paloalto TECHDOCS

SD-WAN 管理员指南

3.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

November 22, 2022

Table of Contents

SD-WAN 概述

了解 SD-WAN，并计划您的配置以确保部署成功。

关于 SD-WAN

软件定义广域网 (SD-WAN) 是指可您使用多种 Internet 和专有服务来创建一种既可降低成本，又可最大化地提升应用程序质量和可用性的智能、动态 WAN 的技术。从 PAN-OS® 9.1 开始，Palo Alto Networks® 通过单一管理系统中的 SD-WAN 覆盖提供强大的安全性。在将您的 WAN 连接到 Internet 时，您无需使用带路由器、防火墙、WAN 路径控制器和 WAN 优化器等组件的昂贵且耗时的 MPLS，您可以通过 Palo Alto Network 防火墙上的 SD-WAN 在使用更少组件的情况下，获得价格更优惠的 Internet 服务。您无需购买和保留其他 WAN 组件。

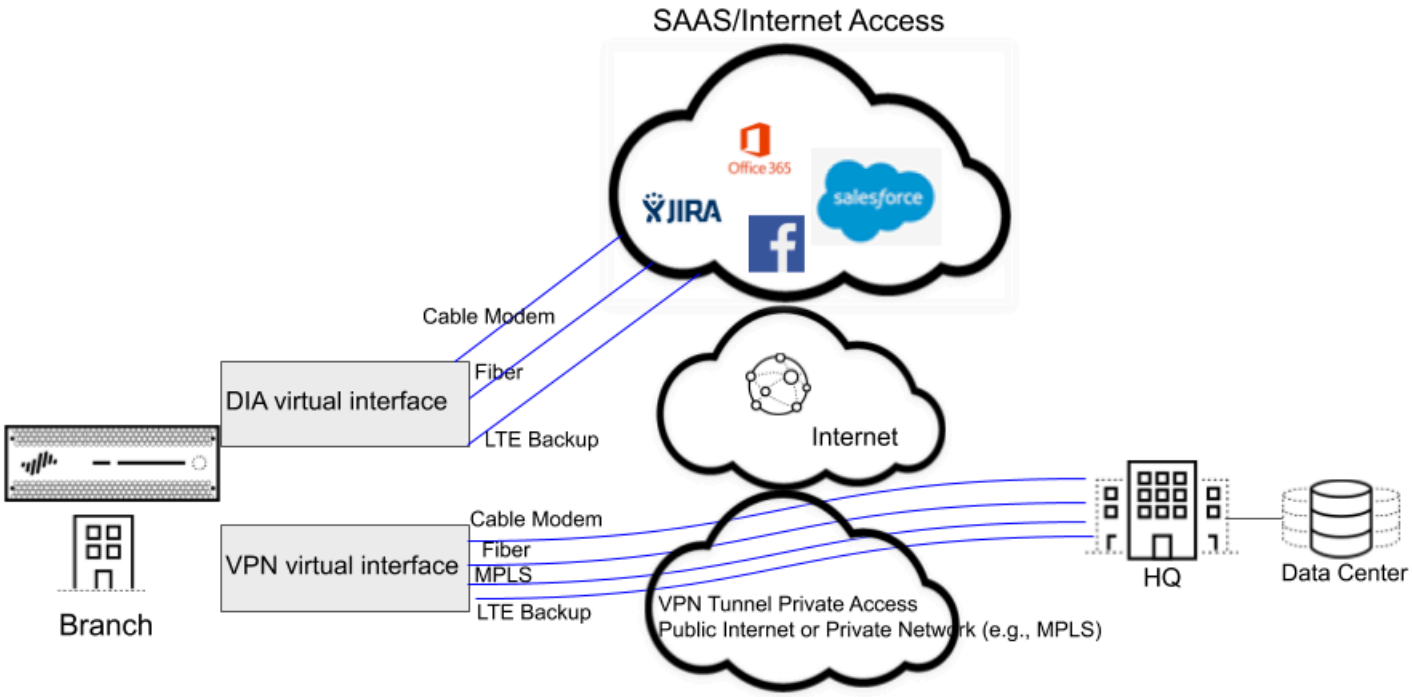
- 具有 SD-WAN 功能的 PAN-OS 安全性
- SD-WAN 链路和防火墙支持
- Prisma Access 中心支持
- 集中管理

具有 **SD-WAN** 功能的 **PAN-OS** 安全性

SD-WAN 插件与 PAN-OS 集成到一起后，只需从一位供应商就可获得 PAN-OS 防火墙的各项安全功能以及 SD-WAN 功能。SD-WAN 覆盖支持根据应用程序、服务、以及每个应用程序和服务允许使用的链路状况选择动态、智能路径。每个链路路径运行状况监控内容包括延迟、抖动和数据包丢失。通过粒度应用程序和服务控制，您可以根据应用程序的类别（任务关键型、延迟敏感型）或应用程序是否满足特定运行状况条件等对其进行优先级排序。因为会话会在不到一秒钟的时间内故障转移到一条性能更好的路径，因此，您可以通过动态路径选择避免供电不足和节点故障问题。

SD-WAN 覆盖可与 User-ID™ 和 App-ID™ 等 PAN-OS 所有安全功能配合使用，为分支机构提供更全面的安全控制。通过 App-ID 整套功能（App-ID 解码器、App-ID 缓存、以及源/目标外部动态列表 [EDL] IP 地址列表），可以标识应用程序，从而实现对 SD-WAN 流量的基于应用程序的控制。您可以通过流量的零信任分段部署防火墙。您可以通过 Panorama Web 界面或 Panorama REST API 配置和管理 SD-WAN。

您可以使用基于云的服务，而不是让您的 Internet 通信流量从分支到中心再到云，您希望 Internet 流量可通过直接连接的 ISP 从分支直接进入云。这种从分支到互联网的访问被称为互联网直接接入 (DIA)。您无需在 Internet 流量中使用中心带宽和花费金钱。因为分支防火墙已经执行安全防护，因此，就不再需要中心防火墙对 Internet 流量实施安全性。将分支上的 DIS 用于 SaaS、Web 浏览或不会回传到中心的高带宽应用程序。下图展示的是由三个从分支到云的链路构成的 DIA 虚拟接口。此外，图中还显示了 VPN 隧道虚拟接口，其包括用于在总部将分支连接到中心的四个链路。



SD-WAN 链路和防火墙支持

您可以通过链路捆绑将使用不同 ISP 与同一目标进行通信的多个物理链路组合成一个虚拟 SD-WAN 接口。防火墙根据应用程序和服务，选择用于会话负载共享的链路（路径选择），并在供电不足或停电时提供故障转移保护。这样，您就可以保证应用程序的最佳性能。防火墙通过虚拟 SD-WAN 接口中的链路自动执行会话负载共享，以充分利用可用带宽。SD-WAN 接口必须具备同一类型的所有连接（DIA 或 VPN）。VPN 链路支持中心辐射型拓扑。

SD-WAN 支持的 WAN 连接类型包括：ADSL/DSL、电缆调制解调器、以太网、光纤、LTE/3G/4G/5G、MPLS、微波/无线电、卫星、WiFi、以及任何作为从以太网至防火墙接口的连接方式。关于如何使用链路的适用策略由您决定。您可以在昂贵的 MPLS 或 LTE 连接之前使用价格较实惠的宽带连接。或是，您可以使用特定的 VPN 隧道以接入某个区域内的特定中心。

有关支持 SD-WAN 软件功能的防火墙型号的完整列表，请参阅 SD-WAN 的系统要求。

如果是购买 Palo Alto Networks 新一代防火墙的新客户，您将使用 SD-WAN 的默认虚拟路由器。如果您是老客户，您可以选择让 PAN-OS 覆盖任何现有虚拟路由器，或是使用 SD-WAN 的新路由器和新区域将 SD-WAN 内容与已有配置分开。

从 PAN-OS 11.0 开始，SD-WAN 插件 3.1 支持高级路由引擎，该引擎使用行业标准配置方法来推进管理员任务。尽管在概念上是等效的，但高级路由引擎使用逻辑路由器而不是虚拟路由器来实例化路由域。启用高级路由时，将创建逻辑路由器并使用高级路由引擎进行路由。当您禁用高级路由时，将创建虚拟路由器并使用旧版引擎进行路由。

Prisma Access 中心支持

PAN-OS Secure SD-WAN 可以通过 SD-WAN 插件 2.2 及更高版本为您提供 Prisma Access 中心支持，让您可以完全控制应用程序的保护方式和位置。Prisma Access 中心支持允许 PAN-OS 防火墙连接到 Prisma Access 计算节点 (CN)，以在 SD-WAN 中心辐射型拓扑中实现云端安全。这种支持可以实现从本地安全到 Prisma Access 的无缝链路故障转移，并且能够混合使用两者以满足您的安全需求。

在同时具有 PAN-OS SD-WAN 防火墙和 Prisma Access 中心的混合拓扑中，SD-WAN 中心作为 Prisma Access CN（IPSec 终端节点），SD-WAN 分支作为 PAN-OS 防火墙。SD-WAN 自动创建 IKE 和 IPSec 隧道，以将分支连接到中心。您可以使用流量分布配置文件创建 SD-WAN 策略以匹配特定的互联网应用程序，并将它们重定向到您选择的 PAN-OS 防火墙或 Prisma Access 部署。本地和云端安全平台可以通过 Prisma Access 中心支持协同工作，提供一个具有由 Panorama 管理的一致安全策略的完整解决方案。

请参阅 SD-WAN 的系统要求，了解 Prisma Access 中心支持所需的最低 PAN-OS 和 SD-WAN 插件版本。

Prisma Access 中心支持具有以下限制：

- 不支持导入和导出与 Prisma Access 相关的 SD-WAN 配置。
- Prisma Access 配置不支持加载、部分加载、恢复和部分恢复。
- 不支持登录现有的 Prisma Access 远程网络安全处理节点 (RN-SPN)。对于连接到 Prisma Access 的现有分支，您需要删除该分支，然后重新登录。
- Prisma Access 防火墙上没有可用的 SD-WAN CLI 命令。
- 在 CN 上，对于源自 CN 的流量没有路径选择。
- SD-WAN 报告和统计数据中未提供 Prisma Access 统计数据。

集中管理

Panorama™ 提供多种配置和管理 SD-WAN 的方法。通过这些方法，可在地理位置分散的多个防火墙上配置多个选项，这比单独配置防火墙更快、更便捷。您可以从单个位置更改网络配置，无需单独配置每个防火墙。通过自动 VPN 配置，Panorama 可配置出具有安全的 IKE/IPSec 连接的分支和中心。VPN 集群定义在地理位置实现相互通信的中心和分支。防火墙使用 VPN 隧道监控分支和中心之间的路径运行状况，从而提供亚秒级供电不足情况检测。

您可以通过 Panorama 仪表板查看 SD-WAN 链路和性能，这样，您就可以调整 SD-WAN 的路径质量阈值等方面，从而提高其性能。集中统计信息和报告包括应用程序和链路性能统计信息、路径运行状况衡量和趋势分析、以及应用程序和链路问题的集中视图。

首先，请了解您的 SD-WAN 用例，然后查看 SD-WAN 配置元素、流量分发方法，最后，计划您的 SD-WAN 配置。为了加快配置速度，最佳做法是导出一个空的 SD-WAN 设备 CSV，输入分支机构 IP 地址、要使用的虚拟器、防火墙站点名称、防火墙所属区域、以及 BGP 路由信息等内容。Panorama 使用 CSV 文件配置 SD-WAN 中心和分支，并在中心和分支之间自动配置 VPN 隧道。SD-WAN 支持通过 EBGP 进行动态路由，并使用 Panorama 的 SD-WAN 插件进行配置，允许所有分支只与中心通信，或是与中心和其他分支通信。

如果 *Panorama* 正在管理多 vsys 防火墙，则必须在 *vsys1* 上配置所有启用 *SD-WAN* 的接口和配置。

SD-WAN 不支持跨多 *VSYS* 防火墙的多个虚拟系统的 *SD-WAN* 配置。

SD-WAN 接口必须配置在同一个虚拟路由器中；它们不能拆分到不同的虚拟路由器中。

SD-WAN 的系统要求

查看适用于 SD-WAN 的 Panorama™ 插件的最低软件版本、插件版本和资源要求。

从 *PAN-OS 11.0* 开始，可以使用插件版本 *3.1* 为 SD-WAN 配置高级路由。

平台	PAN-OS	系统要求	Prisma Access 云配置插件	SD-WAN 插件
Panorama	11.0	• （Panorama 虚拟设备）系统磁盘 — 224GB 系统磁盘 • **CPU**—16 个 CPU • 内存—64GB 内存 • 系统模式—Panorama 模式和仅管理模式 • （仅管理模式下的 M-Series 设备）8TB RAID 日志记录磁盘对已启用	N/A	3.1
	10.2.3-h3		3.2.1-h5	3.0.4
	10.2.1		此版本不支持；预计未来的版本支持。如果您将 SD-WAN 与 Prisma Access 云配置插件配合使用，请不要升级到 PAN-OS 11.0。	3.0.1
	10.2.0			3.0
	10.1.9		3.2.1-h5	2.2.3
	10.1.5-h1		2.1	2.2.1
	10.1.0		2.1	2.2
下一代防火墙	• **PAN-OS 10.2**—10.2.0 • **PAN-OS 10.1**—10.1.4 • **PAN-OS 10.0**—10.0.8	N/A		
Prisma Access 计算节点	10.0.7*	* Prisma Access 计算节点（IPSec 终端节点）必须运行 PAN-OS 10.0.7 或更高的 10.0 版本。如有必要，与您的销		

平台	PAN-OS	系统要求	Prisma Access 云配置插件	SD-WAN 插件
		售团队一起请求升级，然后再尝试将分支机构登入 Prisma Access 中心。		

以下防火墙型号支持 SD-WAN 软件功能：

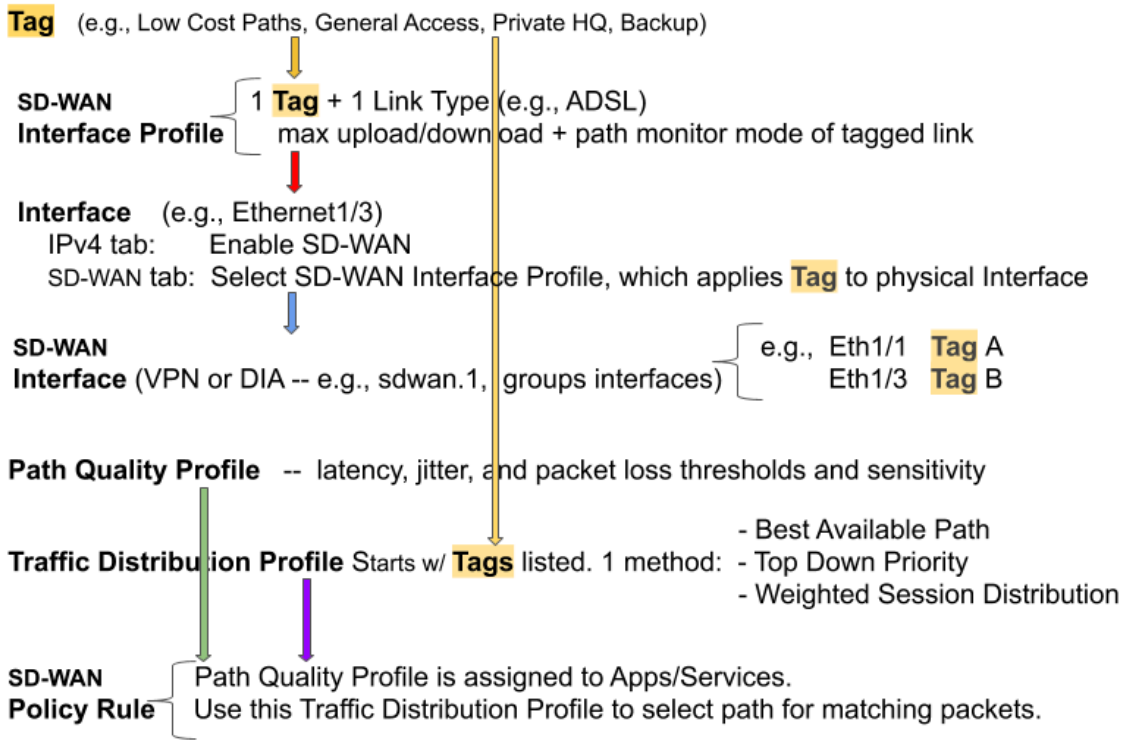
- PA-220 和 PA-220R
- PA-400 系列
- PA-820 和 PA-850
- PA-3200 系列
- PA-800 系列
- PA-5200 系列
- PA-5400 系列
- PA-7000 系列
- VM-50
- VM-100
- VM-300
- VM-500
- VM-700

SD-WAN 配置元素

SD-WAN 配置元素可以协同工作，允许您：

- 将共享一个公共目标的物理以太网接口分组到一个逻辑 SD-WAN 接口。
- 指定链路速度。
- 指定一个便于 SD-WAN 保证可以在路径恶化（或供电不足或断电）时根据其选择一个新的最佳路径的阈值。
- 指定选择新的最佳路径的方法。

此视图清楚显示元素之间的关系。



SD-WAN 配置通过指定某些应用程序或服务从分支进入中心，或从分支进入 Internet 采取的 VPN 隧道或互联网直接接入 (DIA)，从而控制流量采用的链路。对路径进行分组，这样，防火墙可在其中一个路径出现问题后，选择一个新的最佳路径。

- 您选择的 **Tag**（标记）名称用于标识链路；您通过将接口配置文件应用到接口，从而将标记应用到链路（接口），如红色箭头所示。每个链路只能有一个标记。两个黄色箭头代表的是在接口配置文件和流量分发配置文件中应用了标记。您可以通过标记控制流量分发接口的顺序。Panorama 可以通过标记系统配置很多具有 SD-WAN 功能的防火墙接口。
- **SD-WAN Interface Profile**（**SD-WAN** 接口配置文件）指定应用到物理接口的标记，以及接口使用的链路类型（ADSL/DSL、电缆调制解调器、以太网、光纤、LTE/3G/4G/5G、MPLS、微波/无线电、卫星、WiFi 等）。您还可以通过接口配置文件指定 ISP 连接的最大上传和下载速度

(Mbps)。此外，您还可以更改防火墙监控路径的频率；默认情况下，防火墙会适当地监控链路类型。

- 带 IPv4 或 IPv6 地址的第 3 层以太网 **Interface**（接口）可以支持 SD-WAN 功能。您可以将 SD-WAN 接口配置文件应用到此接口（红色箭头），以指示接口的特征。蓝色箭头指示在 SD-WAN 虚拟接口中引用并进行分组的物理接口。
- 虚拟 **SD-WAN Interface**（**SD-WAN** 接口） 是由一个或多个构成您可以路由流量、且带编号的 SD-WAN 虚拟接口的接口形成的 VPN 隧道或 DIA 组。属于 SD-WAN 接口的路径全都进入同一目标 WAN，且使用相同的类型（DIA 或 VPN 隧道）。（标记 A 和标记 B 表示用于可具有不同标记的虚拟接口的物理接口。）
- **Path Quality Profile**（路径质量配置文件）指定最大延迟、抖动和数据包丢失阈值。超出此阈值表示路径已出现问题，防火墙需要根据目标选择一个新路径。您可以通过敏感度设置（高、中、或低）告知防火墙，哪个路径监控参数对应用配置文件的应用程序更重要。绿色箭头表示您在一个或多个 SD-WAN 策略规则中引用路径质量配置文件；因此，您可以为应用至具有不同应用程序、服务、源、目标、区域和用户的规则指定不同的阈值。
- **Traffic Distribution Profile**（流量分发配置文件）指定防火墙如何在当前首选路径超过路径质量阈值时，确定新的最佳路径。您可以指定分发方法用于缩小新路径选择的标记；因此，黄色箭头从标记指向流量分发配置文件。流量分发配置文件指定用于规则的分发方法。
- **SD-WAN Policy Rules**（**SD-WAN** 策略规则）包括前述元素。紫色箭头指示您在（数据包配置文件/服务、源、目标和用户）规则中引用路径质量配置文件和流量分发配置文件，以专门指定防火墙如何为属于会话的数据包执行基于应用程序的 SD-WAN 路径选择。（还可以在 SD-WAN 策略规则中引用 **SaaS Quality Profile**（**SaaS** 质量配置文件）和 **Error Correction Profile**（纠错配置文件）。）

既然您已经了解元素之间的关系，请回顾流量分发方法，然后计划您的 SD-WAN 配置。

计划您的 SD-WAN 配置

计划用于启用了 SD-WAN 的分支和中心防火墙的完整拓扑结构，这样，就可以使用 CSV 文件创建 Panorama™ 模板，然后将配置推送到防火墙。

STEP 1 | 计划分支和中心位置、链路要求和 IP 地址。从 Panorama 开始，您将导出一个空的 SD-WAN 设备 CSV，并在其中填充分支和中心信息。

1. 确定每个（分支或中心）防火墙的角色。
2. 确定哪些分支与哪些中心通信；相互通信的各个分支和中心防火墙功能组就是一个 VPN 集群。例如，您可以按地理位置或功能组织 VPN 集群。
3. 确定每个分支和中心支持的 ISP 链路类型：ADSL/DSL、电缆调制解调器、以太网、光纤、 LTE/3G/4G/5G、MPLS、微波/无线电、卫星和 WiFi。
4. 确定链路类型支持的最大下载和上传带宽 (Mbps)，以及如何对链路实施这些速度控制，如步骤 2 所述。记录 ISP 链路的最大下载和上传带宽 (Mbps)。如果您需要配置 QoS 以控制应用程序带宽，可将此信息用作参考出口最大值。
5. 收集静态或动态分配的分支防火墙公共 IP 地址。防火墙必须拥有可在 Internet 上路由的公共 IP 地址，这样，就能启用和终止往返于 Internet 的 IPSec 隧道和路由应用程序流量。

   ISP 的客户端设备必须直接与防火墙上的以太网接口连接。

   如果您的设备在分支防火墙和中心之间执行 *NAT*，则此 *NAT* 设备可以阻止防火墙启动 *IKE* 对等和 *IPSec* 隧道。如果隧道失败，可与远程 *NAT* 设备的管理员一起解决此问题。
6. 收集分支和中心防火墙的私有网络前缀和序列号。
7. 确定每个防火墙接口的链路类型。

   在分支防火墙上同一以太网接口分配相同的链路类型，以使配置更加容易。例如，*Ethernet1/1* 始终是电缆调制解调器。
8. 确定站点和 SD-WAN 设备的命名约定。

   不得使用“中心”和“分支”等简单的主机名，原因在于自动 *VPN* 配置会使用这些关键字来生成各种配置元素。
9. 如果区域已在配置 SD-WAN 之前就位，则确定如何将这些区域映射到 SD-WAN 在执行路径选择是使用的预定义区域。您将现有区域映射到名为从区域到内部、从区域到中心、从区域到分支、以及从区域到 Internet 的预定义区域。

   您将在 *CSV* 中输入的信息（便于您一次添加多个 *SD-WAN* 设备）包括：序列号、设备类型（分支或中心）、映射到预定义区域（预先存在客户）的区域名称、回环地址、待重新分发的前缀、*AS* 编号、路由器 *ID*、以及虚拟路由器名称。

STEP 2 | 计划用于私有链路的链路捆绑和 VPN 安全性。

通过链路捆绑，可以将多个物理链路组合到一个 SD-WAN 虚拟接口中，以执行路径选择和故障转移保护。通过捆绑多个物理链路，可以在物理链路出现问题时提高应用程序质量。通过 SD-WAN 接口配置文件在多个链路上使用相同的链路标记，可以创建捆绑。链路标记用于标识具有相似访问类型和相似 SD-WAN 策略处理类型的链路捆绑。例如，您可以创建名为低价带宽的两路类型，并将光缆调制解调器和光纤宽带服务包含在其中。

STEP 3 | 标识将使用 SD-WAN 和 QoS 优化的应用程序。

1. 标识将为其提供 SD-WAN 控制和策略的业务关键型和延迟敏感型应用程序。这些应用程序需要良好的用户体验，且容易在链路状况不良时出现故障。

   从最关键和对延迟最敏感的应用程序开始，您可以在 *SD-WAN* 功能运行正常后添加应用程序。

2. 标识需要 QoS 策略以确定带宽优先级的应用程序。这些应用程序就是标识为关键或延迟敏感的应用程序。

   从最关键和对延迟最敏感的应用程序开始，您可以在 *SD-WAN* 功能运行正常后添加应用程序。

STEP 4 | 确定在原链路恶化或出现故障时，想让链路故障转移到不同链路的时间和方式。

1. 决定链路的路径监控模式，即使此时的最佳做法是保留链路类型的默认设置：

   - **Aggressive**（积极的）— 防火墙以固定的频率将探测数据包发送到 SD-WAN 链路的另一端（默认每秒五个探测）。积极的模式适用于路径质量监控是关键的链路；在这种情况下，您需要针对供电不足和停电情况执行快速检测和故障转移。积极的模式提供压秒级检测和故障转移。
   - **Relaxed**（宽松的）— 防火墙在以您配置的探测频率发送探测数据包之间观察到的一个可配置的 7 秒控制时间，这使得路径监控的频率比在积极的模式下更低。宽松的模式适用于带宽非常低的链路，卫星或 LTE 等运行成本昂贵的链路，或快速检测不如节省成本和带宽重要时的情况。

2. 排定防火墙将第一个链路用于新会话的顺序的优先级，以及哪个链路会成为替换出现故障转移的链路的候选链路（如果有多个候选链路）的顺序的优先级。

   例如，如果想让昂贵的备份 LTE 链路成为最后一个使用的链路（仅在廉价的宽带链路被超额订购，或是完全断开时），那么，请使用自上而下优先级流量分发方法，并将 LTE 链路上的标记置于流量分发配置文件的标记列表的最后一位。

3. 对于应用程序和服务，确定路径运行状况阈值。您会根据该阈值，决定路径质量的恶化程度，以让防火墙选择一个新路径（故障转移）。质量特征是延迟（范围为 10-2000ms）、抖动（范围为 10-1000ms）和数据包丢失百分比。

   这些阈值构成您可以在 SD-WAN 策略规则中引用的路径质量配置文件。一旦超过某个阈值（数据包丢失、抖动或延迟），防火墙将为匹配流量选择新的首选路径。例如，当 FTP 数据包来自源区域 XYZ 时，您可以创建一个延迟/抖动/数据包丢失阈值分别为 1000/800/10 的路径质量配置文件 AAA 在规则 1 中使用；当 FTP 数据包来自源 IP 地址 10.1.2.3 时，您可以创建阈值分别为 50/200/5 的路径质量配置文件 BBB 在规则 2 中使

用。最佳做法是从高阈值开始，然后测试应用程序对这些阈值的容忍方式。如果阈值设定过低，应用程序可能会频繁切换路径。

考虑您使用的应用程序和服务是否对延迟、抖动或数据包丢失特别敏感。例如，视频应用程序可能具有良好的缓冲功能，可以减轻延迟和抖动，但对数据包丢失敏感，这会影响用户体验。您可以在配置文件中将路径质量参数的敏感度设为高、中或低。如果延迟、抖动和数据包丢失的敏感度设置是一样的，则防火墙将按照数据包丢失、延迟和抖动的顺序检查参数。

4. 确定是否有链路可以加载应用程序或服务新的共享会话。

STEP 5 | 计划 Panorama 会将其推送到分支和中心以动态路由分支和中心之间流量的 BGP 配置。

1. 计划 BGP 路由信息，包括 4 字节自治系统编号 (ASN)。每个防火墙都处于单独的 AS 中，必须拥有一个唯一的 ASN。此外，每个防火墙还必须拥有一个唯一的路由器 ID。
2. 在已使用 BGP 的环境中使用 BGP 路由实施 SD-WAN 之前，请确保 SD-WAN 插件生成的 BGP 配置不会与现有的 BGP 配置冲突。例如，您必须将现有的 BGP AS 号码和路由器 ID 值作为相应 SD-WAN 设备值。
3. 如果不想使用 BGP 动态路由，请计划使用 Panorama 的网络配置功能将其他路由配置推送出去。您可以在分支和中心之间进行静态路由。只需忽略 Panorama 插件中所有 BGP 信息，并使用普通的虚拟路由器静态路由执行静态路由即可。

STEP 6 | 考虑用于 SD-WAN 虚拟接口、SD-WAN 策略规则、日志大小、IPSec 隧道（包括代理 ID）、IKE 对等端、BGP 和静态路由表、BGP 路由对等端的 防火墙型号容量，以及防火墙型号的性能（App-ID™、威胁、IPSec、解密）。确保您打算使用的分支和中心防火墙型号支持所需容量。

配置 SD-WAN

计划您的 SD-WAN 配置后，安装 SD-WAN 插件，并设置 Panorama™ 管理服务器，以集中管理中心和分支防火墙的 SD-WAN 配置。通过使用 Panorama，可以降低管理 SD-WAN 部署时产生的管理要求和运营开销，还可以更轻松地监控链路运行状况，并在出现问题时实施故障排除。

如果 *Panorama* 正在管理多 vsys 防火墙，则必须在 *vsys1* 上配置所有启用 *SD-WAN* 的接口和配置。

SD-WAN 不支持跨多 *VSYS* 防火墙的多个虚拟系统的 *SD-WAN* 配置。

- 安装 SD-WAN 插件
- 设置用于 SD-WAN 的 Panorama 和防火墙
- 创建链路标记
- 配置 SD-WAN 接口配置文件
- 配置 SD-WAN 物理以太网接口
- （可选）为 SD-WAN 配置聚合以太网接口和子接口
- （可选）为 SD-WAN 配置第 3 层子接口
- 配置 SD-WAN 虚拟接口
- 创建 SD-WAN 接口默认路由
- 配置 SD-WAN 链路管理配置文件
- 配置 SD-WAN 策略规则
- 允许互联网直接接入流量故障转移到 MPLS 链路
- 配置 DIA AnyPath
- 分发不匹配会话
- 添加 SD-WAN 设备到 Panorama
- （可选）配置 SD-WAN HA 设备
- 创建 VPN 集群
- 用 DDNS 服务创建全网状 VPN 集群
- （可选）创建 SD-WAN 静态路由
- （可选）为 SD-WAN 配置高级路由

安装 SD-WAN 插件

必须使用带 SD-WAN 插件的 Panorama™ 管理服务器配置和管理 SD-WAN 部署。如果您的 Panorama 已连接到 Internet，就可以直接从 SD-WAN 下载 SD-WAN 插件，并将其安装在 Panorama 管理服务器上。如果您的 Panorama 尚未连接到 Internet，您可以从 Palo Alto Networks®客户支持门户下载 SD-WAN 插件，并将其安装在 Panorama 管理服务器上。

- 在 Panorama 连接上 Internet 后安装 SD-WAN 插件
- 在 Panorama 未连接到 Internet 时安装 SD-WAN 插件

在 Panorama 连接上 Internet 后安装 SD-WAN 插件

必须使用安装有 SD-WAN 插件的 Panorama™ 管理服务器配置和管理 SD-WAN 部署。Panorama 连接到 Internet 后，您可以直接从 Panorama Web 界面下载和安装 SD-WAN 插件。此插件只能安装在管理您的 SD-WAN 防火墙的 Panorama 上，不得安装在单个中心和分支防火墙上。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **Plugins**（插件），搜索 **sd_wan** 插件，并为最新版本的插件执行 **Check Now**（立即检查）。

STEP 3 | **Download**（下载）并 **Install**（安装）SD-WAN 插件。

STEP 4 | 成功安装 SD-WAN 插件后，请选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

必须先执行此步骤，才能将所有配置更改提交到 Panorama。

STEP 5 | （仅管理模式）启用存储 SD-WAN 监视数据所需的日志记录磁盘。

- **M-Series** 设备 — 所有 M-Series 设备默认标配两对 8TB 日志记录磁盘，在 RAID 1 中。在“仅管理模式”下利用 Panorama 中的 SD-WAN 管理防火墙时，必须启用第一对日志记录磁盘对才能存储 SD-WAN 监视数据。

  1. 登录到 Panorama 命令行界面。
  2. 启用 M-Series 设备默认包含的第一对日志记录磁盘对。

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

  3. 验证日志记录 `Logging Disk Pair A` 为 `Available`：

     ```
     > show system raid detail
     ```

     当 RAID 设置完成时，会显示以下响应：

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

  4. 将日志记录磁盘设置为可用于日志记录。
     1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
     2. 选择 **Disks**（磁盘），并 **Add**（添加）每个阵列。
     3. 单击 **OK**（确定）保存更改。
     4. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
     5. 选择 **Commit**（提交） > **Push to Devices**（推送到设备），选择收集器组，然后 **Push**（推送）您的更改。

- **Panorama** 虚拟设备 — 如果在“仅管理模式”下部署了 Panorama 虚拟设备，则必须将系统磁盘增加到 224GB 才能存储 SD-WAN 监视数据。

STEP 6 | 继续设置用于 SD-WAN 的 Panorama 和防火墙以开始配置您的 SD-WAN 部署。

在 Panorama 未连接到 Internet 时安装 SD-WAN 插件

必须使用带 SD-WAN 插件的 Panorama™ 管理服务器配置和管理 SD-WAN 部署。如果 Panorama 尚未连接到 Internet，必须从 Palo Alto Networks 客户支持门户下载 SD-WAN 插件，并将其上传到 Panorama。此插件只能安装在管理您的 SD-WAN 防火墙的 Panorama 上，不得安装在单个中心和分支防火墙上。

STEP 1 | 登录到 Palo Alto Networks 客户支持门户。

STEP 2 | 选择 **Updates**（更新） > **Software Updates**（软件更新），然后，在筛选条件下拉列表中，选择 **Panorama Integration Plug In**（**Panorama** 集成插件）。

STEP 3 | 找到并下载 **SD-WAN Plug-in**（**SD-WAN** 插件）。

STEP 4 | 登录到 Panorama Web 界面。

STEP 5 | 选择 **Panorama** > **Plugins**（插件），并 **Upload**（上传） SD-WAN 插件。

STEP 6 | **Browse**（浏览）并找到从客户支持门户下载的 SD-WAN 插件，然后单击 **OK**（确定）。

STEP 7 | **Install**（安装）SD-WAN 插件。

STEP 8 | 成功安装 SD-WAN 插件后，请选择 **Commit**（提交）和 **Commit to Panorama**（提交到 **Panorama**）。

必须先执行此步骤，才能将所有配置更改提交到 Panorama。

STEP 9 | （仅管理模式）启用存储 SD-WAN 监视数据所需的日志记录磁盘。

- **M-Series** 设备 — 所有 M-Series 设备默认标配两对 8TB 日志记录磁盘，在 RAID 1 中。在“仅管理模式”下利用 Panorama 中的 SD-WAN 管理防火墙时，必须启用第一对日志记录磁盘对才能存储 SD-WAN 监视数据。

  1. 登录到 Panorama 命令行界面。
  2. 启用 M-Series 设备默认包含的第一对日志记录磁盘对。

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

  3. 验证日志记录 `Logging Disk Pair A` 为 `Available`：

     ```
     > show system raid detail
     ```

     当 RAID 设置完成时，会显示以下响应：

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

  4. 将日志记录磁盘设置为可用于日志记录。
     1. 选择 **Panorama** > **Managed Collectors**（Panorama > 受管收集器），然后编辑日志收集器。
     2. 选择 **Disks**（磁盘），并 **Add**（添加）每个阵列。
     3. 单击 **OK**（确定）保存更改。
     4. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。
     5. 选择 **Commit**（提交） > **Push to Devices**（推送到设备），选择收集器组，然后 **Push**（推送）您的更改。

- **Panorama** 虚拟设备 — 如果在“仅管理模式”下部署了 Panorama 虚拟设备，则必须将系统磁盘增加到 224GB 才能存储 SD-WAN 监视数据。

STEP 10 | 继续设置用于 SD-WAN 的 Panorama 和防火墙以开始配置您的 SD-WAN 部署。

设置用于 SD-WAN 的 Panorama 和防火墙

开始配置 SD-WAN 部署之前，必须将中心和分支防火墙作为受管设备添加，并创建所需模板和设备组配置，以成功将您的 SD-WAN 配置推送到 SD-WAN 防火墙。

- 将您的 SD-WAN 防火墙作为受管设备添加
- 创建 SD-WAN 网络模板
- 在 Panorama 中创建预定义区域
- 创建 SD-WAN 设备组

将您的 SD-WAN 防火墙作为受管设备添加

开始配置您的 SD-WAN 部署之前，必须先安装 SD-WAN 插件，并将您的中心和分支防火墙作为受管设备添加到 Panorama™ 管理服务器。在将您的 SD-WAN 防火墙作为受管设备添加到 Panorama™ 管理服务器时，必须激活 SD-WAN 许可证，以启用防火墙的 SD-WAN 功能。

在将您的 SD-WAN 防火墙作为受管设备添加时，必须配置受管防火墙，以转发日志到 Panorama。Panorama 从配置日志、流量日志、以及链路特征测量结果等多个源收集信息，以生成 SD-WAN 应用程序和链路运行状况信息。

STEP 1 | 启动防火墙 Web 界面。

STEP 2 | 激活您的 SD-WAN 许可证以启用防火墙上的 SD-WAN 功能。

您打算在 SD-WAN 部署中使用的每个防火墙都需要一个唯一的身份验证代码来激活许可证。例如，如果有 100 个防火墙，就必须购买 100 个 SD-WAN 许可证，并使用 100 个唯一的身份验证代码分别激活每个防火墙上的 SD-WAN 许可证。

对于 *VM* 系列防火墙，可将 *SD-WAN* 身份验证代码应用于特定的 *VM* 系列防火墙。如果停用 VM 系列防火墙，可激活同一型号中不同 *VM* 系列防火墙上的 *SD-WAN* 身份验证代码。

确保您的 *SD-WAN* 许可证仍然有效，以继续使用 *SD-WAN*。如果 *SD-WAN* 许可证到期，则会发生以下情况：

- 在您 ***Commit***（提交）任何配置更改时，会显示警告但不会出现提交失败的情况。
- 您的 *SD-WAN* 配置将不再起作用，但不会被删除。
- 防火墙不再监控和收集链路运行状况指标，并停止发送监控探测。
- 防火墙不再发送应用程序和链路运行状况指标到 *Panorama*。
- *SD-WAN* 路径选择逻辑被禁用。
- 虚拟 SD-WAN 接口上出现新的会话轮循机制。
- 现有会话保留在许可证过期时停留的特定链路上。
- 如果发生 *Internet* 中断，流量通过标准路由和 ECMP（如果已配置）流动。

STEP 3 | 将 Panorama IP 地址添加到防火墙。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后 Edit（编辑）Panorama 设置。
2. 在第一个字段中输入 Panorama IP 地址。

   Panorama FQDN 不支持用于 *SD-WAN*。
3. （可选）如果您已在 Panorama 中设置高可用性对，请在第二个字段中输入辅助 Panorama IP 地址。
4. 检验您是否 **Enable pushing device monitoring data to Panorama**（启用推送设备监控数据到 **Panorama**）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

STEP 4 | 配置 Panorama 的日志转发。

要显示监控和报告数据，需要将日志从您的 SD-WAN 防火墙转发到 Panorama。

默认情况下，如果为应用程序流量启用了解密，则会自动启用 *HTTP/2* 检查。使用 *HTTP/2* 连接的父会话不会生成任何流量日志，因为它们不携带任何应用程序流量。然而，由 *HTTP/2* 父会话中的流生成的子会话仍然会生成流量日志。有关查看 *HTTP/2* 连接日志的详细信息，请参阅 Palo Alto Networks 知识库。

STEP 5 | 将一个或多个防火墙添加到 Panorama。

更多有关添加防火墙到 Panorama 的信息，请参阅将防火墙作为受管设备添加。

1. 登录到 Panorama Web 界面。
2. 选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要），并 **Add**（添加）防火墙。
3. 输入防火墙的序列号。
4. 如果在所需设备组和模板创建结束后添加防火墙，请启用（勾选） **Associate Devices**（关联设备）以将新防火墙分配到合适的设备组和模板堆栈。
5. 要使用 CSV 添加多个防火墙，请单击 **Import**（导入），并 **Download Sample CSV**（下载样本 **CSV**） 以填充防火墙信息，然后 **Browse**（浏览） 以导入防火墙。
6. 单击 **OK**（确定）。

STEP 6 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置。

STEP 7 | 在打算用于 SD-WAN 部署中的每个防火墙上重复步骤 2 到步骤 5 。

创建 SD-WAN 网络模板

创建一个可包含 SD-WAN 中心和分支中所有网络配置的模板。您必须为您的中心防火墙创建一个单独的模板和模板堆栈，为您的分支防火墙创建一个单独的模板和模板堆栈。最佳做法是限制用于管理您的 SD-WAN 设备配置的模板和模板堆栈数。通过限制所有中心和分支使用的模板和模板堆栈数，可大大降低管理多个 SD-WAN 中心和分支配置的运营开销。使用模板或模板堆栈变量，可帮助降低使用的模板数。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 创建 SD-WAN 中心网络模板。

1. 选择 **Panorama** > **Templates**（模板），然后 **Add**（添加）新模板。
2. 为模板输入描述性 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. 单击 **OK**（确定）保存您的配置更改。

STEP 3 | 创建中心模板堆栈。

1. 选择 **Panorama** > **Templates**（模板），然后单击 **Add Stack**（添加堆栈）以添加新的模板堆栈。
2. 为模板堆栈输入描述性的 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. **Add**（添加）您在步骤 2 中创建的 SD-WAN 网络模板。
5. 在 **Devices**（设备）部分，勾选用于您所有 SD-WAN 中心防火墙的复选框。
6. 单击 **OK**（确定）保存您的配置更改。

STEP 4 | 创建 SD-WAN 分支网络模板。

1. **Add**（添加）新模板。
2. 为模板输入描述性 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. 单击 **OK**（确定）保存您的配置更改。

STEP 5 | 创建分支模板堆栈。

1. 单击 **Add Stack**（添加堆栈）以添加新的模板堆栈。
2. 为模板堆栈输入描述性的 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. **Add**（添加）您在步骤 4 中创建的 SD-WAN 网络模板。
5. 在 **Devices** 部分，勾选用于您所有 SD-WAN 分支防火墙的复选框。
6. 单击 **OK**（确定）保存您的配置更改。

STEP 6 | **Commit**（提交）配置更改。

在 Panorama 中创建预定义区域

SD-WAN 策略规则使用预定义区域实现内部路径选择和日志转发目的。有两种用例；您的用例取决于是在带现有安全策略规则的当前 PAN-OS® 防火墙上启用 SD-WAN，或是开始启动一个不带先前安全策略规则的全新 PAN-OS 部署。如果当前防火墙的安全策略规则已就位，您可以将当前区域映射到使用 SD-WAN 策略的预定义区域。

SD-WAN 引擎利用预定义区域转发流量。此外，通过在 Panorama™ 模板中创建预定义区域，还可在受管防火墙和 Panorama 之间提供一致的可见性：

- **Zone Internet**（从区域到 **Internet**）— 适用于在不可信 Internet 上往来的流量。
- **Zone to Hub**（从区域到中心）— 适用于从分支防火墙到中心防火墙的流量，以及中心防火墙之间的流量。
- **Zone to Branch**（从区域到分支）— 适用于从中心防火墙到分支防火墙的流量，以及分支防火墙之间的流量。

- **Zone Internal**（从区域到内部）— 适用于指定位置的内部流量。

如果未创建预定义区域，*SD-WAN* 插件将自动在您的分支和中心防火墙上创建预定义区域，但是，您无法在 *Panorama* 中看到他们。

主要有两种预定义区域用例：

- **Existing Zones**（现有区域）— 您已拥有创建用于 User-ID™ 或各种策略（安全策略规则、QoS 策略规则、区域保护和数据包缓冲区保护）的预先存在区域。您必须将预先存在区域映射到 SD-WAN 使用的预定义区域，以便防火墙正确转发流量。因为新的预定义区域仅用于 SD-WAN 转发，因此，您应在所有策略中继续使用预先存在区域。您可以通过创建 CSV 文件，在添加 SD-WAN 设备到 Panorama时映射区域。（如果未使用 CSV 文件，您可以在配置 **Panorama** > **SD-WAN** > **Devices**（设备）并将现有区域添加到 **Zone Internet**（从区域到互联网）、**Zone to Hub**（从区域到中心）、**Zone to Branch**（从区域到分支）以及 **Zone Internal**（从区域到内部）时映射区域。）

  映射的结果是，分支或中心防火墙可以查找转发，以确定 SD-WAN 出口接口，进而确定出口区域。如果未将预先存在区域映射到预定义区域，允许会话不会使用 SD-WAN。映射是必须的，原因在于现有客户已拥有不同的区域名称，防火墙必须将所有这些区域名称缩小到预定义区域。您无需将区域映射到所有预定义区域，但至少应将现有区域映射到 **`Zone to Hub`**（从区域到中心）和 **`Zone to Branch`**（从区域到分支）区域。

- **No Existing Zones**（无现有区域）— 您拥有全新部署的 Palo Alto Networks® 防火墙和 SD-WAN。在这种情况下，您没有进行映射的区域；我们建议您使用 PAN-OS 策略和 User-ID 中的预定义区域简化部署。

开始配置您的 SD-WAN 部署之前，对于这两种用例，您将在 Panorama 中创建名为从区域到 **`Internet`**、从区域到内部、从区域到中心、以及从区域到分支的所需预定义区域。在启动分支和中心防火墙时，您将添加 SD-WAN 设备到 Panorama。对于预先存在的客户，SD-WAN 插件在执行 SD-WAN 策略规则、QoS 策略规则、区域保护、User-ID、以及数据包缓冲区保护时，将使用这些预定义区域实现预先存在区域的内部映射，并将在 Panorama 中使用预定义区域实现区域日志记录和可见性操作。对于新客户，您可以使用预定义区域进行正确的设置。

此外，在您将配置从 Panorama 推送到 SD-WAN 受管设备时，还需要使用预定义区域在您的 SD-WAN 中心和分支之间自动建立 VPN 隧道。

区域名称区分大小写，且必须与此过程中提供的名称匹配。如果区域名称与此过程中描述的名称不匹配，则会在防火墙上提交失败。

在此示例中，我们创建的是名为 **`zone-internet`**（从区域到 **`Internet`**）的区域。

STEP 1 | 登录到 Panorama Web 界面。

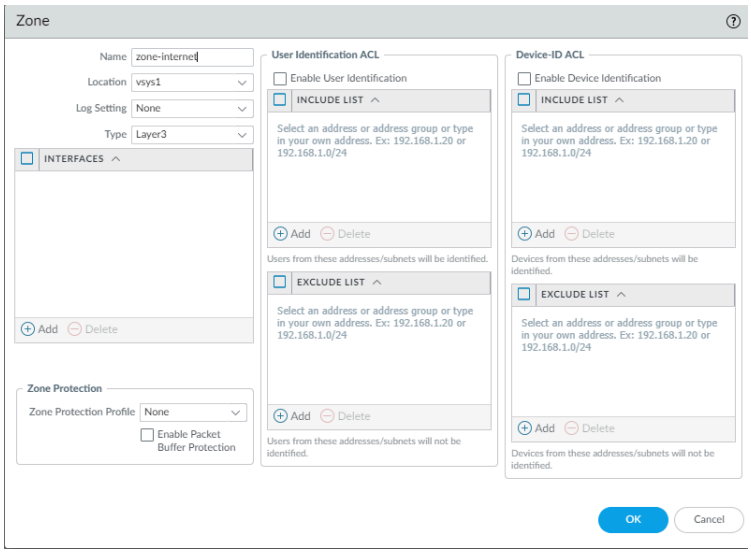
STEP 2 | 选择 **Network**（网络） > **Zones**（区域），然后，从**Template**（模板）上下文下拉列表中，选择您之前创建的网络模板。

STEP 3 | **Add**（添加）新区域。

STEP 4 | 输入 **`zone-internet`**（从区域到 **`Internet`**）等充当区域的 **Name**（名称）。

STEP 5 | 对于 区域 **Type**（类型），请选择 **Layer3**（第 **3** 层）。

STEP 6 | 单击 **OK**（确定）。



STEP 7 | 重复上述步骤以创建剩余区域。您必须创建的区域汇总如下：

- 从区域到分支
- 从区域到中心
- 从区域到内部
- 从区域到 **`Internet`**

STEP 8 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 9 | **Commit**（提交）更改。

创建 SD-WAN 设备组

创建两个包含用于 SD-WAN 中心和分支的所有策略规则和配置对象的设备组（一个用于中心，一个用于分支）。创建用于中心和分支的设备组后，必须在每个设备组中创建一个允许中心和分支区域之间存在流量的安全策略规则。创建这些安全策略规则，以在您创建 VPN 集群后，确保 SD-WAN 插件在创建 VPN 隧道时，允许 SD-WAN 设备区域之间的流量。

在中心防火墙创建相同的配置，在分支防火墙创建相同的配置。这可大大减少必须管理多个 *SD-WAN* 中心和分支配置而出现的运营开销，并允许您更快地排除配置故障，隔离和更新配置问题。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 在 Panorama 中创建预定义区域.

