paloalto TECHDOCS

SD-WAN 管理員指南

3.2

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

Last Revised

May 20, 2024

Table of Contents

SD-WAN 概要介紹

瞭解 SD-WAN 並規劃您的組態以確保成功部署。

關於 SD-WAN

軟體定義廣域網路 (SD-WAN) 是一種技術，可讓您使用多個網際網路和專用服務建立一個動態的智慧型 WAN，這有助於降低成本，並最大程度提升應用程式的品質和可用性。自 PAN-OS® 9.1 版起，Palo Alto Networks® 透過單一管理系統中的 SD-WAN overlay 提供了強大的安全性。無需在路由器、防火牆、WAN 路徑控制器和WAN 最佳化程式等元件上使用昂貴且耗時的 MPLS 來將 WAN 連線到網際網路，Palo Alto Networks 防火牆上的 SD-WAN 可為您提供價格優惠的網際網路服務，且所需設備更少。您無需購買和維護其他 WAN 元件。

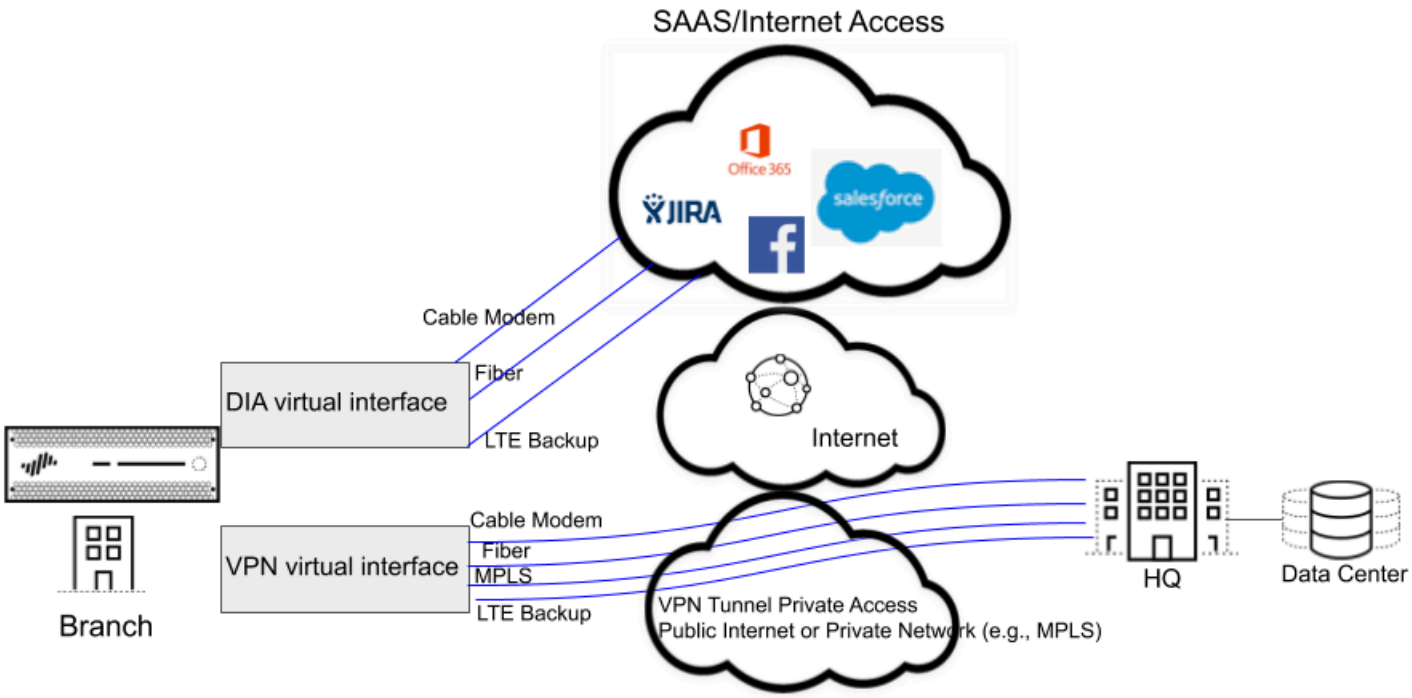
- 具有 SD-WAN 功能的 PAN-OS 安全性
- SD-WAN 連結和防火牆支援
- Prisma Access Hub 支援
- 集中管理

具有 **SD-WAN** 功能的 **PAN-OS** 安全性

SD-WAN 外掛程式與 PAN-OS 整合，因此您可從單個廠商處同時獲得 PAN-OS 防火牆的安全性功能和 SD-WAN 功能。SD-WAN overlay 支援基於應用程式和服務以及每個應用程式和服務可使用的連結情況的動態智慧型路徑選擇。每個連結的路徑健康情況監控包括延遲、抖動和封包遺失。細微的應用程式和服務控制允許您根據應用程式是否具任務關鍵性、是否延遲敏感或是否符合特定健康情況條件等因素對應用程式進行優先排序。動態路徑選擇可避免暫時低壓和節點故障問題，因為工作階段可在一秒內容錯移轉到效能更好的路徑。

SD-WAN overlay 可與 PAN-OS 的所有安全性功能（如 User-ID™ 和 App-ID™）配合運作，為每個分公司提供完整的安全控制。完整的 App-ID 功能套件（App-ID 解碼器、App-ID 快取，以及來源/目的地外部動態清單 [EDL] IP位址清單）可標識用於基於應用程式的 SD-WAN 流量控制的應用程式。您可以部署具有零信任流量分割的防火牆。您可以從 Panorama 網頁介面或 Panorama REST API 集中設定和管理 SD-WAN。

您可能擁有基於雲端的服務，且並不希望網際網路流量從分支流向中樞再流到雲端，而是希望網際網路流量使用直接連線的 ISP 直接從分支流到雲端。從分支到網際網路的此類存取即直接存取網際網路 (DIA)。您無需在網際網路流量上花費中樞頻寬和金錢。分支防火牆已經在執行安全性操作，因此您無需安裝中樞防火牆來對網際網路流量強制執行安全性。在分支上使用 DIA 進行 SaaS、網頁瀏覽或不應回傳到中樞的高頻寬應用程式。下圖對一個 DIA 虛擬介面進行了圖解，該介面由從分支到雲端的三個連結組成。該圖還對一個 VPN 通道虛擬介面進行了圖解，該介面包含將分支連線到總部中樞的四個連結。



SD-WAN 連結和防火牆支援

透過連結統合，您可將多個實體連結（不同的 ISP 用來與同一目的地進行通訊）分組到一個虛擬 SD-WAN 介面。根據應用程式和服務，防火牆從連結（路徑選擇）中進行選擇，以進行工作階段載入共用，並在暫時低壓或斷電的情況下提供容錯移轉保護。這樣，您可以為應用程式提供最佳效能。防火牆透過虛擬 SD-WAN 介面中的連結自動執行工作階段載入共用，以巧妙地使用可用頻寬。SD-WAN 介面必須全部具有相同類型的連線（DIA 或 VPN）。VPN 連結支援中樞和支點拓撲。

SD-WAN 支援以下類型的廣域網連線：ADSL/DSL、纜線數據機、乙太網路、光纖、LTE/3G/4G/5G、MPLS、微波/無線電、衛星、WiFi，以及以乙太網路形式在防火牆介面終止的任何連線。您可以針對如何使用連結制定適當的策略。您可以在昂貴的 MPLS 或 LTE 連線之前使用價格實惠的寬頻連線。或者，您可以使用特定的 VPN 通道來聯絡一個區域中的特定中樞。

如需支援 SD-WAN 軟體功能的防火牆型號的完整清單，請參閱 SD-WAN 的系統要求。

如果您是購買 Palo Alto Networks 新世代防火牆的新客戶，則將對 SD-WAN 使用預設虛擬路由器。如果您是現有客戶，您可以選擇讓 PAN-OS 覆寫任何現有虛擬路由器，或對 SD-WAN 使用新的虛擬路由器和新的區域，以將 SD-WAN 內容與之前存在的組態分離開來。

從 PAN-OS 11.0 開始，SD-WAN 外掛程式 3.1 支援使用行業標準設定方法來幫助完成管理員工作的進階路由引擎。儘管在概念上是等效的，但進階路由引擎使用邏輯路由器而不是虛擬路由器來執行個體化路由網域。當您啟用進階路由時，將建立邏輯路由器並使用進階路由引擎進行路由。當您停用進階路由時，將建立虛擬路由器並使用舊版引擎進行路由。

Prisma Access Hub 支援

藉由 SD-WAN 外掛程式 2.2 及更高版本，PAN-OS Secure SD-WAN 將為您提供 Prisma Access 中樞支援，讓您能夠完全控制應用程式的保護方式和位置。Prisma Access Hub 支援允許 PAN-OS 防火牆連線至 Prisma Access 計算節點 (CN)，以在 SD-WAN 中樞和支點拓撲中實現基於雲端的安全性。這種支援實現了從內部部署安全性到 Prisma Access 的無縫連結容錯移轉，並且能夠混合使用兩者以滿足您的安全性需求。

在具有 SD-WAN 防火牆和 Prisma Access 中樞的混合拓撲中，SD-WAN 中樞是 Prisma Access CN（IPSec 終端節點），而 SD-WAN 分支是 PAN-OS 防火牆。SD-WAN 自動建立 IKE 和 IPSec 通道，將分支連線至中樞。使用流量散佈設定檔，您可以建立 SD-WAN 政策來比對特定的網際網路應用程式，並將其重新導向至您選擇的 PAN-OS 防火牆或 Prisma Access 部署。藉由 Prisma Access 中樞支援，內部部署和雲端安全性平台將協同運作，提供一個完整的解決方案，該解決方案具有由 Panorama 管理的一致的安全性政策。

有關 Prisma Access Hub 支援所需的最低 PAN-OS 和 SD-WAN 外掛程式版本，請參閱 SD-WAN 的系統要求。

Prisma Access 中樞支援具有以下限制：

- 不支援匯入和匯出與 Prisma Access 相關的 SD-WAN 設定。
- 不支援 Prisma Access 設定的載入、部分載入、還原和部分還原。
- 不支援裝載至現有的 Prisma Access 遠端網路安全處理節點 (RN-SPN)。對於連線至 Prisma Access 的現有分支，您需要刪除該分支，然後重新裝載。
- Prisma Access 防火牆上沒有可用的 SD-WAN CLI 命令。
- 在 CN 上，源自 CN 的流量沒有路徑選擇。
- SD-WAN 報告和統計資料中未提供 Prisma Access 統計資料。

集中管理

Panorama™ 提供設定和管理 SD-WAN 的方法，這使得在多個地理位置分散的防火牆上設定多個選項比單獨設定防火牆更快、更容易。您可以從單個位置變更網路組態，而無需單獨設定每個防火牆。Auto VPN 組態允許 Panorama 為分支和中樞設定安全的 IKE/IPSec 連線。VPN 叢集定義每個地理區域中互相通訊的中樞和分支。防火牆使用 VPN 通道來進行分支和中樞之間的路徑健康情況監控，以提供對暫時低壓情況的亞秒級偵測。

Panorama 儀表板提供有關 SD-WAN 連結和效能的詳細資訊，以便您可調整路徑品質閾值和 SD-WAN 的其他方面，以改善其效能。集中統計資料和報告包含應用程式和連結效能統計資料、路徑健康情況度量和趨勢分析，以及應用程式和連結問題的焦點檢視。

請先瞭解 SD-WAN 使用案例，然後檢閱 SD-WAN 組態元素、流量分配方式，並計劃您的 SD-WAN 組態。為大大加快組態設定速度，最佳做法是匯出一個空的 SD-WAN 裝置 CSV，並輸入分公司 IP 位址、要使用的虛擬路由器、防火牆站點名稱、防火牆所屬的區域以及 BGP 路由資訊等各類資訊。Panorama 使用 CSV 檔案來設定 SD-WAN 中樞和分支，以便在中樞和分支之間自動佈建 VPN 通道。SD-WAN 支援透過 eBGP 進行動態路由，並使用 Panorama 的 SD-WAN 外掛程式進行設定，允許所有分支僅與中樞進行通訊，或允許分支與中樞和其他分支進行通訊。

如果 *Panorama* 正在管理多重 vsys 防火牆，則必須在 *vsys1* 上設定所有已啟用 *SD-WAN* 的介面和設定。

SD-WAN 不支援跨多重 *VSYS* 防火牆的多個虛擬系統的 *SD-WAN* 設定。

SD-WAN 介面必須在同一個虛擬路由器中設定；它們不能在虛擬路由器之間分割。

SD-WAN 的系統要求

檢閱適用於 SD-WAN 的 Panorama™ 外掛程式的最低軟體版本、外掛程式版本和資源要求。

從 *PAN-OS 11.0* 開始，您可以使用外掛程式 *3.1* 為 SD-WAN 設定進階路由。

下表提供彼此相容的外掛程式版本。建議您搭配使用 Prisma Access 雲端設定外掛程式版本與表格中所列出的對應相容 SD-WAN 外掛程式版本，因為相容版本包含新功能、錯誤修正程式或增強功能。

平台	PAN-OS	系統要求	Prisma Access 雲端設定外掛程式	SD-WAN 外掛程式
Panorama	11.2.3	• （Panorama 虛擬設備） 系統磁碟—224GB 系統磁碟 • **CPU**—16 個 CPU • 記憶體—— 64GB 記憶體 • 系統模式—Panorama 模式和僅管理模式 • （僅限管理模式下的 M-Series 設備）8TB RAID 日誌記錄磁碟配對已啟用 上述資訊最多適用於 *500* 個受管理的裝置。如需使用最多 *1,000* 個受管理的裝置的相關資訊，請參閱 Panorama 虛擬設備的系統需求	—	3.3.1
	11.2.0		5.0.0-h22	3.3.0
	11.1.5		—	3.2.2
	11.1.3		5.0.0-h31	3.2.1
	11.1.0		4.0.0 和 5.0.0	3.2.0
	11.0.4		5.0.0-h21	3.1.3
	11.0.3		4.0.0 和 5.0.0	3.1.2
	11.0.2		4.0.0	3.1.2
	11.0.2		4.0.0	3.1.1
	11.0.1 *11.0.1* 是建議的 *11.0.x* 版本。		3.2.1.h21	3.0.1-h6
	11.0.0		3.2.1-h3	3.1.0-h6

平台	PAN-OS	系統要求	Prisma Access 雲端設定外掛程式	SD-WAN 外掛程式
	10.2.8		4.0.0-h80、4.1.0-h49 和 5.0.0-h9	3.0.7
	10.2.7		4.0.0 和 5.0.0	3.0.6
	10.2.6		4.0.0	3.0.6
	10.2.5		4.0.0	3.0.5
	10.2.4 *10.2.4* 是建議的 *10.2.x* 版本。		3.2.1-h21	3.0.4
	10.2.3		3.2.1-h5	3.0.4
	10.2.1		此版本不支援；預計未來版本會支援。如果您要搭配使用 SD-WAN 與 Prisma Access 雲端設定外掛程式，則請不要升級至 PAN-OS 11.1。	3.0.1
	10.2.0			3.0.0
	10.1.11		4.0.0 和 5.0.0	2.2.6

平台	PAN-OS	系統要求	Prisma Access 雲端設定外掛程式	SD-WAN 外掛程式
	10.1.11		4.0.0	2.2.5
	10.1.10 *10.1.10* 是建議的 *10.1.x* 版本。		4.0.0	2.2.4
	10.1.9 *10.1.9* 是建議的 *10.1.x* 版本。		3.2.1-h5	2.2.4
	10.1.8		3.2.1-h5	2.2.2
	10.1.5-h1		2.1	2.2.1
	10.1.0		2.1	2.2
新世代防火牆	• **PAN-OS 11.1**—11.1.0 • **PAN-OS 11.0**—11.0.0 • **PAN-OS 10.2**—10.2.0 • **PAN-OS 10.1**—10.1.4 • **PAN-OS 10.0**—10.0.8	無		

平台	PAN-OS	系統要求	Prisma Access 雲端設定外掛程式	SD-WAN 外掛程式
Prisma Access 計算節點	10.0.7*	* Prisma Access 計算節點（IPSec 終端節點）必須執行 PAN-OS 10.0.7 或更高版的 10.0 版本。如有必要，請與您的銷售團隊合作要求升級，然後再嘗試將分公司裝載至 Prisma Access 中樞。		

以下防火牆型號支援 SD-WAN 軟體功能：

- PA-220 和 PA-220R
- PA-400 系列
- PA-820 和 PA-850
- PA-1400 系列
- PA-3200 系列
- PA-3400 Series
- PA-5200 系列
- PA-5400 系列
- PA-7000 系列
- VM-Series 防火牆

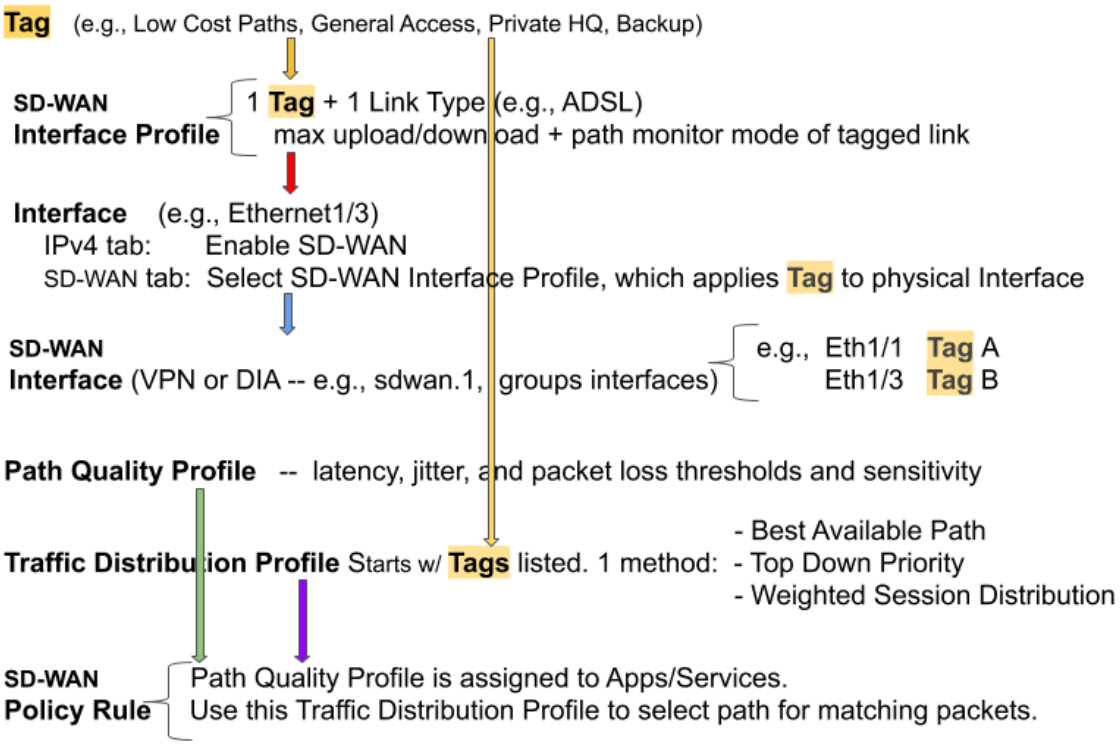
如需特定硬體可用性的詳細資訊，請參閱相容性矩陣。

SD-WAN 組態元素

SD-WAN 組態的元素共同運作，允許您：

- 將共用相同目的地的實體乙太網路介面分組到一個邏輯 SD-WAN 介面。
- 指定連結速度。
- 指定閾值，當指向 SD-WAN 的路徑惡化到該閾值（或暫時低壓或斷電）時，確保選取一條新的最佳路徑。
- 指定選取該新最佳路徑的方法。

此檢視表示各元素關係概覽。



SD-WAN 組態的目標是，透過指定某些應用程式或服務從分支到中樞或從分支到網際網路採用的 VPN 通道或直接網際網路存取 (DIA)，來控制您的流量採用哪些連結。您可以對路徑進行分組，以便在一條路徑惡化時，防火牆可以選取新的最佳路徑。

- 您選擇的 **Tag**（標籤）名稱可標識一個連結；透過將介面設定檔套用到介面的方式，將標籤套用到連結（介面），如紅色箭頭所示。一個連結只能有一個標籤。兩個黃色箭頭表示，在介面設定檔和流量散佈設定檔中引用了同一個標籤。標籤可讓您控制介面用於流量散佈的順序。標籤允許 Panorama 系統化地設定多個具有 SD-WAN 功能的防火牆介面。
- **SD-WAN Interface Profile**（**SD-WAN** 介面設定檔）指定您套用到實體介面的標籤，還指定該介面的連結類型（ADSL/DSL、纜線數據機、乙太網路、光纖、LTE/3G/4G/5G、MPLS、微波/無線電、衛星、WiFi 或其他）。您還可在介面設定檔中指定 ISP 連線的最大上載和下載速度 (Mbps)。您還可變更防火牆監控路徑的頻繁程度；預設情況下，防火牆會以適當的頻率監控連結類型。

- 具有 IPv4 或 IPv6 位址的 Layer3 乙太網路 **Interface**（介面）可支援 SD-WAN 功能。將 SD-WAN 介面設定檔套用到此介面（紅色箭頭）以指示介面的特征。藍色箭頭表示實體介面在一個虛擬 SD-WAN 介面中進行了引用和分組。
- 虛擬 **SD-WAN Interface**（**SD-WAN** 介面）是一個包含一個或多個介面的 VPN 通道或 DIA 群組，這些介面構成了一個有編號的虛擬 SD-WAN 介面，您可以將流量路由到該介面。屬於一個 SD-WAN 介面的路徑都會前往相同目的地廣域網，且都具有相同類型（DIA 或 VPN 通道）。（標籤 A 和標籤 B 表示虛擬介面的實體介面可以有不同的標籤。）
- **Path Quality Profile**（路徑品質設定檔）指定最大延遲、抖動和封包遺失閾值。超出一個閾值表示該路徑效能已惡化，防火牆需要選取一條指向該目標的新路徑。高、中等或低敏感度設定用於指示防火牆，對於該設定檔套用的應用程式，哪個路徑監控參數更為重要。綠色箭頭表示在一個或多個 SD-WAN 原則規則中引用一個路徑規則設定檔；這樣，您可以為套用到具有不同應用程式、來源、目的地、區域和使用者的封包的規則指定不同閾值。
- **Traffic Distribution Profile**（流量散佈設定檔）指定在當前偏好路徑超出路徑品質閾值時，防火牆如何確定新的最佳路徑。指定散佈方式使用的標籤來縮小新路徑選擇範圍。因此，黃色箭頭從標籤指向流量散佈設定檔。流量散佈設定檔指定規則的散佈方法。
- 前面介紹的這些元素共同組成了 **SD-WAN Policy Rules**（**SD-WAN** 原則規則）。紫色箭頭表示在一條規則中引用了一個路徑品質設定檔和一個流量散佈設定檔，與封包應用程式/服務、來源、目的地和使用者一起，明確指示防火牆何時以及如何為不屬於某個工作階段的封包執行基於應用程式的 SD-WAN 路徑選擇。（您還可以在 SD-WAN 原則規則中引用 **SaaS Quality Profile**（**SaaS** 品質設定檔）和 **Error Correction Profile**（錯誤更正設定檔）。）

現在，您已經瞭解了各元素之間的關係，請檢閱流量散佈方法，然後 規劃您的 SD-WAN 組態。

規劃您的 SD-WAN 組態

規劃已啟用 SD-WAN 的分支和中樞的完整拓撲，以便您可以使用 CSV 檔案建立 Panorama™ 範本，然後將組態推送到防火牆。

STEP 1 | 規劃分支和中樞位置、連結要求和IP 位址。您將從 Panorama 匯出一個空的 SD-WAN 裝置 CSV，並在其中填充分支和中樞資訊。

1. 確定每個防火牆的角色（分支還是中樞）。
2. 確定哪個分支將與哪個中樞進行通訊；每個互相通訊的分支和中樞防火牆功能群組就是一個 VPN 叢集。例如，您的 VPN 叢集可能按地理位置或功能進行組織。
3. 確定每個分支和中樞支援的 ISP 連結類型：ADSL/DSL、纜線數據機、乙太網路、光纖、TE/3G/4G/5G、MPLS、微波/無線電、衛星和 WiFi。
4. 確定連結類型支援的最大下載和上載頻寬 (Mbps)，以及您想要如何將這些速度控制套用至連結（如第 2 步中所述）。記錄 ISP 連結的最大下載和上載頻寬 (Mbps)。如果您需要設定 QoS 來控制應用程式頻寬，此資訊將用作參考輸出最大值。
5. 收集分支防火牆的公用 IP 位址，無論它們是靜態指派還是動態指派。防火牆必須有一個可在網際網路上路由的公用 IP 位址，以便它能夠起始和終止 IPSec 通道，並在應用程式與網際網路之間路由流量。

   ISP 的用戶端設備必須直接連線到防火牆上的乙太網路介面。

   如果您在分支防火牆和中樞之間有執行 *NAT* 的裝置，則該 *NAT* 裝置可以阻止防火牆啟動 *IKE* 對等和 *IPSec* 通道。如果通道故障，請與遠端 *NAT* 裝置的管理員合作以解決問題。
6. 收集分支和中樞防火牆的專用網路前置詞和序號。
7. 決定每個防火牆介面的連結類型。

   在各分支防火牆的相同乙太網路介面上配置相同連結類型以簡化組態。例如，*Ethernet1/1* 始終是纜線數據機。
8. 決定網站和 SD-WAN 裝置的命名慣例。

   不要使用簡單的主機名稱 *“hub”* 或 *“branch”*，因為 *Auto VPN* 組態會使用這些關鍵字來產生各種設定元素。
9. 如果在設定 SD-WAN 之前已經存在區域，請決定如何將這些區域對應到 SD-WAN 用於路徑選擇的預先定義區域。您需要將現有區域對應到名為 zone-internal、zone-to-hub、zone-branch 和 zone-internet 的預先定義區域。

   您將輸入至 *CSV* 的資訊（以便您可以一次新增多個 *SD-WAN* 裝置）包括：序號、裝置類型（分支或中樞）、要對應到預先定義區域的區域名稱（現有客戶）、回送位址、要重新散佈的前置詞、*AS* 編號、路由器 *ID* 和虛擬路由器名稱。

STEP 2 | 規劃專用連結的連結組合和 VPN 安全性。

連結組合可讓您將多個實體連結組合到一個虛擬 SD-WAN 介面中，以進行路徑選擇和容錯移轉保護。擁有一個包含多個實體連結的組合，您可以在實體連結惡化時最大程度保障應用程式品質。您可透過向多個連結套用相同連結標籤來建立組合（透過 SD-WAN 介面設定檔）。連結標籤標識具有相似存取類型和相似 SD-WAN 原則處理類型的連結組合。例如，您可以建立一個名為 **`low cost broadband`**（低成本寬頻）的連結標籤，並包含纜線數據機和光纖寬頻服務。

STEP 3 | 識別將使用 SD-WAN 和 QoS 最佳化的應用程式。

1. 識別您將為其提供 SD-WAN 控制和原則的重要和延遲敏感的業務應用程式。這些應用程式需要良好的使用者體驗，且可能在不良的連結條件下無法運作。

   從最重要和延遲敏感度最高的應用程式開始；您可以在 *SD-WAN* 順暢運作後再新增應用程式。

2. 識別需要 QoS 原則的應用程式，以便您可以為頻寬設定優先順序。這些應當是您識別為重要或延遲敏感的應用程式。

   從最重要和延遲敏感度最高的應用程式開始；您可以在 *SD-WAN* 順暢運作後再新增應用程式。

STEP 4 | 確定在原始連結效能降低或故障時容錯移轉到另一個連結的時間和方式。

1. 決定連結的路徑監控模式（最佳做法是保留連結類型的預設設定）：

   - **Aggressive**（積極）—防火牆以固定的頻率將探查封包傳送到 SD-WAN 連結的另一端（預設情況下為每秒五次探查）。積極模式適用於監控路徑品質至關重要的連結；在這種情況下，您需要快速偵測暫時低壓和斷電情況並迅速進行容錯移轉。積極模式可提供亞秒級的偵測和容錯移轉。
   - **Relaxed**（寬鬆）—防火牆在（以您設定的探查頻率）傳送探查封包期間會遵守 7 秒的可設定閒置時間，使得路徑監控的頻率低於積極模式。寬鬆模式適用於頻寬極低的連結、運行成本昂貴的連結（例如衛星或 LTE），或相比快速偵測節省成本和頻寬更為重要的連結。

2. 為防火牆為新工作階段選取第一個連結的情況設定優先順序，以及為連結是用於替換正在容錯移轉的連結的候選連結，且存在多個候選連結的情況設定優先順序。

   例如，如果您希望昂貴的備用 LTE 連結成為最後使用的連結（僅當價格實惠的寬頻連結供不應求或完全斷開時），則請使用「自上而下優先順序」的流量散佈方法，並將 LTE 連結上的標籤放在流量散佈設定檔的標籤清單的最後位置。

3. 對於應用程式和服務，請確定路徑健康情況閾值，如果達到該閾值，則認為路徑品質已下降到足以讓防火牆選取新路徑（容錯移轉）的程度。品質特征為延遲（範圍為 10 到 2,000 毫秒）、抖動（範圍為 10 到 1,000 毫秒）和封包遺失百分比。

   這些閾值構成了路徑品質設定檔，您將在 SD-WAN 原則規則中引用該設定檔。當超出任何單個閾值（封包遺失、抖動或延遲）（且剩餘規則條件均滿足）時，防火牆會為匹配的流量選擇一條新的偏好路徑。例如，您可以建立路徑品質設定檔 AAA，延遲/抖動/封包遺失閾值分別為 1000/800/10，當 FTP 封包從來源區域 XYZ 進入時在規則 1 中使用，同時建立路徑品質設定檔 BBB（閾值為 50/200/5），當 FTP 封包從來源 IP 位址

10.1.2.3 進入時在規則 2 中使用。最佳做法是從較高的閾值開始，並測試應用程式容忍的程度。如果設定的值過低，應用程式可能會過於頻繁地切換路徑。

考慮您正在使用的應用程式和服務是否對延遲、抖動或封包遺失極其敏感。例如，視訊應用程式可能有可以緩解延遲和抖動的良好緩衝處理，但會對封包遺失比較敏感，因為這會影響使用者體驗。您可以在設定檔中將路徑品質參數的敏感度設定為高、中等或低。如果延遲、抖動和封包遺失的敏感度設定相同，防火牆會按封包遺失、延遲、抖動的順序檢查參數。

4. 決定是否有連結來為應用程式或服務載入共用新工作階段。

STEP 5 | 規劃 BGP 組態，Panorama 會將其推送到分支和中樞以在它們之間動態路由流量。

1. 規劃 BGP 路由資訊，包括一個四位元組自治號碼 (ASN)。每個防火牆網站都位於單獨的 AS 中，因此必須具有唯一的 ASN。每個防火牆還必須具有唯一的路由器 ID。
2. 在 BGP 已經投入使用的環境中實作帶有 BGP 路由的 SD-WAN 之前，請確保 SD-WAN 外掛程式產生的 BGP 設定不會與您現有的 BGP 設定衝突。例如，您必須使用現有的 BGP AS 號碼和路由器 ID 值來表示相應的 SD-WAN 裝置值。
3. 如果您不想使用 BGP 動態路由，請規劃使用 Panorama 的網路組態功能來推出其他路由組態。您可以在分支和中樞之間進行靜態路由。僅需刪除 Panorama 外掛程式中的所有 BGP 資訊，並使用標準虛擬路由器靜態路由來執行靜態路由即可。

STEP 6 | 從虛擬 SD-WAN 介面、SD-WAN 原則規則、日誌大小、IPSec 通道（包括 Proxy ID）、IKE 對等、BGP 和靜態路由表、BGP 路由對等方面考慮防火牆型號的容量，以及防火牆模式（App-ID™、威脅、IPSec、加密）的效能。確保您打算使用的分支和中樞防火牆型號支援您需要的功能。

設定 SD-WAN

在 規劃您的 SD-WAN 組態 之後，安裝 SD-WAN 外掛程式並設定 Panorama™ 管理伺服器以集中管理中樞和分支防火牆的 SD-WAN 組態。利用 Panorama，您可以減少管理 SD-WAN 部署的管理要求和營運負荷，能夠更輕鬆地監控連結監控情況並在出現問題時進行疑難排解。

如果 *Panorama* 正在管理多重 vsys 防火牆，則必須在 *vsys1* 上設定所有已啟用 *SD-WAN* 的介面和設定。

SD-WAN 不支援跨多重 *VSYS* 防火牆的多個虛擬系統的 *SD-WAN* 設定。

- 安裝 SD-WAN 外掛程式
- 為 SD-WAN 設定 Panorama 和防火牆
- 建立連結標籤
- 設定 SD-WAN 介面設定檔
- 為 SD-WAN 設定實體乙太網路介面
- （選用）為 SD-WAN 設定彙總乙太網路介面和子介面
- （選用）為 SD-WAN 設定第三層子介面
- 設定虛擬 SD-WAN 介面
- 建立指向 SD-WAN 介面的預設路由
- 設定 SD-WAN 連結管理設定檔
- 設定 SD-WAN 原則規則
- 允許直接網際網路存取流量容錯移轉到 MPLS 連結
- 設定 DIA AnyPath
- 散佈不匹配的工作階段
- 新增 SD-WAN 裝置到 Panorama
- （選用）在 SD-WAN 中樞上設定多個虛擬路由器
- （選用）在 SD-WAN 分支上設定多個虛擬路由器
- （選用）為 SD-WAN 設定 HA 裝置
- 建立 VPN 叢集
- 建立具有 DDNS 服務的完整網狀 VPN 叢集
- （選用）為 SD-WAN 建立靜態路由
- （選用）為 SD-WAN 設定進階路由

安裝 SD-WAN 外掛程式

具有 SD-WAN 外掛程式的 Panorama™ 管理伺服器必須設定並管理 SD-WAN 部署。如果您的 Panorama 連線到網際網路，請直接從 Panorama 下載 SD-WAN 外掛程式並將其安裝在 Panorama 管理伺服器上。如果您的 Panorama 沒有連線到網際網路，請從 Palo Alto Networks® 客戶支援入口網站下載 SD-WAN 外掛程式，並將其安裝在 Panorama 管理伺服器上。

- 當 Panorama 連線至網際網路時安裝 SD-WAN 外掛程式
- 當 Panorama 未連線至網際網路時安裝 SD-WAN 外掛程式

當 Panorama 連線至網際網路時安裝 SD-WAN 外掛程式

安裝了 SD-WAN 外掛程式的 Panorama™ 管理伺服器必須設定並管理 SD-WAN 部署。當 Panorama 連線到網際網路時，您可直接從 Panorama 網頁介面下載並安裝 SD-WAN 外掛程式。僅需在管理 SD-WAN 防火牆的 Panorama 上安裝外掛程式，無需在單個中樞和分支防火牆上安裝。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Plugins**（外掛程式），搜尋 **sd_wan** 外掛程式，然後 **Check Now**（立即檢查）最新版本的外掛程式。

STEP 3 | **Download**（下載）並 **Install**（安裝）SD-WAN 外掛程式。

STEP 4 | 成功安裝 SD-WAN 外掛程式後，選取 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**）。

必須先執行此步驟才可將任何組態變更提交到 Panorama。

STEP 5 | （僅限管理模式）啟用存儲 SD-WAN 監控資料所需的日誌記錄磁碟。

- **M-Series** 設備—依預設，所有 M-Series 設備的 RAID 1 中都有兩對 8TB 日誌記錄磁碟。在僅管理模式下管理利用 Panorama 中的 SD-WAN 的防火牆時，您必須啟用第一對日誌記錄磁碟配對來儲存 SD-WAN 監控資料。

  1. 登入 Panorama CLI。
  2. 啟用 M-Series 設備依預設包含的第一對日誌記錄磁碟配對。

     ```
     > request system raid add A1
     ```

  3. 驗證日誌記錄 `Logging Disk Pair A` 是否為 `Available`：

     ```
     > show system raid detail
     ```

     完成 RAID 設定時會顯示下列回應：

     ```
     Disk Pair A       Available Status         clean Disk id A1
          Present model :ST91000640NS size :953869 MB status :
      active sync
     ```

  4. 使日誌記錄磁盤配對可用於日誌記錄。
     1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
     2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個陣列。
     3. 按一下 **OK**（確定）儲存您的變更。
     4. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
     5. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置），然後選取 Collector Group（收集器群組）並 **Push**（推送）您的變更。

- **Panorama** 虛擬設備—如果您在僅管理模式下部署了 Panorama 虛擬設備，則必須將系統磁碟增加到 224GB 以儲存 SD-WAN 監控資料。

STEP 6 | 繼續 為 SD-WAN 設定 Panorama 和防火牆 以開始設定您的 SD-WAN 部署。

當 Panorama 未連線至網際網路時安裝 SD-WAN 外掛程式

具有 SD-WAN 外掛程式的 Panorama™ 管理伺服器必須設定並管理 SD-WAN 部署。如果您的 Panorama 沒有連線到網際網路，您必須從 Palo Alto Networks 客戶支援入口網站下載 SD-WAN 外掛程式，並將外掛程式上載到 Panorama。僅需在管理 SD-WAN 防火牆的 Panorama 上安裝外掛程式，無需在單個中樞和分支防火牆上安裝。

STEP 1 | 登入 Palo Alto Networks 客戶支援入口網站。

STEP 2 | 選取 **Updates**（更新） > **Software Updates**（軟體更新），在「篩選依據」下拉清單中選取 **Panorama Integration Plug In**（**Panorama** 整合外掛程式）。

STEP 3 | 找到並下載 **SD-WAN Plug-in**（**SD-WAN** 外掛程式）。

STEP 4 | 登入 Panorama 網頁介面。

STEP 5 | 選取 **Panorama** > **Plugins**（外掛程式），然後 **Upload**（上載） SD-WAN 外掛程式。

STEP 6 | **Browse**（瀏覽）並找到從客戶支援入口網站下載的 SD-WAN 外掛程式，然後按一下 **OK**（確定）。

STEP 7 | **Install**（安裝）SD-WAN 外掛程式。

STEP 8 | 成功安裝 SD-WAN 外掛程式後，選取 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**）。

必須先執行此步驟才可將任何組態變更提交到 Panorama。

STEP 9 | （僅限管理模式）啟用存儲 SD-WAN 監控資料所需的日誌記錄磁碟。

- **M-Series** 設備—依預設，所有 M-Series 設備的 RAID 1 中都有兩對 8TB 日誌記錄磁碟。在僅管理模式下管理利用 Panorama 中的 SD-WAN 的防火牆時，您必須啟用第一對日誌記錄磁碟配對來儲存 SD-WAN 監控資料。

  1. 登入 Panorama CLI。
  2. 啟用 M-Series 設備依預設包含的第一對日誌記錄磁碟配對。

     ```
     > request system raid add A1
     ```

  3. 驗證日誌記錄 `Logging Disk Pair A` 是否為 `Available`：

     ```
     > show system raid detail
     ```

     完成 RAID 設定時會顯示下列回應：

     ```
     Disk Pair A       Available Status         clean Disk id A1
          Present model :ST91000640NS size :953869 MB status :
      active sync
     ```

  4. 使日誌記錄磁盤配對可用於日誌記錄。
     1. 選取 **Panorama** > **Managed Collectors**（受管理的收集器），再編輯日誌收集器。
     2. 選取 **Disks**（磁碟），然後 **Add**（新增）每一個陣列。
     3. 按一下 **OK**（確定）儲存您的變更。
     4. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。
     5. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置），然後選取 Collector Group（收集器群組）並 **Push**（推送）您的變更。

- **Panorama** 虛擬設備—如果您在僅管理模式下部署了 Panorama 虛擬設備，則必須將系統磁碟增加到 224GB 以儲存 SD-WAN 監控資料。

STEP 10 | 繼續 為 SD-WAN 設定 Panorama 和防火牆 以開始設定您的 SD-WAN 部署。

為 SD-WAN 設定 Panorama 和防火牆

在能夠開始設定您的 SD-WAN 部署前，您必須將中樞和分支防火牆新增為受管理的裝置，並建立必要的範本和裝置群組設定以成功將 SD-WAN 組態推送到 SD-WAN 防火牆。

- 將您的 SD-WAN 防火牆新增為受管理裝置
- 建立 SD-WAN 網路範本
- 在 Panorama 中建立預先定義區域
- 建立 SD-WAN 裝置群組

將您的 SD-WAN 防火牆新增為受管理裝置

在開始設定 SD-WAN 部署之前，您必須先 安裝 SD-WAN 外掛程式，並將中樞和分支防火牆新增為 Panorama™ 管理伺服器的受管理的裝置。在將 SD-WAN 防火牆新增為 Panorama™ 管理伺服器上的受管理裝置的過程中，您必須啟動 SD-WAN 授權以便為防火牆啟用 SD-WAN 功能。

在將 SD-WAN 防火牆新增為受管理裝置的過程中，您必須設定受管理裝置以將日誌轉送給 Panorama。Panorama 收集來自各個來源的資訊，如組態日誌、流量日誌和連結特征度量，以產生有關 SD-WAN 應用程式和連結健康情況資訊的可見度。

不要讓您的 *Panorama* 管理伺服器連線僅依賴 *SD-WAN* 覆蓋。為了維護可靠的連線（讓 *Panorama* 一律可連線至 *PAN-OS* 防火牆），建議您建立從 *PAN-OS* 防火牆連線至 *Panorama* 的專用 *IPSec* 通道（即位於 *Panorama* 所在中樞/分支之間的 *SD-WAN* 覆蓋外部）。使用此方式，如果 *SD-WAN* 覆蓋受到任何影響，則您可以確保一律可連線 *Panorama* 管理伺服器。

STEP 1 | 啟動防火牆 Web 介面。

STEP 2 | 啟動您的 SD-WAN 授權以在防火牆上啟用 SD-WAN 功能。

您打算在 SD-WAN 部署上使用的每個防火牆都需要一個唯一的驗證碼來啟動授權。例如，如果您有 100 個防火牆，您必須購買 100 個 SD-WAN 授權，並在每個防火牆上使用其中一個唯一的驗證碼啟動每個 SD-WAN 授權。

對於 *VM-Series* 防火牆，您必須針對特定 *VM-Series* 防火牆套用 *SD-WAN* 驗證碼。如果您停用 VM-Series 防火牆，該 *SD-WAN* 驗證碼可以在相同型號的其他 *VM-Series* 防火牆上啟動。

確保您的 *SD-WAN* 授權仍然有效，以繼續利用 *SD-WAN*。如果 *SD-WAN* 授權到期，則會發生以下情況：

- 當您***Commit***（認可）任何組態變更時會顯示一個警告，但不會出現認可失敗。
- 您的 *SD-WAN* 組態不再起作用，但不會被刪除。
- 防火牆不再監控和收集連結監控情況指標，且停止傳送監控探查。
- 防火牆不再將應用程式和連結健康情況指標傳送到 *Panorama*。
- *SD-WAN* 路徑選擇邏輯停用。
- 新的工作階段會在虛擬 SD-WAN 介面上循環配置資源。
- 現有工作階段保留在授權到期時它們所在的特定連結上。
- 如果出現網際網路中斷，則流量按照標準路由和 ECMP（如果已設定）進行。

STEP 3 | 將 Panorama IP 位址新增至防火牆。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），再編輯 [Panorama 設定]。
2. 在第一個欄位中輸入 Panorama IP 位址。

   Panorama FQDN 對 *SD-WAN* 不受支援。

3. （選用）如果您已在 Panorama 中設定高可用性 (HA) 對等，請在第二個欄位中輸入次要 Panorama 的 IP 位址。
4. 確認您啟用將裝置監控資料推送到 **Panorama**。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

STEP 4 | 設定日誌轉送至 Panorama。

必須從您的 SD-WAN 防火牆將日誌轉送到 Panorama 才可顯示 監控與報告 資料。

依預設，如果為應用程式流量啟用了解密，則將自動啟用 *HTTP/2* 檢查。使用 *HTTP/2* 連線的上層工作階段不會產生任何流量日誌，因為它們不承載任何應用程式流量。但是，由 *HTTP/2* 上層工作階段中的串流產生的子工作階段仍會產生流量日誌。有關檢視 *HTTP/2* 連線日誌的更多資訊，請參閱 Palo Alto Networks 知識庫。

STEP 5 | 向 Panorama 新增一個或多個防火牆。

如需瞭解有關將防火牆新增到 Panorama 的更多詳細資料，請參閱將防火牆新增為受管理的裝置。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並 **Add**（新增）防火牆。
3. 顯示防火牆的序號。
4. 如果在已建立所需裝置群組和範本的情況下新增防火牆，請啟用（選中）**Associate Devices**（關聯裝置）以將新防火牆指派到適當的裝置群組和範本堆疊。
5. 要使用 CSV 新增多個防火牆，請按一下 **Import**（匯入）和 **Download Sample CSV**（下載範例 **CSV**）以填充防火牆資訊，然後按一下 **Browse**（瀏覽）以匯入防火牆。
6. 按一下 **OK**（確定）。

STEP 6 | 選取**Commit**（認可），提交並推送您的組態。

STEP 7 | 在您打算在 SD-WAN 部署中使用的每個防火牆上重複第 2 到第 5 步。

建立 SD-WAN 網路範本

建立一個範本，其中包含 SD-WAN 中樞和分支的所有網路組態物件。您必須為中樞防火牆建立一個單獨的範本和範本堆疊，並為分支防火牆建立一個單獨的範本和範本堆疊。最好的做法是，限制用於管理 SD-WAN 裝置組態的範本和範本堆疊的數量。限制所有中樞和分支中使用的範本和範本堆疊的數量可大大減少管理多個 SD-WAN 中樞和分支組態的營運負荷。使用範本或範本堆疊變數幫助減少所使用範本的數量。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 建立 SD-WAN 中樞網路範本。

1. 選取 **Panorama** > **Templates**（範本）並 **Add**（新增）一個新範本。
2. 輸入範本的描述性 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. 按一下 **OK**（確定）儲存組態變更。

STEP 3 | 建立中樞範本堆疊。

1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add Stack**（新增堆疊）以新增一個新的範本堆疊。
2. 輸入範本堆疊的描述性 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. **Add**（新增）在第 2 步中建立的 SD-WAN 網路範本。
5. 在 **Devices**（裝置）部分中，選取所有 SD-WAN 中樞防火牆的核取方塊。
6. 按一下 **OK**（確定）儲存組態變更。

STEP 4 | 建立 SD-WAN 分支網路範本。

1. **Add**（新增）一個新範本。
2. 輸入範本的描述性 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. 按一下 **OK**（確定）儲存組態變更。

STEP 5 | 建立分支範本堆疊。

1. 按一下 **Add Stack**（新增堆疊）以新增新的範本堆疊。
2. 輸入範本堆疊的描述性 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. **Add**（新增）在第 4 步中建立的 SD-WAN 網路範本。
5. 在 **Devices**（裝置）部分中，選取所有 SD-WAN 分支防火牆的核取方塊。
6. 按一下 **OK**（確定）儲存組態變更。

STEP 6 | **Commit**（提交）組態變更。

在 Panorama 中建立預先定義區域

SD-WAN 原則規則使用預先定義的區域來用於內部路徑選擇和流量轉送目的。有兩個使用案例；您的使用案例取決於您是在具有現有安全性原則規則的當前 PAN-OS® 防火牆上啟用 SD-WAN，還是開啟一個沒有安全性原則規則的全新 PAN-OS 部署。如果您的當前防火牆具有安全性原則規則，您需要將現有區域對應到 SD-WAN 原則使用的預先定義區域。

SD-WAN 引擎利用預先定義的區域來轉送流量。此外，在 Panorama™ 範本中建立預先定義的區域可提供受管理防火牆和 Panorama 之間的持續可見性：

- **Zone Internet**（區域網際網路）—對於往返不受信任的網際網路的流量。
- **Zone to Hub**（區域到中樞）—對於從分支防火牆到中樞防火牆的流量以及在中樞防火牆之間流動的流量。
- **Zone to Branch**（區域到分支）—對於從中樞防火牆到分支防火牆的流量以及分支防火牆之間的流量。
- **Zone Internal**（區域內部）—對於特定位置的內部流量。
- **Zone to PA Hub**（區域到 **PA** 中樞）—對於到達 Prisma Access 中樞的內部流量。

如果您沒有建立預先定義的區域，*SD-WAN* 外掛程式將在您的分支和中樞防火牆上自動建立預先定義的區域，但您在 *Panorama* 中將無法看到它們。

預先定義的區域有兩個主要使用案例：

- 現有區域—您已經擁有建立用於 User-ID™ 或各種原則（安全性原則規則、QoS 原則規則、區域保護和封包緩衝保護）的現有區域。您必須將現有區域對應到 SD-WAN 使用的預先定義區域，以便防火牆可以正確轉送流量。您應當繼續在所有原則中繼續使用現有區域，因為新的預先定義區域僅用於 SD-WAN 轉送。您將在透過建立 CSV 檔案進行 新增 SD-WAN 裝置到 Panorama 時對應區域。（如果您不是使用 CSV 檔案，您將在設定 **Panorama** > **SD-WAN** > **Devices**（裝置）時對應區域，並將現有區域新增到 **Zone Internet**（區域網際網路）、**Zone to Hub**（區域到中樞）、**Zone to Branch**（區域到分支）和 **Zone Internal**（區域內部）。）

  對應的結果是分支或中樞防火牆可以進行轉送查閱來確定輸出 SD-WAN 介面，進而確定輸出區域。如果您沒有將現有區域對應到預先定義區域，允許的工作階段將不會使用 SD-WAN。必須進行對應，因為現有客戶已經擁有不同的區域名稱，且防火牆必須將所有這些區域名稱縮小到預先定義的區域。您不一定要將區域對應到所有預先定義的區域，但是您至少應當將現有區域對應到 **Zone to Hub**（區域到中樞）和 **Zone to Branch**（區域到分支）區域。
- 沒有現有區域—您會擁有 Palo Alto Networks® 防火牆和 SD-WAN 的全新部署。在這種情況下，您沒有需要對應的區域；我們建議您使用 PAN-OS 原則和 User-ID 中預先定義的區域來簡化部署。

開始設定 SD-WAN 部署之前，針對這兩種使用案例，您將會在 Panorama 中建立必要的預先定義區域，即 **zone-internet**、**zone-internal**、**zone-to-hub**、**zone-to-branch** 和 **zone-to-pa-hub**。當您裝載分支和中樞防火牆時，您將 新增 SD-WAN 裝置到 Panorama。對於現有客戶，SD-WAN 外掛程式將在執行 SD-WAN 原則規則、QoS 原則規則、區域保護、User-ID 和封包緩衝保護時，將現有區域內部對應到預先定義的區域，並將使用預先定義的區域來獲取 Panorama 中的區域日誌記錄和可見性。對於新客戶，您需要使用預先定義區域適當進行設定。

仍然需要預先定義區域，以便在將組態從 Panorama 推送到受管理的 SD-WAN 裝置時，自動在 SD-WAN 中樞和分支之間設定 VPN 通道。

區域名稱區分大小寫，且必須與此程序中提供的名稱相匹配。如果區域名稱與此程序中描述的名稱不匹配，您將在防火牆上提交失敗。

在此範例中，我們會建立一個名為 **zone-internet** 的區域。

STEP 1 | 登入 Panorama 網頁介面。

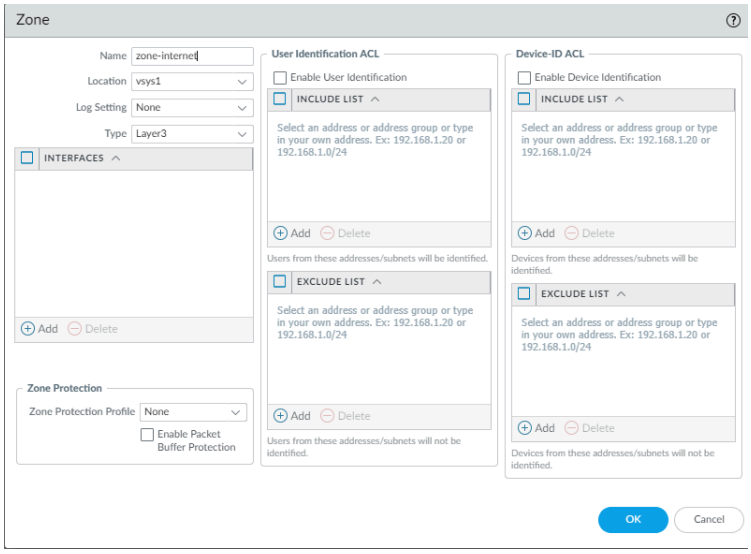
STEP 2 | 選取 **Network**（網路） > **Zones**（區域），然後在 **Template**（範本）內容下拉清單中，選取您之前建立的網路範本。

STEP 3 | **Add**（新增）一個新區域。

STEP 4 | 輸入 **zone-internet** 作為區域的 **Name**（名稱）。

STEP 5 | 對於區域 **Type**（類型），選取 **Layer3**。

STEP 6 | 按一下 **OK**（確定）。



STEP 7 | 重複之前的步驟以建立剩下的區域。總而言之，您必須建立以下區域：

- **zone-to-branch**
- **zone-to-hub**
- **zone-internal**
- **zone-internet**
- **zone-to-pa-hub**

STEP 8 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 9 | **Commit**（提交）您的變更。

建立 SD-WAN 裝置群組

為中樞和分支各建立一個裝置群組，其中包含用於 SD-WAN 分支和中樞的所有原則規則和組態物件。在為中樞和分支建立裝置群組後，您必須在每個裝置群組中建立一個安全性原則規則，以允許在中樞和分支區域之間進行通訊。建立這些安全性原則規則可確保在建立 VPN 叢集後 SD-WAN 外掛程式建立 VPN 通道時，允許 SD-WAN 裝置區域之間進行通訊。

在所有中樞防火牆中設定完全相同的組態，並在所有分支防火牆中設定完全相同的組態。這大大減少了管理多個 *SD-WAN* 中樞和分支的組態的營運負荷，並讓您可以更快地進行疑難排解、隔離和更新組態問題。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 中建立預先定義區域。

STEP 3 | 建立 SD-WAN 中樞裝置群組。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後 **Add**（新增）裝置群組。
2. 輸入 **SD-WAN_Hub** 作為裝置群組的 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. 在 **Devices**（裝置）部分中，選取核取方塊以將 SD-WAN 中樞指派到群組。
5. 對於 **Parent Device Group**（父系裝置群組），選取 **Shared**（共用）。
6. 按一下 **OK**（確定）。

STEP 4 | 建立 SD-WAN 分支裝置群組。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後 **Add**（新增）裝置群組。
2. 輸入 **SD-WAN_Branch** 作為裝置群組的 **Name**（名稱）。
3. （選用）輸入範本的 **Description**（說明）。
4. 在 **Devices**（裝置）部分中，選取核取方塊以將 SD-WAN 分支指派到群組。
5. 對於 **Parent Device Group**（父系裝置群組），選取 **Shared**（共用）。
6. 按一下 **OK**（確定）。

STEP 5 | 建立安全性原則規則以控制流量從分公司流動到中樞內部區域，以及從中樞內部區域流動到分公司。

1. 選取 **Policies**（原則） > **Security**（安全），然後在 **Device Group**（裝置群組）內容下拉清單中選取 **SD-WAN_Hub** 裝置群組。
2. **Add**（新增）新的原則規則。
3. 輸入原則規則的 **Name**（名稱），例如 **SD-WAN access--hub DG**。
4. 選取 **Source**（來源） > **Source Zone**（來源區域），然後 **Add**（新增）**zone-internal**（區域-內部） 和 **zone-to-branch**（區域到分支）。
5. 選取 **Destination**（目的地） > **Destination Zone**（目的地區域），然後 **Add**（新增）**zone-internal**（區域-內部）和 **zone-to-branch**（區域到分支）。
6. 選取 **Application**（應用程式），然後 **Add**（新增）要允許的應用程式。

   如果您使用 *BGP* 路由，則必須允許 *BGP*。

7. 選取 **Actions**（動作），然後選取 **Allow**（允許）以允許您選取的應用程式。
8. 選取 **Target**（目標），然後指定 Panorama™ 應向其推送此規則的目標裝置。

STEP 6 | 建立安全性原則規則以控制從分公司的內部區域到中樞和從中樞到分公司內部區域的流量。

1. 選取 **Policies**（原則） > **Security**（安全），然後在 **Device Group**（裝置群組）內容下拉清單中選取 **SD-WAN_Branch** 裝置群組。
2. **Add**（新增）新的原則規則。
3. 輸入原則規則的 **Name**（名稱），例如 **`SD-WAN access--branch DG`**。
4. 選取 **Source**（來源） > **Source Zone**（來源區域），然後 **Add**（新增）**zone-internal**（區域-內部） 和 **zone-to-hub**（區域到中樞）。
5. 選取 **Destination**（目的地） > **Destination Zone**（目的地區域），然後 **Add**（新增）**zone-internal**（區域-內部）和 **zone-to-hub**（區域到中樞）。
6. 選取 **Application**（應用程式），然後 **Add**（新增）要允許的應用程式。

   如果您使用 *BGP* 路由，則必須允許 *BGP*。

7. 選取 **Actions**（動作），然後選取 **Allow**（允許）以允許您選取的應用程式。
8. 選取 **Target**（目標），然後指定 Panorama 應向其推送此規則的目標裝置。

STEP 7 | 認可並推送您的組態。

1. **Commit**（認可），**Commit and Push**（認可並推送）組態變更。
2. 在「推送範圍」部分中，按一下 **Edit Selections**（編輯選擇）。
3. 啟用（選中）**Include Device and Network Templates**（包含裝置與網路範本），然後按一下 **OK**（確定）。
4. **Commit and Push**（認可並推送）組態變更。

   當您認可和推送裝置群組與範本組態時，會自動執行兩次認可操作。檢視 ***Tasks***（工作）以確認第二次認可成功。這兩次認可操作中，第一次操作始終會失敗。

建立連結標籤

建立一個連結標籤，以標識您希望應用程式和服務在 SD-WAN 流量散佈和容錯移轉保護期間以特定順序使用的一個或多個實體連結。將多個實體連結分組在一起，可在實體連結健康情況惡化時最大化應用程式和服務品質。

當計劃如何對連結分組時，請考慮連結的用途或目的並進行相應的分組。例如，如果您正在設定計劃用於低成本或非業務關鍵流量的連結，請建立一個連結標籤，並將這些介面分組在一起，以確保預期流量主要在這些連結上流動，而不是在可能影響業務關鍵應用程式或服務的昂貴連結上流動。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Objects**（物件） > **Tags**（標籤），然後從 **Device Group**（裝置群組）內容下拉清單中選取適當的裝置群組。

STEP 3 | **Add**（新增）一個新標籤。

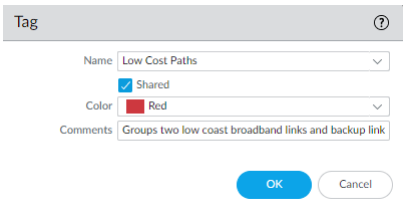
STEP 4 | 輸入標籤的描述性 **Name**（名稱）。例如，低成本路徑、昂貴路徑、一般存取、專用 HQ 或備份。

STEP 5 | 啟用（核取）**Shared**（共用）以使連結標籤對 Panorama™ 管理伺服器上的所有裝置群組和單個 vsys 中樞或分支上的預設 vsys，或您推送到的任何多重 vsys 中樞或分支上的 vsys1 可用。

在設定共用連結標籤前，Panorama 能夠在防火牆組態驗證中引用連結標籤，並將組態成功認可並推送到分支和中樞。如果 Panorama 無法引用連結標籤，則會認可失敗。

STEP 6 | （選用）選取標籤的 **Color**（色彩）。

STEP 7 | 輸入有關標籤的有用 **Comments**（註解）。例如，將兩個低成本寬頻連結和一個備份連結分組在一起，以用於對網際網路的一般存取。



STEP 8 | 按一下 **OK**（確定）儲存組態變更。

STEP 9 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 10 | 設定 SD-WAN 介面設定檔。

設定 SD-WAN 介面設定檔

建立一個 SD-WAN 介面設定檔以定義 ISP 連線的特征，並指定連結的速度以及防火牆監控連結的頻率，然後為連結指定一個連結標籤。當您在多個連結上指定相同連結標籤時，便可將這些實體連結分組（組合）到一個連結組合或粗管。必須先設定一個 SD-WAN 介面設定檔，將其指定給一個已啟用 SD-WAN的乙太網路介面，然後才可儲存該乙太網路介面。

基於通用準則對連結進行分組。例如，根據路徑偏好設定從最慣用到最不慣用對連結進行分組，從根據成本對連結進行分組。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **SD-WAN Interface Profile**（**SD-WAN** 介面設定檔），然後從 **Template**（範本）內容下拉清單中選取適當的範本。

STEP 3 | **Add**（新增）一個 SD-WAN 介面設定檔。

STEP 4 | 為 SD-WAN 介面設定檔輸入一個使用者易記的**Name**（名稱），您將在報告、疑難排解和統計資料中看到該名稱。

STEP 5 | 如果您有多重 vsys Panorama™ 管理伺服器，請選取 vsys **Location**（位置）。預設情況下，會選取 vsys1。

STEP 6 | 選取該設定檔將指派到介面的 **Link Tag**（連結標籤）。

STEP 7 | 為設定檔新增 **Description**（描述）。

STEP 8 | 從預先定義的清單中，選取實體 **Link Type**（連結類型）（**ADSL/DSL**、**Cable modem**（纜線數據機）、**Ethernet**（乙太網路）、**Fiber**（光纖）、**LTE/3G/4G/5G**、**MPLS**、**Microwave/Radio**（微波/無線電）、**Satellite**（衛星）、**WiFi**、**Private Link1**（私人連結 **1**）、**Private Link2**（私人連結 **2**）、**Private Link3**（私人連結 **3**）、**Private Link4**（私人連結 **4**）或 **Other**（其他））。使用 PAN-OS 11.1.3 時，SD-WAN 外掛程式 3.2.1 和更新版本支援其他點對點私人連結類型，例如，**Private Link1**（私人連結 **1**）、**Private Link2**（私人連結 **2**）、**Private Link3**（私人連結 **3**）和 **Private Link4**（私人連結 **4**）。針對 **Private Link1**（私人連結 **1**）、**Private Link2**（私人連結 **2**）、**Private Link3**（私人連結 **3**）和 **Private Link4**（私人連結 **4**）連結類型，我們不支援從 SD-WAN 分支防火牆到 SD-WAN 中樞防火牆的純文字流量。設定任何新的私人連結類型時，請確定您在僅設定公用連結類型的中樞上具有 SD-WAN 政策規則。因為網際網路繫結流量從分支回傳至中樞或無法傳輸至中樞時，所以必須與此 SD-WAN 政策規則相符。否則，將會捨棄流量，因為這些私人連結

（**Private Link1**（私人連結 **1**）、**Private Link2**（私人連結 **2**）、**Private Link3**（私人連結 **3**）和 **Private Link4**（私人連結 **4**））是直接網際網路存取 (DIA) SD-WAN 介面的一部分。

（針對 *PAN-OS 11.1.3* 和更新版本、*SD-WAN* 外掛程式 *3.2.1* 和更新版本）若要啟用其他點對點私人連結類型，您必須確保下列項目：

- *Panorama* 管理伺服器應該在 *PAN-OS 11.1.3* 上執行
- *Panorama* 受管理的裝置必須在 *PAN-OS 11.1.3* 上執行
- *SD-WAN* 外掛程式版本必須為 *3.2.1*

（針對 *PAN-OS 11.2.0* 和更新版本、*SD-WAN* 外掛程式 *3.3.0* 和更新版本）若要啟用其他點對點私人連結類型，您必須確保下列項目：

- *Panorama* 管理伺服器應該在 *PAN-OS 11.2.0* 上執行
- *Panorama* 受管理的裝置必須在 *PAN-OS 11.2.0* 上執行
- *SD-WAN* 外掛程式版本必須為 *3.3.0*

防火牆可以支援任何作為乙太網路連線終止和切換到防火牆的 CPE 裝置。例如，WiFi 存取點、LTE 數據機、雷射/微波 CPE，都可以透過乙太網路切換來終止。

下列連結類型將會形成僅具有相同連結類型的通道：

- 公用（或 ***Other***（其他））連結類型—***Ethernet***（乙太網路）、***ASDL/DSL***、***Cable modem***（纜線數據機）、***Fiber***（光纖）、***LTE/3G/4G/5G***、***WiFi*** 和 ***Other***（其他）。

  任何公用連結類型到任何其他公用連結類型都將會成功建立通道。例如，*[Ethernet-to-Other*（乙太網路到其他）*]* 和 *[Other-to-Other*（其他到其他）*]* 連結類型將會成功建立通道。
- *[Private*（私人）*]* 和 *[Point-to-Point*（點對點）*]* 連結類型—***MPLS***、***Satellite***（衛星）、***Private Link1***（私人連結 ***1***）、***Private Link2***（私人連結 ***2***）、***Private Link3***（私人連結 ***3***）、***Private Link4***（私人連結 ***4***）和 ***Microwave/Radio***（微波/無線電）。

  私人連結類型可以建立只具有相同私人連結類型的通道。例如，「*MPLS* 到 *MPLS*」和「衛星到衛星」連結類型有效，因此將會成功建立通道，但「*MPLS* 到衛星」不會建立通道。

針對在將用於支援 *SD-WAN* 的介面上所定義區域的現有 *PAN-OS* 部署，*Panorama* 可能會在下列情況下，自動將介面的區域名稱設定為其中一個預先定義的 *SD-WAN* 區域：

