御の間隙を阻止できます。

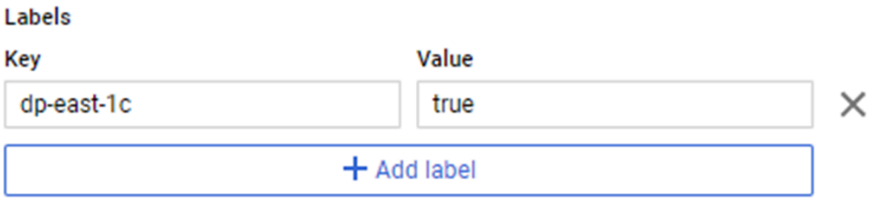
このワークフローでは、VM-Series ファイアウォールをデプロイし、インスタンス上でいくつかのアプリケーションを構成し、Google Stackdriver の監視を有効にしたことを前提としています。

STEP 1 | VPC をモニターするようにファイアウォールを設定します。

STEP 2 | VPC のインスタンスにラベルを付けます。

ラベルは、名前 - 値のペアです。Google Cloud Console、Google API 呼び出し、Google Cloud Shell からリソースにラベルを付けることができます。また、「リソースのラベリング」で説明した通り、インスタンスにラベルを付けるこの作業は、多くのリソースに適用することができます。

インスタンス ブラウザからラベルを追加することもできます。

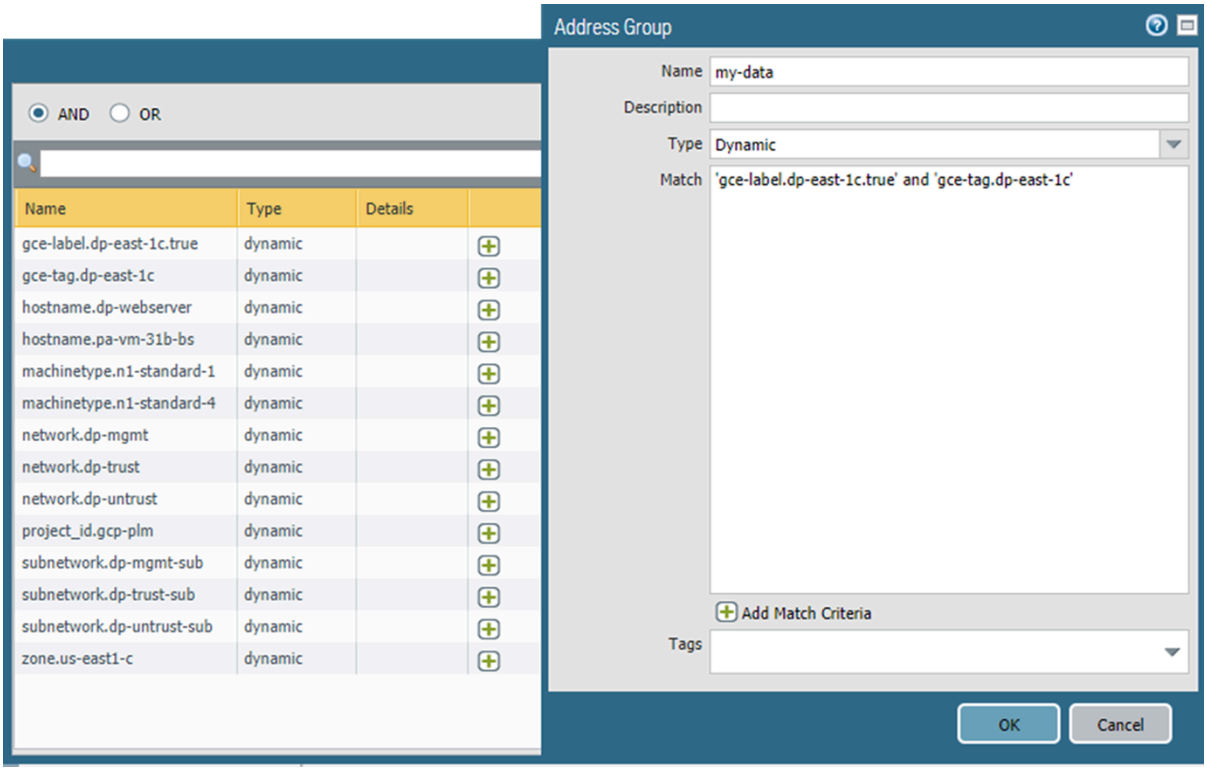


作成するラベルは、セキュリティ ポリシーに役立つ方法でリソースを差別化する戦略をサポートします。

©2023 Palo Alto Networks, Inc.

STEP 3 | ファイアウォール上にダイナミック アドレス グループを作成します。

1. **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. ダイナミック アドレス グループを **Add**（追加）し、**Name**（名前）および **Description**（説明）を指定します。
3. **Type**（タイプ）を **Dynamic**（ダイナミック）に設定します。
4. 一致条件を指定します。
   1. **Add Match Criteria**（一致条件を追加）し、**AND** 演算子を選択します。
   2. 絞り込みまたは照合の基準となる属性を選択します。



5. **OK**をクリックします。
6. **Commit**（コミット）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 4 | セキュリティ ポリシー ルールでダイナミック アドレス グループを使用します。

「my-data」というダイナミック アドレス グループに属する Web サーバーへのインターネット アクセスを許可するルールを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. ルールを **Add**（追加）し、**Name**（名前）にルールの名前を入力して、**Rule Type**（ルール タイプ）が `universal` であることを確認します。
3. **Source**（送信元）タブで、**Source Zone**（送信元ゾーン）に trust を追加します。
4. Source Address（送信元アドレス）セクションで新しい my-data グループを **Add**（追加）します。
5. **Destination**（宛先）タブで、**Destination Zone**（宛先ゾーン）に untrust を追加します。
6. **Service/URL Category**（サービス/URL カテゴリ）タブで、service（サービス）が **application-default** に設定されていることを確認します。
7. **Actions**（アクション）タブで、**Action**（アクション）を Allow（許可）に設定します。
8. Profile Settings（プロファイル設定）で、**Profile Type**（プロファイル タイプ）を **Profiles**（プロファイル）に設定し、Antivirus（アンチ ウイルス）、Anti-Spyware（アンチ スパイウェア）、Vulnerability Protection（脆弱性防御）にデフォルトのプロファイルを関連付けます。
9. **OK**をクリックします。
10. **Commit**（コミット）をクリックします。

STEP 5 | ファイアウォール上に、ダイナミック アドレス グループのメンバーが入力されていることを確認します。

このアドレス グループに属し、ここに表示されるすべての IP アドレスについてポリシーが適用されます。

1. **Policies**（ポリシー） > **Security**（セキュリティ）を選択し、ルールを選択します。
2. ドロップダウン リストから **Inspect**（検査）を選択します。一致条件が正確であるか確認することもできます。
3. **more**（詳細）をクリックし、登録された IP アドレスのリストが表示されることを確認します。

カスタム テンプレートあるいは gcloud CLI を使用して VM-Series ファイアウォールをデプロイ

Google Cloud Platform Marketplace で公開されている VM-Series の公式イメージは、**`paloaltonetworksgcp-public`**プロジェクトで入手できます。これらのイメージを**`gcloud`**コマンドラインから呼び出す、あるいは自身で記述または修正したテンプレート内で参照する場合、イメージへの安全なパスを把握しておく必要があります。

- BYOL: vmseries-byol-*<version>*
- PAYG Bundle 1: vmseries-bundle1-*<version>*
- PAYG Bundle 2: vmseries-bundle2-*<version>*

©2023 Palo Alto Networks, Inc.

gcloud CLI を使用し、現在のイメージ名およびプロジェクトを探します：

```
gcloud compute images list --project paloaltonetworksgcp-public
--no-standard-images
NAME                  PROJECT                    FAMILY  DEPRECATED
STATUS
vmseries-bundle1-810  paloaltonetworksgcp-public
 READY
vmseries-bundle2-810  paloaltonetworksgcp-public
 READY
vmseries-byol-810     paloaltonetworksgcp-public
 READY
```

イメージのパスを確認するには、**--uri** フラグを追加します。

```
gcloud compute images list --project paloaltonetworksgcp-public
--no-standard-images --uri
```

```
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public
/global/images/vmseries-bundle1-810
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public
/global/images/vmseries-bundle2-810
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public
/global/images/vmseries-byol-810
```

たとえば、gcp-two-tier テンプレートを https://github.com/PaloAltoNetworks からダウンロードします。

テンプレートは、イメージ名（PAN-OS バージョンを含むもの）と URL パスを区別します。`two-tier-template.py`で、*image*変数は、たとえば*vmseries-byol-810*のようなイメージ名を予期しています。`vm-series-template.py`は*COMPUTE_URL_BASE*および*sourceImage*の値を使用して、パスを構築します。

©2023 Palo Alto Networks, Inc.

Panorama Plugin for GCPによるVMモニタリング

Panorama plugin for Google Cloud Platform（GCP）バージョン2.0.0により、GCPプロジェクトで認証を受け、その中にデプロイされているVM-Seriesファイアウォールおよび他のVMを監視するための、VMモニタリング設定を作成することができます。プロジェクトへの接続を確立したら、プラグインはPanoramaとGCPアセット間のIPアドレスとタグ通信を取得することができます。事前定義された属性、VM用のユーザー定義のラベル、およびユーザー定義のネットワークタグなどがタグになります（「タグの確認と作成」を参照）。

Panorama plugin for GCPは、動作中のVMから内部/外部IPアドレスを取得し、接続しているGCP VPCのVMから定期的にIPとタグのマッピングを取得します。

タグを使ってVMをダイナミックアドレスグループに編成し、次に特定のVM IPアドレスへのトラフィックを許可/拒否するセキュリティポリシールール内のタグを参照することができます。一貫してセキュリティポリシーを適用するために、ルールをVM-Seriesファイアウォールにプッシュすることができます。

- GCP向けPanorama PluginによるVMモニタリングの設定

GCP向けPanorama PluginによるVMモニタリングの設定

このトピックは、VMモニタリング用のGCPアセットの準備および必要なPanoramaエレメントの確認手順、およびPanorama plugin for Google Cloud Platform（GCP）でのVMモニタリングの設定方法について説明しています。

- VMモニタリング用のGCPアセットの設定
- タグの確認と作成
- GCP向けPanorama PluginによるVMモニタリングの設定
  - VMモニタリング設定のためのPanoramaの準備
  - VMモニタリングの設定

VMモニタリング用のGCPアセットの設定

GCP MarketplaceからデプロイしたVM-Seriesファイアウォール、オートスケーリングファイアウォールテンプレートを使ってデプロイしたファイアウォール、GCPコンソールまたはgcloudコマンドラインから作成したGCEインスタンス、またはGCP内にデプロイされているその他の仮想マシンを監視することができます。MarketplaceからPAN-OS VMをデプロイした場合、「Google Cloud PlatformへのVM-Seriesファイアウォールの設定」の説明に従って作業を行ってください。

IAMロールの確認

VMモニタリング作業用に最低でも次のアクセス許可を保有していることを確認してください。

- GCPコンソールでプロジェクトのサービスアカウントを作成して、プロジェクトの所有者または編集者のアクセス許可を与えます。

  サービスアカウントの作成を自動化することはできません。サービスアカウントを作成するためのアクセス許可がない場合、管理者に作成を依頼して、自分に適切なロールを割り当ててもらってください。

©2023 Palo Alto Networks, Inc.

- サービスアカウントの表示:読み取り専用
- Google MarketplaceからデプロイされたPAN-OS VMの表示:Compute viewer。
- インスタンスへのユーザー定義タグの割り当てプロジェクト所有者、編集者、またはインスタンス管理者.

サービスアカウントの作成

VMモニタリングを設定するためにGCP plugin for Panoramaを使用する前に、GCPコンソールを使って、GCPプロジェクト、それにデプロイされているVM-Seriesファイアウォール、Panoramaに管理させたいその他のVM、および関連するネットワークおよびサブネットワークへのアクセス権限を与えるサービスアカウントを作成する必要があります。GCP plugin for Panoramaは、Googleアセットの事前定義属性、ユーザー定義VMラベル、およびユーザー定義ネットワークタグを取得します。

各プロジェクトには、プロジェクト作成時に自動的に作成された、デフォルトのサービスアカウントがあります。VMモニタリング用に個別のサービスアカウントを作成すると、ユーザーとそのロールをきめ細かく制御することができます。プロジェクトあたり最高100件のサービスアカウントを設定できます。

STEP 1 | Google Cloud Platformコンソールで、監視するプロジェクトを選択します。

STEP 2 | **IAM & Admin** > **Service accounts**（サービスアカウント）を選択して、**+Create Service Account**（サービスアカウントの作成）を選択します。

サービスアカウント名と説明を入力して、**Create**（作成）をクリックします。

STEP 3 | ドロップダウンメニューからロールタイプを選択し、右側から適切なアクセスレベルを選択します。

たとえば、Project > Editorを選択します。サービスアカウントに対して複数のロールを選択できます。

終了したら、**Continue**（続行）をクリックします。

STEP 4 | 特定のユーザーに、このサービスアカウントにアクセスするためのアクセス許可を与えます。前のステップのロールにアクセスためのアクセス許可を与えるには、右側の**Permissions**（アクセス許可）列からメンバーを選択します。

STEP 5 | （任意）**+CREATE KEY**（キーの作成）をクリックして、VM-Seriesファイアウォール、ネットワーク、およびこのサービスアカウントに関連するその他のVMにアクセスするために、Google Cloud CLIの認証を受けるための、認証情報を作成します。

キーは自動的にダウンロードされます。キーは安全な場所に保管してください。生成された秘密鍵のJSONフォーマットは次のようになります。

```
{
  "type": "service_account",
  "project_id": "gcp-xxx",
  "private_key_id": "252e1e7a2e9c84b5d4dbb6195b1de074594b6499",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDAd0i+RMKCtrs0
\n4KHnzTAPrgoBjRgpjyNcvQmdUqHr\n-----END PRIVATE KEY-----\n",
```


©2023 Palo Alto Networks, Inc.

```
  "client_email": "dlp-vm-monit-svc-acct@gcp-
xxx.iam.gserviceaccount.com",
  "client_id": "108932514695821539229",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/
oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/
robot/v1/metadata/x509/dlp-vm-monit-svc-acct%40gcp-
xxx.iam.gserviceaccount.com"
}
```

タグの確認と作成

「タグ」とは、事前定義された属性、ユーザー定義のラベル、およびユーザー定義のネットワークタグなどを表す一般用語です。

- 事前定義タグ（属性）は、Google VM用に自動的に作成されます。VMモニタリングの設定時、8種類の事前定義属性すべてを監視する、または監視する属性のリストを作成することができます。
- VMラベルとネットワークタグ向けに、独自のタグを定義することができます。

VMやネットワークにタグを設定して、それらを識別、グループ化できるようにして、セキュリティポリシーを採用するためのルールを構築することができます。Googleプロジェクト内にデプロイされている、任意のVMにタグを設定することができます。たとえば、VM-Seriesファイアウォール、Webサーバー、アプリケーションサーバー、ロードバランサーなどにタグを設定できます。

- タグはVMと関連付ける必要があります。これは、ネットワークおよびサブネットワークの場合でも当てはまります。
- あるインスタンスに複数のIPアドレスが関連付けられている場合（たとえば、タグを設定するVM-SeriesファイアウォールにTrustおよびUntrustインターフェイスがある）、Panoramaは複数セットのタグ情報を生成します。

Panoramaプラグインが取得、登録できるタグ数の合計は、Panoramaが動作しているPAN-OSのバージョンと管理対象VM-Seriesファイアウォールのバージョンによって異なります。

ネットワークインターフェイス固有の複数のインターフェイスを持つVM上のネットワークインターフェイスにタグを設定するために、Googleゾーン、Googleリージョン、VPC名、およびSubnet（サブネット）名が用いられます。

事前定義属性

Google Cloud Platform plugin for Panoramaは、任意の管理対象VMから次の事前定義タグを取得します:

- プロジェクト**ID**—例: google.project-id.myProjectId。

  Google コンソールでプロジェクト情報を検索するには、プロジェクトを選択して、次に**IAM & Admin** > 設定を選択します。

©2023 Palo Alto Networks, Inc.

- サービスアカウント—メールアドレス形式のサービスアカウント。例: google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com。

  サービスアカウントを探すには、VMインスタンス詳細を参照してください。
- **VPC**名—管理対象VMのVPCネットワーク名。例: google.vpc-name.myvnet。
- サブネット名—管理対象VMインターフェイスに対して作成した、サブネットの名前。たとえば、VM-SeriesファイアウォールのUntrustインターフェイスに対して作成したサブネットの名前は、「google.subnet-name-untrust.web」のようになります。
- **OS SKU**—管理対象VMのデプロイ時に選択したオペレーティングシステム。例: google.os-sku.centos-7。

  *VM*がカスタムイメージを使用している場合、この属性はサポートされません。
- **Google**ゾーン—VMのデプロイ時に選択したゾーン。例: google.zone.us-east1-c。
- **Google**リージョン—選択したゾーンを含むリージョン。例: google.region.us-east1。
- インスタンスグループ名—例: google.instance-group.myInstanceGroup。Googleコンソールでインスタンスグループを表示または作成するには、**Compute Engine** > **Instance Group**（インスタンスグループ）を選択します。

ユーザー定義のラベル

Panoramaは、最大16個のユーザー定義ラベルを使用します。16個より多くのラベルがある場合、ユーザー定義のラベルがアルファベット順にソートされ、最初の16個のタグが使用されます。

ラベルのキーと値のペアについては、Googleの要件を参照してください:キーの最低長は1文字、最大長は63文字で、空にすることはできません。値は空にできます。また、最大文字数は63文字です。

GCPコンソールでラベルを作成または表示するには、**Compute Engine** > **VM Instances**（**VM**インスタンス）に移動して、**Show Info Panel**（情報パネルを表示）を選択します。1つまたは複数のVMを選択して、**Info**（情報）パネルで**Labels**（ラベル）を選択します。**+Add a label**（ラベルの追加）をクリックしてキーと値を追加し、**Save**（保存）をクリックします。

ユーザー定義のネットワークタグ

Panoramaは最大8個のユーザー定義ネットワークタグを使用します。8個より多くのタグがある場合、ユーザー定義のタグがアルファベット順にソートされ、最初の8個のタグが使用されます。

Googleはネットワークタグを次のように制限していることに注意してください。

- タグあたり最大63文字。
- 小文字、数字、およびダッシュを使用することができます。タグは小文字で開始し、数字または小文字で終了する必要があります。

GCPコンソールでネットワークタグを作成または表示するには、**Compute Engine** > **VM Instances**（**VM**インスタンス）に移動して、インスタンスを選択します。インスタンスを**Edit**（編集）し、**Network Tags**（ネットワークタグ）までスクロールしてタグを入力し（カン

 ©2023 Palo Alto Networks, Inc.

マで区切る）、最後に**Save**（保存）を選択します。「ネットワークタグの設定」を参照してください。

GCP向け**Panorama Plugin**による**VM**モニタリングの設定

GCPアセットにタグを設定して、サービスアカウントを作成したら、VMモニタリングを設定できるように、Panoramaがアセットを利用できるようにします。

VMモニタリング設定のための**Panorama**の準備

PanoramaにGCPアセットを管理、監視させるには、次の作業を行ってください。GCP内にデプロイされている任意のVMを、Panoramaの管理対象デバイスにすることができます。

STEP 1 | Panoramaで、VM-Seriesファイアウォールおよび GCPプロジェクトに関連する他のVMを、管理対象デバイスとして追加します。

STEP 2 | デバイスグループを追加して、それに管理対象デバイスを割り当てます。デバイスグループは、グループとして管理する、ファイアウォールまたは仮想システムのグループです。

> *VM*がメンバーになれるデバイスグループは*1*つのみです。デバイスグループは入念にプランニングしてください。

STEP 3 | テンプレートを追加します。テンプレートに名前を付け、デフォルトVPCを受け入れます。

STEP 4 | テンプレートスタックを追加します。スタックを**Add**（追加）し、作成したテンプレートを**Add**（追加）して、デバイスを選択します。

STEP 5 | 変更をコミットします。

VMモニタリングの設定

STEP 1 | まだ作業を行ってない場合は、Panorama Plugin for GCPのインストールを行います。

STEP 2 | Panorama Web インターフェイスにログインして、**Panorama** > **Google Cloud Platform**の順に選択します。

©2023 Palo Alto Networks, Inc.

STEP 3 | VMモニタリングを設定します。

1. 一般設定を行います。

   1. **Panorama** > **Google Cloud Platform** > **Setup**（セットアップ） > **General**（全般）を選択します。設定を編集するには、歯車をクリックします。

      - サービスアカウントを設定したすべてのプロジェクトのVMモニタリングを許可するには、**Enable Monitoring**（モニタリングを有効にする）を選択します。
      - **Monitoring Interval**（モニタリング間隔）を秒単位で入力します。これは、各タグ取得イベント間の時間間隔になります。

2. 通知グループを追加します。通知グループは、PanoramaがIPアドレスとタグのマッピングおよびアップデートをプッシュ配信する、デバイスグループのリストです。

   *1*つのプロジェクトに対して、*1*つの通知グループのみを保有できます。

   1. **Panorama** > **Google Cloud Platform** > **Setup**（セットアップ） > **Notify Groups**（通知グループ）を選択して、**Add**（追加）をクリックします。
   2. Panoramaが取得したVM情報（IPアドレスとタグのマッピング）のプッシュ先にするファイアウォールのグループを示す **Name**（名前）を入力します。
   3. Panoramaがプロジェクトから取得したVM情報（IPアドレスとタグのマッピング）をプッシュ配信する、**Device Groups**（デバイスグループ）を選択します。VM-Seriesファイアウォールはアップデートを使用して、セキュリティポリシーで参照しているダイナミックアドレスグループの、現在のメンバー リストを決定します。

      デバイスグループは入念にプランニングしてください。

   4. 事前定義タグまたはカスタムタグを選択します。

      - **Select All 8 Predefined Tags**（8種類の事前定義タグすべてを選択）—すべての事前定義属性（タグ）を選択する場合に、このオプションを使用します。
      - **Custom Tags**（カスタムタグ）—事前定義属性、ユーザー定義ラベル、およびユーザー定義ネットワークタグのタグリストを作成する場合に、このオプションを選択します。

   5. - 単一の通知グループ内に、関連するすべてのデバイスグループを含めるようにしてください。
      - 通知グループに含まれるファイアウォールに Panorama がプッシュしたタグを登録解除する場合、モニタリング定義を削除する必要があります。
      - 複数の仮想システムで有効なファイアウォール上のすべての仮想システムにタグを登録するためには、各仮想システムを Panorama 上の別のデバイスグループに追加し、デバイスグループを通知グループに割り当てる必要があります。すべて

©2023 Palo Alto Networks, Inc.

の仮想システムを単一のデバイスグループに割り当てる場合、Panorama はタグを単一の仮想システムにのみ登録します。

3. GCPサービスアカウント認証情報を**Add**（追加）します。
   - GCPサービスアカウント認証情報の名前を指定します。
   - （任意）サービスアカウントの説明を入力します。
   - **Browse**（参照）を選択して、サービスアカウントの作成時に生成されたJSONファイルをアップロードします。

   *Panorama Web*インターフェイスを使用する必要があります。*CLI*を使ってサービスアカウントを追加することはできません。

   *1*つの認証情報に対してのみ、サービスアカウントを使用することができます。単一の*JSON*ファイルから、複数の認証情報を作成しないでください。

サービスアカウント認証情報を追加したら、Panoramaコマンドラインから認証情報を検証することができます:

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 4 | **Monitoring Definition**（モニタリング定義）を作成します。

モニタリング定義は、プロジェクトのサービスアカウント認証情報と通知グループから構成されています。プロジェクト内のすべてのネットワーキングプロジェクトが監視され、取得されたタグはモニタリング定義に記載しているデバイスグループにプッシュ配信されます。新しいモニタリング定義を追加すると、デフォルトでそれは有効になります。

プロジェクトはモニタリング定義を*1*つのみ保有でき、モニタリング定義には*1*つの通知グループのみを含めることができます。

1. **Panorama** > **Google Cloud Platform** > **Monitoring Definition**（モニタリング定義）を選択して、Add（追加）をクリックします。
2. モニタリング定義の**Name**（名前）を指定します。
3. 必要に応じてモニタリング対象のプロジェクトやアセットの**Description**（説明）を入力します。
4. 前のステップで作成した、**Service Account**（サービスアカウント）認証情報を選択します。
5. **Notify Group**（通知グループ）を選択します。
6. このサービスアカウントに関連するエレメントのモニタリングを**Enable**（有効）にします。

©2023 Palo Alto Networks, Inc.

STEP 5 | Panorama 上の変更を**Commit**（コミット）します。

モニタリング定義のステータスが Success（成功）と表示されることを確認します。失敗する場合、プロジェクトIDを正しく入力し、サービスの正しいキーおよびIDを指定しているかどうか確認してください。

STEP 6 | Panorama 上で VM 情報を閲覧できることを確認し、ダイナミック アドレス グループ用の一致条件を定義します。

HAフェイルオーバーの際、新たにアクティブになった Panorama がGoogle Cloud Platformに再接続してすべてのモニタリング定義のタグを取得しようと試みます。単一のモニタリング定義に再接続する際にもエラーが発生する場合、Panoramaはシステムログのメッセージを生成します:

```
Unable to process subscriptions after HA switch-over; user-
intervention required.
```

このエラーが表示される場合は、Panoramaで問題を修正してください。たとえば、無効なサブスクリプションを削除する、または有効な認証情報を指定して、変更をコミットし、Panoramaが再接続してすべてのモニタリング定義を取得できるようにする必要があります。

*Panorama*が*Google Cloud Platform*に接続されていない状態でも、ファイアウォールはフェイルオーバー前に取得していたすべてのタグのリストを保持しており、その*IP*アドレスのリストに対して継続してポリシーを適用できます。モニタリング定義を削除する場合、登録されている*VM*に関連するすべてのタグが削除されます。ベストプラクティスとして、アクション中心のHTTPS 宛先へのログ転送を設定して即座に対応できるようにしてください。

©2023 Palo Alto Networks, Inc.

Google Cloud Platform 上の VM-Series ファイアウォールのオートスケーリング

Panorama plugin for Google Cloud Platform（GCP）バージョン2.0.0は、GCPへのVM-Seriesファイアウォールのデプロイを支援し、またGCP内のVMモニタリングまたはオートスケーリングデプロイ環境を保護しているVM-SeriesファイアウォールのPanoramaによる管理を可能にします。Panorama を使用してポリシーとファイアウォールを中央管理すると、ファイアウォールの分散ネットワークを効率的に管理および維持できます。

GCP管理対象インスタンスグループを管理しているPanoramaにより、ネットワークを保護、制御するアプリケーション有効化ポリシーを作成することができます。

オートスケーリングデプロイは、共有VPCネットワーク設定またはVPCネットワークピアリングを使用して、ホストプロジェクトが共有VPCネットワークとVM-Seriesファイアウォールを含み、サービスプロジェクトがVMベースまたはコンテナベースのアプリケーションデプロイ（Kubernetesクラスタ）を含んでいる、共通のVPCネットワークの作成をサポートしています。Palo Alto networks は、VM-Series ファイアウォールをホストプロジェクトに展開し、オプションのサンプルアプリケーションをサービスプロジェクトに展開するためのテンプレートを提供しています。

VM-Seriesファイアウォールに対しては、BYOLおよびPAYGライセンスを使用することができます。ライセンス期間中、VM-SeriesファイアウォールインスタンスはPalo Alto Networksライセンスサーバーと直接対話します。

BYOLを選択した場合、デプロイ環境ではスケールダウンイベントに応じて、ライセンスのインスタンスを無効にすることができます。VM-Seriesファイアウォールのデプロイ情報がPanorama plugin for GCP内に設定されており、ファイアウォールが自動的に削除された場合、Panoramaはファイアウォールのステータスを検出して、そのファイアウォールの登録を自動的に解除します。

- Google Cloud Platform用のオートスケーリングコンポーネント
- GCPオート スケーリングテンプレートのデプロイ

Google Cloud Platform用のオートスケーリングコンポーネント

一般的にGCPオートスケーリングデプロイでは、ホストプロジェクトとサービスプロジェクトを使用して、相互間の共通VPCネットワークを形成します。GCP用Panoramaプラグインは、ホストおよびサービスVPCを使用して、またはホストプロジェクトにVM-Seriesファイアウォールと共有VPCネットワークが含まれており、サービスプロジェクトにアプリケーションデプロイ環境が含まれている共有VPCまたはピアリングVPCネットワーク設定内のホスト/サービスプロジェクトを使用して、単一プロジェクト内のオートスケーリングデプロイ環境を保護することができます。アプリケーションがKubernetesクラスタにデプロイされている場合はピアリングVPCが必要になります。

- オートスケーリングの要件
- Auto Scaling（オートスケーリング）テンプレートのデプロイ準備

©2023 Palo Alto Networks, Inc.

オートスケーリングの要件

- 一般要件—ご自分の環境が、基要件を満たしていることを確認します。
- **GCP用Panorama**プラグイン—まだ作業を行っていない場合はPanorama Plugin for GCPのインストールを行います。

  以前に*GCP用Panorama*バージョン*1.0.0*をインストールしている場合、*2.0.X*をインストールする前にそれを削除してください。アップグレードすることはできません。

- **Palo Alto Networks Auto Scale**テンプレートバージョン**1.0**—Palo Alto Networksは、ホストプロジェクトにVM-Seriesファイアウォールをデプロイし、サービスプロジェクトにサンプルアプリケーションを設定、デプロイするためのテンプレートを提供しています。テンプレートの詳細は、オートスケーリングテンプレートについて」を参照してください。

  テンプレートをGitHub からダウンロードします。このzipファイルには、ファイアウォールおよびアプリケーション向けの個別のzipファイルが含まれています。

Auto Scaling（オートスケーリング）テンプレートのデプロイ準備

オートスケーリングテンプレートをデプロイする前に、以下のタスクを完了してください。

- ホストプロジェクトの準備と必要なサービスアカウント
- ライセンスAPIキーの取得
- 安全なオートスケーリングデプロイのための、GCP用Panoramaプラグインの設定
- オートスケーリングのためのVM-Seriesファイアウォールブートストラップパッケージの準備

ホストプロジェクトの準備と必要なサービスアカウント

ファイアウォールおよびアプリケーションテンプレートをサポートする共有VPCトポロジを形成するには、ホストプロジェクトとサービスプロジェクトが必要です。新しいホストプロジェクトを作成する、または既存のプロジェクトをホストとして動作するように準備することができます。

共有VPCをセットアップするために、組織管理者はホストプロジェクトの管理者にShared VPC Adminロールを許可する必要があります。Shared VPC Admin（共有VPC管理者）は、プロジェクトのホストとしての動作有効にして、Service Project Admin（サービスプロジェクト管理者）ロールをサービスプロジェクト管理者に与えることができます。GCPドキュメントのAdministratorsおよびIAMロールに関するドキュメントを参照してください。

STEP 1 | GCPコンソールで、ホストとして動作するようにGCPプロジェクトを作成します。既存のプロジェクトを使用したい場合は、次のステップに進んでください。

新しいプロジェクトを作成するには、組織を選択するか、また**No organization**（組織なし）を選択し**New Project**（新しいプロジェクト）をクリックしてプロジェクトに関する情

©2023 Palo Alto Networks, Inc.

報を入力します。プロジェクトIDはこの時点での**EDIT**（編集）できることに注意してください。



*CLI*からホストプロジェクトを認証できるように、*Google Cloud SDK*インストールして、設定しておく必要があります。ファイアウォールテンプレートおよびアプリケーションテンプレートのデプロイ、およびホストプロジェクトへのサービスプロジェクトへのアタッチにはコマンドラインインターフェイスを使用します。

STEP 2 | オートスケーリングに必要なAPIとサービスを有効にします。必要なAPIを以下に示します。

- Cloud Pub/Sub API
- Cloud Deployment Manager API
- Cloud Storage API
- Compute Engine API
- Google Compute Engine Instance Group Manager API
- Google Compute Engine Instance Group Updater API
- Google Compute Engine Instance Groups API
- Kubernetes Engine API
- Stackdriver API
- Stackdriver Logging API
- Stackdriver Monitoring API

以下に示すようにGCPコンソールまたGCP CLIから、APIを有効にすることができます。

GCPコンソールから**API**を有効にする

1. ホストプロジェクトを選択して、Navigation（ナビゲーション）メニューから**APIs & Services**（**API**とサービス）を選択します。
2. 必要な各APIを検索、表示します。
3. 「API enabled（API有効）」ステータスが表示されていない任意のAPI**ENABLE**（有効）にします。

CLIから**API**を有効にする

1. CLIから設定を表示して、正しいプロジェクトを使用していることを確認します。

```
gcloud config list
```

間違っている場合は、次のように目的のプロジェクトを設定します。

```
gcloud config set project <project-name
```

2. 次のコマンドを発行して、必要なAPIを有効にします。

```
gcloud services enable pubsub.googleapis.com
gcloud services enable deploymentmanager.googleapis.com
```


©2023 Palo Alto Networks, Inc.

```
gcloud services enable storage-component.googleapis.com
gcloud services enable compute.googleapis.com
gcloud services enable replicapool.googleapis.com
gcloud services enable replicapoolupdater.googleapis.com
gcloud services enable resourceviews.googleapis.com
gcloud services enable container.googleapis.com
gcloud services enable stackdriver.googleapis.com
gcloud services enable logging.googleapis.com
gcloud services enable monitoring.googleapis.com
```

3. 必要なAPIが有効になっていることを確認します。

```
gcloud services list --enabled
```

STEP 3 | VM-Seriesファイアウォールのデプロイするためのサービスアカウントを作成し、サービスまたはKubernetesクラスタのオートスケーリングに必要なIAMロールを割り当てます。

ファイアウォールテンプレートの設定時、VM-Seriesファイアウォール`.yaml`ファイルに、このサービスアカウントのメールアドレスを追加します。ホストプロジェクト内で、テンプレートはこのサービスアカウントの認証情報を使用して、サブネットを持つホストVPCの

©2023 Palo Alto Networks, Inc.

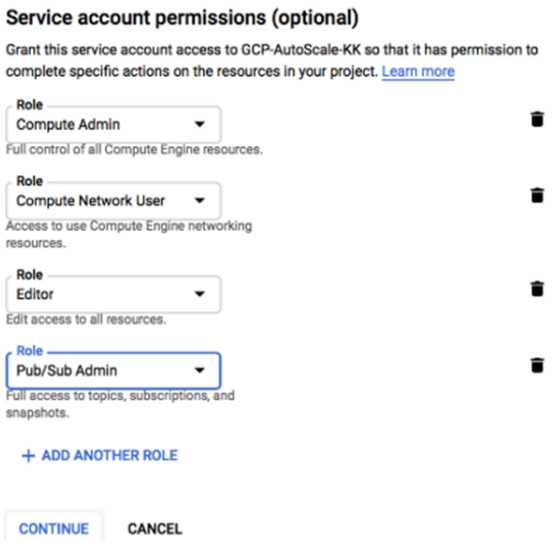
作成、VPCへのVM-Seriesファイアウォールのデプロイ、Stackdriverカスタム測定基準の設定、Pub/Subトピックの作成などが行われます。

1. GCPコンソールで**IAM & Admin** > **Service accounts**（サービスアカウント）を選択して**+CREATE SERVICE ACCOUNT**（サービスアカウントの作成）を選択します。

   サービスアカウントの詳細を記入して**CREATE**（作成）をクリックします。
2. このプロジェクト内のリソースのオートスケーリングに対して、サービスアカウントアクセス許可を割り当てます。

   ドロップダウンメニューからロールタイプを選択し、右側から適切なアクセスレベルを選択します。たとえば、Project Editorを選択します。サービスアカウントに対して複数のロールを選択できます。

   - Compute Engine Compute Admin
   - Compute Engine Compute Network User
   - +Pub/Sub Admin
   - Monitoring Monitoring Metric Writer
   - Stackdriver Stackdriver Accounts Editor
   - Storage Storage Admin
   - （GKEのみ）Kubernetes Kubernetes Engine Cluster Admin
   - （GKEのみ）Kubernetes Kubernetes Engine Viewer

   ロールの追加が完了したら**Continue**（続行）を選択します。
3. **+CREATE KEY**（キーの作成）をクリックして、ホストサービスアカウントのキーを作成します。

   - （任意）このサービスアカウントへの、他のユーザーまたは管理者によるアクセスを許可する場合、そのメールアドレスを追加します。
   - JSON形式で秘密鍵をダウンロードする場合は、JSONをクリックします。
   - 鍵を安全な場所に保管しますGCPオート スケーリングテンプレートのデプロイを行う場合に、この鍵が必要になります。

©2023 Palo Alto Networks, Inc.

4. **DONE (完了)**をクリックします。

STEP 4 | Panorama管理者がこのホストプロジェクトとやり取りするために利用できる、サービスアカウントを作成します。

1. GCPコンソールで**IAM & Admin** > **Service accounts**（サービスアカウント）を選択して**+CREATE SERVICE ACCOUNT**（サービスアカウントの作成）を選択します。
2. サービスアカウントの詳細を記入して**CREATE**（作成）をクリックします。
3. サービスアカウントアクセスを許可します。

   ドロップダウンメニューからロールタイプを選択し、右側から適切なアクセスレベルを選択します。たとえば、Project Editorを選択します。サービスアカウントに対して複数のロールを選択できます。

   - Compute Engine Compute Viewer
   - Deployment Manager Viewer
   - +Pub/Sub Admin

   CONTINUE（続行） をクリックします。
4. **+CREATE KEY**（キーの作成）をクリックして、ホストサービスアカウントのキーを作成します。
   - （任意）このサービスアカウントへの、他のユーザーまたは管理者によるアクセスを許可する場合、そのメールアドレスを追加します。
   - JSON形式で秘密鍵をダウンロードする場合は、JSONを選択します。
   - 鍵を安全な場所に保管します安全なオートスケーリングデプロイのための、GCP用Panoramaプラグインの設定を行う場合に、この鍵が必要になります。

STEP 5 | 任意）CLIで、新しいホストプロジェクトと通信できることを確認します。

1. ご自分のプロジェクトを、作成したホストプロジェクトに設定します。

   ```
   gcloud set project <your-autoscale-host-project-name
   ```
2. オートスケーリング用の設定を作成します。アクティベーションを無効にしていない限り、新しい設定は自動的にアクティブ化されます。

   ```
   gcloud config configurations create <CONFIGURATION_NAME gcloud config list
   ```

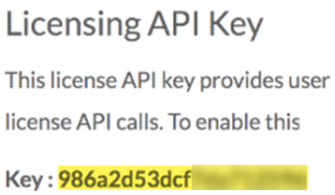
ライセンス**API**キーの取得

GCP内の管理対象アセットにPanoramaがライセンス供与、またはライセンス解除を行えるようにするには、Licensing APIキーが必要です。

©2023 Palo Alto Networks, Inc.

STEP 1 | Support portal（サポートポータル）にログインして**Assets**（アセット） > **Licensing API**（ライセンス**API**）を選択して**Enable**（有効化）をクリックします。キーが表示されます。

このキーを生成するための*Enable*（有効）リンクは、*Super User*（スーパーユーザー）のみが表示できます。Licensing APIキーの有効化、再生成、拡張方法」を参照してください。



STEP 2 | キーを選択して、それをコピーします。

STEP 3 | CLIから、SSHでPanoramaにログインして、次のコマンドを発行します。ここで、<keyは、サポートポータルでコピーしたAPIキーに置き換えてください:

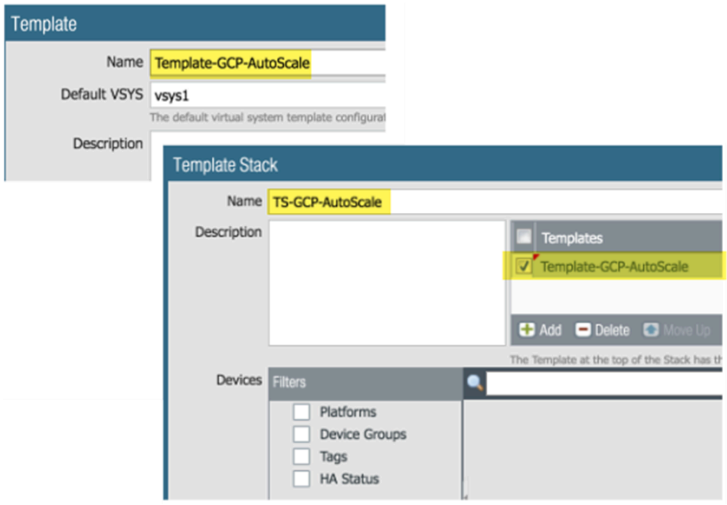
```
request license api-key set key <key
```

```
API Key is successfully set
```

安全なオートスケーリングデプロイのための、**GCP**用**Panorama**プラグインの設定

Panoramaで、オートスケーリングファイアウォールデプロイを支援するためのアセットを作成します。

STEP 1 | テンプレートを作成して、テンプレートを含テンプレートスタックを作成し、変更内容**Commit**（コミット）します。

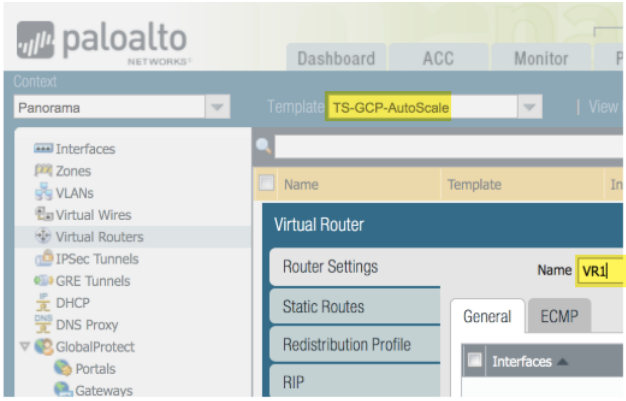


 ©2023 Palo Alto Networks, Inc.

STEP 2 | **Network**（ネットワーク）コンテキストで、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**Virtual Routers**（仮想ルーター） を選択し、仮想ルーター**Add**（追加）します。

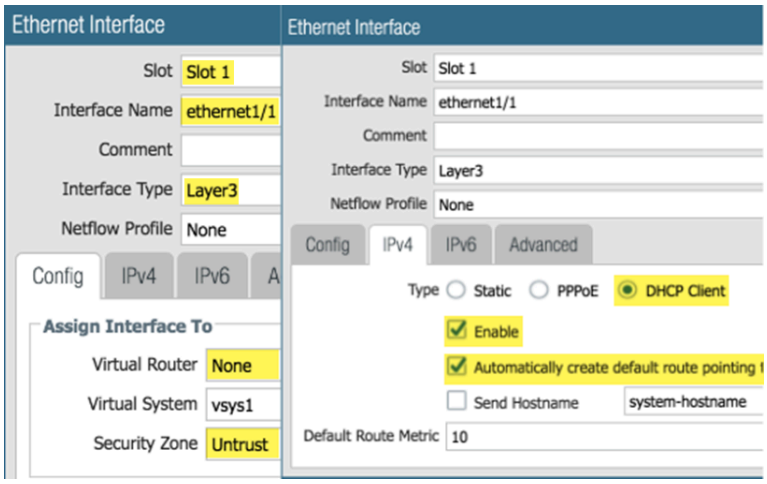
ファイアウォールテンプレートがスタティックルートを作成した時に、それがこの仮想ルーターに追加されます。

オートスケールデプロイ用ルーターは、*1*つのみ定義してください。



STEP 3 | **Network**（ネットワーク）コンテキストで、作成したテンプレートを選択し**Interfaces**（インターフェイス）を選択して**Add Interface**（インターフェイスの追加）を選択します。

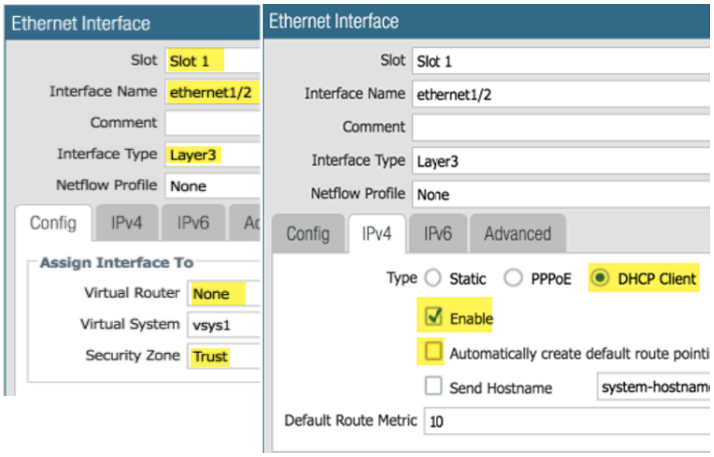
- Config（設定）タブで、スロットを選択し**Interface name**（インターフェイス名）を選択して、Layer3**Interface Type**（インターフェイスタイプ）を選択します**Security Zone**（セキュリティ ゾーン）メニューから**New Zone**（新しいゾーン）を選択して、ゾーンをUntrust に設定し**OK**をクリックします。
- **IPv4**タブ**DHCP Client**（**DHCP**クライアント）および**Automatically create default route pointing to default gateway provided by server**（サーバーが提供する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）（デフォルトで有効）を有効にして**OK**をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 4 | ethernet1/2（Trust） Layer 3インターフェイスを追加します。

- Config（設定）タブで、前のステップと同じスロットを選択し**Interface name**（インターフェイス名）（ethernet1/2）、Layer3**Interface Type**（インターフェイスタイプ）を選択します**Security Zone**（セキュリティ ゾーン）メニューから**New Zone**（新しいゾーン）を選択して、ゾーンをTrust に設定し**OK**をクリックします。
- **IPv4**タブ**DHCP Client**（**DHCP**クライアント）を有効にして**Automatically create default route pointing to default gateway provided by server**（サーバーが提供する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する）を無効にして**OK**をクリックします。



STEP 5 | テンプレートスタックおよび先ほど作成した仮想ルーターに戻ります。仮想ルーターにUntrustおよびTrustインターフェイス（ethernet1/1およびethernet1/2）を配置して**OK**をクリックします。

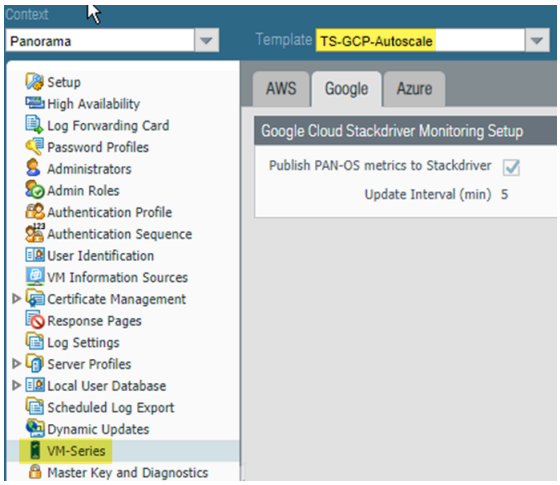


©2023 Palo Alto Networks, Inc.

STEP 6 | オートスケーリングデプロイ環境用のStackdriverを設定します。

Stackdriverを設定するにはPanorama上にVM-Seriesプラグインが必要になります。

1. **Device**（デバイス）コンテキストで、先ほどTemplate（テンプレート）ドロップダウンメニューから作成したテンプレートスタックを選択します。
2. **Device**（デバイス） > **VM-Series** > **Google**を選択して、Edit cog）をクリックしますPublish PAN-OS metrics to Stackdriver（PAN-OS のメトリックを Stackdriver にパブリッシュ）を有効にします。



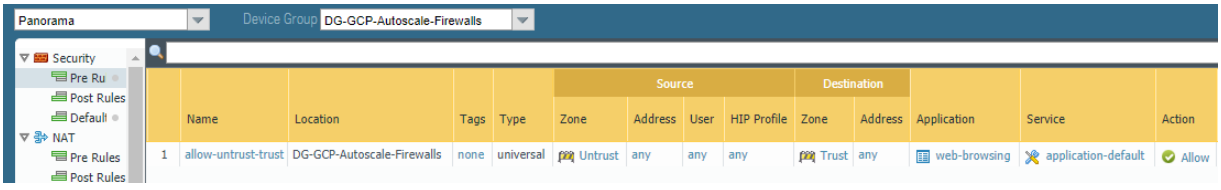
3. 変更をコミットします。

STEP 7 | ステッ1で作成したテンプレートまたはテンプレートスタックを参照する、デバイスグループを作成します。

このデバイスグループには、ファイアウォールテンプレートで作成したVM-Seriesファイアウォールが含まれます。

1. UntrustからTrustへのWebブラウジングトラフィックを許可するセキュリティポリシーを追加します。

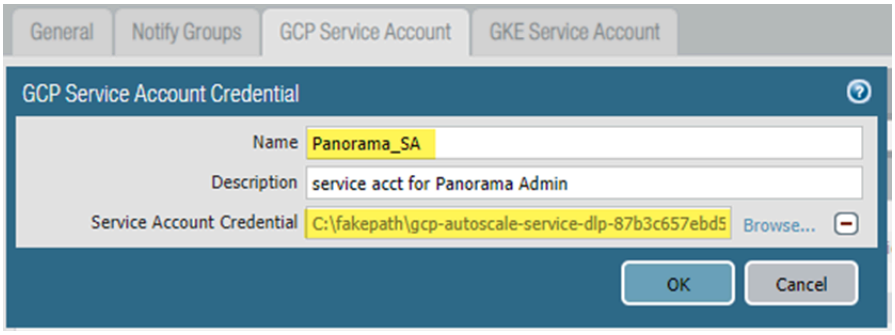
   Policies（ポリシー）コンテキストで、先ほど作成したデバイスグループを選択しますSecurity（セキュリティ） > **Pre Rules**（プレルール） を選択して、次のセキュリティ ポリシーを**Add**（追加）します。



©2023 Palo Alto Networks, Inc.

STEP 8 | ホストプロジェクトのGCPサービスアカウントを設定します。

1. Panoramaコンテキストで、Google Cloud Platformを展開し**Setup**（セットアップ）を選択し**Add**（追加）をクリックします。
2. ステッ4で作成したホストサービスアカウントの名前と説明を指定します。
3. ステッ44で作成したJSON認証情報ファイルをアップロードします。

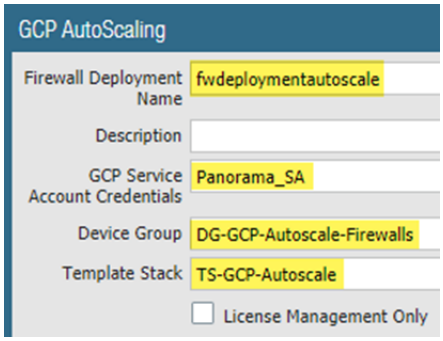


サービスアカウント認証情報を追加したら、Panoramaコマンドラインから認証情報を検証することができます（Webインターフェイスからは検証できません）：

```
request plugins gcp validate-service-account
 gcp_service_account <svc-acct-credential-name
```

STEP 9 | Panorama Plugin for GCPのオートスケーリングの設定

1. Panoramaコンテキストで、Google Cloud Platformを展開してAutoScaling（オートスケーリング）を選択し**Add**（追加）をクリックします。
2. Firewall Deployment Name（ファイアウォールデプロイ名）および必要に応じてデプロイの説明を入力します。
3. GCP Service Account Credential（GCPサービスアカウント認証情報）の場合、ステッ8からのGCPサービスアカウント名を入力します。



4. ステッ7で作成したデバイスグループ、およびステッ1で作成したテンプレートスタックを選択します。
5. トラフィックを保護するために**License Management Only**（ライセンス管理のみ）を無効にします。

STEP 10 | 変更をコミットします。

©2023 Palo Alto Networks, Inc.

オートスケーリングのための**VM-Series**ファイアウォールブートストラップパッケージの準備

ブートストラップ中、ファイアウォールからの初期リクエストがホストIPアドレスとシリアル番号、およびVM認証キーを提供されまるため、PanoramaがVM認証キーを検証し、ファイアウォールを管理デバイスとして追加します。その後、Panorama は適切なデバイス グループとテンプレートにファイアウォールを割り当て、Panorama を使ってファイアウォールを集中的に設定、管理することができます。

この場合、PanoramaでVM認証キーを生成し、そのキーをブートストラップに使用するinit-cfg.txtファイルに組み込む必要があります。VM認証キーにより、Panoramaが新しくブートストラップされたVM-Series ファイアウォールを認証することができるようになります。ブートストラップパッケージには次の項目を含める必要があります。

- /configディレクトリに、Panorama IPアドレスを含むinit-cfg.txtファイル
- /licenseディレクトリに、名前がauthcodesのファイルにVM認証キー

  キーの有効期限は1時間から8760時間（1年）の間のいずれかです。指定した期間が過ぎるとキーが失効し、Panoramaはこの接続リクエストの際に有効な認証キーが無いためにVM-Seriesファイアウォールを登録しなくなります。

STEP 1 | Google Cloud Platform上でVM-Seriesファイアウォールをブートストラップするために必要なフォルダを使ってGoogleストレージバケットを設定します。これらのフォルダに対して、既存のブートストラップパッケージを使用する、または新しいブートストラップパッケージを作成することができます。

STEP 2 | サンプル**`init-cfg.txt`**ファイル内の値を編集して、ご利用の環境向けのファイルをカスタマイズします。

ファイアウォールテンプレートには、サンプル**`init-cfg.txt`**ファイルが含まれています。

パラメータ	Value（値）	コメント
type	dhcp-client	
hostname	<pa-vm	ホストプロジェクトの準備時に割り当てたオプション名。特定のホストが必須で、dhcp-send-hostnameがnoの場合にのみ必要になります。
vm-auth-key	<vmauthkey	Panoramaがファイアウォールを管理対象デバイスとして追加する前に、Panoramaが検証する必要があるキー「Panorama で VM 認証キーを作成する」を参照してください。

©2023 Palo Alto Networks, Inc.

パラメータ	Value（値）	コメント
panorama-server	<panorama-ip	安全なオートスケーリングデプロイのための、GCP用Panoramaプラグインの設定」で設定した、Panorama管理デバイスのIPアドレス。
tplname	<template-stack-name	安全なオートスケーリングデプロイのための、GCP用Panoramaプラグインの設定」で作成したテンプレートスタック。
dgname	<dg-name	Panorama Plugin for GCPで作成したデバイスグループの名前。
dns-primary		ご自分のプライマリDNSサーバー。
dns-secondary		ご自分のセカンダリ DNS サーバー。
dhcp-send-hostname	yes	そのままにしてください。
dhcp-send-client-id	yes	そのままにしてください。
dhcp-accept-server-hostname	yes	そのままにしてください。
dhcp-accept-server-domain	yes	そのままにしてください。

STEP 3 | 編集し`init-cfg.txt`ファイルを、ブートストラップパッケージ`/config`フォルダにアップロードします。

STEP 4 | BYOLを使用している場合`authcodes`と言う名前のテキストファイルを作成し（拡張子なし）、認証コードを追加して、そのファイル`/license`フォルダにアップロードします。

GCPオート スケーリングテンプレートのデプロイ

- オートスケーリングテンプレートについて
- ファイアウォール テンプレートのデプロイ
- サービスプロジェクトの準備
- 共有VPCの設定
- アプリケーションテンプレートのデプロイ

©2023 Palo Alto Networks, Inc.

- 新しいアプリケーションのオンボーディング
- GKEサービステンプレートのサンプル

オートスケーリングテンプレートについて

https://github.com/PaloAltoNetworks/GCP-AutoScalingから、Palo Alto Networksオートスケーリングテンプレートをダウンロードします。このzipファイルには、ファイアウォールおよびアプリケーション向けの個別のzipが含まれています。各zipは、さまざまなファイルを含んでいるテンプレートディレクトリですが、必要なのはYAMLファイルを編集することだけです。

- ファイアウォールテンプレート
- アプリケーションテンプレート

ファイアウォールテンプレート

ファイアウォールディレクトリファイルは、VM-Seriesファイアウォールおよびその他のデプロイリソースを作成します。これは、VM-Seriesファイアウォールの管理、Untrust、Trust向けに、新しいネットワークとサブネットワークを作成します。GCPからPanorama plugin for GCPに情報をリレーするために、Cloud Pub/SubCloud Pub/Subメッセージングサービスもデプロイします。このインフラにより、プラグインはダイナミックアドレスグループを活用して、GCP上で動作しているサービスにルーティングされるインバウンドトラフィックにセキュリティポリシーを適用でき、またオートスケーリングメトリクスを利用して、アプリケーションワークロードリソース需要の増加に対応するためにVM-Seriesファイアウォールをデプロイしたり、不要なファイアウォールを削除したりすることができます。

ロードバランサーを設定するには、外部アプリケーションロードバランサー（ALB）またはネットワークロードバランサー（NLB）の、`.yaml`ファイルを編集します。

- **ALB**（HTTP外部ロードバランサー）

  ALBをカスタマイズするには、`vm-series-fw-alb.yaml`を編集します。

  HTTP外部ロードバランサーは、プロキシベースのロードバランサーで、インターネットからのインバウンド トラフィックにSNATおよびDNATを実施します。HTTPロードバランサーは、TCPポート80および8080のみをサポートするように設計されています。

  ロードバランサーサンドイッチアーキテクチャで、HTTPロードバランサーを使って複数のアプリケーションをサポートするために、GCP HTTPロードバランサー*urlMap*および*namedPort*を使って、異なるURLをロードバランサー内の異なるポートにマップすることができます。その後、VM-Seriesファイアウォールはポートを別のアプリケーションに変換することができます。それぞれが、アプリケーションあたり1つの内部ロードバランサーで表されています。

©2023 Palo Alto Networks, Inc.

- **NLB**（TCPロードバランサー）

  NLBをカスタマイズするには、`vm-series-fw-nlb.yaml`を編集します。

  TCPロードバランサーは、非プロキシベースのロードバランサーです。つまり、インターネットからのインバウンド トラフィックに対してNATは実施しません。

  GCP内のTCPロードバランサーにより、任意のポートを持つ複数のフロントエンドIPアドレスを追加して、複数のアプリケーションをサポートすることができます。

  また、TCPロードバランサーには、一部のアプリケーションでは無効になる、オリジナルのクライアントIPアドレスが保持される利点もあります。

アプリケーションテンプレート

アプリケーションディレクトリは、サンプルのアプリケーションを提供しています。内部ロードバランサー（ILB）を設定、デプロイして、アプリケーションサーバーのPub/Subサービスへの登録、およびVM-SeriesファイアウォールとGCP plugin for Panoramaとの通信を有効にすることができます。

アプリケーションテンプレートをカスタマイズするには、「ファイアウォール テンプレートのデプロイ」および「アプリケーションテンプレート」の説明に従って`apps.yaml`を編集します。

ファイアウォール テンプレートのデプロイ

ホストプロジェクトからファイアウォールテンプレートを編集します。

STEP 1 | ご自分のクラウド環境を反映するように、`vm-series-fw-nlb.yaml`または`vm-series-fw-alb.yaml`環境変数を編集します。

このワークフローにあるサンプルは、NLBを対象にしています。テンプレートパラメータの詳細については、「vm-series-fw-nlb.yaml」または「vm-series-fw-alb.yaml」を参照してください。

```
properties:
    region: us-east1
    zones:
    -us-east1-b
    # Do not modify the lb-type field.
    lb-type: nlb
    cloud-nat: yes
    forwarding-rule-port: 80
```

```
# Only one app is allowed
    urlPath-namedPort-maps:
    - appName: app1
```

```
# ssh key PUBLIC:
```


©2023 Palo Alto Networks, Inc.

```
    - optional
```

オートスケーリングファイアウォールテンプレートでは、単一引用符で囲んで値を入力する必要があります。また、キーの前には「**admin:**」を指定して、後にはスペースを指定する必要があります。これは、「SSH キーペア」で説明しているGoogle Marketplaceテンプレートの構文と同じです。以下に例を示します。

```
    sshkey: 'admin: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDe0gJHd8okxPGWXsmdTdcZBJNI6ONT/NSz6INs2CNtKW
[redacted]
oTKXL8t0SRnOKaKV73NR5KnfpsNfwGxG8aQtEkeMCZIxX+6WOnRf/N4K3
yourname@[redacted].paloaltonetworks.local'
```

```
    bootstrap-bucket: bootstrap-autoscale
```

```
    image: vmseries-byol-814
    machine-type: n1-standard-4
```

service-accountに対して、先ほど作成した（ステップ3）ホストプロジェクトサービスアカウントの、メールアドレスを指定します。

```
     service-account: sa-pan@gcp-autoscale-
kk.iam.gserviceaccount.com
```

fw-instance-tagの値は、デプロイ環境内の管理対象インスタンスグループ名になります。

```
     fw-instance-tag: vm-series-fw
```

オートスケーリング用にメトリックを1つ選択します。値としては、panSessionActive、panSessionUtilization、DataPlaneCPUUtilizationPct、DataPlanePacketBufferUtilizatioまたはpanSessionUtilizationを利用できます。

```
metric: custom.googleapis.com/VMSeries/panSessionActive
```

```
max-size: 2
min-size: 1
target-type: GAUGE
util-target: 100
```

```
# Greenfield deployment
mgmt-network-cidr: 172.22.2.0/24
untrust-network-cidr: 172.22.1.0/24
trust-network-cidr: 172.22.3.0/24
mgmt-network-access-source-range:
- 199.167.54.229/32
```


©2023 Palo Alto Networks, Inc.

```
- 199.167.52.5/32
mgmt-network-access-ports:
- 22
- 443
```

STEP 2 | ファイアウォール テンプレートのデプロイ

```
gcloud deployment-manager deployments create <your-template>
--config apps.yaml
--automatic-rollback-on-error
```

デプロイ後にCLIが出力した、サブネット名、デプロイ名、Panorama Pub/Subトピック名などの出力を書き留めておきます。これらの値は、アプリケーションテンプレートデプロイの共有VPCを設定する場合に必要になります。

ファイアウォールデプロイ名は、Panorama plugin for GCPのオートスケーリング定義内に設定する必要があります。

サービスプロジェクトの準備

アプリケーションに対する個別のサービスプロジェクトを作成する、または既存のプロジェクトを選択します。

共有VPC内のホストおよびサービスプロジェクトの詳細については、「共有VPCの概要」、および「管理者およびIAMロール」を参照してください。ホストプロジェクト管理者には、共有VPCを設定して、アプリケーションプロジェクトをホストプロジェクトのサービスプロジェクトにするための、適切なロールが必要です。詳細は、「共有VPCのプロビジョニング」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 1 | GCPコンソールまたはCLIから、サービスプロジェクトAPIを有効にします。

必要なAPIを以下に示します。

- Cloud Deployment Manager API
- Cloud Pub/Sub API
- Compute Engine API

GCPコンソールから*API*を有効にする

1. サービスプロジェクトを選択して、Navigation（ナビゲーション）メニューから、**APIs & Services**（**API**とサービス）を選択します。
2. 必要な各APIを検索、表示します。
3. 「API enabled（API有効）」ステータスが表示されていない任意のAPIを**ENABLE**（有効）にします。

CLIから*API*を有効にする

1. CLIから設定を表示して、正しいプロジェクトを使用していることを確認します。

```
gcloud config list
```

間違っている場合は、次のように目的のプロジェクトを設定します。

```
gcloud config set project <project-name>
```

2. 次のコマンドを発行して、必要なAPIを有効にします。

```
gcloud services enable deploymentmanager.googleapis.com
gcloud services enable pubsub.googleapis.com
gcloud services enable compute.googleapis.com
```

3. 必要なAPIが有効になっていることを確認します。

```
gcloud services list --enabled
```

STEP 2 | アプリケーションプロジェクトを、ホストプロジェクトのサービスプロジェクトにします。

サービス/アプリケーションはプロジェクト管理者からのサービスアカウントを、次のロールを持つホストはプロジェクトのメンバーとして追加します。

- Compute Network User
- Pub/Sub Admin

STEP 3 | VPC設定を選択します。

- サービスプロジェクトがホストプロジェクト内のネットワークを共有する場合は、「共有VPCの設定」に進みます。
- サービスプロジェクトが、アプリケーションデプロイ環境に対する独自のVPCネットワークを保有している場合は、「ピアリングVPCの設定」に進みます。

©2023 Palo Alto Networks, Inc.

