paloalto TECHDOCS

PAN-OS® 網路管理員指南

Version 10.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

August 9, 2021

Table of Contents

網路

所有 Palo Alto Networks® 新一代防火牆都提供靈活的網路架構，其中包括支援動態路由、交換及 VPN 連線，可讓您將防火牆部署至幾乎任何的網路環境中。

> 網路簡介

網路簡介

網路是防火牆的基本建置區塊，因為它們必須能夠接收、處理和轉送資料。設定防火牆的乙太網路連接埠後，您可從 Tap、虛擬介接、Layer 2、Layer 3 或 AE 介面部署中進行選擇。此外，若要整合至各種網路區段，您可在不同的連接埠上設定不同類型的介面。

要開始聯網，您應該先存取 PAN-OS® 管理員指南中的「開始使用」主題。在那裡，您將瞭解分割網路以及設定介面和區域的資訊。該初始工作會說明如何設定 Layer 3 介面以連線到網際網路、您的內部網路和您的資料中心應用程式。

本 PAN-OS 網路管理員指南將透過如何設定 Tap、虛擬介接、Layer 2、Layer 3 和 AE 等主題，詳細介紹相關資訊。設定網路介面後，即可透過 PDF 或 CSV 格式匯出設定表格資料，以供內部檢閱或稽核。

本指南還解釋了防火牆如何支援多個虛擬路由器以獲取到其他子網路的 Layer 3 路由以及維護單獨的路由集。其余章節介紹靜態路由、動態路由通訊協定以及支援防火牆聯網的主要功能。

- 設定介面
- 虛擬路由器
- 服務路由
- 靜態路由
- RIP
- OSPF
- BGP
- IP 多點傳送
- 路由重新散佈
- GRE 通道
- DHCP
- DNS
- DDNS
- NAT
- NPTv6
- NAT64
- ECMP
- LLDP
- BFD
- 工作階段設定與逾時
- 通道內容檢查
- 網路封包代理程式

設定介面

Palo Alto Networks® 新一代防火牆可以同時在多個部署中運作，因為部署是在介面層級發生的。例如，您可以設定部分介面，讓 Layer 3 介面將防火牆整合到動態路由環境中，同時設定其他介面以整合到 Layer 2 交換網路中。以下主題描述了每種類型的介面部署及其設定方式、如何設定 Bonjour Reflector 以及如何使用介面管理設定檔。

旁接介面

網路旁接是能夠存取跨電腦網路流動之資料的裝置。旁接模式部署可讓您透過交換器 SPAN 或鏡像連接埠，被動地監控跨網路的流量。

SPAN 或鏡像連接埠允許從交換器上的其他連接埠複製流量。透過將防火牆上的介面專用作旁接模式介面，並將其連接至交換器 SPAN 連接埠，交換器 SPAN 連接埠可為防火牆提供鏡像流量。這可在網路流量未流動的情況下，提供網路內的應用程式可見度。

透過在旁接模式下部署防火牆，您無需對網路設計進行任何變更，即可瞭解網路上執行的應用程式。此外，處於旁接模式下，防火牆還可識別網路上的威脅。但請注意，由於在旁接模式下，流量未通過防火牆，因此防火牆不會對流量採取任何動作，例如封鎖存在威脅的流量或套用 QoS 流量控制。

若要設定旁接介面並開始監控網路上的應用程式與威脅：

STEP 1 | 確定要用作旁接介面的連接埠，並將其連線至設定了 SPAN/RSPAN 或連接埠鏡像的交換器。

您將透過防火牆從 SPAN 目的地連接埠傳送網路流量，以便您可以洞察網路上的應用程式與威脅。

STEP 2 | 從防火牆 Web 介面，設定要用作網路旁接的介面。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取對應剛剛連線之連接埠的介面。
2. 選取 **Tap**（旁接） 作為 **Interface Type**（介面類型）。
3. 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）並選取 **New Zone**（新增區域）。
4. 在 Zone（區域）對話方塊中，輸入新區域的 **Name**（名稱），例如 TapZone，然後按一下 **OK**（確定）。

STEP 3 | （選用）建立要使用的任何轉送設定檔。

- 設定日誌轉送。
- 設定 Syslog 監控。

STEP 4 | 建立 Security Profiles（安全性設定檔）以掃描網路流量威脅：

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔）。
2. 針對每種安全性設定檔類型，**Add**（新增）一個新的設定檔，並將動作設為 **alert**（警示）。

   由於防火牆未與流量內聯，因此您無法使用任何封鎖或重設動作。透過設定警示動作，您將可查看防火牆在日誌和 ACC 中偵測到的任何威脅。

STEP 5 | 建立安全性原則規則，以允許流量通過旁接介面。

為旁接模式建立安全性原則規則時，來源區域與目的地區域必須相同。

1. 選取 **Policies**（原則） > **Security**（安全性），然後按一下 **Add**（新增）。
2. 在 **Source**（來源）頁籤中，將 **Source Zone**（來源區域）設定為剛剛建立的 TapZone。
3. 在 **Destination**（目的地）頁籤中，同樣將 **Destination Zone**（目的地區域）設定為 TapZone。
4. 將所有規則比對準則（**Applications**（應用程式）、**User**（使用者）、**Service**（服務）、**Address**（位址））設為 **any**（任何）。
5. 在 **Actions**（動作）頁籤中，設定 **Action Setting**（動作設定）為 **Allow**（允許）。
6. 將 **Profile Type**（設定檔類型）設為 **Profiles**（設定檔），並選取建立的各個安全性設定檔以發出威脅警示。
7. 確認已啟用 **Log at Session End**（工作階段結束時記錄）。
8. 按一下 **OK**（確定）。
9. 將規則置於規則庫的頂端。

STEP 6 | **Commit**（提交）組態。

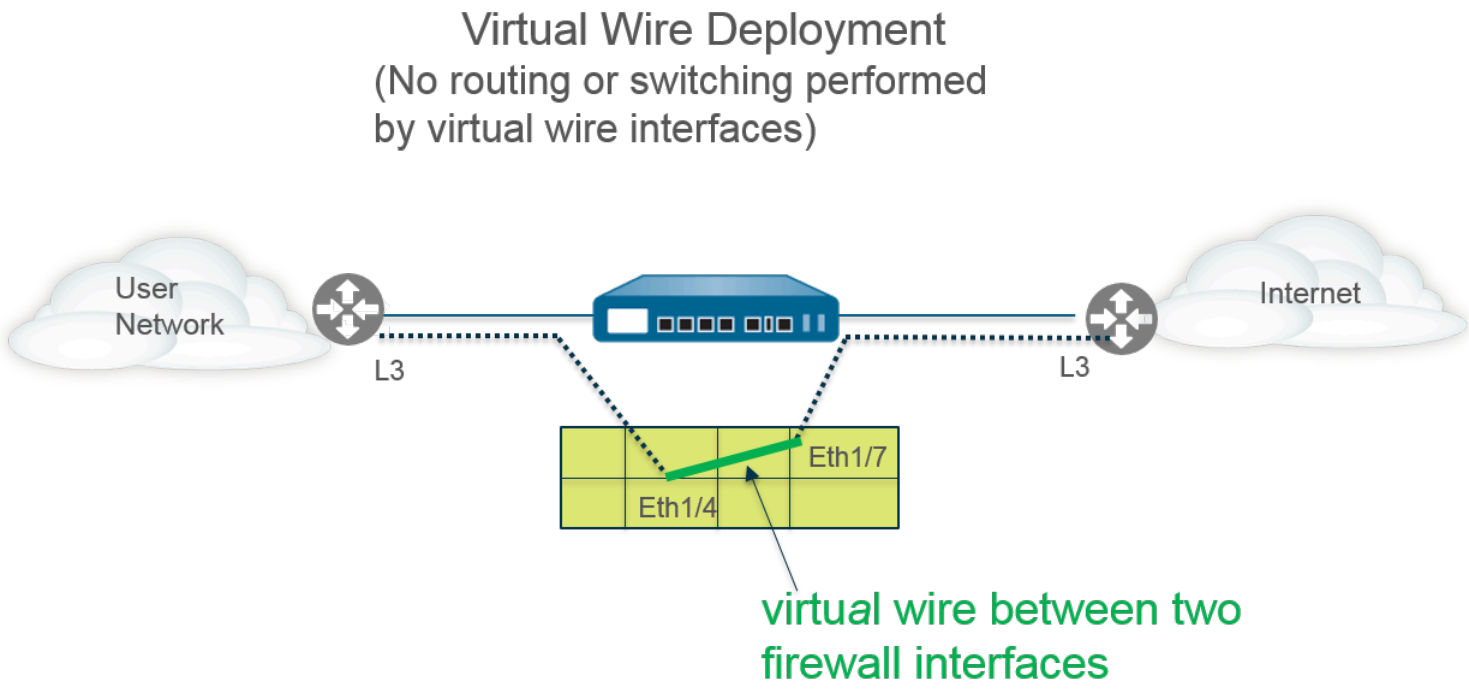
STEP 7 | 監控防火牆日誌（**Monitor**（監控） > **Logs**（日誌））和 **ACC** 以洞察網路上的應用程式與威脅。

Virtual Wire 介面

在 Virtual Wire 部署中，您可以將兩個防火牆連接埠（介面）繫結在一起，從而以透明方式將防火牆安裝在網路區段上。Virtual Wire 將以邏輯方式連線至兩個介面；因此，Virtual Wire 在防火牆內部。

只有在您要無縫整合防火牆到拓撲內並且防火牆上連線的兩個介面無需交換或路由時，才使用 Virtual Wire 部署。對於這兩個介面，防火牆將被視為 ***Wire*** 上的緩衝區。

Virtual Wire 部署簡化了防火牆的安裝和組態，因為您可以將防火牆插入現有拓撲，無需指派 MAC 或 IP 位址到界面、重新設計網路或重新設定周邊網路裝置。Virtual Wire 支援根據虛擬 LAN (VLAN) 標籤封鎖或允許流量，此外還支援安全性原則規則、App-ID、Content-ID, User-ID、解密、LLDP、主動/被動和主動/主動 HA、QoS、區域保護（有一些例外項）、非 IP 通訊協定保護、DoS 保護、封包緩衝區保護、通道內容檢查以及 NAT。



每個 Virtual Wire 介面都直接連線之 Layer 2 或 Layer 3 網路裝置或主機。Virtual Wire 介面沒有 Layer 2 或 Layer 3 位址。當其中一個 Virtual Wire 介面受到框架或封包時，會忽略任何用於交換或路由的 Layer 2 或 Layer 3 位址，但在透過 Virtual Wire 傳遞允許的框架或封包到第二個介面及其所連線之網路裝置前，將套用安全性原則規則或 NAT 原則規則。

您不能為需要支援交換、VPN 通道或路由的介面使用 Virtual Wire 部署，因為它們需要 Layer 2 或 Layer 3 位址。Virtual Wire 介面不會使用介面管理設定檔，該設定檔用於控制 HTTP 及偵測等服務，因此要求介面有一個 IP 位址。

防火牆出廠時有兩個乙太網路連接埠（連接埠 1 和 2），並預先設定為 Virtual Wire 介面，這些介面將允許所有未標記的流量。

如果您正在 ***Cisco TrustSec*** 網路中使用安全性群組標籤 ***(SGT)***，最佳做法是在 ***Layer 2*** 或虛擬連接模式中部署內嵌防火牆。***Layer 2*** 或虛擬連接模式中的防火牆可以檢查已標記流量並提供威脅防禦。

如果您不想使用預先定義的 ***Virtual Wire***，您必須刪除該組態，以防止其干擾您在防火牆上設定的其他設定。請參閱設定外部服務的網路存取權。

- Virtual Wire 上的 Layer 2 和 Layer 3 封包
- Virtual Wire 介面的連接埠速度
- Virtual Wire 上的 LLDP
- Virtual Wire 的彙總介面
- 高可用性 Virtual Wire 支援
- Virtual Wire 介面的區域保護
- VLAN 標記的流量
- Virtual Wire 子介面
- 設定 Virtual Wire

Virtual Wire 上的 Layer 2 和 Layer 3 封包

Virtual Wire 介面將允許 Layer 2 和 Layer 3 封包從所連線的裝置以透明方式傳送，只要套用於相應區域或介面的原則允許流量。Virtual Wire 介面本身不會參與路由或交換。

例如，防火牆不會遞減虛擬連結上傳輸的路徑追蹤封包中的 TTL，因為該連結是透明的，不會被計為躍點。例如操作、管理及維護 (OAM) 通訊協定資料單位 (PDU) 等封包就在不會在防火牆上終止傳輸。因此，Virtual Wire 將允許防火牆保持透明，用作透傳連結，但同時仍提供安全性、NAT 以及 QoS 服務。

為了使橋接通訊協定資料單位 (BPDU) 和其他 Layer 2 控制封包（一般未標記）通過 Virtual Wire 傳輸，必須將介面附加至允許未標記流量（預設）的 Virtual Wire 物件。如果 Virtual Wire 物件的 **Tag Allowed**（允許的標記） 欄位空白，則表示 Virtual Wire 允許未標記的流量。（安全性原則規則將不會套用於 Layer 2 封包。）

為了路由 (Layer 3) 控制封包路由以通過 Virtual Wire 傳輸，您必須套用允許流量透傳的安全性原則規則。例如，套用允許 BGP 或 OSPF 等應用程式的安全性原則規則。

如果您希望能安全性原則規則套用至到達防火牆上 Virtual Wire 介面的 IPv6 流量，則啟用 IPv6 防火牆。否則 IPv6 流量將以透明方式轉送通過 Virtual Wire。

如果您對 Virtual Wire 啟用了多點傳送防火牆，並將其套用至 Virtual Wire 介面，該防火牆將建成多點傳送流量，並根據安全性原則規則決定是否轉送。如果您不啟用多點傳送防火牆，則防火牆將以透明方式轉送多點傳送流量。

Virtual Wire 上的片段與其他介面部署模式相同。

Virtual Wire 介面的連接埠速度

不同防火牆型號提供運作速度不相同的不同銅線和光纖連接埠。Virtual Wire 可繫結兩個相同類型（都為銅線或都為光纖）的乙太網路連接埠，或繫結一個銅線連接埠和一個光纖連接埠。依預

設，防火牆銅線連接埠的 **Link Speed**（連結速度）設為 **auto**（自動），這意味著防火牆自動交涉其速度與傳輸模式（**Link Duplex**（連結雙工））。設定 Virtual Wire 時，還可選取特定 **Link Speed**（連結速度）與 **Link Duplex**（連結雙工），但對於單個 Virtual Wire 中的兩個連接埠，這些設定值必須保持一致。

Virtual Wire 上的 LLDP

Virtual Wire 介面可使用 LLDP 探索相鄰裝置及其功能，而 LLDP 則允許相鄰裝置偵測網路中是否存在防火牆。LLDP 讓疑難排解變得更容易，尤其是在 Virtual Wire 上（通常無法透過傳送偵測或路徑追蹤通過 Virtual Wire 的偵測防火牆）。LLDP 為其他裝置提供偵測網路中防火牆的方式。如果沒有 LLDP，網路管理系統將無法透過 Virtual Wire 偵測是否存在防火牆。

Virtual Wire 的彙總介面

您可以為 Virtual Wire 介面設定彙總介面群組，但 Virtual Wire 並不會使用 LACP。若您在將防火牆連線至其他網路的裝置上設定 LACP，Virtual Wire 將以透明方式傳遞 LACP 封包，但不會傳遞 LACP 功能。

為了使彙總介面群組正常運作，需確保屬於 ***Virtual Wire*** 的同一側上相同 ***LACP*** 群組中所有連結已指派給相同區域。

高可用性 Virtual Wire 支援

如果您設定防火牆使用 Virtual Wire 路徑群組執行高可用性路徑監控，防火牆將嘗試透過從兩個 Virtual Wire 介面送出 ARP 封包的方式，為所設定的目的地 IP 位址解析 ARP。您要監控的目的地 IP 位址必須在與 Virtual Wire 周圍的某一個裝置相同的網路上。

Virtual Wire 介面支援主動/被動技主動/主動 HA。對於採用 Virtual Wire 的主動/主動 HA 部署，必須將已掃描封包傳回至接收防火牆才能保留轉送路徑。因此，如果收到的封包屬於對等 HA 防火牆擁有的工作階段，防火牆會透過 HA3 將封包傳送至對等體。

您可以設定 HA 配對中的被動防火牆，允許防火牆任何端的對等裝置在 HA 容錯移轉送生前，在 Virtual Wire 上預先交涉 LLDP 和 LACP。主動/被動 HA 的 LACP 和 LLDP 預先交涉的這種設定能夠加快 HA 容錯移轉。

Virtual Wire 介面的區域保護

您可以對 Virtual Wire 介面套用區域保護，但由於 Virtual Wire 介面不會執行路由，因此您不能對具有偽造 IP 位址的封包套用基於封包的攻擊防護，也不能抑制 TTL 已過期的 ICMP 錯誤封包或需要分割的 ICMP 封包。

依預設，Virtual Wire 介面會轉送所收到的全部非 IP 流量。但是，您可以套用具有通訊協定保護的區域保護設定檔，以封鎖或允許 Virtual Wire 上安全性區域之間的某些非 IP 通訊協定封包。

VLAN 標記的流量

依預設，Virtual Wire 介面會允許所有未標記的流量。但您可以使用 Virtual Wire 來連接兩個連接埠，並設定任意一個界面根據虛擬 LAN (VLAN) 標籤封鎖或允許流量。VLAN 標籤「0」表示未標記的流量。

您也可以建立多個子介面，將子介面新增至不同的區域，然後根據 VLAN 標籤或 VLAN 標籤與 IP 分類程式 （位址、範圍或子網路）的結合來分類流量，藉此套用細微的原則控制，以控制特定 VLAN 標籤或特定來源 IP 位址、範圍或子網路的 VLAN 標籤。

Virtual Wire 子介面

Virtual Wire 部署可使用 Virtual Wire 子介面區分隔進入各區域的流量。虛擬介接子介面讓您在需要管理來自多個客戶網路的流量時，能夠彈性地執行不同的原則。子介面允許您使用下列準則，將流量分隔並歸類到不同的區域（這些區域可以視需要屬於不同的虛擬系統）：

- **VLAN** 標籤—含子介面的虛擬介接部署（僅 VLAN 標籤）顯示使用 Virtual Wire 子介面和 VLAN 標籤分隔不同客戶流量的 ISP。
- **VLAN** 標籤結合 **IP** 分類程式（位址、範圍或子網路）—在下列範例中，ISP 在管理兩個不同客戶流量的防火牆上有兩個分開的虛擬系統。此範例說明在每個虛擬系統上，如何使用含 VLAN 標籤與 IP 分類程式的Virtual Wire 子介面將流量分類到不同的區域，並為每個網路的客戶套用相關的原則。

虛擬介接子介面工作流程

- 設定兩個 Ethernet 介面作為 Virtual Wire 類型，並將這兩個介面指派給 Virtual Wire 。
- 在父虛擬介接上建立子介面，以分隔 CustomerA 與 CustomerB 流量。確定在一對設定為 Virtual Wire 的子介面上定義的 VLAN 標籤相同。這是必要的，因為 Virtual Wire 不會交換 VLAN 標記。
- 建立新的子介面並定義 IP 分類程式。此工作是選擇性的，只有在您想要額外新增含 IP 分類程式的子介面，以進一步根據 VLAN 標籤與特定來源 IP 位址、範圍或子網路的組合來管理客戶流量時才需要。

您也可以使用 IP 分類程式管理未標記的流量。若要這麼做，您必須建立 VLAN 標籤為「0」的子介面，並定義含 IP 分類程式的子介面，才能使用 IP 分類程式管理未標記流量。

IP 分類僅可用於與 *Virtual* W*ire* 一端相關聯的子介面。在虛擬介接其對應端上定義的子介面必須使用相同的 *VLAN* 標籤，但不得包含 *IP* 分類程式。

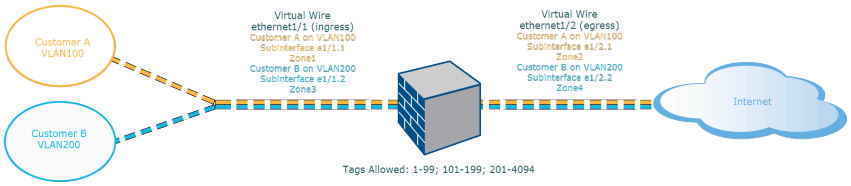


圖 **1:** 含子介面的虛擬介接部署 **(**僅 **VLAN** 標籤**)**

含子介面的 Virtual Wire 部署（僅 VLAN 標籤）說明透過一個實體介面 ethernet1/1 連接至防火牆的 CustomerA 與 CustomerB，該介面設定為 Virtual Wire，為輸入介面。第二個實體介面 ethernet1/2 也屬於虛擬介接，為提供網際網路存取的輸出介面。

對於 CustomerA，您另有子介面 ethernet1/1.1 (Ingress) 與 ethernet1/2.1 (Egress)。對於 CustomerB，您有子介面 ethernet1/1.2 (輸入) 與 ethernet1/2.2 (輸出)。設定子介面時，您必須指派適當的 VLAN 標籤和區域，才能對各個客戶套用原則。在這個範例中，CustomerA 的原則是在 Zone1 和 Zone2 之間建立，CustomerB 的原則是在 Zone3 和 Zone4 之間建立。

當流量從 CustomerA 或 CustomerB 進入防火牆時，系統會先將傳入封包上的 VLAN 標籤對照輸入子介面上定義的 VLAN 標籤進行比對。在此範例中，單一子介面會比對傳入封包上的 VLAN 標籤，因此會選取該子介面。在封包離開對應的子介面之前，系統會評估並套用為區域定義的原則。

在父虛擬介接介面與子介面上不得定義相同的 ***VLAN*** 標籤。確認子介面未包含在上層 ***Virtual Wire*** 介面上「允許的標籤」清單中定義的 ***VLAN*** 標籤 （***Network***（網路） > ***Virtual Wires***（虛擬介接））。

含子介面的 Virtual Wire 部署（VLAN 標籤與 IP 分類程式）說明與一個實體防火牆連線的 CustomerA 與 CustomerB，除了一個預設的虛擬系統外 (vsys1)，該防火牆還有兩個虛擬系統 (vsys)。每個虛擬系統都是獨立的虛擬防火牆，由每個客戶分開管理。每個 vsys 都附加獨立管理的介面/子介面與安全性地區。

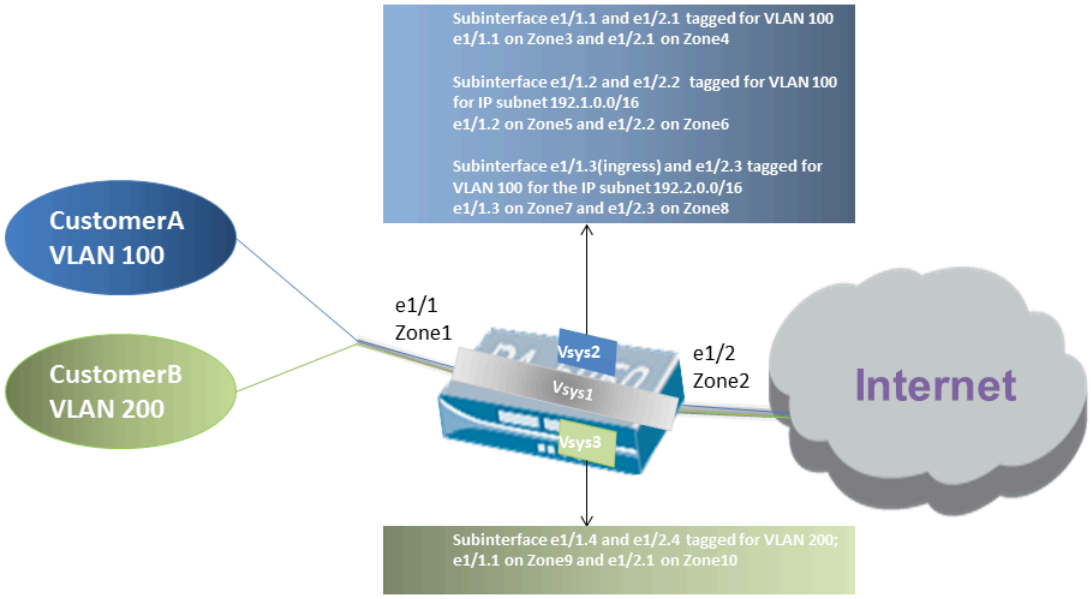


圖 **2:** 含子介面的虛擬介接部署 **(VLAN** 標籤與 **IP** 分類程式**)**

Vsys1 設定為使用實體介面 ethernet1/1 與 ethernet1/2 作為虛擬介接；ethernet1/1 是輸入介面，ethernet1/2 是輸出介面，可提供網際網路存取。此虛擬介接設定為接受所有加標記與未標記的流量，唯 VLAN 標籤 100 與 200 除外，這兩個標籤指派給子介面。

CustomerA 在 vsys2 上管理，CustomerB 在 vsys3 上管理。在 vsys2 與 vsys3 上已使用適當的 VLAN 標籤與區域建立下列 vwire 子介面，以執行原則測量。

客戶	Vsys	Vwire 子介面	區	VLAN 標籤	IP 分類程式
A	2	e1/1.1 (輸入) e1/2.1 (輸出)	Zone3 Zone4	100 100	無
	2	e1/1.2（輸入） e1/2.2（輸出）	Zone5 Zone6	100 100	IP 子網路 192.1.0.0/16
	2	e1/1.3（輸入） e1/2.3（輸出）	Zone7 Zone8	100 100	IP 子網路 192.2.0.0/16
B	3	e1/1.4（輸入） e1/2.4（輸出）	Zone9 Zone10	200 200	無

當流量從 CustomerA 或 CustomerB 進入防火牆時，系統會先將傳入封包上的 VLAN 標籤對照輸入子介面上定義的 VLAN 標籤進行比對。在此範例中，CustomerA 有多個子介面使用相同的 VLAN 標籤。因此，防火牆會先根據封包中的來源 IP 位址將分類縮小到子介面。在封包離開對應的子介面之前，系統會評估並套用為區域定義的原則。

對於傳回路徑流量，防火牆會依照在面對客戶子介面上定義的 IP 分類程序比對目的地 IP 位址，並選取適當的虛擬介接路由流量通過正確的子介面。

在父虛擬介接介面與子介面上不得定義相同的 *VLAN* 標籤。確認子介面未包含在上層 *Virtual Wire* 介面上「允許的標籤」清單中定義的 *VLAN* 標籤 （***Network***（網路） > ***Virtual Wires***（虛擬介接））。

設定 Virtual Wire

下列工作展示了如何設定兩個 Virtual Wire 介面（此範例中為 Ethernet 1/3 及 Ethernet 1/4）以建立虛擬介接。這兩個介面必須擁有相同的 **Link Speed**（連結速度）以及傳輸模式（**Link Duplex**（連結雙工））。例如，1000Mbps 全雙工銅線連接埠相當於 1Gbps 全雙工光纖連接埠。

STEP 1 | 建立第一個 Virtual Wire 介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），並選取已透過線纜連接的介面（此範例中為 **ethernet1/3**）。
2. 將 **Interface Type**（介面類型）設為 **Virtual Wire**。

STEP 2 | 將該介面附加至 Virtual Wire 物件。

1. 在同一個乙太網路介面的 **Config**（組態）頁籤上，選取 **Virtual Wire** 並按一下 **New Virtual Wire**（新 **Virtual Wire**）。
2. 為 Virtual Wire 輸入 **Name**（名稱）。
3. 對於 **Interface1**（介面 **1**），選取剛才設定的介面 (**ethernet1/3**)。（只有已設定為 Virtual Wire 介面的介面才會出現在清單中。）
4. 對於 **Tag Allowed**（允許的標籤），輸入 **0**，以表明允許未標記的流量（例如 BPDU 和其他 Layer 2 控制流量）。標籤 0 表示沒有標籤。輸入其他允許的整數標籤或標籤範圍，用逗號分隔（預設值為 0；範圍為 0 至 4,094）。
5. 如果您希望能夠將安全性原則規則套用至通過 Virtual Wire 的多點傳送流量，則選取 **Multicast Firewalling**（多點傳送防火牆）。否則，多點傳送流量將以透明方式轉送通過 Virtual Wire。
6. 選取 **Link State Pass Through**（連結狀態透傳），以便防火牆能以透明方式運作。如果偵測到 Virtual Wire 的某個連結處於關閉狀態，防火牆會關閉 Virtual Wire 配對中的另一個介面。因此，防火牆兩端的裝置都將看到一致的連結狀態，即使它們之間沒有防火牆。如果您不選取此選項，Virtual Wire 間不會傳播連結狀態。
7. 按一下 **OK**（確定）以儲存 Virtual Wire 物件。

STEP 3 | 確定 Virtual Wire 介面的連結速度。

1. 在同一個乙太網路介面上，選取 **Advanced**（進階），並記錄或變更 **Link Speed**（連結速度）。連接埠類型決定了清單中可用的速度設定。依預設，銅線連接埠將設定為 **auto**（自動）交涉連結速度。這兩個 Virtual Wire 介面必須擁有相同的連結速度。
2. 按一下 **OK**（確定）以儲存乙太網路介面。

STEP 4 | 重複前述步驟以設定第二個 Virtual Wire 介面（此範例中為 **ethernet1/4**）。

選取您建立的 **Virtual Wire** 物件時，防火牆會自動將第二個 Virtual Wire 介面新增為 **Interface2**（介面 **2**）。

STEP 5 | 為每個 Virtual Wire 介面建立單獨的安全性區域。

1. 選取 **Network**（網路） > **Zones**（區域），然後 **Add**（新增） 區域。
2. 輸入區域的 **Name**（名稱）（例如 **`internet`**）。
3. 對於 **Location**（位置），選取要套用該區域的虛擬系統。
4. 對於 **Type**（類型），選取 **Virtual Wire**。
5. **Add**（新增）屬於該區域的 **Interface**（介面）。
6. 按一下 **OK**（確定）。

STEP 6 | （選用）建立安全性原則規則，以允許 Layer 3 流量透傳。

若要允許 Layer 3 流量通過 Virtual Wire，可建立安全性原則規則，以允許從使用者區域到網際網路區域的流量，再建立另一個規則，允許從網際網路區域到使用者區域的流量，然後選取您要允許的應用程式，例如 BGP 或 OSPF。

STEP 7 | （選用）啟用 IPv6 防火牆。

如果您要將安全性原則規則套用至到達 Virtual Wire 的 IPv6 流量，則啟用 IPv6 防火牆。否則，IPv6 流量將以透明方式轉送。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 選取 **Enable IPv6 Firewalling**（啟用 **IPv6** 防火牆）。
3. 按一下 **OK**（確定）。

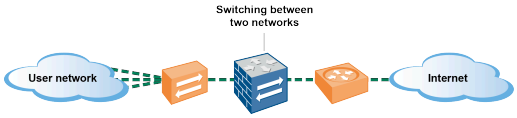
STEP 8 | **Commit**（提交）您的變更。

STEP 9 | （選用）設定 LLDP 設定檔，並將其套用至 Virtual Wire 介面（請參閱 設定 LLDP）。

STEP 10 | （選用）將非 IP 通訊協定控制套用至 Virtual Wire 區域（設定通訊協定保護）。否則，所有非 IP 流量都將透過 Virtual Wire 轉送。

Layer 2 介面

在 Layer 2 部署中，防火牆可在二或多個網路之間交換。裝置將連線至 Layer 2 區段；防火牆將框架轉送至相應連接埠（該連接埠與框架中識別的 MAC 位址關聯）。當需要交換時，設定 Layer 2 介面。



如果您正在 ***Cisco TrustSec*** 網路中使用安全性群組標籤 ***(SGT)***，最佳做法是在 ***Layer 2*** 或虛擬連接模式中部署內嵌防火牆。***Layer 2*** 或虛擬連接模式中的防火牆可以檢查已標記流量並提供威脅防禦。

下列主題介紹了您可以為所需的各種類型部署設定的不同類型的 Layer 2 介面，包括關於如何使用虛擬 LAN (VLAN) 隔離不同群組流量和原則的詳細資料。另一主題介紹了防火牆會如何重寫 Cisco per-VLAN 擴展樹 (PVST+) 或 Rapid PVST+ 橋接通訊協定資料單位 (BPDU) 中的輸入連接埠 VLAN ID 號碼。

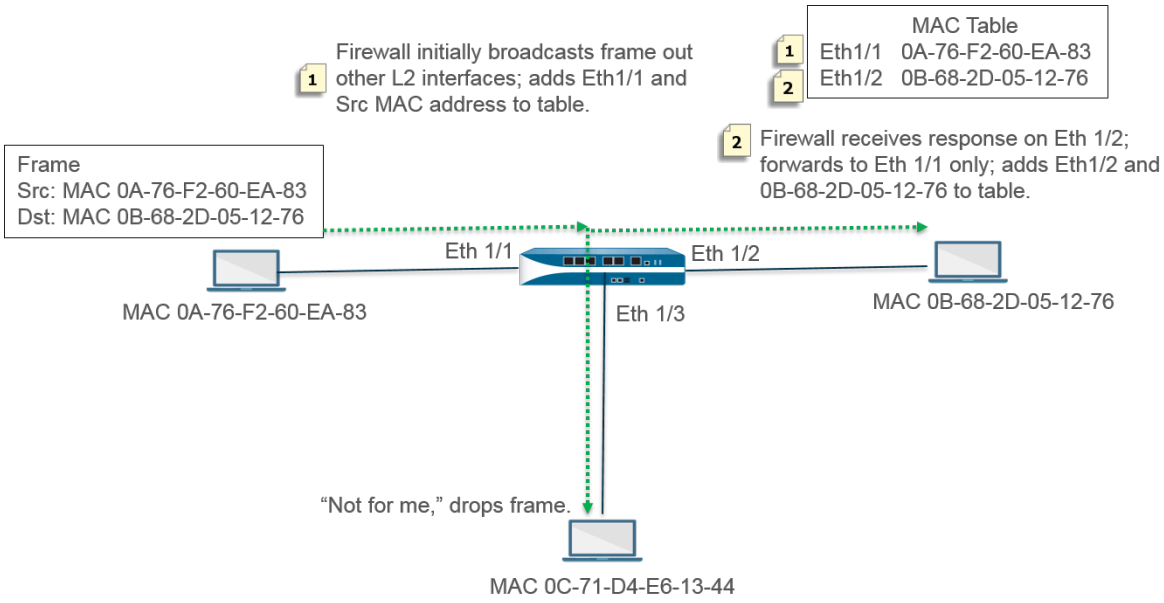
- 不帶 VLAN 的 Layer 2 介面
- 帶 VLAN 的 Layer 2 介面
- 設定 Layer 2 介面
- 設定 Layer 2 介面、子介面和 VLAN
- 管理 Per-VLAN 擴展樹 (PVST+) BPDU 重寫

不帶 VLAN 的 Layer 2 介面

在防火牆上設定 Layer 2 介面，以便其可以用作 Layer 2 網路中（而非在網路邊緣）的交換器。Layer 2 主機在地理位置上可能相互靠近並屬於單一廣播網域。當您為安全性區域指派了介面並對區域套用安全性規則後，防火牆將在 Layer 2 主機之間提供安全性。

在 OSI 型號的 Layer 2 上，主機將透過交換框架的方式，與防火牆通訊以及其他主機相互通訊。框架中包含了乙太網路標頭，其中帶有來源和目的地媒體存取控制 (MAC) 位址（實體硬體位址）。MAC 位址為 48 位元十六進位數字，格式為六個八位元，由冒號或連字號分隔（例如 00-85-7E-46-F1-B2）。

下圖中有一個帶三個 Layer 2 介面的防火牆，每個介面都以一一對應的方式連線一個 Layer 2 主機。



防火牆首先由一個空白的 MAC 表。當來源位址為 0A-76-F2-60-EA-83 的主機向防火牆傳送框架時，防火牆的 MAC 表中沒有目的地位址 0B-68-2D-05-12-76，因此防火牆不知道將框架轉送至哪個介面；所以，防火牆將該框架廣播至所有 Layer 2 介面。防火牆將來源位址 0A-76-F2-60-EA-83 和關聯的 Eth1/1 新增至其 MAC 表。

主機 0C-71-D4-E6-13-44 的收到了廣播，但目的地 MAC 並不是其 MAC 位址，因此它丟棄了封包。

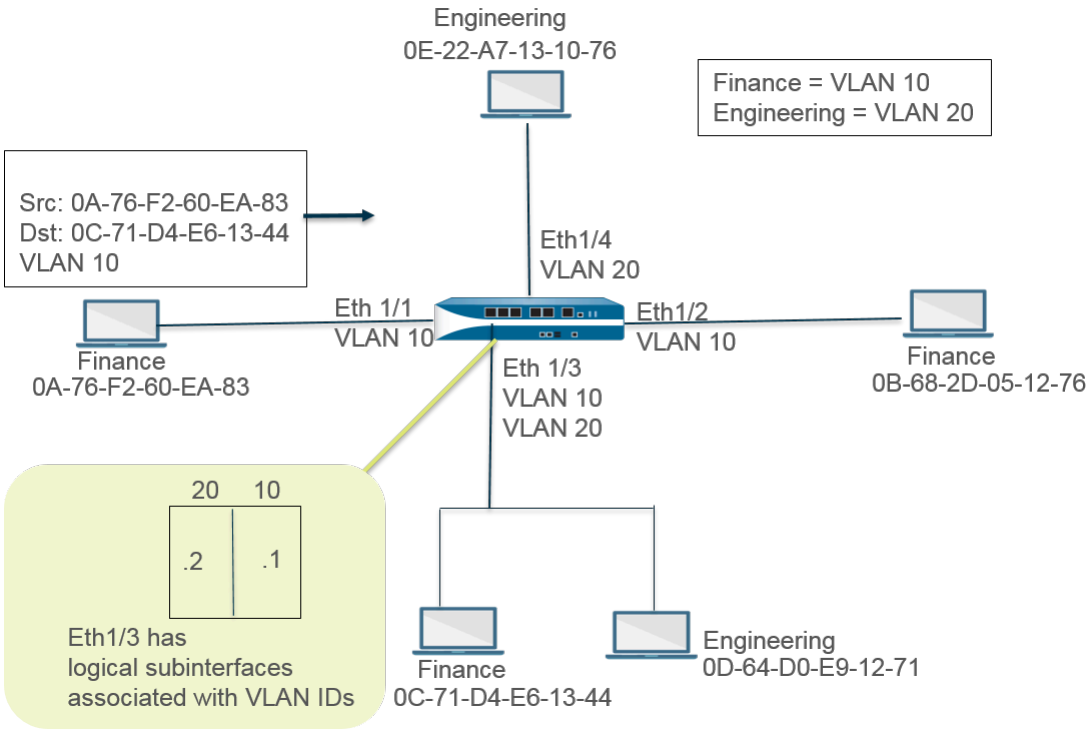
接收介面 Ethernet 1/2 將框架轉送至其主機。當主機 0B-68-2D-05-12-76 回應時，將使用目的地位址 0A-76-F2-60-EA-83；防火牆將 Ethernet 1/2 新增至其 MAC 表，作為連線 0B-68-2D-05-12-76 的介面。

帶 VLAN 的 Layer 2 介面

當您的組織希望將 LAN 分割成單獨的虛擬 LAN (VLAN) 以隔離不同部門的流量和原則時，您可以按邏輯方式將 Layer 2 主機分組成 VLAN，從而將 Layer 2 網路區段分割成多個廣播網域。例如，您可以為財務部和工程部建立 VLAN。為此，您需設定 Layer 2 介面、子介面和 VLAN。

防火牆將用作交換器以轉送帶有乙太網路標頭（其中包含有 VLAN ID）的框架，目的地介面必須有具有該 VLAN ID 的子介面，才能接受該框架並將其轉送至主機。您可以在防火牆上設定一個 Layer 2 介面，並為該介面設定一個或多個邏輯子介面，每一個均帶有 VLAN 標籤 (ID)。

在下圖中，防火牆有四個 Layer 2 介面，它們連線至屬於組織內不同部門的 Layer 2 主機。乙太網路介面 1/3 設定有子介面 .1（標記為 VLAN 10）和 .2（標記為 VLAN 20），因此該區段上有兩個廣播網域。VLAN 10 中的主機屬於財務部；VLAN 20 中的主機屬於工程部。



在此範例中，MAC 位址為 0A-76-F2-60-EA-83 的主機將帶有 VLAN ID 10 的框架傳送至防火牆，然後由防火牆廣播至其他 L2 介面。乙太網路介面 1/3 將接受框架，因為它連線至目的地位址為 0C-71-D4-E6-13-44 的主機，並且其子介面 .1 被指派了 VLAN 10。乙太網路介面 1/3 將框架轉送至財務部的主機。

設定 Layer 2 介面

但您需要 Layer 2 交換並且不需要分隔各 VLAN 的流量時，設定不帶 VLAN 的 Layer 2 介面。

STEP 1 | 設定 Layer 2 介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取介面。**Interface Name**（介面名稱）為固定值，如 ethernet1/1。
2. 對於 **Interface Type**（介面類型），選取 **Layer2**。
3. 選取 **Config**（組態）頁籤，將介面指派給 **Security Zone**（組態）或建立 **New Zone**（新區域）。
4. 在防火牆上建立額外的 Layer 2 介面，連線至其他 Layer 2 主機。

STEP 2 | 提交。

按一下 **OK**（確定）與 **Commit**（提交）。

設定 Layer 2 介面、子介面和 VLAN

但您需要 Layer 2 交換並且需要分隔各 VLAN 的流量時，設定帶 VLAN 的 Layer 2 介面。您可以選擇性地控制 Layer 2 介面上安全性區域之間或 Layer 2 VLAN 上單一區域內介面之間的非 IP 通訊協定。

STEP 1 | 設定 Layer 2 介面和子介面並指派 VLAN ID。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取介面。**Interface Name**（介面名稱）為固定值，如 ethernet1/1。
2. 對於 **Interface Type**（介面類型），選取 **Layer2**。
3. 選取 **Config**（組態）頁籤。
4. 對於 **VLAN**，保留設定 **None**（無）。
5. 將介面指派給 **Security Zone**（安全性區域）或建立 **New Zone**（新區域）。
6. 按一下 **OK**（確定）。
7. 對於反白顯示的乙太網路介面，按一下 **Add Subinterface**（新增子介面）。
8. **Interface Name**（介面名稱）仍為固定值。一段時間後，輸入子介面號碼（範圍為 1 至 9999）。
9. 輸入 VLAN 標籤 ID，範圍為 1 至 4094。
10. 將子介面指派給 **Security Zone**（安全性區域）。
11. 按一下 **OK**（確定）。

STEP 2 | 提交。

按一下 **Commit**（交付）。

STEP 3 | （選用）套用具有通訊協定保護的區域保護設定檔，以控制 Layer 2 區域之間（或 Layer 2 區域內的介面之間）的非 IP 通訊協定封包。

設定通訊協定保護。

管理 Per-VLAN 擴展樹 (PVST+) BPDU 重寫

當為 Layer 2 部署設定防火牆介面時，防火牆將 Cisco per-VLAN 擴展樹 (PVST+) 或 Rapid PVST+ 橋接通訊協定資料單位 (BPDU) 中的輸入連接埠 VLAN ID (PVID) 號碼重寫至正確的輸出 VLAN ID 號碼並將 BPDU 轉送出去。從 PAN-OS 7.1 開始的預設行為允許防火牆在防火牆任意一端的 VLAN 中的 Cisco 交換器之間準確標記 Cisco 專有 PVST + 和 Rapid PVST + 框架，以便使用 Cisco PVST + 和 Rapid PVST + 的擴展樹迴圈偵測可以正常運行。防火牆不會參與擴展樹協定 (STP) 的選擇處理，且其他類型的擴展樹也沒有任何行為變更。

Cisco 交換器必須停用迴圈防護，以便在防火牆上正常使用 *PVST+* 或 *Rapid PVST+ BPDU* 重寫功能。

僅在 Layer 2 乙太網路與彙總乙太網路 (AE) 介面上支援該功能。防火牆支援 PVID 範圍為 1 到 4,094，原生 VLAN ID 為 1，以與 Cisco 原生 VLAN 實作相容。

為支援 PVST + BPDU 重寫功能，PAN-OS 支援 PVST + 原生 VLAN 的概念。傳送到原生 VLAN 或從原生 VLAN 接收的框架沒有使用與原生 VLAN 相等的 PVID 標籤。在同一 Layer 2 部署中，所有交換器和防火牆須具有相同的原生 VLAN，PVST + 才能正常運行。儘管 Cisco 原生 VLAN 預設為 vlan1，但 VLAN ID 可以是 1 之外的數字。

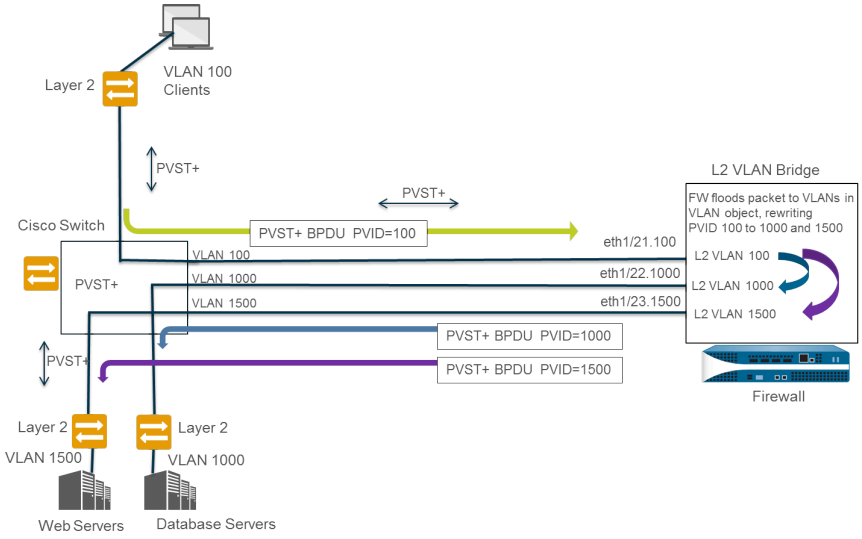
例如，防火牆設定有一個 VLAN 物件（名稱為 VLAN_BRIDGE），該物件說明屬於交換器或廣播網域的介面和子介面。在此示例中，VLAN 包括三個子介面：標籤為 100 的 ethernet1/21.100、標籤為 1000 的 ethernet1/22.1000 和標籤為 1500的 ethernet1/23.1500。

屬於 VLAN_BRIDGE 的子介面如下所示：

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

INTERFACE	INTERFACE TYPE	LINK STATE	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/21	Layer2		Untagged	none	none		Disabled
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust		Disabled
ethernet1/22	Layer2		Untagged	none	none		Disabled
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust		Disabled
ethernet1/23	Layer2		Untagged	none	none		Disabled
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management		Disabled

在下列圖形和說明中顯示了防火牆自動重寫 PVST + BPDU 的順序：



1. 屬於 VLAN 100 的 Cisco 交換器連接埠會把 PVST + BPDU（PVID 和 802.1Q VLAN 標籤設定為 100）傳送至防火牆。
2. 將防火牆介面和子介面設定為 Layer 2 介面類別。防火牆上的輸入子介面使用 VLAN 100 標籤，該 VLAN 與輸入 BPDU 的 PVID 和VLAN 標籤匹配，因此防火牆會接受該 BPDU。防火牆將 PVST + BPDU 爆流到屬於同一 VLAN 物件的所有其他介面（在此示例中為 ethernet1/22.1000 和 ethernet1/23.1500）。如果 VLAN 標籤不匹配，防火牆則會丟棄 BPDU。
3. 當防火牆透過其他介面（屬於同一 VLAN 物件）爆流出 BPDU 時，防火牆將重寫 PVID 和任何 802.1Q VLAN 標籤以匹配輸入介面的 VLAN 標籤。在此示例中，當 BPDU 周遊防火牆上的 Layer 2 橋時，防火牆會將一個子介面的 BPDU PVID 由 100 重寫為 1000，將第二子介面由 100 重寫為 1500。
4. 每個 Cisco 交換器在輸入的 BPDU 上接收正確的 PVID 和 VLAN 標籤，並處理 PVST + 封包以偵測網路中可能存在的迴圈。

以下 CLI 操作命令使您可以管理 PVST + 和 Rapid PVST + BPDU。

全域停用或重新啟用 PVID 的 PVST + 和 Rapid PVST+ BPDU 重寫（預設值為啟用）。

set session rewrite-pvst-pvid <yes|no>

為防火牆設定原生 VLAN ID（範圍為 1 至 4,094；預設值為 1）。

如果在交換器上的原生 *VLAN ID* 為非 *1* 的值，您必須將防火牆上的原生 *VLAN ID* 設定相同的數字；否則，防火牆會將會丟棄具有該 *VLAN ID* 的封包。這適用於幹線和非幹線介面。

set session pvst-native-vlan-id <*vid*>

丟棄所有 STP BPDU 封包。

set session drop-stp-packet <yes|no>

您可能要丟棄所有 STP BPDU 封包原因的示例：

- 如果防火牆的兩端只有一個交換器，而交換器之間沒有其他連線會導致迴圈，則不需要 STP，並且可以在交換器上將其停用 STP 或被防火牆封鎖。
- 如果存在不正常的 STP 交換器不適當的爆流 BPDU，則您可以在防火牆處停止 STP 封包以防止 BPDU 爆流。

驗證是否已啟用 PVST + BPDU 重寫，視閱 PVST 原生 VLAN ID，並確定防火牆是否正在丟棄所有 STP BPDU 封包。

show vlan all

```
pvst+ tag rewrite: disabled
pvst native vlan id:     5
drop stp:                disabled
total vlans shown:       1
名稱       介面              虛擬介面
bridge    ethernet1/1
          ethernet1/2
          ethernet1/1.1
          ethernet1/2.1
```

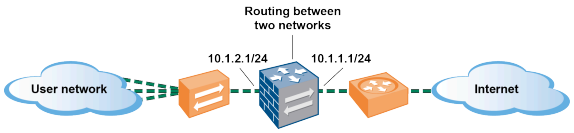
疑難排解 PVST+ BPDU 錯誤。

show counter global

查看 **flow_pvid_inconsistent**的計數器，該計數器計算 PVST + BPDU 封包中的 802.1Q 標籤和 PVID 欄位不匹配的次數。

Layer 3 介面

在 Layer 3 部署中，防火牆可在多個連接埠之間路由流量。您必須先設定您希望防火牆用於為每個 Layer 3 介面路由流量的虛擬路由器，然後方可設定 Layer 3 介面。



如果您正在 *Cisco TrustSec* 網路中使用安全性群組標籤 *(SGT)*，最佳做法是在 *Layer 2* 或虛擬連接模式中部署內嵌防火牆。但是，如果您需要在 *Cisco TrustSec* 網路中使用 *Layer 3* 防火牆，則應在兩個 *SGT* 交換通訊協定 *(SXP)* 對等體之間部署 *Layer 3* 防火牆，並部署防火牆以允許 *SXP* 對等體之間的流量。

下列主題介紹了如何設定 Layer 3 介面以及如何使用芳鄰探索通訊協定 (NDP) 來提供 IPv6 主機並檢視本機網路連結上裝置的 IPv6 位址以快速定位裝置。

- 設定 Layer 3 介面
- 使用 NDP 管理 IPv6 主機

設定 Layer 3 介面

需按照下列程序為 Layer 3 介面（乙太網路、VLAN、回送和通道介面）設定 IPv4 或 IPv6 位址，以便防火牆能夠在這些介面上執行路由。如果使用通道進行路由或者開啟了通道監控，則通道也需要一個 IP 位址。在執行下列工作之前，先定義一個或多個虛擬路由器。

您一般要使用下列程序設定用於連線網際網路的外部介面和用於連線內部網路的介面。您可以在單個介面上設定 IPv4 和 IPv6 位址。

PAN-OS 防火牆最多支援為實體或虛擬 *Layer 3* 介面指派 *16000* 個 *IP* 位址；其中包括 *IPv4* 和 *IPv6* 位址。

如果使用 IPv6 路由，則可以設定防火牆提供 DNS 設定的 IPv6 路由器宣告。防火牆將為 IPv6 DNS 用戶端提供遞迴 DNS 伺服器 (RDNS) 位址和 DNS 搜尋清單，以便用戶端能夠解析 IPv6 DNS 要求。因此，防火牆將為您起到類似於 DHCPv6 伺服器的作用。

STEP 1 | 選取介面，並為其設定一個安全性區域。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路）、**VLAN**、**loopback**（乙太網路） 或 **Tunnel**（通道），具體視乎您需要的介面類型。
2. 選取要設定的介面。
3. 選取 **Interface Type**（通道）—**Layer3**。
4. 在 **Config**（通道）頁籤上，選取**Virtual Router**（虛擬路由器），然後選取要設定的虛擬路由器，例如 **default**（預設）。
5. 對於 **Virtual System**（虛擬系統），選取您要設定的虛擬系統（如果是多虛擬系統防火牆）。
6. 對於 **Security Zone**（安全性區域），選取介面所屬的區域或建立 **New Zone**（新區域）。
7. 按一下 **OK**（確定）。

STEP 2 | 為介面設定 IPv4 位址。

您可以透過下列三種方式為 Layer 3 介面指派 IPv4 位址：

- 靜態
- DHCP 用戶端—防火牆介面用作 DHCP 用戶端，接收動態指定的 IP 位址。防火牆也能夠將 DHCP 用戶端介面所接收的設定傳播到防火牆上運作的 DHCP 伺服器。這最常用於將網際網路服務供應商的 DNS 伺服器設定傳播到防火牆所保護的網路上運作的用戶端機器。
- PPPoE—將介面設定為乙太網路上的點對點通訊協定 (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。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路）、**VLAN**、**loopback**（乙太網路） 或 **Tunnel**（通道），具體視乎您需要的介面類型。
2. 選取要設定的介面。
3. 若要為介面設定靜態 IPv4 位址，可在 **IPv4** 頁籤上，將 **Type**（類型）設定為 **Static**（靜態）。
4. **Add**（新增）**Name**（名稱），然後選擇性地輸入位址的 **Description**（描述）。
5. 對於 **Type**（類型），選取以下任何項：
   - **IP** 網路遮罩—輸入 IP 位址及網路遮罩以指派給介面，例如 208.80.56.100/24。

     如果您為 *Layer 3* 介面位址使用 */31* 子網路遮罩，則必須使用 *.1/31* 位址設定介面，以使 *ping* 等公用程式正常運作。

     如果您設定 *IPv4* 位址回送介面，則必須使用 */32* 子網路遮罩；例如，*192.168.2.1/32*。
   - **IP** 範圍—輸入 IP 位址範圍，例如 192.168.2.1-192.168.2.4。
   - **FQDN**—輸入完整網域名稱。
6. 選取要套用到位址的 **Tags**（標籤）。
7. 按一下 **OK**（確定）。

STEP 3 | 為介面設定乙太網路上的點對點通訊協定 (PPPoE)。請參閱 Layer 3 介面。

HA 主動/主動模式不支援 *PPPoE*。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路）、**VLAN**、**loopback**（回送） 或 **Tunnel**（通道）。
2. 選取要設定的介面。
3. 在 **IPv4** 頁籤上，將 **Type**（類型）設定為 **PPPoE**。
4. 在 **General**（類型）頁籤上，選取 **Enable**（啟用），以為 PPPoE 終止啟用介面。
5. 輸入點對點連線的 **Username**（使用者名稱）。
6. 輸入使用者名稱的 **Password**（密碼），然後 **Confirm Password**（確認密碼）。
7. 按一下 **OK**（確定）。

STEP 4 | 將介面設定為 DHCP 用戶端 以接收動態指派的 IPv4 位址。

HA 主動/主動模式不支援 *DHCP* 用戶端。

STEP 5 | 為介面設定靜態 IPv6 位址。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路）、**VLAN**、**loopback**（回送） 或 **Tunnel**（通道）。
2. 選取要設定的介面。
3. 在 **IPv6** 頁籤上，選取**Enable IPv6 on the interface**（在介面上啟用 **IPv6**），以在介面上啟用 IPv6 定址。
4. 對於 **Interface ID**（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。
5. **Add**（新增）IPv6 **Address**（位址），或選取位址群組。
6. 選取**Enable address on interface**（啟用介面上的位址），以在介面上啟用 IPv6 位址。
7. 選取 **Use interface ID as host portion**（使用介面 **ID** 作為主機部分），以將 Interface ID（介面 ID）作為 IPv6 位址的主機部分。
8. （選用）選取 **Anycast**（任意傳送），使 IPv6 位址（路由） 成為任意傳送位址（路由），這意味著多個位置可以宣告相同的首碼，IPv6 會將任意傳送流量傳送至其認為最近的節點（根據路由通訊協定的成本和其他因素）。
9. （僅限乙太網路介面）選取 **Send Router Advertisement**（傳送路由器宣告）(RA)，以使防火牆能夠在路由器宣告中傳送此位址，在這種情況下，您還必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器宣告）選項（下一個步驟）。
10. （僅限乙太網路介面）輸入 **Valid Lifetime (sec)**（有效存留期（秒））， 在其期間內，防火牆將認為位址有效。有效存留期必須等於或超過 **Preferred Lifetime (sec)**（偏好存留期（秒）） （預設值為 2592000）。
11. （僅限乙太網路介面）輸入有效地址的 **Preferred Lifetime (sec)**（偏好存留期（秒）），這意味在此期間內，防火牆可使用該位址來傳送和接收流量。當偏好存留期到期後，防火牆就無法使用位址來建立新連線，但在 **Valid Lifetime**（有效存留期）到期前，任何現有連線仍然有效（預設值為 604800）。
12. （僅限乙太網路介面）如果系統擁有在不使用路由器就能連線的位址（首碼內），則選取 **On-link**（記錄連結）。
13. （僅限乙太網路介面）如果系統可結合宣告的首碼與介面 ID 來獨立建立 IP 位址，則選取 **Autonomous**（自發）。
14. 按一下 **OK**（確定）。

STEP 6 | （僅限使用 IPv6 的乙太網路或 VLAN 介面）允許防火牆從介面傳送 IPv6 路由器宣告 (RA)，可以調整 RA 參數。

可出於下列原因而調整 *RA* 參數：與使用不同值的路由器/主機互操作。當存在多個閘道時實現快速聚合。例如，設定更小的 ***Min Interval***（最小間隔）、***Max Interval***（最大間隔）和***Router Lifetime***（路由器生命週期），以便 *IPv6* 用戶端/主機能夠在主要閘道失效時快速變更預設閘道並開始轉送至網路中的其他預設閘道。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **IPv6**。
4. 選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。
5. 在 **Router Advertisement**（在介面上啟用 **IPv6**）頁籤上，選取 **Enable Router Advertisement**（啟用路由器宣告）（預設為停用）。
6. （選用）設定 **Min Interval (sec)**（最小間隔（秒）），即防火牆所傳送的 RA 之間的最小間隔（範圍為 3-1350；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。
7. （選用）設定 **Max Interval (sec)**（最大間隔（秒）），即防火牆所傳送的 RA 之間的最大間隔（範圍為 4-1800；預設值為 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。
8. （選用）設定要套用至用於連出封包之用戶端的 **Hop Limit**（躍點限制）（範圍為 1-255；預設值為 64）。輸入 0 代表無躍點限制。
9. （選用）設定 **Link MTU**（連結 **MTU**），即要套用至用戶端的連結最大傳輸單元 (MTU)（範圍為 1280-9192；預設值為 **unspecified**（未指定））。選取 **unspecified**（未指定），不設定連結 MTU。
10. （選用）設定 **Reachable Time (ms)**（可連線時間（毫秒）），即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**（未指定）表示沒有可連線時間值（範圍是 0-3,600,000，預設為 **unspecified**（未指定））。
11. （選用）設定 **Retrans Time (ms)**（重新傳輸時間（毫秒）），即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的重新傳輸計時器。選取 **Unspecified**（未指定）表示沒有重新傳輸時間（範圍是 0-4,294,967,295，預設為 **unspecified**（未指定））。
12. （選用）設定 **Router Lifetime (sec)**（路由器生命週期（秒）），即用戶端將防火牆作為預設閘道的時間長度（範圍為 0-9000；預設值為 1800）。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。
13. 設定 **Router Preference**（路由器偏好設定），如果網路區段中有多個 IPv6 路由器，用戶端將按此設定來選擇偏好的路由器。**High**（高）、**Medium**（中）（預設值）或

Low（低）是 RA 宣告的優先順序，表示防火牆虛擬路由器相對於區段內其他路由器的優先順序。

14. 選取 **Managed Configuration**（受管理組態），向用戶端指示位址可透過 DHCPv6 提供。
15. 選取 **Other Configuration**（其他組態），向用戶端指示可透過 DHCPv6 取得其他位址資訊（例如，DNS 相關設定）。
16. 選取 **Consistency Check**（一致性檢查），讓防火牆驗證其他路由器傳送的 RA 宣告的連結資訊是否一致。防火牆會記錄任何不一致情況。
17. 按一下 **OK**（確定）。

STEP 7 | （僅限使用 IPv6 位址的乙太網路或 VLAN 介面）指定防火牆將在來自此介面的 ND 路由器宣告中宣告的遞迴 DNS 伺服器位址和 DNS 搜尋清單。

RDNS 伺服器和 DNS 搜尋清單是 DNS 用戶端 DNS 組態的一部分，使用戶端能夠解析 IPv6 DNS 要求。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **IPv6** > **DNS Support**（**DNS** 支援）。
4. 在路由器宣告中包含 **DNS** 資訊，以使防火牆傳送 IPv6 DNS 資訊。
5. 對於 DNS **Server**（伺服器），**Add**（新增）遞迴 DNS 伺服器的 IPv6 位址。最多可 **Add**（新增）八個遞迴 DNS 伺服器。防火牆將在 ICMPv6 路由器宣告中，按從上到下的順序傳送伺服器位址。
6. 以秒為單位指定 **Lifetime**（存留期），在此期間，用戶端可使用特定 RDNS 伺服器解析網域名稱。
   - **Lifetime**（存留期）介於您在 **Router Advertisement**（路由器宣告）頁籤上設定的**Max Interval**（最大間隔）和兩倍 **Max Interval**（最大間隔）之間。例如，如果最大間隔為 600 秒，則存留期範圍為 600-1200 秒。
   - 預設 **Lifetime**（存留期）為 1200 秒。
7. 對於 DNS 尾碼，**Add**（新增）一個 **DNS Suffix**（**DNS** 尾碼）（網域名稱最大為 255 位元組）。最多可 **Add**（新增）八個 DNS 尾碼。防火牆將在 ICMPv6 路由器宣告中，按從上到下的順序傳送尾碼。
8. 以秒為單位指定 **Lifetime**（存留期），在此期間，用戶端可使用尾碼。此存留期的範圍和默認值與 **Server**（伺服器）相同。
9. 按一下 **OK**（確定）。

STEP 8 | （乙太網路或 VLAN 介面）指定靜態 ARP 項目。靜態 ARP 項目降低 ARP 處理。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **Advanced**（進階） > **ARP Entries**（**ARP** 項目）。
4. **Add**（新增）**IP Address**（**IP** 位址）及其對應的 **MAC Address**（**MAC** 位址）（硬體或媒體存取控制位址）。對於 VLAN 介面， 您還必須選取 **Interface**（介面）。

   靜態 *ARP* 項目不逾時。預設狀態下，快取中的自動學習 *ARP* 項目逾時 *1,800* 秒；您可自訂 *ARP* 快取逾時；請參閱設定工作階段逾時值。
5. 按一下 **OK**（確定）。

STEP 9 | （乙太網路或 VLAN 介面）指定靜態芳鄰探索通訊協定 (NDP) 項目。適用於 IPv6 的 NDP 執行的功能，與適用於 IPv4 的 ARP 所提供的功能類似。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **Advanced**（進階） > **ND Entries**（**ND** 項目）。
4. **Add**（新增）**IPv6 Address**（**IPv6** 位址）及其對應的 **MAC Address**（**MAC** 位址）。
5. 按一下 **OK**（確定）。

STEP 10 | （選用）在介面上啟用服務。

1. 若要在介面上啟用服務，可選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **Advanced**（進階） > **Other Info**（其他資訊）。
4. 展開 **Management Profile**（管理設定檔）清單，選取設定檔或 **New Management Profile**（新建管理設定檔）。
5. 輸入設定檔的 **Name**（名稱）。
6. 對於 **Permitted Services**（允許的服務），選取服務，例如 **Ping**（偵測），然後按一下 **OK**（確定）。

STEP 11 | **Commit**（提交）您的變更。

STEP 12 | 用纜線連接介面。

將直通式纜線從設定的介面中連接至各網路區段上對應的交換器或路由器。

STEP 13 | 確認介面是否工作。

在 Web 介面中選取 **Network**（網路） > **Interfaces**（介面），然後確認 Link State（連結狀態）欄中的圖示是否為綠色。您也可從 **Dashboard**（儀表板）上的 **Interfaces**（介面）Widget 中監控連結狀態。

STEP 14 | 設定靜態路由和/或動態路由通訊協定（RIP、OSPF 或 BGP），以便虛擬路由能夠路由流量。

- 設定靜態路由
- RIP
- OSPF
- BGP

STEP 15 | 設定預設路由。

設定靜態路由，並將其設定為預設路由。

使用 NDP 管理 IPv6 主機

本主題介紹了如何使用 NDP 提供 IPv6 主機；您因此將不再需要單獨的 DHCPv6 伺服器。其中還介紹了如何使用 NDP 監控 IPv6 位址，以便您快速追蹤違反安全性規則的裝置及相關使用者的 IPv6 和 MAC 位址。

- DNS 組態的 IPv6 路由器宣告
- 為 IPv6 路由器宣告設定 RDNS 伺服器和 DNS 搜尋清單
- NDP 監控
- 啟用 NDP 監控

DNS 組態的 IPv6 路由器宣告

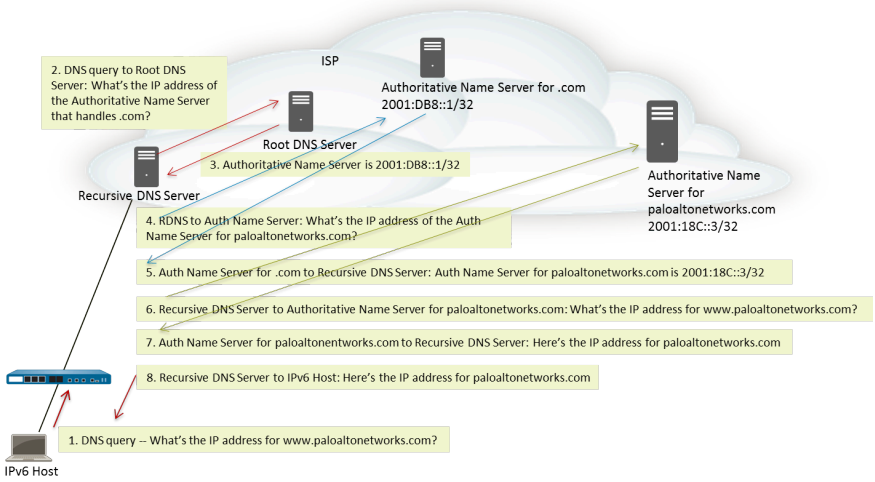
防火牆對芳鄰探索 (ND) 的實作得到增強，因此您可以按照 RFC 6106 DNS 組態的 IPv6 路由器宣告選項為 IPv6 主機提供遞迴 DNS 伺服器 (RDNSS) 選項和 DNS 搜尋清單 (DNSSL) 選項。在設定 Layer 3 介面 時，可在防火牆上設定這些 DNS 選項，以便防火牆能夠提供 IPv6 主機；因此您無需 DHCPv6 伺服器即可提供主機。防火牆將傳送 IPv6 路由器宣告 (RA)，其中包含了作為 DNS 組態一部分的 IPv6 主機，以使它們能夠正常連線網際網路服務。因此，將為 IPv6 主機設定：

- 可解析 DNS 查詢的 RDNS 伺服器位址。
- DNS 用戶端在輸入網域名稱到 DNS 查詢之前附加至不完整網域名稱（一次一個）的網域名稱清單（尾碼）。

所有 PAN-OS 平台上的乙太網路介面、子介面、彙總乙太網路介面以及 Layer 3 VLAN 介面均支援 DNS 組態的 IPv6 路由器宣告。

由於能夠傳送 ***DNS*** 組態的 ***IPv6 RA***，因此防火牆起到了與 ***DHCP*** 類似的作用，而且與作為 ***DNS Proxy***、***DNS*** 用戶端或 ***DNS*** 伺服器的防火牆不相關。

為防火牆設定了 RDNS 伺服器的位址後，防火牆將為 IPv6 主機（DNS 用戶端）提供這些位址。IPv6 主機將使用其中一個或多個位址連線 RDNS 伺服器。遞迴 DNS 伺服器是指 RDNS 伺服器的一系列 DNS 要求，即下圖中所示的三對查詢與回應。例如，當使用者嘗試存取 www.paloaltonetworks.com 時，本機瀏覽器會發現快取中沒有該網域名稱的 IP 位址，用戶端的作業系統中也沒有。用戶端的作業系統向屬於本機 ISP 的遞迴 DNS 伺服器發起 DNS 查詢。



IPv6 路由器宣告中可能包含多個 DNS 遞迴伺服器位址選項，每一個都有相同或不同的存留時間。單一 DNS 遞迴 DNS 伺服器位址選項可能包含多個遞迴 DNS 伺服器位址，只要這些位址具有相同的存留時間。

DNS 搜尋清單是一個包含了防火牆向 DNS 用戶端宣告的網域名稱（尾碼）的清單。防火牆將向 DNS 用戶端提供該清單，以在其不完整 DNS 查詢中使用尾碼。DNS 用戶端會在輸入名稱到 DNS 查詢之前，將尾碼附加（一次一個）至不完整網域名稱，從而在 DNS 查詢中使用完整網域名稱 (FQDN)。例如，如果所設定 DNS 用戶端的使用者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，則用戶端會將清單中的第二個 DNS 尾碼附加至不完整名稱並傳輸新的 DNS 查詢。用戶端會按順序使用 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。

您可以為防火牆設定您希望向 ND DNSSL 選項中 DNS 用戶端路由器的尾碼；接收 DNS 搜尋清單選項的 DNS 用戶端會在其不完整 DNS 查詢中使用這些尾碼。

若要指定 RDNS 伺服器和 DNS 搜尋清單，需為 IPv6 路由器宣告設定 RDNS 伺服器和 DNS 搜尋清單。

為 IPv6 路由器宣告設定 RDNS 伺服器和 DNS 搜尋清單

執行此工作，以設定 IPv6 主機之 DNS 設定的 IPv6 路由器宣告。

STEP 1 | 啟用防火牆以從介面傳送 IPv6 路由器宣告。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取要設定的介面。
3. 在 **IPv6** 頁籤上，選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。
4. 在 **Router Advertisement**（路由器宣告）頁籤上，選取 **Enable Router Advertisement**（啟用路由器宣告）。
5. 按一下 **OK**（確定）。

STEP 2 | 指定防火牆將在來自此介面的 ND 路由器宣告中宣告的遞迴 DNS 伺服器位址和 DNS 搜尋清單。

RDNS 伺服器和 DNS 搜尋清單是 DNS 用戶端 DNS 組態的一部分，使用戶端能夠解析 IPv6 DNS 要求。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **IPv6** > **DNS Support**（**DNS** 支援）。
4. 在路由器宣告中包含 **DNS** 資訊，以使防火牆傳送 IPv6 DNS 資訊。
5. 對於 DNS **Server**（伺服器），**Add**（新增）遞迴 DNS 伺服器的 IPv6 位址。最多可 **Add**（新增）八個遞迴 DNS 伺服器。防火牆將在 ICMPv6 路由器宣告中，按從上到下的順序傳送伺服器位址。
6. 以秒為單位指定 **Lifetime**（存留期），在此期間，用戶端可使用特定 RDNS 伺服器解析網域名稱。
   - **Lifetime**（存留期）介於您在 **Router Advertisement**（路由器宣告）頁籤上設定的**Max Interval**（最大間隔）和兩倍 **Max Interval**（最大間隔）之間。例如，如果最大間隔為 600 秒，則存留期範圍為 600-1200 秒。
   - 預設 **Lifetime**（存留期）為 1200 秒。
7. 對於 DNS 尾碼，**Add**（新增）一個 **DNS Suffix**（**DNS** 尾碼）（網域名稱最大為 255 位元組）。最多可 **Add**（新增）八個 DNS 尾碼。防火牆將在 ICMPv6 路由器宣告中，按從上到下的順序傳送尾碼。
8. 以秒為單位指定 **Lifetime**（存留期），在此期間，用戶端可使用尾碼。此存留期的範圍和默認值與 **Server**（伺服器）相同。
9. 按一下 **OK**（確定）。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

NDP 監控

IPv6 (RFC 4861) 的芳鄰探索通訊協定 (NDP) 執行的功能類似於 IPv4 的 ARP 功能。依預設，防火牆會執行 NDP，利用 ICMPv6 封包探索並追蹤所連線之連結上芳鄰的連結層位址和狀態。

啟用 NDP 監控 因此，您可以檢視本機網路連結上裝置的 IPv6 位址、其 MAC 位址、User-ID 中的關聯使用者名稱（如果裝置使用者使用目錄服務登入）、位址的可連線狀態以及上次報告 NDP 監控器收到來自此 IPv6 位址的路由器宣告的日期和時間。該使用者名稱基於最佳情況；網路上的很多 IPv6 裝置可能沒有使用者名稱，例如印表機、傳真機、伺服器等。

如果您要快速追蹤違反了安全性規則的裝置和使用者，將 IPv6 位址、MAC 位址和使用者名稱顯示於一處將非常有用。您需要與 IPv6 位址對應的 MAC 位址，才能追蹤到 MAC 位址的來源實體交換器或存取點。

NDP 監控功能並不能保證探索所有裝置，因為在防火牆與用戶端之間可能存在其他網路裝置，篩選掉了 *NDP* 或重複位址偵測 *(DAD)* 訊息。防火牆僅能監控其已知存在於介面上的裝置。

NDP 監控功能還能監控來自於用戶端和芳鄰的重複位址偵測 (DAD) 封包。您還可以監控 IPv6 ND 日誌，便於進行疑難排解。

所有 PAN-OS 型號上的乙太網路介面、子介面、彙總乙太網路介面以及 VLAN 介面均支援 NDP 監控。

啟用 NDP 監控

執行此工作，為介面啟用 NDP 監控。

STEP 1 | 啟用 NDP 監控。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 選取您要設定的介面。
3. 選取 **IPv6**。
4. 選取 **Address Resolution**（位址群組）。
5. 選取 **Enable NDP Monitoring**（啟用 **NDP** 監控）。

   啟用或停用 *NDP* 監控後，必須 ***Commit***（提交），然後 *NDP* 監控才能啟動或停止。
6. 按一下 **OK**（確定）。

STEP 2 | Commit（提交）您的變更。

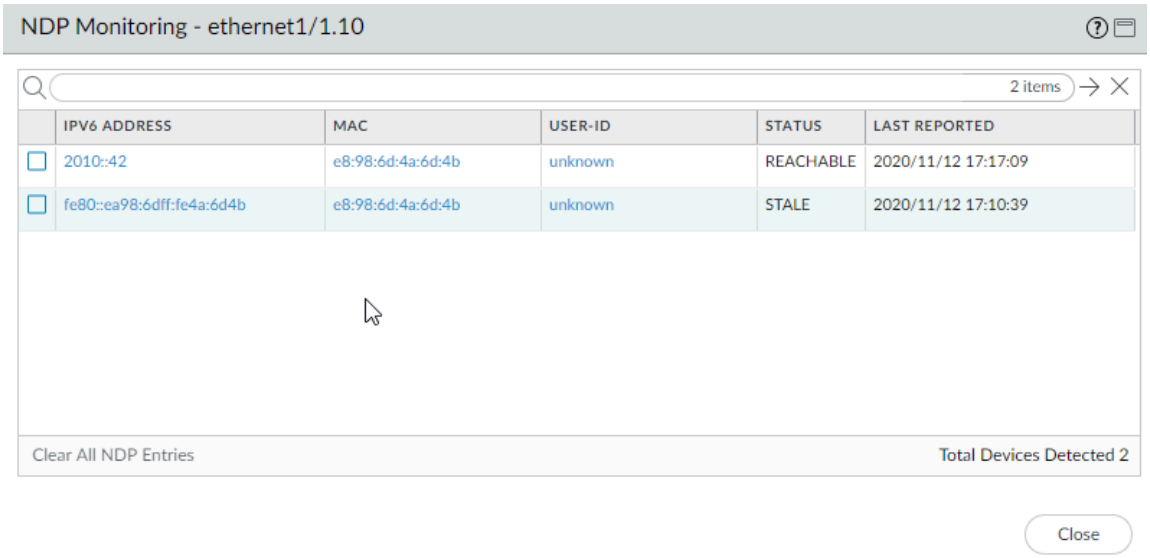
按一下 **Commit**（交付）。

STEP 3 | 監控來自用戶端和芳鄰的 NDP 和 DAD 封包。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取 **Ethernet**（乙太網路） 或 **VLAN**。
2. 對於啟用了 NDP 監控的介面，在 Features（功能）欄中，將滑鼠暫留在 NDP 監控 圖示上：

   介面的 NDP 監控摘要將顯示該介面將在路由器宣告 (RA)（如果 RA 已啟用）中傳送的 IPv6 **Prefixes**（首碼）清單（介面自己的 IPv6 首碼）。

   該摘要中還將顯示 DAD、路由器宣告以及 DNS 支援是否已啟用；是否已設定任何遞迴 DNS 伺服器的 IP 位址；是否已在 DNS 搜尋清單中設定任何 DNS 尾碼。
3. 按一下 NDP 監控圖示以顯示詳細資訊。



   介面的詳細 NDP 監控表中每一列都會顯示防火牆發現的芳鄰 IPv6 位址、相應的 MAC 位址、相應的使用者 ID（基於最佳情況）、位址的可連線狀態、上次報告此 NDP 監控器從此 IP 位址收到 RA 的日期和時間。對於印表機或其他並非基於使用者的主機，將不會顯示使用者 ID。根據 RFC 4861，若 IP 位址狀態為 Stale（過時），將不知道芳鄰是否可以連線。

   右下角為本機網路連結上 **Total Devices Detected**（偵測到的裝置總數）。

   - 在篩選欄位中輸入 IPv6 位址，搜尋要顯示的位址。
   - 選中核取方塊，以顯示或不顯示 IPv6 位址。
   - 按一下數字、右箭頭或左箭頭或垂直捲軸，以前進多個項目。
   - 按一下 **Clear All NDP Entries**（清除所有 **NDP** 項目），可清除整個表格。

STEP 4 | 監控 ND 日誌以便於報告。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **System**（系統）。
2. 在 Type（類型）欄中，檢視 **ipv6nd** 日誌及相應描述。

   例如，`inconsistent router advertisementreceived` 表示防火牆收到的 RA 與即將送出的 RA 不一致。

設定彙總介面群組

彙總介面群組使用 IEEE 802.1AX 連結彙總將多個 Ethernet 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防火牆。彙總介面群組透過在整合介面間實現流量負載平衡，可增加對等體間的頻寬。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。

依預設，則只會在直接連接的對等體間的實體層自動偵測介面失敗。但是，如果您啟用連結彙總控制通訊協定 (LACP)，將會在實體及資料連結層自動偵測介面失敗，無論是否直接連接對等體。如果您設定熱備援，則 LACP 還會啟用自動容錯轉移以備援介面。所有 Palo Alto Networks® 防火牆（VM-Series 除外）型號均支援彙總群組。產品選取工具指示每個防火牆支援的彙總群組數量）。每個彙總群組最多可擁有八個介面。

PAN-OS® 防火牆最多支援為實體或虛擬 Layer 3 介面指派 16000 個 IP 位址；其中包括 IPv4 和 IPv6 位址。

QoS 僅在前八個彙總群組上受支援。

設定彙總群組之前，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），但頻寬和介面類型必須相同。頻寬和介面類型選項包括：

- 頻寬—1Gbps、10Gbps、40Gbps 或 100Gbps。
- 介面類型—HA3、Wirtual Wire、Layer 2 或 Layer 3。

此程序說明僅適用於 *Palo Alto Networks* 防火牆的設定步驟。您還必須在對等體裝置上設定彙總群組。請參閱該裝置的文件以取得指示。

STEP 1 | 設定一般介面群組參數。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後 **Add Aggregate Group**（新增彙總群組）。
2. 在唯讀 **Interface Name**（介面名稱）旁的欄位中，輸入用來識別彙總群組的數字 (1-8)。
3. 對於 **Interface Type**（介面類型)，選取 **HA**、**Virtual Wire**、**Layer2** 或 **Layer3**。
4. 為您選取的 **Interface Type**（介面類型)設定剩餘參數。

STEP 2 | 進行 LACP 設定。

僅在您要為彙總群組啟用 LACP 時執行此步驟。

您無法為 *Virtual Wire* 介面啟用 *LACP*。

1. 先後選取 **LACP** 頁籤及 **Enable LACP**（啟用 LACP）。
2. 將 LACP 狀態查詢的 **Mode**（模式）設為 **Passive**（被動）（防火牆只回應 - 預設）或 **Active**（主動）（防火牆會查詢對等體裝置）。

   作為最佳作法，將一個 *LACP* 對等體設定為主動，將另一個 *LACP* 對等體設定為被動。如果兩個對等都是被動，*LACP* 將無法運作。防火牆無法偵測其對等體裝置的模式。
3. 將 LACP 查詢與回應交換的 **Transmission Rate**（傳輸速率）設定為 **Slow**（慢）（每 30 秒 - 預設）或 **Fast**（快）（每秒）。根據您的網路可以支援多少的 LACP 處理，以及 LACP 對等體偵測與解決介面失敗的速度有多快來選取。
4. 若您希望在不到一秒內啟用容錯轉移到備援介面，則選取 **Fast Failover**（快速容錯轉移）。依預設，該選項會被停用並且防火牆會使用 IEEE 802.1ax 標準來進行容錯轉移處理（需要至少三秒）。

   作為最佳作法，在標準容錯轉移間隔內可能遺失重要資料的部署中，請使用 ***Fast Failover***（快速容錯轉移）。
5. 輸入彙總群組中為使用中的 **Max Ports**（連接埠上限）（介面數）（1 至 8）。如果您指派給群組的介面數超過 **Max Ports**（連接埠上限），則剩餘的介面將處於待命模式。防火牆使用指派（步驟 3）給每個介面的 **LACP Port Priority**（**LACP** 連接埠優先順序）來決定一開始為使用中的介面，以及決定待命介面在容錯移轉時成為使用中介面的順序。如果 LACP 對等體具有不相符的連接埠優先順序值，則具有較低 **System Priority**（系統優先順序）號碼（預設為 32,768；範圍為 1 至 65,535）的對等體的值將取代另一個對等體。
6. （選用）僅針對主動/被動防火牆，如果您要為被動防火牆啟用 LACP 預交涉，則選取 **Enable in HA Passive State**（以 **HA** 被動狀態啟用）。LACP 預交涉可以加快對被動式防火牆的容錯移轉（詳細資訊，請參閱 主動/被動 HA 的 LACP 和 LLDP 預交涉）。

   如果您選取此選項，則無法選取 ***Same System MAC Address for Active-Passive HA***（主動-被動 ***HA*** 的系統 ***MAC*** 位址相同）；預交涉要求每個 *HA* 防火牆上具有唯一的介面 *MAC* 位址。
7. （選用）僅針對主動/被動防火牆，選取 **Same System MAC Address for Active-Passive HA**（主動-被動 **HA** 的系統 **MAC** 位址相同）並為兩個 HA 防火牆指定單一 **MAC Address**（**MAC** 位址）。如果 LACP 對等體此已虛擬化（在網路中顯示為單一裝置），此選項可將容錯移轉延遲降到最低。依預設，會停用此選項：HA 配對中的每個防火牆都有唯一的 MAC 位址。

   如果未虛擬化 *LACP* 對等體，則使用唯一的 *MAC* 位址，以將容錯移轉延遲降到最低。

STEP 3 | 按一下 **OK**（確定）。

STEP 4 | 指派介面給彙總群組。

對於將成為彙總群組成員的每個介面 (1-8) 執行下列步驟。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下相應介面名稱以進行編輯。
2. 將 **Interface Type**（介面類型）設定為 **Aggregate Ethernet**（彙總乙太網路）。
3. 選取您剛剛定義的 **Aggregate Group**（彙總群組）。
4. 選取 **Link Speed**（彙總群組）、**Link Duplex**（連結雙工）與 **Link State**（連結狀態）。

   作為最佳做法，為該群組中每個介面設定相同的連結和雙工值。若為不相符的值，防火牆將預設為較高的速度和全雙工。
5. （選用） 如果您為彙總群組啟用 LACP，則輸入 **LACP Port Priority**（**LACP** 連接埠優先順序）（預設為 32,768；範圍為 1 到 65,535）。如果您指派的介面數超過群組的 **Max Ports**（連接埠上限）值，則連接埠優先順序會決定哪些介面會處於使用中或待命。具有較低數值（較高優先順序）的介面將為使用中。
6. 按一下 **OK**（確定）。

STEP 5 | 如果防火牆具有主動/主動組態並且您將彙總 HA3 介面，則為彙總群組啟用封包轉送。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Active/Active Config**（主動/主動組態），然後編輯 Packet Forwarding（封包轉送）區段。
2. 選取您為 **HA3 Interface**（**HA3** 介面）設定的彙總群組，然後按一下 **OK**（確定）。

STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 驗證彙總群組狀態。

1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。
2. 確認連結狀態欄中彙總群組的圖示為綠色，表示所有的成員介面皆已啟動。如果圖示為黃色，則表示至少一個成員未啟動，但不是全部。如果圖示為紅色，表示所有的成員皆未啟動。
3. 如果您設定 LACP，確認 [功能] 欄顯示彙總群組的 LACP 已啟用圖示。