1. *SD-WAN* 介面在其介面設定檔中設定為點對點私人連結類型（***MPLS***、***Satellite***（衛星）、***Private Link1***（私人連結 ***1***）、***Private Link2***（私人連結 ***2***）、***Private Link3***（私人連結 ***3***）、***Private Link4***（私人連結 ***4***）或 ***Microwave***（微波））。
2. *SD-WAN* 介面設定檔上的 ***VPN Data Tunnel Support***（***VPN*** 資料通道支援）核取方塊已停用（取消核取）。這會指示 *PAN-OS* 在 *SD-WAN VPN* 通道外以純文字形式轉送流量。因為 ***Private Link1***（私人連結 ***1***）、***Private Link2***（私人連結 ***2***）、***Private Link3***（私人連結 ***3***）和 ***Private Link4***（私人連結 ***4***）連結類型不支援從 *SD-WAN* 分支防火牆到 *SD-WAN* 中樞防火牆的純文字流量，所以您設定這些私人連結類型時必須啟用 ***VPN Data Tunnel Support***（***VPN*** 資料通道支援）選項。

在中樞防火牆上，當符合條件 a) 時，區域名稱會設定為「`zone-to-branch`」。在分支防火牆上，當條件 a) 和條件 b) 都符合時，區域名稱會設定為「`zone-to-hub`」。Panorama 會自動執行此步驟以簡化設定，確保中樞和分支防火牆之間的正確通訊。如果您已有參照舊區域名稱的防火牆政策，則必須更新政策以反映新的預先定義 SD-WAN 區域名稱。

STEP 9 | 指定從 ISP 下載的 **Maximum Download**（最大下載）**(Mbps)** 速度，以 MB/S 為單位（範圍為 0 到 100,000；沒有預設值）。您可以使用最多三個小數位輸入範圍，例如 10.456。向您的 ISP 詢問連結速度，或使用 speedtest.net 之類的工具採樣連結的最大速度，並取較長一段時間內最大值的平均值。

STEP 10 | 指定向 ISP 上傳的 **Maximum Upload**（最大上傳）**(Mbps)** 速度，以 MB/S 為單位（範圍為 0 到 100,000；沒有預設值）。您可以使用最多三個小數位輸入範圍，例如 10.456。向您的 ISP 詢問連結速度，或使用 speedtest.net 之類的工具採樣連結的最大速度，並取較長一段時間內最大值的平均值。

STEP 11 | 選取 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格），以啟用介面的正向錯誤更正 (FEC) 或封包複製。您必須在編碼和解碼防火牆上都啟用此選項。您還必須建立錯誤更正設定檔，以套用至特定應用程式的 SD-WAN 原則規則。

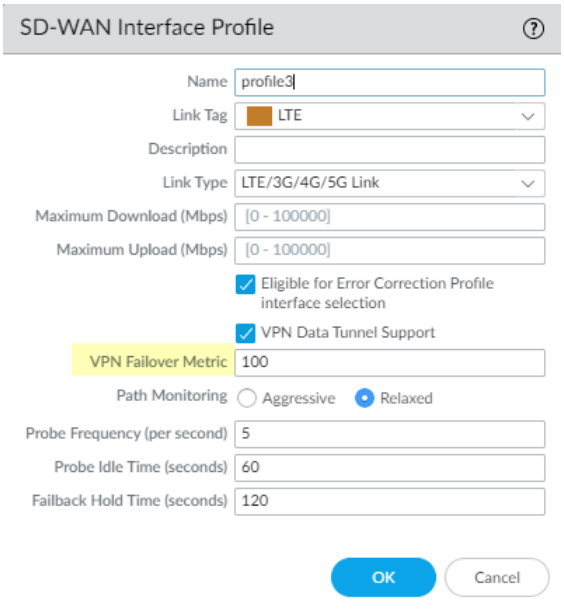
STEP 12 | **VPN Data Tunnel Support**（**VPN** 資料通道支援）會確定分支到中樞的流量和返回流量是通過 VPN 通道流動以增加安全性（預設方法），還是在 VPN 通道之外流動以避免加密負荷。

- 對於具有直接網際網路連線或網際網路中斷能力的共用連結類型（如纜線數據機、ADSL 和其他網際網路連線，請將 **VPN Data Tunnel Support**（**VPN** 資料通道支援）保留啟用。
- 您可以針對 MPLS、衛星或微波這類沒有網際網路中斷能力的私人連結類型停用 **VPN Data Tunnel Support**（**VPN** 資料通道支援），但 **Private Link1**（私人連結 **1**）、**Private**

Link2（私人連結 **2**）、**Private Link3**（私人連結 **3**）和 **Private Link4**（私人連結 **4**）連結類型除外。但是，您必須先確保流量不會被攔截，因為流量將在 VPN 通道外進行傳送。

- （SD-WAN 外掛程式 3.2.1 和更新版本）因為 **Private Link1**（私人連結 **1**）、**Private Link2**（私人連結 **2**）、**Private Link3**（私人連結 **3**）和 **Private Link4**（私人連結 **4**）連結類型不支援從 SD-WAN 分支防火牆到 SD-WAN 中樞防火牆的純文字流量，所以您設定這些私人連結類型時必須啟用 **VPN Data Tunnel Support**（**VPN** 資料通道支援）。
- 分支能具有 DIA 流量，即需要容錯移轉到連線至中樞的私人 MPLS 連結，並從中樞到達網際網路。**VPN Data Tunnel Support**（**VPN** 資料通道支援）設定確定私人資料通過 VPN 通道流動還是在通道外流動，以及容錯移轉的流量使用其他連線（私人資料流未使用的連線）。防火牆使用區域將 DIA 容錯移轉流量和私人 MPLS 流量分割開來。

STEP 13 | 如果您 設定 DIA AnyPath，則主體虛擬介面可以具有多個中樞虛擬介面，因此您必須依照選取特定中樞進行容錯移轉的順序進行優先排序。透過為套用此設定檔的中樞虛擬介面中搭配的 VPN 通道設定 **VPN Failover Metric**（**VPN** 容錯移轉指標）來指定此優先順序。指標越低，容錯移轉期間選取該介面的優先順序就越高。如果多個中樞虛擬介面具有相同的指標值，則 SD-WAN 將以循環方式向其傳送新的工作階段流量。



STEP 14 | （選用）選取 **Path Monitoring**（路徑監控）模式，在該模式中，防火牆會監控您套用此 SD-WAN 介面設定檔的介面。

防火牆會基於 ***Link Type***（連結類型）選擇它認為最佳的監控方式。除非介面（您在套用此設定檔的地方）存在需要更積極或更寬鬆的路徑監控的問題，否則請保留連結類型的預設設定。

- **Aggressive**（積極）—（LTE 和衛星之外的單所有連結類型的預設值）防火牆以固定的頻率將探查封包傳送到 SD-WAN 連結的另一端。如果您需要更快的偵測以及在暫時低壓和斷電情況下進行容錯移轉，請使用此模式。
- **Relaxed**（寬鬆）—（LTE 和衛星連結類型的預設值）防火牆在傳送探查封包組之間等待幾秒（探查閒置時間），讓路徑監控不那麼頻繁。當探查閒置時間到期時，防火牆會以設定

的探查頻率傳送探查七秒。當您擁有低頻寬連結、按使用量收費的連結（如 LTE），或相比偵測節省成本和頻寬更為重要時，請使用此模式。

STEP 15 | 設定探查頻率（每秒），這是防火牆每秒鐘向 SD-WAN 連結的另一端傳送探查封包的次數（範圍為 1 到 5；預設值為 5）。預設設定可對暫時低壓和斷電情況提供亞秒級的偵測。

如果您變更 *Panorama* 範本的探測頻率，則還應在 *Panorama* 裝置群組的路徑品質設定檔中調整 封包遺失百分比。

STEP 16 | 如果您選取 **Relaxed**（寬鬆）路徑監控，您可以設定防火牆在傳送探查封包組期間等待的探查閒置時間（秒）（範圍為 1 到 60；預設值為 60）。

STEP 17 | 輸入容錯回復保留時間（秒），這是防火牆在易錯移轉後將復原的連結恢復為偏好連結之前，防火牆等待復原的連結保持合格的時間（範圍為 20 到 120；預設值為 120）。

STEP 18 | 按一下 **OK**（確定）來儲存設定檔。

STEP 19 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 20 | 監控您的應用程式和連結監控情況指標，產生有關應用程式和連結監控情況效能的報告。如需詳細資訊，請參閱 監控與報告。

為 SD-WAN 設定實體乙太網路介面

在 Panorama 中，設定實體第三層乙太網路介面，然後啟用 SD-WAN 功能。若要設定實體介面，您必須為其指派 IPv4 和 (或) IPv6 位址。您也必須為介面指派完整下一個躍點閘道，然後將 SD-WAN 介面設定檔指派給介面。（SD-WAN 僅支援第三層介面類型；其不支援第二層網路，例如 VPLS。）

在您使用 Panorama 來建立 VPN 叢集並在 CSV 中匯出中樞和分支資訊之後，SD-WAN 外掛程式中的自動 VPN 設定會使用此資訊以針對相關聯的分支和中樞來產生設定，而設定包括預先定義的 SD-WAN 區域，而且會在 SD-WAN 分支與中樞之間建立安全 VPN 通道。如果您在新增 SD-WAN 分支或中樞時在 CSV 或 Panorama 中輸入了 BGP 資訊，Auto VPN 設定還會產生 BGP 設定。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），並從 **Template**（範本）內容下拉式清單中選取適當的範本，再選取插槽號碼（如 Slot1），然後選取介面 (例如，ethernet1/1)。

STEP 3 | 選取 **Layer3** 作為 **Interface Type**（介面類型）。

STEP 4 | 在 **Config**（設定）頁籤上，針對舊版路由引擎，選取 **Virtual Router**（虛擬路由器），或建立新的虛擬路由器。對於 進階路由引擎，選取一個 **Logical Router**（邏輯路由器）或建立一個新的邏輯路由器。

STEP 5 | 為您正在設定的介面指派適當的安全性區域。

例如，如果您要建立指向 ISP 的上行連結，則必須知道您所選擇的乙太網路介面將會前往不受信任的區域。

STEP 6 | 若要在 IPv4 介面上啟用 SD-WAN，請選取 **IPv4** 頁籤，然後 **Enable SD-WAN**（啟用 **SD-WAN**）。

使用 SD-WAN 外掛程式 3.2.0 和更新版本時，您最多可以針對已啟用 SD-WAN 的介面設定四個 IP 位址。SD-WAN 外掛程式只會使用已設定 IP 位址清單中的第一個 IP 位址來建立 SD-WAN 通道。

SD-WAN 只會考慮 **Next Hop Gateway**（下一個躍點閘道）的第一個 **IP** 位址，並忽略清單中的其餘 **IP** 位址。

（僅限 HA 部署）如果您想要從 SD-WAN 外掛程式 3.2.0 版降級至 3.1.0 或更早版本，則請先移除兩個防火牆上的 HA 主動/被動設定，再嘗試降級程序，例如，降級 PAN-OS 和 SD-WAN 外掛程式版本。

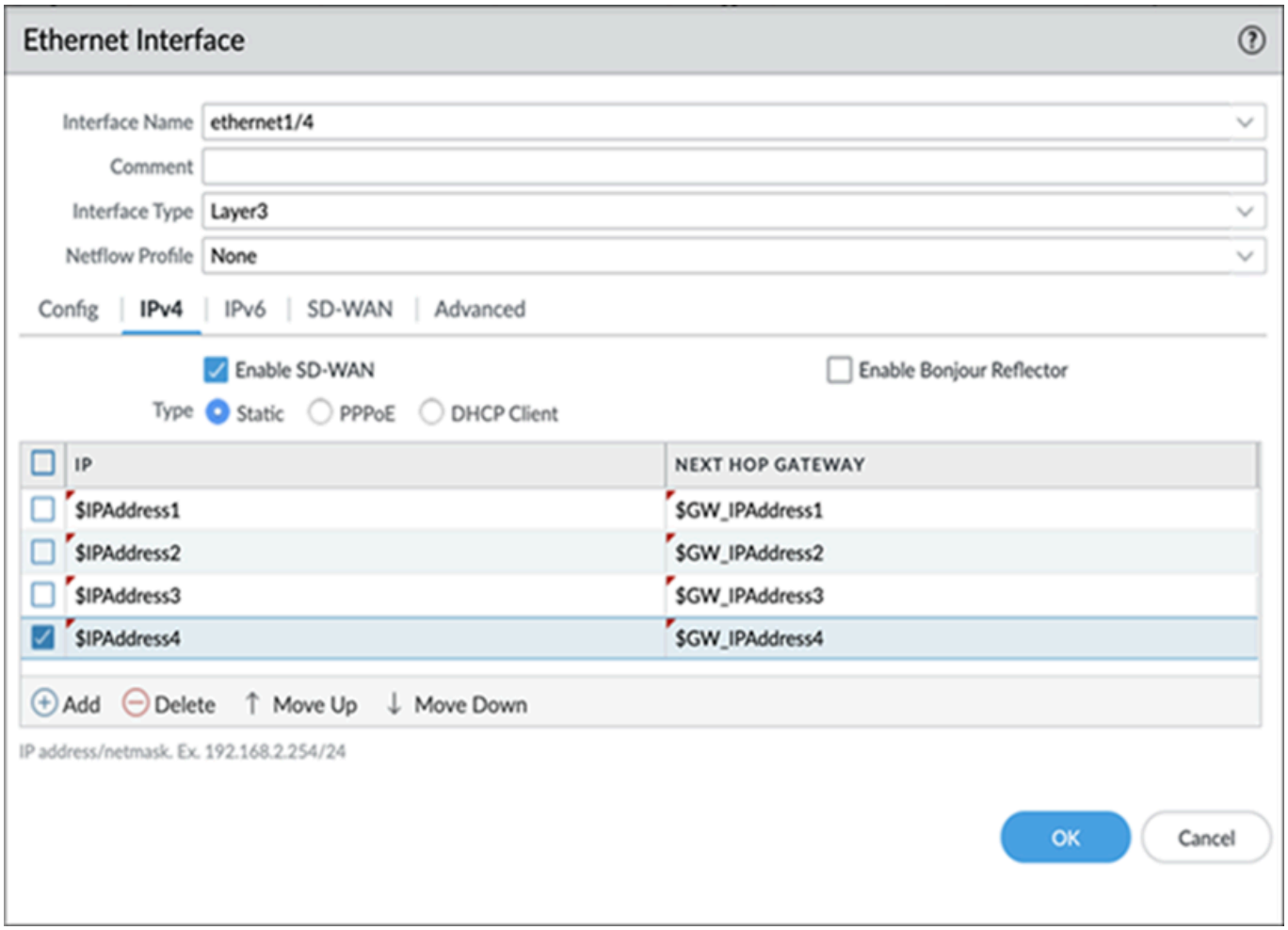
STEP 7 | 針對 IPv4 介面，選取位址的 **Type**（類型）：

- 靜態—在 **IP** 欄位中，為介面新增一個 IPv4 位址和前置詞長度。您可以使用包含一個位址範圍的已定義變數，如 $uplink。輸入 **Next Hop Gateway** 下一個躍點閘道（您剛剛輸入的 IPv4 位址的下一個躍點）的完整 IPv4 位址。下一個躍點閘道必須在與 IPv4 位址相同的子網路上。下一個躍點閘道是您在購買服務時 ISP 為您提供的 ISP 預設路由器的 IP 位址。這是防火牆向其發送流量以到達 ISP 的網路並最終到達網際網路和中樞的下一個躍點 IP 位址。

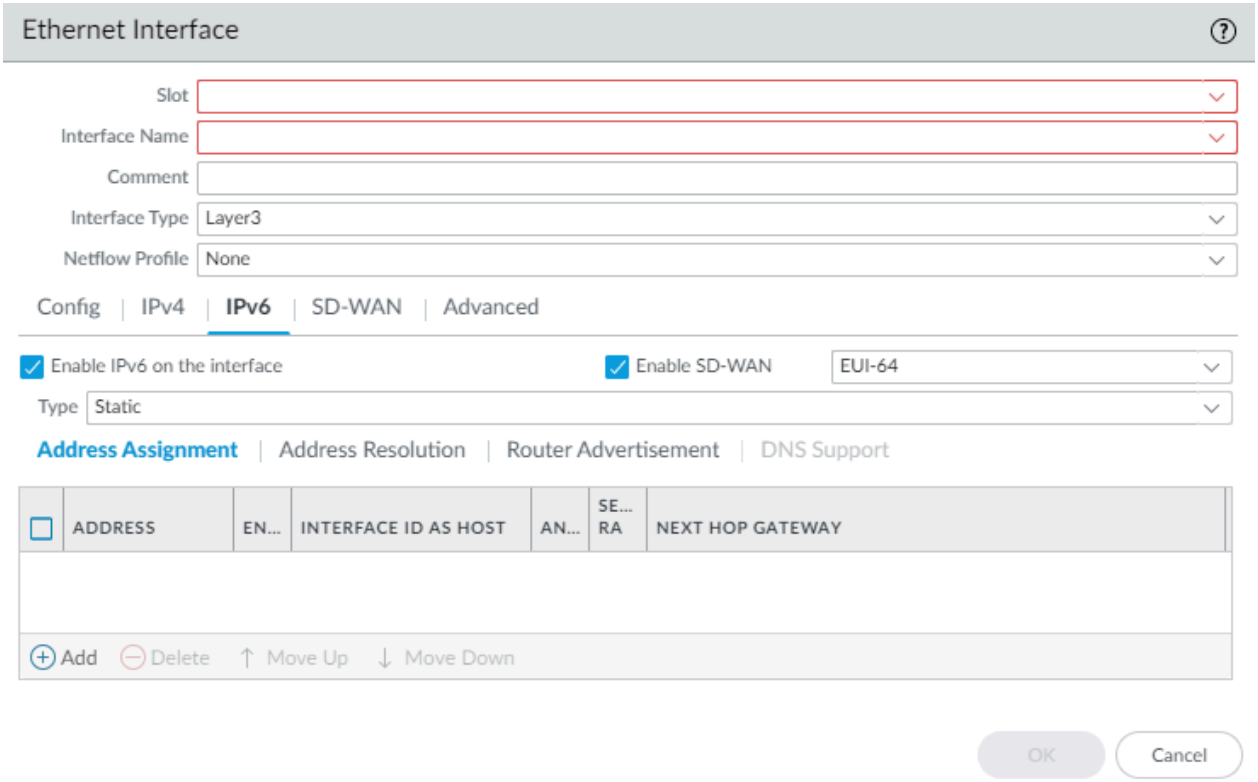
- **PPPoE**—為 DSL 連結 **Enable**（啟用）PPPoE 驗證，輸入 **Username**（使用者名稱）和 **Password**（密碼），然後 **Confirm Password**（確認密碼）。
- **DHCP Client**（**DHCP** 用戶端）—DHCP 指派預設閘道（也稱為 ISP 連線的下一個躍點閘道）非常重要。ISP 將提供所有必要的連線資訊，如動態 IP 位址、DNS 伺服器和預設閘道。

儘管中樞或分支介面支援 *DHCP* 用戶端，但在中樞介面上，您最好指派 ***Static***（靜態）位址而不是 *DHCP* 用戶端。在中樞上使用 *DHCP* 需要 *Palo Alto Networks DDNS* 服務。在中樞網站使用靜態位址可建立更穩定的環境，因為解析 *DHCP IP* 位址變更時不會涉及 *DDNS*，而且因為 *DDNS* 服務在變更時可能需要幾分鐘的時間來註冊新的 *IP* 位址。如果您有多個分支網站連線至中樞網站，則穩定性對於維持網路正常運作而言十分重要。

如果您選取 *[DHCP Client*（*DHCP* 用戶端）*]*，則請務必停用 ***Automatically create default route pointing to default gateway provided by server***（自動建立指向伺服器所提供之預設閘道的預設路由）選項，而此選項預設會予以啟用。



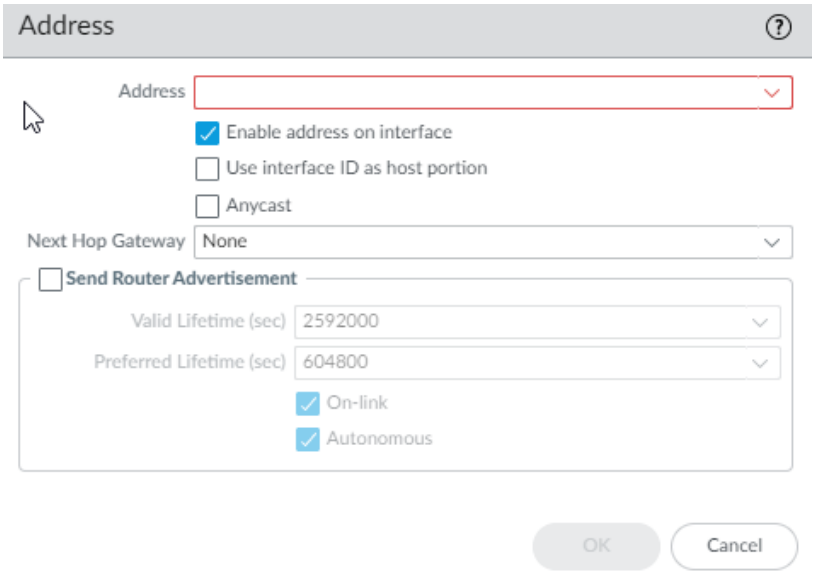
STEP 8 | 若要在 IPv6 介面上啟用 SD-WAN，請選取 **IPv6** 頁籤，並 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Enable SD-WAN**（啟用 **SD-WAN**）。



STEP 9 | 在 **EUI-64 (default 64-bit Extended Unique Identifier)**（**EUI-64**（預設 **64** 位元擴充唯一識別碼））欄位中，輸入十六進位格式的 64 位元 EUI。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。

STEP 10 | 針對 IPv6 介面，將位址的 **Type**（類型）選取為 **Static**（靜態）。選取 **Address Assignment**（位址指派）頁籤。

1. **Add**（新增）介面的 IPv6 **Address**（位址），或選取 **New Variable**（新增變數）以建立變數。SD-WAN 支援每個實體介面有一個 IPv6 位址。
2. **Enable address on interface**（在介面上啟用位址）。



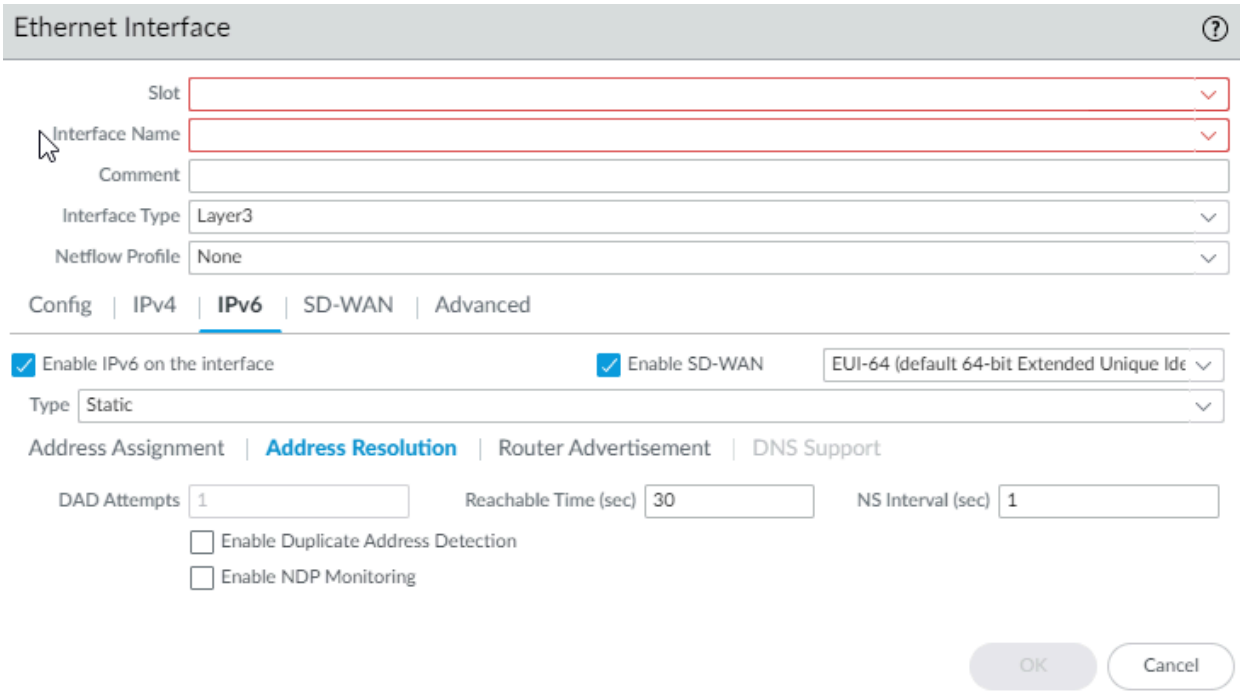
3. **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—請參閱上一步以取得解釋。
4. **Anycast**—選取以將 IPv6 位址（路由）設為 Anycast 位址（路由），這表示多個位置可以公告相同的首碼，而且 IPv6 會根據路由通訊協定的成本和其他因素以將 Anycast 流量傳送至其認為最近的節點。
5. **Next Hop Gateway**（下一個躍點閘道）—輸入 [Next Hop Gateway（下一個躍點閘道）] 的 IPv6 位址（您所輸入 IPv6 位址的下一個躍點）。[Next Hop Gateway（下一個躍點閘道）] 必須在與 IPv6 位址相同的子網路上。下一個躍點閘道是您在購買服務時 ISP 為您提供的 ISP 預設路由器的 IP 位址。其是防火牆傳送流量以到達 ISP 網路、最後到達網際網路和中樞的下一個躍點 IP 位址。
6. **Send Router Advertisement**（傳送路由器公告）—選取以讓防火牆在 [Router Advertisements (RAs)（路由器公告 (RA)）] 中傳送此位址，而在這種情況下，您也必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項（在 **Router Advertisement**（路由器公告）頁籤上）。
7. **Valid Lifetime (sec)**（有效存留時間（秒））—輸入防火牆將位址視為有效的有效存留時間（以秒為單位）。有效的存留時間必須等於或超過 **Preferred Lifetime (sec)**（偏好存留時間（秒））（預設值為 2,592,000）。
8. **Preferred Lifetime (sec)**（偏好存留時間（秒））—輸入偏好有效位址的偏好存留時間（以秒為單位），這表示防火牆可以使用其來傳送和接收流量。偏好存留時間到期之後，

防火牆無法使用位址來建立新連線，但除非有效存留時間（預設值為 604,800）到期，否則任何現有連線都有效。

9. **On-link**（記錄連結）—如果可不使用路由器，連線首碼中內含位址的系統，請選取此選項。
10. **Autonomous**（自發）—如果系統合併所公告的首碼與介面 ID 來獨立建立 IP 位址，則請選取此選項。
11. 按一下 **OK**（確定）。

STEP 11 | 對於靜態 IPv6 介面，設定位址解析。

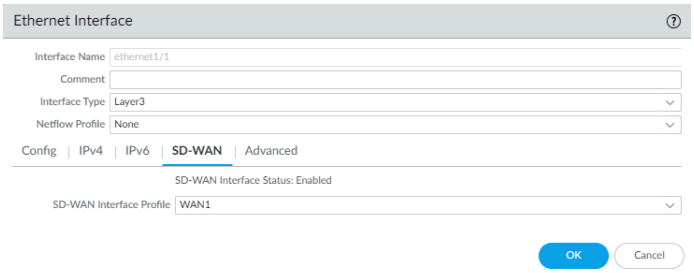
1. 選取 **Address Resolution**（位址群組）。
2. 如果您想要在將潛在 IPv6 位址指派給介面之前驗證其唯一性，請啟用 **Duplicate Address Detection**（重複位址偵測）(DAD)（預設予以啟用）。
3. 如果您選取 **Enable Duplicate Address Detection**（啟用重複位址偵測），則請指定在識別芳鄰的嘗試失敗之前，芳鄰請求 (NS) 間隔內的 **DAD Attempts**（**DAD** 嘗試）次數（範圍為 1 到 10；預設值為 1）。
4. 輸入 **Reachable Time (sec)**（可連線時間（秒）），指定用戶端在收到可連線能力確認訊息後，用來假設芳鄰可連線的時間長度（範圍為 10 至 36,000，預設值為 30）。
5. 輸入 **NS Interval (sec)**（**NS** 間隔（秒））（芳鄰請求間隔），即芳鄰請求之間的時間長度；範圍為 1 到 3,600；預設值為 1
6. **Enable NDP Monitoring**（啟用 **NDP** 監控）以啟用芳鄰探索通訊協定監控。啟用時，您可以選取 [Features（功能）] 欄中的 NDP 圖示，並檢視下列資訊：防火牆所探索到芳鄰的 IPv6 位址、對應的 MAC 位址、User-ID 和狀態（假定在最理想的情況下）。
7. 按一下 **OK**（確定）。



STEP 12 | 如果您想要讓介面傳送 IPv6 路由器公告 (RA)，並選擇性調整 RA 參數，則請依 PAN-OS 網路管理員指南設定第三層介面中所記載來設定路由器公告。

STEP 13 | 在 **SD-WAN** 索引標籤上，選取一個您已經建立的 **SD-WAN** 介面設定檔（或建立一個新的 SD-WAN 介面設定檔）以套用到此介面。SD-WAN 介面設定檔有一個關聯的連結標籤，因此套用此設定檔的介面也將具有該關聯的連結標籤。一個介面僅具有一個連結標籤。

STEP 14 | 按一下 **OK**（確定）以儲存乙太網路介面。

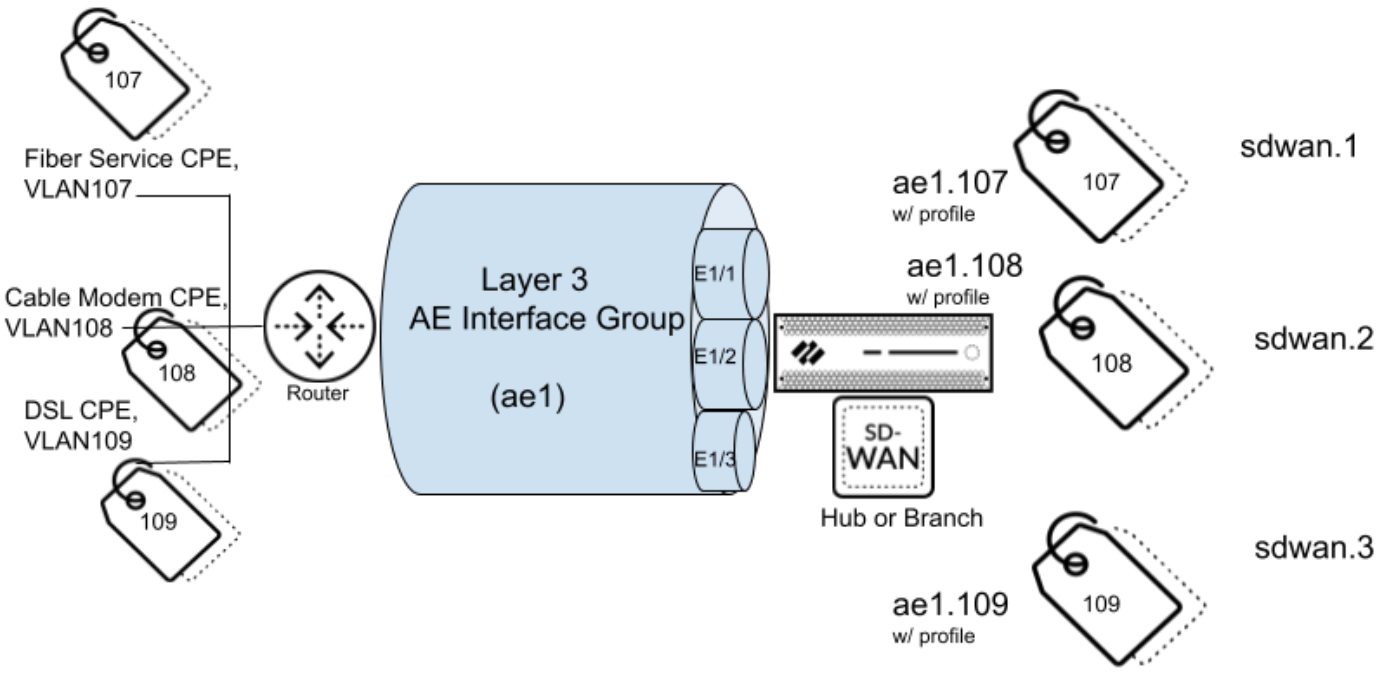


STEP 15 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 16 | （僅 SD-WAN 手動設定）設定虛擬 SD-WAN 介面。如果您要使用自動 VPN，則自動 VPN 設定將會執行此工作。

為 SD-WAN 設定彙總乙太網路介面和子介面

執行 PAN-OS 11.0 和 SD-WAN 外掛程式 2.1.0 的實體防火牆支援彙總乙太網路 (AE) 介面上的 SD-WAN，這樣，舉例來說，資料中心內的 SD-WAN 防火牆可以擁有提供連結備援的實體乙太網路介面的彙總介面群組（組合）。SD-WAN 支援包含或不含子介面的 AE 介面。您可以建立具有多個子介面的 AE 介面，針對不同的 ISP 服務對介面進行標記，以便提供端對端流量分割。因此，您的 ISP 服務可以到達多個實驗室或建築物，而不需要為每個連線使用專用的光纖配對。一個第三層 AE 介面群組會連線到路由器，如下圖所示：



VM-Series 防火牆不支援 *AE* 介面。具有 *AE* 介面的 *SD-WAN* 中樞或分支防火牆不應該屬於與 *VM-Series SD-WAN* 中樞或分支防火牆相同的 *VPN* 叢集，因為 *VM-Series* 防火牆不支援 *AE* 介面。

子介面上不支援 *PPPoE*。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 為 AE 介面群組中的每個 ISP 連線（子介面）設定 SD-WAN 介面設定檔 以定義其連結屬性。

STEP 3 | 建立 AE 介面群組。

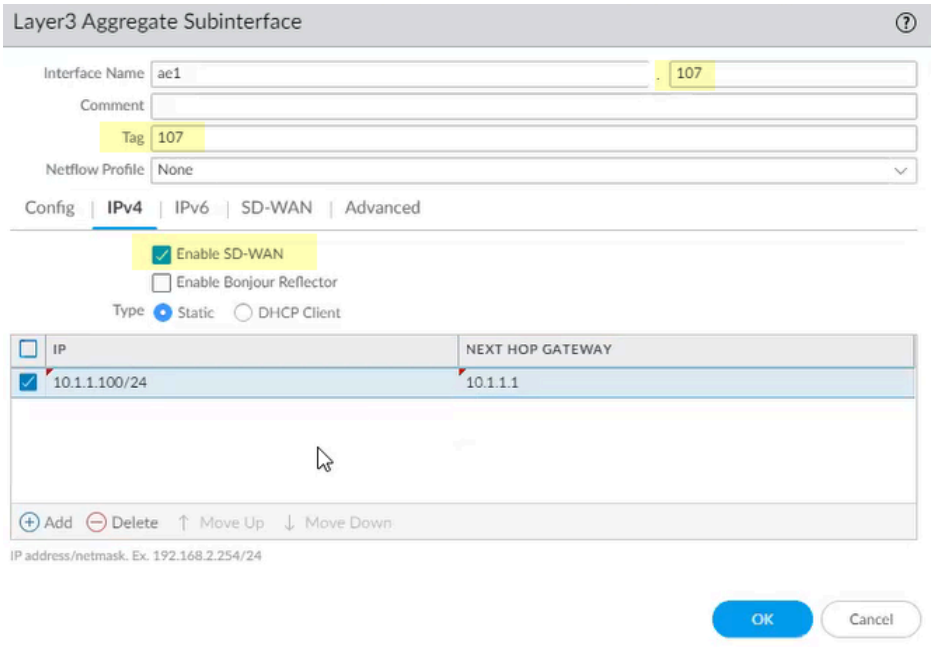
1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），選取一個 Panorama **Template**（範本），然後選取 **Add Aggregate Group**（新增彙總群組）。
2. 在 **Interface Name**（介面名稱）中，輸入編號以識別彙總群組，範圍為 1 至 16。
3. 對於 **Interface Type**（介面類型），選取 **Layer3**。
4. 按一下 **OK**（確定）。

STEP 4 | 將實體介面指派給彙總群組。

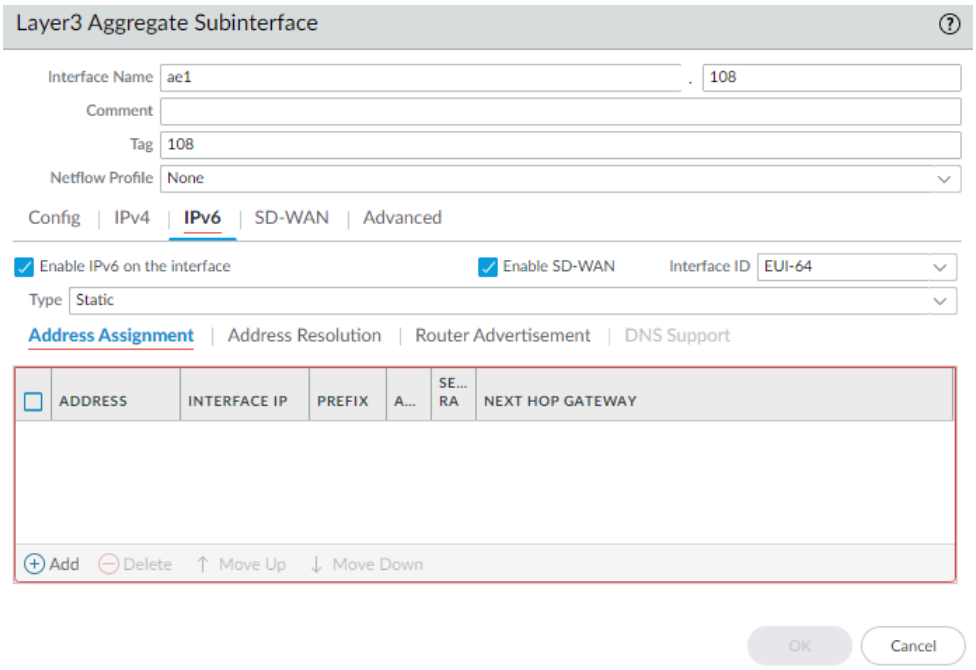
1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後選取要指派到彙總群組的介面。
2. 針對 **Interface Type**（介面類型）選取 **Aggregate Ethernet**（彙總乙太網路）。
3. 選取您建立的彙總群組，例如 ae1。
4. 在 **Advanced**（進階）索引標籤上，選取 **Link Speed**（連結速度）、**Link Duplex**（連結雙工）與 **Link State**（連結狀態）。
5. 按一下 **OK**（確定）。
6. 針對要指派給彙總群組的每個介面重複此步驟。

STEP 5 | 對於彙總群組，建立一個使用靜態 IP 位址的子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），反白顯示彙總群組（如 ae1），然後按一下螢幕底部的 **Add Subinterface**（新增子介面）。
2. 在 **Interface Name**（介面名稱）中，在句點後輸入一個編號，如 107。
3. 輸入 VLAN 標籤以區分不同子介面。將標籤設為與子介面 ID 相同的編號，以方便使用。
4. 若要設定子介面的靜態 IPv4 位址，請選取 **IPv4** 頁籤，然後 **Enable SD-WAN**（啟用 **SD-WAN**）。



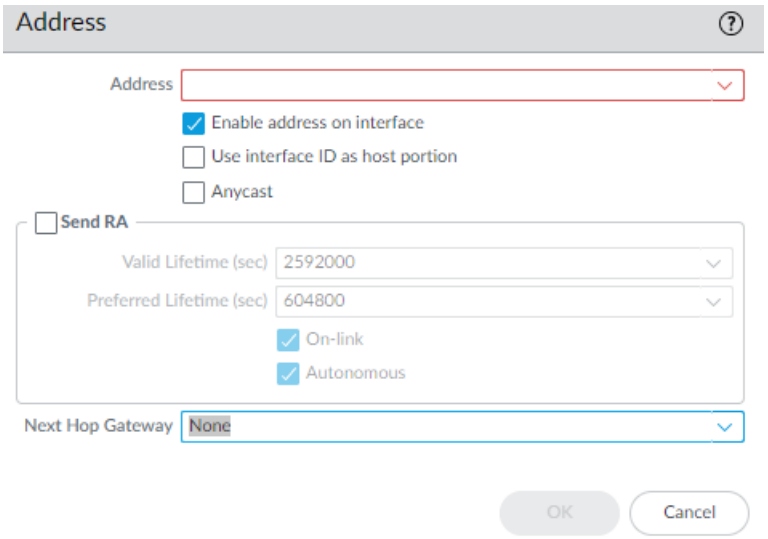
5. 選取位址的 **Type**（類型）：靜態。
6. **Add**（新增）子介面的 **IP** 位址（和子網路遮罩）。
7. 輸入下一個躍點閘道的 IP 位址。
8. 若要設定子介面的靜態 IPv6 位址，請選取 **IPv6** 頁籤，並 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**），然後 **Enable SD-WAN**（啟用 **SD-WAN**）。



9. 在 **EUI-64 (default 64-bit Extended Unique Identifier)**（**EUI-64**（預設 **64** 位元擴充唯一識別碼））欄位中，輸入十六進位格式的 64 位元 EUI。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。如果您在新增位址時啟用 **Use**

interface ID as host portion（使用介面 **ID** 作為主機部分）選項，則防火牆會使用介面 ID 作為該位址的主機部分。

10. 選取 **Address Assignment**（位址指派），然後 **Add**（新增）介面的 IPv6 **Address**（位址），或選取 **New Variable**（新建變數）以建立變數。

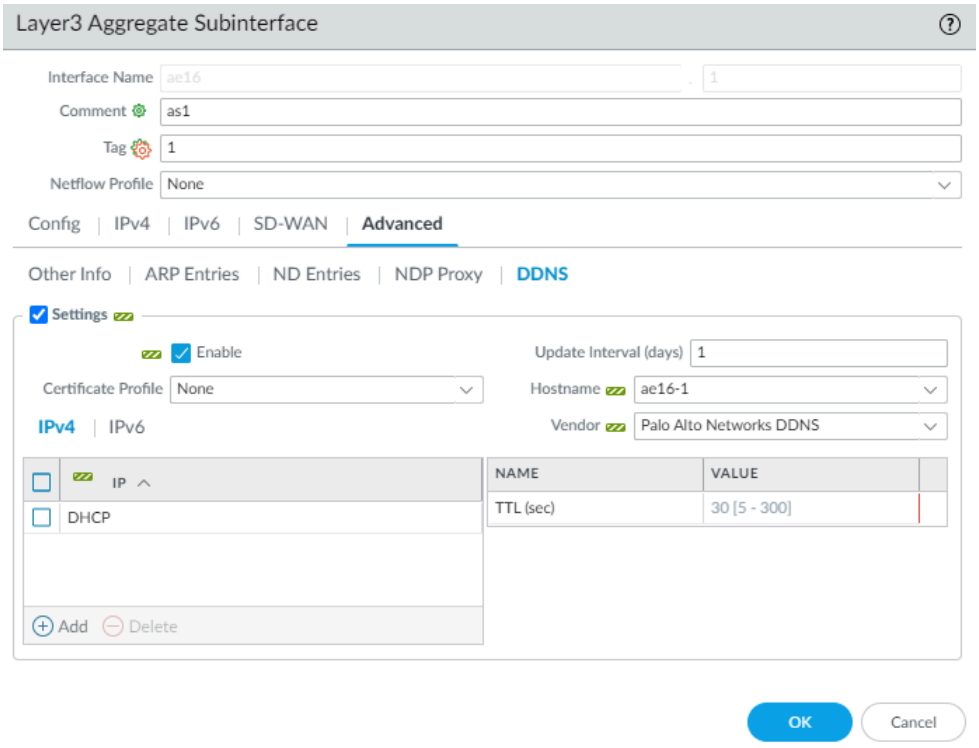


11. **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）；請參閱 **EUI-64** 的先前子步驟。
12. 選取 **Anycast**，以將 IPv6 位址（路由）設為 Anycast 位址（路由），這表示多個位置可以公告相同的首碼，而且 IPv6 會根據路由通訊協定成本和其他因素，以將 Anycast 流量傳送至其認為最近的節點。
13. 輸入 **Next Hop Gateway**（下一個躍點閘道）的 IPv6 位址（您所輸入 IPv6 位址的下一躍點）。[Next Hop Gateway（下一個躍點閘道）] 必須在與 IPv6 位址相同的子網路上。[Next Hop Gateway（下一個躍點閘道）] 是您在購買服務時 ISP 為您提供的 ISP 預設路由器的 IP 位址。其是防火牆傳送流量以到達 ISP 網路、最後到達網際網路和中樞的下一個躍點 IP 位址。
14. 選取 **Send Router Advertisement**（傳送路由器公告），讓防火牆以在 [Router Advertisements (RAs)（路由器公告 (RA)）] 中傳送此位址，而在這種情況下，您也必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項（在 [Router Advertisement（路由器公告）] 頁籤上）。
15. 輸入防火牆將位址視為有效的 **Valid Lifetime (sec)**（有效存留時間（秒））。有效的存留時間必須等於或超過 **Preferred Lifetime (sec)**（偏好存留時間（秒））（預設值為 2,592,000）。
16. 輸入偏好有效位址的 **Preferred Lifetime (sec)**（慣用存留時間（秒）），這表示防火牆可以使用其來傳送和接收流量。偏好存留時間到期之後，防火牆無法使用位址來建立新連線，但除非有效存留時間（預設值為 604,800）到期，否則任何現有連線都有效。
17. 如果可以在沒有路由器的情況下連線首碼內具有位址的系統，則請選取 **On-link**（在連結上）。
18. 如果系統可以合併所公告的首碼與介面 ID 來獨立建立 IP 位址，則請選取 **Autonomous**（自發）。
19. 按一下 **OK**（確定）。

STEP 6 | 靜態位址的替代方案是，針對彙總群組，建立可使用 DHCP 來取得其位址的子介面。

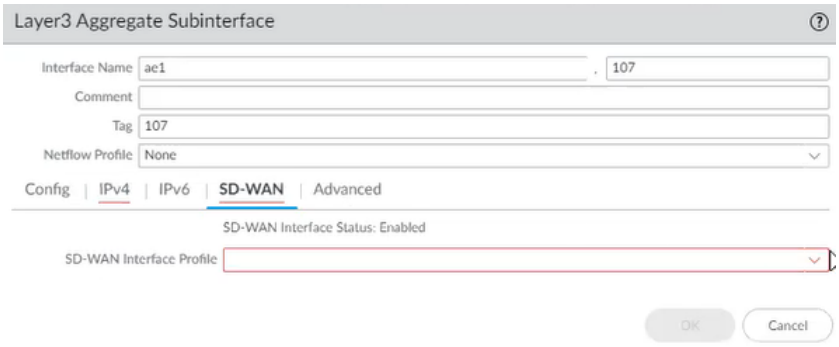
1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後在 **Template**（範本）欄位中選取範本堆疊。
2. 反白顯示彙總群組（如 ae1），然後按一下螢幕底部的 **Add Subinterface**（新增子介面）。
3. 反白顯示子介面，然後按一下螢幕底部的 **Override**（覆寫）。
4. 返白顯示子介面，在 **Interface Name**（介面名稱）中，在句點後輸入一個編號，如 1。
5. 輸入 VLAN 標籤以區分不同子介面。將標籤設為與子介面 ID 相同的編號，以方便使用。
6. 選取 **IPv4** 索引標籤並啟用 **SD-WAN**。

   已彙總介面群組中的子介面僅支援 *IPv4* 位址作為 *DHCP* 用戶端，而不支援 *IPv6* 位址。
7. 選取位址的 **Type**（類型）：**DHCP Client**（**DHCP** 用戶端）。
8. 選取 **Enable**（啟用）。
9. 取消核取（不選取）**Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）。
10. 選取 **Advanced**（進階）索引標籤和 **DDNS** 索引標籤。
11. 選取 **Settings**（設定），然後選取 **Enable**（啟用）。**Hostname**（主機名稱）由 Panorama SD-WAN 外掛程式自動產生。
12. 針對 **Vendor**（廠商）選取 **Palo Alto Networks DDNS**。
13. 按一下 **OK**（確定）。



STEP 7 | 將 SD-WAN 介面設定檔套用至子介面。

1. 反白顯示您建立的子介面，然後選取 **SD-WAN** 索引標籤。
2. 選取您為此連結建立的 **SD-WAN** 介面設定檔，或建立新的設定檔。



3. 按一下 **OK**（確定）。

STEP 8 | 重複先前的步驟，為彙總介面群組建立額外的第三層子介面，並將 SD-WAN 介面設定檔套用至每個子介面。

STEP 9 | **Commit**（認可）。

為 SD-WAN 設定第三層子介面

執行 PAN-OS 11.0 和 SD-WAN 外掛程式 2.1.0 的防火牆在第三層子介面上支援 SD-WAN，以便防火牆可以使用 VLAN 標籤對流量進行分割。以下工作顯示了如何建立使用靜態 IP 位址的第三層子介面以及如何建立使用 DHCP 獲取其位址的子介面。展示了如何為子介面指派 VLAN 標籤和在子介面上啟用 SD-WAN。建立 SD-WAN 介面設定檔以定義每個 ISP 連線並將設定檔指派給相應的子介面（虛擬 SD-WAN 介面）。

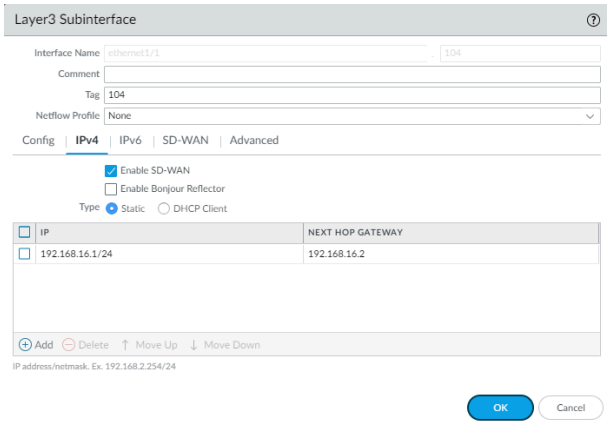
如果在 *VM-Series* 防火牆上設定 *SD-WAN* 第三層子介面，則 *VMware* 設定必須將相應的連接埠群組附加到允許所有 *VLAN* 的那些介面。

子介面上不支援 *PPPoE*。

STEP 1 | 為每個 ISP 連線（子介面）設定 SD-WAN 介面設定檔 以定義其連結屬性。

STEP 2 | 建立可使用靜態 IPv4 位址的第三層子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後在 **Template**（範本）欄位中選取範本。
2. 選取一個介面。
3. 對於 **Interface Type**（介面類型），選取 **Layer3**（第三層），然後按一下 **OK**（確定）。
4. 反白顯示介面，然後按一下螢幕底部的 **Add Subinterface**（新增子介面）。
5. 在 **Interface Name**（介面名稱）和句點之後，輸入子介面編號。
6. 為子介面輸入一個 **Tag**（標籤）（範圍為 1 至 4,094）。將標籤設為與子介面 ID 相同的編號，以方便使用。
7. 在 **IPv4** 索引標籤上，啟用 **SD-WAN**。
8. 選取位址的 **Type**（類型）：靜態。
9. **Add**（新增）**IP** 位址和子網路遮罩。
10. 輸入下一個躍點閘道的 IP 位址。
11. 按一下 **OK**（確定）。

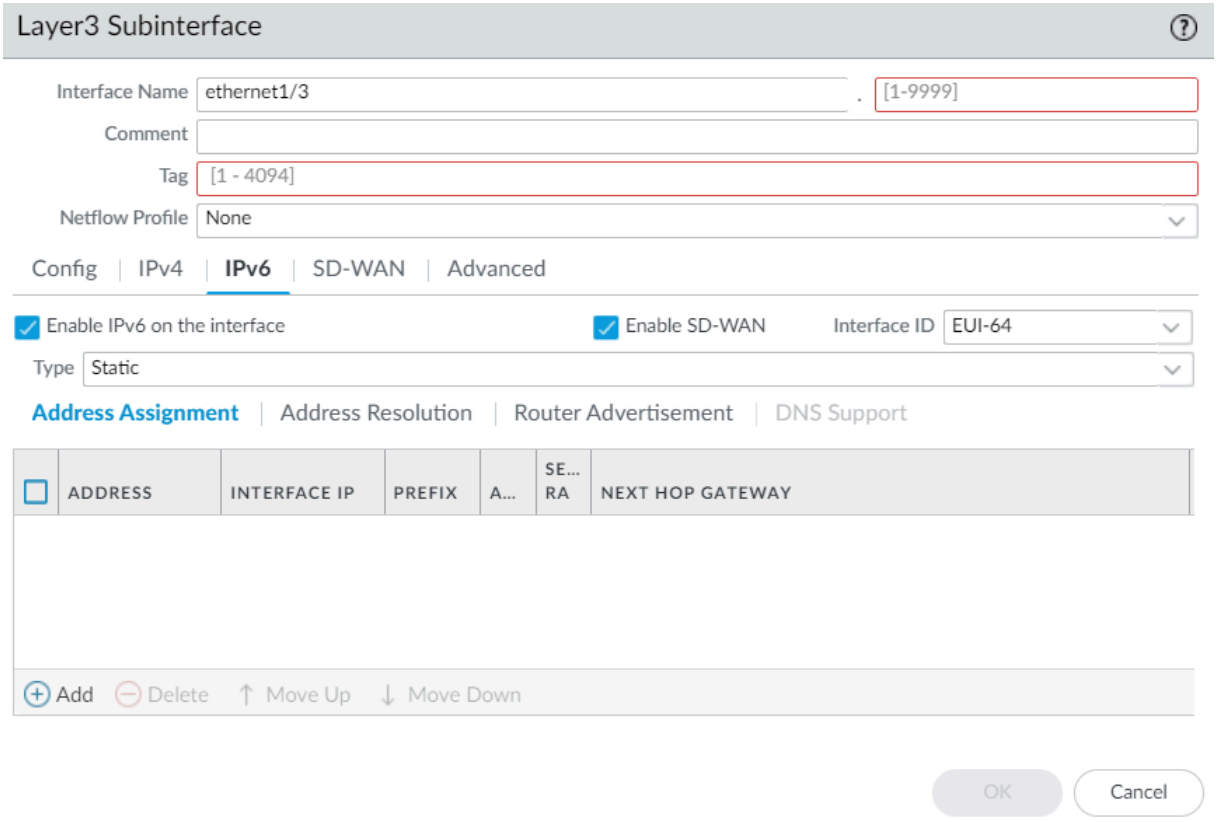


STEP 3 | 建立可使用靜態 IPv6 位址的第三層子介面。

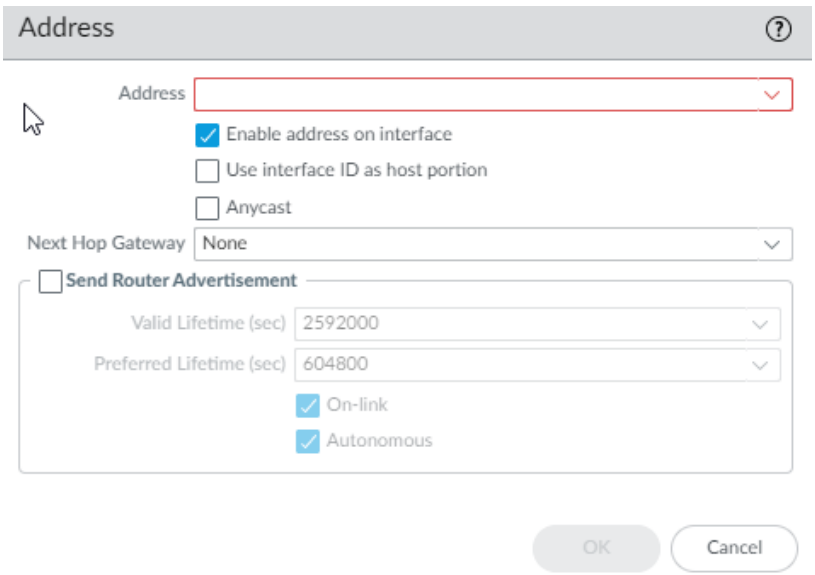
1. 執行可建立使用靜態 IPv4 位址之第三層子介面的步驟的前六個子步驟，因為其針對 IPv6 位址都相同。
2. 在 **IPv6** 頁籤上，選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）和 **Enable SD-WAN**（啟用 **SD-WAN**）。
3. 在 **EUI-64 (default 64-bit Extended Unique Identifier)**（**EUI-64**（預設 **64** 位元擴充唯一識別碼））欄位中，輸入十六進位格式的 64 位元 EUI。如果您將此欄位保留空白，防火牆會使用從實體介面的 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。

4. 選取位址的 **Type**（類型）：靜態。
5. 選取 **Address Assignment**（位址指派）。



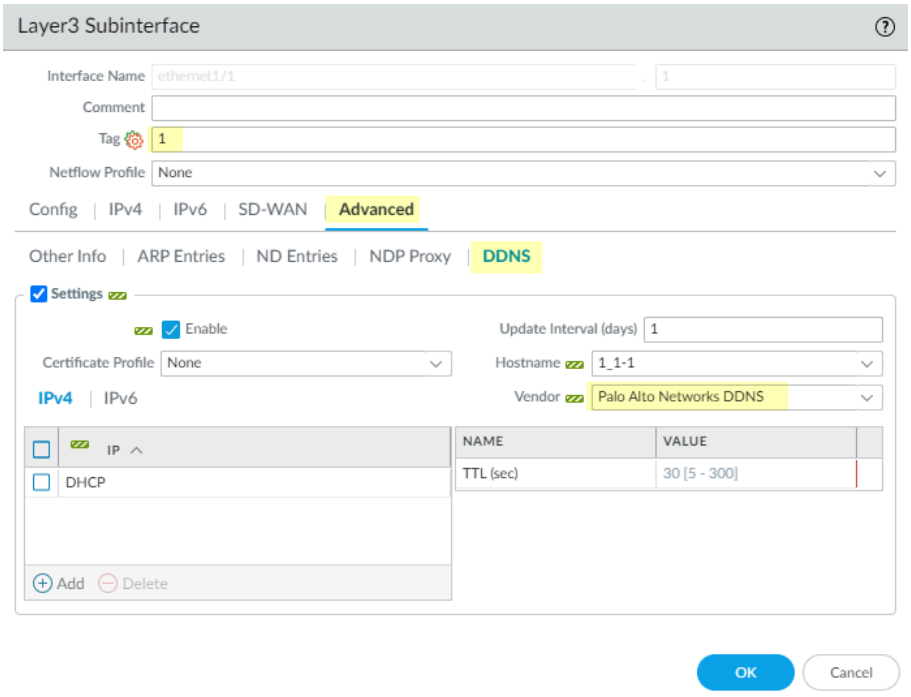
6. **Add**（新增）介面的 IPv6 **Address**（位址），或選取 **New Variable**（新增變數）以建立變數。SD-WAN 支援每個實體介面有一個 IPv6 位址。
7. **Enable address on interface**（在介面上啟用位址）。



8. **Use interface ID as host portion**（使用介面 **ID** 作為主機部分）—請參閱上面的第三個子步驟以取得解釋。
9. **Anycast**—選取以將 IPv6 位址（路由）設為 Anycast 位址（路由），這表示多個位置可以公告相同的首碼，而且 IPv6 會根據路由通訊協定的成本和其他因素以將 Anycast 流量傳送至其認為最近的節點。
10. **Next Hop Gateway**（下一個躍點閘道）—輸入 [Next Hop Gateway（下一個躍點閘道）] 的 IPv6 位址（您所輸入 IPv6 位址的下一個躍點）。[Next Hop Gateway（下一個躍點閘道）] 必須在與 IPv6 位址相同的子網路上。下一個躍點閘道是您在購買服務時 ISP 為您提供的 ISP 預設路由器的 IP 位址。其是防火牆傳送流量以到達 ISP 網路、最後到達網際網路和中樞的下一個躍點 IP 位址。
11. **Send Router Advertisement**（傳送路由器公告）—選取以讓防火牆在 [Router Advertisements (RAs)（路由器公告 (RA)）] 中傳送此位址，而在這種情況下，您也必須在介面上啟用全域 **Enable Router Advertisement**（啟用路由器公告）選項（在 **Router Advertisement**（路由器公告）頁籤上）。
12. **Valid Lifetime (sec)**（有效存留時間（秒））—輸入防火牆將位址視為有效的有效存留時間（以秒為單位）。有效的存留時間必須等於或超過 **Preferred Lifetime (sec)**（偏好存留時間（秒））（預設值為 2,592,000）。
13. **Preferred Lifetime (sec)**（偏好存留時間（秒））—輸入偏好有效位址的偏好存留時間（以秒為單位），這表示防火牆可以使用其來傳送和接收流量。偏好存留時間到期之後，防火牆無法使用位址來建立新連線，但除非有效存留時間（預設值為 604,800）到期，否則任何現有連線都有效。
14. **On-link**（記錄連結）—如果可不使用路由器，連線首碼中內含位址的系統，請選取此選項。
15. **Autonomous**（自發）—如果系統合併所公告的首碼與介面 ID 來獨立建立 IP 位址，則請選取此選項。
16. 按一下 **OK**（確定）。

STEP 4 | 靜態位址的替代方案是，建立可使用 DHCP 取得其 IPv4 位址的第三層子介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後在 **Template**（範本）欄位中選取範本堆疊（不是範本）。
2. 選取一個介面。
3. 對於 **Interface Type**（介面類型），選取 **Layer3**（第三層），然後按一下 **OK**（確定）。
4. 反白顯示介面，然後按一下螢幕底部的 **Add Subinterfaces**（新增子介面）。
5. 反白顯示子介面，然後按一下 **Override**（覆寫）。
6. 反白顯示子介面，在 **Interface Name**（介面名稱）和句點之後，輸入子介面編號。
7. 為子介面輸入一個 **Tag**（標籤）（範圍為 1 至 4,094）。將標籤設為與子介面 ID 相同的編號，以方便使用。
8. 在 **IPv4** 索引標籤上，啟用 **SD-WAN**。
9. 選取位址的類型：選取 **DHCP Client**（DHCP 用戶端），然後 **Enable**（啟用）。
10. 取消核取（不選取）**Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）。
11. 選取 **Advanced**（進階）索引標籤，然後選取 **DDNS** 索引標籤。
12. 選取 **Settings**（設定），然後選取 **Enable**（啟用）。**Hostname**（主機名稱）由 Panorama SD-WAN 外掛程式自動產生。
13. 針對 **Vendor**（廠商）選取 **Palo Alto Networks DDNS**。
14. 按一下 **OK**（確定）。



STEP 5 | 將 SD-WAN 介面設定檔套用至子介面。

1. 反白顯示您建立的子介面，然後選取 **SD-WAN** 索引標籤。
2. 選取您為此連結建立的 **SD-WAN** 介面設定檔，或建立新的設定檔。
3. 按一下 **OK**（確定）。

STEP 6 | 重複前面的步驟以向介面新增更多子介面。

STEP 7 | **Commit**（認可）。

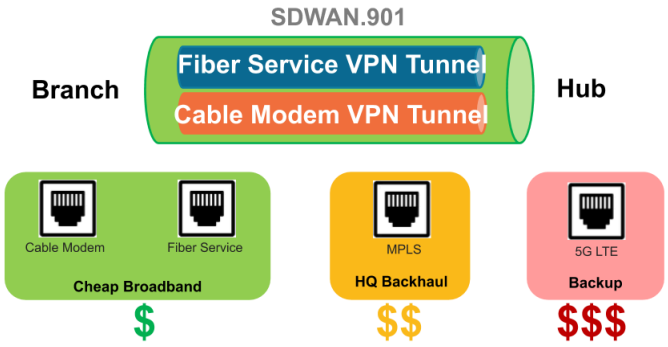
設定虛擬 SD-WAN 介面

如果您在 Panorama 中使用 Auto VPN 組態，它會為您建立 SD-WAN 介面，在這種情況下，您無需建立和設定虛擬 SD-WAN 介面。

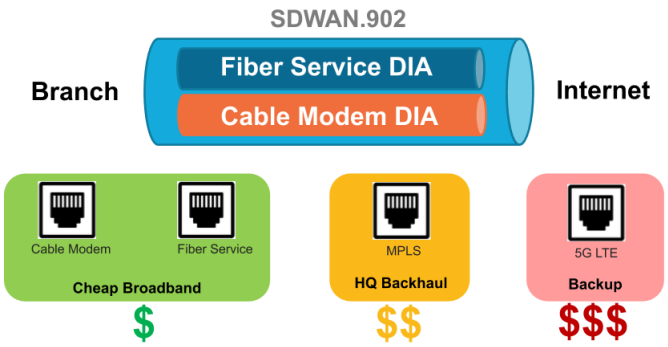
如果您沒有在 Panorama 中使用 Auto VPN 組態，請建立並設定一個虛擬 SD-WAN 介面以指定一個或多個具有 SD-WAN 功能的實體乙太網路介面，這些介面前往同一目的地，如一個特定的中樞或網際網路。事實上，一個虛擬 SD-WAN 介面中的所有連結都必須是相同類型的：全部都是 VPN 通道連結或全部都是直接網際網路存取 (DIA) 連結。

第一個圖展示名為 SDWAN.901 的 SD-WAN 介面範例，而此介面組合兩個使用不同載波的實體介面：Ethernet1/1（纜線數據機連結）和 Ethernet1/2（光纖服務連結）。兩個連結都是從分支到中樞的 VPN 通道。

