PAN-OS Web 介面說明

Version 10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

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

Last Revised

December 10, 2020

Table of Contents

Web 介面基本概念 13
防火牆概要 14
功能與優點 15
上次登入時間和失敗的登入嘗試 16
當日訊息 17
工作管理員 18
語言 20
警示 21
認可變更 22
儲存候選組態 25
還原變更 28
鎖定組態 31
全域尋找 32
威脅詳細資訊 33
AutoFocus 情報摘要 35
組態表匯出 37

儀錶盤 39
儀表板 Widget 40

ACC 43
認識 ACC 44
ACC 頁籤 46
ACC Widget 47
ACC 動作 49
使用頁籤和 Widget 49
使用篩選器—本機篩選器和全域篩選器 50

監控 53
監控 > 日誌 54
日誌類型 54
日誌動作 58
監控 > 外部日誌 60
監控 > 自動關聯引擎 61
監控 > 自動關聯引擎 > 關聯物件 61
Monitor > Automated Correlation Engine > Correlated Events (監視 > 自動關聯引擎 > 關聯事件) 62
監控 > 封包擷取 64
封包擷取概要 64
自訂封包擷取的建置組塊 65
啟用威脅封包擷取 66
監控 > App Scope 68
App Scope 概要 68
App Scope 摘要報告 68
App Scope 異動監控報告 69
App Scope 威脅監控報告 71
App Scope 威脅地圖報告 72

App Scope 網路監控報告 74
App Scope 流量地圖報告 75
監控 > 工作階段瀏覽器 77
監控 > 封鎖 IP 清單 78
封鎖 IP 清單項目 78
檢視或刪除封鎖 IP 清單項目 79
Monitor > Botnet (監視 > Botnet) 80
botnet 報告設定 80
殭屍網路組態設定 80
監控 > PDF 報告 82
監控 > PDF 報告 > 管理 PDF 摘要 82
監視 > PDF 報告 > 使用者活動報告 83
Monitor > PDF Reports > SaaS Application Usage (監測 > PDF 報告 > SaaS 應用程式使用情況) 84
Monitor > PDF Reports > Report Groups (監控 > PDF 報告 > 報告群組) 86
監視 > PDF 報告 > 電子郵件排程器 87
監控 > 管理自訂報告 88
監控 > 報告 89

政策 91
政策類型 92
移動或複製原則規則 93
稽核註解封存檔 94
稽核註解 94
組態日誌 (認可之間) 94
規則變更 95
規則使用方式命中數查詢 96
規則命中數查詢的裝置規則使用方式 96
Policies > Security (原則 > 安全性) 98
安全性原則概要 98
安全性原則規則中的建置組塊 99
建立和管理原則 106
取代或還原安全性原則規則 109
應用程式與使用情況 111
安全性政策最佳化工具 113
Policies > NAT (原則 > NAT) 115
NAT 原則一般頁籤 115
NAT 原始封包頁籤 116
NAT 轉譯封包頁籤 116
NAT 主動/主動 HA 繫結頁籤 119
NAT 目標頁籤 119
Policies > QoS (原則 > QoS) 121
Policies > Policy Based Forwarding (原則 > 基於原則的轉送) 125
基於原則的轉送一般頁籤 125
基於原則的轉送來源頁籤 126
基於原則的轉送目的地/應用程式/服務頁籤 126
基於原則轉送的轉送頁籤 127
基於原則的轉送目標頁籤 128
Policies > Decryption (原則 > 解密) 129
解密一般頁籤 129
解密來源頁籤 130
解密目的地頁籤 131
解密服務/URL 類別頁籤 131

解密選項頁籤 131
解密目標頁簽 132
Policies > Tunnel Inspection（原則 > 通道檢查）134
通道檢查原則中的建置組塊 134
Policies > Application Override（原則 > 應用程式取代）139
應用程式取代一般頁籤 139
應用程式取代來源頁籤 140
應用程式取代目的地頁籤 140
應用程式取代通訊協定/應用程式頁籤 141
應用程式取代目標頁籤 141
Policies > Authentication（原則 > 驗證）143
驗證原則規則的建置組塊 143
建立和管理驗證原則 147
Policies > DoS Protection（原則 > DoS 保護）148
DoS 保護一般頁籤 148
DoS 保護來源頁籤 149
DoS 保護目的地頁籤 149
DoS 保護選項/保護頁籤 150
DoS 保護目標頁簽 151
Policies > SD-WAN（政策 > SD-WAN）153
SD-WAN 一般頁籤 153
SD-WAN 來源籤 153
SD-WAN 目的地頁籤 154
SD-WAN 應用程式/服務頁籤 155
SD-WAN 路徑選取頁籤 156
SD-WAN 目標頁籤 156

物件 159
移動、複製、取代或還原物件 160
移動或複製物件 160
取代或還原物件 160
Objects > Addresses（物件 > 位址）162
Objects > Address Groups（物件 > 位址群組）164
Objects > Regions（物件 > 地區）166
Objects > Dynamic User Groups（物件 > 動態使用者群組）167
Objects > Applications（物件 > 應用程式）169
應用程式概要 169
應用程式上支援的動作 172
定義應用程式 174
Objects > Application Groups（物件 > 應用程式群組）178
Objects > Application Filters（物件 > 應用程式篩選器）179
Objects > Services（物件 > 服務）180
物件 > 服務群組 182
Objects > Tags（物件 > 頁籤）183
建立頁籤 183
以群組形式檢視規則庫 184
管理頁籤 187
Objects > Devices（物件 > 裝置）189
Objects > External Dynamic Lists（物件 > 外部動態清單）190
物件 > 自訂物件 194
Objects > Custom Objects > Data Patterns（物件 > 自訂物件 > 資料模式）194
Objects > Custom Objects > Spyware/Vulnerability（物件 > 自訂物件 > 間諜軟體 / 弱點）199

Objects > Custom Objects > URL Category（物件 > 自訂物件 > URL 類別）.....202
Objects > Security Profiles（物件 > 安全性設定檔）.....204
安全性設定檔中的動作.....204
Objects > Security Profiles > Anti-Spyware Profile（Objects > Security Profiles > Antivirus（物件 > 安全性設定檔 > 防毒）.....207
Objects > Security Profiles > Anti-Spyware Profile（物件 > 安全性設定檔 > 反間諜軟體設定檔）.....210
Objects > Security Profiles > Vulnerability Protection（物件 > 安全性設定檔 > 漏洞保護）.....214
Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）.....218
URL 篩選一般設定.....218
URL 篩選類別.....219
URL 篩選設定.....221
使用者認證偵測.....222
HTTP 標頭插入.....223
URL 篩選內嵌 ML.....224
Objects > Security Profiles > File Blocking（物件 > 安全性設定檔 > 檔案封鎖）.....226
Objects > Security Profiles > WildFire Analysis（物件 > 安全性設定檔 > WildFire 分析）.....228
Objects > Security Profiles > Data Filtering（物件 > 安全性設定檔 > 資料篩選）.....230
Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）.....232
Objects > Security Profiles > Mobile Network Protection（物件 > 安全性設定檔 > 行動網路保護）.....235
Objects > Security Profiles > SCTP Protection（物件 > 安全性設定檔 > SCTP 保護）.....240
Objects > Security Profile Groups（物件 > 安全性設定檔群組）.....245
Objects > Log Forwarding（物件 > 日誌轉送）.....246
Objects > Authentication（物件 > 驗證）.....249
物件 > 解密設定檔.....251
解密設定檔一般設定.....251
用以控制已解密流量的設定.....252
用以控制未解密流量的設定.....256
用以控制已解密 SSH 流量的設定.....256
Objects > Decryption > Forwarding Profile（物件>解密>轉送設定檔）.....258
Objects > SD-WAN Link Management（物件 > SD-WAN 連結管理）.....260
Objects > SD-WAN Link Management > Path Quality Profile（物件 > SD-WAN 連結管理 > 路徑品質設定檔）.....260
Objects > SD-WAN Link Management > SaaS Quality Profile（物件 > SD-WAN 連結管理 > SaaS 品質設定檔）.....261
Objects > SD-WAN Link Management > Traffic Distribution-Profile（物件 > SD-WAN 連結管理 > 流量散佈-設定檔）.....262
Objects > SD-WAN Link Management > Error Correction Profile（物件 > SD-WAN 連結管理 > 錯誤連線設定檔）.....263
Objects > Schedules（物件 > 排程）.....265

網路.....267
網路 > 介面.....268
防火牆介面概要.....268
防火牆介面通用建置組塊.....269
PA-7000 Series 防火牆介面通用建置組塊.....270
旁接介面.....271
HA 介面.....271
Virtual Wire 介面.....272
Virtual Wire 子介面.....273

PA-7000 Series 第二層介面 274
PA-7000 Series 第二層子介面 275
PA-7000 Series 第三層介面 275
第三層介面 283
第三層子介面 292
日誌卡介面 299
日誌卡子介面 300
解密鏡像介面 301
彙總乙太網路 (AE) 介面群組 301
彙總乙太網路 (AE) 介面 304
Network > Interfaces > VLAN (網路 > 介面 > VLAN) 308
Network > Interfaces > Loopback (網路 > 介面 > 回送) 315
Network > Interfaces > Tunnel (網路 > 介面 > 通道) 317
Network > Interfaces > SD-WAN (網路 > 介面 > SD-WAN) 319
Network > Zones (網路 > 區域) 320
安全性區域概要 320
安全性區域的建置組塊 320
Network > VLANs (網路 > VLAN) 323
Network > Virtual Wires (網路 > Virtual Wire) 324
Network > Virtual Routers (網路 > 虛擬路由器) 325
虛擬路由器的一般設定 325
靜態路由 326
路由重新散佈 328
RIP 329
OSPF 331
OSPFv3 335
BGP 340
IP 多點傳送 351
ECMP 354
更多的虛擬路由器執行階段統計資料 356
邏輯路由器的更多執行階段統計資料 365
Network > Routing > Logical Routers (網路 > 路由 > 邏輯路由器) 370
邏輯路由器的一般設定 370
邏輯路由器的靜態路由 372
邏輯路由器的 BGP 路由 373
Network > Routing > Routing Profiles > BGP (網路 > 路由 > 路由設定檔 > BGP) 376
網路 > IPSec 通道 379
IPSec VPN 通道管理 379
IPSec 通道一般頁籤 379
IPSec 通道 Proxy ID 頁籤 381
防火牆的 IPSec 通道狀態 382
IPSec 通道重新啟動或重新整理 382
網路 > GRE 通道 383
GRE 通道 383
Network > DHCP (網路 > DHCP) 385
DHCP 概要 385
DHCP 定址 385
DHCP 伺服器 386
DHCP 轉送 388
DHCP 用戶端 389
Network > DNS Proxy (網路 > DNS Proxy) 390
DNS Proxy 概要 390
DNS Proxy Settings (DNS Proxy 設定) 390

其他 DNS Proxy 動作 393
Network > QoS (網路 > QoS) 394
QoS 介面設定 394
QoS 介面統計資料 395
Network > LLDP (網路 > LLDP) 397
LLDP 概要 397
LLDP 的建置組塊 397
網路 > 網路設定檔 400
Network > 網路設定檔> GlobalProtect IPSec 加密 400
Network > Network Profiles > IKE Gateways (網路 > 網路設定檔 > IKE 閘道) 400
Network > Network Profiles > IPSec Crypto (網路 > 網路設定檔 > IPSec 加密) 406
Network > Network Profiles > IKE Crypto (網路 > 網路設定檔 > IKE 加密) 407
Network > Network Profiles > Monitor (網路 > 網路設定檔 > 監控) 408
Network > Network Profiles > Interface Mgmt (網路 > 網路設定檔 > 介面管理) 409
Network > Network Profiles > Zone Protection (網路 > 網路設定檔 > 區域保護) 410
網路 > 網路設定檔 > QoS 423
Network > Network Profiles > LLDP Profile (網路 > 網路設定檔 > LLDP 設定檔) 425
Network > Network Profiles > BFD Profile (網路 > 網路設定檔 > BFD 設定檔) 426
Network > Network Profiles > SD-WAN Interface Profile (網路 > 網路設定檔 > SD-WAN 介面設定檔) 428

裝置 431
Device > Setup (裝置 > 設定) 432
Device > Setup > Management (裝置 > 設定 > 管理) 433
Device > Setup > Operations (裝置 > 設定 > 操作) 453
啟用 SNMP 監控 458
Device > Setup > HSM (裝置 > 設定 > HSM) 460
硬體安全性模組提供者設定 460
HSM 驗證 461
硬體安全性操作 461
硬體安全性模組提供者組態和狀態 462
硬體安全性模組狀態 462
Device > Setup > Services (裝置 > 設定 > 服務) 464
設定全域和虛擬系統的服務 464
全域服務設定 464
服務路由組態的 IPv4 和 IPv6 支援 466
目的地服務路由 469
Device > Setup > Interfaces (裝置 > 設定 > 介面) 470
Device > Setup > Telemetry (裝置 > 設定 > 遙測) 473
Device > Setup > Content-ID (裝置 > 設定 > 內容 ID) 474
Device > Setup > WildFire (裝置 > 設定 > WildFire) 479
Device > Setup > Session (裝置 > 設定 > 工作階段) 482
工作階段設定 482
工作階段逾時 485
TCP 設定 487
解密設定：憑證撤銷檢查 489
解密設定：正向 Proxy 伺服器憑證設定 490
VPN 工作階段設定 491
Device > High Availability (裝置 > 高可用性) 492
設定 HA 的重要注意事項 492

HA 一般設定 493
HA 通訊 496
HA 連結和路徑監控 498
HA 主動/主動設定 500
叢集組態 502
裝置 > 日誌轉送卡 503
Device > Config Audit（裝置 > 組態稽核） 505
裝置 > 密碼設定檔 506
使用者名稱和密碼需求 506
Device > Administrators（裝置 > 管理員） 508
Device > Admin Roles（裝置 > 管理員角色） 510
Device > Access Domain（裝置 > 存取網域） 512
Device > Authentication Profile（裝置 > 驗證設定檔） 513
驗證設定檔 513
從驗證設定檔匯出的 SAML 元數據 518
Device > Authentication Sequence（裝置 > 驗證順序） 520
Device > Data Redistribution（裝置 > 資料重新散佈） 521
Device > Data Redistribution > Agents（裝置 > 資料重新散佈 > 代理程式） 521
Device > Data Redistribution > Clients（裝置 > 資料重新散佈 > 用戶端） 522
Device > Data Redistribution > Collector Settings（裝置 > 資料重新散佈 > 收集器設定） 522
Device > Data Redistribution > Include/Exclude Networks（裝置 > 資料重新散佈 > 包括/排除網路） 523
Device > Device Quarantine（裝置 > 裝置隔離） 524
裝置 > VM 資訊來源 525
為 VMware ESXi 和 vCenter 伺服器啟用 VM 資訊來源的設定 526
為 AWS VPC 啟用 VM 資訊來源的設定 527
為 Google 計算引擎啟用 VM 資訊來源的設定 528
裝置 > 疑難排解 530
安全性政策比對 530
QoS 政策比對 531
驗證政策比對 532
解密/SSL 政策比對 533
NAT 政策比對 534
基於原則的轉送政策比對 535
DoS 政策比對 536
路由 537
測試 Wildfire 538
Threat Vault 538
Ping 539
追蹤路由 540
日誌收集器連線 541
外部動態清單 542
更新伺服器 542
測試雲端記錄服務狀態 542
測試雲端 GP 服務狀態 543
Device > Virtual Systems（裝置 > 虛擬系統） 544
裝置 > 共用閘道 546
裝置 > 憑證管理 547
Device > Certificate Management > Certificates（裝置 > 憑證管理 > 憑證） 548
管理防火牆及 Panorama 憑證 548
管理預設受信任的憑證授權單位 552
Device > Certificate Management > Certificate Profile（裝置 > 憑證管理 > 憑證設定檔） 553

Device > Certificate Management > OCSP Responder（裝置 > 憑證管理 > OCSP 回應程式）.....555
Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔）.....556
Device > Certificate Management > SCEP（裝置 > 憑證管理 > SCEP）.....558
裝置 > 憑證管理 > SSL 解密排除.....561
Device > Certificate Management > SSH Service Profile（裝置 > 憑證管理 > SSL 服務設定檔）.....563
裝置 > 回應頁面.....565
Device > Log Settings（裝置 > 日誌設定）.....567
選取日誌轉送目的地.....567
定義警報設定.....569
清除記錄.....570
裝置 > 伺服器設定檔.....571
裝置 > 伺服器設定檔 > SNMP 設陷.....572
裝置 > 伺服器設定檔 > Syslog.....574
裝置 > 伺服器設定檔 > 電子郵件.....576
裝置 > 伺服器設定檔 > HTTP.....578
裝置 > 伺服器設定檔 > NetFlow.....581
Device > Server Profiles > RADIUS（裝置 > 伺服器設定檔 > RADIUS）.....582
Device > Server Profiles > TACACS+（裝置 > 伺服器設定檔 > TACACS+）.....584
Device > Server Profiles > LDAP（裝置 > 伺服器設定檔 > LDAP）.....585
Device > Server Profiles > Kerberos（裝置 > 伺服器設定檔 > Kerberos）.....587
Device > Server Profiles > SAML Identity Provider（裝置 > 伺服器設定檔 > SAML 識別提供者）.....588
裝置 > 伺服器設定檔 > DNS.....591
裝置 > 伺服器設定檔 > 多因素驗證.....592
裝置 > 本機使用者資料庫 > 使用者.....594
裝置 > 本機使用者資料庫 > 使用者群組.....595
裝置 > 已排程的日誌匯出.....596
Device > Software（裝置 > 軟體）.....597
Device > Dynamic Updates（裝置 > 動態更新）.....599
Device > Licenses（裝置 > 授權）.....602
裝置 > 支援.....603
Device > Master Key and Diagnostics（裝置 > 主要金鑰與診斷）.....604
部署主要金鑰.....605
Device > Policy Recommendation（裝置 > 政策建議）.....607

使用者識別機制.....609
Device > User Identification > User Mapping（裝置 > 使用者識別 > 使用者對應）.....610
Palo Alto Networks User-ID 代理程式設定.....610
監控伺服器.....616
包含或排除使用者對應的子網路.....619
Device > User Identification > Connection Security（裝置 > 使用者識別 > 連線安全性）.....620
Device > User Identification > Terminal Server Agents（裝置 > 使用者識別 > 終端機伺服器代理程式）.....621
Device > User Identification > Group Mapping Settings Tab（裝置 > 使用者識別 > 群組對應設定頁籤）.....622
Device > User Identification > Authentication Portal（裝置 > 使用者識別 > 驗證入口網站）.....626

GlobalProtect 629
Network > GlobalProtect > Portals (網路 > GlobalProtect > 入口網站) 630
GlobalProtect 入口網站一般頁籤 631
GlobalProtect 入口網站驗證組態頁籤 632
GlobalProtect 入口網站入口資料收集頁籤 634
GlobalProtect 入口網站代理程式頁籤 634
GlobalProtect 入口網站無用戶端 VPN 頁籤 651
GlobalProtect 入口網站衛星頁籤 653
Network > GlobalProtect > Gateways (網路 > GlobalProtect > 閘道) 656
GlobalProtect 閘道一般頁籤 656
GlobalProtect 閘道驗證頁籤 657
GlobalProtect 閘道代理程式頁籤 659
GlobalProtect 閘道衛星頁籤 667
Network > GlobalProtect > MDM (網路 > GlobalProtect > MDM) 670
Network > GlobalProtect > Device Block List (網路 > GlobalProtect > 裝置封鎖清單) 671
網路 > GlobalProtect > 無用戶端應用程式 672
網路 > GlobalProtect > 無用戶端應用程式群組 673
Objects > GlobalProtect > HIP Objects (物件 > GlobalProtect > HIP 物件) 674
HIP 物件一般頁籤 674
HIP 物件行動裝置頁籤 676
HIP 物件修補程式管理頁籤 677
HIP 物件防火牆頁籤 677
HIP 物件反惡意軟體頁籤 678
HIP 物件磁碟備份頁籤 678
HIP 物件磁碟加密頁籤 678
HIP 物件資料遺失防護頁籤 679
HIP 物件憑證頁籤 679
HIP 物件自訂檢查頁籤 680
Objects > GlobalProtect > HIP Profiles (物件 > GlobalProtect > HIP 設定檔) 681
Device > GlobalProtect Client (裝置 > GlobalProtect 用戶端) 683
管理 GlobalProtect 應用程式軟體 683
設定 GlobalProtect 應用程式 684
使用 GlobalProtect 應用程式 684

Panorama Web 介面 687
使用 Panorama Web 介面 688
內容切換 692
Panorama 提交作業 693
在 Panorama 上定義原則 700
傳統模式下 Panorama 虛擬裝置的日誌儲存分割區 702
Panorama > Setup > Interfaces (Panorama > 設定 > 介面) 703
Panorama > 高可用性 706
Panorama > 受管理的 WildFire 叢集 708
受管理的 WildFire 叢集工作 708
受管理的 WildFire 設備工作 709
受管理的 WildFire 資訊 710
受管理的 WildFire 叢集和裝置的管理 713
Panorama > 管理員 722
Panorama > Admin Roles (Panorama > 管理員角色) 724
Panorama > Access Domains (Panorama > 存取網域) 726
Panorama > Managed Devices > Summary (Panorama > 受管理的裝置 > 摘要) 727

受管理防火牆的管理 727
受管理防火牆資訊 728
防火牆軟體和內容更新 730
防火牆備份 731
Panorama > Device Quarantine（Panorama > 裝置隔離） 732
託管設備） > Health（健康狀態 733
Panorama 上的詳細裝置健康狀態 734
Panorama > 範本 738
範本 738
範本堆疊 738
Panorama > Templates > Template Variables（Panorama > 範本 > 範本變數） 739
Panorama > Device Groups（Panorama > 裝置群組） 742
Panorama > 受管理的收集器 744
日誌收集器資訊 744
日誌收集器組態 745
專用日誌收集器的軟體更新 752
Panorama > 收集器群組 754
收集器群組設定 754
收集器群組資訊 758
Panorama > Plugins（Panorama > 外掛程式） 759
Panorama > SD-WAN 760
SD-WAN 裝置 760
SD-WAN VPN 叢集 761
SD-WAN 監控 762
SD-WAN 報告 763
Panorama > VMware NSX 765
設定通知群組 765
建立服務定義 766
設定對 NSX Manager 的存取 766
建立導向規則 768
Panorama > 日誌擷取設定檔 769
Panorama > 日誌設定 770
Panorama > Server Profiles > SCP（Panorama > 伺服器設定檔 > SCP） 772
Panorama > 已排程的設定匯出 773
Panorama > 軟體 774
管理 Panorama 軟體更新 774
顯示 Panorama 軟體更新資訊 775
Panorama > 設備部署 776
管理軟體和內容更新 776
顯示軟體和內容更新資訊 778
排程動態內容更新 778
從 Panorama 復原內容版本 779
管理防火牆授權 780

Web 介面基本概念

下列主題提供防火牆的概要，並說明基本管理工作。

> 防火牆概要
> 功能與優點
> 上次登入時間和失敗的登入嘗試
> 當日訊息
> 工作管理員
> 語言
> 警示
> 認可變更
> 儲存候選組態
> 還原變更
> 鎖定組態
> 全域尋找
> 威脅詳細資訊
> AutoFocus 情報摘要

防火牆概要

Palo Alto Networks® 新世代防火牆會對所有流量（包含應用程式、威脅和內容）進行檢查，並且將該流量關聯到任何地點或任何裝置類型的使用者。使用者、應用程式和內容—企業運作的要素—成為企業安全性原則中不可或缺的要件。這可讓您依據企業原則調整安全措施，並編寫易於瞭解和維護的規則。

在 Security Operating Platform 中，我們的新世代防火牆能夠讓組織：

- 藉由將所有流量分類（無論連接埠如何），以安全的方式啟用應用程式（包括軟體即服務應用程式）、使用者和內容。
- 透過允許所有需要的應用程式並阻止其他所有應用程式，使用正面實施模型降低攻擊的風險。
- 運用安全性原則來阻止已知的漏洞入侵、病毒、勒索軟體、間諜軟體、殭屍網路和其他未知惡意軟體，例如進階持續性威脅。
- 透過細分資料和應用程式以及執行零信任原則來保護資料中心（包括虛擬化資料中心）。
- 在內部部署和雲端環境採用一致的安全性。
- 將 Security Operating Platform 擴展到各地的使用者和裝置，以獲得安全的行動運算能力。
- 獲得集中的可視性並簡化網路安全措施，促使資料變為可化為行動的資料，進而阻止網路攻擊得逞。
- 識別並防止試圖竊取認證的行為，方式為停止向非法網站提交有效的公司認證，並透過在網路層執行驗證原則，消除攻擊者使用被竊取認證進行橫向活動或危害網路的能力。

© 2019 Palo Alto Networks, Inc.

功能與優點

Palo Alto Networks 新一代的防火牆可對獲准存取網路的流量進行更精確的控制。主要功能與優點包括：

- 以應用程式為基礎的原則強化 **(App-ID™)**—當應用程式的識別不只是以通訊協定與埠號為基礎時，根據應用程式類型進行的存取控制將更為有效。App-ID 服務會封鎖高風險的應用程式，以及高風險的行為（例如檔案共用），系統也能夠解密與檢查以安全通訊端層 (SSL) 通訊協定加密的流量。
- 使用者識別 **(User-ID™)**—User-ID 功能允許管理員根據使用者和使用者群組（而不是根據網路區域或位址），設定並強制執行防火牆原則。或者，根據網路區域或位址與使用者和使用者群組，設定並強制執行防火牆原則。防火牆能夠與許多目錄伺服器進行通訊，例如 Microsoft Active Directory、eDirectory、SunOne、OpenLDAP 及大多數其他以 LDAP 為基礎的伺服器，將使用者及群組資訊提供給防火牆。接著您可以使用這些資訊來保護可按照各個使用者或群組定義的安全應用程式啟用。例如，管理員可允許一個組織使用 Web 式應用程式，但不允許公司中其他任何的組織使用該應用程式。您也可以按照使用者和群組，設定應用程式某些元件的精確控制（請參閱使用者識別）。
- 威脅防範—威脅防範服務可使網路免於病毒、蠕蟲、間諜軟體及其他惡意流量的威脅，並可在應用程式與流量來源之間做出區別（請參閱 [物件 > 安全性設定檔]））。
- **URL** 篩選—可以篩選對外連線，以防存取不適當的網站（請參閱 [物件 > 安全性設定檔 > URL 篩選]）。
- 流量可見度 — 大量報告、日誌與通知機制為網路應用程式流量及安全事件提供更詳細的可見度。Web 介面中的應用程式監測中心 (ACC) 可識別出流量最大及安全風險最高的應用程式（請參閱監控）。
- 網路的多功能性與速度 — Palo Alto Networks 防火牆可以增強或取代現有防火牆，並可透明安裝於任何網路中，或設定為支援使用交換器或路由器的環境。單通道平行處理架構為您提供這些流暢的服務速度，使網路延遲的影響降到最低程度。
- **GlobalProtect**—GlobalProtect™ 為現場使用的用戶端系統（例如筆記型電腦）提供安全性，可允許在全世界的任何地方輕鬆而安全地登入。
- 故障保護操作—高可用性 (HA) 支援在任何硬體或軟體發生故障的情況下提供自動故障保護的功能（請參閱 [裝置 > 虛擬系統]）。
- 惡意軟體的分析與報告—WildFire™ 雲端型分析服務可以針對通過防火牆的惡意軟體提供詳細的分析與報告。與 AutoFocus™ 威脅情報服務的整合可讓您評估與貴組織、企業和全域層級的網路流量相關聯的風險。
- **VM-Series** 防火牆—VM-Series 防火牆提供的 PAN-OS® 的虛擬實例適用於虛擬資料中心環境中，並適合私人、公共與混合型雲端運算環境。
- 管理及 **Panorama**—您可以透過直覺式 Web 介面或命令行介面 (CLI) 管理每個防火牆，或能透過 Panorama™ 中央管理系統集中管理所有的防火牆，此系統 Web 介面與 Palo Alto Networks 防火牆的 Web 介面相似。

© 2019 Palo Alto Networks, Inc.

上次登入時間和失敗的登入嘗試

為了偵測權限帳戶（例如 Palo Alto Networks 防火牆或 Panorama 上的管理員帳戶）的誤用情況及防止漏洞利用，Web 介面與命令行介面 (CLI) 會顯示您上次的登入時間及登入時所用使用者名稱的任何失敗登入嘗試。此資訊可讓您輕鬆識別某人是否使用您的管理員認證來發動攻擊。

您登入 Web 介面後，上次登入時間 資訊會出現在視窗左下方。如果自上次成功登入以來出現一次或多次失敗登入，小心圖示會出現在上次登入資訊的右側。將游標停在小心符號的上方可檢視失敗的登入嘗試數目，或按一下以檢視 **Failed Login Attempts Summary**（失敗的登入嘗試摘要）視窗，該視窗將列示管理帳戶名稱、來源 IP 位址及登入失敗原因。

如果您發現並非您本人的多次失敗登入嘗試，應當與網路管理員一起查找執行暴力密碼破解攻擊的系統，然後調查使用者及主機電腦，以失敗及清除任何惡意活動。如果您發現上次登入日期與時間指示帳戶入侵，您應當立即變更密碼，然後執行組態稽核，以確定是否提交可疑組態變更。如果您發現日誌被清除或難以確定使用您的帳戶做出的變更是否得當，則將組態還原至已知的適當組態。

© 2019 Palo Alto Networks, Inc.

當日訊息

如果您或其他管理員設定了當日訊息，或 Palo Alto Networks 內嵌訊息作為軟體或內容發行版本的一部分，則 [當日訊息] 對話方塊會在使用者登入 Web 介面時自動顯示。這可確保使用者看到會影響其打算執行之工作（例如即將重新啟動系統）的重要資訊。

對話方塊每頁顯示一條訊息。如果對話方塊包括選取 **Do not show again**（不要再顯示）的選項，您可對不想在後續登入時顯示此對話方塊的每條訊息選取該選項。

每當 *Message of the Day*（當日訊息）變更時，即時您在之前登入時選取了 *Do not show again*（不要再顯示），該訊息仍會出現在下一工作階段。您接著必須重新選取該選項，以避免在後續工作階段中看到該修改的訊息。

若要導覽對話方塊頁面，按一下對話方塊旁邊的右（ ）和左（ ）箭頭，或者按一下對話方塊底部的頁面選取器（ ）。您 **Close**（關閉）對話方塊後，按一下 Web 介面底部的（ ）訊息可手動重新開啟。

若要設定當日訊息，請選取 **Device**（設備）> **Setup**（設定）> **Management**（管理），然後編輯 橫幅和訊息 設定。

© 2019 Palo Alto Networks, Inc.

工作管理員

按一下 Web 介面底部的 **Tasks**（工作）可顯示您、其他管理員或 PAN-OS 自上次防火牆重新啟動以來啟動的工作（例如，手動認可或自動 FQDN 重新整理）。針對每個工作，工作管理員提供下表所述的資訊與動作。

部分欄依預設為隱藏。若要顯示或隱藏特定欄，請在任何欄標題中開啟下拉式清單，選取 *Columns*（欄），然後視需要選取（顯示）或清除（隱藏）欄名稱。

欄位/按鈕	說明
Q→×	若要篩選工作，請根據其中一個欄的值輸入文字字串，並套用篩選器（→）。例如，輸入 **edl** 將篩選清單以僅顯示 EDLFetch（擷取外部動態清單）工作。若要移除篩選，移除篩選器（×）。
類型	工作類型，例如日誌要求、授權重新整理或認可。若與工作相關的資訊（例如警告）太長而無法放入訊息欄中，您可按一下類型值以檢視所有詳細資訊。
STATUS (狀態)	指出工作是擱置（例如具備已排入佇列狀態的認可）、進行中（例如按主動狀態的日誌要求）、已完成或失敗。對於正在進行的提交，狀態將指示完成百分比。
工作 ID	識別工作的號碼。從 CLI 中，您可以使用工作 ID 以查看關於工作的其他詳細資訊。例如，您可以輸入下列項目，以查看認可佇列中認可工作的位置： `> show jobs id <job-id>` 依預設會隱藏此欄。
結束時間	工作結束的日期與時間。依預設會隱藏此欄。
開始時間	工作開始的日期與時間。對於認可工作，開始時間會指出認可新增至認可佇列的時間。
訊息	顯示工作的詳細資訊。如果項目指出「太多訊息」，您可按一下工作類型來查看訊息。 對於認可工作，訊息包含取消佇列的時間，以指出 PAN-OS 開始執行認可的時間。如需查看管理員為提交輸入的說明，請按一下 **Commit** 說明（提交說明）。如需詳細資訊，請參閱認可變更。
動作	按一下 **x** 以取消由管理員或 PAN-OS 啟動的擱置中認可。此按鈕僅適用於管理員，且該管理員須具有下列預先定義的角色之一：超級使用者、設備管理員、虛擬系統管理員或 Panorama 管理員。
顯示	選取您要顯示的工作。 • **All Tasks**（所有工作）（預設值）

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	• 特定類型的 **All**（所有）工作（**Jobs**（工作）、**Reports**（報告）或 **Log Requests**（日誌要求）） • 所有 **Running**（執行中）工作（進行中） • 所有特定類型的 **Running**（執行中）工作（**Jobs**（工作）、**Reports**（報告）或 **Log Requests**（日誌要求）） • （僅限 Panorama）使用第二個下拉式清單以顯示 **Panorama**（預設值）或特定受管理防火牆的工作。
清除提交佇列	取消由管理員或 PAN-OS 啟動的擱置中認可。此按鈕僅適用於管理員，且該管理員須具有下列預先定義的角色之一：超級使用者、設備管理員、虛擬系統管理員或 Panorama 管理員。

© 2019 Palo Alto Networks, Inc.

語言

依預設，您登入防火牆之電腦的語言設定將決定管理網路介面上顯示的語言。若要手動變更語言，請按一下 **Language**（語言）（網路介面右下方），並從下拉式清單中選取所需語言，然後按一下 **OK**（確定）。網路介面將以選取的語言更新並顯示。

支援的語言包括：法文、日文、西班牙文、簡體中文與繁體中文。

© 2019 Palo Alto Networks, Inc.

警示

警報是防火牆產生的訊息，可指出特定類型的事件數目（例如，加密與解密失敗）已超過為該事件類型設定的閾值（請參閱定義警報設定）。產生警報時，防火牆會建立警報日誌，並開啟 [系統警報] 對話方塊以顯示警報。關閉對話方塊後，您可以隨時按一下 Web 介面底部的 **Alarms**（警報）（

），以重新開啟對話方塊。若要防止防火牆自動開啟特定警報對話方塊，請選取 [未確認警報]，然後按一下 **Acknowledge**（確認）以將警報移至已確認警報清單。

© 2019 Palo Alto Networks, Inc.

認可變更

按一下 Web 介面右上方的 **Commit**（認可），並為防火牆設定擱置中的變更指定相關作業：commit (activate)（認可（啟動））、validate（驗證）或 preview（預覽）。您可以依據管理員或位置來篩選擱置中的變更，然後僅對這些變更進行預覽、驗證和認可。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。

防火牆佇列將提交要求，以便您在之前的提交正在進行中時，啟動新的提交。防火牆會依其啟動順序執行認可，但優先處理防火牆所啟動的自動認可（例如 FQDN 重新整理）。不過，如果佇列中由管理員啟動的認可已達數目上限，則必須等候防火牆完成擱置中認可的處理，才能啟動新的認可。

使用工作管理員可取消認可，或檢視關於擱置中、進行中、已完成或失敗認可的詳細資訊。

[認可] 對話方塊會顯示下表中所述的選項。

欄位/按鈕	說明
認可所有變更	認可您具有管理權限的所有變更（預設值）。選取此選項時，您將無法手動篩選防火牆所認可的組態變更範圍。反之，指派給您用於登入之帳戶的管理員角色會決定認可範圍： • 超級使用者角色—防火牆會認可所有管理員的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限會決定認可範圍（請參閱 [裝置 > 管理員角色]）。若設定檔包含 **Commit For Other Admins**（為其他管理員認可）的權限，則防火牆會認可任何和所有管理員所設定的變更。若管理員角色設定檔不包含 **Commit For Other Admins**（為其他管理員認可）的權限，則防火牆只會認可您的變更，而不會認可其他管理員的變更。 如果您已實作存取網域，防火牆將會自動套用這些網域，以篩選認可範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色為何，防火牆都只會認可指派給您帳戶的存取網域中產生的組態變更。
依做成者認可變更	篩選防火牆所認可的組態變更範圍。指派給您用來登入之帳戶的管理員角色，會決定您的篩選選項： • 超級使用者角色—您可將認可範圍限制到特定管理員做出的變更，和特定位置中的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限，會決定您的篩選選項（請參閱 [裝置 > 管理員角色]）。若設定檔包含 **Commit For Other Admins**（為其他管理員認可）的權限，則您可將認可範圍限制到特定管理員設定的變更，和特定位置中的變更。若您的管理員角色設定檔不包含 **Commit For Other Admins**（為其他管理員認可）的權限，則只能將認可範圍限制到您在特定位置中所做的變更。 篩選認可範圍，如下所示： • 依管理員篩選—即便您的角色允許認可其他管理員的變更，認可範圍依預設仍僅包含您的變更。若要將其他管理員新增至認可範圍，請按一下 **<usernames>**（使用者名稱）連結、選取管理員，然後按一下 **OK**（確定）。 • 依位置篩選—選取特定位置以將變更包含在認可中。 如果您已實作存取網域，防火牆將會根據這些網域自動篩選認可範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色和篩選選取為何，認可範圍都只會包含指派給您帳戶之存取網域中的組態變更。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	載入組態（裝置 > 設定 > 操作（Device > Setup > Operations））後，您必須 *Commit All Changes*（認可所有變更）。 認可虛擬系統的變更時，必須包含對該虛擬機器中的相同規則庫新增、刪除或重新定位了規則的所有管理員所做的變更。
認可範圍	列出有變更待認可的位置。清單是否包含所有變更或變更中的子集取決於若干因素，如針對認可所有變更和依做成者認可變更所述。位置可以是下列任一項： • **shared-object**（共用物件）—在共用位置中定義的設定。 • **policy-and-objects**（原則和物件）—在沒有多重虛擬系統的防火牆上定義的原則規則或物件。 • **device-and-network**（裝置和網路）—全域而並非特定於某虛擬系統的網路和裝置設定（例如介面管理設定檔）。這也適用於沒有多重虛擬系統之防火牆上的網路和裝置設定。 • **<virtual-system>**—在具有多重虛擬系統的防火牆上定義原則規則或物件的虛擬系統名稱。這也包含特定於某虛擬系統（例如區域）的網路和裝置設定。
Location Type（位置類型）	此欄分類擱置中變更的位置： • **Virtual Systems**（虛擬系統）—特定虛擬系統中定義的設定。 • **Other Changes**（其他變更）—非特定於某虛擬系統（例如共用物件）的設定。
包含在認可中 （僅限部分認可）	可讓您選取要認可的變更。依預設會選取 **Commit Scope**（認可範圍）內的所有變更。此欄僅會在您選取 **Commit Changes Made By**（依做成者認可變更）並選取特定管理員之後顯示。 可能有相依性會影響您包含在認可中的變更。例如，如果在您新增某物件後，有另一個管理員編輯了該物件，您就無法僅認可該名管理員的變更，而不認可您自己的變更。
依位置類型分組	依 **Location Type**（位置類型）將 **Commit Scope**（認可範圍）中的組態變更清單分組。
預覽變更	可讓您比較在 **Commit Scope**（認可範圍）中選取的組態與執行中的組態。預覽視窗會以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。 為方便比對 Web 介面區段的變更，您可以設定在每次變更前後顯示 **Lines of Context**（內容行）的預覽視窗。這些內容行來自於您所比較的候選組態與執行中組態的檔案。 預覽結果會顯示在新的瀏覽器視窗中，因此您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參考瀏覽器文件，以取得允許快顯視窗的步驟。
變更摘要	列出要認可變更的個別設定。**Change Summary**（變更摘要）清單會顯示各個設定的下列資訊：

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	• **Object Name**（物件名稱）—可識別原則、物件、網路設定或裝置設定的名稱。 • **Type**（類型）—設定的類型（例如位址、安全性規則或區域）。 • **Location Type**（位置類型）—指出設定是否定義於 **Virtual Systems**（虛擬系統）中。 • **Location**（位置）—定義設定之虛擬系統的名稱。對於非特定於某虛擬系統的設定，此欄會顯示 **Shared**（共用）。 • **Operations**（操作）—指出自上次認可以來對設定執行的每個操作（建立、編輯或刪除）。 • **Owner**（擁有者）—上次對設定進行變更的管理員。 • **Will Be Committed**（將受認可）—指出認可目前是否包含設定。 • **Previous Owners**（先前的擁有者）—在上次變更前對設定進行變更的管理員。 您可以選取性地以欄名稱（例如 **Type**（類型））作為 **Group By**（分組依據）。 選取變更清單中的物件以檢視 **Object Level Difference**（物件層次差異）。
驗證提交	驗證防火牆設定的語法是否正確，以及語意是否完整。輸出會包含認可所將顯示的相同錯誤和警告，包括規則鏡像處理和應用程式相依性警告。驗證程序可讓您在認可前找出錯誤並加以修正（此程序並不會變更執行中的組態）。如果您使用固定認可視窗，而想要確定認可將成功而不發生錯誤，驗證程序將有所幫助。
說明	可讓您輸入說明（最多 512 個字元），以協助其他管理員了解您所做的變更。 認可事件的系統日誌將會截斷超過 *512* 個字元的說明。
提交	開始認可，或在有其他認可擱置的情況下，將您的認可新增至認可佇列。
認可狀態	在認可期間提供進度，然後在認可之後提供結果。認可結果包括成功或失敗、認可變更的詳細資訊以及認可警告。警告包括： • **Commit**（認可）—列出一般確認警告。 • **App Dependency**（應用程式依賴項）—列出現有規則需要的任何應用程式依賴項。 • **Rule Shadow**（規則陰影）—列出任何陰影規則。

© 2019 Palo Alto Networks, Inc.

儲存候選組態

選取防火牆或 Panorama Web 介面右上方的 **Config**（設定）> **Save Changes**（儲存變更）以儲存候選組態的新快照檔案或取代現有的組態檔案。如果在您認可變更之前重新啟動防火牆或 Panorama，則可將候選組態還原為儲存的快照，以還原上次認可後做出的變更。若要還原為快照，選取 **Device**（裝置）> **Setup**（設定）> **Operations**（操作）並 **Load named configuration snapshot**（載入具名組態快照）。如果您在重新啟動後未還原至快照，則候選設定會與上次認可的設定（執行中設定）相同。

您可根據管理員或位置篩選要儲存的組態變更。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。

您應定期儲存變更，如此若防火牆或 *Panorama* 重新啟動您就不會遺失變更。

儲存您對候選組態做出的變更不會啟動這些變更；您必須認可變更才能啟動這些變更。

[儲存變更] 對話方塊會顯示下表中所述的選項：

欄位/按鈕	說明
儲存所有變更	儲存所有您有管理權限的變更（預設值）。當您選取此選項時，您無法手動篩選防火牆儲存的組態變更範圍。反之，指派給您用於登入之帳戶的管理員角色會決定儲存範圍： • 超級使用者角色—防火牆會儲存所有管理員的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限會決定儲存範圍（請參閱 [裝置 > 管理員角色]）。若設定檔包含 **Save For Other Admins**（為其他管理員儲存）的權限，則防火牆會儲存由任何管理員設定的變更。若您的管理員角色設定檔不包含 **Save For Other Admins**（為其他管理員儲存）的權限，則防火牆只會儲存您的變更，而不會儲存其他管理員的變更。 如果您已實作存取網域，防火牆將會自動套用這些網域，以篩選儲存範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色為何，防火牆都只會儲存指派給您帳戶的存取網域中產生的組態變更。
依做成者儲存變更	篩選防火牆所儲存的組態變更範圍。指派給您用來登入之帳戶的管理員角色，會決定您的篩選選項： • 超級使用者角色—您可將儲存範圍限制到特定管理員做成的變更，和特定位置中的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限，會決定您的篩選選項（請參閱 [裝置 > 管理員角色]）。如果設定檔包含 **Save For Other Admins**（為其他管理員儲存）的權限，則您可將儲存範圍限制到特定管理員所設定的變更，以及特定位置中的變更。若您的管理員角色設定檔不包含 **Save For Other Admins**（為其他管理員儲存）的權限，則只能將儲存範圍限制到您在特定位置中所做的變更。 篩選儲存範圍，如下所示： • 依管理員篩選—即便您的角色允許儲存其他管理員的變更，儲存範圍依預設仍僅包含您的變更。若要將其他管理員新增至儲存範圍，請按一

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	下 **usernames**（使用者名稱）連結、選取管理員，然後按一下 **OK**（確定）。 • 依位置篩選—選取特定位置以將變更包含在儲存中。 如果您已實作存取網域，防火牆將會根據這些網域自動篩選儲存範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色和篩選選取為何，儲存範圍都只會包含指派給您帳戶之存取網域中的組態變更。
儲存範圍	列出有變更待儲存的位置。清單是否包含所有變更或變更中的子集取決於若干因素，如針對儲存所有變更和依做成者儲存變更選項所述。位置可以是下列任一項： • **shared-object**（共用物件）—在共用位置中定義的設定。 • **policy-and-objects**（原則和物件）—（僅限防火牆）在沒有多重虛擬系統的防火牆上定義的原則規則或物件。 • **device-and-network**（裝置和網路）—（僅限防火牆）全域而並非特定於某虛擬系統的網路和裝置設定（例如介面管理設定檔）。 • **virtual-system**（虛擬系統）—（僅限防火牆）在具有多重虛擬系統的防火牆上定義原則規則或物件的虛擬系統名稱。這也包含特定於某虛擬系統（例如區域）的網路和裝置設定。 • **device-group**（裝置群組）—（僅限 Panorama）會在其中定義原則規則或物件的裝置群組名稱。 • **template**（範本）—（僅限 Panorama）會在其中定義設定的範本或範本堆疊名稱。 • **log-collector-group**（日誌收集器群組）—（僅限 Panorama）會在其中定義設定的收集器群組名稱。 • **log-collector**（日誌收集器）—（僅限 Panorama）會在其中定義設定的日誌收集器名稱。
Location Type (位置類型)	此欄分類做成變更的位置： • **Virtual Systems**（虛擬系統）—（僅限防火牆）特定虛擬系統中定義的設定。 • **Device Groups**（裝置群組）—（僅限 Panorama）特定裝置群組中定義的設定。 • **Templates**（範本）—（僅限 Panorama）特定範本或範本堆疊中定義的設定。 • **Collector Groups**（收集器群組）—（僅限 Panorama）特定於收集器群組組態的設定。
包含在儲存中 （僅限部分儲存）	可讓您選取要儲存的變更。依預設會選取 **Save Scope**（儲存範圍）內的所有變更。此欄僅會在您選取 **Save Changes Made By**（依做成者儲存變更）並選取特定管理員之後顯示。 可能有相依性會影響您包含在儲存中的變更。例如，如果在您新增某物件後，有另一個管理員編輯了該物件，您就無法僅儲存該名管理員的變更，而不儲存您自己的變更。
依位置類型分組	依 **Location Type**（位置類型）將 **Save Scope**（儲存範圍）中的組態變更清單分組。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
預覽變更	可讓您比較在 **Save Scope**（儲存範圍）中選取的組態與執行中的組態。預覽視窗會以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。 為方便比對 Web 介面區段的變更，您可以設定在每次變更前後顯示 **Lines of Context**（內容行）的預覽視窗。這些內容行來自於您所比較的候選組態與執行中組態的檔案。 由於預覽結果顯示在新視窗中，您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參閱瀏覽器文件，瞭解如何解除封鎖快顯視窗的步驟。
變更摘要	列出要儲存變更的個別設定。**Change Summary**（變更摘要）清單會顯示各個設定的下列資訊： • **Object Name**（物件名稱）—可識別原則、物件、網路設定或裝置設定的名稱。 • **Type**（類型）—設定的類型（例如位址、安全性規則或區域）。 • **Location Type**（位置類型）—指出設定是否定義於 **Virtual Systems**（虛擬系統）中。 • **Location**（位置）—定義設定之虛擬系統的名稱。對於非特定於某虛擬系統的設定，此欄會顯示 **Shared**（共用）。 • **Operations**（操作）—指出自上次認可以來對設定執行的每個操作（建立、編輯或刪除）。 • **Owner**（擁有者）—上次對設定進行變更的管理員。 • **Will Be Saved**（將儲存）—指出儲存操作是否將包含設定。 • **Previous Owners**（先前的擁有者）—在上次變更前對設定進行變更的管理員。 您可以選取性地以欄名稱（例如 **Type**（類型））作為 **Group By**（分組依據）。
Save	將選取的變更儲存至組態快照檔案： • 若您選取 **Save All Changes**（儲存所有變更），防火牆會取代預設組態快照檔案 (.snapshot.xml)。 • 若您選取 **Save Changes Made By**（依做成者儲存變更），請指定新的或現有的組態檔案 **Name**（名稱），並按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

還原變更

選取防火牆或 Panorama Web 介面右上方的 **Config**（設定）> **Revert Changes**（還原變更）以復原自上次認可以來對候選組態所進行的變更。還原變更會將設定還原至執行中組態的值。您可根據管理員或位置篩選要復原的組態變更。位置可以是特定的虛擬系統、共用的原則和物件，或共用的裝置和網路設定。

防火牆或 Panorama 結束處理所有擱置中或正在進行的認可之後，您才能還原變更。您啟動還原程序後，防火牆或 Panorama 會自動鎖定候選和執行中組態，以使其他管理員無法編輯設定或認可變更。完成還原程序後，防火牆或 Panorama 會自動移除鎖定。

[還原變更] 對話方塊會顯示下表中所述的選項：

欄位/按鈕	說明
還原所有變更	還原所有您具有管理權限的變更（預設值）。當您選取此選項時，您無法手動篩選防火牆還原的組態變更範圍。反之，指派給您用於登入之帳戶的管理員角色會決定還原範圍： • 超級使用者角色—防火牆會還原所有管理員的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限會決定還原範圍（請參閱 [裝置 > 管理員角色]）。如果設定檔包含 **Commit For Other Admins**（為其他管理員認可）的權限，則防火牆會還原任何和所有管理員所設定的變更。如果管理員角色設定檔未包含 **Commit For Other Admins**（為其他管理員認可）的權限，則防火牆只會還原您的變更，而不會還原其他管理員的變更。 管理員角色設定檔中，認可的權限也適用於還原。 如果您已實作存取網域，防火牆將會自動套用這些網域，以篩選還原範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色為何，防火牆都只會還原指派給您帳戶的存取網域中產生的組態變更。
依做成者還原變更	篩選防火牆會還原的組態變更範圍。指派給您用來登入之帳戶的管理員角色，會決定您的篩選選項： • 超級使用者角色—您可將還原範圍限制到特定管理員做成的變更，和特定位置中的變更。 • 自訂角色—指派給帳戶的管理員角色設定檔的權限，會決定您的篩選選項（請參閱 [裝置 > 管理員角色]）。若設定檔包含 **Commit For Other Admins**（為其他管理員認可）的權限，則您可將將還原範圍限制到特定管理員設定的變更，和特定位置中的變更。若您的管理員角色設定檔不包含 **Commit For Other Admins**（為其他管理員認可）的權限，則只能將還原範圍限制到您在特定位置中所做的變更。 篩選還原範圍，如下所示： • 依管理員篩選—即便您的角色允許還原其他管理員的變更，還原範圍依預設仍僅包含您的變更。若要將其他管理員新增至復原範圍，請按一下 **<usernames>**（使用者名稱）連結、選取管理員，然後按一下 **OK**（確定）。 • 依位置篩選—選取特定位置以將變更包含在還原中。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	如果您已實作存取網域，防火牆將會根據這些網域自動篩選還原範圍（請參閱 [裝置 > 存取網域]）。無論您的管理角色和篩選選項為何，還原範圍都只會包含指派給您帳戶之存取網域中的組態變更。
還原範圍	列出有變更待還原的位置。清單是否包含所有變更或變更中的子集取決於若干因素，如針對還原所有變更和依做成者還原變更選項所述。位置可以是下列任一項： • **shared-object**（共用物件）—在共用位置中定義的設定。 • **policy-and-objects**（原則和物件）—（僅限防火牆）在沒有多重虛擬系統的防火牆上定義的原則規則或物件。 • **device-and-network**（裝置和網路）—（僅限防火牆）全域而並非特定於某虛擬系統的網路和裝置設定（例如介面管理設定檔）。 • **virtual-system**（虛擬系統）—（僅限防火牆）在具有多重虛擬系統的防火牆上定義原則規則或物件的虛擬系統名稱。這也包含特定於某虛擬系統（例如區域）的網路和裝置設定。 • **device-group**（裝置群組）—（僅限 Panorama）會在其中定義原則規則或物件的裝置群組名稱。 • **template**（範本）—（僅限 Panorama）會在其中定義設定的範本或範本堆疊名稱。 • **log-collector-group**（日誌收集器群組）—（僅限 Panorama）會在其中定義設定的收集器群組名稱。 • **log-collector**（日誌收集器）—（僅限 Panorama）會在其中定義設定的日誌收集器名稱。
Location Type (位置類型)	此欄分類做成變更的位置： • **Virtual Systems**（虛擬系統）—（僅限防火牆）特定虛擬系統中定義的設定。 • **Device Group**（裝置群組）—（僅限 Panorama）特定裝置群組中定義的設定。 • **Template**（範本）—（僅限 Panorama）特定範本或範本堆疊中定義的設定。 • **Log Collector Group**（日誌收集器群組）—（僅限 Panorama）特定於收集器群組組態的設定。 • **Log Collector**（日誌收集器）—（僅限 Panorama）特定於日誌收集器組態的設定。 • **Other Changes**（其他變更）—非特定於任何之前組態區域（例如共用物件）的設定。
包含在還原中 （僅限部分還原）	可讓您選取要還原的變更。依預設會選取 **Revert Scope**（還原範圍）內的所有變更。此欄僅會在您選取 **Commit Changes Made By**（依做成者還原變更）並選取特定管理員之後顯示。 可能有相依性會影響您包含在復原中的變更。例如，如果在您新增某物件後，有另一個管理員編輯了該物件，您就無法僅還原您自己的變更，而不還原該名管理員的變更。
依位置類型分組	依 **Location Type**（位置類型）列出在 **Revert Scope**（還原範圍）中的組態變更。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
預覽變更	可讓您比較在 **Revert Scope**（還原範圍）中選取的組態與執行中的組態。預覽視窗會以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。 為方便比對 Web 介面區段的變更，您可以設定在每次變更前後顯示 **Lines of Context**（內容行）的預覽視窗。這些內容行來自於您所比較的候選組態與執行中組態的檔案。 由於預覽結果顯示在新視窗中，您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參閱瀏覽器文件，瞭解如何解除封鎖快顯視窗的步驟。
變更摘要	列出要還原變更的個別設定。**Change Summary**（變更摘要）清單會顯示各個設定的下列資訊： • **Object Name**（物件名稱）—可識別原則、物件、網路設定或裝置設定的名稱。 • **Type**（類型）—設定的類型（例如位址、安全性規則或區域）。 • **Location Type**（位置類型）—指出設定是否定義於 **Virtual Systems**（虛擬系統）中。 • **Location**（位置）—定義設定之虛擬系統的名稱。對於非特定於某虛擬系統的設定，此欄會顯示 **Shared**（共用）。 • **Operations**（操作）—指出自上次認可以來對設定執行的每個操作（建立、編輯或刪除）。 • **Owner**（擁有者）—上次對設定進行變更的管理員。 • **Will Be Reverted**（將還原）—指示還原操作是否將包含設定。 • **Previous Owners**（先前的擁有者）—在上次變更前對設定進行變更的管理員。 您可以選取性地以欄名稱（例如 **Type**（類型））作為 **Group By**（分組依據）。
還原	還原選取的變更。

© 2019 Palo Alto Networks, Inc.

鎖定組態

為了在並行登入工作階段期間協助讓您與其他防火牆管理員相互配合地進行設定工作，Web 介面可讓您套用設定或認可鎖定，讓其他管理員無法在鎖定遭到移除前變更設定或認可鎖定。

在 Web 介面右上方，鎖定的掛鎖 ( ) 表示已設定一個或多個鎖（括號內為鎖定數）；未鎖定的掛鎖 ( ) 表示未設定任何鎖。按一下掛鎖即可開啟鎖定對話方塊，提供下列選項與欄位。

若要將防火牆設定為在管理員變更候選設定時自動設定認可鎖，請選取 *Device*（設備）> *Setup*（設定）> *Management*（管理），編輯一般設置，啟用 *Automatically Acquire Commit Lock*（自動擷取認可鎖定），然後按一下 *OK*（確定）並 *Commit*（認可）。

當您還原變更時（*Config*（設定）> *Revert Changes*（還原變更）），防火牆會自動鎖定候選設定和執行中的設定，讓其他管理員無法編輯設定或認可變更。在還原程序完成後，防火牆會自動移除鎖定。

欄位/按鈕	說明
admin (管理員)	設定鎖定之管理員的使用者名稱。
位置	在擁有多個虛擬系統 (vsys) 的防火牆上，鎖定範圍可以是特定 vsys 或共用位置。
類型	鎖定類型可以是： • 設定鎖定—封鎖其他管理員對候選設定進行變更。只有設定鎖定的超級使用者或管理員可將其移除。 • 認可鎖定—封鎖其他管理員，不讓其認可對候選設定所進行的變更。提交佇列不接受新提交，直至所有鎖定釋放。此鎖定可防止在兩個管理員正同時進行變更，且第一個管理員在第二個管理員完成之前完成並提交變更時發生衝突。若管理員設定鎖定，在完成提交後，防火牆會自動移除鎖定。設定鎖定的超級使用者或管理員也可將其手動移除。
備註	請輸入最多 256 個字元的文字。這對於想知道鎖定原因的其他管理員非常實用。
建立於	管理員設定鎖定的日期與事件。
已登入	表示設定鎖定的管理員目前是否已登入。
鎖定	若要設定鎖定，按一下 **Take a Lock**（選取鎖定），選取 **Type**（類型），選取 **Location**（位置）（僅限多個虛擬系統防火牆），輸入選用 **Comments**（註解），按一下 **OK**（確定），然後按一下 **Close**（關閉）。
移除鎖定	若要釋放鎖定，選取鎖定，**Remove Lock**（移除鎖定），按一下 **OK**（確定），然後按一下 **Close**（關閉）。

© 2019 Palo Alto Networks, Inc.

全域尋找

全域尋找可搜尋防火牆或 Panorama 的候選組態中是否有特定的字串，例如 IP 位址、物件名稱、原則名稱、威脅 ID、規則 UUID 或應用程名稱。搜尋結果會依類別分組，並提供連結可連至 Web 介面中的組態位置，讓您可以輕鬆找到所有存在或參照字串的位置。

若要啟動全域尋找，請按一下 Web 介面右上角的 **Search**（搜尋）圖示 。您可以在所有 Web 介面頁面和位置使用全域尋找。以下是可幫助您執行成功搜尋的全域尋找功能清單：

- 如果您在已啟用多個虛擬系統的防火牆上啟動搜尋，或如果已定義管理角色，全域尋找將只針對您具備其存取權限的防火牆區域傳回結果。Panorama 裝置群組也是如此；您只會看見您具備其管理權限之裝置群組的搜尋結果。
- 搜尋文字中的空格會以 AND 運算來處理。例如，如果您搜尋 `corp policy`，則組態項目中必須同時有 **corp** 和 **policy** 才會納入搜尋結果中。
- 若要尋找完全相同的字詞，請字詞前後加上引號。
- 若要重新執行先前執行過的搜尋，請按一下 [全域尋找]，系統隨即會顯示最近 20 次搜尋的清單。按一下清單中的任何項目便可再次執行該搜尋。每個管理帳戶都有獨一無二的搜尋歷程清單。

每一個可搜尋的欄位都可進行全域尋找。例如在安全性原則中，您可以搜尋下列欄位：名稱、頁籤、區域、位址、使用者、HIP 設定檔、應用程式、UUID 及服務。若要執行搜尋，請按一下上述任一欄位旁的下拉式清單，然後按一下 **Global Find**（全域尋找）。例如，如果您在名為 l3-vlan-trust 的區域上按一下 **Global Find**（全域尋找），則全域尋找功能會在整個組態中搜尋該區域名稱，並針對每個參照該區域的位置傳回結果。搜尋結果會依類別分組，將游標停留在任何項目上即可檢視詳細資料，或是按一下項目也可以瀏覽至該頁面的組態頁面。

全域尋找不會搜尋防火牆配置給使用者的動態內容（例如日誌、位址範圍或個別的 DHPC 位址）。若為 DHCP，您可以搜尋 DHCP 伺服器屬性，例如 DNS 項目，但您無法搜尋簽發給使用者的個別位址。另一個範例是您在啟用 User-ID™ 功能時，防火牆所收集的使用者名稱。在此狀況下，User-ID 資料庫中存在的使用者名稱或使用者群組只有在設定中也有該名稱或群組時（例如當政策中定義了使用者群組名稱時）才可搜尋。一般而言，您只能搜尋防火牆寫入組態的內容。

想知道更多？

深入了解如何使用全域尋找來搜尋防火牆或 Panorama 組態。

© 2019 Palo Alto Networks, Inc.

威脅詳細資訊

- 監控 > 日誌 > 威脅
- ACC > 威脅活動
- 物件 > 安全性設定檔 > 反間諜軟體/弱點保護

使用威脅詳細資料日誌以學習更多有關防火牆所裝備的威脅特徵碼，以及觸發這些特徵碼的事件。針對以下項目提供威脅詳細資訊：

- 記錄防火牆所偵測的威脅的威脅日誌（**Monitor**（監控）> **Logs**（日誌）> **Threat**（威脅））
- 在您的網路中找到的主要威脅（**ACC** > **Threat Activity**（威脅活動））
- 您要修改或從強制執行中排除的威脅特徵碼（**Objects**（物件）> **Security Profiles**（安全性設定檔）> **Anti-Spyware/Vulnerability Protection**（反間諜軟體/弱點保護））

當您找到想要更多了解的威脅特徵碼，將游標停在 **Threat Name**（威脅名稱）或威脅 **ID** 並按一下 **Exception**（例外）以檢閱威脅詳細資訊。威脅詳細資料可讓您輕易檢查是否已將威脅特徵碼設定為對您的安全性原則的例外，並找到關於特定威脅的最新威脅資料庫資訊。Palo Alto Networks 威脅資料庫的資料庫與防火牆整合，讓您可檢視關於防火牆內容中的威脅特徵碼的展開的詳細資料，或在新瀏覽器視窗中針對已記錄的威脅啟動威脅資料庫搜尋。

根據您正檢視的威脅類型，詳細資料包含下表所述的全部或部分威脅詳細資訊。

威脅詳細資訊	說明
名稱	威脅特徵碼名稱。
ID	唯一威脅特徵碼 ID。選取 **View in Threat Vault**（在威脅資料庫中檢視）以在新瀏覽器視窗中開啟威脅資料庫搜尋，並查詢 Palo Alto Networks 威脅資料庫針對此特徵碼所具有的最新資訊。針對威脅特徵碼的威脅資料庫項目可能包含其他詳細資訊，包括將更新包含至特徵碼的第一個內容版本和上次的內容發行版本，以及支援特徵碼所需的最低 PAN-OS 版本。
說明	關於觸發特徵碼的威脅的資訊。
severity	威脅嚴重性等級：資訊性、低、中、高或關鍵。
CVE	關聯於威脅的公開已知的安全性弱點。一般弱點與曝露點 (CVE) 識別碼對尋找唯一弱點的資訊是最有用的識別碼，因為廠商特定的 ID 通常包含多個弱點。
Bugtraq ID	關聯於威脅的 Bugtraq ID。
廠商 ID	針對弱點的廠商特定的識別碼。例如，MS16-148 是針對一個或多個 Microsoft 弱點的廠商 ID，而 APBSB16-39是一個或多個 Adobe 弱點的廠商 ID。
Reference	您可用來更加了解威脅的參考來源。
豁免設定檔	安全性設定檔，針對威脅特徵碼定義與預設特徵碼動作不同的強制動作。威脅例外僅在豁免設定檔附加至安全性原則規則時是主動狀態（檢查例外是否用在目前安全性規則）。
用在目前安全性規則	主動威脅例外—此欄中的核取符號表示防火牆主動強制執行威脅例外（定義威脅例外的豁免設定檔附加在安全性原則規則中）。

© 2019 Palo Alto Networks, Inc.

威脅詳細資訊	說明
	若清除此欄，則防火牆僅會根據建議的預設特徵碼動作強制執行威脅。
豁免 IP 位址	豁免 IP 位址—您可新增 IP 位址，以便在該位址上篩選威脅例外或檢視現有的 **Exempt IP Addresses**（豁免 **IP** 位址）。此選項只有在相關聯的工作階段有符合豁免 IP 位址的來源或目的地 IP 位址時，才會強制執行威脅例外。針對其他所有工作階段，會根據預設特徵碼動作強制執行威脅。

若您檢視威脅詳細資訊時發生問題，請檢查以下條件：

- 防火牆 *Threat Prevention* 授權為使用中（*Device*（裝置）> *Licenses*（授權））。
- 已安裝最新的防毒、威脅、應用程式內容更新。
- 威脅資料庫存取已啟用（選取 *Device*（裝置）> *Setup*（設定）> *Management*（管理）並編輯 *Logging and Reporting*（日誌記錄與報告）設定以 *Enable Threat Vault Access*（啟用威脅資料庫存取））。
- 預設（或自訂）的防毒、反間碟軟體和弱點保護安全性設定檔已套用到您的安全性原則。

© 2019 Palo Alto Networks, Inc.

AutoFocus 情報摘要

您可以檢視 AutoFocus 所編譯之威脅情報的圖形化概要，以利評估下列防火牆構件的覆蓋率和風險：

- IP 位址
- URL
- 網域
- 使用者代理程式（位於 [資料篩選] 日誌的 [使用者代理程式] 欄中）
- 威脅名稱（僅適用於子類型病毒和 WildFire 病毒的威脅）
- FileName
- SHA-256 雜湊（位於 [WildFire 提交] 日誌的 [檔案摘要] 欄中）

若要檢視 AutoFocus 情報摘要視窗，您必須先擁有作用中的 AutoFocus 訂閱並開啟 AutoFocus 威脅情報（選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）並編輯 AutoFocus 設定）。

啟用 AutoFocus 情報後，將滑鼠懸停於日誌或外部動態清單構件上以開啟下拉選單 (⌄) 然後按一下 **AutoFocus**：

- 檢視流量、威脅、URL 篩選、WildFire 提交、資料篩選和統一等日誌（**Monitor**（監控）> **Logs**（日誌））。
- 檢視外部動態清單項目。

您還可以從防火牆啟動 AutoFocus，進一步調查您發現的相關或可疑的構件。

欄位/按鈕	說明
在 AutoFocus 中搜尋……	按一下可啟動構件的 AutoFocus 搜尋。
分析資訊頁籤	
工作階段	以 WildFire 偵測構件的私人工作階段數目。私人工作階段是僅在與支援帳戶關聯的防火牆上執行的工作階段。將游標停留在工作階段列上方，可檢視每個月的工作階段數目。
範例	與構件相關聯且依 WildFire 裁定（良性、灰色軟體、惡意軟體、網路釣魚）分組的組織和全域範例（檔案和電子郵件連結）。全域是指來自所有 WildFire 提交的範例，而組織則專指您的組織提交給 WildFire 的範例。 按一下 WildFire 裁定，可為以範圍（組織或全域）和 WildFire 裁定篩選的構件啟動 AutoFocus 搜尋。
相符的頁籤	與構件相符的 AutoFocus 頁籤： • 私人頁籤—僅對與您的支援帳戶相關聯的 AutoFocus 使用者顯示。 • 公用頁籤—對所有 AutoFocus 使用者顯示。 • **Unit 42** 頁籤—識別帶來直接安全性風險的威脅和活動。這些頁籤由 Unit 42（Palo Alto Networks 威脅情報和研究團隊）所建立。 • 資訊頁籤—識別商品威脅的 Unit 42 頁籤。 將游標停留在頁籤上方，可檢視頁籤說明和其他頁籤詳細資料。 按一下頁籤，可啟動該頁籤的 AutoFocus 搜尋。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	若要檢視構件的更多相符頁籤，請按一下省略符號（……），以啟動該構件的 AutoFocus 搜尋。AutoFocus 搜尋結果中的 Tags（頁籤）欄會顯示該構件的更多相符頁籤。
被動 DNS 頁籤 Passive DNS（被動 DNS）頁籤會顯示與構件相關聯的被動 DNS 歷程。只有在構件為 IP 位址、網域或 URL 時，此頁籤才會顯示相符資訊。	
要求	提交 DNS 要求的網域。按一下網域可啟動其 AutoFocus 搜尋。
類型	DNS 要求類型（範例：A、NS、CNAME）。
回應	DNS 要求解析成的 IP 位址或網域。按一下 IP 位址或網域，可啟動 AutoFocus 搜尋。 *[回應] 欄不會顯示私人 IP 位址。*
計數	提出要求的次數。
第一次看見	根據被動 DNS 歷程，第一次看見要求、回應和類型組合的日期和時間。
上次看見	根據被動 DNS 歷程，最近一次看見要求、回應和類型組合的日期和時間。
相符雜湊頁籤 [相符雜湊] 頁籤會顯示 WildFire 偵測到構件的五個最近的私人範例。私人範例是僅在與支援帳戶關聯的防火牆上偵測到的範例。	
SHA256	範例的 SHA-256 雜湊。按一下雜湊，可啟動該雜湊的 AutoFocus 搜尋。
檔案類型	範例的檔案類型。
建立日期	WildFire 分析範例並為其指派 WildFire 裁定的日期和時間。
更新日期	WildFire 為範例更新 WildFire 裁定的日期和時間。
裁定	範例的 WildFire 裁定：良性、灰色軟體、惡意軟體或網路釣魚。

© 2019 Palo Alto Networks, Inc.

組態表匯出

管理用戶可以用 PDF 或 CSV 表格格式匯出政策規則庫、物件、託管設備和介面上的資料。匯出的資料為網路介面上可見的資料。對篩選的資料，只有匹配篩選器的資料才會匯出。如果您未套用任何篩選器，則將匯出所有資料。

所有密碼這類敏感資料會用萬元字元（*）隱藏。

設定表匯出成功會生成系統日誌及下載連結。使用該下載連結以在本機儲存 PDF 或 CSV 檔。在您關閉包含該下載連結的視窗後，該特定匯出的下載連結就不可使用。

若要匯出表格資料，按一下 **PDF/CSV** 以設定下列設定：

匯出設定	說明
檔案名稱	輸入用來識別匯出資料的名稱（最多 32 個字元）。該名稱會成為匯出生成的下載檔案名稱。
檔案類型	選取要生成匯出輸出的類型。您可以選擇 PDF 或 CSV 格式。
網頁尺寸	預設網頁尺寸為 Letter（8.5 x 11.0 英吋）您無法變更網頁尺寸。生成的 PDF 預設為直向，並會因為最大欄位數而調整為橫向。
說明 （僅限 PDF）	輸入說明（最大為 255 字元）以提供有關匯出的內容與其他資料。
表格資料	顯示將匯出的表格資料。如果您需要清除先前所設定的篩選器設定,按一下 **Show All Columns**（顯示所有欄位）以顯示所有在選定政策類型下的政策規則。然後您可以新增或移除欄位並套用需要的篩選器。
顯示所有欄位	移除所有篩選器並顯示所有表格欄位。

按一下 **Export**（匯出）以生成設定表格下載連結。

© 2019 Palo Alto Networks, Inc.

儀錶盤

儀錶盤 Widget 會顯示一般防火牆或 Panorama™ 資訊，例如軟體版本、每個介面的狀態、資源使用率，並針對各種日誌類型顯示最多 10 個的項目；日誌 Widget 則會顯示過去一小時內的項目。

儀錶盤 Widget 主題說明儀錶盤的使用方式和可用的 Widget。

儀表板 Widget

根據預設，**Dashboard**（儀表板）會以 **3 Columns**（**3** 欄）的 **Layout**（配置）顯示 Widget，但您可以自訂 **Dashboard**（儀表板），使其改為僅顯示 **2 Columns**（**2** 欄）。

您也可以決定要顯示或隱藏的 Widget，而僅檢視您要監控的 Widget。若要顯示 Widget，請從 **Widget** 下拉式清單中選取 Widget 類別，然後選取 Widget 以將其新增至儀表板（以暗灰文字呈現的 Widget 名稱是已顯示的 Widget）。關閉 Widget（Widget 標頭中的 ✕）即可隱藏（停止顯示）Widget。防火牆和 Panorama 可在您的多次登入間儲存 Widget 顯示設定（分別為各個管理員執行）。

參考 **Last updated**（上次更新）時間戳記，可確認儀表板資料上次重新整理的時間。您可以手動重新整理整個 **Dashboard**（儀表板）（儀表板右上角的 ↻），也可以重新整理個別的 Widget（每個 Widget 標頭內的 ↻）。使用手動儀表板重新整理選項（↻）旁未標記的下拉式清單，可選取整個 **Dashboard**（儀表板）的自動重新整理間隔（以分鐘為單位）：**1 min**（**1** 分鐘）、**2 mins**（**2** 分鐘）或 **5 mins**（**5** 分鐘）；若要停用整個 **Dashboard**（儀表板）的自動重新整理，請選取 **Manual**（手動）。

儀表板 Widget	說明
應用程式 Widget	
前幾大應用程式	顯示工作階段最多的應用程式。區塊大小會指出工作階段的相對數量（將滑鼠游標置於封鎖上方可檢視數量），而顏色則指出安全性風險—從綠色（最低）到紅色（最高）。按一下應用程式可檢視其應用程式設定檔。
前幾大高風險應用程式	除了會顯示工作階段最多的最高風險應用程式以外，其他均與最高排名應用程式相似。
應用程式監測中心風險係數	顯示過去一週處理之網路流量的平均風險係數（1-5）。值越高表示風險越高。
系統 Widget	
一般資訊	顯示防火牆或 Panorama 名稱或型號、Panorama CPU 以及 RAM、Panorama 系統模式、PAN-OS® 或 Panorama 軟體版本、 IPv4 以及 IPv6 管理 IP 資訊、序號、CPU ID 以及 UUID、應用程式威脅，以及 URL 篩選定義版本、目前的日期以及時間，以及自上次重新啟動以來的時間長度。
介面 （僅限防火牆）	指示每個介面的狀態為使用中 (綠色)、關閉 (紅色)，還是未知 (灰色)。
系統資源	顯示管理 CPU 使用情況、資料平面使用情況以及工作計數（透過防火牆或 Panorama 建立的工作階段數目）。
high availability (高可用性)	指出（啟用高可用性 (HA) 時）本機與端點防火牆/Panorama 的高可用性狀態—綠色（主動）、黃色（被動）或黑色（其他）。如需關於高可用性的詳細資訊，請參考 [裝置 > 虛擬系統] 或 [Panorama > 高可用性]。
鎖定	顯示管理員設定的組態鎖。

© 2019 Palo Alto Networks, Inc.

儀表板 Widget	說明
已登入管理員	顯示來源 IP 位址、工作連線類型（Web 介面或 CLI），以及目前登入的每個管理員的工作連線啟動時間。
日誌 Widget	
威脅日誌	威脅日誌中顯示最新 10 筆記錄的威脅 ID、應用程式，以及日期與時間。威脅 ID 是惡意軟體描述或違反 URL 篩選設定檔的 URL。只會顯示過去 60 分鐘內的項目。
URL 篩選日誌	URL 篩選日誌中會顯示最近 60 分鐘的說明以及日期與時間。
資料過濾日誌	資料篩選日誌中會顯示最近 60 分鐘的說明以及日期與時間。
設定日誌	組態日誌中會顯示最新 10 筆項目的管理員使用者名稱、用戶端（網頁介面或 CLI），以及日期與時間。只會顯示過去 60 分鐘內的項目。
系統日誌	系統日誌中顯示最新 10 筆記錄的描述以及日期與時間。 「已安裝的設定」項目可指出已成功認可組態變更。只會顯示過去 *60* 分鐘內的項目。

© 2019 Palo Alto Networks, Inc.

ACC

應用程式控管中心 (ACC) 是一項分析工具，可針對您的網路內的活動提供相關的可操作情報。ACC 可使用防火牆日誌，以圖形化方式表示您的網路上的流量趨勢。圖形化呈現可讓您與資料互動並視覺化網路事件之間的關係，包括使用模式、流量模式以及可疑活動和異常狀況。

> 認識 ACC
> ACC 頁籤
> ACC Widget
> ACC 動作
> 使用頁籤和 Widget
> 使用篩選器—本機篩選器和全域篩選器

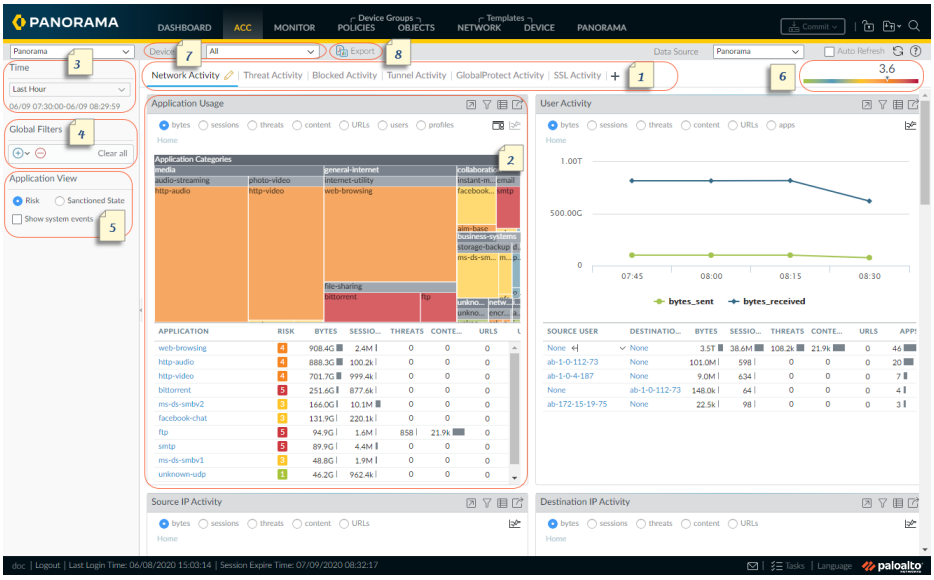
想知道更多？

請參閱使用應用程式控管中心。

認識 ACC

下表列出 ACC 頁籤並說明每個元件。

認識 ACC



1	頁籤	ACC 包含預先定義的頁籤，可讓您檢視網路流量、威脅活動、封鎖的活動、通道活動，以及行動網路活動（如果已啟用 GTP 安全性）。如需各個頁籤的相關資訊，請參閱 ACC 頁籤。
2	**Widget**	每個頁籤都包括預設 Widget 集，可代表與頁籤相關聯的活動和趨勢。Widget 可讓您使用下列篩選器調查資料：位元組（傳入和傳出）、工作階段、內容（檔案和資料）、URL 類別、應用程式、使用者、威脅（惡意、良性、灰色軟體、網路釣魚）以及計數。如需各個 Widget 的相關資訊，請參閱 ACC Widget。
3	時間	各個 Widget 中的圖表和圖形提供即時和歷程檢視。您可選擇自訂範圍或使用預先定義期間，從過去 15 分鐘到過去 90 天，或過去 30 個曆日。 用於呈現資料的預設期間為上一個小時。畫面將顯示日期和時間間隔。例如： `11/11 10:30:00-01/12 11:29:59`
4	全域過濾器	全域篩選器可讓您設定所有頁籤的篩選器。在呈現資料之前，圖表和圖形會先套用所選篩選器。如需使用篩選器的相關資訊，請參閱 ACC 動作。
5	應用程式檢視	應用程式檢視可讓您依據在您的網路上使用的認可和不被認可的應用程式來篩選 ACC 檢視，或依據在您的網路上使用之應用程式的風險層級來篩選。綠色表示認可的應用程式、藍色表示不被認可的應用程式，黃色則表示在不同的虛擬系統或設備群組間會有不同認可狀態的應用程式。

© 2019 Palo Alto Networks, Inc.

認識 ACC		
6	風險計量表	風險計量表（1 = 最低至 5 = 最高）會指出您網路上的相對安全性風險。風險計量表使用多種因素，例如網路上的應用程式類型以及與應用程式相關聯的風險層級、封鎖威脅中的威脅活動和惡意軟體，以及受危害的主機或惡意軟體主機及網域流量。
7	來源	用於顯示畫面的資料在防火牆及 Panorama™ 之間有所不同。您可以使用下列選項來選取要使用何種資料產生 ACC 上的檢視： 虛擬系統：在已針對多重虛擬系統啟用的防火牆上，您可以使用 **Virtual System**（虛擬系統）下拉式清單，將 ACC 顯示畫面變更為包含所有虛擬系統，或僅包含選取的虛擬系統。 設備群組：在 Panorama 上，您可以使用 **Device Group**（設備群組）下拉式清單，將 ACC 顯示畫面變更為包含所有設備群組中的資料，或僅包含選取的設備群組。 資料來源：在 Panorama 上，您也可將顯示畫面變更為使用 **Panorama** 或 **Remote Device Data**（遠端設備資料）（受管理防火牆資料）。當資料來源為 **Panorama** 時，您可針對特定設備群組篩選顯示畫面。
8	匯出	您可以將目前頁籤上顯示的 Widget 匯出為 PDF。

© 2019 Palo Alto Networks, Inc.

ACC 頁籤

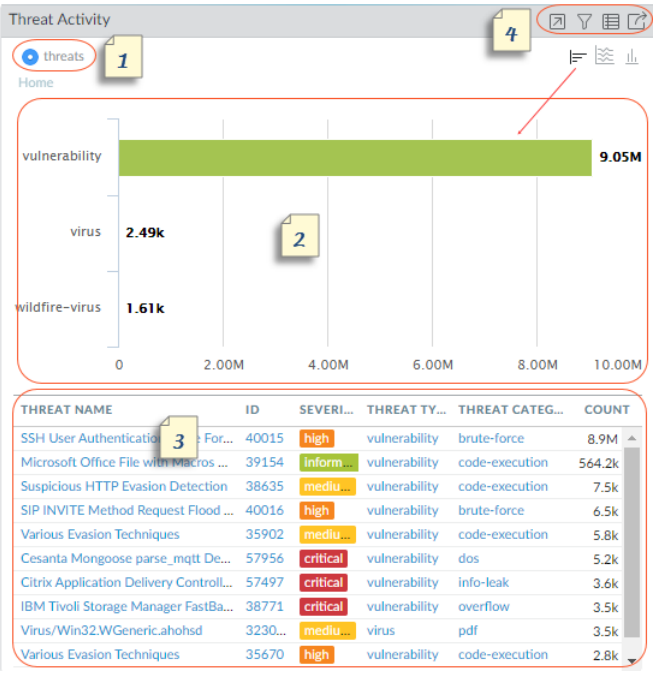
- 網路活動—顯示網路上流量和使用者活動的概要。此檢視著重於最常使用的熱門應用程式、產生流量的前幾名使用者，可向下細分至使用者所存取的位元組、內容、威脅和 URL，以及流量比對發生時最常用的安全性原則規則。此外，您可以依據來源或目的地區域、地區或 IP 位址、ingress 或 egress 介面、主機資訊（如網路上最常用裝置的作業系統）來檢視網路活動。
- 威脅活動—顯示網路上威脅的概要。它著重於主要的威脅—漏洞、間諜軟體、病毒、造訪惡意網域或 URL 的主機、依據檔案類型和應用程式的熱門 WildFire 提交，以及使用非標準連接埠的應用程式。受危害的主機 Widget 以更佳的視覺化技術來補強偵測。它使用關聯事件頁籤的資訊（監控 > 自動關聯引擎 > 關聯事件），依據來源使用者或 IP 位址呈現您的網路上受危害之主機的彙總檢視，並按嚴重性排序。
- 封鎖的活動—專注於禁止進入網路的流量。此頁籤中的 Widget 可讓您依據應用程式名稱、使用者名稱、威脅名稱、內容（檔案和資料）以及熱門安全性規則來檢視遭拒的活動，包括封鎖流量的拒絕動作。
- 行動網路活動—使用從您的安全性原則規則設定產生的 GTP 日誌，以視覺化方式顯示網路上的行動流量。此檢視包括互動式和可自訂的「GTP 事件」、「行動訂閱者活動」和「GTP 拒絕原因」Widget，您可以對這些 Widget 套用 ACC 篩選器，並可加以深入檢視，以解析出您所需的資訊。當您啟用 SCTP Security（SCTP 安全性）時，在頁籤上的 widget 將以視覺化的方式顯示在防火牆上的 SCTP 活動詳情以及每 SCTP 關聯 ID 所送出和接收的區段數量。
- 通道活動—顯示防火牆根據您的通道檢查原則所檢查之通道流量的活動。其資訊包括以通道 ID、監控頁籤、使用者和通道通訊協定（例如 Generic Routing Encapsulation (GRE)、整合封包無線電服務 (GPRS) 使用者資料通道通訊協定 (GTP-U)）和非加密 IPSec 為基礎的通道使用情況。
- **GlobalProtect Activity**（**GlobalProtect** 活動）—顯示 GlobalProtect 部署中使用者活動的概要。資訊包括使用者人數、使用者連線次數、使用者連線的閘道、連線失敗次數及失敗原因、驗證方法摘要與使用的 GlobalProtect 應用程式版本及隔離的端點數。
- **SSL** 活動—顯示基於解密原則和設定檔的解密和未解密 TLS/SSL 流量活動。您可以查看 TLS 活動與非 TLS 活動的比較、已解密流量數量和未解密流量數量的比較、解密失敗的原因以及成功的 TLS 版本和金鑰交換活動。使用此資訊識別導致解密問題的流量，然後使用解密日誌和自訂解密報告範本向下鑽研詳細資料，獲取有關該流量的背景資訊，以便您可以準確地診斷和修正問題。

您還可以依照使用頁籤和 Widgets中的說明自訂頁籤和 *Widgets*。

© 2019 Palo Alto Networks, Inc.

ACC Widget

每個頁籤上的 Widget 均為互動式。您可以設定篩選器並深入檢視顯示畫面，以自訂檢視及專注於您所需的資訊。



每個 Widget 均已結構化，以顯示下列資訊：

1	檢視	您可以依據位元組、工作階段、威脅、計數、使用者、內容、應用程式、URL、惡意、良性、灰色軟體、網路釣魚、檔案（名稱）、資料、設定檔、物件、入口網站、閘道和設定檔來排序資料。每個 Widget 可用的選項有所不同。
2	圖形	圖形顯示選項為樹狀圖、折線圖、橫條圖、堆疊區域圖、堆疊長條圖、圓形圖以及地圖。每個 Widget 可用的選項有所不同，而互動體驗也因圖形類型而有所不同。例如，使用非標準連接埠的應用程式 Widget 可讓您在樹狀圖和折線圖之間選擇。 若要深入檢視顯示畫面，請按一下圖形。您按一下的區域會成為篩選器，讓您可以放大選取項目，並檢視關於該選取項目的詳細資訊。
3	表格	圖形下方的表格會顯示用來呈現圖形之資料的詳細檢視。 您可以按一下並針對表格中的元素設定本機篩選器或全域篩選器。使用本機篩選器時，圖形將更新，且表格會依據該篩選器排序。 使用全域篩選器時，ACC 的檢視會轉為僅顯示您的篩選器特有的資訊。
4	動作	以下是 Widget 標題列中的可用動作： • 最大化檢視—可讓您放大 Widget，並在更大的畫面空間中加以檢視。在最大化檢視中，您除了預設 Widget 檢視中顯示的前十個項目以外，還可看見其他項目。 • 設定本機篩選器—可讓您新增篩選器，以精簡 Widget 內顯示的內容。請參閱使用篩選器—本機篩選器和全域篩選器。

© 2019 Palo Alto Networks, Inc.

		• 跳至日誌 —可讓您直接瀏覽日誌（**Monitor**（監視） > **Logs**（日誌） > **<log-type>**）。系統會使用圖形呈現的時段篩選日誌。 如果您設定了本機和全域篩選器，日誌查詢會連接期間和篩選器，並且僅顯示與您的篩選器集相符的日誌。 • 匯出—可讓您將圖表匯出為 PDF。

如需各個 Widget 的說明，請參閱使用 ACC上的詳細資料。

© 2019 Palo Alto Networks, Inc.

ACC 動作

若要自訂並精簡 ACC 顯示畫面，您可新增及刪除頁籤、新增及刪除 Widget、設定本機和全域篩選器，以及與 Widget 互動。

- 使用頁籤和 Widget
- 使用篩選器—本機篩選器和全域篩選器

使用頁籤和 Widget

下列選項說明如何使用和自訂頁籤和 Widget。

- 新增自訂頁籤。
  1. 選取頁籤清單旁的新增 (+)。
  2. 新增檢視名稱。此名稱將用作頁籤名稱。您可新增最多 10 個自訂頁籤。

- 編輯頁籤。

  選取頁籤，並按一下頁籤名稱旁的編輯以編輯頁籤。

  範例：Threat Activity。

- 將頁籤設為預設
  1. 編輯頁籤。
  2. 選取 以將目前頁籤設定為預設。每次您登入防火牆時，將會顯示此頁籤。

- 儲存頁籤狀態
  1. 編輯頁籤。
  2. 選取 以將您在目前頁籤中的偏好設定儲存為預設。

     已在 HA 端點間對頁籤狀態進行同步，該頁籤狀態包含任何您可能已設定的篩選器。

- 匯出頁籤
  1. 編輯頁籤。
  2. 選取 以輸出目前頁籤。頁籤會以 .txt 檔案下載到您的電腦。您必須啟用快顯視窗以下載檔案。

- 匯入頁籤
  1. 新增自訂頁籤。
  2. 選取 以匯入頁籤。
  3. 瀏覽到文字 (.txt) 檔並選取它。

- 查看檢視中包含的 Widget。
  1. 選取視圖並按一下編輯 ( )。
  2. 選取 **Add Widget**（新增 Widget）下拉式清單，檢閱選取的 widget。

© 2019 Palo Alto Networks, Inc.

- 新增 Widget 或 Widget 群組。
  1. 新增頁籤或編輯預先定義頁籤。
  2. 選取 新增 **Widget** ，接著選取您想新增的 Widget。您最多可選取 12 個 Widget。
  3. （選用）若要建立兩欄配置，請選取 **Add Widget Group**（新增 **Widget** 群組）。您可將 Widget 拖放至兩欄顯示中。當您將 Widget 拖曳至配置時，將向您顯示預留位置以放置 Widget。

     您無法命名 *Widget* 群組。

- 刪除頁籤、Widget 或 Widget 群組。
  - 若要刪除自訂頁籤，請選取頁籤並按一下刪除 (Test)。

    您無法刪除預先定義的頁籤。
  - 若要刪除 Widget 或 Widget 群組，請編輯頁籤，然後按一下刪除 ([X])。您無法復原刪除項目。

- 重設預設檢視。

  在預先定義檢視上，例如封鎖的活動檢視，您可以刪除一或多個 Widget。若您想重設配置以包括頁籤的預設 Widget 集，請編輯頁籤並按一下 **Reset View**（重設檢視）。

使用篩選器—本機篩選器和全域篩選器

為改善詳細資料並精確控制 ACC 顯示的內容，您可使用篩選器：

- **Local Filters**（本機篩選器）—本機篩選器會套用至特定 Widget。本機篩選器可讓您與圖形互動並自訂顯示，以便您深入查看詳細資料並存取您想針對特定 Widget 監控的資訊。您可使用兩種方式套用本機篩選器：按一下圖表或表格中的屬性，或選取 Widget 內的 **Set Filter**（設定篩選器）。**Set Filter**（設定篩選器）可讓您設定在重新啟動之後仍維持原狀的本機篩選器。
- **Global filters**（全域篩選器） — 全域篩選器會在 ACC 上套用。全域篩選器可讓您依最重視的詳細資料轉換顯示畫面，並將無關資訊從目前的顯示畫面中排除。例如，若要檢視與特定使用者和應用程式相關的所有事件，您可以套用使用者的 IP 位址及應用程式以建立全域篩選器，該全域篩選器僅顯示 ACC 的所有頁籤和 Widget 上與該使用者和應用程式相關的資訊。全域篩選器在不同的登入間不會持續。

  您可使用三種方式套用全域篩選器：

- **Set a global filter from a table**（從表格設定全域篩選器）—在任何 Widget 中從表格選取屬性，接著將該屬性套用為全域篩選器。
- **Add a widget filter to be a global filter**（新增 **Widget** 篩選器作為全域篩選器）—將游標停留在屬性上，然後按一下屬性右側的箭頭圖示。此選項可讓您增加用於 Widget 的本機篩選器，並全域套用屬性，以便在 ACC 的所有頁籤上更新顯示。
- **Define a global filter**（定義全域篩選器）—使用 ACC 上的 **Global Filters**（全域篩選器）窗格定義篩選器。

- 設定本機篩選器。

  您也可以按一下圖表下方表格中的屬性以將其套用為本機篩選器。

  1. 選取 Widget 並按一下篩選器 ( )。

© 2019 Palo Alto Networks, Inc.

2. 新增您想要套用的 ( ) 篩選器。
3. 按一下 **Apply**（套用）。這些過濾器在重新啟動之後仍會維持原狀。

Widget 名稱旁將顯示套用於 *Widget* 的本機篩選器數量。

- 從表格設定全域過濾器。

  將游標停留在表格的屬性上，然後按一下出現在屬性右側的箭頭。

- 使用全域篩選器窗格設定全域篩選器。

  新增您想要套用的 ( ) 篩選器。

- 將本機篩選器提升為全域篩選器。
  1. 在 Widget 中的任何表格上，選取屬性。這會將屬性設為本機篩選器。
  2. 若要將篩選器提升為全域篩選器，將游標停留在屬性上，然後按一下屬性右側的箭頭。

- 移除過濾器。

  按一下移除 ( ) 可移除篩選器。

  - **Global filters**（全域篩選器）—位於全域篩選器窗格中。
  - **Local filters**（本機篩選器）—按一下篩選器 ( ) 以開啟設定本機篩選器對話方塊，接著選取篩選器並將其移除。

- 清除所有篩選器。

  - **Global filters**（全域篩選器）—**Clear All**（清除全部）全域篩選器。
  - **Local filters**（本機篩選器）—選取 Widget 並按一下篩選器 ( )。然後在「設定本機篩選器」Widget 中 **Clear all**（清除全部）。

- 否定篩選器。

  選取屬性並否定 ( ) 篩選器。

  - **Global filters**（全域篩選器）—位於全域篩選器窗格中。
  - **Local filters**（本機篩選器）—按一下篩選器 ( ) 以開啟設定本機篩選器對話方塊，新增篩選器，接著對其否定。

- 檢視使用中的篩選器。

  - **Global filters**（全域篩選器）—全域篩選器下的左窗格會顯示已套用全域篩選器的數量。
  - **Local filters**（本機篩選器）—Widget 名稱旁將顯示套用於 Widget 的本機篩選器數量。若要檢視篩選器，請按一下 **Set Local Filters**（設定本機篩選器）。

© 2019 Palo Alto Networks, Inc.

監控

下列主題說明您可用來監控網路上活動的防火牆日誌和報告：

> 監控 > 日誌
> 監控 > 外部日誌
> 監控 > 自動關聯引擎
> 監控 > 封包擷取
> 監控 > App Scope
> 監控 > 工作階段瀏覽器
> 監控 > 封鎖 IP 清單
> Monitor > Botnet（監視 > Botnet）
> 監控 > PDF 報告
> 監控 > 管理自訂報告
> 監控 > 報告

監控 > 日誌

下列主題提供監控日誌的其他資訊。

您想了解什麼內容？	請參閱：
告訴我不同類型的日誌。	日誌類型
篩選器日誌。 匯出日誌。 檢視個別日誌項目的詳細資訊。 修改日誌顯示。	日誌動作
想知道更多？	監控和管理日誌。

日誌類型

- **Monitor**（監控）> **Logs**（日誌）

防火牆顯示所有日誌，以遵守以角色為基礎的管理權限。僅可檢視允許您查看的資料，這視乎您正在檢視的日誌類型而異。如需管理員權限的相關資訊，請檢視Device > Admin Roles（裝置 > 管理員角色）。

日誌類型	說明
流量	顯示每個工作連線的開始與結束項目。每個項目都包括日期與時間、來源與目的地區域、位址、連接埠、應用程式名稱、套用至流量的安全性規則名稱、規則動作（允許、拒絕或捨棄）、ingress 和 egress 介面、位元組數，以及工作階段結束原因。 類型欄指示項目為工作階段開始項目還是結束項目，或指示拒絕工作階段還是丟棄工作階段。「丟棄」表示封鎖流量的安全性規則指定「任何」應用程式，而「拒絕」則表示規則識別特定應用程式。 如果在識別應用程式之前丟棄流量，例如當規則丟棄特定服務的所有流量時，應用程式會顯示為「不可應用」。 深入探究流量日誌，瞭解更多有關個別項目、構件及動作的詳細資訊： • 按一下詳細資訊 ( ) 檢視有關工作階段的其他詳細資訊，例如 ICMP 項目是否在相同來源與目的地之間彙總多個工作階段（**Count**（計數）值將大於 1）。 • 在擁有作用中 AutoFocus™ 授權的防火牆上，將游標停留在 IP 位址、檔名、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。 • 若要新增裝置到隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），開啟裝置的 **Host ID**（主機 **ID**）下拉式清單並 **Block Device**（封鎖裝置）（在快顯對話方塊中）。

© 2019 Palo Alto Networks, Inc.

日誌類型	說明
威脅	顯示由防火牆產生的每個安全性警告的項目。每個項目都包含日期與時間、威脅名稱或 URL、來源與目的地區域、位址、連接埠、應用程式名稱、應用於流量的安全規則名稱，以及警示動作（**allow**（允許）或 **block**（封鎖））及嚴重性。 類型欄表示威脅類型，例如「病毒」或「間諜軟體」。名稱欄是威脅描述或 URL，類別欄是威脅類別（例如「keylogger」）或 URL 類別。 深入探究威脅日誌，瞭解更多有關個別項目、構件及動作的詳細資訊： • 按一下詳細資訊 ( ) 檢視有關威脅的其他詳細資訊，例如項目是否在相同來源與目的地之間彙總多個相同類型的威脅（**Count**（計數）值將大於 1）。 • 在擁有作用中 AutoFocus 授權的防火牆上，將游標停留在 IP 位址、檔名、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。 • 如果啟用本機封包擷取，請按一下下載 ( ) 以存取擷取的封包。若要啟用本機封包擷取，請參考 **Objects**（物件）> **Security Profiles**（安全性設定檔）底下的子區段。 • 若要檢視更多關於威脅的詳細資料，或是要直接從威脅日誌快速設定威脅豁免，請按一下 **Name**（名稱）欄中的威脅名稱。豁免設定檔清單會顯示所有自訂防毒、反間諜軟體和弱點保護設定檔。若要為威脅特徵碼設定豁免，請選取安全性設定檔名稱左邊的核取方塊，然後儲存變更。若要為 IP 位址新增豁免（每個特徵碼最多可豁免 100 個 IP 位址），請反白顯示安全性設定檔，在 [豁免 IP 位址] 區段中新增 IP 位址，然後按一下 **OK**（確定）以進行儲存。若要檢視或修改豁免，請移至相關聯的安全性設定檔，然後按一下 **Exceptions**（例外狀況）頁籤。例如，如果威脅類型是漏洞，請選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **Vulnerability Protection**（漏洞保護），按一下相關聯的設定檔，然後按一下 **Exceptions**（例外狀況）頁籤。 • 若要新增裝置到隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），開啟裝置的 **Host ID**（主機 **ID**）下拉式清單並 **Block Device**（封鎖裝置）（在快顯對話方塊中）。
URL 篩選	顯示 URL 篩選日誌，其可控制網站的存取，以及使用者是否可以對網站提交認證。 選取 [Objects（物件）> Security Profiles（安全設定檔）> URL Filtering（URL 篩選）] 可定義 URL 篩選設定，包括要封鎖或允許的 URL 類別，以及要對何者授與或停用認證提交。您也可以為 URL 啟用 HTTP 標頭選項的記錄。 在擁有作用中 AutoFocus 授權的防火牆上，將游標停留在 IP 位址、檔名、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。
WildFire 提交	顯示防火牆為了進行 WildFire™ 分析所轉送之檔案和電子郵件連結的日誌。WildFire 可以分析樣本並傳回分析結果，其中會包含指派給樣本的 WildFire 裁定（良性、惡意、灰色軟體或網路釣魚）。您可以檢視

© 2019 Palo Alto Networks, Inc.

日誌類型	說明
	Action（動作）欄，以確認防火牆會根據安全性原則規則來允許還是封鎖檔案。 在擁有作用中 AutoFocus 授權的防火牆上，將游標停留在 IP 位址、檔名、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊（位於 File Digest（檔案摘要）欄）旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。
資料篩選	顯示附加資料篩選設定檔的安全性原則日誌，幫助防止諸如信用卡或社會安全號碼等機敏資訊離開受防火牆保護的區域。 若要針對日誌項目詳細資訊的存取設定密碼保護，請按一下 ↓。輸入密碼，然後按一下 **OK**（確定）。如需有關變更或刪除資料保護密碼的指示，請參考 [裝置 > 回應頁面]。 系統會提示您每個工作階段僅輸入一次密碼。
HIP 比對	顯示在比較代理程式所報告的原始 HIP 資料與所定義的 HIP 物件和 HIP 設定檔時，GlobalProtect™ 閘道所識別的所有 HIP 相符項。不同於其他日誌，HIP 相符項即使不符合安全性原則也會記錄下來。如需詳細資訊，請參考 [網路 > GlobalProtect > 入口網站]。 若要新增裝置到隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），開啟裝置的 **Host ID**（主機 **ID**）下拉式清單並 **Block Device**（封鎖裝置）（在快顯對話方塊中）。
GlobalProtect	顯示 GlobalProtect連線日誌。使用此資訊來識別 GlobalProtect 使用者及其用戶端作業系統版本、排除連線與效能問題以及識別使用者連線到的入口網站和閘道。 若要新增裝置到隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），開啟裝置的 **Host ID**（主機 **ID**）下拉式清單並 **Block Device**（封鎖裝置）（在快顯對話方塊中）。
IP-Tag	顯示頁籤如何以及何時應用於特定 IP 位址的資訊。使用此資訊來確定特定 IP 位址是在何時放置在地址群組和原因，以及影響該位址的原則規則。日誌包含接收時間（工作階段中第一個和最後一個到達之封包的日期和時間）、虛擬系統、來源 IP 位址、頁籤、事件、逾時、來源名稱，以及來源類型。
User-ID™	顯示 IP 位址與使用者名稱之對應的相關資訊，例如對應資訊來源、User-ID 代理程式執行對應的時間，以及對應還有多久才會到期。您可以使用此資訊來協助疑難排解 User-ID 問題。例如，如果防火牆對使用者套用了錯誤的原則規則，您可以檢視日誌來確認該使用者是否對應到正確的 IP 位址，以及群組關聯是否正確。
解密	顯示有關不解密設定檔控制之流量的解密工作階段和未解密工作階段的資訊，包括 GlobalProtect 工作階段。 依預設，日誌顯示有關失敗的 SSL 解密交握的資訊。您可以在「解密政策」規則 **Options**（選項）中啟用成功 SSL 解密交握的日誌記錄。日誌顯示大量資訊，可讓您識別弱通訊協定和密碼套件（金鑰交換、加密和驗證演算法）、繞過的解密活動、解密失敗及其原因（例如，憑證鏈不

© 2019 Palo Alto Networks, Inc.

日誌類型	說明
	完整、用戶端驗證、固定憑證）、工作階段結束原因等。例如，使用該資訊來確定是否要允許使用弱通訊協定和演算法的站台。最好封鎖出於業務用途而無需存取的弱站台。 對於流量，防火牆不會解密，並且您向其套用不解密設定檔時，該日誌顯示工作階段由於伺服器憑證驗證問題而被封鎖。 預設的解密日誌大小為 32 MB。然而，若您要解密大量流量，或者啟用了成功的 SSL 解密交握日誌記錄，則可能需要增加日誌大小（**Device**（裝置）> **Setup**（設定）> **Management**（管理）> **Logging and Reporting Settings**（日誌記錄與報告設定）並編輯 **Log Storage**（日誌儲存）配額）。如果您尚無指派的日誌空間，請考慮在解密日誌大小和其他日誌大小之間進行權衡。您記錄的越多，日誌消耗的資源就越多。
GTP	顯示以事件為基礎的日誌，其中會包含各種 GTP 屬性的資訊。這些資訊包括 GTP 事件類型、GTP 事件訊息類型、APN、IMSI、IMEI、使用者 IP 位址，以及下一代防火牆會識別的 TCP/IP 資訊，例如應用程式、來源和目的地位址以及時間戳記。
通道檢查	顯示每個所檢查之通道工作連線的開始與結束項目。日誌中會有接收時間（工作階段中第一個和最後一個到達之封包的日期和時間）、通道 ID、監控頁籤、工作階段 ID、套用至通道流量的安全性規則等資訊。如需詳細資訊，請參閱 Policies > Tunnel Inspection（原則 > 通道檢查）。
SCTP	顯示 SCTP 事件以及依據防火牆在執行狀態偵測、通訊協定驗證和 SCTP 流量篩選時生成的日誌關聯性。SCTP 日誌包含廣泛的 SCTP 資料以及其有效負載協議屬性，如：SCTP 事件類型、區段類型、SCTP 原因代碼、直徑應用程式 ID、直徑指令代碼和區段。除了防火牆識別的一般資料外，還提供如：來源與目的地位址、來源與目的地網路埠、規則和時間戳記 這類 SCTP 資料。如需詳細資料，請參閱物件 > 安全性設定檔 > SCTP 保護。
組態設定	顯示每個組態變更的項目。每個項目都包括日期與時間、管理員使用者名稱、進行變更位置的 IP 位址、用戶端類型（網頁介面或 CLI）、執行的命令類型（無論命令成功還是失敗）、設定路徑以及變更之前和之後的值。
系統	顯示每個系統事件的項目。每個項目都包括日期與時間、事件嚴重性以及事件描述。
警示	警告日誌會記錄系統產生的警告詳細資訊。此日誌中的資訊也會在警報中提供。請參考定義警報設定。
驗證	顯示當使用者嘗試存取網路資源，而其存取權受到驗證原則規則所控制時，所發生之驗證事件的相關資訊。您可以使用此資訊來協助疑難排解存取問題，以及視需要來調整驗證原則。與關聯物件搭配使用時，您也可以使用驗證日誌來識別網路上的可疑活動，例如暴力攻擊。 您也可以選取將驗證規則設定為日誌驗證逾時。這些逾時值會與使用者需要只驗證一次資源就可以重複存取該項資源的該段時間有關。查看逾時的相關資訊可協助您決定是否要加以調整以及該如何調整。

© 2019 Palo Alto Networks, Inc.

日誌類型	說明
	系統日誌會記錄與 *GlobalProtect* 有關以及與管理員的 *Web* 介面存取有關的驗證事件。
統一	顯示最新流量、威脅、URL 篩選、WildFire 提交以及單一檢視中的資料篩選日誌項目。收集日誌檢視可讓您同時調查並篩選這些不同類型的日誌（而非單獨搜尋每個日誌組）。或者，您也可以選取要顯示的日誌類型：按一下篩選器欄位左側的箭頭，然後選取 **traffic**（流量）、**threat**（威脅）、**URL**、**data**（資料）和/或 **wildfire**，僅顯示選取的日誌類型。 在擁有作用中 AutoFocus 授權的防火牆上，將游標停留在 IP 位址、檔名、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。 防火牆顯示所有日誌，以遵守以角色為基礎的管理權限。檢視統一日誌時，僅顯示您有權限查看的日誌。例如，若管理員沒有檢視 WildFire 提交日誌的權限，在檢視統一日誌時，則不會看到 WildFire 提交日誌項目。如需管理員權限的相關資訊，請參考 [裝置 > 管理員角色]。 您可以使用透過 *AutoFocus* 威脅情報入口網站所設定的統一日誌。設定 AutoFocus 搜尋，將 *AutoFocus* 搜尋篩選直接新增至 *Unified* 日誌篩選欄位。 若要新增裝置到隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），開啟裝置的 **Host ID**（主機 **ID**）下拉式清單並 **Block Device**（封鎖裝置）（在快顯對話方塊中）。

日誌動作

下表說明日誌動作。

動作	說明

篩選器日誌	每個日誌頁面的頂端都有篩選欄位。您可新增構件至該欄位，例如 IP 位址或時間範圍，以尋找相符的日誌項目。欄位右側的圖示可讓您套用、清除、建立、儲存及載入篩選器，
	
	Last 90 Days
	
	• 建立篩選器：
	  • 在日誌項目中按一下構件，以新增該構件至篩選器。
	  • 按一下 **Add**（新增）( ) 以定義新的搜尋準則。對於每項條件，請選取定義搜尋類型 **Connector**（連接器（**and** 或 **or**）、搜尋所依據的 **Attribute**（屬性）、定義搜尋範圍的 **Operator**（運算子）以及根據日誌項目進行評估的 **Value**（值）。**Add**（新增）每項準則至篩選欄位，並在完成時 **Close**（關閉）。接著您可套用 (→) 篩選器。
	
	如果 *Value*（值）字串與 *Operator*（運算子）（例如 *has* 或 *in*）相符，則用引號括住該字串，避免出現語法錯誤。例如，如果您按目的地國家篩選，並使用 ***IN*** 作為 *Value*（值）來指定 *INDIA*，則請將篩選輸入為 ***(dstloc eq "IN")***。

© 2019 Palo Alto Networks, Inc.

動作	說明
	日誌篩選 ***(receive_time in last-60-seconds)*** 使顯示的日誌項目數目（及日誌頁數）隨時間增長或減少。 • 套用篩選器—按一下 [套用篩選器] ( ) 以顯示與目前篩選器相符的日誌項目。 • 刪除篩選器 — 按一下 Clear Filter（清除篩選器）( ) 以清除篩選器欄位。 • 儲存篩選器—按一下 [儲存篩選器] ( )，輸入篩選器的名稱，然後按一下 **OK**（確定）。 • 使用儲存的篩選器 — 按一下 Load Filter（載入篩選器）( ) 以新增儲存的篩選器至篩選器欄位。
匯出日誌	按一下 [匯出為 CSV] ( ) 將與目前篩選器相符的所有日誌匯出為 CSV 格式的報告，然後繼續 **Download file**（下載檔案）。依預設，報告包含多達 2,000 行日誌。若要變更產生之 CSV 報告的行限制，請選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）> **Logging and Reporting Settings**（日誌記錄與報告設定）> **Log Export and Reporting**（日誌匯出與報告），然後輸入新的 **Max Rows in CSV Export**（**CSV** 匯出中的最大列數）值。
反白顯示政策動作	選取此選項可反白顯示與動作相符的日誌項目。所篩選出的日誌會以下列顏色反白顯示： • 綠色—允許 • 黃色—繼續，或覆寫 • 紅色—拒絕、丟棄、drop-icmp、rst-client、reset-server、reset-both、block-continue、block-override、block-url、drop-all、sinkhole

變更日誌顯示	若要自訂日誌的顯示：
	• 變更自動重新整理間隔 — 請從間隔下拉式清單中選取間隔（**60 seconds**（60 秒）、**30 seconds**（30 秒）、**10 seconds**（10 秒）或 **Manual**（手動））。
	• 變更每頁顯示的項目數及順序—在 10 個頁面區塊中擷取日誌項目。
	  • 使用頁面底部的頁面控制來導覽日誌清單。
	  • 若要變更每頁的日誌項目數，請從列每個頁面下拉式清單中選取列數（**20**、**30**、**40**、**50**、**75** 或 **100**）。
	  • 若要以遞增或遞減順序排序結果，請使用 **ASC** 或 **DESC** 下拉式清單。
	• 將 IP 位址解析為網域名稱—選取 **Resolve Hostname**（解析主機名稱）開始將外部 IP 位址解析為網域名稱。
	• 變更顯示日誌的順序—選取 **DESC** 以降序顯示日誌（從最近接收時間的日誌項目開始）。選取 **ASC** 以降序顯示日誌（從最早接收時間的日誌項目開始）。

檢視個別日誌項目的詳細資訊。	若要檢視個別日誌項目的相關資訊： • 若要顯示其他詳細資訊，請按一下項目的詳細資訊 ( )。如果來源或目的地在 **Addresses**（位址）頁面中定義了 IP 位址與網域或使用者名稱的對應，則會顯示名稱，而非 IP 位址。若要檢視關聯的 IP 位址，請將滑鼠游標移至名稱上。 • 在擁有作用中 AutoFocus 授權的防火牆上，將游標停留在 IP 位址、URL、使用者代理程式、威脅名稱或日誌項目中包含的雜湊旁邊，然後按一下下拉式清單 ( ) 以開啟該構件的 AutoFocus 情報摘要。

© 2019 Palo Alto Networks, Inc.

監控 > 外部日誌

使用此頁面檢視從 Traps™ Endpoint Security Manager (ESM) 擷取至 Panorama™ 所管理之日誌收集器的日誌。若要在 Panorama 上檢視 Traps ESM 日誌，請執行下列作業：

- 在 Traps ESM 伺服器上，將 Panorama 設定為 Syslog 伺服器並選取要轉送至 Panorama 的記錄事件。事件可能包括安全性事件、政策變更、代理程式和 ESM Server 狀態變更，以及組態設定變更。
- 在以 Panorama 模式部署並具有一或多個受管理日誌收集器的 Panorama 上，設定日誌擷取設定檔 (Panorama > 日誌擷取設定檔) 並將設定檔附加至可儲存 Traps ESM 日誌的收集器群組 (Panorama > 收集器群組)。

外部日誌並未與設備群組相關聯，且只有在您選取 **Device Group**（設備群組）：**All**（全部）時才會顯示，因為並未從防火牆轉送日誌。

日誌類型	說明
Monitor（監控）> **External Logs**（外部日誌）> **Traps ESM** > **Threat**（威脅）	這些威脅事件包括 Traps 代理程式報告的所有防護、通知、暫時和偵測後事件。
Monitor（監控）> **External Logs**（外部日誌）> **Traps ESM** > **Threat**（威脅）	ESM Server 系統事件包括 ESM 狀態相關變更、授權、ESM 技術支援檔案以及與 WildFire 通訊。
Monitor（監控）> **External Logs**（外部日誌）> **Traps ESM** > **Policy**（原則）	政策變更事件包括規則、保護層級、內容更新、雜湊控制日誌和裁定的變更。
Monitor（監控）> **External Logs**（外部日誌）> **Traps ESM** > **Agent**（代理）	代理程式變更事件發生於端點上，包括內容更新、授權、軟體、連線狀態、一次性動作規則、程序和服務以及隔離檔案的變更。
Monitor（監控）> **External Logs**（外部日誌）> **Traps ESM** > **Config**（設定）	ESM 設定變更事件包括授權、管理使用者和角色、程序、限制設定和條件的全系統變更。

Panorama 可以讓端點上的離散安全性事件與網路上的事件產生關聯，以追蹤端點與防火牆間的任何可疑或惡意活動。若要檢視 Panorama 識別的關聯事件，請參閱 Monitor > Automated Correlation Engine > Correlated Events（監視 > 自動關聯引擎 > 關聯事件）。

© 2019 Palo Alto Networks, Inc.

監控 > 自動關聯引擎

自動關聯引擎可追蹤您網路上的模式，並可關聯表示可疑行為增加的事件或導致惡意活動的事件。引擎可擔任您的個人安全性分析師，詳細檢視防火牆上不同日誌的隔離事件、針對特定模式查詢資料，並加以連結以讓您取得可操作的情報。

關聯引擎使用產生關聯事件的關聯物件。關聯事件會校對證據以協助您追蹤看似不相關網路事件的共通點，並提供事件回應重點。

下列型號支援自動關聯引擎：

- Panorama—M 系列裝置和虛擬裝置
- PA-3200 系列防火牆
- PA-5200 Series 防火牆
- PA-7000 系列防火牆

您想了解什麼內容？	請參閱：
何謂關聯物件？	監控 > 自動關聯引擎 > 關聯物件
何謂關聯事件？ 我可以在何處看到關聯比對的比對證據？	Monitor > Automated Correlation Engine > Correlated Events（監視 > 自動關聯引擎 > 關聯事件）
我如何查看關聯比對的圖形檢視？	請參閱 ACC 中受危害的主機 Widget。
想知道更多？	使用自動關聯引擎

監控 > 自動關聯引擎 > 關聯物件

為對抗進步的入侵行為及惡意軟體散佈方式，關聯物件將以特徵碼為基礎的惡意軟體偵測功能延伸至防火牆。它們提供在不同日誌集上識別可疑行為模式的資訊，並收集調查及迅速回應事件所需的證據。

關聯物件為指定比對模式的定義檔、用於執行對應的資料來源，以及要尋找這些模式的時段。模式為查詢資料來源的條件布林結構，且每個模式都獲指派嚴重性及閾值（定義的時間限制內模式符合的發生次數）。模式符合發生時，將記錄關聯事件。

用於執行查詢的資料來源可包括下列日誌：應用程式統計資料、流量、流量摘要、威脅摘要、威脅、資料篩選以及 URL 篩選。例如，關聯物件的定義可包括模式集，該模式會查詢日誌以尋找受感染主機的證據、惡意軟體模式的證據，或惡意軟體在流量內部的活動、URL 篩選及威脅日誌。

關聯物件由 Palo Alto Networks® 定義，且與內容更新一同封裝。您必須具備有效的威脅防範使用授權才能取得內容更新。

預設會啟用所有關聯物件。若要停用物件，請選取物件並按一下 **Disable**（停用）。

關聯物件欄位	說明
名稱和標題	標籤表示關聯物件偵測到的活動類型。
ID	唯一編號可識別關聯物件。此編號位於 6000 Series 中。

© 2019 Palo Alto Networks, Inc.

關聯物件欄位	說明
類別	網路、使用者或主機所受威脅或傷害類型的摘要。
狀態	狀態表示關聯物件為啟用（使用中）或停用（非使用中）。
說明	說明指定防火牆或 Panorama 將分析日誌的比對條件。它說明將用於識別惡意活動或可疑主機行為的增加模式或進展路徑。

Monitor > Automated Correlation Engine > Correlated Events（監視 > 自動關聯引擎 > 關聯事件）

關聯事件將威脅保護功能擴張至防火牆及 Panorama；關聯事件會收集網路上使用者或主機的可疑或異常行為證據。

關聯物件讓您可將特定條件或行為作為中心並追蹤多個日誌來源的共同點。當在網路上觀察到在關聯物件中指定的條件集時，每個比對將記錄為關聯事件。

關聯事件包含下表所列的詳細資訊。

欄位	說明
比對時間	關聯物件觸發比對的時間。
更新時間	比對上次更新的時間戳記。
物件名稱	觸發比對的關聯物件名稱。
來源位址	流量來源使用者的 IP 位址
來源使用者	若 User-ID™ 已啟用，來自目錄伺服器的使用者和使用者群組資訊。
severity	根據造成傷害的程度分級風險。
Summary	概述關聯事件所收集證據的說明。
主機 ID	裝置的主機 ID 若要將裝置新增至隔離清單（**Device**（裝置）> **Device Quarantine**（裝置隔離）），請按一下裝置 **Host ID**（主機 **ID**）旁邊的向下箭頭，然後在顯示的快顯視窗中選取 **Block Device**（封鎖裝置）。

若要檢視詳細日誌檢視，請按一下項目的詳細資訊（ ）。詳細日誌檢視包括比對的所有證據：

頁籤	說明
比對資訊	物件詳細資訊—呈現觸發比對的關聯物件資訊。如需關聯物件的相關資訊，請參閱 [監控 > 自動關聯引擎 > 關聯物件]。

© 2019 Palo Alto Networks, Inc.

頁籤	說明
	比對詳細資訊 — 比對詳細資訊摘要，包括比對時間、在比對證據上的上次更新時間、事件嚴重性以及事件摘要。
比對證據	此頁籤包括所有證實關聯事件的證據。它列出各工作階段所收集證據的詳細資訊。

在 **Correlated Events**（關聯事件）頁籤中查看資訊的圖形顯示畫面，查看 **ACC** > **Threat Activity**（威脅活動）頁籤上「受危害的主機」Widget。在「受危害的主機」Widget 中，顯示畫面由來源使用者和 IP 位址所彙總，並依照嚴重性排序。

若要設定記錄關聯事件時的通知，請移至 **Device**（設備）> **Log Settings**（日誌設定）或 **Panorama** > **Log Settings**（日誌設定）頁籤。

© 2019 Palo Alto Networks, Inc.

監控 > 封包擷取

所有 Palo Alto Networks 防火牆均具備內建封包擷取 (pcap) 功能，您可用來擷取周遊防火牆網路介面的封包。接著您可使用擷取到的資料進行疑難排解，或建立自訂應用程式特徵碼。

封包擷取功能需要大量 *CPU*，且可能降低防火牆效能。請在需要時才使用此功能，並確保在收集所需封包之後關閉此功能。

您想了解什麼內容？	請參閱：
防火牆可使用哪些不同方式來擷取封包？	封包擷取概要
如何產生自訂封包擷取？	自訂封包擷取的建置組塊
如何在防火牆偵測到威脅時產生封包擷取？	啟用威脅封包擷取
我可以在何處下載封包擷取？	封包擷取概要
想知道更多？	
• 開啟安全性設定檔的延伸封包擷取。	Device > Setup > Content-ID（裝置 > 設定 > 內容 ID）
• 使用封包擷取來寫入自訂應用程式簽章。	檢視自訂特徵碼。
• 防止防火牆管理員檢視封包擷取。	定義 Web 介面管理員存取權。
• 請參閱範例。	請參閱獲得封包擷取。

封包擷取概要

您可將 Palo Alto Networks 防火牆設定為執行自訂封包擷取或威脅封包擷取。

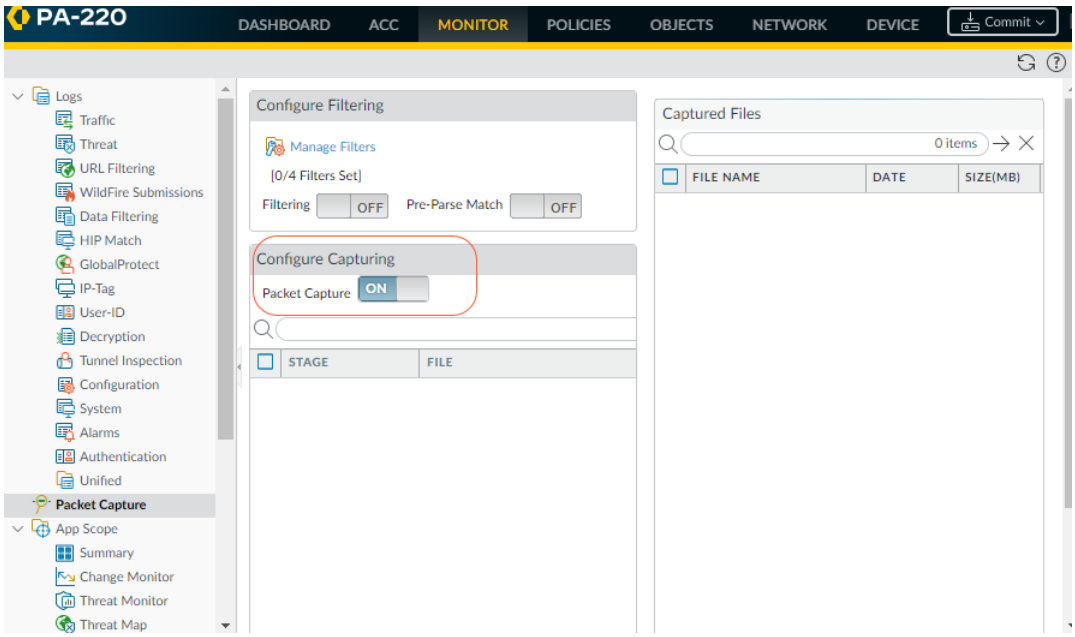
- 自訂封包擷取—擷取所有流量的封包，或以您定義的篩選器為基礎的封包。例如，您可以將防火牆設定為僅擷取進入或離開特定來源、目的地 IP 位址或連接埠的封包。使用這些封包擷取來進行網路流量相關問題的疑難排解，或取得應用程式屬性以寫入自訂應用程式特徵碼 ((**Monitor**（監控）> **Packet Capture**（封包擷取））。您根據階段（丟棄、防火牆、接收或傳輸）定義檔案名稱，在 PCAP 完成後下載擷取檔案區段中的 PCAP。
- 威脅封包擷取—在防火牆偵測到病毒、間諜軟體或漏洞時擷取封包。您在防毒軟體、反間諜軟體及弱點保護安全性設定檔中啟用此功能。這些封包擷取提供威脅內容資訊以協助您判斷攻擊是否成功，或進一步瞭解攻擊者採用的方式。針對威脅的動作必須設為允許或警示，否則將封鎖威脅且無法擷取封包。

  您可在 **Objects**（物件）> **Security Profiles**（安全性設定檔）中設定此類型封包擷取。若要下載（↓）PCAP，請選取 **Monitor**（監控）> **Threat**（威脅）。

© 2019 Palo Alto Networks, Inc.

自訂封包擷取的建置組塊

下表說明在 **Monitor**（監控）> **Packet Capture**（封包擷取）頁面中用來設定封包擷取、啟用封包擷取以及下載封包擷取檔案的元件。



自訂封包擷取建置組塊	設定位置	說明
管理篩選器	設定過濾	啟用自訂封包篩選時，您應定義篩選器，以便僅擷取符合篩選器的封包。這可讓您在 PCAP 中輕鬆找出所需的資訊，並減少防火牆擷取封包所需的處理能力。 按一下 **Add**（新增）來新增篩選器，然後設定下列欄位： • **Id**—輸入或選取過濾的識別碼。 • 輸入介面—選取您要擷取流量的輸入介面。 • 來源—指定要擷取流量的來源 IP 位址。 • 目的地 — 指定要擷取流量的目的地 IP 位址。 • 來源連接埠 — 指定要擷取流量的來源連接埠。 • 目的地連接埠—指定要擷取流量的目的地連接埠。 • 通訊協定—指定要篩選的通訊協定號碼 (1-255)。例如，ICMP 為通訊協定 1。 • **Non-IP** — 選擇如何處理非 IP 流量（排除所有 IP 流量、包含所有 IP 流量、僅包含 IP 流量，或不包含 IP 篩選）。廣播及 AppleTalk 為非 IP 特定的範例。 • **IPv6** — 選取此核取方塊可將 IPv6 封包包含在篩選中。
篩選	設定過濾	在定義篩選器之後，將 **Filtering**（篩選）設定為 **ON**（開啟）。若過濾為關閉，則會擷取所有流量。
Pre-Parse Match	設定過濾	此選項供進階疑難排解之用。當封包進入輸入連接埠之後，它會先繼續完成數個處理步驟，再與預先設定的篩選器針對比對進行剖析。

© 2019 Palo Alto Networks, Inc.

自訂封包擷取建置組塊	設定位置	說明
		封包可能會因為失敗而無法到達篩選階段。例如，如果路由查詢失敗，便會發生這種情況。 將 預先剖析比對設定設定為開，以針對進入系統的每個封包模擬正向比對。這樣可讓防火牆擷取尚未到達篩選程序的封包。如果封包能夠到達篩選階段，則會根據篩選設定加以處理，如果它無法符合篩選準則便將其丟棄。

封包擷取	設定擷取	按一下切換開關可 **ON**（開啟）或 **OFF**（關閉）封包擷取。
		您必須至少選取一個擷取階段。按一下 **Add**（新增）並指定下列資訊：
		• 階段 — 指示要擷取封包的位置：
		  • 丟棄 — 當封包處理遇到錯誤且丟棄封包時。
		  • 防火牆—當封包的工作階段相符或成功建立含工作階段的第一個封包時。
		  • 接收 — 當在資料平面處理器上收到封包時。
		  • 傳輸 — 當在資料背板處理器上載輸封包時。
		• 檔案 — 指定擷取檔案名稱。檔案名稱應以字母開始，且可以包含字母、數字、句點、底線或連字號。
		• 封包計數—指定擷取要在達到該封包數後停止的封包數上限。
		• 位元組計數—指定在達到後即停止擷取的位元組數上限。

擷取的檔案	擷取的檔案	包含先前由防火牆產生的自訂封包擷取清單。按一下檔案以將其下載至電腦。若要刪除封包擷取，請選取封包擷取，然後將其 **Delete**（刪除）。 • 檔案名稱—列出封包擷取檔案。檔案名稱以您針對擷取階段指定的檔案名稱為基礎 • 日期—檔案產生的日期。 • 大小 **(MB)**—擷取檔案的大小。 在您開啟封包擷取並關閉之後，您必須按一下重新整理圖示（⟳），新的 PCAP 檔案才會顯示於清單。
清除所有設定	設定	按一下 **Clear All Settings**（清除所有設定）以關閉封包擷取並清除所有封包擷取設定。 這並不會關閉在安全性設定檔中設定的封包擷取。如需在安全性設定檔上啟用封包擷取的相關資訊，請參閱啟用威脅封包擷取。

啟用威脅封包擷取

- Objects > Security Profiles（物件 > 安全性設定檔）

若要使防火牆在偵測到威脅時擷取封包，請啟用安全性設定檔中的封包擷取選項。

請先選取 **Objects**（物件）> **Security Profiles**（安全性設定檔），接著如下表說明修改所需的設定檔：

© 2019 Palo Alto Networks, Inc.

安全性設定檔中的封包擷取選項	位置
防毒軟體	選取自訂防毒設定檔，接著在 **Antivirus**（防病毒）頁籤中選取 **Packet Capture**（封包擷取）。
反間諜軟體	選取自訂反間諜軟體設定檔，按一下 **DNS Signatures**（**DNS** 簽章）頁籤，接著在 **Packet Capture**（封包擷取）下拉式清單中選取 **single-packet**（單一封包）或 **extended-capture**（延伸擷取）。
漏洞保護	選取弱點保護設定檔，接著在 **Rules**（規則）頁籤中按一下 **Add**（新增）以新增規則或選取現有規則。接著選取 **Packet Capture**（封包擷取）下拉式清單，並選取 **single-packet**（單一封包）或 **extended-capture**（延伸擷取）。

在反間諜軟體和弱點保護設定檔中，您也可啟用例外狀況的封包擷取。按一下 *Exceptions*（例外狀況）頁籤，並在特徵碼的封包擷取欄位中按一下下拉式清單，並選取 *single-packet*（單一封包）或 *extended-capture*（延伸封包）。

（選用）若要根據擷取的封包數量（這以全域設定為基礎）定義威脅封包擷取的長度，請選取 **Device**（裝置）> **Setup**（設定）> **Content-ID**，在 Content-ID™ 設定區段中修改 **Extended Packet Capture Length (packets field)**（延伸封包擷取長度（封包欄位））（範圍為 1-50，預設為 5）。

您在安全性設定檔上啟用封包擷取之後，您必須確認設定檔為安全性規則的一部份。如需如何將安全性設定檔新增至安全性規則的相關資訊，請參閱安全性原則概要。

在安全性設定檔上啟用封包擷取時，每次防火牆偵測到威脅，您即可下載（ ）或匯出封包擷取。

© 2019 Palo Alto Networks, Inc.

監控 > App Scope

下列主題說明 App Scope 功能。

- App Scope 概要
- App Scope 摘要報告
- App Scope 異動監控報告
- App Scope 威脅監控報告
- App Scope 威脅地圖報告
- App Scope 網路監控報告
- App Scope 流量地圖報告

App Scope 概要

App Scope 報告對您網路的下列活動提供圖形化可見度：

- 應用程式使用情況與使用者行為的變化
- 主要耗用網路頻寬的使用者與應用程式
- 網路威脅

使用 App Scope 報告，您可以快速發現是否有任何不尋常或非預期的行為，並協助凸顯有問題的行為；各報告均會提供使用者可自訂的動態網路視窗。報告包括選取資料的選項及顯示的範圍。在 Panorama 上，您也可以針對顯示的資訊選取資料來源。預設資料來源（在新的 Panorama 安裝上）使用可儲存受管理防火牆所轉送日誌的 Panorama 本機資料庫；升級時，預設資料來源是 **Remote Device Data**（遠端設備資料）（受管理防火牆資料）。若要從受管理的防火牆直接擷取並顯示資料的彙總檢視，您現在必須將來源從 **Panorama** 切換為 **Remote Device Data**（遠端設備資料）。

將滑鼠移到圖表上方，再按一下圖表的行或列以切換至 ACC，並提供特定應用程式、應用程式類別、使用者或來源的詳細資訊。

應用程式控管中心圖表	說明
Summary	App Scope 摘要報告
變更監視器	App Scope 異動監控報告
威脅監視器	App Scope 威脅監控報告
威脅地圖	App Scope 威脅地圖報告
網路監測	App Scope 網路監控報告
流量地圖	App Scope 流量地圖報告

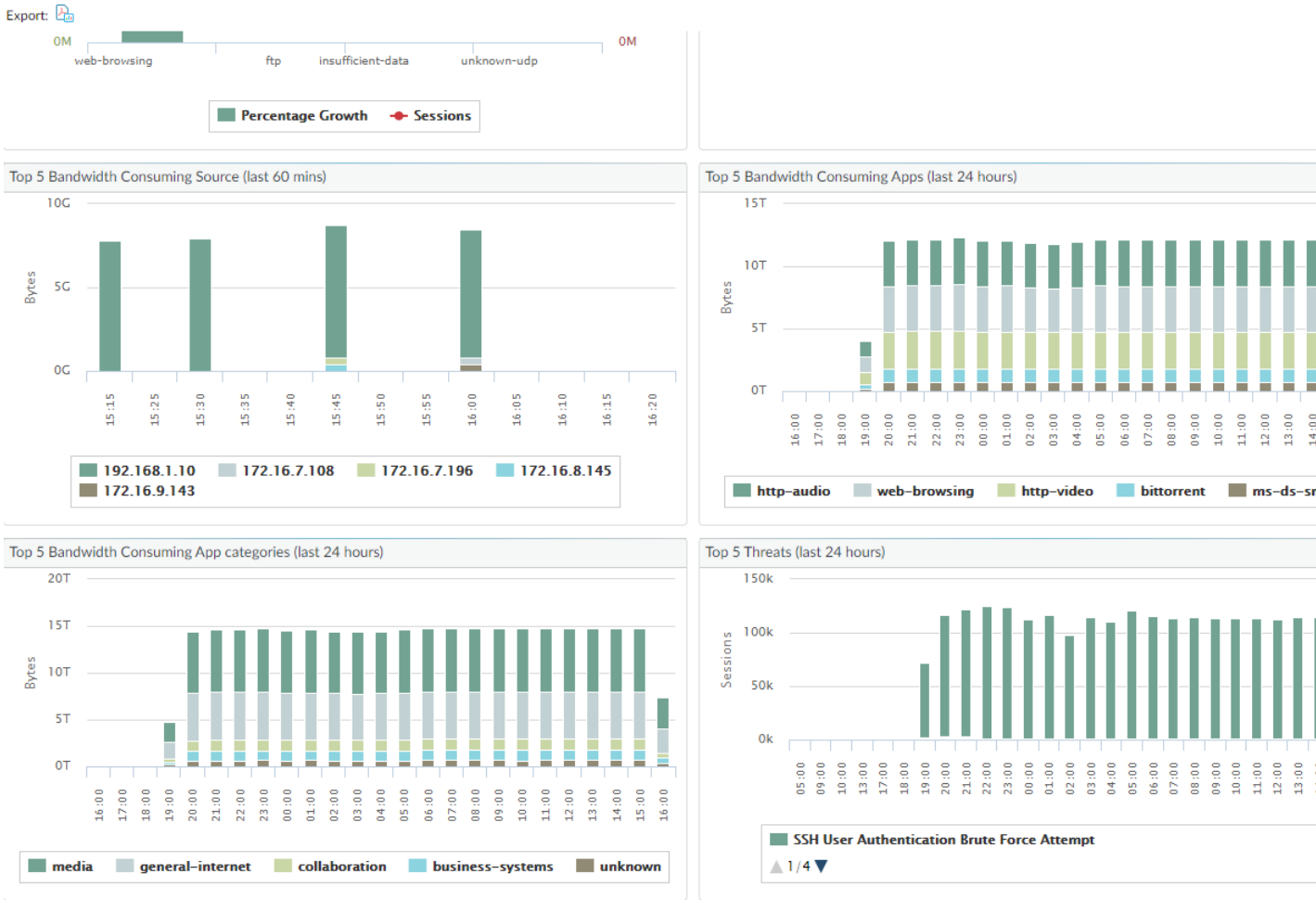
App Scope 摘要報告

摘要報告會顯示前五大使用量增加項、使用量減少項、頻寬消耗應用程式、應用程式類別、使用者和來源的圖表。

若要將摘要報告中的圖表匯出為 PDF，請按一下 **Export**（匯出）( )。會將每一張圖表另存為 PDF 輸出中的頁面。

© 2019 Palo Alto Networks, Inc.

App Scope 摘要報告

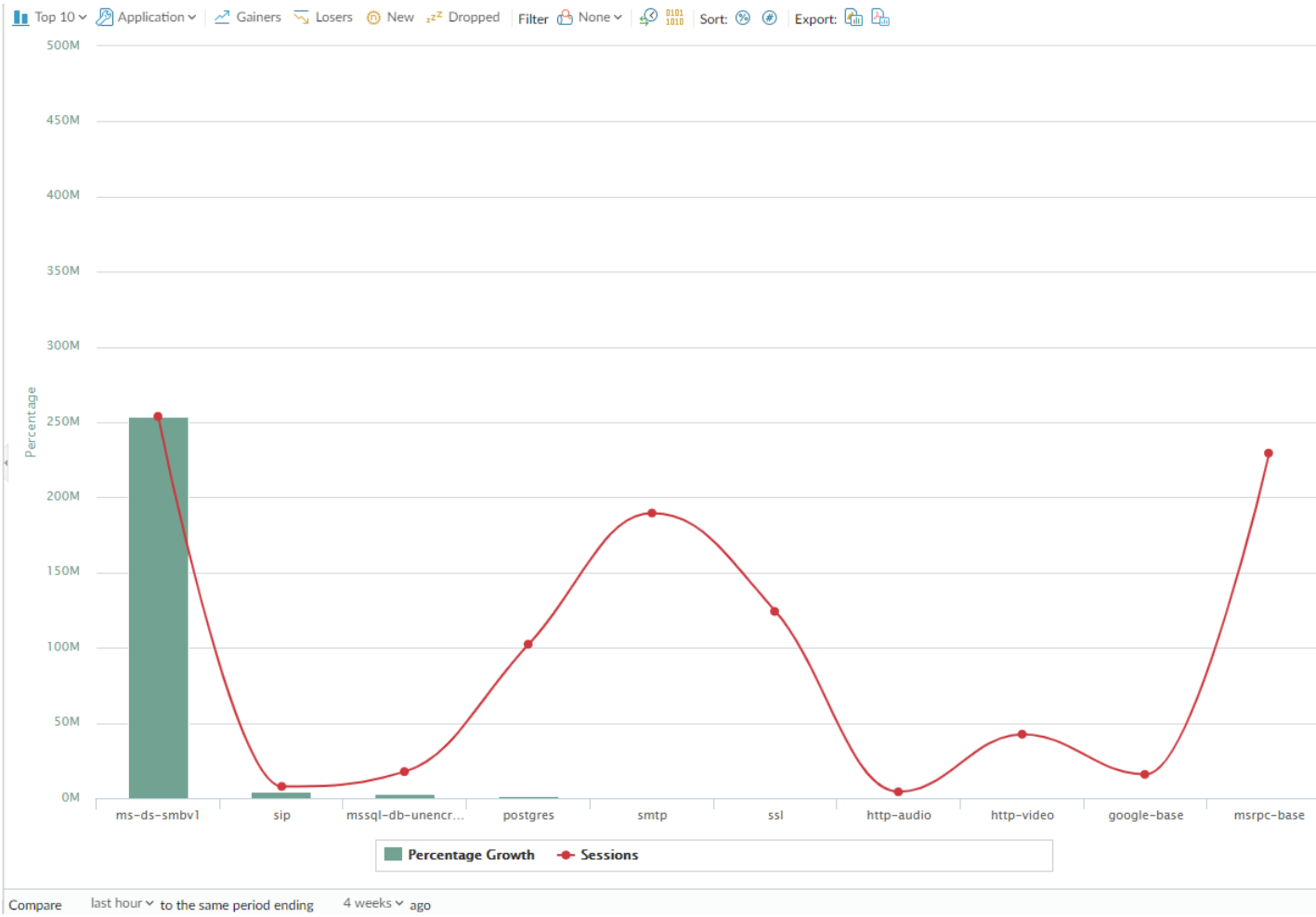


App Scope 異動監控報告

異動監控報告會顯示指定時段內的異動。例如，下圖顯示與過去 24 小時期間相比較，在前一個小時內使用量增加的最高排名應用程式。前幾名的應用程式是由工作階段數量所決定，並按百分比排序。

App Scope 異動監控報告

© 2019 Palo Alto Networks, Inc.



此報告包括下列選項。

異動監控報告選項	說明
頂端列	
前 10 位	決定在圖表中包含最高排名，記錄的數量。
應用程式	決定報告的項目類型：應用程式、應用程式類別、來源或目的地。
獲利者	顯示在測量過程中增加的項目測量。
失敗者	顯示在測量過程中減少的項目測量。
新增	顯示測量過程中新增的項目測量。
已丟棄	顯示測量過程中終止的項目測量。
篩選	套用篩選器以僅顯示所選項目。None（無）會顯示所有項目。

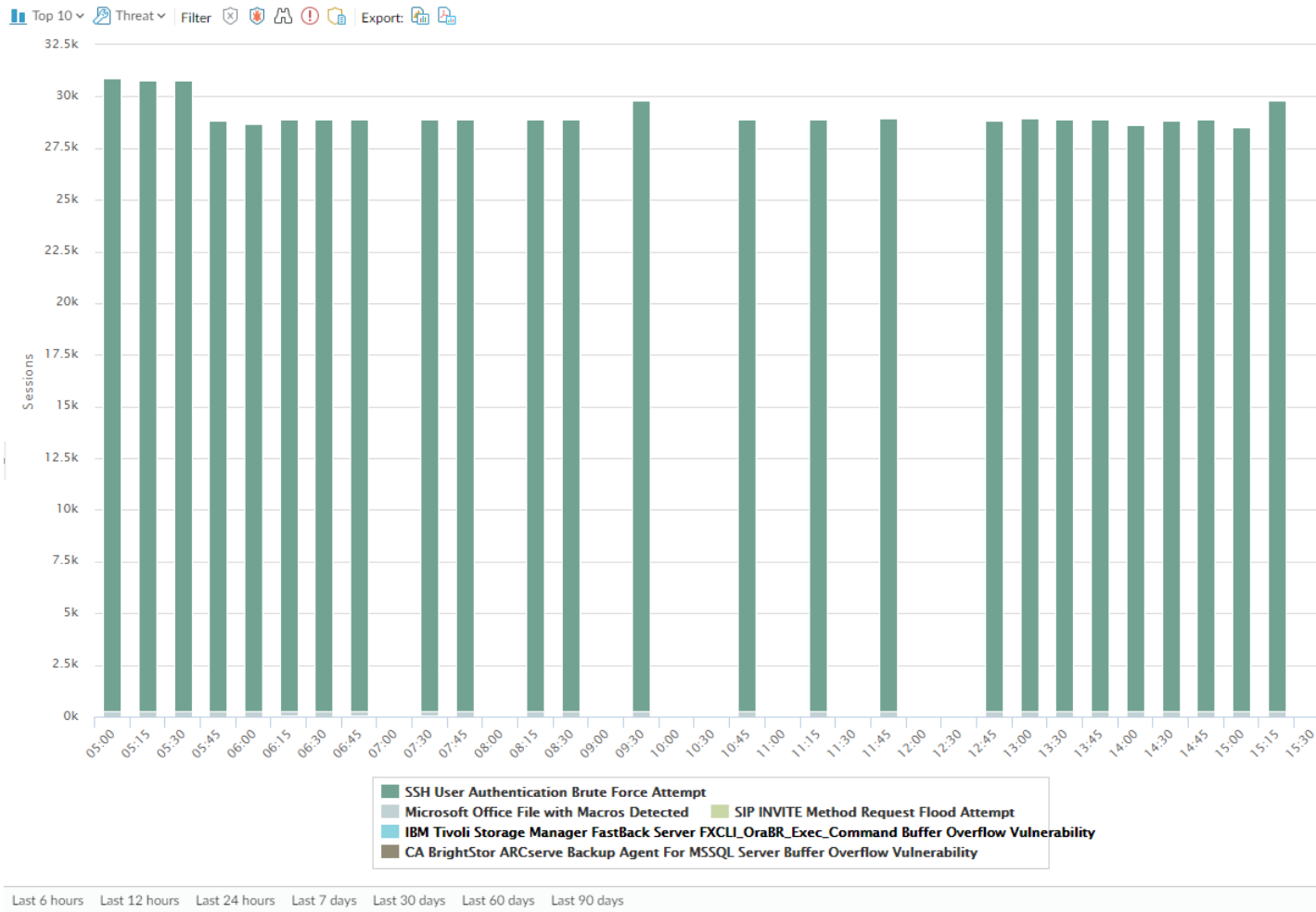
© 2019 Palo Alto Networks, Inc.

異動監控報告選項	說明
計數工作階段與計數位元組	決定顯示工作階段還是位元組資訊。
排序	決定按百分比還是粗略的成長率排序項目。
匯出	將圖形匯出為 .png 影像或 PDF。
底端列	
比較（時間間隔）	指定進行異動測量的時段。

App Scope 威脅監控報告

威脅監視報告顯示所選時段內前幾名的威脅計數。例如，下圖顯示過去 6 個小時的前 10 大威脅類型。

App Scope 威脅監控報告



每個威脅類型都用顏色分類，如圖表下面的圖例所示。此報告包括下列選項。

© 2019 Palo Alto Networks, Inc.

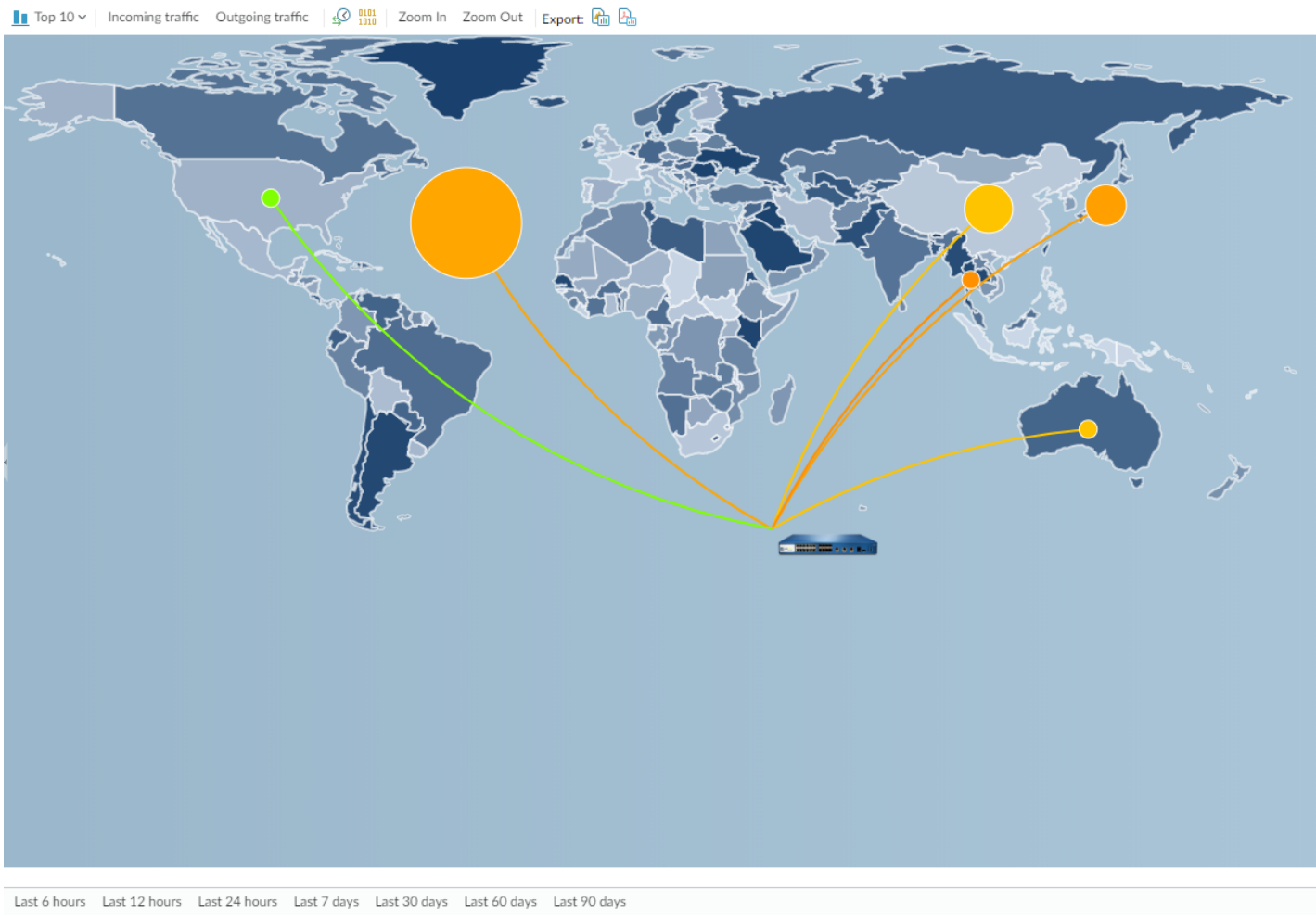
威脅監控報告選項	說明
頂端列	
前 10 位	決定在圖表中包含最高排名，記錄的數量。
威脅	決定測量的項目類型：威脅、威脅類別、來源或目的地。
篩選	套用篩選器以僅顯示所選項目。
	決定將資訊顯示在堆疊式欄圖表還是堆疊式區域圖表中。
匯出	將圖形匯出為 .png 影像或 PDF。
底端列	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	指定進行測量的時段。

App Scope 威脅地圖報告

威脅地圖報告顯示威脅的地理位置圖，包括嚴重性在內。

App Scope 威脅地圖報告

© 2019 Palo Alto Networks, Inc.



每個威脅類型都用顏色分類，如圖表下面的圖例所示。按一下地圖上的國家/地區可 **Zoom In**（放大），然後視需要 **Zoom Out**（縮小）。此報告包括下列選項。

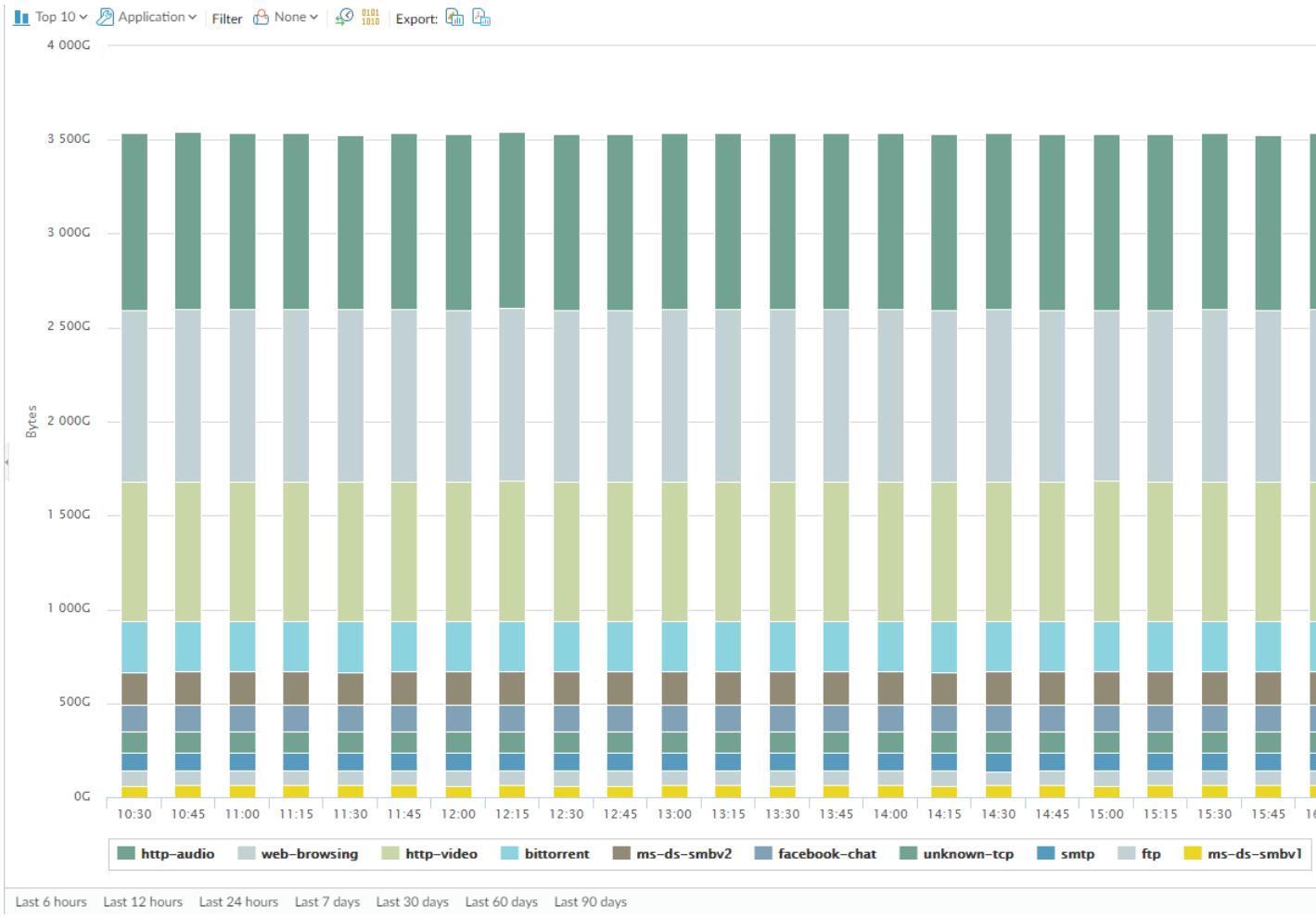
威脅地圖報告選項	說明
頂端列	
前 10 位	決定在圖表中包含最高排名，記錄的數量。
連入威脅	顯示連入的威脅。
連出威脅	顯示連出的威脅。
篩選	套用篩選器以僅顯示所選項目。
放大和縮小	放大和縮小地圖。
匯出	將圖形匯出為 .png 影像或 PDF。
底端列	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 9	選擇進行分析的時間區段。

© 2019 Palo Alto Networks, Inc.

App Scope 網路監控報告

網路監控報告顯示指定時段內用於不同網路功能的頻寬。每個網路服務應用都用顏色分類，如圖表下面的圖例所示。例如，下列影像顯示以工作階段資訊為基礎的過去 7 天應用程式頻寬。

App Scope 網路監控報告



報告包括下列選項。

網路監控報告選項	說明
頂端列	
前 10 位	決定在圖表中包含最高排名，記錄的數量。
應用程式	決定報告的項目類型：應用程式、應用程式類別、來源或目的地。
篩選	套用篩選器以僅顯示所選項目。**None**（無）會顯示所有項目。
計數工作階段與計數位元組	決定顯示工作階段還是位元組資訊。
	決定將資訊顯示在堆疊式欄圖表還是堆疊式區域圖表中。

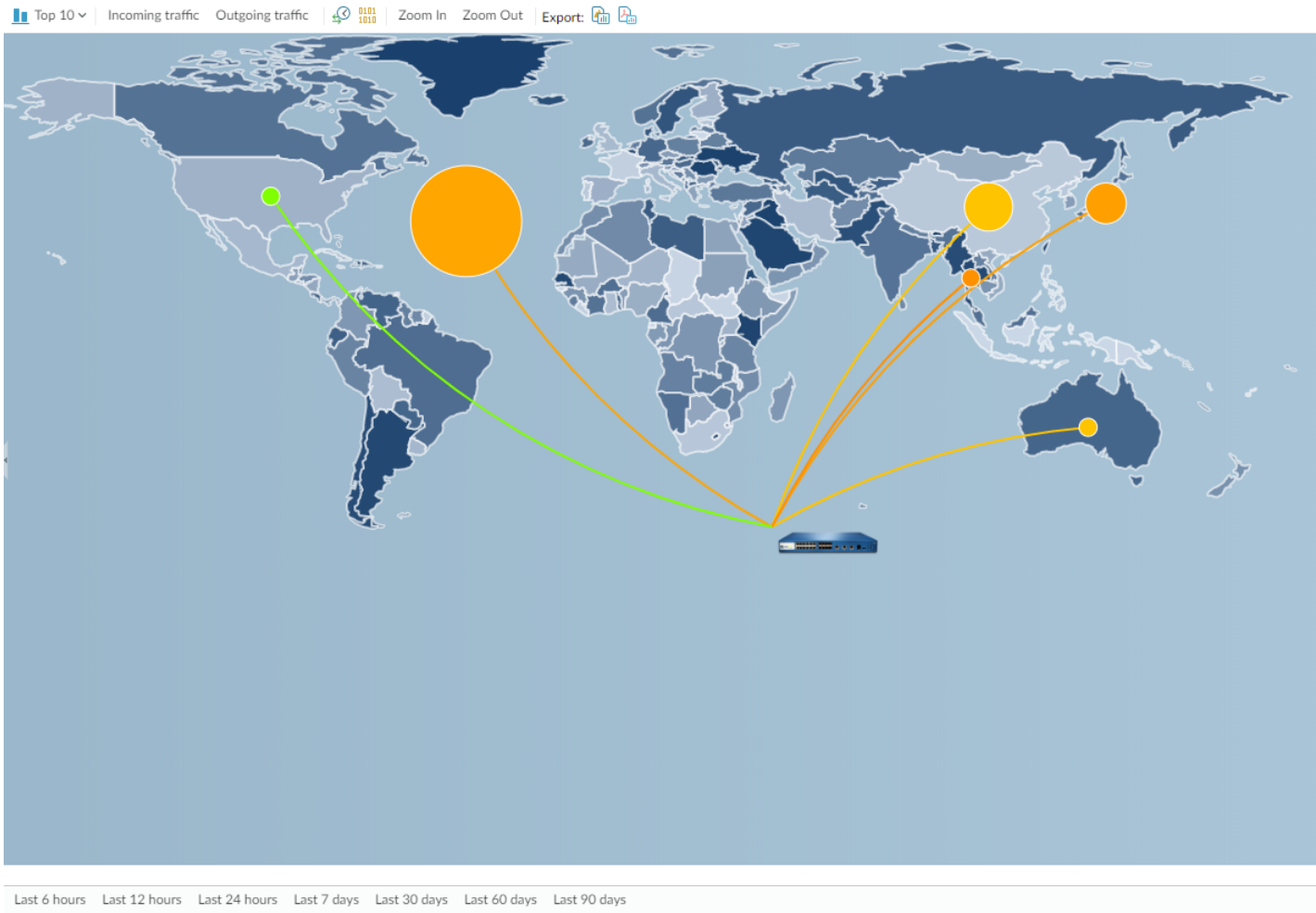
© 2019 Palo Alto Networks, Inc.

網路監控報告選項	說明
匯出	將圖形匯出為 .png 影像或 PDF。
底端列	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	指示進行異動測量的時段。

App Scope 流量地圖報告

流量地圖報告根據工作階段或流量顯示流量的地理視圖。

App Scope 流量地圖報告



每個流量類型都用顏色分類，如圖表下面的圖例所示。此報告包括下列選項。

流量地圖報告選項	說明
頂端列	
前 10 位	決定在圖表中包含最高排名，記錄的數量。

© 2019 Palo Alto Networks, Inc.

流量地圖報告選項	說明
傳入流量	顯示連入的流量。
傳出流量	顯示連出的流量。
計數工作階段與計數位元組	決定顯示工作階段還是位元組資訊。
放大和縮小	放大和縮小地圖。
匯出	將圖形匯出為 .png 影像或 PDF。
底端列	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	指示進行異動測量的時段。

© 2019 Palo Alto Networks, Inc.

監控 > 工作階段瀏覽器

選取 **Monitor**（監控） > **Session Browser**（工作階段瀏覽器）可瀏覽及篩選防火牆上目前執行中的工作階段。如需此頁面篩選選項的相關資訊，請參閱日誌動作。

© 2019 Palo Alto Networks, Inc.

監控 > 封鎖 IP 清單

您可以使用數種方式設定防火牆，將 IP 位址置放在封鎖清單上，包括下列方式：

- 設定採用 **Protect**（保護）動作的 DoS 保護政策規則，並將分類 DoS 保護設定檔套用至此規則。此設定檔包含封鎖持續時間。
- 設定具有漏洞保護設定檔的安全性政策規則（該設定檔使用的規則採用 **Block IP**（封鎖 **IP**）動作），並將此規則套用至某個區域。

在 PA-3200 系列、PA-5200 系列和 PA-7000 系列 防火牆上支援封鎖 IP 清單。

您想了解什麼內容？	請參閱：
封鎖 IP 清單欄位可表示什麼？	封鎖 IP 清單項目
如何篩選、瀏覽或刪除封鎖 IP 清單項目？	檢視或刪除封鎖 IP 清單項目
想知道更多？	設定防毒、反間諜軟體及漏洞保護 針對新工作階段流量湧入的 DoS 保護 監控封鎖的 IP 位址

封鎖 IP 清單項目

- **Monitor**（監控）> **BlockIPList**（封鎖 **IP** 清單）

下表說明防火牆封鎖之來源 IP 位址的封鎖清單項目。

欄位	說明
封鎖時間	IP 位址出現在封鎖 IP 清單上的月 / 日和 hours:minutes:seconds。
類型	封鎖動作的類型：封鎖 IP 位址的是硬體 (hw) 還是軟體 (sw)。 如果您設定了使用弱點保護設定檔的 DoS 保護原則或安全性原則，以封鎖來自來源 IPv4 位址的連線，防火牆將會在封包使用 CPU 或封包緩衝區資源之前，自動在硬體中封鎖該流量。如果攻擊流量超過硬體的封鎖能力，則防火牆會使用軟體來封鎖流量。
來源 IP 位址	防火牆封鎖之封包的來源 IP 位址。
進入區域	為介面指派讓封包進入防火牆的安全性區域。
剩餘時間	IP 位址出現在封鎖 IP 清單上的剩餘秒數。
封鎖來源	您在其中指定封鎖 IP 動作的分類 DoS 保護設定檔名稱或弱點保護物件名稱。
封鎖 IP 總數：y 中的 x（已使用 z%）	在防火牆支援的封鎖 IP 位址數目 (y) 中遭封鎖的 IP 位址計數 (x)，以及已使用的封鎖 IP 位址的對應百分比 (z)。

© 2019 Palo Alto Networks, Inc.

檢視或刪除封鎖 IP 清單項目

瀏覽封鎖 IP 清單項目、檢視詳細資訊，並可按需求刪除項目。

檢視或刪除封鎖 IP 清單項目	
搜尋特定封鎖 IP 清單資訊	選取欄中的值，該值對 **Filters**（篩選器）欄位輸入篩選，按一下右箭頭以針對具有該值的項目啟動搜尋。 按一下 X 以移除篩選器。
檢視超出目前畫面的封鎖 IP 清單項目	在 **Page**（頁面）欄位中輸入頁碼或按一下單箭頭以檢視項目的下一頁或上一頁。按一下雙箭頭以檢視項目的最後一頁或第一頁。
檢視封鎖 IP 清單上關於 IP 位址的詳細資訊。	按一下任何項目的來源 IP 位址，這會連結到具有位址資訊的網路解決方案 WHOIS。
刪除封鎖 IP 清單項目	選取項目，然後按一下 **Delete**（刪除）。 從網頁介面中，僅支援刪除硬體項目。但是，從 *CLI* 中，支援刪除硬體項目和軟體項目。
清除整個封鎖 IP 清單	按一下 **Clear All**（清除全部）以永久刪除所有項目，這表示不再封鎖這些封包。 從網頁介面中，僅支援清理硬體項目的封鎖 *IP* 清單。但是，從 *CLI* 中，支援清理硬體項目和軟體項目。

© 2019 Palo Alto Networks, Inc.

Monitor > Botnet（監視 > Botnet）

Botnet 報告可讓您使用行為式機制來識別網路中的潛在惡意軟體及受 Botnet 感染的主機。報告為每一個主機指定從 1 到 5 的信任分數，指出感染 Botnet 的可能性（1 表示最低，5 表示最可能受到感染）。排程報告之前或視需要執行時，您必須設定其識別為可疑流量的類型。《PAN-OS® 管理員指南》提供有關判讀 Botnet 報告輸出的詳細資訊。

- botnet 報告設定
- 殭屍網路組態設定

botnet 報告設定

- Monitor > Botnet > Report Setting（監視 > Botnet > 報告設定）

在產生 Botnet 報告之前，您必須指定可指出潛在 Botnet 活動的流量類型（請參閱設定 Botnet 報告）。若要對每日報告排程或視需要執行，請按一下 **Report Setting**（報告設定），然後完成下列欄位。若要匯出報告，請選取報告，然後選取 **Export to PDF**（匯出為 PDF）、**Export to CSV**（匯出為 CSV）或 **Export to XML**（匯出為 XML）。

botnet 報告設定	說明
測試執行時間範圍	選取報告的時間間隔—**Last 24 Hours**（過去 24 小時）（預設值）或 **Last Calendar Day**（上一個行事曆日期）。
立即執行	按一下 **Run Now**（立即執行）以手動方式立即產生報告。報告會顯示在 [Botnet 報告] 對話方塊的新頁籤中。
列數	指定在報告中顯示的列數（預設為 100）。
已排程	選取此選項可自動產生每日報告。依預設，會啟用此選項。
查詢建立器	（選用）**Add**（新增）查詢至「查詢建立器」，按照來源/目的地 IP 位址、使用者或區域等屬性篩選報告輸出。例如，如果您知道從 IP 位址 192.0.2.0 啟動的流量不包含任何潛在 Botnet 活動，您可以將 `not (addr.src in 192.0.2.0)` 新增為用於從報告輸出中排除主機的查詢。 • 連接器—選取邏輯連接器（**and** 或 **or**）。如果您選取 **Negate**（否定），報告將排除查詢指定的主機。 • 屬性—選取與防火牆評估 Botnet 活動之主機關聯的區域、位址或使用者。 • 運算子 — 選取可將 **Attribute**（屬性）與 **Value**（值）相關聯的運算子。 • 值 — 輸入符合查詢的值。

殭屍網路組態設定

- Monitor > Botnet > Configuration（監控 > 殭屍網路 > 組態）

若要指定可指示潛在殭屍網路活動的流量類型，請按一下 殭屍網路 頁面右側的 **Configuration**（組態），然後完成下列欄位。設定報告後，您可以隨需加以執行或將其排程為每日執行（請參閱 [監控 > PDF 報告 > 管理 PDF 摘要]）。

預設的殭屍網路報告設定是最佳化的。如果您認為預設值識別誤報，請建立支援票證，以便 *Palo Alto Networks* 可以重新評估這些數值。

© 2019 Palo Alto Networks, Inc.

殭屍網路組態設定	說明
HTTP 流量	**Enable**（啟用）並定義報告中將包含的各類 HTTP 流量的 **Count**（計數）。您輸入的 **Count**（計數）值是必須在報告中呈現的各類流量類型的最小事件數，列示與更高信任分數相關聯的主機（感染殭屍網路的可能性更高）。如果事件數少於 **Count**（計數），則報告會顯示較低的信任分數，或（針對特定流量類型）不顯示主機的項目。 • 惡意軟體 **URL** 造訪（範圍是 2–1000；預設為 5）— 根據惡意軟體與殭屍網路 URL 篩選類別識別使用者與已知惡意軟體 URL 的通訊。 • 使用動態 **DNS**（範圍是 2–1000；預設為 5）— 尋找可指示惡意軟體、殭屍網路通訊或入侵程式套件的動態 DNS 查詢流量。一般而言，使用動態 DNS 網域極具風險性。惡意軟體經常使用動態 DNS 來避免被列入 IP 位址封鎖清單。請考慮使用 URL 篩選來封鎖此類流量。 • 瀏覽至 **IP** 網域（範圍是 2–1000；預設為 10）— 識別瀏覽至 IP 網域而非 URL 的使用者。 • 瀏覽至最近註冊的網域（範圍是 2–1000；預設為 5）—尋找在過去 30 天內已註冊網域的流量。攻擊者、惡意軟體及入侵程式套件經常使用新註冊的網域。 • 來自未知站台的可執行檔（範圍是 2–1000；預設為 5）— 識別從未知 URL 下載的可執行檔。可執行檔是許多感染的一部分，與其他類型的可疑流量相結合時，可以幫助您排定主機調查的優先順序。
未知應用程式	定義確定報告是否包含與可疑不明 TCP 或不明 UDP 應用程式相關聯之流量的臨界值。 • 每小時的工作階段（範圍是 1-3600；預設為 10）—報告包括涉及每小時達到指定應用程式工作階段數目的流量。 • 每小時的目的地（範圍是 1-3600；預設為 10）— 報告包括涉及每小時達到指定應用程式目的地數目的流量。 • 最小位元組（範圍是 1-200；預設為 50）—報告包括應用程式承載等於或大於指定大小的流量。 • 最大位元組（範圍是 1-200；預設為 100）—報告包括應用程式承載等於或小於指定大小的流量。
IRC	選取此選項以包含涉及 IRC 伺服器的流量。

© 2019 Palo Alto Networks, Inc.

監控 > PDF 報告

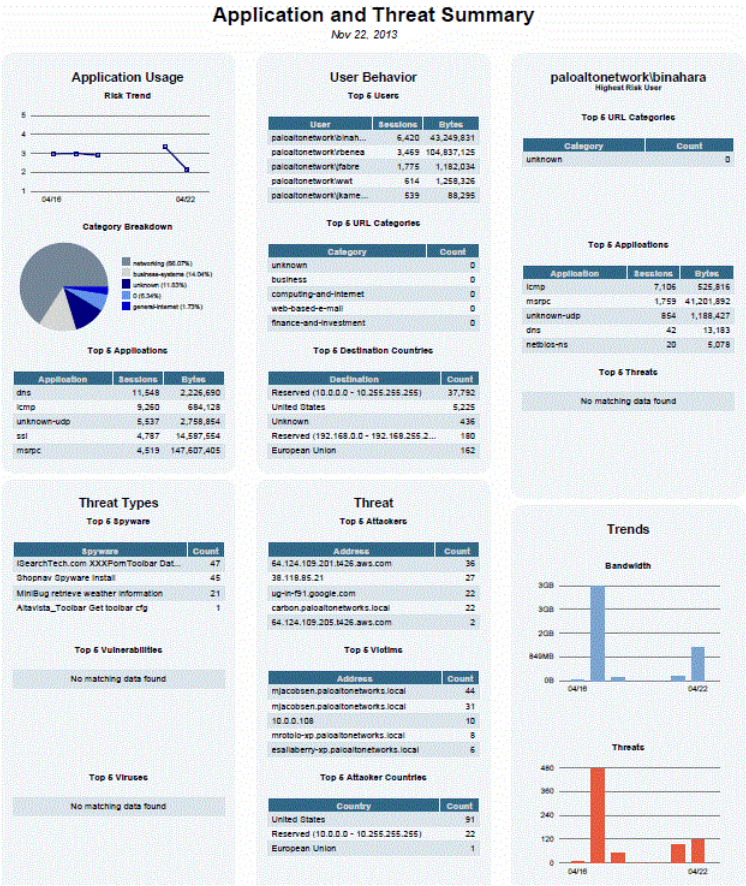
下列主題說明 PDF 報告。

- 監控 > PDF 報告 > 管理 PDF 摘要
- 監視 > PDF 報告 > 使用者活動報告
- Monitor > PDF Reports > SaaS Application Usage（監測 > PDF 報告 > SaaS 應用程式使用情況）
- Monitor > PDF Reports > Report Groups（監控 > PDF 報告 > 報告群組）
- 監視 > PDF 報告 > 電子郵件排程器

監控 > PDF 報告 > 管理 PDF 摘要

PDF 摘要報告包括從現有報告收集的資訊，這些報告以每個類別中的前 5 個 (而非前 50 個) 資料為基礎。報告也包括其他報告中不可用的趨勢圖表。

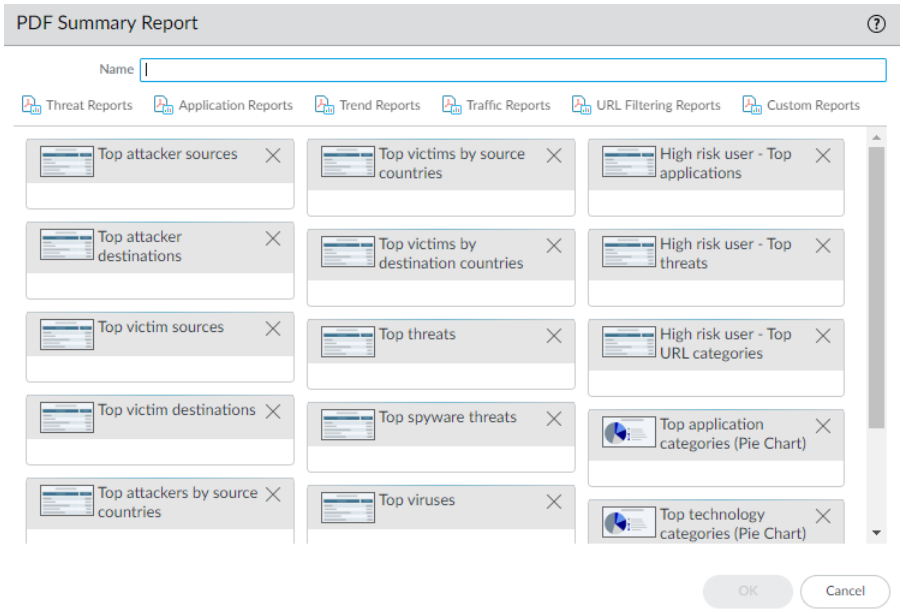
PDF 摘要報告



若要建立 PDF 摘要報告，請按一下 **Add**（新增）。**PDF Summary Report**（**PDF** 摘要報告）頁面會開啟，以顯示所有可用的報告元素。

管理 PDF 報告

© 2019 Palo Alto Networks, Inc.



使用下列一或多個選項來設計報告：

- 若要從報告中移除元素，請按一下刪除 ([X]) 或從相應的下拉式清單中清除項目。
- 在相應的下拉式清單中選取其他元件即可選取。
- 拖放元件以將其移動到報告的其他區域。

最多允許 *18* 個報告元素。如果已經有 *18* 個元素，您必須先刪除現有元素，才能新增元素。

若要 **Save**（儲存）報告，請輸入報告名稱，然後按一下 **OK**（確定）。

若要顯示 PDF 報告，請選取 **Monitor**（監控）> **Reports**（報告），按一下 **PDF Summary Report**（**PDF** 摘要報告）以選取報告，然後在行事曆中按一下日期以下載該日期的報告。

直到新的 *PDF* 摘要報告執行（每隔 *24* 小時自動發生於上午 *2* 點）後，該報告才會出現。

監視 > PDF 報告 > 使用者活動報告

使用此頁面建立摘要個別使用者或使用者群組活動的報告。按一下 **Add**（新增）並指定下列資訊。

使用者/群組活動報告設定	說明
名稱	輸入用來識別報告的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
類型	適用於使用者活動報告：選取 **User**（使用者），並輸入將成為報告主體之使用者的 **Username**（使用者名稱）或 **IP address**（IP 位址）（IPv4 或 IPv6）。
	適用於群組活動報告：選取 **Group**（群組）並輸入 **Group Name**（群組名稱）。
其他篩選器	選擇 **Filter Builder**（篩選器建立器）以建立使用者 / 群組活動報告篩選器。

© 2019 Palo Alto Networks, Inc.

使用者/群組活動報告設定	說明
時間週期	從下拉式清單中選取報告的時間範圍。
包含詳細瀏覽	（選用）選取此選項可在報告中包含詳細的 URL 日誌。 詳細瀏覽資訊可能包含所選使用者或使用者群組的大量日誌（數千個），並可能產生極大的報告。

群組活動報告不包含「*URL* 類別的瀏覽摘要」、「所有其他資訊跨使用者活動報告共用」和「群組活動報告」。

若要依需要執行報告，請按一下 **Run Now**（立即執行）。若要變更報告中顯示的最大列數，請參閱日誌記錄與報告設定。

若要儲存報告，請按一下 **OK**（確定）。您可以接著排程以電子郵件形式傳送的報告（監控 > PDF 報告 > 電子郵件排程器）。

新增日誌篩選

建立日誌篩選器以讓使用者活動和群組活動報告自訂報告。您可以依據應用程式、應用程式特性等篩選活動報告。舉例來說，如果您對沒有憑證的 SaaS 應用程式有興趣，即可建立一個依據該應用程式特性的篩選器。

新增日誌篩選器欄位	說明
日誌篩選器文字方塊	寫下您想要套用在日誌上的篩選器。您可以寫下多個篩選器。
連接器	以其他篩選選項附加此篩選器。對不適用您寫下篩選器的連接器，勾選 **Negate**（否定）核取方塊。
屬性	選擇您想要從功能表上附加的屬性。
運算子	選擇屬性是否等於或不等於值。
值	為屬性設定值。在可用時，將可使用附有可能值的下拉式功能表。

選擇 **Apply**（套用）以將建立篩選器套用在使用者活動或群組活動報告中。

Monitor > PDF Reports > SaaS Application Usage（監測 > PDF 報告 > SaaS 應用程式使用情況）

使用本頁以生成 SaaS 應用程式使用報告，其摘要與周遊於您網路的 SaaS 應用程式相關聯的安全性風險。此預定義報告呈現認可與未受認可的應用程式間的對比、摘要帶有不利託管特性的危險 SaaS 應用程式，以及透過在詳細資料頁面上列出每個類別的熱門應用程式，以突顯應用程式的活動、用法和合規性。您可對您要在網路上允許或封鎖的 SaaS 應用程式，使用此精細風險資料以強制執行政策。

如需產生正確且資訊充足的報告，您必須標記您網路上的認可應用程式（請參閱生成 SaaS 應用程式使用報告）。防火牆與 Panorama 會將無此預先定義標籤的任何應用程式，視為不可在網路上使用。務必了解您的

© 2019 Palo Alto Networks, Inc.

網路上頻繁出現的認可應用程式及不被認可應用程式，因為不被認可的 SaaS 應用程式對資訊安全是一個潛在威脅；它們未經核准用於您的網路，且存在威脅以及遺失私密與機敏資訊的風險。

確保以一致方式標記所有防火牆或設備群組中的應用程式。若相同的應用程式在一個虛擬系統上被標記為認可，在另一個系統或 *Panorama* 上卻被標記為不被認可；應用程式在上級設備群組中被標記為不被認可，在下級設備群組中卻被標記為認可（反之亦然），則 *SaaS* 應用程式使用情況報告將會產生重疊的結果。

在 ACC 上，將 *Application View*（應用程式檢視）設定為 *By Sanctioned State*（依認可狀態），以視覺方式識別在所有虛擬系統或設備群組中具有不同認可狀態的應用程式。綠色表示認可的應用程式，藍色表示不被認可的應用程式，而黃色表示在不同虛擬系統或設備群組中具有不同認可狀態的應用程式。

若要設定報告，請按一下 **Add**（新增），並指定下列資訊：

SaaS 應用程式使用情況報告設定	說明
名稱	輸入用來識別報告的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
時間週期	從下拉式清單中選取報告的時間範圍。此報告包括當天 (產生報告的那一天) 起的資料。
包含日誌來自	從下拉式清單中，選取要針對所選的使用者群組、所選的區域或針對防火牆或 Panorama 上設定的所有使用者群組和區域產生報告。 • 針對選取的使用者群組—選取防火牆或 Panorama 會篩選其日誌的 **User Group**（使用者群組）。 • 針對選取的區域—選取防火牆或 Panorama 會篩選其日誌的 **Zone**（區域）。 • 針對所有使用者群組和區域—您可以報告所有群組，或選擇要查看最多 25 個使用者群組。如果您有超過 25 個群組，防火牆或 Panorama 會顯示報告中的前 25 個群組，並將其他所有使用者群組指派給 Others（其他）群組。
包含報告中的使用者群組資訊 （不適用，前提是您選擇針對**Selected User Group**（選取的使用者群組）產生報告。）	此選項會篩選您要納入報告中之使用者群組的日誌。選取 **manage groups**（管理群組）或 **manage groups for the selected zone**（管理所選區域的群組）連結，以選擇要查看最多 25 個使用者群組。 針對所選區域的特定使用者群組產生報告時，不是所選群組成員的使用者會指派給名為 Others（其他）的使用者群組。
使用者群組	選取您要產生報告的使用者群組。只有當您選擇 **Include logs from**（包含日誌來自）下拉式清單中的 **Selected User Group**（選取的使用者群組）時，才會顯示此選項。
區	選取您要產生報告的區域。只有當您選擇 **Include logs from**（包含日誌來自）下拉式清單中的 **Selected Zone**（選取的區域）時，才會顯示此選項。 您可以接著選取在報告中包含使用者群組資訊。
在報告中包括詳細的應用程式類別資訊	SaaS 應用程式使用情況 PDF 報告由兩部分組成。依預設，報告產生時有兩個部分。報告第一部分（10 頁）聚焦在報告期間在網路上使用的 SaaS 應用程式。 如果您不想要報告的第二部分包括第一部分中所列各應用程式子類別的 SaaS 和非 SaaS 應用程式的詳細資訊，則清除此選項。此報告第二部分包括各子類別前幾大

© 2019 Palo Alto Networks, Inc.

SaaS 應用程式使用情況報告設定	說明
	應用程式的名稱，以及使用者、使用者群組、檔案、傳輸的位元組及這些應用程式所產生的威脅等相關資訊。 若不包括詳細資訊，則報告長度為 10 頁。
報告中的子類別上限	選取是否要在 SaaS 應用程式使用情況報告中使用所有應用程式子類別，或將最大數目限制為 10、15、20 或 25 個子類別。 當您減少最大子類別數目時，詳細的報告會縮短，因為您限制了報告中包含的 SaaS 和非 SaaS 應用程式活動資訊。

按一下 **Run Now**（立即執行）以視需要產生報告。

您可以依需求生成此報告，或可以排程，以定期每日、每週或每月執行。若要將此報告排程，請參閱排程報告以進行電子郵件傳送。

在 PA-220 和 PA-220R 防火牆上，不會將 SaaS 應用程式使用情況當作電子郵件中的 PDF 附件來傳送。反之，電子郵件會包含用以在 Web 瀏覽器中開啟報告的連結。

如需報告的詳細資訊，請參閱管理報告。

Monitor > PDF Reports > Report Groups（監控 > PDF 報告 > 報告群組）

報告群組可讓您建立系統可視作單一彙總 PDF 報告的報告集（包含可選標題頁面以及所有組成的報告），進行編譯與傳送。

報告群組設定	說明
名稱	輸入用來識別報表群組的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
標題頁面	選取此選項以將標題頁面包含在報告中。
Title（職稱）	輸入將顯示為報告標題的名稱。
報告選項/Widget	對於要包含在群組中的每個報告，選取左欄中的報告並將其 **Add**（新增）到右欄。您可以選取下列報告類型： • 預先定義的報告 • 自訂報表 • PDF 摘要報告 • Csv • 日誌檢視—每當您建立自訂報告時，防火牆就會自動建立同名的日誌檢視報告。日誌檢視報告會顯示防火牆用於建立自訂報告內容的日誌。若要包括日誌檢視資料，在建立報告群組時，請新增您的 **Custom Reports**（自訂報告），然後新增相符的 **Log View**（日誌檢視）報告。針對報告群組產生的彙總報告會顯示後面加上日誌資料的自訂報告資料。 在儲存報告群組之後，[報告群組]頁面的 Widget 欄會列出您新增至群組的報告。

© 2019 Palo Alto Networks, Inc.

若要使用報告群組，請參考 [監控 > PDF 報告 > 電子郵件排程器]。

監視 > PDF 報告 > 電子郵件排程器

使用電子郵件排程器，排程以電子郵件形式傳送的報告。新增排程之前，您必須定義報告群組與電子郵件設定檔。請參考 [監控 > PDF 報告 > 報告群組] 和 [設備 > 伺服器設定檔 > 電子郵件]。

排程報告於 2:00 AM 開始執行，當所有排程報告結束執行後，會進行電子郵件轉寄。

電子郵件排程器設定	說明
名稱	輸入用來識別排程的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
報告群組	選取您想要排程的報告群組（監控 > PDF 報告 > 報告群組）或 SaaS 應用程式使用情況報告（監控 > PDF 報告 > SaaS 應用程式使用情況）。
電子郵件設定檔	選取定義電子郵件設定的設定檔。如需定義電子郵件設定檔的資訊，請參考 [設備 > 伺服器設定檔 > 電子郵件]。
週期性	選取產生及傳送報告的頻率。
覆寫電子郵件地址	輸入可選電子郵件地址，以覆寫在電子郵件設定檔中指定的收件人。
傳送測試電子郵件	按一下此選項可將測試電子郵件傳送至所選 **Email Profile**（電子郵件設定檔）中定義的電子郵件地址。

© 2019 Palo Alto Networks, Inc.

監控 > 管理自訂報告

您可以建立自訂報告，視需要或依排程執行（每晚）。若需預定義報告，選擇 **Monitor**（監視）> **Reports**（報告）。

防火牆產生排程的自訂報告後，如果修改了報告設定以變更未來的輸出，則會有使該報告過去的結果變為無效的風險。如果需要修改已排程報告的設定，最佳做法是建立新報告。

Add（新增）自訂報告以建立新報告。若要讓報告以現有範本為基礎，請按一下 **Load Template**（載入範本）並選取範本。若要視需要（而不是根據 **Scheduled**（已排程）時間）產生報告，請按一下 **Run Now**（立即執行）。指定下列設定來定義報告。

自訂報告設定	說明
名稱	輸入用來識別報告的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入自訂報告的說明。
Database	選擇可作為報告的資料來源使用的資料庫。
已排程	選取此選項可每晚執行報告。然後選取 **Monitor**（監控）> **Reports**（報告），即可使用此報告。
時間範圍	選擇固定的時間範圍，或選擇 **Custom**（自訂）並指定日期與時間範圍。
排序方式	選擇排序選項以組織報表，包括要包含在報表中的資訊量。可用選項視選擇的資料庫而定。
分組方式	選擇群組選項以組織報表，包括要包含在報表中的資訊量。可用選項視選擇的資料庫而定。
欄	選取可用欄可包含於自訂報告中，並將其新增（⊕）至選取欄。選取 **Up**（上移）、**Down**（下移）、**Top**（頂部）及 **Bottom**（底部），將所選的欄重新排序。您亦可視需要選取及移除（⊖）之前選取的欄。
查詢建立器	若要建立報告查詢，請指定下列項目並按一下 **Add**（新增）。視需要重複操作來建構完整查詢。 • **Connector**（連接器）— 選擇連接器（**and** 或 **or**）來優先處理您要新增的表示式。 • **Negate**（否定）— 選取此選項可將查詢解譯為否定。在之前的範例中，否定選項可導致對不在過去 24 小時內或非來自不信任區域的項目進行比對。 • **Attribute**（屬性）—選擇資料元素。可用選項視選擇的資料庫而定。 • **Operator**（運算子）—選擇準則以決定是否套用屬性（例如 =）。可用選項視選擇的資料庫而定。 • **Value**（值）—指定要比對的屬性值。

如需詳細資訊，請參閱產生自訂報告。

© 2019 Palo Alto Networks, Inc.

監控 > 報告

防火牆會提供前一天或上週所選日期流量統計資料的各種「前 50 個」報告。

若要檢視報告，請展開頁面右邊的報告類別（例如自訂報告）並選取報告名稱。此頁面會在各節中列出報告。您可以檢視所選時段的每個報告中的資訊。

依預設，防火牆會顯示上一個行事曆日期的所有報告。若要檢視其他日期的報告，請在頁面右下角的行事曆中選取報告產生日期。

若要在防火牆以外的系統上檢視報告，請選取匯出選項：

- 匯出為 **PDF**
- 匯出為 **CSV**
- 匯出為 **XML**

© 2019 Palo Alto Networks, Inc.

政策

下列主題說明防火牆政策類型、如何移動或複製政策，以及說明政策設定：

> 政策類型
> 移動或複製原則規則
> 稽核註解封存檔
> 規則使用方式命中數查詢
> Policies > Security（原則 > 安全性）
> Policies > NAT（原則 > NAT）
> Policies > QoS（原則 > QoS）
> Policies > Policy Based Forwarding（原則 > 基於原則的轉送）
> Policies > Decryption（原則 > 解密）
> Policies > Tunnel Inspection（原則 > 通道檢查）
> Policies > Application Override（原則 > 應用程式取代）
> Policies > Authentication（原則 > 驗證）
> Policies > DoS Protection（原則 > DoS 保護）
> Policies > SD-WAN（政策 > SD-WAN）

政策類型

原則可讓您強制執行規則及自動化動作來控制防火牆的作業。防火牆支援下列原則類型：

- 基本安全性原則，可根據應用程式、來源與目的地區域和位址，也可根據服務（連接埠與通訊協定）（選用），來封鎖或允許網路工作階段。區域會識別傳送或接收流量的實體或邏輯介面。請參閱 Policies > Security（原則 > 安全性）。
- 網路位址轉譯 (NAT) 原則，可轉譯位址與連接埠。請參閱 Policies > NAT（原則 >NAT）。
- 頻寬管理機制 (QoS) 原則，決定在啟用 QoS 的情況下，當流量通過介面時，應如何分級流量來進行處理。請參閱 Policies > QoS（原則 > QoS）。
- 基於原則的轉送原則，可取代路由表並指定流量的輸出介面。請參閱 Policies > Policy Based Forwarding（原則 > 基於原則的轉送）。
- 解密原則，可為安全原則指定流量進行解密分析。每個原則皆可為您要解密的流量指定 URL 類別。除 SSH shell 存取以外，SSH 解密還可用於識別與控制 SSH 通道。請參閱 Policies > Decryption（原則 > 解密）。
- 通道檢查原則用於在通道流量上強制執行安全性、DoS 保護、QoS 原則，並檢視通道活動。請參閱 Policies > Tunnel Inspection（原則 > 通道檢查）。
- 覆蓋原則，可覆蓋防火牆所提供的應用程式定義。請參閱 Policies > Application Override（原則 > 應用程式取代）。
- 驗證原則用於針對存取網路資源的一般使用者定義驗證。請參閱 Policies > Authentication（原則 > 驗證）。
- 阻斷式攻擊 (DoS) 原則可防止遭受 DoS 攻擊，並在回應規則相符情況時採取保護動作。請參閱 [原則 > DoS 保護]。
- SD-WAN 政策用於確定在連結路徑健康情況下降到低於經批准的設定健康情況公制時，來源與目的地區域之間的連結路徑管理。請參閱政策 > SD-WAN。

從 Panorama™ 推送的共用原則會在防火牆 Web 介面上會以橙色顯示。您僅可以在 Panorama 上編輯這些共用原則；您無法在防火牆上編輯它們。

以群組形式檢視規則庫 如果要檢視在一個規則庫中使用的所有頁籤群組。在具有許多規則的規則庫中，呈現頁籤、顏色代碼，以及每個群組中的規則數量能夠為以群組檢視規則庫進行簡化，但仍保留建立的規則階層。

© 2019 Palo Alto Networks, Inc.

移動或複製原則規則

移動或複製原則 時，您可以指派您擁有存取權限的 **Destination**（目的地）（防火牆上的虛擬系統或 Panorama 上的裝置群組），包括 [共用] 位置。

若要移動原則規則，請在 **Policies**（原則）頁籤中選取規則，按一下 **Move**（移動），選取 **Move to other vsys**（移至其他虛擬系統）（僅限防火牆）或 **Move to different rulebase or device group**（移至不同的規則庫或裝置群組）（僅限 Panorama），指定下表中的欄位，接著按一下 **OK**（確定）。

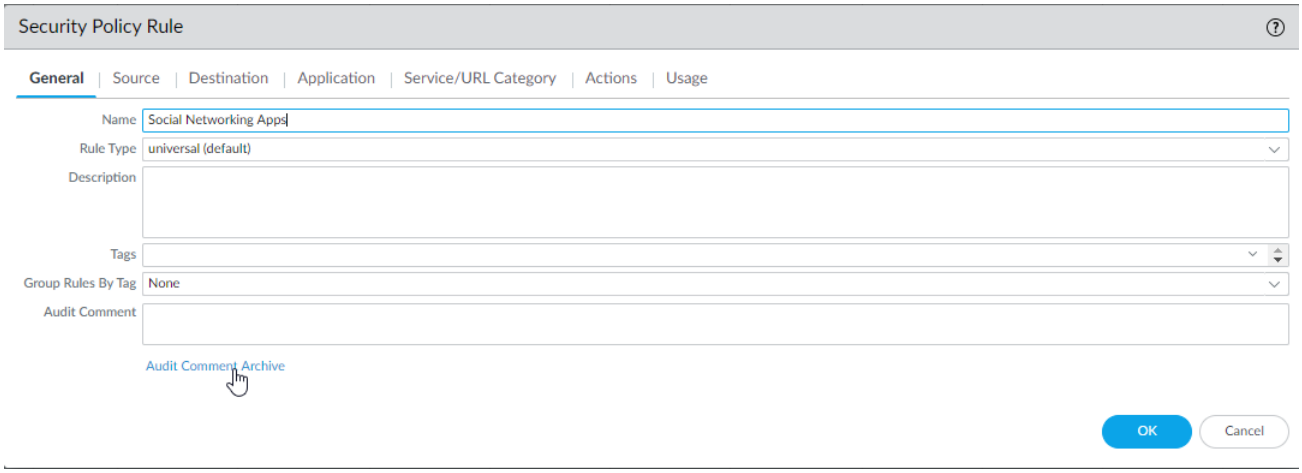
若要複製原則規則，請選取 **Policies**（原則）頁籤中的規則，按一下 **Clone**（複製），指定下表中的欄位，接著按一下 **OK**（確定）。

移動/複製設定	說明
選取的規則	顯示針對該操作所選原則規則的名稱和目前位置（虛擬系統或裝置群組）。
目的地	選取原則或物件的新位置：虛擬系統、裝置群組或 [共用]。預設值為您在 **Policies**（原則）或 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）或 **Device Group**（裝置群組）。
規則順序	選取相對其他規則的規則位置： • 移至頂部 — 規則將位於所有其他規則之前。 • 移至底部 — 規則將位於所有其他規則之後。 • 規則前 — 在相鄰的下拉式清單中，選取後續規則。 • 規則後 — 在相鄰的下拉式清單中，選取之前的規則。
驗證中第一次偵測到錯誤時離開	選取此選項（預設為已選取）以確保防火牆或 Panorama 顯示找到的第一個錯誤，並停止尋找其他錯誤。例如，若目的地不包括您要移動之原則規則所參照的物件，則會發生錯誤。如果清除此選項，防火牆或 Panorama 將會找出所有錯誤，然而顯示這些錯誤。

© 2019 Palo Alto Networks, Inc.

稽核註解封存檔

選取 **Audit Comment Archive**（稽核註解封存檔）即可檢視選定規則的稽核註解歷程記錄、組態日誌和規則變更歷程記錄。



- 稽核註解
- 組態日誌（認可之間）
- 規則變更

稽核註解

檢視選定原則規則的 **Audit Comment**（稽核註解）歷程記錄。套用並儲存篩選，可快速識別特定稽核註解並以 CSV 格式匯出顯示的稽核註解。

欄位	說明
認可時間	提交稽核註解的時間。
稽核註解	稽核註解的內容。
管理員	新增或變更了稽核註解的使用者。
組態版本	組態修訂版本。0 表示第一次建立原則規則並將其提交至 Panorama。

組態日誌（認可之間）

檢視在兩次提交之間選定原則規則產生的組態日誌。套用並儲存篩選，可快速識別特定組態日誌並以 CSV 格式匯出顯示的組態日誌。

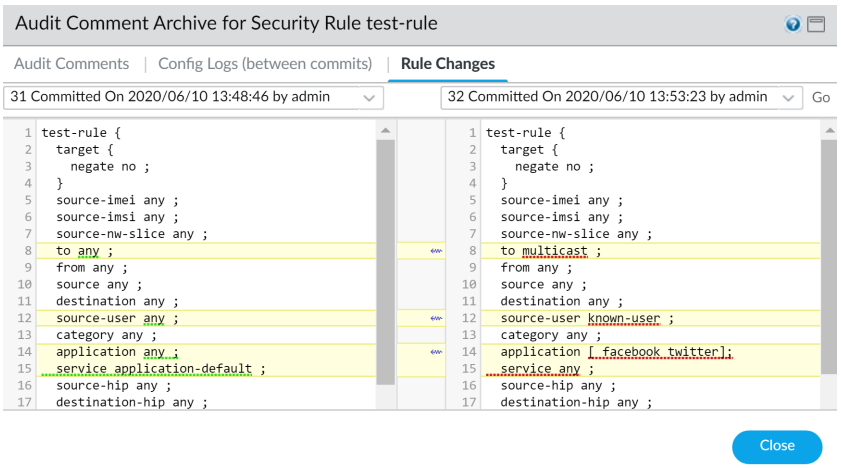
欄位	說明
時間	提交稽核註解的時間。
管理員	稽核註解的內容。

© 2019 Palo Alto Networks, Inc.

欄位	說明
命令	所執行命令的類型。
變更前	變更前的規則資訊。例如，若您重新命令規則，則會顯示之前的名稱。
變更後	變更後的規則資訊。例如，若您重新命令規則，則會顯示新名稱。
裝置名稱	稽核註解變更前的裝置名稱。

規則變更

檢視並比較所選原則規則的組態版本，以分析發生了哪些變更。在下拉式清單中，選取兩個您要進行比較的原則規則組態版本。



© 2019 Palo Alto Networks, Inc.

規則使用方式命中數查詢

- **Policies**（原則）> **Rule Usage**（規則使用情況）

使用規則使用方式查詢，以在指定時段內篩選選定的規則庫。規則使用方式查詢允許您快速篩選原則規則庫，以識別要移除的未使用規則，從而可針對攻擊者減少開放進入點。按一下 **PDF/CSV** 可以 PDF 或 CSV 格式匯出經篩選的規則。若要使用「規則使用方式命中數查詢」，則必須啟用 **Policy Rule Hit Count**（原則規則命中數）設定 (Device > Setup > Management（裝置 > 設定 > 管理）)。

依預設，在原則規則庫中查詢規則使用方式時，會顯示 **Name**（名稱）、**Location**（位置）、**Created**（已建立）、**Modified**（已修改）以及 **Rule Usage**（規則使用方式）欄位。您可以新增更多欄以檢視有關原則規則的其他資訊。

工作	說明
命中數	
時間範圍	指示查詢選定規則庫的時間範圍。從預先確定的時間範圍內選取，或設定 **Custom**（自訂）時間範圍。
使用方式	選取要查詢的規則使用方式：**Any**（任何）、**Unused**（未使用）、**Used**（已使用）或 **Partially Used**（已部分使用）（僅 Panorama）。
自從	（僅自訂時間範圍）選取查詢原則規則庫的日期與時間。
排除在過去 _ 天重設的規則	選取此選項可排除使用者在指定天數內手動重設的所有規則。
動作	
刪除	刪除一個或多個所選政策規則。
啟用	在停用狀態下啟用一個或多個所選政策規則。
停用	停用一個或多個所選政策規則。
PDF/CSV	匯出目前以 PDF 或 CSV 格式顯示的篩選政策規則。
重設規則命中計數器	對於經過篩選且目前顯示的 **Selected rules**（選定規則）或 **All rules**（所有規則），重設其規則使用情況資料。
頁籤	將一個或多個群組標籤套用至一個或多個所選政策規則。群組標籤必須已經存在才可標記政策規則。
取消標記	從一個或多個所選政策規則中移除一個或多個群組標籤。

規則命中數查詢的裝置規則使用方式

從 Panorama 管理伺服器檢視原則規則的規則使用方式時，可以檢視裝置和虛擬系統規則使用方式。**Reset Rule Hit Counter**（重設規則命中數），可重設「命中數」、「第一次命中」與「最後一次命中」。

按一下 **PDF/CSV** 可以 PDF 或 CSV 格式匯出經篩選的規則。

© 2019 Palo Alto Networks, Inc.

欄位	說明
裝置群組	裝置或虛擬系統所屬的裝置群組。
裝置名稱/虛擬系統	裝置群組或虛擬系統的名稱。
命中數	符合原則規則的流量總數。
最後命中	流量最近符合原則規則的日期與時間。
首次命中	流量第一次符合原則規則的日期與時間。
接收到上次更新	上次從裝置至 Panorama 管理伺服器接收規則使用方式資訊的日期與時間。
已建立	原則規則建立的日期與時間。
已修改	原則規則上次修改的日期與時間。若未修改原則規則，則將欄位留空。
狀態	裝置的連線狀態：`Connected`（已連線）或 `Disconnected`（已中斷連線）。

© 2019 Palo Alto Networks, Inc.

Policies > Security（原則 > 安全性）

安全性原則規則會參考安全性區域，並可讓您根據應用程式、使用者或使用者群組及服務（連接埠和通訊協定）允許、限制及追蹤網路上的流量。依預設，本防火牆包括名為 *rule1* 的安全性規則，並允許信任區域到不信任區域的所有流量。

您想了解什麼內容？	請參閱：
何謂安全性原則？	安全性原則概要 針對 Panorama，請參閱移動或複製原則規則
可用來建立安全性原則規則的欄位有哪些？	安全性原則規則中的建置組塊
如何使用 Web 介面來管理安全性原則規則？	建立和管理原則 取代或還原安全性原則規則 應用程式與使用情況 安全性政策最佳化工具
想知道更多？	安全性原則

安全性原則概要

安全性原則可讓您強制執行規則並採取行動，且可視需求做為一般或特定原則。會由上而下針對連入流量逐一與各原則進行比較，由於已套用符合流量的第一個規則，因此更特定的規則必須在更一般的規則之前。例如，如果其他所有流量相關設定都相同，單一應用程式規則必須在所有應用程式規則之前。

為確保當一般使用者嘗試存取您的網路資源時會驗證，防火牆在評估安全性原則前會評估驗證原則。如需詳細資訊，請參閱 *[原則 > 驗證]*。

當流量不符合任何使用者定義規則時，則會套用預設規則。會預先定義預設規則（顯示於安全性規則庫底部）來允許所有區域內流量和拒絕所有區域間流量。雖然這些規則是預先定義之設定的一部分，且預設為唯讀，但您可以 **Override**（取代）它們並變更限制的設定數量，包括頁籤、動作（允許或拒絕）、日誌設定和安全性設定檔。

介面包括下列定義安全性原則規則的頁籤。

- 一般—選取 **General**（一般）頁籤可設定安全性原則的名稱和說明。
- 來源—使用 **Source**（來源）頁籤可定義流量源自的來源區域或來源位址。
- 使用者 — 使用 **User**（使用者）頁籤針對個別使用者或使用者群組強制執行原則。若是在啟用主機資訊設定檔 (HIP) 的情況下使用 GlobalProtect™，您也可以讓原則根據 GlobalProtect 收集的資訊執行。例如，使用者的存取等級可由 HIP 決定，HIP 會通知防火牆使用者的本機組態。根據正在主機上執行的安全性程式、登錄值，以及許多其他檢查，例如主機是否已安裝防毒軟體，HIP 資訊可用於更精確的控制存取。
- 目的地 — 使用 **Destination**（目的地）頁籤定義流量的目的地區域或目的地位址。
- 應用程式 — 使用 **Application**（應用程式）頁籤，根據應用程式或應用程式群組執行原則動作。管理員也可以使用現有的 App-ID™ 特徵碼，並自訂該特徵碼來偵測所有權應用程式或偵測現有應用程式上的特定屬性。可在 **Objects**（物件）> **Applications**（應用程式）中定義自訂的應用程式。
- 服務/URL 類別—在原則中選取 **Service/URL Category**（服務/URL 類別）頁籤以指定特定的 TCP 和/或 UDP 埠號或 URL 類別作為比對準則。

© 2019 Palo Alto Networks, Inc.

- **Actions**（動作）—使用 **Action**（動作）頁籤可決定將根據定義的政策屬性所符合的流量，執行哪些動作。
- **Target**（目標）—選取 **Target**（目標）頁籤，為安全性政策規則指定裝置或標籤。
- **Usage**（使用方式）—選取 **Usage**（使用方式）頁籤以檢視一項規則的使用方式，包括規則檢視的應用程式數量、此規則最後一次檢視到新的應用程式的時間、命中計數資料、過去 30 天的流量以及規則建立和上次編輯的時間。

安全性原則規則中的建置組塊

- Policies > Security（原則 > 安全性）

下節說明安全性原則規則中的各個元件。當您建立安全性原則規則時，您可以設定這裡所說明的選項。

在安全性原則中建立區塊	設定位置	說明
規則編號	無	防火牆會為每個規則自動編號，規則的順序會隨著規則移動而改變。當您篩選規則以符合特定篩選器時，會在規則庫中完整規則集的內容中顯示每個規則及其編號，及其在評估順序中的位置。 Panorama 獨立地為預先規則以及後續規則編號。當 Panorama 將規則推送至受管理的防火牆時，規則編號方式會納入預先規則中的階層、防火牆規則及規則庫內的後續規則，並反映規則順序及其評估順序。
名稱	總言	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
規則類型		指定將規則套用至區域中和 / 或區域之間的流量： • 通用（預設值）—將規則套用至指定的來源和目的地區域中所有符合的區域間和區域內流量。例如，如果您以來源區域 A 和 B 以及目的地區域 A 和 B 建立通用規則，則會將規則套用至區域 A 中的所有流量、區域 B 中的所有流量，以及區域 A 到區域 B 的所有流量，和區域 B 到區域 A 的所有流量。 • 區域內—將規則套用至指定的來源區域（無法為區域內規則指定目的地區域）中的所有符合流量。例如，如果將來源區域設定為 A 和 B，則會將規則套用至區域 A 中的所有流量和區域 B 中的所有流量，但不會套用至區域 A 與區域 B 之間的流量。 • 區域間 — 將規則套用至指定的來源與目的地區域之間的所有符合流量。例如，如果將來源區域設為 A、B 和 C，並將目的地區域設為 A 和 B，則會將規則套用至區域 A 到區域 B 的流量、區域 B 到區域 A 的流量、區域 C 到區域 A 的流量，及區域 C 到區域 B 的流量，但不會套用至區域 A、B 或 C 中的流量。
說明		輸入政策的說明（最多 1,024 個字元）。
標籤		指定原則的頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		分實用。例如，您可能想要使用特定文字（如「解密」與「無解密」）標記特定規則，或針對與該位置相關聯的原則使用特定資料中心名稱。 您也可以將頁籤新增至預設規則。
來源區域	**Source**（來源）	**Add**（新增）來源區域（預設為 **Any**（任何））。區域的類型必須相同（第二層第三層或 Virtual Wire）。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。
來源位址	**Source**（來源）	**Add**（新增）來源位址、位址群組或區域（預設為 **Any**（任何））。從下拉式清單中選取，或從下拉式清單底部選取 **Address**（位址）物件、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。物件>位址以及物件>位址群組分別描述安全性原則規則支援的位址物件以及位址群組的類型。 選取 **Negate**（否定）選項會將規則從指定區域應用於來源位址，但指定的位址除外。
來源使用者	**Source**（來源）	**Add**（新增）受限於此原則的來源使用者或使用者群組： • 任何 — 包含任何流量，不論使用者資料為何。 • 預先登入 — 包含使用 GlobalProtect 連線至網路，但未登入其系統的遠端使用者。在 [入口網站] 上設定 GlobalProtect 端點的 [預先登入] 選項時，將以使用者名稱預先登入識別目前未登入其電腦的任何使用者。您接著可為預先登入使用者建立原則，且使用者即便未直接登入，也會在網域上驗證其電腦，如同這些使用者已完全登入一般。 • 已知使用者—包含所有驗證的使用者，意味已對應使用者資料的任何 IP 位址。此選項等同於網域上的網域使用者群組。 • 未知—包含所有未驗證的使用者，意味未對應至使用者的 IP 位址。例如，您可以使用 **unknown**（未知），供來賓等級的使用者存取某些資訊，因為他們雖然在您的網路上擁有 IP 位址，但不會經過網域驗證，且在防火牆上沒有 IP 位址至使用者對應資訊。 • 選取 — 包含此視窗中選項所決定的所選使用者。例如，您可能想要新增一名使用者、個人清單、部分群組，或手動新增使用者。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。
來源裝置	**Source**（來源）	根據政策 **Add**（新增）主機裝置： • **any**（任何）—包括任何裝置。

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		• **no-hip**（無 **HIP**）—不需要 HIP 資訊。此設定可用來從無法收集或提交 HIP 資訊的第三方裝置進行存取。 • **quarantine**（隔離）—包含隔離清單中的任何裝置（**Device**（裝置）> **Device Quarantine**（裝置隔離））。 • **select**（選取）—包含依據組態而確定的選定裝置。例如，您可以根據型號、作業系統、作業系統系列或供應商新增裝置物件。
來源 HIP 設定檔	**Source**（來源）	**Add**（新增）host information profile（主機資訊設定檔 - HIP）可讓您收集主機安全性狀態的相關資訊，例如它們是否已安裝最新的安全性修補程式以及防毒定義。針對原則強制執行使用主機訊息設定檔會啟用精細安全性，其可確保在獲得允許存取您的網路資源之前，存取您的關鍵資源的遠端主機能夠受到適當維護並嚴格遵守您的安全性標準。支援的來源 HIP 設定檔如下： • **any**（任何）—包含任何端點，無論 HIP 資訊為何。 • **select**（選取）—包含選取透過您設定決定的 HIP 設定檔。例如，您可以新增一個 HIP 設定檔、HIP 設定檔清單，或您可以手動新增 HIP 設定檔。 • **no-hip**（無 **HIP**）—不需要 HIP 資訊。此設定可用來從無法收集或提交 HIP 資訊的第三方用戶端進行存取。
來源用戶	**Source**（來源）	使用以下格式在 5G 或 4G 網路中 **Add**（新增）一個或多個來源用戶： • **Any**（任何） • （僅限 5G）5G 訂閱永久識別碼 (SUPI)，包括 IMSI • IMSI（14 或 15 位數） • IMSI 值的範圍是 11 至 15 位數，以連字號分隔 • IMSI 前綴為六位數字，前綴後帶有星號 (*) 作為萬用字元 • 指定 IMSI 的 EDL
來源設備		使用以下格式在 5G 或 4G 網路中 **Add**（新增）一個或多個來源設備 ID： • **Any**（任何） • （僅限 5G）5G 永久設備識別碼 (PEI)，包括國際行動設備身份 (IMEI) • IMEI（長度為 11 至 16 位數） • 類型指派代碼 (TAC) 的八位數 IMEI 前綴 • 指定 IMEI 的 EDL

網路切片	**Source**（來源）	在 5G 網路中，根據網路切片服務類型 (SST)，**Add**（新增）一個或多個來源網路切片，如下所示：
		• 標準化（預先定義）**SST**
		  • **eMBB**（增強的行動頻寬）—用於更快的速度和更高的資料速率，例如影片串流。
		  • **URLLC**（超可靠的低延遲通訊）—適用於對延遲敏感的關鍵任務應用程式，例如關鍵物聯網（醫療保健、無線支付、家庭控制與車輛通訊）。

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		• **MIoT**（大型物聯網）—例如，智慧電錶、智慧廢物管理、防盜、資產管理與位置追蹤。 • 網路切片 **SST** - 營運商特定—命名並指定切片。切片名稱的格式為文字，後跟逗點 (,) 和數字（範圍是 128 至 255）。例如，Enterprise Oil2,145。
目的地區域	目的地	**Add**（新增）目的地區域（預設為 **any**（任何））。區域的類型必須相同（第二層第三層或 Virtual Wire）。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。 您無法在區域內規則上定義目的地區域，因為這些類型的規則僅比對相同區域中的來源和目的地流量。若要指定符合內部網路區規則的區域，只需要設定來源區域。
目的地位址		**Add**（新增）目的地位址、位址群組或區域（預設為 **Any**（任何））。從下拉式清單中選取，或從下拉式清單底部按一下 **Address**（位址）物件、**Address Group**（位址群組）或 **Regions**（區域），然後指定位址設定。物件>位址以及物件>位址群組分別描述安全性原則規則支援的位址物件以及位址群組的類型。 選取 **Negate**（否定）選項會將規則應用於指定區域中的目的地位址，但指定的位址除外。
目的地裝置		根據政策 **Add**（新增）主機裝置： • **any**（任何）—包括任何裝置。 • **quarantine**（隔離）—包含隔離清單中的任何裝置（**Device**（裝置）> **Device Quarantine**（裝置隔離））。 • **select**（選取）—包含依據組態而確定的選定裝置。例如，您可以根據型號、作業系統、作業系統系列或供應商新增裝置物件。
應用程式	應用程式	**Add**（新增）安全性規則的特定應用程式。如果應用程式具有多個功能，您可以選取整個應用程式或個別功能。如果您選取整個應用程式，會包含所有功能，且會在新增未來功能後自動更新應用程式定義。 如果您在安全性原則規則中使用應用程式群組、篩選或容器，可以懸停在 Application（應用程式）欄中的物件，開啟下拉式清單，並選取 **Value**（值），檢視這些物件的詳細資訊。這可以讓您直接從原則檢視應用程式成員，而不需要導覽至 **Object**（物件）頁籤。 請務必指定一個或多個應用程式，讓您的網路僅允許您希望的應用程式，從而減少攻擊面向並使您可以更好地控制網絡流量。請勿將應用程式設

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		定為 *any*（任何），這會允許任何應用程式的流量，並增加攻擊面向。
服務	服務/URL 類別	選取您想要將其限制在特定 TCP 或 UDP 埠號內的服務。從下拉式清單中選取下列選項之一： • 任何—任何通訊協定或連接埠上都允許或拒絕所選應用程式。 • 應用程式預設值—僅在 **Palo Alto Networks®** 定義的預設連接埠上允許或拒絕選取的應用程式。建議將此選項用於允許原則，因為它能防止應用程式在異常的連接埠和通訊協定上執行，即使不是蓄意的行為，也可能是不想要的應用程式行為和用法出現的徵兆。 使用此選項時，防火牆仍將檢查所有連接埠上的所有應用程式，但應用程式只能在其預設的連接埠和通訊協定上執行。 對於大多數應用程式，使用 *application-default*（應用程式預設值）來防止應用程式使用非標準連接埠或表現出其他規避性行為。如果應用程式的預設連接埠發生變更，防火牆會自動將規則更新為正確的預設連接埠。對於使用非標準連接埠的應用程式（如內部自訂應用程式），請修改應用程式或建立指定非標準連接埠的規則，並僅將規則套用至需要應用程式的流量。 • **Select**（選取）—**Add**（新增）現有的服務或選取**Service**（服務）或**Service Group**（服務群組），指定新項目。（或選取 [物件 > 服務] 和 [物件 > 服務群組]）。
URL 類別		選取安全性規則的 URL 類別。 • 選取 **any**（任何）可允許或拒絕所有工作階段，無論 URL 類別為何。 • 若要指定類別，從下拉式清單中**Add**（新增）一個或多個特定類別（包括自訂類別）。選取 [物件 > 外部動態清單] 可定義自訂類別。
動作設定	動作	選取防火牆對流量採取的 **Action**（動作），此動作與規則中定義的屬性相符： • **Allow**（允許）（預設）—允許相符的流量。 • **Deny (拒絕)**—封鎖比對的流量並強制執行針對要拒絕之應用程式定義的預設*Deny Action*（拒絕動作）。若要檢視依預設為應用程式定義的拒絕動作、檢視應用程式詳細資料（**Objects**（物件）> **Applications**（應用程式））。 由於預設拒絕動作會因應用程式有所不同，因此防火牆可針對某一應用程式封鎖工作階段並傳送重設，同時可無訊息丟棄其他應用程式的工作階段。

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		• **Drop**（丟棄）—無訊息丟棄應用程式。TCP 重設不會傳送至主機或應用程式，除非您選取 **Send ICMP Unreachable**（傳送 **ICMP** 無法連線）。 • **Reset client**（重設用戶端）—傳送 TCP 重設至用戶端裝置。 • **Reset server**（重設伺服器）—傳送 TCP 重設至伺服器裝置。 • **Reset both client and server**（重設用戶端與伺服器）—傳送 TCP 重設至用戶端及伺服器裝置。 • 傳送 **ICMP** 無法連線—僅適用於第三層介面。當您將安全性原則規則設定為丟棄流量或重設連線時，流量將不會抵達目的地主機。在這些情況下，針對丟棄的所有 UDP 流量和 TCP 流量，您可讓防火牆傳送 ICMP 無法連線回應至流量源自的來源 IP 位址。啟用此設定可讓來源適當地關閉或清除工作階段並防止應用程式中斷。 若要檢視在防火牆上設定的 ICMP 無法連線封包速率，請檢視工作階段設定（**Device**（裝置）> **Setup**（設定）> **Session**（工作階段））。 若要取代在預先定義的區域間和區域內規則中定義的預設動作，請參閱取代或還原安全性原則規則。
設定檔設定	動作	若要指定防火牆對符合安全性設定檔規則的封包執行的其他檢查，請選取個別防毒、弱點保護、反間諜軟體、URL 篩選、檔案封鎖、資料篩選、WildFire 分析、行動網路保護和 SCTP 保護設定檔。 若要指定設定檔群組，而非個別設定檔，請選取 **Profile Type**（設定檔類型）為 **Group**（群組），然後選取一個 **Group Profile**（群組設定檔）。 若要定義新的設定檔或設定檔群組，請按一下相應的設定檔旁的 **New**（新增），或選取 **New Group Profile**（新建群組設定檔）。 您也可將安全性設定檔（或設定檔群組）附加至預設規則。
日誌設定及其他設定	動作	若要針對符合此規則的流量在本機流量日誌中產生項目，請選取以下選項： • 工作階段啟動時記錄（預設為停用）—產生工作階段開始時的流量日誌項目。 除基於疑難排解目的或尋找通道工作階段日誌以顯示 *ACC* 中啟動的 *GRE* 通道外，請勿啟用 *Log at Session Start*（工作階段啟動時記錄）。如應用程式在幾個封包之後發生變更（例如，從 *facebook-base* 到 *facebook-chat*），則在階段結束時進行記錄會消耗更少的資源並識別確切的應用程式。 • 工作階段結束時記錄（預設為啟用）—產生工作階段結束時的流量日誌項目。

© 2019 Palo Alto Networks, Inc.

在安全性原則中建立區塊	設定位置	說明
		若已記錄工作階段開始或結束項目，則也會記錄丟棄與拒絕項目。 • 日誌轉送設定檔—若要將本機流量日誌與威脅日誌項目轉送至遠端目的地，例如 Panorama 與系統日誌伺服器，請選取日誌轉送設定檔。 威脅日誌項目的產生由安全性設定檔決定。依需求定義 *New*（新） 日誌設定檔（請參考物件 > 日誌轉送）。 建立並啟用日誌轉送設定檔以將日誌傳送至專用外部儲存裝置。這將會保留日誌，因為防火牆的日誌儲存空間有限，並且在佔用空間時，防火牆會清除最舊的日誌。 您也可以修改預設規則上的日誌設定。指定下列選項的任何組合： • 排程—若要限制規則生效的天數與時間，請從下拉式清單中選取排程。依需求定義 **New**（新）排程（請參考用以控制已解密 SSL 流量的設定）。 • **QoS** 標記—若要變更符合規則之封包上的服務品質 (QoS) 設定，請選取 **IP DSCP** 或 **IP Precedence**（**IP** 優先順序），然後以二進位的格式輸入 QoS 值，或從下拉式清單中選取預先定義的值。如需 QoS 的詳細資訊，請參考服務品質。 • 停用伺服器回應檢驗—停用從伺服器到用戶端的封包檢驗。預設為停用此選項。 從最佳安全性的角度來看，不要啟用 *Disable Server Response Inspection*（停用伺服器回應檢驗）。隨著選取此選項，防火牆僅會檢驗用戶端到伺服器的流量。它不會檢驗伺服器到用戶端的流量，因此無法識別是否在這些流量中有任何威脅。
基本	規則使用情況	• **Rule Created**（規則建立時間）—規則的建立日期和時間。 • **Last Edited**（上次編輯時間）—規則的上次編輯日期和時間。
活動	規則使用情況	• **Hit Count**（命中數）—流量成功配對規則（命中）的總次數。 • **First Hit**（首次命中）—首個規則配對成功的時間。 • **Last Hit**（最後命中）—最後規則配對成功的時間。
應用程式	規則使用情況	• **Applications Seen**（應用程式檢閱數量）—規則允許的應用程式的數量。 • **Last App Seen**（上次看見的應用程式）—自上次在規則上看見新應用程式（以前未見過的應用程式）以來的天數。 • **Compare Applications & Applications Seen**（比較應用程式以及檢閱的應用程式）—按一下以將規則上設定的應用程式

© 2019 Palo Alto Networks, Inc.

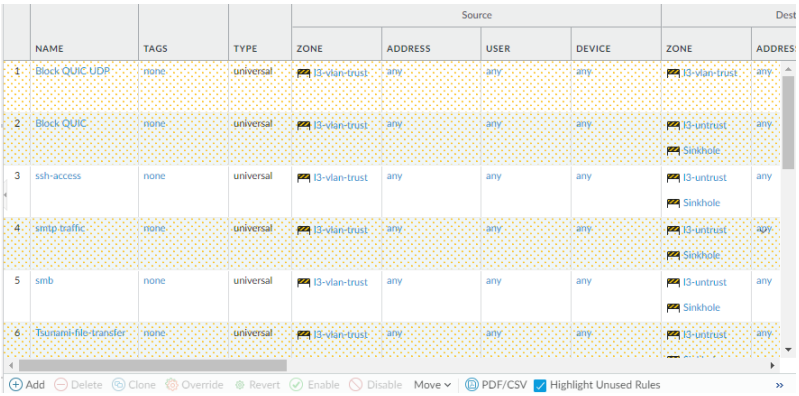
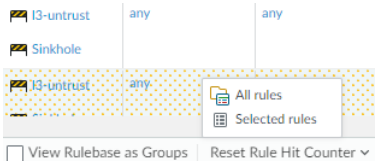
在安全性原則中建立區塊	設定位置	說明
		與規則上顯示的應用程式進行比較。使用此工具可以發現與規則相符的應用程式，並將應用程式新增至規則。
流量（過去 30 天）	規則使用情況	• **Bytes**（位元組）—過去 30 天內規則上的流量（位元組）。 超過 *30* 天的時段將導致最舊的規則保留在清單頂部，因為它們可能具有最多的累積流量。這可能導致較新規則列在較舊規則之下，即使較新規則查看到大量流量亦是如此。
任何（以所有裝置為目標） 僅限 Panorama	**Target**（目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置 僅限 Panorama		選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤 僅限 Panorama		**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標 僅限 Panorama		啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

建立和管理原則

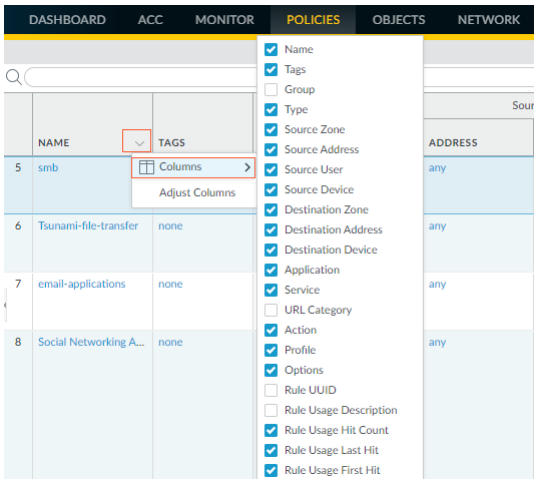
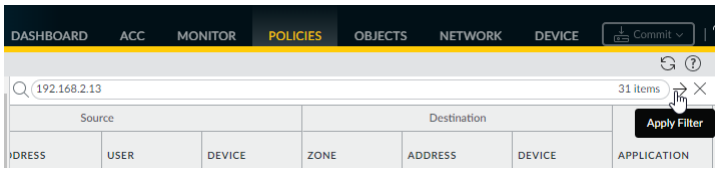
選取 **Policies**（原則）> **Security**（安全性）頁面，可 新增 、修改及管理安全性原則：

工作	說明
Add（新增）	**Add**（新增）新原則規則，或選取基於新規則的規則，並 **Clone Rule**（複製規則）。複製的規則「rule*n*」會插入到所選規則下方，其中，*n* 是使規則名稱成為唯一名稱的下一個可用整數。如需複製的詳細資訊，請參閱移動或複製原則規則。
修改	選取要修改其設定的規則。 若規則從 Panorama 推送，則規則在防火牆上為唯讀且無法在本機上予以編輯。
	Override（覆寫）和 **Revert**（還原）動作僅與「安全性」規則庫底部顯示的預設規則有關。這些預先定義規則（允許所有區域內流量並拒絕所有區域間流量）會指示防火牆如何處理不符規則庫中任何其他規則的流量。由於它們屬於預先定義的設定，因此必須先予以 **Override**（覆寫），您才能編輯選取原則設定。如果您使用 Panorama，則也可以 **Override**（取代）預設規則，然後將這些規則推送至裝置群組或共用內容中的防火牆。您也可以 **Revert**（還原）預設規則，也就是還原預先定義的設定，或從 Panorama 推送的設定。如需詳細資訊，請參閱取代或還原安全性原則規則。

© 2019 Palo Alto Networks, Inc.