共有VPCの設定

ホストプロジェクト内にファイアウォールテンプレートをデプロイしたら、アプリケーションをサポートするサービスプロジェクトを設定します。共有VPC認証情報を持つ管理者は、ホストプロジェクトからこれらの作業を行います。共有VPCの観点からのホストプロジェクトとサービスプロジェクトの詳細については、「共有VPCの概要」を参照してください。

STEP 1 | ファイアウォールテンプレートのデプロイ時に作成したTrust VPCを使って、共有VPCを作成します。

ホスト（ファイアウォール）プロジェクトの共有VPCの設定:

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | ホストプロジェクトにサービス/アプリケーションプロジェクトを添付します。

gcloud compute shared-vpc associated-projects add [SERVICE_PROJECT_ID]--host-project [HOST_PROJECT_ID]

ホストプロジェクト内のすべてのサブネットではなく、特定のサブネットのみを共有するオプションを利用することができます。

STEP 3 | アプリケーションのデプロイにサンプルアプリケーションテンプレートを使用したい場合は、「アプリケーションテンプレートのデプロイ」に進んでください。

すでにアプリケーションをデプロイしており、オートスケーリングデプロイ環境内でそれを保護したい場合は、「既存のオートスケーリングへのアプリケーションの手動オンボーディング」に進みます。

GKEクラスタ内にサービスをデプロイした場合は、「共有VPC内でのGKEクラスタのオンボーディング」に進みます。

ピアリングVPCの設定

VPCネットワークピアリング接続は、2つのVPC間で確立する必要があります。VPCが2つの異なるプロジェクト内に存在している場合、両方のプロジェクト内で接続を作成する必要があります。

STEP 1 | ホストプロジェクト内で、ファイアウォールデプロイ環境のTrust VPCネットワークを、アプリケーションApplication VPCとピアリングします。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
    --network=[MY-LOCAL-NETWORK] \
    --peer-project [SERVICE-PROJECT-ID] \
    --peer-network [PEER-NETWORK-NAME] \
   [--import-custom-routes] \
   [--export-custom-routes]
```

STEP 2 | サービスプロジェクト内で、アプリケーションデプロイ環境のTrust VPCネットワークを、ファイアウォールデプロイ環境のTrust VPCネットワークとピアリングします。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
```


©2023 Palo Alto Networks, Inc.

```
    --network=[MY-LOCAL-NETWORK] \
    --peer-project [HOST-PROJECT-ID] \
    --peer-network [PEER-NETWORK-NAME] \
   [--import-custom-routes] \
    [--export-custom-routes]
```

STEP 3 | アプリケーションのデプロイにサンプルアプリケーションテンプレートを使用したい場合は、「アプリケーションテンプレートのデプロイ」に進んでください。

すでにアプリケーションをデプロイしており、オートスケーリングデプロイ環境内でそれを保護したい場合は、「既存のオートスケーリングへのアプリケーションの手動オンボーディング」に進みます。

GKEクラスタ内にサービスをデプロイした場合は、「ピアリングVPC内でのGKEクラスタのオンボーディング」に進みます。

アプリケーションテンプレートのデプロイ

サービスプロジェクト管理者は、サービスプロジェクトからアプリケーションテンプレートをデプロイします。

STEP 1 | アプリケーションをデプロイするために、個別のアプリケーションプロジェクト（サービスプロジェクト）を作成します（「サービスプロジェクトの準備」を参照）。

STEP 2 | 「apps.yaml」の説明に従って`apps.yaml`ファイルを準備します。

STEP 3 | アプリケーションテンプレートを使って新しいアプリケーションをデプロイし、名前付きポートのラベルを定義します。

```
gcloud deployment-manager deployments create <your-template>
--config apps.yaml
--automatic-rollback-on-error
```

Panorama Plugin for GCPでのオンボーディングされたアプリケーションの表示に進んで続行します。

新しいアプリケーションのオンボーディング

アプリケーションのデプロイにアプリケーションテンプレートを使用する場合、それがホストプロジェクトへの接続を処理します。「サービスプロジェクトの準備」で説明している機能を使って、サービスプロジェクト内にアプリケーションをデプロイしている場合、アプリケーションテンプレートを使ってデプロイしていないアプリケーションを保護することができます。

- 既存のオートスケーリングへのアプリケーションの手動オンボーディング
- GKEクラスタのオンボーディング

既存のオートスケーリングへのアプリケーションの手動オンボーディング

外部ロードバランサーとオートスケーリングVM-Seriesファイアウォールデプロイ環境を使ってデプロイしたアプリケーションを保護するには、次の作業を行ってください。オンボーディングする各アプリケーションに対して、アプリケーション名、名前付きポート、およびパスを指定する必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | ファイアウォールテンプレートのデプロイ時に作成された、HTTP外部ロードバランサーに、新しい名前付きポートとURLパスを追加する準備を行います。

STEP 2 | すべてのインスタンスグループの名前付きポートを、追加のサービス名とポート値で更新します。次の例では、アプリケーションapp2およびapp3をオンボーディングします。

```
gcloud compute instance-groups set-named-ports
fw-template2-fw-igm-us-east1-b
--zone us-east1-b
--named-ports=app1:80,app2:81,app3:82

gcloud compute instance-groups set-named-ports
fw-template2-fw-igm-us-east1-c
--zone us-east1-c
--named-ports=app1:80,app2:81,app3:82
```

STEP 3 | 新しいhttp-health-checkを作成します。

```
gcloud compute backend-services create fw-template2-backend-app3
--protocol="HTTP"
--port-name=app3
--http-health-checks=fw-template2-healthcheck-app3
--load-balancing-scheme="EXTERNAL"
--global
```

STEP 4 | HTTP外部ロードバランサーで作成されたport-nameを使って、新しいバックエンドサービスを作成します。

```
gcloud compute backend-services create fw-template2-backend-app3
--protocol="HTTP" --port-name=app3
--http-health-checks=fw-template2-healthcheck-app3 --load-
balancing-scheme="EXTERNAL"
--global
```

新しいバックエンドサービスが表示されているかどうかを確認します。

```
gcloud compute backend-services list
```

STEP 5 | url-mapsを編集して、新しいパスルールを追加します。以下に例を示します。

```
- paths:
    - /app3
    - /app3/*service:
    https://www.googleapis.com/compute/v1/projects/<project-name>/
global/backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```


©2023 Palo Alto Networks, Inc.

STEP 6 | VM-Seriesファイアウォールを使ってこのアプリケーションを保護するには、gcloud CLI経由でPub/Subメッセージを手動でトリガします。これにより、ファイアウォールテンプレートで作成されたトピックにメッセージが送信されます。

```
gcloud pubsub topics publish
  projects/topics/hj-asg-891ca3-gcp-pavmqa-panorama-apps-
deployment
  --attribute ilb-ip=172.22.9.34,
    app-deployment-name=hj-asg-891ca3-app1,
    ilb-port=80,
    named-port=81,
    network-cidr=172.22.9.0/24,
    fw-deployment-name=hj-asg-891ca3,
    host-project=gcp-pavmqa,
    type=ADD-APP
  --message "ADD-APP"
```

STEP 7 | Panorama Plugin for GCPでのオンボーディングされたアプリケーションの表示。

STEP 8 | （任意（）ilb-ip、ilb-port、またはnamed-portなどのアプリケーション属性を更新するには、pubsubコマンドを発行します:

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment
  --attribute ilb-ip=172.22.9.34,
    app-deployment-name=hj-asg-891ca3-app1,
    ilb-port=80,
    named-port=81,
    network-cidr=172.22.9.0/24,
    fw-deployment-name=hj-asg-891ca3,
    host-project=gcp-pavmqa,
    type=UPDATE-APP
  --message "UPDATE-APP"
```

STEP 9 | （任意）アプリケーションの保護を中止するには、次のコマンドを発行します:

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment
  --attribute ilb-ip=172.22.3.20,app-deployment-name=fw-templ-3-
app-1,
    ilb-port=80,
    named-port=80,
    fw-deployment-name=hj-asg-891ca3,
    type=DEL-APP
  --message "DEL-APP"
```

GKEクラスタのオンボーディング

プライベートGKEクラスタをオンボーディングするために、GCP plugin for Panoramaには次の情報が必要になります。

©2023 Palo Alto Networks, Inc.

- VM-Seriesファイアウォールがサービスの名前付きポート情報を入手できるように、GCPでクラスタのELBフロントエンドをGKEサービスに公開します。
- クラスタAPIサーバーのアドレス。
- クラスタがデプロイされているサービスのサービスアカウント認証情報（JSON形式）。

*GKE*クラスタ名は*24*文字未満でなければなりません。そうすることによって、ピアリング*VPC*設定内にオートスケーリングをデプロイしても、スタティックルート名は*31*文字を超えません。

- 共有VPC内でのGKEクラスタのオンボーディング
- ピアリングVPC内でのGKEクラスタのオンボーディング
- Panorama Plugin for GCPでのオンボーディングされたアプリケーションの表示
- CLIからのデプロイステータスの表示

共有*VPC*内での*GKE*クラスタのオンボーディング

GKEクラスタをオンボーディングするには、サービスプロジェクトとホストプロジェクトTrustネットワークVPCを共有する必要があります。「共有VPCの設定」を参照してください。

セキュリティ上の理由から、オートスケーリングデプロイ環境では、プライベートクラスタのみを使用してください。「プライベートクラスタの作成」を参照してください。

STEP 1 | ホストプロジェクトIDを設定します。

```
gcloud config set project [HOST_PROJECT_ID]
```

STEP 2 | （任意）クラスタのコンピュートゾーンまたはリージョンを設定します。

クラスターがゾーンの場合、次のコマンドを入力します。

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

クラスターがリージョンの場合、次のコマンドを入力します。

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | ホストプロジェクトで、Trust VPCサブネット内のセカンダリ範囲を更新します。

```
gcloud compute networks subnets update [TRUST_SUBNETWORK_NAME]
  --add-secondary-ranges
  [PODS_IP_RANGE_NAME] = [POD_RANGE_CIDR],
```


©2023 Palo Alto Networks, Inc.

```
  [SERVICE_IP_RANGE_NAME]=[SERVICE_RANGE_CIDR]
```

ポッドとサービス*IP*範囲は、次の範囲内でなければなりません:*10.0.0.0/8*、*172.16.0.0/12*、または*192.168.0.0/16*で、サブネットワーク内の既存の*IP*範囲と競合してはいけません。

STEP 4 | サービスプロジェクトで、共有VPC内にプライベートクラスタを作成します。

1. サービスプロジェクトIDを設定します。

```
gcloud config set project [SERVicE_PROJECT_ID]
```

2. 共有VPC内にプライベートクラスタを作成します。

```
gcloud container clusters create  [CLUSTER_NAME]
  --project [SERVICE_PROJECT_ID]
  --zone=[ZONE_NAME]
  --enable-ip-alias
  --enable-private-nodes
  --network projects/[HOST_PROJECT_ID]/global/networks/
[NETWORK_NAME]
  --subnetwork projects/[HOST_PROJECT_ID]/regions/
[REGION_NAME]
  /subnetworks/[TRUST_SUBNETWORK_NAME]
  --cluster-secondary-range-name=[PODS_IP_RANGE_NAME]
  --services-secondary-range-name=[SERVICE_IP_RANGE_NAME]
  --master-ipv4-cidr=[MASTER_IPV4_CIDR]
  --enable-master-authorized-networks
  --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
  [MY_MANAGEMENT_IP/32]
```

STEP 5 | 現在のクラスタコンテキストを確認します:

```
kubectl config current-context
```

STEP 6 | すべてのクラスタコンテキストを確認します:

```
kubectl config get-context
```

STEP 7 | 別のクラスタに変更します:

```
kubectl config use-context [CONTEXT_NAME]
```

GCPコンソールでクラスタを作成した場合、kubeconfigエントリを生成します:

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```


©2023 Palo Alto Networks, Inc.

STEP 8 | .yamlファイル内にクラスタロールを作成します—例:gke_cluster_role.yaml。

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRole
metadata:
  name: gke-plugin-role
rules:
  - apiGroups:
      - ""
    resources:
      - services
    verbs:
      - list
```

STEP 9 | クラスタロールを適用します。

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 10 | .yamlファイル内にクラスタロールバインディングを作成します—例:gke_cluster_role_binding.yaml。

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: gke-plugin-role-binding
subjects:
  - kind: ServiceAccount
    name: [SERVICEACCOUNT_NAME]
    namespace: default
roleRef:
  kind: ClusterRole
  name: gke-plugin-role
  apiGroup: rbac.authorization.k8s.io
```

STEP 11 | クラスタロールバインディングを適用します。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 12 | サービスアカウントを作成します。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 13 | サービスアカウントのシークレットトークンを、JSONフォーマットでエクスポートします。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME]
-o jsonpath='{.secrets[0].name}'`
```


©2023 Palo Alto Networks, Inc.

```
kubectl get secret $MY_TOKEN -o json > [FILE_NAME].json
```

STEP 14 | APIサーバーのアドレスを入手します。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 15 | Panorama plugin for GCPで、サービスアカウント情報を追加します。

Panorama > **Google Cloud Platform** > **Setup**（セットアップ）を選択します。

認証情報に名前を付けて説明を入力し、ステップ14からの**API**サーバーアドレスを入力し、**GKE** サービスアカウント認証情報に関してステップ13でエクスポートした JSON ファイルをアップロードします。

サービスアカウント認証情報を追加したら、Panoramaコマンドラインから認証情報を検証することができます（Webインターフェイスからは検証できません）:

```
request plugins gcp validate-service-account gke_service_account
 <svc-acct-credential-name>
```

STEP 16 | Panorama Plugin for GCPのオートスケーリングの設定

1. Panoramaコンテキストで、Google Cloud Platformを展開してAutoScaling（オートスケーリング）を選択し、**Add**（追加）をクリックします。
2. **Firewall Deployment Name**（ファイアウォールデプロイ名）および必要に応じてデプロイの説明を入力します。
3. **GCP** サービスアカウント認証情報の場合、ホストプロジェクトの準備と必要なサービスアカウントのステップ4で作成した GCP サービスアカウント名を入力します。
4. Panoramaプラグインの設定時に作成した、デバイスグループとテンプレートスタックを選択します。
5. トラフィックを保護するために、**License Management Only**（ライセンス管理のみ）を無効にします。
6. **GKE Cluster Name**（**GKE**クラスタ名）を正確に入力します。
7. （任意）GKEクラスタの**Description**（説明）を入力します。
8. GKEクラスタの**Network CIDR**（ネットワーク**CIDR**）を入力します。
9. GKEクラスタに対応する**GKE Service Account**（**GKE**サービスアカウント）を選択します。

STEP 17 | 変更をコミットします。

STEP 18 | （任意）「サンプルGKEサービステンプレートの使用」の説明に従ってサービステンプレートを作成、デプロイするか、またはGCPコンソールでGKEサービスをデプロイします。

©2023 Palo Alto Networks, Inc.

ピアリングVPC内でのGKEクラスタのオンボーディング

GKEクラスタをオンボーディングするには、「ピアリングVPCの設定」の説明に従って、サービスVPCを作成して、ホストはプロジェクト内のファイアウォールTrustネットワークとピアリングする必要があります。

セキュリティ上の理由から、オートスケーリングデプロイ環境では、プライベートクラスタのみを使用してください。「プライベートクラスタの作成」を参照してください。

STEP 1 | プロジェクトIDを設定します。

```
gcloud config set project [PROJECT_ID]
```

STEP 2 | クラスタのコンピュートゾーンまたはリージョンを設定します。

クラスターがゾーンの場合、次のコマンドを入力します。

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

クラスターがリージョンの場合、次のコマンドを入力します。

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | サービスプロジェクトVPCネットワークを、ポッドとサービスのセカンダリIP範囲で更新します。

```
gcloud compute networks subnets update [GKE_PEERED_VPC_SUBNETWORK]
--region=[REGION]
--add-secondary-ranges PODS_IP_RANGE_NAME=[ip cidr],
  SERVICE_IP_RANGE_NAME=[ip cidr]
```

STEP 4 | クラウドNATを有効にします。

プライベートクラスタをデプロイするために、クラウドNATが必要になります。

```
gcloud compute routers create [ROUTER_NAME]
  --network [NETWORK_NAME]
  --region [REGION_NAME]
```

```
gcloud compute routers nats create [NAT_CONFIG_NAME]
  --router-region [REGION_NAME]
  --router [ROUTER_NAME]
  --nat-all-subnet-ip-ranges
  --auto-allocate-nat-external-ip
```


©2023 Palo Alto Networks, Inc.

STEP 5 | サービスVPC内に新しいプライベートクラスタを作成します。

```
gcloud container clusters create [CLUSTER_NAME]
  --project [SERVICE_PROJECT_ID]
  --zone=[ZONE_NAME]
  --enable-ip-alias
  --network [NETWORK_NAME]
  --subnetwork [SUBNETWORK_NAME]
  --enable-private-nodes
  --cluster-secondary-range-name=[PODS_IP_RANGE_NAME]
  --services-secondary-range-name=[SERVICE_IP_RANGE_NAME]
  --master-ipv4-cidr=[MASTER_IPV4_CIDR]
  --enable-master-authorized-networks
  --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
  [MY_MANAGEMENT_IP/32]
```

STEP 6 | 現在のクラスタコンテキストを確認します:

```
kubectl config current-context
```

STEP 7 | すべてのクラスタコンテキストを確認します:

```
kubectl config get-context
```

STEP 8 | 別のクラスタに変更します:

```
kubectl config use-context [CONTEXT_NAME]
```

GCPコンソールでクラスタを作成した場合、kubeconfigエントリを生成します:

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 9 | .yamlファイル内にクラスタロールを作成します—例:gke_cluster_role.yaml。

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRole
metadata:
  name: gke-plugin-role
rules:
  - apiGroups:
      - ""
    resources:
      - services
    verbs:
      - list
```


©2023 Palo Alto Networks, Inc.

STEP 10 | クラスタロールを適用します。

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 11 | .yamlファイル内にクラスタロールバインディングを作成します—例:gke_cluster_role_binding.yaml。

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: gke-plugin-role-binding
subjects:
  - kind: ServiceAccount
    name: [SERVICEACCOUNT_NAME]
    namespace: default
roleRef:
  kind: ClusterRole
  name: gke-plugin-role
  apiGroup: rbac.authorization.k8s.io
```

STEP 12 | クラスタロールバインディングを適用します。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 13 | サービスアカウントを作成します。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 14 | サービスアカウントのシークレットトークンを、JSONフォーマットでエクスポートします。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME]
-o jsonpath='{.secrets[0].name}'`

kubectl get secret $MY_TOKEN -o json >[FILE_NAME].json
```

STEP 15 | APIサーバーのアドレスを入手します。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```


©2023 Palo Alto Networks, Inc.

STEP 16 | Panorama plugin for GCPで、サービスアカウント情報を追加します。

Panorama > **Google Cloud Platform** > **Setup**（セットアップ）を選択します。

認証情報に名前を付けて、ステップ15の**API server address**（**API**サービスアドレス）を入力し、ステップ14でエクスポートしたJSONファイルをアップロードします。

サービスアカウント認証情報を追加したら、Panoramaコマンドラインから認証情報を検証することができます:

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 17 | Panorama Plugin for GCPのオートスケーリングの設定

1. Panoramaコンテキストで、Google Cloud Platformを展開してAutoScaling（オートスケーリング）を選択し、**Add**（追加）をクリックします。
2. **Firewall Deployment Name**（ファイアウォールデプロイ名）および必要に応じてデプロイの説明を入力します。
3. **GCP Service Account Credential**（**GCP**サービスアカウント認証情報）の場合、ステップ16からのGCPサービスアカウント名を入力します。
4. Panoramaプラグインの設定時に作成した、デバイスグループとテンプレートスタックを選択します。
5. トラフィックを保護するために、**License Management Only**（ライセンス管理のみ）を無効にします。
6. **GKE Cluster Name**（**GKE**クラスタ名）を正確に入力します。
7. （任意）GKEクラスタの**Description**（説明）を入力します。
8. GKEクラスタの**Network CIDR**（ネットワーク**CIDR**）を入力します。
9. GKEクラスタに対応する**GKE Service Account**（**GKE**サービスアカウント）を選択します。

STEP 18 | （任意）サービスプロジェクト内で、「サンプルGKEサービステンプレートの使用」の説明に従ってGKEテンプレートを作成、デプロイするか、またはGCPコンソールを使ってGKEサービスをデプロイします。GKEクラスタのオンボーディング

*Panorama Plugin for GCP*でのオンボーディングされたアプリケーションの表示

オンボーディングされたアプリケーションを表示するには、**Panorama** > **Google Cloud Platform** > **Autoscaling**（オートスケーリング）を選択します。**Details**（詳細）列は、オンボーディングしたアプリケーションがある場合にのみ表示されます。

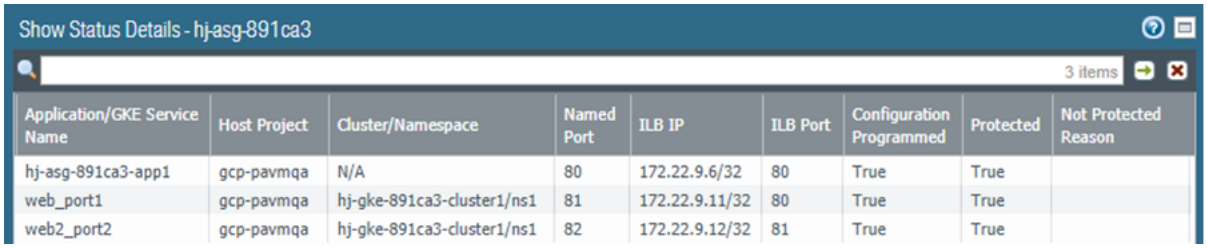
©2023 Palo Alto Networks, Inc.

Firewall Deployment Name	Project ID	Device Group	Template Stack	Details
gcp-asg-fw-peerbrown0	gcp-pavmqa	GCP_ASG_DG_peerbrown0	GCP_ASG_TS_peerbrown0	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-nlb-n642wb	gcp-autoscale-host-250622	gcp-autoscale-dg2	gcp-autoscale-ts2	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-891ca3	gcp-pavmqa	gcp-autoscale-dg-891ca3	gcp-autoscale-ts-891ca3	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-y892bl	gcp-pavmqa	gcp-autoscale-dg-y892bl	gcp-autoscale-ts-y892bl	Show Status Delicense Inactive VMs Trigger GKE Services Sync

Details（詳細）列の各リンクをクリックすると、アクションが実行されます。

©2023 Palo Alto Networks, Inc.

- **Show Status**（ステータスの表示）– GCP VM-Seriesファイアウォールデプロイ環境にオンボーディングされたアプリケーションの詳細をView（表示）します。



Application/GKE Service Name	Host Project	Cluster/Namespace	Named Port	ILB IP	ILB Port	Configuration Programmed	Protected	Not Protected Reason
hj-asg-891ca3-app1	gcp-pavmqa	N/A	80	172.22.9.6/32	80	True	True	
web_port1	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	81	172.22.9.11/32	80	True	True	
web2_port2	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	82	172.22.9.12/32	81	True	True	

次のフィールドには、選択したデプロイ環境から取得された情報が表示されます。これらの値は、Pub/Subメッセージ、またはGKEクラスタサービスのポーリングを介して指定したものです。

- **Application/GKE Service Name**（アプリケーション/**GKE**サービス名）–アプリケーションデプロイ名、またはGKEサービス名。
- **Host Project**（ホストプロジェクト）–ホストプロジェクトの名前。
- **Cluster/Namespace**（クラスタ/名前空間）–GKEクラスタ名に続いて名前空間（例:**`mycluster/namespace9`**）。
- **Named Port**（名前付きポート）–サービスの名前付きポートに割り当てられたポート。
- **ILB IP**–ILB IPアドレス。
- **ILB Port**–ILBポート番号。

  アプリケーションのオートスケーリングの場合、このプロパティは `apps.yaml`内の**`ilb-port`**になります。

  GKEクラスタを保護する場合、この値はクラスタ内にサービスをデプロイするために使用した`.yaml`ファイルに指定されている、GKEクラスタのポート番号になります。
- **Configuration Programmed**– NATルールが存在している場合はTrue、ない場合はFalse。
- **Protected**– アプリケーションが正常にオンボーディングされている場合True、オンボーディングに失敗した場合はFalse。Falseの場合は、**Not Protected Reason**（保護されない理由）列の説明を参照してください。
- **Not Protected Reason–Protected**（保護）がFalseの場合、アプリケーションが保護されていない理由が表示されます。一般的な理由を以下に示します。
  - **Configuration Programmed**–NATルールが存在している場合はTrue、ない場合はFalse。
  - **Protected**–アプリケーションが正常にオンボーディングされている場合True、オンボーディングに失敗した場合はFalse。Falseの場合は、**Not Protected Reason**（保護されない理由）列の説明を参照してください。
  - **Not Protected Reason**–**Protected**（保護）がFalseの場合、アプリケーションが保護されない理由が表示されます。一般的な理由を以下に示します。
    - GKEクラスタにUDPサービスをデプロイした。
    - すでに使用中の名前付きポートを指定した。特定の名前付きポートでは、1つのアプリケーションのみが待機できます。

©2023 Palo Alto Networks, Inc.

    - **License management only**（ライセンス管理のみ）オプションを選択したため、設定をプログラムしない。
    - GKEサービスに対して一致するラベルが見つからなかった。
- **Delicense Inactive VMs**—非アクティブなVMに対するライセンス解除機能をトリガする場合、**Yes**（はい）を選択します。
- **Trigger GKE Services Sync**—クラスター内で動作しているサービスにポーリングを行い、NAT、アドレス、およびサービスオブジェクト、および必要に応じてスタティックルートをプログラムする場合、**Yes**（はい）を指定します。デフォルトでPanoramaは、前回のポーリングの完了後10分後に自動的にポーリングを行います。

*CLI*からのデプロイステータスの表示

Panorama CLIを使って、デプロイしたアプリケーションを管理することができます。コマンドラインは、「Panorama Plugin for GCPでのオンボーディングされたアプリケーションの表示」に記述されているものを並列に実施します。次のコマンドで、**autoscaling_name**は、オートスケーリング設定に入力したファイアウォールデプロイ名です。

- オンボーディング（保護）されたアプリケーションを一覧表示します。

```
show plugins gcp show-protected-apps autoscaling_name <fw-deployment-name>
```

- 指定したデプロイ環境のファイアウォールに対して、ライセンス解除機能をトリガします。

```
request plugins gcp force-delicensing autoscaling_name <fw-deployment-name>
```

- GKEデプロイ環境の場合、プラグインがPub-Subメッセージを読み込んで、プログラムされたNATルールをPub-Subメッセージに基づいて同期するようにします。

```
request plugins gcp gke-service-discovery autoscaling_name <fw-deployment-name>
```

GCP用オートスケーリング テンプレートのパラメータ

テンプレートの.zipファイルは、https://github.com/PaloAltoNetworks/GCP-AutoScalingからダウンロードできます。.zipファイルには、ネットワークロードバランサーおよびアプリケーションロードバランサー設定用ファイアウォールテンプレート、およびアプリケーションテンプレートをサポートするためのディレクトリが含まれています。

テンプレートYAMLファイルは、次の一般的なフォーマットを利用しています:

```
#Copyright and license information
    :
    :
imports:                        <do not change>
    :
    :
resources:
```

 ©2023 Palo Alto Networks, Inc.

```
    -name: vm-series-fw       <do not change>
    -type:vm-series-fw.py     <do not change
    -properties:
    :
    :
outputs:                      <do not change>
    :
    :
```

すべての.yamlファイルで、デプロイのresourcesプロパティをカスタマイズします。importsまたはoutputsセクションは、何も変更しないでください。

- ファイアウォールテンプレート
- アプリケーションテンプレート

ファイアウォールテンプレート

次のセクションは、NLBおよびALBの.yamlファイルの、パラメータの詳細を説明しています。

- vm-series-fw-nlb.yaml
- vm-series-fw-alb.yaml

vm-series-fw-nlb.yaml

vm-series-fw-nlb.yamlテンプレートで、-propertiesを編集します。

パラメータ	サンプル値	コメント
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <ゾーンのリスト>	zones- us-central1-a	該当する場合は、複数のゾーンを次のように記載します。 zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	変更しないでください。
cloud-nat	yes	変更しないでください。
forwarding-rule-port	80	80または8080
urlPath-namedPort-maps-appname	`urlPath-namedPort-maps -MyApplication`	アプリケーション名を入力します。
sshkey	'admin:ssh-rsa <キーを貼り付け>'	「SSH キーペア」を確認してください。単一引用符内に、「**admin:**」と入力し、次に

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
		スペースを1つ入れてから、キーを貼り付けます。これは、Google Marketplaceテンプレートで使用されている構文と同じです。
bootstrap-bucket	bootstrap-autoscale	ブートストラップファイルを含んでいる、GCPバケットの名前。
image	vm-series-byol-814	現在BYOLイメージは、Google Marketplaceから利用できます。 PAYGまたはその他のライセンスモデルを使用している場合、イメージが異なる場合があります。
machine-type	n1-standard-4	n1-standard-4は、BYOLのデフォルトです。 ご利用のライセンスが許可している場合、>VM-Series ファイアウォールの最小システム要件で任意のマシンタイプを使用することができます。
service-account		ホストプロジェクトの一意のサービスアカウント名。
fw-instance-tag	vm-series-fw	GCPで指定したインスタンスタグ。

metric	custom.googleapis.com/VMSeries/panSessionActive	VM-SeriesのカスタムAPIパス、および選択したオートスケーリングメトリック。
		次のいずれかのメトリクスのみを指定してください。
		`panSessionActive`
		`panSessionUtilization`
		`DataPlaneCPUUtilizationPct`
		`DataPlanePacketBufferUtilization`

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
		`panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	現在、有効なタイプはGAUGE（ゲージ）のみです。
util-target	100	

VM-Seriesファイアウォールをデプロイするには、ファイアウォールの管理、Untrust、およびTrustインターフェイス向けに、専用のネットワークとサブネットワークが必要です。グリーンフィールドデプロイ（新しいネットワークを作成するためにテンプレートを設定）またはブラウンフィールドデプロイ（既存のネットワークを使用）向けの情報を記入します。使用しないネットワークデプロイパラメータは忘れずに削除するか、または注釈にしてください。

グリーンフィールドデプロイ:ファイアウォールの、管理、Untrust、およびTrustネットワーク/サブネットワークを作成するための値を入力します。

mgmt-network-cidr	172.22.2.0/24	
untrust-network-cidr	172.22.1.0/24	
trust-network-cidr	172.22.3.0/24	

mgmt-network-access-source-range- <許可されているIP範囲>	`mgmt-network-access-source-range`
	`- <permitted-ip-range-1>`
	`- <permitted-ip-range-2>`	

mgmt-network-access-ports-<ポート番号>	`mgmt-network-access-ports`
	`- 22`
	`- 443`	

ブラウンフィールドデプロイ:既存の各ネットワークまたはサブネットワークの名前を入力します。

mgmt-network	my-mgmt-network	
mgmt-subnet	my-mgmt-subnet	

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
trust-network	my-trust-network	
trust-subnet	my-trust-subnet	
untrust-network	my-untrust-network	
untrust-subnet	my-untrust-subnet	

vm-series-fw-alb.yaml

`vm-series-fw-alb.yaml`テンプレートで、`-properties`を編集します。

パラメータ	サンプル値	コメント
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <ゾーンのリスト>	zones- us-central1-a	該当する場合は、複数のゾーンを次のように記載します。 zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	alb	変更しないでください。
cloud-nat	yes	変更しないでください。
forwarding-rule-port	80	80
connection-draining-timeout	300	タイムアウト値（秒）。

`urlPath-namedPort-maps:`
`- appname:`
`  namedPort:`
`  urlMapPaths:`
`  - '/app1'`
`  - '/app1/*'`
	`urlPath-namedPort-maps:`
	`- appName: app1`
	`  namedPort: 80`
	`urlMapPaths:`
	`  - '/app1'`
	`  - '/app1/*'`
	`- appName: app2`
	`  namedPort: 81`
	`  urlMapPaths:`
	`  - '/app2'`
	`  - '/app2/*'`
		アプリケーションと対応する名前付きポートを表示します。

sshkey	'admin:ssh-rsa <キーを貼り付け>'	「SSH キーペア」を確認してください。単一引用符内に、

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
		「**admin:**」と入力し、次にスペースを1つ入れてから、キーを貼り付けます。これは、Google Marketplaceテンプレートで使用されている構文と同じです。
bootstrap-bucket	bootstrap-bucket-name	ブートストラップファイルを含んでいる、GCPバケットの名前。
image	vm-series-byol-814	現在BYOLイメージは、Google Marketplaceから利用できます。 PAYGまたはその他のライセンスモデルを使用している場合、イメージが異なる場合があります。
machine-type	n1-standard-4	n1-standard-4は、BYOLのデフォルトです。 ご利用のライセンスが許可している場合、>VM-Series ファイアウォールの最小システム要件で任意のマシンタイプを使用することができます。
service-account	サービスプロジェクトの一意のサービスアカウント名。	
fw-instance-tag	vm-series-fw	GCPで指定したインスタンスタグ。

metric	custom.googleapis.com/VMSeries/panSessionActive	VM-SeriesのカスタムAPIパス、および選択したオートスケーリングメトリック。
		次のいずれかのメトリクスのみを指定してください。
		`panSessionActive`
		`panSessionUtilization`
		`DataPlaneCPUUtilizationPct`
		`DataPlanePacketBufferUtilization`

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
		`panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	現在、有効なタイプはGAUGE（ゲージ）のみです。
util-target	100	オートスケーリングの最終利用状況ターゲット値を入力します。
グリーンフィールドデプロイ:ファイアウォールの、管理、Untrust、およびTrustネットワーク/サブネットワークを作成するための値を入力します。		
mgmt-network-cidr	192.168.12.0/24	
untrust-network-cidr	192.168.11.0/24	
trust-network-cidr	192.168.11.0/24	
mgmt-network-access-source-range- <許可されているIP範囲>	`mgmt-network-access-source-range- <許可されているIP範囲-1>- <許可されているIP範囲-2>`	
mgmt-network-access-ports-<ポート番号>	`mgmt-network-access-ports- 22- 443`	
ブラウンフィールドデプロイ:既存の各ネットワークまたはサブネットワークの名前を入力します。		
mgmt-network	existing-vpc-mgmt	
mgmt-subnet	existing-subnet-mgmt	
trust-network	existing-vpc-trust	
trust-subnet	existing-subnet-trust	
untrust-network	existing-vpc-untrust	
untrust-subnet	existing-subnet-untrust	

©2023 Palo Alto Networks, Inc.

アプリケーションテンプレート
apps.yaml

アプリケーションテンプレートはホストプロジェクト（VM-Seriesファイアウォールを含む）とサービスプロジェクト（ファイアウォールデプロイが保護するアプリケーションまたはサービスを含む）間の接続を作成します。

パラメータ	サンプル値	コメント
host-project	your-host-project-name	VM-Seriesファイアウォールデプロイを含むプロジェクトの名前。
fw-deployment-name	my-vm-series-firewall-name	
region	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <ゾーンのリスト>	zones- us-central1-a	該当する場合は、複数のゾーンを次のように記載します。 `zones- us-central1-a - us-central1-b- us-central1-c- us-central1-f`
app-machine-type	n1-standard-2	アプリケーションまたはサービスを実行しているVMのマシンタイプ。ご利用のライセンスが許可している場合、>VM-Series ファイアウォールの最小システム要件で任意のマシンタイプを使用することができます。
app-instance-tag	web-app-vm	このタグ（ラベル）はGCPで割り当てました。
sshkey	'admin:ssh-rsa <キーを貼り付け>'	「SSH キーペア」を確認してください。単一引用符内に、「**admin:**」と入力し、次にスペースを1つ入れてから、キーを貼り付けます。これは、Google Marketplaceテンプレートで使用されている構文と同じです。

©2023 Palo Alto Networks, Inc.

パラメータ	サンプル値	コメント
trust-network	<プロジェクト名>/<VPCネットワーク名>	共有VPCの場合、<プロジェクト名>はホストプロジェクトの名前になります。 ピアリングVPCの場合、<プロジェクト名>はサービスプロジェクトの名前になります。
trust-subnet	<プロジェクト名>/<サブネット名>	共有VPCの場合、<プロジェクト名>はホストプロジェクトの名前になります。 ピアリングVPCの場合、<プロジェクト名>はサービスプロジェクトの名前になります。
trust-subnet-cidr	10.2.0.0/24	グリーンフィールドデプロイの場合、ホストプロジェクトのTrustサブネットCIDR（ファイアウォールテンプレートのtrust-network-cidrパラメータ）。 ブラウンフィールドデプロイの場合、Trustネットワークの CIDR。
vm-series-fw-template-topic	<PubSubトピック>	ファイアウォールデプロイが作成したトピック名を入力します。アプリケーションテンプレートは、トラフィックを転送するためのファイアウォール設定をプログラムするために、メッセージをトピックに投稿します。
ilb-port	80	アプリケーションのinternal-load-balancer-port出力のポート番号を入力します。
urlPath-namedPort	83	urlPath-namedPort出力のポート番号を入力します。

©2023 Palo Alto Networks, Inc.

GKEサービステンプレートのサンプル

これらのサンプルテンプレートは、VM-Seriesファイアウォールによる保護を受けるための、GKEサービスの設定方法を表しています。独自のクラスタサービスを作成するための基本については、「プライベートクラスタの作成」を参照してください。

- サンプルGKEサービステンプレートの使用
- gke_cluster_role.yaml
- gke_cluster_role_binding.yaml
- web-deployment.yaml
- web-service.yaml
- web-deployment-v2.yaml
- web-service-v2.yaml
- サービス内の複数のポート

サンプルGKEサービステンプレートの使用

次の.yamlファイル内のサンプルコンテンツに基づいて、サービステンプレートを作成することができます。一般的に、単一の.yamlファイルを作成します。

VM-Seriesファイアウォールの保護を受けるには、web-service.yamlまたはweb-service-v2.yamlに示されているとおり、クラスタ内のサービスに「panw-named-port=<named_port>」のラベルを設定する必要があります。

1. 次のように、.yaml ファイルをデプロイします。

```
kubectl apply -f [FILE_NAME].yaml
```

2. VPCデプロイを設定します。
   - 共有VPCデプロイ環境で、「共有VPCの設定」の説明に従って共有VPC内のGKEクラスタを起動します。
   - ピアリングVPCデプロイ環境で、GKEクラスタVPCを、ホストプロジェクトのTrustネットワークとピアリングします。「ピアリングVPCの設定」を参照してください。

デプロイの完了後、次方法でサービステンプレート*.yaml*ファイルにデプロイされたすべてのサービスを削除することができます。

```
kubectl delete -f [FILE_NAME].yaml
```

gke_cluster_role.yaml

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRole
metadata:
  name: gke-plugin-role
rules:
  - apiGroups:
      - ""
```


©2023 Palo Alto Networks, Inc.

```
    resources:
      - services
    verbs:
      - list
```

gke_cluster_role_binding.yaml

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: gke-plugin-role-binding
subjects:
  - kind: ServiceAccount
    name: hj-gke-891ca3-cluster1-sa
    namespace: default
roleRef:
  kind: ClusterRole
  name: gke-plugin-role
  apiGroup: rbac.authorization.k8s.io
```

web-deployment.yaml

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: web
  namespace: default
spec:
  selector:
   matchLabels:
    run: web
  template:
   metadata:
    labels:
      run: web
   spec:
    containers:
    - image: gcr.io/google-samples/hello-app:1.0
      imagePullPolicy: IfNotPresent
      name: web
      ports:
      - containerPort: 8080
       protocol:  TCP
```

web-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: web
  namespace: default
  annotations:
    cloud.google.com/load-balancer-type: "Internal"
```


©2023 Palo Alto Networks, Inc.

```
  labels:
    panw-named-port-port1: "80"
spec:
  ports:
  # the port that this service should serve on
  - name: port1
    port: 80
    protocol: TCP
    targetPort: 8080
  selector:
    run: web
  type: LoadBalancer
```

web-deployment-v2.yaml

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: web2
  namespace: default
spec:
  selector:
    matchLabels:
      run: web2
  template:
    metadata:
      labels:
        run: web2
    spec:
      containers:
      - image: gcr.io/google-samples/hello-app:2.0
        imagePullPolicy: IfNotPresent
        name: web2
        ports:
        - containerPort: 8080
          protocol: TCP
```

web-service-v2.yaml

```
apiVersion: v1
  kind: Service
  metadata:
    name: web2
    namespace: default
    annotations:
      cloud.google.com/load-balancer-type: "Internal"
    labels:
      panw-named-port-port2: "81"
  spec:
    ports:
    # the port that this service should serve on
    - name: port2
      port: 81
      protocol: TCP
```


©2023 Palo Alto Networks, Inc.

```
      targetPort: 8080
    selector:
      run: web2
    type: LoadBalancer
```

サービス内の複数のポート

1つのサービス内に複数のポートがある場合、ラベルを編集して以下のサンプルのように、ターゲットポート名と番号を、panw-named-port-<サービス固有のポート名>の形式でマップします。

```
apiVersion: v1
kind: Service
metadata:
  name: carts
  annotations:
    cloud.google.com/load-balancer-type: "Internal"
  labels:
    panw-named-port-carts-http: "6082"
    panw-named-port-carts-https: "6083"
  namespace: default
spec:
  type: LoadBalancer
  ports:
  # the port that this service should serve on
  - name: carts-http
    protocol: TCP
    port: 80
    targetPort: 80
  - name: carts-https
    protocol: TCP
    port: 443
    targetPort: 443
  selector:
    name: carts
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

paloalto TECHDOCS

Cisco ENCS ネットワークでの VM-Series ファイアウォールのセットアップ

Cisco 5400 Series Enterprise Network Compute System（ENCS）アプライアンスが導入されている支社やリモート オフィスで従来のアプライアンス ベースのネットワーク インフラストラクチャを仮想化している場合は、Enterprise NFV Infrastructure Software（NFVIS）を使用して VM-Series ファイアウォールを Cisco ネットワーク内にデプロイできます。VM-Series ファイアウォールは、次世代ファイアウォール機能を備えた仮想ネットワーク機能（VNF）として動作し、すべてのアプリケーションを安全に有効にし、支社やリモート オフィスのユーザーとネットワークを脅威から保護します。

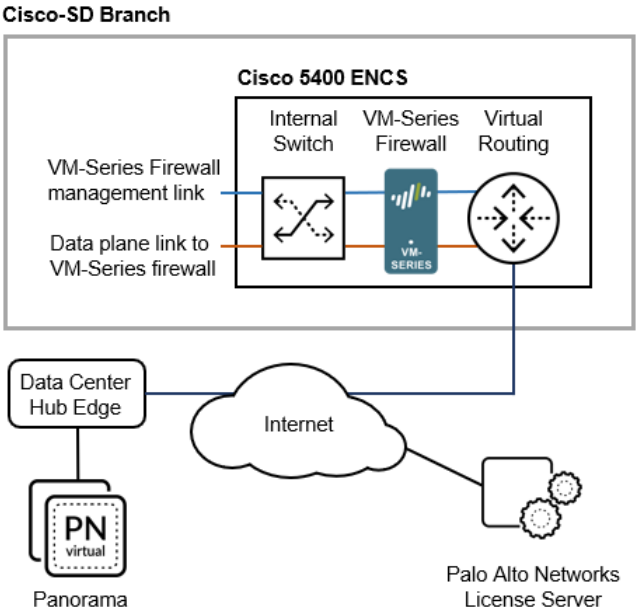
Cisco Enterprise Network Compute System（ENCS）アプライアンスと Cisco Integrated Services Virtual Routers（ISRV）および NFVIS ソフトウェアの組み合わせにより、Software-Defined Branch（SD-Branch）ネットワーク アーキテクチャがサポートされます。

> Cisco ENCS デプロイメントの計画
> Cisco ENCS 用 VM-Series ファイアウォール イメージの準備
> Cisco ENCS での VM-Series ファイアウォールのデプロイ

Cisco ENCS デプロイメントの計画

Cisco SD-Branch で、支社のアプリケーションとユーザーを保護する次世代ファイアウォール機能を備えた VNF として、VM-Series ファイアウォールを Cisco ENCS アプライアンスにデプロイします。バーチャル ワイヤ、レイヤー 2、またはレイヤー 3 デプロイメントにファイアウォールを高可用構成でデプロイできます。

VM-Series ファイアウォールを管理するには、Panorama アプライアンスをオンプレミスまたはクラウドにデプロイできます。次のトポロジは、ブランチ エッジでの VM-Series ファイアウォールを示します。



Cisco ENCS の要件

サポートされている NFVIS のバージョンとハードウェア プラットフォームについては、Palo Alto Networks 互換性マトリックスを参照してください。

- NFVIS でネットワークとブリッジをセットアップします。
  - 仮想 NIC を作成して仮想ブリッジにアタッチします。これにより ENCS アプライアンスがトラフィックを VM-Series ファイアウォールに誘導できます。

    Cisco ENCS アプライアンスでは VM-Series ファイアウォールは最大 8 つのデータプレーン インターフェイスをサポートします。

    Cisco ENCS の VM-Series ファイアウォールのデータプレーン インターフェイスは Virtio モードのみをサポートしています。ENCS SR-IOV および PCI パススルー モードはサポートされていません。
  - VM-Series ファイアウォール管理アクセスのためのネットワーク接続をセットアップします。Panorama を使用している場合は、デプロイするファイアウォールを管理するために Panorama がネットワークへアクセスできることを確認します。
- Python 2.7。コマンド ラインを使用して変換を行う場合にローカル マシンで必要です。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールと **Panorama** の要件

- VM-Series ファイアウォール — VM-50 および VM-100 が推奨されます。VM-Series ファイアウォールに割り当てることができる十分なリソースが ENCS ハードウェアにある場合には、VM-300、VM-500、および VM-700 もサポートされます。「VM-Series のシステム要件」を参照して、Cisco ENCS アプライアンスに、選択した VM-Series モデルをサポートできる十分なリソースがあることを確認してください。
  - qcow2 ファイル（PAN-OS for VM-Series KVM 基本イメージ）: PAN-OS 9.1 以降。「グラフィカル ユーザー インターフェイスでの qcow2 ファイルの変換」のステップ 2 または「コマンド ライン インターフェイスでの qcow2 ファイルの変換」のステップ 2 を参照してください。
  - 要件を満たす VM-Series ファイアウォール キャパシティ ライセンスとサブスクリプションの認証コード。「VM-Series モデルのライセンスタイプ」を参照してください。NFVIS ユーザー インターフェイスで認証コードを入力するか、「コマンド ライン インターフェイスでの qcow2 ファイルの変換」のステップ 4 の説明に従って変換作業フォルダにある **authcodes** テキスト ファイルに認証コードを記述します。
  - PAN-OS 9.1 で、Cisco ENCS 上の VM-Series ファイアウォールは、デフォルトでは、DPDKモードの Virtio をサポートしています。
- Panorama ハードウェア アプライアンスまたはバーチャル アプライアンス1 つの VM-Series ファイアウォールを 1 つの Cisco SD-Branch ネットワークにデプロイすることもできますが、複数のブランチに複数のファイアウォールをデプロイして Panorama から一元的に管理する方法が一般的です。
  - Panorama バージョン 9.1 以降。このバージョンは、ご使用の VM-Series ファイアウォールのバージョン以上でなければなりません。
  - Panorama で生成された VM 認証キー。このキーにより、VM-Series ファイアウォールは Panorama を認証できます。

©2023 Palo Alto Networks, Inc.

Cisco ENCS 用 VM-Series ファイアウォール イメージの準備

NFVIS グラフィカル ユーザー インターフェイスまたはコマンド ライン インターフェイスから PAN-OS qcow2 ファイルを変換できます。

- グラフィカル ユーザー インターフェイスでの qcow2 ファイルの変換
- コマンド ライン インターフェイスでの qcow2 ファイルの変換

グラフィカル ユーザー インターフェイスでの qcow2 ファイルの変換

NFVIS グラフィカル ユーザー インターフェイスを使用して、イメージ パッケージングおよびブートストラップ情報を入力します。

STEP 1 | NFVIS で **VM Life Cycle**（**VM** ライフサイクル） > **Image Repository**（イメージ リポジトリ） > **Image Packaging**（イメージ パッケージング）の順に移動します。

STEP 2 | 以下に示すようにパッケージ情報を入力します。このとき各自の値を指定します。

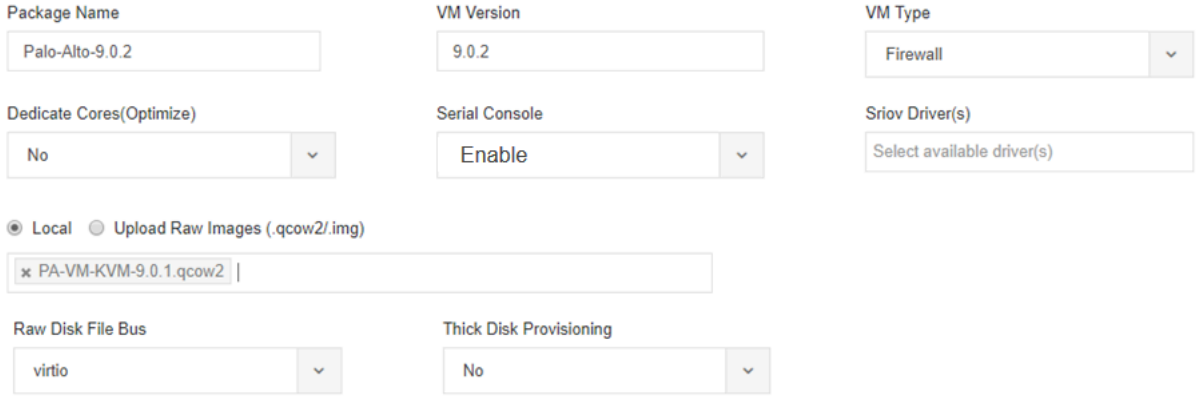
1. **Package Name**（パッケージ名）と **VM Version**（**VM** バージョン）を入力し、**VM Type**（**VM** タイプ）で **Firewall**（ファイアウォール）を選択します。
2. **Serial Console**（シリアル コンソール）を**Enable**（有効）にします。
3. SR-IOV はサポートされていないので、**Sriov Driver(s)**（**Sriov** ドライバ）フィールドは空白のままにします。
4. **Local**（ローカル）を選択して前にアップロードした qcow2 ファイルを選択するか、**Upload Raw Images**（ロー イメージのアップロード）をクリックして qcow2 ファイルをアップロードします。
   - Palo Alto Networksカスタマーサポートポータルにログインします。

     サポート アカウントの作成と VM-Series ファイアウォールの登録をまだ行っていない場合は、これらの操作を行います。
   - **Support**（サポート） > **Software Updates**（ソフトウェア更新）を選択し、**Filter By**（絞り込み）のドロップダウン リストから **Pan OS for VM-Series KVM Base**

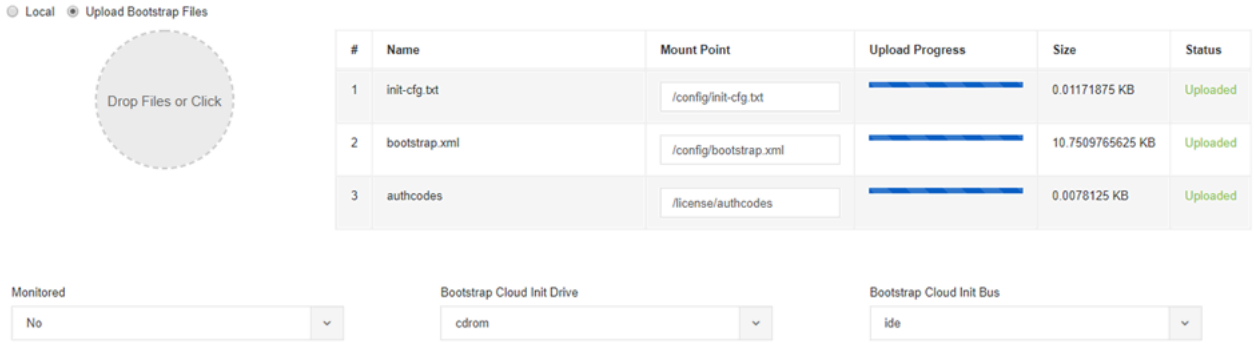
©2023 Palo Alto Networks, Inc.

Image（**Pan OS for VM-Series KVM** 基本イメージ）（バージョン 9.1 など）を選択します。

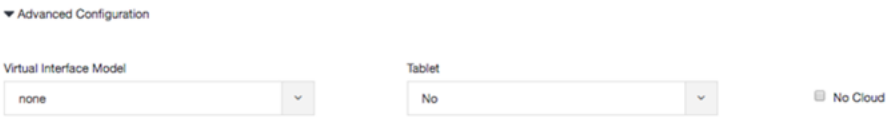
- qcow2 イメージをダウンロードします。



STEP 3 | ブートストラップ ファイルをアップロードします。

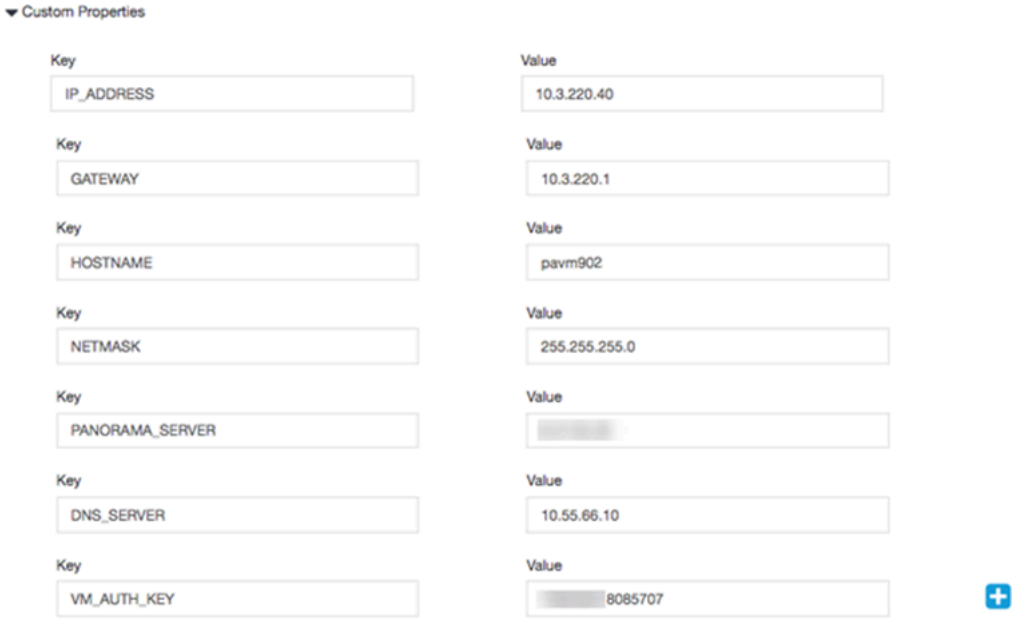


STEP 4 | **Advanced Configuration**（詳細設定）を設定します。



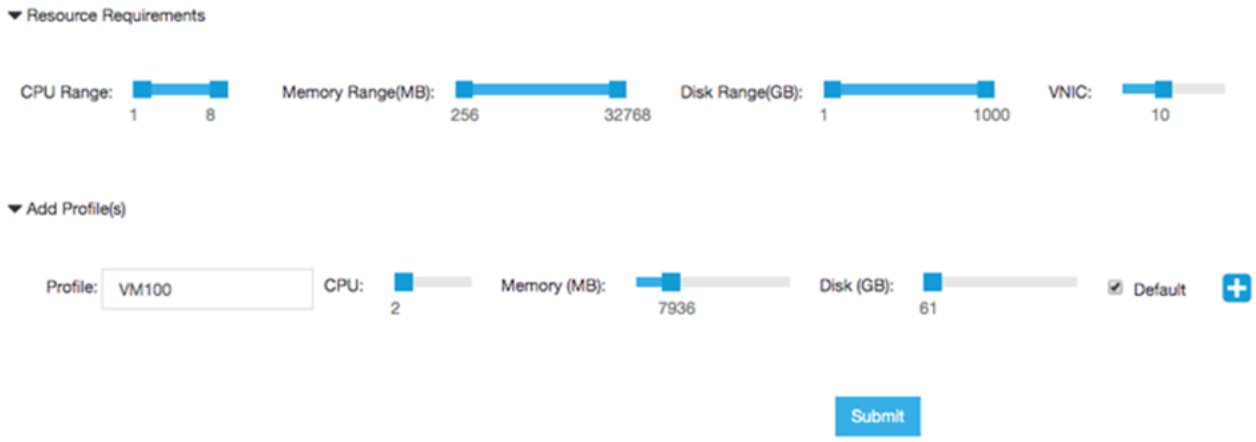
 ©2023 Palo Alto Networks, Inc.

STEP 5 | **Custom Properties**（カスタム プロパティ）の値を入力します。

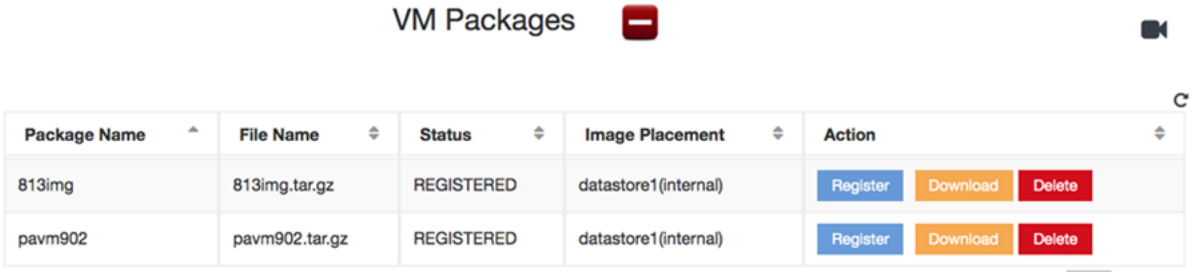


STEP 6 | リソース要件の値を設定してデフォルト プロファイルを選択するか、現行設定のプロファイルを追加します。

Submit（送信）をクリックして、パッケージを保存します。



STEP 7 | **Register**（登録）をクリックして新しいイメージを保存します。



©2023 Palo Alto Networks, Inc.

コマンド ライン インターフェイスでの qcow2 ファイルの変換

コマンド ライン インターフェイスからブートストラップ ファイルを作成するには、ファイル **image_properties_template.xml** を作成してから、VM Image Packaging ユーティリティを使用して **.tar** ファイルを作成します。このファイルは、**nfvpt.py** スクリプトを使用して変換します。出力は **tar.gz** ファイルです。このファイルは NFVIS ユーザー インターフェイスからアップロードできます。

STEP 1 | ローカル マシンで、VM-Series qcow2 イメージを Cisco ENCS 形式に変換するために必要なファイルをダウンロードして保存するフォルダ（変換作業フォルダ）を作成または選択します。

STEP 2 | VM-Series qcow2 イメージを取得します。

1. Palo Alto Networksカスタマーサポートポータルにログインします。

   サポート アカウントの作成と VM-Series ファイアウォールの登録をまだ行っていない場合は、これらの操作を行います。
2. **Support**（サポート） > **Software Updates**（ソフトウェア更新）を選択し、**Filter By**（絞り込み）のドロップダウン リストから **Pan OS for VM-Series KVM Base Image**（**Pan OS for VM-Series KVM** 基本イメージ）（バージョン 9.1 など）を選択します。
3. qcow2 イメージを変換作業フォルダにダウンロードします。

STEP 3 | 変換作業フォルダに次の init-cfg.txt ファイルを作成します。

```
type=static
ip-address=${IP_ADDRESS}
default-gateway=${GATEWAY}
netmask=${NETMASK}
ipv6-address=
ipv6-default-gateway=
hostname=${HOSTNAME}
vm-auth-key=${VM_AUTH_KEY}
panorama-server=${PANORAMA_SERVER}
panorama-server-2=
tplname=
dgname=
dns-primary=${DNS_SERVER}
dns-secondary=
op-command-modes=jumbo-frame, mgmt-interface-swap**
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

STEP 4 | **authcodes** という名前のテキスト ファイル（拡張子なし）を作成し、VM-Series ファイアウォール キャパシティおよびサブスクリプションの認証コードを入力します。ファイルを変換作業フォルダに保存します。

©2023 Palo Alto Networks, Inc.

STEP 5 | 以下の `image_properties_template.xml` ファイルを変換作業フォルダに作成し、各自のデプロイメントの値を指定します。

```
<image_properties>
    <vnf_type>FIREWALL</vnf_type>
    <name>pafw</name>
    <version>9.1.0</version>
    <bootup_time>-1</bootup_time>
    <root_file_disk_bus>virtio</root_file_disk_bus>
    <root_image_disk_format>qcow2</root_image_disk_format>
    <vcpu_min>2</vcpu_min>
    <vcpu_max>8</vcpu_max>
    <memory_mb_min>4096</memory_mb_min>
    <memory_mb_max>16384</memory_mb_max>
    <vnic_max>8</vnic_max>
    <root_disk_gb_min>32</root_disk_gb_min>
    <root_disk_gb_max>60</root_disk_gb_max>
    <console_type_serial>true</console_type_serial>
    <sriov_supported>true</sriov_supported>
    <pcie_supported>false</pcie_supported>
    <monitoring_supported>false</monitoring_supported>
    <monitoring_methods>ICMPPing</monitoring_methods>
    <low_latency>true</low_latency>
    <privileged_vm>true</privileged_vm>
    <custom_property>
        <HOSTNAME> </HOSTNAME>
    </custom_property>
    <custom_property>
        <IP_ADDRESS> </IP_ADDRESS>
    </custom_property>
    <custom_property>
        <NETMASK> </NETMASK>
    </custom_property>
    <custom_property>
        <GATEWAY> </GATEWAY>
    </custom_property>
    <custom_property>
        <PANORAMA_SERVER> </PANORAMA_SERVER>
    </custom_property>
    <custom_property>
        <DNS_SERVER> </DNS_SERVER>
    </custom_property>
    <custom_property>
        <VM_AUTH_KEY> </VM_AUTH_KEY>
    </custom_property>
    <default_profile>VM-50</default_profile>
    <profiles>
        <profile>
                <name>VM-50</name>
                <description>VM-50 profile</description>
                <vcpus>2</vcpus>
                <memory_mb>5120</memory_mb>
                <root_disk_mb>60000</root_disk_mb>
        </profile>
        <profile>
```


©2023 Palo Alto Networks, Inc.

```
                <name>VM-100-n-200</name>
                <description>VM-100 and VM-200 profile</
description>
                <vcpus>2</vcpus>
                <memory_mb>7168</memory_mb>
                <root_disk_mb>60000</root_disk_mb>
        </profile>
        <profile>
                <name>VM-300</name>
                <description>VM-300 profile</description>
                <vcpus>2</vcpus>
                <memory_mb>9216</memory_mb>
                <root_disk_mb>60000</root_disk_mb>
        </profile>
        <profile>
                <name>VM-1000-HV</name>
                <description>VM-1000-HV profile</description>
                <vcpus>4</vcpus>
                <memory_mb>9216</memory_mb>
                <root_disk_mb>60000</root_disk_mb>
        </profile>
        <profile>
                <name>VM-500</name>
                <description>VM-500 profile</description>
                <vcpus>4</vcpus>
                <memory_mb>16384</memory_mb>
                <root_disk_mb>60000</root_disk_mb>
        </profile>
    </profiles>
    <cdrom>true</cdrom>
    <bootstrap_file_1>/config/init-cfg.txt</bootstrap_file_1>
    <bootstrap_file_2>/config/bootstrap.xml</bootstrap_file_2>
    <bootstrap_file_3>/license/authcodes</bootstrap_file_3>
</image_properties>
```

STEP 6 | Image Packaging ユーティリティをダウンロードします。

1. Enterprise NFVIS ユーザー インターフェイスにログインし、**VM Life Cycle**（**VM** ライフサイクル） > **Image Repository**（イメージ リポジトリ）を選択します。
2. **Browse Datastore**（データストアを参照）タブをクリックし、**data** > **intdatastore** > **uploads** > **vmpackagingutility** の順に移動します。
3. `nfvisvmpackagingtool.tar` を変換作業フォルダにダウンロードします。
4. ファイルを untar します。

```
tar -xvf nfvisvmpackagingtool.tar
```

STEP 7 | qcow2、`init-config.txt`、および `authcodes` ファイルが含まれている変換作業フォルダで、`nfvpt.py` スクリプトを実行します。`nfvpt.py` Image Packaging ユーティリティのドキュメントを参照してください。

以下の例では、Palo-Alto-9.1.0 というイメージ ファイルと VM-100 プロファイルが作成されます。オプションはスペースで区切って指定します（例では分かりやすくするためオプショ

©2023 Palo Alto Networks, Inc.