在此圖中，*SD-WAN* 介面中的兩個連結都恰好使用相同連結標籤（價格實惠的寬頻），但 *SD-WAN* 介面中的連結其實可以有不同的連結標籤。



在下圖中，SDWAN.902 會組合 Ethernet1/1 和 Ethernet1/2 連結，兩者都是從分支到網際網路的 DIA 連結：



STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Network**（網路） > **Interfaces**（介面） > **SD-WAN**，然後從 **Template**（範本）內容下拉清單中選取適當的範本。

STEP 3 | 透過在 **sdwan.** 前置詞後輸入一個數字（1 到 9,999 之間），**Add**（新增）一個邏輯 SD-WAN 介面。

自動 *VPN* 設定會建立編號為 *.901*、*.902* 等的 *SD-WAN* 介面。因此，如果您想要手動建立 *SD-WAN* 介面，則請不要使用 *sdwan.90x* 格式作為 *SD-WAN* 介面名稱。同樣地，自動 *VPN* 設定會針對 *IPv6* 介面建立編號為 *.9016* 的 *SD-WAN* 介面，因此，請不要使用 *sdwan.9016* 作為 *SD-WAN* 介面名稱。

STEP 4 | 輸入描述性的 **Comment**（註解）。

新增有幫助性的註解，例如，如果您在「分支」範本上，則可以填寫分支到網際網路或分支到西部 ***USA*** 中樞。您的註解可讓疑難排解更為輕鬆，無需再嘗試解碼日誌和報告中自動產生的名稱。

STEP 5 | 選取 **Protocol**（通訊協定），以指出虛擬 SD-WAN 介面的類型：

- **ipv4** 指出 IPv4 DIA 虛擬介面。
- **ipv6** 指出 IPv6 DIA 虛擬介面。
- **none** 指出 VPN 通道虛擬介面。

STEP 6 | 在 **Config**（設定）標籤上，將 SD-WAN 介面指派給 **Virtual Router**（虛擬路由器）。

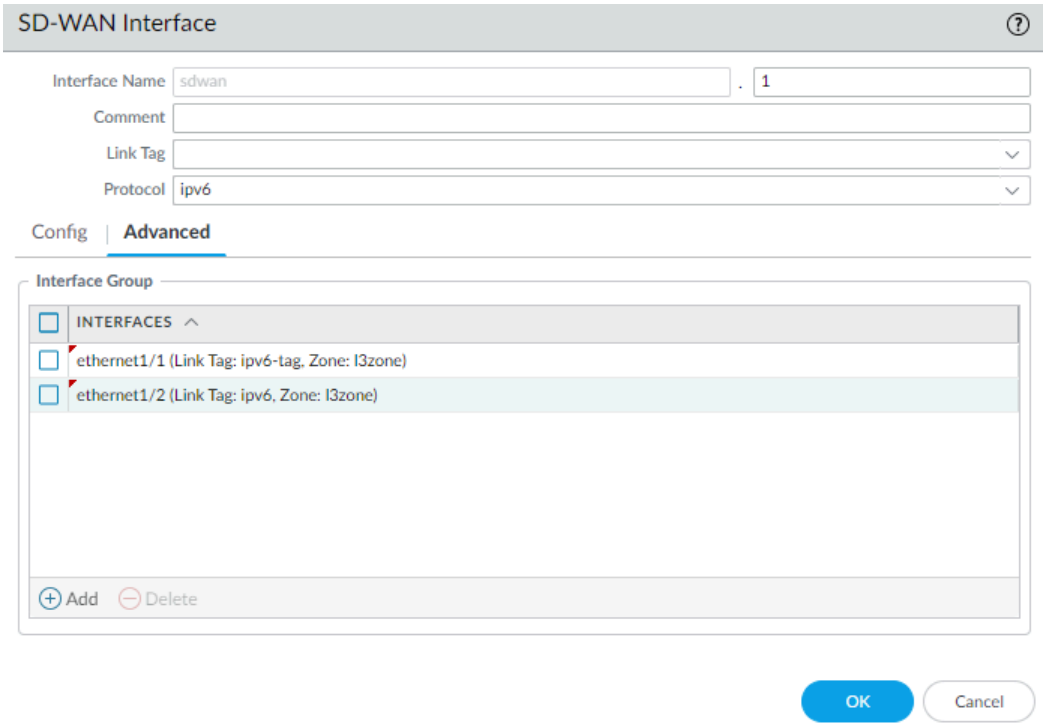
STEP 7 | 將 SD-WAN 介面指派給 **Security Zone**（安全性區域）。

虛擬 SD-WAN 介面及其所有介面成員必須在一個相同的安全性區域中，以確保將相同的安全性原則規則套用到從分支到相同目的地的所有路徑。

STEP 8 | 在 **Advanced**（進階）標籤上，透過選取一個或多個第三層乙太網路介面（對於 DIA）或者一個或多個虛擬 VPN 通道介面（對於中樞）來 **Add Interfaces**（新增介面），這些是前往相同目的地的成員。如果您輸入多個介面，它們必須是相同類型（VPN 通道或 DIA）。

防火牆虛擬路由器使用此虛擬 *SD-WAN* 介面將 *SD-WAN* 流量路由到一個 *DIA* 或中樞位置。在路由過程中，路由表根據封包中的目標 *IP* 位址確定封包將從哪個虛擬 *SD-WAN* 介面離開（輸出介面）。然後，封包匹配的 *SD-WAN* 原則規則中的 *SD-WAN* 路徑健康情況和流量散佈設定檔將確定要使用的路徑（以及路徑惡化時考慮新路徑的順序。）

STEP 9 | 按一下 **OK**（確定）儲存您的組態變更。



STEP 10 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

建立指向 SD-WAN 介面的預設路由

如果您使用服務路由來存取 Panorama™，則必須建立一個指向您所建立的 SD-WAN 介面的預設路由才可啟動防火牆。

自動 VPN 會針對 IPv4 DIA 建立名為 sdwan.901 的虛擬 SD-WAN 介面，並針對 IPv6 DIA 建立名為 sdwan.9016 的虛擬 SD-WAN 介面。其會針對 VPN 通道建立名為 sdwan.902 的虛擬 SD-WAN 介面。自動 VPN 也會建立自己的預設路由，而此路由使用 sdwan.901 (IPv4) 和 sdwan.9016 (IPv6) 介面作為其輸出介面，並且使用低度量，因此 sdwan.901 (IPv4) 介面和 sdwan.9016 (IPv6) 介面優先於您已建立的預設路由。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取您正在處理的 **Template**（範本）。

STEP 3 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器，如 **sdwan**。

STEP 4 | 選取 **Static Routes**（靜態路由）。

STEP 5 | 選取 **IPv4** 或 **IPv6**，然後依 **Name**（名稱）來 **Add**（新增）靜態路由。

STEP 6 | 針對 IPv4 **Destination**（目的地），輸入 0.0.0.0/0。針對 IPv6 **Destination**（目的地），輸入 ::/0。

STEP 7 | 針對輸出 **Interface**（介面），選取您所建立的其中一個邏輯 SD-WAN 介面以啟動防火牆。

您選取的輸出介面可以是除了 *sdwan.901*、*sdwan.902* 或 *sdwan.9016* 之外的任何邏輯 *SD-WAN* 介面。

STEP 8 | 對於 **Next Hop**（下一個躍點），選取 **None**（無）。

STEP 9 | 對於 **Metric**（指標），輸入一個大於 50 的值，這樣，該預設路由不會比 Auto VPN 使用低度量指標建立的預設路由更受偏好。

STEP 10 | 按一下 **OK**（確定）。

STEP 11 | 選取 **Commit**（提交）並 **Commit and Push**（提交和推送）組態變更。

STEP 12 | **Commit**（提交）您的變更。

STEP 13 | 對防火牆上使用服務路由存取 Panorama 的其他範本重複此工作。

設定 SD-WAN 連結管理設定檔

建立並設定路徑品質、SaaS 品質、流量散佈和錯誤更正設定檔以管理 SD-WAN 連結容錯移轉。

- 建立路徑品質設定檔
- 設定 SaaS 監控
- SD-WAN 流量散佈設定檔
- 建立流量散佈設定檔
- 建立錯誤更正設定檔

建立路徑品質設定檔

為每組業務關鍵和延遲敏感的應用程式、應用程式篩選器、應用程式群組、服務、服務物件和服務群組物件建立一個路徑品質設定檔，這些項目對延遲、抖動和封包遺失百分比有獨特的網路品質（健康情況）要求。應用程式和服務可以共用一個路徑品質設定檔。為每個參數指定最大閾值，超過該閾值防火牆將認為路徑已惡化到足以選取更好的路徑。

作為建立路徑品質設定檔的替代方案，您可以使用任何預先定義的路徑品質設定檔，如 **general-business**、**voip-video**、**file-sharing**、**audio-streaming**、**photo-video**和 **remote-access** 等。預先定義的設定檔設定用於最佳化設定檔名稱建議的應用程式和服務類型的延遲、抖動和封包遺失閾值。

Panorama 裝置群組的預先定義路徑品質設定檔基於 *Panorama* 範本的 *SD-WAN* 介面設定檔中的預設 ***Probe Frequency***（探查頻率）設定。如果您變更預設的「探查頻率」設定，則必須在路徑品質設定檔中為防火牆調整 ***Packet Loss***（封包遺失）百分比閾值，這些防火牆位於受在其中變更了介面設定檔的 *Panorama* 範本影響的裝置群組中。

防火牆將延遲、抖動和封包遺失閾值視為 OR 條件，這意味著如果超過任何一個閾值，防火牆都會選取新的最佳（偏好）路徑。延遲、抖動和封包遺失均小於或等於全部三個閾值的任何路徑均被視為合格，且防火牆會根據關聯的流量散佈設定檔選取路徑。

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

如果一條路徑因為超出設定的封包遺失閾值而容錯移轉，防火牆仍然會在故障的路徑上傳送探查封包並在路徑復原時計算其封包遺失百分比。復原路徑上的封包遺失百分比可能要花費大約三分鐘才能降至路徑品質設定檔中設定的封包遺失閾值以下。例如，假設應用程式的 SD-WAN 原則規則有一個路徑品質設定檔，其中指定封包遺失閾值為 1#，而流量散佈設定檔先後在清單上使用標籤 1（已套用至 tunnel.1）和標籤 2（已套用至 tunnel.2）指定自上而下的散佈。當 tunnel.1 超出 1% 的封包遺失時，資料封包容錯移轉到 tunnel.2。在 tunnel.1 復原到 0% 的封包遺失（基於探查封包）後，它可以花費三分鐘的時間讓監控到的 tunnel.1 的封包遺失率降至 1% 以下，然後，防火牆在此時重新選取 tunnel.1 作為最佳路徑。

敏感設定表示對於設定檔套用的應用程式，哪個參數（延遲、抖動或封包遺失）更為重要（偏好）。當防火牆評估連結品質時，它會先考慮一個具有 高設定的參數。例如，當防火牆比較兩個連結時，假設一個連結有 100 毫秒的延遲和 20 毫秒的抖動，而另一個連結有 300 毫秒的延遲和

10 毫秒的抖動。如果延遲的敏感度為高，則防火牆會選擇第一個連結。如果抖動的敏感度為高，則防火牆會選擇第二個連結。如果參數具有相同的敏感度（預設情況下參數設定為中等），防火牆會先評估封包遺失，然後評估延遲，最後評估抖動。

正如SD-WAN 流量散佈設定檔其概念所述，如果您將 Path Monitoring and Probe Frequency（路徑監控和探查頻率）保留為預設設定，新路徑選擇可在一秒內完成。如有變更，新路徑選擇將需要超過一秒鐘。要實現基於封包遺失的亞秒級容錯移轉，您必須將延遲敏感度設定為 **high**（高），並將延遲閾值設定為不超過 250 毫秒。

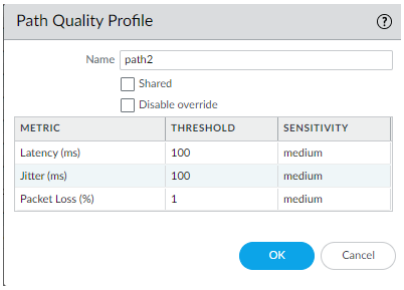
在 SD-WAN 原則規則中引用路徑品質設定檔，以控制防火牆在什麼時候使用新路徑為匹配的應用程式封包替換惡化的路徑。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Device Group**（裝置群組）。

STEP 3 | 選取 **Objects**（物件） > **SD-WAN Link Management**（SD-WAN 連結管理） > **Path Quality Profile**（路徑品質設定檔）。

STEP 4 | 使用一個最大包含 31 個字母數字字元的 **Name**（名稱）**Add**（新增）一個路徑品質設定檔。



STEP 5 | 對於 **Latency**（延遲），按兩下 **Threshold**（閾值）值，然後輸入在超出閾值之前，允許封包離開防火牆、到達 SD-WAN 通道的另一端，然後返回一個回應封包到防火牆可花費的毫秒數（範圍為 10 到 2,000；預設值為 100）。

STEP 6 | 對於 **Latency**（延遲），請選取 **Sensitivity**（敏感度）（低、中等或高）。預設為 中等。

按一下閾值欄末端的箭頭，將閾值將數字升序或降序排列。

STEP 7 | 對於 **Jitter**（抖動），按兩下 **Threshold**（閾值）值，然後輸入毫秒數（範圍為 10 到 1,000；預設值為 100）。

STEP 8 | 對於 **Jitter**（抖動），請選取 **Sensitivity**（敏感度）（低、中等或高）。預設為 中等。

STEP 9 | 對於 **Packet Loss**（封包遺失），按兩下 **Threshold**（閾值）值，並輸入超出閾值前連結上封包遺失的百分比（範圍為 1 到 100.0；預設值為 1）。

設定 ***Packet Loss***（封包遺失）的 ***Sensitivity***（敏感度）無效，因此保留預設設定。

如果您變更 *Panorama* 範本的 *SD-WAN* 介面設定檔的探測頻率，則還應調整 *Panorama* 裝置群組的封包遺失閾值。

STEP 10 | 按一下 **OK**（確定）。

STEP 11 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 12 | **Commit**（提交）您的變更。

STEP 13 | 為每一個裝置群組重複此工作。

設定 SaaS 監控

設定 SaaS 品質設定檔以監控 SaaS 應用程式與分支防火牆之間的直接網際網路存取 (DIA) 連結。

僅支援 *SD-WAN* 的 *PAN-OS* 防火牆支援 *SaaS* 應用程式路徑監控。*Prisma Access Hub* 不支援 *SaaS* 應用程式路徑監控。

- 建立 SaaS 品質設定檔
- 使用案例：為分支防火牆設定 SaaS 監控
- 使用案例：設定中樞防火牆容錯移轉以進行從分支防火牆到同一 SaaS 應用程式目的地的 SaaS 監控
- 使用案例：設定中樞防火牆容錯移轉以進行從分支防火牆到不同 SaaS 應用程式目的地的 SaaS 監控

建立 SaaS 品質設定檔

如果您的分支防火牆具有到軟體即服務 (SaaS) 應用程式的直接網際網路存取 (DIA) 連結，請建立一個 SaaS 品質設定檔以指定應如何監控一個或多個 SaaS 應用程式。SaaS 品質設定檔與 SD-WAN 原則規則相關聯，以確定分支防火牆確定延遲、抖動和封包遺失的路徑品質閾值以及為傳出封包選取偏好路徑的方式。

SaaS 品質設定檔最多支援四個靜態 IP 位址，或每個 SaaS 品質設定檔支援一個完全合格網域名稱 (FQDN) 或 URL。當設定多個靜態 IP 位址時，分支防火牆將根據 SaaS 品質設定檔中 IP 位址的排序方式，按級聯順序一次監控一個 IP 位址。例如，如果新增 IP1、IP2、IP3 和 IP4，則分支防火牆將監控 IP1，以確定是否已超過路徑品質閾值，然後繼續至 IP2，以此類推。

SD-WAN 監控和報告資料顯示 *SaaS* 應用程式和 *SaaS* 應用程式 *IP*、*FQDN* 或 *URL*，因為它當前在與 *SD-WAN* 原則規則關聯的 *SaaS* 品質設定檔中進行設定，與檢視 *SD-WAN* 監控資料時套用的時間篩選器無關。

例如，三天前，您在 *SaaS* 品質設定檔中將 *SaaS* 應用程式的 *IP* 位址初始設定為 ***192.168.10.50***，且流量符合與 *SaaS* 品質設定檔關聯的 *SD-WAN* 原則規則。現在，您重新設定了此現有 *SaaS* 品質設定檔，並將 *SaaS* 應用程式 *IP* 位址變更為 ***192.168.10.20***。當您檢閱 *SD-WAN* 監控資料時，此 *SaaS* 應用程式的所有現有監控資料都會顯示 *IP* 位址 ***192.168.10.20***。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **SaaS Quality Profile**（**SaaS** 品質設定檔），然後指定包含 SD-WAN 設定的 **Device Group**（裝置群組）。

STEP 3 | **Add**（新增）新的 SaaS 品質設定檔。

STEP 4 | 輸入 SaaS 品質設定檔的描述性 **Name**（名稱）。

STEP 5 | （選用）啟用（核取）**Shared**（共用）以使 SaaS 品質設定檔在所有裝置群組之間共用。

STEP 6 | （選用）啟用（核取）**Disable override**（停用覆寫），以停用覆寫本機防火牆上的 SaaS 品質設定檔設定。

只有在上一步中了停用 ***Shared***（共用），才能啟用 ***Disable override***（停用覆寫）。

STEP 7 | 設定 SaaS 監控模式。

- 自動監控 SaaS 應用程式路徑健康情況。

  Adaptive（適應性）監控依預設啟用，可讓分支防火牆被動地監控 SaaS 應用程式工作階段的傳送和接收活動，以確定是否已超過路徑品質閾值。SaaS 應用程式路徑健康情況品質是自動確定的，無需在 SD-WAN 介面上進行任何其他健康情況檢查。

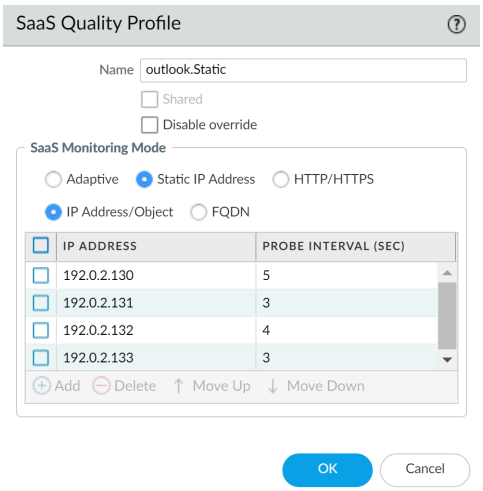
  僅 *TCP SaaS* 應用程式支援適應性 *SaaS* 監控。

- 設定 SaaS 應用程式的靜態 IP 位址。

  為每個需要監控的關鍵 *SaaS* 應用程式建立 *SaaS* 品質設定檔。如果 *SaaS* 應用程式具有多個 *IP* 位址，請為該 *SaaS* 應用程式設定具有多個靜態 *IP* 位址的 *SaaS* 品質設定檔。

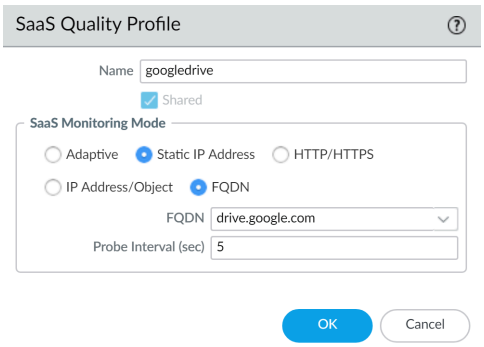
  SaaS 監控佔用大量資源，如果監控大量 *SaaS* 應用程式，可能會影響防火牆效能。最佳做法是僅監控那些需要良好可用性的業務關鍵型 *SaaS* 應用程式。

  1. 選取 **IP Address/Object**（**IP** 位址/物件） > **Static IP Address**（靜態 **IP** 位址），然後 **Add**（新增）一個 IP 位址。
  2. 輸入 SaaS 應用程式的 IP 位址，或選取設定的 address object（位址物件）。
  3. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
  4. 按一下 **OK**（確定）儲存組態變更。



- 設定 SaaS 應用程式的完全合格網域名稱 (FQDN)。

  1. 為 SaaS 應用程式設定 FQDN 位址物件。
  2. 選取 **IP Address/Object**（**IP** 位址/物件） > **FQDN**，然後 **Add**（新增）FQDN。
  3. 為 SaaS 應用程式選取 **FQDN** 位址物件。
  4. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
  5. 按一下 **OK**（確定）儲存組態變更。

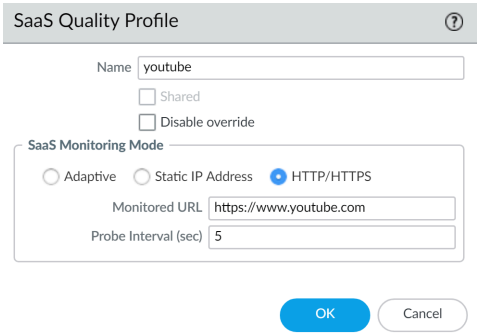


- 設定 SaaS 應用程式的 URL。

  僅連接埠 *80*、*443*、*8080*、*8081* 和 *143* 上的流量支援 *URL* 監控。

  1. 選取 **HTTP/HTTPS**。
  2. 輸入 SaaS 應用程式的 **Monitored URL**（受監控的 **URL**）。
  3. 輸入 **Probe Interval**（探查間隔），分支防火墻將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。

     SaaS 應用程式 HTTP/HTTPS 支援的最小探查間隔為 3 秒。
  4. 按一下 **OK**（確定）儲存組態變更。



STEP 8 | 選取 **Commit**（提交）並 **Commit and Push**（提交和推送）組態變更。

使用案例：為分支防火牆設定 SaaS 監控

如果您的組織在分支防火牆位置利用業務關鍵型 SaaS 應用程式，則可以設定 SaaS 品質設定檔並將其與 SD-WAN 原則規則關聯，以監控關鍵 SaaS 應用程式的延遲、抖動和封包遺失健康情況指標，並將 SD-WAN 分支防火牆中的連結交換為 SaaS 應用程式直接網際網路存取 (DIA) 連結，以確保應用程式的可用性。

如果超過了關鍵業務型 SaaS 應用程式 DIA 連結健康情況指標閾值，則該連結將針對所有新工作階段交換到流量散佈設定檔中設定的下一個 DIA 連結。降級的 DIA 連結上的現有工作階段不會交換到下一個 DIA 連結。

STEP 1 | 設定您的 SD-WAN 部署。

1. 安裝 SD-WAN 外掛程式。
2. 為 SD-WAN 設定 Panorama 和防火牆。
3. 新增 SD-WAN 裝置到 Panorama。
4. （僅限高可用性設定）為 SD-WAN 設定 HA 裝置。
5. 建立 VPN 叢集。

STEP 2 | 建立連結標籤 以分組 SaaS 應用程式 DIA 連結。

為您的 DIA 連結建立多個連結標籤，以便根據連結類型為每個 SaaS 應用程式 DIA 連結套用不同的 SD-WAN 監控設定。

此外，您還可以為多個 DIA 連結建立單個連結標籤，以將這些連結分組為單個連結組合。為多個 DIA 連結建立單個連結標籤可讓您彙總組合連結之間的頻寬，並允許防火牆在多個連結之間散佈工作階段。

STEP 3 | 設定 SD-WAN 介面設定檔，以定義 ISP 連線的特性並指定 DIA 連結的速度、分支防火牆監控連結的頻率，並選取連結標籤以指定 SD-WAN 介面設定檔套用至哪個連結。

如果建立了多個連結標籤，則必須為每個連結標籤設定一個 SD-WAN 介面設定檔。

如果您透過將多個 DIA 連結指派到單個連結標籤來建立連結組合，指定該連結標籤會將 SD-WAN 介面設定檔設定套用至組合中的所有 DIA 連結。

STEP 4 | 為每個 SaaS 應用程式 DIA 連結設定實體乙太網路介面。

DIA 連結的所有實體乙太網路介面必須為 *Layer3*。

STEP 5 | 設定虛擬 SD-WAN 介面 將 SaaS 應用程式 DIA 連結的所有實體乙太網路介面分組為一個介面群組。

防火牆虛擬路由器使用此虛擬 SD-WAN 介面將 SD-WAN 流量路由到一個 DIA 位置。然後，SD-WAN 原則規則中的 SD-WAN 路徑健康情況和流量散佈設定檔將確定要使用的路徑，以及路徑健康情況惡化時考慮新路徑的順序。

STEP 6 | 建立路徑品質設定檔，以設定延遲、抖動和封包遺失閾值以及靈敏度，以便指定分支防火牆何時應交換到下一個 DIA 連結。

STEP 7 | 建立 SaaS 品質設定檔，以指定 SaaS 應用程式以及監控 DIA 連結的頻率。

STEP 8 | 建立流量散佈設定檔，以指定在連結健康情況下降的情況下，分支防火牆交換到 DIA 連結的順序。

STEP 9 | 設定 SD-WAN 原則規則，以指定 SaaS 應用程式和連結健康情況指標，並確定防火牆如何為關鍵 SaaS 應用程式流量選取偏好連結。

在 ***Application***（應用程式）頁籤中，將監控的 *SaaS* 應用程式新增到 *SD-WAN* 原則規則中，以確保 *SaaS* 監控設定僅套用至所需的 *SaaS* 應用程式。

使用案例：設定中樞防火牆容錯移轉以進行從分支防火牆到同一 SaaS 應用程式目的地的 SaaS 監控

如果您的組織在分支防火牆位置利用 SaaS 應用程式，但分支防火牆沒有狀況良好 DIA 連結可供交換，則可以將中樞防火牆設定為容錯移轉替代方案，以維持與 SaaS 應用程式的正常連線。

如果超過了 SaaS 應用程式 DIA 連結健康情況指標閾值，且分支防火牆沒有狀況良好的 DIA 連結可用，則該連結將為所有新工作階段交換到下一個中樞防火牆。降級的 DIA 連結上的現有工作階段不會交換到該中樞防火牆。

例如，假設您的分支和中樞防火牆位於同一區域，並使用相同的目的地 IP 存取 SaaS 應用程式。您可透過在分支防火牆和中樞防火牆上設定名稱相同的 SaaS 品質設定檔，將中樞防火牆設定為在從分支防火牆到 SaaS 應用程式沒有正常 DIA 連結時充當容錯移轉裝置，以在分支防火牆沒有可用狀況良好的 DIA 連結可用時自動容錯移轉到中樞防火牆。這讓您可以為 SaaS 應用程式維護健康的路徑，並能夠維護準確的端對端 SaaS 應用程式監控資料，而不會擁塞網路頻寬。

STEP 1 | 設定您的 SD-WAN 部署。

1. 安裝 SD-WAN 外掛程式。
2. 為 SD-WAN 設定 Panorama 和防火牆。
3. 新增 SD-WAN 裝置到 Panorama。
4. （僅限高可用性設定）為 SD-WAN 設定 HA 裝置。
5. 建立 VPN 叢集。

STEP 2 | 建立連結標籤 以分組 SaaS 應用程式 DIA 連結。

為您的 DIA 連結建立多個連結標籤，以便根據連結類型為每個 SaaS 應用程式 DIA 連結套用不同的 SD-WAN 監控設定。

此外，您還可以為多個 DIA 連結建立單個連結標籤，以將這些連結分組為單個連結組合。

STEP 3 | 設定 SD-WAN 介面設定檔，以定義 ISP 連線的特性並指定 DIA 連結的速度、分支防火牆監控連結的頻率，並選取連結標籤以指定 SD-WAN 介面設定檔套用至哪個連結。

如果建立了多個連結標籤，則必須為每個連結標籤設定一個 SD-WAN 介面設定檔。

如果您透過將多個 DIA 連結指派到單個連結標籤來建立連結組合，指定該連結標籤會將 SD-WAN 介面設定檔設定套用至組合中的所有 DIA 連結。

STEP 4 | 為每個 SaaS 應用程式 DIA 連結設定實體乙太網路介面。

DIA 連結的所有實體乙太網路介面必須為 *Layer3*。

STEP 5 | 設定虛擬 SD-WAN 介面 將 SaaS 應用程式 DIA 連結的所有實體乙太網路介面分組為一個介面群組。

防火牆虛擬路由器使用此虛擬 SD-WAN 介面將 SD-WAN 流量路由到一個 DIA 位置。然後，SD-WAN 原則規則中的 SD-WAN 路徑健康情況和流量散佈設定檔將確定要使用的路徑，以及路徑健康情況惡化時考慮新路徑的順序。

STEP 6 | 為中樞和分支防火牆建立名稱相同的 SaaS 品質設定檔。

必須在中樞和分支防火牆上設定兩個名稱相同的 SaaS 品質設定檔，才能成功利用中樞防火牆作為備用容錯移轉。實現這一點的最簡單方法是在共用裝置群組中建立單個 SaaS 品質設定檔。或

者，您可以在不同的裝置群組中建立兩個名稱相同的 SaaS 品質設定檔，並將它們推送到中樞和分支防火牆。

1. 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **SaaS Quality Profile**（**SaaS** 品質設定檔），然後從「裝置群組」下拉式清單中選取 **Shared**（共用）。
2. **Add**（新增）新的 SaaS 品質設定檔。
3. 輸入 SaaS 品質設定檔的描述性 **Name**（名稱）。
4. 啟用（核取）**Shared**（共用）以使 SaaS 品質設定檔在所有裝置群組之間共用。

   要使 SaaS 品質設定檔可用於分支和中樞防火牆所屬的所有裝置群組，必須執行此操作。
5. 啟用（核取）**Disable override**（停用覆寫），以停用覆寫本機防火牆上的 SaaS 品質設定檔設定。
6. 使用以下方法之一設定 SaaS 監控模式。
   - 設定 SaaS 應用程式的靜態 IP 位址。

     為每個 *SaaS* 應用程式建立一個 *SaaS* 品質設定檔。如果 *SaaS* 應用程式具有多個 *IP* 位址，請為該 *SaaS* 應用程式設定具有多個靜態 *IP* 位址的 *SaaS* 品質設定檔。

     1. 選取 **IP Address/Object**（**IP** 位址/物件） > **Static IP Address**（靜態 **IP** 位址），然後 **Add**（新增）一個 IP 位址。
     2. 輸入 SaaS 應用程式的 IP 位址，或選取設定的 address object（位址物件）。
     3. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     4. 按一下 **OK**（確定）儲存組態變更。
   - 設定 SaaS 應用程式的完全合格網域名稱 (FQDN)。
     1. 為 SaaS 應用程式設定 FQDN 位址物件。
     2. 選取 **IP Address/Object**（**IP** 位址/物件） > **FQDN**，然後 **Add**（新增）FQDN。
     3. 為 SaaS 應用程式選取 **FQDN** 位址物件。
     4. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     5. 按一下 **OK**（確定）儲存組態變更。
   - 設定 SaaS 應用程式的 URL。

     僅連接埠 *80*、*443*、*8080*、*8081* 和 *143* 上的流量支援 *URL* 監控。

     1. 選取 **HTTP/HTTPS**。
     2. 輸入 SaaS 應用程式的 **Monitored URL**（受監控的 **URL**）。
     3. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     4. 按一下 **OK**（確定）儲存組態變更。

STEP 7 | 建立流量散佈設定檔，以指定在連結健康情況下降的情況下，分支防火牆從 DIA 連結交換到中樞防火牆 VPN 連結的順序。

STEP 8 | 設定 SD-WAN 原則規則，以指定 SaaS 應用程式和連結健康情況指標，並確定防火牆如何為關鍵 SaaS 應用程式流量選取偏好連結。

在 ***Application***（應用程式）頁籤中，將監控的 *SaaS* 應用程式新增到 *SD-WAN* 原則規則中，以確保 *SaaS* 監控設定僅套用至所需的 *SaaS* 應用程式。

使用案例：設定中樞防火牆容錯移轉以進行從分支防火牆到不同 SaaS 應用程式目的地的 SaaS 監控

如果您的組織在分支防火牆位置利用 SaaS 應用程式，但分支防火牆沒有狀況良好的 DIA 連結可供交換，則可以將中樞防火牆設定為容錯移轉替代方案，以使用指向其他 SaaS 目的地的 SaaS 品質設定檔來維持與 SaaS 應用程式的正常連線。

如果超過了 SaaS 應用程式 DIA 連結健康情況指標閾值，且分支防火牆沒有狀況良好的 DIA 連結可用，則該連結將為所有新工作階段交換到下一個中樞防火牆。降級的 DIA 連結上的現有工作階段不會交換到該中樞防火牆。

例如，假設您的分支和中樞防火牆位於國家的相反端，且可以存取部署在雲端提供者（例如 GCP）中的 SaaS 雲端應用程式。您可以將中樞防火牆設定為在分支防火牆到 SaaS 應用程式之間沒有正常 DIA 連結的情況下充當容錯移轉裝置。為此，請同時在分支防火牆和中樞防火牆上設定一個名稱相同的 SaaS 品質設定檔，以在分支防火牆沒有可用的正常 DIA 連結時自動容錯移轉到中樞防火牆。在中樞防火牆上設定的 SaaS 品質設定檔以指向最靠近中樞的入口位置，以利用最接近中樞的本機資源。這讓您可以靈活地指定狀況良好的容錯移轉路徑，並能夠維護準確的端對端 SaaS 應用程式監控資料，而不會擁塞網路頻寬。

STEP 1 | 設定您的 SD-WAN 部署。

1. 安裝 SD-WAN 外掛程式。
2. 為 SD-WAN 設定 Panorama 和防火牆。
3. 新增 SD-WAN 裝置到 Panorama。
4. （僅限高可用性設定）為 SD-WAN 設定 HA 裝置。
5. 建立 VPN 叢集。

STEP 2 | 建立連結標籤 以分組 SaaS 應用程式 DIA 連結。

為您的 DIA 連結建立多個連結標籤，以便根據連結類型為每個 SaaS 應用程式 DIA 連結套用不同的 SD-WAN 監控設定。

此外，您還可以為多個 DIA 連結建立單個連結標籤，以將這些連結分組為單個連結組合。

STEP 3 | 設定 SD-WAN 介面設定檔，以定義 ISP 連線的特性並指定 DIA 連結的速度、分支防火牆監控連結的頻率，並選取連結標籤以指定 SD-WAN 介面設定檔套用至哪個連結。

如果建立了多個連結標籤，則必須為每個連結標籤設定一個 SD-WAN 介面設定檔。

如果您透過將多個 DIA 連結指派到單個連結標籤來建立連結組合，指定該連結標籤會將 SD-WAN 介面設定檔設定套用至組合中的所有 DIA 連結。

STEP 4 | 為每個 SaaS 應用程式 DIA 連結設定實體乙太網路介面。

DIA 連結的所有實體乙太網路介面必須為 *Layer3*。

STEP 5 | 設定虛擬 SD-WAN 介面 將 SaaS 應用程式 DIA 連結的所有實體乙太網路介面分組為一個介面群組。

防火牆虛擬路由器使用此虛擬 SD-WAN 介面將 SD-WAN 流量路由到一個 DIA 位置。然後，SD-WAN 原則規則中的 SD-WAN 路徑健康情況和流量散佈設定檔將確定要使用的路徑，以及路徑健康情況惡化時考慮新路徑的順序。

STEP 6 | 為中樞和分支防火牆建立名稱相同的 SaaS 品質設定檔。

必須在中樞和分支防火牆上設定兩個名稱相同的 SaaS 品質設定檔，才能成功利用中樞防火牆作為備用容錯移轉。建立兩個具有相同名稱的 SaaS 品質設定檔，每個設定檔均指向不同裝置群組中的不同 SaaS 應用程式目的地，並將它們推送到中樞和分支防火牆。

1. 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **SaaS Quality Profile**（**SaaS** 品質設定檔），然後從「裝置群組」下拉式清單中選取包含分支防火牆的目標裝置群組。
2. **Add**（新增）新的 SaaS 品質設定檔。
3. 輸入 SaaS 品質設定檔的描述性 **Name**（名稱）。
4. 啟用（核取）**Disable override**（停用覆寫），以停用覆寫本機防火牆上的 SaaS 品質設定檔設定。
5. 使用以下方法之一設定 SaaS 監控模式。
   - 設定 SaaS 應用程式的靜態 IP 位址。

     為每個 *SaaS* 應用程式建立一個 *SaaS* 品質設定檔。如果 *SaaS* 應用程式具有多個 *IP* 位址，請為該 *SaaS* 應用程式設定具有多個靜態 *IP* 位址的 *SaaS* 品質設定檔。

     1. 選取 **IP Address/Object**（**IP** 位址/物件） > **Static IP Address**（靜態 **IP** 位址），然後 **Add**（新增）一個 IP 位址。
     2. 輸入 SaaS 應用程式的 IP 位址，或選取設定的 address object（位址物件）。
     3. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     4. 按一下 **OK**（確定）儲存組態變更。
   - 設定 SaaS 應用程式的完全合格網域名稱 (FQDN)。
     1. 為 SaaS 應用程式設定 FQDN 位址物件。
     2. 選取 **IP Address/Object**（**IP** 位址/物件） > **FQDN**，然後 **Add**（新增）FQDN。
     3. 為 SaaS 應用程式選取 **FQDN** 位址物件。
     4. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     5. 按一下 **OK**（確定）儲存組態變更。
   - 設定 SaaS 應用程式的 URL。

     僅連接埠 *80*、*443*、*8080*、*8081* 和 *143* 上的流量支援 *URL* 監控。

     1. 選取 **HTTP/HTTPS**。
     2. 輸入 SaaS 應用程式的 **Monitored URL**（受監控的 **URL**）。
     3. 輸入 **Probe Interval**（探查間隔），分支防火牆將按照此間隔探查 SaaS 應用程式路徑的健康情況資訊。
     4. 按一下 **OK**（確定）儲存組態變更。

6. 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **SaaS Quality Profile**（**SaaS** 品質設定檔），然後從「裝置群組」下拉式清單中選取包含中樞防火牆的目標裝置群組。
7. 重複步驟 6.2 到 6.5，以在不同的目的地為 SaaS 應用程式建立名稱相同的 SaaS 品質設定檔。

   若要在中樞防火牆所屬的裝置群組中建立名稱相同的 SaaS 品質設定檔，則需要執行此步驟。

STEP 7 | 建立流量散佈設定檔，以指定在連結健康情況下降的情況下，分支防火牆從 DIA 連結交換到中樞防火牆 VPN 連結的順序。

STEP 8 | 設定 SD-WAN 原則規則，以指定 SaaS 應用程式和連結健康情況指標，並確定防火牆如何為關鍵 SaaS 應用程式流量選取偏好連結。

在 ***Application***（應用程式）頁籤中，將監控的 *SaaS* 應用程式新增到 *SD-WAN* 原則規則中，以確保 *SaaS* 監控設定僅套用至所需的 *SaaS* 應用程式。

SD-WAN 流量散佈設定檔

在 SD-WAN 拓撲中，防火牆會對每一個應用程式偵測暫時低壓、斷電和路徑惡化，並選取新的路徑，以確保重要業務應用程式能提供最佳效能。擁有多個 ISP 連結可讓您擴展流量容量並減少成本。如果您將 Path Monitoring and Probe Frequency（路徑監控和探查頻率）保留為預設設定，新路徑選擇可在一秒內完成。如有變更，新路徑選擇將需要超過一秒鐘。

為實作此路徑選擇，防火牆會使用 SD-WAN 原則規則，該規則引用一個流量散佈設定檔，其中指定了如何為工作階段載入散佈選取路徑，以及如何在應用程式的路徑品質惡化且需要容錯移轉到新路徑的情況下選取路徑。

確定應用程式或服務（匹配 SD-WAN 原則規則）應使用哪種流量散佈方法：

- **Best Available Path**（最佳可用路徑）—如果成本不是因素之一，請選取此路徑，您將允許應用程式使用分支之外的任何路徑。防火牆使用路徑品質指標來散佈流量以及容錯移轉到屬於清單中某個連結標籤的一個連結，從而為使用者提供最佳應用程式體驗。
- **Top-Down Priority**（自上而下優先順序）—如果您有一些昂貴或低容量連結，只想將其用作最後手段或者備份連結，則可以使用「自上而下優先順序」方法，並將包含這些連結的標籤放在設定檔中連結標籤清單的最後位置。防火牆會先使用清單最上面的連結標籤來確定工作階段載入流量的連結和容錯移轉的連結。如果根據路徑品質設定檔，第一個連結標籤中的所有連結均不合格，防火牆會從清單的第二個連結標籤中選取一個連結。如果第二個連結標籤中的所有連結均不合格，該程序會視需要繼續，直到在最後一個連結標籤中找到合格的連結。如果所有關聯連結均超載，且沒有滿足品質閾值的連結，防火牆會使用「最佳可用路徑」方法來選取轉送流量的連結。在容錯移轉事件開始時，防火牆會從連結標籤的「自上而下優先順序」清單的最上面開始，查找要進行容錯移轉的連結。
- **Weighted Session Distribution**（加權工作階段散佈）—如果您想要手動載入（匹配規則的）流量到 ISP 和 WAN 連結，且在暫時低壓情況下不需要容錯移轉，請選取此方法。當套用新工作階段（使用單個連結標籤分組的介面將獲得這些工作階段）的靜態百分比時，可以手動指定連結的載入。防火牆使用循環配置方式在具有指定連結標籤的連結之間散佈新工作階段，直到指派了最低百分比的連結達到該工作階段百分比。然後，防火牆以相同方式使用剩餘的連結。對

於對延遲不敏感的應用程式和需要大量連結頻寬容量（如大型分支備份和大型檔案移轉）的應用程式，可以選取此方法。

如果連結出現暫時低壓，防火牆不會將相符流量重新導向到其他連結。

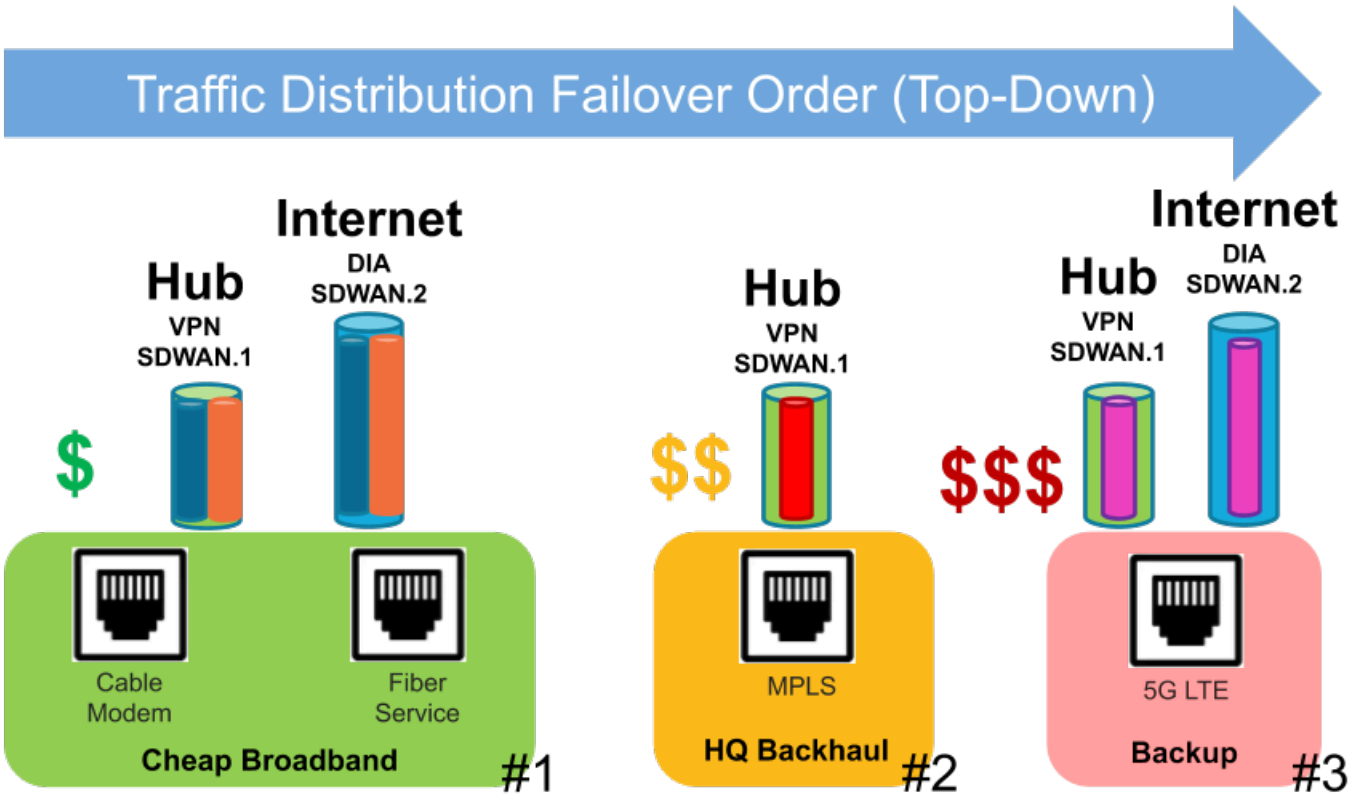
如果路徑出現故障，則您在 SD-WAN 原則規則中為應用程式選擇的流量散佈方法，將和連結群組上的連結標籤一起，確定防火牆是否要選取新的路徑（執行連結容錯移轉）以及如何選取新路徑，如下所示：

路徑情況	自上而下優先順序	最佳可用路徑	加權工作階段散佈
超出路徑健康情況閾值（暫時低壓）的現有路徑上的工作階段	受影響工作階段容錯移轉到更佳路徑（如果可用）	受影響工作階段容錯移轉到更佳路徑（如果可用）	受影響的工作階段不容錯移轉
自上而下或最佳可用路徑復原：現有路徑仍然合格（良好）	受影響的工作階段容錯回復到之前的路徑	受影響的工作階段停留在現有路徑上，不會容錯回復	受影響的工作階段不容錯移轉
自上而下或最佳可用路徑復原：現有路徑未能通過健康情況檢查	所有工作階段容錯回復到之前的路徑	選取的工作階段容錯回復到之前的路徑，直到受影響的現有路徑復原	受影響的工作階段不容錯移轉
現有路徑斷開（斷電）	所有工作階段容錯移轉到清單上的下一條路徑	所有工作階段容錯移轉到下一條最佳路徑	所有工作階段基於權重設定容錯移轉到其他標籤
暫時低壓且沒有合格（更好）的路徑	採用最佳可用路徑	採用最佳可用路徑	採用最佳可用路徑

此外，防火牆在單個連結標籤的介面成員之間自動執行工作階段載入共用。在這些介面接近它們的最大 Mbps 後，如果具有另一個連結標籤的介面具有更好的健康情況指標，新工作階段將流動到這些介面（基於流量散佈方法）。

路徑情況	自上而下優先順序	最佳可用路徑	加權工作階段散佈
具有相同 SD-WAN 標籤的多個連結	在 SD-WAN 標籤內的所有連結上平均共用工作階段載入	基於 SD-WAN 標籤內的最佳路徑共用工作階段載入	基於指派到 SD-WAN 標籤的權重百分比共用工作階段載入
具有不同 SD-WAN 標籤的多個連結	基於清單優先順序共用工作階段載入，先載入第一個 SD-WAN 標籤中的連結。	基於所有 SD-WAN 標籤的最佳路徑共用工作階段載入	基於指派到 SD-WAN 標籤的權重百分比共用工作階段載入

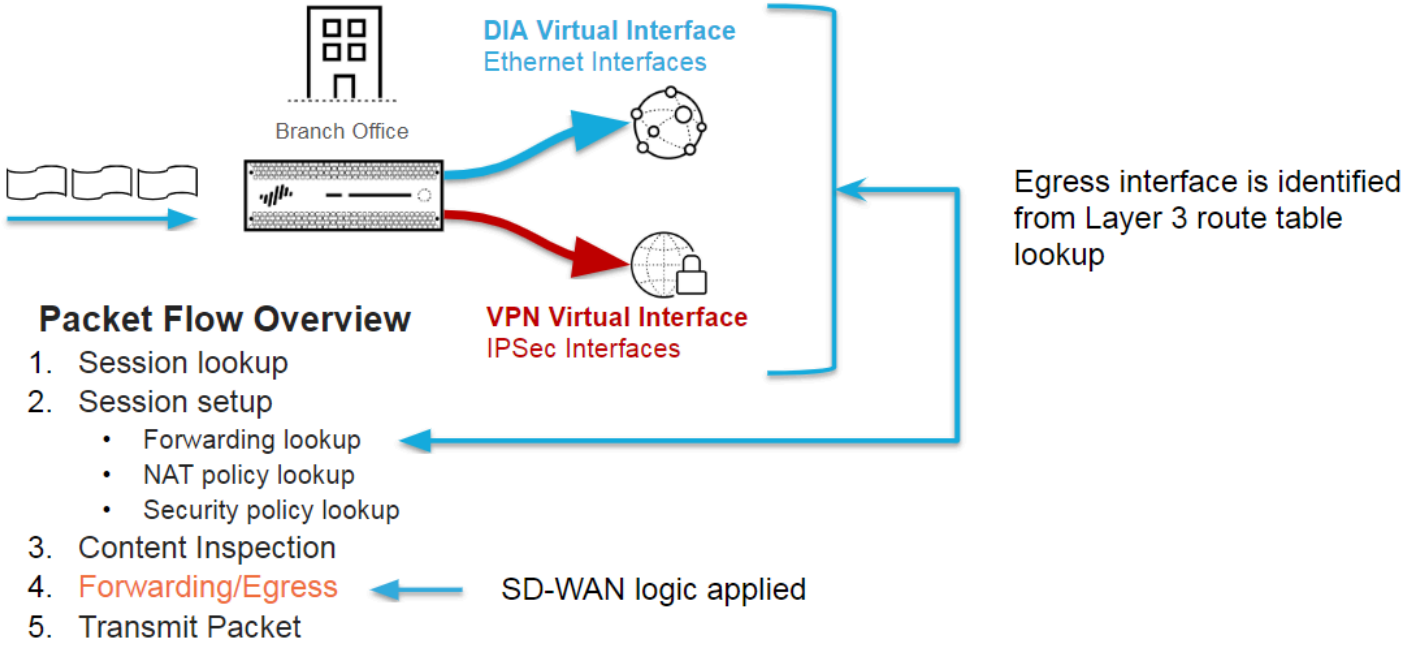
下圖展示了一個使用「自上而下優先順序」方法的流量散佈設定檔的範例。#1、#2 和 #3 是防火牆檢查連結的連結標籤的順序，如有必要，會按此順序查找健康的路徑以完成應用程式工作階段容錯移轉。對於發生的每個單獨的容錯移轉事件，防火牆都從連結標籤的自上而下清單的最上面開始。



1. 在這個「自上而下優先順序」範例中，來自分支的封包搭載一個特定的應用程式（例如 office365-enterprise-access）到達防火牆。防火牆使用路由表來判斷到目的地和傳出介面的下一個躍點，即名為 sdwan.901 的虛擬 SD-WAN 介面通道。安全性原則規則允許封包。然後，封包匹配為中樞指定目的地區域的一條 SD-WAN 原則規則（名為 Office365 to Hub1）。防火牆使用 SD-WAN 政策規則的路徑品質設定檔、流量散佈設定檔和該設定檔的連結標籤來確定要使用來自 sdwan.901 的介面成員（連結）。流量散佈設定檔按以下順序列出了三個連結標籤：#1 便宜寬頻、#2 HQ 回程和 #3 備份（防火牆在查找可進行容錯移轉的連結時會根據此連結標籤順序檢查連結）。
2. 假設所有路徑均合格（根據路徑品質設定檔），防火牆將封包散佈到標記有流量散佈設定檔清單中第一個連結標籤的實體連結：便宜寬頻。sdwan.901 通道有兩個成員介面（兩個載波）：纜線數據機 VPN 通道和光纖服務 VPN 通道。防火牆先按照循環配置方式檢查一個連結，然後選擇它找到的第一個合格連結，例如，纜線數據機連結。
3. 如果第一個「便宜寬頻」連結（纜線數據機）不是合格的連結，則防火牆會選取第二個「便宜寬頻」連結（光纖服務）。
4. 如果第二個便宜寬頻連結（光纖服務）不是合格的連結，防火牆會選取標記有第二個連結標籤「HQ 回程」的連結，這是一個指向相同中樞但更昂貴的 MPLS 連結。

5. 如果 MPLS 連結不是合格的連結，防火牆會選取標記有第三個連結標籤「備份」的連結，這是一個指向相同中樞但更加昂貴的 5G LTE 連結。
6. 如果防火牆沒有找到可進行容錯移轉的合格連結，則會使用「最佳可用」方法來選取一個連結。
7. 在新容錯移轉事件開始時，防火牆會從連結標籤的「自上而下」清單的最上面開始，查找將進行容錯移轉的連結。

請記住，SD-WAN 流量散佈是封包流程邏輯的最後步驟之一。讓我們縮小以檢視封包流動的更大範圍檢視。

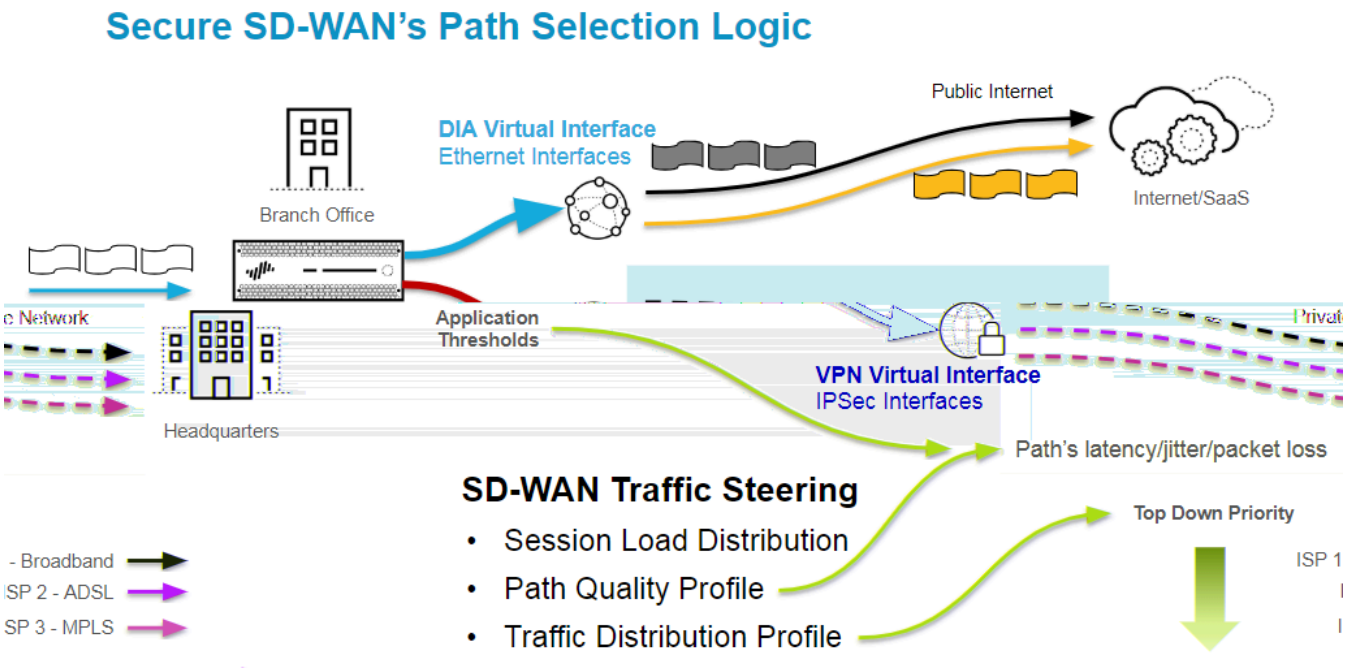


圖中的封包流動詳細資料如下所示：

1. 當一個應用程式的一個工作階段達到防火牆時，防火牆執行工作階段查閱以確定該工作階段是現有工作階段還是新工作階段。
2. 新工作階段會經過工作階段設定：
    1. 轉送查閱—防火牆從第三層路由表或第二層轉送資料庫查閱等獲取輸出區域、輸出介面和虛擬系統。對於匹配 SD-WAN 原則規則的應用程式，防火牆會使用虛擬 SD-WAN 介面作為輸出介面。
    2. NAT 原則查閱—如果工作階段匹配一條 NAT 規則，防火牆會進行另一個轉送查閱來確定最終（轉譯的）輸出介面和區域。
    3. 安全性原則查閱—如果一條安全性原則規則允許該工作階段，則會建立該工作階段並將其安裝在工作階段表中。然後，防火牆會使用 App-ID™ 和 User-ID™ 執行額外的分類。
3. 內容檢查—防火牆會視需要在有效負載和標頭上執行「威脅檢查」（用於 IPS 的反間諜軟體[弱點保護]、防毒、URL 篩選、WildFire® 等）。

4. 「轉送/輸出」階段會執行路徑選擇並轉送封包。在此階段中，會進行 SD-WAN 路徑選擇。
   1. 封包轉送程序—防火牆使用輸出介面來確定轉送網域；執行路由、切換或虛擬介接轉送。
   2. 當應用程式匹配一條 SD-WAN 原則規則時，會進行 SD-WAN 路徑選擇；路徑品質設定檔確定路徑資格；流量散佈設定檔確定路徑選擇的方法以及在選擇期間考慮路徑的順序。
   3. 如有需要，會進行 IPSec/SSL-VPN 通道加密。
   4. 封包輸出程序 - 套用 QoS 成形、DSCP 重寫和 IP 分散（視需要）。
5. 傳輸封包—防火牆透過所選的輸出介面轉送封包。

現在，我們放大來更詳細地查看 SD-WAN 路徑選擇邏輯。



1. 防火牆在轉送查閱期間咨詢路由表；基於匹配一個第三層前置詞的目的地 IP 位址，防火牆確定輸出 SD-WAN 虛擬介面。封包直接前往共用網際網路，或透過一個安全的 VPN 連結返回到中樞。
2. 防火牆透過在 VPN 通道上執行健康情況檢查來監控每條路徑。每個 DIA 環道都有一個監控健康情況資訊的 VPN 通道。
3. SD-WAN 原則規則中的應用程式與一個路徑品質設定檔關聯，防火牆將路徑的實際延遲、抖動和封包遺失平均值與閾值進行比較。
4. 將不會選取延遲、抖動或封包遺失值高於閾值的任何路徑。
5. 然後，SD-WAN 介面中的所有合格路徑都遵從流量散佈設定檔的方法和路徑優先順序（排序）邏輯。SD-WAN 連結標籤會將 ISP 服務分組在一起，這些標籤在流量散佈設定檔中的順序即為路徑選擇期間路徑的優先順序。
6. 這樣，路徑品質設定檔和流量散佈設定檔共同確定要使用的下一條最佳路徑，然後防火牆將流量轉送到該路徑。

建立流量散佈設定檔

基於您的 SD-WAN 設定計劃，根據您希望 SD-WAN 政策規則中的應用程式進行工作階段載入和容錯移轉的方式來建立所需的 SD-WAN 流量散佈設定檔。

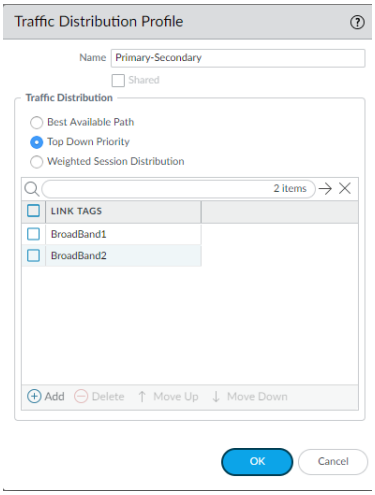
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 確保您已在 SD-WAN 介面設定檔中設定連結標籤，且已提交並推送它們。必須將連結標籤推送到您的中樞和分支，以便 Panorama™ 能成功將您在此流量散佈設定檔中指定的連結標籤關聯到 SD-WAN 介面設定檔。

STEP 3 | 選取 **Device Group**（裝置群組）。

STEP 4 | 建立流量散佈設定檔。

1. 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **Traffic Distribution Profile**（流量散佈設定檔）。
2. 使用一個最大包含 31 個字母數字字元的 **Name**（名稱）**Add**（新增）一個流量散佈設定檔。



3. 僅當您想在所有裝置群組（包括中樞和分支）中使用此流量散佈設定檔時才選取 **Shared**（共用）。
4. 選取一種流量散佈方式，並為該設定檔新增最多四個使用此方式的連結標籤。
   - **Best Available Path**（最佳可用路徑）—**Add**（新增）一個或多個 **Link Tags**（連結標籤）。在初始封包交換期間，在 App-ID 對封包中的應用程式進行分類之前，防火牆會使用標籤中具有最佳健康情況指標的路徑（基於標籤的順序）。在防火牆識別應用程式之後，它會將正在使用的路徑的健康情況（路徑品質）與第一個連結標籤中第一個路徑（介面）的健康情況進行比較。如果原始路徑的健康情況更好，它將保留為所選

路徑；否則，防火牆將替換原始路徑。防火牆會重複此程序，直到評估完連結標籤中的所有路徑。最終路徑是當封包到達時防火牆選取的滿足比對規則的路徑。

當連結變得不合格且必須容錯移轉到下一條最佳路徑時，防火牆每分鐘可將最多 *1000* 個工作階段從不合格的連結移轉到下一條最佳路徑。例如，假設 *tunnel.901* 有 *3,000* 個工作階段；其中 *2,000* 個工作階段符合 *SD-WAN* 原則規則 *A*，*1,000* 個工作階段符合 *SD-WAN* 原則規則 *B*（兩條規則都有設定了 ***Best Path Available***（最佳可用路徑）的流量散佈原則）。如果 *tunnel.901* 變得不合格，它會花費三分鐘的時間將 *3,000* 個工作階段從不合格的連結移轉到下一條最佳路徑。

- **Top Down Priority**（自上而下優先順序）—**Add**（新增）一個或多個 **Link Tags**（連結標籤）。防火牆按自上而下的順序使用您新增的 **Link Tags**（連結標籤）將（符合比對規則的）新工作階段散佈到連結。防火牆會檢查為此設定檔設定的第一個標籤，並檢查使用該標籤的路徑，選取它找到的第一個合格路徑（即位於或低於此規則的路徑品質閾值）。如果從該連結標籤沒有找到合格的路徑，防火牆會檢查使用下一個連結標籤的路徑。如果防火牆在檢查完所有連結標籤中的所有路徑後都沒有找到合格路徑，防火牆會使用 **Best Available Path**（最佳可用路徑）方法。選取的第一條路徑是偏好路徑，直到該路徑的一個路徑品質值超出閾值，此時防火牆會重新從連結標籤清單的頂部開始查找新的偏好路徑。

  如果中樞只有一個連結，則該連結支援所有虛擬介面和 *DIA* 流量。如果您想要以特定順序使用連結類型，則必須將流量散佈設定檔套用至指定自上而下優先順序的中樞，然後排序連結標籤以指定偏好的順序。如果您套用指定最佳可用路徑的流量散佈設定檔，防火牆將使用連結（不論成本如何），選擇表現最佳的分支路徑。總而言之，流量散佈設定檔中的連結標籤，連結標籤已套用至中樞虛擬介面，且 *SD-WAN* 介面設定檔中的***VPN Failover Metric***（*VPN* 容錯移轉指標）僅當流量散佈設定檔指定***Top Down Priority***（自上而下優先順序）時才能運作。

- **Weighted Session Distribution**（加權工作階段散佈）—**Add**（新增）一個或多個 **Link Tags**（連結標籤），然後輸入每個 **Link Tag**（連結標籤）的 **Weight**（權重）百分比，權重總數為 100%。防火牆在連結標籤間執行工作階段載入散佈，直到達到百分比最大值。如果連結標籤中有多條路徑，防火牆會使用循環配置進行平均散佈，直到達到路徑健康情況指標，然後將工作階段散佈到未達到限制的其他成員。

如果多個實體介面具有相同標籤，防火牆將在它們之間平均地散佈相符的工作階段。如果所有路徑都不符合健康情況（路徑品質）閾值，防火牆或選取具有最佳健康情況統計資料的路徑。如果沒有可用的 *SD-WAN* 連結（可能由於斷電），防火牆會使用靜態或動態路由來路由相符的封包。

如果封包應路由到虛擬 *SD-WAN* 介面，但是防火牆根據 *SD-WAN* 原則的流量散佈設定檔無法為工作階段找到偏好路徑，防火牆將隱含使用「最佳可用路徑」方法來查找偏好路徑。防火牆根據防火牆的隱含最終規則來散佈不符合 *SD-WAN* 原則規則的任何應用程式工作階段，也就是無視流量散佈設定檔，以循環配置方式將工作階段散佈給所有可用連結。

如果您想要控制防火牆散佈不匹配的工作階段的方式，請建立最終全部擷取規則，按您指定的順序 散佈不匹配的工作階段 到特定連結。

5. （選用）在新增連結標籤後，使用 **Move Up**（向上移動）或 **Move Down**（向下移動）箭頭變更清單中標籤的順序，以便它們反應您希望防火牆為此設定檔和 SD-WAN 原則規則中的所選應用程式使用連結的順序。
6. 按一下 **OK**（確定）。

STEP 5 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 6 | **Commit**（提交）您的變更。

建立錯誤更正設定檔

正向錯誤更正 (FEC) 是一種錯誤更正方法，透過更正嘈雜的通訊線路上發生的某些資料傳輸錯誤，無需重新傳輸即可提高資料可靠性。FEC 對於對封包遺失或損壞敏感的應用程式（如音訊、VoIP 和視訊會議）很有幫助。使用 FEC，接收防火牆可透過使用傳送編碼器嵌入應用程式流中的同位檢查位元，來復原遺失或損毀的封包。修復流後，SD-WAN 資料便無需容錯移轉到另一個路徑，TCP 也無需重新傳送封包。FEC 還可以透過復原遺失或損壞的封包來幫助 UDP 應用程式，因為 UDP 不會重新傳輸封包。

