

SD-WAN Administrator's Guide

1.0

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 www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 18, 2019

Table of Contents

SD-WAN Overview.....	5
About SD-WAN.....	7
SD-WAN Configuration Elements.....	10
Plan Your SD-WAN Configuration.....	12
 Set Up SD-WAN.....	 15
Install the SD-WAN Plugin.....	17
Install the SD-WAN Plugin When Panorama is Internet-Connected.....	17
Install the SD-WAN Plugin When Panorama is not Internet-Connected.....	17
Set Up Panorama and Firewalls for SD-WAN.....	19
Add Your SD-WAN Firewalls as Managed Devices.....	19
Create an SD-WAN Network Template.....	20
Create the Predefined Zones in Panorama.....	21
Create the SD-WAN Device Groups.....	23
 Configure SD-WAN.....	 25
Create a Link Tag.....	27
Configure an SD-WAN Interface Profile.....	28
Configure a Physical Ethernet Interface for SD-WAN.....	30
Configure a Virtual SD-WAN Interface.....	32
Create a Default Route to the SD-WAN Interface.....	35
Create a Path Quality Profile.....	36
SD-WAN Traffic Distribution Profiles.....	38
Create a Traffic Distribution Profile.....	43
Configure an SD-WAN Policy Rule.....	45
Distribute Unmatched Sessions.....	49
Add SD-WAN Devices to Panorama.....	51
Add an SD-WAN Device.....	51
Bulk Import Multiple SD-WAN Devices.....	52
Configure HA Devices for SD-WAN.....	55
Create a VPN Cluster.....	56
Create a Static Route for SD-WAN.....	58
 Monitoring and Reporting.....	 59
Monitor SD-WAN Application and Link Performance.....	61
Troubleshoot App Performance.....	63
Troubleshoot Link Performance.....	68
Generate an SD-WAN Report.....	72
 Use the CLI.....	 75
Use CLI Commands for SD-WAN Tasks.....	77

SD-WAN Overview

Learn about SD-WAN and plan your configuration to ensure a successful deployment.

- > About SD-WAN
- > SD-WAN Configuration Elements
- > Plan Your SD-WAN Configuration

About SD-WAN

Software-Defined Wide Area Network (SD-WAN) is a technology that allows you to use multiple internet and private services to create an intelligent and dynamic WAN, which helps lower costs and maximize application quality and usability. Beginning with PAN-OS[®] 9.1, Palo Alto Networks[®] offers strong security with an SD-WAN overlay in a single management system. Instead of using costly and time-consuming MPLS with components such as routers, firewalls, WAN path controllers, and WAN optimizers to connect your WAN to the internet, SD-WAN on a Palo Alto Networks firewall allows you to use less expensive internet services and fewer pieces of equipment. You don't need to purchase and maintain other WAN components.

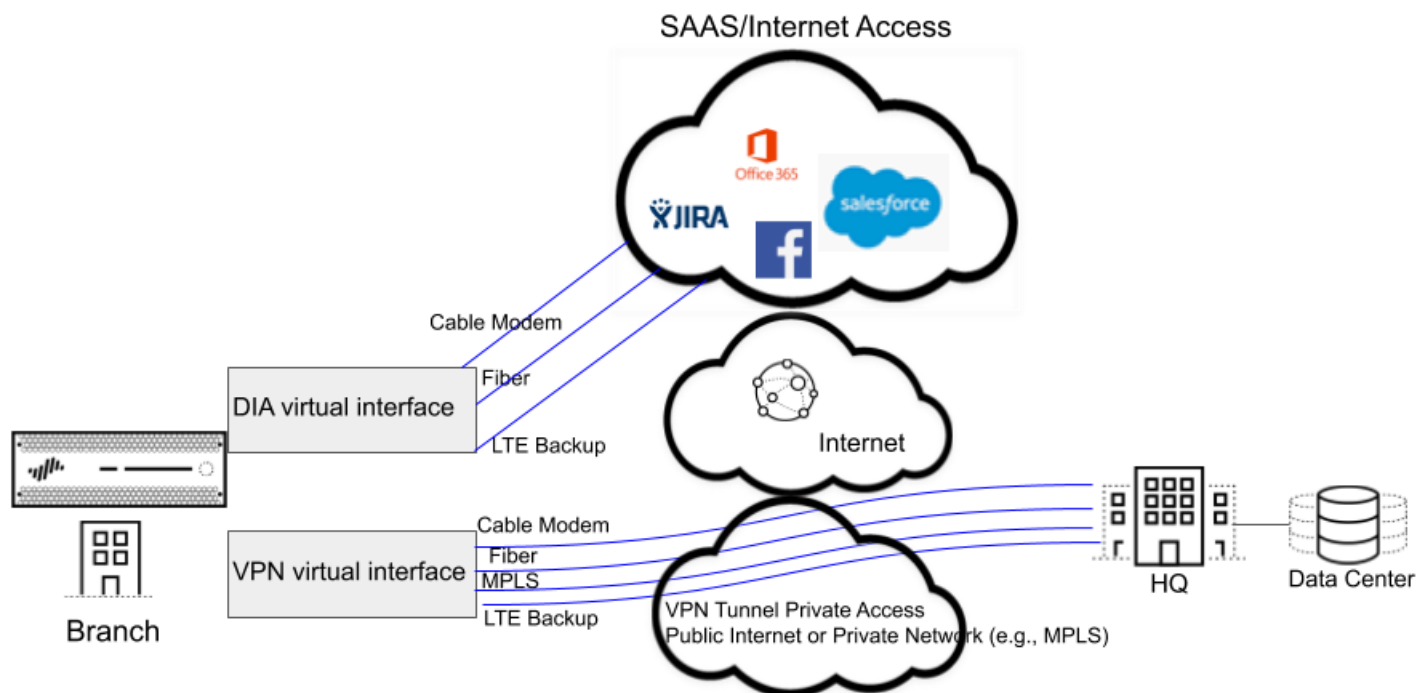
- [PAN-OS Security with SD-WAN Functionality](#)
- [SD-WAN Link and Firewall Support](#)
- [Centralized Management](#)

PAN-OS Security with SD-WAN Functionality

The SD-WAN plugin is integrated with PAN-OS, so that you get the security features of a PAN-OS firewall and SD-WAN functionality from a single vendor. The SD-WAN overlay supports dynamic, intelligent path selection based on applications and services and the conditions of links that each application or service is allowed to use. The path health monitoring for each link includes latency, jitter, and packet loss. Granular application and service controls allow you to prioritize applications based on whether the application is mission-critical, latency-sensitive, or meets certain health criteria, for example. Dynamic path selection avoids brownout and node failure problems because sessions fail over to a better performing path in less than one second.

The SD-WAN overlay works with all PAN-OS security features, such as User-ID[™] and App-ID[™], to provide complete security control to branch offices. The full suite of App-ID capabilities (App-ID decoder, App-ID cache, and source/destination external dynamic list [EDL] IP address lists) identifies applications for application-based control of SD-WAN traffic. You can deploy the firewall with Zero Trust segmentation of traffic. You can configure and manage SD-WAN centrally from the Panorama web interface or the Panorama REST API.

You may have cloud-based services and instead of having your internet traffic flow from branches to the hub to the cloud, you want the internet traffic to flow directly from branches to the cloud using a directly connected ISP. Such access from a branch to the internet is Direct Internet Access (DIA). You don't need to spend your hub bandwidth and money on internet traffic. The branch firewall is already doing security, so you don't need the hub firewall to enforce security on internet traffic. Use DIA on branches for SaaS, web browsing, or heavy-bandwidth applications that shouldn't be backhauled to a hub. The following figure illustrates a DIA virtual interface consisting of three links from the branch to the cloud. The figure also illustrates a VPN tunnel virtual interface consisting of four links that connect the branch to the hub at the headquarters.



SD-WAN Link and Firewall Support

Link bundling allows you to group multiple physical links (that different ISPs use to communicate with the same destination) into a virtual SD-WAN interface. On the basis of applications and services, the firewall chooses from the links (path selection) for session load sharing and to provide failover protection in the event of a brownout or blackout. Thus you are providing the application with the best quality performance. The firewall automatically performs session load sharing over the links in a virtual SD-WAN interface to use available bandwidth advantageously. An SD-WAN interface must have all of the same type of connection (either DIA or VPN). VPN links support the hub-and-spoke topology.

SD-WAN supports the following types of WAN connections: ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, and anything that terminates as Ethernet to the firewall's interface. You decide the appropriate strategy for how to use the links. You could use inexpensive broadband connections before expensive MPLS or LTE connections. Alternatively, you could use specific VPN tunnels to reach specific hubs in a region.

PA-220, PA-220R, PA-820, and PA-850 firewalls are supported as SD-WAN branch firewalls. PA-3200 Series, PA-5200 Series, VM-300, VM-500, and VM-700 firewalls are supported as SD-WAN hub firewalls. Each firewall (branch or hub) requires an SD-WAN subscription. Each Panorama requires the SD-WAN plugin.

If you are a new customer purchasing a Palo Alto Networks next-generation firewall, you will use the default virtual router for SD-WAN. If you are an existing customer, you can choose to either let PAN-OS overwrite any existing virtual routers or use a new virtual router and new zones for SD-WAN to keep SD-WAN content separate from your pre-existing configuration.

Centralized Management

Panorama™ provides the means to configure and manage SD-WAN, which makes configuring multiple options on many geographically-dispersed firewalls much faster and easier than configuring firewalls individually. You can change network configurations from a single location rather than configuring each firewall individually. Auto VPN configuration allows Panorama to configure branches and hubs with secure IKE/IPSec connections. A VPN cluster defines the hubs and branches that communicate with each other in a geographic region. The firewall uses VPN tunnels for path health monitoring between a branch and a hub to provide subsecond detection of brownout conditions.

The Panorama dashboard provides visibility into your SD-WAN links and performance so that you can adjust path quality thresholds and other aspects of SD-WAN to improve its performance. Centralized statistics and reporting include application and link performance statistics, path health measurements and trend analysis, and focused views of application and link issues.

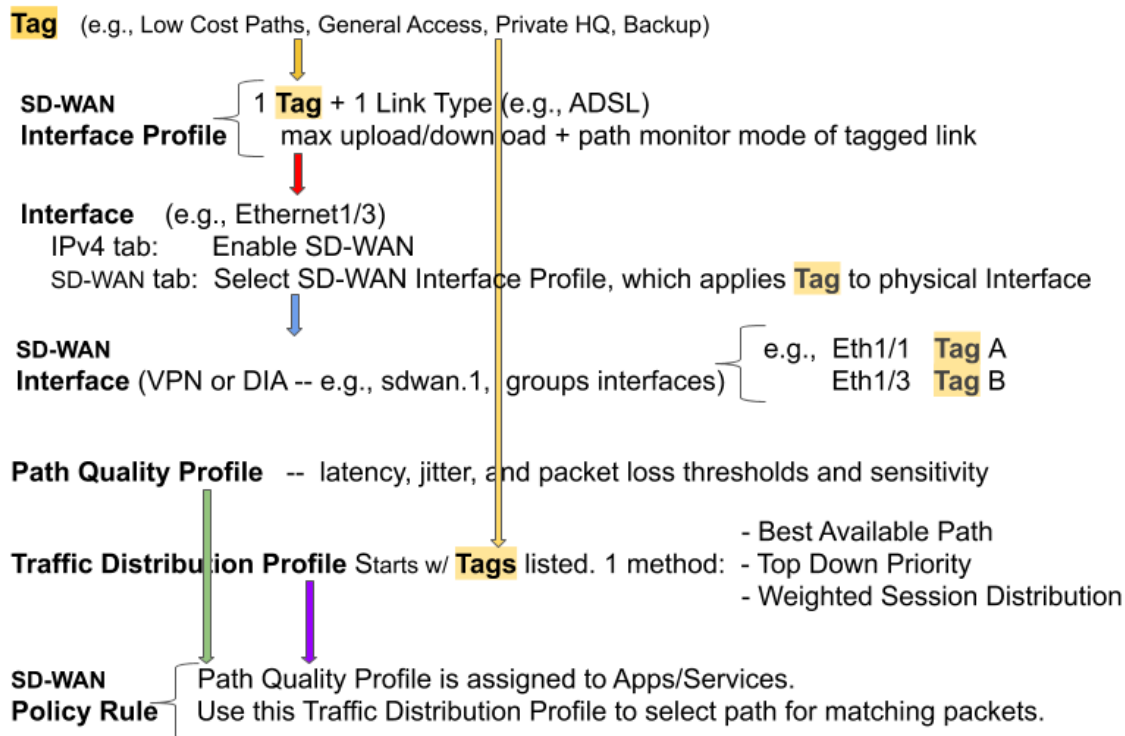
Begin by understanding your SD-WAN use case, then review the SD-WAN configuration elements, traffic distribution methods, and plan your SD-WAN configuration. To greatly accelerate the configuration, the best practice is for you to export an empty SD-WAN device CSV and enter information such as branch office IP address, the virtual router to use, the firewall site name, zones to which the firewall belongs, and BGP route information. Panorama uses the CSV file to configure the SD-WAN hubs and branches and to automatically provision VPN tunnels between hubs and branches. SD-WAN supports dynamic routing through eBGP and is configured using Panorama's SD-WAN plugin to allow all branches to communicate with the hub only or with the hub and other branches.