工作	說明
移動	規則將由上到下評估，並在 **Policies**（原則）頁面上列舉。若要變更對網路流量評估規則的順序，請選取規則以及 **Move Up**（上移）、**Move Down**（下移）、**Move Top**（移至頂部）、**Move Bottom**（移至底部）或 **Move to a different rulebase or device group**（移至其他規則庫或裝置群組）。如需詳細資訊，請參閱移動或複製原則規則。
複製 UUID	複製規則的 UUID 到剪貼簿，以便在搜尋組態或日誌時使用。
Delete（刪除）	選取並 **Delete**（刪除）現有的規則。
啟用/停用	若要停用規則，則選取並 **Disable**（停用）該規則；若要啟用已停用的規則，則選取並 **Enable**（啟用）該規則。
監控規則使用方式	若要識別自上次防火牆重新啟動以來已使用的規則，請選取 **Highlight Unused Rules**（反白顯示未使用的規則）。未使用的規則具有虛線背景。接著您可以決定是要 **Disable**（停用）還是 **Delete**（刪除）規則。目前未使用的規則將顯示黃色圓點背景。當原則規則命中數啟用時，命中數資料會用來決定規則是否未使用。 每個防火牆會為擁有符合項的規則維護一個流量旗標。在重新開機或重新啟動時發生資料層重設時，由於會重設旗標，因此最佳的作法是定期監控這份清單，先判定規則自前次檢查後是否擁有符合項，再刪除或停用該規則。 
原則規則命中數	**Hit Count**（命中數）追蹤該原則規則的總流量命中數。透過重新啟動、升級和資料層重新啟動，總流量命中數持續存在。 或者，**Reset Rule Hit Counter**（重設規則命中計數器）（底部工作表）。若要清除命中數統計資料，則選取 **All Rules**（所有規則），也可以選取特定規則並僅重設 **Selected rules**（選定規則）的命中數統計資料。  檢視 **First Hit**（第一次命中）以識別安全性原則第一次命中的時間。顯示日期格式為：日 hh:mm:ss 年。您無法重設此值。 檢視 **Last Hit**（上次命中）以識別上次使用安全性原則的時間。顯示日期格式為：日 hh:mm:ss 年。您無法重設此值。

© 2019 Palo Alto Networks, Inc.

工作	說明
顯示/隱藏欄	顯示或隱藏顯示在 **Policies**（原則）下的欄。選取用於切換顯示畫面的欄名稱。 
套用篩選器	若要對清單套用篩選器，請從 **Filter Rules**（篩選規則）下拉式清單中選取。若要定義篩選器，請從項目下拉式清單中選取 **Filter**（篩選器）。 預設規則不屬於規則庫篩選，且一律會顯示在篩選的規則清單中。
	若要檢視依原則記錄為相符項目的網路工作階段，請從規則名稱下拉式清單中選取 **Log Viewer**（日誌檢視器）。
	若要顯示目前的值，請從項目下拉式清單中選取 **Value**（值）。您也可以直接從欄工作表編輯、篩選或移除項目。例如，若要檢視位址群組中包括的位址，請將滑鼠移至在 **Address**（位址）欄中的物件，並從下拉式清單中選取 **Value**（值）。這可讓您快速瀏覽位址群組的成員以及對應 IP 位址，而不需要導覽至 **Object**（物件）頁籤。
	若要根據其名稱或 IP 位址尋找原則中使用的物件，請使用篩選器。套用篩選器後，您只會看到與篩選器相符的項目。篩選器還適用於內嵌物件例如，您對 10.1.4.8 進行篩選時，只會顯示包含該位址的原則： 
預覽規則（僅限 Panorama）	**Preview Rules**（預覽規則）可先檢視規則清單，再將規則推送至受管理防火牆。在每個規則集內，會以視覺方式，針對每一個裝置群組（和受管理的防火牆）將規則階層分門別類，並且提供掃描大量規則的能力。
匯出設定表	具有最小唯讀訪問權限的管理角色可以匯出如 **PDF/CSV** 的原則規則庫。您可以在需要時（如稽核時）套用篩選器以建立更多特定表格設定輸出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。

© 2019 Palo Alto Networks, Inc.

工作	說明
反白顯示未使用的規則	在 **Rule Usage**（規則使用方式）欄中反白顯示沒有流量相符項的任何原則規則。
群組	核取 **View Rulebase as Groups**（以群組形式檢視規則庫）方塊後，管理頁籤群組。您可以執行以下動作： • **Move rules in group to different rulebase or device group**（將群組中的規則移動至其他規則庫或裝置群組）—將選定頁籤群組移動至其他裝置群組。 • **Change group of all rules**（變更所有規則的群組）—將選定頁籤群組中的規則移動到規則庫中的其他頁籤群組。 • **Delete all rules in group**（刪除群組中的所有規則）—刪除選定頁籤群組中的所有規則。 • **Clone all rules in group**（複製群組中的所有規則）—將選定頁籤群組中的規則複製到裝置群組。
以群組形式檢視規則庫	**View Rulebase as Groups**（以群組形式檢視規則庫）以使用 **Group Rules by Tag**（依頁籤群組規則）中所用的頁籤檢視原則規則庫。可見的原則規則是屬於選定頁籤群組的規則。
測試原則比對	對選定原則規則庫的保護原則執行測試，以驗證是否拒絕和允許正確的流量。

取代或還原安全性原則規則

預設安全性規則（區域間預設值和區域內預設值）包含您可在防火牆或 Panorama 上覆寫的預先定義設定。若防火牆從設備群組接收預設規則，您也可覆寫群組設定。您執行覆寫的防火牆或虛擬系統會在其組態中儲存規則的本機版本。您可覆寫的設定為完整集合的子集（下列表格列出安全性規則的子集）。如需預設安全性規則的詳細資訊，請參閱 [政策 > 安全性]。

若要覆寫規則，請在防火牆上選取 **Policies**（政策）> **Security**（安全性），或在 Panorama 上選取（政策）> **Security**（安全性）> **Default Rules**（預設規則）。[名稱] 欄會針對您可覆寫的規則顯示繼承圖示（ ）。請選取規則、按一下**Override**（覆寫），並編輯下表中的設定。

若要將已覆寫的規則還原為預先定義的設定，或從 Panorama 設備群組推送的設定，請在防火牆上選取 **Policies**（政策）> **Security**（安全性），或在 Panorama 上選取 **Policies**（政策）> **Security**（安全性）> **Default Rules**（預設規則）。「名稱」欄會針對包含取代值的規則顯示取代圖示（ ）。請選取規則、按一下 **Revert**（還原）並按一下 **Yes**（是）來確認操作。

用以覆寫預設安全性規則的欄位	說明
一般頁籤	
名稱	識別規則為唯讀的 **Name**（名稱）；您無法覆寫該名稱。
規則類型	**Rule Type**（規則類型）為唯讀；您無法覆寫規則類型。
說明	說明為唯讀；您無法覆寫說明。
頁籤	從下拉式清單中選取 **Tags**（頁籤）。 政策標籤是可讓您排序或篩選政策的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可

© 2019 Palo Alto Networks, Inc.

用以覆寫預設安全性規則的欄位	說明
	能想要標記輸入 DMZ 的特定安全性政策、含解密與無解密文字的解密政策，或者對與該位置相關聯的政策使用特定資料中心名稱。
動作頁籤	
動作設定	針對符合規則的流量選取相應 **Actions**（動作）。 • 允許 — （預設）允許流量。 • 拒絕 — 封鎖流量並強制使用針對防火牆拒絕的應用程式定義的預設拒絕動作。若要檢視應用程式預設值定義的拒絕動作，請在 **Objects**（物件）> **Applications**（應用程式）中檢視應用程式詳細資料。 • 丟棄 — 無訊息丟棄應用程式。防火牆不會傳送 TCP 重設訊息至主機或應用程式。 • 重設用戶端—傳送 TCP 重設訊息至用戶端設備。 • 重設伺服器—傳送 TCP 重設訊息至伺服器設備。 • 重設用戶端與伺服器—傳送 TCP 重設訊息至用戶端及伺服器設備。
設定檔設定	設定檔類型—將設定檔或設定檔群組指派給安全性規則： • 若要指定預設安全性設定檔執行的檢查，請選取 **Profiles**（設定檔），接著選取一個或多個 **Antivirus**（防毒）、**Vulnerability Protection**（弱點保護）、**Anti-Spyware**（反間諜軟體）、**URL Filtering**（URL 篩選）、**File Blocking**（檔案封鎖）、**Data Filtering**（資料篩選）、**WildFire Analysis**（**WildFire** 分析）、**SCTP Protection**（**SCTP** 保護）和 **Mobile Network Protection**（行動網路保護）設定檔。 • 若要指派設定檔群組，而非個別設定檔，請選取 **Group**（群組），然後從下拉式清單中選取 **Group Profile**（群組設定檔）。 • 若要定義新設定檔（Objects > Security Profiles（物件 > 安全性設定檔））或設定檔群組，請按一下對應設定檔或群組設定檔下拉式清單中的 **New**（新增）。

日誌設定	指定下列選項的任何組合：
	• 日誌轉送—若要將本機流量日誌與威脅日誌項目轉送至遠端目的地，例如 Panorama 與系統日誌伺服器，請從下拉式清單中選取日誌轉送設定檔。安全性設定檔會決定威脅日誌項目的產生。若要定義新 **Log Forwarding**（日誌轉送）設定檔，請在下拉式清單中選取 **Profile**（設定檔）（請參閱 [物件 > 日誌轉送]）。
	• 若要針對符合此規則的流量在本機流量日誌中產生項目，請選取以下選項：
	  • 工作階段啟動時記錄—產生工作階段開始時的流量日誌項目（預設為選取）。
	  • 工作階段結束時記錄—產生工作階段結束時的流量日誌項目（預設為清除）。
	  若您將防火牆設定為在流量日誌中包括工作階段開始或工作階段結束項目，它也將包括丟棄和拒絕項目。

© 2019 Palo Alto Networks, Inc.

應用程式與使用情況

- Policies > Security > Policy Optimizer > No App Specified > Compare（政策 > 安全性 > 政策最佳化工具 > 無已指定的應用程式 > 比較）（或者按一下 **Apps Seen**（看見的應用程式）中的數字）
- Policies > Security > Policy Optimizer > Unused Apps > Compare（政策 > 安全性 > 政策最佳化工具 > 未使用的應用程式 > 比較）（或者按一下 **Apps Seen**（看見的應用程式）中的數字）
- Policies > Security（政策 > 安全性），然後按一下 **Apps Seen**（看見的應用程式）中的數字

在安全性政策規則的使用方式頁籤上，還可以 **Compare Applications & Applications Seen**（比較應用程式與看見的應用程式）來獲取工具，幫助您從以連接埠為基礎的安全性政策規則移轉到以應用程式為基礎的安全性政策規則，並從 **Applications & Usage**（應用程式與使用方式）中的規則刪除未使用的應用程式。

欄位	說明
時間範圍	顯示應用程式資訊的時段： • **Anytime**（任何時間）—顯示在規則生命週期內看到的應用程式。 • **Past 7 days**（過去 **7** 天）—僅顯示過去 7 天內看到的應用程式。 • **Past 15 days**（過去 **15** 天）—僅顯示過去 15 天內看到的應用程式。 • **Past 30 days**（過去 **30** 天）—僅顯示過去 30 天內看到的應用程式。
規則上的應用程式	在規則上設定的應用程式，或若未在規則上設定任何特定應用程式，則為 **Any**（任何）。您可以根據需要 **Browse**（瀏覽）、**Add**（新增）及 **Delete**（刪除）應用程式，並在規則上設定應用程式，Apps on Rule（規則上的應用程式）旁邊帶圓圈的數字表示應用程式數量。從此位置新增應用程式與在安全性原則規則 **Application**（應用程式）頁籤上新增應用程式的過程相同。
看見的應用程式	所有在符合規則的防火牆上看見並允許的應用程式。Apps Seen（看見的應用程式）旁邊帶圓圈的數字表示在規則上看見的應用程式數量。 • **Applications**（應用程式）—在規則上看見的應用程式。例如，若規則允許網頁瀏覽流量（Apps on Rule（規則上的應用程式）），因為存在許多網頁瀏覽應用程式，您可能會在清單中看到許多應用程式。 • **Subcategory**（子類別）—應用程式的子類別。 • **Risk**（風險）—應用程式的風險評等。 • **First Seen**（最先看見）—在網路上看到應用程式的第一天。 • **Last Seen**（最後看見）—在網路上看到應用程式的最後一天。 *First Seen*（最先看見）和 *Last Seen*（最後看見）的測量間隔為一天，因此在您定義規則的當天，第一天和最後一天為同一天。 • **Traffic (30 days)**（流量（**30** 天））—在過去 30 天內看見的流量（位元組）。 較長的時段會導致最舊的規則保留在清單頂部，因為其可能具有最多的累計流量。這可能導致較新規則列在較舊規則之下，即使較新規則查看到大量流量亦是如此。

© 2019 Palo Alto Networks, Inc.

欄位	說明
看見的應用程式動作	您可在 **Apps Seen**（看見的應用程式）上執行的動作： • **Create Cloned Rule**（建立複製的規則）—複製目前規則。從基於連接埠規則移轉至基於應用程式的規則時，先複製基於連接埠的規則，然後編輯複製項來建立基於應用程式的允許流量的規則。複製的規則將插入原則清單中以連接埠為基礎的規則之上。使用此移轉方法可確保您不會無意中拒絕您要允許的流量—如果複製的規則不允許您所需的所有應用程式，則之後基於連接埠的規則會允許這些應用程式。監控基於連接埠的規則並根據需要調整（複製的）基於應用程式的規則。您確定基於應用程式的規則允許您需要的流量，且只有不需要的流量篩選至基於連接埠的規則時，則可安全地移除基於連接埠的規則。 • **Add to This Rule**（新增至此規則）—將應用程式從 Apps Seen（看見的應用程式）新增至規則。將應用程式新增至規則會將設定為與 **Any**（任何）應用程式相符的規則（以連接埠為基礎的規則）轉換為以應用程式為基礎的規則，而後者會允許您指定的應用程式（新的以應用程式為基礎的規則將替代以連接埠為基礎的規則）。此規則會拒絕您未新增的任何應用程式，就像其他任何基於應用程式的規則一樣。務必識別所有您要允許的應用程式並將其新增至規則中，這樣便不會意外拒絕應用程式。 • **Add to Existing Rule**（新增至現有規則）—將應用程式從 Apps Seen（看見的應用程式）新增至基於現有應用程式 (App-ID) 的規則。這可讓您從基於連接埠的規則中複製基於 App-ID 的規則，隨後將基於連接埠的規則上的更多看見的應用程式新增至 App-ID 規則。 • **Match Usage**（比對使用）—將所有 Apps Seen（看見的應用程式）移至規則（**Match Usage**（比對使用）後，其會列在 Apps on Rule （規則上的應用程式）之下）。如果您確定該規則應允許所有列出的應用程式，則 **Match Usage**（比對使用）非常方便。但是，您必須確定所有列出的應用程式皆是您希望在網路上允許的應用程式。如果在規則上（例如，在允許網頁瀏覽的規則上）看見許多應用程式，則最好複製規則並轉換為基於應用程式的規則。**Match Usage**（比對使用）適用於含有已知應用程式的簡單規則。例如，若用於連接埠 22 的基於連接埠的規則只看見 SSH 流量（這就是它應看見的全部內容），則 **Match Usage**（比對使用）是安全的。

複製對話方塊
新增至此規則對話方塊
將應用程式新增至現有規則對話方塊
	從具有相關應用程式的 **Apps Seen**（看見的應用程式）與 **Create Cloned Rule**（建議複製的規則）或 **Add to Rule**（新增至規則）中選取應用程式時，會列示以下對話方塊：
	• **Name**（名稱）（僅限 Clone（複製）和 Add Apps to Existing Rule（將應用程式新增至現有規則）對話方塊）。
	  • 複製：輸入新複製規則的名稱。
	  • 將應用程式新增至現有規則：從下拉式功能表中選取要將應用程式新增至的規則，或者輸入規則的名稱。
	• **Applications**（應用程式）：
	  • 新增容器應用程式（預設值）：選中所有容器應用程式、在規則上看見的應用程式以及在容器中但是在規則上看不見的應用程式的核取方塊。

© 2019 Palo Alto Networks, Inc.

欄位	說明

	• 新增特定看見的應用程式：僅選取在規則上實際看見的應用程式，取消選取所有其他應用程式。（您可以手動選取容器應用程式和其他應用程式。）
	• **Application**（應用程式）：
	  • 在規則上看見的選定應用程式以綠色反白顯示。
	  • 容器應用程式，反白顯示為灰色，下面列示了個別應用程式。
	  • 在容器中且在規則上看見但未在 **Applications & Usage**（應用程式及使用方式）中選取的個別應用程式（正常文字）。
	  • 規則上未看見的容器中的個別應用程式（斜體）。
	  • 在規則上 **Last Seen**（上次看見）應用程式的日期。
	• **Dependent Applications**（相依應用程式）：
	  • 預設會選中新增應用程式相依性的核取方塊，因為執行選定應用程式需要這些應用程式。
	  • **Depends On**（依賴於）—選定應用程式的相依應用程式清單。選定的應用程式需要執行這些相依應用程式。
	  • **Required By**（要求者）—列示需要相依應用程式（**Depends On**（依賴於））的應用程式。（有時相依應用程式又需要另一個相依應用程式。）
	Clone（複製）、**Add to Rule**（新增至規則）與 **Add Apps to Existing Rule**（將應用程式新增至現有規則）對話方塊有助於確保應用程式不會中斷，讓您能夠適應規則，可透過包含相關個別應用程式實現，這些應用程式與您要複製或新增至規則的應用程式相關。

安全性政策最佳化工具

- Policies > Security > Policy Optimizer（政策 > 安全性 > 政策最佳化工具）

Policies（政策）> **Security**（安全性）> **Policy Optimizer**（政策最佳化工具）顯示：

- **No App Specified**（無指定的應用程式）—將應用程式設定為 **any**（任何）的規則，以便您可識別以連接埠為基礎的規則來轉換為以應用程式為基礎的規則。
- **Unused Apps**（未使用的應用程式）—包含從未符合規則之應用程式的規則。
- **Rule Usage**（規則使用情況）—不同時間段的規則使用情況資訊，包括不同時間段未使用的規則。

欄位	說明
名稱	安全性政策規則的名稱。
服務	任何與安全性政策規則關聯的服務。
流量 (位元組，30 天)	**Traffic (30 days)**（流量（**30** 天））—在過去 30 天內看見的流量（位元組）。 較長的時段會導致最舊的規則保留在清單頂部，因為其可能具有最多的累計流量。這可能導致較新規則列在較舊規則之下，即使較新規則查看到大量流量亦是如此。

© 2019 Palo Alto Networks, Inc.

欄位	說明
允許的應用程式	規則允許的應用程式。開啟 **Application**（應用程式）對話方塊，您可從其中新增及刪除規則上的應用程式。
看見的應用程式	在規則上看到的應用程式數目。按一下該數目，即可開啟 **Applications & Usage**（應用程式與使用方式）對話方塊，讓您可以比較規則上設定的應用程式與在規則上看到的應用程式，並修改應用程式。
沒有新應用程式的天數	自在規則上看見上一個新應用程式以來的天數。
比較	開啟 **Applications & Usage**（應用程式與使用方式）對話方塊，比較規則上設定的應用程式與在規則上看到的應用程式，並修改規則。
（規則使用情況）最後命中	流量符合規則的最近時間。
（規則使用情況）首次命中	流量第一次符合規則的時間。
（規則使用情況）命中計數	流量符合規則的次數。
已修改	上次修改規則的日期與時間。
已建立	規則建立的日期與時間。
時間範圍（僅限規則使用情況）	顯示資料的時間段（天數）。
使用情況（僅限規則使用情況）	顯示： • 指定時間範圍內防火牆上的 **Any**（任何）（所有）規則，無論流量符合規則（使用的規則）還是不符合（未使用的規則）。 • 指定時間範圍內流量與之不相符的 **Unused**（未使用）規則。 • 指定時間範圍內流量與之相符的 **Used**（使用）規則。
排除最近 *xx* 天內重設的規則（僅限規則使用情況）	在指定天數（1-5,000 天）內，不顯示 **Reset Rule Hit Counter**（重設規則命中計數器）的規則。例如，這讓您可以檢查時間範圍內沒有相符流量的較舊規則，同時排除可能沒有時間比對流量的較新規則。
重設日期（僅限規則使用情況）	規則命中計數器重設的最後日期。

© 2019 Palo Alto Networks, Inc.

Policies > NAT（原則 > NAT）

如果您在防火牆上定義第三層介面，您可以設定網路位址轉譯 (NAT) 原則，來指定是否要在公共與私人位址和連接埠之間轉換來源或目的地 IP 位址與連接埠。例如，當流量從內部（受信任）區域傳送至公共（不受信任）區域時，可以將私人來源位址轉譯為公共位址。Virtual Wire 介面上也支援 NAT。

NAT 規則是基於來源與目的地區域、來源與目的地位址及應用程式服務（例如 HTTP）。與安全性原則一樣，會由上而下針對連入流量逐一比對 NAT 原則規則，且會套用第一條符合條件的規則。

視需要將靜態路由新增至本地端路由器，以使所有公共位址的流量皆可傳送至防火牆。您可能也需要將靜態路由新增至防火牆上的接收介面，以將流量傳送回到私人位址。

下表說明 NAT 和 NPTv6（IPv6-to-IPv6 網路首碼轉譯）設定：

- NAT 原則一般頁籤
- NAT 原始封包頁籤
- NAT 轉譯封包頁籤
- NAT 主動/主動 HA 繫結頁籤
- （僅限 Panorama）NAT 目標頁籤

想知道更多？

請參閱 NAT

NAT 原則一般頁籤

- **Policies**（原則）> **NAT** > **General**（一般）

使用 **General**（一般）頁籤可設定 NAT 或 NPTv6 原則的名稱和描述。存在許多原則時，您可以設定頁籤來排序或篩選這些原則。選取您要建立的 NAT 類型，其會影響 **Original Packet**（原始封包）和 **Translated Packet**（轉譯封包）頁籤上的可用欄位。

NAT 規則—一般設定	說明
名稱	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入規則的描述（最多 1024 個字元）。
頁籤	如果您想要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
NAT 類型	指定轉譯類型： • **ipv4** — 在 IPv4 位址間轉譯。 • **nat64** — 在 IPv6 與 IPv4 位址間轉譯。 • **nptv6** — 在 IPv6 首碼間轉譯。

© 2019 Palo Alto Networks, Inc.

NAT 規則—一般設定	說明
	您無法將 IPv4 及 IPv6 位址範圍結合於單一 NAT 規則中。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔	檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。

NAT 原始封包頁籤

- Policies > NAT > Original Packet（政策 > NAT > 原始封包）

選取 **Original Packet**（原始封包）頁籤可定義防火牆將轉譯的來源和目的地區域，或者指定目的地介面和服務類型。您可以設定多個相同類型的來源及目的地區域，並且可將規則套用至指定網路或特定 IP 位址。

NAT 規則—原始封包設定	說明
來源區域/目的地區域	為原始（非 NAT）封包選取一或多個來源與目的地區域（預設為 **Any**（任何））。區域的類型必須相同（第二層，第三層或 Virtual Wire）。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 您可指定多個區域來簡化管理。例如，您可以進行一些設定，以便將多個內部 NAT 位址導向至相同的外部 IP 位址。
目的地介面	指定防火牆轉譯封包的目的地介面。當網路連接至二個擁有不同 IP 位址配發範圍的 ISP 時，您可使用目的地介面來轉譯不同的 IP 位址。
服務	指定防火牆轉譯來源或目的地位址的服務。若要定義新的服務群組，請選取 物件 > 服務群組。
來源位址/目的地位址	指定防火牆要轉譯的來源和目的位址組合。 如為 NPTv6，針對 **Source Address**（來源位址）和 **Destination Address**（目的地位址）設定的前置詞必須為 xxxx:xxxx::/yy 格式。位址不可定義介面識別碼（主機）部分。支援的首碼長度範圍為 /32 到 /64。

NAT 轉譯封包頁籤

- 原則 > NAT > 轉譯封包

有關來源位址轉譯，選取 **Translated Packet**（轉譯的封包）頁籤來決定在來源、位址，以及潛在的連接埠上執行轉譯的轉譯類型。

透過公開 IP 位址存取的內部主機，您也可以啟用目的地位址轉譯。在此情況下，您可以為內部主機在 **Original Packet**（原始封包）頁籤中定義公開來源和目的地位址，並且在 **Translated Packet**（轉譯的封包）頁籤上，您設定 **Static Ip**（靜態 **Ip**）或 **Dynamic IP (with session distribution)**（動態 **IP**（附工作階段散布））並輸入 **Translated Address**（轉譯的位址）。接著，在存取公開位址時，該位址會轉譯成內部主機的內部（目的地）位址。

© 2019 Palo Alto Networks, Inc.

NAT 規則—轉譯封包設定	說明
來源位址轉譯	選取 **Translation Type**（轉譯類型）（動態或靜態位址集區），並輸入來源位址要轉譯到的 IP 位址或位址範圍 (address1-address2)（轉譯位址）。位址範圍的大小受限於位址集區的類型： • 動態 **IP** 與連接埠—按照來源 IP 位址的雜湊選取位址。對於指定的來源 IP 位址，防火牆會對所有工作階段使用相同的轉譯來源位址。對於 NAT 集區中的各個 IP 位址，動態 IP 及連接埠（DIPP）來源 NAT 大約支援 64,000 個同時工作階段。某些型號支援過度訂閱，這可讓單一 IP 代管 64,000 個以上的同時工作階段。 Palo Alto Networks® DIPP NAT 支援的 NAT 工作階段比可用 IP 位址與連接埠數量支援的更多。有了過度訂閱，當目的地 IP 位址唯一時，防火牆在 PA-220、PA-820、PA-850、VM-50、VM-300 和 VM-1000-HV 防火牆上可以同時使用最多兩次 IP 位址與連接埠組合，在 PA-5220 防火牆以及 PA-3200 系列防火牆上為同時四次，在 PA-5250、PA-5260、PA-5280、PA-7050、PA-7080、VM-500 和 VM-700 防火牆上為同時八次。 • 動態 **IP**—轉譯至下一個在特定範圍內的可用位址，但連接埠號碼維持不變。最多支援 32,000 個連續 IP 位址。動態 IP 集區包含多個子網路，因此您可以將內部網路位址轉譯為兩個以上的個別公共子網路。 • 進階（動態 **IP**/連接埠後援）—使用此選項可建立後援集區，這將執行 IP 及連接埠轉譯，並且在主要集區沒有位址可用時使用。您可以使用 **Translated Address**（轉譯位址）選項或 **Interface Address**（介面位址）選項定義集區的位址；後一個選項是針對動態接收 IP 位址的介面。建立後援集區時，確定位址並未與主要集區中的位址重疊。
來源位址轉譯（持續）	• 靜態 **IP** — 始終將相同位址用於轉譯，且不變更連接埠。例如，如果來源範圍是 192.168.0.1-192.168.0.10 且轉譯範圍是 10.0.0.1-10.0.0.10，始終會將位址 192.168.0.2 轉譯為 10.0.0.2。實際上未限制位址範圍。 NPTv6 來源位址轉譯必須使用 **Static IP**（靜態 **IP**）。對於 NPTv6，為 **Translated Address**（轉譯位址）設定的首碼必須以 xxxx:xxxx::/yy 這個格式呈現，而且位址不可定義介面識別碼（主機）部分。支援的首碼長度範圍為 /32 到 /64。 • 無 — 不執行轉譯。
雙向	（選用）若您希望防火牆以您設定的轉譯反方向建立對應轉譯（NAT 或 NPTv6），請啟用雙向轉譯以進行 **Static IP**（靜態 **IP**）來源位址轉譯。 若您啟用雙向轉譯，請務必確保您已具備安全性原則以控制兩個方向的流量。若沒有此類原則，雙向功能可自動以兩個方向轉譯封包。
目的地位址轉譯	設定下列選項以讓防火牆執行目的地 NAT。您通常使用目的地 NAT以允許從公共網路中存取內部伺服器（例如電子郵件伺服器）。
轉譯類型與轉譯位址	選取防火牆在目的地位址執行的轉譯類型： • **None**（無）（預設） • **Static IP**（靜態 **IP**）—輸入初始目的地位址和連接埠號轉譯至的 **Translated Address**（轉譯的位址）（採用 IP 位址或 IP 位址範圍形式）與 **Translated Port**（轉譯的連接埠）號（1 至 65535）。如果 **Translated Port**（轉譯的連接埠）欄位為空，則不會變更目的地連接埠。

© 2019 Palo Alto Networks, Inc.

NAT 規則—轉譯封包設定	說明
	如為 NPTv6，針對目的地首碼 **Translated Address**（轉譯的位址）設定的首碼必須為 xxxx:xxxx::/yy 格式。位址不可定義介面識別碼（主機）部分。支援的首碼長度範圍為 /32 到 /64。 *NPTv6* 不支援轉譯的連接埠，因為 *NPTv6* 為嚴格首碼轉譯。連接埠和主機位址區段將在不變更的情況下轉送。 *IPv4* 的靜態 *IP* 轉譯還可讓您 *Enable DNS Rewrite*（啟用 *DNS* 重寫）（在下面介紹）。 • 動態 **IP**（附工作階段散布）—選取或輸入 **Translated Address**（已轉譯的位址）即 FQDN、位址物件或防火牆選取 translated address（轉譯位址）處的位址群組。如果 DSN 伺服器為 FQDN 返回超過一個的位址，或如果位址物件或位址群組轉譯超過一個 IP 位址，則防火牆會使用特定 **Session Distribution Method**（工作階段散布方法）在那些位址間散布工作階段。
工作階段散佈方式	如果您為目的地 NAT 轉譯選取 **Dynamic IP (with session distribution)**（動態 **IP**（帶工作階段散佈）），則目的地轉譯的位址（轉譯為 FQDN、位址物件或位址群組）可能解析為多個位址。您可以選取防火牆在這些位址之間散佈（指派）工作階段的方式，以提供更平衡的工作階段散佈： • **Round Robin**（循環配置資源）—（預設）按輪流順序將新工作階段指派給 IP 位址。除非您的環境要求您選取其他散佈方法，否則請使用此方法。 • **Source IP Hash**（來源 **IP** 雜湊）— 根據來源 IP 位址的雜湊指派新工作階段。如果您有來自單一來源 IP 位址的傳入流量，則選取**Source IP Hash**（來源 **IP** 雜湊）以外的方法。 • **IP Modulo**（**IP** 模數）—防火牆會將傳入的封包的來源和目的地 IP 位址納入考慮；防火牆執行 XOR 操作和模數運算；結果確定了防火牆指派新工作階段的 IP 位址。 • **IP Hash**（**IP** 雜湊）—使用來源的雜湊以及目的地 IP 位址指派新工作階段。 • **Least Sessions**（最少工作階段）—將新工作階段指派給最少同時進行的工作階段的 IP 位址。如果您有很多生命週期短的工作階段，**Least Sessions**（最少工作階段）會為您提供更平衡的工作階段散佈。
啟用 DNS 重寫	在 PAN-OS 9.0.2 及更新的 9.0 版本中，如果目的地 NAT 政策規則類型是 **ipv4** 並且目的地地址轉譯類型是 **Static IP**（靜態 **IP**），則 **Enable DNS Rewrite**（啟用 **DNS** 重寫）選項可用。如果您使用目的地 NAT 並且使用防火牆一側的 DNS 服務解析另一側上用戶端的 FQDN，則可以啟用 DNS 重寫。當 DNS 回應周遊防火牆時，防火牆會重寫 DNS 回應中的 IP 位址，相對于原始目的地位址或轉譯的目的地位址（DNS 回應與 NAT 政策規則相符）。單個 NAT 政策規則讓防火牆針對符合規則的封包執行 NAT，以及針對符合規則的 DNS 回應中的 IP 位址執行 NAT。您必須指定相對於 NAT 規則，防火牆在 DNS回應中對 IP 位址執行 NAT 的方式：反向或正向： • **reverse**（反向）—（預設值）如果封包是符合規則中的轉譯目的地位址的 DNS 回應，則會使用該規則所用的相反轉譯對 DNS 回應進行轉譯。例如，如果規則將 1.1.1.10 轉譯為 192.168.1.10，則防火牆會將 DNS 回應 192.168.1.10 的重寫為 1.1.1.10。 • **forward**（正向）—如果封包是符合規則中的原始目的地位址的 DNS 回應，則會使用該規則所用的相同轉譯對 DNS 回應進行轉譯。例如，如果規則將 1.1.1.10 轉譯為 192.168.1.10，則防火牆會將 DNS 回應 1.1.1.10 重寫為 192.168.1.10。

© 2019 Palo Alto Networks, Inc.

NAT 主動/主動 HA 繫結頁籤

- Policies > NAT > Active/Active HA Binding（原則 > NAT > 主動/主動 HA 繫結）

只有當防火牆在高可用性 (HA) 主動/主動組態下，才可使用 [主動/主動 HA 繫結] 頁籤。在此組態下，您必須將每個來源 NAT 規則（不論是靜態或動態 NAT）繫結至裝置 ID **0** 或裝置 ID **1**；您必須將每個目的地 NAT 規則繫結至裝置 ID 0、裝置 ID 1、**both**（兩者）（裝置 ID 0 和裝置 ID 1），或繫結至主動 **primary**（主要）主要防火牆。

選取 **Active/Active HA Binding**（主動/主動 **HA** 繫結）設定以將 NAT 規則繫結至 HA 防火牆，如下所示：

- **0**—將 NAT 規則連結至 HA 裝置 ID 0 的防火牆。
- **1**—將 NAT 規則連結至 HA 裝置 ID 1 的防火牆。
- 兩者—將 NAT 規則連結至 HA 裝置 ID 0 的防火牆和 HA 裝置 ID 1 的防火牆。此設定不支援動態 IP 或者動態 IP 及連接埠 NAT。
- 主要—將 NAT 規則連結至 HA 主動-主要狀態的防火牆。此設定不支援動態 IP 或者動態 IP 及連接埠 NAT。

當兩個 HA 端點擁有唯一的 NAT IP 位址集區時，您通常會設定裝置特定 NAT 規則。

當防火牆建立新工作階段時，HA 繫結會決定工作階段可比對的 NAT 規則。繫結必須包含要比對之規則的工作階段擁有者。工作階段會設定防火牆執行 NAT 規則比對，而工作階段會與連結至擁有者的 NAT 規則作比較，並根據其中一項規則進行轉譯。針對裝置特定的規則，防火牆會略過未連結至工作階段擁有者的所有 NAT 規則。例如，假設裝置 ID 1 的防火牆是工作階段擁有者，則該工作階段會設定防火牆。當裝置 ID 1 嘗試將工作階段與 NAT 規則進行比對時，它將略過連結至裝置 0 的所有規則。

如果一個端點失敗，第二個端點會繼續處理失敗端點同步工作階段的流量，包括 NAT 轉譯。Palo Alto Networks 建議您建立連結至裝置 ID 的重複 NAT 規則。因此，會有兩個擁有相同來源轉譯位址和相同目的地轉譯位址的 NAT 規則，一項規則繫結至一個裝置 ID。此組態可讓 HA 端點執行新的工作階段設定工作，並針對繫結至其裝置 ID 的 NAT 規則執行 NAT 規則比對。若沒有建立重複 NAT 規則，運作的端點將嘗試執行 NAT 原則比對，但工作階段不會比對防火牆自身的裝置特定規則，且防火牆將略過未連結至其裝置 ID 的所有其他 NAT 規則。

想知道更多？

請參閱主動 / 主動 HA 模式下的 NAT

NAT 目標頁籤

- （僅限 Panorama）**Policies**（政策）> **NAT** > **Target**（目標）

選取 **Target**（目標）頁簽以選取要向裝置群組中的哪些受管理裝置推送政策規則。您可以透過選取受管理防火牆或指定標籤，來指定要向其推送的受管理防火牆。此外，您可以設定政策規則目標，以向除了指定防火牆之外的所有受管理防火牆推送。

NAT 規則 - 目標設定	說明
任何（以所有裝置為目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤	**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。

© 2019 Palo Alto Networks, Inc.

NAT 規則 - 目標設定	說明
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > QoS（原則 > QoS）

新增 QoS 原則 規則以定義流量，該流量接受特定 QoS 處理，並針對各個 QoS 原則規則指派 QoS 等級，以便在流量離開已啟用 QoS 的介面時，指定所指派的服務等級適用於所有符合相關聯規則的流量。

從 Panorama 中推送至防火牆的 QoS 原則規則會以橙色顯示，且無法在防火牆層級編輯。

此外，若要完全啟用防火牆以提供 QoS：

- 針對各個 QoS 服務等級設定頻寬限制（選取 [網路 > 網路設定檔 > QoS]）以新增或修改 QoS 設定檔。
- 在介面上啟用 QoS（選取 [網路 > QoS]）。

請參考服務品質 以了解完整的 QoS 工作流程、概念及使用案例。

Add（新增）新規則或複製現有規則，然後定義下列欄位。

QoS 原則規則設定	
一般頁籤	
名稱	輸入用來識別規則的名稱（最多 63 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入選取性說明。
頁籤	如果您需要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要標記連入 DMZ 的特定安全性原則，標記含解密與無解密文字的解密原則，或者對與該位置相關聯的原則使用特定資料中心名稱。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔	檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。
來源頁籤	
來源區域	選取一或多個來源區域（預設為 **any**（任何））。區域的類型必須相同（第二層第三層或 Virtual Wire）。
來源位址	指定來源 IPv4 或 IPv6 位址的組合，可以針對該組合覆蓋識別的應用程式。若要選取特定位址，請從下拉式清單中選取 **Select**（選取），並執行下列其中一項操作： • 在可用欄中選取適當位址 和/或位址群組 旁邊的此選項，並按一下 **Add**（新增）來將您的選取新增至所選欄中。 • 在搜尋欄位中輸入名稱的前幾個字元，列出以這幾個字元開頭的所有位址與位址群組。選取清單中的項目可使該選項列於可用欄中。請時常視需要重複此程序，然後按一下 **Add**（新增）。

© 2019 Palo Alto Networks, Inc.

QoS 原則規則設定	
	• 請輸入一或多個 IP 位址（每行一個），有沒有網路遮罩都可以。通用格式為：*<ip_address>/<mask>* • 若要移除位址，請選取位址（所選欄），然後按一下 **Delete**（刪除），或選取 **Any**（任何）來清除所有位址及位址群組。 若要新增可在此原則或其他原則中使用的位址，請按一下 **New Address**（新增位址）。若要定義新位址群組，請選取 Objects > Address Groups（物件 > 位址群組）。
來源使用者	指定將套用 QoS 原則的來源使用者與群組。
否定	如果此頁籤上的指定資訊不相符，選取此選項可套用原則。
目的地頁籤	
目的地區域	選取一或多個目的地區域（預設為 **any**（任何））。區域的類型必須相同（第二層第三層或 Virtual Wire）。
目的地位址	指定來源 IPv4 或 IPv6 位址的組合，可以針對該組合覆蓋識別的應用程式。若要選取特定位址，請從下拉式清單中選取 **Select**（選取），並執行下列其中一項操作： • 在可用欄中選取適當位址 及/或位址群組 旁邊的此選項，並將您的選取 **Add**（新增）至所選欄中。 • 在搜尋欄位中輸入名稱的前幾個字元，列出以這幾個字元開頭的所有位址與位址群組。選取清單中的項目可使該選項列於可用欄中。請時常視需要重複此程序，然後按一下 **Add**（新增）。 • 請輸入一或多個 IP 位址（每行一個），有沒有網路遮罩都可以。通用格式為：*<ip_address>/<mask>*。 • 若要移除位址，請選取位址（所選欄），然後按一下 **Delete**（刪除），或選取 **Any**（任何）來清除所有位址及位址群組。 若要新增可在此原則或其他原則中使用的位址，請按一下 **New Address**（新增位址）。
否定	如果此頁籤上的指定資訊不相符，選取此選項可套用原則。
應用程式頁籤	
應用程式	選取 QoS 規則的特定應用程式。若要定義新應用程式或應用程式群組，請選取 **Objects**（物件）> **Applications**（應用程式）。 如果應用程式具有多個功能，您可以選取整個應用程式或個別功能。如果您選取整個應用程式，會包含所有功能，且會在新增未來功能後自動更新應用程式定義。 如果您在 QoS 規則中使用應用程式群組、篩選或容器，可以使滑鼠停留在應用程式欄中的物件，按一下向下箭頭，並選取 **Value**（值），檢視這些物件的詳細資訊。這可以讓您直接從原則輕鬆檢視應用程式成員，而不需要移至 **Objects**（物件）頁籤。
服務/URL 類別頁籤	

© 2019 Palo Alto Networks, Inc.

QoS 原則規則設定	
服務	選取服務以限制在特定 TCP 與/或 UDP 埠號之內。從下拉式清單中選取下列選項之一： • 任何—任何通訊協定或連接埠上都允許或拒絕所選應用程式。 • 應用程式預設值—僅在 **Palo Alto Networks** 定義的預設連接埠上允許或拒絕選取的應用程式。此選項建議用於允許原則。 • 選取 — 按一下 **Add**（新增）。選取現有的服務或選取服務或服務群組，指定新項目。
URL 類別	選取 QoS 規則的 URL 類別。 • 選取 **Any**（任何），確保無論 URL 類別為何，工作階段都可以符合 QoS 規則。 • 若要指定類別，請按一下 **Add**（新增），從下拉式清單中選取特定類別（包括自訂類別）。您可以新增多個類別。請參考 [物件 > 外部動態清單] 以了解定義自訂類別的相關資訊。
DSCP/TOS 頁籤	
任何	選取 **Any**（任何）選項（預設）可允許原則比對流量，無論為流量定義的差異服務字碼指標 (DSCP) 值或 IP 優先順序/服務類型 (ToS) 為何。
代碼點	選取字碼指標以允許根據 DSCP 或 ToS 值定義的封包 IP 標頭來接收 QoS 處理。DSCP 與 ToS 值用於指出流量要求的服務層級，例如高優先順序或盡力傳遞。在 QoS 原則中使用代碼點作為比對準則，可允許工作階段根據在工作階段開始時偵測到的代碼點來接收 QoS 處理。 繼續 **Add**（新增）代碼點，使流量符合與 QoS 原則： • 為字碼指標指定具描述性的名稱。 • 選取您要作為 QoS 原則比對條件的字碼指標 **Type**（類型），然後選取特定的 **Codepoint**（字碼指標）值。您也可以輸入 **Custom Codepoint**（自訂字碼指標）與 **Binary Value**（二進位值），建立 **Custom Codepoint**（自訂字碼指標）。
其他設定頁籤	
級	選取要指派給規則的 QoS 等級，並按一下 **OK**（確定）。等級特性在 QoS 設定檔中定義。如需設定 QoS 等級設定的相關資訊，請參考 [網路 > 網路設定檔 > QoS]。
排程	• 選取 **None**（無），使原則規則始終保持使用中狀態。 • 從下拉式清單中選取 **Schedule**（排程）（行事曆圖示），以便在啟用規則時，設定單一時間範圍或週期性時間範圍。
目標頁籤（僅限 Panorama）	
任何（以所有裝置為目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。

© 2019 Palo Alto Networks, Inc.

QoS 原則規則設定	
標籤	**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > Policy Based Forwarding（原則 > 基於原則的轉送）

通常，當流量進入防火牆時，進入介面虛擬路由器會根據目的地 IP 位址，指定可決定連出介面與目的地安全性區域的路由。您可以藉由建立基於原則的轉送 (PBF) 規則，指定可決定連出介面的其他資訊，包含來源區域、來源位址、來源使用者、目的地位址、目的地應用程式及目的地服務。指定目的地 IP 位址與連接埠上與應用程式關聯的初始工作階段，將不符合應用程式的特定規則，且將根據後續 PBF 規則（未指定應用程式）或虛擬路由器的轉送表轉送。該目的地 IP 位址與連接埠上針對相同應用程式的所有後續工作階段都將符合應用程式的特定規則。為了確保透過 PBF 規則轉送，不建議使用應用程式的特定規則。

必要時，PBF 規則可用於使用 Forward-to-VSYS 轉送動作，強制流量經過其他虛擬系統。在這種情況下，必須定義將透過防火牆上的特殊輸出介面，將封包從目的地虛擬系統轉送出去的其他 PBF 規則。

下表說明原則路由設定：

- 基於原則的轉送一般頁籤
- 基於原則的轉送來源頁籤
- 基於原則的轉送目的地/應用程式/服務頁籤
- 基於原則轉送的轉送頁籤
- （僅限 Panorama）基於原則的轉送目標頁籤

想知道更多？

請參考基於原則的轉送

基於原則的轉送一般頁籤

選取 **General**（一般）頁籤可設定 PBF 原則的名稱和描述。存在大量原則時，也可以設定標記來排序或篩選這些原則。

欄位	說明
名稱	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入原則的描述（最多 1024 個字元）。
頁籤	如果您需要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要標記連入 DMZ 的特定安全性原則，標記含解密與無解密文字的解密原則，或者對與該位置相關聯的原則使用特定資料中心名稱。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。

© 2019 Palo Alto Networks, Inc.

欄位	說明
稽核註解封存檔	檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。

基於原則的轉送來源頁籤

選取 **Source**（來源）頁籤可定義來源區域或來源位址，從而定義哪些傳入的來源流量將套用轉送政策。

欄位	說明
來源區域	若要選擇來源區域（預設為 any（任何）），請按一下 **Add**（新增），然後從下拉式清單中選取。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。 只有 *Layer 3* 類型區域才支援政策路由。
來源位址	按一下 **Add**（新增）可新增來源位址、位址群組或地區（預設為 [任何]）。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。
來源使用者	按一下 **Add**（新增）可選擇受限於政策的來源使用者或使用者群組。支援以下來源使用者類型： • 任何 — 包含任何流量，不論使用者資料為何。 • 預先登入—包含使用 GlobalProtect™ 連線至網路，但未登入其系統的遠端使用者。在 [入口網站] 上設定 GlobalProtect 應用程式的 [預先登入] 選項時，將以使用者名稱預先登入識別目前未登入其電腦的任何使用者。您接著可為預先登入使用者建立原則，且使用者即便未直接登入，也會在網域上驗證其電腦，如同這些使用者已完全登入一般。 • 已知使用者 — 包含所有驗證的使用者，意味已對應使用者資料的任何 IP。此選項等同於網域上的「網域使用者」群組。 • 未知—包含所有未驗證的使用者，意味未對應至使用者的 IP 位址。例如，您可以使用未知，供來賓等級的使用者存取某些資訊，因為他們雖然在您的網路上擁有 IP，但不會經過網域驗證，且在防火牆上沒有 IP 位址至使用者對應資訊。 • 選取 — 包含此視窗中選項所決定的所選使用者。例如，您可能想要新增一名使用者、個人清單、部分群組，或手動新增使用者。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。

基於原則的轉送目的地/應用程式/服務頁籤

選取 **Destination/Application/Service**（目的地/應用程式/服務）頁籤可定義目的地設定，這些設定將套用到符合轉送規則的流量。

© 2019 Palo Alto Networks, Inc.

欄位	說明
目的地位址	按一下 **Add**（新增）可新增目的地位址或位址群組（預設為任何）。依預設，規則會套用到任一 IP 位址。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）或 **Address Group**（位址群組），然後指定設定。
應用程式/服務	選取 PBF 規則的特定應用程式或服務。若要定義新應用程式，請參考定義應用程式。若要定義應用程式群組，請參考 [物件 > 應用程式群組]。 不建議將應用程式特定的規則與 PBF 搭配使用。只要有可能，請使用服務物件，亦即通訊協定或應用程式所使用的 *Layer 4* 連接埠 *(TCP* 或 *UDP)*。 若要檢視這些應用程式的詳細資訊，請將滑鼠停留在 **Application**（應用程式）欄中的物件上，按一下向下箭頭，然後選取 **Value**（值）。這可以讓您直接從政策輕鬆檢視應用程式資訊，而不需要移至 Object（物件）頁籤。 您不能在 *PBF* 規則中設定自訂應用程式、應用程式篩選器或應用程式群組。

基於原則轉送的轉送頁籤

選取 **Forwarding**（轉送）頁籤定義將套用到符合轉送規則之流量的動作和網路資訊。流量可轉送到下一個躍點 IP 位址、虛擬系統，或者丟棄流量。

欄位	說明
動作	選取下列其中一個選項： • 轉送—指定下一個躍點 IP 位址與輸出介面介面（封包用來到達指定的下一個躍點的介面）。 • 轉送至 **VSYS** — 從下拉式清單中選取要轉送至的虛擬系統。 • 丟棄 — 丟棄封包。 • 無 **PBF** — 不改變封包將經過的路徑。此選項會排除符合在規則中所定義來源/目的地/應用程式/服務準則的封包。比對封包時會使用路由表，而非 PBF；防火牆會使用路由表將符合的流量從重新導向的連接埠中排除。 將 *Forward*（轉送）或 *Forward to VSYS*（轉送至 *VSYS*）用作「動作」，以便您可以將「監控」設定檔套用於流量。（當「動作」不轉送流量時，您無法套用「監控」設定檔。）「監控」設定檔監控 *IP* 位址。如果與 *IP* 位址的連線失敗，則「監控」設定檔將指定動作。
輸出介面	將封包導向至特定的 Egress 介面。
下一個躍點	若您將封包導向至特定介面，請以下列其中一種方式針對該封包指定下一個躍點： • **IP Address**（**IP** 位址）—選取 IP 位址並選取使用 Ipv4 或 Ipv6 位址的位址物件（或建立新的位址物件）。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	• **FQDN**—選取 FQDN 並選取使用 FQDN 的位址物件（或建立新的位址物件）。 • **None**（無）—沒有下一個躍點；該封包遭丟棄。
監控	啟用監控功能以確認對目標 **IP** 位址或下一個躍點 IP 位址的連線。選取 **Monitor**（監控），然後附加監控 **Profile**（設定檔）（預設或自訂，**Network**（網路）> **Network Profiles**（網路設定檔）> **Monitor**（監控）），從而指定當無法連線至 IP 位址時的動作。 設定「監控」設定檔並啟用監控，以便在輸出介面出現故障或路由中斷時，防火牆會在設定檔中執行動作，並最大限度地減少或防止服務中斷。
強制對稱傳回	（若為非對稱的路由環境則為必要）選取 **Enforce Symmetric Return**（強制執行對稱傳回），並在 **Next Hop Address**（下一個躍點位址）清單中輸入一或多個 IP 位址。 若啟用對稱傳回，則可確保會透過流量從網際網路進入時所經過的相同介面轉送出傳回流量（例如從 LAN 上的信任區域傳回至網際網路）。
排程	若要限制規則生效的天數與時間，請從下拉式清單中選取排程。若要定義新的排程，請按一下 New（新增）（請參考 [用以控制已解密 SSL 流量的設定]））

基於原則的轉送目標頁籤

- （僅限 Panorama）**Policies**（政策）> **Policy Based Forwarding**（基於政策的轉送）> **Target**（目標）

選取 **Target**（目標）頁簽以選取要向裝置群組中的哪些受管理裝置推送原則規則。您可以透過選取受管理防火牆或指定標籤，來指定要向其推送的受管理防火牆。此外，您可以設定原則規則目標，以向除了指定防火牆之外的所有受管理防火牆推送。

NAT 規則 - 目標設定	說明
任何（以所有裝置為目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤	**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > Decryption（原則 > 解密）

您可以針對可見度、控制與精確安全性的目的，設定防火牆以解密流量。解密原則可套用至安全通訊端層 (SSL)，包括 SSL 封裝通訊協定，例如 IMAP(S)、POP3(S)、SMTP(S)、FTP(S) 和 Secure Shell (SSH) 流量。SSH 解密可用來解密輸出與輸入 SSH 流量，以確保安全通訊協定未用於傳送不允許的應用程式與內容。

新增解密原則規則以定義您想要解密的流量（例如，您可根據 URL 類別來解密流量）。會按順序針對流量比較解密原則規則，因此更特定的規則必須在更一般性的規則之前。

SSL 轉送代理程式解密需要組態信任的憑證，如果使用者連線至的伺服器擁有由防火牆信任的 CA 簽署的憑證，則會為使用者顯示該憑證。請在 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）頁面上建立憑證，然後按一下憑證的名稱，並選取 **Forward Trust Certificate**（轉送信任憑證）。

防火牆不會對技術破解的應用程式進行解密，例如，因為使用設定 *PIN* 碼的憑證或用戶端驗證。

請參考從 SSL 解密中排除的應用程式清單。

下表說明解密原則設定：

- 解密一般頁籤
- 解密來源頁籤
- 解密目的地頁籤
- 解密服務/URL 類別頁籤
- 解密選項頁籤
- （僅限 Panorama）解密目標頁簽

想知道更多？

請參閱解密

解密一般頁籤

選取 **General**（一般）頁籤可設定解密原則的名稱和描述。存在大量原則時，您也可以設定頁籤來排序或篩選這些原則。

欄位	說明
名稱	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入規則的描述（最多 1024 個字元）。
頁籤	如果您需要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要標記連入 DMZ 的特定安全性原則，標記含解密與無解密文字的解密原則，或者對與該位置相關聯的原則使用特定資料中心名稱。

© 2019 Palo Alto Networks, Inc.

欄位	說明
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔	檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。

解密來源頁籤

選取 **Source**（來源）頁籤可定義來源區域或來源位址，從而定義哪些連入的來源流量將套用解密政策。

欄位	說明
來源區域	按一下 **Add**（新增）可選擇來源區域（預設為 [任何]）。區域的類型必須相同（第二層、第三層或 Virtual Wire）。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。
來源位址	按一下 **Add**（新增）可新增來源位址、位址群組或地區（預設為 [任何]）。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。選取 **Negate**（否定）可選擇除已設定位址以外的任何位址。
來源使用者	按一下 **Add**（新增）可選擇受限於政策的來源使用者或使用者群組。支援以下來源使用者類型： • 任何 — 包含任何流量，不論使用者資料為何。 • 預先登入—包含使用 GlobalProtect 連線至網路，但未登入其系統的遠端使用者。在 [入口網站] 上設定 GlobalProtect 應用程式的 [預先登入] 選項時，將以使用者名稱預先登入識別目前未登入其電腦的任何使用者。您接著可為預先登入使用者建立原則，且使用者即便未直接登入，也會在網域上驗證其電腦，如同這些使用者已完全登入一般。 • 已知使用者 — 包含所有驗證的使用者，意味已對應使用者資料的任何 IP。此選項等同於網域上的「網域使用者」群組。 • 未知—包含所有未驗證的使用者，意味未對應至使用者的 IP 位址。例如，您可以使用未知，供來賓等級的使用者存取某些資訊，因為他們雖然在您的網路上擁有 IP，但不會經過網域驗證，且在防火牆上沒有 IP 至使用者對應資訊。 • 選取 — 包含此視窗中選項所決定的所選使用者。例如，您可能想要新增一名使用者、個人清單、部分群組，或手動新增使用者。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。

© 2019 Palo Alto Networks, Inc.

解密目的地頁籤

選取 **Destination**（目的地）頁籤可定義目的地區域或目的地位址，從而定義將套用政策的目的地流量。

欄位	說明
目的地區域	按一下 **Add**（新增）可選擇目的地區域（預設為 any（任何））。區域的類型必須相同（第二層第三層或 Virtual Wire）。若要定義新區域，請參閱 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。
目的地位址	按一下 **Add**（新增）可新增目的地位址、位址群組或地區（預設為 [任何]）。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。選取 **Negate**（否定）可選擇除已設定位址以外的任何位址。

解密服務/URL 類別頁籤

選取 **服務/URL 類別/URL Category**（服務/URL 類別）頁籤來根據 TCP 連接埠號，將解密政策套用至流量或任何 URL 類別（或類別清單）。

欄位	說明
服務	根據特定 TCP 埠號將解密政策套用至流量。從下拉式清單中選取下列選項之一： • 任何—任何通訊協定或連接埠上都允許或拒絕所選應用程式。 • 應用程式預設值—僅在 Palo Alto Networks 針對應用程式定義的預設連接埠上解密（或豁免解密）所選的應用程式。 • 選取 — 按一下 **Add**（新增）。選擇現有的服務或指定新服務或服務群組。（或選取 Objects > Services（物件 > 服務）和物件 > 服務群組）。
URL Category 頁籤	選取解密規則的 URL 類別。 • 選擇 **any** 可比對任何工作階段，無論 URL 類別為何。 • 若要指定類別，請按一下 **Add**（新增），從下拉式清單中選取特定類別（包括自訂類別）。您可以新增多個類別。請參考定義自訂類別的相關資訊。

解密選項頁籤

使用 **Options**（選項）頁籤可決定是否需要加密符合的流量。如果設定 **Decrypt**（解密），請指定解密類型。您也可以設定或選取解密設定檔來新增其他解密功能。

© 2019 Palo Alto Networks, Inc.

欄位	說明
動作	針對流量，選取 **decrypt**（解密）或 **no-decrypt**（無解密）。
類型	從下拉式清單中選取要解密的流量類型： • **SSL** 正向 代理程式 — 指定政策將解密以外部伺服器為預定目的地的用戶端流量。 • **SSH** 代理程式—指定政策將解密 SSH 流量。此選項可讓您指定 ssh 通道 App-ID 來控制政策中的 SSH 通道。 • **SSL** 輸入檢查 — 指定政策將解密 SSH 內送憑證檢驗流量。
解密規則	將解密設定檔附加至政策規則，以便封鎖和控制某些方面的流量。如需建立解密設定檔的詳細資訊，請選取 物件 > 解密設定檔。
日誌設定	
記錄成功的 SSL 交握	（選用）建立成功的 SSL 解密交握的詳細日誌。預設會停用。 日誌會佔用儲存空間。在記錄成功的 *SSL* 交握之前，請確保具有可用於儲存日誌的資源。編輯 *Device*（裝置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定），以檢查目前的日誌記憶體指派，並在各種日誌類型之間重新指派日誌記憶體。
記錄不成功的 SSL 交握	建立不成功的 SSL 解密交握的詳細日誌，以便您查找解密問題的原因。預設會啟用。 日誌會佔用儲存空間。若要將更多（或更少）日誌儲存空間指派給解密日誌，則請編輯日誌記憶體指派（*Device*（裝置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定））。
日誌轉送	指定轉送 GlobalProtect SSL 交握（解密）日誌的方法和位置。

解密目標頁簽

- （僅限 Panorama）**Policies**（政策）> **Decryption**（解密）> **Target**（目標）

選取 **Target**（目標）頁簽以選取要向裝置群組中的哪些受管理裝置推送政策規則。您可以透過選取受管理防火牆或指定標籤，來指定要向其推送的受管理防火牆。此外，您可以設定政策規則目標，以向除了指定防火牆之外的所有受管理防火牆推送。

NAT 規則 - 目標設定	說明
任何（以所有裝置為目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。

© 2019 Palo Alto Networks, Inc.

NAT 規則 - 目標設定	說明
標籤	**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > Tunnel Inspection（原則 > 通道檢查）

您可設定防火牆以檢查下列純文字通道通訊協定的流量內容：

- 一般路由封裝 (GRE)
- 整合封包無線電服務 (GPRS) 使用者資料通道通訊協定 (GTP-U)；僅在支援 GTP 的防火牆。
- 非加密 IPSec 流量（IPSec 和傳輸模式 AH IPSec 的 NULL 加密演算法）。
- 虛擬廣泛 LAN(VXLAN)

您可使用通道內容檢查以在這些通道類型中的流量上強制執行安全性、DoS 保護、Qos 原則，以及在另一個純文字通道中巢狀的流量上強制執行（例如，在 GRE 通道內 Null 加密的 IPSec）。

建立通道檢查原則，當比對傳入封包時，該原則會決定防火牆將檢查封包中的哪個通道通訊協定，該原則也會指定防火牆該丟棄或繼續處理封包的條件。您可以在 ACC 中檢視通道檢查日誌及通道活動以確認通道流量符合您的企業安全性和使用原則。

防火牆在乙太網路介面與子介面、AE 介面、VLAN 介面、VPN 和 LSVPN 通道上支援通道內容檢查。第三層、第二層、Virtual Wire、旁接部署中支援該功能。通道內容檢查適用於共用閘道及虛擬系統至虛擬系統通訊。

您想了解什麼內容？	請參閱：
可用來建立通道檢查原則的欄位有哪些？	通道檢查原則中的建置組塊
如何檢視通道檢查日誌？	日誌類型與嚴重性等級
想知道更多？	通道內容檢查

通道檢查原則中的建置組塊

選取 **Policies**（原則）> **Tunnel Inspection**（通道檢查），然後新增通道檢測原則規則。您可以使用防火牆檢查純文字通道通訊協定（GRE、GTP-U、非加密 IPSec 和 VXLAN）的內容，並利用通道內容檢查對這些類型的通道中的流量實施安全、DoS 保護和 QoS 原則。所有防火牆模組都支援 GRE 和非加密 IPSec 通道的 tunnel content inspection（通道內容檢查），但只有支援 GTP 的防火牆才支援 GTP-U 通道的通道內容檢查。下表說明您可為通道檢查原則設定的欄位。

通道檢查原則中的建置組塊	設定位置	說明
名稱	總言	為通道檢查原則輸入以英數字元開頭，且包含零或多個英數字元、底線、連字號、點和空格字元的名稱。
說明		（選用）輸入通道檢查原則的說明。
標籤		（選用）輸入一或多個用於報告和記錄的頁籤，以識別受限於通道檢查原則的封包。

© 2019 Palo Alto Networks, Inc.

通道檢查原則中的建置組塊	設定位置	說明
依頁籤對規則分組		輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
稽核註解		輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔		檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。
來源區域	**Source**（來源）	為套用通道檢查原則的封包 **Add**（新增）一或多個來源區域（預設為[任何]）。
來源位址		（選用）為套用通道檢查原則的封包 **Add**（新增）來源 IPv4 或 IPv6 位址、位址群組或地區位址物件（預設為 **Any**（任何））。
來源使用者		（選用）為套用通道檢查原則的封包 **Add**（新增）來源使用者（預設為 **Any**（任何））。
否定		（選用）選取 **Negate**（否定），可選取任何除已指定位址外的位址。
目的地區域	目的地	為套用通道檢查原則的封包 **Add**（新增）一或多個目的地區域（預設值為 **Any**（任何））。
目的地位址		（選用）為套用通道檢查原則的封包 **Add**（新增）目的地 IPv4 或 IPv6 位址、位址群組或地區位址物件（預設為 **Any**（任何））。
否定		（選用）選取 **Negate**（否定），可選取任何除已指定位址外的位址。
通道通訊協定	檢查	**Add**（新增）一或多個要讓防火牆檢查的通道 **Protocols**（通訊協定）： • **GRE**—防火牆會檢查通道中使用 Generic Route Encapsulation 的封包。 • **GTP-U**—防火牆會檢查通道中使用整合封包無線電服務 (GPRS) 使用者資料通道通訊協定 (GTP-U) 的封包。 • **Non-encrypted IPSec**（非加密 **IPSec**）—防火牆會檢查通道中使用非加密 IPSec（Null 加密 IPSec 或傳輸模式 AH IPSec）的封包。 • **VXLAN**—防火牆檢查 VXLAN 有效負載以尋找通道中的封裝內容或應用程式。 若要從您的清單中移除通訊協定，請選取通訊協定並將其 **Delete**（刪除）。

© 2019 Palo Alto Networks, Inc.

通道檢查原則中的建置組塊	設定位置	說明
通道檢查層級上限	**Inspection**（檢查）> **Inspect Options**（檢查選項）	指定防火牆將檢查封裝的 **One Level**（一個層級）（預設）或 **Two Levels (Tunnel In Tunnel)**（二個層級）（通道中的通道）對於 VXLAN，由於檢查僅發生在較外層，請選取 **One Level**（一個層級）。
超過通道檢查層級上限則丟棄封包		（選用）丟棄包含的封裝層級超出您指定通道檢查層級上限的封包。
通道通訊協定嚴格標頭檢查失敗則丟棄封包		（選用）丟棄包含的通道通訊協定所使用的標頭與該通訊協定的 RFC 不相容的封包。不相容的標頭表示有可疑的封包。此選項會使防火牆根據 RFC 2890 驗證 GRE 標頭。 如果您的防火牆以實作舊版 *GRE*（早於 *RFC 2890* 的版本）的裝置建立 *GRE* 通道，請不要啟用此選項。
通道內含未知通訊協定則丟棄封包		（選用）丟棄通道內包含防火牆無法識別之通訊協定的封包。
將掃描的 VXLAN 通道返回至來源		（選用）啟用此選項以將流量返回至原始 VXLAN 通道端點 (VTEP)。例如，使用此選項可將封裝的封包返回到來源 VTEP。僅在第三層、第三層子介面、彙總介面第三層，以及 VLAN 上支援。
啟用安全性選項	**Inspection**（檢查）> **Security Options**（安全選項）	（選用）**Enable Security Options**（啟用安全性選項），以指派通道內容的個別安全性處理所適用的安全性區域。內部內容來源將屬於您所指定的 **Tunnel Source Zone**（通道來源區域），內部內容目的地將屬於您所指定的 **Tunnel Destination Zone**（通道目的地區域）。 若未 **Enable Security Options**（啟用安全性選項），則內部內容來源（預設）會屬於與外部通道來源相同的區域，而內部內容目的地會屬於與外部通道目的地相同的區域。因此，內部內容來源和目的地都會受限於套用到外部通道的來源和目的地區域的相同安全性原則。
通道來源區域		如果您 **Enable Security Options**（啟用安全性選項），請選取您建立的通道區域，內部內容將使用此來源區域來實施原則。 否則，默認情況下內部內容來源與外部通道來源屬於同一個區域，並且外部通道來源區域的原則也適用於內部內容來源區域。
通道目的地區域		如果您 **Enable Security Options**（啟用安全性選項），請選取您建立的通道區域，內部內容將使用此目的地區域來實施原則。 否則，默認情況下內部內容目的地與外部通道目的地屬於同一個區域，並且外部通道目的地區域的原則也適用於內部內容目的地區域。

© 2019 Palo Alto Networks, Inc.

通道檢查原則中的建置組塊	設定位置	說明
監控名稱	**Inspection**（檢查）> **Monitor Options**（監控選項）	（選用）輸入監控名稱，以將類似的流量分組在一起，進而在日誌和報告中監控流量。
監控頁籤 (數字)		（選用）輸入可將類似的流量分組在一起以進行記錄和報告的監控頁籤號碼（範圍是 1 到 16,777,215）。頁籤號碼是全域定義的。 此欄位不適用於 *VXLAN* 通訊協定。*VXLAN* 日誌自動使用 *VXLAN* 標頭中的 *VXLAN* 網路識別碼 *(VNI)*。
工作階段開始時的日誌		（選用）選取此選項可在符合通道檢測原則的純文字通道工作階段開始時生成日誌。此設置將取代適用於工作階段的安全性原則規則中的工作階段開始日誌設定。 通道日誌與流量日誌分開儲存。具有外部通道工作階段（GRE，非加密 IPSec 或 GTP-U）的資訊儲存在通道日誌中，內部流量儲存在流量日誌中。這種分隔使您可以輕鬆報告通道活動（而不是內部活動）與 ACC 和報告功能。 通道日誌的最佳實踐方法是在工作階段開始時和在工作階段結束時記錄日誌，因為對於日誌記錄來說，通道可能非常長壽。例如，*GRE* 通道可能在路由器啟動時會出現，而且可能直到路由器重新啟動時也不會終止。如果您不能在會話階段開始時選取日誌，則您將絕不會在 *ACC* 內看到一個主動的 *GRE*。
工作階段結束時的日誌		（選用）選取此選項可在符合通道檢測原則的純文字通道工作階段結束時擷取日誌。此設置將取代適用於工作階段的安全性原則規則中的工作階段結束日誌設定。
日誌轉送		（選用）從下拉式清單選取一個日誌轉送設定檔以指定轉送通道檢測日誌的地方。（此設定與安全性原則規則中的日誌轉送設定不同，該設定乃適用於流量日誌）。
名稱	**通道 ID** 在預設情況下，如果 沒有設定 VXLAN ID，則會檢查所有流量。 如果您設定了 VXLAN ID，則可以將其用作比對準則，以將流量檢查限制為特定 VNI。	（選用）以英數字元開頭，且包含零或多個英數字元、底線、連字號、點和空格字元的名稱。**Name**（名稱）描述了您正在分組的 VNI。名稱的用途是便於使用，不是記錄、監控或報告的一個因素。
VXLAN ID (VNI)		（選用）輸入單個 VNI，以逗號分隔的 VNI 清單，高達 1600 萬個 VNI（以連字號當作為分隔符號）的範圍，或以上的組合。例如： 1-54,1024,1677011-1677038,94 每個原則的 VXLAN ID 最大數量為 4,096。為保留設定記憶體，請盡可能在範圍內使用。

© 2019 Palo Alto Networks, Inc.

通道檢查原則中的建置組塊	設定位置	說明
任何（以所有裝置為目標） 僅限 Panorama	**Target**（目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置 僅限 Panorama		選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤 僅限 Panorama		**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標 僅限 Panorama		啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > Application Override（原則 > 應用程式取代）

若要變更防火牆將網路流量分類為應用程式的方式，您可以指定應用程式取代原則。例如，如果您要控制其中一個自訂應用程式，可以使用應用程式覆蓋原則，根據區域、來源與目的地位址、連接埠與通訊協定來識別該應用程式的流量。如果您有分類為「未知」的網路應用程式，可以為它們建立新應用程式定義（請參閱定義應用程式）。

如果可能，請避免使用應用程式覆寫原則，因為它們會阻止防火牆使用 *App-ID* 來識別應用程式以及防止針對威脅執行的第七層檢查。為了支援所有權應用程式，最好建立包含應用程式特徵碼的自訂應用程式，以便防火牆執行第七層檢查並針對威脅掃描應用程式流量。如果商業應用程式沒有 *App-ID*，請提交新的 App-ID 請求。如果因為公共應用程式定義（預設連接埠或特徵碼）發生更改，而導致防火牆不再能正確地識別應用程式，請建立支援票證，以便 *Palo Alto Networks* 可以更新定義。在此期間，請建立自訂應用程式，以便防火牆繼續執行第七層流量檢查。

與安全原則一樣，根據需要，應用程式覆蓋原則可以是一般性的，也可以是特定的。會按順序針對流量比較原則規則，因此更特定的規則必須在更一般性的規則之前。

由於 PAN-OS 中的 App-ID 引擎憑藉識別網路流量中的應用程式特定內容來分類流量，因此自訂應用程式定義無法單靠使用埠號來識別應用程式。應用程式定義也必須包含流量（受限於來源區域、來源 IP 位址、目的地區域與目的地 IP 位址）。

若要使用應用程式覆蓋來建立自訂應用程式：

- 建立自訂應用程式（請參閱定義應用程式 ）。如果應用程式僅用於應用程式取代規則，則不需要指定應用程式的特徵碼。
- 定義應用程式覆蓋原則，它可指定應在何時叫用自訂應用程式。原則通常包含執行自訂應用程式之伺服器的 IP 位址，及一組受限的來源 IP 位址或來源區域。

使用下表來設定應用程式取代規則。

- 應用程式取代一般頁籤
- 應用程式取代來源頁籤
- 應用程式取代目的地頁籤
- 應用程式取代通訊協定/應用程式頁籤
- （僅限 Panorama）應用程式取代目標頁籤

想知道更多？

參閱在原則中使用應用程式物件

應用程式取代一般頁籤

選取 **General**（一般）頁籤可設定應用程式覆蓋原則的名稱和描述。存在大量原則時，也可以設定標記來排序或篩選這些原則。

欄位	說明
名稱	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，

© 2019 Palo Alto Networks, Inc.

欄位	說明
	而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入規則的描述（最多 1024 個字元）。
頁籤	如果您需要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要標記連入 DMZ 的特定安全性原則，標記含解密與無解密文字的解密原則，或者對與該位置相關聯的原則使用特定資料中心名稱。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以選取根據頁籤對規則分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔	檢視原則規定過去的稽核註解。稽核註解封存檔可以 CSV 格式匯出。

應用程式取代來源頁籤

選取 **Source**（來源）頁籤可定義來源區域或來源位址，從而定義哪些連入的來源流量將套用應用程式覆寫政策。

欄位	說明
來源區域	**Add**（新增）來源區域（預設為 **any**（任何））。區域的類型必須相同（第二層、第三層或 Virtual Wire）。若要定義新區域，請參閱 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。
來源位址	**Add**（新增）來源位址、位址群組或區域（預設為 **any**（任何））。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。 選取 **Negate**（否定）可選擇除已設定位址以外的任何位址。

應用程式取代目的地頁籤

選取 **Destination**（目的地）頁籤可定義目的地區域或目的地位址，從而定義將套用政策的目的地流量。

© 2019 Palo Alto Networks, Inc.

欄位	說明
目的地區域	按一下 **Add**（新增）可選擇目的地區域（預設為 any（任何））。區域的類型必須相同（第二層、第三層或 Virtual Wire）。若要定義新區域，請參閱 Network > Zones（網路 > 區域）。 多個區域可以用來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。
目的地位址	按一下 **Add**（新增）可新增目的地位址、位址群組或地區（預設為 [任何]）。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）、**Address Group**（位址群組）或 **Regions**（區域），然後指定設定。 選取 **Negate**（否定）可選擇除已設定位址以外的任何位址。

應用程式取代通訊協定/應用程式頁籤

選取 **Protocol/Application**（通訊協定/應用程式）頁籤定義通訊協定（TCP 或 UDP）、連接埠及應用程式，進一步定義政策符合的應用程式屬性。

欄位	說明
通訊協定	選取要允許應用程式覆寫的通訊協定（**TCP** 或 **UDP**）。
連接埠	輸入指定目的地位址的埠號（0 至 65535）或埠號範圍（連接埠 1 - 連接埠 2）。多個連接埠或範圍必須以逗號隔開。
應用程式	為符合以上規則準則的流量選取覆蓋應用程式。覆蓋自訂應用程式時，不會進行任何威脅檢驗。您覆寫預先定義的應用程式支援威脅檢驗時則為例外。 若要定義新的應用程式，請參考 物件 > 應用程式。

應用程式取代目標頁籤

- （僅限 Panorama）**Policies**（政策）> **Application Override**（應用程式取代）> **Target**（目標）

選取 **Target**（目標）頁簽以選取要向裝置群組中的哪些受管理裝置推送政策規則。您可以透過選取受管理防火牆或指定標籤，來指定要向其推送的受管理防火牆。此外，您可以設定政策規則目標，以向除了指定防火牆之外的所有受管理防火牆推送。

NAT 規則 - 目標設定	說明
任何（以所有裝置為目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤	**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。

© 2019 Palo Alto Networks, Inc.

NAT 規則 - 目標設定	說明
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > Authentication（原則 > 驗證）

驗證原則讓您可在一般使用者存取網路資源前驗證他們。

您想了解什麼內容？	請參閱：
可用來建立驗證規則的欄位有哪些？	驗證原則規則的建置組塊
如何使用 Web 介面來管理驗證原則？	建立和管理驗證原則 針對 Panorama，請參閱移動或複製原則規則
想知道更多？	驗證原則

驗證原則規則的建置組塊

每當使用者要求資源時（例如造訪網頁時），防火牆就會評估驗證原則。根據相符的原則規則，防火牆接下來會提示使用者回應不同因素（類型）的一或多個挑戰，例如登入和密碼、語音、簡訊、推送，或一次性密碼 (OTP) 驗證。在使用者回應所有因素後，防火牆會評估安全性原則（請參閱 [原則 > 安全性]），以決定是否允許對資源的存取。

如果使用者透過內部或通道模式下的 GlobalProtect™ 閘道 存取非網頁型資源（例如印表機），防火牆就不會提示使用者進行驗證。此時，使用者將會看見連線失敗訊息。為確保使用者可存取這些資源，請設定驗證入口網站，並教育使用者在看見連線失敗時應造訪該入口網站。請諮詢 *IT* 部門以設定驗證入口網站。

下表說明驗證原則規則中的每個建置組塊或元件。在您新增規則之前，請先完成建立和管理驗證原則中所述的先決條件。

驗證規則中的建置組塊	設定位置	說明
規則編號	無	每個規則會自動編號，其順序會隨著規則移動而改變。當您篩選規則以符合特定篩選器時，**Policies**（原則）> **Authentication**（驗證）頁面會在規則庫之完整規則集的內容中列出每個規則及其號碼，及其在評估順序中的位置。如需詳細資訊，請參閱規則順序及其評估順序。
名稱	總言	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明		輸入規則的描述（最多 1024 個字元）。
頁籤		選取用來排序及篩選規則的頁籤（請參閱 [物件 > 頁籤]）。
依頁籤對規則分組		輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。

© 2019 Palo Alto Networks, Inc.

驗證規則中的建置組塊	設定位置	說明
稽核註解		輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔		檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。
來源區域	**Source**（來源）	**Add**（新增）區域，以僅對從您指定之區域中的介面傳入的流量套用規則（預設值為 **Any**（任何））。 若要定義新區域，請參閱 [網路 > 區域]。
來源位址		**Add**（新增）位址或位址群組，以僅對源自您指定之來源的流量套用規則（預設值為 **Any**（任何））。 選取 **Negate**（否定），可選取已選取的位址以外的任何位址。 若要定義新的位址或位址群組，請參閱 [物件 > 位址] 和 [物件 > 位址群組]。
來源使用者	使用者	選取要套用規則的來源使用者或使用者群組： • 任何—包含任何流量，無論來源使用者為何。 • 預先登入—包含未登入用戶端系統、但其用戶端系統已透過 GlobalProtect 預先登入功能連線至網路的遠端使用者。 • 已知使用者—包含所有在規則引發驗證之前，防火牆已為其進行 IP 位址至使用者名稱對應的使用者。 • 未知—包含防火牆未進行其 IP 位址至使用者名稱對應的所有使用者。在規則引發驗證後，防火牆會根據未知使用者所輸入的使用者名稱建立其使用者對應。 • 選取—僅包含您 **Add**（新增）至來源使用者清單的使用者和使用者群組。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。
來源 HIP 設定檔		**Add**（新增）host information profile（主機資訊設定檔 - HIP）可讓您收集主機安全性狀態的相關資訊，例如它們是否具有最新的安全性修補程式以及防毒定義。如需詳細資訊，或是要定義新的 HIP，請參閱 [物件 > GlobalProtect > HIP 設定檔]。
目的地區域	目的地	**Add**（新增）區域，以僅對進入指定區域中之介面的流量套用規則（預設值為 **Any**（任何））。若要定義新區域，請參閱 [網路 > 區域]。

© 2019 Palo Alto Networks, Inc.

驗證規則中的建置組塊	設定位置	說明
目的地位址		**Add**（新增）位址或位址群組，以僅對您所指定的目的地套用規則（預設值為 **Any**（任何））。 選取 **Negate**（否定），可選取已選取的位址以外的任何位址。 若要定義新的位址或位址群組，請參閱 [物件 > 位址] 和 [物件 > 位址群組]。
服務	服務/**URL** 類別	從下列選項中進行選取，以僅對特定 TCP 和 UDP 連接埠號碼上的服務套用規則： • 任何—指定任何連接埠上使用任何通訊協定的服務。 • 預設值—僅指定 Palo Alto Networks 所定義之預設連接埠上的服務。 • 選取—可讓您 **Add**（新增）服務或服務群組。若要建立新的服務和服務群組，請參閱 [物件 > 服務] 和 [物件 > 服務群組]。 預設選項是 *service-http*。當您為驗證入口網站使用驗證政策時，也請啟用 *service-https* 以確保防火牆為所有網路流量學習使用者至 *IP* 位址對應。
URL 類別		選取要套用規則的 URL 類別： • 選取 **any**（任何）可指定所有流量，無論 URL 類別為何。 • **Add**（新增）類別。若要定義自訂類別，請參閱 [物件 > 自訂物件 > URL 類別]。
驗證執行	動作	選取可指定方法（例如驗證入口網站或瀏覽器質詢）的驗證強制執行物件（Objects（物件）> Authentication（驗證）），以及防火牆用來驗證使用者的驗證設定檔。驗證設定檔會定義使用者須回應單一挑戰還是多因素驗證（請參閱 [裝置 > 驗證設定檔]）。您可以選取預先定義或自訂的驗證強制執行物件。 如果您必須從驗證入口網站政策排除主機或伺服器，請將它們新增至將 *Authentication Enforcement*（驗證執行）指定為 *no-captive-portal*（無被控制的入口網站）的驗證設定檔。然而，驗證入口網站政策會幫助防火牆學習使用者至 *IP* 位址對應，並應盡可能使用。
逾時		若要降低驗證挑戰干擾使用者工作流程的頻率，您可以在防火牆提示使用者進行資源重複存取的一次性驗證時，指定以分鐘為單位的間隔（預設值為 60）。 如果 **Authentication Enforcement**（驗證強制執行）物件指定了多因素驗證，則使用者必須逐一進行各個因素的驗證。

© 2019 Palo Alto Networks, Inc.

驗證規則中的建置組塊	設定位置	說明
		防火牆會記錄時間戳記，並且僅在某個因素的逾時到期後才重新發出挑戰。將時間戳記重新散佈給其他防火牆，可讓您套用逾時，即使最初允許使用者存取的防火牆並非後續對該使用者的存取進行控管的相同防火牆，仍是如此。 *Timeout*（逾時）是更嚴格的安全性（兩次出現驗證提示的間隔時間較短）與使用者體驗（兩次出現驗證提示的間隔時間較長）之間的權衡。存取重要系統以及敏感區域（如資料中心）時，通常需要進行更為頻繁的驗證。對於網路周邊以及那些使用者體驗對其至關重要的企業而言，進行驗證的頻率通常較低。 對於外圍資源，將數值設定為 *480* 分鐘（*8* 小時），對於資料中心資源以及重要系統，設定較低的數值（如 *60* 分鐘）以加強安全性。視需要監控和調整數值。
日誌驗證逾時		如果要讓防火牆在與驗證因素相關聯的 **Timeout**（逾時）到期時即產生驗證日誌，請選取此選項（預設為停用）。啟用此選項，可以有更多資料供存取問題的疑難排解使用。驗證日誌也可以與關聯物件搭配使用，以識別網路上的可疑活動（例如暴力攻擊）。 啟用此選項會增加日誌流量。
日誌轉送		如果要讓防火牆將驗證日誌轉送至 Panorama 或外部服務（例如 syslog 伺服器），請選取日誌轉送設定檔（請參閱 [物件 > 日誌轉送]）。
任何（以所有裝置為目標） 僅限 Panorama	**Target**（目標）	啟用（核取）以將政策規則推送到裝置群組中的所有受管理防火牆。
裝置 僅限 Panorama		選取與裝置群組關聯的一個或多個受管理防火牆以向其推送政策規則。
標籤 僅限 Panorama		**Add**（新增）一個或多個標籤以將政策規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標 僅限 Panorama		啟用（核取）以將政策規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

建立和管理驗證原則

選取 **Policies**（原則）> **Authentication**（驗證）頁面，可建立及管理驗證原則規則：

工作	說明
Add（新增）	建立驗證原則規則之前，請先執行下列必要工作： ❑ 設定 User-ID™ 驗證入口網站設定（請參閱 Device > User Identification > Authentication Portal Settings（裝置 > 使用者識別 > 驗證入口網站設定））。防火牆會使用驗證入口網站顯示驗證規則所需的第一個驗證因素。驗證入口網站也啟動防火牆記錄與驗證逾時期間相關聯的時間戳記，並更新使用者的對應。 ❑ 設定指定防火牆存取驗證使用者服務方法的伺服器設定檔（參閱 Device > Server Profiles（裝置 > 伺服器設定檔））。 ❑ 指派伺服器設定檔至指定驗證設定的驗證設定檔（參閱 Device > Authentication Profile（裝置 > 驗證設定檔））。 ❑ 指派驗證設定檔至指定驗證方法的驗證強制執行物件（參閱 Objects > Authentication（物件 > 驗證））。 若要建立規則，請執行下列其中一個步驟，然後完成驗證原則規則的建置組塊中說明的欄位： • 按一下 **Add**（新增）。 • 選取新規則的基礎規則，然後按一下 **Clone Rule**（複製規則）。防火牆會在選取的規則下方插入複製的規則（名為 <rulename>#），其中，# 是使規則名稱成為唯一名稱的下一個可用整數，並為複製規則製造新的 UUID。如需詳細資訊，請參閱移動或複製原則規則。
修改	若要修改規則，請按一下規則名稱，並編輯驗證原則規則的建置組塊中所述的欄位。 如果防火牆接收到來自 *Panorama* 的規則，該規則將是唯讀的；您只能在 *Panorama* 上加以編輯。
移動	比對流量時，防火牆依據規則在 **Policies**（原則）> **Authentication**（驗證）頁面中列出的順序由上至下評估規則。若要變更評估順序，請選取規則並 **Move Up**（上移）、**Move Down**（下移）、**Move Top**（移至頂部）或 **Move Bottom**（移至底部）。如需詳細資訊，請參閱移動或複製原則規則。
Delete（刪除）	若要移除現有規則，請選取規則並加以 **Delete**（刪除）。
啟用/停用	若要停用規則，請選取規則並加以 **Disable**（停用）。若要重新啟用已停用的規則，請選取規則並加以 **Enable**（啟用）。
反白顯示未使用的規則	若要識別自上次防火牆重新啟動後未比對出流量的規則，請選取 **Highlight Unused Rules**（反白顯示未使用的規則）。接著，您可以決定要停用或刪除未使用的規則。頁面會以黃色虛線背景反白顯示未使用的規則。
預覽規則（僅限 Panorama）	按一下 **Preview Rules**（預覽規則）可先檢視規則清單，再將規則推送至受管理防火牆。在每個規則庫內，頁面都會視覺方式區分各個裝置群組（和受管理的防火牆）的規則階層，以利掃描眾多的規則。

© 2019 Palo Alto Networks, Inc.

Policies > DoS Protection（原則 > DoS 保護）

Dos 保護原則讓您可針對 DoS 攻擊防護個人重大資源，具體方法是指定要拒絕或允許符合來源介面、區域、位址或使用者和 / 或目的地介面、區域、使用者的封包。

或者，您也可選取保護動作並指定 DoS 設定檔，在此設定觸發警報的臨界值（每秒的工作階段或封包數）、啟動保護動作、指出上述丟棄全部全新連線的最大速率。因此，您可以根據彙總工作階段或來源和/或目的地 IP 位址，控制介面、區域、位址與國家/地區之間的工作階段數量。例如，您可以控制與特定位址或位址群組之間的往來流量，或來自特定使用者的流量及適用於特定服務的流量。

防火牆會在強制執行安全性規則之前強制執行 DoS 保護原則規則，以確保防火牆以最有效率方式使用資源。若 DoS 保護原則規則拒絕封包，則該封包永不會到達安全性原則規則。

下表說明 DoS 保護設定檔設定：

- DoS 保護一般頁籤
- DoS 保護來源頁籤
- DoS 保護目的地頁籤
- DoS 保護選項/保護頁籤
- （僅限 Panorama）DoS 保護目標頁簽

想知道更多？

請參閱 DoS Protection Profiles（DoS 保護設定檔）和 Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）。

DoS 保護一般頁籤

- **Policies**（原則）> **DoS Protection**（**DoS** 保護）> **General**（一般）

選取 **General**（一般）頁籤可設定 DoS 保護原則的名稱和說明。存在許多原則時，您也可以設定頁籤來排序或篩選這些原則。

欄位	說明
名稱	輸入用來識別 DoS 保護原則規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入規則的描述（最多 1024 個字元）。
標籤	如果您想要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此頁籤十分實用。例如，您可能想要標記連入 DMZ 的特定安全性原則，標記含解密或無解密文字的解密原則，或者對與該位置相關聯的原則使用特定資料中心名稱。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以根據頁籤對規定分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。

© 2019 Palo Alto Networks, Inc.

欄位	說明
稽核註解封存檔	檢視原則規定過去的稽核註解。您可以 CSV 格式匯出稽核註解封存檔。

DoS 保護來源頁籤

選取 **Source**（來源）頁籤可定義來源介面或來源區域，以及（選擇性地）定義套用 DoS 政策規則的傳入流量的來源位址和來源使用者。

欄位	說明
類型	選取套用 DoS 保護政策規則的來源類型： • 介面—將規則套用至指定介面或介面群組傳入的流量。 • 區域—將規則套用至指定區域中任何介面傳入的流量。 按一下 **Add**（新增）可選取多個介面或區域。
來源位址	選取 **Any**（任何）或 **Add**（新增）並指定一個或多個要套用 DoS 保護政策規則的來源位址。 （選用）選取 **Negate**（否定）可指定規則套用至任何位址，已指定的除外。
來源使用者	指定一個或多個要套用 DoS 保護政策規則的來源使用者： • 任何—包含封包，無論來源使用者為何。 • 預先登入—包含使用 GlobalProtect 連線至網路，但未登入其系統的遠端使用者所提供的封包。在入口網站上設定 GlobalProtect 應用程式的 **pre-logon**（預先登入）時，將以使用者名稱預先登入識別目前未登入其電腦的任何使用者。您接著可為預先登入使用者建立政策，且使用者即便未直接登入，也會在網域上驗證其電腦，如同這些使用者已完全登入一般。 • 已知使用者—包含所有驗證的使用者，意味已對應使用者資料的任何 IP 位址。此選項等同於網域上的「網域使用者」群組。 • 未知—包含所有未驗證的使用者，意味未對應至使用者的 IP 位址。例如，您可以使用 **unknown**（未知），供來賓等級的使用者存取某些資訊，因為他們雖然在您的網路上擁有 IP 位址，但不會經過網域驗證，且在防火牆上沒有 IP 位址至使用者對應資訊。 • 選取—包含本視窗中指定的使用者。例如，您可以選取一名使用者、個人清單、部分群組，或手動新增使用者。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。

DoS 保護目的地頁籤

選取 **Destination**（目的地）頁籤可定義目的地區域或介面及目的地位址，從而定義哪些目的地流量將套用政策。

© 2019 Palo Alto Networks, Inc.

欄位	說明
類型	選取 DoS 保護政策規則要套用的目的地類型： • 介面—將規則套用至前往指定介面或介面群組的封包。按一下 **Add**（新增）並選取一或多個介面。 • 區域—將規則套用至前往指定區域中任何介面的封包。按一下 **Add**（新增）並選取一或多個區域。
目的地位址	選取 **Any**（任何）或 **Add**（新增），並指定一或多個 DoS 保護政策規則要套用的目的地位址。 （選用）選取 **Negate**（否定）可指定規則套用至任何位址，已指定的除外。

DoS 保護選項/保護頁籤

選取 **Option/Protection**（選項 / 保護）頁籤可設定 DoS 保護原則規則的選項，例如套用規則的服務類型、針對符合規則之封包所執行的動作，以及是否觸發相符流量的日誌轉送。您可以定義何時啟動規則的時程。

您也可以選取彙總 DoS 保護設定檔和/或已分類的 DoS 保護設定檔，其可決定超過時會造成防火牆採取保護行動（例如觸發警報、啟動如隨機早期丟棄的行動，以及丟棄超過最大臨界值速率的封包）的臨界值速率。

欄位	說明
服務	按一下 **Add**（新增）並選取要套用 DoS 保護原則的一個或多個服務。預設為 **Any**（任何）服務。例如，如果 DoS 原則保護 Web 伺服器，請指定 Web 應用程式的 HTTP、HTTPS 和任何其他適當的服務連接埠。 對於關鍵伺服器，請建立單獨的 *DoS* 保護規則以保護未使用的服務連接埠，從而幫助防止針對性攻擊。
動作	選取防火牆在符合 DoS 保護原則規則的封包上執行的動作： • 拒絕—丟棄所有符合規則的封包。 • 允許—允許所有符合規則的封包。 • **Protect**（保護）—對符合規則的封包強制執行指定 DoS 保護設定檔內指定的保護。符合規則的封包會計入 DoS 保護設定檔中的臨界值速率，其會依次觸發警報、啟動另一個動作，並在超過最大速率時觸發封包丟棄。 套用 *DoS* 保護的目的是防止 *DoS* 攻擊，因此您通常應使用 *Protect*（保護）。*Deny*（拒絕）會丟棄合法流量以及 *DoS* 流量，而 *Allow*（允許）則不會阻止 *DoS* 攻擊。使用 *Deny*（拒絕）與 *Allow*（允許）僅可在群組內建立例外情況。例如，您可以拒絕來自大多數群組的流量，但允許該流量的子集；或允許來自大多數群組的流量，但拒絕該流量的子集。
排程	指定當 DoS 保護原則規則生效時的排程。預設 **None**（無）的設定表示無排程；原則一律為生效。 或者，選取排程或建立新的排程以控制 DoS 保護原則規則何時生效。輸入排程的 **Name**（名稱）。選取 **Shared**（共用）可與多個虛擬系統防火牆上的每個虛擬系統共用此排程。選取 **Recurrence**（週期性）的 **Daily**（每日）、**Weekly**（每週）或 **Non-recurring**（非

© 2019 Palo Alto Networks, Inc.

欄位	說明
	週期性）。根據 24 小時制，以 hours:minutes 格式新增 **Start Time**（開始時間）和 **End Time**（結束時間）。
日誌轉送	如果您要觸發對外部服務的相符流量之威脅日誌項目的轉送，例如對 Syslog 伺服器或 Panorama，請選取日誌轉送設定檔，或按一下 **Profile**（設定檔）來建立一個新的。 防火牆僅記錄和轉送符合規則中動作的流量。 對於較簡易的管理，透過電子郵件將單獨來自其他「威脅」日誌的 *DoS* 日誌直接轉送給管理員和日誌伺服器。
aggregate	彙總 DoS 保護設定檔設定套用於 DoS 保護規則中指定的組合裝置群組的臨界值，以保護這些伺服器群組。例如，警報速率臨界值 10,000 CPS 意味著當整個群組的新 CPS 總數超過 10,000 CPS 時，防火牆會觸發警報訊息。 選取指定每秒傳入連線觸發警報的閾值速率之彙總 DoS 保護設定檔、啟動動作，以及超過最大速率。所有傳入連線（彙總）會計入彙總 DoS 保護設定檔中所指定的臨界值。 彙總設定檔的 **None**（無）設定表示並未具備臨界值流量的臨界值設定。請參閱 Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）。
已分類	分類 DoS 保護設定檔設定套用於 DoS 保護規則中指定的每個個別裝置的臨界值，以保護個別或小型重要伺服器群組。例如，警報速率閾值 10,000 CPS 意味著當規則中指定之任何個別伺服器的新 CPS 總數超過 10,000 CPS 時，防火牆會觸發警報訊息。 選取此選項並指定下列各項： • 設定檔—選取要套用到此規則的分類 DoS 保護設定檔。 • 位址—如果傳入連線符合 **source-ip-only**、**destination-ip-only** 或 **src-dest-ip-both**，選取是否要將傳入連線計入設定檔中的臨界值。 防火牆耗用更多資源追蹤 *src-dest-ip-both* 計數器，而不是只追蹤來源 *IP* 或目的地 *IP* 計數器。 若您指定已分類 DoS 保護設定檔，則只有符合來源 IP 位址、目的地 IP 位址或目的地 IP 位址配對的傳入連線會計入設定檔中指定的臨界值。例如，您可以指定 **Max Rate**（最大速率）為 100 cps 的分類 DoS 保護設定檔，並指定規則中 **Address**（位址）設定 **source-ip-only**。針對該特殊來源 IP 位址，結果將限制在每秒 100 個連線之內。 不用將 *source-ip-only* 或 *src-dest-ip-both* 用於網際網路連結的區域，因為防火牆無法儲存用於所有可能的網際網路 *IP* 位址的計數器。在周邊區域中使用 *destination-ip-only*。 使用 *destination-ip-only* 保護個別重要裝置。 使用 *source-ip-only* 和 *Alarm*（警報）閾值可監控非網際網路連結區域內的可疑主機。 請參閱 Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）。

DoS 保護目標頁簽

- （僅限 Panorama）**Policies**（政策）> **DoS Protection**（**DoS** 保護）> **Target**（目標）

© 2019 Palo Alto Networks, Inc.

選取 **Target**（目標）頁簽以選取要向裝置群組中的哪些受管理裝置推送原則規則。您可以透過選取受管理防火牆或指定標籤，來指定要向其推送的受管理防火牆。此外，您可以設定原則規則目標，以向除了指定防火牆之外的所有受管理防火牆推送。

NAT 規則 - 目標設定	說明
任何（以所有裝置為目標）	啟用（核取）以將原則規則推送到裝置群組中的所有受管理防火牆。
裝置	選取與裝置群組關聯的一個或多個受管理防火牆以向其推送原則規則。
標籤	**Add**（新增）一個或多個標籤以將原則規則推送到具有指定標籤的裝置群組中的受管理防火牆。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（核取）以將原則規則推送到與除所選裝置和標籤之外的裝置群組關聯的所有受管理防火牆。

© 2019 Palo Alto Networks, Inc.

Policies > SD-WAN（政策 > SD-WAN）

新增 SD-WAN 政策，以根據您設定的健康情況抖動、延遲和封包遺失健康情況指標，為每個應用程式或遍歷相同連結的一組應用程式設定連結路徑管理設定。若關鍵應用程式的來源和目的地之間的某些路徑經歷降級，則 SD-WAN 政策規則將選取新的最佳路徑，以確保敏感和關鍵應用程式根據 SD-WAN 政策規則中為其指派的路徑品質設定檔來執行。

- SD-WAN 一般頁籤
- SD-WAN 來源籤
- SD-WAN 目的地頁籤
- SD-WAN 應用程式/服務頁籤
- SD-WAN 路徑選取頁籤
- （僅限 Panorama）SD-WAN 目標頁籤

SD-WAN 一般頁籤

- **Policies**（政策）> **SD-WAN** > **General**（一般）

選取 **General**（一般）頁籤可設定 SD-WAN 政策的名稱和說明。存在大量原則時，也可以設定標記來排序或篩選這些原則。

欄位	說明
名稱	輸入用來識別規則的名稱。名稱須區分大小寫，最多可包含 63 個字元，可以是字母、數字、空格、連字號和底線。名稱在防火牆上必須為唯一名稱，而在 Panorama 上則必須在其裝置群組和任何父系或子系裝置群組中為唯一名稱。
說明	輸入規則的說明（最多 1024 個字元）。
頁籤	如果您需要標記原則，請 **Add**（新增）並指定頁籤。 原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要使用獨特的標籤標記特定 SD-WAN 政策，以識別規則套用至的特定中樞或分支。
依頁籤對規則分組	輸入頁籤，將相似的原則規定分組。群組頁籤讓您可以根據這些頁籤檢視您的原則規定。您可以選取根據頁籤對規則分組。
稽核註解	輸入註釋以稽核原則規定的建立或編輯。稽核註解須區分大小寫，最多可包含 256 個字元，可以是字母、數字、空格、連字號和底線。
稽核註解封存檔	檢視原則規定過去的稽核註解。稽核註解封存檔可以 CSV 格式匯出。

SD-WAN 來源籤

- **Policies**（政策）> **SD-WAN** > **Source**（來源）

選取 **Source**（來源）頁籤以定義來源區域、來源位址和來源使用者（其定義 SD-WAN 政策套用至的傳入封包）。

© 2019 Palo Alto Networks, Inc.

欄位	說明
來源區域	若要指定來源區域，請選取 **Add**（新增）並選取一個或多個區域，或者選取 **Any**（任何）區域。 指定多個區域可以簡化管理。例如，如果您有三個分支位於不同的區域中，您希望全部三個分支的比對規則和路徑選取保持相同，則可以建立一個 SD-WAN 規則並指定三個來源分區以涵蓋三個分支。 對於 *SD-WAN* 政策規則，僅支援第三層類型區域。
來源位址	若要指定來源位址，可 **Add**（新增）來源位址或外部動態清單 (EDL)、從下拉式清單中選取或選取 **Address**（位址）並建立新的位址物件。或者選取 **Any**（任何）來源位址（預設值）。
來源使用者	若要指定特定使用者，請選取 **Add**（新增）（類型，然後指示 **select**（選取）），然後輸入使用者、使用者清單或使用者群組。或者選取使用者類型： • **any**（任何）—（預設值）包含任何使用者，不論使用者資料為何。 • 預先登入—包含使用 GlobalProtect™ 連線至網路，但未登入其系統的遠端使用者。在 [入口網站] 上設定 GlobalProtect 應用程式的 [預先登入] 選項時，將以使用者名稱預先登入識別目前未登入其電腦的任何使用者。您接著可為預先登入使用者建立原則，且使用者即便未直接登入，也會在網域上驗證其電腦，如同這些使用者已完全登入一般。 • 已知使用者—包含所有驗證的使用者，意味已對應使用者資料的任何 IP 位址。此選項等同於網域上的「網域使用者」群組。 • 未知—包含所有未驗證的使用者，意味未對應至使用者的 IP 位址。例如，您可以使用 **unknown**（未知），供來賓等級的使用者存取某些資訊，因為他們雖然在您的網路上擁有 IP 位址，但不會經過網域驗證，且在防火牆上沒有 IP 位址至使用者對應資訊。 如果防火牆從 *RADIUS*、*TACACS+* 或 *SAML* 識別提供者伺服器收集使用者資訊，而不是從 *User-ID*™ 代理程式收集，則不會顯示使用者清單；您必須手動輸入使用者資訊。

SD-WAN 目的地頁籤

- **Policies**（政策）> **SD-WAN** > **Destination**（目的地）

選取 **Destination**（目的地）頁籤可定義目的地區域或目的地位址，從而定義將套用 SD-WAN 政策規則的流量。

欄位	說明
目的地區域	**Add**（新增）目的地區域（預設為 any（任何））。區域必須是第三層。若要定義新區域，請參考 Network > Zones（網路 > 區域）。 可以新增多個區域來簡化管理。例如，如果您有三個不同的內部區域（行銷、銷售與公共關係），它們都導向不受信任的目的地區域，您可以建立一個適用於所有情況的規則。

© 2019 Palo Alto Networks, Inc.

欄位	說明
目的地位址	**Add**（新增）目的地位址、位址群組、外部動態清單 (EDL) 或地區（預設值為 **Any**（任何））。從下拉式清單中選取，或按一下下拉式清單底部的 **Address**（位址）或 **Address Group**（位址群組），然後指定設定。 選取 **Negate**（否定）可選擇除已設定位址以外的任何位址。

SD-WAN 應用程式/服務頁籤

- **Policies**（政策）> **SD-WAN** > **Application/Service**（應用程式/服務）

選取 **Application/Service**（應用程式/服務）頁籤以指定要套用 SD-WAN 政策規則的應用程式或服務，並指定套用於該應用程式或服務的設定檔（路徑品質、SaaS 品質和錯誤更正設定檔）。

欄位	說明
Saas 品質設定檔	選取路徑品質設定檔，其確定要套用至指定的應用程式和服務的最大抖動、延遲和封包遺失百分比閾值。如果尚未建立路徑品質設定檔，可建立 **New SD-WAN Path Quality Profile**（新的 **SD-WAN** 路徑品質設定檔）。
SaaS 品質設定檔	選取 SaaS 品質設定檔，針對具有直接網際網路存取 (DIA) 至軟體即服務 (SaaS) 應用程式連結的中樞或分支防火牆的延遲、抖動和封包遺失，指定路徑品質閾值。如果尚未建立 SaaS 品質設定檔，則可建立 **New SaaS Quality Profile**（新的 **SaaS** 品質設定檔）。預設值為 **None (disabled)**（無（已停用））。
錯誤更正設定檔	選取 **Error Correction Profile**（錯誤更正設定檔）或建立新的錯誤更正設定檔，用於指定可控制規則中指定應用程式或服務的正向錯誤更正 (FEC) 或路徑複製的參數。中樞或分支防火牆均可使用此設定檔。預設值為 **None (disabled)**（無（已停用））。
應用程式	為SD-WAN 政策規則 **Add**（新增）特定應用程式，或者選取 **Any**（任何）。如果應用程式具有多個功能，可選取整個應用程式或個別功能。如果您選取整個應用程式，會包含所有功能，且會在新增未來功能後自動更新應用程式定義。 如果您在 SD-WAN 政策規則中使用應用程式群組、篩選或容器，可以懸停在 Application（應用程式）欄中的物件上，開啟下拉式清單，並選取 **Value**（值），檢視這些物件的詳細資訊。這可以讓您直接從原則檢視應用程式成員，而不需要導覽至 **Object**（物件）頁籤。 僅新增受延遲、抖動或封包遺失影響的業務關鍵應用程式。避免新增應用程式類別或子類別，因為類別或子類別太廣泛，不允許逐個應用程式控制。
服務	為 SD-WAN 政策規則 **Add**（新增）特定服務，並選取在哪些連接埠上允許或拒絕來自這些服務的封包。 • **any**（任何）—任何通訊協定或連接埠上都允許或拒絕所選服務。 • **application-default**（應用程式預設值）—僅在 **Palo Alto Networks®** 定義的預設連接埠上允許或拒絕所選服務。建議將此選項用於如下政策：指定 **allow**（允許），因為它能防止服務在異常的連接埠和通訊協定上執

© 2019 Palo Alto Networks, Inc.

欄位	說明
	行，即使不是蓄意的行為，也可能是不想要的服務行為和用法出現的徵兆。 使用此選項時，僅實施符合 *SD-WAN* 政策的預設連接埠及動作。可能允許不在預設連接埠上的其他服務，具體取決於安全性政策規則，但是不符合 *SD-WAN* 政策，不會執行任何 *SD-WAN* 政策規則動作。 對於大多數服務，使用 *application-default*（應用程式預設值）來防止應用程式使用非標準連接埠或表現出其他規避性行為。如果服務的預設連接埠發生變更，防火牆會自動將規則更新為正確的預設連接埠。對於使用非標準連接埠的服務（如內部自訂服務），請修改服務或建立指定非標準連接埠的規則，並僅將規則套用至需要服務的流量。 • **Select**（選取）—**Add**（新增）現有的服務或選取**Service**（服務）或**Service Group**（服務群組），指定新項目。（或選取 [物件 > 服務] 和 [物件 > 服務群組]）。

SD-WAN 路徑選取頁籤

- **Policies**（政策）> **SD-WAN** > **Path Selection**（路徑選取）

選取 **Path Selection**（路徑選擇）頁籤，以定義在主要路徑品質超過「路徑品質設定檔」中設定的路徑品質閾值的情況下，要交換的應用程式或服務流量的路徑。

欄位	說明
流量散佈設定檔	從下拉式清單中，選取流量散佈設定檔，其在首選路徑的其中一個路徑健康情況公制超出在規則的路徑品質設定檔中設定的閾值時，確定防火牆如何為應用程式或服務選取替代路徑。

SD-WAN 目標頁籤

- **Policies**（政策）> **SD-WAN** > **Target**（目標）

選取 **Target**（目標）頁籤以選取推送 SD-WAN 政策規則的目標受管理裝置。此頁籤僅在 Panorama 管理伺服器上受支援。

欄位	說明
任何（以所有裝置為目標）	啟用（勾選）以將 SD-WAN 政策規則推送到 Panorama 管理伺服器管理的所有裝置。
裝置	選取一個或多個要向其中推送 SD-WAN 政策規則的裝置。您可以根據裝置狀態、平台、裝置群組、範本、標籤或 HA 狀態來篩選裝置。
標籤	指定原則的頁籤。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	原則頁籤即為允許您排序或篩選原則的關鍵字或字詞。如果已定義許多原則並想要檢視標記有特定關鍵字的項目時，此功能十分實用。例如，您可能想要使用特定文字（如「解密」與「無解密」）標記特定規則，或針對與該位置相關聯的原則使用特定資料中心名稱。 您也可以將頁籤新增至預設規則。
以除了指定的裝置和具有指定標籤的裝置以外的所有裝置為目標	啟用（勾選）以定位政策規則並推送至所有裝置，所選 **Devices**（裝置）或 **Tags**（標籤）除外。

© 2019 Palo Alto Networks, Inc.

物件

物件是可讓您建構、排程及搜尋政策規則的元件，安全性設定檔在安全性政策規則中提供威脅防範。

本節說明如何設定安全性設定檔及您可用於政策的物件：

> Move, Clone, Override, or Revert Objects（移動、複製、取代或還原物件）
> Objects > Addresses（物件 > 位址）
> Objects > Address Groups（物件 > 位址群組）
> Objects > Regions（物件 > 地區）
> Objects > Applications（物件 > 應用程式）
> Objects > Application Groups（物件 > 應用程式群組）
> Objects > Application Filters（物件 > 應用程式篩選器）
> Objects > Services（物件 > 服務）
> Objects > ServiceGroups（物件 > 服務群組）
> Objects > Tags（物件 > 標籤）
> Objects > Devices（物件 > 裝置）
> Objects > GlobalProtect > HIP Objects（物件 > GlobalProtect > HIP 物件）
> Objects>GlobalProtect> HIP Profiles（物件 > GlobalProtect > HIP 設定檔）
> Objects > External Dynamic Lists（物件 > 外部動態清單）
> Objects > Custom Objects（物件 > 自訂物件）
> Objects > Security Profiles（物件 > 安全性設定檔）
> Objects > Security Profiles > Mobile Network Protection（物件 > 安全性設定檔 > 行動網路保護）
> Objects > Security Profiles > SCTP Protection（物件 > 安全性設定檔 > SCTP 保護）
> Objects > Security Profile Groups（物件 > 安全性設定檔群組）
> Objects > Log Forwarding（物件 > 日誌轉送）
> Objects > Authentication（物件 > 驗證）
> Objects > Decryption Profile（物件 > 解密設定檔）
> Objects > SD-WAN Link Management（物件 > SD-WAN 連結管理）
> Objects > Schedules（物件 > 排程）

移動、複製、取代或還原物件

請參閱下列主題以了解修改現有物件的選項：

- 移動或複製物件
- 取代或還原物件

移動或複製物件

移動或複製物件時，您可以指派您擁有存取權限的 **Destination**（目的地）（防火牆上的虛擬系統或 Panorama™ 上的設備群組），包括 [共用] 位置。

若要移動物件，請在 **Objects**（物件）頁籤中選取物件，按一下 **Move**（移動），選取 **Move to other vsys**（移至其他虛擬系統）（僅限防火牆）或 **Move to other device group**（移至其他設備群組）（僅限 Panorama），完成下表中的欄位，接著按一下 **OK**（確定）。

若要複製物件，請選取 **Objects**（物件）頁籤中的物件，按一下 **Clone**（複製），晚成下表中的欄位，接著按一下 **OK**（確定）。

移動/複製設定	說明
選取的物件	顯示針對該操作所選政策或物件的名稱和目前位置（虛擬系統或設備群組）。
目的地	選取原則或物件的新位置：虛擬系統、裝置群組或 [共用]。預設值為您在 **Policies**（原則）或 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）或 **Device Group**（裝置群組）。
驗證中第一次偵測到錯誤時離開	選取此選項（預設為已選取）以確保防火牆或 Panorama 顯示找到的第一個錯誤，並停止尋找其他錯誤。例如，若目的地不包括您要移動之原則規則所參照的物件，則會發生錯誤。如果清除此選項，防火牆或 Panorama 將會找出所有錯誤，然而顯示這些錯誤。

取代或還原物件

在 Panorama 中，您可使用最多四個層級的樹狀階層建立設備群組。在底端層級，裝置群組可以具有上一層、上二層和上三層裝置群組（統稱為父系），底端階層會從上層繼承原則和物件。在頂端層級，裝置群組可以具有下一層、下二層和下三層裝置群組（統稱為子系）。您可覆寫下階項目中的物件，使它的值不同於其上階項目。預設會啟用此覆寫功能。不過，您無法覆寫共用或預設（預先設定）物件。Web 介面會顯示 圖示以指示物件包含繼承值，並顯示 圖示以指示繼承的物件包含覆寫值。

- 覆寫物件—請選取 **Objects**（物件）頁籤，選取將擁有覆寫版本的子系 **Device Group**（設備群組），選取物件，按一下 **Override**（覆寫）並編輯設定。您無法覆寫物件 **Name**（名稱）或 **Shared**（共用）設定。
- 將已覆寫物件還原為其繼承的值—請選取 **Objects**（物件）頁籤，選取包含覆寫版本的 **Device Group**（設備群組），選取物件，按一下 **Revert**（還原），再按一下 **Yes**（是）來確認操作。
- 停用覆寫物件—請選取 **Objects**（物件）頁籤，選取物件所在的 **Device Group**（設備群組），按一下物件名稱以編輯，選取 **Disable override**（停用覆寫），再按一下 **OK**（確認）。該物件的覆寫接著會在從所選 **Device Group**（設備群組）繼承物件的所有設備群組中停用。
- 在 **Panorama** 上使用從共用位置或父系設備群組繼承的值來替代所有物件覆寫—選取 **Panorama** > **Setup**（設定）> **Management**（管理），編輯 Panorama 設定，選取 **Ancestor Objects Take**

© 2019 Palo Alto Networks, Inc.

Precedence（父系項目物件較為優先），接著按一下 **OK**（確定）。接著您必須認可至 Panorama 及包含覆寫的設備群組才可推送繼承的值。

© 2019 Palo Alto Networks, Inc.

Objects > Addresses（物件 > 位址）

位址物件可以包括 IPv4 或 IPv6 位址（單一 IP 位址、一系列位址或子網路）、FQDN 或萬用字元位址（IPv4 位址後接斜線與萬用字元遮罩）。位址物件允許您在原則規則、篩選器以及其他防火牆功能中重複使用相同的位址或位址群組作為來源或目的地位址，而無需為每個實例手動新增每個位址。您可以使用 Web 介面或 CLI 建立位址物件；變更需要執行提交作業才能使物件成為組態的一部分。

首先 **Add**（新增）一個新位址物件，然後指定以下值：

位址物件設定	說明
名稱	輸入一個名稱（最多 63 個字元），然後說明您將要包含在該物作內作為一部分的位址。定義安全性原則規則時，此名稱會顯示在位址清單中。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
共享	如果您想要與下列項目共用此位址，則請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 **(vsys)**—如果您不選取此選項，則位址物件將僅供 **Objects**（物件）頁籤上選定的 **Virtual System**（虛擬系統）使用。 • **Panorama** 上的每個裝置群組—如果您不選取此選項，則位址物件將僅供 **Objects**（物件）頁籤上選定的 **Device Group**（裝置群組）使用。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此位址物件的裝置群組中取代此物件的設定。預設會停用此選取項目，這表示管理員可以取代繼承此物件之任何裝置群組的設定。
說明	輸入物件的描述（最多 1,023 個字元）。

類型	指定位址物件類型和項目：
	• **IP Netmask**（**IP** 網路遮罩）—使用以下表示法輸入 IPv4、IPv6 位址或 IP 位址範圍：*ip_address/mask* 或 *ip_address*，其中遮罩是用於位址網路部分的重要二進位數字。理論上，對於 IPv6 位址，您僅可指定網路部分，不可指定主機部分。例如：
	  • **192.168.80.150/32**—代表一個位址。
	  • **192.168.80.0/24**—代表從 192.168.80.0 到 192.168.80.255 的所有位址。
	  • **2001:db8::/32**
	  • **2001:db8:123:1::/64**
	• **IP Range**（**IP** 範圍）—使用下列格式輸入位址範圍：*ip_address–ip_address*，其中範圍前後端為 IPv4 位址或 IPv6 位址。例如：2001:db8:123:1::1-2001:db8:123:1::22
	• **IP Wildcard Mask**（**IP** 萬用字元遮罩）—使用 Ipv4 位址格式輸入 IP 萬用字元位址，後接斜線與遮罩（必須以零開頭）；例如，10.182.1.1/0.127.248.0。在萬用字元遮罩中，零 (0) 位元表示被比較的位元必須符合 0 涵蓋之 IP 位址中的位元。遮罩中的一 (1) 位元是萬用字元位元，這意味著被比較的位元不需要符合 1 所涵蓋之 IP 位址中的位元。將 IP 位址與萬用字元遮罩轉換為二進位。為了說明相符：在二進位程式碼片段 0011 上，1010 的萬用字元遮罩產生四個相符項（0001、0011、1001 與 1011）。

© 2019 Palo Alto Networks, Inc.

位址物件設定	說明
	您只能在安全性原則規則中使用 *IP* 萬用字元遮罩類型的位址物件。 • **FQDN**—輸入網域名稱。FQDN 最初會在提交時間解析。若 TTL 大於或等於 FQDN 重新整理時間下限，則隨後根據 FQDN 的 TTL 重新整理 FQDN 項目；否則，會在 FQDN 重新整理時間下限時重新整理 FQDN 項目。若設定了代理程式，則 FQDN 會由系統 DNS 伺服器或 DNS代理程式 物件解析。
解析	選取位址類型並輸入 IP 位址或 FQDN 後，按一下 **Resolve**（解析）以分別查看關聯的 FQDN 或 IP 位址（基於防火牆或 Panorama 的 DNS 組態）。 您可以將位址物件從 FQDN 變更為 IP 網路遮罩，反之亦然。若要從 FQDN 變更為 IP 網路遮罩，按一下 **Resolve**（解析）以查看 FQDN 解析到的 IP 位址，然後選取一個並 **Use this address**（使用此位址）。位址物件類型動態更改為 IP 網路遮罩，並且您選取的 IP 位址出現在文字欄位中。 或者，若要將位址物件從 IP 網路遮罩變更為 FQDN，按一下 **Resolve**（解析）以查看 IP 網路遮罩解析到的 DNS 名稱，然後選取 FQDN 並 **Use this FQDN**（使用此 **FQDN**）。類型改變為 FQDN 和 FQDN 顯示於文字欄位中。
標籤	選取或輸入要套用至此位址物件的頁籤。您可以在這裡定義頁籤，或使用 Objects > Tags（物件 > 頁籤）頁籤建立新頁籤。

© 2019 Palo Alto Networks, Inc.

Objects > Address Groups（物件 > 位址群組）

若要簡化安全性政策的建立，可以將需要相同安全性設定的位址合併至位址群組中。位址群組可為靜態或動態。

- 動態位址群組：動態位址群組會藉由查詢標籤並使用標籤式篩選，動態地填入其成員。如果您有經常會變更虛擬機器位置/IP 位址的廣泛虛擬基礎結構，則動態位址群組極為有用。例如，您具有多樣化的容錯轉移設定，或經常佈建新的虛擬機器，並想要將政策套用至與新機器之間的往來流量，而不想在防火牆上修改設定/規則。

  若要在政策中使用動態位址群組，您必須完成下列工作：

  - 定義動態位址群組，並在政策規則中參照它。
  - 將 IP 位址和對應標籤通知防火牆，以便組成動態位址群組的成員。您可以使用外部指令碼（使用防火牆上的 XML API）完成上述工作；若是 VMware 式環境，則選取 **Device**（設備）> **VM Information Sources**（**VM** 資訊來源）以設定好防火牆上的設定。

  動態位址群組也可以包含靜態定義的位址物件。如果建立位址物件並為其套用已指定給動態位址群組的相同標籤，則該動態位址群組將包含符合標籤的所有靜態和動態物件。因此，您可以使用標籤，將動態和靜態物件整合至相同的位址群組。
- 靜態位址群組：靜態位址群組可包含靜態位址物件、動態位址群組，或者是兩個位址物件和動態位址群組的組合。

  若要建立位址群組，請按一下 **Add**（新增）並填寫下列欄位：

位址群組設定	說明
名稱	輸入說明位址群組的名稱（最多 **63** 個字元）。定義安全性原則時，此名稱會顯示在位址清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
共享	若您想讓以下對象使用位址群組，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用位址群組。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用位址群組。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此位址群組物件的設備群組中覆寫該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
說明	輸入物件的說明（最多 1023 個字元）。
類型	選取 **Static**（靜態）或 **Dynamic**（動態）。 若要建立動態位址群組，請使用比對準則來組合群組中包含的成員。使用 **AND** 或 **OR** 運算子來定義 **Match**（比對）準則。 若要檢視比對準則的屬性清單，必須已設定防火牆來存取和擷取來源/主機的屬性。在已設定的資訊來源上，所有虛擬電腦均會向防火牆註冊，且防火牆亦可提取這些電腦，進而擷取 *IP* 位址或設定的變更，而不需要在防火牆上進行任何修改。

© 2019 Palo Alto Networks, Inc.

位址群組設定	說明
	若為靜態位址群組，請按一下 **Add**（新增）並選取一或多個 **Addresses**（位址）。按一下 **Add**（新增），將物件或位址群組新增至位址群組。群組可包含位址物件，及靜態和動態位址群組二者。
標籤	選取或輸入要套用至此位址群組的標籤。如需標籤的相關資訊，請參閱 [物件 > 標籤]。

成員計數和位址	新增位址群組之後，**Objects**（物件）> **Address Groups**（位址群組）頁面上的 [成員計數] 欄會指出物件是以動態或靜態方式填入群組中。
	• 對於靜態位址群組，您可以檢視位址群組中的成員計數。
	• 對於使用標籤來動態填入成員或同時具有靜態和動態成員的位址群組，若要檢視成員，請按一下位址欄中的 **More...**（更多...）連結。您現在可以檢視已註冊至位址群組的 IP 位址。
	  • 類型通常會指出 IP 位址是靜態位址物件或正在動態註冊並顯示 IP 位址。
	  • 動作可讓您從 IP 位址 **Unregister**（取消註冊）**Tags**（標籤）。按一下連結以 **Add**（新增）註冊來源並指定要取消註冊的標籤。

© 2019 Palo Alto Networks, Inc.

Objects > Regions（物件 > 地區）

防火牆支援建立套用至指定國家/地區或其他地區的原則規則。針對安全性原則、解密原則以及 DoS 原則指定來源與目的地時，區域可做為選項使用。您可以從國家/地區的標準清單中選取，或使用本節所述的地區設定，來定義要做為安全性原則規則選項包含的自訂地區。

下表說明區域設定：

地區設定	說明
名稱	選取說明地區的名稱。定義安全性原則時，此名稱會顯示在位址清單中。
地理位置	若要指定緯度與經度，請選此選項並指定值（xxx.xxxxxx 格式）。在應用程式層面的流量與威脅地圖中會使用此資訊。請參考 [監控 > 日誌]。
位址	使用下列任意格式，指定用於識別區域的 IP 位址、IP 位址範圍或子網路： x.x.x.x x.x.x.x-y.y.y.y x.x.x.x/n

© 2019 Palo Alto Networks, Inc.

Objects > Dynamic User Groups（物件 > 動態使用者群組）

若要建立動態使用者群組，請選取 **Objects**（物件）> **Dynamic User Groups**（動態使用者群組），**Add**（新增）新的動態使用者群組，然後設定以下設定：

動態使用者群組設定	說明
名稱	輸入說明動態使用者群組的 **Name**（名稱）（最多 63 個字元）。定義安全性政策規則時，此名稱會顯示在來源使用本清單中。名稱必須是唯一的，且只能使用硬數字元、空格、連字號與底線。
說明	輸入物件的 **Description**（說明）（最多 1023 個字元）。
共用 （僅限 Panorama）	如果您希望動態裝置群組的比對規則可用於 Panorama 上的每個裝置群組，請選取此選項。 *Panorama* 不會與裝置群組共用群組成員。 若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用動態使用者群組的比對規則。
停用覆寫 （僅限 Panorama）	選取此選項，可防止管理員在繼承此物件的裝置群組中覆寫此動態使用者群組的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
比對	**Add Match Criteria**（新增比對規則）以使用 **AND**（與）或 **OR**（或）運算子來包括多個標籤以定義動態使用者群組中的成員。 *Add Match Criteria*（新增比對規則）時，僅顯示現有規則。您可以選取現有標籤，也可以建立新標籤。
標籤	（選用）選取或輸入要套用至動態使用者群組物件的靜態物件標籤。這會標記動態使用者群組物件本身，不會標記群組中的成員。您選取的標籤可讓您將相關項目分組，與比對規則不想關。如需標籤的相關資訊，請參閱 [物件 > 標籤]。

新增動態使用者群組之後，可以檢視該群組的以下資訊：

動態使用者群組欄	說明
位置 （僅限 Panorama）	識別動態使用者群組的比對規則是可用於 Panorama 上的每個裝置群組（**Shared**（共用））還是可用於選定的裝置群組。
使用者	選取 **more**（更多）可查看動態使用者群組中的使用者清單。 • 若要將標籤新增至使用者以包括在群組中，**Register Users**（註冊使用者），然後選取要套用至使用者的 **Registration**

© 2019 Palo Alto Networks, Inc.

動態使用者群組欄	說明
	Source（註冊來源）和 Tags（標籤）。使用者的標籤與群組的準則相符後，防火牆會將使用者新增至動態使用者群組。 • （選用）指定 Timeout（逾時）（以分鐘為單位）（預設值為 0；範圍是 0-43,200）以在指定的時間到期後從群組中去除使用者。 • （選用）Add（新增） Users（使用者）至群組或者從群組中 Delete（刪除）使用者。 • 若要從使用者中去除標籤並防止使用者成為群組的成員，請選取使用者，Unregister Users（取消註冊使用者），然後選取 Registration Source（註冊來源）和 Tags（標籤）。 • 完成檢閱或修改動態使用者群組使用者清單之後，按一下 Close（關閉）。

© 2019 Palo Alto Networks, Inc.

Objects > Applications（物件 > 應用程式）

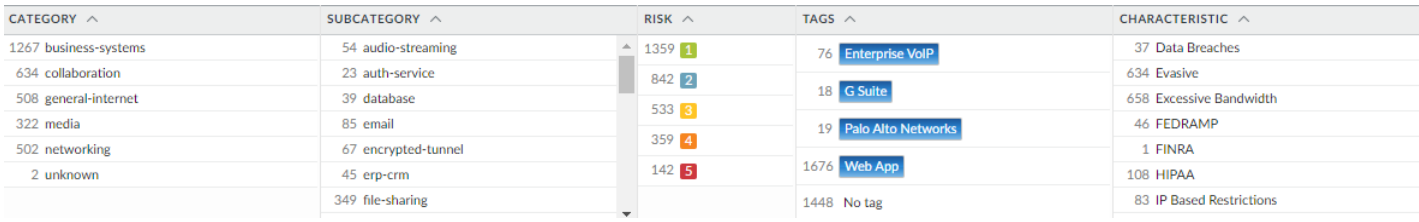
下列主題說明 **Applications**（應用程式）頁面。

您想了解什麼內容？	請參閱
了解應用程式頁面顯示的應用程式設定及屬性。	應用程式概要 應用程式上支援的動作
新增應用程式或修改現有的應用程式。	定義應用程式

應用程式概要

應用程式頁面會列出每個應用程式定義的各種屬性，例如應用程式的相對安全性風險（1 到 5）。風險值以各項條件為基礎，例如應用程式可以共享檔案、易於誤用或嘗試躲避防火牆。值越高表示風險越高。

頁面頂部的應用程式瀏覽器區域如下列出了您可以用來篩選顯示的屬性。每個項目左側的數字表示具有該屬性之應用程式的總數。



每週內容更新會定期包括可讓您針對它們開發特徵碼的新解碼器及內容。

下表說明應用程式詳細資料—自訂應用程式和 Palo Alto® Networks 應用程式可能會顯示以下的部分或所有欄位。

應用程式詳細資料	說明
名稱	應用程式的名稱。
說明	應用程式的描述（最多 255 個字元）。
其他資訊	Web 來源（Wikipedia、Google 與 Yahoo!）連結，包含有關應用程式的其他資訊。
標準連接埠	應用程式用來與網路通訊的連接埠。
取決於	執行此應用程式所需的其他應用程式清單。當建立原則規則以允許所選的應用程式時，您也必須確定允許任何該應用程式所依賴的其他應用程式。
隱含使用	選取的應用程式所依賴，但由於隱含受到支援，而不需要新增至安全性原則規則以允許所選應用程式的其他應用程式。

© 2019 Palo Alto Networks, Inc.

應用程式詳細資料	說明
先前識別為	針對新的 App-ID™ 或已變更的 App-ID，此欄位會指出應用程式先前識別為何。這可協助您根據應用程式的變更評估是否需要原則變更。若停用 App-ID，與該應用程式相關聯的工作階段將作為先前識別的應用程式比對。同樣地，停用的 App-ID 將以它們先前識別為的應用程式顯示在日誌中。
拒絕動作	App-ID 的開發提供預設拒絕動作，會指定防火牆在安全性規則中包括應用程式時，要如何以拒絕動作回應。預設拒絕動作可指定無訊息丟棄或 TCP 重設。您可在安全性原則中覆寫此預設動作。
特性	
具有規避性	針對原始以外的目的使用連接埠或通訊協定，希望能夠周遊防火牆。
耗用頻寬	正常使用情況下，定期消耗至少 1 Mbps。
易遭濫用或誤用	經常用於惡意目的，或可輕鬆設定以暴露使用者不想暴露的內容。
SaaS	在防火牆上，軟體即服務 (SaaS) 分類為服務，其中軟體和基礎結構由應用程式服務供應商提供及管理，但您仍可全權控制資料，包括可建立、存取、共用和傳輸資料的人員。 請記住，在應用程式的分類情況下，SaaS 應用程式會與 Web 服務不同。Web 服務為託管應用程式，其中使用者不擁有資料（例如 Pandora）或服務主要由許多訂閱者基於社交目的而提供的共用資料所構成（例如 LinkedIn、Twitter 或 Facebook）。
能夠進行檔案傳輸	能夠透過網路將檔案從一個系統傳輸至另一系統。
傳遞其他應用程式	能夠傳送其通訊協定內部的其他應用程式。
由惡意軟體使用	我們都知道，惡意軟體會使用應用程式來進行傳播、攻擊或資料竊取，或是隨惡意軟體散佈。
有已知漏洞	具有公開報告的弱點。
全面	可能擁有 1,000,000 位以上的使用者。
繼續掃描其他應用程式	指示防火牆繼續嘗試比對其他應用程式特徵碼。若您不選取此選項，防火牆將在第一個相符特徵碼之後停止尋找其他應用程式相符項目。
SaaS 特性	
數據洩露	在過去三年內可能發布安全資料給不信任來源的應用程式。
服務條款欠佳	具有可能危害企業資料不利服務條款的應用程序。
無憑證	缺少目前符合產業方案或憑證規定的應用程式， 如SOC1、SOC2、SSAE16、PCI、HIPAA、FINRAA 或 FEDRAMP。
財務可行性欠佳	在接下來 18 到 24 個月中，有可能停業的應用程式。

© 2019 Palo Alto Networks, Inc.

應用程式詳細資料	說明
無 IP 限制	對使用者存取沒有主要依 IP 限制的應用程式。
分類	
類別	應用程式類別將為下列其中之一： • 業務系統 • 協同作業 • 一般網際網路 • 媒體 • 網路 • 未知
子類別	分類應用程式的子類別。不同的類別具備不同的相關聯子類別。例如，協同作業類別中的子類別包含電子郵件、檔案共用、立即訊息、網際網路會議、社群業務、社交網站、VoIP 視訊和網頁公佈。而商務系統類別中的子類別包括驗證服務、資料庫、erp-crm、一般業務、管理、辦公室程式、軟體更新和儲存備份。
技術	應用程式技術將為下列其中之一： • 用戶端伺服器：這是一個使用主從架構模型的應用程式，在這種情況下，網路中的一或多個用戶端與一部伺服器進行通訊。 • 網路通訊協定：這是一個應用程式，通常用於系統與系統間的通訊，以利於網路操作。它包含大多數 IP 通訊協定。 • 端點至端點：這是一個直接與其他用戶端通訊以傳輸資訊的應用程式，不會依賴中央伺服器進行通訊。 • 基於瀏覽器：這是一個依賴於 Web 瀏覽器進行運作的應用程式。
風險	已指定的應用程式風險。 若要自訂此設定，請按一下 自訂連結，輸入值 (1-5)，然後按一下 確定。
標籤	已分配給應用程式的標籤。 **Edit Tags**（編輯標籤）以新增或移除應用程式的標籤。
選項	
工作階段逾時	應用程式由於沒有任何活動而逾時的所需時間（以秒為單位，範圍為 1-604800 秒）。這個逾時是針對 TCP 或 UDP 以外的通訊協定。對於 TCP 和 UDP，請參閱此表格後續幾列。 若要自訂此設定，請按一下自訂連結，輸入值，然後按一下確定。
TCP 逾時 (秒)	終止 TCP 應用程式流量的逾時（以秒為單位，範圍為 1-604800）。 若要自訂此設定，請按一下自訂連結，輸入值，然後按一下確定。 值 0表示將使用全域工作階段計時器，對 TCP 而言為 3600 秒。
UDP 逾時（秒）：	終止 UDP 應用程式流量的逾時（以秒為單位，範圍是 1-604800 秒）。 若要自訂此設定，請按一下自訂連結，輸入值，然後按一下確定。

© 2019 Palo Alto Networks, Inc.

應用程式詳細資料	說明
TCP 半關閉狀態 (秒)	在接收第一個 FIN 封包和接收第二個 FIN 封包或 RST 封包之間，工作階段在工作階段表格中停留的時間長度上限（以秒為單位）。如果計時器到期，就會關閉工作階段（範圍為 1-604800 秒）。 預設值：若未在應用程式層級上設定此計時器，則會使用全域設定。 若在應用程式層級上設定此值，則會取代全域 **TCP Half Closed**（**TCP** 半關閉狀態）設定。
TCP 時間等待 (秒)	在接收第二個 FIN 封包或 RST 封包之後，工作階段在工作階段表格中停留的時間長度上限（以秒為單位）。如果計時器到期，就會關閉工作階段（範圍為 1-600 秒）。 預設值：若未在應用程式層級上設定此計時器，則會使用全域設定。 若在應用程式層級上設定此值，則會取代全域 **TCP** 時間等待 設定。
啟用 App-ID	指出 App-ID 為啟用或停用。若停用 App-ID ，該應用程式的流量在安全性原則和日誌中將視為 **Previously Identified As**（先前識別為）App-ID。針對內容發行版本 490 之後新增的應用程式，您可以在檢閱原則對新應用程式的影響時停用它們。在檢閱原則之後，您可選取 **Enable**（啟用）App-ID。您也可以 **Disable**（停用）先前已啟用的應用程式。在多系統防火牆上，您可以在各個虛擬系統中分別停用 App-ID。

當防火牆無法使用 App-ID 識別應用程式時，會將流量分類為未知：unknown-tcp 或 unknown-udp。除了完全模擬 HTTP 的應用程式以外，此行為適用於所有未知的應用程式。如需詳細資訊，請參閱Monitor > Botnet（監視 > Botnet）。

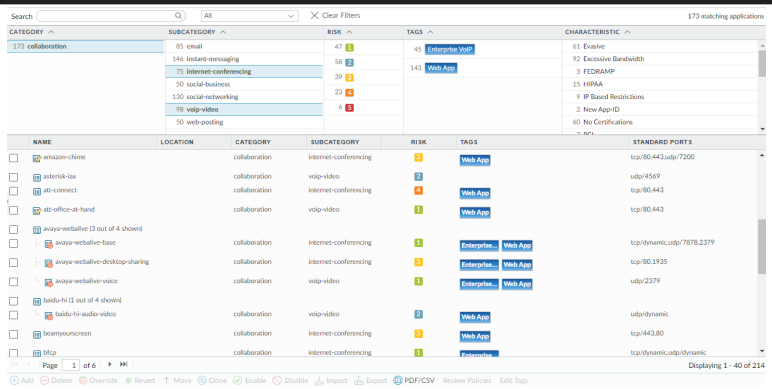
您可以為未知應用程式建立新定義，然後定義新應用程式定義的安全性原則。此外，可以將需要相同安全性設定的應用程式合併至應用程式群組，以簡化安全性原則的建立。

應用程式上支援的動作

您可以在此頁面上執行以下任何一個動作：

應用程式支援的動作	說明
依應用程式篩選	• 若要搜尋特定應用程式，請在 **Search**（搜尋）欄位中輸入應用程式名稱或說明，然後按 **Enter** 鍵。使用下拉式清單可讓您搜尋或篩選特定應用程式或檢視 **All**（全部）應用程式、**Custom applications**（自訂應用程式）、**Disabled applications**（停用的應用程式）或 **Tagged applications**（標記的應用程式）。 會列出應用程式，並會更新篩選欄以顯示符合搜尋之應用程式的統計資料。搜尋將符合部分字串。當您定義安全性原則時，您可以編寫適用於符合已儲存篩選之所有應用程式的規則。當透過符合篩選的內容更新新增應用程式時，會動態更新此類規則。 • 若要依頁面上顯示的應用程式屬性篩選，請按一下做為篩選基礎使用的項目。例如，若要將清單限制於協同合作類別，請按一下 **collaboration**（協同作業），清單將只顯示此類別中的應用程式。

© 2019 Palo Alto Networks, Inc.

應用程式支援的動作	說明
	 • 若要在其他欄上篩選，請按一下其他欄中的項目。篩選是一個連續過程：首先套用類別篩選，然後依次是子類別篩選、技術篩選、風險篩選，最後是特性篩選。例如，若您套用類別、子類別和風險篩選器，即使尚未明確套用技術篩選，技術欄也會自動限於與所選類別及子類別一致的技術。每次您套用一個篩選器，應用程式清單就會自動更新。若要建立新的應用程式篩選器，請參閱 Objects > Application Filters（物件 > 應用程式篩選器）。
新增應用程式。	若要新增應用程式，請參閱定義應用程式。
檢視及 / 或自訂應用程式詳細資訊。	按一下應用程式名稱連結，檢視應用程式說明，包括標準連接埠、應用程式的特性及其他詳細資訊中的風險。如需應用程式設定的詳細資訊，請參閱定義應用程式。 如果應用程式名稱左側的圖示上有黃色的鉛筆（ ），則表示該應用程式為自訂應用程式。
停用應用程式	您可以 **Disable**（停用）應用程式（或多個應用程式），讓應用程式簽名不會對流量進行比對。當應用程式停用時，定義為封鎖、允許或強制使用符合應用程式的安全性規則不會套用至應用程式流量。您可選取停用新內容發行版本包含的應用程式，因為針對應用程式強制執行原則可能會在應用程式時唯一識別時變更。例如，防火牆在新的內容版本安裝之前會允許識別為網頁瀏覽流量的應用程式；而在安裝內容更新之後，唯一識別的應用程式即不再符合允許網頁瀏覽流量的安全性規則。在此情況下，您可以選取停用應用程式，讓符合應用程式特徵碼的流量繼續分類為網路瀏覽流量並受允許。
啟用應用程式	選取停用的應用程式，並 **Enable**（啟用）它，使防火牆能夠根據您設定的安全性原則管理該應用程式。
匯入應用程式	若要匯入應用程式，請按一下 **Import**（匯入）。瀏覽以選取檔案，然後從 **Destination**（目的地）下拉式清單中選取目標虛擬系統。
匯出應用程式	若要匯出應用程式，請選取應用程式的此選項，然後按一下 **Export**（匯出）。依照提示儲存檔案。
匯出應用程式設定表	匯出 **PDF/CSV** 格式的所有應用程式相關資料。僅可匯出網路介面中可見的欄位。請參閱匯出設定表資料。

© 2019 Palo Alto Networks, Inc.

應用程式支援的動作	說明
安裝新內容發行版本後評估政策影響	**Review Policies**（檢閱原則），以在安裝內容發行版本前後評估應用程式的原則強制執行情形。使用 [原則檢閱] 對話方塊檢閱原則對下載內容發行版本中的新應用程式的影響。[原則檢閱] 對話方塊可讓您從現有安全性原則規則中新增或移除擱置中的應用程式（透過內容發行版本下載，但尚未安裝於防火牆的應用程式）；擱置中應用程式的原則變更必須在安裝對應的內容發行版本後才會生效。您也可在下載及安裝內容發行版本時，在 **Device**（裝置）> **Dynamic Updates**（動態更新）頁面上存取 [原則檢閱] 對話方塊。
標記應用程式	您可以選取預先定義的 **sanctioned**（認可）頁籤來標記 SaaS 應用程式。雖然 SaaS 應用程式在應用程式特性詳細資訊中被識別為 **Saas=yes**，您仍可在任何應用程式上使用認可頁籤。 將應用程式頁籤為 *sanctioned*（認可）來幫助將未認可的 *SaaS* 應用程式流量與認可的 *SaaS* 應用程式區分開來。例如，當您在檢查 *SaaS* 應用程式使用情況報告或當您在評估您網絡上的應用程式時。 選取應用程式，按一下 **Edit Tags**（編輯標記），然後從下拉式清單中，選取預先定義的 **Sanctioned**（認可）標籤來識別您要在網路上明確允許的任何應用程式。當您接著產生 SaaS 應用程式使用情況報告（請參閱 [監控 > PDF 報告 > SaaS 應用程式使用情況]）時，您可以對您已認可的應用程式與網路上使用的不被認可的 SaaS 應用程式進行統計資料的比較。 當應用程式被標記為認可時，下列限制適用： • 認可頁籤無法套用於應用程式群組。 • 認可頁籤無法套用於 **Shared**（共用）層級；您僅可按裝置群組或按虛擬系統標記應用程式。 • 認可頁籤無法用於標記容器應用程式中包含的應用程式，例如 Facebook 電子郵件，該應用程式是 Facebook 容器應用程式的一部分。 您亦可 **Remove tag**（移除頁籤）或 **Override tag**（覆寫頁籤）。只有從 Panorama 推送的裝置群組中繼承設定的防火牆才可使用取代選項。

定義應用程式

選取 **Objects**（物件）> **Applications**（應用程式），可為防火牆 **Add**（新增）自訂應用程式，以在套用原則時評估。

新應用程式設定	說明
組態頁籤	
名稱	輸入應用程式名稱（最多 31 個字元）。定義安全原則時，此名稱會顯示在應用程式清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、句點、連字號與底線。第一個字元必須是字母。
共享	若您想讓以下對象使用應用程式，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用應用程式。

© 2019 Palo Alto Networks, Inc.

新應用程式設定	說明
	• Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用應用程式。
停用覆寫（僅限 Panorama）	若要防止管理員在繼承物件的裝置群組中取代此應用程式物件的設定，請選取此選項。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
說明	輸入應用程式的描述做為一般參考（最多 255 個字元）。
類別	選取應用程式類別，例如 **email**（電子郵件）或 **database**（資料庫）。此類別可用來產生前十大應用程式類別圖表，並且可用於篩選（請參考 ACC）。
子類別	選取應用程式子類別，例如 **email**（電子郵件）或 **database**（資料庫）。此子類別可用來產生前十大應用程式類別圖表，並且可用於篩選（請參考 ACC）。
技術	選取應用程式的技術。
父應用程式	為此應用程式指定父應用程式。當工作階段符合父應用程式與自訂應用程式時，適用此設定；但是，會報告自訂應用程式，因為它是更特定的應用程式。
風險	選取與此應用程式關聯的風險層級（1 = 最低至 5 = 最高）。
特性	選取可使應用程式處於風險中的應用程式特性。如需各個特性的說明，請參考特性。
進階頁籤	
連接埠	如果應用程式使用的通訊協定是 TCP 和/或 UDP，請選取 **Port**（連接埠），然後輸入通訊協定與埠號的一或多個組合（一行一個項目）。通用格式為： *<protocol>/<port>* 其中< 連接埠 >是單一連接埠號碼，動態連接埠指派則為 **Dynamic**（動態）。 例如：TCP/動態或 UDP/32。 當使用安全性規則服務欄中的 **app-default**（應用程式預設）時，適用此設定。
IP 通訊協定	若要指定 TCP 或 UDP 以外的 IP 通訊協定，請選取 **IP** 通訊協定，然後輸入通訊協定號碼（1 至 255）。
ICMP 類型	若要指定網際網路控制訊息通訊協定第 4 版 (ICMP) 類型，請選取 **ICMP Type**（**ICMP** 類型），然後輸入類型編號（範圍是 0-255）。
ICMP6 類型	若要指定網際網路控制訊息通訊協定第 6 版 (ICMPv6) 類型，請選取 **ICMP6 Type**（ICMP6 類型），然後輸入類型編號（範圍是 0-255）。
無	若要指定獨立於通訊協定的簽章，請選取無。
逾時	輸入終止閒置應用程式流量之前的秒數（範圍是 0-604800 秒）。零指示使用應用程式的預設逾時。在所有情況下，此值用於 TCP 與 UDP 以外的通訊協定，還用於未指定 TCP 逾時與 UDP 逾時情況下的 TCP 與 UDP 逾時。

© 2019 Palo Alto Networks, Inc.

新應用程式設定	說明
TCP 逾時	輸入終止閒置 TCP 應用程式流量之前的秒數（範圍是 0-604800 秒）。零指示使用應用程式的預設逾時。
UDP 逾時	輸入終止閒置 UDP 應用程式流量之前的秒數（範圍是 0-604800 秒）。零指示使用應用程式的預設逾時。
TCP 半關閉狀態	輸入在接收第一個 FIN 和接收第二個 FIN 或 RST 之間，工作階段在工作階段表格中停留的時間長度上限。如果計時器到期，就會關閉工作階段。 預設值：若未在應用程式層級上設定此計時器，則會使用全域設定。（範圍是 1-604800 秒）。 若在應用程式層級上設定此值，則會覆寫全域 TCP Half Closed（TCP 半關閉狀態）設定。
TCP 時間等待	輸入在接收第二個 FIN 或 RST 之後，工作階段在工作階段表格中停留的時間長度上限。如果計時器到期，就會關閉工作階段。 預設值：若未在應用程式層級上設定此計時器，則會使用全域設定。（範圍是 1-600 秒）。 若在應用程式層級上設定此值，則會覆寫全域 TCP Time Wait（TCP 時間等待）設定。
掃描	根據安全性設定檔（檔案類型、資料模式與病毒），選取您要允許的掃描類型。
特徵碼頁籤	
特徵碼	按一下 **Add**（新增）以新增特徵碼，及指定下列資訊： • 特徵碼名稱—輸入用來識別特徵碼的名稱。 • 註解 — 輸入選取性說明。 • 符合訂購條件 — 選取定義特徵碼條件的順序是否重要。 • 範圍 — 選取僅將此特徵碼套用至目前 **Transaction**（程序）或套用至完整使用者 **Session**（工作階段）。 指定識別特徵碼的條件。這些條件用於產生防火牆用來比對應用程式模式及控制流量的特徵碼： • 若要新增條件，請選取 **Add AND Condition**（新增 **AND** 條件）或 **Add OR Condition**（新增 **OR** 條件）。若要在群組中新增條件，請選取群組，然後按一下新增條件。 • 從下拉式清單中選取 **Operator**（運算子）。選項包括 **Pattern Match**（模式比對）、**Greater Than**（大於）、**Less Than**（小於）及 **Equal To**（等於），並指定下列選項： （僅適用於 [模式比對]） • 內容 — 從可用內容中選取。這些內容可使用動態內容更新來進行更新。 • 模式 — 指定規則運算式來指定套用於自訂應用程式的唯一字串內容值。 執行封包擷取以識別內容。如需規則運算式的模式規則，請參閱模式規則語法。 （適用於 [大於]、[小於]）

© 2019 Palo Alto Networks, Inc.

新應用程式設定	說明
	• 內容 — 從可用內容中選取。這些內容可使用動態內容更新來進行更新 • 值 — 指定比對值（範圍是 0-4294967295）。 • 限定詞與值 —（選用）新增限定詞/值配對。 （僅適用於 [等於]） • 內容—從未知要求及 TCP 或 UDP（例如 unknown-req-tcp）的回應中選取內容，或透過動態內容更新（例如 dnp3-req-func-code）提供的其他內容。 對於未知要求及 TCP 或 UDP 的回應，請指定 • 位置 — 在封包所承載資料中的前四位或第二個四位位元組之間選取。 • 遮罩 — 指定 4 位元組十六進位值，例如 0xffffff00。 • 值 — 指定 4 位元組十六進位值，例如 0xaabbccdd。 對於所有其他內容，請指定與應用程式相關的 **Value**（值）。 若要在群組中移動條件，請選取條件並 **Move Up**（上移）或 **Move Down**（下移）。若要移動群組，請選取群組並 **Move Up**（上移）或 **Move Down**（下移）。您無法將條件從一個群組移至另一個群組。

如果應用程式僅用於應用程式取代規則，則不需要指定應用程式的特徵碼。

© 2019 Palo Alto Networks, Inc.

Objects > Application Groups（物件 > 應用程式群組）

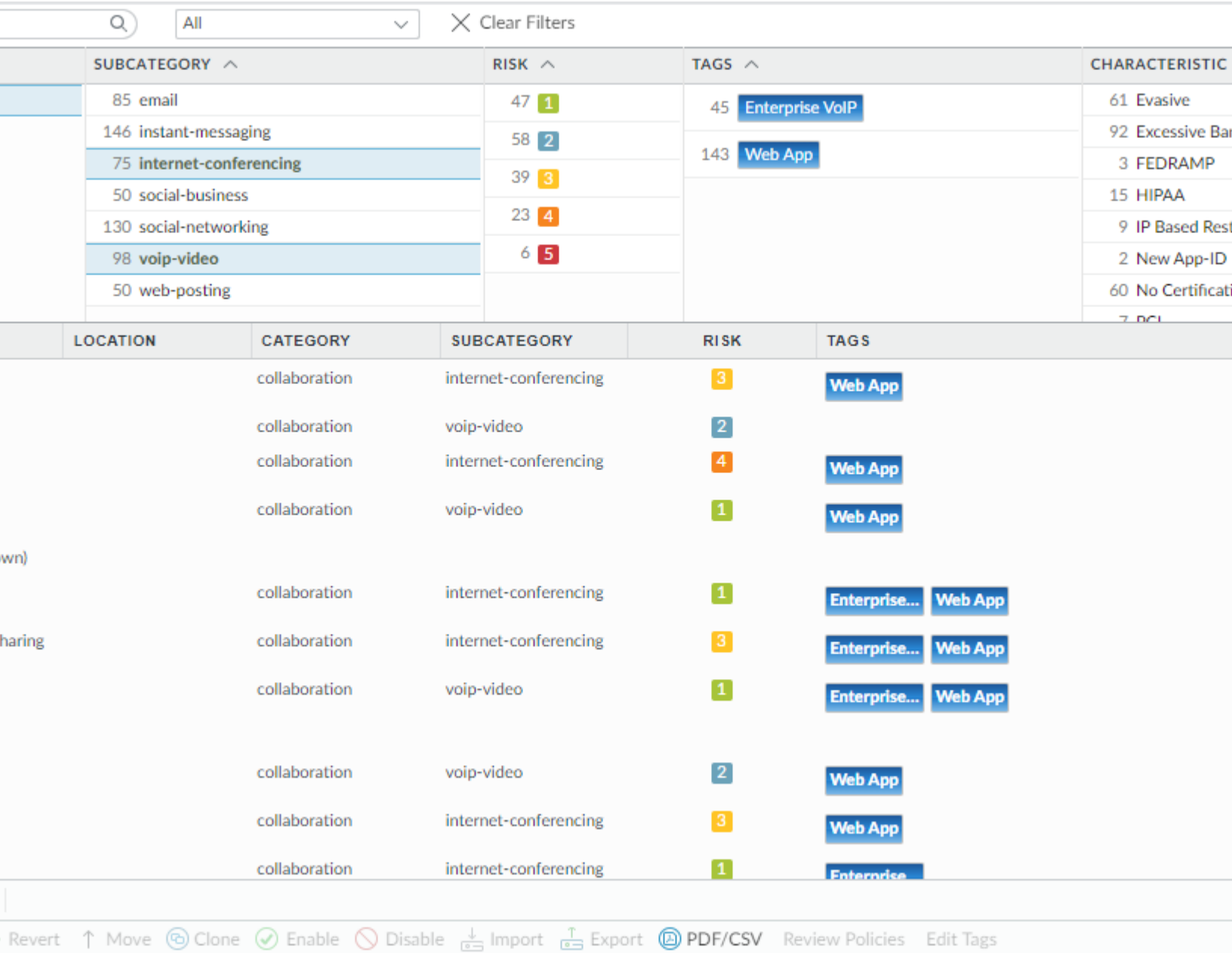
若要簡化安全性政策的建立，可以建立應用程式群組來合併需要相同安全性設定的應用程式。（若要定義新應用程式，請參考定義應用程式。）

新應用程式群組設定	說明
名稱	輸入說明應用程式群組的名稱（最多 31 個字元）。定義安全性政策時，此名稱會顯示在應用程式清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
共享	若您想讓以下對象使用應用程式群組，請選取此選項： 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用應用程式群組。 Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用應用程式群組。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此應用程式群組物件的設備群組中覆寫該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
應用程式	按一下新增，選取要包含在此群組中的應用程式、應用程式過濾與/或其他應用程式群組。

© 2019 Palo Alto Networks, Inc.

Objects > Application Filters（物件 > 應用程式篩選器）

應用程式篩選器有助於簡化重複的搜尋。若要定義應用程式篩選器，請 **Add**（新增）並輸入新篩選器的名稱。在視窗的上方區域中，按一下您要作為篩選基礎使用的項目。例如，若要將清單限制於網路類別，請按一下 **Collaboration**（協同作業）。



若要在其他欄上篩選，請按一下該欄中的項目。篩選是連續的；首先套用類別篩選器，然後依次是子類別篩選器、技術篩選器、風險篩選器、標籤，最後是特性篩選器。

您選取篩選器時，頁面上的應用程式清單將自動更新。

© 2019 Palo Alto Networks, Inc.

Objects > Services（物件 > 服務）

當您為特定應用程式定義安全性政策時，您可以選取一或多個服務來限制應用程式可以使用的埠號。預設服務為 **any**（任何），它允許所有 TCP 與 UDP 連接埠。會預先定義 HTTP 與 HTTPS 服務，但是您可以新增其他服務定義。可以將經常一起指定的服務合併至服務群組，以簡化安全性政策的建立（請參考 [物件 > 服務群組]）。

另外，您可以使用服務物件指定以服務為基礎的工作階段逾時—這表示您可以套用不同的逾時到不同的使用者群組中，就算那些群組使用相同 TCP 或 UDP 服務也一樣，或者，如果您正從自訂應用程式中，以連接埠為基礎的安全性政策遷移至以應用程式為基礎的安全性政策，則您可以輕鬆維持自訂應用程式逾時。

下表說明服務設定：

服務設定	說明
名稱	輸入服務名稱（最多 **63** 個字元）。定義安全性政策時，此名稱會顯示在服務清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入服務的說明（最多 1023 個字元）。
共用	若您想讓以下對象使用服務物件，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用服務物件。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用服務物件。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此服務物件的設備群組中覆寫該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
通訊協定	選取服務使用的通訊協定（**TCP** 或 **UDP**）。
目的地連接埠	輸入服務使用的目的地埠號（0 至 65535）或埠號範圍（連接埠 1 - 連接埠 2）。多個連接埠或範圍必須以逗號隔開。目的地連接埠為必填。
來源連接埠	輸入服務使用的來源埠號（0 至 65535）或埠號範圍（連接埠 1 - 連接埠 2）。多個連接埠或範圍必須以逗號隔開。來源連接埠為選用。
工作階段逾時	為本服務定義工作階段逾時： • 從應用程式繼承（預設）—沒有套用任何服務為基礎的逾時；套用此應用程式逾時。 • 取代—為此服務定義自訂工作階段逾時。繼續填入 TCP 逾時、TCP 半關閉和 TCP 等待時間欄位。
以下設定僅在您選擇覆寫應用程式逾時並為一個服務建立自訂工作階段逾時時才會顯示。	
TCP 逾時	以秒為單位設定 TCP 工作階段在資料傳輸已開始後可維持開啟的時間上限。當超出這個時間時，工作階段關閉。

© 2019 Palo Alto Networks, Inc.

服務設定	說明
	範圍為 1 到 604800。預設值為 3600 秒。
TCP 半關閉狀態	以秒為單位設定在連線僅一方試著關閉連線時，工作階段維持開啟的時間上限。 本設定適用： • 在防火牆接收第一個 FIN 封包後的時長（表示連線的一方正嘗試關閉工作階段），但在接收第二個封包之前（表示連線另一方正在關閉工作階段）。 • 在接到 RST 封包前的時長（表示嘗試重新設定連線）。 如果計時器到期，就會關閉工作階段。 範圍為 1 到 604800。預設值為 120 秒。
TCP 等候時間	以秒為單位設定工作階段在接收二個 FIN 封包的第二個要終止工作階段的封包後，或在接收 RST 封包以重新設定連線後，仍維持開啟的時間上限。 當計時器到期，就會關閉工作階段。 範圍為 1-600。預設值為 15 秒。

© 2019 Palo Alto Networks, Inc.

物件 > 服務群組

若要簡化安全性政策的建立，您可以將安全性設定相同的服務合併至服務群組。若要定義新服務，請參考 [物件 > 服務]。

下表說明服務群組設定：

服務群組設定	說明
名稱	輸入服務群組名稱（最多 63 個字元）。定義安全性政策時，此名稱會顯示在服務清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
共用	若您想讓以下對象使用服務群組，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用服務群組。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用服務群組。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此服務群組物件的設備群組中覆寫該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
服務	按一下 **Add**（新增）可將服務新增至群組。從下拉式清單中選取，或按一下下拉式清單底部的 **Service**（服務）連結，然後指定設定。如需設定的說明，請參考 物件 > 服務。

© 2019 Palo Alto Networks, Inc.

Objects > Tags（物件 > 頁籤）

頁籤可讓您使用關鍵字或字詞分組物件。您可將標籤套用至位址物件、位址群組（靜態和動態）、應用程式、區域、服務、服務群組和政策規則。您還可以使用 SD-WAN 介面設定檔來將鏈接標籤套用至乙太網路介面。您可使用頁籤來排序或篩選物件，並以視覺方式按色彩分辨物件。將色彩套用至頁籤時，**Policy**（原則）頁籤會顯示具有背景色彩的物件。

您必須先建立頁籤，然後才能使用該頁籤對規則進行分組。指派按頁籤分組的規則後，**View Rulebase as Groups**（以群組形式檢視規則庫）可根據指派的頁籤以視覺化方式查看原則規則庫。以群組形式檢視規則庫時，將保持原則順序和優先順序。在此檢視中，選取群組頁籤以查看按該頁籤分組的所有規則。

預先定義的 **Sanctioned**（認可）頁籤可用於標記應用程式（**Objects**（物件）> **Applications**（應用程式））。需要這些頁籤，才能有準確性（監控 > PDF 報告 > SaaS 應用程式使用情況）。

您想了解什麼內容？	請參閱：
如何建立頁籤？	建立頁籤
如何以群組形式檢視規則庫？	以群組形式檢視規則庫
搜尋已標記的規則。 使用頁籤群組規則。 檢視原則中使用的頁籤。 將頁籤套用至原則。	管理頁籤
想知道更多？	• 使用標籤分組及在視覺上區分物件 • SD-WAN 連結頁籤

建立頁籤

- **Objects**（物件）> **Tags**（標籤）

選取 **Tags**（頁籤）可建立頁籤、指派色彩或刪除、重新命名和複製頁籤。每個物件最多可有 64 個頁籤；當一個物件有多個頁籤時，它會顯示第一個套用頁籤的色彩。

在防火牆上，**Tags**（頁籤）頁籤會顯示您在防火牆本機上定義的頁籤，或從 Panorama 推送至防火牆的頁籤。在 Panorama 上，**Tags**（頁籤）頁籤會顯示您在 Panorama 上定義的頁籤。此頁籤不會顯示從 VM 資訊來源（該來源在防火牆上定義以組成動態位址群組）動態擷取的頁籤，亦不會顯示使用 XML 或 REST API 定義的頁籤。

當您建立新頁籤時，將在目前在防火牆或 Panorama 上選取的 Virtual System（虛擬系統）或 Device Group（裝置群組）中自動建立頁籤。

頁籤設定	說明
名稱	輸入唯一的頁籤名稱（最多 127 個字元）。名稱不區分大小寫。
共享	若您想讓以下對象使用頁籤，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用頁籤。

© 2019 Palo Alto Networks, Inc.

頁籤設定	說明
	• Panorama 上的每個裝置群組。若您停用（清除）此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用頁籤。
停用覆寫（僅限 Panorama）	若要防止管理員在繼承頁籤的裝置群組中取代此頁籤的設定，請選取此選項。預設會清除此選項，這表示管理員可取代任何繼承頁籤之裝置群組的設定。
色彩	在下拉式清單中，從調色盤選取色彩（預設為無）。
註解	新增頁籤或說明來說明頁籤的用途。

- 新增頁籤：**Add**（新增）頁籤，然後填寫下列欄位：

  您在 **Policies**（原則）頁籤中建立或編輯原則時，也可建立新頁籤。將在目前選取的 [裝置群組] 或 [虛擬系統] 中自動建立頁籤。
- 編輯頁籤：按一下頁籤以編輯或重新命令頁籤，或為其指派色彩。
- 刪除頁籤：按一下 **Delete**（刪除），並選取頁籤。您無法刪除預先定義的頁籤。
- 移動或複製頁籤：移動或複製頁籤的選項，可讓您在啟用了多個虛擬系統的防火牆上將頁籤複製到或移至不同的「裝置群組」或「虛擬系統」。

  移動或複製，並選取頁籤。選取 **Destination**（目的地）位置—「裝置群組」或「虛擬系統」。若您希望驗證程序在顯示錯誤之前先尋找物件的所有錯誤，請停用（清除）**Error out on first detected error in validation**（驗證中第一次偵測到錯誤時離開）選項。此選項預設為啟用，而驗證程序會在偵測到第一個錯誤停止並僅顯示該錯誤。
- 取代或還原頁籤（僅適用於 Panorama）：若您建立了頁籤，則僅在未選取 **Disable override**（停用取代）選項時，才可以使用 **Override**（取代）選項。**Override**（取代）選項可讓您取代指派給從共用或上階裝置群組所繼承頁籤的色彩。**Location**（位置）是目前的裝置群組。您還可以 **Disable override**（停用取代）以防未來嘗試執行取代。

  Revert（還原）變更可復原頁籤的最近修改。當您還原頁籤時，**Location**（位置）欄位會顯示頁籤繼承來源的裝置群組或虛擬系統。

以群組形式檢視規則庫

- **Policies**（原則）> **<Rulebase Type>**（**<規則庫類型>**）

View Rulebase as Groups（以群組形式檢視規則庫）以使用群組頁籤顯示原則規則庫。以群組形式檢視規則庫時，將保持原則順序和優先順序。在此檢視中，選取群組頁籤以查看按該頁籤分組的所有規則。

以群組形式檢視規則庫時，按一下 **Group**（群組）以移動、變更、刪除或複製選定頁籤群組內的所有規則。下表說明了以群組形式檢視規則庫時可用的規則管理選項。

選項	說明
移動群組中的規則至不同的規則庫或裝置群組	將選定頁籤群組中的所有原則規則移動到其他規則庫或裝置群組。
變更所有規則的群組	將選定頁籤群組中的所有規則移動到其他頁籤群組。
移動群組中的所有規則	將選定頁籤群組中的所有規則移動到規則庫。
刪除群組中的所有規則	刪除選定頁籤群組中的所有規則。

© 2019 Palo Alto Networks, Inc.

選項	說明
複製群組中的所有規則	複製選定頁籤群組中的所有規則。

移動群組中的規則至不同的規則庫或裝置群組

若需要組織規則庫，請選取包含要移動之規則的頁籤群組，然後 **Move Rules in Group to Different Rulesbase or Device Group**（將群組中的規則移動到其他規則庫或裝置群組），以將其重新指派到其他規則庫或裝置群組（而不是單獨移動每個規則）。在將頁籤群組中的規則移動到其他裝置群組之前，裝置群組必須已存在（無法在移動規則時建立裝置群組）。此外，您可以將頁籤群組中的規則移動到同一裝置群組中的其他規則庫。

若要將規則移動到其他規則庫或裝置群組，請輸入以下內容：

欄位	說明
目的地	移動原則規則的目標裝置群組。
（僅 Panorama）目的地類型	選取是要將規則移動到目的地裝置群組的 **Pre-Rulebase**（前置規則庫）還是 **Post-Rulebase**（後置規則庫）。
規則順序	選取規則庫中移動規則的目標位置。您可選取： • **Move Top**（移至頂部）—將規則移動到目的地裝置群組的規則庫頂部。 • **Move Bottom**（移至底部）—將規則移動到目的地裝置群組的規則庫底部。 • **Before Rule**（規則之前）—將規則移動到目的地裝置群組之規則庫中選定規則之前。 • **After Rule**（規則之後）—將規則移動到目的地裝置群組之規則庫中選定規則之後。
驗證中第一次偵測到錯誤時離開	核取此方塊可確定在驗證期間遇到錯誤時將如何顯示錯誤。若已核取，則會單獨顯示每個錯誤。若取消核取，則會彙總錯誤並將其顯示為單個錯誤。 驗證期間偵測到的錯誤會導致規則移動工作失敗，並且不會將規則移動到目的地裝置群組。

變更所有規則的群組

不是編輯每個規則，而是 **Change Group of All Rules**（變更所有規則的群組），以將整個原則規則集從一個頁籤群組移至另一個現有頁籤群組。移至新頁籤群組後，將保留頁籤群組規則的規則順序，但您可以選擇將新規則放在目的地頁籤群組中的規則之前或之後。

若要將規則移動到其他頁籤群組，請指定目的地頁籤群組以及移動的規則的放置位置。

欄位	說明
依照其出現順序選取群組	選取目的地頁籤群組。
移至頂部	**Move Top**（移至頂部）將規則插入目的地頁籤群組的頂部。
移至底部	**Move bottom**（移至底部）將規則插入目的地頁籤群組的底部。

© 2019 Palo Alto Networks, Inc.

移動群組中的所有規則

與其對每個規則單獨進行重新排序，不如 **Move All Rules in Group**（移動群組中的所有規則），以將選定頁籤群組中的所有規則向上或向下移動到規則階層中。移動頁籤群組時，將保留頁籤群組規則內移動規則的規則順序，但您可以選取將規則放在目的地頁籤群組中的規則之前或之後。

若要移動規則，請指定目的地頁籤群組以及移動的規則的放置位置。

欄位	說明
依照其出現順序選取群組	選取目的地頁籤群組。
移至頂部	**Move Top**（移至頂部）將規則插入目的地頁籤群組之前。
移至底部	**Move bottom**（移至底部）將規則插入目的地頁籤群組之後。

刪除群組中的所有規則

若要簡化規則管理，您可以 **Delete All Rules in Group**（刪除群組中的所有規則）以降低安全風險，並透過刪除與選定頁籤群組關聯的未使用或不需要的規則來保持原則規則庫整齊有序。

複製群組中的所有規則

不是手動重新建立頁籤群組中的現有原則規則，而是 **Clone All Rules in Group**（複製群組中的所有規則），以快速複製您選擇的裝置群組和規則庫中選定頁籤群組內的規則。在將頁籤群組中的規則複製到其他裝置群組之前，裝置群組必須已存在（無法在複製規則時建立裝置群組）。此外，您可以將頁籤群組中的規則複製到同一裝置群組中的其他規則庫。

複製的規則會附加有規則名稱和以下格式：`<Rule Name>-1`。如果將規則複製到與第一個複製的規則相同的位置，並且名稱未變更，則會附加該名稱。例如，`<Rule Name>-2`、`<Rule Name>-3` 等。

若要複製規則，請設定下列欄位。

欄位	說明
目的地	複製的原則規則的目標裝置群組。
（僅 Panorama）目的地類型	選取要將規則複製到目的地裝置群組的 **Pre-Rulebase**（前置規則庫）或是 **Post-Rulebase**（後置規則庫）。
規則順序	選取規則庫中複製規則的目標位置。您可選取： • **Move Top**（移至頂部）—將複製的規則插入目的地裝置群組的規則庫頂部。 • **Move Bottom**（移至底部）—將複製的規則插入目的地裝置群組的規則庫底部。 • **Before Rule**（規則之前）—將複製的規則插入目的地裝置群組之規則庫中選定規則之前。 • **After Rule**（規則之後）—將複製的規則插入目的地裝置群組之規則庫中選定規則之後。
驗證中第一次偵測到錯誤時離開	選取此選項可確定在驗證期間遇到錯誤時將如何顯示錯誤。若啟用此項，則會單獨顯示每個錯誤。若停用（清除），則會彙總錯誤並將其顯示為單個錯誤。

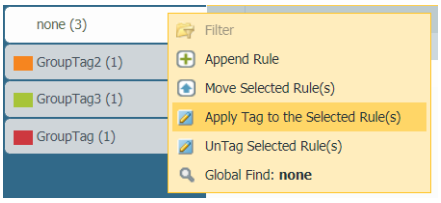
© 2019 Palo Alto Networks, Inc.

欄位	說明
	驗證期間偵測到的錯誤會導致規則複製工作失敗，並且不會將規則複製到目的地裝置群組。

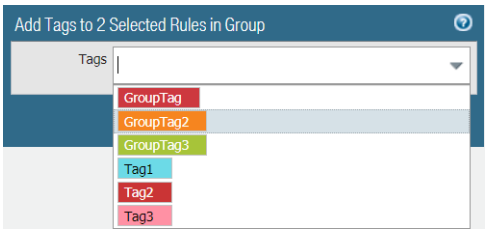
管理頁籤

下表列出按群組頁籤進行規則分組時可執行的動作。

- 標記規則。
  1. 選取 **View Rules as Groups**（以群組形式檢視規則）。
  2. 在右方窗格中選取一個或多個規則。
  3. 從群組頁籤下拉式清單中，**Apply Tag to the Selected Rules**（將頁籤套用至選取的規則）。

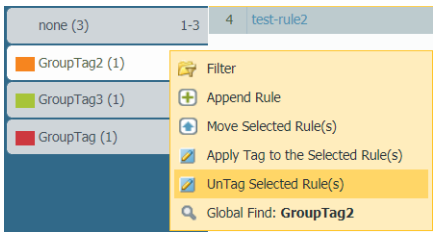


  4. 將頁籤套用至選取的規則。



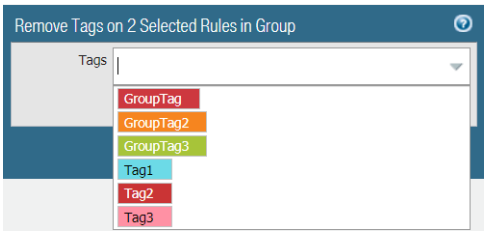
- 檢視指派了群組頁籤的規則。
  1. **View Rulebase as Groups**（以群組形式檢視規則庫）以檢視指派了規則的群組頁籤。
  2. 右方窗格會更新為顯示包含任一選取頁籤的群組頁籤規則。
  3. 選取群組頁籤以檢視指派給該群組的規則。未指派群組頁籤的規則列在 **none**（無）群組中。

- 取消標記規則。
  1. **View Rulebase as Groups**（以群組形式檢視規則庫）以檢視指派了規則的群組頁籤。
  2. 在右方窗格中選取一個或多個規則。
  3. 從群組頁籤下拉式清單中，**Apply Tag to the Selected Rules**（將頁籤套用至選取的規則）。



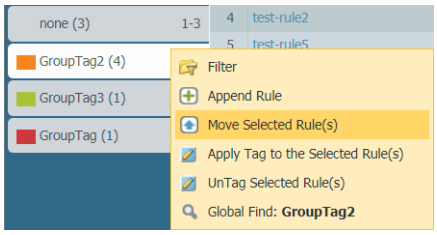
  4. 將頁籤從選取的規則移除。此外，您可以 **Delete All**（刪除全部）指派給規則的頁籤。

© 2019 Palo Alto Networks, Inc.



- 使用頁籤重新排序規則。

  當您 **View Rulebase as Groups**（以群組形式檢視規則庫）時，選取群組頁籤內的一個或多個規則，將滑鼠移至規則編號，然後在下拉式清單中選取 **Move Selected Rule(s)**（移動選取的規則）。若要移動選取群組頁籤內的所有規則，請勿選取任何規則。



  從移動規則視窗的下拉式清單中選取群組頁籤，並針對在下拉式清單中所選的頁籤選取您要 **Move Before**（移至其前）或 **Move After**（移至其後）。

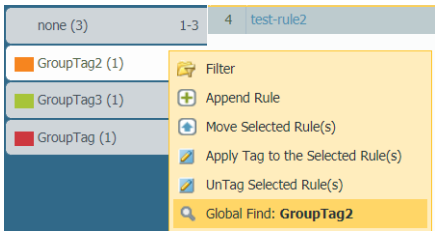
- 新增套用所選標籤的規則。

  當您 **View Rulebase as Groups**（以群組形式檢視規則庫）時，將滑鼠移至群組頁籤，然後在下拉式清單中選取 **Append Rule**（附加規則）。

  新規則將附加到指派給群組頁籤之規則清單的末尾。

- 搜尋群組頁籤。

  當您 **View Rulebase as Groups**（以群組形式檢視規則庫）時，將滑鼠移至群組頁籤，然後從下拉式清單中選取 **Global Find**（全域尋找）。



- 匯出頁籤組態表。

  管理角色可以用 **PDF/CSV** 格式匯出物件組態表，並可以套用篩選器到自訂的表格輸出，使其僅包含您所需要的欄位。僅匯出對話中匯出的欄位為可見。請參閱匯出設定表資料。

© 2019 Palo Alto Networks, Inc.

Objects > Devices（物件 > 裝置）

也稱為裝置字典，此頁面包含裝置物件的中繼資料。檢閱現有裝置物件的資訊或新增裝置物件。在安全性政策中使用裝置物件作為比對規則，您可以建立基於裝置的政策，其中防火牆可以動態更新安全性政策，並將其套用至新裝置和現有裝置。Palo Alto Networks 透過動態更新來更新裝置字典，您可以在 **Device**（裝置）> **Dynamic Updates**（動態更新）> **Device-ID Content**（**Device-ID** 內容）中檢視。

按鈕/欄位	說明
名稱	裝置物件的名稱。
位置	裝置物件的裝置群組位置。
類別	裝置物件的類別（例如，視訊音訊會議）。
設定檔	裝置物件的裝置設定檔。
型號	裝置物件的型號。
作業系統版本	裝置物件的作業系統版本。
作業系統系列	裝置物件的作業系統系列。
廠商	裝置物件的廠商。
新增	按一下 **Add**（新增）以新增裝置物件。輸入 **Name**（名稱），還可以輸入 **Description**（說明）。選擇裝置的其他中繼資料，例如 **Category**（類別）、**OS**（作業系統）和 **Model**（型號）。您也可以 **Browse**（瀏覽）裝置清單，以選取要新增的裝置。按一下 **OK**（確定）確認您的變更。
刪除	選取不再需要的裝置物件，然後將其 **Delete**（刪除）。
移動	選取要移動的裝置物件，然後將其 **Move**（移動）。
複製	選取新裝置設定檔所基於的裝置物件，然後將其 **Clone**（複製）。
PDF/CSV	以 **PDF/CSV** 格式匯出裝置清單。您可以視需要套用篩選器來建立更具體的輸出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。

© 2019 Palo Alto Networks, Inc.

Objects > External Dynamic Lists（物件 > 外部動態清單）

外部動態清單是以 IP 位址、URL、網域名稱、國際行動設備身分 (IMEI) 或國際行動用戶身分 (IMSI) 匯出清單為基礎的位址物件，您可以在政策規則中使用該清單來封鎖或允許流量。這份清單必須是儲存至防火牆可存取之 Web 伺服器的文字檔。依預設，防火牆使用管理 (MGT) 介面來擷取此清單。

如果具有有效的威脅防護授權，Palo Alto Networks 提供了數種內建的動態 IP 位址清單，您可以用其封鎖惡意主機攻擊。我們會根據最新的威脅研究每日更新該清單。

您可以使用 IP 位址清單作為政策規則的來源和目的地中的位址物件；您可以在 URL 篩選設定檔中使用 URL 清單（Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）），或作為安全性政策規則中的比對規則；而且您可以使用網域清單（Objects > Security Profiles > Anti-Spyware Profile（物件 > 安全性設定檔 > 反間諜軟體設定檔））作為指定網域名稱的 Sinkhole。

在每個防火牆型號上，您最多可以使用在所有安全性原則規則中具有唯一來源的 30 個外部動態清單。防火牆對每種清單類型支援的最大項目數目會隨著防火牆型號而有所不同（請參閱每種外部動態清單類型的不同防火牆限制）。僅在外部動態清單使用於政策規則中時，清單項目才會計入最大限制。如果您超過防火牆型號支援的最大項目數，防火牆會產生系統日誌並略過超過限制的項目。若要檢查政策規則中目前使用的 IP 位址、網域、URL、IMEI 和 IMSI 數目以及防火牆上支援的總數，請選取 **List Capacities**（清單容量）（僅限防火牆）。

外部動態清單以由上至下的評估順序顯示。使用頁面底部的方向控制變更清單順序。這讓您能夠對清單進行重新排序，以確保在達到容量限制之前提交外部動態清單中最重要的項目。

當清單是依類型分組時，您無法變更外部動態清單順序。

若要從裝載外部動態清單的主機擷取其最新版本，請選取外部動態清單並 **Import Now**（立即匯入）。

您無法刪除、複製或編輯 *Palo Alto Networks* 惡意 *IP* 位址摘要的設定。

Add（新增）新的外部動態清單，以及如下表所述進行設定。

外部動態清單設定	說明
名稱	輸入可識別外部動態清單的名稱（最多 32 個字元）。此名稱可識別用於政策規則實施的清單。
共用 （僅限多重虛擬系統（多重 vsys）和 Panorama）	若您想讓以下對象使用外部動態清單，請啟用此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。 若您停用（清除）此選項，則僅在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）使用外部動態清單。 • Panorama 上的每個裝置群組。 若您停用（清除）此選項，則僅在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）使用外部動態清單。

© 2019 Palo Alto Networks, Inc.

外部動態清單設定	說明
停用覆寫（僅限 Panorama）	啟用此選項，可防止管理員在繼承此外部動態清單物件的裝置群組中取代該物件的設定。此選項預設為停用（清除），這表示管理員可以覆寫繼承此物件之任何裝置群組的設定。
測試來源 URL（僅限防火牆）	**Test Source URL**（測試來源 **URL**）以確認防火牆可連線至裝載外部動態清單的伺服器。 此測試不會檢查伺服器是否驗證成功。
建立清單頁籤	

類型
您不能在單一清單中混合 *IP* 位址、*URL* 及網域名稱。每份清單必須只包含一種類型的項目。
	從下列類型的外部動態清單中選取：
	• **Predefined IP List**（預先定義的 **IP** 清單）—將 Palo Alto Networks 識別為防彈 IP 位址、已知惡意 IP 位址或高風險 IP 位址的清單用作清單項目的來源（需要有效的威脅防護授權）。
	• **Predefined URL List**（預先定義的 **URL** 清單）—使用 Palo Alto Networks 識別為受信任的網域清單，以將這些網域排除在驗證政策之外。
	• **IP List**（**IP** 清單）（預設）—每個清單可以包括 IPv4 或 IPv6 位址、位址範圍和子網路。清單必須是每行只包含一個 IP 位址、範圍或子網路。例如：
	`192.168.80.150/32`
	`2001:db8:123:1::1 or 2001:db8:123:1::/64`
	`192.168.80.0/24`
	`2001:db8:123:1::1 - 2001:db8:123:1::22`
	在上面的範例中，第一行指示從 192.168.80.0 到 192.168.80.255 的所有位址。子網路或 IP 位址範圍（例如 92.168.20.0/24 或 192.168.20.40 – 192.168.20.50）可算為一個 IP 位址項目，而不算是多個 IP 位址。
	• **Domain List**（網域清單）—每份清單每行只能包含一個網域名稱項目。例如：
	`www.p301srv03.paloalonetworks.com`
	`ftp.example.co.uk`
	`test.domain.net`
	對於外部動態清單中所包含的網域清單，防火牆將建立間諜軟體類型及中等嚴重性的自訂特徵碼集，以便您使用針對自訂網域清單的 sinkhole 動作。
	• **URL** 清單—每份清單每行只能包含一個 URL 項目。例如：
	`financialtimes.co.in`
	`www.wallaby.au/joey`
	`www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx`
	`*.example.com/*`

© 2019 Palo Alto Networks, Inc.

外部動態清單設定	說明
	對於每份 URL 清單，預設動作會設為 **Allow**（允許）。若要編輯預設動作，請參閱 Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）。
類型（續）	• **Subscriber Identity List**（用戶身分清單）—每個清單都包含 3G、4G 或 5G 網路的用戶 ID。在「來源」欄位中，輸入防火牆存取清單的 URL。 • **Equipment Identity List**（設備身分清單）—每個清單都包含 3G、4G 或 5G 網路的設備 ID。在「來源」欄位中，輸入防火牆存取清單的 URL。 根據需要外部動態清單和靜態項目支援的 *3G*、*4G* 和 *5G* 網路識別碼的總數，確定要購買的防火牆型號。
說明	輸入外部動態清單的說明（最多 255 個字元）。
來源	• 如果外部動態清單是預先定義的 IP 清單，請選取 **Palo Alto Networks - Bulletproof IP addresses**（防彈 **IP** 位址）、**Palo Alto Networks - High risk IP addresses**（高風險 **IP** 位址）或 **Palo Alto Networks - Known malicious IP addresses**（已知的惡意 **IP** 位址）作為清單來源。 • 如果外部動態清單是預先定義的 URL 清單，則預設設定為 **panw-auth-portal-exclude-list**。 • 如果外部動態清單是 IP 清單、網域清單或 URL 清單，請輸入包含文字檔案的 HTTP 或 HTTPS URL 路徑（例如 `http://192.0.2.20/myfile.txt`）。 • 如果外部動態清單是網域清單，則預設設定為 **Automatically expand to include subdomains**（自動展開以包含子網域）。此選項使 PAN-OS® 軟體能夠評估外部動態清單檔案中列出的網域名稱所有較低等級的元件。 • 如果外部動態清單是用戶身分清單或設備身分清單，則輸入包含該清單的 URL 路徑。 如果您的外部動態清單包含子網域，則這些展開的項目將計入您的設備型號容量計數。如果您希望手動定義子網域，可以停用此功能。然而，原則規則不會評估清單中未明確定義的子網域。
憑證設定檔 （僅限 IP 清單、網域清單或 URL 清單）	如果外部動態清單有 HTTPS URL，請選取現有憑證設定檔（防火牆和 Panorama）或建立新的 **Certificate Profile**（憑證設定檔）（僅限防火牆），以便驗證裝載清單的 Web 伺服器。如需設定憑證設定檔的詳細資訊，請參閱 [裝置 > 憑證管理 > 憑證設定檔]。 預設值：無（停用憑證設定檔） 若要將您可以用於強制執行原則的外部動態清單數目最大化，請使用相同的憑證設定檔來驗證使用相同來源 *URL* 的外部動態清單，以便將這些清單算為僅只一份外部動態清單。來自相同來源 *URL* 但使用不同憑證設定檔的外部動態清單可算為唯一的外部動態清單。
用戶端驗證	啟用此選項（預設停用）來新增使用者名稱和密碼，以便防火牆在存取需要基本 HTTP 驗證的外部動態清單來源時使用。此設定僅適用於外部動態清單具有 HTTPS URL 時。

© 2019 Palo Alto Networks, Inc.

外部動態清單設定	說明
	• 使用者名稱—輸入有效使用者的名稱來存取清單。 • 密碼/確認密碼—輸入並確認使用者名稱的密碼。
檢查更新	指定防火牆從 Web 伺服器擷取清單的頻率。您可設定防火牆擷取清單的間隔時間為 **Every Five Minutes**（每五分鐘）（預設）、**Hourly**（每小時）、**Daily**（每天）、**Weekly**（每週）或 **Monthly**（每月）。該間隔是相對於上次提交。因此，對於五分鐘間隔，如果上次提交是在一個小時前，則該提交會在 5 分鐘後進行。提交參考該清單的所有政策規則更新，以便防火牆成功地強制執行政策規則。 您不必為預先定義的 *IP* 清單設定頻率，因為防火牆會使用作用中威脅防護授權動態接收內容更新。
清單項目和例外狀況頁籤	
清單項目	顯示外部動態清單中的項目。 • **Add an entry as a list exception**（新增一個項目作為清單例外狀況）—最多選取 100 個項目並按一下 **Submit**（提交）(→)。 • **View an AutoFocus threat intelligence summary for an item**（檢視項目的 **AutoFocus** 威脅情報摘要）—將游標懸停在項目上，然後從下拉式清單中選取 **AutoFocus**。您必須擁有 AutoFocus™ 授權並啟用 AutoFocus 威脅情報才能查看項目摘要（選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）並編輯 **AutoFocus** 設定）。 • **Check if an IP address, domain, or URL is in the external dynamic list**（檢查 **IP** 位址、網域或 **URL** 是否在外部動態清單中）—在篩選欄位中輸入一個值並 **Apply Filter**（套用篩選器）(→)。**Clear Filter**（清除篩選器）(**[X]**) 以返回檢視完整的清單。
手動例外狀況	顯示外部動態清單的例外狀況。 • **Edit an exception**（編輯例外狀況）—選取例外狀況並進行變更。 • **Manually enter an exception**（手動輸入例外狀況）—手動 **Add**（新增）一個新的例外狀況。 • **Remove an exception from the Manual Exceptions list**（從手動例外狀況清單中移除例外狀況）—選取並 **Delete**（刪除）例外狀況。 • **Check if an IP address, domain, or URL is in the Manual Exceptions list**（檢查 **IP** 位址、網域或 **URL** 是否在手動例外狀況清單中）—在篩選欄位中輸入一個值並 **Apply Filter**（套用篩選器）(→)。**Clear Filter**（清除篩選器）(**[X]**) 以返回檢視完整的清單。如果手動例外狀況清單中有重複的項目，您就無法將變更儲存至外部動態清單中。

© 2019 Palo Alto Networks, Inc.

物件 > 自訂物件

建立自動資料模式、漏洞及間諜軟體特徵碼，以及要用於政策的 URL 類別：

- Objects > Custom Objects > Data Patterns（物件 > 自訂物件 > 資料模式）
- Objects > Custom Objects > Spyware/Vulnerability（物件 > 自訂物件 > 間諜軟體 / 弱點）
- Objects > Custom Objects > URL Category（物件 > 自訂物件 > URL 類別）

Objects > Custom Objects > Data Patterns（物件 > 自訂物件 > 資料模式）

下列主題說明資料模式。

您想了解什麼內容？	請參閱：
建立資料模式。	資料模式設定
進一步了解規則運算式資料模式的語法以及查看一些範例。	規則運算式資料模式的語法 規則運算式資料模式範例

資料模式設定

選取 **Objects**（物件）> **Custom Objects**（自訂物件）> **Data Patterns**（資料模式），可定義您可能要篩選的敏感資訊類別。如需定義資料篩選設定檔的相關資訊，請選取 [物件 > 安全性設定檔 > 資料篩選]。

您可以為防火牆建立三種類型的資料模式，供其在掃描敏感資訊時使用：

- 預先定義—使用預先定義的資料模式，掃描檔案中的社會安全號碼和信用卡號碼。
- 規則運算式—使用規則運算式建立自訂資料模式。
- 檔案內容—掃描檔案中的特定檔案內容和值。

資料模式設定	說明
名稱	輸入資料模式名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入資料模式的說明（最多 255 個字元）。
共享	若您想讓以下對象使用資料模式，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用資料模式。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用資料模式。
停用覆寫（僅限 Panorama）	若要防止管理員在繼承物件的設備群組中覆寫此資料模式物件的設定，請選取此選項。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。

© 2019 Palo Alto Networks, Inc.

資料模式設定	說明
模式類型	選取您要建立的資料模式類型： • 預先定義的模式 • 規則運算式 • 檔案內容
預先定義的模式	Palo Alto Networks 提供了預先定義的資料模式，用以掃描檔案中特定類型的資訊，例如信用卡號碼或社會安全號碼。若要根據預先定義的模式設定資料篩選，請 **Add**（新增）模式並選取下列項目： • 名稱—選取用來篩選敏感資料的預先定義模式。如果您挑選預先定義的模式，將會自動填入 說明（說明）。 • 選取您要在其中偵測預先定義模式的 **File Type**（檔案類型）。
規則運算式	**Add**（新增）自訂資料模式。為模式指定說明性 **Name**（名稱）、設定要掃描資料模式的 **File Type**（檔案類型），然後輸入定義 **Data Pattern**（資料模式）的規則運算式。 如需規則運算式資料模式的語法詳細資料和範例，請參閱： • 規則運算式資料模式的語法 • 規則運算式資料模式範例
檔案內容	建立用來掃描檔案內容和相關值的資料模式。例如，您可以 **Add**（新增）一個資料模式，用來篩選文件標題中包含「敏感」、「內部」或「機密」等文字的 Microsoft Word 文件和 PDF。 • 為資料模式指定說明性 **Name**（名稱）。 • 選取您要掃描的 **File Type**（檔案類型）。 • 選取要掃描特定值的 **File Property**（檔案內容）。 • 輸入您要掃描的 **Property Value**（內容值）。

規則運算式資料模式的語法

建立資料模式的常規模式要求和語法取決於您啟用的模式比對引擎：經典或增強（預設）。

模式要求	經典	增強
模式長度	需要 7 個文字字元，不能包含句點 (`.`)、星號 (`*`)、加號 (`+`) 或範圍值 (`[a-z]`)。	需要兩個文字字元。
不區分大小寫	需要您定義所有可能字串的模式以符合字詞的所有變化。 範例：若要比對指定為機密 (confidential) 的任何文件，您必須建立包含「confidential」、「Confidential」和「CONFIDENTIAL」的模式。	允許您在子模式上使用 **i** 選項。 範例：**`((?i)\bconfidential\b)`** 符合 `ConfiDential`

© 2019 Palo Alto Networks, Inc.

PAN-OS® 中的規則運算式語法與傳統規則運算式引擎相似，但是每個引擎都是唯一的。經典語法和增強語法表描述了 PAN-OS 模式比對引擎中支援的語法。

經典語法

模式語法	說明
.	比對任何單一字元。
?	比對前置字元或表示式 0 或 1 次。必須將一般運算式括在括號中。 範例：**(abc)?**
*	比對前置字元或表示式 0 或多次。必須將一般運算式括在括號中。 範例：**(abc)***
+	比對前置字元或規則運算式一或多次。必須將一般運算式括在括號中。 範例：**(abc)+**
|	指定一個「或」另一個。 必須將替代子字串括在括號中。 範例：**((bif)|(scr)|(exe))** 符合 bif、scr 或 exe。
-	指定範圍。 範例：**[c-z]** 符合 c 與 z 之間的任何字元（包括 c 與 z）。
[ ]	比對任何指定的字元。 範例：**[abz]** 符合任何指定的字元—a、b 或 z。
^	比對除指定字元以外的任何字元。 範例：**[^abz]** 符合除以下指定字元以外的任何字元—a、b 或 z。
{ }	比對含有最小值和最大值的字串。 範例：**{10-20}** 符合 10 與 20 位元組之間的任何字串（包括 10 位元組與 20 位元組）。必須在固定字串前面直接指定此項，並且只能使用連字號 (-)。
\	對任何字元執行文字比對。必須在指定的字元前面放置反斜杠 (\)。
&amp	& 符號是特殊字元，因此若要在字串中尋找 &，必須使用 **&amp**。

增強語法

增強模式比對引擎支援所有經典語法及以下語法：

© 2019 Palo Alto Networks, Inc.

模式語法	說明
速記字元類 代表特定類型字元的符號，例如數字或空格。您可以使用大寫字元來否定任何這些速記字元類。	
\s	符合任何空白字元。 範例：**\s** 符合空格、定位字元、換行符號或換頁字元。
\d	符合數字 [0-9] 的字元。 範例：**\d** 符合 0。
\w	符合 ASCII 字元 [A-Za-z0-9_]。 範例：**\w\w\w** 符合 PAN。
\v	符合垂直空格字元，其中包括所有 unicode 換行符號字元。 範例：**\v** 符合垂直空格字元。
\h	符合水平空格，其中包括定位字元和所有「空格分隔符號」Unicode 字元。 範例：**\h** 符合水平空格字元。
有界重複量詞 指定重複上一項的次數。	
{n}	精確符合次數 (*n*)。 範例：**a{2}** 符合 aa。
{n,m}	**{n,m}** 符合從 *n* 至 *m* 次。 範例：**a{2,4}** 符合 aa、aaa 和 aaaa
{n, }	**{n,}** 符合至少 *n* 次。 範例：**a{2,}** 符合 aaaaab 中的 aaaaa.
錨點字元 指定符合表達式的位置。	
^	在字串開頭比對。啟用多行模式 (**m**) 時，在每個換行符號之後也比對。 範例：指定字串 abc，**^a** 符合 a，但 **^b** 不符合任何內容，因為 b 不會出現在字串的開頭。
$	在字串末尾或在字串末尾的換行符號之前比對。啟用多行模式 (**m**) 時，在每個換行符號之前也比對。 範例：指定字串 abc，**c$** 符合 c，但 **a$** 不符合任何內容，因為 a 不會出現在字串的末尾。

© 2019 Palo Alto Networks, Inc.

模式語法	說明
\A	在字串開頭比對。即使啟用了多行模式 (m)，也不會在換行後比對。
\Z	在字串的末尾和最後的換行符號之前比對。即使啟用了多行模式 (m)，也不會在其他換行之前比對。
\z	在字串的絕對末尾處比對。換行前不比對。
選項修飾元 變更子模式的行為。輸入 `(?<option>)` 以啟用，或輸入 `(?-<option>)` 以停用。	
i	啟用不區分大小寫。 範例：`((?i)\bconfidential\b)` 符合 `ConfiDential`。
m	在行的開頭和末尾使 ^ 和 $ 相符。
s	使 . 符合任何內容，包括換行符號。
x	忽略 regex 語彙基元之間的空格。

規則運算式資料模式範例

以下是有效自訂模式的範例：

- .*((Confidential)|(CONFIDENTIAL))
  - 在任意位置尋找文字「Confidential」或「CONFIDENTIAL」
  - 開頭的「.*」指定在資料流中的任意位置尋找
  - 取決於解碼器的區分大小寫要求，這可能不會比對「confidential」（全部小寫）。
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
  - 尋找「Proprietary & Confidential」或「Proprietary and Confidential」
  - 比尋找「Confidential」更精確
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
  - 尋找「Press Release」後面加上以任何形式存在的 draft 這個字，這可能表示新聞稿未準備就緒，無法傳送至公司外部
- .*(Trinidad)
  - 尋找專案代碼名稱，例如「Trinidad」

© 2019 Palo Alto Networks, Inc.

Objects > Custom Objects > Spyware/ Vulnerability（物件 > 自訂物件 > 間諜軟體 / 弱點）

防火牆支援使用防火牆威脅引擎建立自訂間諜軟體與漏洞特徵碼的功能。您可以編寫自訂正規表示式特徵碼，以識別間諜軟體 phone home 通訊或漏洞入侵。所產生的間諜軟體與漏洞特徵碼將可在任何自訂漏洞設定檔中使用。防火牆會尋找網路流量中自訂定義的特徵碼，並針對漏洞入侵採取指定的動作。

每週內容更新會定期包括可讓您針對它們開發特徵碼的新解碼器及內容。

您可以在定義自訂特徵碼時選擇性地包含時間屬性，方法是指定每個間隔的閾值，以在回應攻擊時觸發可能的動作。只有達到臨界值之後才會採取動作。

使用 **Custom Spyware Signature**（自訂間諜軟體特徵碼）頁面來定義反間諜軟體設定檔的特徵碼。使用 **Custom Vulnerability Signature**（自訂漏洞特徵碼）頁面來定義漏洞保護設定檔的特徵碼。

自訂漏洞和間諜軟體特徵碼設定	說明
組態頁籤	
威脅 ID	為設定輸入數字識別碼（間諜軟體特徵碼範圍是 15000-18000 和 6900001 - 7000000；弱點特徵碼範圍是 41000-45000 和 6800001-6900000）。
名稱	指定威脅名稱。
共用	若您想讓以下對象使用自訂特徵碼，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用自訂特徵碼。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（設備群組）才可使用自訂特徵碼。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此特徵碼的設備群組中覆寫該特徵碼的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此特徵碼之任何設備群組的設定。
備註	輸入選擇性註解。
severity	指定指示威脅嚴重性的等級。
預設動作	指定要在符合威脅條件時採取的預設動作。如需動作清單，請參閱安全性設定檔中的動作。
方向	指示從用戶端至伺服器、從伺服器至用戶端，或從兩個方向評估威脅。

© 2019 Palo Alto Networks, Inc.

自訂漏洞和間諜軟體特徵碼設定	說明
受影響的系統	指示威脅涉及用戶端、伺服器、任何一者或兩者。適用於漏洞特徵碼，間諜軟體特徵碼則不適用。
CVE	指定一般漏洞列舉 (CVE) 做為其他背景與分析的外部參考。
廠商	指定漏洞的廠商識別碼作為其他背景與分析的外部參考。
Bugtraq	指定 bugtraq（與 CVE 相似）作為其他背景與分析的外部參考。
Reference	新增任何連結至其他分析或背景資訊。當使用者按一下來自 ACC、日誌或漏洞設定檔的威脅時，所顯示出來的資訊。
特徵碼頁籤	

標準特徵碼	選取 **Standard**（標準），然後 **Add**（新增）一個新特徵碼。指定下列資訊：
	• 標準—輸入用來識別特徵碼的名稱。
	• 註解 — 輸入選取性說明。
	• 符合訂購條件 — 選取定義特徵碼條件的順序是否重要。
	• 範圍 — 選取僅將此特徵碼套用至目前程序或套用至完整使用者工作階段。
	按一下 **Add Or Condition**（新增 Or 條件）或 **Add And Condition**（新增 And 條件）來新增條件。若要在群組中新增條件，請選取群組，然後按一下新增條件。將條件新增至特徵碼，以便在您針對條件定義的參數為 true 時為產生流量的特徵碼。從下拉式清單中選取 **Operator**（運算子）。運算子會針對自訂特徵碼定義必須為 true 的條件類型以比對流量。從 **Less Than**（小於）、**Equal To**（等於）、**Greater Than**（大於）或 **Pattern Match**（模式比對）運算子中選擇。
	• 選擇 **Pattern Match**（特徵碼相符）運算子時，請指定以讓下列內容為 True 以讓特徵碼比對流量：
	  • 內容 — 從可用內容中選取。
	  • 模式 — 指定規則運算式。如需規則運算式的模式規則，請參閱模式規則語法。
	  • 限定詞與值 — 選擇性地新增限定詞/值配對。
	  • 否定—選取 **Negate**（否定），讓自訂特徵碼僅在定義的特徵碼相符條件不為 True 時比對流量。這可讓您確保自訂特徵碼不會在特定條件下觸發。
	  您無法只利用否定條件建立自訂特徵碼；必須至少包含一個正條件才可指定否定條件。此外，若特徵碼範圍設為 *[工作階段]*，則 *[否定]* 條件無法設定為比對流量的最後一個條件。
	  您可以使用新選項定義自訂漏洞或間諜軟體特徵碼的例外狀況，以在流量符合特徵碼及特徵碼例外狀況時否定特徵碼產生。使用此選項可允許網路中可能分類為間諜軟體或漏洞入侵的特定流量。在此情況下，將針對符合特徵碼的流量產生特徵碼；符合特徵碼也符合特徵碼例外狀況的流量將從特徵碼產生和任何相關聯的政策動作（例如封鎖或丟棄）排除。例如，您可將特徵碼定義為針對重新導向 URL 產生；不過，現在您也可建立例外狀況，其不會針對重新導向至受信任網域的 URL 產生特徵碼。

© 2019 Palo Alto Networks, Inc.

自訂漏洞和間諜軟體特徵碼設定	說明

	• 選擇 **Equal To**（等於）、**Less Than**（小於）或 **Greater Than**（大於）運算子時，請指定以讓下列內容為 true 以讓特徵碼比對流量：
	  • 內容 — 從未知要求與 TCP 或 UDP 的回應中選取。
	  • 位置 — 在封包所承載資料中的前四位或第二個四位位元組之間選取。
	  • 遮罩 — 指定 4 位元組十六進位值，例如 0xffffff00。
	  • 值 — 指定 4 位元組十六進位值，例如 0xaabbccdd。

組合特徵碼	選取 **Combination**（組合）並指定下列資訊： 選取 **Combination Signatures**（組合特徵碼），指定定義特徵碼的條件： • 按一下 **Add AND Condition**（新增 **AND** 條件）或 **Add OR Condition**（新增 **OR** 條件）來新增條件。若要在群組中新增條件，請選取群組，然後按一下新增條件。 • 若要在群組中移動條件，請選取條件並按一下 **Move Up**（上移）或 **Move Down**（下移）。若要移動群組，請選取群組並按一下 **Move Up**（上移）或 **Move Down**（下移）。您無法將條件從一個群組移至另一個群組。 選取 **Time Attribute**（時間屬性），指定下列資訊： • 拜訪數 — 指定會觸發任何以政策為基礎之動作的臨界值作為指定秒數 (1-3600) 內的相符次數 (1-1000)。 • 彙總準則 — 指定由來源 IP 位址、目的地 IP 位址，還是來源與目的地 IP 位址的組合追蹤相符次數。 • 若要在群組中移動條件，請選取條件並按一下 **Move Up**（上移）或 **Move Down**（下移）。若要移動群組，請選取群組並按一下 **Move Up**（上移）或 **Move Down**（下移）。您無法將條件從一個群組移至另一個群組。

© 2019 Palo Alto Networks, Inc.

Objects > Custom Objects > URL Category（物件 > 自訂物件 > URL 類別）

使用自訂 URL 別頁面可建立您的自訂 URL 清單，並將其用於 URL 篩選設定檔，或作為原則規則比對準則。在自訂 URL 類別中，您可個別新增 URL 項目，也可匯入包含 URL 清單的文字檔案。

新增到自訂類別的 *URL* 項目必須區分大小寫。

下表說明自訂 URL 設定。

自訂 URL 類別設定	說明
名稱	輸入可識別自訂 URL 類別的名稱（最多 31 個字元）。此名稱在定義 URL 篩選原則時會顯示在類別清單中，對於原則規則中的 URL 類別，則會顯示在比對準則中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入 URL 類別的描述（最多 255 個字元）。
類型	選取類別類型： • **Category Match**（類別相符）—選取 **Category Match**（類別相符）以定義含有符合所有指定的 URL 類別的 URL 的新的自訂類別（URL 必須符合清單中的所有類別）。指定 2-4 個類別。 • **URL List**（**URL** 清單）—選取 **URL List**（**URL** 清單）以新增或匯入類別的 URL 清單。此類別類型還包含在 PAN-OS 9.0 之前新增的 URL。
共用	若您想讓以下對象使用 URL 類別，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您停用（清除）此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用 URL 類別。 • Panorama 上的每個裝置群組。若您停用（清除）此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用 URL 類別。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此自訂 URL 物件的裝置群組中取代該物件的設定。預設會停用此選取項目，這表示管理員可以覆寫繼承此物件之任何裝置群組的設定。
網站	管理自訂 URL 類別的網站（新增或匯入的每個 URL 最多可具有 255 個字元）。 • **Add**（新增）—**Add**（新增）URL，每列僅一個。每個 URL 可採用格式「www.example.com」或包含萬用字元，例如「*.example.com」。如需受支援格式的其他資訊，請參閱 Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）中的封鎖清單。 • **Import**（匯入）— **Import**（匯入）並瀏覽以選取包含 URL 清單的文字檔案。每列只輸入一個 URL。每個 URL 可採用格式「www.example.com」或包含萬用字元，例如「*.example.com」。如

© 2019 Palo Alto Networks, Inc.

自訂 URL 類別設定	說明
	需受支援格式的其他資訊，請參閱 Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）中的封鎖清單。 • **Export**（匯出）—**Export**（匯出）包含在清單中的自訂 URL 項目（匯出為文字檔案）。 • **Delete**（刪除）— **Delete**（刪除）項目以從清單中移除 URL。 若要刪除您在 *URL* 篩選設定檔中已使用的自訂類別，您必須先將動作設定為 *None*（無），才能刪除自訂類別。請參閱 Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）中的類別動作。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles（物件 > 安全性設定檔）

安全性設定檔在安全性政策中提供威脅防範。每個安全性政策規則可包括一或多個安全性設定檔。可用的設定檔類型如下：

- 防毒設定檔，可對蠕蟲、病毒和木馬程式提供保護，以及阻止間諜軟體下載。請參閱 物件 > 安全性設定檔 > 防毒軟體。
- 反間諜軟體設定檔，可封鎖受危害主機上的間諜軟體嘗試對外發起連線或發出訊號至外部命令與控制項 (C2) 伺服器的企圖。請參閱 [物件 > 安全性設定檔 > 反間諜軟體設定檔]。
- 漏洞保護設定檔，可阻止嘗試利用系統瑕疵或取得對系統未經授權之存取。請參閱 [物件 > 安全性設定檔 > 漏洞保護]。
- URL 篩選設定檔，可限制使用者存取特定網站和/或網站類別，例如購物或博弈網站。請參閱 [物件 > 安全性設定檔 > URL 篩選]。
- 檔案封鎖設定檔，可封鎖所選檔案類型，和在指定的工作階段流量方向中封鎖檔案（輸入/輸出/兩者）。請參閱 [物件 > 安全性設定檔 > 檔案封鎖]。
- WildFire™ 分析設定檔，可指定要在 WildFire 設備本機上或在 WildFire 雲端上執行檔案分析。請參閱 [物件 > 安全性設定檔 > WildFire 分析]。
- 資料篩選設定檔可協助防止機密資訊（例如信用卡或社會安全號碼）從受保護的網路外洩。請參閱 [物件 > 安全性設定檔 > 資料篩選]。
- DoS 保護設定檔搭配 DoS 保護政策規則，可保護防火牆免於遭受大量單一工作階段和多重工作階段攻擊。請參閱 Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）。
- 行動網路保護設定檔可讓防火牆檢查、驗證及篩選 GTP 流量。

除了個別設定檔以外，您也可結合時常一起套用的設定檔，並建立安全性設定檔群組（**Objects**（物件）> **Security Profile Groups**（安全性設定檔群組））。

安全性設定檔中的動作

動作會指定防火牆回應威脅事件的方式。由 Palo Alto Networks 定義的每個威脅或病毒特徵碼都包含預設動作，通常會設為 **Alert**（警示）而使用您為通知啟用的選項來通知您，或者設為 **Reset Both**（重設兩者）而重設連線兩端。不過，您可以在防火牆上定義或覆寫動作。下列動作可在定義防毒設定檔、反間諜軟體設定檔、漏洞保護設定檔、自訂間諜軟體物件、自訂漏洞物件或 DoS 保護設定檔時套用。

動作	說明	防毒設定檔	防間諜軟體設定檔	漏洞保護設定檔	自訂物件—間諜軟體和漏洞	DoS 保護設定檔
預設值	採取針對每個威脅特徵碼在內部指定的預設動作。 針對防毒設定檔，會對病毒特徵碼採取預設動作。	✓	✓	✓	—	隨機早期丟棄
允許	允許應用程式流量。 *Allow*（允許）動作不會	✓	✓	✓	✓	—

© 2019 Palo Alto Networks, Inc.

動作	說明	防毒設定檔	防間諜軟體設定檔	漏洞保護設定檔	自訂物件—間諜軟體和漏洞	DoS 保護設定檔
	產生與特徵碼或設定檔相關的日誌。					
警示	針對每個應用程式流量產生警示。警示會儲存在威脅日誌中。	✓	✓	✓	✓	✓ 在攻擊量 (cps) 達到設定檔中設定的警報閾值時產生警示。
丟棄	丟棄應用程式流量。	✓	✓	✓	✓	—
重設用戶端	針對 TCP，會重設用戶端連線。 針對 UDP，將丟棄連線。	✓	✓	✓	✓	—
Reset server（重設伺服器）	針對 TCP，會重設伺服器端連線。 針對 UDP，將丟棄連線。	✓	✓	✓	✓	—
Reset both（重設兩者）	針對 TCP，會重設用戶端及伺服器的連線。 針對 UDP，將丟棄連線。	✓	✓	✓	✓	—
封鎖 **IP**	封鎖來自某來源或來源-目的地配對（可進行指定時段內的設定）的流量。	—	✓	✓	✓	✓
Sinkhole	此動作可將惡意網域 DNS 查詢導向 Sinkhole IP 位址。 此動作適用於 Palo Alto Networks DNS 特徵碼和 物件 > 外部動態清單中包含的自訂網域。	—	—	—	—	—

© 2019 Palo Alto Networks, Inc.

動作	說明	防毒設定檔	防間諜軟體設定檔	漏洞保護設定檔	自訂物件—間諜軟體和漏洞	DoS 保護設定檔
隨機早期丟棄	在每秒連線數達到套用至 DoS 保護規則的 DoS 保護設定檔所設定的啟動速率閾值時，導致防火牆隨機丟棄封包。	—	—	—	—	✓
同步處理 **Cookie**	在每秒連線數達到套用至 DoS 保護規則的 DoS 保護設定檔所設定的啟動速率閾值時，導致防火牆產生 SYN Cookie 以驗證來自用戶端的 SYN。	—	—	—	—	✓

您無法刪除在政策規則中使用的設定檔；您必須先從政策規則中移除設定檔。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Anti-Spyware Profile（Objects > Security Profiles > Antivirus（物件 > 安全性設定檔 > 防毒）

使用 **Antivirus Profiles**（防毒設定檔）頁面設定選項，指示防火牆掃描定義流量上的病毒。設定必須檢查是否感染病毒的應用程式，及在偵測到病毒時採取的行動。預設設定檔會檢查所有列出的通訊協定解碼器是否有病毒，然後針對簡單郵件傳輸通訊協定 (SMTP)、網際網路訊息存取通訊協定 (IMAP) 與郵局通訊協定第 3 版 (POP3) 產生警示，最後根據偵測到的病毒類型，針對其他應用程式採取預設動作（警示或拒絕）。接著會將設定檔附加至安全性原則規則，決定將在哪些特定的區域中檢查周遊的流量。

自訂設定檔可以用來最小化受信任安全性區域之間流量的防毒檢驗，及最大化從不受信任區域 (例如網際網路) 中收到的流量以及傳送至高機密目的地 (例如伺服器群) 的流量的檢驗。

若要新增防毒設定檔，請選取 [新增] 並輸入下列設定：

欄位	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在防毒設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號、句點與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
共用 （僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此防毒設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
動作頁籤 針對不同類型的流量指定動作，例如 FTP 及 HTTP。	
啟用封包擷取	如果您要擷取已識別的封包，請選取此選項。
解碼器與動作	針對您要檢查是否有病毒的每種類型的流量，從下拉式清單中選取動作。您可以為標準防毒特徵碼（**Signature Action**（特徵碼動作）欄）、WildFire 系統產生的特徵碼（**WildFire Signature Action**（**WildFire** 特徵碼動作）欄）以及 WildFire Inline ML 模型即時偵測的惡意威脅（**WildFire Inline ML Action**（**WildFire** 內嵌 **ML** 動作）欄）定義不同的動作。 某些環境可能需要較長的時間才能產生防毒特徵碼，所以此選項能為 Palo Alto Networks 提供的兩種防毒特徵碼類型設定不同的動作。例如，標準防毒特徵碼在發行前需要較長的產生期間（24 小時），而 WildFire 特徵碼可在偵測到威脅後的 15 分鐘內產生和發行。因此，您可能會想要在 WildFire 特徵碼上選取警示動作而非封鎖。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	為了獲得最佳安全性，請複製預設的防毒設定檔，並將所有解碼器的動作以及 *WildFire* 動作設定為 *reset-both*（重設用戶端與伺服器），並將設定檔夾帶到所有允許流量的所有安全性原則規則。
應用程式例外狀況和動作	使用 **Applications Exception**（應用程式例外狀況）表格來定義不檢查的應用程式。例如，若要封鎖除了特定應用程式以外的所有 HTTP 流量，您可以定義應用程式為其例外狀況的防毒設定檔。**Block**（封鎖）是 HTTP 解碼器的動作，**Allow**（允許）是應用程式的例外狀況。針對每個應用程式例外清單，請於偵測到威脅時選取要採取的動作。如需動作清單，請參閱安全性設定檔中的動作。 若要尋找應用程式，請開始在文字方塊中輸入應用程式名稱。會顯示相符的應用程式清單，您可以進行選取。 如果您認為一個合法的應用程式被錯誤地識別為攜帶病毒（誤報），請使用 *TAC* 開啟支援案例，以便 *Palo Alto Networks* 可以分析和修復錯誤識別的病毒。問題解決後，從設定檔中移除該例外。

特徵碼例外狀況頁籤

使用 **Signature Exceptions**（特徵碼例外狀況）頁籤來定義防毒設定檔將忽略的威脅清單。

請僅在您確定識別的病毒不是威脅時（誤報）建立例外狀況。如果您認為您發現了誤報，請使用 *TAC* 開啟支援案例，以便 *Palo Alto Networks* 可以分析和修復錯誤識別的病毒特徵碼。問題解決後，立即從設定檔中移除該例外。

威脅 ID	若要新增您想要忽略的特定威脅，一次輸入一個威脅 ID 並按一下 **Add**（新增）。威脅 ID 會顯示為威脅日誌資訊的一部分。請參考 [監控 > 日誌]。

WildFire 內嵌 ML 頁籤

使用 **WildFire Inline ML**（**WildFire 內嵌 ML**）頁籤可以使用防火牆型機器學習模型，以對檔案啟用和設定即時 WildFire 分析。

啟用 *Wildfire 內嵌 ML* 時，*Palo Alto Networks* 建議將範例轉送到 *WildFire* 雲端。這允許觸發誤判的範例在二次分析時自動得到更正。此外，它提供了用於改進 *ML* 模型以供將來更新的資料。

可用型號	對於每個可用的 WildFire 內嵌 ML **Model**（模型），您可以選取以下動作設定之一： • **enable (inherit per-protocol actions)**（啟用（繼承每個通訊協定的動作）—根據您在 **Action**（動作）頁籤解碼器區段的 **WildFire Inline ML Action**（**WildFire 內嵌 ML 動作**）欄中的選擇來檢查流量。 • **alert-only (override more strict actions to alert)**（僅警報（取代更嚴格的警報動作）—根據您在 **Action**（動作）頁籤解碼器區段的 **WildFire Inline ML Action**（**WildFire 內嵌 ML 動作**）欄中的選擇來檢查流量。嚴重性層級高於警報的任何動作（丟棄、重設用戶端、重設伺服器、重設兩者）都將被取代以發出警報，從而允許流量通過，同時在威脅日誌中產生並儲存警報。 • **disable (for all protocols)**（停用（對於所有通訊協定））—-允許流量通過而無需任何政策動作。

© 2019 Palo Alto Networks, Inc.

欄位	說明
檔案例外狀況	**File Exceptions**（檔案例外狀況）表允許您定義不想分析的特定檔案，例如誤判。 若要建立新的檔案例外狀況項目，請 **Add**（新增）新項目，並提供要從強制執行中排除檔案的部分雜湊、檔案名稱和說明。 若要尋找現有的檔案例外狀況，首先在文字方塊中鍵入部分雜湊值、檔案名稱或說明。將顯示與任何這些值相符的檔案例外狀況清單。 您可以在威脅日誌中找到部分雜湊（*Monitor*（監控）> *Logs*（日誌）> *Threat*（威脅））。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Anti-Spyware Profile（物件 > 安全性設定檔 > 反間諜軟體設定檔）

您可將反間諜軟體設定檔附加至安全性政策規則，以便偵測安裝於網路中系統上的間諜軟體和各類命令與控制項 (C2) 惡意軟體所起始的連線。您可選取兩種預先定義的反間諜軟體設定檔以附加到安全性原則規則。每個設定檔都包括按威脅嚴重性排列的預先定義規則集（包括威脅特徵碼）；每個威脅特徵碼都包括 Palo Alto Networks 指定的預設動作。

- 預設—預設設定檔針對各特徵碼使用建立特徵碼時 Palo Alto Networks 內容套件指定的預設動作。
- 嚴格—嚴格設定檔會取代特徵碼檔案中針對重要、高度及中度嚴重性威脅定義的動作，並將其設為 **reset-both**（重設兩者）動作。產生低度及資訊嚴重性威脅時，則採取預設動作。
- 您也可建立自訂設定檔。例如，您可以針對信任安全性區域間的流量減少反間諜軟體檢驗的嚴格度，並最大化從網際網路接收的流量或傳送至受保護資產（例如伺服器群）之流量的檢驗。

下表說明反間諜軟體設定檔 設定：

反間諜軟體設定檔設定	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在反間諜軟體設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號、句點與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此反間諜軟體設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
特徵碼政策頁籤 反間諜軟體規則讓您可定義自訂嚴重性及針對任何威脅、包含您輸入文字的特定威脅，和/或依威脅類型（例如廣告軟體）採取的動作。 **Add**（新增）規則，也可以選取現有規則並選取 **Find Matching Signatures**（尋找相符特徵碼）以根據該規則篩選威脅特徵碼。	
規則名稱	指定規則名稱。
威脅名稱	輸入 **Any**（任何）可比對所有特徵碼，或輸入文字可比對輸入的文字出現在特徵碼名稱中的任何特徵碼。

© 2019 Palo Alto Networks, Inc.

反間諜軟體設定檔設定	說明
類別	選取類別，或選取任何以符合所有類別。
動作	選取每個威脅的動作。如需動作清單，請參閱安全性設定檔中的動作。 **Default**（預設）動作是依據 Palo Alto Networks 提供的各個特徵碼中預先定義的動作。若要檢視特徵碼的預設動作，請選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **Anti-Spyware**（反間諜軟體），然後 **Add**（新增）或選取現有設定檔。按一下 **Exceptions**（例外狀況）頁籤，然後按一下 **Show all signatures**（顯示所有特徵碼），即可看見所有特徵碼的清單和相關聯的 **Action**（動作）。 為獲得最佳安全性，請使用預先定義之 *strict*（嚴格）設定檔中的「動作」設定。
封包擷取	如果您要擷取已識別的封包，請選取此選項。 選取 **single-packet**（單一封包）可在偵測到威脅時擷取一個封包，或選取 **extended-capture**（延伸擷取）選項來擷取 1 到 50 個封包（預設值為 5 個封包）。延伸擷取將在分析威脅日誌時提供更多有關威脅的內容。若要檢視封包擷取，請選取 **Monitor**（監控）> **Logs**（日誌）> **Threat**（威脅），尋找您所要的日誌項目，然後按一下第二欄中的綠色向下箭頭。若要定義待擷取的封包數目，請選取 **Device**（裝置）> **Setup**（設定）> **Content-ID**（內容-ID），然後編輯 Content-ID™ 設定。 如果對給定威脅的動作為允許，則防火牆不會觸發威脅日誌，且不會擷取封包。如果動作為警示，您可以將封包擷取設定為單一封包或延伸擷取。所有封鎖動作（丟棄、封鎖和重設動作）都會擷取單一封包。裝置上的內容套件確定預設動作。 對極其、較高及適中嚴重性事件啟用延伸擷取。使用 5 個封包的預設延伸擷取值，可提供足夠的資訊來分析大多數情況下的威脅。（過多的封包擷取流量可能會導致丟棄封包擷取。）不要對指示性和低嚴重性事件啟用延伸擷取，因為相較於擷取較高嚴重性事件的資訊相比，其並非十分有用，並且會建立相對較高的低值流量。
severity	選取嚴重性等級（**Critical**（關鍵）、**High**（高）、**Medium**（中）、**Low**（低）或**Informational**（資訊性））。
特徵碼例外狀況頁籤 可讓您針對特定特徵碼變更動作。例如，您可針對特定特徵碼集產生警示，並封鎖符合所有其他特徵碼的所有封包。威脅例外狀況通常是在發生誤判時設定。若要簡化威脅例外狀況的管理，可以直接從 **Monitor**（監控）> **Logs**（日誌）> **Threat**（威脅）清單新增威脅例外狀況。請確保您取得最新的內容更新，以保護您不受新威脅影響且具備任何誤判的新特徵碼。	
例外狀況	**Enable**（啟用）您要為其指派動作的每個威脅，或選取 **All**（全部）來回應所有列出的威脅。清單取決於所選主機、類別與嚴重性。如果清單為空，表示目前選取內容沒有威脅。 使用「IP 位址豁免」以將 IP 位址篩選器新增至威脅例外狀況中。若將 IP 位址新增至威脅例外狀況中，則只有在來源或目的地 IP 位址符合例外狀況中 IP 位址的

© 2019 Palo Alto Networks, Inc.

反間諜軟體設定檔設定	說明
	工作階段觸發特徵碼時，該特徵碼的威脅例外動作才會取代規則的動作。各個特徵碼最多可新增 100 個 IP 位址。使用此選項後，便不需要建立新的原則規則和新的弱點設定檔來建立特定 IP 位址的例外。 僅當您確定識別為間諜軟體的特徵碼不是威脅時，才會建立例外情況（這是誤報）。若您認為自己發現了誤報，請使用 *TAC* 開啟支援案例，以便 *Palo Alto Networks* 可以分析並修正錯誤識別的特徵碼。問題解決後，即會從設定檔中移除該例外情況。
DNS 政策頁籤 **DNS Policies**（**DNS** 政策）設定也可用來識別網路上受感染的主機。這些特徵碼將偵測特定 DNS 查詢，找出與 DNS 威脅相關聯的主機名稱。	
您可以使用單獨的政策動作、日誌嚴重性層級和封包擷取設定，來設定特定的 DNS 特徵碼來源。對於惡意軟體網域執行 DNS 查詢的主機將出現在殭屍網路報告中。此外，若您要抓捕惡意軟體 DNS 查詢，則可以在 **DNS Sinkhole Settings**（**DNS Sinkhole** 設定）中指定 Sinkhole IP。	
DNS 特徵碼來源	允許您選取您在發生 DNS 查詢時要強制執行動作的清單。有兩個預設的 DNS 特徵碼原則選項： • **Palo Alto Networks Content**（**Palo Alto Networks** 內容）—透過動態內容更新來進行更新的本機可下載特徵碼清單。 • **DNS Security**（**DNS** 安全性）—雲端型 DNS 安全性服務，可主動分析 DNS 資料，並提供對完整 Palo Alto Networks DNS 特徵碼資料庫的即時存取權限。 除威脅防禦授權外，此服務還需要購買和啟動 *DNS* 安全性授權。 • **External Dynamic Lists**（外部動態清單）—已建立的動態網域清單可用於根據清單類型（例如，允許清單）強制執行特定動作。依預設，網域清單的政策動作被設定為 **Allow**（允許）並優先於所有其他特徵碼類型。 除威脅防禦授權外，此服務還需要購買和啟動 *DNS* 安全性授權。 預設會抓捕本機存取的 Palo Alto Networks 內容 DNS 特徵碼，而雲端 DNS 安全性設定為允許。如果要使用 DNS 安全性啟用 sinkholing，則必須將 DNS 查詢的動作設定為「抓捕」。用於抓捕的預設位址屬於 Palo Alto Networks (sinkhole.paloaltonetworks.com)。此位址不是靜態的，並且可透過防火牆或 Panorama 上的內容更新進行修改。 **Add**（新增）清單，並選取您已建立類型網域的外部動態清單。若要建立新的清單，請參閱 [物件 > 外部動態清單]。
日誌嚴重性	允許您指定防火牆偵測到與 DNS 特徵碼相符的網域時記錄的日誌嚴重性層級。
政策動作	選取對於已知的惡意軟體網站進行 DNS 查詢時採取的動作。選項包括 **alert**（警示）、**allow**（允許）、**block**（封鎖）或 **sinkhole**（抓捕）。Palo Alto Networks DNS 特徵碼的預設動作為 **sinkhole**（抓捕）。 管理員可使用 DNS Sinkhole 動作所提供的方法，識別網路上使用 DNS 流量的受感染主機，即使當防火牆位於本機 DNS 伺服器北方亦然（例如，防火牆看不到 DNS 查詢的傳送者）。安裝威脅防禦授權，並在安全性設定檔中啟用反間諜

© 2019 Palo Alto Networks, Inc.

反間諜軟體設定檔設定	說明
	軟體設定檔時，將在惡意軟體網域導向的 DNS 查詢上觸發 DNS 型特徵碼。在防火牆位於本機 DNS 伺服器北邊的一般部署中，威脅日誌會將本機 DNS 解析程式識別成流量來源，而非實際的受感染主機。Sinkholing 惡意軟體 DNS 查詢可解決此可見性問題，方法是偽裝回應惡意網域上導向的查詢，使得用戶端嘗試連線至惡意網域（例如，指令與控制項），而非嘗試連線到管理員所指定的 IP 位址。接著可在流量日誌中輕易識別受感染的主機，因為嘗試連線至 sinkhole IP 的任何主機最可能受惡意軟體受影。 在防火牆看不到 *DNS* 查詢的發起者時（通常在防火牆位於本機 *DNS* 伺服器的北邊時）啟用 *DNS sinkhole*，這樣您可以找出遭到感染的主機。若您無法抓捕流量，則將其封鎖。
封包擷取	如果您要擷取已識別的封包，請為給定的來源選取此選項。 在遭抓捕的流量上啟用封包擷取，以便您可以對其進行分析並獲取有關受感染主機的資訊。
DNS Sinkhole 設定	為 DNS 特徵碼來源定義抓捕動作後，指定將用於抓捕的 IPv4 及 / 或 IPv6 位址。依預設，Sinkhole IP 位址設定為 Palo Alto Networks 伺服器。您接著可使用流量日誌，或建立篩選 Sinkhole IP 位址的自訂報告及識別受感染的用戶端。 以下是抓捕 DNS 要求後將發生的事件順序： 受感染的用戶端電腦上的惡意軟體將傳送 DNS 查詢，以解析網際網路上的惡意主機。 用戶端的 DNS 查詢將傳送至內部 DNS 伺服器，接著查詢防火牆另一端的公共 DNS 伺服器。 DNS 查詢符合指定 DNS 特徵碼資料庫來源中的 DNS 項目，因此將在查詢時執行抓捕動作。 受感染的用戶端接著嘗試使用主機啟動工作階段，但改用偽造的 IP 位址。選取 sinkhole 動作時，偽造的 IP 位址是反間諜軟體設定檔 [DNS 特徵碼] 頁籤中所定義的位址。 管理員在威脅日誌中收到惡意 DNS 查詢警示，然後搜尋流量日誌來尋找 sinkhole IP 位址，並且可輕易找到正在嘗試使用 sinkhole IP 位址啟動工作階段的用戶端 IP 位址。
DNS 例外狀況頁籤 DNS 特徵碼例外狀況允許您從政策實施中排除特定的威脅 ID，並為核准的網域來源指定網域/FQDN 允許清單。 若要新增要從原則排除的特定威脅，請選取或搜尋 **Threat Id**（威脅 **ID**），然後按一下 **Enable**（啟用）。每個項目提供物件的威脅內容（**Threat ID**（威脅 **ID**）、**Name**（名稱）和 **FQDN**。 若要 **Add**（新增）網域或 FQDN 允許清單，請提供允許清單的位置及適當的說明。	

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Vulnerability Protection（物件 > 安全性設定檔 > 漏洞保護）

安全性原則規則可以包含弱點保護設定檔的規格，它可決定避免緩衝區溢位、不合法程式碼執行及其他利用系統弱點之嘗試的保護等級。弱點保護功能有兩個可用的預先定義設定檔：

- **Default**（預設值）設定檔可將預設動作套用至所有用戶端與伺服器的重要、高與中等嚴重性弱點。它不會偵測低和資訊弱點保護事件。裝置上的 Palo Alto Networks 內容套件確定預設動作。
- 嚴格設定檔可將封鎖回應套用至所有用戶端與伺服器的重要、高與中等嚴重性間諜軟體事件，並針對低和資訊漏洞保護事件使用預設動作。

自訂設定檔可以用來最小化受信任安全性區域之間流量的弱點檢查，及最大化從不受信任區域（例如網際網路）中收到的流量以及傳送至高機敏目的地（例如伺服器群）的流量的保護。若要將弱點保護設定檔套用至安全性原則，請參考 [原則 > 安全性]。

將漏洞保護設定檔應用至所有允許流量的安全性原則規則，以防禦緩衝區溢位、非法程式碼執行及其他嘗試利用用戶端及伺服器端漏洞的行為。

[規則] 設定指定要啟用的特徵碼集合，以及觸發集合內的特徵碼時要採取的動作。

例外狀況設定可讓您將回應變更為特定特徵碼。例如，除了選取的例外狀況外，您可以封鎖所有符合特徵碼的封包，選取的例外狀況會產生警示。**Exception**（例外狀況）頁籤支援篩選功能。

Vulnerability Protection（漏洞保護）頁面有一組預設欄。其他資訊欄可利用直欄選取器顯示。按一下欄標題右側的箭頭，從 [欄] 子功能表選取欄。

下表說明弱點保護設定檔設定：

弱點保護設定檔設定	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在弱點保護設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號、句點與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此弱點保護設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
規則頁籤	

© 2019 Palo Alto Networks, Inc.