SD-WAN FEC 支援作為編碼器和解碼器的分支和中樞防火牆。FEC 機制使編碼器將備援位元新增到位元串流，且解碼器在必要時使用該資訊修正接收到的資料，然後再將其傳送到目的地。

SD-WAN 還支援將封包複製作為錯誤更正的替代方法。封包複製可以將應用程式工作階段從一個通道完全複製到第二個通道。封包複製比 FEC 需要更多的資源，應當僅用於對丟棄封包容忍度較低的關鍵應用程式。

具有自己的嵌入式復原機制的現代應用程式可能不需要 *FEC* 或封包複製。僅將 *FEC* 或封包複製套用至真正可從這種機制中獲益的應用程式；否則，將引入很多額外的頻寬和 *CPU* 開銷，而沒有任何益處。如果您的 *SD-WAN* 問題是擁塞，則 *FEC* 和封包複製都無濟於事。

FEC 和封包複製功能要求 Panorama 執行 PAN-OS 10.0.2 或更高版本，以及與 PAN-OS 版本相容的 SD-WAN 外掛程式 2.0 或更高版本。編碼器和解碼器必須都執行 PAN OS 10.0.2 或更高版本。如果一個分支或中樞執行的是比所需版本更舊的軟體，則帶有 FEC 或封包複製標頭的流量將在該防火牆上被丟棄。

從 PAN-OS 10.0.3 開始，除了已經支援的中樞-支點拓撲之外，完整網狀拓撲還支援 FEC 和封包複製。

FEC 或封包複製都不得在 DIA 連結上使用；它們僅用於分支和中樞之間的 VPN 通道連結。

僅支援 *SD-WAN* 的 *PAN-OS* 防火牆支援 *FEC* 和封包複製。*Prisma Access Hub* 不支援 *FEC* 和封包複製。

要在編碼器（FEC 或封包複製的起始端）上設定 FEC 或封包複製，請使用 Panorama 進行以下操作：

- 建立一個 SD-WAN 介面設定檔，指定 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格），並將該設定檔套用至一個或多個介面。
- 建立錯誤更正設定檔以實作 FEC 或封包複製。
- 將錯誤更正設定檔套用至 SD-WAN 原則規則，並指定要向其套用該規則的單個應用程式。

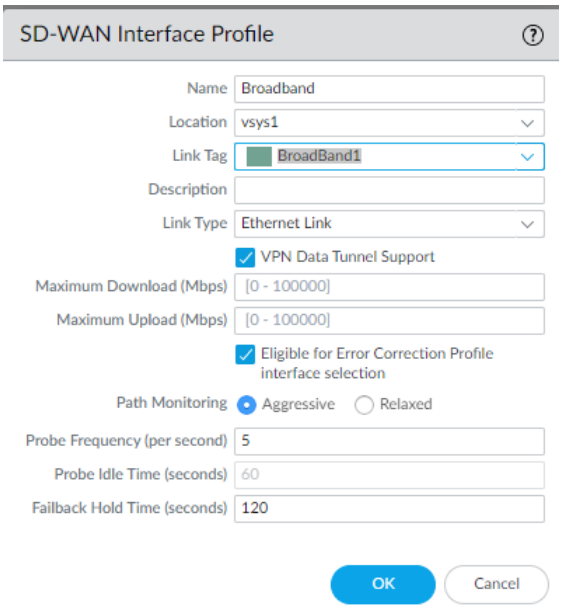
- 將設定推送至編碼器。（解碼器[接收端]不需要進行特定的 FEC 或封包複製設定；只要編碼器啟動錯誤更正，解碼器上將預設啟用該機制。）

FEC 和封包複製支援 *1,340* 個位元組的 *MTU*。大於此大小的封包將不會執行 *FEC* 或封包複製程序。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定 SD-WAN 介面設定檔，在其中選取 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格），以指示防火牆可以自動使用介面（套用了 SD-WAN 介面設定檔的介面）進行錯誤更正。此選項是否預設選取取決於您為設定檔選取的 **Link Type**（連結類型）。

您可以在設定檔中取消核取 ***Eligible for Error Correction Profile interface selection***（符合錯誤更正設定檔介面選取資格），然後將該設定檔套用至昂貴的 *5G LTE* 連結，這樣就永遠不會在該連結上執行昂貴的錯誤更正。

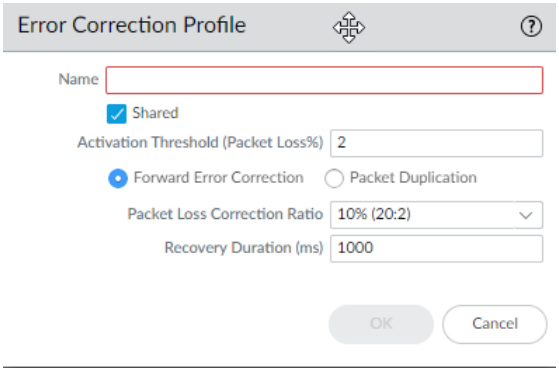


STEP 3 | 為 SD-WAN 設定實體乙太網路介面，並將您建立的 SD-WAN 介面設定檔套用至乙太網路介面。

STEP 4 | 為 FEC 或封包複製建立錯誤更正設定檔。

1. 選取 **Objects**（物件） > **SD-WAN Link Management**（**SD-WAN** 連結管理） > **Error Correction Profile**（錯誤更正設定檔）。
2. **Add**（新增）錯誤更正設定檔，並輸入最多 31 個英數字元的描述性 **Name**（名稱），如 EC_VOIP。
3. 選取 **Shared**（共用）以使錯誤更正設定檔對 Panorama 上的所有裝置群組和單個 vsys 中樞或分支上的預設 vsys，或您將此設定推送到的多重 vsys 中樞或分支上的 vsys1 可用。
4. 指定 **Activate when packet loss exceeds (%)**（封包遺失超過 **(%)** 時啟動）設定—若封包遺失超過此百分比，則在套用此錯誤更正設定檔的 SD-WAN 原則規則中，為設定的應用程式啟動 FEC 或封包複製。範圍是 1 至 99；預設值為 2。
5. 選取 **Forward Error Correction**（正向錯誤更正）或 **Packet Duplication**（封包複製），以指示當 SD-WAN 原則規則引用此 SD-WAN 介面設定檔時防火牆使用哪種錯誤更正方法；預設值為正向錯誤更正。如果選取「封包複製」，則 SD-WAN 將選取透過其傳送重複封包的介面。（SD-WAN 在上一步中選取了您透過 **Eligible for Error Correction Profile interface selection**（符合錯誤更正設定檔介面選取資格）設定的一個介面。）
6. （僅限正向錯誤更正）選取 **Packet Loss Correction Ratio**（封包遺失更正比率）：**10% (20:2)**、**20% (20:4)**、**30% (20:6)**、**40% (20:8)** 或 **50% (20:10)**—同位檢查位元與資料封包的比率，預設值為 10% (20:2)。同位檢查位元與傳送防火牆（編碼器）所傳送資料封包的比率越高，接收防火牆（解碼器）可以修復封包遺失的可能性就越大。然而，比率越高，需要的備援就越多，因此需要更多的頻寬開銷，這是實現錯誤更正的權衡。同位檢查比率套用於編碼防火牆的傳出流量。例如，如果中樞防火牆同位檢查比率為 50%，分支防火牆同位檢查比率為 20%，則中樞防火牆將接收 20%，分支防火牆將接收 50%。
7. 指定 **Recovery Duration (ms)**（復原持續時間（毫秒））—接收防火牆（解碼器）可以使用接收到的同位檢查封包，對遺失的資料封包執行封包復原所花費的最大毫秒數（範圍為 1 至 5,000；預設值為 1,000）。防火牆立即將接收的資料封包傳送至目的地。在復原持續時間期間，解碼器對所有遺失的資料封包執行封包復原。當復原持續時間到期時，所有同位檢查封包都會被釋放。您可在編碼器的錯誤更正設定檔中設定復原持續時間，編碼器會將「復原持續時間」值傳送到解碼器。解碼器上的「復原持續時間」設定沒有影響。

   首先使用預設的「復原持續時間」設定，並根據正常和間歇性暫時低壓情況下的測試，在必要時進行調整。



8. 按一下 **OK**（確定）。

STEP 5 | 設定 SD-WAN 原則規則，引用您在規則中建立的 **Error Correction Profile**（錯誤更正設定檔），並指定要向其套用規則的關鍵應用程式。

設定 *FEC* 或封包複製時，僅在 *SD-WAN* 原則規則中指定一個應用程式。對於 *FEC* 或封包複製，您不得在單個原則規則中組合多個應用程式。

STEP 6 | **Commit**（提交），然後 **Commit and Push**（提交並推送）設定變更到編碼防火牆（分支和中樞）。

設定 SD-WAN 原則規則

SD-WAN 原則規則指定應用程式和/或服務以及流量散佈設定檔，以確定防火牆如何為不屬於現有工作階段且與滿足所有其他條件（如來源和目的地區域、來源和目的地 IP 位址以及來源使用者）的傳入封包選取偏好路徑。SD-WAN 原則規則還指定一個路徑品質設定檔，其中包含延遲、抖動和封包遺失的閾值。當超出其中一個閾值時，防火牆會為應用程式和/或服務選取新路徑。

監控 SD-WAN 流量時，將根據流量進入中樞裝置時推送到中樞裝置的 SD-WAN 原則，對源自中樞裝置後方來源的流量進行評估，且由於已經做出了路徑選擇決定，因此當流量通過分支裝置到達最終目標裝置時，不會根據其 SD-WAN 原則對該流量進行評估。相反，源自分支裝置後方來源的流量將根據推送到分支裝置而不是中樞裝置的 SD-WAN 原則進行評估。Panorama™ 管理伺服器會聚合來自中樞和分支的日誌，對於相同的流量，將顯示兩個工作階段項目，但只有最初評估流量的 SD-WAN 裝置包含 SD-WAN 詳細資料。

在 SD-WAN 原則規則中，您可以引用錯誤更正設定檔，以便可以將正向錯誤更正 (FEC) 或封包複製套用至對丟棄或損壞的封包具有較低容忍度的指定關鍵應用程式。

在 SD-WAN 原則規則中，您還需指定希望 Panorama 向其推送規則的裝置。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Policies**（原則） > **SD-WAN**（**SD-WAN**），然後從 **Device Group**（裝置群組）內容下拉清單中選取適當的裝置群組。

STEP 3 | **Add**（新增） SD-WAN 原則規則。

STEP 4 | 在 **General**（一般）標籤中，輸入規則的描述性 **Name**（名稱）。

STEP 5 | 在 **Source**（來源）標籤中，設定原則規則的來源參數。

1. 新增 **Source Zone**（來源區域）或選取 **Any**（任何）來源區域
2. **Add**（新增）一個或多個來源位址，設定一個外部動態清單 (EDL)，或選取 **Any**（任何）來源位址。
3. **Add**（新增）一個或多個來源使用者，或選取任何來源使用者。

STEP 6 | 在 **Destination**（目的地）標籤上，設定原則規則的目的地參數。

1. **Add**（新增）**Destination Zone**（目的地區域）或選取 **Any**（任何）目的地區域。
2. **Add**（新增）一個或多個目的地位址，設定一個 EDL，或選取 **Any**（任何）目的地位址。

STEP 7 | 在 **Application/Service**（應用程式/服務）頁籤上，附加您的 SD-WAN 連結管理設定檔並指定您的應用程式和服務。

PAN-OS 10.0.2 僅支援關聯 *SaaS* 品質設定檔或錯誤更正，但不支援同時關聯二者。如果將其中一個設定檔與 *SD-WAN* 原則規則相關聯，則不能關聯另一個設定檔。

例如，如果將 *SaaS* 品質設定檔與 *SD-WAN* 原則規則相關聯，則無法將錯誤更正設定檔與同一 *SD-WAN* 原則規則相關聯。

1. 選取 **Path Quality**（路徑品質）或 建立路徑品質設定檔。
2. 如果分支防火牆具有指向 SaaS 應用程式的直接網際網路存取 (DIA) 連結，請選取 **SaaS Quality Profile**（**SaaS** 品質設定檔）或 建立 SaaS 品質設定檔。預設值為 **None (disabled)**（無（已停用））。
3. 選取 **Error Correction Profile**（錯誤更正設定檔）或 建立錯誤更正設定檔，以將正向錯誤更正 (FEC) 或封包複製套用至符合 SD-WAN 政策規則的應用程式。預設值為 **None (disabled)**（無（已停用））。
4. **Add Applications**（新增應用程式）並從清單中選取一個或多個應用程式，或選取 **Any**（任何）應用程式。您選取的所有應用程式都受到選取的路徑品質設定檔中指定的健康情況閾值的限制。如果封包與其中一個應用程式匹配，且該應用程式超過了路徑品質設定檔中的一個健康情況閾值（且封包滿足其餘規則條件），則防火牆將選取新的偏好路徑。

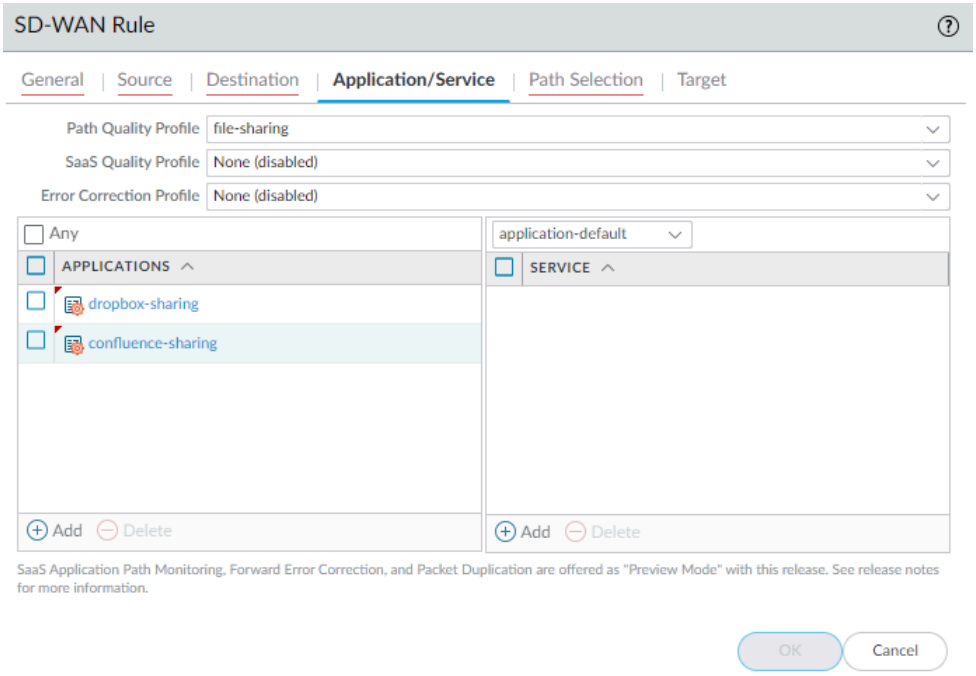
   僅新增業務關鍵應用程式和可用性對路徑情況敏感的應用程式。

   如果將 ***Adaptive***（適應性）模式下的 SaaS 品質設定檔與 *SD-WAN* 原則相關聯，請新增要監控的特定 *SaaS* 應用程式。對符合 *SD-WAN* 原則規則的所有應用程式使用適應性監控可能會影響 *SD-WAN* 防火牆的效能。

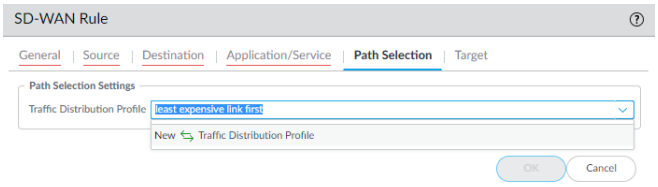
   如果將 SaaS 品質設定檔與指定的 *SaaS* 應用程式相關聯，請將 *SaaS* 應用程式新增到 *SD-WAN* 規則中，以確保 *SaaS* 監控設定僅套用至所需的 *SaaS* 應用程式。
5. **Add Services**（新增服務）並從清單中選取一個或多個項目，或選取 **Any**（任何）服務。您選取的所有服務都受到選取的路徑品質設定檔中指定的健康情況閾值的限制。如果封包

與其中一個服務匹配，且該服務超過了路徑品質設定檔中的一個健康情況閾值（且封包滿足其餘規則條件），則防火牆將選取新的偏好路徑。

僅新增業務關鍵服務和可用性對路徑情況敏感的服務。

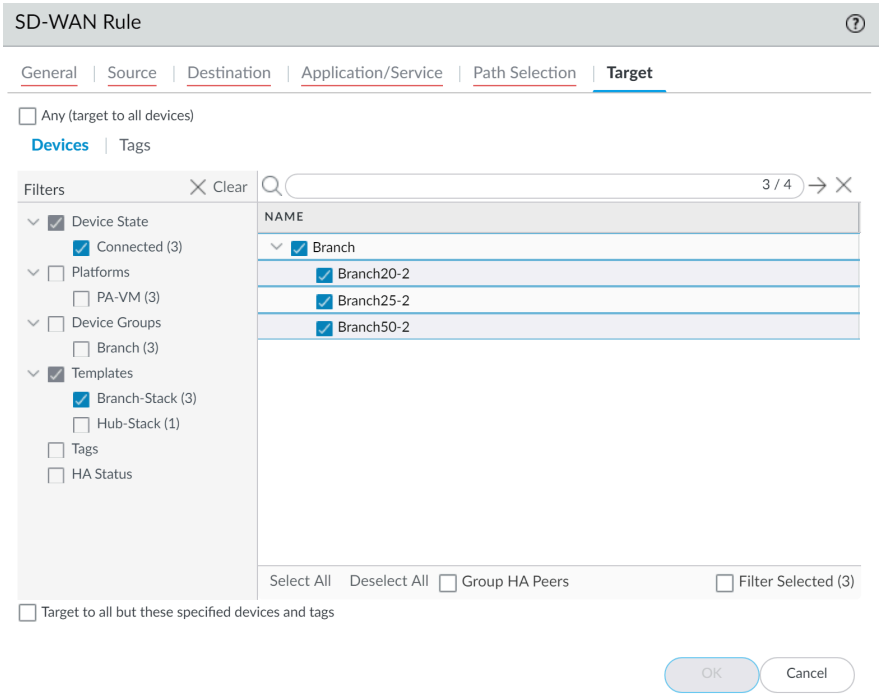


STEP 8 | 在 **Path Selection**（路徑選擇）頁籤上，選取一個 **Traffic Distribution**（流量散佈）設定檔或建立流量散佈設定檔.。當傳入封包（與工作階段沒有關聯）與規則中的所有匹配條件均匹配時，防火牆會使用此流量散佈設定檔選取新的偏好路徑。

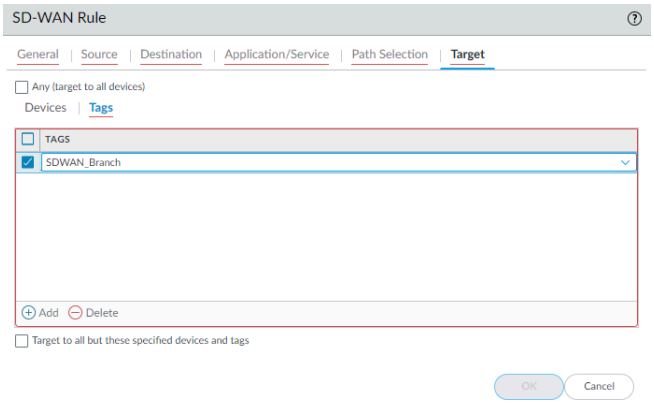


STEP 9 | 在 **Target**（目標）標籤上，使用以下方式之一在裝置群組中指定 Panorama 將向其推送 SD-WAN 原則規則的目標防火牆：

- 選取 **Any**（任何）（以所有裝置為目標）（預設值）以將規則推送到所有裝置。或者，選取 **Devices**（裝置）或 **Tags**（標籤）以指定 Panorama 將向其推送 SD-WAN 原則規則的單裝置。
- 在 **Devices**（裝置）頁籤上，選取一個或多個篩選器以限制顯示在「名稱」欄位的選擇；然後選取一個或多個 Panorama 將向其推送規則的裝置，如此範例中所示：



- 在 **Tags**（標籤）頁籤上，**Add**（新增）一個或多個 **Tags**（標籤），然後選取標籤以指定 Panorama 將規則推送到標記有所選標籤的裝置，如此範例中所示：



- 如果指定了「裝置」或「標籤」，您可以選取**Target to all but these specified devices and tags**（以除了指定裝置和標籤之外的所有裝置為目標），讓 Panorama 將 SD-WAN 原則規則推送到除了指定裝置或有標籤裝置之外的所有裝置。

STEP 10 | 按一下 **OK**（確定）。

STEP 11 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 12 | （最佳做法）建立一個全部擷取 SD-WAN 政策規則到 散佈不匹配的工作階段，以便您可以控制未匹配的工作階段使用的連結，以及檢視 SD-WAN 外掛程式的日誌記錄和報告中未匹配的工作階段。

如果您沒有建立一個全部擷取的規則來散佈未匹配的工作階段，則防火牆將以循環配置順序在所有可用連結之間散佈這些工作階段，因為不存在針對未匹配工作階段的流量散佈設定檔。循環配置散佈未匹配的工作階段可能意外增加成本，並導致應用程式可見度丟失。

STEP 13 | 在設定 SD-WAN 原則規則後，建立一個安全性原則規則以允許流量（例如，**bgp** 作為**Application**（應用程式））從分支流到網際網路、從分支流到中樞以及從中樞流到分支。

STEP 14 | （選用）為關鍵應用程式設定 QoS。

如果 *SD-WAN* 應用程式需要保證的頻寬容量，或者您不希望其他應用程式佔用關鍵業務應用程式的頻寬，請建立 *QoS* 規則以適當控制頻寬。

STEP 15 | 要在 VPN 叢集成員之間自動設定 BGP 路由，請在 SD-WAN 外掛程式中，在分支和中樞之間設定 BGP 路由，以動態路由將受到 SD-WAN 容錯移轉和載入共用限制的流量。

或者，如果您想要在每個防火牆上手動設定 BGP 路由，或使用單獨的 Panorama 範本來設定 BGP 路由（以獲得更多控制權），請將外掛程式中的 BGP 資訊留空。否則，請設定 BGP 路由。

STEP 16 | 為公共虛擬 SD-WAN 介面設定 NAT。

允許直接網際網路存取流量容錯移轉到 MPLS 連結

在一個 SD-WAN 分公司中，防火牆執行分割通道，以便具有共用 IP 位址的所有應用程式都採用指向網際網路的直接網際網路存取 (DIA) 介面，而具有屬於中樞的專有 IP 位址的應用程式都採用 VPN 介面。防火牆在必要時自動將 DIA 應用程式容錯移轉到指向中樞的 MPLS 專用連線，以便傳往網際網路的流量採用通過中樞的替代路徑到達網際網路。為了讓此生效，您必須執行以下操作：

STEP 1 | 在您的分支和中樞之間建立一個 MPLS 連結。當您建立 SD-WAN 介面設定檔時，中樞和分支的連結類型必須均為 **MPLS**。

STEP 2 | 如果您希望私人流量通過 VPN 通道，請在 SD-WAN 介面設定檔中啟用 **VPN** 資料通道支援。如果您停用 **VPN** 資料通道支援，私人資料將在 VPN 通道之外。

STEP 3 | 設定 SD-WAN 原則規則用於特定應用程式、建立路徑品質設定檔以及建立流量散佈設定檔指定自上而下優先順序方法。流量散佈設定檔還必須指定一個 **MPLS** 連結作為容錯移轉選項（使用一個標籤標識）。確認 SD-WAN 原則規則中的應用程式引用了正確的路徑品質和流量散佈設定檔，且流量散佈設定檔指定了自上而下的優先順序。

在中樞和分支上都啟用了 VPN 資料通道支援數且 MPLS 連結正常運行後，防火牆會在必要時自動使用 MPLS 連線對 DIA 流量進行容錯移轉。

STEP 4 | 在中樞組態中，確保中樞具有通往網際網路的路徑，且正確設定了路由以便中樞流量可到達網際網路。

防火牆使用 DIA 虛擬介面和 VPN 虛擬介面來確保公用網際網路流量與私人流量在同一路徑中分開；也就是說，網際網路通訊和私人通訊不會通過同一個 VPN 通道。使用適當的區域進行完整分隔可達到最佳效果。

設定 DIA AnyPath

當來自 ISP 的 SD-WAN 直接網際網路存取 (DIA) 連結出現斷電或暫時低壓時，您需要將這些連結容錯移轉到另一個連結以確保業務連續性。DIA 連結可以容錯移轉到 MPLS 連結，但是您可能沒有 MPLS 連結。DIA 連結必須能夠容錯移轉到具有到網際網路之直接路徑或間接路徑（透過中樞或分支）的另一個連結；DIA 流量可以透過可用的任何路徑存取網際網路，而不僅限於 DIA。DIA AnyPath 支援 DIA 連結容錯移轉到私人 VPN 通道，該 VPN 通道將到達中樞防火牆，然後存取網際網路。此外，如果您的拓撲是完整網狀（分支到分支），且沒有中樞，則 DIA 流量可以容錯移轉到分支防火牆以存取網際網路。

DIA AnyPath 需要 PAN-OS 10.0.3 或更高的 PAN-OS 版本和相容的 SD-WAN 外掛程式版本，這些資訊顯示在相容性矩陣的 Panorama 外掛程式部分的 SD-WAN 表中。

需要網際網路連結以容錯移轉到 VPN 通道 (DIA AnyPath) 的使用案例有如下幾種：

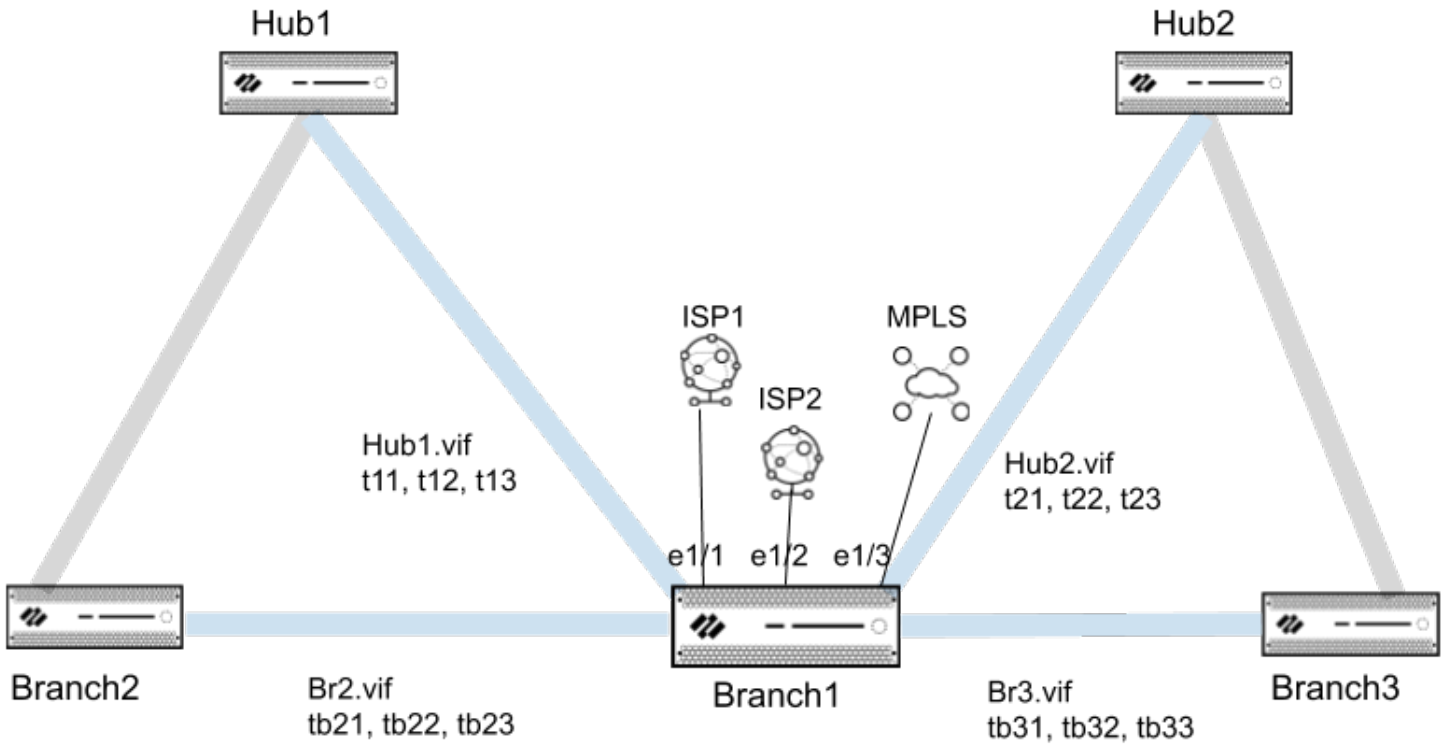
- 您想從昂貴的 MPLS 連結移轉至一個或多個公用網際網路連線，這些連線通常來自不同廠商。
- VPN 叢集中有多個中樞，以允許從主要中樞到一系列備份中樞的瀑布類型容錯移轉。
- 在分割通道場景中，您只希望特定的頻寬密集型應用程式透過分支的 DIA 連結直接連線到網際網路，而不是透過 VPN 通道返回到資料中心中樞，從而節省了 WAN 頻寬成本。如果發生 DIA 暫時低壓或斷電，此應用程式流量將容錯移轉到資料中心中樞以存取網際網路；如果需要，可以隨後容錯移轉到第二個中樞以存取網際網路。
- 在不同的分割通道場景中，您希望大多數網際網路流量都通過 DIA 連結，而不是將流量回傳到資料中心，從而實現網際網路突圍。但是，您希望特定的應用程式（可能需要由另一安全性裝置進行額外掃描或日誌記錄）返回到資料中心。您可建立 SD-WAN 原則規則，將這些應用程式導向到前往中樞的主要路徑，而不是由防火牆路由表中的預設路由確定的常規 DIA 連結。如果出現暫時低壓或斷電的情況，這些應用程式將進行容錯移轉，從而採用分支的 DIA 介面。

DIA AnyPath 引入了主體虛擬介面的概念，可以包括 DIA 連結以及巢狀的中樞虛擬介面和分支虛擬介面（VPN 通道），各自包含自己的連結。主體虛擬介面最多可以包含九個 DIA（乙太網路）介面、中樞虛擬介面和分支虛擬介面。將中樞裝置新增到 Panorama 時，可以將連結標籤指派到中樞。假設您使用 SD-WAN 外掛程式，則 Auto VPN 會將該連結標籤指派到中樞虛擬介面，這使您可以在流量散佈設定檔中指定該標籤，以控制虛擬介面之間的容錯移轉順序。

主體虛擬介面在 *CLI* 命令中稱為 *DIA-VIF*。

主體虛擬介面可以具有屬於不同安全性區域的介面成員。不過，最佳做法是讓主體虛擬介面中的所有成員介面都屬於相同的安全性區域。另一個最佳做法是在主體虛擬介面中至少有一個成員介面是連結類型，如乙太網路、纜線模式、*ADSL*、光纖、*LTE* 或 *WiFi*。

以下拓撲範例顯示了具有兩個 ISP 連線和一個 MPLS 連結的 Branch1。Branch1 還具有一個 Hub1 虛擬介面（該虛擬介面具有三個連線到 Hub1 的 VPN 通道），以及一個 Hub2 虛擬介面（該虛擬介面具有三個連線到 Hub2 的 VPN 通道）。Branch1 還具有一個 branch2 虛擬介面（該虛擬介面具有三個連線到 Branch2 的 VPN 通道），以及一個 branch3 虛擬介面（該虛擬介面具有三個連線到 Branch3 的 VPN 通道）。DIA AnyPath 的目標是設定 DIA 可以容錯移轉到 VPN 通道的順序，以直接或間存取網際網路，從而保持業務連續性。



當您設定一個主體虛擬介面時，它將自動成為預設路由，以便將網際網路流量正確路由到主體虛擬介面的任何成員（DIA 連結和 VPN 隧道）。路徑選取基於 SD-WAN 路徑品質設定檔和流量散佈設定檔，您可以將其設定為使用自上而下優先順序散佈方法來控制容錯移轉順序。在範例拓撲中，流量散佈設定檔可以先列出主體虛擬介面的標籤，然後列出 Hub1 虛擬介面的標籤，之後列出 Hub2 虛擬介面的標籤。

放大到更深層級的容錯移轉優先順序，一個中樞虛擬介面具有多個通道成員，因此您需要一種方法對成員的容錯移轉順序進行優先排序，例如在 LTE VPN 通道之前優先使用頻寬 VPN 通道。您可以使用套用到乙太網路介面的 SD-WAN 介面設定檔中的 **VPN Failover Metric**（**VPN** 容錯移轉指標）指定優先順序。指標值越低，容錯移轉時選取該通道的優先順序就越高。在拓撲範例中，在 Hub1 虛擬介面中，t11 的 VPN 容錯移轉指標低於 t12 會導致網際網路流量先於 t12 容錯移轉到 t11。如果虛擬介面中的多個通道具有相同的指標，則 SD-WAN 將以循環方式向通道傳送新的工作階段流量。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 為中樞虛擬介面或分支虛擬介面中配套的 VPN 通道指定容錯移轉優先順序。

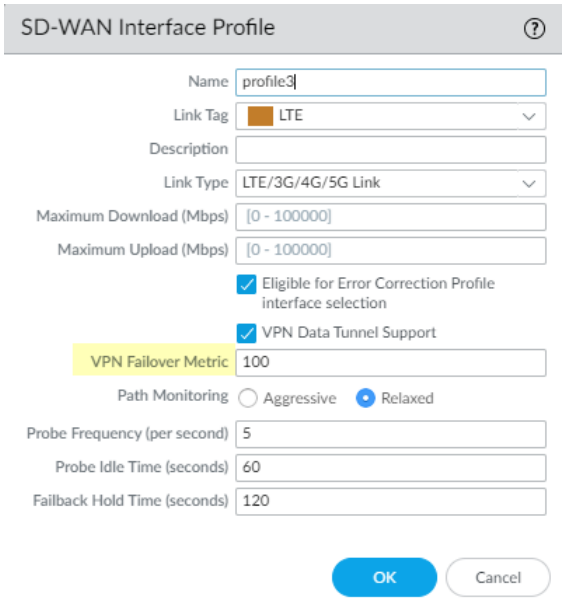
1. 選取或 設定 SD-WAN 介面設定檔。

   最佳做法是設定至少一個連結類型（乙太網路、纜線數據機、*ADSL*、光纖、*LTE* 或 *WiFi*）的介面。

2. 您必須啟用 **VPN Data Tunnel Support**（**VPN** 資料通道支援）。
3. 為 VPN 通道指定 **VPN Failover Metric**（**VPN** 容錯移轉指標）；範圍是 1 至 65,535；預設值為 10。指標值越低，您套用此設定檔的 VPN 通道（連結）的優先順序就越高。

   例如，將指標設定為較低的值，然後將設定檔套用於寬頻介面；然後建立一個不同的設定檔，以設定套用於昂貴 LTE 介面的高指標，確保僅在寬頻容錯移轉後才使用該設定檔。

   如果中樞只有一個連結，則該連結支援所有虛擬介面和 *DIA* 流量。如果您想要以特定順序使用連結類型，則必須將流量散佈設定檔套用至指定自上而下優先順序的中樞，然後排序連結標籤以指定偏好的順序。如果您套用指定最佳可用路徑的流量散佈設定檔，防火牆將使用連結（不論成本如何），選擇表現最佳的分支路徑。總而言之，流量散佈設定檔中的連結標籤，連結標籤已套用至中樞虛擬介面（此工作的步驟 *6*），且 ***VPN*** 容錯移轉指標僅當流量散佈設定檔指定自上而下優先順序時才能運作。



4. 按一下 **OK**（確定）。

STEP 3 | 為 SD-WAN 設定實體乙太網路介面，然後在 SD-WAN 頁籤上，套用在上一步中建立的 SD-WAN 介面設定檔。

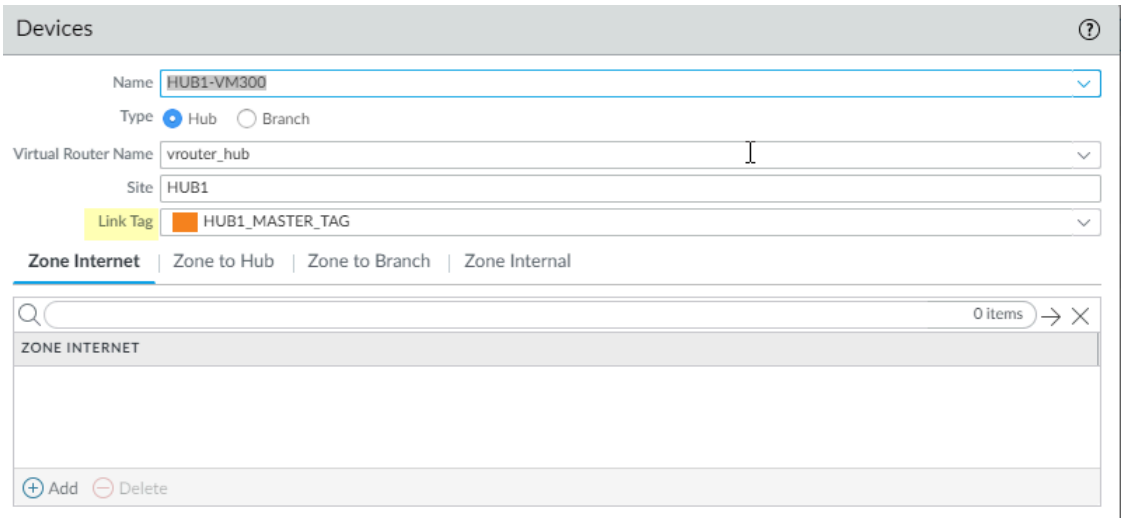
最佳做法是讓主體虛擬介面中的所有介面都屬於相同的安全性區域。

STEP 4 | 重複步驟 2 和 3，設定具有不同 VPN 容錯移轉指標的其他 SD-WAN 介面設定檔，並將設定檔套用至不同的乙太網路介面，以確定容錯移轉到連結的順序。

STEP 5 | 為中樞虛擬介面 建立連結標籤。

STEP 6 | 新增連結標籤到您想要參與 DIA AnyPath 的中樞。

1. 在 **Panorama** > **SD-WAN** > **Devices**（裝置）中，新增一個 SD-WAN 裝置 以新增一個中樞由 Panorama 進行管理。
2. 選取該中樞。
3. 選取您在上一步中建立的 **Link Tag**（連結標籤），該 Auto VPN 套用至整個中樞虛擬介面，而不是單個連結。因此，您可以在「流量散佈設定檔」中引用此「連結標籤」，以指示中樞虛擬介面的 DIA AnyPath 容錯移轉順序。在分支裝置上，Auto VPN 使用此標籤在終止於中樞裝置的 SD-WAN 虛擬介面上填入「連結標籤」欄位。



4. 按一下 **OK**（確定）。

STEP 7 | 重複步驟 5 和 6，為每個中樞虛擬介面建立一個連結標籤，並將該標籤新增到將參與 DIA AnyPath 的每個中樞中。對所有分支虛擬介面執行同樣的操作。

STEP 8 | 建立流量散佈設定檔以實作 DIA AnyPath。

1. 建立流量散佈設定檔。
2. 選取 **Top Down Priority**（自上而下優先順序）。
3. 新增連結標籤，以便它們以您希望其關聯的連結用於容錯移轉的順序顯示。

   例如，如果您的使用案例是某些應用程式先使用 DIA，則先列出 DIA 標籤，然後列出一個中樞虛擬介面標籤，之後列出第二個中樞虛擬介面標籤。如果您的使用案例是讓某些應用程式先進入中樞，然後存取網際網路，則先列出中樞虛擬介面，然後可能列出第二個中樞虛擬介面，最後列出 DIA 標籤。如果採用沒有中樞的完整網狀拓撲，請按所需順序使用 DIA 標籤和分支虛擬介面標籤。

STEP 9 | 為中樞和分支防火牆建立名稱相同的 SaaS Quality Profile（SaaS 品質設定檔）。

必須在中樞和分支防火牆上設定兩個名稱相同的 SaaS 品質設定檔，才能成功利用中樞防火牆作為備用容錯移轉。

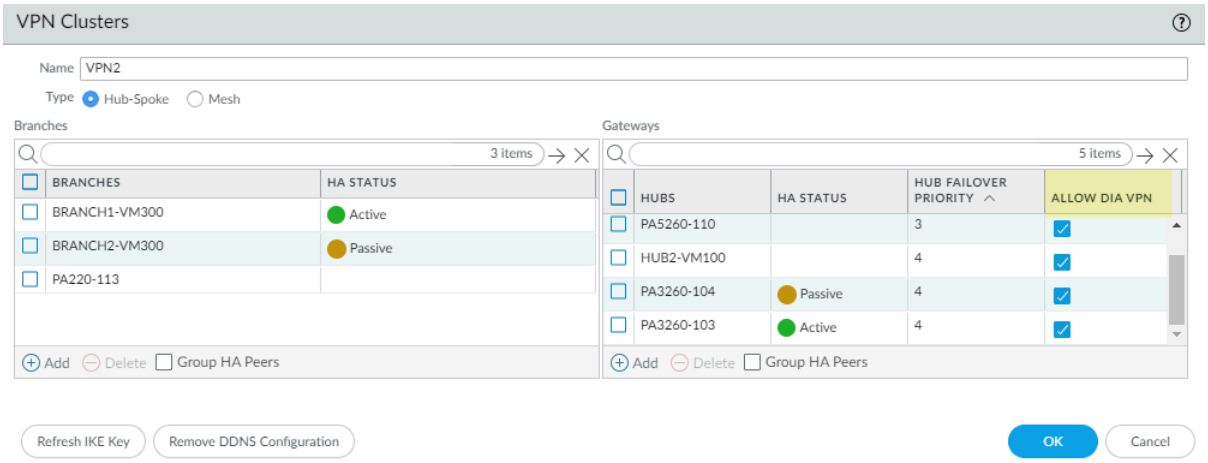
設定容錯移轉到具有相同 SaaS 應用程式目的地的中樞防火牆的最簡單方法是在「共用」裝置群組中建立一個 SaaS 品質設定檔。或者，您可以在不同的裝置群組中建立兩個名稱相同的 SaaS 品質設定檔，並將它們推送到中樞和分支防火牆。

要容錯移轉到具有不同 SaaS 應用程式目的地的中樞防火牆，請建立兩個具有相同名稱的 SaaS 品質設定檔，每個設定檔均指向不同裝置群組中的不同 SaaS 應用程式目的地，並將它們推送到中樞和分支防火牆。

您還必須建立引用此 *SaaS* 品質設定檔的 *SD-WAN* 原則規則，以允許中樞將該 *SaaS* 品質設定檔的連結品質統計資料發佈到分支。這樣做將透過中樞提供端對端 *SaaS* 監控。沒有此 *SD-WAN* 原則規則，您將只有從分支到中樞的連結度量，而沒有從中樞到 *SaaS* 應用程式的連結度量。

STEP 10 | 允許中樞參與 DIA AnyPath。

1. 建立 VPN 叢集，然後選取一個中樞。
2. 為中樞選取 **Allow DIA VPN**（允許 **DIA VPN**）。最多支援四個中樞（參與 DIA AnyPath 和 Prisma Access 中樞的 PAN-OS 中樞的任意組合）。如果它們是 HA 中樞，則總共支援八個中樞。如果您為配對中的一個 HA 對等 **Allow DIA VPN**（允許**DIA VPN**），則必須為另一個 HA 對等也啟用該選項。



STEP 11 | 為特定應用程式建立 SD-WAN 原則規則以使用 DIA AnyPath。

1. 設定 SD-WAN 原則規則。
2. 在 **Application/Service**（應用程式/服務）頁籤上，指定要為其實作 DIA AnyPath 的應用程式和服務。
3. 關聯您在上一步中建立的 **Saas Quality Profile**（**Saas** 品質設定檔）。

   如果要設定具有不同 SaaS 應用程式目的地的 SaaS 品質設定檔，則必須將 SaaS 品質設定檔與每個分支和中樞裝置群組中的 SD-WAN 原則規則相關聯。
4. 在 **Path Selection**（路徑選擇）標籤上，選取您為應用程式建立的 **Traffic Distribution Profile**（流量散佈設定檔）。

STEP 12 | 路由不符合任何 SD-WAN 原則規則的新工作階段，以及路由在 Panorama 或防火牆設定變更期間到達的工作階段。

1. 建立適當的路徑品質設定檔和流量散佈設定檔以處理此類工作階段。
2. 設定 SD-WAN 原則規則，這是這些工作階段的全部擷取規則。
3. 將此規則放在清單的最後。

STEP 13 | **Commit**（提交），然後 **Push to Devices**（推送到裝置）。

STEP 14 | Create a Security Policy Rule（建立安全性原則規則）以允許 DIA 流量前往名為 `zone-internet` 和 `zone-to-hub` 的 **Destination Zones**（目的地區域），然後指定符合該規則的 **Applications**（應用程式）。提交並推送到分支。

STEP 15 | 使用以下 CLI 命令監控 DIA 資訊：

1. **`show sdwan connection <dia-vif-name>`**
2. **`show sdwan path-monitor stats dia-vif all`**
3. **`show sdwan path-monitor dia-anypath`**
4. **`show sdwan path-monitor dia-anypath packet-buffer all`**
5. **`show sdwan path-monitor stats conn-idx <IDX>`**

散佈不匹配的工作階段

防火牆會嘗試將到達 SD-WAN 虛擬介面的工作介面與 SD-WAN 原則規則進行匹配；像對待安全性原則規則一樣，防火牆會按照從上到下的順序檢查 SD-WAN 原則規則。

- 如果存在匹配的 SD-WAN 規則，則防火牆為會該 SD-WAN 原則規則執行路徑監控和流量散佈。
- 如果與清單中的任何 SD-WAN 原則規則都不匹配，工作階段會匹配清單末端隱含的 SD-WAN 原則規則，即基於路由查閱，使用循環配置方式在一個 SD-WAN 介面中的所有連結間散佈不匹配的工作階段。

此外，如果沒有用於特定應用程式的 SD-WAN 原則規則，防火牆不會在特定於 SD-WAN 的可見性工具（如 SD-WAN 外掛程式中的日誌記錄和報告）中追蹤該應用程式的效能。

圖解隱含原則規則：

- 假設防火牆有三條 SD-WAN 原則規則：一條規則指定五個語音應用程式，一條規則指定六個視訊會議應用程式，一條規則指定十個 SaaS 應用程式。
- 一個工作階段，假設是視訊應用程式工作階段，到達了防火牆，但不匹配任何 SD-WAN 原則規則。因為該工作階段沒有匹配任何規則，防火牆沒有路徑品質設定檔或流量散佈設定檔來套用到此工作階段。
- 因此，防火牆會將該視訊應用程式匹配到隱含規則，將每個視訊工作階段散佈到防火牆上所有可用的 SD-WAN 連結標籤及其關聯的連結，這些連結可能是兩種寬頻連結，即 MPLS 連結和 LTE 連結。工作階段 1 前往寬頻介面的一個成員，工作階段 2 前往頻寬介面的另一個成員，工作階段 3 前往 MPLS，工作階段 4 前往 LTE，工作階段 5 前往寬頻介面的第一個成員，工作階段 6 前往寬頻介面的第二個成員，繼續如此循環配置散佈。

您可能不希望讓不匹配的工作階段訴諸於隱含的 SD-WAN 規則，因為您無法控制該工作階段散佈。因此，我們建議您建立一個全部擷取 SD-WAN 原則規則並將其放在 SD-WAN 原則規則清單的最後。全部擷取 SD-WAN 原則規則可讓您：

- 控制不匹配的工作階段使用哪個連結。
- 在 SD-WAN 外掛程式的日誌記錄和報告中檢視防火牆上的所有應用程式（包括不匹配的應用程式工作階段）。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 建立路徑品質設定檔，設定絕不會超過的極高延遲、抖動和封包遺失閾值。例如，2,000 毫秒延遲、1,000 毫秒抖動和 99% 的封包遺失。

STEP 3 | 建立流量散佈設定檔，按照您希望不匹配的工作階段使用與這些連結標籤關聯的連結的順序，指定您想要使用的 SD-WAN 連結標籤。

如果您根本不希望不匹配的應用程式使用特定路徑（實體介面），請從流量散佈設定檔中的連結標籤清單中刪除包含該連結的標籤。例如，如果您不希望電影串流之類的不匹配應用程式使用昂貴的 *LTE* 連結，請從流量散佈設定檔中的連結標籤清單中刪除 *LTE* 連結的連結標籤。

STEP 4 | **Add**（新增）一個全部擷取 SD-WAN 原則規則，然後在 **Application/Service**（應用程式/服務）標籤上，指定您建立的 **Path Quality Profile**（路徑品質設定檔）。

STEP 5 | 針對 **Applications**（應用程式）和 **Service**（服務）選取 **Any**（任何）。

STEP 6 | 在 **Path Selection**（路徑選擇）標籤上，選取您建立的 **Traffic Distribution Profile**（流量散佈設定檔）。

STEP 7 | 將規則 **Move**（移動）到 SD-WAN 原則規則清單的最後位置。

STEP 8 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 9 | **Commit**（提交）您的變更。

新增 SD-WAN 裝置到 Panorama

新增單一 SD-WAN 中樞或分支防火牆，或者使用 CSV 來大量匯入多個 SD-WAN 中樞和分支防火牆（具有預先共用金鑰或憑證驗證類型）。

- 設定 SD-WAN 裝置的憑證式驗證
- 新增一個 SD-WAN 裝置
- 批量匯入多台 SD-WAN 裝置
- 將 PAN-OS 防火牆裝載到 Prisma Access

設定 SD-WAN 裝置的憑證式驗證

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

您可以使用下列兩種驗證類型中的任一種來驗證 SD-WAN 裝置：

- 預先共用金鑰（預設驗證類型）
- 憑證（SD-WAN 外掛程式 3.2.0 和更新版本）

當您使用 SD-WAN 外掛程式 3.2.0 之前的版本來建立新的 SD-WAN 叢集或重新整理金鑰時，SD-WAN 外掛程式會自動產生預先共用金鑰。除了預先共用金鑰驗證類型之外，我們還使用 SD-WAN 外掛程式 3.2.0 和更新版本以針對新世代防火牆提供憑證式驗證，以滿足您的安全性需求。使用憑證式驗證，以針對所有 SD-WAN 網站進行更強大的驗證，將您的安全性提升到一個新的層級。

在執行可支援 SD-WAN 的舊版或進階路由引擎的所有軟體和硬體裝置上，我們支援憑證式驗證。

升級或降級目前的 SD-WAN 外掛程式之前，請遵循升級和降級注意事項中所提到的步驟。

使用下列工作流程，以針對 SD-WAN 裝置來設定憑證式驗證：

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上，針對 SD-WAN 裝置產生憑證。

1. 選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
2. 建立自我簽署根 CA 憑證，或從企業 CA 匯入憑證。根據根 CA，針對 SD-WAN 裝置產生裝置憑證。我們不支援 SCEP 產生的憑證。

   針對每個 SD-WAN 裝置，所產生的憑證都必須是唯一的。即，您無法產生憑證，並將其在多個 SD-WAN 裝置之間共用。

   產生用於 SD-WAN 通道驗證的分支和中樞防火牆憑證時，請記住下列幾點：

   - 兩個不同的中樞裝置可以使用相同的中樞憑證。
   - 如果符合下列條件，則兩個不同的分支裝置可以使用相同的分支憑證：
     - 分支裝置不屬於相同的 VPN 叢集
     - 這些分支裝置所屬的 VPN 叢集之間沒有通用中樞裝置
   - （僅限 HA 部署）如果將兩個不同的分支裝置設定為 HA 成員，則其也可以具有相同的分支憑證。
   - 如果中樞裝置在 VPN 叢集之間通用，則這些 VPN 叢集的分支裝置憑證應該具有所有屬性都具有唯一值的唯一憑證。如果您不確定憑證和其值的唯一性，則提交將會在中樞裝置上失敗（Panorama 上未出現提交失敗）。

   也請確定所產生用於 *SD-WAN* 通道驗證的分葉憑證（分支和中樞防火牆憑證）符合下列準則：

   - 金鑰使用應該具有數位簽名
   - 所有憑證都必須由相同的根 *CA* 進行簽署
   - 裝置憑證必須由根 *CA* 直接進行簽署。
   - 憑證格式應該為 *PKCS12*

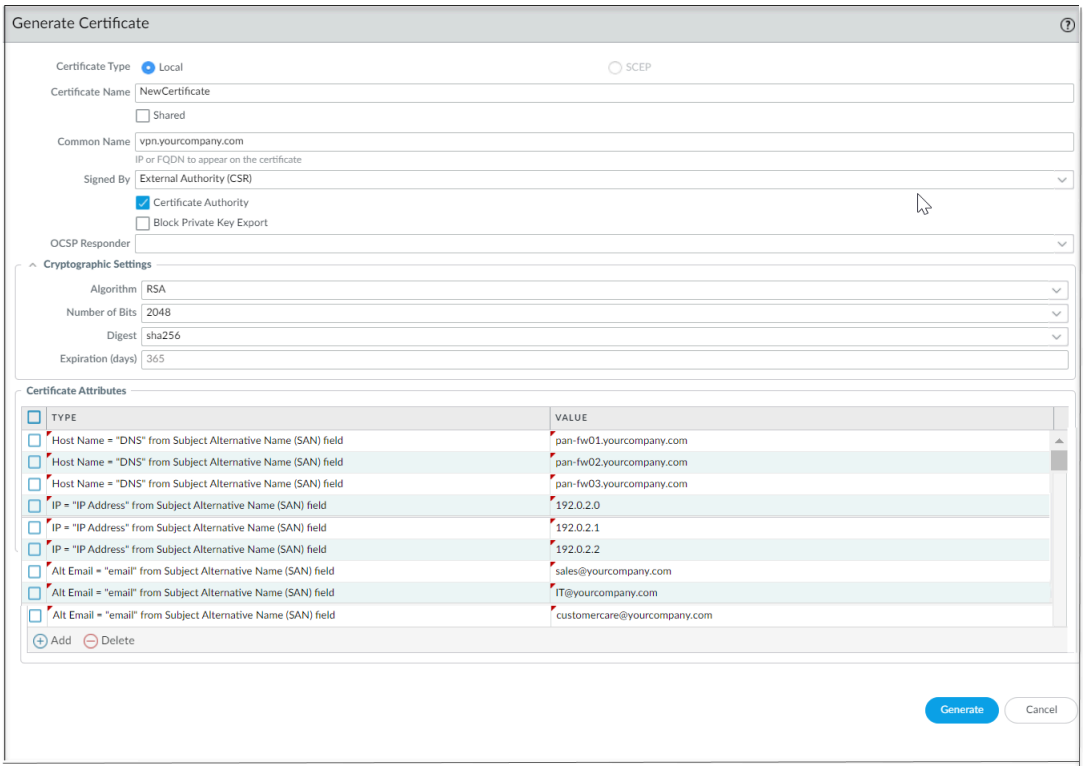
   憑證屬性用於判斷 IKE 閘道的本機 ID 和對等 ID。因此，必須使用下列三個憑證屬性來產生分葉憑證（即用於 SD-WAN 通道驗證的分支和中樞防火牆憑證），而且每個憑證屬性都應該獲指派三個唯一屬性值。否則，將會擲回提交錯誤。

   - FQDN (**Host Name**（主機名稱）)
   - IP 位址 (**IP**)
   - 使用者 FQDN（**Alt Email**（替代電子郵件））

   所有憑證都必須具有唯一 ***Host Name***（主機名稱）、***IP*** 和 ***Alt Email***（替代電子郵件）憑證屬性。即，任何憑證都不應該具有這些通用的屬性值。

   在下列範例中，所產生的 NewCertificate 共具有九個必要憑證屬性。**Host Name**（主機名稱）憑證屬性已設定三個唯一屬性值：pan-fw01.yourcompany.com、pan-fw02.yourcompany.com 和 pan-fw03.yourcompany.com。**IP** 憑證屬性已設定三個唯一屬性值：192.0.2.0、192.0.2.1 和 192.0.2.2。**Alt Email**（替代電子郵件）憑證

屬性已設定三個唯一屬性值：sales@yourcompany.com、IT@yourcompany.com 和 customercare@yourcompany.com。



STEP 3 | （選用）設定包含根 CA 和中繼 CA 的憑證設定檔，以保護伺服器通訊。

1. 選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

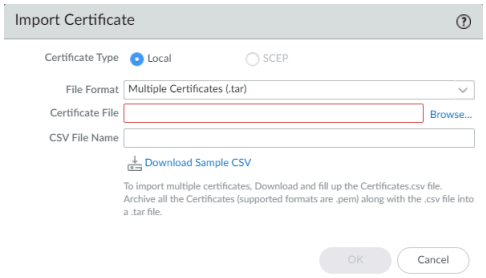
   如果您在憑證設定檔中設定中繼 CA，則也必須包括根 CA。

   此憑證設定檔定義 SD-WAN 中樞和分支如何相互驗證。

STEP 4 | 匯入 CA 憑證，以驗證 SD-WAN 裝置的識別。

1. **Panorama** > 憑證管理 > 憑證
2. 在 Panorama 上，針對叢集中的每個 SD-WAN 裝置匯入 CA 憑證和金鑰配對，或使用 **Multiple Certificates (.tar)**（多個憑證 **(.tar)**）來匯入多個憑證。使用 CSV，以將將憑證大

量匯入至 Panorama 管理伺服器。CSV 允許您一次匯入多個憑證，而不是手動新增每個憑證。



3. **Commit**（提交）您的變更。請務必在匯入憑證之後提交，以進一步設定所匯入的憑證。

STEP 5 | 設定憑證式驗證類型，同時新增要由 Panorama 管理伺服器所管理的 SD-WAN 中樞或分支防火牆。新增裝置時，您需要指定裝置的類型（分支或中樞）、裝置的驗證類型，以及針對每個裝置提供其網站名稱以輕鬆進行識別。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），以新增 SD-WAN 裝置（SD-WAN 中樞或分支防火牆），而 SD-WAN 裝置是由 Panorama 管理伺服器所管理。
2. 選取 **VPN Tunnel**（VPN 通道）頁籤，然後設定 **authentication**（驗證）類型。針對憑證式驗證，選取 **Certificate**（憑證），然後設定憑證相關欄位。新增 SD-WAN 裝置時，必須選取驗證類型。

STEP 6 | 將 PAN-OS 防火牆裝載至 Prisma Access 時，設定憑證式驗證。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置）來選取要連線至 Prisma Access 中樞的 SD-WAN 分支防火牆，然後設定連線。
2. 選取 **Prisma Access Onboarding**（**Prisma Access** 裝載），然後將計算節點 **Add**（新增）至 **Region**（地區）。在 **VPN Tunnel**（**VPN** 通道）中，必須選取驗證類型，才能驗證 CN（Prisma Access 中樞）。針對憑證式驗證，選取 **Certificate**（憑證）作為 **Authentication**（驗證）類型，然後設定憑證相關欄位。將 PAN-OS 防火牆裝載至 Prisma Access 時，必須選取驗證類型。

確保您針對所有分支裝置和所新增的 *Prisma Access* 中樞選取相同的驗證類型。如果您嘗試針對分支和 *Prisma* 中樞使用不同的驗證類型，則 *Panorama* 上會發生提交失敗。

STEP 7 | 設定憑證式驗證，同時建立 VPN 叢集。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集）。
2. 選取 VPN 叢集 **Type**（類型）。
3. 將 **Authentication Type**（驗證類型）選取為 **Certificate**（憑證）。必須指定驗證類型，才能在 VPN 叢集中新增裝置。VPN 叢集應該具有針對其所有裝置所選取的相同驗證類型。您無法變更已新增至 VPN 叢集之 SD-WAN 裝置的驗證類型。如果您想要變更，則請移除 VPN 叢集和其 SD-WAN 裝置，然後使用所選擇的驗證類型對其進行重新設定。根據預設，我們支援 VPN 叢集中裝置的預先共用金鑰驗證類型（如果您尚未手動選取憑證類型）。

STEP 8 | **Commit**（提交）組態變更。

STEP 9 | 選取 **Push to Devices**（推送到裝置）以將您的組態變更推送到受管理的防火牆。

新增一個 SD-WAN 裝置

新增一個 SD-WAN 中樞或分支防火牆，以便由 Panorama™ 管理伺服器進行管理。在新增裝置時，您需要指定裝置的類型（分支還是中樞），還要為每個裝置提供網站名稱以便輕鬆識別。新增裝置之前，請規劃 SD-WAN 設定，以確保您擁有所有必需的 IP 位址，而且瞭解 SD-WAN 拓撲。這可幫助減少組態錯誤。

如果您想要在兩個分支防火牆或兩個中樞防火牆上執行主動/被動 *HA*，則此時不要將這些防火牆新增為 *SD-WAN* 裝置。您將在您為 SD-WAN 設定 HA 裝置時將其單獨新增為 *HA* 對等。

如果您要使用 *BGP* 路由，則必須新增安全性政策規則，以允許 *BGP* 從內部區域到中樞區域，以及從中樞區域到內部區域。如果您想要使用 *4-byte ASN*，您必須先為虛擬路由器啟用 *4-byte ASN*。

檢視 *SD-WAN* 裝置時，如果沒有資料，或螢幕指出未定義 *SD-WAN*，則請查看相容性矩陣，瞭解您要使用的 *Panorama* 版本是否支援您嘗試使用的 *SD-WAN* 外掛程式版本。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後 **Add**（新增）新的 SD-WAN 防火牆。

STEP 3 | 選取受管理的防火牆名稱以新增為 SD-WAN 裝置。您必須先將 SD-WAN 防火牆新增為受管理的裝置，才可將其新增為 SD-WAN 裝置。

STEP 4 | 選取 SD-WAN 裝置的類型。

- 中樞—集中防火牆，部署在主要辦公室或一個中央位置，使用 VPN 連線將所有分支裝置連線到該位置。各分支之間的流量先通過中樞，然後繼續流向目標分支，將各分支連線到位於中樞位置的集中資源。中樞裝置處理流量，執行原則規則，並管理主要辦公室或位置的連結交換。
- 分支—部署在實體分支位置的防火牆，使用 VPN 連線與中樞連線，並提供分支層級的安全性。分支裝置處理流量，執行政策規則，並管理分支位置的連結交換。

STEP 5 | （選用）（PAN-OS 11.1.3 和更新版本，以及 SD-WAN 外掛程式 3.2.1 和更新版本）在 SD-WAN 中樞上設定多個虛擬路由器。

選取 **Enable Multi-VR Support**（啟用多 **VR** 支援）以在 SD-WAN 中樞上設定多個虛擬路由器。

我們已引進 SD-WAN 中樞上的多個虛擬路由器支援，讓您能夠在連線至相同 SD-WAN 中樞的分支裝置上擁有重疊的 IP 子網路位址。當您選取 SD-WAN **Type**（類型）作為中樞時，將能夠選取 **Enable Multi-VR Support**（啟用多 **VR** 支援）選項來設定多個虛擬路由器。

STEP 6 | 選取用於在 SD-WAN 中樞和分支之間進行路由的路由器名稱。預設情況下，會建立一個 `sdwan-default` 虛擬路由器，並啟用 Panorama 以自動推送路由器組態。

（進階路由已啟用）如果您已設定進階路由並且已成功建立邏輯路由器，則路由器名稱將顯示虛擬路由器和邏輯路由器名稱：

- 如果虛擬路由器和邏輯路由器名稱相同，則 **Router Name**（路由器名稱）會顯示相同的名稱，因為進階路由預設會建立與虛擬路由器同名的邏輯路由器。使用進階路由引擎時，相同範本的邏輯路由器名稱和虛擬路由器名稱必須相同，這一點十分重要。
- 如果虛擬路由器和邏輯路由器名稱不同（僅當您手動更新邏輯路由器名稱時才會發生這種情況），則路由器名稱會同時顯示虛擬和邏輯路由器名稱。您可以根據需要選取虛擬路由器（舊版引擎）或邏輯路由器（進階路由引擎）。如果您尚未啟用 **Advanced Routing**（進階路由），則只能從 **Router Name**（路由器名稱） 中選取虛擬路由器（針對舊版引擎）。

（PAN-OS 11.1.3 和更新版本，以及 SD-WAN 外掛程式 3.2.1 和更新版本）啟用多個虛擬路由器（**Enable Multi-VR Support**（啟用多 **VR** 支援））時，請針對 **Virtual Router Name**（虛擬路由器名稱）選取 DIA 虛擬路由器。

STEP 7 | 輸入 SD-WAN 網站名稱，以識別裝置的地理位置或目標。

SD-WAN 網站名稱支援所有大寫和小寫字母數字字元和特殊字元。網站名稱中不支援空格，如果使用，則會導致該網站的監控（***Panorama > Monitoring***（監控））資料無法顯示。

所有 *SD-WAN* 裝置（包括高可用性 *(HA)* 設定中的 *SD-WAN* 裝置）都必須具有唯一的網站名稱。

STEP 8 | 選取為中樞虛擬介面（或分支虛擬介面）建立的連結標籤，Auto VPN 會將其指派給虛擬介面。您將在流量散佈設定檔中使用此連結標籤，以允許中樞（或分支）參與 DIA AnyPath。

STEP 9 | 如果您要在針對中樞執行 NAT 的裝置後面新增中樞，則必須指定該上游 NAT 執行裝置上對外介面的 IP 位址或 FQDN，以讓自動 VPN 設定可以將該位址用作中樞的通道端點位址。這是分公司 IKE 和 IPSec 流程必須能夠到達的 IP 位址。（您必須已經為 SD-WAN 設定一個實體乙太網路介面。）

1. 在 **Upstream NAT**（上游 **NAT**）索引標籤上，啟用 **Upstream NAT**（上游 **NAT**）。
2. 新增一個 **SD-WAN** 介面；選取一個您已經為 SD-WAN 設定的介面。
3. 選取 **IP Address**（**IP** 位址）或 **FQDN**，然後分別輸入不帶子網路遮罩的 IPv4 位址（如 192.168.3.4）或上游裝置的 FQDN。

4. 按一下 **OK**（確定）。

   此外，您還必須在執行 *NAT* 的上游裝置上，設定帶一對一 *NAT* 政策的輸入目的地 *NAT*，而且不得設定到 *IKE* 或 *IPSec* 流量流程的連接埠轉譯。

   如果上游裝置的 *IP* 位址變更，您必須設定新 *IP* 位址，並將其推送到 *VPN* 叢集。您必須在分支和中樞上使用 *CLI* 命令 ***clear vpn ipsec-sa***、***clear vpn ike-sa*** 和 ***clear session all***。您還必須在為 *IP* 位址設定 *NAT* 原則的虛擬路由器上執行 ***clear session all*** 命令。

   第二層介面上不支援上游 *NAT*。

STEP 10 | （僅限完整網狀部署）如果您要在針對分支執行 NAT 的裝置後面新增分支，則必須指定該上游 NAT 執行裝置上對外介面的 IP 位址或 FQDN，或選取 DDNS 以指出 NAT 裝置上介面的 IP 位址是從 Palo Alto Networks DDNS 服務所取得。因此，Auto VPN 組態使用該公共 IP 位址作為分支的通道端點。分公司的 IKE 和 IPSec 流量必須能夠聯絡該 IP 位址。（您必須已經為 SD-WAN 設定一個實體乙太網路介面。）

1. 在 **Upstream NAT**（上游 **NAT**）索引標籤上，啟用 **Upstream NAT**（上游 **NAT**）。
2. 新增一個 **SD-WAN** 介面；選取一個您已經為 SD-WAN 設定的介面。
3. 如果您選取 **NAT IP Address Type**（**NAT IP** 位址類型）為 **Static IP**（靜態 **IP**），則選取 **IP Address**（**IP** 位址）或 **FQDN**，然後分別輸入不帶子網路遮罩的 IPv4 位址（如 192.168.3.4）或上游裝置的 FQDN。
4. 或者，選取 **NAT IP Address Type**（**NAT IP** 位址類型）為 **DDNS**。
5. 按一下 **OK**（確定）。

   此外，您還必須在執行 *NAT* 的上游裝置上，設定帶一對一 *NAT* 政策的輸入目的地 *NAT*，而且不得設定到 *IKE* 或 *IPSec* 流量流程的連接埠轉譯。

   如果上游裝置的 *IP* 位址變更，您必須設定新 *IP* 位址，並將其推送到 *VPN* 叢集。您必須在分支和中樞上使用 *CLI* 命令 ***clear ipsec***、***clear ike-sa*** 和 ***clear session all***。您還必須在為 *IP* 位址設定 *NAT* 原則的虛擬路由器上執行 ***clear session all*** 命令。

   Web 介面中有第二個可以針對分支設定上游 *NAT* 的位置，但下列位置不是偏好位置，您不應該在這兩個地方都針對分支設定上游 *NAT*。可設定上游 *NAT* 的第二個非偏好位置是 *Panorama* 的 ***Network***（網路）> ***Interfaces***（介面）> ***Ethernet***（乙太網路）中，於 ***Template***（範本）欄位中選取範本，並選取乙太網路介面，然後選取 ***SD-WAN*** 頁籤。此時，您可以 ***Enable***（啟用）上游 *NAT*，然後選取 ***NAT IP Address Type***（***NAT IP*** 位址類型）。優先選用第二種方法。如果先透過範本堆疊針對 *Panorama* 上的乙太網路介面設定上游 *NAT*，則 *SD-WAN* 外掛程式將不會變更設定，即使您在外掛程式裝置設定頁面上使用不同的設定也是一樣。僅當未透過範本堆疊在 *Panorama* 上設定任何上游 *NAT* 時，上游 *NAT* 的外掛程式設定才會生效。

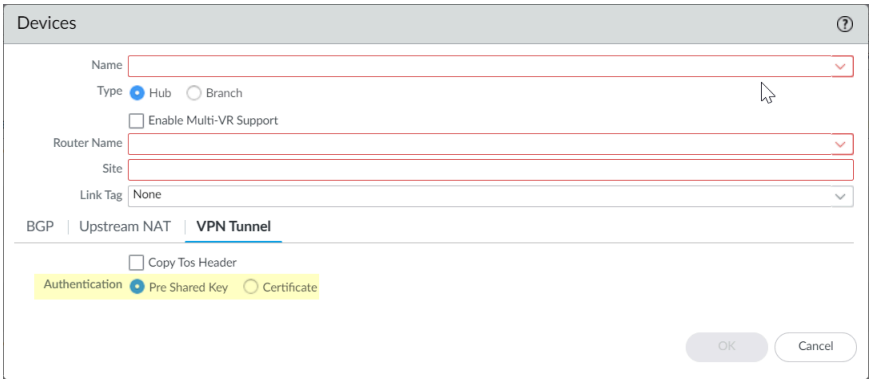
   第二層介面上不支援上游 *NAT*。

STEP 11 | 如果您的應用程式流量帶有服務類型 (ToS) 位元或 Differentiated Services Code Point（區別服務代碼點 - DSCP）(DSCP) 標記，則請將 ToS 欄位從內部標頭複製至通過 VPN 通道之封裝封包的外部 VPN 標頭，以保留 QoS 資訊.