STEP 8 | （僅限 PA-7050 和 PA-7080 防火牆）如果您的彙總介面群組的介面位於不同的線路卡上，則最佳做法是啟用防火牆，以便它可以處理在分佈在多張卡上的 AE 群組的多個介面上接收的分散式 IP 封包。為此，請使用下面的 CLI 操作命令與 **hash** 關鍵字。（為確保完整性，其他兩個關鍵字也會顯示。）

1. 存取 CLI。

2. 使用下列操作 CLI 命令：**set ae-frag redistribution-policy** <**self** | **fixed sXdpX** | **hash**>

   - **self** — （預設）此關鍵字適用於傳統行為；它不支援防火牆處理在 AE 介面群組的多個介面上接收的分散式封包。
   - **fixed s**<*slot-number*>**dp**<*dataplane-cpu-number*>— 取代 *slot-number* 變數，並使用將處理所有 AE 介面之所有成員接收的所有 IP 片段的資料平面之編號取代 *data-plane-cpu-number* 變數。**fixed** 關鍵字主要用於疑難排解目的，不得用於生產。
   - **hash** — 用於讓防火牆處理它在位於多個線路卡上的 AE 介面群組的多個介面上接收的分散式封包。

設定網路區段的 Bonjour Reflector

Apple Bonjour（也稱為零設定網路）可自動探索本機網路上的裝置和服務。例如，Bonjour 允許您無需手動設定印表機的 IP 位址即可連線到印表機。為在本機網路上將名稱轉譯為位址，Bonjour 使用多點傳送 DNS (mDNS)。Bonjour 為其流量使用私人多點傳送範圍，不允許流量路由，從而阻止在使用網路區段的環境（例如，伺服器和用戶端位於不同子網路的環境中）中使用，以實現安全或管理目的。

為在使用區段路由流量的網路環境中支援 Apple Bonjour，您可以在指定的 Layer 3 介面 (L3) 乙太網路或彙總乙太網路 (AE) 介面或子介面間轉送 Bonjour IPv4 流量。Bonjour Reflector 選項允許您將多點傳送 Bonjour 廣告和查詢轉送到 L3 乙太網路和 AE 介面或子介面，確保使用者存取服務和裝置可探索性，而不考慮存留時間 (TTL) 值或躍點限制。

Bonjour 流量轉送支援 *PA-220*、*PA-400*、*PA-800* 和 *PA-3200* 系列。

啟用此選項後，防火牆會將 Bonjour 流量重新導向到您啟用此選項的 L3 和 AE 介面與子介面。You must enable this option on all supported interfaces that you want to manage Bonjour traffic; for example, if you want a specific L3 interface to forward Bonjour traffic to an AE interface, you must enable this option on both interfaces.您可以在最多 16 個介面上啟用此選項。

為阻止迴圈，防火牆將來源 *MAC* 位址修改為防火牆的輸出介面 *MAC* 位址。為幫助防止洪泛攻擊，如果防火牆每秒接收的封包數超過以下表格中指定的數量，防火牆會丟棄封包以保護防火牆和網路。

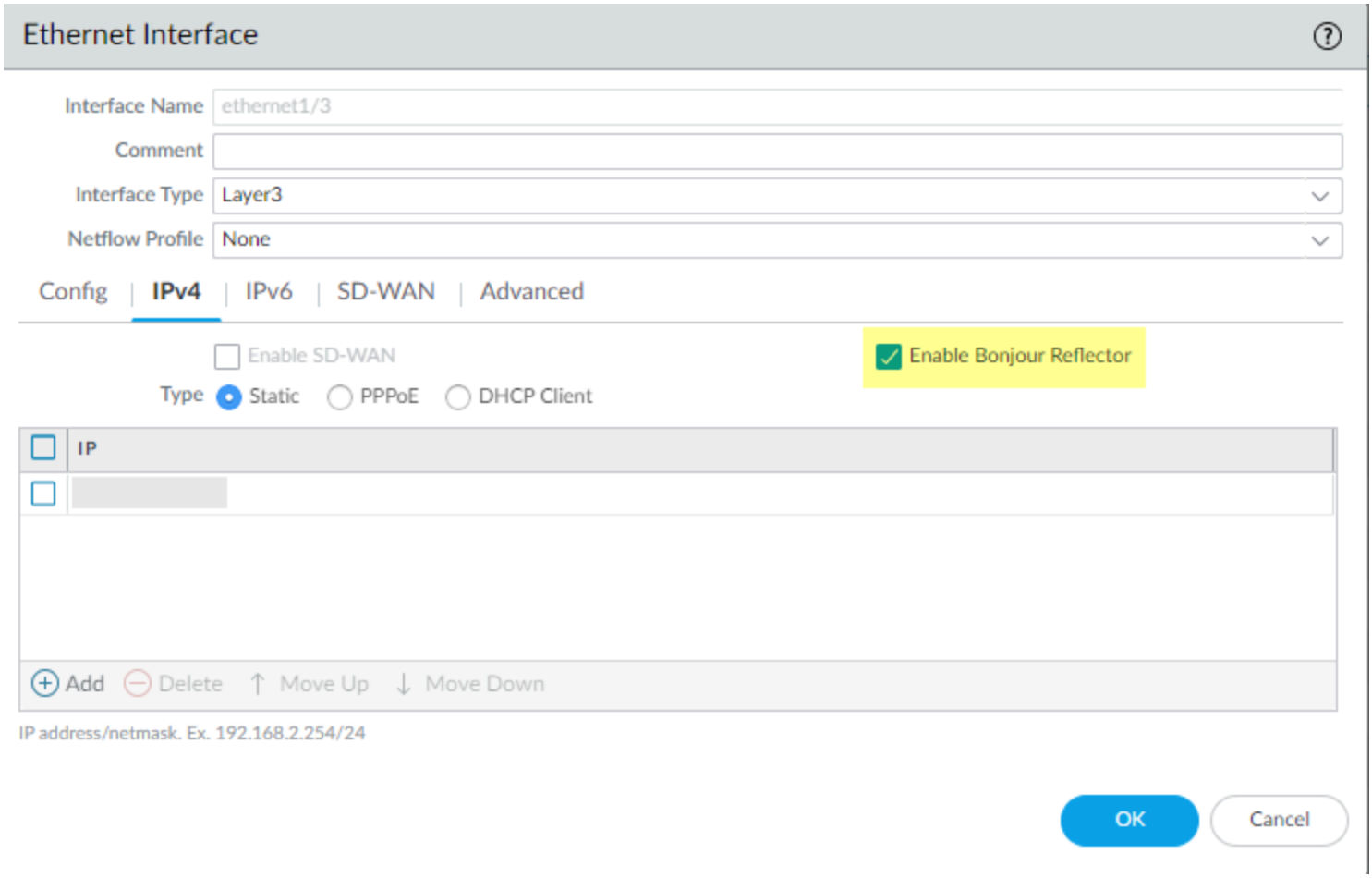
系列	速率限制（每秒）
PA-220	*100*
PA-400	不適用
PA-800	*200*
PA-3200	*500*

STEP 1 | 選取 **Network**（網路） > **Interfaces**（界面）。（網路 > 介面）

STEP 2 | 選取或 **Add**（新增）L3 乙太網路或子介面或 AE 介面。

如果您新增子介面，其必須使用 *0* 以外的標籤。

STEP 3 | 選取 **IPv4**，然後選取 **Enable Bonjour Reflector**（啟用 **Bonjour Reflector**）選項。



STEP 4 | 按一下 **OK**（確定）。

STEP 5 | 為您想要轉送 Bonjour 流量的所有 L3 或 AE 介面和子介面重複步驟 1—4。

您可以在最多 *16* 個不同介面或子介面上啟用此選項。

STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 確認您啟用了 Bonjour Reflector 選項的介面或子介面的 **Features**（功能）欄顯示 `Bonjour Reflector:yes`（ ）。

STEP 8 | 使用 `show bonjour interface` CLI 命令顯示防火牆轉送 Bonjour 流量的所有介面和計數器清單。`rx` 表示介面接收的 Bonjour 封包總數，`tx` 表示介面傳送的 Bonjour 封包總數，`drop` 表示介面丟棄的封包數。

```
admin> show bonjour interface

name                    rx          tx          drop
-------------------------------------------------------
ethernet1/4             1           1           0
```

```
ethernet1/7              0          0          0
ethernet1/7.10           0          0          0
ethernet1/7.20           4          4          0
ae15                     0          0          0
ae16                     0          0          0
ae16.30                  0          2          0
ae16.40                  0          0          0
```

使用介面管理設定檔限制存取

介面管理設定檔透過定義可在防火牆介面管理流量的通訊協定、服務和 IP 位址，保護防火牆免遭未經授權的存取。例如，您可能希望防止使用者透過 ethernet1/1 介面存取防火牆 Web 介面，但允許該介面接收來自網路監控系統的 SNMP 查詢。在此情況下，您會在介面管理設定檔中啟用 SNMP 並停用 HTTP/HTTPS，然後將此設定檔指派給 ethernet1/1。

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）。如果您不將介面管理設定檔指派給介面，則依預設，該介面會拒絕所有 IP 位址、通訊協定和服務的存取權限。

管理 *(MGT)* 介面不需要介面管理設定檔。如果您對防火牆執行初始設定，會限制 *MGT* 介面的通訊協定、服務和 *IP* 位址。在 *MGT* 介面關閉時，允許透過另一個介面進行管理存取讓您可以繼續管理防火牆。

使用介面管理設定檔啟用防火牆介面的存取時，請勿透過網際網路或企業安全性界限內的其他不信任區域啟用管理存取（*HTTP*、*HTTPS*、*SSH* 或 *Telnet*），且不要啟用 *HTTP* 或 *Telnet* 存取，因為這些通訊協定以明文傳輸。請遵循保護管理存取權的最佳做法，確保恰當保護您的防火牆管理存取。

STEP 1 | 設定介面管理設定檔。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理），然後按一下 **Add**（新增）。
2. 選取可在該介面管理流量的通訊協定：**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS** 或 **SNMP**。

   不要啟用 ***HTTP*** 或 ***Telnet***，因為這些通訊協定以明文傳輸，因此不安全。

3. 選取可在該介面管理流量的服務：
   - 回應頁面—用於啟用以下各項的回應頁面：
     - 網頁驗證—為服務網頁驗證回應頁面，防火牆在 Layer 3 介面上將連接埠保留為開啟：6081 用於透明模式中的網頁驗證，6082 用於重新導向模式中的網頁驗證。如需瞭解詳細資料，請參閱驗證原則和驗證入口網站。
     - **URL** 管理員覆寫—詳細資訊，請參閱允許使用密碼存取特定網站。
   - **User-ID**—用於重新散佈資料和驗證時間戳記。
   - **User-ID Syslog Listener-SSL**（**User-ID** 系統日誌接聽程式**-SSL**）或 **User-ID Syslog Listener-UDP**（**User-ID** 系統日誌接聽程式**-UDP**）—用於透過 SSL 或 UDP 來設定 User-ID 以監控用於使用者對應的 Syslog 傳送程式。
4. （選用）**Add**（新增）可存取該介面的 Permitted IP Addresses（許可的 IP 位址）。如果您不將項目新增到該清單，該介面沒有 IP 位址限制。
5. 按一下 **OK**（確定）。

STEP 2 | 將介面管理設定檔指派給介面。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取介面類型：**Ethernet**（乙太網路）、**VLAN**、**Loopback**（回送） 或 **Tunnel**（通道)，接著再選取該介面。
2. 選取 **Advanced**（進階） > **Other info**（其他資訊），然後選取您剛新增的 **Management Profile**（管理設定檔）。
3. 按一下 **OK**（確定）與 **Commit**（提交）。

虛擬路由器

瞭解防火牆上的虛擬路由器如何參與 Layer 3 路由，以及如何設定虛擬路由器。

虛擬路由器概觀

防火牆將透過您手動定義靜態路由或參與 Layer 3 路由通訊協定（動態路由），使用虛擬路由器取得通向其他子網路的 Layer 3 路由。防火牆透過這些方式取得的路由將填入防火牆上的 IP 路由資訊庫 (RIB)。當封包的目的地並非其到達的子網路時，虛擬路由器會從此 RIB 取得最佳路由，將其放入轉送資訊庫 (FIB)，並將封包轉送到 FIB 中定義的下一個躍點路由器。防火牆會使用乙太網路交換以到達同一個 IP 子網路上的其他裝置。（如果您使用 ECMP，則不會將一個最佳路由放入 FIB，在這種情況下，所有等價路由都會被放入 FIB。）

防火牆上定義的乙太網路、VLAN 和通道介面可接收及轉送 Layer 3 封包。目的地區域來源於轉送準則中指定的傳出介面，防火牆將查閱原則規則，以識別其對每個封包套用的安全性原則。除了路由至其他網路裝置以外，如果指定下一個躍點指向其他虛擬路由器，虛擬路由器還可以路由至相同防火牆內的其他虛擬路由器。

您可以在虛擬路由器上設定 Layer 3 介面參與動態路由通訊協定（BGP、OSPFv3 或 RIP），以及新增靜態路由。您也可建立多個虛擬路由器，每個路由器都保持單獨的路由集合，不在虛擬路由器之間共享，讓您為不同的介面設定不同的路由行為。

您可以在每個虛擬路由器中設定一個回送介面，在兩個回送介面之間建立一個靜態路由，然後設定一個動態路由通訊協定到這兩個介面之間的對等，從而設定從一個虛擬路由器到另一個虛擬路由器的動態路由。

在防火牆上定義的每個 Layer 3 乙太網路、回送、VLAN 及通道介面都必須與虛擬路由器相關聯。雖然每個介面只能屬於一個虛擬路由器，但可以為虛擬路由器設定多個路由通訊協定與靜態路由。無論為虛擬路由器設定的靜態路由與動態路由通訊協定為何，都需要有一般設定。

設定虛擬路由器

在防火牆上建立虛擬路由器，參與 Layer 3 路由。

STEP 1 | 從網路管理員收集必要資訊。

- 防火牆上您希望執行路由的介面。
- 靜態、內部 OSPF、外部 OSPF、IBGP、EBGP 與 RIP 的管理距離。

STEP 2 | 建立虛擬路由器，並對其套用介面。

防火牆具有一個名稱為 **default**（預設） 的虛擬路由器。您可以編輯 **default**（預設）虛擬路由器，或新增虛擬路由器。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
2. 選取虛擬路由器（名稱為 **default**（預設）的虛擬路由器或其他虛擬路由器），或者 **Add**（新增）新虛擬路由器的 **Name**（名稱）。
3. 選取 **Router Settings**（路由器設定） > **General**（一般）。
4. 按一下 **Interfaces**（介面）方塊中的 **Add**（新增），選取已定義的介面。

   為所有您要新增到虛擬路由器的介面重複此步驟 。
5. 按一下 **OK**（確定）。

STEP 3 | 設定靜態與動態路由的管理距離。

為網路所需的路由類型設定管理距離。若虛擬路由器有兩個或多個不同路由通向相同目的地時，將會利用管理距離從不同路由通訊協定和靜態路由中選取最佳路徑，優先選擇距離更短的路由。

- 靜態—範圍是 10 至 240；預設值為 10。
- **OSPF** 內部—範圍是 10 至 240；預設值為 30。
- **OSPF** 外部—範圍是 10 至 240；預設值為 110。
- **IBGP**—範圍是 10 至 240；預設值為 200。
- **EBGP**—範圍是 10 至 240；預設值為 20。
- **RIP**—範圍是 10 至 240；預設值為 120。

如果您要使用多個等價路由進行轉送，請參閱 ECMP。

STEP 4 | 提交虛擬路由器一般設定。

按一下 **OK**（確定）與 **Commit**（提交）。

STEP 5 | 根據需要設定乙太網路、回送、VLAN 及通道介面。

設定 Layer 3 介面。

服務路由

瞭解防火牆如何使用服務路由將要求傳送至外部服務，以及如何設定服務路由。

服務路由概觀

依預設，防火牆將使用管理 (MGT) 介面來存取外部服務，例如 DNS 伺服器、外部驗證伺服器、Palo Alto Networks® 服務（如 URL 更新、授權和 AutoFocus）。使用 MGT 介面的替代方式，是設定資料連接埠（一般介面）來存取這些服務。由此介面到伺服器上之服務的路徑，稱為服務路由。服務封包會從指派給外部服務的連接埠離開防火牆，而伺服器會將其回應傳送至設定的來源介面和來源 IP 位址。

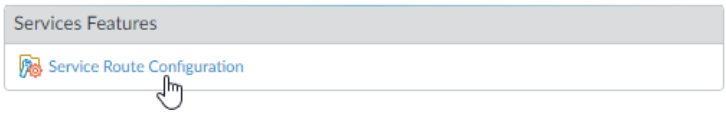
您可以為防火牆全域 設定服務路由，或者在支援多虛擬系統的防火牆上為一個虛擬系統自訂服務路由，以便能夠靈活地使用與虛擬系統關聯的介面。虛擬系統若沒有為特定服務設定的服務路由，即會繼承為該服務全域設定的介面和 IP 位址。

設定服務路由

您可以使用下列程序設定服務路由，以變更防火牆用於傳送請求到外部服務的介面。

STEP 1 | 自訂服務路由。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Global**（全域）（對於不支援多個虛擬系統的防火牆，則忽略 Global（全域）），然後在 Services Features（服務功能）區段中，按一下 **Service Route Configuration**（服務路由組態）。



2. 選取 **Customize**（自訂），然後執行下列其中一項工作，以建立服務路由：
   - 對於預先定義的服務：
     - 選取 **IPv4** 或 **IPv6**，然後按一下您要自訂服務路由的服務連結。

       為了便於對多個服務使用相同來源位址，可選中服務的核取方塊，然後按一下 ***Set Selected Routes***（設定選定的路由），然後再繼續下一步驟。
     - 若要限制來源位址的清單，可選取 **Source Interface**（來源介面），然後（從該介面）選取 **Source Address**（來源位址），作為服務路由。如果已在所選介面上設定了位址物件，也可以將其引用為來源位址。選取 **Any**（任何）來源介面會使所有介面的所有 IP 位址出現在來源位址清單中，供您選取。選取 **Use default**（使用預設）會使防火牆使為服務路由使用管理介面，除非封包目的地 IP 位址與所設定的目的地 IP 位址，在這種情況下，來源 IP 位址要設定為針對 **Destination**（目的地）設定的 **Source Address**（來源位址）。選取 **MGT**（管理）會使防火牆為服務路由使用管理介面，無論使用任何目的地服務路由皆是如此。

       服務路由來源位址不會從引用的介面繼承設定變更，反之亦然。將介面 *IP* 位址修改為其他 *IP* 位址，否則位址物件將不會更新相應的服務路由來源位址。這可能會導致提交失敗並要求您將服務路由更新為有效的來源位址值。
     - 按一下 **OK**（確定）以儲存設定。
     - 如果您要為服務指定 IPv4 和 IPv6 位址，可重複此步驟。
   - 對於目的地服務路由：
     - 選取 **Destination**（目的地），然後 **Add**（新增）**Destination**（目的地）IP 位址。在這種情況下，如果到達的封包具有與所設定的此 **Destination**（目的地）位址相符的目的地 IP 位址，則該封包的來源 IP 位址將被設定為下一步中設定的 **Source Address**（來源位址）。
     - 若要限制來源位址的清單，可選取 **Source Interface**（來源介面），然後（從該介面）選取 **Source Address**（來源位址），作為服務路由。選取 **Any**（任何）來源介面會使所有介面的所有 IP 位址出現在來源位址清單中，供您選取。選取 **MGT**（管理）會使防火牆為服務路由使用管理介面。

- 按一下 **OK**（確定）以儲存設定。

3. 針對您要自訂的每個服務路由，重複之前的步驟。
4. 按一下 **OK**（確定）以儲存服務路由組態。

STEP 2 | **Commit**（認可）。

靜態路由

靜態路由一般與動態路由通訊協定結合使用。您可以為動態路由通訊協定無法到達的位置設定靜態路由。靜態路由需要在網路中每個路由器上手動設定，而動態路由則由防火牆輸入到路由表中；雖然靜態路由需要在所有路由器上進行設定，但在小型網路中，靜態路由比路由通訊協定更合適。

靜態路由設定概要介紹

如果您確定特定 Layer 3 流量使用特定路由而不參與 IP 路由通訊協定，則您可以設定靜態路由使用 IPv4 和 IPv6 。

預設路由為特定靜態路由。如果您不使用動態路由來取得虛擬路由器的預設路由，則您必須設定一個靜態預設路由。若虛擬路由器有一個輸入封包，但在路由表中找不到該封包目的地的相符路由，則虛擬路由器會將該封包傳送至預設路由。預設 IPv4 路由為 0.0.0.0/0；預設 IPv6 路由為 ::/0。您可以同時設定 IPv4 和 IPv6 預設路由。

靜態路由本身並不能變更網路環境或調整以適應網路環境，因此，如果通向靜態定義端點的路由發生故障，一般不會重新路由流量。當時，您可以選擇備份靜態路由，以防出現問題：

- 您可以使用雙向轉送偵測 (BFD) 設定檔來設定靜態路由，以便當您為靜態路由啟用 BFD 並且防火牆與 BFD 對等之間的 BFD 工作階段失敗時，防火牆將從 RIB 及 FIB 表中移除失效的靜態路由並使用較低優先順序的替代路由。
- 您可以為靜態路由設定路徑監控，以便防火牆能使用替代路由。

依預設，靜態路由的管理距離為 10。當防火牆有兩個或多個路由通向同一目的地時，將使用管理距離最短的路由。透過將靜態路由的管理距離增加到大於動態路由，您可以將靜態路由用作動態路由不可用時的備用路由。

在您設定靜態路由時，您可以指定防火牆是否在單點傳送或多點傳送路由表 (RIB) 或二者中安裝 IPv4 靜態路由。例如，您可以僅在多點傳送路由表中安裝 IPv4 靜態路由，因為您只希望多點傳送流量使用該路由。此選項讓您能夠更好地控制流量使用哪一個路由。您可以指定是否在單一路由表中安裝 IPv6 靜態路由。

基於路徑監控的靜態路由移除

當您為靜態路由設定路徑監控時，防火牆將使用路徑監控來偵測通向一個或多個受監控目的地的路徑在何時失效。防火牆隨後可使用替代路由重新路由流量。防火牆對靜態路由使用路徑監控與對 HA 或基於原則的轉送 (PBF) 使用路徑監控非常相似，具體如下：

- 防火牆向您判定為正常並反映了靜態路由可用性的一個或多個受監控目的地傳送 ICMP 偵測訊息（活動訊號訊息）。
- 如果對任何或所有受監控目的地的偵測失敗，防火牆也會認為靜態路由失效，並將其從路由資訊庫 (RIB) 和轉送資訊庫 (FIB) 中移除。RIB 是為防火牆設定的靜態路由以及防火牆從路由通訊協定學得的動態路由的表格。FIB 時防火牆用於轉送封包的路由轉送表。防火牆可從 RIB 中選取同一目的地的替代靜態路由（選取度量值最低的路由），並將其放入 FIB。
- 防火牆將繼續監控失效的路由。當該路由恢復正常，並且（根據失敗條件是 **Any**（任何） 還是 **All**（所有））路徑監控器也恢復開啟狀態時，則先佔保留計時器將開始計時。在保留計時器計時期間，路徑監控器必須保持開啟；然後防火牆將認為該靜態路由已穩定，並將其恢復到 RIB 中。防火牆隨後將比較同一目的地的路由度量值，以確定將哪個路由放入 FIB。

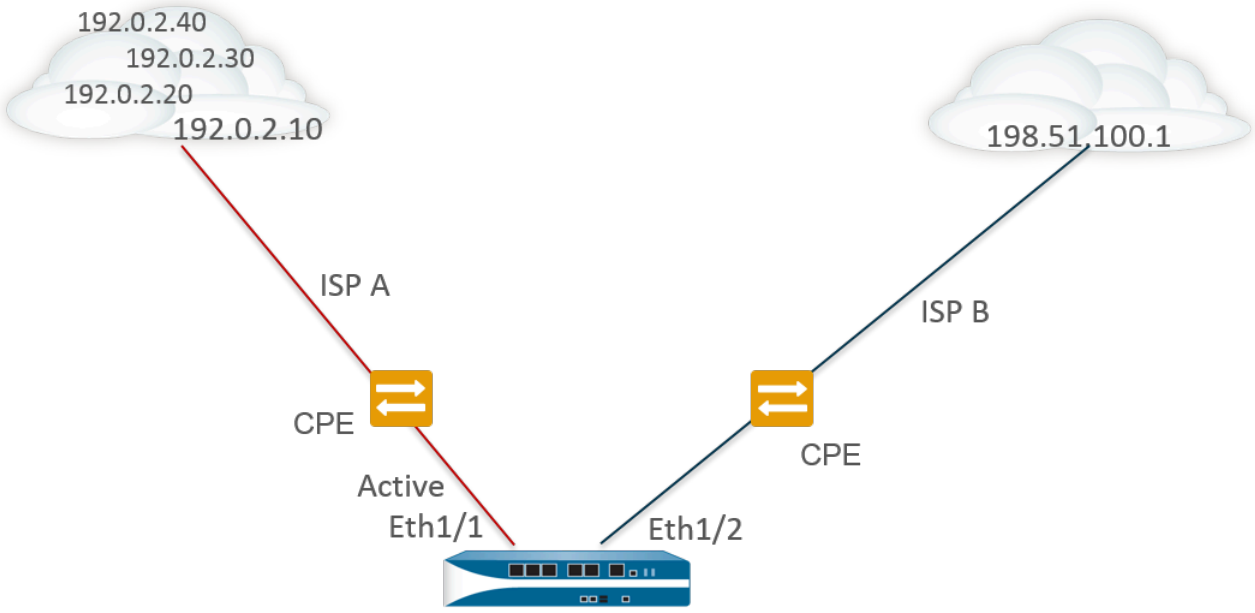
路徑監控是避免將下列路由的流量無訊息丟棄的有效機制：

- 靜態或預設路由。
- 重新散佈到路由通訊協定的靜態或預設路由。
- 其中一個對等體不支援 BFD 時的靜態或預設路由。（最佳做法是不在單一介面上同時啟用 BFD 和路徑監控。）
- 代替使用 PBF 路徑監控的靜態路由或預設路由，這並不會將失效靜態路由從 RIB、FIB 或重新散佈原則中移除。

路徑監控並不會套用於在虛擬路由器之間設定的靜態路由。

在下圖中，防火牆連線至兩個 ISP，用作網際網路的路由備援。主要預設路由為 0.0.0.0（度量值 10）使用下一個躍點 192.0.2.10；次要預設路由 0.0.0.0（度量值 50）使用下一個躍點 198.51.100.1。ISP A 的用戶端裝置 (CPE) 將使主要實體連接保持啟用，即時是在網際網路連線中斷之後。如果手動啟用連結，防火牆將無法偵測該連結是否中斷，是否應使用其 RIB 中的次要路由取代失效的路由。

要避免無訊息丟棄通向失效連結的流量，請設定 192.0.2.20、192.0.2.30 和 192.0.2.40 的路徑監控；如果通向這些目的地的（任何）路徑失效，防火牆會推測通向下一個躍點 192.0.2.10 的路徑也失效，將靜態路由 0.0.0.0（使用下一個躍點 192.0.2.10）從其 RIB 中移除，並用通向同一目的地 0.0.0.0（使用下一個躍點 198.51.100.1）的次要路由取代它。



Route Table

Destination	Next Hop	Metric	Interface	
0.0.0.0/0	192.0.2.10	10	ethernet1/1	X Pings to 192.0.2.20, 192.0.2.30, and 192.0.2.40 fail, so static route remove
0.0.0.0/0	198.51.100.1	50	ethernet1/2	

在設定靜態路由時，其中一個必要欄位就是通向該目的地的下一個躍點。您所設定的下一個躍點類型決定了防火牆將在路徑監控期間執行的動作，具體如下：

如果靜態路由中的下一個躍點類型為：	防火牆用於 **ICMP** 偵測的動作
IP 位址	防火牆將使用靜態路由的來源 IP 位址和輸出介面作為 ICMP 偵測的來源位址和輸出介面。防火牆會將受監控目的地的設定目的地 IP 位址用作偵測的目的地位址。防火牆會將靜態路由的下一個躍點位址用作偵測的下一個躍點位址。
下一個 **VR**	防火牆將使用靜態路由的來源 IP 位址作為 ICMP 偵測的來源位址。輸出介面將取決於來自於下一個躍點的虛擬路由器的查閱結果。受監控目的地的設定目的地 IP 位址將用作偵測的目的地位址。
無	防火牆將使用路徑監控的目的地 IP 位址作為下一個躍點，並向靜態路由中指定的介面傳送 ICMP 偵測。

當靜態路由或預設路由的路徑監控失效時，防火牆會記錄重要事件（path-monitor-failure）。當靜態路由或預設路由的恢復時，防火牆會記錄另一個重要事件（path-monitor-recovery）。

防火牆會同步主動/被動 HA 部署的路徑監控組態，但會封鎖被動 HA 上的輸出 ICMP 偵測，因為它不會主動處理流量。防火牆不會同步主動/主動 HA 部署的路徑監控組態。

設定靜態路由

完成下列工作，為防火牆上的虛擬路由器設定靜態路由或預設路由。

STEP 1 | 設定靜態路由。

1. 選取 **Network**（網路） > **Virtual Router**（虛擬路由器），然後選取要設定的虛擬路由器，例如 **default**（預設）。
2. 設定 **Static Routes**（靜態路由）頁籤。
3. 視乎您要設定的靜態路由類型，選取 **IPv4** 或 **IPv6**。
4. 為路由 **Add**（新增）**Name**（名稱）。
5. 對於 **Destination**（目的地），輸入路由和網路遮罩（例如為 IPv4 位址輸入 192.168.2.2/24，為 IPv6 位址輸入 2001:db8:123:1::1/64）。如果您要建立預設路由，則輸入預設路由（為 IPv4 位址輸入 0.0.0.0/0，為 IPv6 位址輸入 ::/0）。或者，您可以建立類型為 IP 網路遮罩的位址物件。
6. （選用）對於 **Interface**（介面），指定封包用於進入下一個躍點的連出介面。對防火牆使用的介面使用這種更嚴格的控制，而不要對路由表中用作此路由下一個躍點的介面使用。
7. 對於 **Next Hop**（下一個躍點），選取以下任何項：
   - **IP** 位址—如果您希望路由至特定的下一個躍點，則輸入 IP 位址（例如 192.168.56.1 或 2001:db8:49e:1::1）。在 設定 Layer 3 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。如果您要建立預設路由，對於 **Next Hop**（下一個躍點），您必須選取 **IP Address**（**IP** 位址），然後輸入網際網路閘道的 IP 位址（例如 192.168.56.1 或 2001:db8:49e:1::1）。或者，您可以建立類型為 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。
   - 下一個虛擬路由器—如果您要在內部路由至防火牆上的不同路由器，則選取此選項，然後選取虛擬路由器。
   - **FQDN**—輸入 FQDN 或選取使用 FQDN 的位址物件，或建立類型為 FQDN 的新位址物件。

     如果您使用 *FQDN* 作為靜態路由的下一個躍點，*FQDN* 必須解析為與為靜態路由設定的介面屬於同一子網路的 *IP* 位址；否則，防火牆將拒絕進行解析，且 *FQDN* 仍然處於未解析狀態。

     防火牆僅使用 *FQDN* 的 *DNS* 解析得到的一個 *IP* 位址（來自每個 *IPv4* 或 *IPv6* 系列類型）。如果 *DNS* 解析返回多個位址，防火牆會使用與為下一個躍點設定的 *IP* 系列類型（*IPv4* 或 *IPv6*）相符的偏好 *IP* 位址。偏好 *IP* 位址是 *DNS* 伺服器在初始回應中返回的第一個位址。只要此位址出現在後續回應中，無論其順序如何，防火牆都會保留此位址作為偏好位址。
   - 捨棄— 選取此選項後，將丟棄定址到此目的地的封包。

- 無 — 如果路由沒有下一個躍點，請選取此選項。例如，點對點連線無須下一個躍點，因為封包只有一個方向。

8. 輸入路由的 **Admin Distance**（管理距離），以覆寫為此虛擬路由器的靜態路由設定的預設管理距離（範圍為 10 至 240；預設值為 10）。
9. 輸入路由的 **Metric**（公制）（範圍為 1 至 65535）。

STEP 2 | 選擇路由的安裝位置。

選取希望防火牆將靜態路由安裝到哪個 **Route Table**（路由表）(RIB)：

- 單點傳送—將路由安裝至單點傳送路由表。如果您希望路由僅用於單點傳送流量，則選擇此選項。
- 多點傳送—將路由安裝至多點傳送路由表（僅適用於 IPv4 路由）。如果您希望路由僅用於多點傳送流量，則選擇此選項。
- 二者—將路由安裝至單點傳送路由表和多點傳送路由表（僅適用於 IPv4 路由）。如果您希望單點傳送或多點傳送流量使用此路由，則選擇此選項。
- 不安裝—不在任何路由表中安裝路由。

STEP 3 | （選用）如果防火牆型號支援 BFD，您可以將 **BFD Profile**（**BFD** 設定檔）套用至靜態路由，以便在靜態路由失效時，防火牆能將該路由從 RIB 和 FIB 中移除，從而使用替代路由。預設值為 **None**（無）。

STEP 4 | 按兩下 **OK**（確定）。

STEP 5 | **Commit**（提交）組態。

為靜態路由設定路徑監控

使用下列程序設定基於路徑監控的靜態路由移除。

STEP 1 | 為靜態路由啟用路徑監控。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **Static Routes**（靜態路由），再選取 **IPv4** 或 **IPv6**，然後選取您要監控的靜態路由。您最多可監控 128 個靜態路由。
3. 選取 **Path Monitoring**（路徑監控）以啟用路由的路徑監控。

STEP 2 | 為靜態路由設定受監控目的地。

1. 按 **Name**（名稱）**Add**（新增）受監控目的地。您最多可為每個靜態路由新增八個受監控目的地。
2. 選取 **Enable**（啟用）以監控目的地。
3. 對於 **Source IP**（來源 **IP**），選取防火牆在 ICMP 偵測中用於連線受監控目的地的 IP 位址：
   - 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 Dynamic IP Interface Status（動態 IP 介面狀態）視窗中。
4. 位於 **Destination IP**（目的地 **IP**），輸入防火牆將監控其路徑的 IP 位址或位址物件。受監控目的地和靜態路由目的地必須使用相同位址系列（IPv4 或 IPv6）。

   目的地 *IP* 位址應屬於可靠的端點；您不會希望以本身不穩定或不可靠的裝置為基礎監控路徑。
5. （選用）指定 ICMP **Ping Interval (sec)**（偵測間隔（秒）），以確定防火牆監控路徑的頻率（範圍為 1-60；預設為 3）。
6. （選用）指定未從目的地放回的封包 ICMP **Ping Count**（偵測計數），超出此計數後，防火牆將認為靜態路由關閉，並將其從 RIB 和 FIB 中移除（範圍為 3-10；預設值為 5）。
7. 按一下 **OK**（確定）。

STEP 3 | 確定靜態路由的路徑監控是基於一個還是全部受監控目的地，並設定先佔保留時間。

1. 選取 **Failure Condition**（失敗條件），是否在靜態路由的 **Any**（任何）或 **All**（所有）受監控目的地皆無法透過 ICMP 連線時，防火牆才會從 RIB 和 FIB 移除該靜態路由，並將通向同一目的地的度量為次低者的靜態路由新增至 FIB。

   選取 ***All***（所有）能避免（例如）當目的地僅因維護而離線時，單一監控目的地發出靜態路由失敗的信號。

2. （選用）指定**Preemptive Hold Time (min)**（先佔保留時間（分）），在防火牆將靜態路由重新安裝到 RIB 之前，已關閉的路徑監控器必須保持開啟狀態的時間（單位為分鐘）。路徑監控器將評估靜態路由的所有受監控目的地，並將根據 **Any**（任何）或 **All**（所有）失敗條件出現。若在保留時間內連結關閉或波動，當連結重新開啟時，路徑監控器也將開啟；當路徑監控器恢復開啟狀態後，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路由重新安裝至 RIB。範圍為 0-1440；預設值為 2。

3. 按一下 **OK**（確定）。

STEP 4 | 提交。

按一下 **Commit**（交付）。

STEP 5 | 驗證針對靜態路由的路徑監控。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後在相應的虛擬路由器列中選取 **More Runtime Stats**（更多執行階段統計資料）。
2. 在 **Routing**（路由）頁籤中選取 **Static Route Monitoring**（靜態路由鏡像）。
3. 對於靜態路由（目的地），檢視路徑健康是否已啟用。Status（狀態）欄指明了路由狀態為 Up（開啟）、Down（關閉）還是 Disabled（停用）。靜態路由的標幟為：A—使用中，S—靜態，E—ECMP。
4. 定期選取 **Refresh**（重新整理），以查看最新的路徑監控狀態（健康狀況檢查）。
5. 將滑鼠暫留在路由 Status（狀態）上，檢視受監控 IP 位址以及傳送至該路由的受監控目的地的偵測結果。例如，3/5 表示偵測間隔為 3 秒且偵測計數為連續 5 次錯失偵測（防火牆在過去 15 秒中沒有接收到偵測），表示路徑監控偵測到連結失敗。根據選取的是 **Any**（任何）還是 **All**（所有）失敗條件，如果路徑監控處於失敗狀態並且防火牆在 15 秒後收到偵測，該路徑將被認為已開啟，**Preemptive Hold Time**（先佔保留時間）開始計時。

   State（狀態）指示上次受監控偵測結果：成功或失敗。失敗表示有一系列偵測封包（偵測間隔乘以偵測計數）未成功。單個偵測封包失敗並不能反映偵測失敗狀態。

STEP 6 | 檢視 RIB 和 FIB，以確認靜態路由是否已移除。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後在相應的虛擬路由器列中選取 **More Runtime Stats**（更多執行階段統計資料）。
2. 在 **Routing**（路由）頁籤上，選取 **Route Table**（路由表）(RIB)，然後選取 **Forwarding Table**（轉送表）(FIB) 以分別檢視每個表。
3. 選取 **Unicast**（單點傳送）或 **Multicast**（單點傳送）以檢視相應路由表。
4. 對於 **Display Address Family**（顯示位址系列），選取 **IPv4 and IPv6**（**IPv4** 和 **IPv6**）、**IPv4 Only**（僅 **IPv4**）或 **IPv6 Only**（僅 **IPv6**）。
5. （選用）在篩選欄位中，輸入您要搜尋的路由，然後選取相應箭頭，或使用捲軸捲動路由頁面。
6. 查看路由是否已移除。
7. 定期選取 **Refresh**（重新整理），以查看最新的路徑監控狀態（健康狀況檢查）。

若要檢視為路徑監控記錄的事件，可選取 ***Monitor***（監控） ***> Logs***（日誌） ***> System***（系統）。檢視 ***path-monitor-failure*** 的項目，它指示了靜態路由目的地路徑監控失敗，因此該路徑已被移除。檢視 ***path-monitor-recovery*** 的項目，它指示了靜態路由目的地路徑監控已復原，因此該路徑已恢復。

RIP

請考慮 RIP 是否為網路適用的路由通訊協定，如果是，則設定 RIP。

- RIP 概觀
- 設定 RIP

RIP 概觀

路由資訊通訊協定 (RIP) 是針對小型 IP 網路設計的內部閘道通訊協定 (IGP)。RIP 依賴躍點計數來判斷路由；最佳路由的躍點數目最少。RIP 以 UDP 為基礎，並使用連接埠 520 來更新路由。將路由限制為躍點最大值 15，通訊協定可協助防止路由迴圈開發，但也會限制支援的網路大小。設定 RIP 之前，請考慮如果需要超過 15 個躍點，則不會路由流量。同時，RIP 的收斂時間比 OSPF 及其他路由通訊協定要長。

防火牆支援 RIP v2。

設定 RIP

請執行下列程序設定 RIP。

STEP 1 | 設定一般虛擬路由器設定。

STEP 2 | 設定一般 RIP 組態設定。

1. 選取虛擬路由器（**Network**（網路） > **Virtual Routers**（虛擬路由器）），針對虛擬路由器，選取 **RIP**。
2. 選取 **Enable**（啟用）可啟用 RIP 通訊協定。
3. 如果您不想透過 RIP 記住任何預設路由，請選取 **Reject Default Route**（拒絕預設路由）。這是建議的預設設定。

   若要透過 RIP 允許重新散佈預設路由，則清除 **Reject Default Route**（拒絕預設路由）。

STEP 3 | 設定 RIP 的介面。

1. 在 **Interfaces**（介面）頁籤上，從介面組態區段中選取介面。
2. 選取已定義的介面。
3. 選取 **Enable**（啟用）。
4. 選取 **Advertise Default Route**（宣告預設路由）可向具有指定公制值的 RIP 對等宣告預設路由。
5. （選用） 從 **Auth Profile**（驗證設定檔）清單選取設定檔。
6. 從 **Mode**（模式）清單中選取一般、被動或僅傳送。
7. （選用）要為虛擬路由器全域啟用 BFD for RIP，請選取一個 **BFD** 設定檔。
8. 按一下 **OK**（確定）。

STEP 4 | 設定 RIP 計時器。

1. 在 **Timers**（計時器）頁籤上的 **Interval Seconds (sec)**（間隔秒數 （秒））中輸入值。此設定會以秒數定義以下 RIP 計時器間隔長度 （範圍是 1 至 60；預設值是 1）。
2. 指定 **Update Intervals**（更新間隔），以定義路由更新宣告之間的間隔數 （範圍是 1 至 3600；預設值是 30）。
3. 指定 **Expire Intervals**（到期間隔），以定義從路由上次更新到過期這段時間之間的間隔數 （範圍為 1 至 3600；預設值是 120）。
4. 指定 **Delete Intervals**（刪除間隔），以定義從路由到期到刪除這段時間之間的間隔數 （範圍是 1 至 3600；預設值是 180）。

STEP 5 | （選用）設定驗證設定檔。

依預設，防火牆不會對 RIP 芳鄰之間的交換使用 RIP 驗證。您也可以透過簡單的密碼或 MD5 驗證來設定 RIP 芳鄰之間的 RIP 驗證。建議使用 MD5 驗證；它比簡單的密碼更安全。

簡單密碼 **RIP** 驗證

1. 選取 **Auth Profiles**（驗證設定檔），然後為用於驗證 RIP 訊息的驗證設定檔 **Add**（新增）名稱。
2. 選取簡單密碼作為密碼類型。
3. 輸入簡單密碼，然後確認。

MD5 RIP 驗證

1. 選取 **Auth Profiles**（驗證設定檔），然後為用於驗證 RIP 訊息的驗證設定檔 **Add**（新增）名稱。
2. 選取 **MD5**作為密碼類型。
3. **Add**（新增）一個或多個密碼項目，包括：
   - Key-ID（範圍是 0 至 255）
   - 金鑰
4. （選用）選取 **Preferred**（慣用）狀態。
5. 按一下 **OK**（確定）以指定用於驗證傳出訊息的金鑰。
6. 在（虛擬路由器 - RIP 驗證設定檔）對話方塊中，再按一次 **OK**（確定）。

STEP 6 | **Commit**（提交）您的變更。

OSPF

開放式最短路徑優先協定 (OSPF) 是內部閘道通訊協定 (IGP)，最常用於動態管理大規模企業網路中的網路路由。OSPF 可從其他路由器中取得資訊並以連結狀態宣告 (LSA) 的方式向其他路由器宣告路由，來動態確定路由。從 LSA 收集到的這項資訊會用於建構網路的拓撲地圖。拓撲地圖會在網路的路由器之間分享，並用於將可用的路由填入 IP 路由表中。

系統會動態偵測網路拓撲的變更，並使用變更在數秒內產生新的拓撲地圖。此外也會計算每個路由的最短路徑樹狀目錄。最佳路由是使用與路由介面相關聯的公制計算而得。公制包括距離、網路輸送量、連結可用性等。此外，可靜態設定這些公制，以引導出 OSPF 拓撲地圖的結果。

OSPF 的 Palo Alto Networks® 實作完全支援下列 RFC：

- RFC 2328 (適用於 IPv4)
- RFC 5340 (for IPv6)

下列主題提供 OSPF 的詳細資訊，及在防火牆上設定 OSPF 的程序：

- OSPF 概念
- 設定 OSPF
- 設定 OSPFv3
- 設定 OSPF 非失誤性重新啟動
- 確認 OSPF 操作

OSPF 概念

下列主題介紹 OSPF 概念，您必須瞭解這些概念才能設定參與 OSPF 網路的防火牆：

- OSPFv3
- OSPF 芳鄰
- OSPF 區域
- OSPF 路由器類型

OSPFv3

OSPFv3 支援 IPv6 網路內的 OSPF 路由通訊協定。因此，亦支援 IPv6 位址與首碼。OSPFv3 保留了 OSPFv2 (適用於 IPv4) 中大多數的結構與功能，只有微幅的變更。以下為 OSPFv3 中部分的新增功能與變更：

- 為各連結支援多個實例—有了 OSPFv3，您可以透過單一連結執行 OSPF 通訊協定的多個實例。只要指派 OSPFv3 實例 ID 號碼即可達成。當封包的 ID 不同時，指派給實例 ID 的介面就會丟棄該封包。
- 各連結的通訊協定處理—OSPFv3 會操作各連結，而不像 OSPFv2 是操作各 IP 子網路。
- 位址變更—IPv6 位址不在 OSPFv3 封包中，但連結狀態更新封包中的 LSA 承載除外。鄰近的路由器會依路由器 ID 識別。
- 驗證變更—OSPFv3 不包含任何驗證功能。若要在防火牆上設定 OSPFv3，必須有驗證設定檔以指定「封裝安全有效負載」(ESP) 或 IPv6「驗證標頭」(AH)。本版本不支援 RFC 4552 中指定的重新產生金鑰程序。
- 為各連結支援多個實例—每個連結在 OSPFv3 封包標頭在都會有對應的實例 ID。
- 新 **LSA** 類型—OSPFv3 支援兩個新的 LSA 類型：連結 LSA 與內部 區域 首碼 LSA。

RFC 5340 中有所有其他變更的詳細說明。

OSPF 芳鄰

兩個具備 OSPF 功能的路由器經由通用網路連接，並位在同一個 OSPF Area 中形成關係，即為 OSPF 芳鄰。這些路由器之間的連線可透過通用廣播網域或點對點連線建立。此連線是經由交換您好 OSPF 通訊協定封包所建立的。系統會使用這些芳鄰關係在路由器之間交換路由更新。

OSPF 區域

OSPF 在單一自發系統 (AS) 內運作。但是，在此單一 AS 內的網路可劃分成數個區域。依預設，系統會建立區域 0。區域 0 可獨立運作，或作為大量區域的 OSPF 骨幹。每個 OSPF 區域皆以 32 位元識別碼命名，在大多數的狀況下，會寫成與 IP4 位址相同的點-十進位標記法。例如，區域 0 通常寫成 0.0.0.0。

區域中的拓撲是在其自己的連結狀態資料庫中維護的，並隱藏起來讓其他的區域看不到，藉此減少 OSPF 所需的流量路由數量。連接的路由器可透過區域之間的摘要表來共用拓撲。

OSPF 區域類型	說明
骨幹區域	骨幹區域（區域 0）是 OSPF 網路的核心。所有其他的區域都會連接到此核心，區域之間的流量也必須通過它。各區域之間的所有路由是透過骨幹區域散佈的。雖然所有其他的 OSPF 區域必須連接至骨幹區域，但此連接不一定要是直接的，並可透過虛擬連結建立。
一般 OSPF 區域	一般 OSPF 區域內沒有任何限制；此區域可包含所有類型的路由。
虛設常式 OSPF 區域	虛設常式區域不會收到其他自發系統的路由。從虛設常式區域到骨幹區域的路由是透過預設路由執行的。
NSSA 區域	Not So Stubby Area (NSSA) 的縮寫，這是一種會匯入外部路由的虛設常式區域，但有一些限制的例外狀況。

OSPF 路由器類型

在 OSPF 區域內，路由器可分成下列類別。

- 內部路由器—個與相同區域中的裝置有 OSPF 芳鄰關係的路由器。
- 區域界限路由器 **(ABR)**—與多個 OSPF 區域中的裝置有 OSPF 芳鄰關係的路由器。ABR 會從其連線的區域收集拓撲資訊，並將資訊散佈到骨幹區域。
- 骨幹路由器—骨幹路由器是指執行 OSPF 並且有至少一個介面連線至 OSPF 骨幹網路區域的路由器。由於 ABR 一律與骨幹連接，也因此一律歸類為骨幹路由器。
- 自發系統邊界路由器 **(ASBR)**—ASBR 是一種連接到多個路由通訊協定的路由器，會在路由通訊協定之間交換路由資訊。

設定 OSPF

OSPF 可從其他路由器中取得資訊並以連結狀態宣告 (LSA) 的方式向其他路由器宣告路由，來動態確定路由。路由器會保留路由器與目的地之間的連結資訊，且可做出高效率的路由決定。當計算所有遇到的輸出路由器介面與接受 LSA 之介面的總和時，會將成本指派給每個路由器介面，而最佳路由將會是成本最低者。

階層式技術用來限制必須宣告的路由與相關聯 LSA 的數目。由於 OSPF 會動態處理大量路由資訊，因此它的處理器與記憶體需求比 RIP 大。

STEP 1 | 設定一般虛擬路由器設定。

STEP 2 | 啟用 OSPF。

1. 選取 **OSPF** 頁籤。
2. 選取 **Enable**（啟用）可啟用 OSPF 通訊協定。
3. 輸入 **Router ID**（路由器 **ID**）。
4. 如果您不想透過 OSPF 記住任何預設路由，請選取 **Reject Default Route**（拒絕預設路由）。這是建議的預設設定。

   如果您想透過 OSPF 允許重新散佈預設路由，請清除 **Reject Default Route**（拒絕預設路由）。

STEP 3 | 設定區域—OSPF 通訊協定類型。

1. 在 **Areas**（區域）頁籤上，以 *x.x.x.x* 格式為區域 **Add**（新增）**Area ID**（區域 **ID**）。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。
2. 在 **Type**（類型）頁籤上，從區域的 **Type**（類型）清單中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。如果您選取此選項，請進行下列設定：
     - 接受摘要—接受來自其他區域的連結狀態宣告 (LSA)。如果停用虛設常式區域其「區域邊界路由器」(ABR) 介面上的此選項，OSPF 區域將可作為「完全末梢區域」(TSA) 使用，且 ABR 將不會傳播任何摘要 LSA。
     - 宣告預設路由—預設路由 LSA 將包含在對虛設常式區域及設定範圍 1-255 之已設定公制值的宣告中。
   - **NSSA** (Not-So-Stubby Area)—防火牆只會依 OSPF 路由以外的路由離開區域。若選取 NSSA，則依照 **Stub**（虛設常式）的描述選取 **Accept Summary**（接受摘要）與 **Advertise Default Route**（宣告預設路由）。如果您選取此選項，請進行下列設定：
     - 類型—選取 **Ext 1** 或 **Ext 2** 路由類型來宣告預設的 LSA。
     - 外部範圍—**Add**（新增）您要**Advertise**（宣告）的或要 **Suppress**（抑制）宣告的外部路由範圍。
3. 按一下 **OK**（確定）。

STEP 4 | 設定區域—OSFP 通訊協定範圍

1. 在 **Range**（範圍）頁籤上，將區域內的彙總 LSA 目的地位址 **Add**（新增）至子網路。
2. **Advertise**（宣告）或 **Suppress**（抑制）符合子網路的宣告 LSA，然後按一下 **OK**（確定）。重複上述操作可新增其他範圍。

STEP 5 | 設定區域—OSFP 通訊協定介面

1. 在 **Interface**（介面）頁籤上，為區域內將要包含的每個介面 **Add**（新增）下列資訊：
   - **Interface**（介面）—選取介面。
   - **Enable**（啟用）—選取此選項讓 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。若必須手動定義芳鄰，則選擇 **p2mp**（點到多點），然後為所有可透過此介面連線的芳鄰 **Add**（新增）芳鄰 IP 位址。
   - 度量—輸入此介面的 OSPF 度量 （範圍是 0-65535；預設值是 10）。
   - **Priority**（優先順序）—輸入此介面的 OSPF 優先順序。這是選為指定路由器 (DR) 或選為備份指定路由器 (BDR) 之路由器的優先順序（範圍是 0-255；預設值是 1）。當設為零時，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。
   - 計時—如有需要，修改計時設定（不建議修改）。關於這些設定的詳細資訊，請參閱線上說明。
2. 按一下 **OK**（確定）。

STEP 6 | 設定區域#虛擬連結。

1. 在 **Virtual Link**（虛擬連結）頁籤上，為骨幹區域中將包含的每個虛擬連結 **Add**（新增）下列資訊：
   - 名稱—輸入虛擬連結的名稱。
   - **Enable**（啟用）—選取以啟用虛擬連結。
   - **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。
   - 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。
2. 按一下 **OK**（確定）以儲存虛擬連結。
3. 按一下 **OK**（確定）以儲存區域。

STEP 7 | （選用）設定驗證設定檔。

依預設，防火牆不會對 OSPF 芳鄰之間的交換使用 OSPF 驗證。(選用) 您可以透過簡單的密碼或使用 MD5 驗證來設定 OSPF 芳鄰之間的 OSPF 驗證。建議使用 MD5 驗證；它比簡單的密碼更安全。

簡單密碼 **OSPF** 驗證

1. 選取 **Auth Profiles**（驗證設定檔），然後為用於驗證 OSPF 訊息的驗證設定檔 **Add**（新增）名稱。
2. 選取簡單密碼作為密碼類型。
3. 輸入簡單密碼，然後確認。

MD5 OSPF 驗證

1. 選取 **Auth Profiles**（驗證設定檔），然後為用於驗證 OSPF 訊息的驗證設定檔 **Add**（新增）名稱。
2. 選取 **MD5** 作為 **Password Type**（密碼類型），然後 **Add**（新增）一個或多個密碼項目，包括：
   - Key-ID （範圍是 0-255）
   - 金鑰
   - 選取 **Preferred**（慣用）選項以指定用於驗證輸出訊息的金鑰。
3. 按一下 **OK**（確定）。

STEP 8 | 設定進階 OSPF 選項。

1. 在 **Advanced**（進階）頁籤上，選取 **RFC 1583 Compatibility**（**RFC 1583** 相容性）以確保與 RFC 1583 相容。
2. 為 **PF Calculation Delay (sec)**（**SPF** 計算延遲（秒））計時器指定一個值，該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（單位為秒）。較低的值可加快 OSPF 重新聚合。與防火牆對等的路由器應使用相同的延遲值，以最佳化聚合時間。
3. 為 **LSA Interval (sec)**（**LSA** 間隔（秒））計時器指定一個值，這是兩個相同 LSA 實例（相同路由器、相同類型、相同 LSA ID）的傳輸之間的最短間隔時間。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。
4. 按一下 **OK**（確定）。

STEP 9 | **Commit**（提交）您的變更。

設定 OSPFv3

OSPF 支援 IPv4 和 IPv6。如果使用 IPv6，則必須要使用 OSPFv3。

STEP 1 | 設定一般虛擬路由器設定。

STEP 2 | 設定一般 OSPFv3 組態設定。

1. 選取 **OSPFv3** 頁籤。
2. 選取 **Enable**（啟用）可啟用 OSPF 通訊協定。
3. 輸入 **Router ID**（路由器 **ID**）。
4. 如果您不想透過 OSPFv3 記住任何預設路由，請選取 **Reject Default Route**（拒絕預設路由）。這是建議的預設設定。

   如果您想透過 OSPFv3 允許重新散佈預設路由，則清除 **Reject Default Route**（拒絕預設路由）。

STEP 3 | 設定 OSPFv3 通訊協定的驗證設定檔。

OSPFv3 本身沒有任何驗證功能，它完全依賴 IPSec 保護芳鄰間的通訊。

設定驗證設定檔時，您必須使用「封裝安全有效負載」(ESP)（建議）或 IPv6「驗證標頭」(AH)。

ESP OSPFv3 驗證

1. 在 **Auth Profiles**（驗證設定檔）頁籤上，為用於驗證 OSPFv3 訊息的驗證設定檔 **Add**（新增）名稱。
2. 指定安全性原則索引 (**SPI**)（從 00000000 到 FFFFFFFF 的十六進位值）。OSPFv3 相鄰項兩端必須具有相符的 SPI 值。
3. 選取 **ESP** 作為通訊協定。
4. 選取 **Crypto Algorithm**（密碼演算法）。

   您可以選取 **None**（無），或輸入下列其中一個演算法：**SHA1**、**SHA256**、**SHA384**、**SHA512** 或 **MD5**。
5. 如果選取 None（無）以外的 **Crypto Algorithm**（密碼演算法），則輸入 **Key**（無）值，然後確認。

AH OSPFv3 驗證

1. 在 **Auth Profiles**（驗證設定檔）頁籤上，為用於驗證 OSPFv3 訊息的驗證設定檔 **Add**（新增）名稱。
2. 指定安全性原則索引 (**SPI**)。OSPFv3 相鄰項兩端之間的 SPI 必須符合。SPI 號碼必須是介於 00000000 到 FFFFFFFF 的十六進位值。
3. 選取 **AH** 作為通訊協定。
4. 選取 **Crypto Algorithm**（密碼演算法）。

   您必須輸入下列其中一個演算法：**SHA1**、**SHA256**、**SHA384**、**SHA512** 或 **MD5**。
5. 輸入 **Key**（金鑰）值，然後確認。
6. 按一下 **OK**（確定）。
7. 在 [虛擬路由器 - OSPF 驗證設定檔] 對話方塊中，再按一次 **OK**（金鑰）。

STEP 4 | 設定區域—OSPFv3 通訊協定類型。

1. 在 **Areas**（區域）頁籤上，**Add**（新增）**Area ID**（區域 **ID**）。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。
2. 在 **General**（一般）頁籤上，從區域的 **Type**（類型）清單中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。如果您選取此選項，請進行下列設定：
     - 接受摘要—接受來自其他區域的連結狀態宣告 (LSA)。如果停用虛設常式區域其「區域邊界路由器」(ABR) 介面上的此選項，OSPF 區域將可作為「完全末梢區域」(TSA) 使用，且 ABR 將不會傳播任何摘要 LSA。
     - 宣告預設路由—預設路由 LSA 將包含在對虛設常式區域及設定範圍 1-255 之已設定公制值的宣告中。
   - **NSSA** (Not-So-Stubby Area)—防火牆只會依 OSPF 路由以外的路由離開區域。若已選取，請依照虛設常式的描述設定 **Accept Summary**（接受摘要）與 **Advertise Default Route**（宣告預設路由）。如果您選取此選項，請進行下列設定：
     - 類型—選取 **Ext 1** 或 **Ext 2** 路由類型來宣告預設的 LSA。
     - 外部範圍—**Add**（新增）您要啟用或抑制宣告的外部路由範圍。

STEP 5 | 將 OSPFv3 驗證設定檔與區域或介面建立關聯。

對於區域

1. 在 **Areas**（區域）頁籤上，從表格中選取現有的區域。
2. 在 **General**（一般）頁籤上，從 **Authentication**（驗證）清單中，選取先前定義的 **Authentication Profile**（驗證設定檔）。
3. 按一下 **OK**（確定）。

對於介面

1. 在 **Areas**（區域）頁籤上，從表格中選取現有的區域。
2. 選取 **Interface**（介面）頁籤，然後從 **Auth Profile**（驗證設定檔）清單 **Add**（新增）您要與 OSPF 介面關聯的驗證設定檔。
3. 按一下 **OK**（確定）。

STEP 6 | 按一下 **OK**（確定）以儲存區域設定。

STEP 7 | （選用）設定匯出規則。

1. 在 **Export Rules**（匯出規則）頁籤上，選取 **Allow Redistribute Default Route**（允許重新散佈預設路由），以允許透過 OSPFv3 重新散佈預設路由。
2. 按一下 **Add**（新增）。
3. 輸入 **Name**（名稱）；此值必須是有效的 IPv6 子網路或有效的重新散佈設定檔名稱。
4. 選取 **New Path Type**（新路徑類型）、**Ext 1**（外部 **1**）或 **Ext 2**（外部 **2**）。
5. 為使用 32 位元值（小數點十進位表示法）的相符路由指定 **New Tag**（新標籤）。
6. 為新規則指派 **Metric**（度量）（範圍為 1 - -16777215）。
7. 按一下 **OK**（確定）。

STEP 8 | 設定進階 OSPFv3 選項。

1. 如果您想讓防火牆參與 OSPF 拓撲分配，但不用於轉送轉送流量，請在 **Advanced**（進階）頁籤上，選取 **Disable Transit Routing for SPF Calculation**（停用 **SPF** 計算的轉送路由）。
2. 為 **PF Calculation Delay (sec)**（**SPF** 計算延遲（秒））計時器指定一個值，該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（單位為秒）。較低的值可加快 OSPF 重新聚合。與防火牆對等的路由器應使用相同的延遲值，以最佳化聚合時間。
3. 為 **LSA Interval (sec)**（**LSA** 間隔（秒））計時器指定一個值，這是兩個相同 LSA 實例（相同路由器、相同類型、相同 LSA ID）的傳輸之間的最短間隔時間（單位為秒）。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。
4. （選用）設定 OSPF 非失誤性重新啟動。
5. 按一下 **OK**（確定）。

STEP 9 | **Commit**（提交）您的變更。

設定 OSPF 非失誤性重新啟動

OSPF 非失誤性重新啟動會將 OSPF 芳鄰導向，以便在服務停止時，能繼續在短暫的轉換期間透過防火牆使用路由。此行為會增加網路的穩定性，因為當定期短暫停止運作期間，路由表重新設定及相關路由擺動的頻率都會減少。

對於 Palo Alto Networks® 防火牆而言，OSPF 非失誤性重新啟動涉及下列操作：

- 防火牆作為重新啟動裝置—如果防火牆將短暫停止運作或暫時無法使用時，防火牆會將非失誤性 LSA 傳送至 OSPF 芳鄰。必須將芳鄰設定為在（非失誤性重新啟動協助程式）模式中執行。在協助程式模式中，芳鄰會收到非失誤性 LSA，以告知防火牆將在依照 **Grace Period**（寬限期）中定義的指定時段內執行非失誤性重新啟動。在寬限期間，芳鄰會繼續透過防火牆轉送路由，並傳送會透過防火牆宣告路由的 LSA。如果防火牆在寬限期到期前恢復繼續運作，則流量轉送將如以往繼續運作，網路不會中斷。如果防火牆在寬限期到期後未恢復繼續運作，則芳鄰將離開協助程式模式，並恢復正常運作，這將涉及重新設定路由表以避開防火牆。
- 防火牆作為非失誤性重新啟動協助程式—如果芳鄰路由器會短暫停止運作，可設定防火牆在非失誤性重新啟動協助程模式中運作，在這種情況下，防火牆將使用 **Max Neighbor Restart Time**（最大芳鄰重新啟動時間）。當防火牆收到來自其 OSPF 芳鄰的非失誤性 LSA 時，會繼續將流量路由至芳鄰，並透過芳鄰宣告路由，直到寬限期或最大芳鄰重新啟動時間到期為止。如果在芳鄰恢復提供服務前，這兩段期間皆未到期，則流量轉送會如以往般的繼續運作，網路不會中斷。如果在芳鄰恢復提供服務前，其中一段期間到期，則防火牆將離開協助程式模式，並恢復正常運作，這將涉及重新設定路由表以避開網路芳鄰。

STEP 1 | 選取**Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取您要設定的虛擬路由器。

STEP 2 | 選取 **OSPF** > **Advanced**（進階）或 **OSPFv3** > **Advanced**（進階）。

STEP 3 | 確認下列項已選取（預設值皆為啟用）：

- 啟用非失誤性重新啟動
- 啟用協助程式模式
- 啟用嚴格 **LSA** 檢查

上述項皆應保持為已選取，除非您的拓撲另有需求。

STEP 4 | 以秒數設定 **Grace Period**（寬限期）。

STEP 5 | 以秒數設定 **Max Neighbor Restart Time**（最大芳鄰重新啟動時間）。

確認 OSPF 操作

在認可 OSPF 組態後，您可以使用任何下列操作確認 OSPF 是否正在運作：

- 檢視路由表
- 確認 OSPF 相鄰項
- 確認 OSPF 連線已建立

檢視路由表

透過檢視路由表，您能夠瞭解是否已建立 OSPF 路由。您可以從網頁介面或 CLI 存取路由表。如果您使用的是 CLI，請使用下列命令：

- **show routing route**
- **show routing fib**

如果您要使用 Web 介面檢視路由表，可按下列工作流程操作：

STEP 1 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），並在與您關注的虛擬路由器相同的列中，按一下 **More Runtime Stats**（更多執行階段統計資料） 連結。

STEP 2 | 選取 **Routing**（路由） > **Route Table**（路由表）頁籤，然後檢查路由表的 **Flag**（標幟） 欄中是否有透過 OSPF 學得的路由。

確認 OSPF 相鄰項

使用下列工作流程確認 OSPF 相鄰項是否已建立：

STEP 1 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），並在與您關注的虛擬路由器相同的列中，按一下 **More Runtime Stats**（更多執行階段統計資料） 連結。

STEP 2 | 選取 **OSPF** > **Neighbor**（芳鄰），然後檢查 **Status**（狀態） 欄以判斷 OSPF 相鄰項是否已建立。

確認 OSPF 連線已建立

檢視系統日誌，以確認防火牆已建立 OSPF 連線。

STEP 1 | 選取 **Monitor**（監控） > **System**（系統），然後尋找訊息以確認是否已建立 OSPF 相鄰項。

STEP 2 | 選取 **OSPF** > **Neighbor**（芳鄰），然後檢查 **Status** （狀態） 欄以判斷是否已建立 OSPF 相鄰項（全部）。

BGP

邊界閘道通訊協定 (BGP) 是主要的網際網路路由通訊協定。BGP 可根據能夠在自發系統 (AS) 中使用的 IP 首碼來確定網路連線能力，其中 AS 是網路供應商已指定為單一路由原則一部分的一組 IP 首碼。

BGP 概要

BGP 在自發系統（外部 BGP 或 eBGP）之間或 AS（內部 BGP 或 iBGP）內運作，以與 BGP 發言者交換路由和連線能力資訊。防火牆提供包含下列功能的完整 BGP 實作：

- 每個虛擬路由器有一個 BGP 路由實例的規格。
- 每個虛擬路由器的 BGP 設定，包含基本參數（例如本機路由 ID 與本機 AS）與進階選項（例如路徑選取、路由反射程式、BGP 聯盟、路由波動抑制及非失誤性重新啟動）。
- 對等群組與芳鄰設定，包括芳鄰位址、遠端 AS 及進階選項，例如芳鄰屬性與連線。
- 路由原則，用於控制匯入、匯出、宣告、基於首碼的篩選及位址彙總。
- IGP-BGP 互動可使用重新散佈設定檔將路由插入 BGP。
- 驗證設定檔，可為 BGP 連線指定 MD5 驗證金鑰。驗證有助於防止路由洩露並防止成功實施 DoS 攻擊。
- 多通訊協定 BGP (MP-BGP)，允許 BGP 對等體在更新封包中攜帶 IPv6 單點傳送路由和 IPv4 多點傳送路由，允許防火牆及 BGP 對等體使用 IPv6 位址相互通訊。
- 對於前置詞，BGP 支援 AS_PATH 清單中最多 255 個 AS 數字。

MP-BGP

BGP 支援 IPv4 單點傳送首碼，但使用 IPv4 多點傳送路由或 IPv6 單點傳送首碼的 BGP 網路需要多重通訊協定 BGP (MP-BGP)，才能位址類型路由而非 IPv4 單點傳送路由。除了 BGP 對等體可在未啟用 MP-BGP 的情況下攜帶的 IPv4 單點傳送路由以外，MP-BGP 還允許 BGP 對等體在更新封包中攜帶 IPv4 多點傳送路由和 IPv6 單點傳送路由。

這樣，MP-BGP 將為使用原生 IPv6 或雙重堆疊 IPv4 和 IPv6 的 BGP 網路提供 IPv6 連線。服務提供者可向客戶提供 IPv6 服務，企業可使用服務提供者提供的 IPv6 服務。防火牆和 BGP 對等體可使用 IPv6 對等體相互通訊。

為了使 BGP 支援多網路層通訊協定（而非 IPv4 的 BGP）BGP，BGP-4 多重通訊協定擴充功能 (RFC 4760) 將使用防火牆於 BGP 更新封包中傳送和接收的多重通訊協定可連線 NLRI 屬性中的網路層可連線性資訊 (NLRI)。該屬性包含有目的地首碼資訊，包括以下兩個識別碼：

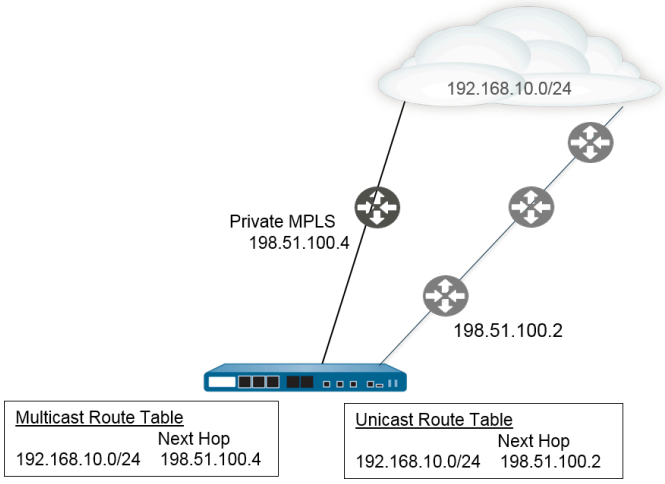
- 位址家族識別碼 (AFI)，由 IANA 在位址家族號碼中定義，指示目的地首碼是 IPv4 還是 IPv6 位址。（PAN-OS 支援 IPv4 和 IPv6 AFI。）
- PAN-OS 中的後續位址家族識別碼 (SAFI) 指示目的地首碼是單點傳送還是多點傳送位址（如果 AFI 是 IPv4），或者目的地首碼是單點傳送位址（如果 AFI 是 IPv6）。PAN-OS 不支援 IPv6 多點傳送。

如果您為 IPv4 多點傳送啟用 MP-BGP，或者您設定了多點傳送靜態路由，防火牆將支援靜態路由使用單獨的單點傳送和多點傳送路由表。您可能希望隔離進入相同目的地的單點傳送流量和多點傳送流量。多點傳送流量可使用與單點傳送流量不同的路徑，因為如果多點傳送流量非常重要，您需要讓其經過更少的躍點或更少的延遲，使其更加高效。

您還可以透過設定在 BGP 匯入或匯出路由、傳送條件式宣告或執行路由重新散佈或路由彙總時，BGP 僅適用單點傳送路由表或多點傳送路由表（或二者）中的路由，來對 BGP 的運作方式實施更多控制。

您可以啟用 MP-BGP 並選取 IPv4「位址家族」和多點傳送「後續位址家族」，或在多點傳送路由表中安裝 IPv4 靜態路由，來使用專用多點傳送 RIB（路由表）。通過上述任何種方法使用多點傳送 RIB 後，防火牆將對所有多點傳送路由和反轉路徑轉送 (RPF) 使用多點傳送 RIB。如果您想對所有路由（單點傳送和多點傳送）使用單點傳送 RIB，則不得透過任何種方式啟用多點傳送 RIB。

在下圖中，192.168.10.0/24 的靜態路由安裝在單點傳送路由表中，其下一個躍點是 198.51.100.2。但是，多點傳送流量可以使用不同路徑進入私人 MPLS 雲端；因此在多點傳送路由表中安裝相同靜態路由並使用不同的下一個躍點 (198.51.100.4)，以確保其路徑不相同。



在您設定這些 BGP 功能時，使用單獨的單點傳送路由表和多點傳送路由表能為您提供更多的靈活性和控制性：

- 按照前面的範例，將 IPv4 靜態路由安裝至單點傳送或多點傳送路由表或二者。（您只能將一個 IPv6 靜態路由安裝至單點傳送路由表）。
- 建立匯入規則，以便將與準則相符的首碼匯入單點傳送或多點傳送路由表或二者。
- 建立匯出規則，以便將與準則相符的首碼從單點傳送或多點傳送路由表或二者匯出（傳送至對等體）。
- 為條件式宣告設定 Non Exist（不存在）篩選器，以便防火牆搜尋單點傳送或多點傳送路由表（或二者），確保路由在該表中不存在，從而使防火牆宣告不同的路由。
- 為條件式宣告設定 Advertise（宣告）篩選器，以便防火牆從單點傳送或多點傳送路由表或二者宣告相符的路由。
- 重新散佈單點傳送或多點傳送路由表或二者中存在的路由。
- 為路由匯總設定宣告篩選器，以便要宣告的彙總路由來自於單點傳送或多點傳送路由表或二者。
- 反之，為路由匯總設定抑制篩選器，以便要抑制（不宣告）的彙總路由來自於單點傳送或多點傳送路由表或二者。

在您為對等體設定使用 IPv6 位址家族的 MP-BGP 時，可以在匯入規則、匯出規則、條件式宣告（「宣告」篩選器或「不存在」篩選器）以及彙總規則（「宣告」篩選器、「抑制」篩選器和「彙總路由屬性」）的 Address Prefix（位址首碼）和 Next Hop（下一個躍點）欄位中使用 IPv6 位址。

設定 BGP

執行下列工作以設定 BGP。

STEP 1 | 設定一般虛擬路由器設定。

STEP 2 | 為虛擬路由器啟用 BGP，指派路由器 ID，然後將路由器指派給 AS。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP**。
3. 為此虛擬路由器 **Enable**（啟用）BGP。
4. 為虛擬路由器的 BGP 指派一個 **Router ID**（路由器 **ID**），一般為 IPv4 位址，以確保路由器 ID 是唯一的。
5. 指派 **AS** 號碼—根據路由器 ID，虛擬路由器所屬的 AS 號碼（範圍為 1 至 4,294,967,295）。
6. 按一下 **OK**（確定）。

STEP 3 | 設定一般 BGP 設定。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **General**（一般）。
3. 選取 **Reject Default Route**（拒絕預設路由）可忽略 BGP 對等宣告的任何預設路由。
4. 選取**Install Route**（安裝路由）可安裝全域路由表中的 BGP 路由。
5. 即使當路由具有不同的多出口鑑別器 (MED) 值時，選取 **Aggregate MED**（彙總 **MED**）也可以啟用路由彙總。
6. 指定 **Default Local Preference**（預設本機偏好設定）值，此值可用於決定不同路徑中的偏好設定。
7. 選取用於確保互通性的 **AS Format**（**AS** 格式）：
   - **2** 位元組（預設值）
   - **4** 位元組

   執行階段統計資料根據 RFC 5396 使用 *asplain* 表示法顯示 *BGP 4* 位元組 *AS* 號碼。
8. 為 **Path Selection**（路徑選取）啟用或停用下列每項設定：
   - 始終比較 **MED**—啟用此比較可從不同自發系統中的芳鄰選擇路徑。
   - 具決定性的 **MED** 比較—啟用此比較可在 IBGP 對等（相同自發系統中的 BGP 對等）宣告的路由之間選擇。
9. 對於 **Auth Profiles**（驗證設定檔），**Add**（新增）一個驗證設定檔。
   - 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。此密碼將在 MD5 驗證中用作金鑰。
10. 按兩下 **OK**（確定）。

STEP 4 | （選用）進行 BGP 設定。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **Advanced**（進階）。
3. 如果您設定了 ECMP 並希望在多個 BGP 自發系統上執行 ECMP，則選取 **ECMP Multiple AS Support**（**ECMP** 多 **AS** 支援）。
4. 為 **EBGP** 執行第一個 **AS**（依預設啟用），使防火牆丟棄未在 AS_PATH 屬性中將 eBGP 對等本身的 AS 號碼列為第一個 AS 號碼的 eBGP 對等所傳入的更新封包。
5. 選取 **Graceful Restart**（非失誤性重新啟動），然後設定下列計時器：
   - 過時路由時間（秒）—指定路由可以處於過時狀態的時間長度（以秒為單位，範圍為 1 至 3600；預設值為 120）。
   - 本機重新啟動時間 秒）—指定本機裝置等待重新啟動的時間長度，以秒為單位。會向對等宣告此值（範圍為 1 至 3,600，預設值為 120）。
   - 最大對等重新啟動時間（秒）—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）。
6. 對於 **Reflector Cluster ID**（反射程式叢集 **ID**），指定代表反射程式叢集的 IPv4 識別碼。
7. 對於 **Confederation Member AS**（聯盟成員 **AS**），指定自發系統編號識別碼（又稱為子 AS 編號），此識別碼僅在 BGP 聯盟中可見。如需詳細資訊，請參閱BGP 聯盟。
8. 為每個您要設定的抑制設定檔 **Add**（新增）下列資訊，選取 **Enable**（啟用），然後按一下 **OK**（確定）：
   - 設定檔名稱—輸入用來識別設定檔的名稱。
   - 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（範圍為 0.0 至 1,000.0；預設值為 1.25）。
   - **Reuse**（重複使用）—指定路由撤銷臨界值，如果低於此值，將會再次使用隱藏路由（範圍為 0.0 至 1,000.0，預設值為 5）。
   - 最大保留時間（秒）—指定無論路由的穩定性為何，可以隱藏路由的時間長度上限（以秒為單位，範圍為 0 至 3,600；預設值為 900）。
   - 可到達的 **Decay Half Life**（秒）—指定一個時間長度，在該時間長度後，如果認為可到達路由，則路由穩定性公制會減半（以秒為單位，範圍為 0 至 3,600；預設值為 300）。
   - 無法到達的 **Decay Half Life** （秒）—指定一個時間長度，在該時間長度後，如果認為無法到達路由，則路由穩定性公制會減半（以秒為單位，範圍為 0 至 3,600；預設值為 300)。
9. 按兩下 **OK**（確定）。

STEP 5 | 設定 BGP 對等群組。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **Peer Group**（對等群組），為對等群組 **Add**（新增）**Name**（名稱），然後 **Enable**（啟用）。
3. 選取 **Aggregated Confed AS Path**（已彙總聯盟 **AS** 路徑），以包含所設定已彙總聯盟 AS 的路徑。
4. 選取 **Soft Reset with Stored Info**（使用已存資訊進行軟重設），以在更新對等設定之後執行防火牆軟重設。
5. 選取對等群組的 **Type**（類型）：
   - **IBGP**—匯出下一個躍點：選取 **Original**（原始）或 **Use self**（使用自我）。
   - **EBGP** 聯盟—匯出下一個躍點：選取 **Original**（原始）或 **Use self**（使用自我）。
   - **EBGP** 聯盟—匯出下一個躍點：選取 **Original**（原始）或 **Use self**（使用自我）。
   - **EBGP**—匯入下一個躍點：選取 **Original**（原始）或 **Use self**（使用自我）；然後 **Export Next Hop**（匯出下一個躍點）：指定 **Resolve**（解析）或 **Use self**（使用自我）。如果您要強制 BGP 從防火牆傳送至另一個 AS 內對等體的更新中的 AS_PATH 屬性中移除私人 AS 號碼，則選取 **Remove Private AS**（移除私人 **AS**）。
6. 按一下 **OK**（確定）。

STEP 6 | 設定屬於該對等群組的 BGP 對等體，然後指定其定址。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **Peer Group**（對等群組），然後選取您建立的對等群組。
3. 對於對等體，依 **Name**（名稱）**Add**（新增）對等體。
4. **Enable**（啟用）對等體。
5. 輸入對等體所述的 **Peer AS**（對等 **AS**）。
6. 選取 **Addressing**（定址）。
7. 對於 **Local Address**（本機位址），選取您要設定 BGP 的 **Interface**（介面）。如果該介面有多個 **IP** 位址，則輸入該介面中將作為 BGP 對等體的 IP 位址。
8. 對於 **Peer Address**（對等位址），選取 **IP** 並輸入 IP 位址或者選取或建立位址物件，或選取 **FQDN** 並輸入 FQDN 或類型為 FQDN 的位址物件。

   防火牆僅使用 *FQDN* 的 *DNS* 解析得到的一個 *IP* 位址（來自每個 *IPv4* 或 *IPv6* 系列類型）。如果 *DNS* 解析返回多個位址，防火牆會使用與為 *BGP* 對等機設定的 *IP* 系列類型（*IPv4* 或 *IPv6*）相符的偏好 *IP* 位址。偏好 *IP* 位址是 *DNS* 伺服器在初始回應中返回的第一個位址。只要此位址出現在後續回應中，無論其順序如何，防火牆都會保留此位址作為偏好位址。
9. 按一下 **OK**（確定）。

STEP 7 | 設定 BGP 對等體的連線設定。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **Peer Group**（對等群組），然後選取您建立的對等群組。
3. 選取您設定的 **Peer**（對等體）。
4. 選取 **Connection Options**（連線）選項。
5. 為對等體選取一個 **Auth Profile**（驗證設定檔）。
6. 設定 **Keep Alive Interval (sec)**（保持運作的間隔（秒））—基於「保留時間」設定的間隔，在此間隔後，來自該對等體的路由將被隱藏（以秒為單位，範圍為 0 至 1200；預設值為 30）。
7. 設定 **Multi Hop**（多重躍點）— IP 標頭中的存留時間 (TTL) 值（範圍為 1 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。
8. 設定 **Open Delay Time (sec)**（**Open** 延遲時間（秒））—從 TCP 交握到防火牆傳送第一個 BGP Open 訊息以建立 BGP 連線的延遲時間（以秒為單位，範圍為 0 至 240；預設值為 0）。
9. 設定 **Hold Time (sec)**（保留時間（秒））—關閉對等連線之前，來自對等體的連續 Keepalive 或 Update 訊息之間可能耗用的時間（以秒為單位，範圍為 3 至 3600，預設值為 90）。
10. 設定 **Idle Hold Time (sec)**（閒置保留時間（秒））—在重新嘗試連線對等體之前的等待時間（以秒為單位，範圍為 1 至 3600，預設值為 15）。
11. 設定 **Min Route Advertisement Interval (sec)**（最小路由公告間隔（秒））— BGP 發言者（防火牆）向宣告路由或撤銷路由的 BGP 對等體傳送兩則連續 Update 訊息的最短間隔時間（以秒為單位，範圍為 1 至 600；預設值為 30）。
12. 對於 **Incoming Connections**（連入連線），輸入 **Remote Port**（遠端連接埠），然後選取 **Allow**（允許）以允許前往此連接埠的連入流量。
13. 對於 **Outgoing Connections**（連出連線），輸入 **Local Port**（本機連接埠），然後選取 **Allow**（允許）以允許來自此連接埠的連出流量。
14. 按一下 **OK**（確定）。

STEP 8 | 設定 BGP 對等體的路由反射程式用戶端、對等處理類型、最大首碼數量以及雙向轉送偵測 (BFD)。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **BGP** > **Peer Group**（對等群組），然後選取您建立的對等群組。
3. 選取您設定的 **Peer**（對等體）。
4. 選取 **Advanced**（進階）。
5. 對於 **Reflector Client**（反射程式用戶端），選取以下任何項：
   - 非用戶端（預設值）—對等體不是路由反射程式用戶端。
   - 用戶端—對等體是路由反射程式用戶端。
   - 網狀用戶端
6. 對於 **Peering Type**（對等處理類型），選取以下任何項：
   - 雙向—兩個 BGP 對等體建立對等連線。
   - 未指定（預設值）。
7. 對於 **Max Prefixes**（最大首碼數量），輸入所支援的 IP 首碼數量上限（範圍為 1 至 100000），或者選取 **unlimited**（無限制）。
8. 若要為 RIP 介面啟用 **BFD**（只要在虛擬路由器層級未對 BGP 停用 BFD 就可取代 BGP 的 BFD 設定），請選取下列其中一項：
   - 預設—對等體僅使用預設 BFD 設定。
   - **Inherit-vr-global-setting**（預設）—對等體將繼承您為虛擬路由器的 BGP 全域選取的 BFD 設定檔。
   - 您設定的 BFD 設定檔—請參閱建立 BFD 設定檔。

   選取 ***Disable BFD***（停用 ***BFD***）以停用 *BFD* 對等體的 *BGP*。
9. 按一下 **OK**（確定）。

STEP 9 | 設定匯入與匯出規則。

匯入與匯出規則用於規則用於與其他路由器匯入和匯出路由（例如，從您的 Internet Service Provider (網際網路服務供應商 - ISP) 匯入預設路由）。

1. 選取 **Import**（匯入），在 **Rules**（規則）欄位 **Add**（新增）名稱，然後 **Enable**（啟用）匯入規則。
2. **Add**（新增）將從其中匯入路由的 **Peer Group**（對等群組）。
3. 選擇 **Match**（比對），然後定義用於篩選路由資訊的選項。您也可以定義多出口鑑別器 (MED) 值，以及到路由器或子網路的下一個躍點值以篩選路由。MED 選項是外部公制，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。
4. 選取 **Action**（動作），並根據 **Match**（比對）頁籤中定義的篩選選項，定義應會發生的動作（允許或拒絕）。如果選取 **Deny**（拒絕），您不需要定義任何其他選項。如果選取 **Allow**（允許），則定義其他屬性。
5. 選取 **Export**（匯出），然後定義匯出屬性，這些屬性與 **Import**（匯入）設定類似，但用於控制從防火牆匯出至芳鄰的路由資訊。
6. 按一下 **OK**（確定）。

STEP 10 | 設定條件式宣告功能，這可讓您在本機 BGP 路由表 (LocRIB) 中沒有不同的路由時 (表示對等或連線能力失敗)，控制要宣告什麼路由。

在要嘗試強制透過某一個 AS 路由到另一個 AS 的情況下，這會大有用處。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，即可使用此功能。

1. 選取 **Conditional Adv**（條件式宣告）並 **Add**（新增）**Policy**（原則）名稱。
2. **Enable**（啟用）條件式宣告。
3. 在 **Used By**（使用者）區段中, **Add**（新增）將使用條件式宣告原則的對等群組。
4. 選取 **Non Exist Filter**（不存在篩選器），然後定義偏好路由的網路首碼。當要宣告的路由出現在本機 BGP 路由表中時，這將指定該路由。如果將宣告首碼，而且首碼符合不存在的篩選器，則將抑制宣告。
5. 選取 **Advertise Filters**（宣告篩選器），並在本機 RIB 路由表中定義當本機路由表沒有不存在篩選器中的路由時，應宣告的路由首碼。如果將宣告首碼，而且首碼不符合不存在的篩選器，則將進行宣告。
6. 按一下 **OK**（確定）。