弱點保護設定檔設定	說明
規則名稱	指定用來識別規則的名稱。
威脅名稱	指定要比對的文字字串。防火牆會搜尋此文字字串的特徵碼名稱，將特徵碼集合套用到規則。
CVE	如果您要將特徵碼限制為也符合指定 CVE 的特徵碼，請指定一般漏洞與曝露點 (CVE)。 每個 CVE 的格式為 CVE-yyyy-xxxx，其中的 yyyy 是年份，xxxx 是唯一識別碼。您可以執行與此欄位有關的字串比對。例如，若要尋找 2011 年的弱點，請輸入「2011」。
主機類型	指定是否將規則的特徵碼限制為用戶端那側、伺服器那側或其中之一（**Any**（任何））的特徵碼。
severity	如果您要將特徵碼限制為也符合指定嚴重性， 請指定要符合的嚴重性（**Informational**（資訊性）、**Low**（低）、**Medium**（中）、**High**（高）或**Critical**（關鍵））。
動作	選取觸發規則時要採取的動作。如需動作清單，請參閱安全性設定檔中的動作。 **Default**（預設）動作是依據 Palo Alto Networks 提供的各個特徵碼中預先定義的動作。若要檢視特徵碼的預設動作，請選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **Vulnerability Protection**（弱點保護）和 **Add**（新增）或選取現有設定檔。按一下 **Exceptions**（例外狀況）頁籤，然後按一下 **Show all signatures**（顯示所有特徵碼），即可看見所有特徵碼的清單和相關聯的 **Action**（動作）。 為了獲得最佳安全性，請將用戶端和伺服器的重大、高和中嚴重性事件的操作設定為 *reset-both*（重設用戶端與伺服器）並同時使用資訊和低嚴重性事件的預設動作。
封包擷取	如果您要擷取已識別的封包，請選取此選項。 選取 **single-packet**（單一封包）可在偵測到威脅時擷取一個封包，或選取 **extended-capture**（延伸擷取）選項來擷取 1 到 50 個封包（預設值為 5 個封包）。延伸擷取會在分析威脅日誌時提供更多的威脅內容。若要檢視封包擷取，請選取 **Monitor**（監控）> **Logs**（日誌）> **Threat**（威脅）並尋找您所要的日誌項目，然後按一下第二欄中的綠色箭頭。若要定義必須擷取的封包數目，請選取 **Device**（裝置）> **Setup**（設定）> **Content-ID**（內容-ID），然後編輯內容-ID 設定。 如果對給定威脅的動作為允許，則防火牆不會觸發威脅日誌，且不會擷取封包。如果動作為警示，您可以將封包擷取設定為單一封包或延伸擷取。所有封鎖動作（丟棄、封鎖和重設動作）都會擷取單一封包。裝置上的內容套件確定預設動作。 對極其、較高及適中嚴重性事件啟用延伸擷取，為低嚴重性事件啟用單一封包擷取。使用 *5* 個封包的預設延伸擷取值，可提供足夠的資訊來分析大多數情況下的威脅。（過多的封包擷取流量可能會導致丟棄封包擷取。）請勿為資訊性事件啟用封包擷取，因為比起擷取更高嚴重性事件的資訊，它不是非常有用，並且會建立相對大量的低數值流量。

© 2019 Palo Alto Networks, Inc.

弱點保護設定檔設定	說明
	使用相同的邏輯應用延伸封包擷取以決定記錄哪些流量—採用您記錄的流量的延伸封包擷取，包含您封鎖的流量。
Exceptions 頁籤	
啟用	針對您要為其指定動作的每個威脅選取 **Enable**（啟用）核取方塊，或選取 **All**（全部）來回應所有列出的威脅。清單取決於所選主機、類別與嚴重性。如果清單為空，表示目前選取內容沒有威脅。
ID	
廠商 ID	如果您要將特徵碼限制為也符合指定廠商 ID 的特徵碼，請指定廠商 ID。 例如，Microsoft 協力廠商 ID 的格式是 MSyy-xxx，其中的 yy 是兩位數的年份，xxx 是唯一識別碼。例如，若要比對 2009 年的 Microsoft 協力廠商，請在搜尋欄輸入「MS09」。
威脅名稱	請僅在您確定識別的威脅不是威脅時（誤報）建立威脅特例。如果您認為您發現了誤報，請使用 *TAC* 開啟支援案例，以便 *Palo Alto Networks* 可以調查錯誤識別的威脅。問題解決後，立即從設定檔中移除該例外。 弱點特徵碼資料庫包含指出暴力密碼破解攻擊的特徵碼；例如在 FTP 暴力密碼破解攻擊時會觸發威脅 ID 40001。當在某時間臨界值發生情況時，暴力密碼破解特徵碼會觸發。針對暴力密碼破解特徵碼，會預先設定臨界值，並且可以按一下 **Vulnerability**（漏洞）頁籤（在已選取 **Custom**（自訂）選項的情況下）上威脅名稱旁邊的編輯（ ），來變更該臨界值。您可以指定每個時間單位的相符次數，以及是否將該臨界值套用至來源、目的地或來源與目的地。 臨界值可以套用至來源 IP、目的地 IP 或來源 IP 與目的地 IP 的組合。 預設動作顯示在括號中。
IP 位址例外狀況	按一下 **IP Address Exemptions**（**IP** 位址豁免）欄，將 IP 位址篩選器 **Add**（新增）至威脅例外狀況中。當您將 IP 位址新增至威脅例外狀況中，只有在來源或目的地 IP 位址符合例外狀況中 IP 位址的工作階段觸發特徵碼時，該特徵碼的威脅例外動作才會優先於規則的動作。各個特徵碼最多可新增 100 個 IP 位址。您必須輸入單點傳播 IP 位址（也就是，沒有網路遮罩的位址），例如 10.1.7.8 或 2001:db8:123:1::1。新增 IP 位址豁免，便不需要建立新的原則規則和新的弱點設定檔來建立特定 IP 位址的例外狀況。
rule	
CVE	**CVE** 欄顯示通用弱點與曝露點 (CVE) 的識別碼。這些唯一且通用的識別碼適用於公開已知的資訊安全性弱點。
主機型	
類別	如果您要將特徵碼限制為符合該類別的特徵碼，選取漏洞類別。
severity	

© 2019 Palo Alto Networks, Inc.

弱點保護設定檔設定	說明
動作	從下拉式清單中選取動作，或從清單頂部的 **Action**（動作）下拉式清單中選取，以將相同動作套用至所有威脅。
封包擷取	如果您要擷取已識別的封包，請選取 **Packet Capture**（封包擷取）。
顯示所有特徵碼	啟用 **Show all signatures**（顯示所有特徵碼）以列出所有特徵碼。如果停用 **Show all signatures**（顯示所有特徵碼），則只會列示例外狀況特徵碼。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > URL Filtering（物件 > 安全性設定檔 > URL 篩選）

您可使用 URL filtering（URL 篩選）設定檔，不僅可控制對網頁內容的存取，還可控制使用者與網頁內容的互動方式。

您想了解什麼內容？	請參閱：
根據 URL 類別控制網站的存取權。	URL 篩選類別
偵測企業認證提交，然後決定使用者可以提交認證的 URL 類別。	使用者認證偵測 URL 篩選類別
若一般使用者未使用最嚴格的安全搜尋設定，則封鎖搜尋結果。	URL 篩選設定
啟用 HTTP 標頭的記錄。	URL 篩選設定
使用自訂 HTTP 標頭控管網站的存取。	HTTP 標頭插入
啟用內嵌 ML 即時分析網頁以確定其是否包含惡意內容。	URL 篩選內嵌 ML
想知道更多？	• 進一步瞭解如何設定 URL 篩選。 • 使用 URL 類別以防範認證網路釣魚。 • 若要建立自訂 URL 類別，請選取 Objects > Custom Objects > URL Category（物件 > 自訂物件 > URL 類別）。 • 若要匯入希望強制執行的 URL 清單，請選取Objects > External Dynamic Lists（物件 > 外部動態清單）。

URL 篩選一般設定

下表說明一般 URL 篩選設定。

一般設定	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性政策時，此名稱會顯示在 URL 篩選設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
共享	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。

© 2019 Palo Alto Networks, Inc.

一般設定	說明
	• Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此設定檔的設備群組中覆寫此 URL 篩選設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。

URL 篩選類別

選取 **Objects**（物件）> **Security Profiles**（安全設定檔）> **URL Filtering**（**URL** 篩選）> **Categories**（類別）以依據 URL 類別控管網站的存取。

類別設定	說明
類別	顯示可以為其定義網路存取與使用原則的 URL 類別與清單。依預設，所有類別的 **Site Access**（網站存取）和 **User Credential Submission**（使用者認證提交）權限設定為 **Allow**（允許）。 URL 類別與清單分組為三個下拉式清單： • **Custom URL Categories**（自訂 **URL** 類別）—選取 Objects > Custom Objects > URL Category（物件 > 自訂物件 > URL 類別）以定義自訂 URL 類別。您可將自訂 URL 類別基於 URL 清單或多個預先定義的類別。 • **External Dynamic URL Lists**（外部動態 **URL** 清單）— 選取 Objects > External Dynamic Lists（物件 > 外部動態清單），可啟用防火牆以從 Web 伺服器匯入 URL 清單。 • **Pre-defined Categories**（預先定義的類別）—列出按 PAN-DB、Palo Alto Networks URL 與 IP 雲端資料庫定義的所有 URL 類別。 *Block*（封鎖）所有已知危險的 *URL* 類別，以防漏洞滲透、惡意軟體下載、命令和控制活動以及資料洩漏：*command-and-control*（命令和控制）、*copyright-infringement*（侵犯著作權）、*dynamic-dns*（動態 *DNS*）、*extremism*（極端）、*malware*（惡意軟體）、*phishing*（網路釣魚）、*proxy-avoidance-and-anonymizers*（代理程式規避與匿名者）、*unknown*（未知）、*newly-registered-domain*（新註冊的網域）、*grayware*（灰色軟體）與 *parked*（暫止）。 若要逐步採用封鎖原則，請設定類別以 *continue*（繼續）並建立自訂回應頁面，向使用者講授您的使用原則並警示他們造訪的網站可能造成威脅。經過一段適當的時間後，轉換為封鎖這些潛在惡意網站的原則。
網站存取	針對每個 URL 類別，選取要在使用者嘗試於該類別存取 URL 時所採取的動作： • 警示 — 允許存取網站，但是每次使用者存取 URL 時，會將警示新增至 URL 日誌。 將 *alert*（警示）設定為您未封鎖之流量類別的「動作」，以便記錄存取嘗試並檢視流量。 • 允許 — 允許存取網站。

© 2019 Palo Alto Networks, Inc.

類別設定	說明
	由於 *allow*（允許）不記錄未封鎖的流量，因此如果要記錄存取嘗試並檢視該流量，請將 *alert*（警示）設定為您未封鎖之流量類別的「動作」。 • **block**（封鎖）—封鎖對網站的存取。若對 URL 類別的網站存取設定為封鎖，則使用者認證提交權限也會自動設定為封鎖。 • **continue**（繼續）—向使用者顯示警告頁面，阻止他們存取網站。若使用者決定忽略警告，則其必須選取 **Continue**（繼續）該網站。 繼續（警告）頁面在設定使用代理程式伺服器的用戶端電腦上未正確顯示。 • **override**（覆寫）—顯示回應頁面，提示使用者輸入有效密碼以獲得對網站的存取權。進行 URL 管理員取代設定（**Device**（裝置）> **Setup**（設定）> **Content ID**），以管理密碼及其他取代設定。（也請在 [裝置 > 設定 > Content-ID] 參閱 [管理設定] 表）。 覆寫頁面在設定使用代理程式伺服器的用戶端電腦上未正確顯示。 • **None**（無）（僅限自訂 URL 類別）—如果您已建立自訂 URL 類別，則將動作設定為 **None**（無），以允許防火牆從 URL 資料庫廠商繼承 URL 篩選類別指派。將動作設定為 **None**（無）可讓您靈活略過 URL 篩選設定檔中的自訂類別，同時允許您將自訂 URL 類別用作原則規則（安全性、解密及 QoS）中的比對準則，以設定例外狀況或強制執行不同動作。若要刪除 URL 類別，您必須在使用自訂類別的任何設定檔中，將動作設定為 **None**（無）。如需自訂 URL 類別的詳細資訊，請參閱 [物件 > 自訂物件 > URL 類別]。
使用者認證提交	針對每個 URL 類別，選取 **User Credential Submissions**（使用者認證提交）以允許或不允許使用者在該類別中將有效公司認證提交至 URL。在您可以基於 URL 類別控制使用者認證提交前，您必須啟用認證提交偵測（選取 **User Credential Detection**（使用者認證偵測）頁籤）。 **Site Access**（網站存取）設定為封鎖的 URL 類別會自動設定為也封鎖使用者認證提交。 • **alert**（警示）—允許使用者將認證提交至網站，但每次在使用者將認證提交至此類別中的網站時產生 URL 篩選日誌。 • **allow**（允許）（預設值）—允許使用者將認證提交至網站。 • **block**（封鎖）—封鎖使用者將認證提交至網站。預設的防網路釣魚回應頁面會封鎖使用者認證提交。 • **Continue**（繼續）—對使用者顯示回應頁面，提示他們選取 **Continue**（繼續）以便將認證提交至網站。依預設，當使用者嘗試將認證提交至系統不鼓勵認證提交的網站時，會顯示防網路釣魚繼續頁面以警告使用者。您可選取建立自訂回應頁面以警告使用者當心網路釣魚嘗試，或對他們宣導勿在其他網站上重新使用有效的公司認證。
檢查 URL 類別	按一下此項目可存取 PAN-DB URL 篩選資料庫，您可以在此輸入 URL 或 IP 位址以檢視分類資訊。
動態 URL 篩選（預設為停用）	選取可啟用雲端查詢以分類 URL。如果本機資料庫無法分類 URL，則會叫用此選項。

© 2019 Palo Alto Networks, Inc.

類別設定	說明
（僅可針對 BrightCloud 設定）	若在 5 秒逾時之後仍未解析 URL，會將回應顯示成 `Not resolved URL`（未解析 `URL`）。 使用 *PAN-DB* 時，此選項預設為啟用，但無法設定。

URL 篩選設定

選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）> **URL Filtering Settings**（**URL** 篩選設定）以強化安全搜尋設定，並啟用 HTTP 標頭日誌記錄。

URL 篩選設定	說明
僅記錄容器頁面 預設值：已啟用	選取此選項可僅記錄符合指定內容類型的 URL。防火牆在工作階段期間不會記錄相關的網路連結，例如廣告和內容連結，這樣可以在記錄相關 URL 時減少日誌記錄和記憶體負載。 如果您使用遮罩來源原始 *IP* 位址的代理，請啟用 HTTP 標頭記錄 *X-Forwarded-For* 選項以保留發起網頁請求的使用者的原始 *IP* 位址。
啟用安全搜尋強制執行 預設值：已停用 使用此功能無需 URL 篩選授權。	選取此選項可強制執行嚴格的安全搜尋篩選。 許多搜尋引擎都有安全搜尋設定，可將搜尋查詢傳回流量中的成人影像與視訊篩選掉。當您選取設定以啟用安全搜尋強制執行，那麼若一般使用者未在搜尋查詢中使用最嚴格的安全搜尋設定時，防火牆便會封鎖搜尋結果。防火牆會針對下列搜尋供應商強制執行安全搜尋：Google、Yahoo、Bing、Yandex 及 YouTube。此設定只能盡力防止，搜尋供應商無法保證對於每個網站都有效。 若要使用安全搜尋強制執行，您必須啟用此設定，然後附加 URL 篩選設定檔安全性原則規則。接著防火牆會封鎖任何符合但未使用最嚴格安全搜尋設定搜尋查詢傳回流量。 如果您在登入 *Yahoo* 時想要在 *Yahoo Japan (yahoo.co.jp)* 上執行搜尋，也必須啟用搜尋設定的鎖定選項。 若要防止使用者使用其他搜尋供應商來略過此功能，可設定 *URL* 篩選設定檔來封鎖搜尋引擎類別，然後允許 *Bing*、*Google*、*Yahoo*、*Yandex* 和 *YouTube* 的存取。
HTTP 標頭記錄	啟用 [HTTP 標頭記錄] 可深入檢視傳送至伺服器的 HTTP 要求所包含的屬性。啟用下列一或多個屬性-值配對時，會在 URL 篩選日誌中加以記錄： • User-Agent—使用者用來存取 URL 的 Web 瀏覽器。此資訊是在 HTTP 要求中傳送給伺服器。例如，User-Agent 可為 Internet Explorer 或 Firefox。日誌中的 User-Agent 值最多支援 1024 個字元。 • Referer—網頁的 URL，可將使用者連結至其他網頁；它是將使用者重新導向（轉介）至正在要求之網頁的來源。日誌中的 Referer 值最多支援 256 個字元。

© 2019 Palo Alto Networks, Inc.

URL 篩選設定	說明
	• X-Forwarded-For—標頭欄位選項，用來保留要求網頁之使用者的 IP 位址。它能讓您識別使用者的 IP 位址，這項功能特別適用於當您在網路上具有 Proxy 伺服器，或您已實作來源 NAT 而遮罩了使用者的 IP 位址，使得所有要求看似源自於 Proxy 伺服器的 IP 位址或一般 IP 位址時。日誌中的 X 轉送針對值最多支援 128 個字元。

使用者認證偵測

選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）> **User Credential Detection**（使用者認證偵測）以在使用者提交公司認證時，啟動防火牆偵測。

設定使用者認證偵測，以便使用者只能向指定的 *URL* 類別中的網站提交認證，從而通過防止認證提交給不受信任類別的網站來減少攻擊面向。如果您針對使用者認證提交封鎖 *URL* 篩選設定檔中所有的 *URL* 類別，則無需檢查認證。

防火牆使用三個方法之一偵測提交到網頁的有效認證。各個方法都需要 User-ID™，這可讓防火牆針對有效的公司認證比較提交到網頁的使用者名稱和密碼。請選取這些方法之一，然後根據 URL 類別繼續防範認證釣魚。

必須設定防火牆以解密要監控監控認證的流量。

使用者認證偵測設定	說明
IP 使用者	此認證偵測方法可檢查有效的使用者名稱提交。您可使用此方法來偵測包含有效公司使用者名稱的認證提交（不論伴隨的密碼為何）。防火牆會決定使用者名稱比對的方式，是藉由驗證使用者名稱符合登入至工作階段來源 IP 位址的使用者。為使用此方法，防火牆會針對 IP 位址到使用者名稱的對應表比對使用者所提交的使用者名稱。為使用此方法，您可使用將 IP 位址對應至使用者中所述的任何使用者對應方法。
群組對應	防火牆會決定使用者提交到受限制網站的使用者名稱，是否符合任何有效的公司使用者名稱。為進行這項決定，防火牆會將提交的使用者名稱與使用者到群組對應表中的使用者名稱清單比對，以便偵測使用者何時將公司使用者名稱提交到屬於受限制類別的網站中。 此方法僅會根據 LDAP 群組成員資格檢查公司使用者名稱提交，這使得該方法易於設定，但較易有誤判。您必須啟用群組對應 以便使用此方法。
網域認證	此認證偵測方法可讓防火牆檢查有效的公司使用者名稱和相關聯的密碼。防火牆會決定使用者提交的使用者名稱和密碼，是否符合相同使用者的公司使用者名稱和密碼。 為進行此決定，防火牆必須能夠將認證提交與效的公司使用者名稱和密碼比對，並驗證使用者所提交的使用者名稱對應至已登入使用者的 IP 位址。使用基於 Windows 的 User-ID 代理程式時才支援此模式，且需要 User-ID 代理程式已安裝於唯讀網域控制器 (RODC)，並已裝備 User-ID 認證服務附加元件。為使用此方法，您必須讓 User-ID 將 IP 位址對應至使用者，具體方法為使用任何受支援的使用者對應方法，包含驗證政策、驗證入口網站和 GlobalProtect™。

© 2019 Palo Alto Networks, Inc.

使用者認證偵測設定	說明
	關於防火牆可用於檢查有效的公司認證提交的各個方法、啟用釣魚防範的步驟，請參閱防範認證釣魚 以獲得詳細資訊。
偵測到有效使用者名稱的日誌安全性	設定日誌的嚴重性，該日誌會指出防火牆已偵測到提交至網站的有效使用者名稱。 此日誌嚴重性相關聯於以下事件：有效的使用者名稱已提交至網站，且網站的認證提交權限有警示、封鎖或繼續。記錄日誌的時機，是當使用者將有效的使用者名稱提交至網站，且受允許的認證提交的嚴重性為資訊性。選取 **Categories**（類別）以檢閱或調整 URL 類別，受允許與封鎖的認證提交是對此 URL 類別進行。 將記錄嚴重性設定為適中或較強。

HTTP 標頭插入

若要透過將 HTTP 標頭與其值插入到 HTTP 請求中來允許防火牆管理網路應用程式存取，請選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）> **HTTP Header Insertion**（**HTTP** 標頭插入）

防火牆僅針對 *HTTP/1.x* 流量支援標頭插入；對於 *HTTP/2* 流量，防火牆不支援標頭插入。

您可以依據預定義的 HTTP 標頭插入類型建立插入項目，或建立自訂類型。一般以自訂 HTTP 標頭執行標頭插入，但您也可以插入標準 HTTP 標頭。

當發生以下狀況時會進行標頭插入：

1. HTTP 請求以一個或多個設定的 HTTP 標頭插入項目比對安全性政策規則。
2. 特定網域符合在 HTTP Host 標頭中所找到的網域。
3. 該動作不會是 `Block`（封鎖）。

防火牆僅可以執行*GET*、*POST*、*PUT*、*HEAD* 的 *HTTP* 標頭插入。

如果您啟用 HTTP 標頭插入，而定義的標頭卻缺少請求，則防火牆會插入此標頭。如果定義的標頭已存在請求中，那麼防火牆會以您指定的值覆寫標頭的值。

Add（新增）一個插入項目或選取現有插入項目進行修改。在必要時，您也可以選取一個插入項目然後 **Delete**（刪除）它。

新 *HTTP* 標頭插入項目的預設封鎖清單動作為封鎖。如果您想要進行不同的動作，請前往URL 篩選類別並選取適當的動作。或者，將此插入項目新增至以希望動作設定的設定檔中。

HTTP 標頭插入設定	說明
名稱	HTTP 標頭插入項目的 **Name**（名稱）。
類型	您想要建立的項目 **Type**（類型）。項目可為預定義或自訂。防火牆使用內容更新來填寫和維護預定義項目。 若要將使用者名稱包括在 HTTP 標頭中，請選取 **Dynamic Fields**（動態欄位）。

© 2019 Palo Alto Networks, Inc.

HTTP 標頭插入設定	說明
網域	當此列表中的網域與 HTTP 請求的主機標頭相匹配時，會產生標頭插入。 如果您正在建立預定義項目，會在內容更新中預定義網域清單。這對大部分用例而言已足夠，但您可以在必要時新增或刪除網域。 若要建立自訂項目，請 **Add**（新增）至少一個網域到清單中。 每個網域名稱最多可以到 256 字元，且每個項目最多可定義 50 個網域。可以使用星號 (*) 作為萬用字元，它會符合指定網域中的任何要求（例如，*.etrade.com）。
標頭	當您建立預定義項目時，標頭清單會透過內容更新預先填入。這對大部分用例而言已足夠，但您可以在必要時新增或刪除標頭。 當您建立一個自訂項目時，新增一個或多個標頭（總數最多為 5）到此清單中。 標頭名稱最多可以到 100 字元，但不包含空格。 若要將使用者名稱包括在 HTTP 標頭中，請選取 **X-Authenticated-User**（擴展驗證使用者），然後選取 **Value**（值），或者 **Add**（新增）新的標頭。
值	最多使用 512 個字元設定 **Value**（值）。標頭值因您要包括在指定網域的 HTTP 標頭中的資訊而異。例如，透過選取預定義類型或透過使用自訂項目管理使用者對 SaaS 應用程式的存取權限。 若要將使用者名稱包括在 HTTP 標頭中，請選取安全裝置需要的網域和使用者名稱格式： • `($domain)\($user)` • `WinNT://($domain)/($user)` 或者，使用 `($user)` 和 `($domain)` 動態語彙基元輸入自訂格式（例如，`($user)@($domain)`）。 防火牆使用群組對應設定檔中的主要使用者名稱填入 user 和 domain 動態語彙基元。 每個值僅使用一次 *`($user)`* 和 *`($domain)`* 動態語彙基元。
日誌	選取 **Log**（日誌）以啟用此標頭插入項目的日誌。

URL 篩選內嵌 ML

選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（URL 篩選）> **Inline ML**（內嵌 **ML**），以使用以防火牆為基礎的機器學習模型來啟用和設定網頁的即時分析。

欄位	說明
使用 **Inline ML**（內嵌 **ML**）頁籤，以啟用和設定政策動作。	
可用模型	針對每個可用的內嵌 ML 模型，您可以選取以下動作之一： • **Alert**（警示）—允許網站，並在 URL 篩選日誌中產生日誌項目。 • **Allow**（允許）—允許網站，不產生日誌項目。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	• **Block**（封鎖）—封鎖網站，使用者將無法繼續存取網站。在 URL 篩選日誌中會產生日誌項目。
例外狀況	您可以為不想分析的特定網站定義 URL **Exceptions**（例外狀況），例如那些可能觸發誤判的網站。 若要新增 URL 例外狀況，必須首先定義一個有效的 EDL（外部動態清單）或自訂 URL 類別。按一下 **Add**（新增）以檢視可用選項並從中選取。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > File Blocking（物件 > 安全性設定檔 > 檔案封鎖）

您可以將檔案封鎖設定檔附加至安全性原則規則（原則 > 安全性），以封鎖使用者上傳或下載指定的檔案類型，或在使用者嘗試上傳或下載指定的檔案類型時產生警示。

為獲得最佳安全性，請應用預定義的*strict*（嚴格）設定檔。如果您需要支援使用被*strict*（嚴格）設定檔封鎖的檔案類型的重要應用程式，請複製*strict*（嚴格）設定檔並僅使您需要的檔案類型成為例外。將複製的設定檔應用於安全性原則規則，該規則將例外限制為僅需要使用檔案類型的來源、目標和使用者。您也可以使用 *Direction*（方向）將例外限制在上傳或下載。

如果您不封鎖所有 *Windows PE* 檔案，則須向 *WildFire* 傳送所有未知檔案進行分析。對於使用者帳戶，請將動作設定為 *continue*（繼續）以幫助防止路過式下載，路過式下載是指惡意網站、電子郵件或快顯視窗讓使用者在無意中下載惡意檔案的行為。告訴使用者，對於在其不知情的情況下進行的檔案傳輸，如果出現繼續提示，則表示其可能在下載惡意檔案。

下表說明檔案封鎖設定檔設定。

檔案封鎖設定檔設定	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在檔案封鎖設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此檔案封鎖設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
規則	定義一或多個規則，以針對所選檔案類型指定要採取的動作（如果有）。若要新增規則，請指定下列項目並按一下 **Add**（新增）： • 名稱—輸入規則名稱（最多 31 個字元）。 • 應用程式—選取規則適用的應用程式或選取 **Any**（任何）。 • 檔案類型 — 按一下檔案類型欄位，然後按一下 **Add**（新增）可檢視支援的檔案類型清單。按一下檔案類型可將其新增至設定檔，視需繼續新增其他檔案類型。若您選取 **Any**（任何），則對所有支援的檔案類型採取定義的動作。 • 方向 — 選取檔案傳輸的方向（上傳、下載或兩者）。 • 動作 — 選取當偵測到所選檔案類型時所採取的動作： • 警示—新增項目到威脅日誌。

© 2019 Palo Alto Networks, Inc.

檔案封鎖設定檔設定	說明
	• 繼續 — 向使用者顯示訊息，指示已要求下載，並要求使用者確認是否繼續。目的是為了警告使用者可能是未知下載（也稱為路過式下載），並讓使用者選取繼續還是停止下載。 以 **continue**（繼續）動作建立檔案封鎖設定檔時，您只能選取應用程式 **web-browsing**（網頁瀏覽）。如果您選取其他任何應用程式，符合安全性原則規則的流量將不通過防火牆，因為將不以繼續頁面提示使用者。 • 封鎖—檔案會遭到封鎖。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > WildFire Analysis（物件 > 安全性設定檔 > WildFire 分析）

使用 WildFire 分析設定檔來指定要在 WildFire 裝置本機上或 WildFire 雲端上執行的 WildFire 檔案分析。您可根據檔案類型、應用程式或檔案傳輸方向（上傳或下載）指定流量要轉送至公共雲端或私人雲端。建立 WildFire 分析設定檔之後，將設定檔新增至原則（**Policies**（原則）> **Security**（安全性）），可讓您進一步將設定檔設定套用至符合該原則的任何流量（例如在原則中定義的 URL 類別）。

使用預先定義的預設設定檔將所有未知檔案轉送至 WildFire 進行分析。此外，設定 WildFire 裝置內容更新以下載和每分鐘安裝，因此您一直能得到最新的支援。

WildFire 分析設定檔設定	
名稱	針對 WildFire 分析設定檔輸入描述名稱（最多 31 個字元）。此名稱會顯示於您在定義安全性原則規則時可選取的 WildFire 分析設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	選取性說明設定檔規則或設定檔的預定用途（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此弱點保護設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
規則	定義一或多個規則以指定流量轉送至 WildFire 公共雲端或 WildFire 裝置（私人雲端）以進行分析。 • 針對您新增至設定檔的任何規則輸入描述 **Name**(名稱)（最多 31 個字元）。 • 新增 **Application**（應用程式）以讓任何應用程式流量根據規則比對並轉送至指定的分析目的地。 • 針對規則選取要在已定義分析目的地分析的 **File Type**（檔案類型）。 *WildFire 私有雲（由 WildFire 裝置託管）不支援 APK、Mac OS X、 檔案夾和 linux 檔案的分析。* • 取決於傳輸方向，將規則套用至流量。您可將規則套用至上傳流量、下載流量或兩者。 • 選取流量要轉送至以進行 **Analysis**（分析）的目的地： • 選取 public-cloud，讓所有符合規則的流量轉送至 WildFire 公共雲端以進行分析。

© 2019 Palo Alto Networks, Inc.

WildFire 分析設定檔設定	
	• 選取 private-cloud，讓所有符合規則的流量轉送至 WildFire 裝置以進行分析。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Data Filtering（物件 > 安全性設定檔 > 資料篩選）

資料篩選可讓防火牆偵測機敏資訊（例如信用卡號或社會安全號碼或公司內部文件），並防止此資料離開安全的網路。在您啟用資料篩選前，請選取 [物件 > 自訂物件 > 資料模式] 以定義您要篩選的資料類型（例如社會安全號碼或包含「機密」字樣的文件標題）。您可以將數個資料模式物件新增至單一資料篩選設定檔，若附加至安全性原則規則，防火牆會掃描允許流量中的每個資料模式，並根據資料篩選設定檔設定來封鎖相符流量。

資料篩選設定檔設定	說明
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在日誌轉送設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此資料篩選設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
資料擷取	選取此選項可自動收集由篩選所封鎖的資料。 在 *[設定]* 頁面上指定管理資料保護的密碼，以檢視您擷取的資料。請參考 *[裝置 > 設定 > 管理]*。
資料模式	新增現有的資料模式用於篩選，或選取 **New**（新增）以設定新的資料模式物件（物件 > 自訂物件 > 資料模式）。
應用程式	指定要包含在篩選規則中的應用程式： • 選取 **any** 可將選取套用至所有列出的應用程式。此選取不會封鎖所有可能的應用程式，僅會封鎖列出的應用程式。 • 按一下新增指定個別應用程式。
檔案類型	指定要包含在篩選規則中的檔案類型： • 選取 **any** 可將選取套用至所有列出的檔案類型。此選取不會封鎖所有可能的檔案類型，僅會封鎖列出的檔案類型。 • 按一下 **Add**（新增）指定個別檔案類型。
方向	指定以上傳方向、下載方向或兩個方向來套用篩選。

© 2019 Palo Alto Networks, Inc.

資料篩選設定檔設定	說明
警示臨界值	指定為了觸發警示而必須在檔案中偵測到資料模式的次數。
封鎖臨界值	封鎖包含至少這麼多資料模式實例的檔案。
日誌嚴重性	定義針對符合此資料篩選設定檔規則的事件而記錄的日誌嚴重性。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > DoS Protection（物件 > 安全性設定檔 > DoS 保護）

DoS 保護設定檔是針對高精度的選定及增強區域保護設定檔所設計。DoS 保護設定檔可指定每秒新連線 (CPS) 觸發警報和動作（指定於 DoS 保護原則）的閾值速率。DoS 保護設定檔也指定 CPS 速率上限，以及遭到封鎖的 IP 位址保留在封鎖 IP 清單上的時間長度。您可在 DoS 保護原則規則中指定 DoS 保護設定檔，您可在其中指定符合規則的封包準則，而原則規則確定設定檔適用的裝置。

建立 *DoS* 保護設定檔與原則，以保護重要的個別裝置或小型裝置群組，尤其是連接網際網路的裝置（如 *Web* 伺服器與資料庫伺服器）。

您可設定彙總與分類 DoS 保護設定檔。您可將彙總設定檔、分類設定檔或每種類型之一套用於 DoS 保護原則規則。若將這兩種設定檔類型套用於同一個規則，則防火牆會先套用彙總設定檔，然後根據需要套用分類設定檔。

- 分類 DoS 保護設定檔已將 **Classified**（分類）選取為 **Type**（類型）。在將分類 DoS 保護設定檔套用於其動作為 **Protect**（保護）的 DoS 保護規則時，如果封包符合指定的位址類型（source-ip-only、destination-ip-only 或 src-dest-ip-both），防火牆會針對設定檔的 CPS 臨界值計算連線。
- 彙總 DoS 保護設定檔已將 **Aggregate**（彙總）選取為 **Type**（類型）。在將彙總 DoS 保護設定檔套用於其動作為 **Protect**（保護）的 DoS 保護規則時，防火牆會針對設定檔的 CPS 臨界值計算符合規則準則的所有連線（規則中指定之裝置群組的連線總數）。

若要將 DoS 保護設定檔套用至 DoS 保護原則，請參閱 [原則 > DoS 保護]。

如果您具有多重虛擬系統 *(multi-vsys)* 環境，並已設定下列項目：

- 外部區域，用來啟用虛擬系統之間的通訊，和
- 共用閘道，可讓虛擬系統對外部通訊共用公用介面及單一 *IP* 位址，且

在外部區域停用下列地區和 *DoS* 保護機制：

- 同步處理 *Cookie*
- *IP* 分散
- *ICMPv6*

若要啟用 *IP* 分散和 *ICMPv6* 保護，請為共用閘道建立個別的區域保護設定檔。

若要對抗共用閘道上的 *SYN* 流量，您可以使用隨機早期丟棄或 *SYN Cookie* 來套用 *SYN* 流量保護設定檔。在外部區域上，隨機早期丟棄只能用於 *SYN* 流量保護。

DoS 保護設定檔設定	
名稱	輸入設定檔名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在日誌轉送設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	輸入設定檔的描述（最多 255 個字元）。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項：

© 2019 Palo Alto Networks, Inc.

DoS 保護設定檔設定	
	• 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此 DoS 保護設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
類型	選取下列其中一個設定檔類型： • **Aggregate**（彙總）—將設定檔中設定的 DoS 臨界值套用至符合套用此設定檔之規則準則的所有連線。例如，具有 SYN 流量 **Alarm Rate**（警報速率）閾值 10,000 CPS 的彙總規則計算符合 DoS 規則之所有裝置的總連線。在群組總 CPS 超過可觸發警報的 10,000 CPS 時，無論 CPS 如何在裝置上傳播。 • **Classified**（分類）—將設定檔中設定的 DoS 臨界值套用至符合分類準則（來源 IP 位址、目的地 IP 位址或來源與目的地 IP 位址配對）的每個個別連線。例如，具有 SYN 流量 **Alarm Rate**（警報速率）閾值 10,000 CPS 的分類規則允許每個裝置達到 10,000 CPS，並在 DoS 規則內指定的任何個別裝置超過 10,000 CPS 時觸發警報。
Flood Protection 頁籤	

SYN 流量頁籤
UDP 流量頁籤
ICMP 流量頁籤
ICMPv6 流量頁籤
其他 IP 流量頁籤
	選取此選項可啟用頁籤上指出的流量保護類型，並指定下列設定：
	• **Action**（動作）—（僅限 **SYN Flood**（**SYN** 流量））在 DoS 保護原則動作為 **Protect**（保護）且傳入 CPS 達到 **Activate Rate**（啟動速率）時防火牆執行的動作。選取下列其中一項：
	  • 隨機早期丟棄—當每秒連線達到 **Activate Rate**（啟動速率）臨界值時，隨機丟棄封包。
	  • **SYN Cookie**使用 SYN Cookie 產生通知，就不需要在 SYN 流量攻擊期間中斷連線。
	  從 *SYN Cookie* 開始，其會公平地處理合法流量，但耗用更多防火牆資源。監控 *CPU* 與記憶體使用率，若 *SYN Cookie* 耗用過多資源，則切換到 *RED*。若您在網路（網際網路）邊緣沒有專用的 *DDoS* 防禦裝置，請一律使用 *RED*，以防止大量 *DoS* 攻擊。
	• **Alarm Rate**（警報速率）—指定產生 DoS 警報的閾值速率 (CPS)（範圍是 0 至 2,000,000 cps，預設為 10,000 cps）。
	  對於分類設定檔，最佳做法是將臨界值設定為高於裝置的平均 CPS 速率的 15-20% 以適應正常波動，並在收到過多警報時調整閾值。對於彙總設定檔，最佳做法是將閾值設定為高於群組平均 CPS 速率的 15-20%。視需要監控和調整臨界值。
	• 啟動速率—指定啟動 DoS 回應的臨界值速率 (cps)。DoS 回應設定於 DoS 保護設定檔的 **Action**（動作）欄位中（隨機早期丟棄或 SYN cookie）。**Activate Rate**（啟動速率）範圍是 0 至 2,000,000 cps，預設值是 10,000 cps。
	  如果 **Action**（動作）是 **Random Early Drop**（隨機早期丟棄）(RED) 臨界值，當每秒連入連線達到 **Activate Rate**（啟動速率）臨界值時，隨即發生

© 2019 Palo Alto Networks, Inc.

DoS 保護設定檔設定	
	RED。如果 CPS 速率提高，則 RED 速率會根據演算法提高。防火牆會繼續使用 RED，直到 CPS 速率達到 **Max Rate**（最大速率）閾值為止。 分類設定檔將確切的 CPS 限制套用到個別裝置，而且您將這些限制以受保護裝置的容量為基礎，因此您不需要逐漸調整 CPS，並且可以將 **Activate Rate**（啟動速率）設定為和 **Max Rate**（最大速率）一樣的閾值。僅在您想要在達到 **Max Rate**（最大速率）前開始丟棄流量到個別伺服器時，將 **Activate Rate**（啟動速率）設定為低於 **Max Rate**（最大速率）。對於彙總設定檔，將閾值設定為正好高於群組的峰值 CPS 速率。視需要監控和調整臨界值。 • 最大速率—指定防火牆允許每秒連入連線的臨界值速率。達到 **Max Rate**（最大速率）臨界值，防火牆會中斷 100% 的新連線 (範圍是 2 至 2,000,000 cps，預設值是 40,000 cps)。 對於分類設定檔，**Max Rate**（最大速率）取決於您正在保護的裝置容量，因此不會遭流量攻擊。對於彙總設定檔，將 **Max Rate**（最大速率）設定為群組容量的 80-90%。視需要監控和調整臨界值。 • 封鎖持續時間—指定時間長度（秒數），在這段期間違規的 IP 位址會保留在封鎖 IP 清單上，而透過該 IP 位址的連線會遭到封鎖。防火牆不會針對警報速率、啟動速率或最大速率臨界值（範圍是 1 至 21,600 秒，預設值是 300 秒），計算在封鎖期間送達的封包。
Resources Protection 頁籤	
工作階段	選取此選項可啟用資源保護。
最大同時工作階段數	指定同時工作階段的最大數目。 • 對於 **Aggregate**（彙總）設定檔類型，此限制會套用至符合套用 DoS 保護設定檔之 DoS 保護規則的所有流量。 • 對於 **Classified**（已分類）設定檔類型，此限制會根據分類（來源 IP、目的地 IP 或來源與目的地 IP）套用至符合套用 DoS 保護設定檔之 DoS 保護規則的流量。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > Mobile Network Protection（物件 > 安全性設定檔 > 行動網路保護）

透過行動網路保護設定檔，防火牆可以檢查 5G 服務型架構 (SBA) 流量中的 GTP 和 HTTP/2。若要檢視此設定檔，您必須在 [裝置 > 設定 > 管理] 中啟用 GTP 安全性。

使用此設定檔中的選項，可啟用 5G HTTP/2、GTP v1-C、GTP v2-C 和 GTP-U 的具狀態檢查，啟用 GTPv1-C、GTP v2-C 和 GTP-U 的通訊協定驗證，以及啟用 GTP-U 內容檢查以掃描 GTP-U 通道中的使用者資料。此外，還可讓您篩選基於 APN、IMSI/IMSI-Prefix 和 RAT 的 GTP 工作階段，並防止使用者 IP 位址偽造。

GTP 檢查設定檔設定	
GTP 檢查	

GTP-C	• 選取 **Stateful Inspection**（具狀態檢查）可讓防火牆檢查 **GTPv1-C** 或 **GTPv2-C** 或兩者。當您啟用具狀態檢查時，防火牆會使用來源 IP、來源連接埠、目的地 IP、目的地連接埠、通訊協定和通道端點 ID (TEID) 來追蹤 GTP 工作階段。它也會檢查及驗證不同類型的 GTP 訊息用來建立 GTP 通道的順序。TEID 可唯一識別 GSN 通道端點。上行和下行的通道是分開的，使用不同的 TEID。
	• 選取防火牆會在有效性檢查失敗時採用的 **Action**（動作）—**Block**（封鎖）或 **Alert**（警示）。警示動作會允許流量通過但產生日誌；封鎖動作會拒絕流量通過並產生日誌。
	• 指定防火牆必須對 GTP 標頭和承載中的資訊元素 (IE) 執行的有效性檢查。防火牆會使用您在下方選取的封鎖或警示動作來處理錯誤。您可以設定防火牆來驗證：
	  • **Reserved IE**（保留的 **IE**）—檢查使用保留 IE 值的 GTPv1-C 或 GTPv2-C 訊息。
	  • **Order of IE**（**IE** 順序）（僅限 GTPv1-C）—檢查 GTPv1-C 訊息中的 IE 順序是否正確。
	  • **IE** 長度—檢查 IE 長度無效的 GTPv1-C 或 GTPv2-C 訊息。
	  • 標頭中保留的欄位—檢查在標頭中使用無效值或保留值且格式錯誤的封包。
	  • 不支援的訊息類型—檢查未知或不正確的訊息類型。

GTP-U	啟用 GTPv1-C 和/或 GTPv2-C 的具狀態檢查，可自動啟用 GTPU-U 具狀態檢查。 您可以指定 GTP-U 承載的下列有效性檢查。 • **Reserved IE**（保留的 **IE**）—檢查使用承載中保留 IE 值的 CTP-U 訊息。 • **Order of IE**（**IE** 順序）—檢查 GTP-U 訊息中的 IE 順序是否正確。 • **Length of IE**（**IE** 長度）—檢查 IE 長度無效的訊息。 • 標頭中保留的欄位—檢查在標頭中使用無效值或保留值且格式錯誤的封包。 • 不支援的訊息類型—檢查未知或不正確的訊息類型。 此外，您也可以針對下列各項設定允許、封鎖或警示動作：

© 2019 Palo Alto Networks, Inc.

GTP 檢查設定檔設定	
	• 一般使用者 **IP** 位址詐騙—設定防火牆，以在用戶使用者裝置的 GTP-U 封包中的來源 IP 位址與在通道設定期間交換之對應 GTP-C 訊息中的 IP 位址不同時進行封鎖或警示。 • **GTP-in-GTP**—您可以設定防火牆在偵測到 GTP-in-GTP 訊息時進行封鎖或警示。在偵測時，防火牆會產生具有重要嚴重性的 GTP 日誌。 • 對於 4G 和 3G，如果您想要檢查並將政策套用至 GTP-U 封包內的使用者資料有效負載，請啟用 **GTP-U Content Inspection**（**GTP-U** 內容檢查）。檢查 GTP-U 內容可讓從 GTP-C 訊息取得的 IMSI 和 IMEI 資訊與在 GTP-U 封包中封裝的 IP 流量相互關聯。
5G-C	對於 5G，請啟用 **5G-HTTP2** 以啟用對 5G HTTP/2 控制封包的檢查，其中可能包含用戶 ID、設備 ID 和網路切片資訊。這讓您可以將從 HTTP/2 訊息中瞭解的用戶 ID (IMSI)、設備 ID (IMEI) 和網路切片 ID 資訊與封裝在 GTP-U 封包中的 IP 流量相關聯。 啟用 **5G-HTTP2** 將停用設定檔的 GTP-C。
篩選選項	
RAT 篩選	依預設，會允許所有無線存取技術 (RAT)。GTP-C Create-PDP-Request 和 Create-Session-Request 訊息會根據 RAT 篩選器進行篩選或允許。您可以指定是否允許、封鎖或警示使用者設備用來存取行動核心網路的下列 RAT： • **UTRAN** • **GERAN** • **WLAN** • **GAN** • **HSPA** 演進 • **EUTRAN** • 虛擬 • **EUTRAN-NB-IoT** • **LTE-M** • **NR** 啟用 **5G-HTTP2** 後提供下列 RAT： • **WLAN** • **EUTRAN** • 虛擬 • **NR**
IMSI 篩選	IMSI (國際行動用戶辨識碼) 是與 GSM、UMTS 和 LTE 網路中的用戶相關聯的唯一識別碼，該識別碼佈建在用戶識別模組 (SIM) 卡中。 IMSI 通常是以 15 位數字（8 個位元組）呈現，但可能更短。IMSI 由三個部分所組成： • 包含三位數字的行動電話國家代碼 (MCC)。MCC 可唯一識別行動用戶的所在國別。 • 包含兩位或三位數字的行動裝置網路代碼 (MNC)；兩位數字符合歐洲標準或三位數字符合北美標準。MNC 可識別行動用戶的歸屬 PLMN。 • 識別 PLMN 內行動用戶的行動用戶識別碼 (MSIN)。

© 2019 Palo Alto Networks, Inc.

GTP 檢查設定檔設定	
	IMSI Prefix（**IMSI** 前置詞）結合 MCC 與 MNC，可讓您 **allow**（允許）、**block**（封鎖）或 **alert**（警示）來自特定 PLMN 的 GTP 流量。依預設會允許所有的 IMSI。 您可以手動輸入，或將包含 IMSI 的 CSV 檔案或 IMSI 前置詞匯入防火牆中。IMSI 可包含萬用字元，例如 310* 或 240011*。 防火牆最多支援 5,000 個 IMSI 或 IMSI 前置詞。
APN 篩選	存取點名稱 (APN) 是使用者設備連接網際網路所需之 GGSN/ PGW 的參考。在 5G 中，有一種資料網路名稱 (DNN) 格式是 APN。APN 由一個或兩個識別碼組成： • APN 網路識別碼，其定義 GGSN/PGW 所連接的外部網路以及行動通訊台選取性要求的服務。這是 APN 的必要部分。 • APN 操作員識別碼，其定義 GGSN/PGW 所在的 PLMN GPRS/EPS 骨幹。這是 APN 的選用部分。 依預設會允許所有的 APN。APN 篩選器可讓您根據 APN 值允許、封鎖或警示 GTP 流量。GTP-C Create-PDP-Request 和 Create-Session-Request 訊息會根據針對 APN 篩選所定義的規則進行篩選或允許。 您可以將 APN 篩選清單手動新增或匯入防火牆中。APN 值必須包含網路 ID 或網路的網域名稱（例如，example.com）與操作員 ID（選取性）。 對 APN 篩選器而言， wildcard '*' 允許您為所有 APN 進行比對。萬用字元並不支援 '*' 和其他字元結合使用。舉例來說，「internet.mnc*」會被視為合格 APN，而不會篩選所有以 internet.mnc 開頭的項目。 防火牆最多支援 1,000 個 APN 篩選器。
GTP 通道限制	
每個目的地同時允許的通道數上限	可讓您限制目的地 IP 位址（例如 GGSN）的最大 GTP-U 通道數目（範圍是 0 至 100,000,000 個通道）
每個目的地同時通道數上限的警示	指定已建立目的地的最大 GTP-U 通道數目時，防火牆觸發警示的閾值。達到所設定的通道限制時，便會產生高嚴重性的 GTP 日誌訊息。
記錄頻率	超出所設定的 GTP 通道限制時，防火牆在產生日誌前所計算的事件數目。此設定可讓您將數量減少為記錄的訊息（範圍是 0 至 100,000,000；預設值為 100）。
過度收費保護	選取虛擬系統以作為您防火牆上的 Gi/ SGi 防火牆。Gi/ SGi 防火牆會檢查透過 Gi/ SGi 介面從 PGW/GGSN 周遊至外部 PDN（封包資料網路）（例如網際網路）的行動用戶 IP 流量，並保護行動用戶的網際網路存取。 當 GGSN 將一般使用者 IP 位址集區中先前使用的 IP 位址指派給行動用戶時，可能會發生過度收費。當網際網路上的惡意伺服器繼續將封包傳送至此 IP 位址時，因為並未關閉針對先前用戶起始的工作階段，此工作階段仍會在 Gi 防火牆上開啟。若不要允許傳送資料，每當 GTP 通道遭到刪除（由 delete-PDP 或 delete-session 訊息偵測）或逾時，針對過度收費保護啟用的防火牆會通知 Gi/ SGi 防火牆，從工作階段表格中刪除屬於用戶的所有工作階段。應在相同的實體防火牆上設定 GTP 安全性和 SGi/ Gi 防火牆，但可以位於不同的虛擬系統。若要根據 GTP-C 事件刪除工作階段，防火牆必須具備所有相關工作階段資訊，而

© 2019 Palo Alto Networks, Inc.

GTP 檢查設定檔設定	
	這只有在您從行動核心網路中適用於 GTPv2 的 SGi + S11 或 S5 介面，和適用於 GTPv1 的 Gi + Gn 介面管理流量時才可行。
其他日誌設定 根據預設，防火牆不會記錄允許的 GTP 訊息。您可以選取性地啟用允許的 GTP 訊息之記錄功能，因為該功能將產生大量日誌，可供您視需要進行疑難排解。除了允許的日誌訊息，此頁籤也可讓您選取性地啟用使用者位置資訊的記錄功能。	
GTPv1-C 允許的訊息	如果您已對 GTPv1-C 訊息啟用具狀態檢查，可讓您選取性地啟用允許的 GTPv1-C 訊息之記錄功能。這些訊息會產生日誌，協助您視需要排解疑難問題。 根據預設，防火牆不會記錄允許的訊息。允許的 GTPv1-C 訊息之記錄選項如下： • **Tunnel Management**（通道管理）—這些 GTPv1-C 訊息用於管理 GTP-U 通道，此種通道會在指定的網路節點配對（如 SGSN 與 GGSN）之間傳送已封裝 IP 封包和訊號訊息。其中包含下列訊息，例如建立 PDP 內容要求、建立 PDP 內容回應、更新 PDP 內容要求、更新 PDP 內容回應、刪除 PDP 內容回應、刪除 PDP 內容回應。 • **Path Management**（路徑管理）—這些 GTPv1-C 訊息通常由 GSN 或無線網路控制器 (RNC) 傳送至其他 GSN 或 RNC，以查明對端是否保持運作。其中包含訊息，例如回應要求和回應回覆。 • **Others**（其他）—這些訊息包含位置管理、行動性管理、RAN 資訊管理和多媒體廣播多點傳送服務 (MBMS) 訊息。
日誌使用者位置	可讓您在 GTP 日誌中包含使用者位置資訊，例如區域代碼和 Cell ID。
封包擷取	可讓您擷取 GTP 事件。
GTPv2-C 允許的訊息	如果您已對 GTPv2-C 啟用具狀態檢查，可讓您選擇性地啟用允許的 GTPv2-C 訊息之記錄功能。這些訊息會產生日誌，協助您視需要排解疑難問題。 根據預設，防火牆不會記錄允許的訊息。允許的 GTPv2-C 訊息之記錄選項如下： • **Tunnel Management**（通道管理）—這些 GTPv2-C 訊息用於管理 GTP-U 通道，此種通道會在指定的網路節點配對（如 SGW 與 PGW）之間傳送已封裝 IP 封包和訊號訊息。其中包含下列訊息類型：建立工作階段要求、建立工作階段回應、建立承載者要求、建立承載者回應、修改承載者要求、修改承載者回應、刪除工作階段要求及刪除工作階段回應。 • **Path Management**（路徑管理）—這些 GTPv2-C 訊息通常由 SGW 或 PGW 等網路節點傳送至其他 PGW、SGW，以查明端點是否保持運作。其中包含訊息，例如回應要求和回應回覆。 • **Others**（其他）—這些訊息包含行動性管理和非 3GPP 存取相關訊息。
GTP-U 允許的訊息	如果您已對 GTPv2-C 或 GTPv1-C 啟用具狀態檢查，可讓您選擇性地啟用允許的 GTP-U 訊息之記錄功能。這些訊息會產生日誌，協助您視需要排解疑難問題。 允許的 GTP-U 訊息之記錄選項如下： • **Tunnel Management**（通道管理）—這些是 GTP-U 訊號訊息，例如錯誤指示。

© 2019 Palo Alto Networks, Inc.

GTP 檢查設定檔設定	
	• **Path Management**（路徑管理）—這些 GTP-U 訊息是由網路節點（例如 eNodeB）傳送給其他網路節點（例如 SGW），以查明端點是否保持運作。其中包含訊息，例如回應要求/回應。 • **G-PDU**—G-PDU (GTP-U PDU) 用於傳送行動核心網路中網路節點內的使用者資料封包；其包含 GTP 標頭加上 T-PDU。
根據新 GTP-U 通道記錄的 G-PDU 封包	啟用此選項以確認防火牆會檢查 GTP-U PDU。防火牆會針對每個新 GTP-U 通道中的指定 G-PDU 封包數目，產生日誌（範圍是 1 至 10；預設值為 1）。
5G-C 允許的訊息	選取 **N11** 以選擇性地啟用對允許的 N11 訊息的記錄。N11 訊息可協助您進行疑難排解，並更深入地瞭解透過 N11 介面針對不同程序交換的 HTTP/2 訊息。僅在「行動網路保護」設定檔中的 **5G-C** 頁籤上啟用 **5G-HTTP2** 時，此欄位才可用。

© 2019 Palo Alto Networks, Inc.

Objects > Security Profiles > SCTP Protection（物件 > 安全性設定檔 > SCTP 保護）

建立 串流控制傳輸協議（SCTP）保護設定檔以指定您想要防火牆驗證和篩選 SCTP 塊的方式。您首先必須啟用 SCTP 安全性（**Device**（裝置）> **Setup**（設定）> **Management**（管理）> **General Settings**（一般設定））以觀看安全性設定檔內的此設定檔類型。您還可以限制多歸屬環境中每個 SCTP 端點的 IP 位址數量，並可以指定防火牆何時記錄 SCTP 事件。建立 SCTP 保護設定檔後，您需要將該設定檔套用於區域的安全性原則上。

支援 SCTP 安全性的防火牆型號有預先定義的 SCTP 保護設定檔（*default-ss7*）讓您可以如現況使用或可以複製 default-ss7 設定檔作為新 SCTP 保護設定檔的基礎。選取物件 > 安全性設定檔 > **SCTP** 保護 並選取 **default-ss7** 以觀看造成此預定義設定檔警示的操作代碼。

SCTP 保護設定檔設定	
名稱	輸入 SCTP 保護設定檔的名稱。
說明	輸入 SCTP 保護設定檔的說明。
SCTP 檢測	
未知區段	選取防火牆接收一個未知區段的 SCTP 封包時的動作（此區段未在 RFC3758、RFC4820、RFC4895、RFC4960、RFC5061或RFC 6525 中定義）： • 允許（預設）—允許封包不經修正通過。 • **alert**（警示）—允許封包不經修正通過，且生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。 • 封鎖—在傳遞封包之前使區段無效並生成 SCTP 日誌。
區段旗標	當防火牆收到有與 RFC4960 不一致區段旗標的 SCTP 封包時時，選取防火牆的動作： • 允許（預設）—允許封包不經修正通過。 • **alert**（警示）—允許封包不經修正通過，且生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。 • 封鎖—丟棄封包並生成 SCTP 日誌。
無效的長度	當防火牆收到有無效長度 SCTP 區段時，選取防火牆的動作： • **allow**（允許）（預設）—允許封包或區段不經修正通過。 • **block**（封鎖）—丟棄封包並生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌儲存頁籤。
多歸屬 IP 位址限制	在防火牆生成警示訊息前，輸入您可為 SCTP 端點設定的最大數目 IP 位址（範圍是 1 到 8；預設為 4）。

© 2019 Palo Alto Networks, Inc.

SCTP 保護設定檔設定	
	SCTP 多歸屬為端點的能力，能支援超過一個與端點相關聯的 IP 位址。若至端點的一條路徑無法通過，則 SCTP 會選取為該關聯提供的另一個目的地 IP 位址。
日誌設定	選取任意設定組合以生成 SCTP 日誌，允許區段、關聯起點與終點以及狀態故障事件： • 關聯開始時的日誌 • 關聯結束時的日誌 • 允許關聯起始區段的日誌 • 允許 **Heartbeat** 區段的日誌 • 允許關聯終止區段的日誌 • 所有控制區段的日誌 • 故障事件狀態日誌 若要防火牆儲存 SCTP 日誌,則您需要分配 SCTP 儲存（請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。
篩選選項	
SCTP 篩選	
名稱	輸入 SCTP 篩選器的名稱。
PPID	指定 SCTP 篩選器的 PPID： • 任何—使防火牆執行您在包含 PPID 的所有 SCTP 數據區段上指定的動作。 • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • 輸入一個有效的 PPID 值（一個未在下拉式選單顯示的值）。舉例來說，H.323 的 PPID 值是 13。 每個 SCTP 篩選器僅可以指定一個 PPID，但您可以為一個 SCTP 保護設定檔指定多個 SCTP 篩選器。
動作	指定防火牆對於包含此特定 PPID 的數據區段所採取的動作： • **allow**（允許）（預設）—允許區段不經修正通過。 • **alert**（警示）—允許區段不經修正通過，且生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。

© 2019 Palo Alto Networks, Inc.

SCTP 保護設定檔設定	
	• **block**（封鎖）—在通過封包前丟棄區段並生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。
SCTP 封包會與清單中的篩選器從上到下比對。如果您為一個設定檔建立超過一個的 SCTP 篩選器，則 SCTP 篩選器的順序就會有所不同。選取一個篩選器並 **Move Up**（上移）或**Move Down**（下移）以在 SCTP 篩選清單中改變其相對優先次序。	
直徑篩選	
名稱	輸入直徑篩選器的名稱。
動作	指定防火牆在包含指定直徑應用程式 ID、指令代碼和 AVP 的直徑區段上所採取的動作。如果偵測到的區段包含指定的直徑應用程式 ID 和任何指定的直徑指令代碼以及任何指定直徑 AVP，則： • **allow**（允許）（預設）—允許區段不經修正通過。 • **alert**（警示）—允許區段不經修正通過，且生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。 • **block**（封鎖）—在通過封包前丟棄區段並生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。
直徑應用程式 ID	指定一個防火牆曾採取特定行動區段的直徑應用程式 ID。 • 任何 • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • 直徑基礎會計 • 直徑常見消息 • 直徑信用控制 或者，您可以輸入一個直徑應用程式 ID 數值（範圍從 0 到 4,294,967,295）。一個直徑篩選器能有一個應用程式 ID。
直徑指令代碼	指定一個防火牆曾採取特定行動區段的直徑指令代碼。選取 **any**（任何），從下拉式選單選取一個直徑指令代碼，或輸入一個特定的值（範圍從 0 到 16,777,215）。下拉式選單僅包含適用於選定直徑應用程式 ID 的指令代碼。您可以在直徑篩選單中新增多個直徑指令代碼。
直徑 AVP	指定一個防火牆曾採取特定行動區段的直徑屬性值對（AVP）。輸入一個或多個 AVP 代碼或值（範圍從 1 到 16,777,215）。
如果您為一個設定檔建立超過一個的直徑篩選器，則直徑篩選器的順序就會有所不同。選取一個篩選器並 **Move Up**（上移）或**Move Down**（下移）以在直徑篩選清單中調整其相對優先次序。	
SS7 篩選	

© 2019 Palo Alto Networks, Inc.

SCTP 保護設定檔設定	
名稱	輸入 SS7 篩選器的名稱。
動作	指定防火牆對於包含此特定 SS7 篩選器元素的 SS7 區段所採取的動作：如果區段被偵測出包含 SCCP 呼叫方 SSN 和任何特定的 SCCP 呼叫方全域標題（GT）值以及任何特定的操作代碼，則： • **allow**（允許）（預設）—允許區段不經修正通過。 • **alert**（警示）—允許區段不經修正通過，且生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。 • **block**（封鎖）—在通過封包前丟棄區段並生成 SCTP 日誌（您需要為這些日誌分配日誌儲存—請見日誌記錄與報告設定下的日誌儲存頁籤：裝置 > 設定 > 管理）。
SCCP 呼叫方 SSN	指定一個防火牆曾採取特定行動區段的 SCCP 呼叫方 SSN。選取從下拉式選單 **any-map** 或 **Add**（新增）一個 SCCP 呼叫方 SSN： • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **SCCP 管理** 一個 SS7 篩選器僅能有一個 SCCP 呼叫方 SSN。
SCCP 呼叫方 GT	指定一個防火牆曾採取特定行動區段的 SCCP 呼叫方 GT 值。選取 **Any**（任何）或 **Add**（新增）最多 15 位數的數值。您也可以使用首碼輸入一組 SCCP 呼叫方 GT 值。例如：876534*.您可以在一個 SS7 篩選器中新增多個 SCCP 呼叫方 GT 值。 SCCP 呼叫方 SSN：**INAP** 和 **SCCP 管理**，這個選項停用。
操作代碼	指定一個防火牆曾採取特定行動區段的操作代碼： 對於下列 SCCP 呼叫方 SSN，選取 **any**（任何）或一個從下拉式選單的操作代碼，或輸入一個特定的值（範圍為 1 到 255）： • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)**

© 2019 Palo Alto Networks, Inc.

SCTP 保護設定檔設定	
	• **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** SCCP 呼叫方 SSN：**CAP**，輸入一個值（範圍為 1 到 255）。 SCCP 呼叫方 SSN：**INAP** 和 **SCCP** 管理，這個選項停用。 您可以在 SS7 篩選器中新增多個操作代碼。
如果您為一個設定檔建立超過一個的 SS7 篩選器，則 SS7 篩選器的順序就會有所不同。選取一個篩選器並 **Move Up**（上移）或**Move Down**（下移）以在 SS7 篩選清單中調整其相對優先次序。	

© 2019 Palo Alto Networks, Inc.

Objects > Security Profile Groups（物件 > 安全性設定檔群組）

防火牆支援建立安全性設定檔群組的功能，這些安全性設定檔群組可以指定安全性設定檔集合，您可以將這些集合視為一個單元，然後將其新增至安全性原則。例如，您可以建立包含防毒、反間諜軟體與弱點保護設定檔的威脅安全性設定檔群組，然後建立包含威脅設定檔的安全性原則。

您可以將防毒、反間諜軟體、弱點保護、URL 篩選以及通常一起指定的檔案封鎖設定檔合併至設定檔群組，來簡化安全原則的建立。

若要定義新的安全性設定檔，請選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）。

下表說明安全性設定檔設定：

安全性設定檔群組設定	說明
名稱	輸入設定檔群組名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔群組，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔群組。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔群組。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此安全性設定檔群組物件的裝置群組中取代該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
設定檔	選取防毒、反間碟軟體、弱點防護、URL 篩選，及/或要包含在此群組中的檔案封鎖設定檔。也可以在安全性設定檔群組中指定資料篩選設定檔。請參考 [物件 > 安全性設定檔 > 資料篩選]。

© 2019 Palo Alto Networks, Inc.

Objects > Log Forwarding（物件 > 日誌轉送）

根據預設，防火牆產生的日誌只駐留在其本機儲存裝置上。不過，如果您可以使用 Panorama™、日誌服務或外部服務（例如 syslog 伺服器）以透過定義日誌轉送設定檔並將其指派給安全性、驗證和 DoS 保護原則規則，來集中監控日誌資訊。日誌轉送設定檔可定義下列日誌類型的轉送目的地：驗證、數據篩選、GTP、SCTP、威脅、流量、URL 篩選和 WildFire® 提交日誌。

有很多原因使您應將日誌轉送到 *Panorama* 或外部儲存裝置，包含：法遵、備援、運行分析、集中監控以及審查威脅行為和長期模式。此外，防火牆具有有限的日誌儲存空間，並且在儲存空間填滿時刪除最舊的日誌。請務必轉送威脅日誌和 *WildFire* 日誌。

若要轉送其他日誌類型，請參閱 [裝置 > 日誌設定]。

若要啟用 *PA-7000* 系列防火牆以轉送日誌或轉送檔案至 *WildFire*®，則您首先必須在 *PA-7000* 系列防火牆設定一個 Log Card Interface（日誌卡介面）。當您完成設定此介面後，防火牆將自動使用此連接埠—不需特殊組態。只要將其中一個 *PA-7000* 系列網路處理卡（*NPC*）上的資料連接埠設定為記錄卡介面類型，並確定將使用的網路可與您的日誌伺服器通訊即可。若為 *WildFire* 轉送，網路必須與 *WildFire* 雲端或 *WildFire* 裝置（或以上兩者）通訊成功。

下表說明日誌轉送設定檔。

日誌轉送設定檔設定	說明
名稱	輸入用來識別設定檔的名稱（最多 64 個字元）。定義安全性原則規則時，此名稱會顯示在日誌轉送設定檔清單中。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 **(vsys)**—如果您停用（清除）此選項，設定檔將僅供 **Objects**（物件）頁籤上選定的 **Virtual System**（虛擬系統）使用。 • **Panorama** 上的每個裝置群組—如果您停用（清除）此選項，設定檔將僅供 **Objects**（物件）頁籤上選定的 **Device Group**（裝置群組）使用。
啟用 Cortex Data Lake 的增強型應用程式日誌記錄（包含流量以及 URL 日誌）（僅限 Panorama）	Palo Alto Networks 雲端服務的增強型應用程式日誌可透過 Cortex Data Lake 訂閱獲得。憑藉增強型應用程式日誌記錄，防火牆可專門收集資料，來深入瞭解在 Palo Alto Networks 雲端服務環境中執行之應用程式的網路活動。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此日誌轉送設定檔的裝置群組中取代該設定檔的設定。預設會停用此選取項目，這表示管理員可以取代繼承此設定檔之任何裝置群組的設定。
說明	輸入說明，以說明此日誌轉送設定檔的目的。
比對清單（未標記）	**Add**（新增）一或多個比對清單設定檔（最多 64 個），以指定轉送目的地、以日誌屬性為基礎的篩選器，進行控制防火牆轉送的日誌，以及要在日誌上執行的動作（例如自動標記）。針對每個比對清單設定檔完成下列兩個欄位（名稱與說明）。

© 2019 Palo Alto Networks, Inc.

日誌轉送設定檔設定	說明
名稱（比對清單設定檔）	輸入用來識別比對清單設定檔的名稱（最多 31 個字元）。
說明（比對清單設定檔）	輸入說明（最多 1,023 個字元）以解釋這個比對清單設定檔的目的。
日誌類型	選取此比對清單設定檔適用的日誌類型：驗證（**auth**）、數據、**gtp**、**sctp**、威脅、流量、通道、**URL** 或 **WildFire**。
篩選	根據預設，防火牆會轉送所選 **Log Type**（日誌類型）的 **All Logs**（所有日誌）。若要轉送日誌的子集，請選取下拉式清單中的現有篩選器，或選取 **Filter Builder**（篩選建立器）以新增篩選器。針對新篩選器中的各個查詢，指定下列欄位並 **Add**（新增）查詢： • 連接器—選取查詢的連接器邏輯（and/or）。若您要將否定套用至邏輯，則選取 **Negate**（否定）。例如，若要避免從不受信任的區域轉送日誌，請選取 **Negate**（否定）、選取 **Zone**（區域）屬性、選取 **equal** 運算子，然後在 [值] 欄中輸入不受信任的區域名稱。 • 屬性—選取日誌屬性。可用的屬性取決於 **Log Type**（日誌類型）。 • 運算子—選取準則以決定是否套用屬性（例如 **equal**）。可用的準則取決於 **Log Type**（日誌類型）。 • 值—指定要比對的屬性值。 若要 display or export（顯示或匯出）篩選器比對的日誌，可 **View Filtered Logs**（檢視篩選的日誌），它可提供與 **Monitoring**（監控）頁籤頁面相同的選項（如：**Monitoring**（監控）> **Logs**（日誌）> **Traffic**（流量））。
Panorama Panorama/記錄服務（僅限 Panorama）	若您要將日誌轉送至日誌收集器或 Panorama 管理伺服器，或轉送日誌至日誌服務，請選取 **Panorama**。 若您啟用此選項，則您必須設定日誌轉送至 Panorama。 若要使用日誌記錄服務，您必須也在 裝置 > 設定 > 管理中**Enable**（啟用） 日誌記錄服務。
SNMP	**Add**（新增）一或多個 SNMP 設陷伺服器設定檔，將日誌當作 SNMP 設陷轉送（請參閱 [裝置 > 伺服器設定檔 > SNMP 設陷]）。
電郵	**Add**（新增）一或多個電子郵件伺服器設定檔，將日誌當作電子郵件通知轉送（請參閱 [裝置 > 伺服器設定檔 > 電子郵件]）。
Syslog	**Add**（新增）一或多個 Syslog 伺服器設定檔，將日誌當作 Syslog 訊息轉送（請參閱 [裝置 > 伺服器設定檔 > Syslog]）。
HTTP	**Add**（新增）一個或多個 HTTP 伺服器設定檔，將日誌當作 HTTP 要求轉送（請參閱 [裝置 > 伺服器設定檔 > HTTP]）。
內建動作	**Add**（新增）要執行的動作時，可以從兩種內建動作中進行選擇—標記和整合。 • 標記—自動新增或移除日誌項目的來源或目的地 IP 位址中的頁籤，以及向防火牆或 Panorama 上的 User-ID 代理程式，或向遠端 User-ID 代理程式註冊 IP 位址和頁籤對應，以便您回應事件並動態執行安全性原則。標記 IP 位址和使用動態位址群組動態強制執行原則的功能，讓您擁有更好的可見度、內容和控制能力，一貫地執行安全性原則（不管 IP 位址在您的網路移到何處）。 進行下列設定：

© 2019 Palo Alto Networks, Inc.

日誌轉送設定檔設定	說明
	• **Add**（新增）動作並輸入用以說明的名稱。 • 選取您要標記的目標 IP 位址—**Source Address**（來源位址）或 **Destination Address**（目的地位址）。 您可以對所有日誌類型（包括日誌項目中的來源或目的地 IP 位址）採取動作。在 [關聯] 日誌和 [HIP 比對] 日誌中，您只可以標誌來源 IP 位址；您無法設定 [系統] 日誌和 [組態] 日誌的動作，因為該日誌類型未在日誌項目中包含 IP 位址。 • 選取動作—**Add Tag**（新增頁籤）或 **Remove Tag**（移除頁籤）。 • 選取要向此防火牆或 Panorama 上的 **Local User-ID**（本機 **User-ID**）代理程式，或向 **Remote User-ID**（遠端 **User-ID**）代理程式註冊 IP 位址和頁籤對應。 • 若要向 **Remote User-ID**（遠端 **User-ID**）代理程式註冊 IP 位址和頁籤對應，請選取將啟用轉送的 HTTP 伺服器設定檔（裝置 > 伺服器設定檔 > HTTP）。 • 設定 IP-Tag **Timeout**（逾時）以設定 IP 位址到頁籤對應維護的時間。將逾時設定為 0 代表著 IP-Tag 對應不會逾時（範圍為 0 到 43200（30 天）；預設值為 0）。 您只能使用 *Add Tag*（新增頁籤）動作設定連線逾時。 • 輸入或選取您要套用或從目標來源或目的地 IP 位址移除的 **Tags**（頁籤）。 • 整合—僅可用於 Azure 上的 VM 系列防火牆。此選項讓您可以用 **Azure-安全性-中心-整合行動**，將轉送選定的日誌到 Azure 安全性中心。 若要在日誌轉送設定檔篩選器基礎上新增裝置到隔離清單，請選取 **Quarantine**（隔離）。

© 2019 Palo Alto Networks, Inc.

Objects > Authentication（物件 > 驗證）

驗證強制執行物件可指定方法和服務，用於驗證存取您網路資源的一般使用者。您可將此物件指派給驗證政策規則，以在流量符合規則時叫用驗證方法和服務（請參閱 Policies > Authentication（政策 > 驗證））。

防火牆具有下列預先定義的唯讀驗證強制執行物件：

- **default-browser-challenge**—防火牆會以透明方式取得使用者驗證認證。如果選取此動作，您必須在設定驗證入口網站時啟用 Kerberos 單一登入 (SSO) 或 NT LAN Manager (NTLM) 驗證。如果 Kerberos SSO 驗證失敗，防火牆將會回復至 NTLM 驗證。如果您未設定 NTLM，或 NTLM 驗證失敗，防火牆會回復至在預先定義的 **default-web-form** 物件中指定的驗證方法。
- **default-web-form**—若要驗證使用者，防火牆會使用您在設定驗證入口網站時指定的憑證設定檔或驗證設定檔。如果您指定了驗證設定檔，防火牆會忽略設定檔中的任何 Kerberos SSO 設定，並對使用者顯示驗證入口網站頁面以輸入驗證認證。
- **default-no-captive-portal**—防火牆會評估安全性原則，但不驗證使用者。

在建立自訂驗證強制執行物件前：

- ❑ 設定伺服器設定檔，以指定如何連線至驗證伺服器（請參閱 Device > Server Profiles（裝置 > 伺服器設定檔））。
- ❑ 將伺服器設定檔指派給可指定 Kerberos 單一登入參數等驗證設定的驗證設定檔（請參閱 Device > Authentication Profile（裝置 > 驗證設定檔））。

若要建立自訂驗證強制執行物件，請按一下 **Add**（新增）並完成下列欄位：

驗證強制執行設定	說明
名稱	輸入描述性名稱（最多 31 個字元），協助您在定義驗證規則時識別物件。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
已共用（僅限 Panorama）	若您想讓以下對象使用物件，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用物件。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用物件。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此驗證執行物件的裝置群組中取代該物件的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此物件之任何設備群組的設定。
驗證方法	選取方法： • **browser-challenge**—防火牆會以透明方式取得使用者驗證認證。若選取此動作，則選取的 **Authentication Profile**（驗證設定檔）必須啟用 Kerberos SSO。 • **web-form**—若要驗證使用者，防火牆會使用您在設定驗證入口網站時指定的憑證設定檔，或您在驗證執行物件中選取的 **Authentication Profile**（驗證設定檔）。如果您選取 **Authentication Profile**（驗證設定檔），防火牆會忽略設定檔中的 Kerberos SSO 設定，並對使用者顯示「驗證入口網站」頁面以輸入驗證認證。 • **no-captive-portal**—防火牆會評估安全性原則，但不驗證使用者。
驗證設定檔	選取驗證設定檔，以指定要用於驗證使用者身分的服務。

© 2019 Palo Alto Networks, Inc.

驗證強制執行設定	說明
訊息	輸入相關指示，告知使用者如何回應其流量觸發驗證規則時所看到的第一個驗證挑戰。此訊息顯示在 **Authentication Portal Comfort Page**（驗證入口網站登入頁面）中。如果您未輸入訊息，則會顯示預設 **Authentication Portal Comfort Page**（驗證入口網站登入頁面）（請參閱 Device > Response Pages（裝置 > 回應頁面））。 防火牆只會對您在 *Authentication Profile*（驗證設定檔）的 *Authentication*（驗證）頁籤中定義的第一個驗證挑戰（因素）顯示 *Authentication Portal Comfort Page*（驗證入口網站登入頁面）（請參閱 Device > Authentication Profile（裝置 > 驗證設定檔））。對於您在防火牆的 *Factors*（因素）頁籤中定義的多因素驗證 *(MFA)* 挑戰，防火牆會顯示 *MFA Login Page*（*MFA* 登入頁面）。

© 2019 Palo Alto Networks, Inc.

物件 > 解密設定檔

解密設定檔讓您可封鎖並控制您已為解密指定的 SSL 和 SSH 流量的特定方面，以及您已明確排除解密的流量。在您建立解密設定檔之後，您接著可以將該設定檔新增至解密政策；根據設定檔設定，將會另外強制執行符合解密政策的任何流量。

預設解密設定檔會在防火牆上設定，且會自動包含在新的解密政策中（您無法修改預設解密設定檔）。按一下 **Add**（新增）來建立新解密設定檔，或選取現有設定檔以 **Clone**（複製）或修改它。

您想了解什麼內容？	請參閱：
新增伺服器設定檔。 啟用解密流量的連接埠鏡像。	解密設定檔一般設定
封鎖和控制已解密的 SSL 流量。	用以控制已解密 SSL 流量的設定
封鎖和控制您已排除解密的流量（例如，歸類為醫療保健或金融服務的流量）。	用以控制未解密流量的設定
封鎖和控制已解密的 SSH 流量。	用以控制已解密 SSH 流量的設定

解密設定檔一般設定

下表描述解密設定檔的一般設定。

解密設定檔—一般設定	說明
名稱	輸入設定檔名稱（最多 **31** 個字元）。當定義解密原則時，此名稱會顯示在解密設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
已共用（僅限 Panorama）	若您想讓以下對象使用設定檔，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用設定檔。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用設定檔。
停用覆寫（僅限 Panorama）	若要防止管理員在繼承設定檔的裝置群組中取代此解密設定檔的設定，請選取此選項。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。
解密鏡像介面 （支援除 AWS、Azure、NSX edition 和 Citrix SDX 上的 VM-Series 防火牆外的所有型號。）	選取要用於解密連接埠鏡像的 **Interface**（介面）。 您必須先取得解密連接埠鏡像授權、安裝授權並重新啟動防火牆，才可啟用解密連接埠鏡像。

© 2019 Palo Alto Networks, Inc.

解密設定檔—一般設定	說明
僅限轉送 （支援除 AWS、Azure、NSX edition 和 Citrix SDX 上的 VM-Series 防火牆外的所有型號。）	若您只想在安全性原則強制執行之後鏡像解密流量，請選取 **Forwarded Only**（僅限轉送）。透過此選項，便能僅鏡像透過防火牆轉送的流量。如果您正將解密的流量轉送至其他威脅偵測裝置，例如 DLP 裝置或其他入侵防禦系統 (IPS)，此選項十分有幫助。若您清除此選項（預設設定），防火牆會在查閱安全性原則前將所有解密的流量鏡像到介面，讓您能夠重播事件並分析會產生威脅或觸發丟棄動作的流量。

用以控制已解密流量的設定

下表說明您可用來控制使用正向 Proxy 解密或輸入檢查所解密防火牆流量的設定（包括「SSL 通訊協定設定」頁籤）。您可使用這些設定來根據以下條件限制或封鎖 TLS 工作階段，包括：外部伺服器憑證的狀態、使用未受支援的加密套件或通訊協定版本，或系統資源處理解密的可用性。

SSL 解密頁籤設定	說明
SSL 正向代理程式頁籤 選取選項來限制或封鎖使用正向 Proxy 解密的 TLS 流量。	
伺服器憑證驗證—選取選項來控制解密流量的伺服器憑證。	
封鎖憑證過期的工作階段	如果伺服器憑證過期，則終止 TLS 連線。這會使得使用者無法接受過期的憑證，並且無法繼續進行 TLS 工作階段。 封鎖到期憑證的工作階段，以免存取可能不安全的網站。
封鎖發行者不受信任的工作階段	如果伺服器憑證簽發者不受信任，則終止 TLS 工作階段。 封鎖簽發者不受信任的工作階段，因為不受信任的簽發者可能會指出媒介攻擊、重播攻擊或其他攻擊。
封鎖包含未知憑證狀態的工作階段	若伺服器傳回「未知」憑證撤銷狀態，則終止 TLS 工作階段。憑證撤銷狀態會指示是否已撤銷憑證信任。 封鎖包含未知憑證狀態的工作階段，以獲得最嚴格的安全性。但是，由於憑證狀態可能由於各種原因而未知，因此可能會過度加強安全性。若封鎖未知憑證狀態會影響您需要用於業務的網站，請勿封鎖包含未知憑證狀態的工作階段。
封鎖憑證狀態檢查逾時的工作階段	若無法在防火牆設定要停止等候憑證狀態服務回應的時間內擷取憑證狀態，則終止 TLS 工作階段。您可以在建立或修改憑證設定檔時（**Device**（裝置）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔））設定 **Certificate Status Timeout**（憑證狀態逾時）值。 在狀態檢查逾時時封鎖工作階段是一種更嚴格的安全性與更好的使用者體驗之間的權衡。若憑證撤銷伺服器回應緩慢，則逾時封鎖可能會封鎖具有有效憑證的網

© 2019 Palo Alto Networks, Inc.

SSL 解密頁籤設定	說明
	站。若您擔憂有效憑證逾時，則可增加憑證撤銷檢查 (CRL) 與線上憑證狀態通訊協定 (OCSP) 的逾時值。
限制憑證延伸	將動態伺服器憑證中使用的憑證延伸限制於金鑰使用及延伸金鑰使用。 若部署不需要其他憑證延伸，則限制憑證延伸。
附加憑證的 CN 值到 SAN 擴展上	啟用防火牆以新增主旨替代名稱 (SAN) 擴展，模擬其作為正向 Proxy 解密一部分呈現給用戶端的驗證。當伺服器驗證僅包含常用名稱（CN）時，防火牆會依據伺服器驗證 CN 新增 SAN 擴展至模擬驗證。 此選項在瀏覽器需要伺服器驗證以使用 SAN 時十分有用，且不再支援依據 CN 的驗證比對；它確保終端用戶可繼續存取他們需要的網路資源，且防火牆可繼續解密工作階段，就算伺服器僅含一個 CN 也一樣。 將憑證的 *CN* 值附加至 *SAN* 延伸，可幫助確保存取要求的網路資源。
不受支援模式檢查—選取選項可控制不受支援的 TLS 應用程式。	
封鎖非支援版本的工作階段	若 PAN-OS 不支援「用戶端 hello」訊息，終止工作階段PAN-OS 支援 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2 和 TLSv1.3。 始終封鎖非支援版本的工作階段，以免存取具有弱通訊協定的網站。在 *SSL Protocol Settings*（*SSL* 通訊協定設定）頁籤上，將通訊協定最低版本設定為 *TLSv1.2*，以封鎖具有弱通訊協定版本的網站。若出於業務目的而需要存取的網站使用較弱的通訊協定，請建立一個允許較弱通訊協定的單獨解密設定檔，並在解密原則規則中進行指定，而該規則僅套用於您必須允許較弱通訊協定的網站。
封鎖加密套件不受支援的工作階段	如果 PAN-OS 不支援 TLS 交握中指定的加密套件，則終止工作階段。 封鎖使用不受支援之加密套件的工作階段。您可在 *SSL Protocol Settings*（*SSL* 通訊協定設定）頁籤上設定允許的加密套件（加密演算法）。不允許使用者連接到具有弱加密套件的網站。
封鎖具有用戶端驗證的工作階段	以正向 Proxy 流量的用戶端驗證終止工作階段。 除非有重要的應用程式需要工作階段，否則封鎖具有用戶端驗證的工作階段，在這個狀況下您應建立單獨的解密設定檔，並僅套用於需要用戶端驗證的流量上。
失敗檢查—選取沒有系統資源可處理解密時所採取的動作。	
若資源不可用則封鎖工作階段	如果沒有系統資源可處理解密，終止工作階段。 是否在資源不可用時封鎖工作階段，是一種更嚴格的安全性與更好的使用者體驗之間的權衡。若您未在資源不可用時封鎖工作階段，則在資源受到影響時，防火

© 2019 Palo Alto Networks, Inc.

SSL 解密頁籤設定	說明
	牆將無法解密您要解密的流量。但是，在資源不可用時封鎖工作階段會影響使用者體驗，因為通常可存取的網站可能暫時無法存取。
若 HSM 不可用則封鎖工作階段	如果無法使用硬體安全性模組 (HSM) 來簽署憑證，則終止工作階段。 若 HSM 不可用，是否封鎖工作階段取決於私密金鑰必須來自何處的相關合規性規則；以及若 HSM 不可用，您希望如何處理加密流量。
在沒有資源的情況下阻止降級	如果系統資源不可用於處理 TLSv1.3 交握（而非降級至 TLSv1.2），則會終止工作階段。 是否在資源不可用時封鎖工作階段，是一種更嚴格的安全性與更好的使用者體驗之間的權衡。如果您在 TLSv1.3 資源不可用時阻止將交握降級至 TLSv1.2，則防火牆會刪除工作階段。如果您不阻止降級交握，則在 TLSv1.3 交握資源不可用時，防火牆會降級為 TLSv1.2。
用戶端延伸	
除去 ALPN	防火牆預設處理和檢查 HTTP/2 流量。但是，您可以透過為防火牆指定 **Strip ALPN**（除去 **ALPN**）來停用 HTTP/2 檢查。選取此選項後，防火牆將移除應用程式層通訊協定交涉 (ALPN) TLS 延伸中包含的任何值。 由於 ALPN 用於保護 HTTP/2 連線安全，因此當沒有為此 TLS 延伸指定任何值時，防火牆會將 HTTP/2 流量降級為 HTTP/1.1 或將其分類為未知 TCP 流量。

對於不支援的模式及失敗模式，會將工作階段快取 *12* 小時，以便相同主機與伺服器配對之間未來的工作階段不解密。啟用選項可改為封鎖這些工作階段。

SSL 輸入檢查頁籤

選取選項來限制或封鎖使用輸入檢查解密的流量。

不受支援模式檢查—選取選項以在 TLS 流量中偵測到不受支援的模式時控制工作階段。

封鎖非支援版本的工作階段	若 PAN-OS 不支援「用戶端 hello」訊息，終止工作階段PAN-OS 支援 SSLv3、TLSv1.0、TLSv1.1、TLSv1.2 和 TLSv1.3。 始終封鎖非支援版本的工作階段，以免存取具有弱通訊協定的網站。在 *SSL Protocol Settings*（*SSL* 通訊協定設定）頁籤上，將通訊協定最低版本設定為 *TLSv1.2*，以封鎖具有弱通訊協定版本的網站。若出於業務目的而需要存取的網站使用較弱的通訊協定，請建立一個允許較弱通訊協定的單獨解密設定檔，並在解密原則規則中進行指定，而該規則僅套用於您必須允許較弱通訊協定的網站。
封鎖加密套件不受支援的工作階段	如果 PAN-OS 不支援使用的加密套件，終止工作階段。 封鎖使用不受支援之加密套件的工作階段。您可在 *SSL Protocol Settings*（*SSL* 通訊協定設定）頁籤上設定允許的加密套件（加密演算法）。不允許使用者連接到具有弱加密套件的網站。

© 2019 Palo Alto Networks, Inc.

SSL 解密頁籤設定	說明
失敗檢查—選取沒有系統資源時所需採取的動作。	
若資源不可用則封鎖工作階段	如果沒有系統資源可處理解密，終止工作階段。 是否在資源不可用時封鎖工作階段，是一種更嚴格的安全性與更好的使用者體驗之間的權衡。若您未在資源不可用時封鎖工作階段，則在資源受到影響時，防火牆將無法解密您要解密的流量。但是，在資源不可用時封鎖工作階段會影響使用者體驗，因為通常可存取的網站可能暫時無法存取。
若 HSM 不可用則封鎖工作階段	如果無法使用硬體安全性模組 (HSM) 來解密工作階段金鑰，則終止工作階段。 若 HSM 不可用，是否封鎖工作階段取決於私密金鑰必須來自何處的相關合規性規則；以及若 HSM 不可用，您希望如何處理加密流量。
在沒有資源的情況下阻止降級	如果系統資源不可用於處理 TLSv1.3 交握（而非降級至 TLSv1.2），則會終止工作階段。 是否在資源不可用時封鎖工作階段，是一種更嚴格的安全性與更好的使用者體驗之間的權衡。如果您在 TLSv1.3 資源不可用時阻止將交握降級至 TLSv1.2，則防火牆會刪除工作階段。如果您不阻止降級交握，則在 TLSv1.3 交握資源不可用時，防火牆會降級為 TLSv1.2。
SSL 通訊協定設定頁籤 選取下列設定以針對 TLS 工作階段流量強制執行通訊協定版本及加密套件。	
通訊協定版本	針對 TLS 工作階段強制使用通訊協定的最低及最高版本。
最低版本	設定可用來建立 TLS 連線的最低通訊協定版本。 將最低版本設定為 *TLSv1.2* 以提供最強安全性。檢閱不支援 *TLSv1.2* 的網站，以查看其是否確實具有合法的業務目的。對於您需要存取且不支援 *TLSv1.2* 的網站，請建立一個單獨的解密設定檔，指定其支援的最強通訊協定版本，並將其套用於解密原則規則，而該規則將弱版本的使用限制為僅限來自必要來源（區域、位址、使用者）的必要網站。
最高版本	設定可用來建立 TLS 連線的最高通訊協定版本。您可選取 [最高] 選項，不指定最高版本；在此情況下，通訊協定版本等於或高於所選的最低支援版本。 將最高版本設定為 *Max*（最高），從而隨著通訊協定的改進，防火牆會自動對其提供支援。 然而，如果您的解密政策支援行動應用程式（其中許多使用釘選的憑證），請將 *Max Version*（最大版本）設定為 *TLSv1.2*。由於 *TLSv1.3* 會加密在之前的 *TLS* 版本中未加密的憑證資訊，防火牆無法基於憑證資訊自動新增解密排除項，這會影響一些行動應用程式。因此，如果您啟用 *TLSv1.3*，防火牆可能會丟棄一些行動應用程式流量，除非您為該流量建立「不解密」原則。如果您瞭解出於業務目的而使用的行動應用程式，請考慮為這些應用程式建立單獨的解密原則和設定檔，以便您可以為所有其他流量啟用 *TLSv1.3*。

© 2019 Palo Alto Networks, Inc.

SSL 解密頁籤設定	說明
金鑰交換演算法	針對 TLS 工作階段強制使用所選的金鑰交換演算法。 預設會啟用所有三種演算法（**RSA**、**DHE** 和 **ECDHE**）。**DHE** (Diffie-Hellman) 與 **ECDHE** (elliptic curve Diffie-Hellman) 為正向 Proxy 或輸入檢查解密啟用 Perfect Forward Secrecy (PFS)（完美轉送密碼 (PFS)）。
加密演算法	針對 TLS 工作階段強制使用所選的加密演算法。 不支援弱 *3DES* 或 *RC4* 加密演算法。（當您使用 *TLSv1.2* 或更高版本作為通訊協定最低版本時，防火牆會自動封鎖這兩種演算法。）若您必須建立例外情況並支援較弱的通訊協定版本，請在解密設定檔中取消核取 *3DES* 與 *RC4*。若出於業務目的而必須存取的網站使用了 *3DES* 或 *RC4* 加密演算法，請建立單獨的解密設定檔並將其套用於僅適用於這些網站的解密原則規則。
驗證演算法	針對 TLS 工作階段強制使用所選的驗證演算法。 封鎖舊的弱 *MD5* 演算法（預設為封鎖）。若無必要網站使用 *SHA1* 驗證，則封鎖 *SHA1*。若出於業務目的而需要存取的任何網站使用了 *SHA1*，請建立單獨的解密設定檔並將其套用於僅適用於這些網站的解密原則規則。

用以控制未解密流量的設定

在已使用 **No Decryption**（不解密）動作設定解密原則（**Policies**（原則）> **Decryption**（解密）> **Action**（動作）），且流量符合該原則的情況下，您可使用 **No Decryption**（不解密）頁籤以啟用設定來封鎖該流量。使用這些選項來控制工作階段的伺服器憑證，雖然防火牆不會解密及檢驗工作階段流量。

不解密頁籤設定	說明
封鎖憑證過期的工作階段	如果伺服器憑證過期，終止 SSL 連線。這會使得使用者無法接受過期的憑證，並且無法繼續進行 SSL 工作階段。 封鎖到期憑證的工作階段，以免存取可能不安全的網站。
封鎖發行者不受信任的工作階段	如果伺服器憑證簽發者不受信任，終止 SSL 工作階段。 封鎖簽發者不受信任的工作階段，因為不受信任的簽發者可能會指出媒介攻擊、重播攻擊或其他攻擊。

用以控制已解密 SSH 流量的設定

下表說明您可用來控制解密輸入及輸出 SSH 流量的設定。這些設定可讓您根據以下條件限制或封鎖 SSH 通道流量，包括：使用未受支援的演算法、偵測 SSH 錯誤，或處理 SSH Proxy 解密的資源可用性。

© 2019 Palo Alto Networks, Inc.

SSH Proxy 頁籤設定	說明
不受支援模式檢查—使用這些選項，在 SSH 流量中偵測到不受支援的模式時控制工作階段。支援的 SSH 版本是 SSH 第 2 版。	
封鎖非支援版本的工作階段	如果 PAN-OS 不支援「用戶端 hello」訊息，終止工作階段。 始終封鎖非支援版本的工作階段，以免存取具有弱通訊協定的網站。在 *SSL Protocol Settings*（*SSL* 通訊協定設定）頁籤上，將通訊協定最低版本設定為 *TLSv1.2*，以封鎖具有弱通訊協定版本的網站。若出於業務目的而需要存取的網站使用較弱的通訊協定，請建立一個允許較弱通訊協定的單獨解密設定檔，並在解密原則規則中進行指定，而該規則僅套用於您必須允許較弱通訊協定的網站。
封鎖演算法不受支援的工作階段	如果 PAN-OS 不支援用戶端或伺服器所指定的演算法，終止工作階段。 始終封鎖演算法不受支援的工作階段，以免存取使用弱演算法的網站。
失敗檢查—選取發生 SSH 應用程式錯誤及沒有系統資源時所需採取的動作。	
發生 SSH 錯誤時封鎖工作階段	如果發生 SSH 錯誤，終止工作階段。
若資源不可用則封鎖工作階段	如果沒有系統資源可處理解密，終止工作階段。 是否在資源不可用時封鎖工作階段，是一種更嚴格的安全性與更好的使用者體驗之間的權衡。若您未在資源不可用時封鎖工作階段，則在資源受到影響時，防火牆將無法解密您要解密的流量。但是，在資源不可用時封鎖工作階段會影響使用者體驗，因為通常可存取的網站可能暫時無法存取。

© 2019 Palo Alto Networks, Inc.

Objects > Decryption > Forwarding Profile（物件>解密>轉送設定檔）

您可以設定解密轉送設定檔以啟用防火牆作為 decryption broker（解密代理程式）動作。解密代理程式防火牆轉送已解密且已檢測至安全鍊的流量—一組內嵌的第三方安全性設備—在其他強制執行時使用。您還可以設定防火牆為安全鏈提供工作階段散布，以確保安全鏈設備不會超額訂閱。當防火牆從安全鏈接收回流量時，防火牆會重新加密流量並將其轉送到適當的目的地。

在建立解密轉送設定檔以啟用解密代理之前，您必須：

- 啟用 Ssl 正向 代理程式 解密。
- 在防火牆上至少分配兩個 Lay 4 介面，用於將解密流量轉送到安全鏈（選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）、編輯介面，選取 **Advanced**（進階）> **Other Info**（其他資料），然後啟用解密轉送）。重覆此工作以啟用第二個介面作為解密轉送介面使用。

在您完成這些工作後，建立一個解密轉送設定檔以將兩個介面配對，並為防火牆將轉送解密流量的安全鍊定義設定。

參閱 Decryption Broker（解密代理程式）以了解更多有關支援解密代理程式與安全鍊部署，以及啟用防火牆作為解密代理程式動作的整體工作流程。

解密轉送設定	說明
名稱	給設定檔一個說明性的名稱。
說明	可選擇說明設定檔設定。
一般頁籤	
安全鍊類型	選擇防火牆轉送解密流量的安全鍊類型： • 路由的（**Layer 3**）：此類安全鏈中的設備使用 Layer 3 介面連接到安全鍊網路—每個介面必須具有指派的 IP 位址和子網遮罩。安全鏈設備設定有靜態路由（或動態路由），將直接輸入和輸出流量引導到安全鏈中的下一個設備並返回到防火牆。 • 透明橋接：在透明橋接安全鍊網絡中，所有安全鏈設備都設定有兩個連接到安全鍊網路的介面。這兩個數據平面介面設定為透明橋接模式；他們沒有指派的 IP 地址、子網遮罩、預設閘道或本機路由表。透明橋接模式下的安全鏈設備在一個介面上接收流量，然後在流量流出下一個內嵌安全鏈設備的路徑之前分析和執行流量。
流量方向	指定防火牆如何透過安全鏈指導解密的輸入和輸入工作階段：在相同方向（單向）或相反方向（雙向）。您選擇的流向取決於構成安全鏈的設備類型。例如，如果安全鏈包含可以檢查工作階段兩端的無狀態設備，則可以選擇單向。
主要介面	選擇防火牆將用來轉送流量到安全鍊的主要和次要介面。主要和次要介面一起形成一對解密轉送介面。僅您設定為解密轉送介面的介面會顯示。
次要介面	
安全鍊頁籤	
啟用	啟用安全鍊。

© 2019 Palo Alto Networks, Inc.

解密轉送設定	說明
名稱	給安全鍊一個說明性的名稱。
首台設備 最近使用設備	選擇安全鏈中第一個設備的 IPv4 位址和最後一個設備，或者定義一個新的位址物件以輕鬆引用設備。
工作階段散佈方式	在轉送到多個路由（Layer 3）安全鏈時，請選擇防火牆將用於在安全鏈之間散布解密工作階段的方法： • **IP** 模數—防火牆根據來源和目的地 IP 位址的模組雜湊指派工作階段。 • **IP** 雜湊—防火牆根據來源和目的地 IP 位址和連接埠數量的IP 雜湊指派工作階段。 • 循環配置資源—防火牆在安全鍊中平均配置工作階段。 • 最低的延遲—防火牆以最低延遲為安全鏈分配更多工作階段。為使此方法按預期工作，您還必須啟用延遲監視和 HTTP 監視（選取 **Health Monitor**（健康情況監控））。
健康情況監控頁籤	
在生命檢查錯誤上	如果與此解密轉送設定檔關聯的所有安全鏈未通過健康狀況檢查，則防火牆選擇 **Bypass Security Chain**（繞過安全鏈）（允許工作階段流量）或 **Block Session**（阻止會話）。 這表示當解密設定檔配定多個安全鏈時，如果單個安全鏈無法執行運行狀況檢查，則防火牆將根據 **Security Chains**（安全鏈）頁籤上指定的方法在剩餘的健康安全鏈中執行工作階段散布—它僅依據在每個安全鍊都失敗事件中的設定封鎖或允許此流量。
健康情況檢查失敗條件	將健康檢查失敗定義為符合任何健康監視條件（**OR Condition**（OR 條件））或滿足所有條件（**AND Condition**（AND 條件））的事件。
路徑監控 延遲監視 HTTP 監視	啟用路徑、延遲或 HTTP 監視或三者的任意組合來識別安全鏈何時未有效處理解密流量。對於您啟用的每種監視類型，定義觸發健康檢查失敗的時間長和計數。 啟用： • 路徑監視以檢查設備連線。 • 延遲監視可以檢查設備處理速度和效率。 • HTTP 監視來檢查設備可用性和回應時間。

© 2019 Palo Alto Networks, Inc.

Objects > SD-WAN Link Management（物件 > SD-WAN 連結管理）

建立設定檔以套用至 SD-WAN 政策規則中指定的應用程式和服務集。每種設定檔類型控制 SD-WAN 連結管理的各個方面。

- Objects > SD-WAN Link Management > Path Quality Profile（物件 > SD-WAN 連結管理 > 路徑品質設定檔）
- Objects > SD-WAN Link Management > SaaS Quality Profile（物件 > SD-WAN 連結管理 > SaaS 品質設定檔）
- Objects > SD-WAN Link Management > Traffic Distribution Profile（物件 > SD-WAN 連結管理 > 流量散佈-設定檔）
- Objects > SD-WAN Link Management > Error Correction Profile（物件 > SD-WAN 連結管理 > 錯誤連線設定檔）

Objects > SD-WAN Link Management > Path Quality Profile（物件 > SD-WAN 連結管理 > 路徑品質設定檔）

SD-WAN 可讓您為具有獨特網路品質要求的每組應用程式、應用程式篩選器、應用程式群組、服務、服務物件和服務群組物件建立一個路徑品質設定檔，然後在 SD-WAN 政策規則中參照該設定檔。在該設定檔中，設定三個參數的最大閾值：延遲、抖動和封包遺失。當 SD-WAN 連結超出任何一個閾值時，防火牆會為符合套用此設定檔之 SD-WAN 規則的封包選取新的最佳路徑。

每個路徑品質參數的敏感度設定可讓您指示防火牆，對於該設定檔套用至應用程式，哪個參數更為重要（偏好）。相比中等或低設定，防火牆會將更多重要性放置在具有高設定的參數上。例如，一些應用程式對封包遺失的敏感度比對抖動或延遲的敏感度高，因此，您可以將封包遺失設為高敏感度，這會導致防火牆先檢查封包遺失。

如果您讓延遲、抖動和封包遺失的敏感度設定保留為預設設定（中等），或者如果您將三個參數都設定為相同的設定，設定檔的優先順序依次是封包遺失、延遲和抖動。

預設情況下，防火牆每 200 毫秒測量一次延遲和抖動，並取最後三個測量值的平均值來衡量滑動視窗中的路徑品質。您可在設定 SD-WAN 介面設定檔時選取積極或寬鬆的路徑監控來修改此行為。

	路徑品質設定檔設定
名稱	使用英數字元、底線、連字號、空格和句點來輸入路徑品質設定檔的名稱，最大長度為 31 個字元。
延遲 (ms)	**Threshold**（閾值）—輸入在超出閾值之前，允許封包離開防火牆、到達 SD-WAN 通道的另一端，然後返回一個回應封包到防火牆可花費的毫秒數（範圍是 10-2,000；預設值為 100）。
	Sensitivity（敏感度）—選取 **high**（高）、**medium**（中）或 **low**（低）（預設值為 **medium**（中））。
抖動 (ms)	**Threshold**（閾值）—輸入毫秒數（範圍是 10 至 1,000；預設值為 100）。
	Sensitivity（敏感度）—選取 **high**（高）、**medium**（中）或 **low**（低）（預設值為 **medium**（中））。

© 2019 Palo Alto Networks, Inc.

	路徑品質設定檔設定
封包遺失 (%)	**Threshold**（閾值）—輸入超出閾值前連結上封包遺失的百分比（範圍是 1-100.0；預設值為 1）。
	Sensitivity（敏感度）—封包遺失的敏感度設定無效，因此保留預設設定（**medium**（中））。

Objects > SD-WAN Link Management > SaaS Quality Profile（物件 > SD-WAN 連結管理 > SaaS 品質設定檔）

SD-WAN 允許您建立軟體即服務 (SaaS) 品質設定檔，以測量中樞或分支防火牆與伺服器端 SaaS 應用程式之間的路徑健康情況品質，從而準確地監控 SaaS 應用程式的可靠性，以及在路徑健康情況品質下降時交換路徑。這讓防火牆能夠準確地確定，何時容錯移轉至不同的直接網際網路存取 (DIA) 連結。

SaaS 品質設定檔允許您使用監控應用程式活動的自適應學習演算法，來指定要監控的 SaaS 應用程式，或者使用應用程式 IP 位址、FQDN 或 URL 來指定 SaaS 應用程式。

	SaaS 品質設定檔設定
名稱	使用英數字元、底線、連字號、空格和句點來輸入路徑品質設定檔的名稱。
已共用（僅限 Panorama）	選中（啟用）以使 SaaS 品質設定檔在所有裝置群組之間共用。
停用取代（僅限 Panorama）	選中（啟用）以停用在受管防火牆上本機取代 SaaS 品質設定檔設定的功能。
SaaS 監控模式	
適應性	監控 SaaS 應用程式工作階段活動的傳送和接收活動，並自動衍生路徑健康情況狀態，而無需在 SD-WAN 介面上進行任何其他健康情況檢查。預設會選中此選項。
靜態 IP 位址	**IP Address/Object**（**IP** 位址/物件）—指定 SaaS 應用程式以使用應用程式 IP 位址進行監控。 • **IP Address**（**IP** 位址）—SaaS 應用程式的 IP 位址。 • **Probe Interval (Sec)**（探查時間間隔（秒））—指定防火牆探查防火牆與 SaaS 應用程式之間路徑品質健康情況的時間間隔（秒）。預設值是 3 秒。 最多支援 4 個靜態 IP 地址。
	FQDN—指定 SaaS 應用程式以使用應用程式完全合格網域名稱 (FQDN) 進行監控。 • **FQDN**—SaaS 應用程式的 FQDN。您必須設定 FQDN 位址物件以指定 FQDN。 SaaS 應用程式 FQDN 必須可解析，以便成功監控 SaaS 應用程式。 • **Probe Interval (sec)**（探查時間間隔（秒））—指定防火牆探查分支防火牆與 SaaS 應用程式之間路徑品質健康情況的時間間隔（秒）。預設值是 3 秒。
HTTP/HTTPS	指定 SaaS 應用程式以使用 HTTP 或 HTTPS URL 進行監控。 • **Monitored URL**（受監控的 **URL**）—SaaS 應用程式的 HTTP 或 HTTPS URL。

© 2019 Palo Alto Networks, Inc.

	SaaS 品質設定檔設定
	• **Probe Interval (sec)**（探查時間間隔（秒））—指定防火牆探查防火牆與 SaaS 應用程式之間路徑品質健康情況的時間間隔（秒）。預設值是 3 秒。

Objects > SD-WAN Link Management > Traffic Distribution-Profile（物件 > SD-WAN 連結管理 > 流量散佈-設定檔）

對於此流量散佈設定檔，選取防火牆用於散佈工作階段並在路徑品質惡化時容錯移轉到更好的路徑的方法。新增連結標籤，防火牆在確定用於轉送 SD-WAN 流量的連結時需要考慮這些標籤。將流量散佈設定檔套用至您建立的每個 SD-WAN 政策規則。

	流量散佈設定檔
名稱	輸入流量散佈設定檔的名稱，可以使用英數字元、底線、連字號、空格和句點，最大長度為 31 個字元。
最佳可用路徑	如果不用考慮成本因素，您將允許應用程式使用分支之外的任何路徑，請選取「最佳可用路徑」。防火牆根據路徑品質指標來散佈流量以及容錯移轉到屬於清單中所有「連結標籤」的連結，從而為使用者提供最佳應用程式體驗。
自上而下優先順序	如果您有一些昂貴或低容量連結，只想將其用作最後手段或者備份連結，則可以選取「自上而下優先順序」方法，並將包含這些連結的標籤放在此設定檔中「連結標籤」清單的最後位置。防火牆會先使用清單最上面的連結標籤來確定工作階段載入流量的連結和容錯移轉的連結。如果第一個「連結標籤」中的所有連結均不合格，防火牆會從清單中的第二個「連結標籤」中選取一個連結。如果第二個連結標籤中的所有連結均不合格，該程序會視需要繼續，直到在最後一個連結標籤中找到合格的連結。如果所有關聯連結均超載，且沒有滿足品質閾值的連結，防火牆會使用「最佳可用路徑」方法來選取轉送流量的連結。 如果應用程式的抖動、延遲或封包遺失超過設定的閾值，則防火牆會在自上而下的連結標籤清單中的第一個開始，尋找容錯移轉至的連結。
加權工作階段散佈	如果您想要手動載入（符合規則的）流量到 ISP 和 WAN 連結，且在暫時低壓情況下不需要容錯移轉，請選取「加權工作階段散佈」。當套用新工作階段（使用單個標籤分組的介面將獲得這些工作階段）的靜態百分比時，可以手動指定連結的載入。對於對延遲不敏感的應用程式和需要大量連結頻寬容量（如大型分支備份和大型檔案移轉）的應用程式，可以選取此方法。請記住，如果連結出現暫時低壓，則防火牆不會將相符流量反映到其他連結。
連結標籤	新增希望防火牆在為此設定檔選擇的連結選取過程中考慮的「連結標籤」。如果您選擇「自上而下優先順序」方法，則標籤的順序很重要；使用「上移」或「下移」來變更標籤的順序。
加權	如果您選擇「加權工作階段散佈」方法，請輸入新增的每個「連結標籤」的百分比。百分比值之和必須等於 100%。

© 2019 Palo Alto Networks, Inc.

Objects > SD-WAN Link Management > Error Correction Profile（物件 > SD-WAN 連結管理 > 錯誤連線設定檔）

如果您的 SD-WAN 流量包含對封包遺失或損毀敏感的應用程式（例如音訊、VoIP 或視訊會議），則可套用正向錯誤更正 (FEC) 或封包複製作為錯誤更正方法。使用 FEC，接收防火牆（解碼器）可透過使用編碼器嵌入應用程式流中的同位檢查位元，來復原遺失或損毀的封包。封包複製是錯誤更正的另一種方法，其中應用程式工作階段從一個通道複製到第二個通道。兩種方法都需要額外的頻寬和 CPU 開銷。因此，僅將 FEC 或封包複製套用於可從此類方法中獲益的應用程式。若要採用這些方法之一，請建立一個錯誤更正設定檔，並在特定應用程式的 SD-WAN 政策規則中引用。

（您還必須透過在 SD-WAN 介面設定檔中指示介面 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格），來指定防火牆可用於選取哪些介面進行錯誤更正。）

	錯誤更正設定檔設定
名稱	為錯誤更正設定檔新增描述性名稱，最多使用 31 個英數字元。
共用	選取該項可將錯誤更正設定檔提供給 Panorama 上的所有裝置群組，以及向其推送設定的多重 vsys 中樞或分支上的每個虛擬系統。 Panorama 可存取在防火牆設定驗證中共用的錯誤更正設定檔，以及成功提交設定並將其推送至分支和中樞。如果 Panorama 無法引用錯誤更正設定檔，則提交失敗。
停用覆寫	若要防止管理員在繼承錯誤更正設定檔的裝置群組中取代此設定檔的設定，請選取此選項。（若選取 **Shared**（共用），則 **Disable override**（停用取代）不可用。）
啟動閾值（封包遺失百分比）	若封包遺失超過此百分比，則在套用錯誤更正設定檔的 SD-WAN 政策規則中，為設定的應用程式啟動 FEC 或封包複製。範圍為 1 至 99；預設為 2。
正向錯誤更正/封包複製	選取是使用正向錯誤更正 (FEC) 還是封包複製。封包複製比 FEC 需要更多的資源。
封包遺失更正比率	（僅正向錯誤更正）同位檢查位元與資料封包的比率。編碼器傳送至解碼器的同位檢查位元與資料封包的比率越高，解碼器可以修復封包遺失的可能性就越大。然而，比率越高，需要的備援就越多，因此需要更多的頻寬開銷，這是實現錯誤更正的權衡。選取其中一個預先定義的比率： • **10% (20:2)**（預設） • **20% (20:4)** • **30% (20:6)** • **40% (20:8)** • **50% (20:10)** 同位檢查比率套用於編碼防火牆的傳出流量。例如，如果中樞同位檢查比率為 50%，分支同位檢查比率為 20%，則中樞將獲得的流量比率為 20%，分支將獲得的流量比率為 50%。
復原持續時間（毫秒）	接收防火牆（解碼器）可以使用接收到的同位檢查封包，對遺失的資料封包執行封包復原所花費的最大毫秒數；範圍為 1 至 5,000；預設為 1,000。

© 2019 Palo Alto Networks, Inc.

	錯誤更正設定檔設定
	防火牆立即將接收的資料封包傳送至目的地。在資料區塊復原期間，防火牆對所有遺失的資料封包執行封包復原。若復原持續時間到期，則該區塊的關聯同位檢查位元將被捨棄。 編碼器將「復原持續時間」值傳送至解碼器；解碼器上的「復原持續時間」設定沒有影響。

© 2019 Palo Alto Networks, Inc.

Objects > Schedules（物件 > 排程）

依預設，安全性原則規則一律有效（所有日期及時間）。若要將安全性原則規則限制於特定時間內，您可以定義排程，然後將其套用至適當的原則。針對每個排程，您都可以指定固定日期與時間範圍，或週期性的每天或每週排程。若要將排程套用至安全性原則，請參考 [原則 > 安全性]。

定義的排程叫用安全性原則規則時，只有新的工作階段會受到套用的安全性原則規則所影響。現有的工作階段不會受到已排程原則所影響。

排程設定	說明
名稱	輸入排程名稱（最多 31 個字元）。定義安全性原則時，此名稱會顯示在排程清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
已共用（僅限 Panorama）	若您想讓以下對象使用排程，請選取此選項： • 多虛擬系統防火牆上的每個虛擬系統 (vsys)。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Virtual System**（虛擬系統）才可使用排程。 • Panorama 上的每個裝置群組。若您清除此選項，則僅有在 **Objects**（物件）頁籤中選取的 **Device Group**（裝置群組）才可使用排程。
停用覆寫（僅限 Panorama）	選取此選項，可防止管理員在繼承此排程的裝置群組中取代該排程的設定。預設會清除此選取項目，這表示管理員可以取代繼承此排程之任何裝置群組的設定。
週期性	選取排程類型（**Daily**（每天）、**Weekly**（每週）或 **Non-Recurring**（非週期性））。
每日	按一下 **Add**（新增），並以 24 小時制 (HH:MM) 指定 **Start Time**（開始時間）和 **End Time**（結束時間）。
每週	按一下 **Add**（新增），選取 **Day of Week**（一週中的一天），並以 24 小時制 (HH:MM) 指定 **Start Time**（開始時間）和 **End Time**（結束時間）。
非週期性	按一下 **Add**（新增）並指定 **Start Date**（開始日期）、**Start Time**（開始時間）、**End Date**（結束日期）和 **End Time**（結束時間）。

© 2019 Palo Alto Networks, Inc.

網路

下列主題說明防火牆網路設定。

> Network > Virtual Wires（網路 > Virtual Wire）
> 網路 > 介面
> Network > Virtual Routers（網路 > 虛擬路由器）
> Network > Zones（網路 > 區域）
> Network > VLANs（網路 > VLAN）
> 網路 > IPSec 通道
> 網路 > GRE 通道
> Network > DHCP（網路 > DHCP）
> Network > DNS Proxy（網路 > DNS Proxy）
> Network > QoS（網路 > QoS）
> Network > LLDP（網路 > LLDP）
> 網路 > 網路設定檔

網路 > 介面

防火牆介面（連接埠）允許防火牆連接其他網路設備，以及防火牆內的其他介面。下列主題說明介面類型及如何設定：

您想了解什麼內容？	請參閱
什麼是防火牆介面？	防火牆介面概要
我不太熟悉防火牆介面，想要知道防火牆介面有哪些元件？	防火牆介面通用建置組塊 PA-7000 Series 防火牆介面通用建置組塊
我已經熟悉防火牆介面，想要知道如何找到設定特定介面類型的資訊？	**實體介面 (Ethernet)** 旁接介面 HA 介面 Virtual Wire 介面 Virtual Wire 子介面 PA-7000 Series 第二層介面 PA-7000 Series 第二層子介面 PA-7000 Series 第三層介面 第三層介面 第三層子介面 日誌卡介面 日誌卡子介面 解密鏡像介面 彙總乙太網路 (AE) 介面群組 彙總乙太網路 (AE) 介面 **邏輯介面** Network > Interfaces > VLAN（網路 > 介面 > VLAN） Network > Interfaces > Loopback（網路 > 介面 > 回送） Network > Interfaces > Tunnel（網路 > 介面 > 通道） Network > Interfaces > SD-WAN（網路 > 介面 > SD-WAN）
想知道更多？	網路

防火牆介面概要

防火牆資料連接埠的介面組態允許流量進入與離開防火牆。Palo Alto Networks® 防火牆可以同時在多個部署中運作，因為您可以 Configure Interfaces（設定頁面）支援不同的部署。例如，您可以在防火牆上針對虛擬介接、第二層、第三層與旁接模式設定乙太網路介面。防火牆支援的介面有：

© 2019 Palo Alto Networks, Inc.

- 實體介面—防火牆支援兩種介質類型（銅線與光纖），它們能夠以不同的傳輸速率傳送與接收流量。您可以將 Ethernet 介面設為下列類型：旁接、高可用性 (HA)、日誌卡（介面與子介面）、解密鏡像、Virtual Wire（介面與子介面）、Layer 2（介面與子介面）、Layer 3（介面與子介面）及彙總 Ethernet。可用的介面類型與傳輸速度會視硬體型號而不同。
- 邏輯介面—包括虛擬區域網路 (VLAN) 介面、回送介面、通道介面及 SD-WAN 介面。您必須先設定實體介面，然後才能定義 VLAN、SD-WAN 或通道介面。

防火牆介面通用建置組塊

選取 **Network**（網路）> **Interfaces**（介面），以顯示及設定大多數介面類型通用的元件。

若想了解您在 *PA-7000 Series* 防火牆上設定介面時，或當您使用 *Panorama*™ 在任何防火牆上設定介面時，須使用哪些獨特或不同的元件，請參閱 PA-7000 系列防火牆介面通用建置組塊。

防火牆介面建置組塊	說明
介面（介面名稱）	介面名稱是預先定義的，無法變更。然而，您可以為子介面、彙總介面、VLAN 介面、回送介面、通道介面及 SD-WAN 介面附加數值尾碼。
介面類型	對於乙太網路介面（**Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）），您可以選取介面類型： • 旁接 • **HA** • **Decrypt Mirror**（解密鏡像）（支援除 VM-Series NSX、Citrix SDX、AWS 和 Azure 上的任何防火牆。） • **Virtual Wire** • 第 **2** 層 • 第 **3** 層 • 日誌卡（僅適用於 PA-7000 Series 防火牆） • **Aggregate Ethernet**（彙總乙太網路）
管理設定檔	選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的 **Management Profile**（管理設定檔）（**Network**（網路）> **Interfaces**（介面）> **<if-config** > **Advanced**（進階）> **Other Info**（其他資料）），讓您可用來在此介面上管理防火牆。
連結狀態	對於 Ethernet 介面，Link State（連結狀態）指示介面目前是否可存取，並可透過網路接收流量： • 綠色 — 已設定並開啟 • 紅色—已設定但停機或停用 • 灰色 — 未設定 將游標停在連結狀態上可顯示工具提示，以指出介面的連結速度與雙工設定。
IP 位址	（選用）設定 Ethernet、VLAN、回送或通道介面的 IPv4 或 IPv6 位址。對於 IPv4 位址，您也可以選取介面的位址模式（**Type**（類型））：**Static**（靜態）、**DHCP Client**（DHCP 用戶端）或 **PPPoE**。
虛擬路由器	將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 Network > Virtual Routers（網路 > 虛擬路由器））。選取 **None**（無）可從介面移除目前的虛擬路由器指派。

© 2019 Palo Alto Networks, Inc.

防火牆介面建置組塊	說明
頁籤（僅限子介面）	輸入子介面的 VLAN 頁籤 (1-4,094)。
VLAN	選取 **Network**（網路）> **Interfaces**（介面）> **VLAN**，並修改現有的 **VLAN** 或 **Add**（新增）新的 VLAN（請參閱 Network > VLANs（網路 > VLANs））。選取 **None**（無）可從介面移除目前的 VLAN 指派。若要在 Layer 2 介面之間啟用切換，或啟用透過 VLAN 介面的路由，必須設定 VLAN 物件。
虛擬系統	如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域	選取介面的 **Security Zone**（安全區域）（**Network**（網路）> **Interfaces**（介面）> **<if-config** > **Config**（組態）），或選取 **Zone**（區域）以定義一個新的。選取 **None**（無）可從介面移除目前的區域指派。
功能	對於 Ethernet 介面，此欄會指定下列功能是否啟用： DHCP 用戶端 DNS proxy 已啟用 GlobalProtect™ 閘道 連結彙總控制協定 (LACP) 連結層探索通訊協定 (LLDP) NDP 監控 Netflow 設定檔 服務品質 (QoS) 設定檔 SD-WAN
備註	說明介面功能或用途。

PA-7000 Series 防火牆介面通用建置組塊

下表說明當您設定 PA-7000 Series 防火牆上的介面時，或使用 Panorama 設定任何防火牆上的介面時，**Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）頁面上有哪些獨特或不同的元件。按一下 **Add Interface**（新增介面）可建立新介面，或選取現有介面（例如 ethernet1/1）以對其編輯。

在 *PA-7000 Series* 防火牆上，您必須在一個資料連接埠上設定 日誌卡介面。

© 2019 Palo Alto Networks, Inc.

PA-7000 Series 防火牆介面建置組塊	說明
插槽	選取介面的插槽號碼 (1-12)。只有 PA-7000 Series 防火牆有多個插槽。如果您使用 Panorama 為任何其他防火牆型號設定介面，請選取 **Slot 1**（插槽 **1**）。
介面（介面名稱）	選取與所選插槽關聯的介面名稱。

旁接介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

您可以使用旁接介面監控連接埠上的流量。

若要設定旁接介面，請按一下未設定的介面名稱（例如，ethernet1/1），並指定下列資訊。

旁接介面設定	設定位置	說明
介面名稱	乙太網路介面	介面名稱是預先定義的，無法變更。
備註		輸入介面的選取性說明。
介面類型		選取 **Tap**（旁接）。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 裝置 > 伺服器設定檔 > NetFlow）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
虛擬系統	**Ethernet Interface**（乙太網路介面）> 設定	如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取子介面的案全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
連結速度	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）	選取以 Mbps 為單位的介面速度（**10**、**100**或**1000**），或選取 **auto**（自動）讓防火牆自動決定速度。
連結雙工		選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態		選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。

HA 介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

每個高可用性 (HA) 介面都有一個特殊功能：一個介面用於組態同步與活動訊號，另一個介面用於同步狀態。如果啟用了主動/主動高可用性，則防火牆會使用第三個 HA 介面來轉送封包。

© 2019 Palo Alto Networks, Inc.

某些 *Palo Alto Networks* 防火牆包含在 *HA* 部署中專用的實體連接埠（一個用於控制連結，一個用於資料連結）。對於不包含專用連接埠的防火牆而言，您必須指定將用於 *HA* 的資料連接埠。如需 *HA* 的其他資訊，請參考 *[設備 > 虛擬系統]*。

若要設定 HA 介面，請按一下未設定的介面名稱（例如，ethernet1/1），並指定下列資訊。

HA 介面設定	說明
介面名稱	介面名稱是預先定義的，無法變更。
備註	輸入介面的選取性說明。
介面類型	選取 **HA**。
連結速度	選取以 Mbps 為單位的介面速度（**10**、**100**或**1000**），或選取 **auto**（自動）讓防火牆自動決定速度。
連結雙工	選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態	選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。

Virtual Wire 介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

虛擬介接將兩個 Ethernet 介面邏輯性地連結在一起，這可讓所有流量在介面之間通過，或只讓已選取 VLAN 標籤的流量在介面之間通過（無法使用其他交換或路由服務）。您也可以建立虛擬介接子介面，並根據 IP 位址、IP 範圍或子網路將流量分類。Virtual Wire 不需要變更相鄰網路設備。虛擬介接可使用兩個相同類型（都為通訊或都為光纖）的 Ethernet 介面，或使用一個銅線介面和一個光纖介面。

若要設定虛擬介接，請先決定要連結的兩種介面（**Network** > **Interfaces** > **Ethernet**）並如同下表說明來配置其設定。

若您正將現有介面用於虛擬介接，首先從任何相關聯的安全性區域中移除介面。

虛擬介接介面設定	設定位置	說明
介面名稱	乙太網路介面	介面名稱是預先定義的，無法變更。
備註		輸入介面的選取性說明。
介面類型		選取 **Virtual Wire**（虛擬介接）。
Virtual Wire	**Ethernet Interface**（乙太網路介面）> 設定	選取虛擬介接，或按一下 **Virtual Wire** 以定義一個新的（Network > Virtual Wires）。選取 **None**（無）可從介面移除目前的虛擬介接指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。

© 2019 Palo Alto Networks, Inc.

虛擬介接介面設定	設定位置	說明
安全性區域		選取介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
連結速度	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）	選取以 Mbps 為單位的特定介面速度或選取**auto**（自動）讓防火牆自動決定速度。虛擬介接的兩個介面必須同速。
連結雙工		選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。虛擬介接的兩個介面的傳輸模式必須相同。
連結狀態		選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。
啟用 LLDP	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **LLDP**	選取此選項可啟用介面的連結層探索通訊協定 (LLDP)。連結層上的 LLDP 功能，可發現相鄰裝置及其功能。
Profile		如果 LLDP 為啟用，請選取要指派給介面的 LLDP 設定，或按一下 **LLDP Profile**（**LLDP** 設定檔）建立新的設定檔（請參閱 [網路 > 網路設定檔 > LLDP 設定檔]）。選取 **None**（無）可設定防火牆使用全域預設值。
在 HA 被動狀態下啟用		若已啟用 LLDP，請選取以設定 HA 被動防火牆預先交涉 LLDP 及其端點，然後防火牆才會變為主動。 若已啟用 LLDP，請選取以設定 HA 被動防火牆，以使 LLDP 封包直接通過防火牆。

Virtual Wire 子介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

Virtual Wire (vwire) 子介面可讓您按 VLAN 標籤，或 VLAN 標籤和 IP 分類程式組合來區隔流量，將標記的流量指派給不同的區域和虛擬系統，然後為符合定義準則的流量強制安全性政策。

若要新增 Virtual Wire 介面 ，請為該介面選取列，按一下 **Add Subinterface**（新增子介面），然後指定下列資訊。

虛擬介接子介面設定	說明
介面名稱	唯讀 **Interface Name**（介面名稱）會顯示您所選 vwire 介面的名稱。在相鄰的欄位中，輸入用來識別子介面的數值尾碼 (1-9,999)。
備註	輸入子介面的選取性說明。
頁籤	輸入子介面的 VLAN Tag（頁籤）(0-4,094)。
Netflow 設定檔	如果您要匯出單向 IP 流量，亦即從 ingress 子介面周遊至 NetFlow 伺服器，請選取伺服器設定檔，或按一下 **Netflow Profile**（Netflow 設定檔）來定義新設定檔（請參閱 裝置 > 伺服器設定檔 > NetFlow）。選取 **None**（無）可從子介面移除目前的 NetFlow 伺服器指派。
IP 分類程式	按一下新增，輸入 IP 位址、IP 範圍或子網路，以分類此 vwire 子介面上的流量。

© 2019 Palo Alto Networks, Inc.

虛擬介接子介面設定	說明
Virtual Wire	選取 Virtual Wire，或按一下 **Virtual Wire** 以定義一個新的（請參閱Network > Virtual Wires（網路 > Virtual Wire））。選取 **None**（無）可從子介面移除目前的虛擬介接指派。
虛擬系統	如果防火牆支援多個虛擬系統，並已啟用該功能，請為子介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域	選取子介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從子介面移除目前的區域指派。

PA-7000 Series 第二層介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）以設定第二層介面。按一下未設定的介面名稱（例如，ethernet1/1），並指定下列資訊。

第二層介面設定	設定位置	說明
介面名稱	乙太網路介面	介面名稱是預先定義的，無法變更。
備註		輸入介面的選取性說明。
介面類型		選取 第二層介面。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
VLAN	**Ethernet Interface**（乙太網路介面）> 設定	若要切換第二層介面，或透過 VLAN 介面啟用路由，請選取現有 VLAN 或按一下 **VLAN** 定義新的 VLAN（請參閱 [網路 > VLAN]）。選取 **None**（無）可從介面移除目前的 VLAN 指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取介面的 **Security Zone**（安全性區域），或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
連結速度	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）	選取以 Mbps 為單位的介面速度（**10**、**100**或**1000**），或選取自動讓防火牆自動決定速度。
連結雙工		選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態		選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。
啟用 LLDP	**Ethernet Interface**（乙	選取此選項可啟用介面的連結層探索通訊協定 (LLDP)。連結層上的 LLDP 功能，可發現相鄰裝置及其功能。

© 2019 Palo Alto Networks, Inc.

第二層介面設定	設定位置	說明
設定檔	太網路介面）> **Advanced**（進階）> **LLDP**	如果 LLDP 為啟用，請選取要指派給介面的 LLDP 設定，或按一下 **LLDP Profile**（**LLDP** 設定檔）建立新的設定檔（請參閱 [網路 > 網路設定檔 > LLDP 設定檔]）。選取 **None**（無）可設定防火牆使用全域預設值。
在 HA 被動狀態下啟用		如啟用 LLDP，選取以讓 HA 被動防火牆預先交涉 LLDP 及其端點，防火牆才會變為主動。

PA-7000 Series 第二層子介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

針對每個設定為實體 Layer 2 介面的 Ethernet 連接埠，您可以為指派給連接埠接收之流量的每個 VLAN 標籤，定義其他邏輯 Layer 2 介面（子介面）。若要在 Layer 2 子介面之間切換，請將相同的 VLAN 物件指派給子介面。

若要設定 PA-7000 Series 第二層介面，請選取實體介面的列，然後按一下 **Add Subinterface**（新增子介面），並指定下列資訊。

第二層子介面設定	說明
介面名稱	唯讀介面名稱會顯示您所選實體介面的名稱。在相鄰的欄位中，輸入用來識別子介面的數值尾碼 (1-9,999)。
備註	輸入子介面的選取性說明。
頁籤	輸入子介面的 VLAN 頁籤 (1-4,094)。
Netflow 設定檔	如果您要匯出單向（亦即從進入子介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從子介面移除目前的 NetFlow 伺服器指派。
VLAN	若要切換第二層介面，或透過 VLAN 介面啟用路由，請選取 VLAN 或按一下 **VLAN** 定義新的 VLAN（請參閱 [網路 > VLAN]）。選取 **None**（無）可從子介面移除目前的 VLAN 指派。
虛擬系統	如果防火牆支援多個虛擬系統，並已啟用該功能，請為子介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域	選取子介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從子介面移除目前的區域指派。

PA-7000 Series 第三層介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

若要設定第三層介面，選取介面（例如，ethernet1/1），並指定下列資訊。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
介面名稱	乙太網路介面	介面名稱是預先定義的，無法變更。
備註		輸入介面的選取性說明。
介面類型		選取 第三層介面 。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
虛擬路由器	**Ethernet Interface**（乙太網路介面）> 设定	選取虛擬路由，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取子介面的案全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
連結速度	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）	選取以 Mbps 為單位的介面速度（**10**、**100** 或 **1000**），或選取 **Auto**（自動）。
連結雙工		選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態		選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。
管理設定檔	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **Other Info**（其他資訊）	選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU		以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（576 至 9,192；預設為 1,500）。如果防火牆任一側的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。
調整 TCP MSS		選取以調整最大區段大小 (MSS) 將任何標頭適應介面 MTU 位元組大小範圍。MTU 位元組大小減去 MSS 調整大小等於 MSS 位於組大小，該值視 IP 通訊協定而定： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）—範圍是 40 至 300；預設為 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）—範圍是 60 至 300；預設為 60。 使用這些設定可解決網路中的 **tunnel**（通道）需要較小 MSS 的情況。如果封包必須分段才能擁有大於 MMS 的位元組，則此設定可啟用調整。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
		封裝增加了標頭長度，因此有助於設定 MSS 調整大小，使 MPLS 標頭或擁有 VLAN 頁籤的通道流量等可支援該位元組。
Untagged Subinterface		指定未標記屬於此 Layer 3 介面的所有子介面。PAN-OS® 會按照封包目的地，選取未標記的子介面作為進入介面。如果目的地是未標記之子介面的 IP 位址，它會對應至子介面。這也表示，必須將反向傳輸的封包所用的來源位址，轉譯為未標記的子介面所用的 IP 位址。此分類機制的另一種影響是，所有多點傳送及廣播封包將指派給基礎介面，而非任何子介面。由於「先開啟最短的路徑」(OSPF) 使用多點傳送，因此防火牆在未標記的子介面上不支援它。
IP 位址 MAC 位址	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **ARP Entries**（**ARP** 項目）	若要新增一或多個靜態位址解析通訊協定 (ARP) 項目，請按一下 **Add**（新增），然後輸入 IP 位址及其相關聯的硬體 (MAC) 位址。若要刪除項目，請選取項目並按一下 **Delete**（刪除）。靜態 ARP 項目可減少 ARP 處理並防止指定位址發生攔截式攻擊。
IPv6 位址 MAC 位址	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **ND Entries**（**ND** 項目）	若要為芳鄰發現協定 (NDP) 新增芳鄰資訊，請按一下 **Add**（新增），然後輸入芳鄰的 IP 位址和 MAC 位址。
啟用 NDP Proxy	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **NDP Proxy**	選取以啟用介面的芳鄰發現協定 (NDP) Proxy。防火牆將回應要求清單中 IPv6 位址其 MAC 位址的 ND 封包。在 ND 回應中，防火牆會為介面傳送自己的 MAC 位址，透過回應所有目的地為這些位址的封包，指示其將用作 Proxy。 如果您使用網路首碼轉譯 IPv6 (NPTv6)，建議您選取 **Enable NDP Proxy**（啟用 **NDP Proxy**）。 如選取 **Enable NDP Proxy**（啟用 **NDP Proxy**），您可透過輸入搜尋字串並按一下 Apply Filter（套用篩選器）(→) 來篩選許多位址項目。
位址		按一下 **Add**（新增），輸入一個或多個 IPv6 位址、IP 範圍、IPv6 子網路，或防火牆將作為 NDP Proxy 的位址物件。理論上而言在這些位址中，某一個位址會與 NPTv6 中來源轉譯的位址相同。位址順序不重要。 如果該位址是子網路，防火牆會為子網路中所有的位址傳送 ND 回應，因此我們建議您也新增防火牆的 IPv6 芳鄰，然後選取 **Negate**（否定）來指示防火牆不要回應這些 IP 位址。
否定		選取位址的 **Negate**（否定）來防止該位址的 NDP Proxy。您可以否定所指定 IP 位址範圍或 IP 子網路的子集。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
啟用 LLDP	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **LLDP**	選取此選項可啟用介面的連結層探索通訊協定 (LLDP)。連結層上的 LLDP 功能，可發現相鄰裝置及其功能。
LLDP 設定檔		如果 LLDP 為啟用，請選取要指派給介面的 LLDP 設定，或按一下 **LLDP Profile**（**LLDP** 設定檔）建立新的設定檔（請參閱 [網路 > 網路設定檔 > LLDP 設定檔]）。選取 **None**（無）可設定防火牆使用全域預設值。
在 HA 被動狀態下啟用		若已啟用 LLDP，選取此選項可讓防火牆作為 HA 被動防火牆預先交涉 LLDP 及其端點，防火牆才會變為主動。
類型	**Ethernet Interface**（乙太網路介面）> **IPv4**	選取將 IPv4 位址類型指派給介面的方法： • **Static**（靜態）—您必須手動指定 IP 位址。 • **PPPoE** — 防火牆將針對 Ethernet 上的點對點通訊協定 (PPPoE) 使用介面。 • **DHCP Client**（**DHCP** 用戶端）—啟用介面做為動態主機組態通訊協定 (DHCP) 用戶端，並接收動態指派的 IP 位址。 *處於高可用性 (HA) 主動#主動組態的防火牆不支援 PPPoE 或 DHCP 用戶端。* 頁籤上顯示的選項會視所選的 IP 位址方式而不同。
設定	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **DDNS**	選取 **Settings**（設定）讓 DDNS 欄位可以設定。
啟用		啟用介面上的 DDNS。您必須先啟用 DDNS 才能對其進行設定。（如果您的 DDNS 組態未完成，您可以儲存它而不啟用它，這樣您就不會丟失部分組態。）
更新間隔（天數）		輸入防火牆傳送至 DDNS 伺服器的更新之間的間隔（以天數為單位），以更新對應到 FQDN 的 IP 位址（範圍為 1 到 30；預設值為 1）。 *在防火牆收到從 DHCP 伺服器為了介面傳送的新 IP 位址時還會更新 DDNS。*
憑證設定檔		建立憑證設定檔以驗證 DDNS 服務。DDNS 服務向防火牆提供由憑證授權單位 (CA) 發佈的憑證。
主機名稱		輸入在 DDNS 伺服器上註冊的介面的主機名稱（例如，host123.domain123.com 或 host123）。除了確認語法是使用 DNS 在網域名稱中允許的有效字元外，防火牆不會驗證主機名稱。
廠商		選取為此介面提供 DDNS 服務的 DDNS 廠商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1**

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
		如果您選取了防火牆指示會在特定日期前逐步淘汰的較舊版本的 *DDNS* 服務，請移至較新版本。 廠商名稱後面的 **Name**（名稱）以及 **Value**（數值）欄位是特定於廠商的。唯讀欄位會通知您防火牆用於連結 DDNS 服務的參數。設定其他欄位，例如 DDNS 服務向您提供的密碼，以及如果防火牆未從 DDNS 伺服器收到回應，防火牆使用的逾時。
IPv4 頁籤 - IP		新增在介面設定的 IPv4 位址，並選取它們。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
IPv6 頁籤 - IPv6		新增在介面設定的 IPv6 位址，並選取它們。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
顯示執行階段資訊		顯示 DDNS 註冊情況：DDNS 供應商、已解析的 FQDN 以及帶有星號 (*) 的對應的 IP 位址指示主要 IP 位址。每個 DDNS 供應商都有自己的返回代碼，用於指示主機名稱更新的狀態和返回日期，以便進行疑難排解。
IPv4 位址 **Type**（類型）= **Static**（靜態）		
ip	**Ethernet Interface**（乙太網路介面）> **IPv4**	按一下 **Add**（新增），然後執行下列其中一個步驟來指定靜態介面的 IP 位址與網路遮罩。 • 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：*ip_address/mask*（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 按一下 **Address**（位址）以建立類型為 **IP netmask**（IP 網路遮罩）的位址物件。 您可以為介面輸入多個 IP 位址。您的防火牆使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 若要刪除 IP 位址，請選取位址並按一下 **Delete**（刪除）。
IPv4 位址 **Type**（類型）= **PPPoE**		
啟用	**Ethernet Interface**（乙太網路介面）> **IPv4** > **PPPoE** > **General**（一般）	選取此選項可啟動 PPPoE 終止介面。
使用者名稱		輸入點對點連線的使用者名稱。
密碼/確認密碼		輸入使用者名稱的密碼和確認密碼。
顯示 PPPoE 用戶端執行階段資訊		（選用）開啟顯示了參數的對話方塊，防火牆會使用這些參數與網際網路服務提供者 (ISP) 交涉建立連線。特定的資訊視 ISP 而定。
驗證	**Ethernet Interface**（乙太網路介面）> **IPv4** > **PPPoE** >	為 PPPoE 通訊選取驗證通訊協定：**CHAP**（Challenge-Handshake 驗證通訊協定）、**PAP**（密碼驗證通訊協定）或預設的自動（讓防火牆決定通訊協定）。選取 **None**（無）可從介面移除目前的通訊協定指派。
靜態位址		執行下列其中一個步驟，來指定網際網路服務提供者指派的 IP 位址（無預設值）：

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
	Advanced（進階）	• 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：*ip_address/mask*（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 按一下 **Address**（位址）以建立類型為 **IP netmask**（IP 網路遮罩）的位址物件。 • 選取 **None**（無）可從介面移除目前的位址指派。
自動建立指向端點的預設路由		選取此選項可在連線時自動建立指向 PPPoE 端點的預設路由。
預設路由度量標準		（選用）針對防火牆與網際網路服務提供者之間的路由，輸入要與預設路由相關聯並用於選取路徑的路由度量標準（優先順序層級）（範圍是 1 至 65,535）。優先順序層級會隨著數值減少而增加。
存取集訊器		（選用）輸入防火牆連線之網際網路服務提供者端上的存取集訊器名稱（無預設值）。
服務		（選用）輸入服務字串（無預設值）。
被動		選取此選項可使用被動模式。在被動模式中，PPPoE 端點會等待存取集訊器傳送第一個框架。
IPv4 位址 **Type**（類型）= **DHCP**		
啟用	**Ethernet Interface**（乙太網路介面）> **IPv4**	選取此選項可在介面上啟動 DHCP 用戶端。
自動建立指向伺服器所提供之預設閘道的預設路由		選取此選項可自動建立預設路由，指向 DHCP 伺服器提供的預設閘道。
傳送主機名稱		選取以讓防火牆（作為 DHCP 用戶端）將介面的主機名稱（選項 12）傳送至 DHCP 伺服器。如果您傳送主機名稱，則在預設情況下，防火牆的主機名稱會是根據主機名稱欄位決定的。您可以傳送該名稱或輸入自訂主機名稱（最多 64 個字元，包括大寫和小寫字母、數字、句點、連字符和底線。
預設路由度量標準		針對防火牆與 DHCP 伺服器之間的路由，輸入要與預設路由相關聯並用於選取路徑的路由度量標準（優先順序層級）（範圍是 1 至 65,535，無預設值）。優先順序層級會隨著數值減少而增加。
顯示 DHCP 用戶端執行階段資訊		選取此選項可顯示接收自 DHCP 伺服器的所有設定，包括 DHCP 租用狀態、動態 IP 指派、子網路遮罩、閘道和伺服器設定（DNS、NTP、網域、WINS、NIS、POP3 和 SMTP）。
對介面啟用 IPv6	**Ethernet Interface**（乙太網路介面）> **IPv6**	選取此選項可在此介面上啟用 IPv6 定址。
介面 ID		以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明

位址		按一下 **Add**（新增），並為每個 IPv6 位址設定下列參數：
		• **Address**（位址）—輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立位址物件。
		• **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。
		• **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。
		• **Anycast**（任一傳播）—選取以包含最近節點中的路由。
		• **Send Router Advertisement**（傳送路由器公告）—選取此選項可啟用此 IP 位址的路由器公告 (RA)。（您必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項。）如需 RA 的詳細資訊，請參閱啟用路由器公告。
		只有在啟用 RA 時才適用剩餘的欄位。
		  • **Valid Lifetime**（有效生命週期）—防火牆將位址視為有效的時間長度（以秒為單位）。有效的生命週期必須等於或超過 **Preferred Lifetime**（偏好的生命週期）（預設值為 2,592,000）。
		  • **Preferred Lifetime**（偏好的生命週期）—偏好的有效位址的時間長度（以秒為單位），意味防火牆可使用該位址來傳送和接收流量。當偏好的生命週期到期後，防火牆就無法使用位址來建立新連線，但在 **Valid Lifetime**（有效生命週期）到期前，任何現有連線仍然有效（預設值為 604,800）。
		  • **On-link**（記錄連結）—如果可不使用路由器，連線首碼中內含位址的系統，請選取此選項。
		  • **Autonomous**（自發）—如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，請選取此選項。

啟用重複的位址偵測	**Ethernet Interface**（乙太網路介面）> **IPv6** > **Address Resolution**（位址解析）	選取此選項可啟用重複的位址偵測 (DAD)，然後設定此區段中的其他欄位。
DAD 嘗試		指定在識別芳鄰的嘗試失敗之前，DAD 的芳鄰請求間隔（**NS Interval**（NS 間隔））內的嘗試次數（範圍是 1 至 10，預設為 1）。
可連線時間		指定在成功查詢與回應之後，芳鄰保持可到達狀態的時間長度（以秒為單位，範圍是 10 至 36,000，預設為 30）。
NS 間隔（芳鄰請求間隔）		指定在指示失敗之前，DAD 嘗試的秒數（範圍是 1 至 10，預設為 1）。
啟用 NDP 監控		選取此選項可啟用芳鄰發現協定 (NDP) 監控。啟用後，您可以選取 NDP 監控（功能欄中的 ）及檢視防火牆所探索芳鄰的相關資訊，例如 IPv6 位址、對應的 MAC 位址和 User-ID (最佳情況)。
啟用路由器公告	**Ethernet Interface**（乙太網路介	若要在 IPv6 介面上提供無狀態位址自動設定 (SLAAC)，請選取並設定此區段中的其他欄位。接收路由器公告 (RA) 訊息的 IPv6 DNS 用戶端會使用此資訊。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
	面）> **IPv6** > **Router Advertisement**（路由器公告）	RA 能夠使防火牆成為非靜態設定之 IPv6 主機的預設閘道，並可將用於位址組態的 IPv6 首碼提供給主機。您可以將個別的 DHCPv6 伺服器搭配此功能使用，將 DNS 及其他設定提供給用戶端。 這是介面的全域設定。若要為個別的 IP 位址設定 RA 選項，請按一下 IP 位址表格中的 **Add**（新增）並設定位址。若為任何 IP 位址設定 RA 選項，您必須為介面選取 **Enable Router Advertisement**（啟用路由器公告）選項。
最小間隔（秒）		指定防火牆所將傳送的 RA 之間的最小間隔（以秒為單位，範圍是 3 至 1,350，預設值為 200）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
最大間隔（秒）		指定 RA 與防火牆之間將傳送的最大間隔（以秒為單位，範圍是 4 至 1,800，預設為 600）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
躍點限制		指定要套用至連出封包之用戶端的躍點限制（範圍是 1 至 255，預設為 64）。輸入 0 代表無躍點限制。
連結 MTU		指定要套用至用戶端的連結最大傳輸單位 (MTU)。選取 **Unspecified**（不指定）表示沒有連結 MTU（範圍是 1,280 至 9,192，預設為不指定）。
可連線時間（毫秒）		指定用戶端在收到可連線能力確認訊息後，假設可用來連線芳鄰的可連線時間（以毫秒為單位）。選取 **Unspecified**（不指定）表示沒有可連線時間值（範圍是 0 至 3,600,000，預設為不指定）。
重新傳輸時間（毫秒）		指定重新傳輸計時器決定用戶端應該等候多長時間（以毫秒為單位），再重新傳輸芳鄰請求訊息。選取 **Unspecified**（不指定）表示沒有重新傳輸時間（範圍是 0 至 4,294,967,295，預設為不指定）。
路由器生命週期（秒）		指定用戶端將防火牆作為預設閘道的時間長度，範圍是 0 至 9,000，預設為 1,800）。零指定防火牆不是預設閘道。當生命週期到期時，用戶端會從其預設路由器清單中移除防火牆項目，並將其他路由器作為預設閘道。
路由器偏好設定		如果網路區段具有多個 IPv6 路由器，用戶端將使用此欄位來選取偏好的路由器。選取 RA 是否將防火牆路由器公告為具有 **High**（高）、**Medium**（中）（預設值）或 **Low**（低）優先順序（相對於區段上的其他路由器而言）。
受管理的組態		選取此選項可向用戶端指示位址透過 DHCPv6 提供。
一致性檢查	**Ethernet Interface**（乙太網路介面）> **IPv6** > **Router Advertisement (cont)**（路由器公告（續））	若要防火牆確認從其他路由器傳送的 RA 正在公告連結的一致資訊，請選取此選項。防火牆會記錄系統日誌中任何不一致的情況；類型為 **ipv6nd**。
其他組態		選取以指出用戶端可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	設定位置	說明
包含路由器公告中的 DNS 資訊	**Ethernet Interface**（乙太網路介面）> **IPv6** > **DNS Support**（**DNS** 支援）	選取此選項可讓防火牆從此 IPv6 乙太網路介面在 NDP 路由器公告 (RA) 訊息中傳送 DNS 資訊。只有在選取此選項後，才能看到此表中的其他 DNS 支援欄位。
伺服器		**Add**（新增）一或多個遞迴 DNS (RDNS) 伺服器位址，以便防火牆從此 IPv6 乙太網路介面在 NDP 路由器公告中傳送。RDNS 伺服器會將一系列 DNS 查詢要求傳送至根 DNS 和授權 DNS 伺服器，最終將 IP 位址提供給 DNS 用戶端。 您可以設定最多 8 部 RDNS 伺服器，讓防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相同順序使用這些位址。選取伺服器並 **Move Up**（上移）或 **Move Down**（下移）來變更伺服器的順序，或 **Delete**（刪除）清單中您不再需要的伺服器。
SA 生命週期		輸入 IPv6 DNS 用戶端收到路由器公告後的最大秒數，然後用戶端才能使用 RDNS 伺服器解析網域名稱（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。
尾碼		**Add**（新增）並設定 DNS 搜尋清單 (DNSSL) 的一或多個網域名稱（尾碼）。最大長度為 255 位元組。 DNS 搜尋清單是 DNS 用戶端路由器在名稱輸入 DNS 查詢之前，附加（一次一個）至不合格網域名稱的網域尾碼清單，因而會在 DNS 查詢中使用完全合格網域名稱。例如，如果 DNS 用戶端嘗試對沒有尾碼的「quality」提交 DNS 查詢，則路由器會將一個期間和 DNS 搜尋清單中的第一個 DNS 尾碼附加至該名稱，然後傳輸 DNS 查詢。如果清單上的第一個 DNS 尾碼是「company.com」，則從路由器產生的 DNS 查詢是針對 FQDN「quality.company.com」。 如果 DNS 查詢失敗，則路由器會將清單中的第二個 DNS 尾碼附加至不合格名稱並傳輸新的 DNS 查詢。路由器會嘗試 DNS 尾碼，直到 DNS 查閱成功（忽略其餘的尾碼），或直到路由器已嘗試清單上的所有尾碼為止。 在芳鄰發現 DNSSL 選項中使用您要提供給 DNS 用戶端路由器的尾碼設定防火牆；接收 DNSSL 選項的 DNS 用戶端會在其不合格 DNS 查詢中使用這些尾碼。 您可以為 DNS 搜尋清單設定最多 8 個網域名稱（尾碼），以便防火牆在 NDP 路由器公告中傳送（順序從上至下）給收件者，然後收件者可依相容順序使用這些位址。選取尾碼並 **Move Up**（上移）或 **Move Down**（下移）來變更順序，或 **Delete**（刪除）不再需要的尾碼。
SA 生命週期		輸入 IPv6 DNS 用戶端收到可在 DNS 搜尋清單上使用網域名稱（尾碼）之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。

第三層介面

- **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）

設定可將流量路由至的乙太網路第三層介面。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
介面名稱	唯讀 **Interface Name**（介面名稱）欄位會顯示您所選實體介面的名稱。
備註	輸入介面的使用者易記的說明。
介面類型	選取 **Layer3**（第三層介面）。
Netflow 設定檔	如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取 Netflow 設定檔，或選取 **Netflow Profile**（**Netflow** 設定檔）來建立新設定檔（請參閱 Device（裝置）> Server Profiles（伺服器設定檔）> NetFlow）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
設定頁籤	
虛擬路由器	將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統	如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或選取 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域	選取介面的安全性區域，或選取 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
IPv4 頁籤	
啟用 SD-WAN	選取 **Enable SD-WAN**（啟用 **SD-WAN**）以針對乙太網路介面啟用 SD-WAN 功能。
啟用 Bonjour Reflector	（僅限 PA-220、PA-800 和 PA-3200 系列）啟用此選項後，防火牆會將此介面上接收和轉送到此介面的 Bonjour 多點傳送廣告和查詢轉送到啟用了此選項的所有其他 L3 和 AE 介面以及子介面。在出於安全或管理目的而使用區段來路由流量的網路環境中，這有助於確保使用者存取與裝置可探索性。您可以在最多 16 個介面上啟用此選項。
IPv4 Type = 靜態	
ip	新增並執行下列其中一個步驟來為介面指定靜態 IP 位址與網路遮罩。 • 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：*ip_address/mask*（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 建立類型為 **IP netmask**（**IP** 網路遮罩）的 **Address**（位址）物件。 您可以為介面輸入多個 IP 位址。您的系統使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 **Delete**（刪除）您不再需要的 IP 位址。
SD-WAN 閘道	如果您已選取 **Enable SD-WAN**（啟用 **SD-WAN**），請輸入 SD-WAN 閘道的 IPv4 位址。
IPv4 類型 PPPoE，一般頁籤	

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
啟用	選取 **Enable**（啟用）以針對 point-to-point protocol over Ethernet (乙太網路點對點通訊協定 - PPPoE) 啟用介面。介面是一個 (PPPoE) 終止點，以支援數位用戶線路 (DSL) 環境中的連線，此環境中有 DSL 數據機但沒有可終止連線的其他 PPPoE 裝置。
使用者名稱	輸入 ISP 為點對點連線提供的使用者名稱。
Password（密碼）與 Confirm Password（確認密碼）	輸入密碼與確認密碼。
顯示 PPPoE 用戶端執行階段資訊	選取以檢視 PPPoE 介面的相關資訊。
IPv4 類型 = PPPoE，進階頁籤	
驗證	選取驗證方法： • **None**（無）—（預設值）針對 PPPoE 介面上無驗證。 • **CHAP**—防火牆針對 PPPoE 介面使用查問交握式驗證通訊協定—RFC-1994。 • **PAP**—防火牆針對 PPPoE 介面使用密碼驗證通訊協定 (PAP)。PAP 沒有 CHAP 安全；PAP 會以明文傳送使用者名稱和密碼。 • **auto**（自動）—防火牆與 PPPoE 伺服器協商驗證方法（CHAP 或 PAP）。
靜態位址	從 PPPoE 伺服器要求所需的 IPv4 位址。PPPoE 伺服器可以指派該位址或其他位址。
自動建立指向端點的預設路由	選取此選項可自動建立預設路由，其指向 DHCP 伺服器提供的預設閘道。
預設路由度量標準	輸入 PPPoE 連線的預設路由公制（優先順序層級）（預設值為 10）。在選擇路由期間，數字愈小的路由其優先順序愈高。例如，會先使用公制為 10 的路由，再使用公制為 100 的路由。
存取集訊器	如果 ISP 提供了存取集訊器的名稱，請輸入該名稱。防火牆將在 ISP 端連線此存取集訊器。這是一個長度為 0-255 個字元的字串值。
服務	防火牆（PPPoE 用戶端）可以將所需的服務要求提供給 PPPoE 伺服器。這是一個長度為 0-255 個字元的字串值。
被動	防火牆（PPPoE 用戶端）等待 PPPoE 伺服器起始連線。如果未啟用該選項，防火牆將起始連線。
IPv4 頁籤，類型 = DHCP 用戶端	
啟用	啟用介面做為 Dynamic Host Configuration Protocol (動態主機設定通訊協定 - DHCP) 用戶端，並接收動態指派的 IP 位址。 *處於高可用性 (HA) 主動/主動組態的防火牆不支援 DHCP 用戶端。*

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
自動建立指向伺服器所提供之預設閘道的預設路由	選取此選項會使防火牆建立指向預設閘道的靜態路由。在用戶端嘗試存取許多目的地，而這些目的地不需要在防火牆的路由表中維護路由時，預設閘道很有用。
傳送主機名稱	選取此選項以向 DHCP 用戶端介面指派主機名稱並將該主機名稱（選項 12）傳送至 DHCP 伺服器，DHCP 伺服器可在 DNS 伺服器上註冊主機名稱。然後，DNS 伺服器可自動管理主機名稱到動態 IP 位址解析。外部主機可根據主機名稱識別介面。預設值表示 `system-hostname`（系統-主機名稱），即在 **Device**（裝置）> **Setup(**設定）> **Management**（管理）> **General Settings**（一般設定）中設定的防火牆主機名稱。或者，輸入介面的主機名稱，長度最多為 64 個字元，包括大寫和小寫字母、數字、句點 (.)、連字符 (-) 和底線 (_)。
預設路由度量標準	為防火牆與 DHCP 伺服器之間的路由輸入預設路由公制（優先順序層級）（範圍是 1 至 65535；沒有預設公制）。在選擇路由期間，數字愈小的路由其優先順序愈高。例如，會先使用公制為 10 的路由，再使用公制為 100 的路由。
顯示 DHCP 用戶端執行階段資訊	選取此選項以查看用戶端繼承自 DHCP 伺服器的所有設定，包括 DHCP 租用狀態、動態 IP 位址指派、子網路遮罩、閘道和伺服器設定（DNS、NTP、網域、WINS、NIS、POP3 和 SMTP）。
IPv6 頁籤	
對介面啟用 IPv6	選取此選項可在介面上啟用 IPv6 定址。
介面 ID	以十六進位格式輸入 64 位元延伸唯一識別碼 (**EUI-64**)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。
位址	新增 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。或者選取現有的 IPv6 位址物件，或建立新的 IPv6 位址物件。
在介面上啟用位址	選取該項以在介面上啟用 IPv6 位址。
使用介面 ID 作為主機部分	選取以使用 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。
Anycast	選取此選項以包含通過最近節點的路由。
傳送路由器公告	選取此選項以啟用此 IP 位址的路由器公告 (RA)。（您必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項。）如需 RA 的詳細資訊，請參閱本表的「啟用路由器公告」。僅當您「啟用路由器公告」時，下列欄位才適用： • **Valid Lifetime**（有效的生命週期）—防火牆將位址視為有效的時間長度（以秒為單位）。有效的 SA 生命週期必須等於或超過 **Preferred Lifetime**（慣用 SA 生命週期）。預設值為 2,592,000。 • **Preferred Lifetime**（偏好的生命週期）—偏好的有效位址的時間長度（以秒為單位），意味防火牆可使用該位址來傳送和接收流量。當偏好的生命週期到期後，防火牆就無法使用該位址來建立新連線，但在 **Valid Lifetime**（有效的生命週期）到期前，任何現有連線仍然有效。預設值為 604,800。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
	• **On-link**（記錄連結）—如果可不使用路由器，連線首碼中內含位址的系統，請選取此選項。 • **Autonomous**（自發）—如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，請選取此選項。
IPv6 頁籤，位址解析頁籤	
啟用重複的位址偵測	選取以啟用啟用重複的位址偵測 (DAD)，然後設定 DAD 嘗試、可連線時間（秒）和 NS 間隔。
DAD 嘗試	指定在識別芳鄰的嘗試失敗之前，DAD 的芳鄰請求間隔（**NS Interval**（NS 間隔））內的嘗試次數（範圍是 1 至 10，預設為 1）。
可連線時間（秒）	指定在成功查詢與回應之後，芳鄰保持可到達狀態的時間長度（以秒為單位，範圍是 1 至 36,000，預設為 30）。
NS 間隔（秒）	指定在指示失敗之前，DAD 嘗試的秒數（範圍是 1 至 10，預設為 1）。
啟用 NDP 監控	選取此選項可啟用芳鄰發現協定 (NDP) 監控。啟用時，您可以選取 NDP（功能欄中的 ）來檢視防火牆所探索到之芳鄰的相關資訊，例如 IPv6 位址、對應的 MAC 位址和 User-ID（依據最佳狀況）。
IPv6 頁籤，路由器公告頁籤	
啟用路由器公告	若要在 IPv6 介面上提供芳鄰發現，請選取此選項並在此區段中設定其他欄位。接收路由器公告 (RA) 訊息的 IPv6 DNS 用戶端會使用此資訊。 RA 能夠使防火牆成為非靜態設定之 IPv6 主機的預設閘道，並可將用於位址組態的 IPv6 首碼提供給主機。您可以將個別的 DHCPv6 伺服器搭配此功能使用，將 DNS 及其他設定提供給用戶端。 這是介面的全域設定。若要為個別的 IP 位址設定 RA 選項，請在 IP 位址表中 **Add**（新增）IPv6 位址並加以設定。若要為任何 IPv6 位址設定 RA 選項，必須為介面 **Enable Router Advertisement**（啟用路由器公告）。
最小間隔（秒）	指定防火牆所將傳送的 RA 之間的最小間隔（以秒為單位，範圍是 3 至 1,350，預設值為 200）。防火牆將以所設定之最小值與最大值之間的隨機間隔傳送 RA。
最大間隔（秒）	指定 RA 與防火牆之間將傳送的最大間隔（以秒為單位，範圍是 4 至 1,800，預設為 600）。防火牆將以所設定之最小值與最大值之間的隨機間隔傳送 RA。
躍點限制	指定要套用至連出封包之用戶端的躍點限制（範圍是 1 至 255，預設值為 64），或者選取 **unspecified**（未指定），這會對應至系統預設值。
連結 MTU	指定要套用至用戶端的鏈路最大傳輸單位 (MTU)（範圍是 1,280 至 1,500），或者預設為 **unspecified**（未指定），這會對應至系統預設值。
可連線時間（毫秒）	指定用戶端在收到可連線能力確認訊息後，假設可用來連線芳鄰的可連線時間（以毫秒為單位）（範圍是 0-3,600,000），或者預設為 **unspecified**（未指定），這會對應至系統預設值。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
重新傳輸時間（毫秒）	指定重新傳輸計時器決定用戶端應該等候多長時間（以毫秒為單位），再重新傳輸芳鄰請求訊息（範圍是 0-4,294,967,295），或者預設為 **unspecified**（未指定），這會對應至系統預設值。
路由器生命週期（秒）	指定用戶端將防火牆作為預設閘道的時間長度（以秒為單位，範圍是 0 至 9,000，預設為 1,800）。零指定防火牆不是預設閘道。當生命週期到期時，用戶端會從其預設路由器清單中移除防火牆項目，並將其他路由器作為預設閘道。
路由器偏好設定	如果網路區段具有多個 IPv6 路由器，用戶端將使用此欄位來選取偏好的路由器。選取 RA 是否將防火牆路由器公告為具有 **High**（高）、**Medium**（中）（預設值）或 **Low**（低）優先順序（相對於區段上的其他路由器而言）。
受管理的組態	選取此選項可向用戶端指示位址透過 DHCPv6 提供。
其他組態	選取以指出用戶端可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。
一致性檢查	若要防火牆確認從其他路由器傳送的 RA 正在公告連結的一致資訊，請選取此選項。防火牆會記錄系統日誌中任何不一致的情況；類型為 **ipv6nd**。
僅當您在 **Router Advertisement**（路由器公告）頁籤上 **Enable Router Advertisement**（啟用路由器公告）時，**DNS Support**（**DNS** 支援）頁籤才可用。	
包含路由器公告中的 DNS 資訊	選取此選項可讓防火牆從這個 IPv6 乙太網路子介面傳送 NDP 路由器公告中的 DNS 資訊。只有在選取此選項後，才能看到其他 DNS 支援欄位（伺服器、生命週期和首碼）。
伺服器	**Add**（新增）一或多個遞迴 DNS (RDNS) 伺服器位址，以便防火牆從此 IPv6 乙太網路介面在 NDP 路由器公告中傳送。RDNS 伺服器會傳送一系列 DNS 查閱要求到根 DNS 與授權的 DNS 伺服器，從而最終對 DNS 用戶端提供 IP 位址。 您可以設定最多 8 部 RDNS 伺服器，讓防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相同順序使用這些伺服器。選取伺服器並 **Move Up**（上移）或 **Move Down**（下移）來變更伺服器的順序，或 **Delete**（刪除）清單中您不再需要的伺服器。
SA 生命週期	輸入 IPv6 DNS 用戶端收到路由器公告後的最大秒數，然後用戶端才能使用 RDNS 伺服器解析網域名稱（範圍是 **Max Interval (sec)**（最大間隔（秒））的值到 **Max Interval (sec)**（最大間隔（秒））的兩倍；預設值為 1,200）。
尾碼	為 DNS 搜尋清單 (DNSSL) **Add**（新增）一個或多個網域名稱（尾碼）。最大長度為 255 位元組。 DNS 搜尋清單是 DNS 用戶端路由器在名稱輸入 DNS 查詢之前，附加（一次一個）至不合格網域名稱的網域尾碼清單，因而會在查詢中使用完全合格網域名稱。例如，如果 DNS 用戶端嘗試針對沒有尾碼的名稱「quality」提交 DNS 查詢，則路由器會在名稱中附加英文句點和 DNS 搜尋清單中的第一個 DNS 尾碼，然後傳輸 DNS 查詢。如果清單上的第一個 DNS 尾碼是「company.com」，則來自路由器的結果查詢是針對完全合格網域名稱「quality.company.com」。 如果 DNS 查詢失敗，則路由器會將清單中的第二個 DNS 尾碼附加至不合格名稱並傳輸新的 DNS 查詢。路由器會一直使用 DNS 尾碼，直到 DNS 查閱成功（忽略剩餘尾碼）或直到路由器嘗試過清單中的所有尾碼。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
	在芳鄰發現 DNSSL 選項中使用您要提供給 DNS 用戶端路由器的尾碼設定防火牆；接收 DNSSL 選項的 DNS 用戶端會在其不合格 DNS 查詢中使用這些尾碼。 您最多可以針對 DNS 搜尋清單選項在 NDP 路由器公告中設定 8 個要由防火牆傳送至收件者的網域名稱（尾碼）（依照由上到下的列示順序），收件者會以相同順序使用這些網域名稱。選取尾碼並 **Move Up**（上移）或 **Move Down**（下移）來變更順序，或 **Delete**（刪除）不再需要的尾碼。
SA 生命週期	輸入 IPv6 DNS 用戶端收到可在 DNS 搜尋清單上使用網域名稱（尾碼）之路由器公告後的最大秒數（範圍是 **Max Interval (sec)**（最大間隔（秒））的值到 **Max Interval (sec)**（最大間隔（秒））的兩倍；預設值為 1,200）。
SD-WAN頁籤	
SD-WAN 介面狀態	如果您在 **IPv4** 頁籤上選取了 **Enable SD-WAN**（啟用 **SD-WAN**），則防火牆會指示 `SD-WAN` 介面狀態：已啟用。如果您未 **Enable SD-WAN**（啟用 **SD-WAN**），則會指示已停用。
SD-WAN 介面設定檔	選取 SD-WAN 介面設定檔以套用至此乙太網路介面，或者新增 SD-WAN 介面設定檔。 *必須為介面 Enable SD-WAN（啟用 SD-WAN），然後才能套用 SD-WAN 介面設定檔。*
上游 NAT	如果您的 SD-WAN 中樞或分支位於正在執行 NAT 的裝置後面，請為中樞或分支 **Enable**（啟用）上游 NAT。
NAT IP 位址類型	選取 IP 位址指派的類型，並指定該 NAT 執行裝置上公開介面的 IP 位址或 FQDN，或指定 DDNS 衍生該位址。因此，自動 VPN 可將該位址用作中樞或分支的通道端點。 • **Static IP**（靜態 **IP**）—選取 **Type**（類型）為 **IP Address**（**IP** 位址）或 **FQDN**，然後輸入 IPv4 位址或 FQDN。 • **DDNS**—動態 DNS (DDNS) 衍生上游 NAT 裝置的 IP 位址。
Advanced Tab（進階頁籤）	
連結速度	選取以 Mbps 為單位的介面速度（**10**、**100** 或 **1000**），或選取 **Auto**（自動）。
連結雙工	選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態	選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。
進階頁籤。其他資訊資頁籤	
管理設定檔	選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU	以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 9,192；預設為 1,500）。如果防火牆任一側的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
調整 TCP MSS	選取以調整最大區段大小 (MSS) 將任何標頭適應介面 MTU 位元組大小範圍。MTU 位元組大小減去 MSS 調整大小等於 MSS 位於組大小，該值視 IP 通訊協定而定： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）—範圍是 40 至 300；預設為 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）—範圍是 60 至 300；預設為 60。 使用這些設定可解決網路中的 **tunnel**（通道）需要較小 MSS 的情況。如果封包必須分段才能擁有大於 MMS 的位元組，則此設定可啟用調整。 封裝增加了標頭長度，因此有助於設定 MSS 調整大小，使 MPLS 標頭或擁有 VLAN 頁籤的通道流量等可支援該位元組。
未標記的子介面	如果未標記此介面的對應子介面，請選取此選項。
進階頁籤，**ARP** 項目頁籤	
IP 位址 MAC 位址	若要新增一或多個靜態位址解析通訊協定 (ARP) 項目，請 **Add**（新增）IP 位址及其相關聯的硬體 [媒體存取控制或 (MAC)] 位址。若要刪除項目，請選取項目並按一下 **Delete**（刪除）。靜態 ARP 項目降低 ARP 處理。
進階頁籤，**ND** 項目頁籤	
IPv6 位址 MAC 位址	若要為芳鄰發現協定 (NDP) 新增芳鄰資訊，請 **Add**（新增）芳鄰的 IPv6 位址和 MAC 位址。
進階頁籤，**NDP Proxy** 頁籤	
啟用 NDP Proxy	啟用介面的芳鄰發現協定 (NDP) Proxy。防火牆將回應要求清單中 IPv6 位址其 MAC 位址的 ND 封包。在 ND 回應中，防火牆會為介面傳送自己的 MAC 位址，因此防火牆接收預定要到清單中位址的封包。 如果您使用網路首碼轉譯 IPv6 (NPTv6)，則建議您啟用 NDP Proxy。 如果選取 **Enable NDP Proxy**（啟用 **NDP Proxy**），您可以輸入篩選器，然後按一下 [套用篩選器]（灰色箭頭），來篩選許多 **Address**（位址）項目。
位址	按一下 **Add**（新增），輸入一個或多個 IPv6 位址、IP 範圍、IPv6 子網路，或防火牆將作為 NDP Proxy 的位址物件。理論上而言在這些位址中，某一個位址會與 NPTv6 中來源轉譯的位址相同。位址順序不重要。 如果該位址是子網路，防火牆會為子網路中所有的位址傳送 ND 回應，因此我們建議您也新增防火牆的 IPv6 芳鄰，然後按一下 **Negate**（否定）來指示防火牆不要回應這些 IP 位址。
否定	將位址 **Negate**（否定）來防止該位址的 NDP Proxy。您可以否定所指定 IP 位址範圍或 IP 子網路的子集。
進階頁籤，**LLDP** 頁籤	
啟用 LLDP	啟用介面的連結層探索通訊協定 (LLDP)。鏈路層的 LLDP 功能，用於探索鄰接裝置及其功能，方法是將 LLDP 資料單位傳送給芳鄰並接收來自芳鄰的 LLDP 資料單位。

© 2019 Palo Alto Networks, Inc.

第三層介面設定	說明
LLDP 設定檔	選取 LLDP 設定檔或者建立新的 LLDP 設定檔。設定檔可讓您設定防火牆的 LLDP 模式、啟用系統日誌與 SNMP 通知以及設定您要傳輸到 LLDP 端點的選用類型-長度-值 (TLV)。
進階頁籤，**DDNS** 頁籤	
設定	選取 **Settings**（設定）讓 DDNS 欄位可以設定。
啟用	啟用介面上的 DDNS。您必須先啟用 DDNS 才能對其進行設定。（如果您的 DDNS 組態未完成，您可以儲存它而不啟用它，這樣您就不會丟失部分組態。）
更新間隔（天數）	輸入防火牆傳送至 DDNS 伺服器的更新之間的間隔（以天數為單位），以更新對應到 FQDN 的 IP 位址（範圍為 1 到 30；預設值為 1）。 在防火牆收到從 *DHCP* 伺服器為了介面傳送的新 *IP* 位址時還會更新 *DDNS*。
憑證設定檔	建立憑證設定檔以驗證 DDNS 服務。DDNS 服務向防火牆提供由憑證授權單位 (CA) 發佈的憑證。
主機名稱	輸入在 DDNS 伺服器上註冊的介面的主機名稱（例如，host123.domain123.com 或 host123）。除了確認語法是使用 DNS 在網域名稱中允許的有效字元外，防火牆不會驗證主機名稱。
廠商	選取為此介面提供 DDNS 服務的 DDNS 廠商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** • （PAN-OS 10.0.3 和更高的 10.0 版）**Palo Alto Networks DDNS**（僅適用於具有 DDNS 的 SD-WAN 全網狀） 如果您選取了防火牆指示會在特定日期前逐步淘汰的較舊版本的 *DDNS* 服務，請移至較新版本。 廠商名稱後面的 **Name**（名稱）以及 **Value**（數值）欄位是特定於廠商的。唯讀欄位會通知您防火牆用於連結 DDNS 服務的參數。設定其他欄位，例如 DDNS 服務向您提供的密碼，以及如果防火牆未從 DDNS 伺服器收到回應，防火牆使用的逾時。
IPv4 頁籤	新增在介面設定的 IPv4 位址，然後選取它們。您最多只能選取 DDNS 廠商允許的 IPv4 位址數量。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
IPv6 頁籤	新增在介面設定的 IPv6 位址，然後選取它們。您最多只能選取 DDNS 廠商允許的 IPv6 位址數量。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
顯示執行階段資訊	顯示 DDNS 註冊情況：DDNS 供應商、已解析的 FQDN 以及帶有星號 (*) 的對應的 IP 位址指示主要 IP 位址。每個 DDNS 供應商都有自己的返回代碼，用於指示主機名稱更新的狀態和返回日期，以便進行疑難排解。

© 2019 Palo Alto Networks, Inc.

第三層子介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

針對每個設定為實體 Layer 3 介面的 Ethernet 連接埠，您可以定義其他邏輯 Layer 3 介面（子介面）。

若要設定 PA-7000 Series 第三層介面，請選取實體介面，**Add Subinterface**（新增子介面），並指定下列資訊。

第三層子介面設定	設定位置	說明
介面名稱	**Layer3** 介面	唯讀 **Interface Name**（介面名稱）欄位會顯示您所選實體介面的名稱。在相鄰的欄位中，輸入用來識別子介面的數值尾碼（1 至 9,999）。
備註		輸入子介面的選取性說明。
頁籤		輸入子介面的 VLAN 頁籤 （1 至 4,094）。
Netflow 設定檔		如果您要匯出單向（亦即從進入子介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從子介面移除目前的 NetFlow 伺服器指派。
虛擬路由器	**Layer3 Subinterface**（第三層子介面）> **Config**（設定）	將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為子介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取子介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從子介面移除目前的區域指派。
類型	**Layer3 Subinterface**（第三層子介面）> **IPv4**	選取將 IPv4 位址類型指派給子介面的方法： • **Static**（靜態）—您必須手動指定 IP 位址。 • **DHCP Client**（**DHCP** 用戶端）—啟用子介面作為動態主機組態通訊協定 (DHCP) 用戶端，並接收動態指派的 IP 位址。 *處於高可用性 (HA) 主動/主動組態的防火牆不支援 DHCP 用戶端。* 頁籤上顯示的選項會視所選的 IP 位址方式而不同。
啟用 Bonjour Reflector	**Layer3 Subinterface**（第三層子介面）> **IPv4**	（僅限 PA-220、PA-800 和 PA-3200 系列）啟用此選項後，防火牆會將此介面上接收和轉送到此介面的 Bonjour 多點傳送廣告和查詢轉送到啟用了此選項的所有其他 L3 和 AE 介面以及子介面。在出於安全或管理目的而使用區段來路由流量的網路環境中，這有助於確保使用者存取與裝置可探索性。您可以在最多 16 個介面上啟用此選項。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
ip	**Layer3 Subinterface**（第三層子介面）> **IPv4, Type = Static**（**IPv4**，類型 = 靜態）	**Add**（新增）並執行下列其中一個步驟來為介面指定靜態 IP 位址與網路遮罩。 • 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：*ip_address/mask*（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 建立類型為 **IP netmask**（**IP** 網路遮罩）的 **Address**（位址）物件。 您可以為介面輸入多個 IP 位址。您的系統使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 **Delete**（刪除）您不再需要的 IP 位址。
啟用	**Layer3 Subinterface**（第三層子介面）> **IPv4, Type = DHCP**（**IPv4**，類型 = **DHCP**）	選取此選項可在介面上啟動 DHCP 用戶端。
自動建立指向伺服器所提供之預設閘道的預設路由		選取此選項可自動建立預設路由，指向 DHCP 伺服器提供的預設閘道。
傳送主機名稱		選取以讓防火牆（作為 DHCP 用戶端）將介面的主機名稱（選項 12）傳送至 DHCP 伺服器。如果您在預設情況下傳送主機名稱，則在預設情況下，防火牆的主機名稱會是根據主機名稱欄位決定的。您可以傳送該名稱或輸入自訂主機名稱（最多 64 個字元，包括大寫和小寫字母、數字、句點、連字符和底線。
預設路由度量標準		（選用）針對防火牆與 DHCP 伺服器之間的路由，您可輸入要與預設路由相關聯並用於選取路徑的路由度量標準（優先順序層級，範圍是 1 至 65535；無預設值）。優先順序層級會隨著數值減少而增加。
顯示 DHCP 用戶端執行階段資訊		選取 **Show DHCP Client Runtime Info**（顯示 **DHCP** 用戶端執行階段資訊）可顯示接收自 DHCP 伺服器的所有設定，包括 DHCP 租用狀態、動態 IP 指派、子網路遮罩、閘道和伺服器設定（DNS、NTP、網域、WINS、NIS、POP3 和 SMTP）。
對介面啟用 IPv6	**Layer3 Subinterface**（第三層子介面）> **IPv6**	選取此選項可在此介面上啟用 IPv6 定址。
介面 ID		以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。
位址		按一下 **Add**（新增），並為每個 IPv6 位址設定下列參數： • **Address**（位址）—輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立位址物件。 • **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。 • **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
		• **Anycast**（任一傳播）—選取以包含最近節點中的路由。 • **Send Router Advertisement**（傳送路由器公告）—選取此選項可啟用此 IP 位址的路由器公告 (RA)。（您必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項。）如需 RA 的詳細資訊，請參閱本表的啟用路由器公告。 只有在啟用 RA 時才適用剩餘的欄位。 • **Valid Lifetime**（有效生命週期）—防火牆將位址視為有效的時間長度（以秒為單位）。有效的 SA 生命週期必須等於或超過 **Preferred Lifetime**（慣用 SA 生命週期）。預設值為 2,592,000。 • **Preferred Lifetime**（偏好的生命週期）—偏好的有效位址的時間長度（以秒為單位），意味防火牆可使用該位址來傳送和接收流量。當慣用 SA 生命週期到期後，防火牆就無法使用位址來建立新連線，但在 **Valid Lifetime**（有效 SA 生命週期）到期前，任何現有連線仍然有效。預設值為 604,800。 • **On-link**（記錄連結）—如果可不使用路由器，連線首碼中內含位址的系統，請選取此選項。 • **Autonomous**（自發）—如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，請選取此選項。
啟用重複的位址偵測	**Layer3 Subinterface**（第三層子介面）> **IPv6** > **Address Resolution**（位址解析）	選取此選項可啟用重複的位址偵測 (DAD)，然後設定此區段中的其他欄位。
DAD 嘗試		指定在識別芳鄰的嘗試失敗之前，DAD 的芳鄰請求間隔（**NS Interval**（NS 間隔））內的嘗試次數（範圍是 1 至 10，預設為 1）。
可連線時間		指定在成功查詢與回應之後，芳鄰保持可到達狀態的時間長度（以秒為單位，範圍是 1 至 36,000，預設為 30）。
NS 間隔（芳鄰請求間隔）		指定在指示失敗之前，DAD 嘗試的秒數（範圍是 1 至 10，預設為 1）。
啟用 NDP 監控		選取此選項可啟用芳鄰發現協定 (NDP) 監控。啟用時，您可以選取 NDP（功能欄中的 ）來檢視防火牆所探索之芳鄰的相關資訊，例如 IPv6 位址、對應的 MAC 位址和 User-ID（依據最佳狀況）。
啟用路由器公告	**Layer3 Subinterface**（第三層子介面）> **IPv6** > **Router Advertisement**（路由器公告）	若要在 IPv6 介面上提供芳鄰發現，請選取此選項並在此區段中設定其他欄位。接收路由器公告 (RA) 訊息的 IPv6 DNS 用戶端會使用此資訊。 RA 能夠使防火牆成為非靜態設定之 IPv6 主機的預設閘道，並可將用於位址組態的 IPv6 首碼提供給主機。您可以將個別的 DHCPv6 伺服器搭配此功能使用，將 DNS 及其他設定提供給用戶端。 這是介面的全域設定。若要為個別的 IP 位址設定 RA 選項，請在 IP 位址表中 **Add**（新增）位址並加以設定。若要為任何 IP 位址設定 RA 選項，您必須為介面 **Enable Router Advertisement**（啟用路由器公告）。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
最小間隔（秒）		指定防火牆所將傳送的 RA 之間的最小間隔（以秒為單位，範圍是 3 至 1,350，預設值為 200）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
最大間隔（秒）		指定 RA 與防火牆之間將傳送的最大間隔（以秒為單位，範圍是 4 至 1,800，預設為 600）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
躍點限制		指定要套用至連出封包之用戶端的躍點限制（範圍是 1 至 255，預設為 64）。輸入 0 代表無躍點限制。
連結 MTU		指定要套用至用戶端的連結最大傳輸單位 (MTU)。選取 **Unspecified**（不指定）表示沒有連結 MTU（範圍是 1,280 至 9,192，預設為不指定）。
可連線時間（毫秒）		指定用戶端在收到可連線能力確認訊息後，假設可用來連線芳鄰的可連線時間（以毫秒為單位）。選取 **Unspecified**（不指定）表示沒有可連線時間值（範圍是 0 至 3,600,000，預設為不指定）。
重新傳輸時間（毫秒）		指定重新傳輸計時器決定用戶端應該等候多長時間（以毫秒為單位），再重新傳輸芳鄰請求訊息。選取 **Unspecified**（不指定）表示沒有重新傳輸時間（範圍是 0 至 4,294,967,295，預設為不指定）。
路由器生命週期（秒）		指定用戶端將防火牆作為預設閘道的時間長度（以秒為單位，範圍是 0 至 9,000，預設為 1,800）。零指定防火牆不是預設閘道。當生命週期到期時，用戶端會從其預設路由器清單中移除防火牆項目，並將其他路由器作為預設閘道。
路由器偏好設定		如果網路區段具有多個 IPv6 路由器，用戶端將使用此欄位來選取偏好的路由器。選取 RA 是否將防火牆路由器公告為具有 **High**（高）、**Medium**（中）（預設值）或 **Low**（低）優先順序（相對於區段上的其他路由器而言）。
受管理的組態		選取此選項可向用戶端指示位址透過 DHCPv6 提供。
其他組態		選取以指出用戶端可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。
一致性檢查	**Layer3 Subinterface**（第三層子介面）> **IPv6** > **Router Advertisement**（路由器公告）（續）	若要防火牆確認從其他路由器傳送的 RA 正在公告連結的一致資訊，請選取此選項。防火牆會記錄系統日誌中任何不一致的情況；類型為 **ipv6nd**。
包含路由器公告中的 DNS 資訊	**Layer3 Subinterface**（第三層子介面）> **IPv6**	選取此選項可讓防火牆從這個 IPv6 乙太網路子介面傳送 NDP 路由器公告中的 DNS 資訊。只有在選取此選項後，才能看到此表中的其他 DNS 支援欄位。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
伺服器	**Subinterface**（第三層子介面）> **DNS Support**（**DNS** 支援）	**Add**（新增）一或多個遞迴 DNS (RDNS) 伺服器位址，以便防火牆從此 IPv6 乙太網路介面在 NDP 路由器公告中傳送。RDNS 伺服器會傳送一系列 DNS 查閱要求到根 DNS 與授權的 DNS 伺服器，從而最終對 DNS 用戶端提供 IP 位址。 您可以設定最多 8 部 RDNS 伺服器，讓防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相同順序使用這些伺服器。選取伺服器並 **Move Up**（上移）或 **Move Down**（下移）來變更伺服器的順序，或 **Delete**（刪除）清單中您不再需要的伺服器。
SA 生命週期		輸入 IPv6 DNS 用戶端收到路由器公告後的最大秒數，然後用戶端才能使用 RDNS 伺服器解析網域名稱（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。
尾碼	**Layer3 Subinterface**（第三層子介面）> **IPv6** > **DNS Support**（**DNS** 支援）（續）	為 DNS 搜尋清單 (DNSSL) **Add**（新增）一個或多個網域名稱（尾碼）。最大長度為 255 位元組。 DNS 搜尋清單是 DNS 用戶端路由器在名稱輸入 DNS 查詢之前，附加（一次一個）至不合格網域名稱的網域尾碼清單，因而會在查詢中使用完全合格網域名稱。例如，如果 DNS 用戶端嘗試針對沒有尾碼的名稱「quality」提交 DNS 查詢，則路由器會在名稱中附加英文句點和 DNS 搜尋清單中的第一個 DNS 尾碼，然後傳輸 DNS 查詢。如果清單上的第一個 DNS 尾碼是「company.com」，則來自路由器的結果查詢是針對完全合格網域名稱「quality.company.com」。 如果 DNS 查詢失敗，則路由器會將清單中的第二個 DNS 尾碼附加至不合格名稱並傳輸新的 DNS 查詢。路由器會一直使用 DNS 尾碼，直到 DNS 查閱成功（忽略剩餘尾碼）或直到路由器嘗試過清單中的所有尾碼。 在芳鄰發現 DNSSL 選項中使用您要提供給 DNS 用戶端路由器的尾碼設定防火牆；接收 DNSSL 選項的 DNS 用戶端會在其不合格 DNS 查詢中使用這些尾碼。 您最多可以針對 DNS 搜尋清單選項在 NDP 路由器公告中設定 8 個要由防火牆傳送至收件者的網域名稱（尾碼）（依照由上到下的列示順序），收件者會以相同順序使用這些網域名稱。選取尾碼並 **Move Up**（上移）或 **Move Down**（下移）來變更順序，或 **Delete**（刪除）不再需要的尾碼。
SA 生命週期	**Layer3 Subinterface**（第三層子介面）> **IPv6** > **DNS Support**（**DNS** 支援）（續）	輸入 IPv6 DNS 用戶端收到可在 DNS 搜尋清單上使用網域名稱（尾碼）之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。
管理設定檔	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **Other**	管理設定檔 — 選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU		以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 9,192；預設為 1,500）。如果防火牆任一側

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
	Info（其他資訊）	的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。
調整 TCP MSS	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **Other Info**（其他資訊）	選取以調整最大區段大小 (MSS) 將任何標頭適應介面 MTU 位元組大小範圍。MTU 位元組大小減去 MSS 調整大小等於 MSS 位於組大小，該值視 IP 通訊協定而定： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）—範圍是 40 至 300；預設為 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）—範圍是 60 至 300；預設為 60。 使用這些設定可解決網路中的 **tunnel**（通道）需要較小 MSS 的情況。如果封包必須分段才能擁有大於 MMS 的位元組，則此設定可啟用調整。 封裝增加了標頭長度，因此有助於設定 MSS 調整大小，使 MPLS 標頭或擁有 VLAN 頁籤的通道流量等可支援該位元組。
IP 位址 MAC 位址	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **ARP Entries**（**ARP** 項目）	若要新增一或多個靜態位址解析通訊協定 (ARP) 項目，請 **Add**（新增）IP 位址及其相關聯的硬體 [媒體存取控制或 (MAC)] 位址。若要刪除項目，請選取項目並按一下 **Delete**（刪除）。靜態 ARP 項目降低 ARP 處理。
IPv6 位址 MAC 位址	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **ND Entries**（**ND** 項目）	若要為芳鄰發現協定 (NDP) 新增芳鄰資訊，請 **Add**（新增），然後輸入芳鄰的 IP 位址和 MAC 位址。
啟用 NDP Proxy	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **NDP Proxy**	啟用介面的芳鄰發現協定 (NDP) Proxy。防火牆將回應要求清單中 IPv6 位址其 MAC 位址的 ND 封包。在 ND 回應中，防火牆會為介面傳送自己的 MAC 位址，因此防火牆接收預定要到清單中位址的封包。 如果您使用網路首碼轉譯 IPv6 (NPTv6)，則建議您啟用 NDP Proxy。 如果選取 **Enable NDP Proxy**（啟用 **NDP Proxy**），您可以輸入篩選器，然後按一下 [套用篩選器]（灰色箭頭），來篩選許多 **Address**（位址）項目。
位址		按一下 **Add**（新增），輸入一個或多個 IPv6 位址、IP 範圍、IPv6 子網路，或防火牆將作為 NDP Proxy 的位址物件。理論上而言在這些位址中，某一個位址會與 NPTv6 中來源轉譯的位址相同。位址順序不重要。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
		如果該位址是子網路，防火牆會為子網路中所有的位址傳送 ND 回應，因此我們建議您也新增防火牆的 IPv6 芳鄰，然後按一下 **Negate**（否定）來指示防火牆不要回應這些 IP 位址。
否定		將位址 **Negate**（否定）來防止該位址的 NDP Proxy。您可以否定所指定 IP 位址範圍或 IP 子網路的子集。
設定	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **DDNS**	選取 **Settings**（設定）讓 DDNS 欄位可以設定。
啟用		啟用介面上的 DDNS。您必須先啟用 DDNS 才能對其進行設定。（如果您的 DDNS 組態未完成，您可以儲存它而不啟用它，這樣您就不會丟失部分組態。）
更新間隔（天數）	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **DDNS**	輸入防火牆傳送至 DDNS 伺服器的更新之間的間隔（以天數為單位），以更新對應到 FQDN 的 IP 位址（範圍為 1 到 30；預設值為 1）。 在防火牆收到從 *DHCP* 伺服器為了介面傳送的新 *IP* 位址時還會更新 *DDNS*。
憑證設定檔		建立憑證設定檔以驗證 DDNS 服務。DDNS 服務向防火牆提供由憑證授權單位 (CA) 發佈的憑證。
主機名稱		輸入在 DDNS 伺服器上註冊的介面的主機名稱（例如，host123.domain123.com 或 host123）。除了確認語法是使用 DNS 在網域名稱中允許的有效字元外，防火牆不會驗證主機名稱。
廠商	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **DDNS**	選取為此介面提供 DDNS 服務的 DDNS 廠商（和版本）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** 如果您選取了防火牆指示會在特定日期前逐步淘汰的較舊版本的 *DDNS* 服務，請移至較新版本。 廠商名稱後面的 **Name**（名稱）以及 **Value**（數值）欄位是特定於廠商的。唯讀欄位會通知您防火牆用於連結 DDNS 服務的參數。設定其他欄位，例如 DDNS 服務向您提供的密碼，以及如果防火牆未從 DDNS 伺服器收到回應，防火牆使用的逾時。
IPv4 頁籤 - IP		新增在介面設定的 IPv4 位址，然後選取它們。您最多只能選取 DDNS 廠商允許的 IPv4 位址數量。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。

© 2019 Palo Alto Networks, Inc.

第三層子介面設定	設定位置	說明
IPv6 頁籤 - IPv6		新增在介面設定的 IPv6 位址，然後選取它們。您最多只能選取 DDNS 廠商允許的 IPv6 位址數量。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
顯示執行階段資訊	**Layer3 Subinterface**（第三層子介面）> **Advanced**（進階）> **DDNS**	顯示 DDNS 註冊情況：DDNS 供應商、已解析的 FQDN 以及帶有星號 (*) 的對應的 IP 位址指示主要 IP 位址。每個 DDNS 供應商都有自己的返回代碼，用於指示主機名稱更新的狀態和返回日期，以便進行疑難排解。

日誌卡介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

如果您在使用日誌處理卡 (LPC) 的 PA-7000 系列防火牆上設定日誌轉送，則必須將一個資料連接埠設定為 **Log Card**（日誌卡）類型。這是因為此防火牆型號的流量和日誌記錄功能，超過管理 (MGT) 介面的功能所致。日誌卡資料連接埠會執行 syslog 轉送、電子郵件、簡易網路管理通訊協定 (SNMP)、Panorama 日誌轉送及 WildFire™ 檔案轉送。

您只能將防火牆上的一個連接埠設定為 *Log Card*（日誌卡）類型。如果啟用日誌轉送，但未將介面設為 *Log Card*（日誌卡）類型，則會在嘗試認可變更時收到錯誤。

若要設定日誌卡介面，請選取尚未設定的介面（例如，ethernet1/16），並設定下表所述的設定。

日誌卡介面設定	設定位置	說明
插槽	乙太網路介面	選取介面的插槽號碼 (1-12)。
介面名稱		介面名稱是預先定義的，無法變更。
備註		輸入介面的選取性說明。
介面類型		選取 **Log Card**（日誌卡）。
IPv4	**Ethernet Interface**（乙太網路介面）> **Log Card Forwarding**（日誌卡轉送）	如果網路使用 IPv4，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv4 位址。 • **Netmask**（網路遮罩）—連接埠之 IPv4 位址的網路遮罩。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv4 位址。
IPv6		如果網路使用 IPv6，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv6 位址。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv6 位址。
連結速度	**Ethernet Interface**（乙太網路介面）>	選取以 Mbps 為單位的介面速度（**10**、**100** 或 **1000**），或選取 **Auto**（自動）（預設），讓防火牆根據連接自動決定速度。對於不可設定速度的介面，**Auto**（自動）將是唯一選項。

© 2019 Palo Alto Networks, Inc.

日誌卡介面設定	設定位置	說明
	Advanced（進階）	建議的最小連接速度為 *1000 (Mbps)*。
連結雙工		根據連接選取介面傳輸模式是全雙工 (**Full**)、半雙工 (**Half**) 還是自動交涉 (**Auto**)。預設值為 **Auto**（自動）。
連結狀態		根據連接選取介面狀態是已啟用 (**Up**)、已停用 (**Down**) 還是自動判斷 (**Auto**)。預設值為 **Auto**（自動）。

日誌卡子介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

若要新增 日誌卡介面，請選取該介面所在的資料列，**Add Subinterface**（新增子介面），然後指定下列資訊。

日誌卡子介面設定	設定位置	說明
介面名稱	**LPC** 子介面	**Interface Name**（介面名稱）（唯讀）會顯示您所選日誌卡介面的名稱。在相鄰的欄位中，輸入用來識別子介面的數值尾碼 (1-9,999)。
備註		輸入介面的選取性說明。
頁籤		輸入子介面的 VLAN **Tag**（頁籤）(0-4,094)。 讓頁籤等於子介面號碼，以方便使用。
虛擬系統	**LPC Subinterface**（LPC 子介面）> **Config**（設定）	選取要將日誌處理卡 (LPC) 子介面指派給哪一個虛擬系統 (vsys)。或者，您可以按一下 **Virtual Systems**（虛擬系統）連結以新增新 vsys。LPC 子介面指派給 vsys 後，對於所有從日誌卡轉送日誌（Syslog、電子郵件、SNMP）的服務，系統會將該介面作為這類服務的來源介面。
IPv4	**Ethernet Interface**（乙太網路介面）> **Log Card Forwarding**（日誌卡轉送）	如果網路使用 IPv4，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv4 位址。 • **Netmask**（網路遮罩）—連接埠之 IPv4 位址的網路遮罩。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv4 位址。
IPv6		如果網路使用 IPv6，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv6 位址。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv6 位址。

© 2019 Palo Alto Networks, Inc.

解密鏡像介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

若要使用解密連接埠鏡像功能，必須選取 **Decrypt Mirror**（解密鏡像）介面類型。此功能可讓您從防火牆建立解密的流量複本，再將複本傳送到可接收原始封包擷取的流量集合工具（例如 NetWitness 或 Solera）以執行封存和分析。對於因論證和歷史用途，或資料洩露保護 (DLP) 功能而需要廣泛擷取資料的組織而言，這是必要的功能。若要啟用此功能，必須取得和安裝免費的授權。

解密網路埠鏡像在公共雲平台不可用於 *VM-Series*（*AWS*、*Azure*、*Google* 雲端平台）、*VMware NSX* 和 *Citrix SDX*。

若要設定解密鏡像介面，請按一下未設定的介面名稱（例如，ethernet1/1），並指定下列資訊。

解密鏡像介面設定	說明
介面名稱	介面名稱是預先定義的，無法變更。
備註	輸入介面的選取性說明。
介面類型	選取 **Decrypt Mirror**（解密鏡像）。
連結速度	選取以 Mbps 為單位的介面速度（**10**、**100**或**1000**），或選取 **auto**（自動）讓防火牆自動決定速度。
連結雙工	選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態	選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。

彙總乙太網路 (AE) 介面群組

- Network > Interfaces > Ethernet > Add Aggregate Group（網路 > 介面 > 乙太網路 > 新增彙總群組）

彙總乙太網路 (AE) 介面群組使用 IEEE 802.1AX 連結彙總將多個乙太網路介面整合到單一虛擬介面，透過該介面可將防火牆連接至另一個網路裝置或其他防火牆。AE 介面群組透過在整合介面間實現流量負載平衡，可增加端點間的頻寬。此外還可提供備援；當一個介面失敗，剩餘介面將繼續支援流量。

設定 AE 介面群組之前，您必須設定其介面。在指派給任何特定彙總群組的介面中，硬體介質可以不同（例如，您可以混合使用光纖和銅線），但頻寬（1Gbps、10Gbps、40Gbps 或 100Gbps）和介面類型（HA3、虛擬介接、第二層或第三層）必須相同。

您可以新增的 AE 介面群組數取決於防火牆型號。產品選取工具表明了每個防火牆型號支援的最大彙總介面數。每個 AE 介面群組最多可擁有八個介面。

在 PA-3200 系列、PA-5200 系列和大部分 PA-7000 系列防火牆上，QoS 僅在前八個 AE 介面群組上受支援。具有 PA-7000-100G-NPC-A 和 SMC-B 的 PA-7000 系列防火牆是例外，在這些防火牆上，QoS 僅在前 16 個 AE 介面群組上受支援。

所有 *Palo Alto Networks* 防火牆（*VM-Series* 除外）型號均支援 *AE* 介面群組。

您可在高可用性 *(HA)* 主動#被動設定中彙總 *HA3*（封包轉送），但僅限於下列防火牆型號：

- *PA-220*
- *PA-800 Series*
- *PA-3200* 系列

© 2019 Palo Alto Networks, Inc.

- *PA-5200 系列*

若要設定 AE 介面群組，請按一下 **Add Aggregate Group**（新增彙總群組）、設定下表所述的設定，然後將介面指派給群組（請參閱彙總乙太網路 (AE) 介面）。

彙總介面群組設定	設定位置	說明
介面名稱	彙總乙太網路介面	此唯讀的 **Interface Name**（介面名稱）設為 **ae**。在相鄰的欄位中，輸入用來識別 AE 介面群組的數值尾碼。數值尾碼的範圍取決於防火牆型號支援的 AE 群組數。在產品選取工具中查看每個防火牆型號支援的最大彙總介面數。
備註		（選用）輸入介面的說明。
介面類型		選取介面類型，可用來控制剩餘的設定需求和選項： • **HA**—只有在介面是主動/主動部署中兩個防火牆之間的 HA3 連結時，才應選取。選擇性地選取 **Netflow Profile**（**Netflow** 設定檔），然後設定 **LACP** 頁籤上的設定（請參閱啟用 LACP）。 • 虛擬介接—（選用）選取**Netflow Profile**（**Netflow** 設定檔），然後設定 **Config**（設定）和 **Advanced**（進階）頁籤上的設定，如虛擬介接設定中所述。 • 第二層—（選用）選取 **Netflow Profile**（**Netflow** 設定檔）；設定 **Config**（設定）和 **Advanced**（進階）頁籤上的設定，如 第二層介面設定中所述；然後選擇性地設定 **LACP** 頁籤（請參閱啟用 LACP）。 • 第三層—（選用）選取 **Netflow Profile**（**Netflow** 設定檔）；設定 **Config**（設定）頁簽、**IPv4** 或 **IPv6** 頁籤和 **Advanced**（進階）頁籤上的設定，如第三層介面設定中所述；然後選擇性地設定 **LACP** 頁籤（請參閱啟用 LACP）。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 Netflow 伺服器）的 IP 流量，請選取伺服器設定檔或 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱裝置 > 伺服器設定檔 > Netflow）。選取 **None**（無）可從 AE 介面群組移除目前的 NetFlow 伺服器指派。
啟用 LACP	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **LACP**	若要為 AE 介面群組啟用連結彙總控制協定 (LACP)，請選取此選項。預設會停用 LACP。 如果啟用 LACP，將會在實體及資料連結層自動偵測介面失敗，無論是否直接連接防火牆及其 LACP 端點。（若不啟用 LACP，則只會在直接連接的對等間的實體層自動偵測介面失敗。）如果您設定熱備援，則 LACP 還會啟用自動容錯轉移至待命介面的功能（請參閱連接埠上限）。
模式		選取防火牆的 LACP 模式。在任意兩個 LACP 對等之間，我們都建議您設定一個作為主動，另一個作為被動。如果兩個對等都是被動，LACP 將無法運作。 • 被動（預設值）—防火牆會被動回應端點裝置的 LACP 狀態查詢。 • 主動 — 防火牆會主動查詢端點裝置的 LACP 狀態（可用或無法回應）。
傳輸速率		選取防火牆交換查詢和回應端點裝置的速率：

© 2019 Palo Alto Networks, Inc.

彙總介面群組設定	設定位置	說明
		• 快—每秒 • 慢（預設值）—每 30 秒
快速容錯移轉		當介面關閉時，若要讓防火牆在一秒內容錯移轉至操作介面，請選取此選項。否則會以標準 IEEE 802.1AX 所定義的速度（至少三秒）發生容錯移轉。
系統優先順序	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **LACP**（續）	參考連接埠優先順序，用來決定防火牆或其對等是否比他者優先適用的數字（請參閱下面連接埠上限）。 數值越低，優先順序越高（範圍是 *1* 到 *65,535*，預設值為 *32,768*）。
連接埠上限		可在任何指定的時間於 LACP 彙總群組中作用的介面數目 (1-8)。此值不可超過指派給群組的介面數目。如果指派的介面數超出作用中介面數，防火牆會使用介面的 LACP 連接埠優先順序來決定哪些介面將處於待機模式。為群組設定個別介面時，可設定 LACP 連接埠優先順序（請參閱彙總乙太網路 (AE) 介面）。
在 HA 被動狀態下啟用		對於在 HA 主動 / 被動設定中部署的防火牆，選取此選項可允許被動防火牆與其主動對等預先交涉 LACP，再進行容錯轉移。預先交涉可加速容錯轉移，因為被動防火牆不必先交涉 LACP 再變為主動。
主動-被動 HA 使用相同的系統 MAC 位址	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **LACP**（續）	此項目僅適用於在 HA 主動 / 被動設定中部署的防火牆；採用主動 / 主動設定的防火牆需要唯一的 MAC 位址。 HA 防火牆端點具有相同的系統優先順序值。但在主動 / 被動部署中，每個防火牆的系統 ID 可以相同或不同，這取決於您是否指派相同的 MAC 位址。 當 *LACP* 端點（同時處於 *HA* 模式）虛擬化（在網路中顯示為單一裝置）後，若要將容錯移轉期間的延遲降到最低，請對防火牆使用相同的系統 *MAC* 位址。若未虛擬化 *LACP* 端點，為每個防火牆使用唯一的 *MAC* 位址可將容錯移轉延遲降到最低。 LACP 使用 MAC 位址，為每一個 LACP 端點衍生一個系統 ID。如果防火牆配對和端點配對有一致的系統優先順序值，LACP 會使用系統 ID 值，參考連接埠優先順序來決定何者優先適用。如果兩個防火牆有相同的 MAC 位址，則二者會有相同的系統 ID，此 ID 將高於或低於 LACP 端點的系統 ID。如果 HA 防火牆具有唯一的 MAC 位址，則某個 HA 防火牆的系統 ID 可能高於 LACP 端點，另一個則可能有較低的系統 ID。在後者的情況下，當防火牆上發生容錯移轉時，系統會切換 LACP 端點與變為主動的防火牆之間的連接埠優先順序。
MAC 位址	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **LACP**（續）	若 **Use Same System MAC Address**（使用相同的系統 **MAC** 位址），請針對主動 / 被動 HA 配對中的兩個防火牆選取系統產生的 MAC 位址，或輸入您自己的 MAC 位址。您必須確認位址是全域唯一的。

© 2019 Palo Alto Networks, Inc.

彙總乙太網路 (AE) 介面

- Network > Interfaces > Ethernet（網路 > 介面 > Etherent）

若要設定 [彙總乙太網路 (AE) 介面]，請先設定 [彙總乙太網路 (AE) 介面群組]，然後按一下要指派給該群組之介面的名稱。在指派給任何特定群組的介面中，硬體介質可以不同（例如，您可以混合使用光纖和銅線），但頻寬和介面類型（例如，Layer 3）必須相同。另外，介面類型必須與針對 AE 介面群組定義的介面類型相同，但您可以在設定每個介面時將類型變為 **Aggregate Ethernet**（彙總乙太網路）。為每個您指派給群組的介面指定以下資料。

如果您為 *AE* 介面群組啟用了連結彙總控制協定 *(LACP)*，請為該群組中的每個介面選取相同的 *Link Speed*（連結速度）和 *Link Duplex*（連結雙工）。若為不相符的值，認可操作將顯示警告，且 *PAN-OS* 將預設為較高的速度和全雙工。

彙總介面設定	設定位置	說明
介面名稱	彙總乙太網路介面	介面名稱是預先定義的，無法變更。
備註		（選用）輸入介面的說明。
介面類型		選取 **Aggregate Ethernet**（彙總乙太網路）。
彙總群組		將介面指派給彙總群組。
連結速度		選取以 Mbps 為單位的介面速度（**10**、**100**或**1000**），或選取 **auto**（自動）讓防火牆自動決定速度。
連結雙工		選取介面傳輸模式是全雙工 (**full**)、半雙工 (**half**) 還是自動交涉 (**auto**)。
連結狀態		選取介面狀態是已啟用 (**up**)、已停用 (**down**) 還是自動判斷 (**auto**)。
LACP 連接埠優先順序		只有為彙總群組啟用連結彙總控制協定 (LACP)，防火牆才會使用此值。如果指派給群組的介面數超出作用中介面數（連接埠上限欄位），防火牆會使用介面的 LACP 連接埠優先順序來決定哪些介面將處於待命模式。數值越低，優先順序越高（範圍是 1-65,535；預設為 32,768）。
虛擬路由器	**Aggregate Ethernet Interface**（彙總乙太網路介面）> 設定	選取彙總乙太網路介面要指派給哪個虛擬路由器。
安全性區域		選取彙總乙太網路介面要指派給哪個安全性區域。
啟用 Bonjour Reflector	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv4**	（僅限 PA-220、PA-800 和 PA-3200 系列）啟用此選項後，防火牆會將此介面上接收和轉送到此介面的 Bonjour 多點傳送廣告和查詢轉送到啟用了此選項的所有其他 L3 和 AE 介面以及子介面。在出於安全或管理目的而使用區段來路由流量的網路環境中，這有助於確保使用者存取與裝置可探索性。您可以在最多 16 個介面上啟用此選項。
對介面啟用 IPv6	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv6**	選取此選項可在此介面上啟用 IPv6。
介面 ID		以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會

© 2019 Palo Alto Networks, Inc.

彙總介面設定	設定位置	說明
		使用從實體介面的 MAC 位址產生的 EUI-64。如果您在新增位址時 **Use interface ID as host portion**（使用介面 **ID** 作為主機部分），則防火牆會將介面 ID 作為該位址的主機部分。

位址		**Add**（新增）IPv6 位址並設定下列參數：
		• 位址 — 輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立此物件。
		• **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。
		• **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。
		• **Anycast**（任一傳播）—選取以包含最近節點中的路由。
		• 傳送 **RA**—選取此選項可啟用此 IP 位址的路由器公告 (RA)。當您選取此選項時，您也必須在介面上全面 **Enable Router Advertisement**（啟用路由器公告）。如需 RA 的詳細資訊，請參閱啟用路由器公告。
		只有在啟用 RA 後，才會顯示其餘欄位：
		  • **Valid Lifetime**（有效生命週期）—防火牆將位址視為有效的時間長度（以秒為單位）。有效的 SA 生命週期必須等於或超過 **Preferred Lifetime**（慣用 SA 生命週期）。預設值為 2,592,000。
		  • **Preferred Lifetime**（偏好的生命週期）—偏好的有效位址的時間長度（以秒為單位），意味防火牆可使用該位址來傳送和接收流量。當偏好的生命週期到期後，防火牆就無法使用位址來建立新連線，但在超出 **Valid Lifetime**（有效生命週期）前，任何現有連線仍然有效。預設值為 604,800。
		  • 記錄連結—如果不使用路由器即可連線公告首碼內含 IP 位址的系統，請選取此選項。
		  • **Autonomous**（自發）—如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，請選取此選項。

啟用重複的位址偵測	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv6** > **Address Resolution**（位址解析）	選取此選項可啟用重複位址偵測 (DAD)，進而讓您能夠指定 **DAD Attempts**（**DAD** 嘗試）的次數。
DAD 嘗試		指定在識別芳鄰的嘗試失敗之前，DAD 的芳鄰請求間隔（**NS Interval**（NS 間隔））內的嘗試次數（範圍是 1-10，預設為 1）。
可連線時間		指定在成功查詢與回應之後，芳鄰保持可到達狀態的時間長度（以秒為單位，範圍是 1-36,000，預設為 30）。
NS 間隔（芳鄰請求間隔）		指定在指出 DAD 嘗試失敗之前經歷的時間長度（以秒為單位，範圍是 1-10，預設值為 1）。
啟用 NDP 監控		選取此選項可啟用芳鄰發現協定監控。啟用後，您可以選取 NDP（功能欄中的 ），並檢視如下資訊：防火牆所發現到的芳鄰 IPv6 位址、對應的 MAC 位址和 User-ID（假定在最理想的情況下）。
啟用路由器公告	**Aggregate Ethernet**	選取此選項可提供 IPv6 頁面上的芳鄰發現，並設定此區段中的其他欄位。接收路由器公告 (RA) 訊息的 IPv6 DNS 用戶端會使用此資訊。

© 2019 Palo Alto Networks, Inc.

彙總介面設定	設定位置	說明
	Interface（彙總乙太網路介面）> **IPv6** > **Router Advertisement**（路由器公告）	RA 能夠使防火牆成為非靜態設定之 IPv6 主機的預設閘道，並可將用於位址組態的 IPv6 首碼提供給主機。您可以將個別的 DHCPv6 伺服器搭配此功能使用，將 DNS 及其他設定提供給用戶端。 這是介面的全域設定。若要為個別的 IP 位址設定 RA 選項，請在 IP 位址表中 **Add**（新增）位址並加以設定。若要為任何 IP 位址設定 RA 選項，您必須為介面 **Enable Router Advertisement**（啟用路由器公告）。
最小間隔（秒）		指定防火牆所將傳送的 RA 之間的最小間隔（以秒為單位，範圍是 3-1,350，預設值為 200）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
最大間隔（秒）		指定 RA 與防火牆之間將傳送的最大間隔（以秒為單位，範圍是 4-1,800，預設為 600）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
躍點限制		指定要套用至連出封包之用戶端的躍點限制（範圍是 1-255，預設為 64）。輸入 **0** 表示無躍點限制。
連結 MTU		指定要套用至用戶端的連結最大傳輸單位 (MTU)。選取 **Unspecified**（不指定）表示沒有連結 MTU（範圍是 1,280-9,192，預設為不指定）。
可連線時間（毫秒）		指定用戶端在收到可連線能力確認訊息後，用來假設芳鄰可供連線的可連線時間（以毫秒為單位）。選取 **Unspecified**（不指定）表示沒有可連線時間值（範圍是 0-3,600,000，預設為不指定）。
重新傳輸時間（毫秒）		指定重新傳輸計時器，以決定用戶端應該等候多長時間（以毫秒為單位），再重新傳輸芳鄰請求訊息。選取 **Unspecified**（不指定）表示沒有重新傳輸時間（範圍是 0-4,294,967,295，預設為不指定）。
路由器生命週期（秒）		指定用戶端將防火牆作為預設閘道的時間長度（以秒為單位，範圍是 0-9,000，預設為 1,800）。零指定防火牆不是預設閘道。當生命週期到期時，用戶端會從其預設路由器清單中移除防火牆項目，並將其他路由器作為預設閘道。
路由器偏好設定		如果網路區段具有多個 IPv6 路由器，用戶端將使用此欄位來選取偏好的路由器。選取 RA 是否將防火牆路由器公告為具有 **High**（高）、**Medium**（中）（預設值）或 **Low**（低）優先順序（相對於區段上的其他路由器而言）。
受管理的組態		選取此選項可向用戶端指示位址透過 DHCPv6 提供。
其他組態		選取以指出用戶端可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。
一致性檢查	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv6** > 路由器公告（續）	若要防火牆確認從其他路由器傳送的 RA 正在公告連結的一致資訊，請選取此選項。防火牆會記錄系統日誌中任何不一致的情況；類型為 **ipv6nd**。

© 2019 Palo Alto Networks, Inc.

彙總介面設定	設定位置	說明
包含路由器公告中的 DNS 資訊	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv6** > **DNS Support**（**DNS** 支援）	選取此選項可讓防火牆從此 IPv6 彙總乙太網路介面在 NDP 路由器公告 (RA) 訊息中傳送 DNS 資訊。只有在選取此選項後，才能看到此表中的其他 DNS 支援欄位。
伺服器		**Add**（新增）一或多個遞迴 DNS (RDNS) 伺服器位址，以便防火牆從此 IPv6 彙總乙太網路介面在 NDP 路由器公告中傳送。RDNS 伺服器會將一系列 DNS 查詢要求傳送至根 DNS 伺服器和授權 DNS 伺服器，最終將 IP 位址提供給 DNS 用戶端。 您可以設定最多 8 部 RDNS 伺服器，讓防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相同順序使用這些位址。選取伺服器並 **Move Up**（上移）或 **Move Down**（下移）來變更伺服器的順序，或 **Delete**（刪除）您不再需要的伺服器。
SA 生命週期		輸入 IPv6 DNS 用戶端收到可使用 RDNS 伺服器來解析網域名稱之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。
尾碼		**Add**（新增）並設定 DNS 搜尋清單 (DNSSL) 的一或多個網域名稱（尾碼）。最大尾碼長度為 255 個位元組。 DNS 搜尋清單是 DNS 用戶端路由器在名稱輸入 DNS 查詢之前，附加（一次一個）至不合格網域名稱的網域尾碼清單，因而會在 DNS 查詢中使用完全合格網域名稱。例如，如果 DNS 用戶端嘗試針對沒有尾碼的名稱「quality」提交 DNS 查詢，則路由器會在名稱中附加英文句點和 DNS 搜尋清單中的第一個 DNS 尾碼，然後傳輸 DNS 查詢。如果清單上的第一個 DNS 尾碼是「company.com」，則來自路由器的結果 DNS 查詢是針對完全合格網域名稱「quality.company.com」。 如果 DNS 查詢失敗，則路由器會將清單中的第二個 DNS 尾碼附加至不合格名稱並傳輸新的 DNS 查詢。路由器會嘗試 DNS 尾碼，直到 DNS 查詢成功（忽略其餘的尾碼），或直到路由器已嘗試清單上的所有尾碼為止。 在芳鄰發現 DNSSL 選項中使用您要提供給 DNS 用戶端路由器的尾碼設定防火牆；接收 DNSSL 選項的 DNS 用戶端會在其不合格 DNS 查詢中使用這些尾碼。 您可以為 DNS 搜尋清單設定最多 8 個網域名稱（後置詞），以便防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相容順序使用這些位址。選取後置詞並 **Move Up**（上移）或 **Move Down**（下移）來變更後置詞的順序，或 **Delete**（刪除）清單中您不再需要的後置詞。
SA 生命週期	**Aggregate Ethernet Interface**（彙總乙太網路介面）> **IPv6** > **DNS** 支援（續）	輸入 IPv6 DNS 用戶端收到可在 DNS 搜尋清單上使用網域名稱（尾碼）之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > VLAN（網路 > 介面 > VLAN）

VLAN 介面可提供到 Layer 3 網路的路由（IPv4 和 IPv6）。您可以將一或多個第二層乙太網路連接埠（請參閱 PA-7000 Series 第二層介面）新增至 VLAN 介面。

VLAN 介面設定	設定位置	說明
介面名稱	**VLAN** 介面	此唯讀的 **Interface Name**（介面名稱）設為 **vlan**。在相鄰的欄位中，輸入用來識別介面的數值尾碼（1 至 9,999）。
備註		輸入介面的選取性說明。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
VLAN	**VLAN Interface**（**VLAN** 介面）> **Config**（設定）	選取 VLAN，或按一下 **VLAN** 以定義新 VLAN（請參閱 [網路 > VLAN]）。選取 **None**（無）可從介面移除目前的 VLAN 指派。
虛擬路由器		將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
管理設定檔	**VLAN Interface**（**VLAN** 界面）> **Advanced**（進階）> **Other Info**（其他資訊）	管理設定檔 — 選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU		以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 9,192；預設為 1,500）。如果防火牆任一側的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。
調整 TCP MSS		選取以調整最大區段大小 (MSS) 將任何標頭適應介面 MTU 位元組大小範圍。MTU 位元組大小減去 MSS 調整大小等於 MSS 位於組大小，該值視 IP 通訊協定而定： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）—範圍是 40 至 300；預設為 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）—範圍是 60 至 300；預設為 60。 使用這些設定可解決網路中的 **tunnel**（通道）需要較小 MSS 的情況。如果封包必須分段才能擁有大於 MMS 的位元組，則此設定可啟用調整。

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明
		封裝增加了標頭長度，因此有助於設定 MSS 調整大小，使 MPLS 標頭或擁有 VLAN 頁籤的通道流量等可支援該位元組。
IP 位址 MAC 位址 介面	**VLAN Interface**（**VLAN** 介面）> **Advanced**（進階）> **ARP Entries**（**ARP** 項目）	若要新增一或多個靜態位址解析通訊協定 (ARP) 項目，請按一下新增，輸入 IP 位址及其相關聯的硬體 [媒體存取控制 (MAC)] 位址，然後選取可以存取硬體位址的 Layer 3 介面。若要刪除項目，請選取項目並按一下 **Delete**（刪除）。靜態 ARP 項目可減少 ARP 處理並防止指定位址發生攔截式攻擊。
IPv6 位址 MAC 位址	**VLAN Interface**（**VLAN** 介面）> **Advanced**（進階）> **ND Entries**（**ND** 項目）	若要為芳鄰發現協定 (NDP) 新增芳鄰資訊，請按一下 **Add**（新增），然後輸入芳鄰的 IPv6 位址和 MAC 位址。
啟用 NDP Proxy	**VLAN Interface**（**VLAN** 介面）> **Advanced**（進階）> **NDP Proxy**	選取以啟用介面的芳鄰發現協定 (NDP) Proxy。防火牆將回應要求清單中 IPv6 位址其 MAC 位址的 ND 封包。在 ND 回應中，防火牆會為介面傳送自己的 MAC 位址，基本上會表示「將目的地為這些位址的所有封包傳送給我」。 （建議）如果您使用網路首碼轉譯 IPv6 (NPTv6)，則建議您啟用 NDP Proxy。 如果選取 **Enable NDP Proxy**（啟用 NDP Proxy），您可以透過以下步驟篩選許多 **Address**（位址）項目：首先輸入篩選器，然後套用（灰色箭頭）。
位址		按一下 **Add**（新增），輸入一個或多個 IPv6 位址、IP 範圍、IPv6 子網路，或防火牆將作為 NDP Proxy 的位址物件。理論上而言在這些位址中，某一個位址會與 NPTv6 中來源轉譯的位址相同。位址順序不重要。 如果該位址是子網路，防火牆會為子網路中所有的位址傳送 ND 回應，因此我們建議您也新增防火牆的 IPv6 芳鄰，然後按一下 **Negate**（否定）來指示防火牆不要回應這些 IP 位址。
否定		選取位址的 **Negate**（否定）來防止該位址的 NDP Proxy。您可以否定所指定 IP 位址範圍或 IP 子網路的子集。
設定	**VLAN Interface**（**VLAN** 介面）> **Advanced**（進階）> **DDNS**	選取設定讓 DDNS 欄位可以設定。
啟用		啟用介面上的 DDNS。您必須先啟用 DDNS 才能對其進行設定。（如果您的 DDNS 組態未完成，您可以儲存它而不啟用它，這樣您就不會丟失部分組態。）
更新間隔（天數）		輸入防火牆傳送至 DDNS 伺服器的更新之間的間隔（以天數為單位），以更新對應到 FQDN 的 IP 位址（範圍為 1 到 30；預設值為 1）。

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明
		在防火牆收到從 *DHCP* 伺服器為了介面傳送的新 *IP* 位址時還會更新 *DDNS*。
憑證設定檔		選取一個您建立的憑證設定檔（或建立一個新的）來驗證 DDNS 服務。DDNS 服務向防火牆提供由憑證授權單位 (CA) 發佈的憑證。
主機名稱		輸入在 DDNS 伺服器上註冊的介面的主機名稱（例如，host123.domain123.com 或 host123）。除了確認語法是使用 DNS 在網域名稱中允許的有效字元外，防火牆不會驗證主機名稱。
廠商		選取為此介面提供 DDNS 服務的 DDNS 廠商（和版本號碼）： • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** 如果您選取了防火牆指示會在特定日期前逐步淘汰的較舊版本的 *DDNS* 服務，請移至較新版本。 廠商名稱後面的 **Name**（名稱）以及 **Value**（數值）欄位是特定於廠商的。某些欄位是唯讀的，用於通知您防火牆用於連結 DDNS 服務的參數。設定其他欄位，例如 DDNS 服務向您提供的密碼，以及如果防火牆未從 DDNS 伺服器收到回應，防火牆使用的逾時。
IPv4 頁籤 - IP		新增在介面設定的 IPv4 位址，並選取它們。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
IPv6 頁籤 - IPv6	**VLAN Interface**（**VLAN** 介面）> **Advanced**（進階）> **DDNS**(續)	新增在介面設定的 IPv6 位址，並選取它們。所有選定的 IP 位址都會在 DDNS 供應商（廠商）處註冊。
顯示執行階段資訊		顯示 DDNS 註冊情況：DDNS 供應商、已解析的 FQDN 以及帶有星號 (*) 的對應的 IP 位址指示主要 IP 位址。每個 DDNS 供應商都有自己的返回代碼，用於指示主機名稱更新的狀態和返回日期，以便進行疑難排解。
對於 **IPv4** 位址		
類型	**VLAN Interface**（**VLAN** 界面）> **IPv4**	選取將 IPv4 位址類型指派給介面的方法： • **Static**（靜態）—您必須手動指定 IP 位址。 • **DHCP Client**（**DHCP** 用戶端）—啟用介面做為動態主機組態通訊協定 (DHCP) 用戶端，並接收動態指派的 IP 位址。 處於高可用性 *(HA)* 主動/主動組態的防火牆不支援 *DHCP* 用戶端。 頁籤上顯示的選項會視所選的 IP 位址方式而不同。

- IPv4 位址 **Type**（類型）= **Static**（靜態）

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明
ip	**VLAN Interface（VLAN 界面）** > **IPv4**	按一下 **Add**（新增），然後執行下列其中一個步驟來指定靜態介面的 IP 位址與網路遮罩。 • 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：*ip_address/mask*（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 建立類型為 **IP netmask**（**IP** 網路遮罩）的 **Address**（位址）物件。 您可以為介面輸入多個 IP 位址。您的系統使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 **Delete**（刪除）您不再需要的 IP 位址。
IPv4 位址 **Type**（類型）= **DHCP**		
啟用	**VLAN Interface（VLAN 界面）** > **IPv4**	選取此選項可在介面上啟動 DHCP 用戶端。
自動建立指向伺服器所提供之預設閘道的預設路由		選取此選項可自動建立預設路由，指向 DHCP 伺服器提供的預設閘道。
傳送主機名稱		選取設定防火牆（作為 DHCP 用戶端）將介面的主機名稱（選項 12）傳送至 DHCP 伺服器。如果您在預設情況下傳送主機名稱，防火牆的主機名稱會是根據主機名稱欄位決定的。您可以傳送該名稱或輸入自訂主機名稱（最多 64 個字元，包括大寫和小寫字母、數字、句點、連字符和底線。
預設路由度量標準		針對防火牆與 DHCP 伺服器之間的路由，輸入要與預設路由相關聯並用於選取路徑的路由度量標準（優先順序層級，範圍是 1 至 65,535，無預設值）。優先順序層級會隨著數值減少而增加。
顯示 DHCP 用戶端執行階段資訊		選取此選項可顯示接收自 DHCP 伺服器的所有設定，包括 DHCP 租用狀態、動態 IP 指派、子網路遮罩、閘道和伺服器設定（DNS、NTP、網域、WINS、NIS、POP3 和 SMTP）。
對 **IPv6** 位址		
對介面啟用 IPv6	**VLAN Interface（VLAN 界面）** > **IPv6**	選取此選項可在此介面上啟用 IPv6 定址。
介面 ID		以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。
位址	**VLAN Interface（VLAN 界面）** > **IPv6(續)**	按一下 **Add**（新增），並為每個 IPv6 位址設定下列參數： • 位址 — 輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立位址物件。

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明

		• **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。
		• **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。
		• **Anycast**（任一傳播）—選取以包含最近節點中的路由。
		• 傳送 **RA**—選取此選項可啟用此 IP 位址的路由器公告 (RA)。當您選取此選項時，您也必須在介面上全面 **Enable Router Advertisement**（啟用路由器公告）。如需 RA 的詳細資訊，請參閱啟用路由器公告。
		
		只有在啟用 RA 時才適用剩餘的欄位。
		
		  • **Valid Lifetime**（有效生命週期）—防火牆將位址視為有效的時間長度（以秒為單位）。有效的 SA 生命週期必須等於或超過 **Preferred Lifetime**（慣用 SA 生命週期）。預設值為 2,592,000。
		  • **Preferred Lifetime**（偏好的生命週期）—偏好的有效位址的時間長度（以秒為單位），意味防火牆可使用該位址來傳送和接收流量。當偏好的生命週期到期後，防火牆就無法使用位址來建立新連線，但在超出 **Valid Lifetime**（有效生命週期）前，任何現有連線仍然有效。預設值為 604,800。
		  • 記錄連結—如果不使用路由器即可連線公告首碼內含 IP 位址的系統，請選取此選項。
		  • **Autonomous**（自發）—如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，請選取此選項。

啟用重複的位址偵測	**VLAN** 介面 > **IPv6** > 位址解析	選取此選項可啟用重複的位址偵測 (DAD)，讓您指定 **DAD Attempts**（**DAD** 嘗試）次數。
DAD 嘗試		指定在識別芳鄰的嘗試失敗之前，DAD 的芳鄰請求間隔（**NS Interval**（NS 間隔））內的嘗試次數（範圍是 1 至 10，預設為 1）。
可連線時間		指定在成功查詢與回應之後，芳鄰保持可到達狀態的時間長度（以秒為單位，範圍是 1 至 36,000，預設為 30）。
NS 間隔（芳鄰請求間隔）		指定在指示失敗之前，DAD 嘗試的秒數（範圍是 1 至 10，預設為 1）。
啟用 NDP 監控		選取此選項可啟用芳鄰發現協定監控。啟用後，您可以選取 NDP（功能欄中的 ），並檢視如下資訊：防火牆所發現到的芳鄰 IPv6 位址、對應的 MAC 位址和 User-ID（假定在最理想的情況下）。
啟用路由器公告	**VLAN** 介面 > **IPv6** > 路由器公告	選取此選項可提供 IPv6 頁面上的芳鄰發現，並設定此區段中的其他欄位。接收路由器公告 (RA) 訊息的 IPv6 DNS 用戶端會使用此資訊。 RA 能夠使防火牆成為非靜態設定之 IPv6 主機的預設閘道，並可將用於位址組態的 IPv6 首碼提供給主機。您可以將個別的 DHCPv6 伺服器搭配此功能使用，將 DNS 及其他設定提供給用戶端。 這是介面的全域設定。若要為個別的 IP 位址設定 RA 選項，請在 IP 位址表中 **Add**（新增）位址並加以設定。若要為任何 IP 位址設定 RA 選項，您必須為介面 **Enable Router Advertisement**（啟用路由器公告）。

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明
最小間隔（秒）		指定防火牆所將傳送的 RA 之間的最小間隔（以秒為單位，範圍是 3 至 1,350，預設值為 200）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
最大間隔（秒）		指定 RA 與防火牆之間將傳送的最大間隔（以秒為單位，範圍是 4 至 1,800，預設為 600）。防火牆將在您設定的最小值與最大值之間的隨機間隔傳送 RA。
躍點限制		指定要套用至連出封包之用戶端的躍點限制（範圍是 1 至 255，預設為 64）。輸入 **0** 表示無躍點限制。
連結 MTU		指定要套用至用戶端的連結最大傳輸單位 (MTU)。選取 **Unspecified**（不指定）表示沒有連結 MTU（範圍是 1,280 至 9,192，預設為不指定）。
可連線時間（毫秒）		指定用戶端在收到可連線能力確認訊息後，用來假設芳鄰可供連線的可連線時間（以毫秒為單位）。選取 **Unspecified**（不指定）表示沒有可連線時間值（範圍是 0 至 3,600,000，預設為不指定）。
重新傳輸時間（毫秒）		指定重新傳輸計時器決定用戶端應該等候多長時間（以毫秒為單位），再重新傳輸芳鄰請求訊息。選取 **Unspecified**（不指定）表示沒有重新傳輸時間（範圍是 0 至 4,294,967,295，預設為不指定）。
路由器生命週期（秒）		指定用戶端將防火牆作為預設閘道的時間長度（以秒為單位，範圍是 0 至 9,000，預設為 1,800）。零指定防火牆不是預設閘道。當生命週期到期時，用戶端會從其預設路由器清單中移除防火牆項目，並將其他路由器作為預設閘道。
路由器偏好設定		如果網路區段具有多個 IPv6 路由器，用戶端將使用此欄位來選取偏好的路由器。選取 RA 是否將防火牆路由器公告為具有 **High**（高）、**Medium**（中）（預設值）或 **Low**（低）優先順序（相對於區段上的其他路由器而言）。
受管理的組態		選取此選項可向用戶端指示位址透過 DHCPv6 提供。
其他組態		選取以指出用戶端可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。
一致性檢查	**VLAN** 介面 > **IPv6** > 路由器公告（續）	若要防火牆確認從其他路由器傳送的 RA 正在公告連結的一致資訊，請選取此選項。防火牆會記錄系統日誌中任何不一致的情況；類型為 **ipv6nd**。
包含路由器公告中的 DNS 資訊	**VLAN Interface**（**VLAN** 介面）> **IPv6** > **DNS Support**（**DNS** 支援）	選取此選項可讓防火牆從此 IPv6 VLAN 介面在 NDP 路由器公告中傳送 DNS 資訊。只有在選取此選項後，才能看到此表中的其他 DNS 支援欄位。
伺服器		**Add**（新增）一或多個遞迴 DNS (RDNS) 伺服器位址，以便防火牆從此 IPv6 VLAN 介面在 NDP 路由器公告中傳送。RDNS 伺服器會將一系列 DNS 查詢要求傳送至根 DNS 伺服器和授權 DNS 伺服器，最終將 IP 位址提供給 DNS 用戶端。 您可以設定最多 8 部 RDNS 伺服器，讓防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相同順序使用這

© 2019 Palo Alto Networks, Inc.