ンが 1 行に 1 つずつ示されています）。カスタム オプションは、コロンを区切り文字として使用するキー値ペアです。

```
./nfvpt.py -o Palo-Alto-9.1.0 -i PA-VM-KVM-9.1.0.qcow2
-n PAN902 -t FIREWALL -r 9.1.0
--monitored false
--privileged true
--bootstrap /config/init-cfg.txt:init-cfg.txt,/license/
authcodes:authcodes
--min_vcpu 2 --max_vcpu 8
--min_mem 4096 --max_mem 16384
--min_disk 10 --max_disk 70
--vnic_max 8
--optimize true
--console_type_serial true
--profile VM-100,"VM-100 profile",2,7168,61440
--default_profile VM-100
--custom HOSTNAME:hello
--custom IP_ADDRESS:10.2.218.24
--custom NETMASK:255.255.255.0
--custom GATEWAY:10.2.218.1
--custom DNS_SERVER:10.55.66.10
--custom PANORAMA_SERVER:0.10.10.0
--custom VM_AUTH_KEY:123451234512345
```

STEP 8 | 変換後のイメージをアップロードします。

1. NFVIS ユーザー インターフェイスで **VM Life Cycle**（**VM** ライフ サイクル） > **Image Repository**（イメージ リポジトリ）を選択し、青色のイメージ アイコンをクリックします。**Drop Files or Click**（ファイルをドロップまたはクリック）の円が表示されます。
2. 変換後のファイルをこの円にドラッグするか、クリックしてファイルを参照し、選択します。
3. Status（ステータス）列で **Start**（開始）をクリックします。

   アップロードが完了すると、イメージが登録され、アップロードしたファイルが **Image Registration**（イメージ登録）タブの **Images**（イメージ）リストに表示されます。

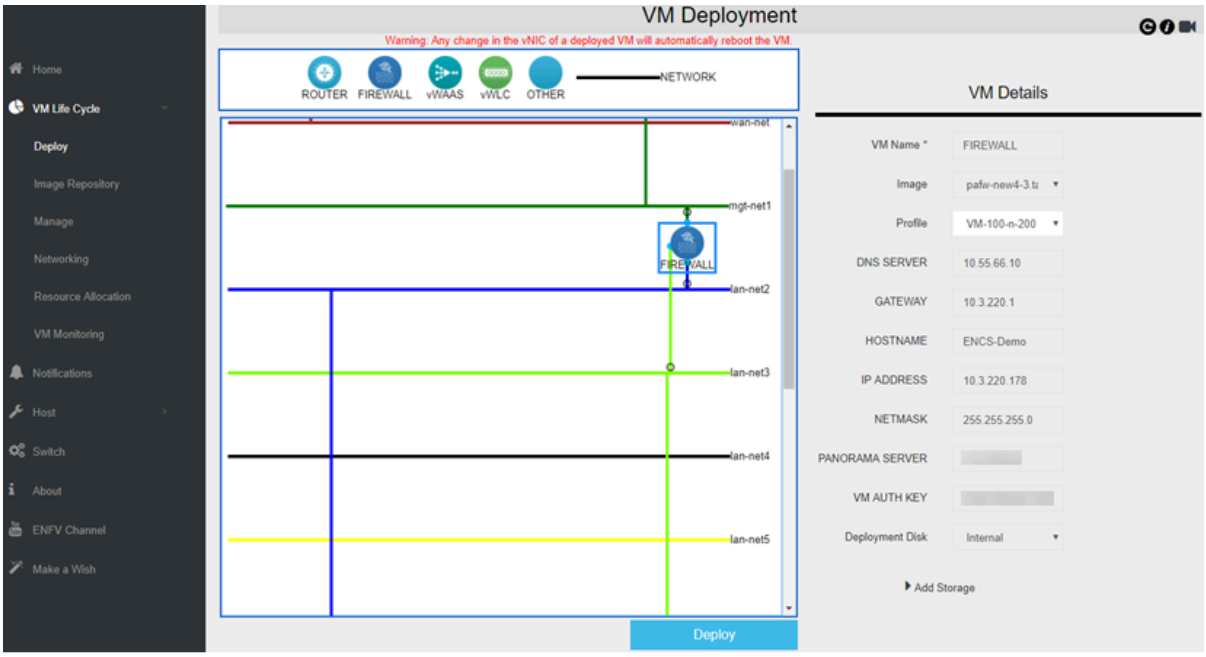
©2023 Palo Alto Networks, Inc.

Cisco ENCS での VM-Series ファイアウォールのデプロイ

ファイアウォールのデプロイを開始する前に、VM-Series ファイアウォールへの管理アクセスのためのネットワーク接続を作成していることを確認します。Panorama を使用している場合は、Panorama がファイアウォールに管理接続していることを確認します。

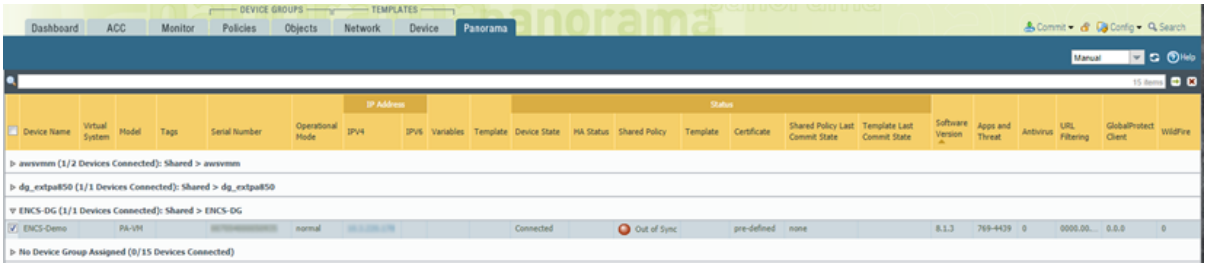
STEP 1 | VM-Series ファイアウォールを展開します。

1. Enterprise NFVIS で **VM Life Cycle**（**VM** ライフ サイクル） > **Deploy**（デプロイ）をクリックします。
2. ファイアウォール アイコンを該当するネットワークにドラッグします。この例では、ファイアウォールによって管理ネットワークと LAN ネットワークが接続されます。



3. VM-Series ファイアウォールをデプロイします。

   Panorama を使用してファイアウォールを管理している場合は、**Panorama** > **Managed Devices**（管理対象デバイス） > **Summary**（サマリー）にファイアウォールが **Connected**（接続）として表示されます。ファイアウォールが Panorama に接続していない場合は、正しい Panorama IP アドレスを指定しており、デバイスがネットワークで通信できることを確認してください。

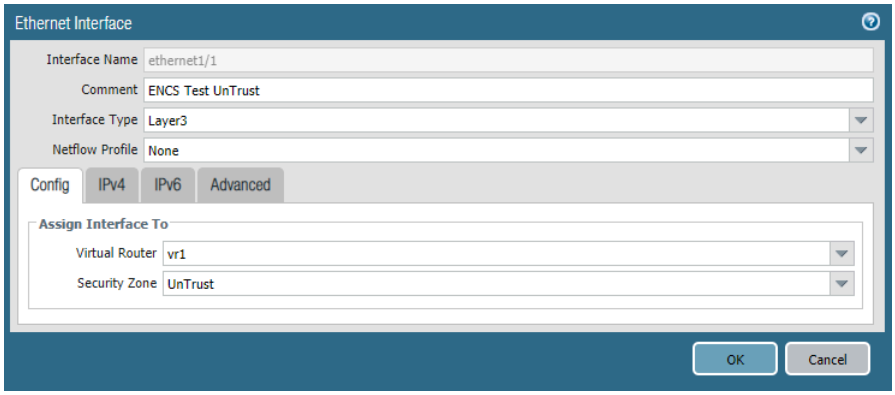


 ©2023 Palo Alto Networks, Inc.

STEP 2 | VM-Series ファイアウォール データプレーン インターフェイスを設定します。

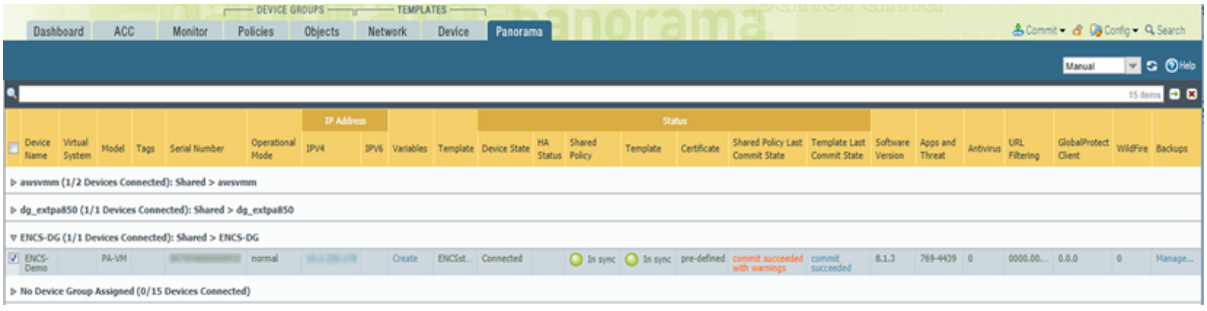
「レイヤー 3 インターフェイスの設定」、「レイヤー 2 インターフェイスの設定」、または「バーチャル ワイヤの設定」を参照してください。Panorama を使用している場合にレイヤー 3 デプロイメントに合わせてファイアウォールを設定する方法を以下に示します。

1. テンプレートを追加し、ファイアウォールをテンプレートに割り当てます。
2. **Network**（ネットワーク）を選択し、Template（テンプレート）のドロップダウン リストから作成したテンプレートを選択します。
3. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
4. **ethernet 1/1**をクリックし、以下のように設定します。
   - **Interface Type**（インターフェイス タイプ）を **Layer3**（レイヤー 3）に設定します。
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - また、**Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。**UnTrust** という新しいゾーンを定義し、**OK** をクリックします。
   - **IPv4** タブで **DHCP Client**（**DHCP** クライアント）または **Static**（静的）を選択します。Static（静的）を選択した場合は、IP アドレスを入力します。



5. ネットワーク インターフェイスごとに b ～ e を繰り返します。
6. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）を選択し、Panorama と管理対象ファイアウォールに対する設定変更をコミットします。

   ファイアウォール インターフェイスのリンク状態が「up」であることを確認します。

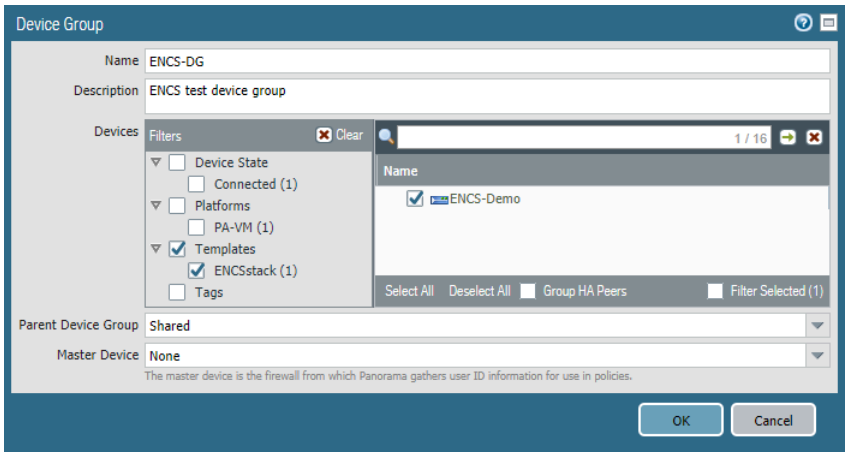


 ©2023 Palo Alto Networks, Inc.

STEP 3 | ネットワークでアプリケーションとユーザーを安全に有効化するようにセキュリティ ポリシーを設定します。

Panorama を使用している場合にデバイス グループを使用して管理対象ファイアウォールのポリシー ルールを一元管理する方法を以下に示します。

1. デバイス グループを追加し、管理対象ファイアウォールをデバイス グループに割り当てます。



2. デバイス グループのセキュリティ ポリシーを設定します。

STEP 4 | VM-Series ファイアウォールがネットワークでトラフィックを保護することを確認します。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Oracle Cloud Infrastructure での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールを Oracle Cloud Infrastructure（OCI）クラウドにデプロイします。OCI に VM-Series をデプロイすると、ワークロードを保護、セグメント化し、高度な脅威を防止し、クラウドへ移行する際のアプリケーションの可視化が向上します。

OCI は、Oracle が提供する高可用ホスト環境でアプリケーションを実行できるようにするパブリック クラウド コンピューティング サービスです。VM-Series ファイアウォールをデプロイすることで、OCI 環境で実行されるアプリケーションとサービスを保護できます。

- OCI シェイプのタイプ
- OCI でサポートされるデプロイメント
- OCI への VM-Series ファイアウォールのセットアップ準備
- Oracle Cloud Marketplace からの VM-Series ファイアウォールのデプロイ
- OCI でのアクティブ/パッシブ HA の設定

OCI シェイプのタイプ

VM-Series ファイアウォールでは以下の OCI VM シェイプがサポートされています。VM シェイプの詳細については、Oracle Cloud Infrastructure のドキュメントを参照してください。

VM-Series モデル	最小 OCI シェイプ
VM-100IPv6	VM.Standard2.4
VM-300IPv6	VM.Standard2.4
VM-500IPv6	VM.Standard2.8
VM-700IPv6	VM.Standard2.16

VM-Series ファイアウォールは、「VM-Series のシステム要件」に記載されている最小システム要件よりも多くのリソースを持つ OCI インスタンスにデプロイできます。VM-Series ファイアウォール モデルに大きなシェイプ サイズを選択した場合。ファイアウォールでは、システム要件ページに記載されている最大数の vCPU コアと最大容量のメモリのみが使用されますが、大きなシェイプによるネットワーク パフォーマンス向上のメリットは得られます。

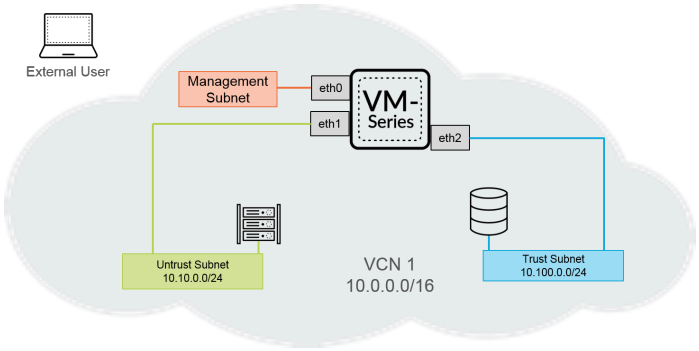
©2023 Palo Alto Networks, Inc.

OCI でサポートされるデプロイメント

OCI で VM-Series ファイアウォールを使用し、次のような状況でクラウド環境を保護します。

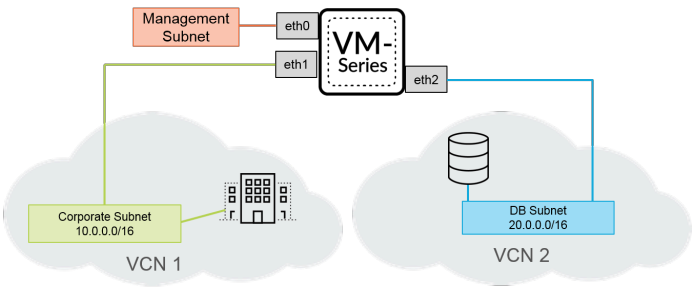
- North-South トラフィック — VM-Series ファイアウォールを使用して、信頼できないソースからクラウド ネットワークに入るトラフィックや、クラウド ネットワークから信頼できないソースに向かうトラフィックを保護できます。いずれのタイプのトラフィックでも、Virtual Cloud Network（VCN:仮想クラウド ネットワーク） でルート テーブル ルールを設定し、ファイアウォールで NAT ポリシー ルールを設定します。

  この例では、アウトバウンド トラフィックが VCN の trust サブネットから出ています。パブリック IP アドレスで送信元アドレス変換ポリシーを設定し、そのトラフィックをファイアウォールにリダイレクトするルート テーブル ルールを設定する必要があります。このルート ルールは、発信トラフィックを、VCN の trust サブネット内のファイアウォール インターフェイスに向かって指示します。ファイアウォールはこのトラフィックを受信すると、トラフィックで送信元アドレス変換を実行し、設定されている他のセキュリティ ポリシーをすべて適用します。



- VCN 間トラフィック（East-West）ー VM-Series ファイアウォールでは、クラウド環境内で VCN 間を移動するトラフィックを保護できます。各サブネットは異なる VCN に属している必要があります。これは、デフォルトでは VCN 内のトラフィックを有効にするためのルート ルールが使用されないためです。このシナリオでは、各 VCN のサブネットに接続しているファイアウォールでインターフェイスを設定します。

  以下の例では、Trust Subnet 内のユーザーが DB Subnet 内のデータへのアクセスを必要としています。DB Subnet CIDR ネクスト ホップに到達するルートを OCI で設定します。これにより、VM-Series ファイアウォールの Trust Subnet ネットワーク インターフェイスが指し示されます。



 ©2023 Palo Alto Networks, Inc.

OCI への VM-Series ファイアウォールのセットアップ準備

Oracle Cloud Infrastructure に VM-Series ファイアウォールをデプロイする前に、準備作業を完了する必要があります。

- Virtual Cloud Network（仮想クラウド ネットワーク）
- SSH 鍵
- 初期設定ユーザー データ

Virtual Cloud Network（仮想クラウド ネットワーク）

仮想クラウド ネットワーク（VCN）は、OCI 環境にセットアップする仮想プライベート ネットワークです。OCI に VM-Series ファイアウォールをデプロイするには、VCN に管理インターフェイス用の最低 3 つの仮想ネットワーク インターフェイス カード（VNIC）および 2 つのデータ インターフェイスが必要になります。

OCI は一連のルート テーブルを使用してトラフィックを VCN から送信します。各サブネットに 1 つのルート テーブルが追加されます。サブネットは VCN の区画です。ルート テーブルを指定しない場合、サブネットは VCN のデフォルト ルート テーブルを使用します。各ルート テーブル ルールが、CIDR に一致するトラフィックの、宛先 CIDR ブロックと次のホップ（ターゲット）を指定しています。宛先 IP アドレスが VCN で指定されている CIDR ブロック外部の場合には、OCI はサブネットのルート テーブルを使用します。VCN 内でトラフィックを有効にする場合にはルート ルールは不要です。トラフィックに重複するルールがある場合、OCI はルート テーブルで最も具体的なルールを使用して、トラフィックをルーティングします。

VCN を出ようとしているトラフィックに一致するルート ルールがない場合、トラフィックはドロップされます。

各サブネットにはルート テーブルが必要です。サブネットに追加されたルート テーブルは変更できません。ただし、ルート テーブルの作成後に、ルート テーブルのルールを追加、削除、編集することはできます。

SSH 鍵

初めてファイアウォールにログインする場合、SSH キー ペアを作成する必要があります。初めてファイアウォールにアクセスする場合、デフォルトのユーザー名とパスワードは使用できません。ファイアウォールが初めてのブートを完了したら、CLI を使ってファイアウォールにアクセスし、新しいユーザー名とパスワードを作成する必要があります。

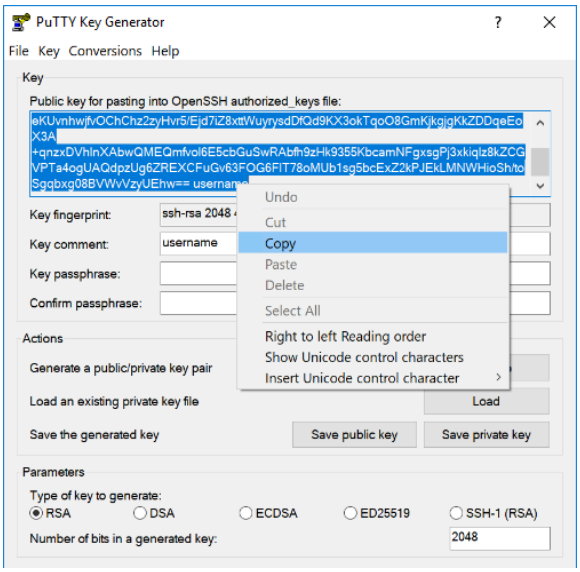
©2023 Palo Alto Networks, Inc.

1. SSH キーペアを作成し、お使いのオペレーティングシステムのデフォルトの場所に SSH キーペアを保存します。
   - Linux あるいは MacOS の場合、`ssh-keygen` を使って .ssh ディレクトリにキー ペアを作成します。
   - Windows の場合、PuTTYgen を使ってキー ペアを作成します。

     Key comment（キーのコメント）フィールドは VM-Series ファイアウォールに影響しません。デフォルトのもの（キーの作成日）を残しても、キー ペアの名前を覚えやすくなるコメントを入力してもかまいません。**Save private key**（秘密鍵の保存）ボタンを使って秘密鍵を .ssh ディレクトリに保存します。
2. 公開鍵の全体を選択します。
   - Linux あるいは MacOS：

     テキストエディタで公開鍵を開いて公開鍵をコピーします。
   - Windows：PuTTY Key Generator を使用して公開鍵を表示する必要があります。PuTTYgen を起動して Load（読み込み）をクリックし、.ssh ディレクトリに保存した秘密鍵を参照します。

     PuTTYgen で下にスクロールしながらキーの全体を選択していることを確認し、右クリックして Copy（コピー）を選択します。



初期設定ユーザー データ

VM-Series ファイアウォール インスタンスを設定する場合、次のブートストラップ パラメータを指定する必要があります。OCI はこの情報を使って、ファイアウォールの初期設定を行います。ファイアウォールにホスト名とライセンスを提供し、状況によってはファイアウォールを Panorama に接続します。

Panorama アプライアンスを保有しており、*Panorama* を使って *VM-Series* ファイアウォールを管理したい場合にのみ、*Panorama*関連フィールドが必要になります。

©2023 Palo Alto Networks, Inc.

フィールド	概要
hostname=	ファイアウォールのホスト名。
vm-auth-key=	Panorama でファイアウォールを登録するための、仮想マシン認証キー。
panorama-server=	PanoramaプライマリサーバーのIPv4あるいはIPv6アドレス。必須フィールドではありませんが、Panorama を使用してファイアウォールの一元管理を行う場合に設定します。
panorama-server-2=	PanoramaセカンダリサーバーのIPv4あるいはIPv6アドレス。必須フィールドではありませんが、推奨されます。
tplname=	Panorama テンプレート スタック名。Panorama サーバーの IP アドレスを追加する場合は、ベスト プラクティスとして、Panorama のテンプレート スタックにファイアウォールを割り当て、このフィールドにテンプレート スタック名を入力して、構成設定を一元的に管理してファイアウォールにプッシュできるようにすることをお勧めします。
dgname=	Panorama デバイス グループ名。Panorama サーバーの IP アドレスを追加する場合は、ベスト プラクティスとして、Panorama 上でデバイス グループを作成してから、このフィールドにデバイス グループ名を入力することで、ファイアウォールを論理的にグループ化して、ポリシー ルールをファイアウォールにプッシュすることができます。
authcodes=	Palo Alto Networks ライセンス サーバーで、VM-Series ファイアウォールにライセンスを供与するために使用されます。
op-command-modes=jumbo-frame	VM-Series ファイアウォールで、ジャンボフレーム モードを有効にするために使用されます。デフォルトで OCI は VM インスタンスをジャンボ モードでデプロイするため、最高のスループットを達成するために、VM-Series ファイアウォールをジャンボ モードで起動することをお勧めします。

©2023 Palo Alto Networks, Inc.

以下の形式で、OCI コンソールにブートストラップ パラメータを貼り付けます。

hostname=<*fw-hostname*>

vm-auth-key=<*auth-key*>

panorama-server=<*panorama-ip*>

panorama-server-2=<*panorama2-ip*>

tplname=<*template-stack-name*>

dgname=<*device-group-name*>

authocodes=<*firewall-authcode*>

op-command-modes=jumbo-frame

©2023 Palo Alto Networks, Inc.

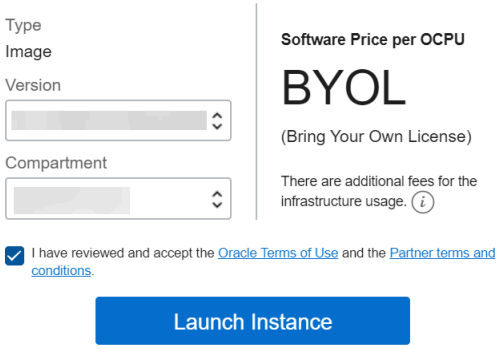
Oracle Cloud Marketplace からの VM-Series ファイアウォールのデプロイ

VM-Series ファイアウォールを Oracle Cloud Marketplace の OCI にデプロイするには、以下の手順を実行します。

STEP 1 | Oracle Cloud Marketplaceにログインします。

STEP 2 | Oracle Cloud Marketplace で VM-Series ファイアウォール アプリケーションを探します。

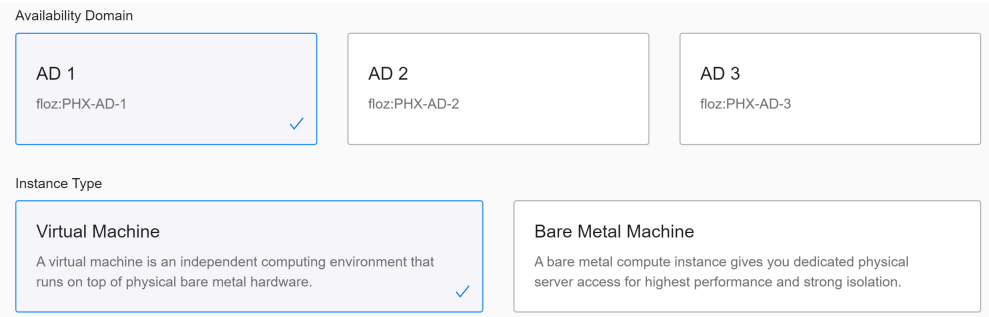
1. Palo AltoNetworks を検索すると、VM-Series ファイアウォールの製品リストが表示されます。
2. オファーを選択します。
3. **Get App**（アプリケーションの入手）をクリックします。
4. **Region**（リージョン）を選択して、**Sign In**（サインイン）をクリックします。
5. **Version**（バージョン）と**Compartment**（コンパートメント）を選択します。
6. Oracle and Partner（Oracle とパートナー） 条項に同意します。
7. **Launch Instance**（インスタンスの起動）をクリックします。



STEP 3 | VM-Series ファイアウォール インスタンスの分かりやすい **Name**（名前）を入力します。

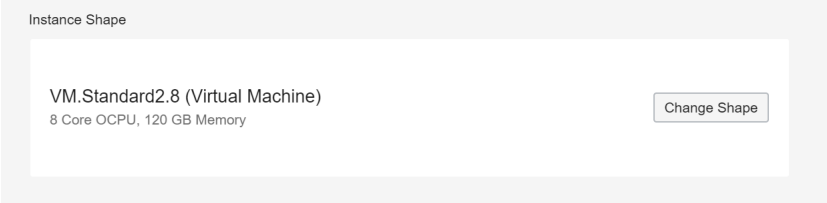
STEP 4 | **Availability Domain**（可用性ドメイン）で可用性ドメインを選択します。

STEP 5 | **Shape Type**（シェイプ タイプ）の下で **Virtual Machine**（仮想マシン）を選択します。

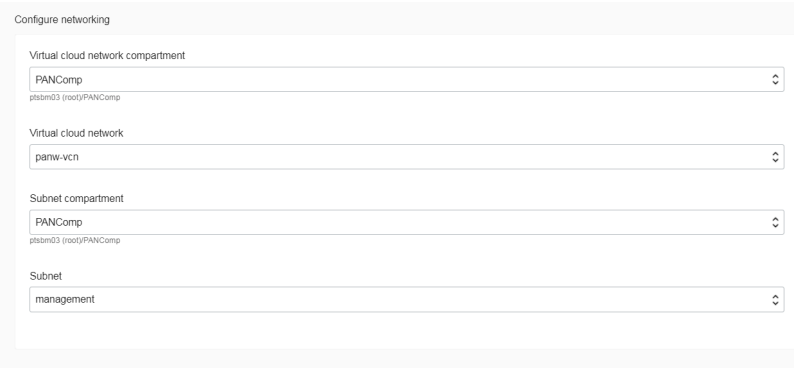


©2023 Palo Alto Networks, Inc.

STEP 6 | VM-Series ファイアウォール モデルに必要な CPU の数、RAM の容量、インターフェイスの数が指定されたシェイプを選択します。各種 Compute シェイプのリソースの量については、Compute Shapes のページを参照してください。各 VM-Series ファイアウォール モデルに必要なリソースの詳細については、「VM-Series のシステム要件」を参照してください。



STEP 7 | Networking（ネットワーキング）の下で、管理インターフェイスの **Virtual cloud network compartment**（仮想クラウド ネットワーク コンパートメント）、**Virtual cloud network**（仮想クラウド ネットワーク）、**Subnet compartment**（サブネット コンパートメント）、および **Subnet**（サブネット）を選択します。VM-Series ファイアウォール インスタンスを作成する際には、インターフェイスを 1 つのみを追加することができます。後ほど、他のインターフェイスを追加することができます。



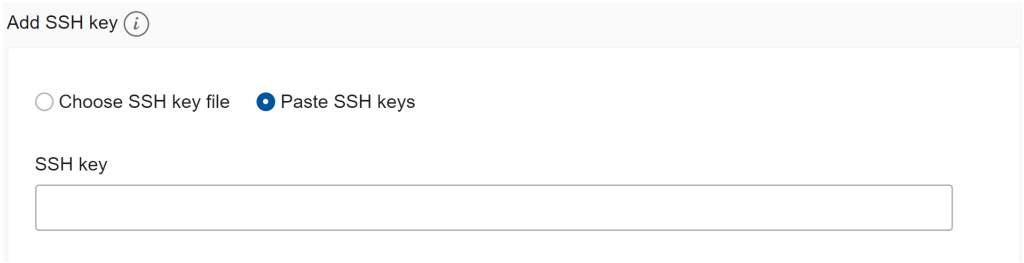
STEP 8 | （任意）デフォルト値よりも大きいサイズのブート ボリュームを設定します。デフォルトで、ブート ボリュームは 60GB に設定されています。ログのアタッチなどの機能をサポートするために、大きなブート ボリュームが必要な場合は、この手順を実行してください。

1. **Custom boot volume size（in GB）**（カスタム ブート ボリューム サイズ（GB））を選択します。
2. 60 以上の値を入力します。VM-Series ファイアウォールに必要な最低ハード ドライブ サイズは、60 GB になります。

©2023 Palo Alto Networks, Inc.

STEP 9 | SSH キーを追加します。

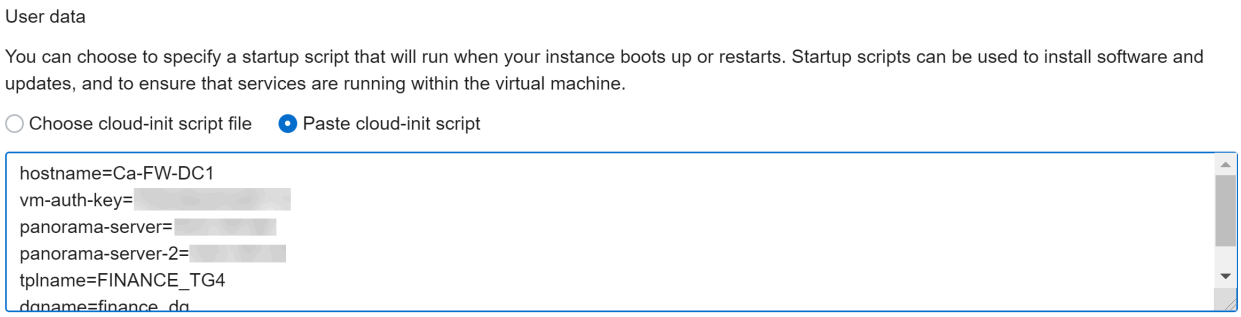
1. **Add SSH Key**（**SSH** キーの追加）で、**Paste SSH Key**（**SSH** キーの貼り付け）を選択します。
2. SSH キーをフィールドに貼り付けます。



STEP 10 | ブートストラップ パラメータを追加します。

1. **Show Advanced Options**（詳細オプションの表示）をクリックします。
2. **User data**（ユーザー データ）で、**Paste cloud-init script**（**cloud-init** スクリプトの貼り付け）を選択します。
3. フィールドに、ブートストラップ パラメータを貼り付けます。

```
hostname=<fw-hostname>
vm-auth-key=<auth-key>
panorama-server=<panorama-ip>
panorama-server-2=<panorama2-ip>
tplname=<template-stack-name>
dgname=<device-group-name>
authcodes=< firewall-authcode >
op-command-modes=jumbo-frame
```



STEP 11 | **Create**（作成）をクリックします。

VM-Series ファイアウォールの起動時に、OCI はプライマリ VNICを作成し、インスタンスにアタッチします。この VNIC は、インスタンス ネットワーク設定で指定したサブネットに存在しており、VM-Series ファイアウォールの管理インターフェイスに接続します。

©2023 Palo Alto Networks, Inc.

STEP 12 | ファイアウォールの新しい管理者パスワードを設定します。

1. 管理 IP アドレスを使用して、VM-Series ファイアウォールのコマンド ライン インターフェイス（CLI）に SSH で接続します。
2. 以下のコマンドを入力してファイアウォールにログインします。

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. 以下のコマンドを使用し、画面上のプロンプトに従って新しいパスワードを設定します。

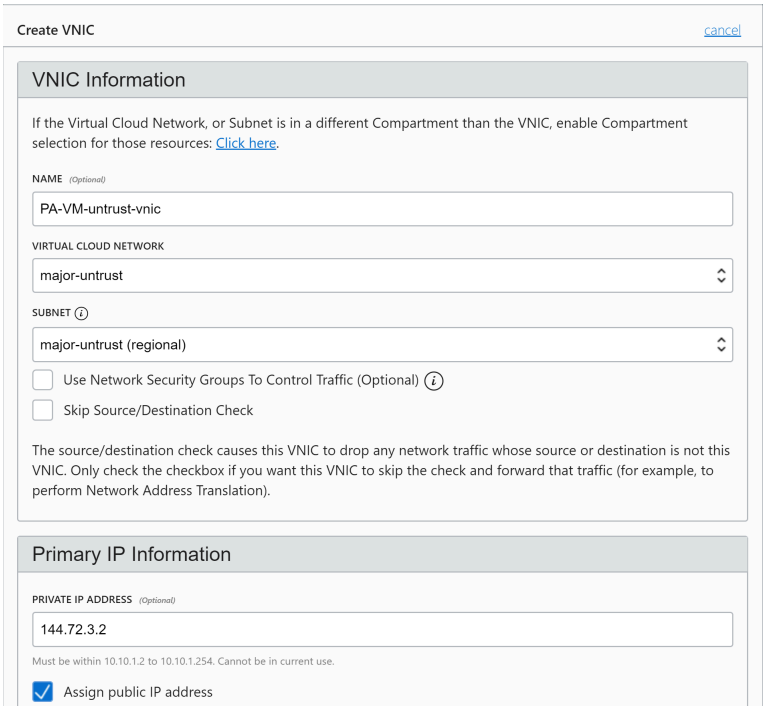
   configure

   set mgt-config users admin password

©2023 Palo Alto Networks, Inc.

STEP 13 | 各データ インターフェイスに対して、VM-Series ファイアウォール インスタンスに vNIC をアタッチします。ファイアウォールには、最低 2 つのデータ インターフェイス（untrust および trust）をアタッチする必要があります。

1. 新しく起動した VM-Series ファイアウォール インスタンスを選択し、**Attached VNICs**（アタッチされている **VNIC**） > **Create VNIC**（**VNIC** を作成）を選択します。
2. **Name**（名前）に分かりやすい vNIC 名を入力します。
3. **Virtual Cloud Network**（仮想クラウド ネットワーク）のドロップダウン リストから VCN を選択します。
4. **Subnet**（サブネット）のドロップダウン リストからサブネットを選択します。
5. **Private IP Address**（プライベート **IP** アドレス）を指定します。これは、vNIC の特定の IP を選択する場合にのみ必要な操作です。IP を指定しない場合、サブネットに割り当てた CIDR ブロックの IP アドレスが OCI により割り当てられます。
6. untrust サブネットなどの公開されている vNIC の場合は **Assign Public IP Address**（パブリック **IP** アドレスの割り当て）を選択します。
7. **Create VNIC**（**VNIC** を作成）をクリックします。
8. デプロイメントで必要な vNIC ごとにこの手順を繰り返します。



 ©2023 Palo Alto Networks, Inc.

STEP 14 | データプレーン ネットワーク インターフェイスをファイアウォール上のレイヤー 3 インターフェイスとして設定します。

1. ファイアウォールにログインします。
2. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）を選択します。
3. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「untrust-zone」 など）を定義し、**OK** をクリックします。
   - **IPv4** タブで、**Static**（静的）を選択します。
   - IP セクションで **Add**（追加）をクリックし、インターフェイスの IP アドレスとネットワーク マスクを入力します。この IP アドレスが、VCN の対応するサブネットに割り当てた IP アドレスと一致することを確認します。たとえば、untrust ゾーンにこのインターフェイスを追加する場合は、VCN で設定されている untrust vNIC IP アドレスを必ず割り当ててください。
4. 管理 vNIC を除く、VCN で設定されている vNIC ごとにこの手順を繰り返します。

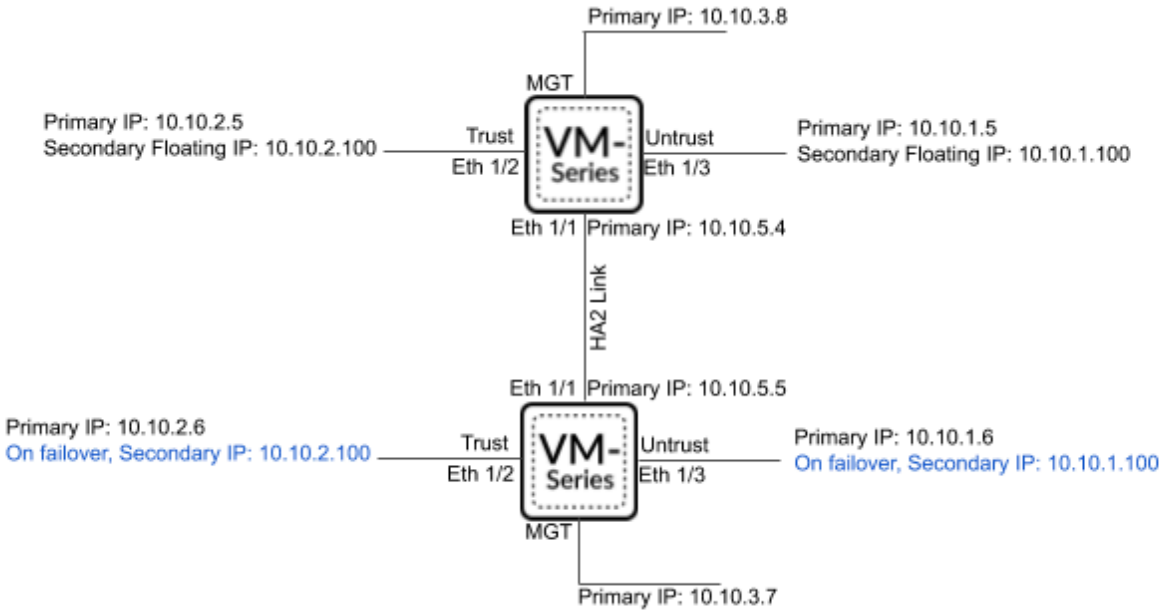
常に、インターフェイス リストの下部にあるインターフェイスのみを削除します。ファイアウォール インターフェイスを誤った順序で削除すると、ファイアウォールと *OCI* の間でインターフェイスの不一致が発生します。たとえば *5* つのデータ インターフェイスがあり、ファイアウォールでインターフェイス *2* を削除し、下部に新しいインターフェイスを追加するとします。ファイアウォールの再起動後には、新たに追加されたインターフェイスはリストの下部に配置されず、削除されたインターフェイス *2* の位置に配置されます。

©2023 Palo Alto Networks, Inc.

OCI でのアクティブ/パッシブ HA の設定

OCI でアクティブ/パッシブ高可用性（HA）構成の VM-Series ファイアウォールのペアを設定できます。アクティブ/パッシブ高可用性（HA）構成の の HA 設定での稼働時間を確保するため、ピア間で迅速に移行可能なセカンダリ フローティング IP アドレスを作成する必要があります。アクティブ ファイアウォールがダウンすると、フローティング IP アドレスはアクティブ ファイアウォールからパッシブ ファイアウォールに移動します。これによってパッシブ ファイアウォールがアクティブ ピアになるとすぐに、トラフィックをスムーズに保護できます。フローティング IP アドレスの他に、HA ピアにはデータを同期し状態情報を維持するために HA リンク（コントロール リンク（HA1）とデータ リンク（HA2））も必要です。

FIPS モードの *OCI* 用 *VM-Series* ファイアウォールは、高可用性をサポートしていません。



フェイルオーバー時にファイアウォールのフローティング IP アドレスの移行を可能にするには、OCI でダイナミック グループにファイアウォール インスタンスを配置する必要があります。ダイナミック グループでは、ファイアウォール インスタンスをプリンシパル アクターとしてグループ化して、ダイナミック グループ内のインスタンスに OCI サービスに対する API コールを許可するポリシーを作成することができます。一致するルールを使って、HA ピア インスタンスをダイナミック グループに追加し、次にある VNIC から別の VNIC に移行するフローティング IP 用のポリシーを作成します。

HA ペア内の VM-Series ファイアウォールは両方とも、同じ数のネットワーク インターフェイスを保有する必要があります。各ファイアウォールには、最低 4 つのインターフェイス（管理、trust、untrust、HA）が必要です。デプロイ環境のニーズに応じて、追加のデータ インターフェイスを設定できます。

©2023 Palo Alto Networks, Inc.

- 管理インターフェイス– プライマリ インターフェイスに関連付けられているプライベートおよびパブリック IP アドレス。管理インターフェイスのプライマリ IP アドレスを、ピア間の HA1 インターフェイス用の IP アドレスとして使用することができます。専用の HA インターフェイスが必要な場合は、各インターフェイスに追加のインターフェイスをアタッチする必要があります（それぞれ合計 5 つのインターフェイス）。
- **untrust** および **trust** インターフェイス–アクティブな HA ピア上のこれらのデータ インターフェイスは、プライマリおよびセカンダリ IP アドレスが必要になります。フェイルオーバー発生時には、パッシブ HA ピアがアクティブ状態に移行すると、セカンダリ プライベート IP アドレスが以前のアクティブ ピアからデタッチされ、現在アクティブな HA ピアにアタッチされます。
- **HA2** インターフェイス–このインターフェイスは、各 HA ピア上に単一の IP アドレスを保有しています。HA2 インターフェイスは、ピアがセッションを同期し、テーブル、IPsec セキュリティ アソシエーション、ARP テーブルを転送するときに使用するデータ リンクです。

©2023 Palo Alto Networks, Inc.

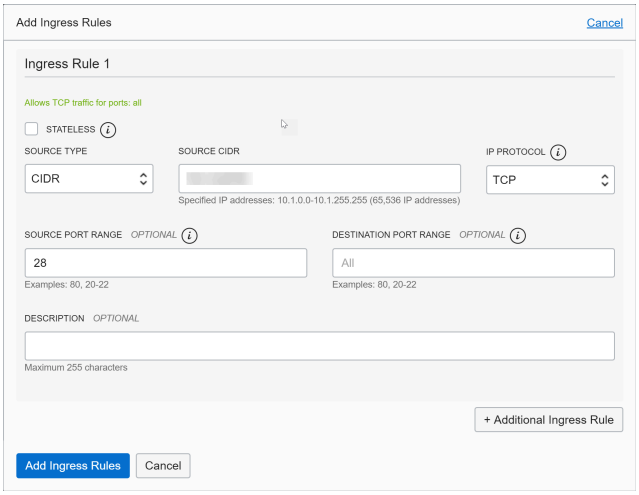
STEP 1 | Oracle Cloud Marketplace からの VM-Series ファイアウォールのデプロイを行って、HA 用のネットワーク インターフェイスを設定します。

1. （任意）各 HA ピアに、専用の HA1 インターフェイスを設定します。
   1. OCI コンソールから、**Compute**（計算） > **Instances**（インスタンス）を選択して、アクティブ ピアのインスタンス名をクリックします。
   2. **Attached VNICs**（アタッチされている **VNIC**）を選択して、**Create VNIC**（**VNIC** の作成）をクリックします。
   3. HA1 インターフェイスに対する、分かりやすい名前を入力します。
   4. VCN とサブネットを選択します。
   5. プライベート IP アドレスを入力します。
   6. **Create VNIC**（**VNIC** を作成）をクリックします。
   7. パッシブ ピア インスタンスで、この作業を繰り返します。
2. 各 HA ピア上に、HA2 インターフェイスを設定します。
   1. OCI コンソールから、**Compute**（計算） > **Instances**（インスタンス）を選択して、アクティブ ピアのインスタンス名をクリックします。
   2. **Attached VNICs**（アタッチされている **VNIC**）を選択して、**Create VNIC**（**VNIC** の作成）をクリックします。
   3. HA2 インターフェイスに対する、分かりやすい名前を入力します。
   4. VCN とサブネットを選択します。HA2 インターフェイスは、データ インターフェイスと異なるサブネットに存在している必要があります。
   5. プライベート IP アドレスを入力します。
   6. **Create VNIC**（**VNIC** を作成）をクリックします。
   7. パッシブ ピア インスタンスで、この作業を繰り返します。
3. アクティブ ピア上のデータプレーン インターフェイスに、セカンダリ IP アドレスを追加します。
   1. OCI コンソールから、**Compute**（計算） > **Instances**（インスタンス）を選択して、アクティブ ピアのインスタンス名をクリックします。
   2. **Attached VNICs**（アタッチされている **VNIC**）を選択して、untrust VNIC をクリックします。
   3. **IP Addresses**（**IP** アドレス）を選択して、**Assign Private IP Address**（プライベート **IP** アドレスの割り当て）をクリックします。
   4. IP アドレスを入力して **Assign**（割り当て） をクリックします。
   5. アクティブ ピア上の各データプレーン インターフェイスに対して、この手順を繰り返します。

©2023 Palo Alto Networks, Inc.

STEP 2 | HA ピアがデータを同期化して、状態情報を管理できるように、セキュリティ ルールを作成します。デフォルトで OCI は、ICMP トラフィックのみを許可しています。必要な HA ポートを開く必要があります。

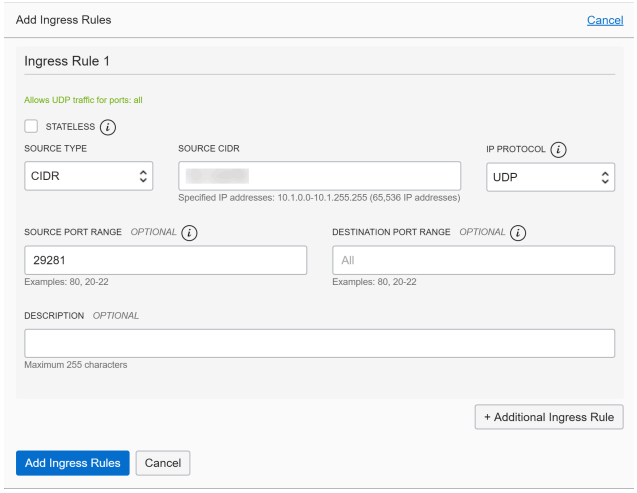
1. HA1 インターフェイス用のポートを開きます。
   1. OCI コンソールから、**Networking**（ネットワーク） > **Virtual Cloud Networks**（仮想クラウド ネットワーク）を選択して、VCN を選択します。
   2. **Subnets**（サブネット）を選択して、HA1 インターフェイスが存在しているサブネットを選択します。
   3. **Security Lists**（セキュリティ リスト）を選択して、デフォルトのセキュリティ リストをクリックして、それを編集します。
   4. **Add Ingress Rule**（入口ルールの追加）をクリックします。
   5. HA ピア HA1 ポート IP アドレスを含む、**Source CIDR**（ソース **CIDR**）を入力します。
   6. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **TCP** を選択します。
   7. **+Additional Ingress Rule**（追加の入口ルール）をクリックします。TCP ポート 28260 および 28769 向けに、2 つの追加ルールを作成する必要があります。
   8. VM-Series ファイアウォールの HA1 リンクの暗号化が有効になっている場合、ICMP および TCP ポート 28 用に追加のルールを作成します。
   9. **Add Ingress Rules**（入口ルールの追加）をクリックします。



2. HA2 インターフェイス用のポートを開きます。
   1. OCI コンソールから、**Networking**（ネットワーク） > **Virtual Cloud Networks**（仮想クラウド ネットワーク）を選択して、VCN を選択します。
   2. **Subnets**（サブネット）を選択して、HA2 インターフェイスが存在しているサブネットを選択します。
   3. **Security Lists**（セキュリティ リスト）を選択して、デフォルトのセキュリティ リストをクリックして、それを編集します。
   4. **Add Ingress Rule**（入口ルールの追加）をクリックします。

©2023 Palo Alto Networks, Inc.

5. HA ピア HA2 ポート IP アドレスを含む、**Source CIDR**（ソース **CIDR**）を入力します。
6. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **UDP** または **IP** を選択します。
7. 伝送モードが UDP の場合、**Source Port Name**（ソース ポート名）に **29281** を入力します。伝送モードが IP の場合、**Source Port Name**（ソース ポート名）に **99** を入力します。
8. **Add Ingress Rules**（入口ルールの追加）をクリックします。

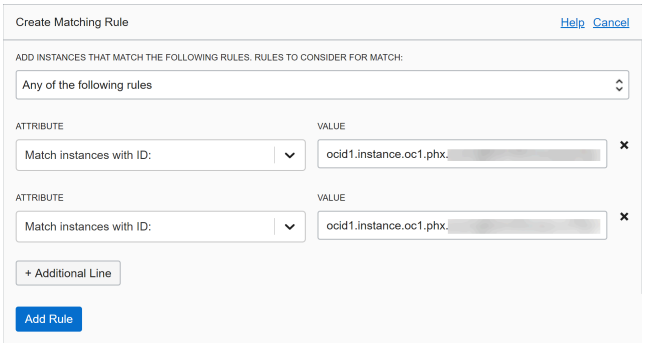


STEP 3 | 両方の HA ピアをダイナミック グループに追加して、HA ピアのフローティング IP アドレスの移行を許可するポリシーを作成します。ダイナミック グループ一致ルールを作成する

©2023 Palo Alto Networks, Inc.

には、HA ピア インスタンスの OCID が必要になるため、それらを手元に用意してルールビルダーに貼り付けてください。

1. ダイナミック グループを作成します。
    1. OCI コンソールから、**Identity**（**ID**） > **Dynamic Groups**（ダイナミック グループ） > **Create Dynamic Group**（ダイナミック グループの作成）を選択します。
    2. ダイナミック グループの、分かりやすい**Name**（名前）を入力します。
    3. **Rule Builder**（ルール ビルダー）をクリックします。
    4. 最初のドロップダウンで、**Any of the following rules**（次の任意のルール）を選択します。
    5. **Attributes**（属性）ドロップダウンから**Match instances with ID:**（インスタンスを ID と照合）を選択して、いずれかのピア OCID を **Value**（値）フィールドに貼り付けます。
    6. **+Additional Line**（追加の行）をクリックします。
    7. **Attributes**（属性）ドロップダウンから**Match instances with ID:**（インスタンスを ID と照合）を選択して、もう一方のピア OCID を **Value**（値）フィールドに貼り付けます。
    8. **Add Rule**（ルールの追加）をクリックします。

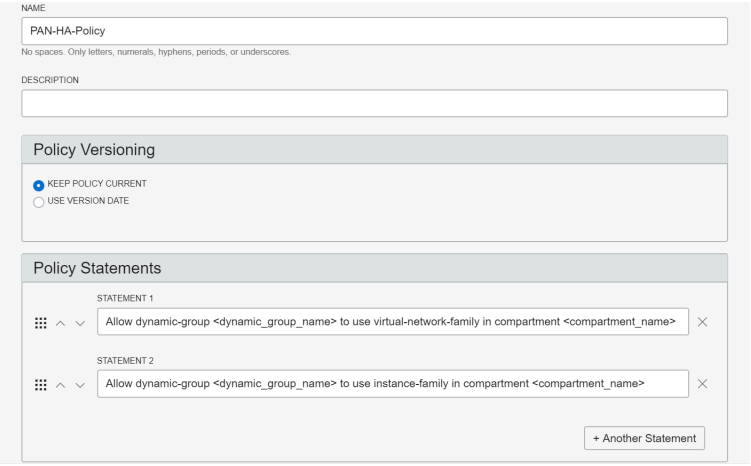


    9. **Create Dynamic Group**（ダイナミック グループの作成）をクリックします。
2. ポリシー ルールを作成します。
    1. OCI コンソールから、**Identity**（**ID**） > **Policies**（ポリシー） > **Create Policy**（ポリシーの作成）を選択します。
    2. **Name**（名前）に、分かりやすいポリシー名を入力します。
    3. 最初のポリシー ステートメントを入力します。

        Allow dynamic-group *<dynamic_group_name>* to use virtual-network-family in compartment *<compartment_name>*
    4. **+Another Statement**（他のステートメント）をクリックします。
    5. 2 番目のポリシー ステートメントを入力します。

        Allow dynamic-group *<dynamic_group_name>* to use instance-family in compartment *<compartment_name>*
    6. **Create**（作成）をクリックします。

©2023 Palo Alto Networks, Inc.



STEP 4 | ファイアウォール上でインターフェイスを設定します。HA2 データ リンクと、untrust および trust インターフェイス向けに最低 2 つの Layer 3 インターフェイスを設定する必要があります。最初の HA ピアでこのワークフローを完了して、次に 2 番目の HA ピアで手順を繰り返してください

1. ファイアウォール インターフェイスにログインします。
2. （任意）管理インターフェイスを HA1 として使用している場合、インターフェイス IP タイプをスタティックに設定して、DNS サーバーを設定する必要があります。
   1. **Device**（デバイス） > **Setup**（セットアップ） > **Interfaces**（インターフェイス） > **Management**（管理）を選択します。
   2. **IP Type**（**IP** タイプ）に**Static**（スタティック）を設定します。
   3. VM-Series ファイアウォール インスタンスのプライマリ VNIC のプライベート **IP address**（**IP** アドレス）を入力します。
   4. **OK** をクリックします。
   5. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
   6. **Edit**（編集）をクリックします。
   7. **Primary DNS Server**（プライマリ **DNS** サーバー）の IP アドレスを入力します。
   8. **OK** をクリックします。
   9. 変更を **Commit (**コミット**)**します。
3. **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、untrust インターフェイスをクリックします。この例で、HA2 インター

 ©2023 Palo Alto Networks, Inc.

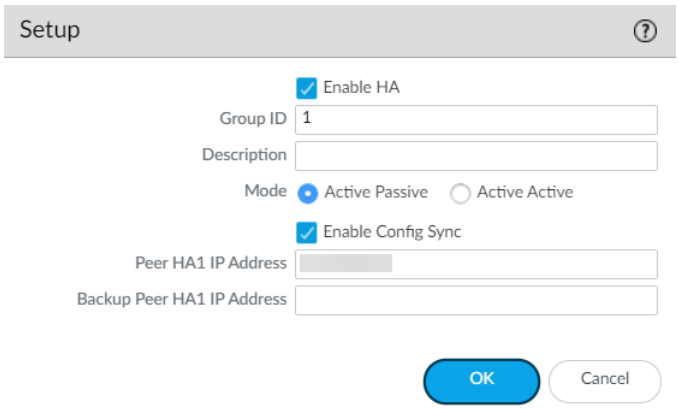
フェイスは 1/1、trust インターフェイスは ethernet 1/2、untrust インターフェイスは ethernet 1/3 になります。

4. **ethernet 1/1** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**HA**
5. **ethernet 1/2** [イーサネット1/1] のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「trust-zone」 など）を定義し、**OK** をクリックします。
   - **IPv4** タブで、**Static**（静的）を選択します。
   - IP セクションで **Add**（追加）をクリックし、インターフェイスのプライマリ IP アドレスとネットワーク マスクを入力します。この IP アドレスが、VCN の対応するサブネットに割り当てた IP アドレスと一致することを確認します。たとえば、trust ゾーンにこのインターフェイスを追加する場合は、VCN で設定されている trust vNIC IP アドレスを必ず割り当ててください。
   - IP セクションで **Add**（追加）をクリックし、セカンダリ フローティング IP アドレスとネットワーク マスクを入力します。
6. **ethernet 1/3** のリンクをクリックし、以下のように設定します。
   - **Interface Type** [インターフェイス タイプ] :**Layer3**
   - **Config**（設定）タブで、デフォルト ルーターにインターフェイスを割り当てます。
   - **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。新しいゾーン（「untrust-zone」 など）を定義し、**OK** をクリックします。
   - **IPv4** タブで、**Static**（静的）を選択します。
   - IP セクションで **Add**（追加）をクリックし、インターフェイスのプライマリ IP アドレスとネットワーク マスクを入力します。この IP アドレスが、VCN の対応するサブネットに割り当てた IP アドレスと一致することを確認します。たとえば、untrust ゾーンにこのインターフェイスを追加する場合は、VCN で設定されている untrust vNIC IP アドレスを必ず割り当ててください。
   - IP セクションで **Add**（追加）をクリックし、セカンダリ フローティング IP アドレスとネットワーク マスクを入力します。

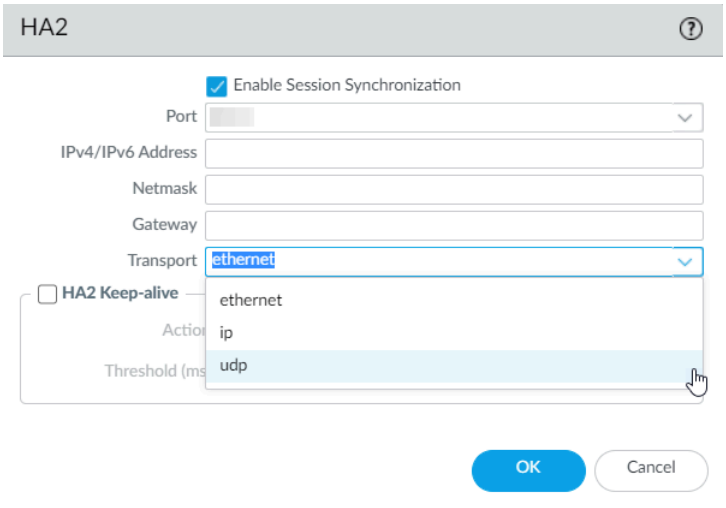
©2023 Palo Alto Networks, Inc.

STEP 5 | HA を有効にします。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General** （全般）を選択します。
2. Setup（セットアップ）の設定を編集します。
3. パッシブ ピアのプライベート IP アドレスを **Peer HA1 IP address**（ピア **HA1 IP** アドレス）フィールドに入力します。
4. **OK** をクリックします。



5. （任意）コントロール リンク（HA1）を編集します。コントロール リンクに管理インターフェイスを使用する予定がなく、インターフェイス（ethernet 1/4 など）を追加している場合は、このセクションを編集して、そのインターフェイスを HA1 通信に使用するインターフェイスとして選択します。
6. データ リンク（HA2）を編集し、**Port**（ポート）として ethernet 1/1 を使用するように設定し、アクティブ ピアの IP アドレスと、サブネットの **Gateway**（ゲートウェイ）IP アドレスを追加します。
7. Transport（伝送）ドロップダウンから、**IP** または **UDP** を選択します。Ethernet はサポートされていません。



8. **OK** をクリックします。

STEP 6 | 変更を **Commit (コミット)**します。

©2023 Palo Alto Networks, Inc.

STEP 7 | パッシブ HA ピア上で、ステップ 4 とステップ 5 を繰り返します。

STEP 8 | 両方のファイアウォール上で HA の設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のファイアウォールで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブな HA ピアで、**Sync to peer**（ピアに同期）をクリックします。
3. ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **Passive**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。
   - アクティブ ファイアウォール: ローカル ファイアウォールの状態が **Active**、**Running Config**（実行コンフィグ） が Synchronized と表示されます。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Alibaba Cloud での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールを Alibaba Cloud にデプロイすることで、Alibaba Cloud 内で作成するネットワークを保護できます。VM-Series ファイアウォールをデプロイし、インターネットに公開されているアプリケーションやハイブリッド クラウド デプロイメントを保護できます。

- Alibaba Cloud での VM-Series ファイアウォール
- Alibaba Cloud での VM-Series ファイアウォールの最小システム要件
- Alibaba Cloud での VM-Series ファイアウォールのデプロイの準備
- Alibaba Cloud での VM-Series ファイアウォールのデプロイ

Alibaba Cloud での VM-Series ファイアウォール

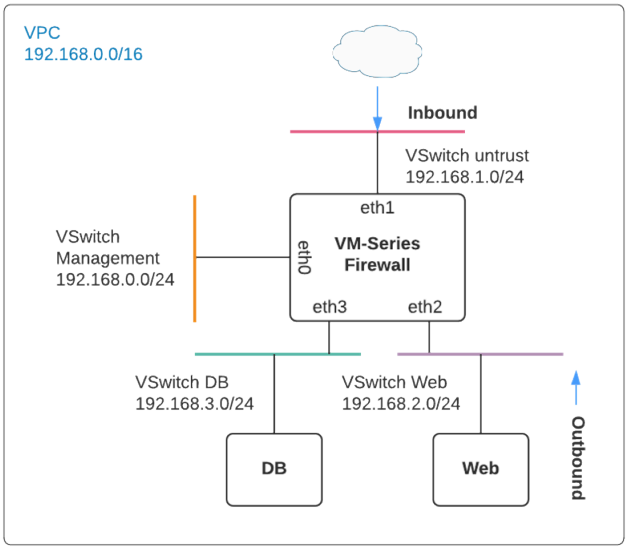
VM-Seriesファイアウォールを、Alibaba Cloud内の保護されたインバウンド/アウトバウンド、North-Southトラフィックにデプロイすることができます。

Alibaba Cloud ではサブネット ルーティングがサポートされていないため、同一 ***VPC*** 内での ***East-West*** トラフィックの保護はサポートされていません。

Alibaba Cloud上のVM-Seriesファイアウォールは KVMハイパーバイザーで動作し、十分なリソースのあるAlibaba Cloudインスタンスを選択した場合には最大8つのネットワーク インターフェイスをサポートします（「Alibaba Cloud での VM-Series ファイアウォールの最小システム要件」を参照）。

Alibaba Cloud上のVM-Seriesファイアウォールは、BYOLライセンスとAlibaba Cloud International RegionsおよびMainland China上のVM-Series ELAをサポートしています。PAYGライセンスは現時点ではサポートされていません。

Alibaba Cloudで、VPCは論理的に仮想ネットワークを分離しています。VPCを作成したら、次の図のようにVSwitchを作成して仮想プライベート ネットワークをさらにセグメント化できます。インバウンド トラフィックを保護するため、ファイアウォールで DNAT と SNAT の両方を設定する必要があります。



VPC外のクライアントからのインバウンド トラフィックは、VM-Seriesファイアウォールのuntrustインターフェイスに送信されます。ファイアウォールはトラフィックを検査し、Trustインターフェイス経由でアプリケーションにこのトラフィックを送信します。アプリケーションから返されたトラフィックは、VM-SeriesファイアウォールのTrustインターフェイスを通過する必要があります。ファイアウォールでは、リターントラフィックフローが検査され、Untrustインターフェイスに送信されます。

一般的にアウトバウンド トラフィックは、外部アプリケーションが起源のトラフィックです。一般に、VPC 内のインターネットに面するトラフィックは（EIP がアタッチされた）NAT ゲートウェイにルーティングされます。そのためには、VPCルーティングテーブルにデフォルトゲートウェイのルートを追加し、VM-Seriesファイアウォールのアプリケーションサブネットの IPアド

©2023 Palo Alto Networks, Inc.

