SD-WAN 管理員指南

1.0

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 2, 2020

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
> SD-WAN 組態元素
> 規劃您的 SD-WAN 組態

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。

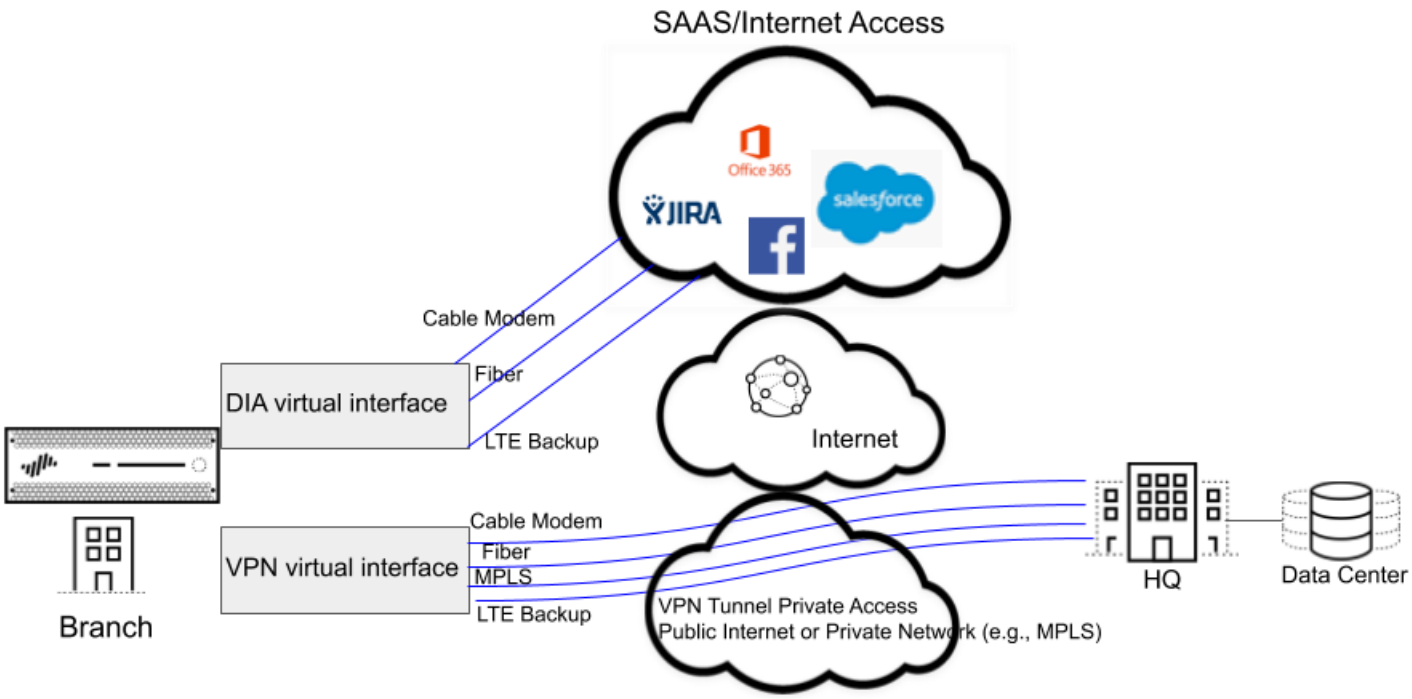
- 具有 SD-WAN 功能的 PAN-OS 安全性
- SD-WAN 連結和防火牆支援
- 集中管理

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。

以下防火牆型號支援 SD-WAN 軟體功能：

- PA-220
- PA-220R
- PA-820
- PA-850
- PA-3200 系列
- PA-5200 系列
- VM-300
- VM-500
- VM-700

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。

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。

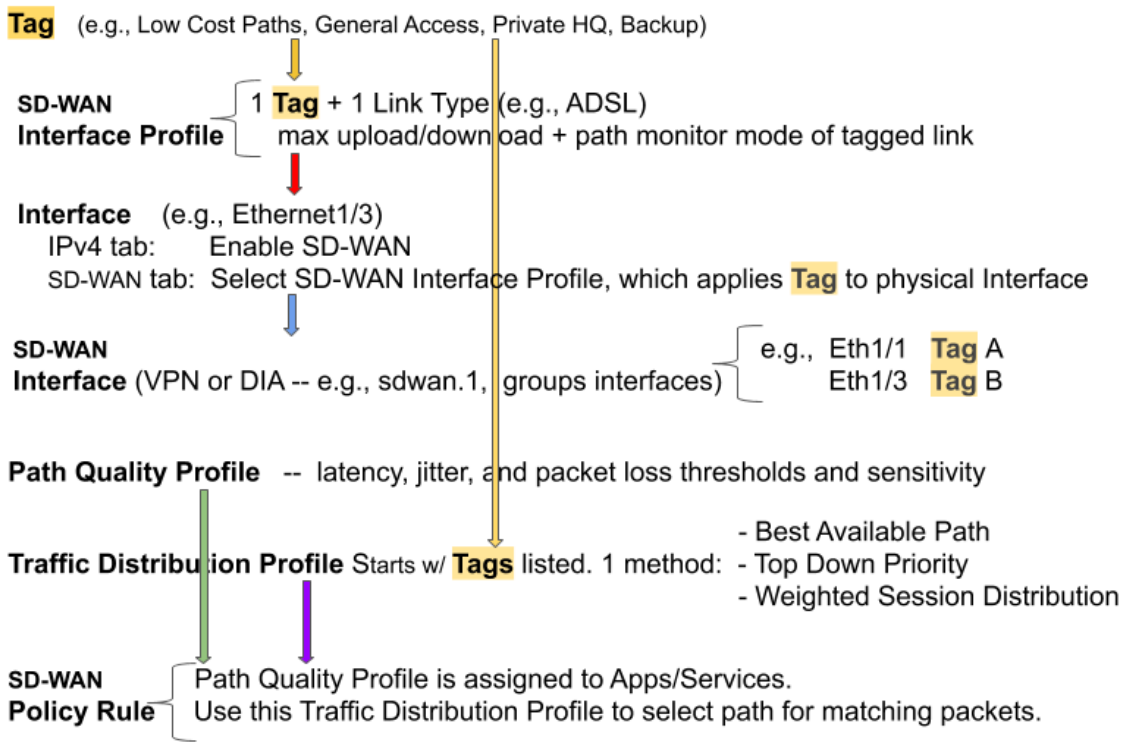
請先瞭解 SD-WAN 使用案例，然後檢閱 SD-WAN 組態元素、流量分配方式，並計劃您的 SD-WAN 組態。為大大加快組態設定速度，最佳做法是匯出一個空的 SD-WAN 裝置 CSV，並輸入分公司 IP 位址、要使用的虛擬路由器、防火牆站點名稱、防火牆所屬的區域以及 BGP 路由資訊等各類資訊。Panorama 使用 CSV 檔案來設定 SD-WAN 中樞和分支，以便在中樞和分支之間自動佈建 VPN 通道。SD-WAN 支援透過 eBGP 進行動態路由，並使用 Panorama 的 SD-WAN 外掛程式進行設定，允許所有分支僅與中樞進行通訊，或允許分支與中樞和其他分支進行通訊。

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 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。

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. 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。

> 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
> 設定虛擬 SD-WAN 介面
> 建立指向 SD-WAN 介面的預設路由
> 建立路徑品質設定檔
> SD-WAN 流量散佈設定檔
> 建立流量散佈設定檔
> #unique_16
> （PAN-OS 9.1.2 和更高的 9.1 版本）允許直接網際網路存取流量容錯移轉到 MPLS 連結
> 散佈不匹配的工作階段
> 新增 SD-WAN 裝置到 Panorama
> （選用）為 SD-WAN 設定 HA 裝置
> 建立 VPN 叢集
> （選用）為 SD-WAN 建立靜態路由

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 | 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 | 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。

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。

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）儲存您的組態變更。

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）儲存您的組態變更。

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）儲存您的組態變更。

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）儲存您的組態變更。

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。

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。

在開始設定 SD-WAN 部署前，對於兩種使用案例，您需要在 Panorama 中建立必需的預先定義區域，即 **`zone-internet`**、**`zone-internal`**、**`zone-to-hub`** 和 **`zone-to-branch`**。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。

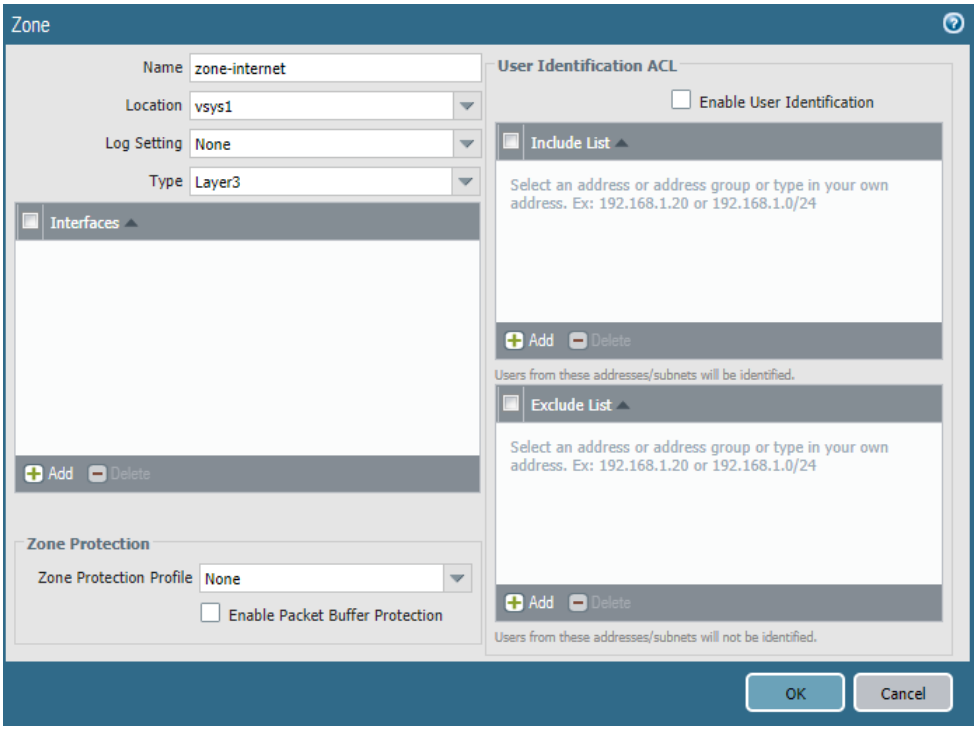
STEP 2 | 選取 **Network**（網路）> **Zones**（區域），然後在 **Template**（範本）內容下拉清單中，選取您之前建立的網路範本。

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**

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。

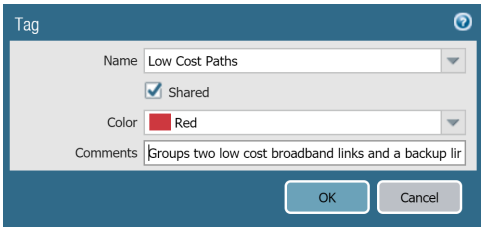
STEP 4 | 輸入標籤的描述性 **Name**（名稱）。例如，低成本路徑、昂貴路徑、一般存取、專用 HQ 或備份。

STEP 5 | 啟用（選中）**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您推送到的任何多重 vsys 中樞或分支上的每個虛擬系統 (vsys) 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）儲存您的組態變更。

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（**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** 或 **Other**（其他）中選取實體 **Link Type**（連結類型）。防火牆可以支援任何作為乙太網路連線終止和切換到防火牆的 CPE 裝置。例如，WiFi 存取點、LTE 數據機、雷射/微波 CPE，都可以透過乙太網路切換來終止。

點對點的專用連結類型（*MPLS*、衛星、微波和其他）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。

STEP 9 | （PAN-OS 9.1.2 和更高的 9.1 版本）**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、衛星或微波之類不具有網際網路中斷能力的專有連結類型停用 **VPN Data Tunnel Support**（**VPN** 資料通道支援）。但是，您必須先確保流量不會被攔截，因為流量將在 VPN 通道外進行傳送。
- 分支能具有 DIA 流量，即需要容錯移轉到連線至中樞的私人 MPLS 連結，並從中樞到達網際網路。**VPN Data Tunnel Support**（**VPN** 資料通道支援）設定確定私人資料通過 VPN 通道流動還是在通道外流動，以及容錯移轉的流量使用其他連線（私人資料流未使用的連線）。防火牆使用區域將 DIA 容錯移轉流量和私人 MPLS 流量分割開來。

STEP 10 | 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）。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 | 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）。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 12 | （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。

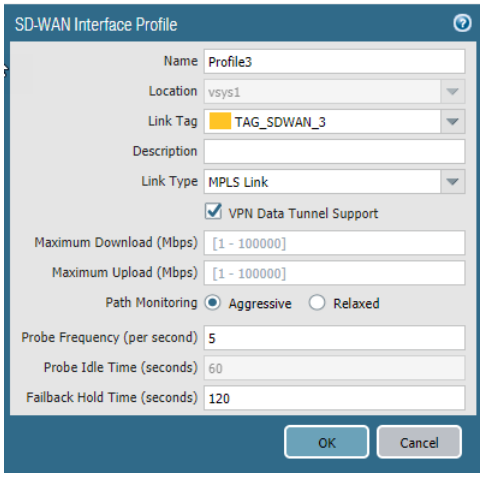
STEP 13 | 設定探查頻率（每秒），這是防火牆每秒鐘向 SD-WAN 連結的另一端傳送探查封包的次數（範圍為 1 到 5；預設值為 5）。預設設定可對暫時低壓和斷電情況提供亞秒級的偵測。

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 14 | 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 15 | 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 16 | 按一下 **OK**（確定）來儲存設定檔。



STEP 17 | **Commit（認可），Commit and Push（認可並推送）組態變更。**

STEP 18 | **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，設定一個實體的第三層乙太網路介面並啟用 SD-WAN 功能。要設定實體介面，您必須為其指派一個 IPv4 位址和下一個躍點閘道，並指派一個 SD-WAN 介面設定檔到該介面。

在您使用 Panorama 建立 VPN 叢集並在 CSV 中匯出中樞和分支資訊後，SD-WAN 外掛程式中的Auto VPN 組態會使用此資訊為關聯的分支和中樞產生一個組態，其中包含預先定義的 SD-WAN 區域，且會在 SD-WAN 分支和中樞之間建立安全 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 組態還會產生 BGP 組態。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Network**（網路）> **Interfaces**（介面）> **Ethernet**（乙太網路），從 **Template**（範本）內容下拉清單中選取適當的範本，選取一個插槽編號，如 Slot1，然後選取一個介面（如 ethernet1/1）。