STEP 11 | 設定彙總選項，以彙總整理 BGP 組態中的路由。

BGP 路由彙總用於控制 BGP 彙總的定址方式。表格中的每個項目都會建立一個彙總位址。這會在得知至少有一個特定路由匹配指定的位址時，在路由表中產生彙總項目。

1. 選取 **Aggregate**（彙總），然後 **Add**（新增）彙總位址的名稱。
2. 輸入網路 **Prefix**（首碼）以作為彙總首碼的主要首碼。
3. 選取 **Suppress Filters**（隱藏篩選器），然後定義會造成隱藏匹配路由的屬性。
4. 選取**Advertise Filters**（宣告篩選器），然後定義會造成一律向對等宣告匹配路由的屬性。
5. 按一下 **OK**（確定）。

STEP 12 | 設定重新散佈規則。

此規則用於將不在本機 RIB 中的主機路由和未知路由重新散佈到對等路由器。

1. 選取**Redist Rules**（重新散佈規則），然後**Add**（新增）新的重新散佈規則。
2. 輸入 IP 子網路的 **Name**（名稱）或選取重新散佈設定檔。您也可以視需要設定新的重新散佈設定檔。
3. **Enable**（啟用）規則
4. 輸入將用於規則的路由 **Metric**（公制）。
5. 在 **Set Origin**（設定原點）清單中，選取 **incomplete**（不完整）、**igp** 或 **egp**。
6. （選用）設定 MED、本機偏好設定、AS 路徑限制及社群值。
7. 按一下 **OK**（確定）。

STEP 13 | **Commit**（提交）您的變更。

使用 MP-BGP 為 IPv4 或 IPv6 單點傳送設定 BGP 對等體

設定 BGP後，可出于下列原因，使用 MP-BGP 為 IPv4 或 IPv6 單點傳送設定 BGP 對等體：

- 為了讓 BGP 對等體攜帶 IPv6 單點傳送路由，為 MP-BGP 設定 **IPv6** 位址系列類型和 **Unicast**（單點傳送）後續位址系列，以便對等體能夠傳送包含 IPv6 單點傳送路由的 BGP 更新。BGP 對等處理（本機位址和對等位址）仍可以是 IPv4 位址或 IPv6 位址。
- 為了對 IPv6 位址（**Local Address**（本機位址）和 **Peer Address**（對等位址）使用 IPv6 位址）執行 BGP 對等處理。

下列工作顯示了如何使用 MP-BGP 啟用 BGP 對等體，以使其能夠攜帶 IPv6 單點傳送路由，從而使用 IPv6 位址執行對等處理。

此工作還顯示了如何檢視單點傳送或多點傳送路由表，以及如何檢視轉送表、BGP 本機 RIB 和 BGP 外部 RIB（路由傳送至芳鄰），以查看來自於單點傳送或多點傳送路由表或特定位址系列（IPv4 或 IPv6）的路由。

STEP 1 | 為對等體啟用 MP-BGP 延伸。

設定以下選項，以便 BGP 對等體能夠在更新封包中攜帶 IPv4 或 IPv6 單點傳送路由，防火牆能夠使用 IPv4 或 IPv6 位址與其對等體通訊。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取您要設定的虛擬路由器。
2. 選取 **BGP**。
3. 選取 **Peer Group**（對等群組），再選取一個對等群組。
4. 選取 BGP 對等體（路由器）。
5. 選取 **Addressing**（定址）。
6. 為該對等體選取 **Enable MP-BGP Extensions**（啟用 **MP-BGP** 延伸）。
7. 針對 **Address Family Type**（位址系列類型），選取 **IPv4** 或 **IPv6**。例如，選取 IPv6。
8. 對于 **Subsequent Address Family**（後續位址系列），選取 **Unicast**（單點傳送）。若您選擇 **IPv4** 作為位址系列，也可以選取 **Multicast**（多點傳送）。
9. 對于 **Local Address**（本地位址），選取 **Interface**（介面），然後可選取一個 **IP** 位址，例如 2001:DB8:55::/32
10. 對于 **Peer Address**（對等位址），輸入該對等體的 **IP** 位址，要使用與本機地址相同的位址系列 (IPv4 或 IPv6)，例如 2001:DB8:58::/32。
11. 選取 **Advanced**（進階）。
12. （選用）啟用傳送者端迴圈偵測。啟用傳送者端迴圈偵測後，防火牆將先在其 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
13. 按一下 **OK**（確定）。

STEP 2 | （選用）建立靜態路由，并將其安裝到單點傳送表中，因為您希望僅將該路由用于單點傳送。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取您要設定的虛擬路由器。
2. 選取 **Static Routes**（靜態路由），再選取 **IPv4** 或 **IPv6**，然后 **Add**（新增）一個路由。
3. 輸入靜態路由的 **Name**（名稱）。
4. 視乎於您使用 IPv4 還是 IPv6，輸入 IPv4 或 IPv6 **Destination**（目的地）首碼和網路遮罩。
5. 選取輸出 **Interface**（介面）。
6. 選取 **Next Hop**（下一個躍點）作為 **IPv6 Address**（**IPv6** 位址）（或者 **IP Address**（**IP** 位址），如果您選擇了 IPv4），然後輸入您要將該靜態路由的單點傳送流量導向到的下一個躍點位址。
7. 輸入 **Admin Distance**（管理距離）。
8. 輸入 **Metric**（度量）。
9. 對于 **Route Table**（路由表），選取 **Unicast**（單點傳送）。
10. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **Commit**（交付）。

STEP 4 | 檢視單點傳送或多點傳送路由表。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
2. 在虛擬路由器所在的列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。
3. 選取 **Routin**（路由） > **Route Table**（路由表）。
4. 對于 **Route Table**（路由表），選取 **Unicast**（單點傳送）或 **Multicast**（多點傳送），以僅顯示這些路由。
5. 對于 **Display Address Family**（顯示位址系列），選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），以金顯示該位址系列的路由。

   不支援選取 ***IPv6 Only***（僅 ***IPv6***）的 ***Multicast***（多點傳送）。

STEP 5 | 檢視轉送表。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
2. 在虛擬路由器所在的列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。
3. 選取 **Routing**（路由） > **Forwarding Table**（轉送表）。
4. 對于 **Display Address Family**（顯示位址系列），選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），以金顯示該位址系列的路由。

STEP 6 | 檢視 BGP RIB 表。

1. 檢視 BGP 本機 RIB，其中顯示了防火牆用于路由 BGP 封包的 BGP 路由。
   1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
   2. 在虛擬路由器所在的列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。
   3. 選取 **BGP** > **Local RIB**（本機 **RIB**）。
   4. 對于 **Route Table**（路由表），選取 **Unicast**（單點傳送）或 **Multicast**（多點傳送），以僅顯示這些路由。
   5. 對于 **Display Address Family**（顯示位址系列），選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），以金顯示該位址系列的路由。

      不支援選取 ***IPv6 Only***（僅 ***IPv6***）的 ***Multicast***（多點傳送）。

2. 檢視 BGP 外部 RIB 表，其中顯示了防火牆用于傳送至 BGP 芳鄰的路由。
   1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
   2. 在虛擬路由器所在的列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。
   3. 選取 **BGP** > **RIB Out**（外部 **RIB**）。
   4. 對于 **Route Table**（路由表），選取 **Unicast**（單點傳送）或 **Multicast**（多點傳送），以僅顯示這些路由。
   5. 對于 **Display Address Family**（顯示位址系列），選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），以金顯示該位址系列的路由。

      不支援選取 ***IPv6 Only***（僅 ***IPv6***）的 ***Multicast***（多點傳送）。

使用 MP-BGP 為 IPv4 多點傳送設定 BGP 對等體

設定 BGP，如果您希望 BGP 對等體能夠在 BGP 更新中學習并傳遞 IPv4 多點傳送路由，則使用 MP-BGP 為 IPv4 多點傳送設定 BGP 對等體。您將能夠將單點傳送流量與多點傳送流量隔離，或者使用 MP-BGP 中所列的功能，以僅適用單點傳送路由表或多點傳送路由表中的路由或同時使用單點傳送路由表和多點傳送路由表中的路由。

如果您僅希望支援多點傳送流量，則必須使用篩選器來清除單點傳送流量。

對于多點傳送流量，防火牆并不支援 ECMP。

STEP 1 | 啟用 MP-BGP 擴充，以便 BGP 對等體能夠交換 IPv4 多點傳送路由。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取您要設定的虛擬路由器。
2. 選取 **BGP**。
3. 選取 **Peer Group**（對等群組），然後選取一個對等群組和 BGP 對等體。
4. 選取 **Addressing**（定址）。
5. 選取 **Enable MP-BGP Extensions**（啟用 **MP-BGP** 延伸）。
6. 對于 **Address Family Type**（位址系列類型），選取 **IPv4**。
7. 對于 **Subsequent Address Family**（後續位址系列），選取 **Unicast**（單點傳送），然後選取 **Multicast**（多點傳送）。
8. 按一下 **OK**（確定）。

STEP 2 | （選用）建立 IPv4 靜態路由，然後僅在多點傳送路由表中安裝。

您可以執行此操作以將 BGP 對等體的多點傳送流量導向至特定的下一個躍點，如 MP-BGP 中的拓撲所示。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取您要設定的虛擬路由器。
2. 選取 **Static Routes**（靜態路由） > **IPv4**，然後 **Add**（新增） 路由 **Name**（名稱）。
3. 輸入 IPv4 **Destination**（目的地）首碼和網路遮罩。
4. 選取輸出 **Interface**（介面）。
5. 選取 **Next Hop**（下一個躍點）作為 **IP Address**（**IP** 位址），然後輸入您要將該靜態路由多點傳送流量導向到的下一個躍點的 IP 位址。
6. 輸入 **Admin Distance**（管理距離）。
7. 輸入 **Metric**（度量）。
8. 對于 **Route Table**（路由表），選取 **Multicast**（多點傳送）。
9. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **Commit**（交付）。

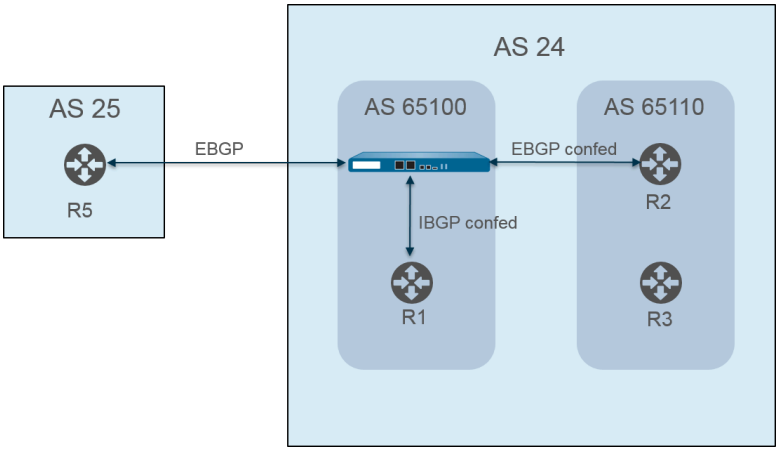
STEP 4 | 檢視路由表。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
2. 在虛擬路由器所在的列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。
3. 選取 **Routin**（路由） > **Route Table**（路由表）。
4. 對于 **Route Table**（路由表），選取 **Unicast**（單點傳送）或 **Multicast**（多點傳送），以僅顯示這些路由。
5. 對于 **Display Address Family**（顯示位址系列），選取 **IPv4 Only**（僅 **IPv4**）、**IPv6 Only**（僅 **IPv6**）或 **IPv4 and IPv6**（**IPv4** 和 **IPv6**），以金顯示該位址系列的路由。

STEP 5 | 若要檢視轉送表、BGP 本機 RIB 或 BGP 外部 RIB 表格，請參閱使用 MP-BGP 為 IPv4 或 IPv6 單點傳送設定 BGP 對等體。

BGP 聯盟

透過 BGP 聯盟，可將自發系統 (AS) 分成兩個或更多子自發系統（子 AS），以減輕 IBGP 全網狀要求所導致的負荷。子 AS 中的防火牆（或其他路由裝置）仍然必須與同一子 AS 中的其他防火牆建立 iBGP 全網狀。子自發系統中需執行 BGP 對等處理，以在主 AS 中實現完全連線。子 AS 中的相互對等的防火牆構成 IBGP 聯盟對等。兩個不同子 AS 中的相互對等的防火牆構成 EBGP 聯盟對等。來自不同的相連自發系統的兩個防火牆構成 EBGP 對等。

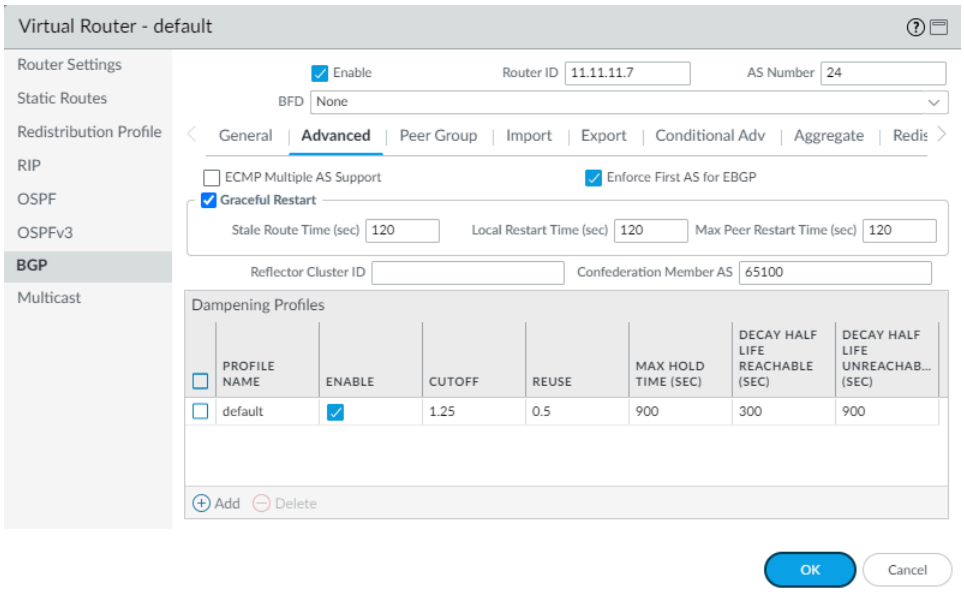


自發系統採用公共（全域指派）AS 號碼進行識別，例如上圖中的 AS 24 與 AS 25。在 PAN-OS 環境中，您為各子 AS 指派唯一的聯盟成員 AS 號碼，此號碼為私密號碼，僅在 AS 中可見。在本圖中，聯盟號碼為 AS 65100 與 AS 65110。（RFC6996，為私用而保留自發系統 (AS)，表明 IANA 保留 AS 號碼 64512-65534 以供私用。）

在 AS 中，子 AS 聯盟彼此之間像是完整的自發系統。但是，防火牆將 AS 路徑傳送至 EBGP 對等時，AS 路徑中僅會顯示公共 AS 號碼；不會包含私密子 AS（聯盟成員 AS）號碼。

防火牆與 R2 之間為 BGP 對等；圖中的防火牆具有以下相關組態設定：

- AS 號碼—24
- 聯盟成員 AS—65100
- 對等處理類型—EBGP 聯盟
- 對等 AS—65110



AS 65110 中的路由器 2 (R2) 採用以下設定：

- AS 號碼—24
- 聯盟成員 AS—65110
- 對等處理類型—EBGP 聯盟
- 遠端 AS—65100

防火牆與 R1 之間同樣為 BGP 對等。防火牆具有以下額外組態：

- AS 號碼—24
- 聯盟成員 AS—65100
- 對等處理類型—IBGP 聯盟
- 對等 AS—65110

R1 採用以下設定：

- AS 號碼—24
- 聯盟成員 AS—65110
- 對等處理類型—IBGP 聯盟
- 遠端 AS—65100

防火牆與 R5 之間為 BGP 對等。防火牆具有以下額外組態：

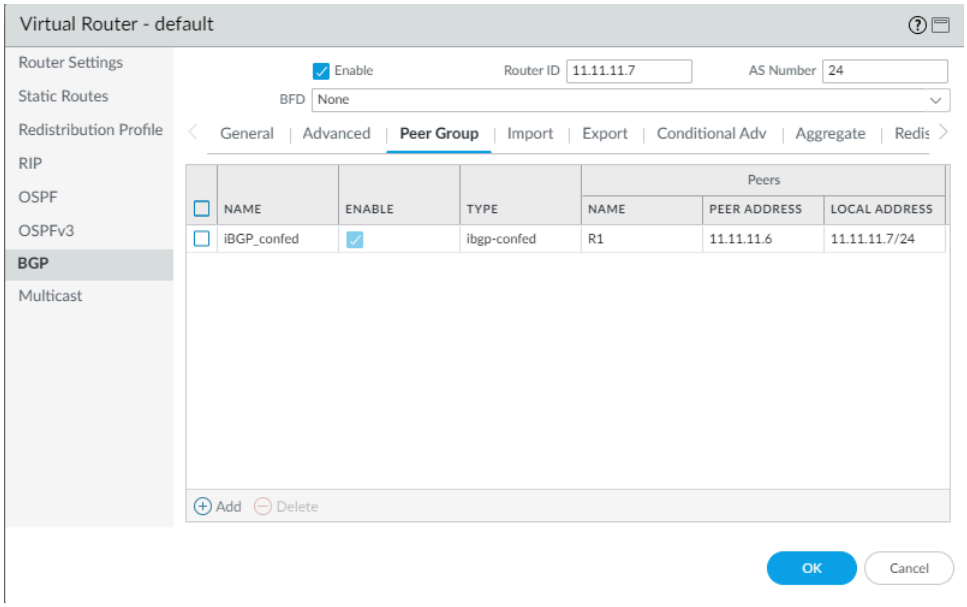
- AS 號碼—24
- 聯盟成員 AS—65100
- 對等處理類型—EBGP
- 遠端 AS—25

R5 採用以下設定：

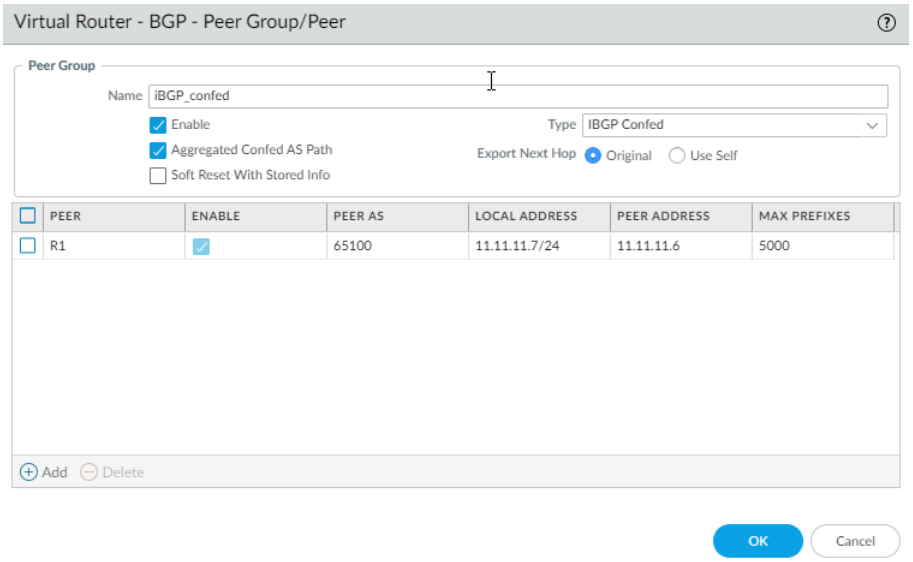
- AS—25

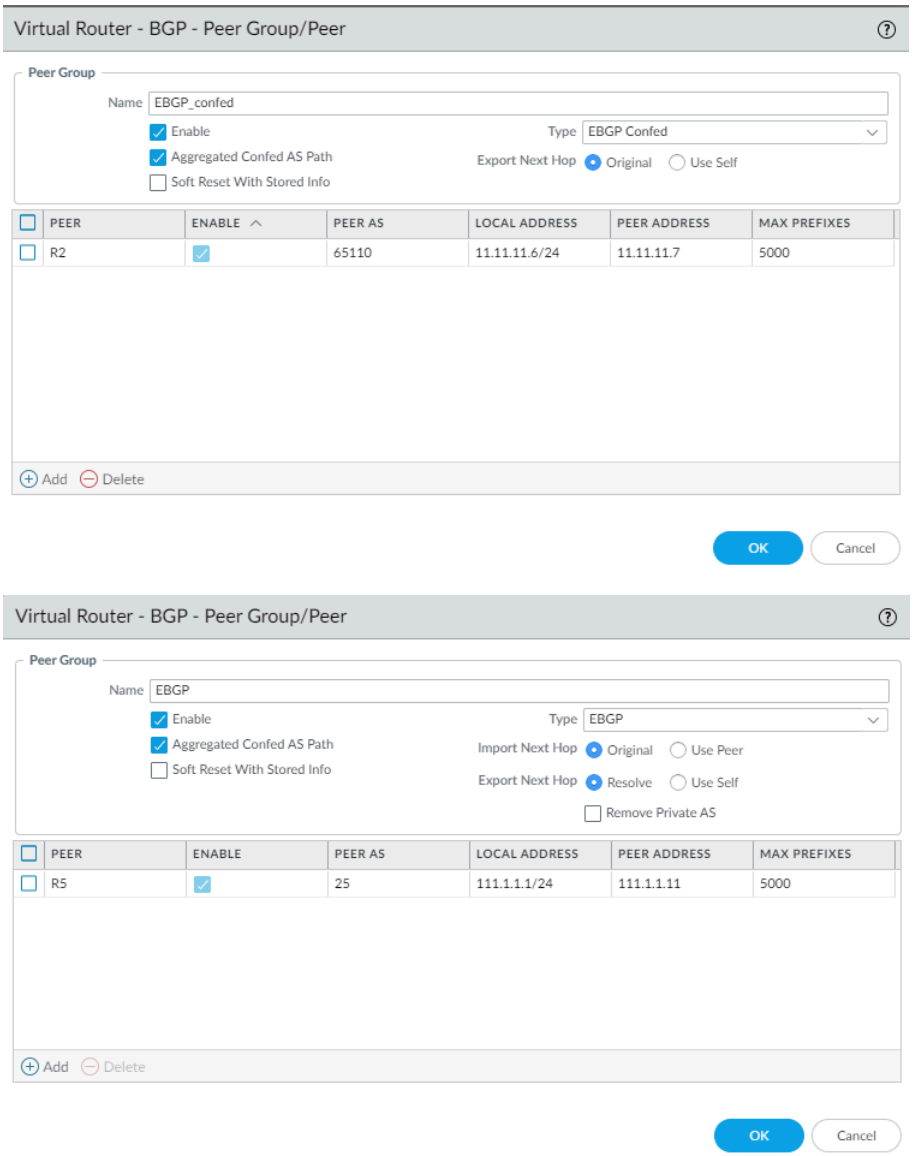
- 對等處理類型—EBGP
- 遠端 AS—24

防火牆設定為與 R1、R2 和 R5 對等後，其對等會顯示在 **Peer Group**（對等群組）頁籤中：

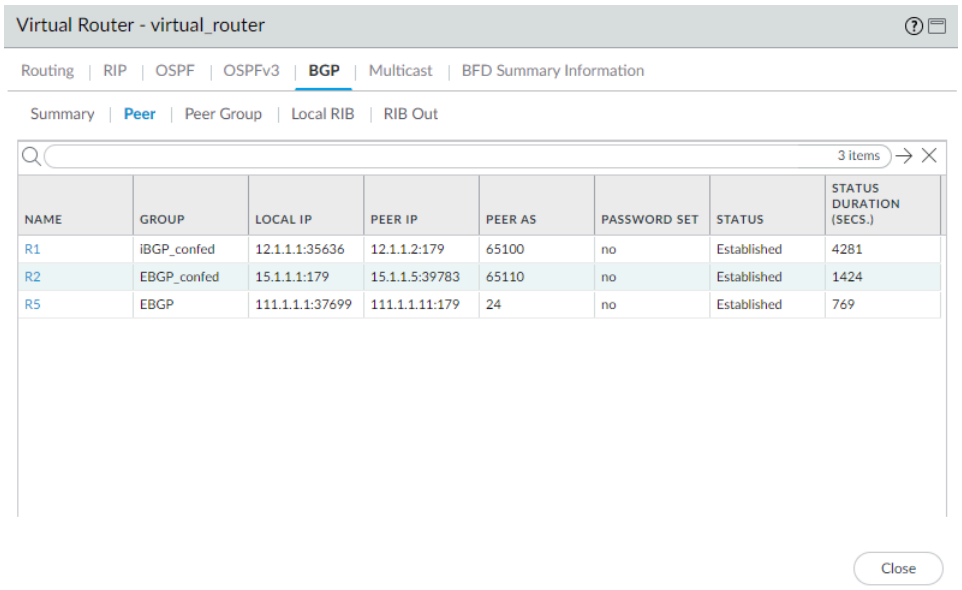


防火牆顯示 R1、R2 和 R5 對等：

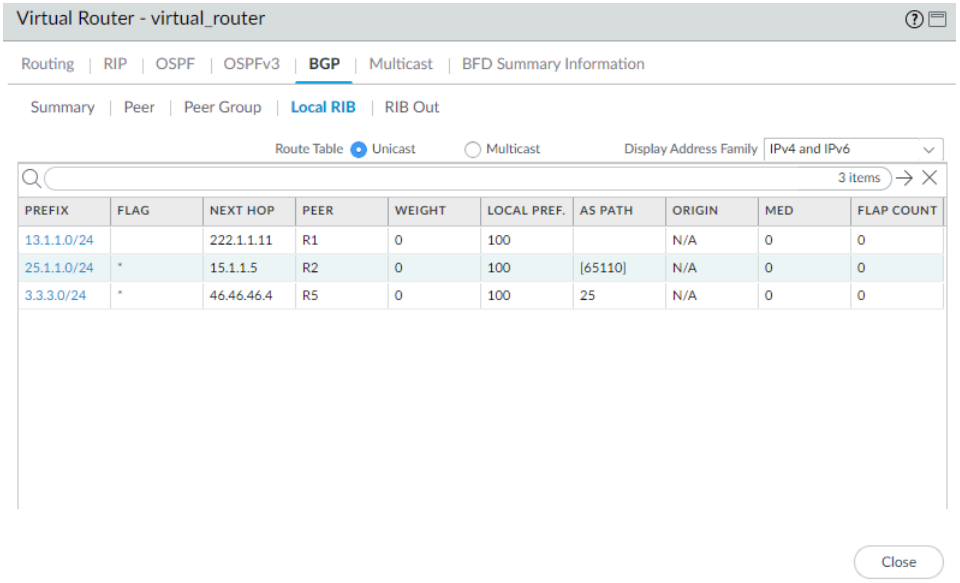




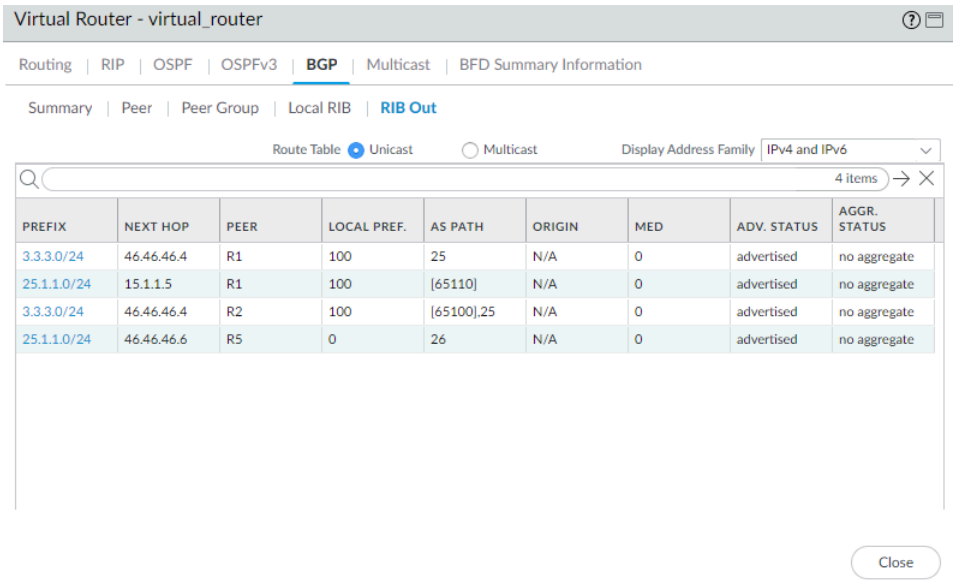
若要驗證已建立防火牆至對等的路由，在虛擬路由器的畫面上，選取 **More Runtime Stats**（更多執行階段統計資料）並選取 **Peer**（對等）頁籤。



選取 **Local RIB**（本機 **RIB**）頁籤，以檢視儲存在路由資訊庫 (RIB) 中的路由資訊。



然後選取 **RIB Out**（外部 **RIB**）頁籤。



IP 多點傳送

IP 多點傳送是一組通訊協定，網路設備使用這些通訊協定透過一次傳輸功能將多點傳送 IP 資料包傳送至一組相應接收端，而不是將流量單點傳送到多個接收端，從而節省頻寬。IP 多點傳送適用於一個來源（或多個來源）到多個接收端之間的通訊（如音訊或視訊串流、IPTV、視訊會議）以及其他通訊的分佈（如新聞和財務資料）。

多點傳送位址標識一組想要接收通往該位址之流量的接收端。您不應使用為特殊用途保留的多點傳送位址，例如範圍 224.0.0.0 到 224.0.0.255 或 239.0.0.0 到 239.255.255.255。多點傳送流量使用 UDP，不會重新傳送遺漏的封包。

Palo Alto Networks® 防火牆支援的 IP 多點傳送與通訊協定獨立多點傳送 (PIM) 位於您為防火牆上虛擬路由器設定的 Layer 3 介面上。

對於多點傳送路由，Layer 3 介面類型可以是乙太網路、彙總乙太網路 (AE)、VLAN、回送或通道。介面群組允許您使用相同的網際網路群組管理通訊協定 (IGMP) 和 PIM 參數一次設定多個防火牆介面，且具有相同的群組權限（允許多點傳送群組接受來自任意來源或僅來自特定來源的流量）。介面只可以屬於一個介面群組。

防火牆支援 Ipv4 多點傳送 - 不支援 Ipv6 多點傳送。防火牆也不支援 Layer 2 或 Virtual Wire 介面類型的 PIM 密集模式 (PIM-DM)、IGMP Proxy、IGMP 靜態加入、任意傳送 RP、GRE 或多點傳送組態。但是，Virtual Wire 介面可以傳遞多點傳送封包。此外，Layer 2 介面可以在不同 VLAN 之間切換 Layer 3 IPv4 多點傳送封包，防火牆將使用輸出介面的 VLAN ID 重新標記 VLAN ID。

必須為虛擬路由器啟用多點傳送，並為輸入和輸出介面啟用 PIM，才能使介面接收或轉送多點傳送封包。除了 PIM 之外，還必須在面向接收端的輸出介面上啟用 IGMP。您必須設定安全性原則規則，以允許 IP 多點傳送流量通往名為 **multicast**（多點傳送）的預先定義 Layer 3 目的地區域或 **any**（任意）目的地區域。

IGMP

網際網路群組管理通訊協定 (IGMP) 是一種 Ipv4 通訊協定，多點傳送接收端使用該通訊協定與 Palo Alto Networks® 防火牆上的介面進行通訊，防火牆使用該通訊協定追蹤多點傳送群組的成員資格。當主機想要接收多點傳送流量時，其 IGMP 的實作會傳送 IGMP 成員資格報告訊息；反之，接收路由器會將 PIM 加入訊息傳送到主機想要加入之群組的多點傳送群組位址。然後，在同一實體網路（例如乙太網路區段）上啟用 IGMP 的路由器使用 PIM 與其他啟用 PIM 的路由器進行通訊，以確定從來源到相應接收端的路徑。

僅在面向多點傳送接收端的介面上啟用 IGMP。接收端離虛擬路由器只有一個 Layer 3 躍點遠。IGMP 訊息是 TTL 值為 1 的 Layer 2 訊息，因此不能通過 LAN。

當您設定 IP 多點傳送時，指定介面是使用 IGMP 第 1 版、IGMP 第 2 版還是 IGMP 第 3 版。您可以強制執行 IP 路由器警示選項 RFC 2113，以便使用 IGMPv2 或 IGMPv3 的傳入 IGMP 封包具有 IP 路由器警示選項。

依預設，介面接受所有多點傳送群組的 IGMP 成員資格報告。您可以設定多點傳送群組權限，以控制虛擬路由器從任何來源（「任意來源多點傳送」或 ASM，基本上為 PIM 稀疏模式 (PIM-SM)）接受成員資格報告的群組。您還可以指定虛擬路由器從特定來源（「PIM 特定來源多點傳送」[PIM-SSM]）接受成員資格報告的群組。如果為 ASM 或 SSM 群組指定權限，則虛擬路由器將拒絕來自其他群組的成員資格報告。介面必須使用 IGMPv3 傳遞 PIM-SSM 流量。

您可以指定 IGMP 可同時處理介面的最大來源數和最大多點傳送群組數。

虛擬路由器定期向多點傳送群組的所有接收端多點傳送 IGMP 查詢。接收端使用 IGMP 成員資格報告回應 IGMP 查詢，該報告用於確認接收端是否仍希望接收該群組的多點傳送流量。虛擬路由器維持一個包含接收端的多點傳送群組表；僅在已加入該群組的多點傳送分佈向下樹狀目錄中仍有接收端時，虛擬路由器才會將多點傳送封包從介面轉送到下一躍點。虛擬路由器不會準確追蹤哪些接收端已加入群組。子網路上只有一個路由器回應 IGMP 查詢，即 IGMP 查詢程式 - IP 位址最低的路由器。

您可以設定具有 IGMP 查詢間隔的介面以及接收端回應查詢所允許的時間量（最大查詢回應時間）。當虛擬路由器從接收端收到 IGMP 離開訊息以離開群組時，虛擬路由器會檢查接收到離開訊息的介面是否未設定 Immediate Leave（立即離開）選項。在未設定 Immediate Leave（立即離開）選項的情況下，虛擬路由器傳送查詢以確定是否仍有該群組的接收端成員。「最後一個成員查詢間隔」指定允許該群組剩餘接收端回應的秒數，並確認它們是否仍然需要該群組的多點傳送流量。

介面支援 IGMP 加強性變數，您可以對其進行調整，以便防火牆隨後調整群組成員資格間隔、其他查詢程式顯示間隔、啟動查詢計數和最後一個成員查詢計數。較高的加強性變數可以容納可能捨棄封包的子網路。

檢視 IP 多點傳送資訊以查看啟用 IGMP 的介面、IGMP 版本、查詢程式位址、加強性設定、多點傳送群組和來源的數量限制，以及介面是否設定為 Immediate Leave （立即離開）。您還可以查看介面所屬的多點傳送群組以及其他 IGMP 成員資格資訊。

Pim

IP 多點傳送使用路由器之間的通訊協定獨立多點傳送 (PIM) 路由通訊協定，確定多點傳送封包從來源到接收端（多點傳送群組成員）所採取之分佈樹狀目錄上的路徑。Palo Alto Networks® 防火牆支援 PIM 稀疏模式 (PIM-SM) (RFC 4601)、PIM 任意來源多點傳送 (ASM)（有時稱為 PIM 稀疏模式）和 PIM 特定來源多點傳送 (SSM)。在 PIM-SM 中，在屬於多點傳送群組的接收端（使用者）要求來源傳送流量之後，來源才會轉送多點傳送流量。當主機想要接收多點傳送流量時，其 IGMP 的實作會傳送 IGMP 成員資格報告訊息，接收路由器隨後會將 PIM 加入訊息傳送到其想要加入之群組的多點傳送群組位址。

- 在 **ASM** 中，接收端使用 IGMP 為多點傳送群組位址要求流量；任何來源皆可產生這種流量。因此，接收端不一定知道傳送端，並且接收端可以接收其不感興趣的多點傳送流量。
- 在 **SSM** (RFC 4607) 中，接收端使用 IGMP 來要求從一個或多個特定來源到多點傳送群組位址的流量。接收端知道傳送端的 IP 位址，並只會接收所需的多點傳送流量。SSM 要求使用 IGMPv3。您可以覆寫預設的 SSM 位址空間，即 232.0.0.0/8。

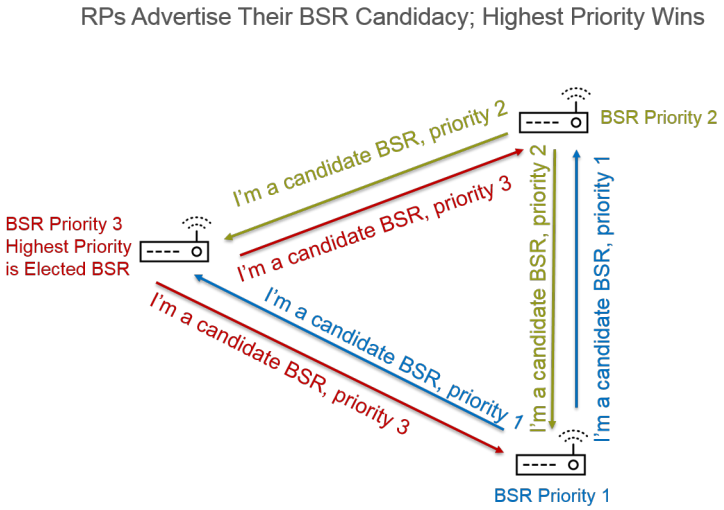
在 Palo Alto Networks 防火牆上設定 IP 多點傳送時，必須為介面啟用 PIM 以轉送多點傳送流量，即使在面向接收端的介面上亦是如此。這與 IGMP 不同，後者僅在面向接收端的介面上啟用。

ASM 需要一個會合點 (RP)，該會合點是一種位於共用分佈樹狀目錄的連接點或根部的路由器。多點傳送網域的 RP 可作為所有多點傳送群組成員向其傳送加入訊息的單一點。此行為降低了路由迴圈發生的可能性，但如果群組成員將其加入訊息傳送到多個路由器，則會發生路由迴圈。（SSM 不需要 RP，因為特定來源多點傳送使用最短路徑樹狀目錄，因此不需要 RP。）

在 ASM 環境中，虛擬路由器可用兩種方法確定哪個路由器是多點傳送的 RP：

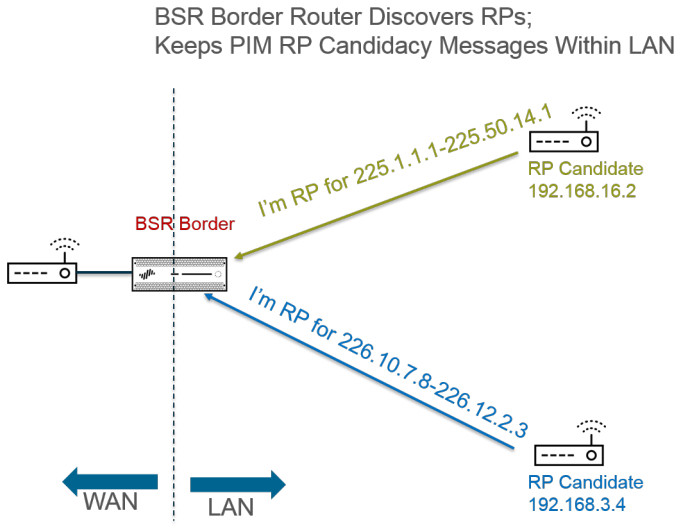
- 靜態 **RP** 至群組的對應—將防火牆上的虛擬路由器設定為充當多點傳送群組的 RP。若要設定本機 RP，則可設定靜態 RP 位址或指定本機 RP 為候選 RP 並動態選擇該 RP（根據最低優先順序值）。您還可以為本機 RP 未涵蓋的不同群組位址範圍靜態設定一個或多個外部 RP，有助於您對多點傳送流量進行負載平衡，從而使所有 RP 不會超載。

- 啟動程序路由器 **(BSR)**—(RFC 5059)—定義 BSR 的角色。首先，BSR 的候選項會彼此宣告其優先順序，然後將優先順序最高的候選項選為 BSR，如下圖所示：



接下來，當候選 RP 定期將 BSR 訊息單點傳送到 BSR（包含其 IP 位址以及它們將在其中充當 RP 的多點傳送群組範圍）時，BSR 會發現 RP。您可以將本機虛擬路由器設定為候選 RP，在這種情況下，虛擬路由器會針對一個或多個特定多點傳送群組宣告其 RP 候選資格。BSR 向 PIM 網域中的其他 RP 傳送 RP 資訊。

在為介面設定 PIM 時，若防火牆上的介面位於遠離企業網路的企業邊界，則可以選取 BSR Border（BSR 邊界）。BSR Border（BSR 邊界）設定可防止防火牆在 LAN 外部傳送 RP 候選資格 BSR 訊息。在下圖中，為面向 LAN 的介面啟用了 BSR Border（BSR 邊界），並且該介面具有最高優先順序。如果虛擬路由器同時具有靜態 RP 和動態 Rp（從 BSR 獲知），則可以在設定本機靜態 RP 時指定靜態 RP 是否應覆寫群組的已知 RP。



為了讓 PIM 稀疏模式通知 RP 其具有向下傳送共用樹狀目錄的流量，RP 必須知道來源。當指定路由器 (DR) 在 PIM 暫存器訊息中封裝來自主機的第一個封包並將該封包單點傳送到其本機網路上的 RP 時，主機通知 RP 其正在向多點傳送群組位址傳送流量。DR 還將刪改訊息從接收端轉送到 RP。RP 維持傳送到多點傳送群組之來源的 IP 位址清單，RP 可以從來源轉送多點傳送封包。

PIM 網域中的路由器為何需要 DR？當路由器向交換器傳送 PIM 加入訊息時，兩個路由器可以接收該訊息並將其轉送到同一個 RP，從而產生備用流量並浪費頻寬。為了防止不必要的流量，PIM 路由器選擇 DR（IP 位址最高的路由器），並且只有 DR 將加入訊息轉送給 RP。或者，您可以為介面群組指派 DR 優先順序，從而優先於 IP 位址比較。提醒一下，DR 正在轉送（單點傳送）PIM 訊息，而不會多點傳送 IP 多點傳送封包。

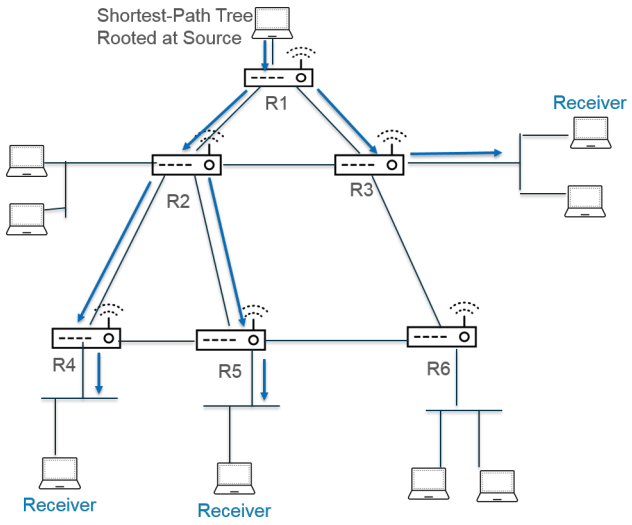
您可以指定介面群組允許與虛擬路由器建立對等關係之 PIM 芳鄰（路由器）的 IP 位址。依預設，所有啟用 PIM 的路由器都可以是 PIM 芳鄰，但使用用於限制芳鄰的選項可以保護 PIM 環境中的虛擬路由器。

- 最短路徑樹狀目錄 (SPT) 與共用樹狀目錄
- PIM 判斷提示機制
- 反轉路徑轉送

最短路徑樹狀目錄 (SPT) 與共用樹狀目錄

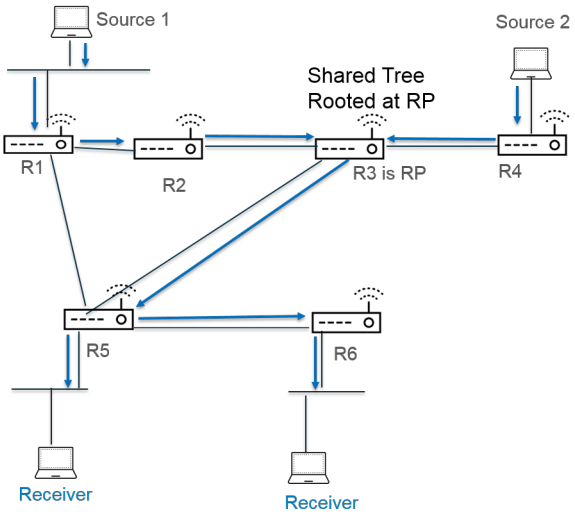
在接收端加入多點傳送群組之後，多重存取網路中的路由器建置將資料傳送到該群組中每個接收端所需的路由路徑。傳送到多點傳送群組的每個 IP 資料包會分配（轉送）給所有成員。路由路徑建構了一種用於多點傳送封包的分佈樹狀目錄。多點傳送分佈樹狀目錄的目標是，路由器在封包達到路徑散度時複製多點傳送封包，路由器必須將封包向下傳送到多條路徑以抵達所有群組成員，但分佈樹狀目錄必須避免將封包向下傳送到不存在相應接收端的路徑。分佈樹狀目錄為以下其中一種：

- 來源樹狀目錄—從多點傳送來源（樹狀目錄的根）經由網路到多點傳送群組中接收端的路徑。來源樹狀目錄是多點傳送封包從來源到接收端可以採用的最短路徑，因此亦稱為最短路徑樹狀目錄 **(SPT)**。傳送端和接收端會標註為來源和多點傳送群組配對，縮寫為 (S, G)；例如 (192.168.1.1, 225.9.2.6)。下圖說明了從來源到三個接收端的三個最短路徑樹狀目錄。



- 共用樹狀目錄—以 RP 而不是多點傳送來源為根的路徑。共用樹狀目錄也稱為 RP 樹狀目錄或 RPT。路由器將來自各種來源的多點傳送封包轉送到 Rp，然後 RP 將封包向下轉送到共用樹狀目錄。共用樹狀目錄會標註為 (*, G)，使用萬用字元作為來源，因為屬於多點傳送群組的所有來

源會共用來自 RP 的相同分佈樹狀目錄。共用樹狀目錄註釋的示例是 (*, 226.3.1.5)。下圖說明了從 RP 的根到接收端的共用樹狀目錄。



特定來源多點傳送 (SSM) 使用來源樹狀目錄分佈。當您設定 IP 多點傳送以使用「任意來源多點傳送」(ASM) 時，您可以透過設定群組的 SPT 臨界值來指定 Palo Alto Networks® 防火牆上的虛擬路由器使用哪個分佈樹狀目錄將多點傳送封包遞送到該群組：

- 依預設，虛擬路由器在收到群組或首碼的第一個多點傳送封包時，會將多點傳送路由從共用樹狀目錄切換到 SPT（**SPT Threshold**（**SPT** 臨界值）設定為 0）。
- 當在任何時間內到達任何介面上之指定多點傳送群組或首碼的封包的總千位元數達到已設定數量時，可以將虛擬路由器設定為切換到 SPT。
- 您可以將虛擬路由器設定為絕不會切換到群組或首碼的 SPT（它會繼續使用共用樹狀目錄）。

SPT 需要更多記憶體，因此請根據群組的多點傳送流量層次選擇設定。如果虛擬路由器切換到 SPT，則封包將從來源（而不是 RP）發出，並且虛擬路由器會向 RP 傳送「刪改」訊息。來源將該群組的後續多點傳送封包向下傳送到最短路徑樹狀目錄。

PIM 判斷提示機制

為了防止多重存取網路上的路由器將相同的多點傳送流量轉送到同一個下一躍點（這會產生備用流量並浪費頻寬），PIM 使用判斷提示機制為多重存取網路選擇單一 PIM 轉送程式。

如果虛擬路由器從介面（虛擬路由器已將其關聯作為封包中所識別之相同 (S,G) 配對的傳出介面）上的來源接收多點傳送封包，則表示這是重複封包。因此，虛擬路由器將包含其度量的判斷提示訊息傳送到多重存取網路上的其他路由器。然後，路由器以這種方式選擇 PIM 轉送程式：

1. PIM 轉送程式是與多點傳送來源管理距離最短的路由器。
2. 若為最短管理距離的連結，則 PIM 轉送程式為具有至來源的最佳單點傳送路由度量的路由器。
3. 若為最佳度量的連結，則 PIM 轉送程式為具有最高 IP 位址的路由器。

未選為 PIM 轉送程式的路由器會停止將流量轉送到 (S,G) 配對中識別的多點傳送群組。

設定 IP 多點傳送時，可以設定虛擬路由器從介面傳送 PIM 判斷提示訊息的間隔（判斷提示間隔）。檢視 IP 多點傳送資訊時，**PIM Interface**（**PIM** 介面）頁籤顯示介面的判斷提示間隔。

反轉路徑轉送

PIM 使用反轉路徑轉送 (RPF) 防止多點傳送路由迴圈，方式是利用虛擬路由器上的單點傳送路由表。當虛擬路由器收到多點傳送封包時，它會在其單點傳送路由表中查找多點傳送封包的來源，以瞭解與該來源 IP 位址相關聯的傳出介面是否為該封包到達的介面。如果介面相符，則虛擬路由器會複製該封包並將其從介面轉送到群組中的多點傳送接收端。如果介面不相符，則虛擬路由器會丟棄該封包。單點傳送路由表基於基礎靜態路由或網路使用的內部閘道通訊協定 (IGP)，例如 OSPF。

PIM 還使用 RPF 建置到來源的最短路徑樹狀目錄，一次一個 PIM 路由器躍點。虛擬路由器具有多點傳送來源的位址，因此虛擬路由器選取上游 PIM 芳鄰作為其返回至來源的下一躍點，虛擬路由器將使用該芳鄰轉送單點傳送封包到來源。下一躍點路由器執行相同動作。

在 RPF 成功並且虛擬路由器在其多點傳送路由資訊庫 (mRIB) 中具有路由項目之後，虛擬路由器在其多點傳送轉送資訊庫（多點傳送轉送表或 mFIB）中維持基於來源的樹狀目錄項目 (S,G) 和共用樹狀目錄項目 (*,G)。每個項目包括來源 IP 位址、多點傳送群組、傳入介面（RPF 介面）和傳出介面清單。一個項目可以有多個傳出介面，因為最短路徑樹狀目錄可以在路由器處形成分支，而路由器必須將封包轉出多個介面以抵達位於向下不同路徑之群組的接收端。當虛擬路由器使用 mFIB 轉送多點傳送封包時，它會先比對 (S,G) 項目，然後再試圖比對 (*,G) 項目。

若要向 BGP 宣告多點傳送來源首碼 （使用 Ipv4 位址系列和多點傳送後續位址系列設定 MP-BGP），則防火牆一律對防火牆在多點傳送後續位址系列下收到的 BGP 路由執行 RPF 檢查。

檢視 IP 多點傳送資訊以瞭解如何檢視 mFIB 和 mRIB 項目。請謹記，多點傳送路由表 (mRIB) 不同於單點傳送路由表 (RIB)。

設定 IP 多點傳送

設定 Palo Alto Networks® 防火牆之虛擬路由器上的介面，以接收和轉送 IP 多點傳送 封包。您必須為虛擬路由器啟用 IP 多點傳送，在輸入介面和輸出介面上設定通訊協定獨立多點傳送 (PIM)，並在面向接收端的介面上設定網際網路群組管理通訊協定 (IGMP)。

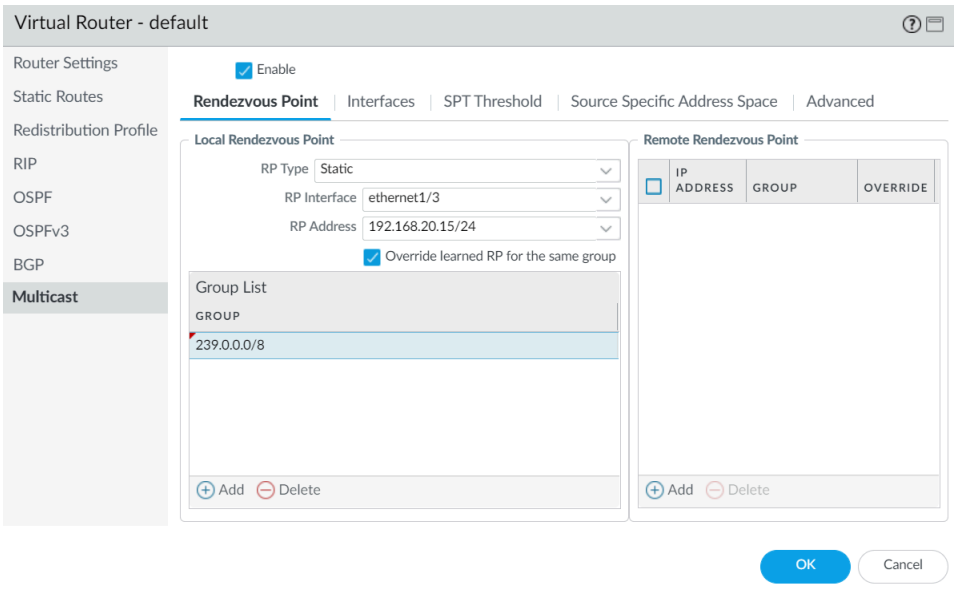
STEP 1 | 針對虛擬路由器啟用 IP 多點傳送。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **Multicast**（多點傳送），然後 **Enable**（啟用）IP 多點傳送。

STEP 2 | （僅限 ASM）若虛擬路由器所在的多點傳送網域使用任意來源多點傳送 (ASM)，請識別並設定多點傳送群組的本機與遠端會合點 (RP)。

1. 選取 **Rendezvous Point**（會合點）。
2. 選取本機 **RP Type**（**RP** 類型），可確定如何選擇 RP（選項為 **Static**（靜態）、**Candidate**（候選）或 **None**（無））：

   - **Static**（靜態）—建立 RP 到多點傳送群組的靜態對應。設定靜態 RP 要求您在 PIM 網域中的其他 PIM 路由器上明確設定相同的 RP。
     - 選取 **RP Interface**（**RP** 介面）。有效的介面類型是 Layer3、Virtual Wire、回送、VLAN、彙總乙太網路 (AE) 和通道。
     - 選取 **RP Address**（**RP** 位址）。所選之 RP 介面的 IP 位址將填入清單。
     - 選取 **Override learned RP for the same group**（覆寫相同群組的已知 **RP**），使該靜態 RP 用作 RP，而不是群組清單中的群組選擇的 RP。
     - **Add**（新增）該 RP 作為 RP 的一個或多個多點傳送 **Groups**（群組）。



   - **Candidate**（候選）—根據優先順序建立 RP 到多點傳送群組的動態對應，使 PIM 網域中的每個路由器自動選擇相同的 RP。
     - 選取候選 RP 的 **RP Interface**（**RP** 介面）。有效的介面類型包括 Layer 3、回送、VLAN、彙總乙太網路 (AE) 與通道。
     - 選取候選 RP 的 **RP Address**（**RP** 位址）。所選之 RP 介面的 IP 位址將填入清單。
     - （選用）變更候選 RP 的 **Priority**（優先順序）。防火牆將候選 RP 的優先順序與其他候選 RP 的優先順序進行比較，以確定哪一個作為指定群組的 RP；防火牆選取優先順序值最低的候選 RP（範圍為 0 到 255；預設值為 192）。
     - （選用）變更 **Advertisement Interval (sec)**（宣告時間間隔（秒））（範圍是 1 到 26,214；預設值為 60）。
     - 輸入與 RP 通訊之多點傳送群組的 **Group List**（群組清單）。
   - **None**（無）—若此虛擬路由器不是 RP，則選取此項。

3. **Add**（新增）遠端會合點，然後輸入該遠端（外部）RP 的 **IP Address**（**IP** 位址）。
4. **Add**（新增）指定的遠端 RP 位址作為 RP 的多點傳送 **Group Addresses**（群組位址）。
5. 選取 **Override learned RP for the same group**（覆寫相同群組的已知 **RP**），使靜態設定的外部 RP 用作 RP，而不是群組位址清單中的群組動態獲知（選擇）的 RP。
6. 按一下 **OK**（確定）。

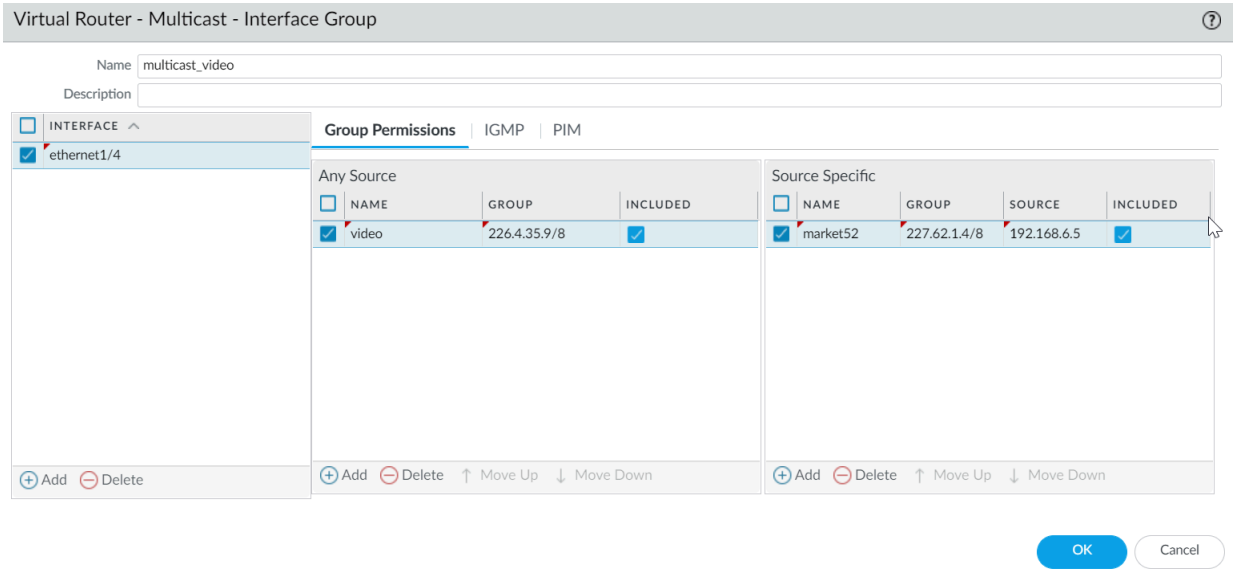
STEP 3 | 指定一組共用多點傳播組態的介面（IGMP、PIM 和群組權限）。

1. 在 **Interfaces**（介面）頁籤上，為介面群組 **Add**（新增）**Name**（名稱）。
2. 輸入 **Description**（描述）。
3. **Add**（新增）**Interface**（介面），然後選取一個或多個屬於該介面群組的 Layer 3 介面。

STEP 4 | （選用）為介面群組設定多點傳送群組權限。依預設，介面群組接受來自所有群組的 IGMP 成員資格報告和 PIM 加入訊息。

1. 選取 **Group Permissions**（群組權限）。
2. 若要為此介面群組設定任意來源多點傳送 (ASM) 群組，則在 Any Source（任意來源）視窗中，**Add**（新增）**Name**（名稱）以識別接受來自任意來源之 IGMP 成員資格報告和 PIM 加入訊息的多點傳送群組。
3. 輸入多點傳送 **Group**（群組）位址或群組位址和/或首碼，便可從這些介面上的任意來源接收多點傳送封包。
4. 選取 **Included**（包含）便可將 ASM **Group**（群組）位址納入介面群組中（預設）。取消選取 **Included**（包含）便可輕鬆地從介面群組中排除 ASM 群組，例如在測試期間。
5. **Add**（新增）要從任意來源接收多點傳送封包的其他多點傳送 **Groups**（群組）（對於介面群組）。
6. 若要在此介面群組中設定特定來源多點傳送 (SSM) 群組，則在 Source Specific（特定來源）視窗中，**Add**（新增）**Name**（名稱）以識別多點傳送群組以及來源位址配對。請勿使用您用於任意來源多點傳送的名稱。（您必須使用 IGMPv3 來設定 SSM。）
7. 輸入想要從指定的「僅限來源」接收多點傳送封包（並且可以在這些介面上接收封包）之群組的多點傳送 **Group**（群組）位址或群組位址和#或首碼。

   您為其指定權限的特定來源群組是虛擬路由器必須視為特定於來源的群組。設定 ***Source Specific Address Space***（特定來源位址空間）（步驟 9），其中包括您為其設定權限的特定於來源的群組。
8. 輸入此多點傳送群組可從中接收多點傳送封包的 **Source**（來源）IP 位址。
9. 選取 **Included**（包含）便可將 SSM 群組以及來源位址配對納入介面群組中（預設）。取消選取 **Included**（包含）便可輕鬆地從介面群組中排除該配對，例如在測試期間。
10. **Add**（新增）僅從特定來源接收多點傳送封包的其他多點傳送 **Groups**（群組）（對於介面群組）。



STEP 5 | 若面向多點傳送接收端的介面必須使用 IGMP 才能加入群組，則為介面群組設定 IGMP。

1. 在 **IGMP** 頁籤上，**Enable**（啟用）IGMP（預設值）。
2. 為介面群組中的各個介面指定 IGMP 參數：
   - **IGMP Version**（**IGMP** 版本）—**1**、**2** 或 **3**（預設值）。
   - **Enforce Router-Alert IP Option**（強制執行路由器警示 **IP** 選項） （預設為停用） - 如果要求使用 IGMPv2 或 IGMPv3 的傳入 IGMP 封包具有 IP 路由器警示選項 RFC 2113，請選取此選項。
   - **Robustness**（加強性）—一種變數，防火牆可用來調整群組成員資格間隔、其他查詢程式顯示間隔、啟動查詢計數及最後一個成員查詢計數（範圍為 1 至 7；預設值為 2）。若此防火牆所在的子網路容易丟失封包，請增加該值。
   - **Max Sources**（來源數上限）—IGMP 可以同時處理介面的最大來源數（範圍為 1 至 65,535；預設值為 **unlimited**（無限制））。
   - **Max Groups**（群組數上限）—IGMP 可以同時處理介面的最大群組數（範圍為 1 至 65,535；預設值為 **unlimited**（無限制））。
   - **Query Interval**（查詢間隔）—為確定接收端是否仍希望接收群組的多點傳送封包，虛擬路由器兩次向接收端傳送 IGMP 成員資格查詢訊息之間的秒數（範圍為 1 至 31,744；預設值為 125）。
   - **Max Query Response Time (sec)**（查詢回應時間上限（秒））—在虛擬路由器確定接收端不再想要接收該群組的多點傳送封包之前，允許接收端回應 IGMP 成員資格查詢訊息的最大秒數（範圍為 0 至 3,174.4，預設值為 10）。
   - **Last Member Query Interval (sec)**（最後一個成員查詢間隔（秒））—接收端在傳送離開群組訊息後，允許接收端回應虛擬路由器傳送之特定於群組的查詢的秒數（範圍為 0.1 至 3,174.4；預設值為 1）。
   - **Immediate Leave**（立即離開） （預設為停用）—若多點傳送群組中只有一個成員，且虛擬路由器收到該群組的 IGMP 離開訊息，設定 Immediate Leave（立即離開）導致虛擬路由器立即從多點傳送路由資訊庫 (mRIB) 和多點傳送轉送資訊庫 (mFIB) 移除該群組以及傳出介面，而不是等待最後一個成員查詢間隔到期。Immediate Leave（立即離開）設定可節省網路資源。在介面群組使用 IGMPv1 時，您無法選取 Immediate Leave（立即離開）。

STEP 6 | 為介面群組設定 PIM 稀疏模式 (PIM-SM)。

1. 在 **PIM** 頁籤上，**Enable**（啟用）PIM（預設為已啟用）。
2. 為介面群組指定 PIM 參數：
   - **Assert Interval**（判斷提示間隔）—虛擬路由器在其選擇 PIM 轉送程式時，兩次向多重存取網路上的其他 PIM 路由器傳送 PIM 判斷提示訊息之間的秒數（範圍為 0 至 65,534；預設值為 177）。
   - **Hello Interval**（**Hello** 間隔）—虛擬路由器兩次從介面群組內的每個介面中傳送 PIM Hello 訊息到其 PIM 芳鄰之間的秒數（範圍為 0 至 18,000；預設值為 30）。
   - **Join Prune Interval**（加入刪改間隔）—虛擬路由器兩次向多點傳送來源上游傳送 PIM 加入訊息（以及 PIM 刪改訊息）之間的秒數（範圍為 0 至 18,000；預設值為 60）。
   - **DR Priority**（**DR** 優先順序）—指定路由器 (DR) 優先順序，用於控制多重存取網路上的哪個路由器將 PIM 加入和刪改訊息轉送至 RP（範圍為 0 至 429,467,295；預設值為 1）。DR 優先順序優先於 IP 位址比較來選擇 DR。
   - **BSR Border**（**BSR** 邊界）—如果介面群組中的介面所在的虛擬路由器為位於企業 LAN 邊界的 BSR，請選取此選項。這將防止 RP 候選資格 BSR 訊息離開 LAN。
3. 透過指定虛擬路由器接受多點傳送封包之每個路由器的 **IP Address**（**IP** 位址），**Add**（新增）一個或多個 **Permitted PIM Neighbors**（許可的 **PIM** 芳鄰）。

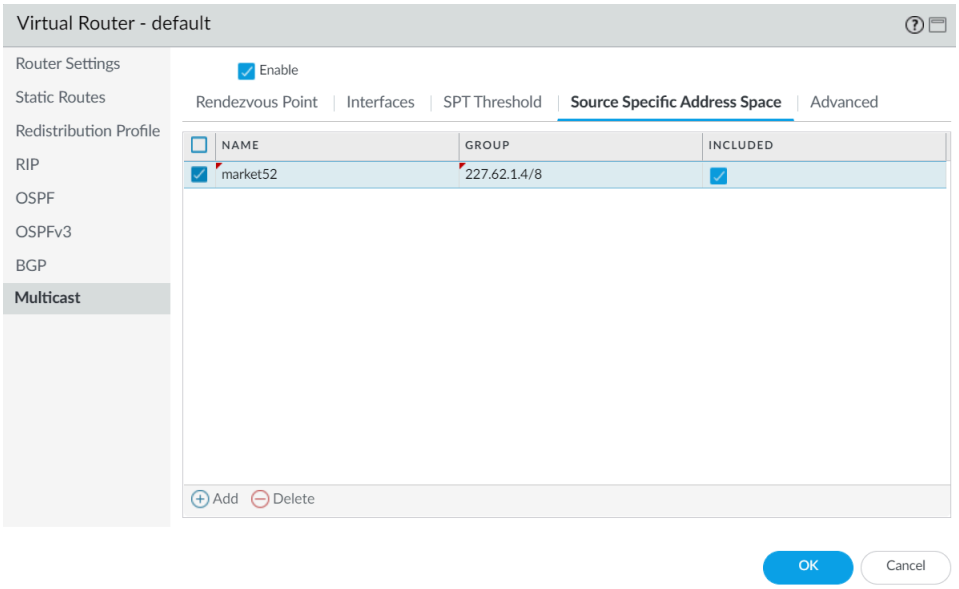
STEP 7 | 按一下 **OK**（確定）以儲存介面群組設定。

STEP 8 | （選用）變更最短路徑樹狀目錄 (SPT) 臨界值，如最短路徑樹狀目錄 (SPT) 與共用樹狀目錄中所述。

1. 選取 **SPT Threshold**（**SPT** 臨界值）並 **Add**（新增）一個 **Multicast Group/Prefix**（多點傳送群組**#**首碼），即要為其指定分佈樹狀目錄的多點傳送群組或首碼。
2. 指定 **Threshold (kb)**（臨界值 **(kb)**）—路由至指定多點傳送群組或首碼的點將從共用樹狀目錄（源自 Rp）切換到 SPT 分佈：
   - **0 (switch on first data packet)**（**0**（第一個資料封包時切換））（預設）—當虛擬路由器接收到群組或首碼的第一個資料封包時，虛擬路由器從共用樹狀目錄切換到該群組或首碼的 SPT。
   - **never (do not switch to spt)**（永不（不切換到 **SPT**））—虛擬路由器會繼續使用共用樹狀目錄，以將封包轉送至群組或首碼。
   - 輸入可以在任何介面和任何時間段內到達多點傳送群組或首碼的多點傳送封包的總千位元數，在此期間，虛擬路由器將變更為該多點傳送群組或首碼的 SPT 分佈。

STEP 9 | 識別多點傳送群組或群組及首碼，可接受僅來自特定來源的多點傳送封包。

1. 選取 **Source Specific Address Space**（特定來源位址空間），並為該空間 **Add**（新增）**Name**（名稱）。
2. 輸入帶有首碼長度的多點傳送 **Group**（群組）位址，確定用於從特定來源接收多點傳送封包的位址空間。如果虛擬路由器接收到 SSM 群組的多點傳送封包，但該群組未包含在 **Source Specific Address Space**（特定來源位址空間）內，則虛擬路由器會捨棄該封包。
3. 選取 **Included**（包含）以包含特定於來源的位址空間作為多點傳送群組位址範圍，虛擬路由器將從該範圍內接受源自允許的特定來源的多點傳送封包。取消選取 **Included**（包含）便可輕鬆地排除群組位址空間以進行測試。
4. 新增其他特定於來源的位址空間以包括您為其指定 SSM 群組權限的所有群組。



STEP 10 | （選用）工作階段在多點傳送群組和來源之間結束後，變更多點傳送路由在 mRIB 中保留的時長。

1. 選取 **Advanced**（進階）頁籤。
2. 指定 **Multicast Route Age Out Time (sec)**（多點傳送路由過時時間 （秒））（範圍為 210 至 7,200；預設值為 210）。

STEP 11 | 按一下 **OK**（確定）儲存多點傳送組態。

STEP 12 | 建立安全性原則規則，以允許多點傳送流量到達目的地區域。

1. 建立安全性原則規則，並在 **Destination**（目的地）頁籤上，為 **Destination Zone**（目的地區域）選取 **multicast**（多點傳送）或 **any**（任何）。**multicast**（多點傳送）區域為預先定義的 Layer 3 區域，符合所有多點傳送流量。**Destination Address**（目的地位址）可為多點傳送群組位址。
2. 設定剩餘的安全性原則規則。

STEP 13 | （選用）在設定路由之前，先啟用多點傳送封包的緩衝。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 啟用 **Multicast Route Setup Buffering**（多點傳送路由設定緩衝）（預設為已停用）。如果多點傳送轉送表 (mFIB) 中尚不存在相應多點傳送群組的項目，則防火牆可以保留多點傳送流量中的第一個封包。**Buffer Size**（緩衝區大小）控制防火牆根據流量緩衝的封包數量。路由安裝在 mFIB 中後，防火牆會自動將緩衝的第一個封包轉送給接收端。（僅在內容伺服器直接連線至防火牆，且多點傳送應用程式無法經受流量中的第一個封包被丟棄時，才需要啟用多點傳送路由設定緩衝。）
3. （選用）變更 **Buffer Size**（緩衝區大小）。緩衝區大小是指設定 mFIB 項目之前，防火牆可以緩衝的每個多點傳送流量的封包數（範圍為 1 到 2,000；預設值為 1,000）。防火牆總共可緩衝最多 5,000 個封包（對於所有流量）。
4. 按一下 **OK**（確定）。

STEP 14 | **Commit**（提交）您的變更。

STEP 15 | 檢視 IP 多點傳送資訊以檢視 mRIB 與 mFIB 項目、IGMP 介面設定、IGMP 群組成員資格、PIM ASM 與 SSM 模式、至 RP 的群組對應、DR 位址、PIM 設定、PIM 芳鄰等等。

STEP 16 | 若為多點傳送流量設定靜態路由，則只能在多點傳送路由表（而不是單點傳送路由表）中安裝路由，以便該路由僅用於多點傳送流量。

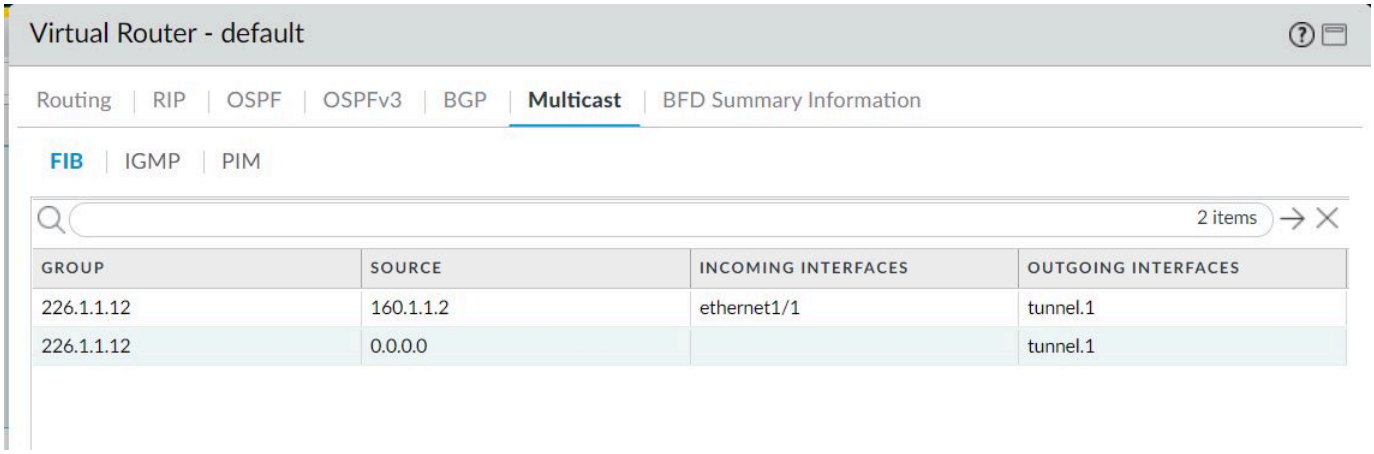
STEP 17 | 若啟用 IP 多點傳送，除非您擁有不同於邏輯單點傳送拓樸的邏輯多點傳送拓樸，否則不必使用 MP-BGP 為 IPv4 多點傳送設定 BGP。僅在您希望在多點傳送後續位址系列下向 BGP 宣告多點傳送來源首碼時，才能使用 Ipv4 位址系列和多點傳送後續位址系列設定 MP-BGP 延伸。

檢視 IP 多點傳送資訊

在您設定 IP 多點傳送路由之後，檢視多點傳送路由、轉送項目以及 IGMP 與 PIM 介面的相關資訊。

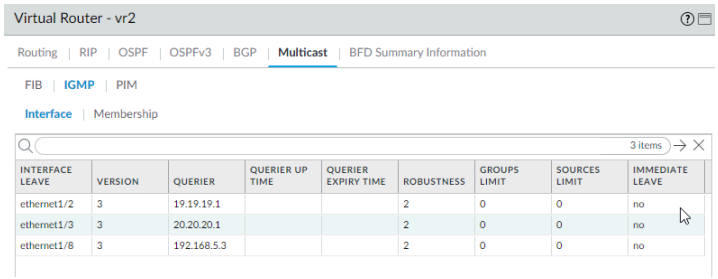
選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），並在您設定的虛擬路由器列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。

1. 選取 **Routing**（路由） > **Route Table**（路由表），然後選取 **Multicast**（多點傳送）圓鈕，以僅顯示多點傳送路由（目的地 IP 多點傳送群組、指向該群組的下一躍點以及傳出介面）。此資訊來源於 mRIB。
2. 選取 **Multicast**（多點傳送） > **FIB** 以檢視來自 mFIB 的多點傳送路由資訊：虛擬路由器所屬的多點傳送群組、相應來源、傳入介面以及送往接收端的傳出介面。

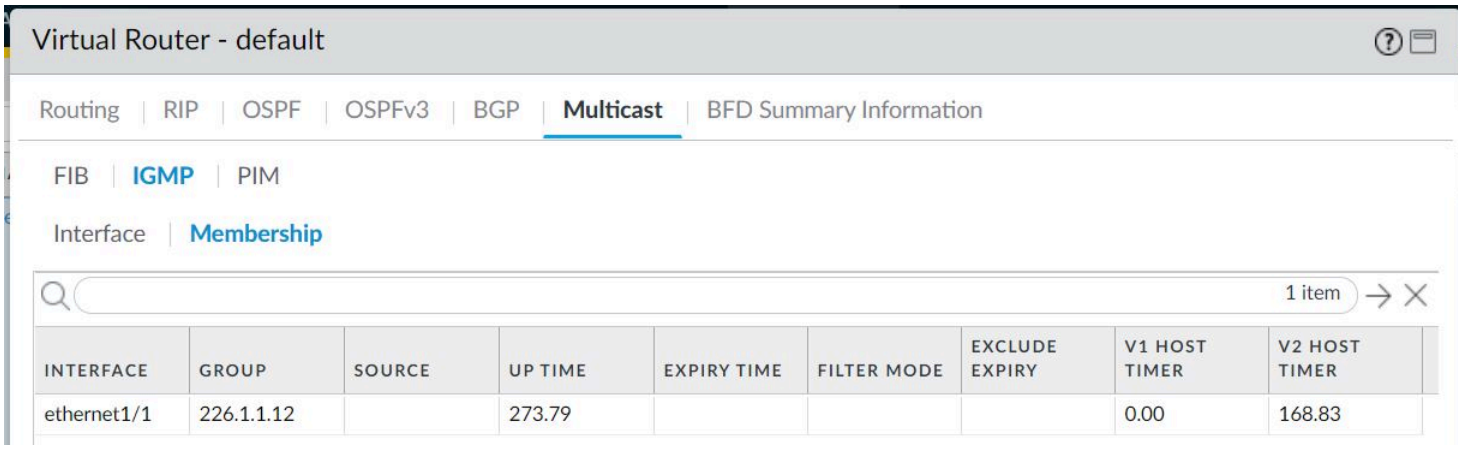


3. 選取 **Multicast**（多點傳送） > **IGMP** > **Interface**（介面） 以檢視啟用 IGMP 的介面、相關聯的 IGMP 版本、IGMP 查詢程式的 IP 位址、查詢程式啟動時間與到期時間、強壯性

設定、多點傳送群組與來源的數量限制，以及介面是否設定為 Immediate leave （立即離開）。

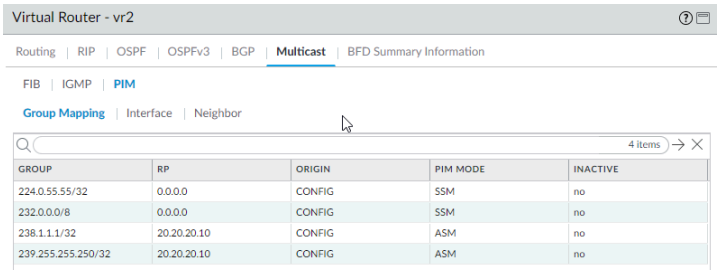


4. 選取 **Multicast**（多點傳送） > **IGMP** > **Membership**（成員資格） 以查看啟用 IGMP 的介面及其所屬的多點傳送群組、來源以及其他 IGMP 資訊。

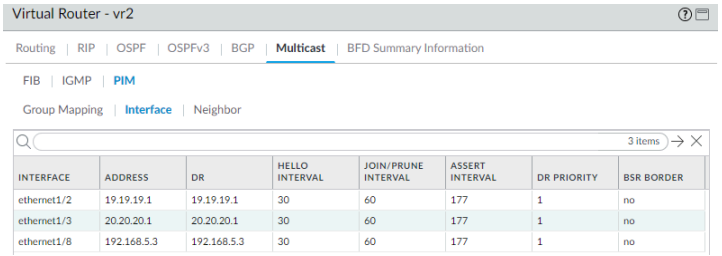


5. 選取 **Multicast**（多點傳送） > **PIM** > **Group Mapping**（群組對應）以檢視對應至 RP 的多點傳送群組、RP 對應的來源、群組的 PIM 模式（ASM 或 SSM）以及群組是否處於非

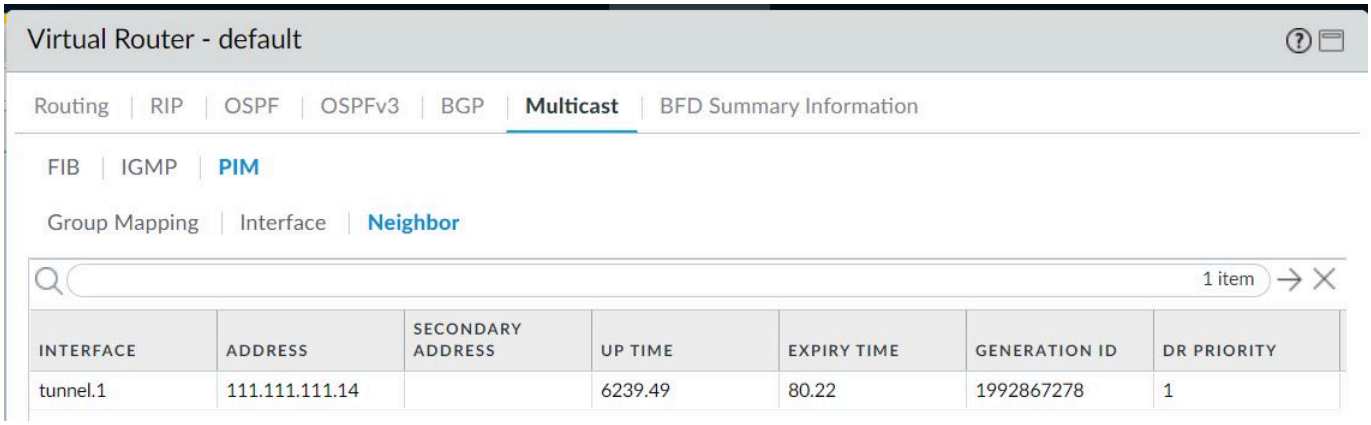
使用中狀態。SSM 模式下的群組不使用 RP，因此顯示的 RP 位址為 0.0.0.0。預設 SSM 群組為 232.0.0.0/8。



6. 選取 **Multicast**（多點傳送） > **PIM** > **Interface**（介面）以檢視介面上 DR 的 IP 位址；DR 優先順序；Hello、加入/刪改以及判斷提示的間隔；以及介面是否為啟動程序路由器 (BSR)。



7. 選取 **Multicast**（多點傳送） > **PIM** > **Neighbor**（芳鄰）以檢視有關作為虛擬路由器的 PIM 芳鄰之路由器的資訊。



路由重新散佈

瞭解並設定路由重新散佈，以提高網路流量的可存取性。

路由重新散佈概觀

在防火牆上重新散佈路由是指向另一個路由通訊協定提供防火牆從某個路由通訊協定學到之路由的過程，能夠提高網路流量的可存取性。學得之路由的過程，能夠提高網路流量的可存取性。透過路由重新散佈，路由器或虛擬路由器可以僅向執行相同路由通訊協定的其他路由宣告或共用路由。您可以將 Ipv4 或 IPv6 BGP、直連或靜態路由重新散佈到 OSPF RIB，將 OSPFv3、直連或靜態路由重新散佈到 BGP RIB。

這意味著，您可以使之前僅透過在特定路由器上手動設定靜態路由的特定網路，對 BGP 自發系統或 OSPF 區域可用。您還可以向 BGP 自發系統或 OSPF 區域宣告本機直連路由，例如私人實驗室網路的路由。

您可能希望授予內部 OSPFv3 網路上的使用者存取 BGP 的權限，以便他們能夠存取網際網路上的裝置。在這種情況下，您要將 BGP 路由重新散佈至 OSPFv3 RIB。

相反地，您可能希望授予外部使用者存取內部網路某些部分的權限，因此您要透過將 OSPFv3 路由重新散佈至 BGP RIB，使內部 OSPFv3 網路透過 BGP 可用。

要 設定路由重新散佈，首先建立重新散佈設定檔。

設定路由重新散佈

執行以下程序來設定路由重新散佈。

STEP 1 | 建立重新散佈設定檔。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。
2. 選取 **Redistribution Profile**（重新散佈設定檔）和 **Ipv4** 或 **IPv6**，然後 **Add**（新增）設定檔。
3. 輸入設定檔的 **Name**（名稱），必須以英數字元開頭，且可包含零或多個底線 (_)、連字號 (-)、點 (.) 或空格（最多 16 個字元）。
4. 為 1 至 255 範圍內的設定檔輸入 **Priority**（優先順序）。防火牆將按順序比對路由和設定檔，從優先順序只最高（優先順序值最低）的設定檔開始。優先順序值高的規則將優先於優先順序值低的規則。
5. 對於 **Redistribute**（重新散佈），選取以下任何項：
   - 可轉散發套件—為與此篩選條件相符的重新散佈路由選取此選項。
   - 無可轉散發套件—為與重新散佈設定檔相符但與此篩選條件不相符的重新散佈路由選取此選項。此選項會將設定檔當作封鎖清單（用於指定不要選取進行重新散佈的路由）處理。例如，如果您有多個用於 BGP 的重新散佈設定檔，則您可以建立 **No Redist**（無可轉散發套件）設定檔，以排除一些首碼，然後建立一個優先順序值較低（較高）的一般重新散佈設定檔。這兩個設定檔將會結合，而優先順序值較高的設定檔將優先。您不能僅有 **No Redist**（無可轉散發套件）設定檔，必須至少有一個 **Redist**（可轉散發套件）設定檔才能重新散佈路由。
6. 在 **General Filter**（一般篩選器） 頁籤，為 Source Type（來源類型）選取一個或多個要重新散佈的路由類型：
   - **bgp**—重新散佈與設定檔相符的 BGP 路由。
   - 直連—重新散佈與設定檔相符的直連路由。
   - **ospf**（僅限 IPv4 ）—重新散佈與設定檔相符的 OSPF 路由。
   - **rip**（僅限 IPv4 ）—重新散佈與設定檔相符的 RIP 路由。
   - **ospfv3**（僅限 IPv6 ）—重新散佈與設定檔相符的 OSPFv3 路由。
   - 靜態—重新散佈與設定檔相符的靜態路由。
7. （選用）對於 **Interface**（介面），**Add**（新增）一個或多個與要比對之路由關聯的輸出介面，以進行重新散佈。若要移除項目，可按一下 **Delete**（刪除）。
8. （選用）對於 **Destination**（目的地），**Add**（新增）要比對之路由的一個或多個 Ipv4 或 IPv6 目的地，以進行重新散佈。若要移除項目，可按一下 **Delete**（刪除）。
9. （選用）對於 **Next Hop**（下一個躍點），**Add**（新增）要比對之路由的一個或多個下一個躍點 IPv4 或 IPv6 目的地，以進行重新散佈。若要移除項目，可按一下 **Delete**（刪除）。
10. 按一下 **OK**（確定）。