レスを次のホップとして指定します。UntrustインターフェイスIPを使用してSNATを設定し、インターネットから戻るトラフィックが VM-Series ファイアウォールを通過するようにします。

サンプル設定については、「Alibaba Cloud での North-South トラフィックの保護」を参照してください。

©2023 Palo Alto Networks, Inc.

Alibaba Cloud での VM-Series ファイアウォールの最小システム要件

Alibaba Cloudで、KVMハイパーバイザー上にVM-Seriesファイアウォールをデプロイすることができます（「VM-Series デプロイメント」を参照）。

- VM-Series ファイアウォールのソフトウェア要件
- VM-Series ファイアウォールで推奨される Alibaba Cloud インスタンス タイプ
- Alibaba Cloud CLI

VM-Series ファイアウォールのソフトウェア要件

Alibaba CloudでVM-Seriesのデプロイ作業を完了するために必要な、ソフトウェアおよびライセンスがあることを確認してください。

- VM-SeriesファイアウォールをAlibaba Cloudにデプロイするには、Alibaba Marketplaceから入手したVM-Seriesイメージを使用する必要があります。イメージには、PAN-OSバージョン10.0.3とVM-Seriesプラグインバージョン2.0.3が含まれています。
- デプロイする前に、VM-Series ELA または BYOL ライセンス、キャパシティ ライセンス、およびサブスクリプション バンドルを選択します。「VM-Series モデルのライセンスタイプ」を参照してください。
- デプロイを完了するには、VM-SeriesファイアウォールにSSHで接続できなければなりません。OSがSSHをサポートしていない場合は、Puttyなどのサードパーティ製ソフトウェアをインストールしてください。

VM-Series ファイアウォールで推奨される Alibaba Cloud インスタンス タイプ

VM-Series ファイアウォールを作成する前に、ご使用の VM-Series モデルの最小システム要件に対応した Elastic Compute Service（ECS）インスタンス タイプを選択します。インスタンス タイプのドキュメントを参照して、選択する ECS インスタンス タイプに、ご使用のネットワーク設定を保護するためのリソースが含まれていることを確認します。

VM-Series モデル	Elastic Compute Service インスタンス タイプ
VM-100IPv6	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-300IPv6	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-500IPv6	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700IPv6	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

©2023 Palo Alto Networks, Inc.

Alibaba Cloud CLI

Aliyun バージョン 3.0.4 以降「Aliyun コマンド ライン インターフェイスを使用するための準備」を参照してください。

©2023 Palo Alto Networks, Inc.

Alibaba Cloud での VM-Series ファイアウォールのデプロイの準備

この作業では Aliyun CLI を使用して VM-Series ファイアウォール用の VPC と VSwitch を作成しますが、作業を開始する前にネットワークについて計画しておく必要があります。保護するアプリケーションを評価し、North-South トラフィックの検査と保護のために VM-Series ファイアウォールをデプロイする位置を決定します。

- ライセンスの選択とネットワークの計画
- Aliyun コマンド ライン インターフェイスを使用するための準備

ライセンスの選択とネットワークの計画

保護する必要があるアプリケーションを評価し、VM-Series ファイアウォールに対しインバウンドおよびアウトバウンド アプリケーション トラフィックの検査を許可するネットワークを作成します。

STEP 1 | VPC を計画して設計します。

1. VPC と VSwitch の CIDR ブロックを含むネットワークを計画します。

   手順の例については、「関連ドキュメント」を参照してください。
2. IPアドレスのプランニングを行います。特定のアドレスまたはアドレス範囲が必要な場合は、『Elastic IP Address User Guide』を参照してください。
3. セキュリティ グループを計画します。

STEP 2 | アプリケーションとネットワークの設定を評価し、アプリケーションとネットワークを保護するために必要なファイアウォールのキャパシティを計算します。

STEP 3 | VM-Series ファイアウォール ライセンスを取得します。

VM-Series ファイアウォールをインストールする際にはライセンスは不要ですが（インストール後にライセンスをアクティベートできます）、ファイアウォールをデプロイする前に、適切な VM-Series モデルと ECS インスタンス タイプを選択する必要があります。

1. VM-Series モデルを選択します。

   VM-Series モデルと ***Alibaba Cloud*** インスタンスに十分なリソースがある場合には、***VM-Series*** ファイアウォールでは最大 *8* つのインターフェイスがサポートされます。モデルを使用できます。

   選択した VM-Series モデルを使用していずれか 1 つを選択します。
2. ニーズに対応する VM-Series キャパシティ ライセンスを選択します。
3. BYOL サブスクリプション バンドルをまだ購入していない場合は、購入します。VM-Seriesサブスクリプションの認証コードを受け取ります。デプロイ時にこれを指定する必要があります。

©2023 Palo Alto Networks, Inc.

STEP 4 | VM-Seriesファイアウォールにアクセスするための、Alibabaアカウントと許可の設定方法を計画します。まず、「セキュリティのFAQ」を参照し、またインスタンスRAMロールについて学習してください。

Aliyun コマンド ライン インターフェイスを使用するための準備

この章はECS Consoleに重点を置いていますが、ECS Consoleで実行するすべての操作は、Aliyun コマンド ライン インターフェイスからも実行できます。VM-Series ファイアウォールを使用して Alibaba Cloud の負荷分散機能を保護するには、CLI が必要です。

最新バージョンの Aliyun（Alibaba Cloud のコマンド ライン インターフェイス）をインストールして設定します。

STEP 1 | AccessKey を作成し、アクセス キー ID とシークレットを安全な場所に保管します。

STEP 2 | Aliryun のサポートされているバージョンを https://github.com/aliyun/aliyun-cli からダウンロードします。

STEP 3 | Aliyun をインストールします。

STEP 4 | Aliyun を設定します。

この設定作業ではアクセス キー情報やその他の情報の入力が求められます。

デプロイ環境でストレージバケットを使用している場合、リージョンはご利用のバケットのリージョンと一致している必要があります。

```
aliyun configure
Configuring profile '' in '' authenticate mode...
Access Key Id [*************8rq]: *************8rq
Access Key Secret [****************************tM2]:
****************************tM2
Default Region Id [us-west-1]: us-west-1
Default Output Format [json]: json (Only support json))
Default Language [zh|en] en: en
Saving profile[] ...Done.
 available regions:
...
```


©2023 Palo Alto Networks, Inc.

Alibaba Cloud での VM-Series ファイアウォールのデプロイ

VM-Series ファイアウォールでは、最小限でも 3 つのインターフェイス（管理、trust、untrust）が想定されます。Alibaba Cloud VPC を作成する場合、この VPC は論理的に切り離されています。仮想プライベート ネットワークをサブネットにセグメント化するには、専用の CIDR ブロックを持つ VSwitch を作成します。VM-Series ファイアウォールには複数のインターフェイスがあるので、すべてのサブネットのトラフィックを検査できます。

一般に外部インバウンド トラフィックは VM-Series ファイアウォールの untrust インターフェイスに入ります。ファイアウォールはインバウンド トラフィックを検査し、trust インターフェイス経由でアプリケーションにこのトラフィックを送信します。アプリケーションからのリターン トラフィックは、ファイアウォールのTrustインターフェイスに向かいます。ファイアウォールはそのリターントラフィックを検査して、Untrustインターフェイスに送信します。

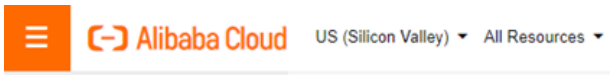
以下のタスクでは、コンソールを使用して VM-Series ファイアウォール インフラストラクチャを作成する手順を説明します。

- VPC の作成とネットワークの設定
- VM-Series ファイアウォールの作成と設定
- Alibaba Cloud での North-South トラフィックの保護
- Alibaba Cloud での負荷分散の設定

VPC の作成とネットワークの設定

Alibaba Cloud コンソールを使用して、VPC、VSwitch、セキュリティ グループ、セキュリティ グループ ルールを作成します。

STEP 1 | VPC コンソールを開き、メニューから該当するリージョンを選択します。選択するリージョンは、Palo Alto Networksがサポートするいずれかのインスタンスタイプを提供していることに注意してください。



STEP 2 | Alibaba Cloud Console ホームページから、**Products and Services**（製品とサービス） > **Networking**（ネットワーキング） > **Virtual Private Cloud**（仮想プライベートクラウド）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 3 | **VCN** を作成します。

このステップでは、VPC と管理 VSwitch、Untrust VSwitch、および Trust VSwitch を作成します。ECS コンソールにより同じフォームを使ってVPC とスイッチが作成されます。

1. **Create VPC**（**VPC**の作成）を選択します。

   VPC 名、IPv4 CIDR ブロック、説明を指定します。「VPCの作成」を参照してください。

プロパティ	値
Name（名前）	指定内容は任意
IPv4 CIDR Bock	指定内容は任意。「CIDRブロックのFAQ」を参照してください。
Resource Group（リソースグループ）	指定内容は任意。

2. **Create VSwitch**（**VSwitch**の作成）を選択します。
   - この VSwitch に **`Management`** という名前を付けます。
   - **Zone**（ゾーン）を選択し、VPC用に指定したブロックのサブセットとなる**IPv4 CIDR Block**を指定して、**Description**（説明）を入力します。
   - 下部の**Add**（追加）をクリックして、他のvSwitchを追加します（**OK**は、すべてのVSwitchesを追加するまでクリックしないでください）。

   「VSwitchの作成」を参照してください。
3. Untrust VSwitch を同じ方法で**Add**（追加）します。
4. Trust VSwitch を**Add**（追加）します。
5. **OK**をクリックします。

   VPC詳細を参照し、必要に応じて変更を行ってから、**Complete**（完了）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 4 | セキュリティ グループとセキュリティ グループ ルールを作成します。

- Alibaba Cloudコンソールホームページから、**Elastic Compute Service** > **Networking & Security**（ネットワークとセキュリティ） > **Security Groups**（セキュリティグループ）を選択します。
- 右上にある **Create Security Group**（セキュリティ グループの作成）を選択します。

1. 管理セキュリティ グループを作成します。

   次のフィールドの入力方法については、「セキュリティグループの作成」を参照してください。

プロパティ	値
テンプレート	カスタマイズ
Security Group Name（セキュリティグループ名）	Management（管理）
Security Group Type（セキュリティグループタイプ）	Basic（基本）
Network Type（ネットワーク タイプ）	VPC
VPC	前に作成した VPC を選択します。
Resource Group（リソースグループ）	指定内容は任意

   - フォームにすべての情報を入力して **OK** をクリックします。

     ECS コンソールで、このセキュリティ グループのルールを作成するよう促されます。このタスクは、VM-Seriesファイアウォールを立ち上げるためのいくつかの基本的なセキュリティグループを説明しています。ネットワーク セキュリティ要件を強制的に適用する他のルールを作成できます。

2. **Create Rules Now**（今すぐルールを作成）を選択して、HTTPSおよびSSH用のルールを作成します。

   Inbound（インバウンド）タブを選択し、**Add Security Group Rule**（セキュリティグループルールの追加）をクリックします。

   - このセキュリティグループで HTTPS を許可するインバウンドルールを作成します。以下に例を示します。

プロパティ	値
Rule Direction（ルール方向）	Inbound（インバウンド）

©2023 Palo Alto Networks, Inc.

プロパティ	値
Action（アクション）	Allow [許可]
Protocol Type（プロトコルタイプ）	HTTPS（443）
Priority（優先順位）	100
Authorization Type（認証タイプ）	「セキュリティグループルールの追加」を参照してください。
Authorization Object（認証オブジェクト）	

- 管理インターフェイスでのSSHを許可するインバウンドルールを作成するために、**Add Security Group Rule**（セキュリティグループルールの追加）をクリックします。

プロパティ	値
Rule Direction（ルール方向）	Inbound（インバウンド）
Action（アクション）	Allow [許可]
Protocol Type（プロトコルタイプ）	Customized TCP（カスタマイズされたTCP）
Port Range（ポート範囲）	1/65535
Authorization Type（認証タイプ）	「セキュリティグループルールの追加」を参照してください。
Authorization Object（認証オブジェクト）	

OK をクリックし、**Back**（戻る）を選択してSecurity Groups（セキュリティ グループ）ページに戻ります。

3. **Create Security Group**（セキュリティグループの作成）を選択して、Untrustセキュリティグループを作成します。

   ルールの作成を促されたら、Untrust セキュリティ グループのルールを作成します。

プロパティ	値
Rule Direction（ルール方向）	Inbound（インバウンド）
Action（アクション）	Allow [許可]

©2023 Palo Alto Networks, Inc.

プロパティ	値
Protocol Type（プロトコルタイプ）	Custom TCP（カスタムTCP）
Port Range（ポート範囲）	1/65535
Priority（優先順位）	100
Authorization Type（認証タイプ）	「セキュリティグループルールの追加」を参照してください。
Authorization Object（認証オブジェクト）	

OK をクリックし、**Back**（戻る）を選択してSecurity Groups（セキュリティ グループ）ページに戻ります。

4. Trust セキュリティ グループを作成します。

   プロンプトが表示されたら、**Add Security Group Rule**（セキュリティグループルールの追加）をクリックして、Untrustルールを複製します。

   VM-Series ファイアウォールの作成と設定に進んで続行します。

VM-Series ファイアウォールの作成と設定

この作業ではECSコンソールを使用して、管理、Untrust、およびTrustの最低3つのインターフェイスを持つVM-Seriesファイアウォールインスタンスを作成します。ECS インスタンスはデフォルトで 1 つの NIC をサポートしており、Elastic Network Interface（ENI）を NIC に自動的にアタッチします。VM-Series ファイアウォールをサポートするため、Untrust Elastic Network Interface と Trust Elastic Network Interface（ENI）を個別に作成し、インスタンスにアタッチする必要があります。

STEP 1 | Alibaba Cloudコンソールのホーム ページから、**Elastic Compute Service** > **Instances & Images**（インスタンスとイメージ） > **Instances**（インスタンス）を選択し、右上にある**Create Instance**（インスタンスの作成）をクリックします。

STEP 2 | **Custom Launch**（カスタム起動）を選択します。

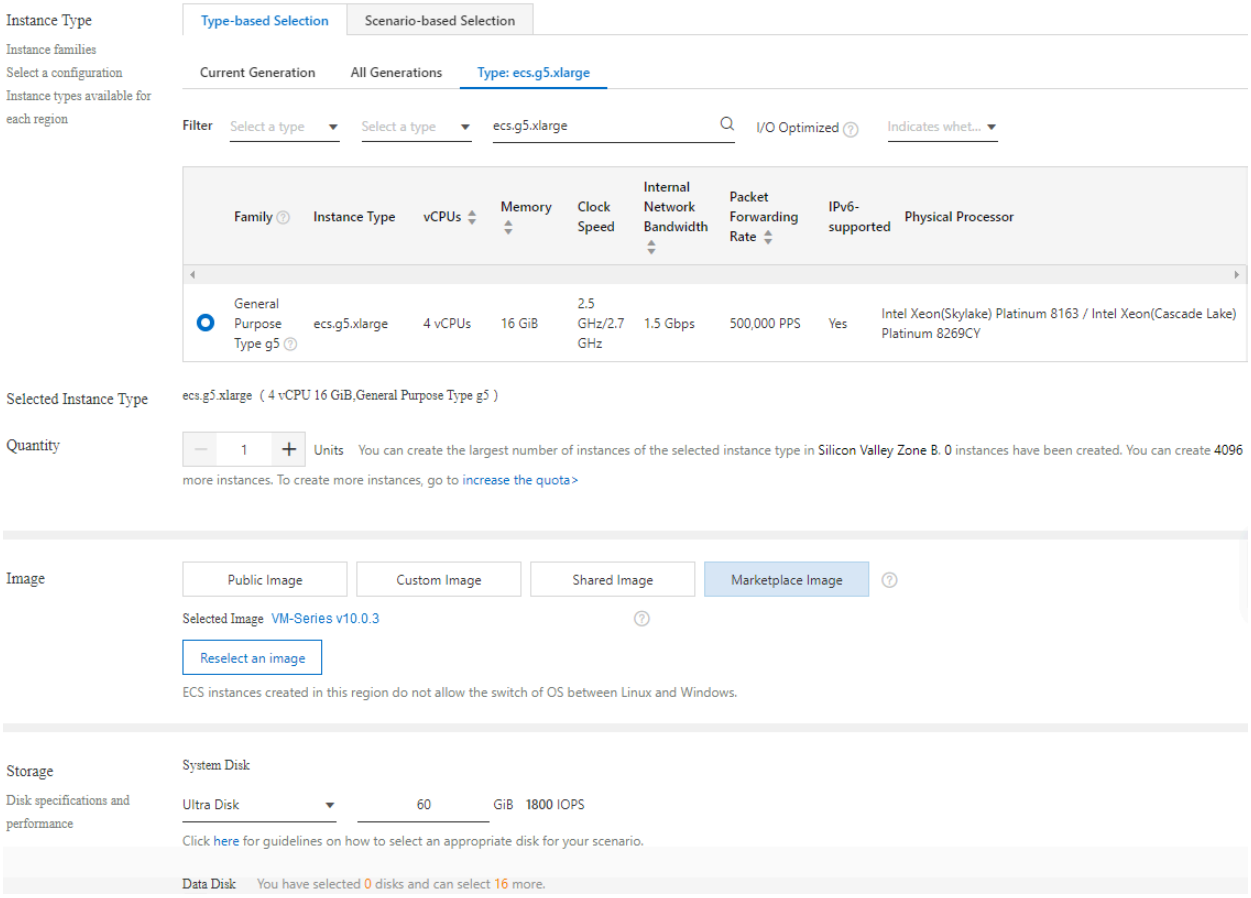
STEP 3 | 基本設定。

1. 以下の値を入力します。以下に例を示します。

プロパティ	値
Billing Method（課金方式）	Subscription （サブスクリプション）

©2023 Palo Alto Networks, Inc.

プロパティ	値
Region （リージョン）	任意の名前。ゾーンも選択できます。選択するリージョンは、必要なインスタンスタイプのいずれかを提供している必要があります。
Instance Type （インスタンスタイプ）	VM-Series ファイアウォールで推奨される Alibaba Cloud インスタンス タイプ内のいずれかのタイプ。インスタンスタイプの検索に、タイプベースの選択を使用することができます。
Image （イメージ）	**Marketplace Image** （マーケットプレイスイメージ）を選択して、Alibaba Marketplaceで「VM-Series」を検索します。イメージは、OSとVM-Seriesファイアウォールを兼ね備えています。
Storage（ストレージ）	ディスクタイプを選択して60GBを指定します。
Snapshot （スナップショット）	指定内容は任意。
期間	指定内容は任意。



2. **Next:**ネットワークを選択します。

©2023 Palo Alto Networks, Inc.

STEP 4 | Networking（ネットワーキング）ページで以下の値を指定します。

1. Network （VPCを選択 ）。
   - 「VPC の作成とネットワークの設定」で作成した VPC を選択します。
   - Management VSwitch（管理 VSwitch）を選択します。
2. Public IP Address (パブリックIPアドレス)。

   パブリックIPアドレスがない場合、**Assign Public IP address** （パブリック**IP**アドレスを割り当て）を有効にすると、システムがアドレスを割り当てます。特定のIPアドレス、または特定の範囲内のアドレスを使用する必要がある場合は、カスタムIPアドレスをリクエストできます。『Elastic IP Address User Guide （エラスティックIPアドレスユーザーガイド）』を参照してください。
3. Security Group （セキュリティグループ）。

   管理セキュリティ グループを選択します。
4. Elastic Network Interface。

   管理インターフェイスがすでに eth0 にアタッチされています。
5. **Next:System Configurations**（次へ: システム設定）を選択します。

STEP 5 | System Configurations（システム設定）ページで、以下の値を入力します。

1. Log On Credentials（ログオン認証情報）:**Key Pair**（キーペア）を選択します。

   パスワード認証はサポートされていません。
2. VM-Series ファイアウォール インスタンスの名前とホスト名を指定します。

   修正が必要な場合は修正します。

   Preview（プレビュー）を選択して、これまでの設定を確認します。
3. 次の**Advanced**（**based or instance RAM roles or cloud-init**）（高度（インスタンス**RAM**ロールまたは**cloud-init**に基づく））で、**Show**（表示）をクリックします。
   - RAMロールは任意です。
   - User Data（ユーザーデータ）フィールドで、キーと値のペアを改行で区切って、基本ブートストラップ情報を入力します。「基本設定のユーザーデータとしての入力（パブリッククラウド）」を参照してください。たとえば、**User Data**（ユーザーデータ）フィールドに、次のように入力します。

```
type=dhcp-client
hostname=Ca-FW-DC1
vm-auth-key=7550362253****
panorama-server=10.*.*.20
panorama-server-2=10.*.*.21
tplname=FINANCE_TG4
dgname=finance_dg
op-cmd-dpdk-pkt-io=on
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
```


©2023 Palo Alto Networks, Inc.

```
dhcp-accept-server-domain=yes
authcodes=I7115398
vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

op-command-modes（*mgmt-interface-swap*および*jumbo frame*）は、*Alibaba Cloud*ではサポートされていません。

op-cmd-dpdk-pkt-io=onは*DPDK*をサポートしています。*PacketMMAP*を指定した場合は、*op-cmd-dpdk-pkt-io=off*を指定します。

グループ化は任意です。注文する前に、**Preview**（プレビュー）を選択して、設定を確認します。

STEP 6 | 利用規約を参照してから、**Create Order**（注文の作成）を選択して、VM-Seriesファイアウォールインスタンスを作成します。

発注書を参照して、**Subscribe**（登録）を選択します。

STEP 7 | コンソールのホームページから、 > **Elastic Compute Service** > **Networks and Security**（ネットワークとセキュリティ） > **ENIs**を選択して、右上の**Create ENI**（**ENI**の作成）を選択します。UntrustおよびTrustインターフェイス向けに、エラスティックネットワークインターフェイスを作成します。

1. Untrust ENI を作成します。

   Actions（アクション）列で、**Bind to Instance**（インスタンスにバインド）を選択して、先ほど作成したインスタンスを選択します。
2. Trust ENIを作成し、それをインスタンスにバインドします。

STEP 8 | Elastic IP（EIP）アドレスを割り当てます。

VM-Series ファイアウォールの管理インターフェイスと Untrust ネットワーク インターフェイスに EIP アドレスを割り当てます。この例では、Trust インターフェイスはインターネットに公開されていないので、3 番目の IP アドレスは不要です。

すでに 2 つの EIP がある場合は、次のステップに進みます。

1. VM-Series ファイアウォール管理インターフェイスに EIP を関連付けます。
2. VM-Series ファイアウォール Untrust ネットワーク インターフェイスに EIP を関連付けます。

   アタッチする 2 番目のインターフェイスを、VM-Series ファイアウォールのネットワーク インターフェイス 1 に割り当てます。

STEP 9 | インスタンスを再起動して、新しいネットワーク インターフェイスをアタッチします。

Instances（インスタンス）リストでインスタンスを選択し、**Manage**（管理）をクリックし、右上にある **Restart**（再起動）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 10 | セキュリティキーを使ってSSHでVM-Seriesファイアウォールにアクセスし、管理者パスワードを設定します:

```
developer1$ ssh -i dev1-vpc1.pem admin@18.***.145.153
Welcome admin.

admin> configure
Entering configuration mode
[edit]
admin# set mgt-config users admin password
Enter password:<password>
Confirm password:<password>
[edit]
admin# commit
```

STEP 11 | VM-Series のファイアウォール Web インターフェイスにアクセスします。

Web ブラウザを開き、管理インターフェイスの EIP を入力します。

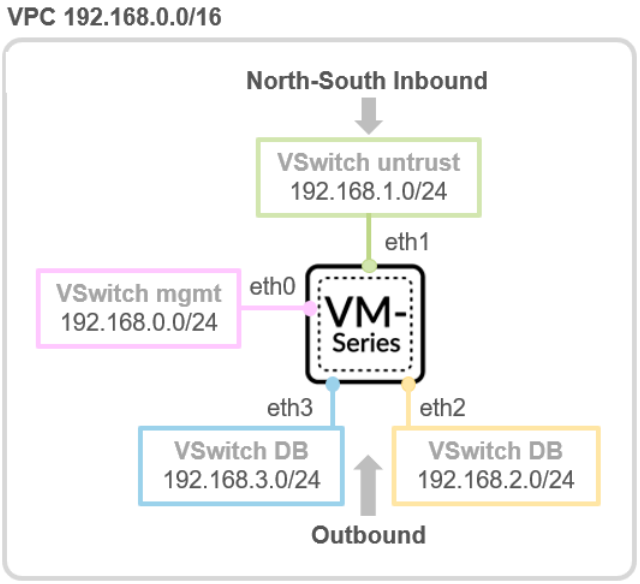
Alibaba Cloud での North-South トラフィックの保護

VPC を作成したら、VSwitch を作成して仮想プライベート ネットワークをサブネットにセグメント化できます。このサンプルには、CIDRが192.168.0.0/16のVPCが存在しています。独自の値を指定することができます。4 つの VSwitch により 4 つのサブネットが作成されます。

VSwitch 名	インターフェイス	サンプルCIDR
mgmt	eth0	192.168.0.0/24
信頼できない	eth1	192.168.1.0/24
web	eth2	192.168.2.0/24
db	eth3	192.168.3.0/24

次の図で、VM-Seriesファイアウォールはwebとdbの2つの信頼する（Trust）サブネットに接続します。外部クライアントが VM-Series ファイアウォールの Untrust インターフェイスにアクセスすると、インバウンド トラフィックが開始されます。ファイアウォールはトラフィックを検査し、アプリケーションにこのトラフィックを送信します。たとえば、ファイアウォールはトラフィックを Trust インターフェイス経由で Web サーバーに送信します。Web サーバーから戻るトラフィックは、VM-Series ファイアウォールの Trust インターフェイスに到達する必要があります。ファイアウォールはリターン トラフィック フローを検査し、Untrust インターフェイス経由で送信します。

©2023 Palo Alto Networks, Inc.



インバウンド トラフィックを保護するため、ファイアウォールで DNAT と SNAT の両方を設定する必要があります。

STEP 1 | インバウンド トラフィックの NAT ルールを作成します。

次に、インバウンド トラフィック保護の NAT ルールの例を示します。

```
            <nat>
               <rules>
                 <entry name="inbound_web">
                   <source-translation>
                     <dynamic-ip-and-port>
                       <interface-address>
                         <interface>ethernet1/2</interface>
                       </interface-address>
                     </dynamic-ip-and-port>
                  </source-translation>
                   <destination-translation>
                     <translated-address>web_server</translated-
address>
                   </destination-translation>
                   <to>
                     <member>untrust</member>
                   </to>
                   <from>
                     <member>any</member>
                   </from>
                   <source>
                    <member>any</member>
                   </source>
                   <destination>
                     <member>fw_untrust</member>
                   </destination>
                   <service>any</service>
                   <to-interface>ethernet1/1</to-interface>
                 </entry>
```

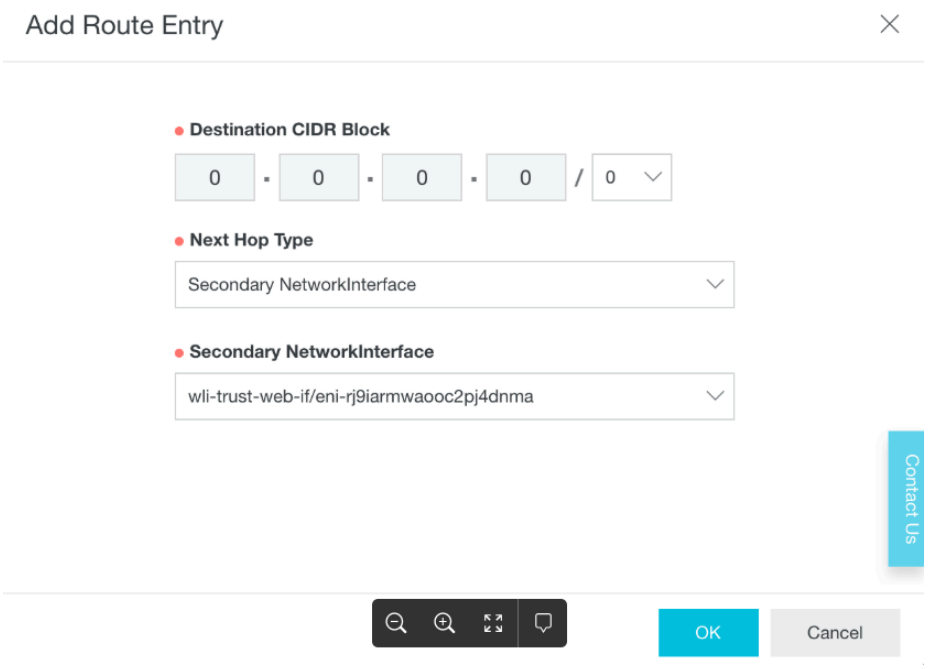

©2023 Palo Alto Networks, Inc.

```
            </rules>
          </nat>

      <address>
          <entry name="fw_untrust">
            <ip-netmask>192.168.1.4</ip-netmask>
          </entry>
          <entry name="fw_trust">
            <ip-netmask>192.168.2.201</ip-netmask>
          </entry>
          <entry name="web_server">
            <ip-netmask>192.168.2.203</ip-netmask>
          </entry>
      </address>
```

STEP 2 | アウトバウンド トラフィックを保護します。

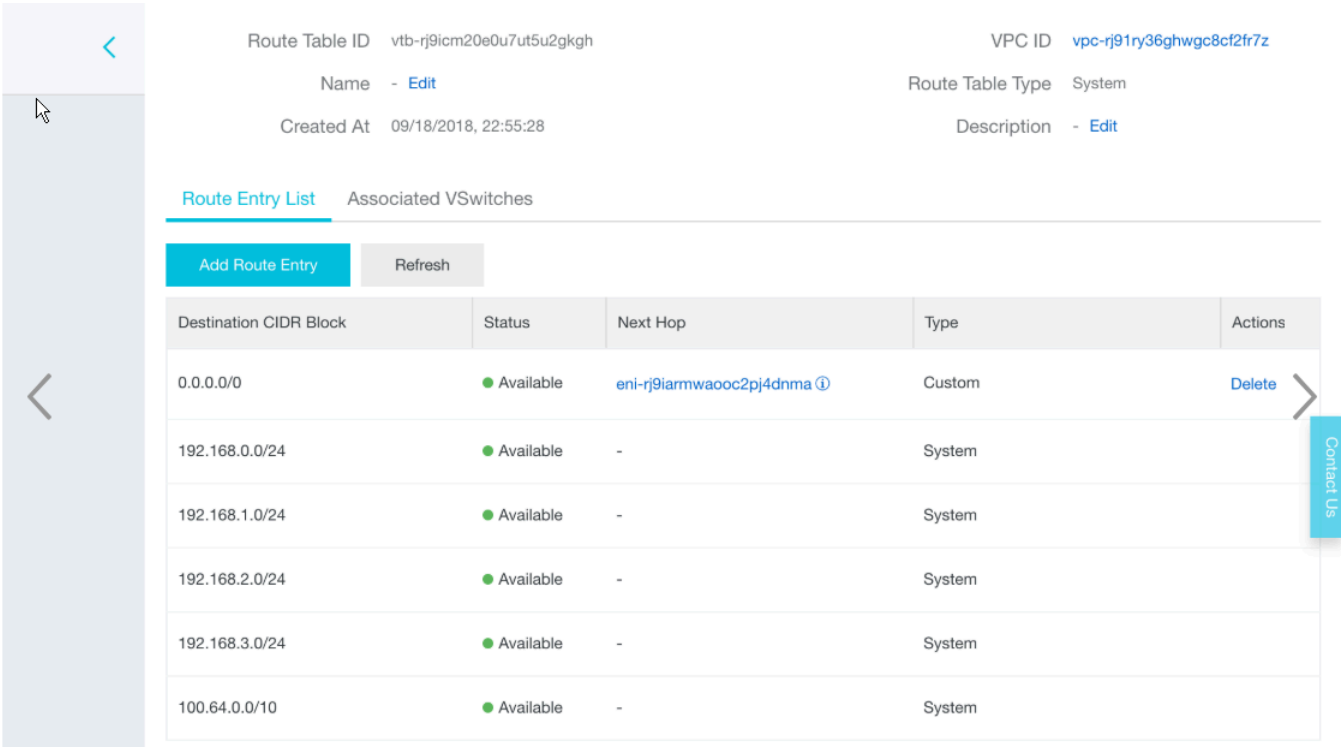
上記の図に示されているように、アプリケーションがアウトバウンド トラフィックを開始します。たとえば Web サーバーは **`yum install`** を実行して rpm パッケージを更新する必要があります。一般に、VPC 内のインターネット向けトラフィックは（EIP がアタッチされた）NAT ゲートウェイにルーティングされます。アウトバウンド トラフィックを保護するため、強制的にアウトバウンド トラフィックが VM-Series ファイアウォールを通過するようにします。

1. Web サーバーのサブネットのファイアウォール IP が含まれている VPC ルーティング テーブルに、デフォルト ゲートウェイ ルートを次のホップとして追加します。



©2023 Palo Alto Networks, Inc.

2. ルート テーブルのエントリーを確認します。



3. Untrust インターフェイス IP を使用して SNAT ルールを設定し、インターネットから戻るトラフィックが VM-Series ファイアウォールを通過するようにします。

   以下に SNAT 設定の例を示します。

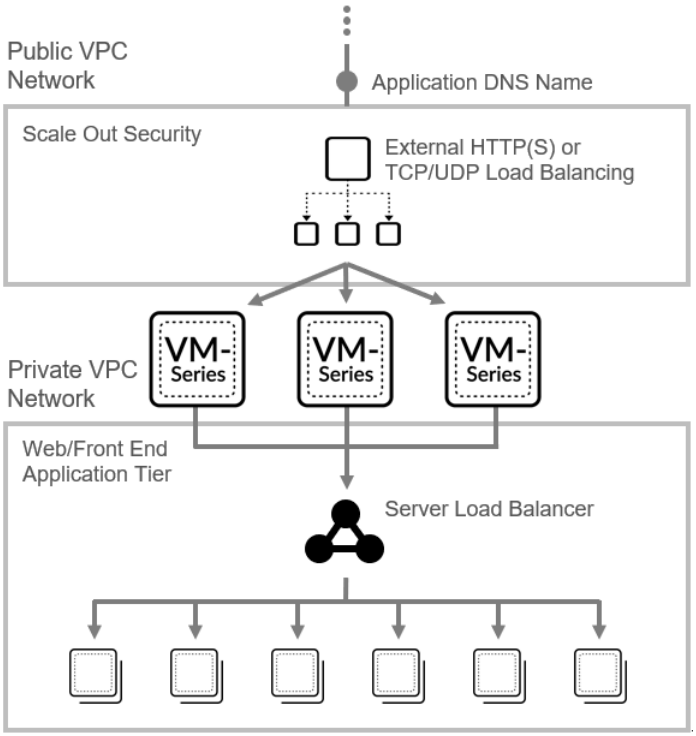
```
<nat>
  <rules>
    <entry name="outbound_web">
      <source-translation>
        <dynamic-ip-and-port>
          <interface-address>
            <interface>ethernet1/1</interface>
          </interface-address>
        </dynamic-ip-and-port>
      </source-translation>
      <to>
        <member>untrust</member>
      </to>
      <from>
        <member>trust</member>
      </from>
      <source>
        <member>any</member>
      </source>
      <destination>
        <member>any</member>
      </destination>
      <service>any</service>
      <to-interface>any</to-interface>
```


©2023 Palo Alto Networks, Inc.

```
                </entry>
              </rules>
            </nat>
```

Alibaba Cloud での負荷分散の設定

Alibaba Cloud では、ロード バランサー サンドイッチ構成（以下に示すようにファイアウォールがパブリック ネットワークとプライベート ネットワークの間にデプロイされている構成）に VM-Series ファイアウォールをデプロイできます。



「VPC の作成とネットワークの設定」で、Untrust ENI と Trust ENI を作成し、VM-Series ファイアウォール インスタンスにセカンダリ ENI としてアタッチしました。

コンソールを使用して複数のバックエンド サービスを Alibaba Server Load Balancer（SLB）に追加すると、SLB から、ネクストホップ バックエンド サーバーのプライマリ ENI にトラフィックが送信されます。プライマリ ENI は管理インターフェイスであるため、トラフィックは検査のために Untrust インターフェイス（セカンダリ ENI）に向かう必要があります。

インターネット トラフィックが管理インターフェイスではなくデータプレーン インターフェイスに向かうことを確認するには、Alibaba CLI を使用して VM-Series ファイアウォール untrust ENI を SLB インスタンスにアタッチします。

次の*CLI*コマンドを使用するには、Aliyunコマンドラインインターフェイスをインストールする必要があります。

STEP 1 | ロード バランサー サンドイッチ構成のパブリック VPC とプライベート VPC を作成し、VM-Series ファイアウォールをデプロイします。

以降の手順は、ご使用の環境に合わせて使用できる CLI コマンドの例です。

©2023 Palo Alto Networks, Inc.

STEP 2 | ロード バランサーを作成します。

```
slb CreateLoadBalancer --RegionId us-west-1 --LoadBalancerName wli-
slb
--VpcId vpc-rj91ry36ghwgc8cf2fr7z --LoadBalancerSpec slb.s1.small
--AddressType internet --MasterZoneId us-west-1a
--SlaveZoneId us-west-1b
{
        "NetworkType": "classic",
        "LoadBalancerName": "**********",
        "Address": "**********,
        "ResourceGroupId": "rg-**********ofi",
        "RequestId": "0B8BA2AA-E837-****-****-B82A8A1D5FBB",
        "AddressIPVersion": "ipv4",
        "LoadBalancerId": "lb-*****************mvz",
        "VSwitchId": "",
        "VpcId": "vpc-*****************r7z"
}
```

STEP 3 | バックエンド サーバーを追加します。

CLI を使用してインターフェイスを *1* つずつ追加します。インターフェイスを追加する順序によって、インターフェイスを受信する *NIC* が決定します。

```
aliyun slb AddBackendServers --LoadBalancerId lb-
*****************mvz
--BackendServers
'[
       {
              "ServerId":"eni-*****************bzw",
              "Type":"eni","Weight":"100"
       }
]'
```

STEP 4 | ヘルス チェックを実行する HTTP リスナーを作成します。

```
aliyun slb CreateLoadBalancerHTTPListener
--LoadBalancerId lb-*****************mvz
--ListenerPort 80 --StickySession on
--HealthCheck on --HealthCheckURI '/'
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Cisco ACI でのファイアウォールのセットアップ

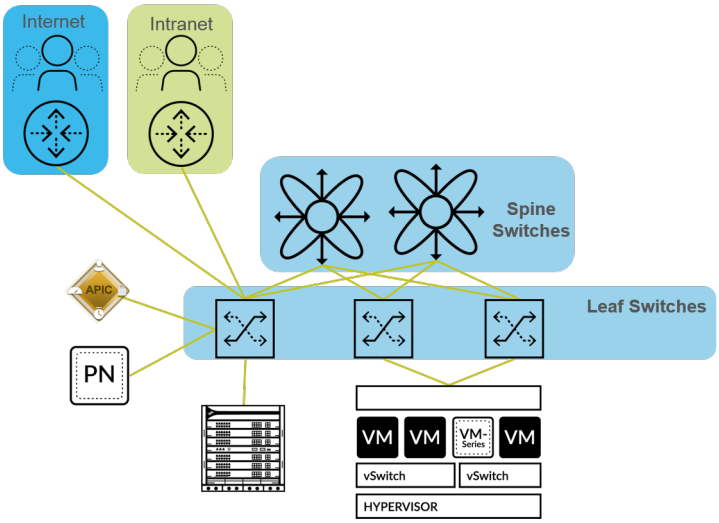
Palo Alto Networks は、サービスとして Cisco Application-Centric Infrastructure（ACI）と統合されています。ACI とは、新しいワークロードやネットワーク サービスを容易にデプロイするための Software Defined Networking（SDN）ソリューションです。Cisco Application Policy Infrastructure Controller（APIC）と呼ばれる SDN コントローラを使用して、エンドポイント グループ（EPG）間にファイアウォール サービスをデプロイします。EPG はアプリケーションまたはアプリケーション層のコンテナとして機能します。ファイアウォールを EPG 間に設置した場合、ファイアウォールで設定したセキュリティ ポリシーによって EPG 間のトラフィックを保護します。APIC を使用するとデータ センター全体のネットワーク トポロジ、ネットワーク ポリシー、接続を 1 つの画面で管理できます。APIC は、ハードウェアベースまたは VM-Series ファイアウォールなど、L4 - L7 デバイスの挿入をサポートしています。一元的なセキュリティ管理には Panorama が必要です。

> Palo Alto Networks ファイアウォールと Cisco ACI の統合
> 統合のための ACI 環境の準備
> ネットワーク ポリシー モードでのファイアウォールと Cisco ACI の統合
> Cisco ACI でのエンドポイント モニタリング

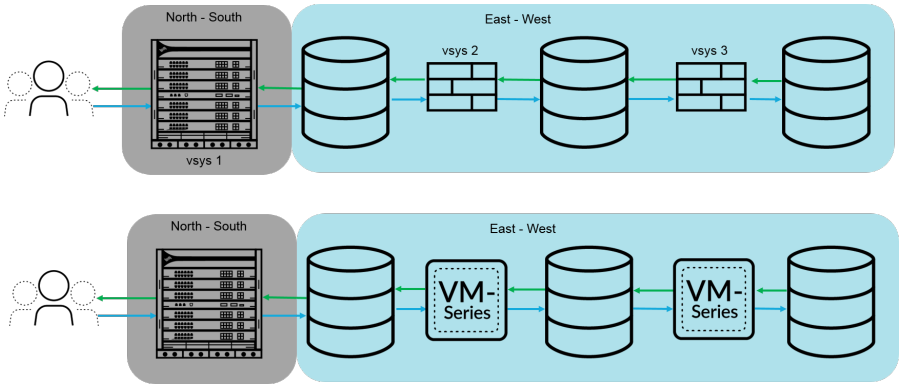
Palo Alto Networks ファイアウォールと Cisco ACI の統合

Palo Alto Networks と Cisco ACI を統合すると、各 EPG 間に L4 - L7 サービスとしてファイアウォールを挿入できます。挿入されたファイアウォールは、EPG 内のアプリケーション階層間の East-West トラフィックや、ユーザーとアプリケーション間の North-South トラフィックを保護します。

以下の図は、統合された Palo Alto Network ファイアウォールを含む物理 ACI デプロイメントの例を示しています。ACI ファブリックのすべてのエンティティはリーフ スイッチに接続されており、リーフ スイッチはより大きなスパイン スイッチに接続されています。ユーザーがアプリケーションにアクセスすると、ACI ファブリックは、トラフィックを目的の宛先に転送します。アプリケーション階層間のトラフィックを保護するため、ネットワーク管理者は、各 EPG 間に L4 - L7 サービスとして Palo Alto Networks ファイアウォールを挿入します。また、サービス グラフを作成し、L4 - L7 デバイスが提供するサービスを定義します。



ファイアウォール サービスをデプロイすると、トラフィックは、以下に示すように論理的に転送されます。各エンティティがどこで、どのように物理的にネットワークに接続されているかに関係なく、トラフィックは、エンド ユーザーやアプリケーションの各階層との間で転送されます。



©2023 Palo Alto Networks, Inc.

ファイアウォールが Cisco ACI に統合されている場合、トラフィックはポリシーベース リダイレクト（PBR）によりファイアウォールに送信されます。また、ファイアウォールの設定と APIC の設定は完全に切り離されています。ネットワーク ポリシー モードはファイアウォールと APIC 間のその他の設定統合に依存しないため、ファイアウォールの設定とデプロイの柔軟性が向上します。

east-west トラフィックの場合は、ファイアウォールの ACI ファブリックでブリッジ ドメインとサブネットを定義します。PBR を使用してトラフィックをファイアウォールに送信する EPG 間のコントラクトを設定します。PBR は、ファイアウォールの IP アドレスと MAC アドレスが含まれているポリシーに基づいて、トラフィックをファイアウォールに転送します。ファイアウォール インターフェイスは常にレイヤー 3 モードであり、トラフィックが受信されると ACI ファブリックに戻されます。コンシューマー接続用とプロバイダー接続用に個別のインターフェイスを設定するか、または入力トラフィックと出力トラフィック用に 1 つのインターフェイスを設定できます。1 つのインターフェイスを設定する方が統合がシンプルになるため、このドキュメントの手順では 1 つのインターフェイスを使用します。インターフェイス、IP アドレス、VLAN を多数設定する必要はありません。ただし、1 つのインターフェイスを使用する場合は、セキュリティ ポリシーを定義する際にゾーン情報を使用できず、ファイアウォールでデフォルトのゾーン内ポリシーを変更してトラフィックを拒否するように設定する必要があります。

north-south トラフィックの場合は、L3Out という名前の専用ポリシーを使用する必要があります。L3Out には、テナントが外部ルーティング デバイスに接続し、外部ネットワークにアクセスするために必要な情報が含まれています。L3Out 接続には、L3Out ポリシーによってアクセス可能なネットワークを表す外部ネットワーク EPG が含まれています。L3Out ですべての外部ネットワークを 1 つの EPG にグループ化できるように、vzAny オブジェクト ACI を使用して VRF 内のすべての EPG を表すことができます。vzAny オブジェクトを使用すると、アウトバウンド トラフィック コントラクトの適用がシンプルになります。これは、新しい EPG が VRF に追加されるたびにコントラクトが自動的に適用されるためです。このシナリオでは、外部ネットワークがコントラクトを提供し、vzAny オブジェクト（すべての内部 EPG）がコントラクトを消費します。

次のセクションでは、次世代ファイアウォールと Cisco ACI 間の統合を構成するコンセプトとコンポーネントについて詳しく説明します。

- サービス グラフ テンプレート
- マルチコンテキスト デプロイメント

サービス グラフ テンプレート

ファイアウォールはサービス グラフを通じて Cisco ACI にデプロイされます。サービス グラフにより、レイヤー 4 - レイヤー 7 デバイス（ファイアウォールなど）をトラフィック フローに統合でき、この際 L4 -L7 デバイスを ACI ファブリック内のサーバーのデフォルト ゲートウェイにする必要がありません。

ACI ファブリックでは、ファイアウォールは APIC でデバイス クラスターとして設定する L4-L7 デバイスとして表されます。1 つのファイアウォールまたは HA ペアとしてデプロイされる 2 つのファイアウォールは、デバイス クラスターとして設定されます。各デバイス クラスターには 1 つ以上の論理インターフェイスが含まれています。論理インターフェイスは、デバイス クラス

 ©2023 Palo Alto Networks, Inc.

ターのインターフェイス情報を記述し、メンバー ファイアウォールのパスを物理または仮想マシン監視（VMM）ドメインからの VLAN にマップします。

サービス グラフ テンプレートは、EPG 間のトラフィック フローに挿入するファイアウォール デバイス クラスターを定義しますまた、サービス グラフ テンプレートはファイアウォールの統合方法と、コンシューマー EPG およびプロバイダー EPG に割り当てられている論理インターフェイスを定義します。作成したサービス グラフ テンプレートを EPG とコントラクトに割り当てます。サービス グラフ テンプレートは特定の EPG またはコントラクトに関連付けられていないため、複数の EPG で再利用できます。その後 APIC はサービス グラフ テンプレートをデプロイするため、このテンプレートを EPG 間のブリッジ ドメインに接続します。

マルチコンテキスト デプロイメント

Cisco ACI 統合では、複数のコンテキストに分割された物理ファイアウォールがサポートされます。これらのコンテキストは、個々のファイアウォールとして ACI で管理されています。物理ファイアウォール上のコンテキストは、ファイアウォール上の仮想システム（vsys）です。各ファイアウォールは、ライセンスが供与されると、特定の数の vsys インスタンスをサポートするようになります。マルチ vsys ファイアウォールを ACI にデプロイするときは、テナントでシャーシ マネージャーを設定してから、ファイアウォール サービスに割り当てる必要があります。

©2023 Palo Alto Networks, Inc.

統合のための ACI 環境の準備

ファイアウォールとデバイス パッケージを統合する前に、以下のステップを実行して、Cisco ACI 環境を準備する必要があります。

STEP 1 | Panorama をデプロイします。

STEP 2 | ファイアウォールをデプロイします。

- 物理ファイアウォール – ファイアウォールのアウトオブバンド管理ポートを 1 つのリーフ スイッチ ポートに接続し、1 つ以上のファイアウォール データ インターフェイスをスイッチに接続します。物理ファイアウォールのファイアウォール インターフェイスは、VLAN を使用して設定し、正しいネットワークに確実に接続するようにします。プラットフォーム固有のインストール ガイドに従って、ファイアウォールをデプロイします。
- VM-Series ファイアウォール – VM-Series ファイアウォール用の仮想ハードウェアを設定するときは、管理インターフェイスのポートグループを設定します。ネットワークに接続されている各 VM-Series ファイアウォールには、専用の仮想 NIC が必要です。ご使用のハイパーバイザに基づいて、VM-Series ファイアウォールをデプロイします。

STEP 3 | 各ファイアウォールおよび Panorama 上で管理 IP アドレスを設定します。

以下に対して初期設定を実行します。

- ハードウェアベース ファイアウォール
- VM-Series ファイアウォール
- Panorama

STEP 4 | Panorama に管理対象デバイスとしてファイアウォールを追加します。

STEP 5 | ファイアウォールに機能ライセンスをインストールします。

- 物理ファイアウォール上で登録、およびライセンスのアクティベーションを行います。
- VM-Series ファイアウォール上で登録、およびVM-Series モデルライセンスのアクティベートを行います。
- Panorama を使用して、ファイアウォールのライセンス管理を行います。

STEP 6 | Cisco ACI ファブリックおよび管理接続を確立します。

この設定の一環として、物理ドメインと VLAN 名前空間を作成します。物理ファイアウォールのデータ インターフェイスが物理ドメインの一部になっていることを確認します。

STEP 7 | Cisco ACI VMM ドメイン プロファイルを作成します。

仮想マシンまたは VM-Series ファイアウォールを使用している場合は、VMware vSphere 環境用の仮想マシン モニター（VMM）ドメイン プロファイルを作成します。VMM ドメインでは、vSphere と ACI ファブリック間の接続ポリシーが指定されます。

©2023 Palo Alto Networks, Inc.

ネットワーク ポリシー モードでのファイアウォールと Cisco ACI の統合

ネットワーク ポリシー モードで 1 つの論理 HA インターフェイスへのポリシー ベース リダイレクトを使用して、高可用性（HA）のファイアウォール ペアを East-West トラフィックまたは North-South トラフィックに統合します。ファイアウォールと ACI ファブリックは個別に設定され、ファイアウォールのアドレス オブジェクトは ACI ファブリックの EPG にマップされます。

east-west または north-south トラフィックを保護するため、ネットワーク ポリシー モードを使用して Palo Alto Networks ファイアウォールをデプロイできます。

- ネットワーク ポリシー モードで East-West トラフィックを保護するファイアウォールのデプロイ
- ネットワーク ポリシー モードで North-South トラフィックを保護するファイアウォールのデプロイ

ネットワーク ポリシー モードで East-West トラフィックを保護するファイアウォールのデプロイ

Cisco ACI 環境で、Palo Alto Networks のファイアウォールをデプロイし、アンマネージド モードとポリシー ベース リダイレクトを使用して east-west トラフィックを保護する手順を説明します。この手順は、以下の作業が完了していることを前提としています。

- ファイアウォールが動作しており、Cisco ACI 環境のリーフ スイッチに接続している。また、各ファイアウォールの管理インターフェイスが APIC からアクセス可能である。
- ファイアウォールがアクティブ/パッシブ HA モードでデプロイされている。この手順では HA ネットワークのセットアップは事前に完了していることを前提としており、このセットアップについては説明しません。

east-west トラフィックを保護するには、ファイアウォールの ACI ファブリックでブリッジ ドメインとサブネットを定義します。PBR を使用してトラフィックをファイアウォールに送信する EPG 間のコントラクトを設定します。PBR は、ファイアウォールの IP アドレスと MAC アドレスが含まれているポリシーに基づいて、トラフィックをファイアウォールに転送します。ファイアウォール インターフェイスは常にレイヤー 3 モードであり、トラフィックが受信されると ACI ファブリックに戻されます。コンシューマー接続用とプロバイダー接続用に個別のインターフェイスを設定するか、または入力トラフィックと出力トラフィック用に 1 つのインターフェイスを設定できます。1 つのインターフェイスを設定する方が統合がシンプルになるため、このドキュメントの手順では 1 つのインターフェイスを使用します。インターフェイス、IP アドレス、VLAN を多数設定する必要はありません。ただし、1 つのインターフェイスを使用する場合は、セキュリティ ポリシーを定義する際にゾーン情報を使用できず、ファイアウォールでデフォルトのゾーン内ポリシーを変更してトラフィックを拒否するように設定する必要があります。

この手順では、ワンアーム モードでファイアウォールをデプロイします。ワンアーム モードでは、トラフィックは 1 つのインターフェイスを通じてファイアウォールに出入りします。この共通ファイアウォール インターフェイスは、サービス グラフ テンプレートのコンシューマー イン

©2023 Palo Alto Networks, Inc.

ターフェイスとプロバイダー テンプレートの両方に使用されます。1 つのインターフェイスを使用すると、設定する必要がある IP アドレス、VLAN、インターフェイスの数が減るため、ファイアウォールとの統合が簡素化されます。ただしワンアーム デプロイメント モデルはゾーン内であるため、セキュリティ ポリシーを定義するときにゾーン情報を使用できません。

ファイアウォール:

- 仮想ルーターとセキュリティ ゾーンの作成
- ネットワーク インターフェイスの設定
- スタティック デフォルト ルートの設定
- EPG のアドレス オブジェクトの作成
- セキュリティ ポリシー ルールの作成

Cisco APIC:

- VLAN プールとドメインの作成
- East-West トラフィックの LLDP および LACP のインターフェイス ポリシーの設定
- ファイアウォールと ACI ファブリック間の接続の確立
- VRF とブリッジ ドメインの作成
- L4-L7 デバイスの作成
- ポリシー ベース リダイレクトの作成
- サービス グラフ テンプレートの作成および適用

仮想ルーターとセキュリティ ゾーンの作成

ファイアウォールで、テナントの VRF ごとに仮想ルーターとゾーンを設定します。

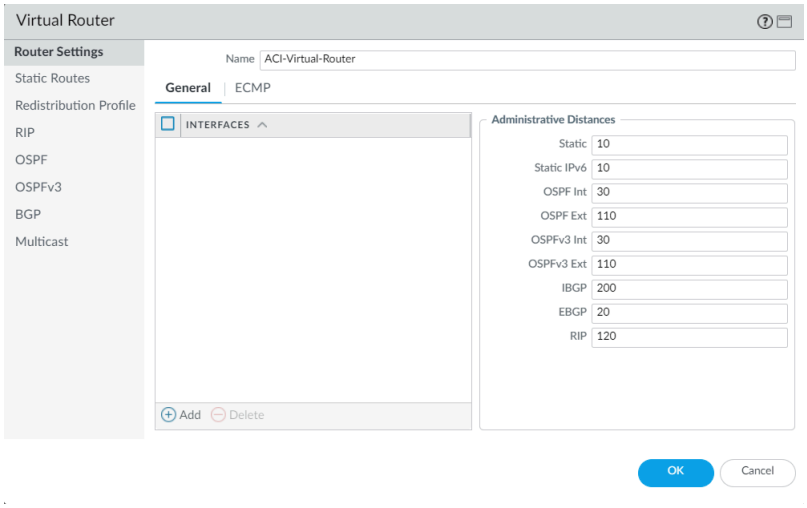
STEP 1 | ファイアウォールにログインします。

STEP 2 | **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、**Add**（追加）をクリックします。

STEP 3 | **Name**（名前）に分かりやすい仮想ルーター名を入力します。

©2023 Palo Alto Networks, Inc.

STEP 4 | **OK**をクリックします。

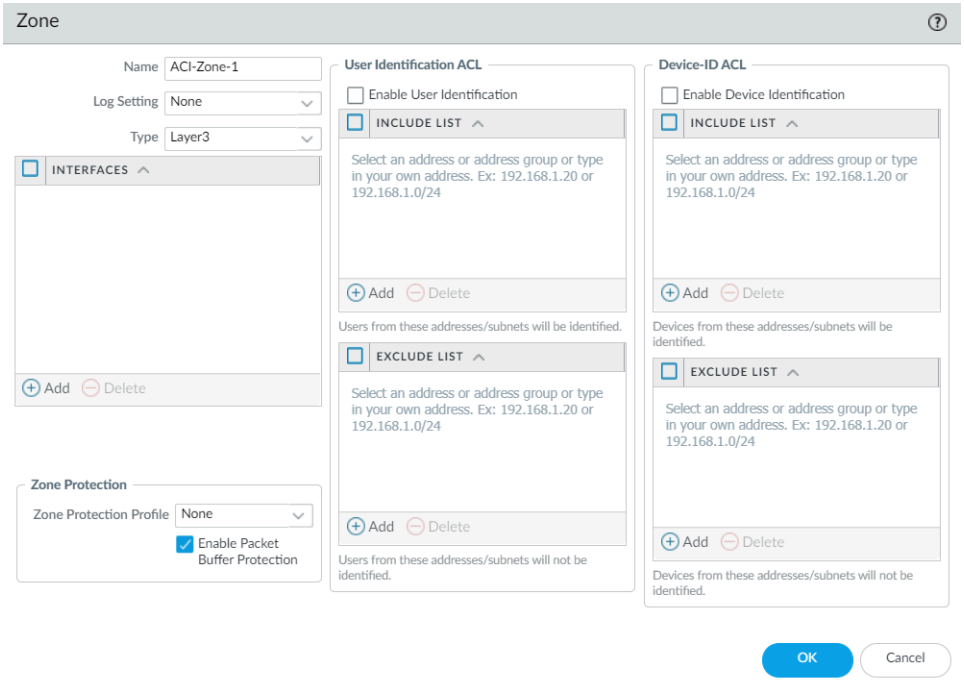


STEP 5 | **Network**（ネットワーク） > **Zones**（ゾーン）を選択し、**Add**（追加）をクリックします。

STEP 6 | **Name**（名前）に分かりやすいゾーン名を入力します。

STEP 7 | **Type**（タイプ）のドロップダウン リストから Layer 3（レイヤー 3）を選択します。

STEP 8 | **OK**をクリックします。



STEP 9 | 変更を **Commit**（コミット）します。

©2023 Palo Alto Networks, Inc.

ネットワーク インターフェイスの設定

ACI リーフ スイッチにファイアウォールを接続するイーサネット インターフェイスを設定します。この設定で使用する VLAN ID 番号は、ACI でファイアウォールに割り当てられている VLAN プールのメンバーである必要があります。

VM-Series ファイアウォールでは集約イーサネット グループはサポートされていません。

STEP 1 | **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、**Add Aggregate Group**（集約グループの追加）をクリックします。

STEP 2 | 2 番目の**Interface Name**（インターフェイス名）フィールドに、集約グループの番号を入力します。

STEP 3 | **Interface Type**（インターフェイス タイプ）のドロップダウン リストから Layer 3（レイヤー 3）を選択します。

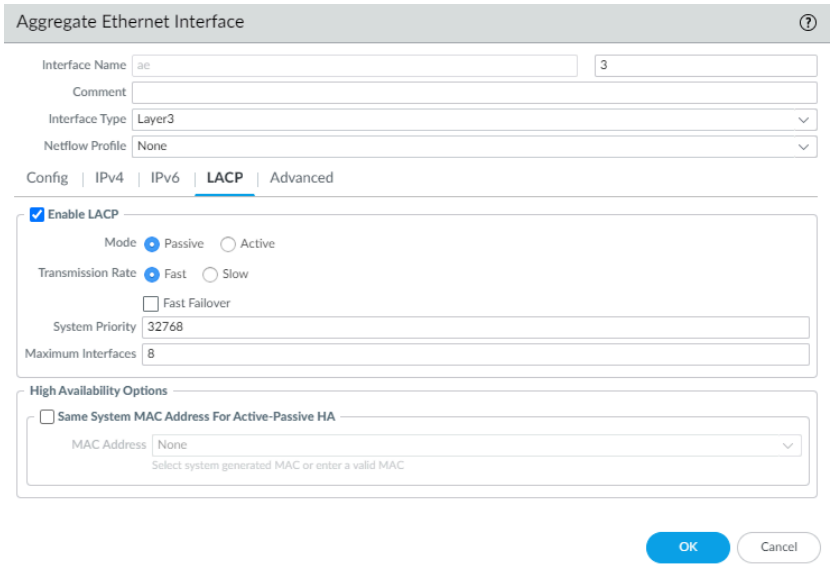
STEP 4 | **LACP** タブを選択し、**Enable LACP**（**LACP** を有効化）を選択します。

STEP 5 | **Transmission Rate**（伝送速度） として**Fast**（高速）を選択します。

STEP 6 | High Availability Options（高可用性オプション）で **Enable in HA Passive State**（**HA**パッシブ ステートを有効にする）を選択します。

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）は選択しないでください。このオプションを選択すると、スイッチに対しファイアウォール ペアが *1* つのデバイスとして示されるため、トラフィックがアクティブなファイアウォールではなく両方のファイアウォールに流れます。

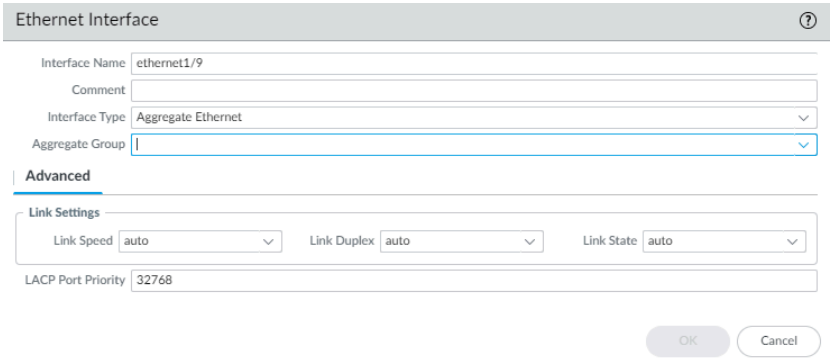
STEP 7 | **OK** をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 8 | イーサネット インターフェイス名をクリックしてこのインターフェイスを設定し、集約グループに追加します。

1. Interface Type（インターフェイス タイプ）のドロップダウン リストから **Aggregate Ethernet**（集約イーサネット） を選択します。
2. 集約イーサネット グループの設定で定義したインターフェイスを選択します。
3. **OK** をクリックします。
4. 集約イーサネット グループの他のメンバー インターフェイスごとにこの手順を繰り返します。



STEP 9 | 集約イーサネット インターフェイスでテナントと VRF のためのサブインターフェイスを追加します。

1. 集約イーサネット グループの行を選択し、**Add Subinterface**（サブインターフェイスの追加）をクリックします。
2. 2 番目の **Interface Name**（インターフェイス名）フィールドに、サブインターフェイスを識別する数値サフィックスを入力します。
3. **Tag**（タグ）フィールドに、サブインターフェイスの VLAN タグを入力します。
4. 以前に設定した仮想ルーターを **Virtual Router**（仮想ルーター）のドロップダウン リストから選択します。
5. 以前に設定したゾーンを **Zone**（ゾーン）のドロップダウン リストから選択します。
6. **IPv4** タブを選択します。
7. **Static**（静的）タイプを選択します。
8. **Add**（追加）をクリックし、CIDR 表記でサブインターフェイスの IP アドレスとネットワーク マスクを入力します。
9. **OK** をクリックします。

スタティック デフォルト ルートの設定

イーサネット サブインターフェイスからサブネット ルーターにトラフィックを転送するスタティック デフォルト ルートを設定します。

STEP 1 | **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、この手順で前に作成した仮想ルーターをクリックします。

STEP 2 | **Static Routes**（静的 ルート） > **IPv4**を選択して **Add**（追加）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 3 | 分かりやすい **Name**（名前）を入力します。

STEP 4 | **Destination**（宛先）フィールドに 0.0.0.0/0 を入力します。

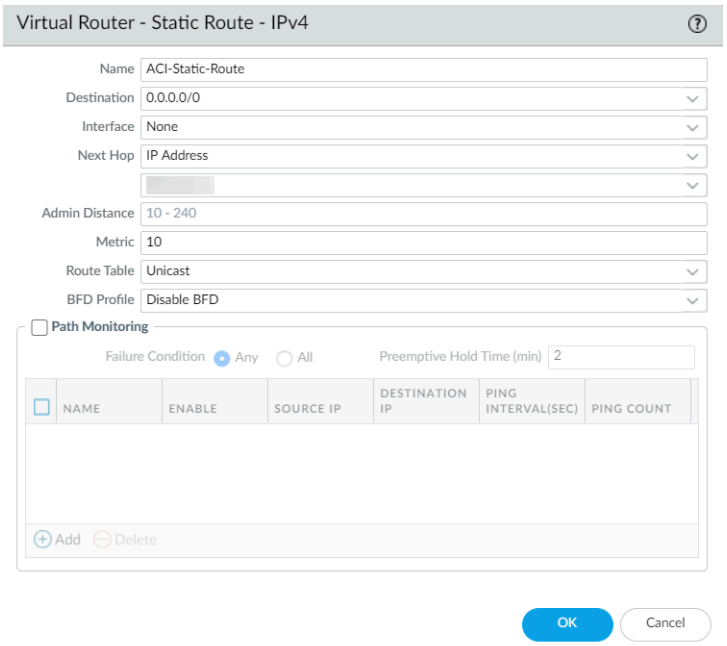
STEP 5 | **Interface**（インターフェイス）のドロップダウン リストから、この手順で前に作成した集約イーサネット グループを選択します。

STEP 6 | **Next Hop**（ネクスト ホップ）のドロップダウン リストから IP Address（IP アドレス）を選択し、ネクスト ホップ ルーターの IP アドレスを入力します。

STEP 7 | **OK** をクリックします。

STEP 8 | 再度 **[OK]** をクリックします。

STEP 9 | 変更を **Commit (**コミット**)**します。



EPG のアドレス オブジェクトの作成

アドレス オブジェクトを定義し、セキュリティ ポリシーで使用するエンドポイント グループ（EPG）にマップする必要があります。アドレス グループは、エンドポイントの IP アドレス範囲を使用してセキュリティ グループをサーバーのグループにマップするための最適な手段です。EPG ごとにアドレス オブジェクトを 1 つずつ作成します。

STEP 1 | **Objects**（オブジェクト） > **Address**（アドレス）を選択して **Add**（追加）をクリックします。

STEP 2 | アドレス オブジェクトの分かりやすい名前を入力します。

STEP 3 | **Type**（タイプ）のドロップダウン リストから IP Netmask（IP ネットマスク）を選択します。

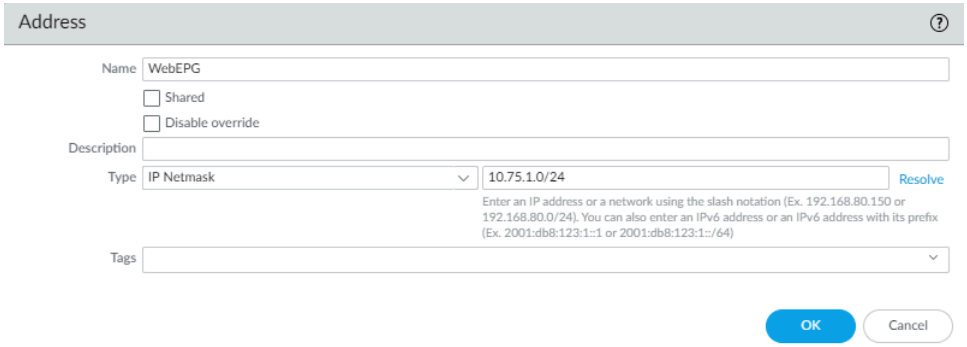
STEP 4 | IP ネットマスクを入力します。

©2023 Palo Alto Networks, Inc.