VLAN 介面設定	設定位置	說明
		些伺服器。選取伺服器並 **Move Up**（上移）或 **Move Down**（下移）來變更伺服器的順序，或 **Delete**（刪除）清單中您不再需要的伺服器。
SA 生命週期		輸入 IPv6 DNS 用戶端收到可使用 RDNS 伺服器來解析網域名稱之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。
尾碼		**Add**（新增）並設定 DNS 搜尋清單 (DNSSL) 的一或多個網域名稱（尾碼）。最大尾碼長度為 255 個位元組。 DNS 搜尋清單是 DNS 用戶端路由器在名稱輸入 DNS 查詢之前，附加（一次一個）至不合格網域名稱的網域尾碼清單，因而會在 DNS 查詢中使用完全合格網域名稱。例如，如果 DNS 用戶端嘗試對沒有尾碼的名稱「quality」提交 DNS 查詢，則路由器會將一個期間和 DNS 搜尋清單中的第一個 DNS 尾碼附加至該名稱，然後傳輸 DNS 查詢。如果清單上的第一個 DNS 尾碼是「company.com」，則來自路由器的結果 DNS 查詢是針對完全合格網域名稱「quality.company.com」。 如果 DNS 查詢失敗，則路由器會將清單中的第二個 DNS 尾碼附加至不合格名稱並傳輸新的 DNS 查詢。路由器會嘗試 DNS 尾碼，直到 DNS 查詢成功（忽略其餘的尾碼），或直到路由器已嘗試清單上的所有尾碼為止。 在芳鄰發現 DNSSL 選項中使用您要提供給 DNS 用戶端路由器的尾碼設定防火牆；接收 DNSSL 選項的 DNS 用戶端會在其不合格 DNS 查詢中使用這些尾碼。 您可以為 DNS 搜尋清單設定最多 8 個網域名稱（尾碼），以便防火牆在 NDP 路由器公告中傳送（從上至下列出的順序）給收件者，然後收件者可依相容順序使用這些位址。選取尾碼並 **Move Up**（上移）或 **Move Down**（下移）來變更順序，或 **Delete**（刪除）清單中您不再需要的尾碼。
SA 生命週期		輸入 IPv6 DNS 用戶端收到可在 DNS 搜尋清單上使用網域名稱（尾碼）之路由器公告後的最大秒數（範圍是最大間隔（秒）的值到最大間隔的兩倍；預設值是 1,200）。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > Loopback（網路 > 介面 > 回送）

使用下列欄位，設定回送介面：

回送介面設定	設定位置	說明
介面名稱	回送介面	此唯讀的 **Interface Name**（介面名稱）設為 **loopback**。在相鄰的欄位中，輸入用來識別介面的數值尾碼 (1-9999)。
備註		輸入介面的選取性說明。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
虛擬路由器	**Loopback Interface**（回送介面）> **Config**（設定）	將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
管理設定檔	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **Other Info**（其他資訊）	管理設定檔 — 選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU		以位元組為單位，輸入在此介面上載送之封包的最大傳輸單位 (MTU)（576-9,192；預設為 1,500）。如果防火牆任一側的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。
調整 TCP MSS		選取以調整最大區段大小 (MSS) 將任何標頭適應介面 MTU 位元組大小範圍。MTU 位元組大小減去 MSS 調整大小等於 MSS 位於組大小，該值視 IP 通訊協定而定： • **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）—範圍是 40-300；預設為 40。 • **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）—範圍是 60-300；預設為 60。 使用這些設定可解決網路中的 **tunnel**（通道）需要較小 MSS 的情況。如果封包必須分段才能擁有大於 MMS 的位元組，則此設定可啟用調整。 封裝增加了標頭長度，因此有助於設定 MSS 調整大小，使 MPLS 標頭或擁有 VLAN 頁籤的通道流量等可支援該位元組。

© 2019 Palo Alto Networks, Inc.

回送介面設定	設定位置	說明
對於 **IPv4** 位址		
ip	**Loopback Interface**（回送界面）> **IPv4**	按一下 **Add**（新增），然後執行下列其中一個步驟來指定靜態介面的 IP 位址與網路遮罩。 • 輸入 IPv4 位址及自網路遮罩 /32；例如 192.168.2.1/32。僅支援 /32 子網路遮罩。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 按一下 **Address**（位址）以建立類型為 **IP netmask**（IP 網路遮罩）的位址物件。 您可以為介面輸入多個 IP 位址。您的系統使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 若要刪除 IP 位址，請選取位址並按一下 **Delete**（刪除）。
對 IPv6 位址		
對介面啟用 IPv6	**Loopback Interface**（回送界面）> **IPv6**	選取此選項可在此介面上啟用 IPv6 定址。
介面 ID		以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。
位址		按一下 **Add**（新增），並為每個 IPv6 位址設定下列參數： • 位址 — 輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立位址物件。 • **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。 • **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。 • **Anycast**（任一傳播）—選取以包含最近節點中的路由。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > Tunnel（網路 > 介面 > 通道）

使用下列欄位，設定通道介面：

通道介面設定	設定位置	說明
介面名稱	隧道接口	此唯讀的 **Interface Name**（介面名稱）設為 **tunnel**。在相鄰的欄位中，輸入用來識別介面的數值尾碼 (1-9999)。
備註		輸入介面的選取性說明。
Netflow 設定檔		如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
虛擬路由器	**Tunnel Interface**（通道界面）> **Config**（設定）	將虛擬路由器指派給介面，或按一下 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 [網路 > 虛擬路由器]）。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統		如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或按一下 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域		選取介面的安全性區域，或按一下 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。
管理設定檔	**Ethernet Interface**（乙太網路介面）> **Advanced**（進階）> **Other Info**（其他資訊）	管理設定檔 — 選取定義通訊協定（例如，SSH、Telnet 和 HTTP）的設定檔，亦即可讓您透過此介面管理防火牆的設定檔。選取 **None**（無）可從介面移除目前的設定檔指派。
MTU		以位元組為單位，輸入在此介面上載送之封包的最大傳輸單位 (MTU)（576-9,192；預設為 1,500）。如果防火牆任一側的電腦執行路徑 MTU 探索 (PMTUD)，且介面接收到超過 MTU 的封包，防火牆會將需要 *ICMP* 分段訊息傳回來源以指出封包過大。
對於 IPv4 位址		
ip	**Tunnel Interface**（通道界面）> **IPv4**	按一下 **Add**（新增），然後執行下列其中一個步驟來指定靜態介面的 IP 位址與網路遮罩。 • 在無類別網域間路由選擇 (CIDR) 標記法中輸入項目：ip_address/mask（例如 192.168.2.0/24）。 • 選取類型為 **IP netmask**（**IP** 網路遮罩）的現有位址物件。 • 按一下 **Address**（位址）以建立類型為 **IP netmask**（IP 網路遮罩）的位址物件。 您可以為介面輸入多個 IP 位址。您的系統使用的轉送資訊庫 (FIB) 決定 IP 位址數上限。 若要刪除 IP 位址，請選取位址並按一下 **Delete**（刪除）。

© 2019 Palo Alto Networks, Inc.

通道介面設定	設定位置	說明
對 IPv6 位址		
對介面啟用 IPv6	**Tunnel Interface**（通道界面）> **IPv6**	選取此選項可在此介面上啟用 IPv6 定址。
介面 ID	**Tunnel Interface**（通道界面）> **IPv6**	以十六進位格式輸入 64 位元延伸唯一識別碼 (EUI-64)（例如，00:26:08:FF:FE:DE:4E:29）。如果您將此欄位保留空白，防火牆會使用從實體介面的 MAC 位址產生的 EUI-64。若在新增位址時啟用 **Use interface ID as host portion**（使用介面 ID 作為主機部分）選項，防火牆會將介面 ID 作為該位址的主機部分。
位址		按一下 **Add**（新增），並為每個 IPv6 位址設定下列參數： • 位址 — 輸入 IPv6 位址及首碼長度（例如，2001:400:f00::1/64）。您也可以選取現有的 IPv6 位址物件，或按一下 **Address**（位址）以建立位址物件。 • **Enable address on interface**（啟用介面上的位址）—選取以啟用介面上的 IPv6 位址。 • **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—選取以將 **Interface ID**（介面 **ID**）作為 IPv6 位址的主機部分。 • **Anycast**（任一傳播）—選取以包含最近節點中的路由。

© 2019 Palo Alto Networks, Inc.

Network > Interfaces > SD-WAN（網路 > 介面 > SD-WAN）

建立虛擬 SD-WAN 介面並新增將進入同一個目的地的乙太網路介面編號。

SD-WAN 介面設定	
介面名稱	此唯讀的 **Interface Name**（介面名稱）設為 **sdwan**。在相鄰的欄位中，輸入用來識別虛擬 SD-WAN 介面的數值尾碼（1 至 9,999）。
備註	最佳做法是輸入介面的使用者易記的說明，例如 `to internet` 或 `to Western USA hub`。您的註解可讓識別介面更為輕鬆，無需再嘗試解碼日誌和報告中自動產生的名稱。
Netflow 設定檔	如果您要匯出單向（亦即從進入介面周遊至 NetFlow 伺服器）的 IP 流量，請選取伺服器設定檔，或按一下 **Netflow Profile**（**Netflow** 設定檔）來定義新設定檔（請參閱 [裝置 > 伺服器設定檔 > Netflow]）。選取 **None**（無）可從介面移除目前的 NetFlow 伺服器指派。
設定頁籤	
虛擬路由器	將虛擬路由器指派給介面，或選取 **Virtual Router**（虛擬路由器）以定義新路由器（請參閱 Network > Virtual Routers（網路 > 虛擬路由器））。選取 **None**（無）可從介面移除目前的虛擬路由器指派。
虛擬系統	如果防火牆支援多個虛擬系統，並已啟用該功能，請為介面選取虛擬系統 (vsys)，或選取 **Virtual System**（虛擬系統）以定義新 vsys。
安全性區域	選取介面的安全性區域，或選取 **Zone**（區域）以定義新區域。選取 **None**（無）可從介面移除目前的區域指派。虛擬 SD-WAN 介面及其所有介面成員必須在一個相同的安全性區域中，以確保將相同的安全性政策規則套用到從分支到相同目的地的所有路徑。
進階頁籤	
介面	選取第三層乙太網路介面（對於 Direct Internet Access [直接網際網絡存取 - DIA]) 或組成此虛擬 SD-WAN 介面的虛擬 VPN 通道介面（對於中樞）。防火牆虛擬路由器使用此虛擬 SD-WAN 介面將 SD-WAN 流量路由到一個 DIA 或中樞位置。介面可以具有不同的標籤。如果您輸入多個介面，它們必須是相同類型（VPN 通道或 DIA）。

© 2019 Palo Alto Networks, Inc.

Network > Zones（網路 > 區域）

下列主題說明網路安全性區域。

您想了解什麼內容？	請參閱：
安全性區域的作用是什麼？	安全性區域概要
可用來設定安全性區域的欄位有哪些？	安全性區域的建置組塊
想知道更多？	使用介面與區域來分割網路

安全性區域概要

安全性區域採用邏輯方法對防火牆上實體與虛擬介面分組，以便控制及記錄在網路上周遊特定介面的流量。必須先將防火牆上的介面指派給安全性區域，介面才能處理流量。一個區域可能會被指派同一類型的多個介面（例如旁接、第二層、第三層介面），但一個介面只能屬於一個區域。

防火牆上的安全性政策使用安全性區域來識別流量的來源及目的地。流量可在區域內自由流動，但在您定義允許流動的安全性政策規則之前，流量無法在不同區域間流動。若要允許或拒絕區域間流量，安全性政策規則必須參考來源區域與目的地區域（而非介面），且區域必須是相同類型；也就是說，安全性政策規則僅能允許或拒絕從一個第二層區域到另一個第二層區域的流量。

安全性區域的建置組塊

若要定義安全性區域，請按一下 **Add**（新增），並指定下列資訊。

安全性區域設定	說明
名稱	輸入區域名稱（最多 31 個字元）。定義安全原則及設定介面時，此名稱會顯示在區域清單中。名稱區分大小寫且必須在整個虛擬路由器中是唯一的。請僅使用字母、數字、空格、連字號、句點與底線。
位置	只有在防火牆支援多個虛擬系統 (vsys) 並啟用該容量時才會顯示此欄位。選取此區域適用的 vsys。
類型	選取區域類型（**Tap**（旁接）、**Virtual Wire**（虛擬介接）、**Layer2**（第二層）、**Layer3**（第三層）、**External**（外部）或 **Tunnel**（通道）），可檢視所有尚未指派給區域的該類型 **Interfaces**（介面）。Layer 2 與 Layer 3 區域類型可列出該類型的所有 Ethernet 介面與子介面。**Add**（新增）您想要指派給區域的介面。 外部區域用於控制單一防火牆上多個虛擬系統的流量。它只會在支援多重虛擬系統的防火牆上顯示，且只有在啟用 **Multi Virtual System Capability**（多重虛擬系統功能）時。如需外部區域的詳細資訊，請參閱保留在防火牆內的 VSYS 間流量。 介面可只屬於某個虛擬系統中的一個區域。

© 2019 Palo Alto Networks, Inc.

安全性區域設定	說明
介面	向區域新增一個或多個介面。
區域保護設定檔	選取指定防火牆對於來自此區域的攻擊將如何回應的設定檔。若要建立新的設定檔，請參閱 [網路 > 網路設定檔 > 區域保護]。最佳做法是使用區域保護設定檔保護每個區域。
啟用封包緩衝區保護	在全域設定封包緩衝區保護（裝置 > 設定 > 工作階段）並在每個區域應用。防火牆僅將封包緩衝區保護應用於進入區域。預設會啟用根據緩衝區使用百分比的封包緩衝區保護。替代方案是基於延遲設定封包緩衝區保護。最佳做法是在每個區域上啟用封包緩衝區保護以保護防火牆緩衝區。
日誌設定	選取用來將區域保護日誌轉送至外部系統的日誌轉送設定檔。 如果您有名為「預設」的日誌轉送設定檔，則在定義新的安全性區域時，將會在此下拉式清單中自動選取該設定檔。您可以在設定新的安全性區域時繼續選取不同的日誌轉送設定檔，而隨時取代此預設設定。若要定義或新增日誌轉送設定檔（並將設定檔命名為「預設」，以自動填入此下拉式清單），請按一下 **New**（新增）（請參考 [物件 > 日誌轉送]）。 如果您設定 *Panorama* 範本中的區域，*Log Setting*（日誌設定）下拉式清單只會列出共用的日誌轉送設定檔；若要指定非共用設定檔，您必須輸入其名稱。
啟用使用者識別	如果您已設定 User-ID™ 來執行 IP 位址至使用者名稱對應（探索），啟用使用者識別可將對應資訊套用至此區域中的流量。如果您清除此選項，則防火牆日誌、報告與原則將排除區域內流量的使用者對應資訊。 依預設，如果您選取此選項，防火牆會將使用者對應資訊套用到區域中所有子網路的流量上。若要將資訊限制到區域內的特定子網路，請使用包含清單與排除清單。 請僅在受信任的區域上啟用 *User-ID*。如果您在外部不受信任的區域（例如網際網路）上啟用 *User-ID* 和用戶端探查，則探查可能會傳送至您受保護的網路以外，而導致 *User-ID* 代理程式服務帳戶名稱、網域名稱和加密密碼雜湊等資訊的揭露，進而讓攻擊者得以對受保護的資源進行未經授權的存取。 只有在區域是位於 *User-ID* 監控的網路範圍內時，*User-ID* 才會對該區域執行發現。如果區域不在該範圍內，防火牆不會將使用者對應資訊套用到區域流量，即使您選取了 *Enable User Identification*（啟用使用者識別）。如需詳細資訊，請參閱在使用者對應中包含或排除子網路。
使用者識別 ACL 包含清單	依預設，如果未指定此清單中的子網路，則防火牆會將其發現的使用者對應資訊套用到此區域的所有流量上，以用於日誌、報告和原則中。 若要限制將使用者對應資訊運用到區域內的特定子網路，然後再運用到每個子網路上，請按一下 **Add**（新增），然後選取位址（或位址群組）物件，或輸入 IP 位址範圍（例如，10.1.1.1/24）。**Include List**（包含清單）是一份允許清單，排除所有其他子網路是隱含的，因此您不必將這些子網路新增至 **Exclude List**（排除清單）。

© 2019 Palo Alto Networks, Inc.

安全性區域設定	說明
	將項目新增到 **Exclude List**（排除清單）只會排除 **Include List**（包含清單）中子網路子集的使用者對應資訊。例如，如果您將 10.0.0.0/8 新增至包含清單，並將 10.2.50.0/22 新增至排除清單，則防火牆會包含 10.2.50.0/22 以外所有 10.0.0.0/8 區域子網路的使用者對應資訊，,並排除 10.0.0.0/8 之外所有區域子網路的資訊。 您只能包含在 *User-ID* 監控之網路範圍內的子網路。如需詳細資訊，請參閱在使用者對應中包含或排除子網路。
使用者識別 ACL 排除清單	若要在 **Include List**（包含清單）中排除子網路子集的使用者對應資訊，請針對每個要排除的子網路 **Add**（新增）位址（或位址群組）物件，或鍵入 IP 位址範圍。 如果您將項目新增至 *Exclude List*（排除清單），但未新增至 *Include List*（包含清單），則防火牆會排除區域內所有子網路的使用者對應資訊，而非僅排除您新增的子網路。

© 2019 Palo Alto Networks, Inc.

Network > VLANs（網路 > VLAN）

防火牆支援符合 IEEE 802.1Q 標準的 VLAN。在防火牆上定義的每個第二層介面都可以與 VLAN 相關聯。可以將同一個 VLAN 指定給多個第二層介面，但每個介面只能屬於一個 VLAN。

VLAN 設定	說明
名稱	輸入 VLAN 名稱（最多 31 個字元）。設定介面時，此名稱會顯示在 VLAN 清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
VLAN 介面	選取 [網路 > 介面 > VLAN] 以允許在 VLAN 外部路由傳送流量。
介面	指定 VLAN 的防火牆介面。
靜態 MAC 組態	指定介面，可透過此介面到達 MAC 位址。此設定項將覆蓋任何已記住的介面與 MAC 對應。

© 2019 Palo Alto Networks, Inc.

Network > Virtual Wires（網路 > Virtual Wire）

選取 **Network**（網路） > **Virtual Wires**（虛擬介接） 可在防火牆上指定兩個虛擬介接介面後，定義虛擬介接（ 網路 > 介面 ）。

虛擬介接設定	說明
Virtual Wire 名稱	輸入虛擬介接名稱（最多 **31** 個字元）。設定介面時，此名稱會顯示在 Virtual Wire 清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
介面	從 Virtual Wire 設定的已顯示清單中，選取兩個 Ethernet 介面。只有當介面具有 Virtual Wire 介面類型且尚未指定給另一個 Virtual Wire 時，才會在此處列出介面。 如需虛擬介接介面的詳細資訊，請參閱虛擬介接介面。
允許加標籤	針對 Virtual Wire 上允許的流量，輸入標籤編號 (0-4094) 或標籤編號範圍 (tag1-tag2)。標籤值為 0（預設值）表示未標記的流量。多個標籤或範圍必須以逗號隔開。會丟棄具有已排除標籤值的流量。 不會變更連入或連出封包上的標籤值。 利用虛擬介接子介面時，**Tag Allowed**（允許加標籤）清單會將列出的標籤所有的流量分類為父虛擬介接。Virtual Wire 子介面必須利用父系的 **Tag Allowed**（允許加標籤）清單中不存在的標籤。
多點傳送防火牆	如果您想要能夠將安全性規則套用至多點傳送流量，請選取此選項。如果沒有啟用此設定，則會在 Virtual Wire 上轉送多點傳送流量。
連結狀態通過	如果您要在偵測到關閉連結狀態的情況下關閉虛擬介接配對中的另一個介面，請選取此選項。如果您不選取或停用此選項，Virtual Wire 間不會傳播連結狀態。

© 2019 Palo Alto Networks, Inc.

Network > Virtual Routers（網路 > 虛擬路由器）

使用您手動定義的靜態路由或透過參與 Layer 3 路由通訊協定（動態路由），防火牆需要虛擬路由器來取得到其他子網路的路由。在防火牆上定義的每個 Layer 3 介面、回送介面及 VLAN 介面都必須與虛擬路由器相關聯。每個介面都可以只屬於一個虛擬路由器。

定義虛擬路由器需要進行一般設定及靜態路由或動態路由通訊協定的任何組合，視網路要求而定。您也可設定其他功能，例如路由重新分配及 ECMP。

您想了解什麼內容？	請參閱
虛擬路由器有哪些必要元件？	虛擬路由器的一般設定
設定：	靜態路由 路由重新散佈 RIP OSPF OSPFv3 BGP IP 多點傳送 ECMP
檢視虛擬路由器的相關資訊。	更多的虛擬路由器執行階段統計資料
想知道更多？	網路

虛擬路由器的一般設定

- 網路> 虛擬路由器 > 路由器設定 > 一般

所有虛擬路由器都需要您指派下表所述的第三層介面和管理距離公制。

虛擬路由器的一般設置	說明
名稱	指定用來說明虛擬路由器的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
介面	選取您要包含在虛擬路由器中的介面。因此，它們可用作虛擬路由器路由表中的傳出介面。 若要指定介面類型，請參考 [網路 > 介面]。 新增介面時，會自動新增其連線的路由。
管理距離	指定下列管理距離：

© 2019 Palo Alto Networks, Inc.

虛擬路由器的一般設置	說明
	• 靜態路由 — 範圍是 10-240；預設為 10。 • **OSPF** 內部—範圍是 10-240；預設為 30。 • **OSPF** 外部—範圍是 10-240；預設為 110。 • **IBGP** — 範圍是 10-240；預設為 200。 • **EBGP** — 範圍是 10-240；預設為 20。 • **RIP** — 範圍是 10-240；預設為 120。

靜態路由

- Network > Virtual Routers > Static Routes（網路 > 虛擬路由器 > 靜態路由）

選取新增一個或多個靜態路由。按一下 **IP** 或 **IPv6** 頁籤，指定使用 IPv4 或 IPv6 位址的路由。通常，您需要在此處設定預設路由 (0.0.0.0/0)。預設路由適用於目的地，以其他方式無法在虛擬路由器的路由表中找到這些項目。

靜態路由設定	說明
名稱	輸入用來識別靜態路由的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
目的地	在無類別網域間路由選取 (CIDR) 標記法中輸入 IP 位址和網路遮罩：*ip_address*/ 遮罩 （例如，適用於 IPv4 的 192.168.2.0/24，或適用於 IPv6 的 2001:db8::/32）。或者，您可以建立類型為 IP 網路遮罩的位址物件。
介面	選取用來將封包轉送至目的地的介面，或設定下一個躍點設定，或執行這兩項操作。
下一個躍點	選取下列其中一項： • **IP Address**（**IP** 位址）—選取以輸入下一躍點路由器的 IP 位址，或選取或建立類型 IP 網路遮罩的位址物件。IPv4 的位址物件必須有 /32 的網路遮罩，IPv6 則是 /128。 • 下一個 **VR** — 選取此選項以選取防火牆中的虛擬路由器做為下一個躍點。這可讓您在單一防火牆中的虛擬路由器之間內部路由。 • **FQDN**—選取以透過 FQDN 識別下一個躍點。然後選取類型 FQDN 的位址物件或建立類型 FQDN 的新位址物件。 • **Discard**（捨棄）—選取您是否想丟棄定址到此目的地的流量。 • **None**（無）—如果路由沒有下一個躍點，請選取此選項。
管理員距離	為靜態路由指定管理距離（10-240；預設為 10）。
指標	為靜態路由指定有效公制 (1 - 65535)。
路由表	選取防火牆安裝靜態路由的路由表： • 單點傳送—將路由安裝至單點傳送路由表。 • 多點傳送—將路由安裝至多點傳送路由表。 • 兩者—將路由安裝至單點傳送與多點傳送路由表。 • 不安裝—不將路由安裝至路由表 (RIB)；防火牆會保留靜態路由以供未來參考，直到您刪除路由為止。

© 2019 Palo Alto Networks, Inc.

靜態路由設定	說明
RFD 設定檔	若要對 PA-3200 系列、PA-5200 系列、PA-7000 系列或 VM 系列防火牆上的靜態路由啟用雙向轉送偵測 (BFD)，請選取下列其中一項： • **default**（預設）（預設 BFD 設定） • 您已在防火牆上建立的 BFD 設定檔 • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔 選取 **None (Disable BFD)**（無（停用 **BFD**）），可對靜態路由停用 BFD。 若要在靜態路由上使用 BFD： • 防火牆及靜態路由的另一端的對等體都必須支援 BFD 工作階段。 • 靜態路由 **Next Hop**（下一個躍點）類型必須是 **IP Address**（IP 位址），且您必須輸入有效的 IP 位址。 • **Interface**（介面）設定不能是 **None**（無）；您必須選取一個介面（即時您使用 DHCP 位址）。
路徑監控	選取以啟用靜態路由的路徑監控。
失敗條件	選取防火牆將監控的路徑視為關閉、因此將靜態路徑視為關閉的條件： • 任何—若靜態路由的任一監控的目的地無法透過 ICMP 連線，防火牆會自 RIB 和 FIB 移除靜態路由，並在動態或靜態路由中，將通向同一目的地的度量為次低者新增至 FIB。 • 所有—若靜態路由的所有監控的目的地皆無法透過 ICMP 連線，防火牆才會自 RIB 和 FIB 移除靜態路由，並在動態或靜態路由中，將通向同一目的地的度量為次低者新增至 FIB。 選取 **All**（所有）能避免（例如）監控的目的地僅因維護而離線時，單一監控的目的地發出靜態路由失敗的信號。
先佔保留時間 (分鐘)	輸入已關閉路徑監控必須保持使用中狀態的分鐘數—該路徑監控會評估其所有監控的目的地成員，且在防火牆將靜態路由重新安裝至 RIB 前，必須保持為使用中。如果計時器到期且連結不關閉或波動，則該連結將被視為穩定，路徑監控可保持為使用中，防火牆可將靜態路由再次新增到 RIB 中。 若在保留時間內連結關閉或波動，則路徑監控會失敗，且當關閉的監控回到使用中狀態時，計時器會重新啟動。若 **Preemptive Hold Time**（先佔保留時間）為 0，會讓防火牆在路徑監控進入使用中狀態時立刻將靜態路由重新安裝至 RIB。範圍為 0-1440；預設值為 2。
名稱	輸入監控的目的地名稱（最多 31 個字元）。
啟用	選取則會為靜態路由啟用對此特定目的地的路徑監控；防火牆會將 ICMP ping 傳送至此目的地。
來源 IP	選取 IP 位址，在對監控的目的地的 ICMP ping 中，防火牆將使用此位址作為來源： • 若介面有多個 IP 位址，請選取一個。 • 依預設，若您選取介面，防火牆會使用指派給介面的第一個 IP 位址。 • 若您選取 **DHCP (Use DHCP Client address)**（**DHCP**（使用 **DHCP** 用戶端位址）），防火牆會使用 DHCP 指派給介面的位址。若要查看 DHCP 位址，可選取**Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）並在

© 2019 Palo Alto Networks, Inc.

靜態路由設定	說明
	乙太網路介面的列中，然後按一下 **Dynamic DHCP Client**（動態 **DHCP** 用戶端）。IP 位址會顯示在動態 IP 介面狀態視窗中。
目的地 Ip	輸入健全、穩定的 IP 位址或位址物件，防火牆將針對該位址進行路徑監控。監控的目的地和靜態路由目的地必須使用相同位址家族（IPv4 或 IPv6）。
Ping 間隔（秒）	以秒為單位指定 ICMP ping 間隔，以決定防火牆監控路徑的頻率（ping 監控的目的地；範圍是 1-60；預設為 3）。
Ping 計數	在此指定者，為防火牆將連結視為關閉前，ICMP ping 封包不從監控的目的地傳回的連續數量。根據 **Any**（任何）或 **All**（全部）失敗條件，若路徑監控在失敗狀態中，則防火牆會自 RIB 移除靜態路由（範圍是 3-10；預設為 5）。 例如，Ping 間隔為 3 秒且 Ping 計數為錯失 ping 5 次（防火牆在過去 15 秒中沒有接收到 ping）表示路徑監控偵測到連結失敗。若路徑監控在失敗狀態中，且防火牆在 15 秒後接收到 ping，則連結會被視為使用中；根據 **Any**（任何）或 **All**（全部）失敗條件，對 **Any**（任何）或 **All**（全部）監控的目的地的路徑監控可被視為使用中，且先佔保留時間會啟動。

路由重新散佈

- Network > Virtual Router > Redistribution Profiles（網路 > 虛擬路由器 > 重新分配設定檔）

重新散佈設定檔可根據需要的網路行為，導向要篩選的防火牆、設定優先順序及執行動作。路由重新分配允許靜態路由與其他通訊協定取得的路由（透過指定路由通訊協定宣告）。

重新分配設定檔必須適用於路由通訊協定，才能發揮作用。如果沒有重新分配規則，每個通訊協定都會分別執行，且不會在其範圍以外通訊。您可以在設定所有路由設定並建立產生的網路拓撲之後，新增或修改重新分配設定檔。

透過定義匯出規則，將重新分配設定檔套用至 RIP 與 OSPF 通訊協定。在 **Redistribution Rules**（重新分配規則）頁籤中，將重新分配設定檔套用至 BGP。請參閱下表。

重新散佈設定檔設定	說明
名稱	**Add**（新增）**Redistribution Profile**（重新散佈設定檔）並輸入設定檔名稱。
優先順序	輸入此設定檔的優先順序（範圍是 1-255）。會按順序比對設定檔（編號越小越先比對）。
重新散佈	選取是否要根據此視窗上的設定執行路由重新分配。 • 重新分配 — 選取此動作可重新分配相符候選路由。如果您選取此選項，請輸入新公制值。公制值越低表示越偏好的路由。 • 無重新分配 — 選取此動作可不重新分配相符候選路由。
General Filter 頁籤	
類型	選取侯選路由的路由類型。
介面	選取介面可指定侯選路由的轉送介面。

© 2019 Palo Alto Networks, Inc.

重新散佈設定檔設定	說明
目的地	若要指定侯選路由的目的地，請輸入目的地 IP 位址或子網路（格式 x.x.x.x 或 x.x.x.x/n），然後按一下新增。若要移除項目，請按一下刪除 (⊖)。
下一個躍點	若要指定侯選路由的閘道，請輸入代表下一個躍點的 IP 位址或子網路（格式 x.x.x.x 或 x.x.x.x/n），然後按一下 **Add**（新增）。若要移除項目，請按一下刪除 (⊖)。
OSPF 篩選器頁籤	
路徑類型	選取侯選 OSPF 路由的路由類型。
區塊	為候選 OSPF 路由指定區域識別碼。輸入 **OSPF area ID**（**OSPF 區域 ID**）（格式 x.x.x.x），然後按一下 **Add**（新增）。 若要移除項目，請按一下刪除 (⊖)。
頁籤	指定 OSPF 頁籤值。輸入數值頁籤值 (1-255)，再按一下 Add（新增）。 若要移除項目，請按一下刪除 (⊖)。
BGP 篩選器頁籤	
社群	為 BGP 路由原則指定社群。
延伸社群	為 BGP 路由原則指定延伸社群。

RIP

- Network > Virtual Routers > RIP（網路 > 虛擬路由器 > RIP）

設定路由資訊協定 (RIP) 包括下列一般設定：

RIP 設定	說明
啟用	選取以啟用 RIP。
拒絕預設路由	（建議）如果您不想透過 RIP 記住任何預設路由，請選取此選項。
BFD	若要對 PA-5200 系列、PA-7000 系列及 VM 系列防火牆上的虛擬路由全局啟用 RIP 雙向轉送偵測 (BFD)，請選取下列其中一項： • **default**（預設）（使用預設 BFD 設定的設定檔） • 您已在防火牆上建立的 BFD 設定檔 • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔 選取 **None (Disable BFD)**（無（停用 **BFD**））可對虛擬路由器的所有 RIP 介面停用 BFD；您無法對單一 RIP 介面啟用 RFD。

此外，必須在下列頁籤上進行 RIP 設定：

- **Interfaces**（介面）：請參閱 RIP 介面頁籤。

© 2019 Palo Alto Networks, Inc.

- **Timers**（計時器）：請參閱 RIP 計時器頁籤。
- **Auth Profiles**（驗證設定檔）：請參閱 RIP 驗證設定檔頁籤。
- **Export Rules**（匯出規則）：請參閱 RIP 匯出規則頁籤。

RIP 介面頁籤

- Network > Virtual Routers > RIP > Interfaces（網路 > 虛擬路由器 > RIP > 介面）

使用下列欄位，設定 RIP 介面：

RIP—介面設定	說明
介面	選取執行 RIP 通訊協定的介面。
啟用	選取以啟用這些設定。
廣告	選取此介面可向具有指定公制值的 RIP 端點宣告預設路由。
指標	指定路由器公告的公制值。只有在啟用 **Advertise**（公告）時才會顯示此欄位。
驗證設定檔	選取設定檔。
模式	選取 **Normal**（一般）、**Passive**（被動）或 **Send-only**（僅限傳送）。
BFD	若要為 RIP 介面啟用 BFD（進而取代 RIP 的 BFD 設定，只要在虛擬路由器層級未對 RIP 停用 BFD），請選取下列其中一項： • **default**（預設）（使用預設 BFD 設定的設定檔） • 您已在防火牆上建立的 BFD 設定檔 • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔 選取 **None (Disable BFD)**（無（停用 **BFD**）），可對 RIP 介面停用 BFD。

RIP 計時器頁籤

- Network > Virtual Router > RIP > Timers（網路 > 虛擬路由器 > RIP > 計時器）

下表說明控制 RIP 路由器更新及到期的計時器。

RIP—計時器設定	說明
RIP 計時	
間隔秒數（以秒為單位）	定義計時器的間隔長度（以秒為單位）。此持續時間用於剩餘的 RIP 計時欄位（範圍是 1-60）。
更新間隔	輸入路由更新宣告之間的間隔數目（範圍是 1-3,600)。
到期間隔	輸入上次更新路由時間與其到期時間之間的間隔數目（範圍是 1-3,600)。
刪除間隔	輸入路由到期時間與其刪除時間之間的間隔數目（範圍是 1-3,600)。

© 2019 Palo Alto Networks, Inc.

RIP 驗證設定檔頁籤

- 網路 > 虛擬路由器 > RIP > 驗證設定檔

依預設，防火牆不會驗證芳鄰之間的 RIP 訊息。若要驗證芳鄰之間的 RIP 訊息，請建立驗證設定檔並將其套用於在虛擬路由器上執行 RIP 的介面。下表說明驗證設定檔頁籤的設定。

RIP—驗證設定檔設定	說明
設定檔名稱	輸入用於驗證 RIP 訊息的驗證設定檔名稱。
密碼類型	選取密碼類型（simple 或 MD5）。 • 如果選取簡式，請輸入簡單密碼然後確認。 • 如果您選取 **MD5**，請輸入一或多個密碼項目，包括金鑰 **ID** (0-255)、金鑰及選用的偏好狀態。針對每個項目按一下新增，然後按一下確定。若要指定用來驗證連出訊息的金鑰，請選取偏好選項。

RIP 匯出規則頁籤

- Network > Virtual Router > RIP > Export Rules（網路 > 虛擬路由器 > RIP > 匯出規則）

RIP 匯出規則可讓您控制虛擬路由器傳送至端點的路由。

RIP—匯出規則設定	說明
允許重新分配預設路由	選取此選項可讓防火牆將其預設路由重新散佈至端點。
重新散佈設定檔	按一下 **Add**（新增），然後選取或建立重新分配設定檔，這可讓您根據所需網路行為修改路由重新分配篩選、優先順序及動作的重新分配設定檔。請參考路由重新散佈。

OSPF

- Network > Virtual Router > OSPF（網路 > 虛擬路由器 > OSPF）

設定「先開啟最短的路徑」(OSPF) 通訊協定需要設定下列一般設定（選用 BFD 除外）：

OSPF 設定	說明
啟用	選取以啟用 OSPF 通訊協定。
拒絕預設路由	（建議）如果您不想透過 OSPF 記住任何預設路由，請選取此選項。
路由器 ID	指定在此虛擬路由器中與 OSPF 實例相關聯的路由器 ID。OSPF 通訊協定使用路由器 ID 來單獨識別 OSPF 實例。
BFD	若要對 PA-5200 系列、PA-7000 系列或 VM 系列防火牆上的虛擬路由器全局啟用 OSPF 雙向轉送偵測 (BFD)，請選取下列其中一項： • **default**（預設）（預設 BFD 設定） • 您已在防火牆上建立的 BFD 設定檔

© 2019 Palo Alto Networks, Inc.

OSPF 設定	說明
	• **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔 選取 **None (Disable BFD)**（無（停用 **BFD**）可對虛擬路由器的所有 OSPF 介面停用 BFD；您無法對單一 OSPF 介面啟用 RFD。

此外，您必須在下列頁籤上設定 OSPF 設定：

- **Areas**（區域）：請參閱 OSPF 區域頁籤。
- **Auth Profiles**（驗證設定檔）：請參閱 OSPF 驗證設定檔頁籤。
- **Export Rules**（匯出規則）：請參閱 OSPF 匯出規則頁籤。
- 進階：請參閱 OSPF 進階頁籤。

OSPF 區域頁籤

- Network > Virtual Router > OSPF > Areas（網路 > 虛擬路由器 > OSPF > 區域）

下表說明 OSPF 區域設定：

OSPF—區域設定	說明
區域	
區域 ID	設定可套用 OSPF 參數的區域。 以 x.x.x.x 格式輸入區域的識別碼。它是每個芳鄰要成為相同區域的一部分必須接受的識別碼。
類型	選取下列其中一個選項。 • 一般—沒有限制；此區域可以包含所有類型的路由。 • **Stub**（虛設常式）—此區域無出口。若要到達此區域之外的目的地，您需要通過與其他區域相連的邊界。在選取此選項的情況下，如果您要接受來自其他區域的此類型連結狀態公告 (LSA)，請選取 **Accept Summary**（接受摘要）。同時，指定是否將預設路由 LSA 及其相關聯度量值（範圍是 1-255）包含在虛設常式區域的公告中。 如果停用虛設常式區域「區域邊界路由器」(ABR) 介面上的 **Accept Summary**（接受摘要）選項，OSPF 區域將可做為完全末梢區域 (TSA) 使用，且 ABR 將不會傳播任何摘要 LSA。 • **NSSA** (Not-So-Stubby Area)—您可以直接離開此區域，但只能透過 OSPF 路由以外的路由離開。在選取此選項的情況下，如果您要接受此類型的 LSA，請選取 **Accept Summary**（接受摘要）。選取 **Advertise Default Route**（公告預設路由），指定是否將預設路由 LSA 及其相關聯度量值 (1-255) 包含在虛設常式區域的公告中。同時，選取用來宣告預設 LSA 的路由類型。如果您要啟用或隱藏透過 NSSA 記住之對於其他區域的公告外部路由，請按一下 **External Ranges**（外部範圍）區段中的 **Add**（新增），並輸入範圍。
範圍	按一下新增將區域中的 LSA 目的地位址彙總至子網路。啟用或隱藏符合子網路的公告 LSA，然後按一下 **OK**（確定）。重複上述操作可新增其他範圍。
介面	**Add**（新增）要包含在區域中的介面，並輸入下列資訊： • 介面 — 選擇介面。

© 2019 Palo Alto Networks, Inc.

OSPF—區域設定	說明

	• 啟用 — 使 OSPF 介面設定生效。
	• 被動—如果您不想讓 OSPF 介面傳送或接收 OSPF 封包，請選取此選項。儘管在您選擇此選項的情況下並不會傳送或接收 OSPF 封包，但介面仍包含在 LSA 資料庫中。
	• **Link type**（連結類型）—如果您要透過多點傳送 OSPF 您好訊息來自動探索可透過介面（例如 Ethernet 介面）存取的所有網路芳鄰，請選擇 **Broadcast**（廣播）。選擇 **p2p**（點對點）可自動發現芳鄰。必須手動定義芳鄰時，請選擇 **p2mp**（單點對多點）。手動定義芳鄰僅適用於 p2mp 模式。
	• 公制 — 輸入此介面的 OSPF 公制 (0-65,535)。
	• **Priority**（優先順序）—輸入此介面的 OSPF 優先順序 (0-255)。它是根據 OSPF 通訊協定選為指定路由器 (DR) 或選為備份 DR (BDR) 之路由器的優先順序。當值為零時，不會將路由器選為 DR 或 BDR。
	• 驗證設定檔—選取先前定義的驗證設定檔。
	• **BFD** — 若要為 OSPF 端點介面啟用雙向轉送偵測 (BFD)（進而覆寫 OSPF 的 **BFD** 設定，只要在虛擬路由器層級未對 OSPF 停用 **BFD**），請選取下列其中一項。
	  • **default**（預設）（預設 BFD 設定）
	  • 您已在防火牆上建立的 BFD 設定檔
	  • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔
	  • 選取 **None (Disable BFD)**（無（停用 **BFD**），可對 OSPF 端點停用 BFD。
	• 您好間隔（秒）— OSPF 程序將您好封包傳送給其直接連線之芳鄰的間隔（以秒為單位，範圍是 0-3600；預設為 10）。
	• 無效計數 — 在 OSPF 將網路芳鄰視為關閉之前，OSPF 未從該網路芳鄰收到您好封包的情況下，該網路芳鄰可能發生您好間隔的次數。**Hello Interval**（**Hello** 間隔）乘以 **Dead Counts**（無效計數）等於無效計時器的值（範圍是 3-20；預設為 4）。
	• 重新傳輸間隔（秒）—在 OSPF 重新傳輸連結狀態公告 (LSA) 之前，OSPF 等待從芳鄰接收 LSA 的時間長度（以秒為單位，範圍是 0-3,600；預設值是 10）。
	• 轉送延遲（秒）—從介面傳出 LSA 之前，該 LSA 延遲的時間長度（以秒為單位，範圍是 0-3,600；預設值是 1）。

介面 (續)	• 非失誤性重新啟動 **Hello** 延遲（秒）—適用於已設定主動/被動高可用性時的 OSPF 介面。**Graceful Restart Hello Delay**（非失誤性重新啟動 **Hello** 延遲）是防火牆以 1 秒間隔傳送非失誤性 LSA 封包所在的時間長度。在這段時間內，不會從正在重新啟動的防火牆傳送 Hello 封包。在重新啟動期間，無效計時器（**Hello Interval**（您好間隔）乘以 **Dead Counts**（無效計數））也會倒數計時。如果無效計時器過短，相鄰項會因非失誤性重新啟動期間發生 Hello 延遲而關閉。因此，建議您將無效計時器至少設定為 **Graceful Restart Hello Delay**（非失誤性重新啟動 Hello 延遲）值的四倍。例如，10 秒的 **Hello Interval**（**Hello** 間隔）和 4 次的 **Dead Counts**（無效計數）會產生 40 秒的無效計時器。若將 **Graceful Restart Hello Delay**（非失誤性重新啟動 **Hello** 延遲）設為 10 秒，該 10 秒的 Hello 封包延遲對 40 秒內的無效計時器而言是適當的，如此一來，相鄰項就不會在非失誤性重新啟動期間逾時（範圍是 1-10；預設為 10）。
虛擬連結	設定虛擬連結設定可保持或增強骨幹區域連線。必須為區域邊界路由器定義設定，且必須在骨幹區域 (0.0.0.0) 中定義設定。按一下新增，針對要包含在骨幹區域中的每個虛擬連結輸入下列資訊，然後按一下確定。

© 2019 Palo Alto Networks, Inc.

OSPF—區域設定	說明
	• 名稱—輸入虛擬連結的名稱。 • **Neighbor ID**（芳鄰 ID）—輸入虛擬連結另一側上路由器（網路芳鄰）的路由器 ID。 • **Transit Area**（轉送區域）—輸入實際包含虛擬連結之轉送區域的區域 ID。 • **Enable**（啟用）—選取以啟用虛擬連結。 • 計時—建議您保留預設計時設定。 • 驗證設定檔—選取先前定義的驗證設定檔。

OSPF 驗證設定檔頁籤

- Network > Virtual Router > OSPF > Auth Profiles（網路 > 虛擬路由器 > OSPF > 驗證設定檔）

下表說明 OSPF 驗證設定檔設定：

OSPF—驗證設定檔設定	說明
設定檔名稱	輸入驗證設定檔的名稱。若要驗證 OSPF 訊息，請先定義驗證設定檔，然後將其套用至 **OSPF** 頁籤上的介面。
密碼類型	選取密碼類型（simple 或 MD5）。 • 如果您選取 **Simple**（簡式），請輸入密碼。 • 如果您選取 **MD5**，請輸入一或多個密碼項目，包括金鑰 **ID** (0-255)、金鑰及選用的偏好狀態。針對每個項目按一下新增，然後按一下確定。若要指定用來驗證連出訊息的金鑰，請選取偏好選項。

OSPF 匯出規則頁籤

- 網路 > 虛擬路由器 > OSPF > 匯出規則

下表說明要匯出 OSPF 路由的欄位：

OSPF—匯出規則設定	說明
允許重新分配預設路由	選取以允許透過 OSPF 重新散佈預設路由。
名稱	選取重新散佈設定檔的名稱。此值必須是 IP 子網路或有效的重新散佈設定檔名稱。
新路徑類型	選擇要套用的公制類型。
新標籤	為具有 32 位元值的相符路由指定標籤。
指標	（選用）指定要與匯出的路由相關聯並用於選取路徑的路由公制（範圍是 1-65,535）。

OSPF 進階頁籤

- Network > Virtual Router > OSPF > Advanced（網路 > 虛擬路由器 > OSPF > 進階）

© 2019 Palo Alto Networks, Inc.

下列欄位說明 RFC 1583 相容性、OSPF 計時器和非失誤性重新啟動：

OSPF—進階設定	說明
RFC 1583 相容性	選取以確保 RFC 1583 (OSPF 版本 2) 的相容性。
計時器	• **SPF** 計算延遲（秒）— 可讓您調整接收新拓撲資訊與執行 SPF 計算之間的延遲時間。較低的值可加快 OSPF 重新聚合。防火牆的路由器對等應該以類似方式調整，使聚合時間最佳化。 • **LSA** 間隔（秒）—指定兩個相同的 LSA 實例（相同路由器、相同類型、相容 LSA ID）的傳輸之間最短的時間。這相當於 RFC 2328 中 MinLSInterval。較低的值可用來在拓撲變更時減少重新聚合時間。
非失誤性重新啟動	• 啟用非失誤性重新啟動—預設會啟用，針對此功能啟用的防火牆將指示鄰近的路由器繼續透過防火牆使用路由，同時發生轉換導致防火牆暫時關閉。 • 啟用協助程式模式—預設會啟用，針對此模式此模式啟用的防火牆會在相鄰的設備重新啟動時，繼續轉送到該設備。 • 啟用嚴格 **LSA** 檢查—預設會啟用，此功能會在拓撲發生變更時，導致 OSPF 協助程式模式啟用的防火牆結束協助程式模式。 • 寬限期（秒）—以秒計算的時段，即端點設備應繼續轉送到正在重新建立的此防火牆相鄰項，或正在重新啟動的路由器（範圍是 5-1,800；預設為 120）。 • 最大芳鄰重新啟動時間—防火牆將接受協助程式模式路由器的寬限期上限（以秒為單位）。如果端點設備在其寬限 LSA 中提供更長的寬限期，防火牆將不會進入協助程式模式（範圍是 5-1,800；預設為 140）。

OSPFv3

- Network > Virtual Router > OSPFv3（網路 > 虛擬路由器 > OSPFv3）

設定「先開啟最短的路徑 v3」(OSPFv3) 通訊協定時，需要設定下表中的前三項設定（BFD 為選用）：

OSPFv3 設定	說明
啟用	選取以啟用 OSPF 通訊協定。
拒絕預設路由	如果您不想透過 OSPF 記住任何預設路由，請選取此選項。
路由器 ID	指定在此虛擬路由器中與 OSPF 實例相關聯的路由器 ID。OSPF 通訊協定使用路由器 ID 來單獨識別 OSPF 實例。
BFD	若要對 PA-5200 系列、PA-7000 系列及 VM 系列防火牆上的虛擬路由器全局啟用 OSPFv3 雙向轉送偵測 (BFD)，請選取下列其中一項： • **default**（預設）（預設 BFD 設定） • 您已在防火牆上建立的 BFD 設定檔 • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔 選取 **None (Disable BFD)**（無（停用 **BFD**））可對虛擬路由器的所有 OSPFv3 介面停用 BFD；您無法對單一 OSPFv3 介面啟用 BFD。

© 2019 Palo Alto Networks, Inc.

此外，在下列頁籤上進行 OSPFv3 設定：

- **Areas**（區域）：請參閱 OSPFv3 區域頁籤。
- **Auth Profiles**（驗證設定檔）：請參閱 OSPFv3 驗證設定檔頁籤。
- **Export Rules**（匯出規則）：請參閱 OSPFv3 匯出規則頁籤。
- 進階：請參閱 OSPFv3 進階頁籤。

OSPFv3 區域頁籤

- Network > Virtual Router > OSPFv3 > Areas（網路 > 虛擬路由器 > OSPFv3 > 區域）

使用下列欄位，設定 OSPFv3 區域。

OSPFv3—區域設定	說明
驗證	選取要為此 OSPF 區域指定的驗證設定檔名稱。
類型	選取下列其中一項： • 一般—沒有限制；此區域可以包含所有類型的路由。 • **Stub**（虛設常式）—此區域無出口。若要到達此區域之外的目的地，您需要通過與其他區域相連的邊界。在選取此選項的情況下，如果您要接受來自其他區域的此類型連結狀態公告 (LSA)，請選取 **Accept Summary**（接受摘要）。同時，指定是否將預設路由 LSA 及其相關聯公制值 (1-255) 包含在殘斷區的宣告中。 如果停用虛設常式區域「區域邊界路由器」(ABR) 介面上的 **Accept Summary**（接受摘要）選項，OSPF 區域將可做為完全末梢區域 (TSA) 使用，且 ABR 將不會傳播任何摘要 LSA。 • **NSSA** (Not-So-Stubby Area)—您可以直接離開此區域，但只能透過 OSPF 路由以外的路由離開。在選取此選項的情況下，如果您要接受此類型的 LSA，請選取 **Accept Summary**（接受摘要）。指定是否將預設路由 LSA 及其相關聯公制值 (1-255) 包含在殘斷區的宣告中。同時，選取用來宣告預設 LSA 的路由類型。如果您要啟用或抑制透過 NSSA 記住之對於其他區域的宣告外部路由，請按一下 **External Ranges**（外部範圍）部分中的 **Add**（新增），並輸入範圍。
範圍	按一下 **Add**（新增）可按子網路彙總區域中的 LSA 目的地 IPv6 位址。啟用或隱藏符合子網路的公告 LSA，然後按一下 **OK**（確定）。重複上述操作可新增其他範圍。
介面	按一下 **Add**（新增），針對要包含在區域中的每個介面輸入下列資訊，然後按一下 **OK**（確定）。 • 介面 — 選擇介面。 • 啟用 — 使 OSPF 介面設定生效。 • 實例 **ID**—輸入 OSPFv3 實例 ID 編號。 • 被動—如果您不想讓 OSPF 介面傳送或接收 OSPF 封包，請選取此選項。儘管在您選擇此選項的情況下並不會傳送或接收 OSPF 封包，但介面仍包含在 LSA 資料庫中。 • **Link type**（連結類型）—如果您要透過多點傳送 OSPF 您好訊息來自動探索可透過介面（例如 Ethernet 介面）存取的所有網路芳鄰，請選擇 **Broadcast**（廣播）。選擇 **p2p**（點對點）可自

© 2019 Palo Alto Networks, Inc.

OSPFv3—區域設定	說明

	動發現芳鄰。必須手動定義芳鄰時，請選擇 **p2mp**（單點對多點）。手動定義芳鄰僅適用於 p2mp 模式。
	• 公制 — 輸入此介面的 OSPF 公制 (0-65,535)。
	• **Priority**（優先順序）—輸入此介面的 OSPF 優先順序 (0-255)。它是根據 OSPF 通訊協定選為指定路由器 (DR) 或選為備份 DR (BDR) 之路由器的優先順序。當值為零時，不會將路由器選為 DR 或 BDR。
	• 驗證設定檔—選取先前定義的驗證設定檔。
	• **BFD** — 若要為 OSPFv3 端點介面啟用雙向轉送偵測 (BFD)（進而覆寫 OSPFv3 的 **BFD** 設定，只要在虛擬路由器層級未對 OSPFv3 停用 **BFD**），請選取下列其中一項。
	  • **default**（預設）（預設 BFD 設定）
	  • 您已在防火牆上建立的 BFD 設定檔
	  • **New BFD Profile**（新 **BFD** 設定檔），用於建立新 BFD 設定檔
	  選取 **None (Disable BFD)**（無（停用 **BFD**），可對 OSPFv3 端點停用 BFD。
	• 您好間隔（秒）— OSPF 程序將您好封包傳送給其直接連線之芳鄰的間隔（以秒為單位，範圍是 0-3600；預設為 10）。
	• 無效計數 — 在 OSPF 將網路芳鄰視為關閉之前，OSPF 未從該網路芳鄰收到您好封包的情況下，該網路芳鄰可能發生您好間隔的次數。**Hello Interval**（**Hello** 間隔）乘以 **Dead Counts**（無效計數）等於無效計時器的值（範圍是 3-20；預設為 4）。
	• 重新傳輸間隔（秒）—在 OSPF 重新傳輸連結狀態公告 (LSA) 之前，OSPF 等待從芳鄰接收 LSA 的時間長度（以秒為單位，範圍是 0-3,600；預設值是 10）。
	• 轉送延遲（秒）—防火牆從介面傳出 LSA 之前，該 LSA 延遲的時間長度（以秒為單位，範圍是 0-3,600；預設值是 1）。

介面（續）	• 非失誤性重新啟動 **Hello** 延遲（秒）—適用於已設定主動/被動高可用性時的 OSPF 介面。**Graceful Restart Hello Delay**（非失誤性重新啟動 **Hello** 延遲）是防火牆以 1 秒間隔傳送非失誤性 LSA 封包所在的時間長度。在這段時間內，不會從正在重新啟動的防火牆傳送 Hello 封包。在重新啟動期間，無效計時器（**Hello Interval**（您好間隔）乘以 **Dead Counts**（無效計數））也會倒數計時。如果無效計時器過短，相鄰項會因非失誤性重新啟動期間發生 Hello 延遲而關閉。因此，建議您將無效計時器至少設定為 **Graceful Restart Hello Delay**（非失誤性重新啟動 Hello 延遲）值的四倍。例如，10 秒的 **Hello Interval**（**Hello** 間隔）和 4 次的 **Dead Counts**（無效計數）會產生 40 秒的無效計時器。若將 **Graceful Restart Hello Delay**（非失誤性重新啟動 **Hello** 延遲）設為 10 秒，該 10 秒的 Hello 封包延遲對 40 秒內的無效計時器而言是適當的，如此一來，相鄰項就不會在非失誤性重新啟動期間逾時（範圍是 1-10；預設為 10）。 • **Neighbors**（芳鄰）—針對 p2pmp 介面，輸入可透過此介面到達之所有芳鄰的芳鄰 IP 位址。
虛擬連結	設定虛擬連結設定可保持或增強骨幹區域連線。必須為區域邊界路由器定義設定，且必須在骨幹區域 (0.0.0.0) 中定義設定。按一下新

© 2019 Palo Alto Networks, Inc.

OSPFv3—區域設定	說明
	增，針對要包含在骨幹區域中的每個虛擬連結輸入下列資訊，然後按一下確定。 • 名稱—輸入虛擬連結的名稱。 • 實例 **ID**—輸入 OSPFv3 實例 ID 編號。 • **Neighbor ID**（芳鄰 ID）—輸入虛擬連結另一側上路由器（網路芳鄰）的路由器 ID。 • **Transit Area**（轉送區域）—輸入實際包含虛擬連結之轉送區域的區域 ID。 • **Enable**（啟用）—選取以啟用虛擬連結。 • 計時—建議您保留預設計時設定。 • 驗證設定檔—選取先前定義的驗證設定檔。

OSPFv3 驗證設定檔頁籤

- 網路 > 虛擬路由器 > OSPFv3 > 驗證設定檔

使用下列欄位，設定 OSPFv3 驗證。

OSPFv3—驗證設定檔設定	說明
設定檔名稱	輸入驗證設定檔的名稱。若要驗證 OSPF 訊息，請先定義驗證設定檔，然後將其套用至 **OSPF** 頁籤上的介面。
SPI	針對遠端防火牆到端點之間的封包穿透機制，指定安全性參數索引 (SPI)。
通訊協定	指定下列任一通訊協定： • **ESP**—封裝安全有效負載通訊協定。 • **AH**—驗證標頭通訊協定
密碼演算法	指定下列其中一項 • 無 — 不使用加密演算法。 • **SHA1**（預設值）—安全性雜湊演算法 1。 • **SHA256** — 安全雜湊演算法　2。一組包含 256 位元摘要的四個雜湊函數集。 • **SHA384** — 安全雜湊演算法　2。一組包含 384 位元摘要的四個雜湊函數集。 • **SHA512** — 安全雜湊演算法　2。一組包含 512 位元摘要的四個雜湊函數集。 • **MD5** — MD5 訊息摘要演算法。
金鑰/確認金鑰	輸入和確認驗證金鑰。
加密（僅限 ESP 通訊協定）	指定下列其中一項： • **3des**（預設值）—使用三個 56 位元密碼金鑰套用三重資料加密演算法 (3DES)。

© 2019 Palo Alto Networks, Inc.

OSPFv3—驗證設定檔設定	說明
	• **aes-128-cbc**—使用 128 位元密碼金鑰套用進階加密標準 (AES)。 • **aes-192-cbc**—使用 192 位元密碼金鑰套用進階加密標準 (AES)。 • **aes-256-cbc**—使用 256 位元密碼金鑰套用進階加密標準 (AES)。 • 空值 — 未使用加密。
金鑰/確認金鑰	輸入和確認加密金鑰。

OSPFv3 匯出規則頁籤

- 網路 > 虛擬路由器 > OSPFv3 > 匯出規則

使用下列欄位來匯出 OSPFv3 路由。

OSPFv3—匯出規則設定	說明
允許重新分配預設路由	選取以允許透過 OSPF 重新散佈預設路由。
名稱	選取重新散佈設定檔的名稱。此值必須是 IP 子網路或有效的重新散佈設定檔名稱。
新路徑類型	選擇要套用的公制類型。
新標籤	為具有 32 位元值的相符路由指定標籤。
指標	（選用）指定要與匯出的路由相關聯並用於選取路徑的路由公制（範圍是 1-65,535）。

OSPFv3 進階頁籤

- 網路 > 虛擬路由器 > OSPFv3 > 進階

使用下列欄位來停用 SPF 計算的轉送路由，設定 OSPFv3 計時器，以及設定 OSPFv3 的非失誤性重新啟動。

OSPFv3—進階設定	說明
停用 SPF 計算的轉送路由	若要在此防火牆傳送的路由器 LSA 中設定 R-位元，以指出該防火牆未啟動，請選取此選項。處於此狀態時，防火牆將參與 OSPFv3，但其他路由器不會傳送傳輸流量。在此狀態下，仍會將本機流量轉送至防火牆。這種做法適用於使用雙主控網路所執行的維護，因為流量可在防火牆之間重新路由且仍可送達。
計時器	• **SPF 計算延遲（秒）**—這是一個延遲計時器，可讓您調整接收新拓撲資訊與執行 SPF 計算之間的延遲時間。較低的值可加快

© 2019 Palo Alto Networks, Inc.

OSPFv3—進階設定	說明
	OSPF 重新聚合。防火牆的路由器對等應該以類似方式調整，使聚合時間最佳化。 • **LSA** 間隔（秒）—此選項可指定兩個相同的 LSA 實例（相同路由器、相同類型、相容 LSA ID）的傳輸之間最短的時間。這相當於 RFC 2328 中 MinLSInterval。較低的值可用來在拓撲變更時減少重新聚合時間。
非失誤性重新啟動	• 啟用非失誤性重新啟動—預設會啟用，針對此功能啟用的防火牆將指示鄰近的路由器繼續透過防火牆使用路由，同時發生轉換導致防火牆暫時關閉。 • 啟用協助程式模式—預設會啟用，針對此模式此模式啟用的防火牆會在相鄰的設備重新啟動時，繼續轉送到該設備。 • 啟用嚴格 **LSA** 檢查—預設會啟用，此功能會在拓撲發生變更時，導致 OSPF 協助程式模式啟用的防火牆結束協助程式模式。 • 寬限期（秒）—以秒計算的時段，即端點設備繼續轉送到正在重新建立的此防火牆相鄰項，或正在重新啟動的路由器（範圍是 5-1,800；預設為 120）。 • 最大芳鄰重新啟動時間 — 防火牆將接受協助程式模式路由器的寬限期上限（秒）。如果端點設備在其寬限 LSA 中提供更長的寬限期，防火牆將不會進入協助程式模式（範圍是 5-800；預設為 140）。

BGP

- Network > Virtual Router > BGP（網路 > 虛擬路由器 > BGP）

要設定邊界閘道通訊協定 (BGP)，您必須設定基本 BGP 設定以啟用 BGP，並依照下表中的說明設定路由器 ID 和 AS 號碼。此外，您還必須將 BGP 端點設定為 BGP 端點群組的一部分。

請依照網路的需求，在下列頁籤上設定其餘 BGP 設定：

- **General**（一般）：請參閱 BGP 一般頁籤。
- 進階：請參閱 BGP 進階頁籤。
- **Peer Group**（遠端群組）：請參閱 BGP 端點群組頁籤。
- **Import**（匯入）：請參閱 BGP 匯入和匯出頁籤。
- **Export**（匯出）：請參閱 BGP 匯入和匯出頁籤。
- **Conditional Adv**（條件式廣告）：請參閱 BGP 條件式公告頁籤。
- **Aggregate**（彙總）：請參閱 BGP 彙總頁籤。
- **Redist Rules**（重新分配規則）：請參閱 BGP 重新散佈規則頁籤。

基本 *BGP* 設定

若要在虛擬路由器上使用 BGP，您必須啟用 BGP，並設定路由器 ID 和 AS 號碼；啟用 BFD 是選用的。

BGP 設定	設定位置	說明
啟用	**BGP**	選取以啟用 BGP。
路由器 ID		輸入要指定給虛擬路由器的 IP 位址。

© 2019 Palo Alto Networks, Inc.

BGP 設定	設定位置	說明
AS 號碼		根據路由器 ID，輸入虛擬路由器所屬的 AS 號碼（範圍是 1-4,294,967,295）。
BFD		若要對 PA-5200 系列、PA-7000 系列或 VM 系列防火牆上的虛擬路由器全局啟用 BGP 雙向轉送偵測 (BFD)，請選取下列其中一項： • **default**（預設）（預設 BFD 設定） • 防火牆上的現有 BFD 設定檔 • 建立 **New BFD Profile**（新 **BFD** 設定檔） 選取 **None (Disable BFD)**（無（停用 **BFD**））可對虛擬路由器的所有 BGP 介面停用 BFD；您無法對單一 BGP 介面啟用 BFD。 如果您全域啟用或停用 *BFD*，所有執行 *BGP* 的介面都會中斷，並以 *BFD* 功能重新啟用，而這可能會干擾到 *BGP* 流量。因此，請在重新整合不會影響到生產流量的離峰時段，在 *BGP* 介面上啟用 *BFD*。

BGP 一般頁籤

- Network > Virtual Router > BGP > General（網路 > 虛擬路由器 > BGP > 一般）

使用下列欄位可設定一般 BGP 設定。

BGP 一般設置	設定位置	說明
拒絕預設路由	**BGP** > **General**（一般）	選取此選項，可忽略 BGP 端點所公告的任何預設路由。
安裝路由		選取此選項，可安裝全域路由表中的 BGP 路由。
彙總 MED		即使當路由具有不同的多出口鑑別器 (MED) 值時，選取此欄位也可以啟用路由彙總。
預設本地偏好設定		指定一個值，讓防火牆用來決定不同路徑的偏好設定。
As Format		選取 2-byte（預設）或 4-byte 格式。您可以進行此設定，以達到交互操作的目的。
始終比較 MED		在不同自發系統中啟用芳鄰路徑的 MED 比較。
具決定性的 MED 比較		啟用 MED 比較，以在 iBGP 端點（相同自發系統中的 BGP 端點）所公告的路由間進行選擇。
驗證設定檔		**Add**（新增）新的驗證設定檔，然後進行下列設定： • 設定檔名稱—輸入用來識別設定檔的名稱。 • 密碼/確認密碼—輸入 BGP 對等體通訊的複雜密碼並確認。 請刪除 (⊖) 您不再需要的設定檔。

© 2019 Palo Alto Networks, Inc.

BGP 進階頁籤

- 網路 > 虛擬路由器 > BGP > 進階

進階 BGP 設定包含多種功能。您可以對多個 BGP 自發系統執行 ECMP。您可以要求 eBGP 端點將其本身的 AS 列為 AS_PATH 屬性中的第一個 AS（以防止詐騙的更新封包）。您可以設定 BGP 非失誤性重新啟動；藉由此機制，BGP 端點可指出它們是否可在 BGP 重新啟動期間保存轉送狀態，以盡可能降低路由波動（上下移動）的可能性。您可以設定路由反射程式和 AS 聯盟；這兩種方法可避免在 AS 中出現全網狀的 BGP 對等。您可以設定路由抑制，以防止在 BGP 網路不穩定和路由波動時發生非必要的路由器聚合。

BGP 進階設定	設定位置	說明
ECMP 多 AS 支援	**BGP** > **Advanced**（進階）	如果您為虛擬路由器啟用了 ECMP，並且想要對多個 BGP 自發系統執行 ECMP，請選取此選項。
針對 EBGP 執行首次 AS		使防火牆丟棄未在 AS_PATH 屬性中將 eBGP 端點本身的 AS 號碼列為第一個 AS 號碼的 eBGP 端點所傳入的更新封包。這會使 BGP 無法進一步處理從非相鄰 AS 送達的詐騙或錯誤更新封包。預設為啟用。
非失誤性重新啟動		啟動 [優雅重新啟動] 選項。 • **Stale Route Time**（過時路由時間）—指定路由可以處於過時狀態的時間長度（以秒為單位，範圍是 1-3,600 秒，預設為 120 秒）。 • **Local Restart Time**（本機重新啟動時間）—以秒為單位指定防火牆重新啟動的時間長度。會向對等宣告此值（範圍是 1-3,600 秒，預設為 120 秒）。 • **Max Peer Restart Time**（最大端點重新啟動時間）—以秒為單位指定防火牆可以接受之對等設備的寬限期重新啟動時間的最大時間長度（範圍 1-3,600 秒，預設為 120 秒）。
反射程式叢集 ID		指定代表反射程式叢集的 IPv4 識別碼。AS 中的路由反射程式（路由器）會執行將其學習的路由重新公告給其端點的角色（而不是要求全網狀連線以及所有端點互相傳送路由）。路由反射程式可簡化設定。
聯盟成員 AS		指定僅可在 BGP 聯絡看到的自發系統數字識別代碼（也稱之為次自發系統編號）。使用 BGP 聯盟，將自發系統分成子自發系統，並減少全網狀對等。
抑制設定檔	**BGP** > **Advanced (cont)**（進階（續））	路由抑制是一個可決定是否要因為路由有所波動而抑制其公告的方法。路由抑制可減少因路由波動而強制路由器重新聚合的次數。設定包括： • 設定檔名稱—輸入用來識別設定檔的名稱。 • **Enable**（啟用）—啟動設定檔。 • 截止—指定路由撤銷臨界值，如果超過此值，將會隱藏路由公告（範圍是 0.0-1,000.0；預設值是 1.25）。 • **Reuse**（重複使用）—指定路由撤銷閾值，如果低於此值，將會再次使用隱藏路由（範圍是 0.0-1,000.0，預設為 5）。 • **Max**（最大）。**Hold Time**（保留時間）—以秒為單位指定可以隱藏路由的最大時間長度，不管它有多不穩定（範圍是 0-3,600 秒，預設為 900 秒）。 • **Decay Half Life Reachable**（可到達的半衰期）—以秒為單位指定一段時間長度，在經過該段時間後，如果防火牆認定路由是可到達的，路由的穩定性度量即減半（範圍是 0-3,600，預設值為 300）。

© 2019 Palo Alto Networks, Inc.

BGP 進階設定	設定位置	說明
		• **Decay Half Life Unreachable**（無法到達的半衰期）—以秒為單位指定一段時間長度，在經過該段時間後，如果防火牆認定路由是無法到達的，路由的穩定性度量即減半（範圍是 0-3,600，預設值為 300）。 請刪除 (⊖) 您不再需要的設定檔。

BGP 端點群組頁籤

- Network > Virtual Router > BGP > Peer Group（網路 > 虛擬路由器 > BGP > 端點群組）

BGP 端點群組是共用設定的 BGP 端點集合；這些設定包括端點群組的類型（例如 EBGP），或是可從虛擬路由器在更新封包中傳送的 AS_PATH 清單中移除私人 AS 號碼的設定。BGP 端點群組可讓您無須以相同的設定來設定多個端點。您必須先設定至少一個 BGP 端點群組，才能設定屬於該群組的 BGP 端點。

BGP 端點群組設定	設定位置	說明
名稱	**BGP** > **Peer Group**（遠端群組）	輸入用來識別端點群組的名稱。
啟用		選取此選項可啟動端點群組。
已彙總聯盟 AS 路徑		選取此選項，可包含已設定的彙總聯盟 AS 的路徑。
使用已存資訊進行軟重設		選取此選項，可在更新端點設定之後執行防火牆的軟重設。

類型		指定端點或群組的類型並進行相關聯的設定（請參閱以下表格中的 **Import Next Hop**（匯入下一個躍點）與 **Export Next Hop**（匯出下一個躍點）描述）。
		• **IBGP** — 指定下列設定：
		  • 匯出下一個躍點
		• **EBGP Confed** — 指定下列設定：
		  • 匯出下一個躍點
		• **IBGP Confed** — 指定下列設定：
		  • 匯出下一個躍點
		• **EBGP**—指定下列設定：
		  • 匯入下一個躍點
		  • 匯出下一個躍點
		  • **Remove Private AS**（移除私人 **AS**）（如果您要強制 BGP 從 AS_PATH 屬性中移除私人 AS 號碼，請選取此選項）。

匯入下一個躍點		為下一個躍點匯入選取一個選項： • **Original**（原始）—使用原始路由公告中提供的下一個躍點位址。 • **Use Peer**（使用端點）—使用端點的 IP 位址作為下一個躍點位址。

© 2019 Palo Alto Networks, Inc.

BGP 端點群組設定	設定位置	說明
匯出下一個躍點		為下一個躍點匯出選取一個選項： • **Resolve**（解析）—使用轉送資訊庫 (FIB) 解析下一個躍點位址。 • **Original**（原始）—使用原始路由公告中提供的下一個躍點位址。 • **Use Self**（使用自我）—以虛擬路由器的 IP 位址取代下一個躍點位址，以確保該位址將會在轉送路徑中。
移除私人 AS		選取此選項，可從 AS_PATH 清單中移除私人自發系統。
名稱	**BGP** > **Peer Group**（端點群組）> **Peer**（端點）	**New**（新增）BGP 端點，並輸入加以識別的名稱。
啟用		選取以啟動端點。
遠端 AS		指定端點的自發系統 (AS)。
啟用 MP-BGP 延伸	**BGP** > **Peer Group**（端點群組）> **Peer**（端點）> **Addressing**（定址）	讓防火牆能夠根據 RFC 4760，針對 IPv4 和 IPv6 以及後續位址系列識別碼選項支援多通訊協定 BGP 位址系列識別碼。
位址家族類型		選取使用此端點的 BGP 工作階段所將支援的 **IPv4** 或 **IPv6** 位址系列。
後續位址系列		選取使用此端點的 BGP 工作階段所將具備的 **Unicast**（單點傳送）或 **Multicast**（多點傳送）後續位址系列通訊協定。
本機位址—介面		選取防火牆介面。
本機位址—IP		選取本機 IP 位址。
對等位址—類型及位址		選取識別端點的位址及類型 • **IP**—選取 IP 然後選取使用 IP 位址的位址物件（或建立使用 IP 位址的新位址物件）。 • **FQDN**—選取 FQDN 然後選取使用 FQDN 的位址物件（或建立使用 FQDN 的新位址物件）。
驗證設定檔	**BGP** > **Peer Group**（端點群組）> **Peer**（端點）> **Connection Options**（連線選項）	選取設定檔，或從下拉式清單中選取 **New Auth Profile**（新增驗證設定檔）。輸入設定檔 **Name**（名稱）、**Secret**（密碼）並 **Confirm Secret**（確認密碼）。
保持運作的間隔		指定一段在超過後即根據保留時間設定對來自端點的路由進行隱藏的間隔（範圍是 0-1,200 秒，預設值為 30 秒）。
多重躍點		在 IP 標頭中設定存留時間 (TTL) 值（範圍是 0 至 255，預設值為 0）。對 eBGP 而言，預設值 0 表示 1。對 iBGP 而言，預設值 0 表示 255。
開啟延遲時間		指定開啟端點 TCP 連線與傳送第一個 BGP 開啟訊息之間的延遲時間（範圍是 0-240 秒，預設值為 0 秒）。
保持時間		指定關閉端點連線之前，來自端點的連續 KEEPALIVE 或 UPDATE 訊息之間可能經過的時間（範圍是 3-3,600 秒，預設值為 90 秒）。

© 2019 Palo Alto Networks, Inc.

BGP 端點群組設定	設定位置	說明
閒置保留時間		指定重新嘗試連線至端點之前在閒置狀態下的等待時間（範圍是 1-3,600 秒，預設值為 15 秒）。
傳入連線—遠端連接埠		指定傳入埠號，並 **Allow**（允許）進入此連接埠的流量。
傳出連線—本機連接埠		指定傳出埠號，並 **Allow**（允許）來自此連接埠的流量
反射程式用戶端	**BGP** > **Peer Group**（端點群組）> **Peer**（端點）> **Advanced**（進階）	選取反射程式用戶端的類型（**Non-Client**（非用戶端）、**Client**（用戶端）或 **Meshed Client**（網狀用戶端））。會與所有內部與外部 BGP 端點共享從反射程式用戶端收到的路由。
遠端類型		指定雙邊端點，或是不指定。
最大首碼		指定支援的 IP 首碼的最大數目（1-100,000 或無限制）。
啟用寄件者端迴圈偵測		可使防火牆先在其 FIB 中檢查路由的 AS_PATH 屬性，再於更新中傳送該路由，以確保端點 AS 號碼不在 AS_PATH 清單中。如果在清單中，防火牆會加以移除，以防止發生迴圈。接收者通常會執行迴圈偵測，但此最佳化功能會讓寄件者執行迴圈偵測。
BFD		若要為 BGP 端點啟用雙向轉送偵測 (BFD)（進而取代 BGP 的 **BFD** 設定；前提是在虛擬路由器層級上未對 BGP 停用 **BFD**），請選取預設設定檔（預設 BFD 設定），即現有的 BFD 設定檔 **Inherit-vr-global-setting**（用以繼承 BGP BFD 設定檔），或選取 **New BFD Profile**（新增 **BFD** 設定檔）（用以建立新的 BFD 設定檔）。選取 **Disable BFD**（停用 **BFD**）可停用 BGP 端點的 BFD。 如果您全域啟用或停用 *BFD*，所有執行 *BGP* 的介面都會中斷，並以 *BFD* 功能重新啟用。這可能會中斷所有 *BGP* 流量。您在介面上停用 *BFD* 後，防火牆會停止與端點的 *BGP* 連接，以便在介面上設定 *BFD*。端點裝置會偵測到 *BGP* 連接中斷，可能導致重新整合，影響生產流量。因此，在重新整合不會影響生產流量的非高峰時段啟用 *BGP* 介面上的 *BFD*。

BGP 匯入和匯出頁籤

- 網路 > 虛擬路由器 > BGP > 匯入
- 網路 > 虛擬路由器 > BGP > 匯出

Add（新增）新的匯入或匯出規則，用以匯入或匯出 BGP 路由。

BGP 匯入和匯出設定	設定位置	說明
規則	**BGP** > **Import or Export**（匯	指定用來識別規則的名稱。

© 2019 Palo Alto Networks, Inc.

BGP 匯入和匯出設定	設定位置	說明
啟用	入或匯出）> **General**（一般）	選取此選項可啟動規則。
使用者		選取將使用此規則的端點群組。
AS-Path 規則運算式	**BGP** > **Import or Export**（匯入或匯出）> **Match**（比對）	指定用來篩選 AS 路徑的規則運算式。
社群規則運算式		指定用來篩選社群字串的規則運算式。
延伸社群規則運算式		指定用來篩選延伸社群字串的規則運算式。
MED		為 0-4,294,967,295 範圍內的路由篩選指定多出口鑑別器值。
路由表		針對 **Import Rule**（匯入規則），指定相符的路由將匯入哪個路由表中：**unicast**（單點傳送）、**multicast**（多點傳送）或 **both**（兩者）。 針對 **Export Rule**（匯出規則），指定將從哪個路由表中匯出相符的路由：**unicast**（單點傳送）、**multicast**（多點傳送）或 **both**（兩者）。
位址首碼		指定用來篩選路由的 IP 位址或前置詞。
下一個躍點		指定用來篩選路由的下一個躍點路由器或子網路
從端點		指定用來篩選路由的端點路由器
動作	**BGP** > **Import or Export**（匯入或匯出）> **Action**（動作）	指定在符合相符條件時所要執行的動作（**Allow**（允許）或 **Deny**（拒絕））。
抑制		指定抑制參數（僅適用於動作為 **Allow**（允許）時）。
本地偏好設定		指定本機偏好設定度量（僅適用於動作為 **Allow**（允許）時）。
MED		指定 MED 值（僅適用於動作為 **Allow**（允許）時）(0- 65,535)。
加權		指定加權值（僅適用於動作為 **Allow**（允許）時）(0- 65,535)。
下一個躍點		指定下一個躍點路由器（僅適用於動作為 **Allow**（允許）時）。
原點		指定原始路由的路徑類型：IGP、EGP 或 incomplete（僅適用於動作為**Allow**（允許）時）。
AS 路徑限制		指定 AS 路徑限制（僅適用於動作為 **Allow**（允許）時）。
AS 路徑		指定 AS 路徑：無、移除、在前面加上、移除並在前面加上（僅適用於動作為允許時）。
社群		指定社群選項：無、全部移除、移除 **Regex**、附加或覆寫（僅適用於動作為允許時）。

© 2019 Palo Alto Networks, Inc.

BGP 匯入和匯出設定	設定位置	說明
延伸社群		指定社群選項：無、全部移除、移除 **Regex**、附加或覆寫（僅適用於動作為允許時）。
		請 **Delete**（刪除）⊖ 您不再需要的規則，或視情況 **Clone**（複製）規則。您也可以選取規則並將其 **Move Up**（上移）或 **Move Down**（下移），以變更其順序。

BGP 條件式公告頁籤

- Network > Virtual Router > BGP > Conditional Adv（網路 > 虛擬路由器 > BGP > 條件式廣告）

BGP 條件式公告可讓您控制本機 BGP 路由表 (LocRIB) 中沒有偏好的路由時（表示對等或連線能力失敗）所要公告的路由。如果您要嘗試強制路由至某一個 AS，例如，如果您有經由多個 ISP 的網際網路連結，而您要將流量路由至一個供應商，且在這個偏好的供應商連線中斷時，才路由至另一個供應商，即可使用此公告。

針對條件式公告，您可以設定 [不存在] 篩選器以指定偏好的路由（**Address Prefix**（位址前置詞）），以及可識別偏好路由的任何其他屬性（例如 AS 路徑規則運算式）。如果在本機 BGP 路由表中找不到與 [不存在] 篩選器相符的路由，防火牆才會允許公告其公告篩選器中指定的替代路由（其他非偏好供應商的路由）。

若要設定條件式公告，請選取 **Conditional Adv**（條件式公告）頁籤、**Add**（新增）條件式公告，然後設定下表中說明的值。

BGP 條件式公告設定	設定位置	說明
原則	**BGP** > **Conditional Adv**（條件式公告）	指定此條件式公告政策規則的名稱。
啟用		選取此選項，可啟用此條件式公告政策規則。
使用者		**Add**（新增）將使用此條件式公告政策規則的端點群組。
[不存在] 篩選器	**BGP** > **Conditional Adv**（條件式公告）> **Non Exist Filters**（[不存在] 篩選器）	使用此子頁籤可指定偏好路由的前置詞。如果要宣告的路由出現在本機 BGP 路由表中，這將指定該路由。（如果將公告的前置詞符合 [不存在] 篩選器，則將隱藏公告。） **Add**（新增）[不存在] 篩選器，並指定用來識別此篩選器的名稱。
啟用		選取此選項，可啟動 [不存在] 篩選器。
AS 路徑規則運算式		指定用來篩選 AS 路徑的規則運算式。
社群規則運算式		指定用來篩選社群字串的規則運算式。
延伸社群規則運算式		指定用來篩選延伸社群字串的規則運算式。
MED		指定路由篩選的 MED 值（範圍是 0-4,294,967,295）。

© 2019 Palo Alto Networks, Inc.

BGP 條件式公告設定	設定位置	說明
路由表		指定防火牆將搜尋哪個路由表（**unicast**（單點傳送）、**multicast**（多點傳送）或 **both**（兩者））以確認是否有相符的路由存在。如果該路由表中沒有相符的路由存在，防火牆才會允許公告替代路由。
位址首碼		為偏好的路由 **Add**（新增）確切的網路層可達性資訊 (NLRI) 前置詞。
下一個躍點		指定用來篩選路由的下一個躍點路由器或子網路。
從端點		指定用來篩選路由的端點路由器。
宣告篩選器	**BGP** > **AdvConditional Adv**（條件式公告）> **Advertise Filters**（公告篩選器）	使用此頁籤，可為本機 RIB 路由表中的路由指定前置詞，以在本機路由表沒有 [不存在] 篩選器中的路由時發出公告。 如果要公告的前置詞不符合 [不存在] 篩選器，則將進行公告。 **Add**（新增）公告篩選器，並指定用來識別此篩選器的名稱。
啟用		選取此選項可啟動篩選器。
AS 路徑規則運算式		指定用來篩選 AS 路徑的規則運算式。
社群規則運算式		指定用來篩選社群字串的規則運算式。
延伸社群規則運算式		指定用來篩選延伸社群字串的規則運算式。
MED		指定路由篩選的 MED 值（範圍是 0-4,294,967,295）。
路由表		指定防火牆在相符的路由將進行有條件地宣告時所使用的路由表：**unicast**（單點傳送）、**multicast**（多點傳送） 或 **both**（兩者）。
位址首碼		針對偏好的路由不存在時所要公告的路由，**Add**（新增）確切的網路層可達性資訊 (NLRI) 前置詞。
下一個躍點		指定用來篩選路由的下一個躍點路由器或子網路。
從端點		指定用來篩選路由的端點路由器。

BGP 彙總頁籤

- Network > Virtual Router > BGP > Aggregate（網路 > 虛擬路由器 > BGP > 彙總）

路由彙總是一個動作，用以將特定路由（前置詞長度較長的路由）結合為單一路由（前置詞長度較短），以減少防火牆所須傳送的路由公告和路由表中的路由。

© 2019 Palo Alto Networks, Inc.

BGP 彙總設定	設定位置	說明
名稱	**BGP** > **Aggregate**（彙總）	輸入彙總規則的名稱。
前置詞		輸入將用來彙總較長前置詞的摘要前置詞（IP 位址/前置詞長度）。
啟用		選取此選項，可啟用路由的這項彙總。
Summary		選取此選項可摘要路由。
AS 設定		選取此選項，可使防火牆針對此彙總規則將 AS 號碼集（AS 集）包含在彙總路由的 AS 路徑中。AS 集是彙總的個別路由中未排序的原點 AS 號碼清單。
名稱	**BGP** > **Aggregate**（彙總）> **Suppress Filters**（隱藏篩選器）	定義會造成隱藏符合路由的屬性。**Add**（新增）並輸入隱藏篩選器的名稱。
啟用		選取此選項，可啟用隱藏篩選器。
AS 路徑規則運算式		為 AS_PATH 指定用來篩選將彙總哪些路由的規則運算式，例如，^5000 表示從 AS 5000 學習的路由。
社群規則運算式		為社群指定用來篩選將彙總哪些路由的規則運算式，例如，500:.* 會比對出含有 500:x 的社群。
延伸社群規則運算式		為延伸社群指定用來篩選將彙總哪些路由的規則運算式。
MED		指定可篩選將彙總哪些路由的 MED。
路由表		指定要將哪個路由表用於應隱藏（而非公告）的彙總路由：**unicast**（單點傳送）、**multicast**（多點傳送）或 **both**（兩者）。
位址首碼		輸入您要隱藏而不公告的 IP 位址。
下一個躍點		輸入您要隱藏之 BGP 前置詞的下一個躍點位址。
從端點		輸入從中接收（您要隱藏的）BGP 前置詞之端點的 IP 位址。
名稱	**BGP** > **Aggregate**（彙總）> **Advertise Filters**（公告篩選器）	為致使防火牆對端點公告符合篩選器的任何路由的公告篩選器定義屬性。按一下 **Add**（新增），並輸入公告篩選器的名稱。
啟用		選取此選項，可啟用此公告篩選器。
AS 路徑規則運算式		為 AS_PATH 指定用來篩選將公告哪些路由的規則運算式。
社群規則運算式		為社群指定用來篩選將公告哪些路由的規則運算式。
延伸社群規則運算式		為延伸社群指定用來篩選將公告哪些路由的規則運算式。
MED		指定用來篩選將公告哪些路由的 MED 值。

© 2019 Palo Alto Networks, Inc.

BGP 彙總設定	設定位置	說明
路由表		指定要將哪個路由表用於彙總路由的宣告篩選器：**unicast**（單點傳送）、**multicast**（多點傳送） 或 **both**（兩者）。
位址首碼		輸入您要讓 BGP 公告的 IP 位址。
下一個躍點		輸入您要讓 BGP 公告之 IP 位址的下一個躍點位址。
從端點		輸入從中接收（您要讓 BGP 公告的）前置詞之端點的 IP 位址。
	BGP > **Aggregate**（彙總） > **Aggregate Route Attributes**（彙總路由屬性）	定義彙總路由的屬性。
本地偏好設定		0-4,294,967,295 範圍內的本機偏好設定。
MED		0-4,294,967,295 範圍內的多出口鑑別器。
加權		0-65,535 範圍內的加權。
下一個躍點		下一個躍點 IP 位址。
原點		路由的來源：**igp**、**egp**、 或 **incomplete**（不完整）。
AS 路徑限制		1-255 範圍內的 AS 路徑限制。
AS 路徑		選取類型：**None**（無）或 **Prepend**（在前面加上）。
社群		選取類型：**None**（無）、**Remove All**（全部移除）、**Remove Regex**（移除 **Regex**）、**Append**（附加）或 **Overwrite**（覆寫）。
延伸社群		選取類型：**None**（無）、**Remove All**（全部移除）、**Remove Regex**（移除 **Regex**）、**Append**（附加）或 **Overwrite**（覆寫）。

BGP 重新散佈規則頁籤

- Network > Virtual Router > BGP > Redist Rules（網路 > 虛擬路由器 > BGP > 重新分配規則）

設定下表中說明的設定，以建立重新散佈 BGP 路由的規則。

BGP 重新散佈規則設定	設定位置	說明
允許重新分配預設路由	**BGP** > **Redist Rules**（重新分配規則）	允許防火牆將其預設路由重新散佈至 BGP 端點。
名稱		**Add**（新增）IP 子網路或先建立重新散佈規則。
啟用		選取此選項，可啟用此重新散佈規則。
路由表		指定路由將重新散佈到哪個路由表中：**unicast**（單點傳送）、**multicast**（多點傳送）或 **both**（兩者）。

© 2019 Palo Alto Networks, Inc.

BGP 重新散佈規則設定	設定位置	說明
指標		輸入 1-65,535 範圍內的度量。
設定原點		為重新散佈的路由選取原點（**igp**、**egp** 或 **incomplete**）。**incomplete** 值表示已連線的路由。
設定 MED		為重新散佈的路由輸入 0-4,294,967,295 範圍內的 MED。
設定本地偏好設定		為重新散佈的路由輸入 0-4,294,967,295 範圍內的本機偏好設定。
設定 AS 路徑限制		為重新散佈的路由輸入 1-255 範圍內的 AS 路徑限制。
設定社群		選取或輸入十進位或十六進位或者 AS:VAL 格式的 32 位元值；AS 和 VAL 都在 0-65535 的範圍內。輸入不超過 10 個的社群。
設定延伸社群		輸入十六進位或是 TYPE:AS:VAL 或 TYPE:IP:VAL 格式的 64 位元值。TYPE 是 16 位元、AS 或 IP 是 16 位元、VAL 是 32 位元。輸入不超過 5 個的延伸社群。

IP 多點傳送

- Network > Virtual Router > Multicast（網路 > 虛擬路由器 > 多點傳送）

設定多點傳送通訊協定需要設定下列標準設定：

多點傳送設定	說明
啟用	選取此選項可啟用多點傳送路由。

此外，必須在下列頁籤上進行設定：

- **Rendezvous Point**（會合點）：請參閱多點傳送會合點頁籤。
- **Interfaces**（介面）：請參閱多點傳送介面頁籤。
- **SPT Threshold**（**SPT** 閾值）：請參閱多點傳送 SPT 閾值頁籤。
- **Source Specific Address Space**（來源特定位址空間）：請參閱多點傳送來源特定位址頁籤。
- 進階：請參閱多點傳送進階頁籤。

多點傳送會合點頁籤

- Network > Virtual Router > Multicast > Rendezvous Point（網路 > 虛擬路由器 > 多點傳送 > 會合點）

使用下列欄位，設定 IP 多點傳送會合點：

多點傳送設定—會合點	說明
代表類型	選擇將在此虛擬路由器上執行的會合點 (RP) 類型。靜態 RP 必須明確設定其他 PIM 路由器上，而候選 RP 則是自動選取而得。

© 2019 Palo Alto Networks, Inc.

多點傳送設定—會合點	說明

	• 無—如果沒有 RP 在此虛擬路由器上執行，請選取此選項。
	• 靜態—指定 RP 的靜態 IP 位址，然後從下拉式清單中選擇 **RP Interface**（**RP** 介面）與 **RP Address**（**RP** 位址）的選項。如果您不使用針對此群組選取的 RP，而要改使用指定的 RP，請選取 **Override learned RP for the same group**（覆寫相同群組的已知 RP）。
	• 候選—為此虛擬路由器上執行的 RP 候選指定下列資資訊：
	  • **RP** 介面 — 選取 RP 的介面。有效的介面類型包括回路、L3、VLAN、彙總 Ethernet 與通道。
	  • **RP** 位址 — 選取 RP 的 IP 位址。
	  • 優先順序 — 指定候選 RP 訊息的優先順序（預設為 192）。
	  • 廣告間隔 — 指定候選 RP 訊息的宣告時間間隔。
	• 群組清單 — 如果您選擇 **Static**（靜態）或 **Candidate**（候選），按一下 **Add**（新增）可指定群組清單，這些群組是此候選 RP 提議成為其 PR 的群組。

遠端 Rendezvous Point	按一下 **Add**（新增）並指定下列資訊： • **IP** 位址 — 指定 RP 的 IP 位址。 • 覆寫相同群組的已知會合點—選取以使用指定的會合點，而不使用針對此群組選取的會合點。 • 群組 — 指定群組清單，指定的位址將做為這些群組的 RP。

多點傳送介面頁籤

- Network > Virtual Router > Multicast > Interfaces（網路 > 虛擬路由器 > 多點傳送 > 介面）

使用下列欄位以設定共用 IGMP、PIM 和群組權限設定的多點傳送介面：

多點傳送設定—介面	說明
名稱	輸入用來識別介面群組的名稱。
說明	輸入選取性說明。
介面	**Add**（新增）一個或多個屬於該介面群組的防火牆介面，因此可共用多點傳送群組權限、IGP 設定和 PIM 設定。
群組權限	指定參與 PIM Any-Source 多點傳送（ASM）或 PIM Source-Specific 多點傳送（SSM）的多點傳送群組： • **Any Source**（任何來源）—**Add**（新增）**Name**（名稱）以識別多點傳送 **Group**（群組），該群組被允許接收來自在介面群組中介面上任何來源的多點傳送流量。此群組預設為 **Included**（包含）在 **Any Source**（任何來源）清單內。取消選取 **Included**（包含）以輕鬆排除沒有刪除群組組態的群組。 • **Source Specific**（來源特定）—為多點傳送 **Group**（群組）和 **Source**（來源）IP 位址配對**Add**（新增）**Name**（名稱），其允許在介面群組中介面上的多點傳送流量。此群組和來源對預設為 **Included**（包含）在 來源特定清單內。取消選取 **Included**（包含）以輕鬆排除沒有刪除組態的群組和來源對。
IGMP	指定 IGMP 流量的設定。必須為多點傳送接收器面向的介面啟用 IGMP。

© 2019 Palo Alto Networks, Inc.

多點傳送設定—介面	說明

	• 啟用—選取以啟用 IGMP 組態。
	• **IGMP** 版本 — 選取要在介面上執行的第 1、2 或 3 版。
	• 強制路由器警示 **IP** 選項—選取以在使用 IGMPv2 或 IGMPv3 時，要求路由器警示 IP 選項。若要與 IGMPv1 相容，您必須停用此選項。
	• 加強性—選取代表網路封包遺失的整數值（範圍是 1 到 7；預設為 2）。如果封包遺失很常見，請選取較高的值。
	• 最大來源—指定介面群組允許的最大來源特定成員數量（範圍為 1 到 65,535 或 無限）。
	• 最大群組—指定此介面群組允許的多點傳送群組數量（範圍為 1 到 65,535 或 無限）。
	• 查詢組態 — 指定下列設定：
	  • 查詢間隔 — 指定傳送一般查詢到所有接收器的時間間隔。
	  • 最大查詢回應時間—指定一般查詢到接收器回應期間的最長時間。
	  • 上次成員查詢間隔 — 指定群組或特來來源查詢訊息（包含以回應傳送的訊息到離開群組的訊息）之間的時間間隔。
	  • 立即離開—選取以在收到離開訊息時立即離開群組。

PIM 組態	指定通訊協定獨立多點傳送 (PIM) 設定： • 啟用—選取以允許此介面接收和/或轉送 PIM 訊息。您必須啟用介面以轉送多點傳送流量。 • 判斷提示間隔—指定 PIM 判斷提示訊息到選取 PIM 轉送器間的時間間隔。 • **Hello** 間隔—指定 PIM Hello 訊息之間的時間間隔。 • 加入剪除間隔—指定 PIM 加入訊息間（以及 PIM 剪除訊息間）的秒數。預設為 60。 • **DR** 優先順序—指定此介面的指定路由器優先順序。 • **BSR** 邊界—選取以將介面當成啟動程序邊界使用。 • **PIM** 芳鄰—按一下 **Add**（新增）將使用 PIM 進行通訊的芳鄰清單。

多點傳送 *SPT* 臨界值頁籤

- Network > Virtual Router > Multicast > SPT Threshold（網路 > 虛擬路由器 > 多點傳送 > SPT 閾值）

最短路徑（SPT）閾值定義虛擬路由器為多點傳送群組或來自共享路徑散布（取自會合點）至來源（也稱為最短路徑或 SPT）散布前置詞切換多點傳送路由的時間點。**Add**（新增）多點傳送群組或前置詞的 SPT 閾值。

SPT 閾值	說明
多點傳送群組/前置詞	在群組或前置詞的吞吐量達到閾值設定時，指定多點傳送路由切換至 SPT 散布的多點傳送位址或前置詞。
閾值（**kbps**）	選取一個設定以指定多點傳送路由切換至對應多點傳送群組或前置詞 SPT 散布的時間點： • **0**（在第一個資料封包抵達時切換）—（預設）當一個群組或前置詞多點傳送封包抵達時，虛擬路由器切換至 SPT 散布。 • 永不（不切換至 **spt**）—虛擬路由器繼續轉送多點傳送流量至共享路徑的群組或前置詞。

© 2019 Palo Alto Networks, Inc.

SPT 閾值	說明
	• 輸入在任何介面和任何時長下可抵達對應多點傳送群組或前置詞的多點傳送封包總千位元數（範圍從 1 到 4,294,967,295）。當吞吐量到達該值時，虛擬路由器即切換至 SPT 散佈。

多點傳送來源特定位址空間頁籤

- 網路 > 虛擬路由器 > 多點傳送 > 來源特定位址空間

Add（新增）可以接收來自僅限特定來源的多點傳送封包的多點傳送群組。這些是與您在 **Multicast**（多點傳送）> **Interfaces**（介面）> **Group Permissions**（群組權限）頁籤中指定作為來源特定的相同多點傳送群組和名稱。

多點傳送設定—來源特定位址空間	說明
名稱	定義多點傳送群組，防火牆將針對此多點傳送群組提供來源特定的多點傳送 (SSM) 服務。
群組	指定一個可以接受來自僅限特定來源的多點傳送封包的多點傳送群組位址。
已包含	選取以包含在 SSM 位址空間的多點傳送群組。

多點傳送進階頁籤

- Network > Virtual Router > Multicast > Advanced（網路 > 虛擬路由器 > 多點傳送 > 進階）

設定多點傳送在工作階段結束後保留在路由表中的時間長度。

多點傳送進階設定	說明
路由逾時時間（秒）	允許您在工作階段結束時，以秒為單位對路由表中剩餘的多點傳送路由調整持續時間（範圍是 210-7200；預設為 210）。

ECMP

- Network > Virtual Routers > Router Settings > ECMP（網路 > 虛擬路由器 > 路由器設定 > ECMP）

等價多路徑 (ECMP) 處理是一種網路功能，可讓防火牆最多使用四個目的地相同的等價路由。若無此功能，則當有多個目的地相同的等價路由時，虛擬路由器會從路由表中選擇其中一個等價路由，然後新增到它的轉送表；虛擬路由器不會使用任何其他的路由，除非所選的路由中斷。啟用虛擬路由器上的 ECMP 功能，可讓防火牆在其轉送表中最多有四個到目的地的等價路徑，這可防火牆可以：

- 透過多個等價連結將流量 (工作階段) 負載平衡到相同的目的地。
- 使用目的地相同之所有連結上的可用頻寬，而非始終不使用某些連結。
- 如果連結失敗，便將指向其他 ECMP 成員的流量動態切換到相同的目的地，而非等待路由通訊協定或 RIB 表選擇替代的路徑，有助於降低連結失敗時的停機時間。

ECMP 負載平衡是在工作階段層級完成的，而非在套件層級完成的。這表示防火牆會在新工作階段開始時選擇等價路徑，而非在防火牆每次收到封包時選擇。

© 2019 Palo Alto Networks, Inc.

啟用、停用或變更現有虛擬路由器上的 *ECMP* 導致系統重新啟動虛擬路由器，這可能會導致工作階段終止。

若要為虛擬路由器設定 ECMP，請選取虛擬路由器，然後選取 **Router Settings**（路由器設定）的 **ECMP** 頁籤，再如說明設定 ECMP 設定。

您想了解什麼內容？	請參閱：
可用來設定 ECMP 的欄位有哪些？	ECMP 設定
想知道更多？	ECMP

ECMP 設定

- Network > Virtual Routers > Router Settings > ECMP（網路 > 虛擬路由器 > 路由器設定 > ECMP）

使用下列欄位可設定等價多路徑 (ECMP) 設定。

ECMP 設定	說明
啟用	**Enable**（啟用）ECMP。 啟用、停用或變更現有虛擬路由器上的 *ECMP* 導致系統重新啟動虛擬路由器，這有時會導致現有工作階段終止。
對稱傳回	（選用）按一下 **Symmetric Return**（對稱傳回）讓傳回封包輸出到相關聯進入封包到達的同一個介面。這會將防火牆設定為在傳送返回封包時使用進入介面，而不是 ECMP 介面，這意味著 **Symmetric Return**（對稱傳回）設定將取代負載平衡。只有從伺服器到用戶端的流量會發生此行為。
嚴格來源路徑	依預設，源自防火牆的 IKE 和 IPSec 流量會從 ECMP 負載平衡方法確定的介面輸出。選取 **Strict Source Path**（嚴格來源路徑），以確保源自防火牆的 IKE 和 IPSec 流量始終從 IPSec 通道的來源 IP 位址所屬的實體介面輸出。當防火牆有多個 ISP 提供到同一目的地的等價路徑時，可以啟用 Strict Source Path（嚴格來源路徑）。ISP 通常執行反向路徑轉送 (RPF) 檢查（或進行其他檢查以防止 IP 位址偽造），以確認流量從其到達的同一介面輸出。因為 ECMP 預設會根據設定的 ECMP 方法選擇輸出介面（而不是選擇來源介面作為輸出介面），這不符合 ISP 的預期，因此 ISP 可能會封鎖合法的回程流量。在這種情況下，請啟用 **Strict Source Path**（嚴格來源路徑），以便防火牆使用 IPSec 通道的來源 IP 位址所屬的介面作為輸出介面。
路徑上限	選取等價路徑數的上限：（2、3 或 4）到可從 RIB 複製到 FIB 之目的地網路（預設值為 2）。
方法	選取其中一個要在虛擬路由器上使用的 ECMP 負載平衡演算法。ECMP 負載平衡是在工作階段層級完成的，而非在套件層級完成的。這表示防火牆 (ECMP) 會在新工作階段開始時選擇等價路徑，而非在每次收到封包時選擇。 • **IP Modulo**（**IP** 模數）（預設值）—虛擬路由器會使用封包標頭中的來源與目的地 IP 位址的雜湊進行負載平衡，確定要使用哪一個 ECMP 路由。 • **IP Hash**（**IP** 雜湊）—有兩種 IP 雜湊方法可用於確定要使用的 ECMP 路由：

© 2019 Palo Alto Networks, Inc.

ECMP 設定	說明
	• 如果您選擇 **IP Hash**（IP 雜湊），則防火牆預設為使用來源的雜湊與目的地 IP 位址。 • 若您 **Use Source Address Only**（僅使用來源位址）（在 PAN-OS 8.0.3 和更新版本中可用），則防火牆將確保屬於同一來源 IP 位址的所有工作階段始終採用相同的路徑。 • 若您還 **Use Source/Destination Ports**（使用來源 / 目的地連接埠），則防火牆將包含任一雜湊計算中的連接埠。您也可以輸入 **Hash Seed**（雜湊種子）值（整數），進一步隨機處理負載平衡。 • **Weighted Round Robin**（加權循環配置資源）—您可以使用此演算法考量不同的連結容量與速度。選擇此演算法時，會開啟 Interface（介面）對話方塊。**Add**（新增）並選取要在加權循環配置資源群組中包含的 **Interface**（介面）。對於每個介面，輸入要用於該介面的 **Weight**（加權）（範圍是 1 至 255；預設值為 100）。特定等價路徑的加權值愈高，便會愈常為新的工作階段選取該等價路徑。應給予較快速連結比較慢速連結還高的加權值，讓更多的 ECMP 流量經過較快速的連結。然後可 **Add**（新增）另一個介面與加權。 • 平衡循環配置資源—將傳入的 ECMP 工作階段平均分配到連結之間。

更多的虛擬路由器執行階段統計資料

在您設定虛擬路由器的靜態路由或路由通訊協定時，請選取最後一欄中的 **Network**（網路）> **Virtual Routers**（虛擬路由器），然後選取 **More Runtime Stats**（更多執行階段統計資料），以查看有關虛擬路由器的詳細資訊，例如路由表、轉送表以及您設定的路由通訊協定和靜態路由。這些視窗提供的資訊超出虛擬路由器的單一畫面可顯示的資訊。此視窗會顯示下列頁籤：

- **Routing**（路由）：請參閱路由頁籤。
- **RIP**（路由資訊通訊協定）：請參閱 RIP 頁籤。
- **BGP**：請參閱 BGP 頁籤。
- **Multicast**（多點傳送）：請參閱多點傳送頁籤。
- **BFD Summary Information**（BFD 摘要資訊）：請參閱 BFD 摘要資訊頁籤。

路由頁籤

下表針對路由表、轉送表、靜態路由監控表說明虛擬路由的執行階段統計資料。

執行階段統計資料	說明
路由表	
路由表	選取 **Unicast**（單點傳送）或 **Multicast**（多點傳送）以顯示單點傳送或多點傳送的路由表。
顯示位址家族	選取 **IPv4 Only**（僅 IPv4）、**IPv6 Only**（僅 IPv6）或 **IPv4 and IPv6**（IPv4 和 IPv6）（預設值）以控制在表格中顯示哪個位址的群組。
目的地	虛擬路由器可到達的網路其 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。

© 2019 Palo Alto Networks, Inc.

執行階段統計資料	說明
指標	路由的公制。當路由通訊協定至同一目的地網路具有多於一個路由時，會偏好有最低度量值的路由。各路由通訊協定會使用不同的度量類型，例如 RIP 使用躍點計數。
加權	路由的加權。例如，當 BGP 至同一個目的地具有多於一個路由時，會偏好有最高加權的路由。
標幟	• **A?B**—主動並透過 BGP 得知。 • **A C**—主動且為內部介面（已連線）—目的地 = 網路的結果。 • **A H**—主動且為內部介面（已連線）—目的地 = 僅限主機的結果。 • **A R**—主動並透過 RIP 得知 • **A S**—主動且為靜態 • **S**—不主動（由於此路由的度量值較高）且為靜態 • **O1**—OSPF 外部類型-1 • **O2**—OSPF 外部類型-2 • **Oi**—區域內 • **Oo**—OSPF 區域間
年齡	路由表中路由項目的壽命。靜態路由沒有壽命。
介面	虛擬路由器的輸出介面用於到達下一個躍點。
重新整理	按一下以在表格中重新整理執行階段統計資料。

轉送表

防火牆會選擇置於 *FIB* 的最佳路由—從路由表 *(RIB)* 向目的地網路。

顯示位址家族	選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）（預設值）以控制要顯示哪個路由表。
目的地	從路由表選取、虛擬路由器可到達的最佳 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。
標幟	• **u**—路由使用中。 • **h**—路由至主機。 • **g**—路由至閘道。 • **e**—防火牆使用等價多重路徑 (ECMP) 選取此路由。 • *****—路由是至目的地網路的偏好路徑。
介面	虛擬路由器將用於到達下一個躍點的輸出介面。
MTU	最大傳輸單位 (MTU)；防火牆將在單一 TCP 封包中傳輸至此目的地的最大位元數。
重新整理	按一下以在表格中重新整理執行階段統計資料。

© 2019 Palo Alto Networks, Inc.

執行階段統計資料	說明
靜態路由監控	
目的地	虛擬路由器可到達的網路，其 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。
指標	路由的公制。當多於一個靜態路由至同一目的地網路時，防火牆會偏好具有最低度量值的路由。
加權	路由的加權。
標幟	• **A?B**—主動並透過 BGP 得知。 • **A C**—主動且為內部介面（已連線）—目的地 = 網路的結果。 • **A H**—主動且為內部介面（已連線）—目的地 = 僅限主機的結果。 • **A R**—主動並透過 RIP 得知 • **A S**—主動且為靜態 • **S**—不主動（由於此路由的度量值較高）且為靜態 • **O1**—OSPF 外部類型-1 • **O2**—OSPF 外部類型-2 • **Oi**—區域內 • **Oo**—OSPF 區域間
介面	虛擬路由器的輸出介面用於到達下一個躍點。
路徑監控 (啟動失敗)	若已針對此靜態路由啟用路徑監控，[啟動失敗] 表示： • 全部—若靜態路由的全部監控的目的地關閉時，防火牆會將靜態路由視為關閉，且將會進行容錯移轉。 • 任何—若靜態路由的任一監控的目的地關閉時，防火牆會將靜態路由視為關閉，且將會進行容錯移轉。 若靜態路由路徑監控已停用，[啟動失敗] 表示 **Disabled**（停用）。
STATUS (狀態)	基於 ICMP ping 至監控的目的地的靜態路由狀態：**Up**（開啟中）、**Down**（關閉），否則針對靜態路由的路徑監控為 **Disabled**（停用）。
重新整理	在表格中重新整理執行階段統計資料。

RIP 頁籤

下表說明虛擬路由器的 RIP 執行階段統計資料。

RIP 執行階段統計資料	說明
摘要頁簽	
間隔秒數	間隔中的秒數。RIP 使用此值（時間長度）控制其更新、到期和刪除間隔。

© 2019 Palo Alto Networks, Inc.

RIP 執行階段統計資料	說明
更新間隔	RIP 路由公告更新之間虛擬路由器傳送至端點的間隔數目。
到期間隔	自上次更新後虛擬路由器從端點接收的間隔數，此間隔數過後，虛擬路由器會將路由從端點改標示為無法使用。
刪除間隔	路由已標示為無法使用後的間隔數，若之間沒有收到更新，防火牆便會從路由表中刪除路由。
介面頁籤	
位址	RIP 有啟用的虛擬路由器其介面的 IP 位址。
驗證類型	驗證類型：簡式密碼、MD5 或無。
允許傳送	勾號表示允許此介面傳送 RIP 封包。
允許接收	勾號表示允許此介面接收 RIP 封包。
廣告預設路由	勾號表示 RIP 會向端點廣告其預設路由。
預設路由度量標準	指派給預設路由的公制值（躍點計數）。公制值愈低，其在路由表中被選為偏好路徑的優先順序愈高。
金鑰 Id	與端點搭配使用的驗證金鑰。
慣用	用於驗證的偏好金鑰。
端點頁籤	
對等位址	到虛擬路由器其 RIP 介面的端點 IP 位址。
上次更新	上次自此端點收到更新的日期與時間。
RIP 版本	端點正在執行的 RIP 版本。
無效的封包	從此端點收到的無效封包計數。防火牆無法剖析 RIP 封包的可能原因：超過路由邊界 x 個位元組、封包中過多路由、不良的子網路、非法的位址、驗證失敗，以及記憶體不足。
無效的路由	從此端點收到的無效路由計數。可能的原因：路由無效、匯入失敗，或記憶體不足。

BGP 頁籤

下表說明虛擬路由器的 BGP 執行階段統計資料。

BGP 執行階段統計資料	說明
摘要頁簽	

© 2019 Palo Alto Networks, Inc.

BGP 執行階段統計資料	說明
路由器 ID	指派給 BGP 實例的路由器 ID。
拒絕預設路由	指出已設定 [拒絕預設路由] 選項，這會造成 VR 忽略由 BGP 端點公告的任何預設路由。
重新分配預設路由	指出是否已設定 [允許重新散佈預設路由] 選項。
安裝路由	指出是否已設定 [安裝路由] 選項，這會造成 VR 將 BGP 路由安裝在全域路由表中。
非失誤性重新啟動	指出是否已啟用 [非失誤性重新啟動]（支援）。
AS 大小	指出選取的 [AS 格式大小] 為 2 個位元組或 4 個位元組。
本機 AS	VR 所屬的 AS 數目。
本地成員 AS	本地成員 AS 數目（只有在 VR 是在聯盟中時有效）。如果 VR 不在聯盟中，則此欄位為 0。
叢集 ID	顯示設定的反射程式叢集 ID。
預設本機偏好設定	顯示針對 VR 設定的預設本機偏好設定。
始終比較 MED	指出是否已設定 [一律比較 MED] 選項，這會進行比較，以從不同自發系統的芳鄰之間選擇路由。
彙總，無論 MED 為何	指出是否已設定 [彙總 MED] 選項，這讓路由即使有不同的 MED 值，仍會彙總路由。
具決定性的 MED 處理	指出是否已設定 [決定性 MED] 比較選項，這讓比較可以在 IBGP 端點公告的路由之間選擇（相同 AS 中的 BGP 端點)。
目前 RIB 輸出項目	RIB 外部表格中的項目數。
尖峰 RIB 外部項目	任何時候已配置 Adj-RIB-Out 路由的尖峰數。
對等頁籤	
名稱	對等名稱。
群組	對等所屬對等群組的名稱。
本機 IP	VR 上 BGP 介面的 IP 位址。
對等 IP	對等的 IP 位址。
對等 AS	對等所屬的自發系統。
密碼設定	指出是否已設定驗證。
STATUS (狀態)	對等的狀態，例如主動、連線、已建立、閒置、OpenConfirm 或 OpenSent。

© 2019 Palo Alto Networks, Inc.

BGP 執行階段統計資料	說明
狀態持續時間 (秒)	對等狀態持續時間。
對等群組頁籤	
群組名稱	對等群組的名稱。
類型	已設定的對等群組類型，例如 EBGP 或 IBGP。
彙總聯盟AS	指出是否已設定 [彙總聯盟 AS] 選項。
軟重設支援	指出對等群組是否支援軟重設。將政策路由至 BGP 對等變更時，可能會影響路由表更新。比起硬重設，一般偏好軟重設 BGP，因為軟重設無須清除 BGP 工作階段，就能更新路由表。
下一個自行躍點	是或否指出是否已設定此選項。
下一個協力廠商	是或否指出是否已設定此選項。
移除私人 AS	指出在傳送更新前，更新是否會先移除 AS_PATH 屬性中的私人 AS 號碼。
本機 RIB 子頁籤	
前置詞	本地路由資訊基礎中的網路前置詞與子網路遮罩。
旗標	* 指出獲選為最佳 BGP 路由的路由。
下一個躍點	前往前置詞的下一個躍點其 IP 位址。
Peer（對等）	端點名稱。
加權	指派給前置詞的加權屬性。如果防火牆有多個前往相同前置詞的路由，則會在 IP 路由表中安裝加權最高的路由。
本機偏好設定。	路由的本地偏好設定屬性，用於在有多個出口點時選擇前往前置詞的出口點。高本地偏好設定優先於低本地偏好設定。
AS 路徑	在前往前置詞網路的路徑中的自發系統清單；系統會在 BGP 更新中公告清單。
原點	前置詞的原點屬性；BGP 得知路由的方式。
MED	路由的多出口鑑別器 (MED) 屬性。MED 是路由的公制屬性，宣告路由的 AS 會假設為外部 AS。低 MED 優先於高 MED。
擺動計數	路由的擺動數目。
RIB 外部頁簽	
前置詞	路由資訊基礎中的網路路由項目。
下一個躍點	前往前置詞的下一個躍點其 IP 位址。

© 2019 Palo Alto Networks, Inc.

BGP 執行階段統計資料	說明
Peer（對等）	VR 將對其公告此路由的端點。
本機偏好設定。	存取前置詞的本地偏好設定屬性，用於在有多個出口點時選擇前往前置詞的出口點。高本地偏好設定優先於低本地偏好設定。
AS 路徑	在前往前置詞網路的路徑中的自發系統清單。
原點	前置詞的原點屬性；BGP 得知路由的方式。
MED	前置詞的多出口鑑別器 (MED) 屬性。MED 是路由的度量屬性，公告路由的 AS 會向外部 AS 建議其值。低 MED 優先於高 MED。
公告STATUS (狀態)	路由的公告狀態。
彙總STATUS (狀態)	指出此路由是否與其他路由彙總。

多點傳送頁籤

下表說明虛擬路由器的 IP 多點傳送執行階段統計資料。

多點傳送執行階段統計資料	說明
FIB 頁籤	
群組	在轉送資訊庫 (FIB) 的路由項目；虛擬路由器將轉送封包的多點傳送群組位址。
來源	該群組多點傳送封包的來源位址。
傳入介面	該群組多點傳送封包抵達的介面。
傳出介面	虛擬路由器轉送該群組多點傳送封包的傳出介面。
IGMP 介面頁籤	
介面	IGMP 已啟用的介面。
版本	在虛擬路由器上執行的網際網路管理通訊協定 (IGMP) 版本 1、2 或 3。
查詢器	連線至介面的多重存取區段上之 IGMP 查詢器的 IP 位址。
查詢器執行時間	IGMP 查詢器已啟動的秒數。
查詢器到期時間	在其他查詢器存留計時器到期前剩餘的秒數。
加強性	IGMP 介面的加強性變數。
群組限制	IGMP 可以同時處理之每個介面的最大群組數。

© 2019 Palo Alto Networks, Inc.

多點傳送執行階段統計資料	說明
來源限制	IGMP 可以同時處理之每個介面的最大來源數。
立即離開	[是] 或 [否] 表示是否已設定 [立即離開]。立即離開表示虛擬路由器會移除轉送表項目中的介面，而不傳送介面 IGMP 群組特有的查詢。
IGMP 成員頁籤	
介面	屬於此群組的介面名稱。
群組	介面所屬的多點傳送群組位址。
來源	傳送多點傳送封包至群組的來源 IP 位址。
執行時間	此成員資格已啟動的秒數。
到期時間	成員資格到期前剩餘的秒數。
篩選模式	包含或排除來源。虛擬路由器已設為包含所有流量，或僅包含來自此來源的流量（包含），或此來源以外任何來源的流量（排除）。
排除到期	介面排除狀態到期前剩餘的秒數。
V1 主機計時器	本地路由器假設距離附加至介面的 IP 子網路上不再有任何 IGMP 版本 1 成員的剩餘對間。
V2 主機計時器	本地路由器假設距離附加至介面的 IP 子網路上不再有任何 IGMP 版本 2 成員的剩餘對間。
PIM 群組對應頁籤	
群組	對應至 Rendezvous Point 的群組其 IP 位址。
會合點	群組會合點的 IP 位址。
原點	表示虛擬路由器得知 RP 的位置。
PIM 模式	ASM 或 SSM。
非現用	表示群組對 RP 的對應是否在非使用中。
PIM 介面頁籤	
介面	參與 PIM 的介面名稱。
位址	介面的 IP 位址。
DR	連接到介面的多重存取區段上之指定路由器的 IP 位址。
Hello 間隔	設定的您好間隔（秒數）。

© 2019 Palo Alto Networks, Inc.

多點傳送執行階段統計資料	說明
加入/剪除間隔	為加入與刪改訊息設定的間隔（秒）。
判斷提示間隔	設定的 PIM 判斷提示間隔（以秒為單位），供虛擬路由器傳送判斷提示訊息。PIM 使用判斷提示機制為多重存取網路選取 PIM 轉送程式。
DR 優先順序	為連線至介面的多重存取區段上之指定路由器設定的優先順序。
BSR 邊界	是或否表示介面是否在啟動程序路由器（BSR）在企業 LAN 邊界所在的虛擬路由器上。
PIM 芳鄰頁籤	
介面	虛擬路由器中的介面名稱。
位址	PIM 芳鄰可從介面到達的 IP 位址。
次要位址	PIM 芳鄰可從介面到達的第二 IP 位址。
執行時間	芳鄰已啟用的時間長度。
到期時間	芳鄰距離因虛擬路由器未收到芳鄰的 Hello 封包而到期的剩餘時間長度。
產生 ID	隨機產生的 32 位元值，每次在介面上啟動或重新啟動 PIM 轉送時都會重新產生（包括路由器自身重新啟動時）。
DR 優先順序	虛擬路由器在最後一個 PIM Hello 訊息中從此芳鄰收到的指定路由器優先順序。

BFD 摘要資訊頁籤

BFD 摘要資訊包含下列資料。

BFD 摘要資訊執行階段統計資料	說明
介面	執行 BFD 的介面。
通訊協定	在介面上執行 BFD 的靜態路由（靜態路由的 IP 位址系列）或動態路由通訊協定。
本機 IP 位址	您設定 BFD 之介面的 IP 位址。
芳鄰 IP 位址	BFD 芳鄰的 IP 位址。
狀態	本機和遠端 BFD 端點的 BFD 狀態：**admin down**（管理員關閉）、**down**（關閉）、**init**（初始） 或 **up**（開啟）。
執行時間	BFD 開啟的時間長度（小時、分鐘、秒和毫秒）。

© 2019 Palo Alto Networks, Inc.

BFD 摘要資訊執行階段統計資料	說明
鑑別器 (本機)	本機 BFD 端點的鑑別器。鑑別器是一個唯一的非零值，對等用它來區分對等之間的多個 BFD 工作階段。
鑑別器 (遠端)	遠端 BFD 端點的鑑別器。
錯誤	BFD 錯誤數。
SESSION DETAILS	按一下 **Details**（詳細資料）可檢視工作階段的 BFD 資訊，例如本機和遠端芳鄰的 IP 位址、上次接收的遠端診斷碼、已傳輸和接收的控制封包數目、錯誤數目、上次導致狀態變更之封包的相關資訊，以及其他資訊。

邏輯路由器的更多執行階段統計資料

在您設定邏輯路由器的靜態路由或路由通訊協定後，請選取 **Network**（網路） > **Logical Routers**（邏輯路由器），然後選取最後一欄中的 **More Runtime Stats**（更多執行階段統計資料），以查看有關邏輯路由器的詳細資訊，例如路由表、轉送表以及您設定的路由通訊協定和靜態路由。這些視窗提供的資訊超出邏輯路由器的單一畫面可顯示的資訊。此視窗會顯示下列頁籤：

- 路由（邏輯路由器的統計資料）
- BGP（邏輯路由器的統計資料）

邏輯路由器的路由統計資料

下表針對路由表、轉送表、靜態路由監控表說明邏輯路由器的執行階段統計資料。

執行階段統計資料	說明
路由表	
顯示位址家族	選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）（預設值）以控制在表格中顯示哪個位址的群組。
目的地	邏輯路由器可到達的網路 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。
通訊協定	指示該路由是靜態路由、連線路由，還是透過 BGP 獲知。
指標	路由的公制。當路由通訊協定至同一目的地網路具有多於一個路由時，會偏好有最低度量值的路由。各路由通訊協定會使用不同的度量類型，例如 RIP 使用躍點計數。
已選取	如果啟用，則該欄位為 true；如果停用，則為空白。
年齡	路由表中路由項目的壽命。

© 2019 Palo Alto Networks, Inc.

執行階段統計資料	說明
主動	如果啟用，則該欄位為 true；如果停用，則為空白。
介面	邏輯路由器的輸出介面將用於到達下一個躍點。
重新整理	按一下以在表格中重新整理執行階段統計資料。
轉送表	
防火牆會選擇置於 *FIB* 的最佳路由—從路由表 *(RIB)* 向目的地網路。	
目的地	從路由表選取、邏輯路由器可到達的網路最佳 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。
MTU	最大傳輸單位 (MTU)；防火牆將在單一 TCP 封包中傳輸至此目的地的最大位元數。
標幟	• **u**—路由使用中。 • **h**—路由至主機。 • **g**—路由至閘道。 • **e**—防火牆使用等價多重路徑 (ECMP) 選取此路由。 • *—路由是至目的地網路的偏好路徑。
介面	邏輯路由器將用於到達下一個躍點的輸出介面。
靜態路由監控	
目的地	邏輯路由器可到達的網路，其 IPv4 位址與網路遮罩，或 IPv6 位址與前置詞長度。
下一個躍點	前往目的地網路的下一個躍點處設備的 IP 位址。0.0.0.0 的下一個躍點表示預設路由。
指標	路由的公制。當多於一個靜態路由至同一目的地網路時，防火牆會偏好具有最低度量值的路由。
介面	邏輯路由器的輸出介面將用於到達下一個躍點。
路徑監控 (啟動失敗)	若已針對此靜態路由啟用路徑監控，[啟動失敗] 表示： • 全部—若靜態路由的全部監控的目的地關閉時，防火牆會將靜態路由視為關閉，且將會進行容錯移轉。 • 任何—若靜態路由的任一監控的目的地關閉時，防火牆會將靜態路由視為關閉，且將會進行容錯移轉。 若靜態路由路徑監控已停用，[啟動失敗] 表示 **Disabled**（停用）。

© 2019 Palo Alto Networks, Inc.

執行階段統計資料	說明
STATUS (狀態)	基於 ICMP ping 至監控的目的地的靜態路由狀態：**Up**（開啟中）、**Down**（關閉），否則針對靜態路由的路徑監控為 **Disabled**（停用）。
重新整理	在表格中重新整理執行階段統計資料。

邏輯路由器的 *BGP* 統計資料

下表說明邏輯路由器的 BGP 執行階段統計資料。

BGP 執行階段統計資料	說明
摘要頁簽	
已啟用	BGP 已啟用：是或否。
路由器 ID	邏輯路由器的路由器 ID。
本機 AS	邏輯路由器所屬的 AS。
執行首次 AS	如果啟用，則該欄位為 true；如果未啟用，則為空白。
快速外部容錯移轉	如果啟用，則該欄位為 true；如果未啟用，則為空白。
預設本機偏好設定	預設本機偏好設定已設定。
非失誤性重新啟動	如果啟用，則該欄位為 true；如果未啟用，則為空白。
最長對等重新啟動時間（秒）	為非失誤性重新啟動設定的最長對等重新啟動時間（秒）。
過時路由時間（秒）	為非失誤性重新啟動設定的過時路由時間（秒）。
始終比較 MED	如果啟用，則該欄位為 true；如果未啟用，則為空白。
具決定性的 MED 比較	如果啟用，則該欄位為 true；如果未啟用，則為空白。
對等頁籤	
名稱	對等名稱。
Peer Group（對等群組）	對等所屬對等群組的名稱。
本機 IP	邏輯路由器上 BGP 介面的 IP 位址。
本機 AS	本機 BGP 防火牆所屬的 AS。
對等 IP	對等的 IP 位址。
遠端 AS	對等所屬的 AS。

© 2019 Palo Alto Networks, Inc.

BGP 執行階段統計資料	說明
開啟/關閉	對等是開啟還是關閉。
狀態	已建立
對等群組頁籤	
名稱	對等群組的名稱。
類型	設定的對等群組類型，例如 ebgp 或 ibgp。
保持活動（秒）	保持活動的時間（秒）。
保持時間（秒）	保持的時間（秒）。
IP	如果啟用，則該欄位為 true；如果未啟用，則為空白。
IPv6	如果啟用，則該欄位為 true；如果未啟用，則為空白。
最小值路由間隔（秒）	最小路由間隔（秒）。
單點傳送	如果啟用，則該欄位為 true；如果未啟用，則為空白。
路由	
名稱	路由表中的 IPv4 或 IPv6 路由：IPv4 或 IPv6 位址和前綴長度。
AS 路徑	路徑中的下一個 AS。
最佳路徑	如果啟用，則該欄位為 true；如果未啟用，則為空白。
MED	0 或空白
指標	0 或空白
Network（網路）	
下一個躍點	到達網路的下一個躍點的 IP 位址被標識為路由（名稱）。
原點	路由的原點：IGP 或不完整
路徑	路徑中的下一個 AS。
路徑來源	指示外部。
對等名稱	
前置詞	
前綴長度	

© 2019 Palo Alto Networks, Inc.

BGP 執行階段統計資料	說明
有效	如果啟用，則該欄位為 true；如果未啟用，則為空白。
加權	路由的加權。

© 2019 Palo Alto Networks, Inc.

Network > Routing > Logical Routers（網路 > 路由 > 邏輯路由器）

使用您手動定義的靜態路由或透過參與第三層路由通訊協定（動態路由），防火牆需要邏輯路由器來取得到其他子網路的路由。在防火牆上定義的每個第三層介面、回送介面及 VLAN 介面都必須與邏輯路由器相關聯。每個介面都可以只屬於一個邏輯路由器。

在 **Device**（裝置）> **Setup**（設定）> **Management**（管理）的「一般設定」中啟用 **Advanced Routing**（進階路由），然後提交並重新啟動防火牆之後，邏輯路由器即可使用。

「進階路由引擎」目前僅處於預覽模式，並且提供有限的功能集。

定義邏輯路由器需要將第三層介面新增至邏輯路由器，並根據網路要求設定靜態路由和 BGP 路由的任意組合。您也可設定其他功能，例如 ECMP。

您想了解什麼內容？	請參閱
邏輯路由器的必要元素	邏輯路由器的一般設定
設定：	靜態路由 BGP BGP 路由設定檔 ECMP
檢視邏輯路由器的相關資訊。	邏輯路由器的更多執行階段統計資料

邏輯路由器的一般設定

- Network > Routing> Logical Routers > General（網路 > 路由 > 邏輯路由器 > 一般）

啟用「進階路由」（**Device**（裝置）> **Setup**（設定）> **Management**（管理））後，防火牆會使用邏輯路由器進行靜態和動態路由。邏輯路由器會要求您指派如下表所述名稱和第三層介面。防火牆上的「進階路由」路由引擎僅支援一個邏輯路由器。

您可以選擇為邏輯路由器設定等價多路徑 (ECMP)。ECMP 處理是一種網路功能，可讓防火牆最多使用四個目的地相同的等價路由。若無此功能，則當有多個目的地相同的等價路由時，虛擬路由器會從路由表中選擇其中一個等價路由，然後新增到它的轉送表；虛擬路由器不會使用任何其他的路由，除非所選的路由中斷。啟用虛擬路由器上的 ECMP 功能，可讓防火牆在其轉送表中最多有四個到目的地的等價路徑，這可防火牆可以：

- 透過多個等價連結將流量 (工作階段) 負載平衡到相同的目的地。
- 使用目的地相同之所有連結上的可用頻寬，而非始終不使用某些連結。
- 如果連結失敗，便將指向其他 ECMP 成員的流量動態切換到相同的目的地，而非等待路由通訊協定或 RIB 表選擇替代的路徑，有助於降低連結失敗時的停機時間。

ECMP 負載平衡是在工作階段層級完成的，而非在套件層級完成的。這表示防火牆會在新工作階段開始時選擇等價路徑，而非在防火牆每次收到封包時選擇。

© 2019 Palo Alto Networks, Inc.

邏輯路由器的一般設定	說明
名稱	指定用來說明邏輯路由器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
介面	新增您要包含在邏輯路由器中的第三層介面。這些介面可用作邏輯路由器路由表中的傳出介面。 若要指定介面類型，請參考 [網路 > 介面]。 新增介面時，會自動新增其連線的路由。
ECMP	
啟用	為邏輯路由器啟用等價多路徑 (ECMP)。
對稱傳回	（選用）按一下 **Symmetric Return**（對稱傳回）讓傳回封包輸出到相關聯進入封包到達的同一個介面。亦即防火牆將使用傳送傳回封包的 ingress 介面，而非使用 ECMP 介面，因此 **Symmetric Return**（對稱傳回）設定會覆寫負載平衡。只有從伺服器到用戶端的流量會發生此行為。
嚴格來源路徑	依預設，源自防火牆的 IKE 和 IPSec 流量會從 ECMP 負載平衡方法確定的介面輸出。選取 **Strict Source Path**（嚴格來源路徑），以確保源自防火牆的 IKE 和 IPSec 流量始終從 IPSec 通道的來源 IP 位址所屬的實體介面輸出。當防火牆有多個 ISP 提供到同一目的地的等價路徑時，您可以啟用「嚴格來源路徑」。ISP 通常執行反向路徑轉送 (RPF) 檢查（或進行其他檢查以防止 IP 位址偽造），以確認流量從其到達的同一介面輸出。因為 ECMP 預設會根據設定的 ECMP 方法選擇輸出介面（而不是選擇來源介面作為輸出介面），這不符合 ISP 的預期，因此 ISP 可能會封鎖合法的回程流量。在這種情況下，請啟用「嚴格來源路徑」，以便防火牆使用 IPSec 通道的來源 IP 位址所屬的介面作為輸出介面。
路徑上限	選取等價路徑數的上限：（2、3 或 4）到可從 RIB 複製到 FIB 之目的地網路。預設為 2。

負載平衡方法	選取其中一個要在虛擬路由器上使用的 ECMP 負載平衡演算法。ECMP 負載平衡是在工作階段層級完成的，而非在套件層級完成的。這表示防火牆 (ECMP) 會在新工作階段開始時選擇等價路徑，而非在每次收到封包時選擇。
	• **IP Modulo**（**IP** 模數）—依預設，虛擬路由器會使用此選項對工作階段進行負載平衡，此選項會使用封包標頭中的來源與目的地 IP 位址的雜湊來決定要使用哪一個 ECMP 路由。
	• **IP Hash**（**IP** 雜湊）—有兩種 IP 雜湊方法可用於確定要使用的 ECMP 路由：
	  • 如果您選擇 **IP Hash**（IP 雜湊），則防火牆預設為使用來源的雜湊與目的地 IP 位址。
	  • 或者，您可以選擇僅使用來源位址（PAN-OS 8.0.3 及更新版本中可用）。IP 雜湊方法可確保所有工作段階屬於總是採取相同路徑的相同來源 IP 位址。
	  • 可選擇選取 **Use Source/Destination Ports**（使用來源 / 目的地連接埠）以包含任一雜湊計算中的連接埠。您也可以輸入 **Hash Seed**（雜湊種子）值（整數），進一步隨機處理負載平衡。

© 2019 Palo Alto Networks, Inc.

邏輯路由器的一般設定	說明
	• 加權循環配置資源—此演算法可用於考量不同的連線容量與速度。選擇此演算法時，會開啟 [介面] 視窗。按一下 **Add**（新增），選取要在加權循環配置資源群組中包含的 **Interface**（介面）。對於每個介面輸入要用於該介面的加權。**Weight**（加權）預設為 100 秒，範圍是 1-255。特定等價路徑的加權值愈高，便會愈常為新的工作階段選取該等價路徑。應給予較快速連結比較慢速連結還高的加權值，讓更多的 ECMP 流量經過較快速的連結。再按一次 **Add**（新增）可新增其他的介面與加權。 • 平衡循環配置資源—將傳入的 ECMP 工作階段平均分配到連結之間。

邏輯路由器的靜態路由

- Network > Routing > Logical Routers > Static（網路 > 路由 > 邏輯路由器 > 靜態）

選取新增一個或多個靜態路由。選取 **IP** 或 **IPv6**，然後 **Add**（新增）使用 IPv4 或 IPv6 位址的路由。通常，您需要在此處設定預設路由 (0.0.0.0/0)。預設路由適用於目的地，無法在邏輯路由器的路由表中找到這些項目。

靜態路由設定	說明
名稱	輸入用來識別靜態路由的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
目的地	在無類別網域間路由選取 (CIDR) 標記法中輸入 IP 位址和網路遮罩：*ip_address*/ 遮罩 （例如，適用於 IPv4 的 192.168.2.0/24，或適用於 IPv6 的 2001:db8::/32）。或者，您可以建立類型為 IP 網路遮罩的位址物件。
介面	選取用來將封包轉送至目的地的傳出介面，或設定下一個躍點設定，或執行這兩項操作。指定介面以對防火牆使用的介面進行更嚴格的控制，而不要使用路由表中用作此路由下一個躍點的介面。
下一個躍點	選取下列其中一項： • **IP Address**（**IP** 位址）—選取以輸入下一躍點路由器的 IP 位址，或選取或建立類型 IP 網路遮罩的位址物件。IPv4 的位址物件必須有 /32 的網路遮罩，IPv6 則是 /128。（在設定第三層介面時）您必須 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**），以使用 IPv6 下一個躍點位址。 • **Discard**（捨棄）—選取您是否想丟棄定址到此目的地的流量。 • **None**（無）—如果路由沒有下一個躍點，請選取此選項。例如，點對點連線不需要下一個躍點，因為封包只有一個傳遞方向。
管理員距離	為靜態路由指定管理距離（範圍是 10 至 240；預設值為 10）。
指標	為靜態路由指定有效的指標（範圍是 1 至 65,535；預設值為 10）。
路徑監控	選取並啟用靜態路由的路徑監控。
失敗條件	選取防火牆將監控的路徑視為關閉、因此將靜態路徑視為關閉的條件： • 任何—若靜態路由的任一監控的目的地無法透過 ICMP 連線，防火牆會自 RIB 和 FIB 移除靜態路由，並在動態或靜態路由中，將通向同一目的地的度量為次低者新增至 FIB。

© 2019 Palo Alto Networks, Inc.

靜態路由設定	說明
	• 所有—若靜態路由的所有監控的目的地皆無法透過 ICMP 連線，防火牆才會自 RIB 和 FIB 移除靜態路由，並在動態或靜態路由中，將通向同一目的地的度量為次低者新增至 FIB。 選取 **All**（所有）能避免（例如）監控的目的地僅因維護而離線時，單一監控的目的地發出靜態路由失敗的信號。
先佔保留時間 (分鐘)	輸入已關閉路徑監控必須保持使用中狀態的分鐘數—該路徑監控會評估其所有監控的目的地成員，且在防火牆將靜態路由重新安裝至 RIB 前，必須保持為使用中。如果計時器到期且連結不關閉或波動，則該連結將被視為穩定，路徑監控可保持為使用中，防火牆可將靜態路由再次新增到 RIB 中。 若在保留時間內連結關閉或波動，則路徑監控會失敗，且當關閉的監控回到使用中狀態時，計時器會重新啟動。若 **Preemptive Hold Time**（先佔保留時間）為 0，會讓防火牆在路徑監控進入使用中狀態時立刻將靜態路由重新安裝至 RIB。範圍是 0 至 1,440；預設值為 2。
名稱	輸入監控的目的地名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
啟用	選取則會為靜態路由啟用對此特定目的地的路徑監控；防火牆會將 ICMP ping 傳送至此目的地。
來源 IP	選取 IP 位址，在對監控的目的地的 ICMP ping 中，防火牆將使用此位址作為來源： • 若介面有多個 IP 位址，請選取一個。 • 依預設，若您選取介面，防火牆會使用指派給介面的第一個 IP 位址。 • 若您選取 **DHCP (Use DHCP Client address)**（**DHCP**（使用 **DHCP** 用戶端位址）），防火牆會使用 DHCP 指派給介面的位址。若要查看 DHCP 位址，可選取**Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）並在乙太網路介面的列中，然後按一下 **Dynamic DHCP Client**（動態 **DHCP** 用戶端）。IP 位址會顯示在動態 IP 介面狀態視窗中。
目的地 Ip	輸入健全、穩定的 IP 位址或位址物件，防火牆將針對該位址進行路徑監控。監控的目的地和靜態路由目的地必須使用相同位址家族（IPv4 或 IPv6）。
Ping 間隔（秒）	指定 ICMP ping 間隔（秒），以確定防火牆監控路徑的頻率（ping 監控的目的地；範圍是 1 至 60；預設值為 3）。
Ping 計數	在此指定者，為防火牆將連結視為關閉前，ICMP ping 封包不從監控的目的地傳回的連續數量。根據 **Any**（任何）或 **All**（全部）失敗條件，若路徑監控處於失敗狀態，則防火牆會自 RIB 移除靜態路由（範圍是 3 至 10；預設值為 5）。 例如，Ping 間隔為 3 秒且 Ping 計數為錯失 ping 5 次（防火牆在過去 15 秒中沒有接收到 ping）表示路徑監控偵測到連結失敗。若路徑監控在失敗狀態中，且防火牆在 15 秒後接收到 ping，則連結會被視為使用中；根據 **Any**（任何）或 **All**（全部）失敗條件，對 **Any**（任何）或 **All**（全部）監控的目的地的路徑監控可被視為使用中，且先佔保留時間會啟動。

邏輯路由器的 BGP 路由

- Network > Routing> Logical Routers > BGP（網路 > 路由 > 邏輯路由器 > BGP）

© 2019 Palo Alto Networks, Inc.

下表說明了針對邏輯路由器進行的 BGP、對等群組、對等和重新散佈設定。

BGP 設定	說明
總言	
啟用	為邏輯路由器啟用 BGP。
路由器 ID	為邏輯路由器的 BGP 指派一個路由器 ID，一般為 IPv4 位址，以確保路由器 ID 是唯一的。
本機 AS	根據路由器 ID 指派邏輯路由器所屬的本機自發系統 (AS)（2 位元組或 4 位元組 AS 編號的範圍為 1 至 4,294,967,295）。
ECMP 多 AS 支援	如果您設定了 ECMP 並希望在多個 BGP 自發系統上執行 ECMP，則啟用。
執行首次 AS	選取該項，使防火牆丟棄未在 AS_PATH 屬性中將 EBGP 對等本身的 AS 編號列為第一個 AS 編號的 EBGP 對等所傳入的更新訊息。（預設為啟用。）
快速容錯移轉	預設會啟用 EBGP 快速容錯移轉。如果 EBGP 快速容錯移轉導致防火牆不必要地撤回 BGP 路由，則將其停用。
預設本機偏好設定	指定預設本機偏好設定，其可用於確定不同路徑中的偏好設定；範圍為 0 至 4,294,967,295；預設為 100。
非失誤性重新啟動—啟用	為 BGP 啟用非失誤性重新啟動，以便在 BGP 重新啟動期間不中斷封包轉送（預設為啟用）。
過時路由時間	指定路由可以保持過時狀態的時長（秒）（範圍是 1 至 3,600，預設為 120）。
最長對等重新啟動時間	指定本機裝置接受對等裝置寬限期重新啟動時間的時間長度上限（以秒為單位，範圍為 1 至 3,600；預設值為 120）。
路徑選擇—始終比較 MED	選取該項可從不同自發系統中的芳鄰選擇路徑；預設為啟用。多出口鑑別器 (MED) 是外部公制，可讓芳鄰知道到 AS 的偏好路徑。值愈低的路徑表示偏好度高於值愈高的路徑。
具決定性的 MED 比較	選取該項以在 IBGP 對等（相同 AS 中的 BGP 對等）所公告的路由間進行選擇。預設為啟用。
Peer Group（對等群組）	
名稱	輸入 BGP 對等群組的名稱。
啟用	啟用對等群組。
類型	選取對等群組的類型為 **IBGP**（內部 BGP、AS 內的對等）或 **EBGP**（外部 BGP—兩個自發系統間的對等）。
AFI IP 單點傳送	選取或建立 AFI IPv4 設定檔，以將設定檔中的設定套用至對等群組；預設為 **None**（無）。

© 2019 Palo Alto Networks, Inc.

BGP 設定	說明
AFI IPv6 單點傳送	選取或建立 AFI IPv6 設定檔，以將設定檔中的設定套用至對等群組；預設為 **None**（無）。
驗證設定檔	選取或建立驗證設定檔，以驗證 BGP 對等通訊；預設為 **None**（無）。
計時器設定檔	選取或建立計時器設定檔以套用至對等群組；預設為 **None**（無）。
多重躍點	在 IP 標頭中設定存留時間 (TTL) 值。範圍為 1 至 255；設定為 0 表示使用預設值：若是 EBGP，則為 1；若是 IBGP，則為 255。
Peer（對等）	
名稱	輸入 BGP 對等的名稱。
啟用	啟用 BGP 對等。
對等 AS	輸入對等所屬的 AS；範圍為 1 至 4,294,967,295。
Peer—Addressing（對等—定址）	
從對等群組繼承 AFI/SAFI 設定	選取要從對等群組繼承 AFI 和後續 AFI (SAFI) 的對等。
AFI IP 單點傳送	（如果停用了 **Inherit AFI/SAFI config from peer**（從對等繼承 **AFI/SAFI** 設定），則可用）選取或建立 AFI IPv4 設定檔，以將設定檔中的設定套用至對等；預設為 **None**（無）。
AFI IPv6 單點傳送	（如果停用了 **Inherit AFI/SAFI config from peer**（從對等繼承 **AFI/SAFI** 設定），則可用）選取或建立 AFI IPv6 設定檔，以將設定檔中的設定套用至對等；預設為 **None**（無）。
本機位址—介面	選取您要為其設定 BGP 的第三層介面。可以選擇設定具有靜態 IP 位址的介面和設定為 DHCP 用戶端的介面。如果選取 DHCP 指派位址的介面，則 **IP** 位址會指示 **None**（無）。DHCP 稍後將為介面指派 IP 位址；當您檢視邏輯路由器的 **More Runtime Stats**（更多執行階段統計資料）時，可以看到該位址。
IP	如果介面具有多個 IP 位址，則輸入要使用的 IP 位址和網路遮罩。
對等位址 - IP	輸入對等的 IP 位址。
Peer—Connection Options（對等—連接選項）這些設定會取代您為對等所屬的對等群組設定的相同選項。	
驗證設定檔	選取或建立驗證設定檔。或者，選取 **inherit (Inherit from Peer-Group)**（繼承（繼承自對等群組））或 **None**（無），這兩者均會導致對等使用為對等群組指定的驗證設定檔。
計時器設定檔	選取或建立計時器設定檔。或者，選取 **inherit (Inherit from Peer-Group)**（繼承（繼承自對等群組））或 **None**（無），這兩者均會導致對等使用為對等群組指定的計時器設定檔。

© 2019 Palo Alto Networks, Inc.

BGP 設定	說明
多重躍點	選取 **inherit (Inherit from Peer-Group)**（繼承（繼承自對等群組））或 **None**（無），這兩者均會導致對等使用為對等群組指定的值。
Peer-Advanced（對等-進階）	
啟用寄件者端迴圈偵測	選取該項可使防火牆先在其轉送資訊庫 (FIB) 中檢查路由的 AS_PATH 屬性，再於更新中傳送該路由，以確保對等 AS 號碼不在 AS_PATH 清單中。如果在清單中，防火牆會加以移除，以防止發生迴圈。預設為啟用。
BGP Redistribution（**BGP** 重新散佈）	
Redistribution Rules（重新散佈規則）	
IPv4 單點傳送	選取或建立重新散佈設定檔，以指定要重新散佈至 IPv4 單點傳送路由表的靜態或連線 IPv4 路由。預設值為 **None**（無）。
IPv6 單點傳送	選取或建立重新散佈設定檔，以指定要重新散佈至 IPv6 單點傳送路由表的靜態或連線 IPv6 路由。預設值為 **None**（無）。
Network（網路）	
IPv4 或 IPv6	選取 **IPv4** 或 **IPv6**。
Network（網路）	新增相應的 IPv4 或 IPv6 網路位址；具有相符網路位址的子網路將公告至邏輯路由器的 BGP 對等。
單點傳送	選取該項以將相符路由安裝至所有 BGP 對等的單點傳送路由表中。

Network > Routing > Routing Profiles > BGP（網路 > 路由 > 路由設定檔 > BGP）

對於邏輯路由器，請使用 BGP 設定檔將設定有效地套用至 BGP 對等群組、對等或重新散佈規則。例如，您可以將計時器設定檔或驗證設定檔套用至 BGP 對等群組或對等。您可以將 IPv4 和 IPv6 的位址系列 (AFI) 設定檔套用至對等群組。您可以將 IPv4 和 IPv6 的重新散佈設定檔套用至 BGP 重新散佈。

BGP 路由設定檔	說明
BGP 驗證設定檔	
名稱	輸入驗證設定檔的名稱（最多 31 個字元）。
密碼	輸入密碼，然後 **Confirm Secret**（確認密碼）。該機密用作 MD5 驗證中的金鑰。
BGP 計時器設定檔	
名稱	輸入計時器設定檔的名稱（最多 31 個字元）。

© 2019 Palo Alto Networks, Inc.

BGP 路由設定檔	說明
保持運作的間隔（秒）	輸入間隔（秒），在此間隔後，根據「保留時間」設定，來自該對等的路由將被隱藏（範圍為 0 至 1,200；預設為 30）。
保持時間（秒）	輸入時長（秒），即關閉對等連線之前，來自對等的連續「保持活動」或「更新」訊息之間可能經過的時間（範圍為 3 至 3,600，預設值為 90）。
最小路由公告間隔（秒）	輸入最短間隔時間（秒），即 BGP 發言者（防火牆）向 BGP 對等傳送用來公告路由或撤銷路由的連續兩則「更新」訊息之間的時間（範圍為 1 至 600；預設值為 30）。
BGP 位址系列設定檔	
名稱	輸入位址系列識別碼 (AFI) 設定檔的名稱（最多 31 個字元）。
IPv4 或 IPv6	選取 AFI 設定檔的類型（IPv4 或 IPv6）。
將所有路徑公告給對等	在 BGP 路由資訊庫 (RIB) 中公告所有路由。
公告每個相鄰 AS 的最佳路徑	啟用以確保 BGP 為每個相鄰 AS 公告最佳路徑，而非針對所有自發系統公告的一般路徑。如果要向所有自發系統公告相同的路徑，請停用此功能。
允許 AS 為以下狀態	指定是否允許包含防火牆自身的自發系統 (AS) 編號的路由： • **Origin**（原始）—即使 AS_PATH 中存在防火牆自身的 AS，也接受路由。 • **Occurrence**（發生頻率）—防火牆自身的 AS 可在 AS_PATH 的次數。 • **None**（無）—（預設設定）不執行任何動作。
如果 AS-Path 等同於 Remote-AS，則在輸出更新中取代 ASN	如果您有多個站台屬於同一 AS（例如，AS 64512），並且它們之間存在另一個 AS，則可以使用 BGP AS 取代功能。兩個站台之間的路由器收到「更新」，該更新公告可存取 AS 64512 的路由。為了避免第二個站台因其也在 AS 64512 中而丟棄該「更新」，中間路由器將 AS 64512 取代為其自己的 ASN，例如 AS 64522。
發起預設路由	選取該項以公告預設路由。如果僅要公告到達特定目的地的路由，則請停用。
Num_prefixes	輸入要從對等接受的最大前綴數。
閾值 (%)	輸入最大前綴數的閾值百分比。如果對等公告超過閾值，則防火牆將執行指定的動作（警告或重新啟動）。範圍為 1 至 100%。
動作	指定超過最大前綴數后防火牆對 BGP 連線執行的動作：日誌中的 **Warning Only**（僅警告）訊息或 **Restart**（重新啟動）BGP 對等連線。
下一個躍點	選取下一個躍點： • **None**（無）—不執行任何動作；計算該芳鄰的下一個躍點。 • **Self**（自我）—停用下一個躍點計算，並使用本機下一個躍點來公告路由。 • **Self Force**（自我強制）—強制將反射路徑的下一個躍點設定為「自我」。
移除私人 AS	若要讓 BGP 從防火牆傳送至另一個 AS 中對等的「更新」中AS_PATH 屬性移除私人 AS 編號，請選取以下其中一個選項：

© 2019 Palo Alto Networks, Inc.

BGP 路由設定檔	說明
	• **All**（全部）—移除所有私人 AS 編號。 • **Replace AS**（取代 **AS**）—用防火牆的 AS 編號取代所有私人 AS 編號。 • **None**（無）—（預設設定）不執行任何動作。
路由反射程式用戶端	將防火牆啟用為 BGP 路由反射程式用戶端。
傳送社群	選取 BGP 社群屬性的類型以傳送輸出「更新」訊息： • **All**（全部）—傳送所有社群。 • **Both**（兩者）—傳送標準社群和延伸社群。 • **Extended**（延伸）—傳送延伸社群。 • **Large**（大型）—傳送大型社群。 • **Standard**（標準）—傳送標準社群。 • **None**（無）—不傳送任何社群。
BGP 重新散佈設定檔	
名稱	輸入重新散佈設定檔的名稱（最多 31 個字元）。
IPv4 或 IPv6	選取 IPv4 或 IPv6 位址系列識別碼 (AFI)，以指定要重新散佈的路由類型。
靜態	選取 **Static**（靜態）和 **Enable**（啟用），以將 IPv4 或 IPv6 靜態路由（與您選取的 AFI 相符）重新散佈至 BGP 對等的 BGP 路由資訊庫 (RIB) 中。
度量	輸入指標以套用於要重新散佈至 BGP 中的靜態路由（範圍為 1 至 65,535）。
已連線	選取 **Connected**（已連線）和 **Enable**（啟用），將 IPv4 或 IPv6 連線的路由（與您選取的 AFI 相符）重新散佈至 BGP 對等的 BGP 路由資訊庫 (RIB) 中。
度量	輸入指標以套用於要重新散佈至 BGP 中的連線路由（範圍為 1 至 65,535）。

© 2019 Palo Alto Networks, Inc.

網路 > IPSec 通道

選取 **Network**（網路）> **IPSec Tunnels**（**IPSec** 通道）可在防火牆之間建立 IPSec VPN 通道並加以管理。這是 IKE/IPSec VPN 設定的階段 2 部分。

您想了解什麼內容？	請參閱：
管理 IPSec VPN 通道。	IPSec VPN 通道管理
設定 IPSec 通道。	IPSec 通道一般頁籤
	IPSec 通道 Proxy ID 頁籤
檢視 IPSec 通道狀態。	防火牆的 IPSec 通道狀態
重新啟動或重新整理 IPSec 通道。	IPSec 通道重新啟動或重新整理
想知道更多？	設定 IPSec 通道。

IPSec VPN 通道管理

- 網路 > IPSec 通道

下表說明如何管理 IPSec VPN 通道。

用來管理 IPSec VPN 通道的欄位	
新增	**Add**（新增）IPSec VPN 通道。如需設定新通道的指示，請參閱 IPSec 通道一般頁籤。
刪除	**Delete**（刪除）不再需要的通道。
啟用	**Enable**（啟用）已停用的通道（通道依預設為啟用狀態）。
停用	**Disable**（停用）您已不想使用但還沒準備要刪除的通道。
PDF/CSV	匯出 **PDF/CSV** 格式的 IPSec 通道設定。您可以套用篩選器以自訂表格輸出且僅包含您需要的欄位。僅可匯出匯出對話中可見的欄位。請參閱匯出設定表資料。

IPSec 通道一般頁籤

- 網路 > IPSec 通道 > 一般

請使用下列欄位來設定 IPSec 通道。

IPSec 通道一般設定	說明
名稱	輸入用來識別通道的 **Name**（名稱）（最多 63 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。

© 2019 Palo Alto Networks, Inc.

IPSec 通道一般設定	說明
	此欄位的 63 個字元限制包含通路名稱及 Proxy ID，這是以分號區隔。
隧道接口	選取現有通道介面，或按一下 **New Tunnel Interface**（新增通道介面）。如需建立通道介面的相關資訊，請參考 [網路 > 介面 > 通道]。
IPv4 或 IPv6	選取 **IPv4** 或 **IPv6** 可設定通道以擁有該 IP 類型位址的端點。
類型	選取要使用自動產生的安全性金鑰，還是手動輸入的安全性金鑰。建議使用自動金鑰。
自動鍵	如果您選取 **Auto Key**（自動金鑰），請指定下列資訊： • **IKE 閘道**—如需 IKE 閘道設定的說明，請參考 [網路 > 網路設定檔 > IKE 閘道]。 • **IPSec 加密設定檔** — 選取現有設定檔或保留預設設定檔。若要定義新的設定檔，請按一下 **New**（新增），並依照 [網路 > 網路設定檔 > IPSec 加密] 中的指示執行操作。 • 按一下 **Show Advanced Options**（顯示進階選項）可存取剩餘的欄位。 • **啟用重播保護**—選取此選項可防範重播攻擊。 • **複製 TOS 標頭** — 將（服務類型）TOS 欄位從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 TOS 資訊。此選項也會複製 [明確擁塞通知] (ECN) 欄位。 • **Add GRE Encapsulation**（新增 **GRE** 封裝）—選取以增加一個封裝在 IPSec 通道的 GRE 標頭。防火牆會在產生 IPSec 標頭後產生 GRE 標頭，以與其他廠商通道端點產生互通性，從而與 IPSec 通道共用 GRE 通道。 • **通道監控**—選取此選項可向裝置管理員警示通道失敗，並提供其他介面的自動故障保護的功能。 您需要將 *IP* 位址指派給通道介面，才能進行監控。 • **目的地 IP**—指定通道監控將用來判斷通道是否正常運作的通道另一端 IP 位址。 • **設定檔** — 選取現有的設定檔，用於判斷通道失敗時所採取的動作。如果監控設定檔中指定的動作是等待復原，防火牆將等待通道運作，且「不」會尋求含路由表的替代路徑。如果使用容錯移轉動作，防火牆將檢查路由表，瞭解是否有替代路由可到達目的地。詳細資訊，請參閱 [網路 > 網路設定檔 > 監控]。
手動金鑰	如果您選取 **Manual Key**（手動金鑰），請指定下列資訊： • **Local SPI** — 針對本機防火牆到端點之間的封包穿透機制，指定本機安全性參數索引 (SPI)。SPI 是新增到表頭的十六進位制索引，能讓 IPSec 通道協助區別 IPSec 流量。 • **介面** — 選取通道端點的介面。 • **本機位址** — 針對做為通道端點的本機介面，選取 IP 位址。 • **遠端 SPI** — 針對遠端防火牆到端點之間的封包穿透機制，指定遠端安全性參數索引 (SPI)。 • **通訊協定** — 選取流量通過通道所使用的通訊協定（**ESP** 或 **AH**）。 • **驗證**—選取通道存取的驗證類型（**SHA1**、**SHA256**、**SHA384**、**SHA512**、**MD5** 或 **None**（無））。

© 2019 Palo Alto Networks, Inc.

IPSec 通道一般設定	說明
	• 金鑰/確認金鑰 — 輸入並確認驗證金鑰。 • 加密—選取通道流量的加密選項（**3des**、**aes-128-cbc**、**aes-192-cbc**、**aes-256-cbc**、**des** 或 **null** [不加密]）。 • 金鑰/確認金鑰 — 輸入並確認加密金鑰。
GlobalProtect 衛星	如果您選取 **GlobalProtect Satellite**（GlobalProtect 衛星），請指定下列資訊： • 名稱 — 輸入用來識別通道的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 • 通道介面—選取現有通道介面，或按一下 [新增通道介面]。 • 入口網站位址—輸入 GlobalProtect™ 入口網站的 IP 位址。 • 介面—從下拉式清單中選取通往 GlobalProtect 入口網站的下行介面。 • 本機 **IP** 位址—輸入連接 GlobalProtect 入口網站的下行介面 IP 位址。 • 進階選項 • 將所有靜態與連接的路由發佈至閘道—選取此選項可將衛星裝置的所有路由發佈到連接衛星的 GlobalProtect 閘道。 • 子網路—按一下 **Add**（新增）可手動新增衛星裝置位置的本機子網路。如果其他衛星裝置正在使用相同的子網路資訊，您必須以 NAT 傳輸通道介面 IP 所有的流量。另外，在這種情況下，衛星裝置不可共用路由，因此將透過通道 IP 進行所有路由。 • 外部憑證授權單位—如果您使用外部 CA 管理憑證，請選取此選項。一旦產生憑證，您需要將憑證匯入衛星，並選取 **Local Certificate**（本機憑證）和 **Certificate Profile**（憑證設定檔）。

IPSec 通道 Proxy ID 頁籤

- 網路 > IPSec 通道 > 代理程式ID

IPSec Tunnel 代理程式 **IDs**（**IPSec** 通道 代理程式 **ID**）頁籤分成兩個子頁籤：**IPv4** 和 **IPv6**。兩種類型的說明類似，下表的 **Local**（本機）與 **Remote**（遠端）欄位說明　IPv4 與 IPv6 間的不同。

IPSec Tunnel 代理程式 **IDs**（**IPSec** 通道 代理程式 **ID**）頁籤可用於指定 IKEv2 的流量選取器。

代理程式 ID IPv4 和 IPv6 設定	說明
代理程式 ID	按一下新增，並輸入用來識別 代理程式 的名稱。 IKEv2 流量選取器會使用此欄位作為 [名稱]。
本地	適用於 IPv4：以 x.x.x.x/遮罩格式（例如 10.1.2.0/24）輸入 IP 位址或子網路。 適用於 IPv6：以 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/前置詞-長度（或依照 IPv6 慣例，例如 2001:DB8:0::/48）輸入 IP 位址和前置詞長度。 IPv6 定址不需要寫入所有的零；前置的零可以省略，某一組連續的零可由兩個相鄰的冒號 (::) 覆寫。 IKEv2 流量選取器的這個欄位會轉換成 [來源 IP 位址]。
遠端	如果端點需要： 若為 IPv4，則以 x.x.x.x/遮罩格式（例如 10.1.1.0/24）輸入 IP 位址或子網路。

© 2019 Palo Alto Networks, Inc.

代理程式 ID IPv4 和 IPv6 設定	說明
	若為 IPv6，則以 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/前置詞-長度（或依照 IPv6 慣例，例如 2001:DB8:55::/48）輸入 IP 位址和前置詞長度。 IKEv2 流量選取器的這個欄位會轉換成 [目的地 IP 位址]。
通訊協定	指定本機與遠端連接埠的通訊協定與埠號： 號碼—指定通訊協定號碼（用於與第三方裝置交互操作）。 • 任何—允許 TCP 與/或 UDP 流量。 • **TCP**—指定本機與遠端 TCP 埠號。 • **UDP**—指定本機與遠端 UDP 埠號。 每個設定的 代理程式 ID 都會計入防火牆的 IPSec VPN 通道容量。 此欄位也作為 IKEv2 流量選取器。

防火牆的 IPSec 通道狀態

- 網路 > IPSec 通道

若要檢視目前定義的 IPSec VPN 通道的狀態，請開啟 **IPSec** 通道頁面。此頁面提供下列狀態資訊：

- 通道狀態（第一個狀態欄）—綠色表示為 IPSec 階段 2 安全性關聯 (SA) 通道。紅色表示 IPSec 階段 2 SA 無法使用或已過期。
- IKE 閘道狀態—綠色表示是有效的 IKE 階段 1 SA 或 IKE 階段 2 SA。紅色表示 IKE 階段 1 SA 無法使用或已過期。
- 通道介面狀態—綠色表示通道介面使用中（由於已停用通道監控，或由於通道監控狀態為使用中且監控的 IP 可連線）。紅色表示由於已啟用通道監控，且無法連線遠端通道監控 IP 位址，因此通道介面已關閉。

IPSec 通道重新啟動或重新整理

- 網路 > IPSec 通道

選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道）可顯示通道狀態。第一個狀態欄中有通道資訊的連結。按一下您想要重新啟動或重新整理的通道，以開啟該通道的 **Tunnel Info**（通道資訊）頁面。按一下清單中的其中一個項目，然後按一下：

- 重新啟動—重新啟動所選的通道。重新啟動會中斷通過通道的流量。
- 重新整理—顯示目前的 IPSec SA 狀態。

© 2019 Palo Alto Networks, Inc.

網路 > GRE 通道

一般路由封裝 (GRE) 通道通訊協定是封裝有效負載通訊協定的裝置電信業者通訊協定。GRE 封包本身封裝在傳輸通訊協定（IPv4 或 IPv6）中。GRE 通道連接防火牆和路由器（或另一個防火牆）之間的點對點邏輯連結中的兩個端點。Palo Alto Networks 防火牆支援終止 GRE 通道。

您想了解什麼內容？	請參閱：
GRE 通道的建置組塊	GRE 通道
如何提供與其他廠商的通道端點的互通性	建立 IPSec 通道時，選取 **Add GRE Encapsulation**（新增 **GRE** 封裝）。
想知道更多？	GRE 通道

GRE 通道

- 網路 > GRE 通道

首先設定通道介面（Network > Interfaces > Tunnel（網路 > 介面 > 通道））。然後新增 Generic Routing Encapsulation (GRE) 通道並提供以下資訊，參照您建立的通道介面：

GRE 通道欄位	說明
名稱	GRE 通道的名稱。
介面	選取要用作本機 GRE 通道端點的介面（來源介面），其為乙太網路介面或子介面、彙總乙太網路 (AE) 介面、回送介面或 VLAN 介面。
本機位址	選取介面的本機 IP 位址以用作通道介面位址。
對等位址	輸入 GRE 通道另一端的 IP 位址。
隧道接口	選取您設定的通道介面。（此介面會在通道為路由下一個躍點時對其進行識別。）
TTL	輸入封裝在 GRE 封包內之 IP 封包的 TTL（範圍為 1 到 255；預設值 64）。
複製 ToS 標頭	選取以將服務類型 (ToS) 欄位從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 ToS 資訊。
保持運作	選取以對 GRE 通道啟用保持運作功能（預設為停用）。若啟用保持運作，依預設，GRE 通道每隔 10 秒需要三個未返回的 keepalive 封包（重試）才能得以關閉，並且 GRE 通道每隔 10 秒需要 5 個保留計時器間隔才能得以恢復。

© 2019 Palo Alto Networks, Inc.

GRE 通道欄位	說明
間隔（秒）	設定 GRE 通道本端傳送 keepalive 封包給通道對等之間的時間間隔，以及 keepalive 封包成功傳送後防火牆重新建立與通道對等的通訊前每個保留計時器等待的時間間隔（範圍為 1 至 50；預設值為 10）。
重試	設定在防火牆認為通道對等關閉之前，未返回 keepalive 封包的時間間隔數（範圍為 1 至 255，預設值為 3）。
保留計時器	設定在防火牆重新建立與通道對等的通訊之前，已成功傳送 keepalive 封包的時間間隔數（範圍為 1 至 64，預設值為 5）。

© 2019 Palo Alto Networks, Inc.

Network > DHCP（網路 > DHCP）

動態主機組態通訊協定 (DHCP) 是標準化通訊協定，可提供 TCP/IP 與連結層組態參數，並提供網路位址，以便在 TCP/IP 網路上動態設定主機。Palo Alto Networks 防火牆上的介面可作為 DHCP 伺服器、用戶端或轉送代理程式。將這些角色指派給不同的介面，可讓防火牆執行多個角色。

您想了解什麼內容？	請參閱：
什麼是 DHCP？	DHCP 概要
DHCP 伺服器如何配置位址？	DHCP 定址
在防火牆上設定介面以作為：	
	DHCP 伺服器
	DHCP 轉送
	Network > DNS Proxy（網路 > DNS Proxy）
想知道更多？	DHCP

DHCP 概要

- Network > DHCP（網路 > DHCP）

DHCP 使用通訊的用戶端-伺服器模型。此模型包含三個防火牆可履行的角色：DHCP 用戶端、DHCP 伺服器，以及 DHCP 轉送代理程式。

- 作為 DHCP 用戶端（主機）的防火牆可向 DHCP 伺服器要求 IP 位址與其他組態設定。用戶端防火牆上的使用者可省下設定的時間與工作，而且不需要知道網路的定址計劃或其他網路資源，也不必知道從 DHCP 伺服器繼承的選項。
- 作為 DHCP 伺服器的防火牆可服務用戶端。透過使用其中一個 DHCP 定址機制，網路管理員能省下設定時間，並能在用戶端不再需要網路連線時重複使用有限數量的 IP 位址。伺服器會將 IP 定址與 DHCP 選項提供給許多用戶端。
- 作為 DHCP 轉送代理程式的防火牆會接聽廣播與單點傳送 DHCP 訊息，並在 DHCP 用戶端與伺服器之間進行轉送訊息。

DHCP 使用使用者資料包通訊協定 (UDP) RFC 768 作為其傳輸通訊協定。用戶端傳送到伺服器的 DHCP 訊息，會傳送到知名的連接埠 67 (UDP—啟動程序通訊協定與 DHCP)。伺服器傳送到用戶端的 DHCP 訊息，會傳送到連接埠 68。

DHCP 定址

DHCP 伺服器將 IP 位址指派或傳送給用戶端的方法有三種：

- 自動配置—DHCP 伺服器從其 **IP Pools**（**IP** 集區）將永久的 IP 位址指派給用戶端。防火牆上的 **Lease**（租期）若指定為 **Unlimited**（無限制），則表示配置為永久的。
- 動態配置—DHCP 伺服器將位址的 **IP Pools**（IP 配發範圍）中可重複使用的 IP 位址指派給用戶端，可使用達所謂租期的時間長度上限。這種位址配置方法對於 IP 位址數目有限的客戶而言很有用；IP 位址會指派給只需要暫時存取網路的用戶端。

© 2019 Palo Alto Networks, Inc.

- 靜態配置 — 網路管理員選擇要指派給用戶端的 IP 位址，DHCP 伺服器會將該位址傳送給用戶端。靜態 DHCP 配置是永久的，做法是設定 DHCP 伺服器，然後選擇 **Reserved Address**（保留的位址）以對應至用戶端防火牆的 **MAC Address**（**MAC** 位址）。即使用戶端中斷連線（登出、重新開機、電力中斷等），DHCP 指派仍維持有效。

  靜態配置 IP 位址很有用，舉例來說，當您的 LAN 上有印表機，但您不想要讓它的 IP 位址不斷改變，因為 IP 位址已透過 DNS 與印表機名稱產生關聯時，就很有幫助。另一個例子就是如果用戶端防火牆有關鍵用途，即使是防火牆關閉、未插電、重新開機或電力中斷下，都必須保持相同的 IP 位址時。

  設定 **Reserved Address**（保留的位址）時，請記住以下重點：

  - 其為 **IP Pools**（**IP** 集區範圍）中的位址。您可以設定多個保留的位址。
  - 如果您未設定 **Reserved Address**（保留的位址)，當用戶端租期到期或重新開機等等時，伺服器的用戶端會收到從配發範圍中新指派的 DHCP （除非您將 **Lease**（租期）指定為 **Unlimited**（無限制））。
  - 如果您將 **IP Pools**（IP 集區範圍）中的所有位置配置為 **Reserved Address**（保留的位址），則會沒有可用的動態位址可指派給下一個要求位址的 DHCP 用戶端。
  - 您可以在未設定 **MAC Address**（**MAC** 位址）的情況下設定 **Reserved Address**（保留的位址）。在此狀況下，DHCP 伺服器不會將 **Reserved Address**（保留的位址）指派給任何防火牆。舉例來說，您可以保留集區中的一些位址，將它們靜態地指派給不使用 DHCP 的傳真機與印表機。

DHCP 伺服器

- 網路 > DHCP > DHCP 伺服器

下節說明 DHCP 伺服器的每個元件。設定 DHCP 伺服器前，您應已設定好 Layer 3 Ethernet 或 Layer 3 VLAN 介面，並已指派給虛擬路由器與區域。您也應知道您網路計劃中 IP 位址的有效配發範圍，這些位址可指定為由 DHCP 伺服器指派給用戶端。

新增 DHCP 伺服器時，請依照下表所述進行設定。

DHCP 伺服器設定	設定位置	說明
介面	**DHCP** 伺服器	將作為 DHCP 伺服器的介面名稱。
模式		選取 **Enabled**（已啟用）或 **Auto**（自動）模式。**Auto**（自動）模式會啟用伺服器，如果在網路上偵測到另一個 DHCP 伺服器，便會將伺服器停用。**Disabled**（已停用）設定會停用伺服器。
配置新 IP 時 Ping IP	**DHCP Server**（**DHCP** 服務器） > **Lease**（租用）	如果您按一下 **Ping IP when allocating new IP**（配置新 **IP** 時 **Ping IP**），則伺服器將 IP 位址指派給其用戶端前會先 ping 該位址。如果 ping 收到回應，則表示已有其他防火牆擁有該位址，因此無法指派它。伺服器會改從集區中指派下一個位址。如果您選取此選項，顯示畫面中的 [探查 IP] 欄會有勾號。
租用		指定租用類型。 • 無限制會讓伺服器從 IP 集區範圍中動態選擇 IP 位址，並永久指派給用戶端。 • **Timeout**（逾時）決定租期會持續多久的時間。輸入 **Days**（日數）與 **Hours**（小時）數，並選擇性地輸入 **Minutes**（分鐘）數。

© 2019 Palo Alto Networks, Inc.

DHCP 伺服器設定	設定位置	說明
IP 集區範圍		指定可設定狀態的 IP 位址配發範圍，DHCP 伺服器會從此範圍中選擇位址並指派給 DHCP 用戶端。 您可以輸入單一位址、位址/<遮罩長度>（例如 192.168.1.0/24），或位址範圍（例如 192.168.1.10-192.168.1.20）。
保留的位址		（選用）從您不想要 DHCP 伺服器動態指派的 IP 集區範圍中指定 IP 位址（格式 x.x.x.x）。 如果您也指定 **MAC Address**（**MAC** 位址）（格式為 xx:xx:xx:xx:xx:xx），則當防火牆透過 DHCP 要求 IP 時，系統會將 **Reserved Address**（保留的位址）指派給與該 MAC 位址相關聯的防火牆。
繼承來源	**DHCP** 伺服器 > **Options**（選項）	選取 **None**（無）（預設），或選取來源 DHCP 用戶端介面或 PPPoE 用戶端介面，將各種伺服器設定傳播至 DHCP 伺服器。如果您指定 **Inheritance Source**（繼承來源），請從下方選取一或多個您要從此來源 **inherited**（繼承）的選項。 指定繼承來源的優點，就是可快速地從來源 DHCP 用戶端的上游伺服器傳輸 DHCP 選項。如果繼承來源上的選項改變了，也會保持更新用戶端的選項。例如，如果繼承來源防火牆覆寫其 NTP 伺服器（已被視為 **Primary NTP**（主要 NTP）伺服器），則用戶端將自動繼承新位址作為其 **Primary NTP**（主要 NTP）伺服器。
檢查繼承狀態		如果您選取 **Inheritance Source**（繼承來源），則按一下 **Check inheritance source status**（檢查繼承來源狀態）可開啟動態 IP 介面狀態視窗，其中顯示從 DHCP 用戶端繼承的選項。
閘道	**DHCP** 伺服器 > **Options (cont)**選項（續）	指定網路閘道（防火牆上的介面）的 IP 位址，用於聯繫與此 DHCP 伺服器不在同一個 LAN 上的任何設備。
子網路遮罩		指定套用到 **IP** 集區範圍中位址的網路遮罩。
選項		針對下列欄位，請按一下下拉式清單，然後選取 **None**（無）或 **inherited**（繼承），或輸入遠端伺服器的 IP 位址，您的 DHCP 伺服器會將此位址傳送給用戶端以存取該服務。如果您選取 **inherited**（繼承），則 DHCP 伺服器會從指定為 **Inheritance Source**（繼承來源）的來源 DHCP 用戶端繼承值。 DHCP 伺服器會將這些設定傳送給其用戶端。 • 主要 **DNS**、次要 **DNS**—偏好與替代網域名稱系統 (DNS) 伺服器的 IP 位址。 • 主要 **WINS**、次要 **WINS** — 偏好與替代 Windows 網際網路名稱服務 (WINS) 伺服器的 IP 位址。 • 主要 **NIS**、次要 **NIS**—偏好與替代網路資訊服務 (NIS) 伺服器的 IP 位址。

© 2019 Palo Alto Networks, Inc.

DHCP 伺服器設定	設定位置	說明
		• 主要 **NTP**、次要 **NTP**—可用網路時間通訊協定 (NTP) 伺服器的 IP 位址。 • **POP3** 伺服器—郵局通訊協定版本 3 (POP3) 伺服器的 IP 位址。 • **SMTP** 伺服器—簡易郵件傳送通訊協定 (SMTP) 伺服器的 IP 位址。 • **DNS** 尾碼 — 當輸入了用戶端無法解析的不合格主機名稱時，讓用戶端在本機使用的尾碼。
自訂 DHCP 選項		按一下 **Add**（新增），然後輸入您想要 DHCP 伺服器傳送給用戶端的自訂選項 **Name**（名稱）。 輸入 **Option Code**（選項代碼）（範圍是 1-254）。 如果已輸入 **Option Code 43**（選項代碼 **43**），則會顯示 [廠商類別識別碼 (VCI)] 欄位。輸入比對準則，系統會將從用戶端的選項 60 傳入的 VCI 與此準則比對。防火牆會注意從用戶端的選項 60 傳入的 VCI，在自己的 DHCP 伺服器表中找到符合的 VCI，然後將對應的值傳回給選項 43 中的用戶端。VCI 比對準則是字串或十六進位的值。十六進位的值必須有 “0x” 的前置詞。 選取 **Inherited from DCHP server inheritance source**（從 **DHCP** 伺服器繼承來源繼承），讓伺服器從繼承來源繼承該選項代碼的值，而不是從您輸入的 **Option Value**（選項值）。 若不要使用此選項，您可以改為執行下列作業： **Option Type**（選項類型）：選取 **IP Address**（**IP** 位址）、**ASCII** 或 **Hexadecimal**（十六進位）以指定用於 [選項值] 的資料類型。 對於 **Option Value**（選項值），按一下 **Add**（新增）並輸入自訂選項的值。

DHCP 轉送

- Network > DHCP > DHCP Relay（網路 > DHCP > DHCP 轉送）

將防火牆介面設定為 DHCP 中繼代理前，請確定您已設定第三層乙太網路或第三層 VLAN 介面，且該介面已指派給虛擬路由器與區域。您想要讓該介面能夠在用戶端與伺服器之間傳遞 DHCP 訊息。每個介面最多可將訊息轉送至八個外部 IPv4 DHCP 伺服器和八個 IPv6 DHCP 伺服器。用戶端 DHCPDISCOVER 訊息會傳送給所有已設定的伺服器，並將第一個回應的伺服器的 DHCPOFFER 訊息轉送回要求的用戶端。

DHCP 轉送設定	說明
介面	將作為 DHCP 轉送代理程式的介面名稱。
IPv4/IPv6	選取您指定的 DHCP 伺服器和 IP 位址類型。
DNS 伺服器 ip 位址	輸入您要將 DHCP 訊息轉進與轉出的 DHCP 伺服器 IP 位址。

© 2019 Palo Alto Networks, Inc.

DHCP 轉送設定	說明
介面	如果您選取 IPv6 作為 DHCP 伺服器的 IP 位址通訊協定，並指定多點傳送位址，則也必須指定傳出介面。

DHCP 用戶端

- Network > Interfaces > Ethernet > IPv4（網路 > 介面 > Ethernet > IPv4）
- Network > Interfaces > VLAN > IPv4（網路 > 介面 > VLAN > IPv4）

將防火牆介面設定為 DHCP 用戶端前，請確定您已設定第三層乙太網路或第三層 VLAN 介面，且該介面已指派給虛擬路由器與區域。如果您必須使用 DHCP 來為您防火牆上的介面要求 IPv4 位址，請執行此工作。

DHCP 用戶端設定	說明
類型	選取 **DHCP Client**（**DHCP** 用戶端），然後 **Enable**（啟用），將介面設為 DHCP 用戶端。
自動建立指向伺服器所提供之預設閘道的預設路由	會讓防火牆建立到預設閘道的靜態路由，這在用戶端嘗試存取許多目的地，而這些目的地不需要在防火牆的路由表中維護路由時很有用。
預設路由度量標準	（選用）為防火牆與 DHCP 伺服器之間的路由輸入**Default Route Metric**（預設路由公制）（優先層級）。在選擇路由期間，數字愈小的路由其優先順序愈高。例如，會先使用公制為 10 的路由，再使用公制為 100 的路由（範圍是 1-65535；無預設值）。
顯示 DHCP 用戶端執行階段資訊	顯示接收自 DHCP 伺服器的所有設定，包括 DHCP 租用狀態、動態 IP 指派、子網路遮罩、閘道和伺服器設定（DNS、NTP、網域、WINS、NIS、POP3 和 SMTP）。

© 2019 Palo Alto Networks, Inc.

Network > DNS Proxy（網路 > DNS Proxy）

DNS 伺服器執行以 IP 位址解析網域名稱（或反向解析）的服務。當您將防火牆設為 DNS Proxy 時，它會作為用戶端與伺服器之間的中介，並會作為 DNS 伺服器以解決來自其 DNS 快取的查詢或將查詢轉送至其他 DNS 伺服器。使用此頁面可進行設定，以決定防火牆要如何作為 DNS Proxy。

您想了解什麼內容？	請參閱：
防火牆 Proxy DNS 如何要求？	DNS Proxy 概要
如何設定 DNS Proxy？	DNS Proxy 設定
如何設定靜態 FQDN 對 IP 位址對應？	
如何管理 DNS Proxy？	其他 DNS Proxy 動作
想知道更多？	DNS

DNS Proxy 概要

您可以設定防火牆作為 DNS 伺服器。首先，建立 DNS 代理程式 並選取 代理程式 所套用的介面。接著，指定防火牆在其 DNS 代理程式 快取中找不到網域名稱時（以及當網域名稱不符合 代理程式 規則時），傳送 DNS 查詢的預設 DNS 主要與次要伺服器。

若要根據網域名稱將 DNS 查詢導向至不同的 DNS 伺服器，請建立 DNS 代理程式 規則。指定多個 DNS 伺服器可確保將 DNS 查詢本地語言化，並能提升效率。例如，您可以將所有的企業 DNS 查詢轉送到企業 DNS 伺服器，並將所有其他的查詢轉送到 ISP DNS 伺服器。

使用下列頁籤來定義 DNS 代理程式（超出預設的 DNS 主要與次要伺服器）：

- 靜態項目—允許您設定防火牆快取並傳送至主機以回應 DNS 查詢的靜態 FQDN 對 IP 位址對應。
- **DNS** 代理程式 規則—允許您指定網域名稱和對應的主要與次要 DNS 伺服器，來解析符合規則的查詢。如果網域名稱不在 DNS 代理程式 快取中，防火牆會在 DNS 代理程式（在查詢到達的介面上）中搜尋相符項目，並根據相符結果將查詢轉送至 DNS 伺服器。如果沒有相符結果，防火牆會將查詢傳送至預設的 DNS 主要與次要伺服器。您可以啟用符合規則之網域的快取。
- **Advanced**（進階）—如果會使用 DNS proxy 物件來解析防火牆產生的 DNS/FQDN 查詢，則必須啟用快取（選取 **Cache**（快取））和 **Cache EDNS Responses**（快取 **EDNS** 回應）。Advanced（進階）頁籤允許您控制 TCP 查詢及 UDP 查詢重試。防火牆會透過設定的介面來傳送 TCP 或 UDP DNS 查詢。當 DNS 查詢回應對於單一 UDP 封包而言太長時，UDP 查詢會切換至 TCP。

DNS Proxy Settings（DNS Proxy 設定）

按一下 **Add**（新增）並設定防火牆作為 DNS Proxy。您可以在防火牆上設定最多 256 個 DNS Proxy。

DNS Proxy Settings（DNS Proxy 設定）	設定位置	說明
啟用	**DNS Proxy**	選取以啟用此 DNS Proxy。

© 2019 Palo Alto Networks, Inc.

DNS Proxy Settings（DNS Proxy 設定）	設定位置	說明
名稱		指定用來識別 DNS Proxy 物件的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置		指定 DNS Proxy 物件要套用到哪一個虛擬系統： • 共用：Proxy 會套用至所有虛擬系統。如果您選取 **Shared**（共用），則不會有 **Server Profile**（伺服器設定檔）欄位。反之，請輸入 **Primary**（主要）與 **Secondary**（次要）DNS 伺服器 IP 位址或位址物件。 • 選取虛擬系統可使用 DNS Proxy；您必須先設定虛擬系統。移至 **Device**（裝置）> **Virtual Systems**（虛擬系統），選取虛擬系統，然後選取 **DNS Proxy**。
繼承來源 （僅限共用位置）		選取要從中繼承預設 DNS 伺服器設定的來源。這通常用於防火牆的 WAN 介面由 DHCP 或 PPPoE 因應的分公司部署。
檢查繼承狀態 （僅限共用位置）		選取以查看目前指定給 DHCP 用戶端與 PPPoE 用戶端介面的伺服器設定。這些設定包括 DNS、WINS、NTP、POP3、SMTP 或 DNS 尾碼。
主要/次要 （僅限共用位置）		指定此防火牆（作為 DNS Proxy）傳送 DNS 查詢的預設主要與次要 DNS 伺服器的 IP 位址。如果找不到主要 DNS 伺服器，防火牆會使用次要 DNS 伺服器。
伺服器設定檔 （僅限虛擬系統位置）		選取或建立新的 DNS 伺服器設定檔。如果虛擬系統的位置指定為 [共用]，則不會顯示此欄位。
介面		**Add**（新增）介面以用作 DNS Proxy。您可以新增多個介面。若要從介面中移除 DNS Proxy，請選取子網路並將其 **Delete**（刪除）。 如果 DNS Proxy 僅用於服務路由功能，則不需要介面。如果您想要目的地服務路由設定來源 IP 位址，請使用目的地服務路由搭配沒有介面的 DNS Proxy。否則，DNS Proxy 會選取介面 IP 位址作為來源（當沒有設定 DNS 服務路由時）。
名稱	**DNS Proxy** > **DNS Proxy Rules**（規則）	必須有名稱，才能透過 CLI 參照與修改項目。
開啟由此對應解析之網域的快取		選取以快取此對應解析的網域。
域名		**Add**（新增）防火牆會比較傳入 FQDN 的一個或多個網域名稱。若 FQDN 符合規則中其中一個網域，防火牆會轉送查詢至為此 Proxy 指定的主要/次要 DNS 伺服器。若要從規則刪除網域名稱，請選取規則並按一下 **Delete**（刪除）。
DNS Server Profile（伺服器設定檔）		選取或新增 DNS 伺服器設定檔可定義虛擬系統的 DNS 設定，包含防火牆傳送網域名稱查詢的主要與次要 DNS 伺服器。

© 2019 Palo Alto Networks, Inc.

DNS Proxy Settings（DNS Proxy 設定）	設定位置	說明
（僅限共用位置）		
主要/次要 （僅限虛擬系統位置）		輸入防火牆傳送相符網域名稱查詢的主要與次要 DNS 伺服器的主機名稱或 IP 位址。
名稱	**DNS Proxy** > 靜態項目	輸入靜態項目的名稱。
FQDN		輸入要對應至位址欄位中定義之靜態 IP 位址的完全合格網域 (FQDN) 名稱。
位址		**Add**（新增）一個或多個對應至此網域的 IP 位址。防火牆會在其 DNS 回應中包含所有這些位置，用戶端則選取要使用哪個 IP 位址。若要刪除位址，請選取位址並按一下 **Delete**（刪除）。
TCP 查詢	**DNS Proxy** > **Advanced**（進階）	選取以使用 TCP 啟用 DNS 查詢。指定防火牆將支援之有關同時擱置 TCP DNS 要求數目上限（**Max Pending Requests**（最大擱置要求數））（範圍是 64 至 256，預設為 64）。
UDP 查詢重試次數	**DNS Proxy** > **Advanced**（進階）	指定 UDP 查詢重試的設定： • **Interval**（間隔）—若 DNS Proxy 未收到回應，則將傳送另一個要求所經過的時間（以秒為單位，範圍是 1 至 30；預設為 2）。 • **Attempts**（嘗試次數）—DNSP 要在其後嘗試下一個 DNS 伺服器的最多嘗試次數（不包括第一次）（範圍是 1 至 30，預設為 5）。
快取	**DNS Proxy** > **Advanced**（進階）	如果此 DNS Proxy 物件用於防火牆產生的查詢（即在 **Device**（裝置）> **Setup**（設定）> **Services**（服務）> **DNS** 下，或在 **Device**（裝置）> **Virtual Systems**（虛擬系統）下），且您選取虛擬系統和 **General**（一般）> **DNS Proxy**），則您必須啟用 **Cache**（快取）（預設情況下啟用）。然後指定以下項目： • 啟用 **TTL**—限制防火牆快取 Proxy 物件的 DNS 項目所需的時間長度。預設為停用 TTL。然後輸入 **Time to Live (sec)**（存留時間（秒））—所有 Proxy 物件的快取項目會加以移除，且新的 DNS 要求必須加以解析並再次快取所經過的秒數。範圍是 60 至 86,400。沒有預設 TTL；會保持項目直到防火牆的快取記憶體用完為止。 • **Cache EDNS Responses**（快取 **EDNS** 回應）—如果使用此 DNS proxy 物件來解析防火牆產生的查詢，則必須啟用 Cache Extension Mechanisms for DNS (EDNS) 回應。防火牆必須能夠快取 DNS 回應，FQDN 位址物件的查詢才能取得成功。

© 2019 Palo Alto Networks, Inc.

其他 DNS Proxy 動作

將防火牆設為 DNS 代理程式 後，您可以在 **Network**（網路） > **DNS** 代理程式 頁面上執行下列動作，以管理 DNS 代理程式設定：

- 修改 — 若要修改 DNS 代理程式，請按一下 DNS 代理程式 組態的名稱。
- 刪除 — 選取 DNS 代理程式 項目，然後按一下 **Delete**（刪除）可移除 DNS 代理程式 組態。
- 停用 — 若要停用 DNS 代理程式，請按一下 DNS 代理程式 項目的名稱，然後清除 **Enable**（啟用）選項。若要啟用已停用的 DNS 代理程式，請按一下 DNS 代理程式 項目的名稱，然後選取啟用。

© 2019 Palo Alto Networks, Inc.

Network > QoS（網路 > QoS）

下列主題說明服務品質 (QoS)。

您想了解什麼內容？	請參閱：
設定介面的頻寬限制，並強制執行離開介面之流量的 QoS。	QoS 介面設定
監控離開啟用 QoS 之介面的流量。	QoS 介面統計資料
想知道更多？	請參閱服務品質瞭解完整的 QoS 工作流程、概念及使用案例。
	選取 Policies > QoS（政策 > QoS）以將 QoS 等級指派給相符的流量，或選取 Network > Network Profiles > QoS（網路 > 網路設定檔 > QoS）以定義最多 8 個 QoS 等級的頻寬限制和優先順序。

QoS 介面設定

啟用介面上的 QoS 以設定介面頻寬限制，及/或啟用介面以強制 Egress 流量的 QoS。啟用 QoS 介面包括將 QoS 設定檔附加至介面。實體介面支援 QoS，視防火牆型號的不同，子介面與彙總乙太網路 (AE) 介面上也支援 QoS。請參閱 Palo Alto Networks 產品比較工具檢視您的防火牆型號支援的 QoS 功能。

首先，**Add**（新增）或修改 QoS 介面，然後進行下表所述的設定。

QoS 介面設定	設定位置	說明
介面名稱	**QoS** 介面 > 實體介面	選取要啟用哪一個防火牆介面上的 QoS。
Egress 最大值 (Mbps)		輸入流量透過此介面離開防火牆的最大吞吐量（以Mbps為單位）。其默認值為 0，它會指定防火牆流量上限（PAN-OS 7.1.16 和更高版本中為 60,000 Mbps；PAN-OS 7.1.15 和更早發行版中為 16,000 Mbps）。 雖然這不是必要的欄位，但建議您一律為 *QoS* 介面定義*Egress Max*（*Egress* 最大值）。
開啟此介面上的 QoS 功能		選取以啟用所選介面上的 QoS。
純文字 隧道接口	**QoS** 介面 > 實體介面 > **Default Profile**（預設設定檔）	針對明碼與通道流量選取預設 QoS 設定檔。您必須為每一項指定預設設定檔。針對明碼流量，預設設定檔會以聚集的方式套用於所有明碼流量。針對通道流量，預設設定檔會個別套用於在詳細設定部分中沒有指定特定設定檔的每一個通道。如需定義 QoS 設定檔的指示，請參考 [網路 > 網路設定檔 > QoS]。
隧道接口		
Egress 保證值 (Mbps)	**QoS Interface**（**QoS** 介面）> **Clear Text Traffic/**	輸入此介面中保證用於純文字或通道流量的頻寬。

© 2019 Palo Alto Networks, Inc.

QoS 介面設定	設定位置	說明
Egress 最大值 (Mbps)	**Tunneled Traffic**（純文字流量/通道流量）	輸入純文字或通道流量透過此介面離開防火牆的最大吞吐量（以Mbps為單位）。其默認值為 0，它會指定防火牆流量上限（PAN-OS 7.1.16 和更高版本中為 60,000 Mbps；PAN-OS 7.1.15 和更早發行版中為 16,000 Mbps）。純文字或通道流量的 **Egress** 最大值必須小於或等於實體介面的 **Egress** 最大值。

新增		• 按一下 **Clear Text Traffic**（純文字流量）頁籤的 **Add**（新增），定義純文字流量處理的其他細微性。按一下個別項目進行下列設定：
		  • 名稱 — 輸入用來識別這些設定的名稱。
		  • **QoS** 設定檔 — 選取要套用至指定介面與子網路的 QoS 設定檔。如需定義 QoS 設定檔的指示，請參考 [網路 > 網路設定檔 > QoS]。
		  • 來源介面 — 選取防火牆介面。
		  • 來源子網路 — 選取子網路以將設定限制於來自該來源的流量，或保持預設值 **Any**（任何）以將設定套用於來自指定介面的任何流量。
		• 按一下 **Tunneled Traffic**（通道流量）頁籤的 **Add**（新增），覆寫特定通道的預設設定檔指派，並且進行下列設定：
		  • 通道介面 — 選取防火牆的通道介面。
		  • **QoS** 設定檔 — 選取要套用至指定通道介面的 QoS 設定檔。
		例如，假設有兩個站台的設定，其中之一有 45 Mbps 的連線連至防火牆，另一個有 T1 的連線連至防火牆。您可以對 T1 站台套用受限的 QoS 設定，使連線不至於多載，同時還可以針對具有 45 Mbps 連線的站台允許更有彈性的設定。
		若要移除純文字或通道流量項目，請清除項目並按一下 **Delete**（刪除）。
		如果留空純文字或通道流量區段，則使用 [實體介面] 頁籤的 [預設設定檔] 區段中指定的值。

QoS 介面統計資料

- 網路 > QoS > 統計資料

對於 QoS 介面，選取 **Statistics**（統計資料）可檢視所設定 QoS 介面的頻寬、工作階段及應用程式資訊。

QoS 統計資料	說明
頻寬	顯示所選節點與等級的即時頻寬圖表。此資訊每兩秒鐘更新一次。 在*QoS* 統計資料畫面中，為 *QoS* 等級設定的 *QoS* 輸出最大和輸出保證值限制可能有些微不同。這是正常的行為，並且是硬體引擎摘要頻寬限制和計數器的方式所造成。沒有操作方面的問題，因為頻寬使用圖會顯示即時值和數量。
應用程式	列出所選 QoS 節點及/或等級的所有使用中應用程式。

© 2019 Palo Alto Networks, Inc.

QoS 統計資料	說明
來源使用者	列出所選 QoS 節點及/或等級的所有使用中來源使用者。
目的地使用者	列出所選 QoS 節點及/或等級的所有使用中目的地使用者。
安全性規則	列出符合並強制執行所選 QoS 節點和/或等級的安全性規則。
QoS 規則	列出符合並強制執行所選 QoS 節點和/或等級的 QoS 規則。

© 2019 Palo Alto Networks, Inc.

Network > LLDP（網路 > LLDP）

連結層發現協定 (LLDP) 提供可在連結層自動發現相鄰設備及其功能的方法。

您想了解什麼內容？	請參閱：
什麼是 LLDP？	LLDP 概要
設定 LLDP。	LLDP 的建置組塊
設定 LLDP 設定檔。	Network > Network Profiles > LLDP Profile（網路 > 網路設定檔 > LLDP 設定檔）
想知道更多？	LLDP

LLDP 概要

LLDP 允許防火牆與芳鄰之間傳送與接收包含 LLDP 資料單位 (LLDPDU) 的乙太網路框架。接收設備會將資訊儲存在簡易網路管理通訊協定 (SNMP) 可存取的 MIB 中。LLDP 可讓網路設備對應其網路拓撲，並了解所連線設備的功能，從而讓疑難排解變得簡單，對於網路拓撲一般不會偵測到防火牆的虛擬介接部署來說更是如此。

LLDP 的建置組塊

若要啟用防火牆上的 LLDP，請按一下 [編輯]，按一下 **Enable**（啟用），若預設設定不符合您的環境，再選擇性地設定下表中顯示的 4 個設定。其他的表格項目可說明狀態與端點統計資料。

LLDP 設定	設定位置	說明
傳輸間隔（秒）	**LLDP** 一般	指定將於一定間隔傳輸 LLDPDU 的秒數（範圍是 1-3,600，預設為 30）。
傳輸延遲（秒）		指定在變更類型-長度-值 (TLV) 元素後 LLDP 傳輸之間延遲的時間（秒）。如果許多網路變更讓 LLDP 變更數達到高點，或是介面擺動，則延遲可幫助防止 LLDPDU 灌爆區段。**Transmit Delay**（傳輸延遲）必須小於 **Transmit Interval**（傳輸間隔）（範圍是 1-600，預設為 2）。
保持時間多重		指定要乘以 **Transmit Interval**（傳輸間隔）的值，以決定總 TTL 保留時間（範圍是 1-100，預設值為 4）。 TTL 保留時間是防火牆會將端點資訊保持有效的時間長度。無論乘數值為何，TTL 保留時間上限為 65,535 秒。
通知間隔		指定當 MIB 變更時傳輸 Syslog 與 SNMP 設陷通知的間隔秒數（範圍是 1-3,600，預設為 5）。

© 2019 Palo Alto Networks, Inc.

LLDP 設定	設定位置	說明
望遠鏡篩選器	**LLDP** > **Status**（狀態）	選擇性地在篩選器列中輸入資料值，然後按一下灰色箭頭，這會造成只顯示包含該資料值的資料列。按一下紅色 X 可清除篩選器。
介面		已獲指派 LLDP 設定檔的介面名稱。
LLDP		LLDP 狀態：啟用或停用。
模式		介面的 LLDP 模式：Tx/Rx、僅限 Tx 或僅限 Rx。
Profile		指派給介面的設定檔名稱。
傳輸總數		傳出介面的 LLDPDU 計數。
已丟棄傳輸		因為錯誤而未傳出介面的 LLDPDU 計數。例如，當系統正在建構 LLDPDU 進行傳輸時發生長度錯誤。
接收總數		介面上收到的 LLDP 框架計數。
已丟棄 TLV		接收時捨棄的 LLDP 框架計數。
錯誤		在介面上收到且包含錯誤的時間-長度-值 (TLV) 元素計數。TLV 錯誤類型包括：一或多個必要 TLV 遺失、順序紊亂、包含超出範圍的資訊，或發生長度錯誤。
無法辨識		在介面上收到 LLDP 本地代理程式無法辨識的 TLV 計數，例如因為 TLV 類型在所保留的 TLV 範圍內而無法辨識時。
逾時		因為適當的 TTL 到期而自「接收 MIB」刪除的項目計數。
清除 LLDP 統計資料		選取此選項，可清除所有 LLDP 統計資料。
望遠鏡篩選器	**LLDP** > **Peers**（端點）	選擇性地在篩選器列中輸入資料值，然後按一下灰色箭頭，這會造成只顯示包含該資料值的資料列。按一下紅色 X 可清除篩選器。
本地介面		偵測到相鄰設備的防火牆介面。
遠端底座 ID		端點的底座 ID；會使用 MAC 位址。
連接埠 ID	**LLDP** > **Peers**（端點）（續）	端點的連接埠 ID。
名稱		對等名稱。
更多資訊		按一下 **More Info**（更多資訊）可看到遠端端點詳細資訊，視 TLV 為必要與選用而定。
底座類型		底座類型為 MAC 位址。
MAC 位址		對等的 MAC 位址。

© 2019 Palo Alto Networks, Inc.

LLDP 設定	設定位置	說明
系統名稱		對等名稱。
系統說明		對等說明。
連接埠說明		對等的連接埠說明。
連接埠類型		介面名稱。
連接埠 ID		防火牆使用介面的 ifname。
系統功能		系統的功能。O=其他，P=重複器，B=橋接器，W=無線-LAN，R=路由器，T=電話
已啟用功能		對等上啟用的功能。
管理位址		對等的管理位址。

© 2019 Palo Alto Networks, Inc.

網路 > 網路設定檔

下列主題說明網路設定檔：

- Network > 網路設定檔> GlobalProtect IPSec 加密
- Network > Network Profiles > IKE Gateways (網路 > 網路設定檔 > IKE 閘道)
- Network > Network Profiles > IPSec Crypto（網路 > 網路設定檔 > IPSec 加密）
- Network > Network Profiles > IKE Crypto（網路 > 網路設定檔 > IKE 加密）
- Network > Network Profiles > Monitor（網路 > 網路設定檔 > 監控）
- Network > Network Profiles > Interface Mgmt（網路 > 網路設定檔 > 介面管理）
- Network > Network Profiles > Zone Protection（網路 > 網路設定檔 > 區域保護）
- 網路 > 網路設定檔 > QoS
- Network > Network Profiles > LLDP Profile（網路 > 網路設定檔 > LLDP 設定檔）
- Network > Network Profiles > BFD Profile（網路 > 網路設定檔 > BFD 設定檔）
- Network > Network Profiles > SD-WAN Interface Profile（網路 > 網路設定檔 > SD-WAN 介面設定檔）

Network > 網路設定檔> GlobalProtect IPSec 加密

使用 **GlobalProtect IPSec Crypto Profiles**（**GlobalProtect IPSec** 密碼設定檔）頁面可指定演算法，用於驗證與加密 GlobalProtect 閘道和用戶端之間的 VPN 通道。新增演算法的順序，即為防火牆套用演算法的順序，並會影響通道安全性與效能。若要變更順序，請選取算法，並按一下 **Move Up**（上移）或 **Move Down**（下移）。

如為 *GlobalProtect* 閘道與衛星（防火牆）之間的 *VPN* 通道，請參閱 *[網路 > 網路設定檔 > IPSec 密碼]*。

GlobalProtect IPSec 密碼設定檔設定	
名稱	輸入用來識別設定檔的名稱。名稱區分大小寫，必須是唯一的，最長可達 **31** 個字元。請僅使用字母、數字、空格、連字號與底線。
加密	按一下 **Add**（新增）並選取所需的加密演算法。若要獲得最高的安全性，請將順序（由上到下）變更為：**aes-256-gcm**、**aes-128-gcm**、**aes-128-cbc**。
驗證	按一下 **Add**（新增）並選取驗證演算法。目前唯一的選項為 **sha1**。

Network > Network Profiles > IKE Gateways (網路 > 網路設定檔 > IKE 閘道)

使用此頁面可管理或定義閘道，包括執行與端點閘道進行交涉的網際網路金鑰交換 (IKE) 通訊協定所需的設定資訊。這是 IKE/IPSec VPN 設定的階段 1 部分。

若要管理、設定、重新啟動或重新整理 IKE 閘道，請參閱下列下列項目：

- IKE 閘道管理
- IKE 閘道一般頁籤
- IKE 閘道進階選項頁籤
- IKE 閘道重新啟動或重新整理

© 2019 Palo Alto Networks, Inc.

IKE 閘道管理

- Network > Network Profiles > IKE Gateways（網路 > 網路設定檔 > IKE 閘道）

下表說明如何管理 IKE 閘道。

管理 IKE 閘道	說明
新增	若要建立新的 IKE 閘道，請按一下 **Add**（新增）。請參閱 IKE 閘道一般頁籤和 IKE 閘道進階選項頁籤，以取得如何設定新閘道的指示。
刪除	若要刪除閘道，請選取閘道並按一下 **Delete**（刪除）。
啟用	若要啟用已停用的閘道，請選取該閘道，然後按一下 **Enable**（啟用）（這是閘道的預設設定）。
停用	若要停用閘道，請選取閘道並按一下 **Disable**（停用）。
PDF/CSV	具有最小唯讀訪問權限的管理角色可以匯出如 **PDF/CSV** 的物件設定表。您可以在稽核等情況下套用篩選以建立更多特定表格組態匯出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。

IKE 閘道一般頁籤

- Network > Network Profiles > IKE Gateways > General（網路 > 網路設定檔 > IKE 閘道 > 一般）

下表說明 configure an IKE gateway（設定 IKE 閘道）的開始設定步驟。IKE 是 IKE/IPSec VPN 處理程序的階段 1。在設定這些設定之後，請參閱 IKE 閘道進階選項頁籤。

IKE 閘道一般設定	說明
名稱	輸入用來識別閘道的 **Name**（名稱）（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
版本	選取閘道所支援且必須同意搭配端點閘道使用的 IKE 版本：**IKEv1 only mode**（僅 **IKEv1** 模式）、**IKEv2 only mode**（僅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 偏好模式）。IKEv2 偏好模式會使閘道針對 IKEv2 進行交涉，而這正是在端點也支援 IKEv2 的情況下，他們會使用的；否則閘道將回復使用 IKEv1。
位址類型	選取閘道使用的 IP 位址類型。**IPv4** 或 **IPv6**。
介面	指定 VPN 通道的輸出防火牆閘道。
本機 IP 位址	針對做為通道端點的本機介面，選取或輸入 IP 位址。
Peer IP Address 類型	選取下列一項設定並輸入端點對應的資料： • **Dynamic**（動態）—如果端點 IP 位址或 FQDN 值為未知，則選取此選項。當端點 IP 位址類型為動態，則依靠端點啟動 IKE 閘道交涉。 • **IP**—輸入 **Peer Address**（端點位址）作為 IPv4 或 IPv6 位址，或作為 IPv4 或 IPv6 位址的位址物件。

© 2019 Palo Alto Networks, Inc.

IKE 閘道一般設定	說明
	• **FQDN**—輸入 **Peer Address**（端點位址）作為 FQDN 或使用 FQDN 的位址物件。 如果您輸入解析超過一個 IP 位址的 FQDN 或 FQDN 位址物件，則防火牆會選取下列來自符合 IKE 閘道的位址類型（IPv4 或 IPv6）位址組中的偏好位址： • 如果沒有任何交涉的 IKE 安全性關聯（SA），則偏好的位址為帶有最小值的 IP 位址。 • 如果位址由 IKE 閘道使用，且位在返回位址組內，則會使用此位址（不論它是否為最小值）。 • 如果位址由 IKE 閘道使用，但並不位在返回位址組內，則會選取新位址：在位址組內最小的位址。 使用 *FDQN* 或 *FQDN* 位址物件減少在環境中的問題，在該環境中端點會受制於動態 *IP* 位址變更（並因此需要您重新設定此 *IKE* 閘道端點位址）。
驗證	選取驗證類型：**Pre-Shared Key**（預先共用金鑰）或 **Certificate**（憑證）類型將伴隨端點閘道出現。請根據您所選取的類型來參閱預先共用金鑰欄位或憑證欄位。
預先共用金鑰欄位	
預先共用金鑰 / Confirm Pre-Shared Key	如果您選取 **Pre-Shared Key**（預先共用金鑰），請輸入用於在整個通道對稱驗證的單一安全性金鑰。此 **Pre-Shared Key**（預先共用金鑰）值為管理員使用 255 ASCII 或 non-ASCII 字元建立的字串。產生字典攻擊難以破解的金鑰；可視需要使用預先共用金鑰。
本機識別	定義本機閘道的格式與識別，來搭配預先共用金鑰使用，以建立 IKEv1 階段 1 SA 與 IKEv2 SA。 選取下列其中一個類型並輸入值：**FQDN**（主機名稱）、**IP** 位址、**KEYID**（十六進位的二進位格式 ID 字串）或使用者 **FQDN**（電子郵件地址）。 如果您不指定一個值，則閘道將使用本機 IP 位址作為 **Local Identification**（本機識別）值。
端點識別	定義端點閘道的類型與識別，以於建立 IKEv1 階段 1 SA 與 IKEv2 SA 期間搭配預先共用金鑰使用。 選取下列其中一個類型並輸入值：**FQDN**（主機名稱）、**IP** 位址、**KEYID**（十六進位的二進位格式 ID 字串）或使用者 **FQDN**（電子郵件地址）。 如果您不指定一個值，則閘道將使用此端點的 IP 位址作為 **Peer Identification**（端點識別）值。
憑證欄位	
本地憑證	如果選取 **Certificate**（憑證）做為 **Authentication**（驗證）類型，請從下拉式清單中選取防火牆上已有的憑證。 或者，您可以匯入憑證或產生新憑證，如下所示： **Import**（匯入）：

© 2019 Palo Alto Networks, Inc.

IKE 閘道一般設定	說明

	• **Certificate Name**（憑證名稱）—輸入正在匯入憑證的名稱。
	• **Shared**（共用）—如果要在多個虛擬系統之間共用此憑證，請按一下此選項。
	• **Certificate File**（憑證檔案）—按一下 **Browse**（瀏覽）按鈕以瀏覽至憑證檔案所在的位置。按一下檔案，然後選取 **Open**（開啟）。
	• **File Format**（檔案格式）—選取下列其中一項：
	  • **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—包含憑證，但不包含金鑰。純文字。
	  • **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—包含憑證與金鑰。
	• **Private key resides on Hardware Security Module**（私人金鑰位於硬體安全性模組）—如果防火牆是金鑰所在 HSM 伺服器的用戶端，請按一下此選項。
	• **Import Private Key**（匯入私密金鑰）—如果私密金鑰位於和憑證檔案不同的檔案中而需匯入時，請按一下此選項。
	  • **Block Private Key Export**（封鎖私密金鑰匯出）—選取 **Import Private Key**（匯入私密金鑰）後，可防止任何管理員（包括超級使用者）匯出私密金鑰。
	  • **Key File**（金鑰檔案）—瀏覽至要匯入的金鑰檔案。此項目適用於您選取 PEM 做為 [檔案格式]。
	  • 複雜密碼與確認複雜密碼 — 輸入以存取金鑰。

本地憑證（續）	**Generate**（產生）： • **Certificate Name**（憑證名稱）—輸入正在建立憑證的名稱。 • **Common Name**（通用名稱）—輸入通用名稱，這是顯示在憑證上的 IP 位址或 FQDN。 • **Shared**（共用）—如果要在多個虛擬系統之間共用此憑證，請按一下此選項。 • **Signed By**（簽署者）—選取外部授權單位 (CSR) 或輸入防火牆 IP 位址。此項目必須是 CA。 • **Certificate Authority**（憑證授權單位）—如果防火牆是根 CA，請按一下此選項。 • **Block Private Key Export**（封鎖私密金鑰匯出）—防止任何管理員（包括超級使用者）匯出私密金鑰。 • **OCSP** 回應程式—輸入 OCSP 以追蹤憑證是有效的或遭到撤銷。 • 演算法—選取 RSA 或 Elliptic Curve DSA，為憑證產生金鑰。 • 位元數—選取 512、1024、2048 或 3072 做為金鑰的位元數。 • 摘要 — 選取 md5、sha1、sha256、sha384 或 sha512 做為從雜湊轉換字串的方法。 • 到期（天數）—輸入憑證的有效天數。 • **Certificate Attribute**（憑證屬性）：類型—選取性地從下拉式清單中選取其他要放在憑證中的屬性類型。 • 值 — 輸入屬性值。
HTTP 憑證交換	按一下 **HTTP Certificate Exchange**（HTTP 憑證交換）並輸入**Certificate URL**（憑證 URL），以使用 Hash-and-URL 方法來告知端點要擷取憑證的地方。憑證 URL 是指儲存憑證的遠端伺服器 URL。

© 2019 Palo Alto Networks, Inc.

IKE 閘道一般設定	說明
	如果端點表示也支援 Hash 和 URL，則會透過交換 SHA1 Hash 與 URL 來交換憑證。 當端點收到 IKE 憑證承載時，它會看到 HTTP URL，並從該伺服器擷取憑證。然後端點將使用在憑證承載中指定的雜湊，來檢查從 HTTP 伺服器下載的憑證。
本機識別	識別如何在憑證中識別本機端點。選取下列其中一個類型並輸入值：辨別名稱（主旨）、**FQDN**（主機名稱）、**IP** 位址 或 使用者 **FQDN**（電子郵件地址）。
端點識別	識別如何在憑證中識別遠端端點。選取下列其中一個類型並輸入值：辨別名稱（主旨）、**FQDN**（主機名稱）、**IP** 位址 或 使用者 **FQDN**（電子郵件地址）。
對等 ID 檢查	選取精確或萬用字元。此設定會套用到正在檢查的端點識別，以驗證憑證。例如，如果端點識別為等同於 domain.com 的名稱，您選取 **Exact**（精確），且在 IKE ID 承載中的憑證名稱為 mail.domain2.com，則 IKE 交涉將失敗。但如果您選取 **Wildcard**（萬用字元），則僅在萬元字元星號（*）前名稱字串中的字元必須符合，在萬用字元後的任何字元可以不同。
允許對等識別與憑證裝載識別不符	如果您想要即使端點識別不符合憑證承載時，仍能有擁有成功 IKE SA 的彈性，請選取此選項。
憑證設定檔	選取設定檔，或建立新的 **Certificate Profile**（憑證設定檔）以設定憑證選項，這些選項會套用到本地閘道要傳送至端點閘道的憑證。請參閱 [裝置 > 憑證管理 > 憑證設定檔]。
啟用端點其擴充金鑰使用的嚴格驗證	若要嚴格控制使用金鑰的方式，請選取此選項。

IKE 閘道進階選項頁籤

- 網路 > 網路設定檔 > IKE 閘道 > 進階選項

設定進階的 IKE 閘道設定（例如被動模式、NAT 周遊）和 IKEv1 設定（例如無效端點偵測）。

IKE 閘道進階選項	說明
啟用 FTP 被動模式	按一下此選項可以使防火牆只回應 IKE 連線，且永不啟動這些連線。
啟用 NAT 周遊	按一下此選項可以讓 IKE 與 UDP 通訊協定使用 UDP 封裝，使得通訊協定能立即通過 NAT 裝置。 如果在 IPSec VPN 終止點之間的裝置上設定網路位址轉譯 (NAT)，則啟用 NAT 周遊。
IKEv1 頁籤	
交換模式	選取自動、加強或主要。在 **auto**（自動）模式（預設）中，裝置可接受 **main**（主要）模式與 **aggressive**（加強）模式交涉要求；但只要有可能，便會啟

© 2019 Palo Alto Networks, Inc.

IKE 閘道進階選項	說明
	動交涉並允許在 **main**（主要)模式中交換。您必須以相同的交換模式設定端點裝置，以讓它接受從第一個裝置啟動的交涉要求。
IKE 密碼設定檔	選取現有的設定檔、保留預設設定檔，或建立新的設定檔。可以為 IKEv1 與 IKEv2 選取不同的設定檔。 如需關於 IKE 加密設定檔的資訊，請參閱 [網路 > 網路設定檔 > IKE 加密]。
啟用分散	按一下此選項可允許本地閘道接收分散的 IKE 封包。分散封包大小上限為 576 位元組。
無效端點偵測	按一下以啟用，並輸入間隔（2 - 100 秒）與重新嘗試前的延遲時間（2 - 100 秒）。連線狀態偵測可識別非使用中或無法使用的 IKE 端點，並可以在端點無法使用時，協助還原遺失的資源。
IKEv2 Tab	
IKE 密碼設定檔	選取現有的設定檔、保留預設設定檔，或建立新的設定檔。可以為 IKEv1 與 IKEv2 選取不同的設定檔。 如需關於 IKE 加密設定檔的資訊，請參閱 [網路 > 網路設定檔 > IKE 加密]。
嚴格 Cookie 驗證	按一下可啟用 IKE 閘道的 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）。 • 啟用 **Strict Cookie Validation**（嚴格 Cookie 驗證）時，一律強制執行 IKEv2 Cookie 驗證；啟動者必須傳送包含 Cookie 的 IKE_SA_INIT。 • 啟用 **Strict Cookie Validation**（嚴格 **Cookie** 驗證）（預設設定）時，系統會對照為 VPN 工作階段設定的全域 **Cookie Activation Threshold**（**Cookie** 啟動臨界值），來檢查半開放 SA 的數目。如果半開放 SA 的數目超過 **Cookie Activation Threshold**（**Cookie** 啟動臨界值），啟動者必須傳送包含 Cookie 的 IKE_SA_INIT。
活性檢查	IKEv2 **Liveness Check**（活性檢查）一律開啟；所有的 IKEv2 封包皆提供活動檢查的用途。按一下此方塊可讓系統在端點已閒置指定的秒數後，傳送空白資訊封包。範圍：2-100。預設值：5。 若有需要，嘗試傳送 IKEv2 封包的一端會嘗試進行活性檢查達 10 次（所有的 IKEv2 封包皆會計入重新傳輸設定)。如果沒有回應，寄件者會關閉並刪除 IKE_SA 與 CHILD_SA。寄件者會寄出另一個 IKE_SA_INIT 重新開始。

IKE 閘道重新啟動或重新整理

- 網路 > IPSec 通道

選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道）可顯示通道狀態。第二個狀態欄中有 IKE 資訊的連結。按一下您想要重新啟動或重新整理的閘道。[IKE 資訊] 頁面隨即開啟。按一下清單中的其中一個項目，然後按一下：

- 重新啟動—重新啟動所選的閘道。重新啟動將中斷通過通道的流量。IKEv1 與 IKEv2 有不同的重新啟動行為，如下所述：
  - **IKEv1**—您可以個別重新啟動（清除）階段 1 SA 或階段 2 SA，只有該 SA 會受到影響。
  - **IKEv2**—讓 IKEv2 SA 重新啟動時會清除所有的子 SA（IPSec 通道）。

    如果您重新啟動 IKEv2 SA，則也會關閉所有基礎的 IPSec 通道。

© 2019 Palo Alto Networks, Inc.

如果您重新啟動與 IKEv2 SA 相關聯的 IPSec 通道（子 SA），重新啟動不會影響 IKEv2 SA。

- 重新整理—顯示目前的 IKE SA 狀態。

Network > Network Profiles > IPSec Crypto（網路 > 網路設定檔 > IPSec 加密）

選取 **Network**（網路）> **Network Profiles**（網路設定檔）> **IPSec Crypto**（**IPSec** 加密）以設定 IPSec 加密設定檔，其根據 IPSec SA 交涉（階段 2）指定 VPN 通道中的驗證與加密通訊協定與演算法。

如為 *GlobalProtect* 閘道與用戶端之間的 *VPN* 通道，請參閱 *[網路 > 網路設定檔> GlobalProtect IPSec 密碼]*。

IPSec 加密設定檔設定	說明
名稱	輸入用來識別設定檔的 **Name**（名稱）（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
IPSec 通訊協定	選取通訊協定以保護在 VPN 通道中周遊的資料： • **ESP**—Encapsulating Security Payload（封裝安全有效承載）通訊協定會將資料加密、驗證來源，及驗證資料完整性。 • **AH**—Authentication Header（驗證標頭）通訊協定會驗證來源並驗證資料完整性。 使用 *ESP* 通訊協定，因為它提供了連線機密性（加密）以及驗證。
加密（僅限 ESP 通訊協定）	按一下 **Add**（新增）並選取所需的加密演算法。若要獲得最高的安全性，請使用 **Move Up**（上移）和 **Move Down**（下移）將順序（從上到下）如下變更：**aes-256-gcm**、**aes-256-cbc**、**aes-192-cbc**、**aes-128-gcm**、**aes-128-ccm**（VM-Series 防火牆不支援此選項)、**aes-128-cbc**、**3des** 和 **des**。您也可以選取 **null**（無加密）。 使用 *AES* 加密的一個形式。（*DES* 和 *3DES* 是脆弱易受攻擊的演算法。）
驗證	按一下 **Add**（新增）並選取所需的驗證演算法。若要獲得最高的安全性，請使用 **Move Up**（上移）和 **Move Down**（下移）將順序（從上到下）如下變更：**sha512**、**sha384**、**sha256**、**sha1**、**md5**。如果 **IPSec Protocol**（IPSec 通訊協定）為 **ESP**，您也可以選取 **none**（無）（無驗證）。 使用 *sha256* 或更強的驗證，因為 *md5* 和 *sha1* 不安全。對於週期簡短的工作階段，使用 *sha256*，對於需要最高安全驗證（例如金融交易）的流量，使用 *sha384* 或更高版本。
DH 群組	為 Internet Key Exchange（IKE，網際網路金鑰交換）選取 Diffie-Hellman (DH) 群組：**group1**（群組 1）、**group2**（群組 2）、**group5**（群組 5）、**group14**（群組 14）、**group19**（群組 19）或 **group20**（群組 20）。若要獲得最高的安全性，請選取數字最高的群組。如果您不想要更新防火牆在

© 2019 Palo Alto Networks, Inc.

IPSec 加密設定檔設定	說明
	IKE 階段 1 期間建立的金鑰，請選取無 **pfs**（無 perfect forward secrecy）：防火牆會重複使用目前的金鑰來進行 IPSec 安全性關聯 (SA) 交涉。
SA 生命週期	選取單位，並輸入交涉金鑰保持有效的時間長度（預設值一小時）。
SA 生命週期	選取選用單位，並輸入金鑰可用於加密的的資料量。

Network > Network Profiles > IKE Crypto（網路 > 網路設定檔 > IKE 加密）

使用 **IKE Crypto Profiles**（**IKE** 密碼設定檔）頁面可指定用於識別、驗證與加密的通訊協定與演算法（IKEv1 或 IKEv2，階段 1）。

若要變更演算法或群組的列出順序，請選取項目，然後按一下 **Move Up**（上移）或 **Move Down**（下移）。順序可決定將設定與遠端端點進行交涉時的第一選取。會先嘗試清單頂端的設定，然後往下嘗試，直到嘗試成功為止。

IKE 加密設定檔設定	說明
名稱	輸入設定檔的名稱。
DH 群組	指定金鑰交換 (DH) 群組的優先順序。按一下 **Add**（新增）並選取群組：**group1**（群組 1）、**group2**（群組 2）、**group5**（群組 5）、**group14**（群組 14）、**group19**（群組 19）或 **group20**（群組 **20**）。若要獲得最高的安全性，請選取項目，然後按一下 **Move Up**（上移）或 **Move Down**（下移），將具有較高數值識別碼的群組移至清單頂端。例如，將 **group14**（群組 14）移到 **group2**（群組 2）上面。
驗證	指定雜湊演算法的優先順序。按一下 **Add**（新增）並選取演算法。若要獲得最高的安全性，請選取項目，然後按一下 **Move Up**（上移）或 **Move Down**（下移）將順序（從上到下）如下變更： • **sha512** • **sha384** • **sha256** • **sha1** • **md5** • （PAN-OS 10.0.3 和更高的 10.0 版本）無 如果您選取 *AES-GCM* 演算法用於加密，則必須選取驗證設定 *none*（無）。會基於所選的 *DH* 群組自動選取雜湊。*DH* 群組 *19* 和以下版本使用 *sha256*；*DH* 群組 *20* 使用 *sha384*。
加密	選取相應的封裝安全有效負載 (ESP) 驗證選項。按一下 **Add**（新增）並選取演算法。若要獲得最高的安全性，請選取項目，然後按一下 **Move Up**（上移）或 **Move Down**（下移）將順序（從上到下）如下變更： • （PAN-OS 10.0.3 和之後的 10.0 版本）**aes-256-gcm**（需要 IKEv2；DH 群組應設定為 **group20**）

© 2019 Palo Alto Networks, Inc.