STEP 2 | （選用一當一般篩選器包括 ospf 或 ospfv3 時）建立 OSPF 篩選器，以進一步指定要重新散佈的 OSPF 或 OSPFv3 路由。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取虛擬路由器。
2. 選取 **Redistribution Profile**（重新散佈設定檔）和 **Ipv4** 或 **IPv6**，然後選取您建立的設定檔。
3. 選取 **OSPF Filter**（**OSPF** 篩選器）。
4. 對於 Path Type（路徑類型），選取下列一個或多個要重新散佈的 OSPF 路徑類型：**ext-1**（外部 **1**）、**ext-2**（外部 **2**）、**inter-area**（區域間） 或 **intra-area**（區域內）。
5. 若要指定從哪個 **Area**（區域）重新散佈 OSPF 或 OSPFv3 路由，則以 IP 位址格式 **Add**（新增）區域。
6. 若要指定 **Tag**（標籤），則以 IP 位址格式 **Add**（新增）標籤。
7. 按一下 **OK**（確定）。

STEP 3 | （選用一當一般篩選器包括 bgp 時）建立 BGP 篩選器，以進一步指定要重新散佈的 BGP 路由。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取虛擬路由器。
2. 選取 **Redistribution Profile**（重新散佈設定檔）和 **Ipv4** 或 **IPv6**，然後選取您建立的設定檔。
3. 選取 **BGP Filter**（**BGP** 篩選器）。
4. 對於 **Community**（社群），按一下 **Add**（新增）以從社群清單中選取，例如公認社群：**local-as**、**no-advertise**、**no-export** 或 **nopeer**。您還可以輸入十進位或十六進位或者 AS:VAL 格式的 32 位元值；其中 AS 和 VAL 都在 0 至 65,535 的範圍內。最多可輸入 10 個項目。
5. 對於 **Extended Community**（擴充社群），**Add**（新增）一個社群，作為十六進位或是 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。最多可輸入 5 個項目。
6. 按一下 **OK**（確定）。

STEP 4 | 選取要重新散佈路由的通訊協定，然後為這些通訊協定設定屬性。

此工作介紹了重新散佈路由到 BGP。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取虛擬路由器。
2. 選取 **BGP** > **Redist Rules**（可轉散發規則）。
3. 選取 **Allow Redistribute Default Route**（允許重新散佈預設路由），以允許防火牆重新散佈預設路由。
4. 按一下 **Add**（新增）。
5. 選取 **Address Family Type**（位址家族類型）：**IPv4** 或 **IPv6**，以指定重新散佈的路由將放入哪個路由表。
6. 為您建立的重新散佈設定檔（其中選取了要重新散佈的路由）選取 **Name**（名稱）。
7. **Enable**（啟用）重新散佈規則。
8. （選用）輸入以下任意值，防火牆將對重新散佈的路由套用這些值：
   - **Metric**（度量），範圍為 1 至 65,535。
   - **Set Origin**（設定來源）—路由的來源：**igp**、**egp** 或 **incomplete**。
   - **Set MED**（設定 **MED**）—MED 值，範圍為 0 至 4,294,967,295。
   - **Set Local Preference**（設定本機喜好設定）—本機喜好設定值，範圍為 0 至 4,294,967,295。
   - **Set AS Path Limit**（設定 **AS** 路徑限制）—AS_PATH 中自發系統的最大數目，範圍為 1 至 255。
   - **Set Community**（設定社群）—選取或輸入十進位或十六進位的 32 位元值，或輸入 AS:VAL 格式的值；其中 AS 和 VAL 都在 0 至 65,525 的範圍內。最多可輸入 10 個項目。
   - **Set Extended Community**（設定擴充社群）—選取或輸入一個社群，作為十六進位或是 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。最多可輸入 5 個項目。
9. 按一下 **OK**（確定）。

STEP 5 | **Commit**（提交）您的變更。

GRE 通道

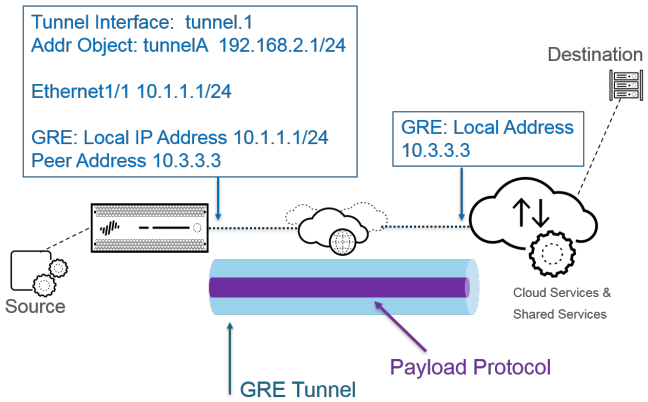
一般路由封裝 (GRE) 通道通訊協定是封裝有效負載通訊協定的裝置電信業者通訊協定。GRE 封包本身封裝在傳輸通訊協定（IPv4 或 IPv6）中。

GRE 通道概要

Generic Routing Encapsulation (GRE) 通道在點對點邏輯連結中連接兩個端點（防火牆和其他設備）。防火牆可以終止 GRE 通道；您可將封包路由或轉送至 GRE 通道。GRE 通道易於使用，通常是進行點對點連線（特別是與雲端中服務或合作夥伴網路連線）的理想通道通訊協定。

當您要將傳送至某個 IP 位址的封包導向至雲端代理程式或合作夥伴網路以採取特定的點對點路徑時，可建立 GRE 通道。封包透過 GRE 通道（在網際網路等傳輸網路上）傳送至雲端服務，同時傳送至目的地位址。這使雲端服務可以在封包上強制執行其服務或原則。

下圖顯示了連線網際網路中的防火牆和雲端服務的 GRE 通道範例。



為達更佳效能並避免單點故障，可透過多個 ***GRE*** 通道（而不是使用單一通道）將多個連線分割至防火牆。每個 ***GRE*** 通道都需要通道介面。

當防火牆允許封包通過（根據原則比對）且封包輸出至 GRE 通道介面時，防火牆將新增 GRE 封裝；其不會產生工作階段。防火牆不會對 GRE 封裝流量執行安全性原則規則查閱；所以您不需要防火牆所封裝 GRE 流量的安全性原則規則。但是，當防火牆收到 GRE 流量時，會產生工作階段，並將所有原則套用至除封裝流量之外的 GRE IP 標頭。防火牆會像處理其他封包一樣處理收到的 GRE 封包。因此：

- 如果防火牆接收 GRE 封包的介面具有與該 GRE 通道（例如，tunnel.1）所關聯之通道介面相同的區域，則來源區域與目的地區域相同。依預設，流量在區域內允許（區域內流量），因此輸入 GRE 流量依預設允許。
- 但是，如果您設定了自己的區域內安全性原則規則以拒絕流量，則必須明確允許 GRE 流量。
- 同樣地，如果 GRE 通道（例如，tunnel.1）所關聯之通道介面的區域與輸入介面的通道不同，則必須設定安全性原則規則才能允許 GRE 流量。

由於防火牆會將通道封包封裝在 GRE 封包中，因此 GRE 標頭的額外 24 位元組將自動以最大傳輸單元 (MTU) 產生較小的 最大區段大小 (MSS)。如果不變更介面的 IPv4 MSS 調整大小，依預設，防火牆會將 MTU 減少 64 位元組（40 位元組 IP 標頭 + 24 位元組 GRE 標頭）。這表示，如果預設 MTU 為 1,500 位元組，MSS 將為 1,436 位元組 (1,500 - 40 - 24 = 1,436)。如果將 MSS 調整大小設為 300 位元組，MSS 將僅為 1,176 位元級 (1,500 - 300 - 24 = 1,176)。

防火牆不支援路由將 GRE 或 IPSec 通道路由到 GRE 通道，但是您可以將 GRE 通道路由到 IPSec 通道。此外：

- GRE 通道不支援 QoS。
- 防火牆不支援單一介面同時作為 GRE 通道端點和解密代理程式。
- GRE 通道不支援在 GRE 通道端點之間設定 NAT。

如果您需要連線到其他廠商的網路，我們建議您設定 IPSec 通道，而不是 *GRE* 通道；僅當此為廠商支援的唯一點對點通道機制時，才應使用 *GRE* 通道。如果遠端端點要求啟用 *GRE over IPSec*，可透過（***Add GRE Encapsulation***（新增 ***GRE*** 封裝））啟用。如果遠端端點要求在 *IPSec* 加密流量前將流量封裝到 *GRE* 通道，則新增 *GRE* 封裝。例如，某些實作要求在 *IPSec* 加密多點傳送流量前對其進行封裝。如果這是環境的要求，且 *GRE* 通道與 *IPSec* 通道共用同一 *IP* 位址，在設定 *IPSec* 通道時，須 ***Add GRE Encapsulation***（新增 ***GRE*** 封裝）。

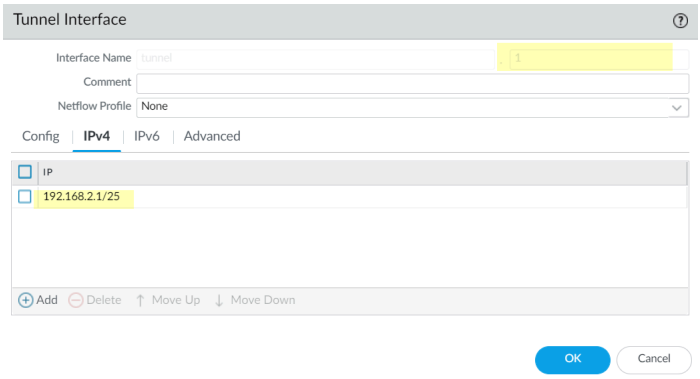
如果您不打算在防火牆上終止 *GRE* 通道，但希望能夠在 *GRE* 通道內檢查和控制通過防火牆的流量，請勿建立 *GRE* 通道。而是對 *GRE* 流量執行通道內容檢查。使用通道內容檢查，您可以檢查通過防火牆的 *GRE* 流量並對其執行原則，但無法建立點對點邏輯連結以達到引導流量的目的。

建立 GRE 通道

建立 Generic Routing Encapsulation (GRE) 通道以在點對點邏輯連結中連接兩個端點。

STEP 1 | 建立通道介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道）。
2. **Add**（新增）通道並輸入 **Interface Name**（介面名稱），後接一個句點和數字（範圍為 1 至 9,999）。例如，**`tunnel.1`**。
3. 在 **Config**（設定）頁籤上，將通道介面指派給 **Virtual Router**（虛擬路由器）。
4. 如果防火牆支援多個虛擬系統，則將通道介面指派給 **Virtual System**（虛擬系統）。
5. 將通道介面指派給 **Security Zone**（安全性區域）。



6. 為通道介面指派 IP 位址。（如果要路由至此通道或監控通道端點，則必須指派 IP 位址。） 選取 **IPv4** 或 **IPv6** 或設定兩者。

   此位址和對等體通道介面之對應位址應在同一子網路，因為它是點對點邏輯連結。

   - （僅 IPv4）在 **IPv4** 頁籤上，**Add**（新增） IPv4 位址或選取位址物件或按一下 **New Address**（新位址），然後指派位址 **Type**（類型）並輸入位址。例如，輸入**`192.168.2.1`**。
   - （僅 IPv6）在 **IPv6** 頁籤上，選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。
     1. 對於 **Interface ID**（介面 **ID**），選取 **EUI-64 (default 64-bit Extended Unique Identifier)**（**EUI-64**（預設 **64** 位元延伸唯一識別碼））。
     2. **Add**（新增）新的 **Address**（位址），選取 IPv6 位址物件，或按一下 **New Address**（新位址），然後指派位址 **Name**（名稱）。**Enable address on interface**（在介面上啟用 **IPv6**），然後按一下 **OK**（確定）。
     3. 選取位址 **Type**（類型）並輸入 IPv6 位址或 FQDN，然後按一下**OK**（確定）保存新位址。
     4. 選取**Enable address on interface**（在介面上啟用 **IPv6**），然後按一下 **OK**（確定）。
7. 按一下 **OK**（確定）。

STEP 2 | 建立 GRE 通道，強制封包穿過特定的點對點路徑。

1. 選取 **Network**（網路） > **GRE Tunnels**（**GRE** 通道），然後按 **Name**（名稱）**Add**（新增） 通道。
2. 選取要用作本機 GRE 通道端點的**Interface**（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。
3. 將 **Local Address**（本機位址）選為 **IP**，並選取您剛才所選取介面之 IP 位址。
4. 輸入 **Peer Address**（對等位址），這是 GRE 通道另一端的 IP 位址。
5. 選取在步驟 1 中建立的 **Tunnel Interface**（通道介面）。（此介面會在通道為路由的輸出 **Interface**（介面）時對其進行識別。）
6. 輸入封裝在 GRE 封包內之 IP 封包的 **TTL**（範圍為 1 到 255；預設值為 64）。
7. 選取 **Copy ToS Header**（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。如果您的網路使用 QoS 並依賴於 ToS 位元執行 QoS 原則，則選取此選項。

STEP 3 | （最佳做法）對 GRE 通道啟用保持運作功能。

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。

1. 選取 **Keep Alive**（保持運作）以對 GRE 通道啟用保持運作功能（預設為停用）。
2. （選用）設定 GRE 通道本端傳送 keepalive 封包給通道對等之間的 **Interval (sec)**（時間間隔（秒））。乘以 **Hold Timer**（保留計時器）時，這也是 GRE 通道恢復之前，防火牆必須成功傳送 keepalive 封包的時間長度（範圍為 1 至 50；預設值為 10）。設定的時間間隔太小會導致環境中出現許多不必要的 keepalive 封包，並需要額外的頻寬和處理。設定的時間間隔太大會使容錯轉移延遲，因為可能無法立即識別錯誤狀況。
3. （選用）輸入 **Retry**（重試）設定，即防火牆認為通道對等體關閉之前，未返回 keepalive 封包的時間間隔數（範圍為 1 至 255；預設值為 3）。當通道關閉時，防火牆會從轉送表中移除與通道相關聯的路由。設定重試設定有助於避免對沒有真正關閉的通道採取措施。
4. （選用）設定 **Hold Timer**（保留計時器），即在防火牆重新建立與通道對等體的通訊之前，已成功傳送 keepalive 封包的 **Intervals**（時間間隔）數（範圍為 1 至 64；預設值為 5）。

STEP 4 | 按一下 **OK**（確定）。

STEP 5 | 設定路由通訊協定或靜態路由，以透過 GRE 通道將流量路由至目的地。例如，設定靜態路由至目的地伺服器的網路，並將輸出 **Interface**（介面）指定為本機通道端點(tunnel.1)。將下一個躍點設為另一端通道的 IP 位址。例如，192.168.2.3。

STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 為通道另一端設定公開 IP 位址、本機和對等體 IP 位址（分別對應防火牆上 GRE 通道的對等體和本機 IP 位址）及路由通訊協定或靜態路由。

STEP 8 | 確認防火牆可以透過 GRE 通道與通道對等體通訊。

1. 存取 CLI。
2. > **ping source 192.168.2.1 host 192.168.2.3**

DHCP

本節說明動態主機設定通訊協定 (DHCP)，以及在 Palo Alto Networks® 防火牆上設定介面作為 DHCP 伺服器、用戶端或轉送代理程式所需的工作。防火牆透過將這些角色指派給不同的介面，而能執行多個角色。

DHCP 概要

DHCP 是在 RFC 2131、 動態主機設定通訊協定中定義的標準通訊協定。DHCP 有兩個主要用途：一是提供 TCP/IP 與連結層設定參數，二是提供網路位址以便在 TCP/IP 網路上動態設定主機。

DHCP 使用通訊的用戶端-伺服器模型。此模型包含三個裝置可履行的角色：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) 的裝置可向 DHCP 伺服器要求 IP 位址與其他設定。用戶端裝置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資源，也不必知道他們從 DHCP 伺服器繼承的選項。
- 作為 DHCP 伺服器的裝置可服務用戶端。透過使用三個 DHCP 定址 機制中的任何一個，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 定址與許多的 DHCP 選項提供給許多用戶端。
- 作為 DHCP 轉送代理程式的裝置會在 DHCP 用戶端與伺服器之間傳輸 DHCP 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)。DHCP 訊息 伺服器傳送到用戶端的，將被傳送到連接埠 68。

Palo Alto Networks® 防火牆上的介面可執行 DHCP 伺服器、用戶端或轉送代理程式的角色。DHCP 伺服器或轉送代理程式的介面必須是 Layer 3 乙太網路、彙總的乙太網路或 Layer 3 VLAN 介面。您可使用適合於任何角色組合的設定來設定防火牆的介面。作為 DHCP 伺服器和用戶端的防火牆 中已摘要每個角色的行為。

防火牆支援 DHCPv4 Server 與 DHCPv6 Relay。

DHCP 伺服器與 DHCP 用戶端的 Palo Alto Networks 實作只支援 IPv4 位址。其 DHCP 轉送實作支援 IPv4 與 IPv6。高可用性主動/主動模式中不支援 DHCP 用戶端。

作為 DHCP 伺服器和用戶端的防火牆

防火牆可以作為 DHCP 伺服器和 DHCP 用戶端。動態主機設定通訊協定 (RFC 2131) 是針對支援 IPv4 與 IPv6 位址所設計。DHCP 伺服器的 Palo Alto Networks® 實作只支援 IPv4 位址。

防火牆 DHCP 伺服器會以下列方式運作：

- DHCP 伺服器收到來自用戶端的 DHCPDISCOVER 訊息時，伺服器會以包含所有預先定義和使用者定義選項（依選項在設定中出現的順序） 的 DHCPOFFER 訊息回覆。用戶端會選取需要的選項，並以 DHCPREQUEST 訊息回應。
- 伺服器收到來自用戶端的 DHCPREQUEST 訊息時，伺服器會以僅包含要求中所指定選項的 DHCPACK 訊息回覆。

防火牆 DHCP 用戶端會以下列方式運作：

- DHCP 用戶端收到來自伺服器的 DHCPOFFER 時，無論其在 DHCPREQUEST 中傳送哪些選項，該用戶端都會自動快取所有提供的選項以供日後使用。
- 依預設且為了節省記憶體消耗，如果用戶端收到代碼的多個值，其只會快取每個選項代碼的第一個值。
- 除非 DHCP 用戶端在其 DHCPDISCOVER 或 DHCPREQUEST 訊息的選項 57 中指定最大值，否則 DHCP 訊息沒有長度上限。

DHCP 訊息

DHCP 使用八個標準訊息類型，這些類型由 DHCP 訊息中的選項類型號碼來識別。例如，當用戶端想要尋找 DHCP 伺服器時，它會在其區域實體子網路上廣播 DHCPDISCOVER 訊息。如果其子網路上沒有 DHCP 伺服器，且 DHCP Helper 或 DHCP 轉送設定正確的話，該訊息會轉送到其他實體子網路上的 DHCP 伺服器。否則，訊息不會超過其源自之子網路的範圍。一或多個 DHCP 伺服器將會以 DHCPOFFER 訊息回應，訊息中包含可用網路位址與其他設定參數。

用戶端需要 IP 位址時，會將 DHCPREQUEST 傳送到一或多個伺服器。當然如果用戶端正在要求 IP 位址，則表示它還沒有 IP 位址，因此 RFC 2131 需要用戶端傳出的廣播訊息其 IP 標頭中的來源位址為 #。

當用戶端向伺服器要求設定參數時，可能會收到多個伺服器的回應。用戶端收到其 IP 位址後，也就是說用戶端至少有一個 IP 位址，且可能有其他設定參數與其繫結。DHCP 伺服器會管理這一類設定參數與用戶端間的繫結。

下表列出 DHCP 訊息。

DHCP 訊息	說明
DHCPDISCOVER	用來尋找可用 DHCP 伺服器的用戶端廣播。
DHCPOFFER	伺服器給用戶端 DHCPDISCOVER 的回應，並提供設定參數。
DHCPREQUEST	給一或多部伺服器的用戶端訊息，可執行下列任何一個動作： · 向一部伺服器要求參數，然後隱含拒絕其他伺服器提供的項目。 · 確認先前配置的位址是正確的，例如在系統重新開機後確認。 · 延長網路位址的租期。
DHCPACK	伺服器給用戶端的認可訊息，內含如確認的網路位址等設定參數。
DHCPNAK	伺服器給用戶端的負向認可，指出用戶端瞭解網路位址是錯誤的 (例如，如果用戶端已移至新的子網路)，或用戶端租期已到期。
DHCPDECLINE	用戶端給伺服器的訊息，指出網路位址已在使用中。
DHCPRELEASE	用戶端給伺服器的訊息，表示放棄該網路位址的使用者，並取消剩餘的租用時間。
DHCPINFORM	用戶端給伺服器的訊息，僅要求本機設定參數；用戶端有外部設定的網路位址。

DHCP 定址

DHCP 位址配置方法

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。請參閱 DHCP 租期小節。
- 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 配置為永久配置，做法是設定 DHCP 伺服器，然後選擇 **Reserved Address**（保留的位址）以對應至用戶端裝置的 **MAC Address**（**MAC** 位址）。即使用戶端登出、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裝置具有關鍵用途，即使是裝置關閉、未插電、重新開機或電力中斷等情況下，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）中的所有位址配置為 **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）指派給任何裝置。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 租期

租期的定義是 DHCP 伺服器將網路位址配置給用戶端使用的時間。租期可在後續要求時延長 (更新)。如果用戶端不再需要該位址，可在租期到之前將位址釋回給伺服器。之後伺服器就能將該位址指派給已用盡未指派位址的其他用戶端。

為 DHCP 伺服器設定的租期，會套用到單一 DHCP 伺服器 (介面) 動態指派給其用戶端的所有位址上。也就是該介面所有動態指派的位址期限皆為 **Unlimited**（無限制），或其 **Timeout**（逾時）值

相同。在防火牆上設定的不同 DHCP 伺服器，其用戶端的租期可以不同。**Reserved Address**（保留的位址）是靜態位址配置，不受租期的影響。

依照 DHCP 標準 RFC 2131，DHCP 用戶端不會等待租期到期，因為是否能得到指派給它的新位址是有風險的。相反的，當 DHCP 用戶端租期到一半時，它會嘗試延長租期，讓它能保留同一個 IP 位址。因此租期就像是滑動窗口。

一般而言，如果已將 IP 位址指派給裝置，但裝置後來離開網路，且租期未延長，DHCP 伺服器會讓租期到期。因為用戶端已離開網路，不再需要該位址，所以伺服器中的租期已到達，且租期的狀態為「已到期」。

防火牆有保留計時器，可防止立即重新指派已到期的 IP 位址。此行為會暫時為裝置保留位址，以免裝置又重新回到網路上。但如果位址集區的位址用盡了，伺服器會在保留計時器到期前就重新配置已到期的位址。當系統需要更多的位址或保留計時器釋放已到期的位址時，系統會自動清除已到期的位址。

在 CLI 中，使用 **show dhcp server lease** 操作命令可檢視有關已配置 IP 位址的相關資訊。如果您不想要等待已到期的租期自動釋出，可以使用 **clear dhcp lease interface *<interface>* expired-only** 命令清除已到期的租期，讓這些位址再次回到集區。您可以使用 **clear dhcp lease interface *<interface>* ip *<ip_address>*** 命令釋放特定 IP 位址。使用 **clear dhcp lease interface *<interface>* mac *<mac_address>***命令釋放特定 MAC 位址。

DHCP 選項

DHCP 與 DHCP 選項的歷史可回溯到啟動程序通訊協定 (BOOTP)。當時主機在開機程序期間會使用 BOOTP 動態地自我設定。主機會從伺服器收到可供下載開機程式的 IP 位址與檔案，並會收到伺服器位址與網際網路閘道的位址。

BOOTP 封包中內含廠商資訊欄位，其中包含一些已標記的欄位，這些欄位包含各種資訊，例如子網路遮罩、BOOTP 檔案大小，及許多其他的值。RFC 1497 中說明 BOOTP Vendor Information Extensions。DHCP 會取代 BOOTP；防火牆不支援 BOOTP。

這些延伸模組最後因使用 DHCP 與 DHCP 主機設定參數，也就是所謂的選項而擴展。與廠商延伸模組類似，DHCP 選項是已標記的資料項目，會將資訊提供給 DHCP 用戶端。系統會以 DHCP 訊息結尾處長度變動的欄位傳送這些選項。例如，DHCP 訊息類型為選項 53，數值 1 表示為 DHCPDISCOVER 訊息。DHCP 選項於 RFC 2132、DHCP Options and BOOTP Vendor Extensions 中定義。

DHCP 用戶端會與伺服器交涉，限制伺服器只傳送用戶端要求的選項。

- 預先定義的 DHCP 選項
- DHCP 選項的多個值
- DHCP 選項 43、55 和 60 及其他自訂選項

預先定義的 DHCP 選項

Palo Alto Networks® 防火牆在 DHCP 伺服器實作中，支援使用者定義和預先定義的 DHCP 選項。此類選項是在 DHCP 伺服器上設定的，並會傳送到將 DHCPREQUEST 傳送到伺服器的用戶端。也就是說用戶端會繼承與實作以編程方式要用戶端接受的選項。

防火牆支援下列在其 DHCP 伺服器上預先定義的選項，下列選項依照其在 **DHCP Server**（DHCP 伺服器）設定畫面上出現的順序顯示：

DHCP 選項	DHCP 選項名稱
51	租期
3	閘道
1	IP 集區子網路 (遮罩)
6	網域名稱系統 (DNS) 伺服器位址（主要與次要）
44	Windows 網際網路名稱服務 (WINS) 伺服器位址 (主要與次要)
41	網路資訊服務 (NIS) 伺服器位址 (主要與次要)
42	網路時間通訊協定 (NTP) 伺服器位址 (主要與次要)

DHCP 選項	DHCP 選項名稱
70	郵局通訊協定第 3 版 (POP3) 伺服器位址
69	簡易郵件傳送通訊協定 (SMTP) 伺服器位址
15	DNS 尾碼

如前所述，您也可以設定廠商特定和自訂選項，其支援 IP 電話和無線基礎結構裝置等各種辦公室裝置。每個選項代碼都支援多個值，其可以是 IP 位址、ASCII 或十六進位格式。透過防火牆增強 DCHP 選項支援，分公司不需要購買和管理自己的 DHCP 伺服器，即可為 DHCP 用戶端提供廠商特定和自訂選項。

DHCP 選項的多個值

您可以針對具有相同 **Option Name**（選項名稱）的 **Option Code**（選項代碼）輸入多個選項值，但特定代碼和名稱組合的所有值都必須是相同類型（IP 位址、ASCII 或十六進位）。如果繼承或輸入某個類型，且稍後針對相同代碼和名稱組合輸入不同類型，則第二個類型會覆寫第一個類型。

您可以使用不同的 **Option Name**（選項名稱）來多次輸入 **Option Code**（選項代碼）。在此狀況下，多個選項名稱之間選項代碼的 **Option Type**（選項類型）可以不同。例如，如果您以 IP 位址類型設定選項 Coastal Server（選項代碼 6），也會允許以 ASCII 類型設定選項 Server XYZ（選項代碼 6）。

防火牆會依從上到下的順序，將選項的多個值（串連在一起）傳送至用戶端。因此，針對選項輸入多個值時，請依偏好順序輸入值，或在清單中移動選項以達到您的偏好順序。防火牆組態中選項的順序會決定選項在 DHCPOFFER 和 DHCPACK 訊息中出現的順序。

您可以輸入以預先定義選項代碼的形式存在的選項代碼，且自訂選項代碼會取代預先定義的 DHCP 選項；防火牆會發出警告。

DHCP 選項 43、55 和 60 及其他自訂選項

下表說明數個 RFC 2132 中所述選項的選項行為。

選項代碼	選項名稱	選項說明/行為
43	廠商特定資訊	從伺服器傳送至用戶端。已設定 DHCP 伺服器以提供給用戶端的廠商特定資訊。只有在伺服器於其表格中具有廠商類別識別碼 (VCI)，且該識別碼符合 VCI 中用戶端的 DHCPREQUEST 時，系統才會將該資訊傳送至用戶端。 選項 43 封包可包含多個廠商特定資訊。其也可包含封裝的廠商特定資料延伸模組。

選項代碼	選項名稱	選項說明/行為
55	參數要求清單	從用戶端傳送至伺服器。DHCP 用戶端要求的設定參數（選項代碼）清單，可能依用戶端的偏好排序。伺服器會嘗試依相同順序以選項回應。
60	廠商類別識別碼 (VCI)	從用戶端傳送至伺服器。DHCP 用戶端的廠商類型和設定。DHCP 用戶端會在 DHCPREQUEST 中將選項代碼 60 傳送至 DHCP 伺服器。當伺服器收到選項 60 時，其會查看 VCI、在自己的表格中尋找相符的 VCI，然後傳回具有該值的選項 43 (對應於 VCI)，從而將廠商特定資訊轉送至正確的用戶端。用戶端和伺服器都具有 VCI 知識。

您可以傳送未在 RFC 2132 中定義的自訂廠商特定選項代碼。選項代碼的範圍可為 1-254，且可具有固定或變動長度。

DHCP 伺服器不會驗證自訂 *DHCP* 選項；您必須確保針對您建立的選項輸入正確的值。

針對 ASCII 和十六進位 DHCP 選項類型，選項值最多可以是 255 組 8 位數。

將介面設定為 DHCP 伺服器

此工作的先決條件是：

- 設定 Layer 3 乙太網路或 Layer 3 VLAN 介面。
- 將介面指派給虛擬路由器和區域。
- 決定網路計劃中 IP 位址的有效集區，您可以將這些位址指定為由 DHCP 伺服器指派給用戶端。
- 收集您要設定的 DHCP 選項、值和廠商類別識別碼。

功能如下：

- 有關 PA-5200 系列和 PA-7000 系列防火牆以外的防火牆型號，請參見產品選擇工具。
- 在 PA-5220 防火牆中，您可設定最多 500 個 DHCP 伺服器以及最多 2,048 個 DHCP 轉送代理程式（減去所設定的 DHCP 伺服器數）。例如，如果您設定 500 個 DHCP 伺服器，您可設定 1,548 個 DHCP 轉送代理程式。
- 在 PA-5250、PA-5260 與 PA-7000 系列防火牆中，您可設定最多 500 個 DHCP 伺服器以及最多 4,096 個 DHCP 轉送代理程式（減去所設定的 DHCP 伺服器數）。例如，如果您設定 500 個 DHCP 伺服器，您可設定 3,596 個 DHCP 轉送代理程式。

執行下列工作可將防火牆上的介面設定為 DHCP 伺服器。

STEP 1 | 選取要作為 DHCP 伺服器的介面。

1. 選取 **Network**（網路） > **DHCP** > **DHCP Server**（**DHCP** 伺服器），然後 **Add**（新增）**Interface**（介面） 名稱，或選取一個。
2. 針對 **Mode**（模式）選取 **enabled**（已啟用）或 **auto**（自動）模式。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。
3. （選用）如果您想讓伺服器將 IP 位址指派給其用戶端前先偵測該位址，請選取 **Ping IP when allocating new IP**（配置新 **IP** 時偵測 **IP**）。

   如果偵測收到回應，則表示其他裝置已擁有該位址，因此無法指派。伺服器會改從集區中指派下一個位址。此行為類似 Optimistic Duplicate Address Detection (DAD)forIPv6,RFC 4429。

   設定選項並返回 *DHCP* 伺服器頁籤後，介面的 ***Probe IP***（探查 ***IP***）欄會表示是否已選取 ***Ping IP when allocating new IP***（配置新 ***IP*** 時偵測 ***IP***）。

STEP 2 | 設定伺服器要傳送給其用戶端的預先定義 DHCP 選項 。

- 在 Options（選項）區段中，選取 **Lease**（租期）類型：
- 無限制會讓伺服器從 IP 配發範圍中動態選擇 **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。
- 繼承來源—保留為 **None**（無），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。

指定繼承來源可讓防火牆從 DHCP 用戶端收到的上游伺服器，快速新增 DHCP 選項。如果來源變更用戶端的選項，其也會讓該選項保持在更新狀態。例如，如果來源取代其 NTP 伺服器（系統已將其視為 **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。

繼承包含多個 *IP* 位址的 *DHCP* 選項時，防火牆只會使用選項中包含的第一個 *IP* 位址，以節約使用快取記憶體。如果您需要單一選項的多個 *IP* 位址，請在該防火牆上直接設定 *DHCP* 選項，而非設定繼承。

- 檢查繼承來源狀態—如果您已選取 **Inheritance Source**（繼承來源），則按一下此連結會開啟 **Dynamic IP Interface Status**（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—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 上的任何裝置。
- 子網路遮罩—與 **IP Pools**（**IP** 配發範圍）中的位址搭配使用的網路遮罩。

針對下列欄位，按一下向下箭頭，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至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。

- 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。
- 次要 **WINS**、次要 **NTP**—可用網路時間通訊協定伺服器的 IP 位址。
- **POP3** 伺服器—郵局通訊協定 (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。

STEP 3 | （選用）設定廠商特定或自訂 DHCP 選項，DHCP 伺服器會將該選項傳送至其用戶端。

1. 在 Custom DHCP Options（自訂 DHCP 選項）區段中，**Add**（新增）描述性 **Name**（名稱）以識別 DHCP 選項。
2. 輸入要設定伺服器提供的 **Option Code**（選項代碼）（範圍是 1-254）。（相關選項代碼，請參閱RFC 2132。）
3. 如果 **Option Code**（選項代碼）為 **43**，則會顯示 **Vendor Class Identifier**（廠商類別識別碼）欄位。輸入 VCI，其為字串或十六進位值（具有 0x 首碼），用於比對來自包含選項 60 之用戶端要求的值。伺服器會在其表格中查閱傳入的 VCI，並傳回選項 43 和對應的選項值。
4. 從 **DHCP** 伺服器繼承來源繼承—請只在您指定 DHCP 伺服器預先定義選項的 **Inheritance Source**（繼承來源），且要讓其他項目也可從此來源 **inherited**（繼承）繼承廠商特定和自訂選項時，選取此項。
5. 檢查繼承來源狀態—如果您已選取 **Inheritance Source**（繼承來源），則按一下此連結會開啟 **Dynamic IP Interface Status**（動態 **IP** 介面狀態），其中顯示從 DHCP 用戶端繼承的選項。
6. 如果您未選取 **Inherit from DHCP server inheritance source**（從 **DHCP** 伺服器繼承來源繼承），請選取 **Option Type**（選項類型）：**IP Address**（**IP** 位址）、**ASCII** 或 **Hexadecimal**（十六進位）。十六進位值必須以 0x 首碼開頭。
7. 輸入您要讓 DHCP 伺服器為該 **Option Code**（選項代碼）提供的 **Option Value**（選項值）。您可以在個別行上輸入多個值。
8. 按一下 **OK**（確定）。

STEP 4 | （選用）新增其他廠商特定或自訂 DHCP 選項。

1. 重複上一步驟以輸入其他自訂 DHCP 選項。

   - 您可以針對具有相同 **Option Name**（選項名稱）的 **Option Code**（選項代碼）輸入多個選項值，但 **Option Code**（選項代碼）的所有值都必須是相同類型 (**IP Address**（**IP** 位址）、**ASCII** (ASCII) 或 **Hexadecimal**（十六進位）)。如果繼承或輸入某個類型，且針對相同 **Option Code**（選項代碼）和相同 **Option Name**（選項名稱）輸入不同類型，則第二個類型會覆寫第一個類型。

     針對選項輸入多個值時，請依偏好順序輸入值，或在清單中移動自訂 DHCP 選項以達到偏好順序。選取選項，然後按一下 **Move Up**（上移）或 **Move Down**（下移）。
   - 您可以使用不同的 **Option Name**（選項名稱）來多次輸入 **Option Code**（選項代碼）。在此狀況下，多個選項名稱之間選項代碼的 **Option Type**（選項類型）可以不同。

2. 按一下 **OK**（確定）。

STEP 5 | 識別可設定狀態的 IP 位址集區，DHCP 伺服器會從此集區中選擇位址並指派給 DHCP 用戶端。

如果您不是網路的網路管理員，請向網路管理員詢問網路計劃中 ***IP*** 位址的有效集區，這些位址可指定為由 ***DHCP*** 伺服器指派給用戶端。

1. 在 **IP Pools**（**IP** 配發範圍）欄位中，**Add**（新增）IP 位址範圍，此伺服器會將此範圍內的位址指派給用戶端。輸入 IP 子網路與子網路遮罩 (例如 192.168.1.0/24) 或 IP 位址範圍 (例如 192.168.1.10-192.168.1.20)。
   - IP 配發範圍或 **Reserved Address**（保留的位址）對於動態 IP 位址指派而言為必要。
   - IP 配發範圍對靜態 IP 位址指派而言為選用，前提是您指派的 IP 位址屬於防火牆介面服務的子網路。
2. （選用）重複此步驟以指定其他 IP 位址集區。

STEP 6 | （選用）從 IP 配發範圍中指定將不動態指派的 IP 位址。如果您也指定 **MAC Address**（**MAC** 位址），則當裝置透過 DHCP 要求 IP 位址時，系統會將 **Reserved Address**（保留的位址）指派給該裝置。

關於 ***Reserved Address***（保留的位址）分配的說明，請參閱DHCP 定址一節。

1. 在 **Reserved Address**（保留的位址）欄位中，按一下 **Add**（新增）。
2. 輸入 **IP Pools**（**IP** 配發範圍）中您不要讓 DHCP 伺服器動態指派的位址（格式為 *x.x.x.x*）。
3. （選用）指定您要將永久指派您剛才指定之 IP 位址的裝置的 **MAC Address**（**MAC** 位址）（格式為 *xx:xx:xx:xx:xx:xx*）。
4. （選用）重複前兩個步驟以保留其他位址。

STEP 7 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

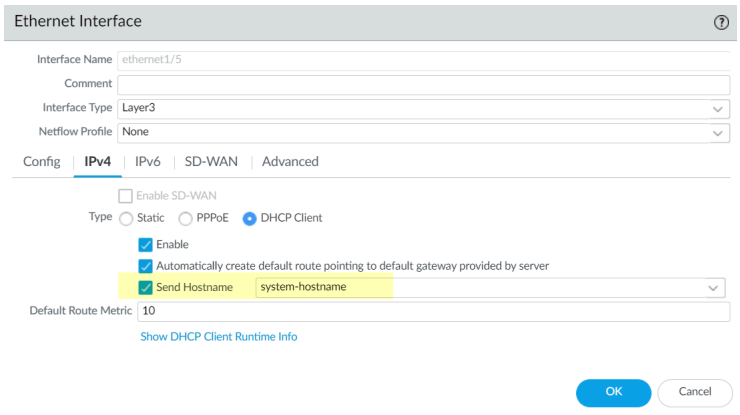
將介面設定為 DHCP 用戶端

將防火牆介面設定為 DHCP 用戶端前，請確定您已設定 Layer 3 介面（乙太網路介面、乙太網路子介面、VLAN 介面、VLAN 子介面、彙總介面、彙總子介面），且該介面已指派給虛擬路由器與區域。如果您需要使用 DHCP 來為介面要求 IPv4 位址，請將介面設定為 DHCP 用戶端。

您還可以將管理介面設定為 DHCP 用戶端。

STEP 1 | 將介面設定為 DHCP 用戶端。

1. 選取 **Network**（網路） > **Interfaces**（界面）。
2. 在 **Ethernet**（乙太網路）或 **VLAN** 頁籤上，**Add**（新增）Layer 3 介面，或者選取您要用作 DHCP 用戶端的已設定 Layer 3 介面。
3. 選取 **Ipv4** 頁籤，而對於 **Type**（類型），選取 **DHCP Client**（**DHCP** 用戶端）。
4. 選取 **Enable**（啟用）。
5. （選用）啟用選項以 自動建立指向伺服器所提供之預設閘道的預設路由（依預設啟用）。啟用此選項會讓防火牆建立到預設閘道的靜態路由，這對用戶端嘗試存取許多不需要在防火牆的路由表中維護路由的目的地時很有用。
6. （選用）啟用選項以 **Send Hostname**（傳送主機名稱）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 伺服器可隨後在 DNS 伺服器上註冊該主機名稱。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 (_)。



7. （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）（優先順序層級）（範圍是 1 至 65,535；預設值是 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。

防火牆與 *DHCP* 伺服器之間的路由的 ***Default Route Metric***（預設路由公制）預設值是 *10*。如果靜態預設值路由 *0.0.0.0/0* 使用 *DHCP* 介面作為其輸出介面，則路由的預設 ***Metric***（公制）也是 *10*。因此，有兩條公制為 *10* 的路由，防火牆可一次隨機選擇其中一條路由，下一次選擇另一條路由。

假設您啟用以下選項：自動建立指向伺服器所提供之預設閘道的預設路由，選取一個虛擬路由器，為 *Layer 3* 介面新增靜態路由，將 ***Metric***（公制）（預設值為 *10*）變更為大於 *10* 的值（在本範例中為 *100*）並提交您的變更。在路由表中，路由公制將不會顯示 *100*。相反，路由將按預期指示預設值為 *10*，因為 *10* 優先於設定值 *100*。然而，如果您將靜態路由的 ***Metric***（公制）變更為小於 *10* 的值（例如 *6*），則在路由表中的路由將更新為顯示設定公制 *6*。

8. （選用）啟用選項 **Show DHCP Client Runtime Info**（顯示 **DHCP** 用戶端執行階段資訊）以檢視用戶端從其 DHCP 伺服器繼承的所有設定。

STEP 2 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

乙太網路介面現在應在 **Ethernet**（乙太網路）頁籤中將 **Dynamic-DHCP Client**（動態 **DHCP** 用戶端）顯示為其 **IP Address**（**IP** 位址）。

STEP 3 | （選用）瞭解防火牆上的哪一個介面被設為 DHCP 用戶端。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後檢查 **IP Address**（**IP** 位址），瞭解哪些介面指示了 DHCP 用戶端。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後檢查 **IP Address**（**IP** 位址），瞭解哪些介面指示了 DHCP 用戶端。

將管理介面設定為 DHCP 用戶端

防火牆上的管理介面支援適用於 IPv4 的 DHCP 用戶端，這使管理介面可以從 DHCP 伺服器接收 IPv4 位址。管理介面還支援 DHCP 選項 12 和選項 61，讓防火牆可將其主機名稱和用戶端識別碼分別傳送至 DHCP 伺服器。

依預設，AWS 和 Azure™ 中部署的 VM 系列防火牆將管理介面用作 DHCP 用戶端以獲得其 IP 位址，而非靜態 IP 位址，因為雲部署需要此功能提供的自動化。依預設，會針對 VM 系列防火牆（AWS 和 Azure 中的 VM 系列防火牆除外）關閉管理介面上的 DHCP。WildFire 和 Panorama 型號上的管理介面不支援此 DHCP 功能。

- 對於基於硬體的防火牆型號（非 ***VM*** 系列），使用靜態 ***IP*** 位址設定管理介面（如可能）。
- 如果防火牆透過 ***DHCP*** 要求管理介面位址，則在 ***DHCP*** 伺服器上指派一個 ***MAC*** 位址保留區用於該防火牆。該保留區確保防火牆在重新啟動後獲得其管理 ***IP*** 位址。如果 ***DHCP*** 伺服器為 ***Palo Alto Networks®*** 防火牆，請參閱將介面設定為 DHCP 伺服器的第 *6* 步以瞭解保留位址的資訊。

如果您將管理介面設定為 DHCP 用戶端，以下限制適用：

- 您不能將 HA 組態的管理介面用於控制連結（HA1 或 HA1 備份）、資料連結（HA2 或 HA2 備份）或封包轉送 (HA3) 通訊。
- 您不能在自訂服務路由（**Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Service Route Configuration**（服務路由組態） > **Customize**（自訂））時選取 **MGT** 作為來源介面。但是，您可選取 **Use default**（使用預設）來透過管理介面路由封包。
- 您不能使用管理界面的動態 IP 位址連線至硬體安全性模組 (HSM)。HSM 用戶端防火牆上的 IP 位址必須為靜態 IP 位址，因為 HSM 將使用 IP 位址驗證防火牆，如果在執行階段 IP 位址發生變更，HSM 上的作業將停止。

此工作的先決條件是管理介面必須能到達 DHCP 伺服器。

STEP 1 | 將管理介面設定為 DHCP 用戶端，以便該介面可從 DHCP 伺服器接收其 IP 位址 (IPv4)、網路遮罩 (IPv4) 和預設閘道。

或者，如果您使用的協調運作系統會接收此資訊，也可以將管理介面的主機名稱和用戶端識別碼傳送至 DHCP 伺服器。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Management Interface Settings（管理介面設定）。
2. 對於 **IP Type** (IP 類型)，選取 **DHCP Client**（**DHCP** 用戶端）。
3. （選用）為防火牆選取一個或兩個選項以傳送至 DHCP Discover 或 Request 訊息中的 DHCP 伺服器。
   - **Send Hostname**（傳送主機名稱）—將 **Hostname**（主機名稱）（如在 **Device**（裝置） > **Setup**（設定） > **Management**（管理） 中定義）作為 DHCP 選項 12 的一部分來傳送。
   - 傳送用戶端 **ID**—將用戶端識別碼作為 DHCP 選項 61 的一部分來傳送。用戶端識別碼可唯一識別 DHCP 用戶端，DHCP 伺服器使用它來索引其組態參數資料庫。
4. 按一下 **OK**（確定）。

STEP 2 | （選用）將防火牆設定為從 DHCP 伺服器接收主機名稱和網域。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 選取一個或兩個選項：
   - 接收 **DHCP** 伺服器提供的主機名稱—讓防火牆可從 DHCP 伺服器接收主機名稱 (如有效)。啟用後，來自 DHCP 伺服器的主機名稱會取代 **Device**（裝置） > **Setup**（設定） > **Management**（管理）中指定的任何現有的 **Hostname**（主機名稱）。如果您要手動設定主機名稱，則不要選取此選項。
   - 接收 **DHCP** 伺服器提供的網域—讓防火牆可從 DHCP 伺服器接收網域。來自 DHCP 伺服器的網域（DNS 尾碼）會取代 **Device**（裝置） > **Setup**（設定） > **Management**（管理）中指定的任何現有的 **Domain**（網域）。如果您要手動設定網域，則不要選取此選項。
3. 按一下 **OK**（確定）。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

STEP 4 | 檢視 DHCP 用戶端資訊。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），以及 Management Interface Settings（管理介面設定）。
2. 按一下 **Show DHCP Client Runtime Info** (顯示 DHCP 用戶端執行階段資訊)。

STEP 5 | （選用）向 DHCP 伺服器申請更新 DHCP 租期（不論租期為多久）。

這個選項在您要檢測或疑難排解網路問題時會很方便。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 Management Interface Settings（管理介面設定）。
2. 按一下 **Show DHCP Client Runtime Info** (顯示 DHCP 用戶端執行階段資訊)。
3. 按一下 **Renew**（更新）。

STEP 6 | （選用）釋放來自 DHCP 伺服器的以下 DHCP 選項：

- IP 位址
- 網路遮罩
- 預設閘道
- DNS 伺服器（主要和次要）
- NTP 伺服器（主要和次要）
- 網域（DNS 尾碼）

釋放後會令 *IP* 位址變得可用，如果不設定其他介面來獲得管理存取權限，就會斷開網路連接並使防火牆變得難以管理。

使用 CLI 操作命令 **`request dhcp client management-interface release`**。

將介面設定為 DHCP 轉送代理程式

若要讓防火牆介面在用戶端與伺服器之間傳輸 DHCP 訊息，必須將防火牆設定為 DHCP 轉送代理程式。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。系統會將用戶端 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其 DHCPOFFER 訊息轉送回要求的用戶端。

功能如下：

- 除 PA-5200 系列與 PA-7000 系列防火牆外，您可在所有防火牆型號中組合設定總計 500 個 DHCP 伺服器 (IPv4) 與 DHCP 轉送代理程式（IPv4 與 IPv6）
- 在 PA-5220 防火牆中，您可設定最多 500 個 DHCP 伺服器以及最多 2,048 個 DHCP 轉送代理程式（減去所設定的 DHCP 伺服器數）。例如，如果您設定 500 個 DHCP 伺服器，您可設定 1,548 個 DHCP 轉送代理程式。
- 在 PA-5250、PA-5260 與 PA-7000 系列防火牆中，您可設定最多 500 個 DHCP 伺服器以及最多 4,096 個 DHCP 轉送代理程式（減去所設定的 DHCP 伺服器數）。例如，如果您設定 500 個 DHCP 伺服器，您可設定 3,596 個 DHCP 轉送代理程式。

在設定 DHCP 轉送代理程式前，請確定您已設定 Layer 3 Ethernet 或 Layer 3 VLAN 介面，且該介面已指派給虛擬路由器與區域。

STEP 1 | 選取 DHCP 轉送。

選取 **Network**（網路） > **DHCP** > **DHCP Relay**（**DHCP** 轉送）。

STEP 2 | 指定 DHCP 轉送代理程式將通訊的每個 DHCP 伺服器其 IP 位址。

1. 在 **Interface**（介面）欄位中，選取您要作為 DHCP 轉送代理程式的介面。
2. 選取 **IPv4** 或 **IPv6**，指示您要指定的 DHCP 伺服器位址類型。
3. 若您核取了 **IPv4**，則在 **DHCP Server IP Address**（**DHCP** 伺服器 **IP** 位址）欄位中，**Add**（新增）您要轉送 DHCP 訊息至/自的 DHCP 伺服器位址。
4. 若您核取了 **IPv6**，則在 **DHCP Server IPv6 Address**（**DHCP** 伺服器 **IPv6** 位址）欄位中，**Add**（新增）您要轉送 DHCP 訊息至/自的 DHCP 伺服器位址。如果您指定多點傳送位址，則還須指定傳出 **Interface**（介面）。
5. （選用）重複步驟前三個步驟，為每個 IP 位址系列輸入最多八個 DHCP 伺服器位址。

STEP 3 | 提交組態。

按一下 **OK**（確定）與 **Commit**（提交）。

監控與疑難排解 DHCP

您可以從 CLI 發出命令，來檢視已指派給 DHCP 用戶端或 DHCP 伺服器已指派的動態位址租期狀態。在租期到期並自動釋放前，您也可以先清除租期。

- 檢視 DHCP 伺服器資訊
- 清除 DHCP 租期
- 檢視 DHCP 用戶端資訊
- 收集 DHCP 的除錯輸出

檢視 DHCP 伺服器資訊

執行此工作，以檢視 DHCP 集區統計資料、伺服器已指派的 IP 位址、對應的 MAC 位址、租期的狀態與期間，以及租期開始的時間。如果已將該位址設定為 **Reserved Address** (保留的位址)，則狀態欄會表示為 `reserved`，且沒有 `duration` 或 `lease_time`。如果將租期設定為 **Unlimited** (無限制)，則 持續時間欄會顯示 `0` 值。

檢視 DHCP 集區統計資料、所指派的 DHCP 伺服器 IP 位址、MAC 位址、租期的狀態與期間，以及租期開始的時間。

```
admin@PA-220> show dhcp server lease interface all
```

```
interface: "ethernet1/2"
Allocated IPs: 1, Total number of IPs in pool: 5. 20.0000% used
ip              mac                state      duration
 lease_time
192.168.3.11    f0:2f:af:42:70:cf  committed  0           Wed Jul
 2 08:10:56 2014
admin@PA-220>
```

檢視 DHCP 伺服器指派給用戶端的選項。

```
admin@PA-220> show dhcp server settings all
```

```
Interface    GW           DNS1        DNS2       DNS-Suffix Inherit
 source
------------------------------------------------------------------------------
ethernet1/2  192.168.3.1  10.43.2.10  10.44.2.10
             ethernet1/3
admin@PA-220>
```

清除 DHCP 租期

您可以透過幾個選項清除 DHCP 租期。

在保留計時器自動解除介面（伺服器）（例如 ethernet1/2）的過期 DHCP 租期之前，先行解除。這些位址會再次回到 IP 集區。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 expired-only
```

解除特定 IP 位址的租期，例如 192.168.3.1。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 ip 192.168.3.1
```

解除特定 MAC 位址的租期，例如 f0:2c:ae:29:71:34。

```
admin@PA-220> clear dhcp lease interface ethernet1/2 mac
 f0:2c:ae:29:71:34
```

檢視 DHCP 用戶端資訊

當防火牆用作 DHCP 用戶端時，若要檢視傳送給防火牆的 IP 位址租期狀態，可使用下列任何命令。

```
admin@PA-220>show dhcp client state <interface_name>
```

```
admin@PA-220> show dhcp client state all
```

```
Interface       State        IP              Gateway
 Leased-until
--------------------------------------------------------------------------------
ethernet1/1     Bound        10.43.14.80     10.43.14.1
 70315
admin@PA-220>
```

收集 DHCP 的除錯輸出

若要手動收集 DHCP 相關的除錯輸出，請使用下列其中一個命令：

```
admin@PA-220> debug dhcpd
```

```
admin@PA-220> debug management-server dhcpd
```

DNS

網域名稱系統 (DNS) 是一種通訊協定，用於將使用者易記的網域名稱，例如 www.paloaltonetworks.com，轉譯（解析）成 IP 位址，以便使用者存取電腦、網站、服務或網際網路或私人網路上的其他資源。

DNS 概要

DNS 在允許使用者存取網路資源中起到了關鍵作用，讓使用者無需記住 IP 位址並讓電腦無需儲存海量對應到 IP 位址的網域名稱。DNS 採用了用戶端/伺服器模型；DNS 伺服器透過以下方式為 DNS 用戶端解析查詢：在快取中查閱網域，並在必要時將查詢傳送至其他伺服器，直至能夠向用戶端回應相應的 IP 位址。

網域名稱的 DNS 結構分多個階層：網域名稱中的頂層網域 (TLD) 可以是一般 TLD (gTLD)：com、edu、gov、int、mil、net 或 org（gov 和 mil 僅適用於美國）或國家/地區代碼 (ccTLD)，例如 au（澳洲）和 us（美國）。ccTLD 一般為國家和自治地區保留。

完整網域名稱 (FQDN) 至少包括主機名稱、次層網域以及 TLD，以在 DNS 結構完整地指定主機位置。例如，www.paloaltonetworks.com 就是一個 FQDN。

當 Palo Alto Networks® 防火牆使用 CLI 或使用者介面中的 FQDN 時，防火牆必須使用 DNS 解析該 FQDN。視乎 ®FQDN 查詢的來源，防火牆將確定使用哪種 DNS 設定來解析查詢。

FQDN 的 DNS 記錄包含存留時間 (TTL) 值，依預設，防火牆根據 DNS 伺服器提供的個別 TTL 來重新整理其快取中的各 FQDN，只要 TTL 大於或等於您在防火牆上設定的 FQDN 重新整理時間下限，或大於或等於 30 秒的預設設定值（未設定 FQDN 重新整理時間下限）。根據其 TTL 值重新整理 FQDN 在安全存取雲端平台服務時特別有用，雲端平台服務經常需要頻繁重新整理 FQDN 以確保提供具有高可用性的服務。例如，支援自動調整規模的雲端環境依賴於 FQDN 解析來動態地上下調整服務規模，而 FQDN 的快速解析功能在此類時間敏感的環境中也非常重要。

透過設定 FQDN 重新整理時間下限，您可限制防火牆支援的 TTL 值大小。如果 IP 位址的變更不是很頻繁，您可設定一個較高的 FQDN 重新整理時間下限，以避免防火牆在不必要時重新整理項目。防火牆使用 DNS TTL 時間和所設定 FQDN 重新整理時間下限中的較大值。

例如，兩個 FQDN 的 TTL 值如下：FQDN 重新整理時間下限會覆寫較小（較快）的 TTL 值。

	TTL	如果 **FQDN** 重新整理時間下限 = **26**	實際重新整理時間
FQDN A	20		26
FQDN B	30		30

當防火牆從解析 FQDN 的 DNS 伺服器或 DNS Proxy 物件接到 DNS 回應時，FQDN 重新整理計時器將開始計時。

此外，您還可設定失效逾時，以設定防火牆在無法存取 DNS 伺服器時繼續使用 FQDN 失效（過期）解析的時間長度。在失效逾時期間結束時，如果 DNS 伺服器仍然無法存取，失效 FQDN 項目將無法解析（防火牆將移除失效 FQDN 項目）。

下列防火牆工作與 DNS 相關：

- 為防火牆設定至少一個 DNS 伺服器，以便其能解析主機名稱。設定主要和次要 DNS 伺服器或指定此類伺服器的 DNS Proxy 物件，如使用案例 1：防火牆需要 DNS 解析所示。

- 自訂防火牆處理由安全性原則規則、報告及管理服務（例如電子郵件、Kerberos、SNMP、syslog 等）為每個虛擬系統啟動的 DNS 解析的方式，如使用案例 2：ISP 租用戶使用 DNS Proxy 來處理在其虛擬系統 內的安全性原則、報告和服務的 DNS 解析。
- 設定防火牆，以用作用戶端的 DNS 伺服器，如使用案例 3：防火牆作為用戶端與伺服器 之間的 DNS Proxy。
- 設定反間諜軟體設定檔，以使用 DNS 查詢識別網路上受感染的主機。
- 啟用規避特徵碼，然後為威脅防禦啟用規避特徵碼。
- 將介面設定為 DHCP 伺服器。這可以使防火牆用作 DHCP 伺服器，並將 DNS 資訊傳送至 DHCP 用戶端，以便所提供的 DHCP 用戶端能夠連線各自的 DNS 伺服器。

DNS Proxy 物件

當設定為 DNS Proxy，防火牆將是 DNS 用戶端與伺服器之間的中介；它可藉由從 DNS Proxy 快取中解析查詢，而作為 DNS 伺服器本身。如果在 DNS Proxy 快取中找不到網域名稱，防火牆會在特定 DNS Proxy 物件（在 DNS 查詢到達的介面上）中的項目間搜尋網域名稱的相符項目。防火牆將根據相符結果將查詢轉送至相應 DNS 伺服器。如果找不到相符結果，防火牆將使用預設的 DNS 伺服器。

您可以在 DNS Proxy 物件中進行設定，以決定防火牆要如何作為 DNS Proxy。您可以將 DNS Proxy 物件指派給單一虛擬系統，或將其共用於所有虛擬系統之間。

- 如果將 DNS Proxy 物件用於虛擬系統，您可以指定 DNS Server Profile（伺服器設定檔），此設定檔會指定主要和次要 DNS 伺服器位址，以及其他資訊。DNS 伺服器設定檔可簡化設定作業。
- 如果共用 DNS Proxy 物件，您必須為 DNS 伺服器至少指定一個主要位址。

使用 *DNS* 服務設定多個租用戶（*ISP* 訂閱者）時，每個租用戶均應定義其本身的 *DNS Proxy*，以區隔租用戶的 *DNS* 服務與其他租用戶的服務。

在 Proxy 物件中，您可以指定以防火牆作為 DNS Proxy 的介面。此介面的 DNS Proxy 不會使用服務路由；對 DNS 要求的回應一律會傳送至為 DNS 要求送達的虛擬路由器指派的介面。

當您 設定 DNS Proxy 物件 時，可以為 DNS Proxy 提供靜態「FQDN 到位址」對應。您還可以建立 DNS Proxy 規則，以控制指定的網域名稱查詢（與 Proxy 規則相符）將被導向至哪個 DNS 伺服器。您可以在防火牆上設定最多 256 個 DNS Proxy 物件。如果 DNS Proxy 物件指派給**Device**（裝置） > **Setup**（設定） > **Services**（服務） > **DNS**或**Device**（裝置） > **Virtual Systems**（虛擬系統） > **vsys** > **General**（一般） > **DNS Proxy**，則您必須啟用快取和快取 **EDNS** 回應 (在 **Network**（網路） > **DNS Proxy** > **Advanced**（進階）項下）。此外，如果此 DNS Proxy 物件設定了 **DNS Proxy** 規則，則這些規則也需要啟用快取（開啟由此對應解析之網域的快取）。

當防火牆收到 FQDN 查詢後（DNS Proxy 快取中沒有該網域名稱），防火牆將比較 FQDN 中的網域名稱與 DNS Proxy 物件的 DNS Proxy 規則中的網域名稱。如果您在單一 DNS Proxy 規則中指定了多個網域名稱，只要查詢與規則中任何個網域名稱相符，就表示查詢與規則相符。DNS Proxy 規則與 FQDN 比對 介紹了防火牆如何確定 FQDN 是否與 DNS Proxy 規則中的網域名稱相符。與規則相符的 DNS 查詢將傳送至為要解析至 Proxy 物件設定的主要 DNS 伺服器。

DNS Server Profile（伺服器設定檔）

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 IP 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）。來源介面可決定虛擬路由器；其中包含路由表格。目的地 IP 位址可從指派了來源介面之虛擬路由器的路由表中查閱。目的地 IP 輸出介面的結果有可能與來源介面不同。封包會從路由表格查閱所決定的目的地 IP 輸出介面輸出，但來源 IP 位址會是設定的位址。來源位址會用作為 DNS 伺服器之回覆中的目的地位址。

虛擬系統報告和虛擬系統伺服器設定檔會將其查詢傳送至為虛擬系統指定的 DNS 伺服器（如果有的話）。（所使用的 DNS 伺服器在 **Device**（裝置） > **Virtual Systems**（虛擬系統） > **General**（一般） > **DNS Proxy** 中定義。） 如果沒有為虛擬系統指定的 DNS 伺服器，則會查詢為防火牆指定的 DNS 伺服器。

您只能為虛擬系統 設定 DNS 伺服器設定檔；它不適用於全域 Shared（共用）位置。

多租用戶 DNS 部署

防火牆會根據 DNS 要求的發出來源，決定處理此要求的方式。ISP 在防火牆上有多個租用戶的環境被稱為多租用戶環境。多租用戶 DNS 部署有三種使用案例：

- 全域管理 **DNS** 解析—防火牆本身需要 DNS 解析，例如，管理平面請求為軟體更新服務等管理事件解析 FQDN。防火牆會使用服務路由聯繫 DNS 伺服器，因為在特定虛擬路由器上，沒有 DNS 要求傳入。
- 虛擬系統的原則和報告 **FQDN** 解析—對於來自於安全性原則、報告或服務的 DNS 查詢，您可以指定虛擬系統（租用戶）專用的一組 DNS 伺服器，或者可以預設為全域 DNS 伺服器。如果您的使用案例需要為每個虛擬系統設定不同的 DNS 伺服器集合，則必須設定 DNS Proxy 物件。解析會隨著被指派 DNS Proxy 的虛擬系統而不同。如果沒有適用於此虛擬系統的特定 DNS 伺服器，則防火牆將使用全域 DNS 設定。
- 虛擬系統的資料平面 **DNS** 解析—此方法也稱為「DNS 解析的網路要求」。租用戶的虛擬系統可進行設定，使指定的網域名稱可在租用戶的 DNS 伺服器上（在其網路中）解析。此方法支援分割 ***DNS***，這表示租用戶也可以將其本身的 ISP DNS 伺服器用於其餘在其本身的伺服器上無法解析的 DNS 查詢。DNS Proxy 物件規則可控制分割 DNS；租用戶的網域會將 DNS 要求重新導向至其 DNS 伺服器，而這些伺服器設定於 DNS 伺服器設定檔中。DNS 伺服器設定檔具有指定的主要和次要 DNS 伺服器，以及 IPv4 和 IPv6 的 DNS 服務路由，會覆寫預設 DNS 設定。

下表彙總了 DNS 解析類型。繫結位置會決定用於解析的 DNS Proxy 物件。為了方便解說，這些使用案例將說明服務提供者可能如何設定 DNS 設定以提供 DNS 服務，用以解析防火牆和租用戶（訂閱者）虛擬系統所需的 DNS 查詢。

解析類型	地點：共享	地點：特定 **Vsys**
防火牆 DNS 解析—由管理平面執行	繫結：全域 說明於使用案例 1	無
安全性設定檔、報告和伺服器設定檔解析—由管理平面執行	繫結：全域 行為與使用案例 1 相同	繫結：特定 vsys 說明於使用案例 2
連接到防火牆上的介面、通過防火牆連至 DNS 伺服器的 DNS 用戶端主機的 DNS Proxy 解析—由資料平面執行	繫結：介面 服務路由：接收到 DNS 要求的介面和 IP 位址。 說明於使用案例 3	

- 使用案例 1：防火牆需要 DNS 解析
- 使用案例 2：ISP 租用戶使用 DNS Proxy 來處理在其虛擬系統 內的安全性原則、報告和服務的 DNS 解析
- 使用案例 3：防火牆作為用戶端與伺服器 之間的 DNS Proxy

設定 DNS Proxy 物件

如果您的防火牆要用作 DNS Proxy，則執行此工作以設定 DNS Proxy 物件。Proxy 物件可在所有的虛擬系統間共用，或套用至特定的虛擬系統。

但啟用防火牆以用作 ***DNS Proxy*** 後，偵測所設計之 ***HTTP*** 或 ***TLS*** 要求的規避特徵碼，可向用戶端連接至原始 ***DNS*** 查詢中指定的網域以外的網域的實例發出警示。最佳做法時，設定 ***DNS Proxy*** 後，啟用規避特徵，以在偵測到所設計的要求後觸發警示。

STEP 1 | 設定 DNS Proxy 物件的基本設定。

1. 選取 **Network**（網路） > **DNS Proxy**，然後 **Add**（新增） 新的物件。
2. 確認已選取 **Enable**（啟用）。
3. 輸入物件的 **Name**（名稱）。
4. 針對 **Location**（位置），選取要套用物件的虛擬系統。如果您選取 **Shared**（共用），則必須指定至少一個 **Primary**（主要）DNS 伺服器位址，並選擇性地指定 **Secondary**（次要）位址。
5. 如果您選取虛擬系統，請選取 DNS 伺服器設定檔作為 **Server Profile**（伺服器設定檔），或按一下 **DNS Server Profile**（**DNS** 伺服器設定檔）以設定新的設定檔。請參閱設定 DNS 伺服器設定檔。
6. 從 Inheritance Source（繼承來源）選取要從中繼承預設 DNS 伺服器設定的來源。預設值為 **None**（無）。
7. 針對 **Interface**（介面）按一下 **Add**（新增），並指定要套用 DNS Proxy 物件的介面。
   - 如果您使用 DNS Proxy 物件執行 DNS 查閱，則需要介面。防火牆會在此介面上接聽 DNS 要求，並進行其 Proxy 處理。
   - 如果您將 DNS Proxy 物件用於服務路由，則介面為選用項目。

STEP 2 | (選用) 指定 DNS Proxy 規則。

1. 在 **DNS Proxy Rules**（**DNS Proxy** 規則）頁籤上，**Add**（新增）規則的 **Name**（名稱）。
2. 如果您要讓防火牆快取已解析的網路，請 **Turn on caching of domains resolved by this mapping**（開啟由此對應解析之網域的快取）。
3. 對於 **Domain Name**（網域名稱），**Add**（新增）一個或多個網域，每列一個項目，防火牆會比較 FQDN 查詢與這些網域。如果查詢與規則中的某一個網域相符，該查詢將被傳送至以下伺服器中的一個，進行解析（視乎於您在前一步中的設定）：
   - 為此 Proxy 物件直接指定的 **Primary**（主要）或 **Secondary**（次要） DNS 伺服器。
   - 在 DNS 伺服器設定檔中為此 Proxy 物件指定的 **Primary**（主要）或 **Secondary**（次要）DNS 伺服器。

   DNS Proxy 規則與 FQDN 比對中介紹了防火牆如何比對 FQDN 中的網域名稱與 DNS Proxy 規則。如果不相符，將由預設 DNS 伺服器解析查詢。
4. 視乎您的 **Location**（位置）設定，執行以下任何步驟：
   - 如果您選擇了虛擬系統，則選取 **DNS Server profile**（**DNS** 伺服器設定檔）。
   - 如果您選擇了 **Shared**（共用），則輸入 **Primary**（主要）位址，可以選擇性地輸入 **Secondary**（次要）位址。
5. 按一下 **OK**（確定）。

STEP 3 | （選用）您可以為 DNS Proxy 提供靜態「FQDN 對位址」項目。靜態 DNS 項目可讓防火牆將 FQDN 解析為 IP 位址，而無須傳送查詢至 DNS 伺服器。

1. 在 **Static Entries**（靜態項目）頁籤上，**Add**（新增）**Name**（名稱）。
2. 輸入完全合格網域名稱 (**FQDN**)。
3. 對於 **Address**（位址），**Add**（新增）FQDN 應對應到的 IP 位址。

   您可以為項目提供額外的 IP 位址。防火牆會在其 DNS 回應中提供所有這些 IP 位址，用戶端會選擇要使用的位址。
4. 按一下 **OK**（確定）。

STEP 4 | 為 DNS Proxy 啟用快取並設定其他進階設定。

1. 在 **Advanced**（進階）頁籤上，選取 **TCP Queries**（**TCP** 查詢），以啟用使用 TCP 的 DNS 查詢。
   - 最大擱置要求—輸入防火牆所將支援的並行、擱置 TCP DNS 要求數上限（範圍為 64-256；預設值為 64）。
2. 對於 **UDP Queries Retries**（**UDP** 查詢重試），輸入：
   - 間隔（秒） — 一段特定的時間（範圍為 1 到 30，預設值為 2），如果在此時間後沒有收到回應，則傳送其他要求。
   - 嘗試次數—在查詢下一個 DNS 伺服器之前的 UDP 查詢次數上限（不包括第一次）（範圍為 1 到 30；預設值為 5。）
3. 選取 **Cache**（快取），以使防火牆快取其所學習的 FQDN 到位址對應。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）（依預設啟用）。

- 選取 **Enable TTL**（啟用 **TTL**），以限制防火牆快取 Proxy 物件的 DNS 解析項目所需的時間長度。預設會停用。
  - 輸入 **Time to Live (sec)**（存留時間（秒）），在此時間過後，將移除為該 Proxy 物件快取的所有項目。移除這些項目後，必須再次解析及快取新的 DNS 要求。範圍為 60-86,400。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。
- 快取 **EDNS** 回應—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**，則您必須啟用此設定。

STEP 5 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

設定 DNS 伺服器設定檔

設定 DNS Server Profile（DNS 伺服器設定檔），將有助於簡化虛擬系統的組態。**Primary DNS**（主要 **DNS**）或 **Secondary DNS**（次要 **DNS**）位址可用來建立虛擬系統傳送至 DNS 伺服器的 DNS 要求。

STEP 1 | 為 DNS 伺服器設定檔命名、選取要套用設定檔的虛擬系統，然後指定主要和次要 DNS 伺服器位址。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **DNS**，然後為 DNS 伺服器設定檔 **Add**（新增）**Name**（名稱）。
2. 針對 **Inheritance Source**（繼承來源），選取要套用設定檔的虛擬系統。
3. 針對 **Inheritance Source**（繼承來源），如果未繼承 DNS 伺服器位址，請選取 **None**（無）。否則，請指定設定檔應繼承設定的 DNS 伺服器。如果您選擇 DNS 伺服器，請按一下 **Check inheritance source status**（檢查繼承來源狀態），以檢視該資訊。
4. 指定 **Primary DNS**（主要 **DNS**）伺服器的 IP 位址，或者若您選擇 **Inheritance Source**（繼承來源），則保留為 **inherited**（已繼承）。

   請注意，如果您指定 *FQDN*，而不是 *IP* 位址，則該 *FQDN* 的 *DNS* 會在 ***Device***（裝置） ***> Virtual Systems***（虛擬系統） ***> DNS Proxy*** 中解析。
5. 指定 **Secondary DNS**（次要 **DNS**）伺服器的 IP 位址，或者若您選擇 **Inheritance Source**（繼承來源），則保留為 **inherited**（已繼承）。

STEP 2 | 根據目標 DNS 伺服器的 IP 位址系列類型是 IPv4 還是 IPv6，來設定防火牆會自動使用的服務路由。

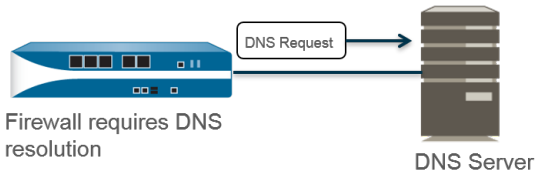
1. 按一下 **Service Route IPv4**（服務路由 **IPv4**），使後續的介面和 IPv4 位址可作為服務路由（如果目標 DNS 位址是 IPv4 位址）。
2. 指定 **Source Interface**（來源介面），以選取服務路由所將使用的 DNS 伺服器來源 IP 位址。防火牆會決定要將該介面指派給哪個虛擬路由器，然後在虛擬路由器的路由表格中執行路由查閱，以連繫目的地網路（根據 **Primary DNS**（主要 **DNS**）位址）。
3. 指定 IPv4 **Source Address**（來源位址），即封包傳送至以 IPv4 位址為來源的 DNS 伺服器。
4. 按一下 **Service Route IPv6**（服務路由 **IPv6**），使後續的介面和 IPv6 位址可作為服務路由（如果目標 DNS 位址是 IPv6 位址）。
5. 指定 **Source Interface**（來源介面），以選取服務路由所將使用的 DNS 伺服器來源 IP 位址。防火牆會決定要將該介面指派給哪個虛擬路由器，然後在虛擬路由器的路由表格中執行路由查閱，以連繫目的地網路（根據 **Primary DNS**（主要 **DNS**）位址）。
6. 指定 IPv6 **Source Address**（來源位址），即封包傳送至以 IPv4 位址為來源的 DNS 伺服器。
7. 按一下 **OK**（確定）。

STEP 3 | 提交組態。

按一下 **OK**（確定）與 **Commit**（提交）。

使用案例 1：防火牆需要 DNS 解析

在此使用案例中，防火牆是針對安全性原則規則、報告、管理服務（例如電子郵件、Kerberos、SNMP、syslog 等）及管理事件（軟體更新服務、動態軟體更新和 WildFire），要求進行 FQDN 的 DNS 解析之用戶端。在動態環境中，FQDN 會更頻繁地發生變更；準確的 DNS 解析可讓防火牆執行準確的原則，提供報告和管理服務，以及處理管理事件。共用的全域 DNS 服務會執行管理平面功能的 DNS 解析。



STEP 1 | 設定您要讓防火牆用於 DNS 解析的主要和次要 DNS 伺服器。

您必須在防火牆上手動設定至少一個 *DNS* 伺服器，否則將無法解析主機名稱；防火牆無法使用其他來源的 *DNS* 伺服器設定，例如 *ISP*。

1. 編輯 Services（服務）設定（為支援多個虛擬系統的防火牆選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Global**（全域）；為不支援多個虛擬系統的防火牆選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務））。
2. 在 **Services**（服務）頁籤上，針對 **DNS** 選取 **Servers**（伺服器），然後輸入 **Primary DNS Server**（主要 **DNS** 伺服器）位址和 **Secondary DNS Server**（次要 **DNS** 伺服器）位址。
3. 繼續移至步驟 3。

STEP 2 | 或者，如果您想要設定進階 DNS 功能（例如，分割 DNS、DNS Proxy 覆寫、DNS Proxy 規則、靜態項目或 DNS 繼承），您可以設定 DNS Proxy 物件。

1. 編輯 Services（服務）設定（為支援多個虛擬系統的防火牆選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Global**（全域）；為不支援多個虛擬系統的防火牆選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務））。
2. 在 **Services**（服務）頁籤上，針對 **DNS** 選取 **DNS Proxy Object**（**DNS Proxy** 物件）。
3. 從 **DNS Proxy** 清單中，選取要用來設定全域 DNS 服務的 DNS Proxy，或選取 **DNS Proxy** 以設定新的 DNS Proxy 物件，具體如下所示：
   1. 按一下 **Enable**（啟用），然後輸入 DNS Proxy 物件的 **Name**（名稱）。
   2. 在支援多個虛擬系統的防火牆上，針對 **Location**（位置），為適用於防火牆範圍內的全域 DNS Proxy 服務選取 **Shared**（共用）。

      共用 *DNS Proxy* 物件不會使用 *DNS* 伺服器設定，因為它們不需要屬於租用戶虛擬系統的特定服務路由。
   3. 輸入 **Primary**（主要）DNS 伺服器 IP 位址。選擇性地輸入 **Secondary**（次要）DNS 伺服器 IP 位址。
4. 選取 **Advanced**（進階）頁籤。確保已啟用 **Cache**（快取） 並已啟用 **Cache EDNS Responses**（快取 **EDNS** 回應）（依預設均為啟用）。
5. 按一下 **OK**（確定）來儲存 DNS Proxy 物件。

STEP 3 | （選用）設定 **Minimum FQDN Refresh Time (sec)**（**FQDN** 重新整理時間下限（秒））以限制防火牆重新整理 FQDN 快取項目的頻率。

依預設，防火牆根據 DNS 記錄中 FQDN 的個別 TTL 重新整理其快取中的各 FQDN，只要 TTL 大於或等於此 FQDN 重新整理時間下限設定（如果您沒有設定 FQDN 重新整理時間下限，則 TTL 須大於或等於 30 秒的預設設定）。若要設定 FQDN 重新整理時間下限，請輸入一個值（單位為秒；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 記錄中的 TTL 值重新整理 FQDN；防火牆不會強制執行 FQDN 重新整理時間下限。防火牆使用 DNS TTL 時間和 FQDN 重新整理時間下限中的較大值。

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地頻繁嘗試 *FQDN* 重新整理。

STEP 4 | （選用）指定 **FQDN Stale Entry Timeout (min)**（**FQDN** 失效項目逾時（分鐘）），即防火牆在無法存取 DNS 伺服器時繼續使用 FQDN 失效解析的時間長度（單位為分鐘；範圍為 0 至 10,080；預設值為 1,440）。

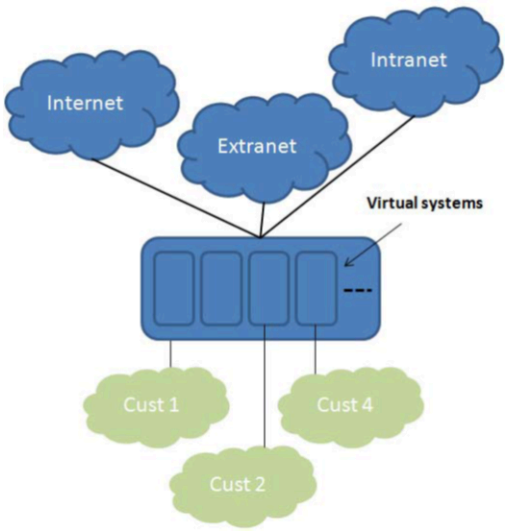
設定為 0 表示防火牆不會繼續使用 FQDN 失效項目。

確保 *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。

STEP 5 | 按一下 **OK**（確定）與 **Commit**（提交）。

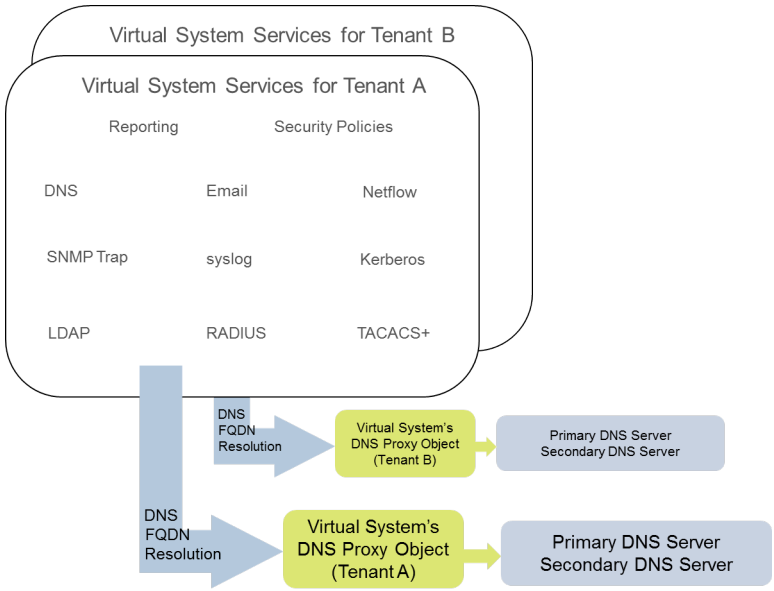
使用案例 2：ISP 租用戶使用 DNS Proxy 來處理在其虛擬系統內的安全性原則、報告和服務的 DNS 解析

在此使用案例中，有多個租用戶（ISP 訂閱者）定義於防火牆上，且對每個租用戶都配置了個別的虛擬系統 (vsys) 和虛擬路由器，用以分割其服務和管理網域。下圖說明防火牆內的數個虛擬系統。



每個租用戶都有其自身安全性原則規則的伺服器設定檔，用於其定義在本身網路中的安全性原則、報告和管理服務（例如電子郵件、Kerberos、SNMP、syslog 等等）。

對於這些服務所起始的 DNS 解析，每個虛擬系統都設定有本身的 DNS Proxy 物件，可讓每個租用戶自訂在其虛擬系統內處理 DNS 解析的方式。任何具有 **Location**（位置）的服務，都會使用為虛擬系統設定的 DNS Proxy 物件決定用來解析 FQDN 的主要（或次要）DNS 伺服器，如下圖所說明。



STEP 1 | 針對每個虛擬系統，指定所要使用的 DNS Proxy。

1. 選取 **Device**（裝置） > **Virtual Systems**（虛擬系統），然後 **Add**（新增）虛擬系統的 **ID**（範圍為 1-255）並選擇性地新增 **Name**（名稱），在此範例中為 Corp1 Corporation。
2. 在 **General**（一般）頁籤上選擇 **DNS Proxy** 或建立新的 Proxy。此範例選取 Corp1 DNS Proxy 作為 Corp1 Corporation 虛擬系統的 Proxy。
3. 針對 **Interfaces**（介面），按一下 **Add**（新增）。在此範例中，Ethernet1/20 會供此租用戶專用。
4. 針對 **Virtual Routers**（虛擬路由器），按一下 **Add**（新增）。名為 Corp1 VR 的虛擬路由器會指派給虛擬系統，以區隔路由功能。
5. 按一下 **OK**（確定）。

STEP 2 | 設定 DNS Proxy 和伺服器設定檔，以支援虛擬系統的 DNS 解析。

1. 選取 **Network**（網路） > **DNS Proxy**，然後按一下 **Add**（新增）。
2. 按一下 **Enable**（啟用），然後輸入 DNS Proxy 的 **Name**（名稱）。
3. 針對 **Location**（位置），選取租用戶的虛擬系統，在此範例中為 Corp1 Corporation (vsys6)。（您可以改為選擇 **Shared**（共用）DNS Proxy 資源。）
4. 針對 **Server Profile**（伺服器設定檔），選擇或建立一個設定檔，用以自訂此租用戶的安全性原則、報告和伺服器設定檔服務的 DNS 解析所使用的 DNS 伺服器。

   如果設定檔尚未設定，請在 **Server Profile**（伺服器設定檔）欄位中按一下 **DNS Server Profile**（**DNS** 伺服器設定檔），以 設定 DNS 伺服器設定檔。

   DNS 伺服器設定檔會識別此虛擬系統的管理 DNS 解析所使用的主要和次要 DNS 伺服器的 IP 位址。
5. 此外，針對此伺服器設定檔選擇性地設定 **Service Route IPv4**（服務路由 **IPv4**）及/或 **Service Route IPv6**（服務路由 **IPv6**），以向防火牆指出要在其 DNS 要求中使用的 **Source Interface**（來源介面）。如果該介面有多個 IP 位址，請同時設定 **Source Address**（來源位址）。
6. 選取 **Advanced**（進階）頁籤。確保已啟用 **Cache**（快取） 並已啟用 **Cache EDNS Responses**（快取 **EDNS** 回應）（依預設均為啟用）。如果 DNS proxy 物件

在**Device**（裝置）> **Virtual Systems**（虛擬系統）> **vsys** > **Genera**（一般）> **DNS Proxy**項下使用，則此為必需項。

7. 按一下 **OK**（確定）。
8. 按一下 **OK**（確定）與 **Commit**（提交）。

您可以使用 ***DNS Proxy Rules***（***DNS Proxy*** 規則）來設定選用的進階功能，例如分割 *DNS*。如有必要，個別的 *DNS* 伺服器設定檔可用來將與 ***DNS Proxy Rule***（***DNS Proxy*** 規則）中的 ***Domain Name***（網域名稱）相符的 *DNS* 解析重新導向至另一組 *DNS* 伺服器。使用案例 *3* 將解說分割 *DNS*。

如果您在相同的 DNS Proxy 物件中使用兩個個別的 DNS 伺服器設定檔，一個用於 DNS Proxy，一個用於 DNS Proxy 規則，將會發生下列行為：

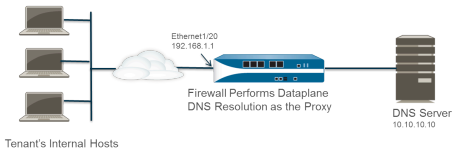
- 如果某個服務路由定義在 DNS Proxy 所使用的 DNS 伺服器設定檔中，它將被優先使用。
- 如果某個服務路由定義在 DNS Proxy 規則所使用的 DNS 伺服器設定檔中，它將不被使用。如果此服務路由不同於 DNS Proxy 使用的 DNS 伺服器設定檔中所定義的，在 **Commit**（提交）程序期間將會顯示下列警告訊息：

```
Warning: The DNS service route defined in the DNS proxy object
 is different from the DNS proxy rule’s service route. Using
 the DNS proxy object’s service route.
```