SD-WAN Configuration Elements

The elements of an SD-WAN configuration work together, allowing you to:

- Group physical Ethernet interfaces that share a common destination into a logical SD-WAN interface.
- Specify link speeds.
- Specify the thresholds at which a deteriorating path (or brownout or blackout) to an SD-WAN warrants selecting a new best path.
- Specify the method of selecting that new best path.

This view indicates the relationships between elements at a glance.



The goal of an SD-WAN configuration is to control which links your traffic takes by specifying the VPN tunnels or direct internet access (DIA) that certain applications or services take from a branch to a hub or from a branch to the internet. You group paths so that if one path deteriorates, the firewall selects a new best path.

- A **Tag** name of your choice identifies a link; you apply the Tag to the link (interface) by applying an Interface Profile to the interface, as the red arrow indicates. A link can have only one Tag. The two yellow arrows indicate that a Tag is referenced in the Interface Profile and the Traffic Distribution profile. Tags allow you to control the order that interfaces are used for traffic distribution. Tags allow Panorama to systematically configure many firewall interfaces with SD-WAN functionality.
- An **SD-WAN Interface Profile** specifies the Tag that you apply to the physical interface, and also specifies the type of Link that interface is (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, or other). The Interface Profile is also where you specify the maximum upload and download speeds (in Mbps) of the ISP's connection. You can also change whether the firewall monitors the path frequently or not; the firewall monitors link types appropriately by default.
- A Layer3 Ethernet **Interface** with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this interface (red arrow) to indicate the characteristics of the interface.

The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.

- A virtual **SD-WAN Interface** is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)
- A **Path Quality Profile** specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.
- A **Traffic Distribution Profile** specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.
- The preceding elements come together in **SD-WAN Policy Rules**. The purple arrow indicates that you reference a Path Quality Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.

Now that you understand the relationship between the elements, review the [traffic distribution methods](#) and then [Plan Your SD-WAN Configuration](#).

Plan Your SD-WAN Configuration

Plan the complete topology of your SD-WAN-enabled branch and hub firewall interfaces so that you can create Panorama™ templates with CSV files and then push the configurations to the firewalls.

STEP 1 | Plan the branch and hub locations, link requirements, and IP addresses. From Panorama you will export an empty SD-WAN device CSV and populate it with branch and hub information.

1. Decide the role of each firewall (branch or hub).
2. Determine which branches will communicate with which hubs; each functional group of branch and hub firewalls that communicate with each other is a VPN cluster. For example, your VPN clusters might be organized geographically or by function.
3. Determine the ISP link types that each branch and hub support: ADSL/DSL, cable mode, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, and WiFi.
4. Determine the maximum download and upload bandwidth (Mbps) that the link types support and how you want to apply these speed controls to links, as described in Step 2. Record the ISP link's maximum download and upload bandwidth (Mbps). This information will serve as reference egress maximums if you need to configure QoS to control the application bandwidth.
5. Gather the public IP addresses of branch firewalls, whether they are static or dynamically assigned. The firewall must have an internet-routable, public IP address so it can initiate and terminate IPsec tunnels and route application traffic to and from the internet.



The ISP's customer premise equipment must be directly connected to the Ethernet interface on the firewall.



If you have a device that performs NAT located between the branch firewall and the hub, the NAT device can prevent the firewall from bringing up IKE peering and IPsec tunnels. If the tunnel fails, work with the administrator of the remote NAT device to resolve the issue.

6. Gather the private network prefixes and serial numbers of branch and hub firewalls.
7. Decide the link type of each firewall interface.



Allocate the same link types on the same Ethernet interfaces across the branch firewalls to make configuration easier. For example, Ethernet1/1 is always cable modem.

8. Decide on the naming conventions for your sites and SD-WAN devices.
9. If you already have zones in place before configuring SD-WAN, decide how to map those zones to the predefined zones that SD-WAN uses for path selection. You will map existing zones to the predefined zones named zone-internal, To_Hub, To_Branch, and zone-internet.



Information you will enter into a CSV (so that you can add multiple SD-WAN devices at once) includes: serial number, type of device (branch or hub), names of zones to map to predefined zones (pre-existing customers), loopback address, prefixes to redistribute, AS number, router ID, and virtual router name.

STEP 2 | Plan link bundles and VPN security for private links.

A link bundle lets you combine multiple physical links into one virtual SD-WAN interface for purposes of path selection and failover protection. By having a bundle of more than one physical link, you maximize application quality in case a physical link deteriorates. You create a bundle by applying the same link tag to multiple links (via an SD-WAN Interface Profile). The link tag identifies a bundle of links that have a similar type of access and similar type of SD-WAN policy handling. For example, you can create a link tag named **low cost broadband** and include the cable modem and fiber broadband services.

STEP 3 | Identify the applications that will use SD-WAN and QoS optimization.

1. Identify the critical and the latency-sensitive business applications for which you will provide SD-WAN control and policies. These are applications that require a good user experience, and are likely to fail under poor link conditions.



Start with the most critical and latency-sensitive applications; you can add applications after SD-WAN is functioning smoothly.

2. Identify the applications that require QoS policies so you can prioritize bandwidth. These should be the same applications you identified as critical or latency-sensitive.



Start with the most critical and latency-sensitive applications; you can add applications after SD-WAN is functioning smoothly.

STEP 4 | Determine when and how you want links to fail over to a different link in the event the original link degrades or fails.

1. Decide on the path monitoring mode for a link, although the best practice is to retain the default setting for the link type:
 - **Aggressive**—The firewall sends probe packets to the opposite end of the SD-WAN link at a constant frequency (five probes per second by default). Aggressive mode is appropriate for links where monitoring path quality is critical; where you need fast detection and failover for brownout and blackout conditions. Aggressive mode provides subsecond detection and failover.
 - **Relaxed**—The firewall observes a configurable idle time between sending probe packets for seven seconds (at the probe frequency you configure), which makes path monitoring less frequent than aggressive mode. Relaxed mode is appropriate for links that have very low bandwidth, links that are expensive to operate, such as satellite or LTE, or when fast detection isn't as important as preserving cost and bandwidth.
2. Prioritize the order in which the firewall selects the first link for a new session and the order in which links should be a candidate to replace a link that is failing over, if there is more than one candidate.

For example, if you want an expensive backup LTE link to be the last link used (only when the inexpensive broadband links are oversubscribed or completely down), then use the Top Down Priority traffic distribution method and place the tag that is on the LTE link last in the list of tags for the Traffic Distribution profile.

3. For the applications and services, determine the path health thresholds at which you consider a path to have degraded enough in quality that you want the firewall to select a new path (fail over). The quality characteristics are latency (range is 10 to 2,000 ms), jitter (range is 10 to 1,000 ms), and packet loss percentage.

These thresholds constitute a Path Quality profile, which you reference in an SD-WAN policy rule. When any single threshold (for packet loss, jitter, or latency) is exceeded (and the remaining rule criteria are met), the firewall chooses a new preferred path for the matching traffic. For example, you can create Path Quality profile AAA with latency/jitter/packet loss thresholds of 1000/800/10 to use in Rule 1 when FTP packets come from source zone XYZ, and create Path Quality profile BBB (with thresholds of 50/200/5) to use in Rule 2 when FTP packets come from source IP address 10.1.2.3. Best practice is to start with high thresholds and test how the application tolerates them. If you set the values too low, the application may switch paths too frequently.

Consider whether the applications and services you are using are especially sensitive to latency, jitter, or packet loss. For example, a video application might have good buffering that mitigates latency and jitter, but would be sensitive to packet loss, which impacts the user experience. You can set the sensitivity of the path quality parameters in the profile to high, medium or low. If the sensitivity settings for latency, jitter, and packet loss are the same, the firewall examines the parameters in the order of packet loss, latency, jitter.

4. Decide if there are links among which to load share new sessions for an application or service.

STEP 5 | Plan the BGP configurations that Panorama will push to branches and hubs to dynamically route traffic between them.

1. Plan BGP route information, including a four-byte autonomous system number (ASN). Each firewall site is in a separate AS and therefore must have a unique ASN. Each firewall must also have a unique Router ID.
2. If you don't want to use BGP dynamic routing, plan to use Panorama's network configuration features to push out other routing configurations. You can do static routing between the branch and hubs. Simply omit all of the BGP information in the Panorama plugin and use normal virtual router static routes to perform static routing.

STEP 6 | Consider the [capacities of firewall models](#) for virtual SD-WAN interfaces, SD-WAN policy rules, log size, IPSec tunnels (including proxy IDs), IKE peers, BGP and static route tables, BGP routing peers, and performance for your firewall mode (App-ID™, threat, IPSec, decryption). Ensure the branch and hub firewall models you intend to use support the capacities you require.

Set Up SD-WAN

Install the SD-WAN plugin on your Panorama™ management server. After you install the plugin, add your hub and branch firewalls as managed firewalls and create the device groups, templates, and template stacks needed to push configurations.

- > Install the SD-WAN Plugin
- > Set Up Panorama and Firewalls for SD-WAN

Install the SD-WAN Plugin

You can download and install the SD-WAN plugin on the Panorama management server from directly on Panorama when internet connected, or by downloading the plugin from the Palo Alto Networks® Customer Support Portal when Panorama is not internet connected.

- [Install the SD-WAN Plugin When Panorama is Internet-Connected](#)
- [Install the SD-WAN Plugin When Panorama is not Internet-Connected](#)

Install the SD-WAN Plugin When Panorama is Internet-Connected

Simplified management of multiple SD-WAN enabled firewalls is enabled by installing the SD-WAN plugin on your Panorama™ management server. When Panorama is connected to the internet, you can download and install the SD-WAN plugin directly from the Panorama web interface. The plugin needs to be installed only on the Panorama managing your SD-WAN firewalls, and not on the individual hub and branch firewalls.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Select **Panorama > Plugins**, search for the **sd_wan** plugin and **Check Now** for the most recent version of the plugin.

STEP 3 | **Download** and **Install** the SD-WAN plugin.

STEP 4 | Continue to [Set Up Panorama and Firewalls for SD-WAN](#) to begin configuring your SD-WAN deployment.

Install the SD-WAN Plugin When Panorama is not Internet-Connected

Simplified management of multiple SD-WAN enabled firewalls is enabled by installing the SD-WAN plugin on your Panorama™ management server. To install the SD-WAN plugin on Panorama when not internet connected, you must download the plugin from the Palo Alto Networks Customer Support Portal and upload the plugin to Panorama. The plugin needs to be installed only on the Panorama managing your SD-WAN firewalls, and not on the individual hub and branch firewalls.

STEP 1 | Log in to the Palo Alto Networks [Customer Support Portal](#).

STEP 2 | Select **Updates > Software Updates**, and in the Filter By drop-down select **Panorama Integration Plug In**.

STEP 3 | Locate and download the **SD-WAN Plug-in**.

STEP 4 | [Log in to the Panorama Web Interface](#).

STEP 5 | Select **Panorama > Plugins** and **Upload** the SD-WAN plugin.

STEP 6 | **Browse** and locate the SD-WAN plugin you downloaded from the Customer Support Portal and click **OK**.

STEP 7 | **Install** the SD-WAN plugin.

STEP 8 | Continue to [Set Up Panorama and Firewalls for SD-WAN](#) to begin configuring your SD-WAN deployment.

Set Up Panorama and Firewalls for SD-WAN

Before you can begin configuring your SD-WAN deployment, you must add your hub and branch firewalls as managed devices, and create the necessary templates and device group configurations to successfully push your SD-WAN configuration to SD-WAN firewalls.

- [Add Your SD-WAN Firewalls as Managed Devices](#)
- [Create an SD-WAN Network Template](#)
- [Create the Predefined Zones in Panorama](#)
- [Create the SD-WAN Device Groups](#)

Add Your SD-WAN Firewalls as Managed Devices

Before you can begin configuring your SD-WAN deployment, you must first [Install the SD-WAN Plugin](#) and add your hub and branch firewalls as managed devices to the Panorama™ management server. As part of adding your SD-WAN firewall as a managed device on the Panorama™ management server, you must activate the SD-WAN license to enable SD-WAN functionality for the firewall.

As part of adding your SD-WAN firewalls as managed devices, you must configure your managed firewalls to forward logs to Panorama. Panorama collects information from multiple sources, such as configuration logs, traffic logs, and link characteristic measurements, to generate the visibility for SD-WAN application and link health information.

STEP 1 | [Launch the Firewall Web Interface.](#)

STEP 2 | [Activate your SD-WAN license](#) to enable SD-WAN functionality on the firewall.

Each firewall you intend to use in your SD-WAN deployment requires a unique auth code to activate the license. For example, if you have 100 firewalls, you must purchase 100 SD-WAN licenses and activate each SD-WAN license on each firewall using one of the 100 unique auth codes.