IKE 加密設定檔設定	說明
	• （PAN-OS 10.0.3 和之後的 10.0 版本）**aes-128-gcm**（需要 IKEv2，且 DH 群組設定為 **group19**） • **aes-256-cbc** • **aes-192-cbc** • **aes-128-cbc** • **3des** • **des** *aes-256-gcm* 和 *aes-128-gcm* 演算法內建驗證；因此，在這種情況下，您必須將 *Authentication*（驗證）設定選取為 *none*（無）。
Kerberos 生命週期	選取時間單位，並輸入交涉的 IKE 階段 1金鑰有效的時間長度（預設為 8 小時）。 • IKEv2—金鑰生命週期到期時，必須重設 SA，否則到期時 SA 必須開始新的階段 1 金鑰交涉。 • IKEv1—到期前不會主動重設階段 1 金鑰。只有當 IKEv1 IPSec SA 到期時才會觸發重設 IKEv1 階段 1 金鑰。
IKEv2 驗證乘數	指定一個用來乘以金鑰生命週期的值（範圍是 0-50；預設為 0）以決定驗證計數。驗證計數是閘道可以執行重設 IKEv2 IKE SA 金鑰的次數，此次數後閘道必須從頭開始重新驗證 IKEv2。此值若為 0，則會停用重新驗證功能。

Network > Network Profiles > Monitor（網路 > 網路設定檔 > 監控）

監控設定檔用來針對以政策為基礎的轉送 (PBF) 規則監控 IPSec 通道，並監控下一個躍點設備。在這兩種情況下，監控設定檔皆可用來指定當資源（IPSec 通道或下一個躍點設備）變得無法使用時要採取的動作。監控設定檔是選用的，但是對於維持網站之間的連線相當有用，並且可確實維持 PBF 規則。下列設定可用來設定監視設定檔。

欄位	說明
名稱	輸入用來識別監控設定檔的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
動作	指定如果通道無法使用時所要採取的動作。如果失去了活動訊號的臨界值，防火牆會採取指定的動作。 • 等待復原—等待通道復原；不採取其他動作。封包將根據 PBF 規則持續傳送。 • 容錯移轉—如果其中一個路徑無法使用，流量將移轉至備份路徑。防火牆會使用路由表查詢決定此工作階段期間的路由。 在這兩種情況下，防火牆都會嘗試與新 IPSec 金鑰交涉以加快復原速度。
間隔	指定活動訊號之間的時間（範圍是 2 至 10；預設為 3）。

© 2019 Palo Alto Networks, Inc.

欄位	說明
閾值	指定在防火牆採取指定動作之前，要失去的活動訊號數（範圍是 2 至 10；預設為 5）。

Network > Network Profiles > Interface Mgmt（網路 > 網路設定檔 > 介面管理）

介面管理設定檔可保護防火牆，防止透過定義防火牆介面允許的服務和 IP 位址進行未經授權的存取。您可將介面管理設定檔指派給第三層乙太網路介面（包括子介面）及邏輯介面（彙總群組、VLAN、回送及通道介面）。若要指派介面管理設定檔，請參閱 [網路 > 介面]。

不要附加允許 *Telnet*、*SSH*、*HTTP* 或 *HTTPS* 至允許從網路或從其他在您企業安全性邊界內未受信任的區域存取介面的介面管理設定檔。這包含您已為 *GlobalProtect* 入口網站或閘道設定的介面；*GlobalProtect* 不需介面管理設定檔，即可啟用入口網站或閘道的存取。請參考保護管理存取的最佳實踐方法以了解如何保護您防火牆和 *Pandorama* 存取的詳細資料。

不要附加允許 *Telenet*、*SSH*、*HTTP* 至一個您已設定 *GlobalProtect* 入口網站或閘道介面上的介面管理設定檔，因為這將會讓管理介面暴露在網際網路中。

欄位	說明
名稱	輸入設定檔名稱（最多 **31** 個字元）。設定介面時，此名稱會顯示在介面管理設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
系統管理服務	• **Telnet** — 用於存取防火牆 CLI。Telnet 使用純文字，不如 SSH 安全。 啟用 *SSH* 而非 *Telnet* 來管理介面上的流量。 • **SSH** — 用於保障安全存取防火牆 CLI。 • **HTTP** — 用於存取防火牆 Web 介面。HTTP 使用純文字，不如 HTTP 安全。 請啟用 *HTTPS* 而非 *HTTP* 來管理介面上的流量。 • **HTTPS** — 用於保障安全存取防火牆 Web 介面。
網路服務	• **Ping** — 用於測試外部服務的連接性。例如，您可 ping 介面，驗證其可從 Palo Alto Networks 更新伺服器接收 PAN-OS 軟體及內容更新。 • **HTTP OCSP** — 用於設定防火牆作為線上憑證狀態通訊協定 (OCSP) 回應程式。如需詳細資訊，請參閱 [裝置 > 憑證管理 > OCSP 回應程式]。 • **SNMP** — 用於處理來自 SNMP 管理員的防火牆統計資料查詢。如需詳細資訊，請參閱啟用 SNMP 監控。 • 回應頁面—用於啟用以下各項的回應頁面： • **Authentication Portal**（驗證入口網站）—用於提供驗證入口網站回應頁面的連接埠會在第三層介面上保持開啟：連接埠 6080 用於 NTLM，6081 用於沒有 SSL/TLS 伺服器設定檔的驗證入口網站，而 6082 則用於有 SSL/TLS 伺服器設定檔的驗證入口網站。如需詳細資訊，請參閱 Device > User

© 2019 Palo Alto Networks, Inc.

欄位	說明
	Identification > Authentication Portal Settings（裝置 > 使用者識別 > 驗證入口網站設定）。 • **URL** 管理員覆寫—如需詳細資訊，請參閱 [設備 > 設定 > Content-ID]。 • **User-ID**—用於啟用使用者在防火牆間對應的重新散佈。 • **User-ID** 系統日誌接聽程式**-SSL** — 用於允許整合 PAN-OS 的 User-ID 代理程式透過 SSL 收集系統日誌訊息。如需詳細資訊，請參閱設定對監控伺服器的存取。 • **User-ID Syslog** 接聽程式**-UDP**—用於允許整合 PAN-OS 的 User-ID 代理程式透過 UDP 收集 Syslog 訊息。如需詳細資訊，請參閱設定對監控伺服器的存取。
許可的 IP 位址	輸入介面允許存取的 IPv4 或 IPv6 位址清單。

Network > Network Profiles > Zone Protection（網路 > 網路設定檔 > 區域保護）

套用到區域的區域保護設定檔可提供保護，以防大多數常見爆流、偵察攻擊、其他封裝型攻擊、使用非 IP 通訊協定，以及具有特定安全群組標記 (SGT) 的 802.1Q (Ethertype 0x8909) 之標頭。區域保護設定檔設計在進入區域（流量會進入防火牆的區域）上提供廣泛的保護，而非設計來保護進入特殊目的地區域的特定端點主機或流量。您可以將一個區域保護設定檔附加至某個區域。

為每個區域應用區域保護設定檔，為 *IP* 流量、偵察、其他封裝型攻擊和非 *IP* 通訊協定攻擊多增加一層保護。防火牆上的區域保護應該是在網路周邊的專用 *DDoS* 裝置之後的第二層保護。

若要增強防火牆上的區域保護功能，請設定 DoS 保護原則（原則 > DoS 保護）來比對特定的區域、介面、IP 位址或使用者。

沒有工作階段符合封裝時才會強制執行區域保護，因為區域保護是以每秒的新連線數 *(cps)* 為基礎，而不是以每秒的封裝數 *(pps)* 為基礎。如果封包符合現有的工作階段，它會略過區域保護設定。

您想了解什麼內容？	請參閱：
如何建立區域保護設定檔？	區域保護設定檔的建置組塊 Flood 攻擊保護 偵察保護 基於封包的攻擊保護 通訊協定保護 乙太網路 SGT 保護

區域保護設定檔的建置組塊

若要建立區域保護設定檔，請 **Add**（新增）設定檔並加以命名。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定	設定位置	說明
名稱	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）	輸入設定檔名稱（最多 31 個字元）。設定區域時，此名稱會出現在區域保護設定檔清單中。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格與底線。
說明		輸入區域保護設定檔的選用性說明。

接著，根據區域所需的保護類型，藉由設定任何設定組合來建立區域保護設定檔：

- Flood 攻擊保護
- 偵察保護
- 基於封包的攻擊保護
- 通訊協定保護
- 乙太網路 SGT 保護

如果您具有多重虛擬系統環境，並已啟用下列項目：

- 外部區域，用來啟用虛擬系統之間的通訊
- 共用閘道，可讓虛擬系統對外部通訊共享公用介面及單一 *IP* 位址

在外部區域，將停用下列區域和 *DoS* 保護機制：

- 同步處理 *Cookie*
- *IP* 分散
- *ICMPv6*

若要為共用閘道啟用 *IP* 分散和 *ICMPv6* 保護，必須為共用閘道建立個別的區域保護設定檔。

若要對抗共用閘道上的 *SYN* 流量，您可以使用 *[隨機早期丟棄]* 或 *SYN Cookie* 來套用 *SYN* 流量保護設定檔；在外部區域上，只能為 *SYN* 流量保護使用 *[隨機早期丟棄]*。

Flood 攻擊保護

- 網路 > 網路設定檔 > 區域保護 > 流量保護

設定一個設定檔，用以防範 SYN、ICMP、ICMPv6 、SCTP INIT 和 UDP 封包流量，以及防範來自其他類型的 IP 封包流量。每秒連線速率；例如，傳送的 SYN 封包不符合現有工作階段，則視為新的連線。

地區保護設定檔設定—流量保護	設定位置	說明
SYN	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（網路 > 網路設定檔 > 區域保護 > 流量保護）	選取此選項可防範 SYN 流量。

動作		選取回應 SYN flood 攻擊時採取的動作。
		• 隨機早期丟棄—丟棄 SYN 封包以減輕流量攻擊：
		  • 當流量超過 **Alert**（警示）速率臨界值時，會產生警報。
		  • 當流量超過 **Activate**（啟動）速率臨界值時，防火牆會隨機丟棄個別 SYN 封包以限制流量。
		  • 當流量超過 **Maximal**（最大）速率臨界值時，則會丟棄所有傳入 SYN 封包。

© 2019 Palo Alto Networks, Inc.

地區保護設定檔設定—流量保護	設定位置	說明
		• **SYN Cookie**—會讓防火牆的行為變得像 Proxy、攔截 SYN、代替要作為 SYN 導向目標的伺服器產生 Cookie，並將附有 Cookie 的 SYN-ACK 傳送至原始來源。防火牆在收到來源傳來附有 Cookie 的 ACK 後，才會將來源視為有效，並且會將 SYN 轉送給伺服器。這是偏好的動作。 *SYN Cookies 會公平地處理合法流量，但消耗的防火牆資源比 RED 多。如果 SYN Cookie 耗用太多資源，請切換到 RED。如果您在防火牆（在網路周邊）前沒有專用的 DDoS 預防裝置，請務必使用 RED。*
警報速率 (連線/秒)	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	輸入區域要在每秒收到多少 SYN 封包數目（與現有工作階段不相符）時觸發警報。您可以在儀表板上和威脅日誌（監控 > 封包擷取）中檢視警報。範圍為 0-2,000,000；預設值為 10,000。 最佳做法是將閾值設定為高於平均區域 CPS 速率 15-20% 以適應正常波動，並在收到過多警示時調整臨界值。
啟動 (連線數/秒)		輸入區域要在每秒收到多少 SYN 封包數目（與現有工作階段不相符）時觸發區域保護設定檔所指定的動作。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄 SYN 封包。範圍是 1 到 2,000,000；預設值為 10,000。 最佳做法是將臨界值設定為略高於區域的峰值 CPS 速率之上，以避免限制合法流量並根據需要調整臨界值。
最大 (連線數/秒)		輸入區域要在每秒收到多少 SYN 封包數目上限（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍是 1 到 2,000,000；預設值為 40,000。跨越此臨界值會封鎖新連線，直到 CPS 速率降到臨界值以下。 最佳做法是將臨界值設定在防火牆容量的 80-90%，同時將消耗防火牆資源的其他功能納入考慮。
ICMP	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	選取此選項可防範 ICMP 流量。
警報速率 (連線/秒)		輸入區域要在每秒收到多少 ICMP 回應要求數目（與現有工作階段不相符的偵測）時觸發攻擊警報。範圍為 0-2,000,000；預設值為 10,000。 最佳做法是將閾值設定為高於平均區域 CPS 速率 15-20% 以適應正常波動，並在收到過多警示時調整臨界值。
啟動 (連線數/秒)		輸入區域要在每秒收到多少 ICMP 封包數目（與現有工作階段不相符）後，才丟棄後續的 ICMP 封包。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄 ICMP 封包。範圍是 1 到 2,000,000；預設值為 10,000。

© 2019 Palo Alto Networks, Inc.

地區保護設定檔設定—流量保護	設定位置	說明
		最佳做法是將臨界值設定為略高於區域的峰值 CPS 速率之上，以避免限制合法流量並根據需要調整臨界值。
最大 (連線數/秒)		輸入區域要在每秒收到多少 ICMP 封包數目上限（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍是 1 到 2,000,000；預設值為 40,000。 最佳做法是將臨界值設定在防火牆容量的 80-90%，同時將消耗防火牆資源的其他功能納入考慮。
SCTP INIT	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	選取啟用包含初始（INIT）區段串流控制傳輸協定（SCTP）封包的保護。INIT 區段無法與其他區段同捆，因此封包被稱為 SCTP INIT 封包。
警報速率 (連線/秒)		輸入區域要在每秒收到多少 SCTP INIT 封包數目（與現有工作階段不相符）時觸發攻擊警報。範圍為 0-2,000,000。每防火牆型號預設值為： • **PA-5280**—10,000 • **PA-5260**—7,000 • **PA-5250**—5,000 • **PA-5220**—3,000 • **VM-700**—1,000 • **VM-500**—500 • **VM-300**—250 • **VM-100**—200 • **VM-50**—100
啟動 (連線數/秒)		輸入區域要在每秒收到多少 SCTP INIT 封包數目（與現有工作階段不相符）後，才丟棄後續的 SCTP INIT 封包。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄 SCTP INIT 封包。範圍為 1 到 2,000,000。每防火牆型號的預設值與警示速率相同。
最大 (連線數/秒)	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	輸入區域要在每秒收到多少 SCTP INIT 封包數目上限（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍為 1 到 2,000,000。每防火牆型號預設值為： • **PA-5280**—20,000 • **PA-5260**—14,000 • **PA-5250**—10,000 • **PA-5220**—6,000 • **VM-700**—2,000 • **VM-500**—1,000 • **VM-300**—500 • **VM-100**—400 • **VM-50**—200
UDP	**Network**（網路）> **Network Profiles**（網	選取此選項可防範 UDP 流量。

© 2019 Palo Alto Networks, Inc.

地區保護設定檔設定—流量保護	設定位置	說明
警報速率 (連線/秒)	路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	輸入區域要在每秒收到多少 UDP 封包數目（與現有工作階段不相符）時觸發攻擊警報。範圍為 0-2,000,000；預設值為 10,000。 最佳做法是將閾值設定為高於平均區域 CPS 速率 15-20% 以適應正常波動，並在收到過多警示時調整臨界值。
啟動 (連線數/秒)		輸入區域要在每秒收到多少 UDP 封包數目（與現有工作階段不相符）時觸發隨機丟棄 UDP 封包的動作。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄 UDP 封包。範圍是 1 到 2,000,000；預設值為 10,000。 最佳做法是將臨界值設定為略高於區域的峰值 CPS 速率之上，以避免限制合法流量並根據需要調整臨界值。
最大 (連線數/秒)		輸入區域要在每秒收到多少 UDP 封包數目上限（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍是 1 到 2,000,000；預設值為 40,000。 最佳做法是將臨界值設定在防火牆容量的 80-90%，同時將消耗防火牆資源的其他功能納入考慮。
ICMPv6	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Flood Protection**（流量保護）（續）	選取此選項可防範 ICMPv6 流量。
警報速率 (連線/秒)		輸入區域要在每秒收到多少 ICMPv6 回應要求數目（與現有工作階段不相符的偵測）時觸發攻擊警報。範圍為 0-2,000,000；預設值為 10,000。 最佳做法是將閾值設定為高於平均區域 CPS 速率 15-20% 以適應正常波動，並在收到過多警示時調整臨界值。
啟動 (連線數/秒)		輸入區域要在每秒收到多少 ICMPv6 封包數目（與現有工作階段不相符）後，才丟棄後續的 ICMPv6 封包。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄 ICMPv6 封包。範圍是 1 到 2,000,000；預設值為 10,000。 最佳做法是將臨界值設定為略高於區域的峰值 CPS 速率之上，以避免限制合法流量並根據需要調整臨界值。
最大 (連線數/秒)		輸入區域要在每秒收到多少 ICMPv6 封包數目上限（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍是 1 到 2,000,000；預設值為 40,000。 最佳做法是將臨界值設定在防火牆容量的 80-90%，同時將消耗防火牆資源的其他功能納入考慮。
其他 **IP**	**Network**（網路）> **Network Profiles**（網路設定）> **Zone**	選取此選項可防範其他 IP（非 TCP、非 ICMP、非 ICMPv6、非 SCTP INIT 和非 UDP）流量。

© 2019 Palo Alto Networks, Inc.

地區保護設定檔設定—流量保護	設定位置	說明
警報速率 (連線/秒)	**Protection**（區域保護）> **Flood Protection**（流量保護）（續）	輸入區域要在每秒收到多少其他 IP 封包（非 TCP、非 ICMP、非 ICMPv6 、非 SCTP INIT 和非 UDP 封包）（與現有工作階段不相符）時觸發攻擊警報。範圍為 0-2,000,000；預設值為 10,000。 最佳做法是將閾值設定為高於平均區域 CPS 速率 15-20% 以適應正常波動，並在收到過多警示時調整臨界值。
啟動 (連線數/秒)		輸入區域要在每秒收到多少其他 IP 封包（非 TCP、非 ICMP、非 ICMPv6 和非 UDP 封包）（與現有工作階段不相符）時觸發隨機丟棄其他 IP 封包的動作。防火牆會使用演算法，隨著攻擊速率的增加而丟棄越來越多的封包，直到攻擊速率達到最大速率為止。如果傳入速率下降到低於啟動臨界值，防火牆就會停止丟棄其他 IP 封包。範圍是 1 到 2,000,000；預設值為 10,000。 最佳做法是將臨界值設定為略高於區域的峰值 CPS 速率之上，以避免限制合法流量並根據需要調整臨界值。
最大 (連線數/秒)		輸入區域要在每秒收到多少其他 IP 封包數目上限（非 TCP、非 ICMP、非 ICMPv6 和非 UDP 封包）（與現有工作階段不相符）後，才丟棄超過上限的封包。範圍是 1 到 2,000,000；預設值為 40,000。 最佳做法是將臨界值設定在防火牆容量的 80-90%，同時將消耗防火牆資源的其他功能納入考慮。

偵察保護

- Network > Network Profiles > Zone Protection > Reconnaissance Protection（網路 > 網路設定檔 > 區域保護 > 偵察保護）

下列設定會定義偵察保護：

區域保護設定檔設定—偵察保護	設定位置	說明
TCP 連接埠掃描	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Reconnaissance Protection**（偵察保護）（網路 > 網路設定檔 > 區域保護 > 偵察保護）	**Enable**（啟用）設定設定檔以啟用 TCP 連接埠掃描保護。
UDP 連接埠掃描		**Enable**（啟用）設定設定檔以啟用 UDP 連接埠掃描保護。
主機掃描		**Enable**（啟用）設定設定檔以啟用主機掃描保護。
動作		系統回應相應偵察嘗試時將採取的動作： • **Allow**（允許）—允許連接埠掃描或主機掃描探測。 • **Alert**（警示）—在指定的時間間隔內，針對每個符合臨界值的連接埠掃描或主機掃描產生警示（預設動作）。 • **Block**（封鎖）—針對指定時間間隔的剩餘時間，丟棄來源與目的地之間所有後續封包。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—偵察保護	設定位置	說明
		• **Block IP**（封鎖 **IP**）—針對指定 **Duration**（持續時間）丟棄所有後續封包（以秒為單位，範圍是 1-3,600）。**Track By**（追蹤方式）可決定是否封鎖來源或來源及目的地流量。例如，每個時間間隔內來自單一來源高於上述臨界值的封鎖嘗試（更嚴格），或擁有來源及目的地對的封鎖嘗試（不太嚴格） 除了您的內部漏洞測試掃描外，封鎖所有偵測掃描。
間隔（秒）		TCP 或 UDP 連接埠掃描偵測的時間間隔（以秒為單位，範圍是 2-65,535；預設為 2）。 主機掃描偵測的時間間隔（以秒為單位，範圍是 2-65,535；預設為 10）。
臨界值 (事件)		指定時間間隔內觸發動作的連接埠事件掃描數或主機事件掃描數（範圍是 2-65,535；預設為 100）。 在封鎖偵察嘗試前，使用預設的事件閾值，以記錄一些用於分析的封包。
來源位址排除		您要從偵察保護中排除的 IP 位址。清單支援最多 20 個 IP 位址或網路遮罩位址物件。 • **Name**（名稱）—為要排除的位址輸入描述性名稱。 • **Address Type**（位址類型）—從下拉式清單中選取 IPv4 或 IPv6。 • **Address**（位址）—從下拉式清單中選取位址或位址物件，或手動輸入一個位址或位址物件。 僅排除執行漏洞測試的可信任內部群組的 *IP* 位址。

基於封包的攻擊保護

- Network > Network Profiles > Zone Protection > Packet Based Attack Protection（網路 > 網路設定檔 > 區域保護 > 基於封包的攻擊保護）

您可以設定以封包為基礎的攻擊保護，以丟棄下列封包類型：

- IP 丟棄
- TCP 丟棄
- ICMP 丟棄
- IPv6 丟棄
- ICMPv6 丟棄

IP 丟棄

若要指示防火牆對其從區域接收的某些 IP 封包執行哪些動作，請指定下列設定：

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
詐騙的 IP 位址	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack Protection**（基於封包的攻擊保護）> **IP Drop**（**IP** 丟棄）	檢查進入封包的來源 IP 位址是否可路由，以及路由介面是否在進入介面所在的同一個區域中。如果任一個條件不成立，會捨棄封包。 僅限在內部區域，丟棄 *Spoofed IP address (*冒名的 *IP* 位址*)* 封包以確保在輸入方面，來源位置與防火牆路由表符合。
嚴格 IP 位址檢查		檢查是否兩個條件均成立： • 來源 IP 位址不是進入介面的子網廣播 IP 位址。 • 來源 IP 位址可透過確切的進入介面路由。 如果任一個條件不成立，會捨棄封包。 對於採用通用準則 (CC) 模式的防火牆，您可啟用登入捨棄封包。在防火牆 Web 介面上，選取 **Device**（裝置）> **Log Settings**（日誌設定）。在管理日誌區段，選取 **Selective Audit**（選取性稽核）並啟用 **Packet Drop Logging**（封包丟棄日誌記錄）。
封鎖分段的流量		捨棄分段 IP 封包。
IP 選項丟棄		選取此群組中的設定可讓防火牆丟棄包含這些 IP 選項的封包。
嚴格的來源路由		丟棄已設定 [嚴格來源路由 IP] 選項的封包。資料包來源可憑借嚴格的來源路由選項來提供閘道或主機在傳送資料包時所必須透過的路由資訊。 丟棄具有嚴格來源路由的封包，因為來源路由允許對手繞過使用目的地 *IP* 位址做為比對準則的安全性原則規則。
鬆散來源路由		丟棄已設定 [鬆散來源路由 IP] 選項的封包。資料包來源可憑借鬆散來源路由選項來提供路由資訊，而且閘道或主機可以選取許多中繼閘道的任何路由，將資料包放到路由的下一個位址。 丟棄具有鬆散來源路由的封包，因為來源路由允許對手繞過使用目的地 *IP* 位址做為比對準則的安全性原則規則。
時間戳記		丟棄已設定 Timestamp IP 選項的封包。
記錄路由		丟棄已設定 Record Route IP 選項的封包。當資料包啟用此選項時，路由傳送資料包的每個路由器都會在標頭中新增它自己的 IP 位址，進而對收件者提供路徑。
security		如果定義安全性選項，丟棄封包。
串流 ID		如果定義串流 ID 選項，丟棄封包。
未知		如果類別及號碼不明，丟棄封包。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
		捨棄未知封包。
格式錯誤的		如果按照 RFC 791、1108、1393 及 2113 的類別、號碼及長度三者的組合不正確，則捨棄封包。 捨棄格式錯誤的封包。

TCP 丟棄

若要指示防火牆對其從區域接收的某些 TCP 封包執行哪些動作，請指定下列設定。

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
不相符的重疊 TCP 區段	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack Protection**（基於封包的攻擊保護）> **TCP Drop**（**TCP** 丟棄）	攻擊者可以建構重疊但資料不同的連線，嘗試造成對連線的錯誤解讀。攻擊者會使用 IP 詐騙與序號預測方法來攔截使用者連線，並插入自己的資料。在下列案例中，當區段資料不符時，使用此設定以回報重疊不符合並丟棄封包： • 此區段位於其他區段中。 • 此區段與其他區段部分重疊。 • 此區段涵蓋其他區段。 此保護機制使用序號來判斷封包在 TCP 資料流中的位置。 丟棄不相符重疊 *TCP* 片段的封包。
分割交握		當工作階段建立程序不使用眾所周知的三方交握時，防止建立 TCP 工作階段。舉例來說，四方或五方分割交握，或同時開放工作階段建立程序，都是不允許的變化。 Palo Alto Networks 新一代的防火牆能針對分割交握與同時開放工作階段建立，正確地處理工作階段與所有的第七層檢驗處理程序，但不設定 **Split Handshake**（分割交握）。當針對區域保護設定檔進行此設定，且設定檔套用到區域時，必須使用標準的三方交握來為該區域的介面建立 TCP 工作階段；不允許有變化。 丟棄含有分割交握的封包。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
含資料的 TCP SYN		若 TCP SYN 封包包含三方交握期間的資料，則防止建立 TCP 工作階段。預設會啟用。
含資料的 TCP SYNACK		若 TCP SYN ACK 封包包含三方交握期間的資料，則防止建立 TCP 工作階段。預設會啟用。
拒絕非 SYN TCP		決定如果 TCP 工作階段設定的第一個封包不是 SYN 封包時，是否拒絕封包： • **global**（全域）—使用透過 **TCP Settings**（**TCP** 設定）或 CLI 指派的系統全域設定。 • **yes**（是）—拒絕非 SYN TCP。 • **no**（否）—接受非 SYN TCP。 在發生封鎖後未設定用戶端和/或伺服器連線的情況下，允許非 *SYN TCP* 流量可能會讓檔案封鎖原則無法如預期般工作。 如果您在區域上設定通道內容檢查並啟用重新比對工作階段，然後僅針對該區域停用 *Reject Non-SYN TCP (*拒絕非 *SYN TCP)*，因此啟用或編輯「通道內容」檢查原則不會導致防火牆丟棄現有的通道工作階段。
非對稱路徑		決定是否丟棄或避開包含非同步 ACK 或視窗外序號的封包。 • **global**（全域）—使用透過 **TCP Settings**（**TCP** 設定）或 CLI 指派的系統全域設定。 • **drop**（丟棄）—丟棄包含非對稱路徑的封包。 • **bypass**（略過）—略過對於包含非對稱路徑的封包進行的掃描。
除去 TCP 選項		決定是否從 TCP 封包中除去 TCP 時間戳記或 TCP 快速開啟選項。
TCP 時間戳記	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack Protection**（基於封包的攻擊保護）> **TCP Drop**（**TCP** 丟棄）	判斷封包在標頭中是否有 TCP 時間戳記，如果有，則從標頭除去該時間戳記。 除去封包中的 *TCP* 時間戳記，以防止時間戳記 *DoS* 攻擊。
TCP 快速開啟		在三方交握期間從 TCP SYN 或 SYN ACK 封包中除去 TCP 快速開啟選項（與資料承載，若有的話）。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
		當清除（停用）此選項時，會允許 TCP 快速開啟選項，藉由包含資料傳遞而保存連線設定的速度。這獨立於含資料的 TCP SYN 與含資料的 TCP SYN-ACK 運作。預設會停用。
多路徑 TCP (MPTCP) 選項		MPTCP 是 TCP 的延伸，允許用戶端藉由同時使用多個路徑以連線至目的地主機而維護連線。依預設，會根據全域 MPTCP 設定停用 MPTCP 支援。 針對與此設定檔相關聯的安全性區域檢閱或調整 MPTCP 設定： • **no**（否）—啟用 MPTCP 支援（不除去 MPTCP 選項）。 • **yes**（是）—停用 MPTCP 支援（除去 MPTCP 選項）。設定此選項時，MPTCP 連線會轉換成標準 TCP 連線，因為 MPTCP 是回溯相容於 TCP。 • **(Default) global**（（預設值）全域）—基於全域 MPTCP 設定支援 MPTCP。依預設，全域 MPTCP 設定為 [是]，因此會停用 MPTCP（會從封包中除去 MPTCP 選項）。您可使用 **TCP Settings**（**TCP** 設定）中的 **Strip MPTCP option**（除去 **MPTCP** 選項）或透過下列 CLI 命令檢閱或調整全域 MPTCP 設定： `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

ICMP 丟棄

若要指示防火牆丟棄其在區域中收到的某些 ICMP 封包，請選取下列設定來加以啟用。

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
ICMP ping ID 0	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack Protection**（基於封包的攻擊保護）> **ICMP Drop**（**ICMP** 丟棄）	如果 ICMP ping 封包的識別碼值是 0，丟棄封包。
ICMP 分段		捨棄由 ICMP 分段組成的封包。
ICMP 大封包（>1024）		捨棄大於 1024 位元組的 ICMP 封包。
捨棄內嵌錯誤訊息的 ICMP		捨棄內嵌錯誤訊息的 ICMP 封包。
隱藏 ICMP TTL 到期錯誤		停止傳送 ICMP TTL 過期的訊息。
隱藏所需 ICMP 片段		停止傳送 ICMP 分段所需訊息，這些訊息回應超出介面 MTU 且已設定不分段 (DF) 位元的封包。此設定將干涉在防火牆背後由主機執行的 PMTUD 程序。

© 2019 Palo Alto Networks, Inc.

IPv6 丟棄

若要指示防火牆丟棄其在區域中收到的某些 IPv6 封包，請選取下列設定來加以啟用。

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
類型 0 的路由標頭	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack Protection**（基於封包的攻擊保護）> **IPv6 Drop**（**IPv6** 丟棄）	捨棄包含類型 0 路由標頭的 IPv6 封包。請參閱 RFC 5095 中有關類型 0 路由標頭資訊。
IPv4 相容位址		捨棄定義為 RFC 4291 IPv4 相容 IPv6 位址的 IPv6 封包。
任一傳送來源位址		捨棄包含任一傳播來源位址的 IPv6 封包。
不需要片段標頭		捨棄含最後片段旗標 (M=0) 且位移為零的 IPv6 封包。
ICMP「封包太大」中的 MTU 少於 1280 位元組		當最大傳輸單位 (MTU) 不到 1,280 個位元組時，捨棄包含「封包太大」ICMPv6 訊息的 IPv6 封包。
跳躍延伸		捨棄包含逐一躍點選項延伸標頭的 IPv6 封包。
Routing extension		捨棄包含路由延伸標頭的 IPv6 封包，該標頭會將封包導向到前往目的地上的一或多個中介節點。
目的地延伸		捨棄包含目的地選項延伸模組的 IPv6 封包，該延伸模組包含僅預定為封包目的地的選項。
延伸標頭中無效的 IPv6 選項		捨棄延伸標頭中包含無效 IPv6 選項的 IPv6 封包。
非零保留欄位		捨棄其標頭中有保留欄位未設為零的 IPv6 封包。

ICMPv6 丟棄

若要指示防火牆對其在區域中收到的某些 ICMPv6 封包執行哪些動作，請選取下列設定來加以啟用。

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
無法到達 ICMPv6 目的地 - 需要遵循明確的安全性規則	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Packet Based Attack**	對於目的地無法到達的 ICMPv6 訊息，即使與現有工作階段相關聯，也需要需要明確的安全性規則比對。
ICMPv6 封包太大 - 需要遵循明確的安全性規則		對於封包太大的 ICMPv6 訊息，即使與現有工作階段相關聯，也需要明確的安全性規則比對。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—基於封包的攻擊保護	設定位置	說明
超過 ICMPv6 時間 - 需要遵循明確的安全性規則	**Protection**（基於封包的攻擊保護）> **ICMPv6 Drop**（**ICMPv6** 丟棄）	對於時間超過的 ICMPv6 訊息，即使與現有工作階段相關聯，也需要明確的安全性規則比對。
ICMPv6 參數問題 - 需要遵循明確的安全性規則		對於參數問題 ICMPv6 訊息，即使與現有工作階段相關聯，也需要明確的安全性規則比對。
ICMPv6 重新導向 - 需要遵循明確的安全性規則		對於重新導向訊息 ICMPv6 訊息，即使與現有工作階段相關聯，也需要明確的安全性規則比對。

通訊協定保護

- Network > Network Profiles > Zone Protection > Protocol Protection（網路 > 網路設定檔 > 區域保護 > 通訊協定保護）

防火牆一般在第二層區域間和 Virtual Wire 區域間允許非 IP 通訊協定。通訊協定保護讓您可控制在第二層 VLAN 或 Virtual Wire 上的安全性區域間或安全性區域內允許（包含）或不允許（排除）哪個非 IP 通訊協定。非 IP 通訊協定的例子包含 AppleTalk、Banyan VINES、VINES、Novell、NetBEUI 和資料採集與監控 (SCADA) 系統例如通用物件導向變電所事件 (GOOSE)。

在您於區域保護設定檔中設定通訊協定保護後，將設定檔套用至第二層 VLAN 或 Virtual Wire 上的進入安全性區域。

在面向網路的區域啟用通訊協定保護，以防止來自您不使用的通訊協定的第二層流量進入您的網路。

區域保護設定檔設定—通訊協定保護	設定位置	說明
規則類型	**Network**（網路）> **Network Profiles**（網路設定）> **Zone Protection**（區域保護）> **Reconnaissance Protection**（偵察保護）（網路 > 網路設定檔 > 區域保護 > 偵察保護）	指定您正針對通訊協定保護建立的清單類型： • **Include List**（包含清單）—僅允許清單上的通訊協定—除了 IPv4 (0x0800)、IPv6 (0x86DD)、ARP (0x0806) 和 VLAN 標記的框架 (0x8100)。隱含拒絕（封鎖）所有其他通訊協定。 • **Exclude List**（排除清單）—僅拒絕清單上的通訊協定；隱含允許所有其他通訊協定。您無法排除 IPv4 (0x0800)、IPv6 (0x86DD)、ARP (0x0806) 或 VLAN 標記的框架 (0x8100)。 使用「包含清單」僅允許您使用的第二層通訊協定，並拒絕所有其他通訊協定。拒絕您在網路上不使用的通訊協定可減少攻擊面。防火牆僅拒絕您新增至「排除清單」的通訊協定，並允許清單中未包含的所有其他通訊協定。如果您未設定「通訊協定保護」，則會允許所有第二層通訊協定。

© 2019 Palo Alto Networks, Inc.

區域保護設定檔設定—通訊協定保護	設定位置	說明
通訊協定名稱		輸入對應至您正新增至清單的 Ethertype 代碼的通訊協定名稱。防火牆不會確認通訊協定名稱符合 Ethertype 代碼，但 Ethertype 代碼會決定通訊協定篩選。
啟用		**Enable**（啟用）清單上的 Ethertype 代碼。若您想要為了測試目的停用通訊協定但不將其刪除，則改為停用該通訊協定。
Ethertype (十六進位)		輸入開頭為 0x 的 Ethertype 代碼（通訊協定，範圍是 0x0000 至 0xFFFF）。清單最多可以有 64 個 Ethertype。 Ethertype 代碼的部分來源是： • IEEE 十六進位 Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

乙太網路 *SGT* 保護

- Network > Network Profiles > Zone Protection > Ethernet SGT Protection（網路 > 網路設定檔 > 區域保護 > 乙太網路 SGT 保護）

對於 Cisco TrustSec 網路中的防火牆，建立附有要排除的第二層安全性群組標籤 (SGT) 清單的區域保護設定檔。將區域保護設定檔套用至第二層、虛擬介接或旁接介面。如果含有 802.1Q (Ethertype 0x8909) 標頭的傳入封包具有與清單中 SGT 相符的 SGT，則防火牆將丟棄該封包。

區域保護設定檔設定	設定位置	說明
第二層 SGT 排除清單	**Network**（網路）> **Network Profiles**（網路設定檔）> **Zone Protection**（區域保護）> **Ethernet SGT Protection**（乙太網路 **SST** 保護）	輸入安全性群組標籤 (SGT) 清單的名稱。
標籤		若 SGT 與套用至區域的區域保護設定檔中此清單相符，則在要排除（丟棄）的封包標頭中輸入第二層 SGT（範圍為 0 至 65,535）。
啟用		針對乙太網路 SGT 保護 **Enable**（啟用）（預設）此排除清單。取消選取 **Enable**（啟用）選項，以停用排除清單。

網路 > 網路設定檔 > QoS

Add（新增）QoS 設定檔，為多達八個服務等級定義頻寬限制及優先順序。您可以為個別等級和集合等級設定保證頻寬與最大頻寬限制。優先順序決定了當存在衝突時應如何處理流量。

若要完全啟用防火牆以提供 QoS，也要：

- ❑ 定義您要接受 QoS 處理的流量（選取 [原則 > QoS]）以新增或修改 QoS 原則。
- ❑ 在介面上啟用 QoS（選取 [網路 > QoS]）。

© 2019 Palo Alto Networks, Inc.

請參閱服務品質 以了解完整的 QoS 工作流程、概念及使用案例。

QoS 設定檔設定	
設定檔名稱	輸入用來識別設定檔的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
輸出最大	輸入流量透過此介面離開防火牆的最大吞吐量（以Mbps為單位）。其默認值為 0，它會指定防火牆流量上限（PAN-OS 7.1.16 和更高版本中為 60,000 Mbps；PAN-OS 7.1.15 和更早發行版中為 16,000 Mbps）。 當 QoS 設定檔啟用於某實體介面時，則其**Egress Max**（輸出最大值）必須小於或等於該實體介面所定義的 **Egress Max**（輸出最大值）。請參閱 [網路 > QoS]。 雖然這不是必要的欄位，但建議您一律為 *QoS* 設定檔定義 *Egress Max*（輸出最大值）。
Egress 保證	輸入保證用於此設定檔的頻寬 (Mbps)。超過輸出保證頻寬時，防火牆將盡力傳送流量。

等級	按一下 **Add**（新增）並指定如何處理個別 QoS 等級。您可以選取要設定的一或多個等級：
	• 等級—如果您未設定等級，仍可在 QoS 原則中包含它。在此情況下，流量受限於整體 QoS 限制。不符合 QoS 原則的流量將指定為等級 4。
	• 優先順序—按一下並選取要指定給此等級的優先順序：
	  • 與超管理器
	  • 高
	  • 中
	  • 低
	當發生衝突時，會捨棄指定為低優先順序的流量。Real-time 優先順序使用它自己個別的佇列。
	• **Egress Max**（輸出最大值）—按一下並輸入此等級的最大吞吐量 (Mbps)。其默認值為 0，它會指定防火牆流量上限（PAN-OS 7.1.16 和更高版本中為 60,000 Mbps；PAN-OS 7.1.15 和更早發行版中為 16,000 Mbps）。QoS 級別的 **Egress Max**（輸出最大值），必須小於或等於為 QoS 設定檔的 **Egress Max**（輸出最大值）。
	雖然這不是必要的欄位，但建議您一律為 *QoS* 設定檔定義 *Egress Max*（輸出最大值）。
	• **Egress** 保證 — 按一下並輸入此等級的保證頻寬 (Mbps)。指派給某一等級的保證頻寬未保留用於該等級 — 未使用的頻寬可繼續用於其他流量。然而，超過用於該流量等級的輸出保證頻寬時，防火牆將盡力傳送該流量。

© 2019 Palo Alto Networks, Inc.

Network > Network Profiles > LLDP Profile（網路 > 網路設定檔 > LLDP 設定檔）

連結層探索通訊協定 (LLDP) 設定檔可讓您設定防火牆的 LLDP 模式、啟用系統日誌與 SNMP 通知，然後設定您要傳輸到 LLDP 端點的選用類型-長度-值 (TLV)。在設定 LLDP 設定檔後，將設定檔指派給一或多個介面。

進一步了解 LLDP，包括如何設定和監控 LLDP。

LLDP 設定檔設定	說明
名稱	指定 LLDP 設定檔名稱。
模式	選取 LLDP 的運作模式：傳輸-接收、 僅傳輸 或 僅接收 。
SNMP Syslog 通知	啟用在全域 **Notification Interval**（通知間隔）發生的 SNMP 陷阱與系統日誌通知。若已啟用，防火牆會依照 **Device**（設備） > **Log Settings**（日誌設定） > **System**（系統） > **SNMP Trap Profile**（**SNMP** 設陷設定檔）和 **Syslog Profile**（**Syslog** 設定檔） 的設定傳送 SNMP 設陷與 Syslog 事件。
連接埠說明	啟用要在連接埠說明 TLV 中傳送的防火牆 ifAlias 物件。
系統名稱	啟用要在系統名稱 TLV 中傳送的防火牆 sysName 物件。
系統說明	啟用要在系統說明 TLV 中傳送的防火牆 sysDescr 物件。
系統功能	啟用要在系統功能 TLV 中透過下列對應傳送的介面部署模式（L3、L2 或虛擬介接）。 • 如果為 L3，則防火牆會公告路由器（位元 6）功能與其他位元（位元 1）。 • 如果為 L2，則防火牆會公告 MAC 橋接器（位元 3）功能與其他位元（位元 1）。 • 如果為 Virtual Wire，則防火牆會宣告重複器（位元 2）功能與其他位元（位元 1）。 SNMP MIB 會將在介面上設定的功能結合成單一項目。
管理位址	啟用要在管理位址 TLV 中傳送的 **Management Address**（管理位址）。您可以輸入最多 4 個管理位址，這些位址會依其指定的順序傳送。若要變更順序，請按一下 **Move Up**（上移）和 **Move Down**（下移）按鈕。
名稱	指定管理位址的名稱。
介面	選取其 IP 位址將為管理位址的介面。如果您選取 **None**（無），您可以在 IPv4 或 IPv6 選項旁的欄位中輸入 IP 位址。
IP 選擇	選取 **IPv4** 或 **IPv6**，然後在相鄰的欄位中，選取或輸入要傳輸作為管理位址的 IP 位址。如果已啟用 **Management Address**（管理位址）TLV，則需要至少一個管理位址。如果沒有設定管理 IP 位址，則系統會使用傳輸介面的 MAC 位址作為傳輸的管理位址。

© 2019 Palo Alto Networks, Inc.

Network > Network Profiles > BFD Profile（網路 > 網路設定檔 > BFD 設定檔）

雙向轉送偵測 (BFD) 能夠極快地偵測連結失敗，可加速容錯轉移至不同的路由。

您想了解什麼內容？	請參閱：
什麼是 BFD？	BFD 概要
可用來建立 BFD 設定檔的欄位有哪些？	BFD 設定檔的建置組塊
檢視虛擬路由器的 BFD 狀態。	檢視 BFD 摘要和詳細資訊
想知道更多？	進一步了解及設定 BFD。 設定下列各項的 BFD： 靜態路由 BGP OSPF OSPFv3 RIP

BFD 概要

BFD 是一項可失敗兩個轉送引擎間雙向路徑失敗的協議，例如介面、資料連結或實際轉送引擎。在 PAN-OS 實作中，其中一個轉向引擎是防火牆上的介面，另一個是已設定的相臨 BFD 端點。以極快的速度進行引擎間的 BFD 失敗偵測，相較於透過連結監視或諸如 Hello 封包或活動訊號等頻繁的動態健康檢查，可實現更快的故障復原。

BFD 偵測到失敗後，它會通知路由通訊協定切換至其他端點路徑。如果對靜態路由設定 BFD，防火牆將從 RIB 及 FIB 表中移除受影響的路由。

下列介面類型均支援 BFD：實體 Ethernet、AE、VLAN、通道（站點到站點 VPN 及 LSVPN），以及 Layer 3 介面的子介面。對於每個靜態路由或動態路由通訊協定，您可啟用或停用 BFD、選取預設 BFD 設定檔，或設定 BFD 設定檔。

BFD 設定檔的建置組塊

- Network > Network Profiles > BFD Profile（網路 > 網路設定檔 > BFD 設定檔）

您可套用預設 BFD 設定檔或您建立的 BFD 設定檔，為靜態路由或動態路由通訊協定啟用 BFD。預設設定檔使用預設 BFD 設定且無法變更。您可 **Add**（新增）新 BFD 設定檔並指定下列資訊。

BFD 設定檔設定	說明
名稱	BFD 設定檔的名稱（最多 31 個字元）。名稱區分大小寫且必須在整個防火牆中是唯一的。請僅使用字母、數字、空格、連字號與底線。
模式	BFD 的運作模式

© 2019 Palo Alto Networks, Inc.

BFD 設定檔設定	說明
	• 主動—BFD 會啟動傳輸控制封包（預設值）。至少其中一個 BFD 端點必須為主動；可都為主動。 • 被動—BFD 會等候端點傳輸控制封包並視需要回應。
所需最小傳輸間隔（毫秒）	您想要 BFD 通訊協定傳輸 BFD 控制封包的最小間隔（毫秒）。PA-7000 系列的最小值為 50；PA-3200 系列的最小值為 100；VM 系列的最小值為 200（最大值為 2000；預設值為 1000）。 如果在同一介面上有多個使用不同 *BFD* 設定檔的通訊協定，請使用相同的 *Desired Minimum Tx Interval*（所需最小傳送間隔）來設定 *BFD* 設定檔。
要求最小傳輸間隔（毫秒）	BFD 可接收 BFD 控制封包的最小間隔（毫秒）。PA-7000 系列的最小值為 50；PA-3200 系列的最小值為 100；VM 系列的最小值為 200（最大值為 2000；預設值為 1000）。
偵測時間乘數	本機系統將從遠端系統接收到的 **Detection Time Multiplier**（偵測時間乘數）乘以遠端系統允許的傳輸間隔（**Required Minimum Rx Interval**（要求最小傳送間）以及最後接收到的**Desired Minimum Tx Interval**（所需最小傳送間隔）取其大）來計算偵測時間。如果偵測時間到期之前 BFD 不從其端點接收 BFD 控制封包，則會發生錯誤（範圍是 2 至 50；預設為 3）。
保持時間（毫秒）	防火牆傳輸 BFD 控制封包之前，連結啟動後的延遲時間（毫秒）。**Hold Time**（保留時間）僅適用於 BFD 主動模式。防火牆若在 **Hold Time**（保留時間）期間接收到 BFD 控制封包，將會加以忽略（範圍是 0-120000，預設值為 0）。預設設定 0 表示 **Hold Time**（保留時間）無傳輸；防火牆在建立連結後立即傳輸並接收 BFD 控制封包。
啟用多重躍點	透過多重躍點啟用 BFD。僅套用於 BGP 實作。
最小 Rx TTL	BFD 將其在支援多重躍點時接受（接收）的最小存留時間值（躍點數）。僅套用於 BGP 實作（範圍是 1-254；無預設值）。

檢視 **BFD** 摘要和詳細資訊

- Network > Virtual Routers（網路 > 虛擬路由器）

下表說明 BFD 摘要資訊。

檢視 BFD 資訊	
檢視 BFD 摘要	選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），並在您關注的虛擬路由器列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。選取 **BFD Summary Information**（BFD 摘要資訊）頁簽。
檢視 BFD 詳細資訊。	在您關注的介面列中，選取 **details**（詳細資訊），以檢視 BFD Details（BFD 詳細資訊）。

© 2019 Palo Alto Networks, Inc.

Network > Network Profiles > SD-WAN Interface Profile（網路 > 網路設定檔 > SD-WAN 介面設定檔）

建立 SD-WAN 介面設定檔以按連結標籤將實體連結進行分組以及控制連結速度和防火牆監控該連結的頻率。

	SD-WAN 介面設定檔
名稱	輸入 SD-WAN 介面設定檔的名稱，最多可以使用 31 個英數字元。該名稱必須以英數字元開頭，可以包含字母、數字、底線 (_)、連字號 (-)、句點 (.)和空格。
連結標籤	選取該設定檔將指派到介面的「連結標籤」，或者新增一個新的標籤。連結標籤可連結防火牆的實體鏈路（不同 ISP）以供在路徑選取或容錯移轉期間選取。
說明	最佳做法是輸入設定檔的使用者易記的說明。
連結類型	從預先定義的清單（**ADSL/DSL**、**Cable Modem**（纜線數據機）、**Ethernet**（以太網絡）、**Fiber**（光纖）、**LTE/3G/4G/5G**、**MPLS**、**Microwave/Radio**（微波/無線電）、**Satellite**（衛星）、**WiFi** 或 **Other**（其他））中選取實體連結類型。防火牆可以支援任何作為乙太網路連線終止和切換到防火牆的 CPE 裝置。例如，WiFi 存取點、LTE 數據機、雷射/微波 CPE，都可以透過乙太網路切換來終止。
最大下載 (Mbps)	輸入從 ISP 下載的最大下載速度 (MB/S)；範圍是 0-100,000，沒有預設值。向您的 ISP 詢問連結速度，或使用 speedtest.net 之類的工具採樣連結的最大速度，並取較長一段時間內最大值的平均值。
最大上傳 (Mbps)	輸入從 ISP 上傳的最大上傳速度 (MB/S)；範圍是 0-100,000，沒有預設值。向您的 ISP 詢問連結速度，或使用 speedtest.net 之類的工具採樣連結的最大速度，並取較長一段時間內最大值的平均值。
符合錯誤更正設定檔介面選取資格	選取此設定可使介面（在其中套用此設定檔）符合編碼防火牆的條件，以選取這些介面進行正向錯誤更正 (FEC) 或封包複製。您可以取消選取此設定，以便絕不會在套用設定檔的昂貴連結（介面）上進行昂貴的 FEC 或封包複製。為設定檔指定的 **Link Type**（連結類型）確定是否選取了 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格）的預設設定。 若要設定 FEC 或封包複製，請建立 SD-WAN 錯誤更正設定檔。
VPN 資料通道支援	確定分支到中樞的流量和返回流量是通過 VPN 通道流動以增加安全性（預設啟用），還是在 VPN 通道之外流動以避免加密負荷。 • 對於具有直接網際網路連線或網際網路中斷能力的共用連結類型（如纜線數據機、ADSL 和其他網際網路連線，請將 **VPN Data Tunnel Support**（**VPN** 資料通道支援）保留啟用。 • 您可以針對 MPLS、衛星或微波之類不具有網際網路中斷能力的專有連結類型停用 **VPN Data Tunnel Support**（**VPN** 資料通道支援）。但是，您必須先確保流量不會被攔截，因為流量將在 VPN 通道外進行傳送。 • 分支能具有 DIA 流量，即需要容錯移轉到連線至中樞的私人 MPLS 連結，並從中樞到達網際網路。**VPN Data Tunnel Support**（**VPN** 資料通道支援）設定確定私人資料通過 VPN 通道流動還是在通道外流動，以及容錯移轉的流量使用其他連線（私人資料流未使用的連線）。防火牆使用區域將 DIA 容錯移轉流量和私人 MPLS 流量分割開來。

© 2019 Palo Alto Networks, Inc.

	SD-WAN 介面設定檔
VPN 容錯移轉指標	（PAN-OS 10.0.3 和更高的 10.0 版）設定 DIA AnyPath 時，需要採用一種方法來指定 DIA 在此進行容錯移轉的中樞虛擬介面或分支虛擬介面中個別 VPN 通道的容錯移轉順序。為 VPN 通道（連結）指定 VPN 容錯移轉指標；範圍是 1 至 65,535；預設值為 10。指標值越低，在容錯移轉期間選取的通道（套用此設定檔的連結）的優先級越高。 例如，將指標設定為較低的值，然後將設定檔套用於寬頻介面；然後建立一個不同的設定檔，以設定套用於昂貴 LTE 介面的高指標，確保僅在寬頻容錯移轉後才使用該設定檔。
路徑監控	選取路徑監控模式，在該模式中，防火牆會監控您套用此 SD-WAN 介面設定檔的介面。 • **Aggressive**（積極）—（LTE 和衛星之外的所有連結類型的預設值）防火牆以固定的頻率將探查封包傳送到 SD-WAN 連結的另一端。 如果您需要更快的偵測以及在暫時低壓和斷電情況下進行容錯移轉，請使用 *Aggressive*（積極）模式。 • **Relaxed**（寬鬆）—（LTE 和衛星連結類型的預設值）防火牆在傳送探查封包組之間等待幾秒（**Probe Idle Time**（探查閒置時間）），讓路徑監控不那麼頻繁。當探查閒置時間到期時，防火牆會以設定的 **Probe Frequency**（探查頻率）傳送探查七秒。 當您擁有低頻寬連結、按使用量收費的連結（如 *LTE*），或相比偵測節省成本和頻寬更為重要時，請使用 *Relaxed*（寬鬆）模式。
探查頻率（每秒）	輸入探查頻率，這是防火牆每秒鐘向 SD-WAN 連結的另一端傳送探查封包的次數（範圍是 1-5；預設值為 5）。
探查閒置時間（秒）	如果您選取 **Relaxed**（寬鬆）路徑監控，您可以設定防火牆在傳送探查封包組期間等待的探查閒置時間（秒）（範圍是 1-60；預設值為 60）。
容錯回復保留時間（秒）	輸入時間長度（以秒為單位），這是防火牆在容錯移轉後將復原的連結恢復為偏好連結之前，防火牆等待復原的連結保持合格的時間（範圍是 20-120；預設值為 120）。容錯回復保留時間可防止太快將復原的連結恢復為偏好連結，導致它立即再次失敗。

© 2019 Palo Alto Networks, Inc.

裝置

請使用下列各節，參照防火牆上基本的系統設定和維護工作的欄位：

- Device > Setup（裝置 > 設定）
- Device > High Availability（裝置 > 高可用性）
- 裝置 > 日誌轉送卡
- Device > Config Audit（裝置 > 組態稽核）
- 裝置 > 密碼設定檔
- Device > Administrators（裝置 > 管理員）
- Device > Admin Roles（裝置 > 管理員角色）
- Device > Access Domain（裝置 > 存取網域）
- Device > Authentication Profile（裝置 > 驗證設定檔）
- Device > Authentication Sequence（裝置 > 驗證順序）
- Device > User Identification（裝置 > 使用者識別）
- Device > Data Redistribution（裝置 > 資料重新散佈）
- Device > Device Quarantine（裝置 > 裝置隔離）
- 裝置 > VM 資訊來源
- 裝置 > 疑難排解
- 裝置 > 虛擬系統
- 裝置 > 共用閘道
- 裝置 > 憑證管理
- 裝置 > 回應頁面
- Device > Log Settings（裝置 > 日誌設定）
- 裝置 > 伺服器設定檔
- 裝置 > 本機使用者資料庫 > 使用者
- 裝置 > 本機使用者資料庫 > 使用者群組
- 裝置 > 已排程的日誌匯出
- 裝置 > 軟體
- Device > GlobalProtect Client（裝置 > GlobalProtect 用戶端）
- Device > Dynamic Updates（裝置 > 動態更新）
- Device > Licenses（裝置 > 授權）
- 裝置 > 支援
- Device > Master Key and Diagnostics（裝置 > 主要金鑰與診斷）
- Device > Policy Recommendation（裝置 > 政策建議）

Device > Setup（裝置 > 設定）

- Device > Setup > Management（裝置 > 設定 > 管理）
- Device > Setup > Operations（裝置 > 設定 > 操作）
- Device > Setup > HSM（裝置 > 設定 > HSM）
- Device > Setup > Services（裝置 > 設定 > 服務）
- Device > Setup > Interfaces（裝置 > 設定 > 介面）
- Device > Setup > Telemetry（裝置 > 設定 > 遙測）
- Device > Setup > Content-ID（裝置 > 設定 > 內容 ID）
- Device > Setup > WildFire（裝置 > 設定 > WildFire）
- Device > Setup > Session（裝置 > 設定 > 工作階段）

© 2019 Palo Alto Networks, Inc.

Device > Setup > Management（裝置 > 設定 > 管理）

- **Device**（裝置）> **Setup**（設定）> **Management(管理**）
- **Panorama** > **Setup**（設定）> **Management**（管理）

在防火牆上，選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）進行管理設定。

在 Panorama™ 上，選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），以設定您使用 Panorama 範本所管理的防火牆。選取 **Panorama** > **Setup**（設定）> **Management**（管理）以設定 Panorama 管理設定。

下列管理設定同時適用於防火牆和 Panorama，除非另有說明。

- 一般設定
- 驗證設定
- 原則規則庫設定
- Panorama 設定：裝置 > 設定 > 管理（防火牆上用來連線至 Panorama 的設定）
- Panorama 設定：Panorama > 設定 > 管理（Panorama 上設定用來連線至防火牆的設定）
- 日誌記錄與報告設定
- 橫幅和訊息
- 最小密碼複雜性
- AutoFocus™
- Cortex Data Lake
- SSH 管理設定檔設定

項目	說明
一般設定	
主機名稱	輸入主機名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。 如果您不輸入值，PAN-OS® 會使用防火牆型號（例如 PA-5220_2）作為預設值。 （選用）您可設定防火牆使用 DHCP 伺服器提供的主機名稱。請參閱接受 DHCP 伺服器提供的主機名稱（僅限防火牆）。 設定唯一的主機名稱以輕鬆識別您正在管理的裝置。
網域	輸入防火牆的網路網域名稱（最多 31 個字元）。 您可選取設定防火牆與 Panorama 以使用 DHCP 伺服器提供的網域。請參閱接受 DHCP 伺服器提供的網域（僅限防火牆）。
接受 DHCP 伺服器提供的主機名稱（僅限防火牆）	（僅當管理介面 IP 類型為 DHCP 用戶端時套用）選取此選項可讓管理介面接受其從 DHCP 伺服器接收的主機名稱。伺服器主機名稱（如有效）將覆寫 [主機名稱] 欄位中指定的任何值。

© 2019 Palo Alto Networks, Inc.

項目	說明
接受 DHCP 伺服器提供的網域（僅限防火牆）	（僅當管理介面 IP 類型為 DHCP 用戶端時套用）選取此選項可讓管理介面接受其從 DHCP 伺服器接收的網域（DNS 尾碼）。伺服器網域將覆寫 **Domain**（網域）欄位中指定的任何值。
登入橫幅	輸入文字（最多 3200 個字元）以顯示於 **Name**（名稱）與 **Password**（密碼）欄位下方的 Web 介面登入頁面。
強制管理員確認登入橫幅	選取此選項可顯示並強制管理員選取登入頁面登入橫幅上方的 **I Accept and Acknowledge the Statement Below**（我接受並確認下方陳述）選項，這會強制管理員在他們可以 **Login**（登入）前承認他們了解並接受訊息內容。
SSL/TLS 服務設定檔	指派現有的 SSL/TLS 服務設定檔或是建立新的服務設定檔，以指定管理介面上允許的憑證和 SSL/TLS 通訊協定設定（請參閱 [裝置 > 憑證管理 > SSL/TLS 服務設定檔]）。防火牆或 Panorama 會使用此憑證來驗證透過管理 (MGT) 介面或透過任何其他支援 HTTP/HTTPS 管理流量的介面存取 Web 介面的管理員（請參閱 [網路 > 網路設定檔 > 介面管理]）。若您選取 **none**（無），則防火牆或 Panorama 會使用預先定義的憑證。 會提供預先定義的憑證以便於使用。如需更佳的安全性，請指派 *SSL/TLS* 服務設定檔。若要確保信任，憑證必須由憑證授權單位 *(CA)* 憑證指派，該憑證是位於用戶端系統的受信任根憑證儲存區。
時區	選取防火牆的時區。
地區設定	從下拉式清單中選取 PDF 報告的語言。請參閱 [監控 > PDF 報告 > 管理 PDF 摘要]。 如果您已為 Web 介面設定特定語言偏好設定，PDF 報告仍將使用 **Locale**（地區設定）中指定的語言。
日期	在防火牆上設定日期；輸入目前日期（格式為 YYYY/MM/DD），或從下拉式清單中選取日期。 您也定義 *NTP* 伺服器（*Device*（裝置）> *Setup*（設定）> *Services*（服務））。
時間	在防火牆上設定時間；輸入目前時間（採用 24 小時格式），或從下拉式清單中選取時間。 您也定義 *NTP* 伺服器（*Device*（裝置）> *Setup*（設定）> *Services*（服務））。
序號 （僅限 Panorama 虛擬裝置）	輸入 Panorama 的序號。您可以在從 Palo Alto Networks® 收到的訂購履行電子郵件中找到序號。
緯度	輸入防火牆的緯度（-90.0 到 90.0）。

© 2019 Palo Alto Networks, Inc.

項目	說明
經度	輸入防火牆的經度（-180.0 到 180.0）。
自動擷取認可鎖定	當您變更候選設定時，選取此選項可自動套用提交鎖定。如需詳細資訊，請參閱鎖定設定。 啟用*Automatically Acquire Commit Lock*（自動擷取認可鎖定）這樣做之後，在第一個管理員提交變更之前，其他管理員均無法進行組態變更。
憑證到期檢查	當盒上的憑證接近到期日時，指示防火牆建立警告訊息。 啟用 *Certificate Expiration Check*（憑證到期檢查），當盒上的憑證接近到期日時，建立警告訊息。
多重虛擬系統功能	在支援此功能的防火牆上，啟用多重虛擬系統的使用（請參閱 [裝置 > 虛擬系統]）。 若要在防火牆上啟用多重虛擬系統，防火牆原則所參考的不同使用者群組不得超過 *640* 個。如有必要，減少使用者群組的數量。然後，在您啟用並新增多個虛擬系統後，原則即會參考各附加虛擬系統的另 *640* 個使用者群組。
URL 篩選資料庫 （僅限 Panorama）	選取 URL 篩選廠商以便使用 Panorama：**brightcloud** 或 **paloaltonetworks** (PAN-DB)。
使用 Hypervisor 指定的 MAC 位址 （僅限 VM-Series 防火牆）	選取此選項，讓 VM-Series 防火牆使用 Hypervisor 指派的 MAC 位址，而非產生使用 PAN-OS 自訂結構描述的 MAC 位址。 若您啟用此選項，並使用介面的 IPv6 位址，則介面 ID 不能使用 EUI-64 格式，否則會從介面 MAC 位址衍生出 IPv6 位址。在高可用性 (HA) 主動/被動設定中，若您使用 EUI-64 格式，則會發生提交錯誤。
GTP 安全	選取此選項可啟用檢查控制平面的能力，以及 GPRS 通道通訊協定 (GTP) 流量中的使用者資料平面訊息。請參閱 Objects（物件）> Security Profiles（安全性設定檔）> Mobile Network Protection（行動網路保護）以設定行動網路保護設定檔，以便您可在 GTP 流量上強制執行政策。
SCTP 安全性	選取此選項可啟用檢查和篩選串流控制傳輸協定（SCTP）封包和區段的能力，以及應用 SCTP 初始化（INIT）流量保護。請參閱 [物件 > 安全性設定檔 > SCTP 保護]。有關 SCTP INIT 流量保護，請參閱Configure SCTP INIT Flood Protection（設定 SCTP INIT 流量保護）。
進階路由	選取此選項可啟用支援 BGP 和靜態路由的進階路由引擎。您必須提交並重新啟動防火牆，以使對新路由引擎的變更生效（或變更回舊的路由引擎）。

© 2019 Palo Alto Networks, Inc.

項目	說明
	進階路由處於預覽模式，並且該功能集受限。
通道加速	選取此選項可提高通過 GRE 通道、VXLAN 通道和 GTP-U 通道流量的效能和輸送量。此選項預設處於啟用狀態。 • **GRE and VXLAN tunnel acceleration**（**GRE** 和 **VXLAN** 通道加速）—在具有 PA-7000-NPC 和 SMC-B 的 PA-3200 系列防火牆和 PA-7000 系列防火牆上受支援。 • **GTP-U tunnel acceleration**（**GTP-U** 通道加速）—在具有 PA-7000-NPC 和 SMC-B 的 PA-7000 系列防火牆上受支援。若要使 GTP-U 通道流量具有通道加速功能，必須啟用「通道加速」，必須啟用 GTP，不能為 GTP-U 通訊協定設定通道內容檢查 (TCI) 政策規則，以及附加行動網路保護設定檔的安全性政策規則必須允許 GTP 流量。 如果停用或重新啟用「通道加速」並提交，則必須重新啟動防火牆。
裝置憑證	
取得憑證	按一下以輸入從 Palo Alto Networks 客戶支援入口網站產生的一次性密碼 (OTP)。若要使用 CSP 成功驗證 Panorama 並利用雲端服務，例如零接觸佈建 (ZTP)、物聯網、裝置遙測和企業資料遺失防護 (DLP)，則需要提供裝置憑證。順利安裝裝置憑證之後，將會顯示以下內容： • **Current Device Certificate Status**（目前的裝置憑證狀態）—裝置憑證的目前狀態（`Valid`（有效）、`Invalid`（無效）或 `Expired`（已過期）） • **Not Valid Before**（在下列時間前無效）—指出裝置憑證開始有效的時間戳記。 • **Not Valid After**（在下列時間後無效）—指出裝置憑證有效過期並且裝置憑證變成 `Invalid`（無效）或 `Expired`（已過期）的時間戳記。 • **Last Fetched Message**（上次擷取的訊息）—該訊息顯示裝置憑證是安裝成功還是裝置憑證安裝失敗。 • **Last Fetched Status**（上次擷取的狀態）—擷取裝置憑證的狀態（`success`（成功）或 `failed`（失敗））。 • **Last Fetched Timestamp**（上次擷取的時間戳記）—上次裝置憑證安裝嘗試的時間戳記。
驗證設定	
驗證設定檔	選取防火牆用來驗證您在外部伺服器而非在防火牆上本機定義之管理員帳戶的驗證設定檔（或順序）（請參閱 [裝置 > 驗證設定檔]）。當外部管理員登入時，防火牆會從外部伺服器要求驗證和授權資訊（例如管理角色）。 根據驗證設定檔所指定的伺服器類型啟用外部管理員的驗證需要其他步驟，其必須為下列其中一項： • RADIUS

© 2019 Palo Alto Networks, Inc.

項目	說明
	• TACACS+ • SAML 管理員可以使用 *SAML* 來驗證 *Web* 介面，但不能驗證 *CLI*。 選取 **None**（無）可停用外部管理員的驗證。 針對您在本機（防火牆上）定義的管理帳戶，防火牆會使用指派給這些帳戶的驗證設定檔進行驗證（請參閱 [裝置 > 管理員]）。
憑證設定檔	選取驗證設定檔可驗證針對憑證型存取防火牆 Web 介面所設定之管理員的用戶端憑證。如需設定憑證設定檔的指示，請參閱 [裝置 > 憑證管理 > 憑證設定檔]。 設定憑證設定檔以確保管理員的主機具有正確的憑證，以使用憑證設定檔中定義的根 *CA* 憑證進行驗證。
閒置逾時	輸入在管理員自動登出之前不包含任何 Web 介面上的活動或 CLI 的最大時間（以分鐘為單位，範圍是 0 到 1,440；預設值為 60）。值為 0 表示非使用狀態未觸發自動登出。 手動及自動重新整理 *Web* 介面頁面（例如 *Dashboard*（儀表板）和 *[系統警報]* 對話方塊）都會重設 *Idle Timeout*（閒置逾時）計數器。若要啟用防火牆，以當您在支援自動重新整理的頁面上時強制執行逾時，請將重新整理間隔設為 *Manual*（手動）或設為大於 *Idle Timeout*（閒置逾時）的值。您也可以停用 *ACC* 頁籤中的 *Auto Refresh*（自動重新整理）。 將 *Idle Timeout*（閒置逾時）設定在 *10* 分鐘，以防止未經授權的使用者在管理員沒有關閉防火牆工作階段時存取防火牆。
API 金鑰生命週期	輸入 API 金鑰有效的時間長度（分鐘）（範圍是 0 至 525,600，預設值為 0）。若值為 0，表示 API 金鑰有效永遠都不會失效。 **Expire All API Keys**（使所有 **API** 金鑰到期），進而讓所有先前產生的 API 金鑰失效。請謹慎使用此選項，因為所有現有金鑰都會失效，並且您當下使用這些 API 金鑰的操作都將停止運作。 在維護窗口期間執行此操作，以便您可以在不打斷正在引用 *API* 金鑰的實施的情況下替換金鑰。
API 金鑰上次到期時間	顯示 API 金鑰上次到期時間的時間戳記。如果您從未重設過您的金鑰，此欄位沒有數值。
失敗的嘗試	輸入在鎖定管理員帳戶前，防火牆將允許 Web 介面及 CLI 登入失敗的嘗試次數（0 到 10）。0 值會指定不受限制的登入嘗試次數。防火

© 2019 Palo Alto Networks, Inc.

項目	說明
	牆在一般操作模式下的預設值為 0，而在 FIP-CC 模式下的預設值為 10。限制登入嘗試次數有助於保護防火牆免遭暴力攻擊。 若您將 *Failed Attempts*（失敗的嘗試）設定為 *0* 以外的值，但將 *Lockout Time*（鎖定時間）保留為 *0*，則系統會忽略 *Failed Attempts*（失敗的嘗試）且一律不會封鎖使用者。 將 *Failed Attempts*（失敗的嘗試）的數量設定為 *5* 或以下，以便在輸入錯誤時允許合理的重試次數，同時防止惡意系統嘗試使用暴力攻擊登入防火牆。
鎖定時間	輸入達到 **Failed Attempts**（失敗的嘗試）限制後，防火牆會鎖定管理員存取 Web 介面與 CLI 的分鐘數（範圍是 0 到 60）。0 值（預設）表示會套用封鎖，直到另一個管理員手動解除鎖定帳戶。 如果您將 *Failed Attempts*（失敗的嘗試）的數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，在設定的登入嘗試失敗次數後，使用者將被鎖定，直到另一位管理員手動解鎖帳戶為止。 將 *Lockout Time*（鎖定時間）設定為至少 *30* 分鐘，以防止惡意行為者連續嘗試登入。
最大工作階段計數	輸入所有管理員和使用者帳戶允許的同時工作階段數目（範圍是 0 至 4）。值 0（預設值）表示允許無限數量的同時工作階段。 在 *FIPS-CC* 模式下，範圍是 *1* 至 *4*，預設值為 *4*。
最大工作階段時間	輸入作用中的非空閒管理員可以保持登入狀態的分鐘數（範圍是 60 至 1,499）。達到此最大工作階段時間後，該工作階段將會終止，並且需要重新驗證才能開始另一個工作階段。預設值設定為 0（30 天），無法手動輸入。如果未輸入任何值，則 **Max Session Time**（最大工作階段時間）預設為 0。 在 *FIPS-CC* 模式下，範圍是 *60* 至 *1,499*，預設值為 *720*。如果未輸入任何值，則 *Max Session Time*（最大工作階段時間）預設為 *720*。
原則規則庫設定	
需要原則頁籤	在建立新原則規則時，最少需要一個頁籤。在您啟用此選項時如果已經存在原則規則，您下次編輯規則必須新增至少一個頁籤。
需要原則說明	在您建立新原則規則時，需要您新增 **Description**（說明）在您啟用此選項時如果已經存在原則規則，您下次編輯規則必須新增 **Description**（說明）。

© 2019 Palo Alto Networks, Inc.

項目	說明
如果原則沒有頁籤或說明，則無法認可	如果您不新增任何頁籤或說明至原則規則，則強制您的認可失敗。如果您啟用此選項時已存在原則規則，您在下次編輯規則時如未新增頁籤或說明，認可將失敗。 如要認可失敗，您必須**Require tag on policies**（在原則上要求頁籤）或**Require description on policies**（需要原則說明）。
原則需要稽核註解	在建立新原則規則時，需要 **Audit Comment**（稽核註解）。在您啟用此選項時如果已經存在原則規則，您下次編輯規則必須新增 **Audit Comment**（稽核註解）。
稽核註解規則運算式	在稽核註解中指定註解格式參數的需求。
原則規則命中數	追蹤流量比對您在防火牆上設定原則規則的頻率。在啟用時，您可以檢視比對每個規則的整體流量命中總數，以及每個規則的建立、修改、首次命中，以及最後一次命中的日期和時間。
原則應用程式使用方式	

Panorama 設定：Device > Setup > Management（裝置 > 設定 > 管理）

在防火牆上或在 Panorama 上的範本中進行下列設定。這些設定會建立從防火牆至 Panorama 的連線。

您也必須在 Panorama 上設定連線和物件共用設定（Panorama 設定：Panorama > 設定 > 管理）。

防火牆使用與 *AES256* 加密的 *SSL* 連接來註冊 *Panorama*。依預設，*Panorama* 與防火牆會運用預先定義的 *2,048* 位憑證及它們用於設定管理及日誌收集的 *SSL* 連線來彼此驗證。如需進一步保護 *Panorama*、防火牆與日誌收集器之間的 *SSL* 連線，請參閱安全用戶端通訊以設定防火牆與 *Panorama* 或日誌收集器之間的自訂憑證。

Panorama 伺服器	輸入 Panorama 伺服器的 IP 位址或 FQDN。如果 Panorama 位於高可用性 (HA) 設定下，請在第二個 **Panorama Servers**（**Panorama** 伺服器）欄位中輸入次要 Panorama 伺服器的 IP 位址或 FQDN。
Panorama 連線的接收逾時	輸入從 Panorama 接收 TCP 訊息的逾時秒數（範圍是 1 到 240；預設為 240）。
Panorama 連線的傳送逾時	輸入將 TCP 訊息傳送至 Panorama 的逾時秒數（範圍是 1 到 240；預設為 240）。
SSL 傳送至 Panorama 的重試計數	輸入嘗試將安全通訊端層 (SSL) 訊息傳送至 Panorama 的重試次數（範圍是 1 到 64；預設為 25）。
啟用自動認可復原	啟用以允許在認可組態並推送到防火牆時，以及在成功推送組態之後以設定的間隔，防火牆自動驗證它與 Panorama 管理伺服器的連線。 啟用後，如果防火牆無法驗證它與 Panorama 管理伺服器的連線，則防火牆與Panorama 管理伺服器會自動將它們的組態恢復為先前正常執行的組態以恢復連線。
檢查 Panorama 連線的嘗試次數	當已啟用 **Enable Automated Commit Recovery**（啟用自動認可復原）時，設定防火牆測試其與 Panorama 管理伺服器的連線的次數。

© 2019 Palo Alto Networks, Inc.

項目	說明
重試之間的間隔（秒）	當已啟用 **Enable Automated Commit Recovery**（啟用自動認可復原）時，設定防火牆測試其與 Panorama 管理伺服器的連線的嘗試次數之間的時間（以秒為單位）。

安全用戶端通訊	啟用 **Secure Client Communication**（安全用戶端通訊）以確保防火牆使用設定的自訂憑證（而非預設憑證）來驗證 SSL 與 Panorama 或日誌收集器的連線。
	• **None**（無）（預設值）—不會設定任何裝置憑證，且會使用預設的預先定義憑證。
	• **Local**（本機）—防火牆會使用本機裝置憑證，以及防火牆上所產生或從現有企業 PKI 伺服器匯入的對應私密金鑰。
	  • **Certificate**（憑證）—選取您生成或匯入的本機裝置憑證。此憑證可能是防火牆唯一的（根據防火牆序號的雜湊），或可能是連線至 Panorama 的所有防火牆所使用之通用裝置憑證。
	  • **Certificate Profile**（憑證設定檔）—從下拉式清單中選取憑證設定檔。憑證設定檔定義用來驗證客戶端憑證的 CA 憑證，以及如何驗證憑證銷狀態。
	• **SCEP**—防火牆會使用簡易憑證註冊通訊協定 (SCEP) 伺服器所產生的裝置憑證和私密金鑰。
	  • **SCEP Profile**（**SCEP** 設定檔）—從下拉式清單中選取 Device（裝置）> Certificate Management（憑證管理）> SCEP。SCEP 設定檔提供 Panorama 根據您企業 PKI 中的 SCEP 伺服器驗證客戶端裝置的必要資料。
	  • **Certificate Profile**（憑證設定檔）—從下拉式清單中選取 Device（裝置）> Certificate Management（憑證管理）> Certificate Profile（憑證設定檔）。憑證設定檔定義用來驗證客戶端憑證的 CA 憑證，以及如何驗證憑證銷狀態。

	• **Customize Communication**（自訂通訊）—防火牆使用其設定的自訂憑證以驗證選取的裝置。
	  • **Panorama Communication**（**Panorama** 通訊）—防火牆使用設定的客戶端憑證以與 Panorama 通訊。
	  • **PAN-DB Communication**（**PAN-DB** 通訊）—防火牆使用設定的客戶端憑證以與 PAN-DB 裝置通訊。
	  • **WildFire Communication**（**WildFire** 通訊）—防火牆使用設定的客戶端憑證以與 WildFire® 裝置通訊。
	  • **Log Collector Communication**（日誌收集器通訊）—防火牆使用設定的客戶端憑證以與日誌收集器通訊。
	  • **Check Server Identity**（檢查伺服器識別）—（僅限 Panorama 和日誌收集器）防火牆會確認伺服器的身份，方法是比對通用名稱 (CN) 與伺服器的 IP 位址或 FQDN。

停用/啟用 Panorama 原則與物件	只有在防火牆上（而非在 Panorama 的範本中）編輯 **Panorama Settings**（Panorama 設定）時才會顯示此選項。 **Disable Panorama Policy and Objects**（停用 **Panorama** 原則與物件）會停用裝置群組原則和物件至防火牆的傳播。依預設，此動作也會從防火牆移除那些原則和物件。若要在停用傳播前保留防火牆上的裝置群組原則與物件的本機複本，請在按一下選項時所開啟

© 2019 Palo Alto Networks, Inc.

項目	說明
	的對話方塊中，選取 **Import Panorama Policy and Objects before disabling**（停用前匯入 **Panorama** 原則與物件）。執行提交後，原則和物件會成為防火牆設定的一部分，且 Panorama 不再對其進行管理。 在一般操作條件下，停用 Panorama 管理是不必要的，否則可能會增加防火牆的維護與設定的複雜度。此選項一般適用於下列情況，即防火牆需要規則和物件值，且這些值必須不同於裝置群組中定義的對應值。例如，將防火牆移出生產環境，並將其移至實驗室環境進行測試。 若要將防火牆原則和物件管理還原至 Panorama，請按一下 **Enable Panorama Policy and Objects**（啟用 **Panorama** 原則與物件）。
停用/啟用裝置與網路範本	只有在防火牆上（而非在 Panorama 的範本中）編輯 **Panorama Settings**（Panorama 設定）時才會顯示此選項。 **Disable Device and Network Template**（停用裝置與網路範本）會停用範本資訊（裝置和網路設定）至防火牆的傳播。依預設，此動作也會從防火牆移除範本資訊。若要在停用傳播前保留防火牆上範本資訊的本機複本，請在選取此選項時所開啟的對話方塊中，選取 **Import Device and Network Templates before disabling**（停用前匯入裝置與網路範本）。執行提交後，範本資訊會成為防火牆設定的一部分，且 Panorama 不再管理該資訊。 在一般操作條件下，停用 *Panorama* 管理是不必要的，否則可能會增加防火牆的維護與設定的複雜度。此選項一般適用於下列情況，即防火牆需要裝置和網路設定值，且這些值必須不同於範本中定義的對應值。例如，將防火牆移出生產環境，並將其移至實驗室環境進行測試。 若要設定防火牆以再次接受範本，請按一下 **Enable Device and Network Templates**（啟用裝置與網路範本）。

Panorama 設定：Panorama > Setup > Management（Panorama > 設定 > 管理）

若是使用 Panorama 來管理防火牆，請在 Panorama 上進行下列設定。這些設定可決定從 Panorama 至受管理防火牆的連線逾時和 SSL 訊息嘗試次數，以及物件共用參數。

您也必須在防火牆上，或在 Panorama 的範本中設定 Panorama 連線設定：請參閱 Panorama 設定：Device > Setup > Management（裝置 > 設定 > 管理）。

防火牆使用與 *AES256* 加密的 *SSL* 連接來註冊 *Panorama*。依預設，*Panorama* 與防火牆會運用預先定義的 *2,048* 位憑證及它們用於設定管理及日誌收集的 *SSL* 連線來彼此驗證。如需進一步保護這些 *SSL* 連線，請參閱自訂安全伺服器通訊，以設定 *Panorama* 及其用戶端之間的自訂憑證。

連線至裝置的接收逾時	輸入從所有受管理防火牆接收 TCP 訊息的逾時秒數（範圍是 1 到 240；預設為 240）。
連線至裝置的傳送逾時	輸入將 TCP 訊息傳送至所有受管理防火牆的逾時秒數（範圍是 1 到 240；預設為 240）。

© 2019 Palo Alto Networks, Inc.

項目	說明
SSL 傳送至裝置的重試計數	輸入嘗試將 安全通訊端層 (SSL) 訊息傳送至受管理防火牆的重試次數（範圍是 1 到 64；預設為 25）。
與裝置共用未使用的位址與服務物件	選取此選項（預設為啟用）可與受管理的防火牆共用所有 Panorama 共用物件與裝置-群組特定物件。 如果您停用此選項，則此裝置會檢查 Panorama 原則的位址、位址群組、服務和服務群組物件的參照，並且不會共用任何未參照的物件。此選項可確保此裝置只會將必需的物件傳送至受管理防火牆，從而減少物件總計數。 如果您有面向裝置群組中特定裝置的政策規則，在該政策中使用的物件視為也在該裝置群組中使用。
在上階項目中定義的物件將有較高的優先順序	當階層中不同層級的裝置群組具有相同類型與名稱但具有不同值的物件時，選取此選項（預設為停用）可指定父系項目群組中的物件值會較子系項目群組中的物件值為優先。這表示當您執行裝置群組認可時，父系值會替代任何取代值。同樣地，此選項會造成共用物件的值取代裝置群組中相同類型與名稱的物件值。 選取此選項會顯示尋找取代的物件連結。
尋找取代的物件	選取此選項（Panorama 設定對話方塊底部）可列出任何鏡像的物件。鏡像的物件是共用位置中的物件，在裝置群組中具有相同名稱但不同值。只有您指定在父系項目中定義的物件將有較高的優先順序時，連結才會顯示。
在群組上啟用報告和篩選器	選取此選項（預設為停用）可讓 Panorama 在本機上儲存使用者名稱、使用者群組名稱，及其自防火牆接收的使用者對群組對應資訊。此選項對 Panorama 中的所有裝置群組是全域的。不過，您也必須在每個裝置群組的層級啟用本機儲存空間，方法是指定主要裝置並設定防火牆為從主要裝置儲存使用者及群組。
安全通訊設定：Panorama > Setup > Management（Panorama > 設定 > 管理）	

自訂安全伺服器通訊	• **Custom Certificate Only**（僅限自訂憑證）—當啟用時，Panorama 僅接受自訂憑證使用受管理防火牆和日誌收集器進行驗證。
	• **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）—從下拉式清單選取 SSL/TLS 服務設定檔。此設定檔會定義防火牆可用來與 Panorama 通訊的憑證和支援的 SSL/TLS 版本。
	• **Certificate Profile**（憑證設定檔）—從下拉式清單中選取憑證設定檔。此憑證設定檔會定義憑證撤銷檢查行為，以及用來驗證用戶端所顯示之憑證鏈結的根 CA。
	• **Authorization List**（授權清單）—用以下欄位**Add**（新增）並設定新的授權檔案，可設定可連線至 Panorama 授權用戶端裝置的準則。授權清單支援最多 16 個設定檔項目。
	  • **Identifier**（識別碼）—選取 **Subject**（主體） 或 **Subject Alt.**（主體別名）。作為驗證識別碼的名稱 。
	  • **Type**（類型）—如果為 **Subject Alt**（主體別名）。若名稱作為識別碼，則選取 **IP**、**hostname**（主機名稱） 或 **e-mail**（電子郵件） 作為識別碼類型。如果您選取 **Subject**（主旨），則您必須使用 **common name**（常見名稱）作為識別碼類型。

© 2019 Palo Alto Networks, Inc.

項目	說明
	• **Value**（值）—輸入識別碼值。 • **Authorize Clients Based on Serial Number**（根據序號授權用戶端）—Panorama 會根據裝置序號的雜湊授權用戶端裝置。 • **Check Authorization List**（檢查授權清單）—Panorama 檢查針對授權清單的用戶端裝置身分。裝置僅需要符合要授權之清單上的一個準則。如果找不到符合項目，就不會授權裝置。 • **Disconnect Wait Time (min)**（中斷連線等候時間（分鐘））—Panorama 在終止目前與其受管理裝置間的連線之前所等候的時間量（分鐘）。接著，Panorama 會使用已設定的安全伺服器通訊設定，重新建立與其受管理裝置間的連線。在您認可安全伺服器通訊設定後，等候時間才開始。

安全用戶端通訊	使用 **Secure Client Communication**（安全用戶端通訊）可確保用戶端 Panorama 使用設定的自訂憑證（而非預設的預定義憑證）來驗證 SSL 與其他 Panorama 在 HA 對或 WildFire 裝置間的連線。
	• **Predefined**（偏好）（預設）—沒有設定任何裝置憑證且 Panorama 使用預設的預定義憑證。
	• **Local**（本機）—Panorama 會使用本機裝置憑證，以及防火牆上所產生或從現有企業 PKI 伺服器匯入的對應私密金鑰。
	  • **Certificate**（憑證）—選取本機裝置憑證。
	  • **Certificate Profile**（憑證設定檔）—從下拉式清單中選取憑證設定檔。
	• **SCEP**—Panormama 會使用簡易憑證註冊通訊協定 (SCEP) 伺服器所產生的裝置憑證和私密金鑰。
	  • **SCEP Profile**（**SCEP** 設定檔）—從下拉式清單中選取 SCEP 設定檔。
	  • **Certificate Profile**（憑證設定檔）—從下拉式清單中選取憑證設定檔。
	• 自訂通訊
	  • **HA Communication**（**HA** 通訊）— Panorama 使用設定的用戶端憑證以其 HA 端點與 HA 通訊。
	  • **WildFire Communication**（**WildFire** 通訊）—Panorama使用設定的客戶端憑證以與 WildFire 裝置通訊。

日誌記錄與報告設定

使用此區段進行修改：

- 針對報告和下列日誌類型的到期期間和儲存配額。設定會在高可用性配對上進行同步。
  - 防火牆在本機產生及儲存的所有類型日誌（**Device**（裝置）> **Setup**（設定）> **Management**（管理））。設定適用於防火牆上的所有虛擬系統。
  - Panorama 模式下的 M-Series 裝置或 Panorama 虛擬裝置本機產生及儲存的日誌：系統、設定、應用程式統計資料和 User-ID™ 日誌（**Panorama** > **Setup**（設定）> **Management**（管理））。
  - 傳統模式下 Panorama 虛擬裝置本機產生及從防火牆收集的所有類型之日誌（**Panorama** > **Setup**（設定）> **Management**（管理））。

針對防火牆傳送至 *Panorama* 日誌收集器的日誌，您要在每個收集器群組中設定儲存配額和到期期間（請參閱 *[Panorama > 收集器群組]*）。

- 用來計算和匯出使用者活動報告的屬性。

© 2019 Palo Alto Networks, Inc.

項目	說明
• 在防火牆或 Panorama 上建立的預先定義報告。	
日誌儲存空間頁籤 （Panorama 管理伺服器和所有防火牆模式，除了 PA-5200 Series 和 PA-7000 Series 防火牆）	針對每個日誌類型，請指定： • **Quota**（配額）—會以百分比表示配置於硬碟上供日誌儲存空間使用的 **Quota**（配額）。當您變更配額值時，相關聯的磁碟配置也會自動變更。如果所有值的總和超過 100%，而您嘗試儲存設定時，會出現紅色的錯誤訊息。如果發生這種情形，請調整比例，使總和不超過 100% 的限制。 *VM-Series 防火牆預設對於 SCTP 日誌儲存、SCTP 摘要、每小時 SCTP 摘要、每日 SCTP 摘要和每週 SCTP 摘要所配置的配額為 0%。* • **Max Days**（天數上限）—日誌到期期間的（範圍是 1 到 2,000）天數長度。防火牆或 Panorama 裝置會自動刪除超過指定期間的日誌。依預設，沒有到期期間，這表示日誌永遠不會到期。 防火牆或 Panorama 裝置會在建立日誌期間進行評估，然後刪除超過到期期間或配額大小的日誌。 若每週摘要日誌在防火牆刪除日誌的次數之間到達到期臨界值，則在下一次刪除之前可以超出臨界值。日誌配額達到大小上限時，新日誌項目開始覆寫最舊的日誌項目。如果減少日誌配額大小，防火牆或 *Panorama* 會在您提交變更時移除最舊的日誌。在 *HA* 主動/被動設定中，被動端點不會接收日誌，且因此不會刪除他們，除非發生容錯移轉而成為使用中狀態。

如果您編輯日誌記錄與報告設定（*Panorama* > *Setup*（設定）> *Management*（管理）），則 *Panorama* 就會顯示此頁籤。如果您使用 *Panorama* 範本來設定防火牆的設定（*Device*（裝置）> *Setup*（設定）> *Management*（管理）），請參閱 單一磁碟儲存空間與多重磁碟儲存空間頁籤。	• **Core Files**（核心檔案）—若您的防火牆遭遇系統程序失敗，它會產生包含關於程序詳細資料和失敗原因的核心檔案。如果核心檔案對於預設核心檔案儲存位置而言太大 (`/var/cores` partition)，您可以啟用 **`large-core`** 檔案選項，以配置替代及較大的儲存位置 (`/opt/panlogs/cores`)。Palo Alto Networks 支援工程師可視需要增加配置的儲存空間。
	
	若要啟用或停用 **`large-core`** 檔案選項，請從設定模式輸入下列 CLI 命令，然後**`commit`**設定：
	
	`# set deviceconfig setting management large-core [yes|no]`
	
	當您停用此選項時，會刪除核心檔案。
	
	您必須從操作模式使用 SCP 來匯出核心檔案：
	
	`> scp export core-file large-corefile`
	
	僅 Palo Alto Networks 支援工程師可判讀核心檔案內容。

© 2019 Palo Alto Networks, Inc.

項目	說明
	• **Restore Defaults**（還原預設值）—選取此選項可還原為預設值。
Session Log Storage（工作階段日誌儲存空間）和 **Management Log Storage**（管理日誌儲存空間）頁籤 （僅限 PA-5200 Series 與 A-7000 Series 防火牆）	PA-5200 Series 與 PA-7000 Series 防火牆會將管理日誌和工作階段日誌儲存在個別磁碟上。選取每一組日誌的頁籤，並設定日誌儲存空間頁籤中所述的設定： • **Session Log Storage**（工作階段日誌儲存空間）—選取 **Session Log Quota**（工作階段日誌配額），並設定配額和流量、威脅、URL 篩選、HIP 相符、User-ID、GTP/通道、SCTP 和驗證日誌的到期期間，以及延伸威脅 PCAP。 • **Management Log Storage**（管理日誌儲存空間）—設定系統、設定與應用程式統計資料，以及 HIP 報告、資料篩選擷取、應用程式 PCAP 和偵錯篩選 PCAP 的配額和到期期間。
Single Disk Storage（單一磁碟儲存空間）和 **Multi Disk Storage**（多重磁碟儲存空間）頁籤 （僅限 Panorama 範本）	如果您使用 Panorama 範本來設定日誌配額和到期期間，請根據指派給範本的防火牆，設定下列其中一個或全部頁籤的設定： • **PA-5200 Series and PA-7000 Series firewalls**（**PA-5200** 系列與 **PA-7000** 系列防火牆）—選取 **Multi Disk Storage**（多重磁碟儲存空間）並設定工作階段日誌儲存空間與管理日誌儲存空間頁籤中的設定。 *PA-5200 Series 防火牆預設對於 SCTP 日誌儲存、SCTP 摘要、每小時 SCTP 摘要、每日 SCTP 摘要和每週 SCTP 摘要所配置的配額為 0%。* • 所有其他防火牆模型—選取**Single Disk Storage**（單一磁碟儲存空間）、選取 **Session Log Quota**（工作階段日誌配額），並設定 Log Storage tab（日誌儲存空間頁籤）上的設定。
日誌匯出與報告頁籤	視需要設定下列日誌匯出與報告設定： • **Number of Versions for Config Audit**（設定檔稽核的版本編號）—輸入丟棄最舊版本之前要儲存的設定版本數（預設為 100）。您可以使用這些儲存的版本來稽核和比較設定中的變更。 • **Number of Versions for Config Backups**（設定檔備份的版本編號）—（僅適用於 Panorama）輸入丟棄最舊備份之前要儲存的設定備份數（預設為 100）。 • **Max Rows in CSV Export**（**CSV** 匯出中的最大列數）—輸入將出現在從流量日誌檢視中 **Export to CSV**（匯出為 **CSV**）產生之 CSV 報告中的最大列數（範圍是 1 到 1,048,576；預設為 65,535）。 • **Max Rows in User Activity Report**（使用者活動報告中的最大列數）—輸入詳細使用者活動報告支援的最大列數（範圍是 1 到 1,048,576，預設為 5,000）。
日誌匯出與報告頁籤（續）	• **Average Browse Time (sec)**（平均瀏覽時間（秒））—設定此變數可調整針對 [監控 > PDF 報告 > 使用者活動報告]（範圍是 0 到 300 秒，預設為 60）以秒數計算瀏覽時間的方式。 計算將忽略分類為網路廣告與內容傳送網路的網站。瀏覽時間計算以記錄在 URL 篩選日誌中的容器頁面為基礎。容器頁面之所以會做為此計算的基礎使用，是因為許多網站都從不應考慮的外部網站載入內容。如需容器頁面的更多資訊，請參閱 [容器頁面]。平均瀏覽時間設定為管理員認為使用者瀏覽網頁應花費的平均時間。在平均瀏覽時間過去之後所做的任何要求都將視為新瀏覽活動。計算將

© 2019 Palo Alto Networks, Inc.

項目	說明
	忽略在第一個要求的時間（開始時間）與平均瀏覽時間之間載入的任何新網頁。此行為的設計目的是排除在感興趣之網頁內載入的任何外部網站。範例：如果平均瀏覽時間設定為 2 分鐘且使用者開啟網頁並檢視該頁面 5 分鐘，則該頁面的瀏覽時間仍將為 2 分鐘。之所以會如此，是因為無法決定使用者檢視指定頁面的時間。 • **Page Load Threshold (sec)**（頁面載入閾值（秒））—可讓您調整將頁面元件載入到頁面上所花費的假設時間秒數（範圍是 0-60；預設值為 20）。會將在第一個頁面載入與頁面載入臨界值之間發生的任何要求假設為頁面的元件。而將在頁面載入臨界值以外發生的任何要求假設為使用者按一下頁面內的連結。頁面載入臨界值也用於 [監控 > PDF 報告 > 使用者活動報告] 的計算。 • **Syslog HOSTNAME Format**（**Syslog HOSTNAME** 格式）—選取是否要在 Syslog 訊息標頭中使用 FQDN、主機名稱或 IP 位址（IPv4 或 IPv6）。此標頭會識別防火牆或訊息來源的 Panorama 管理伺服器。 • **Report Runtime**（報告執行階段）—當防火牆或 Panorama 裝置開始產生每日排程報告時，選取一天的時間（預設為上午 2 點）。 • **Report Expiration Period**（報告到期期間）—設定報告的到期期間天數（範圍是 1 到 2,000）。依預設，沒有到期期間，這表示報告永遠不會到期。防火牆或 Panorama 裝置根據其系統時間，每天於凌晨 2 時刪除到期報告。
	• **Stop Traffic when LogDb full**（在 **LogDb** 已滿時停止流量）（僅適用於防火牆；預設為停用）—如果您想要通過防火牆的流量在日誌資料庫已滿時停止，請選取此選項。 • **Enable Threat Vault Access**（啟用威脅資料庫存取）（預設為啟用）—啟用防火牆來存取威脅資料庫，以收集關於偵測到之威脅的最新資訊。此資訊可供威脅日誌及 ACC 圖表所示的熱門威脅活動使用。 • **Enable Log on High DP Load**（於高 **DP** 載入時啟用日誌）（僅適用於防火牆；預設為停用）—選取此選項可在防火牆上的封包處理負載達到 100% CPU 使用率時指定產生系統日誌項目。 *Enable Log on High DP Load*（於高 *DP* 載入時啟用日誌）允許管理員調查並識別高 *CPU* 使用率的原因。 高 *CPU* 負載可能會導致操作效能下降，因為 *CPU* 沒有足夠的週期來處理所有封包。系統日誌警示您此問題（每分鐘產生一個日誌項目），並可讓您調查可能的原因。 • **Enable High Speed Log Forwarding**（啟用高速日誌轉送）（僅適用於 PA-5200 Series 與 PA-7000 Series 防火牆；預設為停用）—作為最佳實踐方法，選取此選項以轉送日誌給 Panorama，其最大速率為每秒 120,000 日誌。停用時，防火牆會以每秒 80,000 個日誌的最大速率將日誌轉送到 Panorama。 如果您啟用此選項，防火牆不會在本機儲存日誌，或將它們顯示於 **Dashboard**（儀表板）、**ACC** 或 **Monitor**（監控）頁籤。此外，您必須設定日誌轉送至 Panorama 才能使用此選項。

© 2019 Palo Alto Networks, Inc.

項目	說明
	• **Log Collector Status**（日誌收集器狀態）—顯示防火牆是否已成功與散布的日誌收集架構建立連線並向其傳送日誌的狀態。如果防火牆也被設定向記錄日誌服務傳送日誌，請驗證**Logging Service Status**（記錄日誌服務狀態），於記錄日誌服務區段。
（僅限 Panorama）	• **Buffered Log Forwarding from Device**（從裝置轉送的已緩衝記錄）（預設為啟用）—允許防火牆失去與 Panorama 的連線時，緩衝其硬碟（本機儲存裝置）上的日誌項目。還原至 Panorama 的連線時，防火牆將日誌項目轉送至 Panorama；適用於緩衝的磁碟空間取決於防火牆型號的日誌儲存配額，及擱置中翻轉的日誌量。如果耗盡可用空間，則將刪除最早的項目以允許新項目的日誌記錄。 啟用 *Buffered Log Forwarding from Device*（從裝置轉送的已緩衝記錄）以防止在與 *Panorama* 連線中斷時遺失日誌。 • **Get Only New Logs on Convert to Primary**（僅取得轉換至主要的新日誌）（預設為停用）—此選項僅適用於傳統模式下將日誌寫入網路檔案系統 (NFS) 的 Panorama 虛擬裝置。使用 NFS 日誌記錄時，只會將主要 Panorama 安裝至 NFS。因此，防火牆只會將日誌傳送至主動主要 Panorama。此選項可讓您設定防火牆，亦即唯有在發生 HA 容錯轉移時才將最近產生的日誌傳送至 Panorama，且次要 Panorama 會繼續日誌記錄到 NFS（提升至主要後）。此選項通常是為了在經過一段長時間後還原 Panorama 連線時，防止防火牆傳送大量的緩衝日誌。 • **Only Active Primary Logs to Local Disk**（僅適用於本機磁碟的主動主要日誌）（預設為停用）—此選項僅適用於傳統模式下的 Panorama 虛擬裝置。此選項能讓您僅設定主動 Panorama，將日誌儲存至本機磁碟。
	Pre-Defined Reports（預先定義的報告）（預設為啟用）—可在防火牆和 Panorama 上使用應用程式、流量、威脅、URL 篩選和串流控制傳輸協定（SCTP）的預先定義報告。在 **Device**（裝置）> **Setup**（設定）> **Management**（管理）> **General Settings**（一般設定）中啟用 SCTP 安全性後，可使用防火牆和 Panorama 上的 SCTP 預定義報告。 由於防火牆每小時產生結果（以及將其轉寄到其彙總和編譯以進行檢視的 Panorama）會耗用記憶體資源，因此若要降低記憶體使用量，您可以停用與您無關的報告。若要停用報告，請停用此報告選項。 使用 **Select All**（全選）或 **Deselect All**（取消全選）選項以完全啟用或停用預先定義報告的產生。 停用報告之前，請驗證沒有群組報告或 *PDF* 報告在使用它。如果您停用指派給報告組的預先定義的報告，整個報告組將沒有資料。

橫幅和訊息

如需在當日訊息對話方塊中檢視所有訊息，請參閱當日訊息。

© 2019 Palo Alto Networks, Inc.

項目	說明
在您設定當日訊息之後，按一下 *OK*（確定），後續登入的管理員及重新整理其瀏覽器的作用中管理員會立即看到新訊息或更新訊息；不必再認可。這可讓您在執行提交之前，對即將提交的其他管理員發出警告。	
當日訊息 （核取方塊）	當管理員登入此網路介面時，選取此選項可啟用當日訊息對話方塊顯示。
當日訊息 （文字項目欄位）	輸入當日訊息文字（最多 3,200 個字元）。
允許「不要再顯示」	選取此選項（預設為停用）可在當日訊息對話方塊中包含 **Do not show again**（不要再顯示）選項。此選項可讓管理員避免在後續登入時看到相同的訊息。 如果您修改 *Message of the Day*（當日訊息）文字，即時管理員已選取 *Do not show again*（不要再顯示），訊息仍會顯示。管理員必須重新選取該選項，以避免在後續工作階段中修改訊息，除非是再次修改該訊息。
Title (職稱)	輸入當日訊息標題文字（預設為 `Message of the Day`（當日訊息）。
背景顏色	為當日訊息對話方塊選取背景顏色。預設（**None**（無））為淺灰色背景。
圖示	選取預先定義的提示，可顯示在當日訊息對話方塊中的文字上方。 • **None**（無）（預設） • **Error**（錯誤） • **Help**（說明） • 資料 • **Warning**（警告）
標題橫幅	輸入標題橫幅顯示的文字（最多 3,200 個字元）。
頁首顏色	選取標題背景的顏色。預設（**None**（無））為透明背景。
頁首文字顏色	選取標題文字的顏色。預設（**None**（無））為黑色。
標題與頁尾的橫幅相同	如果您想要頁尾橫幅採用與標題橫幅相同的文字及顏色，請選取此選項（預設為啟用）。啟用後，頁尾橫幅文字及顏色的欄位將呈現灰色。
頁尾橫幅	輸入頁尾橫幅顯示的文字（最多 3,200 個字元）。
頁尾顏色	選取頁尾背景的顏色。預設（**None**（無））為透明背景。

© 2019 Palo Alto Networks, Inc.

項目	說明
頁尾文字顏色	選取頁尾文字的顏色。預設（**None**（無））為黑色。
最小密碼複雜性	
已啟用	啟用本機帳戶的最低密碼需求。在使用此功能的情況下，您可以確保防火牆上的本機管理員帳戶遵守一組定義的密碼需求。 您也可以建立含這些選項子集的密碼設定檔，其將覆蓋這些設定並可套用至特定帳戶。如需詳細資訊，請參閱 [裝置 > 密碼設定檔]，另請參閱使用者名稱與密碼需求以取得可用於帳戶之有效字元的相關資訊。 最大密碼長度為 *31* 個字元。避免 *PAN-OS* 不接受的設定要求。例如，請勿設定含 *10* 個大寫、*10* 個小寫、*10* 個數字以及 *10* 個特殊字元的需求，因為這會超出 *31* 個字元的最大長度。 如果您已設定高可用性 (HA)，請務必在設定密碼複雜度選項時使用主要端點，並在變更後快速認可。 最低密碼複雜度設定不適用於您指定 **Password Hash**（密碼雜湊）的本機資料庫帳戶（請參閱 [裝置 > 本機使用者資料庫 > 使用者]）。 需要強大的密碼才能防止暴力網路存取攻擊成功。需要最小長度並使用至少一個大寫字母、小寫字母、數字和特殊字元。此外，請避免在密碼中使用過多重複的字元以及使用者名稱、設定密碼重複使用頻率的限制，並設定密碼變更經常性週期，以便密碼不會長時間使用。密碼要求越強，攻擊者破解密碼的難度就越大。務必採用密碼強度最佳做法 以確保嚴格的密碼。
最小長度	需要最短密碼長度（範圍為 1 到 15 字元）。
最小大寫字母	需要最少大寫字母數（範圍為 0 到 15 字元）。
最小小寫字母	需要最少小寫字母數（範圍為 0 到 15 字元）。
最小數字字母	需要最少數字字母數（範圍為 0 到 15 字元）。
最小特殊字元	需要最少特殊（非英數）字母數（範圍為 0 到 15 字元）。
封鎖重複字元	指定密碼中允許的循序重複字元數（範圍是 2 到 15）。 若您將值設定為 2，則密碼可以連續包含兩次相同的字元，但若連續使用三次以上的相同字元，則密碼將遭到拒絕。 例如，若值設定為 2，則系統將接受密碼 test11 或 11test11，但不接受 test111，因為數字 1 連續出現三次。
Block Username Inclusion (including reversed)	選取此選項可防止在密碼中使用帳戶使用者名稱（或與名稱順序相反的字元）。
新密碼在字元數上有差異	在管理員變更其密碼時，字元必須根據指定值而有所不同。

© 2019 Palo Alto Networks, Inc.

項目	說明
需要在首次登入時變更密碼	選取此選項可提示管理員在首次登入防火牆時變更其密碼。
防止密碼重複使用限制	要求根據指定數量，不重複使用該數量的之前密碼。例如，如果將值設定為 4，您無法重複使用之前 4 個密碼的任何一個（範圍是 0 到 50）。
Block Password Change Period (days)	使用者在到達指定天數之前無法變更其密碼（範圍是 0 到 365 天）。
要求的密碼變更期間（天數）	要求管理員定期變更其密碼（以天數為單位）（範圍是 0 至 365 天）。例如，如果將值設定為 90，則將提示管理員每 90 天變更一次密碼。 您也可以設定 0 到 30 天的到期警告，並指定寬限期。
到期警告期間（天數）	如果設定 **Required Password Change Period**（要求密碼變更期間），則您可以使用此 **Expiration Warning Period**（到期警告期間）以當所需更改日期之前剩餘天數少於指定天數時，於每個日誌中提示使用者變更密碼（範圍為 0 到 30）。
到期後管理員的登入計數（計數）	允許管理員在請求更改日期後登入指定次數（範圍是 0 到 3）。例如，如果您將值設為 3 且他們的帳號已到期，則他們可以在帳戶被鎖定前，在不更改密碼的情況下，再登入 3 次。
Post Expiration Grace Period (days)	允許管理員在其帳戶過期後登入的指定天數（範圍是 0 到 30）。
AutoFocus™	
已啟用	啟用連接至 AutoFocus 入口網站的防火牆，以擷取威脅情報資料，並啟用防火牆與 AutoFocus 間的整合搜尋。 連接至 AutoFocus 後，防火牆將顯示與流量、威脅、URL 篩選、WildFire 提交及資料篩選日誌項目相關的 AutoFocus 資料（**Monitor**（監控）> **Logs**（日誌））。您可以在這些類型的日誌項目上按一下構件（例如 IP 位址或 URL），以顯示該構件的 AutoFocus 結果及統計資料。您接著可以直接從防火牆開啟展開的 AutoFocus 搜尋。 檢查 *AutoFocus* 授權在防火牆上已啟用（*Device*（裝置）> *Licenses*（授權））。如果 *AutoFocus* 授權不顯示，請使用其中一個 *License Management*（授權管理）選項來啟動授權。
AutoFocus URL	輸入 AutoFocus URL： `https://autofocus.paloaltonetworks.com:10443`
佇列逾時（秒）	設定防火牆嘗試查詢 AutoFocus 威脅情報資料的持續時間（以秒為單位）。如果 AutoFocus 入口網站在指定期間結束前未回應，防火牆將關閉連線。
Cortex Data Lake	

© 2019 Palo Alto Networks, Inc.

項目	說明
使用此區段來設定 VM 系列和以硬體為基礎的防火牆，以將日誌轉送到 Cortex Data Lake。下面是設定以下所述選項的完整工作流程： • 開始將日誌記錄到 Cortex Data Lake（不使用 Panorama） • 開始記錄到 Cortex Data Lake（適用於 Panorama 受管理防火牆） 日誌記錄服務現在稱為 *Cortex Data Lake*；但是，一些防火牆功能和按鈕仍然顯示「日誌記錄服務」名稱。	
啟用 Cortex Data Lake	選取此選項以允許防火牆（或者如果您使用的是 Panorama，則為屬於所選 **Template**（範本）的防火牆）將日誌轉送到 Cortex Data Lake（Cortex Data Lake 以前稱為「日誌記錄服務」）。 設定日誌轉送（Objects（物件）> Log Forwarding（日誌轉送））之後，防火牆會將日誌直接轉送到 Cortex Data Lake—對於 Panorama 受管理防火牆也是如此。
啟用重複記錄（僅限 Panorama 受管理防火牆）	**Enable Duplicate Logging**（啟用重複記錄）可除了將日誌傳送到 Cortex Data Lake 之外，繼續將日誌傳送給 Panorama 及分散式日誌收集器。 如果您要評估 Cortex Data Lake，則此選項非常有用—在啟用時，屬於選定範本的防火牆將儲存日誌複本至 Cortex Data Lake 和 Panorama 或散布式日誌收集架構中。
啟用強化應用程式記錄	如果您想要防火牆收集增加 Palo Alto Networks 應用程式網路可見度的資料，則請**Enable Enhanced Application Logging**（啟用強化應用程式日誌）。例如，此加強的網路可見度可讓 Palo Alto Networks Cortex XDR 應用程式更好地分類和建立一般網路活動的基準線，使得防火牆可以偵測到可能代表攻擊的異常行為。 強化應用程式日誌記錄需要日誌記錄服務 (Cortex Data Lake) 授權。您無法檢視這些日誌—它們設計僅能讓 Palo Alto Networks 應用程式占用。
地區	選取防火牆要將日誌轉送至的 Cortex Data Lake（日誌記錄服務）執行個體的地理位置。登入 Cortex 中樞以確認部署 Cortex Data Lake 執行個體所在的地區（在中樞中，選取頂端功能表列上的設定齒輪，然後按一下 **Manage Apps**（管理應用程式））。
PA-7000 系列與 PA-5200 系列防火牆的 Cortex Data Lake 的連線計數	（僅限 PA-7000 系列與 PA-5200 系列防火牆）指定用於將日誌從防火牆傳送到 Cortex Data Lake 的連線數（範圍是 1-20；預設值為 5）。您可以針對防火牆使用 **`request logging-service-forwarding status`** CLI 命令來驗證防火牆和 Cortex Data Lake 之間作用中的連線數。
不使用 Panorama 裝載 （適用於不受 Panorama 管理的防火牆）	可以允許不受 Panorama 管理的防火牆傳送日誌到 Cortex Data Lake。為此，首先需要在 Cortex Data Lake 應用程式中產生金鑰。此金鑰可讓防火牆驗證並安全連線至 Cortex Data Lake。產生金鑰之後，輸入金鑰，然後允許防火牆開始轉送日誌到 Cortex Data Lake。
記錄服務狀態	檢視連線至 Cortex Data Lake的連線狀態。**Show Status**（顯示狀態）以檢視以下檢查的詳細資訊：

© 2019 Palo Alto Networks, Inc.

項目	說明
	• **License**（授權）—成功或错误以指示防火牆是否具有將日誌轉發至 Cortex Data Lake 的有效授權。 • **Certificate**（憑證）—成功或错误以指示防火牆是否成功擷取向 Cortex Data Lake 驗證身份所需的憑證。 • **Customer Info**（客戶資訊）—成功或錯誤以指示防火牆是否具有使用 Cortex Data Lake 所需的客戶識別碼。當狀態為成功時，您也可以看到客戶識別碼。 • **Device Connectivity**（裝置連線）—指示防火牆是否已成功連線至 Cortex Data Lake。
SSH 管理設定檔設定	
伺服器設定檔	一種 SSH 服務設定檔，適用於網路上 CLI 管理連線的 SSH 工作階段。若要套用現有的伺服器設定檔，選取一個設定檔，按一下 **OK**（確定），然後 **Commit**（提交）您的變更。 您必須透過 *CLI* 執行 *SSH* 服務重新啟動，才能啟動設定檔。 如需詳細資訊，請參閱Device > Certificate Management > SSH Service Profile（裝置 > 憑證管理 > SSL 服務設定檔）。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Operations（裝置 > 設定 > 操作）

您可執行下列工作來管理防火牆與 Panorama™ 的執行中及候選組態。若您是使用 Panorama 虛擬裝置，也可以使用本頁面上的設定來設定傳統模式下 Panorama 虛擬裝置的日誌儲存分割區。

您必須在候選設定中認可變更以啟動這些變更，此時這些變更變為執行中設定的一部分。最佳做法是定期儲存候選設定。

您可使用 CLI 的安全複本 (SCP) 命令，將設定檔案、日誌、報告及其他檔案匯出至 *SCP* 伺服器，並將檔案匯入至另一個防火牆或 *Panorama M-Series* 或虛擬裝置。不過，由於日誌資料庫太大，無法在下列型號上實質匯出或匯入，因此不支援整個日誌資料庫的匯出或匯入：*PA-7000* 系列防火牆（所有 *PAN-OS®* 發行版本）、在 *Panorama 6.0* 或更新版本上執行的 *Panorama* 虛擬裝置以及 *Panorama M* 系列裝置（所有 *Panorama* 發行版本）。

功能	說明
設定管理	
還原為上次儲存的設定	還原候選設定（您選取 Web 介面右上方的 **Config**（設定）> **Save Changes**（儲存）時建立或覆寫的快照）的預設快照 (.snapshot.xml)。 （僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要還原的特定裝置群組、範本或範本堆疊設定。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
Revert to running config	還原最後一個執行中組態。此操作將復原自上次認可以來，每一位管理員對候選設定做出的變更。若只要還原特定管理員的變更，請參閱還原變更。 （僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要還原的特定裝置群組、範本或範本堆疊設定。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
儲存具名組態快照	建立不覆寫預設快照 (.snapshot.xml) 的候選設定快照。輸入快照 **Name**（名稱），或選取要覆寫的現有具名快照。 （僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要儲存的特定裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
儲存候選設定	使用目前的候選組態來建立或覆寫候選組態的預設快照 (.snapshot.xml)。這與選取 Web 介面右上方的 **Config**（設定）> **Save Changes**（儲存變更）時所進行的動作相同。若只要儲存特定管理員的變更，請參閱儲存候選組態。 （僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要儲存的特定裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
載入具名組態快照（防火牆） 或	使用下列其中一項來覆寫現有候選組態： • 自訂具名候選組態快照（而非預設快照）。 • 您匯入的自訂具名執行中組態。 • 目前執行中組態。

© 2019 Palo Alto Networks, Inc.

功能	說明
載入具名 Panorama 組態快照	組態必須位於防火牆上或是您要將其載入到的 Panorama 上。 選取組態的 **Name**（名稱）並輸入 **Decryption Key**（解密金鑰），其為防火牆或 Panorama 的主要金鑰（請參閱 [裝置 > 主要金鑰與診斷]）。需要主要金鑰才能解密組態內的所有密碼和私密金鑰。若您要載入匯入的組態，必須輸入您從中匯入的防火牆或 Panorama 主要金鑰。載入操作完成後，您載入組態的防火牆或 Panorama 主要金鑰會將密碼與私密金鑰重新加密。 若要在組態中為所有規則產生新 UUID（例如，如果您正在從其他防火牆載入組態，但在載入組態時想要保留該唯一規則），超級使用者必須為 **Regenerate Rule UUIDs for selected named configuration**（選定的具名組態重新產生規則 **UUID**），以便為所有規則產生新的 UUID。 （僅限 Panorama）透過選取以下內容，指定物件、原則、裝置群組或範本設定以從具名組態中部分載入設定： • **Load Shared Objects**（載入共用物件）—僅載入共用物件以及所有裝置群組和範本組態。 • **Load Shared Policies**（載入共用原則）—僅載入共用原則以及所有裝置群組和範本組態。 • **Select Device Groups & Templates**（選取裝置群組及範本）指定要載入的裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊 • **Retain Rule UUIDs**（保留規則 **UUID**）—將 UUID 保持在目前執行中組態中。
載入組態版本（防火牆） 或 載入 Panorama 組態版本	使用先前儲存於防火牆或 Panorama 上的執行中組態版本來覆寫現有候選組態。 選取組態的 **Name**（名稱）並輸入 **Decryption Key**（解密金鑰），其為防火牆或 Panorama 的主要金鑰（請參閱 [裝置 > 主要金鑰與診斷]）。需要主要金鑰才能解密組態內的所有密碼和私密金鑰。載入操作完成後，主要金鑰會將密碼與私密金鑰重新加密。 （僅限 Panorama）透過選取下列項目，指定物件、原則、裝置群組或範本組態以從具名設定中部分載入設定： • **Load Shared Objects**（載入共用物件）—僅載入共用物件以及所有裝置群組和範本組態。 • **Load Shared Policies**（載入共用原則）—僅載入共用原則以及所有裝置群組和範本組態。 • **Select Device Groups & Templates**（選取裝置群組及範本）指定要載入的裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊
匯出具名組態快照	匯出目前的執行中組態，即候選組態快照，或之前匯入的組態（候選後執行中）。防火牆將組態匯出為使用指定名稱的 XML 檔案。您可在任何網路位置儲存快照。 （僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要匯出的特定裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
匯出組態版本	匯出 XML 檔案格式的執行中設定 **Version**（版本）。

© 2019 Palo Alto Networks, Inc.

功能	說明
	（僅限 Panorama）**Select Device Groups & Templates**（選取裝置群組以及範本）選取要匯出的特定裝置群組、範本或範本堆疊組態。裝置群組以及範本管理員只能選取在其指派的存取網域中指定的裝置群組、範本或範本堆疊。
匯出設定搭售以供 Panorama，並將所有裝置放入一個套件內 （僅限 Panorama）	產生並匯出 Panorama 執行組態備份和每個受管理防火牆的最新版本。若要將每天建立組態套件，並將該套件匯出至 SCP 或 FTP 伺服器的程序自動化，請參閱 [Panorama > 裝置部署]。
匯出或推送裝置設定包 （僅限 Panorama）	系統會提示您選取防火牆，並針對儲存在 Panorama 上的防火牆組態，執行下列其中一個動作： • **Push & Commit**（推送和提交）組態至防火牆。此動作會清理防火牆（移除任何其中的本機組態）並推送儲存在 Panorama 上的防火牆組態。匯入防火牆組態後，使用此選項以清理防火牆，以便您可以使用 Panorama 進行管理。 • 將組態 **Export**（匯出）至防火牆，但不進行載入。若要載入組態，您必須存取防火牆 CLI 並執行設定模式命令 **load device-state**。此命令會清理防火牆，方式如同 **Push & Commit**（推送和提交）選項。 這些選項僅在執行 *PAN-OS 6.0.4* 及更新版本的防火牆上可用。
匯出裝置狀態 （僅限防火牆）	匯出防火牆狀態資訊包。除了執行中組態，狀態資訊還包括從 Panorama 推送的裝置群組及範本設定。如果防火牆是 GlobalProtect™ 入口網站，資訊包還將包含憑證資訊、入口網站管理的衛星清單以及衛星驗證資訊。如果取代防火牆或入口網站，您可透過匯入狀態包來還原取代時匯出的資訊。 您必須手動執行防火牆狀態匯出或建立排程 *XML API* 指令碼，才能將檔案匯出至遠端伺服器。此操作應定期執行，因為衛星憑證經常變更。 若要從 CLI 建立防火牆狀態檔案，請從組態模式執行 **`save device state`**（儲存裝置狀態）指令。會將檔案命名為 `device_state_cfg.tgz` 並儲存在 `/opt/pancfg/mgmt/device-state` 中。匯出防火牆狀態檔案的操作命令是 **`scp export device-state`**（您也可以使用 **`tftp export device-state`**）。 如需使用 XML 或 REST API 的詳細資訊，請參閱《PAN-OS 和 Panorama API 指南》。
Import named config snapshot	從任何網路位置匯入執行中或候選組態。按一下 **Browse**（瀏覽）並選取要匯入的組態檔案。
匯入裝置狀態 （僅限防火牆）	當您選取 **Export device state**（匯出裝置狀態）時匯入您從防火牆匯出的狀態資訊包。除了執行中設定，狀態資訊還包括從 Panorama 推送的裝置群組及範本設定。如果防火牆是 GlobalProtect 入口網站，資訊包還將包含憑證資訊、衛星清單以及衛星驗證資訊。如果取代防火牆或入口網站，您可透過匯入狀態包來還原取代時的資訊。
將裝置組態匯入至 Panorama （僅限 Panorama）	將防火牆組態匯入至 Panorama。Panorama 會自動建立範本以包含網路和裝置組態。針對防火牆上的每個虛擬系統 (vsys)，Panorama 會自動建立裝置群組以包含原則和物件組態。裝置群組在階層中將位於共用位置的下一個層級，但您

© 2019 Palo Alto Networks, Inc.

功能	說明

	可以在完成匯入後將他們重新指派至不同的父系裝置群組（請參閱 [Panorama > VMware NSX]）。
	
	Panorama 上的內容版本（例如，應用程式與威脅資料庫）必須與您將匯入組態之防火牆上的版本相同或更高。
	
	設定下列匯入選項：
	• 裝置—選取 Panorama 將從其匯入組態的防火牆。下拉式清單僅會包含連線至 Panorama 的防火牆，且不會指派至任何裝置群組或範本。您僅可以選取一整個防火牆而非個別的 vsys。
	• 範本名稱—輸入將包含已匯入裝置和網路設定的範本名稱。針對多 VSYS 防火牆，此欄位為空白。針對其他防火牆，預設值為防火牆名稱。您無法使用現有範本的名稱。
	• 裝置群組名稱首碼（僅限於多重 vsys 防火牆）—您可以選取性地新增字元字串，作為每個裝置群組名稱的首碼。
	• 裝置群組名稱—針對多重 VSYS 防火牆，每個裝置群組依預設具有一個 vsys 名稱。針對其他防火牆，預設值為防火牆名稱。您可以編輯預設名稱，但無法使用現有裝置群組的名稱。
	• 將裝置共用物件匯入至 **Panorama** 的共用內容（預設啟用）— Panorama 會選取此選項，這表示 Panorama 會將屬於在防火牆中 Shared（共用）的物件，匯入在 Panorama 中共用的內容。
	
	Panorama 會將所有物件視為在防火牆上共用而無多個虛擬系統。若您停用此選項，*Panorama* 會將共用的防火牆物件複製至裝置群組而非共用的內容。此設定具有下列例外狀況：
	
	  • 若共用的防火牆物件與現有共用的 Panorama 物件具有相同的名稱和值，則匯入會排除防火牆物件。
	  • 若共用的防火牆物件與共用的 Panorama 物件不具有相同的名稱和值，則 Panorama 會將防火牆物件匯入至每個裝置群組。
	  • 若匯入至範本的組態參考共用的防火牆物件，則 Panorama 會將物件匯入至 Shared（共用）的內容，無論您是否選取此選項。
	  • 若共用的防火牆物件參考匯入至範本的組態，則 Panorama 會將物件匯入至裝置群組，無論您是否選取此選項。
	• 規則匯入位置 — 選取 Panorama 將以預先規則或後續規則來匯入原則。無論您的選取為何，Panorama 會將預設安全性規則（intrazone 規則和 interzone 規則）匯入至後續規則庫。
	
	若 *Panorama* 的規則與您所匯入之防火牆規則具有相同名稱，則 *Panorama* 會同時顯示兩個規則。不過，規則名稱必須為唯一：請在 *Panorama* 上執行認可之前刪除其中一個規則，否則認可將失敗。

裝置操作	
重新啟動	若要重新啟動防火牆或 Panorama，則重新啟動裝置。防火牆或 Panorama 會將您登出、重新載入軟體（PAN-OS 或 Panorama）和使用中組態、關閉並記錄現有工作階段，以及建立系統日誌以顯示啟動關閉的管理員名稱。尚未儲存或認可的任何組態變更都會遺失（請參閱（Device > Setup > Operations（裝置 > 設定 > 操作））。

© 2019 Palo Alto Networks, Inc.

功能	說明
	如果沒有 *Web* 介面，請使用下列操作的 *CLI* 指令： **`request restart system`**
關機	若要對防火牆或 Panorama 執行非失誤性關閉，則 **Shutdown Device**（關閉裝置）或 **Shutdown Panorama**（關閉 **Panorama**），然後在提示時按一下 **Yes**（是）。尚未儲存或已認可的任何組態變更遺失。所有管理員都將登出，並將發生下列程序： • 所有登入工作階段都將登出。 • 介面將停用。 • 所有系統程序都將停止。 • 現有工作階段將關閉及記錄。 • 將建立系統日誌，顯示啟動關閉的管理員名稱。如果此日誌項目無法寫入，則會出現警告，且系統將不會關閉。 • 將徹底卸載磁碟機並關閉防火牆或 Panorama 的電源。 您必須在拔下電源後重新插上，然後才能開啟防火牆或 Panorama 的電源。 如果沒有 *Web* 介面，請使用下列 *CLI* 命令： **`request shutdown system`**
重新啟動資料背板	**Restart Dataplane**（重新啟動資料平面）以重新啟動防火牆的資料功能而不重新啟動裝置，。Panorama 或 PA-220、PA-800 Series 或 VM-Series 防火牆上不提供此選項。 如果沒有 *Web* 介面，請使用下列 *CLI* 命令： ***`request restart dataplane`*** 在 PA-7000 Series 防火牆上，每個 NPC 都有資料平面，因此您可以重新啟動 NPC 來執行此操作，方法是執行此指令 **`request chassis restart slot`**.
雜項	
自訂標誌	使用 **Custom Logos**（自訂標誌）可自訂下列任何資訊： • **Login Screen**（登入畫面）背景影像 • **Main UI**（主要 UI）（使用者介面）標頭影像 • **PDF Report Title Page**（PDF 報告的標題頁面）影像。請參考 [監控 > PDF 報告 > 管理 PDF 摘要]。 • **PDF Report Footer**（PDF 報告的頁尾）影像 上傳（<image>）影像檔以預覽它或刪除（）之前上傳的影像。 若要返回預設標誌，請移除您的項目然後 **Commit**（認可）。 對於 **Login Screen**（登入畫面）和 **Main UI**（主要 UI），您可以在它將出現時顯示（）；如必要，防火牆會裁剪影像以符合要求。對於 PDF 報告，防火牆會自

© 2019 Palo Alto Networks, Inc.

功能	說明
	動重新調整影像尺寸，而不用裁剪以符合要求。在所有情況下，預覽會顯示建議的影像尺寸。 任何標誌的影像最大尺寸是 128KB。支援的檔案類型是 png、gif 和 jpg 格式。防火牆不支援交錯式影像檔案或包含 Alpha 色頻的影像檔案，因為此類檔案會干擾 PDF 報告檔的生成。您可能需要聯絡建立影像的製圖者來移除影像的 Alpha 色頻，或確定您正在使用的圖形軟體並未儲存包含 Alpha 色頻功能的檔案。 如需產生 PDF 報告的資訊，請參閱 [監控 > PDF 報告 > 管理 PDF 摘要]。
SNMP 設定	啟用 SNMP 監控。
儲存分割區設定（僅限 Panorama）	傳統模式下 Panorama 虛擬裝置的日誌儲存分割區。

啟用 SNMP 監控

- Device > Setup > Operations（裝置 > 設定 > 操作）

簡易網路管理通訊協定 (SNMP) 是在網路上監控裝置的標準通訊協定。選取 **Operations**（操作）頁面來設定防火牆，以便使用您 SNMP 管理員所支援的 SNMP 版本（SNMPv2c 或 SNMPv3）。針對 MIB 清單，您必須載入至 SNMP 管理員，以便其可以判讀從 防火牆收集而來的統計，請參閱支援的 MIB。若要設定伺服器設定檔，使防火牆與您網路上的 SNMP 設陷目的地通訊，請參閱 設備 > 伺服器設定檔 > SNMP 設陷。SNMP MIB 會定義防火牆產生的所有 SNMP 陷阱。SNMP 陷阱可識別包含唯一物件 ID (OID) 的事件，並將個別欄位定義成變數繫結 (varbind) 清單。按一下 **SNMP Setup**（**SNMP** 設定）並指定下列設定，允許來自 SNMP 管理員的 SNMP GET 要求：

欄位	說明
實體位置	指定防火牆的實體位置。產生日誌或陷阱時，此資訊可讓您識別（在 SNMP 管理員中）產生通知的防火牆。
聯絡人	輸入負責維護防火牆之人員的名稱或電子郵件地址。會在標準系統資訊 MIB 中報告此設定。
Use Specific Trap Definitions	依預設會選取此選項，這表示防火牆會根據事件類型針對每個 SNMP 設陷使用唯一的 OID。若您清除此選項，則每個設陷將具有相同的 OID。
版本	選取 SNMP 版本：**V2c** (預設) 或 **V3**。您的選取項目會控制對話方塊所顯示的剩餘欄位。
適用於 **SNMP V2c**	
SNMP 社群字串	輸入社群子串以便識別 SNMP 管理員的 SNMP 社群和受監控裝置，同時也在社群成員交換 SNMP GET（統計要求）和設陷訊息時，作為密碼以進行彼此驗證。字串最多可以包含 127 個字元，接受所有字元，且區分大小寫。 請勿使用預設社群字串 *public*。因為 *SNMP* 訊息包含純文字的社群字串，當您定義社群成員（管理員存取）時，請考慮網路的安全性需求。

© 2019 Palo Alto Networks, Inc.

欄位	說明
適用於 **SNMP V3**	
名稱/檢視	您可以將一個或多個檢視的群組指派給 SNMP 管理員的使用者，以控制使用者可以從防火牆取得的 MIB 物件（統計）。每個檢視有一組配對的 OID 和 Bitwise 遮罩：OID 會指定一個 MIB，而遮罩（使用十六進位格式）會指定在 MIB 之中（包含相符）或之外（排除相符）的相關聯物件。 例如，若 **OID** 為 1.3.6.1，則比對選項會設定為包含，且遮罩為 0xf0，接著使用者要求的物件必須具有符合 1.3.6.1 中前四個節點 (f = 1111) 的 OID。物件不需要符合剩餘的節點。在此範例中，1.3.6.1.2 符合遮罩，但 1.4.6.1.2 則不相符。 針對每個檢視群組，按一下 **Add**（新增），輸入群組的 （名稱），然後針對您要 **Add**（新增）至群組的每個檢視進行下列設定： • 檢視 — 指定檢視的名稱。名稱最多可以包含 31 個字元，可以使用英數字元、句號、底線或連字號。 • **OID**—指定 MIB 的 OID。 • 選項 — 選取比對邏輯以套用至 MIB。 • 遮罩 — 指定十六進位格式的遮罩。 為了提供所有管理資訊的存取權，請使用最上層的 *OID 1.3.6.1*，將 *Mask*（遮罩）設定為 *0xf0*，並將比對 *Option*（選項）設定為 *include*（包含）。
使用者	當防火牆轉送設陷，且 SNMP 管理員取得防火牆統計時，SNMP 使用者帳戶會提供驗證、隱私權和存取控制。針對每個使用者，請按一下 **Add**（新增），並進行下列設定： • 使用者 — 指定使用者名稱以識別 SNMP 使用者帳戶。您在防火牆上設定的使用者名稱必須與 SNMP 管理員上所設定的使用者名稱相符。使用者名稱最多可包含 31 個字元。 • 檢視—將檢視群組指派給使用者。 • 驗證密碼—指定使用者的驗證密碼。當防火牆轉送陷阱並回應統計要求時，會使用密碼來驗證 SNMP 管理員。防火牆會使用安全雜湊演算法 (SHA-1 160) 將密碼加密。密碼必須為 8-256 個字元，且允許使用所有字元。 • 私人密碼 — 指定使用者的私人密碼。防火牆會使用密碼和進階加密標準 (AES-128) 來加密 SNMP 陷阱並回應統計要求。密碼必須為 8-256 個字元，且允許使用所有字元。

© 2019 Palo Alto Networks, Inc.

Device > Setup > HSM（裝置 > 設定 > HSM）

選取 **Device**（裝置）> **Setup**（設定）> **HSM** 可設定硬體安全性模組 (HSM)、執行操作並檢視 HSM 狀態。

您想了解什麼內容？	請參閱：
硬體安全性模組 (HSM) 的目的是什麼？可以在哪裡找到詳細的設定程序？	使用硬體安全性模組保護金鑰
設定：	硬體安全性模組提供者設定
	HSM 驗證
執行硬體安全性操作	硬體安全性操作
如何檢視 HSM 狀態？	硬體安全性模組提供者組態和狀態
	硬體安全性模組狀態

硬體安全性模組提供者設定

若要在防火牆上設定硬體安全性模組 (HSM)，請編輯 [硬體安全性模組提供者] 設定：

硬體安全性模組提供者設定	說明
設定的提供者	選取 HSM 廠商： • **None**（無）（預設）—防火牆未連接任何 HSM。 • **SafeNet Network HSM** • **nCipher nShield Connect** *HSM* 伺服器版本必須與防火牆上的 HSM client version（HSM 用戶端版本）相容。
模組名稱	新增 HSM 的模組名稱。這可為任何 ASCII 字串，最長 31 個字元。如果您正設定獨立或高可用性的 SafeNet HSM 組態，新增模組名稱最多為 16 個。
伺服器位址	對正在設定的任何 HSM 模組指定 IPv4 位址。
high availability (高可用性) （僅限 SafeNet Network）	（選用）若是在高可用性組態中設定 SafeNet HSM 模組，請選取此選項。您必須為每個 HSM 模組設定模組名稱與伺服器位址。
自動復原重試	指定在容錯轉移至 HSM HA 組態中的其他 HSM 之前，防火牆將嘗試復原其 HSM 連線的次數（範圍是 0 到 500；預設為 0）。

© 2019 Palo Alto Networks, Inc.

硬體安全性模組提供者設定	說明
（僅限 SafeNet Network）	
高可用性群組名稱 （僅限 SafeNet Network）	指定使用於 HSM HA 群組的群組名稱。此名稱由防火牆內部使用。可為任何 ASCII 字串，最長 31 個字元。
移除檔案系統位址 （僅限 nCipher nShield Connect）	在 nShield Connect HSM 設定中使用的遠端檔案系統的 IPv4 位址。

HSM 驗證

選取 **Setup Hardware Security Module**（設定硬體安全性模組），及進行下列設定來驗證至 HSM 的防火牆。

HSM 模組驗證	
伺服器名稱	從下拉式清單中選取 HSM 伺服器名稱，然後選取是否要使用自動或手動產生的憑證進行驗證並建立信任。 • **Automatic**（自動） • **Manual**（手動） 如果選取 **Manual**（手動），您需要匯入並安裝 HSM 伺服器手動產生的憑證。匯出 HSM 用戶端憑證以安裝在 HSM 伺服器上。
管理員密碼	輸入 HSM 的管理員密碼，以驗證 HSM 的防火牆。

硬體安全性操作

若要在 硬體安全性模組（HSM）或連接至該 HSM 的防火牆執行一項操作，則選取 **Device**（設備）> **Setup**（設定）> **HSM** 並在下列確體安全性操作中選取一項：

硬體安全性操作	
設定硬體安全性模組	設定使用 HSM 驗證的防火牆。
顯示詳細資訊	顯示 HSM 伺服器相關資料、HSM 高可用性和 HSM 硬體。
與遠端檔案系統同步（僅限 nCipher nShield Connect）	將 nShield Connect 遠端檔案系統中的重要資料同步至防火牆。
重設組態	移除所有至防火牆的 HSM 連線。您必須在重設 HSM 設定後，重覆所有驗證程序。

© 2019 Palo Alto Networks, Inc.

硬體安全性操作	
選取 HSM 用戶端版本（僅限 SafeNet 網路）	讓您可以選擇在 HSM 用戶端（防火牆）執行的軟體版本。HSM 用戶端版本必須與 HSM 伺服器版本相容。參閱用戶端伺服器版本相容指標的 HSM 廠商文件。

硬體安全性模組提供者組態和狀態

[硬體安全性模組提供者] 區段會顯示 HSM 組態設定和 HSM 的連線狀態。

硬體安全性模組提供者狀態	
設定的提供者	選取防火牆上所設定的 HSM 廠商： • 無 • **SafeNet Network HSM** • **nCipher nShield Connect**
high availability (高可用性)	（僅限 SafeNet Network）如果核取則設定 HSM 高可用性。
高可用性群組名稱	（僅限 SafeNet Network）在防火牆上為 HSM 高可用性設定的群組名稱。
遠端檔案系統位址	（僅限 nShield Connect）遠端檔案系統的位址。
防火牆來源位址	使用於 HSM 服務之連接埠的位址。預設為管理連接埠位址。但可透過 **Device**（設備）> **Setup**（設定）> **Services**（服務）中的 [服務路由設定]，將其指定為不同的連接埠。
防火牆上的 HSM 用戶端版本	顯示安裝的 HSM 用戶端版本。
HSM 保護的主要金鑰	如果核取，會在 HSM 上保護主要金鑰。
STATUS (狀態)	如果防火牆已連線到 HSM 並向其進行驗證，則會顯示綠色，如果防火牆未驗證或已中斷與 HSM 的網路連線，則會顯示紅色。 您也可以參閱硬體安全性模組狀態，以深入了解 HSM 連線。

硬體安全性模組狀態

Hardware Security Module（硬體安全性模組狀態）包含下列已成功驗證的t HSMs 相關資訊。依據設定的 HSM 提供者（SafeNet 或 nCipher），畫面可能不同。

硬體安全性模組狀態	
SafeNet Network HSM	• 序號—如果已成功驗證 HSM 分割區，則顯示 HSM 分割區的序號。 • 分割區—防火牆上所指派 HSM 的分割區名稱。 • 模組狀態—HSM 連線的目前操作狀態。若此表格中顯示了 HSM，則此欄位會顯示 **Authenticated**（已驗證）。

© 2019 Palo Alto Networks, Inc.

硬體安全性模組狀態	
nCipher nShield Connect HSM	• 名稱—HSM 的伺服器名稱。 • **IP** 位址—防火牆上所指派之 HSM 的 IP 位址。 • 模組狀態—HSM 連線的目前操作狀態。如果防火牆已成功地向 HSM 進行驗證，此設定會顯示 **Authenticated**（已驗證），如果驗證失敗，則會顯示 **Not Authenticated**（未驗證）。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Services（裝置 > 設定 > 服務）

下列主題說明防火牆上的全域和虛擬系統服務設定：

- 設定全域和虛擬系統的服務
- 全域服務設定
- 服務路由組態的 IPv4 和 IPv6 支援
- 目的地服務路由

設定全域和虛擬系統的服務

在啟用多重虛擬系統的防火牆上選取 **Services**（服務）可顯示 **Global**（全域）和 **Virtual Systems**（虛擬系統）頁籤，而您可以在其中個別設定防火牆或其虛擬系統用來增加操作效率的服務。（如果防火牆是單一虛擬系統，或已停用多重虛擬系統，則不會顯示 **Virtual Systems**（虛擬系統）頁籤。）

選取 **Global**（全域）可針對整個防火牆設定服務。這些設定也可針對不具有自訂服務設定的虛擬系統作為預設值。

- 編輯 服務/**URL** 類別**s**（服務），以定義 DNS 伺服器、更新伺服器和 代理程式 伺服器的 IP 位址。使用專屬的 **NTP** 頁籤以進行網路時間通訊協定設定。如需可用服務選項的欄位說明，請參閱表 12。
- 在 服務/**URL** 類別 **Features**（服務功能）中，按一下 服務/**URL** 類別 **Route Configuration**（服務路由組態）以指定防火牆如何針對服務與其他伺服器/設備進行通訊，例如 DNS、電子郵件、LDAP、RADIUS、系統日誌等。有兩種方法可設定全域服務路由：
  - **Use Management Interface for all**（針對所有使用管理介面）選項將強制所有防火牆服務透過管理介面 (MGT) 與外部伺服器進行通訊。若您選取此選項，您必須將 MGT 介面設定為允許在防火牆與提供服務的伺服器/設備之間進行通訊。若要設定 MGT 介面，請選取 [設備 > 設定 > 管理]，並編輯設定。
  - **Customize**（自訂）選項可讓您透過設定特定來源介面和 IP 位址來精確控制服務通訊，而服務會將其用於目的地介面，且根據其回應決定目的地 IP 位址。（例如，您可以為防火牆與電子郵件伺服器之間的所有電子郵件通訊設定特定的來源 IP/介面，並為 Palo Alto Networks 服務使用不同的來源 IP/介面。）選取您要自訂的一個或多個服務以便進行相同設定，然後按一下 **Set Selected** 服務/**URL** 類別 **Routes**（設定選取的服務路由）。服務會列於表 13 中，指出服務可針對 **Global**（全域）防火牆還是 **Virtual Systems**（虛擬系統）進行設定，以及服務是否支援 IPv4 和/或 IPv6 來源位址。

Destination（目的地）頁籤是另一個您可以進行自訂的全域服務路由功能。此頁籤會出現在 [服務路由設定] 視窗中，且在目的地服務路由中有相關說明。

使用虛擬系統頁籤以指定單一虛擬系統的服務路由。選取一個位置（虛擬系統）並按一下服務路由組態。選取 **Inherit Global** 服務/**URL** 類別 **Route Configuration**（繼承全域服務路由設定）或自訂虛擬系統的服務路由。若您選擇自訂設定，請選取 **IPv4** 或 **IPv6**。選取您要自訂的一個或多個服務以便進行相同設定，然後按一下 **Set Selected** 服務/**URL** 類別 **Routes**（設定選取的服務路由）。若想了解哪些服務可進行自訂，請參閱表 13。

若要控制和重新導向共用和特定虛擬系統之間的 DNS 查詢，您可以使用 DNS Proxy 和 DNS 伺服器設定檔。

全域服務設定

- Device > Setup > Services（裝置 > 設定 > 服務）

若要控制和重新導向共用和特定虛擬系統之間的 DNS 查詢，您可以使用 DNS Proxy 和 DNS 伺服器設定檔。

© 2019 Palo Alto Networks, Inc.

全域服務設定	說明
服務	
更新伺服器	代表用來從 Palo Alto Networks 下載更新的伺服器 IP 位址或主機名稱。目前的值是 **updates.paloaltonetworks.com**。除非技術支援指示，否則請勿變更伺服器名稱。
驗證更新伺服器身分識別	若您啟用此選項，防火牆或 Panorama 將驗證自其下載軟體或內容套件的伺服器，是否具有受信任憑證授權單位所簽署的 SSL 憑證。這會讓防火牆 或 Panorama 伺服器與更新伺服器之間的通訊，增加額外的安全性層級。 驗證更新伺服器身分識別以驗證伺服器是否具有由受信任授權單位簽署的 *SSL* 憑證。
DNS 設定	選擇 DNS 服務類型—**Servers**（伺服器） 或 **DNS Proxy Object**（DNS Proxy 物件）—對所有 DNS 查詢而言，防火牆啟動可支援 FQDN 位址物件、日誌記錄和防火牆管理。選項包括： • 用來提供網域名稱解析的主要與次要 DNS 伺服器 • 已在防火牆上進行設定的 DNS Proxy 是用來設定 DNS 伺服器的替代方案。如果您啟用 DNS proxy，則必須啟用 **Cache**（快取）和 **EDNS Cache Responses**（**EDNS** 快取回應）（**Network**（網絡） > **DNS Proxy** > **Advanced**（進階））。
主要 DNS 伺服器	為來自防火牆的 DNS 查詢輸入主要 DNS 伺服器的 IP 位址。例如，找到更新伺服器、解析在日誌中的 DNS 或解析以 FDQN 為基礎的位址物件。
次要 DNS 伺服器	（選用）輸入當主要伺服器不可用時，您要使用的次要 DNS 伺服器 IP 位址。
FQDN 重新整理時間下限（秒）	對防火牆重新整理從 DNS 接收之 FQDNs 的速度設定限制。只要 TTL 大於或等於這個 **Minimum FQDN Refresh Time**（**FQDN** 重新整理時間下限）（秒），防火牆就會根據 FQDN 的 TTL 重新整理 FQDN。如果 TTL 小於這個 Minimum FQDN Refresh Time（FQDN 重新整理時間下限），則防火牆將根據這個 Minimum FQDN Refresh Time（FQDN 重新整理時間下限）重新整理 FQDN（即，防火牆不會支援比此設定更快的 TTLs）。計時器會在防火牆從 DNS 伺服器或 DNS Proxy 物件接收到 DNS 回應時開始解析 FQDN（範圍為 0 至 14,400；預設值為 30）。設定為 0 表示防火牆將根據 DNS 中的 TTL 值重新整理 FQDN，並且不會強制執行 FQDN 重新整理時間下限。 如果 *DNS* 中 *FQDN* 的 *TTL* 很短，但 *FQDN* 解析不會像 *TTL* 時間範圍那樣頻繁變更，因此不需要更快的重新整理，則應設定 *FQDN* 重新整理時間下限以避免不必要的 *FQDN* 重新整理嘗試。
FQDN 失效項目逾時（分鐘）	指定防火牆在網路出現故障或無法存取 DNS 伺服器時繼續使用 FQDN 失效解析的時間長度（分鐘）—當未重新整理 FQDN 時（範圍為 0 至 10,080；預設值為 1,440）。值 0 表示防火牆不會繼續使用失效項目。如果在狀態逾時結束時仍無法存取 DNS 伺服器，則 FQDN 項目將無法解析（會移除失效解析）。 確保 *FQDN Stale Entry Timeout*（*FQDN* 失效項目逾時）值足夠短，不允許錯誤的流量轉送（這會帶來安全風險），但足夠長，便可在不導致意外網路故障的情況下實現流量連續性。
Proxy 伺服器區段	

© 2019 Palo Alto Networks, Inc.

全域服務設定	說明
伺服器	如果防火牆需要使用 Proxy 伺服器才能取得 Palo Alto Networks 更新服務，請輸入 Proxy 伺服器的 IP 位址或主機名稱。
連接埠	輸入 Proxy 伺服器的連接埠。
使用者	輸入管理員使用者名稱用來在存取 Proxy 伺服器時進入。
密碼/確認密碼	輸入並確認管理員用來存取 Proxy 伺服器的密碼。
使用 Proxy 傳送日誌至 Cortex 資料湖	使防火牆能夠透過 Proxy 伺服器將日誌傳送到 Cortex Data Lake。
NTP	
NTP 伺服器位址	輸入要用來同步防火牆時鐘之 NTP 伺服器的 IP 位址或主機名稱。您可選擇輸入當主要伺服器變成不可用時，要用來同步防火牆時鐘之第二部 NTP 伺服器的 IP 位址或主機名稱。 當 *NTP* 伺服器保持所有網路防火牆時鐘同步時，排程工作會按預期運行，時間戳記可幫助確定與多個裝置相關的問題的根本原因。設定主要和次要 *NTP* 伺服器，以防無法存取主要 *NTP* 伺服器。

驗證類型	您可以啟用防火牆以驗證來自 NTP 伺服器的時間更新。對於每一部 NTP 伺服器，選取防火牆要使用的驗證類型：
	• 無—（預設）選取此選項可停用 NTP 驗證。
	• 對稱金鑰—選取此選項可讓防火牆使用對稱金鑰交換（共用密碼）來驗證 NTP 伺服器的時間更新。如果選取對稱金鑰，請指定下列值以繼續執行：
	  • 金鑰 **ID**—輸入金鑰 ID (1-65534)。
	  • 演算法—選取 MD5 或 SHA1 演算法以用來為 NTP 進行驗證。
	  • 驗證金鑰/確認驗證金鑰 — 輸入並確認驗證演算法的驗證金鑰。
	• 自動金鑰—選取此選項可讓防火牆使用自動金鑰（公開金鑰密碼編譯）來驗證 NTP 伺服器的時間更新。
	
	啟用 *NTP* 伺服器驗證，以便 *NTP* 伺服器核准用戶端並提供同步更新。

服務路由組態的 IPv4 和 IPv6 支援

下表顯示全域和虛擬系統上服務路由組態的 IPv4 和 IPv6 支援。

服務路由組態設定	全域		虛擬系統	
	IPv4	IPv6	IPv4	IPv6
AutoFocus—AutoFocus™ 伺服器。	✓	—	—	—

© 2019 Palo Alto Networks, Inc.

服務路由組態設定	全域		虛擬系統	
	IPv4	IPv6	IPv4	IPv6
CRL 狀態 — 憑證撤銷清單 (CRL) 伺服器。	✓	✓	—	—
DDNS—動態 DNS 服務。	✓	✓	✓	✓
Panorama 推送的更新—從 Panorama™ 部署過來的內容和軟體更新。	✓	✓	—	—
DNS—網路名稱系統伺服器。 * 針對虛擬系統，DNS 已在 DNS 伺服器設定檔上完成設定。	✓	✓	✓ *	✓ *
外部動態清單—外部動態清單的更新。	✓	✓	—	—
Email—Email 伺服器。	✓	✓	✓	✓
HSM—硬體安全性模組伺服器。	✓	—	—	✓
HTTP—HTTP 轉送。	✓	✓	✓	✓
Kerberos—Kerberos 驗證伺服器。	✓	—	✓	✓
LDAP — 輕量型目錄存取通訊協定伺服器。	✓	✓	✓	✓
MDM—移動裝置管理伺服器。	✓	✓	—	—
多因素驗證—多因素驗證 (MFA) 伺服器。	✓	✓	✓	✓
NetFlow—用來收集網路流量統計的 NetFlow 收集器。	✓	✓	✓	✓
NTP—網路時間通訊協定伺服器。	✓	✓	—	—
Palo Alto Networks 服務—來自 Palo Alto Networks® 和 WildFire® 公共伺服器的更新。這也是用來將預先 10.0 遙測資料轉送至 Palo Alto Networks 的服務路由。（目前的遙測支援將其資料轉送至 Cortex Data Lake。在該情況下，不使用此服務路由。）	✓	—	—	—
Panorama—Panorama 管理伺服器。	✓	✓	—	—
Panorama Log Forwarding（**Panorama** 日誌轉送）（僅限 PA-5200 系列防火牆）—從防火牆到日誌收集器的日誌轉送。	✓	✓	—	—
Proxy — 作為防火牆 Proxy 的伺服器。	✓	✓	—	—

© 2019 Palo Alto Networks, Inc.

服務路由組態設定	全域		虛擬系統	
	IPv4	IPv6	IPv4	IPv6
RADIUS — 遠端驗證撥入使用者服務伺服器。	✓	✓	✓	✓
SCEP — 要求與散佈用戶端憑證的簡易憑證註冊通訊協定。	✓	✓	✓	—
SNMP 設陷—簡易網路管理通訊協定設陷伺服器。	✓	—	✓	—
Syslog—用來記錄系統訊息的伺服器。	✓	✓	✓	✓
TACACS+—用於驗證、授權和會計 (AAA) 服務的終端機存取控制器存取控制系統 Plus (TACACS+) 伺服器。	✓	✓	✓	✓
UID Agent（**UID** 代理程式）—User-ID 代理程式伺服器。	✓	✓	—	✓
URL 更新 — 統一資源定位器 (URL) 更新伺服器。	✓	✓	—	—
VM 監控—當您啟用 Device > VM Information Sources（裝置 > VM 資料來源）時監控虛擬機器資料。 *VM-Series* 防火牆在公共雲中的部置，以監控虛擬機器，必須使用 *MGT* 介面。您無法使用數據平面介面作為服務路由。	✓	✓	✓	✓
Wildfire Private — 私人 Palo Alto Networks WildFire 伺服器。	✓	—	—	—

當自訂一個 **Global**（全域）服務路由時，選取 **Service Route Configuration**（服務路由組態），然後在 **IPv4** 或 **IPv6** 頁籤上，選取一個來自可用服務清單的服務；您也可以選取多重服務與 **Set Selected Service Routes**（設定選取的服務路由）以立即設定多重服務路由。若要限制在 **Source Address**（來源位址）下拉式清單中的選項，請選取一個 **Source Interface**（來源介面），然後從介面選取一個 **Source Address**（來源位址）。設定為 **Any**（任何）的來源介面可讓您從可用的任何介面中選取來源位址。來源位址顯示指定給所選介面的 IPv4 或 IPv6 位址，選取的 IP 位址將是服務流量的來源。如果您想要防火牆使用服務路由的管理介面，您可以 **Use default**（使用預設），不過，如果封包目的地 IP 位址符合所設定的目的地 IP 位址，則將設定來源 IP 位址為針對目的地設定的來源位址。您不必定義目的地位址，因為您設定每個服務時也會設定目的地。例如，當您定義 DNS 伺服器時（**Device**（裝置）> **Setup**（設定）> **Services**（服務）），您將設定 DNS 查詢的目的地。您可以為服務同時指定 IPv4 和 IPv6 位址。

自訂 **Global**（全域）服務路由的另一種方式為選取 **Service Route Configuration**（服務路由組態），然後選取 **Destination**（目的地）。指定一個與傳入封包比較的 **Destination**（目的地）IP 位址。若封包目的地位址符合設定的目的地 IP 位址，則來源 IP 位址將設定為針對目的地設定的來源位址。若要限制在 **Source Address**（來源位址）下拉式清單中的選項，請選取一個 **Source Interface**（來源介面），然後從介面選取一個 **Source Address**（來源位址）。設定為 **Any**（任何）的來源介面可讓您從可用的任何介面中選取來源位址。選取 **MGT**（管理）來源介面會使防火牆為服務路由使用管理介面。

© 2019 Palo Alto Networks, Inc.

當為 **Virtual System**（虛擬系統）設定服務路由時，**Inherit Global Service Route Configuration**（繼承全域服務路由組態）選項表示虛擬系統的所有服務將會繼承全域服務路由設定。或者您可以選取 **Customize**（自訂）、選取 **IPv4** 或 **IPv6**，然後選取一項服務；您也可以選取多項服務並 **Set Selected Service Routes**（設定選定的服務路由）。來源介面包含下列三個選取：

- 繼承全域設定 — 選取的服務會繼承那些服務的全域設定。
- 任何 — 可讓您從任何可用的介面中選取來源位址（特定虛擬系統中的介面）。
- 取自下拉式清單的介面—為此介面的 IP 位址限定 **Source Address**（來源位址）的下拉式清單。

針對 **Source Address**（來源位址），請從下拉式清單中選取一個位址。針對選取的服務，會傳送伺服器的回應到來源位址。

目的地服務路由

- 設備 > 設定 > 服務 > 全域

在 **Global**（全域）頁籤上，當您按一下 **Service Route Configuration**（服務路由組態）後，接著按一下 **Customize**（自訂），然後按一下顯示的 **Destination**（目的地）頁籤。目的地服務路由僅在 **Global**（全域）頁籤下提供使用（非 **Virtual Systems**（虛擬系統）頁籤），因此個別虛擬系統的服務路由無法覆寫與虛擬系統相關聯的路由表項目。

您可以使用目的地服務路由來新增**Customize**（自訂）清單上所不支援的自訂服務重新導向。目的地服務路由是一種設定路由以覆寫轉送資訊庫 (FIB) 路由表的方式。目的地服務路由中的任何設定會覆寫路由表項目。他們可以與任何服務建立或取消關聯。

目的地頁籤可用於下列使用案例：

- 服務不具有應用程式服務路由時。
- 在單一虛擬系統中，您要使用多個虛擬路由或虛擬路由和管理連接埠的組合時。

目的地服務路由設定	說明
目的地	請輸入目的地 IP 位址。帶有目的地位址的傳入封包若符合此位址，則將作為您為此服務路由所指定的來源位址來源。
來源介面	若要限制來源位址下拉式清單，請選取 **Source Interface**（來源介面）。選取 **Any**（任何）在來源位址下拉式清單中造成在所有介面上可用的所有 IP 位址。選取 **MGT**（管理）會使防火牆為服務路由使用管理介面。
來源位址	選取服務路由的 **Source Address**（來源位址）；此位址將作為封包從目的地返回時使用。您不需要輸入目的地位址的子網路。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Interfaces（裝置 > 設定 > 介面）

使用此頁面可設定連線設定、允許的服務，以及所有防火牆模型上的管理 (MGT) 介面與 PA-5200 系列防火牆上的輔助介面（AUX-1 和 AUX-2）之管理存取權。

Palo Alto Networks 建議您一律指定 IP 位址和網路遮罩（適用於 IPv4）或首碼長度（適用於 IPv6），以及每個介面的預設閘道。如果您省略任何 MGT 介面的這些設定（例如預設閘道），則只能透過主控台連接埠存取防火牆以供日後組態變更。

若要設定 *M-500* 裝置，或 *Panorama* 虛擬裝置上的 *MGT* 介面，請參閱 *[*Panorama > 設定 > 介面*]*。

您可以使用回送介面來替代防火牆管理的 *MGT* 介面（網路 > 介面 > 回送）。

項目	說明

類型
（僅限 MGT 介面）
	選取一個：
	• 靜態 — 需要您手動輸入 **IP Address**（IP 位址）(IPv4)、**Netmask**（網路遮罩）(IPv4) 及 **Default Gateway**（預設閘道）。
	• **DHCP** 用戶端 — 組態管理介面作為 DHCP 用戶端，以便防火牆傳送 DHCP Discover 或要求訊息以尋找 DHCP 伺服器。伺服器透過提供 IP 位址 (IPv4)、網路遮罩 (IPv4) 及 MGT 介面預設閘道來做出回應。VM 系列防火牆管理介面上的 DHCP 預設為關閉（AWS 與 Azure 中的 VM 系列防火牆除外）。如果您選取 **DHCP Client**（DHCP 用戶端），（選用）可選取下列用戶端選項其中之一或兩者：
	  • 傳送主機名稱—使 MGT 介面將其主機名稱作為 DHCP 選項 12 的一部分傳送至 DHCP 伺服器。
	  • 傳送用戶端 **ID**—使 MGT 介面將其用戶端識別碼作為 DHCP 選項 61 的一部分來傳送。
	如果您選取 **DHCP Client**（DHCP 用戶端），（選用）按一下 **Show DHCP Client Runtime Info**（顯示 DHCP 用戶端執行階段資訊）以檢視動態 IP 介面狀態：
	• 介面—表示 MGT 介面。
	• IP 位址—MGT 介面的 IP 位址。
	• 網路遮罩—IP 位址的子網路遮罩，指示哪些位元組屬於網路或子網路，哪些位元組屬於主機。
	• 閘道—流量離開 MGT 介面的預設閘道。
	• 主要/次要 NTP—支援 MGT 介面的兩個 NTP 伺服器的 IP 位址。如果 DHCP 伺服器返回 NTP 伺服器位址，防火牆僅會在未手動設定 NTP 伺服器位址時考慮它們。如果手動設定 NTP 伺服器位址，防火牆不會用 DHCP 伺服器中的位址來覆寫它們。
	• 租用時間—指派 DHCP IP 位址的天數、小時數、分鐘數及秒數。
	• 到期時間—在 DHCP 租用將到期時指示年/月/日/小時/分鐘/秒。
	• DHCP 伺服器—回應 MGT 介面 DHCP 用戶端之 DHCP 伺服器的 IP 位址。
	• 網域—MGT 介面所屬網域的名稱。
	• DNS 伺服器—支援 MGT 介面的兩個 DNS 伺服器的 IP 位址。如果 DHCP 伺服器返回 DNS 伺服器位址，防火牆僅會在未手動設定 DNS 伺服器位址時考慮它

© 2019 Palo Alto Networks, Inc.

項目	說明
	們。如果手動設定 DNS 伺服器位址，防火牆不會用 DHCP 伺服器中的位址來覆寫它們。 （選用）您可 **Renew**（更新）指派給 MGT 介面的 IP 位址 DHCP 租用。否則，請 **Close**（關閉）視窗。
Aux 1 / Aux 2 （僅限 PA-5200 Series 防火牆）	選取下列任何選項可啟用輔助介面。這些介面提供以下的 10Gbps (SFP+) 輸送量： • 防火牆管理流量 — 您必須啟用管理員在存取 Web 介面和 CLI 來管理防火牆時會使用的網路服務（通訊協定）。 針對 *Web* 介面啟用 *HTTPS* 而非 *HTTP*，並針對 *CLI* 啟用 *SSH* 而非 *Telnet*。 • 防火牆對等之間的高可用性 (HA) 同步 — 在設定介面後，您必須選取它作為 HA 控制連結（**Device**（裝置）> **High Availability**（高可用性）> **General**（一般））。 • 轉送至 Panorama 的日誌 — 您必須設定啟用 **Panorama Log Forwarding**（**Panorama** 日誌轉送）服務的服務路由（裝置 > 設定 > 服務）。
IP 位址 (IPv4)	如果網路使用 IPv4，請將 IPv4 位址指派給介面。或者，您也可以指派回路的 IP 位址進行防火牆管理（請參閱 [網路 > 介面 > 回送]）。依預設，您輸入的 IP 位址是日誌轉送的來源位址。
網路遮罩 (IPv4)	如果將 IPv4 位址指派給介面，則您也必須輸入網路遮罩（例如，255.255.255.0）。
預設閘道	如果將 IPv4 位址指派給介面，則您也必須將 IPv4 位址指派給預設閘道（閘道必須位於與介面相同的子網路上）。
IPv6 位址/首碼長度	如果網路使用 IPv6，請將 IPv6 位址指派給介面。若要指出網路遮罩，請輸入 IPv6 首碼長度（例如，2001:400:f00::1/64）。
預設 IPv6 閘道	如果將 IPv6 位址指派給介面，則您也必須將 IPv6 位址指派給預設閘道（閘道必須位於與介面相同的子網路上）。
速度	設定介面的資料速率與雙工選項。選取包括全雙工或半雙工下的 10Mbps、100Mbps 與 1Gbps。使用預設自動交涉設定，讓防火牆決定介面速度。 此設定必須與相鄰網路裝置的連接埠設定相符。為確保符合設定，如果相鄰裝置支援該選項，請選取自動交涉。
MTU	以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 1,500；預設為 1,500）。
系統管理服務	• **HTTP**—將此服務用於存取防火牆 Web 介面。 *HTTP* 使用純文字，不如 *HTTP* 安全。因此，*Palo Alto Networks* 建議您啟用 *HTTPS* 而非 *HTTP* 來管理介面上的流量。 • **Telnet**—將此服務用於存取防火牆 CLI。

© 2019 Palo Alto Networks, Inc.

項目	說明
	Telnet 使用純文字，不如 *SSH* 安全。因此，*Palo Alto Networks* 建議您啟用 *SSH* 而非 *Telnet* 來管理介面上的流量。 • **HTTPS**—將此服務用於保障安全存取防火牆 Web 介面。 • **SSH**—將此服務用於保障安全存取防火牆 CLI。
網路服務	若要在介面上啟用該服務，請選取。 • **HTTP OCSP**—將此服務用於設定防火牆作為線上憑證狀態通訊協定 (OCSP) 回應程式。如需詳細資訊，請參閱 [裝置 > 憑證管理 > OCSP 回應程式]。 • **Ping**—將此服務用於測試外部服務的連接性。例如，您可 ping 介面，驗證其可從 Palo Alto Networks 更新伺服器接收 PAN-OS 軟體及內容更新。在高可用性 (HA) 部署中，HA 端點使用 ping 來交換活動訊號備援資訊。 • **SNMP**—將此服務用於處理來自 SNMP 管理員的防火牆統計資料查詢。如需詳細資訊，請參閱啟用 SNMP 監控。 • **User-ID**—使用此服務啟用重新散佈在防火牆間的使用者對應。 • **User-ID Syslog 接聽程式-SSL**—將此服務用於啟用整合 PAN-OS 的 User-ID™ 代理程式透過 SSL 收集 Syslog 訊息。如需詳細資訊，請參閱設定對監控伺服器的存取。 • **User-ID Syslog 接聽程式-UDP**—將此服務用於啟用整合 PAN-OS 的 User-ID 代理程式透過 UDP 收集 Syslog 訊息。如需詳細資訊，請參閱設定對監控伺服器的存取。
許可的 IP 位址	輸入管理員可透過介面從中存取防火牆的 IP 位址。空白清單（預設值）會指定可從任何 IP 位址進行存取。 請勿將清單保留空白；僅指定防火牆管理員的 *IP* 位址可避免未經授權之存取。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Telemetry（裝置 > 設定 > 遙測）

遙測是收集和傳輸資料以進行威脅和支援分析，以及啟用應用程式邏輯的程序。若要將遙測收集並傳輸至 Palo Alto Networks，則必須首先選取一個目的地區域。如果您的組織目前擁有 Cortex Data Lake 授權，則您的目的地區域將僅限於您的 Cortex Data Lake 執行個體所在的區域。

遙測資料用於增強應用程式的功能，進而提升您管理和設定 Palo Alto Networks 產品與服務的能力。這些應用程式讓您能夠更好地了解裝置的運作狀態、效能、容量規劃與設定。Palo Alto Networks 還將持續使用此資料來改善威脅防護，並協助您最大程度地利用產品。

選取 **Device**（裝置）> **Setup**（設定）> **Telemetry**（遙測），以查看目前收集的遙測類別。要變更這些類別，請編輯遙測 Widget。取消選取您不希望防火牆收集的任何類別，然後提交變更。

Generate Telemetry File（產生遙測檔案），以獲取防火牆在下一個遙測傳輸間隔將傳送至 Palo Alto Networks 的資料即時範例。

若要完全停用遙測傳輸，請確保未選中 **Enable Telemetry**（啟用遙測），然後提交變更。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Content-ID（裝置 > 設定 > 內容 ID）

使用 **Content-ID**™ 頁籤可定義 URL 篩選、資料保護與容器頁面等設定。

Content-ID 設定	說明
URL 篩選	
動態 URL 快取逾時	按一下 **Edit**（編輯）並輸入逾時（以小時為單位）。此值在動態 URL 篩選中使用，用來決定項目在從 URL 篩選服務傳回之後保留在快取中的時間長度。此選項僅適用於使用 BrightCloud 資料庫的 URL 篩選。如需 URL 篩選的詳細資訊，選取 [物件 > 安全性設定檔 > URL 篩選]。
URL 繼續逾時	指定使用者必須在執行 **Continue**（繼續）動作後幾分鐘之內，針對相同類別的 URL 再次按下繼續（範圍是 1-86,400，預設值為 15）。
URL 管理員取代逾時	指定使用者輸入 **Admin Override**（管理員取代）密碼之後，必須在幾分鐘之內針對相同類別的 URL 重新輸入該管理員取代密碼（範圍是 1-86,400；預設值為 15）。
對類別查閱保留用戶端要求	啟用此選項可指定防火牆何時無法在其本地快取中找到 URL 的類別資訊，當查詢 PAN-DB 時它將保留網頁要求。 此選項預設為停用。作為 URL 篩選設定檔最佳做法的一部份啟用它。
類別查閱逾時（秒）	指定防火牆將嘗試查閱 URL 的類別的時間（以秒為單位），經過此時間之後，會將類別確定為不可解析（範圍時 1-60 秒；預設值為 2）。
URL 管理員鎖定逾時	指定使用者在嘗試使用 URL 管理員取代密碼三次失敗之後，將遭到鎖定的分鐘數（範圍是 1-86,400；預設值為 30）。
PAN-DB 伺服器 （連線至私人 PAN-DB 伺服器所需）	針對網路上的私人 PAN-DB 伺服器指定 IPv4 位址、IPv6 位址或 FQDN。您可新增最多 20 個項目。 依預設，防火牆會連線至公共 PAN-DB 雲端。私人 PAN-DB 解決方案適用於這樣的企業：他們不允許防火牆直接存取公共雲端上的 PAN-DB 伺服器。防火牆所存取的伺服器包含此 URL 的 PAN-DB 伺服器清單、資料庫、URL 更新，以及用於分類網頁的 URL 查詢。
URL 管理員取代	
URL 管理員取代設定	針對每個您要設定 URL 管理員取代的虛擬系統，按一下 **Add**（新增）並指定 URL 篩選設定檔封鎖網頁且已指定 **Override**（取代）動作時要套用的設定（如需詳細資訊，請參閱 Objects（物件）> Security Profiles（安全性設定檔）> URL Fiiltering（URL 篩選））。 • **Location**（位置）—（僅限多重 VSYS 防火牆）從下拉式清單中選取虛擬系統。

© 2019 Palo Alto Networks, Inc.

Content-ID 設定	說明
	• 密碼 / 確認密碼 — 輸入使用者必須輸入來覆蓋封鎖頁面的密碼。 • **SSL/TLS** 服務設定檔 — 若要指定憑證和允許的 TLS 通訊協定版本，以便透過指定伺服器重新導向時確保通訊安全，請選取 SSL/TLS 服務設定檔。如需詳細資訊，請參閱 [裝置 > 憑證管理 > SSL/TLS 服務設定檔]。 • 模式 — 決定封鎖頁面是以透明方式傳送（它看起來像是源自封鎖的網站），還是將使用者重新導向至指定伺服器。如果您選取 **Redirect**（重新導向），請輸入要重新導向的 IP 位址。 您還可以 **Delete**（刪除）項目。
內容雲端設定	
服務 URL	用於掃描企業資料遺失防護 (DLP) 檔案的雲端服務伺服器 URL。 • **APAC**—`apac.hawkeye.services-edge.paloaltonetworks.com` • **Europe**（歐洲）—`eu.hawkeye.services-edge.paloaltonetworks.com` • **United States**（美國）—`us.hawkeye.services-edge.paloaltonetworks.com`
Content-ID 設定	
允許轉送解密的內容	啟用此選項可將防火牆設定為在連接埠鏡像或傳送WildFire® 檔案以供分析時，將解密的內容轉送至外部服務。 啟用此選項並將所有的未知檔案以解密流量傳送至 *WildFire* 進行分析。 針對使用多個虛擬系統（多重 VSYS）功能的防火牆，您要針對每個虛擬系統個別啟用此選項。選取 **Device**（裝置）> **Virtual Systems**（虛擬系統），並選取您要啟用轉送解密內容的虛擬系統。可在虛擬系統對話方塊中使用此選項。
延伸封包擷取長度	設定在反間諜軟體和弱點保護設定檔中啟用延伸擷取選項時，要擷取的封包數目（範圍是 1 到 50；預設為 5）。
轉送區段超過 TCP App-ID™ 檢驗佇列	選取此選項可轉送區段，並在 App-ID 佇列超過 64 個區段限制時將應用程式分類為 `unknown-tcp`（未知 `TCP`）。使用下列全域計數器檢視超過此佇列的區段數，無論是否啟用或停用此選項： `appid_exceed_queue_limit` 停用此選項可阻止防火牆轉送 TCP 區段，並在 App-ID 檢驗佇列已滿時略過 App-ID 檢驗。 此選項預設為停用，且您應將它保持為停用以獲得最佳安全性。 停用此選項時，您可能會注意到其中有超過 *64* 個區段排入佇列等候 *App-ID* 處理的資料流延遲增加。

© 2019 Palo Alto Networks, Inc.

Content-ID 設定	說明

轉送區段超過 TCP 內容檢驗佇列	選取此選項可轉送 TCP 區段，並在 TCP 檢驗佇列已滿時略過內容檢驗。防火牆可在等候內容引擎時將多達 64 個區段排入佇列。防火牆轉送區段並因內容檢驗佇列已滿而略過內容檢驗時，其將增加下列全域計數器：
	`ctd_exceed_queue_limit`
	停用此選項可阻止防火牆轉送 TCP 區段，並在內容檢驗佇列已滿時略過內容檢驗。若停用此選項，防火牆將丟棄超過佇列限制的任何區段，並增加下列全域計數器：
	`ctd_exceed_queue_limit_drop`
	這對全域計數器將套用於 TCP 和 UDP 封包。如果您在檢視過全域計數器後決定要變更設定，可以使用下列 CLI 命令，從 CLI 內加以修改：
	`set deviceconfig setting ctd tcp-bypass-exceed-queue`
	雖然預設會啟用此選項，不過為取得最佳安全性，*Palo Alto Networks* 建議您停用此選項。不過，由於 *TCP* 重新傳輸而導致的丟棄流量，停用此選項可能會導致效能下降，且部分應用程式可能會引起遺失功能，特別是在高流量環境中。

轉送資料包超過 UDP 內容檢驗佇列	選取此選項可轉送 UDP 資料包，並在 UDP 檢驗佇列已滿時略過內容檢驗。防火牆可在等候內容引擎回應時將多達 64 個資料包排入佇列。防火牆轉送資料包並因 UDP 內容檢驗佇列溢位而略過內容檢驗時，其將增加下列全域計數器：
	`ctd_exceed_queue_limit`
	停用此選項可阻止防火牆轉送資料包，並在 UDP 檢驗佇列已滿時略過內容檢驗。若停用此選項，防火牆將丟棄超過佇列限制的任何資料包，並增加下列全域計數器：
	`ctd_exceed_queue_limit_drop`
	這對全域計數器將套用於 TCP 和 UDP 封包。如果您在檢視過全域計數器後決定要變更設定，可以使用下列命令，從 CLI 內加以修改：
	`set deviceconfig setting ctd udp-bypass-exceed-queue`
	雖然預設會啟用此選項，不過為取得最佳安全性，*Palo Alto Networks* 建議您停用此選項。不過，由於丟棄封包，停用此選項可能會導致效能下降，且部分應用程式可能會引起遺失功能，特別是在高流量環境中。

© 2019 Palo Alto Networks, Inc.

Content-ID 設定	說明
允許 HTTP 進行部分回應	啟用此 HTTP 部分回應選項允許用戶端僅擷取檔案的一部分。當轉送路徑中的下一代防火牆識別並丟棄惡意檔案時，它會終止帶有 RST 封包的 TCP 工作階段。如果 Web 瀏覽器實作 HTTP 範圍選項，它可啟動新工作階段只擷取檔案的剩餘部分。這可阻止防火牆因缺少初始工作階段中的內容而再次觸發相同的特徵碼，同時允許 Web 瀏覽器重新組合檔案並提交惡意內容；為了防止發生此情況，請確保停用此選項。 雖然預設會啟用 *Allow HTTP partial response*（容許 *HTTP* 部分回應），不過為取得最佳安全性，*Palo Alto Networks* 建議您停用此選項。停用此選項不得影響裝置效能；然而可能會影響 *HTTP* 檔案轉送中斷復原。此外，停用此選項可能還會影響串流媒體服務，例如 *Netflix*、*Microsoft Updates* 和 *Palo Alto Networks* 內容更新。
即時特徵碼查閱	
DNS 特徵碼查閱逾時 (毫秒)	指定防火牆查詢 DNS 安全服務的持續時間（毫秒）。如果雲端在指定的時間結束前沒有回應，則防火牆會向要求的用戶端釋出相關的 DNS 回應（範圍是 0 至 60,000；預設為 100）。
X-Forwarded-For 標頭	
使用 X-Forwarded-For 標頭	您不能同時針對 *User-ID* 和安全性政策啟用 *X-Forwarded-For*。 • **Disabled**（已停用）—停用後，防火牆不會在用戶端要求中從 X-Forwarded-For (XFF) 標頭讀取 IP 位址。 • **Enable for User-ID**（針對 **User-ID** 啟用）—當防火牆部署在網際網路和隱藏用戶端 IP 位址的 Proxy 伺服器之間時，啟用此選項以指定 User-ID 從 Web 服務的用戶端要求中的 X-Forwarded-For (XFF) 標頭讀取 IP 位址。User-ID 會使用原則參考的使用者名稱來比對其所讀取的 IP 位址，因此那些原則可以控制和記錄相關聯使用者和群組的存取。若標頭具有多個 IP 位址，則 User-ID 會使用左側的第一個項目。 在某些情況下，標頭值為字元字串，而非 IP 位址。如果字串符合 User-ID 已對應至 IP 位址的使用者名稱，防火牆會在政策中針對群組對應參考使用該使用者名稱。如果字串沒有 IP 位址對應，防火牆會叫用政策規則，當中的來源使用者是設為 **any**（任何）或 **unknown**（未知）。 URL 篩選日誌會在 Source User（來源使用者）欄位中顯示比對後的使用者名稱。若 User-ID 無法執行比對，或並未針對與 IP 位址相關聯的地區啟用，則 Source User（來源使用者）欄位會顯示包含首碼 **`x-fwd-for`** 的 XFF IP 位址。 允許在 *User-ID* 中使用 *XFF* 標頭，以便原始的用戶端 *IP* 位址顯示在日誌中，以防您需要調查問題。 • **Enable for Security Policy**（針對安全性政策啟用）—啟用此選項以指定在用戶端和防火牆之間部署上游裝置（例如 Proxy 伺服器或負載平衡器）時，防火牆從用戶端 Web 服務要求的 X-Forwarded-For (XFF) 標頭中讀取 IP 位址。Proxy 伺服器或負載平衡器 IP 位址將用戶端 IP 位址取代為要求來源 IP。防火牆則可使用 XFF 標頭中的 IP 位址來執行政策。

© 2019 Palo Alto Networks, Inc.

Content-ID 設定	說明
	防火牆使用最近新增至 *XFF* 欄位中的 *IP* 位址。如果要求通過多個上游裝置，則防火牆將根據最後新增的 *IP* 位址套用政策。
Strip-X-Forwarded-For 標頭	啟用此選項可移除 X-Forwarded-For (XFF) 標頭，當防火牆部署在網際網路和 Proxy 伺服器之間時，該標頭中包含要求 Web 服務之用戶端的 IP 位址。防火牆會在轉送要求前將標頭值調整為零，且轉送的封包不包含內部來源 IP 資訊。 啟用此選項不會針對政策中的使用者屬性停用 *XFF* 標頭；防火牆僅在將它用於使用者屬性之後，才會將 *XFF* 值調整為零。 當您允許在 *User-ID* 中使用 *XFF* 標頭時，在傳送封包前也要啟用去除 *XFF* 標頭以保護使用者隱私，並同時不會失去追蹤使用者的能力。啟用這兩個選項讓您可以記錄和追蹤原始使用者 *IP* 位址，同時透過不轉發其原始 *IP* 位址來保護使用者的隱私。
Content-ID 功能	
管理資料保護	為存取可能包含機敏資訊（如信用卡號碼或身份證號碼）的日誌新增其他保護。 按一下 **Manage Data Protection**（管理資料保護）以執行下列工作： • **Set Password**（設定密碼）—如果尚未設定密碼，請輸入並確認新密碼。 • **Change Password**（變更密碼）—輸入舊密碼，然後輸入並確認新密碼。 • **Delete Password**（刪除密碼）—刪除密碼及受保護的資料。
容器頁面	使用這些設定可根據內容類型（如應用程式/pdf、應用程式/soap+xml、應用程式/xhtml+、文字/html、文字/純文字與文字/xml），指定防火牆將追蹤或記錄的 URL 類型。每個虛擬系統都會設定容器頁面，您可以從 **Location**（位置）下拉式清單中選取。如果虛擬系統沒有定義明確的容器頁面，防火牆會使用預設內容類型。 **Add**（新增）並輸入內容類型，或者選取現有的內容類型。 為虛擬系統新增內容類型會覆蓋預設內容類型清單。如果沒有與虛擬系統相關聯的內容類型，會使用預設內容類型清單。

© 2019 Palo Alto Networks, Inc.

Device > Setup > WildFire（裝置 > 設定 > WildFire）

選取 **Device**（裝置）> **Setup**（設定）> **WildFire** 可在防火牆和 Panorama 上設定 WildFire。您可以同時啟用 WildFire 雲端和 WildFire 裝置，以便用於執行檔案分析。您也可以設定將報告的檔案大小限制和工作階段資訊。填入 WildFire 設定之後，您可以透過建立 **WildFire Analysis**（**WildFire** 分析）設定檔（**Objects**（物件）> **Security Profiles**（安全性設定檔）> **WildFire Analysis**（**WildFire** 分析）），指定要轉送至 WildFire 雲端或 WildFire 裝置的檔案。

若要將解密的內容轉送至 *WildFire*，請參考Forward Decrypted SSL Traffic for WildFire Analysis（轉送 *WildFire* 分析的解密 *SSL* 流量）。

WildFire 設定	說明
一般設定	
WildFire 公共雲端	若要將檔案傳送至在美國託管的 WildFire 全域雲端進行分析，請輸入 **`wildfire.paloaltonetworks.com`**。或者，您可以改將檔案傳送至 WildFire 區域雲端進行分析。區域雲端是設計用來遵守依您位置而定的資料隱私期望。 將範例轉發至區域 *WildFire* 雲端，以確保遵守針對您所在地區的資料隱私及合規標準。區域雲端包括： • 歐洲—***`eu.wildfire.paloaltonetworks.com`*** • 日本—***`jp.wildfire.paloaltonetworks.com`*** • 新加坡—***`sg.wildfire.paloaltonetworks.com`***
WildFire 私人雲端	指定 WildFire 設備的 IPv4/IPv6 位址或 FQDN。 防火牆會將要分析的檔案傳送至指定的 WildFire 裝置。 Panorama 會從 WildFire 裝置收集威脅 ID，以允許在防間諜軟體設定檔及您在裝置群組中設定的防毒設定檔中新增威脅例外（僅適用於 DNS 簽署）。Panorama 也會從 WildFire 裝置收集資訊，以填入從執行 PAN-OS 7.0 以前之軟體版本的防火牆接收到之 WildFire 提交日誌中遺失的欄位。
檔案大小限制	指定將轉送到 WildFire 伺服器的最大檔案大小。有關檔案大小限制的所有最佳做法建議，如果限制太大並且會阻止防火牆同時轉發多個大型零日檔案，請根據可供使用的防火牆緩衝區空間量降低並調整最大限制。如果有更多可用的緩衝區空間，則可以將檔案大小限制增加至最佳做法建議之上。最佳做法建議是設定有效限制但又不會過度使用防火牆資源的良好起點。可用的範圍為： • **pe**（可攜式文件格式）—範圍是 1 到 50MB；預設為 16MB。 將 *PE* 檔案的大小設定為 *16MB*。 • **apk**（Android 應用程式）—範圍是 1 到 50MB；預設為 10MB。 將 *APK* 檔案的大小設定為 *10MB*。

© 2019 Palo Alto Networks, Inc.

WildFire 設定	說明
	• **pdf**（可攜式文件格式）—範圍是 100KB 到 51,200KB；預設為 3,072KB。 將 *PDF* 檔案的大小設定為 *3,072KB*。 • **ms-office** (Microsoft Office)—範圍是 200KB 到 51,200KB；預設為 16,384KB。 將 *ms-office* 檔案的大小設定為 *16,384KB*。 • **jar**（封裝的 Java 類別檔案）—範圍是 1 到 20MB；預設為 5MB。 將 *jar* 檔案的大小設定為 *5MB*。 • **flash** (Adobe Flash)—範圍是 1 到 10MB；預設為 5MB。 將 *flash* 檔案的大小設定為 *5MB*。 • **MacOSX**（DMG/MAC-APP/MACH-O PKG 檔案）—範圍是 1 到 50MB；預設為 10MB。 將 *MacOSX* 檔案的大小設定為 *1MB*。 • **archive**（RAR 和 7z 檔案）—範圍是 1 到 50MB；預設為 50MB。 將封存檔檔案的大小設定為 *50MB*。 • **linux** (ELF 檔)—範圍是 1 到 50MB；預設為 50MB。 將 *linux* 檔案的大小設定為 *50MB*。 • **scrip**（指令碼）（JScript、VBScript、PowerShell，以及 Shell Script 檔案）—範圍是 10 到 4096KB；預設為 20KB。 將 *script* 檔案的大小設定為 *20KB*。 之前的值可能因 *PAN-OS* 目前版本或內容發佈版本而有所差異。若要檢視有效的範圍，請按一下 *Size Limit*（大小限制）欄位，隨即會出現快顯視窗來顯示可用的範圍和預設值。
報告有利檔案	啟用此選項後（預設為停用），經過 WildFire 分析並判定為良性的檔案會顯示在 **Monitor**（監控）> **WildFire Submissions**（**WildFire** 提交）日誌中。 即使在防火牆上啟用此選項，由於考慮到可能處理的連結數量，因此不會再記錄 WildFire 視為良性的電子郵件連結。
報告 Grayware 檔案	啟用此選項後（預設為停用），經過 WildFire 分析並判定為灰色軟體的檔案會顯示在 **Monitor**（監控）> **WildFire Submissions**（**WildFire** 提交）日誌中。

© 2019 Palo Alto Networks, Inc.

WildFire 設定	說明
	即使在防火牆上啟用此選項，由於考慮到可能處理的連結數量，因此不會再記錄 *WildFire* 判定為 *Grayware* 的電子郵件連結。 啟用報告灰色軟體檔案至日誌工作階段資訊、網路活動、主機活動，以及其他有助於分析的資訊。
工作階段資訊設定	
設定	指定要轉送到 WildFire 伺服器的資訊。預設情況下，所有選項都是選取的，最佳做法是轉發所有工作階段資訊，以提供統計資料和其他指標，使您能夠採取措施來防止威脅事件： • **Source IP**—傳送疑似問題檔案的來源 IP 位址。 • **Source Port**—傳送疑似問題檔案的來源連接埠。 • **Destination IP**—疑似問題檔案的目的地 IP位址。 • 目的地連接埠—疑似問題檔案的目的地連接埠。 • **Vsys**—識別出疑似惡意軟體的防火牆虛擬系統。 • **Application**—用於傳輸檔案的使用者應用程式。 • **User**—鎖定為目標的使用者。 • **URL**—與疑似問題檔案相關的 URL。 • **Filename**—已傳送的檔案名稱。 • 電子郵件寄件者—在 SMTP 和 POP3 流量中偵測到惡意電子郵件連結時，在 WildFire 日誌和 WildFire 詳細報告中提供寄件者名稱。 • 電子郵件收件者 — 在 SMTP 和 POP3 流量中偵測到惡意電子郵件連結時，在 WildFire 日誌和 WildFire 詳細報告中提供收件者名稱。 • 電子郵件主旨—在 SMTP 和 POP3 流量中偵測到惡意電子郵件連結時，在 WildFire 日誌和 WildFire 詳細報告中提供電子郵件主旨。

© 2019 Palo Alto Networks, Inc.

Device > Setup > Session（裝置 > 設定 > 工作階段）

選取 **Device**（設備）> **Setup**（設定）> **Session**（工作階段）可設定工作階段過時的時間、解密憑證設定，以及與全域工作階段相關的設定，例如防護 IPv6 流量以及政策變更時，使安全政策重新符合現有的工作階段。此頁籤具有下列區段：

- 工作階段設定
- 工作階段逾時
- TCP 設定
- 解密設定：憑證撤銷檢查
- 解密設定：正向 Proxy 伺服器憑證設定
- VPN 工作階段設定

工作階段設定

下表說明工作階段設定。

工作階段設定	說明
重新比對工作階段	按一下 **Edit**（編輯），然後選取 **Rematch Sessions**（重新比對工作階段），使得防火牆將最近設定的安全性政策規則套用至已在進行中的工作階段。依預設會啟用此功能。如果已停用此設定，則只會將任何政策規則變更套用至變更提交後所啟動的這些工作階段。 例如，如果已啟動 Telnet 工作階段，同時設定允許 Telnet 的相關政策規則，而您後續提交政策規則變更來拒絕 Telnet，則防火牆會將修改的政策規則套用至目前的工作階段並封鎖它。 啟用 *Rematch Sessions*（重新比對工作階段）將您最新的安全性政策規則套用於目前使用中工作階段。
ICMPv6 語彙基元陣列大小	輸入用於限制 ICMPv6 錯誤訊息速率的桶大小。語彙基元桶大小是語彙基元桶演算法的參數，可控制 ICMPv6 錯誤封包的突發程度（範圍是 10 至 65,535 個封包；預設為 100）。
ICMPv6 錯誤封包速率	輸入透過防火牆，在全域範圍內每秒允許的 ICMPv6 錯誤封包平均數（範圍為 10 至 65,535；預設為 100）。此值適用於所有介面。如果防火牆達到 ICMPv6 錯誤封包速率，會使用 ICMPv6 語彙基元桶來啟用 ICMPv6 錯誤訊息節流。
啟用 IPv6 防火牆	若要針對 IPv6 流量啟用防火牆功能，請按一下 **Edit**（編輯），然後選取 **IPv6 Firewalling**（**IPv6** 防火牆）。 如果您未啟用 IPv6 防火牆，則防火牆會忽略所有基於 IPv6 的設定。即使在介面上啟用 IPv6 流量，也必須啟用 **IPv6 Firewalling**（**IPv6** 防火牆）選項，這樣 IPv6 防火牆才能運作。
啟用 Jumbo Frame 全域 MTU	選取此選項可在 Ethernet 介面上啟用 Jumbo Frame 支援。巨型框架具有 9,192 位元組的最大傳輸單位 (MTU)，並只能在某些型號上使用。

© 2019 Palo Alto Networks, Inc.

工作階段設定	說明
	• 若未 **Enable Jumbo Frame**（啟用巨型框架），則 **Global MTU**（全域 **MTU**）會預設為 1,500 位元組（範圍是 576 至 1,500）。 • 若 **Enable Jumbo Frame**（啟用巨型框架），則 **Global MTU**（全域 **MTU**）會預設為 9,192 位元組（範圍是 9,192 至 9,216 位元組）。 與普通封包相比，巨型框架最多可以佔用五倍以上的記憶體，並且可將可用封包緩衝區的數量減少 *20%*。這減少了用於亂序、應用程式標識和其他此類封包處理任務的佇列大小。自 *PAN-OS 8.1* 開始，如果啟用巨型框架全域 *MTU* 設定並重新啟動防火牆，則會重新散佈封包緩衝區以更有效地處理巨型框架。 如果啟用巨型框架，而且擁有未特別設定 MTU 的介面，則那些介面將自動繼承巨型框架大小。因此，在您啟用巨型框架之前，若不希望任何介面允許巨型框架，則必須將該介面的 MTU 設為 1,500 位元組或其他值。若要設定介面的 MTU（**Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路）），請參閱 PA-7000 Series 第三層介面。
DHCP 廣播工作階段	如果您的防火牆充當 DHCP 伺服器，請選取此選項以啟用 DHCP 廣播封包的工作階段日誌。DHCP 廣播工作階段選項可為 DHCP 產生增強型應用程式日誌（EAL 日誌），以供 IoT 安全性和其他服務使用。如果未啟用此選項，則防火牆將轉送封包，而不會為 DHCP 廣播封包建立日誌。
NAT64 IPv6 最小網路 MTU	輸入 IPv6 轉譯流量的全域 MTU。預設值 1,280 位元組是以 IPv6 流量的標準最低 MTU 為基礎（範圍是 1,280 至 9,216）。
NAT 超額授權比例	選取 DIPP NAT 過度訂閱比例，即防火牆可同時使用相同轉譯 IP 位址和連接埠配對的次數。減少過度訂閱比例將減少來源裝置轉譯的數目，但會提供較高的 NAT 規則容量。 • **Platform Default**（平台預設）—會關閉過度訂閱比例的明確設定，且套用型號的預設過度訂閱比例。（請在此參閱防火牆型號的預設比例：https://www.paloaltonetworks.com/products/product-selection.html）。 • **1** 倍—1 次。這意味著無過度訂閱；防火牆不能多次同時使用相同轉譯 IP 位址和連接埠配對。 • **2** 倍—2 次 • **4** 倍—4 次 • **8** 倍—8 次
ICMP 無法連線封包速率 (每秒)	定義 ICMP 無法連線的數目上限以回應防火牆每秒可以傳送的數量。此限制由 IPv4 和 IPv6 封包所共用。 預設值為每秒 200 則訊息（範圍是 1 至 65,535）。
加速老化	啟用閒置工作階段的加速過期。 選取此選項可啟用加速過時，然後指定閾值 (%) 與比例係數。 當工作階段表到達加速老化閾值（% 比例），PAN-OS 會將加速老化縮放係數套用到所有工作階段的老化計算。預設的縮放係數為 2，意味加速老化的發生速率是設定的閒置時間的兩倍。將設定的閒置時間除以 2 會導致時間減半而更快逾時。為了計算工作階段的加速過期，PAN-OS 會將設定的閒置時間（適用於工作階段的該類型）除以縮放係數來決定更短的逾時。

© 2019 Palo Alto Networks, Inc.

工作階段設定	說明
	例如，如果縮放係數是 10，一般會在 3,600 秒後逾時之工作階段的逾時速度會加快 10 倍（時間的 1/10），也就是在 360 秒後逾時。 啟用加速老化閾值，並在工作階段表開始填滿時設定可接受的縮放因子以釋放工作階段表空間。
封包緩衝區保護	從 PAN OS 10.0 開始，全域和在每個區域上預設會啟用封包緩衝區保護。作為最佳做法，在全域以及每個區域保持啟用封包緩衝保護，以防止防火牆緩衝區遭到 DoS 攻擊以及加強工作階段和來源。此選項會保護防火牆上的接收緩衝區免於攻擊或濫用流量，濫用流量會造成系統資源進行備份以及合法流量被丟棄。封包緩衝區保護識別違規工作階段，使用隨機早期丟棄 (RED) 作為第一道防線，並在濫用持續時捨棄工作階段或封鎖違規的 IP 位址。若防火牆從特定 IP 位址偵測到許多小工作階段或快速的工作階段建立（或兩者），就會封鎖該 IP 位址。 採用防火牆封包緩衝區使用率的基準測量以理解防火牆的容量，並且確保防火牆設定正確，因此僅一次攻擊造成緩衝區使用量的大幅增加。 • 警示 **(%)**—當封包緩衝區使用情況超過閾值的時間多於 10 秒，則防火牆分鐘都會建立日誌事件。當在全域啟用封包緩衝區保護時（範圍是 0% 至 99%；預設值是 50%），防火牆將產生日誌事件。若值為 0%，則防火牆不會建立日誌事件。從預設閾值開始並根據需要進行調整。 • **Activate (%)**（啟動 **(%)**）—達到閾值時，防火牆會開始將濫用最嚴重的工作階段減速（範圍是 0%-99%；預設值為 80%）。若值為 0%，則防火牆不會套用 RED。從預設閾值開始並根據需要進行調整。

封包緩衝區保護（續）	• （執行 PAN OS 10.0 或更新版本的硬體防火牆）作為以使用率百分比為基礎的封包緩衝區保護的替代方案（如上所述），您可以透過啟用 **Buffering Latency Based**（以緩衝區延遲為基礎），並進行以下設定來觸發以 CPU 處理延遲為基礎的封包緩衝區保護：
	  • **Latency Alert (milliseconds)**（延遲警示（毫秒）—若延遲超過此閾值，則防火牆將開始每分鐘產生一個警示日誌事件（範圍為 1 到 20,000；預設值為 50）。
	  • **Latency Activate (milliseconds)**（延遲啟動（毫秒）—若延遲超過此閾值，則防火牆將對傳入封包啟動隨機早期偵測 (RED)，並開始每 10 秒產生一次啟動日誌（範圍是 1 至 20,000；預設值為 200）。
	  • **Latency Max Tolerate (milliseconds)**（延遲最大容忍（毫秒））—若延遲等於或超過該閾值，則防火牆將使用接近 100% 丟棄可能性的 RED（範圍是 1 至 20,000 毫秒；預設值為 500 毫秒）。
	  若目前延遲是介於「延遲啟動」閾值和「延遲最大容忍」閾值之間的值，則防火牆會按以下方式計算 RED 丟棄可能性：（目前延遲 - **Latency Activate**（延遲啟動）閾值）/（**Latency Max Tolerate**（延遲最大容忍）閾值 - **Latency Activate**（延遲啟動）閾值）。例如，如果目前延遲為 300，「延遲啟動」為 200，「延遲最大容忍」為 500，那麼 (300-200)/(500-200) = 1/3，意味著防火牆使用大約 33% 的 RED 丟棄可能性。

封包緩衝區保護（續）	• **Block Hold Time (sec)**（封鎖保持時間（秒））—捨棄工作階段或封鎖來源 IP 位址前允許工作階段繼續進行的時間（秒）（範圍是 0-65,535；預設值為 60）。此計時器會監控由 RED 減速的工作階段，以檢視其對緩衝區的使用率或延遲是否持續超過設定的閾值。若濫用行為繼續進行超過封鎖保持時間，則捨棄工作階段。若值為 0，則防火牆不會根據封包緩衝區保護捨棄工作階段。以預設值開始，監控封包緩衝區使用率或延遲，並根據需要調整時間值。

© 2019 Palo Alto Networks, Inc.

工作階段設定	說明
	• **Block Duration (sec)**（封鎖持續時間（秒））—被捨棄的工作階段保持被捨棄狀態或被封鎖的 IP 位址保持被封鎖狀態的時間（秒）（範圍是 1 至 15,999,999；預設值為 3,600）。除非封鎖一個 IP 位址一小時對您的業務情況會造成太大的懲罰，請使用預設值。如懲罰太大可降低持續時間。監控封包緩衝區使用率或延遲，並根據需要調整持續時間。 網路位址轉譯 *(NAT)* 可以提高封包緩衝區的使用率。如果這樣會影響緩衝區的利用，請減少 *Block Hold Time (*封鎖保留時間*)* 以更快封鎖個別工作階段和縮短 *Block Duration (*封鎖期間*)*，使來自其他基礎 *IP* 位址的工作階段不會受到不當的處罰。
多點傳送路由設定緩衝處理	選取此選項（預設為停用）可啟用多點傳送路由設定緩衝，當多點傳送路由或轉送資訊庫 (FIB) 項目在相應多點傳送群組中尚未存在時，這將允許防火牆在多點傳送工作階段中保留第一個封包。依預設，防火牆在新工作階段中不緩衝第一個多點傳送封包；而是使用第一個封包來設定多點傳送路由。這是多點傳送流量的預期行為。只有當內容伺服器直接連線至防火牆，且您的自訂應用程式無法經受工作階段中的第一個封包被丟棄，才需要啟用多點傳送路由設定緩衝。
多點傳送路由設定緩衝區大小	如果啟用多點傳送路由設定緩衝，您可調整緩衝區大小，依流量指定緩衝區大小（範圍是 1 至 2,000，預設為 1,000）。 防火牆可緩衝最多 5,000 個封包。

工作階段逾時

有些「工作階段逾時」定義在工作階段中停用後，PAN-OS 在防火牆上保留工作階段的期間。依預設，如果工作階段因通訊協定到期而逾時，PAN-OS 會關閉工作階段。Discard（捨棄）工作階段逾時定義工作階段在 PAN-OS 依據安全性原則規則拒絕此工作階段後，一個工作階段維持開啟的最長時間。

在防火牆上，您可以特別針對 TCP、UDP、ICMP 和 SCTP 工作階段定義逾時數。**Default**（預設）逾時會套用至任何其他類型的工作階段。這些逾時都是全域的，意味它們會套用至防火牆上該類型的所有工作階段。

除了全域設定外，您還能彈性地在 **Objects**（物件）> **Applications**（應用程式） 頁籤上針對個別的應用程式定義逾時值。[選項] 視窗隨即會出現該應用程式的可用逾時。防火牆會將應用程式逾時套用至處於「已建立」狀態的應用程式。設定後，應用程式的逾時會取代全域 TCP 、UDP 或 SCTP 工作階段逾時。

使用此區段的選項，可特別針對 TCP、UDP、ICMP 、SCTP和其他所有類型的工作階段，進行全域工作階段逾時設定。

預設值為最佳數值，最佳做法是使用預設值。然而，您可以因應網路需求修改這些值。將值設得過低可能會降低輕微網路延遲的敏感度，並導致無法與防火牆建立連線。將值設得過高則可能會延遲失敗偵測。

工作階段逾時設定	說明
預設值	可開啟非 TCP/UDP、非 SCTP 或非 ICMP工作階段而無回應的時間長度上限（以秒為單位，範圍是 1 到 15,999,999；預設為 30）。
捨棄預設值	當 PAN-OS 根據防火牆上設定的安全性原則規定拒絕工作階段後，非 TCP/UDP/SCTP 工作階段保持開啟的時間長度上限 （依秒計，範圍是 1 至 15,999,999；預設值是 60）。
捨棄 TCP	當 PAN-OS 根據防火牆上設定的安全性原則規定拒絕工作階段後，TCP 工作階段保持開啟的時間長度上限 （依秒計，範圍是 1 至 15,999,999；預設值是 90）。

© 2019 Palo Alto Networks, Inc.

工作階段逾時設定	說明
捨棄 UDP	當 PAN-OS 根據防火牆上設定的安全性原則規定拒絕工作階段後，UDP 工作階段保持開啟的時間長度上限（依秒計，範圍是 1 至 15,999,999；預設值是 60）。
ICMP	可開啟非 ICMP 工作階段而無回應的時間長度上限（範圍是 1 到 15,999,999；預設為 6）。
掃描	在防火牆清除工作階段並恢復工作階段使用的緩衝區資源之前，工作階段可以保持不活動的時間長度（以秒為單位）。不活動時間是自從封包或時間上次重新整理工作階段以來已經過的時間長度。範圍是 5-30；預設值為 10。
TCP	在 TCP 工作階段處於「已建立」狀態後（交握完成和/或資料傳輸啟動後），TCP 工作階段維持開啟卻無回應的時間長度上限（範圍是 1 到 15,999,999；預設為 3,600）。
TCP 交握	以秒為單位接收 SYN-ACK 與後續的 ACK 以完全建立工作階段之間的時間長度上限（範圍是 1 到 60；預設為 10）。
TCP 起始	啟動 TCP 交握計時器之前接收 SYN 與 SYN-ACK 的時間長度上限（以秒為單位，範圍是 1 到 60；預設為 5）。
TCP 半關閉狀態	啟動第一次 FIN 與接受第二個 FIN 或 RST 之間的時間長度上限（以秒為單位，範圍是 1 到 604,800；預設為 120）。
TCP 時間等待	接受第二個 FIN 或 RST 之後的時間長度上限（以秒為單位，範圍是 1 到 600；預設為 15）。
未確認的 RST	接收無法確認的 RST 之後的時間長度上限（RST 位於 TCP 視窗但具有非預期的序號，或 RST 來自非對稱路徑）；（以秒為單位，範圍是 1 到 600；預設為 30）。
Udp	開啟非 UDP 工作階段而無 UDP 回應的時間長度上限（以秒為單位，範圍是 1 到 1,599,999；預設為 30）。
驗證入口網站	驗證入口網站網頁表單的驗證工作階段逾時秒數（預設為 30，範圍是 1 到 1,599,999）。若要存取要求的內容，使用者必須在此表單中輸入驗證認證並成功驗證。 驗證入口網站網頁表單的驗證工作階段逾時秒數（預設為 30，範圍是 1 到 1,599,999）。若要存取要求的內容，使用者必須在此表單中輸入驗證認證並成功驗證。
SCTP INIT	從防火牆在停止啟動SCTP 關聯之前，必須接收到 INIT ACK 區段的 SCTP INIT 區段時間上限（以秒為單位，範圍是 1 到 60；預設為 5）。
SCTP COOKIE	從防火牆在停止啟動SCTP 關聯之前，必須隨同 cookie 接收到 COOKIE ECHO 區段的附狀態 COOKIE 參數的 SCTP INIT 區段時間上限（以秒為單位，範圍是 1 到 600；預設為 60）。
放棄 SCTP	當 PAN-OS 根據防火牆上設定的安全性原則規定拒絕工作階段後， SCTP 關聯保持開啟的時間長度上限（以秒為單位，範圍是 1 到 604,800；預設為 30）。

© 2019 Palo Alto Networks, Inc.

工作階段逾時設定	說明
SCTP	在關聯中的所有工作階段逾時之前，一個關聯不需 SCTP 流量可以經過的最大時間長度（以秒為單位，範圍是 1 到 604,800；預設為 3,600）。
SCTP 關閉	在防火牆捨棄關閉區段前，SCTP 關閉區段以接收關閉 ACK 區段後，防火牆可等候的時間上限（以秒為單位，範圍是 1 到 600；預設為 30）。

TCP 設定

下表說明 TCP 設定。

TCP 設定	說明
轉送區段超過 TCP 失序佇列	如果您想要防火牆轉送超過 TCP 失序佇列限制（每個工作階段 64 個）的區段，則選取此選項如果您停用此選項，防火牆將丟棄超過失序佇列限制的區段。若要檢視因啟用此選項而使防火牆丟棄區段的計數，請執行以下 CLI 命令： `show counter global tcp_exceed_flow_seg_limit` 此選項預設為停用，且為了達到最安全的部署，您應保持預設值。停用此選項可能導致接收超過 *64* 個失序區段的特定資料流延遲增加。由於 *TCP* 堆疊應處理遺失區段的重新傳輸，因此不應有連線中斷。
允許任意 ACK 回應 SYN	啟用以在 TCP 工作階段設定的第一個封包不是 SYN 封包時全域拒絕封包。 若要控制個別區域保護設定檔的設定，請在 TCP 丟棄 中變更 *Reject Non-SYN TCP*（拒絕非 *SYN TCP*）設定。
丟棄具有 Null 時間戳記選項的區段	TCP 時間戳記會記錄何時傳送區段，並允許防火牆驗證時間戳記對該工作階段有效，以防止 TCP 封裝序號。TCP 時間戳記還可用於計算往返時間。啟用此選項，則防火牆會丟棄具有 Null 時間戳記的封包。若要檢視因啟用此選項而使防火牆丟棄區段的計數，請執行以下 CLI 命令： `show counter global tcp_invalid_ts_option` 此選項預設為啟用，且為了達到最安全的部署，您應保持預設值。啟用此選項不得導致效能下降。然而，如果網路堆疊錯誤產生具有 *Null TCP* 時間戳記選項值的區段，啟用此選項可能導致連線問題。
非對稱路徑	全域設定是否丟棄或略過包含非同步 ACK 或視窗外序號的封包。 • **Drop**（丟棄）—丟棄包含非對稱路徑的封包。

© 2019 Palo Alto Networks, Inc.

TCP 設定	說明
	• **Bypass**（略過）—略過對於包含非對稱路徑的封包進行的掃描。 若要控制個別區域保護設定檔的設定，請在 TCP 丟棄 中變更 *Asymmetric Path*（非對稱路徑）設定。
緊急資料旗標	使用此選項可設定防火牆是否允許 TCP 標頭中的緊急指標（URG 位元旗標）。TCP 標頭中的緊急指標原先是用來透過防火牆將封包從處理佇列中移除，再透過主機中的 TCP/IP 堆疊來將其加速，從而將該封包提升為立即處理。此處理程序即稱為頻外處理。 由於各主機實作緊急指標的方式各有不同，請選取 **Clear**（清除）（預設與建議的設定）以統一做法，透過禁止頻外處理，使承載資料中的頻外位元組成為承載資料的一部分，同時也不再為封包進行緊急處理。此外，**Clear**（清除）設定可確保防火牆將通訊協定堆疊中完全相同的資料流視為封包的目的地主機。若要檢視當此選項設定為 **Clear**（清除）時防火牆清除 URG 旗標的區段計數，請執行以下 CLI 命令： `show counter global tcp_clear_urg` 此旗標預設會設定為 *Clear*（清除）並應保持如此，以實現最安全的部署。這不應導致效能下降；在極少數的情況下，*Telnet* 等應用程式會使用緊急資料功能，可能會使 *TCP* 受到影響。若您將此旗標將設定為 *Do Not Modify*（請勿修改），則防火牆會允許封包帶有 *TCP* 標頭中的 *URG* 位元旗標，並且啟用頻外處理（不建議）。
丟棄無旗標的區段	未設定任何旗標的非法 TCP 區段可用於避開內容檢驗。啟用此選項（預設值）則防火牆會丟棄在 TCP 標頭中未設定任何旗標的封包。若要檢視因為此選項而使防火牆丟棄區段的計數，請執行以下 CLI 命令： `show counter global tcp_flag_zero` 此選項預設為啟用，且為了達到最安全的部署，您應保持預設值。啟用此選項不得導致效能下降。然而，如果網路堆疊錯誤產生沒有 *TCP* 旗標的區段，啟用此選項可能導致連接性問題。
除去 MPTCP 選項	預設會全域啟用，以將（多路徑 TCP）MPTCP 連線轉換為標準 TCP 連線。 若要允許 *MCTCP*，請在 TCP 丟棄 中變更 *Multipath TCP (MPTCP) Options*（多路徑 *TCP (MPTCP)* 選項）設定。
SIP TCP 純文字	選取以下其中一個選項，以在偵測到分段 SIP 標頭時為 SIP TCP 工作階段設定純文字 Proxy 行為。

© 2019 Palo Alto Networks, Inc.

TCP 設定	說明
	• **Always Off**（始終關閉）—停用純文字 Proxy。當 SIP 訊息大小通常小於 MSS 且 SIP 訊息適合在單一區段中時，或者如果您需要確保 TCP Proxy 資源保留用於 SSL 正向 Proxy 或 HTTP/2，請停用 Proxy。 • **Always enabled**（始終啟用）—預設值。將 TCP Proxy 用於 TCP 工作階段的所有 SIP，協助正確重組和排序 TCP 區段以實現 ALG 正常運作。 • **Automatically enable proxy when needed**（在需要時自動啟用 **Proxy**）—若選取該項，將會針對其中 ALG 偵測 SIP 訊息分散的工作階段自動啟用純文字 Proxy。當 Proxy 也用於 SSL 正向 Proxy 或 HTTP/2 時，有助於最佳化 Proxy。
TCP 重新傳輸掃描 （PAN-OS 10.0.2 或更新版本）	如果啟用，則在看到重新傳輸的封包時將掃描原始封包的總和檢查碼。如果原始封包和重新傳送的封包之間的總和檢查碼不同，則會認為重新傳送的封包是惡意的並被丟棄。

解密設定：憑證撤銷檢查

選取 **Session**（工作階段），並在 [解密設定] 中，選取 **Certificate Revocation Checking**（憑證撤銷檢查）來設定下表所述的參數。

工作階段功能：憑證撤銷檢查設定	說明
啟用：CRL	選取此選項可使用憑證撤銷清單 (CRL) 方法來驗證憑證的撤銷狀態。 如果另外啟用線上憑證狀態協定 (OCSP)，防火牆會先嘗試 OCSP；如果 OCSP 伺服器無法使用，防火牆接著會嘗試 CRL 方法。 如需解密憑證的詳細資訊，請參閱解密的金鑰和憑證。
接收逾時：CRL	如果啟用 CRL 方法以驗證憑證撤銷狀態，請以秒為單位指定間隔（1 到 60，預設值為 5），過了此間隔後，防火牆會停止等待 CRL 服務的回應。
啟用：OCSP	選取此選項可使用 OCSP 來驗證憑證的撤銷狀態。
接收逾時：OCSP	如果您啟用了 OCSP 方法以驗證憑證撤銷狀態，請以秒為單位指定間隔（1 到 60，預設值為 5），過了此間隔後，防火牆會停止等待 OCSP 回應程式的回應。
封鎖未知憑證狀態的工作階段	選取此選項可在 OCSP 或 CRL 服務傳回未知的憑證撤銷狀態時封鎖 SSL/TLS 工作階段。否則，防火牆會繼續進行該工作階段。
封鎖憑證狀態檢查逾時的工作階段	選取此選項可在防火牆登錄 CRL 或 OCSP 要求逾時下封鎖 SSL/TLS 工作階段。否則，防火牆會繼續進行該工作階段。
憑證狀態逾時	以秒為單位指定間隔（1 到 60，預設值為 5），過了此間隔後，防火牆會停止等待任何憑證狀態服務的回應，並套用您選擇性定義的任何工作階段封鎖邏輯。**Certificate Status**（憑證狀態逾時）與 OCSP/CRL **Receive Timeout**（接收逾時）有關，如下所述： • 如果您啟用 OCSP 與 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或兩個 **Receive Timeout**（接收逾時）值的彙總。

© 2019 Palo Alto Networks, Inc.

工作階段功能：憑證撤銷檢查設定	說明
	• 如果您僅啟用 OCSP—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status**（憑證狀態逾時）值或 OCSP **Receive Timeout**（接收逾時）值。 • 如果您僅啟用 CRL—在經過以下兩個間隔之中較短的間隔後，防火牆會註冊要求逾時：**Certificate Status Timeout**（憑證狀態逾時）值或 CRL **Receive Timeout**（接收逾時）值。

解密設定：正向 Proxy 伺服器憑證設定

在解密設定（**Session**（工作階段）頁籤）中，選取 **SSL Forward** 代理程式 **Settings**（**SSL** 轉送 代理程式 設定），設定**RSA Key Size**（RSA 金鑰大小）或 **ECDSA Key Size**（ECDSA 金鑰大小）以及 在建立 SSL/TLS 轉送 代理程式 解密的工作階段時， 防火牆向用戶端出示之憑證的雜湊演算法。下表說明參數。

工作階段功能：正向 Proxy 伺服器憑證設定	

RSA 金鑰大小	選取下列其中一項：
	• 由目的地主機定義（預設）—若要防火牆根據目的地伺服器使用的金鑰來產生憑證，請選取此選項：
	  • 如果目的地伺服器使用 RSA 1,024 位元金鑰，防火牆會產生包含該金鑰大小和 SHA1 雜湊演算法的憑證。
	  • 如果目的地伺服器使用大於 1,024 位元的金鑰大小（例如 2,048 位元或 4,096 位元），則防火牆會產生使用 2,048 位元 金鑰與 SHA-256 演算法的憑證。
	• **1024-bit RSA**—若要防火牆產生使用 RSA 1,024 位元金鑰和 SHA1 雜湊演算法的憑證，而不理會目的地伺服器使用的金鑰大小為何，請選取此選項。從 2013 年 12 月 31 日開始，公開憑證授權單位 (CA) 和受歡迎的瀏覽器針對使用少於 2,048 位元之金鑰的 X.509 憑證，提供有限的支援。未來視安全性設定而定，瀏覽器可在出示此類金鑰時警告使用者或將 SSL/TLS 工作階段整個封鎖。
	• **2048-bit RSA**—若要防火牆產生使用 RSA 2,048 位元金鑰和 SHA-256 雜湊演算法的憑證，而不理會目的地伺服器使用的金鑰大小為何，請選取此選項。公開 CA 和受歡迎的瀏覽器支援 2,048 位元金鑰，其提供比 1,024 位元金鑰更佳的安全性。

ECDSA 金鑰大小	選取下列其中一項：
	• 由目的地主機定義（預設）—若要防火牆根據目的地伺服器使用的金鑰來產生憑證，請選取此選項：
	  • 如果目的地伺服器使用 ECDSA 256 位元或 384 位元的金鑰，則防火牆會使用該金鑰大小產生憑證。
	  • 如果目的地伺服器使用大於 384 位元的金鑰大小，則防火牆會產生使用 521 位元金鑰的憑證。
	• **256-bit ECDSA**— 若要防火牆產生使用 ECDSA 256 位元金鑰，而不理會目的地伺服器使用的金鑰大小為何，請選取此選項。
	• **384-bit ECDSA**— 若要防火牆產生使用 ECDSA 384 位元金鑰，而不理會目的地伺服器使用的金鑰大小為何，請選取此選項。

© 2019 Palo Alto Networks, Inc.

VPN 工作階段設定

選取 **Session**（工作階段），並在 [VPN 工作階段設定] 中，設定與建立 VPN 工作階段之防火牆相關的全域設定。下表說明設定。

VPN 工作階段設定	說明
Cookie 啟動閾值	在觸發 Cookie 驗證的上方，指定每個防火牆所允許 IKEv2 半開啟的 IKE SA 的數目上限。當半開啟的 IKE SA 數目超過 Cookie 驗證閾值時，回應程式會要求一個 Cookie，且啟動者必須回應一個包含 Cookie 的 IKE_SA_INIT。若 Cookie 驗證成功，則可以啟動另一個 SA 工作階段。 若值為 0，表示 Cookie 驗證一律開啟。 Cookie 啟動閾值是一種全域防火牆設定，且應低於半開啟 SA 設定的上限，因為這也是一種全域設定（範圍是 0 至 65535；預設為 500）。
半開啟 SA 上限	指定 IKEv2 半開啟的 IKE SA 的數目上限，以便啟動器可以傳送至防火牆而不需取得回應。一旦到達上限，防火牆將不會回應新的 IKE_SA_INIT 封包（範圍是 1 至 65535；預設為 65535）。
快取憑證上限	針對透過防火牆可快取 HTTP 所擷取的端點憑證授權單位 (CA) 憑證指定數目上限。此值僅由 IKEv2 雜湊和 URL 功能所使用（範圍是 1 至 4000；預設為 500）。

© 2019 Palo Alto Networks, Inc.

Device > High Availability（裝置 > 高可用性）

- Device > High Availability（裝置 > 高可用性）

針對備援，請在 HA 配對或 HA 叢集的 high availability（高可用性）設定下部署 Palo Alto Networks 的新世代防火牆。當兩個 HA 防火牆用作 HA 配對時，會有兩個 HA 部署：

- 主動/被動—在此部署中，主動端點會透過兩個專用介面與被動端點持續同步其設定及工作階段資訊。如果主動防火牆上的硬體或軟體中斷，則被動防火牆將自動變為主動，而不會中斷服務。主動/被動 HA 部署支援所有介面模式：Virtual Wire、Layer 2 或 Layer 3。
- 主動/被動—在此部署中，兩個 HA 端點均為主動，且都會處理流量。此類部署最適合涉及非對稱路由的案例，或者您想要允許動態路由通訊協定（OSPF、BGP）以在兩個端點間保持主動狀態的情況。僅在 Virtual Wire 與 Layer 3 介面模式下，才會支援主動/被動 HA。除了 HA1 與 HA2 連結，主動/主動部署需要專用 HA3 連結。HA3 連結用作進行工作階段設定與非對稱流量處理的封包轉送連結。

> 在 *HA* 配對中，兩個端點必須屬於相同的機型、必須正在執行相同的 *PAN-OS* 與內容發行版本，且必須有相同的授權集。
>
> 此外，針對 *VM* 系列防火牆，兩個端點必須屬於相同的 *Hypervisor*，且配置在每個端點的 *CPU* 核心數量必須相同。

在受支援的防火牆型號上，您可以建立 HA 防火牆叢集，以確保資料中心內部和其間工作階段的生存能力。如果連結中斷，工作階段將容錯移轉至叢集中的其他防火牆。這種同步在 HA 對等分佈在多個資料中心，或者其分佈在作用中資料中心和備用資料中心之間的使用案例中很有用。其他使用案例是水平擴展，可以將 HA 叢集成員新增到單個資料中心以擴展安全性並確保工作階段的生存能力。HA 配對可以屬於一個 HA 叢集，其在叢集中算作兩個防火牆。HA 叢集中支援的防火牆數量取決於防火牆型號。

- 設定 HA 的重要注意事項
- HA 一般設定
- HA 通訊
- HA 連結和路徑監控
- HA 主動/主動設定
- 叢集組態

設定 HA 的重要注意事項

以下是設定 HA 配對的重要注意事項。

- 用於本機及對等 IP 的子網路不應在虛擬路由器上的其他任何位置使用。
- 各防火牆上的作業系統與內容發佈版本都應相同。不符可能會阻止端點防火牆同步。
- 主要防火牆 HA 連接埠上的 LED 會亮綠燈，而次要防火牆上則會亮黃燈。
- 若要比較本機與端點防火牆的設定，請使用 **Device**（設備）頁籤上的 **Config Audit**（設定檔稽核）工具，在左側選取方塊中選取所需的本機設定，並在右側選取方塊中選取端點設定。
- 按下 **Dashboard**（儀錶盤）上 HA Widget 中的 **Push Configuration**（推送設定），從 Web 介面同步防火牆。您從中推送設定之防火牆的設定會覆寫對等防火牆的設定。若要在主動式防火牆上從 CLI 同步防火牆，請使用命令：request high-availability sync-to-remote running-config。

> 在包含使用 *10 Gigabit SFP+* 連接埠防火牆的高可用性 *(HA)* 主動/被動設定中，當發生容錯轉移且主動防火牆變更為被動狀態時，*10 Gigabit Ethernet* 連接埠會關閉，然後回復以重新整理連接埠，但在防火牆重新變為主動後才會啟用傳輸。如果您已在監視鄰近設備上的軟體，它會將連接埠視為躍動中，因為它會關閉然後重新開啟。此行為與其他連接埠的動作不同，例如 *1 Gigabit* 乙太網路連接埠，後者已停用但仍允許傳輸，因此鄰近設備偵測不到波動。

© 2019 Palo Alto Networks, Inc.

HA 一般設定

- Device > High Availability > General（裝置 > 高可用性 > 一般）

若要設定高可用性 (HA) 配對或 HA 叢集成員，首先選取 **Device**（裝置）> **High Availability**（高可用性）> **General**（一般），然後進行一般設定。

HA 設定	說明
一般頁籤	
HA 配對設定—設定	**Enable HA Pair**（啟用 **HA** 配對）以啟用 HA 配對功能並存取以下設定： • **Group ID**（群組 **ID**）— 輸入用來識別 HA 配對的號碼（1 到 63）。如果相同的廣播網域上駐留多個 HA 配對，則此欄位為必填（且必須是唯一的）。 • **Description**（說明）—（選用）為 HA 配對輸入說明。 • **Mode**（模式）—設定 HA 部署的類型：**Active Passive**（主動/被動）或 **Active Active**（主動/主動）。 • **Device ID**（裝置 **ID**）—在主動/主動設定下，設定裝置 ID 以確定哪個端點為主動-主要（將 **Device ID**（裝置 **ID**）設定為 **0**）以及哪個端點為主動-次要（將 **Device ID**（裝置 **ID**）設定為 **1**）。 • **Enable Config Sync**（啟用組態同步）—選取此選項可在端點間啟用組態設定同步。 啟用設定同步，以便兩個裝置始終具有相同的設定並以相同的方式處理流量。 • **Peer HA1 IP Address**（對等 **HA1 IP** 位址）—輸入端點防火牆 HA1 介面的 IP 位址。 • **Backup Peer HA1 IP Address**（備份端點 **HA1 IP** 位址）—輸入端點的備份控制連結的 IP 位址。 設定一個備用對等 *HA1 IP* 位址，以便在主連結出現故障時，備份連結可使防火牆保持同步和最新狀態。

主動式/被動式設定	• **Passive Link State**（被動式連結狀態）—選取下列其中一個選項以指定被動防火牆上的資料連結是否應當保持啟用。此選項不適用於 AWS 中的 VM 系列防火牆。
	  • **Shutdown**（關機）—強制介面連結處於關閉狀態。這是預設選項，可確保不在網路中建立迴圈。
	  • **Auto**（自動）—擁有實體連線的連結保持實體開啟，但處於停用狀態；不參與 ARP 學習或封包轉送。這在容錯轉移期間有助於進行整合，因為開啟連結的時間已儲存。為了避免網路迴圈，如果防火牆設定了任何 Layer 2 介面，請勿選取此選項。
	  如果防火牆未設定第二層介面，請將 *Passive Link State*（被動式連結狀態）設定為 *auto*（自動）。
	• **Monitor Fail Hold Down Time (min)**（監控失敗抑制時間（分鐘））—防火牆處於非作用狀態多久時間後將成為被動狀態的分鐘數（範圍是 1 至 60）。此計時器用於因為連結或路徑監控失敗而遺失活動訊號或 Hello 訊息時。

© 2019 Palo Alto Networks, Inc.

HA 設定	說明
選取設定	指定或啟用下列設定： • **Device Priority**（裝置優先順序）— 輸入識別主要防火牆的優先順序值。在配對的兩個防火牆上啟用先佔功能時，具有較低值（優先順序較高）的防火牆會成為主動防火牆（範圍是 0 至 255）。 • **Preemptive**（先佔）— 使較高優先順序防火牆在從失敗復原之後可以繼續執行主動（主動/被動）或主動-主要（主動/主動）操作。若要使較高優先順序防火牆於失敗後復原時能夠繼續執行主動或主動-主要操作，您必須在兩個防火牆上都啟用先佔選項。如果此設定為停用，則即使在較高優先順序防火牆從失敗復原之後，較低優先順序的防火牆仍然會保持主動或主動-主要。 是否啟用 *Preemptive*（先佔）選項視乎您的業務需求而定。如果您需要主裝置作為使用中裝置，請啟用 *Preemptive*（先佔），以便在從故障中復原後，主裝置會先佔次要裝置。如果您需要最少的容錯轉移事件，則停用 *Preemptive*（先佔）選項，以便在容錯轉移後，*HA* 配對不會再次進行容錯轉移，使較高優先順序的防火牆成為主防火牆。 • 活動訊號備份 — 使用 HA 防火牆上的管理連接埠來為活動訊號與您好訊息提供備份路徑。會透過 HA1 控制連結將管理連接埠 IP 位址與 HA 端點共用。不需要其他設定。 如果您在 *HA1* 以及 *HA1* 備份連結使用頻內連接埠，啟用 *Heartbeat Backup*（活動訊號備份）。如果您在 *HA1* 或 *HA1* 備份連結使用管理連接埠，請勿啟用 *Heartbeat Backup*（活動訊號備份）。

	• **HA Timer Settings**（**HA** 計時器設定）—選取其中一個預設的設定檔：
	  • **Recommended**（建議）：使用一般的容錯轉移計時器設定。除非您確定您需要不同的設定，否則最佳做法是使用 **Recommended**（建議）的設定。
	  • **Aggressive**（積極）：使用較快的容錯轉移計時器設定。
	  若要檢視設定檔包含的個別計時器的預設值，請選取 *Advanced*（進階），然後選取 *Load Recommended*（建議的載入）或 *Load Aggressive*（積極的載入）。畫面將顯示硬體機型的預設值。
	  • **Advanced**（進階）：可讓您自訂值以符合下列每個計時器的網路需求：
	  • **Promotion Hold Time (ms)**（提升保留時間（毫秒）—被動對等（在主動/被動模式下）或主動-次要對等（在主動/主動模式下）在失去與 HA 對等之間的通訊後，接管成為主動或主動-主要對等之前需等待的毫秒數。此保留時間將僅在對等失敗宣告之後開始。
	  • **Hello Interval (ms)**（**Hello** 間隔（毫秒））—傳送以確認其他防火牆上的 HA 程式是否可正常操作之 hello 封包間的毫秒數（範圍是 8,000 至 60,000；預設值為 8,000）。
	  • **Heartbeat Interval (ms)**（活動訊號間隔（毫秒））—指定 HA 對等以 ICMP ping 形式交換活動訊號訊息的頻率（範圍是 1,000 至 60,000，無預設值）。

	• **Flap Max**（最大擺動數）—當防火牆自上次保持主動狀態後脫離「主動」狀態的 15 分鐘內可設定的擺動計數。指定在判定防火牆進入暫停狀態，及被動防火牆接管前允許的擺動數上限（範圍是 0 至 16，預設值為 3）。此門檻值亦可設定為「0」（代表在被動防火牆接手前不考慮擺動發生的次數）。

© 2019 Palo Alto Networks, Inc.