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

STEP 4 | 選取一個 **Virtual Router**（虛擬路由器）或建立一個新虛擬路由器。

STEP 5 | 為您正在設定的介面指派適當的安全性區域。

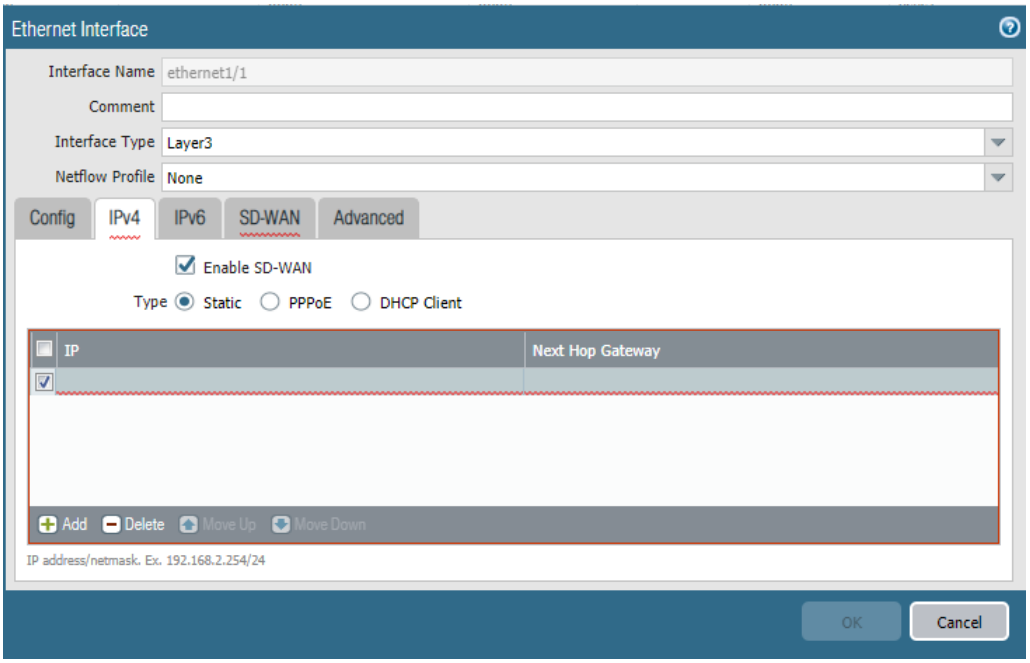
例如，如果您正在建立一個指向 ISP 的上行連結，您必須知道您選擇的乙太網路介面將前往不受信任的區域。

STEP 6 | 在 **IPv4** 索引標籤上，啟用 **SD-WAN**。

STEP 7 | 選取位址的類型：

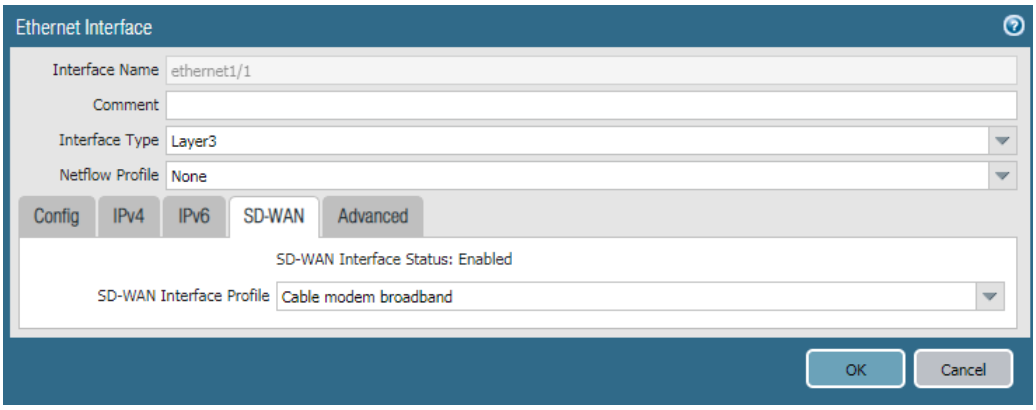
- 靜態—在 **IP** 欄位中，為介面新增一個 IPv4 位址和前置詞長度。您可以使用包含一個位址範圍的已定義變數，如 $uplink。輸入下一個躍點閘道（您剛剛輸入的 IPv4 位址的下一個躍點）的 IPv4 位址。下一個躍點閘道必須在與 IPv4 位址相同的子網路上。下一個躍點閘道是您在購買服務時 ISP 為您提供的 ISP 預設路由器的 IP 位址。這是防火牆向其發送流量以到達 ISP 的網路並最終到達網際網路和中樞的下一個躍點 IP 位址。
- （PAN-OS 9.1.2 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.2 和更高的 1.0 版本）**PPPoE**—為 DSL 連結啟用 PPPoE 驗證，輸入使用者名稱和密碼，以及確認密碼。
- **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。

如果您選取 *DHCP* 用戶端，請確保停用選項自動建立指向伺服器所提供之預設閘道的預設路由，該選項預設情況下為啟用。



STEP 8 | 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 9 | 按一下 **OK**（確定）以儲存乙太網路介面。



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

STEP 11 | （僅 SD-WAN 手動組態）設定虛擬 SD-WAN 介面。如果您使用 Auto VPN，則 Auto VPN 組態將執行此工作。

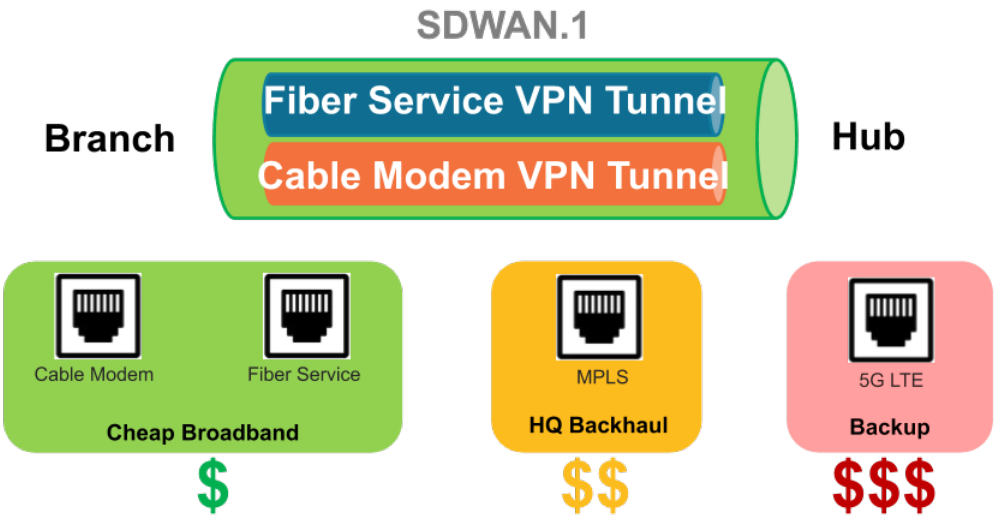
設定虛擬 SD-WAN 介面

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。

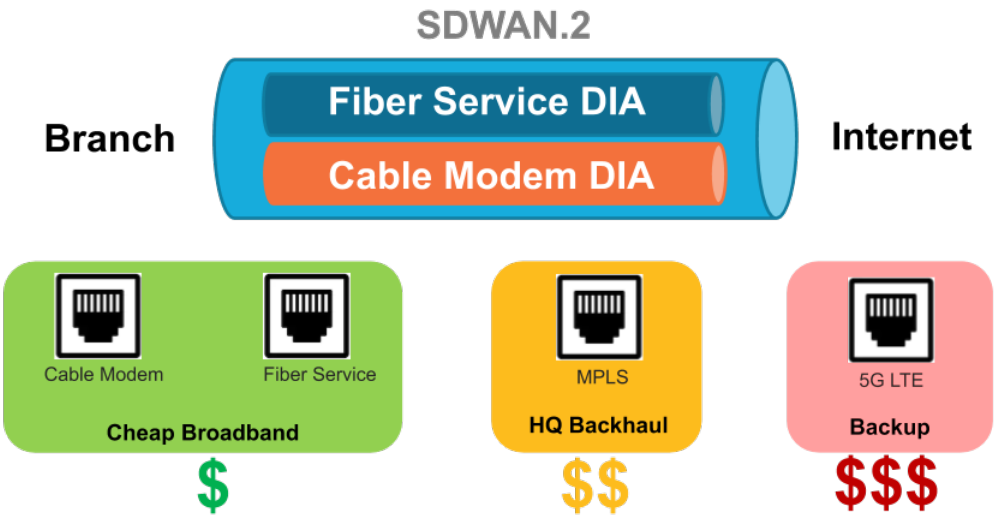
如果您沒有在 Panorama 中使用 Auto VPN 組態，請建立並設定一個虛擬 SD-WAN 介面以指定一個或多個具有 SD-WAN 功能的實體乙太網路介面，這些介面前往同一目的地，如一個特定的中樞或網際網路。事實上，一個虛擬 SD-WAN 介面中的所有連結都必須是相同類型的：全部都是 VPN 通道連結或全部都是直接網際網路存取 (DIA) 連結。

第一個圖說明了一個名為 SDWAN.1 的 SD-WAN 介面的範例，該介面組合了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.2 組合了 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。

Auto VPN 組態會建立編號為 *.901*、*.902* 等（以此類推）的 *SD-WAN* 介面，所以請不要使用這些編號。

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

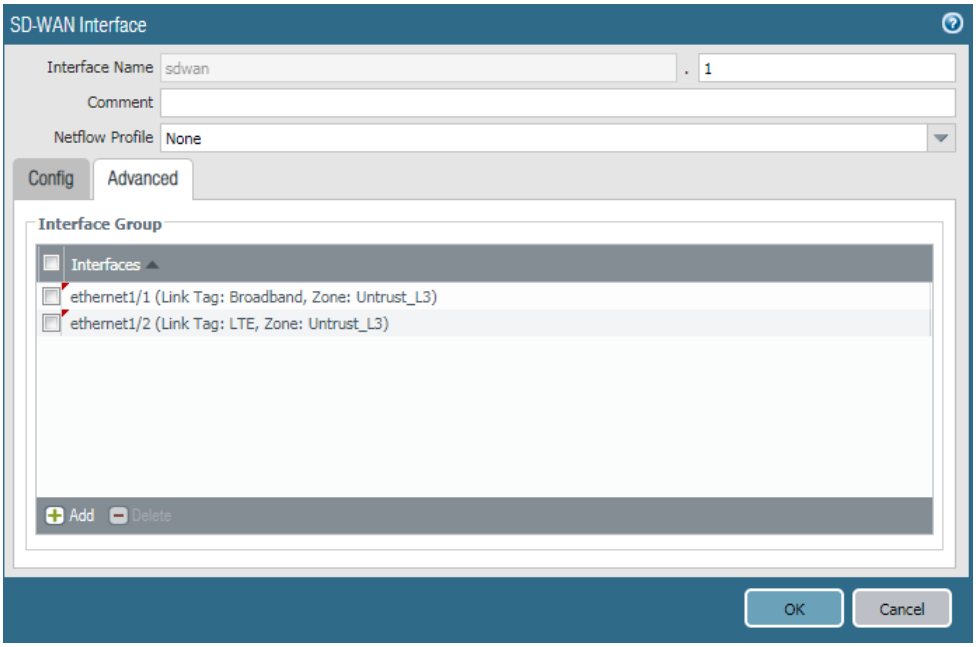
STEP 6 | 將 SD-WAN 介面指派給 **Security Zone**（安全性區域）。

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 7 | 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 8 | 按一下 **OK**（確定）儲存您的組態變更。



STEP 9 | **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。

Auto VPN 會為 DIA 建立一個名為 sdwan.901 的虛擬 SD-WAN 介面，並為 VPN 通道建立一個名為 sdwan.902 的虛擬 SD-WAN 介面。Auto VPN 還會建立其自己的預設路由，該路由使用 sdwan.901 介面作為其輸出介面且使用低指標，這樣，相比您建立的預設路由，sdwan.901 介面會成為偏好介面。

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 **sd-wan**。

STEP 4 | 選取 **Static Routes**（靜態路由）並根據 **Name**（名稱）**Add**（新增）一個靜態路由。

STEP 5 | 對於 **Destination**（目的地），輸入 0.0.0.0/0。

STEP 6 | 對於輸出 **Interface**（介面），選取一個您建立的邏輯 SD-WAN 介面（如 sdwan.1）以啟動防火牆。

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

STEP 7 | 對於 **Next Hop**（下一個躍點），選取 **None**（無）。

STEP 8 | 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 9 | 按一下 **OK**（確定）。

STEP 10 | 選取**Commit**（提交）並 **Commit and Push**（提交和推送）您的組態變更。

STEP 11 | **Commit**（提交）您的變更。

STEP 12 | 對防火牆上使用服務路由存取 Panorama™ 的其他範本重複此工作。

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。

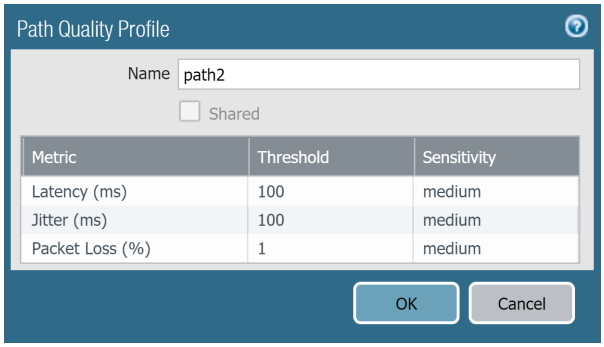
在 SD-WAN 原則規則中引用路徑品質設定檔，以控制防火牆在什麼時候使用新路徑為匹配的應用程式封包替換惡化的路徑。

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）。

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 | 對於 **Packet Loss**（封包遺失），請選取 **Sensitivity**（敏感度）（低、中等或高）。預設為 中等。

STEP 11 | 按一下 **OK**（確定）。

STEP 12 | **Commit**（認可），**Commit and Push**（認可並推送）組態變更。

STEP 13 | **Commit**（提交）您的變更。

STEP 14 | 為每一個裝置群組重複此工作。

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，防火牆不會將匹配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：