For VM-Series firewalls, you apply the SD-WAN auth code against the specific VM-Series firewall. If you [deactivate the VM-Series firewall](#), the SD-WAN auth code can be activated on a different VM-Series firewall of the same model.

STEP 3 | Add the Panorama IP address to the firewall.

1. Select **Device > Setup > Management** and edit the Panorama Settings.
2. Enter the Panorama IP address in the first field.



The Panorama FQDN is not supported for SD-WAN.

3. (Optional) If you have set up a high availability (HA) pair in Panorama, enter the IP address of the secondary Panorama in the second field.
4. Verify that you **Enable pushing device monitoring data to Panorama**.
5. Click **OK**.
6. **Commit** your changes.

STEP 4 | [Configure log forwarding to Panorama.](#)

Forwarding logs from your SD-WAN firewalls to Panorama is required to display [Monitoring and Reporting](#) data.

STEP 5 | Add one or more firewalls to Panorama.

For more details about adding firewalls to Panorama, see [Add a Firewall as a Managed Device](#).

1. [Log in to the Panorama Web Interface](#).
2. Select **Panorama > Managed Devices > Summary** and **Add** the firewall(s).
3. Enter the serial number(s) of the firewalls.
4. If you are adding firewalls when the required device groups and templates are already created, enable (check) **Associate Devices** to assign new firewalls to the appropriate device groups and template stack.
5. To add multiple firewalls using a CSV, click **Import** and **Download Sample CSV** to populate with the firewall information, and then **Browse** to import the firewalls.
6. Click **OK**.

STEP 6 | Select **Commit** and **Commit and Push** your configuration.

STEP 7 | Repeat Steps 2 through 5 on each firewall you intend to use in your SD-WAN deployment.

Create an SD-WAN Network Template

Create a template containing all the networking configuration objects for your SD-WAN hubs and branches. You must create a separate template and template stack for your hub firewalls and a separate template and template stack for your branch firewalls. It is a best practice to limit the number of templates and template stacks used to manage your SD-WAN device configuration. Limiting the number of templates and template stacks used across all hubs and branches greatly reduces the operational overhead of managing the configurations of multiple SD-WAN hubs and branches. Use [template or template stack variables](#) to help reduce the number of templates used.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Create the SD-WAN hub network template.

1. Select **Panorama > Templates** and **Add** a new template.
2. Enter a descriptive **Name** for the template.
3. (Optional) Enter a **Description** for the template.
4. Click **OK** to save your configuration changes.

STEP 3 | Create a hub template stack.

1. Select **Panorama > Templates** and click **Add Stack** to add a new template stack.
2. Enter a descriptive **Name** for the template stack.
3. (Optional) Enter a **Description** for the template.
4. **Add** the SD-WAN network template you created in the Step 2.
5. In the **Devices** section, select the check boxes for all your SD-WAN hub firewalls.
6. Click **OK** to save your configuration changes.

STEP 4 | Create the SD-WAN branch network template.

1. **Add** a new template.
2. Enter a descriptive **Name** for the template.
3. (Optional) Enter a **Description** for the template.
4. Click **OK** to save your configuration changes.

STEP 5 | Create a branch template stack.

1. Click **Add Stack** to add a new template stack.
2. Enter a descriptive **Name** for the template stack.

3. (Optional) Enter a **Description** for the template.
4. **Add** the SD-WAN network template you created in the Step 4.
5. In the **Devices** section, select the check boxes for all your SD-WAN branch firewalls.
6. Click **OK** to save your configuration changes.

STEP 6 | Commit your configuration changes.

Create the Predefined Zones in Panorama

SD-WAN policy rules use predefined zones for internal path selection and traffic forwarding purposes. There are two use cases; your use case depends on whether you are enabling SD-WAN on your current PAN-OS® firewalls that have existing security policy rules or whether you are starting a brand new PAN-OS deployment with no previous security policy rules. If your current firewalls have security policy rules in place, you map your existing zones to the predefined zones that SD-WAN policies use.

Creating the predefined zones in the Panorama™ templates will provide consistent visibility between the managed firewalls and Panorama.



If you don't create the predefined zones, the SD-WAN plugin will automatically create the predefined zones on your branch and hub firewall, but you won't see them in Panorama.

There are two main use cases for predefined zones:


- **Existing Zones**—You already have pre-existing zones that you created for use in User-ID™ or various policies (security policy rules, QoS policy rules, zone protection, and packet buffer protection). You must map the pre-existing zones to the predefined zones that SD-WAN uses so the firewall can properly forward traffic. You should continue to use your pre-existing zones in all of your policies because the new predefined zones are used only for SD-WAN forwarding. You will map the zones when you to [Add SD-WAN Devices to Panorama](#) by creating your CSV file. (If you aren't using a CSV file, you will map zones when you configure **Panorama > SD-WAN > Devices** and add existing zones to **Zone Internet**, **Zone to Hub**, **Zone to Branch**, and **Zone Internal**.)

The result of mapping is that a branch or hub firewall can do a forwarding lookup to determine the egress SD-WAN interface and thus the egress zone. If you don't map pre-existing zones to predefined zones, an allowed session won't use SD-WAN. The mapping is necessary because existing customers have different zone names in place, and the firewall must narrow all of those zone names down to the predefined zones. You don't necessarily have to map zones to all of the predefined zones, but you should map existing zones to at least the **To_Hub** and **To_Branch** zones.

- **No Existing Zones**—You have a brand new deployment of Palo Alto Networks firewalls and SD-WAN. In this case, you don't have zones to map; we recommend you use the predefined zones in your PAN-OS policies and User-ID to simplify deployment.

Before you begin configuring your SD-WAN deployment, for both use cases, you will create the required predefined zones in Panorama named **zone-internet**, **zone-internal**, **To_Hub**, and **To_Branch**, and create two additional zones that you can name as you wish, such as **zone-trust** and **zone-untrust**. When you onboard your branch and hub firewalls, you will [Add SD-WAN Devices to Panorama](#). For pre-existing customers, the SD-WAN plugin will internally map pre-existing zones with these predefined zones when executing SD-WAN policy rules, QoS policy rules, zone protection, User-ID, and packet buffer protection, and will use the predefined zones for zone logging and visibility in Panorama. For new customers, you are properly set up using the predefined zones.

The predefined zones are also required in order to automatically set up VPN tunnels between your SD-WAN hubs and branches when you push the configuration from Panorama to your managed SD-WAN devices.

 *The zone names are case-sensitive and must match the names provided in this procedure. Your commit fails on the firewall if the zone names don't match those described in this procedure.*

In this example, we are creating the zone named **zone-trust**.

STEP 1 | Log in to the [Panorama Web Interface](#).

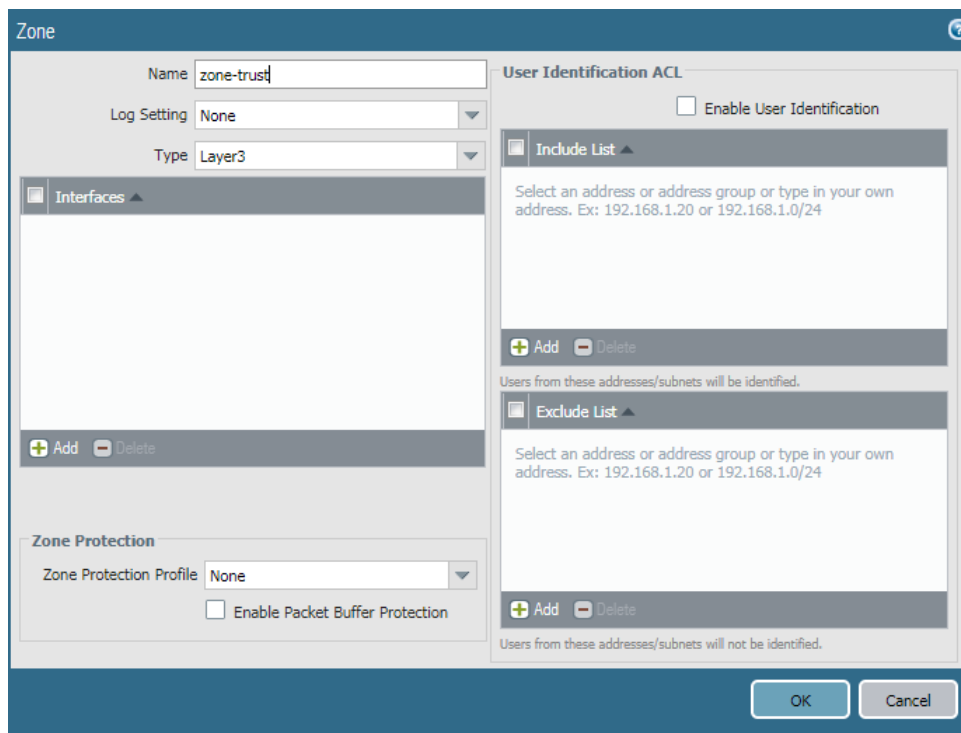
STEP 2 | Select **Network > Zones** and in the **Template** context drop-down, select the [network template](#) you previously created.

STEP 3 | **Add** a new zone.

STEP 4 | Enter **zone-trust**, for example, as the **Name** of the zone.

STEP 5 | For zone **Type**, select **Layer3**.

STEP 6 | Click **OK**.



STEP 7 | Repeat the previous steps to create the remaining zones. In total, you must create the following zones:

- **To_Branch**
- **To_Hub**
- **zone-internal**
- **zone-internet**
- **zone-trust** or a custom zone name

- **zone-untrust** or a custom zone name

STEP 8 | Commit and Commit and Push your configuration changes.

STEP 9 | Commit your changes.

Create the SD-WAN Device Groups

Create device groups, one for your hubs and one for your branches, containing all the policy rules and configuration objects for your SD-WAN hubs and branches. After you create the device groups for your hubs and branches, you must create a Security policy rule in each device group allowing traffic between the hub and branch zones. Creating these Security policy rules ensures that traffic between the SD-WAN device zones is allowed when the SD-WAN plugin creates the VPN tunnels after you [create a VPN cluster](#).



Configure identical configurations across your hub firewalls and an identical configuration across your branch firewalls. This greatly reduces the operational overhead of having to manage the configurations of multiple SD-WAN hubs and branches, and allows you to troubleshoot, isolate, update configuration issues much more rapidly.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Create the Predefined Zones in Panorama.

STEP 3 | Create the SD-WAN hub device group.

1. Select **Panorama > Device Groups** and **Add** a device group.
2. Enter **SD-WAN_Hub** as the **Name** for the device group.
3. (Optional) Enter a **Description** for the template.
4. In the **Devices** section, select the check boxes to assign the SD-WAN hubs to the group.
5. For the **Parent Device Group**, select **Shared**.
6. Click **OK**.

STEP 4 | Create the SD-WAN branch device group.

1. Select **Panorama > Device Groups** and **Add** a device group.
2. Enter **SD-WAN_Branch** as the **Name** for the device group.
3. (Optional) Enter a **Description** for the template.
4. In the **Devices** section, select the check boxes to assign the SD-WAN branches to the group.
5. For the **Parent Device Group**, select **Shared**.
6. Click **OK**.

STEP 5 | Create a Security policy rule to control traffic flows from branch offices to the hub's internal zone and from the hub's internal zone to branch offices.

1. Select **Policies > Security** and in the **Device Group** context drop-down, select the **SD-WAN_Hub** device group.
2. **Add** a new policy rule.
3. Enter a **Name** for the policy rule, such as **SD-WAN access--hub DG**.
4. Select **Source > Source Zone** and **Add** the **zone-internal** and **To_Branch**.
5. Select **Destination > Destination Zone** and **Add** the **zone-internal** and **To_Branch**.
6. Select **Application** and **Add** applications to allow.



You must allow BGP if you are using BGP routing.

7. Select **Actions** and **Allow** to allow the applications you selected.
8. Select **Target** and specify the target devices to which Panorama™ should push this rule.

STEP 6 | Create a Security policy rule to control traffic originating from the branch offices' internal zone to the hub and from the hub to the branch offices' internal zone.

1. Select **Policies > Security** and in the **Device Group** context drop-down, select the **SD-WAN_Branch** device group.
2. **Add** a new policy rule.
3. Enter a **Name** for the policy rule, such as **SD-WAN access--branch DG**.
4. Select **Source > Source Zone** and **Add** the **zone-internal** and **To_Hub**.
5. Select **Destination > Destination Zone** and **Add** the **zone-internal** and **To_Hub**.
6. Select **Application** and **Add** applications to allow.



You must allow BGP if you are using BGP routing.

7. Select **Actions** and **Allow** to allow the applications you selected.
8. Select **Target** and specify the target devices to which Panorama should push this rule.

STEP 7 | Commit and push your configuration.

1. **Commit** and **Commit and Push** your configuration changes.
2. In the Push Scope section, click **Edit Selections**.
3. Enable (check) **Include Device and Network Templates** and click **OK**.
4. **Commit and Push** your configuration changes.



There are two commit operations that are automatically performed when you commit and push the device group and template configuration. View the Tasks to verify that the second commit is successful. Of these two commit operations, the first always fails.