HA 設定	說明
	• **Preemption Hold Time (min)**（先佔保留時間（分鐘）—被動或主動-次要對等在接管成為主動或主動-主要對等之前將等待的分鐘數（範圍是 1 至 60，預設值為 1）。 • **Monitor Fail Hold Up Time (ms)**（監控失敗維持時間（毫秒））— 防火牆在路徑監控或連結監控失敗後，將於其間保持使用中狀態的時間間隔（毫秒）。建議使用此設定，以避免由於相鄰裝置偶爾擺動所致的 HA 容錯轉移（範圍是 0 至 60,000；預設值為 0）。 • **Additional Master Hold Up Time (ms)**（其他主機維持時間（毫秒））— 適用於與「監控失敗維持時間」相同的事件之其他時間（毫秒）（範圍是 0 至 60000，預設值為 500）。其他時間間隔僅適用於主動/被動模式下的主要端點，及適用於主動/主動模式下的主動主要端點。建議使用此計時器，以避免兩個對等同時遇到相同連結或路徑監控失敗時的容錯轉移。
SSH HA 設定檔設定	一種 SSH 服務設定檔，適用於網路上高可用性 (HA) 設備的 SSH 工作階段。若要套用現有的 HA 設定檔，請選取一個設定檔，按一下 **OK**（確定），然後 **Commit**（提交）您的變更。 *您必須透過 CLI 執行 SSH 服務重新啟動，才能啟動設定檔。* 如需詳細資訊，請參閱Device > Certificate Management > SSH Service Profile（裝置 > 憑證管理 > SSL 服務設定檔）。
叢集設定	**Enable Cluster Participation**（啟用叢集參與）以存取叢集設定。支援 HA 叢集的防火牆允許成員防火牆叢集（個人或 HA 配對，其中成對的每個防火牆都計入總數）。防火牆型號支援的每個叢集的成員數如下： • PA-3200 系列：6 名成員 • PA-5200 系列：16 名成員 • PA-7080 系列：4 名成員 • PA-7050 系列：6 名成員 設定叢集： • **Cluster ID**（叢集 ID）—HA 叢集的唯一數字 ID，所有成員都可在其中共用工作階段狀態（範圍是1 至 99；無預設值）。 • **Cluster Description**（叢集說明）—叢集簡短且有用的說明。 • **Cluster Synchronization Timeout (min)**（叢集同步逾時（分鐘）—當另一個叢集成員（例如，處於未知狀態）阻止叢集完全同步時，本機防火牆在進入作用中狀態之前等待的最大分鐘數（範圍為 0 至 30；預設值為 0）。 • **Monitor Fail Hold Down Time (min)**（監控失敗抑制時間（分鐘）—將在其後對失效的連結進行重新測試以查看其是否恢復的分鐘數（範圍為 1 至 60；預設值為 1）。
操作命令	
Suspend local device（或啟用本機裝置）	若要將本機 HA 對等置於暫停狀態並暫時停用其 HA 功能，請使用以下 CLI 操作命令： • `request high-availability state suspend` 若要將暫停的本機 HA 對等恢復到功能狀態，請使用 CLI 操作命令： • `request high-availability state functional`

© 2019 Palo Alto Networks, Inc.

HA 設定	說明
	若要測試容錯移轉，您可以使主動（或主動-主要）防火牆無法啟用。

HA 通訊

- Device > High Availability > HA Communications（裝置 > 高可用性 > HA 通訊）

若要為 HA 配對或 HA 叢集設定 HA 連結，請選取 **Device**（裝置）> **High Availability**（高可用性）> **HA Communications**（**HA** 通訊）。

HA 連結	說明
控制連結 (HA1)/控制連結 (HA1 備份)	HA 配對中的防火牆會使用 HA 連結 來同步處理資料及維護狀態資訊。某些防火牆型號具有專用的控制鏈路以及專用的備份控制鏈路；例如，PA-5200 系列防火牆具有 HA1-A 和 HA1-B。在此情況下，您應該在「選取設定」中啟用「活動訊號備份」選項。如果您針對控制鏈路 HA 連結使用專屬 HA1 連接埠，並針對控制鏈路（HA 備份）使用資料連接埠，建議您啟用 Heartbeat Backup（活動訊號備份）選項。 針對沒有專用 HA 連接埠的防火牆（例如 PA-220 防火牆），您應針對控制連結 HA 連線組態管理連接埠，並針對控制連結 HA1 備份連線使用以類型 HA 設定的資料連接埠介面。由於在此情況下會使用管理連接埠，因此不需要啟用活動訊號備份選項，因為活動訊號備份將已透過管理介面連線發生。 在 AWS 中的 VM 系列防火牆上，管理連接埠將作為 HA1 連結使用。 當針對 *HA* 控制連結使用資料連接埠時，請謹記由於控制訊息必須從資料平面傳送至管理平面，如果在資料平面中發生失敗，端點將無法傳送 *HA* 控制連結資訊並發生容錯轉移。最好使用專用 *HA* 連接埠，或在沒有專用 *HA* 連接埠的防火牆上使用管理連接埠。
控制連結 (HA1)/控制連結 (HA1 備份)	針對主要與備份 HA 控制連結指定下列設定： • 連接埠 — 選取主要與備份 HA1 介面的 HA 連接埠。備份設定為選用。 • **IPv4/IPv6** 位址 — 針對主要與備份 HA1 介面輸入 HA1 介面的 IPv4 或 IPv6 位址。備份設定為選用。 *PA-3200* 系列防火牆不為備份 *HA1* 介面支援 *IPv6* 位址；使用 *IPv4* 位址。 • 網路遮罩—為主要與備份 HA1 介面輸入 IP 位址的網路遮罩（例如 255.255.255.0）。備份設定為選用。 • 閘道—針對主要與備份 HA1 介面輸入預設閘道的 IP 位址。備份設定為選用。 • 連結速度 —（僅限具有專用 HA 連接埠的型號）針對專用 HA1 連接埠選取防火牆間控制連結的速度。 • 連結雙工—（僅限具有專用 HA 連接埠的型號）針對專用 HA1 連接埠選取防火牆間控制連結的雙工選項。 • 已啟用加密 — 在從 HA 端點中匯出 HA 金鑰並將它匯入至此防火牆上之後啟用加密。也必須從此防火牆中匯出此防火牆上的 HA 金鑰並在 HA 端點上匯入它。針對主要 HA1 介面進行此設定。[憑證] 頁面上的匯入/匯出金鑰（請參閱 [裝置 > 憑證管理 > 憑證設定檔]）。 當防火牆不是直接連線時啟用加密（通過網路裝置並可以檢查、處理或擷取流量的 *HA1* 連線）。

© 2019 Palo Alto Networks, Inc.

HA 連結	說明
	• **Monitor Hold Time (ms)**（監控保留時間（毫秒））—輸入防火牆在因控制連結失敗而宣告對等失敗之前將會等待的時間長度，單位為毫秒（範圍是 1,000 到 60,000，預設值為 3,000）。此選項可監控 HA1 連接埠的實體連結狀態。
資料連結 (HA2) 當設定 *HA2* 備份連結時，如果實體連結失敗將會發生備份連結容錯轉移。在啟用 *HA2 keep-alive* 選項的情況下，如果 *HA* 保持運作訊息根據定義的臨界值失敗，也會發生容錯轉移。	針對主要與備份資料連結指定下列設定： • 連接埠 — 選取 HA 連接埠。針對主要與備份 HA2 介面進行此設定。備份設定為選用。 • **IP** 位址 — 針對主要與備份 HA2 介面指定 HA 介面的 IPv4 或 IPv6 位址。備份設定為選用。 • 網路遮罩—針對主要與備份 HA2 介面指定 HA 介面的網路遮罩。備份設定為選用。 • 閘道 — 針對主要與備份 HA2 介面指定 HA 介面的預設閘道。備份設定為選用。如果防火牆 HA2 IP 位址皆在同一個子網路中，閘道欄位應保留空白。 • 啟用工作階段同步 — 啟用工作階段資訊與被動式防火牆間的同步，及選取傳輸選項。 啟動工作階段同步，以便讓次要裝置在其數據平面中具有工作階段，這讓防火牆能夠快速地將封包與同步工作階段比對並快速轉發封包。如果您未啟用工作階段同步，則防火牆必須再次建立工作階段，這會產生延遲並可能導致連線中斷。
	• **Transport**（傳輸）— 選取下列其中一個傳輸選項： • **Ethernet**（以太網路）—當連續或透過交換器連線防火牆時使用 (Ethertype 0x7261)。

© 2019 Palo Alto Networks, Inc.

HA 連結	說明

	• **IP**—當需要第三層傳輸時使用（IP 通訊協定號碼 99）。
	• **UDP** — 用來利用在完整封包而非僅僅是標頭上計算總和檢查碼之事實，與 IP 選項相同（UDP 連接埠 29281）。使用 UDP 模式的優點是提供總和檢查碼來驗證工作階段同步訊息的完整性。
	• （僅限具有專用 HA 連接埠的型號）**Link Speed**（連結速度）—針對專用 HA2 連接埠選取對等間控制連結的速度。
	• （僅限具有專用 HA 連接埠的型號）**Link Duplex**（連結雙工）—針對專用 HA2 連接埠選取對等間控制連結的雙工選項。
	• **HA2 Keep-alive**（**HA2** 保持活動）—最佳做法是選取此選項可監控 HA 對等之間 HA2 資料連結的健康狀況。此選項預設為停用，且您可在一個端點上啟用或兩個端點都啟用。如果啟用，端點將使用保持運作訊息來監控 HA2 連線，根據您設定的 **Threshold**（臨界值）（預設為 10,000 毫秒）來偵測失敗。如果您啟用 HA2 保持活動，將會採用 HA2 保持活動復原動作。選取 **Action**（動作）：
	  • **Log Only**（僅記錄）—將系統日誌中的 HA2 介面失敗記錄為關鍵事件。針對主動/被動部署選取此選項，因為主動端點是唯一的防火牆轉送流量。被動端點處於備份狀態且不轉送流量；因此不需要分割資料路徑。如果您未設定任何 HA2 備份連結，狀態同步將會關閉。如果 HA2 路徑復原，將會產生資訊日誌。
	  • **Split Datapath**（分割資料路徑）—在主動/主動 HA 部署中選取此選項，以在其偵測到 HA2 介面失敗時，指示各端點掌控其本機狀態與工作階段表。沒有 HA2 連線，則不會同步任何狀態與工作階段；此動作允許單獨管理工作階段表以確保各 HA 端點成功轉送流量。為了防止此情況，請設定 HA2 備份連結。
	• **Threshold (ms)**（閾值（毫秒））—在觸發上述其中一個動作之前，保持活動訊息已失敗的持續時間（範圍是 5,000 到 60,000，預設值為 10,000）。

叢集連結	對 HA4 連結進行設定，這是專用的 HA 叢集連結，用於在具有相同叢集 ID 的所有叢集成員之間同步工作階段狀態。叢集成員之間的 HA4 連結能夠偵測叢集成員之間的連線失敗情況。 • **Port**（連接埠）—選取一個 HA 介面作為 HA4 連結（例如 ethernet1/1）。 • **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）—輸入本機 HA4 介面的 IP 位址。 • **Netmask**（網路遮罩）—輸入網路遮罩。 • **HA4 Keep-alive Threshold (ms)**（**HA4** 保持活動閾值（毫秒）—防火牆必須在該範圍內從叢集成員接收保持活動的時長，以了解該叢集成員正在運作；範圍是 5,000 至 60,000；預設值為 10,000。 進行 HA4 備份設定： • **Port**（連接埠）—選取一個 HA 介面作為 HA4 備份連結。 • **IPv4/IPv6 Address**（**IPv4/IPv6** 位址）—輸入本機 HA4 備份連結的位址。 • **Netmask**（網路遮罩）—輸入網路遮罩。

HA 連結和路徑監控

- Device（裝置）> High Availability（高可用性）> Link and Path Monitoring（連結與路徑監控）

若要定義 HA 容錯移轉條件，請設定 HA 連結和路徑監控；選取 **Device**（裝置）> **High Availability**（高可用性）> **Link and Path Monitoring**（連結和路徑監控）。

連結監控和路徑監控不適用於 *AWS* 中的 *VM-Series* 防火牆。

© 2019 Palo Alto Networks, Inc.

HA 連結和路徑監控設定	說明
連結監控	指定下列設定： • **Enabled**（已啟用）—啟用連結監控。連結監控可讓容錯轉移在實體連結或實體連結的群組失敗時觸發。 • **Failure Condition**（失敗條件）—選取當任何或所有監控的連結群組失敗時是否發生容錯轉移。 啟用並設定路徑監控或連結監控，以便在路徑或連結失效時幫助觸發容錯轉移。為路徑監控設定至少一個*Path Group*（路徑群組），並為連結監控設定至少一個*Link Group*（連結群組）。
連結群組	定義監控特定 Ethernet 連結的一或多個連結群組。若要新增連結群組，請指定下列項目並按一下 **Add**（新增）： • **Name**（名稱）—輸入連結群組名稱。 • **Enabled**（已啟用）—啟用連結群組。 • **Failure Condition**（失敗條件）—選取在任何或所有選取的連結失敗時是否發生失敗。 • **Interfaces**（介面）—選取要監控的一或多個乙太網路介面。

路徑監控	指定下列設定：
	• **Enabled**（已啟用）—根據組合或單獨的虛擬介接路徑監控、VLAN 路徑監控和虛擬路由器*路徑監控來啟用路徑監控。路徑監控可讓防火牆監控指定的目的地 IP 位址，方法是傳送 ICMP ping 訊息以確定它們是否有回應。針對 Virtual Wire、第二層或第三層設定進行路徑監控，只進行容錯轉移與連結監控所需的其他網路裝置監控是不足的。
	• **Failure Condition**（失敗條件）：
	  • **Any**（任何）—（預設）當虛擬介接或 VLAN 或虛擬路由器*的路徑監控失敗時，防火牆會觸發 HA 容錯移轉。
	  • **All**（全部）—當對虛擬介接、VLAN 和虛擬路由器*的路徑監控失敗時（啟用這三個選項中的任何一個），防火牆均會觸發 HA 容錯移轉。
	*若啟用了「進階路由」，則「邏輯路由器」將取代「虛擬路由器」，並且可以啟用「邏輯路由器路徑監控」。
	啟用並設定路徑監控或連結監控，以便在路徑或連結失效時幫助觸發容錯轉移。為路徑監控設定至少一個*Path Group*（路徑群組），並為連結監控設定至少一個*Link Group*（連結群組）。

路徑群組	為介面類型定義監控特定目的地位址的一或多個路徑群組。**Add Virtual Wire Path**（新增虛擬介接）、**Add VLAN Path**（新增 **VLAN** 路徑）和 **Add Virtual Router Path**（新增虛擬路由器路徑）。（若啟用了「進階路由」，則可以 **Add Logical Router Path**（新增邏輯路由器路徑）。 對於新增的每種路徑監控類型，請指定以下內容： • **Name**（名稱）—選取虛擬介接、VLAN 或虛擬路由器*進行監控（下拉式選項基於您要新增的路徑監控類型）。 • **Source IP**（來源 **IP**）—對於虛擬介接與 VLAN 介面，輸入在已傳送至下一個躍點路由器（目的地 IP 位址）的 Ping 中所使用之來源 IP 位址。本機路由器必須能夠將位

© 2019 Palo Alto Networks, Inc.

HA 連結和路徑監控設定	說明

	址傳送至防火牆。（路徑群組（與虛擬路由器*相關聯）的來源 IP 位址將自動設定為介面 IP 位址，在路由表中，此介面 IP 位址被指定為指定目的地 IP 位址的輸出介面。）
	• **Enabled**（已啟用）—啟用虛擬介接、VLAN 或虛擬路由器*監控。
	• **Failure Condition**（失敗條件）：
	  • **Any**（任何）（預設）—當任何目的地 IP 群組中發生 Ping 失敗時，防火牆將確定虛擬介接、VLAN 或虛擬路由器*發生了故障。
	  • **All**（全部）—當所有目的地 IP 群組中發生 Ping 失敗時，防火牆將確定虛擬介接、VLAN 或虛擬路由器*發生了故障。
	實際的 *HA* 容錯移轉取決於您為「路徑監控」設定的「失敗條件」，其考慮了虛擬介接、*VLAN* 和虛擬路由器*路徑監控（無論啟用哪一個）。
	• **Ping Interval**（**Ping** 間隔）—指定傳送至目的地 IP 位址的 Ping 之間的間隔（範圍是 200 到 60,000 毫秒，預設值為 200 毫秒）。
	• **Ping** 計數—指定宣告失敗前失敗的 ping 數（範圍是 3 到 10，預設值為 10）。
	*若啟用了「進階路由」，則「邏輯路由器」將取代「虛擬路由器」，並且可以啟用「邏輯路由器路徑監控」。

路徑群組的目的地 IP	• **Destination IP**（目的地 **IP**）—**Add**（新增）一個或多個目的地 IP 位址群組以監控路徑群組。
	  • **Destination IP Group**（目的地 **IP** 群組）—輸入群組的名稱。
	  • **Add**（新增）一個或多個 **Destination IP**（目的地 **IP**）位址以監控群組。
	  • **Enabled**（已啟用）—選取以啟用目的地 IP 群組。
	  • **Failure Condition**（失敗條件）：選取 **Any**（任何）（以指定若群組中的任何 IP 位址都執行 Ping 操作失敗，則認為目的地群組已失敗）或 **All**（全部）（以指定若群組中的所有 IP 位址都執行 Ping 操作失敗，則認為目的地群組已失敗）。

HA 主動/主動設定

- Device > High Availability > Active/Active Config（裝置 > 高可用性 > 主動/主動設定）

若要對主動/主動 HA 配對進行設定，請選取 **Device**（裝置）> **High Availability**（高可用性）> **Active/Active Config**（主動/主動設定）。

主動/主動設定	說明
封包轉送	**Enable**（啟用）端點以透過 HA3 連結轉送封包，對非對稱路由工作階段進行工作階段設定及 Layer 7 檢驗（App-ID、Content-ID 及威脅檢驗）。
HA3 介面	選取您計劃用於在主動/主動 HA 端點之間轉送封包的資料介面。您使用的介面必須是設定為介面類型 **HA** 的專用第二層介面。 如果 *HA3* 連結失敗，主動-次要端點將轉送至非作用狀態。為了防止此情況，請設定連結彙總群組 *(LAG)* 介面，並將兩個或多個實體介面

© 2019 Palo Alto Networks, Inc.

主動/主動設定	說明
	作為 *HA3* 連結。防火牆不支援 *HA3* 備份連結。擁有多個介面的彙總介面將其他額外容量及連結備援，以支援 *HA* 端點之間的封包轉送。 使用 HA3 介面時，您必須在防火牆和所有中間的網路裝置上啟用 Jumbo Frames。若要啟用巨型框架，請選取 **Device**（裝置）> **Setup**（設定）> **Session**（工作階段），然後在「工作階段設定」區段中選取 **Enable Jumbo Frame**（啟用巨型框架）選項。
VR 同步處理	強制 HA 端點上設定的所有虛擬路由器進行同步。 沒有為動態路由通訊協定設定虛擬路由器時，請使用此選項。必須透過交換式網路將兩個對等體都連線至相同的下一個躍點路由器，且只能使用靜態路由。
QoS 同步處理	同步所有實體介面上選取的 QoS 設定檔。當兩個端點的連結速度相似，且需要所有實體介面上的 QoS 設定檔都相同時，請使用此選項。此設定會影響 **Network**（網路）頁籤上 QoS 設定的同步。無論此設定為何，都會同步 QoS 原則。
暫訂保留時間 (秒)	當 HA 主動/主動組態中的防火牆失敗時，它會進入暫訂狀態。暫訂狀態至主動-次要狀態的過渡將觸發暫訂保留時間，在此期間，防火牆先嘗試建立路由相鄰項，並將其填入至路由表，再處理任何封包。若欠缺此計時器，復原防火牆將立即進入主動-次要狀態，並會無訊息捨棄封包，因為它不會有必要的路由（預設值為 60 秒）。
工作階段擁有者選取項	工作階段擁有者負責工作階段的所有 Layer 7 檢驗（App-ID 及 Content-ID））以及為工作階段產生所有流量日誌。選取下列其中一個選項以指定如何決定封包的工作階段擁有者： • 第一個封包—選取此選項可將接收工作階段中第一個封包的防火牆指定為工作階段擁有者。這是可最大限度地減少 HA3 間的流量，並在端點間分配資料平面負載的最佳設定做法。 • 主要裝置—如果您想要主動-主要防火牆擁有所有工作階段，請選取此選項。在此情況下，如果主動-次要防火牆接收第一個封包，它會透過 HA3 連結將所有需要 Layer 7 檢驗的封包轉送至主動-主要防火牆。

虛擬位址	按一下 **Add**（新增），選取 **IPv4** 或 **IPv6** 頁籤，然後再次按一下 **Add**（新增）進入選項，指定要使用的 HA 虛擬位址類型：浮動或 ARP 負載共用。您也可在配對中混合虛擬位址的類型。例如，您可以在 LAN 介面及 WAN 介面的浮動 IP 上使用 ARP 負載共用。
	
	• 浮動 — 輸入會在連結或系統失敗的情況下在 HA 端點之間移動的 IP 位址。在介面上設定兩個浮動 IP 位址，使每個防火牆都有一個位址，然後設定優先順序。如果防火牆之一發生失敗，浮動 IP 位址將會轉換給 HA 端點。
	  • 裝置 **0** 優先順序 — 設定擁有裝置 ID 0 的防火牆的優先順序，以決定哪個防火牆將擁有浮動 IP 位址。有最低值的防火牆將有最高優先順序。
	  • 裝置 **1** 優先順序 — 設定擁有裝置 ID 1 的防火牆的優先順序，以決定哪個防火牆將擁有浮動 IP 位址。有最低值的防火牆將有最高優先順序。
	  • 如果連結狀態為中斷則容錯轉移位址 — 當介面上的連結狀態為關閉時使用容錯轉移位址。
	  • 浮動 **IP** 連接至主動-主要 **HA** 裝置—選取此選項以將浮動 IP 位址連接至主動-主要端點。如果一個端點失敗，即使在故障防火牆復原並變為主動-次要端點之後，流量仍將繼續傳送至主動-主要端點。

虛擬位址（續）	• **ARP** 負載分享—輸入將由 HA 配對共用並會為主機提供閘道服務的 IP 位址。只有當防火牆與主機處於同一廣播網域時，才需要此選項。選取裝置選取演算法：

© 2019 Palo Alto Networks, Inc.

主動/主動設定	說明
	• **IP Modulo**（**IP** 模數）— 選取會根據 ARP 要求者 IP 位址的同位性來選取將回應 ARP 要求的防火牆。 • **IP** 雜湊 — 選取會根據 ARP 要求者 IP 位址的雜湊來選取將回應 ARP 要求的防火牆。

叢集組態

- Device > High Availability > Cluster Config（裝置 > 高可用性 > 叢集組態）

透過選取 **Device**（裝置）> **High Availability**（高可用性）> **Cluster Config**（叢集組態），將成員新增至 HA 叢集。

叢集組態	說明
Add（新增）	**Add**（新增）叢集成員。您必須新增本機防火牆，並且如果使用 HA 配對，則必須將該配對的兩個 HA 對等都新增為叢集成員。 • （支援的防火牆）**Device Serial Number**（裝置序號）—輸入叢集成員的唯一序號。 • （Panorama）**Device**（裝置）—從下拉式清單中選取裝置，然後輸入 **Device Name**（裝置名稱）。 • **HA4 IP Address**（**HA4 IP** 位址）—輸入叢集成員的 HA4 連結的 IP 位址。 • **HA4 Backup IP Address**（**HA4** 備份 **IP** 位址）—輸入叢集成員的備份 HA4 連結的 IP 位址。 • **Session Synchronization**（工作階段同步）—選取該項以啟用與此叢集成員的工作階段同步。 • **Description**（說明）—輸入有用的說明。
Delete（刪除）	選取一個或多個叢集成員，然後從叢集中將其 **Delete**（刪除）。
啟用	（支援的防火牆）您可以確定叢集成員是否與其他成員同步工作階段。依預設，允許所有成員同步工作階段。如果停用一個或多個成員的同步，請選取 **Enable**（啟用），以重新啟用一個或多個成員的同步。
Disable（停用）	（支援的防火牆）選取一個或多個成員，並 **Disable**（停用）與其他成員的同步。
Refresh（重新整理）	（Panorama）選取 **Refresh**（重新整理），以重新整理 HA 叢集中的 HA 裝置清單。

© 2019 Palo Alto Networks, Inc.

裝置 > 日誌轉送卡

- 裝置 > 日誌轉送卡

日誌轉送卡 (LFC) 是一種高效能日誌卡，可將所有資料層日誌（例如流量和威脅）從防火牆轉送到一個或多個外部日誌記錄系統，例如 Panorama 或 syslog 伺服器。由於資料層日誌在本機防火牆上不再可用，因此從管理 Web 介面中移除 ACC 頁籤，並且「監控 > 日誌」僅包含管理日誌（組態，系統與警報）。

您需要為 LFC 設定連接埠。連接埠 1 以 10Gbps 運行，連接埠 9 以 40Gbps 運行。在 **Device > Log Forwarding Card**（裝置 > 日誌轉送卡）內設定連接埠。防火牆使用這些連接埠以將所有資料層日誌轉送到外部系統，例如 Panorama 或 syslog 伺服器。

如需 LFC 要求與元件的相關資訊，請參閱 PA-7000 系列硬體參考指南。

對於 LFC 介面，請設定下表中所述的設定。

LFC 介面設定	說明
名稱	輸入介面名稱。對於 LFC，必須選取 **lfc1/1** 或 **lfc1/9**。
備註	輸入介面的選取性說明。
IPv4	如果網路使用 IPv4，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv4 位址。 • **Netmask**（網路遮罩）—連接埠之 IPv4 位址的網路遮罩。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv4 位址。
IPv6	如果網路使用 IPv6，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv6 位址。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv6 位址。
連結速度	選取以 Mbps 為單位的介面速度（**10000** 或 **40000**），或選取 **auto**（自動）（預設值），讓防火牆根據連線自動決定速度。可用的介面速度取決於使用的連接埠（lfc1/1 或 lfc1/9）。對於不可設定速度的介面，**Auto**（自動）將是唯一選項。
連結狀態	根據連接選取介面狀態是已啟用 (**Up**)、已停用 (**Down**) 還是自動判斷 (**Auto**)。預設值為 **Auto**（自動）。
LACP 連接埠優先順序	只有為彙總群組啟用連結彙總控制協定 (LACP)，防火牆才會使用此值。如果指派給群組的介面數超出作用中介面數（連接埠上限欄位），防火牆會使用介面的 LACP 連接埠優先順序來決定哪些介面將處於待命模式。數值越低，優先順序越高（範圍是 1-65,535；預設為 32,768）。

如果啟用了多個 vsys，則可以使用子介面。若要設定 LFC 子介面，請新增子介面並使用下表內所述的設定。

LFC 子介面設定	說明
介面名稱	**Interface Name**（介面名稱）（唯讀）會顯示您所選日誌卡介面的名稱。在相鄰的欄位中，輸入用來識別子介面的數值尾碼 (1-9,999)。

© 2019 Palo Alto Networks, Inc.

LFC 子介面設定	說明
備註	輸入介面的選取性說明。
頁籤	輸入子介面的 VLAN **Tag**（頁籤）(0-4,094)。 讓頁籤等於子介面號碼，以方便使用。
虛擬系統	選取要將日誌轉送卡 (LFC) 子介面指派給哪一個虛擬系統 (vsys)。或者，您可以按一下 **Virtual Systems**（虛擬系統）連結以新增新 vsys。LFC 子介面指派給 vsys 後，對於所有從日誌卡轉送日誌（Syslog、電子郵件、SNMP）的服務，系統會將該介面作為這類服務的來源介面。
IPv4	如果網路使用 IPv4，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv4 位址。 • **Netmask**（網路遮罩）—連接埠之 IPv4 位址的網路遮罩。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv4 位址。
IPv6	如果網路使用 IPv6，請定義下列項目： • **IP Address**（**IP** 位址）—連接埠的 IPv6 位址。 • **Default Gateway**（預設閘道）—連接埠之預設閘道的 IPv6 位址。

© 2019 Palo Alto Networks, Inc.

Device > Config Audit（裝置 > 組態稽核）

選取 **Device**（設備）> **Config Audit**（設定稽核），可檢視設定檔案間的差異。頁面在單獨的窗格並排顯示設定，並逐行反白顯示差異，以指出新增項（綠色）、修改項（黃色）或刪除項（紅色）：

Added	Modified	Deleted

設定稽核設定	說明
組態名稱下拉式清單（未標記）	選取兩個組態以在（未標記）組態名稱下拉式清單中作比較（預設為 **Running config**（執行中組態）及 **Candidate config**（候選組態）。 您可以輸入與所需設定相關聯之認可作業的 說明（說明）值所衍生出來的文字字串，以篩選下拉式清單（請參閱認可變更）。
內容下拉式清單	使用 **Context**（內容）下拉式清單可指定行數，以在各檔案中反白顯示的差異前後顯示。指定更多行可幫助您將稽核結果關聯至 Web 介面中的設定。如果您將 **Context**（內容）設定為 **All**（全部），結果將會包含整個設定檔案。
開始	按一下 **Go**（前往）可啟動稽核。
上一個（‹‹）及 下一個（››）	在組態名稱下拉式清單中選取連續組態版本時，將啟用這些導覽箭頭。按一下 ‹‹ 以比較下拉式清單中的上一對組態，或按一下 ›› 以比較下一對組態。

© 2019 Palo Alto Networks, Inc.

裝置 > 密碼設定檔

- 裝置 > 密碼設定檔
- Panorama > 密碼設定檔

選取 **Device**（設備）> **Password Profiles**（密碼設定檔）或 **Panorama** > **Password Profiles**（密碼設定檔）為個別本機帳戶設定基本密碼要求。密碼設定檔會覆寫任何您為所有本機帳戶所定義的最低密碼複雜度設定（**Device**（設備）> **Setup**（設定）> **Management**（管理））。

若要將密碼設定檔套用至帳戶，請選取 **Device**（設備）> **Administrators**（管理員）（防火牆）或 **Panorama** > **Administrators**（管理員）（Panorama），選取帳戶，然後選擇 **Password Profile**（密碼設定檔）。

您無法將密碼設定檔指派給使用本機資料庫驗證的管理員帳戶（請參閱 *[設備 > 本機使用者資料庫 > 使用者]*）。

若要建立密碼設定檔，請按一下 **Add**（新增）並指定下表中的資訊。

密碼設定檔設定	說明
名稱	輸入用來識別密碼設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
要求的密碼變更期間（天數）	要求管理員根據所指定的天數（範圍是 0 至 365 天），定期變更其密碼。例如，如果將值設定為 90，則將提示管理員每 90 天變更一次密碼。您也可以設定 0 到 30 天的到期警告，並指定寬限期。
到期警告期間（天數）	如果已設定所需密碼變更週期，則在強制密碼變更日期即將到達時，此設定可用於在每次登入時提示使用者變更其密碼（範圍是 0 到 30）。
到期後管理員的登入計數	允許管理者在其帳戶過期後登入指定次數。例如，如果將值設定為 3 且其帳戶已過期，則其可以在帳戶遭到鎖定之前再登入 3 次（範圍是 0 到 3）。
到期後寬限期（天數）	允許管理員在其帳戶過期後登入指定天數（範圍是 0 到 30）。

使用者名稱和密碼需求

下表列出可在 PAN-OS 與 Panorama 帳戶的使用者名稱與密碼中使用的有效字元。

帳戶類型	使用者名稱和密碼限制
密碼字元集	對任何密碼欄位字元集都沒有限制。
遠端管理員、SSL-VPN 或驗證入口網站	不允許在使用者名稱中使用下列字元： • 倒引號 (`) • 尖括號（< 與 >） • 符號 (&) • 星號 (*)

© 2019 Palo Alto Networks, Inc.

帳戶類型	使用者名稱和密碼限制
	• 符號 (@) • 問號 (?) • 直立線符號 (|) • 單引號 (‘) • 分號 (;) • 雙引號 (") • 貨幣符號 ($) • 括號 ('(' 與 ')') • 冒號 (':')
本機管理員帳戶	以下是本機使用者名稱的允許字元： • 小寫 (a-z) • 大寫 (A-Z) • 數字 (0-9) • 底線 (_) • 句點 (.) • 連字號 (-) 登入名稱開頭不可為連字號 *(-)*。

© 2019 Palo Alto Networks, Inc.

Device > Administrators（裝置 > 管理員）

管理者帳戶控制對防火牆與 Panorama 的存取權。防火牆管理員可以擁有單一防火牆或單一防火牆上虛擬系統的完整或唯讀存取權。防火牆擁有預先定義的 **admin**（管理員）帳戶，該帳戶具有完整存取權。

若要定義 *Panorama* 管理員，請參閱 Panorama > 受管理的裝置 > 摘要。

支援以下驗證選項：

- 密碼驗證 — 管理員輸入使用者名稱與密碼進行登入。此驗證不需要憑證。您可以將此選項與驗證設定檔搭配使用，或進行本機資料庫驗證。
- 用戶端憑證驗證 (Web) — 此驗證不需要使用者名稱或密碼；憑證足以驗證防火牆的存取權。
- 公開金鑰驗證 (SSH) — 管理員可以在需要存取防火牆的電腦上，產生公開/私密金鑰配對，然後將公開金鑰上載到防火牆，允許管理員不輸入使用者名稱與密碼就能進行安全性存取。

若要新增管理員，請按一下 **Add**（新增）並填寫下列資訊：

管理員帳戶設定	說明
名稱	輸入管理員的登入名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、連字號、句點與底線。登入名稱開頭不可為連字號 (-)。
驗證設定檔	選取驗證設定檔進行管理員驗證。您可以使用此設定進行 RADIUS、TACACS+、LDAP、Kerberos、SAML 或本機資料庫驗證。如需詳細資訊，請參閱 [裝置 > 驗證設定檔]。
僅使用用戶端憑證驗證 (Web)	選取此選項可使用用戶端憑證驗證存取 Web。如果您選取此選項，使用者不需要輸入使用者名稱與密碼；憑證足以驗證防火牆的存取權。
新密碼 確認新密碼	輸入及確認管理員的區分大小寫密碼（最多 31 個字元）。您也可以選取 **Setup**（設定）> **Management**（管理），以強制執行最小密碼長度。 若要確保防火牆管理介面保持安全，我們建議您定期變更管理密碼，並使用大小寫字母與數字混合的形式。此外，您還可為防火牆上的所有管理員設定最低密碼複雜度設定。
使用公開金鑰驗證 (SSH)	選取此選項可使用 SSH 公開金鑰驗證。按一下 **Import Key**（匯入金鑰），瀏覽並選取公開金鑰檔案。已上傳的金鑰會顯示在唯讀的文字區域內。 支援的金鑰檔案格式是 IETF SECSH 與 OpenSSH。支援的金鑰演算法是 DSA（1,024 位元）和 RSA（768 - 4,096 位元）。 如果公共金鑰驗證失敗，防火牆將提示管理員輸入使用者名稱與密碼。

© 2019 Palo Alto Networks, Inc.

管理員帳戶設定	說明
管理員類型	將角色指定給此管理員。角色可決定管理員可以檢視及修改的內容。 如果您選取 **Role Based**（以角色為基礎），請從下拉式清單中選取自訂角色設定檔。如需詳細資訊，請參閱 [裝置 > 管理角色]。 如果您選取 **Dynamic**（動態），您可以選取下列其中一個預先定義的角色： • 超級使用者—擁有防火牆的完整存取權，並且可定義新的管理員帳戶和虛擬系統。您必須擁有超級使用者權限，才可建立具有超級使用者權限的管理員使用者。 • 超級使用者（唯讀）—擁有防火牆的唯讀存取權。 • 裝置管理員—擁有所有防火牆設定的完整存取權，但無法定義新的帳戶或虛擬系統。 • 裝置管理員（唯讀）—擁有所有防火牆設定的唯讀存取權，但密碼設定檔（無法存取）和管理員帳戶（僅登入帳戶可見）除外。 • 虛擬系統管理員—對防火牆上的特定虛擬系統具有存取權限，可以建立和管理虛擬系統的特定方面（如果啟用了多虛擬系統功能）。虛擬系統管理員無法存取網路介面、虛擬路由器、IPSec 通道、VLAN、虛擬介接、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。 • 虛擬系統管理員（唯讀）—對防火牆上的特定虛擬系統具有唯讀存取權限，可檢視虛擬系統的特定方面（如果啟用了多虛擬系統功能）。具有唯讀存取權限的虛擬系統管理員無法存取網路介面、虛擬路由器、IPSec 通道、VLAN、虛擬介接、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。
虛擬系統 （僅限虛擬系統管理員角色）	按一下 **Add**（新增），選取管理員可管理的虛擬系統。
密碼設定檔	如果適用，選取密碼設定檔。若要建立新的密碼設定檔，請參閱 [裝置 > 密碼設定檔]。 為管理員建立密碼設定檔，確保管理員密碼在設定的時段後過期。定期變更管理員密碼有助於防止攻擊者使用儲存的或被盜的憑證。

© 2019 Palo Alto Networks, Inc.

Device > Admin Roles（裝置 > 管理員角色）

選取 **Device**（裝置）> **Admin Roles**（管理員角色）可定義管理員角色設定檔，這是決定管理使用者之存取權限和職責的自訂角色。您可在建立管理帳號（裝置 > 動態角色）時指派管理員角色設定檔或動態角色。

若要為 *Panorama* 管理員定義管理員角色設定檔，請參閱（Panorama > 受管理的裝置 > 摘要）。

防火牆具有三個預先定義的角色，可基於通用條件目的進行使用。您可以先使用超級使用者角色設定初始防火牆組態，然後為安全性管理員、稽核管理員與密碼管理員建立管理員帳戶。您建立這些帳戶並套用適當的通用條件管理員角色後，即可使用這些帳戶登入。聯邦資訊處理標準 (FIPS)/通用準則 (CC) FIPS-CC 模式下的預設超級使用者帳戶為 **admin**，預設密碼為 **paloalto**。在標準操作模式下，預設 **admin** 密碼為 **admin**。除非所有角色都擁有對稽核記錄的唯讀存取權（擁有完整讀取/刪除存取權的稽核管理員除外），否則會在功能無重疊的情況下建立預先定義的管理員角色。這些管理員角色無法修改，且定義如下：

- auditadmin—稽核管理員負責定期檢閱防火牆的稽核資料。
- cryptoadmin — 密碼管理員負責設定及維護與建立防火牆的安全連線相關的密碼元件。
- securityadmin—安全管理員負責另外兩個管理角色未處理的其他所有管理工作（例如建立安全性原則）。

若要新增管理員角色設定檔，請按一下 **Add**（新增），並指定下表中說明的設定。

建立自訂角色以限制管理員僅能存取每種類型的管理員所需的內容。對於每個類型的管理員，可就 *Web UI*（網頁使用者介面）、*XML API*，以及 *Command Line*（命令列）和 *REST API* 存取啟用、停用或設定唯讀存取。

管理員角色設定	
名稱	輸入用來識別管理員角色的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	（選用）輸入規則的說明（最多 255 個字元）。
角色	選取管理責任的範圍： • 裝置 — 角色套用於整個防火牆，無論是否有多個虛擬系統 (vsys)。 • 虛擬系統—該角色適用於防火牆上的特定虛擬系統具以及虛擬系統的特定方面（如果啟用了多虛擬系統功能）。基於 **Virtual System**（虛擬系統）的 Admin Role Profile（管理員角色設定檔）無法存取 **Web UI**（網頁使用者介面）頁籤以存取網路介面、VLAN、虛擬介接、IPSec 通道、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網路設定檔。您可以在建立管理帳戶時選取虛擬系統（裝置 > 管理員）。
WebUI	按一下特定 Web 介面功能的圖示，以設定允許的存取權限： • 啟用—選定功能的讀取/寫入存取。 • 唯讀 — 選定功能的唯讀存取。 • 停用—不可存取選定功能。
XML API	按一下特定 XML API 功能的圖示，以設定允許的存取權限（**Enable**（啟用）或 **Disable**（停用）。

© 2019 Palo Alto Networks, Inc.

管理員角色設定	

命令列	為 CLI 存取選取角色類型。預設值為 **None**（無），這表示不允許存取 CLI。其他選項視角色範圍而異：
	• 裝置
	  • 超級使用者—擁有防火牆的完整存取權，並且可定義新的管理員帳戶和虛擬系統。您必須擁有超級使用者權限，才可建立具有超級使用者權限的管理員使用者。
	  • 超級讀取者—擁有防火牆的唯讀存取權。
	  • 裝置管理員—擁有所有防火牆設定的完整存取權，但無法定義新的帳戶或虛擬系統。
	  • 裝置讀取者—擁有所有防火牆設定的唯讀存取權，但密碼設定檔（無法存取）和管理員帳戶（僅登入帳戶可見）除外。
	• 虛擬系統
	  • **vsysadmin**—可存取防火牆上的特定虛擬系統以建立和管理虛擬系統的特定方面。**vsysadmin** 設定不控制防火牆層級與網路層級功能（如靜態及動態路由、介面的 IP 位址、IPSec 通道、VLAN、虛擬介接、虛擬路由器、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網絡設定檔）。
	  • **vsysreader**—對防火牆上的特定虛擬系統和虛擬系統的特定方面具有唯讀存取權限。**vsysadmin** 設定沒有防火牆層級或網路層級功能（如靜態及動態路由、介面的 IP 位址、IPSec 通道、VLAN、虛擬介接、虛擬路由器、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 或網絡設定檔）的存取權限。

REST API	按一下特定 REST API 功能的圖示，以設定允許的存取權限（**Enable**（啟用）、**Read Only**（唯讀）或 **Disable**（停用））。

© 2019 Palo Alto Networks, Inc.

Device > Access Domain（裝置 > 存取網域）

- Device > Access Domain（裝置 > 存取網域）

設定存取網域，將管理員存取權限定於防火牆上的特定虛擬系統。只有在您使用 RADIUS、TACACS+ 或 SAML 識別伺服器 (IdP) 對管理員驗證和授權進行管理時，防火牆才支援存取網域。若要啟用存取網域，您必須定義：

- 部驗證伺服器的伺服器設定檔—請參閱 設備 > 伺服器設定檔 > RADIUS、設備 > 伺服器設定檔 > TACACS+ 和 設備 > 伺服器設定檔 > SAML 識別提供者。
- RADIUS 廠商特定屬性 (VSA)、TACACS+ VSA 或 SAML 屬性。

當管理員嘗試登入防火牆時，防火牆會對外部伺服器查詢管理員的存取網域。外部伺服器會傳回相關聯的網域，接著，防火牆會將管理員限定於您在存取網域中指定的虛擬系統。如果防火牆未使用外部伺服器進行管理員的驗證和授權，則會忽略 **Device**（設備）> **Access Domain**（存取網域）設定。

在 *Panorama* 上，您可以在本機管理存取網域，或使用 *RADIUS VSA*、*TACACS+ VSA* 或 *SAML* 屬性來管理（請參閱 *[*Panorama > 存取網域*]*）。

存取網域設定	說明
名稱	輸入存取網域的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、連字號、底線與句號。
虛擬系統	在 [可用] 欄中選取虛擬系統，然後加以 **Add**（新增）。 只有支援虛擬系統的防火牆支援存取網域。

© 2019 Palo Alto Networks, Inc.

Device > Authentication Profile（裝置 > 驗證設定檔）

使用此頁面，可設定用來驗證管理員和使用者的設定。防火牆與 Panorama 支援本機、RADIUS、TACACS+、LDAP、Kerberos、SAML 2.0 和多因素驗證 (MFA) 服務。

建立至少一個驗證設定檔以提供外部驗證，這會將所有的驗證請求保留在一個位置以便於管理，並使用包括追蹤等服務的標準驗證過程。最佳做法是建立以及將數個驗證設定檔使用不同的方式排出優先順序（*Device*（裝置）> *Authentication Sequence*（驗證順序）），避免出現驗證失敗的問題，並建立至少一個本機登入帳戶，以便在所有外部方法都失敗時使用它。

您也可以使用此頁面，向 SAML 識別提供者 (IdP) 註冊防火牆或 Panorama 服務（例如，對 Web 介面的管理存取）。註冊服務後，防火牆或 Panorama 即可使用 IdP 驗證要求服務的使用者。您可以藉由在 IdP 上輸入服務的 SAML 中繼資料來註冊服務。防火牆和 Panorama 可根據您為服務指派的驗證設定檔自動產生 SAML 中繼資料檔案，而使註冊更為容易；您可將此中繼資料檔案匯出至 IdP。

- 驗證設定檔
- 從驗證設定檔匯出的 SAML 元數據

驗證設定檔

- Device > Authentication Profile（裝置 > 驗證設定檔）

選取 **Device**（裝置）> **Authentication Profile**（驗證設定檔）或 **Panorama** > **Authentication Profile**（驗證設定檔），可管理驗證設定檔。若要建立新的設定檔，請 **Add**（新增）設定檔並完成下列欄位。

設定驗證設定檔之後，請使用 `test authentication` *CLI* 命令確認您的防火牆或 *Panorama* 管理伺服器是否可與後端驗證伺服器通訊，以及驗證要求是否成功。您可以在候選設定上執行驗證測試，以在認可之前確認設定是否正確。

驗證設定檔設定	說明
名稱	輸入用來識別設定檔的名稱。名稱區分大小寫，最多可以有 31 個字元，且可以僅包含字母、數字、空格、連字號和底線。相對於其他驗證設定檔以及驗證順序，目前位置（防火牆或虛擬系統）中的名稱必須為唯一。 在多重虛擬系統模式下的防火牆，若驗證設定檔的 *Location*（位置）是虛擬系統，請勿輸入與 *[共用]* 位置中的驗證順序相同的名稱。同樣地，若設定檔位置為 *[共用] Location*（位置），請勿輸入與虛擬系統中的順序相同的名稱。在這些情況中，您可以認可具有相同名稱的驗證設定檔和順序，但這可能會導致參考錯誤。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。

驗證頁籤

防火牆在叫用您於因素頁籤中新增的任何多因素驗證 (MFA) 服務之前，會先叫用您在此頁籤中設定的驗證服務。

© 2019 Palo Alto Networks, Inc.

驗證設定檔設定	說明
如果防火牆透過 *RADIUS* 與 *MFA* 廠商整合（而非廠商 *API*），則您必須設定該廠商的 *RADIUS* 伺服器設定檔，而非 *MFA* 伺服器設定檔。	
類型	選取提供給使用者所看見的第一個（甚或唯一的）驗證挑戰的服務類型。根據您的選取，對話方塊會顯示您為該服務定義的其他設定。選項包括： • **None**（無）—不使用任何驗證。 • **Local Database**（本機資料庫）—使用防火牆上的本機驗證資料庫。此選項不適用於 Panorama。 • **RADIUS**—使用遠端驗證撥入使用者服務 (RADIUS) 伺服器。 • **TACACS+**—使用終端機存取控制器存取控制系統 Plus (TACACS+) 伺服器。 • **LDAP**—使用輕量型目錄存取通訊協定 (LDAP) 伺服器。 • **Kerberos**—使用 Kerberos 伺服器。 • **SAML**—使用安全性聲明標記語言 2.0 (SAML 2.0) 識別提供者 (IdP)。 管理員可使用 *SAML* 向防火牆或 *Panorama Web* 介面進行驗證，但無法向 *CLI* 驗證。
伺服器設定檔 （僅適用於 RADIUS、TACACS+、LDAP 或 Kerberos）	從下拉式清單選取驗證伺服器設定檔。請參閱 [裝置 > 伺服器設定檔 > RADIUS]、[裝置 > 伺服器設定檔 > TACACS+]、[裝置 > 伺服器設定檔 > LDAP] 或 [裝置 > 伺服器設定檔 > Kerberos]。
IdP 伺服器設定檔 （僅適用於 SAML）	從下拉式清單選取 SAML 識別提供者伺服器設定檔。請參閱 [裝置 > 伺服器設定檔 > SAML 識別提供者]。
從 RADIUS 擷取使用者群組 （僅適用於 RADIUS）	選取此選項，可從 RADIUS 伺服器上定義的廠商特定屬性 (VSA) 收集使用者群組資訊。防火牆會使用這些資訊來比對驗證的使用者與允許清單項目，而不會用來強制執行原則或產生報告。
從 TACACS+ 擷取使用者群組 （僅適用於 TACACS+）	選取此選項，可從 TACACS+ 伺服器上定義的廠商特定屬性 (VSA) 收集使用者群組資訊。防火牆會使用這些資訊來比對驗證的使用者與允許清單項目，而不會用來強制執行原則或產生報告。
登入屬性 （僅適用於 LDAP）	輸入將使用者和功能唯一識別為該使用者之登入 ID 的 LDAP 目錄屬性。
密碼到期警告 （僅適用於 LDAP）	如果驗證設定檔是針對 GlobalProtect 使用者的，請輸入密碼到期之前要開始向使用者顯示通知訊息的天數，以警示使用者的密碼會在 x 天後到期。根據預設，會在密碼到期前七天顯示通知訊息（範圍是 1 到 255）。如果使用者的密碼到期，則無法存取 VPN。 請考慮設定 *GlobalProtect* 代理程式，以使用預先登入的連線方法。如此一來，即使使用者的密碼到期，使用者也能連線網域來變更其密碼。

© 2019 Palo Alto Networks, Inc.

驗證設定檔設定	說明
	如果使用者允許其密碼到期，管理員可指派暫時 LDAP 密碼，讓使用者可以登入 VPN。在此工作流程中，我們建議在入口網站設定中將 **Authentication Modifier**（驗證修改程式）設為 **Cookie authentication for config refresh**（設定重新整理的 Cookie 驗證）（否則，臨時密碼將用來驗證入口網站，但閘道登入會失敗，以致於無法進行 VPN 存取）。
用於簽署要求的憑證 （僅適用於 SAML）	選取防火牆用來對其傳送至識別提供者 (IdP) 的 SAML 訊息進行簽署的憑證。如果您在 **IdP Server Profile**（**IdP** 伺服器設定檔）中啟用 **Sign SAML Message to IdP**（簽署傳送至 **IdP** 的 **SAML** 訊息）選項（請參閱 [裝置 > 伺服器設定檔 > SAML 識別提供者]），則此為必要欄位。若非如此，選取用來簽署 SAML 訊息的憑證將是選用動作。 產生或匯入憑證及其相關聯的私密金鑰時，指定於憑證中的金鑰使用屬性會控制您使用金鑰的方式： • 如果憑證明確列出金鑰使用屬性，則其中一個屬性必須是 [數位簽章]，而您在防火牆上產生的憑證中並無此屬性。在此情況下，您必須從您的企業憑證授權單位 (CA) 或第三方 CA 匯出憑證和金鑰。 • 如果憑證未指定金鑰使用屬性，則您可以將金鑰用於任何用途，包括簽署訊息。在此情況下，您可以使用任何方法來取得憑證和金鑰，以簽署 SAML 訊息。 *Palo Alto Networks 建議使用簽署憑證，以確保傳送至 IdP 的 SAML 訊息能保有完整性。*
啟用單一登出 （僅適用於 SAML）	選取此選項，可讓使用者藉由登出任何單一服務來登出各個已驗證的服務。單一登出 (SLO) 僅適用於使用者透過 SAML 驗證存取的服務。服務可以是組織以外的外部服務，或是內部服務（例如防火牆 Web 介面）。只有在 IdP 伺服器設定檔中輸入 **Identity Provider SLO URL**（識別提供者 **SLO URL**）後，此選項才適用。您無法為驗證入口網站使用者啟用 SLO。 登出使用者後，防火牆會自動移除使用者的 IP 位址-使用者名稱對應。
憑證設定檔 （僅適用於 SAML）	選取防火牆將用於驗證的憑證設定檔： • 在 IdP 伺服器設定檔中指定的 **Identity Provider Certificate**（識別提供者憑證）。IdP 會使用此憑證向防火牆進行驗證。當您 **Commit**（認可）驗證設定檔設定時，防火牆即會驗證憑證。 • IdP 傳送至防火牆以進行單一登入 (SSO) 和單一登出 (SLO) 驗證的 SAML 訊息。IdP 會使用在 IdP 伺服器設定檔中指定的 **Identity Provider Certificate**（識別提供者憑證）來簽署訊息。 請參閱 [裝置 > 憑證管理 > 憑證設定檔]。
使用者網域 與 使用者名稱修改程式 （適用於 SAML 以外的所有驗證類型）	防火牆會使用 **User Domain**（使用者網域）來比對驗證的使用者與允許清單項目，也會將其用於 User-ID 群組對應。 您可以指定 **Username Modifier**（使用者名稱修改程式），以修改使用者在登入期間輸入的網域和使用者名稱的格式。防火牆會使用已修改的字串進行驗證。從下列選項中選取：

© 2019 Palo Alto Networks, Inc.

驗證設定檔設定	說明
	• 若僅要傳送未修改的使用者輸入，請將 **User Domain**（使用者網域）保留空白（預設值），並將 **Username Modifier**（使用者名稱修改程式）設定為變數 **%USERINPUT%**（預設值）。 • 若要在使用者輸入前面加上網域，請輸入 **User Domain**（使用者網域），並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERDOMAIN%\%USERINPUT%**。 • 若要在使用者輸入附加網域，請輸入 **User Domain**（使用者網域）並將 **Username Modifier**（使用者名稱修改程式）設定為 **%USERINPUT%@%USERDOMAIN%**。 若 *Username Modifier*（使用者名稱修改程式）包含 *%USERDOMAIN%* 變數，則 *User Domain*（使用者網域）值會取代任何使用者輸入的網域字串。若您指定 *%USERDOMAIN%* 變數並將 *User Domain*（使用者網域）保留空白，則裝置會移除任何使用者輸入的網域字串。防火牆會針對 *User-ID* 群組對應將網域名稱解析為適當的 *NetBIOS* 名稱。此操作會同時套用至父網域和子網域。*User Domain*（使用者網域）修改程式優先適用於自動衍生的 *NetBIOS* 名稱。 • 若要容許防火牆使用伺服器設定檔類型來決定何時以及如何在驗證順序中修改使用者輸入的格式，請手動輸入 `None`（無）作為 **Username Modifier**（使用者名稱修改程式）。如需此選項的更多資訊，請參閱《PAN-OS 管理員指南》中的設定驗證設定檔和順序。
Kerberos 領域 （適用於 SAML 以外的所有驗證類型）	若您的網路支援 Kerberos 單一登入 (SSO)，請輸入 **Kerberos** 領域（最多 127 個字元）。此為使用者登入名稱中的主機名稱部分。例如，使用者帳戶名稱 user@EXAMPLE.LOCAL 具有領域 EXAMPLE.LOCAL。
Kerberos 金鑰頁籤 （適用於 SAML 以外的所有驗證類型）	若您的網路支援 Kerberos 單一登入 (SSO)，請按一下 **Import**（匯入），接著按一下 **Browse**（瀏覽）以尋找金鑰頁籤檔案，然後按一下 **OK**（確定）。金鑰頁籤包含防火牆的 Kerberos 帳戶資訊（主體名稱和雜湊的密碼），此為進行 SSO 驗證所需。每個驗證設定檔可以有一個金鑰頁籤。驗證期間，防火牆首先會嘗試使用金鑰頁籤來建立 SSO。若成功建立，且使用者嘗試的存取位於允許清單中，則驗證會立即成功。否則，驗證程序會回復為指定 **Type**（類型）的手動驗證（使用者名稱/密碼），此方式不一定是 Kerberos。 如果防火牆處於 *FIPS/CC* 模式，演算法必須為 *aes128-cts-hmac-sha1-96* 或 *aes256-cts-hmac-sha1-96*。否則，您也可以使用 *des3-cbc-sha1* 或 *arcfour-hmac*。不過，如果金鑰頁籤中的演算法不符合票證授予服務發行給用戶端的服務票證中用以啟用 *SSO* 的演算法，*SSO* 程序將會失敗。您的 *Kerberos* 管理員會決定服務票證所使用的演算法。
使用者名稱屬性 （僅適用於 SAML）	輸入 SAML 屬性，以識別來自 IdP 之訊息中的驗證使用者的使用者名稱（預設值為 **username**）。如果 **IdP Server Profile**（**IdP** 伺服器設定檔）包含指定使用者名稱屬性的中繼資料，則防火牆會自動在此欄位中填入該屬性。防火牆會比對從 SAML 訊息中擷取的使用者名稱，與驗證設定檔之 **Allow List**（允許清單）中的使用者和使用者群組。由於您無法設定防火牆以修改使用者在 SAML 登入期間輸入的網域/使用者名稱字串，因此登入使用者名稱必須完全符合 **Allow List**（允許清單）項目。這是唯一的必要 SAML 屬性。

© 2019 Palo Alto Networks, Inc.

驗證設定檔設定	說明
	SAML 訊息可能會將使用者名稱顯示在主旨欄位中。如果使用者名稱屬性未顯示使用者名稱，防火牆將會自動檢查主旨欄位。
使用者群組屬性 （僅適用於 SAML）	輸入 SAML 屬性，以識別來自 IdP 之訊息中的驗證使用者的使用者群組（預設值為 **usergroup**）。如果 **IdP Server Profile**（**IdP** 伺服器設定檔）包含指定使用者群組屬性的中繼資料，則此欄位會自動使用該屬性。防火牆會使用群組資訊來比對驗證的使用者與 **Allow List**（允許清單）項目，而不會用於原則或產生報告。
管理員角色屬性 （僅適用於 SAML）	輸入 SAML 屬性，以識別來自 IdP 之訊息中的驗證使用者的管理員角色（預設值為 **admin-role**）。此屬性僅適用於防火牆管理員，而不適用於使用者。如果 **IdP Server Profile**（**IdP** 伺服器設定檔）包含指定管理員角色屬性的中繼資料，則防火牆會自動在此欄位中填入該屬性。防火牆會比對其預先定義的（動態）角色或管理員角色設定檔與擷取自 SAML 訊息的角色，以強制執行角色型存取控制。如果 SAML 訊息中某個僅具有一個角色的管理員有多個管理員角色值，將只會比對出管理員角色屬性中的第一個（最左側的）值。對於有多個角色的管理員，則可比對出屬性中的多個值。
存取網域屬性 （僅適用於 SAML）	輸入 SAML 屬性，以識別來自 IdP 之訊息中的驗證使用者的存取網域（預設值為 **access-domain**）。此屬性僅適用於防火牆管理員，而不適用於使用者。如果 **IdP Server Profile**（**IdP** 伺服器設定檔）包含指定存取網域屬性的中繼資料，則防火牆會自動在此欄位中填入該屬性。防火牆會比對其本機設定的存取網域與擷取自 SAML 訊息的網域，以強制執行存取控制。如果 SAML 訊息中某個僅具有一個存取網域的管理員有多個存取網域值，將只會比對出存取網域屬性中的第一個（最左側的）值。對於有多個存取網域的管理員，則可比對出屬性中的多個值。
因素頁籤	
啟用其他驗證因素	如果您要讓防火牆在使用者成功回應第一個因素後叫用其他驗證因素/挑戰（指定於 **Authentication**（驗證）頁籤上的 **Type**（類型）欄位中），請選取此選項。 僅透過驗證原則支持終端使用者身份驗證的其他身份驗證因素。不支持 *GlobalProtect* 入口網站和閘道的遠程使用者身份驗證或 *PAN-OS* 或 *Panorama Web* 界面管理員身份驗證的其他因素。雖然您可以設定其他因素，但這些用例不會強制實施。不過您可以使用所有驗證用例的 *RADIUS* 或 *SAML* 以整合 *MFA* 廠商。 設定使用多因素驗證 (MFA) 的驗證設定檔之後，您必須將其指派給驗證強制執行物件（Objects>Authentication（物件 > 驗證）），並將該物件指派給對您的網路資源存取進行控制的驗證原則規則（Policies>Authentication（原則 > 驗證））。
因素	針對防火牆在使用者成功回應第一個因素後所將叫用的每個驗證因素（指定於 **Authentication**（驗證）頁籤上的 **Type**（類型）欄位中），新增 MFA 伺服器設定檔（[裝置 > 伺服器設定檔 > 多因素驗證]）。防火牆會依據您列出提供因素之 MFA 服務的順序，由上至下叫用每個因素。若要變更順序，請選取伺服器設定檔並 **Move Up**（上移）或 **Move Down**（下移）。您最多可指定三個其他因素每個 MFA 服務都會提供一個因素。部分 MFA 服務可讓使用者從若干因素中擇一使用。防火牆可透過廠商 API 與這些 MFA 服務整合。其他 MFA 廠商 API 整合會透過應用程式或應用程式和威脅內容更新定期新增。
進階頁籤	

© 2019 Palo Alto Networks, Inc.

驗證設定檔設定	說明
允許清單	按一下 **Add**（新增）並選取 **All**（全部），或選取可使用此設定檔進行驗證的特定使用者和群組。使用者進行驗證時，防火牆會將相關聯的使用者名稱或群組與此清單中的項目比對。若您沒有新增項目，則使用者無法進行驗證。 為了將驗證限制在擁有合法的業務存取需求的使用者並減少攻擊面向，請指定使用者或使用者群組，請勿使用 *all*（全部）。 若您輸入使用者網域值，則不需要在允許清單中指定網域。例如，若 *User Domain*（使用者網域）為 ***businessinc***，且您要將使用者 ***admin1*** 新增至 *Allow List*（允許清單），則輸入 ***admin1*** 與輸入 ***businessinc\admin1*** 會具有相同效用。您可以指定已存在於目錄服務中的群組，或指定 *LDAP* 篩選器上的自訂群組。
失敗的嘗試 （適用於 SAML 以外的所有驗證類型）	輸入防火牆在鎖定使用者帳戶前所允許失敗的成功登入嘗試次數 (0 至 10)。0 值會指定不受限制的登入嘗試次數。防火牆在一般操作模式下的預設值為 0，而在 FIP-CC 模式下的預設值為 10。 將 *Failed Attempts*（失敗的嘗試）的數量設定為 *5* 或以下，以便在輸入錯誤時允許合理的重試次數，同時防止惡意系統嘗試使用暴力攻擊登入防火牆。 若您將 *Failed Attempts*（失敗的嘗試）設定為 *0* 以外的值，但將 *Lockout Time*（鎖定時間）保留為 *0*，則系統會忽略 *Failed Attempts*（失敗的嘗試）且一律不會封鎖使用者。
鎖定時間 （適用於 SAML 以外的所有驗證類型）	輸入防火牆在使用者達到 **Failed Attempts**（失敗的嘗試）次數上限後封鎖使用者帳戶的分鐘數（範圍是 0 到 60，預設值為 0）。0 值表示會套用封鎖，直到管理員手動解除鎖定使用者帳戶為止。 將 *Lockout Time*（鎖定時間）設定為至少 *30* 分鐘，以防止惡意行為者連續嘗試登入。 若您將 *Lockout Time*（鎖定時間）設定為 *0* 以外的值，但將 *Failed Attempts*（失敗的嘗試）保留為 *0*，則系統會忽略 *Lockout Time*（鎖定時間）且一律不會封鎖使用者。

從驗證設定檔匯出的 SAML 元數據

- Device > Authentication Profile（裝置 > 驗證設定檔）

防火牆及 Panorama 可以使用 SAML 識別提供者 (IdP) 來驗證要求服務的使用者。若為管理員，可存取 Web 介面的服務。若為使用者，服務可為驗證入口網站或 GlobalProtect，其可啟用您網路資源的存取權。若要啟用服務的 SAML 驗證，您必須註冊該服務，方法為在 IdP 上以 SAML 中繼資料格式輸入其相關的特定資訊。防火牆和 Panorama 會簡化註冊，方法是根據您指派給服務的驗證設定檔自動產生 SAML 中繼資料檔案，且您可以將此中繼資料檔案匯出至 IdP。在 IdP 中輸入每個中繼資料欄位的值較輕鬆的替代方式是匯出中繼資料。

匯出檔案中的部分中繼資料衍生自指派給驗證設定檔的 *SAML IdP* 伺服器設定檔（設備 > 伺服器設定檔 > SAML 識別提供者）。不過，匯出的檔案一律會指定 *POST* 作為 *HTTP* 繫結方

© 2019 Palo Alto Networks, Inc.

法，無論 *SAML IdP* 伺服器設定檔中指定的方法為何。*IdP* 會使用 *POST* 方法將 *SAML* 訊息傳送至防火牆或 *Panorama*。

若要從驗證設定檔匯出 SAML 中繼資料，請按一下驗證欄位中的 SAML **Metadata**（中繼資料）連結，並完成下列欄位。若要將中繼資料檔案匯出至 IdP，請參考您的 IdP 文件。

SAML 中繼資料匯出設定	說明
命令	選擇要匯出 SAML 中繼資料的服務： • **management**（管理）（預設值）—提供管理員 Web 介面的存取權。 • **authentication-portal**（驗證入口網站）—透過驗證入口網站提供使用者網路資源的存取權。 • **global-protect**—透過 GlobalProtect 提供一般使用者網路資源的存取權。 您的選項將決定對話方塊顯示哪些其他欄位。
[管理 | 驗證入口網站 | GlobalProtect] 驗證設定檔	輸入您要從中匯出中繼資料的驗證設定檔名稱。預設值是您按一下 **Metadata**（中繼資料）連結從中開啟對話方塊的設定檔。
管理選擇 （僅限管理）	選取指定針對管理流量啟用的介面之選項（例如 MGT 介面）： • 介面—從防火牆上的介面清單選取介面。 • **IP** 主機名稱—輸入介面的 IP 位址或主機名稱。如果您輸入主機名稱，DNS 伺服器必須具有對應至 IP 位址的位址 (A) 記錄。
[驗證入口網站 | GlobalProtect] 虛擬系統 （僅限驗證入口網站或 GlobalProtect）	選取定義驗證入口網站設定或 GlobalProtect 入口網站的虛擬系統。
IP 主機名稱 （僅限驗證入口網站或 GlobalProtect）	輸入服務的 IP 位址或主機名稱。 • **Authentication Portal**（驗證入口網站）—輸入 **Redirect Host**（重新導向主機）IP 位址或主機名稱（**Device**（裝置）> **User Identification**（使用者識別）> **Authentication Portal Settings**（驗證入口網站設定））。 • **GlobalProtect**—輸入 GlobalProtect 入口網站的 **Hostname**（主機名稱）或 **IP Address**（**IP** 位址）。 如果您輸入主機名稱，DNS 伺服器必須具有對應至 IP 位址的位址 (A) 記錄。

© 2019 Palo Alto Networks, Inc.

Device > Authentication Sequence（裝置 > 驗證順序）

- Device > Authentication Sequence（裝置 > 驗證順序）
- Panorama > Authentication Sequence（Panorama > 驗證順序）

在部分環境中，使用者帳戶會位於在多個目錄中（例如 LDAP 和 RADIUS）。驗證順序是一組驗證設定檔，可供防火牆在使用者登入時嘗試用來驗證使用者。防火牆會依清單中從上至下的順序嘗試設定檔，並套用驗證、Kerberos 單一登入、允許清單以及帳戶鎖定值，直到一個設定檔成功驗證使用者。僅在順序中的所有設定檔皆驗證失敗時防火牆才會拒絕存取。如需驗證設定檔的詳細資訊，請參閱 [裝置 > 驗證設定檔]。

設定一個擁有數個驗證設定檔且使用數個不同的驗證方法的驗證順序。設定至少兩個外部驗證方法以及一個本機（內部）方法，以便連線問題不會對驗證造成妨礙。將本機驗證設定檔設定為順序中最後一個設定檔，以便僅在所有外部驗證方法都失效時使用它。（外部驗證提供專用、可靠、集中的驗證服務，包括日誌記錄和疑難排解功能。）

驗證順序設定	說明
名稱	輸入用來識別順序的名稱。名稱區分大小寫，最多可以有 31 個字元，且可以僅包含字母、數字、空格、連字號和底線。相對於其他驗證順序以及驗證設定檔，目前**Location**（位置）（防火牆或虛擬系統）中的名稱必須為唯一。 在具有多個虛擬系統（多 *VSYS* 模式）的防火牆中，若驗證順序的 *Location*（位置）是一個虛擬系統 *(VSYS)*，請勿輸入與 *[共用]* 位置中驗證設定檔相同的名稱。同樣地，若順序 *Location*（位置）為 *Shared*（共用），請勿輸入與 *VSYS* 中的設定檔相同的名稱。在這些情況中您可以使用相同名稱來提交驗證順序和設定檔，但可能會發生參考錯誤。
位置	選取順序可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存順序之後，您無法變更其位置。
使用網域決定驗證設定檔	在使用者以 **User Domain**（使用者網域）或 **Kerberos Realm**（Kerberos 領域）（與順序相關聯的驗證設定檔）登入期間，若您要讓防火牆比對使用者所輸入的網域名稱，然後使用該設定檔驗證使用者，請選取此選項（依預設已選取）。防火牆用來比對的使用者輸入可能是使用者名稱前面的文字（包含反斜線分隔符號），或使用者名稱後面的文字（包含 @ 分隔符號）。若防火牆找不到符合項目，則會依從上至下的順序嘗試驗證設定檔。
驗證設定檔	按一下新增並針對您要新增至順序的每個驗證設定檔從下拉式清單中進行選取。若要變更清單順序，請選取設定檔，並按一下上移或下移。若要移除設定檔，請選取它並按一下 **Delete**（刪除）。 您無法新增指定多因素驗證 *(MFA)* 伺服器設定檔或安全性聲明標記語言 *(SAML)* 識別提供者伺服器設定檔的驗證設定檔。

© 2019 Palo Alto Networks, Inc.

Device > Data Redistribution（裝置 > 資料重新散佈）

這些設定定義防火牆或 Panorama 用於重新散佈資料的方法。

您想了解什麼內容？	請參閱：
新增或刪除資料重新散佈代理程式。	Device > Data Redistribution > Agents（裝置 > 資料重新散佈 > 代理程式）
檢視有關資料重新散佈用戶端的資訊。	Device > Data Redistribution > Clients（裝置 > 資料重新散佈 > 用戶端）
設定資料重新散佈代理程式收集器名稱和預先共用金鑰。	Device > Data Redistribution > Collector Settings（裝置 > 資料重新散佈 > 收集器設定）
定義資料重新散佈代理程式在重新散佈資料時包括或排除的子網路。	Device > Data Redistribution > Include/Exclude Networks（裝置 > 資料重新散佈 > 包括/排除網路）

Device > Data Redistribution > Agents（裝置 > 資料重新散佈 > 代理程式）

使用序號或主機和連接埠資訊來新增資料重新散佈代理程式。

資料重新散佈代理程式設定	說明
名稱	輸入資料重新散佈代理程式的名稱（最多 31 個字元）。請僅使用字母、數字、空格、連字號與底線。
已啟用	選取此選項以啟用資料重新散佈代理程式。

新增代理程式，使用	選取您要新增資料重新散佈代理程式的方式：
	• **Serial Number**（序號）—選取此選項，然後選取序號。
	• **Host and Port**（主機和連接埠）—選取此選項，然後輸入以下主機和連接埠資訊：
	  • **Host**（主機）—輸入主機名稱。
	  • **LDAP Proxy**—選取此選項以將主機用作 LDAP Proxy。
	  • **Port**（連接埠）—輸入代理程式偵聽要求的連接埠號。
	  • **Collector Name**（收集器名稱）—輸入 **Collector Name**（收集器名稱）和 **Pre-Shared Key**（預先共用金鑰），該金鑰會將防火牆或虛擬系統識別為 User-ID 代理程式。

資料類型	選取要重新散佈的資料類型（IP 使用者對應、IP 標籤、使用者標籤、HIP 或隔離清單）。

設定資料重新散佈代理程式之後，您可以檢視以下有關重新散佈代理程式的資訊：

© 2019 Palo Alto Networks, Inc.

資料重新散佈代理程式資訊	說明
序號	代理程式的識別碼。
主機	主機的資訊。
收集器名稱	收集器代理程式的名稱。
HIP	代理程式的主機資訊設定檔。
IP 使用者對應	IP 位址至使用者名稱對應的資訊。
IP 標籤	IP 位址至標籤對應的資訊。
隔離清單	顯示隔離中裝置的清單。
動態使用者群組	使用者名稱至標籤對應的資訊。
已連線	指示代理程式是否已連線至重新散佈服務。

Device > Data Redistribution > Clients（裝置 > 資料重新散佈 > 用戶端）

選取 **Device**（裝置）> **Data Redistribution**（資料重新散佈）> **Clients**（用戶端）以顯示每個重新散佈用戶端的以下資訊：

重新散佈代理程式資訊	說明
主機資訊	用戶端的主機資訊。
連接埠	重新散佈用戶端使用的連接埠。
Vsys ID	與重新散佈用戶端連線的虛擬系統識別碼。
版本	用戶端的 PAN-OS 版本。
狀態	顯示重新散佈用戶端的狀態。
PDF/CSV	具有最小唯讀存取權限的管理角色可以匯出 **PDF/CSV** 等格式的資料重新散佈資訊。
重新整理已連線	更新所有已連線的重新散佈用戶端的資訊。

Device > Data Redistribution > Collector Settings（裝置 > 資料重新散佈 > 收集器設定）

若要設定與 User-ID 重新散佈代理程式的連線，請輸入收集器的名稱和預先共用金鑰。

© 2019 Palo Alto Networks, Inc.

資料重新散佈代理程式設定	說明
收集器名稱	輸入 **Collector Name**（收集器名稱）（最多 255 個英數字元）以識別重新散佈代理程式。
收集器預先共用金鑰/確認收集器預先共用金鑰	輸入並確認收集器的 **Pre-Shared Key**（預先共用金鑰）（最多 255 個英數字元）。

Device > Data Redistribution > Include/Exclude Networks（裝置 > 資料重新散佈 > 包括/排除網路）

使用包含/排除網路清單可定義重新散佈代理程式在重新散佈對應時包含或排除的子網路。

工作	說明
新增	若要將發現限制為特定子網路，請 **Add**（新增）子網路設定檔，然後完成下列欄位： • 名稱—輸入用來識別子網路的名稱。 • 已啟用—選取此選項可對伺服器監控啟用包含或排除子網路。 • 探索 — 選取 User-ID 代理程式是否將 **Include**（包含）或 **Exclude**（排除）子網路。 • 網路位址 — 輸入子網路的 IP 位址範圍。 代理程式會套用隱含全部排除規則至清單。例如，如果您使用 **Include**（包含）選項新增子網路 10.0.0.0/8，代理程式將排除所有其他子網路，即使您並未將它們新增至清單亦是如此。請只在您希望代理程式排除明確包括的子網路子集時，才使用 **Exclude**（排除）選項新增項目。例如，如果您使用 **Include**（包含）選項新增 10.0.0.0/8 以及 **Exclude**（排除）選項新增 10.2.50.0/22，User-ID 代理程式將針對除了 10.2.50.0/22 以外的所有 10.0.0.0/8 子網路執行探索，並將排除 10.0.0.0/8 以外的所有子網路。如果您新增 **Exclude**（排除）設定檔而不新增任何 **Include**（包括）設定檔，代理程式將排除所有子網路，而不只是您新增的子網路。
刪除	若要從清單中移除子網路，請選取子網路並將其 **Delete**（刪除）。 提示：若要從包含/排除網路清單中移除子網路而不刪除其組態，請編輯子網路設定檔，然後清除 **Enabled**（已啟用）。
自訂包含/排除網路	依預設，代理程式會從頂端第一個到底端最後一個，以您新增的順序評估子網路。若要變更評估順序，請按一下**Custom Include/Exclude Network Sequence**（自訂包含/排除網路順序）。然後您可以 **Add**（新增）、**Delete**（刪除）、**Move Up**（上移）或 **Move Down**（下移）子網路以建立自訂評估順序。

© 2019 Palo Alto Networks, Inc.

Device > Device Quarantine（裝置 > 裝置隔離）

Device（裝置）> **Device Quarantine**（裝置隔離）頁面顯示隔離清單中的裝置。執行以下動作，裝置即會出現在此清單中：

- 系統管理員已將裝置手動新增至此清單。

  若要手動 **Add**（新增）裝置，請輸入您需要隔離裝置的 **Host ID**（主機 **ID**），也可選擇輸入 **Serial Number**（序號）。
- 系統管理員從 Traffic（流量）、GlobalProtect 或 Threat（威脅）日誌中選取 Host ID（主機 ID）欄，從該欄中選取一個裝置，然後選取 **Block Device**（封鎖裝置）。
- 該裝置與具有日誌轉送設定檔的安全性政策規則相符，其相符清單具有設定為 **Quarantine**（隔離）的內建動作。

  主機 *ID* 會自動顯示在 *GlobalProtect* 日誌中。為了使主機 *ID* 顯示在流量、威脅或統一日誌中，防火牆必須至少具有一個安全性政策規則，且其 *Source Device*（來源裝置）設定為 *Quarantine*（隔離）。如果在安全性政策中沒有此設定，則流量、威脅或統一日誌將沒有主機 *ID*，並且日誌轉送設定檔也不會生效。
- 使用 API 將裝置新增至隔離清單中。
- 防火牆收到的隔離清單是重新散佈項目的一部分（隔離清單從另一個 Panorama 裝置或防火牆重新散佈）。

裝置隔離表包含以下欄位。

欄位	說明
主機 ID	封鎖主機的主機 ID。
原因	裝置被隔離的原因。原因 **Admin Add**（管理員新增）意味著管理員將裝置手動新增至表中。
時間戳記	管理員或安全性政策規則將裝置新增至隔離清單的時間。
來源裝置/應用程式	將裝置新增至隔離清單的 Panorama、防火牆或第三方應用程式的 IP 位址。
序號	（選用）被隔離裝置的序號（如有）。
使用者名稱	（選用）隔離裝置時登入該裝置的 GlobalProtect 用戶端使用者的使用者名稱。

© 2019 Palo Alto Networks, Inc.

裝置 > VM 資訊來源

使用此頁籤可積極追蹤其中任何資源上部署的虛擬機器 (VM) 變更—VMware ESXi 伺服器、VMware vCenter 伺服器、Amazon Web Services 虛擬私人雲端（AWS-VPC）或 Google 計算引擎（GCE）。

當監控 *ESXi* 主機為 *VM* 系列 *NSX* 版本解決方案的一部分時，使用動態位址群組而非 *VM* 資訊來源來記住虛擬環境中的變更。對於 *VM* 系列 *NSX* 版本解決方案，*NSX Manager* 將為 *Panorama* 提供 *IP* 位址所屬 *NSX* 安全性群組的相關資訊。*NSX Manager* 提供的資訊為在動態位址群組中定義比對準則提供了完整內容，因為它將服務設定檔 *ID* 用作辨別屬性，並在不同的 *NSX* 安全性群組間擁有重疊 *IP* 位址時，允許您適當強制執行原則。

您可以為一個 *IP* 位址註冊最多 *32* 個頁籤。

有兩種方法可監控 VM 資訊來源：

- 防火牆可監控您的 VMware ESXi 伺服器、VMware vCenter 伺服器、GCE 執行個體或 AWS-VPC，並在您佈建或修改受監控來源上設定的來賓時擷取變更。對於每個防火牆，或對於具備多個虛擬系統之防火牆上設定的每個虛擬系統，您最多可以設定 10 個來源。

  下列情況適用於您的防火牆設定在高可用性（HA）組態時：

  - **Active/passive HA configuration**（主動/被動 HA 組態）—只有主動防火牆會監控 VM 資訊來源。
  - **Active/passive HA configuration**（主動 / 被動 **HA** 設定）—只有帶有 `primary`（主要）優先次序的防火牆可監控 VM 資料來源。

  如需 VM 資訊來源和動態位址群組如何同步運作，及如何讓您監控虛擬環境中變更等詳細資訊，請參閱《VM 系列部署指南》。
- 若為 IP 位址至使用者對應，您可以在 Windows User-ID 代理程式或防火牆上設定 VM 資訊來源以監控 VMware ESXi 和 vCenter 伺服器，並在您佈建或修改伺服器上設定的來賓時擷取變更。Windows User-ID 代理程式支援最多 100 個來源。User-ID 代理程式對於 AWS 和 Google 計算引擎的支援不可用。

受監控的 *ESXi* 或 *vCenter* 伺服器上的每個 *VM* 必須已安裝並正在執行 *VMware* 工具。*VMware* 工具提供 指定給每一 *VM IP* 位址和其他值的能力。

為了收集指派給受監控 VM 的值，防火牆會監控下表中的屬性。

VMware 來源上監控的屬性
• UUID • 名稱 • 來賓 OS • 註釋 • VM 狀態—電力狀態可為 `poweredOff`、`poweredOn`、`standBy` 或 `unknown`（未知）。 • 版本 • 網路—虛擬交換器名稱、連接埠群組名稱和 VLAN ID • 容器名稱—vCenter 名稱、資料中心物件名稱、資源集區名稱、叢集名稱、主機、主機 IP 位址。

AWS-VPC 上監控的屬性
• 架構 • 來賓 OS • 映像 ID

© 2019 Palo Alto Networks, Inc.

AWS-VPC 上監控的屬性
• 執行個體 ID • 執行個體狀態 • 執行個體類型 • 金鑰名稱 • 位置—租用、群組名稱、可用性區域 • 私人 DNS 名稱 • 公開 DNS 名稱 • 子網路 ID • 頁籤（金鑰、值）；每個執行個體最多支援 18 個頁籤 • VPC ID

Google 計算引擎（GCE）屬性監控
• VM 的主機名稱 • 機器類型 • 專案 ID • 來源（作業系統類型） • STATUS （狀態） • 子網路 • VPC 網路 • 區

新增—新增 VM 監控的來源，並根據正在監控的來源填寫詳細資訊：

- 針對 VMware ESXi 或 vCenter Server，請參閱啟用 VMware ESXi 和 vCenter 伺服器的 VM 資訊來源的設定。
- 針對 AWS-VPC，請參閱啟用 AWS VPC 的 VM 資訊來源的設定。
- 對於 Google 計算引擎（GCE），請參閱 Settings to Enable VM Information Sources for Google Compute Engine（啟用 Google 計算引擎用 VM 資料來源的設定）。

Refresh Connected（重新整理連線）—重新整理螢幕顯示中的連線狀態；這不會重新整理防火牆和受監控來源之間的連線。

Delete（刪除）—刪除任何您選取的已設定 VM 資料。

PDF/CSV—將 VM 資料來源組態表導出為 PDF 或逗號分隔值（CSV）檔案。請參閱 Configuration Table Export（組態表匯出）。

為 VMware ESXi 和 vCenter 伺服器啟用 VM 資訊來源的設定

下表說明為針對 Vmware ESXi 和 vCenter 伺服器啟用 VM 資訊來源，您可進行的設定。

若要擷取虛擬機器的標籤，防火牆需要在 *VMware ESXi* 和 *vCenter* 伺服器上具有唯讀存取權限的帳戶。

© 2019 Palo Alto Networks, Inc.

為 VMware ESXi 和 vCenter 伺服器啟用 VM 資訊來源的設定	
名稱	輸入用來識別受監視來源的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
類型	選取正在監控的主機/來源為 **ESXi server**（**ESXi** 伺服器）或 **vCenter server**（**vCenter** 伺服器）。
說明	（選用）新增標籤來識別來源的位置或功能。
連接埠	指定主機/來源正在接聽的連接埠。（預設連接埠為 443。）
已啟用	預設會啟用防火牆與設定的來源之間的通訊。 介面上會顯示受監控來源與防火牆之間的連線狀態，如下所示： • 已連線 • 已中斷連線 • 擱置中；停用受監控來源時，連線狀態也會顯示成黃色。 清除 **Enabled**（已啟用）選項可停用主機與防火牆之間的通訊。
逾時	以小時為單位輸入間隔，如果主機在經過此間隔後未回應，則關閉受監視來源的連線（範圍是 2-10；預設為 2）。 （選用）若要變更預設值，選取 **Enable timeout when the source is disconnected**（當來源中斷連線時啟用逾時）並指定值。達到指定的限制時，若無法存取主機或主機未回應，防火牆將關閉至來源的連線。
來源	輸入正在監控之主機/來源的 FQDN 或 IP 位址。
使用者名稱	指定驗證來源所需的使用者名稱。
密碼	輸入密碼並確認輸入。
更新間隔	指定防火牆從來源擷取資訊間隔秒數（範圍是 5-600，預設為 5）。

為 AWS VPC 啟用 VM 資訊來源的設定

下表說明為針對 AWS VPC 啟用 VM 資訊來源，您可進行的設定。

為 AWS VPC 啟用 VM 資訊來源的設定	
名稱	輸入用來識別受監視來源的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
類型	選取 **AWS VPC**。
說明	（選用）新增標籤來識別來源的位置或功能。
已啟用	預設會啟用防火牆與設定的來源之間的通訊。 介面上會顯示受監控來源與防火牆之間的連線狀態，如下所示：

© 2019 Palo Alto Networks, Inc.

為 AWS VPC 啟用 VM 資訊來源的設定	
	• 已連線 • 已中斷連線 • 擱置中；停用受監控來源時，連線狀態也會顯示成黃色。 清除 **Enabled**（已啟用）選項可停用主機與防火牆之間的通訊。
來源	新增虛擬私人雲端所在的 URI。例如，ec2.us-west-1.amazonaws.com 語法是：ec2.<*your_AWS_region*>.amazonaws.com；對於 AWS China，語法是：ec2.<AWS_region>.amazonaws.com.cn
存取金鑰 ID	輸入英數字文字字串以唯一識別擁有或授權存取 AWS 帳戶的使用者。 此資訊是 AWS 安全性認證的一部分。防火牆需要認證（存取金鑰 ID 和密碼存取金鑰）來數位簽署對 AWS 服務所進行的 API 呼叫。
密碼存取金鑰	輸入密碼並確認輸入。
更新間隔	指定防火牆從來源擷取資訊間隔秒數（範圍是 60 至 1,200，預設為 60）。
逾時	以小時為單位的間隔，如果主機在經過此間隔後未回應，則關閉受監視來源的連線（預設為 2）。 （選用）**Enable timeout when the source is disconnected**（當來源中斷連線時啟用逾時）。達到指定的限制、無法存取來源或來源未回應時，防火牆將關閉至來源的連線。
VPC ID	輸入要監控的 AWS-VPC 的 ID，例如，vpc-1a2b3c4d。只會監控此 VPC 中部署的 EC2 實例。 如果設定帳戶來使用預設 VPC，將在 [AWS 帳戶屬性] 下列出預設 VPC ID。

為 Google 計算引擎啟用 VM 資訊來源的設定

Device（設備）**VM** > **Information Sources**（**VM** 資料來源）> **Add**（新增）

以下表格說明您需要啟用 Google 雲端平台上 Google 計算引擎實例的 VM 資料來源時所需的設定。啟用對 Google 計算引擎（GCE）實例的監控，以允許防火牆（實體或虛擬內部部署或在 Google Cloud 中運行）檢索頁籤、標籤和有關在特定項目的 Google Cloud 區域中運行實例的其他元數據。有關 Google 雲端平台上的 VM 系列資料，請參閱 VM-Series Deployment Guide（VM 系列部署指南）。

為 Google 計算引擎啟用 VM 資訊來源的設定	
名稱	輸入用來識別受監視來源的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
類型	選擇 **Google Compute Engine**（**Goggle** 計算引擎）。
說明	（選用）新增標籤來識別來源的位置或功能。
已啟用	防火牆與設定的來源之間的通訊為預設啟用。 介面上會顯示受監控來源與防火牆之間的連線狀態，如下所示：

© 2019 Palo Alto Networks, Inc.

為 Google 計算引擎啟用 VM 資訊來源的設定	
	• 🟢—已連線 • 🔴—中斷連線 • 🟡—擱置中，或監控的來源已停用。 清除 **Enabled**（已啟用）選項可停用設定來源與防火牆之間的通訊。 當您停用通訊時，所有註冊的 IP 位址和頁籤會從相關動態位址分組移除。這表示該政策將不會套用在來自此 Google 雲端專案的 GCE 實例。
服務驗證類型	選擇在 GCE 或服務帳號上執行的 VM 系列。 • **VM-Series running on GCE**（在 **GCE** 中執行的 **VM** 系列）—如果您正啟用 VM 監測的以硬體為主或 VM 系列防火牆並未部署在 Google 雲端平台內，則選擇此選項。 • **Service Account**（服務帳戶）—如果您正監測的 Google 雲端引擎實例位於並未部署在 Google 雲端平台的防火牆上，則選擇此選項。本選項讓您可以使用屬於虛擬機台或應用程式的特殊 Google 帳戶，而非使用個別終端用戶帳戶。 此服務帳戶必須有 IAM 政策（**Compute Engine**（計算引擎）> **Compute Viewer**（計算檢視器）權限），該權限授權訪問 Google API 並允許其查詢 Google 雲端專案中的虛擬機台以獲取虛擬機台的元數據。
服務帳戶驗證	（僅限服務帳戶）使用此認證為服務帳戶上載 JSON 檔案。該文件允許防火牆對實例進行身份驗證並授權訪問元數據。 您可以在 Google Cloud 主控台創建帳戶（**IAM & admin** > **Service Accounts**（服務帳戶））。有關如何創建帳戶、添加密鑰以及下載需要上載到防火牆的 JSON 文件的資料，請參閱 Google 文檔。
專案 ID	輸入您想要監測的 Google 雲端專案的唯一定義字母數字文字字串。
區域名稱	如字串輸入區域名稱，長度最長為 63 字元。例如：`us-west1-a`。
更新間隔	指定防火牆從來源擷取資訊間隔（以秒計）（範圍是 60 至 1,200，預設為 60）。
逾時	以小時為單位的間隔，如果主機在經過此間隔後未回應，則關閉受監視來源的連線（預設為 2）。 （選用）**Enable timeout when the source is disconnected**（當來源中斷連線時啟用逾時）。達到指定的限制、無法存取來源或來源未回應時，防火牆將關閉至來源的連線。當來源中斷連線時，所有從本專案註冊的 IP 位址和頁籤會從動態位址群組中移除。

© 2019 Palo Alto Networks, Inc.

裝置 > 疑難排解

- **Device**（裝置）> **Troubleshooting**（疑難排解）（裝置 > 疑難排解）
- **Panorama** > **Managed Devices**（受管理的裝置）> **Troubleshooting**（疑難排解）

在提交裝置群組或範本組態變更之前，請測試 Web 介面中的功能，以驗證變更並未引入在執行中組態內引入的連線問題，以及原則正確允許或拒絕流量。

- 原則比對測試
  - 安全性政策比對
  - QoS 政策比對
  - 驗證政策比對
  - 解密/SSL 政策比對
  - NAT 政策比對
  - 基於原則的轉送政策比對
  - DoS 政策比對
- 連線測試
  - 路由
  - 測試 Wildfire
  - Threat Vault
  - Ping
  - 追蹤路由
  - 日誌收集器連線
  - 外部動態清單
  - 更新伺服器
  - 測試雲端記錄服務狀態
  - 測試雲端 GP 服務狀態

安全性政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
至	選取流量的目的地區域。
來源	輸入流量來源的 IP 位址。

© 2019 Palo Alto Networks, Inc.

欄位	說明
目的地	輸入流量的目的地 IP 位址。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
來源使用者	輸入流量來源的使用者。
通訊協定	輸入用於路由的 IP 通訊協定。可以為 0 至 255。
在首次允許規則之前顯示所有可能的相符規則	啟用此選項可顯示所有可能的規則相符項，直到第一個相符的規則結果。停用（清除）以僅返回測試結果中的第一個相符規則。
應用程式	選取您要測試的應用程式流量。
類別	選取您要測試的流量類別。
（僅防火牆）檢查 HIP 遮罩	選取以檢查正在存取網路的終端裝置的安全性狀態。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。
	  • `Shared policy disabled on device`（共用裝置上啟用的原則）—裝置上的 Panorama 設定不允許從 Panorama 推送原則。

QoS 政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
至	選取流量的目的地區域。

© 2019 Palo Alto Networks, Inc.

欄位	說明
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
來源使用者	選取流量來源的使用者。
通訊協定	輸入用於路由的 IP 通訊協定。可以為 0 至 255。
應用程式	選取您要測試的應用程式流量。
類別	選取您要測試的流量類別。
字碼指標類型	選取您要測試的字碼指標編碼類型。
字碼指標值	指定字碼指標編碼值： • **DSCP**—0 至 63 • **ToS**—0 至 7

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。
	  • `Shared policy disabled on device`（共用裝置上啟用的原則）—裝置上的 Panorama 設定不允許從 Panorama 推送原則。

驗證政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。

© 2019 Palo Alto Networks, Inc.

欄位	說明
從	輸入流量來源的區域。
至	選取流量的目的地區域。
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
類別	選取您要測試的流量類別。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。
	  • `Shared policy disabled on device`（共用裝置上啟用的原則）—裝置上的 Panorama 設定不允許從 Panorama 推送原則。

解密/SSL 政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
至	選取流量的目的地區域。
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
應用程式	選取您要測試的應用程式流量。

© 2019 Palo Alto Networks, Inc.

欄位	說明
類別	選取您要測試的流量類別。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

NAT 政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
至	選取流量的目的地區域。
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
來源連接埠	輸入流量來源的特定連接埠。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
通訊協定	輸入用於路由的 IP 通訊協定。可以為 0 至 255。
至介面	在要為其傳輸流量的裝置上輸入目的地介面。
HA 裝置 ID	輸入 HA 裝置的 ID： • **0**—主要 HA 對等 • **1**—次要 HA 對等

© 2019 Palo Alto Networks, Inc.

欄位	說明

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。
	  • Shared policy disabled on device（共用裝置上啟用的原則）—裝置上的 Panorama 設定不允許從 Panorama 推送原則。

基於原則的轉送政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
來源介面	在要從其傳輸流量的裝置上輸入介面。
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
來源使用者	輸入流量來源的使用者。
通訊協定	輸入用於路由的 IP 通訊協定。可以為 0 至 255。
應用程式	選取您要測試的應用程式流量。
HA 裝置 ID	HA 裝置的 ID： • **0**—主要 HA 對等 • **1**—次要 HA 對等

© 2019 Palo Alto Networks, Inc.

欄位	說明

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。
	  • Shared policy disabled on device（共用裝置上啟用的原則）—裝置上的 Panorama 設定不允許從 Panorama 推送原則。

DoS 政策比對

欄位	說明
測試組態	
選取測試	選取要執行的原則比對測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
從	輸入流量來源的區域。
至	選取流量的目的地區域。
來源介面	在要從其傳輸流量的裝置上輸入介面。
至介面	在要為其傳輸流量的裝置上輸入目的地介面。
來源	輸入流量來源的 IP 位址。
目的地	輸入流量的目的地 IP 位址。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
來源使用者	輸入流量來源的使用者。
通訊協定	輸入用於路由的 IP 通訊協定。可以為 0 至 255。
結果	選取以檢視已執行測試的結果詳細資料。

© 2019 Palo Alto Networks, Inc.

欄位	說明

	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

路由

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
FiB 查閱，Mfib 查閱	為查閱選取下列其中一項： • **FiB**—在啟動路由表內執行路由查閱 • **Mfib**—在使用中路由表內執行多點傳送路由查閱
目的地 Ip	輸入要為其傳輸流量的 IP 位址。
虛擬路由器	在其內執行路由測試的特定虛擬路由器。從下拉式清單中選取虛擬路由器。
ECMP	
來源 IP	輸入流量來源的特定 IP 位址。
來源連接埠	輸入流量來源的特定連接埠。
目的地 Ip	輸入要為其傳輸流量的特定 IP 位址。
目的地連接埠	輸入要為其傳輸流量的特定目的地連接埠。
結果	選取以檢視已執行測試的結果詳細資料。 （僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊： • 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。 • 防火牆—處理流量的防火牆的名稱 • 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。

© 2019 Palo Alto Networks, Inc.

欄位	說明

	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

測試 Wildfire

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
通道	選取 Wildfire 通道：**Public**（共用）或 **Private**（私用）。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

Threat Vault

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
結果	選取以檢視已執行測試的結果詳細資料。 （僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊： • 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。

© 2019 Palo Alto Networks, Inc.

欄位	說明

	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

Ping

ping 疑難排解測試僅在執行 PAN-OS 9.0 或更高版本的防火牆上受支援。

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
繞過路由表，使用指定的介面	啟用此選項可繞過路由表並使用指定的介面。停用（清除）此選項以測試已設定的路由表。
計數	輸入要傳送的要求數。預設計數是 5。
請勿對回應要求封包進行分段 (IPv4)	啟用此選項不會對測試的回應要求封包進行分段。停用
強制到 IPv6 目的地	啟用以強制測試到 IPv6 目的地。
間隔	指定兩個要求之間的延遲（以秒為單位）（範圍為 1 至 2,000,000,000）。
來源	輸入回應要求的來源位址。
請勿嘗試象徵性地列印位址	啟用此選項可在測試結果中顯示 IP 位址，而不解析 IP 位址主機名稱。停用（清除）以解析 IP 位址主機名稱。
模式	指定十六進位填寫模式。
大小	輸入要求封包的大小（以位元組為單位）（範圍為 0 到 65468）。
TOS	輸入 IP 服務類型值（範圍為 1 到 255）。
TTL	輸入 IP SA 生命週期值（以躍點數表示）—IPv6 躍點限制值（範圍為 1 到 255）。
顯示詳細的輸出	啟用以顯示測試結果的詳細輸出。

© 2019 Palo Alto Networks, Inc.

欄位	說明
主機型	輸入遠端主機的主機名稱或 IP 位址。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。

追蹤路由

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
使用 IPv4	啟用以使用選定裝置的 IPv4 位址。
使用 IPv6	啟用以使用選定裝置的 IPv6 位址。
第一個 TTL	輸入第一個傳出探查封包中使用的存留時間（範圍為 1 到 255）。
最大 TTL	輸入最大存留時間躍點數（範圍為 1 到 255）。
連接埠	輸入探查中使用的基本連接埠號。
TOS	輸入 IP 服務類型值（範圍為 1 到 255）。
等待	輸入等待回應的秒數（範圍為 1 至 99,999）。
暫停	輸入兩次探查之間暫停的時間（以毫秒為單位）（範圍為 1 到 2,000,000,000）。
設定「不分段」位元	如果路徑不支援設定的最大傳輸單元 (MTU)，則啟用此選項，以避免將 ICMP 封包分段為多個封包。
啟用通訊端層級偵錯	啟用此選項允許您在通訊端層級進行偵錯。
閘道	最多指定 8 個鬆散來源路由閘道。

© 2019 Palo Alto Networks, Inc.

欄位	說明
請勿嘗試象徵性地列印位址	啟用此選項可在測試結果中顯示 IP 位址，而不解析 IP 位址主機名稱。停用（清除）以解析 IP 位址主機名稱。
繞過路由表，直接傳送至主機	啟用此選項可繞過任何已設定的路由表，然後直接藉助主機進行測試。
來源	輸入傳出探查封包內的來源位址。
主機型	輸入遠端主機的主機名稱或 IP 位址。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

日誌收集器連線

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出已選取用於測試的裝置和虛擬系統。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：Success（成功）或 Failure（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • N/A（不使用）—測試不適用於該裝置。
	  • Device not connected（裝置未連線）—裝置連線已丟棄。

© 2019 Palo Alto Networks, Inc.

外部動態清單

欄位	說明
選取測試	選取要執行的連線測試。
（僅 Panorama）選取裝置	**Select device/VSYS**（選取裝置/VSYS）以指定要為其測試原則功能的裝置和虛擬系統。根據管理員和裝置群組以及範本使用者的存取網域向其提供裝置和虛擬系統。此外，您可以選取 Panorama 管理伺服器作為裝置。
（僅 Panorama）選定的裝置	列出選取用於測試的裝置和虛擬系統。
URL 測試	指定用於測試連線的 URL。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。

更新伺服器

欄位	說明
選取測試	選取要執行的連線測試。

結果	選取以檢視已執行測試的結果詳細資料。
	（僅 Panorama）在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊：
	• 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。
	• 防火牆—處理流量的防火牆的名稱
	• 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。
	• 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：
	  • `N/A`（不使用）—測試不適用於該裝置。
	  • `Device not connected`（裝置未連線）—裝置連線已丟棄。

測試雲端記錄服務狀態

測試雲端記錄日誌服務的連線狀態。此測試僅適用於執行安裝了雲端服務外掛程式 1.3 版或更高版本的 Panorama 管理伺服器。

© 2019 Palo Alto Networks, Inc.

欄位	說明
選取測試	選取要執行的連線測試。
結果	選取以檢視已執行測試的結果詳細資料。 在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊： • 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。 • 防火牆—處理流量的防火牆的名稱 • 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。 • 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：

測試雲端 GP 服務狀態

測試 GlobalProtect 即服務的連線狀態。此測試僅適用於執行安裝了雲端服務外掛程式 1.3 版或更高版本的 Panorama 管理伺服器。

欄位	說明
選取測試	選取要執行的連線測試。
結果	選取以檢視已執行測試的結果詳細資料。 在為多個受管理裝置執行測試時，結果將顯示每個測試裝置的以下資訊： • 裝置群組—處理流量之防火牆所屬的裝置群組的名稱。 • 防火牆—處理流量的防火牆的名稱 • 狀態—指示測試的狀態：`Success`（成功）或 `Failure`（失敗）。 • 結果—顯示測試結果。若無法執行測試，則會顯示以下其中一項：

© 2019 Palo Alto Networks, Inc.

Device > Virtual Systems（裝置 > 虛擬系統）

虛擬系統 (vsys) 是獨立（虛擬）的防火牆執行個體，您可以在實體防火牆內進行個別管理。每個 VSYS 可以是具有本身安全性原則、執行個體和管理員的獨立防火牆，VSYS 可讓您針對防火牆所提供的所有原則、報告和可見度功能劃分管理。

例如，如果您要為與財務部門關聯的流量自訂安全性功能，您可以定義財務 VSYS，然後再定義專屬於該部門的安全性原則。若要最佳化原則管理，您可以為整體防火牆和網路功能維護個別的管理員帳戶，同時建立 vsys 管理員帳戶以允許存取個別的 vsys。這允許財務部門的 vsys 管理員只管理該部門的安全性原則。

網絡功能（如靜態及動態路由、介面的 IP 位址和 IPSec 通道）與整個防火牆及其所有虛擬系統相關。虛擬系統設定（**Device**（裝置）> **Virtual Systems**（虛擬系統））不控制防火牆層級與網路層級功能（如靜態及動態路由、介面的 IP 位址、IPSec 通道、VLAN、虛擬介接、虛擬路由器、GRE 通道、DHCP、DNS Proxy、QoS、LLDP 和網絡設定檔）。對於每個 VSYS，可以指定實體與邏輯防火牆介面（包括 VLAN 與 Virtual Wire）及安全性區域的集合。如果需要每個 vsys 的路由區段，則必須建立並指派其他虛擬路由器，然後視需要指派介面、VLAN、Virtual Wire。

若您使用 Panorama 範本來定義虛擬系統，您可以將一個 vsys 設定為預設值。預設 VSYS 和多個虛擬系統容量會決定在範本認可期間防火牆是否接受 VSYS 特定設定：

- 啟用了多個虛擬系統功能的防火牆針對範本中定義的任何 VSYS 會接受 VSYS 特定組態。
- 未啟用多個虛擬系統功能的防火牆僅針對預設的 VSYS 接受 VSYS 特定組態。若您未設定預設 vsys，則這些防火牆將不會接受 vsys 特定組態。

PA-3200 系列、*PA-5200* 系列以及 *PA-7000* 系列防火牆支援多個虛擬系統。然而，*PA-3200* 系列防火牆需要授權才能啟用多個虛擬系統。*PA-220* 與 *PA-800* 系列防火牆不支援多個虛擬系統。

啟用多個虛擬系統之前，請考慮下列事項：

- VSYS 管理員會逐個已指派的虛擬系統建立和管理安全性政策所需的所有項目。
- 區域是 vsys 內的物件。在定義原則或原則物件之前，請先從 **Policies**（原則）或 **Objects**（物件）頁籤上的下拉式清單中選取相應的 **Virtual System**（虛擬系統）。
- 您可以針對遠端日誌記錄目的地（SNMP、Syslog 和電子郵件）、應用程式、服務以及設定檔，設定為可供所有虛擬系統（共用）或單一 vsys 使用。
- 若您有多個虛擬系統，則可以選取 vsys 作為 User-ID 中心，以在虛擬系統之間共用 IP 位址到使用者名稱的對應資訊。
- 您可以全域設定（針對防火牆上的所有虛擬系統）或 vsys 特定服務路由（裝置 > 設定 > 服務）。
- 您僅能在本機防火牆上重新命名 VSYS。Panorama 不支援 VSYS 重新命名功能。如果在 Panorama 上重新命名 vsys，會有全新的 vsys，或者新的 vsys 名稱可能對應至防火牆上錯誤的 vsys。

在定義 vsys 之前，必須先在防火牆上啟用多個 vsys 功能。選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理），編輯 **General Settings**（一般設置），選取 **Multi Virtual System Capability**（多個虛擬系統功能），然後按一下 **OK**（確定）。此操作會新增一個 **Device**（裝置）> **Virtual Systems**（虛擬系統）頁面。選取頁面，**Add**（新增）vsys，然後指定下列資訊。

虛擬系統設定	說明
ID	為 VSYS 輸入整數識別碼。如需所支援虛擬系統數的相關資訊，請參閱防火牆型號的資料表。 若您使用 *Panorama* 範本設定 *VSYS*，此欄位將不會顯示。

© 2019 Palo Alto Networks, Inc.

虛擬系統設定	說明
名稱	輸入用來識別 VSYS 的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 若您使用 *Panorama* 範本推送 *VSYS* 組態，則範本中的 *VSYS* 名稱必須符合防火牆上的 *VSYS* 名稱。
允許轉送解密的內容	選取此選項可允許虛擬系統在連接埠鏡像或傳送 WildFire 檔案以供分析時，將解密的內容轉送至服務外部。另請參閱解密連接埠鏡像。
一般頁籤	如果您要將 DNS Proxy 規則套用至此 VSYS，請選取 **DNS Proxy** 物件。（網路 > DNS 代理程式）。 若要包含特殊類型的物件，請選取該類型（介面、VLAN、Virtual Wire、虛擬路由器或可見虛擬系統），然後 **Add**（新增）物件，並從下拉式清單中選取物件。您可以新增一或多個任何類型的物件。若要移除物件，請選取物件並予以 **Delete**（刪除）。
資源頁籤	指定此 VSYS 所允許的以下資源限制：每個欄位將顯示有效值範圍，該範圍視防火牆型號而異。預設設定為 0，這表示 VSYS 的限制即為防火牆型號的限制。但是，特定設定的限制不會複寫到每個 VSYS。例如，如果防火牆有四個虛擬系統，每個虛擬系統的解密規則數不得為每個防火牆允許的解密規則總數。所有虛擬系統的解密規則總數達到防火牆限制時，將無法新增更多。 • 工作階段限制—工作階段的數目上限。 如果您使用 *CLI* 命令 `show session meter`，防火牆將顯示每個資料層允許的工作階段數量上限、虛擬系統目前使用的工作階段數量以及每個虛擬系統的節流工作階段數量。在 *PA-5200* 系列或 *PA-7000* 系列防火牆上，目前所使用的工作階段數量可能大於所設定的工作階段數量上限，因為每個虛擬系統有多個資料層。您在 *PA-5200* 系列或 *PA-7000* 系列防火牆上設定的工作階段數量限制是針對每個資料層，並導致每個虛擬系統的工作階段數量上限更高。 • **Security Rules**（安全性規則）— 安全性規則的數目上限。 • **NAT** 規則 — NAT 規則的數目上限。 • 解密規則 — 解密規則的數目上限。 • **QoS** 規則—QoS 規則的數目上限。 • 應用程式取代規則 — 應用程式取代規則的數目上限。 • **Policy Based Forwarding Rules**（基於原則的轉送規則）— 基於原則的轉送 (PBF) 規則的數目上限。 • **DoS Protection Rules**（**DoS** 保護規則）— 拒絕服務 (DoS) 規則的數目上限。 • 站台對站台 **VPN** 通道 — 站台對站台 VPN 通道的數目上限。 • 並行 **GlobalProtect** 通道 — 並行遠端 GlobalProtect 使用者的數目上限。 • **Inter-Vsys User-ID Data Sharing**（**Vsys** 間 **User-ID** 資料共用）—**Make this vsys a User-ID data hub**（將此 **vsys** 設定為 **User-ID** 資料中心），可允許防火牆上的所有其他虛擬系統，以存取共用使用者對應資訊，或 **Change hub**（變更中心），然後選取新的 VSYS 以將該 VSYS 重新指派為 User-ID 資料中心。需要超級使用者或管理員權限。

© 2019 Palo Alto Networks, Inc.

裝置 > 共用閘道

共用閘道 允許多個虛擬系統在外部通訊時共用單一介面（一般連線到共同的上游網路，例如網際網路服務供應商）。所有虛擬系統都使用一個 IP 位址透過實體介面與外界通訊。會使用一個虛擬路由器來透過共用閘道傳送所有虛擬系統的流量。

共用閘道會使用第三層介面，而且必須設定至少一個第三層介面為共用閘道。源自虛擬系統，並透過共用閘道結束防火牆的通訊，需要有類似的原則才能在兩個虛擬系統之間傳遞通訊。您可以設定「外部虛擬系統」區域來定義虛擬系統中的安全性規則。

共用閘道設定	說明
ID	閘道的識別碼（未由防火牆使用）。
名稱	輸入共用閘道的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。只有名稱為必填。
DNS Proxy	（選用）若設定 DNS Proxy，請選取要使用於網域名稱查詢的 DNS 伺服器。
介面	針對共用閘道將會使用的介面來選取介面。

© 2019 Palo Alto Networks, Inc.

裝置 > 憑證管理

- Device > Certificate Management > Certificates（裝置 > 憑證管理 > 憑證）
- Device > Certificate Management > Certificate Profile（裝置 > 憑證管理 > 憑證設定檔）
- Device > Certificate Management > OCSP Responder（裝置 > 憑證管理 > OCSP 回應程式）
- Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔）
- Device > Certificate Management > SCEP（裝置 > 憑證管理 > SCEP）
- 裝置 > 憑證管理 > SSL 解密排除
- Device > Certificate Management > SSH Service Profile（裝置 > 憑證管理 > SSL 服務設定檔）

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > Certificates（裝置 > 憑證管理 > 憑證）

選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證），可管理（產生、匯入、更新、刪除及撤銷）用來保護網路間通訊的憑證。您也可以匯出和匯入高可用性 (HA) 金鑰，此金鑰可用於保護網路上 HA 端點之間的連線安全。選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Default Trusted Certificate Authorities**（預設受信任的憑證授權單位），可檢視、啟用和停用防火牆信任的憑證授權單位 (CA)。

如需如何實作防火牆與 *Panorama* 上之憑證的詳細資訊，請參考憑證管理。

- 管理防火牆及 Panorama 憑證
- 管理預設受信任的憑證授權單位
- Device > Certificate Management > Certificate Profile（裝置 > 憑證管理 > 憑證設定檔）
- Device > Certificate Management > OCSP Responder（裝置 > 憑證管理 > OCSP 回應程式）
- Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔）
- Device > Certificate Management > SCEP（裝置 > 憑證管理 > SCEP）
- Device > Master Key and Diagnostics（裝置 > 主要金鑰與診斷）

管理防火牆及 Panorama 憑證

- Device > Certificate Management > Certificates > Device Certificates（設備 > 憑證管理 > 憑證 > 設備憑證）
- Panorama > Certificate Management > Certificates（Panorama > 憑證管理 > 憑證）

選取 **Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）或 **Panorama** > **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證）可顯示防火牆或 Panorama 的憑證，這些憑證可用於保障 Web 介面存取安全、SSL 解密或 LSVPN 等工作。

下列是一些憑證的使用方式。請在產生憑證後定義其使用方式（請參閱管理預設受信任的憑證授權單位）。

- **Forward Trust**（轉送信任）—防火牆使用此憑證來簽署伺服器憑證副本，當簽署伺服器憑證的憑證授權單位 (CA) 在防火牆上的受信任 CA 清單中時，防火牆在 SSL 轉送 代理程式 解密 期間向用戶端顯示該憑證。
- **Forward Untrust**（轉送不信任）—防火牆使用此憑證來簽署伺服器憑證副本，當簽署伺服器憑證的憑證授權單位 (CA) 不在防火牆上的受信任 CA 清單中時，防火牆在 SSL 轉送 代理程式 解密 期間向用戶端顯示該憑證。
- **Trusted Root CA**（受信任的根 **CA**）—防火牆針對 SSL 正向 Proxy 解密、GlobalProtect、URL 管理員取代及驗證入口網站，將此憑證用作受信任的 CA。防火牆擁有一份現有信任 CA 的大清單。受信任的根 CA 憑證適用於您企業信任但不屬於預先安裝信任清單一部分的其他 CA。
- **SSL Exclude**（**SSL** 排除）—如果您設定解密例外狀況 以從 SSL/TLS 解密中排除特定伺服器，防火牆將使用此憑證。
- **Certificate for Secure Syslog**（安全 **Syslog** 的憑證）—防火牆使用此憑證來保障向 Syslog 伺服器提交作為 Syslog 訊息的日誌。

若要產生憑證，請按一下 [產生] 並指定下列欄位：

© 2019 Palo Alto Networks, Inc.

在產生憑證後，頁面上會顯示其他用來管理憑證的支援動作。

用以產生憑證的設定	說明
憑證類型	選取產生憑證的實體： **Local**（本機）—防火牆或 Panorama 會產生憑證。 **SCEP**—簡易憑證註冊通訊協定 (SCEP) 伺服器會產生憑證，並將其傳送到防火牆或 Panorama。
憑證名稱	（必要）輸入一個名稱區以識別憑證（在防火牆上最多可使用 63 個字元，在 Panorama 上最多可使用 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
SCEP 設定檔	（僅限 SCEP 憑證）選取 **SCEP Profile**（**SCEP** 設定檔）可定義防火牆或 Panorama 如何與 SCEP 伺服器通訊，並可定義 SCEP 憑證的設定。如需詳細資訊，請參閱 [設備 > 憑證管理 > SCEP]。您可以設定防火牆來作為 GlobalProtect 入口網站，以便視需要要求 SCEP 憑證以及自動部署 憑證到端點中。 [產生憑證] 對話方塊中的剩餘欄位不會套用至 SCEP 憑證。在指定 **Certificate Name**（憑證名稱）和 **SCEP Profile**（**SCEP** 設定檔）之後，請按一下 **Generate**（產生）。
Common Name (通用名稱)	（選用）輸入將顯示在憑證上的 IP 位址或 FQDN。
共享	在具有一個以上虛擬系統 (VSYS) 的防火牆中，若您要讓每個 VSYS 皆可使用憑證，請選取 **Shared**（共用）。
簽署者	若要簽署憑證，您可以使用您匯入到防火牆的憑證授權單位 (CA) 憑證。憑證也可以是自我簽署憑證，若是如此，則是由防火牆擔任 CA 角色。如果您使用 Panorama，也可以選擇產生 Panorama 的自我簽署憑證。 如果已匯入 CA 憑證或已在防火牆上發行憑證（自我簽署），下拉式清單中會包含可用於簽署正在建立之憑證的 CA。 若要產生憑證簽署要求 (CSR)，請選取外部授權 **(CSR)**。在防火牆產生憑證和金鑰配對之後，您可以匯出 CSR 並將它傳送到 CA 以便進行簽署。
certificate authority (憑證授權單位)	若您要防火牆發行憑證，請選取此選項。 將此憑證標記為 CA，可讓您使用此憑證來簽署防火牆上的其他憑證。
封鎖私密金鑰匯出	產生憑證時，選取此選項可阻止所有管理員（包括超級使用者）匯出私密金鑰。
OCSP 回應程式	從下拉式清單選取 OCSP 回應程式設定檔（請參閱 [設備 > 憑證管理 > OCSP 回應程式]）。對應的主機名稱會顯示在憑證中。
演算法	為憑證選取一個金鑰產生演算法：**RSA** 或 **Elliptic Curve DSA**（橢圓曲線 **DSA**）(ECDSA)。 ECDSA 會使用比 RSA 演算法更小的金鑰大小，且因此可提供效能強化功能，以便處理 SSL/TLS 連線。ECDSA 也可提供與 RSA 相同或更高的安全性。建議您將 ECDSA 用於支援 ECDSA 的用戶端瀏覽器和作業系統，但您可能需要選取 RSA 才能與舊版瀏覽器和作業系統相容。

© 2019 Palo Alto Networks, Inc.

用以產生憑證的設定	說明
	執行 *PAN-OS 6.1* 或以前版本的防火牆將刪除任何從 *Panorama* 推送的 *ECDSA* 憑證，且任何由 *ECDSA* 憑證授權單位 *(CA)* 簽署的 *RSA* 憑證在那些防火牆上將成為無效。 您無法使用硬體安全性模組 (HSM) 來儲存 ECDSA 私密金鑰，以便用於 SSL 轉送代理程式 或輸入檢查解密。
位元組數	選取憑證的金鑰長度。 若防火牆處於 FIPS-CC 模式，且金鑰產生 **Algorithm**（演算法）為 **RSA**，則產生的 RSA 金鑰必須為 **2048** 或 **3027** 位元。若 **Algorithm**（演算法）為 **Elliptic Curve DSA**（橢圓曲線 **DSA**），則兩個金鑰長度選項（**256** 和 **384**）將可供使用。
摘要	選取憑證的 **Digest**（摘要）演算法。可用的選項取決於金鑰產生演算法： • **RSA—MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512** • **Elliptic Curve DSA**（橢圓曲線 **DSA**）—**SHA256** 或 **SHA384** 若防火牆處於 FIPS-CC 模式，且金鑰產生 **Algorithm**（演算法）為 **RSA**，則您必須選取 **SHA256**、**SHA384** 或 **SHA512** 作為 **Digest**（摘要）演算法。若 **Algorithm**（演算法）為 **Elliptic Curve DSA**（橢圓曲線 **DSA**），則兩個 **Digest**（摘要）演算法（**SHA256** 和 **SHA384**）將可供使用。 在要求仰賴 *TLSv1.2* 之防火牆服務（例如管理員存取 *Web* 介面）時所使用的用戶端憑證不能以 *SHA512* 作為摘要演算法。用戶端憑證必須使用較低程度的摘要演算法（例如 *SHA384*），否則，您必須在為防火牆服務設定 *SSL/TLS* 服務設定檔時，*Max Version*（最高版本）限制為 *TLSv1.1*（請參閱 *[設備 > 憑證管理 > SSL/TLS 服務設定檔]*）。
到期 (天數)	指定憑證有效的天數（預設是 365）。 如果您在 *GlobalProtect* 衛星設定中指定有效期間，該值將會覆蓋在此欄位中輸入的值。
憑證屬性	**Add**（新增）以指定其他 **Certificate Attributes**（憑證屬性），可識別您正在將憑證發行到的實體。您可以新增以下任何屬性：**Country**（國家）、**State**（州）、**Locality**（地區）、**Organization**（組織）、**Department**（部門）及 **Email**（電子郵件）。此外，您可以指定下列其中一個主旨替代名稱欄位：**Host Name**（主機名稱）(SubjectAltName:DNS)、**IP** (SubjectAltName:IP) 和 **Alt Email**（替代電子郵件）(SubjectAltName:email)。 若要新增國家/地區作為憑證屬性，請從 *Type*（類型）欄中選取 *Country*（國家/地區），然後按一下 *Value*（值）欄來查看 *ISO 6366* 國碼。

若您已設定硬體安全性模組 *(HSM)*，則私人金鑰會儲存在外部 *HSM* 存放區而非防火牆上。

© 2019 Palo Alto Networks, Inc.

其他用來管理憑證的支援動作

產生憑證之後，其詳細資訊會顯示在頁面上並可使用下列動作：

其他用來管理憑證的支援動作	說明
刪除	選取憑證並加以 **Delete**（刪除）。 如果防火牆具有解密政策，您將無法刪除用於設定 *Forward Trust Certificate*（轉送信任憑證）或 *Forward Untrust Certificate*（轉送不信任憑證）的憑證。若要變更憑證使用情況，請參閱管理預設受信任的憑證授權單位。
撤銷	選取要撤銷的憑證，再按一下撤銷。會立刻將憑證設定為已撤銷狀態。不需要認可。
更新	在憑證到期或即將到期的情況下，請選取對應的憑證並按一下更新。設定憑證的有效期間（天數），再按一下 **OK**（確定）。 如果防火牆為簽發憑證的 CA，則防火牆會用與舊憑證序號不同但屬性相同的新憑證予以取代。 如果外部憑證授權單位 (CA) 已簽署憑證，且防火牆使用線上憑證狀態協定 (OCSP) 驗證憑證撤銷狀態，防火牆會使用 OCSP 回應程式資訊更新憑證狀態
匯入	**Import**（匯入）憑證並進行設定，如下所示： • 輸入用來識別憑證的憑證名稱。 • 瀏覽到憑證檔案。如果您匯入 **PKCS12** 憑證及私密金鑰，單一檔案將包含兩者。如果您匯入 **PEM** 憑證，檔案則僅包含憑證。 • 選取憑證的 **File Format**（檔案格式）。 • 如果 HSM 用來儲存此憑證的金鑰，請選取 **Private key resides on Hardware Security Module**（私密金鑰位於硬體安全性模組核取方塊）。如需 HSM 詳細資訊，請參閱 [設備 > 設定 > HSM]。 • 視需要 **Import Private Key**（匯入私密金鑰）（僅限 PEM 格式）。如果您選取 **PKCS12** 作為憑證 **File Format**（檔案格式），則選取的 **Certificate File**（憑證檔案）包含金鑰。如果您選取 **PEM** 格式，請瀏覽到加密的私密金鑰檔案（通常名為 *.key）。對於兩種格式，請輸入 **Passphrase**（複雜密碼）及 **Confirm Passphrase**（確認複雜密碼）。 在您匯入憑證並選取 **Import Private Key**（匯入私密金鑰）時，選取 **Block Private Key Export**（封鎖私密金鑰匯出），可防止任何管理員（包括超級使用者）匯出私密金鑰。 當您將憑證匯入至處於 *FIPS-CC* 模式的 *Palo Alto Networks* 防火牆或 *Panorama* 伺服器，您必須匯入憑證作為 *Base64* 編碼憑證 *(PEM)*，而且必須使用 *AES* 將私密金鑰加密。此外，您必須使用 *SHA1* 作為複雜密碼型金鑰衍生方法。 若要匯入 PKCS12 憑證，請將憑證轉換為 PEM 格式（使用 OpenSSL 之類的工具）；確保您在轉換期間使用的密碼字詞至少 6 個字元。

© 2019 Palo Alto Networks, Inc.

其他用來管理憑證的支援動作	說明
匯出	選取您想要匯出的憑證，按一下 **Export**（匯出），然後選取 **File Format**（檔案格式）： • 加密的私密金鑰與憑證 (PKCS12)—匯出的檔案將包含憑證與私密金鑰。 • Base64 編碼憑證 (PEM)—如果您還想要匯出私密金鑰，請選取 [匯出私密金鑰]，然後輸入 [複雜密碼] 並 [確認複雜密碼]。 • 二進位編碼憑證 (DER)—您僅可匯出憑證，而非金鑰：請略過 [匯出私密金鑰] 及複雜密碼欄位。
匯入 HA 金鑰 匯出 HA 金鑰	HA 金鑰必須在兩個防火牆端點之間進行交換；也就是必須匯出防火牆 1 的金鑰，然後將其匯入防火牆 2，反之亦然。 若要匯入高可用性 (HA) 的金鑰，請按一下 **Import HA Key**（匯入 HA 金鑰），**Browse**（瀏覽）並指定要匯入的金鑰檔案。 若要匯出 HA 的金鑰，按一下匯出 **HA** 金鑰並指定要儲存檔案的位置。
定義憑證的用法	在 [名稱] 欄中，選取憑證，然後選取相應選項來指示如何使用憑證。
PDF/CSV	具有最小唯讀訪問權限的管理角色可以匯出如 **PDF/CSV** 的託管憑證設定表。您可以在稽核等情況下套用篩選以建立更多特定表格組態匯出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。

管理預設受信任的憑證授權單位

- 設備 > 憑證管理 > 憑證 > 受信任的憑證授權單位

使用此頁面以檢視、停用或匯出防火牆所信任且預先包含的憑證授權單位 (CA)。預安裝的 CA 清單包含最常見和受信住的憑證供應商，負責發布防火牆安全連接至網際網路的憑證。每個受信任的根 CA 均會顯示名稱、主旨、簽發者、到期日和有效狀態。

防火牆不信任預設的中繼 CA，因為中繼 CA 不是防火牆和受信任的根 CA 間信任鍊的一部分。您必須手動新增任何您想要防火牆信任的中繼 CA 以及任何您組織需要的其他受信任的企業 CA（**Device**（設備）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（設備憑證））。

Trusted Certificate Authorities 設定	說明
啟用	如果您已停用 CA，您可以加以重新 **Enable**（啟用）。
停用	選取 CA，然後加以 **Disable**（停用）。您可以使用此選項以便只信任特定 CA，或是停用所有其他 CA 並只信任您的本機 CA。
匯出	選取並 **Export**（匯出）CA 憑證。您可以匯入至其他系統或離線檢視憑證。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > Certificate Profile（裝置 > 憑證管理 > 憑證設定檔）

- **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔）
- **Panorama** > **Certificate Management**（憑證管理）> **Certificate Profile**（憑證設定檔）

憑證設定檔會定義要使用哪些憑證授權單位 (CA) 憑證來確認用戶端憑證、如何確認憑證撤銷狀態，以及該狀態對存取有何限制。在為驗證入口網站、GlobalProtect、站台對站台 IPsec VPN、動態 DNS (DDNS)，以及防火牆與 Panorama 的網頁介面存取設定憑證驗證時，您可以選取設定檔。您可以為前述各項服務設定個別的憑證設定檔。

憑證設定檔設定	說明
名稱	（必要）輸入一個名稱區以識別設定檔（在防火牆上最多可使用 63 個字元，在 Panorama 上最多可使用 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
Username Field	如果 GlobalProtect 僅使用憑證進行入口網站和閘道驗證，PAN-OS 軟體會將您在 **Username Field**（使用者名稱欄位）下拉式清單中選取的憑證欄位作為使用者名稱，並將該使用者名稱與 User-ID 服務的 IP 位址做比對： • **Subject**（主體）—通用名稱 • **Subject Alt**（主體別名）—電子郵件或主體名稱。 • 無—通常用於 GlobalProtect 裝置或預先登入驗證。
網域	輸入 NetBIOS 網域，讓 PAN-OS 軟體可透過 User-ID 對應使用者。
CA 憑證	（選用）**Add**（新增）**CA Certificate**（**CA** 憑證）以指派給設定檔。 （選用）如果防火牆使用線上憑證狀態協定 (OCSP) 來確認憑證撤銷狀態，請設定下列欄位以取代預設行為。對於大多數的部署而言，這些欄位並不適用。 • 依預設，防火牆使用憑證中的授權資訊存取 (AIA) 資訊來擷取 OCSP 回應程式資訊。若要覆寫 AIA 資訊，請輸入 **Default OCSP URL**（預設 **OCSP URL**）（開頭為 `http://` 或 `https://`）。 • 依預設，防火牆會使用在 **CA** 憑證欄位中選取的憑證來驗證 OCSP 回應。若要使用不同的憑證進行驗證，請在 **OCSP** 驗證 **CA** 憑證欄位中選取所需憑證。 此外，輸入 **Template Name**（範本名稱）以辨識用於簽署憑證的範本。
使用 CRL	選取此選項可使用憑證撤銷清單 (CRL) 來驗證憑證的撤銷狀態。
使用 OCSP	選取此選項可使用 OCSP 來驗證憑證的撤銷狀態。

© 2019 Palo Alto Networks, Inc.

憑證設定檔設定	說明
	如果選取 *OCSP* 和 *CRL* 二者，防火牆會先嘗試 *OCSP*，如果 *OCSP* 回應程式無法使用，則僅會回復 *CRL* 方法。
CRL 接收逾時	指定間隔（1 到 60 秒），過了此間隔後，防火牆會停止等待 CRL 服務的回應。
Ocsp 接收逾時	指定間隔（1 到 60 秒），過了此間隔後，防火牆會停止等待 OCSP 回應程式的回應。
憑證狀態逾時	指定間隔（1 到 60 秒），過了此間隔後，防火牆會停止等待任何憑證狀態服務的回應，並套用您定義的任何工作階段封鎖邏輯。
如果憑證狀態未知則封鎖工作階段	若要防火牆在 OCSP 或 CRL 服務傳回未知的憑證撤銷狀態時封鎖工作階段，請選取此選項。否則，防火牆會繼續進行該工作階段。
如果在逾時時間內無法擷取憑證狀態，會封鎖工作階段	若要防火牆在登錄 OCSP 或 CRL 要求逾時後封鎖工作階段，請選取此選項。否則，防火牆會繼續進行該工作階段。
若未發行憑證至驗證裝置則封鎖工作階段	（僅限 GlobalProtect）如果您希望防火牆在用戶端憑證主旨中的序號屬性與 GlobalProtect 應用程式向端點報告的主機 ID 不相符時封鎖工作階段，則選取此選項。否則，防火牆會允許這些工作階段。此選項僅適用於GlobalProtect certificate authentication（GlobalProtect 憑證驗證）。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > OCSP Responder（裝置 > 憑證管理 > OCSP 回應程式）

選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **OCSP Responder**（**OCSP** 回應程式），可定義線上憑證狀態協定 (OCSP) 回應程式（伺服器）以確認憑證的撤銷狀態。

除了新增 OCSP 回應程式外，還需要執行下列工作才能啟用 OCSP：

- 啟用防火牆與 OCSP 伺服器之間的通訊：選取 **Device**（裝置）> **Setup**（設定）> **Management**（管理）、在 Management Interface Settings（管理介面設定）中選取 **HTTP OCSP**，然後按一下 **OK**（確定）。
- 如果防火牆將解密輸出 SSL/TLS 流量，您可選取是否設定它來確認目的地伺服器憑證的撤銷狀態：選取 **Device**（裝置）> **Setup**（設定）> **Sessions**（工作階段）、按一下 **Decryption Certificate Revocation Settings**（解密憑證撤銷設定）、在 OCSP 設定中選取 **Enable**（啟用）、輸入 **Receive Timeout**（接收逾時）（防火牆停止等待 OCSP 回應之前所經過的間隔），然後按一下 **OK**（確定）。
- 若要選取性地將防火牆設定為 OCSP 回應程式，請將介面管理設定檔新增至用於 OCSP 服務的介面。首先，選取 **Network**（網路）> **Network Profiles**（網路設定檔）> **Interface Mgmt**（介面管理）、按一下 **Add**（新增）、選取 **HTTP OCSP**，然後按一下 **OK**（確定）。其次，選取 **Network**（網路）> **Interfaces**（介面）、按一下防火牆將用於 OCSP 服務的介面名稱、選取**Advanced**（進階）> **Other info**（其他資訊）、選取您設定的介面管理設定檔，然後按一下 **OK**（確定） 和 **Commit**（認可）。

啟用 *OCSP* 回應程式，以便憑證在被撤消時會通知您，並可以採取適當的操作來建立與入口網站和閘道的安全的連線。

OCSP Responder 設定	說明
名稱	輸入用來識別回應程式的名稱（最多 31 個字元）。名稱區分大小寫。名稱必須是唯一的，且只能使用字母、數字、空格、連字號與底線。
位置	選取回應程式可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取位置；它的值已預先設定為 [共用]。儲存回應程式之後，您就無法變更其 **Location**（位置）。
主機名稱	輸入 OCSP 回應程式的主機名稱（建議）或 IP 位址。PAN-OS 會自動從這個值衍生出 URL 並新增至正在驗證的憑證。如果您將防火牆設為 OCSP 回應程式，則主機名稱必須解析成防火牆為 OCSP 服務所使用介面中的 IP 位址。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔）

- Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔）
- Panorama > Certificate Management > SSL/TLS Service Profile（Panorama > 憑證管理 > SSL/TLS 服務設定檔）

SSL/TLS 服務設定檔會針對使用 SSL/TLS（例如 Web 介面的管理存取）的防火牆或 Panorama 服務，指定伺服器憑證和通訊協定版本或通訊協定範圍。藉由定義通訊協定版本，這些設定檔將可讓您限制可用來確保能夠與要求服務的用戶端系統進行安全通訊的加密套件。

在要求防火牆或 *Panorama* 服務的用戶端系統中，憑證信任清單 *(CTL)* 必須包含發出 *SSL/TLS* 服務設定檔所指定之憑證的憑證授權單位 *(CA)* 憑證。否則，使用者在要求服務時將會看見憑證錯誤。根據預設，大部分的第三方 *CA* 憑證都會顯示在用戶端瀏覽器中。如果企業或防火牆產生的 *CA* 憑證是簽發者，您就必須將該 *CA* 憑證部署至用戶端瀏覽器中的 *CTL*。

若要新增設定檔，請按一下 **Add**（新增），並完成下表中的欄位。

SSL/TLS 服務設定檔設定	說明
名稱	輸入用來識別設定檔的名稱（最多 31 個字元）。名稱區分大小寫。名稱必須是唯一的，且只能使用字母、數字、空格、連字號與底線。
共享	如果防火牆有多個虛擬系統 (VSYS)，則選取此選項將使設定檔可在所有虛擬系統上使用。依預設會清除此選項，且設定檔僅可用於在 **Device**（裝置）頁籤的 **Location**（位置）下拉式清單中選取的 VSYS。
憑證	選取、匯入或產生要與設定檔相關聯的伺服器憑證（請參閱管理防火牆和 Panorama 憑證）。 請勿針對 *SSL/TLS* 服務使用憑證授權單位 *(CA)* 憑證；請僅使用已簽署的憑證。
最低版本 最高版本	選取服務可使用的最舊版（**Min Version**（最低版本））和最新版（**Max Version**（最高版本））TLS。**TLSv1.0**、**TLSv1.1**、**TLSv1.2**、**TLSv1.3** 或 **Max**（最大）（最新的可用版本）。 在執行 *PAN-OS 8.0* 或更新版本、處於 *FIPS/CC* 模式的防火牆上，*TLSv1.1* 是最低支援的 *TLS* 版本；不要選 *TLSv1.0*。 要求倚賴 *TLSv1.2* 的防火牆服務時所使用的用戶端憑證，不可用 *SHA512* 作為摘要演算法。這些用戶端憑證必須使用較低的摘要演算法（例如 *SHA384*），或您必須將服務的 *Max Version*（最高版本）限定為 *TLSv1.1*。 使用最強大的通訊協定版本可以為您的網絡提供最強大的安全性。如果可以，請將 *Min Version*（最低版

© 2019 Palo Alto Networks, Inc.

SSL/TLS 服務設定檔設定	說明
	本）設為 *TLSv1.2*，並將 *Max Version*（最高版本）設為 *Max*（最高）。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > SCEP（裝置 > 憑證管理 > SCEP）

簡易憑證註冊通訊協定 (SCEP) 提供用來將唯一憑證發出至端點、閘道和衛星裝置的機制。選取 **Device**（裝置）> **Certificate Management**（憑證管理）> **SCEP**，可建立 SCEP 設定。

如需有關如何建立 *SCEP* 設定檔的資料，請參考使用 SCEP 部署憑證
.

若要啟動新的 SCEP 設定，請按一下 **Add**（新增），然後完成下列欄位。

SCEP 設定	說明
名稱	指定描述性名稱以識別此 SCEP 設定，例如 SCEP_*Example*。這個名稱會將此 SCEP 設定檔與您可能會在組態設定檔中使用的其他實例區分開。
位置	如果系統有多個虛擬系統，請為設定檔選取位置。位置將識別 SCEP 組態的可用位置。
一次性密碼 (挑戰)	
SCEP 挑戰	（選用）為使 SCEP 型憑證更安全地產生，您可在公開金鑰基礎結構 (PKI) 與各憑證要求的入口網站之間設定 SCEP 挑戰回應機制，即一次性密碼 (OTP)。 在您設定此機制後，其操作不可見，您不必進行進一步輸入。 您選取的挑戰機制將決定 OTP 的來源。如果您選取 **Fixed**（固定），請從 SCEP 伺服器複製 PKI 的註冊挑戰密碼，並在設定為 **Fixed**（固定）時顯示的入口網站 **Password**（密碼）對話方塊中輸入該字串。每當入口網站要求憑證時，都會使用此密碼進行 PKI 的驗證。如果您選取 **Dynamic**（動態），則應輸入您選取的使用者名稱和密碼（可能是 PKI 管理員的認證），以及入口網站用戶端提交這些認證的 SCEP **Server URL**（伺服器 **URL**）。當 SCEP 伺服器根據各憑證要求以透明方式產生入口網站的 OTP 密碼時，此使用者名稱與密碼仍保持相同。（您可以看到畫面在「註冊挑戰密碼是」欄位中重新整理後，此 OTP 將根據每個憑證要求而變更。）PKI 以透通方式將每個新密碼傳輸至入口網站，其接著使用該密碼用於憑證要求。 為了符合美國聯邦資訊處理標準 *(FIPS)*，請選取 *Dynamic*（動態）、指定使用 *HTTPS* 的 *Server URL*（伺服器 *URL*），然後啟用 *SCEP Server SSL Authentication*（*SCEP* 伺服器 *SSL* 驗證）。（*FIPS-CC* 操作會顯示於防火牆登入頁面及防火牆狀態列。）
組態設定	

© 2019 Palo Alto Networks, Inc.

SCEP 設定	說明
伺服器 URL	輸入入口網站要求並從 SCEP 伺服器接收用戶端憑證的 URL。範例： `http://<hostname or IP>/certsrv/mscep/.`
CA-IDENT 名稱	輸入用來識別 SCEP 伺服器的字串。最大長度為 255 位元。

主旨	設定主旨，使其包含關於裝置甚或使用者的識別資訊，並在憑證簽署要求 (CSR) 中將此資訊提供給 SCEP 伺服器。
	用來要求端點的用戶端憑證時，端點會傳送關於裝置的識別資訊，包括其主機 ID 值。主機 ID 值隨裝置類型而異，可以是介面的 GUID (Windows) MAC 位址、Android ID（Android 裝置）、UDID（iOS 裝置）或 GlobalProtect 指派的唯一名稱 (Chrome)。用來要求衛星裝置的憑證時，主機 ID 值將是裝置序號。
	若要在 CSR 中指定其他資訊，請輸入主旨名稱。主旨必須是一個格式為 *<attribute>=<value>* 的辨別名稱，且必須包含通用名稱 (CN) 金鑰。例如：
	`O=acme,CN=acmescep`
	有兩種方法可以指定 CN：
	• （建議使用）語彙基元型 **CN**—輸入其中一個支援的語彙基元 **$USERNAME**、**$EMAILADDRESS** 或 **$HOSTID**。使用使用者名稱或電子郵件地址變數，以確保入口網站要求特定使用者的憑證。若只要要求裝置的憑證，請指定主機 ID 變數。當 GlobalProtect 入口網站將 SCEP 設定推送至代理程式時，主旨名稱的 CN 部分會取代為憑證擁有者的實際值（使用者名稱、主機 ID 或電子郵件地址）。例如：
	`O=acme,CN=$HOSTID`
	• 靜態 **CN**—會將您指定的 CN 作為 SCEP 伺服器所發行之所有憑證的主旨使用。例如：
	`O=acme,CN=acmescep`

主旨替代名稱類型	您選取 **None**（無）以外的類型後，將會顯示一個對話方塊，供您輸入適當的值： • **RFC 822 Name**（**RFC 822** 名稱）—在憑證的主旨或主旨替代副檔名輸入電子郵件名稱。 • **DNS Name**（**DNS** 名稱）—輸入用於評估憑證的 DNS 名稱。 • 統一資源識別項 **(URI)**—輸入用戶端從中取得憑證的 URI 資源。
加密設定	• 位元數—為憑證選取金鑰的 **Number of Bits**（位元數）。如果防火牆處於 FIPS-CC 模式，則產生的金鑰必須至少為 2,048 位元。（FIPS-CC 操作會顯示於防火牆登入頁面及防火牆狀態列。） • 摘要 — 選取憑證的 **Digest**（摘要）演算法：**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。如果防火牆處於 FIPS-CC 模式，您必須選取 **SHA256**、**SHA384** 或 **SHA512** 作為 **Digest**（摘要）演算法。

© 2019 Palo Alto Networks, Inc.

SCEP 設定	說明
用作數位特徵碼	選取此選項可設定端點，以使用憑證中的私密金鑰來驗證數位特徵碼。
用於金鑰編密	選取此選項可設定用戶端端點，以使用憑證中的私密金鑰來加密透過 HTTPS 連線（使用 SCEP 伺服器核發的憑證建立連線）交換的資料。
CA 憑證指紋	（選用）若要確保入口網站會連線至正確的 SCEP 伺服器，請輸入 **CA Certificate Fingerprint**（**CA** 憑證指紋）。從 **Thumbprint**（指紋）欄位中的 SCEP 伺服器介面取得該指紋。 登入 SCEP 伺服器的管理使用者介面（例如，經由 http://<主機名稱或 IP>/CertSrv/mscep_admin/）。複製指紋，並在 **CA Certificate Fingerprint**（**CA** 憑證指紋）中加以輸入。
SCEP 伺服器 SSL 驗證	若要啟用 SSL，請選取 SCEP 伺服器的根 **CA Certificate**（**CA** 憑證）。選取 **Client Certificate**（用戶端憑證）來選取性地在 SCEP 伺服器與 GlobalProtect 入口網站之間啟用相互 SSL 驗證。

© 2019 Palo Alto Networks, Inc.

裝置 > 憑證管理 > SSL 解密排除

檢視及管理 SSL 解密排除。解密排除分為兩種，即預先定義的排除和自訂排除：

- 預先定義的解密排除能讓可能在防火牆加以解密時中斷的應用程式和服務保持加密狀態。Palo Alto Networks 定義了預先定義的解密排除，並在應用程式和威脅內容更新的過程中，定期更新及補強預先定義的排除清單。依預設會啟用預先定義的排除，但您可視需要選擇停用排除。
- 您可以建立自訂解密排除，將伺服器流量排除於解密作業外。所有源自目標伺服器，或預定要傳至該伺服器的流量，都會保持加密狀態。

您也可以根據應用程式、來源、目的地、*URL* 類別和服務，將流量排除在解密外。

使用此頁面上的設定，可修改或新增解密排除以及管理解密排除。

SSL 解密排除設定	說明
修改或 **Add**（新增）解密排除	
主機名稱	輸入可定義自訂解密排除的 **Hostname**（主機名稱）。防火牆會將該主機名稱與用戶端所要求的 SNI 或伺服器憑證中顯示的 CN 相比較。工作階段若有伺服器顯示的 CN 包含已定義的網域，則防火牆會將工作階段排除在解密外。 您可用星號 (*) 作為萬用字元，為與網域關聯的多個主機名稱名建立解密排除項。星號的表現與 URL 類別排除項的脫字符 (^) 的表現相同—每個星號控制主機名稱中的一個子網域（標籤）。這使您可以建立非常具體和非常一般的排除項。例如： • mail.*.com 匹配 mail.company.com，但不匹配 mail.company.sso.com。 • *.company.com 匹配 tools.company.com，但不匹配 eng.tools.company.com. • *.*.company.com 匹配 eng.tools.company.com，但不匹配 eng.company.com. • *.*.*.company.com 匹配 corp.exec.mail.company.com，但不匹配 corp.mail.company.com. • mail.google.* 匹配 mail.google.com，但不匹配 mail.google.uk.com. • mail.google.*.* 匹配 mail.google.co.uk，但不匹配 mail.google.com. 例如，要使用萬用字元將 video-stats.video.google.com 從解密中排除，而不將 video.google.com 從解密中排除，請排除 *.*.google.com。 不管主機名稱前面有多少個星號萬用字元（主機名稱之前沒有非萬用字元標籤），主機名稱都與項目匹配。例如，**.google.com*、**.*.google.com* 和 **.*.*.google.com* 都與 *google.com* 匹配。然而，**.dev.*.google.com* 不匹配 *google.com*，因為標籤 *(dev)* 不是萬用字元。 每個項目的主機名稱都應該是唯一的—如果傳送至防火牆的預先定義項目與現有的自訂項目相符，則會以自訂項目優先。 您無法為預先定義的解密排除編輯主機名稱。
共享	選取 **Shared**（共用），可在多個虛擬系統防火牆中的所有虛擬系統間共用解密排除。

© 2019 Palo Alto Networks, Inc.

SSL 解密排除設定	說明
	依預設會共用預先定義的解密排除，但您可以對特定虛擬系統啟用及停用預先定義和自訂的項目。
說明	（選用）說明您排除在解密外的應用程式，包括應用程式在解密時中斷的原因。
排除	將應用程式排除在解密外。停用此選項，可開始對先前排除在解密外的應用程式進行解密。
管理解密排除	
啟用	**Enable**（啟用）一或多個項目，以將其排除在解密外。
停用	**Disable**（停用）一或多個預先定義的解密排除。 由於解密排除會識別在解密時會中斷的應用程式，因此停用其中一個項目後，將會使應用程式不受支援。防火牆會嘗試解密應用程式，而應用程式將會中斷。若要確保特定的加密應用程式不會進入您的網路，您可以使用此選項。
顯示淘汰項目	**Show obsoletes**（顯示淘汰項目），以檢視 Palo Alto Networks 已不再定義為解密排除的預先定義項目。 更多淘汰項目的相關資訊： 預先定義解密排除的更新（包括移除預先定義的項目）會隨著應用程式和威脅內容更新提供至防火牆。啟用 **Exclude from decryption**（排除於解密外）的預先定義項目將會在防火牆收到不再包含該項目的內容更新時，自動從 SSL 解密排除清單中移除。 不過，停用 **Exclude from decryption**（排除於解密外）的預先定義項目即便在防火牆收到不再包含該項目的內容更新後，仍會保留在 SSL 解密清單中。當您 **Show obsoletes**（顯示淘汰項目）時，將會看見這些已停用且目前未強制執行的預先定義項目；您可以視需要手動移除這些項目。
顯示本機排除快取	**Show Local Exclusion Cache**（顯示本機排除快取）顯示防火牆由於技術原因（例如固定憑證、用戶端驗證或不受支援的密碼）而無法進行解密，且會自動將其排除在解密之外的站台。本機 SSL 解密快取與 SSL 解密排除清單（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））不同，其包含的站台可阻止 Palo Alto Networks 識別出的解密，並且您可以其中新增要選擇的永久解密排除項。防火牆根據與控制流量的解密政策規則關聯的解密設定檔的設定，使用本機發現的解密異常來填入本機 SSL 解密快取。 已排除的站台在本機快取中保留 12 小時，然後過時。每個排除項目均包含有關應用程式、伺服器、防火牆自動將站台從解密中排除的原因、套用至流量的解密設定檔以及 Vsys 的資訊。

© 2019 Palo Alto Networks, Inc.

Device > Certificate Management > SSH Service Profile（裝置 > 憑證管理 > SSL 服務設定檔）

SSH 服務設定檔讓您能夠限制加密和保護資料完整性的密碼、金鑰交換和訊息驗證碼演算法。具體來說，這些設定檔可於 SSH 工作階段期間，加強網路上命令列介面 (CLI)、管理連線與高可用性 (HA) 設備之間的資料保護。您還可以產生新的 SSH 主機金鑰，並指定啟動 SSH 金鑰重設的閾值（資料量、時間間隔和封包計數）。

若要設定 SSH 服務設定檔，**Add**（新增）HA 或管理-伺服器設定檔，根據需要填寫下表中的欄位，然後按一下 **OK**（確定）並 **Commit**（提交）您的變更。

套用設定檔的程序因設定檔類型而有所差異。

- 若要套用 HA 設定檔，請選取 Device > High Availability > General（裝置 > 高可用性 > 一般）。在 SSH HA 設定檔設定下，選取一個現有的設定檔。按一下 **OK**（確定）並 **Commit**（提交）變更。
- 若要套用管理-伺服器設定檔，請選取 Device > Setup > Management（裝置 > 設定 > 管理）。在 SSH 管理設定檔設定下，選取一個現有設定檔。按一下 **OK**（確定）並 **Commit**（提交）變更。

套用設定檔後，必須透過 *CLI* 執行 *SSH* 服務重新啟動，才能啟動設定檔。

SSH 服務設定檔設定	說明
名稱	輸入設定檔的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
密碼	選取伺服器將支援 SSH 工作階段加密的密碼演算法。
KEX	選取伺服器在 SSH 工作階段期間將支援的金鑰交換演算法。
MAC	選取伺服器在 SSH 工作階段期間將支援的訊息驗證碼演算法。
主機金鑰	選取主機金鑰類型和金鑰長度，以產生指定主機金鑰演算法和金鑰長度的新金鑰對。 選取主機金鑰類型後，可以輸入金鑰長度。預設金鑰類型和長度為 *RSA 2048*。
資料	設定 SSH 金鑰重設之前所傳輸的最大資料量 (MB)（範圍為 10 至 4000；預設為您選取的密碼值）。
間隔	設定 SSH 金鑰重設之前的最大時間間隔（秒）（範圍為 10 至 3600；預設為不以時間為基礎的重設金鑰）。

© 2019 Palo Alto Networks, Inc.

SSH 服務設定檔設定	說明
封包數	設定 SSH 金鑰重設之前的最大封包數 (2^n)。 如果未設定此參數，則工作階段將在 2^{28} 個封包之後重設金鑰。為了確保更頻繁地重設金鑰，請指定一個 *12* 至 *27* 之間的值。

© 2019 Palo Alto Networks, Inc.

裝置 > 回應頁面

自訂回應頁面是使用者嘗試存取 URL 時顯示的網頁。您可以提供下載及顯示的自訂 HTML 訊息，而非要求的網頁或檔案。

每個虛擬系統都可以擁有自己的自訂回應頁面。下表說明支援客戶訊息的自訂回應頁面類型。

自訂回應頁面類型	說明
防毒封鎖頁面	因感染病毒而使存取遭到封鎖。
應用程式封鎖頁面	因應用程式遭到安全原則規則封鎖而使存取遭到封鎖。
驗證入口網站登入頁面	防火牆會顯示此頁面，如此使用者便可輸入登入認證，以存取需遵守驗證原則規則的服務（請參閱 [原則 > 驗證]）。輸入訊息告知使用者如何回應此驗證挑戰。防火牆會根據指派給驗證規則的驗證執行物件中所指定的 **Authentication Profile**（驗證設定檔）來驗證使用者（請參閱 [物件 > 驗證]）。 您可以針對每個驗證規則顯示唯一的驗證指示，方法是在相關聯的驗證執行物件中輸入 *Message*（訊息）。物件中定義的訊息會取代驗證入口網站登入頁面中定義的訊息。
資料篩選封鎖頁面	內容是經由資料篩選設定檔比對，並因為檢測到敏感資訊而被封鎖。
檔案封鎖繼續頁面	此頁面可供使用者確認下載應該繼續。只有在安全性設定檔中啟用了繼續功能，才可使用此選項。選取 Objects（物件）> Security Profiles（安全性設定檔）> File Blocking（檔案封鎖）。
檔案封鎖頁面	因檔案存取遭到封鎖而使存取遭到封鎖。
GlobalProtect 應用程式說明頁面	GlobalProtect 使用者的自訂幫助頁面（可從 GlobalProtect 狀態面板上的設定選單存取）。
GlobalProtect 入口網站登入頁面	使用者嘗試驗證 GlobalProtect 入口網站的登入頁面。
GlobalProtect 入口網站首頁	驗證成功的使用者的 GlobalProtect 入口網站首頁。
GlobalProtect 應用程式歡迎頁面	成功連線至 GlobalProtect 的使用者的歡迎頁面。
MFA 登入頁面	防火牆會顯示此頁面，以便使用者在存取需遵守驗證原則規則的服務時回應多因素驗證 (MFA) 挑戰（請參閱 [原則 > 驗證]）。輸入訊息，告知使用者如何回應 MFA 挑戰。
SAML 驗證內部錯誤頁面	通知使用者 SAML 驗證失敗的頁面。頁面所包含的連結可供使用者重試驗證。
SSL 憑證錯誤通知頁面	SSL 憑證已撤銷的通知。
SSL 解密退出頁面	使用者警告頁面指示防火牆將解密 SSL 工作階段以供檢驗。

© 2019 Palo Alto Networks, Inc.

自訂回應頁面類型	說明
URL 篩選與類別比對封鎖頁面	遭 URL 篩選設定檔封鎖的存取，或是因為遭安全性原則規則封鎖的 URL 類別。
URL 篩選繼續與取代頁面	可讓使用者避開封鎖的頁面與初始封鎖原則。例如，使用者如果認為頁面遭到不正確的封鎖，可以按一下 **Continue**（繼續）來繼續進入此頁面。 使用覆蓋頁面時，使用者需要使用密碼才能覆蓋封鎖此 URL 的原則。如需設定取代密碼的相關指示，請參閱 < URL 管理員取代 > 一節說明。
URL 篩選安全搜尋強制封鎖頁面	遭到啟用 **Safe Search Enforcement**（安全搜尋強制執行）選項的 URL 篩選設定檔的安全原則規則封鎖存取。 若是使用 Bing、Google、Yahoo、Yandex 或 YouTube 執行搜尋，且其瀏覽器或搜尋引擎帳戶設定未將 [安全搜尋] 設為嚴格，使用者將看到此頁面。封鎖頁面會指示使用者將 [安全搜尋] 設定設為嚴格。
防網路釣魚封鎖頁面	當使用者嘗試在封鎖認證提交的網頁上輸入有效的公司認證（使用者名稱或密碼）時，向使用者顯示。使用者可以繼續存取網站，但仍無法提交有效的公司認證給任何相關聯的網頁表單。 選取 [物件 > 安全性設定檔 > URL 篩選]，可啟用認證偵測，並根據 URL 類別控制提交至網頁的認證。
防網路釣魚繼續頁面	本頁面會針對將公司認證（使用者名稱和密碼）提交給網站，向使用者發出警告。針對提交認證向使用者發出警告，有助於防止他們重複使用公司認證，並教育他們可能發生的釣魚嘗試。當使用者嘗試將認證提交至 **User Credential Submission**（使用者認證提交）權限設為 **continue**（繼續）的網站時，會看到此頁面（請參閱 [物件 > 安全性設定檔 > URL 篩選]）。他們必須選取 **Continue**（繼續）才能在網站上輸入認證。

您可以執行 **Response Pages**（回應頁面）的下列任何功能。

- 若要匯入自訂 HTML 回應頁面，請按一下您要變更之頁面類型的連結，然後按一下 [匯入/匯出]。瀏覽以找到頁面。會顯示一則訊息，指示匯入是否成功。若要成功匯入，檔案必須為 HTML 格式。
- 若要匯出自訂 HTML 回應頁面，請針對該頁面類型按一下 **Export**（匯出）。選取開啟檔案還是將其儲存至磁碟，如果適用，請選取 **Always use the same option**（使用相同選項）。
- 若要啟用或停用 **Application Block**（應用程式封鎖）頁面或 **SSL Decryption Opt-out**（**SSL** 解密退出選取）頁面，請針對該頁面類型按一下 **Enable**（啟用）。視需要選取或取消選取 **Enable**（啟用）。
- 若要使用預設的回應頁面而非先前上傳的自訂頁面，請刪除自訂封鎖頁面並確認。這會將預設封鎖頁面設為新的使用中頁面。

© 2019 Palo Alto Networks, Inc.

Device > Log Settings（裝置 > 日誌設定）

選取 **Device**（設備）> **Log Settings**（日誌設定）可設定警報、清除日誌，或啟用將日誌轉送至 Panorama、日誌記錄服務以及其他外部服務。

- 選取日誌轉送目的地
- 定義警報設定
- 清除記錄

選取日誌轉送目的地

Device（裝置）> **Log Settings**（日誌設定）

日誌設定頁可讓您設定轉送至以下地點的日誌：

- **Panorama**、**SNMP** 設陷接收器、郵件伺服器、**Syslog** 伺服器與 **HTTP** 伺服器—您也可以從日誌項目中的來源或目的地 IP 位址新增或移除頁籤；除了系統日誌型和組態日誌之外的所有日誌類都支援標記。
- 日誌記錄服務—如果您有日誌記錄服務訂閱，且已啟動日誌記錄服務（裝置 > 設定 > 管理），然後在您設定日誌轉送至 Panorama/日誌記錄服務時，防火牆將傳送日誌到日誌記錄服務。Panorama 將查詢日誌記錄服務以存取日誌、顯示日誌並生成報告。
- **Azure** 安全性中心—Azure 安全性中心的整合僅可用於 Azure 中的 VM 系列防火牆。
  - 如果您從 Azure 安全性中心啟動 VM 系列防火牆，則與此日誌轉送設定檔相連的安全性原則納定將自動啟用。
  - 如果您從 Azure 市場或使用自訂 Azure 範本啟動 VM 系列防火牆，則您必須手動選取 **Azure-安全性-中心-整合**以轉送系統日誌、使用者-ID 日誌和 HIP 比對日誌至 Azure 安全性中心，其他日誌類到，則使用日誌轉送設定檔（請參閱 Objects（物件）> Log Forwarding（日誌轉送））。

您的 *Azure* 訂閱自動啟用免費的安全性中心層級。

您可轉送下列日誌類型：系統、組態、User-ID、HIP 比對和關聯日誌。若要為各個日誌類型指定目的地，請 **Add**（新增）一個或多個比對清單設定檔（最多 64 個）並完成下表所述的欄位。

若要轉送流量、威脅、*WildFire* 提交、*URL* 篩選、資料篩選、通道檢查、*GTP* 和驗證日誌，您必須設定日誌轉送設定檔（請參閱 *[物件 > 日誌轉送]*）。

比對清單設定檔設定	說明
名稱	輸入用來識別比對清單設定檔的名稱（最多 31 個字元）。有效名稱必須以英數字元開頭，且可包含零、英數字元、底線、連字號、點或空格。
篩選	依預設，防火牆會轉送您新增比對清單設定檔的 **All Logs**（所有日誌）。若要轉送日誌的子集，請開啟下拉式清單並選取現有的篩選器或選取 **Filter Builder**（篩選建立器）以新增新的篩選器。針對新篩選器中的各個查詢，指定下列欄位並 **Add**（新增）查詢： • 連接器—選取查詢的連接器邏輯（and/or）。若您要將否定套用至邏輯，則選取 **Negate**（否定）。例如，若要避免從不受信任的區域轉送日誌，請選取 **Negate**（否定）、選取 **Zone**（區域）屬性、選取 **equal** 運算子，然後在 [值] 欄中輸入不受信任的區域名稱。 • 屬性—選取日誌屬性。可用的屬性依日誌類型而異。

© 2019 Palo Alto Networks, Inc.

比對清單設定檔設定	說明
	• 運算子—選取準則以決定是否套用屬性（例如 **equal**）。可用的規則依日誌類型而異。 • 值—指定要比對的屬性值。 若要顯示或匯出篩選器比對的日誌，請選取 **View Filtered Logs**（檢視篩選的日誌）。此頁籤提供與 **Monitoring**（監控）頁籤頁面相同的選項（例如 **Monitoring**（監控）> **Logs**（日誌）> **Traffic**（流量））。 將篩選器設定為轉送全部事件嚴重等級的日誌（預設篩選器為*All Logs*（全部日誌））。如要為不同的嚴重等級建立單獨的日誌轉送方法，請在 *Filter*（篩選器）中指定一個或多個嚴重等級，設定 *Forward Method*（轉送方法），然後在其餘嚴重等級重複此過程。
說明	輸入說明（最多 1,023 個字元）以解釋這個比對清單設定檔的目的。
Panorama / 日誌記錄服務	若您要將日誌轉送至日誌記錄服務、日誌收集器或 Panorama 管理伺服器，請選取 **Panorama** / 日誌記錄服務。若您啟用此選項，則您必須設定日誌轉送至 Panorama。 您無法從防火牆轉送關聯日誌到 *Panorama*。*Panorama* 會根據其接收的防火牆日誌產生關聯日誌。
SNMP	**Add**（新增）一或多個 SNMP 設陷伺服器設定檔，將日誌當作 SNMP 設陷轉送（請參閱 [裝置 > 伺服器設定檔 > SNMP 設陷]）。
電郵	**Add**（新增）一或多個電子郵件伺服器設定檔，將日誌當作電子郵件通知轉送（請參閱 [裝置 > 伺服器設定檔 > 電子郵件]）。
Syslog	**Add**（新增）一或多個 Syslog 伺服器設定檔，將日誌當作 Syslog 訊息轉送（請參閱 [裝置 > 伺服器設定檔 > Syslog]）。
HTTP	**Add**（新增）一個或多個 HTTP 伺服器設定檔，將日誌當作 HTTP 要求轉送（請參閱 [裝置 > 伺服器設定檔 > HTTP]）。
內建動作	**Add**（新增）要執行的動作時，可以從兩種內建動作中進行選擇—標記和整合。 • 標記—您可針對日誌項目中包含來源或目的地 IP 位址的所有日誌類型新增動作，具體方法是視需要設定下列設定。 您只可以標記關聯日誌和 *HIP* 比對日誌中的來源 *IP* 位址。由於日誌類型不包含日誌項目中的 *IP* 位址，因此您無法針對系統日誌和組態日誌設定任何動作。 • **Add**（新增）動作並輸入用以說明該動作的名稱。 • 選取您要自動標記的 IP 位址—**Source Address**（來源位址）或**Destination Address**（目的地位址）。 • 選取動作—**Add Tag**（新增頁籤）或 **Remove Tag**（移除頁籤）。 • 選取要向此防火牆或 Panorama 上的 **Local User-ID**（本機 **User-ID**）代理程式，或向 **Remote User-ID**（遠端 **User-ID**）代理程式註冊 IP 位址和頁籤對應。

© 2019 Palo Alto Networks, Inc.

比對清單設定檔設定	說明
	• 若要向 **Remote User-ID**（遠端 **User-ID**）代理程式註冊 IP 位址和頁籤對應，請選取將啟用轉送的 HTTP 伺服器設定檔（裝置 > 伺服器設定檔 > HTTP）。 • 設定 IP-Tag **Timeout**（逾時）以設定 IP 位址到頁籤對應維護的時間。將逾時設定為 0 代表著 IP-Tag 對應不會逾時（範圍為 0 到 43200（30 天）；預設值為 0）。 您只能使用 *Add Tag*（新增頁籤）動作設定連線逾時。 • 輸入或選取您要套用或從目標來源或目的地 IP 位址移除的 **Tags**（頁籤）。 • 整合—僅可用於 Azure 上的 VM 系列防火牆。**Add**（新增）一個名稱並使用此動作轉送選定的日誌至 Azure 安全性中心。若您並未看見此選項，您的 Azure 訂閱可能沒有在 Azure 安全性中心啟動。 若要在日誌轉送設定檔篩選器基礎上新增裝置到隔離清單，請選取 **Quarantine**（隔離）。

定義警報設定

- Device > Log Settings（裝置 > 日誌設定）

使用 [警報設定]，為 CLI 和 Web 介面設定警報。您可為下列事件設定通知：

- 安全性規則（或規則群組）已符合特定閾值，且位於特定時間間隔內。
- 符合加密/解密失敗閾值。
- 每個日誌類型的日誌資料庫接近已滿；依預設配額會設定為在使用 90% 可用磁碟空間時進行通知。設定警報可讓您在磁碟已滿之前採取動作，並可清除日誌。

啟用警報後，您可以按一下網頁介面底部的 **Alarms**（警報）(Alarms) 以檢視目前的清單。

若要新增警報，請編輯下表中所述的 [警報設定]。

警報日誌設定	說明
啟用警報	只有在您 **Enable Alarms**（啟用警報）時，才會顯示警報。 如果您停用警報，防火牆將不會警示您有重大事件需要處理。例如，系統在主要金鑰即將到期時對您發出警報；如果金鑰在您加以變更前即到期，防火牆會重新開機並進入維護模式，因而需要原廠重設。
啟用 CLI 警報通知	出現警告時啟用 CLI 警告通知。
啟用 Web 警報通知	畫面上會開啟視窗，顯示有關使用者工作階段的警告，包括警告出現時間與確認時間。
啟用可聽式警報	當管理員登入 Web 介面且存在未確認的警報時，警報聲將在管理員的電腦每 15 秒播放一次。管理員確認所有警報之前，警報聲將一直播放。 若要檢視及確認警報，請按一下 **Alarms**（警報）。

© 2019 Palo Alto Networks, Inc.

警報日誌設定	說明
	只有在防火牆處於 FIPS-CC 模式時，才可使用此功能。
加密/解密失敗閾值	指定產生警告前允許的加密/解密失敗次數。
<日誌類型> 日誌資料庫	當日誌資料庫達到指示的最大大小比例時，系統會產生警告。
安全性違規閾值/ 安全性違規時間週期	在 **Security Violations Time Period**（安全性違規時段）設定中指定的期間內（秒），如果特定的 IP 位址或連接埠符合拒絕規則的次數達到 **Security Violations Threshold**（安全性違規閾值）設定中的指定次數，就會產生警報。
違規閾值/ 違規時段/ 安全性政策規則	在 **Violations Time Period**（違規時段）欄位指定的時間內，如果規則集合達到 **Violations Threshold**（違規閾值）欄位指定的規則限制違規次數，即會產生警報。工作階段符合明確的拒絕政策時，即計入違規次數。 使用 **Security Policy Tags**（安全性政策標籤）可指定標籤，規則限制的閾值將針對這些標籤產生警報。定義安全政策時，可以指定這些頁籤。
Selective Audit	僅當防火牆處於 FIPS-CC 模式時，選擇性稽核選項才可用。 指定下列設定： • **FIPS-CC** 特定日誌記錄 — 啟用遵從一般條件 (CC) 所需要的 Verbose 日誌記錄。 • 封包丟棄日誌記錄 — 記錄防火牆丟棄的封包。 • 隱藏登入成功記錄—停止記錄管理員登入防火牆成功。 • 隱藏登入失敗記錄 — 停止記錄管理員登入防火牆失敗。 • **TLS** 工作階段日誌記錄 — 記錄 TLS 工作階段的建立。 • **CA (OCSP/CRL)** 工作階段建立日誌記錄 — 當防火牆使用線上憑證狀態通訊協定 (OCSP) 傳送檢查憑證撤銷狀態的請求或憑證撤銷清單伺服器請求時，記錄防火牆與憑證授權單位之間建立的工作階段。（預設為停用。） • **IKE** 工作階段建立日誌記錄—記錄防火牆上的 VPN 閘道驗證端點時建立的 IPSec IKE 工作階段。端點可以是 Palo Alto Networks 防火牆或用於啟動和終止 VPN 連線的其他安全性設備。日誌中指定的介面名稱是指連結至 IKE 閘道的介面。如果適用，還會顯示 IKE 閘道名稱。停用此選項會停止記錄所有 IKE 日誌記錄事件。（預設為啟用。） • 隱藏管理員 — 停止記錄所列管理者對防火牆組態做出的變更。

清除記錄

- Device > Log Settings（裝置 > 日誌設定）

在 [日誌設定] 頁面上管理日誌時，您可清除防火牆上的日誌。請按一下您要清除的日誌類型，然後按一下 **Yes**（是）以確認要求。

若要自動刪除日誌與報告，您可設定到期期間。如需詳細資訊，請參閱日誌記錄與報告設定。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔

下列主題說明您可以在防火牆上設定的伺服器設定檔設定：

- 裝置 > 伺服器設定檔 > SNMP 設陷
- 裝置 > 伺服器設定檔 > Syslog
- 裝置 > 伺服器設定檔 > 電子郵件
- 裝置 > 伺服器設定檔 > HTTP
- 裝置 > 伺服器設定檔 > NetFlow
- 裝置 > 伺服器設定檔 > RADIUS
- 裝置 > 伺服器設定檔 > TACACS+
- 裝置 > 伺服器設定檔 > LDAP
- 裝置 > 伺服器設定檔 > Kerberos
- 裝置 > 伺服器設定檔 > SAML 識別提供者
- 裝置 > 伺服器設定檔 > DNS
- 裝置 > 伺服器設定檔 > 多因素驗證

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > SNMP 設陷

簡易網路管理通訊協定 (SNMP) 是在網路上監控裝置的標準通訊協定。為了警告您系統事件或網路上的威脅，受監控的裝置會將 SNMP 設陷傳送至 SNMP 管理員（設陷伺服器）。選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **SNMP Trap**（**SNMP** 設陷）或 **Panorama** > **Server Profiles**（伺服器設定檔）> **SNMP Trap**（**SNMP** 設陷）來設定伺服器設定檔，以便啟用防火牆或 Panorama 將設陷傳送至 SNMP 管理員。若要啟用 SNMP GET 訊息（來自 SNMP 管理員的統計要求），請參閱啟用 SNMP 監控。

建立伺服器設定檔之後，您必須指定將觸發防火牆傳送 SNMP 設陷的日誌類型（裝置 > 日誌設定）。如需您必須載入至 SNMP 管理員以便其判讀設陷的 MIB 清單，請參閱支援的 MIB。

請勿刪除任何系統日誌設定或記錄設定檔會使用的伺服器設定檔。

SNMP 設陷伺服器設定檔設定	說明
名稱	輸入 SNMP 設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
版本	選取 SNMP 版本：**V2c** (預設) 或 **V3**。您的選取項目會控制對話方塊所顯示的剩餘欄位。針對任一個版本，您最多可以新增四個 SNMP 管理員。 使用 *SNMPv3*，它提供驗證和其他功能以保證網絡連線的安全。
適用於 **SNMP V2c**	
名稱	指定 SNMP 管理員的名稱。名稱最多可以包含 31 個字元，可以使用英數字元、句號、底線或連字號。
SNMP 管理員	輸入 SNMP 管理員的 FQDN 或 IP 位址。
社群	輸入社群字串以便識別 SNMP 管理員的 SNMP 社群和受監控裝置，同時也在社群成員轉送設陷期間，作為密碼以進行彼此驗證。字串最多可以包含 127 個字元，接受所有字元，且區分大小寫。 請勿使用預設社群字串（請勿將社群字串設定為 *public*（公開）或 *private*（私人））。使用唯一的社群字串，以避免在使用多個 *SNMP* 服務時發生衝突。因為 *SNMP* 訊息包含純文字的社群字串，當您定義社群成員（管理員存取）時，請考慮網路的安全性需求。
適用於 **SNMP V3**	

© 2019 Palo Alto Networks, Inc.

SNMP 設陷伺服器設定檔設定	說明
名稱	指定 SNMP 管理員的名稱。名稱最多可以包含 31 個字元，可以使用英數字元、句號、底線或連字號。
SNMP 管理員	輸入 SNMP 管理員的 FQDN 或 IP 位址。
使用者	輸入用來識別 SNMP 使用者帳戶的使用者名稱（最多 31 個字元）。您在防火牆上設定的使用者名稱必須與 SNMP 管理員上所設定的使用者名稱相符。
EngineID	指定防火牆的引擎 ID。當 SNMP 管理員和防火牆彼此驗證時，設陷訊息會使用此值來唯一識別防火牆。若您將該欄位保留空白，則訊息會使用防火牆序號作為 **EngineID**（引擎 ID）。若您輸入一個值，它必須為十六進位格式，以 0x 作為前致詞，並以其他 10-128 個字元來表示 5-64 位元組（每個位元組 2 個字元）的任何數字。針對高可用性 (HA) 的防火牆，請將該欄位保留空白，以便 SNMP 管理員可以識別傳送陷阱的 HA 端點；否則，該值會進行同步，且兩個端點將使用相同的 **EngineID**（引擎 ID）。
驗證密碼	指定 SNMP 使用者的驗證密碼。防火牆會使用該密碼來驗證 SNMP 管理員。防火牆會使用安全雜湊演算法 (SHA-1 160) 將密碼加密。密碼必須為 8-256 個字元，且允許使用所有字元。
私人密碼	指定 SNMP 使用者的私人密碼。防火牆會使用密碼和進階加密標準 (AES-128) 來加密設陷。密碼必須為 8-256 個字元，且允許使用所有字元。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > Syslog

選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **Syslog** 或 **Panorama** > **Server Profiles**（伺服器設定檔）> **Syslog** 可 設定伺服器設定檔 將防火牆、Panorama 和日誌收集器日誌當作 syslog 訊息，轉送到 syslog 伺服器。若要定義 syslog 伺服器設定檔，請按一下 **Add**（新增）並指定 [新增日誌伺服器] 欄位。

- 若要為系統、設定、*User-ID*、*HIP* 比對及關聯日誌選取 *Syslog* 伺服器設定檔，請參閱 *[裝置 > 日誌設定]*）。
- 若要為流量、威脅、*Wildfire*、*URL* 篩選、資料篩選、通道檢查、驗證和 *GTP* 日誌選取 *Syslog* 伺服器設定檔，請參閱 *[物件 > 日誌轉送]*）。
- 您無法刪除防火牆在任何系統或組態日誌設定或日誌轉送設定檔中使用的伺服器設定檔。

Syslog 伺服器設定	說明
名稱	輸入 Syslog 設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
伺服器頁籤	
名稱	按一下 **Add**（新增）並輸入 Syslog 伺服器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
伺服器	輸入系統日誌伺服器的 IP 位址或 FQDN。
Transport	選取是否透過 UDP、TCP 或 SSL 傳輸系統日誌訊息。 使用 *SSL* 進行加密以及保護傳送至系統日誌伺服器的資料。資料是透過 *UDP* 或 *TCP* 以明文形式傳送，並且在傳輸過程中是可讀的。
連接埠	輸入系統日誌伺服器的連接埠編號（UDP 的標準連接埠是 514；SSL 的標準連接埠是 6514；您必須針對 TCP 指定連接埠編號）。
格式	指定要使用的系統日誌格式：BSD（預設值）或 IETF。
裝置	選取其中一個 Syslog 標準值。選取對應 Syslog 伺服器該如何使用裝置欄位來管理訊息的值。如需裝置欄位的詳細資訊，請參閱 RFC 3164（BSD 格式）或 RFC 5424（IETF 格式）。
自訂日誌格式頁籤	
日誌類型	按一下日誌類型可開啟對話方塊，讓您指定自訂日誌格式。在對話方塊中，按一下欄位可將其新增至 [日誌格式] 區域。您可直接在 [日誌格式] 區域中編輯其他文字字串。按一下 **OK**（確定）以儲存設定。檢視每個可以用於自訂日誌 的欄位說明。

© 2019 Palo Alto Networks, Inc.

Syslog 伺服器設定	說明
	如需有關可用於自訂日誌之欄位的詳細資訊，請參閱 [裝置 > 伺服器設定檔 > 電子郵件]）。
正在逸出	指定逸出序列。**Escaped characters**（逸出的字元）是所有在無空格情況下要逸出的字元清單。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > 電子郵件

選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **Email**（電子郵件）或 **Panorama** > **Server Profiles**（伺服器設定檔）> **Email**（電子郵件），可 設定伺服器設定檔，以轉送日誌作為電子郵件通知。若要定義電子郵件伺服器設定檔，請 **Add**（新增）設定檔並指定電子郵件通知設定。

- 若要為系統、設定、*User-ID*、*HIP* 比對及關聯日誌選取電子郵件伺服器設定檔，請參閱 *[裝置 > 日誌設定]*）。
- 若要為流量、威脅、*Wildfire*、*URL* 篩選、資料篩選、通道檢查、驗證和 *GTP* 日誌選取電子郵件伺服器設定檔，請參閱 *[物件 > 日誌轉送]*）。
- 您還可以排程電子郵件報告（Monitor（監控）> PDF Reports（PDF 報告）> Email Scheduler（電子郵件排程器））
- 您無法刪除防火牆在任何「系統」或「設定日誌」設定或「日誌轉送」設定檔中使用的伺服器設定檔。

電子郵件通知設定	說明
名稱	輸入伺服器設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置 （僅限虛擬系統）	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
伺服器頁籤	
名稱	輸入用來識別伺服器的名稱（最多 31 個字元）。此欄位只是頁籤，無須成為現有電子郵件伺服器的主機名稱。
電子郵件顯示名稱	輸入顯示在電子郵件寄件者欄位中的名稱。
從	輸入寄件者電子郵件地址，例如 security_alert@company.com。
至	輸入收件人的電子郵件地址。
其他收件人	也可選取輸入其他收件人的電子郵件地址。您只能再新增一個收件人。若要新增多名收件人，請新增通訊群組清單的電子郵件地址。
電子郵件閘道	輸入傳送電子郵件的伺服器 IP 位址或主機名稱。
通訊協定	選取您要用於傳送電子郵件的通訊協定（**Unauthenticated SMTP**（未經驗證的 **SMTP**）或 **SMTP over TLS**）。
連接埠	輸入用於傳送電子郵件且與預設值不同的連接埠號（SMTP 為 25，TLS 為 587）。
TLS 版本 （僅限 SMTP over TLS）	選取您要使用的 TLS 版本（**1.2** 或 **1.1**）。

© 2019 Palo Alto Networks, Inc.

電子郵件通知設定	說明
	作為最佳實務，我們強烈建議使用最新的 *TLS* 版本。
驗證方法 （僅限 SMTP over TLS）	選取您要使用的驗證方法： • **Auto**（自動）（預設值）—允許用戶端和伺服器確定驗證方法。 • **Login**（登入）—使用者名稱和密碼使用 Base64 編碼，並將其分開傳輸。 • **Plain**（純文字）—使用者名稱和密碼使用 Base64 編碼，並將其一起傳輸。
憑證設定檔 （僅限 SMTP over TLS）	選取憑證設定檔，以便防火牆用於驗證電子郵件伺服器。
使用者名稱 （僅限 SMTP over TLS）	輸入傳送電子郵件帳戶的使用者名稱。
密碼 （僅限 SMTP over TLS）	輸入傳送電子郵件帳戶的密碼。
確認密碼 （僅限 SMTP over TLS）	確認傳送電子郵件帳戶的密碼。
測試連線 （僅限 SMTP over TLS）	確認電子郵件伺服器與防火牆之間的連線。
自訂日誌格式頁籤	
日誌類型	按一下日誌類型可開啟對話方塊，讓您指定自訂日誌格式。在對話方塊中，按一下欄位可將其新增至 [日誌格式] 區域。按一下 **OK**（確定）儲存您的變更。
正在逸出	指定不含空格的 **Escaped Characters**（逸出字元）（所有字元均不從字面上解釋），並指定 **Escape Character**（逸出字元）的逸出順序。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > HTTP

選取 **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **HTTP** 或 **Panorama** > **Server Profiles**（伺服器設定檔）> **HTTP**，可設定伺服器設定檔來轉送日誌。您可以設定防火牆，將日誌轉送至 HTTP(S) 目的地，或與任何暴露 API 的 HTTP 型的服務整合，並修改 HTTP 要求中的 URL、HTTP 標頭、參數和承載來符合您的需求。您也可以使用 HTTP 伺服器設定檔來存取執行 PAN-OS 整合式 User-ID 代理程式的防火牆，並將一個或多個頁籤註冊至防火牆所產生日誌上的來源或目的地 IP 位址。

若要使用 *HTTP* 伺服器設定檔來轉送日誌：

- 請參閱系統、設定、*User-ID*、*HIP* 配對和關聯日誌的 *[裝置 > 日誌設定]*。
- 請參閱流量、威脅、*WildFire*、*URL* 篩選、資料篩選、通道檢查、驗證和 *GTP* 日誌的 *[物件 > 日誌轉送]*。

如果是用來轉送日誌，您便無法刪除 *HTTP* 伺服器設定檔。若要刪除防火牆或 *Panorama* 上的伺服器設定檔，您必須從 *Device*（裝置）> *Log settings*（日誌設定）或 *Objects*（物件）> *Log Forwarding*（日誌轉送）設定檔刪除所有設定檔的參照。

若要定義 HTTP 伺服器設定檔，**Add**（新增）新的設定檔並在下表中設定設定。

HTTP 伺服器設定	說明
名稱	輸入伺服器設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。有效的名稱必須以英數字元開頭，且可包含零、英數字元、底線、連字號、點或空格。
位置	選取伺服器設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更**Location**（位置）。
頁籤註冊	頁籤註冊允許您在日誌項目中的來源或目的地 IP 位址新增或移除頁籤，並使用 HTTP(S) 在防火牆上將 IP 位址和頁籤對應註冊至 User-ID 代理程式。接著，您可以將使用這些頁籤的動態位址群組定義為篩選規則來決定其成員，並根據頁籤強制執行 IP 位址的原則規則。 **Add**（新增）連線詳細資料，可啟用 HTTP(S) 存取防火牆上的 User-ID 代理程式。 若要將頁籤註冊至 Panorama 上的 User-ID 代理程式，您不需要伺服器設定檔。此外，您無法使用 HTTP 伺服器設定檔將頁籤註冊至 Windows 伺服器上執行的 User-ID 代理程式。
伺服器頁籤	
名稱	**Add**（新增）HTTP(s) 伺服器並輸入名稱（最多 31 個字元）或遠端 User-ID 代理程式。有效的名稱必須是唯一的，並以英數字元開頭；且名稱可包含零、英數字元、底線、連字號、點或空格。 伺服器設定檔可以包含最多四部伺服器。
位址	輸入 HTTP(S) Server（伺服器）的 IP 位址。 針對頁籤註冊，指定設定為 User-ID 代理程式的防火牆 IP 位址。

© 2019 Palo Alto Networks, Inc.

HTTP 伺服器設定	說明
通訊協定	選取通訊協定：HTTP 或 HTTPS。
連接埠	輸入要存取伺服器或防火牆的連接埠號碼。HTTP 的預設連接埠是 80，而 HTTPS 是 443。 針對頁籤註冊，防火牆會使用 HTTP 或 HTTPS 來連線至設定為 User-ID 代理程式之防火牆上的 Web 伺服器。
TLS 版本	選取伺服器上的 SSL 支援的 TLS 版本。預設值為 **1.2**。
憑證設定檔	選取憑證設定檔以用於與伺服器建立 TLS 連線。 在建立與伺服器的安全連線時，防火牆牆使用指定的憑證設定檔驗證伺服器憑證。
HTTP 方法	選取伺服器支援的 HTTP 方法。選項為 GET、PUT、POST（預設值）和 DELETE。 針對 User-ID 代理程式，請使用 GET 方法。
使用者名稱	輸入具有存取權限可完成您所選取之 HTTP 方法的使用者名稱。 如果您要將頁籤註冊至防火牆上的 User-ID 代理程式，必須為具有超級使用者角色之管理員的使用者名稱。
密碼	輸入密碼以驗證伺服器或防火牆。
測試伺服器連線	選取伺服器並 **Test Server Connection**（測試伺服器連線）以測試伺服器的網路連線。 此測試不會測試執行 User-ID 代理程式之伺服器的網路連線。
承載格式頁籤	
日誌類型	隨即顯示適用於 HTTP 轉送的日誌類型。按一下日誌類型可開啟對話方塊，讓您指定自訂日誌格式。
格式	顯示日誌類型是使用預設格式、預先定義格式還是您所定義的自訂承載格式。
預先定義的格式	選取服務或廠商傳送日誌的格式。預先定義格式會透過內容更新推送，並可在您每次於防火牆或 Panorama 上安裝新的內容更新時加以變更。
名稱	輸入自訂日誌格式的名稱。
URI 格式	指定您要使用 HTTP(S) 傳送日誌的資源。 如果您建立自訂格式，**URI** 會是 HTTP 服務上的資源端點。防火牆會將 URI 附加至您稍早定義的 IP 位址，以建構 HTTP 要求的 URL。請確保 URI 與承載格式符合您第三方廠商要求的語法。您可以在 HTTP 標頭、Parameter 和值配對內，使用選取的日誌類型上支援的任何屬性及要求承載。
HTTP 標頭	新增標頭及其對應的值。
參數	包含選用參數和值。

© 2019 Palo Alto Networks, Inc.

HTTP 伺服器設定	說明
酬載	選取您要在 HTTP 訊息中包含作為至外部 Web 伺服器承載的日誌屬性。
傳送測試日誌	按一下此按鈕可驗證外部 Web 伺服器以正確的承載格式接收到要求。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > NetFlow

Palo Alto Networks 防火牆可在其介面上將 IP 流量相關的統計資料匯出，如 NetFlow 欄位至 NetFlow 收集器。NetFlow 收集器是您用於分析網路流量的伺服器，可滿足安全性、管理、會計與疑難排解等用途。所有 Palo Alto Networks 防火牆都支援 NetFlow 第 9 版。防火牆僅支援單向 NetFlow，而非雙向。防火牆會執行介面所有 IP 封包上的 NetFlow 處理，且不支援範例 NetFlow。您可以將第三層、第二層、虛擬介接、旁接、VLAN、回送及通道介面的 NetFlow 記錄匯出。針對彙總乙太網路介面，您可以將彙總群組的記錄匯出，但不能將群組內的個別介面匯出。防火牆支援標準與企業（PAN-OS 特定）NetFlow 範本，可供 NetFlow 收集者用來解譯 NetFlow 欄位。防火牆會根據匯出的資料類型來選取範本：IPv4 或 IPv6 流量，含或不含 NAT，以及含標準或企業特定的欄位。

若要設定 NetFlow 匯出，請 **Add**（新增）NetFlow 伺服器設定檔，以指定接收匯出資料並指定匯出參數的 NetFlow 伺服器。將設定檔指派至介面（請參閱 [網路 > 介面]）後，防火牆會將該介面上所有流量的 NetFlow 資料匯出至指定伺服器。

Netflow 設定	說明
名稱	輸入 NetFlow 設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
範本重新整理速率	防火牆會定期重新整理 NetFlow 範本以重新評估要使用哪個範本（以免匯出資料的類型變更），並將任何變更套用至所選範本中的欄位。根據 NetFlow 收集器的需求，以 **Minutes**（分鐘數）（範圍是 1 到 3,600；預設值是 30）和 **Packets**（封包數）（匯出的記錄—範圍是 1 到 600；預設值是 20）指定防火牆重新整理的速率。防火牆會在任何閾值通過後重新整理範本。需要的重新整理速率視 NetFlow 收集器而定。若將多個 NetFlow 收集器新增至伺服器設定檔，請使用具有最快重新整理速率的收集器值。
主動式逾時	以分鐘為單位，指定防火牆匯出每個工作階段的資料記錄所使用的頻率（範圍是 1 到 60；預設值是 5）。根據您要 NetFlow 收集器用來更新流量統計資料的頻率，以設定頻率。
PAN-OS 欄位類型	針對 NetFlow 記錄中的 App-ID 與 User-ID 匯出 PAN-OS 特定欄位。
伺服器	
名稱	指定用來識別伺服器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
伺服器	指定伺服器的主機名稱或 IP 位址。每個設定檔最多可以新增 2 個伺服器。
連接埠	指定伺服器存取的埠號（預設值是 2055）。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > RADIUS（裝置 > 伺服器設定檔 > RADIUS）

選取 **Device**（設備）> **Server Profiles**（伺服器設定檔）> **RADIUS** 或 **Panorama** > **Server Profiles**（伺服器設定檔）> **RADIUS** 可 進行設定 驗證設定檔參考的遠端驗證撥入使用者服務 (RADIUS) 伺服器（請參閱 Device（裝置）> Authentication Profile（驗證設定檔））。您可以使用 RADIUS 來驗證存取您網路資源的使用者（透過 GlobalProtect 或驗證入口網站）、驗證在防火牆或 Panorama 上本機定義的管理員，以及驗證並授權在 RADIUS 伺服器上外部定義的管理員。

RADIUS 伺服器設定	說明
設定檔名稱	輸入用來識別伺服器設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
僅限管理員使用	選取此選項以指定僅管理員帳戶可使用驗證的設定檔。針對具有多個虛擬系統的防火牆，此選項僅在 **Location**（位置）為 **Shared**（共用）時才會顯示。
逾時	輸入一個 間隔時間（單位為秒），超過此時間後，驗證要求將逾時（範圍是 1-120；預設值為 3）。 如果您是使用 *RADIUS* 伺服器設定檔將防火牆與 *MFA* 服務整合，請輸入可讓使用者有足夠時間回應驗證挑戰的間隔。例如，如果 *MFA* 服務提示輸入一次性密碼 *(OTP)*，使用者需要時間才能在其端點設備上看到 *OTP*，然後在 *MFA* 登入頁面中輸入 *OTP*。
驗證通訊協定	選取防火牆用來保護 RADIUS 伺服器連線安全的 **Authentication Protocol**（驗證通訊協定）： • **PEAP-MSCHAPv2**—（預設）受保護的 EAP (PEAP) 與 Microsoft Challenge-Handshake 驗證通訊協定 (MSCHAPv2) 透過在加密通道中傳輸使用者名稱和密碼，可在 PAP 或 CHAP 上提供改良的安全性。 • **PEAP 附 GTC**—選擇受保護的 EAP（PEAP)）與通用令牌（GTC）以在加密通道中使用一次性權杖。 • **EAP-TTLS 附 PAP**—選擇 EAP 與通道傳輸層安全性協定（TTLS）與 PAP 以在加密通道中為 PAP 傳輸純文字認證。 • **CHAP**—若 RADIUS 伺服器不支援 EAP 或 PAP 且未針對其進行設定，則選取 Challenge-Handshake 驗證通訊協定（CHAP）。 • **PAP**—若 RADIUS 伺服器不支援 EAP 或 CHAP 且未針對其進行設定，則選取密碼驗證通訊協定 (PAP)。
允許使用者在逾期後變更密碼	（PEAP-MSCHAPv2 附 GlobalProtect 4.1 或之後版本）選取此選項以允許 GlobalProtect 使用者變更逾期的密碼。

© 2019 Palo Alto Networks, Inc.

RADIUS 伺服器設定	說明
使外部身分匿名	（PEAP-MSCHAPv2、PEAP 附 GTC 或 EAP-TTLS 附 PAP）此選項預設為啟用，以讓使用者在防火牆以伺服器驗證後建立的外部通道中可以匿名身份。 有些 *RADIUS* 伺服器設定也許無法支援匿名的外部 *ID*，且您也許需要清除此選項。在清除時，使用者名稱以純文字傳送。
憑證設定檔	（PEAP-MSCHAPv2、PEAP 附 GTC 或 EAP-TTLS 附 PAP）選擇或設定憑證設定檔以與 RADIUS 伺服器設定檔相關聯。防火牆會使用 Certificate Profile（憑證設定檔）來向 RADIUS 伺服器驗證身份。
重試次數	指定逾時後重試的次數（範圍是 1–5；預設值為 3）。
伺服器	依偏好順序設定每部伺服器的資訊。 • 名稱—輸入用來識別伺服器的名稱。 • **RADIUS Server**（**RADIUS** 伺服器）—輸入伺服器 IP 位址或 FQDN。 • **Secret/Confirm Secret**（密碼/確認密碼）—輸入與確認金鑰，以驗證及加密防火牆與 RADIUS 伺服器之間的連線。 • **Port**（連接埠）—輸入驗證要求的伺服器連接埠（範圍是 1–65,535；預設值為 1812）。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > TACACS+（裝置 > 伺服器設定檔 > TACACS+）

選取 **Device**（設備）> **Server Profiles**（伺服器設定檔）> **TACACS+** 或 **Panorama** > **Server Profiles**（伺服器設定檔）> **TACACS+** 可 進行設定，定義防火牆或 Panorama 如何連線至終端機存取控制器存取控制系統 Plus (TACACS+) 伺服器（請參閱 Device（裝置）> Authentication Profile（驗證設定檔））。您可以使用 TACACS+ 來驗證存取您網路資源的使用者（透過 GlobalProtect 或驗證入口網站）、驗證在防火牆或 Panorama 上本機定義的管理員，以及驗證並授權在 TACACS+ 伺服器上外部定義的管理員。

TACACS+ 伺服器設定	說明
設定檔名稱	輸入用來識別伺服器設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
僅限管理員使用	選取此選項以指定僅管理員帳戶可使用驗證的設定檔。針對多個 VSYS 防火牆，此選項僅在 **Location**（位置）為 **Shared**（共用）時才會顯示。
逾時	輸入驗證要求將於一定間隔後逾時的秒數（範圍是 1-20；預設為 3）。
驗證通訊協定	選取防火牆用來保護 TACACS+ 伺服器連線的 **Authentication Protocol**（驗證通訊協定）： • **CHAP**—Challenge-Handshake 驗證通訊協定 (CHAP) 是預設及優先使用的通訊協定，因為它比 PAP 更安全。 • **PAP**—若 TACACS+ 伺服器不支援 CHAP 或未針對其進行設定，則選取密碼驗證通訊協定 (PAP)。 • **Auto**（自動）—防火牆會先使用 CHAP 來嘗試驗證。若 TACACS+ 伺服器沒有回應，則防火牆會回復使用 PAP。
使用單一連線來進行所有驗證	選取此選項以針對所有驗證使用相同的 TCP 工作階段。此選項可透過避免需要啟動程序並針對每個驗證事件卸除個別 TCP 工作階段來改善效能。
伺服器	按一下 **Add**（新增）可指定下列每個 TACACS+ 伺服器的設定： • 名稱—輸入用來識別伺服器的名稱。 • **TACACS+ Server**（**TACACS+** 伺服器）—輸入 TACACS+ 伺服器的 IP 位址或 FQDN。 • **Secret/Confirm Secret**（密碼/確認密碼）—輸入與確認金鑰，以驗證及加密防火牆與 TACACS+ 伺服器之間的連線。 • **Port**（連接埠）—輸入驗證要求的伺服器連接埠（預設為 49）。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > LDAP（裝置 > 伺服器設定檔 > LDAP）

- **Device**（裝置）> **Server Profiles**（伺服器設定檔）> **LDAP**
- **Panorama** > **Server Profiles**（伺服器設定檔）> **LDAP**

Add（新增）或選取 LDAP 伺服器設定檔以進行設定驗證設定檔參考的輕量型目錄存取協定 (LDAP) 伺服器（請參閱 Device（裝置）> Authentication Profile（驗證設定檔））。您可以使用 LDAP 來驗證存取您網路資源的使用者（透過 GlobalProtect 或驗證入口網站），以及在防火牆或 Panorama 上本機定義的管理員。

LDAP 伺服器設定	說明
設定檔名稱	輸入用來識別設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
僅限管理員使用	選取此選項以指定僅管理員帳戶可使用驗證的設定檔。針對具有多個虛擬系統的防火牆，此選項僅在 **Location**（位置）為 **Shared**（共用）時才會顯示。
使用此設定檔進行序號檢查	選取此選項以啟用此 LDAP 伺服器設定檔以從管理的端點收集序號。GlobalProtect 入口網站以及閘道使用此資訊來驗證端點是否受到管理（序號是否存在於 Active Directory 中）。
伺服器清單	針對每個 LDAP 伺服器，**Add**（新增）一個主機 **Name**（名稱）、IP 位址或 FQDN（**LDAP Server**（**LDAP** 伺服器）），以及 **Port**（連接埠）（預設為 389）。 設定至少兩個 *LDAP* 伺服器以提供備援。
類型	從下拉式清單中選取伺服器。
基礎 DN	在目錄伺服器中指定根內容，以縮小搜尋使用者或群組資訊的範圍。
繫結 DN	為目錄伺服器指定登入名稱（辨別名稱）。 繫結 *DN* 帳戶須具有讀取 *LDAP* 目錄的權限。
密碼/確認密碼	指定連結帳戶密碼。代理程式會將加密的密碼儲存在設定檔案中。
繫結逾時	指定連線至目錄伺服器時強制使用的時間限制（以秒為單位，範圍是 1 到 30；預設為 30）。

© 2019 Palo Alto Networks, Inc.

LDAP 伺服器設定	說明
搜尋逾時	指定執行目錄搜尋時強制使用的時間限制（以秒為單位，範圍是 1 到 30；預設為 30）。
重試間隔	指定在上一次失敗嘗試之後，系統將於多久間隔秒數之後再嘗試連線至 LDAP 伺服器（範圍是 1 到 3,600；預設為 60）。
要求 SSL/TLS 安全連線	若您要讓防火牆使用 SSL 或 TLS 與目錄伺服器進行通訊，請選取此選項。通訊協定取決於伺服器連接埠： • 389（預設值）—TLS（特別是防火牆會使用開始 TLS 操作，用來升級連接至 TLS 的初始純文字連線。） • 636—SSL • 任何其他連接埠—防火牆首先會嘗試使用 TLS。若目錄伺服器不支援 TLS，則防火牆會回復使用 SSL。 此選項是最佳做法，因為它提高了安全性並且在預設情況下選取。
驗證 SSL 工作階段的伺服器憑證	若您要防火牆驗證目錄伺服器所顯示 SSL/TLS 連線的憑證，請選取此選項（依預設為清除）。防火牆會從兩個方面來驗證憑證： • 憑證為受信任且有效。若要讓防火牆信任憑證，其根憑證授權單位 (CA) 和任何中繼憑證必須位於 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）下方的憑證存放區。 • 憑證名稱必須符合 LDAP 伺服器的主機 **Name**（名稱）。防火牆首先會檢查憑證屬性「Subject AltName」以進行比對，然後嘗試屬性「Subject DN」。若憑證使用目錄伺服器的 FQDN，您必須使用 **LDAP Server**（LDAP 伺服器）欄位中的 FQDN 進行名稱比對才能成功驗證。 若驗證失敗，則連線也會失敗。若要啟用此驗證，您也必須選取 **Require SSL/TLS secured connection**（要求 **SSL/TLS** 安全連線）。 啟用防火牆以為 *SSL* 階段驗證伺服器憑證來提高安全性。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > Kerberos（裝置 > 伺服器設定檔 > Kerberos）

選取 **Device**（設備）> **Server Profiles**（伺服器設定檔）> **Kerberos** 或 **Panorama** > **Server Profiles**（伺服器設定檔）> **Kerberos** 來 設定伺服器設定檔，以便讓使用者原生驗證 Active Directory 網域控制站或 Kerberos V5 相容的驗證伺服器。設定 Kerberos 伺服器設定檔後，您可以將它指派至驗證設定檔（請參閱 Device（裝置）> Authentication Profile（驗證設定檔））。您可以使用 Kerberos 來驗證存取您網路資源的使用者（透過 GlobalProtect 或驗證入口網站），以及在防火牆或 Panorama 上本機定義的管理員。

若要使用 *Kerberos* 驗證，您的後端 *Kerberos* 伺服器必須可在 *IPv4* 位址上進行存取。不支援 *IPv6* 位址。

Kerberos 伺服器設定	說明
設定檔名稱	輸入用來識別伺服器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
僅限管理員使用	選取此選項以指定僅管理員帳戶可使用驗證的設定檔。針對具有多個虛擬系統的防火牆，此選項僅在 **Location**（位置）為 **Shared**（共用）時才會顯示。
伺服器	針對每個 Kerberos 伺服器，請按一下 **Add**（新增），並指定下列設定： • **Name**（名稱）—輸入伺服器的名稱。 • **Kerberos Server**（**Kerberos** 伺服器）—輸入伺服器 IPv4 位址或 FQDN。 • **Port**（連接埠）—輸入選擇性埠號（範圍是 1 到 65,535；預設為 88），用來與伺服器進行通訊。

© 2019 Palo Alto Networks, Inc.

Device > Server Profiles > SAML Identity Provider（裝置 > 伺服器設定檔 > SAML 識別提供者）

使用此頁面註冊安全性聲明標記語言 (SAML) 2.0 識別提供者 (IdP) 與防火牆或 Panorama。註冊是讓防火牆或 Panorama 作為 SAML 服務提供者運作的必要步驟，其可控制您網路資源的存取。當管理員與一般使用者要求資源時，服務提供者會將使用者重新導向至 IdP 以進行驗證。使用者可為 GlobalProtect 或驗證入口網站使用者。管理員可在防火牆和 Panorama 上本機管理，或在 IdP 識別存放中外部管理。您可以設定 SAML 單一登入 (SSO)，以便每個使用者在登入後可自動存取多個資源。您也可以設定 SAML 單一登出 (SLO)，以便每個使用者可透過登出任何單一服務，同時登出每個啟用 SSO 的服務。

驗證順序不支援指定 *SAML IdP* 伺服器設定檔的驗證設定檔。

在大部分情況下，您無法使用 *SSO* 在相同的行動設備上存取多個應用程式。

您無法為驗證入口網站使用者啟用 *SLO*。

建立 SAML IdP 伺服器設定檔最簡單的方式是 **Import**（匯出）包含來自 IdP 之註冊資訊的中繼資料檔案。儲存具有匯入值的伺服器設定檔後，您可以編輯設定檔來修改值。如果 IdP 不提供中繼資料檔案，您可以 **Add**（新增）伺服器設定檔，並手動輸入資訊。建立伺服器設定檔之後，將它指派給驗證設定檔（請參閱 [設備 > 驗證設定檔]）以取得特定防火牆或 Panorama 服務。

SAML 識別提供者伺服器設定	說明
設定檔名稱	輸入用來識別伺服器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取設定檔可用的範圍。在具有多個虛擬系統的防火牆內容中，選取一個虛擬系統或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存設定檔之後，您無法變更其位置。
僅限管理員使用	選取此選項以指定僅管理員帳戶可使用驗證的設定檔。針對具有多個虛擬系統的防火牆，此選項僅在 **Location**（位置）為 **Shared**（共用）時才會顯示。
識別提供者 ID	為 IdP 輸入識別碼。IdP 會提供此資訊。
識別提供者憑證	選取 IdP 用來簽署傳送至防火牆之 SAML 訊息的憑證。您必須選取 IdP 憑證，以確保 IdP 傳送至防火牆之訊息的完整性。若要針對頒發 Certificate Authority (憑證授權單位 - CA) 驗證 IdP 憑證，您必須在任何參考 IdP 伺服器設定檔的驗證設定檔中指定 **Certificate Profile**（憑證設定檔）（請參閱 [裝置 > 驗證設定檔]）。 當您在產生或匯入憑證及其相關聯的私密金鑰時，請記得，憑證中所指定的金鑰使用屬性會控制您金鑰的用途。如果憑證明確列出金鑰使用屬性，則其中一個屬性必須是 [數位簽章]，而您在防火牆上產生的憑證中並無此屬性。在此情況下，您必須從您的企業憑證授權單位 (CA) 或第三方 CA 匯出憑證和金鑰。如果憑證未指定金鑰使用屬性，則您可以將金鑰用於任何用途，包括簽署訊息。在此情況下，您可以使用任何方法來取得憑證和金鑰，以簽署 SAML 訊息。 IdP 憑證支援下列演算法：

© 2019 Palo Alto Networks, Inc.

SAML 識別提供者伺服器設定	說明
	• 公開金鑰演算法—RSA（1,024 位元以上）和 ECDSA（所有大小）。FIPS/CC 模式下的防火牆支援 RSA（2,048 位元以上）和 ECDSA（所有大小）。 • 簽署演算法—SHA1、SHA256、SHA384 和 SHA512。FIPS/CC 模式下的防火牆支援 SHA256、SHA384 和 SHA512。
識別提供者 SSO URL	輸入 IdP 為單一登入 (SSO) 服務所公告的 URL。 如果您透過匯入中繼資料檔案來建立伺服器設定檔，且檔案指定多個 SSO URL，防火牆會使用指定 POST 或重新導向繫結方法的第一個 URL。 *Palo Alto Networks 強烈建議您使用依賴於 HTTPS 的 URL，雖然 SAML 也支援 HTTP。*
識別提供者 SLO URL	輸入 IdP 為單一登出 (SLO) 服務所宣告的 URL。 如果您透過匯入中繼資料檔案建立服務設定檔，且檔案指定多個 SLO URL，防火牆會使用指定 POST 或重新導向繫結方法的第一個 URL。 *Palo Alto Networks 強烈建議您使用依賴於 HTTPS 的 URL，雖然 SAML 也支援 HTTP。*
SSO SAML HTTP 繫結	選取與 **Identity Provider SSO URL**（識別提供者 **SSO URL**）相關聯的 HTTP 繫結。防火牆會使用繫結將 SAML 訊息傳送至 IdP。選項包括： • **POST**—防火牆會使用以 base64 編碼的 HTML 格式傳送訊息。 • 重新導向—防火牆會在 URL 參數內傳送以 base64 編碼和以 URL 編碼的 SSO 訊息。 *如果您匯入具有多個 SSO URL 的 IdP 中繼資料檔案，防火牆會使用第一個 URL 的繫結，其使用 POST 或重新導向方法。防火牆會忽略使用其他繫結的 URL。*
SLO SAML HTTP 繫結	選取與 **Identity Provider SLO URL**（識別提供者 **SLO URL**）相關聯的 HTTP 繫結。防火牆會使用繫結將 SAML 訊息傳送至 IdP。選項包括： • **POST**—防火牆會使用以 base64 編碼的 HTML 格式傳送訊息。 • 重新導向—防火牆會在 URL 參數內傳送以 base64 編碼和以 URL 編碼的 SSO 訊息。 *如果您匯入具有多個 SLO URL 的 IdP 中繼資料檔案，防火牆會使用第一個 URL 的繫結，其使用 POST 或重新導向方法。防火牆會忽略使用其他繫結的 URL。*
識別提供者中繼資料	僅在您從 IdP 上載至防火牆的 IdP 中繼資料檔案 **Import**（匯入）時，才會顯示此欄位。檔案會指定值與新 SAML IdP 伺服器設定檔的簽署憑證。**Browse**（瀏覽）至檔案、指定設定檔名稱及時鐘誤差上限，然後按一下 **OK**（確定）以建立設定檔。您可以選擇性地編輯設定檔以變更匯入的值。
驗證識別提供者憑證	選取此選項以驗證信任鏈以及 IdP 簽署憑證的吊銷狀態（選用）。

© 2019 Palo Alto Networks, Inc.

SAML 識別提供者伺服器設定	說明
	要啟用此選項，憑證授權單位 (CA) 必須簽發您的 IdP 簽署憑證。您必須建立擁有具有簽發 IdP 簽署憑證的 CA 憑證設定檔。在 Authentication Profile（驗證設定檔）中，選取 SAML 伺服器設定檔和憑證設定檔以驗證 IdP 憑證（請參閱 [裝置 > 驗證設定檔]）。 如果您的 IdP 簽署憑證為自我簽署憑證，則沒有信任鏈；因此，您無法啟用此選項。防火牆始終會根據您設定的識別提供者憑證來驗證 SAML 回應或聲明的簽名，無論您是否啟用**Validate Identity Provider Certificate**（驗證識別提供者憑證）選項。如果您的 IdP 提供自我簽署憑證，請確保您使用 PAN-OS 10.0，以減少對 CVE-2020-2021 的接觸。
簽署 SAML 訊息至 IdP	選取此選項可指定傳送至 IdP 的防火牆簽署訊息。防火牆會使用您在憑證設定檔中指定的 **Certificate for Signing Requests**（用於簽署要求的憑證）（請參閱 [設備 > 驗證設定檔]）。 使用簽署憑證可確保傳送至 *IdP* 之訊息的完整性。
時鐘誤差上限	當防火牆驗證其從 IdP 接收到的訊息（範圍是 1 到 900；預設值為 60）時，輸入 IdP 與防火牆系統時間之間的可接受時間差距上限（以秒為單位）。如果時間差距超過此值，則驗證 (validation)（也因此驗證 (authentication)）會失敗。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > DNS

若要簡化虛擬系統的設定，DNS 伺服器設定檔可讓您指定所要設定的虛擬系統、繼承來源或 DNS 伺服器的主要與次要 DNS 位址，以及用於傳送至 DNS 伺服器之封包中的來源介面和來源位址（服務路由）來源介面和來源位址會用作為從 DNS 伺服器回覆的目的地介面和目的地位址。

DNS 伺服器設定檔僅供虛擬系統使用；而非全域 [共用] 位置。

DNS 伺服器設定檔設定	說明
名稱	命名 DNS 伺服器設定檔
位置	選取設定檔所套用的虛擬系統。
繼承來源	若 DNS 伺服器位址並未繼承時，請選取 **None**（無）。否則，請指定設定檔應繼承設定的 DNS 伺服器。
檢查繼承狀態	按一下以查看繼承來源資訊。
主要 DNS	指定主要 DNS 伺服器的 IP 位址。
次要 DNS	指定次要 DNS 伺服器的 IP 位址。
伺服器路由 IPv4	若您要指定讓封包傳送至以 IPv4 位址為來源的 DNS 伺服器，請按一下此選項。
來源介面	指定來源介面，以便讓封包傳送至要使用的 DNS 伺服器。
來源位址	指定 IPv4 來源位址，即封包傳送至以 IPv4 位址為來源的 DNS 伺服器。
伺服器路由 IPv6	若您要指定讓封包傳送至以 IPv6 位址為來源的 DNS 伺服器，請按一下此選項。
來源介面	指定來源介面，以便讓封包傳送至要使用的 DNS 伺服器。
來源位址	指定 IPv6 來源位址，即封包傳送至以 IPv6 位址為來源的 DNS 伺服器。

© 2019 Palo Alto Networks, Inc.

裝置 > 伺服器設定檔 > 多因素驗證

使用此頁面可設定多因素驗證 (MFA) 伺服器設定檔，能定義防火牆連線至 MFA 伺服器的方式。MFA 可以保護您最機密的資源，方法是確保攻擊者無法存取您的網路，並洩露單一驗證因素（例如，竊取登入認證）來橫式移過。設定此伺服器設定檔後，將它指派給要求驗證之服務的驗證設定檔（請參閱 [設備 > 驗證設定檔]）。

對於下列驗證用例，防火牆整合使用 RADIUS 和 SAML 的多重因子驗證（MFA）廠商：

- 遠端使用者透過 GlobalProtect™ 入口網站和閘道進行驗證。
- 管理員在 PAN-OS 和 Panorama™ 網路介面內進行驗證。
- 透過驗證政策進行驗證。

另外，防火牆還可以使用 API 整合 MFA vendors（MFA 廠商）以透過只限終端使用者驗證的驗證政策強制執行 MFA。

設定 *MFA* 的完整程序 除了建立伺服器設定檔以外，還需要其他工作。

驗證順序不支援指定 *MFA* 伺服器設定檔的驗證設定檔。

如果防火牆透過 *RADIUS* 與您的 *MFA* 廠商整合，請設定 *RADIUS* 伺服器設定檔（請參閱 *[設備 > 伺服器設定檔 > RADIUS]*）。防火牆透過 *RADIUS* 支援所有的 *MFA* 廠商。

MFA 伺服器設定	說明
設定檔名稱	輸入用來識別伺服器的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	在具有一個以上虛擬系統 (VSYS) 的防火牆上，選取一個 VSYS 或 **Shared**（共用）位置。儲存設定檔之後，您就無法變更其 **Location**（位置）。
憑證設定檔	選取 **Certificate Profile**（憑證設定檔），可指定設定伺服器安全連線時，防火牆會用來驗證 MFA 伺服器的憑證授權單位 (CA) 憑證。如需詳細資訊，請參閱 [設備 > 憑證管理 > 憑證設定檔]）。

MFA 廠商/值	選取 MFA 廠商 **MFA 廠商**，並為每個廠商屬性輸入 **Value**（值）。屬性會依廠商而有所不同。請參考廠商文件以取得正確的值。
	• **Duo v2**：
	  • **API Host**—Duo v2 伺服器的主機名稱。
	  • **Integration Key**（整合金鑰）與 **Secret Key**（密碼金鑰）—防火牆會使用這些金鑰來驗證 Duo v2 伺服器，並簽署傳送至伺服器的驗證要求。為保護這些金鑰，防火牆上的主要金鑰會自動將它們加密，以便其純文字值不會暴露在防火牆儲存設備中的任何位置。聯絡您的 Duo v2 管理員可取得金鑰。
	  • 逾時—以秒為單位輸入時間，在此時間後，防火牆在嘗試與 **API Host**（**API** 主機）通訊時就會逾時（範圍是 5 到 600；預設值為 30）。此間隔必須比 API 主機與使用者的端點設備之間的逾時還要長。
	  • 基礎 **URI**—如果貴組織主控 Duo v2 伺服器的本機驗證 代理程式 伺服器，請輸入 代理程式 伺服器 URI (預設為 /auth/v2)。
	• **Okta Adaptive**：
	  • **API 主機**—Okta 伺服器的主機名稱。

© 2019 Palo Alto Networks, Inc.

MFA 伺服器設定	說明
	• 基礎 **URI**—如果貴組織主控 Okta 伺服器的本機驗證 代理程式 伺服器，請輸入 代理程式 伺服器 URI (預設為 /api/v1)。 • 語彙基元—防火牆會使用此語彙基元來驗證 Okta 伺服器，並指派傳送至伺服器的驗證要求。為保護語彙基元，防火牆上的主要金鑰會自動將其加密，以便其純文字值不會暴露在防火牆儲存設備中的任何位置。聯絡您的 Okta 管理員可取得語彙基元。 • 組織—貴組織在 **API Host**（**API** 主機）中的子網域。 • 逾時—以秒為單位輸入時間，在此時間後，防火牆在嘗試與 **API Host**（**API** 主機）通訊時就會逾時（範圍是 5 到 600；預設值為 30）。此間隔必須比 API 主機與使用者的端點設備之間的逾時還要長。 • **PingID**： • 基礎 **URI**—如果貴組織主控 PingID 伺服器的本機驗證 代理程式 伺服器，請輸入 代理程式 伺服器 URI (預設為 /pingid/rest/4)。 • 主機名稱—輸入 PingID 伺服器的主機名稱（預設為 idpxnyl3m.pingidentity.com）。 • 使用 **Base64** 金鑰和語彙基元—防火牆會使用金鑰和語彙基元來驗證 PingID 伺服器，並指派傳送至伺服器的驗證要求。為保護金鑰和語彙基元，防火牆上的主要金鑰會自動將它們加密，以便其純文字值不會暴露在防火牆儲存設備中的任何位置。聯絡您的 PingID 管理員可取得值。 • **PingID** 用戶端組織 **ID**—貴組織的 PingID 識別碼。 • 逾時—輸入時間（以秒為單位），在此時間後，防火牆在嘗試與 **Host name**（主機名稱）欄位中指定的 PingID 伺服器通訊時就會逾時（範圍是 5 到 600；預設值為 30）。此間隔必須比 PingID 主機與使用者的端點設備之間的逾時還要長。

© 2019 Palo Alto Networks, Inc.

裝置 > 本機使用者資料庫 > 使用者

您可以在防火牆上設定本機資料庫，以便儲存防火牆管理員、驗證入口網站使用者，以及對 GlobalProtect 入口網站和 GlobalProtect 閘道進行驗證之使用者的驗證資訊。本機資料庫驗證不需要外部驗證服務；您可在防火牆上執行所有帳戶管理。建立本機資料庫並（選用）將使用者指派給群組後（請參閱 Device（裝置）> Local User Database（本機使用者資料庫）> User Groups（使用者群組）），您可以根據本機資料庫 Device（裝置）> Authentication Profile（驗證設定檔）。

您無法設定使用本機資料庫驗證之管理員帳戶的 *[設備 > 密碼設定檔]*。

若要將一般使用者 **Add**（新增）至資料庫，請設定下表中所述的設定。

本機使用者設定	說明
名稱	輸入用來識別使用者的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取使用者帳戶可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存使用者帳戶之後，您無法變更其位置。
模式	使用此欄位來指定驗證選項： • 密碼 — 輸入並確認使用者的密碼。 • **Password Hash**（密碼雜湊）—輸入雜湊的密碼字串。例如，如果您想要重複使用現有 Unix 帳戶的認證，但不知道純文字密碼，只知道雜湊的密碼，那麼此選項很有用。防火牆會接受最多 63 個字元的任何字串，無論用來產生雜湊值的演算法為何。當防火牆為一般模式時，操作 CLI 命令 **`request password-hash password`** 會使用 MD5 演算法，而當防火牆為 CC/FIPS 模式時，會使用 SHA256 演算法。 您針對防火牆設定的任何最低密碼複雜度 參數（*Device*（設備）> *Setup*（設定）> *Management*（管理））不會套用於使用 *Password Hash*（密碼雜湊）的帳戶。
啟用	選取此選項可啟動使用者帳戶。

© 2019 Palo Alto Networks, Inc.

裝置 > 本機使用者資料庫 > 使用者群組

選取 **Device**（設備） > **Local User Database**（本機使用者資料庫） > **User Groups**（使用者群組） 可將使用者群組資訊新增至本機資料庫。

本機使用者群組設定	說明
名稱	輸入用來識別群組的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	選取使用者群組可用的範圍。在具有一個以上虛擬系統 (VSYS) 的防火牆內容中，選取一個 VSYS 或選取 **Shared**（共用）（所有虛擬系統）。在其他任何內容中，您無法選取 **Location**（位置）；它的值已預先設定為 [共用]（防火牆）或 Panorama。儲存使用者群組之後，您就無法變更其 **Location**（位置）。
所有本機使用者	按一下 **Add**（新增）可選取您要新增到群組的使用者。

© 2019 Palo Alto Networks, Inc.

裝置 > 已排程的日誌匯出

您可以排程日誌的匯出，並將它們以 CSV 格式儲存到檔案傳輸通訊協定 (FTP) 伺服器中，或使用安全複本 (SCP) 在防火牆與遠端主機之間安全傳輸資料。日誌設定檔包含排程與 FTP 伺服器資訊。例如，設定檔可以指定於每天凌晨 3 點收集前一天的日誌，並將其儲存在特殊 FTP 伺服器中。

按一下 **Add**（新增）並填寫下列詳細資料：

排程日誌匯出設定	說明
名稱	輸入用來識別設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 建立設定檔之後，無法變更名稱。
說明	輸入選擇性說明（最多 255 個字元）。
啟用	選取此選項可啟用日誌匯出的排程。
日誌類型	選擇日誌類型（**traffic**、**threat**、**gtp**、**sctp**、**tunnel**、**userid**、**auth**、**url**、**data**, **hipmatch** 或 **wildfire**）。預設為流量。
排程匯出開始時間（每日）	使用 24 小時制輸入每天開始匯出的時間 (hh:mm) (00:00 - 23:59)。
通訊協定	選取要用於將日誌從防火牆匯出至遠端主機的通訊協定： • **FTP**—此通訊協定不具有安全性。 • **SCP**—此通訊協定具有安全性。完成剩餘的欄位後，必須按一下 **Test SCP server connection**（測試 **SCP** 伺服器連線）來測試防火牆與 SCP 伺服器之間的連線，且必須確認及接受 SCP 伺服器的主機金鑰。
主機名稱	輸入將用於匯出之 FTP 伺服器的主機名稱或 IP 位址。
連接埠	輸入 FTP 伺服器將會使用的埠號。預設為 21。
path	指定位於將用來儲存匯出資訊之 FTP 伺服器上的路徑。
啟用 FTP 被動模式	選取此選項可使用被動模式來進行匯出。依照預設，會選取此選項。
使用者名稱	輸入用來存取 FTP 伺服器的使用者名稱。預設為 anonymous。
密碼/確認密碼	輸入用來存取 FTP 伺服器的密碼。如果使用者為匿名，則不需要密碼。
測試 SCP 伺服器連線 (僅限 SCP 通訊協定)	如果您將 **Protocol**（通訊協定）設為 **SCP**，則必須按一下按鈕來測試防火牆與 SCP 伺服器之間的連線，然後確認及接受 SCP 伺服器的主機金鑰。 如果您使用 *Panorama* 範本來設定日誌匯出排程，在將範本設定認可至防火牆後，必須執行此步驟。認可範本後，登入每個防火牆、開啟日誌匯出排程，然後按一下 *Test SCP server connection*（測試 *SCP* 伺服器連線）。

© 2019 Palo Alto Networks, Inc.

Device > Software（裝置 > 軟體）

選取 **Device**（設備）> **Software**（軟體）來檢視可用的軟體版本、下載或上載版本、安裝版本（需要支援授權）、從防火牆刪除軟體影像，或檢視版本資訊。

在您升級或降級軟體版本前：

- 檢閱目前 Release Notes（版本資訊）以檢視新功能說明與版本中預設行為的變更並檢視升級軟體的移轉路徑。
- 檢閱此升級與降級考量與在 PAN-OS® 10.0 新功能指南中的升級指示。
- 確保防火牆上的日期與時間設定必須是目前日期與時間。在安裝新版本前，PAN-OS 軟體會進行數位簽署，而且防火牆會檢查簽名。如果防火牆上的日期與時間設定不是目前日期與時間，且防火牆察覺在未來將軟體簽名為錯誤，則它將顯示下列訊息：

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

下表提供此 **Software**（軟體）頁面的使用說明。

軟體選項欄位	說明
版本	列出 Palo Alto Networks 更新伺服器上目前可用的軟體版本。若要檢查 Palo Alto Networks 是否有可用的新軟體版本，請按一下立即檢查。防火牆將使用服務路由，連線至更新伺服器並檢查新版本，如果有可用的更新，則在清單頂端顯示它們。
大小	指出軟體軟體映像檔的大小。
發行日期	表示 Palo Alto Networks 發行可用版本的日期和時間。
支持	表示已上載或已下載至防火牆之軟體影像檔的對應版本。
目前已安裝	表示軟體影像檔的對應版本是否已啟動且是否目前正在防火牆上執行。
動作	指出目前可為對應的軟體影像執行的動作，如下所示： • 下載—對應的軟體版本可在 Palo Alto Networks 更新伺服器上使用；按一下可 **Download**（下載）可用軟體版本。 • 安裝—已將對應的軟體版本下載或上載至防火牆。按一下可 **Install**（安裝）軟體。需要重新啟動以完成升級程序。 • 解除安裝—之前已安裝相應軟體版本；按一下可 **Reinstall**（解除安裝）相同版本。
版本資訊	提供對應軟體更新的版本資訊連結。此連結僅適用於您從 Palo Alto Networks 更新伺服器下載的更新：不適用於上載的更新。
☒	從防火牆移除先前下載或上載的軟體影像。您可能只想刪除無需升級之舊版本的基礎影像。例如，若您執行的是 7.0，您可以移除 6.1 的基礎影像檔，除非您認為可能需要降級。
立即檢查	檢查 Palo Alto Networks 中是否有可用的新軟體更新。

© 2019 Palo Alto Networks, Inc.

軟體選項欄位	說明
上傳	從防火牆可存取的電腦匯入軟體影像。一般而言，您會在防火牆無法存取網際網路時執行此動作，而從 Palo Alto Networks 更新伺服器下載更新時需要執行此動作。如需上載，使用連網電腦造訪 Palo Alto Networks 網站，從支援網站（軟體更新）下載映像檔，將更新下載至您的電腦，然後在防火牆上選取 **Device**（設備）> **Software**（軟體） 並 **Upload**（上載） 軟體映像檔。在高可用性 (HA) 設定中，您可以選取 **Sync To Peer**（同步處理至端點），將匯入的軟體影像推送至 HA 端點。上載之後，**Software**（軟體）頁面會顯示相同資訊（例如版本和大小），以及針對已上載和已下載軟體的 **Install**（安裝）/**Reinstall**（重新安裝）。**Release Notes**（版本資訊）選項在已上載軟體上不可啟用。

© 2019 Palo Alto Networks, Inc.

Device > Dynamic Updates（裝置 > 動態更新）

- Device > Dynamic Updates（裝置 > 動態更新）
- Panorama > Dynamic Updates（Panorama > 動態更新）

Palo Alto Networks 會透過動態更新，包含新的和修訂的應用程式、威脅保護和 GlobalProtect 資料檔案定期發佈更新。防火牆可以擷取這些更新並使用它們來實施原則，而無需變更設定。無需訂閱即可獲得應用程式和一些防毒軟體的更新；剩下的則需訂閱。

您可以檢視最新更新、閱讀每個更新的發行註記，然後選取您要下載及安裝的更新。您也可以還原為之前安裝的更新版本。

為動態更新設定時間表，可讓您定義防火牆檢查和下載或安裝新更新的頻率。特別是對於應用程式和威脅內容更新，您可能希望設置一個時間表，將新的和已修改的應用程式更新錯開後面的威脅更新；這會讓您有更多時間評估新應用程式和修改後的應用程式如何影響您的安全策略，同時確保防火牆始終配備最新的威脅防護。

動態更新選項	說明
版本	列出 Palo Alto Networks 更新伺服器上目前可用的版本。若要檢查 Palo Alto Networks 是否有可用的新軟體版本，請按一下立即檢查。防火牆將使用服務路由，連線至更新伺服器並檢查新的 Content Release 版本，如果有可用的更新，則在清單頂端顯示它們。
上一次檢查	顯示防火牆前次連線到更新伺服器的日期和時間，再檢查是否有可用的更新。
排程	可讓您排程擷取更新的頻率。 您可定義動態內容更新發生的頻率與時間 — **Recurrence**（週期性）與時間 — 以及是否 **Download Only**（僅下載）或 **Download and Install**（下載並安裝）排程更新。 對於防毒和應用程式與威脅更新，您可以選取設定內容更新在防火牆安裝之前必須可用的最短時間臨界值。在極少數的情況下，內容更新中可能存在錯誤，且此臨界值可確保防火牆僅下載在客戶環境中可用並在指定時間內運行的內容版本。 對於應用程式和威脅內容更新，您還可以設置一個臨界值，該臨界值專門用於使用新的和修改過的應用程序的內容更新。一個擴展的應用程式臨界值給您額外的時間來根據新的和修改的應用程式引入的變更來評估和調整您的安全策略。 對於 WildFire 更新，您可以選擇即時擷取特徵碼，從而可以在產生特徵碼後立即對其進行存取。在範例檢查期間下載的特徵碼將儲存在防火牆快取中，並且可用於快速（本機）尋找。此外，為了最大化覆蓋範圍，啟用即時特徵碼後，防火牆還會定期自動下載其他特徵碼套件。這些補充特徵碼將會新增至防火牆快取中，在其變得過時並經過重新整理，或被新特徵碼覆寫之前一直可用。 有關如何最佳地啟用應用程式和威脅更新，以達成不間斷的應用程式可用性和最新威脅防護的指導，請查看 應用程式和威脅更新的最佳實踐方法。

© 2019 Palo Alto Networks, Inc.