- 如果沒有服務路由定義在任何 DNS 伺服器設定檔中，則在需要時將會使用全域服務路由。

使用案例 3：防火牆作為用戶端與伺服器之間的 DNS Proxy

在此使用案例中，防火牆位於 DNS 用戶端與 DNS 伺服器之間。主機位於租用戶連接到防火牆介面的網路上，而防火牆上的 DNS Proxy 依設定作為這些主機的 DNS 伺服器。在這種情況下，防火牆會在其資料平面上執行 DNS 解析。



這種情況會發生在使用分割 *DNS* 時；在這種設定中，DNS Proxy 規則會設定成根據網域名稱比對將 DNS 要求重新導向至 DNS 伺服器。如果沒有相符項目，伺服器設定檔會確定要將要求傳送至哪些 DNS 伺服器，因此有兩種分割 DNS 解析方法。

在資料平面 *DNS* 解析中，從 *PAN-OS* 中的 *DNS Proxy* 到外部 *DNS* 伺服器的來源 *IP* 位址，將是 *Proxy* 的位址（原始要求的目的地 *IP*）。定義在 *DNS* 伺服器設定檔中的任何服務路由，都不會被使用。例如，如果要求從主機 *172.16.1.1* 傳至 *DNS Proxy*（位於 *192.168.1.1*），則傳至 *DNS* 伺服器（位於 *10.10.10.10*）的要求將會以 *192.168.1.1* 作為來源，並以 *10.10.10.10* 作為目的地。

STEP 1 | 選取 **Network**（網路） > **DNS Proxy**，然後按一下 **Add**（新增）。

STEP 2 | 按一下 **Enable**（啟用），然後輸入 DNS Proxy 的 **Name**（名稱）。

STEP 3 | 針對 **Location**（位置），選取租用戶的虛擬系統，在此範例中為 Corp1 Corporation (vsys6)。

STEP 4 | 針對 **Interface**（介面），選取將會從租用戶端主機接收 DNS 要求的介面，在此範例中為 Ethernet1/20。

STEP 5 | 選擇或建立 **Server Profile**（伺服器設定檔），以自訂用來為此租用戶解析 DNS 要求的 DNS 伺服器。

STEP 6 | 在 **DNS Proxy Rules**（**DNS Proxy** 規則）頁籤上，**Add**（新增）規則的 **Name**（名稱）。

STEP 7 | （選用）選取 **Turn on caching of domains resolved by this mapping**（開啟由此對應解析之網域的快取）。

STEP 8 | **Add**（新增）一個或多個 **Domain Name**（網域名稱），每列一個項目。DNS Proxy 規則與 FQDN 比對中介紹了防火牆如何比對 FQDN 與 DNS Proxy 規則中的網域名稱。

STEP 9 | 針對 **DNS** 伺服器設定檔，選取設定檔。防火牆會比較 DNS 要求中的網域名稱與 **DNS Proxy Rules**（**DNS Proxy** 規則）中定義的網域名稱。如果有相符項目，將會使用規則中定義的 **DNS Server profile**（**DNS** 伺服器設定檔）來決定 DNS 伺服器。

STEP 10 | 在此範例中，如果要求中的網域符合 myweb.corp1.com，則會使用在 myweb DNS 伺服器設定檔中定義的 DNS 伺服器。如果沒有相符項目，將會使用在 **Server Profile**（伺服器設定檔）（Corp1 DNS 伺服器設定檔）中定義的 DNS 伺服器。

STEP 11 | 按兩下 **OK**（確定）。

DNS Proxy 規則與 FQDN 比對

在為防火牆設定使用 DNS Proxy 規則的 DNS Proxy 物件時，防火牆將比較 DNS 查詢中的 FQDN 和 DNS Proxy 規則中的網域名稱。防火牆將按下列程序執行比較：

FQDN 與 DNS Proxy 規則的比較	範例
防火牆首先將 FQDN 和 DNS Proxy 規則中的網域名稱語彙基元化。在網域名稱中，由句點 (.) 分隔的字串為一個語彙基元。	***.boat.fish.com** 包含四個語彙基元：**[*] [boat][fish][com]**
比對過程實際上就是準確比對 FQDN 和規則中網域名稱的語彙基元；部分字串不會進行比對。	規則：**fishing** FQDN：**fish** — 不相符
準確比對要求的例外是使用萬用字元—星號 (*)。* 可以與一個或多個語彙基元相符。 這意味著僅由一個萬用字元 (*) 構成的規則可以使任何 FQDN 與一個或多個語彙基元相符。	規則：***.boat.com** FQDN：**www.boat.com** — 相符 FQDN：**www.blue.boat.com** — 相符 FQDN：**boat.com** — 不相符
	規則：***** FQDN：**boat** — 相符 FQDN：**www.boat.com** — 相符 FQDN：**www.boat.com** — 相符
您可以在任何位置使用 *：語彙基元前、語彙基元之間或語彙基元後（但單個語彙基元內不能有其他字元）。	規則：**www.*.com** FQDN：**www.boat.com** — 相符 FQDN：**www.blue.boat.com** — 相符
	規則：**www.*boat.*** FQDN：**www.boat.com** — 相符 FQDN：**www.boat.fish.com** — 相符
	規則：**www.boat*.com** — 無效
網域名稱中任何位置上可以有多個萬用字元 (*)：語彙基元前、語彙基元之間或語彙基元後。每一個不連續的 * 可以與一個或多個語彙基元相符。	規則：**a.*.d.*.com** FQDN：**a.b.d.e.com** — 相符 FQDN：**a.b.c.d.e.f.com** — 相符

FQDN 與 DNS Proxy 規則的比較	範例
	FQDN：**a.d.d.e.f.com** — 相符（第一個 ***** 與 **d** 相符；第二個 ***** 與 **e** 和 **f** 相符） FQDN：**a.d.e.f.com** — 不相符（第一個 ***** 與 **d** 相符；規則中的後一個 **d** 則沒有相符項）
在連續語彙基元中使用萬用字元時，第一個 * 可與一個或多個語彙基元相符；第二個 * 僅與一個語彙基元相符。 這意味著僅由 *.* 構成的規則可以使任何 FQDN 與兩個或多個語彙基元相符。	語彙基元前的連續萬用字元： 規則：　***.*.boat.com** FQDN：**www.blue.boat.com** — 相符 FQDN：**www.blue.sail.boat.com** — 相符
	語彙基元之間的連續萬用字元： 規則：　**www.*.*.boat.com** FQDN：**www.blue.sail.boat.com** — 相符 FQDN：**www.big.blue.sail.boat.com** — 相符
	語彙基元後的連續萬用字元： 規則：　**www.boat.*.*** FQDN：**www.boat.fish.com** — 相符 FQDN：**www.boat.fish.ocean.com** — 相符
	僅包含連續萬用字元： 規則：　*.* FQDN：**boat** — 不相符 FQDN：**www.boat.com** — 相符 FQDN：**www.boat.com** — 相符
同一規則中可以有連續和不連續的萬用字元。	規則：　**a.*.d.*.*.com** FQDN：**a.b.c.d.e.f.com** — 相符（第一個 ***** 與 **b** 和 **c** 相符；第二個 ***** 與 **e** 相符；第三個 ***** 與 **f** 相符） FQDN：**a.b.c.d.e.com** — 不相符（第一個 ***** 與 **b** 和 **c** 相符；第二個 ***** 與 **e** 相符；第三個 ***** 沒有相符項）
Implicit-tail-match 規則提供了額外的速記：	規則：　**www.boat.fish**

FQDN 與 DNS Proxy 規則的比較	範例
只要規則的最後一個語彙基元不是 *，如果規則中的所有語彙基元均與 FQDN 相符，則比較結果就相符，即使 FQDN 末尾有規則沒有的額外語彙基元。	FQDN：**www.boat.fish.com** — 相符 FQDN：**www.boat.fish.ocean.com** — 相符 FQDN：**www.boat.fish** — 相符
此規則結尾為 *，因此 Implicit-tail-match 規則不適用。* 的作用如前所述；可以與一個或多個語彙基元相符。	規則： **www.boat.fish.*** FQDN：**www.boat.fish.com** — 相符 FQDN：**www.boat.fish.ocean.com** — 相符 FQDN：**www.boat.fish** — 不相符（此 FQDN 沒有與規則中 * 相符的語彙基元。）
如果 FQDN 與多個規則相符，則均勢解除 (tie-breaking) 演算法將選取最具體（最長）的規則，也就是說，該演算法會優先選擇具有更多語彙基元和更少萬用字元 (*) 的規則。	規則 1： ***.fish.com** — 相符 規則 2： ***.com** — 相符 規則 3：**boat.fish.com** — 相符，優先選擇 FQDN：**boat.fish.com** FQDN 與所有三個規則均相符；防火牆將使用規則 3，因為它更具體。
	規則 1：***.fish.com** — 不相符 規則 2： ***.com** — 相符 規則 3：**boat.fish.com** — 不相符 FQDN：**fish.com** FQDN 與規則 1 不相符，因為 * 沒有相符的語彙基元。
	規則 1：***.fish.com** — 相符，優先選擇 規則 2： ***.com** — 相符 規則 3：**boat.fish.com** — 不相符 FQDN：**blue.boat.fish.com** FQDN 與規則 1 和規則 2 相符（因為 * 可與一個或多個語彙基元相符）。防火牆將使用規則 1，因為它更具體。
在處理萬用字元 (*) 和 Implicit-tail-match 規則時，可能出現 FQDN 與多個規則相符並且均勢解除演算法給予這些規則相等的權重。	將此 規則：**www.boat** 替換為：

FQDN 與 DNS Proxy 規則的比較	範例
為了避免歧義，如果帶有 Implicit-tail-match 或萬用字元 (*) 的規則可重疊，則可以透過指定末尾的語彙基元來取代 Implicit-tail-match 規則。	規則：**www.boat.com**
建立 DNS Proxy 規則以避免歧義和非預期結果的最佳做法	
在網域名稱中包含頂層網域，以避免叫用可能將 FQDN 與多個規則進行比對的 Implicit-tail-match。	**boat.com**
如果使用萬用字元 (*)，則僅將其用作最左側的語彙基元。 下列做法需要對萬用字元 DNS 記錄和 DNS 階層性質有基本的瞭解。	***.boat.com**
不要在規則中使用多個 *。	
使用 * 建立與 DNS 伺服器關聯的基本規則，使用具有多個語彙基元的規則為與不同伺服器關聯的規則建立例外。 均勢解除演算法將根據相符的語彙基元數，選擇最具體的相符規則。	規則：***.corporation.com** — DNS 伺服器 A 規則：**www.corporation.com** — DNS 伺服器 B 規則：***.internal.corporation.com** — DNS 伺服器 C 規則：**www.internal.corporation.com** — DNS 伺服器 D 規則：**mail.internal.corporation.com** — 與 DNS 伺服器 C 相符 FQDN：**mail.corporation.com** — 與 DNS 伺服器 A 相符

DDNS

瞭解動態 DNS (DDNS) 服務如何更新網域名稱至 IP 位址的對應以將準確的 IP 位址提供給 DNS 用戶端。

動態 DNS 概要

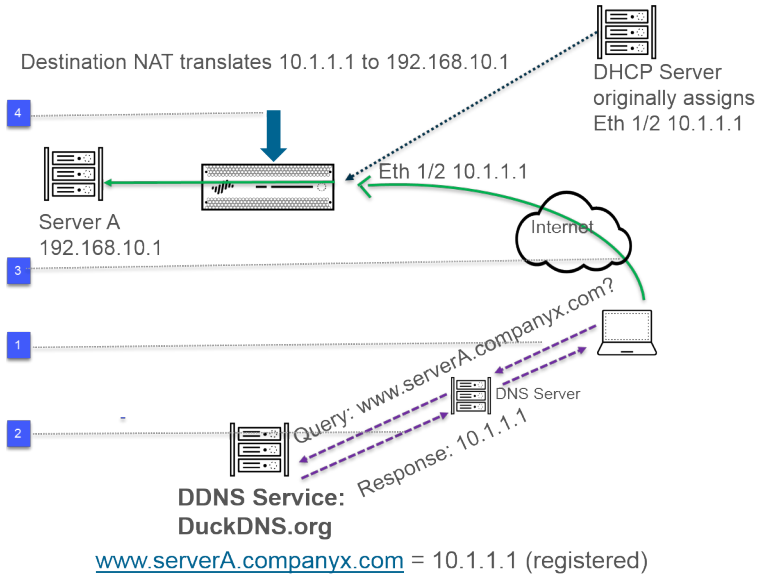
當您在防火牆背後託管服務並在防火牆上使用目的地 NAT 原則存取這些服務，或需要提供對防火牆的遠端存取時，可以在動態 DNS (DDNS) 服務供應商處為介面註冊 IPv4 位址變更（介面是接收動態位址的 DHCP 用戶端或具有靜態位址）或 IPv6 位址變更（僅限靜態位址）。DDNS 服務可以動態更新網域名稱到 IP 位址對應，以向 DNS 用戶端提供準確的 IP 位址，從而可以存取防火牆和防火牆背後的服務。DDNS 通常用於託管服務的分支部署。如果沒有對防火牆介面的 DDNS 支援，您將需要外部元件才能向用戶端提供準確的 IP 位址。

防火牆支援下列 DDNS 服務供應商：DuckDNS、DynDNS、FreeDNS Afraid.org Dynamic API、FreeDNS Afraid.org 及 No-IP。個別 DDNS 服務供應商可以確定其提供的服務，例如一個主機名稱支援多少個 IP 位址及其是否支援 IPv6 位址。Palo Alto Networks® 使用內容更新來新增新的 DDNS 服務供應商並提供服務更新。

對於高可用性 *(HA)* 組態，請確保 *HA* 防火牆對等體（主動/被動或主動/主動）上的內容版本同步，因為防火牆根據目前的 *Palo Alto Networks* 內容發佈版本維護 *DDNS* 組態。*Palo Alto Networks* 可以透過內容發佈變更或棄用現有 *DDNS* 服務。此外，*DDNS* 服務供應商可以變更其提供的服務。*HA* 對等體之間的內容發佈版本不符會影響其使用 *DDNS* 服務的能力。

防火牆不支援在作為乙太網路上點對點通訊協定 *(PPPoE)* 終止點的介面上使用 *DDNS*。

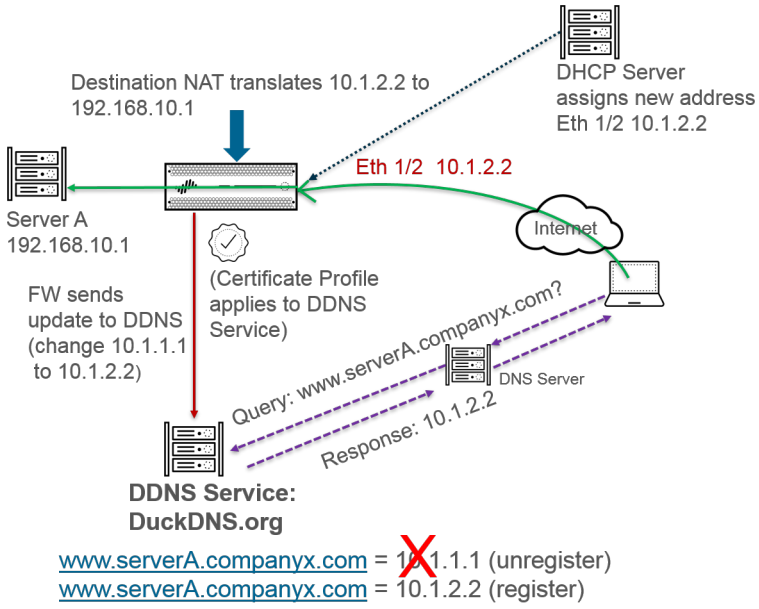
在以下範例中，防火牆是 DDNS 服務供應商的 DDNS 用戶端。最初，DHCP 伺服器為 Ethernet 1/2 介面指派的 IP 位址是 10.1.1.1。目的地 NAT 原則會將公共位址 10.1.1.1 轉譯為防火牆背後伺服器 A 的實際位址 (192.168.10.1)。



1. 當使用者嘗試聯絡 www.serverA.companyx.com 時，使用者會在其本機 DNS 伺服器上查詢 IP 位址。www.serverA.companyx.com（例如，設為 duckdns.org 記錄的 CNAME：serverA.companyx.duckdns.org）是屬於 DDNS 供應商（本例中為 DuckDNS）的網域。DNS 伺服器會向 DDNS 供應商確認該記錄以解析查詢。

2. DNS 伺服器將以 10.1.1.1 回應使用者，10.1.1.1 是 www.serverA.companyx.com 的 IP 位址。
3. 目的地位址為 10.1.1.1 的使用者封包將移至防火牆介面 Ethernet 1/2。
4. 在本範例中，防火牆在將封包傳送至目的地之前，先執行目的地 NAT 並將 10.1.1.1 轉譯為 192.168.10.1。

一段時間後，DHCP 會向防火牆介面指派新的 IP 位址，從而觸發 DDNS 更新，如下所示：



1. DHCP 伺服器為 Ethernet 1/2 指派新的 IP 位址 (10.1.2.2)。
2. 當防火牆收到新位址時，會傳送包含 www.serverA.companyx.com 新位址（DDNS 服務註冊）的 DDNS 服務更新。（防火牆還會根據所設定的更新時間間隔定期傳送更新。防火牆透過 HTTPS 連接埠 443 傳送 DDNS 更新。）

因此，下次用戶端在 DNS 伺服器上查詢 www.serverA.companyx.com 的 IP 位址且 DNS 伺服器檢查 DDNS 服務時，DDNS 服務將傳送已更新的位址 (10.1.2.2)。因此，使用者可以使用更新後的介面位址透過防火牆介面成功存取服務或應用程式。

如果防火牆已設為 *HA* 主動/被動模式，請注意，當兩個 *HA* 防火牆的狀態收斂時，防火牆會向 *DDNS* 服務傳送 *DDNS* 更新。*HA* 狀態收斂後，*DDNS* 會在被動防火牆上停用。例如，當兩個 *HA* 防火牆首次啟動時，兩個防火牆都會傳送 *DDNS* 更新，直至確定其處於 *HA* 主動還是被動模式。在此期間，您仍可在系統日誌中查看 *DDNS* 更新。*HA* 狀態收斂且各防火牆通知用戶端其處於主動還是被動模式後，被動防火牆將不再傳送 *DDNS* 更新。（在 *HA* 主動/主動模式下，各防火牆都具有獨立的 *DDNS* 組態且不會同步 *DDNS* 組態。）

為防火牆介面設定動態 DNS

在為防火牆介面設定 DDNS 之前：

- 確定您在 DDNS 供應商處註冊的主機名稱。
- 從 DDNS 服務取得公開 SSL 憑證並將其匯入防火牆。
- （如果您使用 FreeDNS Afraid.org v1 或 FreeDNS Afraid.org Dynamic API v1）在 DDNS 伺服器上，動態 DNS 服務頁籤包括以下選項：將同一 **IP** 的更新連結在一起嗎？當此選項啟用時，DDNS 服務將更新 DNS 記錄中包含變更中舊 IP 位址的所有主機名稱，而不僅僅是單一主機名稱與 IP 位址。若要避免更新您不打算更新的主機 DNS 記錄，您應停用 **Link updates of the same IP together?**（將同一 **IP** 的更新連結在一起嗎？）選項，以便 DDNS 伺服器僅更新包含具有 DDNS 更新中 IP 位址之特定主機名稱的 DNS 記錄。

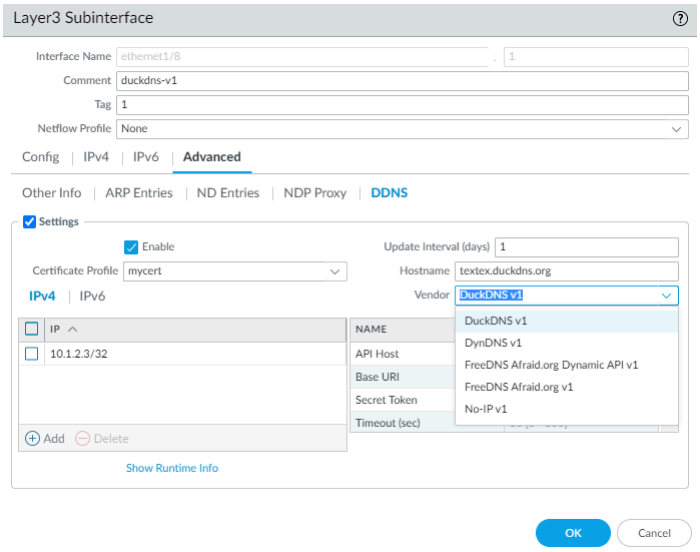
STEP 1 | 設定 DDNS。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取 Layer 3 介面、子介面或彙總乙太網路 (AE) 介面；或選取 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後選取介面或子介面。
2. 選取 **Advanced**（進階） > **DDNS**，然後選取 **Settings**（設定）。
3. **Enable**（啟用）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。）
4. 輸入防火牆傳送至 DDNS 服務的 **Update Interval (days)**（更新之間的間隔（以天數為單位）），以更新對應到 FQDN 的 IP 位址（預設值為 1；範圍為 1 到 30）。根據 IP 位址的變更頻率選擇時間間隔。（防火牆定期傳送的更新不包括防火牆在收到位址變更時傳送的更新。例如，定期傳送的更新可確保每次位址變更時傳送的更新不會遺失。）
5. 輸入在 DDNS 服務中註冊的介面的 **Hostname**（主機名稱）（例如，www.serverA.companyx.com 或 serverA）。

   確保此主機名稱與您在 *DDNS* 服務中註冊的主機名稱相符。您應輸入主機名稱的 *FQDN*；除了確認語法僅使用 *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。
6. 選取 **IPv4** 並選取一個或多個指派給介面的 IPv4 位址，或 **Add**（新增）IPv4 位址以與主機名稱相關聯（例如，10.1.1.1）。您最多只能選取 DDNS 服務允許的 IPv4 位址數量。所有選定的 IPv4 位址都會在 DDNS 服務中註冊。選取至少一個 IPv4 或一個 IPv6 位址。
7. 選取 **IPv6** 並選取一個或多個指派給介面的 IPv6 位址，或 **Add**（新增）IPv6 位址以與主機名稱相關聯。您最多只能選取 DDNS 服務允許的 IPv6 位址數量。所有選定的 IPv6 位址都會在 DDNS 服務中註冊。選取至少一個 IPv4 或一個 IPv6 位址。
8. 選取或使用從 DDNS 服務匯入的 SSL 憑證建立新的憑證設定檔（**Certificate Profile**（憑證設定檔）），以在防火牆第一次連線至 DDNS 服務以註冊 IP 位址及每次更新時驗證

DDNS 服務的 SSL 憑證。當防火牆連線至 DDNS 服務以傳送更新時，DDNS 服務會向防火牆提供由憑證授權單位 (CA) 發佈的 SSL 憑證，以便防火牆可以驗證 DDNS 服務。

9. 選取用於 DDNS 服務的 **Vendor**（廠商）（及版本號碼）。



Palo Alto Networks® 可能會透過內容更新變更支援的 *DDNS* 服務。

在「廠商」欄位中，*Palo Alto Network DDNS* 選擇是為 *Palo Alto Networks* 功能（如 *SD-WAN* 和 *ZTP*）保留的服務，不得選擇用於此當前工作。如果您在未啟用對應的支援功能時錯誤地選取 *Palo Alto Networks DDNS*，將會出現錯誤訊息。

10. 廠商選擇可確定廠商欄位下廠商特定的 **Name**（名稱）與 **Value**（值）欄位。某些值欄位是唯讀的，用於通知您防火牆用於連結 DDNS 服務的參數。設定其餘值欄位，例如 DDNS 服務向您提供的密碼，以及如果防火牆未從 DDNS 服務收到更新，防火牆使用的逾時。
11. 按一下 **OK**（確定）。

STEP 2 | （選用）如果您希望防火牆使用除管理介面以外的其他介面與 DDNS 服務通訊，請為 DDNS 設定服務路由（設定外部服務的網路存取權）。

STEP 3 | **Commit**（提交）您的變更。

STEP 4 | 檢視介面的 DDNS 資訊。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路） 或 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後選取您設定的介面。（DDNS 設定為顯示 DDNS 圖示的介面— —在功能欄位中。）
2. 選取 **Advanced**（進階） > **DDNS**，然後選取 **Settings**（設定）。
3. **Show Runtime Info**（顯示執行階段資訊）以查看介面的 DDNS 資訊，包括上次返回代碼（上次 FQDN 更新結果）和 DDNS 服務上次收到 FQDN 更新的時間（日期與時間）。

NAT

本節說明網路位址轉譯 (NAT) 及如何設定防火牆進行 NAT。您可使用 NAT 將非可路由的私人 IPv4 位址轉譯為一或多個可全域路由的 IPv4 位址，因此能保留組織的可路由 IP 位址。使用 NAT，可以在不洩露主機的真實 IP 位址的情況下讓主機存取公共位址並透過執行連接埠轉送來管理流量。您可使用 NAT 來解決網路設計挑戰，並讓網路具有可彼此通訊的相同 IP 子網路。防火牆支援在 Layer 3 和 Virtual Wire 介面上使用 NAT。

NAT64 選項會互譯 IPv6 與 IPv4 位址、使用不同的 IP 定址結構描述在網路之間提供連線，並因此提供用來 IPv6 定址的移轉路徑。IPv6 對 Ipv6（網路首碼轉譯） (NPTv6) 可將 IPv6 首碼轉譯為另一個 IPv6 首碼。PAN-OS 支援上述所有功能。

如果您在內部網路內使用私人 IP 位址，則必須使用 NAT 將私人位址轉譯為可在外部網路上路由的公共位址。在 PAN-OS 中，您可建立 NAT 原則規則來指示防火牆哪些封包位址和連接埠需要轉譯，以及轉譯後的位址和連接埠為何。

NAT 原則規則

NAT 原則概要介紹

您至少可以設定 NAT 規則來比對封包的來源區域與目的地區域。除了區域外，您還可以根據封包的目的地介面、來源與目的地位址，以及服務來設定比對準則。您可以設定多個 NAT 規則。防火牆會以從上到下的順序評估規則。一旦封包符合某一個 NAT 規則的準則，該封包便不受其他 NAT 規則的約束。因此，您的 NAT 規則清單順序應從最明確到最不明確，讓封包受到您所建立最明確的規則約束。

靜態 NAT 規則不會優先於其他形式的 NAT。因此，若要讓靜態 NAT 運作，靜態 NAT 規則必須在防火牆的清單中位於所有其他 NAT 規則之上。

NAT 規則提供位址轉譯，且不同於可允許或拒絕封包的安全性原則規則。瞭解防火牆套用 NAT 規則與安全性原則規則時的動向邏輯，讓您能夠根據您所定義的區域判斷所需的規則為何，此舉相當重要。您必須設定安全性原則來允許 NAT 流量。

在輸入時，防火牆會檢查封包，並進行路由查閱，以判斷輸出介面與區域。接著，防火牆會根據來源及/或目的地區域，判斷封包是否符合任何已定義的 NAT 規則。然後不是根據後續 NAT 區域，而是根據原始 (預先 NAT) 來源和目的地位址進行評估，並套用符合封包的所有安全性原則。最後在輸出時，為了比對 NAT 規則，防火牆會轉譯來源和/或目的地位址及連接埠號碼。

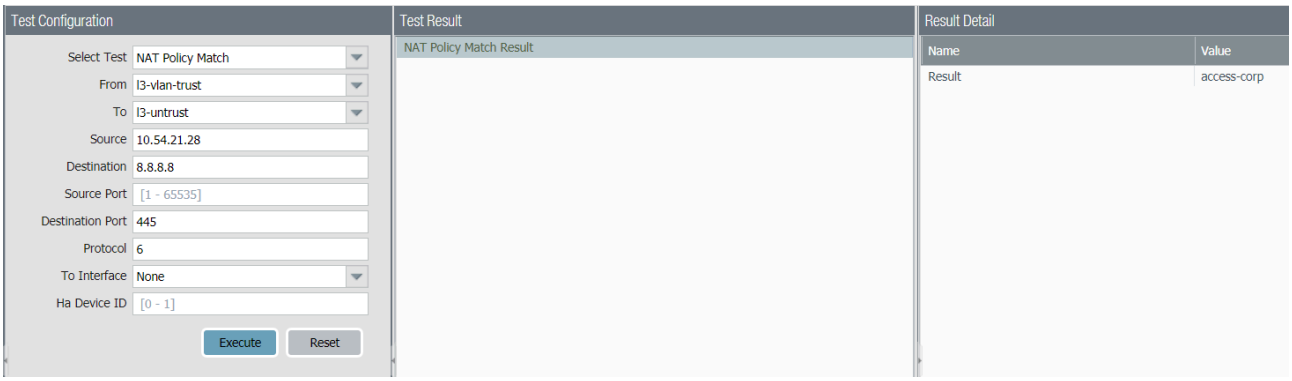
請記住，在封包離開防火牆之前，不會轉譯 IP 位址與連接埠。NAT 規則與安全性原則會套用到原始 IP 位址 (預先 NAT 位址)。系統會根據與預先 NAT IP 位址相關聯的區域設定 NAT 規則。

安全性原則與 NAT 規則不同，因為安全性原則會檢查後續 NAT 區域來判斷是否允許封包。由於 NAT 的特性就是修改來源或目的地 IP 位址，會造成修改封包的傳出介面與區域，因此會在後續 NAT 區域上強制執行安全性原則。

SIP 呼叫在通過防火牆時有時會出現單向音訊，因為呼叫管理員會代表電話傳送一則建立連線的 *SIP* 訊息。當來自呼叫管理員的訊息到達防火牆時，*SIP ALG* 必須讓電話的 *IP* 位址接通 *NAT*。如果呼叫管理員和電話不處在相同的安全性區域，會使用呼叫管理員區域對電話的 *IP* 位址完成 *NAT* 查閱。*NAT* 原則應將此考慮在內。

會將無 NAT 規則設定為允許排除在 NAT 規則（稍後在 NAT 原則中定義）範圍內定義的 IP 位址。若要定義無 NAT 原則，請指定所有相符條件，然後在來源轉譯欄中選取無來源轉譯。

您可以透過選取 **Device**（裝置） > **Troubleshooting**（疑難排解） 並測試流量是否符合 NAT 規則，來驗證經過處理的 NAT 規則。例如：



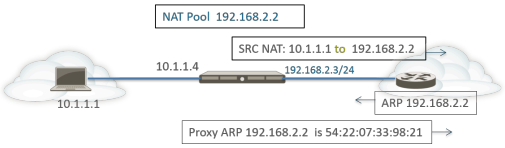
識別為位址物件的 NAT 位址配發範圍

在 NAT 原則規則中設定 **Dynamic IP**（動態 **IP**）或 **Dynamic IP and Port**（動態 **IP** 與連接埠）NAT 位址配發範圍時，通常會透過位址物件設定轉譯位址的配發範圍。每個位址物件可以是主機 IP 位址、IP 位址範圍或 IP 子網路。

由於 *NAT* 規則與安全性原則規則皆使用位址物件，因此要區分兩者的最佳做法就是將用於 *NAT* 的位址物件名稱前加上首碼，例如「*NAT-name*」。

NAT 位址配發範圍的 Proxy ARP

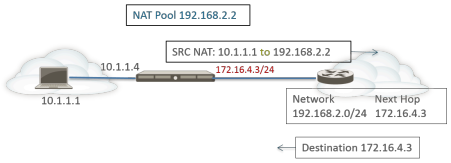
NAT 位址配發範圍不會繫結至任何介面。下圖說明防火牆在 NAT 位址配發範圍中，針對位址執行 Proxy ARP 時的行為。



防火牆會執行用戶端的來源 NAT，並將來源位址 10.1.1.1 轉譯為 NAT 集區中的位址 192.168.2.2。系統會將轉譯的封包傳送至路由器。

針對傳回流量，路由器不瞭解如何到達 192.168.2.2（因此 IP 位址只是 NAT 位址集區中的位址），因此其會將 ARP 請求封包傳送至防火牆。

- 如果位址配發範圍 (192.168.2.2) 與輸出/輸入介面 IP 位址 (192.168.2.3/24) 位於相同的子網路，防火牆可以將 Proxy ARP 回覆傳送至路由器，並表示 IP 位址的 Layer 2 MAC 位址，如上圖所示。
- 如果位址配發範圍 (192.168.2.2) 不是防火牆上介面的子網路，防火牆便不會將 Proxy ARP 回覆傳送至路由器。這表示您必須以必要的路由設定路由器以瞭解要將針對 192.168.2.2 指定的封包傳送至何處，從而確保將傳回流量路由回防火牆，如下圖所示。



來源 NAT 與目的地 NAT

防火牆支援來源位址及/或連接埠轉譯和目的地位址及/或連接埠轉譯。

- 來源 NAT
- 目的地 NAT

來源 NAT

來源 NAT 通常由內部使用者用於存取網際網路，來源位址會經過轉譯，因此能保持隱私。來源 NAT 有三種類型：

- 動態 **IP** 與連接埠 **(DIPP)**—允許多個主機讓其來源 IP 位址轉譯為同一個公共 IP 位址，但連接埠號碼不同。動態轉譯是針對 NAT 位址配發範圍中下一個可用的位址，您可以將其設定為 IP 位址的 **Translated Address**（轉譯的位址） 配發範圍、位址範圍、子網路或這些項目的組合。

  DIPP 是 NAT 位址集區中下一個可用位址的替代項目，可讓您指定 **Interface**（介面）本身的位址。在 NAT 規則中指定介面的優點是，NAT 規則將自動更新，以使用介面之後取得的任何位址。DIPP 有時候也稱為以介面為基礎的 NAT 或網路位址連接埠轉譯 (NAPT)。

  DIPP 具有預設的 NAT 過度訂閱比例，亦即同時使用同一個已轉譯 IP 位址與連接埠配對的次數。如需詳細資訊，請參閱 動態 IP 與連接埠 NAT 過度訂閱 與 修改 DIPP NAT 的過度訂閱比例。

  （僅影響不使用第二代 *PA-7050-SMC-B* 或 *PA-7080-SMC-B* 交換器管理卡的 *PA-7000* 系列防火牆）當您將點對點通道通訊協定 *(PPTP)* 與 *DIPP NAT* 一起使用時，防火牆僅限於僅對一個連線使用轉譯的 *IP* 位址-連接埠對；防火牆不支援 *DIPP NAT*。權宜方案是將 *PA-7000* 系列防火牆升級到第二代 *SMC-B* 卡。

- 動態 **IP**—允許僅將來源 IP 位址（無連接埠號碼）一對一的動態轉譯為 NAT 位址集區中的下一個可用位址。NAT 配發範圍的大小應該等於需要位址轉譯的內部主機數。依預設，如果來源位址配發範圍大於 NAT 位址配發範圍，且最後所有的 NAT 位址皆已配置，則會丟棄需要位址轉譯的新連線。若要取代此預設行為，請使用 **Advanced (Dynamic IP/Port Fallback)**（進階（動態 **IP/**連接埠回復）），以在必要時啟用 DIPP 位址。在上述任何一個狀況下，當工作階段終止且集區中的位址可供使用時，系統便會配置位址，以轉譯新的連線。

  動態 IP NAT 支援可讓您保留動態 IP NAT 位址的選項。

- 靜態 **IP**—允許將來源 IP 位址 1 對 1 的靜態轉譯，但來源連接埠保持不變。靜態 IP 轉譯的常見案例就是必須可供網際網路使用的內部伺服器。

目的地 NAT

當防火牆將目的地位址轉譯為其他目的地位址時，系統會對傳入封包執行目的地 NAT；例如，防火牆將公共目的地位址轉譯為私人目的地位址。目的地 NAT 還提供了相應選項來執行連接埠轉送或連接埠轉譯。

目的地 NAT 允許靜態與動態轉譯：

- 靜態 **IP**—您可透過多種形式設定一對一的靜態轉譯。您可以指定原始封包具有單一目的地 IP 位址、IP 位址範圍或 IP 網路遮罩，只要轉譯的封包格式相同並指定了相同數量的 IP 位址。防火

牆每次都會將原始目的地位址靜態轉譯成相同轉譯目的地位址。也就是說，如果有多個目的地位址，防火牆會一直使用相同的轉譯方式，將為原始封包設定的第一個目的地位址轉譯成為轉譯封包設定的第一個目的地位址，然後將所設定的第二個原始目的地位址轉譯成所設定的第二個轉譯目的地位址，依此類推。

如果您使用目的地 NAT 轉譯靜態 IPv4 位址，也可以使用防火牆一側的 DNS 服務解析另一側上用戶端的 FQDN。當包含 IPv4 位址的 DNS 回應周遊防火牆時，DNS 伺服器會向外部裝置提供內部 IP 位址，或向內部裝置提供外部 IP 位址。從 PAN-OS 9.0.2 開始及在更新的 9.0 版本中，您可設定防火牆以在 DNS 回應（與規則相符）中重寫 IP 位址，以便用戶端接收用於存取目的地服務的合適位址。適用的 DNS 重寫使用案例幫助您確定如何設定此類重寫。

- 動態 **IP**（採用工作階段散佈）—目的地 NAT 允許您將原始目的地位址轉譯為擁有動態 IP 位址的目的地主機或伺服器，表示使用 FQDN 的位址物件，其可從 DNS 返回多個位址。動態 IP（採用工作階段散佈）僅支援 IPv4 位址。使用動態 IP 位址的目的地 NAT，在使用動態 IP 定址的雲端部署中特別有用。

  如果轉譯目的地位址解析為多個位址，防火牆將在多個位址中散佈傳入 NAT 工作階段，以改善工作階段散佈。散佈方法如下：循環配置（預設方法）、來源 IP 雜湊、IP 模數、IP 雜湊或最少工作階段。如果 DNS 伺服器為 FQDN 傳回的 IPv4 位址數超過 32 個，則防火牆會使用封包中的前 32 個位址。

  如果已解譯位址是類型為 *FQDN* 的位址物件，僅可解析為 *IPv6* 位址，則目的地 *NAT* 原則規則會將 *FQDN* 視為未解析。

  使用 **Dynamic IP (with session distribution)**（動態 **IP**（採用工作階段散佈）），可將多個 NAT 前目的地 IP 位址 *M* 轉譯為多個 NAT 後目的地 IP 位址 *N*。此種情況下，可使用單一 NAT 規則執行 *M* x *N* 目的地 NAT 轉譯，實現多對多轉譯方式。

對於目的地 *NAT*，最佳做法為：

- 對靜態 *IP* 位址使用 ***Static IP***（靜態 ***IP***）位址轉譯，此允許防火牆檢查並確保原始目的地位址的數量等於轉譯目的地位址的數量。
- 僅對基於 *FQDN* 的動態位址（防火牆不會對 *IP* 位址執行數目檢查）使用動態 ***IP***（採用工作階段散佈）位址轉譯。

以下為防火牆允許的目的地 NAT 轉譯的常見範例：

轉譯類型	原始封包的目的地位址	對應到轉譯封包的目的地位址	附註
靜態 **IP**	192.168.1.1	2.2.2.2	原始封包和轉譯封包各自有一個可能的目的地位址。
	192.168.1.1-192.168.1.4	2.2.2.1-2.2.2.4	原始封包和轉譯封包各自有四個可能的目的地位址。 192.168.1.1 一直對應至 2.2.2.1

轉譯類型	原始封包的目的地位址	對應到轉譯封包的目的地位址	附註
			192.168.1.2 一直對應至 2.2.2.2 192.168.1.3 一直對應至 2.2.2.3 192.168.1.4 一直對應至 2.2.2.4
	192.168.1.1/30	2.2.2.1/30	原始封包和轉譯封包各自有四個可能的目的地位址。 192.168.1.1 一直對應至 2.2.2.1 192.168.1.2 一直對應至 2.2.2.2 192.168.1.3 一直對應至 2.2.2.3 192.168.1.4 一直對應至 2.2.2.4
動態 **IP**（採用工作階段散佈）	192.168.1.1/30	domainname.com	原始封包有四個目的地位址，若（打個比方）轉譯目的地位址中的 FQDN 解析成五個 IP 位址，則單一 NAT 規則中可能有 20 個目的地 NAT 轉譯。

目的地 NAT 常見的用途就是設定數個 NAT 規則，這些規則會將單一公共目的地位址對應至數個指派給伺服器或服務的私人目的地主機位址。在此狀況下，目的地連接埠號碼會用於識別目的地主機。例如：

- 連接埠轉送—可將公共目的地位址與連接埠號碼轉譯為私人目的地位址，但保持相同的連接埠號碼。
- 連接埠轉譯—可將公共目的地位址與連接埠號碼轉譯為私人目的地位址及不同的連接埠號碼，因此能將實際的連接埠號碼保持隱私。在 NAT 原則規則的 **Translated Packet**（轉譯的封包）頁籤上輸入 **Translated Port**（轉譯連接埠），即可設定連接埠轉譯。請參閱具有連接埠轉譯範例的目的地 NAT。

使用 DNS 重寫設定目的地 NAT 使用案例

當您使用目的地 NAT 執行從一個 IPv4 位址到另一個 IPv4 位址的靜態轉譯時，還可以使用防火牆一側的 DNS 服務解析用戶端的 FQDN。當包含 IP 位址的 DNS 回應周遊防火牆以移至用戶端時，

防火牆不會對該 IP 位址執行 NAT，因此 DNS 伺服器會向外部裝置提供內部 IP 位址，或向內部裝置提供外部 IP 位址，DNS 用戶端因而無法連線至目的地服務。

要避免該問題，您可根據為 NAT 原則規則設定的轉譯 IP 位址，設定防火牆以在 DNS 回應中重寫 IP 位址（來自 A 記錄）。在將回應轉送至用戶端之前，防火牆會在 DNS 回應中對 IPv4 位址（FQDN 解析）執行 NAT；因此，用戶端可以接收用於存取目的地服務的合適位址。單一 NAT 原則規則會使防火牆對與規則相符的封包執行 NAT，還會使防火牆在 DNS 回應中對與規則中之原始目的地位址或轉譯目的地位址相符的 IP 位址執行 NAT。

DNS 重寫發生在全域層級；防火牆會將「原始封包」頁簽上的「目的地位址」對應到「轉譯後封包」頁簽上的「目的地位址」。「原始封包」頁簽上的所有其他欄位將被忽略。當 DNS 回應封包到達時，防火牆會根據方向檢查回應是否包含與對應的目的地位址之一相符的任何 A 記錄，如下所示。

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：**reverse**（反向） 或 **forward**（正向）：

- **reverse**（反向）—如果 DNS 回應與規則中的轉譯目的地位址相符，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 IP 位址 **1.1.1.10** 轉譯為 **192.168.1.10**，則防火牆會將 DNS 回應 **192.168.1.10** 重寫為 **1.1.1.10**。
- **forward**（正向）—如果 DNS 回應與規則中的原始目的地位址相符，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 IP 位址 **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**。

如果您有停用了 *DNS* 重寫的重疊 *NAT* 規則，且其下方的 *NAT* 規則啟用了 *DNS* 重寫並包含在重疊中，則防火牆會根據重疊的 *NAT* 規則重寫 *DNS* 回應（採用 ***reverse***（反向）或 ***forward***（正向）設定）。重寫優先，忽略 *NAT* 規則的順序。

請參閱設定 DNS 重寫的使用案例：

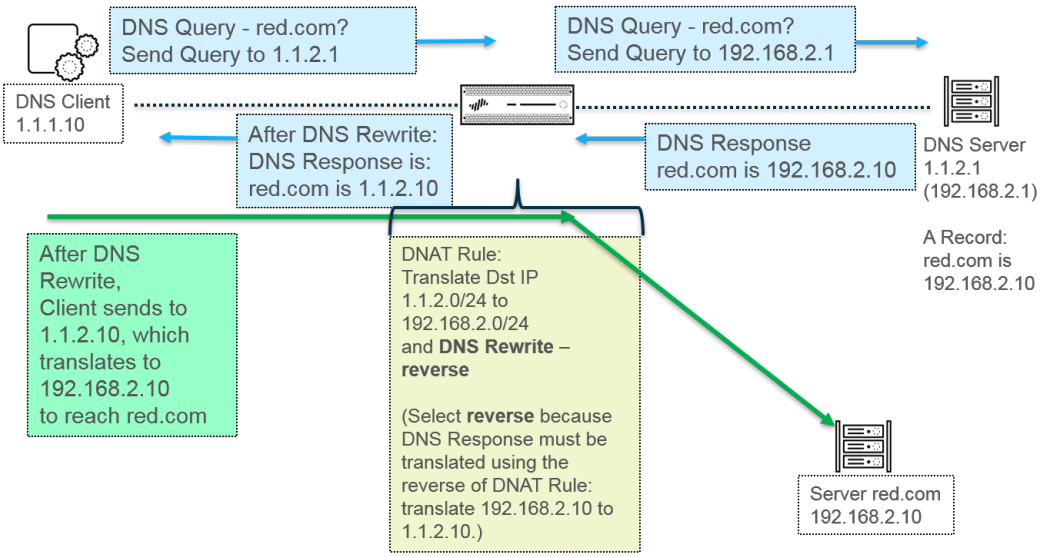
- 使用 DNS 反向重寫設定目的地 NAT 使用案例
- 使用 DNS 正向重寫設定目的地 NAT 使用案例

使用 DNS 反向重寫設定目的地 NAT 使用案例

以下使用案例說明了以 **reverse**（反向）啟用 DNS 重寫的目的地 NAT。這兩個使用案例的不同之處在於，DNS 用戶端、DNS 伺服器及目的地伺服器是位於防火牆的公共端還是內部端。無論哪種情況，DNS 用戶端都與其最終目的地伺服器位於防火牆不同端。（如果 DNS 用戶端與其最終目的地伺服器位於防火牆的相同端，請考慮使用 DNS 正向重寫設定目的地 NAT 使用案例 3 與 4。）

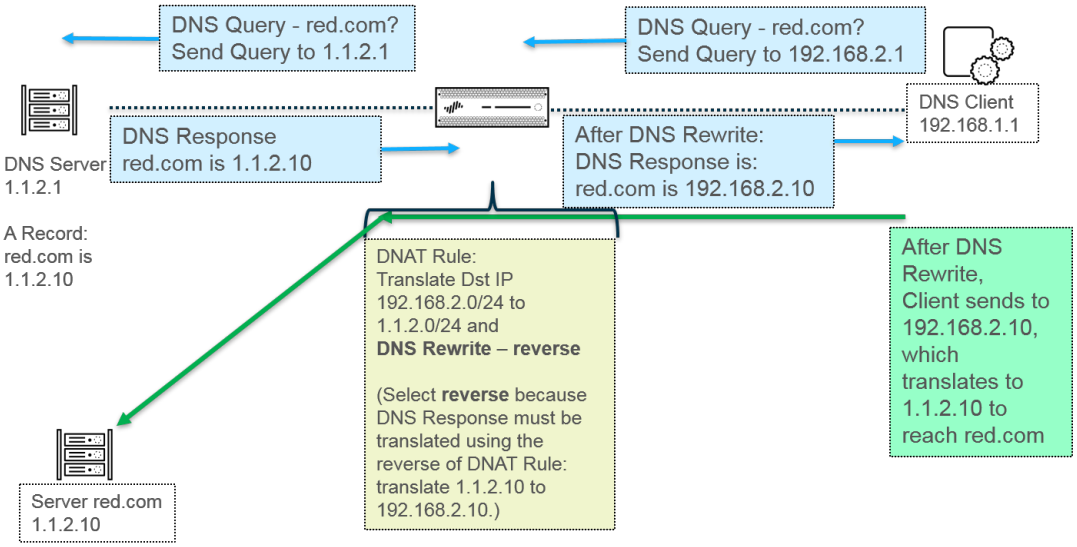
使用案例 1 說明了 DNS 用戶端位於防火牆公共端，而 DNS 伺服器與最終目的地伺服器均位於內部端的情況。本案例要求以反向執行 DNS 重寫。DNS 用戶端查詢 red.com 的 IP 位址。根據 NAT 規則，防火牆會將查詢轉譯（最初移至公共位址 1.1.2.1）為內部位址 192.168.2.1。DNS 伺服器回應，red.com 具有 IP 位址 192.168.2.10。規則包括啟用 **DNS** 重寫 **-** 反向且 DNS 回應 192.168.2.10 與規則中的目的地轉譯位址 192.168.2.0/24 相符，因此防火牆會使用與規則 **reverse**（相反）的轉譯對 DNS 回應進行轉譯。規則顯示，將 1.1.2.0/24 轉譯為 192.168.2.0/24，因此防火牆會將 DNS 回應 192.168.2.10 重寫為 1.1.2.10。DNS 用戶端會接收回應並傳送至 1.1.2.10，規則會將其轉譯為 192.168.2.10 以連線伺服器 red.com。

使用案例 1 摘要：DNS 用戶端與目的地伺服器位於防火牆不同端。DNS 伺服器提供與 NAT 規則中的轉譯目的地位址相符的位址，因此會使用與 NAT 規則 **reverse**（相反）轉譯對 DNS 回應進行轉譯。



使用案例 2 說明了 DNS 用戶端位於防火牆內部端，而 DNS 伺服器與最終目的地伺服器均位於公共端的情況。本案例要求以反向執行 DNS 重寫。DNS 用戶端查詢 red.com 的 IP 位址。根據 NAT 規則，防火牆會將查詢轉譯（最初移至內部位址 192.168.2.1）為公共位址 1.1.2.1。DNS 伺服器回應，red.com 具有 IP 位址 1.1.2.10。規則包括啟用 **DNS** 重寫 **-** 反向且 DNS 回應 1.1.2.10 與規則中的目的地轉譯位址 1.1.2.0/24 相符，因此防火牆會使用與規則 **reverse**（相反）的轉譯對 DNS 回應進行轉譯。規則顯示，將 192.168.2.0/24 轉譯為 1.1.2.0/24，因此防火牆會將 DNS 回應 1.1.2.10 重寫為 192.168.2.10。DNS 用戶端會接收回應並傳送至 192.168.2.10，規則會將其轉譯為 1.1.2.10 以連線伺服器 red.com。

使用案例 2 摘要與使用案例 1 摘要相同：DNS 用戶端與目的地伺服器位於防火牆不同端。DNS 伺服器提供與 NAT 規則中的轉譯目的地位址相符的位址，因此會使用與 NAT 規則 **reverse**（相反）轉譯對 DNS 回應進行轉譯。



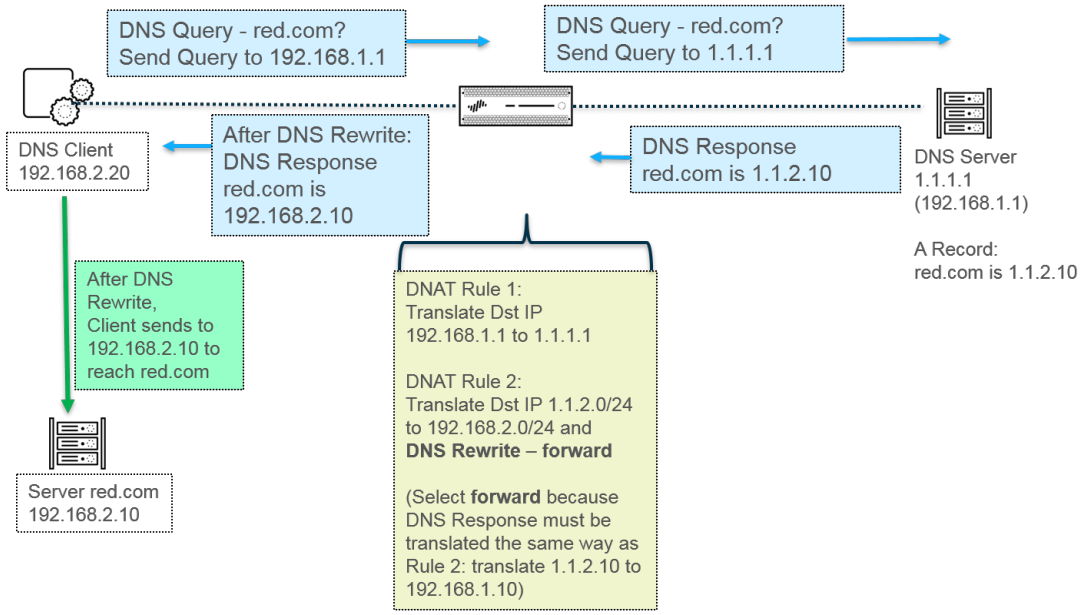
若要實作 DNS 重寫，使用 DNS 重寫設定目的地 NAT。

使用 DNS 正向重寫設定目的地 NAT 使用案例

以下使用案例說明了以 **forward**（正向）啟用 DNS 重寫的目的地 NAT。這兩個使用案例的不同之處在於，DNS 用戶端、DNS 伺服器及目的地伺服器是位於防火牆的公共端還是內部端。無論哪種情況，DNS 用戶端都與其最終目的地伺服器位於防火牆同一端。（如果 DNS 用戶端與其最終目的地伺服器位於防火牆的不同端，請考慮使用 DNS 反向重寫設定目的地 NAT 使用案例 1 與 2。）

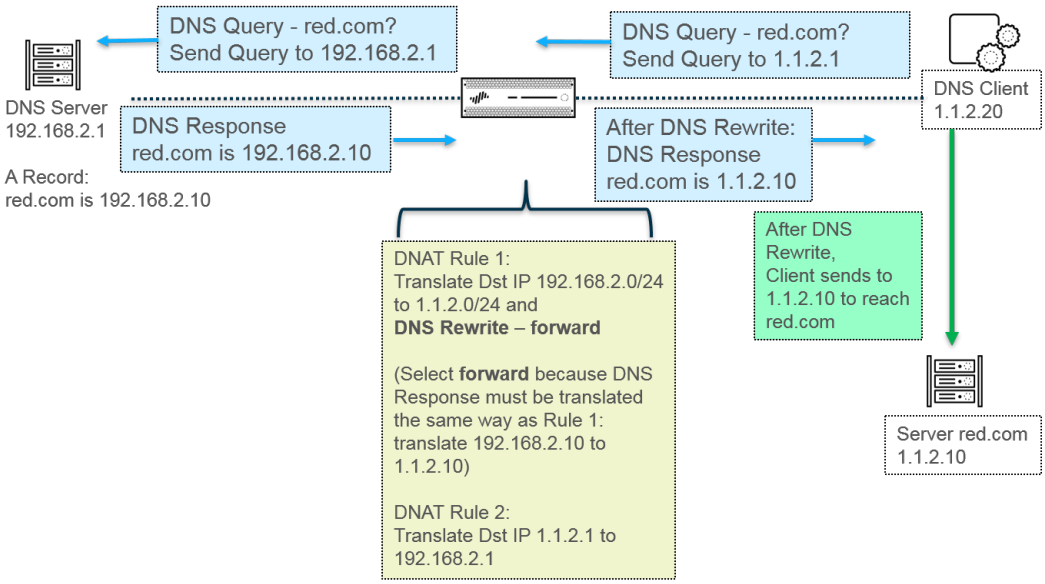
使用案例 3 說明了 DNS 用戶端與最終目的地伺服器均位於防火牆內部端，而 DNS 伺服器位於公共端的情況。本案例要求以正向執行 DNS 重寫。DNS 用戶端查詢 red.com 的 IP 位址。根據規則 1，防火牆會將查詢轉譯（最初移至內部位址 192.168.1.1）為 1.1.1.1。DNS 伺服器回應，red.com 具有 IP 位址 1.1.2.10。規則 2 包括啟用 **DNS** 重寫 - 正向且 DNS 回應 1.1.2.10 與規則 2 中的原始目的地位址 1.1.2.0/24 相符，因此防火牆會使用與規則相同的轉譯對 DNS 回應進行轉譯。規則 2 顯示，將 1.1.2.0/24 轉譯為 192.168.2.0/24，因此防火牆會將 DNS 回應 1.1.2.10 重寫為 192.168.2.10。DNS 用戶端會接收回應並傳送至 192.168.2.10 以連線伺服器 red.com。

使用案例 3 摘要：DNS 用戶端與目的地伺服器位於防火牆同一端。DNS 伺服器提供與 NAT 規則中的原始目的地位址相符的位址，因此會使用與 NAT 規則相同的（**forward**（正向））轉譯對 DNS 回應進行轉譯。



使用案例 4 說明了 DNS 用戶端與最終目的地伺服器均位於防火牆公共端，而 DNS 伺服器位於內部端的情況。本案例要求以正向執行 DNS 重寫。DNS 用戶端查詢 red.com 的 IP 位址。根據規則 2，防火牆會將查詢轉譯（最初移至公共目的地 1.1.2.1）為 192.168.2.1。DNS 伺服器回應，red.com 具有 IP 位址 192.168.2.10。規則 1 包括 啟用 **DNS** 重寫 - 正向 且 DNS 回應 192.168.2.10 與規則 1 中的原始目的地位址 192.168.2.0/24 相符，因此防火牆會使用與規則 相同 的轉譯對 DNS 回應進行轉譯。規則 1 顯示，將 192.168.2.0/24 轉譯為 1.1.2.0/24，因此防火牆會將 DNS 回應 1.1.2.10 重寫為 192.168.2.10。DNS 用戶端會接收回應並傳送至 1.1.2.10 以連線伺服器 red.com。

使用案例 4 摘要與使用案例 3 摘要相同：DNS 用戶端與目的地伺服器位於防火牆同一端。DNS 伺服器提供與 NAT 規則中的原始目的地位址相符的位址，因此會使用與 NAT 規則相同的（**forward**（正向））轉譯對 DNS 回應進行轉譯。



若要實作 DNS 重寫，使用 DNS 重寫設定目的地 NAT。

NAT 規則容量

所允許的 NAT 規則數目視乎防火牆型號。可針對靜態、動態 IP (DIP) 及動態 IP 與連接埠 (DIPP) NAT 設定個別的規則限制。用於這些 NAT 類型的規則數目總和不能超過總 NAT 規則容量。對於 DIPP，規則限制是根據防火牆的超額授權設定（8、4、2 或 1）而定，並假設每個規則有一個已轉譯的 IP 位址。若要瞭解各型號特定的 NAT 規則限制與轉譯的 IP 位址限制，請使用比較防火牆工具。

使用 NAT 規則時請考慮下列事項：

- 如果您已用盡集區資源，即使尚未到達型號允許的規則數目上限，也無法再建立 NAT 規則。
- 如果您合併 NAT 規則，記錄與報告也會合併。系統會依規則提供統計資料，而非依規則內的所有位址提供。如果您需要精確的記錄與報告，請不要結合規則。

動態 IP 與連接埠 NAT 過度訂閱

動態 IP 與連接埠 (DIPP) NAT 可讓您在同時工作階段內使用每個轉譯的 IP 位址與連接埠配對數次 (8、4 或 2 次)。這種可重複使用 IP 位址與連接埠的能力 (也就是所謂的過度訂閱) 讓公共 IP 位址極少的客戶有擴充的能力。這種設計是基於假設主機連線到不同的目的地，因此系統會唯一地識別工作階段，衝突是不可能發生的。過度訂閱比例事實上是位址/連接埠集區原始大小的 8、4 或 2 倍。例如，若允許的同時工作階段預設限制為 64K，則乘以 8 倍的過度訂閱，結果為允許 512K 的同時工作階段。

所允許的過度訂閱比例會視型號而異。超額授權比例是全域性的，會套用到防火牆上。此過度訂閱比例預設為已設定，即使您有足夠的公共 IP 位址而無須過度訂閱，仍會耗用記憶體。您可以將預設設定的比例降低，甚至可降到 1 (這表示沒有過度訂閱)。透過超額授權，您可以減少來源裝置轉譯次數，但會增加 DIP 與 DIPP NAT 規則容量。若要變更預設比例，請參閱修改 DIPP NAT 的過度訂閱比例。

如果您選取 **Platform Default**（平台預設），則超額授權的明確設定會關閉，並套用特定型號的預設超額授權比例，如下表所示。**Platform Default**（平台預設）設定允許升級或降級軟體版本。

下表列出了每個型號的預設（最高）過度訂閱比例。

Model	預設過度訂閱比例
PA-220	2
PA-820	2
PA-850	2
PA-3220	4
PA-3250	4
PA-3260	4
PA-5220	8
PA-5250	8
PA-5260	8
PA-5280	8
PA-7050	8
PA-7080	8
VM-50	2

Model	預設過度訂閱比例
VM-100	2
VM-200	2
VM-300	2
VM-500	8
VM-700	8
VM-1000-HV	2

防火牆最多支援每個 NAT 規則 256 個轉譯 IP 位址，且每個型號支援最大數量的轉譯 IP 位址（針對結合的所有 NAT 規則）。如果超額授權造成超過每個規則的轉譯位址上限 (256 個)，則防火牆將自動減少超額授權比例，盡力讓提交成功。但如果您的 NAT 規則造成轉譯超過型號的轉譯位址上限，則提交將會失敗。

資料平面 NAT 記憶體統計資料

show running global-ippool 命令會顯示與集區的 NAT 記憶體耗用量相關的統計資料。大小欄顯示資源集區正在使用的記憶體位元組數。[比例] 欄顯示超額授權比例 (僅適用於 DIPP 配發範圍)。以下範例輸出說明集區與記憶體統計資料:

```
admin@PA-7050-HA-0 (active-primary)> show running global-ippool

Idx  Type          From                      To           Num   Ref.Cnt   Size     Ratio
1    Dynamic IP    201.0.0.0-201.0.255.255   210.0.0.0    4096  2         657072   N/A
2    Dynamic IP    202.0.0.0-202.0.0.255     220.0.0.0    256   1         41232    N/A
3    Dynamic IP/Port 200.0.2.100-200.0.2.100 200.0.3.11   1     1         68720    8

Usable NAT DIP/DIPP shared memory size: 58490064      ← Total physical NAT memory (bytes)
Used NAT DIP/DIPP shared memory size: 767024 (1.3%)   ← Bytes and % of usable NAT memory
Dynamic IP NAT Pool: 2 (1.19%)        ← Number of DIP pools in use and % of total usable memory that all DIP pools use
Dynamic IP/Port NAT Pool: 1 (0.12%)   ← Number of DIPP pools in use and % of total usable memory that all DIPP pools use
```

對於虛擬系統的 NAT 配發統計資料，**show running ippool** 命令會顯示數欄表示各 NAT 規則使用的記憶體大小與使用的超額授權比例 (針對 DIPP 規則)。以下為此命令的範例輸出。

```
admin@PA-7050-HA-0 vsys1 (active-primary)> show running ippool

VSYS 1 has 4 NAT rules, DIP and DIPP rules:
Rule        Type          Used   Available   Mem Size   Ratio
----------  ------------  -----  ----------  ---------  -------
nat1        Dynamic IP    0      4096        788144     0
nat2        Dynamic IP    0      256         49424      0
nat3        Dynamic IP/Port 0    638976      100976     4
nat11       Dynamic IP    0      4096        788144     0
```

show running nat-rule-ippool rule 命令輸出的欄位中顯示各 NAT 規則使用的記憶體 (位元組)。下列為命令的範例輸出，及所圈出規則的記憶體使用量。

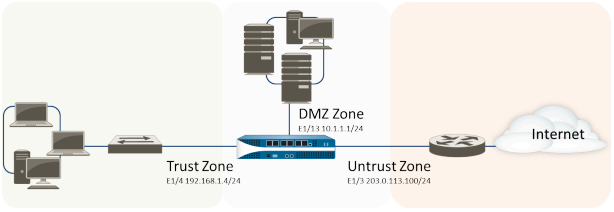
```
admin@PA-7050-HA-0 (active-primary)> show running nat-rule-ippool rule nat1

VSYS 1 Rule nat1:
Rule: nat1, Pool index: 1,  memory usage: 788144
------------------------------------------------
Reserve IP: no
201.0.0.0-201.0.255.255  =>
          210.0.0.0-210.0.15.255

Source          Xlat-Source     Ref.Cnt (F)     TTL(s)

Total IPs in use: 0
Total entries in time-reserve cache: 0
Total freelist left: 4096
```

設定 NAT

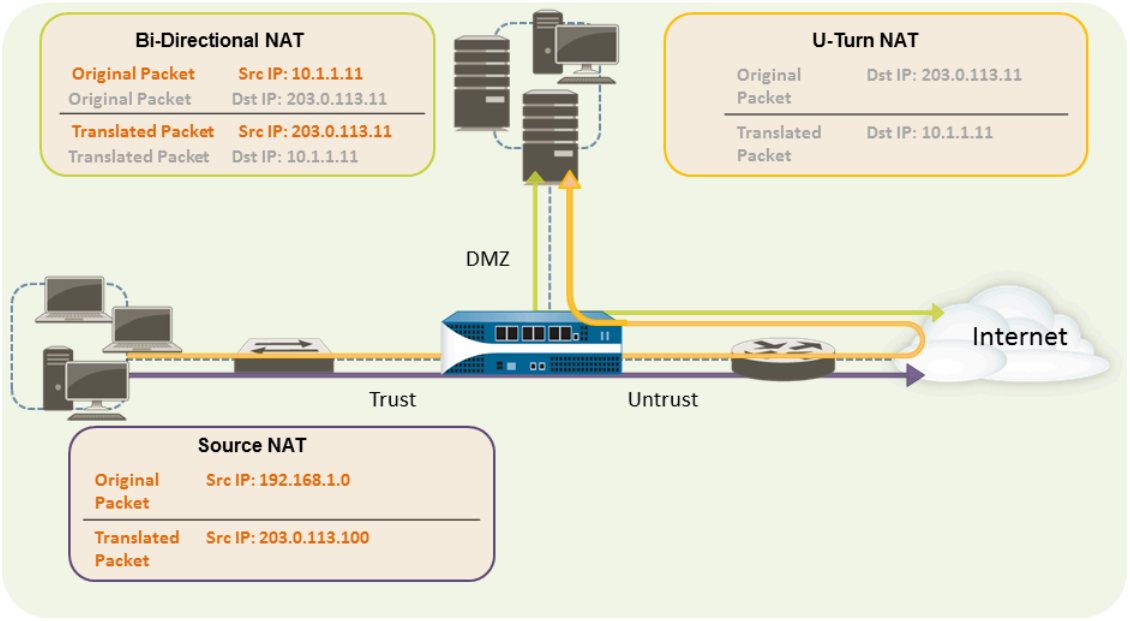
執行下列工作可設定 NAT 的各個方面。除了下列範例外，NAT 組態範例一節中也提供一些範例。

- 將內部用戶端的 IP 位址轉譯為公共 IP 位址（來源 DIPP NAT）
- 啟用內部網路上的用戶端以存取公共伺服器 （目的地 U-Turn NAT）
- 啟用公共伺服器的雙向位址轉譯（靜態來源 NAT）
- 使用 DNS 重寫設定目的地 NAT
- 使用動態 IP 位址設定目的地 NAT
- 修改 DIPP NAT 的過度訂閱比例
- 保留動態 IP NAT 位址
- 停用特定主機或介面的 NAT

本節中的前三個 NAT 範例以下列拓撲為基礎：



基於此拓撲，我們需要建立以下三個 NAT 原則：



- 若要啟用內部網路上的用戶端來存取網際網路上的資源，內部 192.168.1.0 位址將需要轉譯為可公開路由的位址。在此狀況下，我們將設定來源 NAT（上圖中的紫色外框和箭頭），使用輸出介面位址 203.0.113.100 作為從內部區域離開防火牆的所有封包中的來源位址。如需相關說明，請參閱將內部用戶端的 IP 位址轉譯為公共 IP 位址（來源 DIPP NAT）。

- 若要啟用內部網路上的用戶端來存取 DMZ 區域中的公用網頁伺服器，我們必須設定從外部網路將封包重新導向到 10.1.1.11 DMZ 網路上網頁伺服器實際位址的 NAT 規則，其中外部網路中的原始路由表格查閱將決定是否以封包內的目的地位址 203.0.113.11 為基準。為實現此目的，您必須從信任區域 (即封包中的來源位址) 到不信任區域 (即原始目的地位址) 中建立 NAT 規則，以轉譯目的地位址為 DMZ 區域中的位址。此類型的目的地 NAT 稱為 ***U-Turn NAT*** (上圖中的黃色外框和箭頭)。如需相關說明，請參閱啟用內部網路上的用戶端以存取公共伺服器 （目的地 U-Turn NAT）。
- 若要啟用網頁伺服器 (其同時為 DMZ 網路上的私人 IP 位址和可供外部使用者存取的公共位址) 以傳送及接收要求，防火牆必須將傳入的封包從公共 IP 位址轉譯為私人 IP 位址，並將傳出的封包從私人 IP 位址轉譯為公共 IP 位址。在防火牆上，您可使用單一雙向靜態來源 NAT 原則完成轉譯（上圖中的綠色外框和箭頭）。請參閱啟用公共伺服器的雙向位址轉譯（靜態來源 NAT）。

將內部用戶端的 IP 位址轉譯為公共 IP 位址（來源 DIPP NAT)

當內部網路的用戶端傳送要求時，封包中的來源位址會包含內部網路用戶端的 IP 位址。如果您使用內部範圍的私人 IP 位址，用戶端的封包將無法在網際網路上路由，除非您將網路封包中的來源 IP 位址轉譯為可公開路由的位址。

在防火牆上，您可設定來源 NAT 原則，將來源位址（及選用的連接埠）轉譯為公共位址以執行此動作。另一種方式則是將所有封包的來源位址轉譯至防火牆輸出介面，如下列程序所示。

STEP 1 | 為欲使用的外部 IP 位址建立位址物件。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後 **Add**（新增）**Name**（名稱），並選擇性地輸入物件 **Description**（描述）。
2. 從 **Type**（類型）清單中選取 **IP Netmask**（IP 網路遮罩），然後輸入防火牆上外部介面的 IP 位址，在此範例中為 203.0.113.100。
3. 按一下 **OK**（確定）。

雖然您不必在原則中使用位址物件，但因為可簡化管理，讓您在單一位置更新，而不必更新每個參考位址的原則，因此將其視為最佳做法。

STEP 2 | 建立 NAT 原則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入原則的描述性 **Name**（名稱）。
3. （選用）輸入標籤，其為可讓您排序或篩選原則的關鍵字或字詞。
4. 對於 **NAT Type**（**NAT** 類型），選取 **ipv4**（預設）。
5. 在 **Original Packet**（原始封包）頁籤上，在 **Source Zone**（來源區域）區段中選取為內部網路建立的區域（按一下**Add**（新增），然後選取區域），並從 **Destination Zone**（目的地區域）清單中選取為外部網路建立的區域。
6. 在 **Translated Packet**（轉譯的封包）頁籤上，從畫面的來源位址轉譯區段中的 **Translation Type**（轉譯類型）清單中，選取 **Dynamic IP And Port**（動態 **IP** 與連接埠）。
7. 針對 **Address Type**（位址類型），您有兩個選擇。您可以選取 **Translated Address**（轉譯的位址），然後按一下 **Add**（新增）。選取您剛剛建立的位址物件。

   另一個 **Address Type**（位址類型）是 **Interface Address**（介面位址），在此情況下，轉譯的位址將為介面的 IP 位址。針對此選擇，如果介面具有多個 IP 位址，您可以選取 **Interface**（介面），並選擇性地輸入 **IP Address**（**IP** 位址）。
8. 按一下 **OK**（確定）。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

STEP 4 | （選用）存取 CLI 以驗證轉譯。

1. 使用 **`show session all`** 命令來檢視工作階段表，您可在其中驗證來源 IP 位址和連接埠，以及對應的轉譯 IP 位址和連接埠。
2. 使用 *show session id <id_number>* 以檢視工作階段的詳細資料。
3. 如果您已設定動態 IP NAT，請使用 **`show counter global filter aspect session severity drop | match nat`** 命令，以檢查是否有任何工作階段因 NAT IP 配置而失敗。如果已配置動態 IP NAT 配發範圍中的所有位址，則會在要轉譯新連線時丟棄該封包。

啟用內部網路上的用戶端以存取公共伺服器（目的地 U-Turn NAT）

當內部網路上的使用者在 DMZ 中傳送存取公司網頁伺服器的要求時，DNS 伺服器會將其解析為公共 IP 位址。在處理要求時，防火牆將使用封包中的原始目的地 (公共 IP 位址)，並將封包路由至不信任區域的輸出介面。若要讓防火牆在收到信任區域使用者的要求時，瞭解其必須將網頁伺服器公共 IP 位址轉譯為 DMZ 網路上的位址，您必須建立目的地 NAT 規則，讓防火牆將要求傳送至 DMZ 區域的輸出介面，如下所示。

STEP 1 | 建立供網頁伺服器使用的位址物件。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後 **Add**（新增）**Name**（名稱），並選擇性地新增位址物件 **Description**（描述）。
2. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入網頁伺服器的公共 IP 位址，在此範例中為 203.0.113.11。

   您可將位址物件類型從 **IP Netmask**（**IP** 網路遮罩）切換至 **FQDN**，方法如下：按一下 **Resolve**（解析），顯示 FQDN 時，按一下 **Use this FQDN**（使用此 **FQDN**）。或者，對於 **Type**（類型），選取 **FQDN**，並輸入用於位址物件的 FQDN。如果您輸入 FQDN 並按一下 **Resolve**（解析），欄位中會顯示 FQDN 解析的 IP 位址。若要將位址物件 **Type**（類型）從 FQDN 切換至使用此 IP 位址的 IP Netmask（IP 網路遮罩），按一下 **Use this address**（使用此位址），**Type**（類型）會切換至 **IP Netmask**（**IP** 網路遮罩），而且欄位中會顯示 IP 位址。
3. 按一下 **OK**（確定）。

STEP 2 | 建立 NAT 原則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入 NAT 規則的描述性 **Name**（名稱）。
3. 在 **Original Packet**（原始封包）頁籤上，在 **Source Zone**（來源區域）區段中選取為內部網路建立的區域（按一下**Add**（新增），然後選取區域），並從 **Destination Zone**（目的地區域）清單中選取為外部網路建立的區域。
4. 在 **Destination Address**（目的地位址）區段中， **Add**（新增）您為公用 Web 伺服器建立的位址物件。
5. 在 **Translated Packet**（轉譯的封包）頁籤上，針對 Destination Address Translation（目的地位址轉譯）的 **Translation Type**（轉譯類型），選取 **Static IP**（靜態 **IP**），然後輸入指派給 DMZ 網路上網頁伺服器介面的 IP 位址，在此範例中為 10.1.1.11。或者，您可將 **Translation Type**（轉譯類型）選為 **Dynamic IP (with session distribution)**（動態 **IP**（採用工作階段散佈）），並輸入作為位址物件的 **Translated Address**（轉譯的位址）或使用 IP 網路遮罩、IP 範圍或 FQDN 的位址群組。其均可從 DNS 返回多個位址。如果轉譯目的地位址解析為多個位址，防火牆將根據您選取的方法，在多個位址中散佈傳入 NAT 工作階段，可選取的方法如下：**Round Robin**（循環配置）（預設方法）、**Source IP Hash**（來源 **IP** 雜湊）、**IP Modulo**（**IP** 模數）、**IP Hash**（**IP** 雜湊）或 **Least Sessions**（最少工作階段）。
6. 按一下 **OK**（確定）。

STEP 3 | 按一下 **Commit**（交付）。

啟用公共伺服器的雙向位址轉譯（靜態來源 NAT）

當您的公共伺服器在實體配置的網路區段上指派私人 IP 位址時，您需要來源 NAT 規則在輸出時將伺服器的來源位址轉譯為外部位址。您可建立靜態 NAT 規則將來源位址 10.1.1.11 內部為外部網頁伺服器位址，在本範例中為 203.0.113.11。

但是公共伺服器必須啟用，才能傳送與接收封包。您需要採用逆向原則，將公共位址 (也就是從網際網路使用者傳入封包中的目的地 IP 位址) 轉譯為私人位址，讓防火牆可將封包路由至您的 DMZ

網路。您可以建立雙向的靜態 NAT 規則，如下列程序所述。雙向轉譯只是靜態 NAT 的其中一個選項。

STEP 1 | 建立供網頁伺服器內部 IP 位址使用的位址物件。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後 **Add**（新增）**Name**（名稱），並選擇性地輸入物件 **Description**（描述）。
2. 從 **Type**（類型）清單中選取 **IP Netmask**（IP 網路遮罩），然後輸入 DMZ 網路上網頁伺服器的 IP 位址，在此範例中為 10.1.1.11。
3. 按一下 **OK**（確定）。

如果您尚未建立網頁伺服器公共位址的位址物件，您應立即建立該物件。

STEP 2 | 建立 NAT 原則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入 NAT 規則的描述性 **Name**（名稱）。
3. 在 **Original Packet**（原始封包）頁籤上，在 **Source Zone**（來源區域）區段中選取為 DMZ 建立的區域（按一下**Add**（新增），然後選取區域），並從 **Destination Zone**（目的地區域）清單中選取為外部網路建立的區域。
4. 在 **Source Address**（來源位址）區段中， **Add**（新增）您為內部 Web 伺服器位址建立的位址物件。
5. 在 **Translated Packet**（轉譯的封包）頁籤上，在 **Source Address Translation**（來源位址轉譯）區段的 **Translation Type**（轉譯類型）清單中，選取 **Static IP**（靜態 **IP**），然後從 **Translated Address**（轉譯的位址）清單中選取為外部網頁伺服器位址建立的位址物件。
6. 在 **Bi-directional**（雙向）欄位中，選取 **Yes**（是）。
7. 按一下 **OK**（確定）。

STEP 3 | 提交。

按一下 **Commit**（交付）。

使用 DNS 重寫設定目的地 NAT

當您設定對 IPv4 位址執行靜態轉譯的目的地 NAT 原則規則時，也可以設定規則，以便防火牆根據為該規則設定的原始或轉譯 IP 位址，重寫 DNS 回應中的 IPv4 位址。在將回應轉送至用戶端之前，防火牆會在 DNS 回應（與規則相符）中對 IPv4 位址（FQDN 解析）執行 NAT；因此，用戶端可以接收用於存取目的地服務的合適位址。

檢視 DNS 重寫使用案例，以幫助您確定將重寫方向指定為 **reverse**（反向）還是 **forward**（正向）。

您無法在啟用 *DNS* 重寫的同一 *NAT* 規則中啟用 ***Bi-directional***（雙向）來源地址轉譯。

STEP 1 | 建立目的地 NAT 原則規則，指定防火牆對與該規則相符之 IPv4 位址執行靜態轉譯，同時指定當該 IPv4 位址（來自 A 記錄）與 NAT 規則中的原始或轉譯目標位址相符時，防火牆在 DNS 回應中重寫 IP 位址。

1. 選取 **Policies**（原則） > **NAT**，然後 **Add**（新增）NAT 原則規則。
2. （選用）在 **General**（一般）頁籤中，輸入規則的描述性 **Name**（名稱）。
3. 針對 **NAT Type**（**NAT** 類型），選取 **ipv4**。
4. 在 **Original Packet**（原始封包）頁簽中，**Add**（新增）**Destination Address**（目的地位址）。

   您還必須選取一個來源區域或 ***Any***（任何）來源區域，但 *DNS* 重寫會在全域層級發生；僅會符合「原始封包」頁簽上的目的地位址。*DNS* 重寫會忽略「原始封包」頁簽上的所有其他欄位。
5. 在 **Translated Packet**（轉譯的封包）頁籤上，在目的地位址轉譯區段，將 **Translation Type**（轉譯類型）選為 **Static IP**（靜態 **IP**）。
6. 選取一個 **Translated Address**（轉譯的位址）或輸入新位址。
7. **Enable DNS Rewrite**（啟用 **DNS** 重寫）並選取 **Direction**（方向）：
   - 當 DNS 回應中的 IP 位址需要 NAT 規則指定的相反轉譯時，選取 **reverse**（反向）（預設）。如果 DNS 回應符合規則中的轉譯目的地位址，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 IP 位址 1.1.1.10 轉譯為 192.168.1.10，則防火牆會將 DNS 回應 192.168.1.10 重寫為 1.1.1.10。
   - 當 DNS 回應中的 IP 位址需要 NAT 規則指定的相同轉譯時，選取 **forward**（正向）。如果 DNS 回應符合規則中的原始目的地位址，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 IP 位址 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。
8. 按一下 **OK**（確定）。

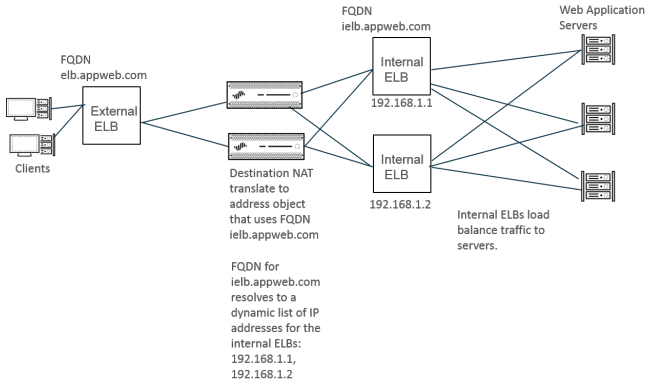
STEP 2 | **Commit**（提交）您的變更。

使用動態 IP 位址設定目的地 NAT

使用 目的地 NAT，將原始目的地位址轉譯為擁有動態 IP 位址且使用 FQDN 的目的地主機或伺服器。使用動態 IP 位址的目的地 NAT，在通常使用動態 IP 定址的雲端部署中特別有用。若雲端中的主機或伺服器擁有新（動態）IP 位址，您無需持續查詢 DNS 伺服器以手動更新 NAT 原則規則，也無需使用單獨的外部元件來藉助最新的 FQDN 至 IP 位址對應更新 DNS 伺服器。

當您使用動態 IP 位址設定目的地 NAT 時，您應當僅使用 FQDN（而不是 IP 網路遮罩或 IP 範圍）。

在以下範例拓撲中，用戶端要連線到代管雲端 web 應用程式的伺服器。外部彈性負載平衡器 (ELB) 連線到防火牆，而防火牆連線到與伺服器相連的內部 ELB。隨時間變化，Amazon Web Services (AWS)（打個比方）會依據服務需求為指派給內部 ELB 的 FQDN 新增（及移除）IP 位址。針對內部 ELB 的 NAT 使用 FQDN 可實現靈活性，有助於原則在不同時間解析成不同 IP 位址，由於採用動態更新，目的地 NAT 更易於使用。



STEP 1 | 使用您要向其轉譯位址的伺服器 FQDN 建立位址物件。

1. 選取 **Objects**（物件） > **Addresses**（位址）並依 **Name**（名稱）（如 **post-NAT-Internal-ELB**）**Add**（新增） 位址物件。
2. 選取 **FQDN** 作為 **Type**（類型）並輸入 FQDN。在此範例中，FQDN 為 **ielb.appweb.com**。
3. 按一下 **OK**（確定）。

STEP 2 | 建立目的地 NAT 原則。

1. 選取 **Policies**（原則） > **NAT**，並在 **General**（一般） 頁籤上依據 **Name**（名稱）**Add**（新增）NAT 原則規則。
2. 選取 **ipv4** 作為 **NAT Type**（**NAT** 類型）。
3. 在 **Original Packet**（原始封包）頁籤上，**Add**（新增）**Source Zone**（來源區域）與 **Destination Zone**（目的地區域）。
4. 在 **Translated Packet**（轉譯的封包）頁籤上的 Destination Address Translation（目的地位址轉譯）區段中，選取 **Dynamic IP (with session distribution)**（動態 **IP**（採用工作階段散佈））作為 **Translation Type**（轉譯類型）。
5. 對於 **Translated Address**（轉譯的位址），請選取您為 FQDN 建立的位址物件。在此範例中，FQDN 為 **`post-NAT-Internal-ELB`**。
6. 對於 **Session Distribution Method**（工作階段散佈方法），選取下列其中一項：
   - **Round Robin**（循環配置資源）（預設值）—按輪流順序將新工作階段指派給 IP 位址。除非有變更散佈方法的理由，否則循環配置資源散佈可能適用。
   - **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 位址的流量，則無需選取來源 IP 雜湊；請選取其他方法。
   - **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）—根據來源和目的地 IP 位址的雜湊指派新工作階段。
   - **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。

   在多個 *IP* 位址間散佈工作階段之前，防火牆不會從目的地 *IP* 位址清單中移除重複的 *IP* 位址。防火牆會以在非重複位址間散佈工作階段的方式，在重複位址間散佈工作階段。（例如，如果已轉譯的位址是位址物件的位址群組，且其中一個位址物件是解析為 *IP* 位址的 *FQDN*，而另一個位址物件是包含相同 *IP* 位址的範圍，則轉譯集區會出現重複位址。）
7. 按一下 **OK**（確定）。

STEP 3 | **Commit**（提交）您的變更。

STEP 4 | （選用）您可設定防火牆重新整理 FQDN 的頻率（使用案例 1：防火牆需要 DNS 解析）。

修改 DIPP NAT 的過度訂閱比例

如果您的公共 IP 位址足夠，不需要使用 DIPP NAT 過度訂閱，您可以減少過度訂閱比例，因此得到更多允許的 DIP 與 DIPP NAT 規則。

STEP 1 | 檢視 DIPP NAT 過度訂閱比例。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **Session Settings**（工作階段設定）。檢視 **NAT Oversubscription Rate**（**NAT** 超額授權比例）設定。

STEP 2 | 設定 DIPP NAT 過度訂閱比例。

1. 編輯工作階段設定區段。
2. 在 **NAT Oversubscription Rate**（**NAT** 超額授權比例）清單中，選取 **1x**、**2x**、**4x** 或 **8x**，視您要的比例而定。

   Platform Default（平台預設）設定會套用相應型號的預設超額授權設定。如果您不要超額授權，請選取 ***1x***。
3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

保留動態 IP NAT 位址

您可以保留動態 IP NAT 位址 (針對可設定的時段)，以防止將這些位址配置為需要轉譯之不同來源 IP 位址的轉譯位址。設定時，保留會套用至所有進行中的轉譯動態 IP 位址和任何新轉譯。