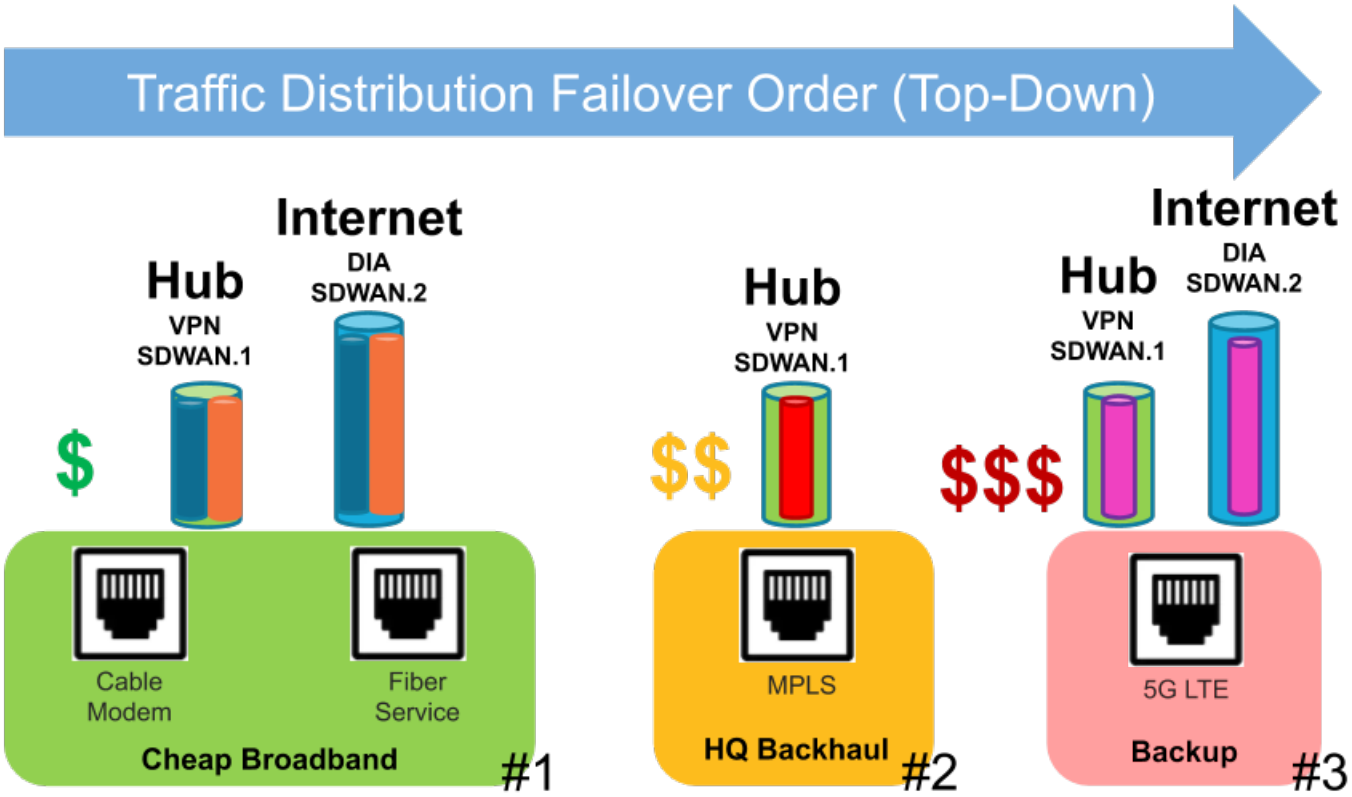
路徑情況	自上而下優先順序	最佳可用路徑	加權工作階段散佈
超出路徑健康情況閾值（暫時低壓）的現有路徑上的工作階段	受影響工作階段容錯移轉到更佳路徑（如果可用）	受影響工作階段容錯移轉到更佳路徑（如果可用）	受影響的工作階段不容錯移轉
自上而下或最佳可用路徑復原：現有路徑仍然合格（良好）	受影響的工作階段容錯回復到之前的路徑	受影響的工作階段停留在現有路徑上，不會容錯回復	受影響的工作階段不容錯移轉
自上而下或最佳可用路徑復原：現有路徑未能通過健康情況檢查	所有工作階段容錯回復到之前的路徑	選取的工作階段容錯回復到之前的路徑，直到受影響的現有路徑復原	受影響的工作階段不容錯移轉
現有路徑斷開（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

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
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）。

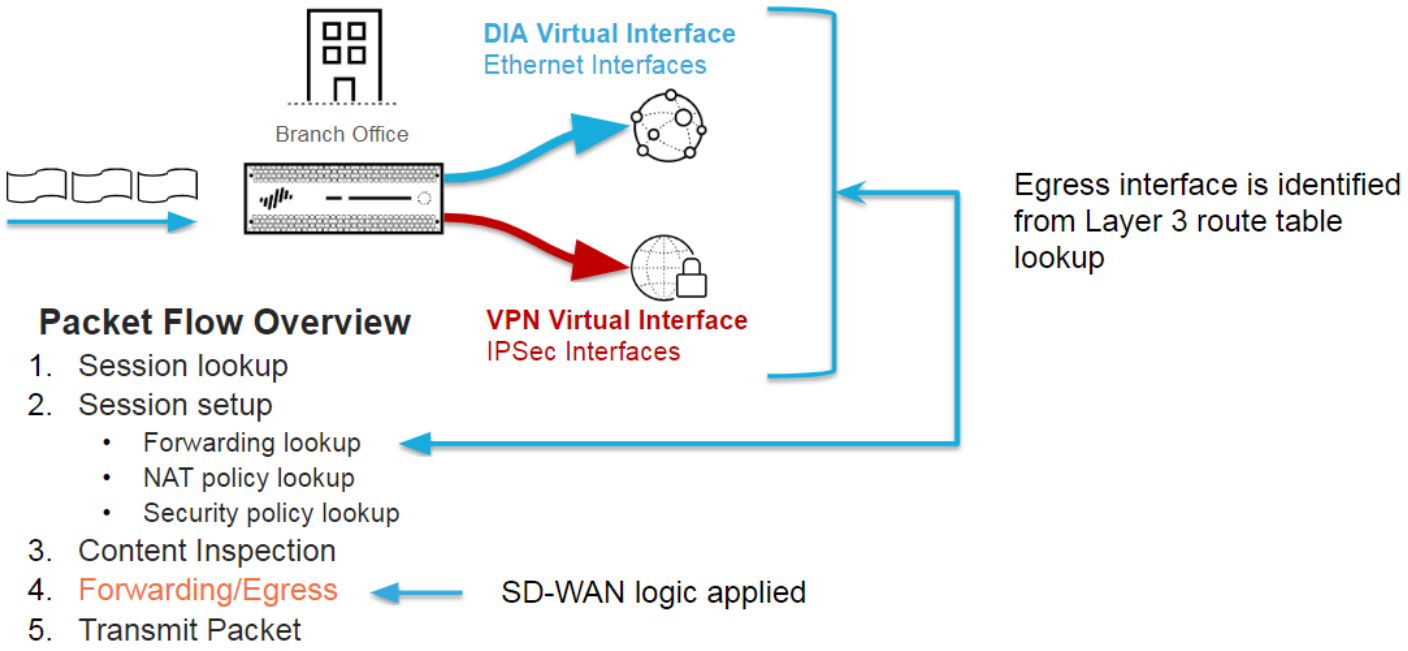
路徑情況	自上而下優先順序	最佳可用路徑	加權工作階段散佈
具有相同 SD-WAN 標籤的多個連結	在 SD-WAN 標籤內的所有連結上平均共用工作階段載入	基於 SD-WAN 標籤內的最佳路徑共用工作階段載入	基於指派到 SD-WAN 標籤的權重百分比共用工作階段載入
具有不同 SD-WAN 標籤的多個連結	基於清單優先順序共用工作階段載入，先載入第一個 SD-WAN 標籤中的連結。	基於所有 SD-WAN 標籤的最佳路徑共用工作階段載入	基於指派到 SD-WAN 標籤的權重百分比共用工作階段載入

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確定到目的地和傳出介面的下一個躍點，即名為 sdwan.1 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 原則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.1 的哪個介面成員（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.1 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。



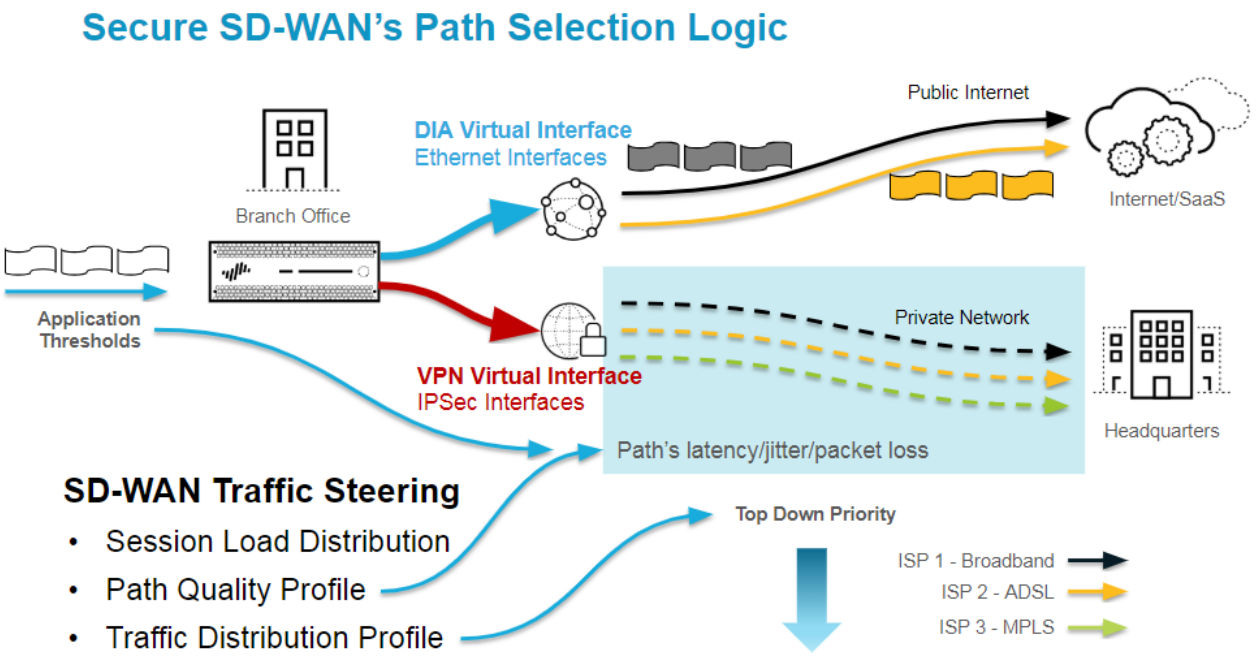
圖中的封包流動詳細資料如下所示：

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 組態計劃，根據您希望 SD-WAN 原則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。

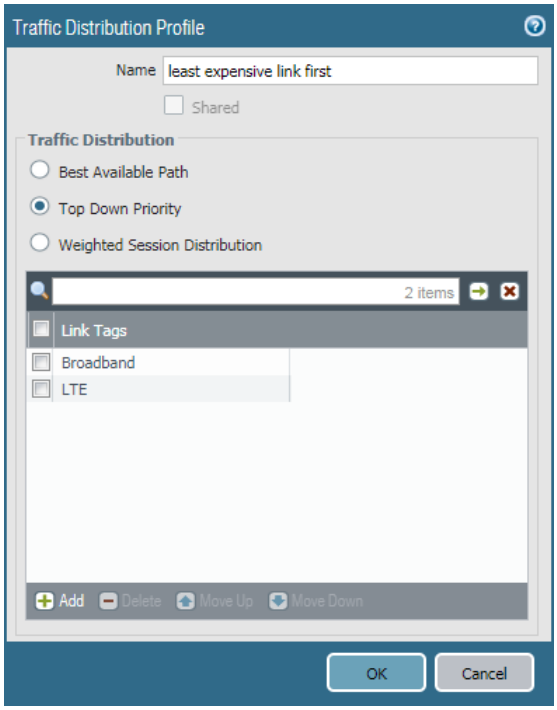
STEP 1 | 登入 Panorama 網頁介面。

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。
- **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。

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。從 PAN-OS 9.1.2 開始，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 | （PAN-OS 9.1.2 和更高的 9.1 版本）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 | #unique_16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。

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

新增單個 SD-WAN 中樞或分支防火牆，或使用 CSV 批量匯入多個 SD-WAN 中樞和分支防火牆。

- 新增一個 SD-WAN 裝置
- 批量匯入多台 SD-WAN 裝置

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。在新增裝置前，計劃您的 SD-WAN 組態以確保您擁有全部必需的 IP 位址，且 SD-WAN 拓撲能夠得到很好的理解。這可幫助減少組態錯誤。

如果您的 Palo Alto Networks® 防火牆有現有區域，您要將它們對應到 SD-WAN 中使用的預先定義區域。

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。

如果您使用 *BGP* 路由，您必須新增一個安全性原則規則，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*。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > 裝置 並**Add**（新增）一個新的 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，執行原則規則，並管理分支位置的連結交換。

STEP 5 | 選取用於在 SD-WAN 中樞和分支之間進行路由的虛擬路由器名稱。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。

STEP 6 | 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。網站名稱中不支援使用空格，如果使用，會導致該網站的監控（*Panorama* > *SD-WAN* > 監控）資料無法顯示。

STEP 7 | （PAN-OS 9.1.3 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.3 和更高的 1.0 版本）如果您要在為中樞執行 NAT 的裝置後面新增一個中樞，則必須指定該上游 NAT 執行裝置上對外介面的 IP 位址或 FQDN，以便 Auto VPN 組態可以將該位址用作中樞的通道端點的位址。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. 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）。

> 您還必須輸入帶一對一 *NAT* 原則的輸入目的地 *NAT*，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，您必須重新設定新 *IP* 位址，並將其推送到 *VPN* 叢集成員。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。

STEP 8 | （對於現有客戶為必需項）將您的現有區域對應到針對 SD-WAN 使用的預先定義區域。

> 當您將現有區域對應到 *SD-WAN* 區域時，您必須修改您的安全性原則規則，並將 *SD-WAN* 區域新增到正確的 *Source*（來源）和 *Destination*（目的地）區域。