動態更新選項	說明
檔案名稱	列出檔案名稱；它包含內容版本資訊。
功能	列出內容版本可能包含的特徵碼類型。 針對應用程式與威脅內容發行版本，此欄位可能會顯示選項以便檢閱 **Apps, Threats**（應用程式與威脅）。按一下此選項以檢視在防火牆上安裝最新 Content Release 版本之後才能提供使用的新應用程式特徵碼。您也可以使用 **New Applications**（新應用程式）對話方塊來 **Enable/Disable**（啟用/停用）新的應用程式。若您要避免來自正在進行唯一識別（若先前未知應用程式已識別，且進行不同分類，則應用程式在內容安裝之前和之後可能會視為不同）之應用程式的任何原則影響，您可能會選取停用包含在 Content Release 中的新應用程式
類型	指出下載包含完整資料庫更新或增量更新。
大小	顯示內容更新套件的大小。
發行日期	Palo Alto Networks 發行 Content Release 的日期和時間。
已下載	此欄中的核取記號表示已將對應的 Content Release 版本下載到防火牆。
目前已安裝	此欄中的核取記號表示對應的 Content Release 版本目前正在防火牆上執行。
動作	指出目前可為對應的軟體影像執行的動作，如下所示： • 下載—在 Palo Alto Networks 更新伺服器上已提供對應的代理程式軟體版本；按一下可 **Download**（下載）內容發行版本。如果防火牆無法存取網際網路，請使用連線到網際網路的電腦以前往 Customer Support Portal（客戶支援入口網站）並選取 **Dynamic Updates**（動態更新）。找出您想要的內容發行版本，然後按一下 **Download**（下載）以儲存更新封包到您的本機電腦中。接著手動 **Upload**（上載）軟體影像至防火牆。此外，下載應用程式和威脅內容發行版本，可啟用 **Review Policies**（檢閱原則）選項，針對受到此版本包含的新應用程式特徵碼影響的原則進行。 • **Review Policies**（檢閱原則）（僅適用於應用程式與威脅內容）—檢閱包含在內容發行版本中之新應用程式的任何原則影響。使用此選項以評估安裝內容更新之前和之後對應用程式所進行的處理。您也可以使用 Policy Review（原則檢閱）對話方塊來新增或移除擱置中的應用程式（下載時包含內容發行版本的應用程式，但並未安裝於防火牆上），該應用程式可能涉及現有的安全性原則規則；擱置中應用程式的原則變更在安裝對應的內容發行版本之前不會造成影響。 • **Review Apps**（檢閱應用程式）（僅應用程式和威脅內容）—檢視在防火牆上安裝最新的內容發行版本之後才能提供使用的新和修改的應用程式特徵碼。如果內容更新引入了可能影響關鍵應用程式執行的變更，則這些應用程式將被標記為建議進行策略檢閱。按一下檢閱原則以查看內容更新如何影響您的現有安全原則，或者您可以停用應用程序，直到您有時間查看應用程式的原則影響為止。 • 安裝 — 已將對應的內容發行版本下載至防火牆。按一下可 **Install**（安裝）更新。安裝新的應用程式與威脅內容發行版本時，系統會提示您選項以便在內容更新時停用新應用程式。此選項會針對最新威脅啟用保護，同時在準備任何原則更新之後提供您啟用應用程式的彈性，因為對新應用程式會造成影響（若要啟用您先前已停用的應用程式，請選取 [動態更新] 頁

© 2019 Palo Alto Networks, Inc.

動態更新選項	說明
	面上的 **Apps, Threats**（應用程式與威脅），或選取 **Objects**（物件）> **Applications**（應用程式））。 • 還原 — 先前已下載對應的 Content Release 版本。若要重新安裝相同的版本，請按一下 **Revert**（還原）。
文件	提供對應版本的版本資訊連結。
☒	從防火牆移除先前下載的 Content Release 版本。
上傳	如果防火牆不能存取 Palo Alto Networks 更新伺服器，您可以從 [Palo Alto Networks 支援] 網站的 [動態更新] 區段手動下載動態更新。將更新下載至電腦後，將更新 **Upload**（上傳）至防火牆。接著，您可選取 **Install From File**（從檔案安裝），並選取您已下載的檔案。
從檔案安裝	將更新檔案手動上傳至防火牆後，請使用此選項安裝檔案。在 **Package Type**（套件類型）下拉式清單中，選取您正在安裝的更新類型（**Application and Threats**（應用程式與威脅）、**Antivirus**（防毒）或 **WildFire**），按一下 **OK**（確定），選取您想要安裝的檔案，然後再次按一下 **OK**（確定）以開始安裝。

© 2019 Palo Alto Networks, Inc.

Device > Licenses（裝置 > 授權）

選取 **Device**（設備）> **Licenses**（授權），可在所有防火牆型號上啟動授權。當您從 Palo Alto Networks 購買使用授權後，您會接收到用來啟動一或多個授權金鑰的驗證碼。

在 VM 系列防火牆上，此頁面也可讓您停用虛擬機器 (VM)。

您可在 [授權] 頁面上執行下列動作：

- 從授權伺服器擷取授權金鑰：選取以啟用需要驗證碼的已購買訂閱（您已在支援入口網站上將其啟動）。
- 使用授權碼啟動功能：選取以啟用需要驗證碼的已購買訂閱（您尚未在支援入口網站上將其啟動）。接著輸入您的授權碼，然後按一下 **OK**（確定）。
- 手動上載授權金鑰：如果防火牆無法連線至授權伺服器，而您想要手動上載授權金鑰，請從 https://support.paloaltonetworks.com 下載授權金鑰檔案，並將其儲存至本機。按一下 [手動上載授權金鑰]、按一下 [瀏覽]、選取檔案，然後按一下 [確定]。

  若要啟用 *URL* 過濾的授權，您必須安裝授權、下載資料庫，然後按一下啟動。若為 *URL* 篩選使用 *PAN-DB*，您將需要先 *Download*（下載）初始種子資料庫，然後按一下 *Activate*（啟動）。

  您也可以執行 *CLI* 命令 ***request url-filtering download paloaltonetworks region < regionname>***。
- 停用 **VM**：此選項可使用「自帶授權版」型號在 VM 系列防火牆上取得，支援永久和期限式授權；而視需要的授權型號不支援此功能。當您不再需要 VM 系列防火牆實例時，請按一下 **Deactivate VM**（停用 VM）。它可讓您釋放所有使用此選項的作用中授權，包括訂閱授權、VM 容量授權和支援權利。授權會記入您的帳戶，以便您稍後需要時將授權套用在 VM 系列防火牆的新實例上。授權停用後，VM 系列防火牆功能即會停用，且防火牆處於未授權狀態。然而，組態則保持不變。
  - 若 VM-Series 防火牆無法直接存取網際網路，請按一下 **Continue Manually**（手動繼續）。防火牆會產生一個語彙基元檔案。按一下 **Export license token**（匯出授權語彙基元），將語彙基元檔案儲存至本機電腦，然後重新啟動防火牆。登入 Palo Alto Networks 支援入口網站、選取 **Assets**（資產）> **Devices**（設備），然後選取 **Deactivate VM**（停用 **VM**）以使用此語彙基元檔案並完成停用程序。
  - 按一下 **Continue**（繼續）以停用 VM 系列防火牆上的授權。按一下 **Reboot Now**（立即重新啟動）來完成授權停用程序。
  - 若您要取消並關閉 Deactivate VM（停用 VM）視窗，請按一下 **Cancel**（取消）。
- **Upgrade VM Capacity**（升級 **VM** 容量）：此選項可讓您升級目前授權之 VM-Series 防火牆的容量。在升級容量時，VM-Series 防火牆將保有其升級前所擁有的所有設定和訂閱。
  - 如果您的防火牆可連線至授權伺服器—選取 **Authorization Code**（授權碼）、在授權碼欄位中輸入您的授權碼，然後按一下 **Continue**（繼續）以啟動容量升級。
  - 如果您的防火牆無法連線至授權伺服器—選取 **License Key**（授權金鑰）、按一下 **Complete Manually**（手動完成）以產生語彙基元檔案，然後將語彙基元檔案儲存至您的本機電腦。接著，登入 Palo Alto Networks 支援入口網站、選取 **Assets**（資產）> **Devices**（設備），然後選取 **Deactivate License(s)**（停用授權）以使用語彙基元檔案。將您 VM-Series 防火牆的授權金鑰下載至本機電腦、將授權金鑰新增至防火牆，然後按一下 **Continue**（繼續）以完成容量升級。
  - 如果您的防火牆可連線至授權伺服器，但您沒有授權碼—選取 **Fetch from license server**（從授權伺服器擷取），接著，在嘗試升級容量前，在授權伺服器上升級防火牆的容量授權，然後在確認已於授權伺服器上升級授權後，按一下 **Continue**（繼續）以啟動容量升級。

© 2019 Palo Alto Networks, Inc.

裝置 > 支援

- 裝置 > 支援
- Panorama > 支援

選取 **Device**（設備） > **Support**（支援） 或 **Panorama** > **Support**（支援） 以存取支援相關選項。您可以檢視 Palo Alto Networks 聯絡人資訊、檢視您的支援到期日，並根據防火牆的序號，從 Palo Alto Networks 檢視產品和安全性警示。

在此頁面執行下列任何功能：

- 支援—提供關於設備支援狀態的資訊，並提供連結以使用驗證代碼啟動支援。
- 生產警示/應用程式與威脅警示—存取/重新整理此頁面時，將從 Palo Alto Networks 更新伺服器擷取這些警示。若要檢視生產警示或應用程式與威脅警示的詳細資料，請按一下警示名稱。如果指定版本有大規模的召回或緊急問題，將發佈生產警示。如果探索到嚴重威脅，將發佈應用程式與威脅警示。
- 連結—提供通用支援連結來協助您管理設備，以及存取支援聯絡資訊。
- 技術支援檔案—按一下 **Generate Tech Support File**（產生技術支援檔案）產生系統檔案，可讓支援團隊排解使用防火牆時可能遇到的問題。產生檔案後，**Download Tech Support File**（下載技術支援檔案），然後將其傳送至 Palo Alto Networks 支援部門。

  如果將瀏覽器設定為下載後開啟檔案，您應關閉該選項，以便瀏覽器下載支援檔案，而不會嘗試開啟或擷取該檔案。
- 統計資料傾印檔案（僅限防火牆）—按一下 **Generate Stats Dump File**（產生統計資料傾印檔案）產生一組 XML 報告，以摘要過去 7 天的網路流量。產生報告後，您可 **Download Stats Dump File**（下載統計資料傾印檔案）。Palo Alto Networks 或授權合作夥伴系統工程師使用報告來產生「安全性生命週期檢視 (SLR)」。SLR 會反白顯示網路上已發現的內容，以及可能出現的相關業務或安全性風險，且一般作為評估程序的一部份。如需 SLR 的詳細資訊，請聯絡 Palo Alto Networks 或授權合作夥伴系統工程師。
- 核心檔案—如果您的防火牆遭遇系統程序失敗，會產生包含關於程序詳細資料的核心檔案以及失敗原因。按一下 **Download Core Files**（下載核心檔案）連結可檢視可用核心檔案的清單，然後按一下核心檔案名稱可加以下載。下載檔案後，將其上載至 Palo Alto Networks 支援案例，以取得解決問題的協助。

  只有 *Palo Alto Networks* 支援工程師才能判讀核心檔案的內容。

© 2019 Palo Alto Networks, Inc.

Device > Master Key and Diagnostics（裝置 > 主要金鑰與診斷）

- **Device**（裝置）> **Master Key and Diagnostics**（主要金鑰與診斷）
- **Panorama** > **Master Key and Diagnostics**（主要金鑰與診斷）

編輯主要金鑰，能將防火牆或 Panorama 上所有的密碼和私密金鑰（例如驗證存取 CLI 之管理員的 RSA 金鑰）進行加密。將密碼和金鑰加密可提高安全性，確保其純文字值不會暴露於防火牆或 Panorama 上的任何位置。

還原預設主要金鑰的唯一方法，是執行原廠重設。

Palo Alto Networks 建議您設定新的主要金鑰而非使用預設金鑰、將金鑰儲存在安全的位置，並定期進行更新。如需額外的隱私性，您可以使用硬體安全性模組將主要金鑰加密（請參閱 [裝置 > 設定 > HSM]）。在每個防火牆或 Panorama 管理伺服器上設定唯一的主要金鑰，以確保得知某部裝置之主要金鑰的攻擊者無法存取您任何其他裝置上的密碼和私密金鑰。不過，在下列情況下，您必須在多部裝置使用相同的主要金鑰：

- 高可用性 **(HA)** 設定—如果您在 HA 設定中部署防火牆或 Panorama，同時在配對中的防火牆或 Panorama 管理伺服器上使用相同的主要金鑰。否則，HA 同步不會運作。
- **Panorama** 會將設定推送至防火牆—如果您是使用 Panorama 將設定推送至受管理的防火牆，請在 Panorama 和受管理的防火牆上使用相同的主要金鑰。否則，從 Panorama 推送運作將會失敗。

若要設定主要金鑰，請編輯主要金鑰設定，並使用下表設定以決定適當的值：

主要金鑰與診斷設定	說明
主要金鑰	啟用以設定唯一的主要金鑰。停用（清除）以使用預設主要金鑰。
目前主要金鑰	指定目前用來在防火牆上加密所有私人金鑰與密碼的金鑰。
新增主要金鑰 確認主要金鑰	若要變更主要金鑰，請輸入 16 字元字串並確認新金鑰。
SA 生命週期	指定主要金鑰將於多少 **Days**（天）及多少 **Hours**（小時）之後過期。範圍是 1-438,000 天（50 年）。 您在目前的金鑰到期之前，必須設定新的主要金鑰。如果主要金鑰到期，防火牆或 Panorama 就會自動以維護模式重新啟動。接著，您必須執行原廠重設。 將 *Lifetime*（存留時間）設定為兩年或更短，具體取決於裝置執行的加密次數。裝置執行的加密次數越多，就應設定越短的 *Lifetime*（存留時間）。關鍵考慮因素是不要在變更主要金鑰之前用完唯一加密。每個主要金鑰最多可以提供 *2 ^^ 32* 個唯一加密，然後重複加密，這存在安全性風險。 為主要金鑰設定 *Time for Reminder*（提醒時間），在出現提醒通知時，變更主要金鑰。

© 2019 Palo Alto Networks, Inc.

主要金鑰與診斷設定	說明
提醒時間	當防火牆產生到期警報時，請在主要金鑰到期前，輸入多少 **Days**（天數）及多少 **Hours**（小時）。防火牆會自動開啟 System Alarms（系統警報）對話方塊來顯示警報。 設定提醒，以便主要金鑰在排程的維護時段內到期之前，您有充足的時間來設定新主要金鑰。當 *Time for Reminder*（提醒時間）到期且防火牆或 *Panorama* 傳送通知日誌時，變更主要金鑰，不要等到 *Lifetime*（存留時間）到期。對於分組裝置，追蹤每個裝置（例如，*Panorama* 管理的防火牆和防火牆 *HA* 配對），當群組中任何裝置的提醒值到期時，變更主要金鑰。 為了確保會顯示到期警報，可選取 *Device*（裝置）> *Log Settings*（日誌設定），編輯 *Alarm Settings*（警報設定），然後 *Enable Alarms*（啟用警報）。
儲存於 HSM	若是在硬體安全性模組 (HSM) 上加密主要金鑰，則啟用此選項。您無法在 DHCP 用戶端或 PPPoE 之類的動態介面上使用 HSM。 未同步 HA 模式下端點防火牆之間的 HSM 設定。因此，HA 配對中的每個端點可連線至不同的 HSM 來源。若是使用 Panorama，並需要維持同步兩個端點上的設定，請在受管理防火牆上使用 Panorama 範本來設定 HSM 來源。 PA-220 不支援 HSM。
自動更新主要金鑰	啟用以在指定的天數和小時數內自動更新主要金鑰。停用（清除）以讓主要金鑰在設定的金鑰存留時間後過期。 透過指定延展主要金鑰加密的 **Days**（天數）和 **Hours**（小時數）（範圍為 1 小時到 730 天），**Auto Renew with Same Master Key**（使用相同的主要金鑰自動更新）。 如果啟用 *Auto Renew Master Key*（自動更新主要金鑰），請進行設定，以使總時間（存留時間加自動更新時間）不會導致裝置用完唯一加密。例如，如果您認為裝置將在兩年半內耗用完主要金鑰的唯一加密次數，則可以將 *Lifetime*（存留時間）設定為兩年，將 *Time for Reminder*（提醒時間）設定為 *60* 天，並將 *Auto Renew Master Key*（自動更新主要金鑰）設定為 *60-90* 天，以在 *Lifetime*（存留時間）到期之前提供額外的時間來設定新的主要金鑰。但是，最佳做法仍然是在存留時間到期之前變更主要金鑰，以確保沒有裝置重複加密。
通用準則	在通用條件模式下，可以使用其他選項來執行密碼演算法自我測試與軟體完整性自我測試。也會包含排程器來指定兩個自我測試的執行時間。

部署主要金鑰

直接從 Panorama 部署主要金鑰或更新受管理防火牆、日誌收集器或 WF-500 裝置的現有主要金鑰。

欄位	說明
部署主要金鑰	

© 2019 Palo Alto Networks, Inc.

欄位	說明
篩選	根據平台、裝置群組、範本、頁籤、HA 狀態或軟體版本篩選要顯示的受管理裝置。
裝置名稱	受管理防火牆的名稱。
軟體版本	執行於受管理的裝置的軟體版本。
狀態	受管理的裝置的連線狀態可以為：Connected、Disconnected 或 Unknown。
部屬主要金鑰工作狀態	
裝置名稱	受管理防火牆的名稱。
狀態	主要金鑰部署工作的狀態。
結果	主要金鑰部署工作的結果。可為 OK 或 FAIL。
進度	主要金鑰部署工作的進度 (%)。
詳細資訊	主要金鑰部署工作的相關詳細資料。若工作失敗，則會在此處顯示說明失敗原因的詳細資料。
Summary	
進度	顯示進度條，指示主要金鑰部署工作的進度。顯示以下資訊： • **Results Succeeded**（已成功的結果）—已成功部署主要金鑰的裝置數。 • **Results Pending**（擱置中的結果）—主要金鑰部署工作目前在其中處於擱置中的裝置數。 • **Results Failed**（失敗的結果）—其中的主要金鑰部署工作失敗的裝置數。

© 2019 Palo Alto Networks, Inc.

Device > Policy Recommendation（裝置 > 政策建議）

從 IoT 安全性應用程式檢視有關政策規則建議的資訊。政策規則建議使用防火牆從網路流量中收集的中繼資料，來確定允許裝置採取何種行為。您可以在 **Device**（裝置）> **Dynamic Updates**（動態更新）> **Device-ID Content**（裝置 **ID** 內容）中，檢查政策規則推薦版本。

按鈕/欄位	說明
政策匯入詳細資訊	檢視有關政策規則建議的詳細資訊，例如裝置群組 **Location**（位置）、**rule name**（規則名稱）、匯入政策的 **user**（使用者）、政策規則建議是否 **Is Updated**（已更新）、匯入政策規則建議的時間，以及上次更新政策規則建議的時間。
裝置設定檔	政策規則建議中來源裝置的裝置設定檔。
來源區域	政策規則建議的來源區域。
位址	政策規則建議的來源位址。
位置	可以使用此政策規則建議的 Panorama 裝置上的裝置群組。
目的地裝置設定檔	防火牆允許政策規則建議的目的地裝置設定檔。
裝置 IP	政策規則建議允許的裝置的 IP 位址。
FQDN	政策規則建議根據裝置的典型行為，將其識別為允許的完全合格網域名稱 (FQDN)。
目的地區域	政策規則建議允許的目的地區域。
安全性設定檔	政策規則建議允許的安全性設定檔。
服務	政策規則建議允許的服務（例如 `ssl`）。
URL 類別	政策規則建議允許的 URL 篩選類別。
應用程式	政策規則建議允許的應用程式。
標籤	識別政策規則建議的政策規則之標籤。 請勿變更政策規則的標籤；如果變更標籤，防火牆將無法重建政策對應。
內部裝置	識別裝置是來自網路內部區域（`Yes`（是）），還是來自外部網際網路區域（`No`（否））。

© 2019 Palo Alto Networks, Inc.

按鈕/欄位	說明
作用中建議	識別此政策規則建議是 `active`（作用中）並且目前在安全性政策中使用，還是已從安全性政策中將其 `removed`（移除）。
動作	識別此政策規則建議的動作（預設為 `allow`（允許））。
有新的更新可用	識別此政策規則建議有新的更新，您必須從 IoT 安全性應用程式匯入該更新。匯入政策規則建議更新時，防火牆會動態更新安全性政策規則。如果您有多個裝置群組，則該值將保持 `Yes`（是），直至您將政策規則建議更新匯入所有裝置群組。
匯入政策	使用 IoT 安全性應用程式，以 **Activate**（啟動）您的政策規則建議後，**Import Policy**（匯入政策），以便匯入政策規則建議，進而在您的安全性政策規則中使用。
移除政策對應	如果您不再需要裝置的政策規則建議，則可以 **Remove Policy Mapping**（移除政策對應）。 您還必須刪除政策規則建議的政策規則。
重建所有對應	如果對應不同步（例如，如果您還原之前的設定），則可以 **Rebuild All Mappings**（重建所有對應）來還原政策規則建議對應。

使用者識別機制

使用者識別 (User-ID™) 是 Palo Alto Networks® 的下一代防火牆功能，該功能與一系列企業目錄及終端機服務無縫整合，使應用程式活動及原則連結至使用者名稱及群組而非僅僅是 IP 位址。設定 User-ID 可使應用程式控管中心 (ACC)、App-Scope、報告及日誌皆包含使用者名稱及使用者 IP 位址。

> Device > User Identification > User Mapping（裝置 > 使用者識別 > 使用者對應）
> Device > User Identification > Connection Security（裝置 > 使用者識別 > 連線安全性）
> Device > User Identification > Terminal Server Agents（裝置 > 使用者識別 > 終端機伺服器代理程式）
> Device > User Identification > Group Mapping Settings（裝置 > 使用者識別 > 群組對應設定）
> Device > User Identification > Authentication Portal Settings（裝置 > 使用者識別 > 驗證入口網站設定）

想知道更多？

請參閱 User-ID

Device > User Identification > User Mapping（裝置 > 使用者識別 > 使用者對應）

設定防火牆上執行之整合 PAN-OS 的 User-ID 代理程式可將 IP 位址對應至使用者名稱。

您想了解什麼內容？	請參閱：
設定整合 PAN-OS 的 User-ID 代理程式。	Palo Alto Networks User-ID 代理程式設定
管理當中 User-ID 代理程式可監控使用者對應資訊的伺服器存取權限。	監控伺服器
將 IP 位址對應至使用者名稱時，管理防火牆包含或排除的子網路。	包含或排除使用者對應的子網路
想知道更多？	使用 PAN-OS 整合的 User-ID 代理程式設定使用者對應。

Palo Alto Networks User-ID 代理程式設定

這些設定定義 User-ID 代理程式用於執行使用者對應的方法。

您想了解什麼內容？	請參閱：
啟用 User-ID 代理程式可使用 Windows Management Instrumentation (WMI) 來探查用戶端系統或透過 HTTP 或 HTTPS 在 Windows Remote Management (WinRM) 監控伺服器，以取得使用者對應資訊。	伺服器監控帳戶
以 User-ID 代理程式監控伺服器日誌以獲得使用者對應資料。	伺服器監控
啟用 User-ID 代理程式可探查用戶端系統，以取得使用者對應資訊。	用戶端探測
請確保使用者漫遊並取得新的 IP 位址時，防火牆取得最新的使用者對應資訊。	快取
設定 User-ID 代理程式可剖析系統日誌訊息，以取得使用者對應資訊。	系統日誌篩選器
設定 User-ID 代理程式可省略對應程序中的特定使用者名稱。	忽略使用者清單

© 2019 Palo Alto Networks, Inc.

伺服器監控帳戶

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Server Monitor**（伺服器監控）

若要設定整合 PAN-OS 的 User-ID 代理程式以使用 Windows Management Instrumentation (WMI) 來探查用戶端系統或使用 Windows Remote Management (WinRM) over HTTP 或 Windows Remote Management (WinRM) over HTTPS 來監控伺服器以取得使用者對應資訊，請完成下列欄位。

您還可以 設定對受監控伺服器的存取，方式為設定 Kerberos 伺服器，以使用 Windows Remote Management (WinRM) over HTTP 或 Windows Remote Management (WinRM) over HTTPS 驗證伺服器監控。

因為 *WMI* 探查會信任從端點回報的資料，*Palo Alto Network* 建議您請勿使用這個方法在高安全性網路中取得 *User-ID* 對應資訊。如果您藉由剖析 *Active Directory (AD)* 安全性事件日誌或 *syslog* 訊息，或是藉由使用 *XML API* 來設定 *User-ID* 代理程式以取得對應資訊，*Palo Alto Networks* 建議您停用 *WMI* 探查。

如果您必須使用 *WMI* 探查，請勿在外部、不受信任的介面上啟用它。這麼做會造成代理程式在您的網路外部傳送包含機密資訊（例如 *User-ID* 代理程式服務帳戶的使用者名稱、網域名稱和密碼雜湊）的 *WMI* 探查。攻擊者很有可能會入侵此資訊來滲透並取得您網路的進一步存取權。

Active Directory 驗證設定	說明
使用者名稱	為防火牆將使用的帳戶輸入網域認證（**User Name**（使用者名稱）及 **Password**（密碼）），以存取 Windows 資源。帳戶需要執行關於用戶端電腦的 WMI 查詢及監控 Microsoft Exchange 伺服器與網域控制的權限。使用適用於 **User Name**（使用者名稱）的網域\使用者名稱語法。若您 設定對受監控伺服器的存取 且使用 Kerberos 進行伺服器驗證，則輸入 Kerberos 使用者主體名稱 (UPN)。
網域的 DNS 名稱	輸入受監控伺服器的 DNS 名稱。若您 設定對受監控伺服器的存取 且使用 Kerberos 進行伺服器驗證，則輸入 Kerberos 領域網域。當您 設定對受監控伺服器的存取時，若使用 **WinRM-HTTP** 作為傳輸通訊協定，則必須進行此設定。
密碼/確認密碼	輸入並確認防火牆用來存取 Windows 資源之帳戶的密碼。
Kerberos 伺服器設定檔	選取 Kerberos 伺服器的 Kerberos 伺服器設定檔，該伺服器用於控制對領域的存取，以透過 WinRM over HTTP 或 WinRM over HTTPS 從受監控的伺服器擷取安全性日誌和工作階段資訊。

用於設定整合 *PAN-OS* 的 *User-ID* 代理程式以監控伺服器及探查用戶端的完整程序除了定義 *Active Directory* 驗證設定之外，還需要完成其他工作。

伺服器監控

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Server Monitor**（伺服器監控）

若要藉由搜尋伺服器安全性事件日誌中的登入事件來啟用 User-ID 代理程式將 IP 位址對應至使用者名稱，請設定下表中所述的設定。

© 2019 Palo Alto Networks, Inc.

如果 *Windows* 伺服器日誌、*Windows* 伺服器工作階段或 *eDirectory* 伺服器的查詢負載高，在查詢之間觀察到的延遲可能會大幅超過您指定的頻率或間隔。

用於設定整合 *PAN-OS* 的 *User-ID* 代理程式以監控伺服器的完整程序 除了設定伺服器監控設定之外，還需要其他工作。

伺服器監控設定	說明
啟用安全性記錄	選取此選項可在 Windows 伺服器上啟用安全性日誌監控。
伺服器日誌監控頻率（秒）	以秒為單位，指定防火牆向 Windows 伺服器安全性日誌查詢使用者對應資訊的頻率（範圍是 1-3600，預設為 2）。此為防火牆結束處理最後一個查詢以及防火牆傳送下一個查詢之間的間隔。 如果日誌監控不經常發生，則可能無法使用最新的 *IP* 位址到使用者對應。如果防火牆過於頻繁地監控日誌，則可能會影響網域控制器、記憶體、*CPU* 以及 *User-ID* 原則強制執行。從 *2-30* 秒的範圍內的數值開始，然後根據性能影響或使用者對應更新的頻率修改該值。
啟用工作階段	選取此選項可在受監控的伺服器上啟用使用者工作階段監控。每次使用者連線到伺服器時，都會建立工作階段；防火牆可使用此資訊來識別使用者 IP 位址。 請勿 *Enable Session*（啟用工作階段）。此設定需要 *User-ID* 代理程式具有 *Active Directory* 帳戶與伺服器運算子權限，以便讀取所有使用者工作階段。反之，您應使用 *Syslog* 或 *XML API* 整合來監控擷取所有裝置類型與作業系統之登入及登出事件的來源（而非僅 *Windows* 作業系統），例如無線控制器及 *NAC*。
伺服器工作階段讀取頻率（秒）	以秒為單位，指定防火牆向 Windows 伺服器使用者工作階段查詢使用者對應資訊的頻率（範圍是 1-3600，預設為 10）。此為防火牆結束處理最後一個查詢以及開始下一個查詢之間的間隔。
Novell eDirectory 查詢間隔（秒）	以秒為單位，指定防火牆向 Novell eDirectory 伺服器查詢使用者對應資訊的頻率（範圍是 1-3600，預設為 30）。此為防火牆結束處理最後一個查詢以及開始下一個查詢之間的間隔。
Syslog 服務設定檔	針對防火牆及 User-ID 代理程式監控的任何 Syslog 寄件者之間的通訊，選取指定憑證的 SSL/TLS 服務設定檔以及允許的 SSL/TLS 版本。如需詳細資訊，請參閱裝置 > 憑證管理 > SSL/TLS 服務設定檔 和Syslog 篩選器。如果您選取 **none**（無），防火牆將使用其預先定義的自我簽署憑證。

用戶端探測

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Client Probing**（用戶端探測）

您可以設定 User-ID 代理程式以針對使用者對應程序識別的每個用戶端系統執行 WMI 用戶端探查。User-ID 代理程式將定期探查各個已知 IP 位址以確認相同的使用者仍為登入狀態。當防火牆遭遇無使用者對應的 IP 位址時，將傳送位址至代理程式以立即探查。若要設定用戶端探查設定，請完成下列欄位。

© 2019 Palo Alto Networks, Inc.

請勿在高安全性網路上啟用用戶端探查。請勿在外部不信任的介面上啟用用戶端探查。用戶端探查可能會生成大量的網路流量，在設定錯誤時可能會造成安全威脅，並且如果在外部不信任的區域中啟用，用戶端探查可能會允許攻擊者在您的網路外傳送探測，並導致揭露 *User-ID* 代理程式服務帳戶名稱、網域名稱，以及加密的密碼雜湊。反之，從更多隔離與受信任來源收集使用者對應資訊，例如網域控制器及透過與 *Syslog* 或 *XML API* 整合，可帶來額外好處，讓您能夠安全地從任何裝置類型或作業系統而非僅有 *Windows* 用戶端擷取使用者對應資訊。

用於設定整合 *PAN-OS* 的 *User-ID* 代理程式以探查用戶端的完整程序除了設定用戶端探查設定之外，還需要其他工作。

PAN-OS 整合式 *User-ID* 代理程式不支援 *NetBIOS* 探查，但 Windows-based User-ID 代理程式支援該探查。

用戶端探查設定	說明
啟用探查	選取此選項可啟用 WMI 探查。
探查間隔（分鐘）	輸入以分鐘為單位的探查間隔（範圍是 1-1440；預設為 20）。此為防火牆結束處理最後一個要求以及開始下一個要求之間的間隔。 在大型部署中，必須適當設定間隔，以便有時間探查各個已識別使用者對應程序的用戶端。例如，如果您有 6,000 個使用者，而且間隔為 10 分鐘，則需要各個用戶端每秒處理 10 個 WMI 要求。 如果探查的要求負載高，在要求之間觀察到的延遲可能會大幅超過您指定的間隔。

快取

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Cache**（快取）

若要確保在使用者漫遊並取得新的 IP 位址時，防火牆可取得最新的使用者對應資訊，請設定從防火牆快取中清除使用者對應的逾時。此逾時會套用至透過驗證入口網站以外的任何方法學習到的使用者對應。對於透過驗證入口網站學習到的對應，請在驗證入口網站設定中設定逾時（Device > User Identification > Authentication Portal Settings（裝置 > 使用者識別 > 驗證入口網站設定）、**Timer**（計時器）和 **Idle Timer**（閒置計時器）欄位）。

若要在不包含網域的情況下，匹配從 User-ID 來源收集的使用者名稱，則請將防火牆設定為允許不需網域進行使用者名稱匹配。您應只在使用者名稱未在全部網域中重覆的情況下使用本選項。

快取設定	說明
啟用使用者識別逾時	選取此選項可啟用使用者對應項目的逾時值。當達到項目的逾時值，防火牆將清除項目並收集新的對應。這將確保使用者漫遊並取得新的 IP 位址時，防火牆取得最新的資訊。 啟用逾時以確保防火牆具有最新的使用者到 *IP* 位址對應資訊。
使用者識別逾時（分鐘）	為使用者對應項目設定以分鐘為單位的逾時值（範圍是 1 到 3,600，預設值為 45）。

© 2019 Palo Alto Networks, Inc.

快取設定	說明
	將逾時數值設定為 *DHCP* 租約生命週期的一半，或 *Kerberos* 票證的生命週期。 如果您設定防火牆以重新散佈對應資訊，則每個防火牆將會根據您在該防火牆上設定的逾時來清除對應項目，而不是根據轉送防火牆中的逾時設定。
允許不需網域進行使用者名稱匹配	選取本選項以允許防火牆在 User-ID 來源未提供網域時進行使用者匹配。若要避免使用者辨識出錯，若您的使用者名稱未在全網域中重覆，請只選取本選項。 在您啟用本選項前，請驗證防火牆已從 *LDAP* 伺服器截取群組對應。

重新分配

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Redistribution**（重新分配）

若要啟用防火牆或虛擬系統以作為重新散佈使用者對應資訊以及與驗證挑戰相關聯之時間戳記的 User-ID 代理程式，請設定下表中所述的設定。您稍後將此防火牆連線至會接收對應資訊和時間戳記的裝置（例如 Panorama）時，裝置會使用這些欄位將防火牆或虛擬系統識別為 User-ID 代理程式。

設定防火牆重新散佈使用者對應資訊與驗證時間戳記的完整程序 除了指定重新散佈設定之外，還需要其他工作。

依預設，具有多個虛擬系統的防火牆不會跨其虛擬系統重新散佈使用者對應資訊，然而您可以設定它們進行重新散佈。

重新散佈設定	說明
收集器名稱	輸入用來識別防火牆或虛擬機器作為 User-ID 代理程式的收集器名稱（最多 255 個英數字元）。
預先共用金鑰/確認預先共用金鑰	輸入用來識別防火牆或虛擬機器作為 User-ID 代理程式的預先共用金鑰（最多 255 個英數字元）。

系統日誌篩選器

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Syslog Filters**（**Syslog** 篩選器）

User-ID 代理程式使用 Syslog 剖析設定檔來篩選 Syslog 訊息，此訊息是從代理伺服器監控 IP 位址至使用者對應資訊的 Syslog 寄件者所傳來（請參閱設定對受監控伺服器的存取）。每個設定檔都可以剖析下列任一種事件類型的 Syslog 訊息，但無法同時剖析兩者：

- 驗證（登入）事件—用來對防火牆新增使用者的對應。
- 登出事件—用來刪除不再是最新狀態的使用者對應。刪除過時對應在 IP 位址指派經常變更的環境中會很實用。

© 2019 Palo Alto Networks, Inc.

Palo Alto Networks 會透過應用程式內容更新向防火牆提供預先定義的 Syslog 剖析設定檔。若要在廠商發展出新的篩選器時動態更新設定檔清單，請排程這些動態內容更新（請參閱Device > Dynamic Updates（裝置 > 動態更新））。預先定義的設定檔可供防火牆全域使用，您所設定的自訂設定檔則只適用於在 **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）下選取的虛擬系統（**Location**（位置））。

Syslog 訊息必須符合下列準則才可供 User-ID 代理程式進行剖析：

- 每個訊息都必須是單行文字字串。換行字元 (\n) 或歸位字元加上換行字元 (\r\n) 是用來分行的分隔符號。
- 個別訊息的大小上限為 8,000 位元組。
- 透過 UDP 傳送的訊息必須包含在單一封包中；透過 SSL 傳送的日誌訊息可跨越多個封包。單一封包可包含多個訊息。

若要設定自訂設定檔，請按一下 **Add**（新增），並指定下表所述的設定。此表格中的欄位說明會使用來自 Syslog 訊息的登入事件範例，其採用下列格式：

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```

將 *User-ID* 代理程式設定為剖析 *Syslog* 寄件者以取得使用者對應資訊時的完整程序，除了要建立 *Syslog* 剖析設定檔外，還必須進行其他工作。

欄位	說明
Syslog 剖析設定檔	輸入設定檔的名稱（最多 63 個英數字元）。
說明	輸入設定檔的說明（最多 255 個英數字元）。
類型	指定用來篩選使用者對應資訊的剖析類型。 • **Regex Identifier**（**Regex** 識別碼）—使用 **Event Regex**（事件 **Regex**）、**Username Regex**（使用者名稱 **Regex**）及 **Address Regex**（位址 **Regex**）來指定說明搜尋模式的規則運算式，以便從 Syslog 訊息中識別和擷取使用者識別資訊。防火牆會使用 regex 來比對 Syslog 訊息中的驗證或登出事件，以及比對相符訊息內的使用者名稱和 IP 位址。 • **Field Identifier**（欄位識別碼）—使用 **Event String**（事件字串）、**Username Prefix**（使用者名稱前置詞）、**Username Delimiter**（使用者名稱分隔符號）、**Address Prefix**（位址前置詞）、**Address Delimiter**（位址分隔符號）及 **Addresses Per Log**（日誌位址）欄位，來指定用於比對驗證或登出事件以及從 Syslog 訊息中識別使用者對應資訊的字串。 對話方塊中的其餘欄位會隨著您的選取項目而有所不同。請如下列資料列所述設定欄位。
事件 Regex	輸入用於識別成功驗證或登出事件的 regex。對於此表格所使用的訊息範例，regex **`(authentication\ success)`** 會擷取 `authentication success` 字串的第一個 **`{1}`** 實例。空格前面的反斜線是標準的 regex 逸出字元，指示 regex 引擎不要將空格視為特殊字元。
使用者名稱 Regex	輸入用於識別驗證成功或登出訊息中使用者名稱欄位的 regex。對於此表格所使用的訊息範例，regex **`User:([a-zA-Z0-9\\\._]+)`** 會比對 `User:johndoe_4` 字串，並擷取 acme\johndoe1 作為使用者名稱。

© 2019 Palo Alto Networks, Inc.

欄位	說明
位址 Regex	輸入用來識別驗證成功或登出訊息中的 IP 位址部分的 regex。在此表格所使用的訊息範例中，規則運算式 **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** 會比對 IPv4 位址 `Source:192.168.0.212`，並將 192.168.0.212 作為 IP 位址來新增到使用者名稱對應中。
事件字串	輸入比對字串來識別驗證成功或登出訊息。對於此表格所使用的訊息範例，您會輸入 **`authentication success`** 字串。
使用者名稱前置詞	輸入比對字串來識別驗證或登出 Syslog 訊息內使用者名稱欄位的開頭。此欄位不支援 **`\s`**（用於空格）或 **`\t`** （用於定位字元）之類的 regex 運算式。在此表格所使用的訊息範例中，`User:` 會識別使用者名稱欄位的開頭。
使用者名稱分隔符號	輸入標記驗證或登出訊息內使用者名稱欄位結尾的分隔符號。使用 \s 可表示獨立空格（如訊息範例所示），使用 \t 則可表示頁籤。
位址首碼	輸入比對字串來識別 Syslog 訊息中 IP 位址欄位的開頭。此欄位不支援 **`\s`**（用於空格）或 **`\t`** （用於定位字元）之類的 regex 運算式。在此表格所使用的訊息範例中，`Source:` 會識別位址欄位的開頭。
位址分隔符號	輸入標記驗證成功或登出訊息中 IP 位址欄位結尾的比對字串。例如，輸入 **`\n`** 可指出要以分行符號作為分隔符號。
日誌位址	輸入為您想要防火牆剖析 IP 位址的最大數目（預設值為 1；範圍為 1 至 3）。

忽略使用者清單

- **Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（代理程式設定）> **Ignore User List**（忽略使用者清單）

忽略使用者清單會定義哪些使用者帳戶不需要 IP 位址至使用者名稱對應（例如，自助服務機帳戶）。若要設定清單，請按一下 **Add**（新增），然後輸入使用者名稱。您可將星號用作萬用字元來比對多個使用者名稱，但只能用作項目中的最後一個字元。例如，**corpdomain\it-admin*** 會比對 **corpdomain** 網域中使用者名稱以字串 **it-admin** 開頭的所有管理員。您可新增最多 5,000 個從使用者對應中排除的項目。

在 *User-ID* 代理程式防火牆（而不是用戶端防火牆）上定義忽略使用者清單。如果您在用戶端防火牆上定義忽略使用者清單，清單中的使用者在重新散佈時仍然會進行對應。

監控伺服器

- Device > User Identification > User Mapping（裝置 > 使用者識別 > 使用者對應）

使用 Server Monitoring（伺服器監控）區段來定義 Microsoft Exchange Server、Active Directory (AD) 網域控制站、Novell eDirectory 伺服器或 User-ID 代理程式監控登入事件的 syslog 傳送端。

- 設定對受監控伺服器的存取
- 管理對受監控伺服器的存取
- 包含或排除使用者對應的子網路

© 2019 Palo Alto Networks, Inc.

設定對受監控伺服器的存取

使用 Server Monitoring（伺服器監控）區段可 **Add**（新增）伺服器設定檔，以指定防火牆所將監控的伺服器。

設定至少兩個受 *User-ID* 監控的伺服器，以便在一個伺服器出現故障時，防火牆仍然可以學習 *IP* 位址到使用者名稱的對應。

在設定整合 *PAN-OS* 的 *User-ID* 代理程式以監控伺服器的完整程序 中，除了建立伺服器設定檔外，還須執行其他工作。

伺服器監控設定	說明
名稱	輸入伺服器的名稱。
說明	輸入伺服器的描述。
已啟用	選取此選項可啟用此伺服器的日誌監控。
類型	選取伺服器類型。您的選項將決定此對話方塊顯示哪些其他欄位。 • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • 系統日誌寄件者
傳輸通訊協定（僅限 Microsoft Active Directory 和 Microsoft Exchange）	選取傳輸通訊協定： • **WMI** —（預設）使用 Windows Management Instrumentation (WMI) 來探測每個已學習的 IP 位址，並驗證同一使用者是否仍然登入。 • **Win-RM-HTTP**—透過 HTTP 使用 Windows Remote Management (WinRM) 來監控伺服器上的安全日誌和工作階段資訊。此選項需要 伺服器監控帳戶 中 Kerberos **Domain's DNS Name**（網域的 **DNS** 名稱）。 • **Win-RM-HTTPS**—透過 HTTPS 使用 Windows Remote Management (WinRM) 來監控伺服器上的安全日誌和工作階段資訊。在使用 Kerberos 驗證時如需要求使用 Windows 伺服器進行伺服器憑證驗證，請確認您在 全域服務設定 中設定 NTP 並選取 Root CA 作為憑證設定檔（Device > User Identification > Connection Security（裝置 > 使用者識別 > 連線安全性））。
網路位址	輸入受監控伺服器的伺服器 IP 位址或 FQDN。如果使用 Kerberos 進行伺服器驗證，則必須輸入 FQDN。如果 **Type**（類型）是 **Novell eDirectory**，則不支援此選項。
伺服器設定檔（僅適用於 Novell eDirectory）	選取用來連線至 Novell eDirectory 伺服器的 LDAP 伺服器設定檔（Device > Server Profiles > LDAP（裝置 > 伺服器設定檔 > LDAP））。
連線類型（僅適用於 Syslog 傳送端）	選取 User-ID 代理程式要在 **UDP** 連接埠 (514) 還是 **SSL** 連接埠 (6514) 上接聽 syslog 訊息。如果您選取 **SSL**，則您在啟用伺服器監控時選取的 **Syslog Service Profile**（**Syslog** 服務設定檔）將決定允許的 SSL/TLS 版本，以及防火牆用來保護 syslog 傳送端連線的憑證。

© 2019 Palo Alto Networks, Inc.

伺服器監控設定	說明
	根據安全性最佳做法，使用整合 *PAN-OS* 的 *User-ID* 代理程式將 *IP* 位址對應至使用者名稱時，請選取 *SSL*。如果您選取 *UDP*，請確定 *syslog* 傳送端和用戶端皆位於專用的安全網路上，以防止不受信任的主機將 *UDP* 流量傳送至防火牆。
篩選 （僅適用於 Syslog 傳送端）	如果伺服器 **Type**（類型）為 **Syslog Sender**（**Syslog** 傳送端），請新增一或多個 Syslog 剖析設定檔，用以擷取從這個伺服器接收之 syslog 訊息中的使用者名稱和 IP 位址。您可以新增自訂設定檔（請參閱Syslog 篩選器）或預先定義的設定檔。為每個設定檔設定 **Event Type**（事件類型）： • 登入—User-ID 代理程式會剖析登入事件的 syslog 訊息，以建立使用者對應。 • 登出—User-ID 代理程式會剖析登出事件的 syslog 訊息，以刪除非現行的使用者對應。在動態指派 IP 位址的網路中，自動刪除可確保代理程式只會將每個 IP 位址對應至目前相關聯的使用者，而提升使用者對應的精確性。 如果您新增預先定義的 *Syslog* 剖析設定檔，請檢查其名稱，以確認它是要比對登入還是登出事件。
預設網域名稱 （僅適用於 Syslog 傳送端）	（選用）如果伺服器**Type**（類型）為 **Syslog Sender**（Syslog 傳送端），則輸入一個網域名稱以取代您 syslog 訊息使用者名稱中的當前網域名稱，或如果您的 syslog 訊息不包含網域，則在使用者名稱前面加上網域。

管理對受監控伺服器的存取

在 [伺服器監控] 區段執行下列工作，以管理 User-ID 代理程式監控使用者對應資訊的伺服器存取權限。

工作	說明
顯示伺服器資訊	對於每個受監控的伺服器，[使用者對應] 頁面會顯示 User-ID 代理程式與伺服器的連線狀態。**Add**（新增）伺服器後，防火牆將嘗試連線該伺服器。如果連線嘗試成功，[伺服器監控] 區段將在 [狀態] 欄中顯示 [已連線]。如果防火牆無法連線，狀態將顯示錯誤狀況，例如連線遭拒或連線逾時。 如需伺服器監控區段顯示的其他欄位的詳細資訊，請參閱設定對受監控伺服器的存取。
新增	若要設定對受監控伺服器的存取，請 **Add**（新增）User-ID 代理程式將監控使用者對應資訊的每個伺服器。
刪除	若要從使用者對應程序（探索）移除伺服器，請選取該伺服器，然後將其 **Delete**（刪除）。 提示：若要從探索中移除伺服器而不刪除其組態，請編輯伺服器項目，然後清除 **Enabled**（已啟用）。
深入瞭解	您可以使用 DNS 自動 **Discover**（探索）Microsoft Active Directory 網域控制站。防火牆將按照 **Device**（設備）> **Setup**（設定）> **Management**（管理）頁面 **General Settings**（一般設置）區段 **Domain**（網域）欄位中輸入的網域名稱發現網域控制站。探索網域控制站後，防火牆將在伺服器監視清單中建立一個項目；然後您可以啟用用於監視的伺服器。

© 2019 Palo Alto Networks, Inc.

工作	說明
	探索功能僅適用於網域控制站；不適用於交換伺服器或 *eDirectory* 伺服器。

包含或排除使用者對應的子網路

- Device > User Identification > User Mapping（裝置 > 使用者識別 > 使用者對應）

使用包含/排除網路清單可定義 User-ID 代理程式在執行 IP 位址到使用者名稱的對應（探索）時，User-ID 代理程式將包含或排除的子網路。依預設，如果您沒有新增任何子網路至該清單，User-ID 代理程式將對所有子網路中的使用者識別來源執行發現，針對擁有公共 IPv4 位址的用戶端系統使用 WMI 探查時除外。（公共 IPv4 位址是指在 RFC 1918 與 RFC 3927 範圍之外的位址）。

若要針對公共 IPv4 位址啟用 WMI 探查，您必須將其子網路新增至該清單，並將 **Discovery**（探索）選項設定為 **Include**（包含）。如果您將防火牆設定為重新散佈使用者對應資料 至其他防火牆，則您在清單中指定的限制將套用至重新散佈的資訊。

使用包含和排除清單來定義防火牆執行使用者對應的子網路。

您可以在包含/排除網路清單上執行下列工作：

工作	說明
新增	若要將發現限制為特定子網路，請 **Add**（新增）子網路設定檔，然後完成下列欄位： • 名稱—輸入用來識別子網路的名稱。 • 已啟用—選取此選項可對伺服器監控啟用包含或排除子網路。 • 探索 — 選取 User-ID 代理程式是否將 **Include**（包含）或 **Exclude**（排除）子網路。 • 網路位址 — 輸入子網路的 IP 位址範圍。 User-ID 代理程式會套用隱含全部排除規則至清單。例如，如果您使用 **Include**（包含）選項新增子網路 10.0.0.0/8，User-ID 代理程式將排除所有其他子網路，即使您並未將它們新增至清單。請只在您希望 User-ID 代理程式排除明確包括的子網路子集時，才使用排除選項新增項目。例如，如果您使用 **Include**（包含）選項新增 10.0.0.0/8 以及 **Exclude**（排除）選項新增 10.2.50.0/22，User-ID 代理程式將針對除了 10.2.50.0/22 以外的所有 10.0.0.0/8 子網路執行探索，並將排除 10.0.0.0/8 以外的所有子網路。如果您新增 **Exclude**（排除）設定檔而不新增任何 **Include**（包含）設定檔，User-ID 代理程式將排除所有子網路，而不只是您新增的子網路。
刪除	若要從清單中移除子網路，請選取子網路並將其 **Delete**（刪除）。 提示：若要從包含/排除網路清單中移除子網路而不刪除其組態，請編輯子網路設定檔，然後清除 **Enabled**（已啟用）。
自訂包含/排除網路	依預設，User-ID 代理程式會從頂端第一個到底端最後一個，以您新增的順序評估子網路。若要變更評估順序，請按一下**Custom Include/Exclude Network Sequence**（自訂包含/排除網路順序）。然後您可以 **Add**（新增）、**Delete**（刪除）、**Move Up**（上移）或 **Move Down**（下移）子網路以建立自訂評估順序。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > Connection Security（裝置 > 使用者識別 > 連線安全性）

編輯（⚙）使用者 User-ID 連線安全性設定，以選取防火牆使用的憑證設定檔，驗證 Windows User-ID 代理程式所顯示的憑證。防火牆會使用選取的憑證設定檔來驗證 User-ID 代理程式的識別，方法是驗證代理程式所顯示的伺服器憑證。

工作	說明
User-ID 憑證設定檔	從下拉式清單中選取驗證 Windows User-ID 代理程式時要使用的憑證設定檔，或選取 New Certificate Profile（新增憑證設定檔）以建立新的憑證設定檔。選取 **None**（無）可移除憑證設定檔並改用預設的驗證。 在您 設定對受監控伺服器的存取 使用 Kerberos 的伺服器驗證時如需要求使用 Windows 伺服器進行伺服器憑證驗證，請確認您在 全域服務設定 中設定 NTP 並選取 Root CA 作為憑證設定檔。
全部移除（僅限範本組態）	將附加至所選範本之 User-ID 連線安全性設定的憑證設定檔移除。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > Terminal Server Agents（裝置 > 使用者識別 > 終端機伺服器代理程式）

在支援共用同一 IP 位址的多個使用者的系統上，終端機服務 (TS) 代理程式會透過對每個使用者配置連接埠範圍來識別個別使用者。TS 代理程式會通知每一個連線的防火牆的配置連接埠範圍，以便防火牆可根據使用者及使用者群組強制執行原則。

所有防火牆型號都可以從最多 5,000 個多使用者系統收集使用者名稱對連接埠對應資訊。防火牆可從中收集對應資訊的 TS 代理程式的數目會依防火牆型號而有所不同：

您必須先安裝及設定 *TS* 代理程式，再設定其存取權限。用於設定終端伺服器使用者之使用者對應的完整程序 除了設定與 *TS* 代理程式的連線，還需要完成其他工作。

您可以執行下列工作來管理 TS 代理程式的存取權限。

工作	說明
顯示資訊/重新整理已連接項目	在 **Terminal Server Agents**（終端機伺服器代理程式）頁面上，Connected（已連線）欄顯示防火牆與 TS 代理程式的連線狀態。綠色圖示表示連線成功，黃色圖示表示連線已停用，紅色圖示表示連線失敗。如果您認為自您首次開啟頁面後連線狀態可能已變更，請按一下 **Refresh Connected**（重新整理已連接項目）以更新狀態顯示。
新增	若要設定對 TS 代理程式的存取，請 **Add**（新增）代理程式並設定下列欄位： • 名稱—輸入用來識別 TS 代理程式的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 • **Host**（主機）—輸入安裝 TS 代理程式之終端機伺服器的靜態 IP 位址或主機名稱。 • **Port**（連接埠）—輸入埠號（預設為 5009），TS 代理程式服務會在該埠號上與防火牆通訊。 • **Alternative Hosts**（替代主機）—如果安裝 TS 代理程式的終端機伺服器具有多個 IP 位址，且這些位址可能以傳出流量的來源 IP 位址形式呈現，請 **Add**（新增），然後另外輸入最多 8 個靜態 IP 位址或主機名稱。 • **Enabled**（已啟用）—選取此選項可讓防火牆與 TS 代理程式通訊。
刪除	若要移除啟用對 TS 代理程式存取的組態，請選取代理程式，然後按一下 **Delete**（刪除）。 若要停用對 *TS* 代理程式的存取而不刪除其組態，請編輯代理程式，然後清除 *Enabled*（已啟用）選項。
PDF/CSV	具有最小唯讀訪問權限的管理角色可以匯出如 **PDF/CSV** 的裝置組態表。您可以在稽核等情況下套用篩選以建立更多特定表格組態匯出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > Group Mapping Settings Tab（裝置 > 使用者識別 > 群組對應設定頁籤）

- **Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定）

為根據使用者及使用者群組定義安全性原則與報告，防火牆會擷取目錄伺服器上所指定及維護的群組清單和對應的成員清單。防火牆支援各種 LDAP 目錄伺服器，其中包括 Microsoft Active Directory (AD)、Novell eDirectory 和 Sun ONE 目錄伺服器。

每個防火牆或 Panorama 可以跨所有原則參考的不同使用者群組之數目會依型號而有所不同：不論何種型號，您都必須先設定 LDAP 伺服器設定檔（裝置 > 伺服器設定檔 > LDAP），然後您才能建立新群組對應組態。

用於將使用者名稱對應至群組的完整程序 除了建立群組對應組態之外，還需要完成其他工作。

Add（新增）並依照需求設定下列欄位，以建立群組對應組態。若要移除群組對應組態，請選取它並加以 **Delete**（刪除）。如果您想要停用群組對應組態而不將其刪除，請編輯設定並清除 **Enabled**（已啟用）選項。

如果您建立使用同一基本識別名稱 *(DN)* 或 *LDAP* 伺服器的多個群組對應設定，則群組對應設定不能包含重疊的群組（例如，一個群組對應設定的包含清單不能包含也在另一群組對應設定中的群組）。

群組對應組態—伺服器設定檔	設定位置	說明
名稱	**Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定）	輸入用來識別群組對應組態的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
伺服器設定檔	**Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定）> **Server Profile**（伺服器設定檔）	選取要針對此防火牆上群組對應所使用的 LDAP 伺服器設定檔。
更新間隔		指定間隔（秒），過了此間隔後，防火牆將啟動與 LDAP 目錄伺服器的連線，以取得針對此防火牆原則中使用的群組所進行的任何更新（範圍是 60 到 86,400）。
使用者網域		依預設，**User Domain**（使用者網域）為空白：防火牆會自動偵測 Active Directory 伺服器的網域名稱。若您輸入值，它將取代防火牆從 LDAP 來源擷取的任何網域名稱。您的項目必須為 NetBIOS 名稱。 此欄位僅會影響從 *LDAP* 來源擷取的使用者名稱和群組名稱。若要取代與使用者驗證的使用者

© 2019 Palo Alto Networks, Inc.

群組對應組態—伺服器設定檔	設定位置	說明
		名稱相關聯的網域，請設定您指派給該使用者之驗證設定檔的 *User Domain*（使用者網域）和 *Username Modifier*（使用者名稱修改程式）（請參閱 *[裝置 > 驗證設定檔]*）。
群組物件		• 搜尋篩選器 — 輸入指定擷取及追蹤哪些群組的 LDAP 查詢。 • 物件類別—輸入群組定義。預設為 objectClass=group，這說明系統會擷取與群組 **Search Filter**（搜尋篩選器）相符且 objectClass=group 之目錄中的所有物件。
使用者物件		• 搜尋篩選器 — 輸入指定擷取及追蹤哪些使用者的 LDAP 查詢。 • 物件類別 — 輸入使用者物件定義。例如，在 Active Directory 中，objectClass 是*user*。
已啟用		選取此選項可啟用群組對應的伺服器設定檔。
擷取受管理的裝置清單		有關 GlobalProtect 部屬，請選取此選項以允許防火牆從目錄伺服器（例如 Active Directory）擷取序號。這讓 GlobalProtect 能夠識別連線中的端點的狀態，並根據端點序號的存在強制執行 HIP 型安全性原則。
使用者屬性	**Device > User Identification > Group Mapping Settings > User and Group Attributes**（裝置 > 使用者識別 > 群組對應設定 > 使用者和群組屬性）	指定識別使用者的目錄屬性： • **Primary Username**（主要使用者名稱）—指定 User-ID 來源為使用者名稱提供的屬性（例如，**`userPrincipalName`** 或 **`sAMAccountName`**） 主要使用者名稱是防火牆在日誌、報告和原則組態中識別使用者的方式，即使防火牆從 *User-ID* 來源接收其他格式也是如此。如果您不指定格式，則防火牆為 *Active Directory* 預設使用 `sAMAccountName` 格式，為 *Novell eDirectory* 和 *Sun ONE* 目錄伺服器預設使用 `uid` 格式。 • **E-Mail**—指定 User-ID 來源為電子郵件地址提供的屬性。預設值為 **`mail`**。 • **Alternate Username 1-3**（備用使用者名稱 1-3）—最多可以指定三個與您可以傳送的 User-ID 格式相對應的其他屬性。

© 2019 Palo Alto Networks, Inc.

群組對應組態—伺服器設定檔	設定位置	說明
		如果您設定 *Active Directory* 伺服器，替代使用者名稱 *1* 預設為 `userPrincipalName`。
群組屬性		指定 User-ID 來源使用的屬性來識別群組： • **Group Name**（群組名稱）—指定 User-ID 來源用於群組名稱屬性的屬性。Active Directory 的預設值為 `name`，Novell eDirectory 或 Sun ONE 目錄服務器的預設值為 `cn`。 • **Group Member**（群組成員）—指定 User-ID 來源用於群組成員的屬性。預設值為 `member`（成員）。 • **E-Mail**—指定 User-ID 來源為電子郵件地址使用的屬性。預設值為 `mail`。
可用群組 包含的群組	**Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定）> **Group Include List**（群組包含清單）	在您建立安全性規則時，使用這些欄位來限制防火牆顯示的群組數量。瀏覽 LDAP 樹狀結構，尋找要在規則中使用的群組。若要包含群組，則選取並新增 (⊕) 至可用群組清單。若要從清單中移除群組，則從包含的群組清單中選取並刪除 (⊖)。 僅包含您需要的群組，以便防火牆僅為必要的群組檢索使用者群組對應，而不是擷取 *LDAP* 目錄中的整個路徑。
名稱 LDAP 篩選器	**Device**（裝置）> **User Identification**（使用者識別）> **Group Mapping Settings**（群組對應設定）> **Custom Group**（自訂群組））	根據 LDAP 篩選器建立自訂群組，以便您使用不符 LDAP 目錄現有使用者群組的使用者屬性為基礎來建立防火牆原則。 User-ID 服務會將符合篩選器的所有 LDAP 目錄使用者對應至自訂群組。如果您建立一個辨別名稱 (DN) 與現有 Active Directory 群組網域名稱相同的自訂群組，防火牆將在該名稱的所有參照中使用自訂群組（例如在原則和日誌中）。若要建立自訂群組，**Add**（新增）並設定下列欄位： • 名稱 — 在群組對應組態中為目前防火牆或虛擬系統輸入一個唯一的自訂群組名稱。 • **LDAP** 篩選器 — 輸入最多 2,048 個字元的篩選器。 僅使用篩選器中的索引屬性可加速 *LDAP* 搜尋，並使 *LDAP* 目錄伺服器的效能影響降到最低；防火牆不會驗證 *LDAP* 篩選器。 **Included Groups**（包含群組）和 **Custom Group**（自訂群組）清單的合併上限是 640 個項目。

© 2019 Palo Alto Networks, Inc.

群組對應組態—伺服器設定檔	設定位置	說明
		若要刪除自訂群組，請選取它並加以 **Delete**（刪除）。若要複製自訂群組，請選取它並 **Clone**（複製），然後視需要編輯欄位。 新增或複製自訂群組後，您必須 *Commit*（認可）您的變更後，新的自訂群組才可在原則和物件中提供使用。

© 2019 Palo Alto Networks, Inc.

Device > User Identification > Authentication Portal（裝置 > 使用者識別 > 驗證入口網站）

編輯（⚙）驗證入口網站設定，可將防火牆設定為驗證流量與驗證政策規則相符的使用者。

如果驗證入口網站使用 *SSL/TLS* 服務設定檔（Device > Certificate Management > SSL/TLS Service Profile（裝置 > 憑證管理 > SSL/TLS 服務設定檔））、驗證設定檔（Device > Authentication Profile（裝置 > 驗證設定檔）），或憑證設定檔（Device > Certificate Management > Certificate Profile（裝置 > 憑證管理 > 憑證設定檔）），則在您開始使用前請先設定設定檔。設定驗證入口網站的完整程序除了設定這些設定檔之外，還需要其他工作。您必須 *Enable Captive Portal*（啟用驗證入口網站）才能強制執行驗證政策（請參閱 Policies（政策）> Authentication（驗證））。

欄位	說明
啟用驗證入口網站	選取此選項可啟用驗證入口網站。
閒置計時器（分鐘）	針對驗證入口網站工作階段以分鐘為單位輸入使用者存留時間 (TTL) 值（範圍是 1 到 1,440；預設為 15）。此計時器會重設驗證入口網站使用者有活動的每段時間。如果使用者閒置時間超過 **Idle Timer**（閒置計時器）值，PAN-OS 將移除驗證入口網站使用者對應，且使用者必須再次登入。
計時器（分鐘）	這是 TTL 上限（分鐘），為任何驗證入口網站工作階段可維持對應的時間量上限（範圍是 1 到 1,440；預設為 60）。此持續時間結束後，PAN-OS 將移除對應，且使用者必須重新驗證，即使工作階段仍處於作用中。此計時器可避開失效的對應，且將取代 **Idle Timer**（閒置計時器）值。 您應該一律將 *Timer*（計時器）的到期值設定為大於 *Idle Timer*（閒置計時器）值。
SSL/TLS 服務設定檔	若要指定防火牆伺服器憑證及允許的通訊協定以保護重新導向要求，請選取 SSL/TLS 服務設定檔（裝置 > 憑證管理 > SSL/TLS 服務設定檔）。如果選取 **None**（無），防火牆會針對 SSL/TLS 連線使用其本機預設憑證。 在 *SSL/TLS* 服務設定檔中，將 *Min Version*（最低版本）設定為 *TLSv1.2* 並將 *Max Version*（最高版本）設定為 *Max*（最高），以針對 *SSL/TLS* 通訊協定漏洞提供最強的安全性。將 *Max Version*（最高版本）設定為 *Max*（最高）可確保當更強大的通訊協定可供使用時，防火牆永遠都會使用最新版本。 若要透通地重新導向使用者而不顯示憑證錯誤，請指派與憑證相關聯的設定檔，該憑證符合您重新導向 web 要求的介面 IP 位址。
驗證設定檔	您可以選取驗證設定檔（裝置 > 驗證設定檔），在使用者的流量符合驗證原則規則（原則 > 驗證）時，對它們進行驗證。不過，您在驗證入口網站設定中選取的驗證設定檔僅適用於參考其中一個預設驗證強制執行物件的規則（Objects（物件）> Authentication（驗證））。這通常是在升級至 PAN-OS 8.0 之後的案例，因為驗證規則最初會參考預設物件。針對驗證強制執行物件的規則，請在您建立物件時，選取驗證設定檔。

© 2019 Palo Alto Networks, Inc.

欄位	說明
供輸入驗證提示 (UDP) 的 GlobalProtect 網路連接埠	指定 GlobalProtect™ 用來從多因素 (MFA) 閘道接收輸入驗證提示的連接埠。（範圍是 1 到 65,536；預設值為 4,501）。若要支援多因素驗證，GlobalProtect 端點必須接收並確認從 MFA 閘道輸入的 UDP 提示。當 GlobalProtect 端點在指定的網路連接埠上接收到 UDP 訊息，且 UDP 訊息是來自受信任的防火牆或閘道時，GlobalProtect 會顯示驗證訊息（請參閱自訂 GlobalProtect 應用程式）。
模式	選取防火牆針對驗證擷取 web 要求的方式： • **Transparent**（透明）—防火牆會根據驗證規則來攔截 Web 要求，並模擬原始目的地 URL，發行 HTTP 401 訊息以提示使用者進行驗證。但是，由於防火牆沒有目的地 URL 的實際憑證，因此瀏覽器會在使用者嘗試存取安全的網站時顯示憑證錯誤。因此，只能在必要時使用此模式，例如 Layer 2 或 Virtual Wire 部署。 • **Redirect**（重新導向）—防火牆會根據驗證規則來攔截 Web 要求，並將它們重新導向至指定的重新導向主機。防火牆會使用 HTTP 302 重新導向來提示使用者進行驗證。最佳做法是使用 **Redirect**（重新導向），因為它提供了更好的終端使用者體驗（不顯示憑證錯誤，並允許使用階段 cookie 使瀏覽不間斷，因為 **Redirect**（重新導向）在連線逾時到期時不會重新對應）。不過，它需要您在指派給進入第三層介面的介面管理設定檔上啟用回應頁面（請參閱 Network（網路）> Network Profiles（網路設定檔）> Interface Mgmt（介面管理）和 PA-7000 Series Layer 3 Interface（PA-7000 系列第三層介面））。 另一項重新導向模式的優勢在於，該模式允許工作階段 Cookie，這可讓使用者持續瀏覽驗證的網站，而無需在每次逾時到期時重新對應。這對在 IP 位址間漫遊的使用者（例如，從企業 LAN 到無線網路）特別實用，因為只要工作階段維持開啟，他們就不需要在 IP 位址變更時重新驗證。 如果驗證入口網站因為瀏覽器僅提供憑證給受信任的站台，而使用 *Kerberos SSO*，就需要 *Redirect*（重新導向）模式。如果驗證入口網站使用多因素驗證 *(MFA)*，也需要 *Redirect*（重新導向）模式。
工作階段 Cookie （僅適用於重新導向模式）	• **Enable**（啟用）—選取此選項可啟用工作階段 Cookie。 • **Timeout**（逾時）—如果您 **Enable**（啟用）工作階段 Cookie，此計時器將以分鐘為單位指定 Cookie 無效的時間（範圍是 60-10,080；預設為 1,440）。 將連線逾時的數值設置得足夠短，以便它不會在 *cookie* 中導致失效的使用者對應項目，但足夠長到不會在工作階段期間多次提示使用者進行登入來提升良好的使用者體驗。從小於或等於 *480* 分鐘（*8* 小時）的數值開始，並根據需要調整數值。 • 漫遊—如果要在 IP 位址變更但工作階段啟動（例如，當端點從有線網路移至無線網路時）的情況下保留 Cookie，請選取此選項。只有當 Cookie 逾時或使用者關閉瀏覽器時，使用者才必須重新驗證。
重新導向主機 （僅適用於重新導向模式）	指定內部網路主機名稱，該名稱將解析為防火牆將要求重新導向的目標 Layer3 介面 IP 位址。 如果使用者透過 *Kerberos* 單一登入 *(SSO)* 進行驗證，*Redirect Host*（重新導向主機）必須與 Kerberos 金鑰頁籤中指定的主機名稱相同。
憑證設定檔	您可以選取憑證設定檔（裝置 > 憑證管理 > 憑證設定檔）在使用者的流量符合驗證原則規則（原則 > 驗證）時，對它們進行驗證。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	若為這種驗證類型，驗證入口網站會提示使用者的端點瀏覽器顯示用戶端憑證。因此，您必須將用戶端憑證部署至每一個使用者系統。此外，在防火牆上，您必須安裝核發用戶端憑證並將 CA 憑證指派給憑證設定檔的憑證授權單位 (CA) 憑證。這是唯一讓 Mac OS 和 Linux 端點啟用透通驗證的驗證方法。

GlobalProtect

GlobalProtect™ 提供完整基礎結構讓您管理行動工作者，讓所有使用者不管使用什麼設備或身在何處，都能夠安全地進行存取。下列防火牆 Web 介面頁面可讓您設定和管理 GlobalProtect 元件：

> Network > GlobalProtect > Portals（網路 > GlobalProtect > 入口網站）
> Network > GlobalProtect > Gateways（網路 > GlobalProtect > 閘道）
> Network > GlobalProtect > MDM（網路 > GlobalProtect > MDM）
> Network > GlobalProtect > Device Block List（網路 > GlobalProtect > 裝置封鎖清單）
> 網路 > GlobalProtect > 無用戶端應用程式
> 網路 > GlobalProtect > 無用戶端應用程式群組
> Objects > GlobalProtect > HIP Objects（物件 > GlobalProtect > HIP 物件）
> Objects > GlobalProtect > HIP Profiles（物件 > GlobalProtect > HIP 設定檔）
> Device > GlobalProtect Client（裝置 > GlobalProtect 用戶端）

想知道更多？

請參閱《GlobalProtect 管理員指南》以深入了解 GlobalProtect，包括 GlobalProtect 基礎結構的設定細節、如何使用主機資訊來強制執行政策，以及 GlobalProtect 一般部署的逐步設定指示。

Network > GlobalProtect > Portals（網路 > GlobalProtect > 入口網站）

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）可設定及管理 GlobalProtect™ 入口網站。入口網站提供 GlobalProtect 基礎結構的管理功能。參與 GlobalProtect 網路的每個端點都會收到其入口網站的組態，包括可用閘道的相關資訊，以及應用程式連線到閘道可能需要的任何用戶端憑證。此外，無論是 Mac 筆記型電腦或是 Windows 端點，入口網站都能為其控制 GlobalProtect 應用程式的行為和散佈。對於 Linux 端點，您必須從支援網站獲取軟體；對於行動裝置，透過 Apple App Store（iOS 裝置）、Google Play（Android 裝置）及 Microsoft Store (Windows Phone) 和其他 Windows UWP 裝置散佈 GlobalProtect 應用程式；對於 Chromebooks，透過 Chromebook 管理主控台或 Google Play 散佈 GlobalProtect 應用程式。

若要新增入口網站組態，請按一下新增開啟 [GlobalProtect 入口網站] 對話方塊。

您想了解什麼內容？	請參閱：
應當為 GlobalProtect 入口網站進行哪些一般設定？	GlobalProtect 入口網站一般頁籤
如何將驗證設定檔指派給入口網站組態？	GlobalProtect 入口網站驗證頁籤
如何定義 GlobalProtect 應用程式從端點收集的資料？	GlobalProtect 入口網站入口資料收集頁籤
我們能夠設定哪些用戶端驗證選項？	GlobalProtect 入口網站代理程式驗證頁籤
如何根據作業系統、使用者及/或使用者群組，將組態指派給特定裝置群組？	GlobalProtect 入口網站代理程式設定選取準則頁籤
如何進行內部閘道設定及優先順序設定？	GlobalProtect 入口網站代理程式內部頁籤
如何進行外部閘道設定及優先順序設定？	GlobalProtect 入口網站代理程式外部頁籤
如何為不同類型的使用者建立獨立的用戶端組態？	GlobalProtect 入口網站代理程式頁籤
我可以對 GlobalProtect 應用程式進行哪些外觀與行為自訂？	GlobalProtect 入口網站代理程式應用程式頁籤
如何設定資料收集選項？	GlobalProtect 入口網站代理程式資料收集頁籤
如何設定 GlobalProtect 入口網站來允許存取 Web 應用程式，而不需安裝 GlobalProtect 應用程式？	GlobalProtect 入口網站無用戶端 VPN 頁籤
如何將 VPN 連結擴展到用作衛星的防火牆？	GlobalProtect 入口網站衛星頁籤
想知道更多？	如需設定入口網站的詳細逐步指示，請參考《*GlobalProtect* 管理員指南》的 < 設定 GlobalProtect 入口網站 >。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站一般頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **General**（一般）

選取 **General**（一般）頁籤，以定義 GlobalProtect 應用程式用於連線到 GlobalProtect 入口網站的網路設定。（選用）您可停用登入頁面或為 GlobalProtect 指定自訂入口網站登入及說明頁面。如需如何建立和匯入自訂頁面的相關資訊，請參考 GlobalProtect 管理員指南的自訂入口網站登入、歡迎和說明頁面。

GlobalProtect 入口網站設定	說明
名稱	輸入入口網站的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	針對處於多個虛擬系統模式的防火牆，**Location**（位置）是虛擬系統 (vsys)，您可在其中使用 GlobalProtect 入口網站。對於未處於多重虛擬系統模式的防火牆，**Location**（位置）選項不可用。儲存入口網站後，您便無法變更 **Location**（位置）。
網路設定	
介面	選取將作為遠端端點與防火牆通訊 ingress 之防火牆介面的名稱。 不要附加允許 *Telenet*、*SSH*、*HTTP* 至一個您已設定 *GlobalProtect* 入口網站或閘道介面上的介面管理設定檔，因為這將會讓管理介面暴露在網際網路中。請參考保護管理存取的最佳實踐方法以了解如何保護存取您管理網路的詳細資料。
IP 位址	指定要用來執行 GlobalProtect 入口網站 Web 服務的 IP 位址。選取 **IP Address Type**（**IP** 位址類型），然後輸入 **IP Address**（**IP** 位址）。 • IP 位址類型可以是 **IPv4**（僅限 IPv4 流量）、**IPv6**（僅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。 • IP 位址必須與 IP 位址類型相容。例如，172.16.1.0（適用於 IPv4）或 21DA:D3:0:2F3b（適用於 IPv6）。 • 如果您選取 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），請輸入其各自適用的 IP 位址類型。
日誌設定	
記錄成功的 SSL 交握	（選用）建立成功的 SSL 解密交握的詳細日誌。預設會停用。 日誌會佔用儲存空間。在記錄成功的 *SSL* 交握之前，請確保具有可用於儲存日誌的資源。編輯 *Device*（裝置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定），以檢查目前的日誌記憶體指派，並在各種日誌類型之間重新指派日誌記憶體。
記錄不成功的 SSL 交握	建立不成功的 SSL 解密交握的詳細日誌，以便您查找解密問題的原因。預設會啟用。 日誌會佔用儲存空間。若要將更多（或更少）日誌儲存空間指派給「解密」日誌，請編輯日誌記憶體指派（*Device*（裝

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站設定	說明
	置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定））。
日誌轉送	指定轉送 GlobalProtect SSL 交握（解密）日誌的方法和位置。
外觀	
入口網站登入頁面	（選用）選取一個供使用者存取入口網站的自訂登入頁面。您可以選取 **factory-default**（原廠預設值）頁面或 **Import**（匯入）自訂頁面。預設值為 **None**（無）。若要防止 Web 瀏覽器存取此頁面，請 **Disable**（停用）此頁面。
入口網站登陸頁面	（選用）選取入口網站的自訂登陸頁面。您可以選取 **factory-default**（原廠預設值）頁面或 **Import**（匯入）自訂頁面。預設值為 **None**（無）。
應用程式說明頁面	（選用）選取一個自訂說明頁面，以協助使用者使用 GlobalProtect。您可以選取 **factory-default**（原廠預設值）頁面或 **Import**（匯入）自訂頁面。GlobalProtect 應用程式軟體提供原廠預設值頁面。如果您選取自訂協助頁面，則 GlobalProtect 入口網站提供 GlobalProtect 入口網站組態的協助頁面。當您將預設值設為 **None**（無）時，GlobalProtect 應用程式會抑制此頁面並從功能表中移除此選項。

GlobalProtect 入口網站驗證組態頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Authentication**（驗證）

選取 **Authentication**（驗證）頁籤以設定一系列 GlobalProtect™ 入口網站設定：

- 入口網站及伺服器用於驗證的 SSL/TLS 服務設定檔。服務設定檔獨立於驗證中的其他設定。
- 唯一驗證計劃主要基於使用者端點的作業系統，其次基於選取性驗證設定檔。
- （選用）**Certificate Profile**（憑證設定檔），可讓 GlobalProtect 使用特定憑證設定檔來驗證使用者。用戶端憑證必須與憑證設定檔相符（如果用戶端憑證為安全性計劃的一部分）。

GlobalProtect 入口網站驗證設定	說明
伺服器驗證	
SSL/TLS 服務設定檔	選取現有 SSL/TLS 服務設定檔。設定檔指定憑證及允許的通訊協定來保障管理介面上的流量安全性。通用名稱 (CN) 及（如果適用）與設定檔關聯的憑證 Alternative Name（主旨替代名稱）(SAN) 欄位，必須符合您在 **General**（一般）頁籤所選 **Interface**（介面）的 IP 位址或 FQDN。 在 *GlobalProtect VPN* 組態中，使用與受信任第三方 *CA* 憑證關聯的設定檔，或您的內部企業 *CA* 所產生的憑證。
用戶端驗證	
名稱	輸入用於識別用戶端驗證組態的名稱。（用戶端驗證組態獨立於 SSL/TLS 服務設定檔。）

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站驗證設定	說明
	您可建立多個用戶端驗證組態並主要依作業系統來區分，其次依唯一的驗證設定檔來區分（對於相同的作業系統）。例如，您不僅可為不同的作業系統新增用戶端驗證組態，而且可將不同的組態用於依唯一驗證設定檔區分的相同作業系統。（您應當從最具體到最一般對這些設定檔排序。例如，所有使用者及任何作業系統為最一般。） 您也可以在 **pre-logon**（預先登入）模式中建立 GlobalProtect 部署到應用程式的組態（在使用者已登入系統之前），或要套用到任何使用者的組態。（預先登入建立到 GlobalProtect 閘道的 VPN 通道，使用者才可登入 GlobalProtect。）
作業系統	若要在端點上部署特定於作業系統 (OS) 的用戶端驗證設定檔，請 **Add**（新增）作業系統（**Any**（任何）、**Android**, **Chrome**、**iOS**、**Linux**、**Mac**、**Windows**，或 **WindowsUWP**）。作業系統是組態間的差異因素。（請參閱驗證設定檔進一步了解差異。） **Browser**（瀏覽）及 **Satellite**（衛星）的其他選項可讓您指定用於特定案例的驗證設定檔。選取 **Browser**（瀏覽）可指定驗證設定檔，用於驗證從 Web 瀏覽器存取入口網站以便下載 GlobalProtect 應用程式（Windows 及 Mac）的使用者。選取 **Satellite**（衛星）可指定用於驗證衛星 (LSVPN) 的驗證設定檔。
驗證設定檔	除了依作業系統區分用戶端驗證組態，您還可指定驗證設定檔來進一步區分。（您可建立 **New Authentication Profile**（新驗證設定檔）或選取現有設定檔。）若要為作業系統設定多個驗證選項，您可建立多個用戶端驗證設定檔。 如果您在 *Gateways*（閘道）設定了 *LSVPN*，您將無法儲存該組態，除非您在此處選取了驗證設定檔。此外，如果您計劃使用序號來驗證衛星，無法尋找或驗證防火牆序號時，入口網站必須擁有可用的驗證設定檔。 另請參閱 [裝置 > 驗證設定檔]。
使用者名稱頁籤	指定 GlobalProtect 入口網站登入自訂使用者名稱頁籤。舉例來說，使用者名稱（僅限）或電子郵件位址（使用者名稱@網域）。
密碼頁籤	指定 GlobalProtect 入口網站登入自訂密碼頁籤。例如：密碼（土耳其文）或 **Passcode**（雙因子、以權杖為主的認證）。
驗證訊息	為幫助使用者了解其登入所需的認證類型，請輸入訊息或保留預設訊息。訊息最大長度為 256 個字元。
允許使用使用者認證或用戶端憑證進行驗證	如果您選取 **No**（否），則使用者必須使用使用者憑證以及用戶端憑證對閘道進行驗證。如果您選取**Yes**（是），則使用者可以使用使用者憑證或用戶端憑證對閘道進行驗證。
憑證設定檔	
憑證設定檔	（選用）選取入口網站用於比對這些來自使用者端點之用戶端憑證的 **Certificate Profile**（憑證設定檔）。只有當用戶端憑證與憑證設定檔相符時，入口網站才可使用此設定檔來驗證使用者。 如果您將**Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **No**（否），您則必須選取 **Certificate Profile**（憑證設定檔）。如果您將**Allow Authentication with User**

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站驗證設定	說明
	Credentials OR Client Certificate（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **Yes**（是），**Certificate Profile**（憑證設定檔）則是可選項。 憑證設定檔獨立於作業系統。此外，即使您啟用驗證取代，此設定檔仍可運作。

GlobalProtect 入口網站入口資料收集頁籤

選取 **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> **<portal-config>** > **Portal Data Collection**（入口網站資料收集），可定義 GlobalProtect 應用程式從端點收集且在使用者成功登入入口網站後於設定選取條件資料內傳送的資料。

GlobalProtect 入口網站資料收集設定	說明
憑證設定檔	選取 GlobalProtect 入口網站使用的憑證設定檔與 GlobalProtect 應用程式傳送的機械憑證比對。
自訂檢查	定義應用程式所要收集的自訂主機資訊： • **Windows—Add**（新增）特殊登錄機碼或金鑰值的檢查。 • **Mac—Add**（新增）特殊 plist 機碼或金鑰值的檢查。

GlobalProtect 入口網站代理程式頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）

選取 **Agent**（代理程式）頁籤，以定義代理程式組態設定。GlobalProtect 入口網站將於首次建立連線後部署裝置組態。

您還可以指定入口網站自動部署受信任的根憑證授權單位 (CA) 憑證與中繼憑證。如果端點不信任 GlobalProtect 閘道及 GlobalProtect Mobile Security Manager 使用的伺服器憑證，則端點需要這些憑證來建立與找到或 Mobile Security Manager 的 HTTPS 連線。入口網站將您在此指定的憑證推送至具有該用戶端組態的用戶端。

若要新增受信任的根 CA 憑證，請 **Add**（新增）現有憑證或 **Import**（匯入）新憑證。若要在儲存於用戶端的憑證中安裝（以透明方式）需要 SSL 轉送 Proxy 解密的受信任根 CA 憑證，請選取 **Install in Local Root Certificate Store**（在本機根憑證存放區中安裝）。

指定 *GlobalProtect* 應用程式用於驗證 *GlobalProtect* 入口網站和閘道身份的受信任根 *CA* 憑證。如果入口網站和閘道提供的憑證尚未由發佈受信任的根 *CA* 的同一憑證授權單位簽署或發佈，則 *GlobalProtect* 應用程式無法與入口網站和閘道建立連線。

如果具有需要不同組態的不同使用者類別，您可建立獨立的代理程式組態來支援它們。入口網站隨後會使用使用者名稱或群組名稱，以及用戶端的作業系統來決定要部署的代理程式組態。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。入口網站找到符合項時，會將對應的組態傳遞給應用程式。因此，如果您有多個代理程式組態，請務必排序這些設定，讓更特殊的組態（即適用於特定使用者或作業系統的組態）比更常見的組態優先適用。使用 **Move Up**（上移）和 **Move Down**（下移）來對組態重新排序。視需要 **Add**（新增）新代理程式組態。如需設定入口網站和建立代理程式組態的詳細資訊，請參考《GlobalProtect 管理員指南》的 **<** GlobalProtect 入口網站 **>**。當您 **Add**（新增）代理程式組態或修改現有設定時，**Configs**（設定）視窗會隨即開啟，並顯示五個頁籤，如下表所述：

© 2019 Palo Alto Networks, Inc.

- GlobalProtect 入口網站代理程式驗證頁籤
- GlobalProtect 入口網站代理程式設定選取準則頁籤
- GlobalProtect 入口網站代理程式內部頁籤
- GlobalProtect 入口網站代理程式外部頁籤
- GlobalProtect 入口網站代理程式應用程式頁籤
- GlobalProtect 入口網站代理程式 HIP 資料收集頁籤

GlobalProtect 入口網站代理程式驗證頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **Authentication**（驗證）

選取 **Authentication**（驗證）頁籤，以設定套用於代理程式組態的驗證設定。

GlobalProtect 入口網站用戶端驗證組態設定	說明
驗證頁籤	
名稱	為此用戶端驗證組態輸入描述性名稱。
用戶端憑證	（選用）選取將用戶端憑證散佈到端點的來源，接著會將憑證提供給閘道。如果您設定相互 SSL 驗證，將需要用戶端憑證。 如果在入口網站用戶端組態中為預先登入設定 SCEP，入口網站將產生儲存於系統憑證存放區的機器憑證，以進行閘道驗證與連線。 若要使用防火牆的 **Local**（本機）憑證，而非透過 **SCEP** 從 PKI 產生的憑證，請選取已上傳至防火牆的憑證。 如果使用內部 CA 將憑證散佈到端點，請選取 **None**（無）（預設值）。當您選取 **None**（無）時，入口網站不推送憑證至端點。
儲存使用者認證	選取 **Yes**（是）在應用程式上儲存使用者名稱及密碼，或選取 **No**（否）在每次連線時強制使用者提供密碼，以透明方式透過端點或手動輸入一個。選取 **Save Username Only**（僅儲存使用者名稱）可在每次使用者連線時僅儲存使用者名稱。選取 **Only with User Fingerprint**（僅透過使用者的指紋）以允許生物登入。在端點上啟用了生物登入時，GlobalProtect 會在指紋符合端點上受信任的指紋範本時使用已儲存的認證。 請勿儲存使用者憑證，因為這會使未經授權的使用者更容易存取敏感資源和機密資訊。使用者每次連線至 *GlobalProtect* 時都應手動輸入憑證。
驗證覆寫	
產生 Cookie 以供驗證取代	選取此選項可設定入口網站，用於產生加密的端點特定 Cookie。使用者首次驗證入口網站之後，入口網站會將 Cookie 傳送至端點。
接受 Cookie 以供驗證取代	選取此選項可設定防火牆透過有效的加密 Cookie 來驗證端點。端點提供有效的 Cookie 後，入口網站可驗證透過入口網站加密的 Cookie，解密 Cookie，接著驗證使用者。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站用戶端驗證組態設定	說明
Cookie 生命週期	指定 cookie 有效的小時數、天數或週數。生命週期一般為 24 小時。範圍是 1–72 小時，1–52 週或 1–365 天。Cookie 到期後，使用者必須輸入登入認證，入口網站隨後會對新 Cookie 加密以傳送至使用者端點。
加密/解密 Cookie 的憑證	選取要用於加密與解密 Cookie 的憑證。 確保入口網站及閘道使用相同的憑證來加密與解密 *Cookie*。（將憑證設定為閘道用戶端組態的一部分。請參閱 *[網路 > GlobalProtect > 閘道]*。
需要動態密碼（雙因素驗證）的元件	
若要設定 GlobalProtect 支援動態密碼（例如一次性密碼 (OTPs)），請指定入口網站或閘道需要使用者輸入動態密碼。若啟用雙因素驗證，GlobalProtect 將運用採用登入認證（例如 AD）與憑證的常規驗證。 啟用入口網站或雙因素驗證閘道類型後，入口網站或閘道將在進行初始入口網站驗證之後，提示使用者提交認證與第二個 OTP（或其他動態密碼）。 然而，如果您也啟用了驗證取代，將會使用加密 Cookie 來驗證使用者（首次驗證使用者的新工作階段之後），從而先佔使用者需求以重新輸入認證（只要 Cookie 有效）。因此，只要 Cookie 有效，使用者將在必要時以透明方式登入。指定 Cookie 的生命週期。	
入口網站	選取此選項可使用動態密碼來連線至入口網站。
內部閘道—全部	選取此選項可使用動態密碼來連線至內部閘道。
外部閘道 - 僅限手動	選取此選項可使用動態密碼來連線至設定為 **Manual**（手動）閘道的外部閘道。
外部閘道—自動發現	選取此選項可使用動態密碼來連線至任何剩餘外部閘道，應用程式可自動探索未設定為 **Manual**（手動）的閘道。

GlobalProtect 入口網站代理程式設定選取準則頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **Config Selection Criteria**（設定選取條件）

選取 **Config Selection Criteria**（設定選取條件）頁籤，以設定用於在具有管理和非管理端點的部署中識別端點類型的相符準則。入口網站可以根據端點類型將指定的組態推送到端點。

GlobalProtect 入口網站設定選取條件設定	說明
使用者/使用者群組頁籤	
作業系統	**Add**（新增）一個或多個端點作業系統 (OS) 以指定哪些端點接收此組態。入口網站自動記住端點的作業系統，並將該作業系統的詳細資訊納入用戶端組態中。您可選取 **Any**（任何）作業系統或特定作業系統

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站設定選取條件設定	說明
	（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows** 或 **WindowsUWP**）。
使用者/使用者群組	**Add**（新增）此組態要套用的特定使用者或使用者群組。 您必須先設定群組對映（*Device*（裝置）> *User Identification*（使用者識別）> *Group Mapping Settings*（群組對映設定）），才能選取使用者群組。 若要將此組態部署到所有使用者，請從 **User/User Group**（使用者/使用者群組）下拉式清單中選取 **any**（任何）。若要在預先登入模式下將此組態僅部署到使用 GlobalProtect 應用程式的使用者，請從 **User/User Group**（使用者/使用者群組）下拉式清單中選取 **pre-logon**（預先登入）。
裝置檢查	
機器帳戶存在，其裝置序號為	根據 Active Directory 中是否存在端點序號來設定相符準則。
憑證設定檔	選取 GlobalProtect 入口網站使用的憑證設定檔與 GlobalProtect 應用程式傳送的機械憑證比對。
自訂檢查	
自訂檢查	選取此選項可定義要比對的自訂主機資訊。
登錄機碼	若要在 Windows 端點中檢查特定的登錄機碼，請 **Add**（新增）要比對的 **Registry Key**（登錄機碼）。若只要比對缺少指定登錄機碼或機碼值的端點，請啟用 **Key does not exist or match the specified value data**（機碼不存在或不符合指定的值資料）選項。若要比對特定值，**Add**（新增）**Registry Value**（登錄值）和 **Value Data**（值資料）。若要比對確實沒有指定值或值資料的端點，請選取 **Negate**（否定）。
Plist	若要在 macOS 端點中檢查屬性清單 (plist) 中的特定項目，請 **Add**（新增）**Plist** 名稱。若只比對沒有指定 plist 的端點，請啟用 **Plist does not exist**（**Plist** 不存在）選項。若要比對 plist 內的特定機碼值組，請 **Add**（新增） **Key**（機碼）和對應 **Value**（值）。若要比對確實沒有指定機碼或值的端點，請選取 **Negate**（否定）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站代理程式內部頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **Internal**（內部）

選取 **Internal**（內部）頁籤以設定代理程式組態的內部閘道設定。

GlobalProtect 入口網站內部設定	說明
內部主機偵測	
內部主機偵測	選取此選項可讓 GlobalProtect 應用程式判定其是否在企業網路中。此選項僅套用於設定為與內部閘道通訊的端點，並且是對這些端點的最好做法。 當使用者嘗試登入時，應用程式使用指定為特定 **IP Address**（**IP** 位址）的 **Hostname**（主機名稱）執行內部主機的反向 DNS 查詢。如果端點在企業網路中，主機將用作可到達的參考點。如果應用程式發現主機，端點則在網路中且應用程式連線至內部閘道；如果應用程式未能找到內部主機，則端點不在網路中且應用程式建立到其中一個外部閘道的通道。 • IP 位址類型可以是 **IPv4**（僅限 IPv4 流量）、**IPv6**（僅限 IPv6 流量）或兩者兼具。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4** 和 **IPv6**。 • IP 位址必須與 IP 位址類型相容。例如，172.16.1.0（適用於 IPv4）或 21DA:D3:0:2F3b（適用於 IPv6）。 • 如果您選取 **IPv4** 和 **IPv6**，請輸入其各自適用的 IP 位址類型。
主機名稱	輸入在內部網路中解析為以上 IP 位址的 **Hostname**（主機名稱）。
內部閘道	
指定應用程式要求存取的內部閘道，還可提供 HIP 報告（如果在 GlobalProtect Portals Agent Data Collection Tab（GlobalProtect 入口網站代理程式資料收集頁籤）中啟用了 HIP）。	**Add**（新增）包括下列資訊的內部閘道： • 名稱 — 用來識別閘道的頁籤（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 • 位址—閘道的 IP 位址或防火牆介面 FQDN。該值必須與閘道伺服器憑證中的通用名稱 (CN) 與 SAN（如指定）相符。例如，如果使用 FQDN 來產生憑證，您必須在此處輸入 FQDN。 • 來源位址—端點的來源位址或位址集區。當使用者連線時，GlobalProtect 會辨識裝置的來源位址。只有 IP 位址已納入來源位址集區的 GlobalProtect 應用程式可以驗證此閘道，並傳送 HIP 報告。 • **DHCP** 選項 **43** 代碼（僅限 Windows 和 Mac）—用於選取閘道的 DHCP 子選項代碼。指定一或多個子選項代碼（以 10 進位表示）。GlobalProtect 應用程式會從子選項代碼所定義的值中讀取閘道位址。

GlobalProtect 入口網站代理程式外部頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **External**（外部）

選取 **External**（外部）頁籤以設定代理程式組態的外部閘道設定。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站外部設定	說明
截止時間（秒）	指定應用程式在選取最佳閘道之前，等候所有可用閘道回應的秒數。對於隨後的連線請求，應用程式嘗試僅連線在截止之前回應的這些閘道。值為 0 表示應用程式使用 **App**（應用程式）頁籤中 **AppConfigurations**（應用程式組態）內的 **TCP Connection Timeout**（**TCP** 連線逾時）（範圍是 0 到 10；預設為 5）。
外部閘道	
指定當不在企業網路時建立通道，應用程式可嘗試連線的防火牆清單。	**Add**（新增）包括下列資訊的外部閘道： • 名稱 — 用來識別閘道的頁籤（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。 • 位址—閘道設定所在的防火牆介面 IP 位址或 FQDN。該值必須與閘道伺服器憑證中的 CN（與 SAN（如指定））相符。例如，如果使用 FQDN 來產生憑證，您還必須在此處輸入 FQDN。 • 來源區域—端點的來源區域。當使用者連線時，GlobalProtect 會辨識端點所在區域，並只允許使用者連線到針對該區域所設定的閘道。在選取閘道時，會先考慮使用來源閘道，然後才是閘道優先順序。 • 優先順序—選取值（**Highest**（最高）、**High**（高）、**Medium**（中）、**Low**（低）、**Lowest**（最低）或 **Manual only**（僅限手動））以協助應用程式判斷要使用的閘道。**Manual only**（僅限手動）可防止 GlobalProtect 應用程式在用戶端啟用了 **Auto Discovery**（自動發現）時，嘗試連線到此閘道。此應用程式將首先聯絡所有擁有 **Highest**（最高）、**High**（高）或 **Medium**（中）優先順序的特定閘道，並建立提供最快回應閘道的通道。若較高優先順序閘道無法聯絡，則應用程式接下來會聯絡任何較低優先順序的閘道（除 **Manual only**（僅限手動）閘道外）。 • 手動—選取此選項可讓使用者手動選取（或切換至）閘道。GlobalProtect 應用程式可連線至任何設定為 **Manual**（手動）的外部閘道。當應用程式連線至其他閘道時，現有通道將斷開連線且建立新通道。手動閘道也可以有主要閘道以外的其他驗證機制。如果重新啟動端點，或如果執行重新發現，GlobalProtect 應用程式將會連線至主要閘道。如果有一組需要暫時連線至特定閘道以存取網路之安全區段的使用者，此功能非常有用。
第三方 VPN	
第三方 VPN	若要導向 GlobalProtect 應用程式以略過選取的第三方 VPN 用戶端，以便 GlobalProtect 不與其產生衝突，請 **Add**（新增）該 VPN 用戶端的名稱：從清單中選取名稱，或在提供的欄位輸入名稱。如果您設定此功能，GlobalProtect 將略過指定 VPN 用戶端的路由設定。

GlobalProtect 入口網站代理程式應用程式頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **App**（應用程式）

選取 **App**（應用程式）頁籤，指定一般使用者如何與其系統上所安裝的 GlobalProtect 應用程式互動。針對您所建立的不同 GlobalProtect 代理程式組態，您也可以定義不同的應用程式設定。請參閱 GlobalProtect 管理員指南，進一步了解有關 GlobalProtect 應用程式自訂設定最新的更新資訊。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
歡迎頁面	選取在連線到 GlobalProtect 後，向終端使用者展示的歡迎頁面。您可以選取 **factory-default**（原廠預設值）頁面或 **Import**（匯入）自訂頁面。預設值為 **None**（無）。
應用程式組態	

連接方法	• 視需要（手動使用者啟動的連線）— 使用者必須啟動 GlobalProtect 應用程式，然後啟動到入口網站的連線並輸入其 GlobalProtect 認證。此選項主要用於遠端存取的連線。
	• 使用者登入（始終開啟）— GlobalProtect 應用程式在使用者登入端點後自動與入口網站建立連線。入口網站透過向應用程式提供適當的代理程式組態做出回應。隨後，應用程式會將通道設定為從入口網站接收的代理程式組態中指定的其中一個閘道。
	• 預先登入—預先登入可確保遠端的 Windows 和 Mac 使用者永遠會連線到公司網路，並在使用者登入端點時啟用使用者登入指令碼和網域原則的應用程式。因為端點能夠以彷彿位於內部的方式連線到公司網路，因此使用者可以在其密碼過期時，使用新的密碼來登入，或是在忘記密碼時獲得復原密碼的協助。GlobalProtect 應用程式會先使用預先登入建立 VPN 通道至 GlobalProtect 閘道，才讓使用者登入端點；端點會透過向閘道提交預先安裝的機器憑證來要求驗證。然後，在 Windows 端點上，閘道會將 VPN 通道從預先登入使用者重新指派給已登入端點的使用者名稱；而在 Mac 端點上，應用程式則會先中斷連線再為使用者建立新的 VPN 通道。
	
	預先登入有兩種連線方法，不論是哪一種，都能啟用相同的預先登入功能，系統會先執行此功能，再讓使用者登入端點。不過，在使用者登入端點後，預先登入連線方法就會決定要在何時建立 GlobalProtect 應用程式連線：
	
	  • 預先登入（一律開啟）—GlobalProtect 應用程式會自動嘗試對 GlobalProtect 閘道進行連線和重新連線。行動裝置不支援預先登入功能，因此，如果您指定了這種連線方法，系統會將它預設為 **User-logon (Always On)**（使用者登入（一律開啟））連線方法。
	  • **Pre-logon then On-demand**（預先登入後依需求）—使用者必須開啟 GlobalProtect 應用程式，然後手動啟動連線。行動裝置不支援預先登入功能，因此，如果您指定了這種連線方法，系統會將它預設為 **On-demand (Manual user initiated connection)**（視需要（手動使用者啟動的連線））連線方法。

GlobalProtect 應用程式配置刷新時間間隔（小時）	指定 GlobalProtect 入口網站重新整理應用程式組態之前的等候小時數（範圍是 1 至 168；預設為 24）。
允許使用者禁用 GlobalProtect 應用程式	指定是否允許使用者停用 GlobalProtect 應用程式程式，如果是，停用應用程式之前，必須執行哪些動作： • 允許 — 允許任何使用者視需停用 GlobalProtect 應用程式。 • 不允許 — 不允許使用者停用 GlobalProtect 應用程式。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	• 允許但須提供註解—允許使用者在其端點上停用 GlobalProtect 應用程式，但需要其提交停用應用程式的原因。 • 允許但須提供密碼—允許使用者輸入密碼來停用 GlobalProtect 或應用程式。此選項需要使用者輸入並確認密碼值，例如，輸入時不顯示密碼。通常，管理員發生意外或非預期事件之前向使用者提供密碼，以免使用者使用 GlobalProtect VPN 連線網路。您可透過電子郵件或發佈於組織網站上的公告來提供密碼。 • 允許且須提供票証 — 此選項可啟用挑戰回應機制，使用者嘗試停用 GlobalProtect 後，端點將顯示 8 字元十六進位票証要求號碼。使用者必須聯絡防火牆管理員或支援團隊（最好透過電話聯絡以確保安全性）並提供該號碼。從防火牆 (**Network**（網路）> **GlobalProtect** > **Portals**（入口網站）)，管理員或支援人員接著可以按一下 **Generate Ticket**（一般票證）並輸入此票證 **Request**（請求） 號碼以獲得**Ticket**（票證） 編號（也是 8 位元十六進位號碼）。管理員或支援人員向使用者提供該票證號碼，使用者接著可將它輸入到挑戰欄位以停用應用程式。
允許使用者解除安裝 GlobalProtect 應用程式	指定是否允許使用者解除安裝 GlobalProtect 應用程式程式，如果是，解除安裝應用程式之前，必須執行哪些動作： • **Allow**（允許）—允許任何使用者視需解除安裝 GlobalProtect 應用程式。 • **Disallow**（不允許）—不允許終端使用者解除安裝 GlobalProtect 應用程式。 • **Allow with Password**（允許但須提供密碼）—強制要求輸入密碼才能解除安裝 GlobalProtect 應用程式。此選項需要使用者輸入並確認密碼，然後才能繼續執行解除安裝作業。您可透過電子郵件或發佈於組織網站上的公告來提供密碼。 此選項需要內容發行版本 8196-5685 版及以上。
允許使用者升級 GlobalProtect 應用程	指定終端使用者是否可升級 GlobalProtect 應用程式軟體，如果可以，它們是否可選取升級時間： • 不允許 — 防止使用者升級應用程式軟體。 • 允許手動 — 允許使用者手動檢查，並在 GlobalProtect 應用程式中選取 **Check Version**（檢查版本）來啟動升級。 • 允許（提示時）（預設值）—防火牆啟動新版本時提示使用者，並允許使用者在方便時升級其軟體。 • 允許（以透明方式）—每當入口網站上有可用的新版本時，即自動升級應用程式軟體。 • 內部—每當入口網站中有新版本可用，等到端點內部連線到公司網路後，就自動升級應用程式軟體。這可防止因為連線頻寬不足而在升級時導致系統延遲。
允許使用者登出 GlobalProtect 應用程式 （僅限 Windows、macOS、iOS、Android 和 Chrome）	指定是否允許使用者手動登出 GlobalProtect 應用程式。 • **Yes**（是）—允許任何使用者視需登出 GlobalProtect 應用程式。 • **No**（否） — 不允許使用者登出 GlobalProtect 應用程式。 此選項需要內容發行版本 8196-5685 版及以上。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
使用單一登入 (Windows)	選取 **No**（否）以停用單一登入 (SSO)。啟用 SSO（預設）後，GlobalProtect 應用程式會自動使用 Windows 登入認證進行驗證，然後連線至 GlobalProtect 入口網站與閘道。GlobalProtect 也可封裝協力廠商認證，以確保即使是正在使用協力廠商認證提供者來封裝 Windows 登入認證時，Windows 使用者仍會驗證與連線。
使用單一登入 (macOS)	選取 **No**（否）以停用單一登入 (SSO)。啟用 SSO（預設）後，GlobalProtect 應用程式會自動使用 macOS 登入認證進行驗證，然後連線至 GlobalProtect 入口網站與閘道。 此選項需要內容發行版本 8196-5685 版及以上。
登出時清空單一登入認證 （僅限 Windows）	選取 **No**（否）可在使用者登出時保留單一登入認證。選取 **Yes**（是）（預設值）可清除認證，並強制使用者在下次登入時輸入認證。
Kerberos 身份驗證失敗時使用預設身份驗證	選取 **No**（否）可僅使用 Kerberos 驗證。選取 **Yes**（是）（預設值）可在驗證 Kerberos 失敗後，使用預設驗證方法重新驗證。此功能僅支援 Windows 和 Mac 端點。
VPN 連線逾時自動復原	輸入從 0 到 180 的逾時值（分鐘）以指定 GlobalProtect 應用程式在通道因為網路不穩定或端點狀態透過輸入而改變而採取的行動；預設值為 30。 • 0—停用此功能，使得 GlobalProtect 在通道斷開連線後不會嘗試重新建立通道。 • 1-180—啟用此功能，使得 GlobalProtect 在通道關閉一段未超出您在這裡指定的逾時時間時，會嘗試重新建立通道連線。例如，若逾時時間為 30 分鐘，GlobalProtect 在通道斷開連線 45 分鐘的情況下，不會嘗試新建立通道。然而，如果通道中斷連線 15 分鐘，因為斷線分鐘數並沒有超過逾時值，GlobalProtect 會嘗試重新連線。 透過一直開啟的 *VPN*，如果使用者在逾時值到期之前，從外部網路切換至內部網路，*GlobalProtect* 不會執行網路重新搜索。如此，*GlobalProtect* 重新建立通道至最後得知的外部閘道。若要觸發內部主機偵測，使用者必須從 *GlobalProtect* 主控台選取 *[重新發現網路]*。
VPN 連線復原嘗試之間的等待時間	以秒為單位輸入時間值，當您啟用 **Automatic Restoration of VPN Connection Timeout**（VPN 連線逾時自動復原）時，GlobalProtect 應用程式在嘗試重新建立與最後一次連線閘道間的等候時間。依據您的網路狀況，指定較長或較短的等候時間。範圍是 1 到 60；預設值為 5。
對網路存取執行 GlobalProtect 連線	選取 **Yes**（是）以強制讓所有網路流量周遊 GlobalProtect 通道。如果網路存取無需 GlobalProtect 且 GlobalProtect 停用或中斷連線時，使用者仍可存取網際網路，則選取 **No**（否）（預設值）。 若要在流量被封鎖之前為使用者提供說明，設定 **Traffic Blocking Notification Message**（流量封鎖通知訊息）並選取指定何時顯

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	示此訊息 (**Traffic Blocking Notification Delay**（流量封鎖通知延遲）)。 若要允許所需流量建立與網頁認證的連線，請指定一個 **Captive Portal Exception Timeout**（被控制的入口網站例外逾時）。使用者必須在逾時之前驗證入口網站。如要提供額外指示，請設定 **Captive Portal Detection Message**（被控制的入口網站偵測訊息），並可選取指定何時顯示訊息 **Captive Portal Notification Delay**（被控制的入口網站通知延遲）。 大多數情況中，使用預設選項 *No*（否）。選取 *Yes*（是）會阻擋所有來自以及流向端點的網路流量，直到應用程式連接到企業內的內部閘道或企業網路外的外部閘道。
已啟用對網路存取執行 **GlobalProtect** 連線並且未建立 **GlobalProtect** 連線時允許流向指定主機/網絡的流量	如果需要，當您執行 GlobalProtect 以存取網路但未建立連線時，您可以設定最多 10 個您想要允許存取的 IP 位址或網路區段。使用逗號來區隔多個值。排除可讓使用者在 GlobalProtect 中斷連線時存取本機資源，從而提高使用者體驗。例如，當 GlobalProtect 未連線時，GlobalProtect 可以排除連結-本機位址，以允許存取連結本機網路區段或廣播網域。
網頁驗證例外逾時（秒）	若要強制使用 GlobalProtect 來進行網路存取，但要提供寬限期讓使用者有足夠的時間來連線到被控制的入口網站，請以秒為單位指定逾時值（範圍是 0 到 3600）。例如，值為 60 表示，在 GlobalProtect 偵測到被控制的入口網站後，使用者必須在 1 分鐘內登入到被控制的入口網站。值為 0 表示，GlobalProtect 不允許使用者連線到被控制的入口網站，且會立即封鎖存取。
在執行被控制的入口網站偵測時自動在預設瀏覽器中啟動網頁	若要在執行被控制的入口網站偵測時自動啟動預設網頁瀏覽器，以便使用者可以無縫登入至被控制的入口網站，請輸入您想要用於進行初次連線嘗試的網站的完全合格網域名稱 (FQDN) 或 IP 位址，以在預設 Web 瀏覽器啟動時啟動 Web 流量（最大長度為 256 個字元）。然後，網頁驗證會攔截此網站連線嘗試，并將預設 Web 瀏覽器重新導向至網頁驗證登入頁面。若此欄位為空（預設），則 GlobalProtect 不會在網頁驗證偵測時自動啟動預設 Web 瀏覽器。
流量封鎖通知延遲（秒）	以秒為單位來指定值，以決定要在何時顯示通知訊息。GlobalProtect 會在可以連線到網路後，開始倒數計時顯示通知的時間（範圍是 5 到 120；預設為 15）。
顯示流量封鎖通知訊息	指定在必須使用 GlobalProtect 來進行網路存取時，是否要顯示訊息。選取 **No**（否）以停用訊息。選取 **Yes**（是）可啟用訊息（GlobalProtect 會在自身已中斷連線卻偵測到可以連線到網路時顯示此訊息）。
流量封鎖通知訊息	自訂通知訊息，在必須使用 GlobalProtect 來進行網路存取時，對使用者顯示此訊息。GlobalProtect 會在自身已中斷連線卻偵測到可以連線到網路時顯示此訊息。此訊息會指出為何要封鎖流量，並提供如何連線的指示。例如：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	`To access the network, you much first connect to GlobalProtect.` 此訊息必須為 512 個或更少的字元。
允許使用者屏除流量封鎖通知	選取 **No**（否）以始終顯示流量封鎖通知。依預設，此值會設為 **Yes**（是），亦即允許使用者關閉通知。
顯示被控制的入口網站偵測訊息	指定當 GlobalProtect 偵測到被控制的入口網站時，是否要顯示訊息。選取 **Yes**（是）以顯示訊息。選取 **No**（否）（預設值）以隱藏訊息（GlobalProtect 不會在偵測到被控制的入口網站時顯示訊息）。 如果您啟用被控制的入口網站偵測訊息，系統會在被控制的入口網站例外逾時到達前 *85* 秒顯示訊息。因此，如果被控制的入口網站例外逾時是 *90* 秒或更短的時間，則系統會在偵測到被控制的入口網站後經過 *5* 秒時顯示訊息。
網頁驗證偵測訊息	自訂通知訊息，以在 GlobalProtect 所偵測到的網路另外指示要連線到被控制的入口網站時，對使用者顯示此訊息。例如： `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.` 此訊息必須為 512 個或更少的字元。
被控制的入口網站偵測延遲	如果您啟用被控制的入口網站偵測訊息，則可以指定被控制的入口網站偵測之後 GlobalProtect 顯示偵測訊息的延遲（以秒為單位）（範圍是 1-120；預設值為 5）。
用戶端憑證商店查找	選取憑證類型，或應用程式在其個人憑證存放區查詢的憑證。GlobalProtect 應用程式使用憑證來驗證入口網站或閘道，然後建立到 GlobalProtect 閘道的 VPN 通道。 • 使用者—透過使用者帳戶的本機憑證進行驗證。 • 機器 — 透過端點的本機憑證進行驗證。此憑證套用於允許使用端點的所有使用者帳戶。 • 使用者與機器（預設值）—透過使用者憑證與機器憑證進行驗證。
SCEP 憑證更新週期（天數）	此機制用於在憑證實際到期之前更新 SCEP 產生的憑證。指定憑證到期前入口網站可從 PKI 系統中的 SCEP 伺服器要求新憑證的最大天數（範圍是 0 到 30；預設為 7）。值 0 表示入口網站在重新整理用戶端組態時，不會自動更新用戶端憑證。 對於取得新憑證的應用程式，使用者必須在更新期間登入（入口網站在此更新期間不要求使用者提供新憑證，除非使用者已登入）。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	例如，假設用戶端憑證的使用期限為 90 天，且此憑證更新期為 7 天。如果使用者在憑證使用期限的最後 7 天內登入，入口網站會產生憑證並與重新整理的用戶端組態一起下載憑證。請參閱 GlobalProtect 應用程式設定重新整理時間間隔（小時）。
用戶端憑證擴充金鑰使用物件識別碼 (OID)	透過指定用戶端憑證擴充金鑰使用物件識別碼 (OID) 輸入。此設定可確保 GlobalProtect 應用程式只選取用於用戶端驗證的憑證，並讓 GlobalProtect 儲存該憑證供日後使用。
在移除智慧卡上保持連線 （僅限 Windows）	選取 **Yes**（是）可在使用者移除包含用戶端憑證的智慧卡時保持連線。選取 **No**（否）（預設值）則可在使用者移除智慧卡時終止連線。
允許覆蓋用戶端憑證中的使用者名稱	選取 **No**（否）以強制 GlobalProtect 使用用戶端憑證中的使用者名稱，阻止 GlobalProtect 覆蓋該使用者名稱（預設啟用）。
啟用進階視圖	選取 **No**（否）可將應用程式的使用者介面限制為最基本檢視。
允許使用者屏除歡迎頁	選取 **No**（否）可在每次使用者啟動連線時，強制顯示歡迎頁面。此限制可防止使用者關閉重要資訊，例如組織需要用於保持遵守的條款和條件。
啟用重新發現網路選項	選取 **No**（否）可防止使用者手動啟動網路重新探索。
啟用 Resubmit Host Profile（重新提交主機設定檔）選項	選取 **No**（否）可防止使用者手動觸發最新 HIP 的重新提交。
允許使用者更改入口網站位址	選取 **No**（否）會在 GlobalProtect 應用程式中停用 **Home**（首頁）頁籤的 **Portal**（入口網站）欄位。然而，由於使用者接著將無法指定入口網站進行連線，因此您必須在 Windows 登錄或 Mac plist 中提供預設的入口網站位址： • **Windows 登錄**—`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` with key `Portal` • **Mac plist**—`/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` with key `Portal` 如需關於預先部署入口網站位址的詳細資訊，請參閱《GlobalProtect 管理員指南》中的 < 可自訂的應用程式設定 > 。
允許使用者繼續使用無效入口網站伺服器憑證	選取 **No**（否）可防止應用程式在入口網站憑證無效時，建立與入口網站的連線。
顯示 GlobalProtect 圖示	選取 **No**（否）可在端點上隱藏 GlobalProtect 圖示。如果隱藏圖示，使用者則無法執行某些工作，例如檢視疑難排解資訊，變更密碼，重新探索網路，或視需連線。然而，必須進行使用者互動時，會顯示 HIP 通知訊息、登入提示及憑證對話方塊。
使用者切換通道重命名逾時（秒） （僅限 Windows）	指定使用 Microsoft 的遠端桌面通訊協定 (RDP) 登入端點之後，GlobalProtect 閘道驗證遠端使用者所需的秒數（範圍是 0 到

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	600；預設為 0）。要求遠端使用者在顯示時間內進行驗證以確保安全性。 驗證新使用者並切換使用者通道後，閘道將對通道重新具名。 值 0 表示目前使用者的通道未重新具名，而會立即終止。在此情況下，遠端使用者將取得新通道，且對閘道驗證無時間限制（除非設定 TCP 逾時）。
預先登入通道重新命名逾時（秒）（僅限 Windows）	此設定可控制 GlobalProtect 會如何處理將端點連線到閘道的預先登入通道。 值為 -1 表示，預先登入通道不會在使用者登入端點後逾時；GlobalProtect 會將通道重新命名以將其重新指派給使用者。不過，即使重新命名失敗或使用者未登入 GlobalProtect 閘道，通道仍會持續存在。 值為 0 表示，當使用者登入端點時，GlobalProtect 會立即終止預先登入通道，但不會將它重新命名。在此情況下，GlobalProtect 會為使用者啟動新的通道，而不會允許使用者透過預先登入通道來進行連線。一般來說，此設定最適合在 **Connect Method**（連線方法）設為 **Pre-logon then On-demand**（預先登入然後視需要）時使用，因為此連線方法會強迫使用者在啟動登入後手動啟動連線。 值為 1 到 600 代表在使用者登入端點後，預先登入通道可保持作用中狀態的秒數。在這段時間內，GlobalProtect 會在預先登入通道上強制執行原則。如果在逾時期間內，使用者驗證 GlobalProtect 閘道，GlobalProtect 會將通道重新指派給使用者。如果使用者未在逾時前驗證 GlobalProtect 閘道，GlobalProtect 將會終止預先登入通道。
使用者登出後保留通道逾時（秒）	若要讓 GlobalProtect 在使用者登出端點後保留現有的 VPN 通道，請指定 **Preserve Tunnel on User Logoff Timeout**（使用者登出後保留通道逾時）值（範圍為 0 至 600 秒；預設值為 0 秒）。若您接受預設值 0，則 GlobalProtect 在使用者登出後不會保留通道。
顯示系統託盤通知 （僅限 Windows）	選取 **No**（否）可隱藏使用者的通知。選取 **Yes**（是）（預設值）可在系統匣區域顯示通知。
自訂密碼到期訊息 （僅限 LDAP 驗證）	建立自訂訊息可在密碼即將到期時對使用者顯示該訊息。最大訊息長度為 200 個字元。
IPSec 不可靠時自動使用 SSL（小時）	指定 GlobalProtect 應用程式 **Automatically Use SSL When IPSec Is Unreliabl**（當 **IPSec** 不可靠時自動使用 **SSL**）的時間（以小時為單位；範圍是 0-168 小時）。如果您設定此選項，則 GlobalProtect 應用程式在指定的時段內不會嘗試建立 IPSec 通道。每當 IPSec 通道因通道保持運作逾時而關閉時，此計時器會啟動。 如果您接受預設值 0，且應用程式可以成功建立 IPSec 通道，則其不會返回以建立 SSL 通道。只有無法建立 IPSec 通道時，其才會返回建立 SSL 通道。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	此選項需要內容發行版本_____及以上。
GlobalProtect 連線 MTU（位元組）	輸入介於 1000 至 1420 位元組之間的 GlobalProtect 連線最大傳輸單位 (MTU) 值，該值由 GlobalProtect 應用程式用於連線至閘道。預設值為 1400 位元組。對於透過 MTU 值低於 1500 位元組標準網路連線的使用者，您可以最佳化其連線體驗。透過減小 MTU 的大小，可以消除 VPN 通道連線在經過多個網際網路服務供應商 (ISP) 和 MTU 低於 1500 位元組的網路路徑時，因分段而導致的效能和連線問題。
最大內部閘道連接嘗試次數	輸入 GlobalProtect 代理程式在首次嘗試失敗後應當重新嘗試連線至內部閘道的最大次數（範圍是 0 到 100；預設為 0，這表示 GlobalProtect 應用程式未重新嘗試連線）。透過增加值，可讓應用程式在以下情況下自動連線至內部閘道：首次連線嘗試期間暫時關閉或無法到達，但在指定重新嘗試次數用盡前重新開啟。增加值還可確保內部閘道接收最新的使用者及主機資訊。
入口網站連接逾時（秒）	請求連線至入口網站因入口網站無任何回應而逾時前的秒數（從 1 到 600）。當您的防火牆執行的應用程式和威脅內容版本早於 777-4484 時，預值值為 30。以內容版本 777-4484 版開始，預設值為 5。
TCP 連接逾時（秒）	由於連線任一端無回應使得 TCP 連線要求逾時之前的秒數（從 1 到 600）。當您的防火牆執行的應用程式和威脅內容版本早於 777-4484 時，預值值為 60。以內容版本 777-4484 版開始，預設值為 5。
TCP 接收逾時（秒）	由於缺少 TCP 要求的某些部分回應使得 TCP 連線要求逾時之前的秒數（範圍是 1 到 600；預設為 30）。
使用由通道指派的 DNS 伺服器解析所有的 FQDN（僅限 Windows）	（GlobalProtect 4.0.3 及更新版本）當 GlobalProtect 通道連接於 Windows 端點時，設定 DNS 解析度偏好。 • 選取 **Yes**（是）（預設）以啟用 GlobalProtect 應用程式，讓 Windows 端點使用您在閘道上設定的 DNS 伺服器解析所有 DNS 查詢，而非讓端點傳送一些 DNS 查詢到在實體介面卡上設定的 DNS 伺服器。 • 如果未解析閘道上設定的 DNS 伺服器初始查詢，選取 **No**（否），以允許 Windows 端點將 DNS 查詢傳送至設定在實體介面卡上的 DNS 伺服器。此選項會保留原生 Windows 行為，以遞歸方式查詢所有介面卡上全部的 DNS 伺服器，但可能導致解析部分 DNS 查詢需要很長的等待時間。 若要設定GlobalProtect 應用程式 4.0.2 和較早版本的 DNS 設定，請使用 **Update DNS Settings at Connect**（連線時更新 DNS 設定）選項。
連線時更新 DNS 設定 （僅限 Windows）（棄用）	（GlobalProtect 4.0.2 及更舊版本）設定 GlobalProtect 通道的 DNS 伺服器偏好： • 選取 **No**（否）（預設）讓 Windows 端點在初始查詢傳送至設定在閘道的 DNS 伺服器未獲得解析時，傳送 DNS 查詢到在實

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	體介面卡上設定的 DNS 伺服器。此選項會保留原生 Windows 行為，以遞歸方式查詢所有介面卡上全部的 DNS 伺服器，但可能導致解析部分 DNS 查詢需要很長的等待時間。 • 選取 **Yes**（是）以啟用 Windows 端點使用您在閘道上設定的 DNS 伺服器解析所有 DNS 查詢，而非端點上實體介面卡上設定的 DNS 伺服器。啟用此選項時，GlobalProtect 會嚴格強制執行閘道 DNS 設定，並覆寫所有實體介面卡的靜態設定。 當啟用此設定時，（設定為是）*GlobalProtect* 可復原先前儲存的 *DNS* 失敗，因而可以避免端點解析 *DNS* 查詢。此功能被棄用且以用更精進的實作取代，因此不會發生這種情形。如果您之前使用此功能，則我們建議您升級到 *GlobalProtect* 應用程式 *4.0.3* 或更新版本。 若要設定 GlobalProtect 應用程式 4.0.3 或更新版本的 DNS 設定，請使用 **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel**（使用通道指派的 DNS 伺服器解析所有 FQDN）選項。
偵測每個連線的 Proxy （僅限 Windows）	選取 **No**（否）可自動偵測 proxy 連線入口網站，並使用該 proxy 進行後續連線。選取 **Yes**（是）（預設值）可在每次連線時自動偵測 proxy。
透過代理程式設定通道（僅限 Windows 和 Mac）	指定 GlobalProtect 是否必須使用或繞過代理。選取**No**（否）以要求 GlobalProtect 繞過代理。選取**Yes**（是）以要求 GlobalProtect 使用代理。基於 GlobalProtect 代理程式的使用、端點操作系統和通道類型，網路流量的行為將有所不同。
Windows 安全中心 (WSC) 狀態變更後立即傳送 HIP 報告 （僅限 Windows）	選取 **No**（否）可防止 GlobalProtect 應用程式在 Windows 安全中心 (WSC) 變更時傳送 HIP 資料。選取 **Yes**（是）（預設值）可在 WSC 狀態變更時立即傳送 HIP 資料。
從 MFA 閘道啟用輸入驗證提示	若要支援多重要素驗證 (MFA)，GlobalProtect 端點必須收到從閘道傳來的 UDP 提示並進行確認。選取 **Yes**（是）可讓 GlobalProtect 端點收到提示並進行確認。選取 **No**（否）（預設值）可讓 GlobalProtect 封鎖閘道所傳來的 UDP 提示。
供輸入驗證提示 (UDP) 使用的網路連接埠	指定連接埠號碼，以供 GlobalProtect 端點從 MFA 閘道收取輸入驗證提示。預設連接埠為 4501。若要變更連接埠，請指定 1 到 65535 的數字。
受信任的 MFA 閘道	指定受 GlobalProtect 端點信任而可用於多重要素驗證的防火牆或驗證閘道清單。當 GlobalProtect 端點在指定的網路連接埠上收到 UDP 訊息時，GlobalProtect 只會在 UDP 提示是來自受信任的閘道時顯示驗證訊息。
輸入驗證訊息	自訂通知訊息，以在使用者嘗試存取需要另外驗證的資源時顯示此訊息。當使用者嘗試存取需要額外驗證的資源時，GlobalProtect 會收到一個包含輸入驗證提示的 UDP 封包，並顯示此訊息。UDP 封包也包含您在 Configure Multi-Factor Authentication（設定多因素驗證）時所指定的驗證入口網站頁面 URL。GlobalProtect 會自動將 URL 附加到訊息。例如：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
	`You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` 此訊息必須為 255 個或更少的字元。
IPv6 偏好	指定 GlobalProtect 端點通訊所偏好使用的通訊協定。選取 **No**（否）可將偏好的通訊協定變更為 IPv4。選取 Yes（是）（預設值）則可將 IPv6 設為雙堆疊環境偏好使用的連線。
變更密碼訊息	自訂一則訊息以在使用者改變其主動式目錄（AD）密碼時指定密碼原則或需求。例如： `Passwords must contain at least one number and one uppercase letter.` 此訊息對二字節的 Unicode 語言（如：簡中）必須為 255 個或更少的字元。若為日文，此訊息必須為 128 個或更少的字元。
日誌閘道選取條件	選取 **Yes**（是）讓 GlobalProtect 應用程式能夠將閘道選取條件日誌轉送防火牆。預設值為 **No**（否）。該應用程式不會將閘道選取條件的增強日誌轉送到防火牆。
在啟動時顯示狀態面板（僅限 Windows）	選取**Yes**（是）以在使用者首次建立連線時自動顯示 GlobalProtect 狀態面板。選取**No**（否）以在使用者首次建立連線時自壓制 GlobalProtect 狀態面板。
停用 GlobalProtect 應用程式	
密碼/確認密碼	如果 **Allow User to Disable GlobalProtect App**（允許使用者停用 GlobalProtect 應用程式）的設定為 **Allow with Passcode**（允許且須提供密碼），請輸入密碼，然後確認。作為密碼處理—記錄密碼並儲存在安全位置。您可透過電子郵件或發佈至您公司網站的支援區域，將密碼散佈給新 GlobalProtect 使用者。 如果某些情況阻止端點建立 VPN 連線且啟用此功能，使用者可在應用程式介面中輸入此密碼，以停用 GlobalProtect 應用程式及存取網際網路，而無需使用 VPN。
使用者可停用的次數上限	指定在使用者必須連線到防火牆前，使用者可以停用 GlobalProtect 的最大次數。預設值 0 表示對使用者可停用應用程式的次數沒有限制。
停用逾時（分鐘）	指定 GlobalProtect 應用程式可被停用的最大分鐘數。指定時間過後，應用程式嘗試連線至防火牆。預設值 0 表示停用期限無限制。 設定停用逾時以限制使用者可以停用該應用程式的時間。這可確保 *GlobalProtect* 在逾時結束時恢復並建立 *VPN*，以保護使用者以及使用者對資源的存取。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 應用程式組態設定	說明
Mobile Security Manager 設定	
Mobile Security Manager	如果正在使用 GlobalProtect Mobile Security Manager 進行行動裝置管理 (MDM)，請在 GP-100 裝置上輸入裝置簽入（註冊）介面的 IP 位址或 FQDN。
註冊連接埠	連線到 GlobalProtect Mobile Security Manager 進行註冊時，應該使用行動端點的連接埠編號。依預設，Mobile Security Manager 會在連接埠 443 上接聽。 請保留此連接埠號碼，以便在註冊程序期間不會針對用戶端憑證提示行動端點使用者（其他可能的值是 *443*、*7443* 及 *8443*）。

GlobalProtect 入口網站代理程式 *HIP* 資料收集頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）> *<agent-config>* > **HIP Data Collection**（**HIP** 資料收集）

選取 **HIP Data Collection**（**HIP** 資料收集）頁籤以定義應用程式從 HIP 報告中的端點收集的資料：

GlobalProtect HIP 資料收集組態設定	說明
收集 HIP 資料	清除此選項可防止應用程式收集及傳送 HIP 資料。 啟用 *GlobalProtect* 以為 *HIP* 型原則強化收集 *HIP* 資料，讓防火牆可以將端點獲得的 *HIP* 資料與 *HIP* 物件以及#或您設定的 *HIP* 設定檔比對，並應用適當的原則。
等候時間上限（秒數）	指定應用程式在提交可用資料之前應搜尋 HIP 資料的秒數（範圍是 10-60；預設為 20）。
憑證設定檔	選取 GlobalProtect 入口網站使用的憑證設定檔與 GlobalProtect 應用程式傳送的機械憑證比對。
排除類別	選取 **Exclude Categories**（排除類別）可指定您不想要應用程式收集 HIP 資料的主機資訊類別。選取 HIP 收集要排除的 **Category**（類別）（例如 data-loss-prevention）。在選取類別後，您可 **Add**（新增）特定廠商，然後可以從廠商 **Add**（新增）特定產品，視需進一步調整排除。按一下 **OK**（確定）可在每個對話方塊儲存設定。
自訂檢查	選取 **Custom Checks**（自訂檢查）可定義應用程式所要收集的自訂主機資訊。例如，如果廠商或產品清單不含建立 HIP 物件所需要的任何應用程式，您可以建立自訂檢查以判定該應用程式是否已安裝（具有對應的 Windows 登錄或 Mac Plist 機碼）或目前正在執行（具有對應的執行中程序）： • **Windows—Add**（新增）特殊登錄機碼或金鑰值的檢查。 • **Windows—Add**（新增）特殊 plist 機碼或金鑰值的檢查。

© 2019 Palo Alto Networks, Inc.

GlobalProtect HIP 資料收集組態設定	說明
	• 處理清單—**Add**（新增）您想要在使用者端點上檢查是否正在執行的程序。例如，若要確定是否正在執行某軟體應用程式，請將可執行檔的名稱新增至程序清單。您可以將程序新增至 **Windows** 頁籤、**Mac** 頁籤或兩者。

GlobalProtect 入口網站無用戶端 VPN 頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Clientless VPN**（無用戶端 **VPN**）

您現在可以將 GlobalProtect 入口網站設定為對一般企業 Web 應用程式（採用 HTML、HTML5 和 JavaScript 技術）提供安全的遠端存取。使用者可從具有 SSL 功能的 Web 瀏覽器獲得安全存取的好處，而不必安裝 GlobalProtect 軟體。當您需要為合作夥伴或派遣員工啟用應用程式存取權時，以及要安全地啟用未受管理的資產（包括個人裝置）時，此功能相當實用。若要使用此功能，您必須從 GlobalProtect 入口網站在裝載無用戶端 VPN 的防火牆上安裝 GlobalProtect 訂閱。接著可依照下表的說明，選取 **Clientless VPN**（無用戶端 **VPN**）頁籤，以在入口網站上進行 GlobalProtect 無用戶端 VPN 設定。

GlobalProtect 入口網站無用戶端組態設定	說明
一般頁籤	
無用戶端 VPN	選取 **Clientless VPN**（無用戶端 **VPN**）可指定無用戶端 VPN 工作階段的一般資訊：
主機名稱	Web 應用程式登陸頁面裝載所在之 GlobalProtect 入口網站的 IP 位址或 FQDN。GlobalProtect 無用戶端 VPN 會使用此主機名稱重新編寫應用程式 URL。 如果您使用網路位址轉譯 *(NAT)* 來提供 *GlobalProtect* 入口網站的存取權，則您輸入的 *IP* 位址或 *FQDN* 必須符合（或解析為）*GlobalProtect* 入口網站的 *NAT IP* 位址（公用 *IP* 位址）。
安全性區域	無用戶端 VPN 組態的區域。此區中所定義的安全性規則會控制使用者可存取哪些應用程式。
DNS Proxy	會解析應用程式名稱的 DNS 伺服器。選取 **DNS Proxy**伺服器或設定 **New DNS Proxy**（新的 **DNS Proxy**）（網路 > DNS Proxy）。
登入存留時間	無用戶端 SSL VPN 工作階段的有效 **Minutes**（分鐘）數（範圍是 60 到 1,440）或 **Hours**（小時）數（範圍是 1 到 24；預設為 3）。指定時間過後，使用者就必須重新驗證並啟動新的無用戶端 VPN 工作階段。
非使用狀態逾時	無用戶端 SSL VPN 工作階段可以持續閒置的 **Minutes**（分鐘）數（範圍是 5 到 1,440；預設為 30）或 **Hours**（小時）數（範圍是 1 到 24)。如果在指定的時間長度內使用者未曾活動過，使用者就必須重新驗證並啟動新的無用戶端 VPN 工作階段。
最大使用者數	可以同時登入到入口網站的使用者數目上限（預設是 10；範圍是 1 到未達上限）。在達到使用者數目上限時，其他無用戶端 VPN 使用者就無法登入到入口網站。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站無用戶端組態設定	說明
應用程式頁籤	
應用程式至使用者對應	**Add**（新增）一或多個 **Applications to User Mapping**（應用程式至使用者對應）以便讓使用者與所發行的應用程式相符。此對應可控制哪些使用者或使用者群組可以使用無用戶端 VPN 來存取應用程式。您必須先定義應用程式和應用程式群組，再將它們對應到使用者（[網路 > GlobalProtect > 無用戶端應用程式] 和 [網路 > GlobalProtect > 無用戶端應用程式群組]）。 • **Name**（名稱）—輸入對應的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。 • **Display application URL address bar**（顯示應用程式 **URL** 位址列）—選取此選項以顯示從使用者可以在應用程式登陸頁面未發行的應用程式上啟動的應用程式 URL 位址列。在啟用時，使用者可以按一下頁面上的 **Application URL**（應用程式 **URL**）連結並指定一個 URL。
使用者/使用者群組	您可 **Add**（新增）目前應用程式組態所套用的個別使用者或使用者群組。這些使用者有權使用 GlobalProtect 無用戶端 VPN 來啟動所設定的應用程式。 您必須先設定群組對應（*Device*（裝置）> *User Identification*（使用者識別）> *Group Mapping Settings*（群組對應設定）），才能選取群組。 除了使用者與群組，您還可指定何時要將這些設定套用於使用者或群組： • **any**（任何）—套用於所有使用者的應用程式組態（無需 **Add**（新增）使用者或使用者群組）。 • **select**（選取）—僅套用於您 **Add**（新增）至此清單的使用者與使用者群組的應用程式組態。
應用程式	您可以在對應中 **Add**（新增）個別的應用程式或應用程式群組。您納入組態中的 **Source Users**（來源使用者）可以使用 GlobalProtect 無用戶端 VPN 來啟動您所新增的應用程式。
加密設定頁籤	
通訊協定版本	選取所需的最低和最高 TLS/SSL 版本。TLS 版本越高，連線就越安全。選項包括 **SSLv3**、**TLSv1.0**、**TLSv1.1** 或 **TLSv1.2**。
金鑰交換演算法	選取金鑰交換所支援的演算法類型。選項包括 **RSA**、Diffie-Hellman (**DHE**) 或 Elliptic Curve Ephemeral Diffie-Hellman (**ECDHE**)。
加密演算法	選取所支援的加密演算法。建議使用 **AES128** 或更高級的演算法。
驗證演算法	選取所支援的驗證演算法。選項包括：**MD5**、**SHA1**、**SHA256** 或 **SHA384**。建議使用 **SHA256** 或更高級的演算法。
伺服器憑證驗證	針對應用程式在出示伺服器憑證時所發生的下列問題，啟用所要採取的動作： • **Block sessions with expired certificate**（封鎖憑證過期的工作階段）—如果伺服器憑證已到期，則封鎖應用程式的存取。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站無用戶端組態設定	說明
	• **Block sessions with expired certificate**（封鎖簽發者不受信任的工作階段）—如果伺服器憑證是由不受信任的憑證授權單位所簽發，則封鎖應用程式的存取。 • **Block sessions with unknown certificate status**（封鎖包含未知憑證狀態的工作階段）—如果 OCSP 或 CRL 服務所傳回的憑證撤銷狀態未知，則封鎖應用程式的存取。 • **Block sessions on certificate status check timeout**（在憑證狀態檢查逾時後封鎖工作階段）—如果在憑證狀態檢查逾時後才收到憑證狀態服務所傳來的回應，則封鎖應用程式的存取。
代理程式頁籤	
名稱	一個高達 31 個字元的頁籤以識別代理程式伺服器，GlobalProtect 入口網站使用代理伺服器存取已發行的應用程式。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
網域	新增由代理程式伺服器所提供的網域。
使用代理程式	選取此選項可讓 GlobalProtect 入口網站使用代理程式伺服器來存取已發行的應用程式。
伺服器 連接埠	指定代理程式伺服器的主機名稱（或 IP 位址）和連接埠號碼。
使用者 密碼	指定要登入代理程式伺服器所需提供的使用者名稱和密碼。再次輸入密碼以進行驗證。
進階設定頁籤	
重新寫入排除網域清單	（選用）**Add**（新增）網域名稱、主機名稱或 IP 位址到 **Rewrite Exclude Domain List**（重新編寫排除網域清單）。無用戶端 VPN 會作為反向 Proxy 並且會修改已發行之應用程式所傳回的頁面。當遠端使用者存取該 URL 時，其要求會經過 GlobalProtect 入口網站。在某些情況下，應用程式的頁面可能不必透過入口網站來存取。請指定不能重新編寫而應該排除在重新編寫規則之外的網域。 主機和網域名稱不支援路徑。主機和網域名稱的萬用字元 (*) 只能出現在名稱開頭處（例如，*.etrade.com）。

GlobalProtect 入口網站衛星頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Satellite**（衛星）

衛星是 Palo Alto Networks® 防火牆（通常位於分公司），可作為 GlobalProtect 應用程式來使衛星建立至 GlobalProtect 閘道的 VPN 連線。如同 GlobalProtect 應用程式，衛星可從入口網站接收其初始組態（包括憑證和 VPN 組態路由資訊），並使衛星連線至所有設定的閘道以建立 VPN 連線。

在分公司防火牆上進行 GlobalProtect 衛星設定前，您必須設定 WAN 連線的介面，然後設定安全性區域及原則，以便分公司 LAN 能夠與網際網路進行通訊。接著可依照下表的說明，選取 **Satellite**（衛星）頁籤，在入口網站上進行 GlobalProtect 衛星設定。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站衛星組態設定	說明
總言	• 名稱 — GlobalProtect 入口網站上此衛星組態的名稱。 • 組態重新整理間隔（小時）— 衛星應多久檢查一次入口網站的組態更新（範圍是 1-48 小時；預設為 24 小時）。
裝置	使用防火牆 **Serial Number**（序號）**Add**（新增）衛星。入口網站可接受序號或登入認證，以識別要求連線的使用者；如果入口網站不接收序號，則會要求登入認證。如果您透過其防火牆序號識別衛星，則當衛星首次連線以取得驗證憑證及其初始組態時，不必提供使用者登入認證。 在衛星透過序號或登入認證驗證之後，**Satellite Hostname**（衛星主機名稱）將自動新增至連接埠。
登記使用者/使用者群組	入口網站會使用 **Enrollment User/User Group**（登記使用者/使用者群組）設定（含或不含序號）來比對衛星與該組態。若衛星與序號不符，則必須作為個別使用者或群組成員來驗證。 **Add**（新增）您要使用該組態來控制的使用者或群組。 您必須在防火牆中啟用群組對應（*Device*（裝置）> *User Identification*（使用者識別）> *Group Mapping Settings*（群組對應設定）），才可限制特定群組的組態。
閘道	按一下 **Add**（新增），可輸入該組態可建立 IPSec 通道的閘道衛星的 IP 位址或主機名稱。在 **Gateways**（閘道）欄位中輸入用來設定閘道的介面其 FQDN 或 IP 位址。您可以將 IP 位址指定為 **IPv6** 和（或）**IPv4**。選取 **IPv6 Preferred**（**IPv6** 偏好）可在雙堆疊環境中指定 IPv6 連線的偏好設定。 （選用）如果您正將兩個以上的閘道新增至組態，**Routing Priority**（路由優先順序）會幫助衛星挑選優先使用的閘道（範圍是 1 到 25）。數字愈小，優先順序愈高（對於可用閘道）。衛星會將路由器優先順序乘以 10，以決定路由公制。 系統會將閘道發行的路由安裝在衛星上，作為靜態路由。靜態路由的公制為公制優先順序的 *10* 倍。如果您有多個閘道，請務必設定路由器優先順序，以便備份閘道所公告路由的度量，會比主要閘道所公告相同路由的度量還高。例如，如果您為主要閘道與備份閘道分別設定 *1* 與 *10* 的路由器優先順序，則衛星將使用 *10* 作為主要閘道的度量，使用 *100* 作為備份閘道的度量。 如果 **Publish all static and connected routes to Gateway**（將所有靜態與連接的路由發佈至閘道）（**Network**（網路）> **IPSec tunnels**（**IPSec** 通道）> **<tunnel** > **Advanced**（進階）—僅當您選取 **GlobalProtect Satellite on the <tunnel** > **General**（一般）時可用）。
受信任的根 CA	按一下 **Add**（新增），然後選取 CA 憑證，以用於核發閘道伺服器憑證。衛星受信任的根 CA 憑證會與入口網站代理程式組態同時推送至端點。 指定受信任的根 *CA* 以驗證閘道伺服器憑證，並建立前往 *GlobalProtect* 閘道的安全 *VPN* 通道連線。所有的閘道應使用相同的簽發者。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 入口網站衛星組態設定	說明
	如果根 *CA* 憑證在入口網站上不存在，您可 *Import*（匯入）或 *Generate*（產生）一個，用於核發閘道伺服器憑證。
用戶端憑證	
本地	• 核發憑證—選取負責核發憑證的根 CA，以供入口網站在成功驗證衛星後向其核發憑證。如果所需憑證在防火牆上已不存在，您可 **Import**（匯入）或 **Generate**（產生）憑證。 如果憑證已未駐留在防火牆上，您可 *Import*（匯入）或 *Generate*（產生）核發憑證。 • **OCSP** 回應程式—選取 OCSP 回應程式，以供衛星針對入口網站和閘道所提出的憑證，驗證其撤銷狀態。選取 **None**（無）以指定 OCSP 不用於驗證憑證撤銷。 啟用衛星 *OCSP* 回應程式，以便憑證在被撤銷時會通知您，並可以採取適當的操作來建立與入口網站和閘道的安全的連線。若要啟用衛星 *OCSP* 回應程式，您還必須在憑證撤銷檢查設定中啟用 *CRL* 以及 *OCSP*（*Device*（裝置）> *Setup*（啟動）> *Session*（工作階段）> *Decryption Settings*（解密設定））。 • 有效期間（天數）—指定 GlobalProtect 衛星憑證使用期限（範圍是 7 到 365；預設為 7）。 • 憑證更新週期（天數）—指定到期前憑證可自動更新的天數（範圍是 3 到 30；預設為 3）。
SCEP	• **SCEP**—選取 SCEP 設定檔來產生用戶端憑證。如果設定檔不在下拉式清單中，您可建立一個 **New**（新的）設定檔。 • 憑證更新週期（天數）—指定到期前憑證可自動更新的天數（範圍是 3 到 30；預設為 3）。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > Gateways（網路 > GlobalProtect > 閘道）

選取 **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）可設定 GlobalProtect 閘道。閘道可為 GlobalProtect 應用程式或應用程式，或為 GlobalProtect 衛星提供 VPN 連線。

從 [GlobalProtect 閘道] 對話方塊，**Add**（新增）一個新的閘道組態或選取現有閘道組態進行修改。

您想了解什麼內容？	請參閱：
可為 GlobalProtect 閘道進行哪些一般設定？	GlobalProtect 閘道一般頁籤
如何設定閘道用戶端驗證？	GlobalProtect 閘道驗證頁籤
如何進行通道及網路設定，以啟用應用程式來建立與閘道連接的 VPN 通道？	GlobalProtect 閘道代理程式頁籤
如何進行通道及網路設定，以啟用衛星與用作衛星的閘道建立 VPN 連線？	GlobalProtect 閘道衛星頁籤
想知道更多？	如需設定入口網站的詳細逐步指示，請參考《GlobalProtect 管理員指南》的設定 GlobalProtect 閘道。

GlobalProtect 閘道一般頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **General**（一般）

選取 **General**（一般）頁籤可定義應用程式可連線的閘道介面，並指定閘道如何驗證端點。

GlobalProtect 閘道一般設定	說明
名稱	輸入閘道的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	針對處於多個虛擬系統模式的防火牆，**Location**（位置）是虛擬系統 (vsys)，您可在其中使用 GlobalProtect 閘道。針對不是在多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示在 [GlobalProtect 閘道] 對話方塊中。 儲存閘道組態後，您便無法變更其 *Location*（位置）。
網路設定區域	
介面	選取將用作遠端端點 ingress 介面之防火牆介面的名稱。（這些介面必須已存在。） 不要附加允許 *Telenet*、*SSH*、*HTTP* 至一個您已設定 *GlobalProtect* 入口網站或閘道介面上的介面管理設定檔，因為

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道一般設定	說明
	這將會讓管理介面暴露在網際網路中。請參考保護管理存取的最佳實踐方法以了解如何保護存取您管理網路的詳細資料。
IP 位址	（選用）指定用於存取閘道的 IP 位址。選取 **IP Address Type**（**IP** 位址類型），然後輸入 **IP Address**（**IP** 位址）。 • IP 位址類型可以是 **IPv4**（僅限 IPv4 流量）、**IPv6**（僅限 IPv6 流量）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。如果您的網路支援雙堆疊組態（也就是會同時執行 IPv4 和 IPv6），請使用 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）。 IP 位址必須與 IP 位址類型相容。例如，172.16.1.0（適用於 IPv4）或 21DA:D3:0:2F3b（適用於 IPv6）。如果您選取 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），請輸入其各自適用的位址類型。
日誌設定	
記錄成功的 SSL 交握	（選用）建立成功的 SSL 解密交握的詳細日誌。預設會停用。 日誌會佔用儲存空間。在記錄成功的 *SSL* 交握之前，請確保具有可用於儲存日誌的資源。編輯 *Device*（裝置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定），以檢查目前的日誌記憶體指派，並在各種日誌類型之間重新指派日誌記憶體。
記錄不成功的 SSL 交握	建立不成功的 SSL 解密交握的詳細日誌，以便您查找解密問題的原因。預設會啟用。 日誌會佔用儲存空間。若要將更多（或更少）日誌儲存空間指派給「解密」日誌，請編輯日誌記憶體指派（*Device*（裝置）> *Setup*（設定）> *Management*（管理）> *Logging and Reporting Settings*（日誌記錄與報告設定））。
日誌轉送	指定轉送 GlobalProtect SSL 交握（解密）日誌的方法和位置。

GlobalProtect 閘道驗證頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Authentication**（驗證）

選取 **Authentication**（驗證）頁籤可識別 SSL/TLS 服務設定檔，並設定用戶端驗證的詳細資訊。您可新增多個用戶端驗證組態。

GlobalProtect 閘道驗證設定	
SSL/TLS 服務設定檔	選取 SSL/TLS 服務設定檔，用於保障此 GlobalProtect 閘道的安全。有關服務設定檔的內容詳細資料，請參閱裝置 > 驗證管理 > SSL/TLS 服務設定檔。
用戶端驗證區域	
名稱	輸入用於識別此組態的唯一名稱。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道驗證設定	
作業系統	依預設，組態套用於所有端點。您可依作業系統（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows** 或 **WindowsUWP**）、依 **Satellite**（衛星）裝置或依第三方 IPSec VPN 用戶端（**X-Auth**（擴展驗證））來縮小端點清單。 作業系統是多個組態間的主要差異因素。如果您需要將多個組態用於作業系統，您可進一步依驗證設定檔的選取來區分組態。 從最具體設定（位於清單頂部）到最一般組態（位於清單底部）來排序。
驗證設定檔	從下拉式清單中選取驗證設定檔或順序，可驗證對閘道的存取。參考 [裝置 > 驗證設定檔]。 對於用戶端驗證，請確保驗證設定檔使用 *RADIUS* 或 *SAML* 進行雙因素驗證。如果您不使用 *RADIUS* 或 *SAML*，則除了驗證設定檔之外，還需要設定憑證設定檔。
使用者名稱頁籤	指定 GlobalProtect 閘道登入自訂使用者名稱頁籤。舉例來說，使用者名稱（僅限）或電子郵件位址（使用者名稱@網域）。
密碼頁籤	指定 GlobalProtect 閘道登入自訂密碼頁籤。例如：密碼（土耳其文）或 **Passcode**（雙因子、以權杖為主的認證）。
驗證訊息	為了幫助使用者瞭解他們應使用哪些憑證來登入此閘道，您可輸入訊息或保留預設訊息。訊息長度最多為 256 個字元。
允許使用使用者認證或用戶端憑證進行驗證	如果您選取 **No**（否），則使用者必須使用使用者憑證以及用戶端憑證對閘道進行驗證。如果您選取**Yes**（是），則使用者可以使用使用者憑證或用戶端憑證對閘道進行驗證。
憑證設定檔	
憑證設定檔	（選用）選取閘道用於比對這些來自使用者端點之用戶端憑證的 **Certificate Profile**（憑證設定檔）。只有當用戶端憑證與憑證設定檔相符時，閘道才可使用此設定檔來驗證使用者。 如果您將**Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **No**（否），您則必須選取 **Certificate Profile**（憑證設定檔）。如果您將**Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者憑證或用戶端憑證進行驗證）選項設定為 **Yes**（是），**Certificate Profile**（憑證設定檔）則是可選項。 憑證設定檔獨立於作業系統。
封鎖隔離裝置的登入	指定是否封鎖隔離清單中 GlobalProtect 用戶端裝置的閘道登入（**Device**（裝置）> **Device Quarantine**（裝置隔離））。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道代理程式頁籤

- **Network**（網路）> **GlobalProtect** > **Portals**（入口網站）> *<portal-config>* > **Agent**（代理程式）

選取 **Agent**（代理程式）可進行通道設定，讓應用程式使用閘道建立 VPN 通道。此外，此頁籤可讓您指定 VPN 逾時、DNS 與 WINS 網路服務，以及與附加至安全性原則規則的 HIP 設定檔相符或不相符時，提供給使用者的 HIP 通知訊息。

在下列頁籤進行代理程式設定：

- 通道設定頁籤
- 用戶端設定頁籤
- 用戶端 IP 配發頁籤
- 網路服務頁籤
- 連線設定頁籤
- 影片流量頁籤
- HIP 通知頁籤

通道設定頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Tunnel Settings**（通道設定）

選取 **Tunnel Settings**（通道設定）頁籤以啟用通道以及設定通道參數。

如設定外部閘道，需要通道參數。如設定內部閘道，則通道參數為選用。

GlobalProtect 閘道用戶端通道模式組態設定	說明
通道模式	選取 **Tunnel Mode**（通道模式）可啟用通道模式，然後指定下列設定： • 通道介面—選取用於存取閘道的通道介面。 • 最大使用者數 — 指定可同時存取閘道以進行驗證、HIP 更新和 GlobalProtect 應用程式更新的使用者人數上限。如果已達到最大使用者人數，則會拒絕後續使用者存取，同時顯示一則訊息，指出已達到最大使用者人數（範圍依平台而有所不同，且當此欄為空白時，會顯示人數）。 • 啟用 **IPSec** — 選取此選項可針對終端流量啟用 IPSec 模式，使 IPSec 成為主要方法，而 SSL-VPN 成為後援方法。啟用 IPSec 之前，剩餘選項不可用。 • **GlobalProtect IPSec** 密碼—選取 GlobalProtect IPSec 密碼設定檔，該設定檔可針對 VPN 通道指定驗證和加密演算法。**default**（預設）設定檔會使用 AES-128-CBC 加密和 sha1 驗證。如需詳細資訊，請參閱 [網路 > 網路設定檔 > GlobalProtect IPSec 密碼]。 • 啟用 **X-Auth** 支援—選取此選項可在啟用 IPSec 時，啟用 GlobalProtect 閘道中的延伸驗證 (X-Auth) 支援。有了 X-Auth 的支援，支援 X-Auth（例如 Apple iOS 與 Android 裝置上的 IPSec VPN 用戶端，和 Linux 上的 VPNC 用戶端）的第三方 IPSec VPN 用戶端可以用 GlobalProtect 閘道建立 VPN 通道。[X 驗證] 選項提供 VPN 閘道至特定 GlobalProtect 閘道的遠端存取。由於 X-Auth 存取權提供有限的 GlobalProtect 功能，因此請考慮使用 GlobalProtect App，簡化 GlobalProtect 在 iOS 和 Android 裝置上提供的完整安全性功能集存取。 選取 **X-Auth Support**（**X-Auth** 支援）可啟動 **Group Name**（群組名稱）和 **Group Password**（群組密碼）選項：

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端通道模式組態設定	說明
	• 如果有指定群組名稱與群組密碼，驗證第一階段需要雙方使用這組認證資料進行驗證。第二階段需要有效的使用者名稱與密碼，由 [驗證] 區段中設定的驗證設定檔進行驗證。 • 如果沒有定義群組名稱與群組密碼，驗證第一階段會根據第三方廠商 VPN 用戶端提出的有效憑證進行。接著，此憑證由驗證區段中設定的憑證設定檔進行驗證。 • 依預設，當用來建立 IPSec 通道的金鑰到期時，使用者不需要重新驗證。若需要重新驗證使用者，請清除 **Skip Auth on IKE Rekey**（跳過對 IKE 重設金鑰的驗證）選項。

用戶端設定頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Client Settings**（用戶端設定）

選取 **Client Settings**（用戶端設定），可在 GlobalProtect 應用程式使用閘道建立通道時，對端點上的虛擬網路介面卡進行設定。

某些用戶端設定選項必須在您啟用通道模式，並在通道設定頁籤上定義通道介面後，才可供使用。

GlobalProtect 閘道用戶端設定和網路設定	說明
設定選取條件頁籤	
名稱	輸入用來識別用戶端設定組態的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
來源使用者	**Add**（新增）此組態要套用的特定使用者或使用者群組。 您必須先設定群組對應（*Device*（裝置）> *User Identification*（使用者識別）> *Group Mapping Settings*（群組對應設定）），才能選取使用者和群組。 如要將此設定部屬給所有使用者，請從 **Source User**（來源使用者）下拉選單中選取**any**（任何）一個。如要在 **pre-logon**（預先登入）模式將此設定僅部屬給擁有 GlobalProtect apps 的使用者，請在 **Source User**（來源使用者）下拉選單中選取預先登入。 僅當使用者符合 *Source User*（來源使用者）、*OS* 以及*Source Address*（來源位址）的條件時，才會將用戶端設定組態部署至使用者。
作業系統	若要根據端點的作業系統來部署此組態，請 **Add**（新增）作業系統（**Android**、**Chrome**、**iOS**、**IoT**、**Linux**、**Mac**、**Windows**、**WindowsUWP**）。或者，您也可以將該值設定為 **Any**（任何），從而只根據使用者或使用者群組，而非端點的作業系統來部署組態。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端設定和網路設定	說明
	僅當使用者符合 *Source User*（來源使用者）、*OS* 以及*Source Address*（來源位址）的條件時，才會將用戶端設定組態部署至使用者。
來源位址	若要根據使用者位址部屬該組態，請 **Add**（新增）來源 **Region**（區域）或本機 **IP Address**（**IP** 位址）（IPv4 和 IPv6）。若要將該組態部屬至所有使用者位置，請勿指定 **Region**（區域）或 **IP Address**（**IP** 位址）。如果您的使用者正在運行 GlobalProtect 應用程式 4.0 及更早的版本，則還必須將這些欄位留空，因為較舊的 GlobalProtect 應用程式版本不支持此功能。 如嘗試連線的位置與您設定的 *Region*（區域）或 *IP Address*（*IP* 位址）相符，則 *Source Address*（來源位址）比對成功。 僅當使用者符合 *Source User*（來源使用者）、*OS* 以及*Source Address*（來源位址）的條件時，才會將用戶端設定組態部署至使用者。
驗證取代頁籤	
驗證覆寫	在使用者使用透過驗證或憑證設定檔指定的驗證結構描述進行首次驗證後，啟用閘道即可使用安全、裝置特定的加密 Cookie 來驗證使用者。 • 產生用於驗證覆寫的 **Cookie** — 在 Cookie 存留期間，每次使用者驗證閘道時，代理程式將提供此 Cookie。 • **Cookie Lifetime**（**Cookie** 存留時間）—指定 Cookie 有效的小時數、天數或週數。生命週期一般為 24 小時。範圍是 1–72 小時，1–52 週或 1–365 天。Cookie 到期後，使用者必須輸入登入認證，閘道隨後會對新 Cookie 加密以傳送至使用者裝置。 • 接受用於驗證覆寫的 **Cookie** — 選取此選項可設定閘道使用加密 Cookie 接受驗證。當代理程式提供 Cookie 時，閘道將驗證 Cookie 已經過閘道加密，再驗證使用者。 • 用於加密/解密 **Cookie** 的憑證 — 選取閘道使用的憑證，以在加密與解密 Cookie 時使用。 確保閘道及入口網站均使用相同的憑證來加密與解密 *Cookie*。
IP 集區頁籤	
從授權伺服器擷取 Framed-IP-Address 屬性	選取此選項可讓 GlobalProtect 閘道使用外部驗證伺服器來指派固定 IP 位址。啟用此選項時，GlobalProtect 閘道會使用來自驗證伺服器的 Framed-IP-Address 屬性，將 IP 位址配置給連線中裝置。
驗證伺服器 IP 配發範圍	**Add**（新增）要指派給遠端使用者的 IP 位址的子網路或範圍。建立通道時，GlobalProtect 閘道會使用來自驗證伺服器的 Framed-IP-Address 屬性，將此範圍中的 IP 位址配置給連線中裝置。您可以新增 IPv4 位址（例如 192.168.74.0/24 和

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端設定和網路設定	說明
	192.168.75.1-192.168.75.100）或 IPv6 位址（例如 2001：aa :: 1-2001：aa :: 10）。 只有在您啟用 **Retrieve Framed-IP-Address attribute from authentication server**（從授權伺服器擷取 Framed-IP-Address 屬性）後，才可啟用並設定 **Authentication Server IP Pool**（驗證伺服器 IP 配發範圍）。 驗證伺服器 *IP* 集區必須大到足以支援所有工作階段。*IP* 位址指派是固定的，在使用者中斷連線之後會保留該位址。設定不同子網路中的多個範圍，將可讓系統為用戶端提供不會與用戶端上其他介面發生衝突的 *IP* 位址。 網路內的伺服器及路由器必須將此 IP 集區的流量傳送至防火牆。例如，針對 192.168.0.0/16 網路，遠端使用者可接收位址 192.168.0.10。
IP 配發範圍	**Add**（新增）要指派給遠端使用者的 IP 位址範圍。建立通道時，將會在使用此範圍內之位址的遠端使用者端點上建立介面。您可以新增 IPv4 位址（例如 192.168.74.0/24 和 192.168.75.1-192.168.75.100）或 IPv6 位址（例如 2001：aa :: 1-2001：aa :: 10）。 為了避免衝突，*IP* 集區必須大到足以支援所有工作階段。閘道會維護用戶端和 *IP* 位址的索引，讓用戶端在下次連線時可自動接收相同的 *IP* 位址。設定不同子網路中的多個範圍，將可讓系統為用戶端提供不會與用戶端上其他介面發生衝突的 *IP* 位址。 網路內的伺服器及路由器必須將此 IP 集區的流量傳送至防火牆。例如，針對 192.168.0.0/16 網路，系統可能會為遠端使用者指定位址 192.168.0.10。
分割通道頁籤	
存取路由頁籤	
無本機網路直接存取	選取此選項可停用分割通道，包含在 Windows 和 Mac 作業系統端點上直接存取本機網路。此功能可防止使用者將流量傳送至 Proxy 或本機資源，例如家用印表機。建立通道時，所有流量都會透過通道進行路由，且受限於防火牆的原則強制。
包含	**Add**（新增）要包含在 VPN 通道中的路由。這些路由是閘道推送至遠端使用者端點的路由，用以指定使用者端點可透過 VPN 連線傳送哪些項目。 若要包含所有目的地子網路或位址物件，請 *Include*（包含）*0.0.0.0/0* 以及 *::/0* 作為存取路由。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端設定和網路設定	說明
排除	**Add**（新增）要排除於 VPN 通道外的路由。這些路由是透過端點上的實體介面卡，而非透過虛擬介面卡（通道）傳送。 您可以將透過 VPN 通道傳送的路由定義為包含在通道中的路由、排除於通道外的路由，或是兩者的組合。例如，您可以設定分割通道，讓遠端使用者在無須透過 VPN 通道的情況下存取網際網路。排除的路由應比包含的路由更明確，以避免排除掉超出原有預期的流量。 若未包含或排除路由，則每個要求都會透過通道傳送（無分割通道）。在此情況下，每個網際網路要求都會通過防火牆，然後傳送至網路。此方法可防止外部人員存取使用者端點，以及取得內部網路存取權（在使用者端點作為橋接器的情況下）。
網域與應用程式頁籤	
包含網域	使用網域和網路埠（可選）將要包含在 VPN 通道中的軟體作為服務（SaaS）或公共雲應用程式新增。這些應用程式是閘道推送至遠端使用者端點的路由，用以指定使用者端點可透過 VPN 連線傳送哪些項目。 您可以為每個網域設定網路埠清單。若沒有設定任何網路埠，則所有該特定網域的網路埠都應遵從本原則。
排除網域	使用網域和網路埠（可選）將要從 VPN 通道中排除的軟體作為服務（SaaS）或公共雲應用程式新增。這些應用程式是透過端點上的實體介面卡，而非虛擬介面卡（通道）傳送。 您可以為每個網域設定網路埠清單。若沒有設定任何網路埠，則所有該特定網域的網路埠都應遵從本原則。 若未包含或排除任何網域，則每個要求都會透過通道傳送（無分割通道）。在此情況下，每個網際網路請求都會通過防火牆，並傳送至網路。這種方法可以防止來自使用者端點的外部人員獲得內部網路的存取權。
包含用戶端應用程式處理名稱	使用應用程式處理名稱將要包含在 VPN 通道中的軟體作為服務（SaaS）或公共雲應用程式新增。這些是閘道推送至遠端使用者的端點的應用程式，用以指定使用者端點可透過 VPN 連線傳送哪些項目。
排除客戶端應用程式處理名稱	使用應用程式處理名稱將要從 VPN 通道中排除的軟體作為服務（SaaS）或公共雲應用程式新增。這些應用程式是透過端點上的實體介面卡，而非虛擬介面卡（通道）傳送。 若未包含或排除任何應用程式，則每個要求都會透過通道傳送（無分割通道）。在此情況下，每個網際網路請求都會通過防火牆，並傳送至網路。這種方法可以防止來自使用者端點的外部人員獲得內部網路的存取權。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端設定和網路設定	說明
網路服務頁籤	
DNS 伺服器	指定 DNS 伺服器的 IP 位址，以此用戶端組態設定的 GlobalProtect app 會向此 IP 位址傳送 DNS 查詢。您可以新增多個 DNS 伺服器，以逗號分隔每個 IP 位址。
DNS 尾碼	在無法解析輸入的不合格主機名稱時，指定端點應在本機使用的 DNS 尾碼。您可以透過以逗號分隔每個尾碼來輸入多個 DNS 尾碼（最多 100 個）。

用戶端 *IP* 配發頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Client IP Pool**（用戶端 **IP** 集區）

選取 **Client IP Pool**（用戶端 **IP** 集區）頁籤以設定用於指派 IPv4 或 IPv6 位址到所有連線到 GlobalProtect™ 閘道的全域 IP 配發。

GlobalProtect 閘道用戶端 IP 配發組態設定	說明
IP 配發範圍	**Add**（新增）要指派給遠端使用者的 IPv4 或 IPv6 位址範圍。在建立通道後，GlobalProtect 閘道配置在此範圍內的 IP 位址至所有透過該通道連接的端點。 如果您在此閘道層級設定 *IP* 配發（網路 > *GlobalProtect* > 閘道 > *<gateway-config>* > *GlobalProtect* 閘道設定 > 代理程式 > 用戶端 *IP* 配發），則請不要在此用戶端層級設定任何 *IP* 配發（網路 > *GlobalProtect* > 閘道 > *<gateway-config>* > *GlobalProtect* 閘道設定 > 代理程式 > 用戶端設定 > *<client-setting>* > 設定 > *IP* 配發）。

網路服務頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Network Services**（網路服務）

選取 **Network Services**（網路服務）頁籤，可在 GlobalProtect 應用程式使用閘道建立通道時，設定指派給端點上的虛擬網路介面卡的 DNS 設定。

只有已啟用通道模式並在通道設定頁籤上定義通道介面時，才能使用網路服務選項。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端網路服務組態設定	說明
繼承來源	選取來源，此來源會將 DNS 伺服器及其他設定從選取的 DHCP 用戶端或 PPPoE 用戶端介面傳播到 GlobalProtect 應用程式的組態。透過這個全用戶端的網路組態，如 DNS 伺服器和 WINS 伺服器的伺服器會繼承 Inheritance Source 中選取的介面組態。
檢查繼承狀態	按一下 [繼承來源] 可以查看目前指派給用戶端介面的伺服器設定。
主要 DNS 次要 DNS	輸入向用戶端提供 DNS 之主要及次要伺服器的 IP 位址。
主要 WINS 次要 WINS	輸入向端點提供 Windows Internet Naming Service (WINS) 之主要及次要伺服器的 IP 位址。
繼承 DNS 尾碼	選取此選項，從繼承來源繼承 DNS 尾碼。
DNS 尾碼	**Add**（新增）在無法解析輸入的不合格主機名稱時，輸入端點應在本機使用的尾碼。您可以透過以逗號分隔每個尾碼來輸入多個尾碼（最多 100 個）。

連線設定頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Connection Settings**（連線設定）

選取 **Connection Settings**（連線設定）頁籤以定義 GlobalProtect™ 應用程式的逾時設定與驗證 cookie 使用限制。

GlobalProtect 閘道用戶端通道模式連線設定	說明
逾時組態	
登入存留時間	指定單一閘道登入工作階段允許的天數、小時數或分鐘數。
非使用狀態登出	指定天數、小時數或分鐘數，非作用中工作階段會於這段時間之後自動登出。
中斷閒置狀態的連線	指定應用程式停止透過 VPN 通道路由流量後端點登出 GlobalProtect 應用程式之前經過的時間（分鐘）。
驗證 cookie 使用限制	
停用 SSL VPN 的自動還原	啟用此選項可防止 SSL VPN 通道自動還原。 若啟用此選項，*GlobalProtect* 將不會支援復原 *VPN*。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道用戶端通道模式連線設定	說明
將驗證 cookie 的使用（用於自動還原 VPN 通道或驗證覆寫）限於	啟用此選項可根據以下條件之一限制驗證 cookie 使用： • 為其發佈驗證 **cookie** 的原始來源 **IP**—驗證 cookie 的使用限於與最初發佈 cookie 的端點具有相同公共來源 IP 位址的端點。 • 原始來源 **IP** 網路範圍—驗證 cookie 的使用限於具有指定網路 IP 位址範圍內公共來源 IP 位址的端點。輸入 **Source IPv4 Netmask**（來源 **IPv4** 網路遮罩）以指定 IPv4 位址的範圍，或輸入 **Source IPv6 Netmask**（來源 **IPv6** 網路遮罩）以指定 IPv6 位址的範圍。 若將網路遮罩設定為 0，則會對指定的 IP 位址類型停用此選項。例如，若入口網站或閘道僅支援一種 IP 位址類型（IPv4 或 IPv6），或者若要僅對一種 IP 位址類型啟用此選項（當入口網站或閘道同時支援 IPv4 和 IPv6 時），則可將網路遮罩設定為 0。在給定的閘道組態中，您只能將一個網路遮罩組態為 0；您不能同時將兩個網路遮罩皆設定為 0。 若您接受 **Source IPv4 Netmask**（來源 **Ipv4** 網路遮罩）預設值 32，則驗證 cookie 的使用限於與最初發佈 cookie 的端點的具有相同公共 IPv4 位址的端點。若您接受 **Source IPv6 Netmask**（來源 **Ipv6** 網路遮罩）預設值 128，則驗證 cookie 的使用限於與最初發佈 cookie 的端點的具有相同公共 IPv6 位址的端點。

影片流量頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **Video Traffic**（影片流量）

選取 **Video Traffic**（影片流量）頁籤，從 VPN 通道中排除影片直播流量。

GlobalProtect 閘道影音流量組態設定	說明
從通道排除視訊應用程式	選取此選項讓影音串流流量從 VNP 通道中排除。
應用程式	**Add**（新增）或 **Browse**（瀏覽）您想要從 VPN 通道排除的影音串流應用程式。 此影音重新導向功能可應用於以下應用程式中的任何影音流量類型： • Youtube • Dailymotion • Netflix 其他影音串流應用程式，僅以下幾種影音類型可以重新導向： • MP4 • WebM • MPEG 影音串流流量僅可從 VPN 通路排除。如果您不排除任何影音串流應用程式的話，所有的請求就會透過該通路（而非分割通道）進行路由。在此情況下，每個

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道影音流量組態設定	說明
	網際網路請求都會通過防火牆，並傳送至網路。這種方法可以防止來自使用者端點的外部人員獲得內部網路的存取權。

HIP 通知頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Agent**（代理程式）> *<agent-config>* > **HIP Notification**（**HIP** 通知）

選取 **HIP Notification**（**HIP** 通知）頁籤可定義當使用主機資訊設定檔 (HIP) 強制執行安全性規則時，使用者會看到的通知訊息。

僅當您建立 HIP 設定檔並將其新增至安全性原則時，才可使用這些選項。

GlobalProtect 代理程式 HIP 通知組態設定	說明
HIP 通知	**Add**（新增）HIP 通知並設定選項。您可為 **Match Message**（比對訊息）、**Not Match Message**（不比對訊息）或兩者的 **Enable**（啟用）通知，接著指定是否 **Show Notification As**（顯示通知為）**System Tray Balloon**（系統匣球形文字說明）或 **Pop Up Message**（快顯訊息）。然後指定訊息是否比對。 使用這些設定來通知一般使用者電腦狀態，例如，主機系統尚未安裝必要應用程式的警告訊息。您也可以針對符合訊息啟用 **Include Mobile App List**（包括行動應用程式清單）選項，指示哪些應用程式會觸發 HIP 相符。 您可將 *HIP* 通知訊息的格式設定為 *Rich HTML*，其中可以包含外部網站與資源的連結。請按一下 *Rich Text* 設定工具列中的超連結圖示（ ）以新增連結。

GlobalProtect 閘道衛星頁籤

- **Network**（網路）> **GlobalProtect** > **Gateways**（閘道）> *<gateway-config>* > **Satellite**（衛星）

衛星是 Palo Alto Networks 防火牆（通常位於分公司），可作為 GlobalProtect 應用程式來建立至 GlobalProtect 閘道的 VPN 連線。選取**Satellite**（衛星）頁籤定義閘道通道和網路設定，讓衛星與其建立 VPN 連線。您也可以設定衛星公告的路由。

- 通道設定頁籤
- 網路設定頁籤
- 路由篩選器頁籤

GlobalProtect 閘道衛星組態設定	說明
通道設定頁籤	
通道組態	選取 **Tunnel Configuration**（通道組態）並選取現有 **Tunnel Interface**（通道介面），或從下拉清單中選取 **New Tunnel Interface**（新通道介面）。如需詳細資訊，請參閱 [網路 > 介面 > 通道]。

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道衛星組態設定	說明
	• 重播攻擊偵測—防止遭受重播攻擊。 如果您啟用了衛星通道組態，則請啟用 *Replay attack detection*（重播攻擊偵測）以保護 *GlobalProtect* 衛星免受重播攻擊。 • 複製 **TOS** — 將服務類型 (ToS) 標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 (ToS) 資訊。 • 組態重新整理間隔（小時）—指定衛星應多久檢查一次入口網站的組態更新（範圍是 1-48 小時；預設為 2 小時）。
通道監控器	選取 **Tunnel Monitoring**（通道監控）可允許衛星裝置監控閘道通道連線，讓衛星裝置在連線中斷時能容錯移轉至備份閘道。 • 目的地位址—指定通道監控將用來判定是否能連線至閘道的 **IPv4** 或 **IPv6** 位址（例如，在網路上由閘道保護的 IP 位址）。或者，如果您為通道介面設定 IP 位址，您可以將此欄位保留空白，通道監控器會改用通道介面來判斷連線是否作用中。 • 通道監控設定檔—**Failover**（容錯移轉）至另一個閘道是唯一一種 LSVPN 所支援的通道監控設定檔。 如果您啟用了衛星通道組態，則請啟用 *Tunnel Monitoring*（通道監控）並設定通道監控設定檔以控制容錯轉移行為。
加密設定檔	選取 **IPSec Crypto Profile**（IPSec 加密設定檔），或建立新設定檔。Crypto 設定檔決定識別的通訊協定與演算法、驗證與 VPN 通道的加密。由於 LSVPN 中的通道端點雙方是您組織內的信任防火牆，因此您通常可以使用預設設定檔，該設定檔會使用 ESP 通訊協定、DH group2、AES 128 CVC 加密和 SHA-1 驗證。如需詳細資訊，請參閱 [網路 > 網路設定檔> GlobalProtect IPSec 加密]。
網路設定頁籤	
繼承來源	選取來源，此來源會將 DNS 伺服器及其他設定從選取的 DHCP 用戶端或 PPPoE 用戶端介面傳播至 GlobalProtect 衛星組態。透過這個全網路組態，如 DNS 伺服器會繼承「繼承來源」中選取的介面設定。
主要 DNS 次要 DNS	輸入向衛星提供 DNS 之主要及次要伺服器的 IP 位址。
DNS 尾碼	按一下 **Add**（新增）來在無法解析輸入的不合格主機名稱時，輸入衛星應在本機使用的尾碼。您可以使用逗號區隔尾碼來輸入多個尾碼。
繼承 DNS 尾碼	選取此選項來在無法解析輸入的不合格主機名稱時，將 DNS 尾碼傳送至在本機使用的衛星。
IP 配發範圍	**Add**（新增）IP 位址範圍，留待 VPN 通道建立時，將其指派給衛星上的通道介面。您可以指定 IPv6 或 IPv4 位址。 *IP* 集區必須大到足以支援所有工作階段。*IP* 位址指派是動態的，在衛星中斷連線之後不會保留該位址。設定不同子網路中的

© 2019 Palo Alto Networks, Inc.

GlobalProtect 閘道衛星組態設定	說明
	多個範圍，將可讓系統為衛星提供不會與衛星上其他介面發生衝突的 *IP* 位址。 網路內的伺服器及路由器必須將此 IP 集區的流量傳送至防火牆。例如，針對 192.168.0.0/16 網路，系統可能會為衛星指派位址 192.168.0.10。 如果您使用的是動態路由，請確定您為衛星指定的 IP 位址配發範圍，不會與您手動指派給閘道與衛星其通道介面的 IP 位址重疊。
存取路由	按一下 **Add**（新增），然後輸入路由，如下所示： • 如果您想要將衛星的所有流量路由穿越通道，請將此欄保留空白。 • 若要僅路由部分的流量穿越閘道（稱做分割通道），請指定必須穿越通道的目的地子網路。在此狀況下，衛星將使用自己的路由表來路由目的地不是指定存取路由流量。例如，您可以選取只將目的地為您公司網路的流量穿越通道，並使用本地衛星來啟用安全網際網路存取。 • 如果您想要啟用衛星之間的路由，請為各個衛星所保護的網路輸入摘要路由。
路由篩選器頁籤	
接受發行的路由	啟用 **Accept published routes**（接受發行的路由），接受衛星公告的路由並將其置於閘道的路由表中。若未選取此選項，閘道不會接受衛星公告的任何路由。
允許的子網路	若要針對衛星公告的路由制訂更嚴格的限制，請 **Add**（新增）允許的子網路並定義閘道可接受哪些子網路的路由；將篩選掉由衛星公告，並且不屬於清單的子網路。例如，如果所有衛星在 LAN 端上都是以 192.168.x.0/24 子網路設定，您可以在閘道上設定允許的路由 192.168.0.0/16。此組態使得唯有當閘道位於 192.168.0.0/16 子網路時，閘道才會接受來自衛星的路由。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > MDM（網路 > GlobalProtect > MDM）

若是使用 Mobile Security Manager 來管理一般使用者行動端點，而且正在使用啟用 HIP 功能的原則強制執行，則您必須設定閘道與 Mobile Security Manager 通訊，才能擷取受管理裝置的 HIP 報告。

Add（新增）Mobile Security Manager 的 MDM 資訊，讓閘道能夠與 Mobile Security Manager 通訊。

GlobalProtect MDM 設定	說明
名稱	輸入 Mobile Security Manager 的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
	如果防火牆處於多個虛擬系統模式中，MDM 設定會顯示虛擬系統 (vsys)，您可在其中使用 Mobile Security Manager。針對並未處於多重虛擬系統模式的防火牆，此欄位在 MDM 對話方塊中不顯示。儲存 Mobile Security Manager 之後，您就無法變更其位置。
連線設定	
伺服器	輸入 Mobile Security Manager 上介面的 IP 位址或 FQDN，閘道將連線該介面以擷取 HIP 報告。確定具有此介面的服務路由。
連線連接埠	連線連接埠是 Mobile Security Manager 接聽 HIP 報告要求的位置。預設連接埠為 5008，與 GlobalProtect Mobile Security Manager 接聽的連接埠相同。如果正在使用協力廠商的 Mobile Security Manager，請輸入該伺服器將在其上接聽 HIP 報告要求的連接埠編號。
用戶端憑證	選取在建立 HTTPS 連線時，將向 Mobile Security Manager 出示的閘道之用戶端憑證。只有將 Mobile Security Manager 設定為使用相互驗證時才需要此憑證。
受信任的根 CA	按一下 **Add**（新增），然後選取用來針對介面（閘道將連線至該介面以擷取 HIP 報告）核發憑證的根 CA 憑證。（此伺服器憑證可能與在 Mobile Security Manager 上為端點簽入介面核發的憑證不同）。您必須匯入根 CA 憑證並將其新增至此清單。

© 2019 Palo Alto Networks, Inc.

Network > GlobalProtect > Device Block List（網路 > GlobalProtect > 裝置封鎖清單）

選取 **Network**（網路） > **GlobalProtect** > **Device Block List**（裝置封鎖清單）（僅限防火牆）可將端點新增至 GlobalProtect 裝置封鎖清單。不允許此清單上的端點建立 GlobalProtect VPN 連線。

裝置封鎖清單設定	說明
名稱	輸入裝置封鎖清單的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	針對處於多個虛擬系統模式的防火牆，**Location**（位置）是虛擬系統 (vsys)，您可在其中使用 GlobalProtect 閘道。針對不是在多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示在 [GlobalProtect 閘道] 對話方塊中。儲存閘道組態後，您便無法變更其 **Location**（位置）。
主機 ID	輸入可識別端點的唯一 ID，即主機名稱與唯一裝置 ID 的組合。對於每個主機 ID，請指定相應的主機名稱。
主機名稱	輸入用來識別裝置的主機名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。

© 2019 Palo Alto Networks, Inc.

網路 > GlobalProtect > 無用戶端應用程式

選取 **Network**（網路） > **GlobalProtect** > **Clientless App**（無用戶端應用程式），以新增透過 GlobalProtect 無用戶端 VPN 存取的應用程式。您可以新增個別的無用戶端應用程式，然後選取 **Network**（網路） > **GlobalProtect** > **Clientless App Groups**（無用戶端應用程式群組） 來定義應用程式群組。

GlobalProtect 無用戶端 VPN 可對使用 HTML、HTML5 和 JavaScript 技術的一般企業 Web 應用程式提供安全的遠端存取權限。使用者可從具有 SSL 功能的 Web 瀏覽器獲得安全存取的優點，而不必安裝 GlobalProtect 軟體。這種做法適用於您需要讓合作夥伴或承包商能夠存取應用程式以及安全地啟用未受管理的資產（包括個人設備）時。

您需要 **GlobalProtect Clientless VPN**（**GlobalProtect** 無用戶端 **VPN**）動態更新才能使用此功能。此功能也需要您從 GlobalProtect 入口網站在裝載無用戶端 VPN 的防火牆上安裝 GlobalProtect 使用授權。

無用戶端應用程式設定	說明
名稱	輸入應用程式的說明性名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
位置	針對處於多個虛擬系統模式的防火牆，**Location**（位置）是虛擬系統 (vsys)，您可在其中使用 GlobalProtect 閘道。針對不是在多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示在 [GlobalProtect 閘道] 對話方塊中。儲存閘道組態後，您便無法變更其 **Location**（位置）。
應用程式首頁 URL	輸入應用程式所在的 URL（最多 4095 個字元）。
應用程式說明	（選用）輸入應用程式的說明（最多 255 個字元）。請僅使用字母、數字、空格、連字號與底線。
應用程式圖示	（選用）上載圖示以在發行的應用程式頁面上識別應用程式。您可以進行瀏覽以上載圖示。

© 2019 Palo Alto Networks, Inc.

網路 > GlobalProtect > 無用戶端應用程式群組

選取 **Network**（網路）> **GlobalProtect** > **Clientless App Groups**（無用戶端應用程式群組），以群組透過 GlobalProtect 無用戶端 VPN 存取的應用程式。您可以將現有無用戶端應用程式新增至某個群組，或為此群組設定新的無用戶端應用程式。群組適合於同時使用多個應用程式時。例如，您可能有一組要針對無用戶端 VPN 存取權限設定的標準 SaaS 應用程式（例如 Workday、JIRA 或 Bugzilla）。

無用戶端應用程式群組設定	說明
名稱	輸入應用程式群組的說明性名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
位置	針對處於多個虛擬系統模式的防火牆，**Location**（位置）是虛擬系統 (vsys)，您可在其中使用 GlobalProtect 閘道。針對不是在多重虛擬系統模式下的防火牆，**Location**（位置）欄位不會顯示在 [GlobalProtect 閘道] 對話方塊中。儲存閘道組態後，您便無法變更其 **Location**（位置）。
應用程式	從下拉式清單中 **Add**（新增）**Application**（應用程式），或設定新的無用戶端應用程式並將其新增至群組。若要設定新的無用戶端應用程式，請參考 [網路 > GlobalProtect > 無用戶端應用程式]。

© 2019 Palo Alto Networks, Inc.

Objects > GlobalProtect > HIP Objects（物件 > GlobalProtect > HIP 物件）

選取 **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件） 可定義主機資訊設定檔 (HIP) 的物件。HIP 物件提供比對準則，用於篩選應用程式報告的、您想要用於強制執行政策原始資料。例如，如果原始主機資料包含端點上若干防毒套件的相關資訊，您可能會關注特定應用程式，因為您的公司需要該套件。對於此情況，您將建立 HIP 物件，用於比對您想要強制執行的特定應用程式。

若要判斷需要的 HIP 物件，最好的方法是確定要如何使用主機資訊來強制執行政策。請注意，HIP 物件只是建置組塊，可讓您建立安全性政策可以使用的 HIP 設定檔。因此，您可能需要維持單純的物件，符合某種情況，例如，呈現特殊類型的必要軟體、特定網域中的成員資格，或呈現特定的端點作業系統。利用這種做法，您可以靈活建立極精細的 HIP 擴張政策。

若要建立 HIP 物件，請按一下 **Add**（新增）開啟 [HIP 物件] 對話方塊。如需在特定欄位中輸入之資訊的說明，請參閱下表。

- HIP 物件一般頁籤
- HIP 物件行動裝置頁籤
- HIP 物件修補程式管理頁籤
- HIP 物件防火牆頁籤
- HIP 物件反惡意軟體頁籤
- HIP 物件磁碟備份頁籤
- HIP 物件磁碟加密頁籤
- HIP 物件資料遺失防護頁籤
- HIP 物件憑證頁籤
- HIP 物件自訂檢查頁籤

如需建立 HIP 擴張之安全性政策的詳細資訊，請參考《*GlobalProtect* 管理員指南》的 **<** 設定 HIP 型政策強化 **>**。

HIP 物件一般頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **General**（一般）

選取**General**（一般）頁籤，指定新 HIP 物件的名稱，及設定物件來比對一般主機資訊，例如網域、作業系統，或其具有的網路連線類型。

HIP 物件一般設定	說明
名稱	輸入 HIP 物件的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
共享	如果您選取 **Shared**（共用），目前的 HIP 物件可用於： 如果您已登入處於多個虛擬系統模式的防火牆，則防火牆上所有的虛擬系統都可使用。如果您清除此選項，則僅有在 **Objects**（物件）頁籤中 **Virtual System**（虛擬系統）下拉式清單中選取的虛擬系統才可使用物件。針對並未處於多個虛擬系統模式的防火牆，此選項在 HIP 物件對話方塊中不可用。 Panorama™ 上所有的裝置群組。如果您清除此選項，則僅有在 **Objects**（物件）頁籤中 **Virtual System**（虛擬系統）下拉式清單中選取的裝置群組才可使用物件。

© 2019 Palo Alto Networks, Inc.

HIP 物件一般設定	說明
	儲存物件後，您便無法變更其共用設定。選取 **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）可查看目前的 **Location**（位置）。
說明	（選用）輸入說明。
主機資訊	選取此選項可啟動設定主機資訊的選項。
受管理	根據端點是否被管理篩選。若要比對受管理的端點，請選取 **Yes**（是）。若要比對不受管理的端點，請選取 **No**（否）。
停用覆寫（僅限 Panorama）	控制裝置群組中的 HIP 物件取代存取權，這些群組是在 **Objects**（物件）頁籤中所選 **Device Group**（裝置群組）的子系。若想防止管理員在子系裝置群組中利用取代其繼承值來建立物件的本機複本，請選取此選項。依預設將清除此選項（覆寫已啟用）。
網域	若要比對網域名稱，請從下拉式清單中選取運算子，然後輸入要比對的字串。
作業系統	若要比對主機作業系統，請從第一個下拉式清單選取 **Contains**（包含），從第二個下拉式清單選取廠商，然後從第三個下拉式清單選取作業系統版本，或選取 **All**（全部）以比對所選廠商的任何作業系統版本。
用戶端版本	若要比對特定的版本號碼，請從下拉式清單選取運算子，然後在文字方塊中輸入要符合（或不符合）的字串。
主機名稱	若要比對特定的主機名稱或主機名稱的部分，請從下拉式清單選取運算子，然後在文字方塊中輸入要符合（或不符合，視您選取的運算子而定）的字串。
主機 ID	主機 ID 是 GlobalProtect 為了識別主機所指派的唯一 ID。主機 ID 值會依裝置類型而有所不同： • **Windows**—Windows 登錄中儲存的機器 GUID (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS**—第一個內建實體網路介面的 MAC 位址 • **Android**—Android ID • **iOS**—UDID • **Linux**—從系統 DMI 表格擷取的產品 UUID • **Chrome**—GlobalProtect 所指派的唯一英數字串，長度為 32 個字元 若要比對特定的主機 ID，請從下拉式清單選取運算子，然後在文字方塊中輸入要符合（或不符合，視您選取的運算子而定）的字串。
序號	若要比對全部或部分端點序號，請從下拉式清單中選取運算式，然後輸入要比對的字串。
網路	使用此欄位可在特定的行動裝置網路組態中啟用篩選。此比對準則僅適用於行動裝置。 從下拉式清單選取運算子，然後從第二個下拉式清單選取要篩選的網路連線類型：**Wifi**、**Mobile**（行動）、**Ethernet**（乙太網路）（僅適用於 **Is Not**（不是）篩選）或 **Unknown**（未知）。選取網路類型後，輸入要比對的其他任何字串（如果可用），例如行動裝置電信業者或 Wifi **SSID**。

© 2019 Palo Alto Networks, Inc.

HIP 物件行動裝置頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Mobile Device**（行動裝置）

選取**Mobile Device**（行動裝置）頁籤，針對從執行 GlobalProtect 應用程式的行動裝置所收集的資料啟用 HIP 比對。

若要收集行動裝置屬性並在 *HIP* 強制性原則中使用它們的話，*GlobalProtect* 就需要一個 *MDM* 伺服器。*GlobalProtect* 目前支援 *HIP* 與 *AirWatch MDM* 伺服器的整合。

HIP 物件行動裝置設定	說明
行動裝置	選取此選項可根據執行 GlobalProtect 應用程式的行動裝置所收集的資料啟用篩選，並啟用 [裝置]、[設定] 及 [應用程式] 頁籤。
裝置頁籤	• 型號—若要比對特定的裝置型號，請從下拉式清單中選取運算子，然後輸入要比對的字串。 • 頁籤 — 若要比對 GlobalProtect Mobile Security Manager 上定義的頁籤值，請從第一個下拉式清單選取運算子，再從第二個下拉式清單選取頁籤。 • 電話號碼—若要比對全部或部分裝置電話號碼，請從下拉式清單中選取運算子，然後輸入要比對的字串。 • **IMEI**—若要比對全部或部分裝置的國際行動娛樂裝置識別 (IMEI) 號碼，請從下拉式清單中選取運算子，然後輸入要比對的字串。
設定頁籤	• 密碼—根據裝置是否有密碼集進行選取。若要比對具有密碼集的裝置，請選取 **Yes**（是）。若要比對沒有密碼集的裝置，請選取否。 • **Rooted/Jailbroken**—根據裝置是否已 Root 或 Jailbreak 而進行選取。若要比對已刷機或已破解的裝置，請選取 **Yes**（是）。若要比對尚未刷機/破解的裝置，請選取 **No**（否）。 • 磁碟加密 — 根據是否已加密裝置資料進行篩選。若要比對已啟用磁碟加密的裝置，請選取是。若要比對尚未啟用磁碟加密的裝置，請選取否。 • 前次簽入後歷經的時間—根據裝置前次使用 MDM 簽入的時間進行選取。從下拉式清單選取運算子，然後指定簽入時段的天數。例如，您可以定義物件以符合前 5 天內尚未簽入的裝置。

應用程式頁籤	• 應用程式—（僅限 Android 裝置）選取此選項可根據裝置上安裝的應用程式，及裝置是否已安裝任何受惡意軟體影響的應用程式，以啟用篩選。
	• **Criteria**（準則）頁籤
	  • 具有惡意軟體—選取 **Yes**（是）可比對已安裝受惡意軟體影響之應用程式的裝置。選取 **No**（否）可比對未安裝受惡意軟體影響之應用程式的裝置。選取 **None**（無）可以不將 **Has Malware**（具有惡意軟體）作為比對準則。
	• **Include**（包含）頁籤
	  • 套件—若要比對已安裝特定應用程式的裝置，請 **Add**（新增）應用程式，然後以反向 DNS 格式輸入唯一的應用程式名稱。例如 com.netflix.mediaclient，然後輸入對應的應用程式 **Hash**（雜湊），GlobalProtect 應用程式將會計算此雜湊並使用裝置 HIP 報告來提交。

© 2019 Palo Alto Networks, Inc.

HIP 物件修補程式管理頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Patch Management**（修補程式管理）

選取**Patch Management**（修補程式管理）頁籤可針對 GlobalProtect 端點的修補程式狀態啟用 HIP 比對。

HIP 物件修補程式管理設定	說明
修補程式管理	選取此選項可根據主機的修補程式管理狀態啟用比對，並啟用準則及廠商頁籤。
準則頁籤	指定下列設定： • 已啟用—比對主機上是否已安裝修補程式管理軟體。 • 已啟用—比對是否已在主機上啟用修補程式管理軟體。如果清除 **Is Installed**（已安裝）選項，會將此欄位自動設定為 **None**（無）並停用編輯。 • 嚴重性—從邏輯運算子清單中選取，比對主機是否遺失特定嚴重性值的修補程式。 使用下列在 GlobalProtect 嚴重性值和 OPSWAT 嚴重性評級間的鏡像，了解每個值代表的意義： • **0**—低 • **1**—中 • **2**—重要 • **3**—重要 • 檢查—比對端點是否缺少修補程式。 • 修補程式 — 比對主機是否具有特定的修補程式。按一下 **Add**（新增）並輸入要檢查的特定修補程式的 KB 文章 ID。例如，輸入 `3128031` 以檢查 Microsoft Office 2010 (KB3128031) 32 位元版本的更新。
廠商頁籤	定義特定的修補程式管理軟體廠商及產品，以便在端點上尋找是否有符合項。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下新增以選取特定的 **Product**（產品）。按一下 **OK**（確定）以儲存設定。

HIP 物件防火牆頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Firewall**（防火牆）

選取 **Firewall**（防火牆）頁籤，以根據 GlobalProtect 端點的防火牆軟體狀態啟用 HIP 比對。

HIP 物件防火牆設定
選取 **Firewall**（防火牆）可根據主機的防火牆軟體狀態啟用比對： • 已安裝—比對是否已在主機上安裝防火牆軟體。 • 已啟用 — 比對是否已在主機上啟用防火牆軟體。如果清除 **Is Installed**（已安裝）選項，會將此欄位自動設定為 **None**（無）並停用編輯。 • 廠商和產品 — 定義特定的防火牆軟體廠商和/或產品，以便在主機上尋找是否有符合項。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下**Add**（新增）以選取特定的 **Product**（產品）。按一下 **OK**（確定）以儲存設定。 • 排除廠商 — 選取此選項可比對沒有指定廠商軟體的主機。

© 2019 Palo Alto Networks, Inc.

HIP 物件反惡意軟體頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Anti-Malware**（反惡意軟體）

選取 **Anti-Malware**（反惡意軟體）頁籤可根據 GlobalProtect 端點的防毒軟體或反間諜軟體涵蓋範圍來啟用 HIP 比對。

HIP 物件反惡意軟體設定

選取t **Anti-Malware**（反惡意軟體）以根據主機上的防毒或反間軟體涵蓋範圍啟用比對。依照下列步驟定義其他比準則：

- 已安裝—比對是否已在主機上安裝防毒或反間諜軟體。
- 即時保護—比對是否已在主機上啟用防毒或反間諜軟體即時保護。如果清除 **Is Installed**（已安裝）選項，會將此欄位自動設定為 **None**（無）並停用編輯。
- 病毒定義版本 — 在指定的天數內或發行的版本中，比對病毒定義何時更新。
- 產品版本—比對防毒或反間諜軟體的特定版本。若要指定版本，請從下拉式清單選取運算子，然後輸入代表產品版本的字串。
- 最後掃描時間—指定是否根據前次執行反毒或防間諜軟體掃描的時間進行比對。從下拉式清單選取運算子，然後指定要比對的 **Days**（天數）或 **Hours**（小時）數字。
- 廠商和產品 — 定義特定的防毒或反間諜軟體廠商及/或產品，以便在主機上尋找是否有符合項。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下**Add**（新增）以選取特定的 **Product**（產品）。按一下 **OK**（確定）以儲存設定。
- 排除廠商 — 選取此選項可比對沒有指定廠商軟體的主機。

HIP 物件磁碟備份頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Disk Backup**（磁碟備份））

選取 **Disk Backup**（磁碟備份）頁籤可根據 GlobalProtect 用戶端的磁碟備份狀態啟用 HIP 比對。

HIP 物件磁碟備份設定

選取 **Disk Backup**（磁碟備份）可根據主機的磁碟備份狀態來啟用比對，然後針對符合項定義其他比對準則，如下所示：

- 已啟用—比對是否已在主機上安裝磁碟備份軟體。
- 上次備份的時間—指定是否根據前次執行磁碟備份的時間進行比對。從下拉式清單選取運算子，然後指定要比對的 **Days**（天數）或 **Hours**（小時）數字。
- 廠商和產品 — 定義特定的磁碟備份軟體廠商及產品，以便根據主機進行比對。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下**Add**（新增）以選取特定的 **Product**（產品）。按一下 **OK**（確定）以儲存設定。
- 排除廠商 — 選取此選項可比對沒有指定廠商軟體的主機。

HIP 物件磁碟加密頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Disk Encryption**（磁碟加密）

選取 **Disk Encryption**（磁碟加密）頁籤，以根據 GlobalProtect 用戶端的磁碟加密狀態啟用 HIP 比對。

© 2019 Palo Alto Networks, Inc.

HIP 物件磁碟加密設定	說明
磁碟加密	選取 **Disk Encryption**（磁碟加密）可根據主機的磁碟加密狀態啟用比對。
準則	指定下列設定： • 已安裝 — 比對是否已在主機上安裝磁碟加密軟體。 • 加密的位置—按一下 **Add**（新增），指定在決定是否符合時，用於檢查磁碟加密的磁碟機或路徑： • 加密的位置—輸入特定位置來檢查主機上的加密。 • 狀態—指定如何從下拉式清單選取運算子，然後選取可能的狀態來比對加密位置的狀態（**full**（完整）、**none**（無）、**partial**（部分）、**not-available**（無法使用））。 按一下 **OK**（確定）以儲存設定。
廠商	定義特定的磁碟加密軟體廠商及產品，以便根據端點進行比對。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下**Add**（新增）以選取特定的 **Product**（產品）。按一下 **OK**（確定），儲存設定並返回 **Disk Encryption**（磁碟加密）頁籤。

HIP 物件資料遺失防護頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Data Loss Prevention**（資料遺失防護）

選取 **Data Loss Prevention**（資料遺失防護）頁籤，以根據 GlobalProtect 端點是否執行資料遺失軟體來設定 HIP 比對。

HIP 物件資料遺失防護設定
選取 **Data Loss Prevention**（資料遺失防護）可根據主機（僅限 Windows 主機）的資料遺失防護 (DLP) 狀態來啟用比對，然後為符合項定義其他比對準則，如下所示： • 已安裝 — 比對是否已在主機上安裝 DLP 軟體。 • 已啟用—比對是否已在主機上啟用 DLP 軟體。如果清除 **Is Installed**（已安裝）選項，會將此欄位自動設定為 **None**（無）並停用編輯。 • 廠商和產品—定義特定的 DLP 軟體廠商和/或產品，以便在主機上尋找是否有符合項。按一下 **Add**（新增），然後從下拉式清單選取 **Vendor**（廠商）。（選用）按一下**Add**（新增）以選取特定的 **Product**（產品）。按一下 **OK**（確定）以儲存設定。 • 排除廠商 — 選取此選項可比對沒有指定廠商軟體的主機。

HIP 物件憑證頁籤

- **Objects**（物件）> **GlobalProtect** > **HIP Objects**（**HIP** 物件）> *<hip-object>* > **Certificate**（憑證）

選取 **Certificate**（憑證）頁籤，以根據憑證設定檔和其他憑證屬性啟用 HIP 比對。

HIP 物件憑證設定
選取 **Validate Certificate**（驗證憑證），以根據憑證設定檔和憑證屬性啟用比對。然後，定義比對準則，如下所示：

© 2019 Palo Alto Networks, Inc.

HIP 物件憑證設定
• **Certificate Profile**（憑證設定檔）—選取 GlobalProtect 閘道將用於驗證 HIP 報告中傳送之機器憑證的憑證設定檔。 • **Certificate Field**（憑證欄位）—選取用於比對機器憑證的憑證屬性。 • **Value**（值）—為屬性設定值。

HIP 物件自訂檢查頁籤

- **Objects**（物件） > **GlobalProtect** > **HIP Objects**（**HIP** 物件） > *<hip-object>* > **Custom Checks**（自訂檢查）

選取 **Custom Checks**（自訂檢查）頁籤，針對 GlobalProtect 入口網站上已定義的任何自訂檢查啟用 HIP 比對。如需將自訂檢查新增至 HIP 收集的詳細資訊，請參閱。Network > GlobalProtect > Portals（網路 > GlobalProtect > 入口網站）。

HIP 物件自訂檢查設定	說明
自訂檢查	選取 **Custom Checks**（自訂檢查），可根據 GlobalProtect 入口網站已定義的任何自訂檢查上啟用比對。
處理程序清單	若要在主機系統中檢查特定程序，請按一下 **Add**（新增），然後輸入程序名稱。依預設，應用程式會檢查正在執行的程序；如果只想要查看是否特定的程序並未執行，請清除 **Running**（執行中）選項。程序可為操作系統層級程序或使用者空間應用程式程序。
登錄機碼	若要在 Windows 主機中檢查特定的登錄機碼，請按一下 **Add**（新增）並輸入要比對的 **Registry Key**（登錄機碼）。若只要比對缺少指定登錄機碼或機碼值的主機，請核取 **Key does not exist or match the specified value data**（機碼不存在或不符合指定的值資料）方塊。 若要比對特定值，按一下 **Add**（新增），然後輸入 **Registry Value**（登入值）和 **Value Data**（值資料）。若要比對確實沒有指定值或值資料的主機，請選取 **Negate**（否定）。 按一下 **OK**（確定）以儲存設定。
Plist	若要在 Mac 主機中檢查「屬性清單 (Plist)」中的特定項目，請按一下 **Add**（新增）並輸入 **Plist** 名稱。若只要比對沒有指定 Plist 的主機，請選取 **Plist does not exist**（Plist 不存在）。 若要比對 Plist 內的特定機碼-值配對，請按一下 **Add**（新增），然後輸入 **Key**（機碼）和要比對的對應 **Value**（值）。若要比對確實沒有指定機密或值的主機，請選取 **Negate**（否定）。 按一下 **OK**（確定）以儲存設定。

© 2019 Palo Alto Networks, Inc.

Objects > GlobalProtect > HIP Profiles（物件 > GlobalProtect > HIP 設定檔）

選取 **Objects**（物件）> **GlobalProtect** > **HIP Profiles**（**HIP** 設定檔）可建立 HIP 設定檔（一起評估的 HIP 物件集合，用於監控或強制執行安全性政策），用於設定啟用 HIP 的安全性政策。建立 HIP 設定檔時，您可以使用布林邏輯來結合先前建立的 HIP 物件（以及其他 HIP 設定檔），如此在針對導出的 HIP 設定檔評估流量時，就會得到符合或不符合結果。如果有符合項，則將執行對應的政策規則；如果沒有符合項，則針對下一個規則，及使用任何其他政策比對準則來評估流量。

若要建立 HIP 設定檔，請按一下 **Add**（新增）。下表提供應在 HIP 設定檔對話方塊的欄位中輸入的資訊。如需設定 GlobalProtect 和建立 HIP 擴張之安全政策的工作流程等詳細資訊，請參考《*GlobalProtect* 管理員指南》的 < 設定 HIP 型政策強化 >。

HIP 設定檔設定	說明
名稱	輸入設定檔的名稱（最多 **31** 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
說明	（選用）輸入說明。
共用	選取 **Shared**（共用）可使目前的 HIP 設定檔適用以下情況： • 如果您已登入處於多個虛擬系統模式的防火牆，則防火牆上所有的虛擬系統都可使用。如果您清除此選項，則僅有在 **Objects**（物件）頁籤 **Virtual System**（虛擬系統）下拉式清單中選取的虛擬系統才可使用設定檔。針對並未處於多個虛擬系統模式的防火牆，此選項在 HIP 設定檔對話方塊中不顯示。 • Panorama 上所有的設備群組。如果您清除此選項，則僅有在 **Objects**（物件）頁籤中 **Virtual System**（虛擬系統）下拉式清單中選取的設備群組才可使用設定檔。 儲存設定檔後，您便無法變更其 **Shared**（共用）設定。選取 **Objects**（物件）> **GlobalProtect** > **HIP Profiles**（**HIP** 設定檔）可查看目前的 **Location**（位置）。
停用覆寫（僅限 Panorama）	控制會覆寫對設備群組中 HIP 設定檔的存取權，這些群組是在 **Objects**（物件）頁籤中所選 **Device Group**（設備群組）的子系。若您想防止管理員在子系設備群組中利用覆寫其繼承值來建立設定檔的本機複本，請選取此選項。依預設將清除此選項（覆寫已啟用）。
比對	按一下**Add Match Criteria**（新增比對準則）開啟 [HIP 物件/設定檔建立器]。 選取要作為比對準則的第一個 HIP 物件或設定檔，然後將其新增（⊕）至 [HIP 物件/設定檔建立器] 對話方塊的 **Match**（比對）文字方塊。請注意，若只有當物件中的準則對流量而言不為 true 時，方允許 HIP 設定檔將物件評估為符合，請先選取 **NOT** 再新增物件。 為正在建立的設定檔繼續新增比對準則，確定在每次加法之間選取適當的布林運算子（**AND** 或 **OR**）；請在適當的情況下使用 **NOT** 運算子。 若要建立複雜的布林運算式，則必須在 **Match**（比對）文字方塊中，於適當的位置手動新增括號，確保使用所要的邏輯來評估 HIP 設定檔。例如，下列運算式表示 HIP 設定檔將比對具有 FileVault 磁碟加密（Mac 作業系統）或 TrueCrypt

© 2019 Palo Alto Networks, Inc.

HIP 設定檔設定	說明
	磁碟加密（Windows 系統），且同時屬於必要的網域，並已安裝 Symantec 防毒用戶端之主機的流量： `((“MacOS” and “FileVault”) or (“Windows” and “TrueCrypt”)) and “Domain” and “SymantecAV”` 將物件及設定檔新增到新 HIP 設定檔後，按一下 **OK**（確定）。

© 2019 Palo Alto Networks, Inc.

Device > GlobalProtect Client（裝置 > GlobalProtect 用戶端）

下列主題說明如何設定及管理 GlobalProtect 應用程式。

您想了解什麼內容？	請參閱：
檢視關於 GlobalProtect 軟體版本的詳細資訊。	管理 GlobalProtect 代理程式軟體
安裝 GlobalProtect 軟體。	設定 GlobalProtect 代理程式
使用 GlobalProtect 軟體。	使用 GlobalProtect 代理程式
想知道更多？	如需設定 GlobalProetect 軟體的詳細逐步指示，請參考《GlobalProtect 管理員指南》的部署 GlobalProtect APP 軟體。

管理 GlobalProtect 應用程式軟體

選取 **Device**（裝置）> **GlobalProtect Client**（**GlobalProtect** 用戶端）（ 僅限防火牆 ）可下載並啟動託管入口網站之防火牆上的 GlobalProtect 應用程式軟體。之後，連線至入口網站的端點將下載應用程式軟體。在您指定入口網站的代理程式組態中，您可定義入口網站推送軟體至端點的方式與時間。組態會決定應用程式連線時是否要自動升級、是否要提示使用者進行升級，或是否要對特定使用者組禁止升級。如需詳細資訊，請參閱允許使用者升級 GlobalProtect 應用程式。如需用於散佈 GlobalProtect 應用程式軟體的選項，以及部署軟體的逐步指示等詳細資訊，請參考《GlobalProtect 管理員指南》的部署 GlobalProtect 應用程式軟體。

對於初次下載與安裝的 *GlobalProtect* 應用程式，端點的使用者必須以管理員權限登入。後續升級不需要管理員權限。

GlobalProtect 用戶端設定	說明
版本	這是在 Palo Alto Networks 更新伺服器上提供的 GlobalProtect 應用程式軟體的版本號碼。若要查看 Palo Alto Networks 是否有可用的新應用程式軟體版本，請按一下 **Check Now**（立即檢查）。防火牆將使用服務路由，連線至更新伺服器確定是否有新版本可用，並在清單頂端顯示它們。
大小	應用程式軟體包的大小。
發行日期	Palo Alto Networks 發行可用版本的日期和時間。
已下載	此欄中的核取記號表示已下載到防火牆的應用程式軟體套件的對應版本。
目前已啟動	此欄中的核取記號表示已在防火牆上啟動，並可由連線中的應用程式下載的應用程式軟體套件的對應版本。一次只能啟動軟體的一個版本。
動作	指出目前可為對應的應用程式軟體套件執行的動作，如下所示： • 下載—在 Palo Alto Networks 更新伺服器上已提供對應的應用程式軟體版本。按一下 **Download**（下載）可啟動下載。如果防火牆不能

© 2019 Palo Alto Networks, Inc.

GlobalProtect 用戶端設定	說明
	存取網際網路，請使用連線網際網路的電腦以前往 客戶支援網站，然後選取**Updates**（更新） > **Software Updates**（軟體更新） 尋找並 **Download**（下載）您本機電腦的新應用程式軟體版本。接著手動 **Upload**（上載）應用程式至防火牆。 • 啟動 — 已將對應的應用程式軟體版本下載至防火牆，但應用程式還無法下載它。按一下 **Activate**（啟動）可啟動軟體並啟用應用程式升級。若要啟動您以手動方式上傳至防火牆的軟體更新，請按一下 **Activate From File**（從檔案啟動），並從下拉式清單中選取要啟動的版本（接著可能需要重新整理畫面，版本才會顯示為 **Currently Activated**（目前已啟動））。 • 重新啟動—對應的應用程式軟體已啟動並準備好進行端點下載。由於一次只能在防火牆上啟用一個 GlobalProtect 應用程式軟體版本，因此若一般使用者需要存取目前使用中版本之外的不同版本，您必須 **Activate**（啟動）後者，使該版本成為 **Currently Active**（目前使用中）版本。
版本資訊	提供對應應用程式版本的 GlobalProtect 版本資訊連結。
☒	從防火牆移除先前下載的應用程式軟體影像檔。

設定 GlobalProtect 應用程式

GlobalProtect 應用程式是安裝在端點（通常是筆記型電腦）上的應用程式，用於支援與入口網站和閘道的 GlobalProtect 連接。本應用程式由 GlobalProtect 服務（PanGP 服務）支援。

請確認您已針對您的主機作業系統（*32* 位元或 *64* 位元），選取正確的安裝選項。如果您在 *64* 位元主機上安裝，請針對初始安裝使用 *64* 位元瀏覽器及 *Java* 組合。

若要安裝應用程式，請開啟安裝程式檔案，並依照螢幕上指示執行。

使用 GlobalProtect 應用程式

這個頁籤位在 **GlobalProtect** 設定 面板中，在啟動 GlobalProtect 應用程式並從 GlobalProtect 狀態面板上的設定功能表選擇**Settings**（設定）時開啟。其中包含關於狀態和設定的有用資料，並提供有助於解決疑難排解連線問題的資料。

- 一般頁籤—顯示使用者名稱以及與 GlobalProtect 有關的入口網站。您也可以從本頁籤新增、刪除或修改入口網站。
- 連線頁籤—顯示為 GlobalProtect 應用程式設定的閘道，並提供下列有關各個閘道的資料：
  - 閘道名稱
  - 通道狀態
  - 驗證狀態
  - 連線類型
  - 閘道 IP 位址或 FQDN（僅可用於外部模式）

  在內部模式中，*Connection*（連線）頁籤會顯示可用閘道的完整清單。而在外部模式中，*Connection*（連線）頁籤會顯示連接的閘道以及有關這些閘道的其他詳細資料（如閘道 *IP* 位址與正常運行時間）。
- 主機設定檔頁籤—顯示 GlobalProtect 透過主機資訊設定檔 (HIP)，用來監控並強化的安全性政策。按一下**Resubmit Host Profile**（重新提交主機設定檔）以手動重新將 HIP 數據提交至閘道。

© 2019 Palo Alto Networks, Inc.

- 疑難排解頁籤—在 macOS 端點上，本頁籤讓您可以**Collect Logs**（收集日誌）並設定**Logging Level**（日誌記錄層級）。在 Windows 端點上，本頁籤讓您可以 **Collect Logs**（收集日誌）、設定 **Logging Level**（日誌記錄層級）並檢視以下有助於疑難排的資料。
  - 網路設定—顯示目前的系統設定。
  - 路由表 — 顯示目前如何路由 GlobalProtect 連線的相關資訊。
  - 通訊端—顯示目前使用中連線的通訊端資訊。
  - 日誌—可讓使用者顯示 GlobalProtect 應用程式與服務的日誌。選擇日誌類型與偵錯等級。按一下 **Start**（開始）可開始日誌記錄，按一下 **Stop**（停止）可終止日誌記錄。
- 通知頁籤—顯示 GlobalProtect 應用程式上觸發的通知清單。要檢視特定通知的更多詳細資料，在通知上按兩下即可。

© 2019 Palo Alto Networks, Inc.

Panorama Web 介面

Panorama™ 是 Palo Alto Networks® 新一代防火牆系列的集中管理系統。Panorama 讓您從單一位置即可監控在網路上的所有應用程式、使用者和內容，然後使用此資訊來建立政策，以控制及保護網路。使用 Panorama 執行集中式政策及防火牆管理，可提升您管理分散式防火牆網路的作業效率。ˇPanorama 既適用於專用硬體（M-Series）設備，也可作為 VMware 虛擬設備（在 ESXi 伺服器或 vCloud Air 上執行）。

雖然許多 Panorama Web 介面檢視和設定與您在防火牆 Web 介面上所見者相同，下列主題會說明唯獨在 Panorama Web 介面上可用的選項，用於管理 Panorama、防火牆、日誌收集器。

> Use the Panorama Web Interface（使用 Panorama Web 介面）
> Context Switch（內容切換）
> Panorama 提交作業
> Defining Policies on Panorama（在 Panorama 上定義原則）
> Log Storage Partitions for a Panorama Virtual Appliance in Legacy Mode（傳統模式下 Panorama 虛擬裝置的日誌儲存分割區）
> Panorama > Setup > Interfaces（Panorama > 設定 > 介面）
> Panorama > 高可用性
> Panorama > 受管理的 WildFire 叢集
> Panorama > 管理員
> Panorama > Admin Roles（Panorama > 管理員角色）
> Panorama > Access Domains（Panorama > 存取網域）
> Panorama > Managed Devices > Summary（Panorama > 受管理的裝置 > 摘要）
> 託管設備）> Health（健康狀態
> Panorama > 範本
> Panorama > Device Groups（Panorama > 裝置群組）
> Panorama > 受管理的收集器
> Panorama > 收集器群組
> Panorama > Plugins（Panorama > 外掛程式）
> Panorama > SD-WAN
> Panorama > VMware NSX
> Panorama > 日誌擷取設定檔
> Panorama > 日誌設定
> Panorama > Server Profiles > SCP（Panorama > 伺服器設定檔 > SCP）
> Panorama > 已排程的設定匯出
> Panorama > 軟體
> Panorama > 設備部署

想知道更多？

請參閱《Panorama 管理員指南》以了解關於設定和使用 Panorama 以便集中管理的詳細資訊。

使用 Panorama Web 介面

Panorama 與防火牆的 Web 介面都具有相同的外觀及風格。不過，Panorama Web 介面包含附加選項和 Panorama 特定的頁籤，用於管理 Panorama 與使用 Panorama 來管理防火牆與日誌收集器。

下列通用欄位會顯示在多個 Panorama Web 介面頁面的標題或頁尾中。

通用欄位	說明
脈絡	您可使用左側功能表上方的 **Context**（內容）下拉式清單，在 Panorama Web 介面與防火牆 Web 介面之間進行切換（請參閱內容切換）。
↻	在 **Dashboard**（儀表板）和 **Monitor**（監控）頁籤中，按一下頁籤標頭的重新整理（↻）以手動重新整理這些頁籤中的資料。您也可以使用頁籤標頭右方的未標記下拉式清單，以分鐘為單位選取自動重新整理間隔（**1 min**（**1** 分鐘）、**2 mins**（**2** 分鐘）或 **5 mins**（**5** 分鐘））；若要停用自動重新整理，選取 **Manual**（手動）。
存取網域	存取網域會定義對特定裝置群組、範本、個別防火牆的存取（透過 **Context**（內容）下拉式清單）。若您以管理員身分登入且有多個存取網域指派給您的帳戶，則 **Dashboard**（儀表板）、**ACC** 和 **Monitor**（監控）頁籤只會顯示您在 Web 介面的頁尾中選取的 **Access Domain**（存取網域）資訊（例如日誌資料）。 若系統僅將一個存取網域指派給您的帳戶，則 *Web* 介面不會顯示 *Access Domain*（存取網域）下拉式清單。
裝置群組	裝置群組由防火牆和虛擬系統構成，您是以群組方式進行管理（請參閱 [Panorama > 裝置群組]）。**Dashboard**（儀表板）、**ACC** 和 **Monitor**（監控）頁籤只會顯示您在頁籤標頭中選取的 **Device Group**（裝置群組）資訊（例如日誌資料）。在 **Policies**（原則）和 **Objects**（物件）頁籤中，您可以設定特定 **Device Group**（裝置群組）的設定，或全部裝置群組（選取 **Shared**（共用））的設定。
範本	範本是具有通用網路和裝置設定的防火牆群組，範本堆疊是範本的組合（請參閱 [Panorama > 範本]）。在 **Network**（網路）和 **Device**（裝置）頁籤中，您可對特定 **Template**（範本）或範本堆疊進行設定。由於您僅能在個別範本中編輯設定，因此若您選取範本堆疊，則這些頁籤中的設定會是唯讀狀態。
檢視方式:裝置 模式	依預設，**Network**（網路）和 **Device**（裝置）頁籤會顯示這些設定和值：該值所適用的防火牆處於正常操作模式、且支援多重虛擬系統和 VPN。然而，您可使用下列選項以篩選頁籤，以便僅顯示您要編輯的模式特定設定： • 在 **Mode**（模式）下拉式清單中，選取或清除 **Multi VSYS**（多重虛擬系統）、**Operational Mode**（操作模式）和 **VPN Mode**（**VPN** 模式）選項。 • 在 **View by**（檢視者）中選取以下項目，設定所有模式選項以反映特定防火牆的模式組態：**Device**（裝置）下拉式選單。

Panorama 頁籤提供下列頁面來管理 Panorama 和日誌收集器。

© 2019 Palo Alto Networks, Inc.

Panorama 頁面	說明
設定	針對下列工作，選取 **Panorama** > **Setup**（設定）： • 指定一般設定（例如 Panorama 主機名稱）和驗證、日誌、報告、AutoFocus™、橫幅、當日訊息、密碼複雜度的設定。這些設定與您對防火牆的設定相似：請選取 [裝置 > 設定 > 管理]。 • 備份並還原組態、重新啟動 Panorama，並關閉 Panorama。這些操作與您對防火牆執行的操作相似：請選取 [裝置 > 設定 > 操作]。 • 定義 DNS、NTP 和 Palo Alto Networks 更新的伺服器連線。這些設定與您對防火牆的設定相似：請選取 [裝置 > 設定 > 服務]。 • 定義 Panorama 介面的網路設定。選取 [裝置 > 設定 > 介面]。 • 指定 WildFire™ 裝置的設定。這些設定與您對防火牆的設定相似：請選取 [裝置 > 設定 > WildFire]。 • 管理硬體安全性模組 (HSM) 設定。這些設定與您對防火牆的設定相似：選取 [裝置 > 設定 > HSM]。
高可用性	可讓您為一對 Panorama 管理伺服器設定高可用性 (HA)。請選取 [Panorama > 高可用性]。
設定稽核	讓您可檢視組態檔案間的差異。請選取 [裝置 > 設定稽核]。
密碼設定檔	可讓您為 Panorama 管理員定義密碼設定檔。請選取 [裝置 > 密碼設定檔]。
管理員	可讓您設定 Panorama 管理員帳戶。請選取 [Panorama > 管理員]。 如果已鎖定管理員帳戶，*Administrators*（管理員）頁面會在 *[鎖定的使用者]* 欄中顯示鎖定圖示。您可以按一下鎖來解除鎖定帳戶。
管理員角色	可讓您定義管理員角色，針對存取 Panorama 的管理員，該管理員角色控制其權限和責任。請選取 [Panorama > 管理員角色]。
存取網域	可讓您控制管理員存取裝置群組、範本、範本堆疊和防火牆的 Web 介面。請選取 [Panorama > 存取網域]。
驗證設定檔	可讓您指定驗證 Panorama 存取的設定檔。請選取 [裝置 > 驗證設定檔]。
驗證順序	可讓您指定要用於允許存取 Panorama 的驗證設定檔系列。請選取 [裝置 > 驗證順序]。
使用者識別機制	讓您能夠設定自訂憑證設定檔，以便與 User-ID 代理程式進行相互驗證。選取 Device（裝置）> User Identification（使用者識別）> Connection Security（連線安全性）。
資料重新散佈	讓您能夠有選擇地將資料重新散佈至其他防火牆或 Panorama 管理系統。選取 Device（裝置）> Data Redistribution（資料重新散佈）。
受管理的裝置	可讓您管理防火牆，包含將防火牆作為受管理的裝置新增至 Panorama、顯示防火牆連線及授權狀態、標記防火牆、更新防火牆軟體與內容，以及載入組態備份。選取 Panorama > Managed Devices（託管裝置）> Summary（摘要）。

© 2019 Palo Alto Networks, Inc.

Panorama 頁面	說明
範本	可讓您管理 **Device**（裝置）及 **Network**（網路）頁籤中的組態選項。在您部署具有相同或類似組態的多個防火牆時，範本與範本堆疊可讓您減少所需的管理工作。請選取 [Panorama > 範本]。
裝置群組	可讓您設定裝置群組，根據功能、網路區段或地理位置對防火牆進行分組。裝置群組可包含實體防火牆、虛擬防火牆及虛擬系統。 一般而言，裝置群組中的防火牆需要類似的原則組態。使用 Panorama 上的 **Policies**（原則）與 **Objects**（物件）頁籤，裝置群組提供了分層方法的實作方式，可用來管理受管理的防火牆網路之間的原則。您可以在最多四層的樹狀階層中，將裝置群組巢狀化。子系群組會自動繼承上階群組和共用位置的原則和物件。請選取 [Panorama > 裝置群組]。
受管理的收集器	可讓您管理日誌收集器。由於您使用 Panorama 設定日誌收集器，因此這些收集器也就是所謂的「受管理收集器」。受管理的收集器可以位於 Panoramam 管理伺服器（M-Series 裝置、或處於 Panorama 模式的 Panorama 虛擬裝置）或專用日誌收集器（處於日誌收集器模式的 M-Series 裝置）的本機上。請選取 [Panorama > 受管理的收集器]。 您也可以安裝專用日誌收集器的軟體更新。 您可以將 Panorama 管理伺服器轉換成 DedicatedLogCollector。
收集器群組	可讓您管理收集器群組。收集器群組以邏輯方式對日誌收集器分組，讓您可以套用相同的組態設定並向其指派防火牆。Panorama 將日誌均勻散佈於日誌收集器的所有磁碟之間，並橫跨收集器群組的所有成員。請選取 [Panorama > 收集器群組]。
外掛程式	可讓您管理第三方整合的外掛程式，例如 VMware NSX。請選取 [Panorama > VMware NSX]。
Vmware NSX	可讓您自動化佈建 VM-Series 防火牆，透過啟用 NSX Manager 與 Panorama 之間的通訊來實現。請選取 [Panorama > VMware NSX]。
憑證管理	可讓您設定及管理憑證、憑證設定檔和金鑰。請選取 [管理防火牆及 Panorama 憑證]。
日誌設定	可讓您將日誌轉送到簡易網路管理通訊協定 (SNMP) 設陷接收器、syslog 伺服器、電子郵件伺服器和 HTTP 伺服器。請選取 [裝置 > 日誌設定]。
伺服器設定檔	可讓您針對向 Panorama 提供服務的不同的伺服器類型進行設定檔設定。選取下列任何一項，以設定特定伺服器類型： • 裝置 > 伺服器設定檔 > 電子郵件 • 裝置 > 伺服器設定檔 > HTTP • 裝置 > 伺服器設定檔 > SNMP 設陷 • 裝置 > 伺服器設定檔 > Syslog • 裝置 > 伺服器設定檔 > RADIUS • 裝置 > 伺服器設定檔 > TACACS+ • 裝置 > 伺服器設定檔 > LDAP • 裝置 > 伺服器設定檔 > Kerberos

© 2019 Palo Alto Networks, Inc.

Panorama 頁面	說明
	• 裝置 > 伺服器設定檔 > SAML 識別提供者
已排程的設定匯出	可讓您每天將 Panorama 和防火牆組態匯出至 FTP 伺服器或安全複本 (SCP) 伺服器。請選取 [Panorama > 已排程的設定匯出]。
軟體	可讓您更新 Panorama 軟體。選取 Panorama > 軟體。
動態更新	可讓您檢視最新應用程式定義與新安全性威脅的相關資訊，如防毒特徵碼（需要威脅防護授權），並使用新定義更新 Panorama。請選取 [裝置 > 動態更新]。
支援	可讓您從 Palo Alto Networks 中存取產品與安全性警示。請選取 [裝置 > 支援]。
設備部署	可讓您部署防火牆與日誌收集器的軟體與內容更新。請選取 [Panorama > 裝置部署]。
主要金鑰與診斷	可讓您指定要在 Panorama 上加密私密金鑰的主要金鑰。依預設，即使您不指定新的主要金鑰，Panorama 仍會以加密形式儲存私密金鑰。請選取 [裝置 > 主要金鑰與診斷]。

© 2019 Palo Alto Networks, Inc.

內容切換

在每個 Panorama Web 介面頁面的標頭中，您都可以使用左側功能表上方的 **Context**（內容）下拉式清單，在 Panorama Web 介面與防火牆 Web 介面之間進行切換。選取防火牆時，Web 介面會重新整理以顯示所選防火牆所有的頁面與選項，便於您在本機上管理。下拉式清單只會顯示您具有管理存取權的防火牆（請參閱 [Panorama > 存取網域]），以及已連線至 Panorama 的防火牆。

您可以使用篩選器，依據平台（型號）、設備群組、範本、標籤或 HA 狀態來搜尋防火牆。您也可以在篩選列中輸入文字字串，依設備名稱進行搜尋。

處於高可用性 (HA) 模式的防火牆會有彩色背景的圖示，以指出其 HA 狀態。

© 2019 Palo Alto Networks, Inc.