針對進行中的轉譯和新轉譯，將來源 IP 位址轉譯為可用的轉譯 IP 位址時，即使與該特定來源 IP 相關的所有工作階段都已到期，系統仍會保留該配對。使用該來源 IP 位址轉譯的所有工作階段都到期後，每個來源 IP 位址保留計時器便會開始。動態 IP NAT 是一對一轉譯；單一來源 IP 位址會轉譯為單一轉譯 IP 位址，系統會在已設定配發範圍中，從這些可用的位址中進行動態選擇。因此，在該保留因新工作階段未開始而到期之前，任何其他來源 IP 位址都無法使用保留的轉譯 IP 位址。在經過沒有使用中的工作階段時段後，每次來源 IP/轉譯 IP 對應的新工作階段開始時都會重設計時器。

依預設，不會保留任何位址。您可以為防火牆或虛擬系統保留動態 IP NAT 位址。

為防火牆保留動態 IP NAT 位址。

輸入下列命令：

```
admin@PA-3250# set setting nat reserve-ip yes
```

```
admin@PA-3250# set setting nat reserve-time <1-604800 secs>
```

為虛擬系統保留動態 IP NAT 位址。

輸入下列命令：

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-ip yes
```

```
admin@PA-3250# set vsys <vsysid> setting nat reserve-time <1-604800
 secs>
```

例如，假設將 **nat reserve-time** 設定為 28800 秒（8 小時）時，動態 IP NAT 集區為 30 個位址，且正在進行 20 個轉譯。現在系統會保留這 20 個轉譯，讓使用每個來源 IP/轉譯 IP 對應的最後一個工作階段（屬於任何應用程式）到期時，僅為該來源 IP 位址保留轉譯 IP 位址達 8 小時，以免來源 IP 位址需要再次轉譯。此外，由於已配置剩餘的 10 個轉譯位址，系統會為其

來源 IP 位址保留每個轉譯位址，每個位址都具有會在該來源 IP 位址的最後一個工作階段到期時開始的計時器。

透過這種方式，您可以將每個來源 IP 位址重複轉譯為配發範圍中的相同 NAT 位址；即使該轉譯位址沒有使用中的工作段階，系統也不會將配發範圍中保留的轉譯 IP 位址指派給其他主機。

假設來源 IP/轉譯 IP 對應的所有工作階段都已到期，且 8 小時的保留計時器已開始。該轉譯的新工作階段開始後，計時器會停止，且工作階段會繼續執行直到其全部結束為止，這時保留計時器會再次開始，並保留轉譯的位址。

在您輸入 **`set setting nat reserve-ip no`** 命令或將 **`nat reserve-time`** 變更為不同值以停用保留計時器之前，動態 IP NAT 配發範圍上的保留計時器都會保持有效。

保留的 CLI 命令不會影響動態 IP 與連接埠 (DIPP) 或靜態 IP NAT 配發範圍。

停用特定主機或介面的 NAT

您可以設定來源 NAT 與目的地 NAT 規則以停用位址轉譯。您可能會有例外狀況，像是不要子網路上的某個主機進行 NAT，或是不要讓離開特定介面的流量進行 NAT。下列程序說明如何停用主機的來源 NAT。

STEP 1 | 建立 NAT 原則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增），為原則新增描述性 **Name**（名稱）。
2. 在 **Original Packet**（原始封包）頁籤上，在 **Source Zone**（來源區域）區段中選取為內部網路建立的區域（按一下**Add**（新增），然後選取區域），並從 **Destination Zone**（目的地區域）清單中選取為外部網路建立的區域。
3. 針對 **Source Address**（來源位址），按一下 **Add**（新增），然後輸入主機位址。按一下 **OK**（確定）。
4. 在 **Translated Packet**（轉譯的封包）頁籤上，從畫面的來源位址轉譯區段中的 **Translation Type**（轉譯類型）清單中，選取 **None**（無）。
5. 按一下 **OK**（確定）。

STEP 2 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

系統會依從上到下的順序處理 *NAT* 規則，因此將 *NAT* 豁免原則置於其他 *NAT* 原則之前，可確保在要豁免的來源發生位址轉譯之前先處理該原則。

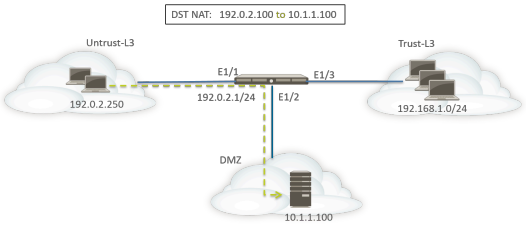
NAT 組態範例

目的地 NAT 範例—一對一對應

設定 NAT 和安全性規則時最常見的錯誤是參考區域和位址物件。在目的地 NAT 規則中使用的位址一律會參考封包中的原始 IP 位址（也就是預先轉譯的位址）。執行原始封包中目的地 IP 位址的路由查閱之後，便會決定 NAT 規則中的目的地區域 (也就是預先 NAT 目的地 IP 位址)。

安全性原則中的位址也會參考原始封包中的 IP 位址（也就是預先 NAT 位址）。但是，目的地區域是終端主機實際連線的區域。換句話說，執行後續 NAT 目的地 IP 位址的路由查閱之後，便會決定安全性規則中的目的地區域。

在下列一對一目的地 NAT 對應範例中，來自名為 Untrust-L3 之區域的使用者使用 IP 位址 192.0.2.100，存取名為 DMZ 之區域中的伺服器 10.1.1.100。



設定 NAT 規則之前，請考慮此案例的事件順序。

- 主機 192.0.2.250 會針對位址 192.0.2.100（目的地伺服器的公共位址）傳送 ARP 要求。
- 防火牆會收到 Ethernet1/1 介面上目的地 192.0.2.100 的 ARP 要求封包，並處理該要求。由於已設定的目的地 NAT 規則，防火牆會以自己的 MAC 位址回應 ARP 要求。
- 系統會針對比對來評估 NAT 規則。針對要轉譯的目的地 IP 位址，您必須建立從區域 untrust-l3 至區域 untrust-l3 的目的地 NAT 規則，才能將目的地 IP 192.0.2.100 轉譯為 10.1.1.100。
- 決定轉譯的位址之後，防火牆會針對目的地 10.1.1.100 執行路由查閱，以決定輸出介面。在此範例中，輸出介面為區域 DMZ 中的 Ethernet1/2。

- 防火牆會執行安全性原則查閱，以檢查是否已允許從區域 Untrust-L3 至 DMZ 的流量。

  原則方向會與輸入區域和伺服器實際所在區域相符。

  安全性原則會參考原始封包中的 *IP* 位址，其中具有目的地位址 *192.0.2.100*。

- 防火牆會將封包轉送至伺服器外的輸出介面 Ethernet1/2。封包離開防火牆時，目的地位址會變更為 10.1.1.100。

針對此範例，位址物件是對 webserver-private (10.1.1.100) 和 Webserver-public (192.0.2.100) 而設定的。已設定的 NAT 規則可能如下所示：

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Webserver-public	any	none	destination-translation address: webserver-private

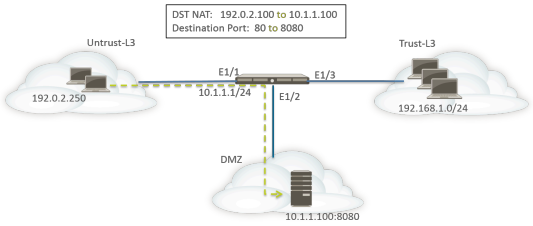
NAT 規則的方向會根據路由查閱的結果。

可提供來自 untrust-l3 區域之伺服器存取的已設定安全性原則可能如下所示：

	Source		Destination						
NAME	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Webserver access	Untrust-L3	any	DMZ	Webserver-pu...	web-browsing	any	Allow	none	

具有連接埠轉譯範例的目的地 NAT

在此範例中，已將網頁伺服器設定為接聽連接埠 8080 上的 HTTP 流量。用戶端會使用 IP 位址 192.0.2.100 和 TCP 連接埠 80 來存取網頁伺服器。已將目的地 NAT 規則設定為將 IP 位址和連接埠轉譯為 10.1.1.100 和 TCP 連接埠 8080。位址物件是對 webserver-private (10.1.1.100) 和 Servers-public (192.0.2.100) 而設定的。



您必須在防火牆上設定下列 NAT 和安全性規則：

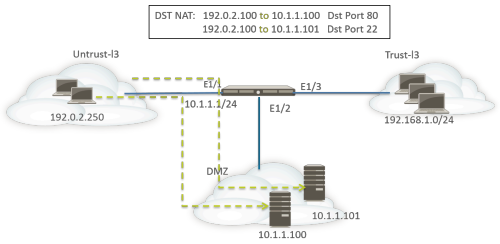
		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	any	none	destination-translation address: webserver-private port: 8080

			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow

使用 **`show session all`** CLI 命令可驗證轉譯。

目的地 NAT 範例—一對多對應

在此範例中，一個 IP 位址會對應至兩個不同的內部主機。防火牆會使用應用程式來識別其要將流量轉送至哪台內部主機。



系統會將所有 HTTP 流量傳送至主機 10.1.1.100，而將 SSH 流量傳送至伺服器 10.1.1.101。需要下列位址物件：

- 伺服器中預先轉譯 IP 位址的位址物件
- SSH 伺服器中實際 IP 位址的位址物件
- 網頁伺服器中實際 IP 位址的位址物件

建立對應的位址物件：

- Servers-public：192.0.2.100
- SSH-server：10.1.1.101
- webserver-private：10.1.1.100

NAT 規則可能如下所示：

		Original Packet						Translated Packet	
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Dst NAT-webserver	none	Untrust-L3	Untrust-L3	any	any	Servers-public	service-http	none	destination-translation address: webserver-private
Dst NAT-SSH	none	Untrust-L3	Untrust-L3	any	any	Servers-public	custom-ssh	none	destination-translation address: SSH-server

安全性規則可能如下所示：

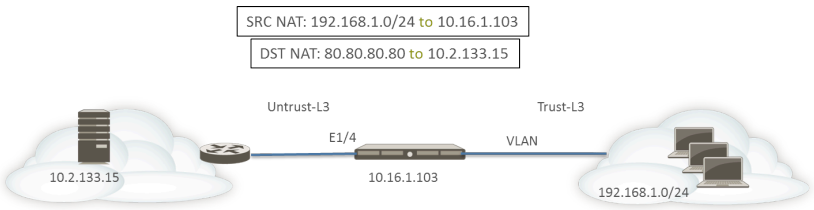
			Source				Destination					
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Webserver access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	web-browsing	any	Allow
SSH access	none	universal	Untrust-L3	any	any	any	DMZ	Servers-public	any	ssh	any	Allow

來源與目的地 NAT 範例

在此範例中，NAT 規則會在用戶端和伺服器之間轉譯封包的來源和目的地 IP 位址。

- 來源 NAT—將從 Trust-L3 區域中的用戶端傳送至 Untrust-L3 區域中的伺服器之封包中的來源位址，從網路 192.168.1.0/24 中的私人位址轉譯為防火牆上輸出介面的 IP 位址 (10.16.1.103)。動態 IP 與連接埠轉譯也會轉譯連接埠號碼。

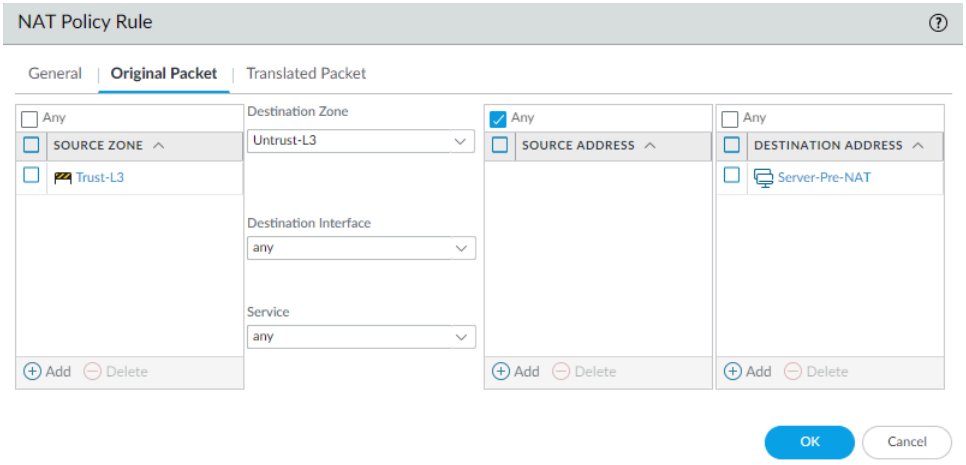
- 目的地 NAT—系統會將從用戶端傳送至伺服器之封包中的目的地位，從伺服器的公共位址 (80.80.80.80) 轉譯為伺服器的私人位址 (10.2.133.15)。

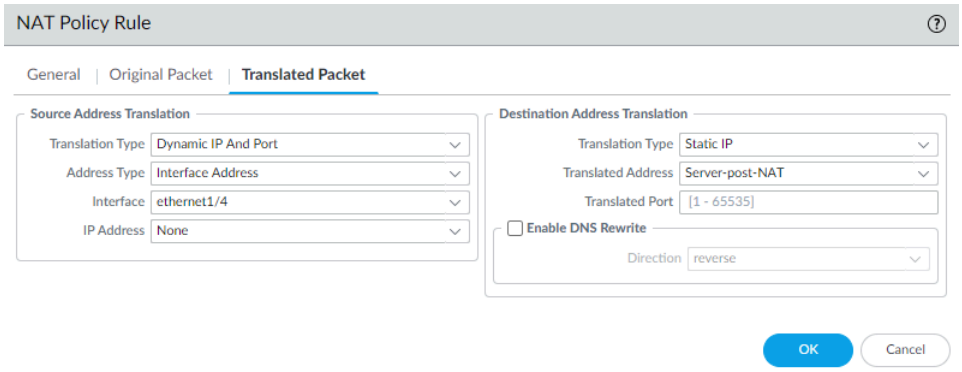


已針對目的地 NAT 建立下列位址物件。

- 伺服器預先 NAT：80.80.80.80
- 伺服器後續 NAT：10.2.133.15

下列螢幕擷取畫面說明如何設定來源和目的地 NAT 原則的範例。





若要確認轉譯，請使用 CLI 命令 **show session all filter destination 80.80.80.80**。系統會將用戶端位址 192.168.1.11 及其連接埠號碼轉譯為 10.16.1.103 和某個連接埠號碼。目的地位址 80.80.80.80 會轉譯為 10.2.133.15。

虛擬連接來源 NAT 範例

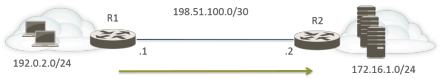
Palo Alto Networks® 防火牆的虛擬連接部署包含為終端裝置提供透明安全性的優勢。您可以針對在虛擬連接中設定的介面設定 NAT。系統允許所有 NAT 類型：來源 NAT（動態 IP、動態 IP 與連接埠、靜態）和目的地 NAT。

由於並未將 IP 位址指派給虛擬介接中的介面，因此您無法將 IP 位址轉譯為介面 IP 位址。您必須設定 IP 位址配發範圍。

在虛擬連接介面上執行 NAT 時，建議您將來源位址轉譯成不同的子網路，而不是轉譯成在相鄰裝置進行通訊的子網路。防火牆不會針對 NAT 位址執行 Proxy ARP。您必須在上游和下游路由器上設定適當的路由，以在虛擬連接模式中轉譯封包。鄰近裝置將只能解析 IP 位址的 ARP 要求，而這些 IP 位址只存在虛擬連接另一端的裝置介面上。關於 Proxy ARP 的詳細說明，請參閱 NAT 位址配發範圍的 Proxy ARP。

在下列來源 NAT 範例中，安全性原則（未顯示）已從名為 vw-trust 的 Virtual Wire 區域設定至名為 vw-untrust 的區域。

在下列拓撲中，已設定兩個路由器以提供子網路 192.0.2.0/24 和 172.16.1.0/24 之間的連線。已在子網路 198.51.100.0/30 中設定路由器之間的連結。已在兩個路由器上設定靜態路由以建立網路之間的連線。在環境中部署防火牆之前，每個路由器的拓撲和路由表如下所示：



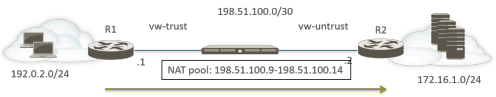
R1 上的路由：

目的地	下一個躍點
172.16.1.0/24	198.51.100.2

R2 上的路由：

目的地	下一個躍點
192.0.2.0/24	198.51.100.1

現在已在兩個 Layer 3 裝置之間的虛擬連接模式中部署防火牆。已在防火牆上設定範圍是 198.51.100.9 至 198.51.100.14 的 NAT IP 位址集區。所有從子網路 192.0.2.0/24 中之用戶端存取網路 172.16.1.0/24 中之伺服器的通訊，都會到達 R2，轉譯來源位址範圍為 198.51.100.9 至 198.51.100.14。來自伺服器的回應將導向至這些位址。



若要讓來源 NAT 得以運作，您必須在 R2 上設定適當的路由，以免以其他位址為目標的封包遭到丟棄。以下路由表顯示 R2 上的已修改路由表；路由會確保指向目的地

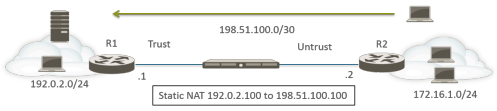
198.51.100.9-198.51.100.14 的流量（也就是子網路 198.51.100.8/29 上的主機）將透過防火牆傳回 R1。

R2 上的路由：

目的地	下一個躍點
198.51.100.8/29	198.51.100.1

虛擬連接靜態 NAT 範例

在此範例中，安全性原則已從名為 Trust 的虛擬連接區域設定至名為 Untrust 的虛擬連接區域。主機 192.0.2.100 會靜態轉譯為位址 198.51.100.100。啟用 **Bi-directional**（雙向）選項後，防火牆會從 Untrust 區域產生 NAT 原則至 Trust 區域。Untrust 區域上的用戶端會使用 IP 位址 198.51.100.100 存取伺服器，防火牆會將該位址轉譯為 198.0.2.100。伺服器在 192.0.2.100 啟動的任何連線都會轉譯為來源 IP 位址 198.51.100.100。



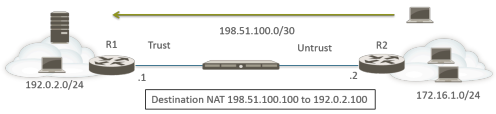
R2 上的路由：

目的地	下一個躍點
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
Static NAT	Trust	Untrust	any	webserver-private	any	any	static-ip webserver-public bi-directional: yes	none

虛擬連接目的地 NAT 範例

Untrust 區域內的用戶端會使用 IP 位址 198.51.100.100 存取伺服器，防火牆會將該位址轉譯為 192.0.2.100。必須設定從 Untrust 區域至 Trust 區域的 NAT 和安全性原則。



R2 上的路由：

目的地	下一個躍點
198.51.100.100/32	198.51.100.1

	Original Packet						Translated Packet	
NAME	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
DST NAT	Untrust	Trust	any	any	webserver-public	any	none	destination-translation address: webserver-private

NPTv6

IPv6 對 IPv6 Network Prefix Translation（網路首碼轉譯）(NPTv6) 會對 IPv6 首碼執行無狀態的靜態轉譯，將其轉譯為其他 IPv6 首碼（不會變更連接埠號碼）。NPTv6 有四項主要優勢：

- 您可以防止從多個資料中心宣告供應商獨立位址導致的非對稱路由問題。
- NPTv6 允許宣告多個特定路由，讓傳回流量到達與傳輸流量相同的防火牆。
- 私人和公共位址互為獨立；您可以變更其中一個位址而不會影響另一個。
- 您可以將 唯一本機位址 轉譯為可全域路由的位址。

本主題建立在對 NAT 的基礎瞭解上。設定 NPTv6 之前，請確定您已熟悉 NAT 概念。

- NPTv6 概要介紹
- 如何使用 NPTv6
- NDP Proxy
- NPTv6 和 NDP Proxy 範例
- 建立 NPTv6 原則

NPTv6 概要介紹

本節說明 IPv6 對 IPv6 Network Prefix Translation（網路首碼轉譯）(NPTv6) 及如何對其進行設定。NPTv6 可於 RFC 6296 中定義。Palo Alto Networks® 並未實作 RFC 中定義的所有功能，但已實作的功能與 RFC 相容。

NPTv6 可將 IPv6 首碼無狀態轉譯為另一個 IPv6 首碼。其為無狀態轉譯，這表示其不會追蹤轉譯位址的連接埠或工作階段。NPTv6 與可設定狀態的 NAT66 不同。Palo Alto Networks 支援 NPTv6 RFC 6296 首碼轉譯，而不支援 NAT66。

由於 IPv4 空間中的位址限制，您需要 NAT才能將不可路由的私人 IPv4 位址轉譯為一或多個可全域路由的 IPv4 位址。針對使用 IPv6 定址的組織，由於 IPv6 位址充足，因此不需要將 IPv6 位址轉譯為 IPv6 位址。但是，仍有某些需要 使用 NPTv6 的原因，讓您需要在防火牆轉譯 IPv6 首碼。

請務必瞭解 ***NPTv6*** 不提供安全性。一般而言，無狀態網路位址轉譯僅提供位址轉譯功能，而不提供任何安全性。***NPTv6*** 不會隱藏或轉譯連接埠號碼。您必須在每個方向中正確地設定防火牆安全性原則，以確保透過您預期的方式控制流量。

NPTv6 會轉譯 IPv6 位址的首碼部分，但不會轉譯主機部分或應用程式連接埠號碼。其只會複製主機部分，因此這部分會在防火牆的兩端保持相同。主機部分也會在封包標頭中保持可見。

下列防火牆型號支援 NPTv6（NPTv6 具有硬體查閱，但封包會通過 CPU）：

- PA-7000 系列防火牆
- PA-5200 系列防火牆
- PA-3200 系列防火牆
- PA-800 防火牆
- PA-220 防火牆

VM-Series 防火牆支援 NPTv6，但無法讓硬體執行工作階段查閱。

- 唯一本機位址
- 使用 NPTv6 的原因

唯一本機位址

RFC 4193 唯一本機 IPv6 單點傳送位址已定義本機位址 (ULA)，其為 IPv6 單點傳送位址。您可以將其視為等同於私人 IPv4 位址的 IPv6（如 RFC 1918 私人網際網路的位址配置中所識別），其無法全域路由。

ULA 為全域唯一位址，但無法全域路由。ULA 適用於本機通訊，以及可在網站或少數網站之間等有限區域中路由。Palo Alto Networks® 不建議您指派 ULA，但以 NPTv6 設定的防火牆會轉譯收到的首碼，包含 ULA。

使用 NPTv6 的原因

雖然可全域路由的公共 IPv6 位址充足，您可能會因為某些原因而要轉譯 IPv6 位址。NPTv6：

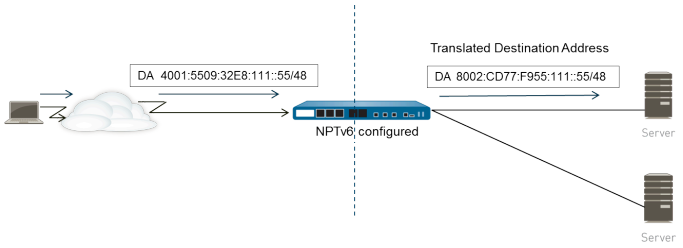
- 防止非對稱路由—如果多個資料中心將供應商獨立位址空間（例如 /48）宣告至全域網際網路，便會發生非對稱路由。您可以使用 NPTv6 從地區防火牆宣告多個特定路由，而傳回流量會到達與轉譯程式轉譯來源 IP 位址相同的防火牆。
- 提供位址獨立性—如果已變更全域首碼（例如，由 ISP 變更或因合併組織而變更），您也不需要變更本機網路中使用的 IPv6 首碼。相反地，您可以隨意變更內部位址，而不會中斷用於從網際網路的私人網路中存取服務的位址。無論是哪種狀況，您都只需更新 NAT 規則，而非重新指派網路位址。
- 針對路由轉譯 **ULA**—您可以在私人網路中指派 唯一本機位址，並讓防火牆將其轉譯為可全域路由的位址。因此，您可以擁有私人定址和可路由轉譯位址功能的便利性。
- 降低暴露 **IPv6** 首碼的風險—如果您不會轉譯網路首碼，則暴露 IPv6 首碼的風險較低，但 NPTv6 並非安全措施。未轉譯每個 IPv6 位址的介面識別碼部分，其在防火牆的兩端保持相同，且任何看到封包標頭的人都可看到此項目。此外，首碼並不安全，其他人也可決定此部分。

如何使用 NPTv6

為 NPTv6 設定原則時，Palo Alto Networks® 防火牆會在兩個方向中執行靜態的一對一 IPv6 轉譯。該轉譯是根據 RFC 6296 中所述的演算法執行。

在某個使用情況下，執行 NPTv6 的防火牆位於內部網路和外部網路（例如網際網路）之間，其中外部網路會使用可全域路由的首碼。在輸出方向中傳輸資料包時，外部首碼會取代內部來源首碼，這稱為來源轉譯。

在另一個使用情況下，在輸入方向中傳輸資料包時，內部首碼會取代目的地首碼（稱為目的地轉譯）。下圖說明目的地轉譯 NPTv6 的特性：只轉譯 IPv6 位址的首碼部分。其不會轉譯位址的主機部分，而這部分會在防火牆的兩端保持相同。在下圖中，防火牆兩端的主機識別碼都是 111::55。



請務必瞭解 NPTv6 不提供安全性。計劃您的 NPTv6 NAT 原則時，也請記得在每個方向中設定安全性原則。

NAT 或 NPTv6 原則規則無法將來源位址和轉譯的位址同時設定為任何。

在您要執行 IPv6 首碼轉譯的環境中，下列三個防火牆功能會搭配運作：NPTv6 NAT 原則、安全性原則和 NDP Proxy。

防火牆不會轉譯下列項目：

- 防火牆的芳鄰探索 (ND) 快取中已包含的位址。
- 子網路 0xFFFF（根據 RFC 6296 附錄 B）。
- IP 多點傳送位址。
- 首碼長度等於或少於 /31 的 IPv6 位址。
- 連結本機位址。如果防火牆在虛擬連接模式中運作，則不會有要轉譯的 IP 位址，且防火牆不會轉譯連結本機位址。
- 使用 TCP 驗證選項 (RFC 5925) 驗證端點的 TCP 工作階段位址。

使用 NPTv6 時，由於 NPTv6 在慢速路徑中執行，因此快速路徑流量的效能會受到影響。

NPTv6 只能在防火牆產生和終止通道時，與 IPSec IPv6 搭配使用。由於會修改來源和/或目的地 IPv6 位址，因此可能無法轉送 IPSec 流量。封裝封包的 NAT 穿透技術可讓 IPSec IPv6 與 NPTv6 搭配使用。

- 總和檢查碼中立對應
- 雙向轉譯
- 套用至特定服務的 NPTv6

總和檢查碼中立對應

防火牆所執行的 NPTv6 對應轉譯屬於總和檢查碼中立，這表示「... 使用標準網際網路總和檢查碼演算法計算總和檢查碼時，這些對應造成 IP 標頭產生相同的 IPv6 虛擬標頭總和檢查碼 (RFC 1071)」。 請參閱 RFC 6296 第 2.6 節以取得總和檢查碼中立對應的詳細資訊。

如果您正在使用 NPTv6 執行目的地 NAT，您可以在 **`test nptv6`** CLI 命令的語法中，提供防火牆介面的內部 IPv6 位址和外部首碼/首碼長度。CLI 會以要在 NPTv6 設定中用於到達目的地之總和檢查碼中立的公共 IPv6 位址回應。

雙向轉譯

當您建立 NPTv6 原則時，**Translated Packet**（轉譯的封包） 頁籤中的 **Bi-directional**（雙向） 選項可為您提供方便的方法，讓防火牆以您設定的轉譯反方向建立對應的 NAT 或 NPTv6 轉譯。**Bi-directional**（雙向）預設為停用。

若您啟用 ***Bi-directional***（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。缺少這類原則時，***Bi-directional***（雙向）功能將允許封包自動雙向轉譯，您可能不希望此情況發生。

套用至特定服務的 NPTv6

Palo Alto Networks 的 NPTv6 實作提供篩選封包的功能，可限制要採用轉譯的封包。請記住，NPTv6 不會執行連接埠轉譯。由於 NPTv6 只會轉譯 IPv6 首碼，因此其沒有動態 IP 與連接埠 (DIPP) 轉譯的概念。但是，您可以指定只有特定服務連接埠的封包才會接受 NPTv6 轉譯。若要執行此操作，請 建立 NPTv6 原則，以指定原始封包中的 **Service**（服務）。

NDP Proxy

適用於 IPv6 的芳鄰探索通訊協定 (NDP) 執行的功能，與適用於 IPv4 的位址解析通訊協定 (ARP) 所提供的功能類似。RFC 4861 已定義適用於 IP 版本 6 (IPv6) 的芳鄰探索。主機、路由器和防火牆會使用 NDP 在已連線連結上決定芳鄰連結層位址、追蹤可到達的芳鄰，以及更新已變更的芳鄰連結層位址。端點會宣告其自己的 MAC 位址和 IPv6 位址，也會請求來自端點的位址。

當節點具有可代表該節點轉送封包的鄰近裝置時，NDP 也支援 ***proxy*** 的概念。裝置（防火牆）會執行 NDP Proxy 的角色。

Palo Alto Networks® 防火牆在其介面上支援 NDP 和 NDP Proxy。當您設定防火牆作為位址的 NDP Proxy 時，這會讓防火牆傳送芳鄰探索 (ND) 宣告，並回應來自對等的 ND 請求，這些請求會要求在防火牆背後指派給裝置之 IPv6 首碼的 MAC 位址。您也可以設定防火牆不會回應的 Proxy 要求位址（否定位址）。

事實上，預設會啟用 NDP，且基於下列原因，設定 NPTv6 時，您需要設定 NDP Proxy：

- NPTv6 的無狀態性質需要可指示防火牆回應傳送至特定 NDP Proxy 位址的 ND 封包，而不回應否定 NDP Proxy 位址的方法。

  由於 ***NDP Proxy*** 表示防火牆會在防火牆背後到達這些位址，但芳鄰不在防火牆背後，因此建議您在 ***NDP Proxy*** 組態中否定芳鄰的位址。

- NDP 會讓防火牆儲存其 ND 快取中芳鄰的 MAC 位址和 IPv6 位址。（請參閱 NPTv6 和 NDP Proxy 範例 中的圖。） 由於針對可在防火牆 ND 快取中找到的位址執行 NPTv6 轉譯會造成衝突，因此防火牆不會對這些位址執行該轉譯。如果快取中位址的主機部分與芳鄰位址的主機部分重疊，且將快取中的首碼轉譯為與芳鄰相同的首碼（因為防火牆上的輸出介面屬於與芳鄰相同的子網路），則會產生與芳鄰的合法 IPv6 位址完全相同的轉譯位址，並因此發生衝突。（如果嘗試執行 NPTv6 轉譯發生在 ND 快取中的位址，則資訊 syslog 訊息會記錄事件：`NPTv6 Translation Failed.`）

啟用 NDP Proxy 的介面收到針對 IPv6 位址要求 MAC 位址的 ND 請求時，便會發生下列結果：

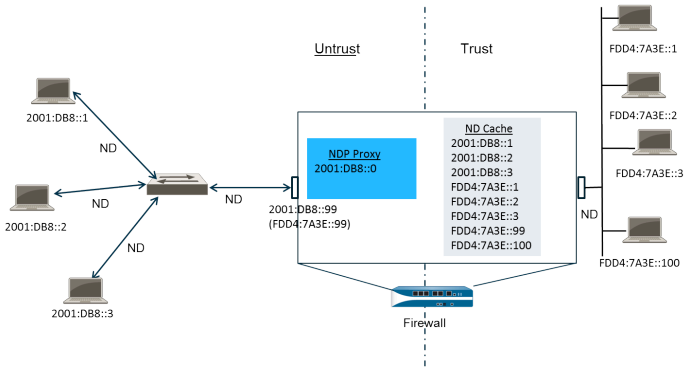
- 防火牆會搜尋 ND 快取以確保來自請求的 IPv6 位址並未包含於其中。如果在 ND 快取中包含位址，防火牆便會忽略 ND 請求。
- 如果來源 IPv6 位址為 0，這表示封包為重複的位址偵測封包，且防火牆會忽略 ND 請求。
- 防火牆會執行 NDP Proxy 位址的最長首碼比對搜尋，並找到請求中最相符的位址。如果已核取比對的否定欄位（在 NDP Proxy 清單中），則防火牆會丟棄 ND 請求。
- 只有在最長首碼比對搜尋相符，且並未否定相符的位址時，NDP Proxy 才會回應 ND 請求。防火牆會以 ND 封包回應，並提供自己的 MAC 位址作為指向查詢目的地之下一個躍點的 MAC 位址。

為了成功支援 NDP，防火牆不會針對下列項目執行 NDP Proxy：

- 重複的位址偵測 (DAD)。
- ND 快取中的位址（因為此類位址不屬於防火牆，而是屬於已探索芳鄰）。

NPTv6 和 NDP Proxy 範例

下圖介紹了 NPTv6 和 NDP Proxy 如何協同運作。



- NPTv6 範例中的 ND 快取
- NPTv6 範例中的 NDP Proxy
- NPTv6 範例中的 NPTv6 轉譯
- 不轉譯 ND 快取中的芳鄰

NPTv6 範例中的 ND 快取

在上述範列中，多個端點會透過交換器連線至防火牆，而 ND 會發生於端點和交換器之間、交換器和防火牆之間，以及防火牆和信任端的設備之間。

防火牆識別端點時會將其位址儲存至 ND 快取。已在信任端上將信任的端點 FDDA:7A3E::1、FDDA:7A3E::2 和 FDDA:7A3E::3 連線至防火牆。FDDA:7A3E::99 是防火牆本身的轉譯位址；其公共位址為 2001:DB8::99。已探索不受信任端上的端點位址，並出現在 ND 快取中：2001:DB8::1、2001:DB8::2 和 2001:DB8::3。

NPTv6 範例中的 NDP Proxy

在我們的案例中，我們要讓防火牆針對防火牆背後裝置上的首碼作為 NDP Proxy。當防火牆是指定位址/範圍/首碼組合的 NDP Proxy，且其在 ND 請求或宣告中看到來自此範圍的位址，則只要具有該特定位址的裝置並未先回應、未在 NDP Proxy 設定中否定位址，且位址未在 ND 快取中，防火牆便會回應。防火牆會執行首碼轉譯（如下所述）並將封包傳送至信任端，其中可能會或不會將該位址指派給裝置。

在此範例中，ND Proxy 表格包含網路位址 2001:DB8::0。當介面看到 2001:DB8::100 的 ND 時，L2 交換器上的其他設備都不會要求封包，因此該 Proxy 範圍讓防火牆要求該封包，並隨後轉譯為防火牆會將其傳出至信任端的 FDD4:7A3E::100。

NPTv6 範例中的 NPTv6 轉譯

在此範例中，我們將 **Original Packet**（原始封包）的 **Source Address**（來源位址）設定為 FDD4:7A3E::0，且將 **Destination**（目的地）設定為 **Any**（任何）。並以 **Translated Address**（轉譯的位址）2001:DB8::0 設定 **Translated Packet**（轉譯的封包）。

因此，來源為 FDD4:7A3E::0 的傳出封包會轉譯為 2001:DB8::0。具有網路 2001:DB8::0 中目的地首碼的傳入封包會轉譯為 FDD4:7A3E::0。

不轉譯 ND 快取中的芳鄰

在本範例中，這些是在防火牆背後且具有主機識別碼 :1、:2 和 :3 的主機。如果將這些主機的首碼轉譯為存在於防火牆以外的首碼，且這些裝置也具有主機識別碼 :1、:2 和 :3，由於位址的主機識別碼部分保持不變，因此產生的轉譯位址會屬於現有裝置，並導致定址衝突。為了避免重疊主機識別碼產生的衝突，NPTv6 不會轉譯在其 ND 快取中找到的位址。

建立 NPTv6 原則

如果您想設定 NAT NPTv6 原則以將 IPv6 首碼轉譯為另一個 IPv6 首碼，請執行此工作。此工作的先決條件是：

- 啟用 IPv6。選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段）。按一下 **Edit**（編輯），然後選取 **IPv6 Firewalling**（**IPv6** 防火牆）。
- 針對 Layer 3 乙太網路介面，設定有效的 IPv6 位址並啟用 IPv6。選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），選取介面，然後在 **IPv6** 頁籤上選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。
- 由於 NPTv6 不提供安全性，因此請建立網路安全性原則。
- 決定您是否想執行來源轉譯、目的地轉譯或兩者都執行。
- 識別要套用 NPTv6 原則的區域。
- 識別原始和轉譯的 IPv6 首碼。

STEP 1 | 建立新 NPTv6 原則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入 NPTv6 原則規則的描述性 **Name**（名稱）。
3. （選用）輸入 **Description**（說明）和 **Tag**（標籤）。
4. 針對 **NAT Type**（**NAT** 類型），選取 **NPTv6**。

STEP 2 | 指定傳入封包的比對規則；符合所有規則的封包便是要採用 NPTv6 轉譯的封包。

兩種類型的轉譯都需要區域。

1. 在 **Original Packet**（原始封包）頁籤上，將 **Source Zone**（來源區域）保留為 **Any**（任何），或 **Add**（新增）要套用原則的來源區域。
2. 輸入要套用原則的 **Destination Zone**（目的地區域）。
3. （選用）選取 **Destination Interface**（目的地介面）。
4. （選用）選取 **Service**（服務）以限制要轉譯的封包類型。
5. 如果您正在執行來源轉譯，請輸入 **Source Address**（來源位址）或選取 **Any**（任何）。該位址可以是位址物件。下列限制適用於 **Source Address**（來源位址）和 **Destination Address**（目的地位址）：
   - 雖然可以丟棄首碼中前置的零，但對於 **Original Packet**（原始封包）和 **Translated Packet**（轉譯的封包），**Source Address**（來源位址）和 **Destination Address**（目的地位址）的首碼必須為 xxxx:xxxx::/yy 格式。
   - IPv6 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。
   - 您無法將 **Source Address**（來源位址）和 **Destination Address**（目的地位址）同時設定為**Any**（任何）。
6. 如果您正在執行來源轉譯，則可以選擇性地輸入 **Destination Address**（目的地位址）。如果您正在執行目的地轉譯，則必須輸入 **Destination Address**（目的地位址）。目的地

位址（允許位址物件）必須為網路遮罩，而不僅僅是 IPv6 位址，也不能是一個範圍。首碼長度必須必須在 /32 到 /64 範圍內（包含 /32 和 /64）。例如 2001:db8::/32。

STEP 3 | 指定轉譯的封包。

1. 在 **Translated Packet**（轉譯的封包）頁籤上，若要執行來源轉譯，請在（來源位址轉譯）區域中，針對 **Translation Type**（轉譯類型）選取 **Static IP**（靜態 **IP**）。如果您不想執行來源轉譯，請選取 **None**（無）。
2. 如果您選擇 **Static IP**（靜態 **IP**），則會顯示 **Translated Address**（轉譯的位址）欄位。輸入轉譯的 IPv6 首碼或位址物件。請參閱上一個步驟中所列的限制。

   將 ***Translated Address***（轉譯的位址）設定為防火牆不受信任介面位址之首碼的最佳做法。例如，如果非受信任介面具有位址 *2001:1a:1b:1::99/64*，則將 ***Translated Address***（轉譯的位址）設定為 *2001:1a:1b:1::0/64*。
3. （選用）如果您想讓防火牆以您設定的轉譯反方向建立對應的 NPTv6 轉譯，則選取 **Bi-directional**（雙向）。

   若您啟用 ***Bi-directional***（雙向）轉譯，請務必確保您已具備安全性原則規則以控制兩個方向的流量。缺少這類原則規則時，***Bi-directional***（雙向）轉譯將允許封包自動雙向轉譯，您可能不希望此情況發生。
4. 若要執行目的地轉譯，請選取 **Destination Address Translation**（目的地位址轉譯）。在 **Translated Address**（轉譯的位址）欄位中，選擇位址物件，或輸入您的內部目的地位址。
5. 按一下 **OK**（確定）。

STEP 4 | 設定 NDP Proxy。

當您設定防火牆作為位址的 NDP Proxy 時，這會讓防火牆傳送芳鄰探索 (ND) 宣告，並回應來自對等的 ND 請求，這些請求會要求在防火牆背後指派給裝置之 IPv6 首碼的 MAC 位址。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取介面。
2. 在 **Advanced**（進階） > **NDP Proxy** 頁籤上，選取 **Enable NDP Proxy**（啟用 **NDP Proxy**），然後按一下 **Add**（新增）。
3. 針對啟用 NDP Proxy 的項目，輸入 **IP Address (es)**（**IP** 位址）。其可以是位址、位址範圍或首碼和首碼長度。IP 位址順序不重要。在理想的狀態下，這些位址會與您在 NPTv6 原則中設定的轉譯位址相同。

   如果位址為子網路，*NDP Proxy* 會回應子網路中的所有位址，因此您應該透過選取的 ***Negate***（否定）列出該子網路中的芳鄰，如上一個步驟中所述。
4. （選用）針對您不想啟用 NDP Proxy 的項目，輸入一或多個位址，並選取 **Negate**（否定）。例如，您可以從上一個步驟中設定的 IP 位址範圍或首碼範圍中，否定較小的位址子集。建議您否定防火牆芳鄰的位址。

STEP 5 | 提交組態。

按一下 **OK**（確定）與 **Commit**（提交）。

NAT64

當您仍需要與 IPv4 網路通訊時，NAT64 提供了一種轉換成 IPv6 的方式。當您需要從僅有 IPv6 的網路與 IPv4 網路通訊時，可以使用 NAT64 將來源和目的地位址從 IPv6 轉譯成 IPv4（或相反）。NAT64 可讓 IPv6 用戶端存取 IPv4 伺服器，並可讓 IPv4 用戶端存取 IPv6 伺服器。在設定 NAT64 之前，您應瞭解 NAT。

NAT64 概要介紹

您可以在 Palo Alto Networks® 防火牆上設定兩種類型的 NAT64 轉譯；每一種都將在兩個 IP 位址家族之間執行雙向轉譯：

- 防火牆支援使用具狀態的 NAT64 進行 IPv6 啟動的通訊，這種轉移會將多個 IPv6 位址對應到一個 IPv4 位址，從而節省 IPv4 位址。（不支援無狀態 NAT64，這種轉譯方式會將一個 IPv6 位址對應到一個 IPv4 位址，並不能節約 IPv4 位址。）為 IPv6 啟動的通訊設定 NAT64
- 防火牆支援利用靜態繫結進行 IPv4 啟動的通訊，這種方式會將一個 IPv4 位址和連接埠號碼對應到一個 IPv6 位址。為 IPv4 啟動的通訊設定 NAT64此外還支援連接埠重寫，這種方式可將一個 IPv4 和連接埠號碼轉移成帶多個連接埠號碼的 IPv6 位址，從而節約更多的 IPv4 位址。為 IPv4 啟動的與連接埠轉譯的通訊設定 NAT64

IPv4 位址可用於 NAT44 和 NAT64；無需保留僅用於 NAT64 的 IPv4 位址集區。

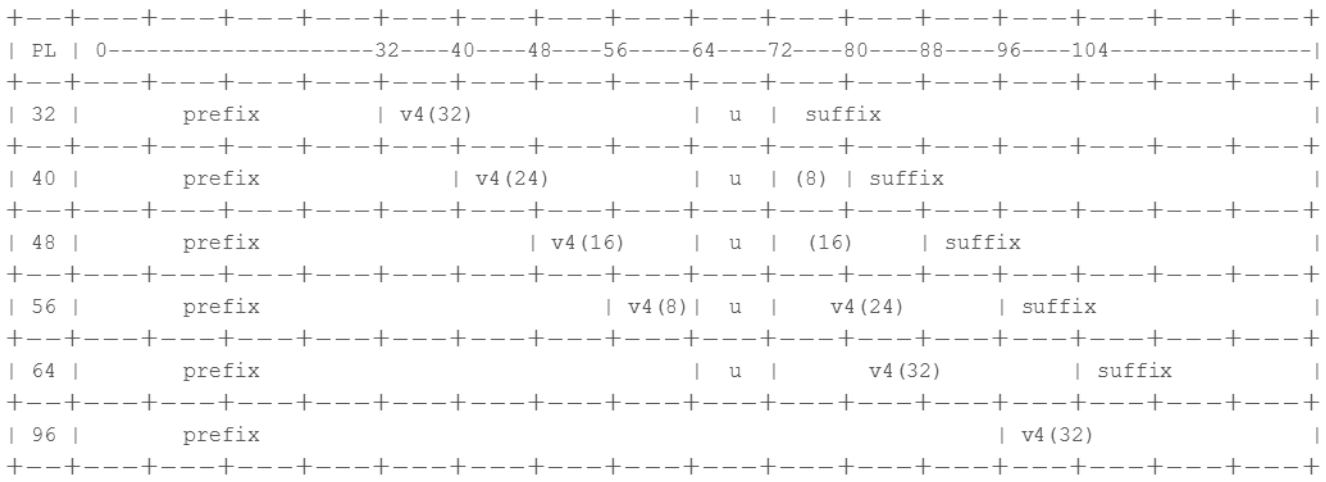
NAT64 在 Layer 3 介面、子介面和通道介面上運作。若要在 Palo Alto Networks 防火牆上使用 NAT64 進行 IPv6 啟動的通訊，您必須部署協力廠商 DNS64 伺服器 或解決方案，以分隔 DNS 查詢功能與 NAT 功能。DNS64 伺服器會將其從公用 DNS 伺服器接收的 IPv4 位址編碼成 IPv6 主機使用的 IPv6 位址，從而在 IPv6 主機和 IPv4 DNS 伺服器之間進行轉譯。

Palo Alto Networks 支援下列 NAT64 功能：

- 傳回 (NAT U-Turn)；此外，NAT64 還可透過丟棄所有具有來源首碼 64::/n 的 IPv6 封包，防止傳回迴圈攻擊。
- 按 RFC 6146 轉譯 TCP/UDP/ICMP 封包；防火牆將盡最大努力轉譯未使用應用程式層級閘道 (ALG) 的其他通訊協定。例如，防火牆可轉譯 GRE 封包。這種轉譯具有與 NAT44 相同的限制：如果您沒有為可使用單獨控制和資料通道的通訊協定設定 ALG，防火牆將不瞭解傳回流量。
- 按照 RFC 4884 在原始資料包欄位有 ICMP 長度屬性的 IPv4 和 IPv6 之間進行的轉譯。

內嵌 IPv4 的 IPv6 位址

NAT64 可按 RFC 6052 IPv4/IPv6 轉譯程式的 IPv6 定址 中所述使用內嵌 IPv4 的 IPv6 位址。內嵌 IPv4 的 IPv6 位址是一個 32 位元中編碼了 IPv4 位址的 IPv6 位址。IPv6 首碼長度（圖中的 PL）決定了 IPv4 位址在 IPv6 位址中的編碼位置，具體如下：



防火牆支援轉移使用這些首碼的 /32、/40、/48、/56、/64 和 /96 子網路。單一防火牆支援多個首碼；每個 NAT64 規則使用一個首碼。首碼可以是公認首碼 (64:FF9B::/96) 或組織的唯一網路特定首碼 (NSP)（用於控制位址轉譯程式）（DNS64 裝置）。NSP 一般是組織的 IPv6 首碼內的網路。DNS64 通常將 u 欄位和尾碼設定為零；防火牆會忽略這些欄位。

DNS64 伺服器

如果您需使用 DNS，而且要使用 IPv6 啟動的通訊執行 NAT64 轉譯，則必須使用協力廠商 DNS64 伺服器或利用公認首碼或 NSP 建立的其他 DNS64 解決方案。當 IPv6 主機嘗試存取網際網路上的 IPv4 主機或網域時，DNS64 伺服器將向權威 DNS 伺服器查詢對應到該主機的 IPv4 位址。DNS 伺服器將位址記錄（A 記錄）傳回 DNS64 伺服器，其中包含了該主機名稱的 IPv4 位址。

DNS64 伺服器將 IPv4 位址轉換成十六進位，並根據首碼長度將其編碼成其設定使用的 IPv6 首碼（公認首碼或您的 NSP）的相應八位元，最終產生內嵌 IPv4 的 IPv6 位址。DNS64 伺服器將 AAAA 記錄傳送至將內嵌 IPv4 之 IPv6 位址對應至 IPv4 主機名稱的 IPv6 主機。

路徑 MTU 探索

IPv6 並不會分割封包，因此防火牆將使用兩種方法來降低對分割封包的需求：

- 當防火牆轉譯 DF（不分割）位元為零的 IPv4 封包時，表示傳送者希望防火牆分割過大的封包，但防火牆不會為 IPv6 網路（轉譯後）分割封包，因為 IPv6 不會分割封包。您可以防火牆將在轉譯前 IPv4 分割成的最小大小。此設定為 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小網路 **MTU**）值，使用 RFC 6145 IP/ICMP 轉譯演算法編譯。您可以將 **NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小網路 **MTU**） 設定為最大值（**Device**（裝置） > **Setup**（設定） > **Session**（工作階段）），這會使防火牆在將 IPv4 封包轉譯成 IPv6 之前，先將其分割成最小大小的 IPv6。（**NAT64 IPv6 Minimum Network MTU**（**NAT64 IPv6** 最小網路 **MTU**） 並不會變更介面 MTU。）
- 防火牆用於減少分割的另一種方法是路徑 MTU 探索 (PMTUD)。在 IPv4 啟動的通訊中，如果要轉譯的 IPv4 封包設定了 DF 位元並且輸出介面的 MTU 小於封包，則防火牆將使用 PMTUD 丟棄封包，並向來源傳回 ICMP「Destination Unreachable - fragmentation needed」（目的地不可連線 - 需要分割）訊息。來源將為該目的地降低路徑 MTU，並重新傳送封包，直至路徑 MTU 連續減小，允許傳送封包。

IPv6 啟動的通訊

由 IPv6 啟動的與防火牆之間的通訊和與 IPv4 拓撲中來源 NAT 的通訊類似。當 IPv6 主機需要與 IPv4 伺服器通訊時，為 IPv6 啟動的通訊設定 NAT64。

在 NAT64 原則規則中，將原始來源設定為 IPv6 主機位址或 Any（任何）。將目的地 IPv6 位址設定為公認首碼或 DNS64 伺服器使用的 NSP。（不能在規則中設定完整的 IPv6 目的地位址。）

如果您需使用 DNS，則需使用 DNS64 伺服器以將 IPv4 DNS「A」結果轉換成與 NAT64 首碼合併的「AAAA」結果。如果您不使用 DNS，則需依據 RFC 6052 規則，使用防火牆上設定的 IPv4 目的地位址及 NAT64 首碼建立位址。

對於使用 DNS 的環境，下方的範例拓撲說明了與 DNS64 伺服器的通訊。必須設定 DNS64 伺服器使用公認首碼 64:FF9B::/96 或網路特定的首碼（必須符合 RFC 6052）（/32、/40、/48、/56、/64 或 /96）。

在防火牆的轉譯端，轉譯類型必須為動態 IP 和連接埠，以便實作具狀態 NAT64。您可以將來源轉譯位址設定為防火牆上輸出介面的 IPv4 位址。您不能設定目的地轉譯欄位；防火牆將首先在規則的原始目的地位址中尋找首碼長度，然後根據首碼從輸入封包的原始目的地 IPv6 位址擷取已編碼的 IPv4 位址，從而轉譯位置。

在查閱 NAT64 規則之前，防火牆必須執行路由查閱，以尋找輸入封包的目的地安全性區域。您必須確保可透過目的地區域指派連線 NAT64 首碼，因為 NAT64 首碼不能被防火牆路由。防火牆可能將 NAT64 首碼指派給預設路由或丟棄 NAT64 首碼（如果沒有路由）。防火牆將不會尋找目的地區域，因為 NAT64 首碼並未列於與輸出介面和區域關聯的路由表中。

您還必須設定一個通道介面（無終止點）。您可以將 NAT64 首碼套用於通道，並套用適當區域，以確保 NAT64 首碼的 IPv6 流量指派到適當的目的地區域。此外，通道還具備這一優勢：若流量與 NAT64 規則不相符，會丟棄採用 NAT64 首碼的 IPv6 流量。您在防火牆上設定的路由通訊協定會在其路由表中查閱 IPv6 首碼，以尋找目的地區域，然後查看 NAT64 規則。

下圖說明了 DNS64 伺服器在名稱解析過程中的作用。在此範例中，DNS64 伺服器被設定使用公認首碼 64:FF9B::/96。

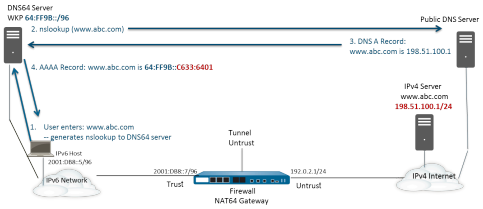
1。IPv6 主機上的使用者輸入 URL www.abc.com，對 DNS64 伺服器產生了一次名稱伺服器查閱 (nslookup)。

2.DNS64 伺服器將 nslookup 傳送至 www.abc.com 的公用 DNS 伺服器，要求其 IPv4 位址。

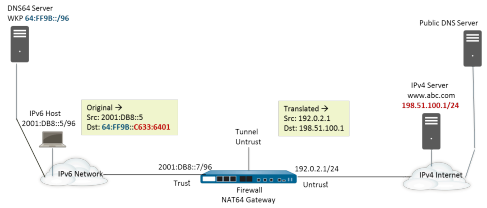
3.DNS 伺服器傳回 A 記錄，向 DNS64 提供 IPv4 位址。

4.DNS64 向 IPv6 使用者傳送 AAAA 記錄，將 IPv4 小數點十進位位址 198.51.100.1 轉換為十六進位的 C633:6401，並建起嵌入 IPv6 首碼 64:FF9B::/96。[198 = C6 hex; 51 = 33 hex; 100 = 64 hex; 1 = 01 hex.] 結果是產生一個內嵌 IPv4 的 IPv6 位址 64:FF9B::C633:6401。

請注意在 /96 首碼中，IPv4 位址是 IPv6 位址中編碼的最後四個八位元。如果 DNS64 伺服器使用 /32、/40、/48、/56、/64 首碼，IPv4 位址將如 RFC 6052 中所示編碼。



完成透明名稱解析後，IPv6 主機立即向防火牆傳送一個封包，其中包含 DNS64 伺服器確定的 IPv6 來源位址以及目的地 IPv6 位址 64:FF9B::C633:6401。防火牆將依 NAT 規則執行 NAT64 轉譯。



為 IPv6 啟動的通訊設定 NAT64

此設定工作及相應位址與 IPv6 啟動的通訊一節中的圖片對應。

STEP 1 | 在防火牆上啟用要運作的 IPv6 。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 選取 **Enable IPv6 Firewalling**（啟用 **IPv6** 防火牆）。
3. 按一下 **OK**（確定）。

STEP 2 | 為 IPv6 目的地位址建立位址物件（預轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64-IPv4 Server。
3. 對於 **Type**（類型），選取 **IP Netmask**（IP 網路遮罩），然後輸入 IPv6 首碼以及符合 RFC 6052（/32、/40、/48、/56、/64 或 /96）的網路遮罩。可以是公認首碼或您在 DNS64 伺服器上設定的網路特定首碼。

   在此範例中，輸入 64:FF9B::/96。

   來源和目的地必須有相同的網路遮罩（首碼長度）。

   （您不必輸入完整目的地位址，因為根據首碼長度，防火牆將從傳入封包中的原始目的地 IPv6 位址擷取編碼的 IPv4 位址。在此範例中，傳入封包中的首碼編碼為十六進位的 C633:6401，對應於 IPv4 目的地位址 198.51.100.1。）
4. 按一下 **OK**（確定）。

STEP 3 | （選用）為 IPv6 來源位址建立位址物件（預轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱）。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 IPv6 主機的位址，在此範例中，為 2001:DB8::5/96。
4. 按一下 **OK**（確定）。

STEP 4 | （選用）為 IPv4 來源位址建立位址物件（已轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱）。
3. 對於 **Type**（類型），選取 **IP Netmask**（IP 網路遮罩），然後輸入防火牆輸出介面的 IPv4 位址，在此範例中，為 192.0.2.1。
4. 按一下 **OK**（確定）。

STEP 5 | 建立 NAT64 規則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般） 頁籤上，輸入 NAT64 規則的 **Name**（名稱），例如 nat64_ipv6_init。
3. （選用）輸入 **Description**（說明）。
4. 針對 **NAT Type**（**NAT** 類型），選取 **nat64**。

STEP 6 | 指定原始來源和目的地資訊。

1. 對於 **Original Packet**（原始封包），**Add**（新增）**Source Zone**（來源區域），可以是受信任區域。
2. 選取 **Destination Zone**（目的地區域），在此範例中，為非受信任區域。
3. （選用）選取 **Destination Interface**（目的地介面）或默認值（**any**（任何））。
4. 對於 **Source Address**（來源位址），選取 **Any**（任何），或 **Add**（新增）您為 IPv6 主機建立的位址物件。
5. 對於 **Destination Address**（目的地位址），**Add**（新增）您為 IPv6 目的地建立的位址物件，在此範例中，為 nat64-IPv4 Server。
6. （選用）對於 **Service**（服務），選取 **any**（任何）。

STEP 7 | 指定轉譯的封包資訊。

1. 對於 **Translated Packet**（轉譯的封包），在 **Source Address Translation**（來源位址轉譯）中，為 **Translation Type**（轉譯類型）選取 **Dynamic IP and Port**（動態 **IP** 及連接埠）。
2. 對於 **Address Type**（位址類型），選取以下任何項：
   - 選取 **Translated Address**（轉譯的位址），然後 **Add**（新增）您為 IPv4 來源位址建立的位址物件。
   - 選取 **Interface Address**（介面位址），在這種情況下，轉譯的來源位址為防火牆輸出介面的 IP 位址和網路遮罩。針對此選擇，如果介面具有多個 IP 位址，可選取 **Interface**（介面），並選擇性地輸入 **IP Address**（**IP** 位址）。
3. 不選取 **Destination Address Translation**（目的地位址轉譯）。（防火牆將根據 NAT64 規則的原始目的地中指定的首碼長度，從傳入封包中的 IPv6 首碼擷取 IPv4 位址。）
4. 按一下 **OK**（確定），以儲存 NAT64 原則規則。

STEP 8 | 設定通道介面，以模擬網路遮罩非 128 的回送介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Tunnel**（通道），然後 **Add**（新增） 通道。
2. 針對 **Interface Name**（介面名稱），輸入數值尾碼，例如 .2。
3. 在 **Config**（組態）頁籤上，選取要設定 NAT64 的 **Virtual Router**（虛擬路由器）。
4. 對於 **Security Zone**（安全性區域），選取與 IPv4 伺服器目的地（安全性區域）相關的目的地區域。
5. 在 **IPv6** 頁籤上，選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。
6. 按一下 **Add**（新增），然後對於 **Address**（位址），選取 **New Address**（新位址）。
7. 輸入位址的 **Name**（名稱）。
8. （選用）輸入通道位址的 **Description**（描述）。
9. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 IPv6 首碼和首碼長度，在此範例中，為 64:FF9B::/96。
10. 按一下 **OK**（確定）。
11. 選取**Enable address on interface**（在介面上啟用 **IPv6**），然後按一下 **OK**（確定）。
12. 按一下 **OK**（確定）。
13. 按一下 **OK**（確定）以儲存通道。

STEP 9 | 建立安全性原則，以允許來自受信任區域的 NAT 流量。

1. 選取 **Policies**（原則） > **Security**（安全性），然後**Add**（新增） 規則 **Name**（名稱）。
2. 選取 **Source**（來源），然後 **Add**（新增）**Source Zone**（來源區域）；選取 **Trust**（受信任）。
3. 對於 **Source Address**（來源位址），選取 **Any**（任何）。
4. 選取 **Destination**（目的地），然後 **Add**（新增）**Destination Zone**（目的地區域）；選取 **Untrust**（非受信任）。
5. 對於 **Application**（應用程式），選取 **any**（任何）。
6. 對於 **Actions**（動作），選取 **Allow**（允許）。
7. 按一下 **OK**（確定）。

STEP 10 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

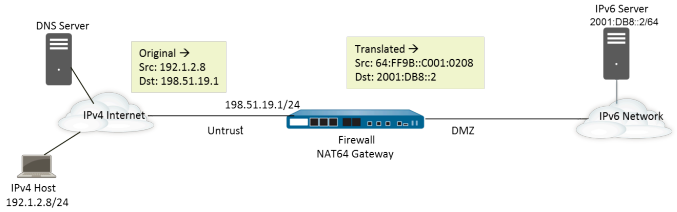
STEP 11 | 進行疑難排解或檢視 NAT64 工作階段。

```
> show session id <session-id>
```

為 IPv4 啟動的通訊設定 NAT64

由 IPv4 啟動的與 IPv6 伺服器之間通訊和與 IPv4 拓撲中目的地 NAT 的通訊類似。目的地 IPv4 位址將透過一對一靜態 IP 轉譯（而非多對一轉譯）對應到目的地 IPv6 位址。

防火牆會將來源 IPv4 位址解碼成 RFC 6052 中定義的公認首碼 64:FF9B::/96。所轉譯的目的地位址為實際的 IPv6 位址。當組織提供從公用非受信任區域存取組織 DMZ 區域內 IPv6 伺服器的權限時，一般會採用 IPv4 啟動的通訊。此拓撲不會使用 DNS64 伺服器。



STEP 1 | 在防火牆上啟用要運作的 IPv6 。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 選取 **Enable IPv6 Firewalling**（啟用 **IPv6** 防火牆）。
3. 按一下 **OK**（確定）。

STEP 2 | （選用）當 IPv4 封包的 DF 位元設定為零（因為 IPv6 不會分割封包），要確保 IPv6 封包不會超出目的地 IPv6 網路的路徑 MTU。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 對於 **NAT64 IPv6 Minimum Network MTU**（NAT64 IPv6 最小網路 MTU），輸入防火牆將 IPv4 封包分割成的最小位元組數（範圍為 1280-9216，預設值為 1280），以便轉譯成 IPv6。

   如果您不希望防火牆在轉譯前分割 *IPv4* 封包，則將該 *MTU* 設定為 *9216*。如果轉譯的 *IPv6* 封包仍然超出此值，防火牆會丟棄封包，並簽發 *ICMP* 封包，指示無法連線目的地，需要分割。
3. 按一下 **OK**（確定）。

STEP 3 | 為 IPv4 目的地位址建立位址物件（預轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_ip4server。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入非受信任區域內的防火牆介面的 IPv4 位址。該位址不得使用任何網路遮罩或僅使用 /32 網路遮罩。此範例將使用 198.51.19.1/32。
4. 按一下 **OK**（確定）。

STEP 4 | 為 IPv6 來源位址建立位址物件（已轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_ip6source。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 NAT64 IPv6 位址以及符合 RFC 6052（/32、/40、/48、/56、/64 或 /96）的網路遮罩。

   在此範例中，輸入 64:FF9B::/96。

   （防火牆使用 IPv4 來源位址 192.1.2.8 將 首碼編碼，其相當於十六進位的 C001:0208。）
4. 按一下 **OK**（確定）。

STEP 5 | 為 IPv6 目的地位址建立位址物件（已轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_server_2。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 IPv6 伺服器的 IPv6 位址（目的地）。該位址不得使用任何網路遮罩或僅使用 /128 網路遮罩。此範例中使用 2001:DB8::2/128。
4. 按一下 **OK**（確定）。

STEP 6 | 建立 NAT64 規則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入 NAT64 規則的 **Name**（名稱），例如 nat64_ipv4_init。
3. 針對 **NAT Type**（**NAT** 類型），選取 **nat64**。

STEP 7 | 指定原始來源和目的地資訊。

1. 對於 **Original Packet**（原始封包），**Add**（新增）**Source Zone**（來源區域），其可能是非受信任區域。
2. 選取 **Destination Zone**（目的地區域），其可能是受信任區域或 DMZ 區域。
3. 對於 **Source Address**（來源位址），選取 **Any**（任何），或為 IPv4 主機 **Add**（新增）位址物件。
4. 對於 **Destination Address**（目的地位址），為 IPv4 目的地 **Add**（新增）位址物件，在此範例中，為 nat64_ip4server。
5. 對於 **Service**（服務），選取 **any**（任何）。

STEP 8 | 指定轉譯的封包資訊。

1. 對於 **Translated Packet**（轉譯的封包），在**Source Address Translation**（來源位址轉譯）中，為 **Translation Type**（轉譯類型）選取 **Static IP**（靜態 **IP**）。
2. 對於 **Translated Address**（轉譯的位址），選取您建立的來源轉譯位址物件 nat64_ip6source。
3. 對於 **Destination Address Translation**（目的地位址轉譯），在 **Translated Address**（轉譯的位址）中，指定單一 IPv6 位址（位址物件，在此範例中為 nat64_server_2，或伺服器的 IPv6 位址）。
4. 按一下 **OK**（確定）。

STEP 9 | 建立安全性原則，以允許來自非受信任區域的 NAT 流量。

1. 選取 **Policies**（原則） > **Security**（安全性），然後**Add**（新增） 規則 **Name**（名稱）。
2. 選取 **Source**（來源），然後 **Add**（新增）**Source Zone**（來源區域）；選取 **Untrust**（非受信任）。
3. 對於 **Source Address**（來源位址），選取 **Any**（任何）。
4. 選取 **Destination**（目的地），然後 **Add**（新增）**Destination Zone**（目的地區域）；選取 **DMZ**。
5. 對於 **Actions**（動作），選取 **Allow**（允許）。
6. 按一下 **OK**（確定）。

STEP 10 | Commit（提交）您的變更。

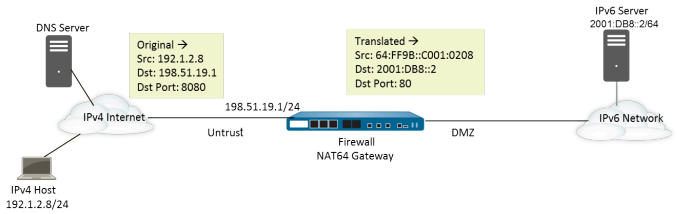
按一下 **Commit**（交付）。

STEP 11 | 進行疑難排解或檢視 NAT64 工作階段。

```
> show session id <session-id>
```


為 IPv4 啟動的與連接埠轉譯的通訊設定 NAT64

此工作建立在為 IPv4 啟動的通訊設定 NAT64的基礎之上，但控制 IPv6 網路的組織更偏向於將公用目的地連接埠號轉譯成內部連接埠號，從而將其與防火牆 IPv4 非受信任端的用戶隔離開。在此範例中，連接埠 8080 將轉譯成連接埠 80。為此，需在 NAT64 原則規則的原始封包中，建立新服務，指定目的地連接埠為 8080。對於轉譯的封包，轉譯連接埠為 80。



STEP 1 | 在防火牆上啟用要運作的 IPv6 。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 選取 **Enable IPv6 Firewalling**（啟用 **IPv6** 防火牆）。
3. 按一下 **OK**（確定）。

STEP 2 | （選用）當 IPv4 封包的 DF 位元設定為零（因為 IPv6 不會分割封包），要確保 IPv6 封包不會超出目的地 IPv6 網路的路徑 MTU。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。
2. 對於 **NAT64 IPv6 Minimum Network MTU**（NAT64 IPv6 最小網路 MTU），輸入防火牆將 IPv4 封包分割成的最小位元組數（範圍為 1280-9216，預設值為 1280），以便轉譯成 IPv6。

   如果您不希望防火牆在轉譯前分割 *IPv4* 封包，則將該 *MTU* 設定為 *9216*。如果轉譯的 *IPv6* 封包仍然超出此值，防火牆會丟棄封包，並簽發 *ICMP* 封包，指示無法連線目的地，需要分割。
3. 按一下 **OK**（確定）。

STEP 3 | 為 IPv4 目的地位址建立位址物件（預轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_ip4server。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入非受信任區域內的防火牆介面的 IPv4 位址和網路遮罩。此範例將使用 198.51.19.1/24。
4. 按一下 **OK**（確定）。

STEP 4 | 為 IPv6 來源位址建立位址物件（已轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_ip6source。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 NAT64 IPv6 位址以及符合 RFC 6052（/32、/40、/48、/56、/64 或 /96）的網路遮罩。

   在此範例中，輸入 64:FF9B::/96。

   （防火牆使用 IPv4 來源位址 192.1.2.8 將 首碼編碼，其相當於十六進位的 C001:0208。）
4. 按一下 **OK**（確定）。

STEP 5 | 為 IPv6 目的地位址建立位址物件（已轉譯）。

1. 選取 **Objects**（物件） > **Addresses**（位址），然後按一下 **Add**（新增）。
2. 輸入物件的 **Name**（名稱），例如 nat64_server_2。
3. 對於 **Type**（類型），選取 **IP Netmask**（**IP** 網路遮罩），然後輸入 IPv6 伺服器的 IPv6 位址（目的地）。此範例中使用 2001:DB8::2/64。

   來源和目的地必須有相同的網路遮罩（首碼長度）。
4. 按一下 **OK**（確定）。

STEP 6 | 建立 NAT64 規則。

1. 選取 **Policies**（原則） > **NAT**，然後按一下 **Add**（新增）。
2. 在 **General**（一般）頁籤上，輸入 NAT64 規則的 **Name**（名稱），例如 nat64_ipv4_init。
3. 針對 **NAT Type**（**NAT** 類型），選取 **nat64**。

STEP 7 | 指定原始來源和目的地資訊，然後建立服務，以限制轉譯為單一輸入連接埠號。

1. 對於 **Original Packet**（原始封包），**Add**（新增）**Source Zone**（來源區域），其可能是非受信任區域。
2. 選取 **Destination Zone**（目的地區域），其可能是受信任區域或 DMZ 區域。
3. 對於 **Service**（服務），選取新 **Service**（服務）。
4. 為服務輸入 **Name**（名稱），例如 Port_8080。
5. 選取 **TCP** 作為 **Protocol**（通訊協定）。
6. 對於 **Destination Port**（目的地連接埠），然後輸入 8080。
7. 按一下 **OK**（確定）以儲存服務。
8. 對於 **Source Address**（來源位址），選取 **Any**（任何），或為 IPv4 主機 **Add**（新增）位址物件。
9. 對於 **Destination Address**（目的地位址），為 IPv4 目的地 **Add**（新增）位址物件，在此範例中，為 nat64_ip4server。

STEP 8 | 指定轉譯的封包資訊。

1. 對於 **Translated Packet**（轉譯的封包），在**Source Address Translation**（來源位址轉譯）中，為 **Translation Type**（轉譯類型）選取 **Static IP**（靜態 **IP**）。
2. 對於 **Translated Address**（轉譯的位址），選取您建立的來源轉譯位址物件 nat64_ip6source。
3. 對於 **Destination Address Translation**（目的地位址轉譯），在 **Translated Address**（轉譯的位址）中，指定單一 IPv6 位址（位址物件，在此範例中為 nat64_server_2，或伺服器的 IPv6 位址）。
4. 將私人目的地 **Translated Port**（轉移連接埠）號指定為防火牆將公用目的地連接埠轉移成的連接埠號，在此範例中，為 80。
5. 按一下 **OK**（確定）。

STEP 9 | 建立安全性原則，以允許來自非受信任區域的 NAT 流量。

1. 選取 **Policies**（原則） > **Security**（安全性），然後**Add**（新增） 規則 **Name**（名稱）。
2. 選取 **Source**（來源），然後 **Add**（新增）**Source Zone**（來源區域）；選取 **Untrust**（非受信任）。
3. 對於 **Source Address**（來源位址），選取 **Any**（任何）。
4. 選取 **Destination**（目的地），然後 **Add**（新增）**Destination Zone**（目的地區域）；選取 **DMZ**。
5. 對於 **Actions**（動作），選取 **Allow**（允許）。
6. 按一下 **OK**（確定）。

STEP 10 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

STEP 11 | 進行疑難排解或檢視 NAT64 工作階段。