STEP 3 | 创建 SD-WAN 中心设备组。

1. 选择 **Panorama** > **Device Groups**（设备组），然后 **Add**（添加）设备组。
2. 输入 **`SD-WAN_Hub`** 作为设备组 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. 在 **Devices**（设备）部分中，选择复选框以将 SD-WAN 中心分配到组。
5. 对于 **Parent Device Group**（父设备组），请选择 **Shared**（共享）。
6. 单击 **OK**（确定）。

STEP 4 | 创建 SD-WAN 分支设备组。

1. 选择 **Panorama** > **Device Groups**（设备组），然后 **Add**（添加）设备组。
2. 输入 **`SD-WAN_Branch`** 作为设备组 **Name**（名称）。
3. （可选）输入模板的 **Description**（说明）。
4. 在 **Devices**（设备）部分中，选择复选框以将 SD-WAN 分支分配到组。
5. 对于 **Parent Device Group**（父设备组），请选择 **Shared**（共享）。
6. 单击 **OK**（确定）。

STEP 5 | 创建一个用于控制从分支机构前往中心内部区域，以及从中心内部区域前往分支机构的通信流量安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全），然后从 **Device Group**（设备组）上下文下拉列表中，选择 **SD-WAN_Hub** 设备组。
2. **Add**（添加）新策略规则。
3. 输入策略规则 **Name**（名称），例如 **`SD-WAN access--hub DG`**。
4. 选择 **Source**（源） > **Source Zone**（源区域），然后 **Add**（添加）**zone-internal**（从区域到内部）和 **zone-to-branch**（从区域到分支）。
5. 选择 **Destination**（目标） > **Destination Zone**（目标区域），然后 **Add**（添加）**zone-internal**（从区域到内部）和 **zone-to-branch**（从区域到分支）。
6. 选择 **Application**（应用程序），然后 **Add**（添加）允许的应用程序。

   如果使用 *BGP* 路由，必须允许 *BGP*。
7. 选择 **Actions**（操作）和 **Allow**（允许）以允许您选择的应用程序。
8. 选择 **Target**（目标），然后指定 Panorama™ 应推送此规则到其中的目标设备。

STEP 6 | 创建一个用于控制从分支机构内部区域前往中心，以及从中心前往分支机构内部区域的通信流量安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全），然后从 **Device Group**（设备组）上下文下拉列表中，选择 **SD-WAN_Branch** 设备组。
2. **Add**（添加）新策略规则。
3. 输入策略规则 **Name**（名称），例如 **`SD-WAN access--branch DG`**。
4. 选择 **Source**（源） > **Source Zone**（源区域），然后 **Add**（添加）**zone-internal**（从区域到内部）和 **zone-to-hub**（从区域到中心）。
5. 选择 **Destination**（目标） > **Destination Zone**（目标区域），然后 **Add**（添加）**zone-internal**（从区域到内部）和 **zone-to-hub**（从区域到中心）。
6. 选择 **Application**（应用程序），然后 **Add**（添加）允许的应用程序。

   如果使用 *BGP* 路由，必须允许 *BGP*。

7. 选择 **Actions**（操作）和 **Allow**（允许）以允许您选择的应用程序。
8. 选择 **Target**（目标），然后指定 Panorama 应推送此规则到其中的目标设备。

STEP 7 | 提交并推送您的配置。

1. **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。
2. 在推送范围部分，单击 **Edit Selections**（编辑选择）。
3. 启用（勾选）**Include Device and Network Templates**（包括设备和网络模板），然后单击 **OK**（确定）。
4. **Commit and Push**（提交并推送）您的配置更改。

   在您提交并推送设备组和模板配置时，有两种自动执行的提交操作。查看 ***Tasks***（任务）以验证第二次提交是否成功。就这两次提交操作而言，第一次提交始终会失败。

创建链路标记

创建一个链路标记，以标识在 SD-WAN 流量分发和故障转移保护期间，让应用程序和服务以特定顺序使用的一个或多个物理链路。在物理链路运行状况出现问题时，通过对多个物理链路的分组，您可以提高应用程序和服务的质量。

在计划链路分组方式时，请考虑链路的使用或用途，然后对其进行相应地分组。例如，如果配置的链路专用于低成本或非业务关键型流量，请创建链路标记，并对这些接口进行分组，确保预期流量主要在这些链路上流动，而不是在可能会影响关键业务应用程序或服务的昂贵链路上流动。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Object**（对象） > **Tags**（标记），然后从 **Device Group**（设备组）上下文下拉列表中选择合适的设备组。

STEP 3 | **Add**（添加）新标记。

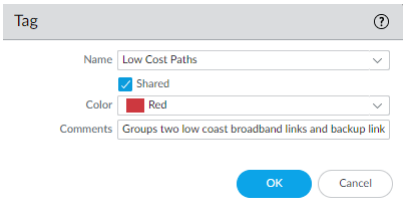
STEP 4 | 为标记输入描述性的 **Name**（名称）。例如，低成本路径、昂贵路径、常规访问、私有 HQ 或备份。

STEP 5 | 启用（勾选）**Shared**（共享），这样，Panorama™ 管理服务器上的所有设备组、单一 vsys 中心或分支上的默认 vsys，以及您作为推送对象的任何多 vsys 中心或分支上的 vsys1 都能使用链路标记。

通过配置共享链路标记，Panorama 可以引用防火墙配置验证中的链路标记，成功将配置提交并推送到分支和中心。如果 Panorama 无法引用链路标记，则提交失败。

STEP 6 | （可选）选择标记的 **Color**（颜色）。

STEP 7 | 输入标记相关的有用 **Comments**（注释）。例如，对两个低成本宽带链路和一个备份链路进行分组，实现对 **`Internet`** 的常规访问。



STEP 8 | 单击 **OK**（确定）保存您的配置更改。

STEP 9 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 10 | 配置 SD-WAN 接口配置文件.

配置 SD-WAN 接口配置文件

创建 SD-WAN 接口配置文件，以定义 ISP 连接特征，指定链路速度以及防火墙监控链路的频率，并指定用于此链路的链路标记。一旦为多个链路指定相同的链路标记后，就可以将这些物理链路分组（捆绑）到链路包或粗管中。必须先配置 SD-WAN 接口配置文件，并将其指定用于启用了 SD-WAN 功能的以太网接口，然后才能保存以太网接口。

根据通用标准对链路进行分组。例如，按路径偏好（从最喜欢到最不喜欢）对链路分组，或是按成本对链路分组。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Network**（网络） > **Network Profiles**（网路配置文件） > **SD-WAN Interface Profile**（**SD-WAN** 接口配置文件），然后从 **Template**（模板）上下文下拉列表中选择合适的模板。

STEP 3 | **Add**（添加） SD-WAN 接口配置文件。

STEP 4 | 输入用于 SD-WAN 接口配置文件的用户友好型 **Name**（名称） 。您将在报告、故障排除和统计信息中看到此名称。

STEP 5 | 如果拥有多个 vsys Panorama™ 管理服务器，请选择 vsys **Location**（位置）。默认选择 vsys1。

STEP 6 | 选择此配置文件将分配给接口的 **Link Tag**（链路标记）。

STEP 7 | 添加配置文件的 **Description**（说明）。

STEP 8 | 从预定义列表中选择物理 **Link Type**（链路类型）（**ADSL/DSL**、 **Cable modem**（光缆调制解调器）、**Ethernet**（以太网）、**Fiber**（光纤）、 **LTE/3G/4G/5G**、**MPLS**、 **Microwave/Radio**（微波/无线电）、 **Satellite**（卫星）、 **WiFi**或 **Other**（其他））。防火墙支持实现防

火墙以太网连接和移交的任何 CPE 设备，例如， WiFi 接入点、LTE 调制解调器、激光/微波 CPE 等都可通过以太网移交实现。

点对点专有链路类型（*MPLS*、卫星、微波等）形成的隧道仅具有一种链路类型；例如，*MPLS* 到 *MPLS*，卫星到卫星等。例如，*MPLS* 链路和以太网链路之间不会创建隧道。

对于在将用于支持 *PAN-OS SD-WAN* 的接口上定义区域的现有 *PAN-OS* 部署，*Panorama* 可能会在以下条件下自动将接口的区域名称配置为预定义的 *SD-WAN* 区域之一：

1. *SD-WAN* 接口在其接口配置文件中配置为点对点专用链路类型（***MPLS***、***Satellite***（卫星）或 ***Microwave***（微波））。
2. 已在 *SD-WAN* 接口配置文件上禁用 ***VPN Data Tunnel Support***（***VPN*** 数据隧道支持）复选框（未选中）。这指示 *PAN-OS* 在 *SD-WAN VPN* 隧道之外以明文形式转发流量。

在中心防火墙上，当满足条件 a) 时，区域名称配置为 `zone-to-branch`。在分支防火墙上，当同时满足条件 a) 和条件 b) 时，区域名称配置为 `zone-to-hub`。Panorama 将自动执行此步骤以简化配置，从而确保中心和分支防火墙之间正确通信。如果预先存在的防火墙策略引用旧区域名称，则必须更新策略以反映新的预定义 SD-WAN 区域名称。

STEP 9 | 指定源自 ISP 的 **Maximum Download (Mbps)**（最大下载 **(Mbps)**） 速度，以兆比特/秒为单位（范围为 0-100,000；没有默认值）。最多可以使用三位小数来输入一个范围，例如 10.456。询问 ISP 以获取链路速度，或使用 speedtest.net 等工具采样链路的最大速度，并取很长一段时间内的平均最大值。

STEP 10 | 指定发往 ISP 的 **Maximum Upload (Mbps)**（最大上传 **(Mbps)**）速度，以兆比特/秒为单位（范围为 0-100,000；没有默认值）。最多可以使用三位小数来输入一个范围，例如 10.456。询问 ISP 以获取链路速度，或使用 speedtest.net 等工具采样链路的最大速度，并取很长一段时间内的平均最大值。

STEP 11 | 选择 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件），为接口启用转发纠错 (FEC) 或数据包重复。您必须在编码和解码防火墙上都启用此功能；还必须创建纠错配置文件，以应用于特定应用程序的 SD-WAN 策略规则。

STEP 12 | **VPN Data Tunnel Support**（**VPN** 数据隧道支持）确定从分支到中心的流量以及返回流量是通过 VPN 隧道来增加安全性（默认方法），还是在 VPN 隧道外流动以避免加密开销。

- 对具有 Internet 直接连接或 Internet 中断功能的公共链路类型启用 **VPN Data Tunnel Support**（**VPN** 数据隧道支持），例如，电缆调制解调器、ADSL 等其他 Internet 连接。
- 您可以对不具有互联网中断功能的 MPLS、卫星或微波等私有链路类型禁用**VPN Data Tunnel Support**（**VPN** 数据隧道支持）。但是，您必须先确定此流量不会因为从 VPN 隧道外发送而被拦截。
- 分支可能拥有需要故障转移到与中心连接的私有 MPLS 链路的 DIA 隧道，然后从中心连接 Internet。**VPN Data Tunnel Support**（**VPN** 数据隧道支持）设置确定私有数据是否经 VPN 隧道流出，或是从此隧道外流过，以及故障转移流量是否使用私有数据流不会使用的其他连接。防火墙使用区域对源自 MPLS 私有流量的 DIA 故障转移流量进行分段。

STEP 13 | 如果您配置 DIA AnyPath，则一个主体虚拟接口可以有多个中心虚拟接口，因此必须确定为故障转移选择特定中心的优先顺序。通过为捆绑在应用此配置文件的中心虚拟接口中的 VPN 隧道设置 **VPN Failover Metric**（**VPN** 故障转移指标）来指定此优先级。指标越低，故障转移期间要选择的接口优先级就越高。如果多个中心虚拟接口中具有相同的指标值，SD-WAN 将以循环方式向它们发送新的会话流量。

STEP 14 | （可选）选择防火墙可在其中监控应用此 SD-WAN 接口配置文件的接口的 **Path Monitoring**（路径监控）模式。

防火墙根据 ***Link Type***（链路类型）选择其认为的最佳监控方法。除非应用此配置文件的接口出现的问题需要采取更积极或更宽松的路径监控，否则不得更改默认设置。

- **Aggressive**（积极的）— （默认适用于除 LTE 和卫星之外的所有链路类型）防火墙以固定的频率将探测数据包发送到 SD-WAN 链路的另一端。如果您需要针对供电不足和停电情况进行更快的检测和故障转移，请使用此模式。
- **Relaxed**（宽松的）— （默认适用于 LTE 和卫星链路类型）防火墙发送探测数据包集之间会安排几秒钟的间歇时间（**Probe Idle Time**（探测空闲时间）），从而降低路径控制的频率。探测空闲时间结束后，防火墙根据配置的 **Probe Frequency**（探测频率）发送七秒钟的探测。如果您使用的是低带宽链路、您的链路按使用情况收费（例如，LTE），或是在快速检测不如节省成本和带宽重要时，可以使用此模式。

STEP 15 | 设置 **Probe Frequency (per second)**（探测频率（每秒）），即防火墙在一秒内发送探测数据包到 SD-WAN 链路另一端的次数（范围为 1-5；默认为 5）。默认设置可提供亚秒级的供电不足和停电情况检测。

如果更改 *Panorama* 模板的探测频率，还需调整 *Panorama* 设备组的路径质量配置文件中的 ***Packet Loss***（数据包丢失）百分比阈值。

STEP 16 | 如果选择 **Relaxed**（宽松的）路径监控，还可以设置防火墙在发送探测数据包集之间需要等待的 **Probe Idle Time (seconds)**（探测空闲时间（秒））（范围为 1-60；默认为 60）。

STEP 17 | 在链路执行故障转移后将此链路恢复为首选链路之前，输入防火墙等待链路恢复以保持合格的 **Failback Hold Time (seconds)**（故障恢复保持时间（秒））（范围为 20-120；默认值为 120）。

STEP 18 | 单击 **OK**（确定）保存配置文件。

STEP 19 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 20 | 监控您的应用程序和链路路径运行状况指标，并生成应用程序和链路运行状况性能报告。有关详细信息，请参阅监控和报告。

配置 SD-WAN 物理以太网接口

在 Panorama™ 中，配置以太网第 3 层物理接口，并启用 SD-WAN 功能。要配置物理接口，必须为其分配一个 IPv4 地址和一个完全合格的下一个跃点网关，并将 SD-WAN Interface Profile（SD-WAN 接口配置文件）分配给此接口。（SD-WAN 仅支持第 3 层接口类型；它不支持第 2 层网络，如 VPLS。）

使用 Panorama 创建 VPN 集群，并在 CSV 中导出中心和分支信息后，SD-WAN 插件中的自动 VPN 配置将使用此信息为相关的分支和中心生成一个配置，该配置包含预定义 SD-WAN 区域，并能在 SD-WAN 分支和中心之间创建安全的 VPN 隧道。此外，如果您在添加 SD-WAN 分支或中心时在 CSV 或 Panorama 中输入 BGP 信息，自动 VPN 配置还能生成 BGP 配置。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），从 **Template**（模板）上下文下拉列表中选择适当的模板，并选择插槽编号（例如，Slot1），然后选择接口（例如，ethernet1/1）。

STEP 3 | 选择 **Interface Type**（接口类型）为 **Layer3**。

STEP 4 | 对于旧版引擎，选择 **Virtual Router**（虚拟路由器）或新建一个虚拟路由器。对于高级路由引擎，选择一个 **Logical Router**（逻辑路由器）或新建一个逻辑路由器。

STEP 5 | 分配一个适用于您配置的接口的 **Security Zone**（安全区域）。

例如，如果配置的是 ISP 上行链路，就必须知道选中的以太网接口将进入不可信区域。

STEP 6 | 在 **IPv4** 选项卡中，**Enable SD-WAN**（启用 **SD-WAN**）。

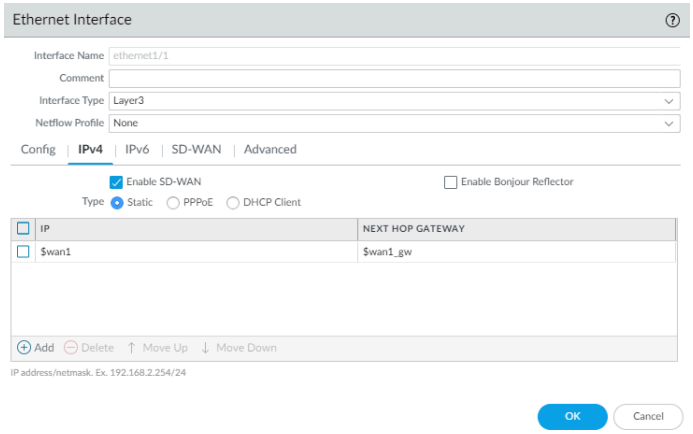
STEP 7 | 选择地址 **Type**（类型）：

- **Static**（静态）— 在 **IP** 字段中， **Add**（添加）此接口的 IPv4 地址和前缀长度。您可以将定义变量（例如，$uplink）与一系列地址一起使用。输入完全合格的 **Next Hop Gateway**（下一个跃点网关）的 IPv4 地址（您刚刚输入的 IPv4 地址的下一个跃点）。下一个跃点网关必须与 IPv4 地址处于同一子网中。下一个跃点网关是 ISP 在您购买服务时为您分配的 ISP 默认路由器的 IP 地址。也是防火墙发送流量以进入 ISP 网络，最终进入 Internet 和中心的下一个跃点 IP 地址。
- **PPPoE** — 为 DSL 链路 **Enable**（启用）PPPoE 身份验证，输入 **Username**（用户名）和 **Password**（密码），并 **Confirm Password**（确认密码）。

- **DHCP Client**（**DHCP** 客户端）— 重要的是 DHCP 必须为 ISP 连接分配一个默认网关，也称为下一个跃点网关。ISP 将提供动态 IP 地址、DNS 服务器和默认网关等所需的全部连接信息。

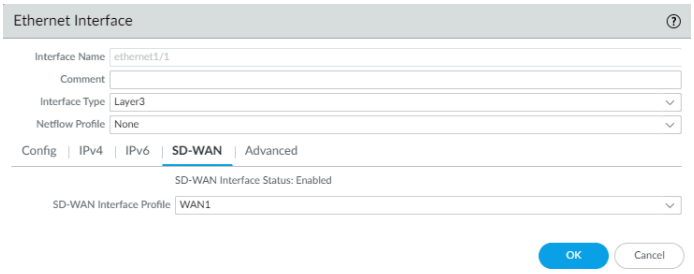
尽管中心或分支接口均支持 *DHCP* 客户端，但在中心接口上，您最好分配 ***Static***（静态）地址而不是 *DHCP* 客户端。需要 *Palo Alto Networks DDNS* 服务才能在中心上使用 *DHCP*。在中心站点使用静态地址可以创建更稳定的环境，因为解析 *DHCP IP* 地址变化不涉及 *DDNS*，并且如果 *DDNS* 服务变化，那么该服务可能需要几分钟时间来注册新 *IP* 地址。如果您有多个分支站点连接到中心站点，那么稳定性对于保持网络正常运行至关重要。

如果选择 *DHCP* 客户端，请务必禁用选项 ***Automatically create default route pointing to default gateway provided by server***（自动创建指向服务器所提供的默认网关的默认路由），该选项在默认情况下启用。



STEP 8 | 在 **SD-WAN** 选项卡上，选择您已创建的 **SD-WAN Interface Profile**（**SD-WAN** 接口配置文件）（或新建一个 SD-WAN 接口配置文件）以应用至此接口。SD-WAN 接口配置文件具有关联的链路标记，因此，应用此配置文件的接口将拥有一个相关的链路标记。一个接口只能有一个链路标记。

STEP 9 | 单击 **OK**（确定）以保存以太网接口。

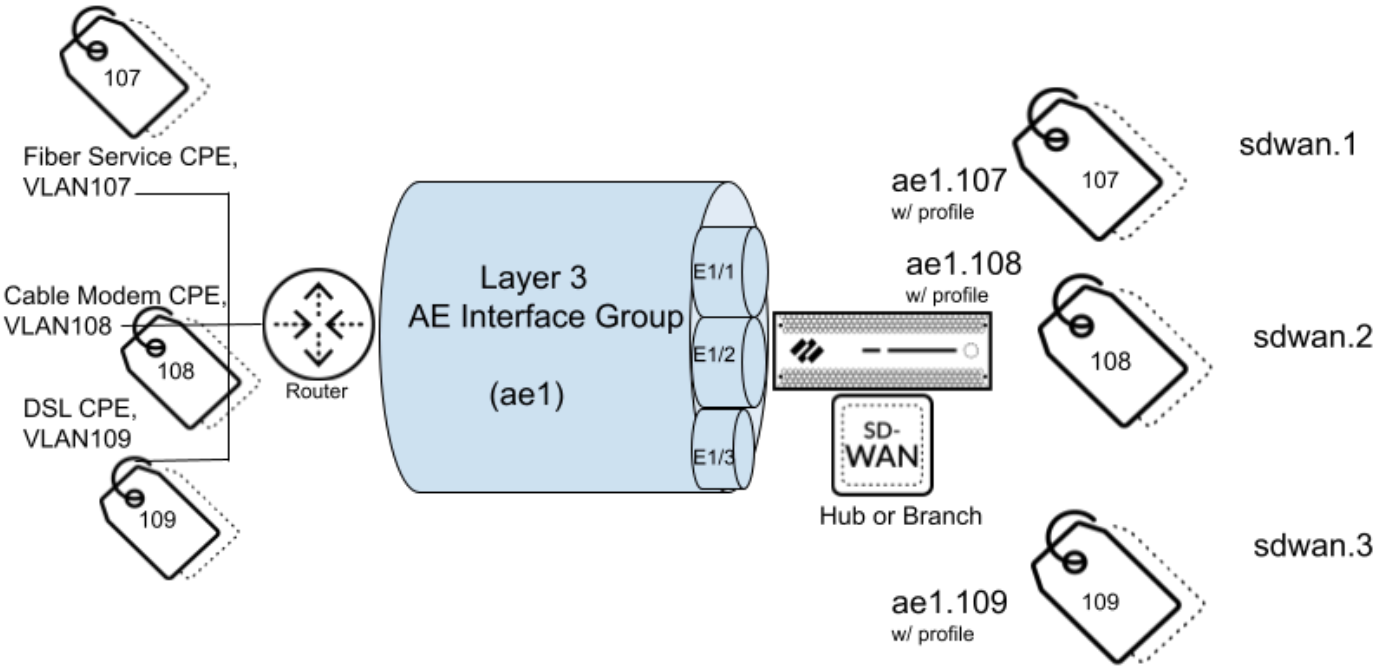


STEP 10 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 11 | （仅限 SD-WAN 手动配置）配置 SD-WAN 虚拟接口。如果使用自动 VPN，此任务将由自动 VPN 配置执行。

为 SD-WAN 配置聚合以太网接口和子接口

运行 PAN-OS 11.0 和 SD-WAN 插件 2.1.0 的物理防火墙支持聚合以太网 (AE) 接口上的 SD-WAN，以便数据中心中的 SD-WAN 防火墙等可以具有提供链路冗余的物理以太网接口的聚合接口组（捆绑）。SD-WAN 支持 AE 接口（不论是否带子接口）。您可以创建带子接口的 AE 接口，且可以针对不同的 ISP 服务对子接口进行标记，以提供端到端的流量分段。因此，您的 ISP 服务可以到达多个实验室或建筑物，而无需针对每个连接配备一对专用光纤。第 3 层 AE 接口组与路由器相连，如下图所示：



VM 系列防火墙不支持 *AE* 接口。具有 *AE* 接口的 *SD-WAN* 中心或分支防火墙不应与 *VM* 系列 *SD-WAN* 中心或分支防火墙属于同一 *VPN* 集群，因为 *VM* 系列防火墙不支持 *AE* 接口。

子接口上不支持 *PPPoE*。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 针对 AE 接口组中的每个 ISP 连接（子接口）配置 SD-WAN 接口配置文件以定义其链路属性。

STEP 3 | 创建 AE 接口组。

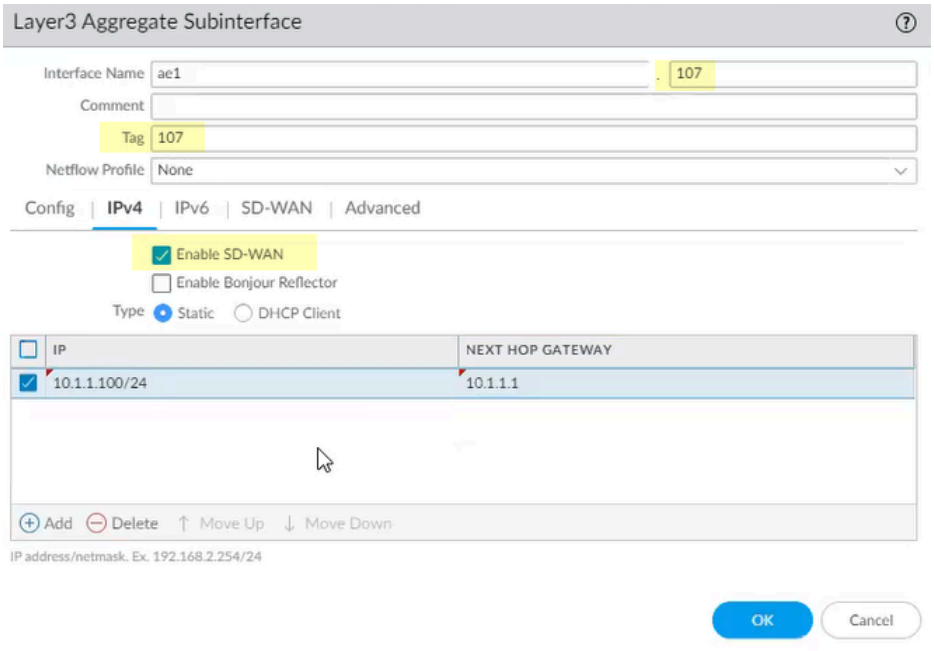
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），选择 Panorama **Template**（模板），然后 **Add Aggregate Group**（添加聚合组）。
2. 对于 **Interface Name**（接口名称），请输入标识聚合组的数字；范围为 1 至 16。
3. 对于 **Interface Type**（接口类型），请选择 **Layer3**（第 **3** 层）。
4. 单击 **OK**（确定）。

STEP 4 | 将物理接口分配给聚合组。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择要分配给聚合组的接口。
2. 针对 **Interface Type**（接口类型）选择 **Aggregate Ethernet**（聚合以太网）。
3. 选择您创建的 **Aggregate Group**（聚合组）；例如，ae1。
4. 在 **Advanced**（高级）选项卡中，选择 **Link Speed**（链路速度）、**Link Duplex**（链路双工）和 **Link State**（链路状态）。
5. 单击 **OK**（确定）。
6. 对要分配给聚合组的每个接口重复此步骤。

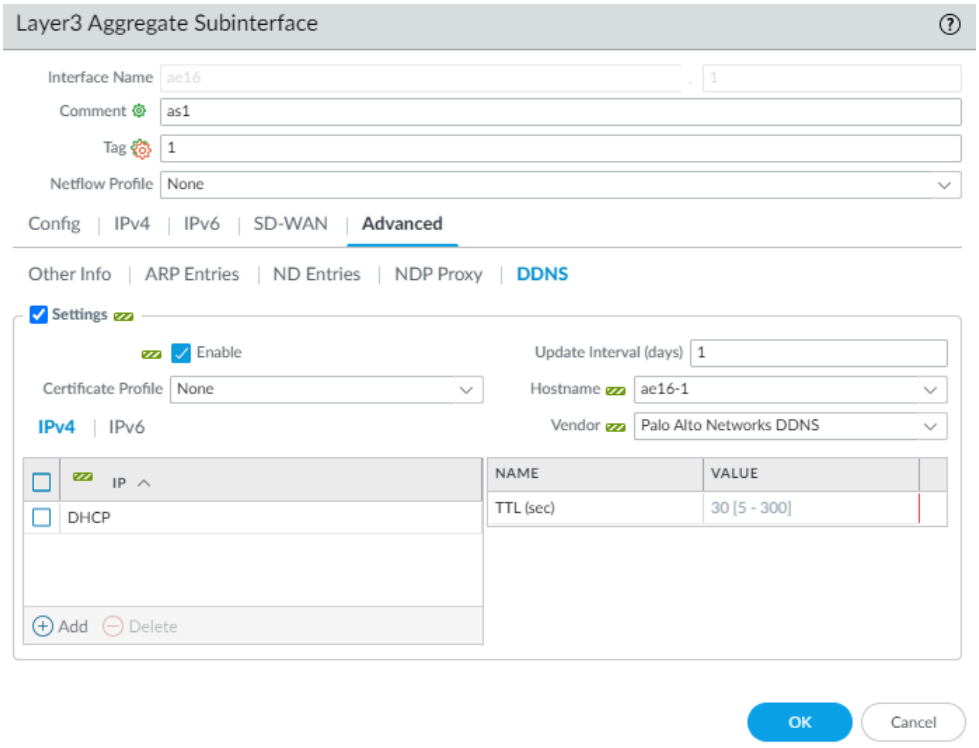
STEP 5 | 对于聚合组，创建一个使用静态 IP 地址的子接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），突出显示聚合接口，例如 ae1，然后单击屏幕底部的 **Add Subinterface**（添加子接口）。
2. 对于 **Interface Name**（接口名称），在句点后输入一个数字，例如 107。
3. 输入 VLAN **Tag**（标记）以区分子接口。为了便于使用，将该标记与子接口 ID 保持一致。
4. 选择 **IPv4** 选项卡并 **Enable SD-WAN**（启用 **SD-WAN**）。
5. 选择地址 **Type**（类型）：**Static**（静态）。
6. **Add**（添加）子接口的 **IP** 地址（和子网掩码）。
7. 输入 **Next Hop Gateway**（下一个跃点网关）的 IP 地址。
8. 单击 **OK**（确定）。



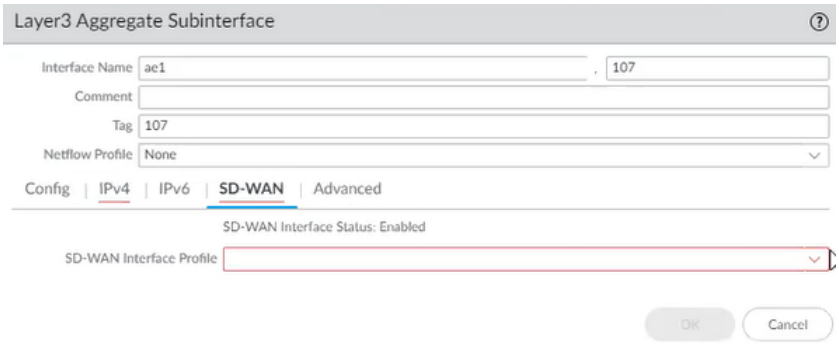
STEP 6 | 或者，对于聚合组，创建一个使用 DHCP 获取其地址的子接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后在 **Template**（模板）字段中选择模板堆栈。
2. 突出显示聚合接口，例如 ae1，然后单击屏幕底部的 **Add Subinterface**（添加子接口）。
3. 突出显示该子接口并单击屏幕底部的 **Override**（覆盖）。
4. 突出显示子接口，对于 **Interface Name**（接口名称），在句点后输入一个数字，例如 1。
5. 输入 VLAN **Tag**（标记）以区分子接口。为了便于使用，将该标记与子接口 ID 保持一致。
6. 选择 **IPv4** 选项卡并 **Enable SD-WAN**（启用 **SD-WAN**）。
7. 选择地址 **Type**（类型）：**DHCP** 客户端。
8. 选择 **Enable**（启用）。
9. 取消勾选（不选择）**Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）。
10. 选择 **Advanced**（高级）选项卡和 **DDNS** 选项卡。
11. 选择 **Settings**（设置），然后选择 **Enable**（启用）。**Hostname**（主机名）由 Panorama SD-WAN 插件自动生成。
12. 针对 **Vendor**（供应商）选择 **Palo Alto Networks DDNS**。
13. 单击 **OK**（确定）。



STEP 7 | 将 SD-WAN 接口配置文件应用于子接口。

1. 突出显示您创建的子接口并选择 **SD-WAN** 选项卡。
2. 选择您为此链路创建的 **SD-WAN Interface Profile**（**SD-WAN** 接口配置文件）或创建新的配置文件。



3. 单击 **OK**（确定）。

STEP 8 | 重复前面的步骤，为聚合接口组创建额外的第 3 层子接口，并将 SD-WAN 接口配置文件应用于每个子接口。

STEP 9 | **Commit**（提交）。

为 SD-WAN 配置第 3 层子接口

运行 PAN-OS 11.0 和 SD-WAN 插件 2.1.0 的防火墙在第 3 层子接口上支持 SD-WAN，以便防火墙可以使用 VLAN 标记对流量进行分段。以下任务展示了如何创建使用静态 IP 地址的第 3 层子接口，以及如何创建使用 DHCP 获取其地址的子接口。其中介绍了如何将 VLAN 标记分配给子接口并在子接口上启用 SD-WAN。创建 SD-WAN 接口配置文件以定义每个 ISP 连接，并将配置文件分配给相应的子接口（虚拟 SD-WAN 接口）。

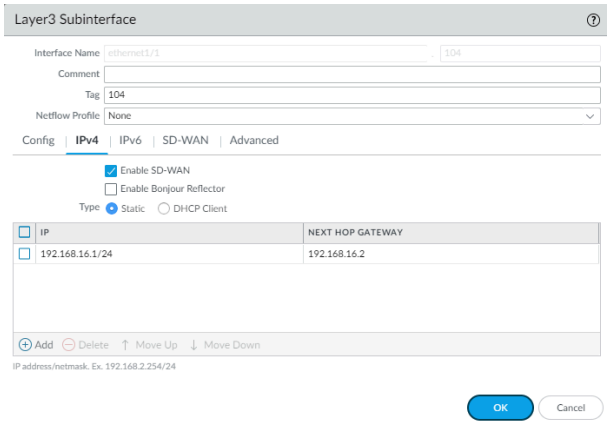
如果在 *VM* 系列防火墙上配置 *SD-WAN* 第 *3* 层子接口，则 *VMware* 配置必须将相应的端口组连接到允许所有 *VLAN* 的接口。

子接口上不支持 *PPPoE*。

STEP 1 | 针对每个 ISP 连接（子接口）配置 SD-WAN 接口配置文件以定义其链路属性。

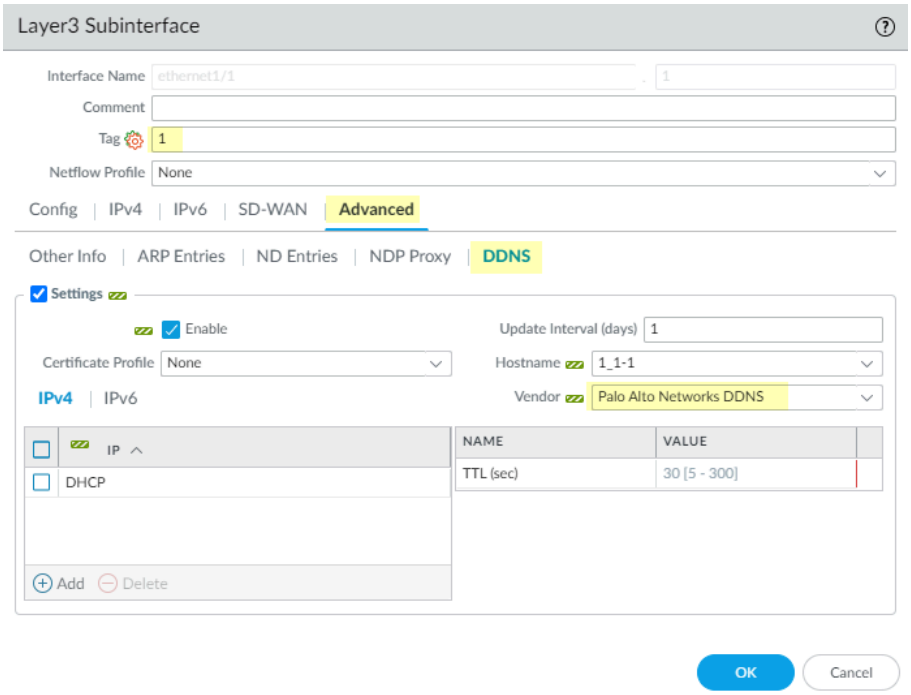
STEP 2 | 创建一个使用静态 IP 地址的第 3 层子接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后在 **Template**（模板）字段中选择一个模板。
2. 选择一个接口。
3. 对于 **Interface Type**（接口类型），请选择 **Layer3**（第 **3** 层）并单击 **OK**（确定）。
4. 突出显示该接口，然后单击屏幕底部的 **Add Subinterface**（添加子接口）。
5. 在 **Interface Name**（接口名称）和句点之后，输入子接口编号。
6. 输入子接口的 **Tag**（标记）（范围为 1 至 4,094）。为了便于使用，将该标记与子接口 ID 保持一致。
7. 在 **IPv4** 选项卡中，**Enable SD-WAN**（启用 **SD-WAN**）。
8. 选择地址 **Type**（类型）：**Static**（静态）。
9. **Add**（添加）**IP** 地址和子网掩码。
10. 输入 **Next Hop Gateway**（下一个跃点网关）的 IP 地址。
11. 单击 **OK**（确定）。



STEP 3 | 或者，创建一个使用 DHCP 获取其地址的第 3 层子接口。

1. 选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后在 **Template**（模板）字段中选择模板堆栈（而非模板）。
2. 选择一个接口。
3. 对于 **Interface Type**（接口类型），请选择 **Layer3**（第 **3** 层）并单击 **OK**（确定）。
4. 突出显示该接口，然后单击屏幕底部的 **Add Subinterfaces**（添加子接口）。
5. 突出显示该子接口并单击 **Override**（覆盖）。
6. 突出显示该子接口，并在 **Interface Name**（接口名称）和句点之后输入子接口编号。
7. 输入子接口的 **Tag**（标记）（范围为 1 至 4,094）。为了便于使用，将该标记与子接口 ID 保持一致。
8. 在 **IPv4** 选项卡中，**Enable SD-WAN**（启用 **SD-WAN**）。
9. 选择地址 **Type**（类型）：**DHCP Client**（**DHCP** 客户端）和 **Enable**（启用）。
10. 取消勾选（不选择）**Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器所提供的默认网关的默认路由）。
11. 依次选择 **Advanced**（高级）选项卡和 **DDNS** 选项卡。
12. 选择 **Settings**（设置），然后选择 **Enable**（启用）。**Hostname**（主机名）由 Panorama SD-WAN 插件自动生成。
13. 针对 **Vendor**（供应商）选择 **Palo Alto Networks DDNS**。
14. 单击 **OK**（确定）。



STEP 4 | 将 SD-WAN 接口配置文件应用于子接口。

1. 突出显示您创建的子接口并选择 **SD-WAN** 选项卡。
2. 选择您为此链路创建的 **SD-WAN Interface Profile**（**SD-WAN** 接口配置文件）或创建新的配置文件。
3. 单击 **OK**（确定）。

STEP 5 | 重复前面的步骤，将更多子接口添加到接口。

STEP 6 | **Commit**（提交）。

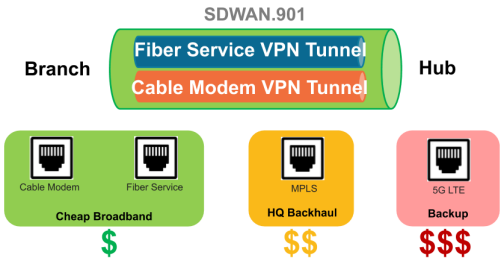
配置 SD-WAN 虚拟接口

如果在 Panorama 中使用自动 VPN 配置，则可以为您创建 SD-WAN 接口，在这种情况下，您无需创建和配置 SD-WAN 虚拟接口。

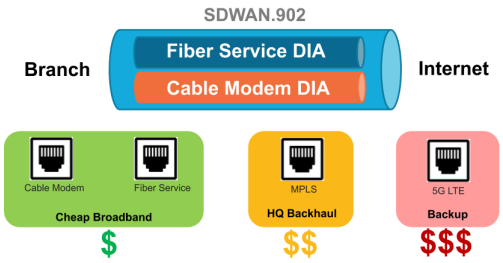
如果未将自动 VPN 配置用于 Panorama，请创建和配置一个 SD-WAN 虚拟接口，以指定一个或多个到达特定中心或互联网等同一目的地并支持 SD-WAN 功能的以太网物理接口。事实上，SD-WAN 虚拟接口中的所有链路类型必须相同，包括所有 VPN 隧道链路或所有互联网直接接入 (DIA) 链路。

在第一幅图中，给出的是名为 SDWAN.1 的 SD-WAN 接口示例。该接口捆绑了两个使用不同运营商的物理接口：Ethernet1/1（电缆调制解调器链路）和 Ethernet1/2 （光纤服务链路）。两个链路都是从分支到中心的 VPN 隧道。

在此图中，*SD-WAN* 接口中的这两个链路碰巧都使用相同的链路标记（廉价宽带），但是，*SD-WAN* 接口中的链路可以具有不同的链路标记。



在下图中，SDWAN.2 将 Ethernet1/1 和 Ethernet1/2 链路捆绑在一起，这两个都是从分支到 Internet 的 DIA 链路：



STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Network**（网络） > **Interfaces**（接口） > **SD-WAN**，然后从 **Template**（模板） 上下文下拉列表中选择合适的模板。

STEP 3 | 通过在 **sdwan.** 前缀后方输入从 1 到 9,999 其中一个数字，**add**（添加） 一个 SD-WAN 逻辑接口。

自动 *VPN* 配置创建的 *SD-WAN* 接口编号为 *.901*、*.902* 等，因此，请不要使用这些数字。

STEP 4 | 输入描述性 **Comment**（注释）。

添加有用的注释，例如，在分支模板上时，请添加从分支到 ***Internet*** 或从分支到美国西部中心。通过您的注释，可使故障排除更加容易，无需尝试解密日志和报告中自动生成的名称。

STEP 5 | 在 **Config**（配置）选项卡上，将 SD-WAN 接口分配给 **Virtual Router**（虚拟路由器）。

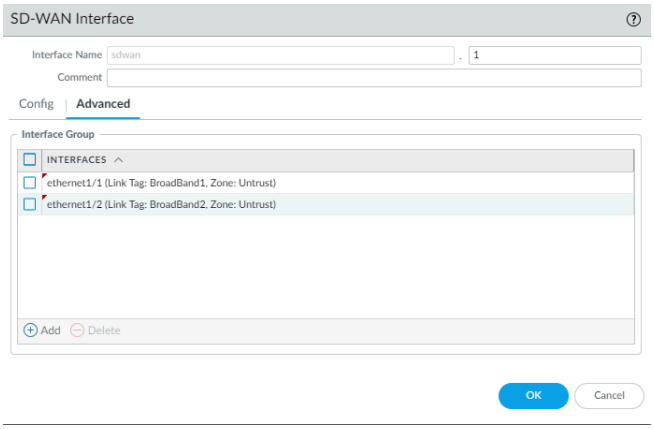
STEP 6 | 将 SD-WAN 接口分配到 **Security Zone**（安全区域）。

SD-WAN 虚拟接口及其所有接口成员均必须处于同一安全区域，确保从分支到同一目的地的所有路径均使用相同的安全策略规则。

STEP 7 | 在 **Advanced**（高级）选项卡上，通过选择一个或多个第 3 层以太网接口（用于 DIA）或多个 VPN 隧道虚拟接口（用于中心），**Add**（添加） 其成员前往同一目的地的 **Interfaces**（接口）。如果输入多个接口，这些接口的类型必须一致（VPN 隧道或 DIA）。

防火墙虚拟路由器通过此 *SD-WAN* 虚拟接口将 *SD-WAN* 流量路由到 *DIA* 或中心位置。路由时，路由表根据数据包中的目标 *IP* 地址，确定数据包将从其退出的 *SD-WAN* 虚拟接口（出口接口）。然后，与数据包匹配的 *SD-WAN* 策略规则中的 *SD-WAN* 路径运行状况和流量分发配置文件将决定使用的路径（以及路径出现问题时考虑使用的新路径顺序）。

STEP 8 | 单击 **OK**（确定）保存您的配置更改。



STEP 9 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

创建 SD-WAN 接口默认路由

如果您通过服务路由访问 Panorama™，若要启动防火墙，必须创建一个指向您创建的 SD-WAN 接口的默认路由。

自动 VPN 创建一个名为 sdwan.901 的 SD-WAN 虚拟接口用于 DIA，并创建一个名为 sdwan.902 的 SD-WAN 虚拟接口用于 VPN 隧道。自动 VPN 还会为自己创建一个默认路由，其使用 sdwan.901 接口充当出口接口，并使用较低的指标。这样，sdwan.901 接口成为您创建的默认路由上的首选接口。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择您正在使用的 **Template**（模板）。

STEP 3 | 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），例如**sd-wan**。

STEP 4 | 选择 **Static Routes**（静态路由），然后按 **Name**（名称） **Add**（添加）静态路由。

STEP 5 | 对于 **Destination** （目标），请输入 0.0.0.0/0。

STEP 6 | 对于出口 **Interface**（接口），请选择您创建的其中一个 SD-WAN 逻辑接口以启动防火墙，如 sdwan.1。

> 您选择的出口接口可以是除 *sdwan.901* 或 *sdwan.902* 以外的任何 *SD-WAN* 逻辑接口。

STEP 7 | 对于 **Next Hop**（下一个跃点），请选择 **None**（无）。

STEP 8 | 对于 **Metric**（指标），请输入一个大于 50 的值，这样，此默认路由将不再优先于自动 VPN 使用低指标创建的默认路由。

STEP 9 | 单击 **OK**（确定）。

STEP 10 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 11 | **Commit**（提交）更改。

STEP 12 | 对防火墙上使用服务路由访问 Panorama 的其他模板重复此任务。

配置 SD-WAN 链路管理配置文件

创建并配置路径质量、SaaS 质量、流量分配和纠错配置文件以管理 SD-WAN 链路故障转移。

- 创建路径质量配置文件
- 配置 SaaS 监控
- SD-WAN 流量分发配置文件
- 创建流量分发配置文件
- 创建纠错配置文件

创建路径质量配置文件

根据延迟、抖动和数据包丢失百分比，为具有独特网络质量（运行状况）要求的关键业务和延迟敏感型应用程序集、应用程序筛选器、应用程序组、服务、服务对象和服务组对象创建路径质量配置文件。应用程序和服务可以共享路径质量配置文件。指定每个参数的最大阈值，若超过此阈值，防火墙会认为路径已出现问题，需要选择一条更好的路径。

作为创建路径质量配置文件的替代方法，您可以使用 **general-business**、 **voip-video**、**file-sharing**、**audio-streaming**、 **photo-video** 和 **remote-access** 等任何预定义路径质量配置文件。预定义配置文件可以按配置文件名称，优化建议的应用程序和服务类型延迟、抖动和数据包丢失阈值。

用于 *Panorama* 设备组的预定义路径质量配置文件基于 *Panorama* 模板的 *SD-WAN* 接口配置文件默认***Probe Frequency***（探测频率）设置。如果更改默认探测频率设置，则必须调整用于设备组中会在更改接口配置文件时，受到 *Panorama* 模板影响的防火墙的路径质量配置文件 ***Packet Loss***（数据包丢失）百分比阈值。

防火墙将延迟、抖动和数据包丢失阈值用作 OR 条件，意思就是说，一旦超过其中一个阈值，防火墙就会选择新的最佳（首选）路径。其延迟、抖动和数据包丢失小于等于所有三个阈值的路径都被视为合格的，防火墙将根据关联的流量分发配置文件选择路径。

默认情况下，防火墙每 200ms 测量 **latency**（延迟）和 **jitter**（抖动）一次，取最后三个测量值的平均值，从而衡量滑动窗口中的路径质量。您可以通过在配置 SD-WAN 接口配置文件时选择积极的或宽松的路径监视来修改这一行为。

如果路径因超过配置的 **packet loss**（数据包丢失）阈值而执行故障转移，则防火墙仍会在故障路径上发送探测数据包，并在路径恢复时计算其数据包丢失百分比。恢复路径上的丢包百分比需要约三分钟才能下降到路径质量配置文件中配置的丢包阈值以下。例如，假定应用程序的 SD-WAN 策略规则有一个将数据包丢失阈值指定为 1% 的路径质量配置文件，以及一个在列表中将自上而下分发配置文件先指定为标记 1（适用于 tunnel.1），然后指定为标记 2（适用于 tunnel.2）的流量分发配置文件。一旦 tunnel.1 超过数据包丢失阈值 1%，数据包将故障转移到 tunnel.2。tunnel.1 的数据包丢失百分比为 0% 时（基于探测数据包），可能最多需要三分钟的时间让监控的 tunnel.1 的数据包丢失率下降至 1% 以下，此时防火墙再次选择 tunnel.1 作为最佳路径。

敏感性设置指示对于应用配置文件的应用程序而言，延迟、抖动或数据包丢失这些参数，哪一个更重要（是首选）。防火墙评估链路质量时，应先考虑带 **high**（高）设置的参数。例如，在防火

墙对两个链路进行比较时，假定一个链路的延迟为 100ms，抖动为 20ms；另一个链路的延迟为 300ms，抖动为 10ms。如果延迟的敏感性为高，则防火墙选择第一个链路。如果抖动的敏感性为高，则防火墙选择第二个链路。如果参数的敏感性相同（参数默认设为 **medium**（中）），防火墙会先评估数据包丢失，随后是延迟，最后是抖动。

如SD-WAN 流量分发配置文件概念所述，如果使用路径监视和探测频率默认设置，则新路径选择可在一秒内完成；否则，新路径选择用时大于一秒。要实现基于数据包丢失的亚秒级故障转移，您必须将延迟敏感度设置为 **high**（高），并将延迟阈值设置为不超过 250 毫秒。

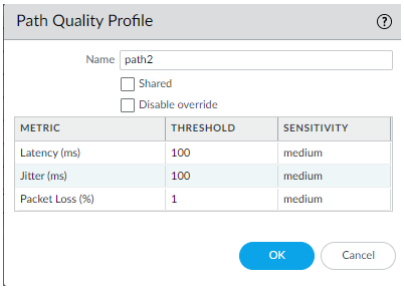
引用 SD-WAN 策略规则中的路径质量配置文件，以确定防火墙将用于匹配应用程序数据包的恶化路径更换为新路径的阈值。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Device Group**（设备组）。

STEP 3 | 选择 **Objects**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **Path Quality Profile**（路径质量配置文件）。

STEP 4 | 按 **Name**（名称）（最多使用 31 个字母数字字符构成）**Add**（添加） 路径质量配置文件。



STEP 5 | 对于 **Latency**（延迟），双击 **Threshold**（阈值）数值，然后输入允许数据包离开防火墙并到达 SD-WAN 隧道另一端，允许响应数据包在超过阈值之前返回到防火墙的毫秒数（范围为 10-2,000；默认为 100）。

STEP 6 | 对于 **Latency**（延迟），请选择 **Sensitivity**（敏感性） （**low**（低）、**medium**（中）或 **high**（高））。默认为 **medium**（中）。

单击阈值列末尾的箭头，以按数字升序或降序对阈值进行排序。

STEP 7 | 对于 **Jitter**（抖动），双击 **Threshold**（阈值）数值，然后输入毫秒数（范围为 10-1,000；默认为 100）。

STEP 8 | 对于 **Jitter**（抖动），请选择 **Sensitivity**（敏感性） （**low**（低）、**medium**（中）或 **high**（高））。默认为 **medium**（中）。

STEP 9 | 对于 **Packet Loss**（数据包丢失），双击 **Threshold**（阈值）数值，然后输入超出阈值之前链路上的数据包丢失百分比（范围为 1-100.0；默认为 1）。

数据包丢失（***Packet Loss***）的 ***Sensitivity***（敏感性）设置将不起作用，因此，可以不管默认设置。

如果更改用于 *Panorama* 模板的 *SD-WAN* 接口配置文件的探测频率，还需调整 *Panorama* 设备组的数据包丢失百分比阈值。

STEP 10 | 单击 **OK**（确定）。

STEP 11 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 12 | **Commit**（提交）更改。

STEP 13 | 对每个设备组重复此任务。

配置 SaaS 监控

配置 SaaS 质量配置文件以监控 SaaS 应用程序和分支防火墙之间的直接互联网访问 (DIA) 链路。

仅启用了 *SD-WAN* 的 *PAN-OS* 防火墙支持 *SaaS* 应用程序路径监视。*Prisma Access* 中心不支持 *SaaS* 应用程序路径监视。

- 创建一个 SaaS 质量配置文件
- 用例：为分支防火墙配置 SaaS 监控
- 用例：为从分支防火墙到同一 SaaS 应用程序目标的 SaaS 监控配置中心防火墙故障转移
- 用例：为从分支防火墙到不同 SaaS 应用程序目标的 SaaS 监控配置中心防火墙故障转移

创建一个 SaaS 质量配置文件

如果您的分支防火墙具有指向软件即服务 (DIA) 应用程序的直接互联网访问 (DIA) 链路，请创建一个 SaaS 质量配置文件以指定应如何监控一个或多个 SaaS 应用程序。SaaS 质量配置文件与 SD-WAN 策略规则关联，以确定分支防火墙如何确定延迟、抖动和数据包丢失的路径质量阈值，并为传出数据包选择首选路径。

SaaS 质量配置文件最多支持 4 个静态 IP 地址，或者每个 SaaS 质量配置文件支持一个完全限定域名 (FQDN) 或 URL。当配置了多个静态 IP 地址时，分支防火墙会根据 IP 地址在 SaaS 质量配置文件中的顺序，以级联顺序一次监控一个 IP 地址。例如，如果添加 IP1、IP2、IP3 和 IP4，则分支防火墙将监控 IP1 以确定是否超过了路径质量阈值，然后继续监控 IP2，依此类推。

SD-WAN 监控和报告数据显示 *SaaS* 应用程序和 *SaaS* 应用程序 *IP*、*FQDN* 或 *URL*，因为其当前在与 *SD-WAN* 策略规则关联的 *SaaS* 质量配置文件中配置，而与查看 *SD-WAN* 监控数据时应用的时间筛选器无关。

例如，三天前，您在 *SaaS* 质量配置文件中最初将 *SaaS* 应用程序的 *IP* 地址配置为 ***192.168.10.50***，且将流量与 *SaaS* 质量配置文件关联的 *SD-WAN* 策略规则匹配。今天，您重新配置了这个现有的 *SaaS* 质量配置文件，并将 *SaaS* 应用程序 *IP* 地址更改为 ***192.168.10.20***。查看 *SD-WAN* 监控数据时，此 *SaaS* 应用程序的所有现有监控数据都显示 *IP* 地址 ***192.168.10.20***。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Object**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **SaaS Quality Profile**（**SaaS** 质量配置文件），并指定包含 SD-WAN 配置的 **Device Group**（设备组）。

STEP 3 | **Add**（添加）一个新的 SaaS 质量配置文件。

STEP 4 | 为 SaaS 质量配置文件输入描述性 **Name**（名称）。

STEP 5 | （可选）启用（勾选）**Shared**（共享）可使所有设备组共享 SaaS 质量配置文件。

STEP 6 | （可选）启用（勾选）**Disable override**（禁用覆盖）可在本地防火墙禁用覆盖 SaaS 质量配置文件配置。

Disable override（禁用覆盖）只能在前一步中禁用 ***Shared***（共享）时启用。

STEP 7 | 配置 SaaS 监控模式。

- 自动监控 SaaS 应用程序路径运行状况。

  默认情况下，**Adaptive**（自适应）监控允许分支防火墙被动地监控 SaaS 应用程序会话的发送和接收活动，以确定是否超过了路径质量阈值。SaaS 应用程序路径运行状况质量是自动确定的，无需对 SD-WAN 接口进行任何额外的运行状况检查。

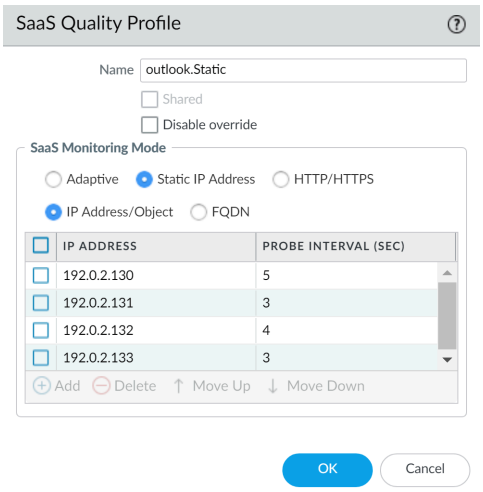
  自适应 *SaaS* 监控仅支持 *TCP SaaS* 应用程序。

- 为 SaaS 应用程序配置静态 IP 地址。

  为每个需要监控的关键 *SaaS* 应用程序创建 *SaaS* 质量配置文件。如果 *SaaS* 应用程序有多个 *IP* 地址，请为该 *SaaS* 应用程序配置具有多个静态 *IP* 地址的 *SaaS* 质量配置文件。

  SaaS 监控是资源密集型的，如果监控大量 *SaaS* 应用程序，可能会影响防火墙性能。最好的做法是只监控那些需要良好可用性的业务关键型 *SaaS* 应用程序。

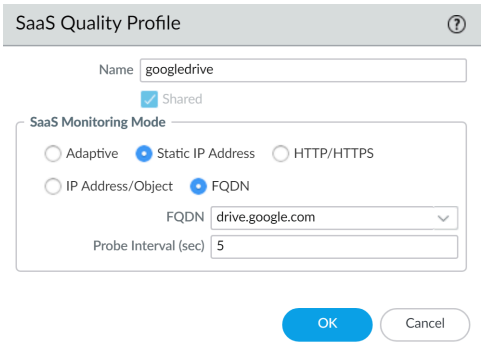
  1. 选择 **IP Address/Object**（**IP** 地址/对象）> **Static IP Address**（静态 **IP** 地址）并 **Add**（添加）一个 IP 地址。
  2. 输入 SaaS 应用程序的 IP 地址，或选择一个配置的地址对象。
  3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
  4. 单击 **OK**（确定）保存您的配置更改。



- 为 SaaS 应用程序配置完全限定域名 (FQDN)。

  1. 为 SaaS 应用程序配置 FQDN 地址对象。
  2. 选择 **IP Address/Object**（**IP** 地址/对象）> **FQDN** 并 **Add**（添加）FQDN。
  3. 为 SaaS 应用程序选择 **FQDN** 地址对象。
  4. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。

5. 单击 **OK**（确定）保存您的配置更改。

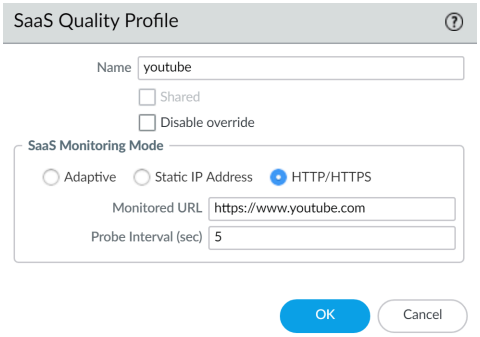


- 为 SaaS 应用程序配置 URL。

  仅通过端口 *80*、*443*、*8080*、*8081* 和 *143* 的流量支持 *URL* 监控。

  1. 选择 **HTTP/HTTPS**。
  2. 输入 SaaS 应用程序的 **Monitored URL**（受监控的 **URL**）。
  3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。

     SaaS 应用程序 HTTP/HTTPS 支持的最小探测间隔为 3 秒。
  4. 单击 **OK**（确定）保存您的配置更改。



STEP 8 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

用例：为分支防火墙配置 SaaS 监控

如果您的组织正在分支防火墙位置利用业务关键型 SaaS 应用程序，您可以配置 SaaS 质量配置文件，并将其与 SD-WAN 策略规则关联，以监控关键 SaaS 应用程序的延迟、抖动和数据包丢失的运行状况指标，并将 SD-WAN 分支防火墙的链路交换到直接互联网访问 (DIA) 链路上的 SaaS 应用程序，以确保应用程序可用性。

如果超过业务关键型 SaaS 应用程序的 DIA 链路运行状况指标阈值，则链路将交换到下一个在流量分发配置文件中为所有新会话配置的 DIA 链路。降级 DIA 链路上的现有会话不会交换到下一个 DIA 链路。

STEP 1 | 设置您的 SD-WAN 部署。

1. 安装 SD-WAN 插件.
2. 设置用于 SD-WAN 的 Panorama 和防火墙.
3. 添加 SD-WAN 设备到 Panorama.
4. （仅限高可用性配置）配置 SD-WAN HA 设备。
5. 创建 VPN 集群.