Panorama 提交作業

按一下 Web 介面右上方的 **Commit**（認可），並選取對 Panorama 組態之擱置中變更的操作，以及 Panorama 推送至防火牆、日誌收集器、WildFire 叢集和裝置的變更：

- **Commit**（認可）> **Commit to Panorama**（認可至 **Panorama**）—啟動您在 Panorama 管理伺服器的組態中做出的變更。此行動也會將裝置群組、範本、收集器群組、WildFire 叢集和裝置變更認可至 Panorama 組態，而不將變更推送至防火牆、日誌收集器、WildFire 叢集和裝置。僅認可至 Panorama 組態可讓您儲存未準備好在防火牆、日誌收集器、 WildFire 叢集和裝置上啟動的變更。

  當將組態推送至受管理的裝置時，*Panorama 8.0* 和更新版本會推送執行中組態，即認可至 *Panorama* 的組態。*Panorama 7.1* 及更早版本會推送候選組態，包含未認可的變更。因此，*Panorama 8.0* 和更新版本不讓您將變更推送至受管理的裝置，直至您先將變更認可至 *Panorama*。
- **Commit**（認可）> **Push to Devices**（推送至裝置）—將 Panorama 執行中組態推送給裝置群組、範本、收集器群組、WildFire 叢集和裝置。
- **Commit**（認可）> **Commit and Push**（認可並推送）—將所有組態變更認可至本機 Panorama 組態，並將 Panorama 執行中設定推送至裝置群組、範本、收集器群組和 WildFire 叢集和裝置。

您可依管理員或位置篩選擱置中變更並僅認可、推送、驗證或預覽這些變更。位置可能是特定裝置群組、範本、收集器群組、日誌收集器、WildFire 裝置和叢集、共用設定或 Panorama 管理伺服器。

當您認可變更時，該變更會成為執行中組態的一部分。您尚未認可的變更是候選組態的一部分。Panorama 會將認可要求排入佇列，以便您在之前的認可正在進行中時，啟動新的認可。Panorama 會依啟動順序執行認可，但優先處理由 Panorama 啟動的自動認可（例如 FQDN 重新整理）。然而，如果佇列已達到管理員啟動認可的數目上限，您必須等候 Panorama 完成擱置認可處理，才能啟動新的認可。您可使用工作管理員（Tasks）來清除認可佇列或查看認可的相關詳細資訊。如需組態變更、提交程序、提交驗證及提交佇列的詳細資訊，請參閱Panorama 提交與驗證操作。您也可以儲存候選組態、還原變更、和匯入、匯出或載入組態（裝置 > 設定 > 操作）。

下列選項適用於認可、驗證或預覽組態變更。

欄位/按鈕	說明
當您選取 **Commit**（認可）> **Commit to Panorama**（認可至 **Panorama**）或 **Commit**（認可）> **Commit and Push**（認可並推送）來認可至 Panorama 時，適用下列選項。	
認可所有變更	認可您具有管理權限的所有變更（預設值）。當您選取此選項時，您無法手動篩選 Panorama 認可的組態變更範圍。反之，指派給您用於登入之帳戶的管理員角色會決定認可範圍： • 超級使用者角色—Panorama 會認可所有管理員的變更。 • 自訂角色—指派給您帳戶之管理員角色設定檔的權限會決定認可範圍（請參閱 [Panorama > 管理員角色]）。若設定檔包括 **Commit For Other Admins**（為其他管理員認可）的權限，則 Panorama 會認可由任何管理員設定的變更。若您的管理員角色設定檔不包含 **Commit For Other Admins**（為其他管理員認可）的權限，則 Panorama 只會認可您的變更，而不會認可其他管理員的變更。 若您已實作存取網域，則 Panorama 會自動套用這些網域以篩選認可範圍（請參閱 [Panorama > 存取網域]）。無論您的管理角色為何，Panorama 都只會認可指派給您帳戶的存取網域中產生的組態變更。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
依做成者認可變更	篩選 Panorama 認可之組態變更的範圍。指派給您用來登入之帳戶的管理員角色，會決定您的篩選選項： • 超級使用者角色—您可將認可範圍限制到特定管理員做出的變更，和特定位置中的變更。 • 自訂角色—指派給您帳戶之管理員角色設定檔的權限會決定篩選選項（請參閱 [Panorama > 管理員角色]）。若設定檔包含 **Commit For Other Admins**（為其他管理員認可）的權限，則您可將認可範圍限制到特定管理員設定的變更，和特定位置中的變更。若您的管理員角色設定檔不包含 **Commit For Other Admins**（為其他管理員認可）的權限，則只能將認可範圍限制到您在特定位置中所做的變更。 篩選認可範圍，如下所示： • 依管理員篩選—即便您的角色允許認可其他管理員的變更，認可範圍依預設仍僅包含您的變更。若要將其他管理員新增至認可範圍，請按一下 *<usernames>*（使用者名稱）連結、選取管理員，然後按一下 **OK**（確定）。 • 依位置篩選—選取特定位置以將變更包含在認可中。 若您已實作存取網域，Panorama 會自動根據這些網域篩選認可範圍（請參閱 [Panorama > 存取網域]）。無論您的管理角色和篩選選取為何，認可範圍都只會包含指派給您帳戶之存取網域中的組態變更。 載入組態（裝置 > 設定 > 操作（Device > Setup > Operations））後，您必須 *Commit All Changes*（認可所有變更）。 當您將變更認可至裝置群組時，必須包含對該裝置群組中的相同規則庫新增、刪除或重新定位了規則的所有管理員所做的變更。
認可範圍	列出有變更待認可的位置。清單是否包含所有變更或變更中的子集取決於若干因素，如針對認可所有變更和依做成者認可變更所述。位置可以是下列任一項： • **shared-object**（共用物件）—在共用位置中定義的設定。 • *<device-group*（裝置群組）*>*—會在其中定義原則規則或物件的裝置群組名稱。 • *<template*（範本）*>*—會在其中定義設定的範本或範本堆疊名稱。 • *<log-collector-group*（日誌收集器群組）*>*—會在其中定義設定的收集器群組名稱。 • *<log-collector*（日誌收集器）*>*—會在其中定義設定的日誌收集器名稱。 • *<wildfire-appliances*（*wildfire* 裝置）*>*—會在其中定義設定的 WildFire 裝置序號。 • *<wildfire-appliance-clusters*（*wildfire* 裝置叢集）*>*—會在其中定義設定的 WildFire 叢集名稱。
Location Type (位置類型)	此欄分類擱置中變更的位置： • **Panorama**—特定於 Panorama 管理伺服器組態的設定。 • **Device Group**（裝置群組）—特定裝置群組中定義的設定。 • **Template**（範本）—特定範本或範本堆疊中定義的設定。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	• **Log Collector Group**（日誌收集器群組）—特定於收集器群組組態的設定。 • **Log Collector**（日誌收集器）—特定於日誌收集器組態的設定。 • **WildFire Appliance Clusters**（**Wildfire** 裝置叢集）—特定於 WildFire 裝置叢集組態的設定。 • **WildFire Appliances**（**Wildfire** 裝置）—特定於 WildFire 裝置的設定。 • **Other Changes**（其他變更）—非特定於任何之前組態區域（例如共用物件）的設定。
包含在認可中 （僅限部分認可）	可讓您選取要認可的變更。依預設會選取 **Commit Scope**（認可範圍）內的所有變更。此欄僅會在您選取 **Commit Changes Made By**（依做成者認可變更）並選取特定管理員之後顯示。 可能有相依性會影響您包含在認可中的變更。例如，如果在您新增某物件後，有另一個管理員編輯了該物件，您就無法僅認可該名管理員的變更，而不認可您自己的變更。
依類型分組	依 **Location Type**（位置類型）將 **Commit Scope**（認可範圍）中的組態變更清單分組。
預覽變更	可讓您比較在 **Commit Scope**（認可範圍）中選取的組態與執行中的組態。預覽視窗會以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。 為方便比對 Web 介面區段的變更，您可以設定在每次變更前後顯示 **Lines of Context**（內容行）的預覽視窗。這些內容行來自於您所比較的候選組態與執行中組態的檔案。 預覽結果會顯示在新的瀏覽器視窗中，因此您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參考瀏覽器文件，以取得允許快顯視窗的步驟。
變更摘要	列出要認可變更的個別設定。**Change Summary**（變更摘要）清單會顯示各個設定的下列資訊： • **Object Name**（物件名稱）—可識別原則、物件、網路設定或裝置設定的名稱。 • **Type**（類型）—設定的類型（例如位址、安全性規則或區域）。 • **Location Type**（位置類型）—指出是在 **Device Groups**（裝置群組）、**Templates**（範本）、**Collector Groups**（收集器群組）、**WildFire Appliances**（**WildFire** 裝置）或 **Wildfire Appliance Clusters**（**WildFire** 裝置叢集）中定義設定。 • **Location**（位置）—定義設定的裝置群組、範本、收集器群組、WildFire 叢集或 WildFire 裝置的名稱。針對未在這些位置中定義的設定，此欄會顯示 **Shared**（共用）。 • **Operations**（操作）—指出自上次認可以來對設定執行的每個操作（建立、編輯或刪除）。 • **Owner**（擁有者）—上次對設定進行變更的管理員。 • **Will Be Committed**（將受認可）—指出認可是否將包含設定。 • **Previous Owners**（先前的擁有者）—在上次變更前對設定進行變更的管理員。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	您可以選取性地以欄名稱（例如 **Type**（類型））作為 **Group By**（分組依據）。
驗證提交	驗證 Panorama 組態的語法是否正確，以及語意是否完整。輸出會包含認可所將顯示的相同錯誤和警告，包括規則鏡像處理和應用程式相依性警告。驗證程序可讓您在認可前找出錯誤並加以修正（此程序並不會變更執行中的組態）。如果您使用固定認可視窗，而想要確定認可將成功而不發生錯誤，驗證程序將有所幫助。
當您透過選取 **Commit**（認可）> **Push to Devices**（推送至裝置）或 **Commit**（認可）> **Commit and Push**（認可並推送）來將組態變更推送至受管理的裝置時，適用下列選項。	
推送範圍	列出有待推送變更的位置。依預設，範圍包含的位置取決於您選取的下列選項： • **Commit**（認可）> **Commit and Push**（認可並推送）—範圍包含有需要 Panorama 認可之變更的所有位置。 • **Commit**（認可）> **Push to Devices**（推送至裝置）—範圍包含與 Panorama 執行中設定非同步之實體（防火牆、虛擬系統、日誌收集器、WildFire 叢集、WildFire 裝置）相關聯的所有位置（若需同步化狀態，請參閱 Panorama > Managed Devices > Summary（Panorama > 受管理的裝置 > 摘要）和 Panorama > Managed Collectors（Panorama > 受管理的收集器））。 針對兩個選項，Panorama 均依下列方式篩選 **Push Scope**（推送範圍）： • 管理員—Panorama 套用與 **Commit Scope**（認可範圍）相同的篩選（請參閱 認可所有變更或依做成者認可變更）。 • 存取網域—若您實作存取網域，Panorama 會根據這些網域自動篩選 **Push Scope**（推送範圍）（請參閱 [Panorama > 存取網域]）。無論您的管理角色和篩選選取為何，範圍都只會包含指派給您帳戶之存取網域中的組態變更。 您可針對 **Push Scope**（推送範圍）編輯選項而非接受預設位置。
Location Type (位置類型)	此欄分類擱置中變更的位置： • **Device Groups**（裝置群組）—特定裝置群組中定義的設定。 • **Templates**（範本）—特定範本或範本堆疊中定義的設定。 • **Log Collector Groups**（日誌收集器群組）—特定於收集器群組組態的設定。 • **WildFire Clusters**（**Wildfire** 叢集）—特定於 WildFire 叢集組態的設定。 • **WildFire Appliances**（**Wildfire** 裝置）—特定於 WildFire 裝置組態的設定。
實體	針對各裝置群組或範本，此欄列出包含於推送操作中的防火牆（依裝置名稱或序號）或虛擬系統（依名稱）。 若您將變更推送至收集器群組，則該操作會包含群組中成員的所有日誌收集器，即使該日誌收集器並未列出。
編輯選取	按一下以選取要包含在推送操作中的實體：

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
	• 裝置群組與範本 • 日誌收集器群組 • WildFire 裝置和叢集 *Panorama* 無法讓您將尚未認可的變更推送至 *Panorama* 組態。
裝置群組與範本	**Edit Selections**（編輯選項）並選取 **Device Groups**（裝置群組）或 **Templates**（範本），在以下列中顯示選項。
篩選器	篩選範本、範本堆疊、裝置群組以及相關的防火牆與虛擬系統之清單。 您還可以根據其提交狀態、裝置狀態、標籤和高可用性 (HA) 狀態來篩選受管理防火牆。
名稱	選取要包含在推送操作中的範本、範本堆疊、裝置群組、防火牆或虛擬系統。
上次提交狀態	指出防火牆與虛擬系統組態是否與 Panorama 中的範本或裝置群組同步。
HA 狀態	指出所列示防火牆的高可用性 (HA) 狀態。 • **Active**（主動）—正常流量處理操作狀態。 • **Passive**（被動）—正常備份狀態。 • **Initiating**（啟動中）—開機後，防火牆處於此狀態會持續最多 60 秒。 • **Non-functional**（非作用中）—錯誤狀態。 • **Suspended**（已暫停）—管理員已停用防火牆。 • **Tentative**（暫訂）—針對於主動/主動組態中的連結或路徑監控事件。
變更擱置中 (Panorama) 提交	指出您將變更推送至所選的防火牆和虛擬系統前，是否需要 Panorama 認可（是或否）。
預覽變更欄	**Preview Changes**（預覽變更）以比較您在 **Push Scope**（推送範圍）中選取的組態與 Panorama 執行中組態。Panorama 會篩選輸出以僅顯示您在 **Device Groups**（裝置群組）或 **Templates**（範本）頁籤中選取的結果。預覽視窗會以不同的顏色指出哪些變更是新增（綠色）、修改（黃色）或刪除（紅色）。 預覽結果會顯示在新的瀏覽器視窗中，因此您的瀏覽器必須允許快顯視窗。如果預覽視窗未開啟，請參考瀏覽器文件，以取得允許快顯視窗的步驟。
全選	選取清單中的所有項目。
取消全選	取消選取清單中的所有項目。
全部展開	顯示指派給範本、範本堆疊或裝置群組的防火牆和虛擬系統。
全部摺疊	僅顯示範本、範本堆疊或裝置群組，而非指派給它們的防火牆或虛擬系統。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
群組 HA 端點	針對在高可用性 (HA) 組態中作為端點的防火牆進行分組。結果清單會先顯示主動防火牆（在主動/主動組態中為主動-主要防火牆），再顯示被動防火牆（在主要/主動組態中為主動-次要防火牆）。這可讓您輕鬆識別 HA 模式下的防火牆。套用共用原則時，您可以套用至群組配對，而非套用至個別配對。 對於主動/被動組態中的 *HA* 端點，考慮將兩個防火牆或其虛擬系統新增至同一裝置群組、範本或範本堆疊，以便您可將組態同時推送至兩個端點。
驗證	按一下以驗證您正在推送至所選防火牆和虛擬系統的組態。工作管理員會自動開啟以顯示驗證狀態。
已選取篩選器	若要清單僅顯示特定防火牆或虛擬系統，請選取該防火牆或虛擬系統，然後選取 **Filter Selected**（已選取篩選器）。
與應徵者設定合併	（預設為選取）將下列二者合併：從 Panorama 推送的組態變更，以及管理員在目標防火牆本機上實作的任何擱置中組態變更。推送操作會觸發 PAN-OS® 以認可合併的變更。如果清除此選項，認可將排除防火牆上的候選組態。 如果您允許防火牆管理員在防火牆本機上認可變更，而且不想在從 *Panorama* 認可變更時包含這些本機變更，則清除此選項。 另一個最佳做法是，在防火牆上執行組態稽核以檢閱任何本機變更，再透過 Panorama 推送變更（請參閱 [裝置 > 設定稽核]）。
包含裝置與網路範本 （僅限裝置群組頁籤）	（預設為選取）在單一操作中將裝置群組變更和相關聯的範本變更都推送至所選的防火牆和虛擬系統。若要作為單獨的操作來推送這些變更，請清除此選項。
強制範本值	（預設為停用）取代所有本機組態，並移除在範本或範本堆疊中不存在、或在本機組態中已取代的所選防火牆上的所有物件。推送操作會還原防火牆上的所有現有組態，並確保防火牆僅繼承範本或範本堆疊中定義的設定。 如果您在啟用 *Force Template Values*（強制範本值）的情況下推送一個設定，則防火牆上所有的取代值都將替換為範本中的數值。在使用此選項之前，請檢查防火牆上的取代值，以確保您的提交不會導致任何意外的網路中斷或因為更換這些取代值導致的問題。
日誌收集器群組	**Edit Selections**（編輯選項）並選取 **Log Collector Groups**（日誌收集器群組）以包含於推送操作中。此頁籤顯示下列選項： • **Select All**（全選）—選取清單中的每個收集器群組。 • **Deselect All**（取消全選）—取消選取清單中的每個收集器群組。
WildFire 裝置和叢集	**Edit Selections**（編輯選項）並選取 **WildFire Appliances and Clusters**（**WildFire** 裝置和叢集）以顯示下列選項。

© 2019 Palo Alto Networks, Inc.

欄位/按鈕	說明
篩選器	篩選 WildFire 裝置和叢集的清單。
名稱	選取 WildFire 裝置和叢集，Panorama 會針對該裝置和叢集推送變更。
上次提交狀態	指出 WildFire 裝置和叢集組態是否與 Panorama 同步。
移除選取	移除在「推送範圍」中列出的所有防火牆。
驗證裝置群組推送	驗證推送範圍清單中您正推送至裝置群組的組態。工作管理員會自動開啟以顯示驗證狀態。
驗證範本推送	驗證推送範圍清單中您正推送至範本的組態。工作管理員會自動開啟以顯示驗證狀態。
依位置類型分組	選取以使用 **Location Type**（位置類型）分組推送範圍清單。
您認可 Panorama 組態或將變更推送至裝置時適用下列選項。	
說明	輸入說明（最多 512 個字元）以協助其他管理員了解您做出的變更。 認可事件的系統日誌將會截斷超過 *512* 個字元的說明。
認可/推送/認可並推送	開始認可，或在有其他認可擱置的情況下，將認可新增至認可佇列。

© 2019 Palo Alto Networks, Inc.

在 Panorama 上定義原則

Panorama™ 的裝置群組可讓您集中管理防火牆上的原則。您在 Panorama 上建立的原則會是預先規則或後續規則；預先規則和後續規則可讓您在實作原則時建立分層方法。

您可在共用內容中，將預先規則和後續規則定義為所有受管理防火牆的共用原則，或定義於某個裝置群組內容中，使其成為某個裝置群組的特定規則。由於預先規則和後續規則是在 Panorama 上定義，然後從 Panorama 推送至受管理的防火牆，因此，您可以在受管理的防火牆上檢視這些規則，但只能在 Panorama 中編輯預先規則和後續規則。

- 預先規則—新增至規則順序的頂端，並且將優先評估的規則。您可以使用預先規則強制執行組織的可接受使用原則。例如，您可以封鎖存取特定 URL 類別或允許所有使用者的 DNS 流量。
- 後續規則—新增至規則順序的底部，並且在預先規則和防火牆本機上定義的規則之後才會評估的規則。後續規則通常包含會根據 App-ID™、User-ID™ 或服務拒絕他人存取流量的規則。
- 預設規則—用來指定防火牆如何處理不符合任何預先規則、後續規則或本機防火牆規則的流量。這些規則是預先定義的 Panorama 設定的一部分。若要 **Override**（取代）及啟用對這些規則中選定的設定進行編輯的功能，請參閱取代或還原安全性原則規則。

Preview Rules（預覽規則）可讓您先檢視完整規則清單，再將規則推送至受管理防火牆。在每個規則集內，會以視覺方式，針對每一個裝置群組（和受管理的防火牆）將規則階層分門別類，並且提供掃描大量規則的能力。

當您新增規則時，會顯示規則的靜態操作資料。通用唯一識別碼 (UUID) 欄位會為規則顯示 36 個字元的 UUID。防火牆會根據每個規則產生 UUID。然而，如果您要從 Panorama 推送規則，則這些規則會具有相同的 UUID，它們也會顯示在組合規則預覽中。**Created**（建立）欄位顯示了規則新增到規則庫的時間和日期。此外，**Modified**（修改）欄位顯示了規則上次編輯的時間和日期。如果原則規則是在升級到 PAN-OS 9.0 之前建立的，則會使用 **First Hit**（首次命中）資料產生 **Created**（建立）日期。如果規則不存在 **First Hit**（首次命中），則會使用防火牆或 Panorama 管理伺服器升級到 PAN-OS 9.0 的時間和日期產生建立（建立）日期。

當您在 Panorama 中新增或編輯規則時，會顯示 **Target**（目標）頁籤。您可以使用此頁籤將規則套用至特定防火牆，或是定義規則的 **Device Group**（裝置群組）（或共用位置）的子系裝置群組。在 **Target**（目標）頁籤中，您可以選取 **Any**（任何），這表示規則會套用至所有防火牆和子系裝置群組。若要以特定防火牆或裝置群組為目標，請取消選取 **Any**（任何），然後依名稱選取特定防火牆或裝置群組。若要排除特定防火牆或裝置群組，請取消選取 **Any**（任何）、依名稱選取特定防火牆或裝置群組，然後選取 **Target to all but these specified devices**（以指定裝置以外的所有裝置為目標）。如果裝置群組和防火牆的清單很長，您可以套用篩選器，依屬性（例如平台）或相符名稱的文字字串來搜尋項目。

在 Panorama 中成功增加並推送規則後， **Rule Usage**（規則使用方式）將顯示該規則是由裝置群組中的所有裝置使用、裝置群組中的某些裝置部分使用，還是裝置群組中的裝置不使用。Panorama 使用原則規則命中數（默認情況下啟用）基於託管防火牆確定規則使用方式。在 Panorama 上下文中，您可以檢視全部裝置群組共用原則規則的使用方式。此外，您可以將上下文變更為單個裝置群組，並查看裝置群組中所有裝置的總原則規則使用方式。**Preview Rules**（預覽規則）將顯示該裝置群組中每一個原則規則的 **Hit Count**（命中數）、**Last Hit**（最後命中）和**First Hit**（首次命中）。總流量命中數以及首先和最後命中時間戳記將在重新啟動、更新和重新啟動事件時持續存在。請參閱 Monitor Policy Rule Usage（監控原則規則使用方式）。

Group Rules by Tag（依頁籤群組規則）以應用頁籤，讓您可以將相似的原則規則分組以更好地將規則功能視覺化，並更輕鬆地管理規則庫中的策略規則。由頁籤分組的規則會顯示頁籤群組的清單，但會保留規則排列優先順序。您可以將規則附加到頁籤群組的末尾、將規則移動到其他頁籤群組，將其他頁籤應用到頁籤群組中的規則，以及使用群組頁籤進行篩選或搜尋。

如要追蹤原則規則的變更，新增一個 **Audit Comment**（稽核註解），說明您進行的變更以及建立或修改規則的原因。在您輸入稽核註解並確認組態變更後，稽核註解會儲存在 **Audit Comment Archive**（稽核註解封存檔）中，您可以在稽核註解封存檔中檢視選取的規則過去的全部稽核註解。您可以在「全域尋找」中搜尋稽核註解。稽核註解封存檔是唯讀的。

可訪問原則頁籤的管理使用者可以匯出以 **PDF/CSV** 顯示在網路介面的原則規則。請參閱匯出設定表資料。

© 2019 Palo Alto Networks, Inc.

若要建立原則，請參閱每個規則庫的相關章節：

- Policies > Security（原則 > 安全性）
- Policies > NAT（原則 > NAT）
- Policies > QoS（原則 > QoS）
- Policies > Policy Based Forwarding（原則 > 基於原則的轉送）
- Policies > Decryption（原則 > 解密）
- Policies > Application Override（原則 > 應用程式取代）
- Policies > Authentication（原則 > 驗證）
- Policies > DoS Protection（原則 > DoS 保護）
- Policies > SD-WAN（政策 > SD-WAN）

© 2019 Palo Alto Networks, Inc.

傳統模式下 Panorama 虛擬裝置的日誌儲存分割區

- Panorama > Setup > Operations（Panorama > 設定 > 操作）

依預設，傳統模式的 Panorama 虛擬裝置會使用單一磁碟分割區來儲存所有資料；並且會配置其中的 10.89GB 來儲存日誌。增加磁碟大小並不會增加日誌儲存容量；不過，您可以使用下列選項修改日誌儲存容量：

- 網路檔案系統 **(NFS)**—只有在 VMware ESXi 伺服器上執行的傳統模式 Panorama 虛擬裝置可使用安裝 NFS 儲存區的選項。若要安裝 NFS 儲存區，請選取 [雜項] 區段中的 **Storage Partition Setup**（儲存分割區設定），將 **Storage Partition**（儲存分割區）設定為 **NFS V3**，並設定 表格：NFS 儲存區設定。
- 預設內部儲存區—還原為預設內部儲存分割區（僅適用於先前已設定了其他虛擬記錄磁碟或安裝到 NFS 上之 ESXi 伺服器或 vCloud Air 平台上的 Panorama）。若要還原為預設內部儲存分割區，請選取雜項區段中的 **Storage Partition Setup**（儲存分割區設定），並將 **Storage Partition**（儲存分割區）設定為 **Internal**（內部）。
- 虛擬記錄磁碟—您可以為 VMware ESXi 5.5 版和更新版本上所執行的 Panorama 或為 VMware vCloud Air 平台上所執行的 Panorama 新增其他虛擬磁碟（最多 8TB）。不過，Panorama 會停止使用原磁碟上預設的 10.89GB 日誌儲存空間並會將現有日誌複製到新磁碟上。（舊版 ESXi 最多只支援 2TB 虛擬磁碟。）

您必須在變更儲存分割區設定後重新啟動 *Panorama*：選取 *Panorama* > *Setup*（設定）> *Operations*（操作）和 *Reboot Panorama*（重新啟動 *Panorama*）。

NFS 儲存區不適用於 *Panorama* 模式的 *Panorama* 虛擬裝置，也不適用於 *M-Series* 裝置。

表 **1:** 表格：**NFS** 儲存區設定

Panorama 儲存分割區設定—NFS V3	說明
伺服器	輸入 NFS 伺服器的 FQDN 或 IP 位址。
日誌目錄	指定日誌將駐留之目錄的完整路徑名稱。
通訊協定	指定用於與 NFS 伺服器通訊的通訊協定（UDP 或 TCP）。
連接埠	指定與 NFS 伺服器通訊的連接埠。
讀取大小	為 NFS 讀取操作指定大小上限（單位是位元組，範圍是 256 到 32,768）。
寫入大小	為 NFS 寫入操作指定大小上限（單位是位元組，範圍是 256 到 32,768）。
安裝時複製	選取此選項可安裝 NFS 分割區，並且當 Panorama 啟動時，會將任何現有日誌複製到伺服器上的目的地目錄。
測試日誌記錄分割區	選取此選項可執行安裝 NFS 分割區的測試，並顯示成功或失敗訊息。

© 2019 Palo Alto Networks, Inc.

Panorama > Setup > Interfaces（Panorama > 設定 > 介面）

- Panorama > Setup > Interfaces（Panorama > 設定 > 介面）

選取 **Panorama** > **Setup**（設定） > **Interfaces**（介面）以設定介面，Panorama 使用該介面管理防火牆和日誌收集器，將軟體和內容更新部署至防火牆和日誌收集器，從防火牆收集日誌，並與收集器群組通訊。依預設，Panorama 在對防火牆和日誌收集器的所有通訊中使用管理 (MGT) 介面。

若要減少 *MGT* 介面上的流量，請設定其他介面以部署更新、收集日誌、與收集器群組通訊。在有大量日誌流量的環境中，您可以針對日誌收集設定數個介面。此外，為改進管理流量的安全性，您可以為 *MGT* 介面定義個別的子網路（*IPv4 Netmask*（網路遮罩）或 *IPv6 Prefix Length*（前置詞長度）），該子網路較其他介面的子網路更具私密性。

可用的介面視 Panorama 型號而不同。

介面	速度上限	M-500 Appliance 設備	Panorama 虛擬設備
管理 (MGT)	1Gbps	✓	✓
Ethernet1 (Eth1)	1Gbps	✓	—
Ethernet2 (Eth2)	1Gbps	✓	—
Ethernet3 (Eth3)	1Gbps	✓	—
Ethernet4 (Eth4)	10Gbps	✓	—
Ethernet5 (Eth5)	10Gbps	✓	—

若要設定介面，按一下介面名稱並進行下表所述的設定。

請務必為 *MGT* 介面指定 *IP* 位址、網路遮罩（針對 *IPv4*）或前置詞長度（針對 *IPv6*）、預設閘道。如果您省略某些設定的值（例如預設閘道），則未來需要變更設定時，您只能透過主控台連接埠存取 *Panorama*。除非您指定這三個設定，不然無法為其他介面認可設定。

介面設定	說明
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	您必須啟用介面才能對其進行設定。MGT 介面則屬例外，其依預設會是啟用狀態。
IP 位址 (IPv4)	如果網路使用 IPv4 位址，請將 IPv4 位址指派給介面。
網路遮罩 (IPv4)	如果將 IPv4 位址指派給介面，則您也必須輸入網路遮罩（例如 255.255.255.0）。
預設閘道 (IPv4)	如果將 IPv4 位址指派給介面，則您也必須將 IPv4 位址指派給預設閘道（閘道必須位於與介面相同的子網路上）。

© 2019 Palo Alto Networks, Inc.

介面設定	說明
IPv6 位址/首碼長度	如果網路使用 IPv6 位址，請將 IPv6 位址指派給介面。若要指出網路遮罩，請輸入 IPv6 首碼長度（例如，2001:400:f00::1/64）。 對於所有 *M-Series* 設備和在私人雲端環境（*ESXi*、*vCloud Air*、*KVM* 或 *Hyper-V*）中部署的 *Panorama* 虛擬設備上的 *MGT* 介面，支援 *IPv6* 位址。對於在公用雲端環境（*Amazon Web Services (AWS)*、*AWS GovCloud*、*Microsoft Azure* 或 *Google Cloud Platform*）中部署的 *Panorama* 虛擬設備上的 *MGT* 介面，不支援 *IPv6* 位址。
預設 IPv6 閘道	如果將 IPv6 位址指派給介面，則您也必須將 IPv6 位址指派給預設閘道（閘道必須位於與介面相同的子網路上）。 對於所有 *M-Series* 設備和在私人雲端環境（*ESXi*、*vCloud Air*、*KVM* 或 *Hyper-V*）中部署的 *Panorama* 虛擬設備上的 *MGT* 介面，支援 *IPv6* 位址。對於在公用雲端環境（*Amazon Web Services (AWS)*、*AWS GovCloud*、*Microsoft Azure* 或 *Google Cloud Platform*）中部署的 *Panorama* 虛擬設備上的 *MGT* 介面，不支援 *IPv6* 位址。
速度	將全雙工或半雙工下的介面速度設定至 10Mbps、100Mbps、1Gbps 或 10Gbps（僅限 Eth4 和 Eth5）。使用預設自動交涉設定，可讓 Panorama 決定介面速度。 此設定必須與相鄰網路設備的介面設定相符。為確保符合設定，如果相鄰裝置支援該選項，請選取自動交涉。
MTU	以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 1,500；預設為 1,500）。
設備管理及設備日誌收集	啟用介面（在 MGT 介面上預設為啟用）以管理防火牆和日誌收集器，並收集其日誌。您可啟用多個介面以執行這些功能。
收集器群組通訊	啟用收集器群組通訊的介面（預設為 MGT 介面）。只有一個介面可執行此功能。
Syslog 轉送	啟用轉送 syslog 的介面（預設為 MGT 介面）。只有一個介面可執行此功能。
設備部署	啟用介面以將軟體和內容更新部署至防火牆和日誌收集器（預設為 MGT 介面）。只有一個介面可執行此功能。
系統管理服務	• **HTTP**—可讓您存取 Panorama Web 介面。HTTP 使用純文字，不如 HTTP 安全。 請啟用 *HTTPS* 而非 *HTTP* 來管理介面上的流量。 • **Telnet**—可讓您存取 Panorama CLI。Telnet 使用純文字，不如 SSH 安全。 • **HTTPS**—可讓您安全存取 Panorama Web 介面。

© 2019 Palo Alto Networks, Inc.

介面設定	說明
	請啟用 *SSH* 而非 *Telnet* 來管理介面上的流量。 • **SSH**—可讓您安全存取防火牆 CLI。
網路連線服務	**Ping** 服務在任何介面都可用。您可使用 ping 測試 Panorama 介面和外部服務之間的連線。在高可用性 (HA) 部署中，HA 端點使用 ping 來交換活動訊號備援資訊。 下列服務則只能在 MGT 介面上使用： • **SNMP**—可讓 Panorama 處理來自 SNMP 管理員的統計資料查詢。如需詳細資訊，請參閱啟用 SNMP 監控。 • **User-ID**—讓 Panorama 可重新散佈從 User-ID 代理程式接收的使用者對應資訊。
許可的 IP 位址	輸入 IP 位址，管理員可在此介面上從該位址存取 Panorama。空白清單（預設值）會指定可從任何 IP 位址進行存取。 請勿將此清單保留空白；（僅）指定 *Panorama* 管理員的 *IP* 位址可防止未經授權的存取。

© 2019 Palo Alto Networks, Inc.

Panorama > 高可用性

若要在 Panorama 上啟用高可用性 (HA)，請按下表所述進行設定。

Panorama HA 設定	說明
設定 按一下編輯 ( ) 可進行下列設定：	
啟用 HA	選取以啟用 HA。
Peer HA IP Address	在端點上輸入 MGT 介面的 IP 位址。
Enable Encryption	啟用後，MGT 介面會加密 HA 端點之間的通訊。啟用加密前，將 HA 金鑰從每個 HA 端點匯出，並將金鑰匯入其他端點。您可在 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證）頁面匯入和匯出 HA 金鑰（請參閱管理防火牆和 Panorama 憑證）。 在啟用加密的情況下，*HA* 連線會使用 *TCP* 連接埠 *28*，在未啟用加密的情況下，*HA* 連線會使用 *TCP* 連接埠 *28769*。
Monitor Hold Time (ms)	以毫秒為單位輸入系統因控制連結失敗而採取動作之前將會等待的時間（範圍為 1,000 至 60,000；預設值為 3,000）。
選取設定 按一下編輯 ( ) 可進行下列設定：	
優先順序 （在 Panorama 虛擬裝置上需要）	此設定可確定哪個端點為防火牆日誌的主要收件者。在 HA 配對中將一個端點指派為 **Primary**（主要）裝置，而將另一個指派為 **Secondary**（次要）裝置。 當您設定傳統模式下的 Panorama 虛擬應用程式的日誌儲存分割區時，您可使用其內部磁碟（預設值）或網路檔案系統 (NFS) 以供日誌儲存。如果您設定 NFS，僅主要收件者可接收防火牆日誌。若您設定內部磁碟儲存，防火牆依預設會將日誌傳送至主要和次要端點，但您可變更此預設值，具體方法是在記錄日誌與報告設定中啟用 **Only Active Primary Logs to Local Disk**（僅將主動主要日誌傳送至本機磁碟）。
先佔	選取可使主要 Panorama 在從失敗復原之後繼續主動操作。如果此設定為停用，則即使在主要 Panorama 從失敗復原之後，次要 Panorama 仍然會保持主動。
HA 計時器設定	您的選項會決定剩餘 HA 選項設定的值，該值用於控制容錯轉移速度： • **Recommended**（建議）—對於一般（預設值）容錯移轉計時器設定，可選取此選項。若要查看相關的值，請選取 **Advanced**（進階）與 **Load Recommended**（建議的載入）。 • **Aggressive**（積極）—對於更快的容錯轉移計時器設定，可選取此選項。若要查看相關的值，請選取 **Advanced**（進階）與 **Load Aggressive**（積極的載入）。 • 進階—選取此選項可顯示剩餘的 HA 選取設定，並可自訂其值。 請參閱下列設定的 **Recommended**（建議）以及 **Aggressive**（積極）值。

© 2019 Palo Alto Networks, Inc.

Panorama HA 設定	說明
Promotion Hold Time (ms)	輸入主要端點關閉後，次要 Panorama 端點接管之前需等候的毫秒數（範圍是 0 至 60,000）。建議（預設）值為 2,000；加強值為 500。
Hello 間隔（毫秒）	輸入 Hello 封包傳送間的毫秒數（範圍是 8,000 至 60,000），傳送 Hello 封包是用於確認其他端點是否可正常操作。建議（預設）值及積極值為 8,000。
Heartbeat Interval (ms)	指定 Panorama 傳送 ICMP ping 至 HA 端點的頻率（毫秒，範圍是 1,000 至 60,000）。建議（預設）值為 2,000；加強值為 1000。
先佔保留時間（分鐘）	此欄位僅在您也選取 **Preemptive**（先佔）時適用。輸入被動 Panorama 端點從導致容錯轉移的事件復原後，回復到主動狀態之前將等候的分鐘數（範圍是 1 至 60）。建議（預設）值及積極值為 1。
監控失敗維持時間（毫秒）	指定 Panorama 在路徑監控失敗後，嘗試重新進入被動狀態之前的毫秒數（範圍是 0 至 60,000）。在此期間內，如果發生失敗，被動端點就無法接管主動端點。此間隔可讓 Panorama 避免由於相鄰裝置偶而波動所致的容錯轉移。建議（預設）值及積極值為 0。
Additional Master Hold Up Time (ms)	指定先佔端點在接管主動端點之前保持被動狀態的毫秒數（範圍是 0 至 60,000）。建議（預設）值為 7,000；加強值為 5,000。
路徑監控 按一下編輯（ ）以設定 HA 路徑監控。	
已啟用	選取以啟用路徑監控。路徑監控可讓 Panorama 監控指定的目的地 IP 位址，方法是傳送 ICMP ping 訊息以確定它們是否有回應。
失敗條件	選取當 **Any**（任何）或 **All**（全部）監控的路徑群組無法回應時是否發生容錯轉移。
路徑群組 若要為 HA 路徑監控建立路徑群組，請按一下 **Add**（新增）並填寫下列欄位：	
名稱	指定路徑群組的名稱。
已啟用	選取以啟用路徑群組。
失敗條件	選取當 **Any**（任何）或 **All**（全部）指定的目的地位址無法回應時是否發生失敗。
Ping 間隔	指定 ICMP 回應訊息間的毫秒數（範圍是 1,000 至 60,000；預設為 5,000），ICMP 回應訊息會確認至目的地 IP 位址的路徑為使用中。
Ping 計數	指定宣告失敗前失敗的 ping 數（範圍是 3 至 10；預設為 3）。
目的地 IP	輸入要監控的一個或多個目的地 IP 位址。使用逗號來分隔多個位址。

© 2019 Palo Alto Networks, Inc.

Panorama > 受管理的 WildFire 叢集

- Panorama > 受管理的 WildFire 叢集
- Panorama > 受管理的 WildFire 設備

您可以在叢集中管理 WildFire 設備，或作為獨立於 Panorama M-Series 或虛擬設備的設備管理。管理叢集（**Panorama** > **Managed WildFire Clusters**（受管理 **WildFire** 叢集））與管理獨立設備（**Panorama** > **Managed WildFire Appliances**（受管理 **WildFire** 設備））共用許多通用管理和設定工作，因此兩者都包含於下列主題中。

在您將 WildFire 設備新增至 Panorama 後，使用 Web 介面以將這些設備新增至叢集，並作為叢集管理這些設備，或作為獨立設備管理這些設備。

- 受管理的 WildFire 叢集工作
- 受管理的 WildFire 設備工作
- 受管理的 WildFire 資訊
- 受管理的 WildFire 叢集和裝置的管理

受管理的 WildFire 叢集工作

您可以從 Panorama 建立和移除 WildFire 設備叢集。此外，您也可以當在設定從某個叢集匯入到另一個叢集時節省設定時間。

工作	說明
建立叢集	視需要 **Create Cluster**（建立叢集），輸入新叢集的名稱，然後按一下 **OK**（確定）。 您在本機所設定並藉由新增個別的 WildFire 設備節點而新增到 Panorama 的現有叢集，會與其 WildFire 節點和節點角色一起列出（**Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備））。 叢集名稱必須是有效的子網域名稱，以小寫字元或數字開頭，而且可以包含連字號（只有當連字號不是叢集名稱內的第一個或最後一個字元時）—不允許使用空格或其他字元。叢集名稱的最大長度為 63 個字元。 在建立叢集之後，您可以將受管理的 WildFire 設備新增至叢集，並在 Panorama 上進行管理。當您將 WildFire 設備新增至 Panorama 時，您就會自動向 Panorama 註冊該設備。 您最多可以在 Panorama 上建立 10 個受管理的 WildFire 叢集，而且每個叢集最多可以擁有 20 個 WildFire 設備節點。Panorama 最多可以管理加總起來共 200 個的獨立設備和叢集節點。
匯入叢集設定	**Import Cluster Config**（匯入叢集設定）可匯入現有的叢集設定。如果您先選取叢集再 **Import Cluster Config**（匯入叢集設定），**Controller**（控制器）和 **Cluster**（叢集）會自動填入所選叢集的適當資訊。如果您未先選取叢集就 **Import Cluster Config**（匯入叢集設定），則必須選取 **Controller**（控制器），而 **Cluster**（叢集）則會根據您所選取的控制器節點自動填入。 在匯入設定之後，**Commit to Panorama**（認可至 **Panorama**）以將匯入的候選設定儲存到 Panorama 的執行中設定。
從 Panorama 移除	如果您不再需要從 Panorama 管理 WildFire 叢集，請 **Remove From Panorama**（從 **Panorama** 移除），然後選取 **Yes**（是）來確認您的動作。在從

© 2019 Palo Alto Networks, Inc.

工作	說明
	Panorama 管理移除叢集之後，您可以從控制器節點本機管理該叢集。如果您想要再次集中管理叢集而不是在本機管理時，您可以隨時將該叢集新增回 Panorama 設備。
加密 WildFire 叢集設備至設備通訊	若要加密在一個叢集中的 WildFire 應用程式間的資料通訊，則**Enable**（啟用）在**Secure Cluster Communication**（安全叢集通訊）下的解密。 WildFire 使用預定義驗證或自訂驗證以在設備間進行通訊。自訂憑證僅限用在您 **Customize Secure Server Communication**（自訂安全伺服器通訊）以及啟用 **Custom Certificate Only**（僅限自訂憑證）時。 在 FIP-CC 模式中操作 WildFire 叢集需要解密。用於 FIPS-CC 模式中的自訂憑證必須符合 FIPS-CC 需求。 在您啟用安全叢集通訊後，您可以新增其他託管 WildFire 設備至叢集中。新近新增的設備會自動使用安全叢集通訊設定。

受管理的 WildFire 設備工作

您可以在 Panorama 設備上新增、移除和管理獨立的 WildFire 設備。在新增獨立的設備之後，您可以將其新增至 WildFire 設備叢集來作為叢集節點，或者，您也可以把這些設備當作個別的獨立設備來進行管理。

工作	說明

新增設備	**Add Appliance**（新增設備）可將一或多個 WildFire 設備新增到 Panorama 設備以集中進行管理。在不同列（換行）輸入每個 WildFire 設備的序號。Panorama 最多可以管理加總起來共 200 個的 WildFire 叢集節點和獨立的 WildFire 設備。
	在您要於 Panorama 上管理的每個 WildFire 設備上，設定 Panorama 設備（Panorama 伺服器）的 IP 位址或 FQDN，並（選擇性）使用下列 WildFire 設備 CLI 命令來設定備用的 Panorama 伺服器：
	`set deviceconfig system panorama-server <ip-address | FQDN>`
	`set deviceconfig system panorama-server-2 <ip-address | FQDN>`

匯入設定	選取 WildFire 設備並 **Import Config**（匯入設定）以便（只）將該設備的執行中設定匯入到 Panorama。 在匯入設定之後，**Commit to Panorama**（認可至 **Panorama**）以將匯入的候選設定儲存到 Panorama 的執行中設定。
移除	如果您不再需要從 Panorama 管理 WildFire 設備，請 **Remove**（移除）該設備，然後選取 **Yes**（是）來確認您的動作。在從 Panorama 管理移除設備之後，您可以在設備本機使用其 CLI 來管理該項設備。如有需要，當您想要再次集中管理設備而不是在本機管理時，您也可以隨時將該設備新增回 Panorama 設備。

© 2019 Palo Alto Networks, Inc.

受管理的 WildFire 資訊

選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集）可針對每個受管理的叢集顯示下列資訊（您也可以從此頁面選取獨立的設備，然後顯示其資訊），選取 **Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）則可針對獨立的設備顯示資訊。

除非另行說明，否則下表中的資訊會同時適用於 WildFire 叢集和獨立設備。先前已對叢集或設備設定的資訊會預先填入。

受管理的 WildFire 資訊	說明
裝置	設備名稱。 受管理的 WildFire 叢集檢視會顯示叢集所群組的設備，包括可供新增至叢集的獨立設備，以及序號（以括號括住）與設備名稱（序號不是名稱的一部分）。
序號 （僅限受管理的 WildFire 設備檢視）	設備的序號。受管理的 WildFire 叢集檢視會在和設備名稱相同的欄中顯示序號（序號不是名稱的一部分）。
軟體版本	設備上所安裝和執行的軟體版本。
IP 位址	設備的 IP 位址。
已連線	設備和 Panorama 之間的連線狀態—已連線或已中斷連線。
叢集名稱	設備會納入其中作為節點之叢集的名稱；這裡不會顯示獨立設備的任何資訊。
分析環境	分析環境（vm1、vm2、vm3、vm4 或 vm5）。每個分析環境都代表一組作業系統和應用程式： • vm-1 支援 Windows XP、Adobe Reader 9.3.3、Flash 9、PE、PDF 和 Office 2003 與舊版 Office。 • vm-2 支援 Windows XP、Adobe Reader 9.4.0、Flash 10n、PE、PDF 和 Office 2007 與舊版 Office。 • vm-3 支援 Windows XP、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 與舊版 Office。 • vm-4 支援 Windows 7 32 位元、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 與舊版 Office。 • vm-5 支援 Windows 7 64 位元、Adobe Reader 11、Flash 11、PE、PDF 和 Office 2010 與舊版 Office。
內容	內容發行版本的版本號碼。
Role	設備角色： • **Standalone**（獨立）—該設備不是叢集節點。 • **Controller**（控制器）—該設備是叢集控制器節點。 • **Controller Backup**（控制器備份）—該設備是叢集控制器備份節點。 • **Worker**（背景工作）—該設備是叢集內的背景工作節點。
設定狀態	設備的設定同步化狀態。Panorama 設備會檢查 WildFire 設備設定，並報告設備設定和該設備在 Panorama 上所儲存之設定之間的設定差異。

© 2019 Palo Alto Networks, Inc.

受管理的 WildFire 資訊	說明
	• **In Sync**（同步）—設備設定和其在 Panorama 上所儲存的設定同步。 • **Out of Sync**（不同步）—設備設定和其在 Panorama 上所儲存的設定不同步。可以使滑鼠停留在放大鏡上來顯示同步失敗原因。

叢集狀態
（僅限受管理的 WildFire 叢集頁面）
	叢集狀態會為每個叢集節點顯示三種類型的資訊：
	• 可用的服務（一般作業狀況）：
	  • **wfpc**（WildFire 私人雲端）— 惡意軟體樣本分析和報告服務。
	  • 特徵碼—本機特徵碼產生服務。
	• 作業進度—作業名稱後接冒號 (:) 和狀態：
	  • 作業—解除、暫停和重新啟動作業的狀態。
	  • 進度狀態—每項作業的作業狀態通知都相同：已要求、進行中、已拒絕、成功、失敗。
	  例如，如果您暫停節點但作業仍在進行，叢集狀態會顯示 `suspend:ongoing`，或者，如果您重新啟動節點且已要求作業，但作業尚未開始，則叢集狀態會顯示 `reboot:requested`。
	• 錯誤狀況：
	  叢集狀態會顯示下列錯誤狀況：
	  • 叢集—`cluster:offline` 或 `cluster:splitbrain`。
	  • 服務—`service:suspended` 或 `service:none`。

上次提交狀態	如果最新的認可成功，則狀態為認可成功，如果最新的認可失敗，則狀態為認可失敗。選取狀態即可檢視最後一次認可的詳細資料。
使用率 > 檢視	

檢視	**View**（檢視）叢集或設備的使用率統計資料。您只能檢視個別的設備（**Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備））或只能檢視叢集的統計資料（**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集））。
	• **Appliance**（設備）—（僅限獨立設備檢視）設備序號。
	• **Cluster**（叢集）—（僅限叢集檢視）叢集名稱。您也可以選取不同的叢集來進行檢視。
	• **Duration**（持續時間）—顯示所收集和顯示的統計資料是來自哪個時段。您可以選取不同的持續時間：
	  • **15** 分鐘
	  • 前一小時
	  • 過去 **24** 小時（預設值）
	  • 前 **7** 天
	  • 全部
	Utilization（使用率）**View**（檢視）具有四個頁籤，而且在每個頁籤上，您都可以決定要根據所設定的**Duration**（持續時間）來顯示的內容。

一般頁籤	**General**（一般）頁籤會顯示叢集或設備的資源使用率彙總統計資料。其他頁籤則會顯示依檔案類型分類之資源使用率的更細微資訊： • **Total Disk Usage**（磁碟使用量總計）—叢集或設備的磁碟使用量總計。

© 2019 Palo Alto Networks, Inc.

受管理的 WildFire 資訊	說明

	• **Verdict**（裁定）—裁定的 **Total**（總計）數量，每種指派給檔案之裁定類型的數量—**Malware**（惡意軟體）、**Grayware**（灰色軟體）和 **Benign**（良性）；以及有多少裁定是 **Error**（錯誤）裁定。
	• **Sample Statistics**（樣本統計資料）—**Submitted**（已提交）和 **Analyzed**（已分析）的樣本總數，以及有多少樣本的分析 **Pending**（擱置中）。
	• 分析環境及系統使用狀況：
	  • **File Type Analyzed**（分析的檔案類型）所分析之檔案的類型—**Executable**（可執行檔）、**Non-Executable**（非可執行檔）或 **Links**（連結）。
	  • **Virtual Machine Usage**（虛擬機器使用量）—用於分析各種檔案類型的虛擬機器數量，以及有多少虛擬機器可供用來分析各種檔案類型。例如，針對可執行檔，VM 使用量可能是 6/10（使用了六個 VM，有十個 VM 可供使用）。
	  • **Files Analyzed**（分析的檔案）—所分析之各類型檔案的數量。

可執行檔頁籤、非可執行檔頁籤和連結頁籤	**Executable**（可執行檔）、**Non-Executable**（非可執行檔）和 **Links**（連結）會顯示類似的各類型檔案相關資訊：
	• **Verdict**（裁定）—依檔案類型分類之裁定的詳細資料。您可以篩選結果：
	  • 搜尋方塊—輸入搜尋字詞可篩選裁定。搜尋方塊會指出清單中的檔案類型（項目）數目。在您輸入搜尋字詞之後，套用篩選器（→）或清除篩選器（×），然後輸入一組不同的字詞。
	  • **File Type**（檔案類型）—依類型列出檔案。例如，**Executable**（可執行檔）頁籤會顯示 .exe 和 .dll 檔案類型；**Non-Executable**（非可執行檔）頁籤會顯示 .pdf、.jar、.doc、.ppt、.xls、.docx、.pptx、.xlsx、.rtf、class 和 .swf 檔案類型；**Links**（連結）頁籤則會顯示 elink 檔案類型資訊。
	  • 對於每種 **File Type**（檔案類型），上述各個頁籤都會顯示 **Malware**（惡意軟體）、**Grayware**（灰色軟體）和 **Benign**（良性）的裁定總數，**Error**（錯誤）裁定數目，以及 **Total**（總計）裁定數量。
	• 樣本統計資料—依檔案類型分類之樣本分析的詳細資料。
	  • 搜尋方塊—和裁定搜尋方塊相同。
	  • **File Type**（檔案類型）—和 **Verdict**（裁定）**File Type**（檔案類型）相同。
	  • 對於每種 **File Type**（檔案類型），各個頁籤都會顯示 **Submitted**（已提交）進行分析之檔案的總數，**Analyzed**（已分析）的總數，以及 **Pending**（擱置中）分析數量。

已連線的防火牆 > 檢視	
檢視	**View**（檢視）已連線到叢集或設備之防火牆的相關資訊。您只能檢視個別的設備（**Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備））或只能檢視叢集的統計資料（**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集））。 • **Appliance**（設備）—（僅限獨立設備檢視）設備序號。 • **Cluster**（叢集）—（僅限叢集檢視）叢集名稱，您也可以選取不同的叢集來進行檢視。 • **Refresh**（重新整理）—重新整理顯示。

© 2019 Palo Alto Networks, Inc.

受管理的 WildFire 資訊	說明
已註冊頁籤和正在提交樣本頁籤	**Registered**（已註冊）頁籤會顯示已註冊到叢集或設備之防火牆的相關資訊，無論防火牆是否正在提交樣本。 **Submitting Samples**（正在提交樣本）頁籤會顯示正在將樣本提交到 WildFire 叢集或設備之防火牆的相關資訊。 這兩個頁籤上所顯示的資訊類型以及其篩選資訊的方式都很類似： • 搜尋方塊—輸入搜尋字詞可篩選防火牆清單。搜尋方塊會指出清單中的防火牆（項目）數目。在您輸入搜尋字詞之後，套用篩選器 (→) 或清除篩選器 (×)，然後輸入一組不同的字詞。 • **S/N**（序號）—防火牆的序號。 • **IP Address**（**IP** 位址）—防火牆的 IP 位址。 • **Model**（型號）—防火牆的型號。 • **Software Version**（軟體版本）—防火牆上所安裝和執行的軟體版本。

受管理的 WildFire 叢集和裝置的管理

選取 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集），然後選取叢集來加以管理，或選取 WildFire 裝置（**Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 裝置））來管理獨立的裝置。**Panorama** > **Managed WildFire Cluster**（受管理的 **WildFire** 叢集）檢視會列出叢集節點（屬於叢集成員的 WildFire 裝置）和獨立裝置，讓您可以將可用裝置新增至叢集。叢集負責管理節點，因此選取叢集節點只會提供有限的管理功能。

除非另行說明，否則下表中的設定和說明會同時適用於 WildFire 叢集和 WildFire 獨立裝置。先前已在叢集或裝置上設定的資訊會預先填入。您首先必須認可變更與在 Panorama 上的其他資料，然後將新的組態推送至裝置上。

setting	說明
一般頁籤	
名稱	叢集或裝置 **Name**（名稱）或是裝置序號。
啟用 DNS （僅限 WildFire 叢集）	為叢集 **Enable DNS**（啟用 **DNS**）服務。
將防火牆註冊至	要將防火牆註冊到的網域名稱。格式必須為 **`wfpc.service.`***cluster-name*>**`.`**<*domain*>。例如，預設網域名稱是 **`wfpc.service.mycluster.paloaltonetworks.com`**。
內容更新伺服器	輸入 **Content Update Server**（內容更新伺服器）位置或使用預設的 **`wildfire.paloaltonetworks.com`**，讓叢集或裝置能夠從容傳遞網路基礎結構中最接近的伺服器收到內容更新。連線到全域雲端可讓您獲得好處，因為您可以根據威脅分析，從所有連線到雲端的來源存取特徵碼和更新，而不必只仰賴本機威脅的分析。
檢查伺服器識別	**Check Server Identity**（檢查伺服器識別）可確認更新伺服器的身分識別，它會比對憑證中的通用名稱 (CN) 與伺服器的 IP 位址或 FQDN。

© 2019 Palo Alto Networks, Inc.

setting	說明
WildFire 雲端伺服器	輸入全域 **WildFire Cloud Server**（**WildFire** 雲端伺服器）位置或使用預設的 `wildfire.paloaltonetworks.com`，讓叢集或裝置可以將資訊傳送至最接近的伺服器。您可以選取是否要傳送資訊，以及要將哪些類型的資訊傳送至全域雲端（**WildFire Cloud Services**（**WildFire** 雲端服務））。
範例分析影像	選取叢集或裝置，以用來分析樣本的 VM 影像（預設為 vm-5）。您可以取得惡意軟體測試檔案 (WildFireAPI)以查看樣本分析結果。
WildFire 雲端服務	如果叢集或裝置連線到全域 WildFire 雲端伺服器，您可以選取是否要對全域雲端 **Send Analysis Data**（傳送分析資料）、**Send Malicious Samples**（傳送惡意樣本）、**Send Diagnostics**（傳送診斷）至全域雲端或任何以上三項動作組合。您也可以選取是否在全域雲端執行 **Verdict Lookup**（裁定查閱）。將資訊傳送至全域雲端會讓整個 WildFire 使用者社群獲得好處，因為共用資訊會讓每個裝置更加能夠識別出惡意流量，並防止惡意流量周遊網路。
樣本資料保留	良性或灰色軟體樣本和惡意樣本的保留天數： • **Benign/Grayware**（良性/灰色軟體）樣本—範圍是 1 到 90；預設為 14。 • **Malicious**（惡意）樣本—最小值為 1，且沒有最大值（無限）；預設為無限。
分析環境服務	**Environment Networking**（環境網路）可讓虛擬機器與網際網路通訊。您可以選取 **Anonymous Networking**（匿名網路）來進行匿名通訊，但是您必須先選取 **Environment Networking**（環境網路）才能啟用 **Anonymous Networking**（匿名網路）。 不同的網路環境會產生不同類型的分析負載，一切取決於是需要分析更多文件，還是需要分析更多可執行檔。視環境需求而定，您可以將偏好的分析環境設定為對 **Executables**（可執行檔）或對 **Documents**（文件）配置更多資源。**Default**（預設值）配置會在 **Executables**（可執行檔）和 **Documents**（文件）之間取得平衡。 可用資源數量則取決於叢集中有多少 WildFire 節點。
特徵碼產生	選取您是否要讓叢集或裝置產生 AV、DNS、URL或任何以上三項結合的特徵碼。
裝置頁籤	
主機名稱 （僅限獨立的 WildFire 裝置）	輸入 WildFire 裝置的主機名稱。
Panorama 服务器	針對裝置或負責管理叢集的主要 Panorama 輸入其 IP 位址或 FQDN。
Panorama 伺服器 2	針對裝置或負責管理叢集的備份 Panorama 輸入其 IP 位址或 FQDN。
網域	輸入裝置叢集或裝置的網域名稱。
主要 DNS 伺服器	輸入主要 DNS 伺服器的 IP 位址。
次要 DNS 伺服器	輸入次要 DNS 伺服器的 IP 位址。
timezone	選取要用於叢集或裝置的時區。

© 2019 Palo Alto Networks, Inc.

setting	說明
緯度 （僅限獨立的 WildFire 裝置）	輸入 WildFire 裝置的緯度。
經度 （僅限獨立的 WildFire 裝置）	輸入 WildFire 裝置的經度。
主要 NTP 伺服器	輸入主要 NTP 伺服器的 IP 位址，並將驗證類型設定為 **None**（無）（預設）、**Symmetric Key**（對稱金鑰）或 **Autokey**。 將驗證類型設定為 **Symmetric Key**（對稱金鑰）會再顯示 4 個欄位： • **Key ID**（金鑰 **ID**）—輸入驗證金鑰 ID。 • **Algorithm**（演算法）—設定驗證演算法 **SHA1** 或 **MD5**。 • **Authentication Key**（驗證金鑰）—輸入驗證金鑰。 • **Confirm Authentication Key**（確認驗證金鑰）—再次輸入驗證金鑰來加以確認。
次要 NTP 伺服器	輸入次要 NTP 伺服器的 IP 位址，並將驗證類型設定為 **None**（無）、**Symmetric Key**（對稱金鑰）或 **Autokey**。 將驗證類型設定為 **Symmetric Key**（對稱金鑰）會再顯示 4 個欄位： • **Key ID**（金鑰 **ID**）—輸入驗證金鑰 ID。 • **Algorithm**（演算法）—設定驗證演算法 **SHA1** 或 **MD5**。 • **Authentication Key**（驗證金鑰）—輸入驗證金鑰。 • **Confirm Authentication Key**（確認驗證金鑰）—再次輸入驗證金鑰來加以確認。
登入橫幅	輸入會在使用者登入叢集或裝置時顯示的橫幅訊息。
日誌記錄頁籤（包括系統頁籤和組態頁籤）	
新增	**Add**（新增） 日誌轉送設定檔 （**Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集） > *<cluster>* > **Logging**（日誌記錄） > **System**（系統） 或 **Panorama** > **Managed WildFire Clusters**（受管理的 **WildFire** 叢集） > *<cluster>* > **Logging**（日誌記錄） > **Configuration**（組態））以轉送： • 系統或組態日誌，以 SNMP 設陷的形式轉送到 SNMP 設陷接收器。 • Syslog 訊息，轉送到 Syslog 伺服器。 • 電子郵件通知，轉送到電子郵件伺服器。 • HTTP 要求，轉送到 HTTP 伺服器。 其他日誌類型則不受支援（請參閱裝置 > 日誌設定）。 日誌轉送設定檔會指定要轉送哪些日誌，以及要轉送到哪些目的地伺服器。請針對每個設定檔完成下列設定： • **Name**（名稱）—此名稱可識別僅由英數字元和底線組成的日誌設定（最多 31 個字元）— 不允許空格和特殊字元。 • **Filter**（篩選器）—依預設，Panorama 裝置會轉送指定設定檔的 **All Logs**（所有日誌）。若要轉送一部分的日誌，請選取篩選器（**severity eq critical**、**severity**

© 2019 Palo Alto Networks, Inc.

setting	說明
	eq high、severity eq informational、severity eq low 或 severity eq medium），或是選取 Filter Builder（篩選器建立器）來建立新的篩選器。 • Description（說明）—輸入說明（最多 1,023 個字元）來說明設定檔的目的。

新增 > 篩選器 > 篩選器建立器	使用 Filter Builder（篩選器建立器）來建立新的日誌篩選器。選取 Create Filter（建立篩選器）來建構篩選器，並為新篩選器內的每個查詢指定下列設定，然後 Add（新增）查詢：
	• Connector（連接器）—選取連接器邏輯（and 或 or）。如果您要套用否定，請選取 Negate（否定）。例如，若要避免轉送一部分的日誌說明，請選取 Description（說明）來作為屬性，選取 contains 來作為運算子，然後輸入說明字串來作為值，以識別您不想轉送的說明。
	• Attribute（屬性）—選取日誌屬性。選項會依日誌類型而異。
	• Operator（運算子）—選取準則來決定屬性的套用方式（例如 contains）。選項會依日誌類型而異。
	• Value（值）—指定要比對的屬性值。
	• Add（新增）—新增篩選器。
	若要顯示或匯出篩選器比對的日誌，請選取 View Filtered Logs（檢視篩選的日誌）。
	• 若要尋找相符的日誌項目，您可新增構件至該欄位，例如 IP 位址或時間範圍。
	• 選取您想要觀看日誌的時段：前 15 分鐘、前1 小時、前 6 小時、前 12 小時、前 24 小時、前 7 天、前 30 天 或全部（預設）。
	• 使用時段下拉式清單右側的選項可套用、清除、新增、儲存及載入篩選器：
	  • Apply filters（套用篩選器）（→）—顯示符合搜尋欄位中字詞的日誌項目。
	  • Clear filters（清除篩選器）（×）—清除篩選器欄位。
	  • Add a new filter（新增新的篩選器）（⊕）—定義新的搜尋準則（您會進入 Add Log Filter（新增日誌篩選器），其功用與建立篩選器類似）。
	  • Save a filter（儲存篩選器）（）—輸入篩選器的名稱，然後按一下 OK（確定）。
	  • Use a saved filter（使用儲存的篩選器）（）—新增儲存的篩選器至篩選器欄位。
	  • Export to CSV（匯出為 CSV）（）—將日誌匯出為 CSV 格式的報告，然後 Download file（下載檔案）。依預設，報告包含多達 2,000 行日誌。若要變更產生之 CSV 報告的行限制，請選取 Device（裝置）> Setup（設定）> Management（管理）> Logging and Reporting Settings（日誌記錄與報告設定）> Log Export and Reporting（日誌匯出與報告），然後輸入新的 Max Rows in CSV Export（CSV 匯出中的最大列數）值。
	您可以變更每頁顯示的項目數目和順序，而且可以使用頁面左下角的頁面控制項來瀏覽日誌清單。會擷取 10 頁的日誌項目。
	• 每頁—使用下拉式清單來變更每頁的日誌項目數量（20、30、40、50、75 或 100）。
	• ASC 或 DESC—選取 ASC 可依遞增順序排序結果（最舊的日誌項目最先顯示），選取 DESC 則可依遞減順序排序（最新的日誌項目最先顯示）。預設為 DESC。
	• Resolve Hostname（解析主機名稱）—選取此選項可將外部 IP 位址解析為網域名稱。

© 2019 Palo Alto Networks, Inc.

setting	說明
	• **Highlight Policy Actions**（反白顯示原則動作）—指定動作並加以選取來反白顯示符合動作的日誌項目。所篩選出的日誌會以下列顏色反白顯示： • 綠色—允許 • 黃色—繼續，或取代 • 紅色—拒絕、丟棄、drop-icmp、rst-client、reset-server、reset-both、block-continue、block-override、block-url、drop-all、sinkhole
刪除	選取然後 **Delete**（刪除）您要從系統或組態日誌清單中移除的日誌轉送設定。
驗證頁籤	
驗證設定檔	選取已設定的驗證設定檔以定義驗證服務，該服務將驗證 WildFire 設備或 Panorama 管理員的登入憑證。
失敗的嘗試	輸入在鎖定管理員之前 WildFire 設備在 CLI 上允許的失敗登入嘗試次數（範圍是 0 至 10；預設值為 10）。限制登入嘗試有助於保護 WildFire 設備免受暴力密碼破解攻擊。0 值會指定不受限制的登入嘗試次數。 如果您將 *Failed Attempts*（失敗的嘗試）數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，則管理員將無限期被鎖定，直至另一位管理員手動解鎖該被鎖定的管理員為止。如果沒有建立其他管理員，您必須在 *Panorama* 上重新設定 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）設定，並將設定變更推送至 *WildFire* 設備。要確保管理員永不被鎖定，讓 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）都使用預設值 *(0)*。 將 *Failed Attempts*（失敗的嘗試）數量設定為 *5* 或以下，以便在輸入錯誤時允許合理的重試次數，同時防止惡意系統嘗試使用暴力密碼破解攻擊登入 *WildFire* 設備。
鎖定時間（分鐘）	輸入達到 **Failed Attempts**（失敗的嘗試）限值（範圍是 0 至 60；預設值為 5）後，WildFire 設備鎖定管理員，使其無法存取 CLI 的分鐘數。0 值表示會套用封鎖，直到另一個管理員手動解除鎖定帳戶。 如果您將 *Failed Attempts*（失敗的嘗試）數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，則管理員將無限期被鎖定，直至另一位管理員手動解鎖該被鎖定的管理員為止。如果沒有建立其他管理員，您必須在 *Panorama* 上重新設定 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）設定，並將設定變更推送至 *WildFire* 設備。要確保管理員永不被鎖定，讓 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）都使用預設值 *(0)*。 將 *Lockout Time*（鎖定時間）設定為至少 *30* 分鐘，以防止惡意行為者連續嘗試登入。
閒置逾時（分鐘）	輸入在管理員自動登出之前不包含任何 CLI 上的活動的最大分鐘數（範圍是 0 至 1,440；預設值為「無」）。值為 0 表示非使用狀態未觸發自動登出。

© 2019 Palo Alto Networks, Inc.

setting	說明
	將 *Idle Timeout*（閒置逾時）設定在 *10* 分鐘，以防止未經授權的使用者在管理員沒有關閉工作階段時存取 *WildFire* 設備。
最大工作階段計數	輸入管理員可以同時開啟的作用中工作階段數目，預設值為 0，這意味著 WildFire 設備可以有無限數量的同時作用中工作階段。
最大工作階段時間	輸入管理員在自動登出之前可登入的分鐘數。默認值為 0，這意味著即使空閒，管理員也可以無限期登入。
本機管理員	新增並設定 WildFire 設備的新管理員。這些專管 WildFire 設備的管理員可在此頁面進行管理（**Panorama** > **Managed WildFire Appliances**（受管理的 **WildFire** 設備）> **Authentication**（驗證））。
Panorama 管理員	在 Panorama 上匯入現有管理員。這些管理員在 Panorama 上建立，並匯入至 WildFire 設備。
叢集頁籤（僅限受管理的 WildFire 叢集）和介面頁籤（僅限受管理的 WildFire 裝置） 您必須將裝置新增至 Panorama 才能管理介面，將裝置新增至叢集才能管理節點介面。	
裝置 （僅限叢集頁籤）	選取叢集節點可存取該節點的裝置頁籤和介面頁籤。裝置頁籤節點資訊會預先填入，而且除了主機名稱外都無法設定。介面頁籤會列出節點介面。選取一種如下敘述中管理的介面： • 介面名稱管理 • 介面名稱分析環境網路 • 介面名稱 Ethernet2 • 介面名稱 Ethernet3
介面名稱管理	管理介面為 Ethernet0。設定或檢視管理介面設定： • **Speed and Duplex**（速度與雙工）—選取 **auto-negotiate**（自動交涉）（預設）、 **10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex** 或 **1Gbps-full-duplex**。 • **IP Address**（**IP** 位址）—輸入介面的 IP 位址。 • **Netmask**（網路遮罩）—輸入介面的網路遮罩。 • **Default Gateway**（預設閘道）—輸入預設閘道的 IP 位址。 • **MTU**—輸入以位元組為單位的 MTU（範圍是 576 到 1,500；預設為 1,500）。 • **Management Services**（管理服務）—啟動您要支援的管理服務。您可以支援 **Ping**、**SSH** 和 **SNMP** 服務。 如果您使用 Proxy 伺服器來連線到網際網路，請進行 Proxy 設定： • **Server**（伺服器）—Proxy 伺服器的 IP 位址。 • **Port**（連接埠）—Proxy 伺服器上所設定用來接聽 Panorama 裝置要求的連接埠號碼。 • **User**（使用者）—Proxy 伺服器上所設定用於驗證的使用者名稱。 • **Password**（密碼）和 **Confirm Password**（確認密碼）—Proxy 伺服器上所設定用於驗證的密碼。 • **Clustering Services**（叢集服務）（僅限叢集頁籤）—選取 HA 服務：

© 2019 Palo Alto Networks, Inc.

setting	說明
	• **HA**—如果叢集中有兩個控制器節點，您可以將管理介面設定為 HA 介面，讓這兩個控制器節點都能使用管理資訊。如果您所設定的叢集節點是主要控制器節點，請將它標記為 **HA** 介面。 或者，根據您使用 WildFire 裝置乙太網路介面的方式而定，您也可以將 Etherent2 或 Ethernet3 分別設定為主要和備份控制器節點上的 HA 和 HA 備份介面。例如，您可以使用 Ethernet 2 作為 HA 和 HA 備份介面。在主要和備份控制器節點上，HA 和 HA 備份介面必須是相同的介面（管理、Ethernet2 或 Ethernet3）。您無法使用 Ethernet1 作為 HA/HA 備份介面。 • **HA Backup**（**HA** 備份）—如果您所設定的叢集節點是備份控制器節點，請將它標記為 **HA Backup**（**HA** 備份） 介面。 指定介面上允許的 IP 位址： • **Search box**（搜尋方塊）—輸入搜尋字詞可篩選出允許的 IP 位址清單。搜尋方塊會指出清單中的 IP 位址（項目）數目，以讓您知道清單有多長。在您輸入搜尋字詞之後，套用篩選器 (→) 或清除篩選器 (×)，然後輸入一組不同的字詞。 • **Add**（新增）—新增一個允許的 IP 位址。 • **Delete**（刪除）—選取並 **Delete**（刪除）您要從管理介面存取中移除的 IP 位址。
介面名稱分析環境網路	為 WildFire 裝置叢集或獨立的 WildFire 裝置分析環境網路介面（Ethernet1，也稱為 VM 介面）進行設定： • **Speed and Duplex**（速度與雙工）—設定為 **auto-negotiate**（自動交涉）（預設）、 **10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex** 或 **1Gbps-full-duplex**。 • **IP Address**（**IP** 位址）—輸入介面的 IP 位址。 • **Netmask**（網路遮罩）—輸入介面的網路遮罩。 • **Default Gateway**（預設閘道）—輸入預設閘道的 IP 位址。 • **MTU**—輸入以位元組為單位的 MTU（範圍是 576 到 1,500；預設為 1,500）。 • **DNS Server**（**DNS** 伺服器）—輸入 DNS 伺服器的 IP 位址。 • **Link State**（連結狀態）—將介面連結狀態設定為 **Up**（正常）或 **Down**（失效）。 • 管理服務—如果您要讓介面支援偵測服務，請啟用 **Ping**。 指定介面上允許的 IP 位址： • **Search box**（搜尋方塊）—輸入搜尋字詞可篩選出允許的 IP 位址清單。搜尋方塊會指出清單中的 IP 位址（項目）數目，以讓您知道清單有多長。在您輸入搜尋字詞之後，套用篩選器 (→) 或清除篩選器 (×)，然後輸入一組不同的字詞。 • **Add**（新增）—新增一個允許的 IP 位址。 • **Delete**（刪除）—選取您要從管理介面存取中移除的 IP 位址，然後 **Delete**（刪除）。
介面名稱 Ethernet2 介面名稱 Ethernet3	您可以為 Ethernet2 和 Ethernet3 介面設定相同的參數： • **Speed and Duplex**（速度與雙工）—設定為 **auto-negotiate**（自動交涉）（預設）、 **10Mbps-half-duplex**、**10Mbps-full-duplex**、**100Mbps-half-duplex**、**100Mbps-full-duplex**、**1Gbps-half-duplex** 或 **1Gbps-full-duplex**。

© 2019 Palo Alto Networks, Inc.

setting	說明

	• **IP Address**（**IP** 位址）—輸入介面的 IP 位址。
	• **Netmask**（網路遮罩）—輸入介面的網路遮罩。
	• **Default Gateway**（預設閘道）—輸入預設閘道的 IP 位址。
	• **MTU**—輸入以位元組為單位的 MTU（範圍是 576 到 1,500；預設為 1,500）。
	• 管理服務—如果您要讓介面支援偵測服務，請啟用 **Ping**。
	• **Clustering Services**（叢集服務）—選取叢集服務：
	  • **HA**—如果叢集中有兩個控制器節點，您可以將 Ethernet2 或 Ethernet3 介面設定為 HA 介面，讓這兩個控制器節點都能使用管理資訊。如果您所設定的叢集節點是主要控制器節點，請將它標記為 **HA** 介面。
	  或者，根據您使用 WildFire 裝置乙太網路介面的方式而定，您也可以將管理介面 (Ethernet1) 分別設定為主要和備份控制器節點上的 HA 和 HA 備份介面。在主要和備份控制器節點上，HA 和 HA 備份介面必須是相同的介面（管理、Ethernet2 或 Ethernet3）。您無法使用 Ethernet1 作為 HA/HA 備份介面。
	  • **HA Backup**（**HA** 備份）—如果您所設定的叢集節點是備份控制器節點，請將它標記為 **HA Backup**（**HA** 備份）介面。
	  • **Cluster Management**（叢集管理）—將 Ethernet2 或 Ethernet3 介面設定為用於全叢集管理和通訊的介面。

Role （僅限叢集頁籤）	當叢集具有成員裝置時，裝置角色可以是控制器、控制器備份或背景工作。選取 **Controller**（控制器）或 **Backup Controller**（備份控制器）可變更用於叢集裝置中各個角色的 WildFire 裝置。變更控制器會在變更角色期間遺失資料。
瀏覽 （僅限叢集頁籤）	**Clustering**（叢集）頁籤會列出叢集中的 WildFire 裝置節點。**Browse**（瀏覽）可檢視和新增 Panorama 裝置已管理的獨立 WildFire 裝置： • **Search box**（搜尋方塊）—輸入搜尋字詞可篩選出節點清單。搜尋方塊會指出清單中的裝置（項目）數目，以讓您知道清單有多長。在您輸入搜尋字詞之後，套用篩選器 (→) 或清除篩選器 (×)，然後輸入一組不同的字詞。 • **Add Nodes**（新增節點）—新增 (⊕) 節點至叢集。 新增至叢集的第一個 WildFire 裝置會自動成為控制器節點。所新增的第二個 WildFire 裝置會自動成為控制器備份節點。 您最多可以對叢集新增 20 個 WildFire 裝置。在新增控制器和控制器備份節點後，後續新增的所有節點都是背景工作節點。
刪除 （僅限叢集頁籤）	從裝置清單選取一或多個裝置，然後從叢集中加以 **Delete**（刪除）。只有在叢集中有兩個控制器節點時，您才能移除某個控制器節點。
管理控制站 （僅限叢集頁籤）	選取 **Manage Controller**（管理控制器）可從屬於叢集的 WildFire 裝置節點中指定 **Controller**（控制器）和 **Controller Backup**（控制器備份）。系統預設會選取目前的控制器節點和備份控制器節點。備份控制器節點不能和主要控制器節點相同。
通訊頁籤	
自訂安全伺服器通訊	• **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）—從下拉式清單選取 SSL/TLS 服務設定檔。此設定檔會定義連線的裝置可用來與 WildFire 通訊的憑證和支援的 SSL/TLS 版本。

© 2019 Palo Alto Networks, Inc.

setting	說明

	• **Certificate Profile**（憑證設定檔）—從下拉式清單中選取憑證設定檔。此憑證設定檔會定義憑證撤銷檢查行為，以及用來驗證用戶端所顯示之憑證鏈結的根 CA。
	• **Custom Certificate Only**（僅限自訂憑證）—當啟用時，WildFire 僅接受自訂憑證使用連線的裝置進行驗證。
	• **Check Authorization List**（檢查驗證清單）—會針對授權清單檢查連線至 WildFire 的用戶端裝置。裝置僅需要符合要授權之清單上的一個項目。如果找不到符合項目，就不會授權裝置。
	• **Authorization List**（驗證清單）—**Add**（新增）並完成下列欄位，以設定驗證用戶端裝置的條件。驗證清單支援最多 16 個項目。
	  • **Identifier**（識別碼）—選取 **Subject**（主體） 或 **Subject Alt.**（主體別名）。作為驗證識別碼的名稱 。
	  • 類型—如果為 **Subject Alt**（主體別名）。若名稱 作為識別碼，則選取 **IP**、**hostname**（主機名稱） 或 **e-mail**（電子郵件） 作為識別碼類型。如果您選取 **Subject**（主體），則通用名稱為識別碼類型。
	  • **Value**（值）—輸入識別碼值。

安全用戶端通訊	使用 **Secure Client Communication**（安全用戶端通訊）可確保防火牆使用設定的自訂憑證（而非預設的預定義憑證）來驗證 SSL 與另一個 WildFire 裝置的連線。
	• 預定義—（預設）沒有設定裝置憑證—WildFire 使用預設的預定義憑證。
	• **Local**（本機）—防火牆會使用本機裝置憑證，以及防火牆上所產生或從現有企業 PKI 伺服器匯入的對應私密金鑰。
	  • **Certificate**（憑證）：選取本機裝置憑證。
	  • **Certificate Profile**（憑證設定檔）：從下拉式清單選取憑證設定檔。
	• **SCEP**—WildFire 會使用簡易憑證註冊通訊協定 (SCEP) 伺服器所產生的裝置憑證和私密金鑰。
	  • **SCEP Profile**（**SCEP** 設定檔）：從下拉式清單選取 SCEP 設定檔。
	  • **Certificate Profile**（憑證設定檔）：從下拉式清單選取憑證設定檔。

安全叢集通訊	選取 **Enable**（啟用）以加密 WildFire 裝置間的通訊。預設的憑證使用預定義的憑證類型。若要使用使用者定義的自訂憑證，您必須設定 **Customize Secure Server Communication**（自訂安全伺服器通訊）並啟用 **Custom Certificate Only**（僅客戶憑證）。

© 2019 Palo Alto Networks, Inc.

Panorama > 管理員

選取 **Panorama** > **Administrators**（管理員）以建立和管理 Panorama 管理員的帳戶。

如果您以具有超級使用者角色的管理員身分登入 Panorama，按一下 Locked User（鎖定的使用者）欄中的鎖定圖示，即可將其他管理員的帳戶解除鎖定。遭到鎖定的管理員無法存取 Panorama。Panorama 會鎖定超出允許的連續嘗試存取 Panorama 失敗次數（如指派給帳戶的 **Authentication Profile**（驗證設定檔）中所定義）的管理員（請參閱 [設備 > 驗證設定檔]）。

若要建立管理員帳戶，請按一下 **Add**（新增）並如下表所述進行設定。

管理員帳戶設定	說明
名稱	輸入管理員的登入使用者名稱（最多 15 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、連字號和底線。
驗證設定檔	選取驗證設定檔或順序以驗證此管理員。如需詳細資訊，請參閱 [設備 > 驗證設定檔] 或 [設備 > 驗證順序]）。
僅使用用戶端憑證驗證 (Web)	選取以使用用戶端憑證驗證存取 Web 介面。如果您選取此選項，則不需要使用者名稱（**Name**（名稱））與 **Password**（密碼）。
密碼/確認密碼	輸入及確認管理員的區分大小寫密碼（最多 15 個字元）。若要確保安全性， Palo Alto Networks 建議管理員定期更改密碼，並使用大小寫字母與數字組合的形式。務必採用密碼強度最佳做法 以確保嚴格的密碼。 設備群組及範本管理員無法存取 **Panorama** > **Administrators**（管理員）。若要變更本機密碼，管理員可按一下其使用者名稱（在 Web 介面底部的 **Logout**（登出）旁邊）。這也適用於具有自訂 Panorama 角色的管理員，其 **Panorama** > **Administrators**（管理員）的存取權已停用。 您可以將密碼驗證與 **Authentication Profile**（驗證設定檔）（或順序），或本機資料庫搭配使用。 選取 **Password Profile**（密碼設定檔）（請參閱 [設備 > 密碼設定檔]）並設定最低密碼複雜度參數（請參閱 [設備 > 設定 > 管理]），可以設定密碼到期參數，但僅限於 Panorama 在本機驗證的管理帳戶。
使用公開金鑰驗證 (SSH)	選取以使用 SSH 公開金鑰驗證：按一下 **Import Key**（匯入金鑰）、**Browse**（瀏覽）以選取公開金鑰檔案，並且按一下 **OK**（確定）。[管理員] 對話方塊會在唯讀文字區域中顯示已上載的金鑰。 支援的金鑰檔案格式是 IETF SECSH 與 OpenSSH。支援的金鑰演算法是 DSA（1,024 位元）和 RSA（768 至 4,096 位元）。 如果公開金鑰失敗，*Panorama* 會顯示登入與密碼的提示。
管理員類型	選取的類型會決定管理員角色選項： • **Dynamic**（動態）—此角色可提供 Panorama 和受管理防火牆的存取權。當新增新功能時，Panorama 會自動更新動態角色的定義，您永遠不用手動更新這些定義。

© 2019 Palo Alto Networks, Inc.

管理員帳戶設定	說明
	• **Custom Panorama Admin**（自訂 **Panorama** 管理員）—具有 Panorama 功能讀取/寫入存取權、唯讀存取權或無存取權的可設定角色。 • **Device Group and Template Admin**（設備群組與範本管理員）—具有設備群組與範本功能讀取/寫入存取權、唯讀存取權或無存取權的可設定角色，存取範圍是指派給您為此管理員選取之存取網域的設備群組與範本功能。

管理員角色
（動態管理員類型）
	選取預先定義的角色：
	• **Superuser**（超級使用者）—可完整讀取/寫入存取 Panorama 及所有設備群組、範本和受管理防火牆。
	• **Superuser (Read Only)**（超級使用者（唯讀））—可唯讀存取 Panorama 及所有設備群組、範本和受管理防火牆。
	• **Panorama administrator**（**Panorama** 管理員）—Panorama 的完整存取權，但不包括下列動作：
	  • 建立、修改或刪除 Panorama 或防火牆管理員及角色。
	  • 匯出、驗證、還原、儲存、載入或匯入設定（**Device**（裝置）> **Setup**（設定）> **Operations**（操作））。
	  • 在 **Panorama** 頁籤中設定 **Scheduled Config Export**（已排程的設定匯出）。

Profile （自訂 Panorama 管理員管理員類型）	選取自訂 Panorama 角色（請參閱 [Panorama > 託管設備>摘要]）。
管理員角色的存取網域 （設備群組與範本管理員管理員類型）	針對每個您想要指派給管理員的存取網域（最多 25 個），**New**（新增）下拉式清單中的 **Access Domain**（存取網域）（請參閱 [Panorama > 存取網域]），然後按一下相鄰的 [管理員角色] 儲存格，並從下拉式清單中選取自訂設備群組與範本管理員角色（請參閱 [Panorama > 託管設備>摘要]）。可存取多個網域的管理員登入 Panorama 時，**Access Domain**（存取網域）下拉式清單會顯示在 Web 介面的頁尾中。管理員可以選取任何已指派的存取網域以過濾 Panorama 顯示的監視和設定資料。**Access Domain**（存取網域）選項也會篩選 **Context**（內容）下拉式清單顯示的防火牆。 如果您使用 *RADIUS* 伺服器驗證管理員，則必須將管理員角色和存取網域對應至 RADIUS VSA。由於 *VSA* 字串支援有限的字元數，如果您針對管理員設定存取網域/角色配對上限（*25* 個），則每個存取網域和每個角色的 *[名稱]* 值不得超過平均 *9* 個字元。
密碼設定檔	選取 **Password Profile**（密碼設定檔）（請參閱 [設備 > 密碼設定檔]）。

© 2019 Palo Alto Networks, Inc.

Panorama > Admin Roles（Panorama > 管理員角色）

管理員角色設定檔是可定義存取權限與管理員職責的自訂角色。例如，指派給管理員的角色可控制他可以產生哪些報告，以及管理員可以檢視或變更的裝置群組或範本組態。

對於裝置群組和範本管理員，您可以將個別的角色指派給已指派給管理帳戶的每個存取網域（請參閱 [Panorama > 存取網域]）。將角色對應至存取網域，可讓您對管理員可以在 Panorama 上存取的資訊進行非常細微的控制。例如，請考慮以下案例：您設定的存取網域包含您的資料中心防火牆的所有裝置群組，而您將該存取網域指派給能夠監控資料中心流量但不能設定防火牆的管理員。在此情況下，您會將存取網域對應至某個角色，該角色已啟用所有監控權限，但會停用裝置群組設定的存取權。

若要建立管理員角色設定檔，請 **Add**（新增）設定檔並如下表所述進行設定。

如果您使用 *RADIUS* 伺服器驗證管理員，請將管理員角色和存取網域對應至 RADIUS 廠商特定屬性 (VSA)。

Panorama 管理員角色設定	說明
名稱	輸入用來識別管理員角色的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。
說明	（選用）輸入角色的說明。
Role	選取管理責任的範圍：**Panorama** 或 **Device Group and Template**（裝置群組與範本）。
網頁使用者介面	從下列選項中選取，為 Panorama 內容（**Web UI list**（網頁使用者介面清單））及防火牆內容（**Context Switch UI list**（內容切換使用者介面清單））中的特定功能設定允許的存取類型： • 啟用（✓）—讀取及寫入存取權限 • 唯讀（🔒）— 唯讀存取權限 • 停用（⊗）—無存取權限
XML API （僅限 Panorama 角色）	為 Panorama 及受管理防火牆選取 XML API 存取類型（**Enable**（啟用）或 **Disable**（停用））： • 報告—存取 Panorama 及防火牆報告。 • 日誌—存取 Panorama 及防火牆日誌。 • 組態—擷取或修改 Panorama 及防火牆組態的權限。 • 操作要求—在 Panorama 及防火牆上執行操作命令的權限。 • 認可—認可 Panorama 及防火牆組態的權限。 • **User-ID** 代理程式—User-ID 代理程式存取權限。 • 匯出—從 Panorama 及防火牆匯出檔案的權限（例如組態、封鎖或回應頁面、憑證及金鑰）。 • 匯入—將檔案匯入 Panorama 及防火牆的權限（例如軟體更新、內容更新、授權、組態、憑證、封鎖頁面及自訂日誌）。
命令列	為 CLI 存取選取角色類型：

© 2019 Palo Alto Networks, Inc.

Panorama 管理員角色設定	說明

（僅限 Panorama 角色）	• **None**（無）—（預設值）不允許存取 Panorama CLI。
	• **superuser**（超級使用者）—完整存取 **Panorama**。
	• **superreader**（超級讀取者）—唯讀存取 **Panorama**。
	• **panorama-admin**（**Panorama** 管理員）—完整存取 **Panorama**，但不包括下列動作：
	  • 建立、修改或刪除 Panorama 管理員及角色。
	  • 匯出、驗證、還原、儲存、載入或匯入組態。
	  • 排程組態匯出。

REST API （僅限 Panorama 角色）	為 Panorama 及受管理防火牆選取套用於每個 REST API 端點的存取類型（**Enable**（啟用）、**Read Only**（唯讀）或 **Disable**（停用））：您可以將角色存取權限指派給以下類別的端點。 • 物件 • 政策 • 網路 • 裝置

© 2019 Palo Alto Networks, Inc.

Panorama > Access Domains（Panorama > 存取網域）

Access domains（存取網域）控制裝置群組及範本管理員對特定裝置群組（以管理政策及物件）、物件（以管理網路及裝置設定）、受管理防火牆的網頁介面（透過內容切換）以及受管理防火牆的 REST API 的存取權限。您可以定義最多 4,000 個存取網域，並在本機使用 RADIUS 廠商特定屬性 (VSA)、TACACS+ VSAs 或 SAML 屬性管理這些網域。若要建立存取網域，請 **Add**（新增）網域並如下表所述進行設定。

存取網域設定	說明
名稱	輸入存取網域的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、連字號和底線。
共用物件	針對此存取網域中的裝置群組從共用位置繼承的物件，選取下列其中一個存取權限。無論權限為何，管理員都無法取代共用或預設（預先定義）物件。 • 讀取—管理員可以顯示和複製共用物件，但無法針對這些物件執行任何其他操作。新增非共用物件或複製共用物件時，目的地必須是存取網域中的裝置群組，而非「共用」。 • 寫入—管理員可以針對共用物件執行所有操作。這是預設值。 • 僅限共用—管理員只可將物件新增至 [共用]。管理員也可以顯示、編輯和刪除共用物件，但無法移動或複製這些物件。此選項的結果是除了顯示非共用物件以外，該管理員無法針對這些物件執行任何操作。
裝置群組	啟用或停用存取網域中特定裝置群組的讀寫權限。您也可以按一下全部啟用或全部停用。針對裝置群組啟用讀取/寫入存取權會自動針對其子系啟用相同的存取權。如果您手動停用子系，其最高上階的存取權會自動變更為唯讀。依預設，將針對所有裝置群組停用存取權。 若要讓清單僅顯示特定裝置群組，請選取裝置名稱和 **Filter Selected**（已選取篩選器）。 如果您將共用物件的存取權設定為 *shared-only*（僅限共用），*Panorama* 會將唯讀存取權套用至任何您指定讀取/寫入存取權的裝置群組。
範本	針對每個您要指派的範本或範本堆疊，按一下新增，並從下拉式清單中選取該範本或範本堆疊。
裝置內容 （對應 [存取網域] 頁面中的 [裝置/虛擬系統] 欄）	選取管理員可以切換內容的防火牆，以執行本機組態。如果清單較長，您可以透過 **Device State**（裝置狀態）、**Platforms**（平台）、**Device Groups**（裝置群組）、**Templates**（範本）、**Tags**（頁籤）和 **HA Status**（**HA** 狀態）進行篩選。
日誌收集器群組	針對每個您要指派的收集器群組，**Add**（新增）並從下拉式清單中選取。

© 2019 Palo Alto Networks, Inc.

Panorama > Managed Devices > Summary（Panorama > 受管理的裝置 > 摘要）

Panorama 管理的 Palo Alto Networks 防火牆稱為受管理的設備。Panorama 可以管理執行相同主版本或較早受支援版本的防火牆，但 Panorama 無法管理執行更新主版本的防火牆。例如，執行 PAN-OS 10.0 的 Panorama 可以管理執行 PAN-OS 10.0 及更早版本的防火牆。另外，不建議管理執行維護版本比 Panorama 晚的防火牆，因為這可能導致功能未按預期工作。例如，如果 Panorama 執行的是 PAN-OS 10.0.0，則不建議管理執行 PAN-OS 10.0.1 或更高維護版本的防火牆。如需更多版本資訊，請參閱 PAN-OS 10.0 版本資訊。如需受支援 PAN-OS 版本的更多資訊，請參閱生命週期結束摘要。

- 受管理防火牆的管理
- 受管理防火牆資訊
- 防火牆軟體和內容更新
- 防火牆備份

受管理防火牆的管理

您可以在防火牆上執行下列管理任務：

工作	說明
新增	**Add**（新增）防火牆並輸入其序號（每列一個）可將其新增為受管理的裝置。**Managed Devices**（受管理的裝置）視窗隨後會顯示受管理防火牆的資訊，包括連線狀態、已安裝的更新，以及在初始組態期間設定的屬性。 檢查 **Associate Devices**（相關裝置）方塊，以將防火牆以及裝置群組或範本堆疊相關聯。 以 CSV 格式 **Import**（匯入）數個防火牆，以 Panorama 管理伺服器進行管理。範例 CSV 檔案可供下載。 接下來，輸入每個防火牆上的 Panorama 管理伺服器 IP 位址（請參閱 [裝置 > 設定 > 管理]），讓 Panorama 可以管理防火牆。 防火牆透過具有 *AES-256* 加密的 *SSL* 連線在 *Panorama* 上註冊。*Panorama* 與防火牆運用 *2,048* 位憑證及用於組態管理及登入收集的 *SSL* 連接來彼此驗證。
重新關聯	將一個或多個選定的防火牆重新指派給其他裝置群組或範本堆疊。
刪除	選取一個或多個防火牆，然後從 Panorama 管理的防火牆清單中 **Delete**（刪除）。
頁籤	選取一或多個防火牆的核取方塊，按一下 **Tag**（頁籤），並輸入最多 31 個字元的文字字串或選取現有頁籤。請勿使用空格。當 Web 介面顯示較長防火牆清單時（例如，在安裝軟體的對話方塊中），頁籤可提供篩選清單的方法。例如，您可使用名為分公司的頁籤，來跨網路篩選所有分公司防火牆。
安裝	**Install**（安裝）防火牆軟體以及內容更新。
群組 HA 端點	若要讓 **Managed Devices**（受管理的裝置）頁面針對在高可用性 (HA) 組態中作為端點的防火牆進行分組，請選取 **Group HA Peers**（群組 **HA** 端點）。然後您可僅選取在兩個端點或不在每個 HA 配對的任何端點上執行動作。

© 2019 Palo Alto Networks, Inc.

工作	說明
管理（備份）	**Manage**（管理）防火牆備份。
PDF/CSV	具有最小唯讀訪問權限的管理角色可以匯出如 **PDF/CSV** 的託管防火牆表。您可以在稽核等情況下套用篩選以建立更多特定表格組態匯出。僅可匯出網路介面中可見的欄位。請參閱 Configuration Table Export（組態表匯出）。
部署主要金鑰	為一個或數個裝置部屬一個主要金鑰或更新現有金鑰。

受管理防火牆資訊

選取 **Panorama** > **Managed Devices**（託管裝置） > **Summary**（摘要）可針對每個受管理防火牆顯示下列資訊。

受管理防火牆資訊	說明
裝置群組	顯示防火牆為其中成員的裝置群組名稱。依預設，將隱藏此欄，雖然您可以透過選取任何欄標頭中的下拉式清單，並選取 **Columns**（欄） > **Device Group**（裝置群組） 以顯示該欄。 此頁面根據防火牆裝置群組顯示在叢集中的防火牆。每個叢集都具有標頭列，該列會顯示階層中的裝置群組名稱、已指派防火牆總數、已連線防火牆數和裝置群組路徑。例如，資料中心（**2** 個裝置已連線，共 **4** 個）：**Shared**（共用） > **Europe**（歐洲） > **Data center**（資料中心） 會表示名為 **Data center**（資料中心） 的裝置群組具有四個成員防火牆（其中兩個已連線），且是名為 **Europe**（歐洲） 之裝置群組的子項。您可以摺疊或展開任何裝置群組以隱藏或顯示其防火牆。
裝置名稱	顯示防火牆的主機名稱或序號。 對於 VM 系統 NSX 版防火牆，防火牆名稱將附加至 ESXi 主機的主機名稱。例如，PA-VM：Host-NY5105
虛擬系統	列出處於多個虛擬系統模式的防火牆可用的虛擬系統。
Model	顯示本防火牆型號。
標籤	顯示為每個防火牆/虛擬系統定義的頁籤。
序號	顯示防火牆的序號。
操作模式	顯示防火牆的操作模式。可以是 FIPS-CC 或一般
IP 位址	顯示防火牆/虛擬系統的 IP 位址。
	IPv4—防火牆/虛擬系統的 IPv4 位址。
	IPv6—防火牆/虛擬系統的 IPv6 位址。
變數	透過從範本堆疊中的裝置複製裝置特定變數定義以建立它們，或編輯現有變數定義以建立此裝置唯一的變數。如果裝置與範本堆疊不相關，則此欄

© 2019 Palo Alto Networks, Inc.

受管理防火牆資訊	說明
	位將為空白。預設變數定義皆從範本堆疊繼承而來。參閱 Create or Edit Variable Definition on a Device（在裝置上建立或編輯變數定義）。
範本	顯示指派防火牆的範本堆疊。
STATUS (狀態)	裝置狀態—表示 Panorama 與防火牆之間的連線狀態。已連線或已中斷連線。 VM-Series 防火牆可以具有其他兩個狀態： • 已停用 —表示您已直接在防火牆上或透過選取 **Deactivate VMs**（停用 **VM**）（**Panorama** > **Device Deployment**（裝置部署）> **Licenses**（授權））來停用虛擬電腦，並移除防火牆上所有的授權及權利。由於停用程序會移除 VM 系列防火牆上的序號，因此已停用防火牆不再連線至 Panorama。 • 部分停用 — 表示您已從 Panorama 啟動授權停用程序，但由於防火牆已離線且 Panorama 無法與其通訊，因此尚未完整完成該程序。
	HA 狀態 — 表示防火牆的下列狀態： • 主動 — 正常流量處理操作狀態 • 被動 — 正常備份狀態 • 啟動中—啟動後，防火牆處於此狀態會持續最多 60 秒 • 非作用中 — 錯誤狀態 • 已暫停 — 管理員已停用防火牆 • 暫訂 — 對於主動/主動組態中的連結或路徑監控
	共用原則 — 表示防火牆上的原則和物件組態是否與 Panorama 同步。
	範本 — 表示防火牆上的網路和裝置組態是否與 Panorama 同步。
狀態（續）	憑證—表示受管理的裝置的用戶端憑證狀態。 • 已預先定義—受管理的裝置會使用預先定義的憑證來驗證 Panorama。 • 已部署—自訂憑證已成功地部署在受管理的裝置上。 • 將在 **N** 天 **N** 小時後到期—目前所安裝的憑證將在不到 30 天後到期。 • 將在 **N** 分鐘後到期—目前所安裝的憑證將在不到 1 天後到期。 • 已通過用戶端識別檢查—憑證的通用名稱符合連線裝置的序號。 • **OCSP** 狀態不明—Panorama 無法從 OCSP 回應程式取得 OCSP 狀態。 • 無法使用 **OCSP** 狀態—Panorama 無法聯絡 OCSP 回應程式。 • **CRL** 狀態不明—Panorama 無法從 CRL 資料庫取得撤銷狀態。 • 無法使用 **CRL** 狀態—Panorama 無法聯絡 CRL 資料庫。
	• **OCSP/CRL** 狀態不明—Panorama 無法取得 OCSP 或撤銷狀態（當兩者同時啟用時）。 • 無法使用 **OCSP/CRL** 狀態—Panorama 無法聯絡 OCSP 或 CRL 資料庫（當兩者同時啟用時）。 • 不受信任的簽發者—受管理的裝置有自訂憑證，但伺服器無法驗證該憑證。 上次提交狀態 — 表示防火牆的上次提交是成功還是失敗。

© 2019 Palo Alto Networks, Inc.

受管理防火牆資訊	說明
軟體版本 | 應用程式與威脅 | 防毒 | URL 篩選 | GlobalProtect™ 用戶端 | WildFire	顯示目前在防火牆上安裝的軟體和內容版本。如需詳細資訊，請參閱防火牆軟體和內容更新。
備份	防火牆每次提交時，PAN-OS 將自動傳送防火牆組態至 Panorama。按一下 **Manage**（管理）可檢視可用組態備份，或選取載入一個。如需詳細資訊，請參閱防火牆備份。
上次主要金鑰推送	顯示從 Panorama 至防火牆的主要金鑰的狀態。
	狀態—顯示最新的主要金鑰推送狀態。可以是 `Success`（成功）或 `Failed`（失敗）。如果主要金鑰尚未從 Panorama 推送至防火牆，則會顯示 `Unknown`（未知）。
	Timestamp（時間戳記）—顯示從 Panorama 推送的最近一次主要金鑰的日期以及時間。
容器—如果您部署了 CN 系列防火牆來保護 Kubernetes 叢集上的容器化應用程式工作負載，請使用以下欄。	
容器節點數量	顯示已連線至註冊到 Panorama 的管理平面 (CN-Mgmt) 的容器化防火牆資料平面 (CN-NGFW) 的數量。 針對每對 CN-Mgmt pod，該值可以是 0 至 30 個 CN-NGFW pod。
容器附註	未來使用

建立裝置變數定義

當裝置第一次新增至範本堆疊時，您有建立裝置特定變數定義的選項，該定義乃從範本堆疊中的裝置複製，或者您可以透過 **Panorama** > **Managed Devices**（託管的裝置）> **Summary**（摘要）來編輯範本變數定義。所有變數定義預設為自範本堆疊繼承，且僅可以取代—而無法刪除—該個別裝置的變數定義。您可以在 IKE 閘道設定（介面）和 HA 設定（群組 ID）中所有組態、介面區域裡，使用變數取代 IP 位址物件和 IP 位址常值（IP 網路遮罩、IP 範圍、FQDN）。

建立裝置變數定義資料	說明
是否從其他範本堆疊克隆裝置變數定義？	
否	檢視現有變數定義並在必要時編輯。See Panorama > 範本 > 範本變數。
是	選取一個在下拉式清單中的裝置，從該裝置複製變數定義，然後選取您想要複製的特定變數定義。

防火牆軟體和內容更新

若要在受管理防火牆上安裝軟體或內容更新，請先使用 **Panorama** > **Device Deployment**（設備部署）頁面來下載或上載 Panorama 更新。接著，請選取 **Panorama** > **Managed Devices**（受管理的設備）頁面，按一下 **Install**（安裝），然後完成下列欄位。

© 2019 Palo Alto Networks, Inc.

若要減少管理 *(MGT)* 介面上的流量，您可以將 *Panorama* 設定為使用不同介面來部署更新（請參閱 Panorama > 設定 > 介面*)*。

防火牆軟體/內容更新安裝選項	說明
類型	選取您要安裝的更新類型：PAN-OS **Software**（軟體）、**GlobalProtect Client**（GlobalProtect 用戶端）軟體、**Apps and Threats**（應用程式與威脅）特徵碼、**Antivirus**（防毒）特徵碼、**WildFire** 或 **URL Filtering**（URL 篩選）。
檔案	選取更新影像。下拉式清單中只會包含您使用 **Panorama** > **Device Deployment**（設備部署）頁面所下載或上載至 Panorama 的映像檔。
篩選器	選取篩選器可篩選設備清單。
裝置	選取您要安裝影像的防火牆。
裝置名稱	防火牆名稱
目前版本	目前安裝於防火牆上的選取 **Type**（類型）的更新版本。
HA 狀態	表示防火牆的下列狀態： • 主動 — 正常流量處理操作狀態 • 被動 — 正常備份狀態 • 啟動中—啟動後，防火牆處於此狀態會持續最多 60 秒 • 非作用中 — 錯誤狀態 • 已暫停 — 管理員已停用防火牆 • 暫訂 — 對於主動/主動組態中的連結或路徑監控
群組 HA 端點	選取以針對在高可用性 (HA) 組態中作為端點的防火牆進行分組。
已選取篩選器	若要讓設備清單僅顯示特定防火牆，請選取對應的設備名稱，並選取 **Filter Selected**（已選取篩選器）。
僅上載至設備	選取此選項可將映像檔上載到防火牆，但不會自動將防火牆重新啟動。在您手動啟動防火牆時安裝該影像。
安裝後重新啟動設備（僅限軟體）	選取此選項可上載並安裝軟體映像。安裝程序會觸發重新啟動。
在內容更新中停用新應用程式（僅限應用程式與威脅）	選取以在更新（相對於上次安裝的更新為新更新）中停用應用程式。這可針對最新威脅，同時讓您在準備好任何原則更新之後靈活啟用應用程式。接著，若要啟用應用程式，請登入防火牆，選取 **Device**（裝置）> **Dynamic Updates**（動態更新），在功能欄中按一下 **Apps**（應用程式）以顯示新應用程式，然後對每個您想要啟用的應用程式按一下 **Enable/Disable**（啟用/停用）。

防火牆備份

- Panorama > Managed Devices（Panorama > 受管理的設備）

© 2019 Palo Alto Networks, Inc.

Panorama 會自動備份您認可至受管理防火牆的每個設定變更。若要為防火牆管理備份，選取 **Panorama** > **Managed Devices**（受管理的設備），按一下防火牆備份欄中的 **Manage**（管理），然後執行任何下列工作。

若要設定在 *Panorama* 上儲存的防火牆設定備份數，請選取 *Panorama* > *Setup*（設定）> *Management*（管理），編輯 *[日誌記錄與報告設定]*，選取 *Log Export and Reporting*（日誌匯出與報告），並輸入 *Number of Versions for Config Backups*（設定備份的版本數目）（預設為 *100*）。

工作	說明
顯示已儲存或已提交組態的詳細資訊。	在備份的版本欄中，按一下儲存的組態檔案名稱或提交的組態版本號，可顯示相關 XML 檔案的內容。
將已儲存或已提交的組態還原至候選組態。	在備份的動作欄中，按一下 **Load**（載入）與 **Commit**（認可）。 載入防火牆組態將還原本機裝置組態，而不還原從 Panorama 推送的組態。在您 **Load**（載入）防火牆備份之後，必須內容切換至防火牆網頁介面或啟動防火牆網頁介面以進行 **Commit**（提交）。
移除儲存的組態。	在已儲存備份的動作欄中，按一下刪除（✕）。

Panorama > Device Quarantine（Panorama > 裝置隔離）

Panorama > **Device Quarantine**（裝置隔離）頁面顯示隔離清單中的裝置。執行以下動作，裝置即會出現在此清單中：

- 系統管理員已將裝置手動新增至此清單。

  若要手動 **Add**（新增）裝置，請輸入您需要隔離裝置的 **Host ID**（主機 **ID**），也可選擇輸入 **Serial Number**（序號）。
- 系統管理員從「流量」、GlobalProtect 或「威脅」日誌中選取「主機 ID」欄，從該欄中選取一個裝置，然後選取 **Block Device**（封鎖裝置）。
- 該裝置與具有日誌轉送設定檔的安全性政策規則相符，其相符清單具有設定為 **Quarantine**（隔離）的內建動作。

  主機 *ID* 會自動顯示在 *GlobalProtect* 日誌中。為了使「主機 *ID*」顯示在「流量」、「威脅」或「統一」日誌中，*Panorama* 設備必須至少具有一個安全性政策規則，且其 *Source Device*（來源裝置）設定為 *Quarantine*（隔離）。如果在安全性政策中沒有此設定，則「流量」、「威脅」或「統一」日誌將沒有「主機 *ID*」，並且日誌轉送設定檔也不會生效。
- 使用 API 將裝置新增至隔離清單中。
- Panorama 設備收到的隔離清單是重新散佈項目的一部分（隔離清單從另一個 Panorama 設備或防火牆重新散佈）。

裝置隔離表包含以下欄位。

欄位	說明
主機 ID	封鎖主機的主機 ID。
原因	裝置被隔離的原因。**Admin Add**（管理員新增）的原因意味著管理員將裝置手動新增至表中。

© 2019 Palo Alto Networks, Inc.

欄位	說明
時間戳記	管理員或安全性政策規則將裝置新增至隔離清單的時間。
來源裝置/應用程式	將裝置新增至隔離清單的 Panorama、防火牆或第三方應用程式的 IP 位址。
序號	（選用）被隔離裝置的序號（如有）。
使用者名稱	（選用）隔離裝置時登入該裝置的 GlobalProtect 用戶端使用者的使用者名稱。

託管設備） > Health（健康狀態

Panorama™ 讓您可以監測託管防火牆的硬體來源與性能。Panorama 將時間趨勢性能資料（CPU、記憶體、CPS和吞吐量）、日誌記錄性能、環境資料（如風扇、RAID狀態和電源）集中到一起，並將（如提交、內容安裝和軟體升級）與健康數據產生關聯。當防火牆偏離其計算出的基準線時，Panorama 會將其回報為偏離的設備以協助快速辨識、診斷和解決任何硬體問題。

您可以使用本頁來：

檢視詳細的設備健康狀態。	檢視由 Panorama 託管的設備健康狀態度量。
群組 HA 端點	檢視哪些防火牆為同一群組以協助辨識潛在問題並決定防火牆是否有或哪一個有受到任何硬體資源或性能問題影響。
PDF/CSV	具有最小唯讀訪問權限的管理角色可以匯出 **PDF/CSV** 格式的託管防火牆表。您可以在必要時（如審核時）套用篩選以建立更多特定表格設定輸出。僅可匯出網路介面中可見的欄位。請參閱匯出設定表資料。

Panorama > Managed Devices（託管設備） *> Health*（健康狀態）*# All Devices*（所有設備）

使用本頁檢視下列每個防火牆的資料。

健康資訊	說明
裝置名稱	顯示防火牆的主機名稱或序號。 對於 VM 系統 NSX 版防火牆，防火牆名稱將附加至 ESXi 主機的主機名稱。例如，PA-VM：Host-NY5105
Model	防火牆型號
裝置	
吞吐量（Kbps）	隨時間變化的數據吞吐量（五分鐘平均值），以千字元/秒為單位。
CPS	隨時間變化的每秒總連線數（五分鐘平均值）。

© 2019 Palo Alto Networks, Inc.

健康資訊	說明
工作階段	
計數（工作階段）	隨時間變化的總工作時段計數。
資料背板	
CPU（%）	資料背板上的總 CPU 使用率。
管理平面	
CPU（%）	管理平面上的總 CPU 使用率。
MEM (%)	管理平面上的總記憶體使用率。
日誌記錄速率（每秒日誌數）	防火牆轉送日誌至 Panorama 或日誌收集器的速率（一分鐘平均）。
風扇	顯示每個風扇托盤中風扇的狀態、當前狀態、RPM 和最後一次故障狀態。風扇狀態顯示方式為 *A*/*B*，*A* 代表良好、運轉中風扇的數量，而 *B* 為在防火牆中的風扇總數。虛擬防火牆則顯示 N/A。
電源供應器	顯示現今、當前狀態以及最後一次故障的時間戳記。電源供應器狀態顯示方式為 *A*/*B*，*A* 代表良好、運轉中電源供應器的數量，而 *B* 為在裝置中的電源供應器總數。虛擬防火牆則顯示 N/A。
連接埠	在防火牆內使用中的連接埠總數。連接埠狀態顯示方式為 *A*/*B*，*A* 代表良好、運轉中連接埠的數量，而 *B* 為在設備中的連接埠總數。

Panorama > Managed Devices（託管設備）*> Health*（健康狀態）*# Deviating Devices*（偏離的設備）

偏離的設備頁籤顯示有任何度量偏離其計算出基準線的設備，並以紅色顯示那些偏離的度量值。度量健康狀態基準線由給定的 7 天度量值加上標準偏離值所平均的健康性能來決定。

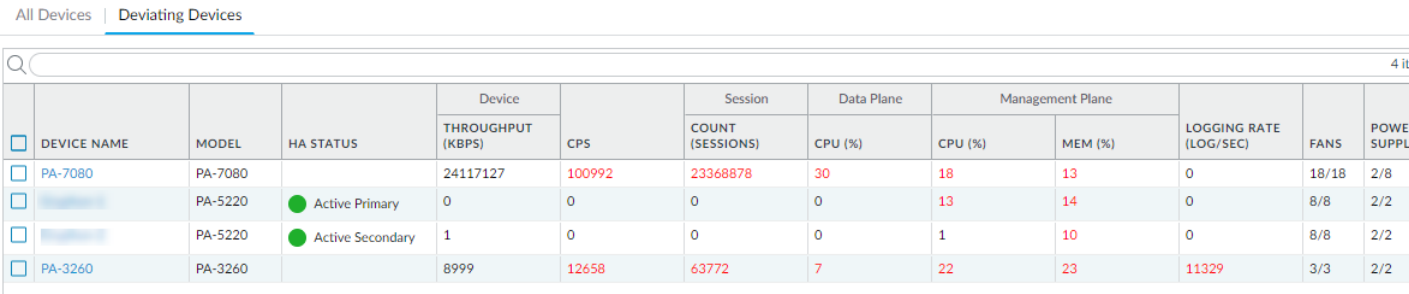


圖 1: 偏離度量範例

Panorama 上的詳細裝置健康狀態

您可以透過按一下所有裝置頁籤或偏離的裝置頁籤中的裝置名稱，來檢視個別的防火牆詳細裝置健康狀態記錄。詳細裝置檢視使用時間篩選條件提供健康狀態記錄，並顯示與裝置相關聯的元數據。裝置健康狀態資料以表格或如同 widge 般顯示，在可能的情況下提供時間趨勢數據的圖形表示。

© 2019 Palo Alto Networks, Inc.

管理詳細裝置檢視

除了與防火牆關聯的描述性元數據外，詳細裝置檢視還顯示詳細的防火牆健康狀態資料。在適用的情況下，您可以設定 Settings（設定）（⚙）以獲取 Widget 的其他選項或最大化面板（⊡）以放大 Widget。

欄位	說明
動作	
時間篩選器	選取時間篩選條件以從下拉式清單檢視裝置健康狀態記錄。您可以選取最近 **12** 個小時、**24** 個小時、**7** 天、**15** 天、**30** 天 或 **90** 天。
顯示平均值	選取在所有時間趨勢 Widget 上所顯示的平均和標準時間散佈。您可以選取無、最近 **24** 小時、**7** 天 或 **15** 天。
重新整理	以最新的資料重新整理顯示的資料。
列印 PDF	生成目前顯示的頁籤 PDF。 您需要啟用彈出視窗以選取下載位置並存取此 *PDF*。
系統資料	
系統資料	與裝置有關聯的元數據：IP 位址、軟體版本、防毒軟體版本、HA 狀態、序號、應用程式和威脅版本、Wildfire 版本、VSYS 模式、模組和裝置模式。

工作階段

工作階段頁籤顯示通過防火牆的工作階段資料。此資料以六個個別的圖表顯示。

欄位	說明
吞吐量	一段時間（五分鐘平均值）的資料吞吐量，以千字元/秒（Kbps）為單位。
工作階段數	隨時間變化的總工作時段計數。
每秒連線數	隨時間變化的每秒總連線數（五分鐘平均值）。
每秒傳送的封包	通過裝置的每秒總封包數（五分鐘平均值）。
全域工作階段表使用率（僅 PA-7000 和 PA-5200 應用裝置）	具有全域工作階段表的防火牆，其隨時間推移的全域工作階段表百分比（五分鐘平均值）。
工作階段表使用	顯示防火牆隨時間變化的每一個資料平面工作階段表使用百分比（五分鐘平均值）。
SSL 解碼工作階段資料	顯示解密 SSL 工作階段隨時間變化的數量（五分鐘平均值）。

© 2019 Palo Alto Networks, Inc.

欄位	說明
SSL Proxy 工作階段使用	顯示 Proxy 工作階段隨時間變化的使用率（五分鐘平均值）。

環境

Environments（環境）頁籤顯示如電力供應、風扇托架和磁碟機的清況、狀態與硬體運作情形。本頁籤僅在硬體為基礎的防火牆顯示：

欄位	說明
風扇狀態	顯示每個風扇托盤中風扇的狀態、當前狀態、RPM 和最後一次故障狀態。風扇狀態顯示方式為 *A*/*B*，*A* 代表良好、運轉中風扇的數量，而 *B* 為在防火牆中的風扇總數。虛擬防火牆則顯示 `N/A`。
電源	顯示現今、當前狀態以及最後一次故障的時間戳記。電源供應器狀態顯示方式為 *A*/*B*，*A* 代表良好、運轉中電源供應器的數量，而 *B* 為在裝置中的電源供應器總數。虛擬防火牆則顯示 `N/A`。
過熱狀態	顯示裝置的每一個插槽是否有任可過熱警報。如果有警報啟動，則防火牆也會在這裡顯示有關確切溫度和位置的更特定資料。
系統磁碟狀態	顯示 root、pancfg、panlogs 和 panrepo 掛載的可用、已用的和使用率。 系統磁碟狀態也顯示了磁碟名稱、尺寸和啟用 RAID 防火牆的 RAID 狀態。

介面

介面頁籤顯示所有防火牆實體介面的狀態與統計數值。

欄位	說明
介面名稱	介面名稱。選取一個介面以檢視選定介面的位元速率、每秒封包、錯誤和丟棄圖表。
狀態	介面狀態：`Admin Up`（管理上移）、`Admin Down`（管理下移）、`Operational Up`（操作上移）或 `Operational Down`（操作下移）。
位元速率	顯示接收和傳送資料的位元速率（bps）。
每秒傳送的封包	顯示接收和傳送資料的每秒封包數。
錯誤	顯示接收和傳送資料的每秒錯誤數。
捨棄	顯示接收和傳送資料的每秒中斷連線數。

© 2019 Palo Alto Networks, Inc.

記錄

日誌記錄頁籤顯示託管防火牆的日誌記錄率和連線。

欄位	說明
記錄速率	顯示裝置轉送日誌到 Panorama 或日誌收集器的一分鐘平均速率.
日誌記錄連線	顯示所有可用的日誌轉送連線，包含他們的啟用或停用狀態。
外部日誌轉送	顯示各種外部日誌轉送法類型的已傳送、已丟棄和平均轉送率（日誌/每秒）。

資源

資源頁籤顯示防火牆的 CPU 和記憶體統計數值。

欄位	說明
管理平面記憶體	以百分比顯示時間趨勢、管理平面記憶體五分鐘平均值。
封包緩衝區	以百分比顯示時間趨勢、封包緩衝區使用率五分鐘平均值。在多重資料平面系統中，會以不同顏色顯示包含不同的資料平面、CPU 和封包緩衝區。
封包描述元	以百分比顯示時間趨勢、封包描述元使用率五分鐘平均值。在多重資料平面系統中，會以不同顏色顯示包含不同的資料平面、CPU 和封包緩衝區。
CPU 管理平面	以百分比顯示時間趨勢、CPU 管理平面五分鐘平均值。
CPU 資料平面	顯示時間趨勢、CPU 資料平面每核心利用率五分鐘平均值。對於多資料平面系統，您可以選取要檢視哪一個資料平面的選取器。
掛載	顯示裝置系統檔案資料。此顯示包含掛載名稱、配置（KB）、已用（KB）和可用（KB）空間，以及利用率。

high availability（高可用性）

高可用性頁籤顯示防火牆和其 HA 端點的 HA 狀態。上方的 widget 顯示裝置與其端點的設定和內容版本。下方的 widget 則提供有關先前 HA 容錯轉移和相關理由的資料，包含哪一個防火牆經歷了該次故障。

© 2019 Palo Alto Networks, Inc.

Panorama > 範本

透過 **Device**（設備）和 **Network**（網路）頁籤，您可以使用範本或範本堆疊（範本的組合）將一般基礎設定部署至多個需要類似設定的防火牆。使用 Panorama 管理防火牆設定時，您可以使用設備群組（管理共用政策和物件）和範本（管理共用設備和網路設定）的組合。

除了建立範本或範本堆疊的對話方塊中可用的設定之外，**Panorama** > **Templates**（範本）還會顯示下列欄：

- 類型 — 將列示項目識別為範本或範本堆疊。
- 堆疊—列示指派給範本堆疊的範本。

您想進行什麼操作？	請參閱：
新增、複製、編輯或刪除範本	範本
新增、複製、編輯或刪除範本堆疊。	範本堆疊
想知道更多？	範本與範本堆疊
	管理範本與範本堆疊

範本

Panorama 支援最多 1,024 個範本。您可以 **Add**（新增）一個範本並如下列表格所述的設定來設定。在創建一個範本後，還需要 Configure a Template Stack（設定範本堆疊）並在可以管理防火牆前將範本和防火牆新增至範本堆疊中。在設定範本後，您必須在 Panorama 中認可變更（請參閱 Panorama 認可操作）。

刪除一個範本並不會刪除 *Panorama* 已推送至防火牆的值。

範本設定	說明
名稱	輸入範本名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號、英文句點和底線。 在 **Device**（設備）和 **Network**（網路）頁籤中，此名稱將顯示在 **Template**（範本）下拉式清單中。您在這些頁籤中修改的設定只會套用至所選 **Template**（範本）。
說明	輸入範本的說明。

範本堆疊

可設定範本堆或指定範本進行範本堆疊。為範本堆疊指定防火牆使得您可以將所有必要設定推送至防火牆，而不用在每個單獨的範本上新增每一個設定。Panorama 支援最多 1,024 個堆疊。您可以 **Add Stack**（新增堆疊）以創建新的範本堆疊並如下列表格所述的設定來設定。設定範本堆疊後，您必須在 Panorama 中認可變更（請參閱 Panorama 認可操作）。另外，在您設定已指派給堆疊的防火牆網路與設備設定之後，您必須執行範本提交，並將設定推送至防火牆。

© 2019 Palo Alto Networks, Inc.

刪除範本堆疊或從範本堆疊移除防火牆並不會刪除 *Pnorama* 先前推送至防火牆的值；然而，當您從範本堆疊移除防火牆時，*Panorama* 不會再將新的更新推送至該防火牆。

範本堆疊設定	說明
名稱	輸入堆疊名稱（最多 31 個字元）。名稱區分大小寫、必須是唯一的、必須以英文字母開頭且只能包含字母、數字、連字號和底線。在 **Device**（設備）和 **Network**（網路）頁籤中，**Template**（範本）下拉式清單會顯示堆疊名稱和指派給該堆疊的範本。
說明	輸入堆疊的說明。
範本	**Add**（新增）您想要包含於堆疊的每個範本（至多 8 個）。 如果範本具有重複的設定，則在推送設定至指定的防火牆時，Panorama 只會推送在清單中位置較高的範本設定。例如，如果 Template_A 在清單中位於 Template_B 的上方，且兩個範本都定義 ethernet1/1 介面，那麼 Panorama 會從 Template_A 套用 ethernet1/1 定義，而非 Template_B。若要變更設定檔的清單順序，請選取設定檔，並 **Move Up**（上移）或 **Move Down**（下移）。 *Panorama* 不會在堆疊中驗證範本組合，因此請將您的範本排定順序以避免無效的關係。
裝置	選取您想要新增至堆疊的每個防火牆。 如果防火牆清單較長，您可以透過 **Platforms**（平台）、**Device Groups**（設備群組）、**Tags**（頁籤）和 **HA Status**（**HA** 狀態）篩選清單。 您可以將具有不相符模式（*VPN* 模式、多個系統模式或操作模式）的防火牆指派給相同堆疊。*Panorama* 只會將模式特定設定推送至支援這些模式的防火牆。
全選	選取清單中的每一個防火牆。
取消全選	取消選取清單中的每一個防火牆。
群組 HA 端點	分組作為高可用性 (HA) 端點的防火牆。這可讓您輕鬆識別具有 HA 組態的防火牆。從範本堆疊推送設定時，您可以推送至群組配對，而非分別套用至每個防火牆。
已選取篩選器	若要僅顯示特定防火牆，請選取防火牆，然後選取 **Filter Selected**（已選取篩選器）。

Panorama > Templates > Template Variables（Panorama > 範本 > 範本變數）

- 新範本變數建立
- 編輯現有範本變數
- 在裝置上建立或編輯變數定義

您可以為範本和範本堆疊定義變數（**Panorama** > 範本）或為單獨的裝置編輯現有變數（**Panorama** > 託管裝置 > 摘要）。變數是在範本或範本堆疊上定義的組態元件，可在您使用 Panorama 管理防火牆組態時提供靈活性和可再使用性。您可以使用變數取代：

- 此組態中所有範圍的 IP 位址（包含 IP 網路遮罩、IP 範圍和 FQDN）。

© 2019 Palo Alto Networks, Inc.

- 在 IKE 閘道設定中和在 HA 組態中（群組 ID）的介面
- SD-WAN 設定中的設定元素（AS 編號、QoS 設定檔、輸出最大值、連結標籤）。

當您在範本堆疊中新增防火牆時，他們會自動繼承您為範本或範本堆疊所建立的變數。

範本變數資料	說明
名稱	變數定義名稱。
範本（裝置與範本堆疊）	顯示變數定義所屬的範本名稱。
類型	顯示變數定義類型： • **IP Netmask**（**IP** 網路遮罩）—定義靜態 IP 或網路位址。 • **IP Range**（**IP** 範圍）—定義 IP 範圍。例如，192.168.1.10-192.168.1.20。 • **FQDN**—定義完整符合資格的網域名稱 。 • **Group ID**（群組 **ID**）—定義高可用性群組 ID。如需詳細資料，請參閱主動/被動 HA 組態指南。 • **Device Priority**（裝置優先順序）—定義裝置優先順序，以指示防火牆在主動-被動高可用性 (HA) 設定中應扮演主動角色的偏好設定。 • **Device ID**（裝置 **ID**）—定義用於在主動-主動高可用性 (HA) 設定中指派裝置優先順序評估器的裝置 ID。 • **Interface**（介面）—定義防火牆中的防火牆介面。僅可用於 IKE 閘道組態上。 • **AS Number**（**AS** 編號）—定義要在 BGP 設定中使用的自發系統編號。 • **QoS Profile**（**QoS** 設定檔）—定義要在 QoS 設定中使用的服務品質 (QoS) 設定檔。 • **Egress Max**（輸出最大值）—定義要在 QoS 設定檔設定中使用的輸出最大值。 • **Link Tag**（連結標籤）—定義要在 SD-WAN 設定中使用的連結標籤。
值	顯示變數定義的設定值。
新增（範本與範本堆疊）	新增新範本變數定義。
刪除	刪除已有的範本變數定義
複製	複製已有的範本變數定義
取代（範本與範本堆疊）	取代自範本堆疊或裝置繼承的現有範本變數定義。您無法更改變數類型或名稱且您無法取代特定裝置的變數。
復原（範本與範本堆疊）	若要清除範本堆疊或裝置層級上的取代值；復原取代變數至初始範本變數定義。
獲得僅在裝置上使用的值（僅限裝置）	使用在防火牆中使用的選定變數。必要條件為在 Panorama 能夠擷取值前，範本或範本堆變數已定義並推送至防火牆。從防火牆截取的值將取代範本或範本堆疊變數以建立特定裝置的變數。如果變數定義已推送至防火牆，Panorama 將返回該變數`Value not found`（未發現值）。

© 2019 Palo Alto Networks, Inc.

新範本變數建立

新增 新範本變數定義。

新範本變數定義資料	說明
名稱	變數定義名稱。所有變數定義名稱必須以錢符號字元（「$」）開頭。
類型	選取變數定義類型：**IP Netmask**（**IP** 網路遮罩）、**IP Range**（**IP** 範圍）、**FQDN**、**Group ID**（群組 **ID**）、**Device Priority**（裝置優先順序）、**Device ID**（裝置 **ID**）、**Interface**（介面）、**AS Number**（**AS** 編號）、**QoS Profile**（**QoS** 設定檔）、**Egress Max**（輸出最大值）或 **Link Tag**（連結標籤）。
值	輸入變數定義的期望值。

編輯現有範本變數

您可以在建立變數後的任何時間點為範本或範本堆疊編輯範本變數定義（**Panorama** > 範本）。管理範本變數以在必要時選取變數並編輯可用值。

在裝置上建立或編輯變數定義

前往 **Panorama** > 託管的裝置 > 摘要 以建立變數定義或取代從 Panorama 範本或範本堆疊推送出來的範本變數。範本變數包含：

- 此組態所有範圍內的 IP 位址（包含 IP 網路遮罩、IP 範圍和 FQDN）。
- 在 IKE 閘道組態中的介面或 HA 組態（群組 ID）
- SD-WAN 設定中的設定元素（AS 編號、QoS 設定檔、輸出最大值、連結標籤）。

建立裝置變數能讓您從相同範本堆疊中複製取代的特定裝置變數，而不用個別地重新建立它們。所有變數定義預設為自範本或範本堆疊繼承，且僅可以取代—您無法為個別裝置刪除或建立新的變數定義。

透過從範本堆疊中現有裝置複製變數定義或**Edit**（編輯）現有裝置變數定義， 以**Create**（建立）裝置變數定義。

© 2019 Palo Alto Networks, Inc.

Panorama > Device Groups（Panorama > 裝置群組）

裝置群組由您要作為群組管理的防火牆與虛擬系統組成，例如管理公司中的分公司群組或個別部門群組的防火牆。Panorama 套用原則時，會將這些群組都視為單一單位。防火牆僅能屬於一個裝置群組，但由於在 Panorama 中虛擬系統為不同的實體，因此您可以將防火牆內的虛擬系統指派給不同的裝置群組。

您可以在共用位置下最多四層的樹狀階層中將裝置群組巢狀化，以在防火牆網路之間實作管理原則的分層方法。在底端層級，裝置群組可以具有上一層、上二層和上三層裝置群組（統稱為父系），底端階層會從上層繼承原則和物件。在頂端層級，裝置群組可以具有下一層、下二層和下三層裝置群組（統稱為子系）。當您選取 **Panorama** > **Device Groups**（裝置群組）時，名稱欄會顯示此裝置群組階層。

在新增、編輯或刪除裝置群組後，請執行 Panorama 認可及裝置群組認可（請參閱 Panorama 認可操作）。Panorama 隨後會將組態變更推送至已指派給裝置群組的防火牆；Panorama 支援最多 1,024 個裝置群組。

若要設定裝置群組，請 **Add**（新增）裝置群組並按下表所述進行設定。

裝置群組設定	說明
名稱	輸入用來識別群組的名稱（最多 31 個字元）。名稱區分大小寫且必須在整個裝置群組階層間是唯一的，而且只能包含字母、數字、空格、連字號和底線。
說明	輸入裝置群組的說明。
裝置	選取您想要新增至裝置群組的每個防火牆。如果防火牆清單較長，您可以透過 **Device State**（裝置狀態）、**Platforms**（平台）、**Templates**（範本）或 **Tags**（頁籤）進行選取。[篩選器] 區段會針對每個類別，（在括號中）顯示受管理防火牆數。 如果裝置群組的目的單純是組織用途（即用於包含其他裝置群組），則您不需要將防火牆指派給該群組。
全選	選取清單中的每一個防火牆與虛擬系統。
取消全選	取消選取清單中的每一個防火牆與虛擬系統。
群組 HA 端點	選取以針對在高可用性 (HA) 組態中作為端點的防火牆進行分組。然後清單會在括號中，先顯示主動（在主動/主動組態中為主動主要）防火牆，再顯示被動（在主要/主動組態中為主動次要）防火牆。這可讓您輕鬆識別 HA 模式下的防火牆。套用共用原則時，您可以套用至群組配對，而非套用至個別配對。 針對主動/被動組態中的 *HA* 端點，請考慮同時將兩者的防火牆或虛擬系統新增至相同的裝置群組。這可讓您將組態同時套用至兩個端點。
已選取篩選器	若要讓裝置清單僅顯示特定防火牆，請選取該防火牆，然後選取 **Filter Selected**（已選取篩選器）。
父系裝置群組	相對於您定義的裝置群組，選取階層上方的裝置群組（或共用位置）（預設為 **Shared**（已共用））。

© 2019 Palo Alto Networks, Inc.

裝置群組設定	說明
主要裝置	若要根據使用者名稱和使用者群組設定原則規則和報告，您必須選取 **Master Device**（主要裝置）。Panorama 會從該防火牆接收使用者名稱、使用者群組名稱和使用者名稱至群組對應資訊。 當您變更 *Master Device*（主要裝置）或將其設定為 *None*（無）時，*Panorama* 會遺失從防火牆接收的所有使用者和群組資訊。
從主要裝置儲存使用者和群組	只有在您選取 **Master Device**（主要裝置）時，才會顯示此選項。此選項讓 Panorama 在本機上儲存使用者名稱、使用者群組名稱、其從 **Master Device**（主要裝置）接收的使用者名稱至群組對應資訊。若要啟用本機儲存，您也必須選取 **Panorama** > **Setup**（設定）> **Management**（管理），編輯 Panorama 設定，並在群組中啟用報告和篩選。
動態新增的裝置屬性—當新裝置新增至裝置群組時，Panorama 會將指定的授權碼和 PAN-OS 軟體版本動態套用到新裝置。這只有裝置群組在 Panorama 中與 NSX 服務定義相關聯後才會顯示。	
授權碼	針對新增到此裝置群組的裝置輸入要套用的授權碼。
SW 版本	針對新增到此裝置群組的裝置選取要套用的軟體版本。

© 2019 Palo Alto Networks, Inc.

Panorama > 受管理的收集器

Panoramam 管理伺服器（M-Series 裝置、或 Panorama 模式下的 Panorama 虛擬裝置）可以管理專用日誌收集器（在日誌收集器模式下的 M-Series 裝置或 Panorama 虛擬裝置）。各個 Panorama 管理伺服器也具有本機上預先定義的日誌收集器（名為預設），用於處理其直接從防火牆接收的日誌。（[傳統] 模式下的 Panorama 虛擬裝置會儲存直接從防火牆接收的日誌，而無需使用專用日誌收集器。）

若要使用 Panorama 管理專用日誌收集器，請將日誌收集器其新增為受管理的收集器。

您想進行什麼操作？	請參閱：
顯示日誌收集器資訊	日誌收集器資訊
新增、複製、編輯或刪除日誌收集器	日誌收集器組態
在日誌收集器上更新 Panorama 軟體	專用日誌收集器的軟體更新
想知道更多？	集中記錄日誌與報告
	設定受管理收集器

日誌收集器資訊

選取 **Panorama** > **Managed Collectors**（受管理的收集器）可顯示日誌收集器的下列資訊。其他參數則可在日誌收集器設定期間進行設定。

日誌收集器資訊	說明
收集器名稱	識別此日誌收集器的名稱。此名稱顯示為日誌收集器主機名稱。
序號	用作日誌收集器的 Panorama 設備序號。如果日誌收集器位於本機，則這是 Panorama 管理伺服器的序號。
軟體版本	安裝於日誌收集器上的 Panorama 軟體版本。
IP 位址	日誌收集器管理介面的 IP 位址。
已連線	日誌收集器與 Panorama 之間的連線狀態。
組態狀態/詳細資訊	表示日誌收集器上的組態設定是否與 Panorama 同步。
執行階段狀態/詳細資訊	此日誌收集器與收集器群組中的其他日誌收集器之間的連線狀態。
日誌重新散佈狀態	某些動作（例如，新增磁碟）會導致日誌收集器重新分配其磁碟配對間的日誌。此欄以百分比表示重新分配程序中的完成狀態。
上次提交狀態	表示收集器群組對日誌收集器的提交是成功還是失敗。

© 2019 Palo Alto Networks, Inc.

日誌收集器資訊	說明
統計資料	在您完成日誌收集器設定之後，按一下 **Statistics**（統計資料）可檢視磁碟資訊、CPU 效能以及平均記錄速率（日誌數/秒）。為了更加了解您正在檢閱的日誌範圍，您也可以檢視日誌收集器已接收的最舊日誌資訊。 如果您使用 SNMP 管理員來進行集中監控，您也可以在 *panLogCollector MIB* 中看到記錄統計資料。

日誌收集器組態

選取 **Panorama** > **Managed Collectors**（受管理的收集器），以管理日誌收集器。當您 **Add**（新增）日誌收集器來作為受管理的收集器時，您所進行的設定會根據日誌收集器位置和是否將 Panorama 部署在高可用性 (HA) 組態而有所不同：

- 專用日誌收集器—當您新增日誌收集器時，**Interfaces**（介面）頁籤一開始並不會顯示。您必須輸入日誌收集器的序號（收集器序號），按一下 **OK**（確定），然後編輯日誌收集器以顯示介面設定。
- 單獨（非 **HA**）或主動 **(HA) Panorama** 管理伺服器的本機預設日誌收集器—在輸入 Panorama 管理伺服器的序號（**Collector S/N**（收集器序號））後，收集器對話方塊只會顯示 **Disks**（磁碟）、**Communication**（通訊）設定，以及一小組 **General**（一般）設置。日誌收集器會從 Panorama 管理伺服器的組態衍生其所有其他設定的值。
- （僅限 HA）被動 **Panorama** 管理伺服器的本機預設日誌收集器—Panorama 會將此日誌收集器視為遠端收集器，因此其設定方式必須和專用日誌收集器的設定方式相同。

用於設定日誌收集器的完整程序需要完成其他工作。

您想了解什麼內容？	請參閱：
識別日誌收集器並定義其與 Panorama 管理伺服器和 外部服務的連線。	一般日誌收集器設定
設定對日誌收集器 CLI 的存取。	日誌收集器驗證設定
設定專用日誌收集器用於管理流量、收集器群組通訊和日誌收集的介面。	日誌收集器介面設定
設定儲存從防火牆收集之日誌的 RAID 磁碟。	日誌收集器 RAID 磁碟設定
將日誌收集器設定為從 User-ID 代理程式接收使用者對應資訊。	User-ID 代理程式設定
將日誌收集器設定為對 Windows User-ID 代理程式進行驗證。	連線安全性
針對 Panorama、其他日誌收集器和防火牆的通訊設定安全性設定。	通訊設定

© 2019 Palo Alto Networks, Inc.

一般日誌收集器設定

- Panorama > 受管理的收集器 > 一般

設定如下表所述的設定，以識別日誌收集器並定義其與 Panorama 管理伺服器、DNS 伺服器與 NTP 伺服器的連線。

日誌收集器的一般設置	說明
收集器	（必要）輸入用作日誌收集器的 Panorama 設備序號。如果日誌收集器位於本機，請輸入 Panorama 管理伺服器的序號。
收集器名稱	輸入用來識別此日誌收集器的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。 此名稱顯示為日誌收集器主機名稱。
安全 Syslog 的輸入憑證	選取要讓受管理的收集器能夠從 Traps™ ESM 伺服器安全地擷取日誌所必須使用的憑證。此憑證稱為輸入憑證，因為 Panorama/受管理的收集器是用來接收 Traps ESM（用戶端）所傳送之日誌的伺服器；如果日誌擷取設定檔的 **Transport**（傳輸）通訊協定是 **SSL**，則必須有此憑證。
安全 Syslog 的憑證	選取憑證，將 Syslog 安全轉送至外部 Syslog 伺服器。憑證必須選取 **Certificate for Secure Syslog**（安全性 **Syslog** 的憑證）選項（請參閱管理防火牆及 Panorama 憑證）。將 Syslog 伺服器設定檔指派給包含此日誌收集器的收集器群組時（請參閱 [Panorama > 收集器群組]、**Panorama** > **Collector Groups**（收集器群組）> **Collector Log Forwarding**（收集器日誌轉送）），伺服器設定檔的 **Transport**（傳輸）通訊協定必須是**SSL**（請參閱 [設備 > 伺服器設定檔 > Syslog]）。
Panorama 伺服器 IP	指定管理此日誌收集器之 Panorama 管理伺服器的 IP 位址。
Panorama 伺服器 IP 2	如果在高可用性 (HA) 組態中部署 Panorama 管理伺服器，請指定次要端點的 IP 位址。
網域	輸入日誌收集器的網域名稱。
主要 DNS 伺服器	輸入主要 DNS 伺服器的 IP 位址。日誌收集器會針對 DNS 查詢使用此伺服器（例如尋找 Panorama 管理伺服器）。
次要 DNS 伺服器	（選用）輸入當主要伺服器不可用時，您要使用的次要 DNS 伺服器 IP 位址。
主要 NTP 伺服器	輸入主要 NTP 伺服器（若存在）的 IP 位址或主機名稱。如果您未使用 NTP 伺服器，可以手動設定日誌收集器時間。
次要 NTP 伺服器	（選用）輸入當主要伺服器不可用時，您要使用的次要 NTP 伺服器 IP 位址與主機名稱。
timezone	選取日誌收集器的時區。
緯度	輸入日誌收集器的緯度（-90.0 到 90.0）。流量與威脅對應使用 App Scope 的緯度。
經度	輸入日誌收集器的經度（-180.0 到 180.0）。流量與威脅對應使用 App Scope 的經度。

© 2019 Palo Alto Networks, Inc.

日誌收集器驗證設定

- Panorama > Managed Collectors > Authentication（Panorama > 受管理的收集器 > 驗證）

日誌收集器模式（專用日誌收集器）下的 M-Series 設備或 Panorama 虛擬設備沒有網頁介面；只有 CLI。您可使用 Panorama 管理伺服器在專用日誌收集器上設定大多數設定，但某些設定需要 CLI 存取。若要為 CLI 存取進行驗證設定，請設定如下表所述的設定。

日誌收集器驗證設定	說明
驗證設定檔	選取已設定的驗證設定檔以定義驗證服務，該服務將驗證專用日誌收集器或 Panorama 管理員的登入憑證。
失敗的嘗試	輸入在鎖定管理員之前專用日誌收集器在 CLI 上允許的失敗登入嘗試次數（範圍是 0 至 10；預設值為 10）。限制登入嘗試有助於保護 WildFire 設備免受暴力密碼破解攻擊。0 值會指定不受限制的登入嘗試次數。 如果您將 *Failed Attempts*（失敗的嘗試）數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，則管理員將無限期被鎖定，直至另一位管理員手動解鎖該被鎖定的管理員為止。如果沒有建立其他管理員，您必須在 *Panorama* 上重新設定 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）設定，並將組態變更推送至日誌收集器。要確保管理員永不被鎖定，讓 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）都使用預設值 *(0)*。 將 *Failed Attempts*（失敗的嘗試）的數量設定為 *5* 或以下，以便在輸入錯誤時允許合理的重試次數，同時防止惡意系統嘗試使用暴力密碼破解攻擊登入專用日誌收集器。
鎖定時間（分鐘）	輸入達到 **Failed Attempts**（失敗的嘗試）限值（範圍是 0 至 60；預設值為 5）後，專用日誌收集器鎖定管理員，使其無法存取 CLI 的分鐘數。0 值表示會套用封鎖，直到另一個管理員手動解除鎖定帳戶。 如果您將 *Failed Attempts*（失敗的嘗試）數值設定為 *0* 以外的數字，但將 *Lockout Time*（鎖定時間）保留為 *0*，則管理員將無限期被鎖定，直至另一位管理員手動解鎖該被鎖定的管理員為止。如果沒有建立其他管理員，您必須在 *Panorama* 上重新設定 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）設定，並將組態變更推送至日誌收集器。要確保管理員永不被鎖定，讓 *Failed Attempts*（失敗的嘗試）和 *Lockout Time*（鎖定時間）都使用預設值 *(0)*。 將 *Lockout Time*（鎖定時間）設定為至少 *30* 分鐘，以防止惡意行為者連續嘗試登入。
閒置逾時（分鐘）	輸入在管理員自動登出之前不包含任何 CLI 上的活動的最大分鐘數（範圍是 0 至 1,440；預設值為「無」）。值為 0 表示非使用狀態未觸發自動登出。 將 *Idle Timeout*（閒置逾時）設定為 *10* 分鐘，以防止未經授權的使用者在管理員沒有關閉工作階段時存取專用日誌收集器。

© 2019 Palo Alto Networks, Inc.

日誌收集器驗證設定	說明
最大工作階段計數	輸入管理員可以同時開啟的作用中工作階段數目，預設值為 0，這意味著專用日誌收集器可以有無限數量的同時作用中工作階段。
最大工作階段時間	輸入管理員在自動登出之前可登入的分鐘數。預設值為 0，這意味著即使閒置，管理員亦可無限期登入。
本機管理員	新增並設定專用日誌收集器的新管理員。這些管理員專屬於專用日誌收集器，可從此頁面進行管理（**Panorama** > **Managed Collectors**（受管理收集器）> **Authentication**（驗證））。
Panorama 管理員	匯入 Panorama 上設定的現有管理員。這些管理員在 Panorama 上建立，並匯入至專用日誌收集器。

日誌收集器介面設定

- Panorama > Managed Collectors > Interfaces（Panorama > 受管理的收集器 > 介面）

依預設，專用日誌收集器（處於日誌收集器模式的M-Series 裝置）會使用管理 (MGT) 介面來處理管理流量、日誌收集及收集器群組通訊。不過，Palo Alto Networks 建議您針對日誌收集和收集器群組通訊指派不同的介面，以降低 MGT 介面的流量。您可以透過為 MGT 介面定義比其他介面的子網路更具私密性的不同子網路，來增強安全性。若要使用不同介面，您必須先在 Panorama 管理伺服器上設定這些介面（請參閱 [裝置 > 設定 > 管理]）。可供用於日誌收集和收集器群組通訊的介面會隨日誌收集器裝置型號而不同。例如，M-500 裝置存在下列介面：Ethernet1 (1Gbps)、Ethernet2 (1Gbps)、Ethernet3 (1Gbps)、Ethernet4 (10Gbps) 和 Ethernet5 (10Gbps)。

若要設定介面，請選取連結並設定如下表所述的設定。

若要完成 *MGT* 介面的設定，必須指定 *IP* 位址、網路遮罩（適用於 *IPv4*）或首碼長度（適用於 *IPv6*）和預設閘道。如果提交部分設定（例如，您可能略過預設閘道），只能透過主控台連接埠存取防火牆或 *Panorama* 以進行設定變更。

請一律認可完整的 *MGT* 介面組態。除非指定 *IP* 位址、網路遮罩（適用於 *IPv4*）或首碼長度（適用於 *IPv6*）和預設閘道，否則無法提交其他介面的設定。

日誌收集器介面設定	說明
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	您必須啟用介面才能對其進行設定。MGT 介面則屬例外，其依預設會是啟用狀態。
速度與雙工	設定介面的資料速率與雙工選項。選取包括全雙工或半雙工下的 10Mbps、100Mbps、1Gbps 和 10Gbps（僅限 Eth4 和 Eth5）。使用預設 **auto-negotiate**（自動交涉）設定，讓日誌收集器決定介面速度。 此設定必須與相鄰網路裝置的介面設定相符。
IP 位址 (IPv4)	如果網路使用 IPv4 位址，請將 IPv4 位址指派給介面。
網路遮罩 (IPv4)	如果將 IPv4 位址指派給介面，則您也必須輸入網路遮罩（例如 255.255.255.0）。

© 2019 Palo Alto Networks, Inc.

日誌收集器介面設定	說明
預設閘道 (IPv4)	如果將 IPv4 位址指派給介面，則您也必須將 IPv4 位址指派給預設閘道（閘道必須位於與 MGT 介面相同的子網路上）。
IPv6 位址/首碼長度	如果網路使用 IPv6 位址，請將 IPv6 位址指派給介面。若要指出網路遮罩，請輸入 IPv6 首碼長度（例如，2001:400:f00::1/64）。
預設 IPv6 閘道	如果將 IPv6 位址指派給介面，則您也必須將 IPv6 位址指派給預設閘道（閘道必須位於與介面相同的子網路上）。
MTU	以位元組為單位，輸入在此介面上傳送之封包的最大傳輸單位 (MTU)（範圍是 576 到 1,500；預設為 1,500）。
裝置日誌收集	啟用介面以便從防火牆收集日誌。對於具有高日誌流量的部署，您可以啟用多個介面來執行此功能。MGT 介面上預設會啟用此功能。
收集器群組通訊	啟用收集器群組通訊的介面（預設為 MGT 介面）。只有一個介面可執行此功能。
Syslog 轉送	啟用轉送 syslog 的介面（預設為 MGT 介面）。只有一個介面可執行此功能。
網路連線服務	任何介面都能使用 **Ping** 服務，而且此服務可讓您測試日誌收集器介面和外部服務之間的連線。 下列服務則只能在 MGT 介面上使用： • **SSH**—可讓您安全存取防火牆 CLI。 • **SNMP**—讓介面可以從 SNMP 管理員接收統計資料查詢。如需詳細資訊，請參閱啟用 SNMP 監控。 • **User-ID**—讓日誌收集器能夠重新分配從 User-ID 代理程式收到的使用者對應資訊。
許可的 IP 位址	輸入可透過此介面存取日誌收集器之系統的 IP 位址。 若清單是空白的（預設值），則表示任何用戶端系統都能進行存取。 *Palo Alto Networks* 建議您不要讓此清單空白；請（僅）指定 *Panorama* 管理員的用戶端系統以防止未經授權的存取。

日誌收集器 *RAID* 磁碟設定

- Panorama > 受管理的收集器 > 磁碟

在 M-Series 裝置或 Panorama 虛擬裝置上設定記錄磁碟後，您可以將這些磁碟 **Add**（新增）至日誌收集器組態。

依預設，M-Series 裝置隨附於第一個 RAID 1 磁碟配對（安裝在擴充插槽 A1 和 A2 中）。在軟體中，擴充插槽 A1 和 A2 中的磁碟配對名為磁碟配對 A。其餘擴充插槽則依序命名如下：磁碟配對 B、磁碟配對 C，依此類推。例如，M-500 裝置支援高達 12 個磁碟配對。您可以在相同裝置內安裝 2TB 或 1TB 磁碟的配對，不過，每個配對中的兩個磁碟機必須有相同的磁碟大小。

針對 24TB 的儲存容量，Panorama 虛擬裝置最多可支援 12 個虛擬記錄磁碟。

© 2019 Palo Alto Networks, Inc.

新增磁碟配對後，日誌收集器會重新分配其所有磁碟中的現有日誌，每 TB 的日誌可能會花費數小時。重新散佈程序期間會降低最大日誌擷取速率。在 **Panorama** > **Managed Collectors**（受管理的收集器）頁面中，[日誌重新散佈狀態] 欄會以百分比表示完成狀態。

如果您使用 SNMP 管理員來進行集中監控，您可以在 *panLogCollector MIB* 中看到記錄統計資料。

User-ID 代理程式設定

- Panorama > 受管理的收集器 > User-ID 代理程式

專用日誌收集器可從最多 100 個 User-ID 代理程式接收使用者對應。代理程式可以是在防火牆上執行的 PAN-OS 整合式 User-ID 代理程式或基於 Windows 的 User-ID 代理程式。在具有多重虛擬程式的防火牆上，每個虛擬程式都可以用作個別的 User-ID 代理程式。日誌收集器可將使用者對應重新散佈至防火牆或 Panorama 管理伺服器。

設定使用者對應和enableusemapping 重新散佈的完整程序需要完成除了 *User-ID* 代理程式之外的其他工作。

若要設定專用日誌收集器以連線到 User-ID 代理程式，請 **Add**（新增）一個日誌收集器，並依照下表所述進行設定：

User-ID 代理程式設定	說明
名稱	輸入用來識別 User-ID 代理程式的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、空格、連字號和底線。 對於用作 *User-ID* 代理程式的防火牆，此欄位不必與收集器名稱欄位相符。
主機型	• 基於 **Windows** 的 **User-ID** 代理程式—輸入安裝 User-ID 代理程式的 Windows 主機 IP 位址。 • 防火牆（**PAN-OS** 整合式 **User-ID** 代理程式）—輸入介面的主機名稱或 IP 位址，防火牆使用該介面重新散佈使用者對應。
連接埠	輸入 User-ID 代理程式接聽 User-ID 要求的埠號。預設為連接埠 5007，但您可以指定任何可用連接埠。不同的 User-ID 代理程式可使用不同的連接埠。 某些舊版的 *User-ID* 代理程式將使用連接埠 *2010* 作為預設連接埠。
收集器名稱	這些欄位參考的收集器是 User-ID 代理程式，而不是日誌收集器。僅在代理程式是重新散佈使用者對應至日誌收集器的防火牆或虛擬系統時，欄位才適用。輸入 **Collector Name**（收集器名稱）和 **Pre-Shared Key**（預先共用金鑰），該金鑰會將防火牆或虛擬系統識別為 User-ID 代理程式。您所輸入的值必須與設定防火牆或虛擬系統時所輸入的值相同，以作為 User-ID 代理程式（請參閱重新散佈）。
收集器預先共用金鑰/確認收集器預先共用金鑰	
已啟用	選取以啟用日誌收集器與 User-ID 代理程式間的通訊。

© 2019 Palo Alto Networks, Inc.

連線安全性

- **Device**（裝置）> **User Identification**（使用者識別）> **Connection Security**（連線安全性）
- **Panorama** > **User Identification**（使用者識別）> **Connection Security**（連線安全性）

用來設定日誌收集器所使用的憑證設定檔，以驗證 Windows User-ID 代理程式所提供的憑證。日誌收集器會使用選取的憑證設定檔，藉由驗證 User-ID 代理程式所提供的伺服器憑證，來確認該代理程式的識別。

工作	說明
User-ID 憑證設定檔	從下拉式清單中，選取防火牆或 Panorama 用來驗證 Windows User-ID 代理程式的憑證設定檔，或選取 **New Certificate Profile**（新建憑證設定檔）以建立新的設定檔。選取 **None**（無）以移除憑證設定檔。

通訊設定

- Panorama > 受管理的收集器 > 通訊

若要在日誌收集器與 Panorama、防火牆和其他日誌收集器之間設定自訂憑證型驗證，請依照下表中的說明進行設定。

通訊設定	說明
安全伺服器通訊—啟用 **Secure Server Communication**（安全伺服器通訊），可對連線至日誌收集器的用戶端設備進行識別驗證。	
SSL/TLS 服務設定檔	從下拉式清單中選取 SSL/TLS 服務設定檔。此設定檔會定義日誌收集器所提供的憑證，並指定與日誌收集器之間的通訊可接受的 SSL/TLS 版本範圍。
憑證設定檔	從下拉式清單中選取憑證設定檔。此憑證設定檔會定義憑證撤銷檢查行為，以及用來對用戶端提供的憑證鏈進行驗證的根 CA。
僅限自訂憑證	此選項啟用時，日誌收集器僅接受以自訂憑證進行對受管理的防火牆和日誌收集器的驗證。
根據序號驗證用戶端	日誌收集器會根據用戶端設備序號的雜湊授權給這些設備。
檢查驗證清單	連線至此日誌收集器的用戶端設備或設備群組，會依據授權清單受到檢查。
中斷連線等候時間（分鐘）	日誌收集器在中斷目前與其受管理設備間的連線之前所等候的時間量。接著，日誌收集器會使用已設定的安全伺服器通訊設定，重新建立與其受管理設備間的連線。等候時間從認可安全伺服器通訊設定後起算。
授權清單	授權清單—選取新增並完成下列欄位，以設定準則。 • 識別碼 —選取 **Subject**（主體）或 **Subject Alt.**（主體別名）。作為驗證識別碼的名稱 。 • 類型—如果為主體別名。若要選取名稱為識別碼，請選取 **IP**、**Hostname**（主機名稱）或 **E-mail**（電子郵件）作為識別碼類型。如果選取主體，則會以通用名稱作為識別碼類型。 • **Value**（值）—輸入識別碼值。

© 2019 Palo Alto Networks, Inc.

通訊設定	說明
安全用戶端通訊—啟用 **Secure Client Communication**（安全用戶端通訊），可確保會使用指定的用戶端憑證透過 Panorama、防火牆或其他日誌收集器的 SSL 連線來驗證日誌收集器。	
憑證類型	選取用來保護通訊的設備憑證類型（無、本機或 SCEP）
無	如果選取 **None**（無），則不會設定設備憑證，且不會使用安全用戶端通訊。這是預設選取項目。
本地	日誌收集器會使用本機設備憑證，以及在日誌收集器上產生或從現有企業 PKI 伺服器匯入的私密金鑰。
	憑證—選取本機裝置憑證。此憑證可以是防火牆上的唯一憑證（根據日誌收集器序號的雜湊），或是所有連線至 Panorama 的日誌收集器所使用的通用設備憑證。
	憑證設定檔—從下拉式清單中選取憑證設定檔。此憑證設定檔會用來定義日誌收集器的伺服器驗證。
SCEP	日誌收集器會使用簡易憑證註冊通訊協定 (SCEP) 伺服器所產生的設備憑證和私密金鑰。
	SCEP 設定檔—從下拉式清單中選取 SCEP 設定檔。
	憑證設定檔—從下拉式清單中選取憑證設定檔。此憑證設定檔會用來定義日誌收集器的伺服器驗證。
檢查伺服器識別	用戶端設備會比對通用名稱 (CN) 與伺服器的 IP 位址或 FQDN，以確認伺服器的識別。

專用日誌收集器的軟體更新

- Panorama > 受管理的收集器

若要在專用日誌收集器上安裝軟體影像，請下載影像或將影像上載至 Panorama（請參閱 [Panorama > 設備部署]），然後按一下 **Install**（安裝），並完成下列欄位。

由於 *Panorama* 管理伺服器與本機預設日誌收集器共用作業系統，因此當您在 *Panorama* 管理伺服器上安裝軟體更新時，會更新兩者（請參閱 *[Panorama > 軟體]*）。

針對專用日誌收集器，您也可以選取 *Panorama > Device Deployment*（設備部署）> *Software*（軟體）以安裝更新（請參閱管理軟體和內容更新）。

若要減少管理 *(MGT)* 介面上的流量，您可以將 *Panorama* 設定為使用不同介面來部署更新（請參閱 Panorama > 設定 > 介面*)*。

在日誌收集器上安裝軟體更新的欄位	說明
檔案	選取已下載或已上載的軟體影像。
裝置	選取要安裝軟體的日誌收集器。對話方塊顯示每個日誌收集器的下列資訊： • 設備名稱—專用日誌收集器的名稱。

© 2019 Palo Alto Networks, Inc.

在日誌收集器上安裝軟體更新的欄位	說明
	• 目前版本—目前安裝於日誌收集器上的 Panorama 軟體版本。 • HA Status（HA 狀態）**HA** 狀態—此欄不會套用至日誌收集器。專用日誌收集器不支援高可用性。
已選取篩選器	若要僅顯示特定日誌收集器，請選取日誌收集器，然後選取 **Filter Selected**（已選取篩選器）。
僅上載至設備（不要安裝）	選取此選項可上載軟體至日誌收集器，而不會自動重新啟動。在您登入日誌收集器 CLI 並執行 **`request restart system`** 操作命令而以手動方式重新啟動之前，不會安裝此影像。
安裝後重新啟動設備	選取以上載並自動安裝軟體。安裝程序將重新啟動日誌收集器。

© 2019 Palo Alto Networks, Inc.

Panorama > 收集器群組

每個收集器群組可擁有最多 16 個日誌收集器，您可向其指派防火牆來轉送日誌。您接著可使用 Panorama 來查詢日誌收集器，以進行彙總日誌檢視和調查。

名稱為預設的預先定義收集器群組包含預先定義的日誌收集器，其位於 *Panorama* 管理伺服器的本機上。

- 收集器群組設定
- 收集器群組資訊

收集器群組設定

若要設定收集器群組，請按一下 **Add**（新增）並完成下列欄位。

收集器群組設定	設定位置	說明
名稱	**Panorama** > **Collector Groups**（收集器群組）> **General**（一般）	輸入用來識別此收集器群組的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
日誌儲存空間		指出收集器群組接收的防火牆日誌儲存配額總計，以及可用空間。 按一下儲存配額連結，可設定下列日誌類型的儲存 **Quota(%)**（配額 (%)）和到期期間（**Max Days**（天數上限））： • **Detailed Firewall Logs**（詳細防火牆日誌）—包含 **Device**（裝置）> **Setup**（設定）> **Logging and Reporting Settings**（記錄和報告設定）中的所有日誌類型，例如流量、威脅、HIP 比對、動態註冊的 IP 位址（IP 頁籤）、延伸 PCAP、GTP 和通道、應用程式統計資料等。 • **Summary Firewall Logs**（摘要防火牆日誌）—包含 **Device**（裝置）> **Setup**（設定）> **Logging and Reporting Settings**（記錄和報告設定）中的所有摘要日誌，例如流量摘要、威脅摘要、URL 摘要，以及 GTP 和通道摘要。 • **Infrastructure and Audit Logs**（基礎結構和稽核日誌）—包含設定、系統、User-ID 和驗證日誌。 • **Palo Alto Networks Platform Logs**（**Palo Alto Networks** 平台日誌）—包含 Traps 和其他 Palo Alto Networks 產品所產生的日誌。 • **3rd Party External Logs**（第三方外部日誌）—包含 Palo Alto Networks 提供的其他廠商整合所產生的日誌。 若要使用預設設定，請按一下 **Restore Defaults**（還原預設值）。
最小保留期間（天數）		輸入 Panorama 在收集器群組的所有日誌收集器中保留的最小日誌保留期間（1-2,000）。目前的日期減去最舊日誌的

© 2019 Palo Alto Networks, Inc.

收集器群組設定	設定位置	說明
		日期後若小於定義的保留期間下限時，Panorama 便會產生作為警示違規的系統日誌。
收集器群組成員		**Add**（新增）將屬於此收集器群組的日誌收集器（最多 16 個）。您可以新增 **Panorama** > **Managed Collectors**（受管理的收集器）頁面中提供的任何日誌收集器。任何特定收集器群組的所有日誌收集器都必須屬於相同型號：例如，全部是 M-500 裝置，或全部是 Panorama 虛擬裝置。 將日誌收集器新增至現有收集器群組後，*Panorama* 會重新分配所有日誌收集器中的現有日誌，每 *TB* 的日誌可能會花費數小時。重新分配程序期間會降低最大日誌記錄速率。在 *Panorama* > *Collector Groups*（收集器群組）頁面中，*Log Redistribution State*（日誌重新散佈狀態）欄會以百分比指出程序的完成狀態。
在收集器上啟用日誌備援		如果您選取此選項，收集器群組中的每個日誌都會具有兩個複本，且每個複本都會位於不同的日誌收集器。此備援可確保如果任何日誌收集器無法使用，您仍不會遺失任何日誌：您可以看到所有轉寄至收集器群組的日誌，並針對所有日誌資料執行報告。如果收集器群組具有多個日誌收集器，且每個日誌收集器都具有相同的磁碟數，才能使用日誌備援。 在 **Panorama** > **Collector Groups**（收集器群組）頁面中，Log Redistribution State（日誌重新散佈狀態）欄會以百分比指出程序的完成狀態。任何特定收集器群組的所有日誌收集器都必須屬於相同型號：例如，全部是 M-500 裝置，或全部是 Panorama 虛擬裝置。 由於啟用備援會建立更多日誌，因此此設定需要更多儲存容量。由於每個日誌收集器都必須散佈每個接收的日誌複本，因此啟用備援會讓收集器群組中的日誌處理流量加倍，並讓最大日誌記錄速率減半。（收集器群組空間用盡時，其會刪除較舊的日誌。）
轉送至偏好設定清單中的全部收集器		（僅適用於 PA-5200 Series 和 PA-7000 Series 防火牆）選取此選項，可將日誌傳送至偏好設定清單中的每個日誌收集器。Panorama 會使用循環配置資源負載平衡選取哪個日誌收集器會在任何給定的時間接收日誌。此選項預設為停用：防火牆只會將日誌傳送至清單中的第一個日誌收集器，除非該日誌收集器無法使用（請參閱裝置/收集器）。
啟用安全性 Inter Lc 通訊		啟用在收集器群組中日誌收集器間相互 SSL 認證的自訂憑證。
位置	**Panorama** > **Collector Groups**（收集器群組）> **Monitoring**（監控）	指定收集器群組的位置。

© 2019 Palo Alto Networks, Inc.

收集器群組設定	設定位置	說明
聯絡人		指定電子郵件聯絡人（例如監控日誌收集器的 SNMP 管理員的電子郵件地址）。
版本		指定用於與 Panorama 管理伺服器通訊的 SNMP 版本：**V2c** 或 **V3**。 SNMP 可讓您收集日誌收集器的相關資訊，包括連線狀態、磁碟機統計資料、軟體版本、平均 CPU 使用情況、平均日誌/秒，和每種日誌類型的儲存期間。您可以每個收集器群組為基礎，取得 SNMP 資訊。
SNMP 社群字串（僅限 V2c）		輸入 **SNMP Community String**（SNMP 社群子串），以便識別 SNMP 管理員與受監社群和受監控裝置（在此情況下為日誌收集器），同時作為密碼對社群成員進行彼此驗證。 請勿使用預設社群字串 *public*；此字串廣為人知，因此不具有安全性。
檢視（僅限 V3）		**Add**（新增）一組 SNMP 檢視，然後在 **Views**（檢視）中輸入該群組的名稱。 每個檢視有一組配對的物件識別碼 (OID) 和 Bitwise 遮罩：OID 會指定一個受管理資訊庫 (MIB)，而遮罩（使用十六進位格式）會指定在 MIB 之中（包含相符）或之外（排除相符）的可存取 SNMP 物件。 對於群組中的每個檢視，請 **Add**（新增）下列設定： • **View**（檢視）—輸入檢視的名稱。 • **OID** — 輸入 OID。 • **Option**（選項）（包含或排除）—選取檢視是否排除或包含 OID。 • **Mask**（遮罩）—為 OID 上的篩選指定遮罩值（例如 0xf0）。
使用者（僅限 V3）		為每個 SNMP 使用者 **Add**（新增）下列設定： • **Users**（使用者）—輸入使用者名稱，以驗證 SNMP 管理員使用者。 • **View**（檢視）—選取使用者的檢視群組。 • **Authpwd**（驗證密碼）—輸入用來向 SNMP 管理員驗證使用者的密碼（最少八個字元）。僅支援安全雜湊演算法 (SHA)，用於對密碼加密。 • **Privpwd**（私人密碼）—輸入用來對 SNMP 管理員的 SNMP 訊息進行加密的私人密碼（最少八個字元）。僅支援進階加密標準 (AES)。
裝置/收集器	**Panorama** > **Collector Groups**（收集器群組）> **Device Log Forwarding**（裝置日誌轉送）	日誌轉送偏好設定清單可控制哪些防火牆可將日誌轉送至哪些日誌收集器。對於 **Add**（新增）至清單的每個項目，您可以 **Modify**（修改）裝置清單以指派一或多個防火牆，也可在收集器清單中 **Add**（新增）一或多個日誌收集器。

© 2019 Palo Alto Networks, Inc.

收集器群組設定	設定位置	說明
		根據預設，您在清單項目中指派的防火牆只會將日誌傳送至主要（第一個）日誌收集器（只要該收集器是可用的）。如果主要日誌收集器失敗，防火牆會將日誌傳送至次要日誌收集器。如果次要日誌收集器失敗，則防火牆會將日誌傳送至第三日誌收集器，依此類推。若要變更順序，請選取日誌收集器，並按一下 **Move Up**（上移）或 **Move Down**（下移）。 您可以在 *General*（一般）頁籤中選取轉送至偏好設定清單中的所有收集器，以取代 *PA-5200 Series* 和 *PA-7000 Series* 的預設日誌轉送行為。

系統
組態設定
HIP 比對
流量
威脅
WildFire
關聯
GTP
驗證
使用者-ID
通道
IP-Tag
	Panorama > **Collector Groups**（收集器群組）> **Collector Log Forwarding**（收集器日誌轉送）	對於要從這個收集器群組轉送至外部服務的各類防火牆日誌，您可以 **Add**（新增）一或多個比對清單設定檔。這些設定檔會指定所要轉送的日誌，以及目的地伺服器。請針對每個設定檔完成下列設定：
		
		• **Name**（名稱）—輸入用來識別比對清單設定檔的名稱（最多 31 個字元）。
		• **Filter**（篩選器）—根據預設，防火牆會轉送套用此比對清單設定檔之類型的 **All Logs**（所有日誌）。若要轉送日誌子集，請選取現有的篩選器，或選取 **Filter Builder**（篩選器建立器）以新增篩選器。針對新篩選器中的各個查詢，指定下列欄位並 **Add**（新增）查詢：
		  • **Connector**（連接器）—選取連接器邏輯 (and/or)。如果您要套用否定，請選取 **Negate**（否定）。例如，若要避免從不受信任的區域轉送日誌，請選取 **Negate**（否定）、選取 **Zone**（區域）屬性、選取 **equal** 運算子，然後在 [值] 欄中輸入不受信任的區域名稱。
		  • 屬性—選取日誌屬性。選項會依日誌類型而異。
		  • **Operator**（運算子）—選取決定如何套用屬性的準則（例如 **equal**）。選項會依日誌類型而異。
		  • 值—指定要比對的屬性值。
		
		若要顯示或匯出 篩選器比對的日誌，請選取 **View Filtered Logs**（檢視篩選的日誌）。此頁籤提供與 **Monitoring**（監控）頁籤頁面相同的選項（例如 **Monitoring**（監控）> **Logs**（日誌）> **Traffic**（流量））。
		
		• **Description**（說明）—輸入不超過 1,023 個字元的說明，用以解釋此比對清單設定檔的用途。
		• 目的地伺服器—對於每個伺服器類型，您可以 **Add**（新增）一或多個伺服器設定檔。若要設定伺服器設定檔，請參閱 [裝置 > 伺服器設定檔 > SNMP 設陷]、[裝置 > 伺服器設定檔 > Syslog]、[裝置 > 伺服器設定檔 > 電子郵件] 或 [裝置 > 伺服器設定檔 > HTTP]。
		• 內建動作—您可以為 [系統] 和 [設定] 日誌以外的所有日誌類型 **Add**（新增）動作：
		  • 為 **Action**（動作）輸入描述性名稱。

© 2019 Palo Alto Networks, Inc.

收集器群組設定	設定位置	說明
		• 選取您要標記的 IP 位址—**Source Address**（來源位址）或 **Destination Address**（目的地位址）。您只可以標記關聯日誌和 HIP 比對日誌中的來源 IP 位址。 • 選取動作—**Add Tag**（新增頁籤）或 **Remove Tag**（移除頁籤）。 • 選取要將頁籤註冊至此 Panorama 上的本機 User-ID 代理程式，或是遠端 User-ID 代理程式。 若要將頁籤註冊至 **Remote device User-ID Agent**（遠端裝置 **User-ID** 代理程式），請選取將啟用轉送的 HTTP 伺服器設定檔。 • 設定 IP-Tag **Timeout**（逾時）以設定 IP 位址到頁籤對應維護的時間。將逾時設定為 0 代表著 IP-Tag 對應不會逾時（範圍為 0 到 43200（30 天）；預設值為 0）。 您只能使用 *Add Tag*（新增頁籤）動作設定連線逾時。 • 輸入或選取您要套用或從目標來源或目的地 IP 位址移除的 **Tags**（頁籤）。
擷取設定檔	**Panorama** > **Collector Groups**（收集器群組）> **Log Ingestion**（日誌擷取）	**Add**（新增）一或多個可讓 Panorama 從 Traps ESM 伺服器接收日誌的日誌擷取設定檔。若要設定新的日誌擷取設定檔，請參閱 [Panorama > 日誌擷取設定檔]。

收集器群組資訊

選取 **Panorama** > **Collector Groups**（收集器群組），可顯示收集器群組的下列資訊。在您完成日誌收集器設定後，將可設定其他欄位。

收集器群組資訊	說明
名稱	用於識別收集器群組的名稱。
已啟用備援	表示是否已為收集器群組啟用日誌備援。完成或修改日誌收集器設定後，您可以為收集器群組啟用日誌備援。
收集器	將日誌收集器指派給收集器群組。
日誌重新散佈狀態	某些動作（例如，啟用日誌備援）會導致收集器群組重新分配其日誌收集器中的日誌。此欄以百分比表示重新分配程序中的完成狀態。

© 2019 Palo Alto Networks, Inc.

Panorama > Plugins（Panorama > 外掛程式）

- **Panorama** > 外掛程式
- **Device**（裝置）> **Plugins**（外掛程式）

選取 **Panorama** > **Plugins**（外掛程式）以安裝、移除和管理支援 Panorama 上第三方整合的外掛程式。

（僅在 VM 系列防火牆提供）選取 **Device**（裝置）> **Plugins**（外掛程式）以安裝、移除和管理 VM 系列防火牆的外掛程式。

外掛程式	說明
上傳	讓您可從本機目錄上傳外掛程式安裝檔案。這不會安裝外掛程式。上傳安裝檔案後，安裝連結會成為作用中。
檔案名稱	外掛程式檔案名稱。 當您在 Panorama 上安裝 **vm_series**（**vm** 系列）外掛程式時，可以使用 **Device**（裝置）> **VM-Series**（**vm** 系列）頁面在公共雲端的環境（AWS、Azure 和 Google）上部署的 VM 系列防火牆上管理和提交範本組態。
版本	外掛程式版本號碼。
平台	支援外掛程式的型號。
發行日期	此版本外掛程式的發行日期。
大小	外掛程式檔案大小。
已安裝	提供 Panorama 上各個外掛程式的目前安裝狀態。
動作	• **Install**（安裝）—安裝外掛程式的指定版本。新版本的安裝外掛程式會取代先前安裝的版本。 • **Delete**（刪除）—刪除指定的外掛程式檔案。 • **Remove Config**（移除設定）—移除與外掛程式相關的所有組態。若要完全移除與外掛程式相關的所有設定，您還必須在使用 **Remove Config**（移除設定）之後執行並 **Uninstall**（解除安裝）。 • **Uninstall**（解除安裝）—移除外掛程式的目前安裝。這不會從 Panorama 移除外掛程式檔案。若您解除安裝外掛程式，則您會遺失任何與外掛程式相關的組態。僅在完全移除相關組態時使用。

© 2019 Palo Alto Networks, Inc.

Panorama > SD-WAN

下載並安裝 Panorama SD-WAN 外掛程式以集中管理、監控和產生報告。透過將分支新增並關聯至其適當的中樞，以及將這些分支和中樞裝置關聯至適當區域，來從 Panorama 設定 SD-WAN 拓撲。設定 SD-WAN 拓撲後，即可監控所有設定裝置和路徑的路徑健康情況指標，以隔離應用程式和連結問題，以及了解一段時間後的連結效能。此外，您可以產生報告以進行稽核。

您想進行什麼操作？	請參閱：
新增、編輯或刪除分支和中樞裝置	SD-WAN 裝置
新增、編輯或刪除 VPN 叢集	SD-WAN VPN 叢集
監控路徑健康情況	SD-WAN 監控
產生健康情況報告	SD-WAN 報告

SD-WAN 裝置

- **Panorama** > **SD-WAN** > **Devices**（裝置）

SD-WAN 裝置是組成您的 VPN 叢集和 SD-WAN 拓撲的分支或中樞。

欄位	說明
名稱	輸入識別 SD-WAN 裝置的名稱。
類型	選取 SD-WAN 裝置的類型： • **Hub**（中樞）—部署在主要辦公室或位置（例如資料中心或企業總部）的集中式防火牆，所有分支裝置均使用 VPN 連線來進行連接。分支之間的流量先通過中樞，再繼續到達目標分支。分支連線至中樞，以存取中樞位置的集中式資源。中樞裝置處理流量，執行原則規則，並管理主要辦公室或位置的連結交換。 • **Branch**（分支）—部署在實體分支位置的防火牆，使用 VPN 連線與中樞連線，並提供分支層級的安全性。分支連線至中樞以存取集中式資源。分支裝置處理流量，執行政策規則，並管理分支位置的連結交換。
虛擬路由器名稱	選取用於在 SD-WAN 中樞和分支之間進行路由的虛擬路由器。預設情況下，會建立一個 `sdwan-default` 虛擬路由器，並啟用 Panorama 以自動推送路由器組態。
站台	輸入使用者易記的站台名稱，用於識別中樞或分支。例如，輸入部署分支裝置所在的城市名稱。
連結標籤	（PAN-OS 10.0.3 和更新版本的 10.0 版本）對於中樞，選取為中樞虛擬介面建立的「連結標籤」，以便中樞可以參與 DIA AnyPath。Auto VPN 將此連結標籤套用至整個中樞虛擬介面，而非個別連結。您在「流量散佈設定檔」中引用此「連結標籤」，以指示容錯移轉至該中樞虛擬介面的順序。在分支裝置上，Auto VPN 使用此標籤在終止於中樞裝置的 SD-WAN 虛擬介面上填入「連結標籤」欄位。
區域網際網路	**Add**（新增）一個或多個安全性區域，以識別往返不信任來源的流量。

© 2019 Palo Alto Networks, Inc.

欄位	說明
區域中樞	**Add**（新增）一個或多個安全性區域，以識別往返 SD-WAN 中樞裝置的流量。
區域分支	**Add**（新增）一個或多個安全性區域，以識別往返 SD-WAN 分支裝置的流量。
內部區域	**Add**（新增）一個或多個安全性區域，以識別往返企業網路上受信任裝置的流量。
路由器 ID	指定 BGP 路由器 ID。邊界閘道通訊協定 (BGP) 路由器 ID 在所有路由器之間必須是唯一的。 使用回送位址作為路由器 *ID*。
回送位址	為 BGP 對等指定靜態回送 IPv4 位址。
AS 編號	輸入自發系統編號，以定義到網際網路的常用路由政策。AS 編號對於每個中樞和分支位置必須是唯一的。 使用 *4* 位元組的私人 *BGP AS* 編號，以不干擾任何可公開路由的 *AS* 編號。
重新散佈設定檔名稱	選取或建立重新散佈設定檔，以控制將哪些本機前置詞從分支傳遞至中樞路由器。依預設，所有本機連線的網際網路前置詞都會公告至中樞位置。 *Palo Alto Networks* 不會重新散佈從 *ISP* 處獲取的分公司預設路由。

SD-WAN VPN 叢集

- **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN 叢集**）

將 SD-WAN 分支裝置與一個或多個 SD-WAN 中樞裝置關聯，以允許分支和中樞位置之間進行安全通訊。當您在 SD-WAN VPN 叢集中關聯分支和中樞裝置時，防火牆會根據您指定的 VPN 叢集類型，在站台之間建立所需的 IKE 和 IPSec VPN 連線。

欄位	說明
名稱	輸入用於識別 VPN 叢集的名稱。
類型	選取 SD-WAN VPN 叢集的類型： • **Hub Spoke**（中樞支點）—SD-WAN 拓撲，其中主要辦公室或位置的集中式防火牆充當使用 VPN 連線進行連接的分支裝置間的閘道。分支之間的流量先通過中樞，再繼續到達目標分支。
分支	**Add**（新增）一個或多個分支裝置，以便與一個或多個中樞關聯。
中樞	**Add**（新增）一個或多個中樞裝置，以便與一個或多個分支裝置關聯。如果新增多個中樞，則使用路徑健康情況品質指標來控制哪個是主要中樞，哪些是次要中樞。

© 2019 Palo Alto Networks, Inc.

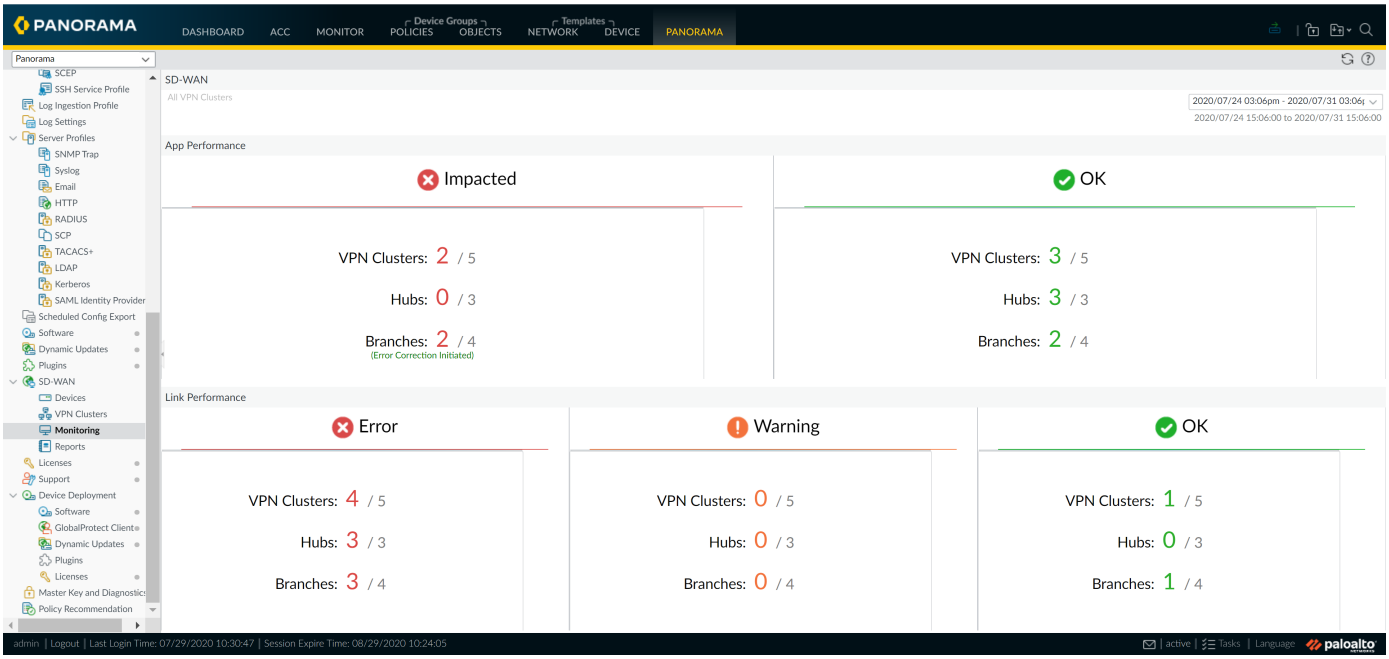
SD-WAN 監控

- **Panorama** > **SD-WAN** > **Monitoring**（監控）

「監控」頁籤是一個儀表板，顯示所有 SD-WAN 裝置健康情況指標的摘要 Widget。此工具提供有關 SD-WAN 網路活動的可操作情報，可讓您快速識別引起效能問題的應用程式或連結。您可以在指定時間段內檢視所有 VPN 叢集或特定 VPN 叢集的路徑品質和連結效能。

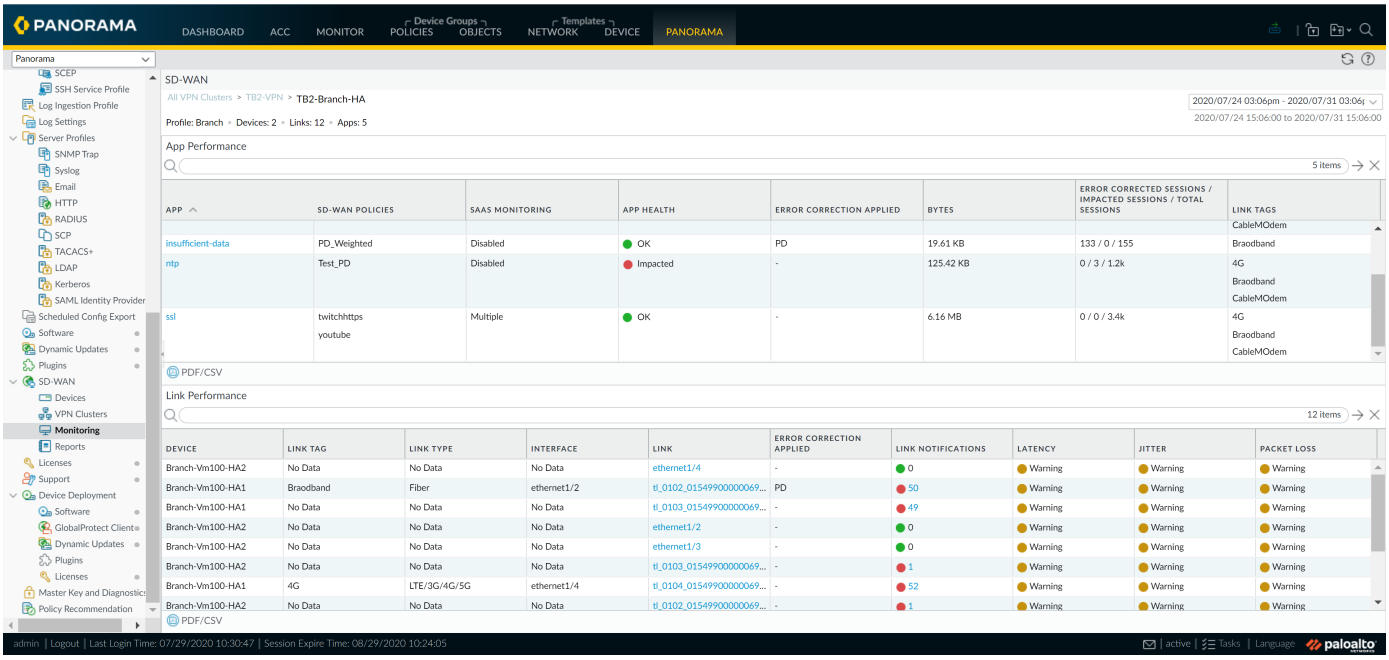
您可以一目了然地檢視具有以下內容的 VPN 叢集的總數：應用程式效能受到影響的分支或中樞防火牆，以及運作狀態良好的分支或中樞防火牆。您可以檢視以下 VPN 叢集的應用程式和連結健康情況狀態：

- 應用程式效能
  - **Impacted**（受影響）—VPN 叢集中的一個或多個應用程式，對於這些應用程式，在可選擇的路徑清單中，沒有任何路徑的抖動、延遲或封包遺失效能滿足或低於路徑品質設定檔中指定的閾值。
  - **OK**（正常）—VPN 叢集中的應用程式運作狀態良好，並且沒有抖動、延遲或封包遺失效能。
- 連結效能
  - **Error**（錯誤）—VPN 叢集中的一個或多個站台，對於這些站台，在可選擇的路徑清單中，沒有任何路徑的抖動、延遲或封包遺失效能滿足或低於路徑品質設定檔中指定的閾值。
  - **Warning**（警告）—VPN 叢集中的一個或多個站台的連結具有抖動、延遲或封包遺失效能測量，與指標的七天移動平均值相比不利。
  - **OK**（正常）—VPN 叢集中的連結運作狀態良好，並且沒有抖動、延遲或封包遺失效能。



按一下任何 Widget，以獲取所需健康情況狀態的所有 VPN 叢集的深入檢視。此外，您可以使用站台篩選器可基於連結通知、延遲偏差、抖動偏差、封包遺失偏差或受影響的應用程式檢視 VPN 叢集。

© 2019 Palo Alto Networks, Inc.



SD-WAN 報告

- **Panorama** > **SD-WAN** > **Reports**（報告）

針對在指定時段內健康情況下降頻率最高的前幾大應用程式或連結，產生應用程式或連結效能報告，以便進行稽核。設定報告後，必須 **Run Now**（立即執行）以便檢視報告。可以匯出報告 功能目前不起作用。可以採用哪種格式來匯出報告？

欄位	說明
名稱	輸入識別報告用途的名稱。
報告類型	選取要執行的報告類型： • **App Performance**（新增效能）—產生報告，詳細說明 SD-WAN 中所有應用程式流量的健康情況指標。 • **Link Performance**（連結效能）—產生報告，詳細說明 SD-WAN 中跨連結流量的健康情況指標。
叢集	從下拉式清單中，選取要為其產生報告的叢集。預設會選取 **all**（全部）。
站台	從下拉式清單中，選取要為其產生報告的站台。預設會選取 **all**（全部）。 如果為叢集選取 **all**（全部），則必須為歸類於叢集的所有站台產生報告。如果選取了特定叢集，則可以選取要為其產生報告的特定站台。
應用程式（僅限應用程式效能報告類型）	從下拉式清單中，選取要為其產生報告的應用程式。預設會選取 **all**（全部）。 如果為站台選取了 **all**（全部），則必須為歸類於該站台的所有應用程式產生報告。如果選取了特定站台，則可以選取要為其產生報告的特定應用程式。
連結標籤（僅限連結效能報告類型）	從下拉式清單中，選取要為其產生報告的連結標籤。預設會選取 **all**（全部）。

© 2019 Palo Alto Networks, Inc.

欄位	說明
	如果為站台選取了 **all**（全部），則必須為在站台下建立的所有連結標籤產生報告。如果選取了特定站台，則可以選取要為其產生報告的特定連結標籤。
連結類型（僅限連結效能報告類型）	從下拉式清單中，選取要為其產生報告的連結類型。預設會選取 **all**（全部）。 如果為連結標籤選取了 **all**（全部），則必須為在連結標籤下建立的所有連結類型產生報告。如果選取了特定連結標籤，則可以選取要為其產生報告的特定連結類型。
前 N 個	指定要包含在報告中的應用程式或連結數量。您可以選取報告包含前 5 個、10 個、25 個、50 個、100 個、250 個、500 個或 1000 個執行中應用程式或連結。預設會選取 **5**。
時段	設定執行報告的時段。預設會選取 **None**（無），這會使用所有應用程式和連結效能資料來產生報告。

© 2019 Palo Alto Networks, Inc.

Panorama > VMware NSX

若要自動化佈建 VM 系列 NSX 版本防火牆，您必須啟用 NSX Manager 與 Panorama 之間的通訊。當 Panorama 將 VM 系列防火牆註冊為 NSX Manager 上的服務時，NSX Manager 具備必要的組態設定，可讓您在叢集中每台 ESX(i) 主機上佈建新一個或多個的 VM 系列防火牆的實例。

您想了解什麼內容？	請參閱：
如何設定通知群組？	設定通知群組
如何定義 VM 系統 NSX 版防火牆的組態？	建立服務定義
如何設定 Panorama 與 NSX Manager 間的通訊？	設定對 NSX Manager 的存取
如何定義 VM-Series NSX 版本防火牆的導向規則？	建立導向規則
如何設定防火牆以在動態 vSphere 環境中一貫執行政策？	選取[物件 > 位址群組] 和 [政策 > 安全性] 若要啟用 Panorama 與防火牆，以學習虛擬環境中的變更，請使用動態位址群組作為安全性政策預先規則中的來源與目的地位址物件。
想知道更多？	請參閱設定 VM-Series NSX 版本防火牆

設定通知群組

- Panorama > 通知群組

下表說明 Panorama 通知群組設定。

通知群組設定	說明
名稱	為您的通知群組輸入說明性名稱。
通知設備	核取對網路上部署的虛擬機器進行新增或修改時，必須通知之設備群組的方塊。 佈建新的虛擬電腦或修改現有電腦時，會將虛擬網路中的變更作為 Panorama 更新提供。若進行此設定，Panorama 將填入並更新政策規則參考的動態位址物件，以便指定設備群組中的防火牆接收動態位址群組中註冊的 IP 位址的變更。 若要啟用通知，請確保選取每一個您想要啟用通知的設備群組。如果您無法選取設備群組（核取方塊不可用），這表示設備群組將自動包含於設備群組階層。 此通知程序會在網路上建立內容感知及維護應用程式安全性。例如，如果您在部署新應用程式或網頁伺服器時，必須通知硬體式的周邊防火牆群組，則此程序會針對指定的設備群組啟動動態位址群組的自動重新整理。此外，參照動態位址物件的所有政策規則現在都會自動包含最近部署或修改的任何應用程式或網頁伺服器，並可依據您的準則安全地啟用。

© 2019 Palo Alto Networks, Inc.

建立服務定義

- Panorama > VMware NSX > 服務定義

服務定義可讓您在 NSX Manager 上將 VM-Series 防火牆註冊為合作夥伴安全性服務。您可在 Panorama 上定義最多 32 項服務定義，並在 NSX Manager 上同步定義。

通常，您將為 ESXi 叢集中的每個租用戶建立一項服務定義。每項服務定義指定用於部署防火牆的 OVF（PAN-OS 版），並包含安裝在 ESXi 叢集上的 VM 系統防火牆的組態。若要指定組態，服務定義必須擁有唯一的範本、唯一的設備群組以及將要使用服務定義部署之防火牆的授權驗證碼。防火牆部署完畢後，它將連線至 Panorama 並接收其組態設定（包括防火牆將保障的每個租用戶或部門的區域）以及在服務定義中指定之設備群組的政策定義。

若要新增服務定義，請依照下表所述進行設定。

欄位	說明
名稱	輸入您想要在 NSX Manager 上顯示之服務的名稱。
說明	（選用）輸入頁籤來說明此服務定義的目的或功能。
裝置群組	選取要將這些 VM 系列防火牆指派給哪個設備群組或設備群組階層。如需詳細資訊，請參閱 [Panorama > VMware NSX]。
範本	選取要將 VM 系列防火牆指派給哪個範本。如需詳細資訊，請參閱 [Panorama > 範本]。 每個服務定義必須指派給唯一的範本或範本堆疊。 一個範本可以有多個相關聯的區域（NSX 的 NSX 服務設定檔區域）。對於單一租用戶部署，請在範本中建立一個區域（NSX 服務設定檔區域）。如果您擁有多租用戶部署，請為每個子租用戶建立區域。 當您建立新 NSX 服務設定檔區域後，將會自動附加至一對 Virtual Wire 子介面。如需詳細資訊，請參閱 [網路 > 區域]。
VM 系列 OVF URL	輸入 URL（IP 位址或主機名稱和路徑），供 NSX Manager 存取 OVF 檔案以佈建新 VM 系列防火牆。
通知群組	從下拉式清單中選取通知群組。

設定對 NSX Manager 的存取

- Panorama > VMware NSX > 服務管理員

若要讓 Panorama 能夠與 NSX Manager 通訊，請依照下表所述 **Add**（新增）設定並加以設定。

服務管理員	說明
服務管理員名稱	輸入名稱以識別做為服務的 VM-Series 防火牆。此名稱會顯示在 NSX Manager 上，並可視需要用於部署 VM 系列防火牆。 支援最多 63 個字元；僅使用字母、數字、連字號和底線。
說明	（選用）輸入標籤來說明此服務的目的或功能。

© 2019 Palo Alto Networks, Inc.

服務管理員	說明
NSX Manager URL	指定 Panorama 將用於建立 NSX Manager 連線的 URL。
NSX Manager 登入	輸入在 NSX Manager 上設定的驗證認證，即使用者名稱和密碼。Panorama 使用這些認證來驗證 NSX Manager。
NSX Manager 密碼	
確認 NSX 管理員密碼	
服務定義	指定與此服務管理員相關聯的服務定義。每個服務管理員最多可支援 32 個服務定義。

對 Panorama 認可變更後，VMware 服務管理員視窗會顯示 Panorama 與 NSX Manager 之間的連線狀態。

同步狀態	說明
STATUS (狀態)	顯示 Panorama 與 NSX Manager 之間的連線狀態。 成功連線顯示為已註冊—Panorama 和 NSX Manager 已同步，並且將 VM-Series 防火牆註冊為 NSX Manager 上的服務。 對於未成功連線，狀態可能是： • 連線錯誤 — 無法連線/建立與 NSX 管理員的網路連線。 • 未驗證—存取認證（使用者名稱及/或密碼）不正確。 • 未註冊 — 服務管理員、服務定義或服務設定檔無法使用，或已在 NSX Manager 上刪除。 • 非同步 — Panorama 上定義的組態設定不同於 NSX 管理員上定義的組態設定。按一下 **Out of sync**（非同步），瞭解失敗原因詳細資訊。例如，NSX 管理員可能具有與 Panorama 上定義的之名稱相同的定義。若要修正錯誤，請使用錯誤訊息上列示之服務定義來驗證 NSX 管理員上的服務定義。在 Panorama 與 NSX 管理員上的組態同步之前，您無法在 Panorama 上新增新服務定義。
同步處理動態物件	按一下 **Synchronize Dynamic Objects**（同步處理動態物件）可重新整理 NSX 管理員的動態物件資訊。同步處理動態物件可讓您在虛擬環境中維護變更內容，並可讓您自動更新政策規則中使用的動態位址群組，以便安全地啟用應用程式。 在 *Panorama* 上，您只能檢視從 *NSX Manager* 中動態註冊的 *IP* 位址。*Panorama* 不會顯示直接登錄到防火牆的動態 *IP* 位址。如果您使用 *VM* 資訊來源（在 *VM* 系列 *NSX* 版防火牆上不受支援）或 *XML API* 將 *IP* 位址動態註冊到防火牆，則您必須登入到每個防火牆，才能檢視從防火牆上的完整動態 *IP* 位址（*Panorama* 推送及在本機註冊）清單。
NSX 組態同步	選取 **NSX Config-Sync**（**NSX** 設定同步），可同步處理在 Panorama 上設定的服務定義與 NSX Manager。如果在 Panorama 上有任何擱置提交，則此選項不可用。 如果同步失敗，請檢視錯誤訊息中的詳細資訊，以瞭解錯誤是在 Panorama 上還是 NSX Manager 上。例如，當您刪除 Panorama 上的服務定義時，如果服務定義參照 NSX

© 2019 Palo Alto Networks, Inc.

同步狀態	說明
	Manager 上的規則，則與 NSX Manager 的同步將會失敗。使用錯誤訊息資訊可確定失敗原因，以及您需要採取修正動作的情況（在 Panorama 或在 NSX Manager 上）。

建立導向規則

- Panorama > VMware NSX > 導向規則

導向規則可決定叢集中的哪些來賓所傳入的何種流量會導向至 VM-Series 防火牆。

欄位	說明
自動產生導向規則	根據設定如下的安全性規則產生導向規則： • 屬於註冊至 NSX 服務管理員的父系或子系裝置群組。 • 具有與來源和目的地相同的區域（不是任何對任何）。 • 僅有一個區域。 • 沒有為原則設定的靜態位址群組、IP 範圍或網路遮罩。 根據預設，透過 Panorama 產生的導向規則不會設定 NSX 服務，且 NSX 流量方向會設為「進出」。產生導向規則後，您可以更新個別的導向規則以變更 NSX 流量方向，或新增 NSX 服務。Panorama 會在您自動產生導向規則時自動填入下列欄位，但 [說明] 和 [NSX 服務] 除外。
名稱	輸入要在 NSX Manager 上顯示之導向規則的名稱。自動產生時，Panorama 會為每個導向規則加上首碼 auto_，並將安全性原則規則名稱中的任何空格取代為底線（_）。
說明	（選用）輸入頁籤來說明此服務定義的目的或功能。
NSX 流量導向	指定重新導向至 VM-Series 防火牆之流量的方向。 • 進出—建立 NSX 的 INOUT 規則。往來於來源與目的地之間的指定流量類型，會重新導向至 VM-Series 防火牆。Panorama 會將此流量方向用於自動產生的導向規則。 • 傳入—建立 NSX 的 IN 規則。從目的地傳至來源的指定流量類型，會重新導向至 VM-Series 防火牆。 • 傳出—建立 NSX 的 OUT 規則。從來源傳至目的地的指定流量類型，會重新導向至 VM-Series 防火牆。
NSX 服務	選取要重新導向至 VM-Series 防火牆的應用程式（Active Directory 伺服器、HTTP、DNS 等）流量。
裝置群組	從下拉式清單中選取裝置群組。所選的裝置群組將決定要套用至導向規則的安全性原則。裝置群組必須與 NSX 服務定義相關聯。
安全性原則	自動產生的導向規則所依據的安全性原則規則。

© 2019 Palo Alto Networks, Inc.

Panorama > 日誌擷取設定檔

使用日誌擷取設定檔以讓 Panorama 從外部來源接收日誌。在 PAN-OS 8.0.0 中，Panorama（在 Panorama 模式下）可作為 Syslog 接收者，使用 Syslog 從 Traps ESM 伺服器擷取日誌。將透過內容更新推送對新外部日誌來源的支援和較新的 Traps ESM 版本更新。

若要啟用日誌擷取，您必須將 Panorama 設定為 Traps ESM 伺服器上的 Syslog 接收器，在 Panorama 定義日誌擷取設定檔，並將日誌擷取設定檔附加至日誌收集器群組。

若要新增新的外部 Syslog 擷取設定檔，請 **Add**（新增）設定檔並依照下表所述進行設定。

欄位	說明
名稱	輸入外部 Syslog 擷取設定檔的名稱。您可新增最多 255 個設定檔。
來源名稱	輸入外部來源的名稱或 IP 位址，該外部來源將傳送日誌。設定檔中最多可新增 4 個來源。
連接埠	輸入連接埠，Panorama 將可透過網路在該連接埠上存取，且將使用連接埠進行通訊和接聽。 針對 Traps ESM，選取範圍在 23000-23999 之間的值。您可在 Traps ESM 上設定相同埠號以啟用 Panorama 和 ESM 之間的通訊。
Transport	選取 TCP、UDP 或 SSL。若您選取 SSL，您必須在 [Panorama > 受管理收集器 > 一般] 中針對安全 syslog 通訊設定輸入憑證。
外部日誌類型	從下拉式清單中選取日誌類型。
版本	從下拉式清單中選取版本。

使用 [監控 > 外部日誌] 以檢視從 Traps ESM 伺服器擷取到 Panorama 的資訊。

© 2019 Palo Alto Networks, Inc.

Panorama > 日誌設定

使用 **Log Settings**（日誌設定）頁面以將以下日誌類型轉送至外部服務：

- Panoramam 管理伺服器（M-Series 裝置或 Panorama 模式下的 Panorama 虛擬裝置）在本機上產生的系統、組態、User-ID 和關聯日誌。
- 傳統模式下的 Panorama 虛擬裝置在本機上產生或從防火牆收集的所有類型的日誌。

針對防火牆傳送至日誌收集器的日誌，請完成日誌收集器組態以啟用轉送至外部伺服器。

啟動前，您必須先定義外部服務的伺服器設定檔（請參閱 [裝置 > 伺服器設定檔 > SNMP 設陷]、[裝置 > 伺服器設定檔 > Syslog]、[裝置 > 伺服器設定檔 > 電子郵件] 和 [裝置 > 伺服器設定檔 > HTTP]）。然後 **Add**（新增）一個或多個比對清單設定檔並依照下表進行設定。

比對清單設定檔設定	說明
名稱	輸入用來識別比對清單設定檔的名稱（最多 31 個字元）。
篩選	依預設，Panorama 會轉送日誌類型中的 **All Logs**（所有日誌），您正針對該日誌類型新增比對清單設定檔。若要轉送日誌的子集，請開啟下拉式清單並選取現有的篩選器或選取 **Filter Builder**（篩選建立器）以新增新的篩選器。針對新篩選器中的各個查詢，指定下列欄位並 **Add**（新增）查詢： • 連接器—選取查詢的連接器邏輯（and/or）。若您要將否定套用至邏輯，則選取 **Negate**（否定）。例如，若要避免從不受信任的區域轉送日誌，請選取 **Negate**（否定）、選取 **Zone**（區域）屬性、選取 **equal** 運算子，然後在 [值] 欄中輸入不受信任的區域名稱。 • 屬性—選取日誌屬性。選項取決於日誌類型。 • 運算子—選取準則以決定是否套用屬性（例如 **equal**）。可用選項取決於日誌類型。 • 值—指定查詢要比對的屬性值。 若要顯示或匯出 篩選器比對的日誌，請選取 **View Filtered Logs**（檢視篩選的日誌）。此頁籤提供與 **Monitoring**（監控） 頁籤頁面相同的選項（例如 **Monitoring**（監控） > **Logs**（日誌） > **Traffic**（流量））。
說明	輸入最多 1,024 個字元的說明來解釋這個比對清單設定檔的目的。
SNMP	**Add**（新增）一或多個 SNMP 設陷伺服器設定檔，將日誌當作 SNMP 設陷轉送（請參閱 [裝置 > 伺服器設定檔 > SNMP 設陷]）。
電郵	**Add**（新增）一或多個電子郵件伺服器設定檔，將日誌當作電子郵件通知轉送（請參閱 [裝置 > 伺服器設定檔 > 電子郵件]）。
Syslog	**Add**（新增）一或多個 Syslog 伺服器設定檔，將日誌當作 Syslog 訊息轉送（請參閱 [裝置 > 伺服器設定檔 > Syslog]）。
HTTP	**Add**（新增）一個或多個 HTTP 伺服器設定檔，將日誌當作 HTTP 要求轉送（請參閱 [裝置 > 伺服器設定檔 > HTTP]）。
內建動作	除了系統日誌與組態日誌之外的所有日誌類型都可以設定動作。

© 2019 Palo Alto Networks, Inc.

比對清單設定檔設定	說明
	• **Add**（新增）動作並輸入用以說明的名稱。 • 選取您要標記的 IP 位址—**Source Address**（來源位址）或 **Destination Address**（目的地位址）。 • 選取動作—**Add Tag**（新增頁籤）或 **Remove Tag**（移除頁籤）。 • 選取是否在此裝置上將頁籤散佈至本機 User-ID 代理程式，或至遠端 User-ID 代理程式。 • 若要將頁籤散佈至 **Remote device User-ID Agent**（遠端裝置 **User-ID** 代理程式），請選取將啟用轉送的 HTTP 伺服器設定檔。 • 設定 IP-Tag **Timeout**（逾時）以設定 IP 位址到頁籤對應維護的時間。將逾時設定為 0 代表著 IP-Tag 對應不會逾時（範圍為 0 到 43200（30 天）；預設值為 0）。 您只能使用 *Add Tag*（新增頁籤）動作設定連線逾時。 • 輸入或選取您要套用或從目標來源或目的地 IP 位址移除的 **Tags**（頁籤）。您只可以標記關聯日誌和 HIP 比對日誌中的來源 IP 位址。

© 2019 Palo Alto Networks, Inc.

Panorama > Server Profiles > SCP（Panorama > 伺服器設定檔 > SCP）

- Panorama > Server Profiles > SCP（Panorama > 伺服器設定檔 > SCP）

選取 **Panorama** > **Server Profiles**（伺服器設定檔） > **SCP** 進行安全複本通訊協定 (SCP) 伺服器設定，在網路上安全地複制和傳輸檔案，以便您可以自動下載和安裝氣隙 Panorama™ 管理伺服器管理的受管理防火牆、日誌收集器和 WildFire® 設備的內容更新。

SCP 伺服器設定	說明
名稱	輸入用來識別伺服器設定檔的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、空格、連字號與底線。
伺服器	輸入伺服器 IP 位址或 FQDN。
連接埠	輸入用於檔案傳輸的伺服器連接埠（範圍是 1–65,535；預設值為 22）。
使用者名稱	輸入用於存取 SCP 伺服器的使用者名稱。
密碼 確認密碼	輸入並確認用於存取 SCP 伺服器的使用者名稱的區分大小寫密碼。

© 2019 Palo Alto Networks, Inc.

Panorama > 已排程的設定匯出

若要在 Panorama 和防火牆上對匯出所有執行中組態進行排程，請 **Add**（新增）匯出工作，然後依照下表所述進行設定。

如果 *Panorama* 具備高可用性 *(HA)* 組態，就必須為每個端點執行這些指示，才能確保已排程的匯出在容錯移轉後會繼續進行。*Panorama* 不會在 *HA* 端點之間同步排程的組態匯出。

排程組態匯出設定	說明
名稱	輸入用來識別組態匯出工作的名稱（最多 31 個字元）。名稱區分大小寫，且必須是唯一。請僅使用字母、數字、連字號與底線。
說明	輸入選取性說明。
啟用	選取此選項可啟用匯出工作。
排程匯出開始時間（每日）	指定每天開始匯出的時間（24 小時制，格式為 HH:MM）。
通訊協定	選取要用於將日誌從 Panorama 匯出至遠端主機的通訊協定。安全複製 (**SCP**) 是安全性通訊協定；**FTP** 不是。
主機名稱	輸入目標 SCP 或 FTP 伺服器的 IP 位址或主機名稱。
連接埠	輸入目標伺服器上的埠號。
path	指定將儲存匯出組態的目標伺服器資料夾或目錄路徑。 例如，如果組態包儲存在頂層資料夾 Panorama 內名為 exported_config 的資料夾中，則每種伺服器類型的語法為： • SCP 伺服器：/Panorama/exported_config • FTP 伺服器：/Panorama/exported_config 以下字元：**.**（句點）、**+**、**{** 和 **}**、**/**、**-**、**_**、**0-9**、**a-z** 和 **A-Z**。檔案 **Path**（路徑）中不支援空格。
啟用 FTP 被動模式	選取以使用 FTP 被動模式。
使用者名稱	指定存取目標系統所需的使用者名稱。
密碼/確認密碼	指定存取目標系統所需的密碼。 使用最長 15 個字元的密碼。如果密碼超過 15 個字元，則測試 SCP 連線將顯示錯誤，因為防火牆在嘗試連線到 SCP 伺服器時會對密碼進行加密，並且加密密碼的長度最多只能為 63 個字元。
測試 SCP 伺服器連線	選取以測試 Panorama 與 SCP 主機/伺服器之間的通訊。 若要啟用資料的安全傳輸，您必須確認並接受 SCP 伺服器的主機金鑰。在接受主機金鑰之前，不會建立連線。如果 Panorama 具備 HA 組態，就必須為每個 HA 端點執行此驗證，讓每個 HA 端點接受 SCP 伺服器的主機金鑰。

© 2019 Palo Alto Networks, Inc.

Panorama > 軟體

使用此頁面可在 Panorama 管理伺服器上管理 Panorama 軟體更新。

- 管理 Panorama 軟體更新
- 顯示 Panorama 軟體更新資訊

管理 Panorama 軟體更新

選取 **Panorama** > **Software**（軟體） 可執行下表所述的各項工作。

依預設，*Panorama* 管理伺服器可儲存最多兩項軟體更新。為了釋放空間以進行更新，伺服器會自動刪除最舊的更新。您可以變更 Panorama 儲存的軟體映像檔數，並手動刪除影像檔以釋放空間。

請參考安裝 Panorama 的內容與軟體更新了解關於版本相容性的重要資訊。

工作	說明
立即檢查	如果 Panorama 可存取網際網路，請按一下 **Check Now**（立即檢查），顯示最新的更新資訊（請參閱顯示 Panorama 軟體更新資訊）。 如果 Panorama 不能存取外部網路，請使用瀏覽器來造訪軟體更新網站，取得更新資訊。
上傳	若要在 Panorama 不能存取網際網路時上傳軟體映像檔，請使用瀏覽器造訪軟體更新站台，尋找所需版本及下載軟體映像檔至 Panorama 可存取的電腦，選取 **Panorama** > **Software**（軟體），按一下 **Upload**（上傳），**Browse**（瀏覽）並選取軟體映像檔，然後按一下 **OK**（確定）。上傳完成後，「已下載」欄將顯示核取標記，「動作」欄將顯示 **Install**（安裝）。
下載	如果 Panorama 可存取網際網路，請 **Download**（下載）（[動作] 欄）所需版本。下載完成時，「已下載」欄將顯示核取標記。
安裝	**Install**（安裝）（Action（動作）欄）軟體映像檔。安裝完成後，Panorama 會在重新啟動時將您登出。 *Panorama* 會定期執行檔案系統完整性檢查 *(FSCK)*，以防止 *Panorama* 系統檔案損毀。此檢查會在重新啟動八次之後，或在上次執行 *FSCK 90* 天之後重新啟動時發生。如果正在執行 *FSCK*，*Web* 介面及 *SSH* 登入畫面會顯示警告，在其完成之前您將無法登入。完成此程序的時間因儲存系統的大小而有所不同；對於較大系統，可能會花費幾小時的時間才能讓您重新登入 *Panorama*。若要檢視進度，請設定對於 *Panorama* 的主控台存取權。
版本資訊	如果 Panorama 可存取網際網路，您可以存取所需軟體版本的 **Release Notes**（版本資訊），並檢閱版本變更、修正、已知問題、相容性問題及預設行為的變更。 如果 Panorama 不能存取網際網路，請使用瀏覽器來造訪軟體更新網站，並下載適當版本。
☒	不再需要或需要釋放空間以儲存更多影像時，請刪除軟體影像。

© 2019 Palo Alto Networks, Inc.

顯示 Panorama 軟體更新資訊

選取 **Panorama** > **Software**（軟體） 可顯示下列資訊。若要顯示 Palo Alto Networks 的最新資訊，請按一下 **Check Now**（立即檢查）。

軟體與內容更新資訊	說明
版本	Panorama 軟體版本
大小	軟體影像的大小 (MB)。
發行日期	Palo Alto Networks 發行更新的日期和時間。
支持	指示影像是否可供安裝。
目前已安裝	核取標記指示已安裝的更新。
動作	指示可供映像檔使用的動作（**Download**（下載）、**Install**（安裝）或 **Reinstall**（重新安裝））。
版本資訊	按一下 **Release Notes**（版本資訊）可存取所需軟體版本的版本資訊，並檢閱版本變更、修正、已知問題、相容性問題及預設行為的變更。
☒	不再需要或需要釋放空間以儲存更多下載或上載項時，請刪除更新。

© 2019 Palo Alto Networks, Inc.

Panorama > 設備部署

您可使用 Panorama 以將軟體和內容更新部署至多個防火牆與日誌收集器，並管理防火牆授權。

您想了解什麼內容？	請參閱：
將軟體與內容更新部署至防火牆與日誌收集器。	管理軟體和內容更新
查看安裝了哪些軟體與內容更新，以及哪些軟體與內容更新可供下載及安裝。	顯示軟體和內容更新資訊
排程防火牆與日誌收集器的自動內容更新	排程動態內容更新
從 Panorama 復原一個或多個防火牆的內容版本。	從 Panorama 復原內容版本
檢視、啟動、停用及重新整理授權。 檢視防火牆授權的狀態。	管理防火牆授權
想知道更多？	管理授權和更新。

管理軟體和內容更新

- Panorama > Device Deployment > Software（Panorama > 裝置部署 > 軟體）

Panorama 提供下列選項供您將軟體和內容更新部署到防火牆和日誌收集器。

若要減少管理 *(MGT)* 介面上的流量，您可以將 *Panorama* 設定為使用不同介面來部署更新（請參閱 Panorama > 設定 > 介面*)*。

Panorama 裝置部署選項	說明
下載	若要在 Panorama 連線至網際網路時部署軟體更新或內容更新，請 **Download**（下載）更新。下載完成時，Available（可用）欄會顯示 Downloaded（已下載）。您接著可以： • 安裝 PAN-OS/Panorama 軟體更新或內容更新。 • 啟動 GlobalProtect™ 應用程式或 SSL VPN 用戶端軟體更新。
升級	如果有可用的 BrightCloud URL 篩選內容更新，請按一下 **Upgrade**（升級）。升級成功後，您可在防火牆上安裝更新。
安裝	在您下載或上傳 PAN-OS 軟體、Panorama 軟體或內容更新之後，請按一下 Action（動作）欄中的 **Install**（安裝），然後選取： • **Devices**（裝置）—選取要安裝更新的防火牆或日誌收集器。如果清單較長，請使用篩選器。選取 **Group HA Peers**（群組 HA 端點）可針對為高可用性 (HA) 端點的防火牆

© 2019 Palo Alto Networks, Inc.

Panorama 裝置部署選項	說明
	進行分組。這可讓您輕鬆識別具有 HA 組態的防火牆。若要僅顯示特定防火牆或日誌收集器，請選取它們，然後選取 **Filter Selected**（已選取篩選器）。 • 僅上傳至裝置（僅限軟體）—選取此選項可上傳軟體而不會自動安裝。您必須手動安裝該軟體。 • **Reboot device after install**（安裝後重新啟動裝置）（僅限軟體）—選取此選項可指定要讓安裝程序自動重新啟動防火牆或日誌收集器。重新啟動之後才能完成安裝。 • **Disable new apps in content update**（在內容更新中停用新應用程式）（僅限應用程式與威脅）—選取此選項可在更新（相對於上次安裝的更新為新更新）中停用應用程式。這可針對最新威脅，同時讓您在準備好任何原則更新之後靈活啟用應用程式。接著，若要啟用應用程式，請登入防火牆，選取 **Device**（裝置）> **Dynamic Updates**（動態更新），在功能欄中按一下 **Apps**（應用程式）以顯示新應用程式，然後對每個您想要啟用的應用程式按一下 **Enable/Disable**（啟用/停用）。 您也可以選取 *Panorama* > *Managed Devices*（受管理的裝置）來安裝防火牆軟體和內容更新，或選取 *Panorama* > *Managed Collectors*（受管理的收集器）來安裝專用日誌收集器的軟體更新。
啟用	在您下載或上傳 GlobalProtect 應用程式軟體更新之後，按一下 Action（動作）欄中的 **Activate**（啟動），然後選取下列選項： • **Devices**（裝置）—選取要在其上啟動更新的防火牆。如果清單較長，請使用篩選器。選取 **Group HA Peers**（群組 HA 端點）可針對為高可用性 (HA) 端點的防火牆進行分組。這可讓您輕鬆識別具有 HA 組態的防火牆。若要僅顯示特定防火牆，請選取防火牆，然後選取 **Filter Selected**（已選取篩選器）。 • **Upload only to device**（僅上傳至裝置）—如果您不想讓 PAN-OS 自動啟動上傳的映像，請選取此選項。您必須登入防火牆並啟動它。
版本資訊	按一下 **Release Notes**（版本資訊）可存取所需軟體版本的版本資訊，並檢閱版本變更、修正、已知問題、相容性問題及預設行為的變更。
文件	按一下 **Documentation**（文件）可存取所需內容發佈版本的版本資訊。
☒	不再需要或在您想要釋放空間以儲存更多下載或上傳項時，請刪除軟體或內容更新。
立即檢查	**Check Now**（立即檢查）以顯示軟體和內容更新資訊。
上傳	若要在 Panorama 未連線至網際網路時部署軟體或內容更新，請從軟體更新或動態更新網站將更新下載至電腦，選取與更新類型相對應的 **Panorama** > **Device Deployment**（裝置部署）頁面，按一下 **Upload**（上傳），選取更新 **Type**（類型）（僅限內容更新），選取上傳的檔案，然後按一下 **OK**（確定）。然後安裝或啟動更新的步驟取決於類型： • **PAN-OS or Panorama software**（**PAN-OS** 或 **Panorama** 軟體）—上傳完成後，「已下載」欄將顯示核取標記，「動作」欄將顯示 **Install**（安裝）。 • **GlobalProtect** 用戶端或 **SSL VPN** 用戶端軟體—從檔案啟動。 • 動態更新—從檔案安裝。
從檔案安裝	在您上傳內容更新後，請按一下 **Install from File**（從檔案安裝），選取內容 **Type**（類型），選取更新的檔案名稱，然後選取防火牆或日誌收集器。

© 2019 Palo Alto Networks, Inc.

Panorama 裝置部署選項	說明
從檔案啟動	在您上傳 GlobalProtect 應用程式軟體更新後，請按一下 **Activate from File**（從檔案啟動），選取更新的檔案名稱，然後選取防火牆。
排程	選取此選項可排程動態內容更新。

顯示軟體和內容更新資訊

- Panorama > 裝置部署 > 軟體

選取 **Panorama** > **Device Deployment**（設備部署） > **Software**（軟體） 可顯示 PAN-OS **Software**（軟體）、**GlobalProtect Client**（**GlobalProtect** 用戶端）軟體，以及目前已安裝或可供下載及安裝的 **Dynamic Updates**（動態更新）（內容）。**Dynamic Updates**（動態更新）頁面依內容類型（防毒、應用程式與威脅、URL 篩選及 WildFire）組織資訊，並指示上次檢查更新資訊的日期與時間。若要顯示 Palo Alto Networks 的最新軟體或內容資訊，請按一下 **Check Now**（立即檢查）。

軟體與內容更新資訊	
版本	軟體或內容更新版本。
檔案名稱	更新檔案的名稱。
平台	為更新指定的防火牆或日誌收集器機型。指出軟體防火牆機型的編號（例如，`7000` 表示 PA-7000 Series 防火牆），`VM` 表示 VM-Series 防火牆，`M` 表示 M-Series 設備。
功能	（僅限內容）列出內容版本可能包含的特徵碼類型。
類型	（僅限內容）指出下載包含完整資料庫更新或增量更新。
大小	更新檔案的大小。
發行日期	Palo Alto Networks 發行更新的日期和時間。
支持	（僅限 PAN-OS 或 Panorama 軟體）表示更新已下載或已更新。
已下載	（僅限 SSL VPN 用戶端軟體、GlobalProtect 用戶端軟體或內容）核取標記表示內容已下載。
動作	表示您可對更新執行的動作：下載、升級、安裝或啟動。
文件	（僅限內容）提供所需內容發佈版本的版本資訊連結。
版本資訊	（僅限軟體）提供所需軟體發佈版本的版本資訊連結。
☒	不再需要或在您想要釋放空間以儲存更多下載或上載項時，請刪除更新。

排程動態內容更新

- Panorama > Device Deployment > Dynamic Updates（Panorama > 設備部署 > 動態更新）

© 2019 Palo Alto Networks, Inc.

若要對自動下載與安裝更新排程，請按一下 **Schedules**（排程），再按一下 **Add**（新增），然後進行如下所述的設定：

動態更新排程設定	
名稱	輸入用來識別排程工作的名稱（最多 31 個字元）。名稱區分大小寫且必須是唯一的，而且只能包含字母、數字、連字號和底線。
已停用	選取以停用排程工作。
下載來源	選取內容更新的下載來源。您可以選取以從 Palo Alto Networks **Updates Server**（更新伺服器）或 **SCP** 伺服器下載內容更新。
SCP 設定檔（僅限 SCP）	選取要從中下載的已設定 SCP 設定檔。
SCP 路徑（僅限 SCP）	在 SCP 伺服器上輸入用於下載內容更新的特定路徑。
類型	選取要排程的內容更新類型：**App**（應用程式）、**App and Threat**（應用程式與威脅）、**Antivirus**（防毒）、**WildFire** 或 **URL Database**（URL 資料庫）。
週期性	選取 Panorama 檢查更新伺服器的間隔。週期性選項依更新類型而異。
時間	若為 **Daily**（每日）更新，請選取 24 小時制的 **Time**（時間）。 若為 **Weekly**（每週）更新，則選取星期的 **Day**（日期），並選取 24 小時制的 **Time**（時間）。
在內容更新時停用新應用程式	僅當您將更新 **Type**（類型）設定為 **App**（應用程式）或 **App and Threat**（應用程式與威脅），將 **Action**（動作）設定為 **Download and Install**（下載並安裝）時，才能在內容更新中停用新應用程式。 選取以在更新（相對於上次安裝的更新為新更新）中停用應用程式。這可針對最新威脅，同時讓您在準備好任何政策更新之後靈活啟用應用程式。接著，若要啟用應用程式，請登入防火牆，選取 **Device**（裝置）> **Dynamic Updates**（動態更新），在功能欄中按一下 **Apps**（應用程式）以顯示新應用程式，然後對每個您想要啟用的應用程式按一下 **Enable/Disable**（啟用/停用）。
動作	• **Download Only**（僅下載）—Panorama™ 將下載排程的更新。您必須在防火牆與日誌收集器上手動安裝更新。 • **Download and Install**（下載並安裝）—Panorama 將下載並自動安裝排程的更新。 • **Download and SCP**（下載和 **SCP**）—Panorama 將下載內容更新套件並將其傳輸至指定的 SCP 伺服器。
裝置	選取 **Devices**（設備），然後選取將接收排程內容更新的防火牆。
日誌收集器	選取 **Log Collectors**（日誌收集器），然後選取將接收排程內容更新的受管理的收集器。

從 Panorama 復原內容版本

- Panorama > 設備部署 > 動態更新

© 2019 Palo Alto Networks, Inc.

快速地從 Panorama 為一個或多個防火牆的應用程式、版本應用程式與威脅、防毒、WildFire 和 WildFire 內容更新 **Revert Content**（復原內容）版本至先前安裝的內容版本。您所復原的內容版本必須早於目前安裝在防火牆的版本。復原內容可用於運行 Panorama 8.1 的版本上。只要防火牆上的本機復原功能可用，就可以復原防火牆的內容。

欄位	說明
篩選	篩選您要復原哪一個設備的內容。您可以依下列條件進行篩選： • 設備狀態 • 平台 • 裝置群組 • 範本 • 標籤 • HA 狀態 • 軟體版本（PAN-OS） • 目前內容版本
裝置	選擇一個或多個要復原的設備。顯示以下設備內容： • 設備名稱—防火牆名稱。 • 目前版本—目前安裝於此設備的內容版本。如果目前沒有安裝任何版本，則欄位將顯示 0。 • 先前版本（內容）—先前安裝在執行 PAN 8.1 或之後版本防火牆上的內容。如果先前沒有安裝任何內容版本，或如果防火牆執行的版本早於 PAN-OS 8.1 版，則欄位將為空白。 • 軟體版本—目前安裝在此設備上的 PAN-OS 版本。 • HA 狀態—當在 HA 配對中時，顯示 HA 狀態。如果設備並不在 HA 配對中，則欄位將為空白。
群組 HA 配對	檢視此方塊至群組 HA 配對

當您選定要復原的設備後，按一下 **OK**（確認）。

管理防火牆授權

- Panorama > 設備部署 > 授權

選取 **Panorama** > **Device Deployment**（設備部署）> **Licenses**（授權）可執行下列工作：

- 更新無法直接進行內部存取之防火牆的授權—請按一下 [重新整理]。
- 在防火牆上啟動授權—若要在防火牆上啟動授權，請按一下 **Activate**（啟動），選取防火牆，然後在 [驗證碼] 欄輸入 Palo Alto Networks 針對該防火牆提供的驗證碼。
- 停用安裝在 VM-Series 防火牆上的所有授權以及訂閱/權利—按一下 **Deactivate VMs**（停用虛擬電腦），選取防火牆（清單僅顯示執行 PAN-OS 7.0 或更新版本的防火牆），然後按一下：
  - 繼續—停用授權，並透過授權伺服器自動註冊變更。授權會重新記入您的帳戶，且可重複使用。
  - 手動完成 — 產生一個語彙基元檔案。如果 Panorama 沒有網際網路直接存取權，請使用此選項。若要完成停用程序，您必須登入支援入口網站，選取 **Assets**（資產），按一下 **Deactivate License(s)**（停用授權），上載語彙基元檔案，然後按一下 **Submit**（提交）。在您完成停用程序之後。

© 2019 Palo Alto Networks, Inc.

您也可以檢視受管理防火牆的目前授權狀態。對於無法直接存取網際網路的防火牆，Panorama 將自動執行授權伺服器每日簽入，擷取授權更新與續約，以及將其推送至防火牆。簽入是上午 1 時與 2 時間的硬性設定；您必須變更此排程。

防火牆授權資訊	
裝置	防火牆名稱
虛擬系統	表示防火牆支援 ✓ 或不支援 ⊗ 多個虛擬系統。
威脅防禦	表示授權為作用中✓、非作用中 ⊗ 或已到期 ⚠（隨附到期日期）。
URL	
支援	
GlobalProtect 閘道	
GlobalProtect 入口網站	
WildFire	
VM 系列容量	指出這是 ✓ 否 ⊗ 為 VM-Series 防火牆。

© 2019 Palo Alto Networks, Inc.