STEP 5 | **OK** をクリックします。

STEP 6 | EPG ごとにこの操作を繰り返します。

STEP 7 | 変更を **Commit (コミット)**します。



セキュリティ ポリシー ルールの作成

EPG 間のトラフィックの移動を制御するセキュリティ ポリシー ルールを作成します。デフォルトでは、ファイアウォールではすべてのゾーン内トラフィックが許可されます。EPG はすべて同じゾーン内にあるため、EPG 間のすべてのトラフィックが許可されます。新しいルールを作成する前に、デフォルトのゾーン内ルールを allow（許可）から deny（拒否）に変更します。

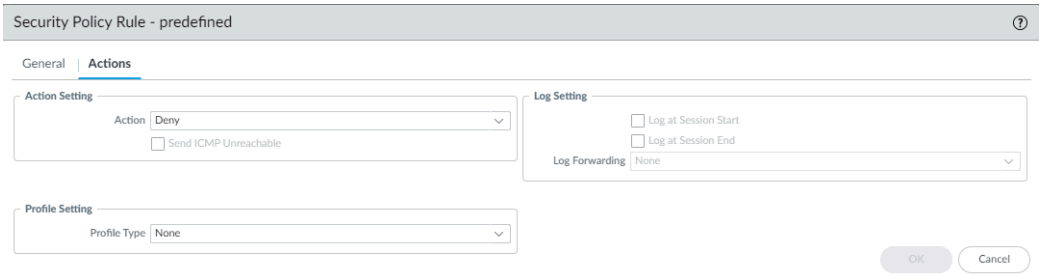
STEP 1 | **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。

STEP 2 | intrazone-default をクリックしてその行を強調表示し、**Override**（オーバーライド）をクリックします。

STEP 3 | **Action**（アクション）タブを選択します。

STEP 4 | **Action**（アクション）のドロップダウン リストから Deny（拒否）を選択します。

STEP 5 | **OK** をクリックします。



STEP 6 | 必要に応じて、EPG 用に作成したゾーンとアドレス オブジェクトに基づいて追加のセキュリティ ポリシー ルールを設定します。

VLAN プールとドメインの作成

インターフェイスを EPG の ACI インフラストラクチャにアタッチする際に、ファイアウォールに VLAN を割り当てるために使用される VLAN プールを設定します。ファイアウォールの VLAN プールには静的 VLAN 範囲が含まれている必要があります。

©2023 Palo Alto Networks, Inc.

ファイアウォールの専用ドメインを設定します。ファイアウォールのドメインは、VLAN を EPG にマップするときに必要です。物理ファイアウォールの物理ドメインを作成し、VM-series ファイアウォールの VMM ドメインを作成します。

STEP 1 | VLAN プールを作成します。

1. APIC にログインします。
2. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Pools**（プール） > **VLAN** を選択します。
3. **VLAN** を右クリックし、**Create VLAN Pool**（**VLAN** プールの作成）を選択します。
4. **Name**（名前）に 分かりやすい VLAN プール名を入力します。
5. Allocation Mode（割り当てモード）で **Dynamic Allocation**（動的割り当て）を選択します。
6. カプセル化ブロック（**Encap Blocks**）の右側にあるプラス（+）ボタンをクリックします。
7. **VLAN Range**（**VLAN** 範囲）フィールドに VLAN 範囲を入力します。
8. Allocation Mode（割り当てモード）のドロップダウン リストから **Static Allocation**（静的割り当て）を選択します。
9. **OK**をクリックします。
10. **Submit**（送信） をクリックします。

STEP 2 | （物理ファイアウォールのみ）物理ドメインを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Physical and External Domains**（物理ドメインと外部ドメイン） > **Physical Domains**（物理ドメイン）を選択します。
2. **Physical Domain**（物理ドメイン）を右クリックして**Create Physical Domain**（物理ドメインの作成）を選択します。
3. **Name**（名前）に分かりやすい物理ドメイン名を入力します。
4. 前の手順で作成した VLAN プールを VLAN Pool（VLAN プール）リストから選択します。
5. **Submit**（送信） をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 3 | （VM-Series ファイアウォールのみ）VMM ドメインを作成します。

1. **Virtual Networking**（仮想ネットワーキング） > **VMM Domains**（**VMM** ドメイン） > **VMware** を選択します。
2. **VMware** を右クリックして、**Create vCenter Domain**（**vCenter** ドメインの作成）を選択します。
3. **Name**（名前）に分かりやすい VMM ドメイン名を入力します。
4. **Virtual Switch**（仮想スイッチ）のドロップダウン リストから **VMware vSphere Distributed Switch**（**VMware vSphere** 分散スイッチ）を選択します。
5. **Encapsulation**（カプセル化）のドロップダウン リストから **VLAN** を選択します。
6. **VLAN Pool**（**VLAN** プール）のドロップダウン リストから VLAN プールを選択します。
7. **vCenter Credentials**（**vCenter** 認証情報）の右側にあるプラス（+）ボタンをクリックします。
8. 分かりやすい **Profile Name**（プロファイル名）と vCenter ログイン情報を入力します。
9. **vCenter** の右側にあるプラス（+）ボタンをクリックします。
10. 分かりやすい **Name**（名前）を入力します。
11. Type（タイプ）のドロップダウン リストから vCenter を選択します。
12. **IP/Hostname**（**IP/**ホスト名）の下に vCenter IP アドレスを入力します。
13. 作成した vCenter 認証情報プロファイルを **Associated Credential**（関連付けられている認証情報）のドロップダウン リストから選択します。
14. **Submit**（送信） をクリックします。

East-West トラフィックの LLDP および LACP のインターフェイス ポリシーの設定

ファイアウォールに接続する ACI インターフェイスで LLDP と LACP を有効にするポリシーを作成します。

LLDP は、ACI 環境で転送が正しく機能するために必要です。エンドポイントを必要とするスイッチでエンドポイントが検出されない場合には、ACI はリーフ スイッチにサブネット ルーター インターフェイスをデプロイしません。LLDP により、サブネット ルーター インターフェイスが必要であるかどうかを判別できます。

LACP は、リンク障害発生時に高い復元力と回復スピードを発揮します。

©2023 Palo Alto Networks, Inc.

STEP 1 | LLDP インターフェイス ポリシーを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Interface Policies**（インターフェイス ポリシー） > **Policies**（ポリシー） > **LLDP Interface**（**LLDP** インターフェイス）を選択します。
2. **LLDP Interface**（**LLDP** インターフェイス）を右クリックし、**Create LLDP Interface Policy**（**LLDP** インターフェイス ポリシーの作成）を選択します。
3. **Name**（名前）に分かりやすい LLDP インターフェイス ポリシー名を入力します。
4. **Receive State**（受信状態）で **Enabled**（有効）を選択します。
5. **Transmit State**（送信状態）で **Enabled**（有効）を選択します。
6. **Submit**（送信） をクリックします。

STEP 2 | LACP を有効にするポート チャネル ポリシーを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Interface Policies**（インターフェイスポリシー） > **Policies**（ポリシー） > **Port Channel**（ポート チャネル）を選択します。
2. **Port Channel**（ポート チャネル）を右クリックし、**Create Port Channel Policy**（ポート チャネル ポリシーの作成）を選択します。
3. **Name**（名前）に分かりやすいポート チャネル ポリシー名を入力します。
4. **Mode**（モード）のドロップダウン リストから **LACP Active**（**LACP** アクティブ）を選択します。
5. **Submit**（送信） をクリックします。

ファイアウォールと ACI ファブリック間の接続の確立

この手順で以前にファイアウォールで設定したイーサネット インターフェイス（または集約イーサネット グループ）を使用して、VPC 接続を通じてファイアウォールをリーフ スイッチにアタッチします。1 つ以上のインターフェイスをリーフ スイッチの同じポートに接続します。

STEP 1 | **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Quick Start**（クイック スタート）を選択します。

STEP 2 | **Configure an interface, PC, and VPC**（インターフェイス、**PC**、および **VPC** の設定）をクリックします。

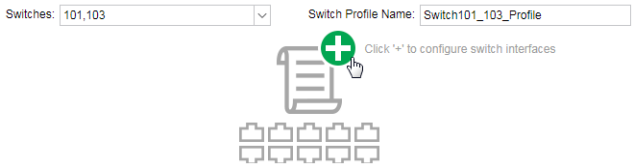
STEP 3 | 緑色と白色のプラス（+）をクリックします。



STEP 4 | ファイアウォールが接続している 1 つ以上のリーフ スイッチを **Switches**（スイッチ）のドロップダウン リストから選択します。

 ©2023 Palo Alto Networks, Inc.

STEP 5 | 緑色と白色のプラス（+）をクリックします。



STEP 6 | **Interface Type**（インターフェイス タイプ）として VPC を選択します。

STEP 7 | **Interfaces**（インターフェイス）フィールドに、ファイアウォールがリーフ スイッチへの接続に使用するインターフェイスの数を入力します。

STEP 8 | **Interface Selector Name**（インターフェイス セレクター名）フィールドに分かりやすい名前を入力します。

STEP 9 | **LLDP Policy**（**LLDP** ポリシー）のドロップダウン リストから **LLDP-Enabled**（**LLDP** 有効）を選択します。

STEP 10 | **Port Channel Policy**（ポートチャネル ポリシー）のドロップダウン リストから **LACP Active**（**LACP** アクティブ）を選択します。

STEP 11 | **Attached Device Type**（アタッチ デバイス タイプ）のドロップダウン リストで、物理ファイアウォールの場合は **Bare Metal**（ベア メタル）を選択し、VM-Series の場合は **ESX Hosts**（**ESX** ホスト）を選択します。

STEP 12 | **Domain**（ドメイン）で **Choose One**（**1** つ選択）を選択します。

STEP 13 | この手順で前に作成した物理ドメインまたは VMM ドメインを **Domain**（ドメイン）のドロップダウン リストから選択します。

STEP 14 | **Save**（保存）をクリックします。

STEP 15 | **Save**（保存）をクリックし、次に **Submit**（送信）をクリックします。

STEP 16 | HA ペアの 2 番目のファイアウォールについてこの手順を繰り返します。

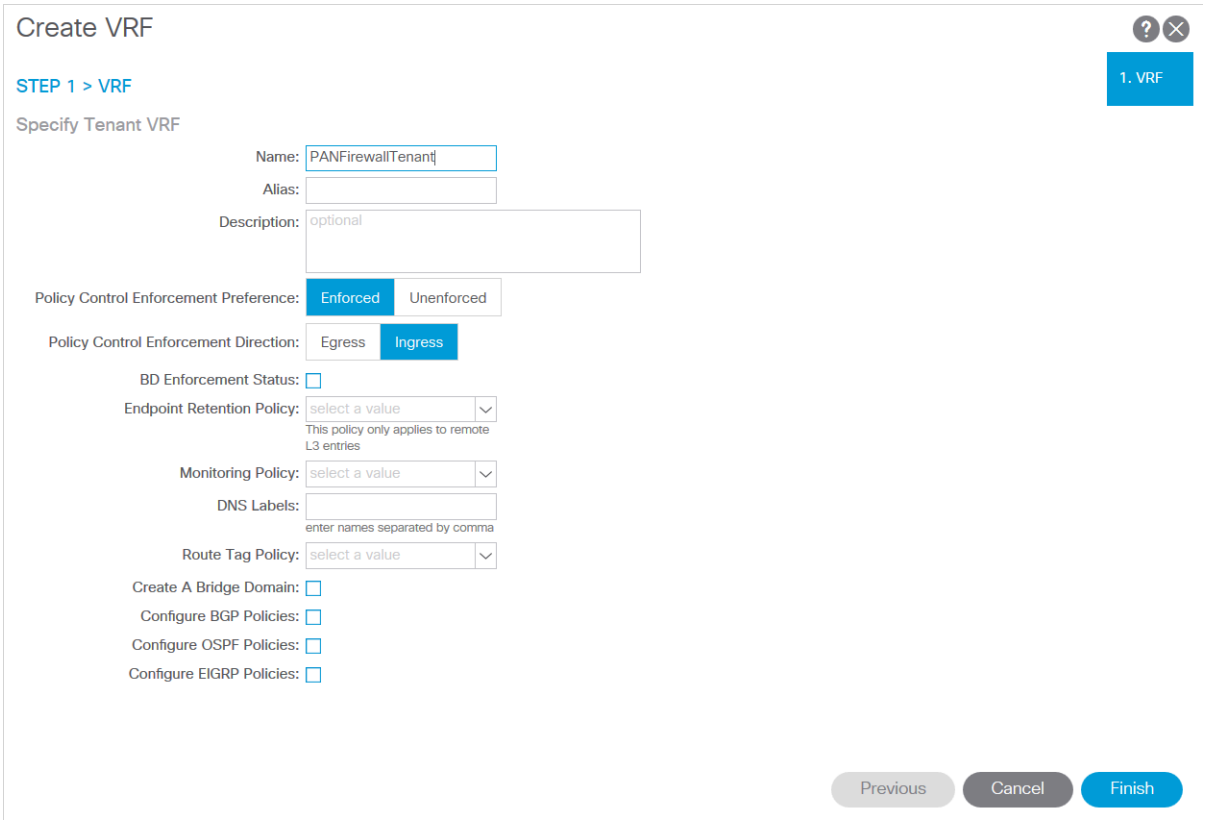
VRF とブリッジ ドメインの作成

テナントには、すべてのブリッジ ドメインとサブネットのための VRF が必要です。この例では、ファイアウォールとエンドポイント用の 1 つの共通 VRF を作成します。次に、ファイアウォールの専用ブリッジ ドメインを設定し、データプレーン学習を無効にします。ポリシーベース リダイレクトをブリッジ ドメインで使用するには、データプレーン学習を無効にする必要があります。

©2023 Palo Alto Networks, Inc.

STEP 1 | VRF を作成します。

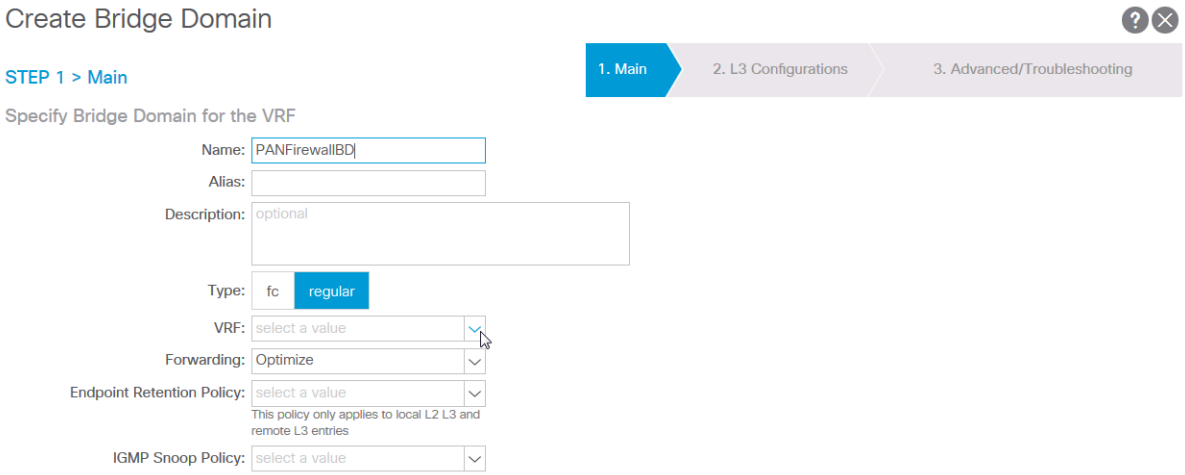
1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Network**（ネットワーク） > **VRFs**を選択します。
3. **VRFs** を右クリックし、**Create VRF**（**VRF** の作成）を選択します。
4. **Name**（名前）に分かりやすい VRF 名を入力します。
5. **Create A Bridge Domain**（ブリッジ ドメインの作成）チェック ボックスをオフにします。
6. **Finish**（完了）をクリックします。



 ©2023 Palo Alto Networks, Inc.

STEP 2 | ファイアウォールのブリッジ ドメインを作成します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Networking**（ネットワーキング） > **Bridge Domains**（ブリッジ ドメイン）を選択します。
3. **Bridge Domains**（ブリッジ ドメイン）を右クリックして **Create Bridge Domains**（ブリッジ ドメインの作成）を選択します。
4. **Name**（名前）に分かりやすいブリッジ ドメイン名を入力します。
5. 前の手順で作成した VRF を **VRF** のドロップダウン リストから選択します。
6. **Next**（次へ）をクリックします。



L4-L7 デバイスの作成

ACI がファイアウォールをトラフィック フローに挿入できるようにするため、APIC でファイアウォールを L4-L7 デバイスとして定義する必要があります。APIC で L4-L7 デバイスをデバイス クラスタとして設定します。このデバイス クラスタは、1 つのファイアウォールまたは 1 つのデバイスとして動作するファイアウォール HA ペアを表す構成体です。デバイスクラスタには1つ以上の論理インターフェイスが含まれています。このインターフェイスは、物理ドメインのVLANを含むメンバー ファイアウォールのパスを定義します。

STEP 1 | **Tenants**（テナント）タブでテナント名をダブルクリックします。

STEP 2 | **Services**（サービス） > **L4-L7** > **Devices**（デバイス）を選択します。

STEP 3 | **Devices**（デバイス）を右クリックし、**Create L4-L7 Device**（**L4-L7** デバイスの作成）を選択します。

STEP 4 | **Managed**（管理対象）チェック ボックスをオフにします。

STEP 5 | **Name**（名前）に分かりやすい L4-L7 デバイス名を入力します。

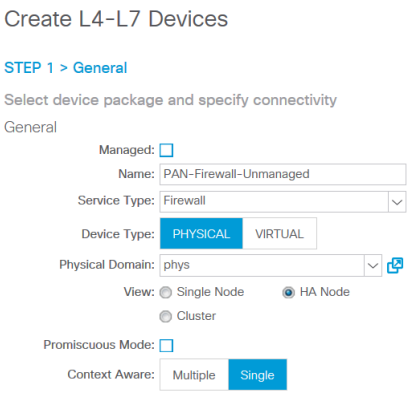
STEP 6 | **Service Type**（サービス タイプ）のドロップダウン リストから **Firewall**（ファイアウォール）を選択します。

©2023 Palo Alto Networks, Inc.

STEP 7 | **Device Type**（デバイス タイプ）のドロップダウン リストで、物理ファイアウォールの場合は **Physical**（物理）を選択し、VM-Series ファイアウォールの場合は **Virtual**（仮想）を選択します。

STEP 8 | 前に作成した物理ドメインまたは VMM ドメインを **Domain**（ドメイン）のドロップダウン リストから選択します。

STEP 9 | **View**（表示）で HA Node（HA ノード）を選択します。



STEP 10 | **Device 1**（デバイス **1**）で **Device Interfaces**（デバイス インターフェイス）の右側にあるプラス（+）ボタンをクリックします。

STEP 11 | **Name**（名前）にこのインターフェイスの分かりやすい名前を入力します。

STEP 12 | **Path**（パス）で HA ペアのプライマリ ファイアウォールのパスを選択します。

STEP 13 | **Update**（更新）をクリックします。

STEP 14 | **Device 2**（デバイス **2**）で **Device Interfaces**（デバイス インターフェイス）の右側にあるプラス（+）ボタンをクリックします。

STEP 15 | **Name**（名前）にこのインターフェイスの分かりやすい名前を入力します。

STEP 16 | **Path**（パス）で HA ペアのセカンダリ ファイアウォールのパスを選択します。

STEP 17 | **Update**（更新）をクリックします。

STEP 18 | **Cluster**（クラスタ）で **Cluster Interfaces**（クラスタインターフェイス） の右側にあるプラス（+）ボタンをクリックします。

STEP 19 | **Name**（名前）に分かりやすいクラスタ名を入力します。

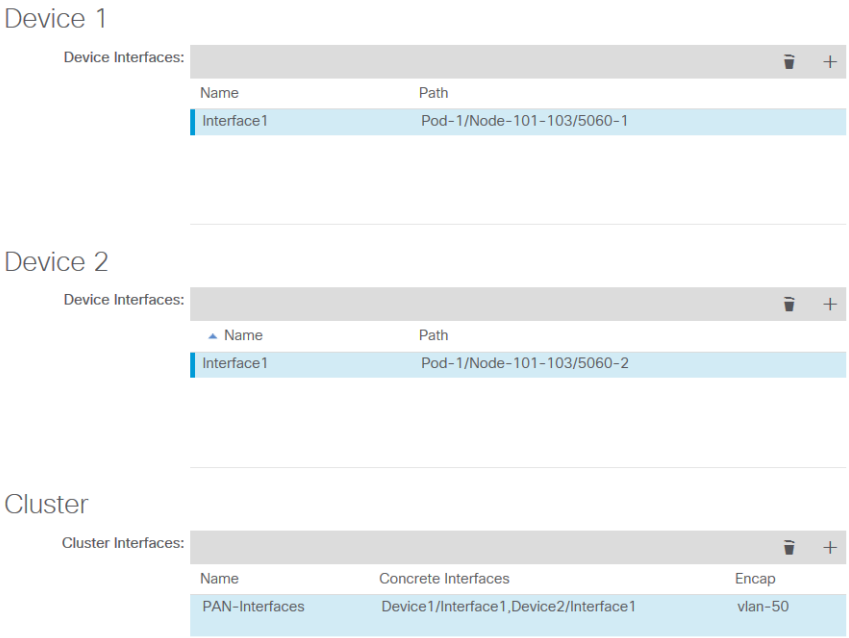
STEP 20 | 先ほど設定した 2 つのインターフェイスを **Concrete Interfaces**（具象インターフェイス）のリストから選択します。APIC では、2 つのインターフェイスを設定する必要があります。ただし、ファイアウォールと ACI ファブリック間の接続が 1 つのみであるため、1 つのインターフェイスだけが使用されます。

STEP 21 | **Encap**（カプセル化）の下で、前に作成した静的 VLAN プールの VLAN を入力します。トラフィックは、ここで割り当てる VLAN のファイアウォールにリダイレクトされます。

©2023 Palo Alto Networks, Inc.

STEP 22 | **Update**（更新）をクリックします。

STEP 23 | **Finish**（完了）をクリックします。



ポリシー ベース リダイレクトの作成

EPG 間のトラフィックをファイアウォールに送信するポリシー ベース リダイレクトを設定します。ポリシー ベース リダイレクトは、ファイアウォールのインターフェイスの MAC アドレスを使用します。APIC で PBR 設定を行う前に、ファイアウォールの MAC アドレスを取得しておく必要があります。

STEP 1 | ファイアウォールの MAC アドレスを取得します。

1. ファイアウォール CLI にログインします。
2. **`command show interface all`** を使用して、設定したインターフェイスの MAC アドレスを表示します。
3. リダイレクトされたトラフィックを受信するインターフェイスの MAC アドレスをコピーします。

©2023 Palo Alto Networks, Inc.

STEP 2 | L4-L7 ポリシー ベース リダイレクトを作成します。

1. APIC にログインします。
2. **Tenants**（テナント）タブでテナント名をダブルクリックします。
3. **Policies**（ポリシー） > **Protocol**（プロトコル） > **L4-L7 Policy Based Redirect**（**L4-L7** ポリシー ベース リダイレクト）を選択します。
4. **L4-L7 Policy Based Redirect**（**L4-L7** ポリシー ベース リダイレクト）を右クリックし、**Create L4-L7 Policy Based Redirect**（**L4-L7** ポリシー ベース リダイレクトの作成）を選択します。
5. **Name**（名前）に分かりやすいポリシー ベース リダイレクト名を入力します。
6. **Destinations**（宛先）の右側にあるプラス（+）ボタンをクリックします。
7. **IP** フィールドに、リダイレクトされたトラフィックを受信するインターフェイスの IP アドレスをコピーします。
8. **MAC** フィールドに、ファイアウォール CLI からコピーした MAC アドレスを入力します。
9. **OK**をクリックします。
10. **Submit**（送信） をクリックします。

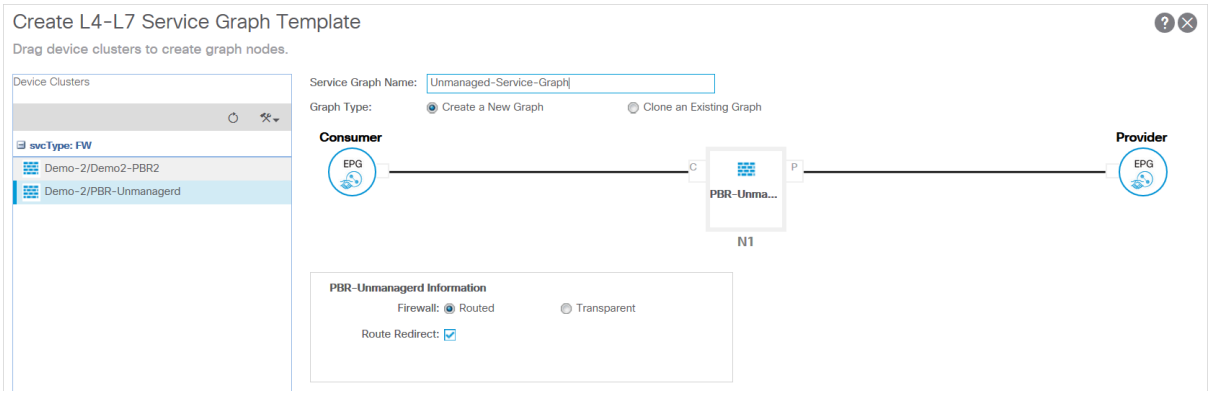
サービス グラフ テンプレートの作成および適用

ポリシー ベース リダイレクト統合でファイアウォールを表すデバイス クラスタを使用するサービス グラフ テンプレートを作成します。サービス グラフの作成が完了したら、トラフィックを保護するためサービス グラフを EPG に適用します。コントラクトとコントラクト フィルター ルールにより、ファイアウォールに転送できるトラフィックが定義されます。

©2023 Palo Alto Networks, Inc.

STEP 1 | サービス グラフ テンプレートを作成します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Services**（サービス） > **L4-L7** > **L4-L7 Service Graph Templates**（**L4-L7** サービス グラフ テンプレート）を選択します。
3. **L4-L7 Service Graph Template**（**L4-L7** サービス グラフ テンプレート）を右クリックし、**Create L4-L7 Service Graph Template**（**L4-L7** サービス グラフ テンプレートの作成）を選択します。
4. **Graph Name**（グラフ名）に、分かりやすいサービス グラフ テンプレート名を入力します。
5. **Graph Type**（グラフ タイプ）で **Create a New One**（新規作成）を選択します。
6. 前の手順で作成した L4-L7 デバイスをクリックし、コンシューマー EPG とプロバイダー EPG の間にドラッグします。
7. **Firewall**（ファイアウォール）で **Routed**（ルーテッド）を選択します。
8. **Routed Redirect**（ルーテッド リダイレクト）を選択します。
9. **Submit**（送信） をクリックします。



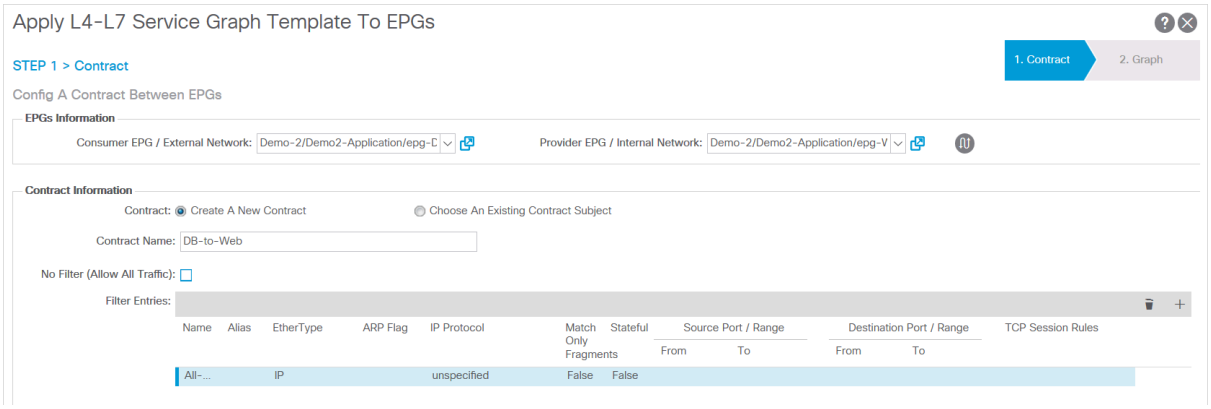
STEP 2 | サービス グラフ テンプレートを適用します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Services**（サービス） > **L4-L7**を選択します。
3. **EPGs Information**（**EPG** 情報）ペインの**Consumer EPG**（コンシューマー **EPG**）と**Provider EPG**（プロバイダー **EPG**）のドロップダウン リストから、コンシューマー EPG とプロバイダー EPG を選択します。
4. **Create a New Contract**（コントラクトの新規作成）を選択します。
5. **Contract Name**（コントラクト名）に、分かりやすいコントラクト名を入力します。
6. **No Filter**（**Allow All Traffic**）（フィルターなし（すべてのトラフィックを許可））をクリアします。このオプションを使用することは推奨されません。EPG 間のすべてのト

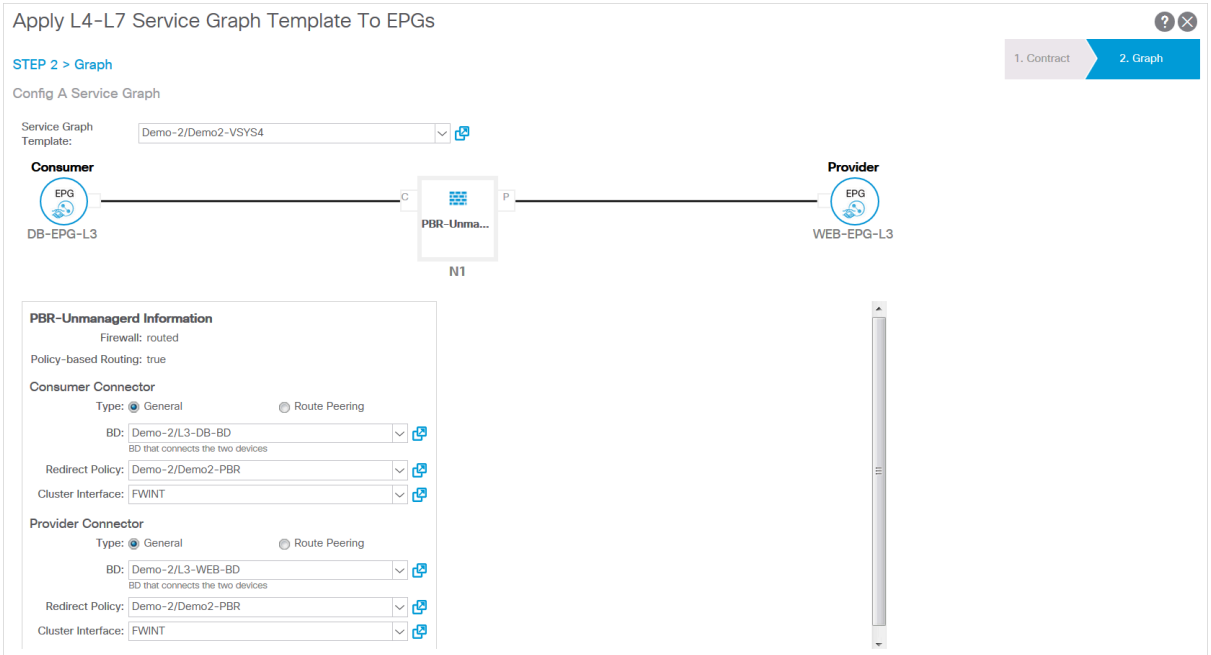
©2023 Palo Alto Networks, Inc.

ラフィックをファイアウォールに転送できるようにするには、そのためのフィルターを作成することが推奨されます。

7. **Filter Entries**（フィルター エントリ） の右側にあるプラス（+）アイコンをクリックします。
8. EPG 間を通過してファイアウォールにリダイレクトできるトラフィックを定義するルールを 1 つ以上作成します。
9. **Next**（次へ）をクリックします。



10. 前の手順で作成したサービス グラフ テンプレートを **Service Graph Template**（サービス グラフ テンプレート）のドロップダウン リストから選択します。
11. コンシューマー ペインとプロバイダー ペインで、ファイアウォールが含まれているブリッジ ドメインを **BD** のドロップダウン リストから選択します。
12. 前に作成したポリシー ベース リダイレクトを **Redirect Policy**（リダイレクト ポリシー）のドロップダウン リストから選択します。
13. L4-L7 デバイスを使用して作成したクラスタインターフェイスを **Cluster Interface**（クラスタインターフェイス）のドロップダウン リストから選択します。



©2023 Palo Alto Networks, Inc.

ネットワーク ポリシー モードで North-South トラフィックを保護するファイアウォールのデプロイ

ポリシー ベース リダイレクトでアンマネージド モードを使用してデータ センターを出入りする north-south トラフィックを保護するには、ネットワーク ポリシー モードを使用します。この手順は、以下の作業が完了していることを前提としています。

- ファイアウォールが動作しており、Cisco ACI 環境のリーフ スイッチに接続している。また、各ファイアウォールの管理インターフェイスが APIC からアクセス可能である。
- ファイアウォールがアクティブ/パッシブ HA モードでデプロイされている。この手順では HA ネットワークのセットアップは事前に完了していることを前提としており、このセットアップについては説明しません。

ACI ファブリック外部のネットワークへの外部接続を確立するには、L3Out を設定する必要があります。L3Out は、外部ルーティング デバイスをテナントに接続するために必要なパラメータが含まれている専用ポリシーです。L3Out にはさらに、L3Out 経由でアクセス可能なネットワークを表す外部 EPG（APIC UI では外部ネットワークと呼ばれます）が含まれています。外部 EPG は動的に取り込まれず、ゼロトラスト モデルに従っているため、EPG でネットワークを定義する必要があります。設定を容易にするため、ネットワーク 0.0.0.0/0 を設定してすべてのネットワークを外部 EPG に割り当てることができます。

インバウンド トラフィックを保護するため、HA ペアのいずれかまたは両方のファイアウォールを境界リーフ スイッチに接続します。境界リーフ スイッチとは、外部ルーターへのレイヤー 3 接続を提供するリーフ スイッチです。ファイアウォールは、vPC ペアの各リーフ スイッチで設定されている OSPF（open shortest path first）プロトコルを使用して境界リーフ スイッチとピアリングし、スイッチ仮想インターフェイス（SVI）を使用してファイアウォールと通信します。ファイアウォールで、データセンターに接続するインターフェイス専用の仮想ルーターを設定します。さらに、この手順には次のものが含まれています。

アウトバウンド トラフィックの場合、ファイアウォールは OSPF を使用して外部ネットワークを境界リーフ スイッチにアドバタイズします。また外部ネットワーク EPG は、ファイアウォールがアドバタイズするすべてのネットワークがこの EPG に接続することを許可するように設定されています。vzAny 管理対象オブジェクトと外部ネットワーク EPG 間のコントラクトを作成し、VRF 内の EPG からのトラフィックがファイアウォール経由で外部ネットワークに到達することを許可します。vzAny 管理対象オブジェクトを使用すると、EPG ごとに個別のコントラクトを作成するのではなく、VRF 内のすべての EPG を 1 つまたは複数のコントラクトに統合できます。vzAny 管理対象オブジェクトに収集された EPG は、外部 EPG が提供するコントラクトを消費します。

サービス マネージャー モードとは異なり、ACI インフラストラクチャとファイアウォールの管理は個別に行われます。

APIC –

- VLAN プールと仮想ルーティング ドメインの作成
- North-South トラフィックの LLDP および LACP のインターフェイス ポリシーの設定
- 外部ルーティング ネットワークの作成
- 外部ファイアウォールへのサブネットのアドバタイズの設定

©2023 Palo Alto Networks, Inc.

- アウトバウンド コントラクトの作成
- インバウンド Web コントラクトの作成
- EPG へのアウトバウンド コントラクトとインバウンド コントラクトの適用

ファイアウォール –

- North-South トラフィック用の仮想ルーターとセキュリティ ゾーンの作成
- ネットワーク インターフェイスの設定
- ルートの再配信と OSPF の設定
- 外部接続のための NAT の設定

VLAN プールと仮想ルーティング ドメインの作成

ACI ファブリックで EPG をサポートするため、インターフェイスをインフラストラクチャにアタッチするときにファイアウォールに VLAN を割り当てるための VLAN プールを作成します。ファイアウォールには静的 VLAN 範囲を使用してください。

また、VLAN を EPG にマップするため物理ドメインを作成する必要もあります。ファイアウォール専用の物理ドメインを作成する手順を以下に示します。

STEP 1 | VLAN プールを作成します。

1. APIC にログインします。
2. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Pools**（プール） > **VLAN** を選択します。
3. **VLAN** を右クリックし、**Create VLAN Pool**（**VLAN** プールの作成）を選択します。
4. **Name**（名前）に 分かりやすい VLAN プール名を入力します。
5. Allocation Mode（割り当てモード）で **Dynamic Allocation**（動的割り当て）を選択します。
6. カプセル化ブロック（**Encap Blocks**）の右側にあるプラス（+）ボタンをクリックします。
7. **VLAN Range**（**VLAN** 範囲）フィールドに VLAN 範囲を入力します。
8. Allocation Mode（割り当てモード）のドロップダウン リストから **Static Allocation**（静的割り当て）を選択します。
9. **OK**をクリックします。
10. **Submit**（送信） をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 2 | 外部ルーティング ドメインを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Physical and External Domains**（物理ドメインと外部ドメイン） > **External Domains**（外部ドメイン）を選択します。
2. **External Routed Domain**（外部ルーティング ドメイン）を右クリックして **Create Layer 3 Domain**（レイヤー 3 ドメインの作成）を選択します。
3. **Name**（名前）に分かりやすい物理ドメイン名を入力します。
4. 前の手順で作成した VLAN プールを VLAN Pool（VLAN プール）リストから選択します。
5. **Submit**（送信） をクリックします。

North-South トラフィックの LLDP および LACP のインターフェイス ポリシーの設定

ファイアウォールに接続する ACI インターフェイスで LLDP と LACP を有効にするポリシーを作成します。

LLDP は、ACI 環境で転送が正しく機能するために必要です。エンドポイントを必要とするスイッチでエンドポイントが検出されない場合には、ACI はリーフ スイッチにサブネット ルーター インターフェイスをデプロイしません。LLDP により、サブネット ルーター インターフェイスが必要であるかどうかを判別できます。

LACP は、リンク障害発生時に高い復元力と回復スピードを発揮します。

STEP 1 | LLDP インターフェイス ポリシーを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Interface Policies**（インターフェイス ポリシー） > **Policies**（ポリシー） > **LLDP Interface**（**LLDP** インターフェイス）を選択します。
2. **LLDP Interface**（**LLDP** インターフェイス）を右クリックし、**Create LLDP Interface Policy**（**LLDP** インターフェイス ポリシーの作成）を選択します。
3. **Name**（名前）に分かりやすい LLDP インターフェイス ポリシー名を入力します。
4. **Receive State**（受信状態）で **Enabled**（有効）を選択します。
5. **Transmit State**（送信状態）で **Enabled**（有効）を選択します。
6. **Submit**（送信） をクリックします。

STEP 2 | LACP を有効にするポート チャネル ポリシーを作成します。

1. **Fabric**（ファブリック） > **Access Policies**（アクセス ポリシー） > **Interface Policies**（インターフェイスポリシー） > **Policies**（ポリシー） > **Port Channel**（ポート チャネル）を選択します。
2. **Port Channel**（ポート チャネル）を右クリックし、**Create Port Channel Policy**（ポート チャネル ポリシーの作成）を選択します。
3. **Name**（名前）に分かりやすいポート チャネル ポリシー名を入力します。
4. **Mode**（モード）のドロップダウン リストから **LACP Active**（**LACP** アクティブ）を選択します。
5. **Submit**（送信） をクリックします。

©2023 Palo Alto Networks, Inc.

外部ルーティング ネットワークの作成

ファイアウォールは IP ルーティング情報をレイヤー 3 OSPF ネットワーク経由で ACI へ渡します。ACI は、接続の回復力のために、各スイッチに IP アドレスが設定されているリーフ スイッチでスイッチ仮想インターフェイス（SVI）を使用します。OSPF を使用してファイアウォールとピアリングするレイヤー 3 ルーティング ネットワークを作成します。

STEP 1 | **Tenants**（テナント）タブでテナント名をダブルクリックします。

STEP 2 | **Networking**（ネットワーキング） > **External Routed Networks**（外部ルーティング ネットワーク）を選択します。

STEP 3 | **External Routed Networks**（外部ルーティング ネットワーク）を右クリックして**Create Routed Outside**（外部ルーティングの作成）を選択します。

STEP 4 | **Name**（名前）フィールドに分かりやすい外部ルーティング ネットワーク名を入力します。

STEP 5 | 外部に接続している VRF を **VRF** のドロップダウン リストから選択します。

STEP 6 | 前に作成した外部ルーティング ドメインを **External Routed Domain**（外部ルーティング ドメイン）のドロップダウン リストから選択します。

STEP 7 | **OSPF** を選択します。

STEP 8 | **OSPF Area ID**（**OSPF** エリア **ID**）を入力します。このエリア ID は、10 進数形式またはドット付きの 10 進数型式で指定できます。たとえばエリア 1 はエリア 0.0.0.1 と同じであり、エリア 271 はエリア 0.0.1.15 と同じです。エリア ID の範囲は 0（0.0.0.0）～ 4294967295（255.255.255.255）です。

STEP 9 | **OSPF Area Type**（**OSPF** エリア タイプ）で **Regular Area**（標準エリア）を選択します。

STEP 10 | **Nodes and Interface Profiles**（ノードとインターフェイス プロファイル）の右側にあるプラス（+）ボタンをクリックし、ファイアウォールに接続している境界リーフ スイッチのノードのノード プロファイルを作成します。

STEP 11 | **Name**（名前）フィールドに分かりやすいノード プロファイル名を入力します。

©2023 Palo Alto Networks, Inc.

STEP 12 | ノード プロファイルにノードをアタッチします。

1. **Nodes**（ノード）の右側にあるプラス（+）ボタンをクリックします。**Select Node**（ノードの選択）ウィンドウが開きます。
2. ファイアウォールが接続しているノードを **Node ID**（ノード **ID**）のドロップダウン リストから選択します。
3. リーフ スイッチにアタッチしているルーターの IP アドレスを **Router ID**（ルーター **ID**）に入力します。
4. **OK** をクリックします。
5. **Nodes and Interface Profiles**（ノードとインターフェイス プロファイル）の右側にあるプラス（+）ボタンをクリックします。
6. **Name**（名前）フィールドに分かりやすいノード プロファイル名を入力します。
7. **Nodes**（ノード）の右側にあるプラス（+）ボタンをクリックします。**Select Node**（ノードの選択）ウィンドウが開きます。
8. セカンダリ HA ファイアウォールが接続しているノードを **Node ID**（ノード **ID**）のドロップダウン リストから選択します。
9. 2 番目のリーフ スイッチにアタッチしているルーターの IP アドレスを **Router ID**（ルーター **ID**）に入力します。
10. **OK** をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 13 | ノード プロファイルの OSPF インターフェイス プロファイルをアタッチします。

1. **Name**（名前）に分かりやすい OSPF インターフェイス プロファイルの名前を入力します。
2. **Next**（次へ）をクリックします。
3. OSPF Policy（OSPF ポリシー）のドロップダウン リストから **Create OSPF Interface Policy**（**OSPF** インターフェイス ポリシーの作成）を選択します。
4. **Name**（名前）に分かりやすい OSPF インターフェイス ポリシーの名前を入力します。
5. **MTU Ignore**（**MTU** 無視） を選択します。
6. **Submit**（送信） をクリックします。
7. **Next**（次へ）をクリックします。
8. **SVI** をクリックします。
9. **SVI Interfaces**（**SVI** インターフェイス）の右側にあるプラス（+）ボタンをクリックします。**Select SVI**（**SVI** の選択）ウィンドウが開きます。
10. **Virtual Port Channel**（仮想ポート チャネル）をクリックします。
11. ファイアウォールがリーフ スイッチに接続するポートとポート チャネル インターフェイスへのパスを選択します。
12. **Encap**（カプセル化） に、レイヤー 3 外部プロファイルに使用される VLAN カプセル化を入力します。
13. Mode（モード）で **Trunk**（トランク）を選択します。
14. **Side A IPv4 Primary Address**（サイド **A IPv4** プライマリ アドレス）フィールドに、レイヤー 3 外部プロファイルにアタッチしているパスのプライマリ IP アドレスを入力します。
15. **Side B IPv4 Primary Address**（サイド **B IPv4** プライマリ アドレス）フィールドに、レイヤー 3 外部プロファイルにアタッチしているパスのセカンダリ IP アドレスを入力します。
16. **OK** をクリックします。

STEP 14 | **OK** をクリックして Create Interface Profile（インターフェイス プロファイルの作成）ウィンドウを閉じます。

STEP 15 | **OK** をクリックして Create Node Profile（ノード プロファイルの作成）ウィンドウを閉じます。

STEP 16 | **Next**（次へ）をクリックします。

STEP 17 | **External EPG Networks**（外部 **EPG** ネットワーク）の右側にあるプラス（+）ボタンをクリックします。**Create Routed Outside**（外部ルーティングの作成）ウィンドウが開きます。

STEP 18 | **Name**（名前）フィールドに分かりやすい外部ネットワーク名を入力します。

©2023 Palo Alto Networks, Inc.

STEP 19 | 外部ネットワークにサブネットを追加します。

1. **Subnets**（サブネット）の右側にあるプラス（+）ボタンをクリックします。
2. サブネットのデフォルト ゲートウェイの IP アドレスとマスクを入力します。
3. **Export Route Control Subnet**（ルート制御サブネットのエクスポート）を選択します。
4. **External Subnets for External EPG**（外部 **EPG** の外部サブネット）を選択します。
5. **OK** をクリックします。

STEP 20 | **Finish**（完了）をクリックします。

外部ファイアウォールへのサブネットのアドバタイズの設定

デフォルトでは、ACI ファブリックのサブネットは外部ネットワークにアドバタイズされません。サブネットを外部にアドバタイズするように設定する必要があります。

STEP 1 | **Tenants**（テナント）タブでテナント名をダブルクリックします。

STEP 2 | **Networking**（ネットワーキング） > **Bridge Domains**（ブリッジ ドメイン） > **<your bridge domain>** を選択します。

STEP 3 | **L3 Configurations**（**L3** 設定）をクリックします。

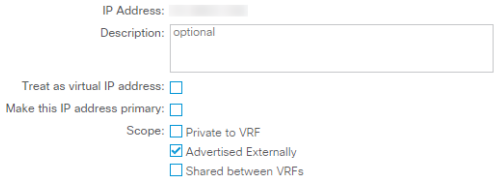
STEP 4 | **Associated L3 Outs**（関連付けられている **L3** アウト）の右側にあるプラス（+）ボタンをクリックします。

STEP 5 | 前の手順で作成したレイヤー 3 外部ルーティング ネットワーク接続を **L3 Out**（**L3** アウト）のドロップダウン リストから選択します。

STEP 6 | **Update**（更新）をクリックします。

STEP 7 | **Networking**（ネットワーキング） > **Bridge Domains**（ブリッジ ドメイン） > **<your bridge domain>** > **Subnets**（サブネット） > **<externally advertised subnet>** を選択します。

STEP 8 | Scope（スコープ）を **Advertised Externally**（外部にアドバタイズ）に設定します。



STEP 9 | **Submit**（送信） をクリックします。

アウトバウンド コントラクトの作成

DNS、NTP、HTTP、HTTPS トラフィックを許可するフィルターを使用してコントラクトを作成します。このコントラクトを使用して、VRF 内のすべてのエンドポイントが外部ネットワークに到達できるようにします。ただしファイアウォールに送信されるトラフィックを制限します。

STEP 1 | **Tenants**（テナント）タブでテナント名をダブルクリックします。

©2023 Palo Alto Networks, Inc.

STEP 2 | **Contracts**（コントラクト） > **Filters**（フィルター）を選択します。

STEP 3 | **Filters**（フィルター）を右クリックして**Create Filter**（フィルターの作成）を選択します。

STEP 4 | **Name**（名前）フィールドに分かりやすいフィルター名を入力します。

STEP 5 | UDP トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **UDP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **udp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **dns** を選択します。
6. **Update**（更新）をクリックします。

STEP 6 | TCP トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **TCP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **tcp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **dns** を選択します。
6. **Update**（更新）をクリックします。

STEP 7 | NTP トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **NTP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **udp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）フィールドに 123 と入力します。
6. **Update**（更新）をクリックします。

STEP 8 | HTTP トラフィックのフィルター項目を作成します。

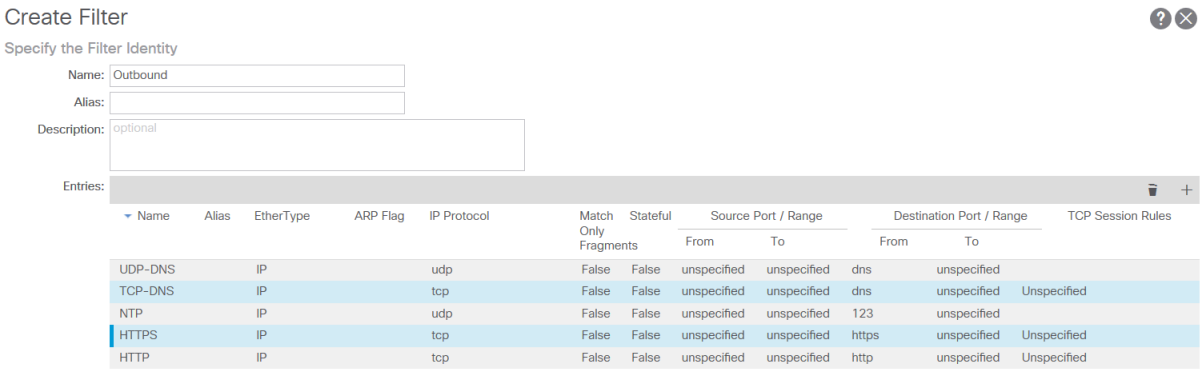
1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **HTTP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **tcp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **http** を選択します。
6. **Update**（更新）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 9 | HTTPS トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **HTTP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **tcp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **https** を選択します。
6. **Update**（更新）をクリックします。

STEP 10 | **Submit**（送信） をクリックします。



STEP 11 | アウトバウンド トラフィックのコントラクトを作成します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックし、**Contracts**（コントラクト）を選択します。
2. **Contracts**（コントラクト）を右クリックし、**Create Contract**（コントラクトの作成）を選択します。
3. **Name**（名前）に分かりやすいコントラクト名を入力します。
4. **Subjects**（サブジェクト） の右側にあるプラス（+）ボタンをクリックします。
5. **Name**（名前）に分かりやすいサブジェクト名を入力します。
6. **Filters**（フィルター） の右側にあるプラス（+）ボタンをクリックします。
7. 前に作成したフィルターをドロップダウン リストから選択します。
8. **OK**をクリックします。

STEP 12 | **Submit**（送信） をクリックします。

インバウンド Web コントラクトの作成

インバウンド トラフィックが、ファイアウォールの背後にあるサーバーに到達できるようにするため、コントラクトとフィルターも作成する必要があります。HTTP および HTTPS Web トラフィックに対し、ファイアウォールの背後にあるリソースへのアクセスを許可するコントラクトとフィルターを作成する手順を説明します。

STEP 1 | **Tenants**（テナント）タブでテナント名をダブルクリックします。

 ©2023 Palo Alto Networks, Inc.

STEP 2 | **Contracts**（コントラクト） > **Filters**（フィルター）を選択します。

STEP 3 | **Filters**（フィルター）を右クリックして**Create Filter**（フィルターの作成）を選択します。

STEP 4 | **Name**（名前）フィールドに分かりやすいフィルター名を入力します。

STEP 5 | HTTP トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **HTTP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **tcp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **http** を選択します。
6. **Update**（更新）をクリックします。

STEP 6 | HTTPS トラフィックのフィルター項目を作成します。

1. **Entries**（エントリ） の右側にあるプラス（+）ボタンをクリックします。
2. **Name**（名前）フィールドに分かりやすい **TCP** フィルター名を入力します。
3. **EtherType** のドロップダウン リストから **IP** を選択します。
4. **IP Protocol**（**IP** プロトコル）のドロップダウン リストから **tcp** を選択します。
5. **Destination Port From**（宛先ポートへのアクセス元）のドロップダウン リストから **https** を選択します。
6. **Update**（更新）をクリックします。

STEP 7 | **Submit**（送信） をクリックします。

STEP 8 | インバウンド Web トラフィックのコントラクトを作成します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックし、**Contracts**（コントラクト）を選択します。
2. **Contracts**（コントラクト）を右クリックし、**Create Contract**（コントラクトの作成）を選択します。
3. **Name**（名前）に分かりやすいコントラクト名を入力します。
4. **Subjects**（サブジェクト） の右側にあるプラス（+）ボタンをクリックします。
5. **Name**（名前）に分かりやすいサブジェクト名を入力します。
6. **Filters**（フィルター） の右側にあるプラス（+）ボタンをクリックします。
7. 前に作成したフィルターをドロップダウン リストから選択します。
8. **OK**をクリックします。

STEP 9 | **Submit**（送信） をクリックします。

©2023 Palo Alto Networks, Inc.

EPG へのアウトバウンド コントラクトとインバウンド コントラクトの適用

該当する EPG にインバウンド コントラクトとアウトバウンド コントラクトを適用する必要があります。

VRF 内のすべての EPG（EPG コレクション）がトラフィックを外部の宛先へ送信するには、各内部 EPG が外部 EPG とのコントラクトを設定する必要があります。通常、各内部 EPG と外部 EPG の間で個別のコントラクトを作成する必要があります。ただし vzAny オブジェクトを使用すると、すべての EPG に対して同一コントラクトを動的に適用できます。EPG コレクションはコントラクトを消費し、外部 EPG はコントラクトを提供します。コントラクトで特定のトラフィック プロファイルを設定するか、またはすべてのトラフィックをファイアウォールに送信して、ファイアウォールがデータセンターからのトラフィックを制御するようにできます。また、VRF に参加する新しい EPG には常にコントラクトが自動的に適用されます。

内部 EPG がプロバイダーであり、外部 EPG がコンシューマーであるようにするため、インバウンド コントラクトを適用します。内部 EPG に入るトラフィックは最初にコントラクトと突き合わせてチェックされ、その後、許可されたすべてのトラフィックは必要に応じてファイアウォールによりさらに保護されます。

STEP 1 | アウトバウンド コントラクトを VRF 内のすべての EPG に適用します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Networking**（ネットワーキング） > **VRFs** > **<you VRF>** > **EPG Collection for VRF**（**VRF** の **EPG** コレクション）を選択します。
3. **Consumed Contracts**（消費コントラクト）の右側にあるプラス（+）ボタンをクリックします。
4. **Name**（名前）のドロップダウン リストからアウトバウンド コントラクトを選択します。
5. **Update**（更新）をクリックします。
6. **Networking**（ネットワーキング） > **External Routed Networks**（外部ルーティング ネットワーク） > **<your external routed network>** > **Networks**（ネットワーク） > **External**（外部）を選択します。
7. **Provided Contracts**（提供されるコントラクト）の右側にあるプラス（+）ボタンをクリックします。
8. **Name**（名前）のドロップダウン リストからアウトバウンド コントラクトを選択します。
9. **Update**（更新）をクリックします。

©2023 Palo Alto Networks, Inc.

STEP 2 | 内部 EPG がインバウンド コントラクトを外部 EPG に提供するため、インバウンド コントラクトを適用します。

1. **Tenants**（テナント）タブでテナント名をダブルクリックします。
2. **Application Profiles**（アプリケーション プロファイル） > **<your application profile>** > **Application EPGs**（アプリケーション **EPG**） > **<your application EPG>** > **Contracts**（コントラクト）を選択します。
3. **Contracts**（コントラクト）を右クリックし、**Add Provided Contract**（提供されるコントラクトを追加）を選択します。
4. **Contract**（コントラクト）のドロップダウン リストからインバウンド コントラクトを選択します。
5. **Submit**（送信） をクリックします。
6. 同じテナントで、**Networking**（ネットワーキング） > **External Routed Networks**（外部ルーティング ネットワーク） > **<your external routed network>** > **Networks**（ネットワーク） > **External**（外部）を選択します。
7. Contracts（コントラクト）タブで、**Consumed Contracts**（消費コントラクト）の右側にあるプラス（+）ボタンをクリックします。
8. **Name**（名前）のドロップダウン リストからインバウンド コントラクトを選択します。
9. **Update**（更新）をクリックします。

North-South トラフィック用の仮想ルーターとセキュリティ ゾーンの作成

ファイアウォールで、ACI のテナントと VRF に対応する仮想ルーターとセキュリティ ゾーンを作成します。

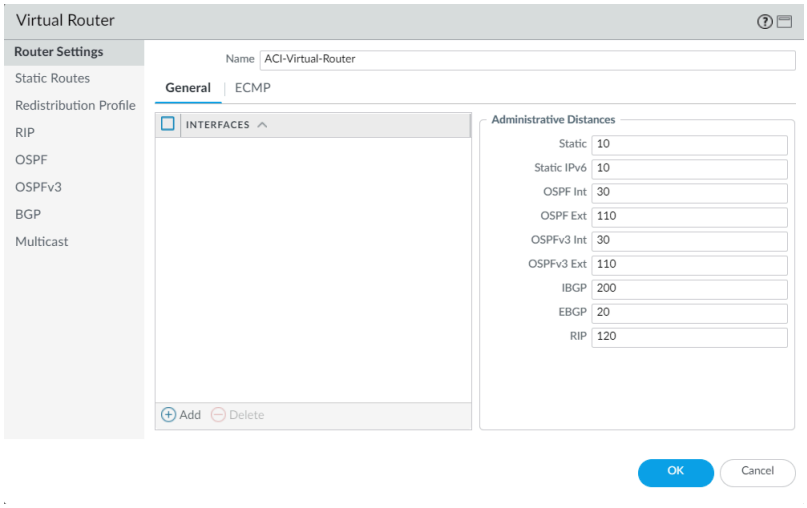
STEP 1 | ファイアウォールにログインします。

STEP 2 | **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、**Add**（追加）をクリックします。

STEP 3 | **Name**（名前）に分かりやすい仮想ルーター名を入力します。

©2023 Palo Alto Networks, Inc.

STEP 4 | **OK** をクリックします。

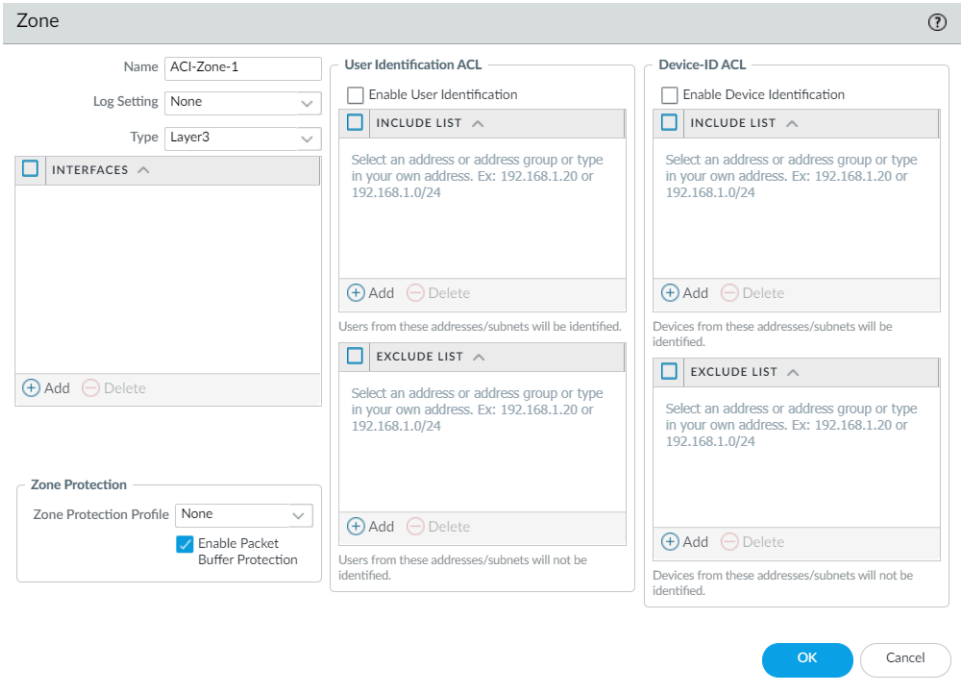


STEP 5 | **Network**（ネットワーク） > **Zones**（ゾーン）を選択し、**Add**（追加）をクリックします。

STEP 6 | **Name**（名前）に分かりやすいゾーン名を入力します。

STEP 7 | **Type**（タイプ）のドロップダウン リストから Layer 3（レイヤー 3）を選択します。

STEP 8 | **OK** をクリックします。



STEP 9 | 変更を **Commit (**コミット**)** します。

ネットワーク インターフェイスの設定

集約イーサネット インターフェイス、メンバー インターフェイス、およびファイアウォールが ACI リーフ スイッチへの接続に使用するサブインターフェイスを設定します。VM-Series ファイ

©2023 Palo Alto Networks, Inc.