STEP 2 | 创建链路标记，对 SaaS 应用程序 DIA 链路进行分组。

为您的 DIA 链路创建多个链路标记，以根据链路类型为每个 SaaS 应用程序 DIA 链路应用不同的 SD-WAN 监控设置。

此外，您还可以为多个 DIA 链路创建一个链路标记，以将链路集合成一个链路包。为多个 DIA 链路创建一个链路标记允许您在绑定链路之间聚合带宽，并允许防火墙在多个链路之间分发会话。

STEP 3 | 配置 SD-WAN 接口配置文件以定义您的 ISP 连接的特征并指定 DIA 链路的速度、分支防火墙监控链路的频率，并选择链路标记以指定 SD-WAN 接口配置文件适用的链路。

如果您创建了多个链路标记，您必须为每个链路标记配置 SD-WAN 接口配置文件。

如果通过将多个 DIA 链路分配到一个链路标记创建了链路包，指定该链路标记会将 SD-WAN 接口配置文件设置应用到链路包的所有 DIA 链路中。

STEP 4 | 为每个 SaaS 应用程序 DIA 链路配置物理以太网接口。

DIA 链路的所有物理以太网接口必须是 *Layer3*。

STEP 5 | 配置 SD-WAN 虚拟接口，将 SaaS 应用程序 DIA 链路的所有物理以太网接口集合成一个接口组。

防火墙虚拟路由器通过此 SD-WAN 虚拟接口将 SD-WAN 流量路由到 DIA 位置。SD-WAN 策略规则中的 SD-WAN 路径运行状况和流量分发配置文件然后将决定使用的路径以及路径运行状况恶化时考虑使用的新路径顺序。

STEP 6 | 创建路径质量配置文件可配置延迟、抖动和数据包丢失阈值和敏感性，以指定分支防火墙何时应交换到下一个 DIA 链路。

STEP 7 | 创建 SaaS 质量配置文件以指定您的 SaaS 应用程序和 DIA 链路受到监控的频率。

STEP 8 | 创建流量分发配置文件以在链路运行状况恶化的情况下指定分支防火墙交换到 DIA 链路的顺序。

STEP 9 | 配置 SD-WAN 策略规则以指定 SaaS 应用程序和链路运行状况指标，并确定防火墙为关键 SaaS 应用程序流量选择首选链路的方式。

在 ***Application***（应用程序）选项卡中，将监控的 *SaaS* 应用程序添加到 *SD-WAN* 策略规则中，以确保 *SaaS* 监控设置仅应用于所需的 *SaaS* 应用程序。

用例：为从分支防火墙到同一 SaaS 应用程序目标的 SaaS 监控配置中心防火墙故障转移

如果您的组织在分支防火墙位置利用 SaaS 应用程序，但分支防火墙没有可交换的正常 DIA 链路，则可以将分支防火墙配置为故障转移备选方案，以维护到 SaaS 应用程序的正常连接。

如果超过 SaaS 应用程序 DIA 链路的正常指标阈值，且分支防火墙没有可用的正常 DIA 链路，则该链路将交换到下一个中心防火墙以用于所有新会话。降级 DIA 链路上的现有会话不会交换到中心防火墙。

例如，假设您的分支和中心防火墙位于同一个区域，并使用相同的目标 IP 访问 SaaS 应用程序。您可以通过在分支和中心防火墙上配置同名的 SaaS 质量配置文件，将中心防火墙配置为在分支防火墙与 SaaS 应用程序之间没有正常 DIA 链路的情况下充当故障转移，从而在分支防火墙与 SaaS 应用程序之间没有正常 DIA 链路时自动故障转移到中心防火墙。这允许您能为 SaaS 应用程序维持正常的路径，并能够维护准确的端对端 SaaS 应用程序监控数据，同时不造成网络宽带拥堵。

STEP 1 | 设置您的 SD-WAN 部署。

1. 安装 SD-WAN 插件.
2. 设置用于 SD-WAN 的 Panorama 和防火墙.
3. 添加 SD-WAN 设备到 Panorama.
4. （仅限高可用性配置）配置 SD-WAN HA 设备。
5. 创建 VPN 集群.

STEP 2 | 创建链路标记，对 SaaS 应用程序 DIA 链路进行分组。

为您的 DIA 链路创建多个链路标记，以根据链路类型为每个 SaaS 应用程序 DIA 链路应用不同的 SD-WAN 监控设置。

此外，您还可以为多个 DIA 链路创建一个链路标记，以将链路集合成一个链路包。

STEP 3 | 配置 SD-WAN 接口配置文件以定义您的 ISP 连接的特征并指定 DIA 链路的速度、分支防火墙监控链路的频率，并选择链路标记以指定 SD-WAN 接口配置文件适用的链路。

如果您创建了多个链路标记，您必须为每个链路标记配置 SD-WAN 接口配置文件。

如果通过将多个 DIA 链路分配到一个链路标记创建了链路包，指定该链路标记会将 SD-WAN 接口配置文件设置应用到链路包的所有 DIA 链路中。

STEP 4 | 为每个 SaaS 应用程序 DIA 链路配置物理以太网接口。

DIA 链路的所有物理以太网接口必须是 *Layer3*。

STEP 5 | 配置 SD-WAN 虚拟接口，将 SaaS 应用程序 DIA 链路的所有物理以太网接口集合成一个接口组。

防火墙虚拟路由器通过此 SD-WAN 虚拟接口将 SD-WAN 流量路由到 DIA 位置。SD-WAN 策略规则中的 SD-WAN 路径运行状况和流量分发配置文件然后将决定使用的路径以及路径运行状况恶化时考虑使用的新路径顺序。

STEP 6 | 为中心和分支防火墙创建同名的 SaaS 质量配置文件。

必须在中心和分支防火墙上配置两个同名的 SaaS 质量配置文件，以成功将中心防火墙用作备用故障转移。实现这一目标的最简单方法是在共享设备组中创建一个 SaaS 质量配置文件。或者，

您可以在不同的设备组中创建两个同名的 SaaS 质量配置文件，并将其推送至您的中心和分支防火墙。

1. 选择 **Object**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **SaaS Quality Profile**（**SaaS** 质量配置文件），然后从设备组下拉菜单中选择 **Shared**（共享）。
2. **Add**（添加）一个新的 SaaS 质量配置文件。
3. 为 SaaS 质量配置文件输入描述性 **Name**（名称）。
4. 启用（勾选）**Shared**（共享）可使所有设备组共享 SaaS 质量配置文件。

   必须执行这一步，才能使 SaaS 质量配置文件对您的分支和中心防火墙所属的所有设备组可用。
5. 启用（勾选）**Disable override**（禁用覆盖）可在本地防火墙禁用覆盖 SaaS 质量配置文件配置。
6. 用以下方法之一配置 SaaS 监控模式。
   - 为 SaaS 应用程序配置静态 IP 地址。

     为每个 *SaaS* 应用程序创建一个 *SaaS* 质量配置文件。如果 *SaaS* 应用程序有多个 *IP* 地址，请为该 *SaaS* 应用程序配置具有多个静态 *IP* 地址的 *SaaS* 质量配置文件。

     1. 选择 **IP Address/Object**（**IP** 地址/对象） > **Static IP Address**（静态 **IP** 地址）并 **Add**（添加）一个 IP 地址。
     2. 输入 SaaS 应用程序的 IP 地址，或选择一个配置的地址对象。
     3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
     4. 单击 **OK**（确定）保存您的配置更改。
   - 为 SaaS 应用程序配置完全限定域名 (FQDN)。
     1. 为 SaaS 应用程序配置 FQDN 地址对象。
     2. 选择 **IP Address/Object**（**IP** 地址/对象） > **FQDN** 并 **Add**（添加）FQDN。
     3. 为 SaaS 应用程序选择 **FQDN** 地址对象。
     4. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
     5. 单击 **OK**（确定）保存您的配置更改。
   - 为 SaaS 应用程序配置 URL。

     仅通过端口 *80*、*443*、*8080*、*8081* 和 *143* 的流量支持 *URL* 监控。

     1. 选择 **HTTP/HTTPS**。
     2. 输入 SaaS 应用程序的 **Monitored URL**（受监控的 **URL**）。

3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
4. 单击 **OK**（确定）保存您的配置更改。

STEP 7 | 创建流量分发配置文件以在链路运行状况恶化的情况下指定分支防火墙从 DIA 链路交换到 VPN 链路，再到中心防火墙的顺序。

STEP 8 | 配置 SD-WAN 策略规则以指定 SaaS 应用程序和链路运行状况指标，并确定防火墙为关键 SaaS 应用程序流量选择首选链路的方式。

在 ***Application***（应用程序）选项卡中，将监控的 *SaaS* 应用程序添加到 *SD-WAN* 策略规则中，以确保 *SaaS* 监控设置仅应用于所需的 *SaaS* 应用程序。

用例：为从分支防火墙到不同 SaaS 应用程序目标的 SaaS 监控配置中心防火墙故障转移

如果您的组织在分支防火墙位置利用 SaaS 应用程序，但分支防火墙没有可交换的正常 DIA 链路，则可以将分支防火墙配置为故障转移备选方案，以使用指向不同 SaaS 应用程序目标的 SaaS 质量配置文件来维护到 SaaS 应用程序的正常连接。

如果超过 SaaS 应用程序 DIA 链路的正常指标阈值，且分支防火墙没有可用的正常 DIA 链路，则该链路将交换到下一个中心防火墙以用于所有新会话。降级 DIA 链路上的现有会话不会交换到中心防火墙。

例如，假设您的分支和中心防火墙位于该国家/地区的相对侧，并访问部署在云提供商（如 GCP）中的 SaaS 云应用程序。您可以配置中心防火墙，以在分支防火墙到 SaaS 应用程序之间没有正常 DIA 链路时充当故障转移。为此，可以在分支和中心防火墙上配置同名的 SaaS 质量配置文件，以在分支防火墙没有正常 DIA 链路可用时实现到中心防火墙的自动故障转移。在中心防火墙上配置的 SaaS 质量配置文件指向离中心最近的入口位置，以利用离它最近的本地资源。这允许您能灵活指定正常的故障转移路径，并能够维护准确的端对端 SaaS 应用程序监控数据，同时不造成网络带宽拥堵。

STEP 1 | 设置您的 SD-WAN 部署。

1. 安装 SD-WAN 插件.
2. 设置用于 SD-WAN 的 Panorama 和防火墙.
3. 添加 SD-WAN 设备到 Panorama.
4. （仅限高可用性配置）配置 SD-WAN HA 设备。
5. 创建 VPN 集群.

STEP 2 | 创建链路标记，对 SaaS 应用程序 DIA 链路进行分组。

为您的 DIA 链路创建多个链路标记，以根据链路类型为每个 SaaS 应用程序 DIA 链路应用不同的 SD-WAN 监控设置。

此外，您还可以为多个 DIA 链路创建一个链路标记，以将链路集合成一个链路包。

STEP 3 | 配置 SD-WAN 接口配置文件以定义您的 ISP 连接的特征并指定 DIA 链路的速度、分支防火墙监控链路的频率，并选择链路标记以指定 SD-WAN 接口配置文件适用的链路。

如果您创建了多个链路标记，您必须为每个链路标记配置 SD-WAN 接口配置文件。

如果通过将多个 DIA 链路分配到一个链路标记创建了链路包，指定该链路标记会将 SD-WAN 接口配置文件设置应用到链路包的所有 DIA 链路中。

STEP 4 | 为每个 SaaS 应用程序 DIA 链路配置物理以太网接口。

DIA 链路的所有物理以太网接口必须是 *Layer3*。

STEP 5 | 配置 SD-WAN 虚拟接口，将 SaaS 应用程序 DIA 链路的所有物理以太网接口集合成一个接口组。

防火墙虚拟路由器通过此 SD-WAN 虚拟接口将 SD-WAN 流量路由到 DIA 位置。SD-WAN 策略规则中的 SD-WAN 路径运行状况和流量分发配置文件然后将决定使用的路径以及路径运行状况恶化时考虑使用的新路径顺序。

STEP 6 | 为中心和分支防火墙创建同名的 SaaS 质量配置文件。

必须在中心和分支防火墙上配置两个同名的 SaaS 质量配置文件，以成功将中心防火墙用作备用故障转移。创建两个同名且指向不同设备组中的不同 SaaS 应用程序目标的 SaaS 质量配置文件，并将它们推送至您的中心和分支防火墙。

1. 选择 **Object**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **SaaS Quality Profile**（**SaaS** 质量配置文件），然后从设备组下拉菜单中选择包含分支防火墙的目标设备组。
2. **Add**（添加）一个新的 SaaS 质量配置文件。
3. 为 SaaS 质量配置文件输入描述性 **Name**（名称）。
4. 启用（勾选）**Disable override**（禁用覆盖）可在本地防火墙禁用覆盖 SaaS 质量配置文件配置。
5. 用以下方法之一配置 SaaS 监控模式。
   - 为 SaaS 应用程序配置静态 IP 地址。

     为每个 *SaaS* 应用程序创建一个 *SaaS* 质量配置文件。如果 *SaaS* 应用程序有多个 *IP* 地址，请为该 *SaaS* 应用程序配置具有多个静态 *IP* 地址的 *SaaS* 质量配置文件。

     1. 选择 **IP Address/Object**（**IP** 地址/对象） > **Static IP Address**（静态 **IP** 地址）并 **Add**（添加）一个 IP 地址。
     2. 输入 SaaS 应用程序的 IP 地址，或选择一个配置的地址对象。
     3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
     4. 单击 **OK**（确定）保存您的配置更改。
   - 为 SaaS 应用程序配置完全限定域名 (FQDN)。
     1. 为 SaaS 应用程序配置 FQDN 地址对象。
     2. 选择 **IP Address/Object**（**IP** 地址/对象） > **FQDN** 并 **Add**（添加）FQDN。
     3. 为 SaaS 应用程序选择 **FQDN** 地址对象。
     4. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
     5. 单击 **OK**（确定）保存您的配置更改。
   - 为 SaaS 应用程序配置 URL。

     仅通过端口 *80*、*443*、*8080*、*8081* 和 *143* 的流量支持 *URL* 监控。

     1. 选择 **HTTP/HTTPS**。
     2. 输入 SaaS 应用程序的 **Monitored URL**（受监控的 **URL**）。

3. 输入 **Probe Interval**（探测间隔），分支防火墙按照此间隔探测 SaaS 应用程序路径，以了解运行状况信息。
4. 单击 **OK**（确定）保存您的配置更改。

6. 选择 **Object**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **SaaS Quality Profile**（**SaaS** 质量配置文件），然后从设备组下拉菜单中选择包含中心防火墙的目标设备组。
7. 重复步骤 6.2 到 6.5，为位于不同目标的 SaaS 应用程序创建同名的 SaaS 质量配置文件。

   必须执行这一步，才能在您的中心防火墙所属的设备组中创建同名的 SaaS 质量配置文件。

STEP 7 | 创建流量分发配置文件以在链路运行状况恶化的情况下指定分支防火墙从 DIA 链路交换到 VPN 链路，再到中心防火墙的顺序。

STEP 8 | 配置 SD-WAN 策略规则以指定 SaaS 应用程序和链路运行状况指标，并确定防火墙为关键 SaaS 应用程序流量选择首选链路的方式。

在 ***Application***（应用程序）选项卡中，将监控的 *SaaS* 应用程序添加到 *SD-WAN* 策略规则中，以确保 *SaaS* 监控设置仅应用于所需的 *SaaS* 应用程序。

SD-WAN 流量分发配置文件

在 SD-WAN 拓扑结构中，防火墙检测各个应用程序是否存在供电不足、断电和路径恶化等现象，然后选择一个新路径，确保您能为您的业务关键型应用程序获得最佳性能。具有多个 ISP 链路可以扩展流量容量，降低成本。如果使用 路径监控和探测频率默认设置，则新路径选择可在一秒内完成；否则，新路径选择用时大于一秒。

要实施此类路径选择，防火墙使用的 SD-WAN 策略规则引用了指定如何选择会话负载分发路径，以及如何在应用程序路径质量出现问题时故障转移到更好的路径的流量分发配置文件。

确定与 SD-WAN 策略规则匹配的应用程序或服务应使用的流量分发方法：

- **Best Available Path**（最佳可用路径）— 在不计成本，且允许应用程序使用分支以外的任何路径时，选择此方法。防火墙使用路径质量指标分发流量，故障转移到属于列表中链路标记的链路之一，从而为用户提供最佳的应用程序体验。
- **Top-Down Priority**（自上而下优先级）— 如果您只想将昂贵或低容量链路用作最后的选择或备份链路，请使用自上而下优先级方法，将包含这些链路的标记置于配置文件中链路标记列表的最后一位。防火墙首先使用列表中排名第一的链路标记确定会话负载流量使用的链路以及执行故障转移的链路。如果根据路径质量配置文件，排名第一的链路标记中的链路都不合格，防火墙将从列表中排名第二的链路标记中选择一个链路。如果排名第二的链路标记中的链路也都不合格，则根据需要继续执行此过程，直至防火墙在之后一个链路标记中找到合格的链路。如果所有关联链路都过载，且没有链路满足质量阈值要求，则防火墙使用最佳可用路径方法选择用于转发流量的链路。开始执行故障转移时，防火墙采用自上而下优先级方法，从链路标记列表中优先级最高的开始，以查找执行故障转移的链路。

- **Weighted Session Distribution**（加权会话分发）— 如果您想手动加载与规则匹配的流量到 ISP 和 WAN 链路，且您无需在断电情况下执行故障转移时，可以选择此方法。您可以在应用新会话静态百分比时，手动指定链路负载。此会话是采用单个链路标记进行分组的接口所获取的会话。防火墙使用循环调度法在具有指定链路标记的链路上分发新会话，直至分配最低百分比的链路达到此会话的百分比。随后，防火墙以相同的方式使用剩余链路。对于对延迟不敏感，且需要大量链路带宽容量（例如，大的分支备份和大的文件传输）的应用程序，您可以选择此方法。

  如果链路出现断电情况，防火墙不会将匹配流量重定向到不同的链路。

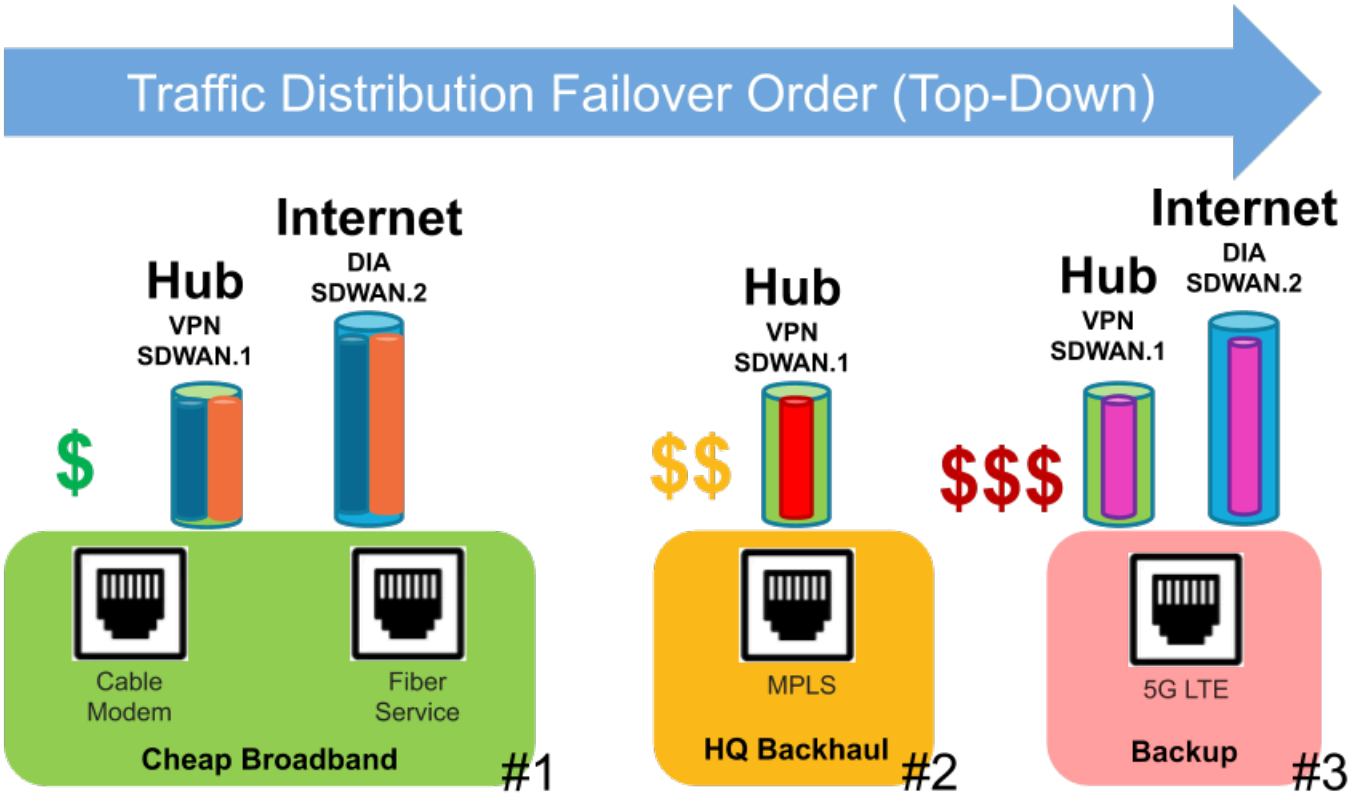
如果路径运行状况出现故障，您可以根据在 SD-WAN 策略规则中为应用程序选择的流量分发方法，以及链路组上的链路标记确定防火墙是否会选择一个新路径（执行链路故障转移），以及如何选择，如下所示：

路径运行状况	自上而下优先级	最佳可用路径	加权会话分发
现有路径上的会话与路径健康阈值不匹配（供电不足）	受影响的会话故障转移到更好的路径（如有）	受影响的会话故障转移到更好的路径（如有）	受影响会话未执行故障转移
自上而下或最佳可用路径已恢复：现有路径仍合格（良好）	受影响会话无法返回到先前路径	受影响会话停在现有路径中，无法返回	受影响会话未执行故障转移
自上而下或最佳可用路径已恢复：现有路径无法执行运行状况检查	所有会话都无法返回到先前路径	受影响的现有路径恢复之前，所选会话无法返回到先前路径	受影响会话未执行故障转移
现有路径已关闭（断电）	所有会话均故障转移到列表中的下一个路径	所有会话均故障转移到下一个最佳路径	所有会话均根据加权设置故障转移到其他标记
供电不足，且无合格（更好的）路径	采用最佳可用路径	采用最佳可用路径	采用最佳可用路径

此外，防火墙会在单个链路标记的接口成员上自动执行会话负载共享。在这些接口达到最大 Mbps 后，如果这些接口具有更好的运行状况指标，新会话将根据流量分发方法流向带不同链路标记的接口。

路径运行状况	自上而下优先级	最佳可用路径	加权会话分发
多个链路具有相同的 SD-WAN 标记	在 SD-WAN 标记的链路上平均共享会话负载	在 SD-WAN 标记中基于最佳路径共享会话负载	基于分配给 SD-WAN 标记的权重百分比共享到 SD-WAN 标记
多个链路具有不同的 SD-WAN 标记	首先在第一个 SD-WAN 标记的负载链路上，基于列表优先级共享会话负载。	从所有 SD-WAN 标记中，基于最佳路径共享会话负载	基于分配给 SD-WAN 标记的权重百分比共享到 SD-WAN 标记

下图展示的是使用自上而下优先级方法的流量分发配置文件示例。链路标记顺序 #1、#2 和 #3 是在必要时，防火墙进行检查，以找到运行状况良好的路径，从而完成应用程序会话故障转移的顺序。对于出现的每个单独的故障转移事件，防火墙采用自上而下优先级，从链路标记列表开始。

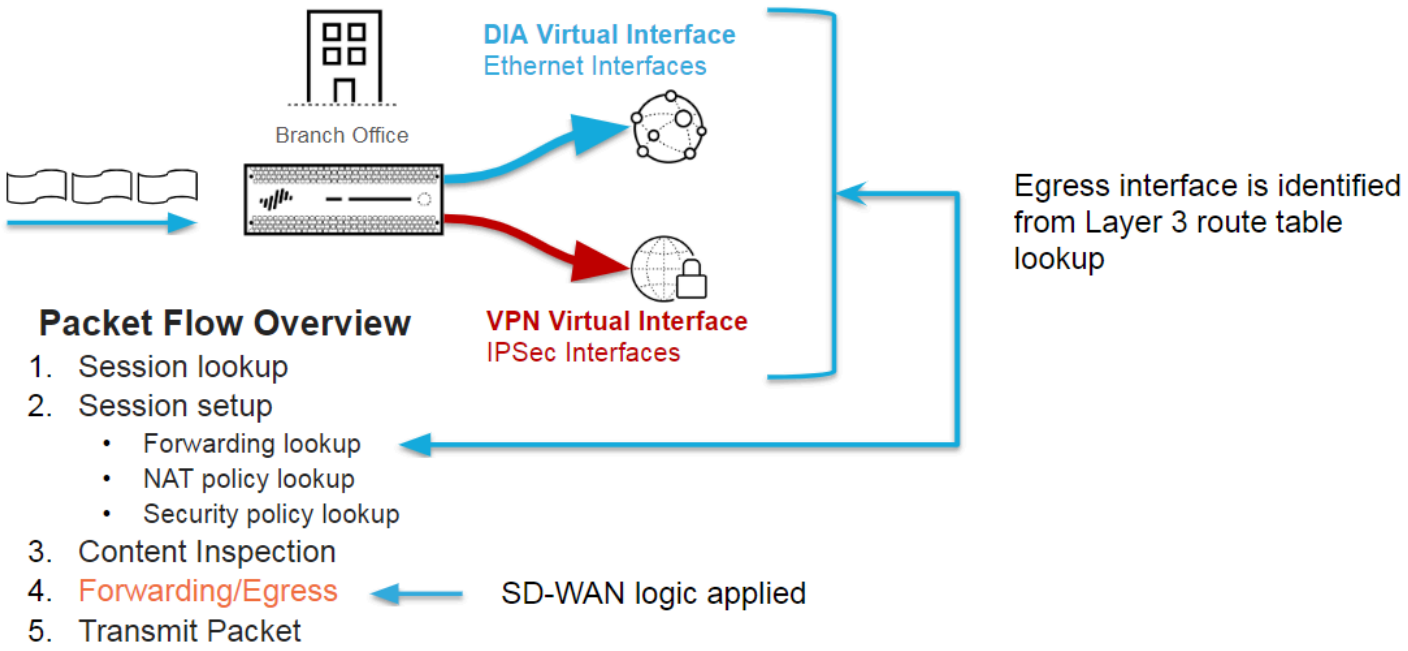


1. 在此自上而下优先级示例中，来自分支的，并承载有特定应用程序（例如，office365-enterprise-access）的数据包会到达防火墙。防火墙使用路由表来确定目标和传出接口的下一个跃点。该传出接口是名为 sdwan.1 的 SD-WAN 虚拟接口隧道。安全策略规则允许数据包。随后，数据包与用于指定中心目标区域的 SD-WAN 策略规则（名为 Office365 to Hub1）进行匹配。防火墙使用 SD-WAN 策略规则的路径质量配置文件、流量分发配置文件、以及此配置文件的链路标记来确定要从 sdwan.1 中使用的接口成员（链路）。流量分发配置文件按此顺序列出了三个链路标

记：#1，便宜宽带；#2，HQ 回程；#3，备份（此顺序也是防火墙用于检查链路，以找到可以执行故障转移的链路的链路标记的顺序）。

2. 假定所有路径都合格（与路径质量配置文件匹配），防火墙会将数据包分发到流量分发配置文件列表中带第一个链路标记的物理链路之一：便宜宽带。隧道 sdwan.1 有两个成员接口（两个运营商）：电缆调制解调器 VPN 隧道和光纤服务 VPN 隧道。防火墙首先通过循环调度检查链路，然后选择它找到的第一个合格链路，例如，电缆调制解调器链路。
3. 如果第一便宜宽带链路（电缆调制解调器）不是合格的链路，防火墙将选择第二便宜宽带链路（光纤服务）。
4. 如果第二便宜宽带链路（光纤服务）也是不合格的链路，防火墙将选择带 #2 链路标记的 HQ 回程链路。这是指向同一中心的较贵的 MPLS 链路。
5. 如果 MPLS 链路不是合格的链路，防火墙将选择带 #3 的链路标记备份链路。这是指向同一中心更贵的 5G LTE 链路。
6. 如果防火墙未能找到可以执行故障转移的合格链路，将使用最佳可用方法选择一个链路。
7. 开始执行新的故障转移时，防火墙采用自上而下优先级方法，从链路标记列表中优先级最高的开始，以查找执行故障转移的链路。

切记，SD-WAN 流量分发是数据包流逻辑的后续步骤之一。让我们放大以更开阔的视野查看数据包流。

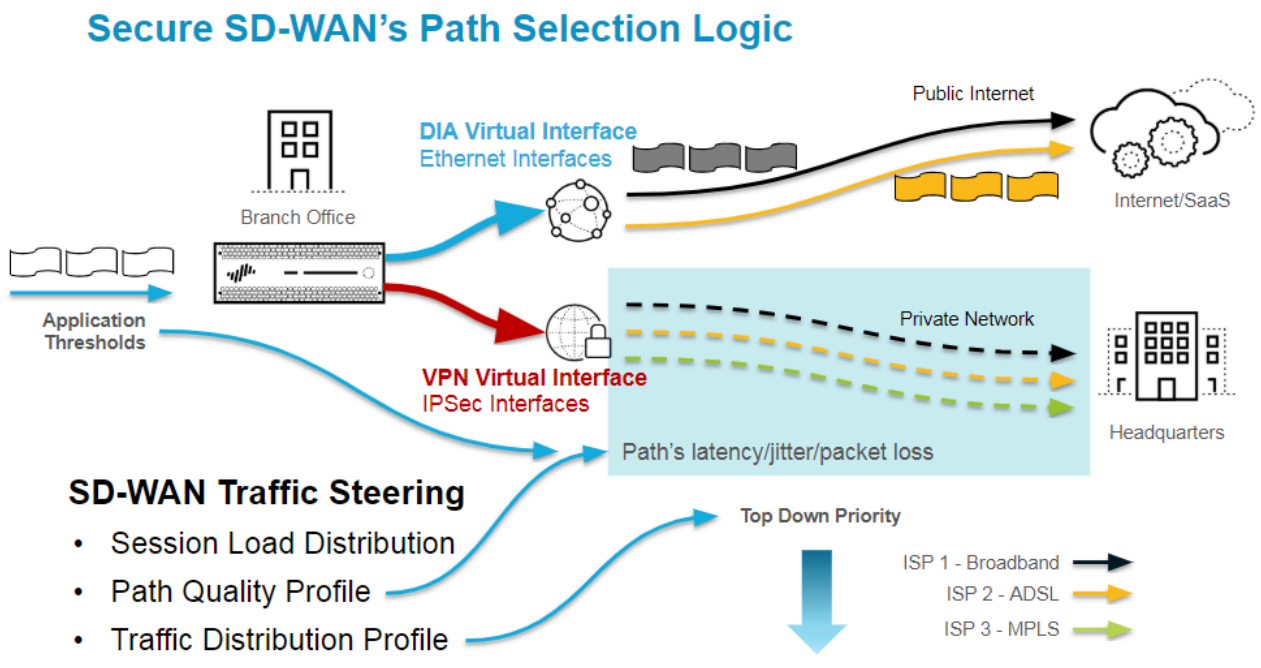


数据包流详细信息如下所示：

1. 一旦应用程序会话到达防火墙，防火墙会执行会话查找，以确定此会话是现有会话，还是新会话。

2. 新会话将经过会话设置：
    1. 转发查找 — 防火墙通过查找第 3 层路由表或第 2 层转发数据库等获取出口区域、出口接口和虚拟系统。对于匹配 SD-WAN 策略规则的应用程序，防火墙使用 SD-WAN 虚拟接口充当出口接口。
    2. NAT 策略查找 —如果会话匹配 NAT 规则，防火墙执行另一个转发查找，以确定最终（转换后的）出口接口和区域。
    3. 安全策略查找 — 如果安全策略规则允许会话，则会在会话表中创建和安装会话。随后，防火墙使用 App-ID™ 和 User-ID™ 执行其他分类。
3. 内容检查 — 防火墙根据需要对有效负载和标头执行威胁查找（IPS 防间谍软件【漏洞保护】、防病毒、URL 筛选、 WildFire® 等）。
4. 在转发/出口阶段执行路径检查，并转发数据包。在此阶段，会执行 SD-WAN 路径选择。
    1. 数据包转发过程 — 防火墙使用入口接口确定转发域；执行路由、切换或虚拟线路转发。
    2. 一旦应用程序匹配 SD-WAN 策略规则，就会执行 SD-WAN 路径选择；路径质量配置文件确定路径资格；流量分发配置文件确定路径选择方法以及选择时考虑路径的顺序。
    3. 根据需要，执行 IPSec/SSL-VPN 隧道加密。
    4. 数据包出口过程 — 应用 QoS 整形、DSCP 重写和 IP 分段（如需要）。
5. 发送数据包 — 防火墙通过选择的出口接口转发数据包。

现在，我们可以通过放大以更详细地检查 SD-WAN 路径选择逻辑。



1. 防火墙在转发查询时会查阅路由表；随后，防火墙根据匹配第 3 层前缀的目标 IP 地址，确定 SD-WAN 出口虚拟接口。数据包可以直接进入公共 Internet，也可以通过安全的 VPN 链路返回到中心。

2. 防火墙通过在 VPN 隧道上执行运行状况检查来监控各个路径。每个 DIA 回路都有一个用于监控运行状况信息的 VPN 隧道。
3. SD-WAN 策略规则中的应用程序与路径质量配置文件相关联，防火墙会将路径的延迟、抖动和数据包丢失的实际平均值与阈值进行比较。
4. 不得选择延迟、抖动或数据包丢失值大于阈值的路径。
5. 随后， SD-WAN 虚拟接口中的所有合格路径都将使用流量分发配置文件的方法和路径优先级（排序）逻辑。 SD-WAN 链路标记将 ISP 服务组合在一起，并且，在流量分发配置文件中，这些标记的顺序在路径选择时对路径进行优先排序。
6. 因此， 路径质量配置文件和 流量分发配置文件共同确定要使用的下一个最佳路径，然后，防火墙从此链路转出流量。

创建流量分发配置文件

根据您的 SD-WAN 配置计划，您可以基于您希望 SD-WAN 策略规则中的应用程序如何执行会话加载和故障转移的方式，创建所需要的 SD-WAN 流量分发配置文件。

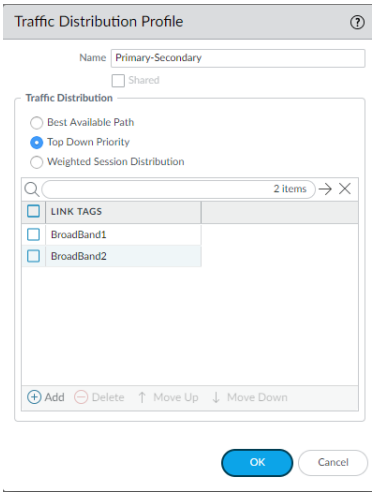
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 确保已在 SD-WAN 接口配置文件中完成链路标记的配置，并提交和推送这些标记。必须将链路标记推送到您的中心和分支，使 Panorama™ 能够成功将此流量分发配置文件中指定的链路标记与 SD-WAN 接口配置文件关联。

STEP 3 | 选择 **Device Group**（设备组）。

STEP 4 | 创建流量分发配置文件。

1. 选择 **Objects**（对象） > **SD-WAN Link Management**（**SD-WAN** 链路管理） > **Traffic Distribution Profile**（流量分发配置文件）。
2. 按**Name**（名称）（最多使用 31 个字母数字字符构成）**Add**（添加） 流量分发配置文件。



3. 如果您想在所有设备组（包括中心和分支）中使用此流量分发配置文件，请只选择 **Shared**（共享）。
4. 选择一种流量分发方法，并最多添加四个将此方法用于此配置文件的链路标记。

   - **Best Available Path**（最佳可用路径） —**Add**（添加）一个或多个 **Link Tags**（链路标记）。初始数据包交换期间，在 App-ID 对数据包中应用程序分类之前，防火墙根据标记顺序使用标记中具有最佳运行状况指标的路径。防火墙标识应用程序后，会将正在使用的路径运行状况（路径质量）与第一个链路标记中的第一个路径（接口）的运行状况进行比较。如果原始路径的运行状况更好，它将保留所选路径；否则，防火墙会替换原始路径。防火墙重复此过程，直至链路标记中所有路径的评估结束。最终路径是防火墙在满足匹配条件的数据包到达时选择的路径。

     一旦链路不合格，且必须故障转移到下一个最佳路径，防火墙可将最多 *1000* 个会话从不合格链路迁移到下一个最佳路径。例如，假定 *tunnel.901* 有 *3000* 个会话；其中 *2000* 个会话与 *SD-WAN* 策略规则 *A* 匹配，另外 *1000* 个会话与 *SD-WAN* 策略规则 *B* 匹配（两个规则使用的流量分发配置文件都配置有 ***Best Path Available***（最佳可用路径））。如果 *tunnel.901* 不合格，则需要 *3* 分钟的时间将这 *3000* 个会话从不合格链路迁移到下一个最佳路径。

   - **Top Down Priority**（自上而下优先级）—**Add**（添加）一个或多个 **Link Tags**（链路标记）。防火墙根据您添加的自上而下的 **Link Tags**（链路标记）顺序将满足匹配条件的新会话分发到链路。防火墙检查配置用于此配置文件的第一个标记，并检查使用此标记的路径，然后选择其认为合格的第一个路径（小于等于此规则的路径质量阈值）。如果防火墙未从链路标记中找到合格路径，则会检查使用下一个链路标记的路径。如果防火墙在检查完所有链路标记中的路径后仍未找到合格的路径，会使用 **Best Available Path**（最佳可用路径）方法。选择的第一个路径为首选路径，直至超出此路

径的其中一个路径质量阈值，一旦超过，防火墙将再次从链路标记顶部开始，查找新的首选路径。

如果中心只有一个链路，则该链路支持所有虚拟接口和 *DIA* 流量。如果要按特定顺序使用链路类型，则必须将流量分发配置文件应用于指定自上而下优先级的中心，然后对链路标记进行排序以指定首选顺序。如果应用的是指定最佳可用路径的流量分发配置文件，则无论成本如何，防火墙都将使用该链路来选择性能最佳的分支路径。总之，流量分发配置文件中的链路标记，即应用于中心虚拟接口的链路标记和 *SD-WAN* 接口配置文件中的 ***VPN Failover Metric***（***VPN*** 故障转移衡量指标）仅在流量分发配置文件指定 ***Top Down Priority***（自上而下优先级）时才起作用。

- **Weighted Session Distribution**（加权会话分发）— **Add**（添加）一个或多个 **Link Tags**（链路标记），然后输入各个 **Link Tag**（链路标记）的 **Weight**（加权）百分比，使加权百分比总和为 100%。防火墙在链路标记之间执行会话负载分发，直至达到其最大百分比。如果链路标记中有多个路径，防火墙会使用循环调度法平均分发，直至达到路径运行状况指标，然后，将会话分发到未达到限制的其他成员。

  如果多个物理接口采用相同的标记，则防火墙在这些接口之间平均分发匹配会话。如果所有路径都未达到运行状况（路径质量）阈值，防火墙将选择具有最佳运行状况统计信息的路径。如果因停电导致没有可用的 *SD-WAN*，防火墙将使用静态或动态路由传送匹配数据包。

  如果数据包被路由到 *SD-WAN* 虚拟接口，但是防火墙未能依据 *SD-WAN* 策略的流量分发配置文件找到用于会话的首选路径，则防火墙隐式使用最佳可用路径方法来查找首选路径。防火墙根据其隐式的最终规则分发与 *SD-WAN* 策略规则不匹配的任何应用程序会话。根据此规则，会话以循环调度顺序在所有可用链路之间分发，与流量分发配置文件无关。

  如果您希望控制防火墙分发不匹配会话的方式，请创建一个全面的最终规则以分发不匹配会话，从而按您指定的顺序指定链路。

5. （可选）链路标记添加结束后，使用 **Move Up**（上移）或 **Move Down**（下移）箭头更改列表中的标记顺序，以反映出您想防火墙将链路用于此配置文件以及 SD-WAN 策略规则中选中应用程序的顺序。
6. 单击 **OK**（确定）。

STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 6 | **Commit**（提交）更改。

创建纠错配置文件

转发纠错 (FEC) 是一种在嘈杂的通信线路上纠正某些数据传输错误的方法，从而在不需要重新传输的情况下提高数据可靠性。FEC 对于对数据包丢失或损坏敏感的应用程序有帮助，如音频、VoIP 和视频会议。通过 FEC，接收防火墙可通过部署发送编码器嵌入到应用程序流中的奇偶校验位来恢复丢失或损坏的数据包。修复流避免了 SD-WAN 数据故障转移到另一条路径或 TCP 重新发送

数据包的需求。由于 UDP 不会重新传输数据包，FEC 还可以通过恢复丢失或损坏的数据包来帮助 UDP 应用程序。

SD-WAN FEC 支持作为编码器和解码器的分支和中心防火墙。FEC 机制让编码器向位元流添加冗余位，解码器在将接收到的数据发送到目的地之前，根据需要使用该信息来校正接收到的数据。

SD-WAN 还支持数据包重复作为纠错的替代方法。数据包重复将应用程序会话从一个隧道完全复制到第二个隧道。数据包重复比 FEC 需要更多的资源，应只用于对丢弃的数据包容忍度较低的关键应用程序。

具有自己的嵌入式恢复机制的现代应用程序可能不需要 *FEC* 或数据包重复。仅将 *FEC* 或数据包重复应用于真正受益于这种机制的应用程序；否则，会导致大量额外的带宽和 *CPU* 开销，而不会带来任何好处。如果 *SD-WAN* 的问题是拥堵，则 *FEC* 和数据包重复都没有帮助。

FEC 和数据包重复功能要求 Panorama 运行 PAN-OS 10.0.2 或更高版本、SD-WAN 插件 2.0 或与 PAN-OS 版本兼容的更高版本。编码器和解码器都必须运行 PAN-OS 10.0.2 或更高版本。如果一个分支或中心运行的软件版本比要求的版本旧，那么带有 FEC 或数据包重复标头的流量将在该防火墙上被丢弃。

从 PAN-OS 10.0.3 开始，除已提供支持的中心辐射型拓扑外，全网状拓扑也支持 FEC 和数据包复制。

在 DIA 链路上不应使用 FEC 或数据包重复；它们仅用于分支和中心之间的 VPN 隧道链路。

仅启用了 *SD-WAN* 的 *PAN-OS* 防火墙支持 *FEC* 和数据包重复。*Prisma Access* 中心不支持 *FEC* 和数据包重复。

要在编码器上配置 FEC 或数据包重复（启动 FEC 或数据包重复的一侧），请使用 Panorama：

- 创建一个指定 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件）的 SD-WAN 接口配置文件，并将该配置文件应用于一个或多个接口。
- 创建一个纠错配置文件来实现 FEC 或数据包重复。
- 将纠错配置文件应用于 SD-WAN 策略规则，并指定该规则适用的单个应用程序。
- 将配置推送到编码器。（解码器 [接收侧] 不需要 FEC 或数据包重复的特定配置；只要编码器启动纠错，解码器上的机制默认是启用的。）

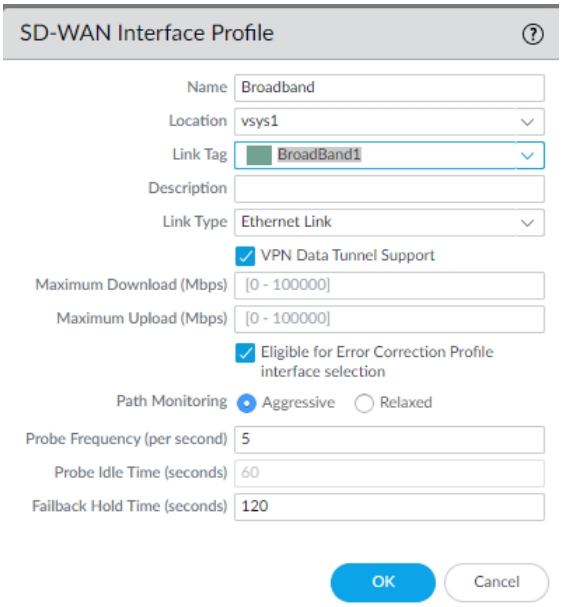
FEC 和数据包重复支持 *1,340* 字节的 *MTU*。大于该值的数据包将不会通过 *FEC* 或数据包重复过程。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置 SD-WAN 接口配置文件，在此处选择 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件），以表示防火墙可以自动使用接口（应用 SD-

WAN 接口配置文件的地方）进行纠错。此选项是否默认为已选择取决于为配置文件选择的 **Link Type**（链路类型）。

例如，您可以在配置文件中取消选中 ***Eligible for Error Correction Profile interface selection***（纠错配置文件接口的选择条件），并将该配置文件应用于昂贵的 *5G LTE* 链路，以便从不在该链路上执行昂贵的纠错。