Configure SD-WAN

After you Plan Your SD-WAN Configuration and Set Up SD-WAN, use the Panorama™ management server to centrally manage your SD-WAN configuration for hub and branch interfaces. By leveraging Panorama, you reduce the management requirements and operational overhead for administrating your SD-WAN deployment, and can more easily monitor your link health and troubleshoot issues should they arise.

- > Create a Link Tag
- > Configure an SD-WAN Interface Profile
- > Configure a Physical Ethernet Interface for SD-WAN
- > Configure a Virtual SD-WAN Interface
- > Create a Default Route to the SD-WAN Interface
- > Create a Path Quality Profile
- > SD-WAN Traffic Distribution Profiles
- > Create a Traffic Distribution Profile
- > Configure an SD-WAN Policy Rule
- > Distribute Unmatched Sessions
- > Add SD-WAN Devices to Panorama
- > (Optional) Configure HA Devices for SD-WAN
- > Create a VPN Cluster
- > (Optional) Create a Static Route for SD-WAN

Create a Link Tag

Create a link tag to identify one or more physical links that you want applications and services to use in a specific order during SD-WAN traffic distribution and failover protection. Grouping multiple physical links allows you to maximize the application and service quality if the physical link health deteriorates.

When planning how to group your links, consider the use or purpose of the links and group them accordingly. For example, if you are configuring links intended for low-cost or non-business-critical traffic, create a link tag and group these interfaces together to ensure that the intended traffic flows primarily on these links, and not on more expensive links that may impact business-critical applications or services.

STEP 1 | [Log in to the Panorama Web Interface.](#)

STEP 2 | Select **Objects > Tags** and select the appropriate device group from the **Device Group** context drop-down.

STEP 3 | **Add** a new tag.

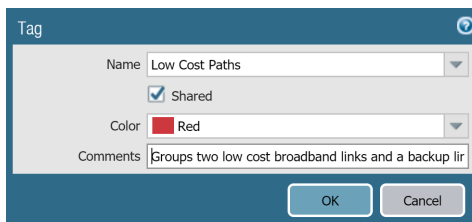
STEP 4 | Enter a descriptive **Name** for the tag. For example; Low Cost Paths, Expensive Paths, General Access, Private HQ, or Backup.

STEP 5 | (**Best Practice**) Enable (check) **Shared** to make the Link Tag available to all device groups on the Panorama™ management server and to every virtual system (vsys) on any multi-vsys hub or branch that you push to.

By configuring a Shared Link Tag, Panorama is able to reference the Link Tags in the firewall configuration validation and successfully commits and pushes the configuration to branches and hubs. The commit fails if Panorama is unable to reference a Link Tag.

STEP 6 | (**Optional**) Select a **Color** for the tag.

STEP 7 | Enter helpful **Comments** about the tag. For example, **Group two low cost broadband links and a backup link for general access to the internet.**



STEP 8 | Click **OK** to save your configuration changes.

STEP 9 | **Commit** and **Commit and Push** your configuration changes.

STEP 10 | [Configure an SD-WAN Interface Profile.](#)

Configure an SD-WAN Interface Profile

Create an SD-WAN interface profile to define the characteristics of ISP connections and to specify the speed of links and how frequently the firewall monitors the link, and specify a Link Tag for the link. When you specify the same Link Tag on multiple links, you are grouping (bundling) those physical links into a link bundle or fat pipe. You must configure an SD-WAN interface profile and specify it for an Ethernet interface enabled with SD-WAN before you can save the Ethernet interface.



Group links based on a common criterion. For example, group links by path preference from most preferred to least preferred, or group links by cost.

STEP 1 | Log in to the [Panorama Web Interface](#).

STEP 2 | Select **Network > Network Profiles > SD-WAN Interface Profile** and select the appropriate template from the **Template** context drop-down.

STEP 3 | **Add** an SD-WAN interface profile.

STEP 4 | Enter a user-friendly **Name** for the SD-WAN interface profile, which you'll see in reporting, troubleshooting, and statistics.

STEP 5 | Select the vsys **Location** if you have a multi-vsys Panorama™ management server. By default, vsys1 is selected.

STEP 6 | Select the **Link Tag** that this profile will assign to the interface.

STEP 7 | Add a **Description** for the profile.

STEP 8 | Select the physical **Link Type** from the predefined list (**ADSL/DSL**, **Cable modem**, **Ethernet**, **Fiber**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio**, **Satellite**, **WiFi**, or **Other**). The firewall can support any CPE device that terminates and hands off as an Ethernet connection to the firewall; for example, WiFi access points, LTE modems, laser/microwave CPEs all can terminate with an Ethernet handoff.

STEP 9 | Specify the **Maximum Download (Mbps)** speed from the ISP in megabits per second (range is 1 to 100,000; there is no default). Ask your ISP for the link speed or sample the link's maximum speeds with a tool such as speedtest.net and take an average of the maximums over a good length of time.

STEP 10 | Specify the **Maximum Upload (Mbps)** speed to the ISP in megabits per second (range is 1 to 100,000; there is no default). Ask your ISP for the link speed or sample the link's maximum speeds with a tool such as speedtest.net and take an average of the maximums over a good length of time.

STEP 11 | (**Optional**) Select the **Path Monitoring** mode in which the firewall monitors the interfaces where you apply this SD-WAN Interface Profile.



The firewall selects what it considers the best monitoring method based on Link Type. Retain the default setting for the link type unless an interface (where you apply this profile) has issues that require more aggressive or more relaxed path monitoring.

- **Aggressive**—(Default for all link types except LTE and Satellite) Firewall sends probe packets to the opposite end of the SD-WAN link at a constant frequency. Use this mode if you need fast detection and failover for brownout and blackout conditions.
- **Relaxed**—(Default for LTE and Satellite link types) Firewall waits for a number of seconds (the **Probe Idle Time**) between sending sets of probe packets, making path monitoring less frequent. When the probe idle time expires, firewall sends probes for seven seconds at the **Probe Frequency** configured. Use this mode when you have low bandwidth links, links that charge by usage (such as LTE), or when fast detection isn't as important as preserving cost and bandwidth.

STEP 12 | Set the **Probe Frequency (per second)**, which is the number of times per second that the firewall sends a probe packet to the opposite end of the SD-WAN link (range is 1 to 5; default is 5). The default setting provides subsecond detection of brownout and blackout conditions.



If you change the Probe Frequency for a Panorama template, you should also adjust the Packet Loss percentage threshold in a Path Quality profile for a Panorama device group.

STEP 13 | If you select **Relaxed** path monitoring, you can set the **Probe Idle Time (seconds)** that the firewall waits between sets of probe packets (range is 1 to 60; default is 60).

STEP 14 | Enter the **Failback Hold Time (seconds)** that the firewall waits for a recovered link to remain qualified before the firewall reinstates that link as the preferred link after it has failed over (range is 20 to 120; default is 120).

STEP 15 | Click **OK** to save the profile.

STEP 16 | **Commit** and **Commit and Push** your configuration changes.

STEP 17 | Monitor your application and link path health metrics, and generate reports of your application and link health performance. For more information, see [Monitoring and Reporting](#).

Configure a Physical Ethernet Interface for SD-WAN

In Panorama™, configure a physical, Layer 3 Ethernet interface and enable SD-WAN functionality. To configure a physical interface, you must assign it an IPv4 address and next hop gateway, and assign an [SD-WAN Interface Profile](#) to the interface.

After you use Panorama to create a VPN cluster and export your hub and branch information in the CSV, Auto VPN configuration in the SD-WAN plugin uses this information to generate a configuration for the associated branches and hubs that includes the predefined SD-WAN zones and creates secure VPN tunnels between SD-WAN branches and hubs. Auto VPN configuration also generates the BGP configuration if you enter BGP information the CSV or in Panorama when you add an SD-WAN branch or hub.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Select **Network > Interfaces > Ethernet**, select the appropriate template from the **Template** context drop-down, select a slot number, such as Slot1, and select an interface (for example, ethernet1/1).

STEP 3 | Select the **Interface Type** as **Layer3**.

STEP 4 | Select a **Virtual Router** or create a new Virtual Router.

STEP 5 | Assign the **Security Zone** that is appropriate for the interface you're configuring.

For example, if you are creating an uplink to an ISP, you must know that the Ethernet interface you chose is going to an untrusted zone.

STEP 6 | On the **IPv4** tab, **Enable SD-WAN**.

STEP 7 | Select **Type** of address:

- **Static**—In the **IP** field, **Add** an IPv4 address and prefix length for the interface. You can use a defined variable, such as \$uplink, with a range of addresses. Enter the IPv4 address of the **Next Hop Gateway** (the next hop from the IPv4 address you just entered). The Next Hop Gateway must be on the same subnet as the IPv4 address. The Next Hop Gateway is the IP address of the ISP's default router that the ISP gave you when you bought the service. It is the next hop IP address to which the firewall sends traffic to reach the ISP's network, and ultimately, the internet and the hub.
- **PPPoE**—**Enable PPPoE**, enter the **Username** and **Password**, and **Confirm Password**.
- **DHCP Client**—It is critical that DHCP assigns a default gateway, also known as the next hop gateway for the ISP connection. The ISP will provide all the necessary connectivity information, such as dynamic IP address, DNS servers, and the default gateway.



If you select DHCP Client, be sure to disable the option Automatically create default route pointing to default gateway provided by server, which is enabled by default.

The screenshot shows the 'Ethernet Interface' configuration window with the 'SD-WAN' tab selected. The 'Interface Name' is 'ethernet1/6', 'Interface Type' is 'Layer3', and 'Netflow Profile' is 'None'. Under 'Enable SD-WAN', the 'Type' is set to 'Static'. A table for IP configuration is shown with one row selected. The table has columns for 'IP' and 'Next Hop Gateway'. Below the table are buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. A hint text says 'IP address/netmask. Ex. 192.168.2.254/24'. At the bottom are 'OK' and 'Cancel' buttons.

IP	Next Hop Gateway
<input checked="" type="checkbox"/>	

STEP 8 | On the **SD-WAN** tab, select an **SD-WAN Interface Profile** that you already created (or create a new [SD-WAN Interface Profile](#)) to apply to this interface. The SD-WAN Interface Profile has an associated link tag, so the interfaces where this profile is applied will have the associated link tag. An interface can have only one link tag.

STEP 9 | Click **OK** to save the Ethernet interface.

The screenshot shows the 'Ethernet Interface' configuration window with the 'SD-WAN' tab selected. The 'Interface Name' is 'ethernet1/1', 'Interface Type' is 'Layer3', and 'Netflow Profile' is 'None'. Under 'SD-WAN Interface Status: Enabled', the 'SD-WAN Interface Profile' is set to 'Cable modem broadband'. At the bottom are 'OK' and 'Cancel' buttons.


STEP 10 | **Commit** and **Commit and Push** your configuration changes.

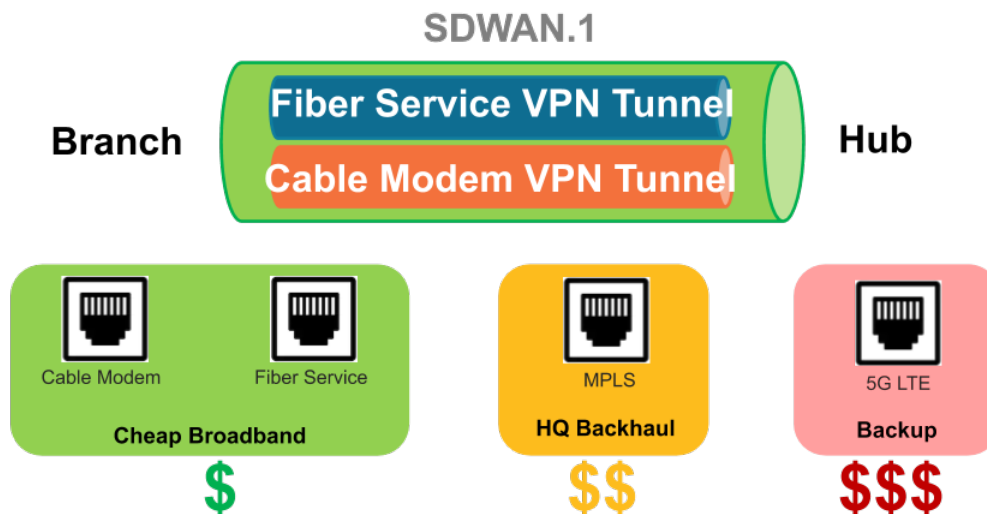
STEP 11 | Configure a [Virtual SD-WAN Interface](#).