1. 選取 **VPN Tunnel**（**VPN** 通道）頁籤。
2. 選取 **Copy ToS Header**（複製 **ToS** 標頭）。
3. 按一下 **OK**（確定）。

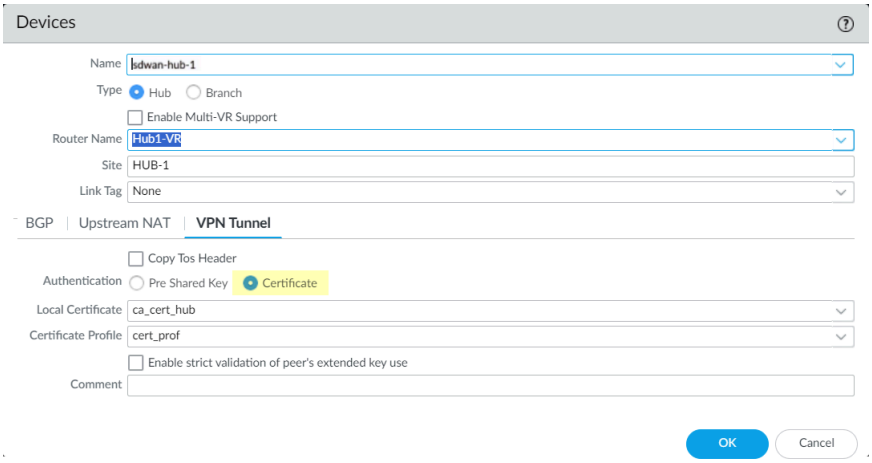
STEP 12 | （必要）（SD-WAN 外掛程式 3.2.0 和更新版本）指定如何驗證對等。

選取 **Authentication**（驗證）類型：**Pre Shared Key**（預先共用金鑰）或 **Certificate**（憑證）。如果您選擇預先共用金鑰，則將會自動產生預先共用金鑰。



- 您必須針對 *SD-WAN* 叢集中的每個裝置使用唯一憑證。
- 將 *SD-WAN* 裝置新增至 *VPN* 叢集之後，就無法變更驗證類型。
- （僅限 *HA* 部署）如果您已在 *Panorama* 中設定高可用性 *(HA)* 配對，則主動和被動防火牆必須使用相同的憑證。在 *RMA* 程序期間，您必須使用與主動防火牆相同的憑證來設定更換防火牆。如果撤銷主動防火牆的憑證，並推送新憑證，則被動防火牆也必須使用新憑證來進行更新。即，主動和被動防火牆必須具有高可用性部署中所設定的相同憑證。

STEP 13 | （只在啟用憑證驗證類型時）設定憑證式驗證。



1. 選取已在 Panorama 上的 **Local Certificate**（本機憑證）、**Import**（匯入）憑證，或 **Generate**（產生）新憑證。

   - 若需 **Import**（匯入）憑證，先匯入憑證供 IKEv2 閘道驗證使用，然後回到此工作。我們不支援 SCEP 產生的憑證。
   - 如果您想要 **Generate**（產生）新憑證，則請先在 Panorama 上產生憑證，然後回到此工作。針對每個 SD-WAN 裝置，所產生的憑證都必須是唯一的。即，您無法產生憑證，也無法將其共用至多個 SD-WAN 裝置。

     產生用於 SD-WAN 通道驗證的分支和中樞防火牆憑證時，請記住下列幾點：

     - 兩個不同的中樞裝置可以使用相同的中樞憑證。
     - 如果符合下列條件，則兩個不同的分支裝置可以使用相同的分支憑證：
       - 分支裝置不屬於相同 VPN 叢集。
       - 這些分支裝置所屬的 VPN 群集之間沒有通用中樞裝置。
     - （僅限 HA 部署）如果將兩個不同的分支裝置設定為 HA 成員，則其也可以具有相同的分支憑證。
     - 如果中樞裝置在 VPN 叢集之間通用，則這些 VPN 叢集的分支裝置憑證應該具有所有屬性都具有唯一值的唯一憑證。如果您不確定憑證和其值的唯一性，則提交將會在中樞裝置上失敗（Panorama 上未出現提交失敗）。

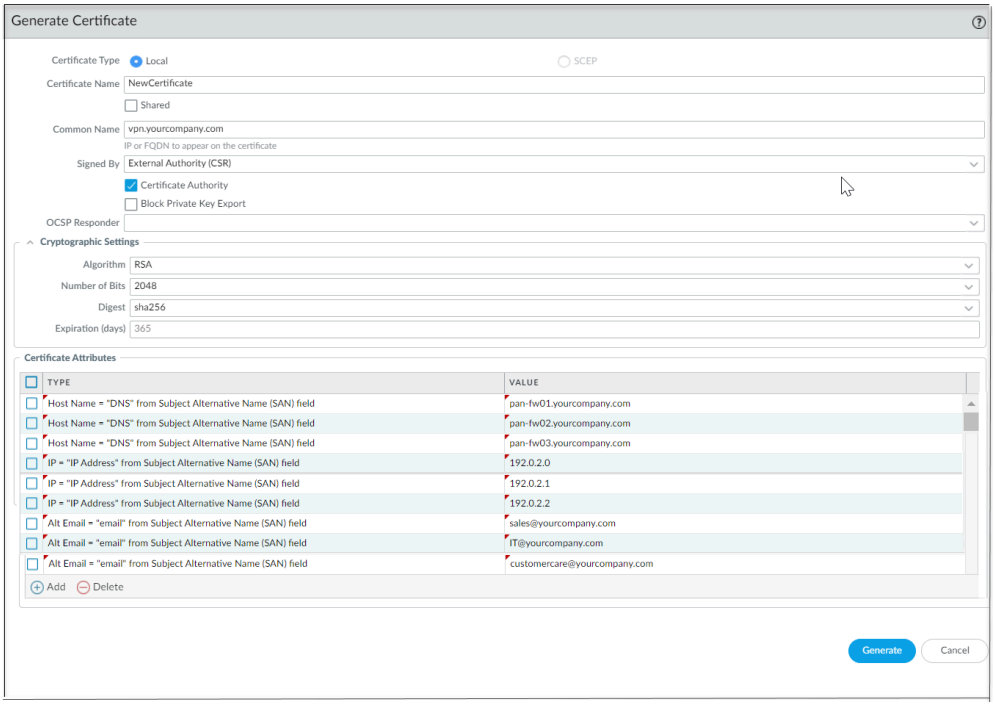
       也請確定所產生用於 *SD-WAN* 通道驗證的分葉憑證（分支和中樞防火牆憑證）符合下列準則：

       - 金鑰使用應該有數位簽章。
       - 所有憑證都必須由相同根 *CA* 進行簽署。
       - 裝置憑證必須由根 *CA* 直接進行簽署。
       - 憑證格式應該為 *PKCS12*。

- 憑證屬性用於判斷 IKE 閘道的本機 ID 和對等 ID。因此，必須使用下列三個憑證屬性來產生分葉憑證（即用於 SD-WAN 通道驗證的分支和中樞防火牆憑證），而且每個憑證屬性都應該獲指派三個唯一屬性值。否則，將會擲回提交錯誤。
  - FQDN（**Host Name**（主機名稱））
  - IP address（IP 位址）**(IP)**
  - User FQDN（使用者 FQDN）（**Alt Email**（替代電子郵件））

  所有憑證都必須具有唯一 ***Host Name***（主機名稱）、***IP*** 和 ***Alt Email***（替代電子郵件）憑證屬性。即，所有憑證都不應該共同具有這些屬性值。

  在下面的範例中，所產生的 NewCertificate 共有九個必要憑證屬性。**Host Name**（主機名稱）憑證屬性已設定三個唯一屬性值：pan-fw01.yourcompany.com、pan-fw02.yourcompany.com 和 pan-fw03.yourcompany.com。**IP** 憑證屬性已設定三個唯一屬性值：192.0.2.0、192.0.2.1 和 192.0.2.2。**Alt Email**（替代電子郵件）憑證屬性已設定三個唯一屬性值：sales@yourcompany.com、IT@yourcompany.com 和 customercare@yourcompany.com。



2. （選用）選擇 **Certificate Profile**（憑證設定檔）。憑證設定檔包含如何驗證對等閘道的相關資訊。
3. （選用）若要嚴格控制金鑰的使用方式，請 **Enable strict validation of peer's extended key use**（對對等的擴充金鑰使用方法啟用嚴格驗證）。

STEP 14 | （選用）設定 BGP 路由。

要在 VPN 叢集成員之間自動設定 BGP 路由，請在下面輸入 BGP 資訊。如果您想要在每個防火牆上手動設定 BGP 路由，或使用單獨的 Panorama 範本來設定 BGP 路由以獲得更多控制權，請將下面的 BGP 資訊留空。

在 *BGP* 已經投入使用的環境中實作帶有 *BGP* 路由的 *SD-WAN* 之前，請確保 *SD-WAN* 外掛程式產生的 *BGP* 設定不會與您預先存在的 *BGP* 設定衝突。例如，您必須使用現有的 *BGP AS* 號碼和路由器 *ID* 值來表示相應的 *SD-WAN* 裝置值。如果外掛程式產生的 *BGP* 設定與您現有的 *BGP* 設定衝突，則優先選用現有的 *BGP* 設定。如果您希望優先選用推送的設定，則必須在進行 *Panorama* 推送時啟用強制範本值。

1. 選取 **BGP** 索引標籤並啟用 **BGP** 以便為 SD-WAN 流量設定 BGP 路由。
2. 輸入 BGP 路由器 **ID**，在所有的路由器當中必須是唯一的。
3. 輸入 **AS** 號碼。自治號碼指定了通常定義的到網際網路的路由原則。AS 號碼必須對每個中樞和分支位置都是唯一的。

STEP 15 | 若要將 BGP 設定為使用 IPv4，請選取 **IPv4 BGP**。不論您的 BGP 環境僅是 IPv4 還是雙重堆疊（IPv4 和 IPv6），您都必須啟用 IPv4 BGP。

1. 啟用 **IPv4 BGP** 支援。

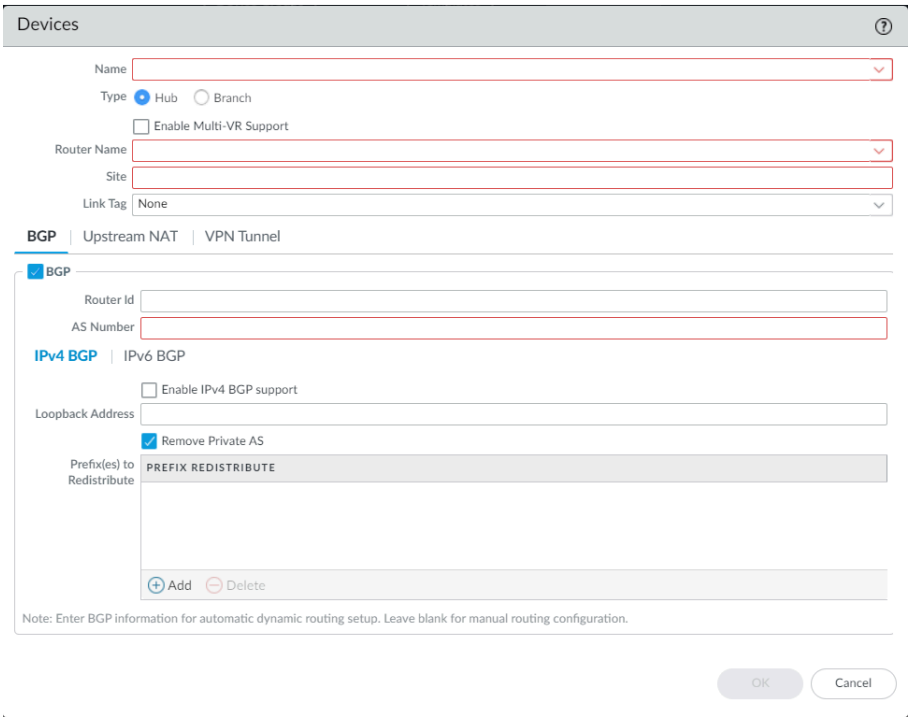
   針對已升級的設定（已存在的 *SD-WAN IPv4* 設定），預設會選取 ***Enable IPv4 BGP support***（啟用 ***IPv4 BGP*** 支援）。否則，明確地 ***Enable IPv4 BGP support***（啟用 ***IPv4 BGP*** 支援）。
2. 為 BGP 對等指定一個靜態 IPv4 回送位址。Auto VPN 組態會使用指定的 IPv4 位址自動建立一個回送介面。如果您指定現有回送位址，則提交將會失敗，因此，您必須指定目前還不是回送位址的 IPv4 位址。
3. 如果您有終端需要在 SD-WAN BGP 拓撲中與中樞或分支防火牆交換路由，且因此您不想從 BGP 更新中的 AS_PATH 屬性中移除私人 AS 號碼（64512 到 65534），則停用移除

私人 **AS** 選項（預設為啟用）。這種情況下，您希望允許私人 AS 號碼將 SD-WAN 私人 AS 留在 BGP 更新中。

移除私人 ***AS*** 設定適用於分支或中樞防火牆上的所有 *BGP* 對等群組。如果您需要此設定在 *BGP* 對等群組或對等之間有所不同，則必須設定 *SD-WAN* 外掛程式外部的設定。

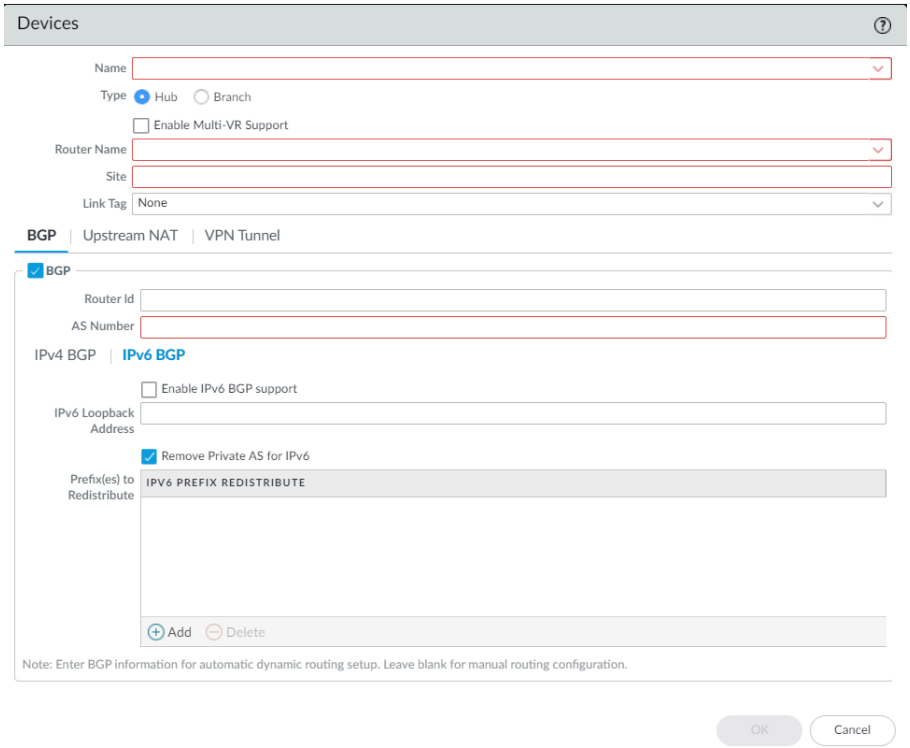
如果您已變更 ***Remove Private AS***（移除私人 ***AS***）設定，並提交至所有 *SD-WAN* 叢集節點，然後降級至 *2.0.2* 之前的 *SD-WAN* 外掛程式版本，則必須在 *SD-WAN* 外掛程式外部或直接在防火牆上執行與 ***Remove Private AS***（移除私人 ***AS***）相關的所有設定。

4. **Add**（新增） **Prefix(es) to Redistribute**（要重新散佈的首碼）。在中樞裝置上，您至少必須透過 SD-WAN 通道來輸入一個要重新散佈的首碼。分支裝置沒有此必要設定需求，因為預設會重新散佈連線到分支位置的子網路。



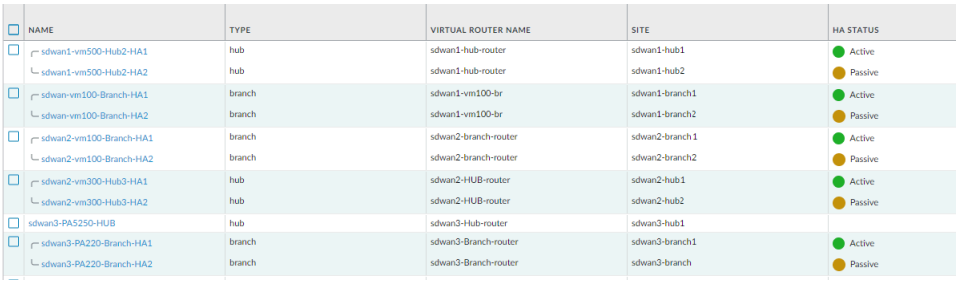
STEP 16 | 若要將 BGP 設定為使用 IPv6，請選取 **IPv6 BGP**。

1. 啟用 **IPv6 BGP** 支援。
2. 為 BGP 對等指定一個靜態 **IPv6** 回送位址。自動 VPN 設定會使用您指定的相同 IPv6 位址來自動建立回送介面。如果您指定現有回送位址，則提交將會失敗，因此，您必須指定目前還不是回送位址的 IPv6 位址。
3. 透過 SD-WAN 通道，**Add**（新增） **Prefix(es) to Redistribute**（要重新散佈的首碼）。在中樞裝置上，您至少必須透過 SD-WAN 通道來輸入一個要重新散佈的首碼。分支裝置沒有此必要設定需求，因為預設會重新散佈連線到分支位置的子網路。



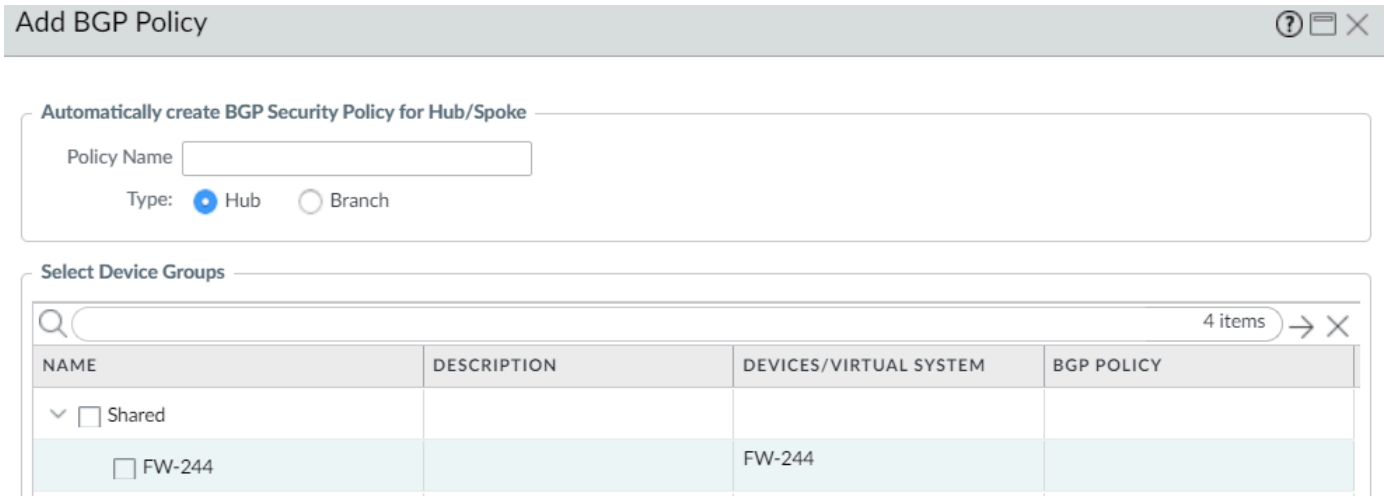
STEP 17 | 按一下 **OK**（確定）。

STEP 18 | 選取螢幕底部的 **Group HA Peers**（群組 **HA** 對等）以顯示同時作為 HA 對等的分支（或中樞）。



STEP 19 | 讓 Panorama 建立一個安全性原則規則並推送到防火牆，該規則允許 BGP 在分支和中樞之間執行。

1. 在螢幕底部，選取 **IPv4 BGP Policy**（**IPv4 BGP** 政策）或 **IPv6 BGP Policy**（**IPv6 BGP** 政策），然後 **Add**（新增）政策規則。
2. 為 Panorama 將自動建立的安全性原則規則輸入一個原則名稱。
3. 選取 **Type**（類型）作為 **Hub**（中樞）或 **Branch**（分支）。
4. 選取裝置群組以指定 Panorama 將向其推送安全性原則規則的裝置群組。
5. 按一下 **OK**（確定）。



STEP 20 | 選取 **Push to Devices**（推送到裝置）以將您的組態變更推送到受管理的防火牆。

批量匯入多台 SD-WAN 裝置

新增多台 SD-WAN 裝置以快速裝載分支和中樞防火牆，而不是每次手動新增一個裝置。在新增裝置時，您需要指定裝置的類型（分支還是中樞），還要為每個裝置提供網站名稱以便輕鬆識別。新增裝置之前，請規劃 SD-WAN 設定，以確保您擁有所有必需的 IP 位址，而且瞭解 SD-WAN 拓撲。這可幫助減少組態錯誤。

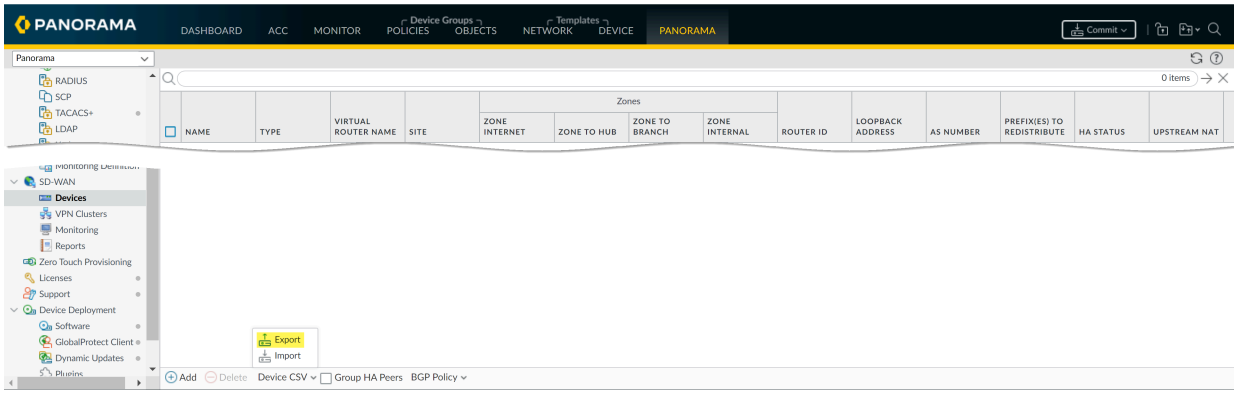
如果您想要在兩個分支防火牆或兩個中樞防火牆上執行主動/被動 *HA*，則不要在 *CSV* 檔案中將這些防火牆新增為 *SD-WAN* 裝置。您將在您為 SD-WAN 設定 HA 裝置時將其單獨新增為 *HA* 對等。

如果您要使用 *BGP* 路由，則必須新增安全性政策規則，以允許 *BGP* 從內部區域到中樞區域，以及從中樞區域到內部區域。如果您想要使用 *4-byte* 自治號碼 *(ASN)*，您必須先為虛擬路由器啟用 *4-byte ASN*。

如果您的 Palo Alto Networks 防火牆具有預先存在的區域，則您要將其對應至 SD-WAN 中所使用的預先定義區域。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置） > **Device CSV**（裝置 **CSV**），並 **Export**（匯出）一個空 SD-WAN 裝置 CSV。CSV 允許您一次匯入多個分支和中樞裝置，而不是手動新增每個裝置。



STEP 3 | 使用分支和中樞資訊填充 SD-WAN 裝置 CSV 並儲存 CSV。除非另有說明，否則所有必填欄位都必須填寫。針對每個中樞和分支，輸入下列資訊：

- **device-serial**（裝置序號）—分支或中樞防火牆的序號。
- **type**（類型）—指定裝置是分支還是中樞。
- **site**（網站）—輸入 SD-WAN 裝置網站名稱，助您識別裝置的地理位置或目標。

  SD-WAN 網站名稱支援所有大寫和小寫字母數字字元和特殊字元。網站名稱中不支援空格，如果使用，則會導致該網站的監控（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控））資料無法顯示。

  所有 *SD-WAN* 裝置（包括高可用性 *(HA)* 設定中的 *SD-WAN* 裝置）都必須具有唯一的網站名稱。
- **router-name**—輸入要用於在 SD-WAN 中樞與分支之間進行路由傳送的虛擬路由器。根據預設，Panorama 會建立 `sdwan-default` 虛擬路由器，並讓 Panorama 自動推送路由器設定。
- **vif-link-tag**—指定連結標籤，以在應用程式和服務於 SD-WAN 流量散佈和容錯移轉期間使用此連結時識別中樞。
- （選用）**router-id**（路由器 **ID**）—指定 BGP 路由器 ID，這必須在所有的虛擬路由器或邏輯路由器中是唯一的。

  輸入回送位址作為路由器 *ID*。

  在 *BGP* 已經投入使用的環境中實作帶有 *BGP* 路由的 *SD-WAN* 之前，請確保 *SD-WAN* 外掛程式產生的 *BGP* 設定不會與您現有的 *BGP* 設定衝突。例如，您必須使用現有的 *BGP AS* 號碼和路由器 *ID* 值來表示相應的 *SD-WAN* 裝置值。
- （選用）**as-number**（自治號碼）—輸入中樞或分支上虛擬路由器所屬的專用 AS 的ASN。SD-WAN 外掛程式僅支援專用自治系統。ASN 必須對每個中樞和分支都是

唯一的。4-byte ASN 範圍為 4,200,000,000 到 4,294,967,294 或 64512.64512 到 65535.65534。2-byte ASN 範圍為 64512 到 65534。

使用 *4-byte* 專用 *ASN*。

在 *BGP* 已經投入使用的環境中實作帶有 *BGP* 路由的 *SD-WAN* 之前，請確保 *SD-WAN* 外掛程式產生的 *BGP* 設定不會與您現有的 *BGP* 設定衝突。例如，您必須使用現有的 *BGP AS* 號碼和路由器 *ID* 值來表示相應的 *SD-WAN* 裝置值。

- （選用）**ipv4-bgp-enable**—指定 yes 或 no，以啟用或停用 IPv4 位址的 BGP。
- （選用）**loopback-address**—指定用於 BGP 對等處理的靜態回送 IPv4 位址。SD-WAN 外掛程式 3.1.1 和更新 3.1 版本支援用於 BGP 對等處理的 IPv6 回送位址。
- （選用）**remove-private-as**—如果您的端點需要在 SD-WAN BGP 拓撲中與中樞或分支防火牆交換路由，而且因此您不想要從 BGP 更新的 AS_PATH 屬性中移除私人 AS 號碼（64512 到 65534），則指定 no 以停用 [Remove Private AS（移除私人 AS）] 選項（預設予以啟用）。

  此設定適用於分支或中樞防火牆上的所有 BGP 對等群組。如果您需要此設定在 BGP 對等群組或對等之間有所不同，則必須設定 SD-WAN 外掛程式外部的設定。
- （選用）**prefix-redistribute**（前置詞重新散佈）—輸入分支通知中樞它可以到達的 IP 前置詞。如要新增多個前置詞，請使用一個空格、一個 & 符號和一個空格來分隔，如 192.2.10.0/24 & 192.168.40.0/24。預設情況下，分支防火牆會將所有本機連線的網際網路前置詞通知到中樞。

  Palo Alto Networks 不會重新散佈從 *ISP* 處學到的分公司預設路由。
- （選用）**ipv6-bgp-enable**—指定 yes/no，以啟用/停用 IPv6 位址的 BGP。
- （選用）**ipv6-loopback-address**—指定用於 BGP 對等處理的靜態回送 IPv6 位址。
- （選用）**ipv6-prefix-redistribute**—輸入 IPv6 首碼，以從分支重新散佈到中樞路由器。根據預設，所有本機連線的網際網路 IPv6 首碼都會公告至中樞位置。
- （選用）**copy-tos-header**—指定 yes/no 來啟用/停用此選項，以將 [Type of Service（服務類型 - ToS）] 標頭從封裝封包的內部 IP 標頭複製至外部 IP 標頭，以保留原始 ToS 資訊。
- **authentication-type**—指定裝置（中樞或分支）所支援的驗證類型：預先共用金鑰或憑證驗證。
- （僅適用於 **Certificate**（憑證）驗證類型）**certificate-name**—輸入憑證名稱。名稱區分大小寫，而且防火牆上最多可以有 63 個字元，或 Panorama 上最多可以有 31 個字元。名稱必須是唯一的，且只能使用字母、數字、連字號與底線。

  針對預先共用金鑰驗證類型，此欄位應該空白。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	device-serial	type	site	router-name	vif-link-tag	router-id	as-number	ipv4-bgp-enable	loopback-addres	remove-private-a	prefix-redistribut	ipv6-bgp-enable	ipv6-loopback-a	ipv6-prefix-redis	copy-tos-he	authentication-ty	certificate-name
2		hub	hub1	hub_VR			65520			yes						pre-shared-key	
3		branch	branch	branch_VR			65501			yes						pre-shared-key	
4		branch	siteC	branch_VR			65502			yes						certificate	brcert1_cacert
5		hub	siteA	hub_VR			65525			yes						certificate	hub_cacert
6																	

STEP 4 | 將 SD-WAN 裝置 CSV 匯入到 Panorama。

確認 Panorama 上沒有擱置中的提交或匯入失敗。

1. 在 Panorama 上，選取 **Panorama** > **SD-WAN** > **Devices**（裝置） > **Device CSV**（裝置 **CSV**），並 **Import**（匯入）您在上一步中編輯的 CSV。
2. **Browse**（瀏覽）並選取 SD-WAN 裝置 CSV。
3. 按一下 **OK**（確定）匯入 SD-WAN 裝置。

STEP 5 | 確認您的 SD-WAN 裝置已成功新增。

NAME	TYPE	ROUT... NAME	SITE	LINK TAG	ROUT... ID	IPV4 LOOP... ADDR...	IPV6 LOOP... ADDR...	AS NUMB...	REMO... PRIVA... AS (IPV4)	REMO... PRIVA... AS (IPV6)	IPV4 PREFI... TO REDIS...	IPV6 PREFI... TO REDIS...	HA STATUS	UPSTR... NA...	Prisma Access Onboarding				AUTH...	CERTI... NAME	CERTI... EXPIRY
															INTER...	TENA...	REGIO...	IPSEC TERMI... NODE			
Hub254-2	hub	hub_VR	hub1	hub_tag				65432	true	true									Pre Shared Key		
Branch50-2	branch	branch...	branch					65433	true	true									Pre Shared Key		
Branch25-2	branch	branch...	siteC					64543	true	true									Certifi...	brcert...	Sep 18 00:45:... 2024 GMT
Branch20-2	hub	hub_VR	siteA					64532	true	true									Certifi...	hub_c...	Sep 18 00:49:... 2024 GMT

STEP 6 | **Commit**（提交）組態變更。

STEP 7 | 選取 **Push to Devices**（推送到裝置）以將您的組態變更推送到受管理的防火牆。

將 PAN-OS 防火牆裝載到 Prisma Access

SD-WAN 外掛程式 2.2 提供 Prisma Access 中樞支援，其中，連線至 Prisma Access 計算節點 (CN) 的 PAN-OS 防火牆會在 SD-WAN 中樞和支點拓撲中實現雲端型安全性。在此拓撲中，SD-WAN 中樞是 Prisma Access CN（IPSec 終端節點），SD-WAN 分支是 PAN-OS 防火牆。最多支援四個中樞（參與 DIA AnyPath 和 Prisma Access 中樞的 PAN-OS 中樞的任意組合）。SD-WAN 自動建立 IKE 和 IPSec 通道，將分支連線至中樞。檢閱 SD-WAN 和 Prisma Access 的系統要求。

請務必先設定 *Prisma Access*，然後再設定 *SD-WAN*。

- 如果您要開始全新的 *Prisma Access* 設定，則請閱讀 Prisma Access 管理員指南，然後完成第 *1* 階段和第 *2* 階段設定步驟。
- 如果您已經在執行 *Prisma Access*，請確保第 *1* 階段已完成，然後完成第 *2* 階段。

以下流程圖顯示了兩個設定階段的順序以及每個階段中的基本步驟。帶有連結的完整 Prisma Access 先決條件和 SD-WAN 的設定步驟遵循流程圖。

第 1 階段—PRISMA ACCESS	第 2 階段—SD-WAN
（先完成第 **1** 階段）	（在完成第 **1** 階段後才開始）
1. 為租用戶設定基礎結構子網路、基礎結構 BGP AS、範本堆疊和裝置群組。 2. 為特定區域設定範本堆疊、範本、裝置群組、信任和不受信任的區域以及頻寬配置。	1. 使用啟用了 SD-WAN 的介面設定分支防火牆。 2. 登入 Panorama 網頁介面。 3. 指定回送位址的 BGP 本機位址集區。

第 1 階段—PRISMA ACCESS	第 2 階段—SD-WAN
（先完成第 1 階段）	（在完成第 1 階段後才開始）
3. 確保您的 Prisma Access 部署已獲得遠端網路授權。 4. 確保您的部署按計算位置配置頻寬，而不是按位置配置。 5. 確保您已將頻寬指派給與您要裝載的位置相對應的計算位置。 6. 執行本機提交並推送到 Prisma Access 雲端。	4. 選取 SD-WAN 分支防火牆以連線至 Prisma Access 中樞並設定連線。 5. 提交並推送設定到雲端。 6. 確認裝載完成。 7. 將分支防火牆同步到 Prisma Access。 8. 提交至 Panorama。 9. 推送到裝置。 10. 檢視建立的新介面。 11. 確認 IPSec 通道已啟動。 12. 確認 IKE 閘道已啟動。 13. 建立 SD-WAN 政策規則以產生監控資料。 14. 提交然後提交並推送到分支防火牆。 15. 監控 Prisma Access 中樞應用程式和連結效能。

在將 SD-WAN 連線至 Prisma Access 之前，您必須有介面已啟用 SD-WAN 的分支防火牆。此外，確保您已為一個或多個租用戶執行以下 Prisma Access 先決條件；這些是第 1 階段的步驟：

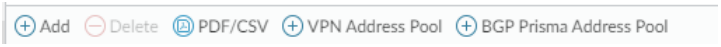
1. 對於 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定），在 **Service Setup**（服務設定）頁面上為租用戶設定基礎結構子網路、基礎結構 BGP AS、範本堆疊和裝置群組。
2. 在 **Remote Networks**（遠端網路）頁面上，為特定區域設定範本堆疊、範本、裝置群組、信任和不受信任的區域以及頻寬配置。
3. 確定您的 Prisma Access 部署已取得遠端網路的授權，方法是選取 **Panorama** > **Licenses**（授權），然後檢查授權資訊。
   - 2020 年 11 月 17 日之後可用的授權會在 **Net Capacity**（淨容量）區域中顯示可用於遠端網路的授權頻寬數量。
   - 2020 年 11 月 17 日之前可用的授權會在 **Total Mbps**（總 **Mbps**）下方的 **GlobalProtect Cloud Service for Remote Networks**（遠端網路的 **GlobalProtect** 雲端服務）區域中顯示可用的遠端網路頻寬。
4. 確保您的部署按計算位置配置頻寬，而不是按位置配置。
5. 確保您已將頻寬指派給與您要裝載的位置相對應的計算位置。Prisma Access 為您配置給區域的每 500 Mbps 頻寬配置一個 IPSec 終端節點。
6. 執行本機提交並推送到 Prisma Access 雲端。

在您使用 Prisma Access 執行第 1 階段的上述步驟後，對 SD-WAN 執行以下第 2 階段步驟。

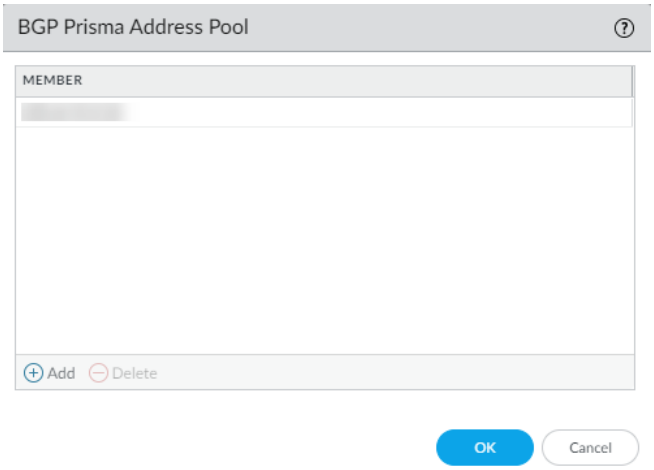
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 指定回送位址的 BGP 本機位址集區。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集）。
2. 在螢幕底部，選取 **BGP Prisma Address Pool**（**BGP Prisma** 位址集區）。



3. 為 Prisma Access 的本機 BGP 位址 **Add**（新增）一個未使用的私人子網路（首碼和網路遮罩）。



4. 按一下 **OK**（確定）。
5. **Commit**（認可）。

如果已裝載 *Prisma Access*，請勿簡單地變更現有的位址集區。如果您需要變更位址集區，請在維護期間執行下列步驟，以將位址集區變更更新至 *SD-WAN* 分支和 *Prisma Access CN*：

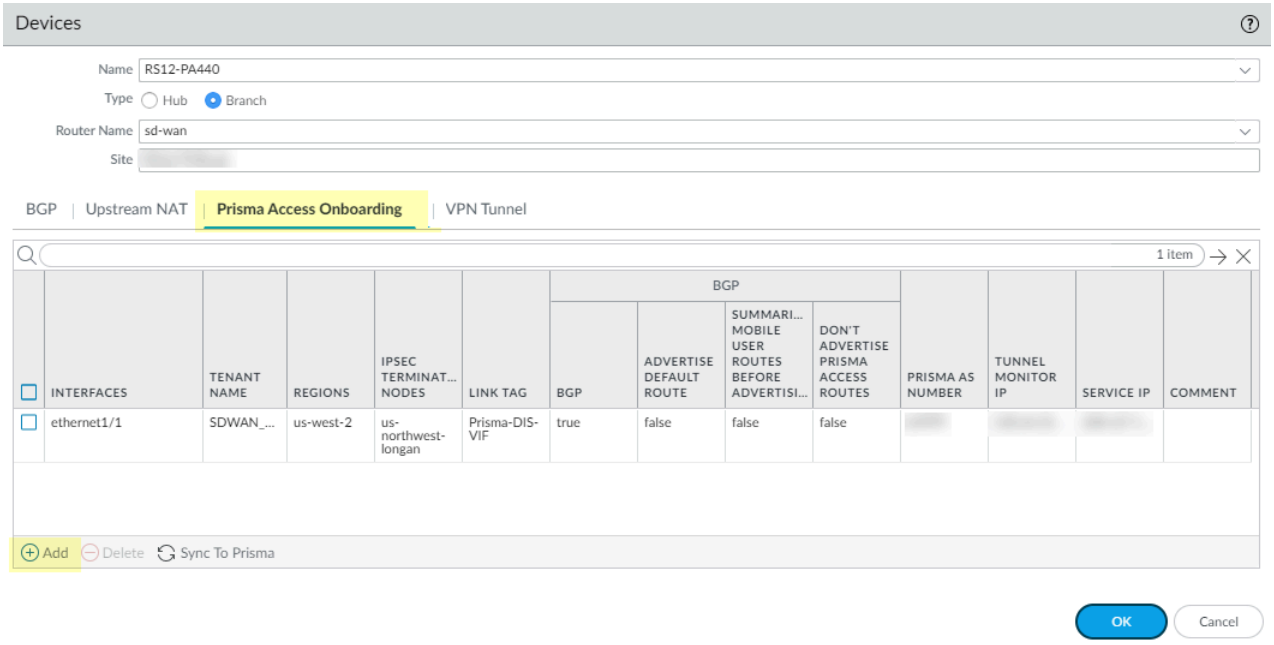
1. 使用 *Panorama* 存取 *SD-WAN* 分支並刪除將受位址集區變更影響的現有裝載；然後執行本機提交。
2. 更新 *VPN* 位址集區，然後執行本機提交。
3. 再次執行 *Prisma Access* 裝載，然後執行本機提交和推送。

STEP 3 | 選取 SD-WAN 分支防火牆以連線至 Prisma Access 中樞並設定連線。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置）。
2. 選取已啟用 SD-WAN 的分支防火牆，其名稱隨後會填入 **Name**（名稱）欄位。
3. 選取裝置 **Type**（類型）作為 **Branch**（分支）。
4. 選取 **Router Name**（路由器名稱）。
5. 輸入 **Site**（網站）。

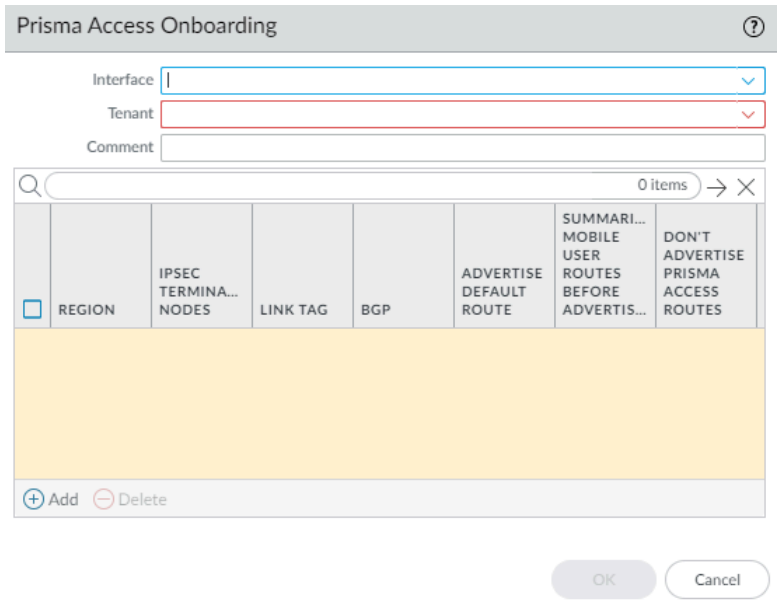
   所有 *SD-WAN* 裝置都必須具有唯一的網站名稱。

6. 選取 **Prisma Access Onboarding**（**Prisma Access** 裝載）和 **Add**（新增）。



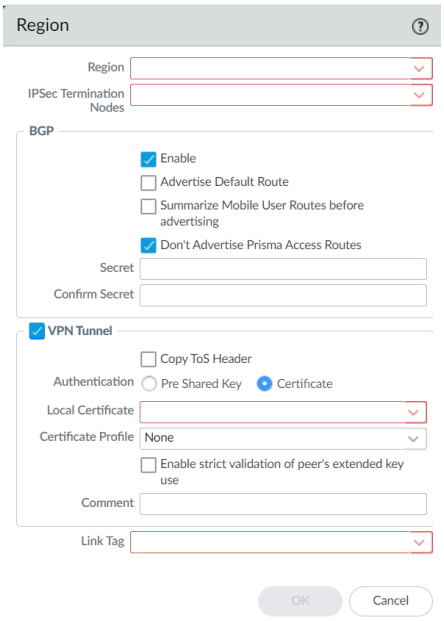
7. 在防火牆上選取一個已啟用 SD-WAN 的本機 **Interface**（介面）以連線至 Prisma Access 中樞。
8. 選取一個 Prisma Access **Tenant**（租用戶）（為單一租用戶環境選取 **default**（預設值））。

   分支防火牆上的所有 SD-WAN 介面都必須使用相同的 Prisma Access 租用戶。
9. 輸入有用的 **Comment**（註解）。



10. 透過選取 CN（Prisma Access 中樞）所在的區域，將計算節點 **Add**（新增）至 **Region**（區域）。

    每個介面可以有多個區域。



11. 從節點清單中選取一個 **IPSec Termination Node**（**IPSec** 終端節點）（GP 閘道）；該清單基於 Prisma Access 之前為該區域啟動的節點。您正在選擇該分支所連線的中樞。SD-WAN 自動 VPN 設定與此節點建立 IKE 和 IPSec 關係和通道。
12. **Enable**（啟用）BGP 以在分支和中樞之間進行通訊（依預設啟用）。
13. **Advertise Default Route**（公告預設路由）可允許將 Prisma Access 中樞的預設路由公告至分支防火牆。

14. **Summarize Mobile User Routes before advertising**（在公告之前摘要行動使用者路由）可讓 Prisma Access 中樞公告摘要的行動使用者 IP 子網路路由，從而減少向分支機構公告的數量。
15. **Don't Advertise Prisma Access Routes**（不公告 **Prisma Access** 路由）可防止 IPSec 終端節點/中樞將其 Prisma Access 路由公告至 SD-WAN 分支。
16. 輸入用於進行 BGP 通訊驗證的 **Secret**（密碼）並 **Confirm Secret**（確認密碼）。
17. （SD-WAN 外掛程式 3.2.0 和更新版本）設定 VPN 通道參數和驗證類型，以驗證 PAN-OS 防火牆和 Prisma Access 中樞。
    1. （選用）如果您想要保留封裝封包中的服務類型 (ToS) 資訊，則請選取 **Copy TOS Header**（複製 **TOS** 標頭）。

       如果通道內有多個工作階段（各有不同的 *ToS* 值），則複製 *ToS* 標頭可能會導致 *IPSec* 封包無序到達。
    2. 選取 **Authentication**（驗證）：**Pre Shared Key**（預先共用金鑰）或 **Certificate**（憑證）。

       確定您針對所有分支裝置和所新增的 *Prisma Access* 裝置選取相同的驗證類型。

       如果選取作為地區的驗證類型，則會自動產生預先共用金鑰。
18. 選取 **Certificate**（憑證），以設定憑證式驗證。
19. （只有在啟用 **Certificate**（憑證）驗證類型時）執行 SD-WAN 分支防火牆的 Prisma Access 裝載之前，憑證必須存在於 Panorama 上。我們不支援 SCEP 產生的憑證。選取 **Local Certificate**（本機憑證）—已在 Panorama 上的憑證。

    確定您在 Panorama 中所具有的憑證符合下列項目，以成功進行 Prisma Access 裝載程序：

    - 針對每個 SD-WAN 裝置，憑證必須是唯一的。即，您無法在多個 SD-WAN 裝置之間共用憑證。

      產生用於 SD-WAN 通道驗證的分支和中樞防火牆憑證時，請記住下列幾點：

      - 兩個不同的中樞裝置可以使用相同的中樞憑證。
      - 如果符合下列條件，則兩個不同的分支裝置可以使用相同的分支憑證：
        - 分支裝置不屬於相同 VPN 叢集
        - 這些分支裝置所屬 VPN 叢集之間沒有通用中樞裝置
      - （僅限 HA 部署）如果兩個不同的分支裝置設定為 HA 成員，則也可以具有相同的分支憑證。
      - 如果中樞裝置在 VPN 叢集之間通用，則這些 VPN 叢集的分支裝置憑證應該具有所有屬性都具有唯一值的唯一憑證。如果您不確定憑證和其值的唯一性，則提交將會在中樞裝置上失敗（Panorama 上未出現提交失敗）。

也請確定所產生用於 *SD-WAN* 通道驗證的分葉憑證（分支和中樞防火牆憑證）符合下列準則：

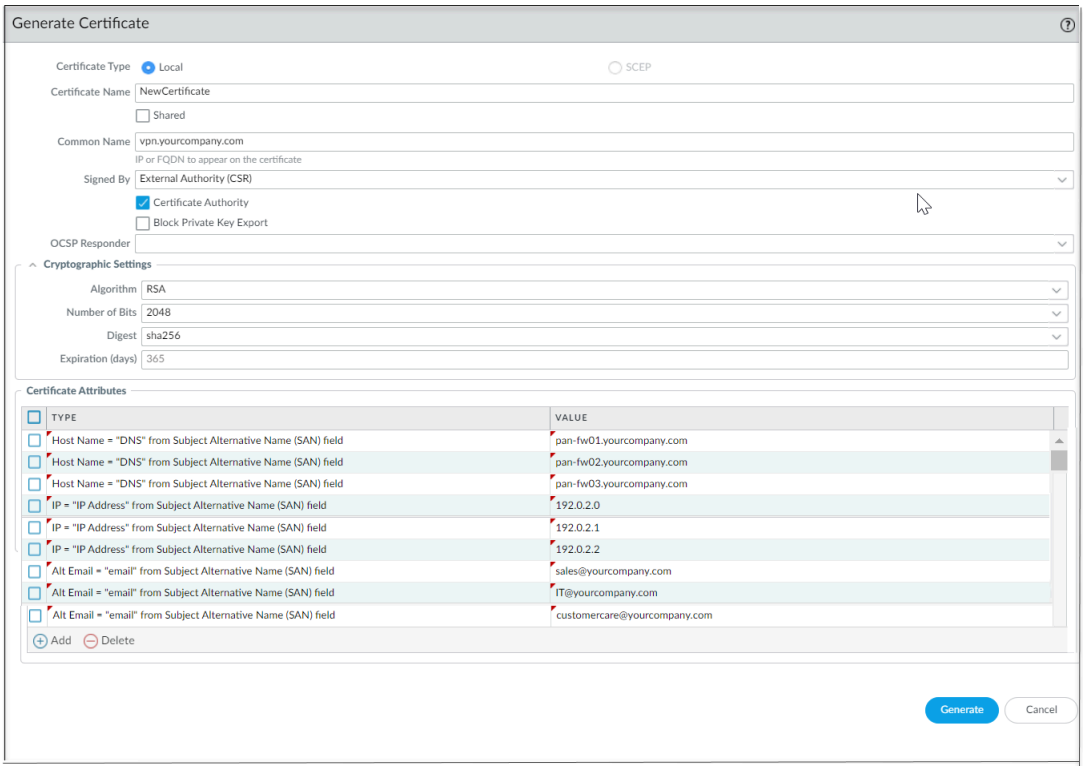
- 金鑰使用應該具有數位簽名
- 所有憑證都必須由相同的根 *CA* 進行簽署
- 裝置憑證必須由根 *CA* 直接進行簽署
- 憑證格式應該為 *PKCS12*

- 憑證屬性用於判斷 IKE 閘道的本機 ID 和對等 ID。因此，必須使用下列三個憑證屬性來產生分葉憑證（即用於 SD-WAN 通道驗證的分支和中樞防火牆憑證），而且每個憑證屬性都應該獲指派三個唯一屬性值。否則，將會擲回提交錯誤。
  - FQDN (**Host Name**（主機名稱）)
  - IP 位址 (**IP**)
  - 使用者 FQDN (**Alt Email**（替代電子郵件）)

  所有憑證都必須具有唯一 ***Host Name***（主機名稱）、***IP*** 和 ***Alt Email***（替代電子郵件）憑證屬性。即，所有憑證都不應該共同具有這些屬性值。

  在下面的範例中，所產生的 NewCertificate 共有九個必要憑證屬性。**Host Name**（主機名稱）憑證屬性已設定三個唯一屬性值：pan-fw01.yourcompany.com、pan-fw02.yourcompany.com 和 pan-fw03.yourcompany.com。**IP** 憑證屬性已設定三個唯一屬性值：192.0.2.0、192.0.2.1 和 192.0.2.2。**Alt Email**（替代電子郵件）憑證

屬性已設定三個唯一屬性值：sales@yourcompany.com、IT@yourcompany.com 和 customercare@yourcompany.com。

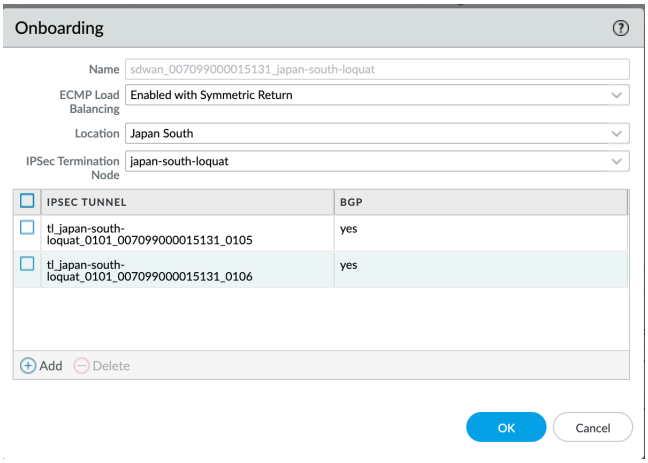


20. （選用）（只有在啟用 **Certificate**（憑證）驗證類型時）選擇 **Certificate Profile**（憑證設定檔）。憑證設定檔包含如何驗證對等閘道的相關資訊。
21. （選用）若要嚴格控制金鑰的使用方式，請 **Enable strict validation of peer's extended key use**（對對等的擴充金鑰使用方法啟用嚴格驗證）。
22. 為中樞選取 **Link Tag**（連結標籤）。

    當您想要為 *Prisma Access* 中樞啟用 *ECMP* 時，將多個分支介面裝載到同一計算節點 *(CN)*，並在這些分支介面上使用相同的連結標籤。
23. 按一下 **OK**（確定）。顯示內容將包括對等 AS 號碼和 Prisma Access 提供的通道監控 IP 位址。

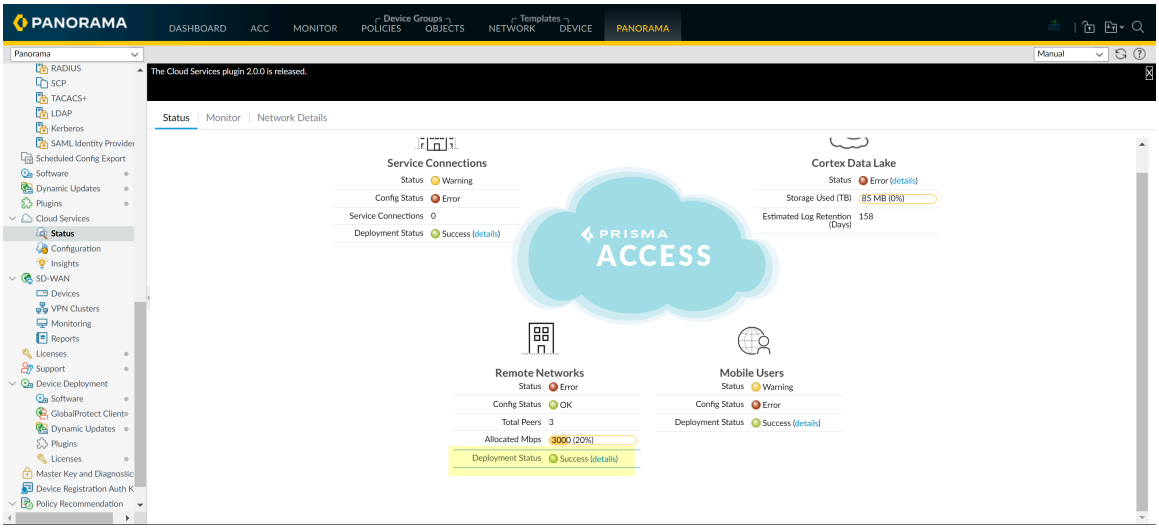
STEP 4 | 將設定 **Commit and Push**（提交並推送）至雲端，Prisma Access 根據要求的頻寬啟動正確數量的 IPSec 終端節點。

當多個 *IPSec* 通道進入同一個 *CN* 時，*Prisma Access* 設定透過對稱傳回啟用了 *ECMP*，如此 *Prisma Access* 範例所示：

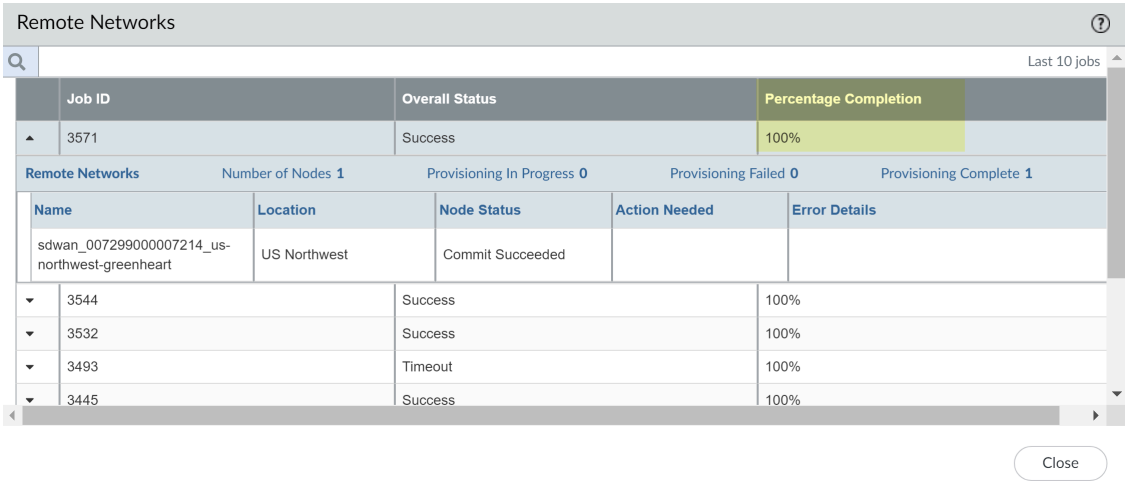


STEP 5 | 確認裝載完成。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態）並確認遠端網路部署狀態顯示為 success。



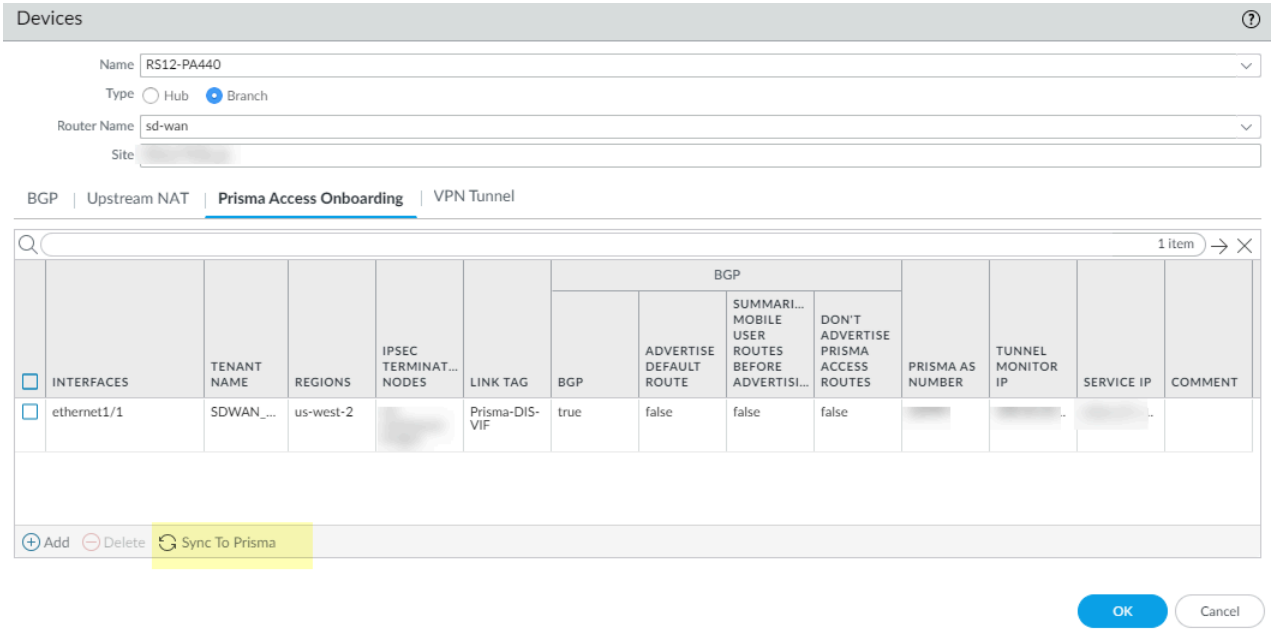
2. 選取遠端網路部署狀態 **details**（詳細資訊）。
3. 確認 Prisma Access 節點完成顯示 100%。



STEP 6 | 將分支防火牆同步到 Prisma Access 以擷取 CN 的服務 IP 位址。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置）。
2. 選取 SD-WAN 分支裝置。
3. 選取 **Prisma Access Onboarding**（**Prisma Access** 裝載）和 **Sync To Prism**（同步至 **Prism**）（並回應訊息以繼續）。對每個分支裝置重複此動作。

成功同步至 *Prisma* 後，您將在 *SD-WAN* 分支防火牆上看到 *Prisma Access* 設定參數。如果沒有，請等待大約 *15* 分鐘，然後重複 *Sync to Prisma*（同步至 *Prisma*）。如有必要，前往 *Prisma Access* 外掛程式並確認 *CN* 裝載已完成（您可以看到指派了頻寬和 *IP* 位址的 *CN*）。確認後，重試 *Sync to Prisma*（同步至 *Prisma*）。



STEP 7 | **Commit**（提交）至 Panorama。

STEP 8 | **Push to Devices**（推送到裝置） 可推送到本機分支防火牆。**Edit Selections**（編輯選擇）可選取推送範圍選擇。選取正確的 **Template**（範本）和 **Device Group**（裝置群組）。

STEP 9 | 在分支防火牆上，選取 **Network**（網路） > **Interfaces**（介面） > **SD-WAN** 並查看使用您建立的連結標籤建立、指派給名為 **zone-to-pa-hub** 的安全性地區，並具有連接至 CN 的 IPSec 通道的新介面。

STEP 10 | 選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道）並確認 IPSec 通道已啟動。

STEP 11 | 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）並確認 IKE 閘道已啟動。

STEP 12 | 建立 SD-WAN 政策規則以產生監控資料。

需要執行此步驟來對 Prisma Access Hub 延遲、抖動和封包遺失資料進行基準測量，以實現準確的流量散佈。SD-WAN 監控資料從符合您的 SD-WAN 政策規則的流量中產生。

1. 建立流量散佈設定檔。
2. 建立路徑品質設定檔具有高延遲、抖動和封包遺失閾值。

   需要路徑品質設定檔，才能建立 SD-WAN 政策規則。建立具有高閾值的路徑品質設定檔允許您對 Prisma Access 中樞的延遲、抖動和封包遺失進行基準測量，而不會導致應用程式切換至不同的連結。
3. 設定 SD-WAN 原則規則.