アウォールを使用している場合は、集約インターフェイスではなく個別のインターフェイスを使用してください、

VM-Series ファイアウォールでは集約イーサネット グループはサポートされていません。

STEP 1 | **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、**Add Aggregate Group**（集約グループの追加）をクリックします。

STEP 2 | 2 番目の**Interface Name**（インターフェイス名）フィールドに、集約グループの番号を入力します。

STEP 3 | **Interface Type**（インターフェイス タイプ）のドロップダウン リストから Layer 3（レイヤー 3）を選択します。

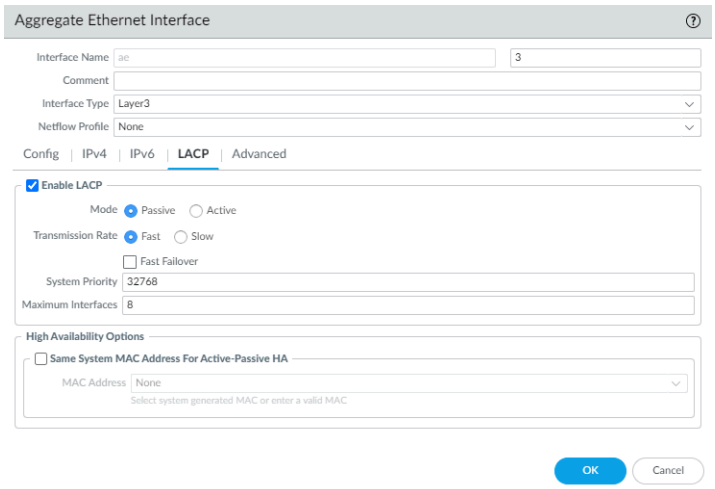
STEP 4 | **LACP** タブを選択し、**Enable LACP**（**LACP** を有効化）を選択します。

STEP 5 | **Transmission Rate**（伝送速度） として**Fast**（高速）を選択します。

STEP 6 | High Availability Options（高可用性オプション）で **Enable in HA Passive State**（**HA**パッシブ ステートを有効にする）を選択します。

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）は選択しないでください。このオプションを選択すると、スイッチに対しファイアウォール ペアが *1* つのデバイスとして示されるため、トラフィックがアクティブなファイアウォールではなく両方のファイアウォールに流れます。

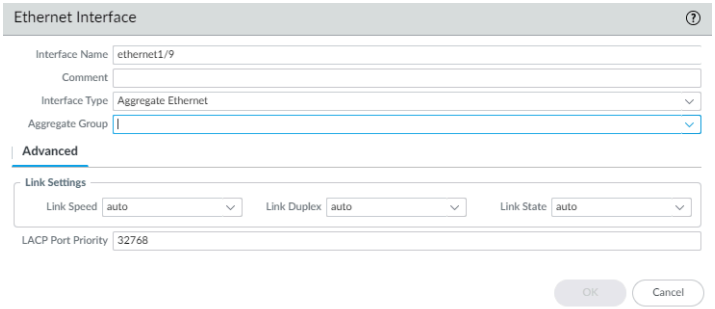
STEP 7 | **OK** をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 8 | イーサネット インターフェイス名をクリックしてこのインターフェイスを設定し、集約グループに追加します。

1. Interface Type（インターフェイス タイプ）のドロップダウン リストから **Aggregate Ethernet**（集約イーサネット） を選択します。
2. 集約イーサネット グループの設定で定義したインターフェイスを選択します。
3. **OK** をクリックします。
4. 集約イーサネット グループの他のメンバー インターフェイスごとにこの手順を繰り返します。



STEP 9 | 集約イーサネット インターフェイスでテナントと VRF のためのサブインターフェイスを追加します。

1. 集約イーサネット グループの行を選択し、**Add Subinterface**（サブインターフェイスの追加）をクリックします。
2. 2 番目の **Interface Name**（インターフェイス名）フィールドに、サブインターフェイスを識別する数値サフィックスを入力します。
3. **Tag**（タグ）フィールドに、サブインターフェイスの VLAN タグを入力します。
4. 以前に設定した仮想ルーターを **Virtual Router**（仮想ルーター）のドロップダウン リストから選択します。
5. 以前に設定したゾーンを **Zone**（ゾーン）のドロップダウン リストから選択します。
6. **IPv4** タブを選択します。
7. **Static**（静的）タイプを選択します。
8. **Add**（追加）をクリックし、CIDR 表記でサブインターフェイスの IP アドレスとネットワーク マスクを入力します。
9. **OK** をクリックします。

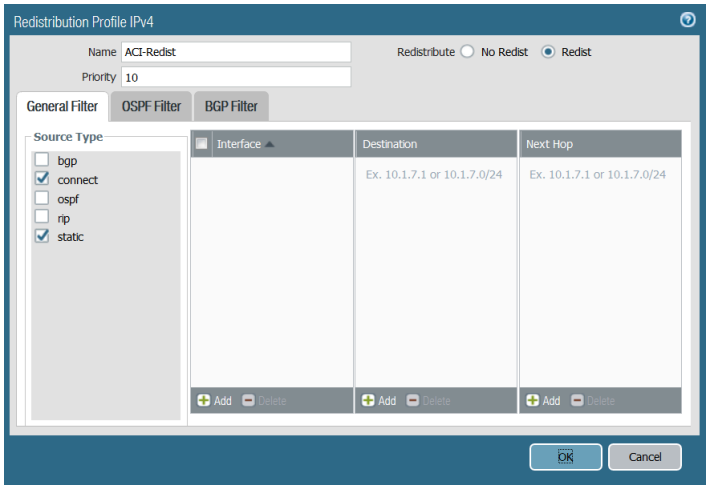
ルートの再配信と OSPF の設定

ファイアウォールからのルーティング情報を、リーフ スイッチに接続している外向きのルーターに対して使用可能にするため、ルートの再配信を設定します。次にファイアウォールで OSPF を設定し、ルーター ID、エリア番号、インターフェイスを割り当て、隣接を形成します。

©2023 Palo Alto Networks, Inc.

STEP 1 | ルートの再配信を設定します。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、前に作成した仮想ルーターをクリックします。
2. **Redistribution Profile**（再配信プロファイル） > **IPv4** > **Add**（追加）を選択します。
3. **Name**（名前）フィールドに分かりやすい再配信プロファイル名を入力します。
4. 優先度を入力します。
5. **Redistribute**（再配信）で **Redist**（再配信）を選択します。
6. 一般フィルター（**General Filters**）で **connect**（接続）と **static**（静的）を選択します。
7. **OK** をクリックします。



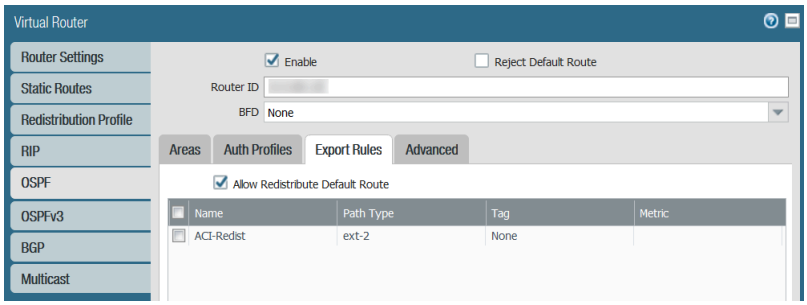
STEP 2 | OSPF を設定する。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター）を選択し、前に作成した仮想ルーターをクリックします。
2. **Router Settings**（ルーター設定） > **ECMP** を選択し、さらに **Enable**（有効）を選択します。
3. **OSPF** を選択し、**Enable**（有効）を選択します。
4. OSPF の **Router ID**（ルーター **ID**）を入力します。
5. **Area**（エリア）で**Add**（追加）をクリックします。
6. **Area ID**（エリア **ID**）を入力します。この値は、APIC で外部のルーティング ネットワークを作成したときに割り当てた値と一致している必要があります。ファイアウォー

©2023 Palo Alto Networks, Inc.

ルでは、これはドット付き 10 進数形式で入力する必要があります。APIC でエリア ID として 10 を入力した場合、ファイアウォールではこれは 0.0.0.10 に相当します。

7. **Interface**（インターフェイス） > **Add**（追加）を選択します。
8. 外部ネットワーク EPG に接続するインターフェイスを入力して **OK** をクリックします。
9. **Export Rules**（エクスポート ルール） > **Add**（追加）を選択します。
10. **Name**（名前）のドロップダウン リストから、先ほど作成した再配信リストを選択して **OK** をクリックします。
11. **Allow Redistribute Default Route**（デフォルト ルートの再配信を許可）を選択します。
12. **OK** をクリックします。



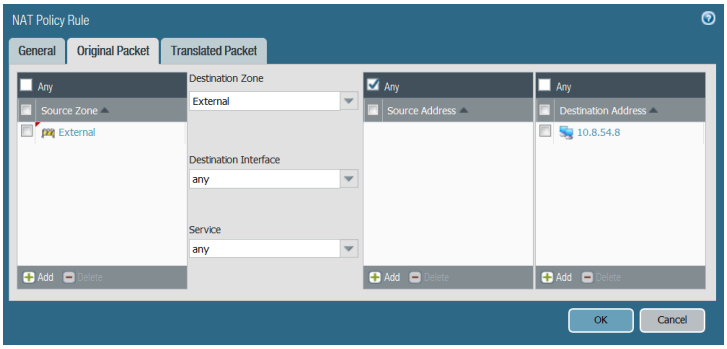
外部接続のための NAT の設定

NAT を設定する必要があるのは、ファイアウォールでデータセンター外部のネットワークへの接続に外部インターフェイスを使用している場合のみです。NAT は必須ではありませんが、以下の手順に従ってデータセンターのプライベート IP アドレスを外部のパブリック IP アドレスに変換できます。NAT をセットアップするため、最初にデータセンターの EPG 内部にあるトラフィック流入サーバーのアドレス変換を設定します。次に、EPG からのアウトバウンド トラフィックの送信元アドレスを外部インターフェイス IP アドレスに変換する NAT ポリシーを設定します。

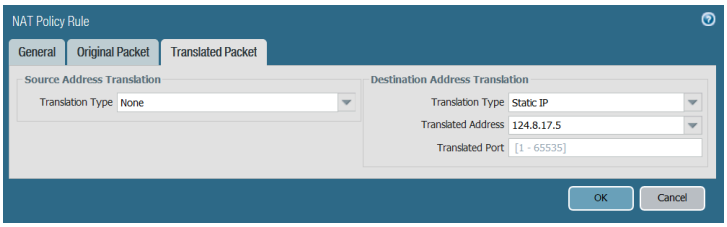
©2023 Palo Alto Networks, Inc.

STEP 1 | データセンターの EPG に流入するトラフィックのアドレス変換を設定します。

1. **Policies**（ポリシー） > **NAT** を選択して **Add**（追加）をクリックします。
2. **Name**（名前）に分かりやすい NAP ポリシー ルール名を入力します。
3. **Original Packet**（元のパケット）を選択し、**Source Zone**（送信元ゾーン）の下の**Add**（追加）をクリックします。
4. ドロップダウン リストから送信元ゾーンを選択します。
5. **Destination Zone**（宛先ゾーン）のドロップダウン リストから宛先ゾーンを選択します。
6. **Source Address**（送信元アドレス）で **Any**（いずれか）を選択します。
7. **Destination Address**（宛先アドレス）で **Add**（追加）をクリックし、外部 IP アドレスを入力します。



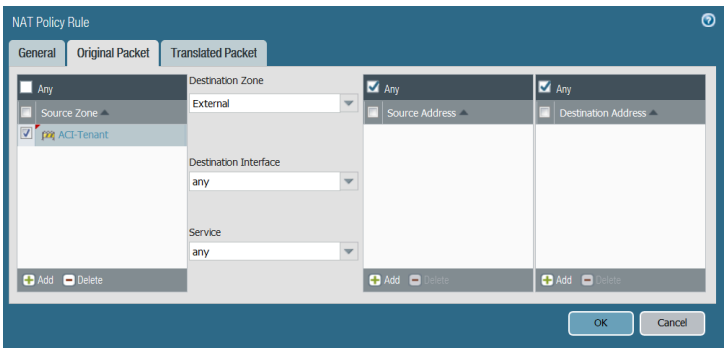
8. **Translated Packet**（変換済みパケット）タブの **Destination Address Translation**（宛先アドレスの変換）で **Translation Type**（変換タイプ）を選択します。
9. **Translated Address**（変換後アドレス）のドロップダウン リストからアドレスを選択します。
10. **OK** をクリックします。



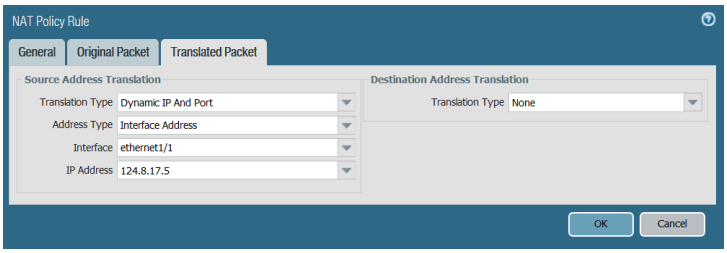
©2023 Palo Alto Networks, Inc.

STEP 2 | アウトバウンド トラフィックのアドレス変換を設定します。

1. **Policies**（ポリシー） > **NAT** を選択して **Add**（追加）をクリックします。
2. **Name**（名前）に分かりやすいアウトバウンド NAT ポリシー名を入力します。
3. **Original Packet**（元のパケット）を選択し、**Source Zone**（送信元ゾーン）の下の**Add**（追加）をクリックします。
4. ACI テナントと VRF に一致するゾーンを選択します。
5. **Destination Zone**（宛先ゾーン）のドロップダウン リストから外部ゾーンを選択します。



6. **Translated Packet**（変換済みパケット）タブの **Source Address Translation**（送信元アドレスの変換）で **Translation Type**（変換タイプ）を選択します。
7. 追加の必須アドレス情報を入力します。
8. **OK** をクリックします。



STEP 3 | 変更を **Commit (**コミット**)**します。

©2023 Palo Alto Networks, Inc.

Cisco ACI でのエンドポイント モニタリング

Panorama 用 Cisco ACI プラグインを使用すると、ダイナミック アドレス グループ（DAG）を使用して Cisco ACI ファブリックのセキュリティ ポリシーを作成できます。このプラグインは Cisco ACI 環境で Application Policy Infrastructure Controller（APIC）ファブリックの変更をモニタリングし、変更に関する情報を Panorama と共有します。Cisco ACI プラグインがインストールされている各 Panorama では、最大 16 の APIC クラスターをサポートできます。各モニタリング定義には 1 つのクラスターと 1 つの通知グループが含まれています。

Cisco ACI プラグインがモニタリングできるエンドポイントの数は、Panorama に割り当てられているメモリの量に応じて異なります。Panorama 仮想アプライアンスを使用している場合は、ご使用の環境のエンドポイントに必要な量のメモリを必ず割り当ててください。仮想 Panorama の準備の詳細については、『Panorama 管理者ガイド』を参照してください。

Panorama のメモリ	Endpoints（エンドポイント）
8GB	10,000
16GB	20,000

Cisco ACI プラグインはエンドポイント情報を処理し、ダイナミック アドレス グループに IP アドレスを配置するための一致基準として使用できるタグのセットに変換します。これらのタグの形式は次通りです。

cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.{epg_<EPG> | uepg_<micro-EPG>}

- **cisco.cl_<cluster>**— このタグは、Cisco ACI クラスターに基づいて IP アドレスを ダイナミック アドレス グループ にグループ化し、クラスターの名前を表示します。
- **cisco.cl_<cluster>.tn_<tenant>**— このタグは、テナントに基づいて IP アドレスを ダイナミック アドレス グループ にグループ化し、クラスターとテナントの名前を表示します。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>**—このタグは、アプリケーション プロファイルに基づいて IP アドレスを ダイナミック アドレス グループ にグループ化し、クラスター、テナント、およびアプリケーション プロファイルの名前を表示します。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.epg_<EPG>**— このタグは、EPG に基づいて IP アドレスを ダイナミック アドレス グループ にグループ化し、クラスター、テナント、アプリケーション プロファイル、および EPG の名前を表示します。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.uepg_<micro-EPG>**— このタグは、マイクロ EPG に基づいて IP アドレスを ダイナミック アドレス グループ にグループ化し、クラスター、テナント、アプリケーション プロファイル、およびマイクロ EPG の名前を表示します。
- **cisco.cl_ <cluster> .tn_ <tenant> .l2out_ <L2-external-endpoint>**— このタグは、L2外部エンドポイントに基づいてIPアドレスを ダイナミック アドレス グループ にグループ化し、クラスター、テナント、およびL2外部エンドポイントの名前を表示します。

©2023 Palo Alto Networks, Inc.

- **cisco.cl_ <cluster> .tn_ <tenant> .bd_ <bridge-domain> .subnet_ <subnet>**— このタグは、サブネットに基づいて IPアドレスを ダイナミック アドレス グループ にグループ化し、クラスター、テナント、ブリッジドメイン、およびサブネットの名前を表示します。

エンドポイントの IP アドレスからタグへのマッピング情報を取得するには、Cisco ACI 環境の APIC ファブリックごとにモニタリング定義を設定する必要があります。モニタリング定義では、Panorama が APIC に接続するために必要なユーザー名とパスワードが指定されます。また、デバイス グループと、Panorama がタグをプッシュするファイアウォールを含む対応通知グループも指定されます。モニタリング定義の設定が完了し、Cisco ACI プラグインがタグを取得したら、ダイナミック アドレス グループ を作成し、タグを一致条件として追加できます。

Cisco ACI プラグインは 2 つの間隔を使用して APIC から情報を取得します。1 番目の間隔は、モニタリング間隔です。

- モニタリング間隔 – モニタリング間隔は、プラグインがファブリックの変更を照会するまでに待機する時間です。変更が発生しなかった場合は、モニタリング間隔がリセットされます。変更が検出された場合は、プラグインは変更を処理してからモニタリング間隔をリセットします。デフォルトのモニタリング間隔は 60 秒です。モニタリング間隔は 60 秒～ 1 日（86,400 秒）に設定できます。
- 完全同期間隔 – 完全同期間隔とは、発生した変更に関係なくプラグインがすべてのファブリックの動的オブジェクトを更新するまでに待機する時間です。これにより、モニタリング間隔で変更イベントを検出できなかった場合にもプラグインがファブリックと同期します。デフォルトの完全同期間隔は 10 分です。完全同期間隔は、600 秒（10 分）から 86,400 秒（1 日）の間の値に設定できます。

  完全同期間隔は Panorama CLI を使用して設定する必要があります。

モニタリング間隔に完全同期間隔よりも大きい値を設定すると、完全同期間隔が無視され、モニタリング間隔ごとに完全同期が実行されます。

Panorama と APIC の間の接続が失われた場合、Panorama は再接続を 5 回試行します。5 回の試行が失敗すると、Panorama はクラスター内の変更のモニタリングを停止し、システム ログに再接続の試行を出力します。回復してクラスターのモニタリングを再開するには、Panorama でコミットを実行する必要があります。

- Cisco ACI 用 Panorama プラグインのインストール
- Cisco ACI プラグインの設定
- Cisco ACI Dashboard 用 Panorama プラグイン

Cisco ACI 用 Panorama プラグインのインストール

Cisco ACI でのエンドポイント モニタリングを開始するため、Cisco ACI プラグインをダウンロードし、Panorama にインストールします。

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。HA ペアの Panorama にプラグインをインストールする際は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

©2023 Palo Alto Networks, Inc.

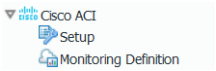
STEP 1 | ACI 環境にデプロイされているエンドポイントの数に対応できる十分なメモリが仮想 Panorama にあることを確認します。

STEP 2 | **Panorama** > **Plugins**（プラグイン）を選択します。

STEP 3 | **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。

STEP 4 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 5 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。



Cisco ACI プラグインの設定

プラグインのインストールが完了したら、モニタリング間隔を設定し、通知グループを設定し、Panorama と APIC ファブリック間の接続を確立する必要があります。

STEP 1 | （任意）完全同期間隔を設定します。

1. Panorama CLI にログインします。
2. 設定モードに切り替えます。

   admin@Panorama> configure
3. 以下のコマンドを使用して完全同期間隔を設定します。デフォルトの間隔は 600 秒（10 分）です。範囲は 600 ～ 86,400 秒（1 日）です。

   admin@Panorama# **set plugins cisco full-sync-interval <interval-in-seconds>**

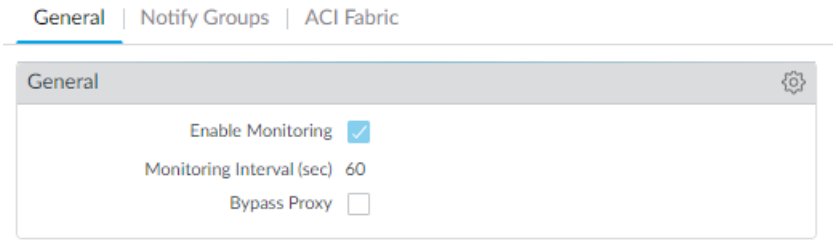
STEP 2 | Panorama Web インターフェイスにログインします。

STEP 3 | Panorama 上にファイアウォールをファイアウォールとして追加してデバイスグループを作成し、Panorama が取得した VM 情報をそれらのグループに通知するよう設定できるようにする必要があります。デバイスグループには、VM-Series ファイアウォールやハードウェアファイアウォール上の仮想システムも含められます。

©2023 Palo Alto Networks, Inc.

STEP 4 | モニタリングを有効にして、モニタリング間隔を設定し、プロキシのバイパスを有効にします。

1. **Panorama** > **Cisco ACI** > **Setup**（セットアップ） > **General**（全般）を選択します。
2. **Enable Monitoring**（モニタリングの有効化）を選択します。これにより、デプロイメント内のすべてのクラスタのモニタリングが有効になります。
3. **Monitoring Interval**（モニタリング間隔）を秒単位で設定します。モニタリング間隔は、Panorama が APIC から最新のネットワーク情報を取得する頻度です。デフォルトは 60 秒で、範囲は 60 ～ 86,400 秒（1 日）です。
4. （任意）Bypass Proxy（プロキシのバイパス）を選択して、Panorama と APIC 間の通信に対して設定されているプロキシ サーバー設定をバイパスします。プロキシ サーバー設定は、**Panorama** > **Setup**（セットアップ） > **Services**（サービス） > **Proxy Server**（プロキシ サーバー）で設定されています。このコマンドを実行すると、Panorama が APIC と直接通信しながら、他のサービスのためにプロキシ通信は維持されます。



STEP 5 | 通知グループを作成します。

1. **Panorama** > **Cisco ACI** > **Setup**（セットアップ） > **Notify Groups**（通知グループ）を選択します。
2. **Add**（追加）をクリックします。
3. **Name**（名前）に通知グループの分かりやすい名前を入力します。
4. ACI デプロイメントのデバイス グループを選択します。

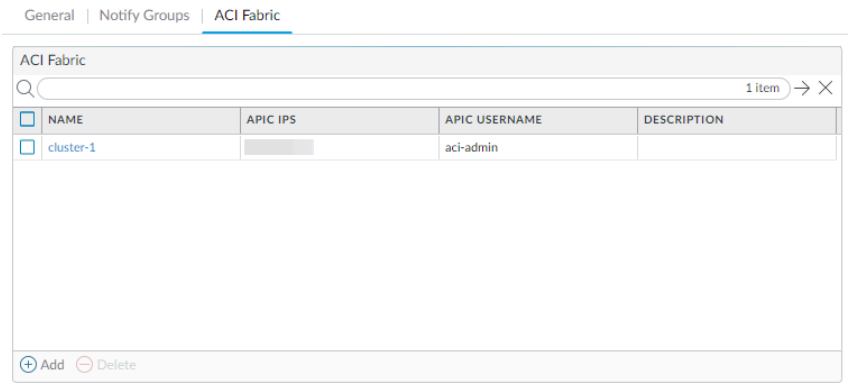
©2023 Palo Alto Networks, Inc.

STEP 6 | ACI ファブリック情報を追加します。

1. **Panorama** > **Cisco ACI** > **Setup**（セットアップ） > **ACI Fabric**（**ACI** ファブリック）を選択します。
2. **Name**（名前）に分かりやすいクラスタ名を入力します。
3. クラスタ内の各 APIC の IP アドレスまたは FQDN をコンマで区切って入力します。

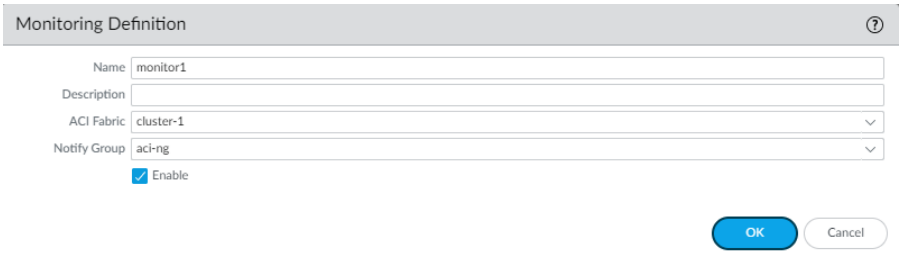
   FQDN を使用する場合は *URL* に *https://* を含めないでください。

4. APIC ユーザー名を入力します。
5. APIC パスワードを入力して確認します。
6. **OK** をクリックします。



STEP 7 | モニタリング定義を設定します。

1. **Panorama** > **Cisco ACI** > **Monitoring Definition**（モニタリング定義）を選択し、**Add**（追加）をクリックします。
2. この定義を使用する Cisco ACI クラスタを識別する **Name**（名前）、および任意で説明を入力します。
3. **Cluster Info**（クラスタ情報）および **Notify Group**（通知グループ）を選択します。
4. **OK** をクリックします。



STEP 8 | 変更を **Commit (**コミット**)**します。

©2023 Palo Alto Networks, Inc.

STEP 9 | Panorama 上で EPG 情報を閲覧できることを確認し、ダイナミック アドレス グループ用の一致条件を定義します。

一部のブラウザ拡張機能が、*Panorama* と *APIC* の間の *API* コールをブロックすることがあります。これが原因で、*Panorama* は一致条件を受信できなくなります。ブラウザ拡張機能を使用しているときに *Panorama* で一致条件が表示されない場合は、その拡張機能と *Synchronize Dynamic Objects*（動的オブジェクトの同期）を無効にして、*Panorama* に対して使用可能なタグを取り込みます。

Panorama は、新しいモニタリング定義の処理とダイナミック アクセスに使用できる一致条件の取り込みを即時に行いません。*EPG* 情報を検証する前に、設定したモニタリング間隔が経過するまで待ってください。

STEP 10 | EPG のアドレスがダイナミック アドレス グループに追加されていることを確認します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. ダイナミック アドレス グループの Addresses（アドレス）列で **More**（すべて表示）をクリックします。

   Panorama に、指定した一致条件に基づいてダイナミック アドレス グループに追加された IPアドレスのリストが表示されます。

STEP 11 | ポリシー内でダイナミック アドレス グループを使用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **[追加]** をクリックし、ポリシーの **[名前]** および **[説明]** を入力します。
3. **Source Zone (**送信元ゾーン**)** を追加して、トラフィックの送信元となるゾーンを指定します。
4. トラフィックが終端する **Destination Zone (**宛先ゾーン**)** を追加します。
5. **Destination Address (**宛先アドレス**)** については、先ほど作成したダイナミック アドレス グループを選択します。
6. トラフィックに対するアクション（**[許可]** または **[拒否]**）を指定し、必要に応じてデフォルト セキュリティ プロファイルをルールに関連付けます。
7. 手順 1～6 を繰り返し、もう 1 つポリシー ルールを作成します。
8. **Commit**（コミット）をクリックします。

   詳細については、「ポリシー内でのダイナミック アドレス グループの使用」を参照してください。

STEP 12 | APIC から動的オブジェクトをいつでも更新できます。更新するには、動的オブジェクトを同期します。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キ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有効化することができます。

1. **Panorama** > **Cisco ACI** > **Monitoring Definition**（モニタリング定義）を選択します。

©2023 Palo Alto Networks, Inc.

2. **Synchronize Dynamic Objects**（動的オブジェクトを同期）をクリックします。

HA フェイルオーバー発生時には、新たにアクティブになった *Panorama* が *APIC* に再接続してすべてのモニタリング定義のタグを取得しようと試みます。単一のモニタリング定義に再接続する際にもエラーが発生する場合、*Panorama* はシステム ログのメッセージを生成します。

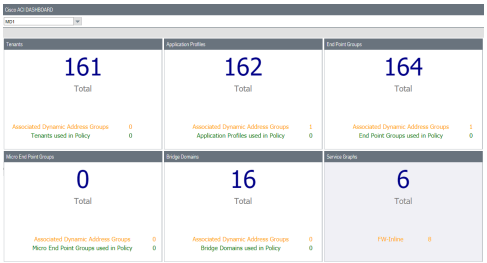
```
Unable to process subscriptions after HA switch-over;
 user-intervention required.
```

このエラーが発生する場合は *Panorama* にログインし、無効な *APIC IP* を削除したり有効な認証情報を指定したりするなどして問題を解決し、変更をコミットし、*Panorama* が再接続してすべてのモニタリング定義を取得できるようにする必要があります。*Panorama* が *APIC* に接続されていない状態でも、ファイアウォールはフェイルオーバー前に取得していたすべてのタグのリストを保持しており、その *IP* アドレスのリストに対して継続してポリシーを適用できます。フェイルオーバー エラーを解決する前にコミットを実行しないと、新しいアクティブ *Panorama* が *IP* からタグへのマッピング情報をプッシュせず、マッピング情報がファイアウォールから消去されます。ベストプラクティスとして、アクション中心のHTTPS 宛先へのログ転送を設定して即座に対応できるようにすることで、この問題を監視します。

Cisco ACI Dashboard 用 Panorama プラグイン

Cisco ACI Dashboard 用 Panorama プラグインは、プラグインが監視している ACI インフラを俯瞰したビューを提供しています。ダッシュボードは 2 つのページから成り立っています。最初のページは、プラグインが監視している各種オブジェクトの概要を、クリック可能な一連のタイルに表示しています。タイルをクリックすると、2 番目のページに移動して、タイルに表示されているオブジェクトの詳細情報が表示されます。

プラグインのインストール後、**Panorama** > **Cisco ACI** > **Dashboard**（ダッシュボード）を選択して、ダッシュボードにアクセスすることができます。



ダッシュボードは、*Panorama*に設定されているプレルール セキュリティ ポリシーのみクエリを行ったり、その数をカウントしたりします。ポストルール、デフォルト ルール、または *NAT* ルールは対象外です。

©2023 Palo Alto Networks, Inc.

ダッシュボード タイル	概要
Tenant Tags（テナント タグ） *APIC* でテナントのヘルス スコアが *0* の場合、そのテナントに関する情報は取得されません。そのため、*Panorama* のテナント カウントは、*APIC* の合計カウントとは一致しません。	Panorama が APIC から取得したテナント数合計を表示します。また、テナントに関連するダイナミック アドレス グループ数、およびポリシーで使用されているテナント数も表示されます。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **Tenant Name**（テナント名）—Panorama が取得したすべてのテナントを表示します。 • **Tenant Tag**（テナント タグ）—各テナントに関連する Panorama タグ。 • **Dynamic Address Group**（ダイナミック アドレス グループ）—記載されているタグに関連するダイナミック アドレス グループを表示します。 • **In Policy**（ポリシーで使用）—記載されているダイナミック アドレス グループがポリシーで使用されている場合に表示されます。
Application Profiles（アプリ	Panorama が APIC から取得したアプリケーション プロファイル数合計を表示します。また、アプリケーション プロファイルに関連するダイ

©2023 Palo Alto Networks, Inc.

ダッシュボード タイル	概要
ケーション プロファイル）	ナミック アドレス グループ数、およびポリシーで使用されているアプリケーション プロファイル数も表示されます。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **Application Profile Name**（アプリケーション プロファイル名）—Panoramaが取得したすべてのアプリケーション プロファイルを表示します。 • **Tenant Name**（テナント名）—記載されているアプリケーション プロファイルに関連するテナントを表示します。 • **Application Profile Tag**（アプリケーション プロファイル タグ）—各アプリケーション プロファイルに関連する Panorama タグ。 • **Dynamic Address Group**（ダイナミック アドレス グループ）—記載されているタグに関連するダイナミック アドレス グループを表示します。 • **In Policy**（ポリシーで使用）—記載されているダイナミック アドレス グループがポリシーで使用されている場合に表示されます。
End Point Groups（エンドポイント グループ）	Panorama が APIC から取得したエンドポイント グループ（EPG）数合計を表示します。また、EPG に関連するダイナミック アドレス グループ数、およびポリシーで使用されている EPG 数も表示されます。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **EPG Name**（**EPG** 名）—Panorama が取得したすべての EPG を表示します。 • **Application Profile Name**（アプリケーション プロファイル名）—EPG に関連するアプリケーション プロファイルを表示します。 • **Tenant Name**（テナント名）—記載されているアプリケーション プロファイルに関連するテナントを表示します。 • **EPG Tag**（**EPG** タグ）—各 EPG に関連する Panorama タグ。 • **Dynamic Address Group**（ダイナミック アドレス グループ）—記載されているタグに関連するダイナミック アドレス グループを表示します。 • **In Policy**（ポリシーで使用）—記載されているダイナミック アドレス グループがポリシーで使用されている場合に表示されます。
Micro End Point Groups（マイクロ	Panorama が APIC から取得したマイクロ エンドポイント グループ（EPG）数合計を表示します。また、マイクロ EPG に関連するダイナ

©2023 Palo Alto Networks, Inc.

ダッシュボード タイル	概要
エンドポイント グループ）	ミック アドレス グループ数、およびポリシーで使用されているマイクロ EPG 数も表示されます。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **Micro EPG Name**（マイクロ **EPG** 名）—Panorama が取得したすべてのマイクロ EPG を表示します。 • **Application Profile Name**（アプリケーション プロファイル名）—マイクロ EPG に関連するアプリケーション プロファイルを表示します。 • **Tenant Tag**（テナント タグ）—記載されているアプリケーション プロファイルに関連するテナントを表示します。 • **Micro EPG Tag**（マイクロ **EPG** タグ）—各マイクロ EPG に関連する Panorama タグ。 • **Dynamic Address Group**（ダイナミック アドレス グループ）—記載されているタグに関連するダイナミック アドレス グループを表示します。 • **In Policy**（ポリシーで使用）—記載されているダイナミック アドレス グループがポリシーで使用されている場合に表示されます。
Bridge Domains（ブリッジ ドメイン）	Panorama が APIC から取得したブリッジ ドメイン数合計を表示します。また、ブリッジ ドメインに関連するダイナミック アドレス グループ数、およびポリシーで使用されているブリッジ ドメイン数も表示されます。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **Bridge Domain Name**（ブリッジ ドメイン名）—Panorama が取得したすべてのブリッジ ドメインを表示します。 • **Tenant Name**（テナント名）—記載されているブリッジ ドメインに関連するテナントを表示します。 • **Bridge Domain Tag**（ブリッジ ドメイン タグ）—各ブリッジ ドメインに関連する Panorama タグ。 • **Dynamic Address Group**（ダイナミック アドレス グループ）—記載されているタグに関連するダイナミック アドレス グループを表示します。 • **In Policy**（ポリシーで使用）—記載されているダイナミック アドレス グループがポリシーで使用されている場合に表示されます。

©2023 Palo Alto Networks, Inc.

ダッシュボード タイル	概要
Service Graphs（サービス グラフ）	プラグインが監視しているサービス グラフ数合計、および監視対象サービス グラフと合致するファイアウォール数。 ドリル ダウンして以下の列を表示サルには、タイルをクリックします。 • **Service Graph Name**（サービス グラフ名）—Panoramaが取得したすべてのサービス グラフを表示します。 • **Producer EPG**（プロデューサー **EPG**）—サービス グラフに関連するプロデューサー EPG を表示します。 • **FW InLine**—サービス グラフに関連するファイアウォールを表示します。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

Cisco CSP での VM-Series ファイアウォールのセットアップ

VM-Series ファイアウォールをネットワーク仮想サービスとして Cisco Cloud Security Platform（CSP）にデプロイできます。Cisco CSP は RHEL KVM プラットフォームであるため、VM-Series ファイアウォールは KVM 用 VM-Series ファイアウォールの基本イメージを使用してデプロイされます。

Cisco CSP に VM-Series ファイアウォールをデプロイすることで、ワークロードを保護し、高度な脅威を防ぎ、仮想ネットワーク上のアプリケーションの可視化を向上できます。

> Cisco CSP での VM-Series のシステム要件
> Cisco CSP での VM-Series ファイアウォールのデプロイ

Cisco CSP での VM-Series のシステム要件

Cisco CSP には、VM-Series ファイアウォールの複数のインスタンス（スタンドアロンまたは HA ペア）を作成およびデプロイできます。

VM-Series ファイアウォールは次の要件を満たしていなければなりません。

- サポートしているバージョンの CSP と PAN-OS については、互換性マトリックスを参照してください。
- ブートストラップ パッケージ（ISO ファイルに変換）
- VM-Series モデルの最小ハードウェア要件については、「VM-Series のシステム要件」を参照してください。
- 2 つ以上のネットワークインターフェイス（vNIC）。1 つは管理インターフェイスの vNIC 専用、もう 1 つはデータ インターフェイス用です。データ トラフィック用の vNIC は 8 つまで追加できます。
- Cisco CSP 上の VM-Series ファイアウォールは、VM-50 を除くすべての VM-Series モデルをサポートしています。
- SR-IOV とパケット MMAP モードのみ: DPDK はサポートされていません。

©2023 Palo Alto Networks, Inc.

Cisco CSP での VM-Series ファイアウォールのデプロイ

VM-Series ファイアウォールを Cicso CSP にデプロイするには、以下の手順を実行します。

STEP 1 | VM-Series qcow2 ベース イメージ ファイルをカスタマー サポート ポータルからダウンロードします。

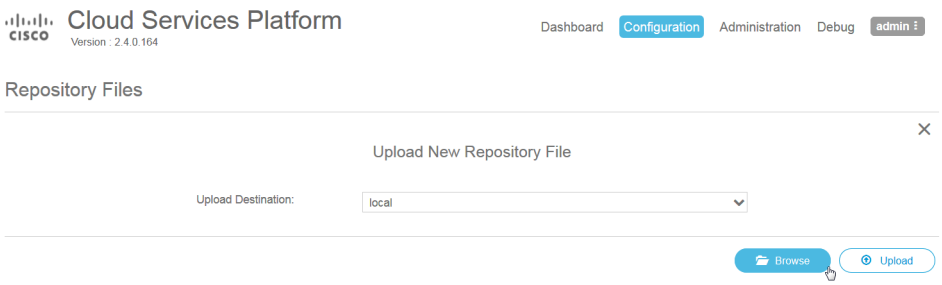
STEP 2 | VM-Series ファイアウォールのブートストラップ ISO ファイルを作成します。

1. VM-Series ファイアウォールの ブートストラップ パッケージ を作成します。
2. 使い慣れているツールを使用して、ブートストラップ パッケージを含む ISO ファイルを作成します。

STEP 3 | Cisco CSP Web インターフェイスにログインします。

STEP 4 | VM-Series ファイアウォールの qcow2 イメージと ISO ファイルをアップロードします。

1. **Configuration**（設定） > **Repository**（リポジトリ）を選択します。
2. プラス（+）アイコンをクリックします。
3. **Browse**（参照）をクリックして qcow2 ファイルに移動します。
4. **Upload**（アップロード）をクリックします。
5. **Browse**（参照）をクリックして ISO ファイルに移動します。
6. **Upload**（アップロード）をクリックします。



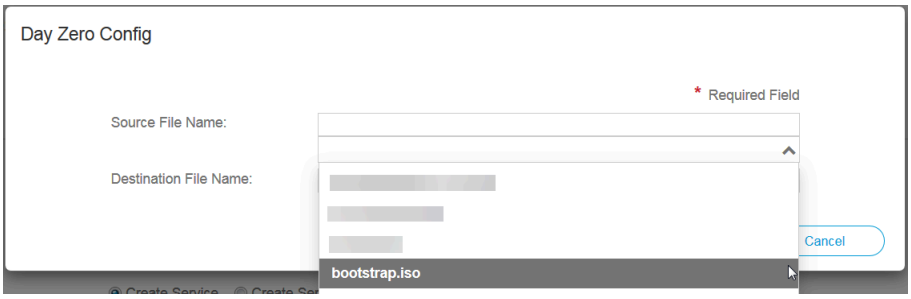
©2023 Palo Alto Networks, Inc.

STEP 5 | VM-Series ファイアウォール サービスを作成します。

1. VM-Series ファイアウォールの分かりやすい名前を **Name**（名前）に入力します。
2. ドロップダウン リストから **Target Host Name**（ターゲット ホスト名）を選択します。
3. アップロードした qcow2 ファイルを **Image Name**（イメージ名）のドロップダウン リストから選択します。



4. Day Zero Config（デイ ゼロ設定）を選択します。
   1. **Day Zero Config**（デイ ゼロ設定）のプラス（+）アイコンをクリックします。
   2. **Source File Name**（ソース ファイル名）のドロップダウン リストからブートストラップ ISO ファイルを選択します。
   3. **Submit**（送信） をクリックします。



5. VM-Series ファイアウォール モデルに必要な数のコアとメモリを割り当てます。
6. ブートストラップ ISO ファイルで設定されている VM-Series インターフェイスの数に対応できる十分な数の vNIC を追加します。

サービス インスタンスの作成とデプロイの詳細については、Cisco Cloud Service Platform のドキュメントを参照してください。

STEP 6 | ブートストラップ プロセスが完了したら、ブートストラップ ISO ファイルに指定した管理 IP アドレスを使用して VM-Series ファイアウォールにログインします。

ファイアウォールが稼働しており、ブートストラップ パッケージで定義したパラメータに基づいて設定されているはずです。

©2023 Palo Alto Networks, Inc.

Cisco TrustSec のエンドポイント監視

Cisco TrustSec の Panorama Plugin をインストールして設定し、環境内のエンドポイントのIPアドレスを取得して、ダイナミック アドレス グループを使用してそれらのエンドポイントのセキュリティポリシーを構築します。

- Cisco TrustSec 用 Panorama プラグイン
- Cisco TrustSec 用 Panorama プラグインのインストール
- Cisco TrustSec 用 Panorama プラグインの設定
- Cisco TrustSec用Panoramaプラグインのトラブルシューティング

Cisco TrustSec 用 Panorama プラグイン

Cisco TrustSec 用 Panorama プラグインにより、ダイナミック アドレス グループを使って TrustSec 環境のセキュリティ ポリシーを作成することができます。このプラグインは、TrustSec セキュリティ グループの変更を監視して、その情報を Panorama で登録し、IP 情報をファイアウォールに転送します。そのため、Panorama は対応するエンドポイントに正しいポリシーを適用することができます。Cisco TrustSec 用 Panorama プラグインは、最大 16 台の pxGrid（Cisco ISE）サーバーをサポートしています。

Cisco TrustSec の *Panorama* プラグインは現在、動的オブジェクトをサポートしていますが、静的オブジェクトはサポートしていません。

Panorama プラグインはエンドポイント情報を処理し、処理した情報を一連のタグに変換します。これらのタグは、ダイナミック アドレス グループ に IP アドレスを含めるときの一致条件として使用できます。Panorama は、pxGrid サーバー上の各セキュリティ グループ タグ（SGT）に対してタグを作成します。これらのタグの形式は次通りです。

cts.svr_<pxgrid-server-name>.sgt_<SGT-name>

エンドポイントの IP アドレスからタグへのマッピング情報を取得するには、環境の pxGrid ごとにモニタリング定義を設定する必要があります。pxGrid サーバー設定はユーザー名とパスワードを指定しており、Panorama が pxGrid に接続するためのモニタリング定義により参照されます。また、Panorama の証明書プロファイルを使って pxGrid サーバー ID を検証するように、プラグインを設定することができます。また、デバイス グループと、Panorama がタグをプッシュするファイアウォールを含む対応通知グループも指定されます。モニタリング定義の設定が完了し、プラグインがタグを取得したら、ドメイン アドレス グループを作成し、タグを一致条件として追加できます。

The Panorama Plugin for Cisco TrustSecバージョン1.0.2以降は、Bulk Sync（一括同期）およびPubSubモニタリングモードをサポートしています。プラグインは、Panoramaのバージョンに基づいてモードを選択します。Panoramaのバージョンが10.0.0未満の場合は一括同期モード、10.0.0以降の場合はPubSubモードを使用します。ユーザーインターフェイスには、デフォルトのモニタリングモードの設定オプションが表示されます。

- 一括同期
- PubSub

一括同期

一括同期モードは、モニタリング間隔と完全同期間隔の 2 種類の間隔を使って、pxGrid サーバーから情報を取得します。このモードは、Panoramaバージョン10.0.0 未満にPanorama Plugin for Cisco TrustSecバージョン1.0.2以降がインストールされている場合のデフォルトモードになります。Panoramaバージョン10.0.0未満は、configdへの10秒ごとのIP-tabアップデートをサポートしています。

- モニタリング間隔 – モニタリング間隔は、プラグインが変更を照会するまでに待機する時間です。変更がなかった場合は、モニタリング間隔がリセットされます。変更があった場合

©2023 Palo Alto Networks, Inc.

は、変更が処理されてからモニタリング間隔がリセットされます。デフォルトのモニタリング間隔は 60 秒です。モニタリング間隔は 10 秒～ 1 日（86,400 秒）に設定できます。

Cisco TrustSec 1.0.0 用 *Panorama* プラグインがインストールされている場合、最低モニタリング間隔は *30* 秒です。

- 完全同期間隔 – 完全同期間隔とは、発生した変更に関係なくプラグインがすべての pxGrid サーバーの動的オブジェクトを更新するまでに待機する時間です。これにより、モニタリング間隔で変更イベントを検出できなかった場合にもプラグインが pxGrid サーバーと同期します。完全同期間隔は、600 秒（10 分）～86,400 秒（1 日）の間の値に設定できます。完全同期間隔はPanorama CLIから設定する必要があります。

モニタリング間隔が完全同期間隔よりも大きい場合、完全同期間隔が無視され、モニタリング間隔ごとに完全同期が実行されます。

PubSub

PubSubモードは、Cisco ISEサーバー（サブスクリプションデーモン）から直接通知を監視し、IPタグを解析して、関連する情報をタグ処理デーモン（tag-proc）に送信します。PubSubは、Panoramaバージョン10.0.0以降にPanorama Plugin for Cisco TrustSecバージョン1.0.2以降がインストールされている場合のデフォルトモードになります。Panoramaバージョン10.0.0以降は、100ミリ秒ごとの、configdへのIP-tabアップデートをサポートしています。

- プッシュ間隔–プッシュ間隔は、各プッシュ配信間の時間です。前のプッシュ配信に時間がかかりすぎた場合、次のプッシュ配信は前のプッシュ完了後即座に行われます。最低プッシュ配信間隔は100ミリ秒（0秒）で、最大は60秒になります。デフォルトのプッシュ間隔は0秒です。
- **Enable Full Sync**（完全同期を有効にする）–このオプションを有効にすると、完全な更新が行われます。完全同期を有効にした場合、完全同期間隔を設定することができます。デフォルトはno（なし）です。
- 完全同期間隔 – 完全同期間隔とは、発生した変更に関係なくプラグインがすべての pxGrid サーバーの動的オブジェクトを更新するまでに待機する時間です。デフォルトの完全同期間隔は 10 分です。完全同期間隔は、600 秒（10 分）～86,400 秒（1 日）の間の値に設定できます。完全同期間隔はPanorama CLIから設定する必要があります。
- **Reconnection interval**（再接続間隔）–初期の再接続間隔は1秒で、前の再接続が失敗した場合は2倍になります。最大の再接続間隔は64秒です。再接続の試行回数に制限はありません。

©2023 Palo Alto Networks, Inc.

Cisco TrustSec 用 Panorama プラグインのインストール

Cisco TrustSec でのエンドポイント モニタリングを開始するため、Cisco TrustSec プラグインをダウンロードし、Panorama にインストールします。プラグインのバージョンとPanoramaのバージョンの相関については、互換性マトリックスの「Panoramaプラグイン」を参照してください。

*Cisco TrustSec*プラグインのアップグレード/ダウングレードでは、コミットを行う必要があります。

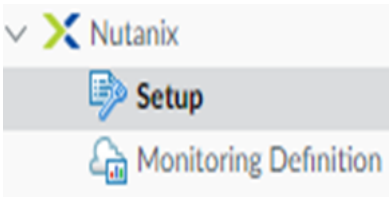
Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。HA ペアの Panorama アプライアンスにプラグインをインストールする際は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 1 | **Panorama** > **Plugins**（プラグイン）を選択します。

STEP 2 | 最新バージョンのプラグインを入手するには、**Check Now**（今すぐチェック）をクリックします。

STEP 3 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 4 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。



 ©2023 Palo Alto Networks, Inc.

Cisco TrustSec 用 Panorama プラグインの設定

プラグインをインストールしたら、Cisco TrustSec プラグイン 設定に通知グループを割り当てる必要があります。通知グループは、Panorama が pxGrid サーバーから取得したすべてのタグをプッシュ配信する必要があるファイアウォールを含む、デバイス グループのリストです。

Cisco TrustSec プラグインをインストールした各 Panorama は、最大 16 台の pxGrid サーバーと 16 件のモニタリング定義をサポートすることができます。各モニタリング定義には 1 つの pxGrid サーバーと 1 つの通知グループが含まれています。

Cisco TrustSec の *Panorama* プラグインは現在、動的オブジェクトをサポートしていますが、静的オブジェクトはサポートしていません。

次の設定手順は、一括同期およびPubSubの両方のモニタリングモードに対応しています。モニタリングモードに基づいて、一部のユーザーインターフェイス機能が有効になる、または表示されます。

STEP 1 | 完全同期間隔をデフォルトの 600 秒（10 分）から変更したい場合は、適切な値を設定します。

1. Panorama CLI にログインします。
2. 設定モードに切り替えます。

   admin@Panorama> configure
3. 以下のコマンドを使用して完全同期間隔を設定します。範囲は 600 ～ 86,400 秒（1 日）です。

   admin@Panorama# set plugins cisco_trustsec full-sync-interval <interval-in-seconds>

STEP 2 | Panorama Web インターフェイスにログインします。

STEP 3 | Panorama 上にファイアウォールをファイアウォールとして追加してデバイスグループを作成し、Panorama が取得した VM 情報をそれらのグループに通知するよう設定できるようにする必要があります。デバイスグループには、VM-Series ファイアウォールやハードウェア ファイアウォール上の仮想システムも含められます。

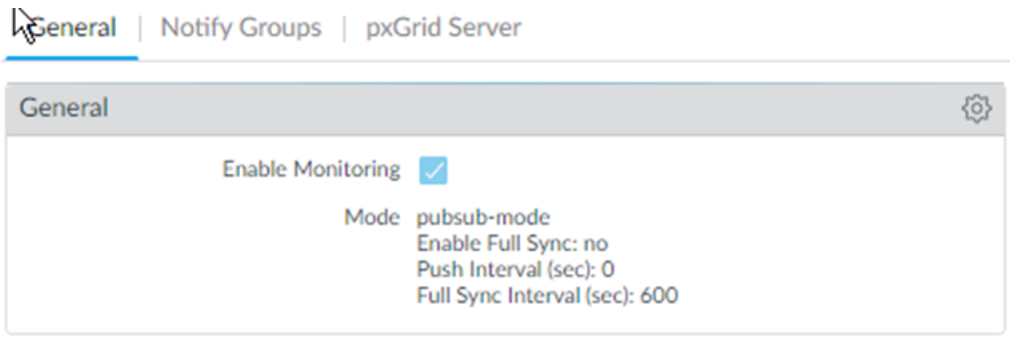
©2023 Palo Alto Networks, Inc.

STEP 4 | Cisco TrustSecのモニタリングを設定します。

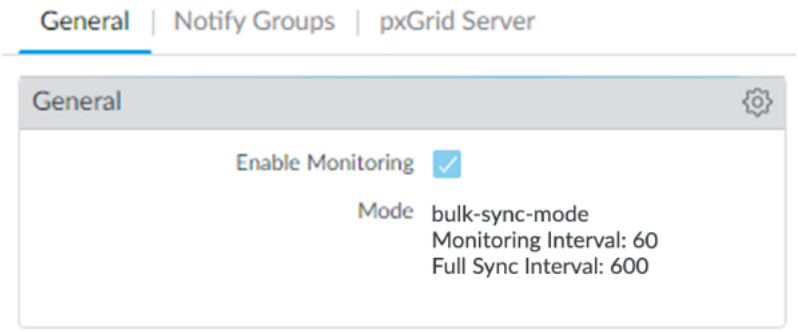
1. **Panorama** > **Cisco TrustSec** > **Setup**（セットアップ） > **General**（全般）を選択します。

   デフォルトで、**Enable Cisco TrustSec Monitoring**（**Cisco TrustSec**モニタリングを有効にする）は有効になっています。これにより、デプロイメント内のすべてのクラスタのモニタリングが有効になります。

   Panorama 10.0.0以降にPanorama plugin for Cisco TrustSec 1.0.2以降がインストールされている場合、PubSubモニタリングモードが選択されます。



   プラグインがPanorama 10.0.0以前にインストールされている場合、Bulk Syncモードが選択されます。



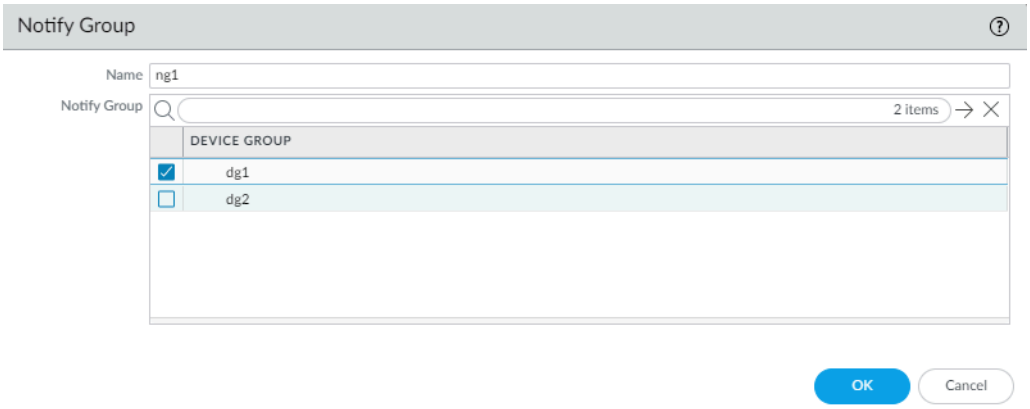
2. 設定パラメータを編集するには、歯車をクリックします。
   - **Push Interval**（プッシュ間隔）（PubSubのみ）—最低0、最大60秒を指定します。デフォルトは0（100 ミリ秒）です。
   - **Enable Full Sync**（完全同期を有効にする）（PubSubのみ、任意）—完全同期を有効にする場合に、このオプションを選択します。デフォルトはno（なし）です。
   - **Full Sync Interval**（完全同期間隔）。
     - PubSub—Enable Full Sync（完全同期を有効にする）を選択している場合、完全同期間隔（秒）を設定することができます。デフォルト値は600で、範囲は600 ～ 86400秒（1日）です。
     - Bulk Sync（一括同期）—デフォルトで、Bulk Syncモードが有効になっています。範囲は600～86400秒（1日）で、デフォルト値は600です。
   - **Monitoring Interval**（モニタリング間隔）（Bulk Syncのみ）—10～86400秒、デフォルトは60—PanoramaがpxGridサーバーにエンドポイントアドレス情報をポーリング

 ©2023 Palo Alto Networks, Inc.

する間隔を設定します。これは、モニタリングイベントの終了と、次のイベントの開始間の期間です。

STEP 5 | 通知グループを作成します。

1. **Panorama** > **Cisco TrustSec** > **Setup**（セットアップ） > **Notify Groups**（通知グループ）を選択します。
2. **Add**（追加）をクリックします。
3. **Name**（名前）に通知グループの分かりやすい名前を入力します。
4. 以前に作成したデバイス グループを選択します。



STEP 6 | （任意）pxGrid サーバーのサーバー ID 検証を有効にしている場合、Panorama で証明書プロファイルを設定します。

STEP 7 | pxGrid クライアント名とクライアント パスワードを作成、アクティブ化して承認します。

1. Panorama CLI にログインします。
2. 以下のコマンドを実行してクライアント名を作成します。
   - 証明書プロファイルがある場合は、次のようにクライアント名を作成します。

     admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>
   - ステップ6をスキップし、証明書がない場合は、次のコマンドを入力します:

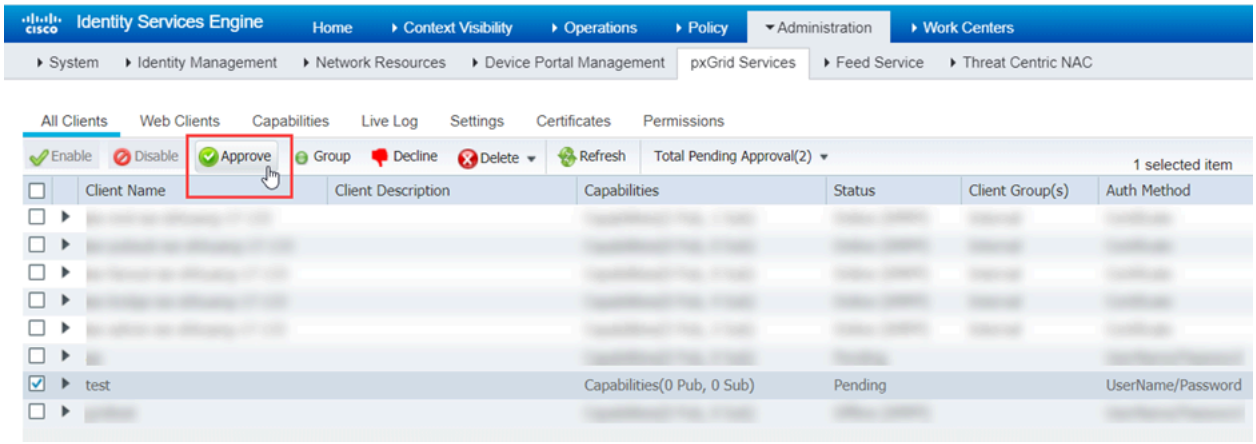
     request plugins cisco_trustsec create-account server-cert-verification-enabled no client-name <client-name>host <host-name>
3. 以下のコマンドを実行してクライアント名を作成します。

```
admin@Panorama> request plugins cisco_trustsec create-account
 client-name test host 10.10.10.15

AccountCreate in progress...
AccountCreate successful.
  client nodename: test
  client password: PmVKBmPgf63Hypq
```

 ©2023 Palo Alto Networks, Inc.

```
AccountActivate in progress...
AccountActivate successful.

Please approve the account on the server.
```

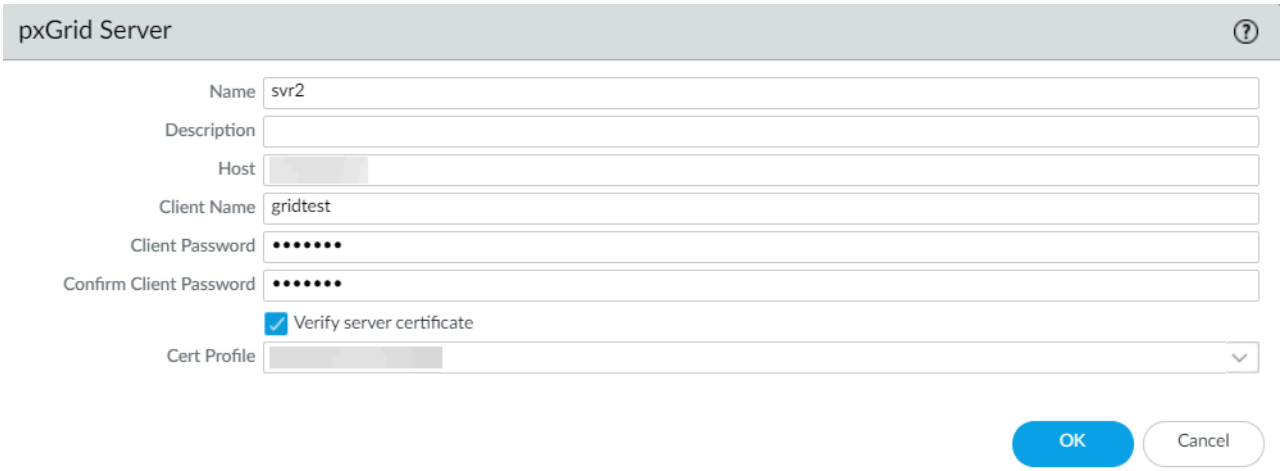
4. Cisco ISE サーバーにログインして、アカウントを承認します。
5. **Administration**（管理） > **pxGrid Services**（**pxGrid** サービス） > **All Clients**（すべてのクライアント）を選択します。
6. Panorama で作成したクライアント名を選択します。
7. **Approve**（承認）をクリックします。



©2023 Palo Alto Networks, Inc.

STEP 8 | pxGrid サーバー情報を追加します。Cisco TrustSec 用 Panorama プラグインは、最大 16 台の pxGrid（Cisco ISE）サーバーをサポートしています。

1. **Panorama** > **Cisco TrustSec** > **Setup**（セットアップ） > **pxGrid Server**（**pxGrid** サーバー）を選択します。
2. **Name**（名前）に、分かりやすい pxGrid サーバー名を入力します。
3. **Host**（ホスト）フィールドに、pxGrid サーバーの IP アドレスまたは FQDN を入力します。
4. 前のステップで作成したクライアント名を入力します。
5. 前のステップで作成したクライアントのパスワードを入力、確認します。
6. pxGrid サーバー ID を検証します。
   1. **Verify server certificate**（サーバー証明書の確認）を選択します。
   2. **Cert Profile**（証明書プロファイル）ドロップダウンから証明書プロファイルを選択します。
7. **OK** をクリックします。



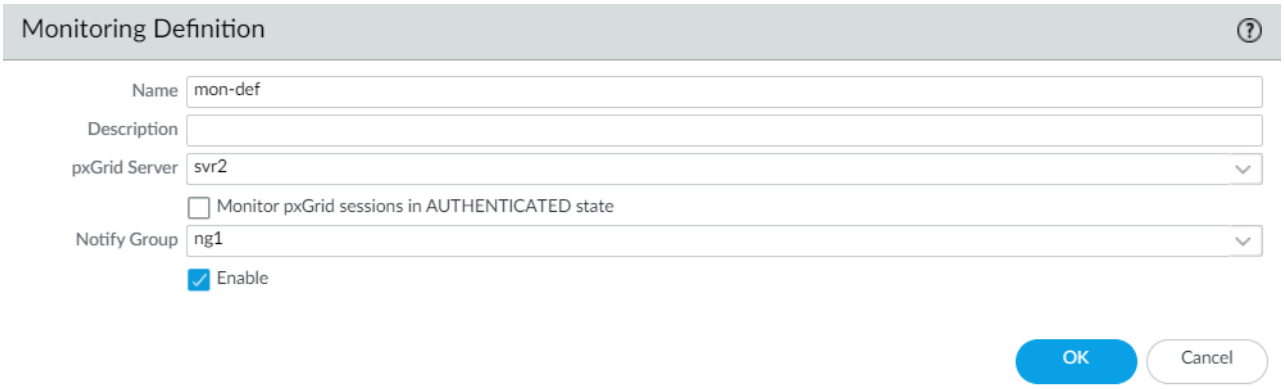
STEP 9 | モニタリング定義を設定します。

1. **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（モニタリング定義）を選択し、**Add**（追加）をクリックします。
2. このモニタリング定義を識別する **Name**（名前）、および必要に応じて**Description**（説明）を入力します。
3. **pxGrid Server**（**pxGrid** サーバー）を選択します。
4. （任意）**Monitor pxGrid sessions in AUTHENTICATED state**（**AUTHENTICATED** 状態の **pxGrid** セッションを監視）するように、Panorama を設定します。デフォルトでPanoramaは、「STARTED」 状態のセッションからIPとタグのマッピングを取得します。ISEセッションは、対応するアカウンティング開始パケットが存在する場合に、

©2023 Palo Alto Networks, Inc.