STEP 3 | 配置 SD-WAN 物理以太网接口并将创建的 SD-WAN 接口配置文件应用于以太网接口。

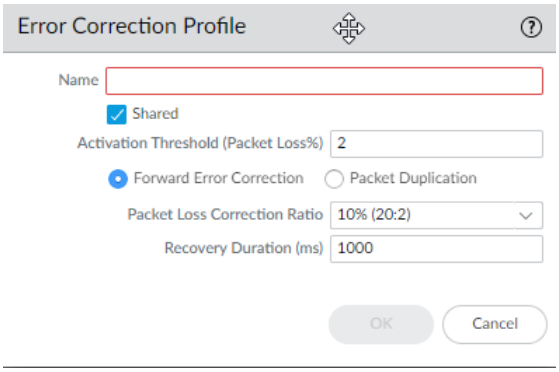
STEP 4 | 为 FEC 或数据包重复创建纠错配置文件。

1. 选择 **Objects**（对象）> **SD-WAN Link Management**（**SD-WAN** 链路管理）> **Error Correction Profile**（纠错配置文件）。
2. **Add**（添加）纠错配置文件，并输入最多 31 个字母数字字符的描述性 **Name**（名称）；例如，EC_VOIP。
3. 勾选 **Shared**（共享）可将纠错配置文件用于 Panorama 上的所有设备组、单一 vsys 中心或分支上的默认 vsys，以及您推送此配置的多 vsys 中心或分支上的 vsys1。
4. 指定 **Activate when packet loss exceeds (%)**（数据包丢失超过 **(%)** 时激活）设置 — 一旦数据包丢失超过此百分比，则会为应用此纠错配置文件的 SD-WAN 策略规则中配置的应用程序激活 FEC 或数据包重复。范围为 1 至 99；默认为 2。
5. 选择 **Forward Error Correction**（转发纠错）或 **Packet Duplication**（数据包重复）以指示当 SD-WAN 策略规则引用此 SD-WAN 接口配置文件时防火墙使用的纠错方法；默认为转发纠错。如果选择数据包重复，SD-WAN 将选择一个接口来发送重复的数据包。（SD-WAN 选择您在上一步中用 **Eligible for Error Correction Profile interface selection**（纠错配置文件接口的选择条件）配置的接口之一。）
6. （仅转发纠错）选择 **Packet Loss Correction Ratio**（数据包丢失纠正率）：**10% (20:2)**、**20% (20:4)**、**30% (20:6)**、**40% (20:8)** 或 **50% (20:10)** — 奇偶校验位与数据包的比

率，默认为 10% (20:2)。发送防火墙（编码器）发送的奇偶校验位与数据包的比率越高，接收防火墙（解码器）修复数据包丢失的概率就越高。但是，比率越高，需要的冗余就更多，因此，会需要更多的带宽开销，这是为实现纠错的权衡做法。奇偶校验率适用于编码防火墙传出流量。例如，如果中心防火墙奇偶校验率为 50%，分支防火墙奇偶校验率为 20%，则中心防火墙将接收 20%，分支防火墙将接收 50%。

7. 指定 **Recovery Duration (ms)**（恢复持续时间（毫米））— 接收防火墙（解码器）使用接收到的奇偶校验数据包对丢失的数据包执行数据包恢复所花费的最长毫秒数（范围为 1 至 5,000；默认为 1,000）。防火墙立即发送其接收到的数据包给目标。在恢复期间，解码器将为任何丢失的数据包执行数据包恢复。当恢复持续时间到期时，将释放所有奇偶校验数据包。您可以在编码器的纠错配置文件中配置恢复持续时间，该配置文件将恢复持续时间值发送到解码器。解码器上的恢复持续时间设置没有任何影响。

   从使用默认恢复持续时间设置开始，并根据对正常和间歇性供电不足的测试进行调整（如有必要）。



8. 单击 **OK**（确定）。

STEP 5 | 配置 SD-WAN 策略规则，引用您在规则中创建的 **Error Correction Profile**（纠错配置文件），并指定该规则适用的关键应用程序。

在配置 *FEC* 或数据包重复时，仅在 *SD-WAN* 策略规则中指定一个应用程序。您不应将多个应用程序合并到针对 *FEC* 或数据包复制的单个策略规则中。

STEP 6 | 将您的配置更改 **Commit**（提交）和 **Commit and Push**（提交并推送）至编码防火墙（分支和中心）。

配置 SD-WAN 策略规则

SD-WAN 策略规则指定应用程序和/或服务以及流量分发配置文件，以确定防火墙如何为不属于现有会话、且符合所有其他标准（例如，源和目标区域、源和目标 IP 地址、以及源用户等）的传入数据包选择首选路径。SD-WAN 策略规则还可指定用于延迟、抖动和数据包丢失阈值的路径质量配置文件。一旦超过其中一个阈值，防火墙将为应用程序和/或服务检测一条新路径。

监控您的 SD-WAN 流量时，将根据推送到中心设备的 SD-WAN 策略，评估源自中心设备下游的源的流量在进入中心设备时的状况。此外，因为已经做出路径选择，分支设备无法根据 SD-WAN 策略，在流量通过分支设备流向最终目标设备时对其进行评估。相反，将根据推送到分支设备（而非中心设备）的 SD-WAN 策略，评估源自分支设备下游的源的流量状况。Panorama™ 管理服务器聚合中心和分支的日志，对于相同的流量，会显示两个会话条目，但仅最初用于评估流量的 SD-WAN 设备包含 SD-WAN 详细信息。

在 SD-WAN 策略规则中，您可以引用纠错配置文件，以便为对丢弃或损坏的数据包具有低容忍度的指定关键应用程序应用转发纠错 (FEC) 或数据包重复。

在 SD-WAN 策略规则中，还可以指定想让 Panorama 推送此规则的设备。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Policies**（策略） > **SD-WAN**，然后从 **Device Group**（设备组）上下文下拉列表中选择合适的设备组。

STEP 3 | **Add**（添加）SD-WAN 策略规则。

STEP 4 | 在 **General**（常规）选项卡上，输入规则的描述性 **Name**（名称）。

STEP 5 | 在 **Source**（源）选项卡上，配置策略规则的源参数。

1. 添加 **Source Zone**（源区域）或选择 **Any**（任何）源区域
2. **Add**（添加）一个或多个源地址，建立一个 external dynamic list（外部动态列表）(EDL)，或选择 **Any**（任何）源地址。
3. **Add**（添加）一个或多个源用户，或选择 **any**（任何）源用户。

STEP 6 | 在 **Destination**（目标）选项卡上，配置策略规则的目标参数。

1. **Add**（添加） **Destination Zone**（目标区域），或选择 **Any**（任何）目标区域。
2. **Add**（添加）一个或多个目标地址，建立 EDL，或选择 **Any**（任何） 目标地址。

STEP 7 | 在 **Application/Service**（应用程序/服务）选项卡上，附加 SD-WAN 链路管理配置文件并指定应用程序和服务。

PAN-OS 10.0.2 只支持关联 *SaaS* 质量配置文件或纠错，但不同时支持两者。如果将其中一个配置文件与 *SD-WAN* 策略规则关联，则无法将另一个配置文件与之关联。

例如，如果将 *SaaS* 质量配置文件与 *SD-WAN* 策略规则关联，则无法将纠错配置文件与同一 *SD-WAN* 策略规则关联。

1. 选择 **Path Quality**（路径质量）或创建路径质量配置文件。
2. 如果分支防火墙具有到 SaaS 应用程序的直接互联网访问 (DIA) 链路，请选择 **SaaS Quality Profile**（**SaaS** 质量配置文件）或创建一个 SaaS 质量配置文件。默认为 **None**（无）（已禁用）。
3. 选择 **Error Correction Profile**（纠错配置文件）或创建纠错配置文件以将转发纠错 (FEC) 或数据包重复应用于与 SD-WAN 策略规则匹配的应用程序。默认为 **None**（无）（已禁用）。
4. **Add Applications**（添加应用程序），然后从列表中选择一个或多个应用程序，或选择 **Any**（任何）应用程序。您选择的所有应用程序都受限于您选中的路径质量配置文件中指定的运行状况阈值。如果数据包与其中一个应用程序匹配，且该应用程序超出路径质量配置文件中其中一个运行状况阈值（并且，该数据包与其与规则条件匹配），则防火墙选择新的首选路径。

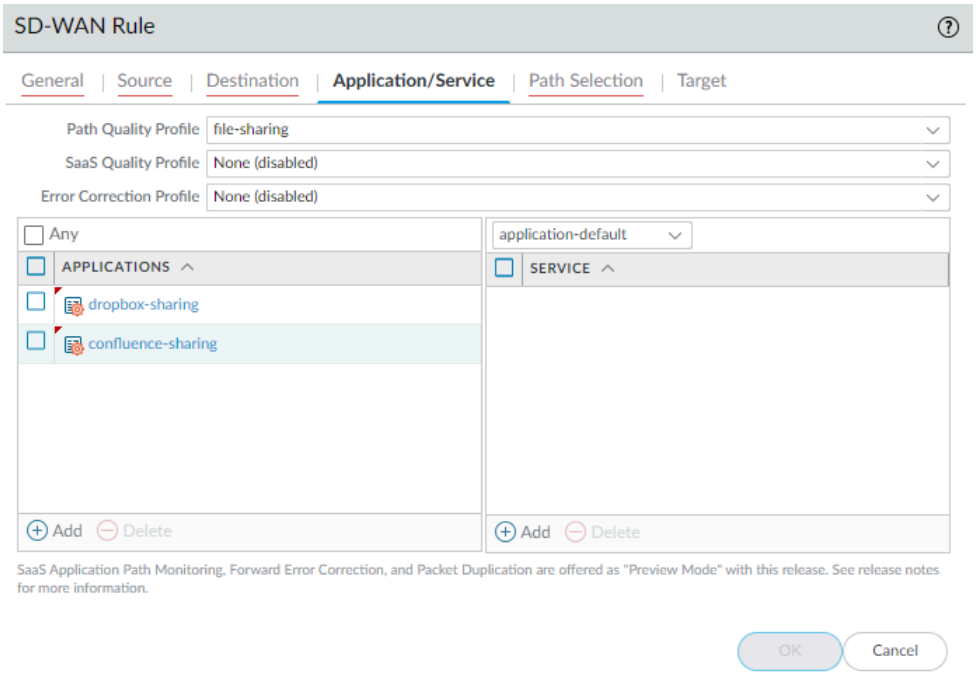
   仅添加关键业务应用和对路径条件敏感的应用，以保证其可用性。

   如果将 ***Adaptive***（自适应）模式下的 SaaS 质量配置文件与 *SD-WAN* 策略关联，请添加要监控的特定 *SaaS* 应用程序。对匹配 *SD-WAN* 策略规则的所有应用程序使用自适应监控可能会影响 *SD-WAN* 防火墙的性能。

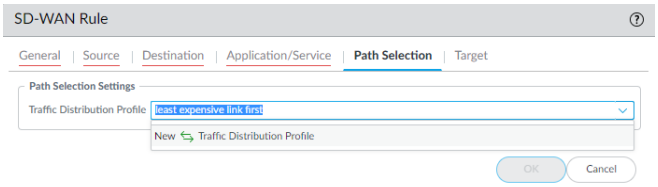
   如果将 SaaS 质量配置文件与指定的 *SaaS* 应用程序关联，请将 *SaaS* 应用程序添加到 *SD-WAN* 规则，以确保 *SaaS* 监控设置仅应用于所需的 *SaaS* 应用程序。
5. **Add Services**（添加服务），然后从列表中选择一个或多个服务，或选择 **Any**（任何）服务。您选择的所有服务都受限于您选中的路径质量配置文件中指定的运行状况阈值。如

果数据包与其中一个服务匹配，且该服务超出路径质量配置文件中其中一个运行状况阈值（并且，该数据包与其与规则条件匹配），则防火墙选择新的首选路径。

仅添加关键业务服务和对路径条件敏感的服务，以保证其可用性。

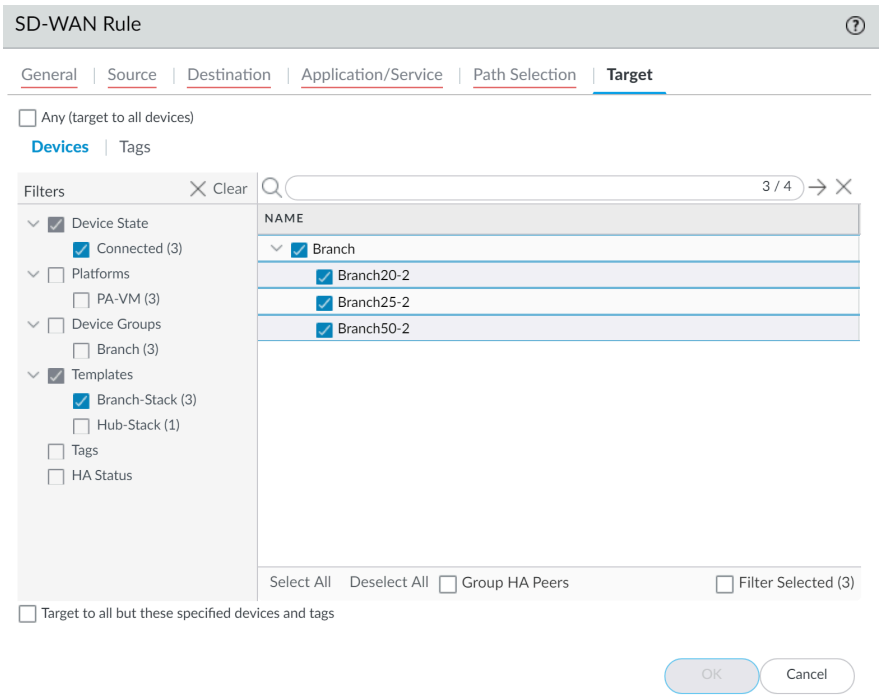


STEP 8 | 在 **Path Selection**（路径选择）选项卡上，选择 **Traffic Distribution**（流量分发）配置文件或创建流量分发配置文件。如果与会话无关的传入数据包与规则中的所有匹配条件匹配，则防火墙使用此流量分发配置文件选择新的首选路径。

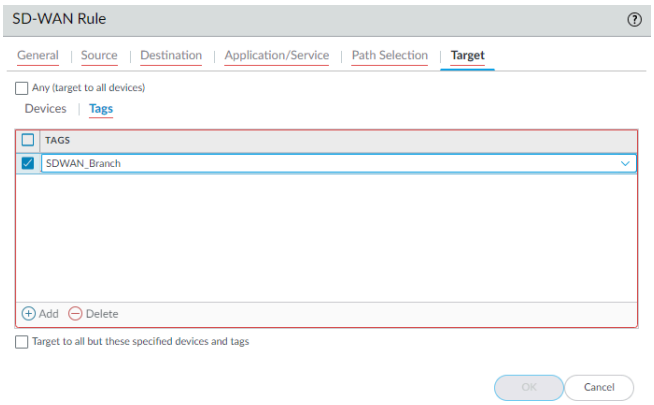


STEP 9 | 在 **Target**（目标）选项卡上，使用以下方法之一指定设备组中的目标防火墙，Panorama 将 SD-WAN 策略规则推送到该设备组。

- 选择 **Any (target to all devices)**（任何（针对所有设备））（默认）以推送规则到所有设备。或者，选择 **Devices**（设备）或 **Tags**（标记）以指定 Panorama 推送 SD-WAN 策略规则的设备。
- 在 **Devices**（设备）选项卡上，选择一个或多个筛选器，以限制名称字段中出现的选择；然后选择一个或多个 Panorama 推送此规则的设备；如本例所示：



- 在 **Tags**（标记）选项卡中，**Add**（添加）一个或多个 **Tags**（标记），并选择标记以指定 Panorama 推送规则到带选中标记的设备，如本例所示：



- 如果已指定设备或标记，您可以选择 **Target to all but these specified devices and tags**（除这些指定设备和标记以外的所有目标），使 Panorama 推送 SD-WAN 策略规则到除指定设备或标记设备以外的所有设备。

STEP 10 | 单击 **OK**（确定）。

STEP 11 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 12 | （最佳实践）创建一个全面的 SD-WAN 策略规则以分发不匹配会话，这样，您可以控制任何未匹配会话使用的链路，查看 SD-WAN 插件日志记录和报告中的未匹配会话。

如果未创建一个全面的规则来分发未匹配会话，则防火墙将以轮询调度方式，在所有可用链路之间分发这些会话，原因是未配置用于未匹配会话的流量分发配置文件。采用轮询调度的方式分发未匹配会话可能会意外增加成本，导致应用程序的可见性下降。

STEP 13 | SD-WAN 策略规则配置结束后，请创建安全策略规则以允许流量（例如，**bgp** 充当 **Application**（应用程序））从分支流向 Internet，从分支流向中心，以及从中心流向分支。

STEP 14 | （可选）为关键应用程序配置 QoS。

如果 *SD-WAN* 应用程序需要确保带宽容量，或是您不想其他应用程序使用关键业务应用程序的带宽，请创建 *QoS* 规则以正确控制带宽。

STEP 15 | 要在 VPN 集群成员之间自动设置 BGP 路由，请在 SD-WAN 插件中的分支和中心之间配置 BGP 路由，以动态路由实施 SD-WAN 故障转移和负载共享的流量。

或者，如果要在各个防火墙上手动配置 BGP 路由，或是使用单独的 Panorama 模板配置 BGP 路由以获得更多控制，请将插件中的 BGP 信息留空。相反，请配置 BGP 路由。

STEP 16 | 为面向公众的 SD-WAN 虚拟接口配置 NAT。

允许互联网直接接入流量故障转移到 MPLS 链路

在 SD-WAN 分支机构，防火墙执行拆分隧道，从而让带公共 IP 地址的所有应用程序都通过互联网直接接入 (DIA) 接口与 Internet 连接，中心内带私有 IP 地址的应用程序通过 VPN 接口接入。防火墙会根据需要自动将 DIA 应用程序故障转移到中心的 MPLS 私有连接，从而让通向互联网的流量选择一条替代路径从中心到达互联网。为实现这一点，必须执行以下操作：

STEP 1 | 在分支和中心之间创建一个 MPLS 链路。在 创建 SD-WAN 接口配置文件时，中心和分支的链路类型必须均为**MPLS**。

STEP 2 | 如果想让私有流量经过 VPN 隧道，必须启用 SD-WAN 接口配置文件中的 **VPN Data Tunnel Support**（**VPN** 数据隧道支持）。如果禁用 **VPN Data Tunnel Support**（**VPN** 数据隧道支持），则私有数据从 VPN 隧道外经过。

STEP 3 | 为特定应用程序配置 SD-WAN 策略规则，创建路径质量配置文件，并为指定 **Top Down Priority**（自上而下优先级）的方法创建流量分发配置文件。流量分发配置文件还必须指定一个 **MPLS** 链路，充当故障转移选项之一（按标记标识）。验证 SD-WAN 策略规则中的应用程序是否引用了正确的路径质量和流量分发配置文件，且流量分发配置文件是否指定自上而下优先级。

启用中心和分支上的 VPN 数据隧道支持，且 MPLS 链路运行后，防火墙根据需要自动使用 MPLS 连接实现 DIA 流量故障转移。

STEP 4 | 在中心配置中，确保中心具有通往 Internet 的路径，且已为中心流量设置正确的，通往 Internet 的路由。

防火墙使用 DIA 虚拟接口和 VPN 虚拟接口，以确保同一路径中公共 Internet 流量与私有流量相分离；即，Internet 流量和私有流量不会经过相同的 VPN 隧道。具有适当分区的完全分段充分发挥作用。

配置 DIA AnyPath

当来自 ISP 的 SD-WAN 直接互联网访问 (DIA) 链路遇到断电或供电不足时，您需要将这些链路故障转移到另一个链路以确保业务连续性。DIA 链路可以故障转移到 MPLS 链路，但可能没有 MPLS 链路。DIA 链路必须能够故障转移到另一个具有到互联网的直接路径或间接路径（通过中心或分支）的链路；DIA 流量可以通过任何可用路径到达互联网，并不限于 DIA。DIA AnyPath 支持 DIA 链路故障转移到进入中心防火墙的专用 VPN 隧道，然后到达互联网。此外，如果您的拓扑结构是全网状（分支到分支）且没有中心，那么 DIA 流量可以故障转移到分支防火墙以到达互联网。

DIA AnyPath 需要 PAN-OS 10.0.3 或更高的 PAN-OS 版本以及兼容的 SD-WAN 插件版本，如兼容性矩阵的 Panorama 插件部分的 SD-WAN 表所示。

希望互联网链路故障转移到 VPN 隧道 (DIA AnyPath) 的用例有几种：

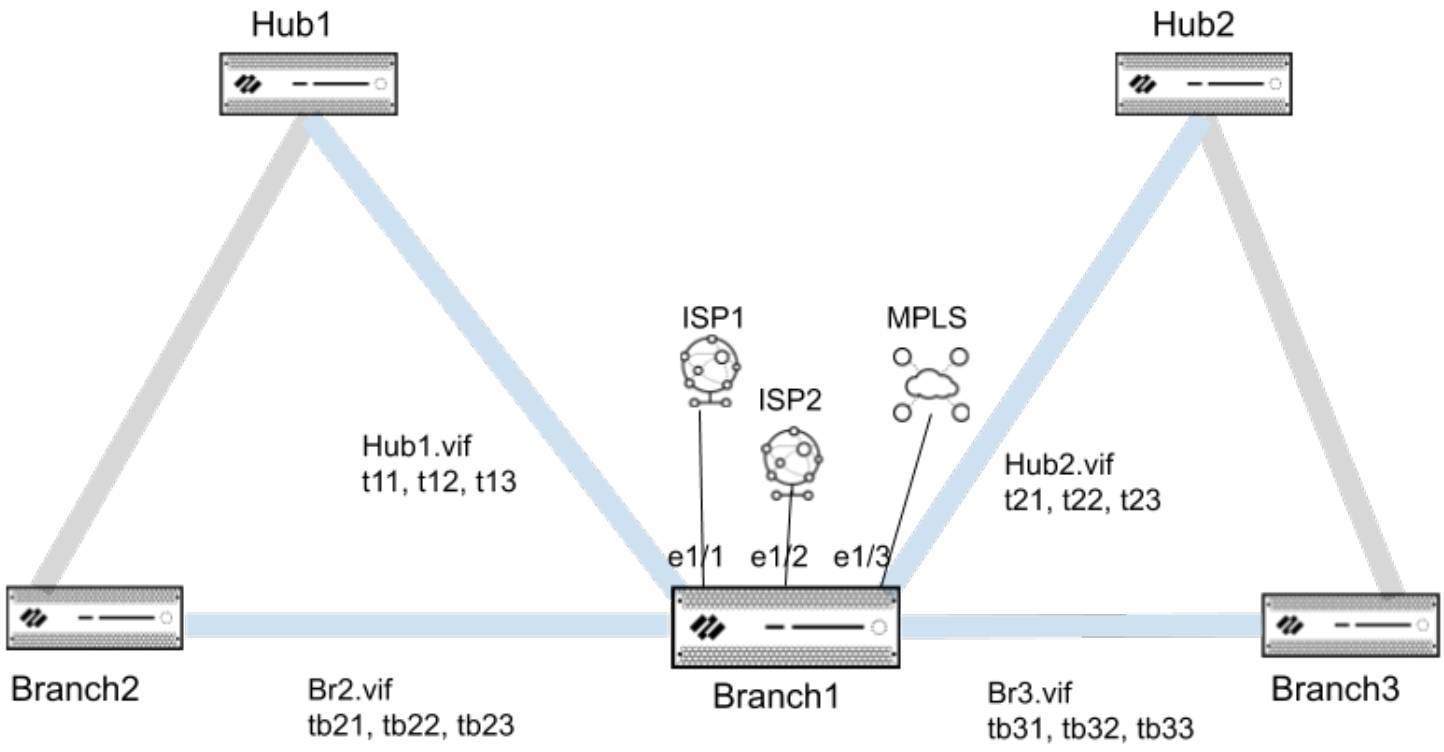
- 您希望从昂贵的 MPLS 链路过渡到通常来自不同供应商的一个或多个公共互联网连接。
- VPN 集群中有多个中心，允许从主中心到一系列备份中心的瀑布式故障转移。
- 在拆分隧道方案中，您只希望特定的带宽密集型应用程序通过分支的 DIA 链路直接连接到互联网，而不是通过 VPN 隧道返回到数据中心，从而节省 WAN 带宽成本。在 DIA 供电不足或断电的情况下，此应用程序流量将故障转移到数据中心以到达互联网；如果需要，可以随后故障转移到第二个中心以到达互联网。
- 在另一种拆分隧道方案中，您希望大部分互联网流量都通过 DIA 链路出去，而不是将流量回程到数据中心进行互联网分路。但是，您希望特定的应用程序（可能需要其他安全设备进行额外的扫描或记录）返回到数据中心。您可以创建一个 SD-WAN 策略规则，将这些应用程序定向到中心的主路径，而不是由防火墙路由表中的默认路由确定的普通 DIA 链路。在供电不足或断电的情况下，这些应用程序将故障转移到分支的 DIA 接口。

DIA AnyPath 引入了主体虚拟接口的概念，该主体虚拟接口可以包括 DIA 链路和嵌套的中心虚拟接口以及分支虚拟接口（VPN 隧道），每个虚拟接口都包含自己的链路。主体虚拟接口最多可以有九个 DIA（以太网）接口、中心虚拟接口和分支虚拟接口。将中心设备添加到 Panorama 时，可以将链路标记分配给中心。假设您使用 SD-WAN 插件，Auto VPN 会将该链路标记分配给中心虚拟接口，从而允许您在流量分发配置文件中指定该标记，以控制虚拟接口之间的故障转移顺序。

主体虚拟接口在 *CLI* 命令中称为 *DIA-VIF*。

主体虚拟接口可以具有属于不同安全区域的接口成员。但是，最佳做法是让主体虚拟接口中的所有成员接口都属于同一安全区域。另一个最佳做法是让主体虚拟接口中至少一个成员接口的链路类型为以太网、电缆模式、*ADSL*、光纤、*LTE* 或 *WiFi*。

下面的拓扑结构示例显示具有两个 ISP 连接和一个 MPLS 链路的 Branch1。Branch1 还有一个 Hub1 虚拟接口（其中 3 个 VPN 隧道连接到 Hub1）和一个 Hub2 虚拟接口（其中 3 个 VPN 隧道连接到 Hub2）。Branch1 还有一个 Branch2 虚拟接口（其中 3 个 VPN 隧道连接到 Branch2）和一个 Branch3 虚拟接口（其中 3 个 VPN 隧道连接到 Branch3）。DIA AnyPath 的目标是配置 DIA 故障转移到 VPN 隧道的顺序，以便直接或间接地到达互联网，从而保持业务连续性。



配置主体虚拟接口时，它将自动成为默认路由，以便将互联网流量正确路由到主体虚拟接口的任何成员（DIA 链路和 VPN 隧道）。路径选择基于 SD-WAN 路径质量配置文件和流量分发配置文件，您可以将其设置为使用自上而下的优先级分布方法来控制故障转移顺序。在示例拓扑结构中，流量分发配置文件可以首先列出主体虚拟接口的标记，然后列出 Hub1 虚拟接口的标记，之后再列出 Hub2 虚拟接口的标记。

放大到更深层次的故障转移优先级，中心虚拟接口具有多个隧道成员，因此您需要一种方法来确定成员的故障转移顺序优先级，例如在 LTE VPN 隧道之前优先使用宽带 VPN 隧道。使用应用于以太网接口的 SD-WAN 接口配置文件中的 **Vpn Failover Metric**（**Vpn** 故障转移指标）指定优先级。指标值越低，故障转移时要选择的隧道的优先级就越高。在拓扑结构示例中，在 Hub1 虚拟接口中，t11 的 VPN 故障转移指标比 t12 的低，导致互联网流量先于 t12 故障转移到 t11。如果虚拟接口中的多个隧道具有相同的指标，SD-WAN 将以循环方式向隧道发送新的会话流量。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 为捆绑在中心虚拟接口或分支虚拟接口中的 VPN 隧道指定故障转移优先级。

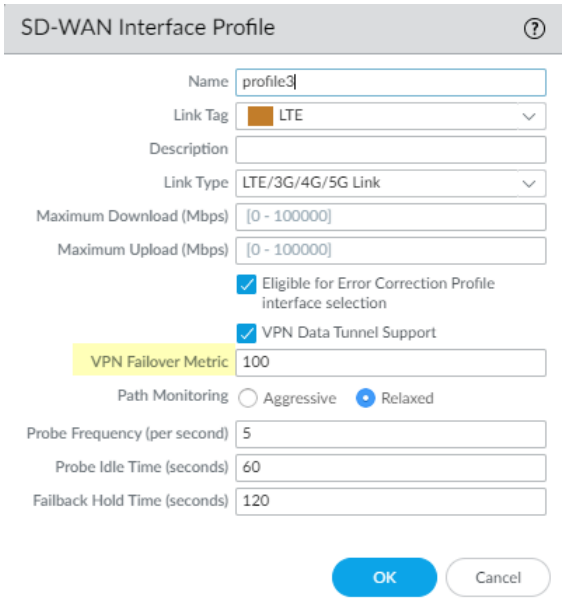
1. 选择或配置 SD-WAN 接口配置文件。

   最佳做法是至少配置一个链路类型为以太网、电缆调制解调器、*ADSL*、光纤、*LTE* 或 *WiFi* 的接口。

2. 必须启用 **VPN Data Tunnel Suppor**（**VPN** 数据隧道支持）。
3. 指定 VPN 隧道的 **VPN Failover Metric**（**VPN** 故障转移指标）；范围为 1-65,535；默认为 10。指标值越低，应用此配置文件的 VPN 隧道（链路）优先级越高。

   例如，将此指标设为一个较低的值，并应用配置文件到宽带接口；然后创建一个不同的配置文件，该配置文件会设置一个较高的指标，以将其应用到昂贵的 LTE 接口，确保仅在宽带完成故障转移后才会使用此接口。

   如果中心只有一条链路，则该链路支持所有虚拟接口和 *DIA* 流量。如果要按特定顺序使用链路类型，则必须将流量分发配置文件应用于指定自上而下优先级的中心，然后对链路标记进行排序以指定首选顺序。如果应用的是指定最佳可用路径的流量分发配置文件，则无论成本如何，防火墙都将使用该链路来选择性能最佳的分支路径。总之，流量分发配置文件中的链路标记，即应用于中心虚拟接口的链路标记（此任务中的第 *6* 步）和 ***VPN*** 故障转移衡量指标仅在流量分发配置文件指定自上而下优先级时才起作用。



4. 单击 **OK**（确定）。

STEP 3 | 配置 SD-WAN 物理以太网接口并在 SD-WAN 选项卡上，应用在上一步中创建的 SD-WAN 接口配置文件。

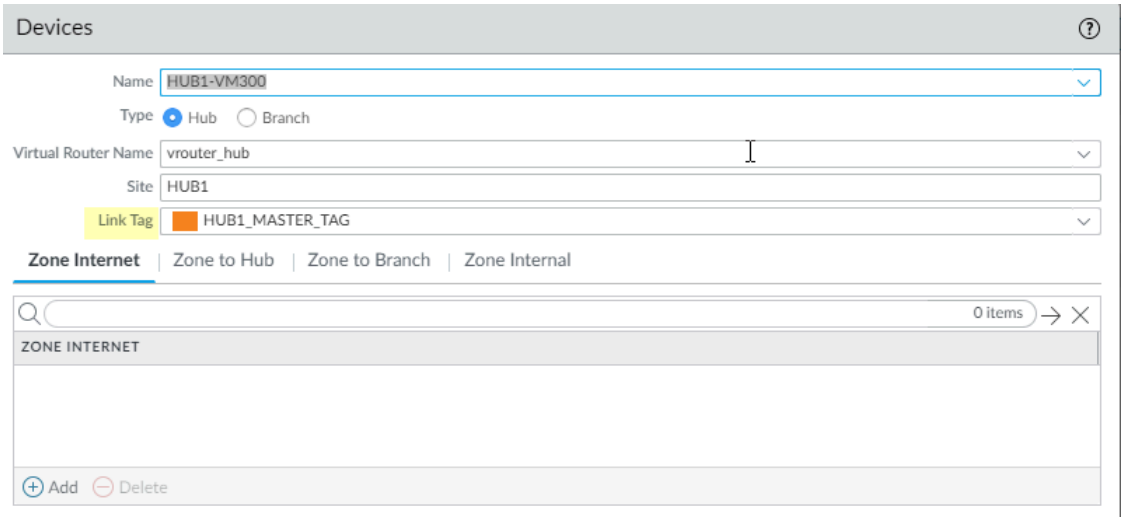
最佳做法是让主体虚拟接口中的所有接口都属于同一安全区域。

STEP 4 | 重复步骤 2 和 3 以使用不同的 VPN 故障转移指标配置其他 SD-WAN 接口配置文件，并将这些配置文件应用于不同的以太网接口，以确定链路发生故障转移的顺序。

STEP 5 | 创建链路标记以用于中心虚拟接口。

STEP 6 | 将链路标记添加到要参与 DIA AnyPath 的中心。

1. 在 **Panorama** > **SD-WAN** > **Devices**（设备）中，添加 SD-WAN 设备以添加要由 Panorama 管理的中心。
2. 选择中心。
3. 选择在上一步中创建的 **Link Tag**（链路标记），自动 VPN 将应用于整个中心虚拟接口，而不是单个链路。因此，您可以在流量分发配置文件中引用此链路标记，以指示用于 DIA AnyPath 故障转移顺序的中心虚拟接口。在分支设备上，自动 VPN 将使用此标签填充终止于中心设备的 SD-WAN 虚拟接口的链路标签字段。



4. 单击 **OK**（确定）。

STEP 7 | 重复步骤 5 和 6，为每个中心虚拟接口创建链路标记，并将该标记添加到将参与 DIA AnyPath 的每个中心。对所有分支虚拟接口执行相同的操作。

STEP 8 | 创建流量分发配置文件以实现 DIA AnyPath。

1. 创建流量分发配置文件.
2. 选择 **Top Down Priority**（自上而下优先级）。
3. 添加链路标记，使它们按您希望其关联链路用于故障转移的顺序显示。

   例如，如果您的用例是让某些应用程序首先使用 DIA，则首先列出 DIA 标记，然后列出中心虚拟接口标记，之后再列出第二个中心虚拟接口标记。如果您的用例是让某些应用程序先转到中心，然后再转到互联网，请首先列出中心虚拟接口，然后或许列出第二个中心虚拟接口，最后列出 DIA 标记。如果您的全网状结构没有中心，请按所需顺序使用 DIA 标记和分支虚拟接口标记。

STEP 9 | 为中心和分支防火墙创建同名的 SaaS 质量配置文件。

必须在中心和分支防火墙上配置两个同名的 SaaS 质量配置文件，以成功将中心防火墙用作备用故障转移。

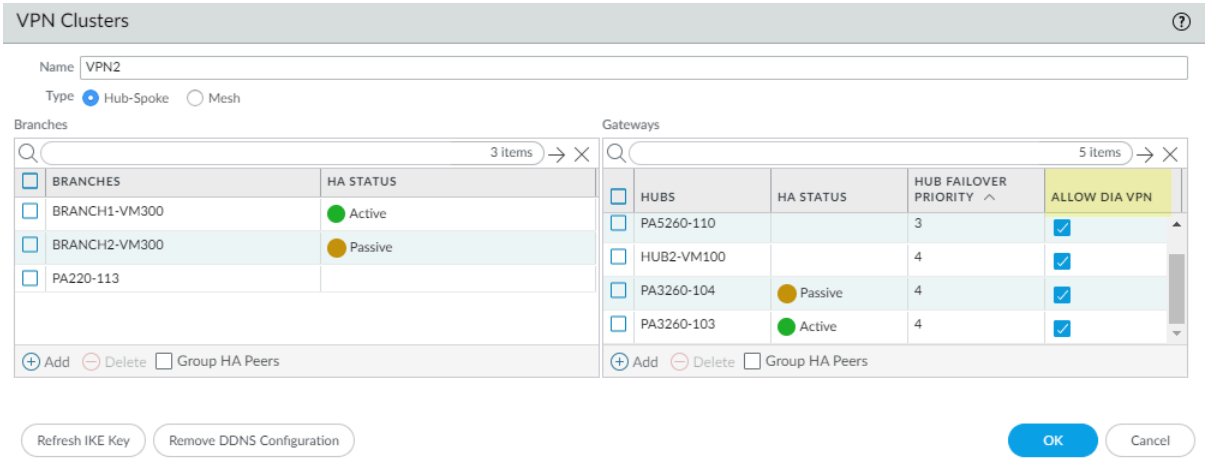
配置故障转移到具有相同 SaaS 应用程序目标的中心防火墙的最简单方法是在共享设备组中创建单个 SaaS 质量配置文件。或者，您可以在不同的设备组中创建两个同名的 SaaS 质量配置文件，并将其推送至您的中心和分支防火墙。

要故障转移到具有不同 SaaS 应用程序目标的中心防火墙，请创建两个同名且指向不同设备组中的不同 SaaS 应用程序目标的 SaaS 质量配置文件，并将它们推送至您的中心和分支防火墙。

您还必须创建引用此 *SaaS* 质量配置文件的 *SD-WAN* 策略规则，以便允许中心向分支通告 *SaaS* 质量配置文件的链路质量统计信息。这样做将通过中心提供端到端 *SaaS* 监控。如果没有此 *SD-WAN* 策略规则，您将只有从分支到中心的链路测量，而无从中心到 *SaaS* 应用程序的链路测量。

STEP 10 | 允许中心参与 DIA AnyPath。

1. 创建 VPN 集群并选择一个中心。
2. 为中心选择 **Allow DIA VPN**（允许 **DIA VPN**）。最多支持四个中心（参与 DIA AnyPath 和 Prisma Access 中心的 PAN-OS 中心的任意组合）。如果它们是 HA 中心，则共支持八个中心。如果您对一对中的一个 HA 对等设备 **Allow DIA VPN**（允许 **DIA VPN**），则必须为另一个 HA 对等设备也启用该项。



STEP 11 | 为特定应用程序创建 SD-WAN 策略规则以使用 DIA AnyPath。

1. 配置 SD-WAN 策略规则.
2. 在 **Application/Service**（应用程序/服务）选项卡上，指定要为其实现 DIA AnyPath 的应用程序和服务。
3. 关联您在上一步中创建的 **SaaS Quality Profile**（**SaaS** 质量配置文件）。

   如果要配置具有不同 SaaS 应用程序目标的 SaaS 质量配置文件，则必须将 SaaS 质量配置文件与每个分支和中心设备组中的 SD-WAN 策略规则关联。
4. 在 **Path Selection**（路径选择）选项卡上，选择您为应用程序创建的 **Traffic Distribution Profile**（流量分发配置文件）。

STEP 12 | 路由不匹配任何 SD-WAN 策略规则的新会话以及在 Panorama 或防火墙配置更改期间到达的会话。

1. 创建适当的路径质量配置文件和流量分发配置文件来处理此类会话。
2. 配置 SD-WAN 策略规则这是这些会话的一个全面规则。
3. 将规则放在列表的最后。

STEP 13 | **Commit**（提交）并 **Push to Devices**（推送到设备）。

STEP 14 | 创建安全策略规则，以允许 DIA 流量流入名为从区域到互联网和从区域到中心的 **Destination Zones**（目标区域），并指定受该规则约束的 **Applications**（应用程序）。提交并推送到分支。

STEP 15 | 使用以下 CLI 命令监控 DIA 信息：

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>**

分发不匹配会话

防火墙尝试将到达 SD-WAN 虚拟接口的的会话与 SD-WAN 策略规则进行匹配；防火墙按自上而下的顺序检查 SD-WAN 策略规则，这与安全策略规则采用的顺序一致。

- 如果与 SD-WAN 规则匹配，防火墙将对此 SD-WAN 安全规则执行路径监控和流量分发。
- 如果不与列表中的任何 SD-WAN 策略规则匹配，则会话会与列表末尾的隐式 SD-WAN 策略规则进行匹配，该策略规则使用循环调度法在 SD-WAN 接口内的所有链路上分发不匹配会话。

此外，如果没有用于特定应用程序的 SD-WAN 策略规则，防火墙不会跟踪应用程序在特定于 SD-WAN 的可见性工具中的性能，例如 SD-WAN 插件中的日志记录和报告。

隐式策略规则说明如下：

- 假定防火墙有 3 个 SD-WAN 策略规则：一个规则用于指定五个语音应用程序，一个规则用于指定六个视频会议应用程序，一个规则用于指定十个 SaaS 应用程序。
- 视频应用程序会话等会话到达防火墙，与所有 SD-WAN 策略规则都不匹配。因为会话与规则不匹配，因此，防火墙没有应用于会话的路径质量配置文件或流量分发配置文件。
- 因此，防火墙将视频应用程序与隐式规则进行匹配，并将各个视频会话在所有可用的 SD-WAN 链路标记以及防火墙相关链路（这可能是两个宽带链路，即，MPLS 链路和 LTE 链路）中进行分发。会话 1 进入其中一个宽带接口成员，会话 2 进入另一个宽带接口成员，会话 3 进入 MPLS，会话 4 进入 LTE，会话 5 进入第一个宽带接口成员，会话 6 进入第二个宽带接口成员，且循环调度分发将继续。

您可能不希望让不匹配会话求助于匹配隐式 SD-WAN 规则，原因在于您对此会话分发没有控制权。相反，我们建议您创建一个全面的 SD-WAN 策略规则，并将其置于 SD-WAN 策略规则列表的最后。通过一个全面的 SD-WAN 策略规则，您可以：

- 控制不匹配会话使用的链路。
- 在 SD-WAN 插件的日志记录和报告中查看防火墙上所有应用程序（包括不匹配应用程序会话）。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 创建路径质量配置文件设置非常高、且永远不会被超过的延迟、抖动和数据包丢失阈值。例如，2000ms 延迟，1000ms 抖动，和 99% 数据丢失。

STEP 3 | 创建流量分发配置文件指定您要使用的 SD-WAN 链路标记，并以不匹配会话使用与这些链路标记关联的链路的顺序。

如果您完全不希望不匹配应用程序使用指定路径（物理接口），请从流量分发配置文件的链路标记列表中删除包含此链路的标记。例如，如果您不想电影流等不匹配应用程序使用昂贵的 *LTE* 链路，请从流量分发配置文件的链路标记列表中删除 *LTE* 链路的链路标记。

STEP 4 | **Add**（添加）一个全面的 SD-WAN 策略规则，然后在 **Application/Service**（应用程序/服务）选项卡上，指定您创建的 **Path Quality Profile**（路径质量配置文件）。

STEP 5 | 选择 **Any**（任何）用于 **Applications**（应用程序）和 **Service**（服务）。

STEP 6 | 在 **Path Selection**（路径选择）选项卡上，选择您创建的 **Traffic Distribution Profile**（流量分发配置文件）。

STEP 7 | 将规则向下**Move**（移动）到 SD-WAN 策略规则列表的最后一位。

STEP 8 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的配置更改。

STEP 9 | **Commit**（提交）更改。

添加 SD-WAN 设备到 Panorama

添加一个 SD-WAN 中心或分支防火墙，使用 CSV 批量导入多个 SD-WAN 中心和分支防火墙。

- 添加 SD-WAN 设备
- 批量导入多个 SD-WAN 设备
- Prisma Access 板载 PAN-OS 防火墙

添加 SD-WAN 设备

添加一个由 Panorama™ 管理服务器进行管理的 SD-WAN 中心或分支防火墙。添加设备时，请指定设备类型（分支或中心）和每个设备的站点名称，以便于识别。添加设备之前，请计划您的 SD-WAN 配置，确保您拥有全部所需 IP 地址，且充分理解了该 SD-WAN 拓扑结构。这有助于减少任何配置错误。

如果您的 Palo Alto Networks®防火墙拥有一个预先存在区域，您可以将其映射到 SD-WAN 中使用的预定义区域。

如果想在两个分支防火墙或两个中心防火墙之间运行主动/被动 *HA*，此时不得将这些防火墙作为 *SD-WAN* 设备添加。您可以在配置 SD-WAN HA 设备时将它们作为 *HA* 对等设备单独添加。

如果使用 *BGP* 路由，必须添加安全策略规则，允许 *BGP* 从内部区域进入中心区域，从中心区域进入内部区域。如果使用 *4* 字节 *ASN*，必须首先启用用于虚拟路由器的 *4* 字节 *ASN*。

查看 *SD-WAN* 设备时，如果没有数据或屏幕指示 *SD-WAN* 未定义，请在 Compatibility Matrix（兼容性矩阵）中检查您正在使用的 *Panorama* 版本是否支持您尝试使用的 *SD-WAN* 插件版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Devices**（设备），然后 **Add**（添加） 新的 SD-WAN 防火墙。

STEP 3 | 选择受管防火墙 **Name**（名称），将其作为 SD-WAN 设备添加。在将 SD-WAN 防火墙作为 SD-WAN 设备添加之前，必须先将 SD-WAN 防火墙作为受管设备添加。

STEP 4 | 选择 SD-WAN 设备的 **Type**（类型）。

- **Hub**（中心）— 部署在主要机构或位置的集中防火墙，所有分支设备通过 VPN 连接与其相连接。分支之间的流量经过中心再前往目标分支，并在中心位置将分支与集中资源相连。中心设备在主要机构或位置处理流量、实施策略规则，并管理链路交换。
- **Branch**（分支）— 部署在物理分支位置的防火墙，它通过 VPN 连接与中心相连接，并提供分支级别的安全保障。分支设备在分支位置处理流量、实施策略，并管理链路交换。

STEP 5 | 选择用于在 SD-WAN 中心和分支之间进行路由的 **Router Name**（路由器名称）。默认情况下，将创建一个 `sdwan-default` 虚拟路由器，促使 Panorama 自动推送路由器配置。

（已启用 **Advanced Routing**（高级路由））如果已配置高级路由，并且已成功创建逻辑路由器，则 **Router Name**（路由器名称）将显示虚拟路由器和逻辑路由器名称：

- 如果虚拟路由器和逻辑路由器名称相同，则 **Router Name**（路由器名称）将显示同一个名称。因为默认情况下，高级路由会创建与虚拟路由器同名的逻辑路由器。使用高级路由引擎时，逻辑路由器名称必须与同一模板的虚拟路由器名称相同。
- 如果虚拟路由器和逻辑路由器名称不同（仅在手动更新逻辑路由器名称时会出现这种情况），则路由器名称同时显示虚拟路由器名称和逻辑路由器名称。您可以根据需要选择虚拟路由器（用于旧版引擎）或逻辑路由器（用于高级路由引擎）。如果您尚未启用 **Advanced Routing**（高级路由），则在 **Router Name**（路由器名称）中只有虚拟路由器（用于旧版引擎）供您选择。

STEP 6 | 输入 SD-WAN **Site**（站点）名称，以确定设备的物理地理位置或用途。

SD-WAN 站点名称支持所有大小写字母数字和特殊字符。不得在站点名称中使用空格，否则会导致该站点的监控（***Panorama*** > ***Monitoring***（监控））数据无法显示。

所有 *SD-WAN* 设备（包括高可用性 *(HA)* 配置中的 *SD-WAN* 设备）必须具有唯一的站点名称。

STEP 7 | 选择为中心虚拟接口（或分支虚拟接口）创建的 **Link Tag**（链路标记），Auto VPN 会将其分配给虚拟接口。您将在流量分发配置文件中使用此链路标记，以允许中心（或分支）参与 DIA AnyPath。

STEP 8 | 如果要在为中心执行 NAT 的设备后方添加一个中心，必须指定该上游 NAT 执行设备上面向公众的接口的 IP 地址或 FQDN，这样，自动 VPN 配置可使用此地址充当中心的隧道端点。分支机构的 IKE 和 IPSec 流必须可以抵达该 IP 地址。（您必须已经 为 SD-WAN 配置一个物理以太网接口。）

1. 在 **Upstream NAT**（上游 **NAT**） 选项卡中，启用**Upstream NAT**（上游 **NAT**）。
2. **Add**（添加） **SD-WAN interface**（**SD-WAN** 接口）；选择已为 SD-WAN 配置的接口。
3. 选择 **IP Address**（**IP** 地址） 或 **FQDN**，然后分别输入不带子网掩码的 IPv4 地址（例如，192.168.3.4），或是上游设备的 FQDN。

4. 单击 **OK**（确定）。

   此外，在执行 *NAT* 的上游设备上，您还必须使用一对一 *NAT* 策略设置入站目标 *NAT*，且不得配置 *IKE* 或 *IPSec* 通信流量端口转换。

   如果上游设备的 *IP* 地址发生更改，必须配置新的 *IP* 地址，并将其推送到 *VPN* 集群。您必须在分支和中心上使用 *CLI* 命令 ***clear ipsec***、***clear ike-sa***和 ***clear session all*** 。此外，还必须在配置用于 *IP* 地址的 *NAT* 策略虚拟路由器上使用 ***clear session all***（清除所有会话）命令。

   第 *2* 层接口上不支持上游 *NAT*。

STEP 9 | 如果要在为分支执行 NAT 的设备后面添加一个分支，则必须指定该上游 NAT 执行设备上面向公众的接口的 IP 地址或 FQDN，或者选择 DDNS 以指示 NAT 设备上接口的 IP 地址是从 Palo Alto Networks DDNS 服务中获得的。因此，自动 VPN 配置使用该公共 IP 地址作为分支的隧道端点。分支机构的 IKE 和 IPSec 流必须可以抵达该 IP 地址。（您必须已经 为 SD-WAN 配置一个物理以太网接口。）

1. 在 **Upstream NAT**（上游 **NAT**） 选项卡中，启用**Upstream NAT**（上游 **NAT**）。
2. **Add**（添加） **SD-WAN interface**（**SD-WAN** 接口）；选择已为 SD-WAN 配置的接口。
3. 如果选择 **NAT IP Address Type**（**NAT IP** 地址类型）为 **Static IP**（静态 **IP**），请选择 **IP Address**（**IP** 地址）或 **FQDN**，然后分别输入不带子网掩码的 IPv4 地址（例如，192.168.3.4），或是上游设备的 FQDN。
4. 或者，选择 **NAT IP Address Type**（**NAT IP** 地址类型）为 **DDNS**。

5. 单击 **OK**（确定）。

此外，在执行 *NAT* 的上游设备上，您还必须使用一对一 *NAT* 策略设置入站目标 *NAT*，且不得配置 *IKE* 或 *IPSec* 通信流量端口转换。

如果上游设备的 *IP* 地址发生更改，必须配置新的 *IP* 地址，并将其推送到 *VPN* 集群。您必须在分支和中心上使用 *CLI* 命令 ***clear ipsec***、***clear ike-sa*** 和 ***clear session all***。此外，还必须在配置用于 *IP* 地址的 *NAT* 策略虚拟路由器上使用 ***clear session all***（清除所有会话）命令。

在 *UI* 中还有第二个位置可以为分支配置上游 *NAT*，但以下位置不是首选，您不应该在这两个位置为分支配置上游 *NAT*。配置上游 *NAT* 的第二个非首选位置位于 ***Network***（网络）> ***Interfaces***（接口）> ***Ethernet***（以太网）的 *Panorama* 上，在 ***Template***（模板）字段中选择一个模板，然后选择一个以太网接口，并选择 ***SD-WAN*** 选项卡。此时，您可以 ***Enable***（启用）上游 *NAT*，并选择 ***NAT IP Address Type***（***NAT IP***地址类型）。第二种方法优先。如果首先通过模板堆栈为 *Panorama* 上的以太网接口配置了上游 *NAT*，则 *SD-WAN* 插件不会更改设置，即使您在插件设备配置页面上使用不同的设置。只有在 *Panorama* 上没有通过模板堆栈配置上游 *NAT* 时，上游 *NAT* 的插件配置才会生效。