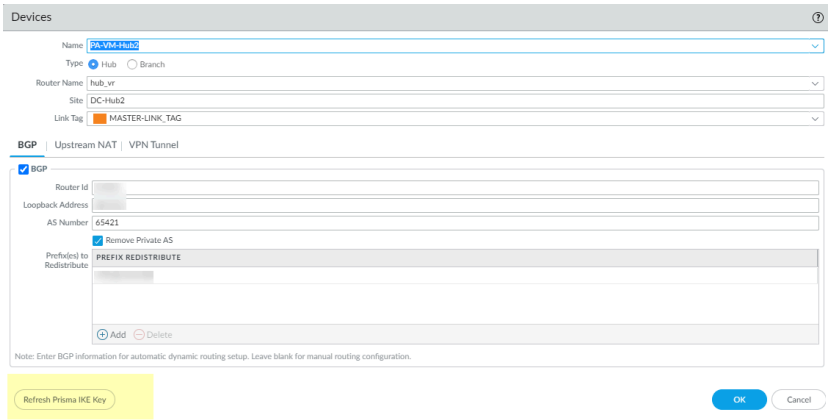
STEP 13 | **Commit**（提交）和 **Commit and Push**（提交並推送）到分支防火牆。

STEP 14 | （只有在啟用 **Pre Shared Key**（預先共用金鑰）驗證類型時）重新整理 Prisma IKE 預先共用金鑰。

如果您需要變更目前用於保護分支與 *Prisma* 中樞間之 *IPSec* 連線的 *Prisma IKE* 金鑰，則請執行此步驟以隨機產生通道的新金鑰，並更新通道的兩側。當中樞和分支不忙碌時執行此步驟。

請勿手動建立名稱以「*gw-*」開頭的 *IKE* 閘道，因為此類名稱會保留在裝載期間建立 *Prisma IKE* 時使用。這個重新整理 *Prisma IKE* 預先共用金鑰的步驟會重新整理所有這類名稱的 *IKE* 閘道（如果具有 *Prisma Access* 所建立的 *IKE* 閘道以外的任何 *IKE* 閘道）。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後選取裝置。
2. 在螢幕底部，選取 **Refresh Prisma IKE Key**（重新整理 **Prisma IKE** 金鑰）。



3. 將出現一則訊息，通知您重新整理 `IKE` 金鑰將更新分支和 `Prisma Access` 中樞之間的所有 `SD-WAN` 通道，並且需要同時將設定推送到所有分支和 `Prisma Access` 中樞裝置。最佳做法建議是在維護期間執行重新整理，因為流量可能會受到影響。您要繼續嗎？如果您想要繼續，則選取 `Yes`。

STEP 15 | **Commit**（提交）和 **Commit and Push**（提交並推送）到分支防火牆。

STEP 16 | 監控 Prisma Access Hub 應用程式和連結效能以瞭解 Prisma Access 連結的延遲、抖動和封包遺失基準。

需要執行此步驟來收集準確的延遲、抖動和封包遺失資料，以微調您的 Prisma Access 中樞路徑品質設定檔。

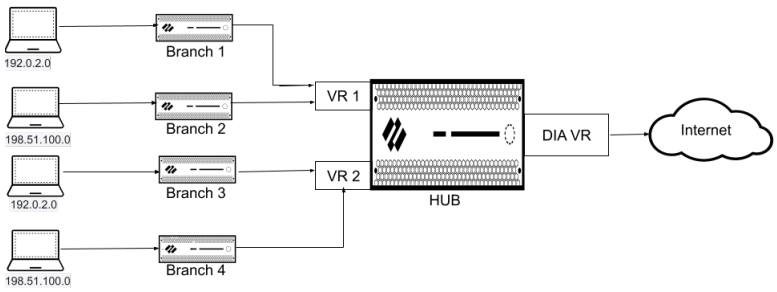
在 SD-WAN 中樞上設定多個虛擬路由器

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

（PAN-OS 11.1.3 和更新版本，以及 SD-WAN 外掛程式 3.2.1 和更新版本）我們已引進 SD-WAN 中樞上的多個虛擬路由器支援，而此功能可讓您在連線至相同 SD-WAN 中樞的分支裝置上具有重疊的 IP 子網路位址。使用此功能時，您可以有多個具有重疊子網路的邏輯路由網域。當您啟用此功能時，只有在重疊子網路位於不同的虛擬路由器時，SD-WAN 中樞才支援重疊子網路。

根據預設，會停用 SD-WAN 中樞上的多個虛擬路由器。

下圖展示具有兩個虛擬路由器的 SD-WAN 中樞。在 SD-WAN 中樞上啟用多個虛擬路由器支援，四個連線至相同 SD-WAN 中樞的分支即可具有重疊的 IP 子網路，或屬於不同的實體，並獨立運作，因為其流量會流向不同的虛擬路由器。



SD-WAN 中樞防火牆和 Prisma Access 中樞上都支援多虛擬路由器功能。分支連線至已啟用多虛擬路由器功能的內部部署中樞時，您可以將 Prisma Access 從分支裝載為中樞。

設定多個虛擬路由器，同時新增 SD-WAN 中樞防火牆（**Panorama** > **SD-WAN** > **Devices**（裝置））。

匯入 SD-WAN 裝置時，不支援使用 CSV 檔案來匯入多個虛擬路由器相關設定。

在 SD-WAN 中樞上啟用多個虛擬路由器時，我們支援進階路由。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後 **Add**（新增）新的 SD-WAN 防火牆。

建立中樞範本時，請新增參與 SD-WAN 中樞的所有虛擬路由器，而在 SD-WAN 中樞上，將啟用多個虛擬路由器。使用 SD-WAN 外掛程式來新增 SD-WAN 裝置之前，您必須執行此作業。建立中樞範本時，請確保分支上的虛擬路由器名稱與中樞上的其中一個虛擬路由器相符。

STEP 3 | 若要在 SD-WAN 中樞上設定多個虛擬路由器：

- 將 SD-WAN 裝置的 **Type**（類型）選取為 **Hub**（中樞）。
- 選取 **Enable Multi-VR Support**（啟用多 **VR** 支援）。

針對 **Virtual Router Name**（虛擬路由器名稱）所選取的虛擬路由器會用作中樞直接網際網路存取 (DIA) 虛擬路由器，並被視為預設虛擬路由器。**BGP** 頁籤下方所指定的設定必須是 DIA 虛擬路由器所特有。

- 在 *SD-WAN* 中樞上啟用多虛擬路由器功能時，我們不支援 *FEC* 和封包複製。
- 只有中樞-支點拓撲才支援 *SD-WAN* 中樞上的多虛擬路由器功能（完整網狀拓撲則不予支援）。
- 若要處理 *SD-WAN* 中樞上的網際網路流量，*SD-WAN* 政策必須確定只有在 *MPLS* 連結具有網際網路存取和 *NAT* 時才會選取 *MPLS* 標籤。
- 在 *SD-WAN* 中樞功能上啟用多虛擬路由器支援時，*PAN-OS* 不支援在 *SD-WAN VPN* 通道外部以純文字轉送流量（在 ***SD-WAN Interface Profile***（***SD-WAN*** 介面設定檔）上停用 ***VPN Data Tunnel Support***（***VPN*** 資料通道支援）時）。

Palo Alto Networks 防火牆上所支援的虛擬路由器數目如下：

Palo Alto Networks 防火牆	支援的最大虛擬路由器數目	支援的最大 **SD-WAN** 中樞虛擬路由器數目
PA-3400	11	10
PA-5220 和 PA-5410	20	20
PA-5250 和 PA-5430	125	50
PA-5420	50	20
PA-5260、PA-5280、PA-5400、PA-5440、PA-5445 和 PA-7000。	225	50

STEP 4 | （選用）設定虛擬路由器。

1. 選取 **Virtual Routers**（虛擬路由器） 頁籤，以針對 SD-WAN 中樞設定多個虛擬路由器。
2. BGP 路由預設會使用 IPv4，因此已啟用 **Enable IPv4 BGP Support**（啟用 **IPv4 BGP** 支援），而且您無法變更此設定。
3. 輸入 **Virtual Router**（虛擬路由器）的名稱。
4. 在中樞範本中，選取適用於您正在設定之虛擬路由器的已建立 **Zone**（區域）（**Network**（網路） > **Zones**（區域））。

   如果您在 ***Multi-VR Configuration***（多 ***VR*** 設定）中針對兩個以上的虛擬路由器設定相同的區域，則請確定虛擬路由器未設定重疊子網路。
5. （選用）輸入虛擬 **Router ID**（路由器 **ID**），而此 ID 在所有路由器中都必須是唯一的。
6. 為 BGP 對等指定一個靜態 IPv4 回送位址。自動 VPN 設定會使用您指定的相同 IPv4 位址來自動建立回送介面。如果您指定一個現有回送位址，提交將失敗。因此您應當指定一個當前不是回送位址的 IPv4 位址。
7. 輸入 **AS** 號碼。自治號碼指定了通常定義的到網際網路的路由原則。AS 號碼必須對每個中樞和分支位置都是唯一的。
8. 如果您有終端需要在 SD-WAN BGP 拓撲中與中樞或分支防火牆交換路由，且因此您不想從 BGP 更新中的 AS_PATH 屬性中移除私人 AS 號碼（64512 到 65534），則停用移除私人 **AS** 選項（預設為啟用）。這種情況下，您希望允許私人 AS 號碼將 SD-WAN 私人 AS 留在 BGP 更新中。

   移除私人 ***AS*** 設定適用於分支或中樞防火牆上的所有 *BGP* 對等群組。如果您需要此設定在 *BGP* 對等群組或對等之間有所不同，則必須設定 *SD-WAN* 外掛程式外部的設定。

   如果您已變更 ***Remove Private AS***（移除私人 ***AS***）設定，並提交至所有 *SD-WAN* 叢集節點，然後後續降級至 *2.0.2* 之前的 *SD-WAN* 外掛程式版本，則必須在 *SD-WAN* 外掛程式外部或直接在防火牆上執行與 ***Remove Private AS***（移除私人 ***AS***）相關的所有設定。
9. 輸入要重新散佈的前置詞。在一個中樞裝置上，您必須輸入至少一個要重新散佈的前置詞。
10. 按一下 **OK**（確定）
11. 按一下 **Virtual Routers**（虛擬路由器）頁籤底部的 **Add**（新增）以新增更多虛擬路由器。

在 SD-WAN 分支上設定多個虛擬路由器

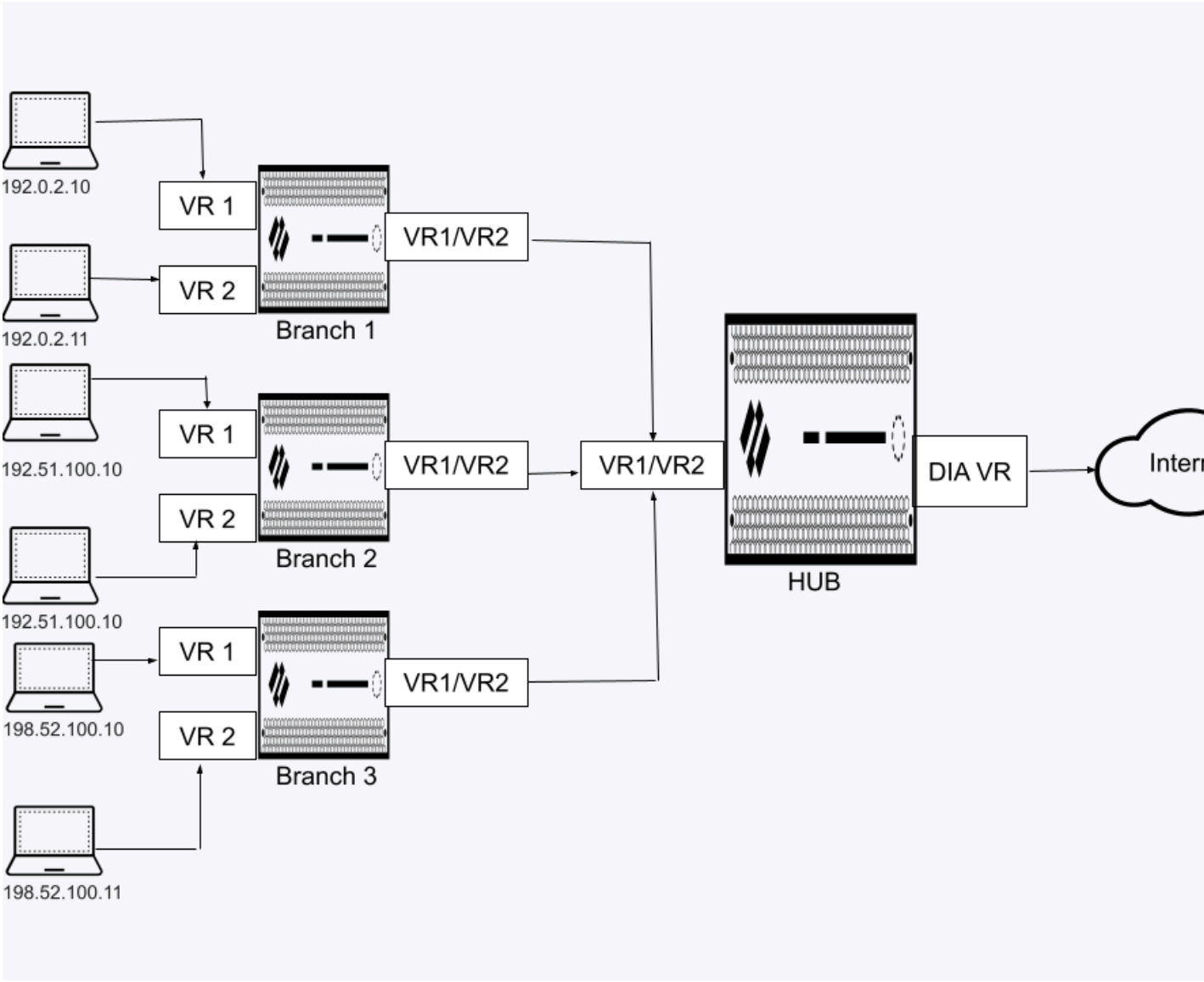
這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

(PAN-OS 11.2.3 和更新 11.2 版本以及 SD-WAN 外掛程式 3.3.1 和更新 3.3 版本）我們已引進 SD-WAN 分支上的多個虛擬路由器支援，以在中樞和分支裝置上具有重疊的 IP 子網路位址。使用此功能時，您可以有多個具有重疊子網路的邏輯路由網域。

在 SD-WAN 分支裝置上啟用多個虛擬路由器之前，請確定下列項目：

- 分支所連線的中樞裝置必須支援多個虛擬路由器。
- 分支所連線的中樞裝置必須具有分支裝置中存在的所有虛擬路由器。
- 在 VPN 叢集中，若要讓分支具有多虛擬路由器支援，您必須先在所有中樞上啟用多虛擬路由器支援。

下圖展示三個 SD-WAN 分支，而且每個分支都已設定一或多個虛擬路由器。在 SD-WAN 分支上啟用多個虛擬路由器支援，三個連線至相同 SD-WAN 中樞的分支即可具有重疊的 IP 子網路，或屬於不同的實體，並獨立運作，因為其流量會流向不同的虛擬路由器。



STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後 **Add**（新增）新的 SD-WAN 防火牆。

STEP 3 | 若要在 SD-WAN 分支裝置上設定多個虛擬路由器：

- 將 SD-WAN 裝置的 **Type**（類型）選取為 **Branch**（分支）。
- 選取 **Enable Multi-VR Support**（啟用多 **VR** 支援）。

針對 **Virtual Router Name**（虛擬路由器名稱）所選取的虛擬路由器會用作分支直接網際網路存取 (DIA) 虛擬路由器，並被視為預設虛擬路由器。**BGP** 頁籤下方所指定的設定必須是 DIA 虛擬路由器所特有。

- 在 *SD-WAN* 分支上啟用多虛擬路由器功能時，我們不支援 *FEC* 和封包複製。
- 只有中樞-支點拓撲才支援 *SD-WAN* 分支上的多虛擬路由器功能（完整網狀拓撲則不予支援）。
- 若要處理 *SD-WAN* 分支上的網際網路流量，*SD-WAN* 政策必須確定只有在 *MPLS* 連結具有網際網路存取和 *NAT* 時才會選取 *MPLS* 標籤。
- 在 *SD-WAN* 分支功能上啟用多虛擬路由器支援時，*PAN-OS* 不支援在 *SD-WAN VPN* 通道外部以純文字轉送流量（在 ***SD-WAN Interface Profile***（***SD-WAN*** 介面設定檔）上停用 ***VPN Data Tunnel Support***（***VPN*** 資料通道支援）時）。

在 SD-WAN 分支裝置上，最多支援 20 個虛擬路由器。不過，SD-WAN 分支上所支援的虛擬路由器數目會因平台而不同：

Palo Alto Networks 防火牆	支援的最大虛擬路由器數目	支援的最大 **SD-WAN** 分支虛擬路由器數目
PA-460	5	5
PA-450	5	5
PA-445	3	3
PA-440	3	3
PA-415	3	3
PA-1420	10	10
PA-1410	10	10
PA-850	5	5
PA-820	5	5
PA-3200	10	10

STEP 4 | （選用）設定虛擬路由器。

1. 選取 **Virtual Routers**（虛擬路由器） 頁籤，以針對 SD-WAN 分支設定多個虛擬路由器。
2. BGP 路由預設會使用 IPv4，因此已啟用 **Enable IPv4 BGP Support**（啟用 **IPv4 BGP** 支援），而且您無法變更此設定。
3. 輸入 **Virtual Router**（虛擬路由器）的名稱。
4. 選取虛擬路由器的唯一區域。

   在具有多個虛擬路由器設定的 VPN 叢集中，虛擬路由器參與多虛擬路由器設定的每個裝置（分支或中樞）必須具有唯一區域。
5. （選用）輸入虛擬 **Router ID**（路由器 **ID**），而此 ID 在所有路由器中都必須是唯一的。
6. 為 BGP 對等指定一個靜態 IPv4 回送位址。自動 VPN 設定會使用您指定的相同 IPv4 位址來自動建立回送介面。如果您指定一個現有回送位址，提交將失敗。因此您應當指定一個當前不是回送位址的 IPv4 位址。
7. 輸入 **AS** 號碼。自治號碼指定了通常定義的到網際網路的路由原則。AS 號碼必須對每個中樞和分支位置都是唯一的。
8. 如果您有終端需要在 SD-WAN BGP 拓撲中與中樞或分支防火牆交換路由，且因此您不想從 BGP 更新中的 AS_PATH 屬性中移除私人 AS 號碼（64512 到 65534），則停用移除私人 **AS** 選項（預設為啟用）。這種情況下，您希望允許私人 AS 號碼將 SD-WAN 私人 AS 留在 BGP 更新中。

   移除私人 ***AS*** 設定適用於分支或中樞防火牆上的所有 *BGP* 對等群組。如果您需要此設定在 *BGP* 對等群組或對等之間有所不同，則必須設定 *SD-WAN* 外掛程式外部的設定。

   如果您已變更 ***Remove Private AS***（移除私人 ***AS***）設定，並提交至所有 *SD-WAN* 叢集節點，然後後續降級至 *2.0.2* 之前的 *SD-WAN* 外掛程式版本，則必須在 *SD-WAN* 外掛程式外部或直接在防火牆上執行與 ***Remove Private AS***（移除私人 ***AS***）相關的所有設定。
9. 輸入要重新散佈的前置詞。在一個中樞裝置上，您必須輸入至少一個要重新散佈的前置詞。
10. 按一下 **OK**（確定）
11. 按一下 **Virtual Routers**（虛擬路由器）頁籤底部的 **Add**（新增）以新增更多虛擬路由器。

為 SD-WAN 設定 HA 裝置

您可以將兩個防火牆設定為主動/被動 HA 模式下的分支（或將兩個防火牆設定為主動/被動 HA 模式下的中樞）以成為 SD-WAN 環境的一部分。在這種情況下，Panorama™ 需要將相同組態推送到主動對等和被動對等，而不是區別對待兩個防火牆。為實現此目的，您需要在為 SD-WAN 新增裝置前設定主動/被動 HA，以便 Panorama 能夠意識到這些裝置是 HA 對等並為其推送相同的組態。（僅支援 HA 主動/被動模式。）

在開始之前閱讀以下程序，以便您不會在將 *HA* 對等新增為 *SD-WAN* 裝置後認可。

在 *HA* 中，防火牆不同步 *SD-WAN* 工作階段散佈統計資料。完成 *HA* 容錯移轉後，工作階段散佈統計資料僅顯示新工作階段的統計資料；現有工作階段的統計資料會遺失。

STEP 1 | 在 HA 對等上啟用 SD-WAN 前，在支援 SD-WAN 的兩個防火牆型號上設定主動/被動 HA。

STEP 2 | 將 HA 對等新增為 SD-WAN 裝置，但不要執行最後一步將其認可。

STEP 3 | 在 Panorama 上，選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）。

STEP 4 | 在螢幕底部，選取 **Group HA Peers**（群組 **HA** 端點）。確認在「狀態」顯示下，HA 狀態欄包含兩個防火牆，一個主動，一個被動。Panorama 可以識別 HA 狀態，並在您認可時將相同 SD-WAN 組態推送到兩個 HA 對等。

STEP 5 | **Commit**（認可）以及 **Commit and Push**（認可並推送）。

建立 VPN 叢集

在您的 SD-WAN 組態中，您必須設定一個或多個 VPN 叢集，以確定哪個分支與那個中樞進行通訊，並在該分支和中樞裝置之間建立安全連線。VPN 叢集是裝置的邏輯分組，因此，在的UI裝置進行邏輯分組時，請考慮地理位置或功能之類的因素。

PAN-OS® 同時支援中樞-支點和完整網狀 SD-WAN VPN 拓撲。在中樞-支點拓撲中，主要辦公室或位置的集中防火牆中樞充當分支裝置之間的閘道。中樞-分支連線是一個 VPN 通道。在此組態中，分支之間的流量必須通過中樞。

當首次使用直接網際網路存取 (DIA) 連結對 SD-WAN 中樞或分支防火牆進行 設定虛擬 SD-WAN 介面 時，會自動建立一個名為 `autogen_hubs_cluster` 的 VPN 叢集，且 SD-WAN 防火牆會自動新增到該 VPN 叢集。這允許 Panorama™ 管理伺服器 監控 SD-WAN 應用程式和連結效能 受 SD-WAN 防火牆保護的裝置並存取起亞網路之外的資源。此外，您將來設定的具有 DIA 連結的任何 SD-WAN 防火牆都將自動新增到 `autogen_hubs_cluster` VPN 叢集，其中包含具有 DIA 連結的所有中樞和分支，以允許 Panorama 監控應用程式和連結效能。`autogen_hubs_cluster` 僅用於監控應用程式和連結監控情況，不會在具有 DIA 連結的中樞和分支之間建立 VPN 通道。如果您需要使用 VPN 通道連線中樞和分支，您必須建立一個新 VPN 叢集，並將所需的中樞和分支全部新增到該叢集。

當您選取 **Pre-shared key**（預先共用金鑰）作為 **Authentication Type**（驗證類型）時，會針對 VPN 叢集中的所有中樞和分支建立強式隨機IKE 預先共用金鑰來保護 VPN 通道的安全，而且每個防火牆都有可加密預先共用金鑰的主要金鑰。系統會保護預先共用金鑰，即使管理員也不可查看。您可以重新整理 IKE 預先共用金鑰，Panorama 會將該金鑰傳送到叢集的所有成員。

請在叢集成員不忙碌時重新整理預先共用金鑰。

當您選取 **Certificate**（憑證）作為 **Authentication Type**（驗證類型）時，SD-WAN VPN 叢集中的中樞和分支會以憑證式驗證為基礎。

SD-WAN 外掛程式升級至 2.1.0 之後，單個 VPN 叢集中的中樞和分支防火牆必須要麼全部執行 PAN-OS 10.0.4（或更新的 10.0 版本），要麼全部執行 10.1.0，而非混合使用兩個版本。

檢視 *VPN* 叢集時，如果沒有資料，或螢幕指出未定義 *SD-WAN*，則請查看相容性矩陣，瞭解您要使用的 *Panorama* 版本是否支援您嘗試使用的 *SD-WAN* 外掛程式版本。

兩個乙太網路連接埠（或是子介面或 AE 介面）（DIA 連結）之間是否形成 IPv4 或 IPv6 IPSec 通道取決於乙太網路介面（或是子介面或 AE 介面）具有 IPv4 位址還是 IPv6 位址。如果兩個介面都有 IPv4 位址，則會建立 IPv4 通道。如果兩個介面都有 IPv6 位址，則會建立 IPv6 通道。在雙重堆疊的情況下，會建立 IPv4 通道。

通道介面 IP 位址來自 VPN 集區。您可以建立與 IPv4 位址集區無關的 IPv6 位址集區。如果同時設定 IPv4 和 IPv6 位址，則通道介面只會獲指派 IPv4 位址，如下表所示。如果耗盡 IPv4 VPN 位址集區，而且具有 IPv6 位址集區，則會針對通道介面指派 IPv6 位址。如果僅設定 IPv4，則通道將會使用 IPv4 位址。如果僅設定 IPv6，則通道將會使用 IPv6 位址。

VPN 集區	已設定		
IPv4	是	是	否。
IPv6	是	否。	是
通道介面 IP	僅限 IPv4	僅限 IPv4	僅限 IPv6

STEP 1 | 規劃您的分支和中樞 VPN 拓撲以確定哪些分支與哪個中樞進行通訊。如需詳細資訊，請參閱規劃您的 SD-WAN 組態。

STEP 2 | 登入 Panorama 網頁介面。

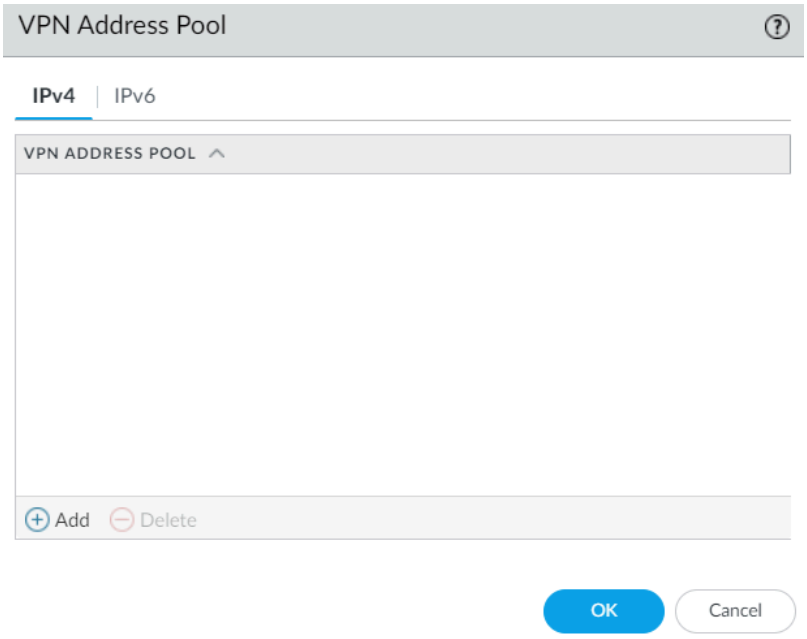
STEP 3 | 為 Auto VPN 設定建立的 IPSec VPN 通道指定 IP 位址範圍。

Auto VPN 組態會在一個中樞和多個分支之間建立一個 *VPN* 通道，並向通道端點指派 *IP* 位址。輸入您想要自動 *VPN* 用作 *VPN* 通道位址的子網路範圍。您最多可以輸入 *20* 個 *IP* 首碼/網路遮罩範圍。自動 *VPN* 會從該集區中提取 *VPN* 通道位址，方法是先從最大範圍中進行提取（針對位址系列），然後在必要時從下一個最大範圍進行提取。您必須為集區設定至少一個範圍。如果您在將組態推送到中樞或分支前沒有執行此步驟，則「認可並推送」將失敗。

如果您從較早的 *SD-WAN* 外掛程式版本升級，則必須檢查您的範圍是否仍然正確。如果不正確，則請輸入新範圍。在您 ***Commit***（認可）後，所有通道都將斷開連線並使用新通道，因此，請在流量較低的時間段執行此工作。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集）。
2. 在螢幕底部，選取 **VPN Address Pool**（**VPN** 位址集區）。

3. 選取 **IPv4** 或 **IPv6**，然後 **Add**（新增）具有一或多個（最多 20 個）**Member**（成員）IP 位址和網路遮罩範圍的位址集區，例如分別為 192.168.0.0/16 或 2001::/16。
4. 按一下 **OK**（確定）。



如果已裝載 *Prisma Access*，則請不要只變更現有的位址集區。如果您需要變更位址集區，請在維護期間執行下列步驟，以將位址集區變更更新至分支和 *Prisma Access CN*：

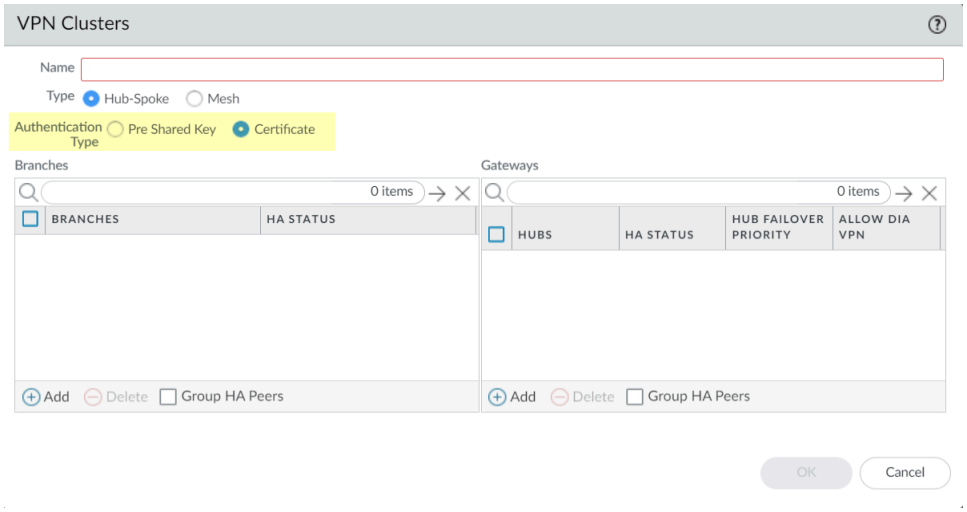
1. 使用 *Panorama* 存取 *SD-WAN* 分支並刪除將受位址集區變更影響的現有裝載；然後執行本機提交。
2. 更新 *VPN* 位址集區，然後執行本機提交。
3. 再次執行 *Prisma Access* 裝載，然後執行本機提交和推送。

STEP 4 | 設定 VPN 叢集。根據需要重複此步驟以建立 VPN 叢集。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集），然後 **Add**（新增）VPN 叢集。
2. 輸入 VON 叢集的描述性名稱。

   VPN 叢集名稱中不支援使用底線和空格，如果使用，則會導致叢集的監控（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控））資料無法顯示。請慎重選擇 *VPN* 叢集的名稱以便將來無需再變更。*SD-WAN* 監控資料基於舊的叢集名稱產生，無法重新同步到一個新的叢集名稱中去，且在監控 *VPN* 叢集或產生報告時會導致所報告叢集的數量出現問題。
3. 選取 VPN 叢集 **Type**（類型）。

   PAN-OS 10.0.2 和更低的 *11.0* 版本僅支援 ***Hub-Spoke***（中樞-支點）*VPN* 叢集類型。從 *PAN-OS 10.0.3* 開始，您可以 建立具有 DDNS 服務的完整網狀 VPN 叢集。
4. （SD-WAN 外掛程式 3.2.0 和更新版本）選取 **Authentication type:Pre-Shared Key**（驗證類型**:** 預先共用金鑰）或 **Certificate**（憑證）。必須指定驗證類型，才能在 VPN 叢集中新增裝置。VPN 叢集應該具有針對其所有裝置所選取的相同驗證類型。



當您針對 VPN 叢集選取驗證類型時，只會將已設定與 VPN 叢集相同驗證類型的分支和中樞新增至 VPN 叢集。例如，當您選取憑證作為 VPN 叢集的驗證類型時，新增至叢集的所有中樞和分支都應該已設定憑證作為驗證類型。

您無法修改已設定 VPN 叢集的驗證類型或 VPN 叢集名稱。若要進行變更，請移除 VPN 叢集和其 SD-WAN 裝置，然後使用新的驗證類型或 VPN 叢集名稱重新進行設定。根據預設，我們支援 VPN 叢集中裝置的預先共用驗證類型（如果未手動選取憑證方法）。

- 設定 *VPN* 叢集之後，您無法變更叢集名稱或其驗證類型（叢集和裝置層級）。
- 您無法在單一 *VPN* 叢集內使用不同的驗證類型。即，*VPN* 叢集驗證類型必須與 *VPN* 叢集中的所有 *SD-WAN* 裝置相符。任何差異都會導致提交失敗。
- 您可以具有已設定不同驗證類型的不同 *VPN* 叢集。
- 在 *VPN* 叢集中，您無法具有已選取不同驗證類型的 *SD-WAN* 裝置。如果 *SD-WAN* 中樞是兩個 *VPN* 叢集的一部分，則這兩個叢集應該已設定相同的驗證類型。

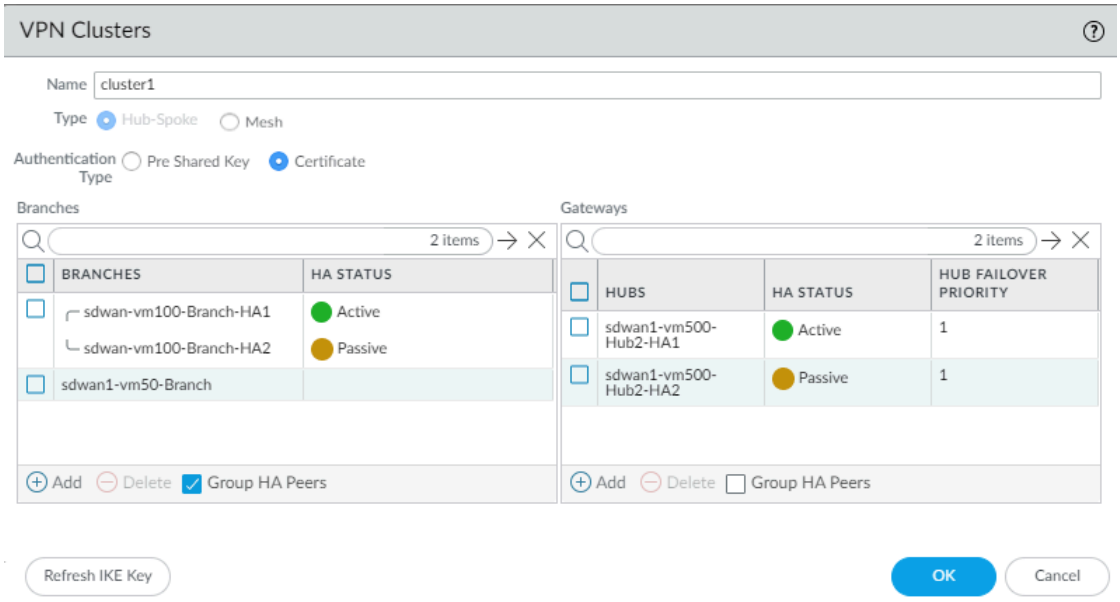
如果您想要將現有 VPN 叢集的驗證類型變更為 **Certificate**（憑證），則請刪除 VPN 叢集，然後使用您選擇的驗證類型重新予以建立。

建立具有憑證驗證類型的 VPN 叢集之後，如果您想要降級到不支援憑證驗證類型的 PAN-OS 或 SD-WAN 外掛程式版本，則請遵循下列步驟：

- 刪除現有的 VPN 叢集。SD-WAN 裝置驗證將會在降級時自動變更為預先共用金鑰。
- 降級至您偏好設定的 PAN-OS 或 SD-WAN 外掛程式版本。請參閱 SD-WAN 的系統需求，以瞭解用於設定憑證驗證類型所需的最低 PAN-OS 和 SD-WAN 外掛程式版本。

升級或降級目前的 SD-WAN 外掛程式之前，請遵循升級和降級注意事項中所提到的步驟。

5. **Add**（新增）一個或多個您確定需要互相通訊的分支裝置。
   - 選取 **Group HA Peers**（群組 **HA** 對等）以同時顯示作為 HA 對等的分支裝置。



   - 選取要新增至叢集的分支裝置。

- 按一下 **OK**（確定）。

6. **Add**（新增）一個或多個您確定需要與分支裝置通訊的中樞裝置。

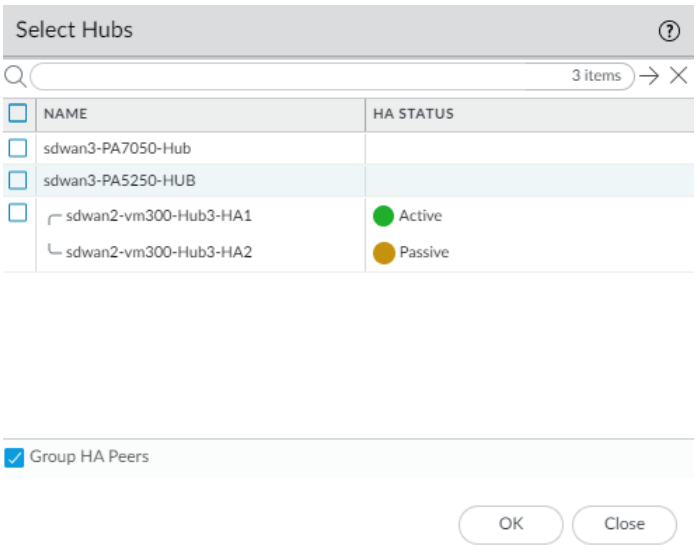
   HA 設定中的 SD-WAN 中樞被視為單一 SD-WAN 中樞防火牆。

   MPLS 和衛星連結類型將形成僅具有相同連結類型的通道，例如 *MPLS* 到 *MPLS* 和衛星到衛星。將不會在 *MPLS* 連結和乙太網路連結之間建立通道。

   針對 3.1.3 之前的 SD-WAN 版本，您最多可以將四個 SD-WAN 中樞防火牆新增至 VPN 叢集。

   （SD-WAN 外掛程式 3.2.1 和更新版本）您最多可以將 16 個 SD-WAN 中樞防火牆新增至 VPN 叢集。基於 ECMP，VPN 叢集內 16 個中樞中只有四個可以具有相同的中樞優先順序。任何針對四個以上 SD-WAN 中樞設定相同優先順序的嘗試都會導致提交錯誤。

   - 選取 **Group HA Peers**（群組 **HA** 對等）以同時顯示作為 HA 對等的中樞裝置。
   - 選取要新增至叢集的中樞，然後按一下 **OK**（確定）。



   - 對於具有多個中樞的任何新的或之前存在的 VPN 叢集，您必須確定中樞的優先順序，以確定：a) 傳送到特定中樞的流量，以及 b) 隨後的中樞容錯移轉順序。中樞容錯移轉優先級範圍為 1 到 4。升級後，預設優先級將設定為 4。外掛程式將中樞容錯移轉優先級內部轉譯為 BGP 本機偏好設定編號，如以下表格所示。優先級值越低，優先級和本機偏好設定就越高。針對 SD-WAN 3.1.3 之前的版本，一個叢集最多支援四個中樞。使用 SD-WAN 外掛程式 3.2.1 和更新版本時，您最多可以將 16 個 SD-WAN 中樞防火牆新增至 VPN 叢集。主動/被動 HA 配對計為一個中樞。多個中樞可以具有相同的優先級；HA 配對必須具有相同的優先級。Panorama 使用分支的 BGP 範本將中樞的本機偏好設定推送到叢集中的分支。

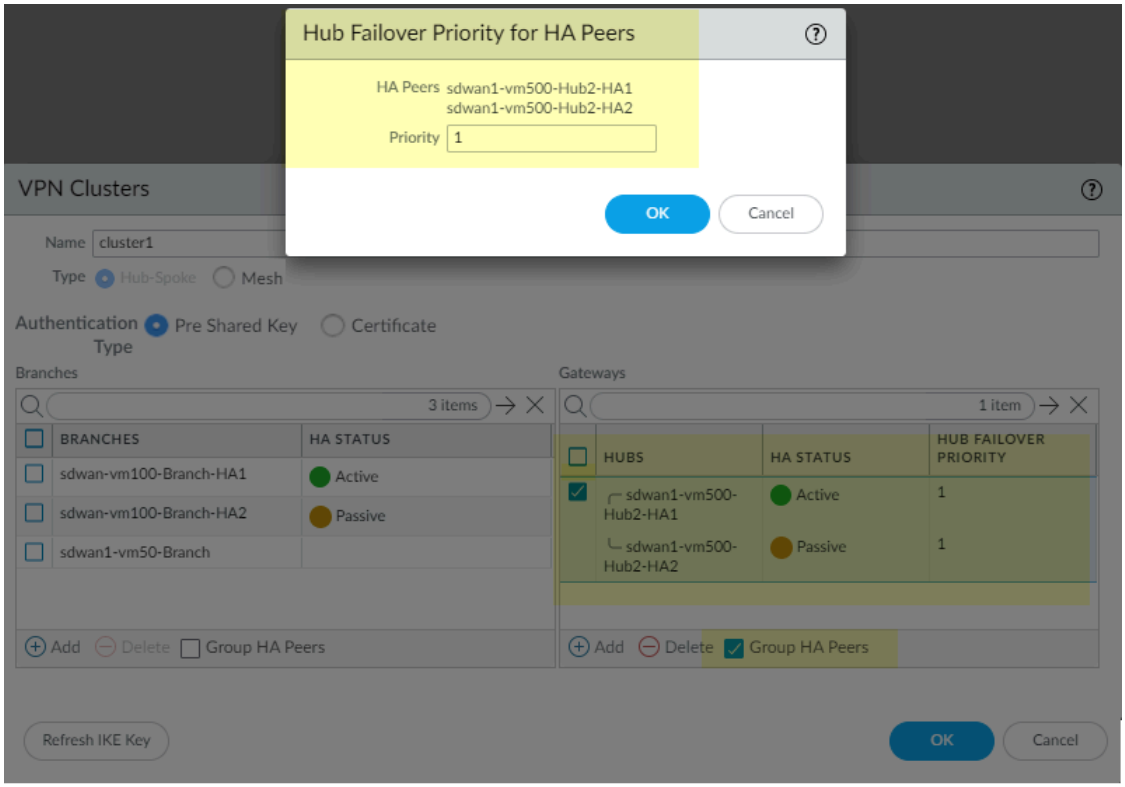
中樞容錯移轉優先順序	本機偏好設定
1	250
2	200

中樞容錯移轉優先順序	本機偏好設定
3	150
4	100

如果多個中樞具有相同的優先順序，則 *Panorama* 會在每個分支防火牆的兩個位置中啟用 *ECMP*，以判斷分支如何選取路徑。針對虛擬路由器啟用 *ECMP*（***Network***（網路） > ***Virtual Routers***（虛擬路由器） > ***ECMP***），而且針對 *BGP* 啟用 ***ECMP Multiple AS Support***（***ECMP*** 多 ***AS*** 支援）（***Network***（網路） > ***Virtual Routers***（虛擬路由器） > ***BGP*** > ***Advanced***（進階））。如果叢集中的所有中樞都具有唯一優先順序，則會在分支上停用 *ECMP*。如果中樞優先順序設定變更，則 *Panorama* 會重新評估是啟用還是停用 *ECMP*。

- 如果您已選取 **Group HA Peers**（群組 **HA** 對等），則請選取配對，然後按一下 **Hub Failover Priority**（中樞容錯移轉優先順序）欄位；輸入單一 **Priority**（優先順

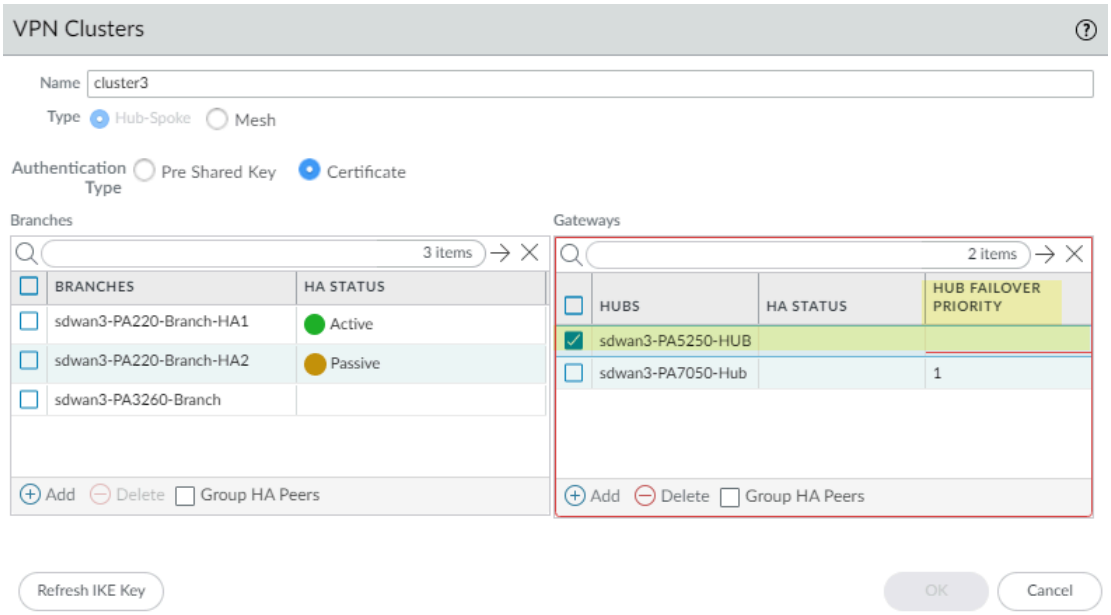
序）（範圍為 1 到 4），這將套用至 HA 配對中的兩個中樞，然後按一下 **OK**（確定）。



僅有已設定的 *HA* 配對才會顯示 *[Hub Failover Priority for HA Peers*（*HA* 對等的中樞容錯移轉優先順序）*]* 視窗。如果您新增 *HA* 配對，則必須分別針對兩個新對等都設定中樞容錯移轉優先順序。

如果您針對屬於未分組 *HA* 對等的中樞指派不同的優先順序，然後選取 ***Group HA Peers***（群組 ***HA*** 對等）和 ***Submit***（提交），則會收到錯誤訊息。

- 針對不是 HA 配對的中樞，選取中樞，然後按一下 **Hub Failover Priority**（中樞容錯移轉優先順序）欄位；輸入優先順序（範圍為 1 到 4）。



7. 按一下 **OK**（確定）以儲存 VPN 叢集。

STEP 5 | 將分支中的額外前置詞發佈到中樞。

防火牆會自動重新散佈（發佈）從分支到中樞的所有非公開已連線路由。您還可以重新散佈從分支到中樞的任何額外前置詞。***Prefix(es) to Redistribute***（要重新散佈的前置詞）欄位接受一個前置詞清單，而不是單個前置詞。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後選取分支防火牆。
2. 選取 **BGP**，然後 **Add**（新增）一個或多個具有網路遮罩的 IP 位址到**Prefix(es) to Redistribute**（要重新散佈的前置詞）。
3. 按一下 **OK**（確定）。

STEP 6 | **Commit**（認可），然後 **Commit to Panorama**（認可至 **Panorama**）。

STEP 7 | （SD-WAN 外掛程式 2.0.1和更高的 2.0 版本）如果中樞-支點 VPN 叢集中的中樞防火牆具有 DHCP 或 PPPoE 介面，則必須使用 DDNS。選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後在 **Template**（範本）欄位中，針對中樞選取範本堆疊。

STEP 8 | （SD-WAN 外掛程式 2.0.1 和更高的 2.0 版本）選取其 IP 位址指示 `Dynamic-DHCP Client`（動態 DHCP 用戶端）或 PPPOE 的介面，按一下螢幕底部的 **Override**（覆寫），然後按一下 **OK**（確定）以關閉。

STEP 9 | （SD-WAN 外掛程式 2.0.1 和更高的 2.0 版本）在 Panorama 上驗證是否已設定 DDNS 設定。

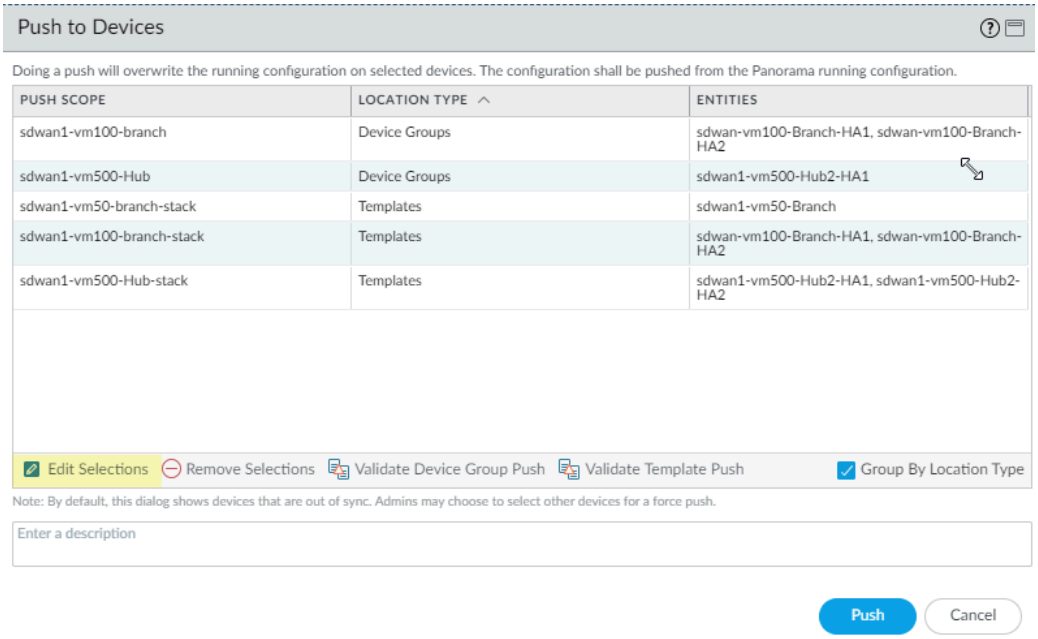
1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後再次選取相同介面。
2. 選取 **Advanced**（進階） > **DDNS**。
3. 可以看到，DDNS 設定自動設定了 **Hostname**（主機名稱），且 **Vendor**（廠商）設定為 `Palo Alto Networks DDNS`。
4. 按一下 **OK**（確定）。

STEP 10 | （SD-WAN 外掛程式 2.0.1 和更高的 2.0 版本）**Commit**（提交），然後 **Commit to Panorama**（提交至 **Panorama**）。

STEP 11 | 將組態推送至中樞。

在 *Panorama* 為中樞建立虛擬 *SD-WAN* 介面時，*Panorama* 並不一定使用連續的介面編號建立介面。它可能隨機跳過一個介面編號，例如，*sdwan.921*、*sdwan.922*、*sdwan.924*、*sdwan.925*。儘管有不連續的編號，*Panorama* 仍然會為 *SD-WAN* 介面建立正確的編號。使用可操作 *CLI* 命令 ***show interface sdwan?*** 來查看 *SD-WAN* 介面。

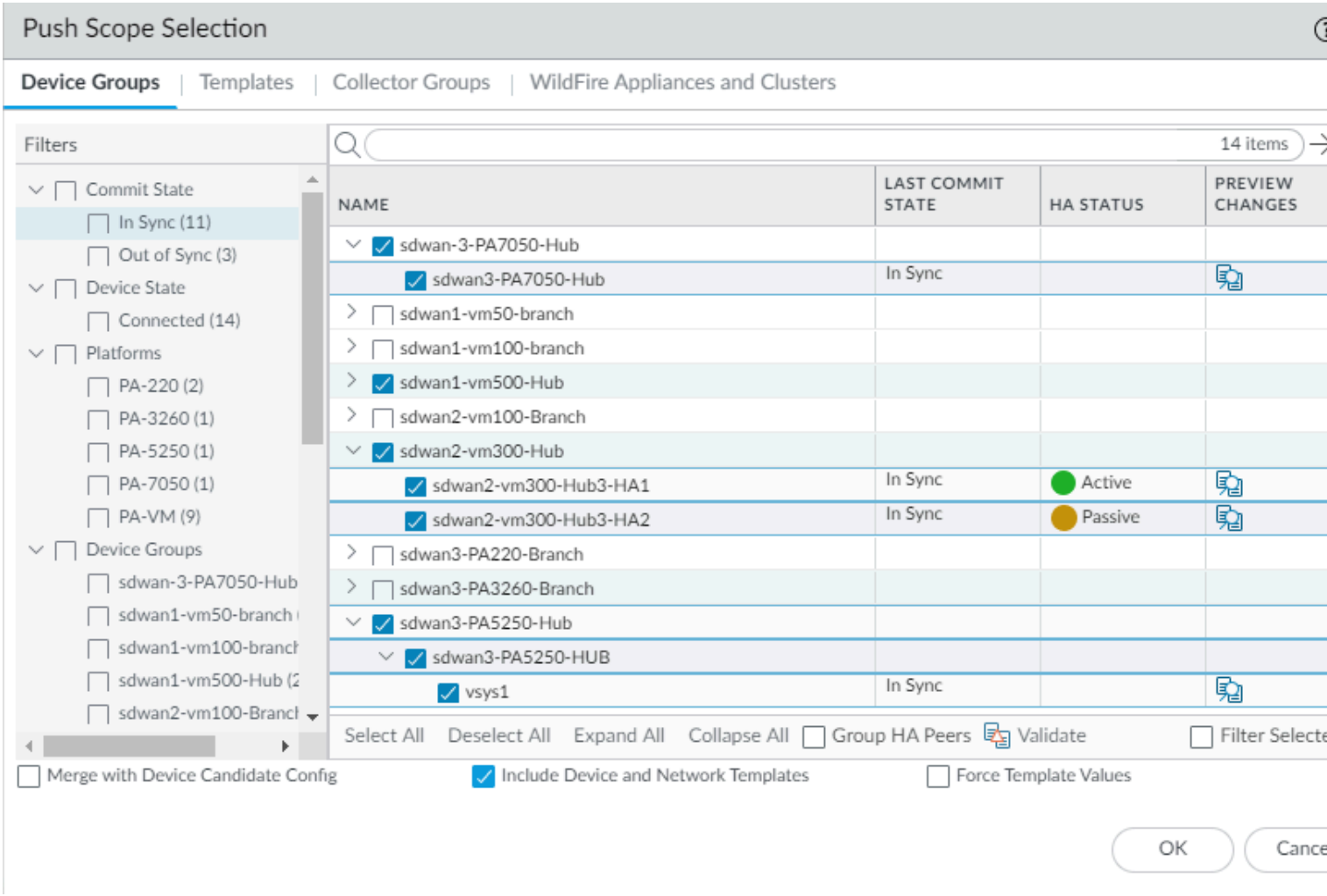
1. 選取 **Commit**（認可），然後選取 **Push to Devices**（推送到裝置）。
2. 在螢幕左下角 **Edit Selections**（編輯選擇）。



3. 取消選取 **Filter Selected**（已選取篩選器）。
4. 按一下 **Deselect All**（取消全選）。
5. 選取中樞裝置群組。選取螢幕底部的 **Include Device and Network Templates**（包含裝置與網路範本）。您必須先推送到中樞，然後才可推送到分支。

   大多數分支通過其服務提供者具有動態 IP 位址，由於中樞沒有分支的 IP 位址，因而分支必須啟動 IKE/IPSec 連線。為確保中樞已準備好接收 IKE/IPSec 連線，必須在分支的組態

之前認可並推送中樞的組態。這樣，當推送分支組態且分支啟動指向中樞的連線時，中樞已經就緒。



6. 選取 **Templates**（範本）標籤，然後選取 **Deselect All**（取消全選）。
7. **Push Scope**（推送範圍）是裝置群組。將組態 **Push**（推送）至中樞。

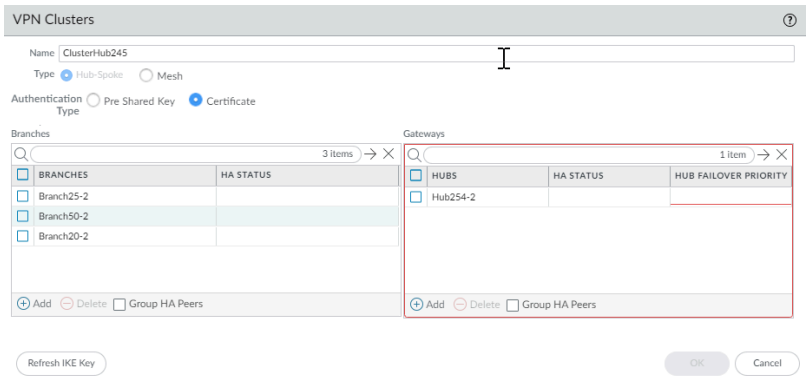
STEP 12 | 重複之前的步驟，但是選取您的分支裝置群組，將組態推送到分支。

STEP 13 | 重新整理 IKE 預先共用金鑰。

如果您需要變更用於保護 *VPN* 叢集裝置之間的 *IPSec* 連線的當前 *IKE* 金鑰，請執行此步驟以隨機產生用於叢集的新金鑰。

請在叢集成員不忙碌時執行此步驟。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集），然後選取叢集。
2. 在螢幕底部，選取 **Refresh IKE Key**（重新整理 **IKE** 金鑰）。



3. 會出現一則訊息，通知您重新整理 IKE 金鑰會為 VPN 叢集中的每個 SD-WAN 防火牆產生新的安全性關聯 (SA)。這可能會造成服務中斷。您要繼續嗎？ 是 | 否 如果您想要繼續，則選取 Yes（是）。
4. **Commit**（認可）。

   在 ***Refresh IKE Key***（重新整理 ***IKE*** 金鑰）後，您必須提交到整個叢集；部分提交將導致通道關閉。
5. **Push to Devices**（推送到裝置）。

建立具有 DDNS 服務的完整網狀 VPN 叢集

從 PAN-OS 10.0.3 開始，SD-WAN 除了中樞-支點拓撲之外，還支援完整網狀拓撲。此網狀拓撲可以包含具有或不具有中樞的分支。當分支需要互相直接通訊時，請使用完整網狀拓撲。完整網狀拓撲的使用案例包括具有分支和中樞的零售商以及具有或不具有中樞的企業。

一些防火牆介面使用 DHCP 來獲取其 IP 位址。分公司通常使用消費者級別的網際網路服務並接收動態 IP 位址，當然，該位址可以變更。因此，防火牆需要動態 DNS (DDNS)，以便 DDNS 服務可以偵測到執行 SD-WAN 的防火牆介面的公開 IP 位址。當您將 DDNS 設定推送到所有防火牆時，會通知每個防火牆向 Palo Alto Networks DDNS 雲端服務註冊其外部介面 IP 位址，以便將該 IP 位址轉換為 FQDN。

需要 DDNS 的另一個原因是來自 ISP 的 CPE 裝置可能正在執行來源 NAT。（動態 IP 位址可能會進行來源 NAT 轉譯，也可能不會）。DDNS 服務允許防火牆向 DDNS 伺服器註冊公開 IP 位址。當您具有用於分支到分支網狀的裝置連線時，Auto VPN 會與 DDNS 服務聯絡，以便這些防火牆能夠提取其在 DDNS 雲端中註冊的公用 IP 位址，並使用這些公共 IP 位址建立 IKE 對等和 VPN 通道。如果 CPE 裝置正在執行來源 NAT，則新增要由 Panorama 管理的 SD-WAN 分支裝置時，將啟用 **Upstream NAT**（上游 **NAT**），且 NAT IP 位址類型將為 **DDNS**。

對於使用來源 *NAT* 的 *CPE* 裝置或上游路由裝置，您負責在該裝置上建立一對一的目的地 *NAT* 規則（無連接埠轉譯），以將外部 *IP* 位址轉譯回指派給防火牆介面的私人 *IP* 位址。這種轉譯允許 *IKE* 和 *IPSec* 通訊協定重新進入防火牆。（*Palo Alto Networks* 對執行來源 *NAT* 的上游 *CPE* 或上游路由器沒有存取權限。）

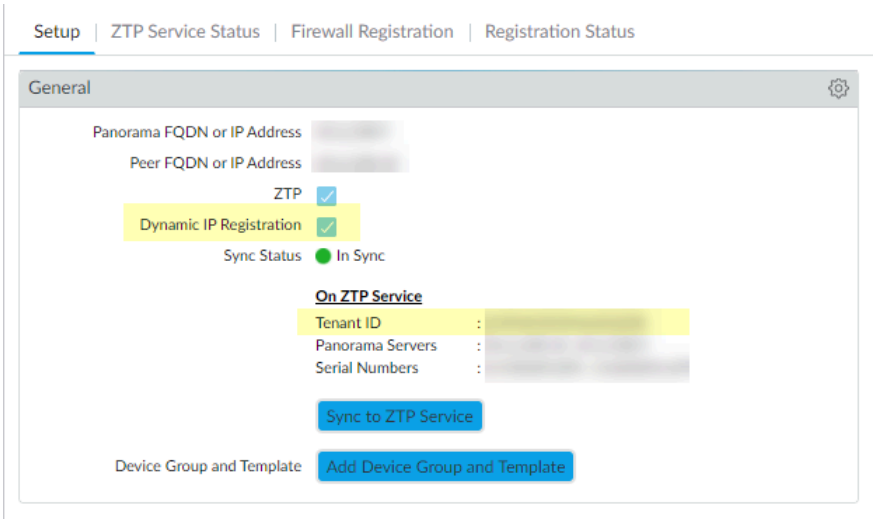
具有 DDNS 服務的 SD-WAN 完整網狀拓撲具有以下要求：

- PAN-OS 10.0.3 或更新 11.1 版本
- SD-WAN 外掛程式 2.0.1 或更高的 2.0 版本
- 已下載、安裝和設定 ZTP 外掛程式 1.0.1 或更高的 1.0 版本，以便利用與 ZTP 關聯的 DDNS。Panorama 必須已註冊 ZTP 且與 ZTP 服務通訊。
- 應用程式和威脅內容版本 8354 或更高的版本
- 所有參與完整網狀 DDNS 的防火牆都必須在相同的客戶支援入口網站 (CSP) 帳戶下註冊。
- 所有參與完整網狀 DDNS 的防火牆都必須安裝最新的裝置憑證。正確驗證防火牆、Panorama 和雲端服務是重要的安全程序，需要裝置憑證以及 CSP 和 ZTP 服務。
- 如果您的防火牆或其他網路裝置可控制位於 Palo Alto Networks 防火牆前方的傳出流量，則必須變更該裝置上的設定，以允許來自已啟用 DDNS 的介面的流量傳輸至下列 FQDN：
  - https://myip.ngfw-ztp.paloaltonetworks.com/ （以獲取 WhatsMip 服務）
  - https://ngfw-ztp.paloaltonetworks.com/ （以獲取 DDNS 註冊服務）