「STARTED」状態になります。セッションのアカウンティング開始パケットが存在しない場合、セッション状態は「AUTHENTICATED」になります。

5. **Notify Group**（通知グループ）を選択します。
6. **OK** をクリックします。



STEP 10 | 変更を **Commit (**コミット**)**します。

STEP 11 | Panoramaがダイナミックアドレスグループ定義のためにSGTタグを学習できるように、アクティブなISEセッションを作成します。アクティブなセッションを作成するには、ISEを使ってデバイスを認証します。

Panoramaは、ISE上でSGTタグを収集しません。

©2023 Palo Alto Networks, Inc.

STEP 12 | ダイナミック アドレス グループを作成して、そのアドレスがダイナミック アドレス グループに追加されていることを確認します。

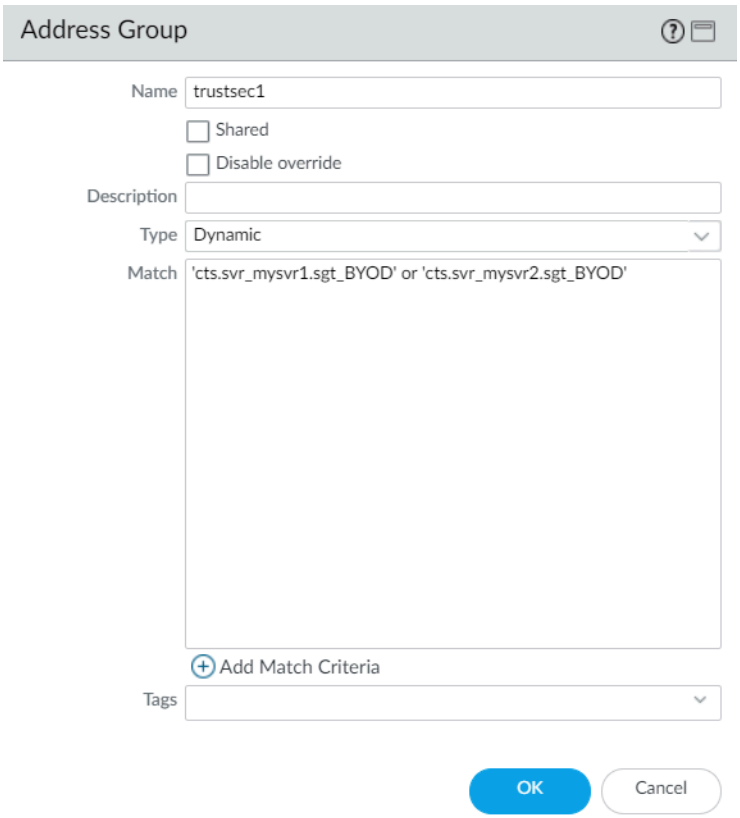
1. **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. Cisco TrustSec 環境内のエンドポイントのモニタリング用に作成したデバイス グループを、**Device Group**（デバイス グループ）ドロップダウンから選択します。
3. **Add**（追加）をクリックし、ダイナミック アドレス グループの **Name**（名前）および **Description**（説明）を入力します。

   ダイナミックアドレスグループの命名規則は、**`cts.svr_<server-name>.sgt_<SGT-name>`**となります。
4. **Type**（タイプ）で **Dynamic**（ダイナミック）を選択します。
5. **Add Match Criteria**（一致条件の追加）をクリックします。
6. **And** 演算子または **Or** 演算子を選択し、セキュリティ グループ名の横にあるプラス（+）アイコンをクリックして、ダイナミック アドレス グループに演算子を追加します。

   Panoramaは、アクティブセッションから学習したセキュリティグループタグのみを表示できます。ライブセッションのセキュリティグループタグは、一致条件リストに表示されます。
7. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
8. ダイナミック アドレス グループの Addresses（アドレス）列で **More**（すべて表示）をクリックします。

   Panorama に、指定した一致条件に基づいてダイナミック アドレス グループに追加された IP アドレスのリストが表示されます。

©2023 Palo Alto Networks, Inc.



STEP 13 | ポリシー内でダイナミック アドレス グループを使用します。

ダイナミックアドレスグループは、それをポリシーに添付するまでは空の状態になります。ポリシーがダイナミックアドレスグループを使用しない限り、ダイナミックアドレスグループに*IP*アドレスは表示されません。

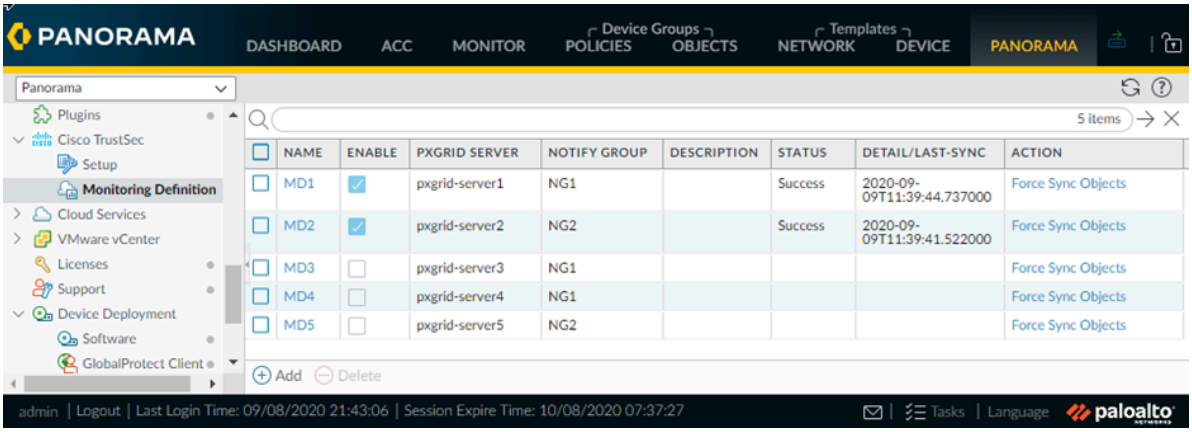
1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. [追加] をクリックし、ポリシーの [名前] および [説明] を入力します。
3. **Source Zone** (送信元ゾーン) を追加して、トラフィックの送信元となるゾーンを指定します。
4. トラフィックが終端する **Destination Zone** (宛先ゾーン) を追加します。
5. **Destination Address** (宛先アドレス)では、作成したダイナミック アドレス グループを選択します。
6. トラフィックに対するアクション（[許可] または [拒否]）を指定し、必要に応じてデフォルト セキュリティ プロファイルをルールに関連付けます。
7. 手順 1～6 を繰り返し、もう 1 つポリシー ルールを作成します。
8. **Commit**（コミット）をクリックします。

STEP 14 | （任意）pxGrid サーバーから動的オブジェクトをいつでも更新できます。更新するには、動的オブジェクトを同期します。動的オブジェクトを同期することで、仮想環境の変更に

©2023 Palo Alto Networks, Inc.

関するコンテキ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ダイナミック 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有効化することができます。

1. **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（モニタリング定義）を選択します。
2. **Synchronize Dynamic Objects**（動的オブジェクトを同期）をクリックします。



©2023 Palo Alto Networks, Inc.

Cisco TrustSec用Panoramaプラグインのトラブルシューティング

- プラグインのステータスコマンド
- コマンドのデバッグ
- ログのデバッグ

プラグインのステータスコマンド

- カウンタのクリア:

```
clear plugins cisco-trustsec counters
```

- モニターステータスの表示:

```
show plugins cisco-trustsec status
```

- カウンタの表示:

```
show plugins cisco-trustsec counters
```

コマンドのデバッグ

- ダイナミックアドレスグループ内のIPアドレスを確認します。

```
show object registered-ip tag <tag>
```

```
show object registered-ip all
```

- サーバーからIPアドレスのタグを取得します。取得したip-tag（IPとタグ）のマッピングは、`plugin_cisco_trustsec.log`に記録されます。IPとタグのマッピングは、サーバーに関連する通知グループにプッシュ配信されることはありません。失敗した場合、再試行は行われません。

```
debug plugins cisco-trustsec query pxgrid-server $server-name ip
 $ip-address
```

- サーバーとの同期、およびマッピングのconfigdプロセスへのプッシュ配信が強制されます。失敗した場合、再試行は行われません。

```
request plugins cisco-trustsec synchronize-dynamic-objects name
 $server-name
```


©2023 Palo Alto Networks, Inc.

- すべてのサーバーとの同期、およびマッピングのconfigdプロセスへのプッシュ配信が強制されます。失敗した場合、再試行は行われません。

```
request plugins cisco-trustsec synchronize-dynamic-objects all
```

- configdプロセスからVM-Seriesファイアウォールへのマッピングの同期が強制されます。失敗した場合、再試行は行われません。

```
request plugins cisco-trustsec sync
```

ログのデバッグ

ログはディスク上の次の場所に存在しています:

```
/opt/plugins/var/log/pan/plugin_cisco_trustsec.log
/opt/plugins/var/log/pan/plugin_cisco_trustsec_sub.log
/opt/plugins/var/log/pan/plugin_cisco_trustsec_ret.log
/opt/plugins/var/log/pan/plugin_cisco_trustsec_proc.log
```

ログファイル（Panoramaデバイスにインストールされているすべてのプラグインが共有）のサイズ制限は、1000万バイトです。ログファイルは、93,000のセッションログインを受け付けます。ログのローテーションを設定した場合、バックアップログは186,000セッションのログインをサポートできます。

- プラグインのデバッグレベルを変更します。

```
request plugins debug level $level plugin-name cisco_trustsec
```

  - **off**（オフ）:ログのデバッグは行われません。
  - **low**（低）:基本デバッグログのみをダンプします。
  - **medium**（中）:詳細デバッグログをダンプします。
  - **high**（高）:サーバーとのリクエスト/レスポンスメッセージを含め、すべてをダンプします。
- 複数のログを単一のログファイルに結合します。

```
request plugins cisco-trustsec merge-logs
```


©2023 Palo Alto Networks, Inc.

- CLIにデバッグログを表示します:
  - Panoramaバージョン10.0.0未満にインストールされたCisco TrustSecプラグインバージョン1.0.2以降:

    ```
    tail mp-log plugin_cisco_trustsec_merged.log
    ```

  - Panoramaバージョン10.0.0以降にインストールされたCisco TrustSecプラグインバージョン1.0.2以降:

    ```
    tail follow yes plugins-log
    ```


©2023 Palo Alto Networks, Inc.

paloalto TECHDOCS

Nutanix AHVでのVM-Seriesファイアウォールのセットアップ

VM-Series firewall for Nutanix AHV により、Nutanix Acropolis Hypervisor を実行可能なデバイス上に、VM-Series ファイアウォールをデプロイすることができます。Nutanix AHV 上で VM-Series ファイアウォールの管理に Panorama を使用している場合、Nutanix 用 Panorama プラグインを使って VM のモニタリングを行うことができます。これにより、Nutanix 環境の変更を動的にファイアウォールに通知して、ネットワークに参加した仮想マシンに確実にポリシーを適用することができます。

> Nutanix AHV での VM-Series ファイアウォールのデプロイ
> Nutanix での VM モニタリング

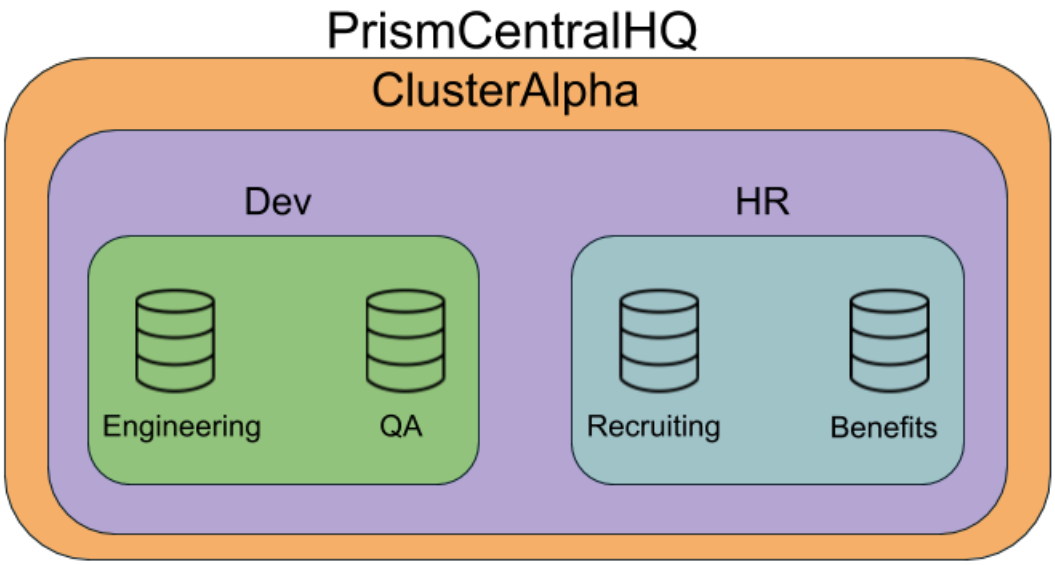
Nutanix での VM モニタリング

Nutanix 環境での変更を監視し、ダイナミック アドレス グループを使ってポリシーを作成するには、Nutanix 用 Panorama プラグインをインストール、設定します。

- Nutanix 上の VM モニタリングについて
- Nutanix 用 Panorama プラグインのインストール
- Nutanix 用 Panorama プラグインの設定

Nutanix 上の VM モニタリングについて

Nutanix 用 Panorama プラグインは、Nutanix 環境内の仮想マシン監視することにより、ダイナミック アドレス グループを簡単に利用できるようにします。Prism Central は、Nutanix 環境内のエンティティを、値で分類、フィルタリングを行い、それをグループ化します。Panorama は、Prism Central で定義されたカテゴリと値に基づいて、タグを作成します。仮想マシンがカテゴリに配置され、値が割り当てられると、Panorama は仮想マシンの IP アドレスに対応するタグを適用します。その後、Panorama 内のダイナミック アドレス グループの一致条件としてタグを使用して、セキュリティ ポリシーを作成することができます。



上記の例では、2 つのカテゴリ Dev および HR が存在しており、それぞれ 2 つの値を保有しています。これらのカテゴリは、Prism Central のクラスタ内に存在しています。Nutanix 環境のモニタリングを開始したら、Panorama は値、カテゴリ、クラスタ、および Prism Centralを使ってタグを生成します。ダイナミック アドレス グループの一致条件を表示する際に、タグは以下のフォーマットで表示されます。

ntnx.PC-<prism-central-name>.CL-<cluster-name>.<category>.<value>

上記の例の情報を使って、Panorama は次のタグを作成します。

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.Engineering`

`ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.QA`

©2023 Palo Alto Networks, Inc.

```
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Recruiting
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Benefits
```

これらのカテゴリ内のワークロードを保護するには、ダイナミック アドレス グループの一致条件として、このようなタグを使用します。その後、ダイナミック アドレス グループを、セキュリティ ポリシー ルール内のソースおよび宛先アドレス グループとして使用することができます。ダイナミック アドレス グループに仮想マシンが参加した場合、作成したポリシーが自動的に適用されます。

Nutanix 用 Panorama プラグインのインストール

Nutanix でのエンドポイント モニタリングを開始するため、Nutanix 用 Panorama プラグインをダウンロードしてインストールします。

Panorama HA 構成がある場合、各 Panorama ピアに対してこのインストール作業を繰り返してください。HA ペアの Panorama にプラグインをインストールする際は、アクティブ ピアより前にパッシブ ピアにプラグインをインストールします。プラグインをパッシブ ピアにインストールすると、パッシブ ピアはノンファンクショナル状態になります。プラグインをアクティブ ピアにインストールすると、パッシブ ピアは再びファンクショナル状態に戻ります。

STEP 1 | Panorama ユーザー インターフェイスにログインします。

STEP 2 | **Panorama** > **Plugins**（プラグイン）を選択します。

STEP 3 | **Check Now**（今すぐチェック）を選択して、利用可能な更新のリストを取得します。

STEP 4 | Action（アクション）列にある **Download**（ダウンロード）をクリックしてインストールを実行します。

STEP 5 | プラグインのバージョンを選択し、Action（アクション）列にある**Install**（インストール）をクリックしてプラグインをインストールします。インストールが完了すると Panorama からメッセージが表示されます。

Nutanix 用 Panorama プラグインの設定

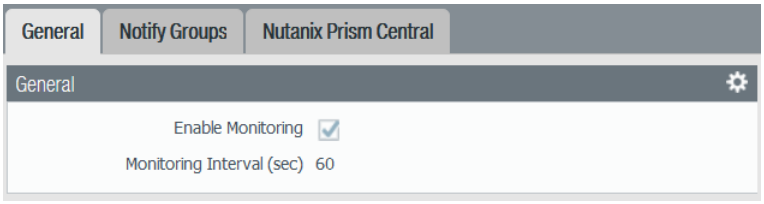
プラグインのインストールが完了したら、以下の手順に従って Panorama と Prism Central 間の接続を確立します。

STEP 1 | Panorama Web インターフェイスにログインします。

©2023 Palo Alto Networks, Inc.

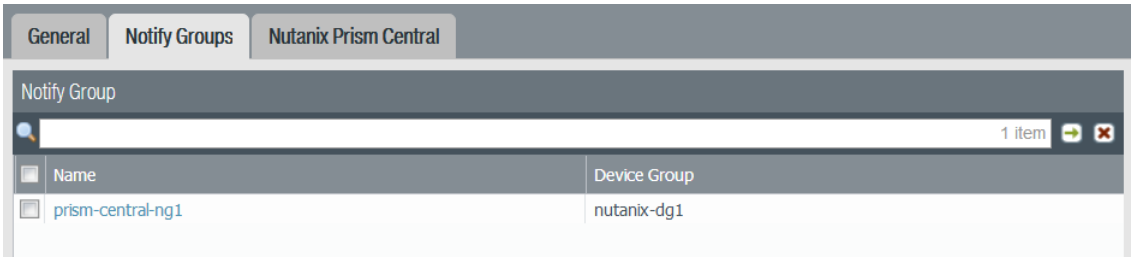
STEP 2 | モニタリングを有効にして、モニタリング間隔を設定します。

1. **Panorama** > **Nutanix** > **Setup**（セットアップ） > **General**（全般）を選択します。
2. **Enable Monitoring**（モニタリングの有効化）を選択します。
3. **Monitoring Interval**（モニタリング間隔）を秒単位で設定します。モニタリング間隔は、Panorama が Prism Central から最新のネットワーク情報を取得する頻度です。



STEP 3 | 通知グループを作成します。

1. **Panorama** > **Nutanix** > **Setup**（セットアップ） > **Notify Groups**（通知グループ）を選択します。
2. **Add**（追加）をクリックします。
3. **Name**（名前）に通知グループの分かりやすい名前を入力します。
4. Nutanix デプロイメントのデバイス グループを選択します。



©2023 Palo Alto Networks, Inc.

STEP 4 | Prism Central の情報を追加します。

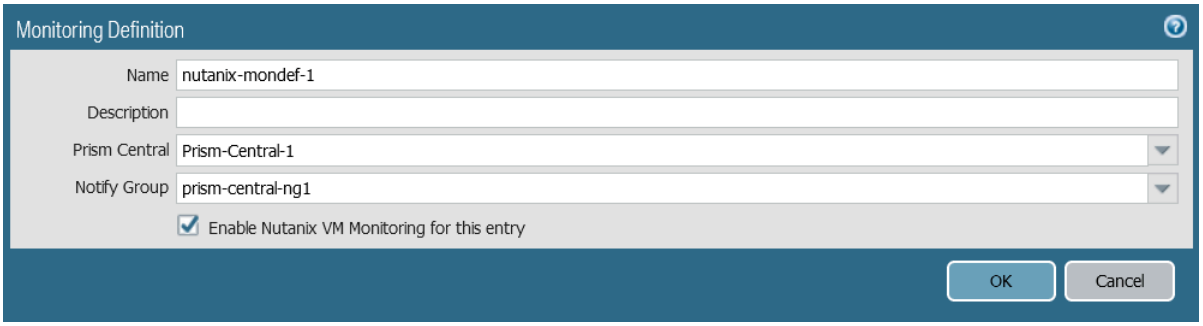
1. **Panorama** > **Nutanix** > **Setup**（セットアップ） > **Nutanix Prism Central** を選択します。
2. **Add**（追加）をクリックします。
3. **Name**（名前）に、分かりやすいPrism Central 名を入力します。
4. Prism Central の IP アドレスまたは FQDN を入力します。
5. Prism Central のユーザー名を入力します。
6. Prism Central のパスワードを入力、確認します。
7. **Validate**（検証）をクリックして、Prism Central 認証情報が正しく入力されていることを確認します。

   OK をクリックした後、*Nutanix Prism Central Info* ウィンドウに戻って、*Validate*（検証）ボタンをクリックすると、認証情報検証エラー メッセージが表示されます。これは予定通りの動作です。パスワード フィールドにはドットが表示されていますが、このフィールドは空です。そのため、*Panorama*が正常に *Prism Central* に接続している場合でも、検証が失敗してしまいます。
8. **OK** をクリックします。



STEP 5 | モニタリング定義を設定します。

1. **Panorama** > **Nutanix** > **Monitoring Definition**（モニタリング定義）を選択し、**Add**（追加）をクリックします。
2. この定義を使用する Prism Central を識別する**Name**（名前）、および任意で説明を入力します。
3. **Prism Central** および **Notify Group**（通知グループ）を選択します。
4. **OK** をクリックします。

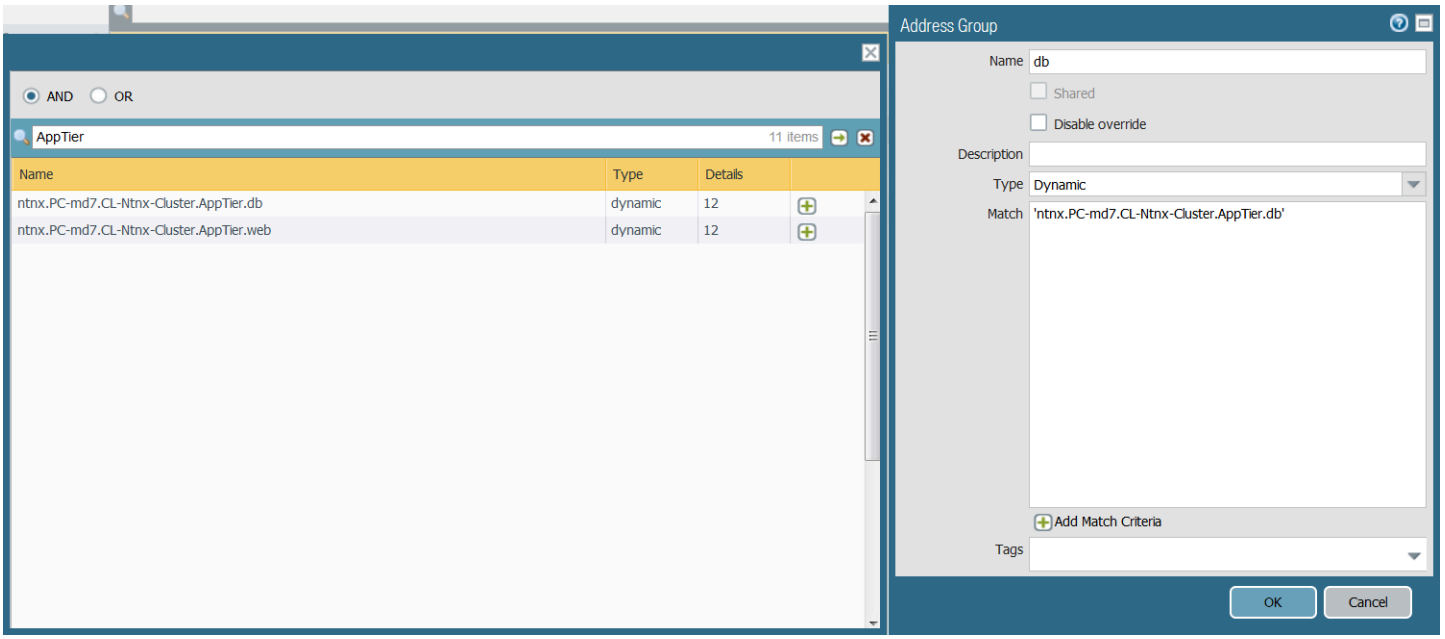


©2023 Palo Alto Networks, Inc.

STEP 6 | 変更を **Commit (コミット)**します。

STEP 7 | Panorama 上で VM 情報を閲覧できることを確認し、ダイナミック アドレス グループ用の一致条件を定義します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択し、**Add**（追加）をクリックします。
2. ダイナミック アドレス グループの、分かりやすい **Name**（名前）を入力します。
3. Type（タイプ）のドロップダウン リストから **Dynamic**（ダイナミック） を選択します。
4. **Add Match Criteria**（一致条件の追加）をクリックします。グループのメンバーを決定する一致条件として、ダイナミック タグを選択できます。**And** または **Or** 演算子を選択し、フィルタリングまたは照合に使用する属性を選択して **OK** をクリックします。
5. 変更を **Commit (コミット)**します。

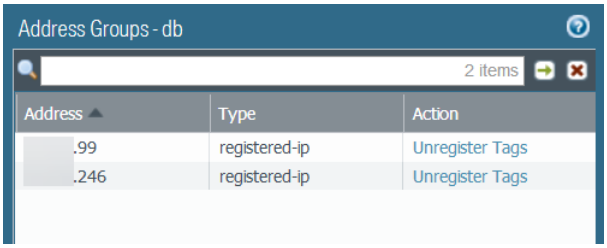


©2023 Palo Alto Networks, Inc.

STEP 8 | VM のアドレスがダイナミック アドレス グループに追加されていることを確認します。

1. **Panorama** > **Objects**（オブジェクト） > **Address Groups**（アドレス グループ）を選択します。
2. ダイナミック アドレス グループの Addresses（アドレス）列で **More**（すべて表示）をクリックします。

   Panorama に、指定した一致条件に基づいてダイナミック アドレス グループに追加された IPアドレスのリストが表示されます。



STEP 9 | ポリシー内でダイナミック アドレス グループを使用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **[追加]** をクリックし、ポリシーの **[名前]** および **[説明]** を入力します。
3. **Source Zone (**送信元ゾーン**)** を追加して、トラフィックの送信元となるゾーンを指定します。
4. トラフィックが終端する **Destination Zone (**宛先ゾーン**)** を追加します。
5. **Destination Address (**宛先アドレス**)** については、先ほど作成したダイナミック アドレス グループを選択します。
6. トラフィックに対するアクション（**[許可]** または **[拒否]**）を指定し、必要に応じてデフォルト セキュリティ プロファイルをルールに関連付けます。
7. ステップ 1～6 を繰り返し、もう 1 つポリシー ルールを作成します。
8. **Commit**（コミット）をクリックします。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのブートストラップ

ブートストラップによりお客様のネットワークに適した構成のパッケージを作成でき、そのパッケージを使用してVM-Series ファイアウォールをどこでもデプロイできるため、ネットワークに新しいVM-Series ファイアウォールを再現可能かつ合理的なプロセスでデプロイすることができます。

スタートアップ時にファイアウォールが完全に設定されているように、完全設定を使ってファイアウォールをブートストラップする、またはファイアウォールをブートするための最低限の初期設定を持つ基本設定を利用して、その後Panoramaに登録して設定を完了することができます。

基本設定を選択し、AWS、Azure、またはGCP上にデプロイする場合、負の゛ーとストラップパッケージと`init-cfg.txt`ファイルを使用することができます。ユーザーデータを使ってブートストラップすることも可能です。ファイルにブートストラップ設定パラメータを指定する代わりに、VM-Seriesファイアウォールの立ち上げ時に、パラメータをキーと値のペアとして、直接AWSまたはGCPユーザーインターフェイスに入力することができます。Azureにも、AzureCLIからアクセスできるテンプレートまたは他のテキストファイルに、ブートストラップパラメータを指定する手続きが用意されています。

ブートストラップパッケージを作成する場合、それを外部デバイス（仮想ディスク、仮想CD-ROM 、またはバケットなどのクラウドストレージデバイス）から配布します。

- ブートストラップ方法の選択
- VM-Series ファイアウォールのブートストラップ ワークフロー
- ブートストラップ パッケージ
- ブートストラップ設定ファイル
- Panorama で VM 認証キーを生成
- init-cfg.txt ファイルの作成
- Bootstrap.xml ファイルの作成
- ブートストラップ用ライセンスの準備
- ブートストラップ パッケージの準備
- AWS 上での VM-Series ファイアウォールのブートストラップ
- Azure 上の VM-Series ファイアウォールのブートストラップ
- ESXi における VM-Series ファイアウォールのブートストラップ
- Google Cloud Platform 上の VM-Series ファイアウォールのブートストラップ
- Hyper-V における VM-Series ファイアウォールのブートストラップ
- KVM 上での VM-Series ファイアウォールのブートストラップ
- ブートストラップの結果を検証
- ブートストラップのエラー

ブートストラップ方法の選択

基本設定または完全設定を使って、VM-Seriesファイアウォールをブートストラップすることができます。

完全設定は、ブートストラップパッケージを使用します。ブート時にファイアウォールを完全に設定するために必要な、すべてが含まれています。これには、設定パラメータ（init-cfg.txt内）、コンテンツのアップデート、およびソフトウェアのバージョンなどが含まれています。完全設定には、init-cfg.txtおよびbootstrap.xmlファイルの両方を含めることができます。

設定方法	設定場所	コメント
ブートストラップパッケージ内の/config/bootstrap.xmlに、完全設定の情報を指定します。	パブリッククラウドストレージ AWS S3バケット、Azureストレージアカウント、またはGoogleストレージバケット。	• ストレージバケット内の完全ブートストラップパッケージ。 • クラウドストレージと、それにアクセスするIAMロールが必要です。

基本設定は、VM-Seriesファイアウォールを起動、ライセンス供与、登録するための、必要最低限の設定です。基本設定は、プラグイン、コンテンツ、ソフトウェアイメージ、またはbootstrap.xmlをサポートしていません。

ファイアウォールのブート後、Panoramaに接続して設定を完了する、またはファイアウォールにログインして手動でコンテンツやソフトウェアを更新することができます。次の表では、基本設定の保管とアクセスに利用できる、3種類の方法を簡単に比較しています。

設定方法	設定場所	コメント
init-cfg.txt 基本設定パラメータを、ブートストラップパッケージ内のconfig/init-cfg.txtに、キーと値のペアとして保管します。	パブリッククラウドストレージ • AWS S3バケット • Azureストレージアカウント • GCPストレージバケット	• クラウドストレージと、それにアクセスするIAMロールが必要です。Panorama管理者には、バケットへのアクセスも許可する必要があります。
ユーザーデータ パブリッククラウドユーザーインターフェイスに、設定パラメータをキーと値のペアとして入力します。	**VM**インスタンス • Alibaba:ユーザーデータ • AWS：ユーザーデータ • Azure：カスタムデータ • GCP:GCPメタデータ	• 初期設定パラメータはVMとともに保管されます。 • ストレージと関連するIAMロールを分離する必要はありません。

©2023 Palo Alto Networks, Inc.

設定方法	設定場所	コメント
	• Oracle Cloud Infrastructure:ユーザーデータ	
AWS Secret Manager AWS Secret Managerに設定パラメータを、キーと値のペアとして入力します。	AWS Secret Manager内で暗号化されます。	• シークレットを作成するには、IAMロールが必要です。その他のユーザーに、シークレットを取得するためのアクセス許可を与えることができます。 • シークレットを取得するには、ユーザーデータを使ってシークレット名を渡します。

基本設定と完全設定のワークフローを比較するには、「VM-Seriesはファイアウォールブートストラップのワークフロー」を参照してください。

- 基本設定
- 完全設定

基本設定

基本設定には、初期設定とライセンスが含まれます。ブートストラップパッケージを使用して、初期設定のキーと値のペアを渡す、またはユーザーデータとしてブートストラップパラメータのキーと値のペアを入力することができます。

Panoramaを使用しない場合、初期設定を利用してファイアウォールのブートストラップを行い、次にログインして手動で設定を完了することができます。Panoramaを使用する場合、初期設定にはPanoramaサーバーのIPアドレスおよびVM Auth Key（VM認証キー）のブートストラップパラメータを含める必要があります。そうすることで、ブートストラップされたファイアウォールをPanoramaに登録し、完全設定を完了することができます。

- 基本設定のブートストラップパッケージへの追加
- 基本設定のユーザーデータとしての入力（パブリッククラウド）
- AWS Secrets Managerでの基本設定の保存

基本設定のブートストラップパッケージへの追加

基本設定は、VM-Seriesファイアウォールを起動、ライセンス供与、登録し、該当する場合はPanoramaと接続するための、必要最低限の設定です。ブートストラップパッケージi内に、設定（init-cfg.txt）を配布します。

基本設定のユーザーデータとしての入力（パブリッククラウド）

パブリッククラウドのユーザーインターフェイスからVM-Seriesファイアウォールをデプロイする場合、立ち上げ/デプロイプロセス中にユーザーデータとして設定パラメータを入力

©2023 Palo Alto Networks, Inc.

することができます。クラウドアカウントからファイアウォールをデプロイするため、およびPanorama（ご利用の場合）にアクセスするために十分なアクセス許可を保有している場合、ブートストラップパッケージの作成、設定ファイルの作成、およびクラウドストレージに関連するその他のブートストラップ作業（ストレージへの外部アクセスを許可するストレージバケット、IAMロール、またはサービスアカウント）をスキップすることができます。

設定パラメータにはInit-cfg.txt ファイルのコンポーネント内の値が含まれています。また、次の値はユーザーデータとしてのみ利用できます。

- **authcodes**—VM-Seriesファイアウォールの登録に使用される認証コード。.例:**authcodes=I7115398**。
- **mgmt-interface-swap**—AWSまたはGCPデプロイ環境で、VM-Seriesファイアウォールがロードバランサーの背後にある場合に、管理インターフェイスのスワップに用いられます。例:**mgmt-interface-swap=enable**。

設定パラメータをキーと値のペアとして、Alibaba、AWS、GCP、またはOCIユーザーインターフェイスに直接入力することができます。テキストファイルから、またはAWS Cloud Formationテンプレート、Azure ARMテンプレート、GCP YAMLファイル、またはTerraformテンプレートなどの、クラウド独自のテンプレートから、設定を定義することも可能です。

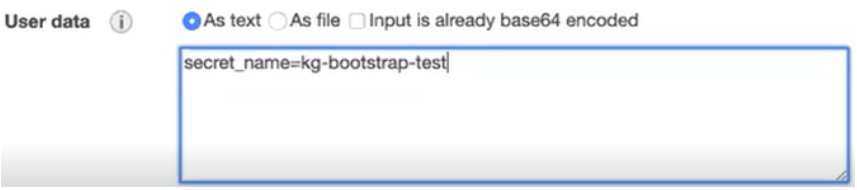
各クラウドのユーザーデータに対する用語を異なっており、またブートストラップパラメータ間の区切り文字も異なっています。

- **Alibaba Cloud**ユーザーデータ —各パラメータを区切るには改行（\n）を使用します。あるパラメータに複数のオプションがある場合は、カンマでそれらを区切ります。
- **AWS** ユーザーデータ – セミコロン、または改行 （\n） を使用します。パラメータに複数のオプションが存在している場合は、カンマでオプションを区切ります。以下に例を示します。

```
type=dhcp-client; op-command-modes=mgmt-interface-swap,jumbo-frame;
plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30
vm-series-auto-registration-pin-id=abcdefgh1234****;
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

```
type=dhcp-client
op-command-modes=mgmt-interface-swap,jumbo-frame
vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

基本設定をAWS Secrets Managerに保存することを選択した場合、ユーザーデータフィールドにシークレット名をキーと値のペアとして入力します。以下に例を示します。



 ©2023 Palo Alto Networks, Inc.

- **Azure** カスタムデータ – セミコロンを使用します。パラメータに複数のオプションが存在している場合は、カンマでオプションを区切ります。以下に例を示します。

```
type=dhcp-client; op-command-modes=jumbo-frame;
plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30
vm-series-auto-registration-pin-id=abcdefgh1234****;
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

- **GCP**カスタムメタデータ– YAMLファイルやTerraformテンプレートなどのファイル内で、各パラメータに対して改行（\n）を使用します。パラメータに複数のオプションがある場合は、カンマでそれらを区切ります。以下に例を示します。

```
type=dhcp-client
op-command-modes=mgmt-interface-swap,jumbo-frame
plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30
vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

- **Oracle Cloud Infrastructure**ユーザーデータ –各パラメータを区切るには改行（\n）を使用します。あるパラメータに複数のオプションがある場合は、カンマでそれらを区切ります。

AWS Secrets Managerでの基本設定の保存

AWS Secrets Managerを使って基本設定をシークレットとして保存し、次にユーザーデータを使ってVMを、シークレット内に保管されているパラメータでブートストラップすることができます。この作業を行うには、Secrets Managerを使用するためのアクセス許可が必要です。

- シークレットの作成者は、完全なSecrets Manager管理者アクセス許可を保有している必要があります。Secrets Manager管理者は、「AWS Secrets Managerの認証とアクセス制御」で説明しているように、他のユーザーにシークレットの使用を許可することができます。

  たとえば、次のポリシーステートメントを利用して、シークレット値を入手することができます:

```
{
  "Version": "2012-10-17",
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource":
      "arn:aws:secretsmanager:us-east-1:688382******:secret:My_bts-
******"
    }
}
```

  シークレットのlist、get、およびrotateなどの、アクセス許可が必要なアクションについては、「AWS Secrets ManagerのIAMポリシーまたはシークレットポリシーで使用できるアクション、リソース、およびコンテキストキー」を参照してください。

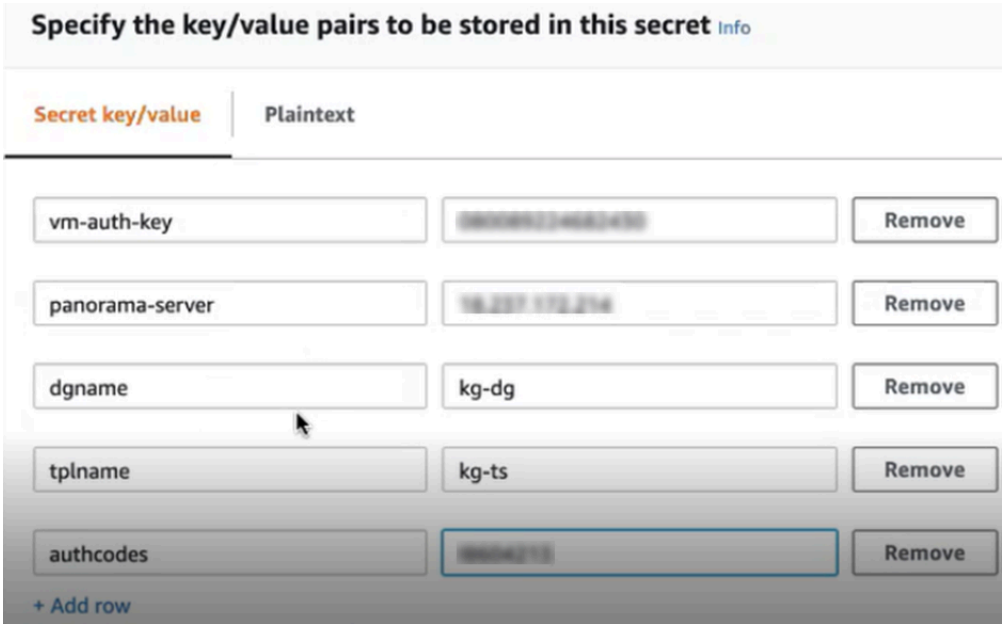
- （任意）シークレットを暗号化するために、AWS Secrets ManagerからDefaultEncryptionKeyを使用することができます。

©2023 Palo Alto Networks, Inc.

STEP 1 | AWSコンソールにログインして、Security, Identity and Compliance（セキュリティ、アイデンティティ、およびコンプライアンス）から、**Secrets Manager**を選択して、次に**Store a new secret**（新しいシークレットの保存）を選択します。

STEP 2 | **other type of secrets**（その他のタイプのシークレット）を選択します。

1. 基本設定を定義するために、キーと値のペアを入力します。



> *AWS*シークレット内で、***mgmt-interface-swap***はキーと値のペアとして機能しません。***op-command-modes=mgmt-interface-swap***と入力する必要があります。

2. DefaultEncryptionKeyを選択して、**Next**（次へ）をクリックします。

STEP 3 | シークレット名と説明を指定します。

1. AWSアカウントが安全にシークレットにアクセスできるように、リソースアクセス許可を編集します。以下に例を示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::sn-bootstrap"
    },
    {
        "Sid": "VisualEditor1",
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::sn-bootstrap/*"
    },
    {
```


©2023 Palo Alto Networks, Inc.

```
        "Effect": "Allow",
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager:us-
east-1:688382******:
                            secret:My_bootstrap"
    }
  ]
}
```

2. （任意）コマンドラインからシークレットを調査することができます（アクセス許可がある場合）。以下に例を示します。

```
# aws secretsmanager get-secret-value --secret-id My_bootstrap
{
    "ARN": "arn:aws:secretsmanager:us-east-1:688382******:
                secret:My_bootstrap",
    "Name": "My_bootstrap",
    "VersionId": "01b6853d-e187-479f-***********",
    "SecretString": "{\"mgmt-interface-swap\":\"enable\",
        \"vm-auth-key\":\"AAA\",\"panorama-server\":
\"10.*.*.1\",
        \"panorama-server-2\":\"10.*.*.2\",\"dgname\":\"dg-
s0000h\",
        \"tplname\":\"tpl-santosh\",\"license-authcode\":
\"AAAA\"}",
    "VersionStages": [ "AWSCURRENT" ],
    "CreatedDate": 1581018411.847
}
```

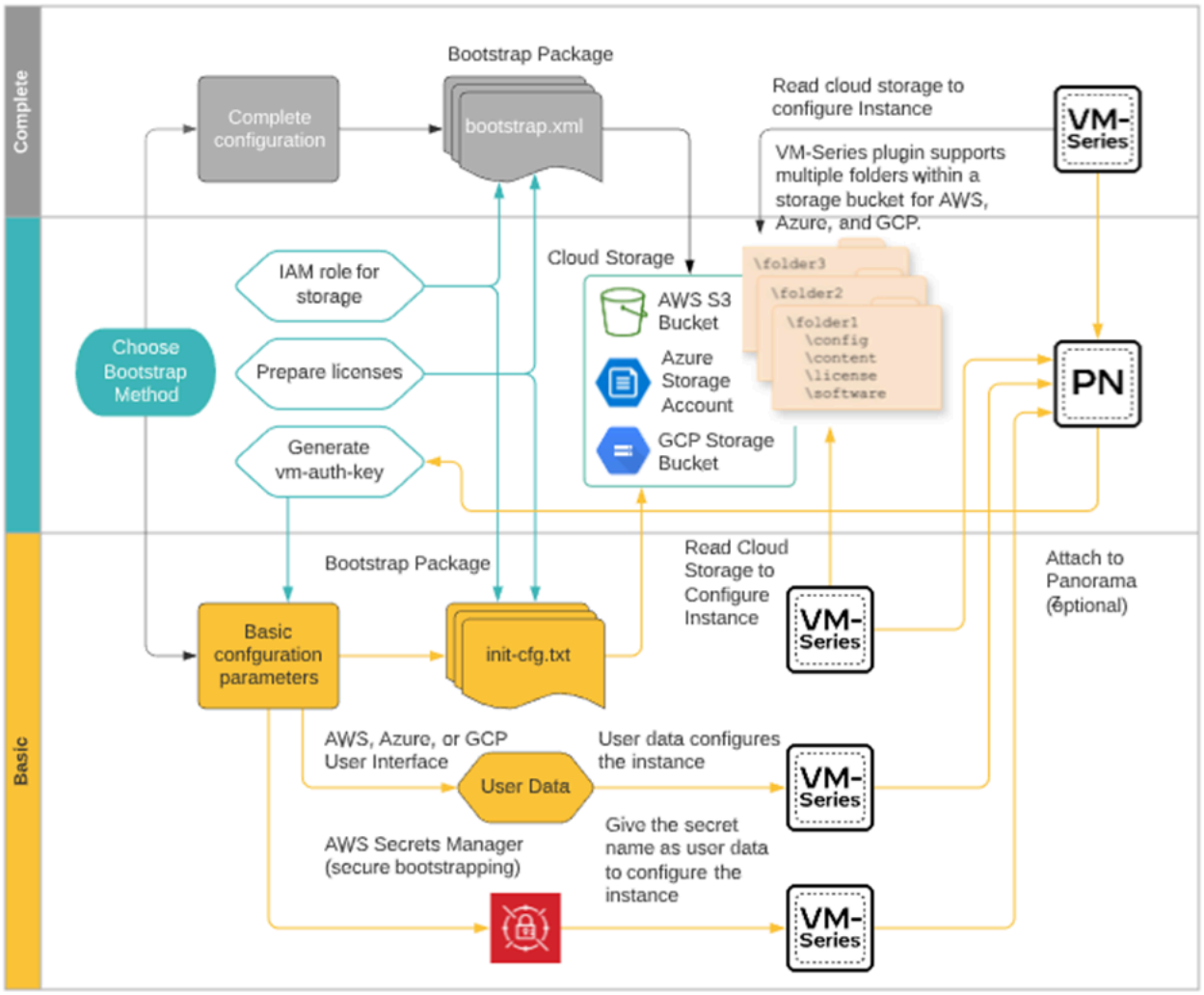
完全設定

完全設定を利用すると、ブートアップ時にファイアウォールが完全に設定されます。bootstrap.xmlファイルには、VM-Seriesプラグインの初期設定、ライセンス、ソフトウェア、コンテンツ、およびバージョンが含まれています。**bootstrap.xml**を手動で作成する、または「bootstrap.xmlファイルの作成」の説明に従って既存の設定をエクスポートすることができます。

©2023 Palo Alto Networks, Inc.

VM-Series ファイアウォールのブートストラップ ワークフロー

VM-Seriesファイアウォールをブートストラップするには、次の作業を行ってください。完全ブートストラップおよび基本ブートストラップの手順の概要については、次の図を参照してください。



STEP 1 | （任意）セキュリティ上の理由から、ファイアウォールが工場出荷時のデフォルト設定になっている場合にのみブートストラップを行えます。ブートストラップパッケージを使用して、以前に設定済みのVM-Series ファイアウォールをブートストラップする場合は、ファイアウォールを出荷時のデフォルト設定にリセットしてください。

©2023 Palo Alto Networks, Inc.

STEP 2 | ブートストラップ方法を選択します。

ブートストラップパッケージについて理解したら、完全設定を使用するか、または基本設定を使用するか、そして必要に応じてブートストラップしたファイアウォールをPanoramaで管理するかどうかを評価、判断します。

基本設定を使用する場合は、ブートストラップパッケージを使用するか、またはユーザーデータ内に設定パラメータをキーと値のペアとして入力するかを判断します。

STEP 3 | （任意）ブートストラップ中の VM-Series ファイアウォールを管理する Panorama を使用する場合は、PanoramaでVM認証キーを生成します。このキーは、**`init-cfg.txt`**ファイルに指定するか（**`vm-auth-key`**）、またはユーザーデータとしてキーと値のペアを入力する必要があります。

STEP 4 | ブートストラップ用にライセンスを準備します。

STEP 5 | 基本設定を選択し、ユーザーデータを使ってブートストラップを行う場合は、ステップ7に進みます。

基本設定とブートストラップパッケージを使用する場合は、init-cfg.txtファイルを作成して、ブートストラップパッケージの準備を行います。

完全設定を使用する場合は、bootstrap.xmlファイルを作成して、完全ブートストラップパッケージの準備を行います。

STEP 6 | ブートストラップパッケージを準備して、ご利用のハイパーバイザーに適した配布フォーマットでブートストラップパッケージを保存します。

STEP 7 | VM-Seriesファイアウォールのブートストラップを行います。

- AWS 上での VM-Series ファイアウォールのブートストラップ
- Azure 上の VM-Series ファイアウォールのブートストラップ
- ESXi における VM-Series ファイアウォールのブートストラップ
- Google Cloud Platform 上の VM-Series ファイアウォールのブートストラップ
- Hyper-V における VM-Series ファイアウォールのブートストラップ
- KVM 上での VM-Series ファイアウォールのブートストラップ

STEP 8 | ブートストラップの完了を検証します。

©2023 Palo Alto Networks, Inc.

ブートストラップ パッケージ

ブートストラップ プロセスは、ファイアウォールが工場出荷時のデフォルト状態になっている際に初回のブート時のみ実行されます。

- ブートストラップ パッケージの構造
- ブートストラップパッケージの配信

ブートストラップ パッケージの構造

ブートストラップ パッケージには、`/config`、`/license`、`/software`、`/content` の 4 つのフォルダ（空である場合でも）が含まれていなければなりません。`/plugins`フォルダは任意です。例については、「ブートストラップ パッケージの準備」を参照してください。

- **/Config** フォルダ–構成ファイルを含みます。このフォルダには2つのファイル（`init-cfg.txt`および`bootstrap.xml`）を含められます。詳細には、「ブートストラップ設定ファイル」を参照してください。

  ブートストラップで*VM-Series*ファイアウォールを*Panorama*に事前登録したい場合、*Panorama*で*VM*認証キーを生成し、生成されたキーを`init-cfg.txt`ファイルに含める必要があります。「Panorama で VM 認証キーを作成する」を参照してください。

- **/license**フォルダ–そのファイアウォールで有効化したいライセンスおよびサブスクリプション用のライセンス キーあるいは認証コードを含みます。ファイアウォールがインターネットに接続されていない場合、Palo Alto Networksサポートポータルから手動でライセンス キーを取得するか、ライセンスAPIを使用してキーを取得後、各キーをこのフォルダに保存する必要があります。詳細は「ブートストラップ用ライセンスの準備」」を参照してください。

  個々の認証コードの代わりに認証コード バンドルを含めることで、ファイアウォールに紐付けられたすべてのライセンス キーをファイアウォールあるいはオーケストレーション サービスが同時に取得できるようにする必要があります。バンドルではなく個々の認証コードを使用する場合、ファイアウォールはファイルに含まれた最初の認証コード用のライセンス キーのみを取得します。

- **/software**フォルダ–新規に準備したVM-Seriesファイアウォールをネットワークに適したPAN-OSバージョンにアップグレードするために必要なソフトウェアイメージを含みます。現在のバージョンから、VM-Seriesファイアウォールをアップグレードさせたい最後のPAN-OSソフトウェアバージョンに至るまでの間に存在するソフトウェアバージョンをすべて含める必要があります。互換性マトリックスの「VM-Seriesファイアウォールハイパーバイザーサポート」を参照してください。
- **/content**フォルダ–VM-Seriesファイアウォール上の有効なサブスクリプションのためのアプリケーション、脅威アップデート、WildFireアップデート、BrightCloud URLフィルタリングデータベースが含まれます。目的のPAN-OSバージョンに必要な最低限のコンテンツバージョンを含める必要があります。PAN-OSのバージョンに関連して、必要最低限のコンテンツバージョンがない場合、VM-Series ファイアウォールはソフトウェアのアップグレードを完了できません。

©2023 Palo Alto Networks, Inc.

- **/plugins folder**— 1 つの VM-Series プラグイン イメージが含まれているオプションのフォルダです。

ブートストラップパッケージの配信

ブートストラップパッケージを VM-Series ファイアウォールに送る際に使用するファイルの種類はハイパーバイザーに応じて異なります。次の表を使用して、ハイパーバイザーまたはクラウドベンダーがサポートするファイルの種類を決定してください。

ブートストラップ用の外部デバイス（ブートストラップパッケージ形式）	AWS	Azure	ESXi	Google	Hyper-V	KVM
CD-ROM（ISOイメージ）	—	—	はい	—	はい	はい
ブロック ストレージ デバイス	—	—	はい	—	はい	はい
ストレージアカウント	—	はい	—	—	—	—
ストレージ バケット	はい	—	—	はい	—	—

ストレージデバイスをファイアウォールにアタッチする際、ファイアウォールはブートストラップ パッケージを検索し、見つかった場合、ファイアウォールはそのブートストラップ パッケージで定義されている設定を使用します。

ファイルにPanoramaサーバーのIPアドレスを含めた場合、ファイアウォールは Panorama に接続します。ファイアウォールがインターネットに接続されている場合、ファイアウォールはライセンスサーバーにアクセスしてUUIDを更新し、ライセンス キーおよびサブスクリプションを取得します。次にファイアウォールはアセットとしてPalo Alto Networksサポートポータルに追加されます。ファイアウォールがインターネットに接続されていない場合、ファイアウォールはブートストラップ パッケージに含めたライセンス キーを使用するか、Panoramaに接続して適切なライセンスを取得し、それを管理対象のファイアウォールにデプロイします。

©2023 Palo Alto Networks, Inc.

ブートストラップ設定ファイル

ブートストラップパッケージの**config/init-cfg.txt**には、基本設定を含める必要があります。完全な設定（**/config/bootstrap.xml**ファイル）は任意です。

ブートストラップパッケージに**init-cfg.txt**ファイルと**bootstrap.xml**ファイルを含めた場合、ファイアウォールがそれらのファイルの設定を結合します。設定の重複が存在している場合は、**init-cfg.txt**ファイルに定義されている値が使用されます。

- init-cfg.txt
- bootstrap.xml

init-cfg.txt

IP アドレスの種類（スタティックあるいは DHCP）、IP アドレス（IPv4 のみ、あるいは IPv4 と IPv6 の両方）、ネットマスク、デフォルトゲートウェイなど、ファイアウォールの管理インターフェイスを構成するために必要な基本情報が含まれています。DNSサーバーのIPアドレス、PanoramaのIPアドレス、およびデバイスグループとテンプレートのスタック パラメータは任意です。

汎用の名称と**init-cfg.txt**を使用する、または特定しやすくするために、各ファイアウォールの UUID あるいはシリアル番号をファイル名の頭に付けて具体的な名前を付けることができます（例：**0008C100105-init-cfg.txt**）。

ファイアウォールはブートを行う間、UUIDあるいはシリアル番号が一致するテキストファイルを検索し、それが見つからなかった場合は汎用のファイル名**init-cfg.txt**で検索を行います。サンプル ファイルについては「init-cfg.txt ファイルの作成」を参照してください。

Panorama を使用してブートストラップされた *VM-Series* ファイアウォールを管理する場合は、次の通りに行います：

- *Panorama*で*VM*認証キーを生成し、そのキーを***init-cfg.txt***ファイルに組み込む必要があります。詳細については、「Panorama で VM 認証キーを生成」を参照してください。
- ファイアウォールを管理する *Panorama* アプライアンスは、*Panorama* モードでなければなりません。*Panorama*アプライアンスを管理専用モードで使用すると、管理専用モードの*Panorama*にはファイアウォールログを保存できるログコレクター グループがないため、ファイアウォールログは削除されます。

bootstrap.xml

オプションの**bootstrap.xml**ファイルには、ファイアウォール向けの完全な設定が含まれています。Panoramaを使用してファイアウォールを一元的に管理していない場合は、起動時に設定

©2023 Palo Alto Networks, Inc.

されたファイアウォールをデプロイするプロセスを自動化する手段が**bootstrap.xml**ファイルによって提供されます。

設定は手動で定義することも、既存のファイアウォールから現在アクティブな設定（**running-config.xml**）をエクスポートしてそのファイルを**bootstrap.xml**として保存することもできます。**bootstrap.xml**ファイルをエクスポートする場合、必ずご自分のデプロイ環境と同じプラットフォームあるいはハイパーバイザーにデプロイされているファイアウォールからXMLファイルをエクスポートするようにしてください。「bootstrap.xml ファイルの作成」を参照してください。

 ©2023 Palo Alto Networks, Inc.

Panorama で VM 認証キーを生成

Panoramaを使用してブートストラップ中のVM-Series ファイアウォールをマージしたい場合、Panorama で VM 認証キーを生成し、そのキーを基本設定（init-cfg.txt）ファイルに含める必要があります。VM認証キーにより、Panoramaが新しくブートストラップされたVM-Series ファイアウォールを認証することができるようになります。そのため、Panorama を使用してファイアウォールを管理するには、Panorama 用の IP アドレスと VM 認証キーを基本設定ファイルに含め、ライセンス認証コードをブートストラップ パッケージの /license フォルダに含める必要があります。こうすることで、初回の Panorama への接続リクエストの際にファイアウォールが IP アドレス、シリアル番号、および VM 認証キーを提供できるようになり、Panorama が VM 認証キーの有効性を検証して、ファイアウォールを管理対象のデバイスとして追加できるようになります。基本設定ファイルでデバイスグループおよびテンプレートを提供する場合、Panoramaはファイアウォールを適切なデバイスグループおよびテンプレートに割り当てるため、Panoramaを使用して中央からファイアウォールを構成・管理することができるようになります。

キーの有効期限は1時間から8760時間（1年）の間のいずれかです。指定した期間が過ぎるとキーが失効し、Panoramaはこの接続リクエストの際に有効な認証キーが無いためにVM-Seriesファイアウォールを登録しなくなります。

STEP 1 | Panorama CLIにログインするか、APIにアクセスします。

- CLI で次の操作コマンドを実行します。

  ```
  request bootstrap vm-auth-key generate lifetime <1-8760>
  ```

  次は、24 時間有効なキーを生成する例です。

  ```
  request bootstrap vm-auth-key generate lifetime 24
  VM auth key 755036225328715 generated. Expires at: 2015/12/29
   12:03:52
  ```

- API で次の操作コマンドを実行します。

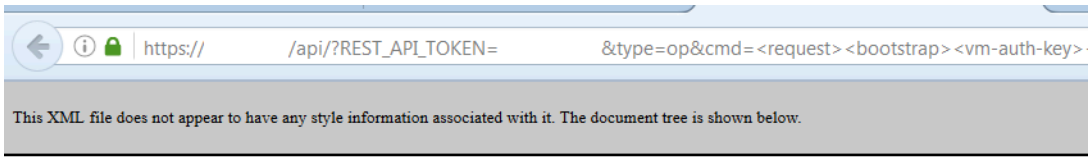
  ```
  https://<Panorama_IP_address>/api/?
  type=op&cmd=<request><bootstrap><vm-auth-
  key><generate><lifetime><number-of-hours></lifetime></generate></
  vm-auth-key></bootstrap></request>
  ```

  この有効期限は VM 認証キーが有効な時間数です。

©2023 Palo Alto Networks, Inc.

STEP 2 | Panorama で作成した VM 認証キーの有効期間を確認します。ファイアウォールが Panorama に登録するのに十分な有効期間になっていることを確認します。

```
https://<Panorama_IP_address>/api/?
type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-
auth-key></bootstrap></request>
```



This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
- <response status="success">
  - <result>
    - <bootstrap-vm-auth-keys>
      - <entry>
          <vm-auth-key>085812955845977</vm-auth-key>
          <expiry-time>2016/03/17 08:35:05</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>136387033275034</vm-auth-key>
          <expiry-time>2016/05/20 14:12:59</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>178644792323541</vm-auth-key>
          <expiry-time>2016/06/10 16:25:36</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>221348425464173</vm-auth-key>
          <expiry-time>2016/05/20 13:54:25</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>245832696687351</vm-auth-key>
          <expiry-time>2015/12/22 17:53:48</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>386239691539160</vm-auth-key>
          <expiry-time>2016/03/02 11:09:46</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>420246530153909</vm-auth-key>
          <expiry-time>2016/03/09 00:57:01</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>431216710324086</vm-auth-key>
          <expiry-time>2016/03/09 00:57:09</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>445486056501180</vm-auth-key>
          <expiry-time>2016/05/20 14:12:52</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>633795692572911</vm-auth-key>
          <expiry-time>2016/03/09 14:50:38</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>798346857952985</vm-auth-key>
          <expiry-time>2016/05/20 14:08:14</expiry-time>
        </entry>
      </bootstrap-vm-auth-keys>
    </result>
  </response>
```


STEP 3 | 生成された VM 認証キーを基本設定（init-cfg.txt）ファイルに追加します。「init-cfg.txt ファイルの作成」を参照してください。

©2023 Palo Alto Networks, Inc.

init-cfg.txt ファイルの作成

init-cfg.txtファイルは、VM-Seriesファイアウォールのブートストラップを実行するために必要です。このファイルには、ファイアウォールがネットワークに接続する際に必要な基本情報が記述されています。

- Init-cfg.txt ファイルのコンポーネント
- Init-cfg.txt のサンプル ファイル

init-cfg.txtファイルを作成するには、以下の手順を実行します。

STEP 1 | 新しいテキストファイルを作成します。

メモ帳、EditPad、あるいはその他のテキストエディタを使用してプレーンテキストのファイルを作成します。

STEP 2 | ファイアウォールの管理インターフェイスのための基本ネットワーク設定を追加します。

このファイルで必要なパラメータが一つでも欠けている場合、ファイアウォールはブートストラップ プロセスを中止し、デフォルトの*IP*アドレス*192.168.1.1*を使用して起動します。ファイアウォールのシステムログを表示すればブートストラップのエラーが発生した理由を確認できます。エラーについては、「ライセンス API」を参照してください。

各フィールドのキーと値の間にはスペースを入れません。*mgmtsrvr*側でパースを行う際にエラーが生じるおそれがあるため、スペースを含めないでください。

- 静的IPアドレスを使用して管理インターフェイスを構成するには、IPアドレス、アドレスの種類、デフォルトゲートウェイ、ネットマスクを指定する必要があります。IPv4 アドレスは必須で、IPv6 アドレスは任意です。構文については、「サンプル ファイル init-cfg.txt」を参照してください。
- 管理インターフェイスをDHCPクライアントとして構成するには、アドレスの種類のみを指定する必要があります。管理インターフェイスでDHCPクライアントを有効化する場合、ファイアウォールはファイルで定義されているIPアドレス、デフォルトゲートウェイ、ネットマスク、IPv6アドレス、IPv6デフォルトゲートウェイの値を無視します。構文については、「サンプル ファイル init-cfg.txt」を参照してください。

管理インターフェイスでDHCPクライアントを有効化する場合、ファイアウォールはDHCPが割り当てられたIPアドレスを選び、ネットワーク中からファイアウォールにアクセスできるようになります。DHCPが割り当てられたIPアドレスはDashboard [ダッシュボード]のGeneral Information [一般情報]ウィジェット上で、あるいはCLIコマンド**show system info**を実行して表示することができます。しかし、デフォルトの静的管理IPアドレス192.168.1.1はファイアウォール上の現在アクティブな設定（**show config running**）に保持されます。この静的IPアドレスにより、ファイアウォールへのDHCPアクセスが遮断された場合でも、常にファイアウォールへの接続を回復できるようになります。

©2023 Palo Alto Networks, Inc.

STEP 3 | VM 認証キーを追加して VM-Series ファイアウォールを Panorama に登録します。

VM-Seriesファイアウォールを Panorama に追加するには、Panorama で生成した VM 認証キーを基本設定（**init-cfg.txt**）ファイルに追加する必要があります。キーの生成の詳細は、「Panorama で VM 認証キーを生成」を参照してください。

STEP 4 | Panoramaにアクセスするための詳細情報を追加します。

- プライマリおよびセカンダリPanoramaサーバー用のIPアドレスを追加します。
- ファイアウォールを割り当てたいテンプレートおよびデバイスグループを指定します。

STEP 5 | （推奨）デバイス証明書インストール用のVM-Series登録PINと値を追加します。

起動時にVM-Seriesファイアウォールにデバイス証明書をインストールしたい場合は、CSP上でVM-Series登録PIN IDと値を生成して、**init-cfg.txt**ファイルに含める必要があります。このPINと値は、PAYGライセンスを使用する任意のサイトライセンスにも適用されます。

STEP 6 | （任意）ファイアウォール用の追加パラメータを含めます。

- プライマリおよびセカンダリDNSサーバー用のIPアドレスを追加します。
- ファイアウォールのホスト名を追加します。
- ジャンボフレームまたは複数仮想システム（あるいは両方）を有効化します。
- AWSまたはGCP上のVM-Seriesファイアウォールで、管理インターフェイスのスワップ（mgmt）およびデータプレーンインターフェイス（ethernet 1/1）を有効化します。管理インターフェイスの変更の詳細は、「Amazon ELB で使用する管理インターフェイスのマッピング」または「Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ」を参照してください。
- DPDK を有効または無効にします。

Init-cfg.txt ファイルのコンポーネント

init-cfg.txtファイルのブートストラップパラメータを以下の表に示します。

項目	の意味
type=	管理IPアドレスのタイプ（staticあるいはdhcp-client）。このフィールドは必須です。
ip-address=	IPv4 アドレス。タイプが dhcp-client の場合、このフィールドは無視されます。タイプが static の場合、IPv4 アドレスが必要です。ipv6-address フィールドは任意で含めることができます。 AWSおよびAzureにおけるVM-Seriesファイアウォールでは、管理IPアドレスおよびネットマスク構成を指定することはできません。定義した場合、ファイアウォールは指定された値を無視します。

©2023 Palo Alto Networks, Inc.