第 *2* 层接口上不支持上游 *NAT*。

STEP 10 | （对预先存在客户是必须的）将您的预先存在区域映射到 SD-WAN 预定义区域。

在将您的现有区域映射到 *SD-WAN* 区域时，必须修改您的安全策略规则，并添加 *SD-WAN* 区域到正确的 ***Source***（源）和 ***Destination***（目标）。

1. 选择 **Zone Internet**（从区域到互联网），并 **Add**（添加）可将 SD-WAN 流量传出到 Internet 的预先存在区域。
2. 选择 **Zone to Hub**（从区域到中心），并 **Add**（添加）可将 SD-WAN 流量传出到中心的预先存在区域。
3. 选择 **Zone to Branch**（从区域到分支），并 **Add**（添加） 可将 SD-WAN 流量传出到分支的预先存在区域。
4. 选择 **Zone Internal**（从区域到内部），并 **Add**（添加） 可将 SD-WAN 流量传出到内部区域的预先存在区域。

STEP 11 | （PAN-OS 10.2.1 及更高的 11.0 版本，以及 SD-WAN 插件 3.0.1 及更高的 3.0 版本）如果应用程序流量使用服务类型 (ToS) 位或差分服务代码点 (DSCP) 标记进行标记，请将 ToS 字段从内部 IPv4 标头复制到通过 VPN 隧道的封装数据包的外部 VPN 标头，以保留 QoS 信息。

1. 选择 **VPN Tunnel**（**VPN** 隧道）选项卡。
2. 选择 **Copy ToS Header**（复制 **ToS** 标头）。
3. 单击 **OK**（确定）。

STEP 12 | （可选）配置边界网关协议 (BGP) 路由。

要在 VPN 集群成员之间自动设置 BGP 路由，请输入下面的 BGP 信息。如果要在各个防火墙上手动配置 BGP 路由，或是使用单独的 Panorama 模板配置 BGP 路由以获得更多控制，请将下面的 BGP 信息留空。

在已使用 *BGP* 的环境中使用 *BGP* 路由实施 *SD-WAN* 之前，请确保 *SD-WAN* 插件生成的 *BGP* 配置不会与预先存在的 *BGP* 配置冲突。例如，您必须将现有的 *BGP AS* 号码和路由器 *ID* 值作为相应 *SD-WAN* 设备值。如果插件生成的 *BGP* 配置与预先存在的 *BGP* 配置冲突，则预先存在的 *BGP* 配置优先。如果您希望推送的配置优先，则必须在执行 *Panorama* 推送时启用强制模板值。

1. 选择 **BGP** 选项卡，并启用 **BGP**，以配置用于 SD-WAN 流量的 BGP 路由。
2. 输入 BGP **Router ID**（路由器 **ID**），该 ID 在所有路由器中必须是唯一的。
3. 输入 **AS Number**（**AS** 编号）。自治系统编号指定通常定义的 Internet 路由策略。每个中心和分支位置的 AS 编号必须是唯一的。

STEP 13 | 如果要将配置 BGP 为使用 IPv4，请选择 **IPV4 BGP**。

1. **Enable IPv4 BGP support**（启用 **IPv4 BGP** 支持）。
2. 指定用于 BGP 对等设备的静态 IPv4 **Loopback Address**（回环地址）。通过自动 VPN 配置，可自动创建与指定 IPv4 地址相同地址的回环接口。如果指定一个现有回环地址，则提交将失败，因此，您应指定一个尚不属于回环地址的 IPv4。
3. 如果您的端点需要与 SD-WAN BGP 拓扑中的中心或分支防火墙交换路由，因此不想从 BGP 更新中的 AS_PATH 属性中删除私有 AS 编号（64512 到 65534），请禁用 **Remove Private AS**（删除私有 **AS**）选项（默认值为“启用”）。在这种情况下，您希望允许私有 AS 编号在 BGP 更新中保留 SD-WAN 私有 AS。

   Remove Private AS（删除私有 ***AS***）设置适用于分支或中心防火墙上的所有 *BGP* 对等组。如果需要此设置在 *BGP* 对等组或对等之间有所不同，则必须在 *SD-WAN* 插件之外配置此设置。

   如果更改 ***Remove Private AS***（删除私有 ***AS***）设置，提交到所有 *SD-WAN* 集群节点，然后降级到早于 *2.0.2* 的 *SD-WAN* 插件版本，则与 ***Remove Private AS***（删除私有 ***AS***）相关的所有配置都必须在 *SD-WAN* 插件之外或直接在防火墙上完成。
4. 添加 **Prefix(es) to Redistribute**（要重新分配的前缀）。在中心设备中，您必须至少输入一个要重新分配的前缀。分支设备未设有此选项；会默认对连接到分支位置的子网进行重新分配。

STEP 14 | （SD-WAN 插件 3.1.1 及更高的 3.1 版本） 如果要将配置 BGP 为使用 IPv6，请选择 **IPV6 BGP**。

1. **Enable IPv6 BGP support**（启用 **IPv6 BGP** 支持）。
2. 指定用于 BGP 对等设备的静态 IPv6 **Loopback Address**（回环地址） 。通过自动 VPN 配置，可自动创建与指定 IPv6 地址相同地址的回环接口。如果指定一个现有回环地址，则提交将失败，因此，您应指定一个尚不属于回环地址的 IPv6。
3. 添加 **Prefix(es) to Redistribute**（要重新分配的前缀）。在中心设备中，您必须至少输入一个要重新分配的前缀。分支设备未设有此选项；会默认对连接到分支位置的子网进行重新分配。

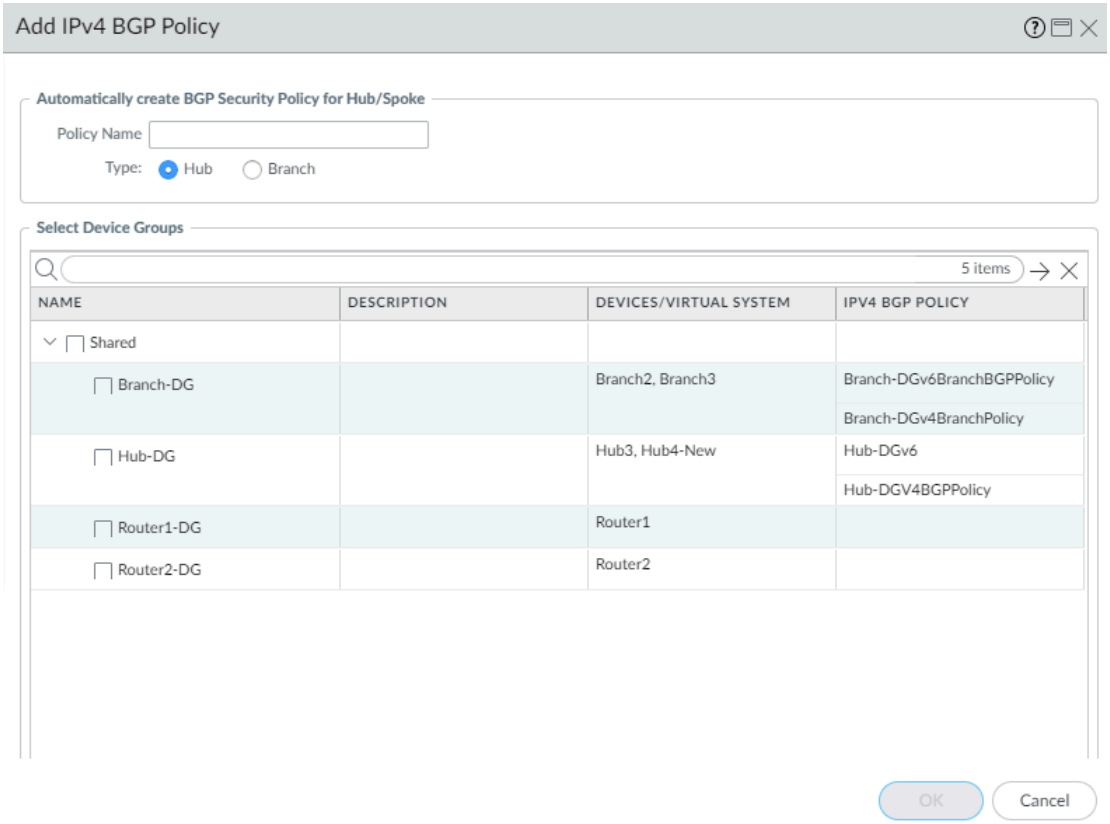
STEP 15 | 单击 **OK**（确定）。

STEP 16 | 选择屏幕底部的 **Group HA Peers**（组 **HA** 对等设备）以显示与 HA 对等设备一起运行的分支（或中心）。

NAME	TYPE	VIRTUAL ROUTER NAME	SITE	HA STATUS
sdwan1-vm500-Hub2-HA1	hub	sdwan1-hub-router	sdwan1-hub1	Active
sdwan1-vm500-Hub2-HA2	hub	sdwan1-hub-router	sdwan1-hub2	Passive
sdwan-vm100-Branch-HA1	branch	sdwan1-vm100-br	sdwan1-branch1	Active
sdwan-vm100-Branch-HA2	branch	sdwan1-vm100-br	sdwan1-branch2	Passive
sdwan2-vm100-Branch-HA1	branch	sdwan2-branch-router	sdwan2-branch 1	Active
sdwan2-vm100-Branch-HA2	branch	sdwan2-branch-router	sdwan2-branch2	Passive
sdwan2-vm300-Hub3-HA1	hub	sdwan2-HUB-router	sdwan2-hub1	Active
sdwan2-vm300-Hub3-HA2	hub	sdwan2-HUB-router	sdwan2-hub2	Passive
sdwan3-PA5250-HUB	hub	sdwan3-Hub-router	sdwan3-hub1	
sdwan3-PA220-Branch-HA1	branch	sdwan3-Branch-router	sdwan3-branch1	Active
sdwan3-PA220-Branch-HA2	branch	sdwan3-Branch-router	sdwan3-branch	Passive

STEP 17 | 通过 Panorama 创建一个允许 BGP 在分支和中心之间运行的安全策略规则，并将其推送到防火墙。

1. 选择屏幕底部的 **IPv4 BGP Policy**（**IPv4 BGP** 策略）或 **IPv6 BGP Policy**（**IPv6 BGP** 策略）（具体取决于您使用的 BGP 地址类型），然后选择 **Add**（添加）策略。
2. 输入 Panorama 将自动创建的安全策略规则 **Policy Name**（策略名称）。
3. 选择 **Type**（类型）作为 **Hub**（中心）或 **Branch**（分支）。
4. **Select Device Group**（选择设备组）以指定 Panorama 推送安全策略规则的目标设备组。
5. 单击 **OK**（确定）。



STEP 18 | 选择 **Push to Devices**（推送到设备）以将您的配置更改推送到受管防火墙。

批量导入多个 SD-WAN 设备

添加多个 SD-WAN 设备（而非一次手动添加一个设备）可快速登录到分支和中心防火墙。添加设备时，请指定设备类型（分支或中心）和每个设备的站点名称，以便于识别。添加设备之前，请计划您的 SD-WAN 配置，确保您拥有全部所需 IP 地址，且充分理解了该 SD-WAN 拓扑结构。这有助于减少任何配置错误。

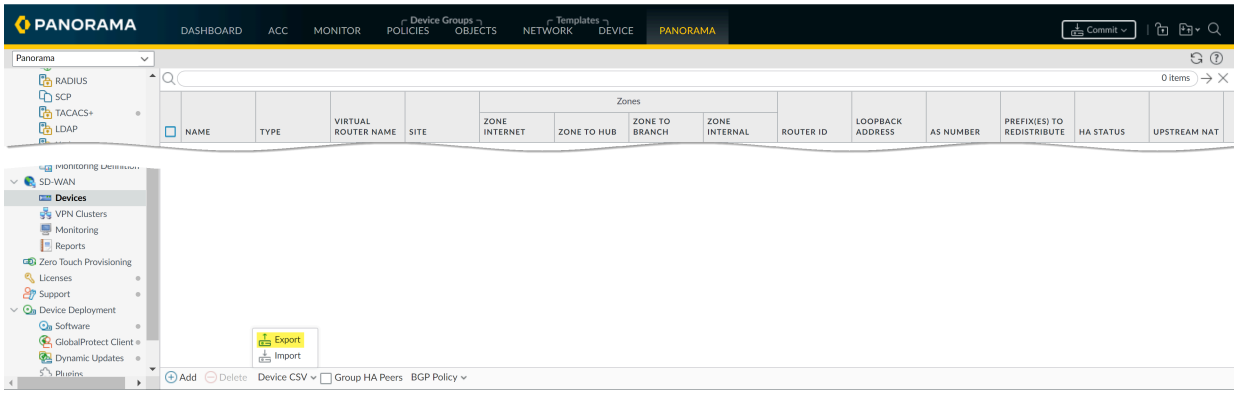
如果想在两个分支防火墙或两个中心防火墙之间运行主动/被动 *HA*，不得在 *CSV* 文件中将这些防火墙作为 *SD-WAN* 设备添加。您可以在配置 SD-WAN HA 设备时将它们作为 *HA* 对等设备单独添加。

如果使用 *BGP* 路由，必须添加安全策略规则，允许 *BGP* 从内部区域进入中心区域，从中心区域进入内部区域。如果想使用 *4* 字节自治系统编号 *(ASN)*，必须首先启用用于虚拟路由器的 *4* 字节 *ASN*。

如果您的 Palo Alto Networks 防火墙拥有一个预先存在区域，您可以将其映射到 SD-WAN 中使用的预定义区域。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Devices**（设备） > **Device CSV**（设备 **CSV**），然后 **Export**（导出） 空的 SD-WAN 设备 CSV。您可以通过此 CSV 一次导入多个分支和中心设备，而不是每次手动添加一个设备。



STEP 3 | 使用分支和中心信息填充 SD-WAN 设备 CSV，然后将其保存。除非另有说明，否则，所有字段均为必填字段。您必须为每个中心和分支输入以下内容：

- **device-serial**（设备序列号）— 分支或中心防火墙的序列号。
- **type**（类型）— 指定设备是分支或中心设备。
- **site**（站点）— 输入 SD-WAN 设备站点名称，以帮助您确定设备的物理地理位置或用途。

  SD-WAN 站点名称支持所有大小写字母数字和特殊字符。不得在站点名字中使用空格，否则会导致该站点的监控（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监控））数据无法显示。

  所有 *SD-WAN* 设备（包括高可用性 *(HA)* 配置中的 *SD-WAN* 设备）必须具有唯一的站点名称。
- （对预先存在客户是必须的）将您的预先存在区域映射到 SD-WAN 预定义区域。

  在将您的现有区域映射到 *SD-WAN* 区域时，必须修改您的 安全策略规则，并添加 *SD-WAN* 区域到正确的 ***Source***（源）和 ***Destination***（目标）。

  - **zone-internet**（从区域到 **Internet**）— 输入预先存在区域的名称，SD-WAN 流量将从该区域传出以通向 Internet。
  - **zone-to-branch**（从区域到分支）— 输入预先存在区域的名称，SD-WAN 流量将从该区域传出以通向分支。
  - **zone-to-hub**（从区域到中心）— 输入预先存在区域的名称，SD-WAN 流量将从该区域传出以通向中心。
  - **zone-internal**（从区域到内部）— 输入预先存在区域的名称，SD-WAN 流量将从该区域传出以通向内部区域。
- （可选）**loopback-address**（回环地址）— 指定用于边界网关协议 (BGP) 对等设备的静态回环 IPv4 地址。
- （可选） **prefix-redistribute**（前缀重新分发）— 输入分支通知中心其可到达的 IP 前缀。要添加多个前缀，请用空格、与符号 (&) 以及空格将前缀分开，例如，192.2.10.0/24 & 192.168.40.0/24。默认情况下，分支防火墙将本地连接的 Internet 前缀通告给中心。

  Palo Alto Networks 不会重新分发从 *ISP* 获得的分支机构默认路由。
- （可选）**as-number**（**AS** 编号）— 输入属于中心或分支虚拟路由器的私有 AS 的 ASN。SD-WAN 插件仅支持私有自治系统。每个中心和分支的 ASN 必须是唯一的。4 字节 ASN 范

围为 4,200,000,000 到 4,294,967,294，或 64512.64512 到 65535.65534。2 字节 ASN 范围为 64512 到 65534。

使用 *4* 字节私有 *ASN*。

在已使用 *BGP* 的环境中使用 *BGP* 路由实施 *SD-WAN* 之前，请确保 *SD-WAN* 插件生成的 *BGP* 配置不会与现有的 *BGP* 配置冲突。例如，您必须将现有的 *BGP AS* 号码和路由器 *ID* 值作为相应 *SD-WAN* 设备值。

- （可选） **router-id**（路由器 **ID**）— 指定 BGP 路由器 ID。所有虚拟路由器或逻辑路由器的 ID 均必须是唯一的。

  输入回环地址作为路由器 *ID*。

  在已使用 *BGP* 的环境中使用 *BGP* 路由实施 *SD-WAN* 之前，请确保 *SD-WAN* 插件生成的 *BGP* 配置不会与现有的 *BGP* 配置冲突。例如，您必须将现有的 *BGP AS* 号码和路由器 *ID* 值作为相应 *SD-WAN* 设备值。

- **vr-name**（**VR** 名称）— 输入用于在 SD-WAN 中心和分支之间进行路由的虚拟路由器或逻辑路由器的名称。默认情况下，Panorama 将创建一个 `sdwan-default` 虚拟路由器，可以自动推送路由器配置。

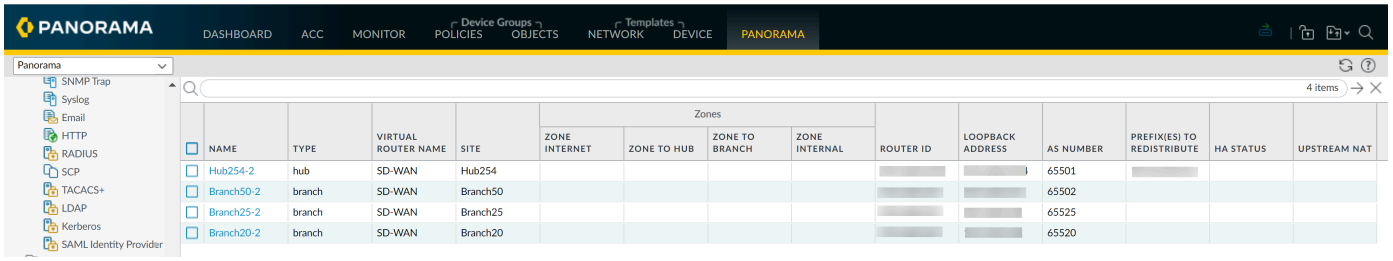
	A	B	C	D	E	F	G	H	I	J	K	L
1	device-serial	type	site	zone-internet	zone-to-branch	zone-to-hub	zone-internal	loopback-addres	prefix-redistribut	as-number	router-id	vr-name
2		branch	Branch20							65520		SD-WAN
3		hub	Hub254							65501		SD-WAN
4		branch	Branch50							65502		SD-WAN
5		branch	Branch25							65525		SD-WAN

STEP 4 | 将 SD-WAN 设备 CSV 导入到 Panorama。

确保 Panorama 上无任何暂挂提交，否则导入将失败。

1. 在 Panorama 上，选择 **Panorama** > **SD-WAN** > **Devices**（设备） > **Device CSV**（设备 **CSV**），然后 **Import**（导入）您在上一步中编辑的 CSV。
2. **Browse**（浏览）并选择 SD-WAN 设备 CSV。
3. 单击 **OK**（确定）以导入 SD-WAN 设备。

STEP 5 | 检验您的 SD-WAN 设备是否已成功添加。



STEP 6 | **Commit**（提交）配置更改。

STEP 7 | 选择 **Push to Devices**（推送到设备）以将您的配置更改推送到受管防火墙。

Prisma Access 板载 PAN-OS 防火墙

SD-WAN 插件 2.2 提供 Prisma Access 中心支持，从而使连接到 Prisma Access 计算节点 (CN) 的 PAN-OS 防火墙可以在 SD-WAN 中心辐射拓扑中实现云端安全。在这种拓扑结构中，SD-WAN 中心作为 Prisma Access CN（IPSec 终端节点），SD-WAN 分支作为 PAN-OS 防火墙。最多支持四个中心（参与 DIA AnyPath 和 Prisma Access 中心的 PAN-OS 中心的任意组合）。SD-WAN 自动创建 IKE 和 IPSec 隧道，以将分支连接到中心。参阅 SD-WAN 和 Prisma Access 的系统要求。

必须先配置 *Prisma Access*，然后配置 *SD-WAN*。

- 如要开始全新的 *Prisma Access* 配置，请阅读 Prisma Access 管理员指南，完成第 *1* 阶段和第 *2* 阶段的配置步骤。
- 如果 *Prisma Access* 已经在运行，请确保第 *1* 阶段已完成，然后完成第 *2* 阶段。

以下流程图显示了两个配置阶段的顺序以及每个阶段中的基本步骤。包含链路和 SD-WAN 配置步骤的 Prisma Access 完整先决条件遵循流程图。

第 **1** 阶段 — **PRISMA ACCESS** （首先完成第 **1** 阶段）	第 **2** 阶段 — **SD-WAN** （完成第 **1** 阶段后再开始）
1. 为租户设置基础架构子网、基础架构 BGP AS、模板堆栈和设备组。 **2.** 为特定区域设置模板堆栈、模板、设备组、信任和不信任区域以及带宽分配。 **3.** 确保您的 Prisma Access 部署已获得访问远程网络的许可。 **4.** 确保您的部署按计算位置分配带宽，而不是按位置分配带宽。 **5.** 确保您已为与您要登录的位置相对应的计算位置分配了带宽。 **6.** 执行本地提交并推送到 Prisma Access 云端。	**1.** 通过启用了 SD-WAN 的接口配置分支防火墙。 **2.** 登录 Panorama Web 界面。 **3.** 为回环地址指定 BGP 本地地址池。 **4.** 选择 SD-WAN 分支防火墙以连接到 Prisma Access 中心并配置连接。 **5.** 提交配置并将其推送到云端。 **6.** 确认已完成登录。 **7.** 将分支防火墙同步到 Prisma Access。 **8.** 提交到 Panorama。 **9.** 推送到设备。 **10.** 查看已创建的新接口。 **11.** 确认 IPSec 隧道已运行。 **12.** 确认 IKE 网关已运行。 **13.** 创建 SD-WAN 策略规则以生成监视数据。 **14.** 提交，然后提交并推送到分支防火墙。 **15.** 监视 Prisma Access 中心应用程序和链路性能。

在将 SD-WAN 连接到 Prisma Access 之前，必须确保有一个分支防火墙的接口已经启用了 SD-WAN 接口。此外，请确保您已为一个或多个租户执行了以下 Prisma Access 先决条件；这些是第 1 阶段的步骤：

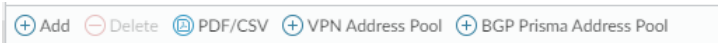
1. 对于 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置），请在 **Service Setup**（服务设置）页面上为租户设置基础架构子网、基础架构 BGP AS、模板堆栈和设备组。
2. 在 **Remote Networks**（远程网络）页面上，为特定区域设置模板堆栈、模板、设备组、信任和不信任区域以及带宽分配。
3. 通过选择 **Panorama** > **Licenses**（许可证）并检查您的许可证信息，确保您的 Prisma Access 部署已获得远程网络访问许可。
   - 2020 年 11 月 17 日之后可用的许可证在 **Net Capacity**（净容量）区域中显示针对远程网络的许可带宽量。
   - 2020 年 11 月 17 日之前可用的许可证在 **Total Mbps**（总 **Mbps**）下方的 **GlobalProtect Cloud Service for Remote Networks**（**GlobalProtect** 远程网络云服务）区域显示可用远程网络带宽。
4. 确保您的部署按计算位置分配带宽，而不是按位置分配带宽。
5. 确保您已为与您要登录的位置相对应的计算位置分配了带宽。您每为一个区域分配 500 Mbps 带宽，Prisma Access 就会分配一个 IPSec 终端节点。
6. 执行本地提交并推送到 Prisma Access 云端。

通过 Prisma Access 执行第 1 阶段的上述步骤后，对 SD-WAN 执行以下第 2 阶段步骤。

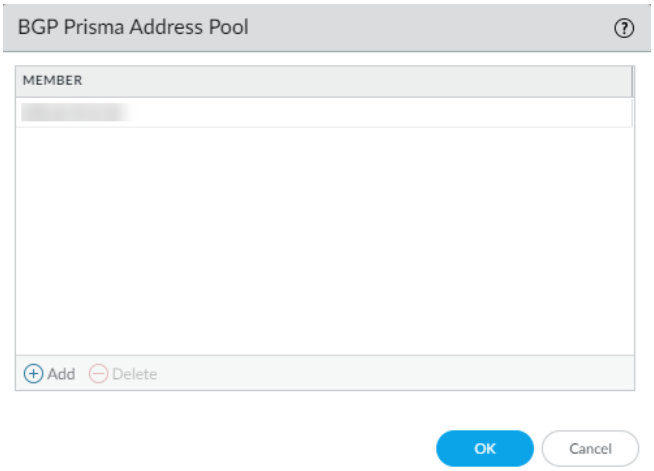
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 为回环地址指定 BGP 本地地址池。

1. 选择 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群）。
2. 在屏幕底部，选择 **BGP Prisma Address Pool**（**BGP Prisma** 地址池）。



3. 为 Prisma Access 的本地 BGP 地址 **Add**（添加）未使用的专用子网（前缀和网络掩码）。



4. 单击 **OK**（确定）。
5. **Commit**（提交）。

如果 *Prisma Access* 已登录，请勿更改现有地址池。如果需要更改地址池，请在维护窗口期间执行以下步骤，以使用变更的地址池更新 *SD-WAN* 分支和 *Prisma Access CN*：

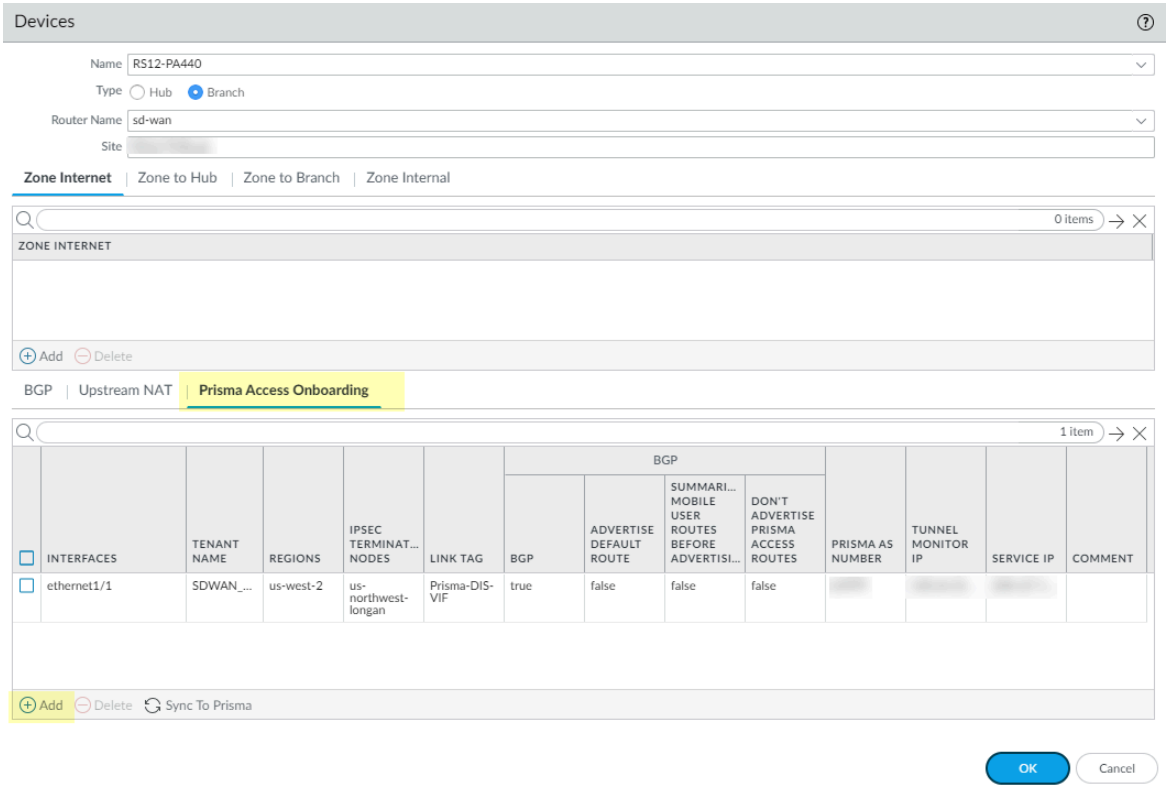
1. 使用 *Panorama* 访问 *SD-WAN* 分支并删除地址池更改将影响的现有登录；然后进行本地提交。
2. 更新 *VPN* 地址池，然后进行本地提交。
3. 再次执行 *Prisma Access* 登录，然后执行本地提交和推送。

STEP 3 | 选择 SD-WAN 分支防火墙以连接到 Prisma Access 中心并配置连接。

1. 选择 **Panorama** > **SD-WAN** > **Devices**（设备）。
2. 选择启用了 SD-WAN 的分支防火墙，其名称随后将填充 **Name**（名称）字段。
3. 将设备 **Type**（类型）选择为 **Branch**（分支）。
4. 选择 **Router Name**（路由器名称）。
5. 进入 **Site**（网站）。

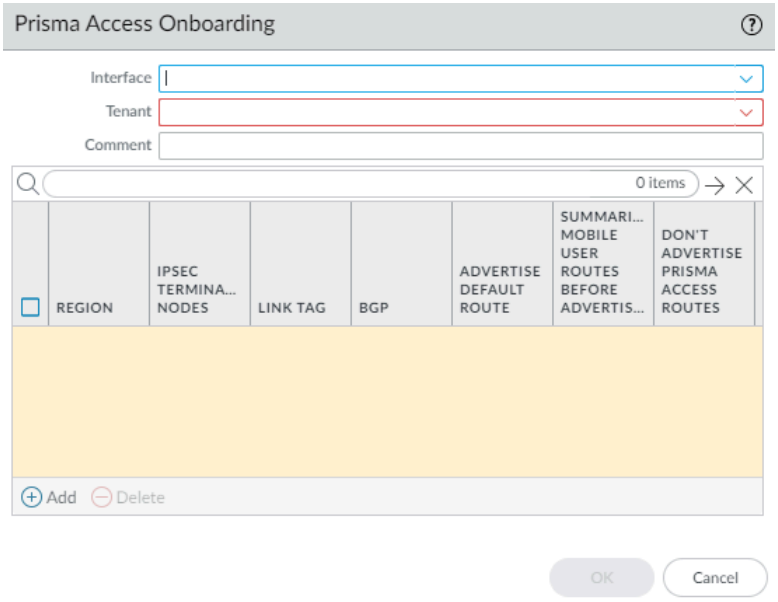
   所有 *SD-WAN* 设备都必须具有一个唯一的站点名称。

6. 选择 **Prisma Access Onboarding**（**Prisma Access** 登录）并 **Add**（添加）。



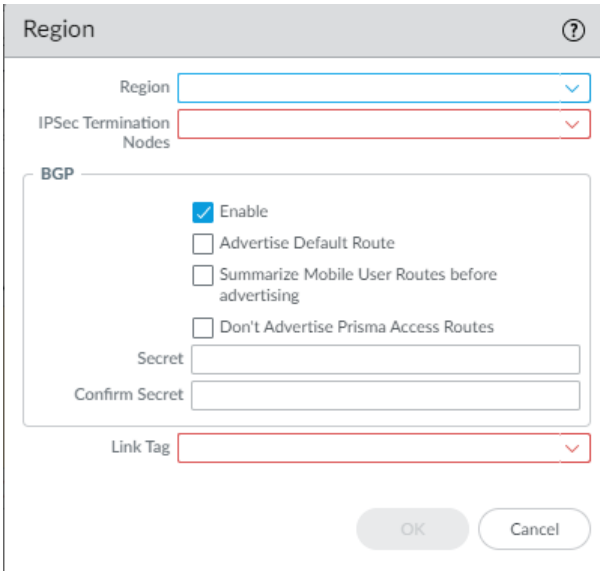
7. 在防火墙上选择一个支持 SD-WAN 的本地 **Interface**（接口）以连接到 Prisma Access 中心。
8. 选择一个 Prisma Access **Tenant**（租户）（为单个租户环境选择 **default**（默认））。

   分支防火墙上的所有 SD-WAN 接口都必须使用相同的 Prisma Access 租户。
9. 输入有用的 **Comment**（注释）。



10. 通过选择 CN（Prisma Access 中心）所在的 **Region**（区域），向区域 **Add**（添加）计算节点。

    每个接口可以有多个区域。



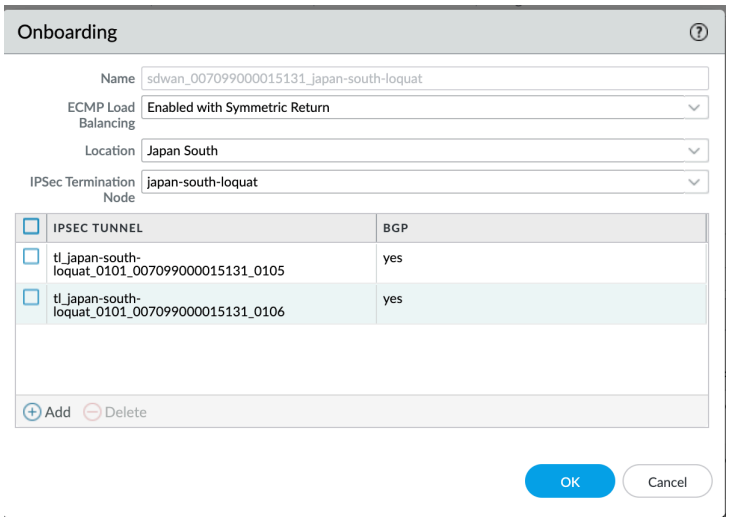
11. 从节点列表中选择一个 **IPSec Termination Node**（**IPSec** 终端节点）（GP 网关）；该列表基于 Prisma Access 之前在该地区启动的节点。您正在选择此分支所连接的中心。SD-WAN Auto VPN 配置与该节点建立 IKE 和 IPSec 关系和隧道。
12. 为分支和中心之间的通信 **Enable**（启用） BGP（默认设置为“启用”）。
13. **Advertise Default Route**（通告默认路由），允许将 Prisma Access 中心的默认路由通告到分支防火墙。
14. **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由），让 Prisma Access 中心通告汇总的移动用户 IP 子网路由，从而减少分支的通告数量。

15. **Don’t Advertise Prisma Access Routes**（不要通告 **Prisma Access** 路由），以防止 IPSec 终端节点/中心向 SD-WAN 分支通告其 Prisma Access 路由。
16. 输入用于验证 BGP 通信的 **Secret**（密钥） 并 **Confirm Secret**（确认密钥）。
17. 为中心选择 **Link Tag**（链路标签）。

    如要为 *Prisma Access* 中心启用 *ECMP*，可以将多个分支接口接入同一个计算节点 *(CN)*，并在这些分支接口上使用相同的链路标签。
18. 单击 **OK**（确定）。显示屏将包括 Prisma Access 提供的对等 AS 编号和隧道监视器 IP 地址。

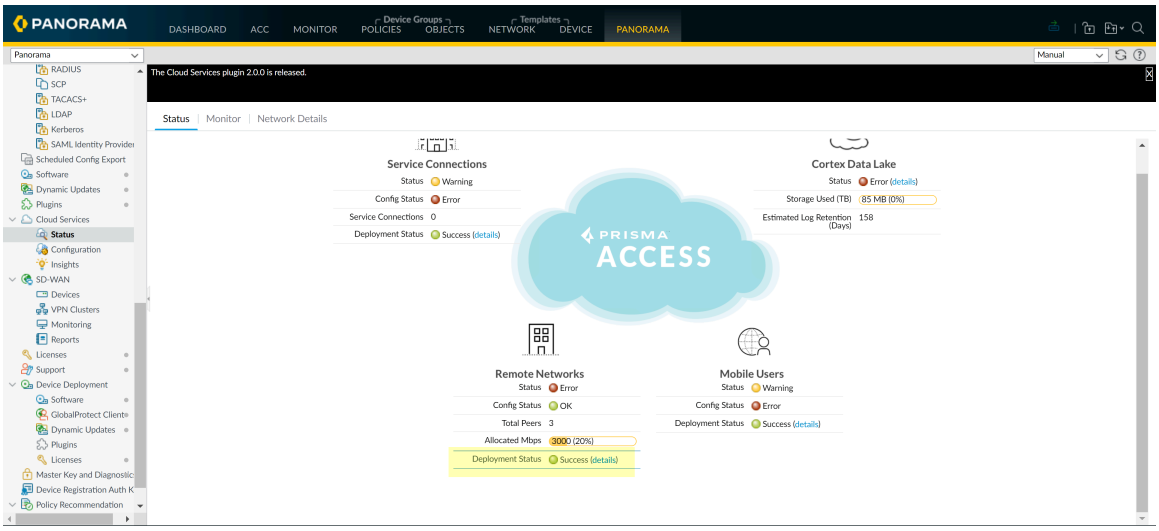
STEP 4 | **Commit and Push**（提交并推送）配置到云端，Prisma Access 会在云端根据所请求的带宽启动正确数量的 IPsec 终端节点。

当多个 *IPSec* 隧道进入同一个 *CN* 时，*Prisma Access* 配置将通过对称返回启用 *ECMP*，如此 *Prisma Access* 示例所示：

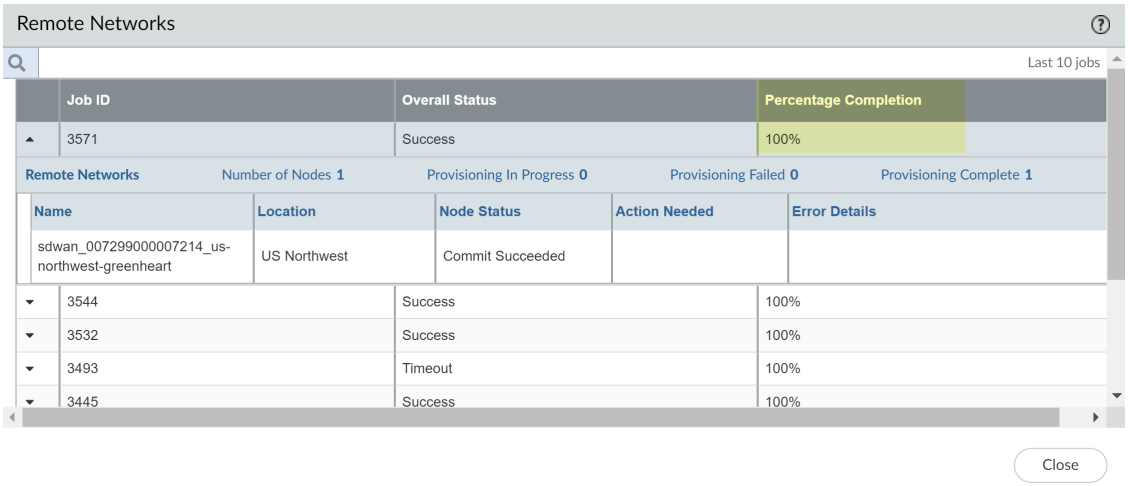


STEP 5 | 确认已完成登录。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态）并确认远程网络部署状态显示 `success`。



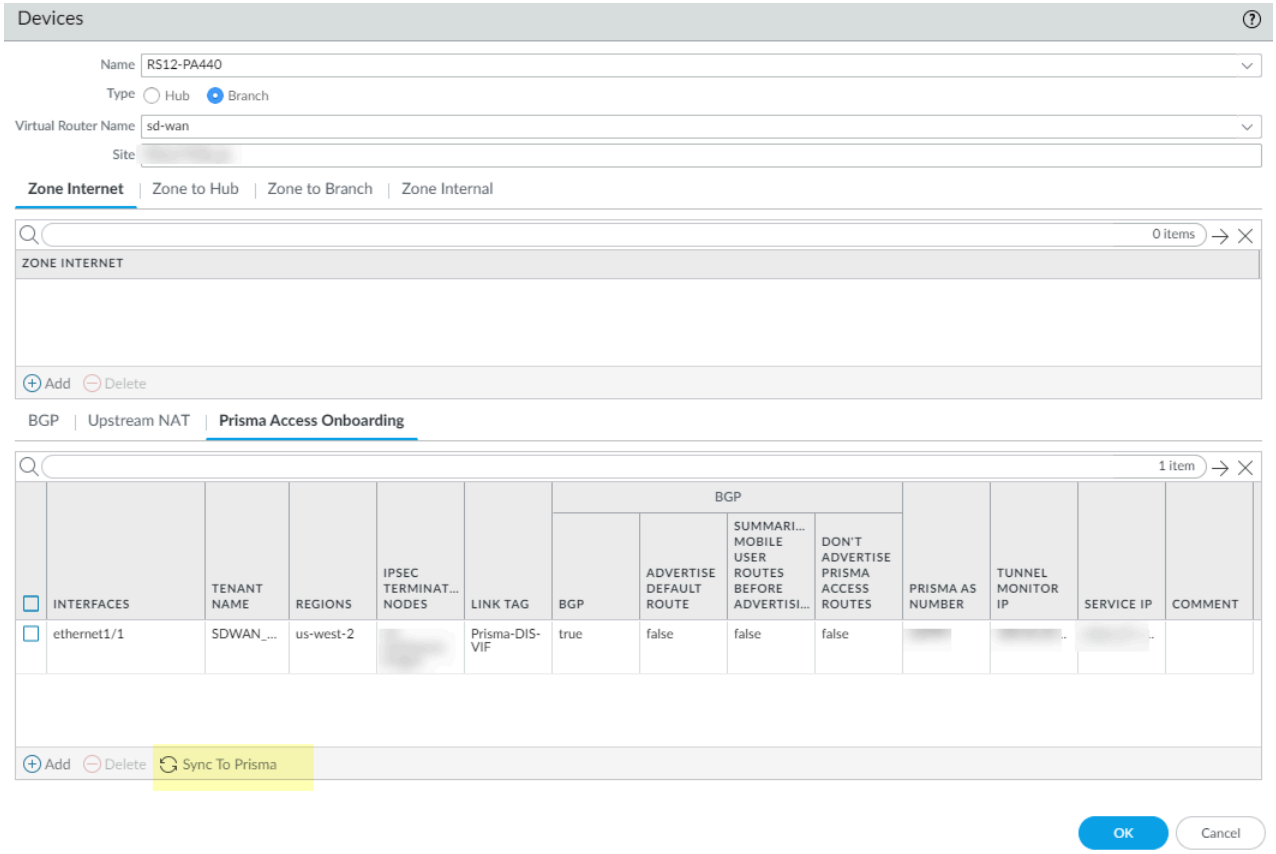
2. 选择远程网络部署状态的 **details**（详细信息）。
3. 确认 Prisma Access 节点完成度显示 100%。



STEP 6 | 将分支防火墙同步到 Prisma Access 以检索 CN 的服务 IP 地址。

1. 选择 **Panorama** > **SD-WAN** > **Devices**（设备）。
2. 选择 SD-WAN 分支设备。
3. 选择 **Prisma Access Onboarding**（**Prisma Access** 登录）并 **Sync To Prisma**（同步到 **Prisma**）（然后回复消息以继续）。对每个分支设备重复此操作。

成功同步到 *Prisma* 后，您将在 *SD-WAN* 分支防火墙上看到 *Prisma Access* 配置参数。如果没有看到，请等待大约 *15* 分钟，然后再次同步到 *Prisma*。如有必要，请转到 *Prisma Access* 插件并验证 *CN* 登录是否已完成（您可以看到分配了带宽和 *IP* 地址的 *CN*）。验证后，重试同步到 *Prisma*。



STEP 7 | **Commit**（提交）到 Panorama。

STEP 8 | **Push to Devices**（推送到设备）以推送到本地分支防火墙。**Edit Selections**（编辑选择）以选择推送范围选择。选择正确的 **Template**（模板）和 **Device Group**（设备组）。

STEP 9 | 在分支防火墙上，选择 **Network**（网络） > **Interfaces**（接口） > **SD-WAN**，然后查看使用您创建的链路标签（分配给名为 **zone-to-pa-hub**（从区域到 **PA** 中心）的安全区域）以及使用连接到 CN 的 IPSec 隧道创建的新接口。

STEP 10 | 选择 **Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）并确认 IPsec 隧道已经启动。

STEP 11 | 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关）并确认 IKE 网关已启动。

STEP 12 | 创建 SD-WAN 策略规则以生成监视数据。

需要执行此步骤才能为 Prisma Access 中心延迟、抖动和数据包丢失数据设置基线，以实现准确的流量分配。SD-WAN 监视数据从与您的 SD-WAN 策略规则匹配的流量中生成。

1. 创建流量分发配置文件.
2. 使用高延迟、抖动和数据包丢失阈值创建路径质量配置文件。

   创建 SD-WAN 策略规则需要路径质量配置文件。如果使用高阈值创建路径质量配置文件，则可以为 Prisma Access 中心的延迟、抖动和数据包丢失设置基线，而不会导致应用程序切换到其他链路。
3. 配置 SD-WAN 策略规则.