Configure a Virtual SD-WAN Interface

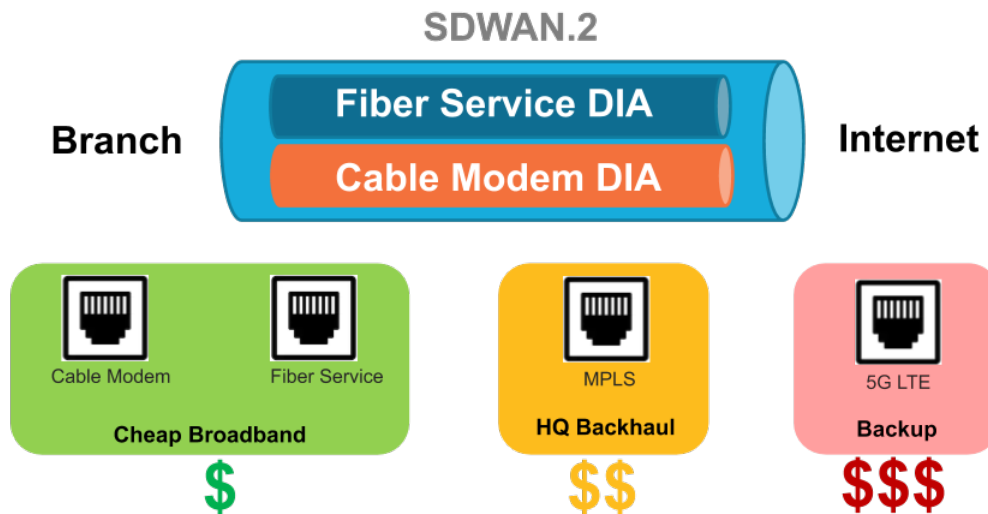
Create and configure a virtual SD-WAN interface to specify one or more physical, SD-WAN-capable [ethernet interfaces](#) that go to the same destination, such as to a specific hub or to the internet. In fact, all links in a virtual SD-WAN interface must be the same type: all VPN tunnel links or all direct internet access (DIA) links.

The first figure illustrates an example of an SD-WAN interface named SDWAN.1 that bundles two physical interfaces, which use different carriers: Ethernet1/1 (the cable modem link) and Ethernet1/2 (the fiber service link). Both links are a VPN tunnel from the branch to the hub.

 In this figure, both links in the SD-WAN interface happen to use the same link tag (*Cheap Broadband*), but links in an SD-WAN interface can have different link tags.



In the following figure, SDWAN.2 bundles Ethernet1/1 and Ethernet1/2 links, which are both DIA links from the branch to the internet:



STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Network > Interfaces > SD-WAN** and select the appropriate template from the **Template** context drop-down.

STEP 3 | Add a logical SD-WAN interface by entering a number (in the range 1 to 9,999) after the **sdwan.** prefix.

STEP 4 | Enter a descriptive **Comment**.



*Add a helpful comment, such as **Branch to internet** or **Branch to western USA hub** if you are on the Branch template. Your comment makes troubleshooting easier rather than trying to decipher auto-generated names in logs and reports.*

STEP 5 | On the **Config** tab, assign the SD-WAN interface to a **Virtual Router**.

STEP 6 | Assign the SD-WAN interface to a **Security Zone**.

The virtual SD-WAN interface and all of its interface members must be in the same Security zone, thus ensuring the same Security policy rules apply to all paths from the branch to the same destination.

STEP 7 | On the **Advanced** tab, **Add Interfaces**, which are members that go to the same destination, by selecting one or more Layer 3 Ethernet interfaces (for DIA) or one more virtual VPN tunnel interfaces (for hub). If you enter more than one interface, they must all be the same type (either VPN tunnel or DIA).



The firewall virtual router uses this virtual SD-WAN interface to route SD-WAN traffic to a DIA or a hub location. During routing, the route table determines which virtual SD-WAN interface (egress interface) the packet will exit based on the destination IP address in the packet. Then the SD-WAN path health and Traffic Distribution profiles in the SD-WAN policy rule that the packet matches determine which path to use (and the order in which to consider new paths if a path deteriorates.)

STEP 8 | Click **OK** to save your configuration change.

STEP 9 | **Commit** and **Commit and Push** your configuration changes.

Create a Default Route to the SD-WAN Interface

If you are using a service route to access Panorama, to bring up the firewall you must create a default route that points to an SD-WAN interface you created.

Auto VPN creates a virtual SD-WAN interface named `sdwan.901` for DIA and creates a virtual SD-WAN interface named `sdwan.902` for VPN tunnels. Auto VPN also creates its own default route that uses the `sdwan.901` interface as its egress interface and uses a low metric, so that the `sdwan.901` interface is preferred over the default route you created.

STEP 1 | Log in to the [Panorama Web Interface](#).

STEP 2 | Select the **Template** you are working on.

STEP 3 | Select **Network > Virtual Routers** and select a virtual router, such as **sd-wan**.

STEP 4 | Select **Static Routes** and **Add** a static route by **Name**.

STEP 5 | For **Destination**, enter `0.0.0.0/0`.

STEP 6 | For egress **Interface**, select one of the logical SD-WAN interfaces you created to bring up the firewall, such as `sdwan.1`.



The egress interface you select can be any logical SD-WAN interface except `sdwan.901` or `sdwan.902`.

STEP 7 | For **Next Hop**, select **None**.

STEP 8 | For **Metric**, enter a value greater than 50, so that this default route is not preferred over the default route that Auto VPN creates with a low metric.

STEP 9 | Click **OK**.

STEP 10 | Select **Commit** and **Commit and Push** your configuration changes.

STEP 11 | **Commit** your changes.

STEP 12 | Repeat this task for other templates on firewalls that use a service route to access Panorama™.

Create a Path Quality Profile

Create a Path Quality profile for business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage. Applications and services can share a Path Quality profile. Specify the maximum threshold for each parameter, above which the firewall considers the path deteriorated enough to select a better path.

As an alternative to creating a Path Quality profile, you can use any of the predefined Path Quality profiles, such as **general-business**, **voip-video**, **file-sharing**, **audio-streaming**, **photo-video**, and **remote-access**, and more. The predefined profiles are set up to optimize the latency, jitter, and packet loss thresholds for the type of applications and services suggested by the name of the profile.



The predefined Path Quality profiles for a Panorama device group are based on the default Probe Frequency settings in the SD-WAN Interface profile for a Panorama template. If you change the default Probe Frequency setting, you must adjust the Packet Loss percentage threshold in the Path Quality profile for the firewalls in a Device Group that are affected by the Panorama template where you changed the Interface profile.

The firewall treats the latency, jitter, and packet loss thresholds as OR conditions, meaning if any one of the thresholds is exceeded, the firewall selects the new best (preferred) path. Any path that has latency, jitter, and packet loss less than or equal to all three thresholds is considered qualified and the firewall selected the path based on the associated Traffic Distribution profile.

By default, the firewall measures **latency** and **jitter** every 200ms and takes an average of the last three measurements to measure path quality in a sliding window. You can modify this behavior by selecting aggressive or relaxed path monitoring when you [Configure an SD-WAN Interface Profile](#).

If a path fails over because it exceeded the configured **packet loss** threshold, the firewall still sends probing packets on the failed path and calculates its packet loss percentage as the path recovers. It can take approximately three minutes for the packet loss percentage on a recovered path to fall below the packet loss threshold configured in the Path Quality profile. For example, suppose an SD-WAN policy rule for an application has a Path Quality profile that specifies a packet loss threshold of 1% and a Traffic Distribution profile that specifies Top Down distribution with tag 1 (applied to tunnel.1) first on the list and tag 2 (applied to tunnel.2) next on the list. When tunnel.1 exceeds 1% packet loss, the data packets fail over to tunnel.2. After tunnel.1 recovers to 0% packet loss (based on probing packets), it can take up to three minutes for the monitored packet loss rate for tunnel.1 to drop below 1%, at which time the firewall then selects tunnel.1 as the best path again.

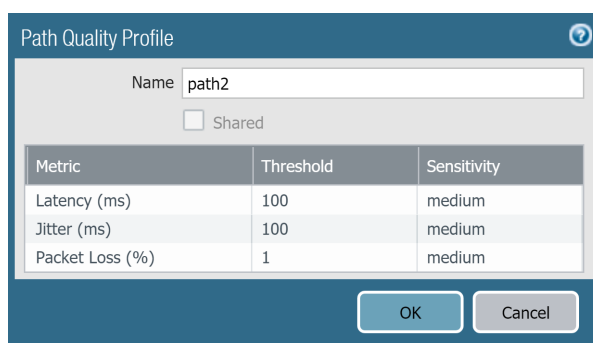
Reference the Path Quality profile in an [SD-WAN policy rule](#) to control the threshold at which the firewall replaces a deteriorating path with a new path for matching application packets.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Select a **Device Group**.

STEP 3 | Select **Objects > SD-WAN Link Management > Path Quality Profile**.

STEP 4 | **Add** a Path Quality profile by **Name** using a maximum of 31 alphanumeric characters.



The dialog box is titled "Path Quality Profile" and has a help icon in the top right corner. It contains a "Name" field with the value "path2" and an unchecked "Shared" checkbox. Below these is a table with three columns: "Metric", "Threshold", and "Sensitivity". The table has three rows: "Latency (ms)" with a threshold of 100 and sensitivity of medium; "Jitter (ms)" with a threshold of 100 and sensitivity of medium; and "Packet Loss (%)" with a threshold of 1 and sensitivity of medium. At the bottom right are "OK" and "Cancel" buttons.

Metric	Threshold	Sensitivity
Latency (ms)	100	medium
Jitter (ms)	100	medium
Packet Loss (%)	1	medium

STEP 5 | For **Latency**, double-click the **Threshold** value and enter the number of milliseconds allowed for a packet to leave the firewall, arrive at the opposite end of the SD-WAN tunnel, and a response packet to return to the firewall before the threshold is exceeded (range is 10 to 2,000; default is 100).

STEP 6 | (Optional) For **Latency**, select the **Sensitivity** (low, medium, or high). Default is **medium**.

The sensitivity setting indicates which path monitoring parameter (latency, jitter, or packet loss) is more important (preferred) for the application(s) to which the profile applies. The firewall places more importance on a parameter with a high setting than a parameter with a medium or low setting. If the parameters have the same sensitivity (by default the parameters are set to **medium**), the preference order is packet loss, latency, jitter.



Click the arrow at the end of the **Threshold** column to sort thresholds in ascending or descending numerical order.

STEP 7 | For **Jitter**, double-click the **Threshold** value and enter the number of milliseconds (range is 10 to 1,000; default is 100).

STEP 8 | (Optional) For **Jitter**, select the **Sensitivity** (low, medium, or high). Default is **medium**.

STEP 9 | For **Packet Loss**, double-click the **Threshold** value and enter the percentage of packets lost on the link before the threshold is exceeded (range is 1 to 100.0; default is 1).



If you change the **Probe Frequency** in an SD-WAN Interface profile for a Panorama template, you should also adjust the **Packet Loss** threshold for a Panorama device group.

STEP 10 | (Optional) For **Packet Loss**, select the **Sensitivity** (low, medium, or high). Default is **medium**.

STEP 11 | Click **OK**.

STEP 12 | **Commit** and **Commit and Push** your configuration changes.

STEP 13 | **Commit** your changes.

STEP 14 | Repeat this task for every Device Group.

SD-WAN Traffic Distribution Profiles

In an SD-WAN topology, the firewall detects a brownout, a blackout, and path deterioration *per application* and selects a new path to ensure you experience the best performance for your critical business applications. Having multiple ISP links allows you to scale your traffic capacity and reduce costs. The new path selection occurs in less than one second if you leave [Path Monitoring and Probe Frequency](#) with default settings; otherwise, new path selection could take more than one second.

To implement such path selection, the firewall uses SD-WAN policy rules, which reference a Traffic Distribution profile that specifies how to select paths for session load distribution and for failover to a better path when path quality for an application deteriorates.

Decide which traffic distribution method an application or service (that matches an SD-WAN policy rule) should use:

- **Best Available Path**—Select this method if cost is not a factor and you will allow applications to use any path out of the branch. The firewall uses path quality metrics to distribute traffic and to fail over to one of the links belonging to a Link Tag in the list, thus providing the best application experience to users.
- **Top-Down Priority**—If you have expensive or low-capacity links that you want used only as a last resort or as a backup link, use the Top-Down Priority method and place the tags that include those links last in the list of Link Tags in the profile. The firewall uses the top Link Tag in the list first to determine the links on which to session load traffic and on which to fail over. If none of the links in the top Link Tag are qualified based on the Path Quality profile, the firewall selects a link from the second Link Tag in the list. If none of the links in the second Link Tag are qualified, the process continues as necessary until the firewall finds a qualified link in the last Link Tag. If all associated links are overloaded and no link meets quality thresholds, the firewall uses the Best Available Path method to select a link on which to forward traffic. At the start of a failover event, the firewall starts at the top of the Top-Down Priority list of Link Tags to find a link to which it fails over.
- **Weighted Session Distribution**—Select this method if you want to manually load traffic (that matches the rule) onto your ISP and WAN links and you don't require failover during brownout conditions. You manually specify the link's load when you apply a static percentage of new sessions that the interfaces grouped with a single Link Tag will get. The firewall distributes new sessions using round robin among the links having the specified Link Tags, until the link assigned the lowest percentage reaches that percentage of sessions. The firewall then uses the remaining link(s) in the same manner. You might select this method for applications that aren't sensitive to latency and that require a lot of the link's bandwidth capacity, such as large branch backups and large file transfers.



If the link experiences brownout, the firewall doesn't redirect the matching traffic to a different link.