1. 選取**Zone Internet**（區域網際網路），並**Add**（新增）將輸出 SD-WAN 流量到網際網路的現有區域。
2. 選取**Zone to Hub**（區域到中樞），並**Add**（新增）將輸出 SD-WAN 流量到中樞的現有區域。
3. 選取**Zone to Branch**（區域到分支），並**Add**（新增）將輸出 SD-WAN 流量到分支的現有區域。
4. 選取**Zone Internal**（區域內部），並**Add**（新增）將輸出 SD-WAN 流量到內部區域的現有區域。

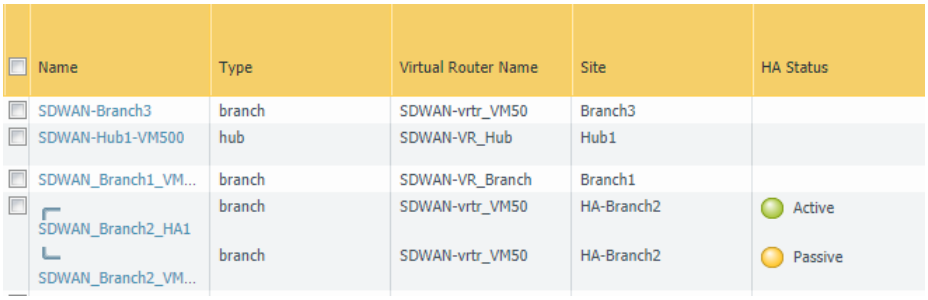
STEP 9 | （選用）設定邊界閘道通訊協定 (BGP) 路由。

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。

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. 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。
4. 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。
5. 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。分支裝置沒有此選項；預設情況下會重新散佈連線到分支位置的子網路。

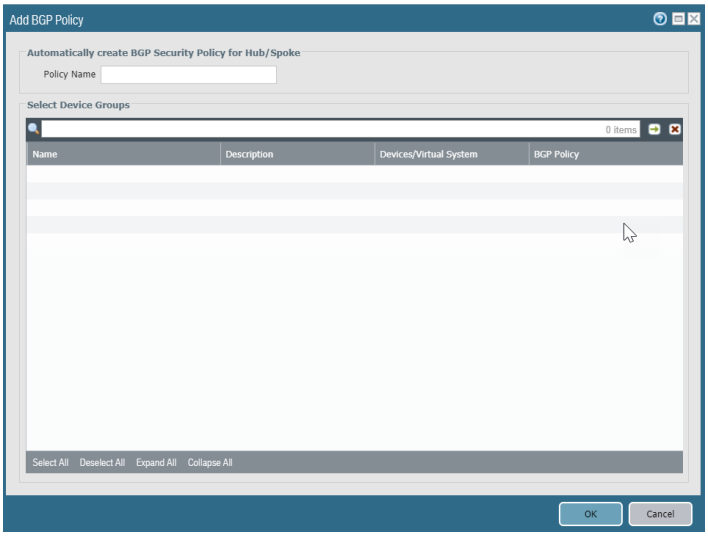
STEP 10 | 按一下 **OK**（確定）。

STEP 11 | （SD-WAN 外掛程式 1.0.1 和更高版本）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 12 | （PAN-OS 9.1.2 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.2 和更高的 1.0 版本）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. 選取螢幕底部的 **BGP Policy**（**BGP** 原則），然後選擇 **Add**（新增）。
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。
4. 按一下 **OK**（確定）。



STEP 13 | 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。在新增裝置前，計劃您的 SD-WAN 組態以確保您擁有全部必需的 IP 位址，且 SD-WAN 拓撲能夠得到很好的理解。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。

如果您使用 *BGP* 路由，您必須新增一個安全性原則規則，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 防火牆有現有區域，您要將它們對應到 SD-WAN 中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。您必須為每個中樞和分支輸入以下資訊：

- **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。網站名稱中不支援使用空格，如果使用，會導致該網站的監控（*Panorama* > *SD-WAN* > 監控）資料無法顯示。
- （對於現有客戶為必需項）將您的現有區域對應到針對 SD-WAN 使用的預先定義區域。

  當您將現有區域對應到 *SD-WAN* 區域時，您必須修改您的安全性原則規則，並將 *SD-WAN* 區域新增到正確的 *Source*（來源）和 *Destination*（目的地）區域。

  - **zone-internet**（區域-網際網路）—輸入 SD-WAN 流量將輸出到網際網路的現有區域的名稱。
  - **zone-to-branch**（區域到分支）—輸入 SD-WAN 流量將輸出到分支的現有區域的名稱。
  - **zone-to-hub**（區域到中樞）—輸入 SD-WAN 流量將輸出到中樞的現有區域的名稱。
  - **zone-internal**（區域-內部）—輸入 SD-WAN 流量將輸出到內部區域的現有區域的名稱。
- （選用）**loopback-address**（回送位址）—指定用於 Border Gateway Protocol（邊界閘道通訊協定 - BGP）對等的靜態回送 IPv4 位址。
- （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* 處獲取的分公司預設路由。
- （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*。
- （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中是唯一的。

  輸入回送位址作為路由器 *ID*。
- **vr-name**（虛擬路由器名稱）—輸入用於在 SD-WAN 中樞和分支之間進行路由的虛擬路由器的名稱。預設情況下，Panorama 會建立一個 `sdwan-default` 虛擬路由器，且能夠自動推送路由器組態。

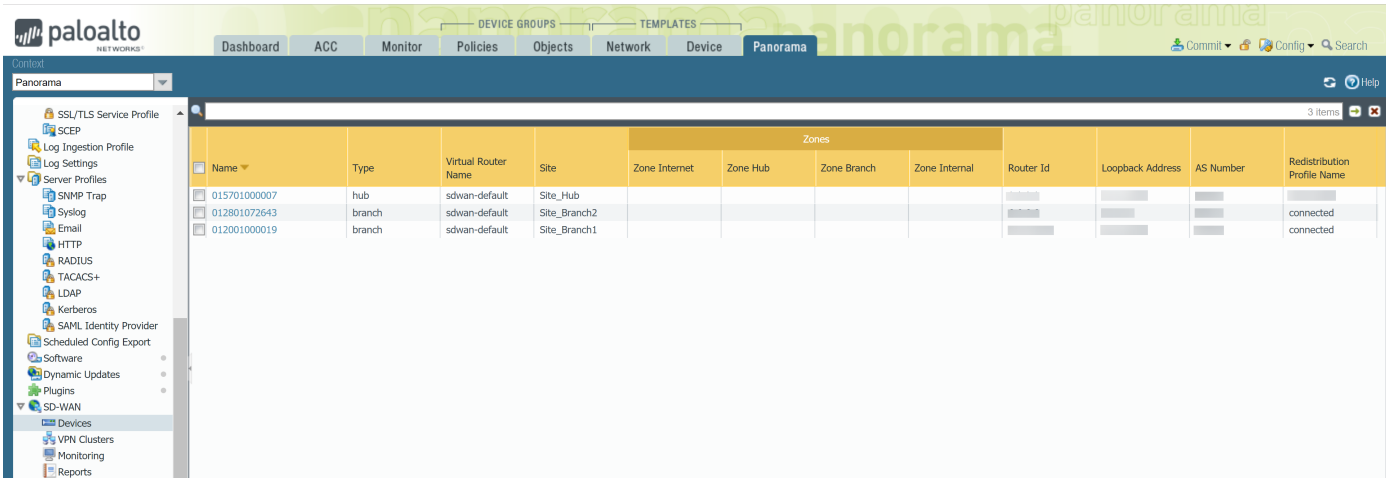
	A	B	C	D	E	F	G	H	I	J	K
1	device-serial	type	site	zone-internet	zone-branch	zone-hub	zone-internal	loopback-address	prefixes redist	as-number	router-id
2	12001000019	branch	Site_Branch1					2.2.2.2/32		65420	5.5.5.5/32
3	12801072643	branch	Site_Branch2					3.3.3.3		65413	6.6.6.6
4	15710000007	hub	Site_Hub					1.1.1.1/32	10.0.0.0/8	65432	1.1.1.1

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。



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。

為 SD-WAN 設定 HA 裝置

您可以在 SD-WAN 環境中設定處於主動/被動 HA 模式的兩個分支或兩個中樞。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。

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。

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® 9.1.0 僅支援中樞-支點 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。

完整網狀 *SD-WAN VPN* 拓撲在 *PAN-OS 9.1.0* 中不受支援。

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。

將為 VPN 叢集中的所有中樞和分支建立一個強大的隨機 IKE 預先共用金鑰，以保護 VPN 通道，且每個防火牆都有一個主要金鑰，用於加密該預先共用金鑰。系統會保護預先共用金鑰，即使管理員也不可查看。從 PAN-OS 9.1.2 開始，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。

在叢集成員不忙碌時重新整理預先共用金鑰。

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 | （PAN-OS 9.1.2 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.2 和更高的 1.0 版本）為 Auto VPN 組態建立的 IPSec VPN 通道指定 IP 位址範圍。

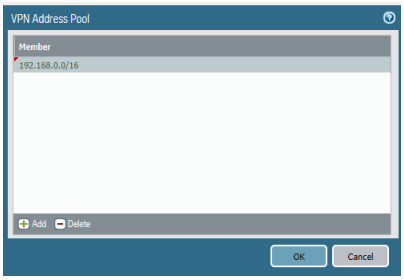
Auto VPN 組態會在一個中樞和多個分支之間建立一個 *VPN* 通道，並向通道端點指派 *IP* 位址。輸入您希望 *Auto VPN* 用作 *VPN* 通道的子網路範圍。您可以輸入最多 *20* 個 *20 IP* 前置詞/網路遮罩範圍。*Auto VPN* 從該集區中提取 *VPN* 通道位址，首先從最大範圍提取（必要時從下一個最大範圍提取）。您必須為集區設定至少一個範圍。如果您在將組態推送到中樞或分支前沒有執行此步驟，則「認可並推送」將失敗。

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. **Add**（新增）一個或多個（最多 20 個）**Member**（成員）IP 位址和網路遮罩範圍，例如 192.168.0.0/16。

4. 按一下 **OK**（確定）。



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

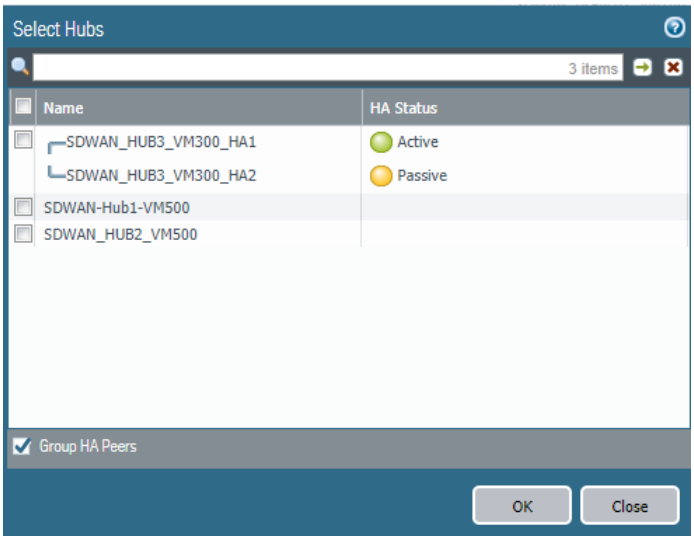
1. 選取 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 叢集），然後 **Add**（新增）一個 VPN 叢集。
2. 輸入 VON 叢集的描述性名稱。

   VPN 叢集名稱中不支援使用底線和空格，如果使用，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）。

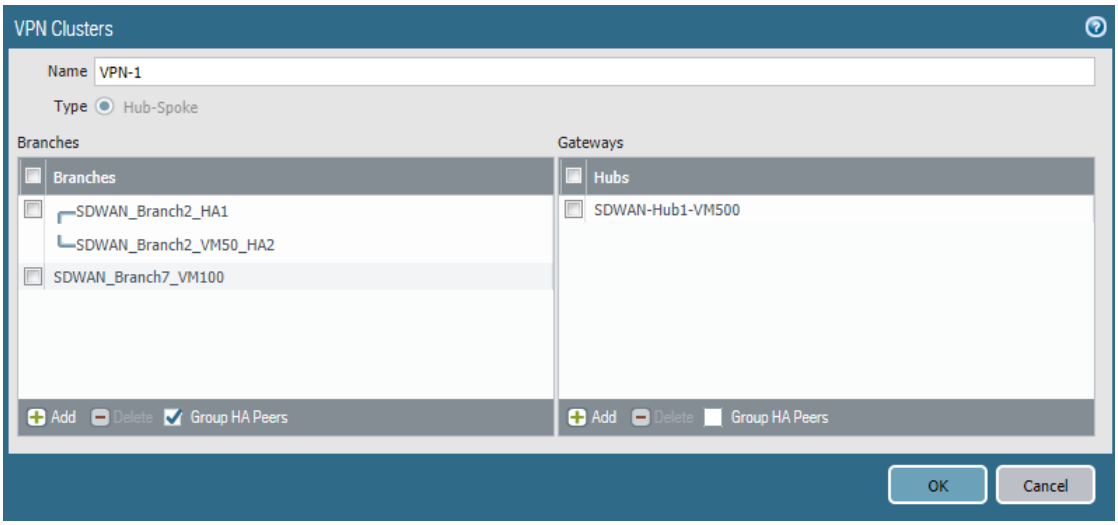
   PAN-OS 9.1.0 中僅支援 *Hub-Spoke*（中樞-支點）*VPN* 叢集類型。
4. **Add**（新增）一個或多個您確定需要互相通訊的分支裝置。
   - （SD-WAN 外掛程式 1.0.1 和更高的 1.0 版本）選取 **Group HA Peers**（群組 **HA** 端點）以將對等一起顯示。
   - 選取要新增至叢集的分支裝置。
   - 按一下 **OK**（確定）。
5. **Add**（新增）一個或多個您確定需要與分支裝置通訊的中樞裝置。如果新增了多個中樞裝置，您必須使用路由指標來控制哪個是主要裝置哪個是輔助裝置。

   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。

   - （SD-WAN 外掛程式 1.0.1 和更高的 1.0 版本）選取 **Group HA Peers**（群組 **HA** 端點）以將對等一起顯示。
   - 選取要新增至叢集的中樞。
   - 按一下 **OK**（確定）。



6. （SD-WAN 外掛程式 1.0.1 和更高的 1.0 版本）在「分支」或「閘道」區域選取 **Group HA Peers**（群組 **HA** 端點）以將 HA 對等一起顯示。



7. 按一下 **OK**（確定）儲存您的組態變更。

STEP 5 | （PAN-OS 9.1.2 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.2 和更高的 1.0 版本）在指向中樞的分支前發佈額外前置詞。