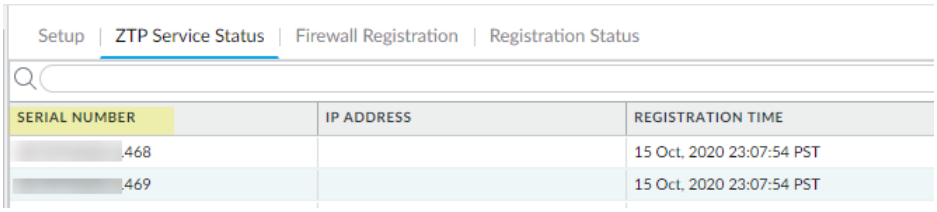
STEP 1 | 為 Panorama 以及作為中樞或分支的所有受管理防火牆安裝最新的裝置憑證。

STEP 2 | 安裝 ZTP 外掛程式 1.0.1 以設定零接觸佈建。

1. 在 Panorama 管理員指南中，閱讀 ZTP 概要。
2. 安裝 ZTP 外掛程式。
3. 設定 ZTP 安裝程式管理員帳戶。
4. 選取 **Panorama** > **Zero Touch Provisioning**（零接觸佈建） > **Setup**（設定），然後編輯「一般」設定以啟用 **Dynamic IP Registration**（動態 **IP** 註冊）。
5. 按一下 **OK**（確定）。「一般」設定使用租用戶 ID 編號指示「ZTP 服務開啟」。



6. 選取 **ZTP Service Status**（**ZTP** 服務狀態）並確認已列出防火牆序號。



STEP 3 | 如果尚未安裝 SD-WAN 外掛程式 2.0.1 或更高的 2.0 版本，請安裝。

STEP 4 | 在 Panorama 上 **Commit**（提交）。

STEP 5 | 登入 Panorama 網頁介面。

STEP 6 | 建立 VPN 位址集區，如 建立 VPN 叢集 中所示。

STEP 7 | 建立完整網狀 VPN 叢集。

1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集）。
2. 選取 **Mesh**（網狀）作為 **Type**（類型）。
3. **Add**（新增）需要互相通訊的 **Branches**（分支）。
4. （選用）如果您還希望網狀叢集中有中樞，則 **Add**（新增）一個或多個 **Hubs**（中樞）。
5. 按一下 **OK**（確定）。

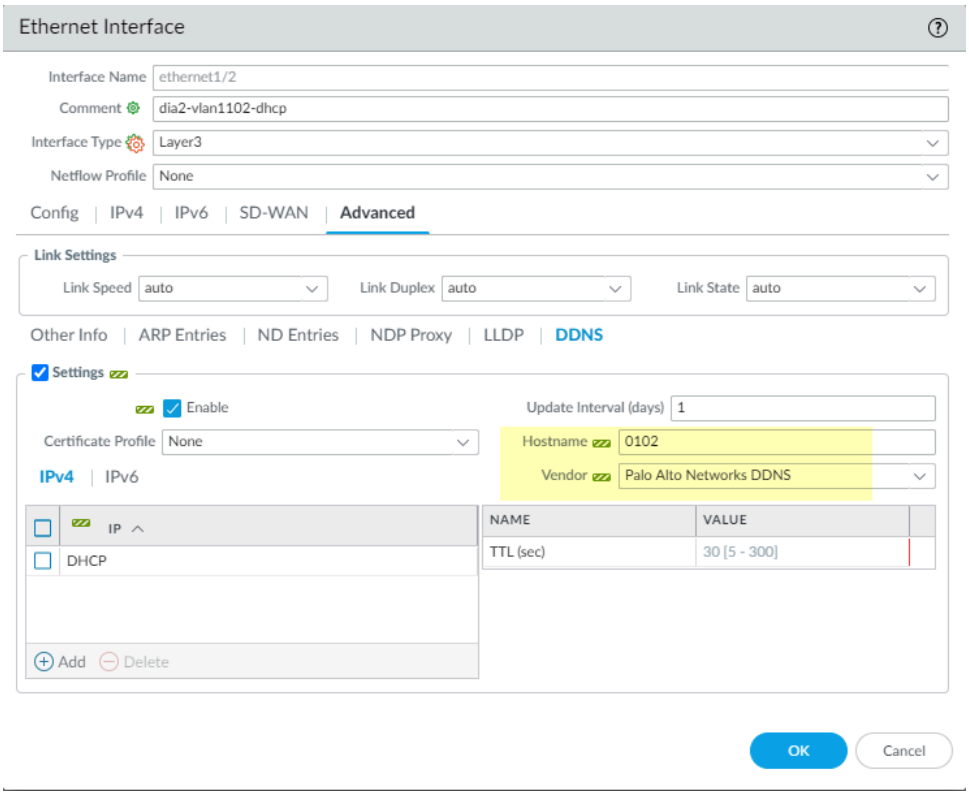
STEP 8 | **Commit**（認可），然後 **Commit to Panorama**（認可至 **Panorama**）。如果防火牆具有靜態 IP 位址，則表示已完成。如果 VPN 網狀叢集中的分支或中樞防火牆具有 DHCP 或 PPPoE 介面，則必須使用 DDNS，因此請按照以下步驟繼續此程序。

STEP 9 | 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後在 **Template**（範本）欄位中，為特定分支選取範本堆疊。

STEP 10 | 選取其 IP 位址指示 `Dynamic-DHCP Client`（動態 DHCP 用戶端）或PPPOE 的介面，按一下螢幕底部的 **Override**（覆寫），然後按一下 **OK**（確定）以關閉。

STEP 11 | 在 Panorama 上驗證是否已設定 DDNS 設定。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後再次選取同一介面。
2. 選取 **Advanced**（進階） > **DDNS**。
3. 可以看到，DDNS 設定已基於介面名稱自動設定了 **Hostname**（主機名稱），且 **Vendor**（廠商）設定為 `Palo Alto Networks DDNS`。例如，在 Ethernet1/2 介面上，最終的主機名稱為 0102。



4. 按一下 **OK**（確定）。

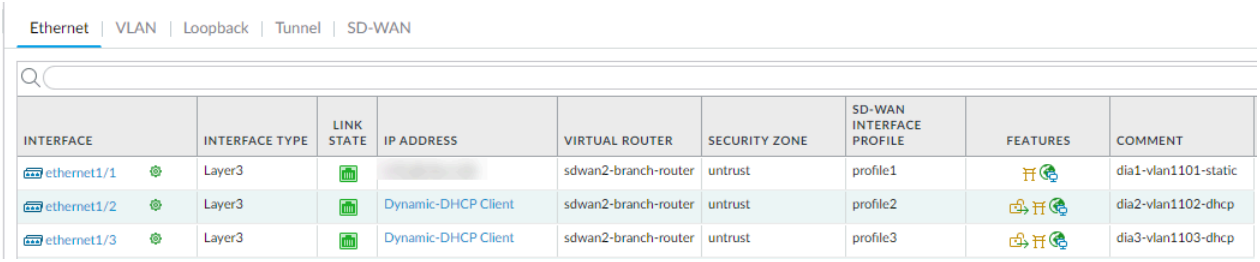
STEP 12 | 如果 VPN 叢集包括任何具有 DHCP 或 PPPoE 介面的中樞，請重複步驟 9 至 11，但在 **Template**（範本）欄位中，為特定中樞選取範本堆疊。

即使中樞不在完整網狀叢集中，而是在中樞-支點叢集中，如果中樞使用 *DHCP* 或 *PPPOE* 獲取 *SD-WAN* 介面的 *IP* 位址，也必須執行覆寫步驟來啟用 *DDNS*。

STEP 13 | **Commit**（提交）至 Panorama 並 **Push to Devices**（推送到裝置）。

STEP 14 | 在分支防火牆上確認分支已設定 DDNS。

1. 登入分支防火牆。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），對於您設定的乙太網路介面，捲動到「功能」欄中的 DDNS 資訊圖示，查看廠商、主機名稱、IP 位址和其他 DDNS 資訊。



STEP 15 | 在叢集的另一個分支上，可以看到，介面的對等位址是系統產生的用於 DDNS 註冊的 FQDN。

1. 登入另一個分支，選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）。
2. 可以看到，對等位址是一個安全的名稱，不能輕易引用且不顯示公司資訊；例如 0101.8ced8460fcc5177cd3665ce41b6345323a15a612b8e52ec1d9ec057a582cb4.t13855f6c9a92c

STEP 16 | 檢視分支和中樞的 FQDN 並更新 DDNS 資訊。

1. 存取 CLI。
2. 檢視其他分支和中樞的 FQDN（由 DDNS 產生）：**`show dns-proxy fqdn all`**
3. 更新 DDNS 位址：**`request system fqdn refresh`**

為 SD-WAN 建立靜態路由

除了 BGP 路由之外（或作為替代方案），您可以建立靜態路由來路由您的 SD-WAN 流量。

您可以使用 Panorama™ 或直接在防火牆中樞或分支上設定靜態路由。如果您想要使用 Panorama，您應當熟悉設定範本或範本堆疊變數的程序。您將建立一個變數來用作靜態路由中的目的地，如以下程序中所示。（您也可以針對下一個躍點建立變數。）您需要將（前往中樞的）靜態路由推送到分支。您需要將（前往分支的）靜態路由推送到中樞。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定範本或範本堆疊變數，然後使用以下格式輸入變數 **Name**（名稱）：*$peerhostname_clustername.customname*。例如，$branchsanjose_clusterca.10 或 $DIA_cluster2.location3。在貨幣符號 ($) 後，變數中的元素為：

- *peerhostname*（對等主機名稱）—靜態路由前往的目的地中樞或分支的主機名稱。對於指向網際網路的靜態路由，peerhostname（對等主機名稱）必須為 **DIA**。除了對等的主機名稱外，還可選擇使用對等的序號。如果對等是 HA 配對的一部分，您可以使用兩個 HA 防火牆之一的主機名稱或序號。
- *clustername*（叢集名稱）—目的地中樞或分支所屬的 VPN 叢集的名稱。
- *customname*（自訂名稱）—您選擇的文字字串；您不能在 customname（自訂名稱）中使用句點 (.)。

您可以擁有多個指向相同對等的靜態路由，這意味著變數將具有相同的 peerhostname（對等主機名稱）和 clustername（叢集名稱），透過使用不同的 customname（自訂名稱）來區分變數。

STEP 3 | 選取變數 **Type**（類型）為 **IP Netmask**（**IP** 網路遮罩），然後輸入包含斜線和網路遮罩長度的目的地 IP 位址，如 192.168.2.1/24。針對 IPv6，輸入具有斜線和首碼長度的 IPv6 位址，例如 2001:DB8::/32。

STEP 4 | 按一下 **OK**（確認）以儲存變數。

STEP 5 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後選取一個虛擬路由器。

STEP 6 | 選取 **Static Routes**（靜態路由）。

STEP 7 | 選取 **IPv4** 或 **IPv6**，然後 **Add**（新增）靜態路由的 **Name**（名稱）。

STEP 8 | 對於 **Destination**（目的地），選取您建立的變數。

STEP 9 | 對於 **Interface**（介面），從下拉式清單中進行選取，該清單僅包含範本中的介面；例如，Ethernet1/1、Tunnel.x 或 sdwan.xx。

STEP 10 | 針對 **Next Hop**（下一個躍點），選取 **IP Address**（**IP** 位址）或 **IPv6 Address**（**IPv6** 位址），然後輸入靜態路由的下一個躍點（靜態路由所到達的中樞或分支）的 IP 位址或變數。

STEP 11 | 按一下 **OK**（確定）。

STEP 12 | **Commit**（認可），**Commit and Push**（認可並推送）您的變更。

Auto VPN 組態將靜態路由的「介面」欄位中的 **sdwan** 關鍵字替換為它根據目的地變數確定的輸出虛擬 SD-WAN 介面。這樣，路由表中的靜態路由指示前往已識別 VPN 叢集中對等主機的流量將輸出虛擬 SD-WAN 介面，以到達指定的下一個躍點。

STEP 13 | 為返回流量設定靜態路由。

為 SD-WAN 設定進階路由

進階路由引擎允許防火牆擴展規模，並為大型資料中心、ISP、企業和雲端使用者提供穩定、高效能和高可用性的路由功能。進階路由引擎依賴於行業標準的設定方法，這有助於完成管理員工作。其允許建立用於不同功能（例如篩選、重新散佈和指標變更）的設定檔，所有這些都可以跨邏輯路由器使用。這些設定檔能夠更細微地篩選每個動態路由通訊協定的路由，並改進跨多個通訊協定的路由重新散佈。

儘管在概念上是等效的，但進階路由引擎使用邏輯路由器而不是虛擬路由器來執行個體化路由網域。

與虛擬路由器不同，邏輯路由器不會依預設建立；您必須在設定路由功能之前建立邏輯路由器。

您可以根據網路需求使用進階路由引擎或舊版引擎：

- 當您啟用進階路由時，將建立邏輯路由器並使用進階路由引擎進行路由。
- 當您停用 **Advanced Routing**（進階路由）時，將建立虛擬路由器並使用舊版引擎進行路由。

進階路由引擎支援多個邏輯路由器（在舊版路由引擎上稱為虛擬路由器）。例如，進階路由引擎具有更方便的功能表選項，並且您可以在套用至 BGP 對等群組或對等體的設定檔（驗證、計時器、位址家族或重新散佈設定檔）中輕鬆進行更多 BGP 設定。

進階路由引擎支援靜態路由、MP-BGP、OSPFv2、OSPFv3、RIPv2、通訊協定無關的多點傳送稀疏模式 (PIM-SM)、PIM 特定來源多點傳送 (SSM)、BFD、重新散佈、路由篩選至 RIB、存取清單、首碼清單和路由對應。

您需要以下內容才能在 SD-WAN 上設定進階路由引擎：

平台	執行 **PAN-OS** 版本的防火牆	**SD-WAN** 外掛程式
Panorama™	11.1 和更新版本	3.1.0 與更新版本

SD-WAN 外掛程式會根據進階路由選項的值建立邏輯路由器或虛擬路由器。啟用進階路由時，將建立邏輯路由器；否則將建立虛擬路由器。

當您在範本堆疊中啟用進階路由且執行 Panorama 提交並推送至防火牆時，SD-WAN 外掛程式會執行移轉指令碼以在邏輯路由器中建立 SD-WAN 相關物件（靜態、介面、重新散佈設定檔、BGP）。移轉指令碼會為同一範本建立與虛擬路由器名稱相同的邏輯路由器名稱。因此，中樞和分支始終具有相同的路由器名稱。

移轉後，*Panorama* 不允許您刪除已移轉的虛擬路由器。

Panorama SD-WAN 外掛程式 3.1.0 可以同時管理使用進階路由引擎的防火牆和使用舊版路由引擎的防火牆。其好處是您可以將選定的受管理防火牆移轉至新的進階路由引擎，同時仍然在其他防火牆上保留現有的舊版路由引擎設定。

儘管 SD-WAN 外掛程式 3.1.0 對防火牆的管理與路由引擎無關，但一個受管理的防火牆上一次只能有一個路由引擎設定有效。您可以使用 **Advanced Routing**（進階路由）選項來啟用或停用進階路由引擎。每次變更防火牆將使用的引擎（啟用或停用進階路由以分別存取進階引擎或舊版引擎）時，您必須提交設定並重新啟動防火牆以使變更生效。

在切換到進階路由引擎之前，請備份您當前的設定。同樣，如果您使用啟用或停用進階路由的範本堆疊設定 *Panorama*，則在提交並將範本堆疊推送到裝置後，您必須重新啟動範本堆疊中的裝置才能使變更生效。

設定 *Panorama* 時，為所有使用相同進階路由設定（全部啟用或全部停用）的裝置建立裝置群組和範本堆疊。*Panorama* 不會將啟用了進階路由的設定推送到不支援進階路由的小型防火牆。對於這些防火牆，*Panorama* 將推送舊版設定（如果存在）。

確保降級到適當的 SD-WAN 外掛程式和 PAN-OS 版本，如果您計劃使用虛擬路由器，則停用 **Advanced Routing**（進階路由）。在降級 SD-WAN 外掛程式時，使用已停用 **Advanced Routing**（進階路由）的單獨範本（在這種情況下，會建立虛擬路由器）。

如果您已設定 **Advanced Routing**（進階路由）並想切換到虛擬路由器，則停用進階路由以返回至之前儲存的虛擬路由器設定。在嘗試降級過程（例如降級 PAN-OS 和 SD-WAN 外掛程式版本）之前，在停用進階路由後提交並推送對防火牆所做的任何變更。

如果啟用進階路由，則必須在同一邏輯路由器中設定 SD-WAN 介面；它們不能在邏輯路由器之間分割。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 將 Panorama 升級到 11.1，並安裝 SD-WAN 外掛程式 3.1.0。

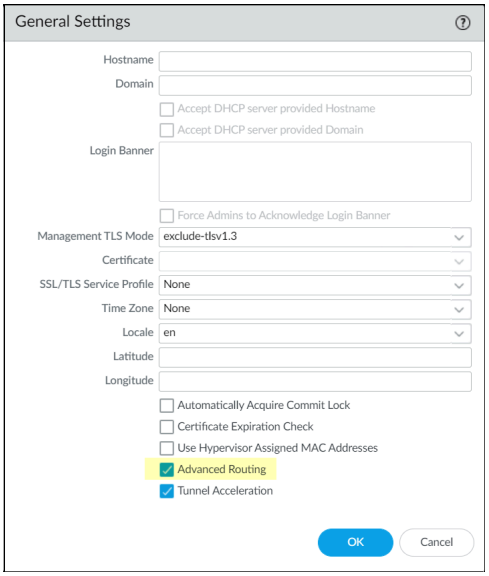
STEP 3 | 將您的中樞和分支防火牆作為受管理的裝置新增到 Panorama™ 管理伺服器。

STEP 4 | 在啟用進階路由之前備份當前設定。

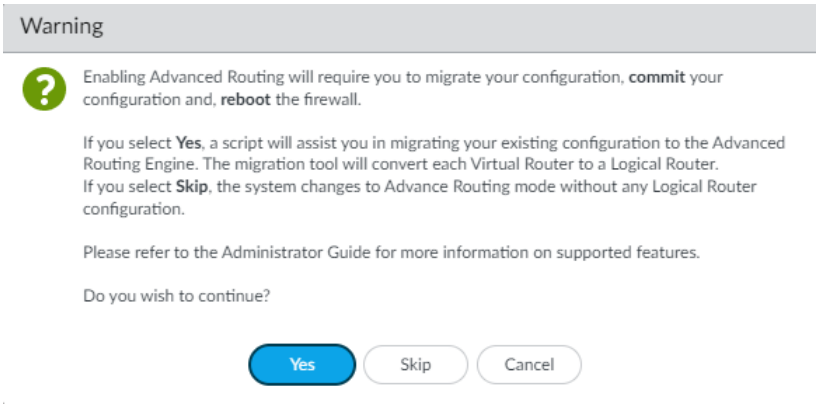
STEP 5 | 在 **Device**（裝置）部分，從 **Template**（範本）內容下拉式清單中選取適當的範本堆疊。

STEP 6 | 啟用進階路由引擎。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 General Settings（一般設定）。
2. 啟用 **Advanced Routing**（進階路由）。SD-WAN 外掛程式將根據進階路由選項的值建立邏輯路由器或虛擬路由器。啟用進階路由時，將建立邏輯路由器。否則將建立虛擬路由器。

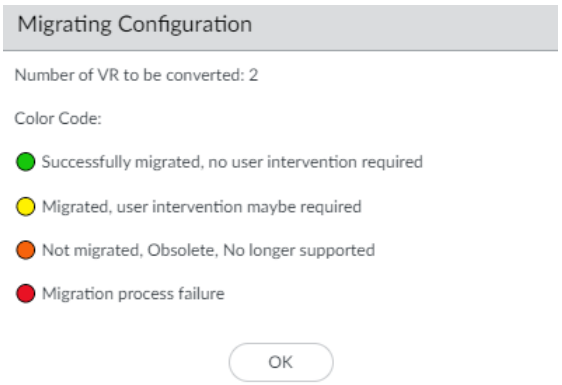


3. 按一下 **OK**（確定）。
4. 出現有關移轉的警告消息；按一下 **Yes**（是）以繼續。

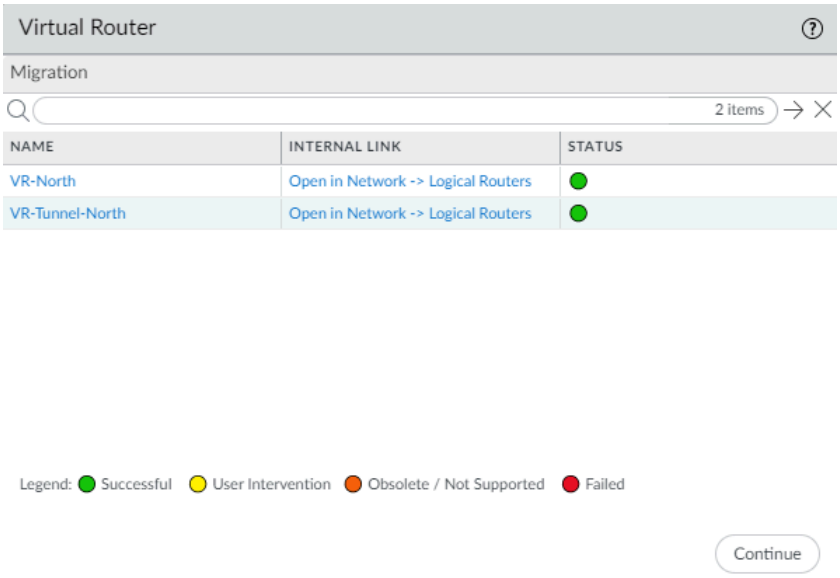


按一下 **Yes**（是）後，一個內建的移轉指令碼會將您現有的設定移轉到進階路由引擎。如果您選取 **Skip**（略過），則會為進階路由引擎建立一個空設定。

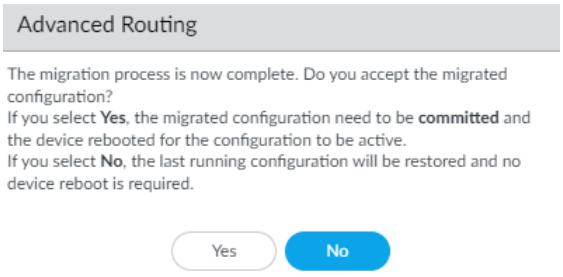
Migration Configuration（移轉設定）會顯示指示移轉狀態的顏色代碼。



在 **Virtual Router**（虛擬路由器）中，檢閱範本堆疊中範本的 **STATUS**（狀態）。成功移轉的 **STATUS**（狀態）應為綠色。否則，對未通過移轉的任何範本採取必要的動作。



成功的移轉會自動將每個虛擬路由器轉換為相應的邏輯路由器。必須提交設定並重新啟動防火牆才能使變更生效。



5. **Commit**（認可）。
6. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後選取 **Reboot Device**（重新啟動裝置）。

STEP 7 | 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

STEP 8 | 將您的設定變更提交並推送到受管理的防火牆。**Push to Devices**（推送至裝置）用於檢視在所選 SD-WAN 防火牆中新增的邏輯路由器。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置） 和 **Edit Selections**（編輯選擇）。
2. 選取 **Templates**（範本）並從清單中選擇範本堆疊和範本。
3. 啟用 **Force Template Values**（強制範本值）以使用更新的範本值覆寫本機設定。在使用此選項之前，請檢查防火牆上的取代值，以確保您的提交不會導致任何意外的網路中斷或因為更換這些取代值導致的問題。
4. 按一下 **OK**（確定）并 **Push**（推送）至裝置。

STEP 9 | 重新登入防火牆。

STEP 10 | 選取 **Network**（網路）。

請注意功能表項目，它們比舊版功能表上的單個項目（虛擬路由器）更符合行業標準且更詳細。**Routing**（路由）包括 **Logical Routers**（邏輯路由器）和 **Routing Profiles**（路由設定檔），而路由設定檔包括 **BGP**、**BFD**、**OSPF**、**OSPFv3**、**RIPv2**、**Filters**（篩選器）和 **Multicast**（多點傳送）。

STEP 11 | 當您的設定中有多個範本堆疊時，您必須分別為每範本堆疊啟用 **Advanced Routing**（進階路由）。對您打算為進階路由更新的防火牆上的其他範本堆疊重複步驟 5 到 10。

根據我們的設計要求，在使用進階路由引擎時，邏輯路由器名稱必須與同一範本的虛擬路由器名稱相同。這意味著中樞和分支始終具有相同的路由器名稱。當手動而不是使用移轉指令碼建立邏輯路由器時，您必須確保邏輯路由器名稱和虛擬路由器名稱相同。

STEP 12 | 在 SD-WAN 部署中選取虛擬路由器或邏輯路由器。

選取 **Panorama** > **SD-WAN** > 裝置，以新增將由 Panorama 管理伺服器管理的 SD-WAN 裝置（SD-WAN 中樞或分支防火牆）。

除了用於新增 SD-WAN 裝置的現有設定選項外，您現在還可以為 **Router Name**（路由器名稱）選取邏輯路由器（用於進階路由引擎）或虛擬路由器（用於舊版引擎）。使用進階路由引擎時，同一範本的邏輯路由器名稱和虛擬路由器名稱必須相同，這一點很重要。

選取用於在 SD-WAN 中樞和分支之間進行路由的 **Router Name**（路由器名稱）（邏輯或虛擬路由器）：

- 如果虛擬路由器和邏輯路由器名稱相同，則 **Router Name**（路由器名稱）顯示同一個名稱。
- 如果虛擬路由器名稱和邏輯路由器名稱不同，則 **Router Name**（路由器名稱）會同時顯示虛擬路由器名稱和邏輯路由器名稱。您可以根據需要選取虛擬路由器（舊版引擎）或邏輯路由器（進階路由引擎）。

監控與報告

監控 VPN 叢集中應用程式和連結的健康情況狀態並產生報告，以識別並解決問題。要讓 Panorama™ 管理伺服器顯示 SD-WAN 應用程式和連結健康情況資訊，您必須在 將您的 SD-WAN 防火牆新增為受管理裝置 時啟用 SD-WAN 防火牆以將裝置監控資料推送到 Panorama，並設定將日誌轉送到 Panorama。如果您沒有設定 SD-WAN 防火牆將日誌轉送到 Panorama，SD-WAN **Monitoring**（監控）將不會顯示應用程式或連結監控情況資訊。

要讓 *Panorama* 收集 *SD-WAN* 監控資料，必須將 *SD-WAN* 設定從 *Panorama* 推送到 *SD-WAN* 防火牆。如果未顯示 *SD-WAN* 監控資料，請驗證是否成功推送了 *SD-WAN* 設定。

- 監控 SD-WAN 工作
- 監控 SD-WAN 應用程式和連結效能
- 監控 Prisma Access Hub
- 產生 SD-WAN 報告

監控 SD-WAN 工作

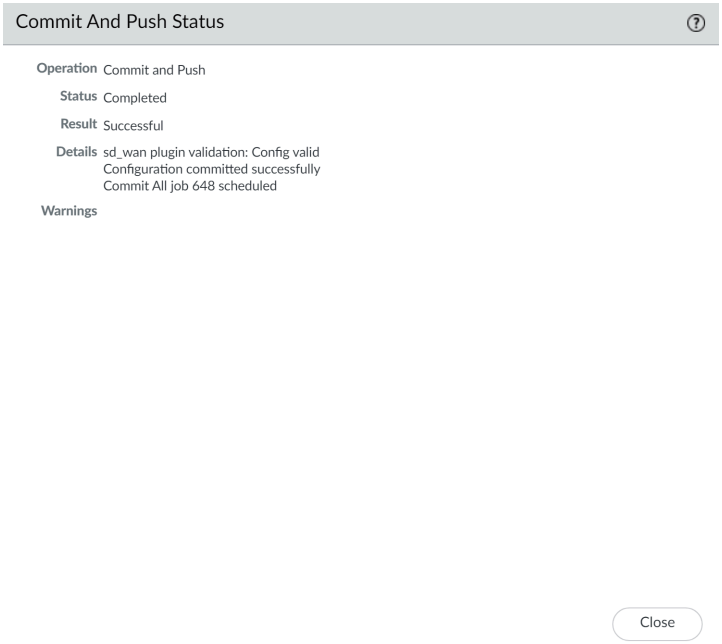
監控提交、推送和從 Panorama™ 管理伺服器執行的其他 SD-WAN 工作，以獲取有關特定工作的洞察和詳細資訊。

如果工作成功但帶有警告或者工作失敗，您可以檢視詳細的警告和描述以更好地了解如何解決設定錯誤。此外，您可以檢視上次推送狀態詳細資料，以檢閱有關導致工作警告或錯誤的原因的詳細資訊。

STEP 1 | 登入 Panorama 網頁介面。

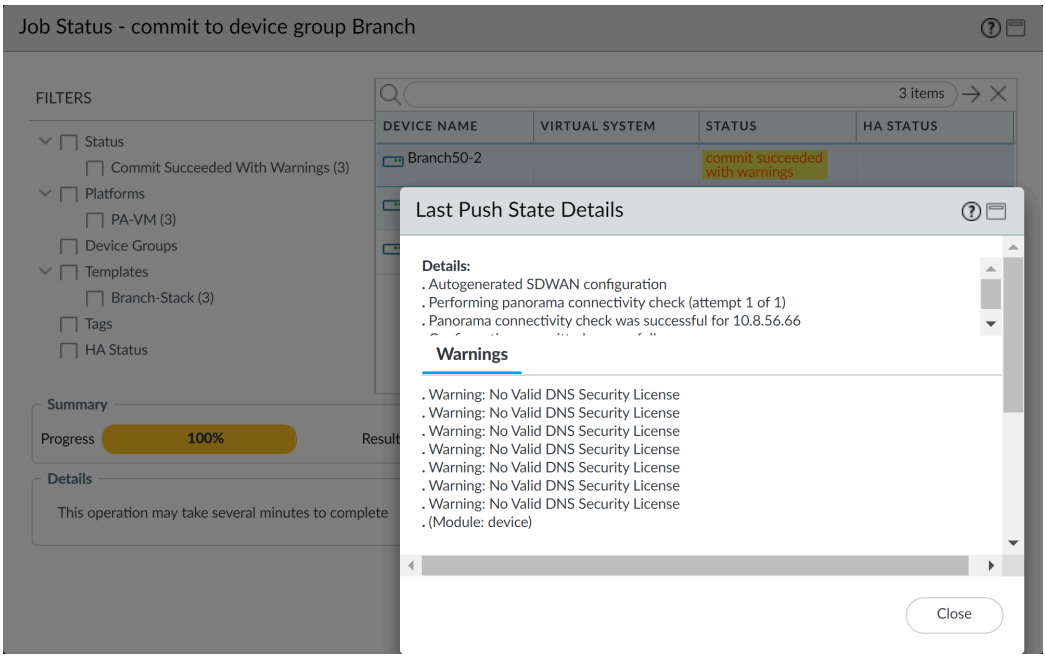
STEP 2 | 在編輯 SD-WAN 組態後，**Commit**（提交）您的變更以檢視工作狀態。

工作狀態視窗顯示執行的操作、結果，以及與工作狀態相關的任何詳細資料和警告。



STEP 3 | 檢視成功但帶有警告或者失敗的工作的上次推送詳細資料。

1. 按一下網頁介面下方的 **Tasks**（工作）（ Tasks ）以開啟工作管理員。
2. 按一下 SD-WAN 工作的工作 **Type**（類型）。
3. 按一下工作 **Status**（狀態）以檢視工作的上次推動狀態詳細資料。
4. 檢閱上次推送狀態詳細資料以識別並解決組態問題。



監控 SD-WAN 應用程式和連結效能

監控 VPN 叢集中的應用程式和連結效能，透過檢視所有 VPN 叢集中的摘要資訊，然後依次向下鑽研以將問題隔離到受影響的網站、應用程式和連結，從而對問題進行疑難排解。SD-WAN 流量的可視性顯示在接收流量的 SD-WAN 防火牆上。例如，對於從中樞防火牆到分支防火牆的流量，SD-WAN 監控資料反映在分支防火牆上。登陸儀表板顯示：

- 應用程式效能
  - **Impacted**（受影響）—VPN 叢集中的一個或多個應用程式，對於這些應用程式，在防火牆可選擇的路徑清單中，沒有任何路徑的抖動、延遲或封包遺失效能滿足路徑品質設定檔中指定的閾值。
  - **OK**（成功）—沒有出現抖動、延遲或封包遺失問題的 VPN 叢集、中樞和分支的數量。
- 連結效能
  - **Error**（錯誤）—VPN 叢集中的一個或多個網站具有連線問題，例如當通道或虛擬介面 (VIF) 關閉時。
  - 警告—連結具有頻寬（在具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0 中受支援）頻寬（在具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本中受支援）的 VPN 叢集、中樞和分支數目；超過度量 7 天移動平均值的抖動、延遲或封包遺失效能測量值。
  - 正常—沒有頻寬（在具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0 中受支援）頻寬（在具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本中受支援）的 VPN 叢集、中樞和分支數目；抖動、延遲或封包遺失效能問題。

  從 PAN-OS 11.2.0 開始，SD-WAN 外掛程式 3.3.0 和更新版本支援「頻寬」，這是連結效能的主要度量。從 PAN-OS 11.1.5 開始，SD-WAN 外掛程式 3.2.2 和更新版本支援「頻寬」，這是連結效能的主要度量。

如果中樞或分支防火牆設定了包含正向錯誤更正的 SD-WAN 原則規則，則會顯示 `Error Correction Initiated`（已啟動錯誤更正）訊息，通知您中樞或分支防火牆已偵測到應用程式傳輸資料中的錯誤，且已更正。

僅當流量從 *SD-WAN* 中樞流向 *SD-WAN* 分支且與附加了錯誤更正設定檔的 SD-WAN 原則規則相符時，*SD-WAN* 中樞才會顯示 *`Error Correction Initiated`*（已啟動錯誤更正）。

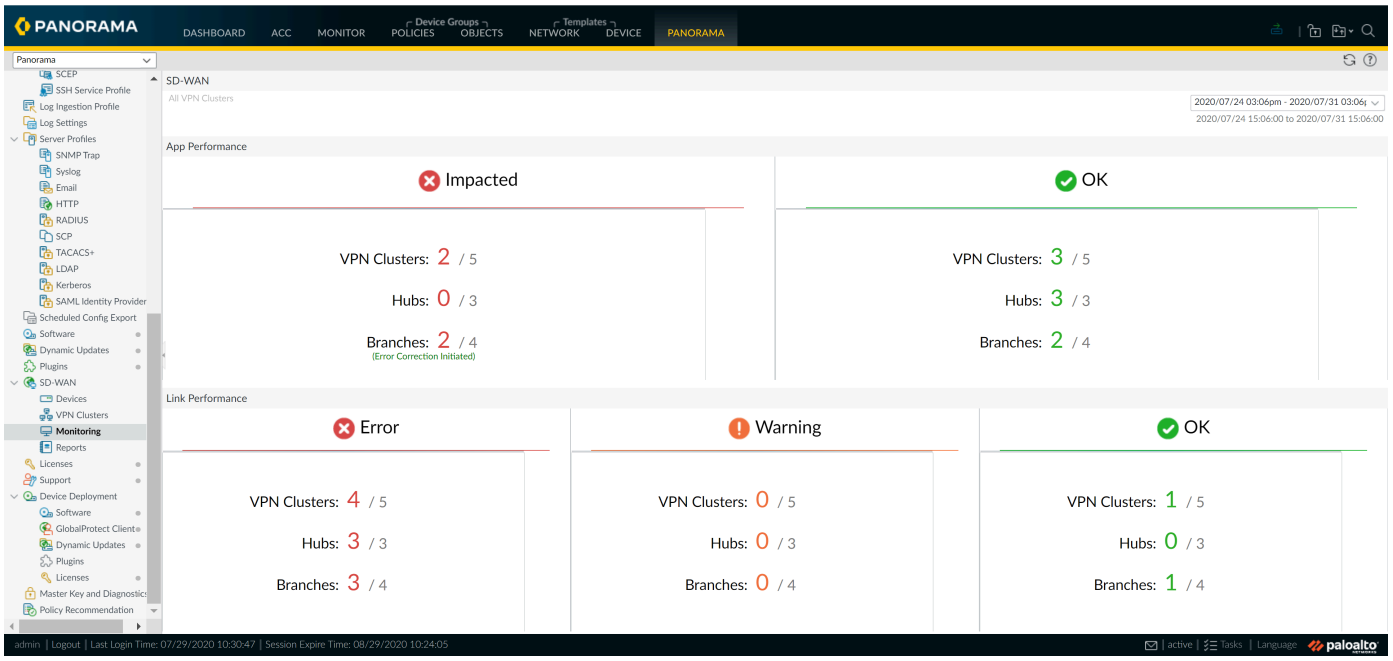
從登陸儀表板中，將檢視縮小到具有「錯誤」或「警告」狀態的受影響應用程式或連結。然後選取受影響的網站以檢視網站層級的詳細資料。從網站中，檢視應用程式層級或連結層級的詳細資料。

請參閱 監控 Prisma Access Hub 應用程式和連結效能 以監控 Prisma Access 中樞的應用程式和連結效能。

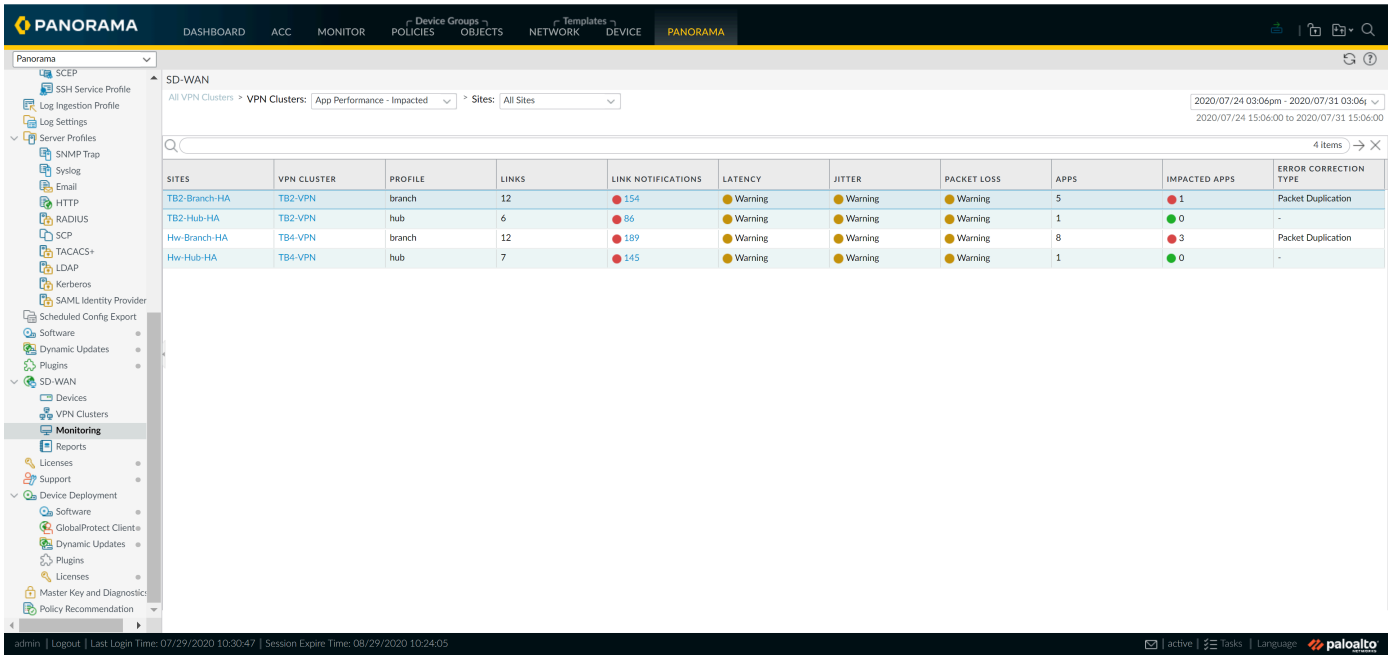
如果沒有資料或螢幕指示 *SD-WAN* 未定義，請查看相容性矩陣，瞭解您使用的 *Panorama* 版本是否支援您嘗試使用的 *SD-WAN* 外掛程式版本。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama > SD-WAN > Monitoring**（監控）以檢視 VPN 叢集、中樞和分支的健康情況狀態摘要概覽。



STEP 3 | 按一下可指出 [Impacted（受影響）]、[Error（錯誤）] 或 [Warning（警告）] 計數的 [App Performance（應用程式效能）] 或 [Link Performanc（連結效能）] 摘要，以根據頻寬（在具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0 中受支援，以實現連結效能）、頻寬（在具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本中受支援）、延遲、抖動和封包遺失來檢視網站和其狀態的詳細清單。



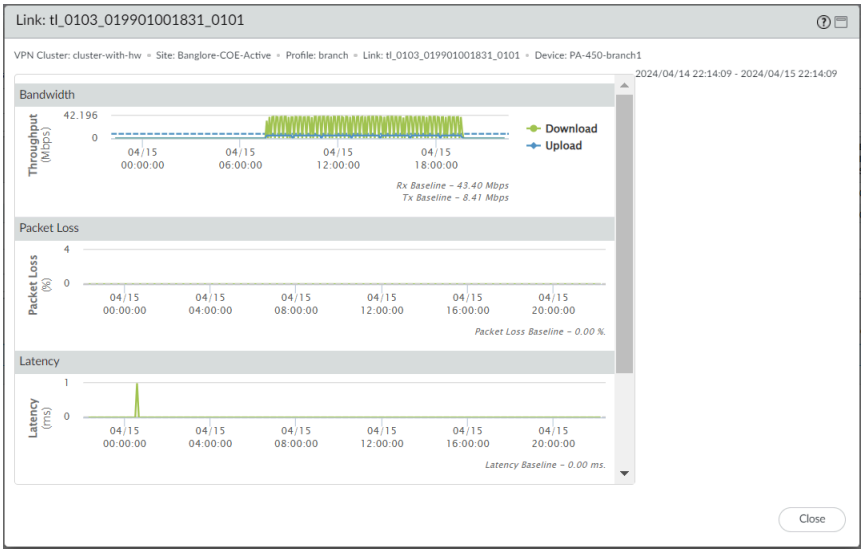
STEP 4 | 按一下顯示「錯誤」或「警告」的網站以查看一個 VPN 叢集。網站資料顯示應用程式效能和連結效能，包括受影響的應用程式。此外，使用網站篩選器可基於連結通知、延遲偏差、抖動偏差、封包遺失偏差或受影響的應用程式檢視 VPN 叢集。

（具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0）（具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本）您現在可以檢視 VPN 叢集中所選取網站的新連結效能參數 **maximum upload/download speed**（最大上傳/下載速度）。

按一下每個 **Link**（連結）以檢視基準頻寬（在具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0 中受支援）頻寬（在具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本中受支援）；針對通道所測量的抖動、封包遺失和延遲。

（具有 SD-WAN 外掛程式 3.3.0 和更新版本的 PAN-OS 11.2.0）（具有 SD-WAN 外掛程式 3.2.2 和更新版本的 PAN-OS 11.1.5 和更新版本）**Bandwidth**（頻寬）圖顯示實體和通道連結的滾動最大上傳和下載速度。

- 針對實體連結，此圖會顯示作為最大值的 SD-WAN 介面設定檔設定（如果已設定）。否則，此圖會顯示實體連結到目前為止所看到作為最大值的最大 Tx 和 Rx 值。
- 針對通道連結，此圖會顯示通道到目前為止所看到作為最大值的最大 Tx 和 Rx 值。



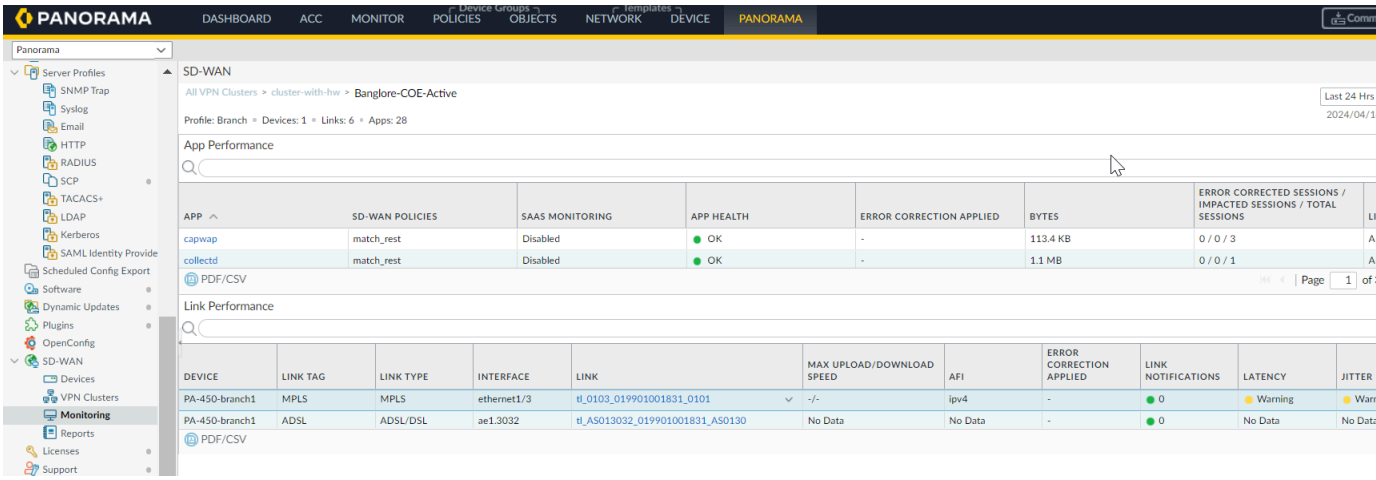
對於直接網際網路存取 (DIA) 連結上的 SaaS 應用程式，**SaaS Monitoring**（**SaaS** 監控）欄指示該應用程式是否在 SaaS Quality（SaaS 品質）設定檔中建立並與一個或多個 SD-WAN 原則規則相關聯。

- `Disabled`（已停用）—該應用程式不是在 SaaS 品質設定檔中設定的 SaaS 應用程式。
- `Enabled`（已啟用）—該應用程式是在 SaaS 品質設定檔中設定的 SaaS 應用程式，且與一個或多個 SD-WAN 政策相關聯。

如果您將應用程式的錯誤更正設定檔與 SD-WAN 原則規則相關聯，則 **Error Correction Applied**（已套用錯誤更正）欄將顯示是否套用了錯誤更正以及套用了哪種類型的錯誤更正。此外，您可以檢視 **Error Corrected Sessions**（已更正錯誤的工作階段數）**/Impacted**

Sessions（受影響的工作階段數）**/Total Sessions**（工作階段總數），以瞭解在指定的時間範圍內，分支或中樞防火牆更正了多少個工作階段的錯誤。

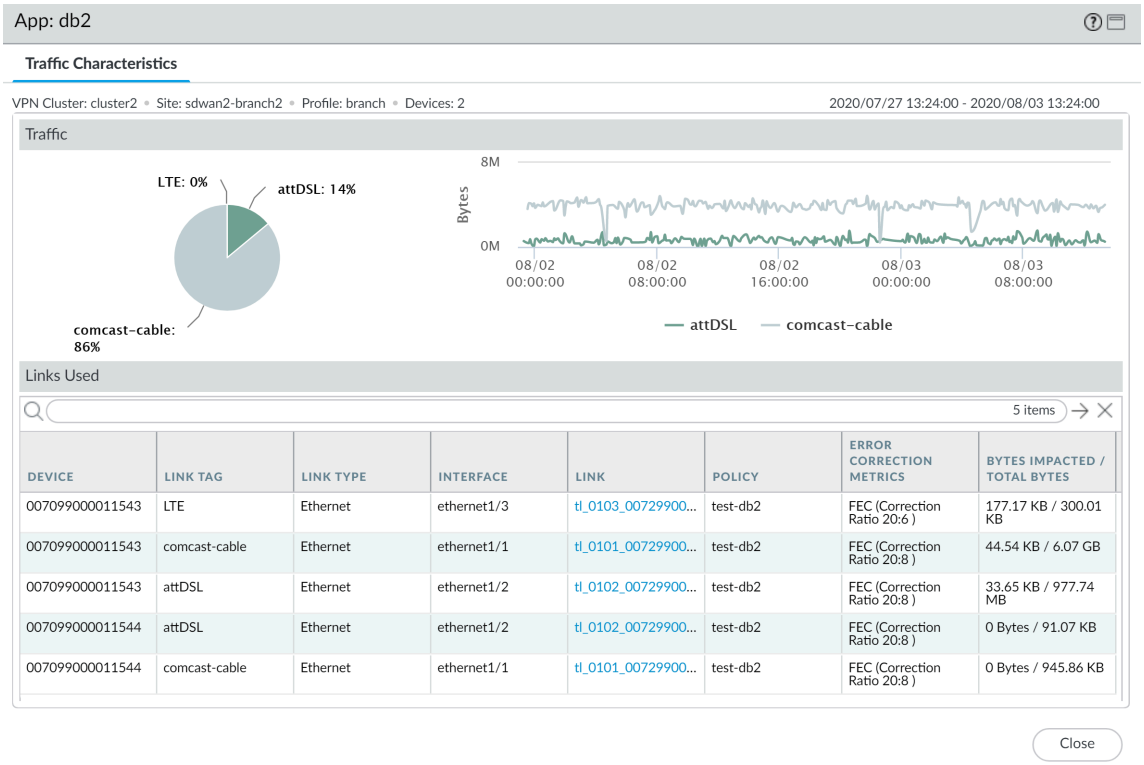
按一下 **PDF/CSV**，將網站中應用程式和連結的詳細健康情況資訊以 PDF 或 CSV 格式匯出

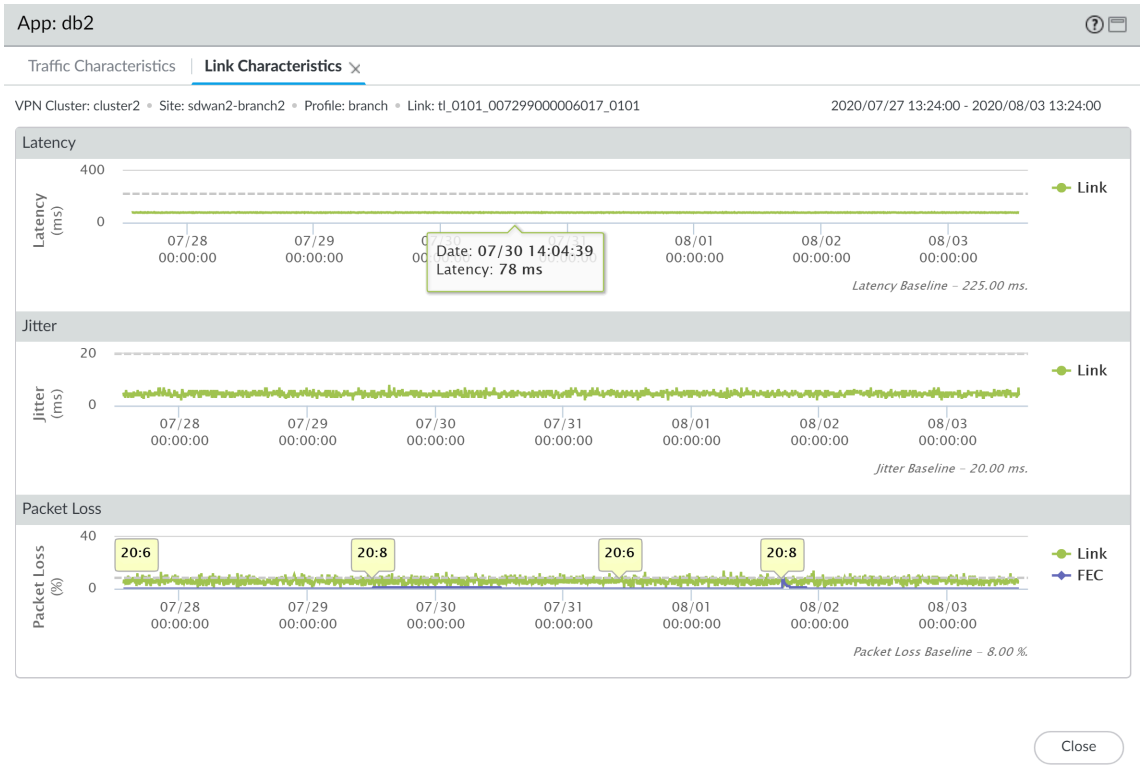


STEP 5 | 按一下具有需要關注的應用程式的分支或中樞。

STEP 6 | 按一下受影響的應用程式以檢視應用程式層級或連結層級的詳細資料。

例如，檢視應用程式的連結特性以瞭解應用程式在指定連結上的延遲、抖動和封包遺失情況。此外，您還可以檢視何時對連結套用了錯誤更正。





監控 Prisma Access Hub

對您的 Prisma Access Hub 應用程式和連結效能進行基準測量和監控，以瞭解如何設定和修改 SD-WAN 連結管理設定檔。

- 對您的 Prisma Access Hub 應用程式和連結效能進行基準測量
- 監控 Prisma Access Hub 應用程式和連結效能

對您的 Prisma Access Hub 應用程式和連結效能進行基準測量

在您 設定 SD-WAN 連結管理設定檔 之前，Palo Alto Networks 建議您對 Prisma Access Hub 應用程式和連結效能進行基準測量，以更好地了解 Prisma Access Hub 的正常有效負載活動，以避免為不需要的應用程式和流量進行不必要的連結交換。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 將 PAN-OS 防火牆裝載到 Prisma Access。

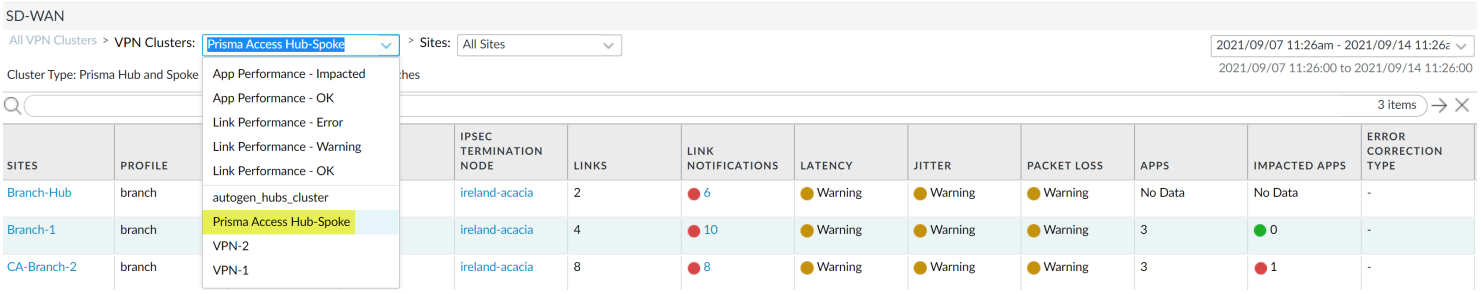
STEP 3 | 選取 **Panorama** > **SD-WAN** > **Monitoring**（監控），並修改 SD-WAN 監控時間範圍。

用於對 Prisma Access Hub 應用程式和連結效能進行基準測量的時間越長，基準就越準確。至少使用三天的應用程式和連結效能資料來對用於建立 SD-WAN 連結管理設定檔的延遲、抖動和封包遺失資料進行基準測量。

Palo Alto Networks 建議評估七天的應用程式和連結效能資料，以確定 *Prisma Access Hub* 的延遲、抖動和封包遺失基準。

STEP 4 | 篩選 SD-WAN 監控以僅顯示您的 Prisma Access 中樞-支點 VPN 叢集。

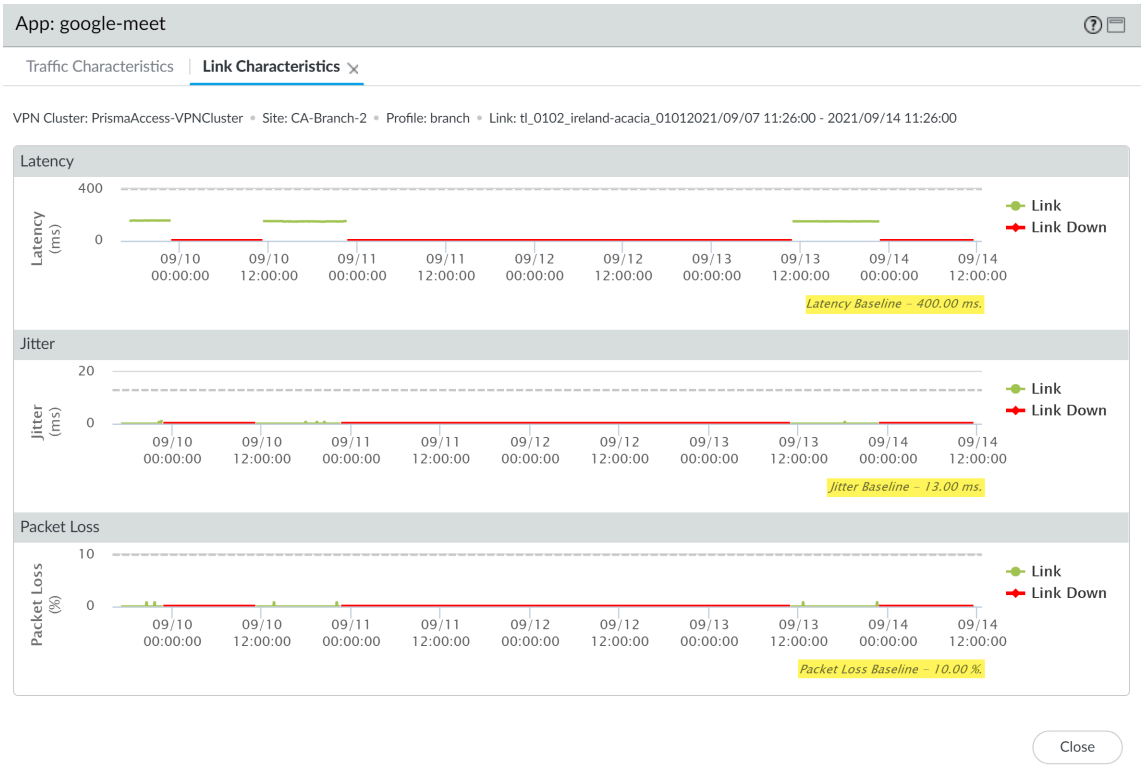
1. 按一下表明「受影響」、「錯誤」或「警告」計數的「應用程式效能」或「連結效能」摘要，以基於延遲、抖動和封包遺失檢視網站及其狀態的詳細清單。
2. 在 VPN叢集複選器中，選取 **Prisma Access Hub-Spoke**（**Prisma Access** 中樞-支點）。
3. 按一下網站以檢視 Prisma Access Hub 的詳細健康資訊。



STEP 5 | 檢閱 Prisma Access Hub 應用程式的連結特性。

1. 按一下 App Performance（應用程式效能）部分的應用程式以檢視流量特性和用於應用程式流量的連結。
2. 按一下每個連結可檢視該應用程式在連結上測得的延遲、抖動和封包遺失基準。

   對所有連結重複此操作，直到您收集到足夠的基準資料來修改您的 Prisma Access Hub 路徑品質設定檔。



STEP 6 | 根據您收集的延遲、抖動和封包遺失基準修改您的 Prisma Access Hub 路徑品質設定檔。

STEP 7 | 根據需要繼續設定 SD-WAN。

STEP 8 | 監控 Prisma Access Hub 應用程式和連結效能以進一步微調您的 SD-WAN 連結管理設定檔。

監控 Prisma Access Hub 應用程式和連結效能

監控 Prisma Access Hub 的應用程式和連結效能，透過檢視所有 VPN 叢集中的摘要資訊，然後依次向下鑽研以將問題隔離到受影響的網站、應用程式和連結，從而對問題進行疑難排解。SD-WAN 流量的可視性顯示在接收流量的 Prisma Access 部署或 SD-WAN 防火牆上。例如，對於從中樞防火牆到分支防火牆的流量，SD-WAN 監控資料反映在分支防火牆上。登陸儀表板顯示：

- 應用程式效能
  - **Impacted**（受影響）—VPN 叢集中的一個或多個應用程式，對於這些應用程式，在防火牆可選擇的路徑清單中，沒有任何路徑的抖動、延遲或封包遺失效能滿足路徑品質設定檔中指定的閾值。
  - **OK**（成功）—沒有出現抖動、延遲或封包遺失問題的 VPN 叢集、中樞和分支的數量。

- 連結效能
  - **Error**（錯誤）—VPN 叢集中的一個或多個網站具有連線問題，例如當通道或虛擬介面 (VIF) 關閉時。
  - **Warning**（警告）—其連結的抖動、延遲或封包遺失效能度量值超出指標的七天移動平均值的 VPN 叢集、中樞和分支數量。
  - **OK**（成功）—沒有出現抖動、延遲或封包遺失問題的 VPN 叢集、中樞和分支的數量。

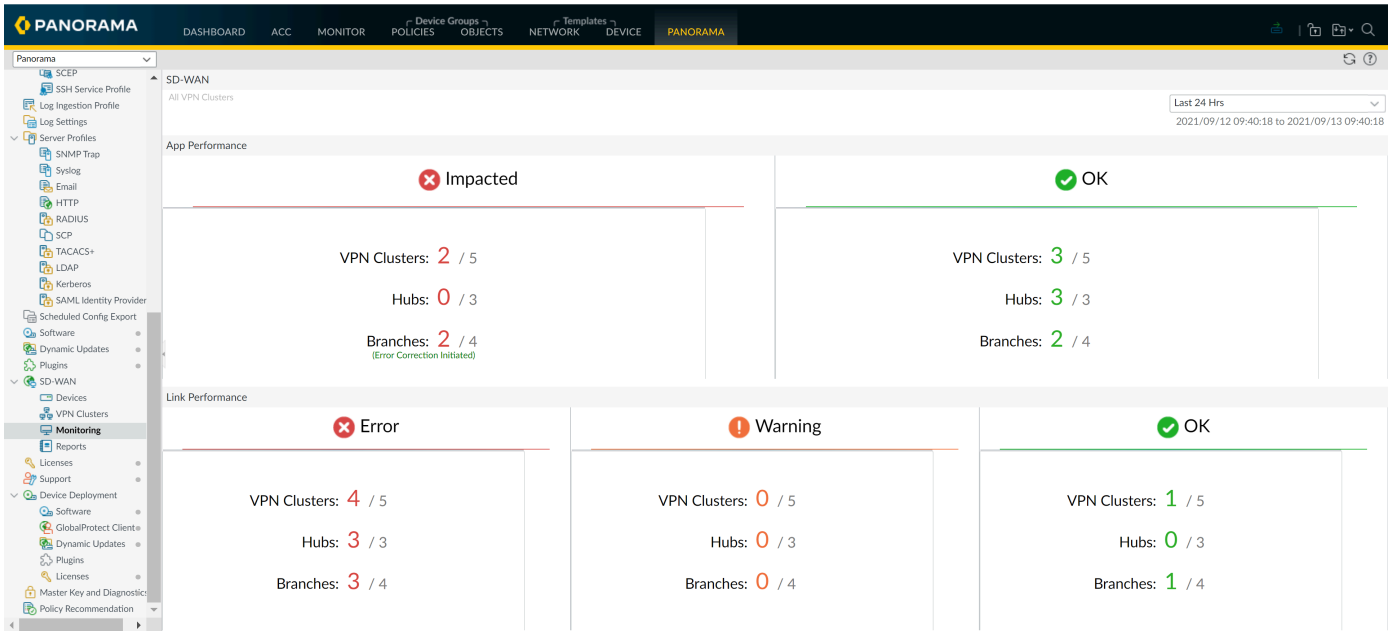
從登陸儀表板中，將檢視縮小到具有「錯誤」或「警告」狀態的受影響應用程式或連結。然後選取受影響的網站以檢視網站層級的詳細資料。從網站中，檢視應用程式層級或連結層級的詳細資料。

請參閱 監控 SD-WAN 應用程式和連結效能 以監控所有 SD-WAN 網站上的應用程式和連結效能

如果沒有資料或螢幕指示 *SD-WAN* 未定義，請查看相容性矩陣，瞭解您使用的 *Panorama* 版本是否支援您嘗試使用的 *SD-WAN* 外掛程式版本。

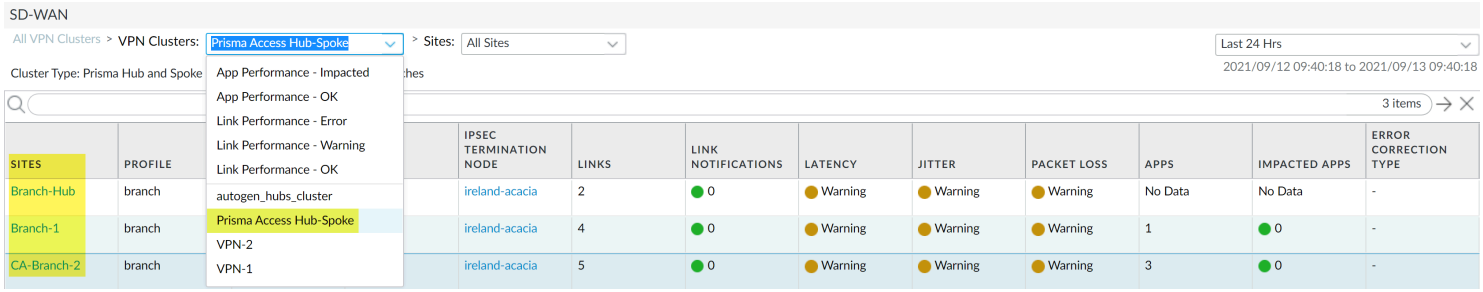
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama > SD-WAN > Monitoring**（監控）以檢視 VPN 叢集、中樞和分支的健康情況狀態摘要概覽。