In the event of a failing path condition, the traffic distribution method you choose for application(s) in an SD-WAN policy rule, along with the Link Tags on groups of links, determine if and how the firewall selects a new path (performs link failover) as follows:

Path Condition	Top-Down Priority	Best Available Path	Weighted Session Distribution
Session on existing path failed a path health threshold (brownout)	Affected session fails over to better path (if available)	Affected session fails over to better path (if available)	Affected sessions don't fail over
Top-Down or Best Available Path	Affected session fails back to previous path	Affected session stays on existing path, doesn't fail back	Affected sessions don't fail over

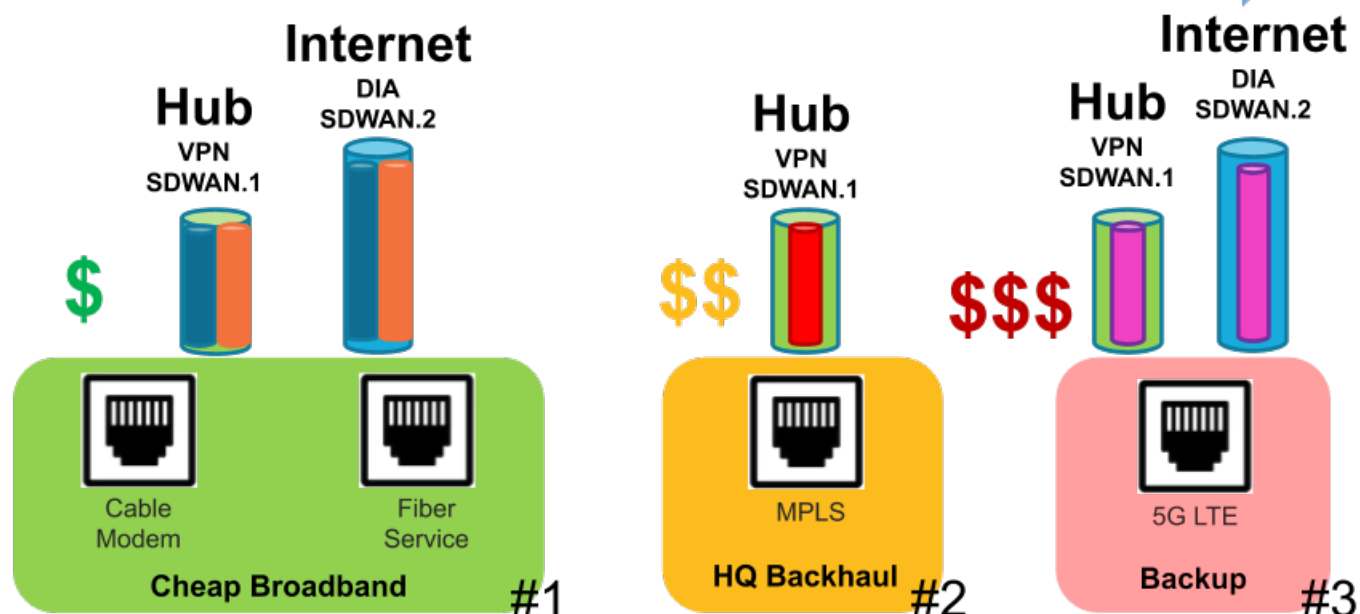
Path Condition	Top-Down Priority	Best Available Path	Weighted Session Distribution
recovered: existing path is still qualified (good)			
Top-Down or Best Available Path recovered: existing path fails a health check	All sessions fail back to previous path	Selective sessions fail back to previous path until affected existing path recovers	Affected sessions don't fail over
Existing path is down (blackout)	All sessions fail over to next path on list	All sessions fail over to next best path	All sessions fail over to other tags based on weight settings
Brownout with no qualified (better) path	Take best available path	Take best available path	Take best available path

Additionally, the firewall automatically performs session load sharing among interface members of a single Link Tag. After those interfaces approach their maximum Mbps, new sessions flow over to interfaces having a different Link Tag (based on the traffic distribution method) if those interfaces have better health metrics.

Path Condition	Top-Down Priority	Best Available Path	Weighted Session Distribution
Multiple links with the same SD-WAN Tag	Share session load equally among links within SD-WAN Tag	Share session load based on best path within SD-WAN Tag	Share session load based on % weight assigned to SD-WAN Tag
Multiple links with different SD-WAN Tags	Share session load based on list priority, load link(s) in first SD-WAN Tag first.	Share session load based on best path from all SD-WAN Tags	Share session load based on % weight assigned to SD-WAN Tags

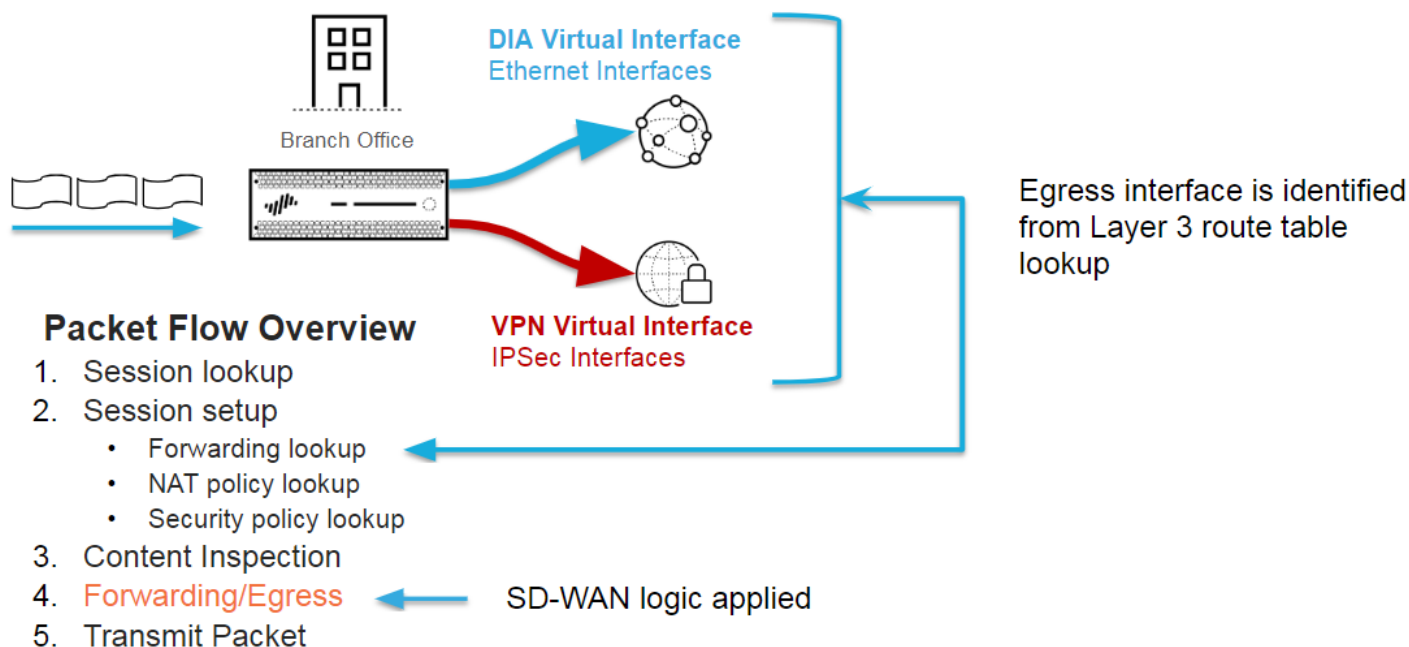
The following figure illustrates an example of a Traffic Distribution profile that uses the Top-Down Priority method. The #1, #2, and #3 are the order of Link Tags of links the firewall examines, if necessary, to find a healthy path to complete an application session failover. For each separate failover event that arises, the firewall starts at the beginning of the Top-Down list of Link Tags.

Traffic Distribution Failover Order (Top-Down)



1. In this Top-Down Priority example, packets from a branch carrying a specific application (for example, office365-enterprise-access) arrive at the firewall. The firewall uses the route table to determine the next hop to the destination and the outgoing interface, which is the virtual SD-WAN interface tunnel named sdwan.1. The Security policy rule allows the packets. The packets then match an SD-WAN policy rule (named Office365 to Hub1) that specifies the destination zone for the hub. The firewall uses the SD-WAN policy rule's Path Quality profile, Traffic Distribution profile, and that profile's Link Tags to determine which interface member (link) from sdwan.1 to use. The Traffic Distribution profile lists three Link Tags in this order: #1 Cheap Broadband, #2 HQ Backhaul, and #3 Backup (which is the order of Link Tags the firewall examines links to find a link to which it can fail over).
2. Assuming all paths are qualified (by the Path Quality profile), the firewall distributes the packets to one of the physical links tagged with first Link Tag in the Traffic Distribution profile list: Cheap Broadband. The sdwan.1 tunnel has two member interfaces (two carriers): the cable modem VPN tunnel and the fiber service VPN tunnel. The firewall first examines a link by round-robin, and chooses the first link it finds that is qualified, for example, the cable modem link.
3. If the first Cheap Broadband link (cable modem) isn't a qualified link, the firewall selects the second Cheap Broadband link (fiber service).
4. If the second Cheap Broadband link (fiber service) isn't a qualified link, the firewall selects the link tagged with the #2 link tag HQ Backhaul, which is a more expensive MPLS link to the same hub.
5. If the MPLS link isn't a qualified link, the firewall selects the link tagged with the #3 link tag Backup, which is an even more expensive 5G LTE link to the same hub.
6. If the firewall doesn't find a qualified link to fail over to, it uses the Best Available method to select a link.
7. Upon the start of a new failover event, the firewall starts at the top of the Top-Down list of Link Tags to find a link to which it will fail over.

Keep in mind that SD-WAN traffic distribution is one of the later steps in the packet flow logic. Let's zoom out to see a broader view of the packet flow.

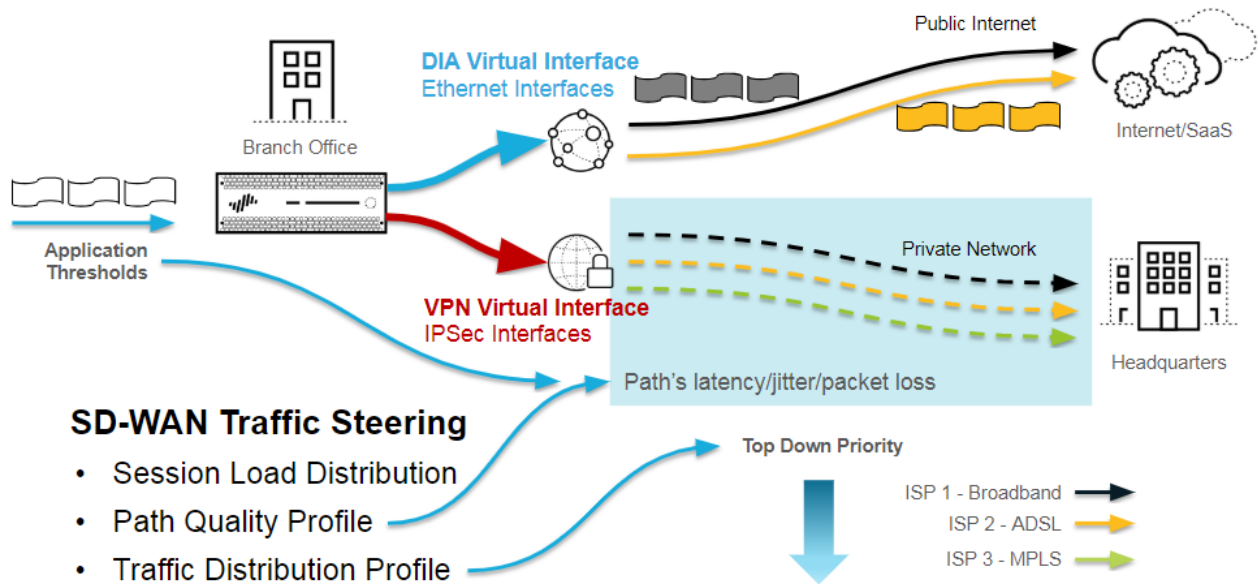


Packet flow details for the figure are as follows:

1. When a session for an application arrives at the firewall, the firewall performs session lookup to determine if the session is an existing session or new session.
2. A new session goes through session setup:
 1. Forwarding lookup—The firewall gets the egress zone, egress interface, and virtual system from the Layer 3 route table or Layer 2 Forwarding Database lookup, etc. For applications that match an SD-WAN policy rule, the firewall uses the virtual SD-WAN interface as the egress interface.
 2. NAT Policy lookup—If session matches a NAT rule, firewall does another forwarding lookup to determine the final (translated) egress interface and zone.
 3. Security Policy lookup—If a Security Policy rule allows the session, the session is created and installed in the session table. The firewall then performs additional classification using App-ID™ and User-ID™.
3. Content Inspection—The firewall performs Threat Inspection (Anti-Spyware for IPS [Vulnerability Protection], Antivirus, URL Filtering, WildFire®, etc.) on payload and headers as needed.
4. The Forwarding/Egress stage performs path selection and forwards the packets. This stage is where SD-WAN path selection occurs.
 1. Packet Forwarding Process—The firewall uses the ingress interface to determine the forwarding domain; performs routing, switching, or virtual wire forwarding.
 2. SD-WAN path selection occurs when the application matches an SD-WAN policy rule; the Path Quality profile determines path qualification; the Traffic Distribution profile determines the method of path selection and the order in which paths are considered during the selection.
 3. IPsec/SSL-VPN tunnel encryption occurs if needed.
 4. Packet Egress Process - QoS shaping, DSCP rewrite, and IP fragmentation are applied (if needed).
5. Transmit Packet—The firewall forwards the packet over the selected egress interface.