在 *PAN-OS 9.1.0* 中，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。從 *PAN-OS 9.1.2* 開始，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。

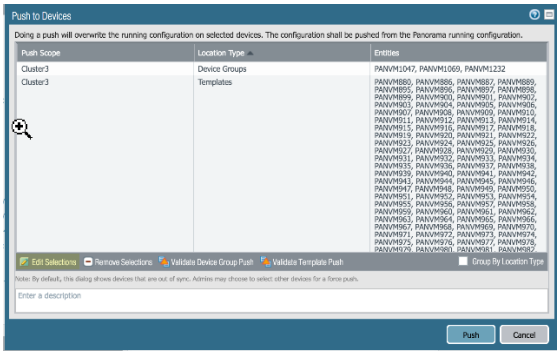
1. 選取 **Panorama** > **SD-WAN** > **Devices**（裝置），然後選取一個分支防火牆。
2. 選取 **BGP**，然後 **Add**（新增）一個或多個具有網路遮罩的 IP 位址到**Prefix(es) to Redistribute**（要重新散佈的前置詞）。
3. 按一下 **OK**（確定）。

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

STEP 7 | 將組態推送至中樞。

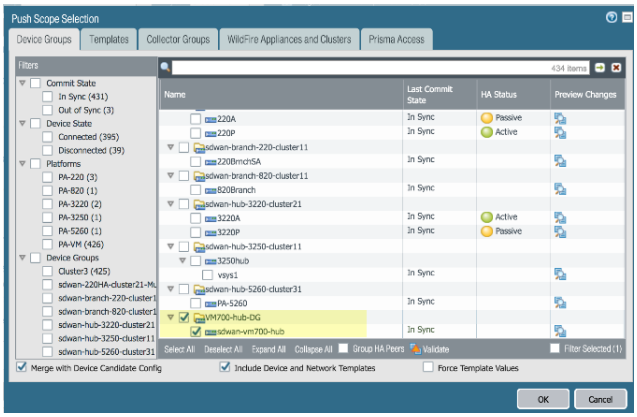
在 *Panorama* 為中樞建立虛擬 *SD-WAN* 介面時，*Panorama* 並不一定使用連續的介面編號建立介面。它可能隨機跳過一個介面編號，例如，*sdwan.921*、*sdwan.922*、*sdwan.924*、*sdwan.925*。儘管有不連續的編號，*Panorama* 仍然會為 *SD-WAN* 介面建立正確的編號。使用可操作 *CLI* 命令 ***show interface sdwan?*** 來查看 *SD-WAN* 介面。

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。

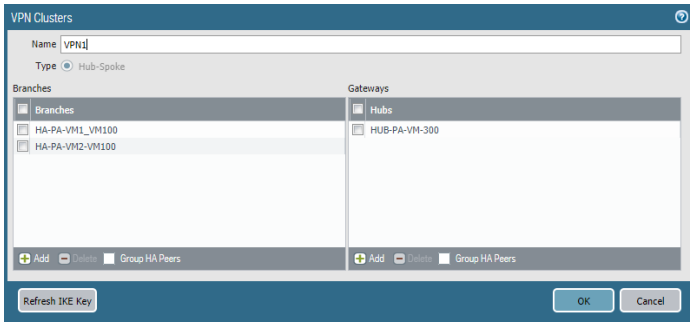
STEP 8 | 重複之前的步驟，但是選取您的分支裝置群組，將組態推送到分支。

STEP 9 | （PAN-OS 9.1.2 和更高的 9.1 版本，以及 SD-WAN 外掛程式 1.0.2 和更高的 1.0 版本）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。

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**），然後選取一個叢集。
2. 在螢幕底部，選取 **Refresh IKE Key**（**重新整理 IKE 金鑰**）。



3. **Commit**（**認可**）。
4. **Push to Devices**（**推送到裝置**）。

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 | 針對變數 **Type**（類型）選取 **Interface**（介面）。

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）> **IPv4**，然後 **Add**（新增）靜態路由 **Name**（名稱）。

STEP 7 | 對於 **Destination**（目的地），選取您建立的變數。

STEP 8 | 對於 **Interface**（介面），選取 **sd_wan**。

STEP 9 | 對於 **Next Hop**（下一個躍點），選取 **IP Address**（**IP** 位址），然後輸入靜態路由下一個躍點的 IP 位址（靜態路由前往的中樞或分支）。

STEP 10 | 按一下 **OK**（確定）。

STEP 11 | **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 **sd_wan** 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 12 | 為返回流量設定靜態路由。

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 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。

- 監控 SD-WAN 工作
- 監控 SD-WAN 應用程式和連結效能
- 對應用程式效能進行疑難排解
- 對連結效能進行疑難排解
- 產生 SD-WAN 報告

監控 SD-WAN 工作

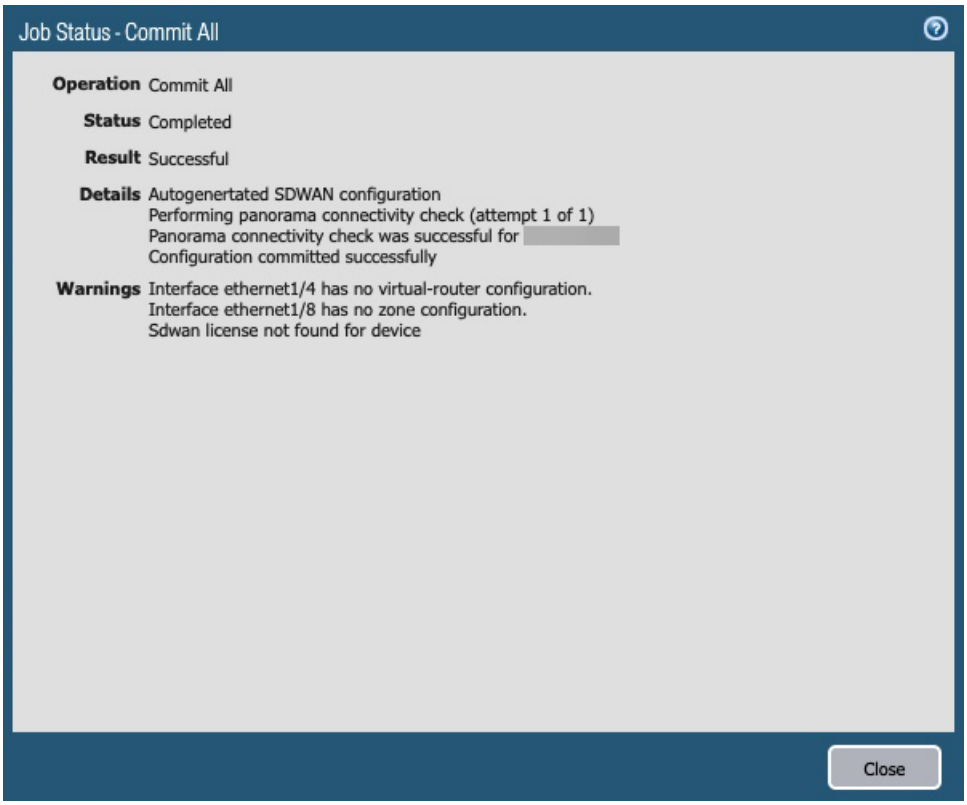
監控提交、推送和從 Panorama™ 管理伺服器執行的其他 SD-WAN 工作，以獲取有關特定工作的洞察和詳細資訊。

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。

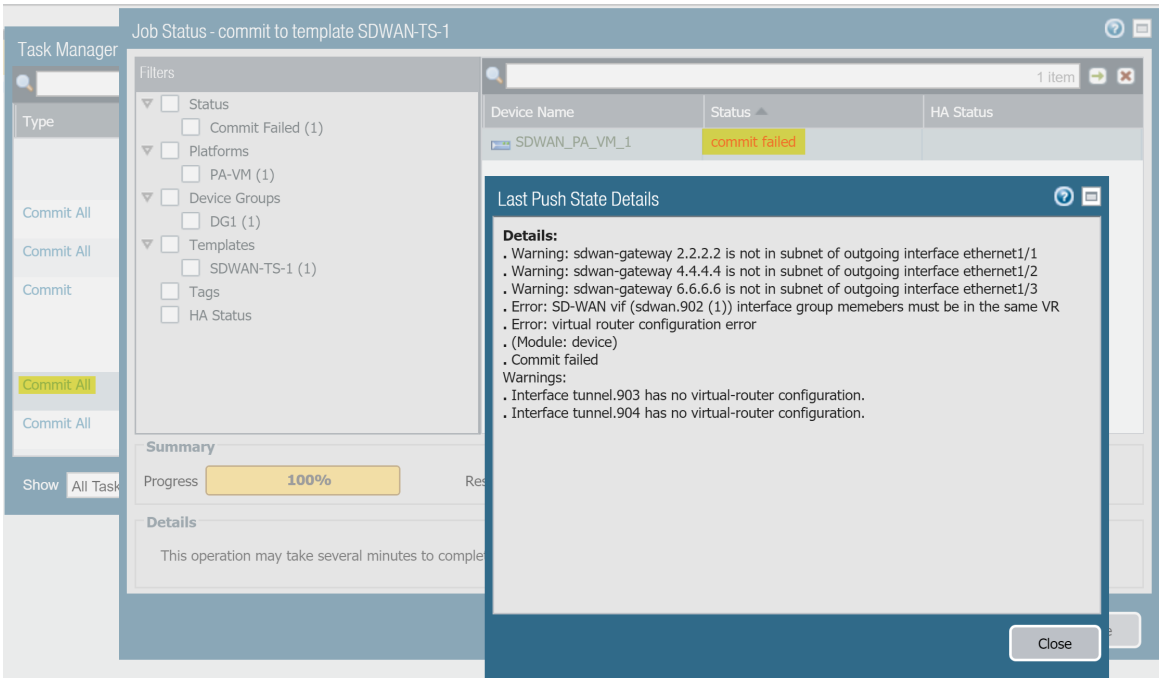
STEP 2 | 在編輯 SD-WAN 組態後，**Commit**（提交）您的變更以檢視工作狀態。

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

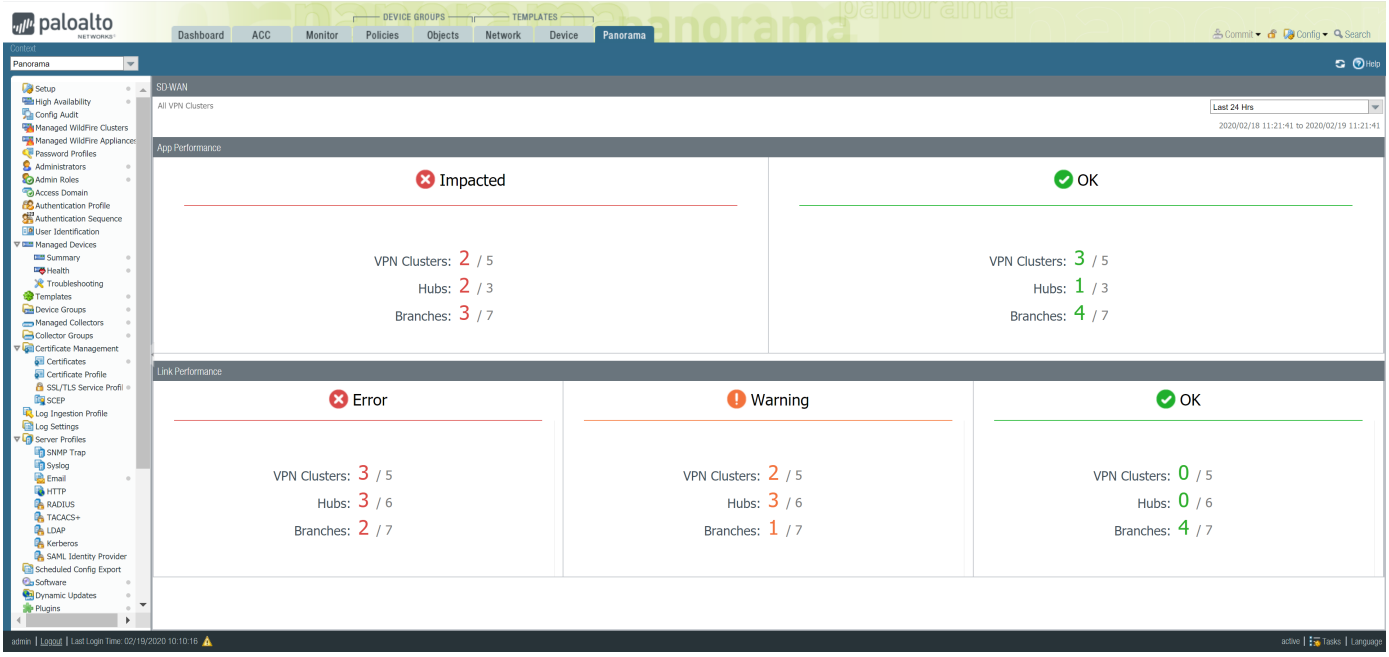
監控 VPN 叢集中的應用程式和連結效能，透過檢視所有 VPN 叢集中的摘要資訊，然後依次向下鑽研以將問題隔離到受影響的網站、應用程式和連結，從而對問題進行疑難排解。登陸儀表板顯示：