STEP 3 | 篩選 SD-WAN 監控以僅顯示您的 Prisma Access 中樞-支點 VPN 叢集。

1. 按一下表明「受影響」、「錯誤」或「警告」計數的「應用程式效能」或「連結效能」摘要，以基於延遲、抖動和封包遺失檢視網站及其狀態的詳細清單。
2. 在 VPN叢集複選器中，選取 **Prisma Access Hub-Spoke**（**Prisma Access** 中樞-支點）。
3. 按一下網站以檢視 Prisma Access Hub 的詳細健康資訊。



STEP 4 | 檢閱 Prisma Access Hub 的詳細健康資訊。

網站資料顯示 Prisma Access 裝載詳細資訊，以及應用程式效能和連結效能，包括受影響的應用程式。

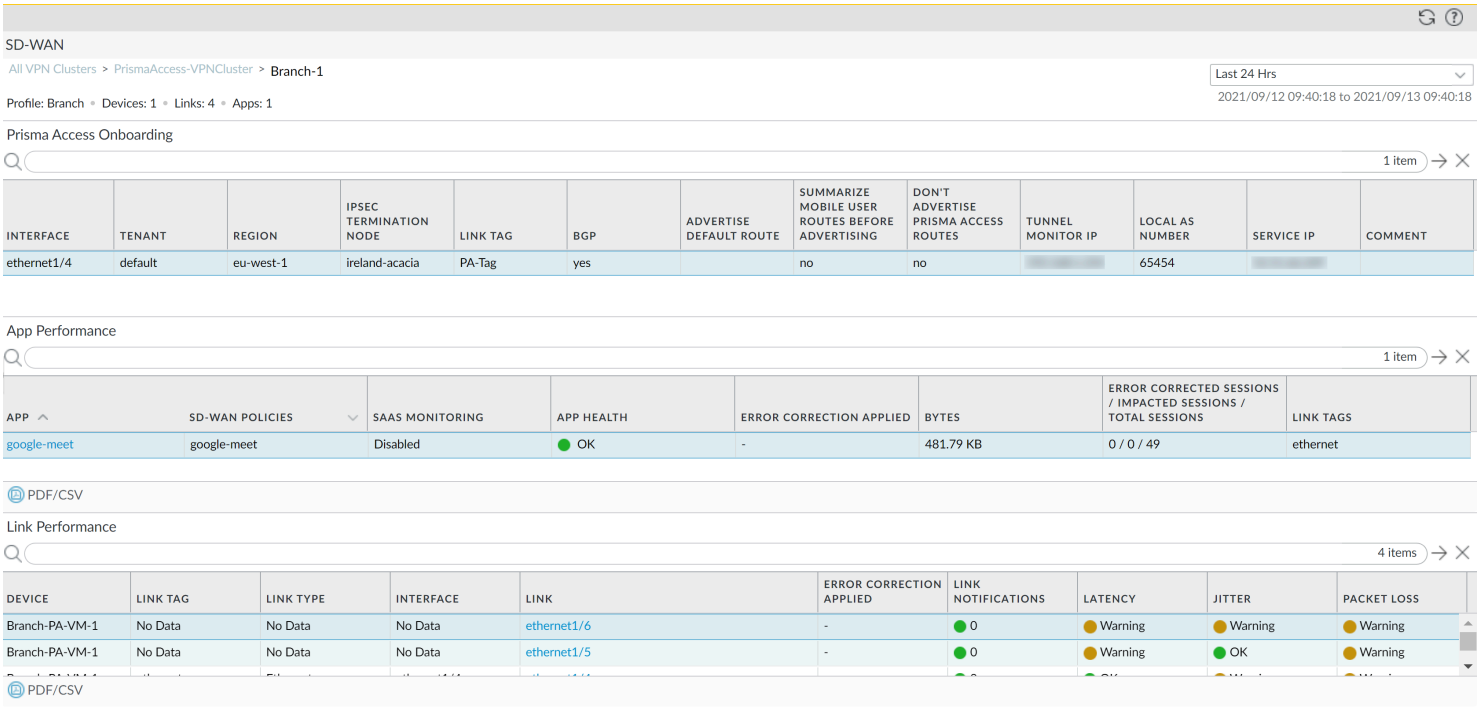
對於直接網際網路存取 (DIA) 連結上的 SaaS 應用程式，**SaaS Monitoring**（**SaaS** 監控）欄指示該應用程式是否在 SaaS Quality（SaaS 品質）設定檔中建立並與一個或多個 SD-WAN 原則規則相關聯。

- `Disabled`（已停用）—該應用程式不是在 SaaS 品質設定檔中設定的 SaaS 應用程式。
- `Enabled`（已啟用）—該應用程式是在 SaaS 品質設定檔中設定的 SaaS 應用程式，且與一個或多個 SD-WAN 政策相關聯。

如果您將應用程式的錯誤更正設定檔與 SD-WAN 原則規則相關聯，則 **Error Correction Applied**（已套用錯誤更正）欄將顯示是否套用了錯誤更正以及套用了哪種類型的錯誤更正。此外，您可以檢視 **Error Corrected Sessions**（已更正錯誤的工作階段數）**/Impacted**

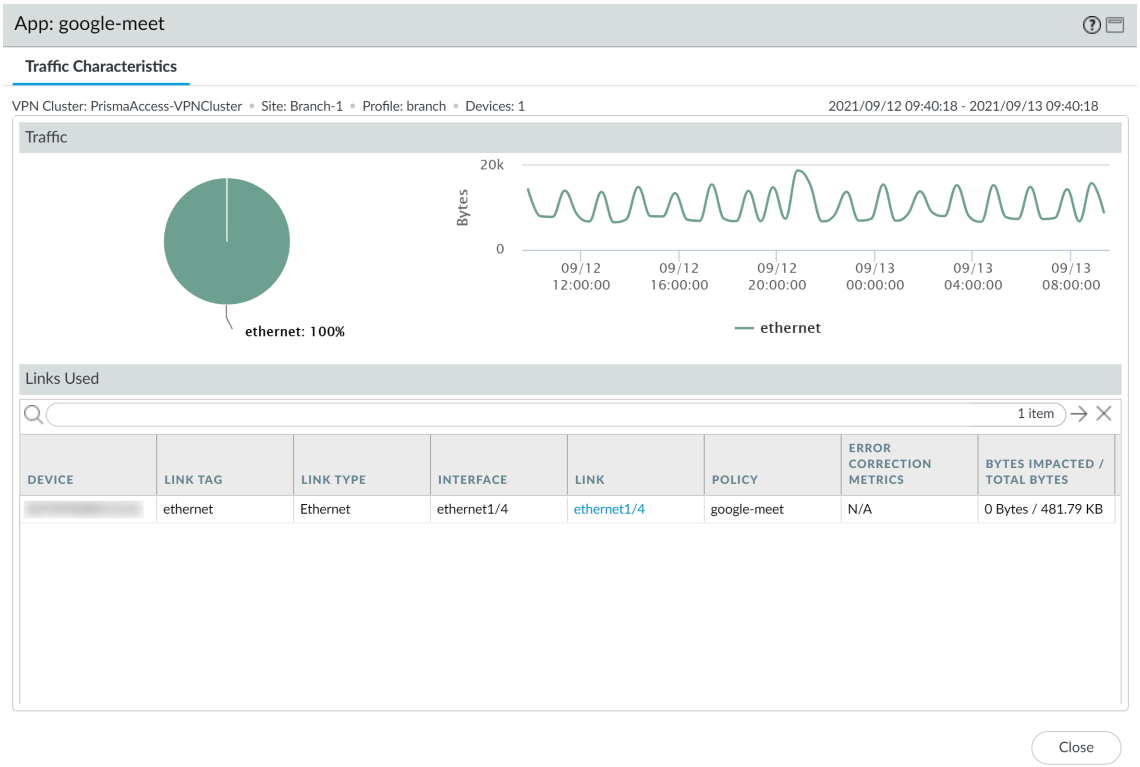
Sessions（受影響的工作階段數）**/Total Sessions**（工作階段總數），以瞭解在指定的時間範圍內，分支或中樞防火牆更正了多少個工作階段的錯誤。

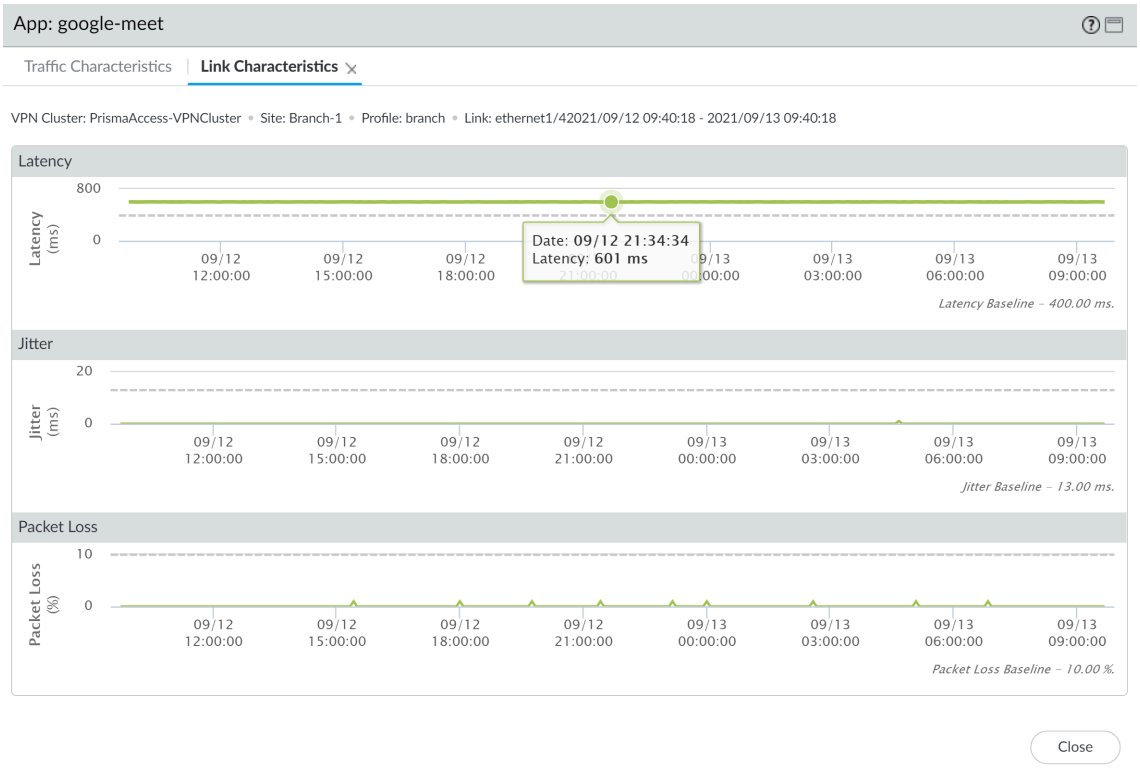
按一下 **PDF/CSV**，將網站中應用程式和連結的詳細健康情況資訊以 PDF 或 CSV 格式匯出



STEP 5 | 按一下受影響的應用程式以檢視應用程式層級或連結層級的詳細資料。

例如，檢視應用程式的連結特性以瞭解應用程式在指定連結上的延遲、抖動和封包遺失情況。此外，您還可以檢視何時對連結套用了錯誤更正。





產生 SD-WAN 報告

設定並產生 SD-WAN 報告，詳細描述路徑品質下降頻率最高的前幾個應用程式或連結。應用程式或連結在報告中顯示順序基於受影響的資料量；受影響的資料越多，應用程式或連結顯示在報告中的位置就越高。SD-WAN 報告視需要產生，無法排程。使用 SD-WAN 報告確認正確的應用程式或連結輸送量，或確保使用者未注意到應用程式或連結的影響。例如，如果您的 ISP 保證連結上一定量的輸送量，請為該連結產生一個「連結效能」報告以驗證是否遵守了保證的頻寬。

從 Panorama™ 管理伺服器，您只能為所有已啟用 SD-WAN 的防火牆中的應用程式或連結產生報告。要為單個防火牆處理的應用程式或連結產生報告，您必須在防火牆上本機建立並產生報告。

如果沒有資料或螢幕指示 *SD-WAN* 未定義，請查看相容性矩陣，瞭解您使用的 *Panorama* 版本是否支援您嘗試使用的 *SD-WAN* 外掛程式版本。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama > SD-WAN > Reports**（報告），然後 **Add**（新增）一個新報告。

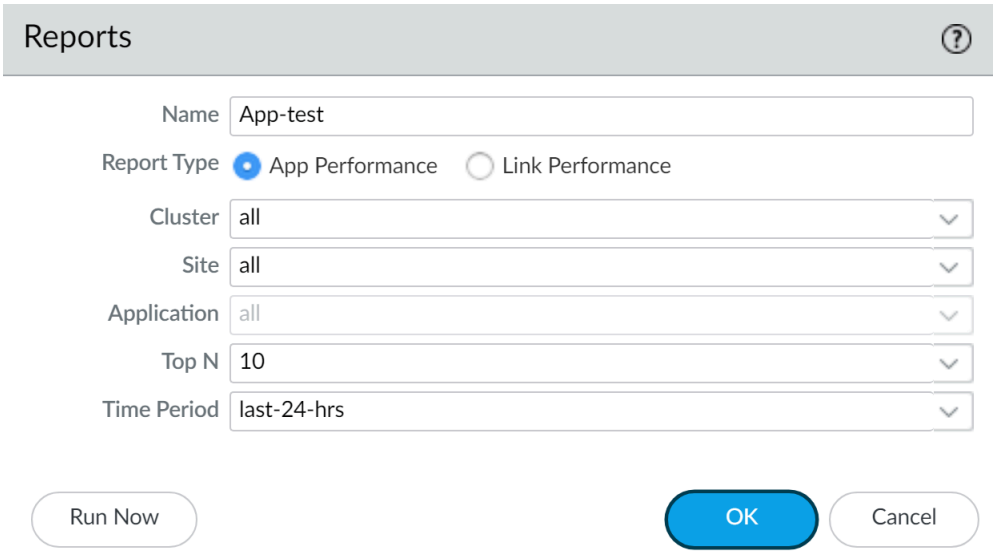
STEP 3 | 設定 SD-WAN 報告參數。

1. 輸入報告的描述性 **Name**（名稱）。
2. 選擇要產生的 **Report Type**（報告類型）：
   - 選取 **App Performance**（應用程式效能）以產生僅詳述應用程式健康情況效能的報告。
   - 選取 **Link Performance**（連結效能）以產生僅詳述連結健康情況效能的報告。
3. 選取要為其產生報告的 VPN **Cluster**（叢集）。預設情況下，會選取 **all**（全部）。
4. 選取所選 VPN 叢集內要為其產生報告的 **Site**（網站）。預設情況下，會選取 **all**（全部）。

   如果您已選取 **all**（全部）叢集，那麼此欄位將以灰色顯示，無法選取網站。
5. （僅應用程式效能）選取要為其產生報告的 **Application**（應用程式）。

   如果您已選取 **all**（全部）叢集和網站，那麼此欄位將以灰色顯示，無法選取單個應用程式。
6. （僅連結效能）選取要為其產生報告的 **Link Tag**（連結標籤）。選取一個連結標籤會為叢集或網站中使用該標籤分組的所有連結產生報告。預設情況下，會選取 **all**（全部）。
7. （僅連結效能）選取要為其產生報告的 **Link Type**（連結類型）。選取一個連結類型會為叢集或網站中指定類型的所有連結產生報告。預設情況下，會選取 **all**（全部）。
8. 選取要包含在報告中的 **Top N**（前 **N** 個）應用程式或連結。此設定確定要包含在報告中的出現健康情況下降的應用程式或連結數量。預設情況下，報告包括出現健康情況下降的前 **5** 個應用程式或連結。
9. 指定要產生報告的 **Time Period**（時間週期）。預設情況下，會選取 **None**（無）並查詢應用程式和連結的整個健康情況狀態歷程記錄。

STEP 4 | 按一下 **Run Now**（立即執行）以產生報告。



STEP 5 | 檢視產生的報告，並按一下 **Export XML**（匯出 **XML**）以 XML 格式將報告匯出到本機裝置。就緒時，按一下 **Close**（關閉）。

App Performance Report by application - top 10 apps across all clusters and all sites

Time period 2020-09-15 14:14:24 to 2020-09-16 14:14:24

CLUSTER	SITE	APP	SAAS MONITORING	AVG FLAP/SESSION	IMPACTED/TOT... BYTES PER APP	ERROR CORRECTED/IM... SESSIONS PER APP	POLICIES	Link Info			
								LINK TAG	LINK TYPE	ERROR CORRECTED METRICS	IMPACTED/... BYTES PER LINK TAG
ClusterHub245	Branch20	ssh	Disabled	175	9.08GB/339.08...	0/4/12	Tunnel_SCP	BroadBand2	ADSL/DSL		4.45GB/23....
							Tunnel_SCP	BroadBand1	Cablemodem		4.62GB/51....
ClusterHub245	Hub254	bgp	Disabled	16	904.35KB/19.4...	0/1/1		BroadBand2			904.24KB/9...
								BroadBand1	Ethernet		117.00b/11...
ClusterHub245	Branch50	ftp	Disabled	0	900.00b/1.64KB	0/1/2	Tunnel_FTP	BroadBand1	Cablemodem		900.00b/1.6...
ClusterHub245	Branch20	bgp	Disabled	15	380.00b/18.68...	0/1/1		BroadBand2	ADSL/DSL		170.00b/17...
								BroadBand1	Cablemodem		210.00b/21...
autogen_hubs_cl...	Hub254	dropbox-base	Disabled	0	0/38.41KB	0/0/33	DIA	BroadBand1	Ethernet		0/27.47KB
							DIA	BroadBand2	Ethernet		0/10.94KB
ClusterHub245	Branch20	taobao	Disabled	0	0/1.65MB	0/0/1.4k	DIA	BroadBand2	ADSL/DSL		0/729.81KB
							DIA,test-rule	BroadBand1	Cablemodem		0/962.53KB
ClusterHub245	Branch25	netbios-dg	Disabled	0	0/3.56KB	0/0/15	test-rule	BroadBand1	Cablemodem		0/3.56KB
ClusterHub245	Branch25	youku-base	Disabled	0	0/167.28KB	0/0/115	DIA	BroadBand2	ADSL/DSL		0/20.36KB
							DIA,test-rule	BroadBand1	Cablemodem		0/146.92KB
ClusterHub245	Hub254	insufficient-data	Disabled	0	0/24.92KB	0/0/105	BranchToBranch...	BroadBand1	Ethernet		0/13.05KB
							BranchToBranch...	BroadBand2	Ethernet		0/11.87KB
autogen_hubs_cl...	Hub254	apt-get	Disabled	0	0/62.36KB	0/0/2	DIA	BroadBand1	Ethernet		0/62.36KB

Export XML Close

STEP 6 | 在「報告」快線視窗中，按一下 **OK**（確定）以儲存您的已設定報告。

STEP 7 | **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

疑難排解

使用 Panorama™ 管理伺服器命令行介面 (CLI) 檢視 SD-WAN 資訊並執行操作。

將 CLI 命令用於 SD-WAN 工作

使用以下 CLI 命令以檢視和清除 SD-WAN 資訊，以及檢視 SD-WAN 全域計數器。您還可以檢視 VPN 通道資訊、BGP 資訊和 SD-WAN 介面資訊。

如果您想要 ...	使用 ...
檢視或清除 **SD-WAN** 資訊	
• 檢視 SD-WAN 介面的路徑名稱和 ID、其狀態、本機和對等 IP 位址以及通道介面編號。	`> show sdwan connection all | <sdwan-interface>`
• 檢視散佈掃虛擬 SD-WAN 介面的每個通道成員的工作階段數量和百分比。	`> show sdwan session distribution policy-name <sdwan-policy-name>`
• 檢視傳送流量到指定虛擬 SD-WAN 介面的 SD-WAN 原則規則的名稱，以及流量散佈方法，設定的延遲、抖動和封包遺失閾值，為規則標識的連結標籤，和成員通道介面。	`> show sdwan rule vif sdwan.x`
• 檢視 SD-WAN 事件，如路徑選擇和路徑品質度量。 對於 *PAN-OS 10.0.0* 和 *10.0.1*，當您進行 *SD-WAN* 設定變更（例如，路徑品質設定檔變更）導致選取了不同的 *SD-WAN* 路徑時，流量日誌不會計數或記錄路徑變更。	`> show sdwan event`
• 清除 SD-WAN 事件。	`> clear sdwan event`

• 檢視虛擬 SD-WAN 介面（指定介面編號或名稱）上的延遲、抖動和封包遺失。
 	
在三個時間範圍內對延遲、抖動和封包遺失進行度量並取平均值。每個時間範圍都有一個健康情況版本，當健康情況參數值（超出閾值）變更時，該版本會遞增。除即時度量值外，還有當前使用度量值，即在上次即時值變更超出閾值時參數的值。
	`> show sdwan path-monitor stats vif <sdwan.x>`
	
	`> show sdwan path-monitor stats vif <sdwan-interface-name>`

如果您想要 ...	使用 ...
• 檢視指定工作階段匹配的 SD-WAN 原則規則的名稱，來源和目的地通道介面，為規則設定的延遲、抖動和封包遺失百分比，以及流量散佈方法。 對於 *PAN-OS 10.0.0* 和 *10.0.1*，當您進行 *SD-WAN* 設定變更（例如，路徑品質設定檔變更）導致選取了不同的 *SD-WAN* 路徑時，流量日誌不會計數或記錄路徑變更。	**> show sdwan session path-select session-id <session-id>**
• 檢視虛擬 SD-WAN 連結的監控模式（積極或寬鬆）和更新間隔。	**> show sdwan path-monitor parameter path-name <sdwan-path-name>**
• 檢視虛擬 SD-WAN 介面的監控模式（積極或寬鬆）、更新間隔和探查統計資料。	**> show sdwan path-monitor parameter vif <sdwan.x>**
檢視全域計數器以對 **SD-WAN** 進行疑難排解	

• 在分支上，驗證傳送的 SD-WAN 探查要求封包的數量等於接收到的探查回覆封包的數量。
 	
在分支防火牆上，大多數 SD-WAN 通道都是啟動器，這意味著通道將啟用 SD-WAN 路徑監控探查。
	> show counter global filter delta yes
	
	`flow_sdwan_prob_req_tx`
	
	`flow_sdwan_prob_reply_rx`

• 在中樞上，驗證接收的 SD-WAN 探查要求封包的數量等於傳送的探查回覆封包的數量。
 	
在中樞防火牆上，大多數 SD-WAN 通道都是回應程式，這意味著通道將停用 SD-WAN 路徑監控探查。
	> show counter global filter delta yes
	
	`flow_sdwan_prob_req_rx`
	
	`flow_sdwan_prob_reply_tx`

檢視 **VPN** 通道資訊	
• 檢視防火牆上建立的所有通道。	**> show vpn flow**

如果您想要 ...	使用 ...
• 檢視按名稱標識的單個通道的詳細資料。	`> show vpn flow name <name>`
• 檢視按 ID 標識的單個通道的詳細資料。	`> show vpn flow tunnel-id <tunnel-id>`
• 檢視所有通道的 Internet Key Exchange (網際網路金鑰交換 - IKE) 階段 1 和階段 2 詳細資料。	`> show vpn ike-sa`
• 檢視特定閘道的 IKEv2 安全性關聯 (SA) 和 IKEv2 IPSec 子 SA。	`> show vpn ike-sa gateway <gateway>`
• 檢視通道詳細資料。	`> show vpn tunnel`
檢視 **BFD** 資訊	
• 檢視虛擬路由器的 BGP 摘要。	`> show routing protocol bgp summary virtual-router <virtual-router>`
• 檢視 BGP 對等摘要。	`> show routing protocol bgp peer peer-name <peer-name> virtual-router <virtual-router>`
• 檢視本機路由資訊庫 (RIB) 的摘要。	`> show routing protocol bgp loc-rib`
檢視 **RIB** 和 **FIB** 中的 **SD-WAN** 介面資訊	
• 檢視新 SD-WAN 輸出介面。	`> show routing route`
• 檢視轉送資訊庫 (FIB) 中的 SD-WAN 介面。	`> show routing fib`

更換 SD-WAN 裝置

退貨商品驗證 (RMA) 程序可讓您將故障或機能失常的 SD-WAN 裝置更換為分公司或資料中心網站的全新或重複使用的功能良好 SD-WAN 裝置。SD-WAN 裝置可能會因多種原因而故障或機能失常，例如裝置晶片故障、裝置設定錯誤或日常磨損。如果 SD-WAN 裝置因機能失常或整體故障而無法使用，則請使用 RMA 程序來更換故障或機能失常的裝置。

如果您嘗試更換現有部署中的 SD-WAN 防火牆，但未遵循正確的 RMA 程序，則 Panorama™ 和受管理的裝置上會發生提交失敗。

開始 RMA 程序之前：

- 檢閱開始 RMA 防火牆更換前。
- SD-WAN 會根據裝置序號來產生 IPSec 閘道和 keyID 這類設定。因此，您必須更新 SD-WAN 的更換防火牆序號，以辨識新的防火牆並避免提交失敗。尋找您的 SD-WAN 設定是否具有舊防火牆的 IPSec 或 VPN 物件參考：
  - 若要更換高可用性 (HA) 部署中的分支防火牆，請登入中樞防火牆，然後選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）。搜尋舊防火牆的序號（不含空格）。如果您取得一或多個搜尋結果，則指出 SD-WAN 在閘道設定中參考舊的防火牆序號。在這種情況下，建議您中斷舊分支防火牆與 Panorama 和 HA 部署的連線。
  - 若要更換沒有中樞的完整網狀部署中的防火牆，請在任何分支防火牆上搜尋舊的防火牆序號。如果您取得一或多個搜尋結果，則指出 SD-WAN 在閘道設定中參考舊的防火牆序號。在這種情況下，建議您中斷舊分支防火牆與 Panorama 和網狀部署的連線。
  - 若要更換獨立防火牆，則不需要搜尋序號。

存在 RMA 時，請使用下列工作流程來還原受管理防火牆上的設定。

STEP 1 | 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集），然後刪除舊防火牆。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後刪除舊防火牆。

STEP 3 | 將變更提交至 Panorama。

STEP 4 | （僅限 HA 部署）將變更推送到所有中樞和其他 HA 對等（需要更換的舊防火牆除外）。繼續之前，請確保中樞和獨立防火牆上的提交都成功。如果搜尋舊防火牆序號未傳回任何閘道設定，則您可以跳過此步驟。

STEP 5 | 設定 RMA 更換防火牆。

STEP 6 | （僅限 HA 部署）在更換防火牆與獨立防火牆之間建立 HA 連線。數值較小的防火牆就等於有較高的優先順序，表示將其指定為主動防火牆。若要避免更換防火牆成為主動 HA 對等，請確定其未獲指派較高的裝置優先順序。

STEP 7 | 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後新增新的分支防火牆。

STEP 8 | 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集），然後新增新的分支防火牆。

STEP 9 | 將變更提交至 Panorama。

STEP 10 | 選取 **Commit**（提交） > **Push to Devices**（推送至裝置），然後將整個 Panorama 受管理設定推送至中樞以及分支的兩個 HA 對等。

當您 ***Push to Devices***（推送至裝置）時，*Panorama* 會嘗試將變更推送至叢集中的所有裝置，以實現 *HA* 以及中樞和支點部署。若要避免將變更推送至所有裝置，請在 *[Push Scope*（推送範圍）*]* 中選取 ***Edit Selections***（編輯選取），然後停用 ***Device Groups***（裝置群組）裝置和 ***Templates***（範本）中的所有其他裝置。

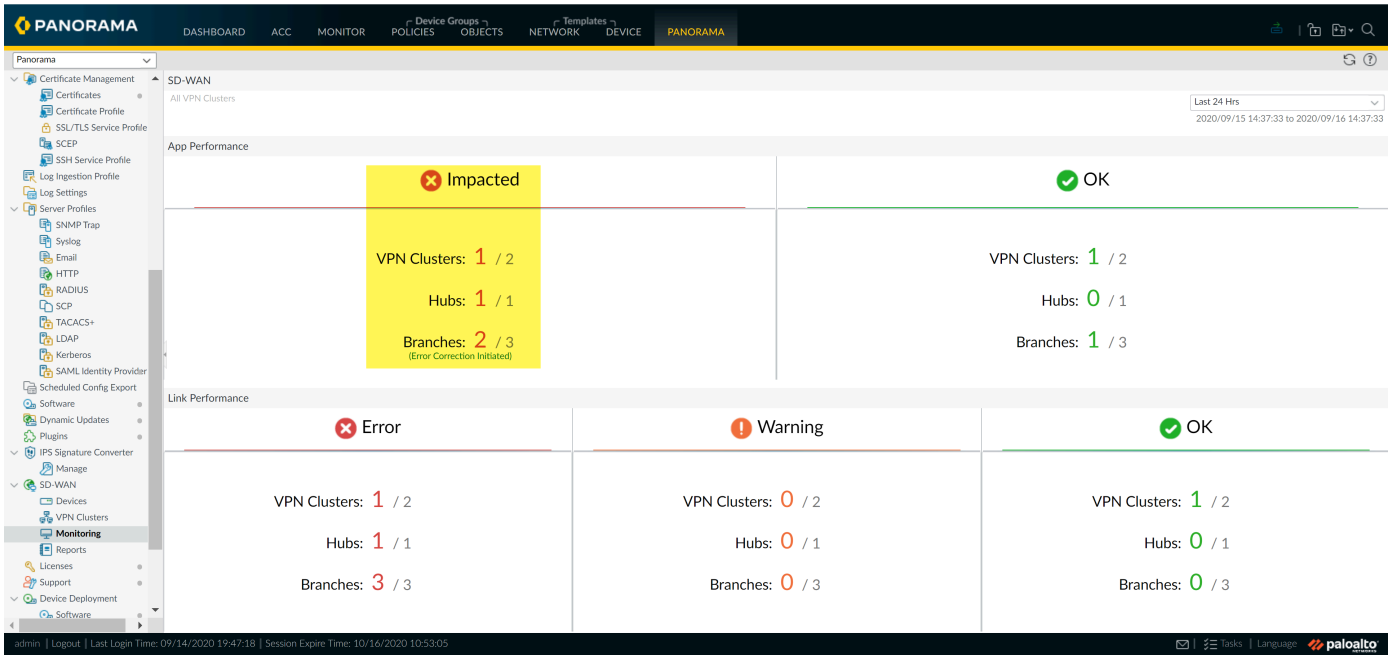
- 在中樞和支點部署中，選取中樞防火牆以及要將設定推送至其中的分支系統的 *HA* 範本堆疊。因此，未選取的網站可能會不同步。
- 在完整網狀部署中，必須將變更推送至叢集中的所有裝置。

對應用程式效能進行疑難排解

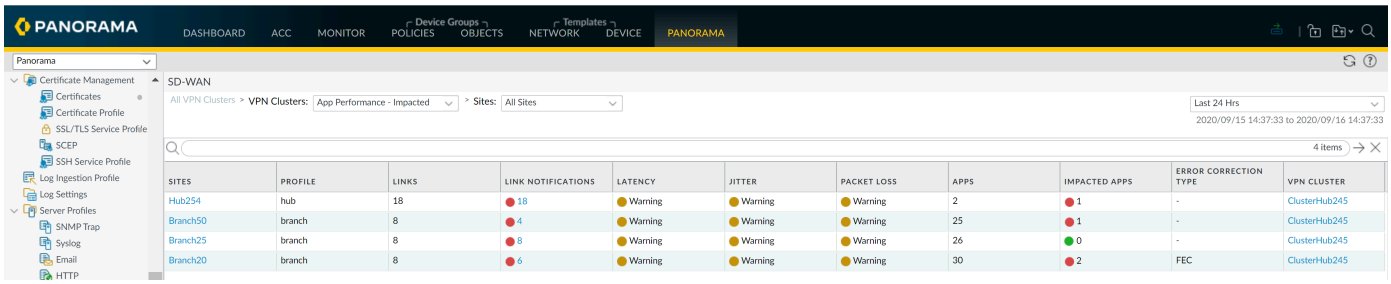
要確保使用者體驗不受影響，務必要瞭解導致應用程式和服務效能下降的原因。瞭解 VPN 叢集為什麼受到影響以及應用程式流量容錯移轉到其他連結有助於調整您的 SD-WAN 組態。

STEP 1 | 登入 Panorama 網頁介面。

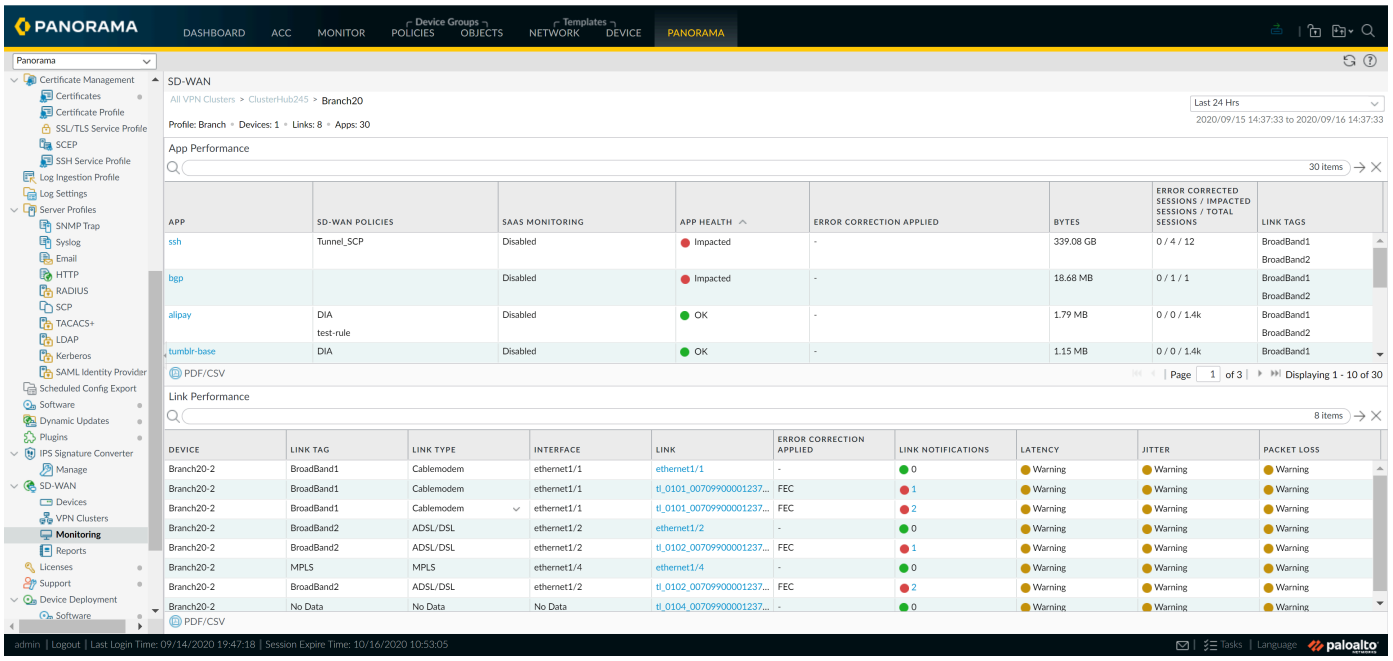
STEP 2 | 選取 **Panorama** > **SD-WAN** > **Monitoring**（監控）並檢視 **Impacted**（受影響）的 VPN 叢集。



STEP 3 | 基於 **Site**（網站）下拉式清單中的偏好指標篩選 VPN 叢集，並選取時間範圍。在此範例中，我們檢視過去 12 小時內包含受影響 VPN 叢集的 **All Sites**（所有網站）。

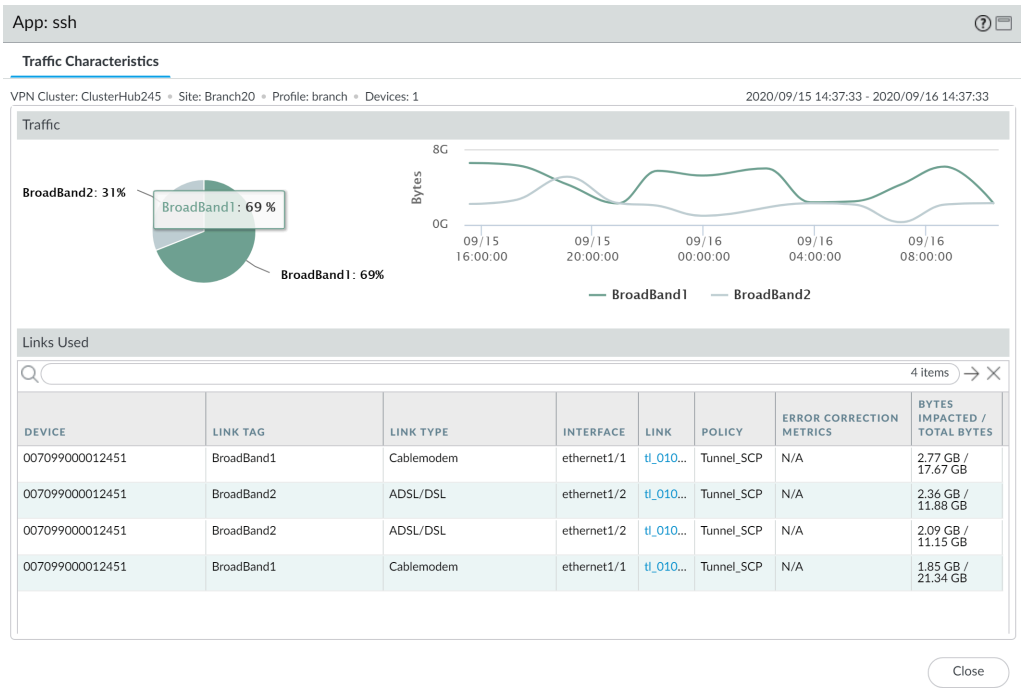


STEP 4 | 在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。



STEP 5 | 在「應用程式效能」部分中，按一下應用程式以檢視有關應用程式流量的詳細流量特性資訊，如網際網路服務和使用的連結：

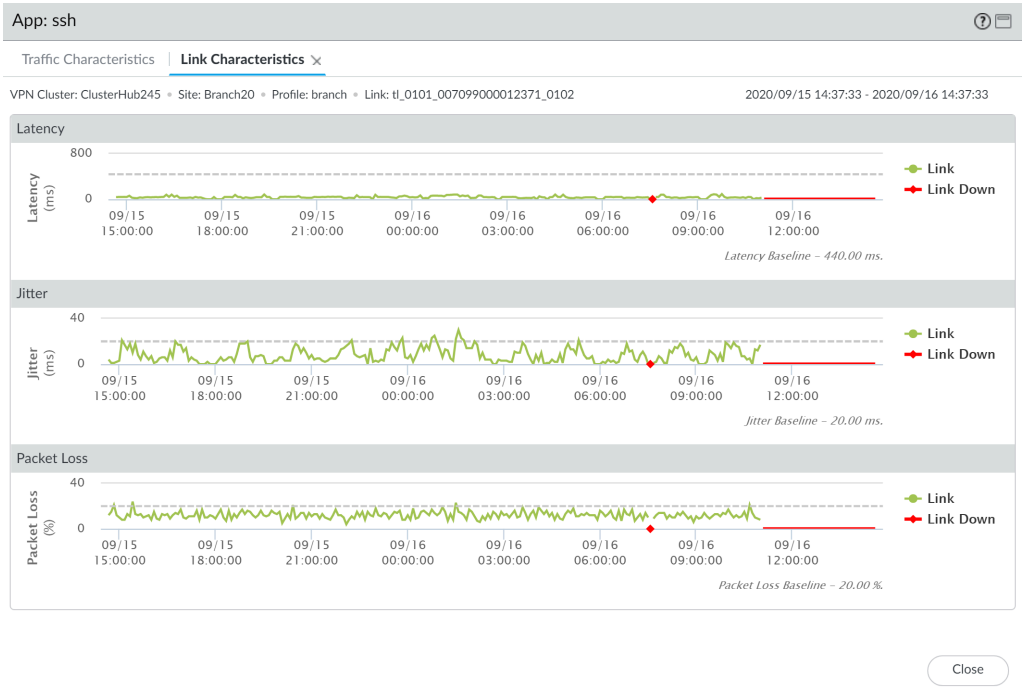
- 檢閱圓形圖以瞭解整個網際網路服務中應用程式流量的詳細資訊。
- 檢閱線條圖以瞭解每個網際網路服務在一段時間內傳輸了多少位元組的資料。
- 檢閱「使用的連結」部分以瞭解應用程式流量使用了哪些連結，以及瞭解在所選時間範圍內的總位元組中有多少位元組受到影響。



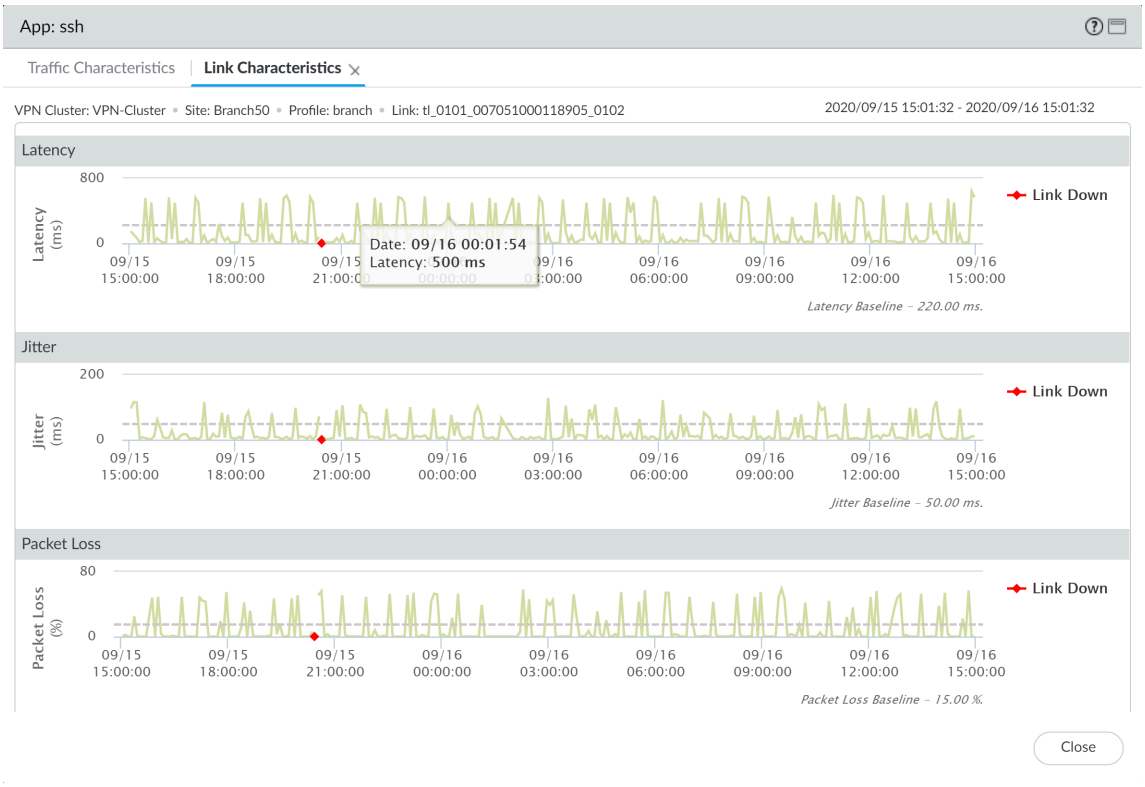
STEP 6 | 調查哪個健康情況指標導致應用程式交換連結。

帶點的線條表示健康情況指標的七日平均值。

1. 在「流量特性」標籤的「使用的連結」部分中，按一下乙太網路連結以檢視在第 2 步中指定的時間範圍內的詳細連結特性（延遲、抖動和封包遺失），以調查哪個健康情況指標導致應用程式交換連結。



2. 在 **Traffic Characteristics**（流量特性）頁籤中，選取另一個連結以檢視次要應用程式連結的連結特性，以更好地瞭解是什麼導致 VPN 叢集受到影響。



STEP 7 | 在找出應用程式流量受影響的原因後，考慮以下方案來解決問題：

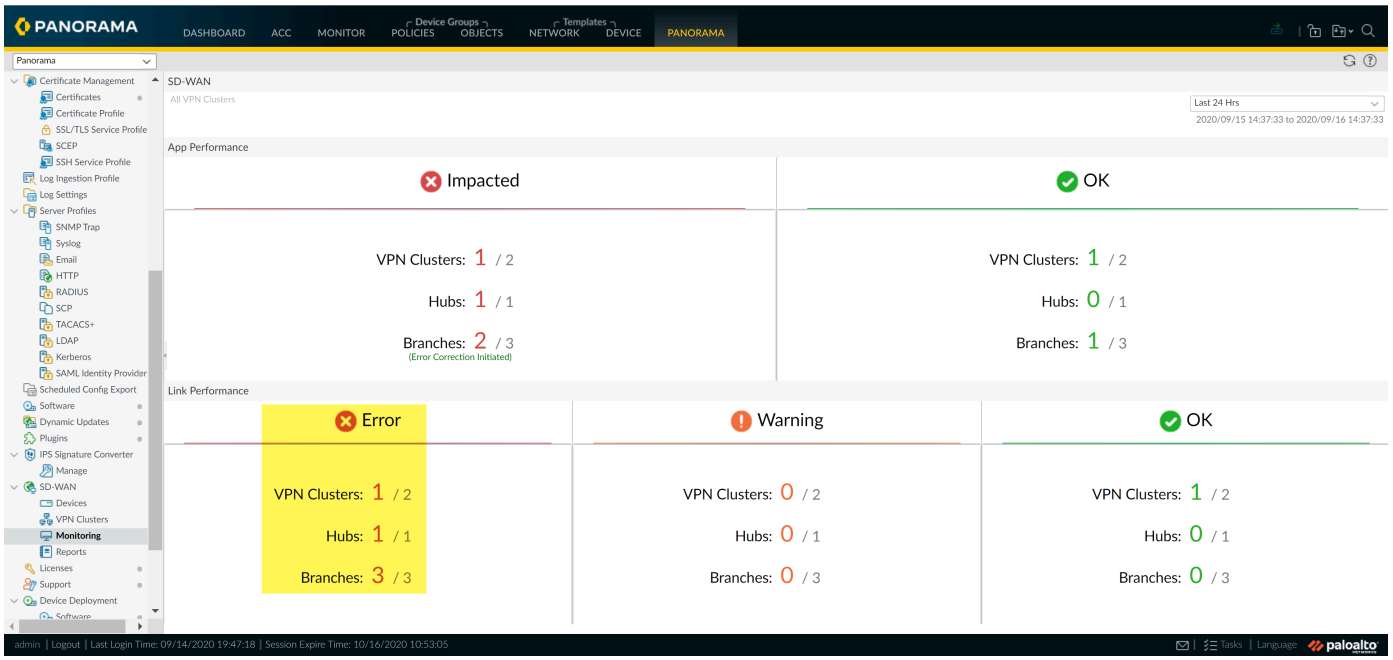
- 考慮新增額外連結到 Traffic Distribution Profile（流量散佈設定檔）。為應用程式流量新增可進行容錯移轉的額外連結，確保應用程式流量和使用者體驗不會受到健康情況下降的連結的影響。
- 在您的 Path Quality Profile（路徑品質設定檔）中重新設定健康情況閾值。可能是健康情況閾值過於嚴格，導致不必要的連結容錯移轉。例如，某個應用程式的封包遺失率在達到 18% 時使用者體驗才會受到影響，但是封包遺失閾值設定為 10%，這會導致在完全沒有必要的情況下應用程式容錯移轉到另一個連結。
- 咨詢您的網際網路服務提供商 (ISP) 以確定是否存在您無法控制但他們可以解決的網路影響。

對連結效能進行疑難排解

要確保使用者使用應用程式和服務的體驗不受影響，務必要瞭解導致應用程式和服務效能下降的原因。瞭解您的 VPN 叢集為什麼具有受影響的連結有助於調整您的 SD-WAN 組態，以確保使用應用程式和服務的使用者體驗不會受到健康情況下降的連結的影響。

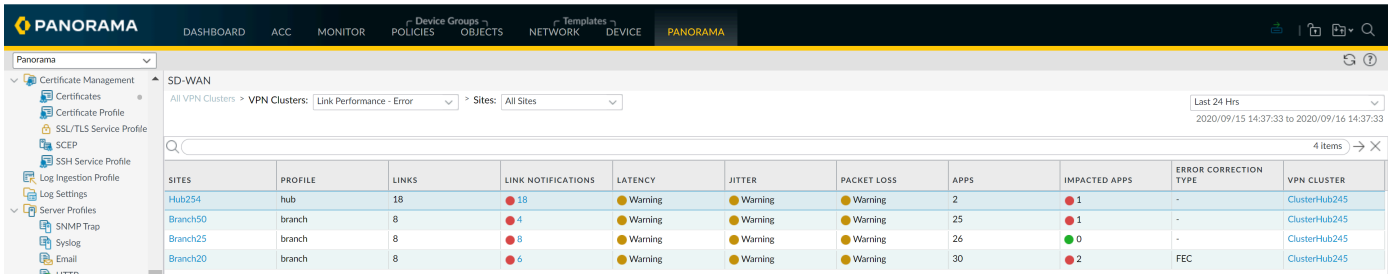
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama > SD-WAN > Monitoring**（監控）並檢視 **Impacted**（受影響）的 VPN 叢集。

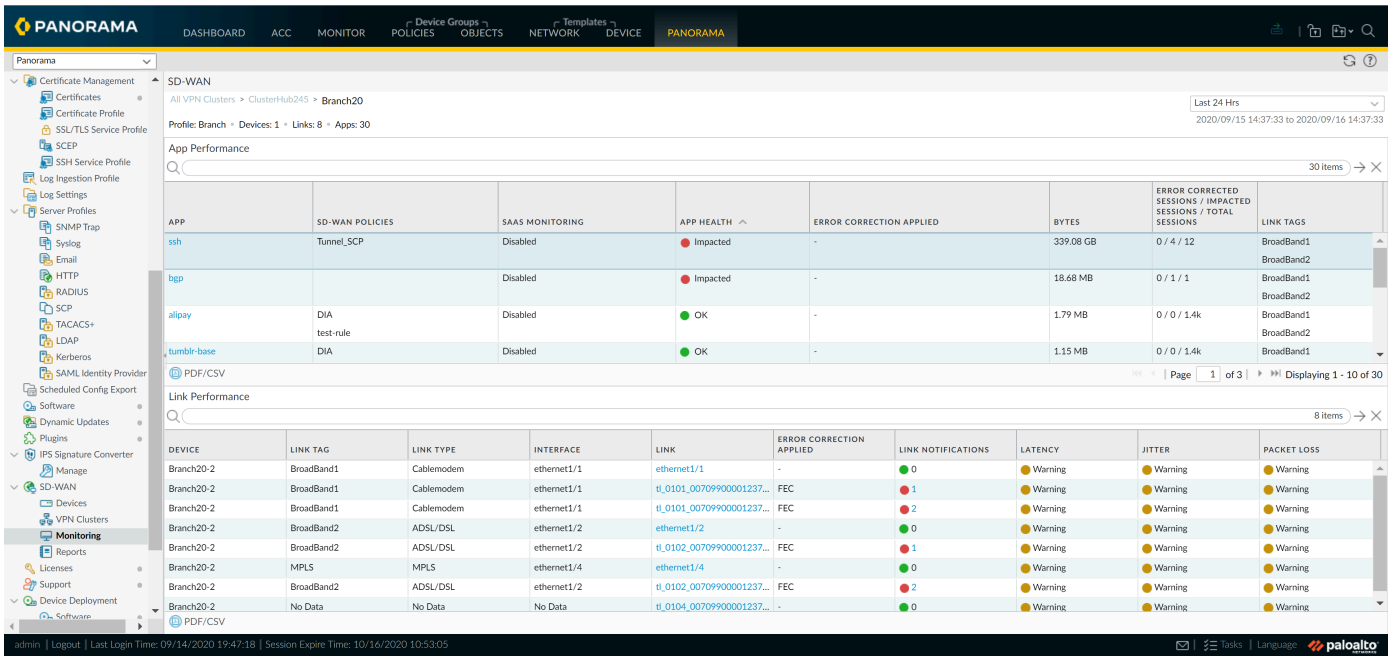


STEP 3 | 基於 **Site**（網站）下拉式清單中的偏好指標篩選 VPN 叢集，並選取時間範圍。在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。

在此範例中，我們檢視過去 24 小時內包含受影響 VPN 叢集的 **All Sites**（所有網站）。

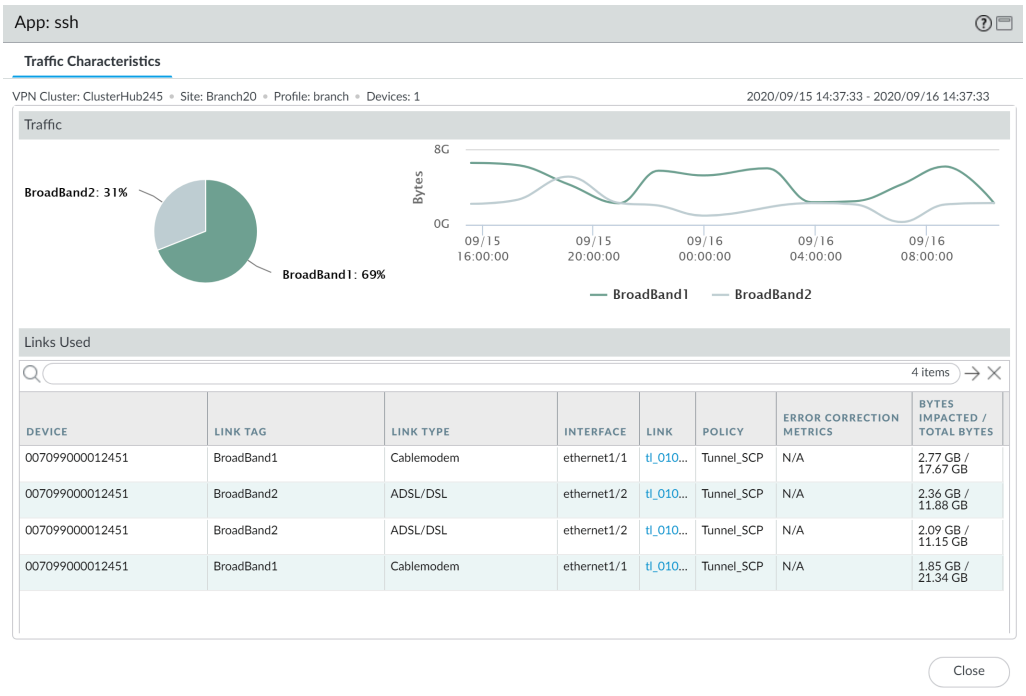


STEP 4 | 在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。



STEP 5 | 在「應用程式效能」部分中，按一下應用程式以檢視有關應用程式流量的詳細流量特性資訊，如網際網路服務和使用的連結：

- 檢閱圓形圖以瞭解整個網際網路服務中應用程式流量的詳細資訊。
- 檢閱線條圖以瞭解每個網際網路服務在一段時間內傳輸了多少位元組的資料。
- 檢閱「使用的連結」部分以瞭解應用程式流量使用了哪些連結，以及瞭解在所選時間範圍內的總位元組中有多少位元組受到影響。

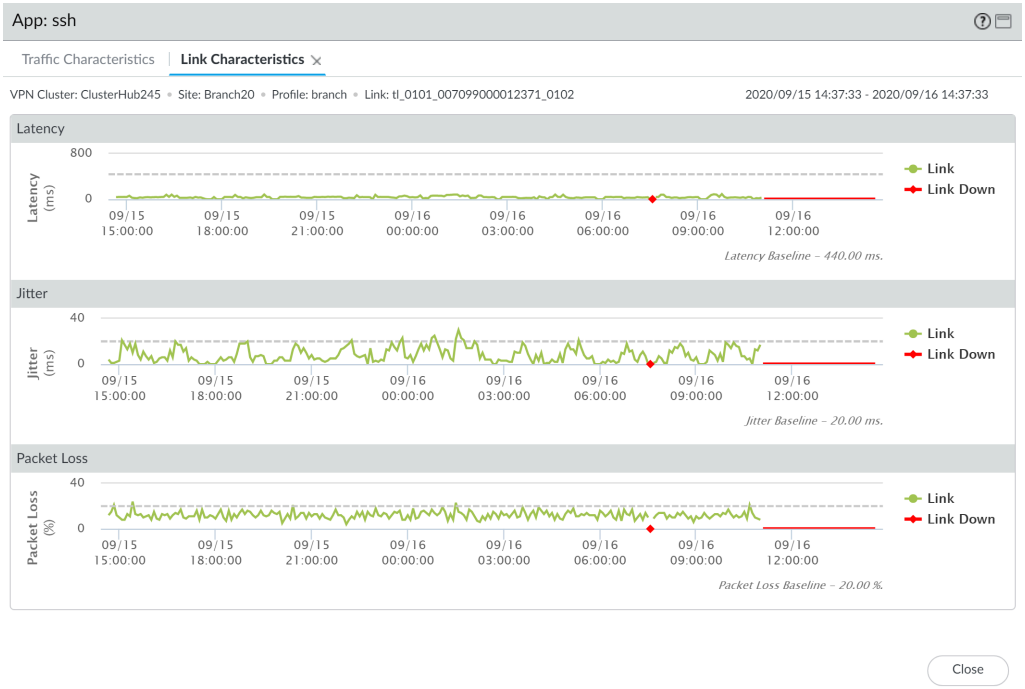


STEP 6 | 調查哪個健康情況指標導致應用程式交換連結。

帶點的線條表示當您 建立路徑品質設定檔 時設定的閾值。

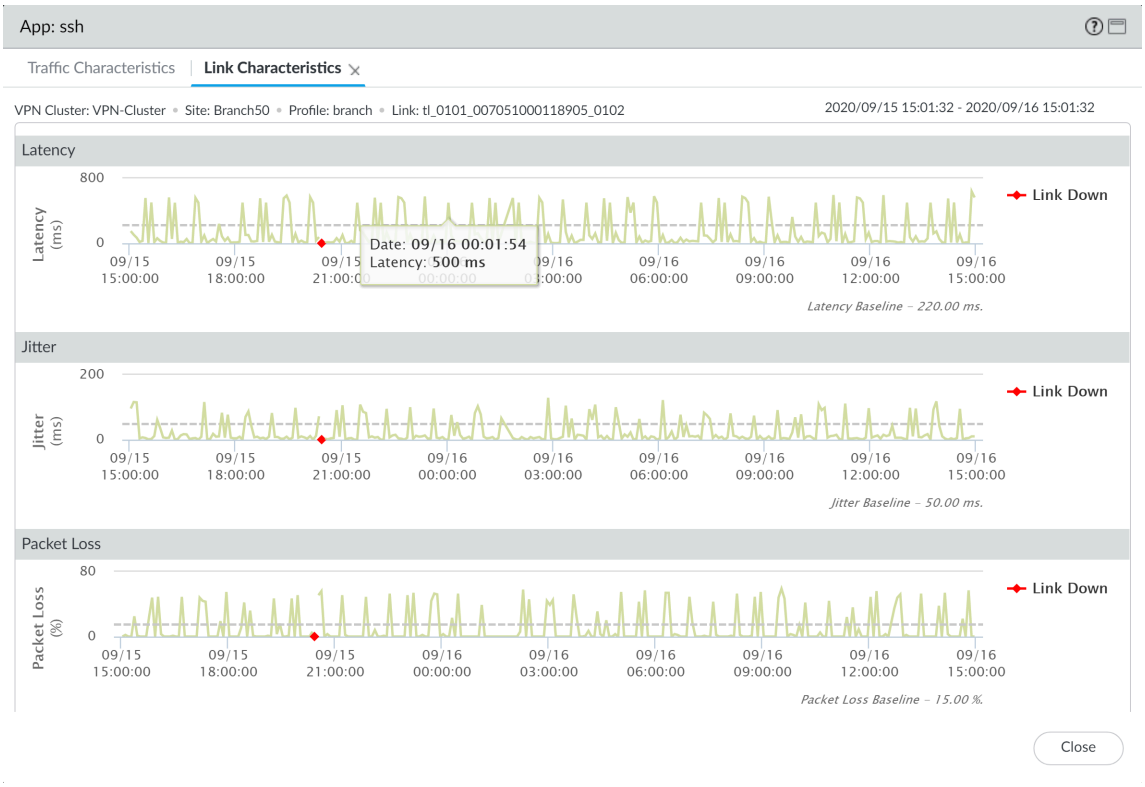
1. 在「流量特性」標籤的「使用的連結」部分中，按一下乙太網路連結以檢視在第 2 步中指定的時間範圍內的詳細連結特性（延遲、抖動和封包遺失），以調查哪個健康情況指標導致應用程式交換連結。在此範例中，我們檢視乙太網路 1/1，可以看到，封包遺失百分

比經常超出應用程式的路徑品質設定檔中設定的閾值，可以得出結論，這就是應用程式流量容錯移轉到下一個最佳連結的原因。



2. 在 **Traffic Characteristics**（流量特性）標籤中，選取另一個連結以檢視連結特性。在此範例中，我們檢視乙太網路 1/4，可以看到，在應用程式容錯移轉後，該應用程式的乙太網路 1/4 的抖動超出設定的閾值。這會強制應用程式容錯移轉回到乙太網路 1/1。

   由於兩個連結的健康情況指標均已超出，應用程式流量沒有可容錯移轉的健康連結，導致 VPN 叢集變得受影響。



STEP 7 | 在找出應用程式流量受影響的原因後，考慮以下方案來解決問題：

- 考慮新增額外連結到 Traffic Distribution Profile（流量散佈設定檔）。為應用程式流量新增可進行容錯移轉的額外連結，確保應用程式流量和使用者體驗不會受到健康情況下降的連結的影響。
- 在您的 Path Quality Profile（路徑品質設定檔）中重新設定健康情況閾值。可能是健康情況閾值過於嚴格，導致不必要的連結容錯移轉。例如，某個應用程式的封包遺失率在達到 18% 時使用者體驗才會受到影響，但是封包遺失閾值設定為 10%，這會導致在完全沒有必要的情況下應用程式容錯移轉到另一個連結。
- 咨詢您的網際網路服務提供商 (ISP) 以確定是否存在您無法控制但他們可以解決的網路影響。

升級您的 SD-WAN 防火牆

檢閱 Panorama 外掛程式 SD-WAN 2.1 版本資訊，然後使用以下程序升級 Panorama 和受管理的 SD-WAN 防火牆。

STEP 1 | 安裝 Panorama 的內容與軟體更新。

STEP 2 | 升級受管理的日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器。
- 當 Panorama 未連線至網際網路時升級日誌收集器。

STEP 3 | 升級您的 SD-WAN 中樞防火牆。

在升級分支防火牆之前，您必須將中樞防火牆從 *PAN-OS 10.0.0* 升級到 *PAN-OS 10.0.1* 或更新版本。在中樞防火牆之前升級分支防火牆可能會產生錯誤的監控資料（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控）），且 *SD -WAN* 連結會錯誤地顯示為 *down*（關閉）。

- 當 Panorama 連線至網際網路時升級防火牆。
- 當 Panorama 未連線至網際網路時升級防火牆。

STEP 4 | 升級您的 SD-WAN 分支防火牆。

- 當 Panorama 連線至網際網路時升級防火牆。
- 當 Panorama 未連線至網際網路時升級防火牆。

安裝 SD-WAN 外掛程式

在利用 SD-WAN 的 Panorama™ 管理伺服器和防火牆上，安裝 SD-WAN 外掛程式版本。

請參閱 Palo Alto Networks Panorama 外掛程式相容性矩陣並檢閱目標 SD-WAN 外掛程式版本所需的最低 PAN-OS 版本。請參閱升級 SD-WAN 外掛程式與相容的 PAN-OS 版本，以升級與 SD-WAN 外掛程式版本相容的 Panorama 管理伺服器和 Palo Alto Networks 防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上，安裝 SD-WAN 外掛程式版本。

對於採用高可用性 (HA) 設定的 Panorama，在 Panorama HA 對等上重複此步驟。

1. 選取 **Panorama** > **Plugins**（外掛程式）和 **Check Now**（立即檢查），瞭解最新的 **sd_wan** 外掛程式版本。
2. **Download**（下載）並 **Install**（安裝） SD-WAN 外掛程式的最新版本。
3. 成功安裝 SD-WAN 外掛程式後，選取 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**）。

   必須先執行此步驟才可將任何組態變更提交到 Panorama。

STEP 3 | 成功安裝新的外掛程式版本之後，請檢視 Panorama **Dashboard**（儀表板），並在「一般資訊」Widget 中確認 `SD-WAN plugin` 顯示您已安裝的 SD-WAN 外掛程式版本。

解除安裝 SD-WAN 外掛程式

要從 Panorama 管理伺服器解除安裝 SD-WAN 外掛程式，您必須先從 Panorama 移除 SD-WAN 外掛程式組態，然後才可成功解除安裝 SD-WAN 外掛程式。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 移除允許 BGP 在 SD-WAN 中樞和分支之間執行的任何安全性原則規則。

1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置） > **BGP Policy**（**BGP** 原則），然後 **Remove**（移除）安全性原則規則。
2. 按一下 **OK**（確定）儲存組態變更。

STEP 3 | 選取 **Panorama** > **Plugins**（外掛程式），然後針對 SD-WAN 外掛程式選取 **Remove Config**（移除設定）。

STEP 4 | 選取**Commit**（提交），然後 **Commit and Push**（提交並推送）組態變更到受管理的防火牆。

STEP 5 | **Uninstall**（解除安裝）SD-WAN 外掛程式。

在系統提示時按一下 **OK**（確定）以繼續解除安裝 SD-WAN 外掛程式。