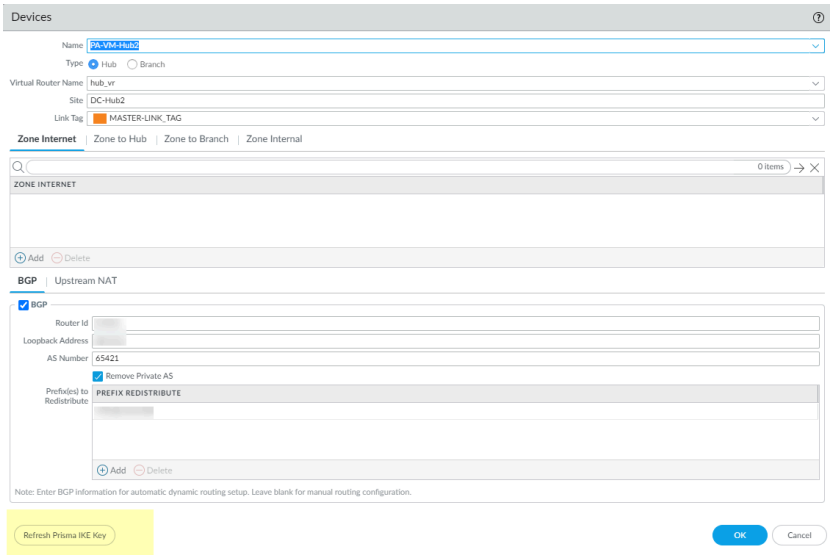
STEP 13 | **Commit**（提交）然后 **Commit and Push**（提交并推送）到分支防火墙。

STEP 14 | 刷新 Prisma IKE 预共享密钥。

如果您需要更改当前用于保护分支与 *Prisma* 中心之间 *IPSec* 连接的 *Prisma IKE* 密钥，请执行此步骤，为隧道随机生成新密钥并更新隧道两端。在中心和分支不繁忙时执行此步骤。

请勿手动创建名称以“*gw_*”开头的 *IKE* 网关，因为此类名称仅供登录期间创建 *Prisma IKE* 时使用。如果除了 *Prisma Access* 创建的网关之外还有其他网关，则刷新 *Prisma IKE* 预共享密钥的这一步会刷新所有此类命名的 *IKE* 网关。

1. 选择 **Panorama** > **SD-WAN** > **Devices**（设备），然后选择设备。
2. 在屏幕底部，选择 **Refresh Prisma IKE Key**（刷新 **Prisma IKE** 密钥）。



3. 将出现一条消息通知您刷新 IKE 密钥将更新分支和 Prisma Access 中心之间的所有 SD-WAN 隧道，并且需要将配置同步推送到所有分支和 Prisma Access 中心设

备。最佳实践建议是在维护窗口期间执行刷新，因为流量可能会受到影响。是否要继续？如果要继续，请选择 Yes（是）。

STEP 15 | **Commit**（提交）然后 **Commit and Push**（提交并推送）到分支防火墙。

STEP 16 | 监视 Prisma Access 中心应用程序和链路性能以了解指向 Prisma Access 的链路的延迟、抖动和数据包丢失基线。

如需收集准确的延迟、抖动和丢包数据以微调 Prisma Access 中心路径质量配置文件，必须执行这一步。

配置 SD-WAN HA 设备

您可以将两个防火墙配置为活动/被动 HA 模式下的分支（或将两个防火墙配置为活动/被动 HA 模式下的中心），作为 SD-WAN 环境的一部分。在这种情况下，Panorama™ 需要将相同的配置推送到主动对等端和被动对等端，而不是单独处理两个防火墙。为此，必须先添加 SD-WAN 设备，然后配置主动/被动 HA，这样，Panorama 就能将这些设备视为 HA 对等设备，并为其推送相同的配置。（仅支持 HA 活动/被动模式）。

开始前请通读以下步骤，避免在将 *HA* 对等设备作为 *SD-WAN* 设备添加之后进行提交。

在 *HA* 中，防火墙不同步 *SD-WAN* 会话分布统计信息。*HA* 故障转移后，会话分布统计仅显示新会话的统计信息；现有会话的统计数据丢失。

STEP 1 | 启用 HA 对等端上的 SD-WAN 之前，请在两个支持 SD-WAN 的防火墙型号中 配置主动/被动 HA。

STEP 2 | 将 HA 对等设备作为 SD-WAN 设备添加，但不得执行最后一步 **Commit**（提交）。

STEP 3 | 在 Panorama 上，选择 **Panorama** > **Managed Devices**（受管设备） > **Summary**（摘要）。

STEP 4 | 在屏幕底部，选择 **Group HA Peers**（分组 **HA** 对等端）。确认在状态显示下，HA 状态列包含两个防火墙，一个为主动，一个为被动。Panorama 知晓 HA 状态，并在您提交时，将相同的 SD-WAN 配置推送给两个 HA 对等端。

STEP 5 | **Commit**（提交），然后 **Commit and Push**（提交并推送）。

创建 VPN 集群

在您的 SD-WAN 配置中，必须配置一个或多个 VPN 集群，以确定哪些分支与哪些中心通信，并在分支和中心设备之间创建安全连接。VPN 集群是设备的逻辑分组，因此，在逻辑分组设备时，请考虑地理位置或功能等因素。

PAN-OS® 同时支持中心辐射型和全网状 SD-WAN VPN 拓扑。在中心辐射型拓扑结构中，位于主要办公室或地点的集中防火墙中心充当分支设备之间的网关。中心到分支之间的连接形成 VPN 隧道。在此配置中，分支之间的流量必须经过中心。

在您第一次通过互联网直接接入 (DIA) 链路，为 SD-WAN 中心或分支防火墙配置 SD-WAN 虚拟接口时，会自动创建一个名为 `autogen_hubs_cluster` 的 VPN 集群，且 SD-WAN 防火墙会自动添加到此 VPN 集群。这样，Panorama™ 管理服务器可以针对受 SD-WAN 防火墙保护的设备监控 SD-WAN 应用程序和链路性能，并访问企业网络之外的资源。此外，使用您将来配置的 DIA 链路的任何 SD-WAN 防火墙会被自动添加到使用 DIA 链路的所有中心和分支的 VPN 集群 `autogen_hubs_cluster` 中，以允许 Panorama 监控应用程序和链路性能。`autogen_hubs_cluster` 仅用于监控应用程序和链路运行状况，不会通过 DIA 链路在中心和分支之间创建 VPN 隧道。如果要通过 VPN 隧道连接中心和分支，必须新建一个 VPN 集群，将所需的全部中心和分支都添加到该集群。

在 VPN 集群中为所有中心和分支创建一个强大的随机 IKE 预共享密钥，以保护 VPN 隧道，且每个防火墙都有一个用于加密预共享密钥的主密钥。系统可以保护预共享密钥，甚至可使其免受管理员影响。您可以刷新 Panorama 发送到集群所有成员的 IKE 预共享密钥。

在集群成员不忙时刷新预共享密钥。

将 SD-WAN 插件升级到 2.1.0 后，单个 VPN 集群中的中心和分支防火墙必须全部运行 PAN-OS 10.0.4（或更高的 10.0 版本）或 10.1.0，而不是两个版本的组合。

查看 *VPN* 集群时，如果没有数据或屏幕指示 *SD-WAN* 未定义，请在 Compatibility Matrix（兼容性矩阵）中检查您正在使用的 *Panorama* 版本是否支持您尝试使用的 *SD-WAN* 插件版本。

STEP 1 | 计划分支和中心的 VPN 拓扑结构，以确定哪个分支与所有中心进行通信。有关详细信息，请参阅计划您的 SD-WAN 配置。

STEP 2 | 登录到 Panorama Web 界面。

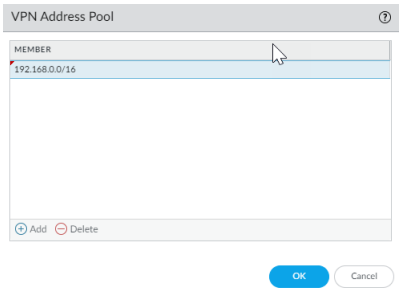
STEP 3 | 为自动 VPN 配置创建的 IPSec VPN 隧道指定 IP 地址。

自动 *VPN* 配置在中心和分支之间创建 *VPN* 隧道，并将 *IP* 地址分配给隧道端点。输入想让自动 *VPN* 用作 *VPN* 隧道地址的子网范围。您最多可以输入 *20* 个 *IP* 前缀/子网掩码范围值。自动 *VPN* 从该池中提取 *VPN* 隧道地址，首先从最大的范围值开始提取（且根据需要提取下一个最大范围值）。您必须至少为池配置一个范围值。如果您在推送配置到中心或分支前尚未执行此步骤，则提交和推送操作将失败。

如果从更早的 *SD-WAN* 插件版本升级，则必须检查您的范围值是否仍然正确。如果不正确，请输入新的范围值。***Commit***（提交）后，所有隧道都将被丢弃，并使用新隧道，因此，请在低流量时执行此任务。

1. 选择 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群）。
2. 在屏幕底部，选择 **VPN Address Pool**（**VPN** 地址池）。

3. **Add**（添加）一个或多个（最多 20 个）**Member**（成员） IP 地址和子网掩码范围值，例如，192.168.0.0/16。
4. 单击 **OK**（确定）。



如果 *Prisma Access* 已登录，请勿更改现有地址池。如果需要更改地址池，请在维护窗口期间执行以下步骤，以使用变更的地址池更新分支和 *Prisma Access CN*：

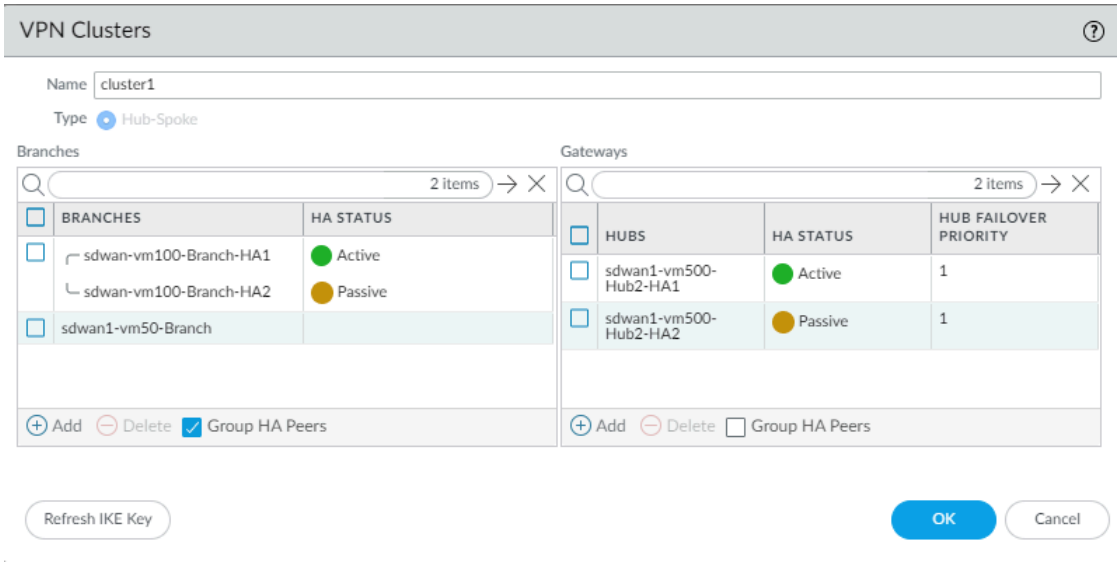
1. 使用 *Panorama* 访问 *SD-WAN* 分支并删除地址池更改将影响的现有登录；然后进行本地提交。
2. 更新 *VPN* 地址池，然后进行本地提交。
3. 再次执行 *Prisma Access* 登录，然后执行本地提交和推送。

STEP 4 | 配置 VPN 集群。重复此步骤以根据需要创建 VPN 集群。

1. 选择 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群），然后**Add**（添加）VPN 集群。
2. 输入 VPN 群集的描述性名称。

   不得在 *VPN* 集群名字中使用下划线和空格，否则会导致该集群的监控（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监控））数据无法显示。请仔细选择 *VPN* 集群的名称，以免去后续更名的麻烦。*SD-WAN* 监控数据根据旧的集群名称生成，无法与新的集群名称协调，且会在监控 *VPN* 集群或生成报告时，使报告的集群数出现问题。
3. 选择 VPN 集群 **Type**（类型）。

   PAN-OS 10.0.2 和更早的 *11.0* 版本仅支持 ***Hub-Spoke***（中心辐射型）*VPN* 集群类型。从 *PAN-OS 10.0.3* 开始，您可以用 DDNS 服务创建全网状 VPN 集群。
4. **Add**（添加）一个或多个您确定需要相互通信的分支设备。
   - 选择 **Group HA Peers**（分组 **HA** 对等设备）以显示一起作为 HA 对等设备的分支设备。

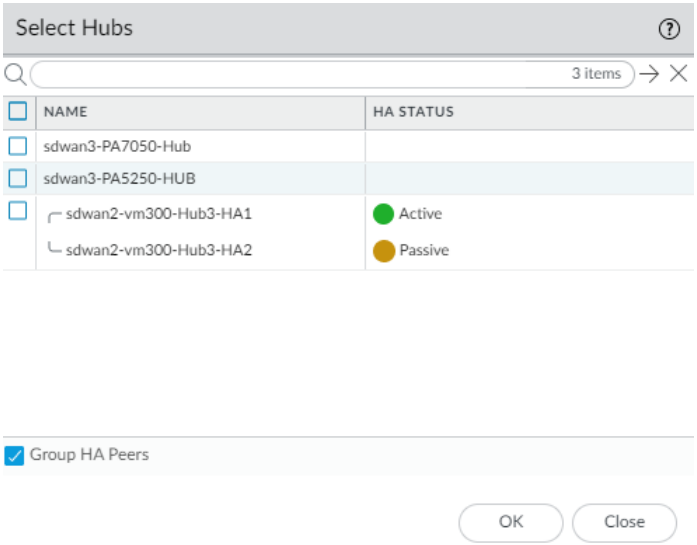


   - 选择要添加到集群的分支设备。
   - 单击 **OK**（确定）。
5. **Add**（添加）一个或多个您认为需要与分支设备进行通信的中心设备。

   最多可添加四个 SD-WAN 中心防火墙到 VPN 集群中。HA 配置中的 SD-WAN 中心被视为单一的 SD-WAN 中心防火墙。

   MPLS 和卫星链路类型形成的隧道仅具有一种链路类型；例如，*MPLS* 到 *MPLS*，卫星到卫星等。例如，*MPLS* 链路和以太网链路之间不会创建隧道。

- 选择 **Group HA Peers**（分组 **HA** 对等设备）以显示一起作为 HA 对等设备的中心设备。
- 选择要添加到集群的中心，然后单击 **OK**（确定）。



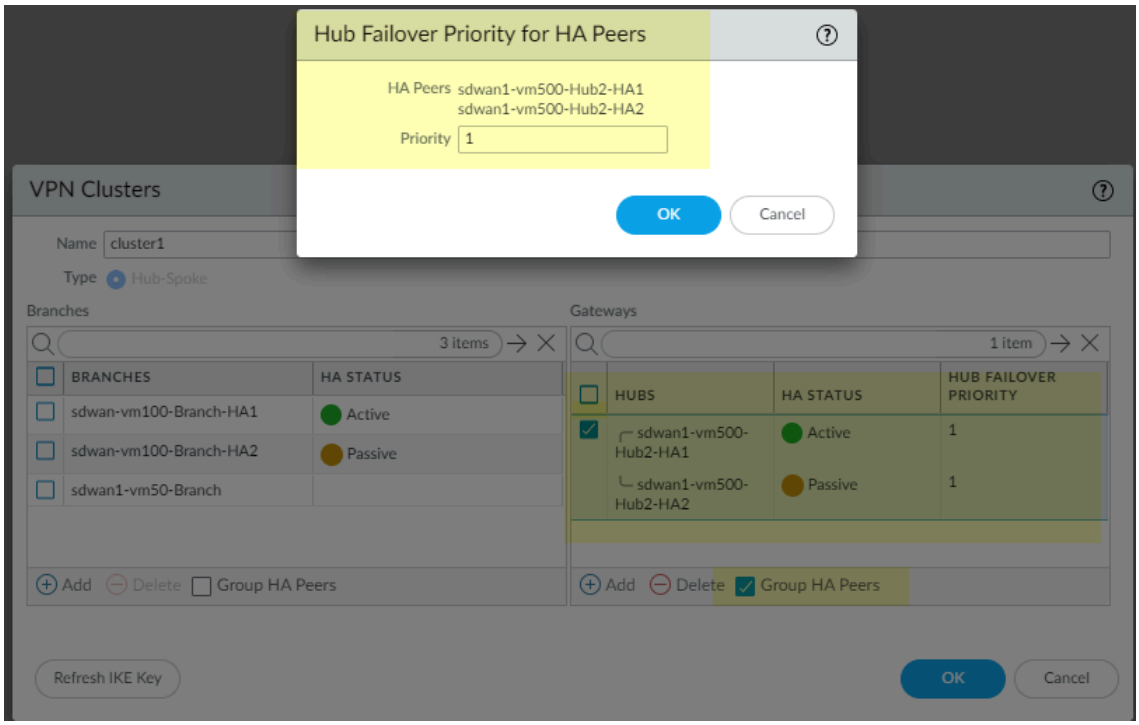
- 对于有一个以上中心的任何新建或现有 VPN 集群，必须确定中心的优先级，以确定 a) 流量被发送到指定中心；b) 随后的中心故障转移顺序。中心故障转移优先级范围为 1 到 4。如果进行升级，则默认优先级设置为 4。插件在内部把中心故障转移优先顺序转换为 BGP 本地首选项编码，如下表所示。优先级的值越低，则优先级和本地首选项编码越高。一个集群最多能支持四个中心。一个活动/被动 HA 对视为一个中心。多个中心可以有相同的优先级；HA 对必须拥有相同的优先级。Panorama 使用分支的 BGP 模板将中心的本地首选项推送到集群分支。

中心故障转移	本地首选项
1	250
2	200
3	150

中心故障转移	本地首选项
4	100

如果多个中心的优先级相同，则 *Panorama* 将启用每个分支防火墙两处的 *ECMP* 以确定分支选择路径的方法。对虚拟路由器启用 *ECMP*（***Network***（网络） > ***Virtual Routers***（虚拟路由器） > ***ECMP***），对 *BGP* 启用 ***ECMP Multiple AS Support***（***ECMP*** 多个 ***AS*** 支持）（***Network***（网络） > ***Virtual Router***（虚拟路由器） > ***BGP*** > ***Advanced***（高级））。如果集群中的所有中心都有唯一的优先级，则在分支上禁用 *ECMP*。如果中心优先级配置发生更改，*Panorama* 会重新评估是启用还是禁用 *ECMP*。

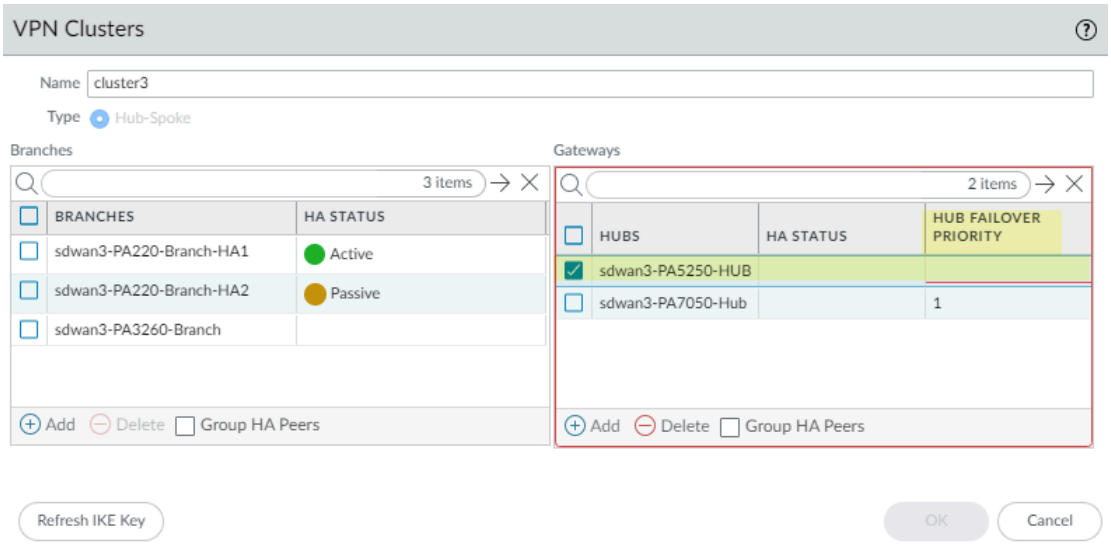
- 如果选择了 **Group HA Peer**（分组 **HA** 对等设备），请选择对并单击 **Hub Failover Priority**（中心故障转移优先级）字段；输入应用于 HA 对中的两个中心的一个 **Priority**（优先级）（范围为 1 到 4），然后单击 **OK**（确定）。



HA 对等设备的中心故障转移优先级窗口仅对已配置的 *HA* 对显示。如果添加了新的 *HA* 对等设备，则必须为两个新对等设备单独配置中心故障转移优先级。

如果您为是未分组 *HA* 对等设备的中心分配不同的优先级，并选择 ***Group HA Peers***（分组 ***HA*** 对等设备）和 ***Submit***（提交），则将收到一条错误消息。

- 对于不是 HA 对的中心，选择一个中心，然后单击 **Hub Failover Priority**（中心故障转移优先级）字段；输入一个优先级（范围为 1 到 4）。



6. 单击 **OK**（确定）以保存 VPN 集群。

STEP 5 | 在分支处向中心通告附加前缀。

防火墙自动将所有非公共的连接路由从分支重新分发（通告）到中心。您还可以将任何其他前缀从分支重新分发到中心。***Prefix(es) to Redistribute***（待重新分发的前缀）字段接受前缀列表，而不仅仅是一个前缀。

1. 选择 **Panorama** > **SD-WAN** > **Devices**（设备），然后选择分支防火墙。
2. 选择 **BGP**，然后 **Add**（添加）一个或多个带子网掩码的 IP 地址到**Prefix(es) to Redistribute**（待重新分发的前缀）中。
3. 单击 **OK**（确定）。

STEP 6 | **Commit**（提交），然后 **Commit to Panorama**（提交到 **Panorama**）。

STEP 7 | （SD-WAN 插件 2.0.1 和 2.0 的更高版本）如果您在中心辐射型 VPN 集群中的中心防火墙有 DHCP 或 PPPoE 接口，则必须使用 DDNS。选择 **Network**（网络）> **Interfaces**（接口）> **Ethernet**（以太网），然后在 **Template**（模板）字段为中心选择模板堆栈。

STEP 8 | （SD-WAN 插件 2.0.1 和 2.0 的更高版本）选择 IP 地址表示动态 DHCP 客户端或 PPPOE 的接口，单击屏幕底部的 **Override**（覆盖），然后单击 **OK**（确定）以关闭。

STEP 9 | （SD-WAN 插件 2.0.1 和更高版本 2.0）在 Panorama 上验证是否已配置 DDNS 设置。

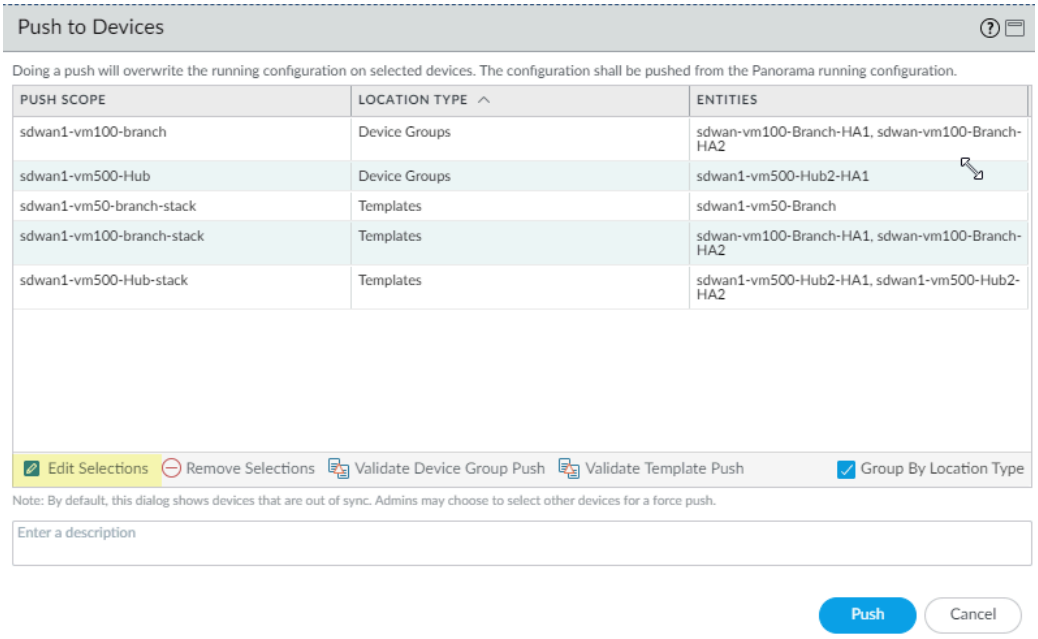
1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后再次选择相同的接口。
2. 选择 **Advanced**（高级） > **DDNS**。
3. 确保为 DDNS 设置自动配置了 **Hostname**（主机名），且 **Vendor**（供应商）设置为 `Palo Alto Networks DDNS`。
4. 单击 **OK**（确定）。

STEP 10 | （SD-WAN 插件 2.0.1 和 2.0 的更高版本）**Commit**（提交）并 **Commit to Panorama**（提交至 **Panorama**）。

STEP 11 | 将配置推送到中心。

Panorama 创建用于中心的 *SD-WAN* 虚拟接口时，无需使用连续接口编号创建此接口。它可以随机跳过一个接口编号，例如，*sdwan.921*、*sdwan.922*、*sdwan.924*、*sdwan.925*。尽管编号不连续，但是 *Panorama* 可以创建正确的 *SD-WAN* 接口编号。使用 *CLI* 操作命令 ***show interface sdwan?***（显示接口 *sdwan*？）查看 *SD-WAN* 接口。

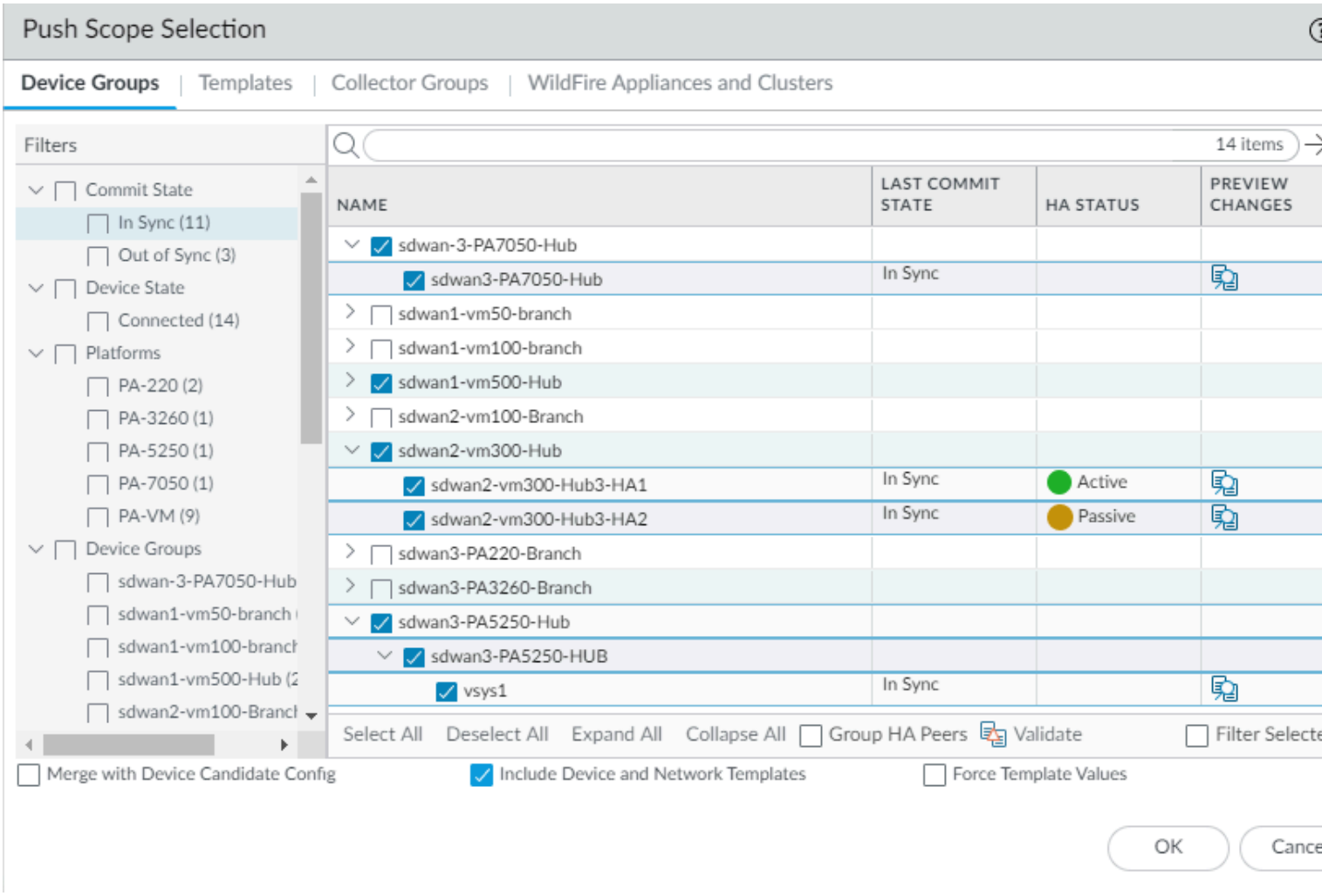
1. 选择 **Commit**（提交）和 **Push to Devices**（推送到设备）。
2. 屏幕左下方的 **Edit Selections**（编辑选项）。



3. 取消选择 **Filter Selected**（筛选器已选择）。
4. 单击 **Deselect All**（取消全选）。
5. 选择您的中心设备组。选择屏幕底部的 **Include Device and Network Templates**（包括设备和网络模板）。您必须先推送到分支，然后再推送到中心。

   大多数分支都有其服务提供商提供的动态 IP 地址，因此，分支必须启动 IKE/IPSec 连接，原因在于中心不具有分支的 IP 地址。为确保中心做好接收 IKE/IPSec 连接的准备，

必须先提交和推送中心的配置，然后再提交和推送分支的配置。因此，在分支配置推送结束，且分支启动到中心的连接时，中心已就绪。



6. 选择 **Template**（模板）选项卡，然后 **Deselect All**（取消全选）。
7. **Push Scope**（推送范围）是设备组。将配置 **Push**（推送）到防火墙。

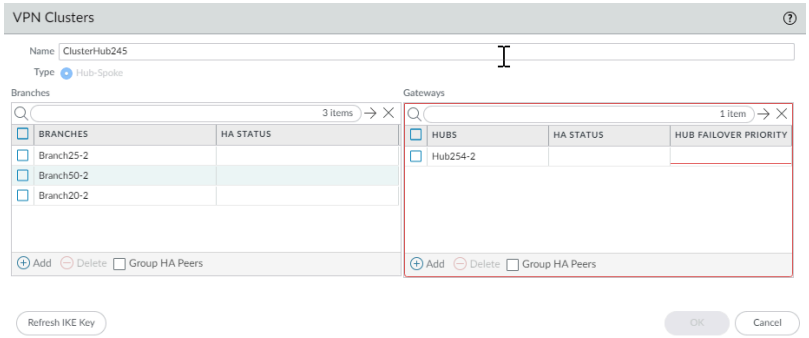
STEP 12 | 重复上一步，但选择分支设备组，以将配置推送到分支。

STEP 13 | 刷新 IKE 预共享密钥。

如果想更改当前用于保护 *VPN* 集群设备之间 *IPSec* 连接的 *IKE* 密钥，请执行此步骤，为集群随机生成一个新的密钥。

在集群成员不繁忙时执行此步骤。

1. 选择 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群），然后选择集群。
2. 在屏幕底部，选择 **Refresh IKE Key**（刷新 **IKE** 密钥）。



3. 此时将显示一条消息，通知您刷新 IKE 密钥将为 VPN 集群中的每个 SD-WAN 防火墙生成新的安全关联 (SA)。这可能导致服务中断。是否要继续？是 | 否 如果要继续，请选择 Yes（是）。
4. **Commit**（提交）。

   Refresh IKE Key（刷新 ***IKE*** 密钥）后，必须向整个集群提交；部分提交会破坏隧道。
5. **Push to Devices**（推送到设备）。

用 DDNS 服务创建全网状 VPN 集群

从 PAN-OS 10.0.3 开始，SD-WAN 除了支持中心辐射型拓扑结构之外，还支持全网状拓扑结构。网状结构可以包含有中心或无中心的分支。在分支需要直接相互通信时使用全网状结构。全网状结构的用例示例包括拥有分支和中心的零售商和在有中心和无中心的情况下运营的企业。

部分防火墙接口用 DHCP 获得它们的 ID 地址。分支机构通常使用消费者级别的互联网服务，并接收动态 IP 地址，该 IP 地址当然是可以更改的。因此，防火墙需要动态 DNS (DDNS)，以便 DDNS 服务能够检测运行 SD-WAN 的防火墙接口的面向公众的 IP 地址。向所有防火墙推送 DDNS 设置时，这会通知每个防火墙向 Palo Alto Nwtwork DDNS 云服务注册其外部接口 IP 地址，以便将 IP 地址转换为 FQDN。

DDNS 也是必要的，因为来自 ISP 的 CPE 设备可能正在执行源 NAT。（动态 IP 地址可能是也可能不是转换的源 NAT。）DDNS 服务允许防火墙向 DDNS 服务器注册面向公众的 IP 地址。将设备连接至分支到分支的网状结构时，自动 VPN 会联系这些防火墙的 DDNS 服务，以获取在 DDNS 云中注册的公共 IP 地址，并使用这些公共 IP 地址创建 IKE 对等和 VPN 隧道。如果 CPE 设备正在执行源 NAT，当添加一个 SD-WAN 分支设备以由 Panorama 管理时，您将启用 **Upstream NAT**（上游 **NAT**），且 NAT IP 地址类型将为 **DDNS**。

对于 *CPE* 设备或使用源 *NAT* 的上游路由设备，您负责在该设备上创建一对一目标 *NAT* 规则（不带端口转换）以将外部 *IP* 地址转换回分配给防火墙接口的专用 *IP* 地址。这种转换允许 *IKE* 和 *IPSec* 协议返回防火墙。（*Palo Alto Networks* 没有访问上游 *CPE* 或访问执行源 *NAT* 的上游路由器的权限。）

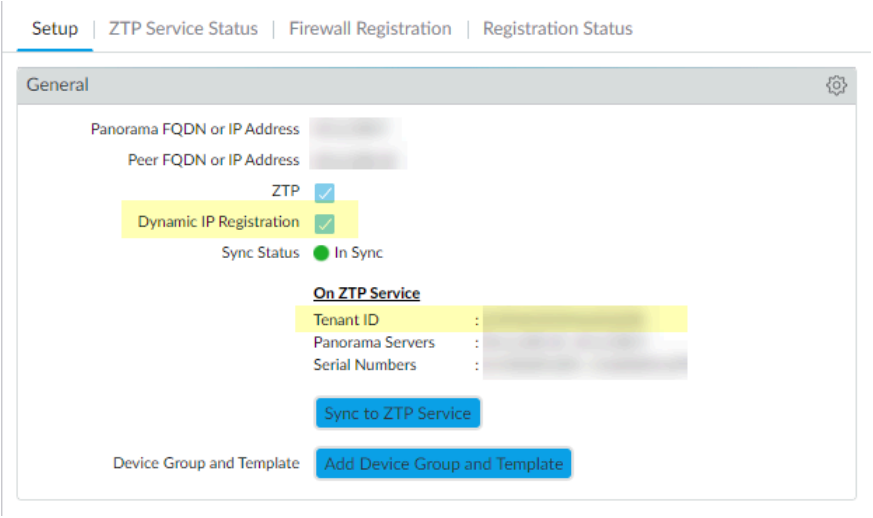
具有 DDNS 服务的 SD-WAN 全网状结构需要以下条件：

- PAN-OS 10.0.3 或更高的 11.0 版本
- SD-WAN 插件 2.0.1 或 2.0 的更高版本
- ZTP 插件 1.0.1 或 1.0 的更高版本已下载、安装并配置，以便利用与 ZTP 关联的 DDNS。Panorama 必须是 ZTP 注册的，并与 ZTP 服务通信。
- 应用程序和威胁内容发布版本 8354 或更高版本
- 所有参与全网状 DDNS 的防火墙必须在同一客户支持门户 (CSP) 帐户下注册。
- 所有参与全网状 DDNS 的防火墙必须安装最新的设备证书。正确验证防火墙、Panorama 和云服务是重要的安全程序，需要设备证书以及 CSP 和 ZTP 服务。
- 如果您的防火墙或其他控制传出流量的网络设备位于 Palo Alto Networks 防火墙前，您必须更改该设备上的配置，以允许从启用 DDNS 的接口向以下 FQDN 发送流量：
  - https://myip.ngfw-ztp.paloaltonetworks.com/ （以到达 whatsmyIP 服务）
  - https://ngfw-ztp.paloaltonetworks.com/ （以到达 DDNS 注册服务）

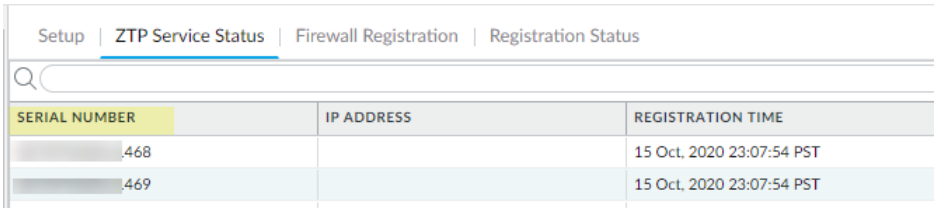
STEP 1 | 为 Panorama 和所有作为中心或分支的受管防火墙 安装最新的设备证书。

STEP 2 | 安装 ZTP 插件 1.0.1 以设置零接触配置。

1. 阅读 Panorama 管理员指南中的 ZTP 概述。
2. 安装 ZTP 插件。
3. 配置 ZTP 安装程序管理员帐户。
4. 选择 **Panorama** > **Zero Touch Provisioning**（零接触配置） > **Setup**（设置），然后编辑 General（常规）设置以启用 **Dynamic IP Registration**（动态 **IP** 注册）。
5. 单击 **OK**（确定）。General（常规）设置表示带租户 ID 编号的 On ZTP 服务。



6. 选择 **ZTP Service Status**（**ZTP** 服务状态），然后确认防火墙序列号已列出。



STEP 3 | 如果还没有这样做，请安装 SD-WAN 插件 2.0.1 或 2.0 的更高版本。

STEP 4 | 在 Panorama 上 **Commit**（提交）。

STEP 5 | 登录到 Panorama Web 界面。

STEP 6 | 按创建 VPN 集群所示创建 VPN 地址池。

STEP 7 | 创建全网状 VPN 集群。

1. 选择 **Panorama** > **SD-WAN** > **VPN Clusters**（**VPN** 集群）。
2. 选择 **Type**（类型）为 **Mesh**（网状结构）。
3. **Add**（添加） 需要相互通信的 **Branch**（分支）。
4. （可选）如果网状结构中也需要中心，您可以 **Add**（添加）一个或多个 **Hub**（中心）。
5. 单击 **OK**（确定）。

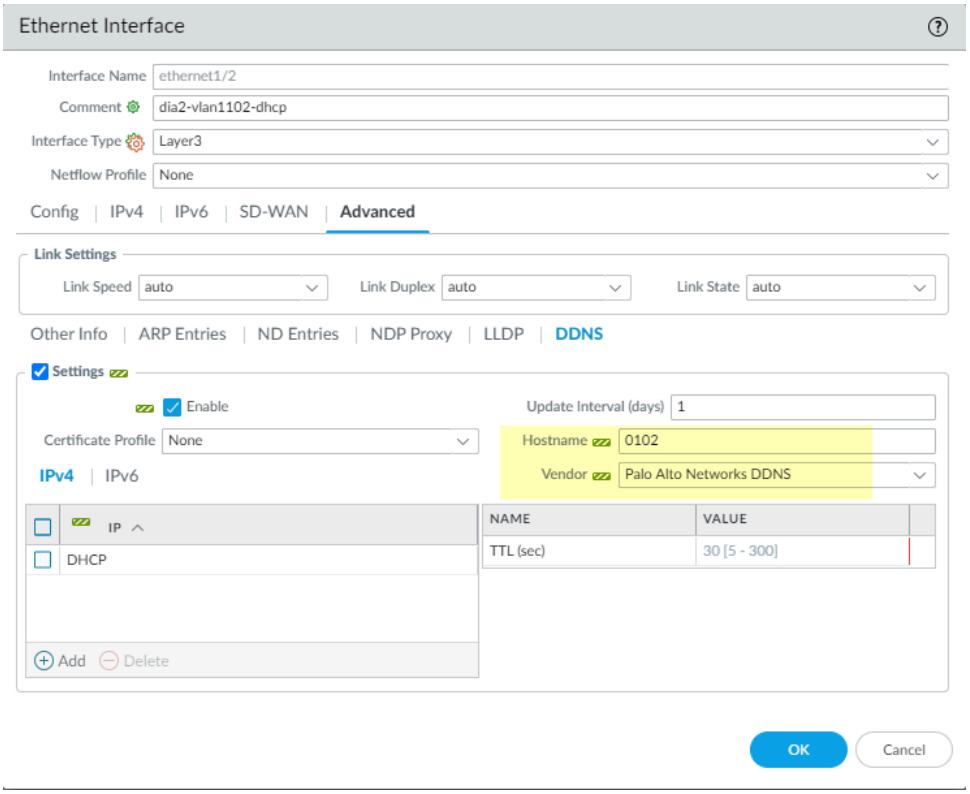
STEP 8 | **Commit**（提交），然后 **Commit to Panorama**（提交到 **Panorama**）。如果您的防火墙有静态 IP 地址，则已完成。如果您的 VPN 网状结构中的分支或中心防火墙有 DHCP 或 PPPoE 接口，则您必须使用 DDNS，因此，请按以下步骤继续此程序。

STEP 9 | 在 **Template**（模板）字段中选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），为特定分支选择模板堆栈。

STEP 10 | 选择 IP 地址指示动态 `DHCP` 客户端或 `PPPOE` 的接口，单击屏幕底部的 **Override**（覆盖），然后单击 **OK**（确定）以关闭。

STEP 11 | 在 Panorama 上验证是否已配置 DDNS 设置。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后再次选择相同的接口。
2. 选择 **Advanced**（高级） > **DDNS**。
3. 确保根据接口名称为 DDNS 设置自动配置了 **Hostname**（主机名），且 **Vendor**（供应商）设置为 `Palo Alto Networks DDNS`。例如，在 Ethernet1/2 接口上，生成的主机名为 0102。



4. 单击 **OK**（确定）。

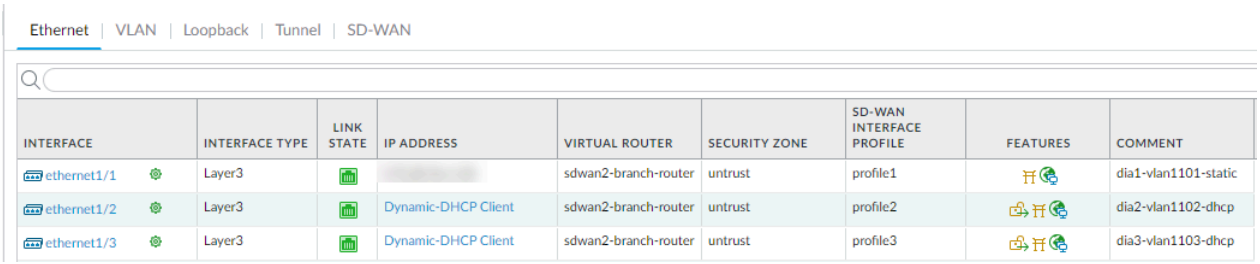
STEP 12 | 如果 VPN 群集包括任何具有 DHCP 或 PPPoE 接口的中心，请重复步骤 9 至 11，但在 **Template**（模板）字段中，为特定中心选择模板堆栈。

即使您的中心不在全网状集群中，而是在中心辐射式集群中，如果该中心使用 *DHCP* 或 *PPPOE* 以获得其 *SD-WAD* 接口的 *IP* 地址，您必须执行覆盖步骤以启用 *DDNSS*。

STEP 13 | **Commit**（提交） 至 Panorama 并 **Push to Devices**（推送到设备）。

STEP 14 | 在分支防火墙上验证分支是否已配置 DDNS。

1. 登录到分支防火墙。
2. 选择 **Network**（网络） > **Interface**（接口） > **Ethernet**（以太网），对于您已配置的以太网接口，滚动功能列的 DDNS 信息图标以查看供应商、主机名、IP 地址和其他 DDNS 信息。



STEP 15 | 在集群的另一个分支上，确保接口的对等地址是由系统生成的用于 DDNS 注册的 FQDN。

1. 登录到另一个分支并选择 **Network**（网络） > **Network Profile**（网络配置文件） > **IKE Gateway**（**IKE** 网关）。
2. 确保对等地址是一个不轻易被引用且不显示公司信息的安全名称；例如 0101.8ced8460fcc5177cd3665ce41b6345323a15a612b8e52ec1d9ec057a582cb4.t13855f6c9a92d6[...]e18a0d9

STEP 16 | 查看分支和中心的 FQDN 并更新 DDNS 信息。

1. 访问 CLI。
2. 查看其它分支和中心的 FQDN（由 DDNS 生成）：全部显示 **`dns-proxy fqdn`**
3. 更新 DDNS 地址：请求系统 **`fqdn`** 刷新

创建 SD-WAN 静态路由

除了 BGP 路由（或除了充当 BGP 路由的替代），您可以创建静态路由来传送您的 SD-WAN 流量。

静态路由有两种配置方式：使用 Panorama™ 配置，或直接在中心或分支防火墙上配置。如果使用 Panorama，则必须熟悉配置模板或模板堆栈变量的过程。您将创建一个变量充当静态路由的目标，如以下过程所示。您将推送（到达中心的）静态路由到分支。您将推送（到达分支的）静态路由到中心。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 配置模板或模板堆栈变量，然后输入以下格式的变量 **Name**（名称）：$*peerhostname_clustername.customname*。例如，$branchsanjose_clusterca.10 或 $DIA_cluster2.location3。在变量中，美元符号 ($) 之后的元素为：

- *peerhostname*— 静态路由前往的目标中心或分支的主机名。对于 Internet 静态路由，peerhostname 必须为 **DIA**。或者，对等端的主机名可以使用对等端的序列号。如果对等端是 HA 对的一部分，则可以使用两个 HA 防火墙中其中一个的主机名或序列名。
- *clustername*— 目标中心或分支所属的 VPN 集群的名称。
- *customname*— 您选择的文本字符串；不能在 customname（自定义名称）中使用句点 (.)。

对于相同的对等端，您可以使用多个静态路由，也就是说，变量可以拥有相同的 peerhostname 和 clustername；您可以通过使用不同的 customname 来区分变量。

STEP 3 | 选择变量 **Type**（类型）为 **IP Netmask**（**IP** 网络掩码），并输入带斜杠和网络掩码长度的目标 IP 地址，例如 192.168.2.1/24。

STEP 4 | 单击 **OK**（确定）以保存变量。

STEP 5 | 选择 **Network**（网络）> **Virtual Routers**（虚拟路由器），然后选择虚拟路由器。

STEP 6 | 选择 **Static Routes**（静态路由）> **IPv4**，并为该静态路由 **Add**（添加）一个 **Name**（名称）。

STEP 7 | 对于 **Destination**（目标），请选择您创建的变量。

STEP 8 | 对于 **Interface**（接口），从下拉列表中选择，下拉列表仅包括模板的接口；例如，Ethernet1/1、Tunnel.x 或 sdwan.xx。

STEP 9 | 对于 **Next Hop**（下一个跃点），请选择 **IP Address**（**IP** 地址），并输入用于静态路由的下一个跃点的 IP 地址（静态路由进入的中心或分支）。

STEP 10 | 单击 **OK**（确定）。

STEP 11 | **Commit**（提交），然后 **Commit and Push**（提交并推送）您的更改。

自动 VPN 配置将静态路由接口字段中的 **sdwan** 关键字替换为可以根据目标变量进行确定的 SD-WAN 虚拟出口接口。因此，路由表中的静态路由表明，已标识 VPN 集群中前往对等主机的流量将经过 SD-WAN 虚拟出口接口，到达指定的下一个跃点。

STEP 12 | 配置用于返回流量的静态路由。

为 SD-WAN 配置高级路由

高级路由引擎允许防火墙进行扩展，并为大型数据中心、ISP、企业和云用户提供稳定、高性能和高可用性的路由功能。高级路由引擎依赖于行业标准的配置方法，这有助于管理员完成任务。它允许创建用于不同功能（例如过滤、再分配和指标更改）的配置文件，所有这些功能都可以在逻辑路由器上使用。这些配置文件的粒度更精细，可以筛选每个动态路由协议的路由、改进跨多个协议的路由重新分发。

尽管在概念上是等效的，但高级路由引擎使用逻辑路由器而不是虚拟路由器来实例化路由域。

与虚拟路由器不同，默认情况下不创建逻辑路由器；在配置路由功能之前必须创建逻辑路由器。

您可以根据网络要求使用高级路由引擎或旧版引擎：

- 启用高级路由时，将创建逻辑路由器并使用高级路由引擎进行路由。
- 禁用 **Advanced Routing**（高级路由）时，将创建虚拟路由器并使用旧版引擎进行路由。

高级路由引擎支持多个逻辑路由器（在旧版路由引擎上称为虚拟路由器）。例如，高级路由引擎具有更便捷的菜单选项，并且您可以在配置文件（身份验证、计时器、地址系列或重新分发配置文件）中轻松配置更多应用于 BGP 对等组或对等体的 BGP 设置。

高级路由引擎支持静态路由、MP-BGP、OSPFv2、OSPFv3、RIPv2、协议无关组播 — 稀疏模式 (PIM-SM)、PIM 源特定组播 (SSM)、BFD、重新分发、路由过滤到 RIB、访问列表、前缀列表和路由映射。

您需要满足以下条件才能在 SD-WAN 上配置高级路由引擎：

平台	运行 **PAN-OS** 版本的防火墙	**SD-WAN** 插件
Panorama™	11.0 及更高版本	3.1.0 及更高版本

SD-WAN 插件根据高级路由选项的值创建逻辑路由器或虚拟路由器。如果启用高级路由，将创建逻辑路由器；否则，将创建虚拟路由器。

当您在模板堆栈中启用高级路由，并执行 Panorama 提交且推送到防火墙时，SD-WAN 插件会运行迁移脚本以在逻辑路由器中创建 SD-WAN 相关对象（静态、接口、重新分发配置文件、BGP）。迁移脚本创建的逻辑路由器名称与同一模板的虚拟路由器名称相同。因此，中心和分支始终具有相同的路由器名称。

迁移后，*Panorama* 不允许您删除迁移的虚拟路由器。

Panorama SD-WAN 插件 3.1.0 可以使用高级路由引擎同时管理防火墙，也可以使用旧版路由引擎同时管理防火墙。这个功能的好处是，您可以将选定的托管防火墙迁移到新的高级路由引擎，同时在其他防火墙上保持当前的旧版路由引擎配置。

虽然 SD-WAN 插件 3.1.0 不管在旧版还是高级路由引擎上都可以管理防火墙，但在托管防火墙上一次只能有一个路由引擎配置生效。您可以使用 **Advanced Routing**（高级路由）选项启用或禁用高级路由引擎。每次更改防火墙将使用的引擎（启用或禁用高级路由以分别访问高级引擎或旧版引擎）时，必须提交配置并重新启动防火墙才能使更改生效。

在切换到高级路由引擎之前，请备份当前配置。同样地，如果您使用启用或禁用了高级路由的模板堆栈配置 *Panorama*，则在提交并将模板堆栈推送到设备后，您必须重新启动模板堆栈中的设备才能使更改生效。

配置 *Panorama* 时，为所有使用相同高级路由设置（全部启用或全部禁用）的设备创建设备组和模板堆栈。*Panorama* 不会将启用了高级路由的配置推送到不支持高级路由的小型防火墙。对于这些防火墙，*Panorama* 将推送旧版配置（如有）。

如果您计划使用虚拟路由器，请确保降级到适当的 SD-WAN 插件和 PAN-OS 版本，并禁用 **Advanced Routing**（高级路由）。降级 SD-WAN 插件时，使用单独的模板禁用 **Advanced Routing**（高级路由）（在本例中，创建了虚拟路由器）。

如果您已配置 **Advanced Routing**（高级路由）并想要切换到虚拟路由器，则禁用高级路由以返回到之前保存的虚拟路由器配置。在尝试降级程序（例如降级 PAN-OS 和 SD-WAN 插件版本）之前，提交并推送禁用高级路由后对防火墙所做的任何更改。

如果启用高级路由，则 SD-WAN 接口必须配置在同一个逻辑路由器中；它们不能拆分到不同的逻辑路由器中。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 将 Panorama 升级到 11.0 并安装 SD-WAN 插件 3.1.0。

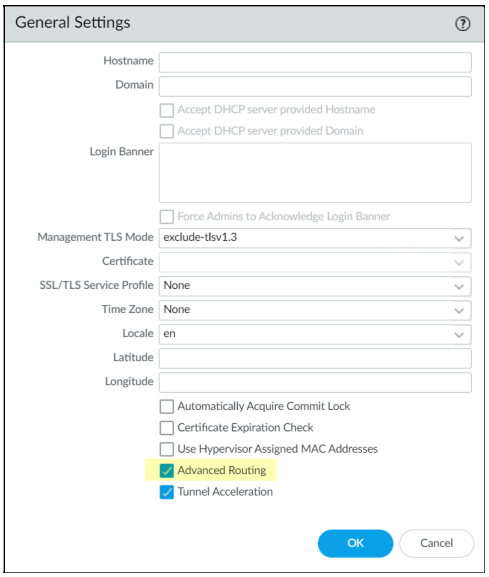
STEP 3 | 将您的中心和分支防火墙作为托管设备添加到 Panorama ™ 管理服务器中。

STEP 4 | 在启用高级路由之前备份当前的配置。

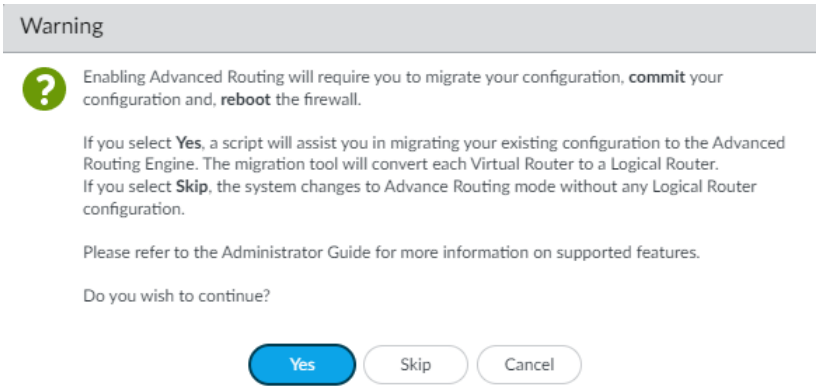
STEP 5 | 在 **Device**（设备）部分中，从 **Template**（模板）上下文下拉列表中选择相应的模板堆栈。

STEP 6 | 启用高级路由引擎。

1. 选择 **Device**（设备）> **Setup**（设置）> **Management**（管理），然后编辑常规设置。
2. 启用 **Advanced Routing**（高级路由）。SD-WAN 插件将根据高级路由选项的值创建逻辑路由器或虚拟路由器。启用高级路由后，将创建逻辑路由器。否则，将创建虚拟路由器。

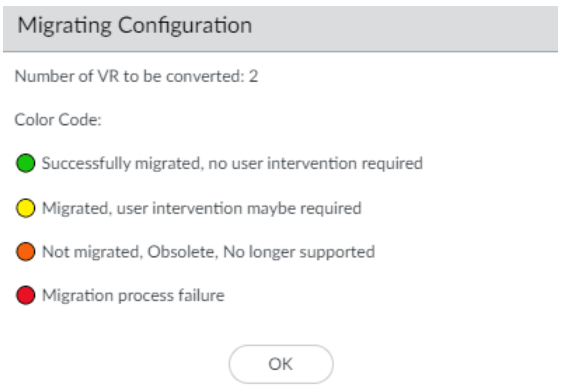


3. 单击 **OK**（确定）。
4. 将出现有关迁移的警告消息；单击 **Yes**（是）继续。

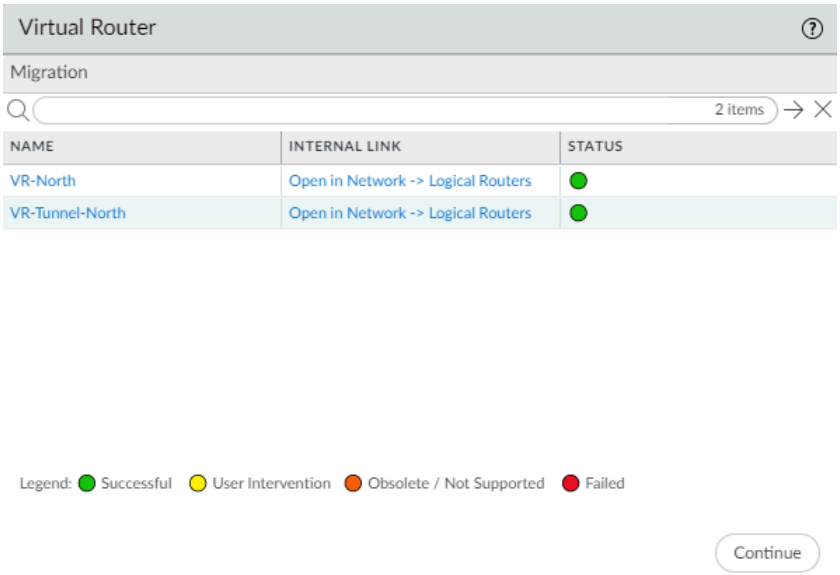


单击 **Yes**（是）后，内置迁移脚本会将您的现有配置迁移到高级路由引擎中。如果选择 **Skip**（跳过），则会为高级路由引擎创建一个空配置。

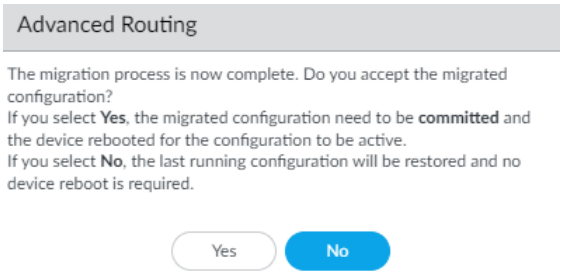
Migration Configuration（迁移配置）将显示指示迁移状态的颜色代码。