```
> show session id <session-id>
```


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擁有四個目的地相同的等價路徑，這可讓防火牆：

- 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。
- 有效使用指向相同目的地相同之連結上的所有可用頻寬，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，而非必須等待路由通訊協定或 RIB 表選擇替代的路徑/路由。當連結失敗時，這可協助縮短停機時間。

所有 Palo Alto Networks® 防火牆型號都支援 ECMP，而 PA-7000 系列、PA-5200 系列、以及 PA-3200 也具有硬體轉送支援。VM 系列防火牆只透過軟體支援 ECMP。無法執行硬體卸載的工作階段效能會受到影響。

Layer 3、Layer 3 子介面、VLAN、通道和彙總乙太網路介面都支援 ECMP。

您可以針對靜態路由和防火牆支援的任何動態路由通訊協定設定 ECMP。

由於路由表容量是以路徑數為基礎，而具有四個路徑 ECMP 路由會耗用路由表容量的四個項目，因此 ECMP 會影響路由表容量。由於以工作階段為基礎的標籤將流量對應至特定介面時會使用較多記憶體，因此 ECMP 實作可能會稍微降低路由表容量。

使用靜態路由的虛擬路由器對虛擬路由器路由不支援 ECMP。

如需 HA 對等失敗時選取 ECMP 路徑的相關資訊，請參閱 在主動/主動 HA 模式下的 ECMP。

以下幾節說明 ECMP 及如何對其進行設定。

- ECMP 負載平衡演算法
- 在虛擬路由器上設定 ECMP
- 針對多個 BGP 自發系統啟用 ECMP
- 驗證 ECMP

ECMP 負載平衡演算法

假設防火牆的路由資訊庫 (RIB) 具有指向單一目的地的多個等價路徑。等價路徑數上限預設為 2。ECMP 會從 RIB 選擇兩個最佳的等價路徑，以複製到轉送資訊庫 (FIB)。然後 ECMP 會根據負載平衡方法，從 FIB 中的兩個路徑中選擇，決定防火牆要在此工作階段期間用於目的地的路徑。

系統會在工作階段層級（而非封包層級）完成 ECMP 負載平衡，防火牆 (ECMP) 選擇等價路徑時，便會開始新的工作階段。系統會將指向單一目的地的等價路徑視為 ECMP 路徑成員或 ECMP 群組成員。ECMP 會根據您設定的負載平衡演算法，從指向 FIB 目的地的多個路徑中選擇，決定要用於 ECMP 流量的路徑。虛擬路由器只能使用一個負載平衡演算法。

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。

四個演算法選擇分別強調不同的優先順序，如下所述：

- 以雜湊為基礎的演算法可設定工作階段綁定的優先順序—**IP Modulo**（**IP** 模數）和 **IP Hash**（**IP** 雜湊）演算法會根據封包標頭中的資訊（例如來源和目的地位址）使用雜湊。由於指定工作階段中每個流量的標頭都包含相同的來源和目的地資訊，因此這些選項會設定工作階段綁定的優先順序。如果您選取 **IP Hash**（**IP** 雜湊） 演算法，雜湊可以基於來源和目的地位址，也可以僅基於來源位址。使用僅基於來源位址的 IP 雜湊，會使屬於相同來源 IP 位址的所有工作階段一直從可用的多個路徑中選取相同的路徑。因此，該路徑被認為有黏性，在必要時更容易進行疑難排解。您可以選擇性地設定 **Hash Seed**（雜湊種子）值；如果您具有指向相同目的地的大量工作階段，且未在 ECMP 連結之間平均散佈這些工作階段，則可藉此進一步隨機處理負載平衡。
- 平衡演算法可設定負載平衡的優先順序—**Balanced Round Robin**（平衡循環配置資源）演算法會在連結之間平均散佈傳入的工作階段，並偏好在工作階段綁定之間負載平衡。（循環配置資源表示最近選擇項目的選擇順序。） 此外，如果在 ECMP 群組中新增或移除路由（例如，如果群組中的路徑停擺），虛擬路由器會在群組中的連結之間重新平衡工作階段。此外，如果工作階段中的流量因中斷而必須交換路由，當與工作階段相關聯的原始路由再次變為可用，且虛擬路由器再次重新平衡負載時，工作階段中的流量會還原至原始路由。
- 加權演算法可設定連結容量和/或速度的優先順序—作為 ECMP 通訊協定標準的延伸模組，Palo Alto Networks® 實作提供 **Weighted Round Robin**（加權循環配置資源）負載平衡選項，其會考量防火牆的輸出介面上不同的連結容量和速度。您可以透過此選項，使用連結容量、速度和延遲等因素，根據連結效能將 **ECMP Weights**（**ECMP** 權數）（範圍是 1 至 255；預設值是 100）指派給介面，以確保負載平衡並充分利用可用的連結。

  例如，假設防火牆具有指向 ISP 的備援連結：ethernet1/1 (100 Mbps) 和 ethernet1/8 (200 Mbps)。雖然這些是等價路徑，但透過 ethernet1/8 的連結可提供更大的頻寬，且因此可以處理比 ethernet1/1 連結更大的負載。因此，若要確保負載平衡功能考量連結容量和速度，您可以將權數 200 指派給 ethernet1/8，並將權數 100 指派給 ethernet1/1。2:1 的權數比例會讓虛擬路由器將傳送至 ethernet1/1 的工作階段數兩倍的工作階段傳送至 ethernet1/8。但是，由

於 ECMP 通訊協定以工作階段為基礎的本質，使用 **Weighted Round Robin**（加權循環配置資源）演算法時，防火牆只能盡量在 ECMP 連結之間負載平衡。

請記住，將 ECMP 權數指派給介面的目的是決定負載平衡（以影響選擇的等價路徑），而非路由選擇（從可能具有不同成本的路由中選擇路由）。

請以較小的權數指派速度較慢或容量較低的連結。並以較大的權數指派速度較快或容量較高的連結。透過這種方式，防火牆可以根據這些比例來散佈工作階段，而非過度使用作為其中一個等價路徑的低容量連結。

在虛擬路由器上設定 ECMP

請使用下列程序在虛擬路由器上啟用 ECMP。先決條件如下所述：

- 指定屬於虛擬路由器的介面（**Network**（網路） > **Virtual Routers**（虛擬路由器） > **Router Settings**（路由器設定） > **General**（一般））。
- 指定 IP 路由通訊協定。

啟用、停用或變更現有虛擬路由器的 ECMP 會造成系統重新啟動虛擬路由器，這可能會造成工作階段終止。

STEP 1 | 針對虛擬路由器啟用 ECMP。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取要啟用 ECMP 的虛擬路由器。
2. 選取 **Router Settings**（路由器設定） > **ECMP**，然後選取 **Enable**（啟用）。

STEP 2 | （選用）啟用從伺服器將封包對稱傳回至用戶端。

選取 **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。也就是防火牆將使用傳送傳回封包的輸入介面，而非使用 ECMP 介面。**Symmetric Return**（對稱傳回）設定會取代負載平衡。只有從伺服器到用戶端的流量會發生此行為。

STEP 3 | 啟用 **Strict Source Path**（嚴格來源路徑），以確保源自防火牆的 IKE 和 IPSec 流量從 IPSec 通道的來源 IP 位址所屬的實體介面輸出。

啟用 ECMP 時，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。或者，透過啟用嚴格來源路徑，您可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，可以啟用此功能。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 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，RPF 檢查成功，且 ISP 允許回程流量。

STEP 4 | 將可從路由資訊庫 (RIB) 複製（指向目的地網路）的等價路徑數上限指定給轉送資訊庫 (FIB)。

針對允許的 **Max Path**（路徑上限），輸入 **2**、**3** 或 **4**。預設值：2.

STEP 5 | 選取虛擬路由器的負載平衡演算法。如需負載平衡方法及其之間差異的詳細資訊，請參閱 ECMP 負載平衡演算法 。

針對 **Load Balance**（負載平衡），從 **Method**（方法）清單中選取下列其中一個選項：

- **IP** 模數（預設）—使用封包標頭中的來源和目的地 IP 位址的雜湊，以決定要使用哪個 ECMP 路由。
- **IP** 雜湊—有兩種 IP 雜湊方法可用於確定要使用的 ECMP（在步驟 5 中選取雜湊選項）：
  - 使用來源位址的雜湊（PAN-OS 8.0.3 及更新版本中可用）。
  - 使用來源和目的地 IP 位址的雜湊（預設的 IP 雜湊方法）。
- 平衡循環配置資源—在 ECMP 之間使用循環配置資源，並在路徑數變更時重新平衡路徑。
- 加權循環配置資源—使用循環配置資源和相對權數從 ECMP 路徑之間選取。在下方步驟 6 中指定權數。

STEP 6 | （僅限 IP 雜湊） 設定 IP 雜湊選項。

如果您已選取 **IP Hash**（**IP** 雜湊）作為 **Method**（方法）：

1. 如果您要確保所有屬於相同來源 IP 位址的所有工作階段始終從可用的多個路徑中選取相同的路徑，則選取 **Use Source Address Only**（僅使用來源位址）（在PAN-OS 8.0.3 及更新版本中可用）。IP 雜湊選項提供了路徑粘性，簡化了疑難排解。如果您不選取此選項或者您使用 PAN-OS 8.0.3 之前的版本，IP 雜湊將使用來源和目的地 IP 位址（預設的 IP 雜湊方法）。

   如果您選取 ***Use Source Address Only***（僅使用來源位址），則不得從 *Panorama* 向執行 *PAN-OS 8.0.2*、*8.0.1* 或 *8.0.0* 的防火牆推送組態。

2. 若要在 **IP Hash**（**IP** 雜湊）計算中使用來源或目的地連接埠號碼，請選取 **Use Source/Destination Ports**（使用來源/目的地連接埠）。

   啟用此選項和 ***Use Source Address Only***（僅使用來源位址）將會使路徑的選擇隨機化，即使對於屬於相同來源 *IP* 位址的工作階段也是如此。

3. 輸入 **Hash Seed**（雜湊種子）值（最多九位數的整數）。指定 **Hash Seed**（雜湊種子）值以進一步隨機處理負載平衡。如果您擁有 Tuple 資訊相同的大量工作階段，則指定雜湊種子值非常實用。

STEP 7 | （僅限 Weighted Round Robin（加權循環配置資源））在 ECMP 群組中定義每個介面的權數。

如果您已選取 **Weighted Round Robin**（加權循環配置資源）作為 **Method**（方法），請針對作為要路由至相同目的地之流量輸出點的介面，定義每個介面的權數（也就是作為 ECMP 群組一部分的介面，例如為 ISP 提供備援連結的介面或企業網路核心業務應用程式的介面）。

權數愈大，便會愈常為新的工作階段選取該等價路徑。

向速度較快之連結指定的權數應該比速度較慢之連結更大，讓更多的 *ECMP* 流量經過較快的連結。

1. 按一下 **Add**（新增），並選取 **Interface**（介面），以建立 ECMP 群組。
2. 在 ECMP 群組中 **Add**（新增）其他介面。
3. 按一下 **Weight**（權數）並指定每個介面的相對權數（範圍是 1-255；預設值是 100）。

STEP 8 | 儲存組態。

1. 按一下 **OK**（確定）。
2. 根據 ECMP 組態變更提示，按一下 **Yes**（是）以重新啟動虛擬路由器。重新啟動虛擬路由器可能會造成現有工作階段終止。

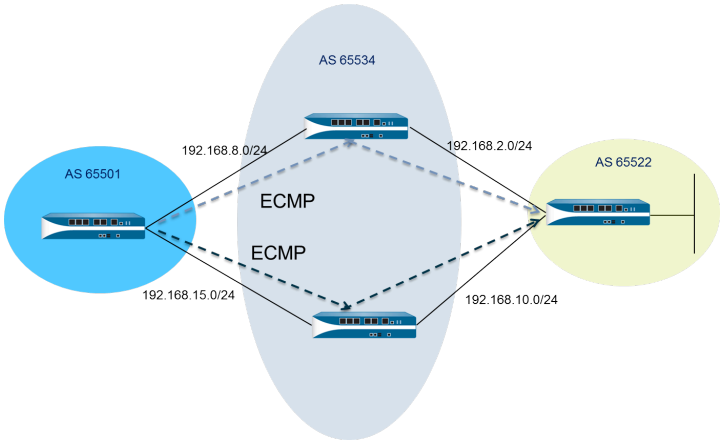
只有在透過 *ECMP* 修改現有虛擬路由器時，才會顯示此訊息。

STEP 9 | Commit（提交）您的變更。

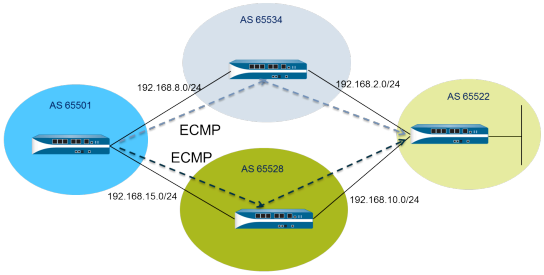
Commit（提交）組態。

針對多個 BGP 自發系統啟用 ECMP

如果您已設定 BGP，且想要在多個自發系統之間啟用 ECMP，請執行下列工作。此工作假設已設定 BGP。在下圖中，兩個指向目的地的 ECMP 路徑會通過屬於單一 BGP 自發系統中單一 ISP 的兩個防火牆。



在下圖中，兩個指向目的地的 ECMP 路徑會通過屬於不同 BGP 自發系統中兩個不同 ISP 的兩個防火牆。



STEP 1 | 設定 ECMP。

請參閱在虛擬路由器上設定 ECMP。

STEP 2 | 針對 BGP 路由，在多個自發系統之間啟用 ECMP。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取要針對多個 BGP 自發系統啟用 ECMP 的虛擬路由器。
2. 選取 **BGP** > **Advanced**（進階），然後選取 **ECMP Multiple AS Support**（**ECMP** 多 **AS** 支援）。

STEP 3 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

驗證 ECMP

針對 ECMP 設定的虛擬路由器會表示轉送資訊庫 (FIB) 表格中的哪些路由是 ECMP 路由。路由的 ECMP 旗標 (E) 表示其參與指向該路由下一個躍點的輸出介面 ECMP。若要驗證 ECMP，可使用下列程序查看 FIB，並確認某些路由是否為等價多路徑。

STEP 1 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。

STEP 2 | 在啟用 ECMP 的虛擬路由器列中，按一下 **More Runtime Stats**（更多執行階段統計資料）。

STEP 3 | 選取 **Routing**（路由） > **Forwarding Table**（轉送表）以查看 FIB。

在該表中，指向相同目的地的多個路由（來自不同介面）都具有「*E*」旗標。星號「*」代表 *ECMP* 群組的偏好路徑。

LLDP

Palo Alto Networks 防火牆® 支援連結層探索通訊協定 (LLDP)，該通訊協定可在連結層上運作，以探索鄰近裝置及其功能。LLDP 允許防火牆及其他網路設備和芳鄰之間傳送與接收 LLDP 資料單位 (LLDPDU)。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 讓疑難排解變得更容易，尤其是 Virtual Wire 部署，因為在此部署中，通常無法透過 ping 或路徑追蹤偵測防火牆。

LLDP 概要

連結層發現協定 (LLDP) 使用 MAC 位址在 OSI 模型的 Layer 2 執行。LLDPDU 是一系列在乙太網路框架中封裝的類型長度值 (TLV) 元素。IEEE 802.1AB 標準為 LLDPDU 定義三個 MAC 位址：01-80-C2-00-00-0E、01-80-C2-00-00-03 和 01-80-C2-00-00-00。

Palo Alto Networks® 防火牆針對傳輸和接收 LLDP 資料單位，只支援一個 MAC 位址：01-80-C2-00-00-0E。傳輸時，防火牆會使用 01-80-C2-00-00-0E 作為目的地 MAC 位址。接收時，防火牆會使用 01-80-C2-00-00-0E 作為目的地 MAC 位址來處理資料包。如果防火牆在其介面上收到 LLDPDU 的其他兩個 MAC 位址，防火牆會在執行此功能之前，採取相同的轉送動作，如下所述：

- 如果介面類型為 vwire，防火牆會將資料包轉送至其他連接埠。
- 如果介面類型為 L2，防火牆會將資料包傳輸至其餘的 VLAN。
- 如果介面類型為 L3，防火牆會丟棄資料包。

不支援 Panorama 與 WildFire 設備。

不支援 LLDP 的介面類型為 TAP、高可用性 (HA)、解密鏡像、Virtual Wire/vlan/L3 子介面，以及 PA-7000 系列日誌處理卡 (LPC) 介面。

LLDP 乙太網路框架具有下列格式：

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLVs	End of LLDPDU TLV	Frame Check Sequence
	01:80:C2:00:00:0E or 01:80:C2:00:00:03 or 01:80:C2:00:00:00	Station's Address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

在 LLDP 乙太網路框架中，TLV 結構具有下列格式：

TLV Type	TLV Information String Length	TLV Information String
7 bits	9 bits	0-511 octets

在 LLDP 中支援的 TLV

LLDPDU 包含必要和選用 TLV。下表列出防火牆支援的必要 TLV：

必要 **TLV**	**TLV** 類型	說明
底座 ID TLV	1	識別防火牆底座。每個防火牆都必須只能擁有一個唯一底座 ID。Palo Alto Networks® 型號上的底座 ID 子類型為 4（MAC 位址），且會使用 MAC 位址 Eth0 以確保唯一性。
連接埠 ID TLV	2	識別傳送 LLDPDU 的連接埠。每個防火牆都會針對每個傳輸的 LLDPDU 訊息，使用一個連接埠 ID。連接埠 ID 子類型為 5（介面名稱），且會唯一識別傳輸連接埠。防火牆會使用介面的 ifname 作為連接埠 ID。
存留時間 (TTL) TLV	3	指定從對等收到的 LLDPDU 資訊在本機防火牆中保持有效的長度（單位秒數）（範圍是 0-65,535）。該值是 LLDP 保留時間的乘數。TTL 值為 0 時，與設備相關聯的資訊便不再有效，且防火牆會從 MIB 中移除該項目。
LLDPDU TLV 結尾	0	在 LLDP 乙太網路框架中表示 TLV 的結尾。

下表列出 Palo Alto Networks 防火牆支援的選用 TLV：

選用 **TLV**	**TLV** 類型	關於防火牆實作的目的和註記
連接埠說明 TLV	4	以字母數字格式說明防火牆的連接埠。使用 ifAlias 物件。
系統名稱 TLV	5	以字母數字格式設定的防火牆名稱。使用 sysName 物件。
系統說明 TLV	6	以字母數字格式說明防火牆。使用 sysDescr 物件。
系統功能	7	說明介面的部署模式，如下所述： · 透過路由器（位元 6）功能與「其他」位元（位元 1）宣告 L3 介面。 · 透過 MAC 橋接器（位元 3）功能與「其他」位元（位元 1）宣告 L2 介面。 · 透過重複器（位元 2）功能與「其他」位元（位元 1）宣告虛擬介接介面。
管理位址	8	用於防火牆管理的一或多個 IP 位址，如下所述： · 管理 (MGT) 介面的 IP 位址

選用 **TLV**	**TLV** 類型	關於防火牆實作的目的和註記
		· 介面的 IPv4 和/或 IPv6 位址 · 回送位址 · 在管理位址欄位中輸入的使用者定義位址 如果未提供管理 IP 位址，則預設會使用傳輸介面的 MAC 位址。 其中包含已指定管理位址的介面號碼。以及已指定管理位址指定的硬體介面 OID（如果適用）。 如果已指定多個管理位址，系統會從清單頂端開始，依其指定順序傳送這些位址。支援最多四個管理位址。 此為選用參數且可保留為停用。

LLDP Syslog 訊息和 SNMP 設陷

防火牆會在 SNMP 管理員可監控的 MIB 中儲存 LLDP 資訊。如果您想讓防火牆傳送關於 LLDP 事件的 SNMP 設陷通知和 syslog 訊息，則必須在 LLDP 設定檔中啟用 **SNMP Syslog Notification**（**SNMP Syslog** 通知）。

根據 RFC 5424 Syslog 通訊協定和 RFC 1157 簡易網路管理通訊協定，發生 MIB 變更時，LLDP 會傳送 syslog 和 SNMP 設陷訊息。**Notification Interval**（通知間隔）會以速率限制這些訊息，該 LLDP 全域設定預設為 5 秒且可設定。

由於 LLDP syslog 和 SNMP 設陷訊息具有速率限制，因此提供給這些程序的某些 LLDP 資訊可能與您檢視 LLDP 狀態資訊時看到的目前 LLDP 統計資料不相符。這是正常的預期行為。

每個介面（乙太網路或 AE）可收到最多 5 個 MIB。每個不同的來源都具有一個 MIB。如果超過限制，則會觸發錯誤訊息 `tooManyNeighbors`。

設定 LLDP

若要設定 LLDP 並建立 LLDP 設定檔，您必須是超級使用者或裝置管理員 (deviceadmin)。防火牆介面支援最多五個 LLDP 端點。

STEP 1 | 在防火牆上啟用 LLDP。

選取 **Network**（網路） > **LLDP**，然後編輯 LLDP General（一般）區段；選取 **Enable**（啟用）。

STEP 2 | (選用) 變更 LLDP 全域設定。

1. 針對 **Transmit Interval (sec)**（傳輸間隔（秒）），指定 LLDPDU 傳輸的間隔 (單位秒數)。範圍是 1 至 3600；預設值為 30。
2. 針對 **Transmit Delay (sec)**（傳輸延遲（秒）），指定在 TLV 元素進行變更後，傳送 LLDP 傳輸之間的延遲時間（單位秒數）。如果許多網路變更讓 LLDP 變更數達到高點，或是介面擺動，則延遲可協助防止 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 至 600；預設值為 2。
3. 針對 **Hold Time Multiple**（保留時間乘數），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 至 100；預設值為 4。無論乘數值為何，TTL 保留時間上限為 65535 秒。
4. 對於 **Notification Interval**（通知間隔），指定發生 MIB 變更時，傳輸 LLDP Syslog 訊息及 SNMP 設陷的間隔（單位為秒）。範圍是 1 至 3600；預設值為 5。
5. 按一下 **OK**（確定）。

STEP 3 | 建立 LLDP 設定檔。

關於可選 TLV 的描述，請參閱 LLDP 中支援的 TLV。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **LLDP Profile**（**LLDP** 設定檔），然後為 LLDP 設定檔 **Add**（新增）**Name**（名稱）。
2. 針對 **Mode**（模式），選取 **transmit-receive**（傳輸-接收）（預設）、**transmit-only**（傳輸-接收）或 **receive-only**（僅接收）。
3. 按一下 **SNMP Syslog Notification**（**SNMP Syslog** 通知），以啟用 SNMP 通知和 Syslog 訊息。如果已啟用，則會使用全域 **Notification Interval**（通知間隔）。防火牆會依照 **Device**（裝置） > **Log Settings**（日誌設定） > **System**（系統） > **SNMP Trap**

Profile（**SNMP** 設陷設定檔） 與 **Syslog Profile**（**Syslog** 設定檔） 的設定，傳送 SNMP 設陷與 Syslog 事件。

4. 對於可選的 TLV，選取您要傳輸的 TLV：
   - 連接埠說明
   - 系統名稱
   - 系統說明
   - 系統功能
5. （選用）選取 **Management Address**（管理位址）以新增一個或多個管理位址，並 **Add**（新增）一個**Name**（名稱）。
6. 選取要從其取得管理位址的 **Interface**（介面）。如果已啟用 **Management Address**（管理位址）TLV，則需要至少一個管理位址。如果未設定管理 IP 位址，則系統會使用傳輸介面的 MAC 位址作為管理位址 TLV。
7. 選取 **IPv4** 或 **IPv6**，在相鄰的欄位中，從清單（其中列出在選取的介面上設定的位址）中選取 IP 位址或輸入位址。
8. 按一下 **OK**（確定）。
9. 允許使用最多四個管理位址。如果您指定多個 **Management Address**（管理位址），系統會從清單頂端開始，依其指定順序傳送這些位址。若要變更位址的順序，請選取位址，並使用 **Move Up**（上移）或 **Move Down**（下移）按鈕。
10. 按一下 **OK**（確定）。

STEP 4 | 將 LLDP 設定檔指派給介面。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取要指派 LLDP 設定檔的介面。
2. 選取 **Advanced**（進階） > **LLDP**。
3. 選取 **Enable LLDP**（啟用 **LLDP**），將 LLDP 設定檔指派給介面。
4. 針對 **Profile**（設定檔），選取您已建立的設定檔。選取 **None**（無）會啟用具有基本功能的 LLDP：傳送三個必要 TLV 並啟用 **transmit-receive**（傳輸-接收）模式。

   若要建立新設定檔，請按一下 **LLDP Profile**（**LLDP** 設定檔），並依照上述步驟的說明執行。
5. 按一下 **OK**（確定）。

STEP 5 | **Commit**（提交）您的變更。

檢視 LLDP 設定和狀態

執行下列程序可檢視 LLDP 設定和狀態。

STEP 1 | 檢視 LLDP 全域設定。

選取 **Network**（網路） > **LLDP**。

在 LLDP 一般畫面上，**Enable**（啟用）表示是否已啟用 LLDP。

- 如果已啟用 LLDP，則會顯示已設定的全域設定（傳輸間隔、傳輸延遲、保留時間乘數和通知間隔）。
- 如果未啟用 LLDP，則會顯示全域設定的預設值。

關於這些值的說明，請參閱設定 LLDP。

STEP 2 | 檢視 LLDP 狀態資訊。

1. 選取 **Status**（狀態）頁籤。
2. （選用）輸入篩選器以限制顯示的資訊。

介面資訊：

- 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。
- 設定檔—指派給介面的設定檔名稱。

傳輸資訊：

- 傳輸總數—傳出介面的 LLDPDU 計數。
- 已丟棄的傳輸—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。

接收資訊：

- 接收總數—介面上收到的 LLDP 框架計數。
- 已丟棄的 **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 TLV 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—在介面上收到且 LLDP 本機代理程式無法辨識的 TLV 計數。例如，TLV 類型在保留的 TLV 範圍中。
- 過時—因為適當的 TTL 到期而從「接收 MIB」刪除的項目計數。

STEP 3 | 檢視在介面上看到之每個芳鄰的摘要 LLDP 資訊。

1. 選取 **Peers**（對等）頁籤。
2. (選用) 輸入篩選器以限制顯示的資訊。

本機介面—偵測到相鄰裝置的防火牆介面。

遠端底座 **ID**—對等的底座 ID。將使用的 MAC 位址。

連接埠 **ID**—對等的連接埠 ID。

名稱—對等名稱。

更多資訊—提供下列遠端對等詳細資訊（視 TLV 為必要與選用而定）：

- 底座類型：MAC 位址。
- MAC 位址：對等的 MAC 位址。
- 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
- 啟用的功能：對等上啟用的功能。
- 管理位址：對等的管理位址。

清除 LLDP 統計資料

您可以清除特定介面的 LLDP 統計資料。

清除特定介面的 LLDP 統計資料。

1. 選取 **Network**（網路） > **LLDP** > **Status**（狀態），然後在左方欄中選取一或多個要清除 LLDP 統計資料的介面。
2. 按一下畫面底端的 **Clear LLDP Statistics**（清除 **LLDP** 統計資料）。

BFD

防火牆支援雙向轉送偵測 (BFD) (RFC 5880)，這是一種通訊協定，可識別兩個路由對等之間雙向路徑中的失敗。BFD 失敗偵測速度極快，相較於透過連結監控或諸如您好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。要求可用性及極快故障復原的高關鍵任務資料中心和網路，需要 BFD 提供的極快失敗偵測。

BFD 概要

當您啟用 BFD 時，BFD 會使用三方交握從一個端點（防火牆）到其位於連結對等的 BFD 對等之間建立一個工作階段。控制封包會執行交握並交涉 BFD 設定檔中設定的參數，包括對等可傳送並接收控制封包的最小間隔。IPv4 和 IPv6 的 BFD 控制封包是透過 UDP 連接埠 3784 傳輸。多重躍點支援的 BFD 控制封包是透過 UDP 連接埠 4784 傳輸。透過以上任何連接埠傳輸的 BFD 控制封包以 UDP 封包封裝。

在建立 BFD 工作階段後，Palo Alto Networks® 實作 BFD 會在異步模式下進行，意味著兩個端點會以交涉的間隔互傳控制封包 （像您好封包那樣運作）。如果對等不在偵測時間（計算方法是交涉傳輸間隔乘以偵測時間乘數）內接收控制封包，對等會認為工作階段已關閉。（防火牆不支援要求模式，在要求模式下，控制封包僅在必要時而非定期傳送。）

當您為靜態路由啟用 BFD 並且防火牆與 BFD 對等之間的 BFD 工作階段失敗時，防火牆將從 RIB 及 FIB 表中移除失敗的路由並允許較低優先順序的替代路徑來接管。在為路由通訊協定啟用 BFD 後，BFD 會通知路由通訊協定切換至其他對等路徑。因此，防火牆和 BFD 對等會在新路徑上重新匯聚。

BFD 設定檔允許您設定 BFD 設定，將其套用到防火牆上的一個或多個路由通訊協定或靜態路由。如果您在不組態設定檔的情況下啟用 BFD，防火牆會使用其預設 BFD 設定檔（及其所有預設設定）。您無法變更預設 BFD 設定檔。

當介面執行使用其他 BFD 設定檔的多個通訊協定時，BFD 會使用具有最低 **Desired Minimum Tx Interval**（所需最小 **Tx** 間隔）的設定檔。請參閱適用於動態路由通訊協定的 BFD。

主動/被動 HA 對等會同步 BFD 組態及工作階段；主動/主動 HA 對等則不會。

BFD 可於 RFC 5880 中標準化。PAN-OS 不支援 RFC 5880 的所有元件；請參閱 BFD 的不受支援的 RFC 元件。

PAN-OS 還支援 RFC 5881，www.rfc-editor.org/rfc/rfc5881.txt。在此情況下，BFD 會追蹤兩個使用 IPv4 或 IPv6 的系統之間的單躍點，因此兩個系統會直接互連。BFD 還會從 BGP 連接的對等追蹤多個躍點。PAN-OS 遵循 BFD 封裝，如 RFC 5883，www.rfc-editor.org/rfc/rfc5883.txt 中所述。但是，PAN-OS 不支援驗證。

- BFD 型號、介面和用戶端支援
- BFD 的不受支援的 RFC 元件
- 適用於靜態路由的 BFD
- 適用於動態路由通訊協定的 BFD

BFD 型號、介面和用戶端支援

以下防火牆型號不支援 BFD：PA-800 系列、PA-220 以及 VM-50 防火牆。支援 BFD 的型號支援最大數目的 BFD 工作階段，如產品選擇工具中所列。

BFD 可在實體乙太網路、彙總乙太網路 (AE)、VLAN 和通道介面（站對站 VPN 和 LSVPN）以及 Layer 3 子介面上執行。

支援的 BFD 用戶端包括：

- 由單躍點組成的靜態路由（IPv4 和 IPv6）

- OSPFv2 和 OSPFv3（介面類型包括廣播、點對點和單點對多點）
- 由單躍點或多重躍點組成的 BGP IPv4 和 IPv6 (IBGP、EBGP)
- RIP（單躍點）

BFD 的不受支援的 RFC 元件

- 要求模式
- 驗證
- 傳送或接收回應封包；但是，防火牆會傳送到達虛擬連接或旁接介面的回應封包。（對於來源或目的地，BFD 回應封包具有相同的 IP 位址。）
- 輪詢序列
- 擁塞控制

適用於靜態路由的 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都必須支援 BFD 工作階段。靜態路由僅在 **Next Hop**（下一個躍點）類型為 **IP Address**（**IP** 位址）時才有 BFD 設定檔。

如果介面設定有多個靜態路由至對等（BFD 工作階段具有相同的來源 IP 位址和相同的目的地 IP 位址），則單一 BFD 工作階段會自動處理多個靜態路由。此行為會減少 BFD 工作階段。若靜態路由具有不同的 BFD 設定檔，則具有最小 **Desired Minimum Tx Interval**（所需最小 **Tx** 間隔）的設定檔生效。

在要在 DHCP 或 PPPoE 用戶端介面上為靜態路由設定 BFD 的部署中，必須執行兩次提交。為靜態路由啟用 BFD 要求 **Next Hop**（下一個躍點）類型必須為 **IP Address**（**IP** 位址）。但在 DHCP 或 PPPoE 介面提交時，介面 IP 位址與下一個躍點 IP 位址（預設閘道）不明。

您必須先為此介面啟用 DHCP 或 PPPoE 用戶端、執行提交並等待 DHCP 或 PPPoE 伺服器向防火牆傳送用戶端 IP 位址和預設閘道 IP 位址。然後，您可以設定靜態路由（使用 DHCP 或 PPPoE 用戶端的預設閘道位址作為下一個躍點）、啟用 BFD 並執行第二次提交。

適用於動態路由通訊協定的 BFD

除了適用於靜態路由的 BFD 外，防火牆還針對 BGP、OSPF 和 RIP 路由通訊協定支援 BFD。

Palo Alto Networks® 實作多重躍點 *BFD* 遵循 RFC 5883，適用於多重躍點路徑的雙向轉送偵測 (BFD) 的封裝部分，但不支援驗證。一種權宜方案是在 *VPN* 通道中為 *BGP* 設定 *BFD*。*VPN* 通道可在不重複 *BFD* 驗證的情況下提供驗證。

當您為 OSPFv2 或 OSPFv3 廣播介面啟用 BFD 時，OSPF 會僅與指定路由器 (DR) 及備份指定路由器 (BDR) 建立一個 BFD 工作階段。在點對點介面上，OSPF 會與直接連線之芳鄰建立一個 BFD 工作階段。在單點對多點介面上，OSPF 會與每個對等建立一個 BFD 工作階段。

防火牆不在 OSPF 或 OSPFv3 虛擬連結上支援 BFD。

每個路由通訊協定可擁有介面上的獨立 BFD 工作階段。或者，兩個或以上的路由通訊協定（BGP、OSPF 和 RIP）可共用介面上的一個 BFD 工作階段。

如果在相同介面上為多個通訊協定啟用 BFD 並且通訊協定的來源 IP 位址與目的地 IP 位址也相同，這些通訊協定會共用單個 BFD 工作階段，因此降低介面上的資料平面負荷 (CPU) 以及流量負載。如果您為這些通訊協定設定不同的 BFD 設定檔，則僅使用一個 BFD 設定檔：具有最低 **Desired Minimum Tx Interval**（所需最小 **Tx** 間隔）的設定檔。如果設定檔具有相同的 **Desired Minimum Tx Interval**（所需最小 **Tx** 間隔），首先建立的工作階段使用的設定檔生效。在靜態路由與 OSPF 共用相同工作階段的情況下，由於靜態工作階段是在提交後馬上建立，而 OSPF 等到相鄰項開啟，因此靜態路由的設定檔生效。

在這些情況下使用單一 BFD 工作階段的益處是，此行為可更高效地使用資源。防火牆可以使用節省的資源來在不同介面上支援多個 BFD 工作階段或者針對不同的來源 IP 與目的地 IP 位址對支援 BFD。

相同介面上的 IPv4 和 IPv6 一律建立不同的 BFD 工作階段，即使它們可以使用相同的 BFD 設定檔。

如果您同時實作 *BGP BFD* 和 *HA* 路徑監控，*Palo Alto Networks* 建議您不要實作 *BGP Graceful Restart*（非失誤性重新啟動）。當 *BFD* 對等體的介面出現故障並且路徑監控也出現故障時，*BFD* 可以從路由表中移除受影響的路由，並在非失誤性重新啟動生效前，將此變更同步到被動 *HA* 防火牆。如果您決定實作 *BGP BFD*、*BGP* 非失誤性重新啟動和 *HA* 路徑監控，則應為 *BFD* 設定大於預設值的 *Desired Minimum Tx Interval*（所需最小 *Tx* 間隔）和 *Detection Time Multiplier*（偵測時間乘數）。

設定 BFD

在您閱讀 BFD 概要（包含支援的防火牆型號與介面）後，先執行以下步驟，再設定 BFD：

- 設定一個或多個虛擬路由器。
- 如果您將 BFD 套用到靜態路由，則設定一個或多個靜態路由。
- 如果您將 BFD 套用到路由通訊協定，則設定路由通訊協定（BGP、OSPF、OSPFv3 或 RIP）。

BFD 實作的效力取決於多種要素，例如流量負載、網路條件、*BFD* 設定的積極程度以及資料平面的繁忙程度。

STEP 1 | 建立 BFD 設定檔。

若您變更 *BFD* 設定檔中現有 *BFD* 工作階段正在使用的設定並提交變更，然後防火牆刪除該 *BFD* 工作階段並使用新設定建立它，防火牆會傳送一個本機狀態設為 *admin down* 的 *BFD* 封包。對等體裝置不一定會拍動路由通訊協定或靜態路由，取決於對等體實作 RFC 5882，*3.2* 部分。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **BFD Profile**（**BFD** 設定檔），然後為 BFD 設定檔 **Add**（新增）**Name**（名稱）。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。
2. 選擇 BFD 的運作 **Mode**（模式）：
   - 主動—BFD 啟動向對等體傳送控制封包（預設）。至少其中一個 BFD 對等體必須為主動；可都為主動。
   - 被動—BFD 等候對等體傳送控制封包並視需回應。

STEP 2 | 設定 BFD 間隔。

1. 輸入 **Desired Minimum Tx Interval (ms)**（所需最小 **Tx** 間隔（毫秒））。這是您希望 BFD 通訊協定（稱為 BFD）傳送 BFD 控制封包的最小間隔（以毫秒計）；您因此會與對等體交涉傳輸間隔。PA-7000 和 PA-5200 系列防火牆的最小間隔為 50；VM 系列防火牆的最小間隔為 200。最大值為 2,000；預設值為 1,000。

   建議將 *PA-7000* 系列防火牆的 ***Desired Minimum Tx Interval***（所需最小 ***Tx*** 間隔）設定為 *100* 或以上；若值低於 *100*，存在導致 *BFD* 擺動的風險。

   如果在同一介面上有多個使用不同 *BFD* 設定檔的路由通訊協定，請使用相同的 ***Desired Minimum Tx Interval***（所需最小 ***Tx*** 間隔）來設定 *BFD* 設定檔。
2. 輸入 **Required Minimum Rx Interval (ms)**（要求最小 **Rx** 間隔（毫秒））。這是 BFD 可接收 BFD 控制封包的最小間隔（毫秒）。PA-7000 和 PA-5200 系列防火牆的最小間隔為 50；VM 系列防火牆的最小間隔為 200。最大值為 2,000；預設值為 1,000。

   建議將 *PA-7000* 系列防火牆的 ***Required Minimum Rx Interval***（要求最小 ***Rx*** 間隔）設定為 *100* 或以上；若值低於 *100*，存在導致 *BFD* 擺動的風險。

STEP 3 | 設定 Detection Time Multiplier（偵測時間乘數）。

輸入 **Detection Time Multiplier**（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 未從其對等體收到 BFD 控制封包，則會發生故障。範圍是 2 到 50；預設值為 3。

例如，傳輸間隔 300 毫秒 x 3（偵測時間乘數） = 900 毫秒偵測時間。

當設定 *BFD* 設定檔時，需考慮：防火牆是基於工作階段的裝置，通常位於網路或資料中心邊緣，並且可能具有比專用路由器更慢的連結。因此，防火牆可能需要比允許的最快設定更長的間隔及更高的乘數。偵測時間太短可能導致偵測出錯誤的連線失敗，例如因暫時性的網路擁塞。

STEP 4 | 設定 BFD 保留時間。

輸入 **Hold Time (ms)**（保留時間（毫秒））。此為 BFD 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。如果 BFD 在 **Hold Time**（保留時間）期間接收 BFD 控制封包，則會略過它們。範圍為 0-120000。預設為 0，表示 **Hold Time**（保留時間）無傳輸；BFD 在建立連結後立即傳輸並接收 BFD 控制封包。

STEP 5 | （選用—僅針對 BGP IPv4 實作）為 BFD 設定檔進行躍點相關設定。

1. 選取 **Multihop**（多重躍點）以透過 BGP 多重躍點啟用 BFD。
2. 輸入 **Minimum Rx TTL**（最小 **Rx TTL**）。此為 BGP 支援多重躍點 BFD 時 BFD 將在 BFD 控制封包中接受（接收）的最小存留值（躍點數）。（範圍為 1-254；無預設）。

   如果收到的 TTL 小於所設定的 **Minimum Rx TTL**（最小 **Rx TTL**），防火牆將丟棄相應封包。例如，如果對等體在 5 個躍點之外，躍點將 TTL 為 100 的 BFD 封包傳輸至防火牆，以及如果防火牆的 **Minimum Rx TTL**（最小 **Rx TTL**）設為 96 或以上，防火牆會丟棄封包。

STEP 6 | 儲存 BFD 設定檔。

按一下 **OK**（確定）。

STEP 7 | （選用）為靜態路由啟用 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。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取設定靜態路由所在的虛擬路由器。
2. 設定 **Static Routes**（靜態路由）頁籤。
3. 選取 **IPv4** 或 **IPv6** 頁籤。
4. 選取要套用 BFD 所在的靜態路由。
5. 選取一個 **Interface**（介面）（即使您使用的是 DHCP 位址）。**Interface**（介面）設定不能為 **None**（無）。
6. 對於 **Next Hop**（下一個躍點），選取 **IP Address**（**IP** 位址），然後輸入尚未指定的 IP 位址。
7. 對於 **BFD** 設定檔—選取下列其中一項：
   - 預設—僅使用預設設定。
   - 您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。
   - 新建 **BFD** 設定檔—允許您建立 BFD 設定檔。

   選取 ***None (Disable BFD)***（無（停用 ***BFD***）），可對此靜態路由停用 *BFD*。
8. 按一下 **OK**（確定）。

IPv4 或 **IPv6** 頁籤上的 BFD 欄表示為靜態路由設定的 BFD 設定檔。

STEP 8 | （選用）為所有 BGP 介面或為單一 BGP 對等體啟用 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。這可能會中斷所有 *BGP* 流量。在介面上啟用 *BFD* 後，防火牆會停止與對等體的 *BGP* 連接，以便在介面上設定 *BFD*。對等體裝置會偵測到 *BGP* 連接中斷，可能導致重新整合。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*。

如果您同時實作 *BGP BFD* 和 *HA* 路徑監控，*Palo Alto Networks* 建議您不要實作 *BGP Graceful Restart*（非失誤性重新啟動）。當 *BFD* 對等體的介面出現故障並且路徑監控也出現故障時，*BFD* 可以從路由表中移除受影響的路由，並在非失誤性重新啟動生效前，將此變更同步到被動 *HA* 防火牆。如果您決定實作 *BGP BFD*、*BGP* 非失誤性重新啟動和 *HA* 路徑監控，則應為 *BFD* 設定大於預設值的 *Desired Minimum Tx Interval*（所需最小 *Tx* 間隔）和 *Detection Time Multiplier*（偵測時間乘數）。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取要設定 BGP 的虛擬路由器。
2. 選取 **BGP** 頁籤。
3. （選用）若要將 BFD 套用到虛擬路由器上的所有 BGP 介面，請在 **BFD** 清單中選取以下項之一，然後按一下 **OK**（確定）：
   - 預設—僅使用預設設定。
   - 您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。
   - 新建 **BFD** 設定檔—允許您建立 BFD 設定檔。

   選取 ***None (Disable BFD)***（無（停用 ***BFD***）可對虛擬路由器上的所有 *BGP* 介面停用 *BFD*；您無法對單一 *BGP* 介面啟用 *BFD*。
4. （選用）若要對單一 BGP 對等體介面啟用 BFD（只要不停用，就會取代 BGP 的 **BFD** 設定），可執行下列工作：
   1. 選取 **Peer Group**（對等群組）頁籤。
   2. 選取對等群組。
   3. 選取對等體。
   4. 在 **BFD** 清單中，選取以下任何選項：

      預設—僅使用預設設定。

      Inherit-vr-global-setting（預設）—BGP 對等體可繼承您為虛擬路由器的 BGP 全域選取的 BFD 設定檔。

      您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。

      選取 ***Disable BFD***（停用 ***BFD***）可停用 *BGP* 對等體的 *BFD*。
5. 按一下 **OK**（確定）。
6. 按一下 **OK**（確定）。

BGP - 對等群組/對等體清單上的 BFD 欄表示為此介面設定的 BFD 設定檔。

STEP 9 | (選用) 全域地為 OSPF 或 OSPFv3 或為一個 OSPF 介面啟用 BFD。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取要設定 OSPF 或 OSPFv3 的虛擬路由器。
2. 選取 **OSPF** 或 **OSPFv3** 頁籤。
3. （選用）在 **BFD** 清單中，選取以下項之一，為所有 OSPF 或 OSPFv3 介面啟用 BFD，然後按一下 **OK**（確定）：
   - 預設—僅使用預設設定。
   - 您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。
   - 新建 **BFD** 設定檔—允許您建立 BFD 設定檔。

   選取 ***None (Disable BFD)***（無（停用 ***BFD***））可對虛擬路由器上的所有 *OSPF* 介面停用 *BFD*；您無法對單一 *OSPF* 介面啟用 *BFD*。
4. (選用) 若要對單一 OSPF 對等體介面啟用 BFD (只要不停用，就會因此取代 OSPF 的 **BFD** 設定），請執行下列工作：
   1. 選取 **Areas**（區域）頁籤並選取區域。
   2. 在 **Interface**（介面）頁籤上選取介面。
   3. 在 **BFD** 清單中，選取以下任何選項，為指定的 OSPF 對等體設定 BFD：

      預設—僅使用預設設定。

      Inherit-vr-global-setting（預設）—OSPF 對等體可為虛擬路由器繼承 OSPF 或 OSPFv3 的 **BFD** 設定。

      您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。

      選取 ***Disable BFD***（停用 ***BFD***）可為 *OSPF* 或 *OSPFv3* 介面停用 *BFD*。
   4. 按一下 **OK**（確定）。
5. 按一下 **OK**（確定）。

OSPF **Interface**（介面）頁籤上的 BFD 欄表示為此介面設定的 BFD 設定檔。

STEP 10 | （選用）全域地為所有 RIP 或單一 RIP 介面啟用 BFD。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取要設定 RIP 的虛擬路由器。
2. 選取 **RIP** 頁籤。
3. （選用）在 **BFD** 清單中，選取以下項之一，為虛擬路由器上所有的 RIP 介面啟用 BFD，然後按一下 **OK**（確定）：
   - 預設—僅使用預設設定。
   - 您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。
   - 新建 **BFD** 設定檔—允許您建立 BFD 設定檔。

   選取 無（停用 ***BFD***可對虛擬路由器上的所有 *RIP* 介面停用 *BFD*；您無法對單一 *RIP* 介面啟用 *BFD*。
4. (選用) 若要對單一 RIP 介面啟用 BFD（只要不停用，就會因此取代 RIP 的 **BFD** 設定），請執行下列工作：
   1. 選取 **Interfaces**（介面）頁籤並選取介面。
   2. 在 **BFD** 清單中，選取以下任何選項：

      預設—僅使用預設設定。

      Inherit-vr-global-setting（預設）—RIP 介面可繼承您為虛擬路由器的 RIP 全域選取的 BFD 設定檔。

      您設定的 BFD 設定檔—請參閱設定 BFD 設定檔。

      選取 ***None (Disable BFD)***（無（停用 ***BFD***），可對 *RIP* 介面停用 *BFD*。
   3. 按一下 **OK**（確定）。
5. 按一下 **OK**（確定）。

Interface（介面）頁籤上的 BFD 欄表示為此介面設定的 BFD 設定檔。

STEP 11 | 提交組態。

按一下 **Commit**（交付）。

STEP 12 | 檢視 BFD 摘要及詳細資訊。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），找到相關虛擬路由器，然後按一下 **More Runtime Stats**（更多執行階段統計資料）。
2. 選取 **BFD Summary Information**（BFD 摘要資訊）頁籤以查看摘要資訊，例如 BFD 狀態與執行階段統計資料。
3. （選用）在相應介面列中，選取 **details**（詳細資訊），以檢視 參考：BFD 詳細資料。

STEP 13 | 監控透過路由設定引用的 BFD 設定檔；監控 BFD 統計資料、狀況和狀態。

使用以下 CLI 操作命令：

- **show routing bfd active-profile [***<name>***]**
- **show routing bfd details [interface***<name>***][local-ip***<ip>***][multihop] [peer-ip** *<ip>***][session-id][virtual-router***<name>***]**
- **show routing bfd drop-counters session-id** *<session-id>*
- **show counter global | match bfd**

STEP 14 | （選用）清除 BFD 傳輸、接收和丟棄計數器。

```
clear routing bfd counters session-id all | <1-1024>
```

STEP 15 | （選用）清除用於偵錯的 BFD 工作階段。

```
clear routing bfd session-state session-id all | <1-1024>
```


參考：BFD 詳細資料

若要查看虛擬路由器的下列 BFD 資訊，請參閱步驟檢視 BFD 摘要及詳細資訊。

名稱	值（範例）	說明
工作階段 ID	1	BFD 工作階段的 ID 號碼。
介面	ethernet1/12	BFD 執行時選取的介面。
通訊協定	STATIC(IPV4) OSPF	在介面上執行 BFD 的靜態路由（靜態路由的 IP 位址系列）和/或動態路由通訊協定。
本機 IP 位址	10.55.55.2	介面的 IP 位址。
芳鄰 IP 位址	10.55.55.1	BFD 芳鄰的 IP 位址。
RFD 設定檔	預設 *(此 BFD 工作階段擁有多個 BFD 設定檔。最低「(所需最小 Tx 間隔（毫秒）) 」用於選取有效設定檔。)	套用給介面的 BFD 設定檔的名稱。 由於範例介面具有靜態路由及使用不同設定檔執行 BFD 的 OSPF，因此防火牆使用最低 **Desired Minimum Tx Interval**（所需最小 **Tx** 間隔）的設定檔。在此範例中，使用的設定檔為預設設定檔。
狀態（本機/遠端）	開啟/開啟	本機和遠端 BFD 對等的 BFD 狀態。可能的狀態包括管理員關閉、關閉、起始和開啟。
執行時間	2h 36m 21s 419ms	BFD 開啟的時間長度（小時、分鐘、秒和毫秒）。
鑑別器（本機/遠端）	1391591427/1	本機和遠端 BFD 對等的鑑別器。
模式	主動	在介面上設定 BFD 所處的模式：主動或被動。
要求模式	已停用	PAN-OS 不支援 BFD 要求模式，因此其一律處於已停用狀態。
多重躍點	已停用	BFD 多重躍點：已啟用或已停用。
多重躍點 TTL		多重躍點的 TTL；範圍為 1-254。如果多重躍點已停用，欄位為空。
本機診斷代碼	0（無診斷）	診斷代碼表示本機系統上次狀態發生變化的原因：

名稱	值（範例）	說明
		0—無診斷 1—控制偵測時間已到期 2—回應功能失效 3—芳鄰發出工作階段關閉的訊號 4—轉送平面重設 5—路徑關閉 6—串連路徑關閉 7—管理性關閉 8—反向串連路徑關閉
上次收到的遠端診斷代碼	0（無診斷）	上次從 BFD 對等收到的診斷代碼。
傳輸保留時間	0ms	BFD 傳輸 BFD 控制封包之前連結啟動後的保留時間（毫秒）。保留時間為 0 毫秒表示立即傳輸。範圍為 0-120000 毫秒。
收到的 Rx 間隔下限	1000ms	從對等收到的 Rx 間隔下限；BFD 對等可接收控制封包的間隔。最大值為 2000 毫秒。
交涉的傳輸間隔	1000ms	BFD 對等同意傳送互傳 BFD 控制封包的傳輸間隔（毫秒）。最大值為 2000 毫秒。
收到的乘數	3	從 BFD 對等收到的偵測時間乘數值。傳輸時間乘以乘數等於偵測時間。如果偵測時間到期之前 BFD 未從其對等體收到 BFD 控制封包，則會發生故障。範圍為 2-50。
偵測時間（已超出）	3000ms (0)	計算的偵測時間（交涉的傳輸間隔乘以乘數）和超出偵測時間的毫秒數。
Tx 控制封包數（最後）	9383（420 毫秒前）	傳送的 BFD 控制封包數 (以及 BFD 傳輸最近控制封包以來的時間長度)。
Rx 控制封包數（最後）	9384（407 毫秒前）	接收的 BFD 控制封包數（以及 BFD 接收最近控制封包以來的時間長度）。
代理程式資料平面	插槽 1 - DP 0	在 PA-7000 系列防火牆上，指派來為此 BFD 工作階段處理封包的資料平面 CPU。
錯誤	0	BFD 錯誤數。

名稱	值（範例）	說明
造成狀態發生變化的最後一個封包		
版本	1	BFD 版本。
輪詢位元	0	BFD 輪詢位元；0 表示未設定。
所需 Tx 間隔下限	1000ms	造成狀態發生變化的最後一個封包的所需傳輸間隔下限。
需要的 Rx 間隔下限	1000ms	造成狀態發生變化的最後一個封包的所需接收間隔下限。
偵測乘數	3	造成狀態發生變化的最後一個封包的偵測乘數。
我的鑑別器	1	遠端鑑別器。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。
您的鑑別器	1391591427	本機鑑別器。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。
診斷代碼	0（無診斷）	造成狀態發生變化的最後一個封包的診斷代碼。
長度	24	BFD 控制封包的長度（位元組）。
要求位元	0	PAN-OS 不支援 BFD 要求模式，因此要求位元一律設為 0（已停用）。
最後位元	0	PAN-OS 不支援輪詢序列，因此最後位元一律設為 0（已停用）。
多點位元	0	此位元為未來對 BFD 進行單點對多點延伸而保留。在傳輸和接收端，它都必須為零。
控制平面獨立位元	1	· 如果設為 1，傳輸系統的 BFD 實作不會與其控制平面關聯 （即，BFD 在轉送平面中實作，並可在控制平面中斷時繼續運作）。在 PAN-OS 中，此位元一律設為 1。 · 如果設為 0，傳輸系統的 BFD 實作與其控制平面關聯。
驗證存在位元	0	PAN-OS 不支援 BFD 驗證，因此驗證存在位元一律設為 0。

名稱	值（範例）	說明
需要的回應 Rx 間隔下限	0ms	PAN-OS 不支援 BFD 回應功能，因此此項一律為 0 毫秒。

工作階段設定與逾時

本節說明會影響 TCP、UDP 與 ICMPv6 工作階段的全域設定，以及 IPv6、NAT64、NAT 過度訂閱、巨型框架大小、MTU、加速老化和網頁認證驗證。另外也有設定 (重新比對工作階段) 可讓您將新設定的安全性原則套用到已在進行中的工作階段。

下方的前幾個主題簡短摘述 OSI 模型的傳輸層、TCP、UDP 及 ICMP。如需通訊協定的詳細資訊，請參閱其各自的 RFC。其餘的主題則說明工作階段逾時與設定。

傳輸層工作階段

網路工作階段是二或多個通訊裝置之間持續一段時間的訊息交換。工作階段會建立，並在結束時卸除。OSI 模型中有三層：傳輸層、工作階段層和應用程式層，在這三層有不同類型的工作階段發生。

傳輸層在 OSI 模型的 Layer 4 運作，提供可靠或不可靠的資料端對端傳送與流量控制。在傳輸層實作工作階段的網際網路通訊協定包括傳輸控制通訊協定 (TCP) 與使用者資料包通訊協定 (UDP)。

TCP

傳輸控制通訊協定 (TCP) (RFC 793) 是網際網路通訊協定 (IP) 套件的主要通訊協定之一，非常普遍，因此常與 IP 一起合稱為 ***TCP/IP***。由於 TCP 在傳輸與接收區段時會提供錯誤檢查、認可已接收區段，以及重新排序到達順序錯誤的區段，因此其公認為可靠的傳輸通訊協定。TCP 也會要求並重新傳輸已丟棄的區段。TCP 為可設定狀態，並以連線為導向，表示在工作階段期間，系統會在寄件者與接收者之間建立持續的連線。TCP 會控制封包流量， 因此可處理網路擁塞的狀況。

TCP 在工作階段設定期間會執行交握，以啟動與認可工作階段。傳輸資料後，系統會依序關閉工作階段，其中兩端都會傳輸 FIN 封包，並透過 ACK 封包認可該封包。啟動 TCP 工作階段的交握通常是啟動者和接聽程式之間的三方交握（訊息交換），或是四方或五方分割交握，或同時開放等變化。TCP 分割交握丟棄說明如何防止建立 TCP 分割交握工作階段。

使用 TCP 作為其傳輸通訊協定的應用程式包括：超文字傳輸通訊協定 (HTTP)、超文字安全傳輸通訊協定 (HTTPS)、檔案傳輸通訊協定 (FTP)、簡易郵件傳送通訊協定 (SMTP)、Telnet、郵局通訊協定第 3 版 (POP3)、網際網路訊息存取通訊協定 (IMAP) 及安全殼層 (SSH)。

下列主題詳細說明 TCP 的 PAN-OS 實作。

- TCP 半關閉與 TCP 時間等待計時器
- 未驗證的 RST 計時器
- TCP 分割交握丟棄
- 最大區段大小 (MSS)

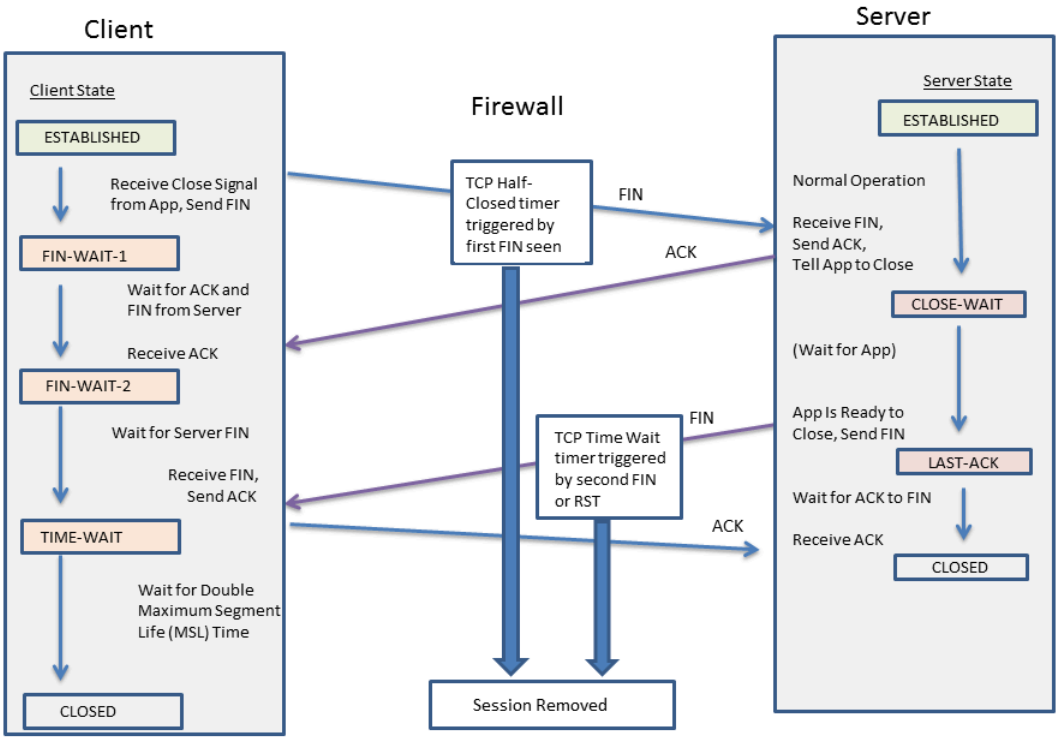
您可以設定基於封包的攻擊防護，從而在允許封包進入相應區域之前，先丟棄具有不適當特性的 IP、TCP 和 IPv6 封包或將不適當選項從封包中剝除。您還可以 設定流量保護，分別指定將會觸發警報、使防火牆隨機丟棄 SYN 封包或使用 SYN Cookie 以及讓防火牆丟棄超出最大速率的 SYN 封包的每秒 SYN 連線數（不比對現有工作階段）。

TCP 半關閉與 TCP 時間等待計時器

TCP 連線終止程序使用 TCP 半關閉計時器，該計時器由防火牆看到工作階段的第一個 FIN 所觸發。計時器名為「TCP 半關閉」，是因為連線只有一端會傳送 FIN。第二個計時器，「TCP 時間等待」，是由第二個 FIN 或由 RST 所觸發的。

如果防火牆只有一個由第一個 FIN 觸發的計時器，則過短的設定會將半關閉的工作階段永久關閉。相反地，過長的設定會讓工作階段表過度成長，而可能用盡所有的工作階段。兩個計時器可讓您擁有相對較長的 TCP 半關閉計時器與相對較短的 TCP 時間等待計時器，因此會迅速地使全關閉工作階段老化，並快速地控制工作階段表的大小。

下圖說明 TCP 連線終止程序期間觸發防火牆的兩個計時器。



基於下列理由，TCP 時間等待計時器應設為小於 TCP 半關閉計時器的值：

- 看到第一個 FIN 之後所允許的時間愈長，愈能讓連線的另一端有時間完全關閉工作階段。
- 如時間等待計時器的時間較短，則是因為在看到 RST 或第二個 FIN 後，工作階段不需要長時間保持開啟之故。時間等待計時器的時間愈短，就愈快釋出資源，但仍能讓防火牆有時間看到最後一個 ACK，並可能重新傳輸其他的資料包。

如果您將 TCP 時間等待計時器的值設定為大於 TCP 半關閉計時器的值，則系統將接受認可，但實際上 TCP 時間等待計時器將不會超過 TCP 半關閉計時器的值。

您可以為計時器進行全域設定，也可以根據應用程式而逐一設定。依預設會為所有的應用程式使用全域設定。如果您在應用程式層級上設定 TCP 等待計時器，則這些計時器會取代全域設定。

未驗證的 RST 計時器

如果防火牆收到的重設 (RST) 封包無法驗證（因為它在 TCP 窗口內的序號不是預期序號，或它來自非對稱的路徑），則未驗證的 RST 計時器會控制過時的工作階段。預設值為 30 秒，範圍是 1-600 秒。未驗證的 RST 計時器提供額外的安全措施，將於下方的第二點中說明。

RST 封包會有三個可能的結果：

- 在 TCP 窗口外的 RST 封包會被丟棄。
- 在 TCP 窗口內但沒有真正預期序號的封包則不予以驗證，並採用未驗證的 RST 計時器設定。此行為可幫助防止拒絕服務 (DoS) 攻擊，此類攻擊會將隨機的 RST 封包傳送到防火牆，嘗試中斷現有的工作階段。

- 在 TCP 窗口內且具有確切預期序號的 RST 封包會採用 TCP 時間等待計時器設定。

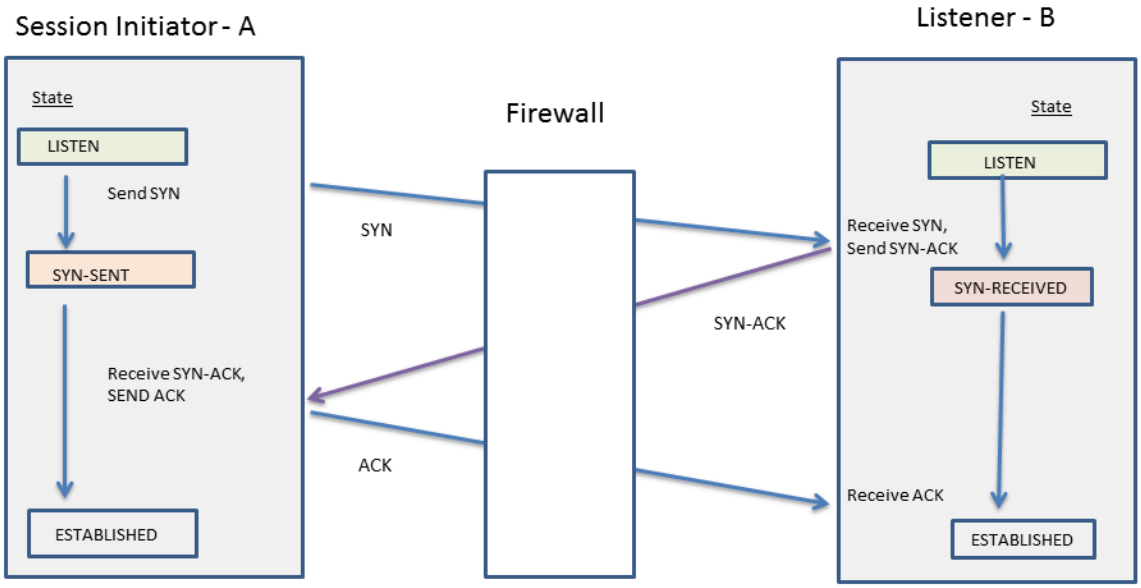
TCP 分割交握丟棄

如果工作階段建立程序不使用知名的三方交握，而使用四方或五方分割交握，或同時開放等變化，則區域保護設定檔中的 **Split Handshake**（分割交握）選項會防止建立 TCP 工作階段。

Palo Alto Networks® 新一代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 Layer 7 處理程序，而無需啟用 **Split Handshake**（分割交握）選項。除非是在提供可用的 **Split Handshake**（分割交握）選項（造成 TCP 分割交握遭到丟棄）的情況下。當針對區域保護設定檔設定 **Split Handshake**（分割交握）選項，且將設定檔套用到區域時，您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；不允許使用變化。

Split Handshake（分割交握）選項預設為停用。

下圖說明透過啟動者（通常是用戶端）和接聽程式（通常是伺服器）之間的 PAN-OS 防火牆，用於建立 TCP 工作階段的標準三方交握。



Split Handshake（分割交握）選項是針對指派給區域的區域保護設定檔所設定的選項。身為區域成員的介面會丟棄伺服器所傳送的任何同步處理 (SYN) 封包，並防止使用下列交握變化。圖中的字母 A 表示工作階段啟動者，而 B 表示接聽程式。交握的每個編號區段都具有箭頭以表示從寄件者至接收者的區段方向，而每個區段則表示控制位元設定。

4-Way Split Handshake (Version 1)	4-Way Split Handshake (Version 2)	Simultaneous Open	5-Way Split Handshake
1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B ACK	1. A → B SYN 2. A ← B SYN 3. A → B SYN-ACK 4. A ← B SYN-ACK	1. A → B SYN 2. A ← B ACK 3. A ← B SYN 4. A → B SYN-ACK 5. A ← B ACK

您可以防止建立 TCP 分割交握工作階段。

最大區段大小 (MSS)

最大傳輸單位 (MTU) 是表示可以在單一 TCP 封包中傳輸的最大位元組數的值。MTU 包括標頭長度，因此 MTU 減去標頭中的位元組數等於最大區段大小 (MSS)，即可以在單一封包中傳輸的最大資料位元組數。

可設定的 MSS 調整大小（如下所示）允許防火牆傳送其標頭長於預設設定允許長度的流量。封裝增加了標頭長度，因此您可增加 MSS 調整大小，以使該位元組適應 MPLS 標頭或擁有 VLAN 標籤的通道流量。

如果為封包設定 DF （不分段）位元，則擁有較大 MSS 調整大小及較小的 MSS 會特別有用，因此較長標頭不會導致封包長度超出允許的 MTU。如果已設定 DF 位元且超出 MTU，將捨棄較大的封包。

您可以全域設定防火牆，以對超過輸出介面 *MTU* 的 *IPv4* 封包進行分割，即使在封包設定了 *DF* 位元時也是如此。使用 *CLI* 命令 ***debug dataplane set ip4-df-ignore yes*** 為 *Layer 3* 實體介面和 *IPSec* 通道介面啟用此功能。使用 *CLI* 命令 ***debug dataplane set ipv4-df-ignore no*** 將防火牆還原為預設行為。

防火牆在以下 Layer 3 介面類型上對 IPv4 和 IPv6 位址支援可設定的 MSS 調整大小：乙太網路、子介面、彙總乙太網路 (AE)、VLAN 和回送。IPv6 MSS 調整大小僅在介面上啟用 IPv6 時適用。

如果在介面上已啟用 *IPv4* 和 *IPv6* 並且兩種 *IP* 位址格式之間 *MSS* 調整大小不同，與此 *IP* 類型對應的適當 *MSS* 值用於 *TCP* 流量。

對於 IPv4 和 IPv6 位址，防火牆適應大於預期的 TCP 標頭長度。在 TCP 封包擁有大於計劃長度的標頭的情況下，防火牆會選擇以下兩個值中的較大值作為 MSS 調整大小：

- 設定的 MSS 調整大小

- TCP 同步處理中 TCP 標頭的長度 (20) + IP 標頭長度的總和

此行為意味著防火牆會在必要時取代設定的 MSS 調整大小。例如，如果您設定 MSS 調整大小為 42，則預計 MSS 等於 1458 （預設 MTU 大小減去調整大小 [1500 - 42]）。但是，TCP 封包在標頭中有 4 個額外位元組的 IP 選項，因此 MSS 調整大小 (20+20+4) 等於 44，大於設定的 MSS 調整大小 42。產生的 MSS 為 1500-44=1456 位元組，小於預期值。

要設定 MSS 調整尺寸，請參閱設定工作階段設定。

Udp

使用者資料包通訊協定 (UDP) (RFC 768) 是 IP 套件中的另一個主要通訊協定，也是 TCP 的替代通訊協定。UDP 沒有狀態，也沒有連線，因為沒有交握可設定工作階段，寄件者與接收者之間沒有連線，封包會採用不同的路由到達單一的目的地。UDP 被視為不可靠的通訊協定，因為它未提供認可、錯誤檢查、重新傳輸或重新排序資料包等功能。由於沒有提供這些功能所需的負荷，因此 UDP 能減少延遲，比 TCP 更為快速。UDP 被稱做盡力而為的通訊協定，因為它沒有任何機制或保證可確保資料會到達其目的地。

UDP 資料包封裝在 IP 封包內。UDP 雖然會使用總和檢查碼檢查資料的完整性，但不會在網路介面層級執行錯誤檢查。錯誤檢查假設為不必要的，或是由應用程式執行，而非由 UDP 本身執行。UDP 沒有機制可處理封包的流量控制。

UDP 通常用於需要較快速度、時間緊迫、即時傳送的應用程式，例如 Voice over IP (VoIP)、音訊與視訊串流及線上遊戲。UDP 以交易為導向，因此也供要回應許多用戶端小規模查詢的應用程式使用，如網域名稱系統 (DNS) 與簡單式檔案傳輸通訊協定 (TFTP) 等。

您還可以在防火牆上使用區域保護設定檔設定流量保護，分別指定將會觸發警報、使防火牆隨機丟棄 UDP 封包以及讓防火牆丟棄超出最大速率的 UDP 封包的每秒 UDP 連線數（不比對現有工作階段）。（雖然 UDP 無連線，但防火牆仍會根據工作階段追蹤 IP 封包中的 UDP 資料包；因此，如果 UDP 封包與現有工作階段不相符，則會被視為新工作階段，並計為臨界值內的一次連線。）

ICMP

網際網路控制訊息通訊協定 (ICMP) (RFC 792) 是網際網路通訊協定套件中的另一個主要通訊協定，在 OSI 模型的網路層運作。ICMP 用於診斷與控制，可傳送 IP 作業的相關錯誤訊息，或有關要求的服務或是否可到達主機或路由器的訊息。透過使用各種 ICMP 訊息，可實作如路徑追蹤與 ping 等網路公用程式。

ICMP 是無連線的通訊協定，不會開啟或維護真正的工作階段。但是，兩個裝置之間的 ICMP 訊息會被視為工作階段。

Palo Alto Networks® 防火牆支援 ICMPv4 與 ICMPv6。您可以透過下列幾種方式控制 ICMPv4 和 ICMPv6 封包：

- 建立 基於 ICMP 和 ICMPv6 的安全性原則規則，並在規則中選取 **icmp** 或 **ipv6-icmp** 應用程式。
- 在 設定工作階段設定 時控制 ICMPv6 速率限制。
- 設定流量保護，分別指定將會觸發警報、觸發防火牆隨機丟棄 ICMP 或 ICMPv6 封包以及讓防火牆丟棄超出最大速率的 ICMP 或 ICMPv6 封包的每秒 ICMP 或 ICMPv6 連線數（不比對現有工作階段）。
- 設定基於封包的攻擊防護，基於封包的攻擊防護：
  - 對於 ICMP，您可以丟棄特定類型的封包，或者抑制傳送特定封包。
  - 對於 ICMPv6 封包（類型 1、2、3、4 和 137），您可以指定防火牆使用 ICMP 工作階段金鑰來比對安全性原則規則，以確定是否允許 ICMPv6 封包。（防火牆將使用安全性原則規則，覆寫使用內嵌封包確定工作階段對應的預設行為。） 當防火牆丟棄與安全性原則規則相符的 ICMPv6 封包時，防火牆會在流量日誌中記錄詳細資訊。

基於 ICMP 和 ICMPv6 的安全性原則規則

只有安全性原則規則允許工作階段時，防火牆才會轉送 ICMP 或 ICMPv6 封包（和防火牆轉送其他類型封包一樣）。防火牆將使用兩種方式之一確定工作階段的相符情況，具體視乎於封包是 ICMP 或 ICMPv6 錯誤封包，還是與 ICMP 或 ICMPv6 資訊封包相反的重新導向封包：

- **ICMP** 類型 **3**、**5**、**11** 和 **12** 以及 **ICMPv6** 類型 **1**、**2**、**3**、**4** 和 **137**—依預設，防火牆會從造成錯誤（叫用封包）的原始資料包查閱資訊的內嵌 IP 封包位元組。如果內嵌封包與現有工作階段相符，防火牆將按與該工作階段相符之安全性原則規則中規定的工作，轉送或丟棄 ICMP 或 ICMPv6 封包。（對於 ICMPv6 類型，您可以使用基於封包的攻擊保護，覆寫此預設行為。）

- 其餘 **ICMP** 或 **ICMPv6** 封包類型—防火牆會將 ICMP 或 ICMPv6 封包視為屬於新工作階段。如果原則規則與封包相符（防火牆將其識別為 **icmp** 或 **ipv6-icmp** 工作階段），防火牆會根據安全性原則規則中的工作轉送或丟棄封包。安全性原則計數器和流量日誌會反映相應的動作。

  如果沒有與封包相符的安全性原則規則，防火牆將套用預設安全性原則規則，允許區域內流量，而封鎖區域間流量（預設會對這些規則停用日誌記錄）。

  雖然您可以覆寫預設規則以啟用日誌記錄或變更預設動作，但我們不建議您變更特定情況的預設行為，因為將會影響這些預設規則所影響的所有流量。這種情況下，可建立安全性原則規則，以明確控制和記錄 *ICMP* 或 *ICMPv6* 封包。

  可使用兩種方式建立明確的安全性原則規則，以處理非錯誤或重新導向封包的 ICMP 或 ICMPv6 封包：

  - 建立安全性原則以允許（或拒絕）所有 **ICMP** 或 **ICMPv6** 封包—在安全性原則規則中，指定應用程式 **icmp** 或 **ipv6-icmp**；防火牆將分別允許（或拒絕）所有與 ICMP 通訊協定號碼 (1) 或 ICMPv6 通訊協定號碼 (58) 相符的 IP 封包通過防火牆。
  - 建立自動應用程式和安全性原則規則，以允許（或拒絕）進出該應用程式的封包—這種更細微的方式可讓您 控制特定的 ICMP 或 ICMPv6 類型和代碼。

ICMPv6 速率限制

ICMPv6 速率限制是一種節流機制，可防止發生爆流的狀況與 DDoS 攻擊的企圖。此實作採用錯誤封包速率與語彙基元陣列，兩者一起運作時可以節流，並確保 ICMP 封包不會灌爆由防火牆保護的網路區段。

首先，全域 **ICMPv6 Error Packet Rate (per sec)**（**ICMPv6** 錯誤封包速率（每秒））會控制允許 ICMPv6 錯誤封包通過防火牆的速率，預設值為每秒 100 個封包，範圍是每秒 10 到 65535 個封包。如果防火牆到達 ICMPv6 錯誤封包速率，語彙基元陣列便會開始運作，系統會開始節流，如下所述。

邏輯語彙基元陣列的概念會控制可傳輸 ICMP 訊息的速率。基元陣列中的語彙基元數目是可設定的，每一個語彙代表一個可傳送的 ICMPv6 訊息。每傳送 ICMPv6 訊息一次，語彙基元計數就會減少，當基元陣列中的語彙到達零時，便再也不會傳送 ICMPv6 訊息，直到另一個語彙基元新增到基元陣列為止。語彙基元陣列的預設大小為 100 個語彙基元 (封包)，範圍是 10 到 65535 個語彙基元。

若要變更預設的語彙基元陣列大小或錯誤封包速率，請參閱 設定工作階段設定 一節。

控制特定的 ICMP 或 ICMPv6 類型和代碼

使用此工作建立自訂 ICMP 或 ICMPv6 應用程式，然後建立安全性原則規則，以允許或拒絕該應用。

STEP 1 | 為 ICMP 或 ICMPv6 訊息類型和代碼建立自訂應用程式。

1. 選取 **Object**（物件） > **Applications**（應用程式），然後 **Add**（新增） 應用程式。
2. 在 **Configuration**（組態）頁籤上，輸入 自訂應用程式的 **Name**（名稱）和 **Description**（描述）。例如，輸入名稱 ping6。
3. 對於 **Category**（類別），選取 **networking**（網路）。
4. 對於 **Subcategory**（子類別），選取 **ip-protocol**（**IP** 通訊協定）。
5. 對於 **Technology**（技術），選取 **network-protocol**（網路通訊協定）。
6. 按一下 **OK**（確定）。
7. 在 **Advanced**（進階）索引標籤上，選取 **ICMP Type**（**ICMP** 類型）或 **ICMPv6 Type**（**ICMPv6** 類型）。
8. 對於 **Type**（類型），輸入指定您要允許或拒絕的 ICMP 或 ICMPv6 訊息類型的數字（範圍為 0-255）。例如 Echo Request 訊息（偵測）為 128。
9. 如果類型包含了代碼，則輸入套用於您要允許或拒絕的 **Type**（類型）值的 **Code**（代碼）數字（範圍為 0-255）。某些 **Type**（類型）值僅有代碼 0。
10. 按一下 **OK**（確定）。

STEP 2 | 建立安全性原則規則，以允許或拒絕您所建立的自訂應用程式。

建立安全性原則規則。在 **Application**（應用程式）頁籤上，指定您所建立的自訂應用程式名稱。

STEP 3 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

設定工作階段逾時值

工作階段逾時值定義當工作階段不活動後，PAN-OS 在防火牆上維護工作階段的持續時間。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。您可以特別針對 TCP、UDP 和 ICMP 工作階段定義逾時數。預設逾時會套用至任何其他類型的工作階段。逾時是全域的，意味著它們會套用至防火牆上該類型的所有工作階段。

此外，您還可執行全域 ARP 快取逾時設定，控制防火牆在快取中保持 ARP 項目（IP 位址至硬體位址對應）的時長。

除了全域設定外，您還可在 **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。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 或 UDP 工作階段逾時。

如果您在應用程式層級上變更 *TCP* 或 *UDP* 計時器，這些用於預先定義的應用程式以及共用自訂應用程式的計時器，將在所有虛擬系統中得以實作。如果應用程式的計時器需獨立於虛擬系統，則必須建立自訂應用程式，向其指派唯一計時器，然後將自訂應用程式指派至唯一虛擬系統。

如果您需針對 TCP、UDP、ICMP、網頁認證驗證或其他類型的工作階段，變更其全域工作階段逾時設定的預設值，請執行以下工作。所有的值皆以秒為單位。

預設值是最佳值。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。

STEP 1 | 存取工作階段逾時。

選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Timeouts（工作階段逾時）。

STEP 2 | （選用）變更雜項逾時值。

- **Default**（預設值）—非 TCP/UDP 或非 ICMP 工作階段在沒有回應的情況下可開啟的時間長度上限（範圍是 1 至 15,999,999；預設值是 30）。
- **Discard Default**（捨棄預設值）—當 PAN-OS 根據防火牆上設定的安全性原則拒絕工作階段後，非 TCP/UDP 工作階段保持開啟的時間長度上限（範圍是 1 至 15,999,999；預設值是 60）。
- **Scan**（掃描）—將任何工作階段視為處於非使用中後，該工作階段保持開啟的時間長度上限；當應用程式超過為該應用程式定義的應用程式緩慢臨界值時，便會將其視為處於非使用中（範圍是 5 至 30；預設值是 10）。
- 驗證入口網站 — 網頁驗證網頁表單的驗證工作階段逾時。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（範圍是 1 至 15,999,999；預設值是 30）。
- 在必須重新驗證使用者之前，若要先定義其他驗證入口網站逾時（例如閒置計時器和到期時間），可選取 **Device**（裝置） > **User Identification**（使用者識別） > **Authentication Portal Settings**（驗證入口網站設定）。請參閱設定驗證入口網站。

STEP 3 | （選用）變更 TCP 逾時。

- 捨棄 **TCP**—當系統根據防火牆上設定的安全性原則拒絕工作階段後，TCP 工作階段保持開啟的時間長度上限。範圍是 1 至 15,999,999；預設值為 90。
- **TCP**—當 TCP 工作階段處於「已建立」狀態後（亦即在完成交握後和/或正在傳輸資料時），TCP 工作階段在沒有回應的狀況下保持開啟的時間長度上限。範圍為 1 至 15,999,999；預設值為 3,600。
- **TCP** 交握—在收到 SYN-ACK 與後續的 ACK 以完全建立工作階段之間允許的時間長度上限。範圍是 1 至 60；預設值為 10。
- **TCP** 起始—啟動 TCP 交握計時器前，在收到 SYN 與 SYN-ACK 之間允許的時間長度上限。範圍是 1 至 60；預設值為 5。
- **TCP** 半關閉—在收到第一個 FIN 和收到 RST 或第二個 FIN 之間的時間長度上限。範圍是 1 至 604,800；預設值為 120。
- **TCP** 時間等待—在收到 RST 或第二個 FIN 後的時間長度上限。範圍是 1 至 600；預設值為 15。
- 未驗證的 **RST**—在收到無法驗證的 RST（RST 在 TCP 窗口內，但序號不是預期序號，或 RST 來自非對稱路徑）後的時間長度上限。範圍是 1 至 600；預設值為 30。
- 另請參閱（選用）變更雜項逾時值一節中的 **Scan**（掃描）逾時。

STEP 4 | （選用）變更 UDP 逾時。

- 捨棄 **UDP**—當系統根據防火牆上設定的安全性原則拒絕工作階段後，UDP 工作階段保持開啟的時間長度上限。範圍為 1 到 15,999,999；預設值為 60。
- **UDP**—在沒有 UDP 回應的情況下 UDP 工作階段保持開啟的時間長度上限。範圍是 1 至 15,999,999；預設值為 30。
- 另請參閱（選用）變更雜項逾時值一節中的 **Scan**（掃描）逾時。

STEP 5 | （選用）變更 ICMP 逾時。

- **ICMP**—在沒有 ICMP 回應的情況下 ICMP 工作階段可開啟的時間長度上限。範圍為 1 到 15,999,999；預設值為 6。
- 另請參閱（選用）變更雜項逾時值一節中的 **Discard Default**（捨棄預設值）和 **Scan**（掃描）逾時。

STEP 6 | 按一下 **OK**（確定）與 **Commit**（提交）。

STEP 7 | （選用）變更 ARP 快取逾時。

1. 存取 CLI 並指定防火牆在快取中保持 ARP 項目的秒數。使用操作命名 **`set system setting arp-cache-timeout`** <*value*>，其中範圍為 60 至 65,535；預設值為 1,800。

   如果您減少逾時值，而且快取中現有項目的 TTL 大於新的逾時值，則防火牆會移除這些項目並重新整理 ARP 快取。如果您增加逾時值，而且現有項目的 TTL 小於新的逾時值，則它們會依據 TTL 過期，而且防火牆會快取逾時值更大的新項目。
2. 使用操作 CLI 命令 **`show system setting arp-cache-timeout`** 檢視 ARP 快取逾時設定。

設定工作階段設定

本主題說明逾時值以外的各種工作階段設定。如果您必須變更預設設定，請執行下列工作。

STEP 1 | 變更工作階段設定。

選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 Session Settings（工作階段設定）。

STEP 2 | 指定是否對已在進行中的工作階段套用新設定的安全性原則規則。

選取 **Rematch all sessions on config policy change**（設定原則變更時重新比對所有工作階段）以對已在進行中的工作階段套用新設定的安全性原則規則。依預設會啟用此功能。如果您清除此核取方塊，所執行的任何原則規則僅適用於提交原則變更後啟動的工作階段。

例如，如果已啟動 Telnet 工作階段，同時設定允許 Telnet 的相關原則規則，而您後續提交原則變更來拒絕 Telnet，則防火牆會將修改的原則套用至目前的工作階段並封鎖它。

STEP 3 | 進行 IPv6 設定。

- **ICMPv6** 語彙基元陣列大小—預設值：100 個語彙基元。請參閱 ICMPv6 速率限制小節。
- **ICMPv6** 錯誤封包速率（每秒）—預設值：100.請參閱 ICMPv6 速率限制小節。
- 啟用 **IPv6** 防火牆—啟用 IPv6 的防火牆功能。如果未啟用 IPv6，所有 IPv6 組態都會遭到忽略。即使為介面啟用 IPv6，也必須啟用 **IPv6 Firewalling**（IPv6 防火牆）設定，IPv6 才能運作。

STEP 4 | 啟用 Jumbo Frame 並設定 MTU。

1. 選取 **Enable Jumbo Frame**（啟用 Jumbo Frame）以在乙太網路介面上啟用 Jumbo Frame 支援。巨型框架具有 9,216 位元組的最大傳輸單位 (MTU)，並只能在特定型號上使用。
2. 根據是否啟用 Jumbo Frame 設定 **Global MTU**（全域 **MTU**）：
   - 如果未啟用 Jumbo Frame，**Global MTU**（全域 **MTU**）將預設為 1,500 位元組；範圍是 576 到 1,500 位元組。
   - 如果啟用 Enable Jumbo Frame（啟用 Jumbo Frame），則 **Global MTU**（全域 **MTU**）預設為 9,192 位元組；範圍是 9,192 到 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隊列大小。對於 *PAN-OS 8.1*，如果啟用巨型框架全域 *MTU* 設定並重新啟動防火牆，然後重新散佈封包緩衝區以更有效地處理*Jumbo* 框架。

如果啟用啟用巨型框架，而且擁有未特別設定 MTU 的介面，則那些介面將自動繼承啟用巨型框架大小。因此，在您啟用巨型框架之前，如果您有任何您不想要有巨型框架的介面，您必須將該介面的 MTU 設定為 1500 位元組或其他值。

如果您匯入（***Device***（裝置） **> *Setup***（設定） **> *Operations***（操作） **> *Import***（匯入））並載入已啟用 *Jumbo Frame* 的組態，然後提交至沒有啟用 *Jumbo Frame* 的防火牆，則 ***Enable Jumbo Frame***（啟用 ***Jumbo Frame***）設定不會提交至組態。您應當先 ***Enable Jumbo Frame***（啟用 ***Jumbo Frame***），重新啟動，然後匯入、載入和提交組態。

STEP 5 | 調整 NAT 工作階段設定。

- **NAT64 IPv6 Minimum Network MTU**（NAT64 IPv6 最小網路 MTU）—為 IPv6 轉譯的流量設定全域 MTU。預設值為 1,280 位元組，這是以 IPv6 流量的標準最小 MTU 為基礎。
- **NAT** 過度訂閱比例—如果將 NAT 設為「動態 IP 與連接埠」(DIPP) 轉譯，則可設定過度訂閱比例，如此便會乘以可同時使用同一個已轉譯 IP 位址與連接埠配對的次數。比例是 1、2、4 或 8。預設設定基於防火牆型號。
- 比例為 1 則表示沒有過度訂閱，每個已轉譯的 IP 位址與連接埠配對一次只能使用一次。
- 如果設定為 **Platform Default**（平台預設），則比例的使用者設定為停用，且會套用相應型號的預設過度訂閱比例。

降低過度訂閱比例會減少來源裝置轉譯次數，但會提供更高的 NAT 規則容量。

STEP 6 | 調整加速過時設定。

選取 **Accelerated Aging**（加速過時）以讓閒置的工作階段加速過時。您也可變更臨界值 (%) 和縮放係數：

- 加速過時臨界值—當加速過時開始時，工作階段表滿的百分比。預設值為 80%。當工作階段表到達此臨界值 (% 滿) 時，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。
- 加速過時縮放係數—加速過時計算中使用的縮放係數。預設的縮放係數為 2，這表示加速老化發生的速率是所設定閒置時間的兩倍快。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老化，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。

例如，如果縮放係數是 10，一般會在 3600 秒後逾時之工作階段的逾時速度可能加快 10 倍 (時間的 1/10)，也就是在 360 秒後逾時。

STEP 7 | 啟用封包緩衝區保護。

1. 選取封包緩衝區保護，以使防火牆能夠針對可能導致封包緩衝區爆滿並造成合法流量被丟棄的工作階段採取相應措施；預設為啟用。
2. 如果啟用封包緩衝區保護，您可以調整指示防火牆將如何回應封包緩衝區濫用的臨界值和計時器。
   - **Alert (%)**（警示 **(%)**）：當封包緩衝區利用率超出此臨界值時，防火牆將建立日誌事件。預設臨界值為 50%，範圍為 0% 至 99%。若此值設定為 0%，則防火牆不會建立日誌事件。
   - **Activate (%)**（啟用 **(%)**）：當封包緩衝區利用率超出此臨界值時，防火牆將對濫用的工作階段套用隨機早期丟棄 (RED)。預設設定為 80%，範圍為 0% 至 99%。若此值設定為 0%，則防火牆不會套用 RED。

     警示事件將記錄在系統日誌內。丟棄流量、捨棄工作階段和封鎖 ***IP*** 位址事件記錄在威脅日誌內。

   - **Block Hold Time (sec)**（封鎖保留時間（秒））：在捨棄工作階段之前，允許 RED 降低的工作階段繼續進行的時間。依預設，封鎖保持時間為 60 秒。範圍是 0 至 65,535 秒。若此值設定為 0，則防火牆不會根據封包緩衝區保護捨棄工作階段。
   - **Block Duration (sec)**（封鎖持續時間（秒））：此設定定義了工作階段保持捨棄或 IP 位址保持封鎖狀態的持續時間。預設為 3,600 秒，範圍是 0 秒至 15,999,999 秒。若此值設定為 0，則防火牆不會根據封包緩衝區保護捨棄工作階段或封鎖 IP 位址。

STEP 8 | 啟用多點傳送路由設定封包的緩衝。

1. 選取 **Multicast Route Setup Buffering**（多點傳送路由設定緩衝），在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不存在時，使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。此選項預設為停用。

2. 如果您啟用緩衝，也可以調整 **Buffer Size**（緩衝區大小），依流量指定緩衝區大小。防火牆可緩衝最多 5,000 個封包。

   您也可以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，方法是在處理您的虛擬路由器的虛擬路由器上進行多點傳送設定（在虛擬路由器組態中的 ***Multicast***（多點傳送） **> *Advanced***（進階）頁籤上設定 ***Multicast Route Age Out Time (sec)***（多點傳送路由過時時間（秒））。）

STEP 9 | 儲存工作階段設定。

按一下 **OK**（確定）。

STEP 10 | 調整 Layer 3 介面的 最大區段大小 (MSS) 調整大小設定。

1. 選取 **Network**（網路） > **Interfaces**（介面），再選取 **Ethernet**（乙太網路）、**VLAN** 或 **Loopback**（回送），然後選取 Layer 3 介面。
2. 選取 **Advanced**（進階） > **Other Info**（其他資訊）。
3. 選取 **Adjust TCP MSS**（調整 **TCP MSS**），然後為以下一項或兩項輸入值：
   - **IPv4 MSS Adjustment Size**（**IPv4 MSS** 調整大小）（範圍為 40 至 300 位元組；預設為 40 位元組）。
   - **IPv6 MSS Adjustment Size**（**IPv6 MSS** 調整大小）（範圍為 60 至 300 位元組；預設為 60 位元組）。
4. 按一下 **OK**（確定）。

STEP 11 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

STEP 12 | 變更 Jumbo 框架組態後，重新啟動防火牆。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作）。
2. 按一下 **Reboot Device**（重新啟動裝置）。

工作階段散佈原則

工作階段散佈原則定義了 PA-5200 和 PA-7000 系列防火牆將如何在防火牆上個資料平面處理器 (DP) 間散步安全性處理（App-ID、Content-ID、URL 篩選、SSL 解密以及 IPSec）。每項原則都專門針對特定類型網路環境及防火牆組態而設計，以確保防火牆以最高效率散佈工作階段。例如，雜湊工作階段散佈原則最適合使用大型來源 NAT 的環境。

防火牆上的 DP 數目視乎防火牆型號：

防火牆型號	資料平面處理器數目
PA-7000 系列	視乎所安裝網路處理卡 (NPC) 的數目。每個 NPC 都有多個資料平面處理器 (DP)，您可以在防火牆中安裝多個 NPC。
PA-5220 防火牆	1 *PA-5220* 防火牆僅有一個 *DP*，因此工作階段散佈原則將不起作用。將原則設定為預設值（循環配置）。
PA-5250 防火牆	2
PA-5260 與 PA-5280 防火牆	3
PA-5450 防火牆	視乎所安裝資料處理卡 (DPC) 的數目。

下列主題提供了可用工作階段散佈原則、如何變更使用中原則以及如何檢視工作階段散佈統計資料的相關資訊。

- 工作階段散佈原則說明
- 變更工作階段散佈原則以及檢視統計資料

工作階段散佈原則說明

下表列出了工作階段散佈原則的相關資訊，以協助您確定最適合您所用環境和防火牆組態的原則。

工作階段散佈原則	說明
已修正	允許您指定防火牆將用於安全性處理的資料平面處理器 (DP)。 可將此原則用於偵錯。
hash	防火牆根據來源位址或目的地位址的雜湊來散佈工作階段。基於散佈的雜湊可提升 NAT 位址資源管理的效率，並

工作階段散佈原則	說明
	避免潛在 IP 位址或連接埠衝突，從而減少 NAT 工作階段設定的延遲。 可在使用大型來源 NAT 搭配動態 IP 轉譯或動態 IP 及連接埠轉譯或兩者的環境中使用此原則。當使用動態 IP 轉譯時，則選取 **source** 位址選項。當使用動態 IP 和連接埠轉譯時，則選取 **destination** 位址選項。
輸入插槽（PA-7000 系列防火牆上的預設值）	（僅限 PA-7000 系列防火牆）將新工作階段指派給工作階段的首個封包抵達的 NPC 上的 DP。要根據工作階段負載演算法選取 DP，但在這種情況下，將限制工作階段使用輸入 NPC 上的 DP。 視乎流量和網路拓撲，此原則一般能降低流量需要在交換結構中周遊的機率。 如果輸入和輸出都在同一個 NPC 上，可使用此原則來減少延遲。對於有多個 NPC 的防火牆（例如 PA-7000 20G 和 PA-7000 20GXM），此原則可用於隔離相應 NPC 的更大容量，並協助隔離 NPC 失效的影響。
隨機	防火牆將隨機選取 DP 進行工作階段處理。
循環配置（PA-5200 系列防火牆上的預設值）	防火牆會根據循環配置演算法，在使用中資料平面之間選取資料平面處理器，以便在所有資料平面上共用輸入/輸出和安全性處理功能。 可在僅需建議並可預測負載平衡演算法的低到中等要求環境中使用此原則。 在高要求環境中，我們建議您使用工作階段負載演算法。
工作階段負載	此原則與循環配置原則相似，但使用了基於權重的演算法來確定如何散佈工作階段以實現各 DP 的平衡。由於工作階段存留時間各不相同，DP 可能並不能保持恆定負載。例如，如果防火牆有三個 DP，DP0 使用了 25% 容量，DP1 使用了 25% 容量，DP2 使用了 50% 容量，新工作階段指派將優先使用了更少容量的 DP。這有助於促進長期負載平衡。 可在工作階段散佈於多個 NPC 插槽的環境中使用此原則，例如在插槽間彙總介面群組中，或在具備非對稱轉送的環境中使用。如果防火牆裝備了一系列具有不同工作階段容量的 NPC，您還可以使用此原則或輸入插槽原則（例如 PA-7000 20G 和 PA-7000 20GXM NPC 的組合）。
對稱雜湊	（執行 PAN-OS 8.0 或更新版本的 PA-5200 系列和 PA-7000 系列防火牆）防火牆將按已排序之來源和目的地

工作階段散佈原則	說明
	IP 位址的雜湊選取 DP。對於伺服器到用戶端 (s2c) 流量和用戶端到伺服器 (c2s) 流量（假設防火牆不使用 NAT），此原則將產生相同的結果。 可在高要求 IPSec 或 GTP 部署中使用此原則。 對於這些通訊協定，每個方向都將被視為單向流量，無法像對方提供流程元組。此原則能確保兩個方向均被指派相同的 DP，因此無需進行 DP 之間的通訊，從而提升了效能並減小了延遲。

變更工作階段散佈原則以及檢視統計資料

下表列出了如何檢視和變更工作階段散佈原則以及如何檢視防火牆中每個資料平面處理器 (DP) 的工作階段統計資料。

工作	命令

顯示工作階段散佈原則。	使用 **show session distribution policy** 命令檢視使用中工作階段散佈原則。
	下列輸出源自於帶有四個 NPC（安裝於插槽 2、10、11 和 12）而並啟用了 ingress-slot 散佈原則的 PA-7080 防火牆：
	`> show session distribution policy`
	`Ownership Distribution Policy: ingress-slot`
	`Flow Enabled Line Cards: [2, 10, 11, 12]Packet Processing Enabled Line Cards: [2, 10, 11, 12]`

變更使用中工作階段散佈原則。	使用 **set session distribution-policy *<policy>*** 命令變更使用中工作階段散佈原則。 例如，若要選取 session- load 原則，則輸入下列命令： `> set session distribution-policy session-load`
檢視工作階段散佈統計資料。	使用 **show session distribution statistics** 命令檢視防火牆上的資料平面處理器 (DP) 以及每個使用中 DP 上的工作階段數量。 下列為 PA-7080 防火牆的輸出：

工作	命令
	> show session distribution statistics DP Active Dispatched Dispatched/sec --- s1dp0 78698 7829818 1473 s1dp1 78775 7831384 1535 s3dp0 7796 736639 1488 s3dp1 7707 737026 1442 **DP Active column** 中列出了所安裝的 NPC 上的每一個資料平面。前兩個字元表示插槽號碼，後三個字元表示資料平面號碼。例如，s1dp0 表示插槽 1 中 NPC 上的資料平面 0，s1dp1 表示插槽 1 中 NPC 上的資料平面 1。 **Dispatched** 欄顯示資料平面自防火牆上次重新啟動後所處理的工作階段總數。 **Dispatched/sec** 欄列出了分派速率。若您將 **Dispatched** 欄中的數字加起來，總和為防火牆上的使用中工作階段數。您還可以執行 **show session info** CLI 命令來檢視使用中工作階段總數。 *PA-5200* 系列防火牆的輸出都相似，只是 *DP* 數量視乎於型號，而且只有一個 *NPC* 插槽 *(s1)*。

防止建立 TCP 分割交握工作階段

您可以在區域保護設定檔中設定 TCP 分割交握丟棄，以防止建立未使用標準三方交握的 TCP 工作階段。此工作假設您為介面指派了一個安全性區域，在該區域，您要防止 TCP 分割交握建立工作階段。

STEP 1 | 設定區域保護設定檔，以防止使用三方交握以外的項目建立工作階段的 TCP 工作階段。

1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後 **Add**（新增） 新設定檔（或選取現有設定檔）。
2. 如果要建立新設定檔，請輸入設定檔的 **Name**（名稱），然後輸入選用 **Description**（說明）。
3. 選取 **Packet Based Attack Protection**（基於封包的攻擊保護） > **TCP Drop**（**TCP** 丟棄），然後選取 **Split Handshake**（分割交握）。
4. 按一下 **OK**（確定）。

STEP 2 | 將設定檔套用至一或多個安全性地區。

1. 選取 **Network**（網路） > **Zones**（區域），然後選取要指派區域保護設定檔的區域。
2. 在 Zone（區域）視窗中，從 **Zone Protection Profile**（區域保護設定檔）清單中，選取您在上一步中設定的設定檔。

   或者，您可以按一下 **Zone Protection Profile**（區域保護設定檔），在此開始建立新設定檔，在此情況下您可以相應地繼續執行。
3. 按一下 **OK**（確定）。
4. （選用）重複步驟 1-3 以將設定檔套用至其他區域。

STEP 3 | Commit（提交）您的變更。

按一下 **OK**（確定）與 **Commit**（提交）。

通道內容檢查

防火牆無需終止通道即可檢查純文字通道通訊協定的流量內容：

- 一般路由封裝 (GRE) (RFC 2784)
- 非加密 IPSec 流量 [IPSec 的 NULL 加密演算法 (RFC 2410) 與傳輸模式 AH IPSec 的 NULL 加密演算法]
- 整合封包無線電服務 (GPRS) 使用者資料通道通訊協定 (GTP-U)
- 虛擬可延伸區域網路 (VXLAN) (RFC 7348)

通道內容檢查僅適用於純文字通道，不適用於攜帶加密流量的 *VPN* 或 *LSVPN* 通道。

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 IPSec 通道）。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。

所有型號的防火牆均支援 GRE、非加密 IPSec 和 VXLAN 通訊協定通道內容檢查。僅支援 GTP 安全性的防火牆支援 GTP-U 通道內容檢查—有關支援 GTP 和 SCTP 安全性的防火牆型號 PAN-OS 版本，請參閱相容性矩陣。

依預設，受支援的防火牆執行通道加速，以提高流量通過 GRE 通道、VXLAN 通道和 GTP-U 通道的效能和輸送量。通道加速提供了硬體卸載功能，以減少執行流程查閱所需的時間，並允許通道流量根據內部流量更有效地散佈。但是，您可以 停用通道加速 以進行疑難排解。

- 通道內容檢查概要介紹
- 設定通道內容檢查
- 檢視已檢查的通道活動
- 檢視日誌中的通道資訊
- 根據標記的通道流量建立自訂報告
- 停用通道加速

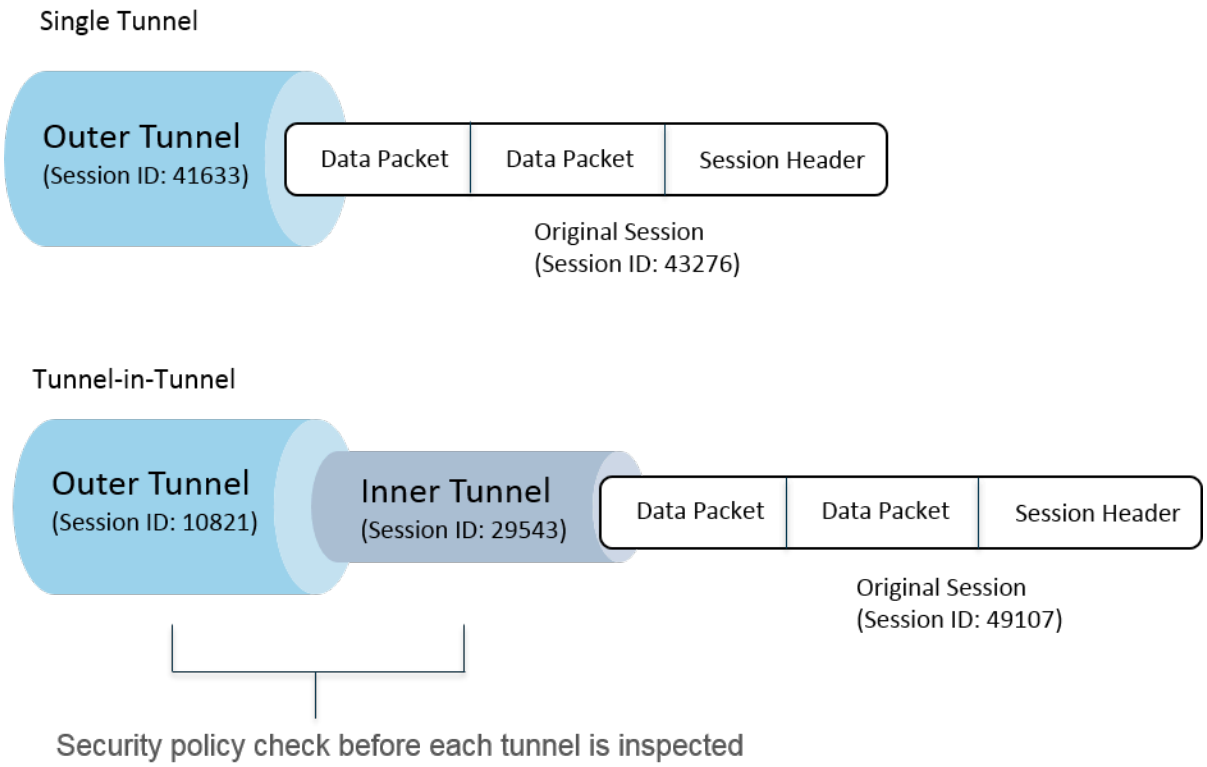
通道內容檢查概要介紹

如果您首先沒有機會終止通道，您的防火牆可檢查網路上任何位置的通道內容。只要防火牆在 GRE、非加密 IPSec、GTP-U 或 VXLAN 通道的路徑中，則防火牆可檢查通道內容。

- 希望檢查通道內容的企業客戶可以使用 GRE、VXLAN 或非加密 IPSec 通道傳送防火牆上的部分或全部流量。為了安全性、QoS 和報告等方面的原因，您可能希望檢查通道內的流量。
- 服務提供者客戶可以使用 GTP-U 通道傳送來自行動裝置的資料流量。您可能希望檢查內部內容而不終止通道通訊協定，並希望記錄來自於使用者的使用者資料。

防火牆支援在乙太網路介面與子介面、AE 介面、VLAN 介面、VPN 和 LSVPN 通道介面上檢查通道內容。（防火牆檢查的純文字通道可能位在終止於防火牆的 VPN 或 LS VPN 通道內，因此是 VPN 或 LSVPN 通道介面。換句話說，當防火牆是 VPN 或 LSVPN 端點時，防火牆可以檢查通道內容檢查支援的任何非加密通道通訊協定的流量。）

Layer 3、Layer 2、Virtual Wire、旁接部署中支援通道內容檢查。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。



前面的圖片中介紹了防火牆可執行的兩個層級的通道內容檢查。當設定了通道內容檢查原則規則的防火牆收到封包時：

- 防火牆將執行安全性原則檢查，以確定是允許還是拒絕封包中的通道通訊協定（應用程式）。（IPv4 和 IPv6 封包通訊協定是通道內支援的通訊協定。）
- 如果安全性原則允許封包進入，則防火牆會按照來源區域、來源位址、來源使用者、目的地區域和目的地位址來比對封包與通道檢查原則規則。通道檢查原則規則確定了防火牆將檢查的通

道通訊協定、允許的最大封裝層級（單一通道或通道內的通道）、是否允許包含未通過 RFC 2780 嚴格標頭檢查之通道通訊協定的封包，以及是否允許包含未知通訊協定的封包。

- 如果封包通過了通道檢查原則規則的比對準則，則防火牆將檢查其內部內容，這些內容需符合安全性原則（必要）以及您指定的其他可選原則。（支援的原始工作階段原則類型列於下表中）。
- 若防火牆尋找其他通道，則防火牆將遞迴剖析封包，以分析第二個標頭，此時就處在封裝的第二層級；因此，與通道區域相符的第二個通道檢查原則規則必須為防火牆允許最高兩個層級的通道檢查層級，才能繼續處理封包。
  - 如果規則允許兩個層級的檢查，則防火牆將對該內部通道執行安全性原則檢查，然後哦再執行通道檢查原則檢查。您在內部通道中使用的通道通訊協定可能與您在外部通道中使用的通道通訊協定不相同。
  - 如果規則不允許兩個層級的檢查，防火牆將根據您是否設定其丟棄封裝層級數大於所設定之最高通道檢查層級的封包，來執行相應動作。

依預設，封裝在通道中的內容屬於與通道相同的安全性區域，也需符合保護該區域的安全原則規則。但是，您可以設定一個通道區域，讓您能夠靈活地為內部內容設定與通道安全性原則規則不同的安全性原則規則。如果您對通道區域使用不同的通道檢查原則，則必須將最高通道檢查層級設定而兩層，因為按照定義，防火牆將檢查第二層封裝。

防火牆不支援用於比對終止於防火牆之通道流量的通道檢查原則；防火牆會丟棄與內部通道工作階段相符的封包。例如，若某個 IPSec 通道終止於防火牆，則不要建立與您終止之通道相符的通道檢查原則規則。防火牆已經檢查過內部通道流量，因此不需要通道檢查原則規則。

雖然通道內容檢查將作用於共用閘道以及虛擬系統與虛擬系統之間的通信，但您無法為共用閘道以及虛擬系統與虛擬系統之間的通信指派通道區域；它們要符合自己所屬通道的安全性原則規則。

內部通道工作階段和外部通道工作階段計數不能超過防火牆型號的最大工作階段容量。

下表用核取記號指示了您可以對外部通道工作階段、內部通道工作階段以及內部原始工作階段套用的原則類型：

原則類型	外部通道工作階段	內部通道工作階段	內部原始工作階段
App-Override（應用程式覆寫）	✓ 僅限 VXLAN	–	✓
DoS 保護	✓	✓	✓
NAT	✓	–	–
基於原則的轉送 (PBF) 和對稱傳回	✓	–	–

原則類型	外部通道工作階段	內部通道工作階段	內部原始工作階段
QoS	–	–	✓
安全性（必要）	✓	✓	✓
使用者-ID	✓	✓	✓
地區保護	✓	✓	✓

VXLAN 與其他通訊協定不同。防火牆可以使用兩組不同工作階段金鑰中的任意一組來為 VXLAN 產生外部通道工作階段。

- VXLAN UDP 工作階段—一個六元組金鑰（區域、來源 IP、目的地 IP、通訊協定、來源連接埠和目的地連接埠）可以建立 VXLAN UDP 工作階段。
- VNI 工作階段—一個包含通道 ID（VXLAN 網路識別碼，VNI）並使用區域、來源 IP、目的地 IP、通訊協定和通道 ID (VNI) 的五元組金鑰可以建立 VNI 工作階段。

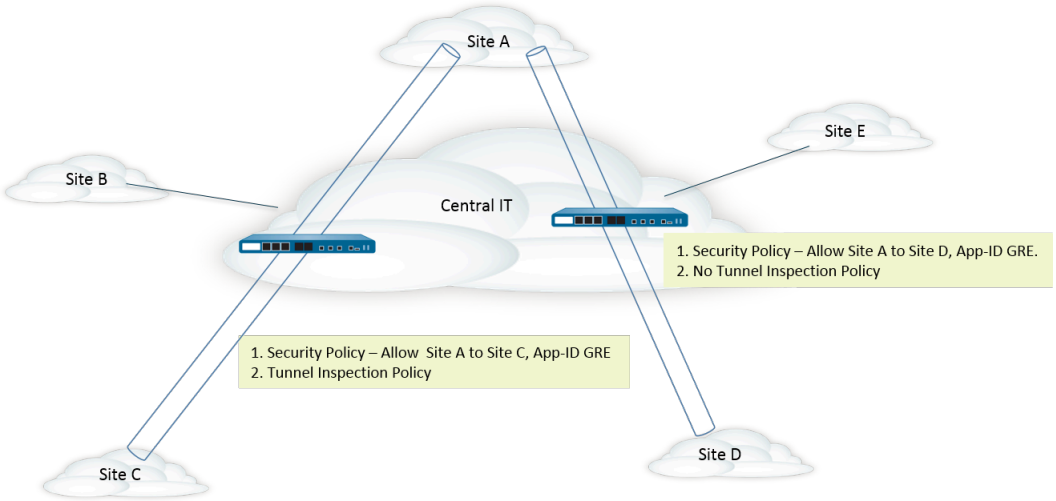
您可以在 ACC 上檢視已檢查的通道活動或檢視日誌中的通道資訊。為了便於快速檢視，可設定監控標籤，以便能透過該標籤監控通道活動並篩選日誌結果。

ACC 通道活動在多個檢視表中提供了資料。對於通道 ID 使用量、通道監控 ID以及通道應用程式使用量，**bytes**（位元組數）、**sessions**（工作階段數）、**threats**（威脅數）、**content**（內容）和 **URLs** 的資料均來自於流量摘要資料庫。對於通道使用者、通道來源 IP 和通道目的地 IP 活動，**bytes**（位元組數）和 **sessions**（工作階段數）的資料來自於流量摘要資料庫，**threats**（威脅數）的資料來自於威脅摘要，**URLs** 的資料來自於 URL 摘要，**contents**（內容）的資料來自於資料資料庫（威脅日誌的子集）。

如果您在介面上啟用 NetFlow，NetFlow 將僅擷取外部通道的統計資料，以免重複計數（計算外部和內部流程的位元組數）。

對於您所用防火牆型號的通道檢查原則規則和通道區域容量，請參閱產品選擇工具。

下圖介紹了一家有多個部門的公司，該公司使用了多個不同的安全性原則和一個通道檢查原則。中央 IT 團隊負責連線各個地區。有一個通道用於連結站台 A 和站台 C；其他通道用於連接站台 A 和站台 D。中央 IT 團隊在每個通道路徑的防火牆上都部署了一個防火牆；站台 A 和站台 C 之間通道上的防火牆將執行通道檢查；站台 A 和站台 D 之間通道上的防火牆沒有通道檢查原則，因為該通道中的流量非常敏感。



設定通道內容檢查

執行此工作，為您在通道中允許的通道通訊協定設定通道內容檢查。

STEP 1 | 建立安全性原則規則，允許使用特定應用程式（如 GRE 應用程式）的封包通過通道（從來源區域到目的地區域）。

建立安全性原則規則

防火牆可在工作階段開始、工作階段結束時或同時在兩個時間點建立通道檢查日誌。為安全性原則規則指定***Actions***（動作）時，為存留時間較長的通道工作階段（如 *GRE* 工作階段）選取***Log at Session Start***（工作階段開始時記錄）。

STEP 2 | 建立通道檢查原則規則。

1. 選取**Policies**（原則） > **Tunnel Inspection**（通道檢查），然後**Add**（新增） 原則規則。
2. 在**General**（一般）頁籤上，輸入通道檢查原則規則**Name**（名稱），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。
3. 選用）輸入**Description**（說明）。
4. 選用）如需用於報告和記錄，指定**Tag**（標籤），來識別需符合通道檢查原則規則的封包。

STEP 3 | 指定用於確定通道檢查原則規則適用之封包來源的準則。

1. 選取**Source**（來源）頁籤。
2. 從區域清單**Add**（新增）**Source Zone**（來源區域）（預設為**Any**（任何））。
3. 選用**Add**（新增）**Source Address**（來源位址）。您可以輸入 IPv4 或 IPv6 位址、位址群組或地理區域位址物件**Any**（任何））。
4. 選用）選取**Negate**（否定），可選擇任何除您指定位址外的位址。
5. 可選**Add**（新增）**Source User**（來源使用者）（預設為**any**（任何））**Known-user**（已知使用者）是已經過驗證的使用者**Unknown**（未知）使用者則未經過驗證。

STEP 4 | 指定用於確定通道檢查原則規則適用之封包目的地的準則。

1. 選取**Destination**（目的地）頁籤。
2. 從區域清單**Add**（新增）**Destination Zone**（目的地區域）（預設為**Any**（任何））。
3. 選用**Add**（新增）**Destination Address**（目的地位址）。您可以輸入 IPv4 或 IPv6 位址、位址群組或地理區域位址物件（預設為**Any**（任何））。

   您還可以設定新位址或位址群組。
4. 選用）選取**Negate**（否定），可選擇任何除您指定位址外的位址。

STEP 5 | 指定防火牆將為此規則檢查的通道通訊協定。

1. 選取**Inspection**（檢查）頁籤。
2. **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 (GRE) 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**—防火牆會檢查通道中使用虛擬可延伸區域網路 (VXLAN) 通道通訊協定的封包。

STEP 6 | 指定防火牆檢查的封裝層級數以及防火牆丟棄封包的條件。

1. 選取**Inspect Options**（檢查選項）。
2. 選取防火牆將檢查的**Maximum Tunnel Inspection Levels**（通道檢查層級數上限）：
   - **One Level**（一層）（預設值）—防火牆將僅檢查外部通道中的內容。

     對於 VXLAN，防火牆會檢查 VXLAN 有效負載以尋找通道中的封裝內容或應用程式。由於 VXLAN 檢查僅發生在外部通道，您必須選取**One Level**（一個層級）。
   - 兩層（通道內的通道）—防火牆將檢查外部通道和內部通道中的內容。
3. 選取下列任何選項、所有選項或不選，指定防火牆是否在相應條件下丟棄封包：
   - 如果超出通道檢查層級數上限，則丟棄封包—如果封包中包含的封裝層級數量大於所設定的**Maximum Tunnel Inspection Levels**（通道檢查層級數上限），防火牆將丟棄該封包。
   - 如果通道通訊協定無法嚴格檢查標頭，則丟棄封包—如果封包中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，防火牆將丟棄該封包。不相容的標頭可能表示有可疑的封包。此選項會使防火牆根據 RFC 2890 驗證 GRE 標頭。

     如果防火牆使用執行RFC 2890 之前的 *GRE* 版本為 *GRE* 提供通道，則不得啟用***Drop packet if tunnel protocol fails strict header check***（如果通道通訊協定無法嚴格檢查標頭，則丟棄封包）選項。
   - 如果通道內有未知通訊協定，則丟棄封包—如果封包中包含了防火牆無法識別的通道內通訊協定，防火牆將丟棄該封包。

     例如，如果選取此選項，防火牆將丟棄與通道檢查原則規則相符的加密 IPSec 封包，因為防火牆無法讀取這些封包。因此，您可以允許 IPSec 封包，但防火牆將僅允許非加密 IPSec 和 AH IPSec 封包。
   - **Return scanned VXLAN tunnel to source**（將掃描的 **VXLAN** 通道返回至來源）—當流量重新導向至防火牆時，VXLAN 將封裝封包。流量導向在公共雲端環境中最為常見。啟用**Return scanned VXLAN tunnel to source**（將掃描的 **VXLAN** 通道返回至來源）以將封裝後的封包返回至原始 VXLAN 通道端點 (VTEP)。此選項僅在第三層、第三層子介面、彙總介面第三層，以及 VLAN 上支援。
4. 按一下**OK**（確定）。

STEP 7 | 管理通道檢查原則規則。

使用以下選項管理通道檢查原則規則：

- （篩選欄位）—僅顯示篩選欄位中指定名稱的通道原則規則。
- 刪除—移除所選的通道原則規則。
- 複製**Add**（新增）按鈕的替代選項；用於複製選定的規則並提供新名稱（稍後可修改）。
- 啟用—啟用選定的通道原則規則。
- 啟用—停用選定的通道原則規則。
- 移動—移動選定的通道原則規則；將按照從上到下的順序，對照規則評估封包。
- 醒目提示未使用的規則—醒目提示自防火牆上次重新啟動以來，沒有相符封包的通道原則規則。

STEP 8 | 選用）為通道內容建立通道來源區域和通道目的地區域，並為每個區域設定安全性原則規則。

最佳做法是為通道流量建立通道區域。因此，防火牆將為具有相同五元組（來源 *IP* 位址及連接埠、目標 *IP* 位址及連接埠、通訊協定）經由通道之封包和不經由通道之封包建立單獨的工作階段。

為 *PA-5200* 系列防火牆上的通道流量指派通道區域，將使防火牆在軟體中執行通道檢查；通道檢查將不會卸載到硬體上。

1. 如果您希望通道內容符合與外部通道區域（之前設定）不同的安全性原則規則，可選取**Network**（網路） > **Zones**（區域），然後為通道來源區域**Add**（新增）**Name**（名稱）。
2. 對於**Location**（位置），選取虛擬系統。
3. 對於**Type**（類型），選取**Tunnel**（通道）。
4. 按一下**OK**（確定）。
5. 重複這些子步驟，建立通道目的地區域。
6. 為通道來源區設定安全性原則規則。

   由於您可能不知道通道流量的來源或流量的方向，並且不希望意外地禁止應用程式流量經過通道，可在安全性原則規則中，將兩個通道區域指定為***Source Zone***（來源區域），將兩個通道區域指定為***Destination Zone***（目的地區域），或者為來源區域和目的地區域選取***Any***（任何），然後指定***Applications***（應用程式）。
7. 為通道目的地區設定安全性原則規則。上一步中為通道來源區域設定安全性原則規則的提示也適用於通道目的地區域。

STEP 9 | 選用）為內部內容指定通道來源區域和通道目的地區域。

1. 將通道來源區域和通道目的地區域（您剛才新增）指定為內部內容區域。選取**Policies**（原則） > **Tunnel Inspection**（通道檢查），然後在**General**（一般） 頁簽上，選取您建立的通道檢查原則**Name**（名稱）。
2. 選取**Inspection**（檢查）。
3. 選取**Security Options**（安全性選項）。
4. **Enable Security Options**（啟用安全性選項）（預設為停用），使內部內容來源屬於您所指定的**Tunnel Source Zone**（通道來源區域），以及使內部內容目的地屬於您所指定的**Tunnel Destination Zone**（通道目的地區域）。

   若未**Enable Security Options**（啟用安全性選項），則內部內容來源會屬於與外部通道來源相同的來源區域，而內部內容目的地會屬於與外部通道目的地相同的目的地區域，這意味著它們要遵循適用於外部區域的相同安全性原則規則。
5. 對於**Tunnel Source Zone**（通道來源區域），選取您在上一步中建立的相應通道區域，以便與該區域相關聯的原則適用於通道來源區域。否則，依預設，內部內容會使用與外部通道相同的來源區域，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。
6. 對於**Tunnel Destination Zone**（通道目的地區域），選取您在上一步中建立的相應通道區域，以便與該區域相關聯的原則適用於通道目的地區域。否則，依預設，內部內容會使用與外部通道相同的目的地區域，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。

   如果您為通道檢查原則規則設定了***Tunnel Source Zone***（通道來源區域）和***Tunnel Destination Zone***（通道目的地區域），則應在通道檢查原則規則的相符準則中設定特定的***Source Zone***（來源區域）（步驟3）和特定的***Destination Zone***（目的地區域）（步驟4），而不是指定***Any***（任何）***Source Zone***（來源區域）和***Any***（任何）***Destination Zone***（目的地區域）。此提示可確保區域重新指派方向與上層區域恰當對應。

   在 *PA-5200* 系列或 *PA-7080* 防火牆上，如果您在檢查 *VXLAN* 時使用多點傳送底層，則內部工作階段將在多個資料平面複製，並會發生競爭情況。為避免丟棄部分封包，須符合以下要求：

   - 您必須設定單獨的通道內容檢查規則，以比對流入各 *VXLAN* 通道端點 *(VTEP)* 的 *VXLAN* 封包。
   - 您必須在單獨的規則中指定通道區域。使用不同的通道區域會使各端點的內部工作階段不同。不會發生競爭情況，且不會丟棄封包。
7. 按一下**OK**（確定）。

STEP 10 | 針對與通道檢查原則規則相符的流量設定監控選項。

1. 選取**Policies**（原則） > **Tunnel Inspection**（通道檢查），然後選取您建立的通道檢查原則規則。
2. 選取**Inspection**（檢查） > **Monitor Options**（監控選項）。
3. 輸入**Monitor Name**（監控器名稱），將類似流量分組在一起，以便於記錄和報告。
4. 輸入**Monitor Tag (number)**（監控標籤（號碼）），將類似的流量分組在一起以進行記錄和報告（範圍為 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 *VNI ID*。

   如果您標記通道流量，可稍後在通道檢查日誌中的篩選監控標籤，並使用 *ACC* 檢視基於監控標籤的通道活動。
5. **Override Security Rule Log Setting**（取代安全性規則日誌設定），為滿足所選通道檢查原則規則的工作階段啟用日誌記錄與日誌轉送選項。如果您不選取此設定，通道日誌產生和日誌轉送由適用於通道流量的安全性原則規則的日誌設定所確定。可透過將通道檢查日誌組態設定為分開儲存通道日誌與流量日誌，來取代控制流量日誌的安全性原則規則中的日誌轉送設定。通道檢查日誌儲存外部通道（GRE、非加密 IPSec、VXLAN 或者 GTP-U）工作階段，而流量日誌儲存內部流量。
6. 選取**Log at Session Start**（工作階段開始時記錄），以在工作階段開始時記錄流量。

   通道日誌的最佳做法是在工作階段開始時和結束時均進行記錄，因為通道可保持較長時間。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。如果不在工作階段開始時記錄，將永遠無法在 *ACC* 中看到存在使用中 *GRE* 通道。
7. 選取**Log at Session End**（工作階段結束時記錄），以在工作階段結束時記錄流量。
8. 選取**Log Forwarding**（日誌轉送）設定檔，該設定檔確定防火牆將滿足通道檢查規則的工作階段的通道日誌轉送至何處。或者，如果組態日誌轉送，您可建立新的日誌轉送設定檔。
9. 按一下**OK**（確定）。

STEP 11 | 選用，僅限 VXLAN設定 **VXLAN ID (VNI)**。依預設，會檢查所有 VXLAN 網路介面 (VNI)。如果您設定一個或多個 VXLAN ID，原則僅檢查這些 VNI。

僅 *VXLAN* 通訊協定使用通道 *ID* 頁籤指定 *VNI*。

1. 選取**Tunnel Id**（通道 **ID**）頁籤，然後按一下**Add**（新增）。
2. 指定**Name**（名稱）。名稱的用途是便於使用，不是記錄、監控或報告的一個因素。
3. 在**VXLAN ID (VNI)** 欄位，輸入單個 VNI，以逗號分隔的 VNI 清單，VNI（以連字號當作為分隔符號）的範圍，或以上的組合。例如，您可以指定下列內容：

   1677002,1677003,1677011-1677038,1024

STEP 12 | 選用）若已啟用**Rematch Sessions**（重新比對工作階段）**Device**（裝置） > **Setup**（設定） > **Session**（工作階段）），需針對控制通道安全性原則規則的區域停用**Reject Non-SYN TCP**（拒絕非 **SYN TCP**），確保在您建立或修訂通道檢查原則時，防火牆不會丟棄現有工作階段。

當您執行以下工作時，防火牆將顯示下列警告：

- 建立通道檢查原則規則。
- 透過新增**Protocol**（通訊協定）或將**Maximum Tunnel Inspection Levels**（通道檢查層級數上限）從**One Level**（一層）增加到**Two Levels**（兩層）來編輯通道檢查原則規則。
- 透過新增區域或將一個區域變更為另一個區域，在**Security Options**（安全性選項）頁簽中**Enable Security Options**（啟用安全性選項）。

警告:對現有通道工作階段啟用通道檢查原則，將導致通道內的現有 *TCP* 工作階段被視為非 *SYN TCP* 流量。為了確保在啟用通道檢查原則時，現有工作階段不會被丟棄，使用區域保護設定檔將區域的***Reject Non-SYN TCP***（拒絕非 ***SYN TCP***）設定為***no***（否），然後將其套用於控制通道安全性原則的區域。在防火牆識別現有的工作階段之後，您即可將***Reject Non-SYN TCP***（拒絕非 ***SYN TCP***）設定為***yes***（是）或***global***（全域）來重新啟用該設定。

1. 選取**Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後**Add**（新增） 設定檔。
2. 輸入設定檔的**Name**（名稱）。
3. 選取**Packet Based Attack Protection**（基於封包的攻擊防護） > **TCP Drop**（**TCP** 丟棄）。
4. 對於**Reject Non-SYN TCP**（拒絕非 **SYN TCP**），選取**no**（否）。
5. 按一下**OK**（確定）。
6. 選取**Network**（網路） > **Zones**（區域），然後選取控制通道安全性原則規則的區域。
7. 對於**Zone Protection Profile**（區域保護設定檔），選取您剛剛建立的區域保護設定檔。
8. 按一下**OK**（確定）。
9. 重複前三個子步驟（12f、12g 以及 12h），將區域保護設定檔套用於控制通道安全性原則規則的其他區域。
10. 在防火牆識別現有的工作階段之後，即可將**Reject Non-SYN TCP**（拒絕非 **SYN TCP**）設定為**yes**（是）或**global**（全域）來重新啟用該設定。

STEP 13 | 選用）限制通道內流量分散。

1. 選取**Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），然後依**Name**（名稱）**Add**（新增） 設定檔。
2. 輸入**Description**（描述）。
3. 選取**Packet Based Attack Protection**（基於封包的攻擊防護） > **IP Drop**（**IP** 丟棄） > **Fragmented traffic**（分散的流量）。
4. 按一下**OK**（確定）。
5. 選取**Network**（網路） > **Zones**（區域），然後選取要限制分散的通道區域。
6. 對於**Zone Protection Profile**（區域保護設定檔），選取您剛才建立的設定檔，已將區域保護設定檔套用於通道區域。
7. 按一下**OK**（確定）。

STEP 14 | **Commit**（提交）您的變更。

檢視已檢查的通道活動

執行下列工作，以檢視所檢查通道的活動。

STEP 1 | 選取 **ACC**，然後選取一個 **Virtual System**（虛擬系統）或 **All**（全部）虛擬系統。

STEP 2 | 選取 Tunnel Activity（通道活動）。

STEP 3 | 選取一個時段進行檢視，例如過去 24 小時或過去 30 天。

STEP 4 | 對於 Global Filters（全域篩選器），按一下 + 或 - 按鈕，以對通道活動使用 ACC 篩選器。

STEP 5 | 檢視已檢查的通道獲取哦那個；您可以按 **bytes**（位元組數）、**sessions**（工作階段數）、**threats**（威脅數）、**content**（內容數）或 **URLs**（**URL** 數）顯示並排序每個視窗中的資料。每個視窗都將用圖形和表格的形式顯示通道資料的不同方面：

- 通道 **ID** 使用量—每個通道通訊協定會列出使用該通訊協定之通道的通道 ID。表格中會列出該通訊協定的位元組、工作階段、威脅、內容和 URL 的總數。將游標暫留在通道 ID 上，可顯示每個通道 ID 的詳細資訊。
- 通道監控標籤—每個通道通訊協定會列出使用該標籤之通道的通道監控標籤。表格中會列出該標籤和通訊協定的位元組、工作階段、威脅、內容和 URL 的總數。將游標暫留在通道監控標籤上，可顯示每個標籤的詳細資訊。
- 通道應用程式使用量—應用程式類別以圖形方式顯示了分組為媒體、一般娛樂、協作以及網路的應用程式類型（按風險大小以不同顏色編碼）。應用程式表格還列出了每個應用程式的使用者數目。
- 通道使用者活動—以圖形方式顯示傳送的位元組數、接收的位元組數等，X 軸為日期和時間。將游標暫留在圖中某個點上，可檢視該點的資料。來源使用者和目的地使用者表格中列出了每個使用者的資料。
- 通道來源 **IP** 活動—以圖形和表格方式顯示來自於某個 IP 位址上攻擊者的位元組數、工作階段數以及威脅數。將游標暫留在圖中某個點上，可檢視該點的資料。
- 通道目的地 **IP** 活動—以圖形和表格方式顯示目的地 IP 位址。檢視例如某個 IP 位址上每個受害者遭遇的威脅。將游標暫留在圖中某個點上，可檢視該點的資料。

檢視日誌中的通道資訊

您可以檢視通道檢查日誌本身或檢視其他類型日誌中的通道檢查資訊。

GRE、非加密 **IPSec** 及 **GTP-U** 通訊協定

- 當有相符的 TCI 流量規則時，GRE、IPSec 和 GTP-U 通訊協定將記錄在通道檢查日誌中，包含通道日誌類型、相符的通訊協定、設定的監控名稱及監控標籤（號碼）。
- 當沒有相符的 TCI 規則時，所有通訊協定都將記錄在流量日誌下。

VXLAN 通訊協定

- 當有相符的 TCI 流量規則時，VXLAN 通訊協定將記錄在通道檢查日誌中，包含通道 (VXLAN) 日誌類型、設定的監控名稱及通道 ID (VNI)。

  在內部工作階段的流量日誌中，通道檢查標幟表示 VNI 工作階段。上層工作階段是在建立內部工作階段時執行的工作階段，因此其 ID 可能與目前的工作階段 ID 不符。
- 當沒有相符的 TCI 規則時，VNI 工作階段將記錄在流量日誌中，包含 UDP 通訊協定、來源連接埠 0 和目的地連接埠 4789（預設）。

檢視通道檢查日誌。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Tunnel Inspection**（通道檢查），然後檢視日誌資料，以識別流量中使用的通道 **Applications**（應用程式）以及任何問題，例如未通過嚴格標頭檢查之封包的較大計數等。
2. 按一下詳細日誌檢視 ()，以檢視日誌的詳細資訊。

檢視其他日誌中的通道檢查資訊。

1. 選取 **Monitor**（監控） > **Logs**（日誌）。
2. 選取 **Traffic**（流量）、**Threat**（威脅）、**URL Filtering**（**URL** 篩選）、**WildFire Submissions**（**WildFire** 提交）、**Data Filtering**（資料篩選）或 **Unified**（統一）。
3. 對於日誌項目，按一下詳細日誌檢視 ()。
4. 在 Flags（標幟）視窗中，查看是否已核取 **Tunnel Inspected**（通道已檢查）標幟。通道檢查標幟指示防火牆使用了通道檢查原則來檢查內部內容或內部通道。上層工作階段資訊指外部通道（相對於內部通道）或內部通道（相對於內部內容）。

   在 **Traffic**（流量）、**Threat**（威脅）、**URL Filtering**（**URL** 篩選）、**WildFire Submissions**（**WildFire** 提交）、**Data Filtering**（資料篩選）日誌中，內部工作階段日誌的詳細日誌檢視表中僅顯示上一層資訊，不會顯示通道日誌資訊。如果您設定了兩層通道檢查，則可以顯示該上一層的上層工作階段，以檢視上兩層的日誌。（您必須監控上一步中所示的 **Tunnel Inspection**（通道檢查）日誌，以檢視通道日誌資訊。）
5. 如果您要檢視已檢查通道的內部工作階段日誌，可按一下 General（一般）區段中的 **View Parent Session**（檢視上層工作階段）連結，以查看外部工作階段資訊。

根據標記的通道流量建立自訂報告

您可以根據對通道流量套用的標籤建立報告，以收集資訊。

STEP 1 | 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告），然後按一下 **Add**（新增）。

STEP 2 | 對於 Database（資料庫），選取 Traffic（流量）、Threat（威脅）、URL、Data Filtering（資料篩選）或 WildFire Submissions（WildFire 提交）日誌。

STEP 3 | 對於 Available Columns（可用欄），選取 Flags（標幟）和 Monitor Tag（監控標籤）以及您要在報告中包括的其他資料。

您還可以產生自訂報告。

停用通道加速

依預設，受支援的防火牆執行通道加速，以提高流量通過 GRE 通道、VXLAN 通道和 GTP-U 通道的效能和輸送量。通道加速提供了硬體卸載功能，以減少執行流程查閱所需的時間，並允許通道流量根據內部流量更有效地散佈。

PA-3200 系列防火牆和帶有 PA-7000-100G-NPC-A 與 PA-7050-SMC-B 或 PA-7080-SMC-B 的 PA-7000 系列防火牆支援 GRE 和 VXLAN 通道加速。您可以停用通道加速以進行疑難排解。停用通道加速後，會同時停用 GRE、VXLAN 和 GTP-U 通道的通道加速。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。

STEP 2 | 取消選取 **Tunnel Acceleration**（通道加速）以將其停用。

STEP 3 | 按一下 **OK**（確定）。

STEP 4 | **Commit**（認可）。

STEP 5 | 重新啟動防火牆。

STEP 6 | （選用）驗證通道加速的狀態。

1. 存取 CLI。
2. **> show tunnel-acceleration**

   系統輸出為 **Enabled**（已啟用）或 **Disabled**（已停用）。僅針對 GTP-U 的額外狀態和原因：

   - **Disabled**（已停用）—GTP-U 通道加速在防火牆型號上不受支援或 GTP 安全性已停用。
   - **Error (TCI with GTP-U configured unexpectedly)**（錯誤（意外設定了具有 GTP-U 的 TCI）—當通道加速啟用時，設定了具有 GTP-U 通訊協定的 TCI。
   - **Enabled**（已啟用）—通道加速已啟用；GTP-U 通道加速尚未執行。GTP 安全性已啟用，但尚未重新啟動。
   - **Installed**（已安裝）—GTP-U 通道加速正在執行。

網路封包代理程式

網路封包代理程式篩選網路流量並將其轉送到一個或多個協力廠商安全設備的外部安全鏈。網路封包代理程式替代了 PAN-OS 8.1 中引入的解密代理程式功能，並將其功能擴展為包括轉送非解密 TLS 流量和非 TLS 流量（純文字）以及解密 TLS 流量。處理所有類型流量的能力在金融和政府機構等高度安全的環境中尤其有價值。

PA-7000 系列、PA-5400系列、PA-5200 系列、PA-3200 系列裝置以及 VM-300 和 VM-700 型號裝置支援網路封包代理程式。它需啟用 SSL 正向 Proxy 解密，其中防火牆充當工作階段流量的受信任協力廠商（或媒介）。

防火牆介面不能同時為解密代理程式和 ***GRE*** 通道端點。

網路封包代理程式概觀

如果您使用一個或多個協力廠商安全設備（安全鏈）作為整個安全套件的一部分，則可以使用網路封包代理程式篩選網路流量並將其轉送到這些安全設備。網路封包代理程式取代了 PAN-OS 8.1 中引入的解密代理程式功能。

與解密代理程式一樣，網路封包代理程式提供解密能力和安全鏈管理。這消除了為這些功能提供專用裝置的複雜性，簡化了您的網路，並降低了資本和運營成本。與加密代理程式一樣，網路封包代理程式也提供健康情況檢查，以確保通往安全鏈的路徑是健康的，並提供當一個安全鏈出現故障時處理流量的選項。

網路封包代理程式擴展了防火牆的安全鏈轉送能力，讓您不僅可以篩選並轉送解密 TLS 流量，還可以基於應用程式、使用者、裝置、IP 位址和區域，將非解密 TLS 和非 TLS（純文字）流量轉送到一個或多個安全鏈。這些功能在金融和政府機構等高度安全的環境中尤其有價值。

升級和降級：

- 當您在具有解密代理程式授權的防火牆上升級到 PAN-OS 10.1 時：
  - 在重新啟動防火牆後，授權名稱會自動變更為網路封包代理程式。

    無論防火牆是獨立防火牆還是 *HA* 配對的一部分，抑或是在您將網路封包代理程式授權從 *Panorama* 推送到防火牆時，您都必須重新啟動防火牆才能使授權生效並更新使用者介面。
  - PAN-OS 將任何現有解密代理程式轉送設定檔（**Profiles**（設定檔） > **Decryption**（解密） > **Forwarding Profile**（轉送設定檔））轉譯為封包代理程式設定檔。
  - PAN-OS 將用於轉送流量到安全鏈的任何現有解密原則規則轉譯為網路封包代理程式原則規則。
  - PAN-OS 從使用者介面移除解密代理程式設定檔，並將其替換為封包代理程式設定檔（**Profiles**（設定檔） > **Packet Broker**（封包代理程式）），同時新增網路封包代理程式原則（**Policies**（原則） > **Network Packet Broker**（網路封包代理程式））。
- 當您從 PAN-OS 10.1 降級到 PAN-OS 10.0 時：
  - PAN-OS 將任何現有的封包代理程式設定檔轉譯為解密代理程式轉送設定檔。
  - PAN-OS 會移除網路封包代理程式規則庫並列印一條警告訊息。您必須將網路封包代理程式原則規則重新設定為用於解密轉送的解密原則規則。
  - 授權名稱仍然是網路封包代理程式（重新啟動後，所有 PAN-OS 版本中的授權名稱從解密代理程式變更為網路封包代理程式，且不影響解密代理程式的運作）。但是，該功能是解密代理程式功能，而不是網路封包代理程式功能。
  - PAN-OS 從使用者介面中移除網路封包代理程式設定檔，並將其替換為解密轉送設定檔，同時從使用者介面中移除網路封包代理程式原則（不會發生替換；您使用解密原則規則僅將解密正向 Proxy 流量轉送到安全鏈）。

使用網路封包代理程式的要求：

- 您必須在防火牆上安裝免費的封包代理程式授權。如果沒有此免費授權，您將無法在介面中存取封包代理程式原則和設定檔。

- 防火牆必須至少有兩個可用的 Layer 3 乙太網路介面用作專用封包代理程式轉送介面對。
  - 您可以設定多個專用網路封包代理程式轉送介面對，以連線到不同的安全鏈。
  - 對於每個安全鏈，專用網路封包代理程式介面對必須在同一個安全性區域中。
  - 這對專用介面連線到安全鏈中的第一個和最後一個裝置。

  網路封包代理程式支援路由的 ***Layer 3*** 安全鏈和透明橋接 ***Layer 1*** 安全鏈。對於路由的 ***Layer 3*** 鏈，一個封包代理程式轉送介面對可以使用正確設定的交換器、路由器或其他裝置連線到多個 ***Layer 3*** 安全鏈，以在防火牆和安全鏈之間執行所需的 ***Layer 3*** 路由。
- 專用網路封包代理程式轉送介面無法使用動態路由通訊協定。
- 安全鏈中的所有裝置都不能修改原始工作階段的來源或目的地 IP 位址、來源或目的地連接埠或者通訊協定，因為防火牆無法將修改過的工作階段與原始工作階段進行匹配，從而會丟棄流量。

網路封包代理程式支援：

- 解密 TLS、非解密 TLS 和非 TLS 流量。
- SSL 正向 Proxy、SSL 輸入檢查和加密的 SSH 流量。
- 路由的 Layer 3 安全鏈。
- 透明橋接 Layer 1 安全鏈。

  您可以在同一防火牆上設定路由的 ***Layer 3*** 和 ***Layer 1*** 透明橋接安全鏈，但您必須為每種類型使用不同的轉送介面對。
- 流經鏈的單向流量：進入鏈的所有流量在一個專用介面上流出防火牆，並在另一個專用介面上返回防火牆，因此所有流量都以相同的方向流經專用網路封包代理程式介面對。

  兩個防火牆轉送介面必須在同一區域中。
- 流經安全鏈的雙向流量：
  - 用戶端到伺服器 (c2s) 流量在一個專用防火牆代理程式介面上流出防火牆，並在另一個專用防火牆代理程式介面上返回防火牆。
  - 伺服器到用戶端 (s2c) 流量使用與 c2s 流量相同的兩個專用防火牆代理程式介面，但流量以相反的方向流經安全鏈。s2c 流量進入鏈的防火牆代理程式介面與 c2s 流量從鏈返回防火牆的介面相同。s2c 流量返回防火牆的防火牆代理程式介面與 c2s 流量流出到鏈的介面相同。

  兩個防火牆轉送介面必須在同一區域中。

網路封包代理程式不支援多點傳送、廣播或解密 ***SSH*** 流量。

網路封包代理程式的運作方式

將防火牆連線到一系列協力廠商安全性裝置的高層級工作流程是：

1. 確定要轉送的非解密 TLS、解密 TLS 和非 TLS（TCP 和 UDP）流量。
2. 確定安全鏈拓撲。確定每個安全鏈的裝置是否透明地轉送流量（橋接），或者裝置是否基於 Layer 3 資訊路由流量。使用多個安全鏈有助於負載平衡流量。此外，決定當安全鏈未通過健康情況檢查時，是繞過安全鏈（流量通過防火牆上的正常處理程序，並相應地予以轉送或封鎖）還是封鎖流量。
3. 在將流量轉送到安全鏈的防火牆上安裝免費的網路封包代理程式授權。
4. 確定一個或多個防火牆介面對，以將流量轉送到一個或多個安全鏈，並在這些介面上啟用網路封包代理程式。
5. 設定至少一個封包代理程式設定檔。
6. 設定至少一個網路封包代理程式原則。

要使用一系列協力廠商安全性裝置來檢查流量，請在防火牆上設定三個物件：

- 介面—一個或多個 Layer 3 乙太網路防火牆介面對，用於將流量從防火牆轉送到安全鏈並從安全鏈接收傳回的處理後流量。在設定設定檔和原則規則之前設定網路封包代理程式介面對，因為您需要在設定檔中指定介面對。
- 封包代理程式設定檔—設定檔控制如何將您在原則中定義的流量轉送到安全鏈。每個網路封包代理程式原則規則都有一個關聯的封包代理程式設定檔。設定檔定義安全鏈是路由的 Layer 3 鏈還是 Layer 1 透明橋接鏈、通過鏈的流量方向（單向或雙向）、專用網路封包代理程式防火牆介面以及如何監控防火牆與安全鏈之間連線的健康情況。對於多個路由的 Layer 3 安全鏈，您可以指定每條鏈的第一個和最後一個裝置以及關聯流量的工作階段散佈（負載平衡）方法。
- 網路封包代理程式原則規則—原則規則定義要轉送到每個安全鏈或針對多個路由的 (Layer 3) 鏈進行負載平衡的應用程式流量。原則規則定義要轉送到安全鏈之流量的來源和目的地、使用者、應用程式及服務。原則規則還定義要轉送到安全鏈的流量類型：您可以選擇解密 TLS 流量、非解密 TLS 流量、非 TLS 流量或流量類型的任意組合。您還可以在每個原則規則中新增一個封包代理程式設定檔，以指定要向其轉送流量的安全鏈（以及所有其他設定檔特徵）。

  使用原則最佳化工具檢閱和加強網路封包代理程式原則規則。

為了將應用程式流量與網路封包代理程式原則規則匹配，網路封包代理程式會在防火牆 App-ID 快取中查閱應用程式。如果應用程式不在 App-ID 快取中，則防火牆會繞過安全鏈，並將安全性原則允許規則中設定的任何威脅檢查套用至流量。如果應用程式位於 App-ID 快取中，則防火牆以網路封包代理程式原則規則及其關聯封包代理程式設定檔中指定的方式將流量轉送到安全鏈。

對於非解密 TLS 和非 TLS 流量，防火牆將在第一個工作階段的 App-ID 快取中安裝應用程式，因此防火牆按照網路封包代理程式原則和設定檔中指定的方式處理流量。

對於解密 TLS 流量，在應用程式的第一個工作階段中，網路封包代理程式不知道工作階段正在被解密，並將「ssl」視為應用程式。底層特定應用程式尚不可知或未安裝在 App-ID 快取中，因此代理程式查閱失敗且流量會繞過安全鏈。流量仍受安全性原則允許規則上設定的任何威脅檢查的約束。當防火牆解密流量時，防火牆會瞭解該特定應用程式並將其安裝在 App-ID 快取中。對於同一應用程式的第二個和後續解密工作階段，由於該特定應用程式現在已位於 App-ID 快取中，網路封包代理程式將查閱成功，且防火牆會按預期將流量轉送到安全鏈。

準備部署網路封包代理程式

採取以下動作為部署網路封包代理程式做準備：

1. 獲取並啟動免費網路封包代理程式授權。
   1. 登入客戶支援入口網站。
   2. 在左側導覽窗格上，選取 **Assets**（資產） > **Devices**（裝置）。
   3. 找到要在其中啟用解密代理程式或解密連接埠鏡像的裝置，然後選取 **Actions**（動作）（鉛筆圖示）。
   4. 在 Activate Licenses（啟動授權）下方，選取 **Activate Feature License**（啟動功能授權）
   5. 選取 **Network Packet Broker**（網路封包代理程式）免費授權。
   6. 按一下 **Agree and Submit**（同意並提交）。
2. 在防火牆上安裝授權。
   1. 選取 **Device**（裝置） > **Licenses**（授權）
   2. 按一下 **Retrieve license keys from the license server**（從授權伺服器擷取授權金鑰）。
   3. 確認 **Device**（裝置） > **Licenses**（授權）頁面顯示網路封包代理程式授權現在已在防火牆上處於作用狀態。
   4. 重新啟動防火牆（**Device**（裝置） > **Setup**（設定） > **Operations**（操作））。在防火牆重新啟動之前，網路封包代理程式無法進行設定。

      您可以將網路封包代理程式授權從 *Panorama* 推送至受管理防火牆。您必須重新啟動防火牆才能使授權生效並更新使用者介面。
3. 為網路封包代理程式啟用 App-ID 快取。
   1. App-ID 預設停用。使用設定模式 CLI 命令將其啟用：

      ```
      admin@PA-3260# set deviceconfig setting application cache yes
      ```
   2. 啟用防火牆使用 App-ID 快取來識別應用程式：

      ```
      admin@PA-3260# set deviceconfig setting application use-cache-
      for-identification yes
      ```

   查看設定，確認 `Application cache`（應用程式快取）設定為 `yes`（是），且 `Use cache for appid`（將快取用於 `appid`）設定為 `yes`（是）：

   ```
   admin@PA-3260> show running application setting
   Application setting:
   Application cache              : yes
   Supernode                      : yes
   Heuristics                     : yes
   Cache Threshold                : 1
   Bypass when exceeds queue limit: no
   Traceroute appid               : yes
   ```