- 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。

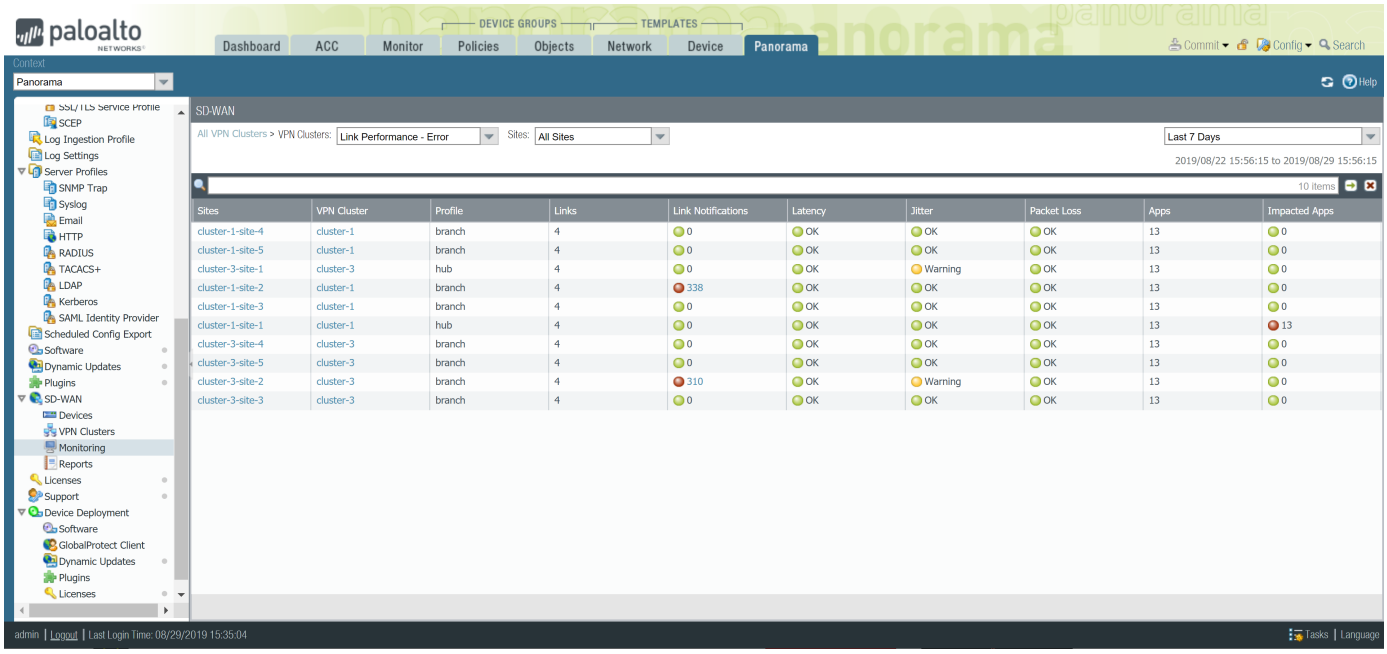
從登陸儀表板中，將檢視縮小到具有「錯誤」或「警告」狀態的受影響應用程式或連結。然後選取受影響的網站以檢視網站層級的詳細資料。從網站中，檢視應用程式層級或連結層級的詳細資料。

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。



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。

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。

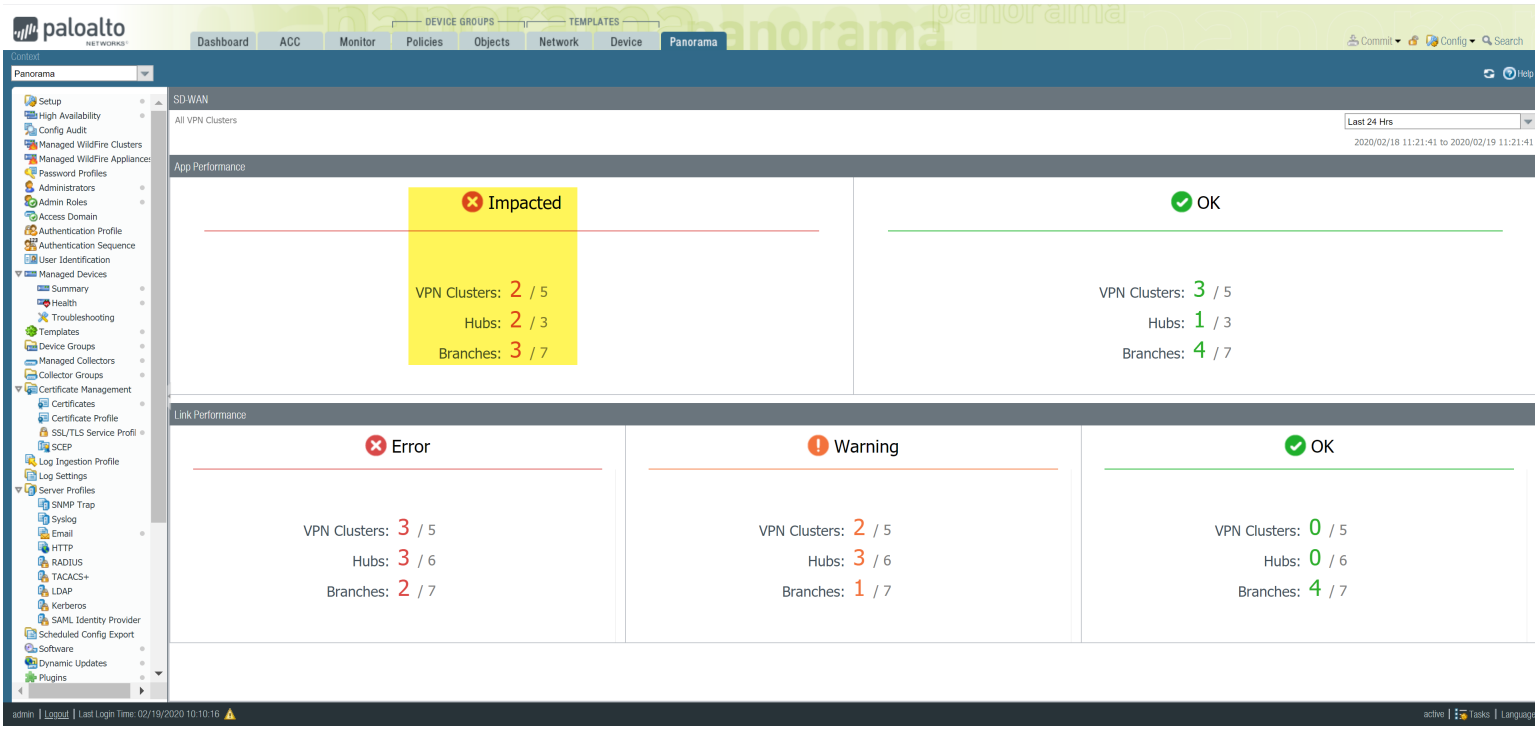
STEP 6 | 按一下受影響的應用程式以檢視應用程式層級或連結層級的詳細資料。

對應用程式效能進行疑難排解

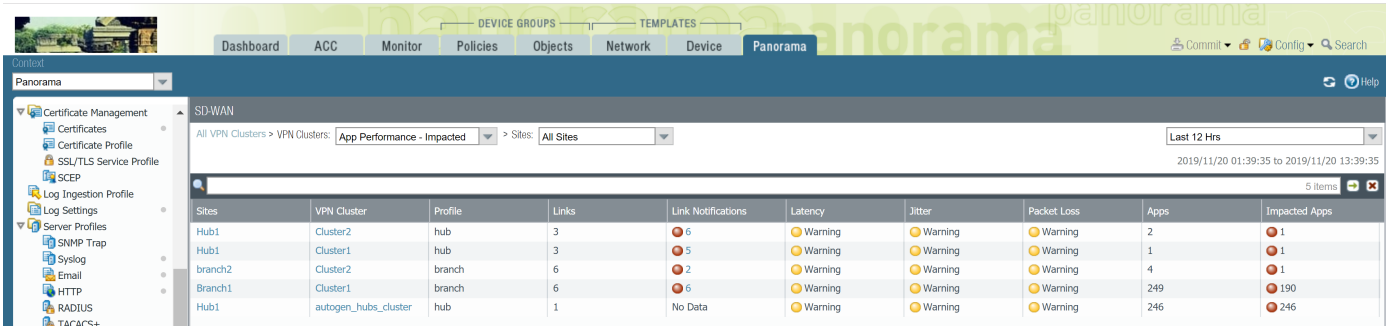
要確保使用者體驗不受影響，務必要瞭解導致應用程式和服務效能下降的原因。瞭解 VPN 叢集為什麼受到影響以及應用程式流量容錯移轉到其他連結有助於調整您的 SD-WAN 組態。

STEP 1 | 登入 Panorama 網頁介面。

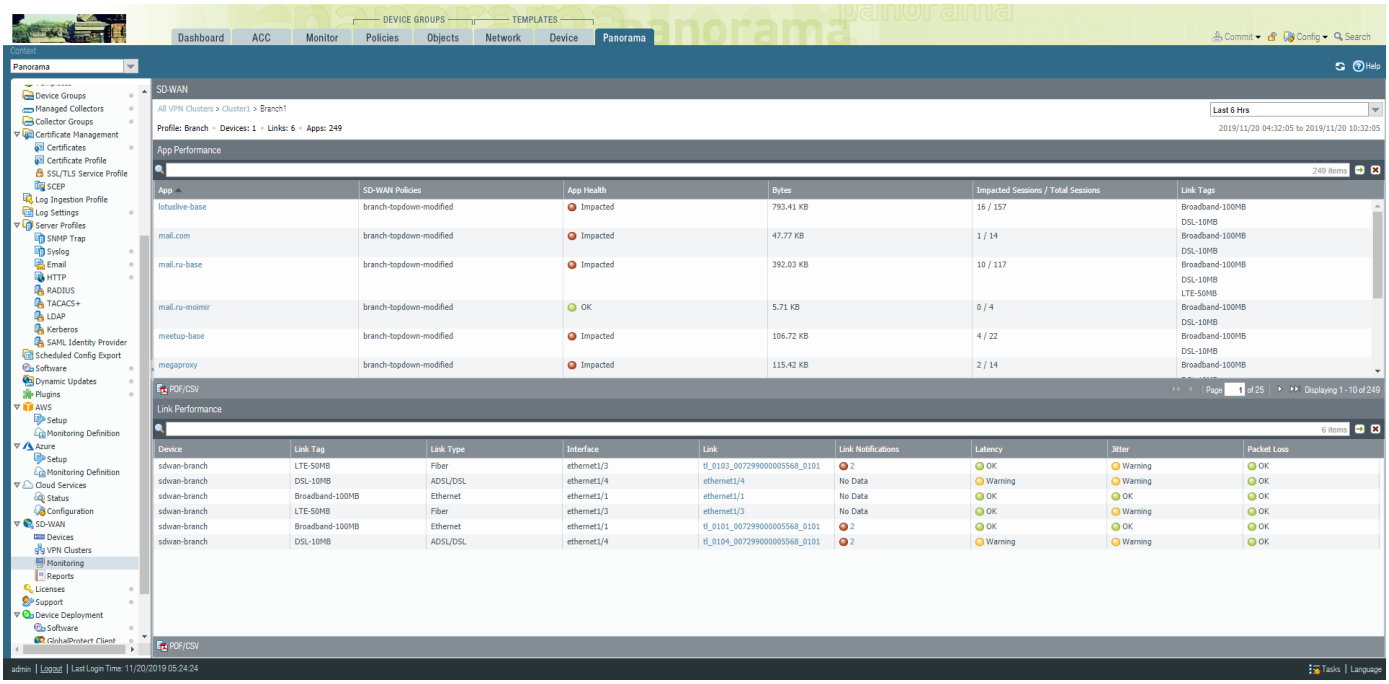
STEP 2 | 選取 **Panorama** > **SD-WAN** > **Monitoring**（監控）並檢視 **Impacted**（受影響）的 VPN 叢集。