在 **Virtual Router**（虚拟路由器）中查看模板堆栈中模板的 **STATUS**（状态）。成功迁移的 **STATUS**（状态）应为绿色。否则，请对所有未成功迁移的模板采取必要的操作。



成功迁移后，每个虚拟路由器均将自动转换为相应的逻辑路由器。必须提交配置并重新启动防火墙才能使更改生效。



5. **Commit**（提交）。
6. 选择 **Device**（设备）> **Setup**（设置）> **Operations**（操作），然后选择 **Reboot Device**（重启设备）。

STEP 7 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

STEP 8 | 将您的配置更改提交并推送到受管防火墙。**Push to Devices**（推送到设备）以查看在所选 SD-WAN 防火墙中添加的逻辑路由器。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）和 **Edit Selections**（编辑选择）。
2. 选择 **Templates**（模板）并从列表中选择模板堆栈和模板。
3. 启用 **Force Template Values**（强制模板值）以使用更新的模板值覆盖本地配置。在使用此选项之前，检查防火墙上的替代值，确保您的提交不会导致任何意外的网络中断，或是因替换这些替代值而产生问题。
4. 单击 **OK**（确定）并 **Push**（推送）到设备。

STEP 9 | 重新登录防火墙。

STEP 10 | 选择 **Network**（网络）。

请注意菜单项，它们比旧版菜单上的单个项目（虚拟路由器）更符合行业标准并且更详细。**Routing**（路由）中包含 **Logical Routers**（逻辑路由器）和 **Routing Profiles**（路由配置文件），其中包括 **BGP**、**BFD**、**OSPF**、**OSPFv3**、**RIPv2**、**Filters**（筛选器）和 **Multicast**（组播）。

STEP 11 | 当配置中有多个模板堆栈时，必须单独为每个模板堆栈启用 **Advanced Routing**（高级路由）。对于要为高级路由更新的防火墙上的其他模板堆栈，重复步骤 5 到 10。

根据我们的设计要求，使用高级路由引擎时，逻辑路由器名称必须与同一模板的虚拟路由器名称相同。这意味着中心和分支始终具有相同的路由器名称。手动创建逻辑路由器而不是使用迁移脚本时，必须确保逻辑路由器名称和虚拟路由器名称相同。

STEP 12 | 在 SD-WAN 部署中选择虚拟或逻辑路由器。

选择 **Panorama** > **SD-WAN** > **Devices**（设备），以添加一个由 Panorama 管理服务器进行管理的 SD-WAN 设备（SD-WAN 中心或分支防火墙）。

除了用于添加 SD-WAN 设备的现有配置选项外，您现在还可以为 **Router Name**（路由器名称）选择逻辑路由器（用于高级路由引擎）或虚拟路由器（用于旧版引擎）。使用高级路由引擎时，逻辑路由器名称必须与同一模板的虚拟路由器名称相同。

选择用于在 SD-WAN 中心和分支之间进行路由的 **Router Name**（路由器名称）（逻辑或虚拟路由器）：

- 如果虚拟路由器和逻辑路由器名称相同，则 **Router Name**（路由器名称）将显示一个名称。
- 如果虚拟路由器和逻辑路由器名称不同，则 **Router Name**（路由器名称）同时显示虚拟路由器名称和逻辑路由器名称。您可以根据需要选择虚拟路由器（用于旧版引擎）或逻辑路由器（用于高级路由引擎）。

监控和报告

监控 VPN 集群中应用程序和链路运行状况，并生成相关报告，以标识和解决问题。为了便于 Panorama™ 管理服务器显示 SD-WAN 应用程序和链路运行状况信息，必须启用 SD-WAN 防火墙，将设备监视数据推送到 Panorama，并在将您的 SD-WAN 防火墙作为受管设备添加时配置 Panorama 的日志转发。如果尚未配置 SD-WAN 防火墙以将日志转发到 Panorama，则 SD-WAN **Monitoring**（监控）将不会显示应用程序或链路运行状况信息。

为了便于 *Panorama* 收集 *SD-WAN* 监控数据，必须将 *Panorama* 的 *SD-WAN* 配置推送到您的 *SD-WAN* 防火墙。如果未显示 *SD-WAN* 监控数据，请验证您是否成功推送了 *SD-WAN* 配置。

- 监控 SD-WAN 任务
- 监控 SD-WAN 应用程序和链路性能
- 监视 Prisma Access 中心
- 生成 SD-WAN 报告

监控 SD-WAN 任务

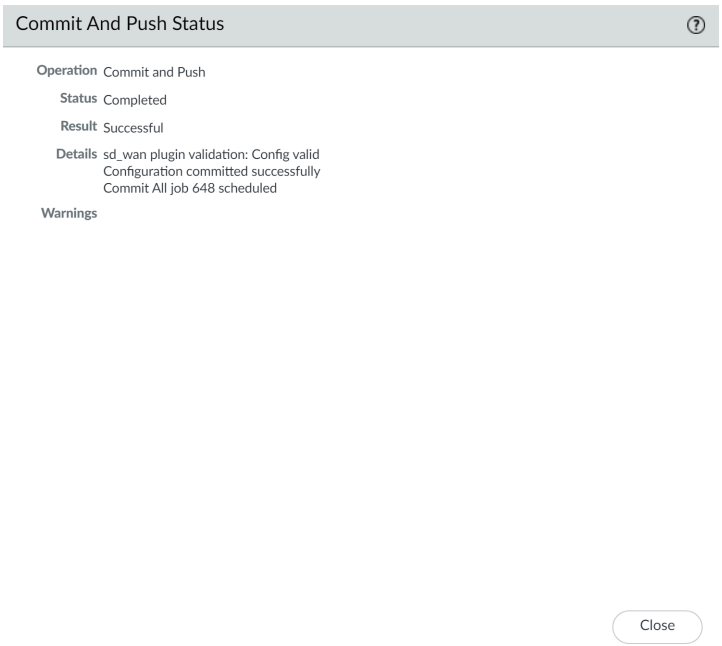
监控从 Panorama™ 管理服务器执行的提交、推送和其他 SD-WAN 任务，以获取特定任务有关的见解和详细信息。

如果任务结束后显示警告或失败，可以查看详细的警告和说明，以便更好地了解如何解决配置错误。此外，您还可以查看最后推送状态的详细信息，以查看导致任务出现警告或错误的原因的详细信息。

STEP 1 | 登录到 Panorama Web 界面。

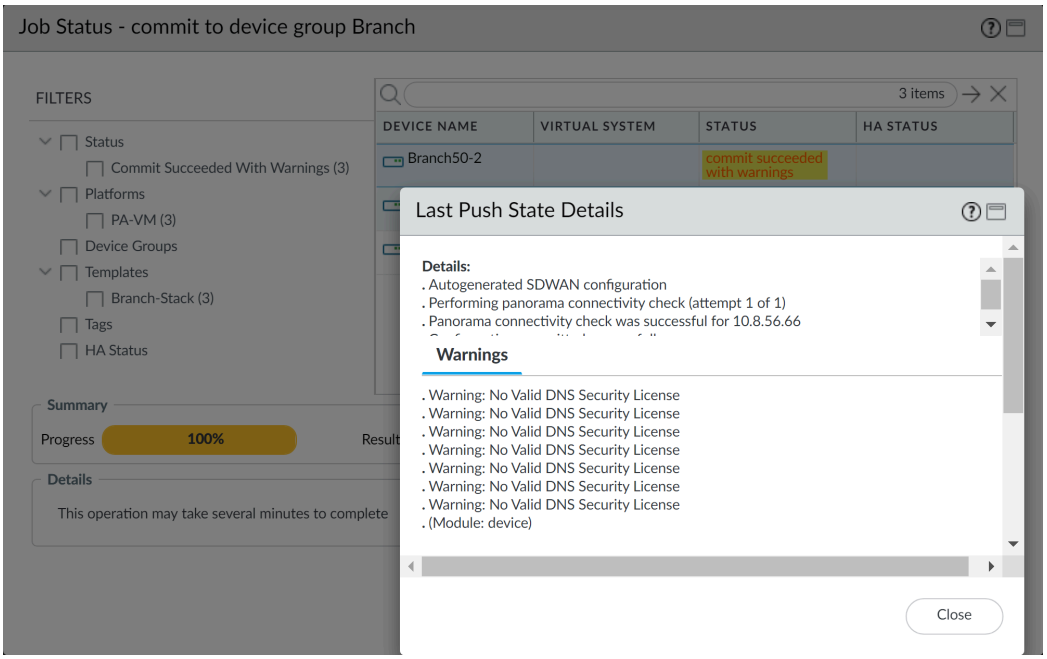
STEP 2 | 编辑 SD-WAN 配置后，**Commit**（提交）您的更改以查看作业状态。

作业状态窗口显示执行的操作、结果、以及与作业状态相关的任何详细信息和警告。



STEP 3 | 查看结束后出现警告或失败的作业的最后推送详细信息。

1. 单击 Web 界面底部的 **Tasks**（任务）(Tasks) 以打开任务管理器。
2. 单击用于 SD-WAN 任务的作业 **Type**（类型）。
3. 单击作业 **Status**（状态）以查看作业的最后推送状态详细信息。
4. 查看最后推送状态详细信息以标识和解决配置问题。



监控 SD-WAN 应用程序和链路性能

通过查看所有 VPN 集群的摘要信息，然后依次进行深入探究，将受影响的站点、应用程序和链路问题隔离，从而监控 VPN 集群中应用程序和链路性能，以解决问题。SD-WAN 流量的可见性显示在接收流量的 SD-WAN 防火墙上。例如，对于从中心防火墙到分支防火墙的流量，SD-WAN 监控数据将反映在分支防火墙上。登录仪表板将显示：

- 应用程序性能
  - **Impacted**（受影响的）— VPN 集群中的一个或多个应用，其路径的抖动、延迟或数据包丢失性能都没有达到路径列表中，防火墙选择路径质量配置文件的指定阈值。
  - **OK**（正常）— 从未出现抖动、延迟或数据包丢失性能问题的 VPN 集群、中心和分支的数量。
- 链路性能
  - **Error**（错误）— VPN 中有一个或多个站点在隧道或虚拟接口 (VIF) 断开时出现连接等问题。
  - **Warning**（警告）— 与超过七天动态指标平均值的抖动、延迟、或数据包丢失性能衡量相关的 VPN 集群、中心和分支的数量。
  - **OK**（正常）— 从未出现抖动、延迟或数据包丢失性能问题的 VPN 集群、中心和分支的数量。

如果中心或分支防火墙的 SD-WAN 策略规则配置了转发纠错，则会显示 `Error Correction Initiated`（纠错已启动）消息，通知您中心或分支防火墙检测到并更正了应用程序传输数据中的错误。

仅当流量从 *SD-WAN* 中心发往 *SD-WAN* 分支且与附加了纠错配置文件的 SD-WAN 策略规则匹配时，*SD-WAN* 中心才会显示 *`Error Correction Initiated`*（纠错已启动）。

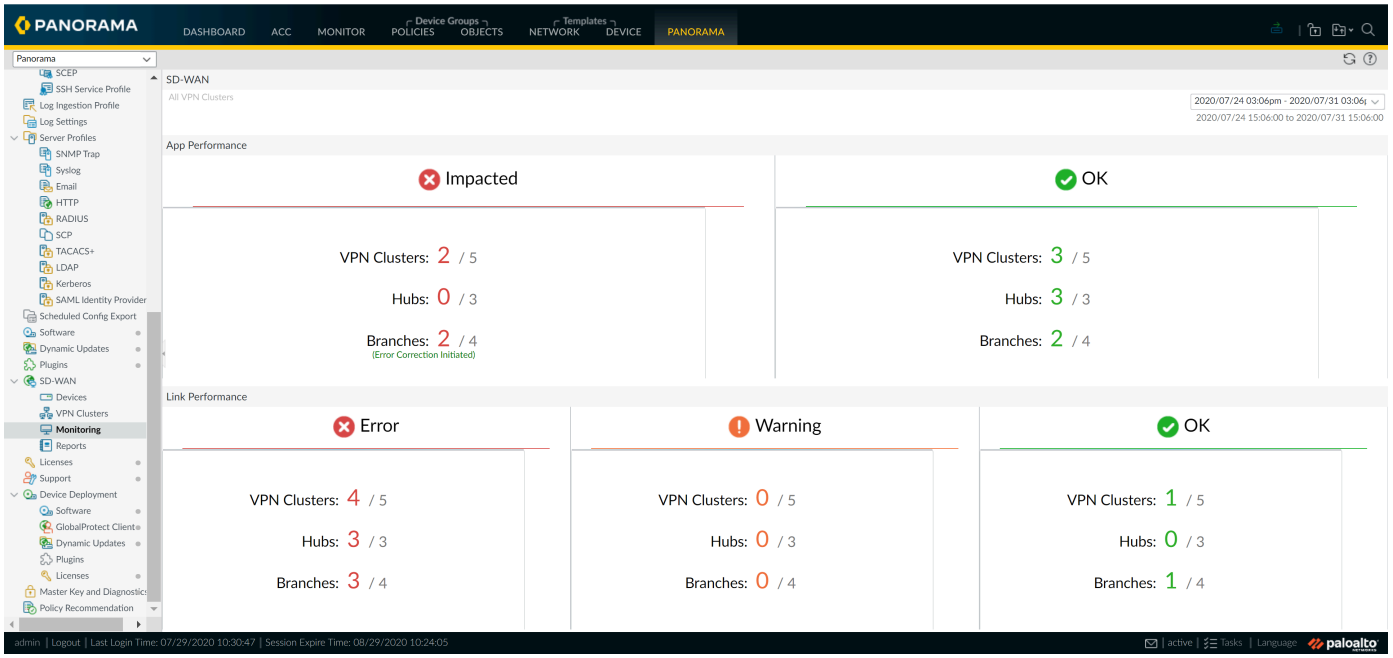
在登录仪表板中，将查看范围缩小到出现错误或警告状态的受影响应用程序或链路。然后，选择受影响的站点以查看站点级别详细信息。从站点中，查看应用程序级别或链路级别详细信息。

参阅监视 Prisma Access 中心应用程序和链路性能以监视 Prisma Access 中心的应用程序和链路性能。

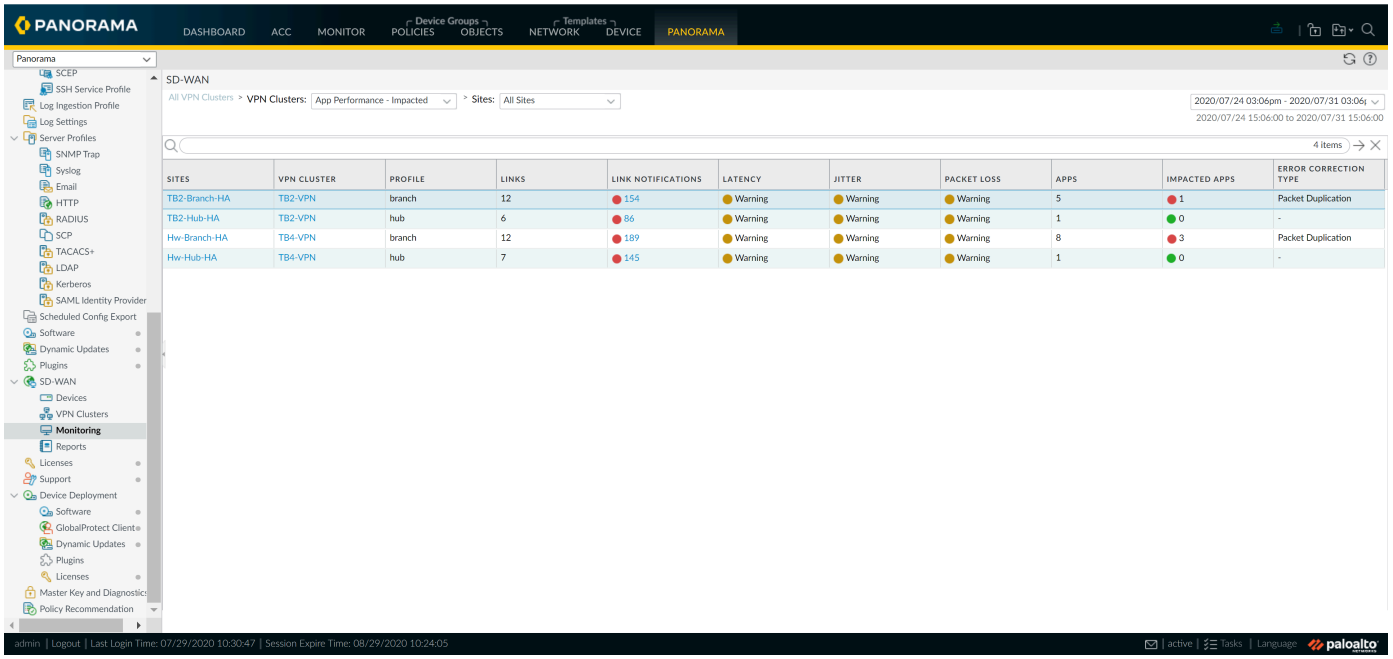
如果没有数据或屏幕指示 *SD-WAN* 未定义，请在 Compatibility Matrix（兼容性矩阵）中检查您正在使用的 *Panorama* 版本是否支持您尝试使用的 *SD-WAN* 插件版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Monitoring**（监控） 以快速查看 VPN 集群、中心和分支运行状况摘要。



STEP 3 | 单击指示受影响的、错误或警告计数的应用程序性能或链路性能摘要，以根据延迟、抖动和数据包丢失查看详细的站点和站点状态列表。



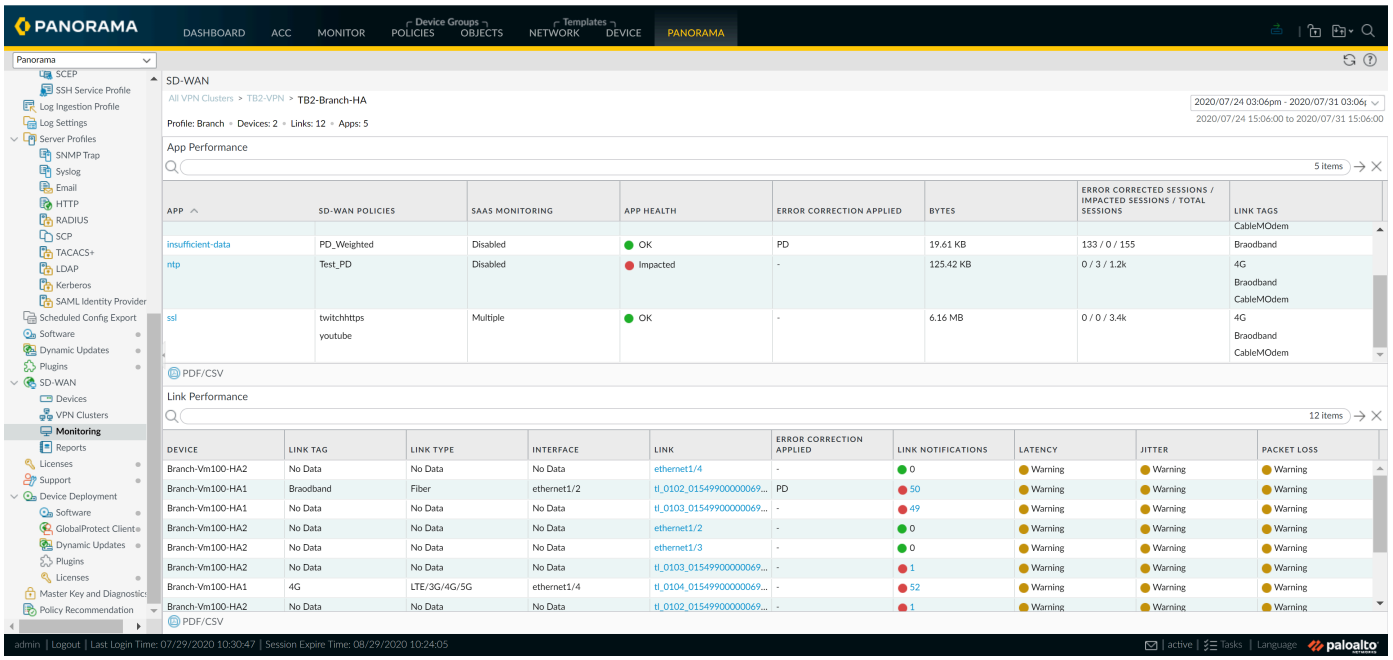
STEP 4 | 单击显示警告或错误的站点，以在 VPN 集群中查看。此站点显示应用程序性能和链路性能，包括受影响的应用程序。此外，使用站点筛选器，根据链路通知、延迟偏差、抖动偏差、数据包丢失偏差或受影响的应用程序查看 VPN 集群。

对于从直接互联网访问 (DIA) 链路访问的 SaaS 应用程序，**SaaS Monitoring**（**SaaS** 监控）列表示该应用程序是否是在 SaaS 质量配置文件中创建，是否与一个或多个 SD-WAN 策略规则关联。

- 禁用 — 该应用程序不是在 SaaS 质量配置文件中配置的 SaaS 应用程序。
- `Enabled` — 该应用程序是在 SaaS 质量配置文件中配置的 SaaS 应用程序，并与一个或多个 SD-WAN 策略关联。

如果您将一个纠错配置文件与一个应用程序的 SD-WAN 策略规则关联，则 **Error Correction Applied**（纠错已应用）列显示是否应用纠错和应用了哪种纠错类型。此外，您可以查看 **Error Corrected Sessions/Impacted Sessions/Total Sessions**（纠错会话/受影响会话/会话总数），了解在特定时间段内，分支或中心防火墙在会话总数中为多少会话进行了纠错。

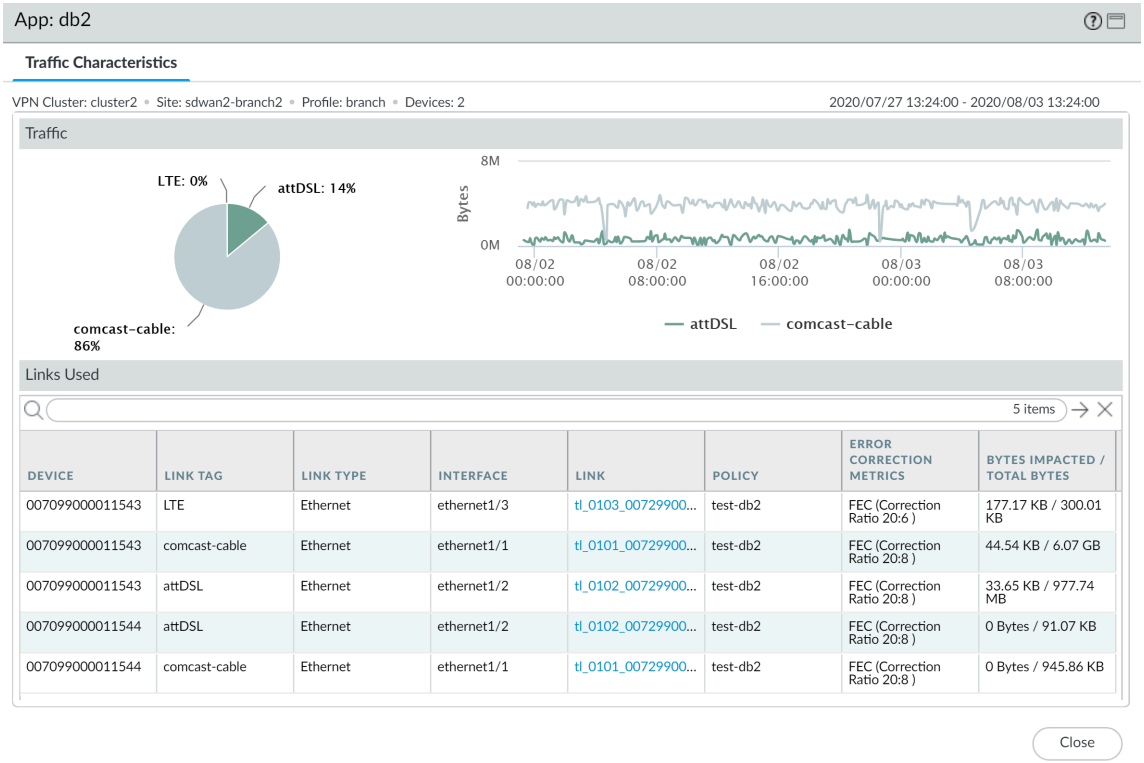
单击 **PDF/CSV** 以导出 PDF 或 CSV 格式的、站点中应用程序和链路详细的运行状况信息。

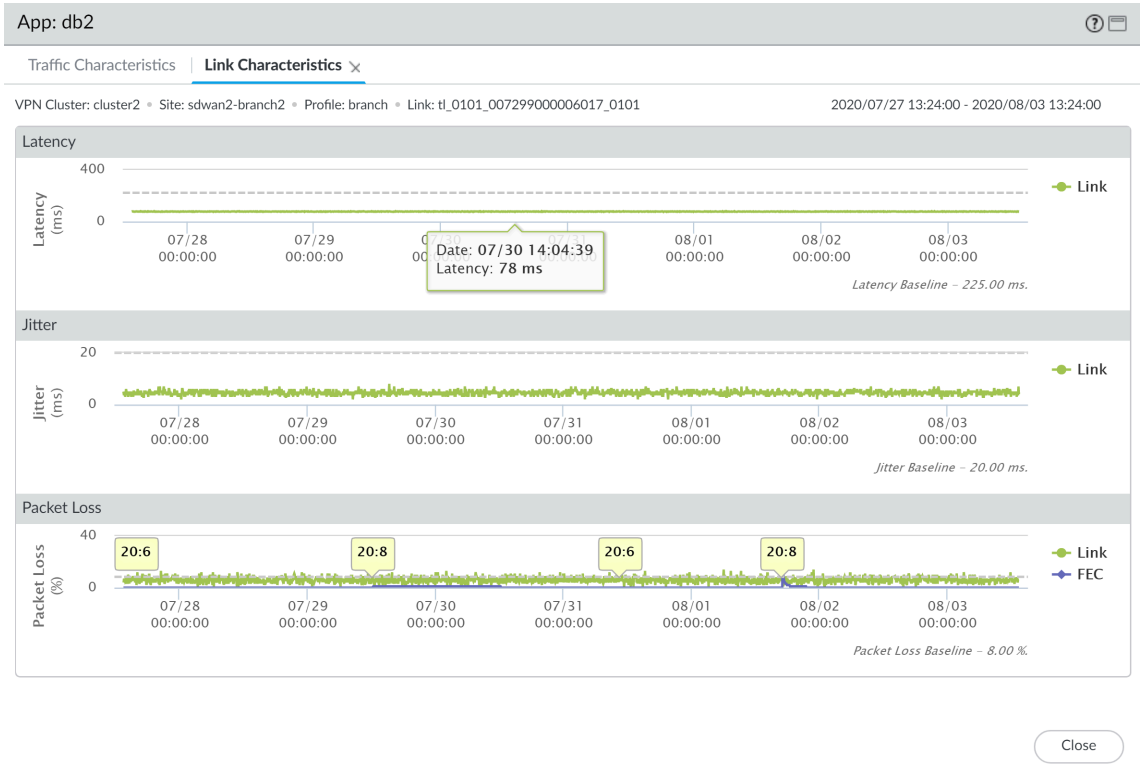


STEP 5 | 单击包括需要关注的应用程序的分支或中心。

STEP 6 | 单击受影响的应用程序以查看应用程序级别或链路级别的详细信息。

例如，查看应用程序的链路特征，了解应用程序在特定链路上的延迟、抖动和数据包丢失情况。此外，还可以查看何时对链路应用了纠错。





监视 Prisma Access 中心

为您的 Prisma Access 中心应用程序和链路性能设定基线并进行监视，了解如何配置和修改您的 SD-WAN 链路管理配置文件。

- 为您的 Prisma Access 中心应用程序和链路性能设定基线
- 监视 Prisma Access 中心应用程序和链路性能

为您的 Prisma Access 中心应用程序和链路性能设定基线

在您配置 SD-WAN 链路管理配置文件之前，Palo Alto Networks 建议您为 Prisma Access 中心应用程序和链路性能设定基线，以更好地了解 Prisma Access 中心的正常有效负载活动，从而避免为不需要它的应用程序和流量进行不必要的链路交换。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | Prisma Access 板载 PAN-OS 防火墙.

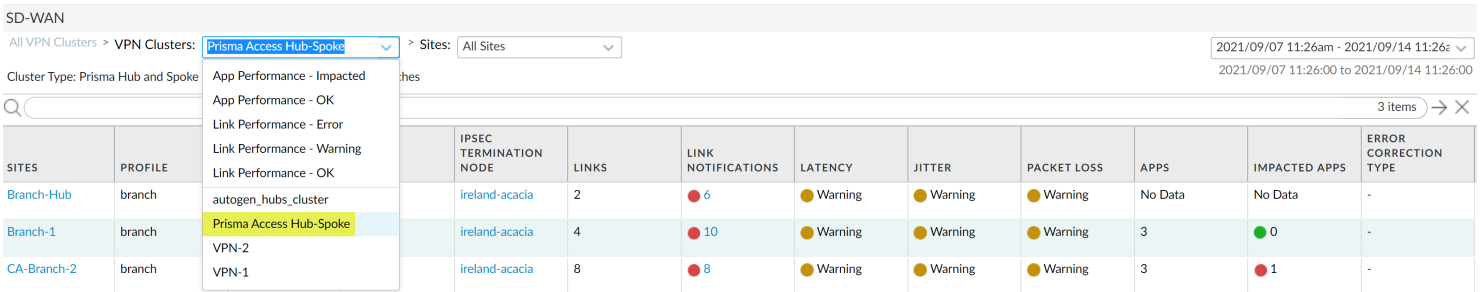
STEP 3 | 选择 **Panorama** > **SD-WAN** > **Monitoring**（监视）并修改 SD-WAN 监视时间范围。

您用于为 Prisma Access 中心应用程序和链路性能创建基线的时间范围越长，基线就越准确。至少使用三天的应用程序和链路性能来为用于创建 SD-WAN 链路管理配置文件的延迟、抖动和数据包丢失数据创建基线。

Palo Alto Networks 建议评估 *7* 天的应用程序和链路性能数据，以便为 *Prisma Access* 中心的延迟、抖动和数据包丢失创建基线。

STEP 4 | 筛选 SD-WAN 监视以仅显示您的 Prisma Access 中心辐射型 VPN 集群。

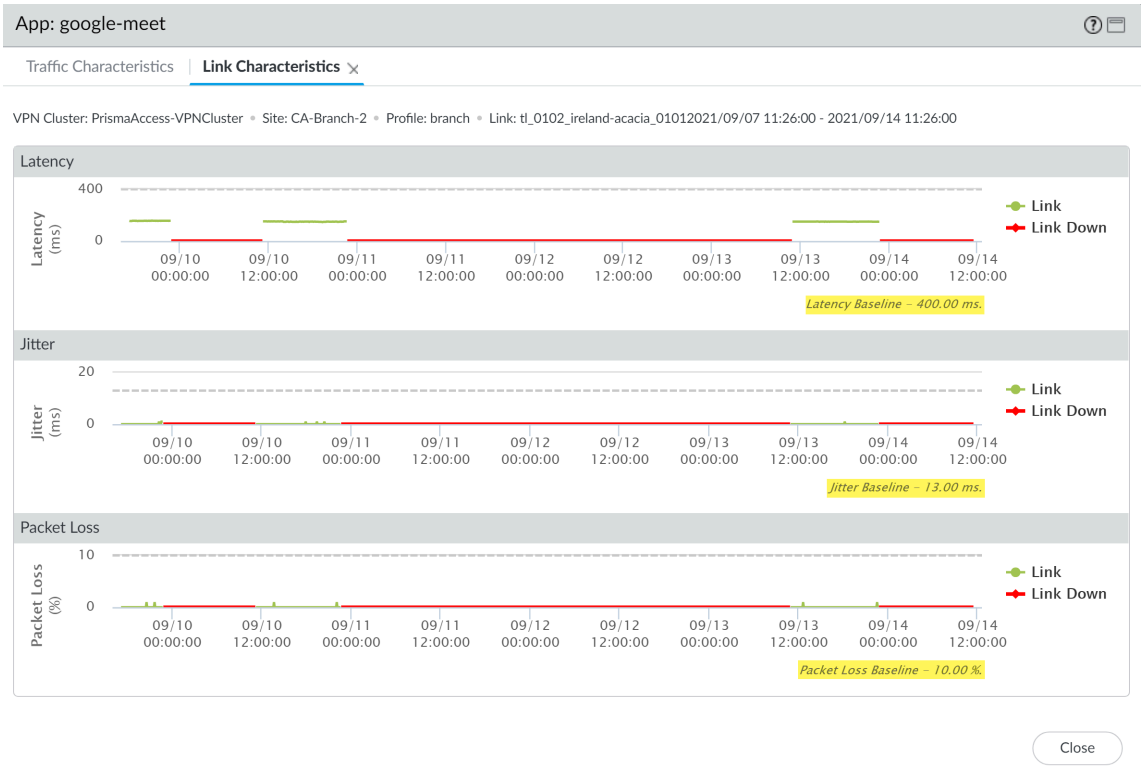
1. 单击指示受影响的、错误或警告计数的应用程序性能或链路性能摘要，以根据延迟、抖动和数据包丢失查看详细的站点和站点状态列表。
2. 在 VPN 集群筛选器中，选择 **Prisma Access Hub-Spoke**（**Prisma Access** 中心辐射型）。
3. 单击一个站点以查看 Prisma Access 中心的详细运行状况。



STEP 5 | 查看 Prisma Access 中心应用程序的链路特征。

1. 单击应用程序性能部分中的应用程序以查看流量特征和用于应用程序流量的链路。
2. 单击每个链路以查看在整个链路上为应用程序测量的延迟、抖动和数据包丢失基线。

   对所有链路重复此操作，直到您收集到足够的基准数据来修改 Prisma Access 中心路径质量配置文件。



STEP 6 | 根据您收集的延迟、抖动和数据包丢失基线修改 Prisma Access 中心路径质量配置文件 。

STEP 7 | 根据需要继续配置 SD-WAN。

STEP 8 | 监视 Prisma Access 中心应用程序和链路性能以进一步微调您的 SD-WAN 链路管理配置文件。

监视 Prisma Access 中心应用程序和链路性能

通过查看所有 Prisma Access 中心的摘要信息，然后依次进行深入探究，将受影响的站点、应用程序和链路问题隔离，从而监视 VPN 集群中应用程序和链路性能，以解决问题。SD-WAN 流量的可见性显示在 Prisma Access 部署上或接收流量的 SD-WAN 防火墙上。例如，对于从中心防火墙到分支防火墙的流量，SD-WAN 监控数据将反映在分支防火墙上。登录仪表板将显示：

- 应用程序性能
  - **Impacted**（受影响的）— VPN 集群中的一个或多个应用，其路径的抖动、延迟或数据包丢失性能都没有达到路径列表中，防火墙选择路径质量配置文件的指定阈值。
  - **OK**（正常）— 从未出现抖动、延迟或数据包丢失性能问题的 VPN 集群、中心和分支的数量。
- 链路性能
  - **Error**（错误）— VPN 中有一个或多个站点在隧道或虚拟接口 (VIF) 断开时出现连接等问题。
  - **Warning**（警告）— 与超过七天动态指标平均值的抖动、延迟、或数据包丢失性能衡量相关的 VPN 集群、中心和分支的数量。
  - **OK**（正常）— 从未出现抖动、延迟或数据包丢失性能问题的 VPN 集群、中心和分支的数量。

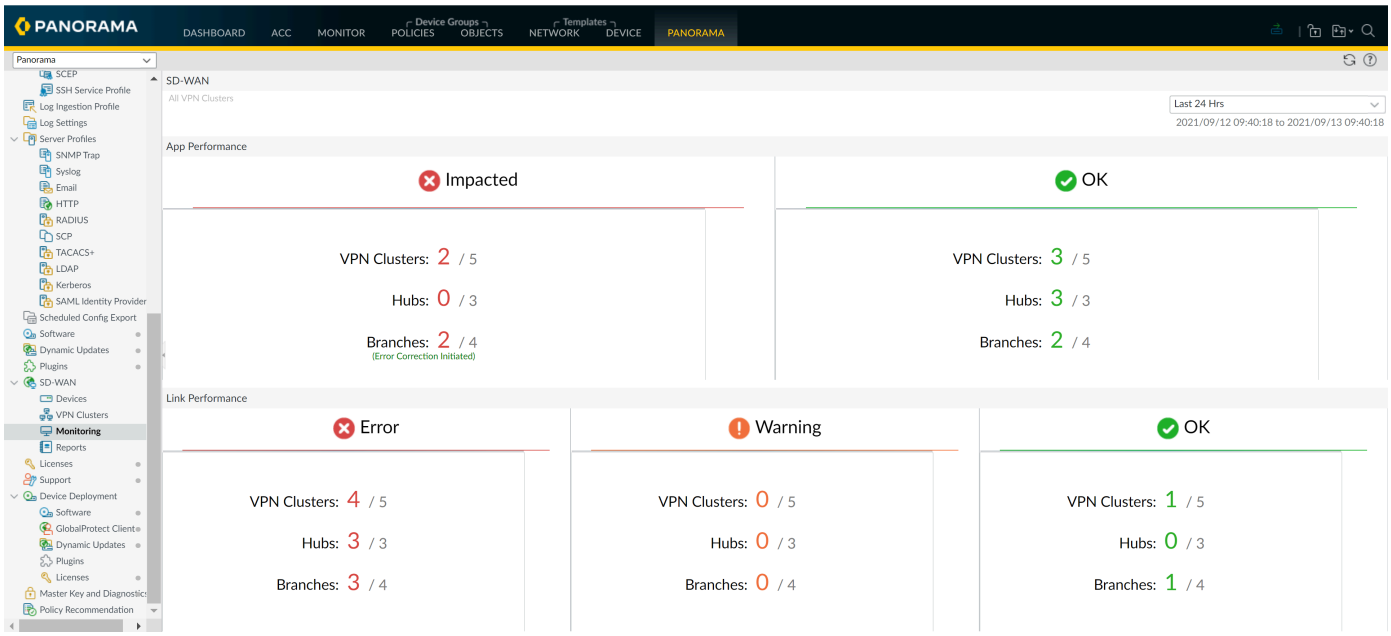
在登录仪表板中，将查看范围缩小到出现错误或警告状态的受影响应用程序或链路。然后，选择受影响的站点以查看站点级别详细信息。从站点中，查看应用程序级别或链路级别详细信息。

请参阅监控 SD-WAN 应用程序和链路性能以监视所有 SD-WAN 站点的应用程序和链路性能。

如果没有数据或屏幕指示 *SD-WAN* 未定义，请在 Compatibility Matrix（兼容性矩阵）中检查您正在使用的 *Panorama* 版本是否支持您尝试使用的 *SD-WAN* 插件版本。

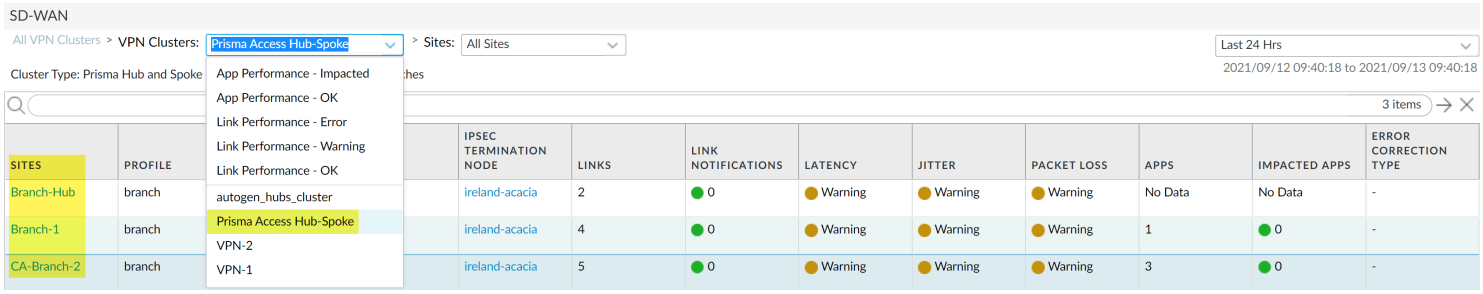
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Monitoring**（监控） 以快速查看 VPN 集群、中心和分支运行状况摘要。



STEP 3 | 筛选 SD-WAN 监视以仅显示您的 Prisma Access 中心辐射型 VPN 集群。

1. 单击指示受影响的、错误或警告计数的应用程序性能或链路性能摘要，以根据延迟、抖动和数据包丢失查看详细的站点和站点状态列表。
2. 在 VPN 集群筛选器中，选择 **Prisma Access Hub-Spoke**（**Prisma Access** 中心辐射型）。
3. 单击一个站点以查看 Prisma Access 中心的详细运行状况。



STEP 4 | 查看 Prisma Access 中心的运行状况详情。

站点数据显示 Prisma Access 登录详细信息以及应用程序性能和链路性能，包括受影响的应用程序。

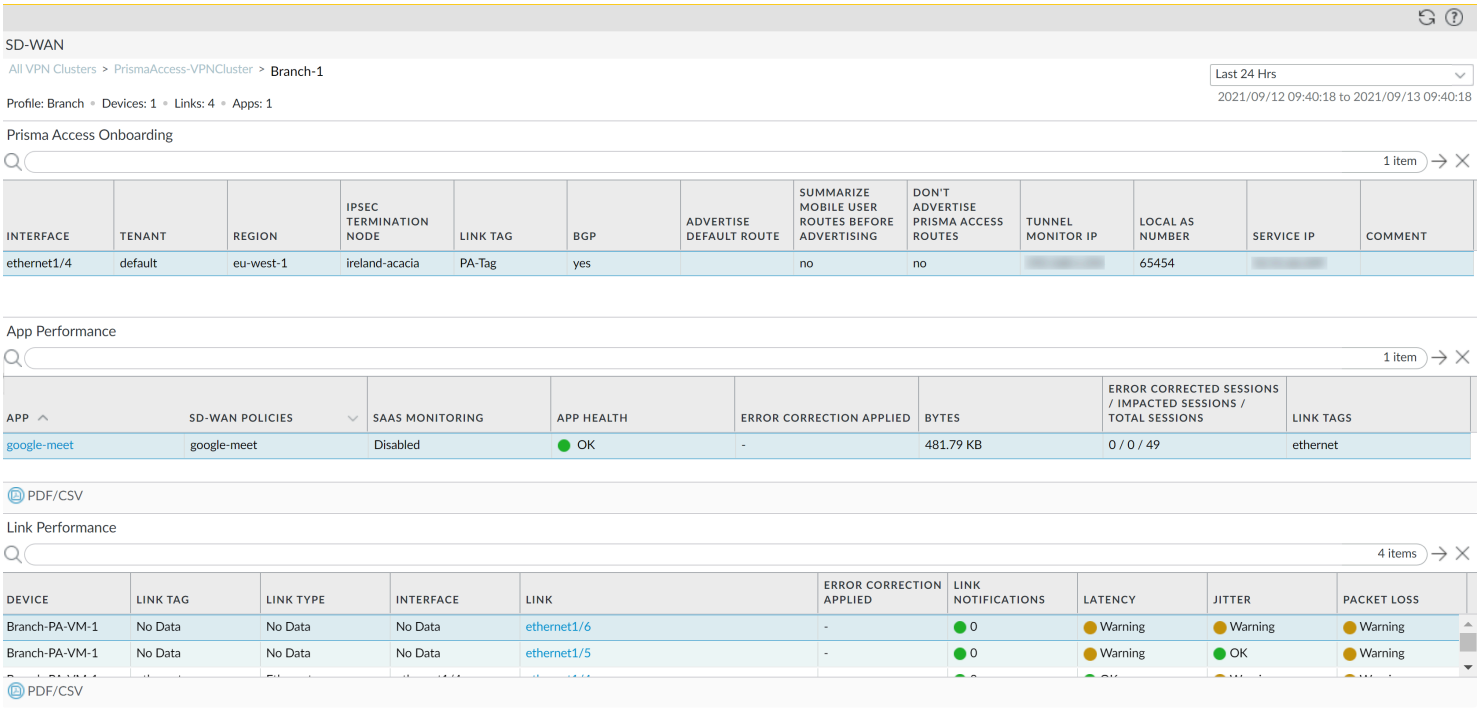
对于从直接互联网访问 (DIA) 链路访问的 SaaS 应用程序，**SaaS Monitoring**（**SaaS** 监控）列表示该应用程序是否是在 SaaS 质量配置文件中创建，是否与一个或多个 SD-WAN 策略规则关联。

- 禁用 — 该应用程序不是在 SaaS 质量配置文件中配置的 SaaS 应用程序。
- `Enabled` — 该应用程序是在 SaaS 质量配置文件中配置的 SaaS 应用程序，并与一个或多个 SD-WAN 策略关联。

如果您将一个纠错配置文件与一个应用程序的 SD-WAN 策略规则关联，则 **Error Correction Applied**（纠错已应用）列显示是否应用纠错和应用了哪种纠错类型。此外，您可以查看 **Error**

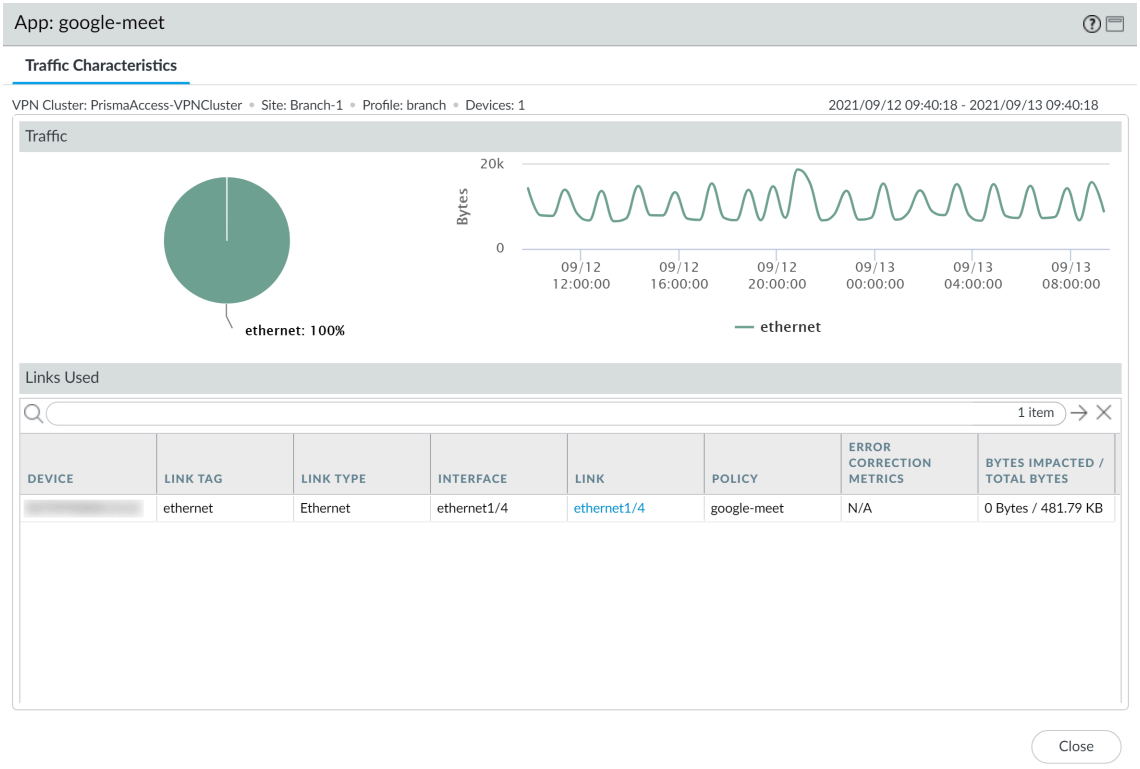
Corrected Sessions/Impacted Sessions/Total Sessions（纠错会话/受影响会话/会话总数），了解在特定时间段内，分支或中心防火墙在会话总数中为多少会话进行了纠错。

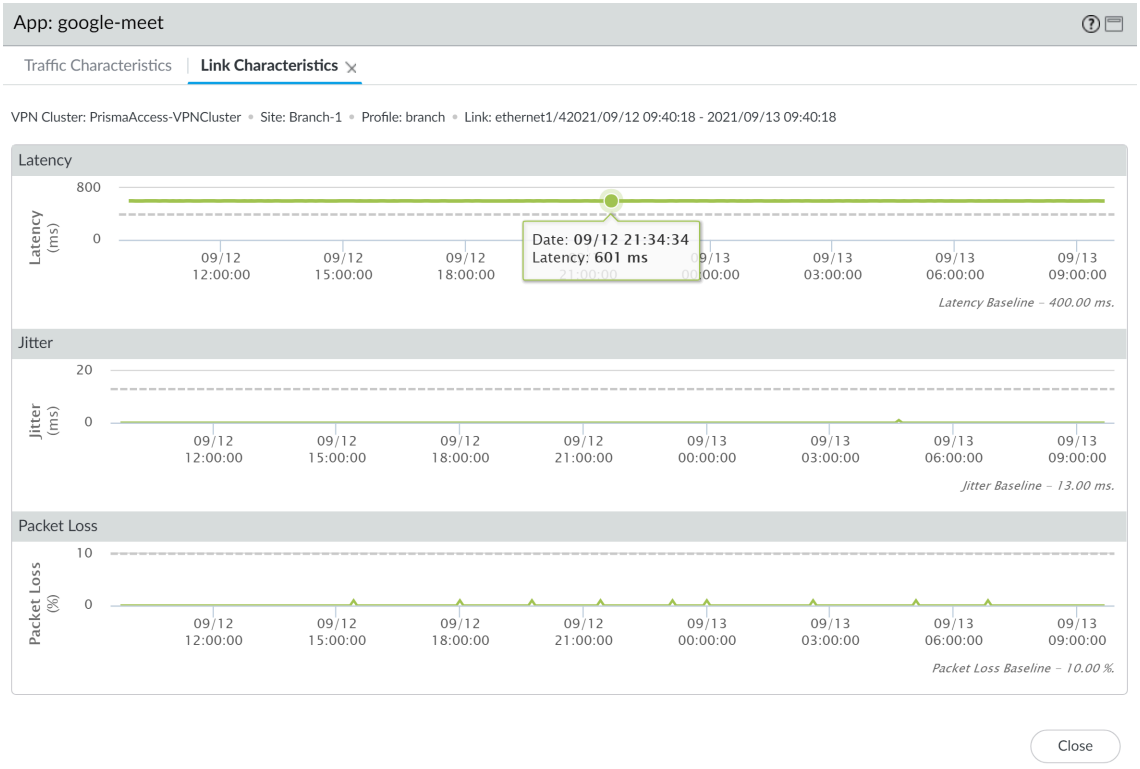
单击 **PDF/CSV** 以导出 PDF 或 CSV 格式的、站点中应用程序和链路详细的运行状况信息。