```
Traceroute TTL threshold      : 30
Use cache for appid           : yes
Use simple appsigs for ident  : yes
Use AppID cache on SSL/SNI    : no
Unknown capture               : on
Max. unknown sessions         : 5000
Current unknown sessions      : 33
Application capture           : off
```

```
Current APPID Signature
   Memory Usage               : 16768  KB (Actual 16461  KB)
      TCP 1 C2S               : regex 11898  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4263   states
      UDP 1 S2C               : regex 1605   states
```

4. 確定要轉送到一個或多個安全鏈的流量。
5. 確定每個安全鏈的拓撲，並確定是使用 Layer 1 透明橋接轉送還是路由的 Layer 3 轉送，從而確定您在防火牆上設定哪種類型的安全鏈。考量事項包括：
   - 您是想跨多個鏈負載平衡流量（使用路由的 Layer 3 安全鏈透過路由器、交換器或其他路由裝置跨多個鏈散佈工作階段）、使用單個鏈，還是對不同類型的流量使用不同的安全鏈。對於多個 Layer 1 透明橋接鏈，您需要為每個安全鏈提供一個專用防火牆介面對，因為 Layer 1 連線不會路由。
   - 是使用單向還是雙向流量流經安全鏈。
6. 決定將哪些防火牆介面對用作專用網路封包代理程式轉送介面。
   - 對於多個 Layer 1 透明橋接鏈，您需要為每個 Layer 1 安全鏈提供一個專用防火牆介面對。您可以設定原則規則，向不同的安全鏈傳送特定流量。
   - 對於路由的 Layer 3 鏈，一個專用防火牆介面對可以透過交換器、路由器或其他能夠路由的裝置在多個 Layer 3 安全鏈之間負載平衡流量。
   - 對於路由的 Layer 3 鏈，您可以使用多個專用防火牆介面對使用不同的原則規則向不同的安全鏈傳送特定流量。

設定透明橋接安全鏈

Layer 1 透明橋接安全鏈透過一系列直接連線的資料檢查和處理安全裝置，從一個防火牆介面轉送流量，然後再透過另一防火牆介面傳回流量，而無需路由流量。

在設定 Layer 1 透明橋接安全鏈之前，請採取步驟 準備部署網路封包代理程式，並確保防火牆與安全鏈裝置之間的實體連線正確。

若要跨多個透明橋接安全鏈散佈工作階段，請在防火牆上為您要用於負載平衡流量的每個安全鏈建立一個 Layer 1 透明橋接安全鏈。防火牆上的每個透明橋接安全鏈都需要兩個專用的 Layer 3 乙太網路介面。檢查以確保您擁有足夠的空閒乙太網路介面用於要設定的拓撲。

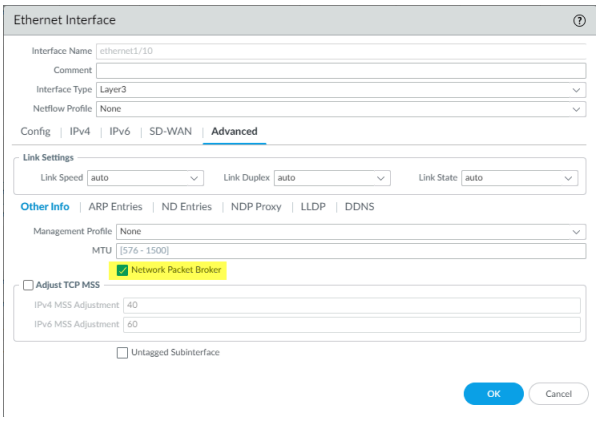
Layer 1 透明橋接安全鏈無法容錯移轉至另一個安全鏈，因為它們未路由。

STEP 1 | 啟用兩個 Layer 3 乙太網路介面作為網路封包代理程式轉送介面。

1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。
2. 選取一個未使用的乙太網路介面作為兩個網路封包代理程式轉送介面中的一個。
3. 將 **Interface Type**（介面類型）設為 **Layer3**。
4. 在 **Config**（設定）索引標籤上，選取一個要向其指派介面的區域。

   您必須在同一區域中設定兩個安全鏈介面。

5. 最佳做法是，在 **Config**（設定）索引標籤上，使用或建立一個專用虛擬路由器來指派介面。使用專用的虛擬路由器可確保網路封包代理程式介面流量與其他流量保持分離。
6. 選取 **Advanced**（進階），然後選取 **Network Packet Broker**（網路封包代理程式）以啟用介面。



7. 按一下 **OK**（確定）儲存介面組態。
8. 在另一個未使用的乙太網路介面上重複此程序以設定另一個網路封包代理程式轉送介面。

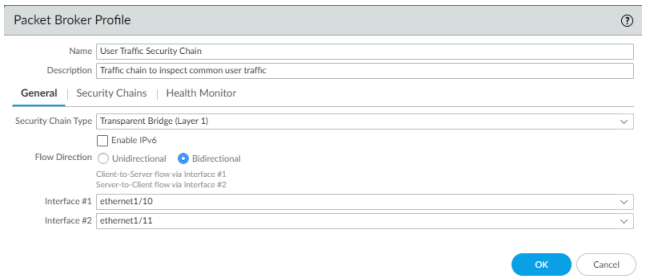
STEP 2 | 設定封包代理程式設定檔以控制如何將流量轉送到 Layer 1 透明橋接安全鏈。

1. 選取 **Objects**（物件） > **Packet Broker Profile**（封包代理程式設定檔），然後 **Add**（新增）新設定檔或修改現有設定檔。
2. 為設定檔提供 **Name**（名稱）和 **Description**（說明），以便您可以輕鬆識別其用途。
3. 在 **General**（一般）索引標籤上：
   - 選取 **Transparent Bridge (Layer 1)**（透明橋接 **(Layer 1)**）作為 **Security Chain Type**（安全鏈類型）。
   - 如果流量為 IPv6 流量，請 **Enable IPv6**（啟用 **IPv6**）。
   - 選取 **Flow Direction**（流量方向）。

     您的網路拓撲決定了使用單向流還是雙向流。使用任一方法的效能大致相同。

     要使用一個防火牆介面將 c2s 和 s2c 工作階段流轉送到安全鏈，並使用另一個防火牆介面接收從安全鏈傳回的這兩個工作階段流，則選取 **Unidirectional**（單向）。

     要使用介面 **1** 將 c2s 流轉送到安全鏈並接收來自安全鏈的 s2c 流，同時使用介面 **2** 將 s2c 流轉送到安全鏈並接收來自安全鏈的 c2s 流，則選取 **Bidirectional**（雙向）。
   - 在介面 **1** 和介面 **2** 中指定網路封包代理程式轉送介面對。必須同時啟用兩個介面才能使用網路封包代理程式（參見 準備部署網路封包代理程式）。在設定哪個介面是介面 **1** 以及哪個介面是介面 **2** 時，請注意流向。



4. **Security Chains**（安全鏈）索引標籤不用於透明橋接。
5. 在 **Health Monitor**（健康情況監控）索引標籤上：
   - 選取您想要執行的一種或多種健康情況監控類型，以便您可以控制在安全鏈出現故障時發生的情況。您可以選取 **Path Monitoring**（路徑監控）、**HTTP Monitoring**（**HTTP** 監控）和 **HTTP Monitoring Latency**（**HTTP** 監控延遲）中的一個、兩個或全部。

     Path Monitoring（路徑監控）— 使用 ping 檢查裝置連線。

     HTTP Monitoring（**HTTP** 監控）— 檢查裝置可用性和回應時間。

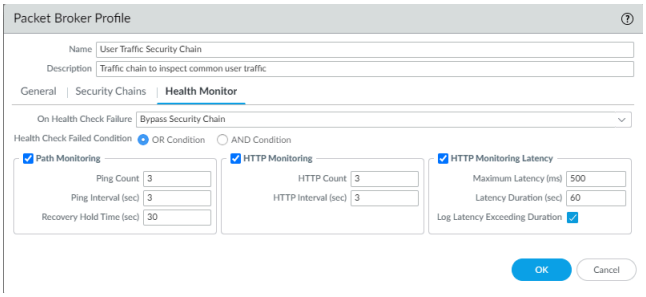
     HTTP Monitoring Latency（**HTTP** 監控延遲）— 檢查裝置處理速度和效率。當您選取此選項時，也會自動啟用 **HTTP Monitoring**（**HTTP** 監控）。
   - 啟用一種或多種類型的健康情況監控會啟用 **On Health Check Failure**（當健康情況檢查失敗時）選項，該選項確定當出現安全鏈健康情況故障時，防火牆如何處理安全鏈流量。選項包括 **Bypass Security Chain**（繞過安全鏈）和 **Block Session**（封鎖工作階段）。

Bypass Security Chain（繞過安全鏈）— 防火牆將流量轉送到其目的地而不是安全鏈，並將任何設定的安全設定檔和保護套用至流量。

Block Session（封鎖工作階段）— 防火牆封鎖工作階段。

您選取的方式取決於，當無法透過安全鏈執行流量時，您希望如何處理流量。

- 如果您選取多個健康情況檢查選項，請選取希望當任何一個監控選項記錄到失敗條件（**OR Condition**（**OR** 條件））時，防火牆將健康情況檢查視為失敗（健康情況檢查失敗條件），還是僅當所有選定監控選項都記錄到失敗條件（**AND Condition**（**AND** 條件））時，才將健康情況檢查視為失敗。例如，如果您啟用全部三個健康情況檢查選項且其中一個選項記錄到失敗條件，如果您已選取 **OR Condition**（**OR** 條件），則防火牆認為安全鏈連線失敗，並執行您在 **On Health Check Failure**（當健康情況檢查失敗時）中指定的動作。如果您選取了 **AND Condition**（**AND** 條件），防火牆仍會認為連線是健康的，因為其中兩個健康指標仍然正常。



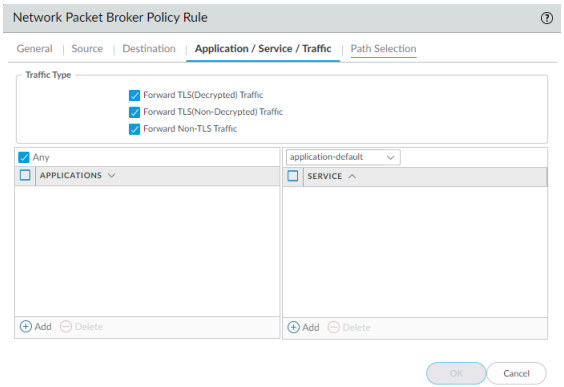
6. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 設定封包代理程式原則以定義要轉送到 Layer 1 透明橋接安全鏈的流量。

1. 選取 **Policies**（原則） > **Network Packet Broker**（網路封包代理程式），然後 **Add**（新增）新原則規則或修改現有原則規則。
2. 在 **General**（一般）索引標籤上，為原則規則提供 **Name**（名稱）和 **Description**（說明），以便您可以輕鬆識別其用途。新增 **Audit Comment**（稽核註解），並套用標籤（如果您使用標籤）。
3. 在 **Source**（來源）索引標籤上，確定您希望規則轉送到安全鏈的流量的來源區域、IP 位址、使用者和裝置。
4. 在 **Destination**（目的地）索引標籤上，確定您希望規則轉送到安全鏈的流量的目的地區域、IP 位址和裝置。
5. 在 **Application/Service/Traffic**（應用程式/服務/流量）索引標籤上，確定您希望規則轉送到安全鏈的應用程式和服務。除非是您希望使用非標準連接埠的規則控制應用程式（如內部自訂應用程式），否則最佳做法是將 **Service**（服務）設定為 **Application Default**（應用程式預設值），以便封鎖應用程式透過使用非標準連接埠實現迴避。

   對於 **Traffic Type**（流量類型），選取您希望規則轉送到安全鏈的所有流量類型。**Forward TLS(Decrypted) Traffic**（轉送 **TLS**（解密）流量）是預設選擇。您可以選取 **Forward TLS(Decrypted) Traffic**（轉送 **TLS**（解密）流量）、**Forward TLS(Non-Decrypted)**（轉送

TLS（非解密））和 **Forward Non-TLS Traffic**（轉送非 **TLS** 流量）的任意組合以轉送到安全鏈。



6. 在 **Path Selection**（路徑選擇）索引標籤上，選取您在步驟 2 中建立的封包代理程式設定檔，或建立一個新設定檔，來控制如何將原則規則控制的流量傳送到安全鏈。

STEP 4 | 重複步驟 1 到步驟 3，建立更多 Layer 1 透明橋接安全鏈。

對於每一個 Layer 1 透明橋接安全鏈：

- 用作網路封包代理程式轉送介面的兩個乙太網路介面必須專用於每個安全鏈。用於透明橋接安全鏈的乙太網路介面不能用於任何其他用途或承載任何其他流量。
- 每個網路封包代理程式轉送介面對都會連線到一個 Layer 1 透明橋接安全鏈。

您可以建立網路封包代理程式原則規則來負載平衡流量，這些規則將在透明橋接安全鏈之間相對平均地分割流量。您也可以使用原則規則，引導特定流量和流量類型通過特定安全鏈。

Layer 1 透明橋接安全鏈無法容錯移轉至另一個安全鏈，因為它們未路由。使用封包代理程式設定檔中的 ***Health Monitor***（健康情況監控）索引標籤，設定當透明橋接安全鏈故障時如何處理流量。

設定路由的 Layer 3 安全鏈

路由的 Layer 3 安全鏈將流量轉送到一系列資料檢查和處理安全裝置，然後使用防火牆上的兩個專用轉送介面返回防火牆。

在設定路由的 Layer 3 安全鏈之前，請採取步驟 準備部署網路封包代理程式，並確保防火牆與安全鏈裝置之間的實體連線正確。檢查以確保防火牆上有足夠的空閒乙太網路介面用於要設定的拓撲。

您在防火牆上設定的每個路由的 Layer 3 安全鏈都需要兩個專用的 Layer 3 乙太網路介面，它們可以連線到一個 Layer 3 安全鍊，或者使用防火牆與安全鏈之間適當設定的路由器、交換器或類似裝置將工作階段（負載平衡）散佈到最多 64 個 Layer 3 安全鏈。

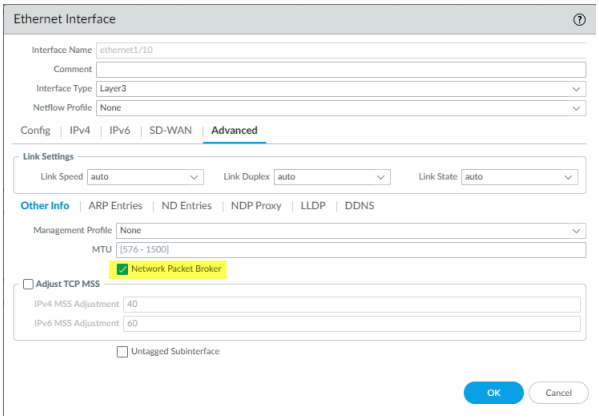
網路封包代理程式無法在路由的 *Layer 3* 安全鏈上轉送 *IPv6* 流量。要轉送 *IPv6* 流量，請使用透明橋接 *(Layer 1)* 安全鏈。

STEP 1 | 啟用兩個 Layer 3 乙太網路介面作為網路封包代理程式轉送介面。

1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。
2. 選取一個未使用的乙太網路介面作為兩個網路封包代理程式轉送介面中的一個。
3. 將 **Interface Type**（介面類型）設為 **Layer3**。
4. 在 **Config**（設定）索引標籤上，選取一個要向其指派介面的區域。

   您必須在同一區域中設定兩個安全鏈介面。

5. 最佳做法是，在 **Config**（設定）索引標籤上，使用或建立一個專用虛擬路由器來指派介面。使用專用的虛擬路由器可確保網路封包代理程式介面流量與其他流量保持分離。
6. 選取 **Advanced**（進階），然後選取 **Network Packet Broker**（網路封包代理程式）以啟用介面。



7. 按一下 **OK**（確定）儲存介面組態。
8. 在另一個未使用的乙太網路介面上重複此程序以設定另一個網路封包代理程式轉送介面。

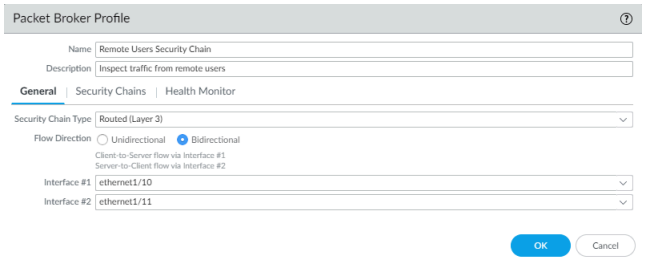
STEP 2 | 設定封包代理程式設定檔以控制如何將流量轉送到路由的 Layer 3 安全鏈。

1. 選取 **Objects**（物件） > **Packet Broker Profile**（封包代理程式設定檔），然後 **Add**（新增）新設定檔或修改現有設定檔。
2. 為設定檔提供 **Name**（名稱）和 **Description**（說明），以便您可以輕鬆識別其用途。
3. 在 **General**（一般）索引標籤上：
   - 選取 **Routed (Layer 3)**（已路由 **(Layer 3)**）作為 **Security Chain Type**（安全鏈類型）。
   - 選取 **Flow Direction**（流量方向）。

     您的網路拓撲決定了使用單向流還是雙向流。使用任一方法的效能大致相同。

     要使用一個防火牆介面將 c2s 和 s2c 工作階段流轉送到安全鏈，並使用另一個防火牆介面接收從安全鏈傳回的這兩個工作階段流，則選取 **Unidirectional**（單向）。

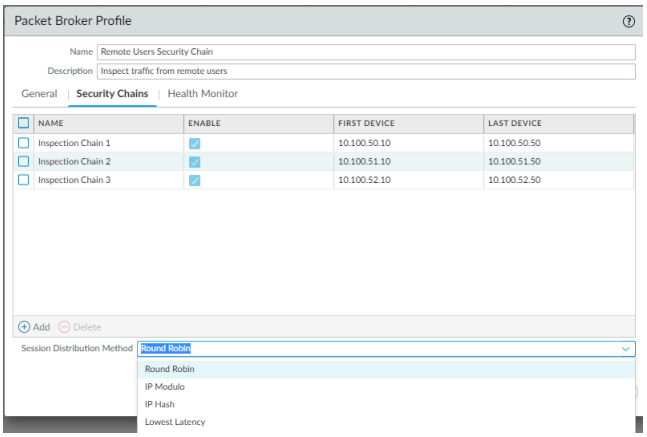
     要使用介面 **1** 將 c2s 流轉送到安全鏈並接收來自安全鏈的 s2c 流，同時使用介面 **2** 將 s2c 流轉送到安全鏈並接收來自安全鏈的 c2s 流，則選取 **Bidirectional**（雙向）。
   - 在介面 **1** 和介面 **2** 中指定網路封包代理程式轉送介面對。必須同時啟用兩個介面才能使用網路封包代理程式（參見步驟 1）。在設定哪個介面是介面 **1** 以及哪個介面是介面 **2** 時，請注意流向。



工作階段散佈（負載平衡）僅適用於新工作階段。防火牆不會在工作階段中間重新平衡流量。防火牆僅將工作階段散佈到狀態為「*up*」（作用中、健康）的安全鏈。

4. 在 **Security Chains**（安全鏈）索引標籤上，**Add**（新增）要連線的每個路由的 Layer 3 安全鏈中第一個和最後一個裝置的 IP 位址。您必須至少指定一個安全鏈，否則防火牆無法將流量路由到安全鏈，且您無法儲存設定檔。

   如果指定多個路由的 Layer 3 安全鏈，則還需要在防火牆和安全鏈之間放置正確設定的路由器、交換器或類似裝置以執行正確的路由。此外，指定 **Session Distribution Method**（工作階段散佈方式）以負載平衡安全鏈之間的流量。



5. 在 **Health Monitor**（健康情況監控）索引標籤上：

   - 選取您想要執行的一種或多種健康情況監控類型，以便您可以控制在安全鏈出現故障時發生的情況。

     您可以選取 **Path Monitoring**（路徑監控）、**HTTP Monitoring**（**HTTP** 監控）和 **HTTP Monitoring Latency**（**HTTP** 監控延遲）中的一個、兩個或全部。

     Path Monitoring（路徑監控）— 使用 ping 檢查裝置連線。

     HTTP Monitoring（**HTTP** 監控）— 檢查裝置可用性和回應時間。

     HTTP Monitoring Latency（**HTTP** 監控延遲）— 檢查裝置處理速度和效率。當您選取此選項時，也會自動啟用 **HTTP Monitoring**（**HTTP** 監控）。

   - 啟用一種或多種類型的健康情況監控會啟用 **On Health Check Failure**（當健康情況檢查失敗時）選項，該選項確定當出現安全鏈健康情況故障時，防火牆如何處理安全鏈流量。

     如果在一組路由的 Layer 3 網路封包代理程式介面上設定了多個安全鏈，則在一個安全鏈發生故障時，流量將容錯移轉到其余健康的安全鏈。如果沒有可用於處理容錯移轉流量的安全鏈，防火牆將採取 **On Health Check Failure**（當健康情況檢查失敗時）中設定的動作。選項包括 **Bypass Security Chain**（繞過安全鏈）和 **Block Session**（封鎖工作階段）。

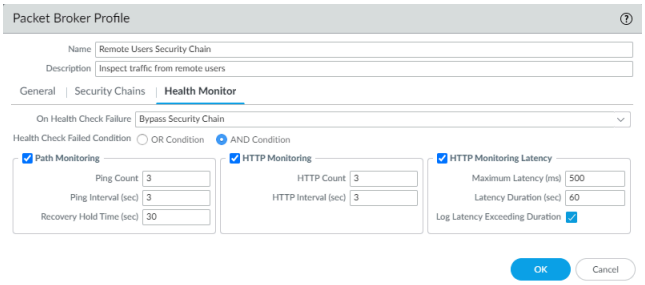
     Bypass Security Chain（繞過安全鏈）— 防火牆將流量轉送到其目的地而不是安全鏈，並將任何設定的安全設定檔和保護套用至流量。

     Block Session（封鎖工作階段）— 防火牆封鎖工作階段。

     您選取的方式取決於，當無法透過安全鏈執行流量時，您希望如何處理流量。

   - 如果您選取多個健康情況檢查選項，請選取希望當任何一個監控選項記錄到失敗條件（**OR Condition**（**OR** 條件））時，防火牆將健康情況檢查視為失敗（健康情況檢查失敗條件），還是僅當所有選定監控選項都記錄到失敗條件（**AND Condition**（**AND** 條件））時，才將健康情況檢查視為失敗。例如，如果您啟用全部三個健康情況檢查選項且其中一個選項記錄到失敗條件，如果您已選取 **OR Condition**（**OR** 條件），則防火牆認為安全鏈連線失敗，並執行您在 **On Health Check Failure**（當健康情況檢查失敗時）中

指定的動作。如果您選取了 **AND Condition**（**AND** 條件），防火牆仍會認為連線是健康的，因為其中兩個健康指標仍然正常。

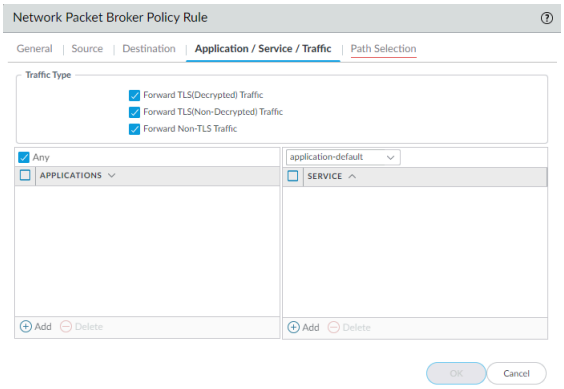


6. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 設定封包代理程式原則以定義要轉送到路由的 Layer 3 安全鏈的流量。

1. 選取 **Policies**（原則） > **Network Packet Broker**（網路封包代理程式），然後 **Add**（新增）新原則規則或修改現有原則規則。
2. 在 **General**（一般）索引標籤上，為原則規則提供 **Name**（名稱）和 **Description**（說明），以便您可以輕鬆識別其用途。新增 **Audit Comment**（稽核註解），並套用標籤（如果您使用標籤）。
3. 在 **Source**（來源）索引標籤上，確定您希望規則轉送到安全鏈的流量的來源區域、IP 位址、使用者和裝置。
4. 在 **Destination**（目的地）索引標籤上，確定您希望規則轉送到安全鏈的流量的目的地區域、IP 位址和裝置。
5. 在 **Application/Service/Traffic**（應用程式/服務/流量）索引標籤上，確定您希望規則轉送到安全鏈的應用程式和服務。除非是您希望使用非標準連接埠的規則控制應用程式（如內部自訂應用程式），否則最佳做法是將 **Service**（服務）設定為 **Application Default**（應用程式預設值），以便封鎖應用程式透過使用非標準連接埠實現迴避。

   對於 **Traffic Type**（流量類型），選取您希望規則轉送到安全鏈的所有流量類型。**Forward TLS(Decrypted) Traffic**（轉送 **TLS**（解密）流量）是預設選擇。您可以選取 **Forward TLS(Decrypted) Traffic**（轉送 **TLS**（解密）流量）、**Forward TLS(Non-Decrypted)**（轉送 **TLS**（非解密））和 **Forward Non-TLS Traffic**（轉送非 **TLS** 流量）的任意組合以轉送到安全鏈。



6. 在 **Path Selection**（路徑選擇）索引標籤上，選取您在步驟 2 中建立的封包代理程式設定檔，或建立一個新設定檔，來控制如何將原則規則控制的流量傳送到安全鏈。

STEP 4 | 如果要建立使用不同專用防火牆介面對的單獨路由 Layer 3 安全鏈，請重複步驟 1 到步驟 3 以建立更多網路封包代理程式安全鏈。用作網路封包代理程式轉送介面的兩個 Layer 3 乙太網路介面必須專用於安全鏈，不能用於任何其他用途或承載任何其他流量。

網路封包代理程式 HA 支援

除了使用封包代理程式設定檔中可用的路徑和延遲健康情況監控來防止安全鏈故障外，您也可以在具有網路封包代理程式轉送介面的防火牆上設定高可用性 (HA)，以防止防火牆故障。設定路徑監控和 HA 不僅可防止安全鏈故障，還可防止防火牆故障。

網路封包代理程式支援主動/被動 HA 配對。主動/主動 HA 配對不受支援，因為必須在封包代理程式設定檔中指定專用代理程式轉送介面。

容錯移轉後，解密 SSL 流量會重設，因為 SSL 狀態未在 HA 節點之間同步。如果工作階段已正確同步，且已正確地重新學習 TCP 順序，則純文字流量會繼續。

網路封包代理程式的使用者介面變更

網路封包代理程式替代了 PAN-OS 8.1 中引入的解密代理程式功能，並將其功能擴展為包括將非解密 TLS 和非 TLS 以及解密 TLS 流量轉送到安全鏈。為了支援網路封包代理程式，PAN-OS 10.1 使用者介面進行了以下變更：

- 新原則（**Policies**（原則） > **Network Packet Broker**（網路封包代理程式））讓您能夠設定要轉送到安全鏈的特定流量，並附加一個網路封包代理程式設定檔來控制如何將指定流量轉送到安全鏈。

  解密代理程式使用解密原則規則僅將解密 *TLS* 流量轉送到安全鏈。新的網路封包代理程式原則規則讓您不僅可以選擇解密的 *TLS* 流量，還可以選擇加密的 *TLS* 流量和非 *TLS* 流量。

- 新設定檔（**Objects**（物件） > **Packet Broker Profile**（封包代理程式設定檔））取代舊設定檔（**Objects**（物件） > **Decryption**（解密） > **Decryption Broker Profile**（解密代理程式設定檔）），讓您能夠準確設定如何將流量轉送到安全鏈以及監控路徑和延遲健康情況。在 **General**（一般）索引標籤上，您輸入專用防火牆網路封包代理程式轉送介面對的欄位名稱分別從「主要介面」和「次要介面」變更為 **Interface #1**（介面 **1**）和 **Interface #2**（介面 **2**）。

- 當您選取 **Policies**（原則） > **Network Packet Broker**（網路封包代理程式）時，之後您可以在 **Policy Optimizer**（原則最佳化工具）中選取任何 Rule Usage（規則使用情況）選項，來檢視網路封包代理程式原則使用情況資訊。**Rule Usage**（規則使用情況）統計資料可幫助您評估是需要保留未使用的網路封包代理程式規則，還是可以將其刪除並收緊規則庫以減少攻擊面。

- 由於網路封包代理程式取代了解密代理程式，解密原則不再處理到安全鏈的代理流量。出於該原因，在 **Options**（選項）索引標籤上，**Decrypt and Forward**（解密並轉送）選項不再是原則可採取的 **Action**（動作），**Forwarding Profile**（轉送設定檔）欄位也會移除，因為現在，解密設定檔僅在解密原則上有效。

- 在 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）中，當您將 **Interface Type**（介面類型）設定為 Layer 3，然後選取 **Advanced**（進階）索引標籤時，用於啟用介面作為網路封包代理程式之轉送介面的核取方塊的名稱從「解密轉送」變更為 **Network Packet Broker**（網路封包代理程式）。

- 對於 **Device**（裝置） > **Admin Roles**（管理員角色），在 **Web UI** 索引標籤上，有兩處變更：

  - 在 **Policies**（原則）下，您現在可以設定 **Network Packet Broker**（網路封包代理程式）管理員角色權限。
  - 在 **Objects**（物件）下，**Decryption**（解密） > **Forwarding Profile**（轉送設定檔）選項已移除，並替換為用於管理員角色權限的 **Packet Broker Profile**（封包代理程式設定檔）選項。

- 在防火牆上，對於 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告），當您從「詳細日誌」中選取 **Traffic Log**（流量日誌）作為 **Database**（資料庫）時，在 **Available Columns**（可用欄）清單中，您現在可以選取 **Forwarded to Security Chain**（已轉送至安全鏈）。

  在 Panorama 上，對於 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告），當您從「詳細日誌」中選取 **Panorama Traffic Log**（**Panorama** 流量日誌）作為 **Database**（資料庫）時，在 **Available Columns**（可用欄）清單中，您現在可以選取 **Forwarded to Security Chain**（已轉送至安全鏈）。

- 在流量日誌中，「解密轉送」欄已重新命名為 **Forwarded to Security Chain**（已轉送至安全鏈）。在流量日誌的詳細檢視中，在 **Flags**（標幟）區段，核取方塊「解密已轉送」已重新命名為 **Forwarded to Security Chain**（已轉送至安全鏈）。
- 該功能的免費授權從「解密代理程式」重新命名為 **Packet Broker**（封包代理程式）。如果您的防火牆上有免費的解密代理程式授權，當您升級到 PAN-OS 10.1 時，名稱會自動變更。僅名稱發生變更，對功能沒有影響。

網路封包代理程式的限制

大多數 Palo Alto Networks 平台支援網路封包代理程式，但有部分不支援，也有部分存在一些限制：

- Prisma Access 或 NSX 中不支援。
- AWS、Azure 和 GCP 僅支援路由的 Layer 3 安全鏈。

網路封包代理程式在 Panorama 上對受管理防火牆有一些限制，另有一些使用限制。在 Panorama 上：

- 如果您將網路封包代理程式授權推送至受管理防火牆，則必須重新啟動防火牆，才能安裝授權和相關聯的使用者介面元素。
- 您無法在共用內容中建立封包代理程式設定檔，因為您在封包代理程式設定檔中設定特定介面。
- 不同的裝置群組無法共用相同的封包代理程式設定檔。
- Panorama 無法將網路封包代理程式設定（網路封包代理程式原則規則和設定檔）推送至包含執行早於 10.1 之 PAN-OS 版本的防火牆的裝置群組。

  如果您希望在某個裝置群組中使用網路封包代理程式，而該裝置群組包含執行多個 PAN-OS 版本的防火牆，且其中部分防火牆執行早於 10.1 的 PAN-OS 版本執行，則必須先將 10.1 之前的防火牆升級至 PAN-OS 10.1，或從裝置群組移除 10.1 之前的防火牆，然後才能推送網路封包代理程式設定。

  > 您可以使用 ***Panorama*** 將附加至解密原則規則的封包代理程式設定檔推送到已安裝解密代理程式授權的 ***10.1*** 之前的防火牆。規則（***Options***（選項）索引標籤）的 ***Action***（動作）必須是 ***Decrypt and Forward***（解密並轉送），且您必須將封包代理程式設定檔附加到規則（***Options***（選項）索引標籤上的 ***Decryption Profile***（解密設定檔）設定）。***10.1*** 之前的防火牆將封包代理程式設定檔用作解密代理程式的解密轉送設定檔。解密原則規則會確定防火牆套用資料檔的流量。
  >
  > 解密原則規則控制的流量必須是解密 ***SSL*** 流量（解密代理程式不支援加密的 ***SSL*** 流量或純文字流量）。

- 當您從 PAN-OS 10.0 升級至 PAN-OS 10.1 時，只有用於解密代理程式的本機解密原則規則會移轉至網路封包代理程式規則。從 Panorama 推送至防火牆的解密代理程式原則規則會在 Panorama 上自動移轉，但不會在防火牆上自動移轉。在防火牆上本機設定的解密代理程式原則規則只會移轉至該防火牆上的網路封包代理程式規則。對於在 Panorama 上設定的規則，Panorama 必須對防火牆執行另一次提交推送，才能同步已移轉至 Panorama 上的網路封包代理程式規則的解密代理程式規則。
- 當您從 PAN-OS 10.1 降級到 PAN-OS 10.0 時，網路封包代理程式規則會自動移除。

網路封包代理程式也有一些使用限制：

- 如果網路封包代理程式防火牆也會執行來源網路位址轉譯 (SNAT)，且流量為純文字流量，則防火牆會對流量執行 NAT，並將流量轉送至安全鏈。安全鏈設備只會看到 NAT 位址，而不會看到原始來源位址：

  1. 防火牆會對用戶端的流量執行 NAT。
  2. 防火牆會將流量轉送至安全鏈，且所有路由都必須基於 NAT 位址。
  3. 由於封包中的來源位址現在是 NAT 位址，因此安全鏈設備只會看到 NAT 位址。它們看不到實際的用戶端來源位址。
  4. 當安全鏈將流量傳回到防火牆時，結果是防火牆不知道使用者是誰。

  您可以透過檢查工作階段的流量日誌並將封包與這些日誌關聯，來找出該工作階段的來源使用者。流量日誌包含原始來源位址（您可以從中判斷來源使用者）和 SNAT 位址。

  您可以在防火牆之外的裝置上執行 *NAT* 來避免這種情況。

- 不支援解密 SSH、多點傳送和廣播流量。
- 使用 RSA 憑證時，SSL 輸入檢查不支援用戶端驗證。
- 在 Layer 1 透明橋接模式中，如果安全鏈發生故障，不會進行容錯移轉，因為當您使用透明橋接連線時，每對專用網路封包代理程式防火牆介面只會連線到一個安全鏈。（您無法路由 Layer 1 上的流量，只能將其轉送到下一個連線的裝置。）
- 您只能在 Layer 1 透明橋接模式中轉送 IPv6 流量。您無法在已路由 (Layer 3) 模式中轉送 IPv6 流量。
- 您無法使用通道或回送介面作為網路封包代理程式介面。
- 網路封包代理程式介面無法使用動態路由通訊協定。
- 兩個介面都必須位於同一區域。
- 安全鏈中的裝置無法修改原始工作階段的來源 IP 位址、目的地 IP 位址、來源連接埠、目的地連接埠或通訊協定，因為防火牆無法將修改過的工作階段與原始工作階段進行匹配，從而會丟棄流量
- 僅對於主動/被動 HA 防火牆配對支援網路封包代理程式的高可用性。對於主動/主動防火牆配對，則不支援網路封包代理程式的高可用性。
- SSL 流量不支援高可用性。容錯移轉時會重設 SSL 工作階段。
- 當您從 PAN-OS 10.0 升級至 PAN-OS 10.1 時，用於解密代理程式的本機解密原則規則會移轉至網路封包代理程式規則。
- 當您從 PAN-OS 10.1 降級到 PAN-OS 10.0 時，網路封包代理程式規則會自動移除。

對網路封包代理程式進行疑難排解

如果您在設定網路封包代理程式時遇到問題，請檢查以下項目：

- 防火牆設定：
  - 檢查轉送介面對上的下一個躍點路由，確保其指定了正確的裝置介面。
  - 鏈裝置和防火牆介面的 IP 位址，確保在封包代理程式設定檔中正確輸入了此等資訊。
  - 如果啟用了 HA，請檢查設定檔中是否指定了正確的介面。
  - 檢查通過鏈的流量流向。
  - 確保設定檔指示適當的安全鏈類型。
- 安全鏈設定；檢查：
  - 安全鏈中每個設備的 IP 位址、下一個躍點位址和預設閘道。
  - 防火牆和安全鏈之間任何裝置（路由器、交換器等）的設定，查找是否存在 IP 位址、下一個躍點和預設閘道設定錯誤。
  - 防火牆和鏈之間的路徑。
- 檢查防火牆流量日誌，以驗證是否按照預期為代理程式的流量設定了「已轉送」標幟。
- 有用的 CLI 命令包括：
  - `show rulebase network-packet-broker`
  - `show running network-packet-broker status`
  - `show running network-packet-broker statistics`
  - `show running application-cache all`
  - `show running application setting`—確認已啟用 App-ID 快取且該快取用於 App-ID，檢查快取閾值設定等。