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）。

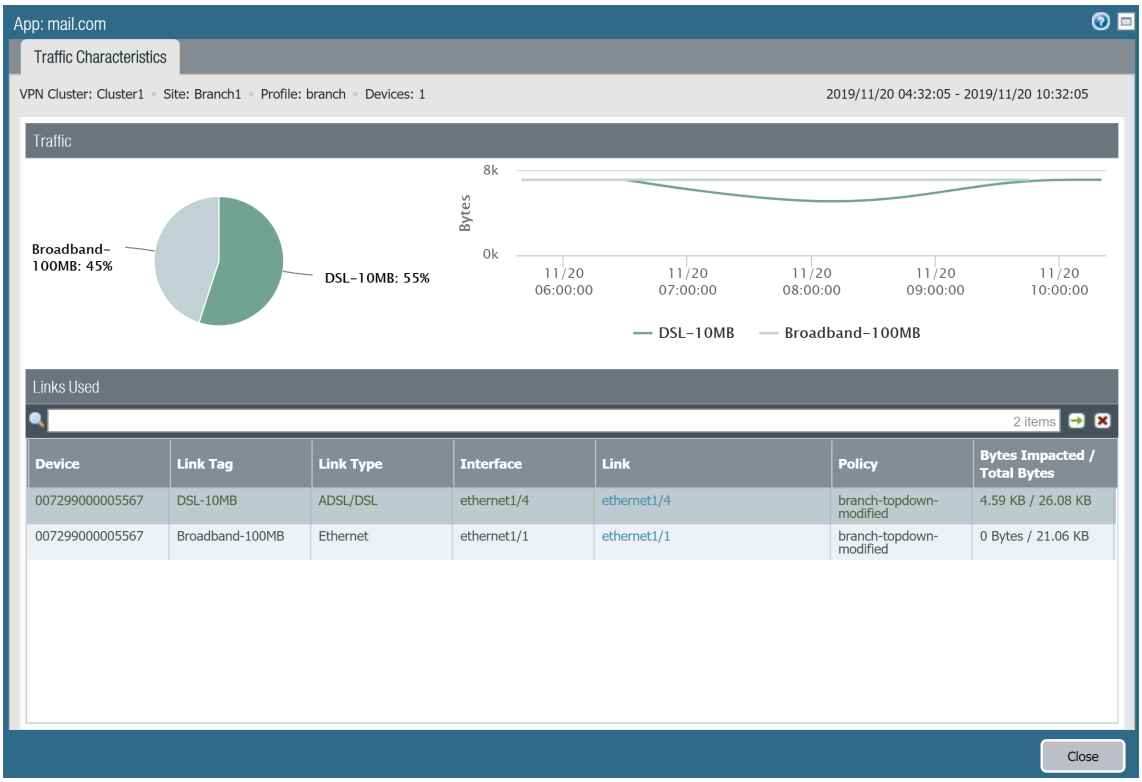


STEP 4 | 在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。



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：

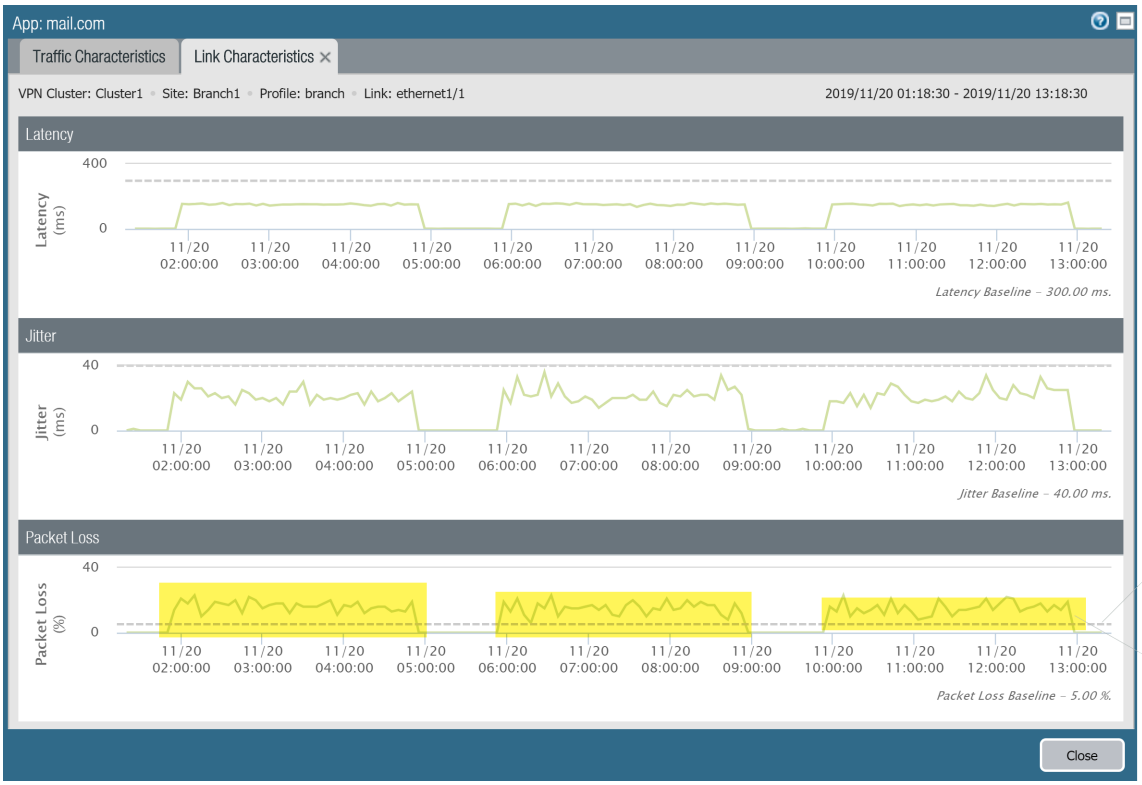
- 檢閱圓形圖以瞭解整個網際網路服務中應用程式流量的詳細資訊。
- 檢閱線條圖以瞭解每個網際網路服務在一段時間內傳輸了多少位元組的資料。
- 檢閱「使用的連結」部分以瞭解應用程式流量使用了哪些連結，以及瞭解在所選時間範圍內的總位元組中有多少位元組受到影響。



STEP 6 | 調查哪個健康情況指標導致應用程式交換連結。

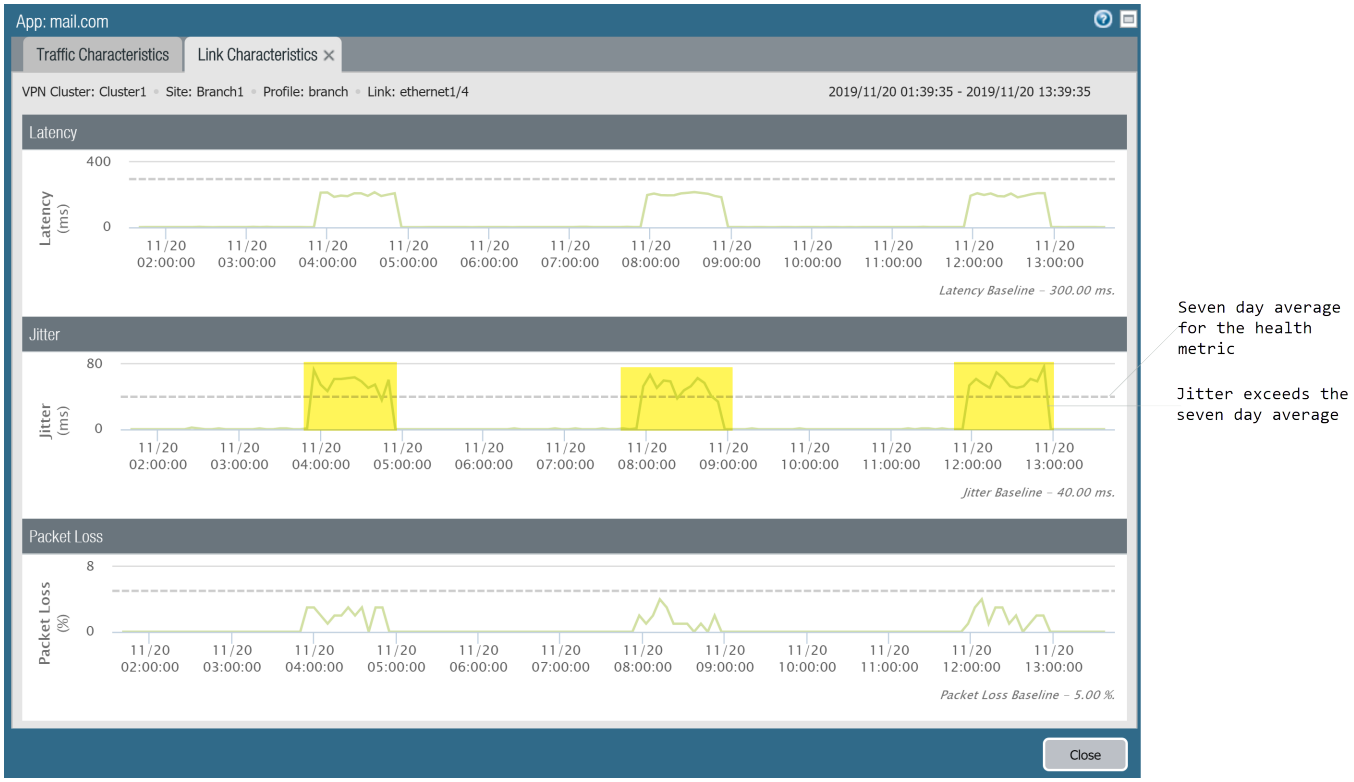
帶點的線條表示健康情況指標的七日平均值。

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。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七日平均閾值，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，該連結的乙太網路 1/4 的抖動超出七日平均閾值。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：

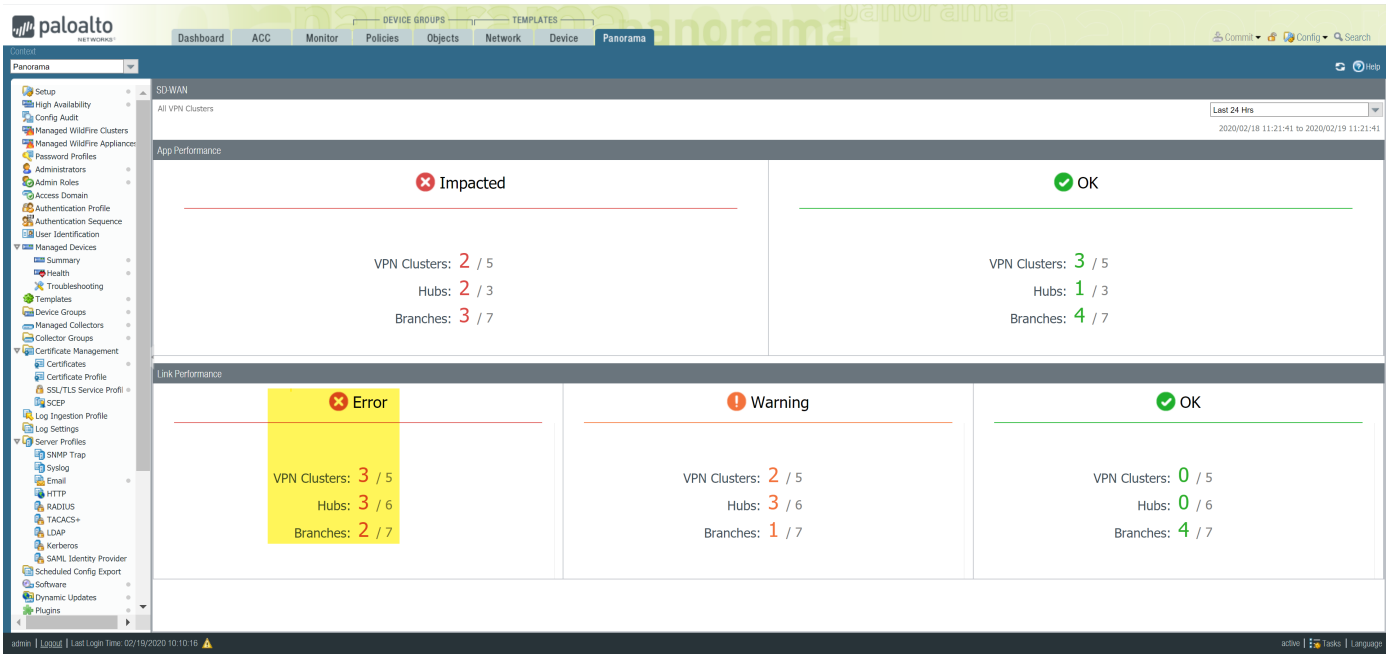
- 考慮新增額外連結到 Traffic Distribution Profile（流量散佈設定檔）。為應用程式流量新增可進行容錯移轉的額外連結，確保應用程式流量和使用者體驗不會受到健康情況下降的連結的影響。
- 在您的 Path Quality Profile（路徑品質設定檔）中重新設定健康情況閾值。可能是健康情況閾值過於嚴格，導致不必要的連結容錯移轉。例如，某個應用程式的封包遺失率在達到 18% 時使用者體驗才會受到影響，但是封包遺失閾值設定為 10%，這會導致在完全沒有必要的情況下應用程式容錯移轉到另一個連結。
- 咨詢您的網際網路服務提供商 (ISP) 以確定是否存在您無法控制但他們可以解決的網路影響。

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。

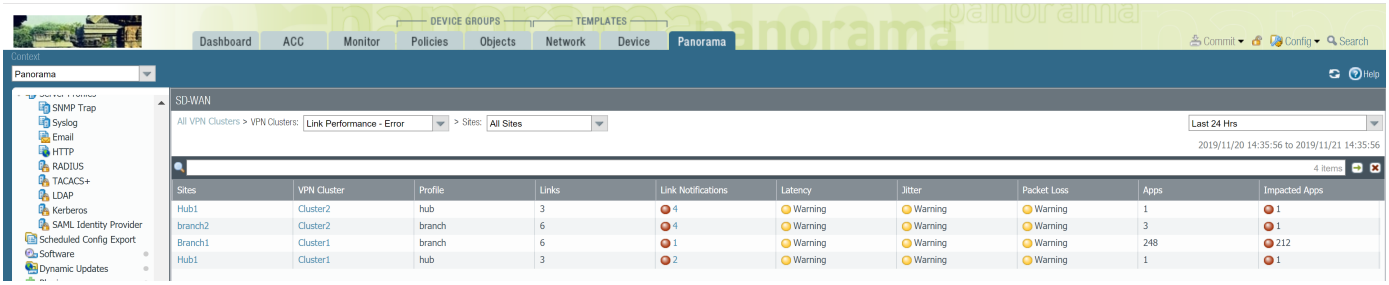
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **SD-WAN** > **Monitoring**（監控）並檢視 **Impacted**（受影響）的 VPN 叢集。

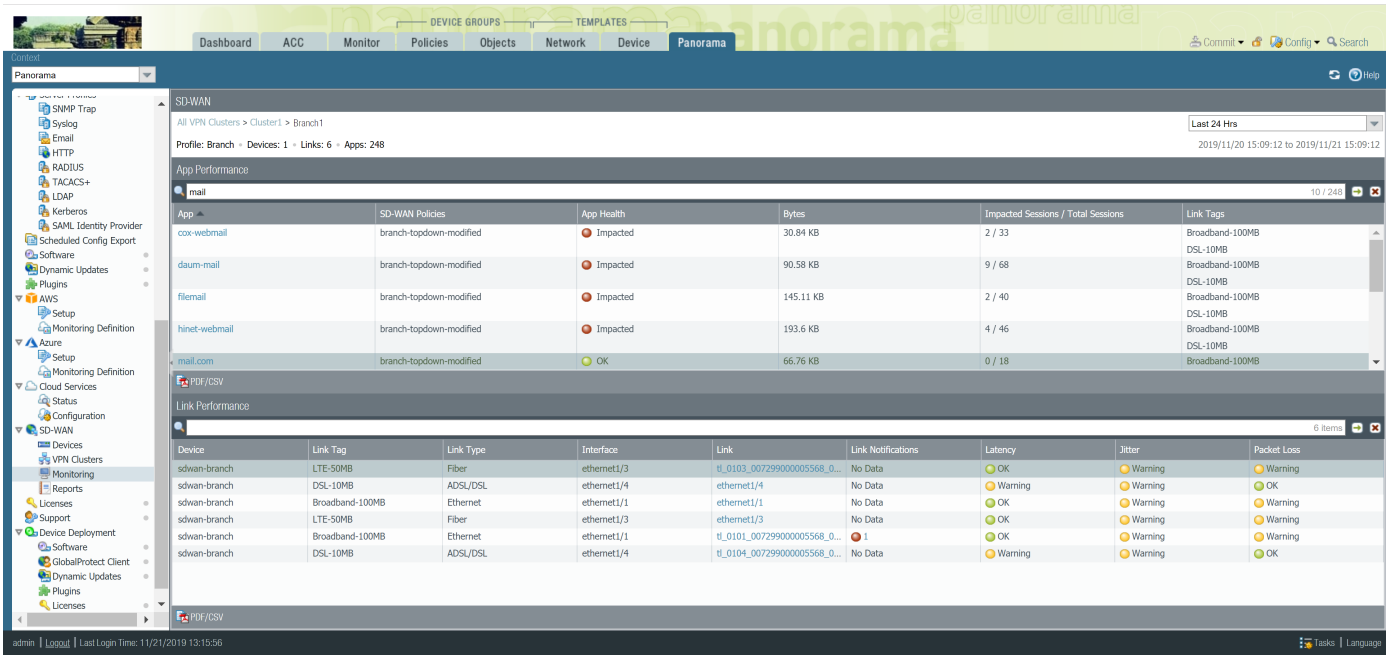


STEP 3 | 基於 **Site**（網站）下拉式清單中的偏好指標篩選 VPN 叢集，並選取時間範圍。在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。