Now we zoom back in to examine the SD-WAN path selection logic in more detail.

Secure SD-WAN's Path Selection Logic



1. The firewall consults the route table during Forwarding lookup; based on the destination IP address matching a Layer 3 prefix, the firewall determines the egress SD-WAN virtual interface. The packet is either going directly to the public internet or going back to the hub through a secure VPN link.
2. The firewall monitors each path by performing health checks that run over a VPN tunnel. Each DIA circuit has a VPN tunnel that monitors health information.
3. The application in the SD-WAN policy rule is associated with a Path Quality profile, and the firewall compares the path's actual average latency, jitter, and packet loss values to the threshold values.
4. Any path that has a higher latency, jitter, or packet loss value than the threshold is not selected.
5. All qualifying paths in the virtual SD-WAN interface are then subjected to the Traffic Distribution profile's method and path priority (ordering) logic. SD-WAN link tags group ISP services together, and the order of these tags in the Traffic Distribution profile prioritizes the paths during path selection.
6. Thus, the [Path Quality Profile](#) and the [Traffic Distribution profile](#) together determine the next best path to use and the firewall forwards the traffic out that link.

Create a Traffic Distribution Profile

Based on your SD-WAN configuration plan, create the [SD-WAN Traffic Distribution Profiles](#) you need based on how you want the applications in your SD-WAN policy rules to be session loaded and to fail over.

STEP 1 | Log in to the [Panorama Web Interface](#).

STEP 2 | Ensure you already configured the Link Tags in an [SD-WAN interface profile](#) and committed and pushed them. The Link Tags must be pushed to your hubs and branches in order for Panorama™ to successfully associate the Link Tags you specify in this Traffic Distribution profile to an SD-WAN interface profile.

STEP 3 | Select a **Device Group**.

STEP 4 | Create a Traffic Distribution profile.

1. Select **Objects > SD-WAN Link Management > Traffic Distribution Profile**.
2. **Add** a Traffic Distribution profile by **Name** using a maximum of 31 alphanumeric characters.

3. Select **Shared** only if you want to use this traffic distribution profile across all Device Groups (both hubs and branches).
4. Select one traffic distribution method and add a maximum of four Link Tags that use this method for this profile.
 - **Best Available Path**—Add one or more **Link Tags**. During the initial packet exchanges, before App-ID has classified the application in the packet, the firewall uses the path in the tag that has the best health metrics (based on the order of tags). After the firewall identifies the application, it compares the health (path quality) of the path it was using to the health of the first path (interface) in the first Link Tag. If the original path's health is better, it remains the selected path; otherwise, the firewall replaces the original path. The firewall repeats this process until it has evaluated all the paths in the Link Tag. The final path is the path the firewall selects when a packet arrives that meets the match criteria.

- **Top Down Priority—Add** one or more **Link Tags**. The firewall distributes new sessions (that meet the match criteria) to links using the top-to-bottom order of the **Link Tags** you added. The firewall examines the first tag configured for this profile, and examines the paths that use that tag, selecting the first path it finds that is qualified (that is at or below the Path Quality thresholds for this rule). If no qualified path is found from that Link Tag, firewall examines the paths that use the next Link Tag. If the firewall finds no path after examining all paths in all of the Link Tags, the firewall uses the **Best Available Path** method. The first path selected is the preferred path until one of the Path Quality thresholds for that path is exceeded, at which point the firewall again starts at the top of the Link Tag list to find the new preferred path.
- **Weighted Session Distribution—Add** one or more **Link Tags** and then enter the **Weight** percentage for each **Link Tag** so that the weights total 100%. The firewall performs session load distribution between Link Tags until their percentage maximums are reached. If there is more than one path in the Link Tag, the firewall distributes equally using round-robin until the path health metrics are reached, and then distributes sessions to the other member(s) that are not at the limit.



If multiple physical interfaces have the same tag, the firewall distributes matching sessions evenly among them. If all paths fail a health (path quality) threshold, the firewall selects the path that has the best health statistics. If no SD-WAN links are available (perhaps due to a blackout), the firewall uses static or dynamic routing to route the matching packets.



If a packet is routed to a virtual SD-WAN interface, but the firewall cannot find a preferred path for the session based on the SD-WAN policy's Traffic Distribution profile, the firewall implicitly uses the Best Available Path method to find the preferred path. The firewall distributes any application sessions that don't match an SD-WAN policy rule based on the firewall's implicit, final rule, which distributes the sessions in round-robin order among all available links, regardless of the Traffic Distribution profile.



If you prefer to control how the firewall distributes unmatched sessions, create a final catch-all rule to [Distribute Unmatched Sessions](#) to specific links in the order you specify.

5. (Optional) After adding Link Tags, use the **Move Up** or **Move Down** arrows to change the order of tags in the list, so they reflect the order in which you want the firewall to use links for this profile and for the selected applications in the SD-WAN policy rule.
6. Click **OK**.

STEP 5 | Commit and Commit and Push your configuration changes.

STEP 6 | Commit your changes.

Configure an SD-WAN Policy Rule

An SD-WAN policy rule specifies application(s) and/or service(s) and a traffic distribution profile to determine how the firewall selects the preferred path for an incoming packet that doesn't belong to an existing session and that matches all other criteria, such as source and destination zones, source and destination IP addresses, and source user. The SD-WAN policy rule also specifies a path quality profile of thresholds for latency, jitter, and packet loss. When one of the thresholds is exceeded, the firewall selects a new path for the application(s) and/or service(s).

When [monitoring](#) your SD-WAN traffic, traffic originating from a source behind the hub device is evaluated against the SD-WAN policies pushed to the hub device as it enters the hub device, and because the path selection decision has already been made, the branch device does not evaluate the traffic against its SD-WAN policies as it passes through the branch device to the final target device. Conversely, traffic originating from a source behind the branch device is evaluated against the SD-WAN policies pushed to the branch device and not by hub device. The Panorama™ management server aggregates the logs from both the hub and branch, and for the same traffic, two session entries are displayed but only the SD-WAN device that originally evaluated the traffic contains the SD-WAN details.

In an SD-WAN policy rule, you also specify the devices to which you want Panorama to push the rule.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Select **Policies > SD-WAN** and select the appropriate device group from the **Device Group** context drop-down.

STEP 3 | **Add** an SD-WAN policy rule.

STEP 4 | On the **General** tab, enter a descriptive **Name** for the rule.

STEP 5 | On the **Source** tab, configure the source parameters of the policy rule.

1. Add the **Source Zone** or select **Any** source zone
2. **Add** one or more source addresses, set an [external dynamic list](#) (EDL), or select **Any** Source Address.
3. **Add** one or more source users or select **any** Source User.

STEP 6 | On the **Destination** tab, configure the destination parameters of the policy rule.

1. **Add** the **Destination Zone** or select **Any** destination zone.
2. **Add** one or more destination addresses, set an EDL, or select **Any** Destination Address.

STEP 7 | On the **Application/Service** tab, select a **Path Quality** profile or [Create a Path Quality Profile](#).

STEP 8 | **Add Applications** and select one or more applications from the list or select **Any** applications. All applications you select are subject to the health thresholds specified in the Path Quality profile you selected. If a packet matches one of these applications and that application exceeds one of the health thresholds in the Path Quality profile (and the packet matches the remaining rule criteria), the firewall selects a new preferred path.



Add only business-critical applications and applications that are sensitive to path conditions for their usability.

STEP 9 | **Add Services** and select one or more services from the list or select **Any** services. All services you select are subject to the health thresholds specified in the Path Quality profile you

selected. If a packet matches one of these services and that service exceeds one of the health thresholds in the Path Quality profile (and the packet matches the remaining rule criteria), the firewall selects a new preferred path.



Add only business-critical services and services that are sensitive to path conditions for their usability.

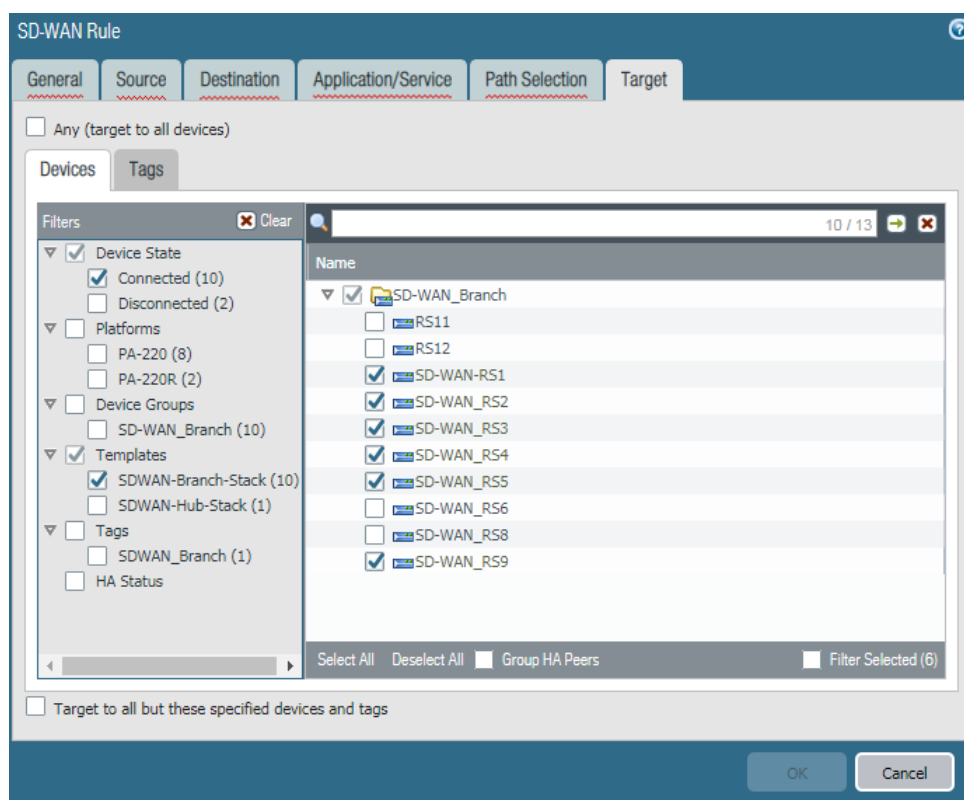
The screenshot shows the 'SD-WAN Rule' configuration window with the 'Path Selection' tab selected. The 'Path Quality Profile' is set to 'file-sharing'. Under the 'Applications' section, 'confluence-sharing' is selected. Under the 'Service' section, 'application-default' is selected. The window includes 'Add' and 'Delete' buttons for both sections, and 'OK' and 'Cancel' buttons at the bottom right.

STEP 10 | On the **Path Selection** tab, select a **Traffic Distribution** profile or [Create a Traffic Distribution Profile](#). When an incoming packet (unassociated with a session) matches all the match criteria in the rule, the firewall uses this Traffic Distribution profile to select a new preferred path.

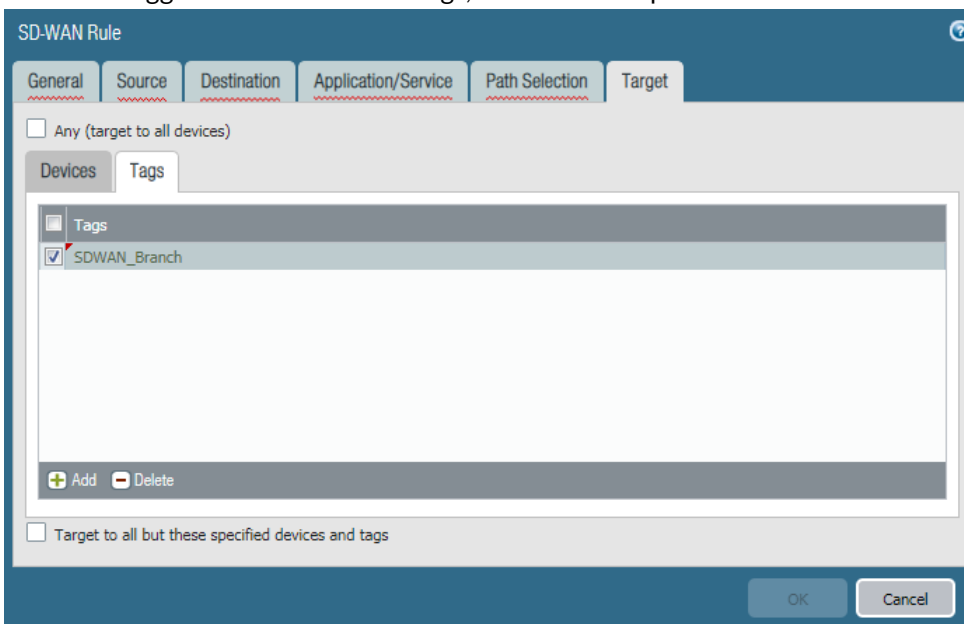
The screenshot shows the 'SD-WAN Rule' configuration window with the 'Path Selection' tab selected. The 'Path Selection Settings' section is expanded, showing the 'Traffic Distribution Profile' set to 'least expensive link first'. The window includes 'OK' and 'Cancel' buttons at the bottom right.