STEP 5 | 单击受影响的应用程序以查看应用程序级别或链路级别的详细信息。

例如，查看应用程序的链路特征，了解应用程序在特定链路上的延迟、抖动和数据包丢失情况。此外，还可以查看何时对链路应用了纠错。





生成 SD-WAN 报告

配置并生成一份详细描述路径质量下降最频繁、且排名靠前的应用程序或链路的 SD-WAN 报告。报告中应用程序或链路的出现顺序依据受影响的数据量而定；受影响的数据越多，报告中出现的应用程序或链路越多。SD-WAN 报告按需要生成，无法通过计划生成。使用 SD-WAN 报告验证应用程序或链路的吞吐量是否正确，或是确保用户不会注意到应用程序或链路的影响。例如，如果 ISP 保证链路上有一定的吞吐量，会为此链路生成一个链路性能报告，以检验是否遵守保证的带宽。

在 Panorama™ 管理服务器中，您只能为所有启用了 SD-WAN 功能的防火墙上的应用程序或链路生成报告。要为单个防火墙处理的应用程序或链路生成报告，您必须在防火墙上本地创建和生成报告。

如果没有数据或屏幕指示 *SD-WAN* 未定义，请在 Compatibility Matrix（兼容性矩阵）中检查您正在使用的 *Panorama* 版本是否支持您尝试使用的 *SD-WAN* 插件版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Reports**（报告），然后 **Add**（添加）新报告。

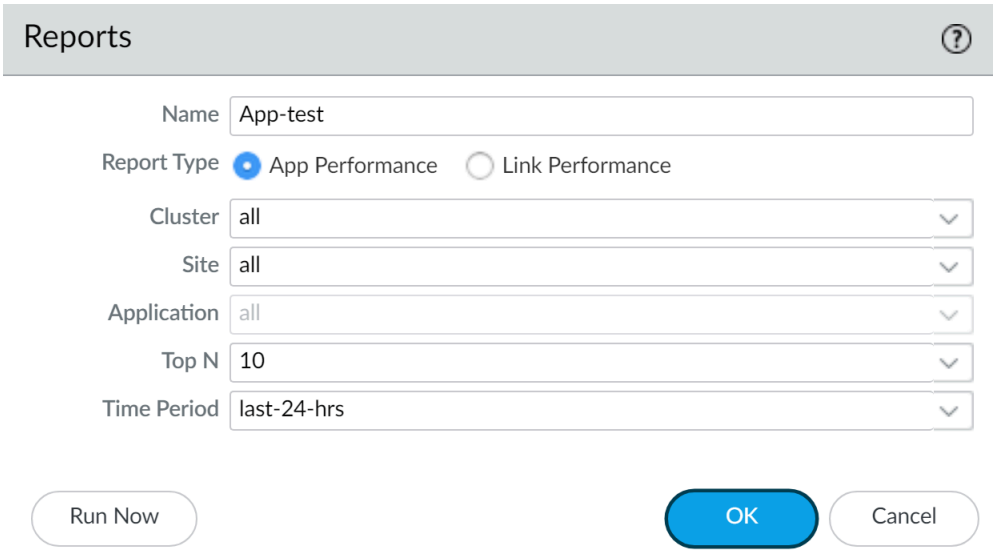
STEP 3 | 配置 SD-WAN 报告参数。

1. 输入报告的描述性 **Name**（名称）。
2. 选择要生成的 **Report Type**（报告类型）：
   - 选择 **App Performance**（应用程序性能）生成一份仅对应用程序运行状况进行详细描述的报告。
   - 选择 **Link Performance**（链路性能）生成一份仅对链路运行状况进行详细描述的报告。
3. 选择要为其生成报告的 VPN **Cluster**（集群）。默认选择 **all**（全部）。
4. 选择要为其生成报告的所选 VPN 集群的 **Site**（站点）。默认选择 **all**（全部）。

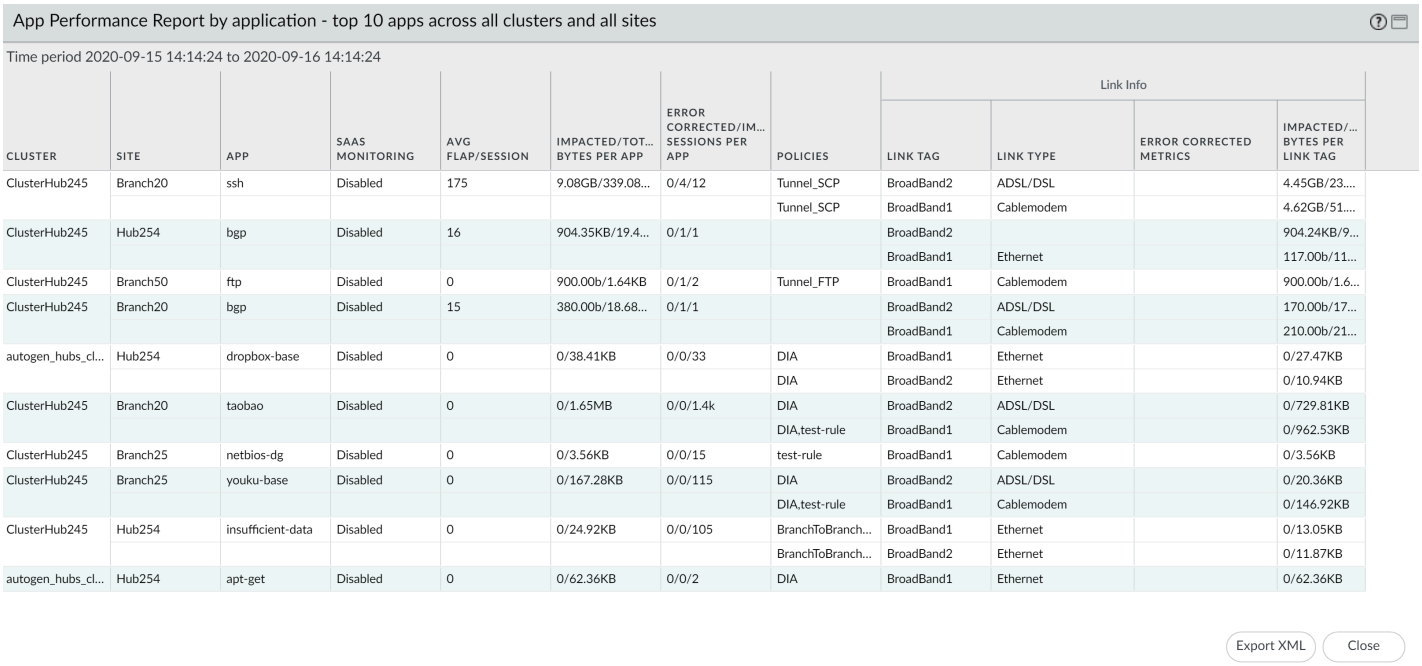
   如果选择 **all**（全部）集群，则此字段显示为灰色，且无法勾选站点。
5. （仅限应用程序性能）选择要为其生成报告的 **Application**（应用程序）。

   如果选择 **all**（全部）集群和站点，则此字段显示为灰色，且无法勾选单个应用程序。
6. （仅限链路性能）选择要为其生成报告的 **Link Tag**（链路标记）。勾选链路标记后，会为在集群或站点中使用此标记进行分组的所有链路生成一份报告。默认选择 **all**（全部）。
7. （仅限链路性能）选择要为其生成报告的 **Link Type**（链路类型）。勾选链路类型后，会为集群或站点中指定类型的所有链路生成一份报告。默认选择 **all**（全部）。
8. 选择报告中包含的 **Top N**（前 **N** 个）应用程序或链路。通过此设置，可以确定报告中包含的、出现运行状况恶化的应用程序或链路的数量。默认情况下，报告中包含前 **5** 个出现运行状况恶化的应用程序或链路。
9. 指定在其中生成报告的 **Time Period**（时段）。默认会选择 **None**（无），然后，查询应用程序或链路整个运行状况历史记录。

STEP 4 | 单击 **Run Now**（立即运行）以生成报告。



STEP 5 | 查看生成的报告，然后 **Export XML**（导出 **XML**） 以将 XML 格式的报告导出到您的本地设备。准备就绪后，请单击 **Close**（关闭）。



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 | 在报告弹出窗口中，单击 **OK**（确定）以保存您配置的报告。

STEP 7 | **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

故障排除

使用 Panorama™ 管理服务器命令行接口 (CLI) 查看 SD-WAN 信息，然后执行操作。

将 CLI 命令用于 SD-WAN 任务

使用以下 CLI 命令查看和清除 SD-WAN 信息，以及查看 SD-WAN 全局计数器。此外，您还可以查看 VPN 隧道信息、BGP 信息和 SD-WAN 接口信息。

如果您要...	请使用...
查看或清除 **SD-WAN** 信息	
• 查看 SD-WAN 接口的路径名称和 ID、他们的状态、本地和对等 IP 地址、以及隧道接口编号。	`> show sdwan connection all | <sdwan-interface>`
• 查看分发给 SD-WAN 虚拟接口各个隧道编号的会话数和百分比。	`> show sdwan session distribution policy-name <sdwan-policy-name>`
• 查看将流量发送到指定 SD-WAN 虚拟接口的 SD-WAN 策略规则名称，以及流量分发方法，配置的延迟、抖动和数据包丢失阈值，标识用于规则的链路标记，以及成员隧道接口。	`> show sdwan rule vif sdwan.x`
• 查看路径选择和路径质量测量等 SD-WAN 事件。 对于 *PAN-OS 10.0.0* 和 *10.0.1*，当您更改 *SD-WAN* 配置（例如路径质量配置文件更改）而导致选择了不同的 *SD-WAN* 路径时，流量日志不会计算或记录此次路径更改。	`> show sdwan event`
• 清除 SD-WAN 事件。	`> clear sdwan event`
• 查看 SD-WAN 虚拟接口（指定接口编号和名称）上的延迟、抖动和数据包丢失。 在三个时间框架内对延迟、抖动和数据包丢失进行测量，并获取平均值。每个时间框架都有一个随（超出阈值的）运行状况参数	`> show sdwan path-monitor stats vif <sdwan.x>`

如果您要...	请使用...
值更改而递增的运行状况版本。除实时测量外，还会采用当前使用测量，从而显示在上次实时测量值更改超出阈值时的参数值。	`> show sdwan path-monitor stats vif <sdwan-interface-name>`
• 查看与指定会话匹配的 SD-WAN 策略规则名称，源和目标隧道接口，配置用于规则的延迟、抖动和数据包丢失百分比，以及流量分发方法。 对于 *PAN-OS 10.0.0* 和 *10.0.1*，当您更改 *SD-WAN* 配置（例如路径质量配置文件更改）而导致选择了不同的 *SD-WAN* 路径时，流量日志不会计算或记录此次路径更改。	`> show sdwan session path-select session-id <session-id>`
• 查看（积极的或宽松的） SD-WAN 虚拟链路的监控模式以及更新间隔。	`> show sdwan path-monitor parameter path-name <sdwan-path-name>`
• 查看（积极的或宽松的） SD-WAN 虚拟链路的监控模式、更新间隔以及探测统计信息。	`> show sdwan path-monitor parameter vif <sdwan.x>`
查看全局计数器以排除 **SD-WAN** 故障	

• 在分支上，验证发送的 SD-WAN 探测请求数据包数量是否与接收到的探测回复数据包数量一致。
 	
在分支防火墙上，大多数 SD-WAN 隧道都是启动器，这就是说，隧道已启用 SD-WAN 路径监控探测。
	`> show counter global filter delta yes`
	
	`flow_sdwan_prob_req_tx`
	
	`flow_sdwan_prob_reply_rx`

• 在中心上，验证接收到的 SD-WAN 探测请求数据包数量是否与发送的探测回复数据包数量一致。
 	
在中心防火墙上，大多数 SD-WAN 都是响应者，这就是说，隧道已启用 SD-WAN 路径监控探测。
	`> show counter global filter delta yes`
	
	`flow_sdwan_prob_req_rx`
	
	`flow_sdwan_prob_reply_tx`

查看 **VPN** 隧道信息	

如果您要...	请使用...
• 查看防火墙上创建的所有隧道。	`> show vpn flow`
• 查看按名称标识的各个隧道的详细信息。	`> show vpn flow name <name>`
• 查看按 ID 标识的各个隧道的详细信息。	`> show vpn flow tunnel-id <tunnel-id>`
• 查看所有隧道的互联网密钥交换 (IKE) 阶段 1 和阶段 2 的详细信息。	`> show vpn ike-sa`
• 查看特定网关的 IKEv2 安全关联 (SA) 和 IKEv2 IPSec 子 SA。	`> show vpn ike-sa gateway <gateway>`
• 查看隧道详细信息。	`> show vpn tunnel`
查看 **BGP** 信息	
• 查看虚拟路由器的 BGP 摘要。	`> show routing protocol bgp summary virtual-router <virtual-router>`
• 查看 BGP 对等的摘要。	`> show routing protocol bgp peer peer-name <peer-name> virtual-router <virtual-router>`
• 查看本地路由信息库 (RIB) 的摘要。	`> show routing protocol bgp loc-rib`
查看 **RIB** 和 **FIB** 中的 **SD-WAN** 接口信息	
• 查看新的 SD-WAN 出口接口。	`> show routing route`

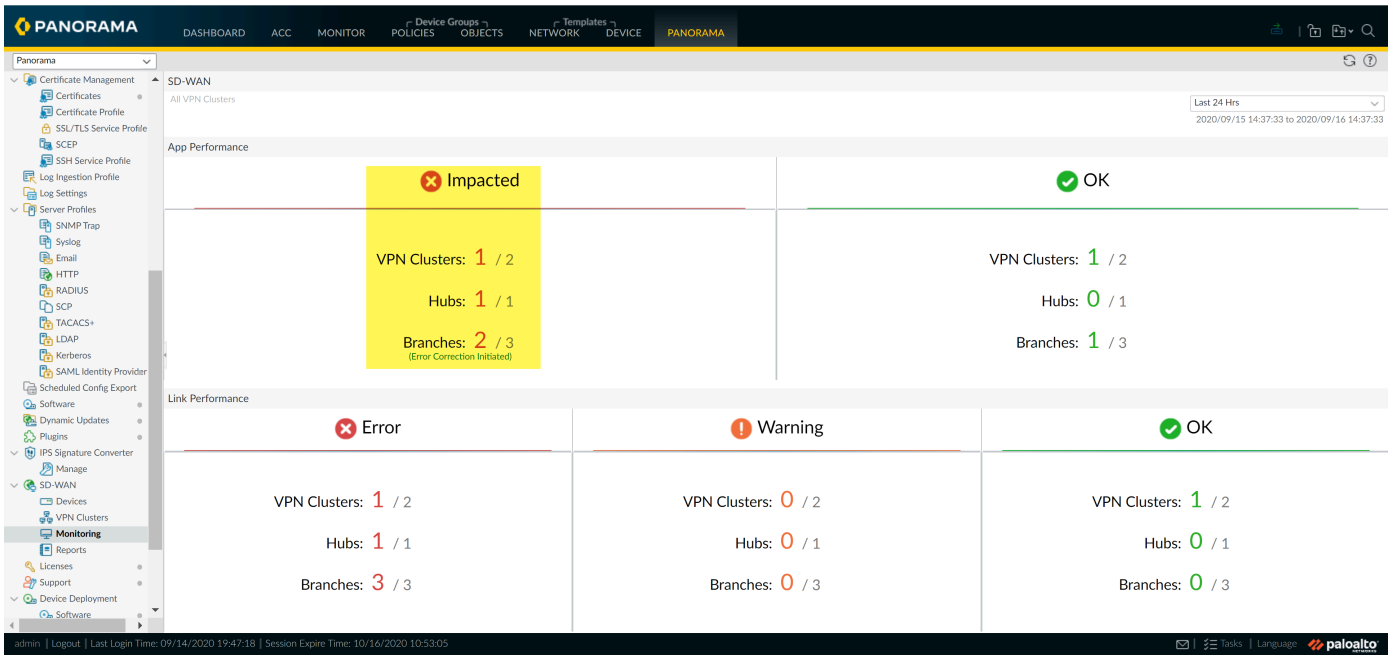
如果您要...	请使用...
• 查看转发信息库 (FIB) 中的 SD-WAN 接口。	`> show routing fib`

排除应用程序性能故障

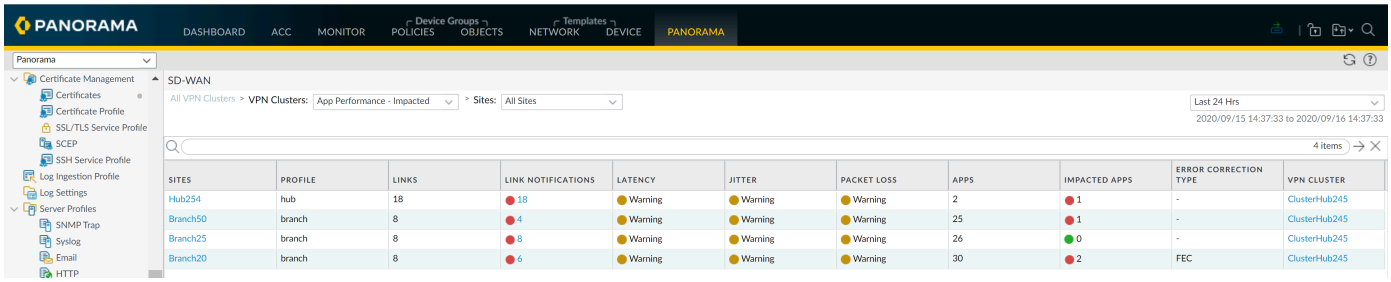
了解导致应用程序和服务性能下降的原因是确保用户体验不会受影响的必要一环。了解导致 VPN 集群受影响的原因，以及应用程序流量故障转移到不同链路的原因，可帮助您对 SD-WAN 配置进行微调。

STEP 1 | 登录到 Panorama Web 界面。

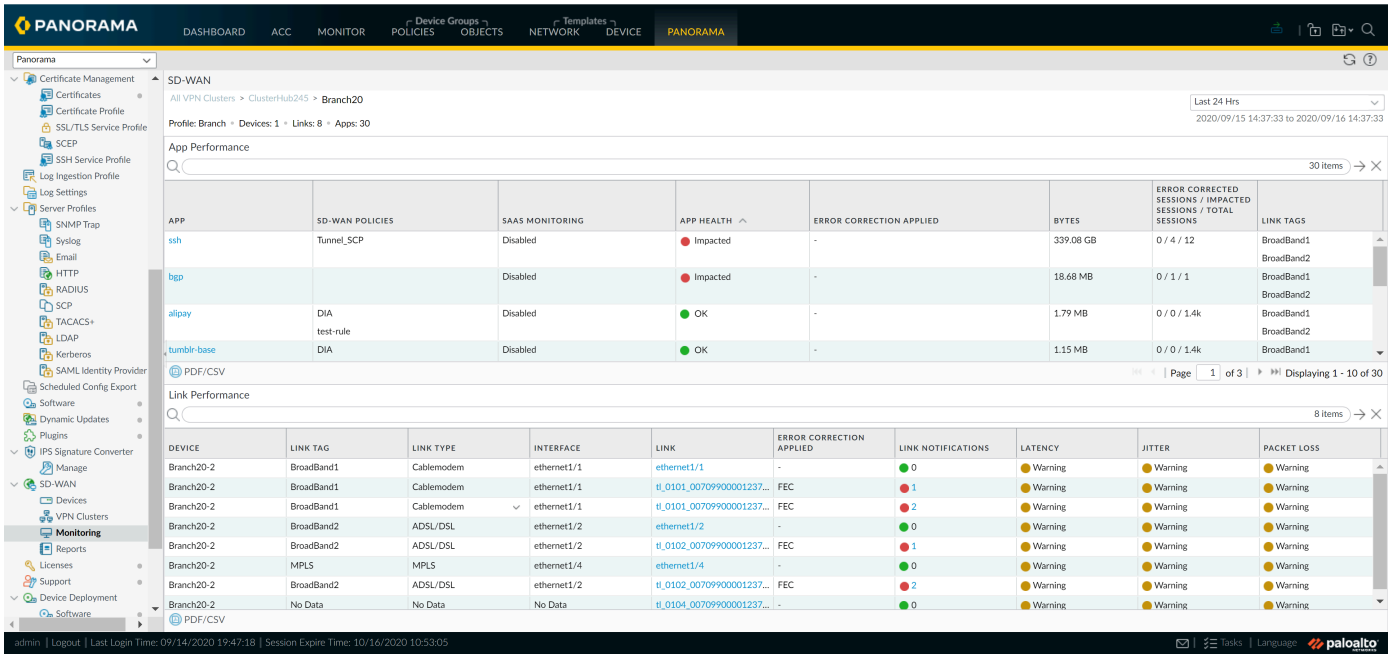
STEP 2 | 选择 **Panorama** > **SD-WAN** > **Monitoring**（监控），然后查看 **Impacted**（受影响的）VPN 集群。



STEP 3 | 基于从 **Site**（站点）下拉列表中获得的首选指标筛选 VPN 集群，然后选择时间框架。在此示例中，我们将查看最近 12 小时内包含受影响 VPN 集群的 **All Sites**（所有站点）。

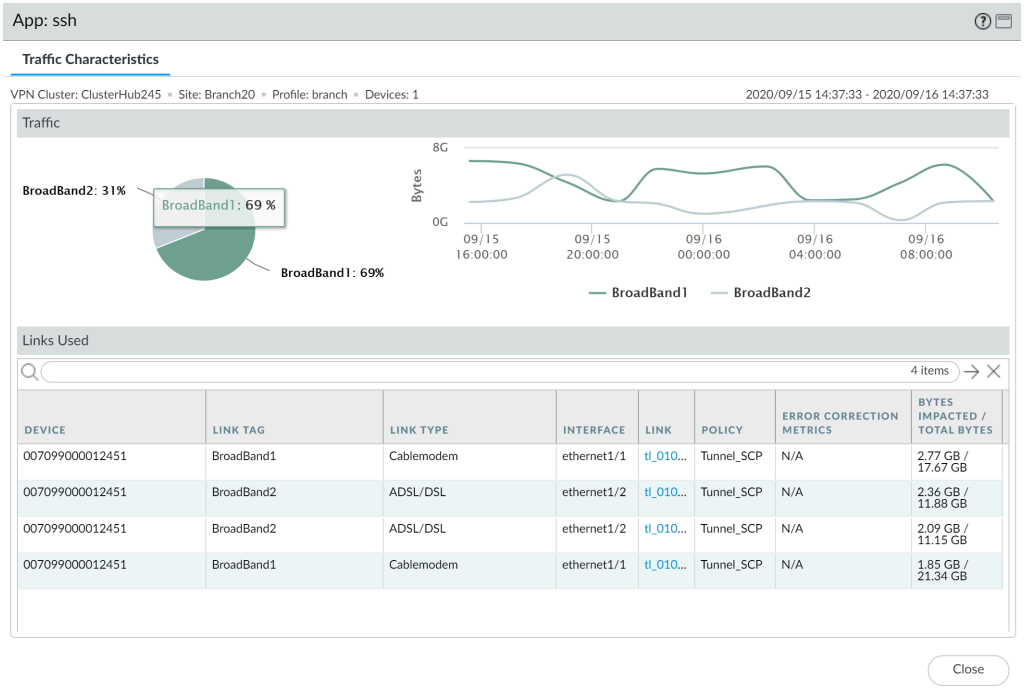


STEP 4 | 在站点列中，选择受影响的中心或分支防火墙，以查看受影响的应用程序和相应的链路性能。



STEP 5 | 在应用程序性能部分，单击应用程序以查看应用程序流量相关的详细的流量特征信息，例如，Internet 服务和使用的链路：

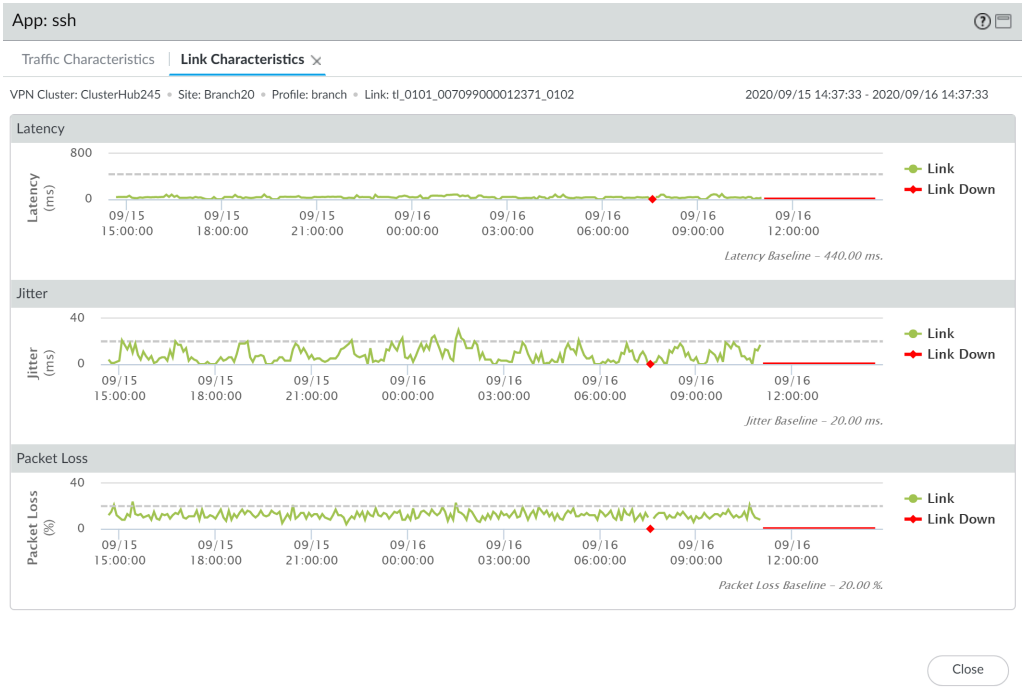
- 查看饼图以了解整个 Internet 服务中细分的应用程序流量。
- 查看线形图以了解随着时间的推移，每个 Internet 服务中传输的数据字节数。
- 查看使用的链路部分以了解应用程序流量使用的链路，并了解在所选时间框架内，总字节中有多少字节受到影响。



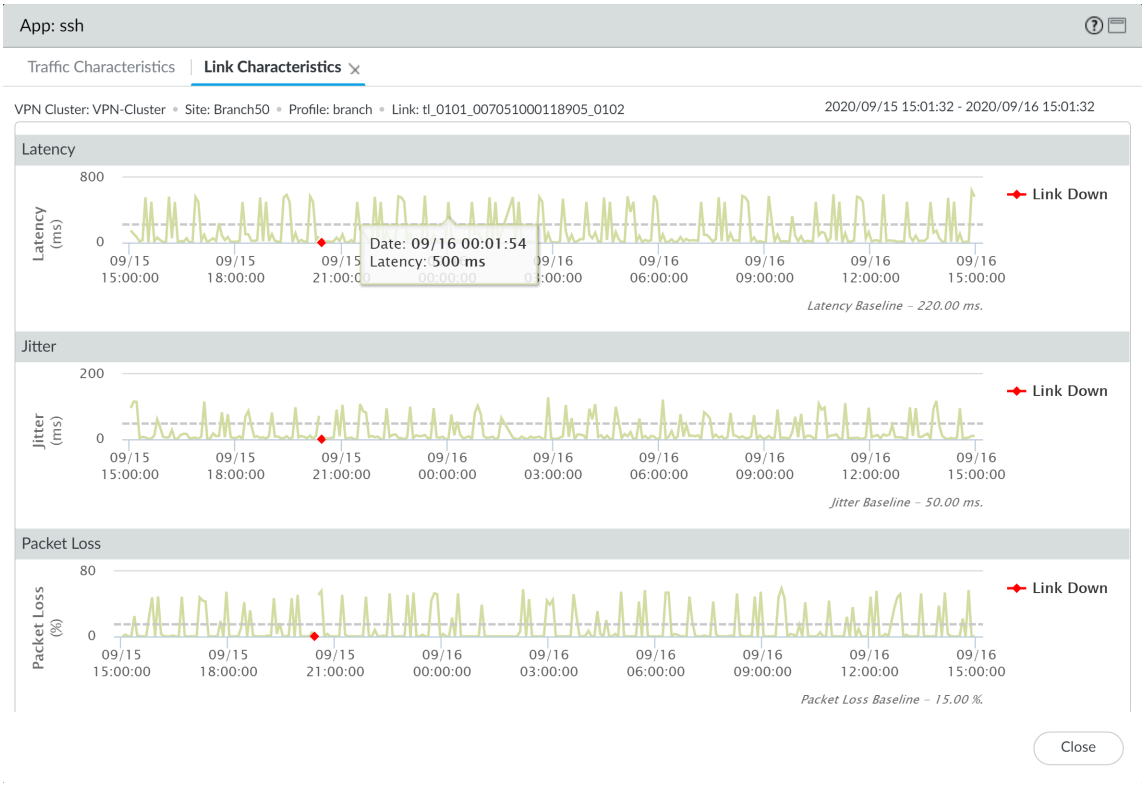
STEP 6 | 调查导致应用程序交换链路的运行状况指标。

虚线表示运行状况指标七天平均值。

1. 在流量特征选项卡的使用的链路部分，单击以太网链路以详细查看在步骤2中指定的时间框架内的链路特征（延迟、抖动和数据包丢失），以调查导致应用程序交换链路的运行状况指标。



2. 在 **Traffic Characteristics**（链路特征）选项卡中，选择其他链路，查看辅助应用程序链路的链路特征，以更好了解导致 VPN 集群受影响的原因。



STEP 7 | 在确定导致应用程序流量受影响的原因后，请考虑以下解决问题的方法：

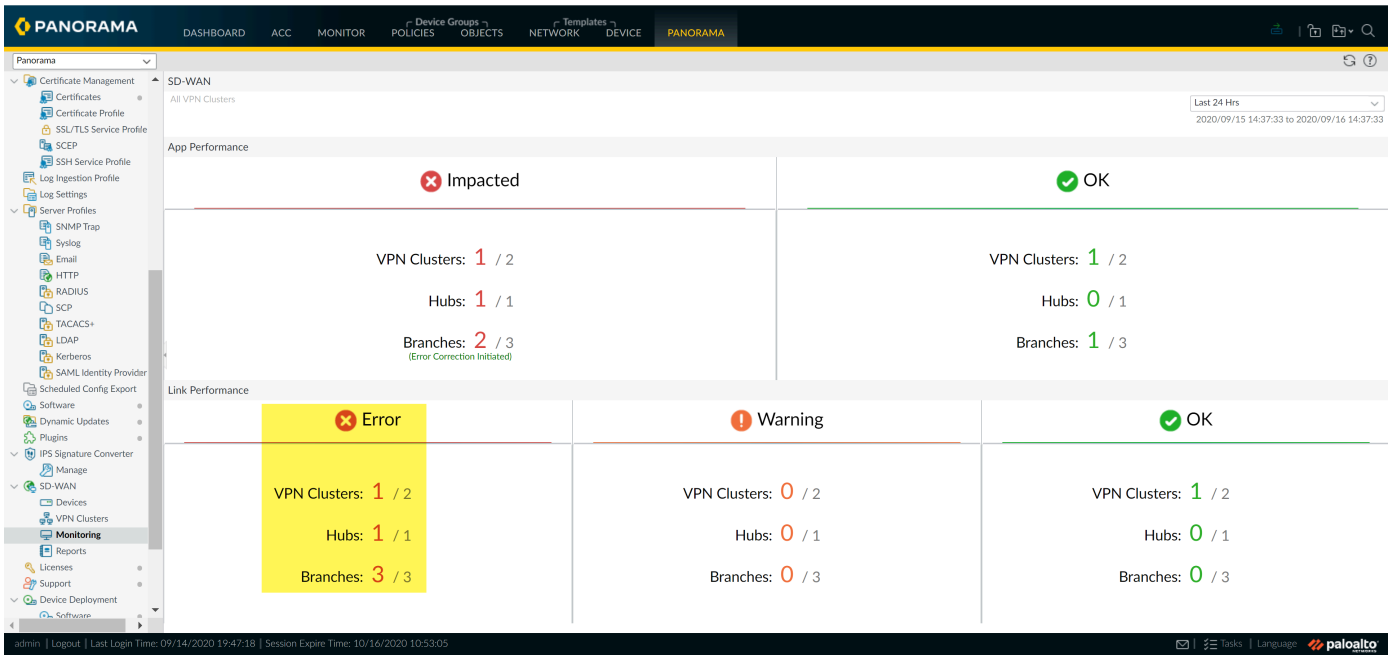
- 考虑将其他链路添加到 流量分发配置文件。通过为应用程序流量添加可以执行故障转移的其他链路，有助于确保应用程序流量和用户体验不会受到运行状况下降的链路的影响。
- 在 路径质量配置文件中重新配置运行状况阈值。有可能是运行状况阈值太严格，导致不必要的链路故障转移。例如，如果您的应用程序只有在超过 18% 数据包丢失时才会影响用户体验，采用 10% 的数据包丢失阈值可能会导致应用程序故障转移到无需使用的其他链路。
- 请咨询您的 Internet 服务提供商 (ISP)，确定对您网络的影响是否超出您的控制，但却在他们的解决范围内。

排除链路性能故障

了解导致链路性能下降的原因是确保用户体验在使用应用程序和服务时不会受影响的必要一环。了解 VPN 集群中链路受影响的原因有助于对 SD-WAN 配置执行微调，确保用户体验在使用应用程序和服务是不会受到运行状况下降的链路的影响。

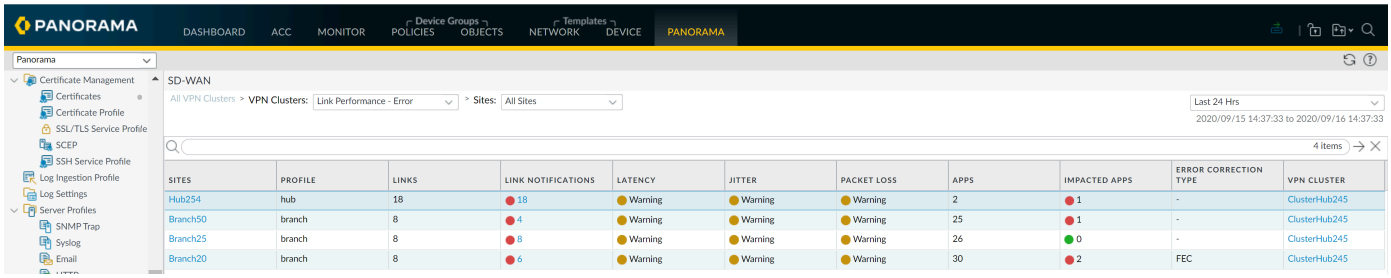
STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 选择 **Panorama** > **SD-WAN** > **Monitoring**（监控），然后查看 **Impacted**（受影响的）VPN 集群。

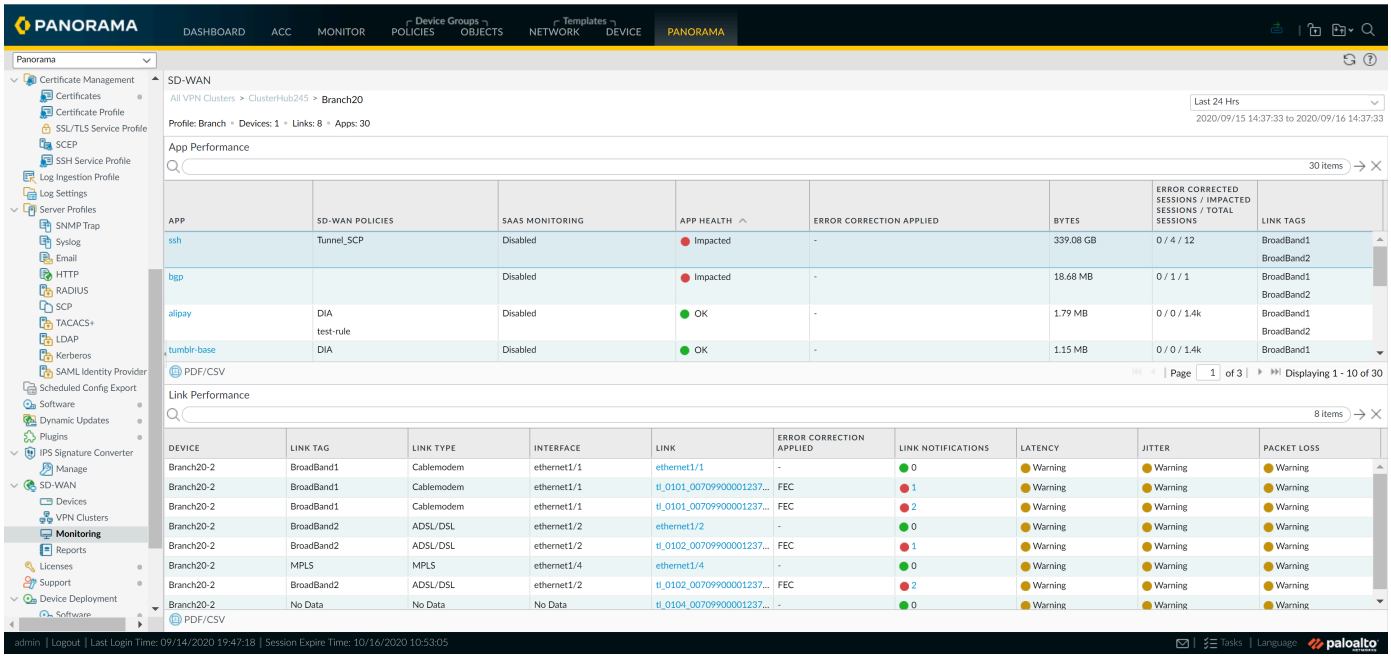


STEP 3 | 基于从 **Site**（站点）下拉列表中获得的首选指标筛选 VPN 集群，然后选择时间框架。在站点列中，选择受影响的中心或分支防火墙，以查看受影响的应用程序和相应的链路性能。

在此示例中，我们将查看最近 24 小时内包含受影响 VPN 集群的 **All Sites**（所有站点）。

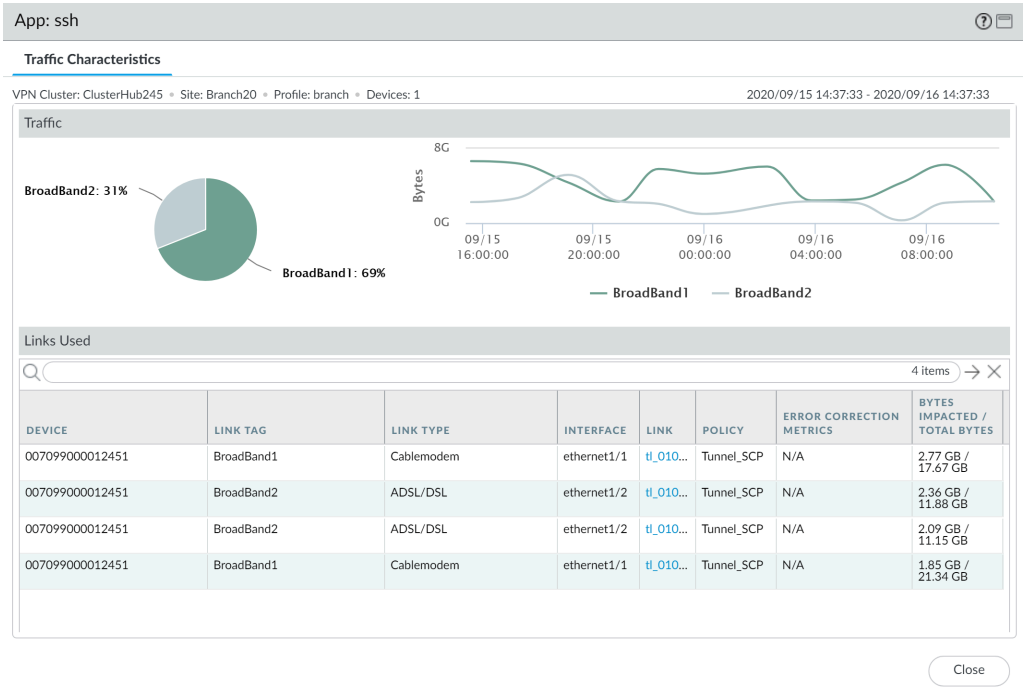


STEP 4 | 在站点列中，选择受影响的中心或分支防火墙，以查看受影响的应用程序和相应的链路性能。



STEP 5 | 在应用程序性能部分，单击应用程序以查看应用程序流量相关的详细的流量特征信息，例如，Internet 服务和使用的链路：

- 查看饼图以了解整个 Internet 服务中细分的应用程序流量。
- 查看线形图以了解随着时间的推移，每个 Internet 服务中传输的数据字节数。
- 查看使用的链路部分以了解应用程序流量使用的链路，并了解在所选时间框架内，总字节中有多少字节受到影响。

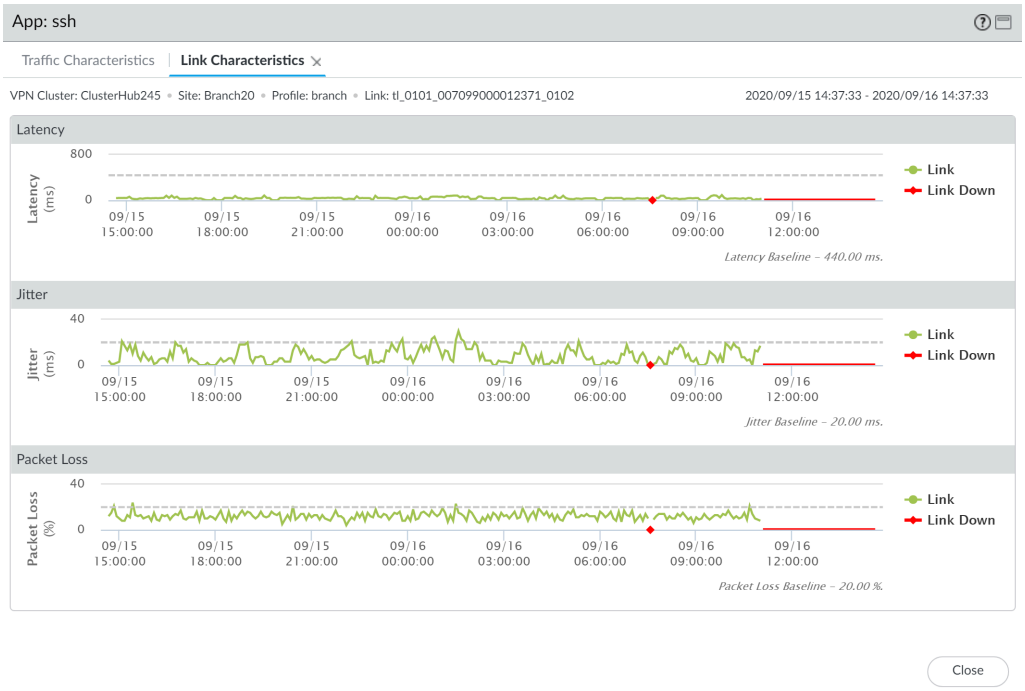


STEP 6 | 调查导致应用程序交换链路的运行状况指标。

虚线指示在您创建路径质量配置文件时配置的阈值。

1. 在流量特征选项卡的使用的链路部分，单击以太网链路以详细查看在步骤2中指定的时间框架内的链路特征（延迟、抖动和数据包丢失），以调查导致应用程序交换链路的运行状况指标。在此示例中，我们查看的是以太网 1/1。我们发现，数据包丢失百分比经常超过

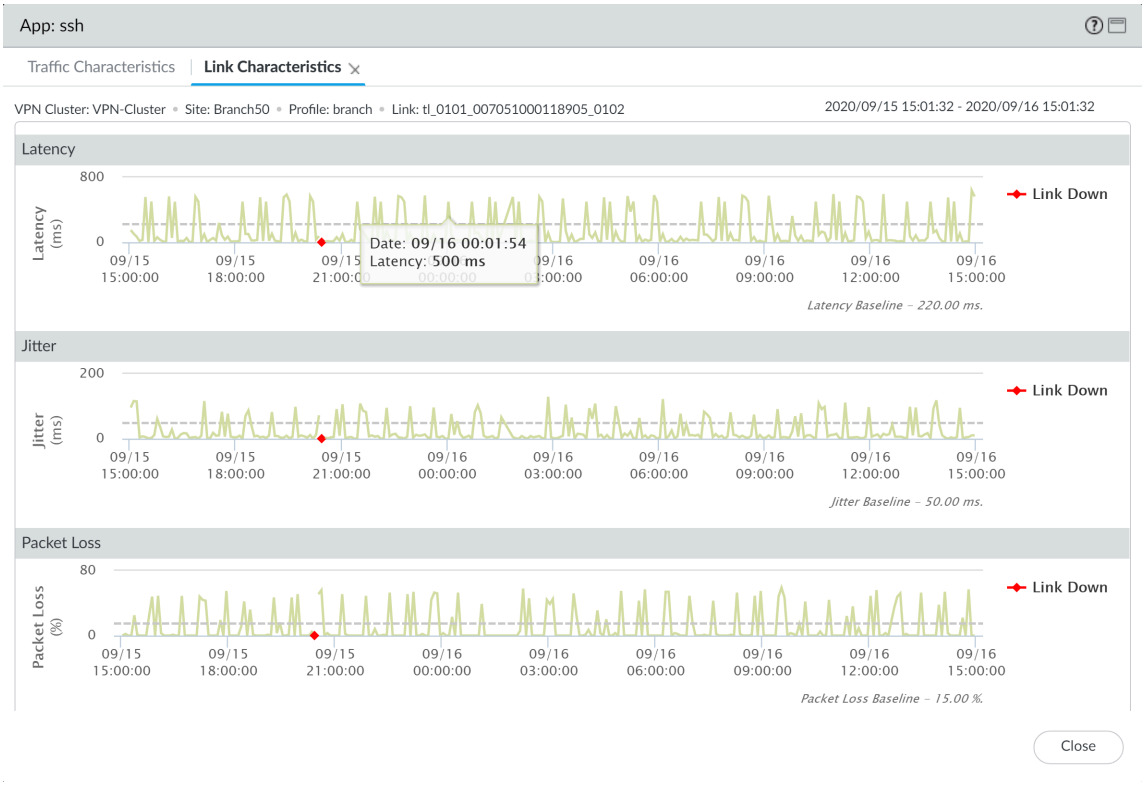
此应用程序在路径质量配置文件中配置的阈值。因此，可以得出结论，这就是导致应用程序流量故障转移到下一个最佳链路的原因。



2. 在 **Traffic Characteristics**（链路特征）选项卡中，选择另一个链路以查看链路特征。在此示例中，我们查看的是以太网 1/4。我们发现，在应用程序流量执行故障转移后，以太网

1/4 在此应用程序上的抖动值超出了配置阈值。这就迫使应用程序流量故障转移回到以太网 1/1。

两个链路使用的运行状况指标都超过阈值，因此，应用程序流量没有可以执行故障转移的运行状况良好的链路，从而导致 VPN 集群受到影响。



STEP 7 | 在确定导致应用程序流量受影响的原因后，请考虑以下解决问题的方法：

- 考虑将其他链路添加到 流量分发配置文件。通过为应用程序流量添加可以执行故障转移的其他链路，有助于确保应用程序流量和用户体验不会受到运行状况下降的链路的影响。
- 在 路径质量配置文件中重新配置运行状况阈值。有可能是运行状况阈值太严格，导致不必要的链路故障转移。例如，如果您的应用程序只有在超过 18% 数据包丢失时才会影响用户体验，采用 10% 的数据包丢失阈值可能会导致应用程序故障转移到无需使用的其他链路。
- 请咨询您的 Internet 服务提供商 (ISP)，确定对您网络的影响是否超出您的控制，但却在他们的解决范围内。

升级您的 SD-WAN 防火墙

查看适用于 SD-WAN 2.1 的 Panorama 插件发行说明，然后按照以下步骤升级您的 Panorama 和受管 SD-WAN 防火墙。

STEP 1 | 安装 Panorama 的内容和软件更新。

STEP 2 | 升级您的受管日志收集器。

- 当 Panorama 连接上互联网时升级日志收集器。
- 当 Panorama 未连接互联网时升级日志收集器。

STEP 3 | 升级您的 SD-WAN 中心防火墙。

在升级分支防火墙之前，您必须将中心防火墙从 *PAN-OS 10.0.0* 升级到 *PAN-OS 10.0.1* 或更高发行版本。在中心防火墙之前升级分支防火墙可能导致错误的监视数据（***Panorama*** > ***SD-WAN*** > ***Monitoring***（监视）），且 *SD-WAN* 链接会错误地显示为 *down*（禁用）。

- 当 Panorama 连接上互联网时升级防火墙。
- 当 Panorama 未连接互联网时升级防火墙。

STEP 4 | 升级您的 SD-WAN 分支防火墙。

- 当 Panorama 连接上互联网时升级防火墙。
- 当 Panorama 未连接互联网时升级防火墙。

升级 SD-WAN 插件

升级安装在您的 Panorama™ 管理服务器和防火墙（使用 SD-WAN）上的 SD-WAN 插件版本。

请参阅 Palo Alto Networks Panorama 插件兼容性矩阵，并查看目标 SD-WAN 插件版本所需的最低 PAN-OS 版本。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 升级 Panorama 上的 SD-WAN 插件版本。

如果 Panorama 为高可用性 (HA) 配置，则在 Panorama HA 对等设备上重复这个步骤。

1. 选择 **Panorama** > **Plugin**（插件）并 **Check Now**（立即检查）最新的 **sd_wan** 插件版本。
2. **Download**（下载）并 **Install**（安装）最新的 SD-WAN 插件版本。

STEP 3 | 成功安装新插件版本后，查看 Panorama **Dashboard**（仪表板）并在常规信息小部件中验证 `SD-WAN plugin` 版本是否显示您升级到的 SD-WAN 插件版本。

卸载 SD-WAN 插件

要从 Panorama 管理服务器卸载 SD-WAN 插件，必须先将 SD-WAN 插件配置从 Panorama 删除，然后才能成功卸载 SD-WAN 插件。

STEP 1 | 登录到 Panorama Web 界面。

STEP 2 | 删除允许 BGP 在 SD-WAN 中心和分支之间运行的任何安全策略规则。

1. 选择**Panorama** > **SD-WAN** > **Devices**（设备） > **BGP Policy**（**BGP** 策略），然后 **Remove**（删除） 安全策略规则。
2. 单击 **OK**（确定）保存您的配置更改。

STEP 3 | 选择 **Panorama** > **Plugins**（插件），然后选择 **Remove Config**（删除配置）用于 SD-WAN 插件。

STEP 4 | 选择 **Commit**（提交），然后 **Commit and Push**（提交并推送）配置更改到受管防火墙。

STEP 5 | **Uninstall**（卸载）SD-WAN 插件。

在提示您继续卸载 SD-WAN 插件时，请单击 **OK**（确定）。