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）。

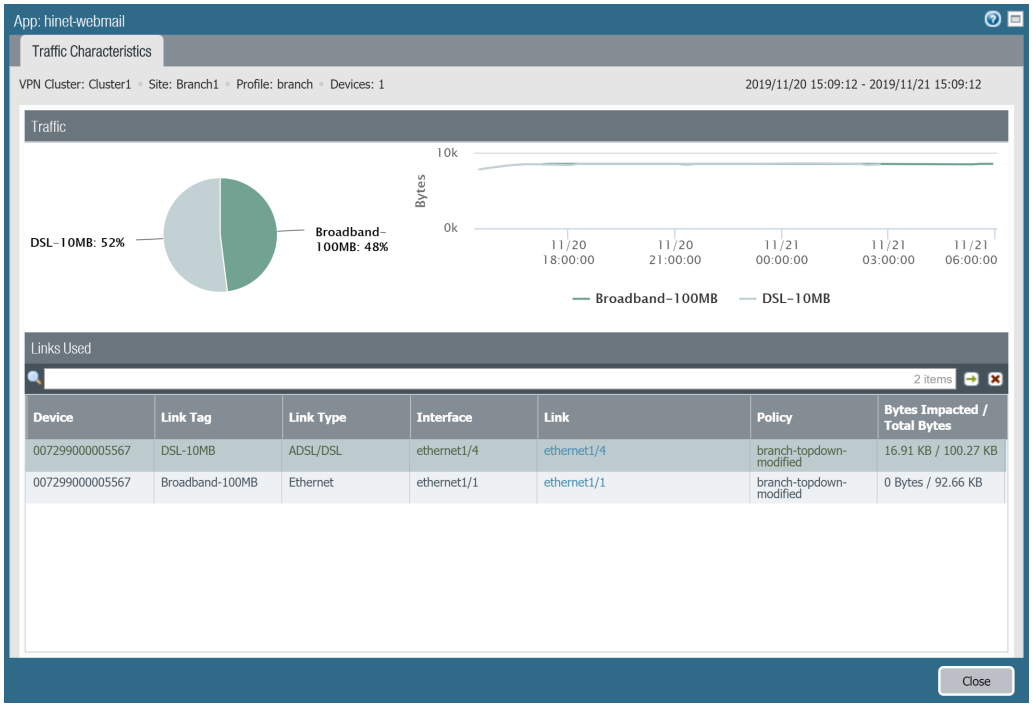


STEP 4 | 在「網站」欄中，選取受影響的中樞或分支防火牆以檢視受影響的應用程式和相應的連結效能。



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：

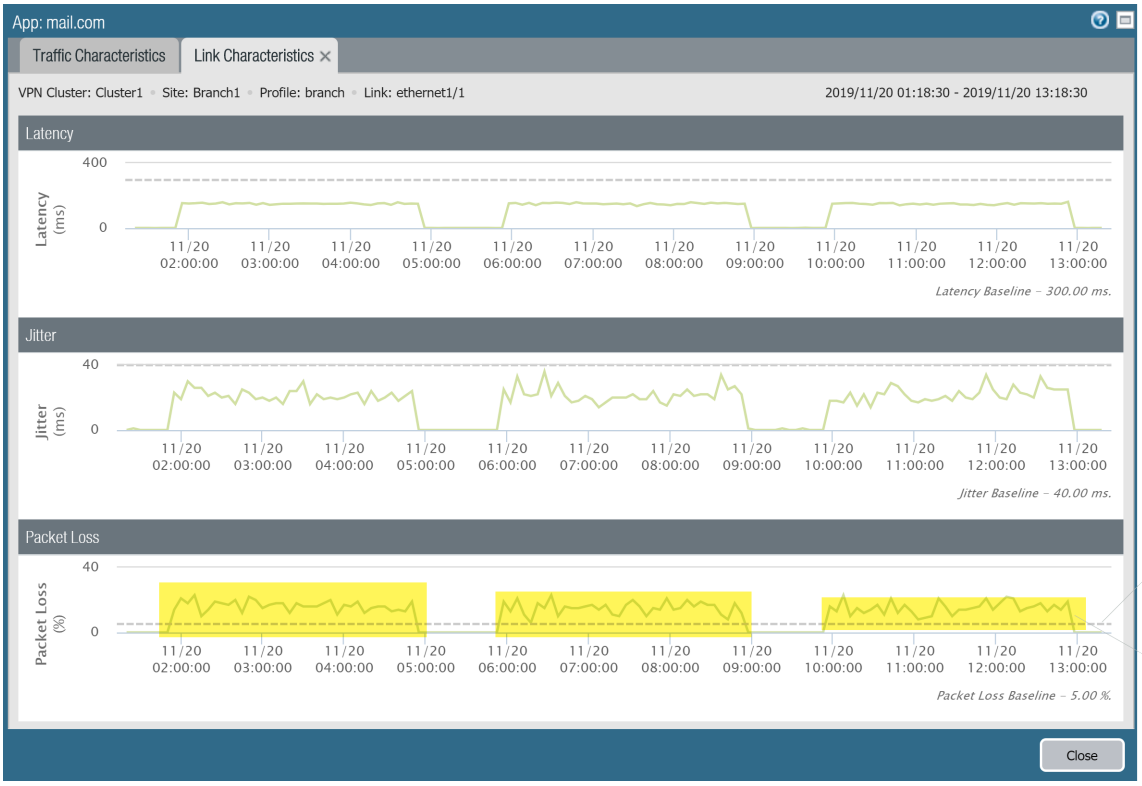
- 檢閱圓形圖以瞭解整個網際網路服務中應用程式流量的詳細資訊。
- 檢閱線條圖以瞭解每個網際網路服務在一段時間內傳輸了多少位元組的資料。
- 檢閱「使用的連結」部分以瞭解應用程式流量使用了哪些連結，以及瞭解在所選時間範圍內的總位元組中有多少位元組受到影響。



STEP 6 | 調查哪個健康情況指標導致應用程式交換連結。

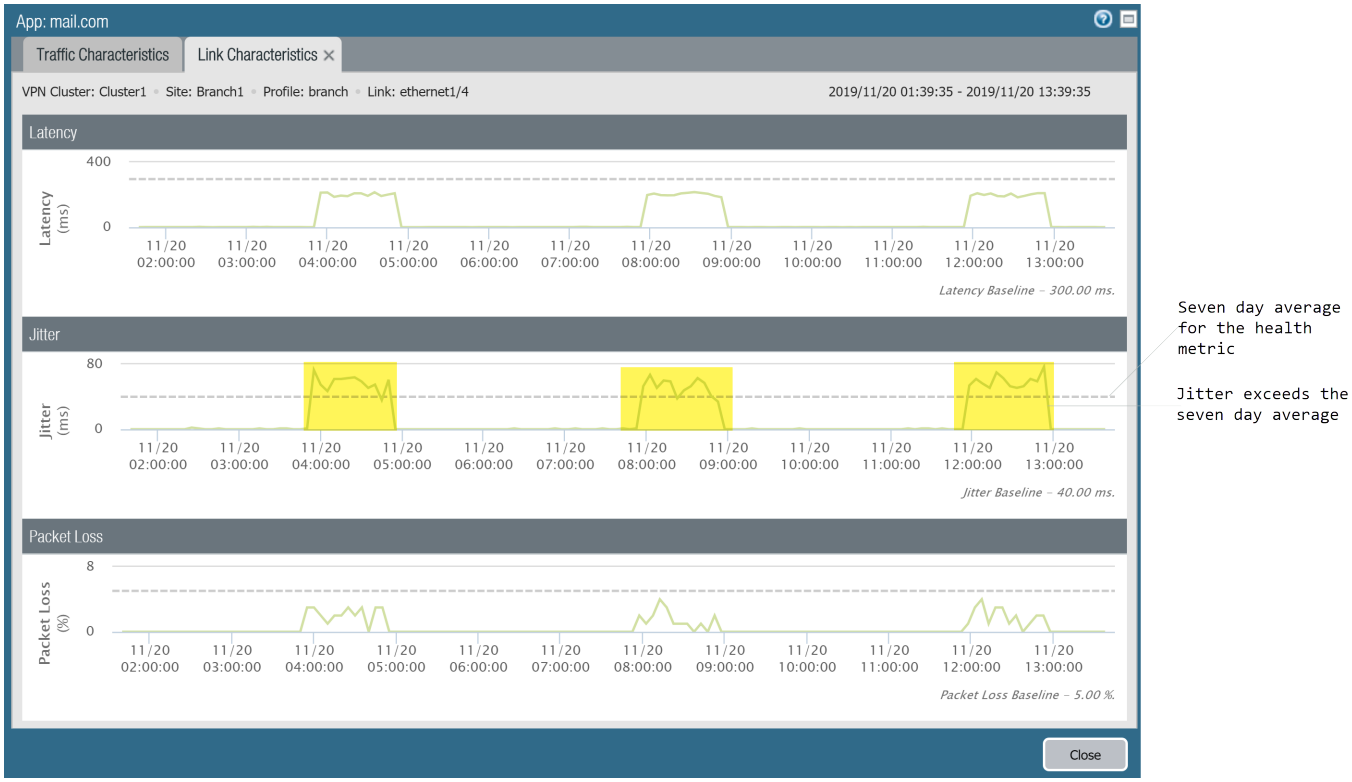
帶點的線條表示當您 建立路徑品質設定檔 時設定的閾值。

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。

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。

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。

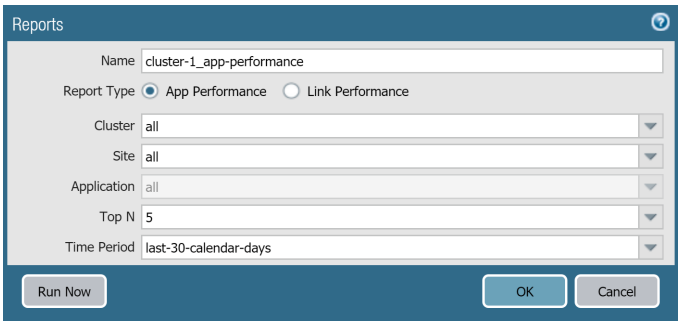
STEP 3 | 設定 SD-WAN 報告參數。

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）。

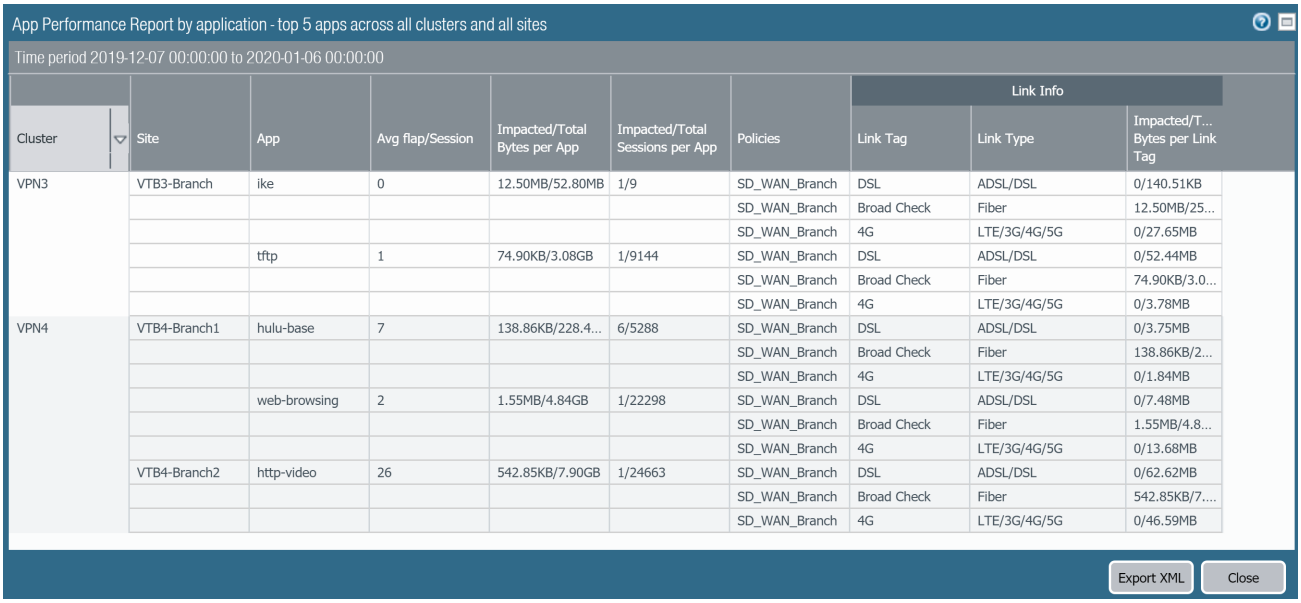
   如果您已選取 **all**（全部）叢集，那麼此欄位將以灰色顯示，無法選取網站。
5. （僅應用程式效能）選取要為其產生報告的 **Application**（應用程式）。

   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）。



Cluster	Site	App	Avg flap/Session	Impacted/Total Bytes per App	Impacted/Total Sessions per App	Policies	Link Info		
							Link Tag	Link Type	Impacted/T... Bytes per Link Tag
VPN3	VTB3-Branch	ike	0	12.50MB/52.80MB	1/9	SD_WAN_Branch	DSL	ADSL/DSL	0/140.51KB
						SD_WAN_Branch	Broad Check	Fiber	12.50MB/25...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/27.65MB
		tftp	1	74.90KB/3.08GB	1/9144	SD_WAN_Branch	DSL	ADSL/DSL	0/52.44MB
						SD_WAN_Branch	Broad Check	Fiber	74.90KB/3.0...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/3.78MB
VPN4	VTB4-Branch1	hulu-base	7	138.86KB/228.4...	6/5288	SD_WAN_Branch	DSL	ADSL/DSL	0/3.75MB
						SD_WAN_Branch	Broad Check	Fiber	138.86KB/2...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/1.84MB
		web-browsing	2	1.55MB/4.84GB	1/22298	SD_WAN_Branch	DSL	ADSL/DSL	0/7.48MB
						SD_WAN_Branch	Broad Check	Fiber	1.55MB/4.8...
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/13.68MB
	VTB4-Branch2	http-video	26	542.85KB/7.90GB	1/24663	SD_WAN_Branch	DSL	ADSL/DSL	0/62.62MB
						SD_WAN_Branch	Broad Check	Fiber	542.85KB/7....
						SD_WAN_Branch	4G	LTE/3G/4G/5G	0/46.59MB

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
> 解除安裝 SD-WAN 外掛程式

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。	`> 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>`
• 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。	`> 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>`

如果您想要 ...	使用 ...
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`
• 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>`

如果您想要 ...	使用 ...
• 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`

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 | （僅針對 SD-WAN 外掛程式 1.0.2 和之後的版本）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）儲存您的組態變更。

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。