項目	の意味
default-gateway=	管理インターフェイスのIPv4デフォルトゲートウェイ。タイプが dhcp-client の場合、このフィールドは無視されます。タイプがstaticであり、かつip-addressが使用されている場合、このフィールドは必須になります。
netmask=	IPv4ネットマスク。タイプが dhcp-client の場合、このフィールドは無視されます。タイプがstaticであり、かつip-addressが使用されている場合、このフィールドは必須になります。
ipv6-address=	任意）管理インターフェイスのIPv6 アドレスおよび/プレフィックス。タイプが dhcp-client の場合、このフィールドは無視されます。タイプが static の場合、必須の ip-address フィールドと一緒にこのフィールドを指定することができます。
ipv6-default-gateway=	管理インターフェイスのIPv6デフォルトゲートウェイ。タイプが dhcp-client の場合、このフィールドは無視されます。タイプがstaticであり、かつipv6-addressが使用されている場合、このフィールドは必須になります。
hostname=	ファイアウォールのホスト名。
panorama-server=	Panoramaプライマリサーバーの IPv4あるいはIPv6アドレス。必須フィールドではありませんが、Panorama を使用してファイアウォールの一元管理を行う場合に設定します。
panorama-server-2=	Panoramaセカンダリサーバーの IPv4あるいはIPv6アドレス。必須フィールドではありませんが、推奨されます。
tplname=	Panoramaテンプレート スタック名。Panorama サーバーの IP アドレスを追加する場合は、ベスト プラクティスとして、Panorama のテンプレート スタックにファイアウォールを割り当て、このフィールドにテンプレート スタック名を入力して、構成設定を一元的に管理してファイアウォールにプッシュできるようにすることをお勧めします。
dgname=	Panoramaデバイス グループ名。Panorama サーバーの IP アドレスを追加する場合は、ベスト プラクティスとして、Panorama 上でデバイス グループを作成してから、このフィールドにデバイス グループ名を入力することで、ファイアウォールを論理的にグループ化して、ポリシー ルールをファイアウォールにプッシュすることができます。
cgname =	Panoramaコレクターグループの名前。ファイアウォールをブートストラップしてログを Panorama コレクタグループに送信する場合は、最初に Panorama でコレクタグループを構成してから、ログを

©2023 Palo Alto Networks, Inc.

項目	の意味
	Panorama に転送するようにファイアウォールを構成する必要があります。 M-Series アプライアンスではデフォルトのコレクタグループが事前定義済みであり、すでにローカルログコレクタがメンバーとして組み入れられています。Panorama バーチャル アプライアンスでは、コレクタ グループを追加してローカル ログ コレクタをメンバーとして追加する必要があります。
dns-primary=	DNSプライマリサーバーのIPv4あるいはIPv6アドレス。
dns-secondary=	DNSセカンダリサーバーのIPv4あるいはIPv6アドレス。
vm-auth-key=	Panorama用の仮想マシンの認証キー（Panorama で VM 認証キーを生成」を参照）。ハードウェア ファイアウォールのブートストラップの場合、このフィールドは無視されます。
op-command-modes=	次の値は許可されます: multi-vsys、jumbo-frame、mgmt-interface-swap複数の値を入力する場合は、各項目をスペースあるいはコンマで区切ります。 • **multi-vsys**–ハードウェア ベースのファイアウォールのみ）複数仮想システムを有効化。 • ジ**jumbo-frame**–すべてのレイヤー 3 インターフェイスのデフォルトの MTU サイズを 9192 バイトに設定します。 • **mgmt-interface-swap** – AWS、Google、ESXi、KVM 上の VM-Series ファイアウォールのみ）ファイアウォールのデプロイ時に管理インターフェース（MGT）とデータプレーンインターフェース（ethernet 1/1）を入れ替えられるようにします。詳細は、次を参照してください。 • Amazon ELB で使用する管理インターフェイスのマッピング • Google Cloud Platform の負荷分散のための管理インターフェイスのスワップ • ESXi 上での VM-Series CLI を使用した管理インターフェースのスワップ • KVM 上での VM-Series CLI を使用した管理インターフェースのスワップ
op-cmd-dpdk-pkt-io=	値**on**または**off**を指定することでファイアウォールがデータ プレーン開発キット（DPDK）をサポートする環境で DPDK を有効化または無効化できます。DPDK は、Linux カーネルをバイパスすることで、ホストがパケットをより高速に処理できるようにします。NIC とのやり取りはドライバと DPDK ライブラリを使用して実行されます。

©2023 Palo Alto Networks, Inc.

項目	の意味
plugin-op-commands=	VM-Seriesプラグイン操作コマンドを指定します。 複数のコマンドは、単一行にカンマ区切り形式で、スペースを入れないで入力する必要があります。 • **sriov-access-mode-on** – このコマンドはESXi およびKVM ハイパーバイザー上の VM-Series ファイアウォールに対してのみ有効になります。 KVM の場合のみ**sriov-access-mode-on**を有効にする場合**op-command-modes=jumbo-frame**は有効にしないでください。 • **aws-gwlb-inspect:enable** –VM-SeriesとAWS Gateway Load Balancerの統合を有効にします。 • **aws-gwlb-associate-vpce:<VPCE-ID@ethernet<**サブインターフェース – ファイアウォール上VPCエンドポイントとVM-Seriesインターフェイスの関連付けまたはサブインターフェースを関連付けることができます。指定したインターフェイスは、セキュリティゾーンに割り当てられます。 • **aws-gwlb-overlay-routing:enable** – AWS GWLB と統合する場合、このコマンドを使用しAWS での VM-Series のオーバーレイルーティングの有効化を行います。 • **set-dp-cores:<#-cores** – ソフトウェア NGFW ライセンスでデプロイされた PAN-OS 10.1 以降を実行しているVM-Series ファイアウォールのデータプレーン vCPU の数をカスタマイズします。このオプションは NSX-T ではサポートされていません。詳細は、データプレーンコアのカスタマイズ」を参照してください。 • **numa-perf-optimize:enable** - VM-Series プラグイン 2.1.2 以降がインストールされている VM-Series ファイアウォールで NUMA パフォーマンスの最適化を有効にします。詳細は、VM-Series での NUMA パフォーマンス最適化の有効化」を参照してください。
dhcp-send-hostname=	yesあるいはnoの値がDHCPサーバーから返されます。yesの場合、ファイアウォールは自身のホスト名をDHCPサーバーに送信します。タイプがdhcp-clientの場合にのみ評価されるフィールドです。
dhcp-send-client-id=	yesあるいはnoの値がDHCPサーバーから返されます。yesの場合、ファイアウォールは自身のクライアントIDをDHCPサーバーに送信します。タイプがdhcp-clientの場合にのみ評価されるフィールドです。

©2023 Palo Alto Networks, Inc.

項目	の意味
dhcp-accept-server-hostname=	yesあるいはnoの値がDHCPサーバーから返されます。yesの場合、ファイアウォールはDHCPサーバーから送信される自身のホスト名を承認します。タイプがdhcp-clientの場合にのみ評価されるフィールドです。
dhcp-accept-server-domain=	yesあるいはnoの値がDHCPサーバーから返されます。yesの場合、ファイアウォールはDHCPサーバーから送信される自身のDNSサーバーを承認します。タイプがdhcp-clientの場合にのみ評価されるフィールドです。
vm-series-auto-registration-pin-id AND vm-series-auto-registration-pin-value	VM-Seriesファイアウォールへのデバイス証明書インストール用のVM-Series登録PIN IDと値。PIN IDと値により、ファイアウォールのPAYGインスタンスに対する、AutoFocusおよびCortex Data Lake用サイトライセンスの自動アクティブ化も有効になります。 この登録PIN IDと値Palo Alto Networks CSP上で生成する必要があります。PIN IDと値の生成については、VM-Seriesファイアウォールへのデバイス証明書のインストール」を参照してください。

Init-cfg.txt のサンプル ファイル

次の基本設定サンプル ファイルは、このファイルでサポートされているすべてのパラメータを示しています。また、必須のパラメータが太字で表示されています。

サンプル **init-cfg.txt** ファイル（スタティック IP アドレス）	サンプル **init-cfg.txt** ファイル（**DHCP** クライアント）
type=static	**type=dhcp-client**
ip-address=10.*.*.19	ip-address=
default-gateway=10.*.*.1	default-gateway=
netmask=255.255.255.0	netmask=
ipv6-address=2001:400:f00::1/64	ipv6-address=
ipv6-default-gateway=2001:400:f00::2*	ipv6-default-gateway=
hostname=Ca-FW-DC1	hostname=Ca-FW-DC1
vm-auth-key=7550362253****	vm-auth-key=7550362253****
panorama-server=10.*.*.20	panorama-server=10.*.*.20
panorama-server-2=10.*.*.21	panorama-server-2=10.*.*.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg	dgname=finance_dg

©2023 Palo Alto Networks, Inc.

サンプル **init-cfg.txt** ファイル（スタティック IP アドレス）	サンプル **init-cfg.txt** ファイル（**DHCP** クライアント）
dns-primary=10.5.6.6	dns-primary=10.5.6.6
dns-secondary=10.5.6.7	dns-secondary=10.5.6.7
op-command-modes=jumbo-frame,mgmt-interface-swap**	op-command-modes=jumbo-frame,mgmt-interface-swap**
op-cmd-dpdk-pkt-io=***	op-cmd-dpdk-pkt-io=***
plugin-op-commands=	plugin-op-commands=
dhcp-send-hostname=no	dhcp-send-hostname=yes
dhcp-send-client-id=no	dhcp-send-client-id=yes
dhcp-accept-server-hostname=no	dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=no	dhcp-accept-server-domain=yes
vm-series-auto-registration-pin-id=abcdefgh1234**	**vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987**	**vm-series-auto-registration-pin-value=zyxwvut-0987****

©2023 Palo Alto Networks, Inc.

AWS上のVM-Seriesファイアウォールでは、管理 IP アドレスおよびネットマスク構成を指定することはできません。AWS はバックエンドのメタデータ ファイルを使用して管理 IP アドレスおよびネットマスクを割り当てるため、定義された場合、ファイアウォールは指定した値を無視します。

*IPv6 アドレスを含める場合は、IPv6 デフォルト ゲートウェイが必要です。

**`mgmt-interface-swap`操作コマンドは AWSまたはGCP上のVM-Seriesファイアウォールでのみ機能します。

***`op-cmd-dpdk-pkt-io=off`は、ESXi、KVM、およびGCP上のVM-SeriesファイアウォールでDPDKを無効にするためのパラメータです（デフォルトでは、DPDKは有効になっています）。

**** `vm-series-auto-registration-pin-id`および`vm-series-auto-registration-pin-value`は、次の2つの場合に必要になります。

- AutoFocusまたはCortex Data Lakeのサイトライセンスのアクティブ化で、VM-SeriesファイアウォールのPay-As-You-Go（PAYG）ライセンスオプションがある場合。
- VM-Seriesファイアウォールでデバイス証明書を取得、インストールする場合。

©2023 Palo Alto Networks, Inc.

Bootstrap.xml ファイルの作成

これらの説明に従って、ターゲットのデプロイ環境と同じプラットフォームまたはハイパーバイザー上で動作しているファイアウォールから設定をエクスポートします。

STEP 1 | ファイアウォールから構成ファイルをエクスポートします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択します。
2. エクスポートする構成ファイルを選択します。
   - 現在アクティブな設定をエクスポートするには、Configuration Management（設定管理）セクションで **Export named configuration snapshot**（名前を付けて保存した設定スナップショットをエクスポート）し、ドロップダウンリストから **running config.xml**（実行中の **config.xml**）を選択します。
   - 過去のファイアウォールの設定をエクスポートするには、Configuration Management（設定管理） セクションで **Export configuration version**（構成バージョンをエクスポート）し、ドロップダウンリストから適切な構成バージョンを選択します。

STEP 2 | 設定ファイル名を変更して保存します。

1. ファイル名を`bootstrap.xml`に変更します。

   このファイル名が完全に一致（大文字と小文字は区別される）しなければブートストラッププロセスが成功しません。
2. `bootstrap.xml`ファイルを`init-cfg.txt`ファイルと同じ場所に保存します。

©2023 Palo Alto Networks, Inc.

ブートストラップ用ライセンスの準備

ブートストラップ プロセス中にファイアウォールにライセンスを付与するには、認証コードを購入し、ブートストラップを開始する前に Palo Alto Networks のサポート ポータルでライセンスおよびサブスクリプションを登録しておく必要があります。

BYOL を実行している VM-Series ファイアウォールの場合（従量制のライセンス—PAYG はこれに該当しない）、キャパシティ認証コード、サポート サブスクリプション、その他の必要なサブスクリプションを含んだ認証コード バンドルを持っていなければなりません。ブートストラップのためのライセンスを準備するプロセスは、ファイアウォールがブートストラップの際にインターネットにアクセスできるかどうかによって異なります。

- 直接インターネット アクセス – ファイアウォールがインターネットに直接接続している状態です。
- 間接インターネット アクセス – ファイアウォールの代わりに直接インターネットに接続してライセンス キーを取得できる Panorama によってファイアウォールが管理されている状態です。
- インターネット アクセスなし – ファイアウォールの代わりにライセンス キーを取得するオーケストレーション サービスあるいはカスタム スクリプトをファイアウォールが使用している状態です。

インターネット アクセスがある VM-Series ファイアウォールの場合

実施時は`/license`フォルダにて認証コードを入力します。

間接インターネット アクセスがある VM-Series ファイアウォールの場合

1. Palo Alto Networks のサポート サイトで認証コードを登録します。
   1. サポートポータルに移動、ログインし、**Assets**（アセット） > **Register New Device**（新規デバイスの登録） > **Register device using Serial Number or Authorization Code**（シリアル番号または認証コードを使用してデバイスを登録）を選択します。
   2. VM-Series ファイアウォールの登録を行うには、以下の手順を実行します。
   3. **Submit**（送信） をクリックします。
2. Palo Alto Networks のサポート サイトで認証コードをアクティベートしてライセンス キーを生成します。
   1. サポートポータルに移動してログインし、**Assets**（アセット）タブを選択します。
   2. 各シリアル番号に対して、**Action**（アクション）リンクをクリックします。
   3. **Activate Auth-Code**（認証コードのアクティベーション）ボタンを選択します。
   4. **Authorization code**（認証コード）を入力し、**Agree**（同意する）、**Submit**（送信）をクリックします。
   5. ライセンス キーをダウンロードし、ローカル フォルダに保存します。
   6. ブートストラップ パッケージの準備に続きます。ダウンロードしたライセンス キーはブートストラップ パッケージの `\license` フォルダに追加する必要があります。

©2023 Palo Alto Networks, Inc.

ファイアウォールの代わりにカスタム スクリプトあるいはオーケストレーション サービスがインターネットにアクセスできる場合。

スクリプトあるいはサービスが、ファイアウォールをデプロイするハイパーバイザから CPU ID および UUID を取得し、CPU ID、UUID、API キーおよび認証コードを入手した状態で Palo Alto Networks のサポート ポータルにアクセスして必要なキーを取得しなければなりません。「ライセンス API」を参照してください。

 ©2023 Palo Alto Networks, Inc.

ブートストラップ パッケージの準備

AWS、Azure、またはGCP上で、パブリッククラウドストレージ内にブートストラップパッケージを作成することができます。

- VM-Seriesプラグインバージョン1.0.13以前、およびバージョン2.0.0と2.0.1は、ストレージバケット単位のブートストラップパッケージをサポートしています。
- VM-Seriesプラグインバージョン2.0.2以降も、パブリッククラウドストレージバケット内のサブフォルダをサポートしています。バケット内に、複数のフォルダやサブフォルダを作成して、それぞれにブートストラップパッケージを配置することができます。一般的にフォルダは、Panoramaデバイスグループなどの、VMグループの設定を表しています。

  ブートストラップパッケージにアクセスするには、ブートストラップフォルダへのフルパスを指定します。例: `my-storage/my-firewalls/bootstrap-2020-10-15`

ブートストラップ パッケージを準備するには、以下の手順を実行します。

STEP 1 | ブートストラップ パッケージのトップレベル ディレクトリ構造を作成します。

ローカルクライアントまたはラップトップで、またはパブリッククラウドストレージバケット内に、次のフォルダを作成します。

```
/config
/content
/software
/license
/plugins
```

フォルダは空でかまいませんが、**/config**、**/license**、**/software**、および **/content** フォルダが揃っていなければなりません。**/plugins**フォルダはオプションであり、PAN-OSのリリースとは別にVM-Seriesプラグインをアップグレードする場合にのみ必要です。

ブートストラップ構造には、他のファイルやフォルダを保管しないでください。他のファイルやフォルダを追加すると、ブートストラップが失敗してしまいます。

```
/my-storage
   /my-firewalls
      /internal      /external
        /config        /config
        /content       /content
        /license       /license
        /plugins       /plugins
        /software      /software
```


©2023 Palo Alto Networks, Inc.

STEP 2 | 各フォルダにコンテンツを追加します。

このプロセスの概要については、「ブートストラップ パッケージ」を参照してください。**/config** フォルダのファイルの詳細は、「ブートストラップ設定ファイル」を参照してください。

```
/config
  0008C100105-init-cfg.txt
  0008C100107-init-cfg.txt
  bootstrap.xml
/content
  panupv2-all-contents-488-2590
  panup-all-antivirus-1494-1969
  panup-all-wildfire-54746-61460
/software
  PanOS_vm-10.0.0
/license
  authcodes
  0001A100110-url3.key
  0001A100110-threats.key
  0001A100110-url3-wildfire.key
/plugins
  vm_series-2.0.2
```

- *license* フォルダにキーを保存する場合、分かりやすいファイル命名規則を使用できますが、ファイル名に *.key* 拡張子を付けてください。認証コードの場合、*authcodes* という名前のテキスト ファイル（ファイル拡張子なし）を作成して認証コードをこのファイルに追加し、*license* フォルダに保存します。
- 個々の認証コードの代わりに認証コード バンドルを使用すると、ファイアウォールに紐付けられたすべてのライセンス キーをファイアウォールあるいはオーケストレーション サービスが同時に取得できるようになります。バンドルの代わりに個々の認証コードを使用する場合、ファイアウォールはファイルに含まれた最初の認証コード用のライセンス キーのみを取得します。
- */plugins* フォルダには、*VM-Series* プラグイン バイナリを *1* つだけ保管します。複数のプラグイン バージョンを保管しないでください。

STEP 3 | ブートストラップ パッケージを作成します。

VM-Series ファイアウォールの場合、ハイパーバイザに適した形式のイメージファイルを作成します。「ブートストラップパッケージの配信」を参照してください。

©2023 Palo Alto Networks, Inc.

AWS 上での VM-Series ファイアウォールのブートストラップ

STEP 1 | ブートストラップ方法を選択します。

- 基本設定をブートストラップパッケージに追加するには、ステップ2に進みます。
- ユーザーデータとして基本設定を入力する、またはAWSシークレットから基本設定を取得するためにユーザーデータを使用する場合は、ステップ3に進みます。

STEP 2 | 読み取りアクセスを有効にするために、S3バケットとIAMロールを準備します。

ファイルを使ってブートストラップを行うには、プロセスを完了させるために必要な AWS S3 および IAM の許可について知っておく必要があります。ポリシーを作成する詳細な方法は、AWS ドキュメントの「顧客管理ポリシーの作成」を参照してください。

VM-Series ファイアウォールの管理インターフェイスは、S3 バケットにアクセスしてブートストラップを完了できなければなりません。S3 バケットがインターネット経由でアクセスできるように、パブリック IP アドレスまたは Elastic IP アドレスのどちらかを管理インターフェイスに割り当てることができます。もしくは、VPC と S3 バケットの間にプライベート接続を作成し、ファイアウォール管理インターフェイス上ではインターネット アクセスを有効にしない場合には、S3 バケットと同じリージョンに AWS VPC エンドポイントを作成してください。詳細については、VPC エンドポイントの設定に関する AWS ドキュメントを参照してください。

1. インラインポリシーを持つ IAM を作成し、S3 バケット（ListBucket、GetObject）への読込権限を有効化します。IAM ロールの作成、ロールを割り当てるアカウントやAWSサービスの定義、ロールを割り当てたアプリケーションが使用してよいAPIアクションやリソースの定義の詳細な手順については、AWSドキュメントの IAM Roles for Amazon EC2（Amazon EC2用のIAMロール）を参照してください。VM-Series ファイアウォールを起動する際、このロールを割り当てて S3 バケットへの読込権限、およびブートストラップを正常に行うためのバケットに含まれたオブジェクトを有効化する必要があります。
2. AWSコンソールで、Amazon Simple Storage Service（S3）バケットを作成するか、または既存のS3バケット内にサブディレクトリを作成します。

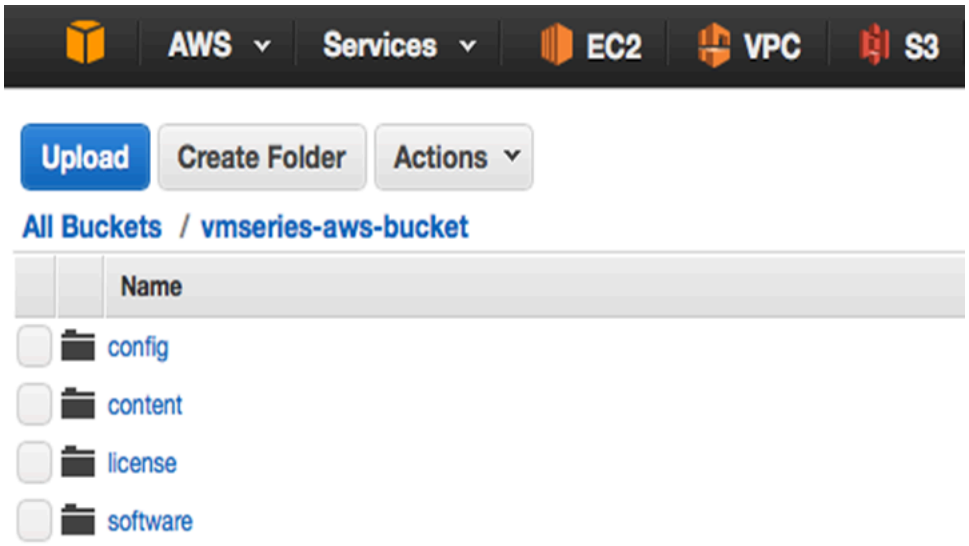
   次の例のS3バケット（vmseries-aws-bucket）は、All Bucketsルート フォルダ レベルにあります。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::<bucketname>"]
   },
   {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
```


©2023 Palo Alto Networks, Inc.

```
        "Resource": ["arn:aws:s3:::<bucketname>/*"]
        }
    ]
}
```

3. 「ブートストラップ パッケージの準備」で説明しているように、S3バケット内にフォルダを作成します。
   - S3バケット内に構造を直接作成します。



   - 任意各フォルダにコンテンツを追加します。フォルダを空にしておくことはできますが、\config、\content、\license、および\softwareのすべてのフォルダが必要になります。\pluginsフォルダは任意です。

> *Amazon S3*へのログインを有効化している場合、*S3*バケット内に自動的に*Logs* フォルダが作成されます。この *Logs* フォルダは *S3* バケットへのアクセスに関する問題のトラブルシューティングを行う際に役立ちます。

STEP 3 | AWS上のVM-Seriesファイアウォールの起動以下のいずれかを選択します。

- **`init-cfg.txt`**–ファイルを使ってファイアウォールを設定する場合、ステップ 2.1で作成したIAMロールをアタッチして、**Advanced Details**（高度な詳細）セクションを展開し、**User Data**（ユーザーデータ）フィールドに、S3バケット、ディレクトリ、またはサブディレクトリへのパスを指定します。例:

```
vmseries-bootstrap-aws-s3bucket=<bucketname>
```

or

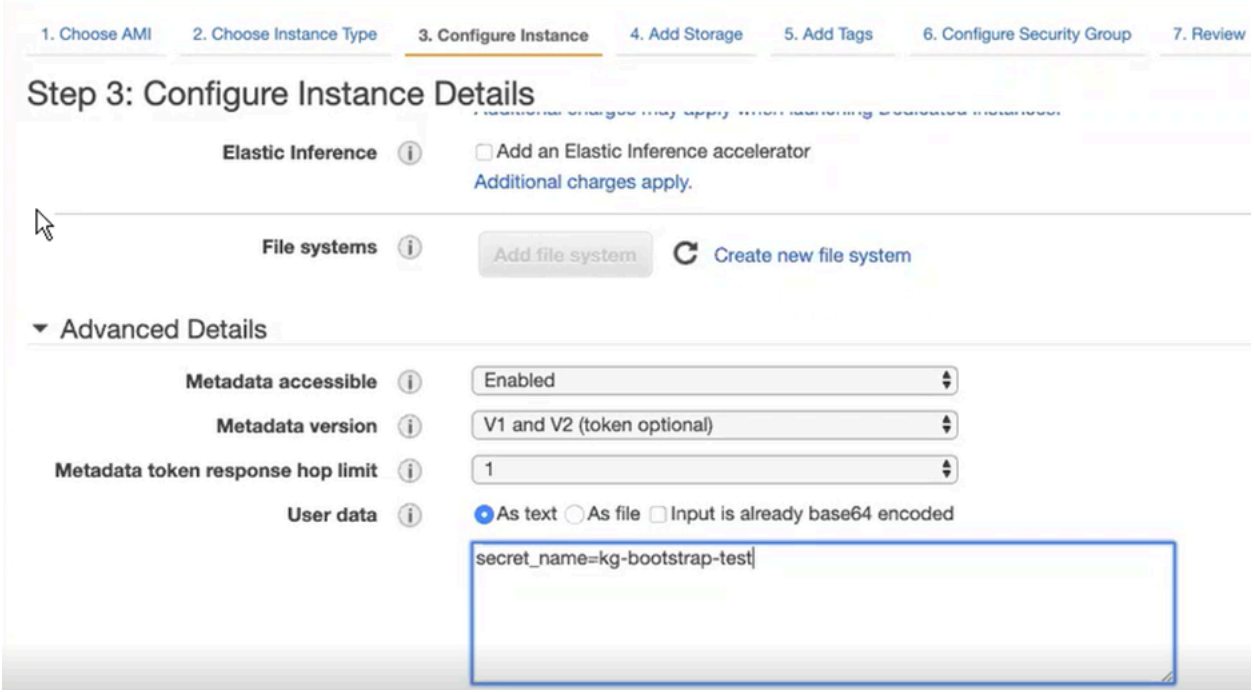
```
vmseries-bootstrap-aws-s3bucket=<bucketname/directoryname>
```

- ユーザーデータ–ユーザーデータを使ってファイアウォールを設定する場合、**Advanced Details**（高度な詳細）セクションを展開して**User Data**（ユーザーデータ）フィールド

©2023 Palo Alto Networks, Inc.

に、「基本設定のユーザーデータとしての入力（パブリッククラウド）」の説明に従って初期ブートストラップパラメータを入力します。

- **AWS Secrets Manager**—「AWS Secrets Managerでの基本設定の保存」の説明に従って基本設定を保管している場合、**Advanced Details**（高度な詳細）セクションを展開して、**User Data**（ユーザーデータ）フィールドで**As text**（テキスト）を選択し、シークレット名をキーと値のペアとして入力します。以下に例を示します。

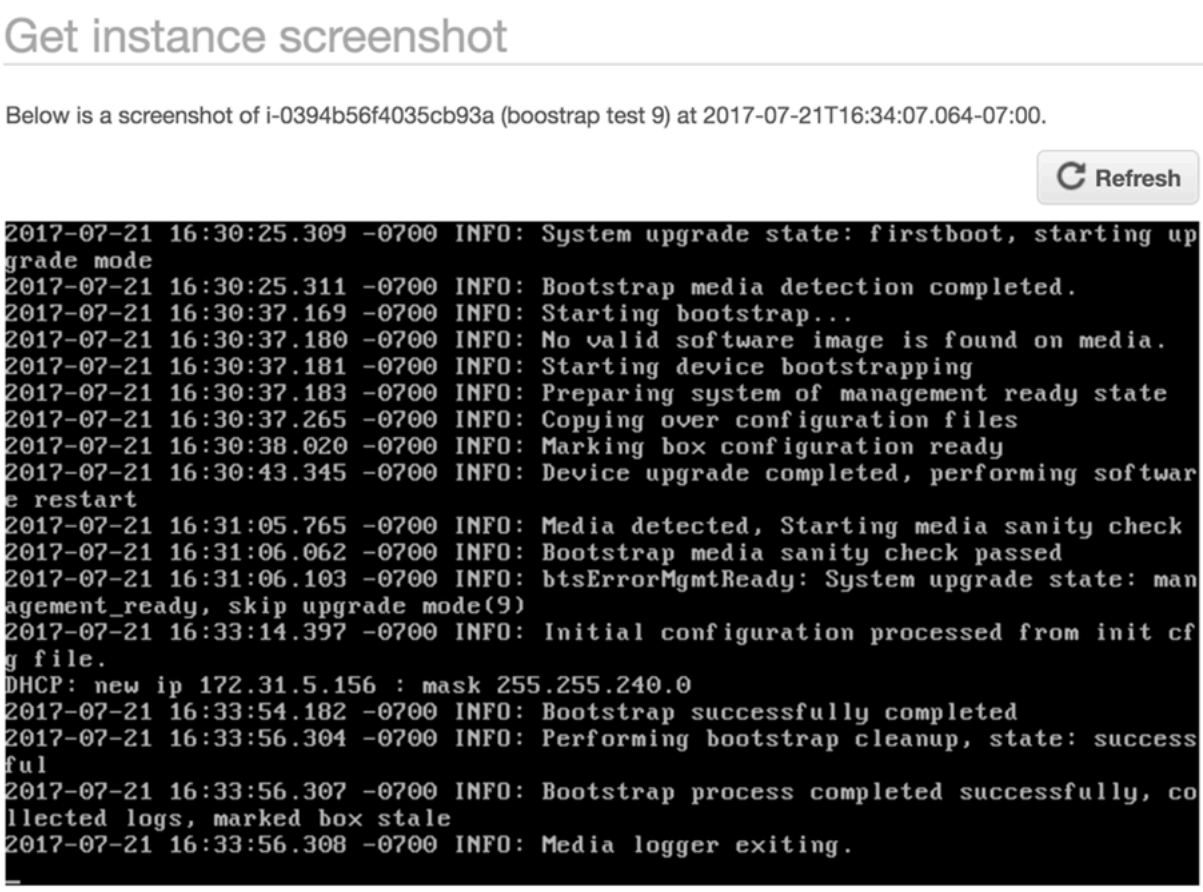


Review and Launch（確認して起動）を選択します。詳細については、「AWS 上の VM-Series ファイアウォールの起動」を参照してください。

©2023 Palo Alto Networks, Inc.

STEP 4 | ブートストラップの結果を検証します。AWS 管理コンソールでファイアウォール インスタンスを選択し、**Actions**（アクション） > **Instance Settings**（インスタンスの設定） > **Get Instance Screenshot**（インスタンス スクリーンショットの取得）を選択します。

- 画面は、処理中のブートストラップを表しています。成功したブートストラップを以下に示します。



- S3バケットを使用しており、S3バケットに正しい権限が割り当てられていないか、またはS3バケットに4つのフォルダがすべて揃っていないと、次のエラー メッセージが表示されます。



 ©2023 Palo Alto Networks, Inc.

Azure 上の VM-Series ファイアウォールのブートストラップ

Azure 上の VM-Series ファイアウォールは、ブートストラッピング用の*Azure Files*サービスをサポートします 。

STEP 1 | ブートストラップ方法を選択します。

- 基本設定をブートストラップパッケージに追加するには、ステップ2に進みます。

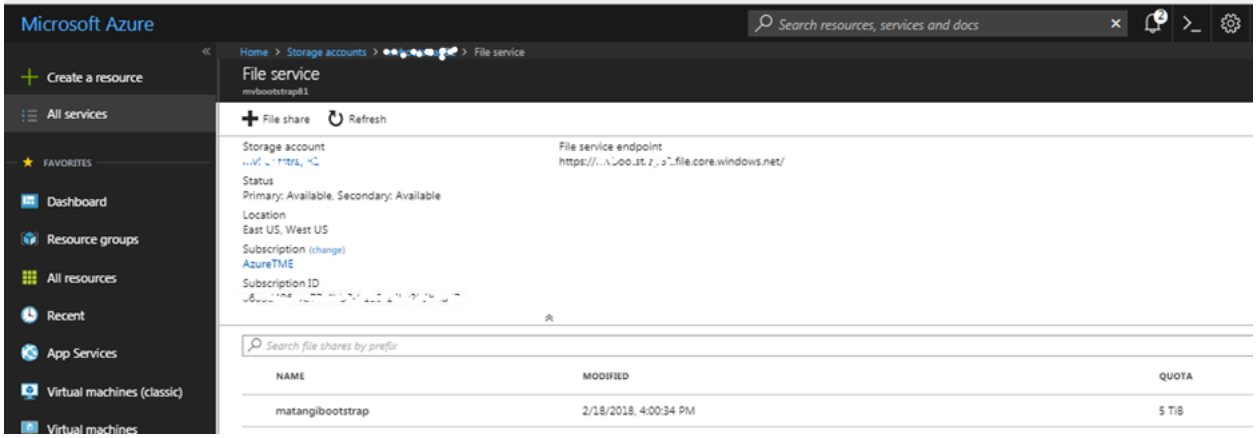
  Azure上の VM-Series ファイアウォールのブートストラップ パッケージを管理するには、Azure 上のストレージ アカウントを熟知し、ブートストラップ パッケージに必要なフォルダ構造を含むファイル共有とディレクトリ オブジェクトの作成方法を理解する必要があります。ファイル共有をホストするストレージ アカウントと同じリージョンにデプロイされたすべてのファイアウォールがファイルに同時にアクセスできるように、多くの仮想マシン間で Azure ファイル共有機能を共有できます。

  VM-Series ファイアウォールの管理インターフェイスは、ブートストラップを完了できるようにブートストラップ パッケージを保持するファイル共有にアクセスできる必要があります。

- 基本設定のユーザーデータとしての入力（パブリッククラウド）を行うには、ステップ3.2に進んでください。

STEP 2 | Azure Files サービス内でブートストラップ パッケージを設定します。

1. Azure ポータルで、ストレージ アカウントを選択するか作成します。
2. Azure Files サービス内にファイル共有を作成します。

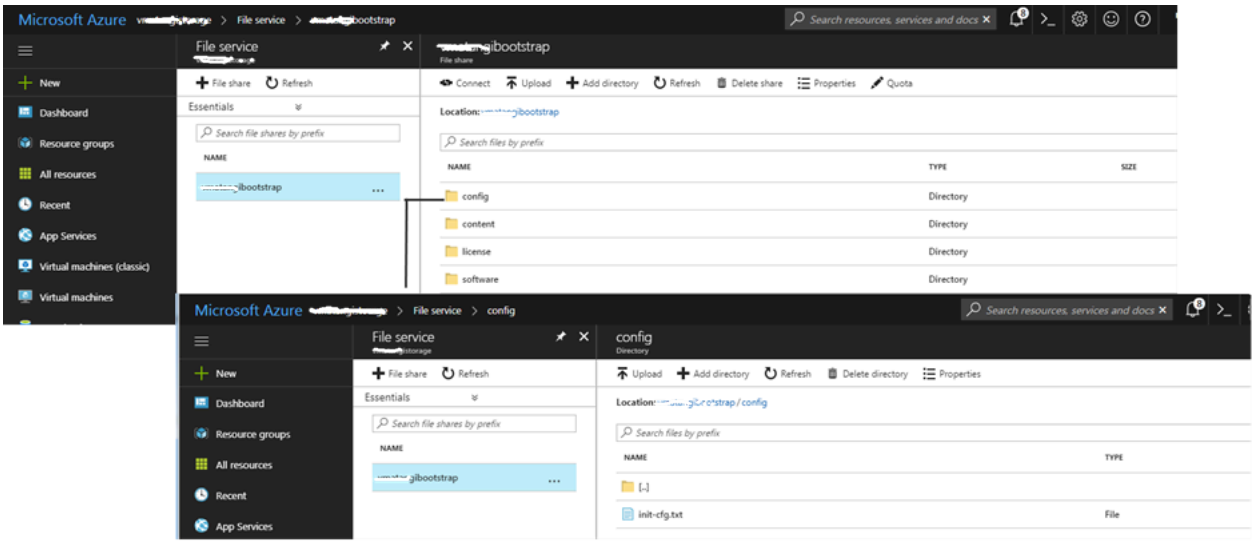


3. ストレージ アカウント内にフォルダを作成します。

   - rootフォルダに直接ブートストラップ用のトップレベルディレクトリ構造を作成して、各ブートストラップ用のサブフォルダを作成します。
   - 各フォルダにコンテンツフォルダを追加します。フォルダは空でかまいませんが、4つのフォルダ（config、license、software、およびcontent）すべてが親フォル

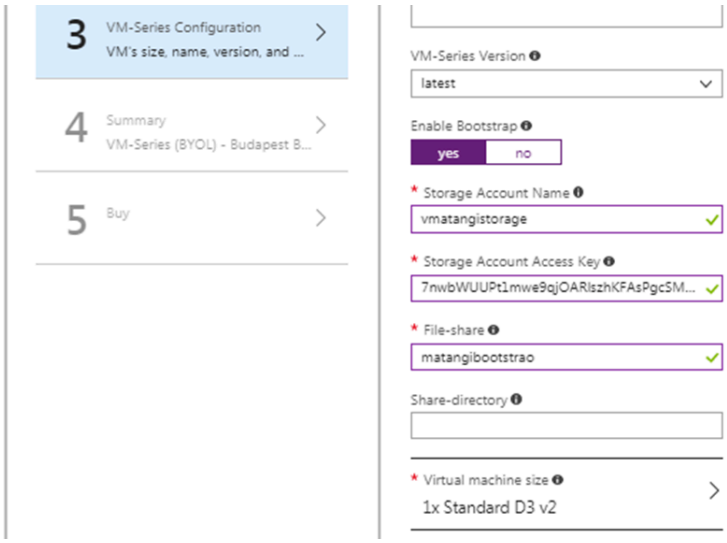
©2023 Palo Alto Networks, Inc.

ダ内に存在していなければなりません。次のスクリーンショットでは`config` フォルダに `init-cfg.txt` ファイルがアップロードされていることが分かります。



STEP 3 | Azure マーケットプレイスからの VM-Series ファイアウォールのデプロイ（ソリューションテンプレート）。

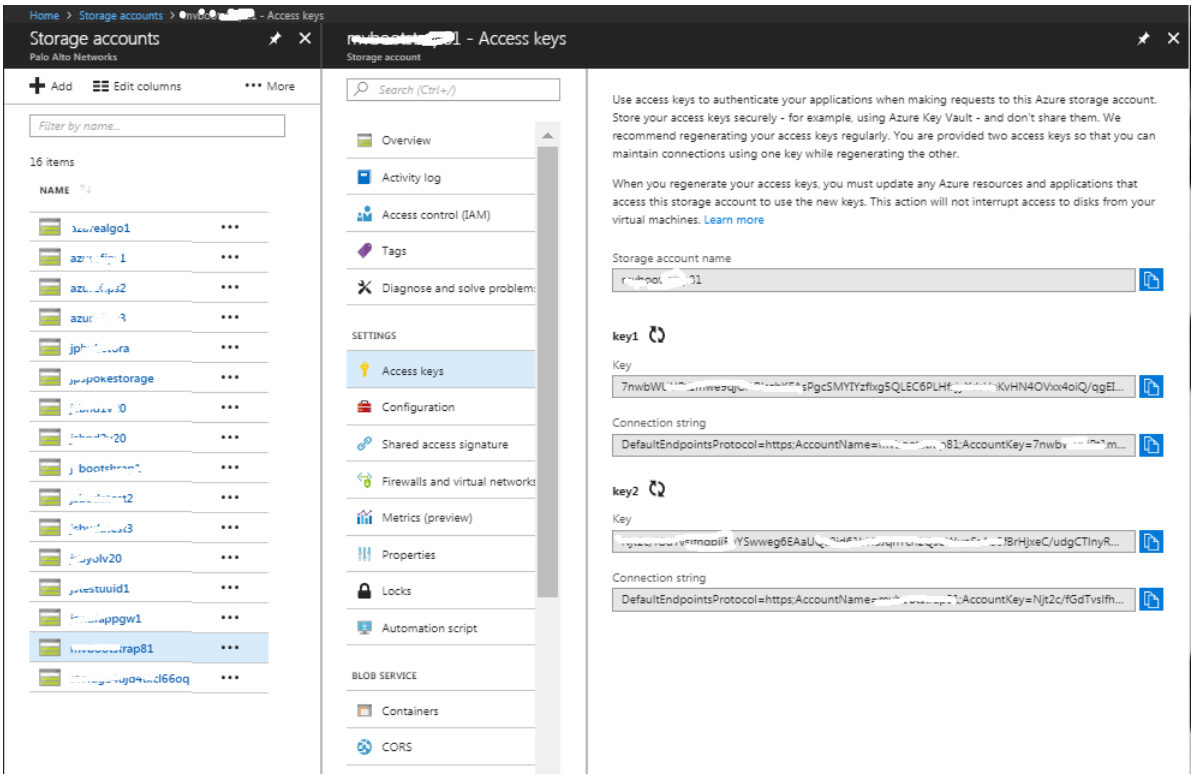
- ファイアウォールの設定にファイルを使用する場合は、ステップ3.1に進んでください。
- ファイアウォールの設定にカスタムデータを使用する場合は、ステップ3.2に進んでください。



1. ブートストラップパッケージを使用する場合は、[ブートストラップを有効にする:はい]を選択し、ブートストラップファイルを保持するファイル共有にアクセスするために必要な情報を提供します。
   1. ストレージのアカウント名– ブートストラップ フォルダのファイル共有を作成した Azure ストレージ アカウントです。
   2. ストレージ アカウントのアクセスキー–ファイアウォールはストレージ アカウントを認証し、その中に保存されているファイルにアクセスするには、このアクセス

©2023 Palo Alto Networks, Inc.

キーが必要です。このアクセスキーをコピーするには、ストレージ アカウント名を選択してから、**Setttings**（設定） > **Access Keys**（アクセスキー）を選択します。



3. **File-share**（ファイルシェア）–ブートストラップパッケージを保管しているファイルシェア名。
4. （任意）**Share-directory**（共有ディレクトリ）–ファイルシェア内のサブフォルダへのパス。異なる設定のブートストラップ設定用のリポジトリとして機能する共通のファイルシェアがある場合は、共有ディレクトリを使用してフォルダ階層を作成し、共通のファイルシェア内の特定のサブフォルダ セットにアクセスできます。

2. カスタムデータとして設定パラメータを入力します。キーと値のペアについては、「基本設定のユーザーデータとしての入力（パブリッククラウド）」を参照してください。各キーと値のペアは、セミコロンで区切ります。以下に例を示します。

```
type=dhcp-client; op-command-modes=jumbo-frame;
vm-series-auto-registration-pin-id=abcdefgh1234****;
vm-series-auto-registration-pin-value=zyxwvut-0987****
```

「Azure仮想マシン上でのカスタムデータとCloud-Init」のいずれかの方法を使って、カスタムデータを提供します。

STEP 4 | ブートストラップの結果を検証します。

©2023 Palo Alto Networks, Inc.

ESXi における VM-Series ファイアウォールのブートストラップ

ISO イメージまたは仮想ハードディスクを使用して VM-Series ファイアウォールをブートストラップできます。

- ISO を使用した ESXi における VM-Series ファイアウォールのブートストラップ
- Block Storage デバイスを使用した ESXi における VM-Series ファイアウォールのブートストラップ

ISO を使用した ESXi における VM-Series ファイアウォールのブートストラップ

ISO を使用する ESXi サーバー上で VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

STEP 1 | ISOイメージを作成し、Virtual Machine File System（VMFS）データストアあるいはNetwork File System（NFS）ボリュームにアップロードします。

1. ブートストラップ パッケージの準備。
2. ISO イメージを作成します。イメージファイルを作成するために使用するツールは、クライアントのオペレーティングシステムによって変わります。
3. ESX/ESXiホストにアクセスできるVMFSデータストアあるいはNFSボリュームにISOイメージをアップロードします。

STEP 2 | ファイアウォールをデプロイします。

1. ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング。

   デフォルト設定では、ファイアウォールは 2 つのネットワークインターフェイス（一つは管理トラフィック用、もう一つはデータトラフィック用）とともにデプロイされます。ファイアウォール上にある最初のイーサネット インターフェイス（管理インターフェイス）が、デバイス管理のために割り当てられた仮想スイッチ ポートグループに接続されていることを確認します。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ イメージをファイアウォールに添付します。

1. **Inventory**（インベントリ）リストで VM-Series ファイアウォールを選択します。
2. **Edit Settings**（設定編集）をクリックし、**Virtual Hardware**（仮想ハードウェア）を選択します。
3. **CD DVD drive**（**CD DVD**ドライブ）のドロップダウンリストから **Datastore iso file**（データストア **iso** ファイル）を選択し、ISOイメージを参照します。
4. ファイアウォールをパワーオンします。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
5. ブートストラップの結果を検証.

Block Storage デバイスを使用した ESXi における VM-Series ファイアウォールのブートストラップ

ブロック ストレージ デバイスを使用する ESXi サーバー上で VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

STEP 1 | ブートストラップ パッケージと仮想ハードディスクを作成します。

1. ブートストラップ パッケージを作成します。
2. Linux 仮想マシンをデプロイします。
3. Linux 仮想マシンで、ブートストラップ パッケージの準備を行います。フォルダは空でかまいませんが、4 つのフォルダがすべて揃っていなければなりません。
4. 39 GB 未満の新しいデータディスクを Linux 仮想マシンに割り当てます。
5. ディスクをパーティション分けし、ファイルシステムのフォーマットをext3にします。
6. 新しいファイルシステム用のディスクを作成し、ディスクを Linux 仮想マシンにマウントします。
7. ブートストラップ パッケージのコンテンツをディスクにコピーします。
8. ディスクをアンマウントします。
9. Linux 仮想マシンからディスクをディスパッチします。作成したブートストラップ ディスクを記述した Disk File（ディスク ファイル）の内容をメモします。データストア名とディスクへのパスが示されています。Delete Files From Datastore（データストアからファイルを削除）チェックボックスは選択しないでください。このチェックボックスを選択するとディスクが削除されます。

STEP 2 | ファイアウォールをデプロイします。

1. ESXi サーバー上の VM-Series ファイアウォールのプロビジョニング。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ パッケージをファイアウォールに添付します。

1. Inventory（インベントリ）リストで VM-Series ファイアウォールを選択します。
2. **Edit Settings**（設定編集）をクリックし、**Virtual Hardware**（仮想ハードウェア）を選択します。
3. New Device（新規デバイス）ドロップダウンから**Existing Hard Disk**（既存のハードディスク）を選択します。メモをとっておいたデータストアとパスの情報に従ってブートストラップ ディスクを選択します。
4. ファイアウォールをパワーオンします。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
5. ブートストラップの結果を検証。

©2023 Palo Alto Networks, Inc.

Google Cloud Platform 上の VM-Series ファイアウォールのブートストラップ

STEP 1 | ブートストラップ方法を選択します。

STEP 2 | Google Cloud Console にログインします。

- ブートストラップパッケージに基本設定を追加するには、「ブートストラップパッケージの準備」の説明に従ってブートストラップファイルを作成し、ステップ3に進みます。
- 基本設定をカスタムメタデータとして入力する場合は、ステップ4に進みます。

©2023 Palo Alto Networks, Inc.

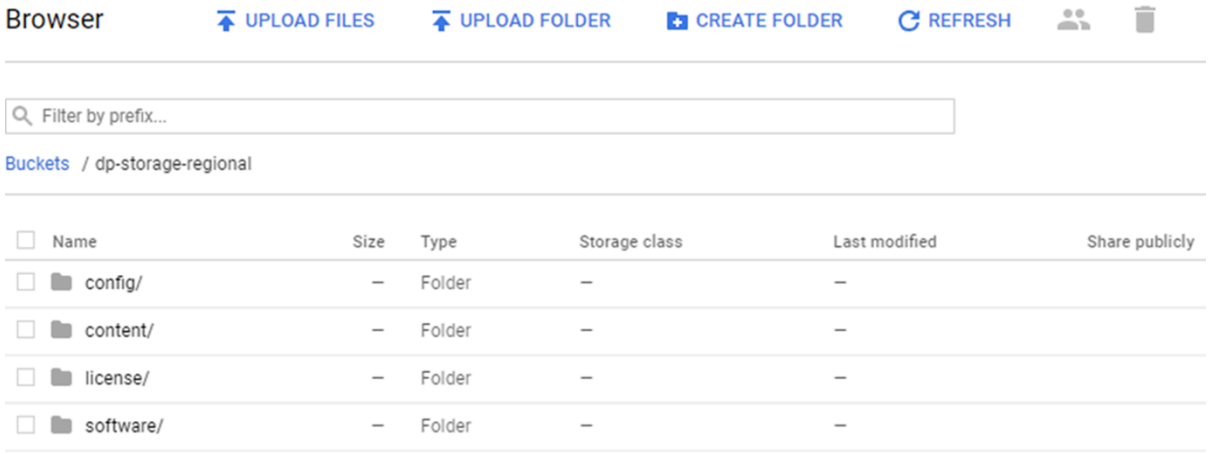
STEP 3 | **Storage**（ストレージ） > **Browser**（ブラウザ）を選択して、**Create Bucket**（バケットの作成）をクリックします。

Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイするを行う際、このバケットを使用してファイアウォールのブートストラップを行うことができます。

同じプロジェクトで Google ストレージ バケットを使用してブートストラップする場合は、devstorage.read_only IAM 権限が必要です。

トップレベルでバケットを作成、記入する、またはサブフォルダを持つバケットを作成して、多数のブートストラップパッケージに同じバケットを共有させることができます。

1. バケット名を入力し、デフォルトのストレージ クラスを選択して、場所を選択します。ストレージ バケット内の場所は、コンピューティング エンジン インスタンス用に指定したゾーンと互換性がなければなりません。
2. **Create**（作成）をクリックします。
3. ストレージ ブラウザで、バケット名をクリックして開きます。
4. **Create Folder**（フォルダ作成）をクリックして、 フォルダの `config` の名前を付けます。**Create**（作成）をクリックします。
5. `content`、`license`、`software` 用のフォルダを次の通りに作成して繰り返します。すべてのフォルダが、例え空であっても存在する必要があります。



6. （任意）**`init-cfg.txt`**ファイルを作成した場合は、`config`フォルダを開きます。**Upload Files**（ファイルのアップロード）をクリックして、**`init-cfg.txt`** ファイルを参照して選択し、**Open**（開く）をクリックします。
7. `license`（ライセンス）フォルダを開き、**`authcodes`** ファイルをアップロードします。
8. すべてのブートストラップ ファイルをアップロードするまで続行します。

STEP 4 | 初期設定パラメータをメタデータとして追加します。「基本設定のユーザーデータとしての入力（パブリッククラウド）」の説明に従って、各キーと値のペアを**Add**（追加）します。

STEP 5 | デプロイメントの詳細については、「Google Cloud Platform Marketplace から VM-Series ファイアウォールをデプロイする」を参照してください。

©2023 Palo Alto Networks, Inc.

Hyper-V における VM-Series ファイアウォールのブートストラップ

ISO イメージまたは仮想ハードディスクを使用して VM-Series ファイアウォールをブートストラップできます。

- ISO を使用した Hyper-V での VM-Series ファイアウォールのブート処理
- Block Storage デバイスを使用した Hyper-V における VM-Series ファイアウォールのブートストラップ

ISO を使用した Hyper-V での VM-Series ファイアウォールのブート処理

Hyper-V サーバー上で ISO イメージを使用して VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

STEP 1 | ISO イメージを作成します。

1. ブートストラップ パッケージの準備。
2. ISO イメージを作成します。イメージファイルを作成するために使用するツールは、クライアントのオペレーティングシステムによって変わります。
3. Hyper-VホストにアクセスできるところにISOイメージをアップロードします。

STEP 2 | ファイアウォールをデプロイします。

1. Hyper-V Manager を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング。

   デフォルト設定では、ファイアウォールは 2 つのネットワークインターフェイス（一つは管理トラフィック用、もう一つはデータトラフィック用）とともにデプロイされます。ファイアウォール上にある最初のイーサネット インターフェイス（管理インターフェイス）が、デバイス管理のために割り当てられた vSwitch に接続されていることを確認します。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ イメージをファイアウォールに添付します。

1. Hyper-V Manager で**Virtual Machines**（仮想マシン）のリストから VM-Series ファイアウォールを選択します。
2. 設定 > ハードウェア > **IDE** コントローラ > **DVD** ドライブをクリックします。

   複数の *DVD* ドライブがある場合は、*ISO* イメージを最初のドライブに適用する必要があります。
3. Media（メディア）以下にある**Image file**（イメージファイル）のラジオボタンをクリックします。
4. **Browse**（参照）をクリックし、アップロード済みのISOイメージを選択します。
5. **Apply**（適用）および**Ok**をクリックして仮想マシン設定画面を閉じます。
6. ファイアウォールをパワーオンします。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
7. ブートストラップの結果を検証。

Block Storage デバイスを使用した Hyper-V における VM-Series ファイアウォールのブートストラップ

ブロック ストレージ デバイスを使用する Hyper-V サーバー上で VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

©2023 Palo Alto Networks, Inc.

STEP 1 | ブートストラップ パッケージと仮想ハードディスクを作成します。

1. Linux 仮想マシンをデプロイします。
2. Linux 仮想マシンで、ブートストラップ パッケージの準備を行います。フォルダは空でかまいませんが、4 つのフォルダがすべて揃っていなければなりません。
3. 39 GB 未満の新しいデータディスクを Linux 仮想マシンに割り当てます。
   1. Linux バーチャル マシンをパワーオンします。
   2. Hyper-V で Virtual Machines（仮想マシン）のリストから Linux 仮想マシンを選択します。
   3. **Settings**（設定） > **Hardware**（ハードウェア） > **IDE Controller**（**IDE** コントローラ）を選択します。
   4. **Hard Drive**（ハード ドライブ）を選択して**Add**（追加）をクリックします。
   5. **Virtual Hard Disk**（仮想ハードディスク）を選択して**New**（新規）をクリックします。
   6. 画面に表示される指示に従って新しい VHD を作成します。新しい VHD の名前とパスをメモします。
   7. **Apply**（適用）をクリックしてから**OK**をクリックして仮想マシン設定画面を閉じます。
   8. Linux 仮想マシンの電源を入れます。
4. Linux 仮想マシンの CLI に接続します。
5. ディスクをパーティション分けし、ファイルシステムのフォーマットをext3にします。
6. 新しいファイルシステム用のディスクを作成し、ディスクを Linux 仮想マシンにマウントします。
7. ブートストラップ パッケージのコンテンツをディスクにコピーします。
8. ディスクをアンマウントします。
9. Linux 仮想マシンからディスクをディスパッチします。
   1. Linux バーチャル マシンをパワーオンします。
   2. Virtual Machines（仮想マシン）のリストから Linux 仮想マシンを選択します。
   3. **Settings**（設定） > **Hardware**（ハードウェア） > **IDE Controller**（**IDE** コントローラ）を選択します。
   4. 作成した VHD を選択します。
   5. **Remove**（削除）を選択します。これにより VHD が切り離されますが、削除はされません。

STEP 2 | ファイアウォールをデプロイします。

1. Hyper-V Manager を使用した Hyper-V ホスト上の VM-Series ファイアウォールのプロビジョニング。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ ディスク イメージをファイアウォールに添付します。

1. Virtual Machines（仮想マシン）のリストからファイアウォールを選択します。
2. **Settings**（設定） > **Hardware**（ハードウェア） > **IDE Controller**（**IDE** コントローラ）を選択します。
3. **Hard Drive**（ハード ドライブ）を選択して**Add**（追加）をクリックします。
4. **Virtual Hard Disk**（仮想ハードディスク）を選択してから **Browse**（参照）を選択します
5. 作成したブートストラップ VHD を参照して選択し、**Open**（開く）を選択します。
6. **Apply**（適用）をクリックしてから **OK** をクリックして仮想マシン設定画面を閉じます。
7. ファイアウォールをパワーオンします。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
8. ブートストラップの結果を検証.

©2023 Palo Alto Networks, Inc.

KVM 上での VM-Series ファイアウォールのブートストラップ

KVM 上で ISO イメージまたは仮想ハードディスクを使用して VM-Series ファイアウォールをブートストラップできます。

- ISO を使用した KVM における VM-Series ファイアウォールのブートストラップ
- Block Storage デバイスを使用した KVM における VM-Series ファイアウォールのブートストラップ

ISO を使用した KVM における VM-Series ファイアウォールのブートストラップ

ISO を使用する KVM サーバー上で VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

STEP 1 | ISO イメージを作成します。

1. ブートストラップ パッケージを準備します。
2. ISO イメージを作成します。イメージファイルを作成するために使用するツールは、クライアントのオペレーティングシステムによって変わります。
3. KVMホストにアクセスできるところにISOイメージをアップロードします。

STEP 2 | ファイアウォールをデプロイします。

1. KVM に VM-Series ファイアウォールをインストールします。

   デフォルト設定では、ファイアウォールは 2 つのネットワークインターフェイス（一つは管理トラフィック用、もう一つはデータトラフィック用）とともにデプロイされます。ファイアウォール上にある最初のイーサネット インターフェイス（管理インターフェイス）が、デバイス管理のために割り当てられた仮想スイッチ ポートグループに接続されていることを確認します。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ イメージをファイアウォールに添付します。

1. virt-managerでVM-Seriesファイアウォールをダブルクリックし、コンソールを開きます。
2. **View**（ビュー） > **Details**（詳細）に移動して VM ハードウェアの詳細を確認します。
3. **Add Hardware**（ハードウェアを追加）をクリックしてAdd New Virtual Hardware（新しい仮想ハードウェアを追加）メニューを開きます。
4. デバイスの種類をIDE CDROMに変更します。
5. **Select managed or other existing storage**（管理対象あるいはその他の既存のストレージを選択）ラジオボタンをクリックし、**Browse**（参照）をクリックします。作成済みのISOイメージを探し、**Choose Volume**（ボリュームを選択）をクリックします。
6. **Finish**（完了）をクリックして Add New Virtual Hardware（新しい仮想ハードウェアを追加）メニューを閉じます。
7. **Virtual Machine**（仮想マシン） > **Run**（起動）に移動してファイアウォールの電源を投入します。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
8. ブートストラップの結果を検証します。

Block Storage デバイスを使用した KVM における VM-Series ファイアウォールのブートストラップ

ブロック ストレージ デバイスを使用する KVM サーバー上で VM-Series ファイアウォールのブートストラップをするためには、以下の手順を実行します。

STEP 1 | ブートストラップ パッケージと仮想ハードディスクを作成します。

1. ブートストラップ パッケージを作成します。
2. 39 GB 未満のサイズで新しいディスク イメージを作成し、ディスクをパーティション分けしてファイル システムのフォーマットを ext3 にします。この処理で使用するツールは、クライアントのオペレーティング システムによって変わります。
3. ディスク イメージ ファイルをマウントして、準備してあるブートストラップ パッケージをディスク イメージ ファイルにコピーします。
4. ブートストラップ パッケージのコンテンツをディスクにコピーします。
5. ディスク イメージをアンマウントします。
6. KVM ホストにアクセスできる場所にディスク イメージ ファイルをアップロードします。

STEP 2 | ファイアウォールをデプロイします。

1. KVM に VM-Series ファイアウォールをインストールします。
2. ファイアウォールの電源は入れません。

©2023 Palo Alto Networks, Inc.

STEP 3 | ブートストラップ ディスク イメージをファイアウォールに添付します。

1. virt-manager で VM-Series ファイアウォールをダブルクリックし、コンソールを開きます。
2. **View**（ビュー） > **Details**（詳細）を選択して VM ハードウェアの詳細を確認します。
3. **Add Hardware**（ハードウェアを追加）をクリックしてAdd New Virtual Hardware（新しい仮想ハードウェアを追加）メニューを開きます。
4. **Storage**（ストレージ）を選択し、**Select or create custom storage**（カスタム ストレージを選択または作成）を選択します。
5. **Manage**（管理）ボタンをクリックして**Choose Storage Volume**（ストレージ ボリュームを選択）ダイアログを開き、作成してあるディスク イメージ ファイルを選択します。
6. Choose Volume（ボリュームを選択）を選択します。
7. デバイス タイプが Disk Device（ディスク デバイス）であることを確認してください。また、Bus Type（バス タイプ）は変更しないでください。
8. Finish（完了）をクリックします。
9. ファイアウォールをパワーオンします。ブートストラップ プロセスとともにファイアウォールが立ち上がり、この状態が数分続きます。プロセスが成功したか失敗したかどうかを示すステータスメッセージがコンソールに表示されます。
10. ブートストラップの結果を検証します。

©2023 Palo Alto Networks, Inc.

ブートストラップの結果を検証

ブートストラップ中、コンソールに基本ステータス ログが表示され、プロセスが完了したことを確認できるようになっています。

STEP 1 | **panorama-server**、**tplname**、**dgname**を`init-cfg.txt`ファイルに含めている場合、Panoramaが管理するデバイス、デバイスグループ、テンプレート名をチェックしてください。

STEP 2 | 一般システム設定および構成内容を確認します。Web インターフェイスにアクセスして、**Dashboard**（ダッシュボード） > **Widgets**（ウィジェット） > **System**（システム）を選択するか、または CLI 操作コマンドの **show system info** および **show config running** を使用します。

STEP 3 | ライセンスのインストール状態を確認します。**Device**（デバイス） > **Licenses**（ライセンス）を選択するか、または CLI 操作コマンドの **request license info** を使用します。

STEP 4 | Panorama の構成が終了していれば、Panorama でコンテンツバージョンおよびソフトウェアバージョンを管理します。Panoramaの構成が終了していなければ、Webインターフェイスを使用してコンテンツバージョンおよびソフトウェアバージョンを管理します。

©2023 Palo Alto Networks, Inc.

ブートストラップのエラー

ブートストラップ プロセスの際にエラーメッセージを受け取った場合、次の表で詳細を確認します。

エラーメッセージ（重大度）	理由
ブートストラップ イメージのエラー（高）	• ブートストラップ パッケージで外部デバイスが未検出です。 または • 外部デバイスにあるイメージファイルからブートを行う際に重大なエラーが発生しました。ブートストラップ プロセスが中断されました。
外部デバイスにブートストラップ設定ファイルがありません（高）	外部デバイスにブートストラップ設定ファイルがありません。
必須のネットワーク情報のパラメータがブートストラップ設定ファイル内に無いか、不正です。	ブートストラップに必要なネットワークパラメータが不正か、存在しません。ブートストラップのエラーを引き起こした値（IPアドレス、ネットマスク、デフォルトゲートウェイ）がエラーメッセージにリストアップされます。
Failed to install license key for file <license-key-filename> (high)	ライセンス キーを適用できませんでした。このエラーは、使用したライセンス キーが不正であることを示します。適用できなかったライセンス キーの名前が表示されます。
Failed to install license key using authcode <authcode> (high)	The license auth code could not be applied.This error indicates that the license auth code used was invalid.The output includes the name of the authcode that could not be applied.
Failed content update commits (high)	The content updates were not successfully applied.
USB media prepared successfully using given bundle (informational)	The bootstrap image has been successfully complied on the USB flash device. <username>:Successfully prepared the USB using bundle <bundlename>
ブートストラップ成功（通知）	ブートストラップ設定ファイルでファイアウォールを正しく準備できました。インストールされたライセンス キー、ブートストラップ設定ファイルの名前が表示されます。VM-Seriesファイアウォールの場合のみ、PAN-OSバージョンおよびコンテンツアップデートのバージョンも表示されます。

©2023 Palo Alto Networks, Inc.

ブートストラップ パッケージについての情報とブートストラップ パッケージの準備を行う方法をご確認ください。

 ©2023 Palo Alto Networks, Inc.