STEP 11 | On the **Target** tab, use one of the following methods to specify the target firewalls in the device group to which Panorama pushes the SD-WAN policy rule:

- Select **Any (target to all devices)** (the default) to push the rule to all devices. Alternatively, select **Devices** or **Tags** to specify the devices to which Panorama pushes the SD-WAN policy rule.
- On the **Devices** tab, select one or more filters to restrict the selections that appear in the Name field; then select one or more devices to which Panorama pushes the rule, as in this example:



- On the **Tags** tab, **Add** one or more **Tags** and select the tag(s) to specify that Panorama push the rule to devices that are tagged with the selected tags, as in this example:



- If you specified Devices or Tags, you can select **Target to all but these specified devices and tags** to have Panorama push the SD-WAN policy rule to all devices except for the specified devices or tagged devices.

STEP 12 | Click **OK**.

STEP 13 | **Commit** and **Commit and Push** your configuration changes.

STEP 14 | (Best Practice) Create a catch-all SD-WAN policy rule to [Distribute Unmatched Sessions](#) so that you can control which links any unmatched sessions use and view unmatched sessions in logging and reports in the SD-WAN plugin.



If you don't create a catch-all rule to distribute unmatched sessions, the firewall distributes them in round-robin order among all available links because there is no traffic distribution profile for unmatched sessions. Round-robin distribution of unmatched sessions can increase your costs unexpectedly and result in loss of application visibility.

STEP 15 | After configuring your SD-WAN policy rules, [Create a Security Policy Rule](#) to allow traffic (for example, **bgp** as an **Application**) from branches to the internet, from branches to hubs, and from hubs to branches.

STEP 16 | (Optional) [Configure QoS](#) for critical applications.



If the SD-WAN applications need guaranteed bandwidth capacities or if you do not want other applications taking bandwidth from critical business applications, create QoS rules to control the bandwidth properly.

STEP 17 | To automatically set up BGP routing between VPN cluster members, in the SD-WAN plugin, [Configure BGP](#) routing between branches and hubs to dynamically route traffic that will be subject to the SD-WAN failover and load sharing.

Alternatively, if you want to manually configure BGP routing on each firewall or use a separate Panorama template to configure BGP routing (for more control), leave the BGP information in the plugin blank. Instead, configure BGP routing.

STEP 18 | Configure NAT for public-facing virtual SD-WAN interfaces.

Distribute Unmatched Sessions

The firewall attempts to match sessions that arrive at an SD-WAN virtual interface to an SD-WAN policy rule; the firewall examines the SD-WAN policy rules in order from the top down, just as it does for Security policy rules.

- If there is an SD-WAN rule match, the firewall executes the path monitoring and traffic distribution for that SD-WAN policy rule.
- If there is no match to any SD-WAN policy rule in the list, the session matches an implied SD-WAN policy rule at the end of the list that uses the round-robin method to distribute unmatched sessions among all links in one SD-WAN interface, which is based on the route lookup.

Furthermore, if there is no SD-WAN policy rule for a specific application, the firewall doesn't track that application's performance in the SD-WAN-specific visibility tools such as logging and reports in the SD-WAN plugin.

To illustrate the implied policy rule:

- Suppose the firewall has three SD-WAN policy rules: one rule specifies five voice applications, one rule specifies six video conferencing applications, and one rule specifies ten SaaS applications.
- A session, for example, a video application session, arrives at the firewall and doesn't match any of the SD-WAN policy rules. Because the session didn't match a rule, the firewall has no path quality profile or traffic distribution profile to apply to the session.
- Therefore, firewall matches the video application to the implied rule and distributes each video session among all of the available SD-WAN link tags and their associated links on the firewall, which could be two broadband links, an MPLS link, and an LTE link. Session 1 goes to one member of the broadband interface, session 2 goes to another member of the broadband interface, session 3 goes to MPLS, session 4 goes to LTE, session 5 goes to the first member of the broadband interface, session 6 goes to the second member of the broadband interface, and the round-robin distribution continues.

You may not want to let your unmatched sessions resort to matching the implied SD-WAN rule because you have no control over that session distribution. Instead, we recommend you create a catch-all SD-WAN policy rule and place it last in the list of SD-WAN policy rules. A catch-all SD-WAN policy rule lets you:

- Control which links the unmatched sessions use.
- View all of the applications on the firewall (including unmatched application sessions) in logging and reports in the SD-WAN plugin.

STEP 1 | [Log in to the Panorama Web Interface.](#)

STEP 2 | [Create a Path Quality Profile](#) that sets very high latency, jitter, and packet loss thresholds that will never be exceeded. For example, 2,000ms latency, 1,000ms jitter, and 99% packet loss.

STEP 3 | [Create a Traffic Distribution Profile](#) that specifies the SD-WAN link tags you want to use, in the order in which you want the links associated with those link tags to be used by unmatched sessions.



If you don't want unmatched applications to use a specific path (physical interface) at all, omit the tag that includes that link from the list of link tags in the traffic distribution profile. For example, if you don't want an unmatched application such as movie streaming to use the expensive LTE link, omit the link tag for the LTE link from the list of link tags in the traffic distribution profile.

STEP 4 | Add a catch-all **SD-WAN policy rule** and on the **Application/Service** tab, specify the **Path Quality Profile** that you created.

STEP 5 | Select **Any** for the **Applications** and **Service**.

STEP 6 | On the **Path Selection** tab, select the **Traffic Distribution Profile** you created.

STEP 7 | **Move** the rule down to the last position in the list of SD-WAN policy rules.

STEP 8 | **Commit** and **Commit and Push** your configuration changes.

STEP 9 | **Commit** your changes.

Add SD-WAN Devices to Panorama

Add a single SD-WAN hub or branch firewall or use a CSV to bulk import multiple SD-WAN hub and branch firewalls.

- [Add an SD-WAN Device](#)
- [Bulk Import Multiple SD-WAN Devices](#)

Add an SD-WAN Device

Add an SD-WAN hub or branch firewall to be managed by the Panorama™ management server. When adding your devices, you specify what type of device it is (branch or hub) and you give each device their site name for easy identification. Before adding your devices, [plan your SD-WAN configuration](#) to ensure you have all the required IP addresses and that the SD-WAN topology is well understood. This helps in reducing any configuration errors.

If you have pre-existing zones for your Palo Alto Networks® firewalls, you will be mapping them to the predefined zones used in SD-WAN.



If you want to have Active/Passive HA running on two branch firewalls or two hub firewalls, do not add those firewalls as SD-WAN devices at this time. You will add them as HA peers separately when you [Configure HA Devices for SD-WAN](#).



If you are using BGP routing, you must add a security policy rule to allow BGP from the internal zone to the hub zone and from the hub zone to the internal zone. If you want to use 4-byte ASNs, you must first enable 4-byte ASNs for the virtual router.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | Select **Panorama > SD-WAN > Devices** and **Add** a new SD-WAN firewall.

STEP 3 | Select the managed firewall **Name** to add as an SD-WAN device. You must [add your SD-WAN firewalls as managed devices](#) before you can add them as an SD-WAN device.

STEP 4 | Select the **Type** of SD-WAN device.

- **Hub**—A centralized firewall deployed at a primary office or location to which all branch devices connect using a VPN connection. Traffic between branches passes through the hub before continuing to the target branch, and connects branches to centralized resources at the hub location. The hub device processes traffic, enforces policy rules, and manages link swapping at the primary office or location.
- **Branch**—A firewall deployed at a physical branch location that connects the hub using a VPN connection and provides security at the branch level. The branch device processes traffic, enforces policy rules, and manages link swapping at the branch location.

STEP 5 | Select the **Virtual Router Name** to use for routing between the SD-WAN hub and branches. By default, an `sdwan-default` virtual router is created and enables Panorama to automatically push router configurations.

STEP 6 | Enter the SD-WAN **Site** name to identify the geographical location or purpose of the device.

STEP 7 | (Required for pre-existing customers) Map your pre-existing zones to predefined zones used for SD-WAN.

1. Select **Zone Internet** and **Add** the pre-existing zones that will egress SD-WAN traffic to the internet.
2. Select **Zone to Hub** and **Add** the pre-existing zones that will egress SD-WAN traffic to the hub.
3. Select **Zone to Branch** and **Add** the pre-existing zones that will egress SD-WAN traffic to the branch.
4. Select **Zone Internal** and **Add** the pre-existing zones that will egress SD-WAN traffic to an internal zone.

STEP 8 | (Optional) Configure Border Gateway Protocol (BGP) routing.

1. Enable **BGP** to configure BGP routing for SD-WAN traffic.
2. Enter the BGP **Router ID**, which must be unique among all routers.
3. Specify a static IPv4 **Loopback Address** for BGP peering.
4. Enter the **AS Number**. The autonomous system number specifies a commonly defined routing policy to the internet. The AS number must be unique for every hub and branch location.
5. Enter **Prefix(es) to Redistribute**.

STEP 9 | Click **OK**.

STEP 10 | **Commit** your configuration changes.

STEP 11 | Select **Push to Devices** to push your configuration changes to your managed firewalls.

Bulk Import Multiple SD-WAN Devices

Add multiple SD-WAN devices to quickly onboard branch and hub firewalls, rather than manually adding each device one at a time. When adding your devices, you specify what type of device it is (branch or hub) and you give each device its site name for easy identification. Before adding your devices, [plan your SD-WAN configuration](#) to ensure you have all the required IP addresses and that the SD-WAN topology is well understood. This helps reduce any configuration errors.



If you want to have Active/Passive HA running on two branch firewalls or two hub firewalls, do not add those firewalls as SD-WAN devices in your CSV file. You will add them as HA peers separately when you [Configure HA Devices for SD-WAN](#).



If you are using BGP routing, you must add a security policy rule to allow BGP from the internal zone to the hub zone and from the hub zone to the internal zone. If you want to use 4-byte autonomous system numbers (ASNs), you must first enable 4-byte ASNs for the virtual router.

If you have pre-existing zones for your Palo Alto Networks firewalls, you will be mapping them to the predefined zones used in SD-WAN.

STEP 1 | Log in to the [Panorama Web Interface](#).

STEP 2 | Select **Panorama > SD-WAN > Devices > Device CSV** and **Export** an empty SD-WAN device CSV. The CSV allows you to import multiple branch and hub devices at once, rather than adding each device manually.



STEP 3 | Populate the SD-WAN device CSV with the branch and hub information and save the CSV. All fields are required unless noted otherwise. You must enter the following for each hub and branch:

- **device-serial**—The serial number of the branch or hub firewall.
- **type**—Specify whether the device is a **branch** or a **hub**.
- **site**—Enter the SD-WAN device site name to help you identify the geographical location or purpose of the device.
- **(Required for pre-existing customers)** Map your pre-existing zones to predefined zones used for SD-WAN.
 - **zone-internet**—Enter the names of pre-existing zones that SD-WAN traffic will egress to reach the internet.
 - **zone-to-branch** —Enter the names of pre-existing zones that SD-WAN traffic will egress to reach a branch.
 - **zone-to-hub**—Enter the names of pre-existing zones that SD-WAN traffic will egress to reach a hub.
 - **zone-internal**—Enter the names of pre-existing zones that SD-WAN traffic will egress to reach an internal zone.
- **(Optional) loopback-address**—Specify a static loopback IPv4 address for Border Gateway Protocol (BGP) peering.
- **(Optional) prefix-redistribute**—Enter IP prefixes that the branch informs the hub it can reach. To add more than one prefix, separate prefixes with a space, an ampersand (&), and a space; for example, 192.2.10.0/24 & 192.168.40.0/24. By default, the branch firewall advertises all locally connected internet prefixes to the hub.



Palo Alto Networks does not redistribute the branch office default route(s) learned from the ISP.

- **(Optional) as-number**—Enter the ASN of the private AS to which the virtual router on the hub or branch belongs. The SD-WAN plugin supports only private autonomous systems. The ASN must be unique for every hub and branch. The 4-byte ASN range is 4,200,000,000 to 4,294,967,294 or 64512.64512 to 65535.65534. The 2-byte ASN range is 64512 to 65534.



Use a 4-byte private ASN.

- **(Optional) router-id**—Specify the BGP router ID, which must be unique among all virtual routers.



Enter the Loopback Address as the router ID.

- **vr-name**—Enter the name of the virtual router to use for routing between the SD-WAN hub and branches. By default, Panorama creates an `sdwan-default` virtual router and can automatically push router configurations.

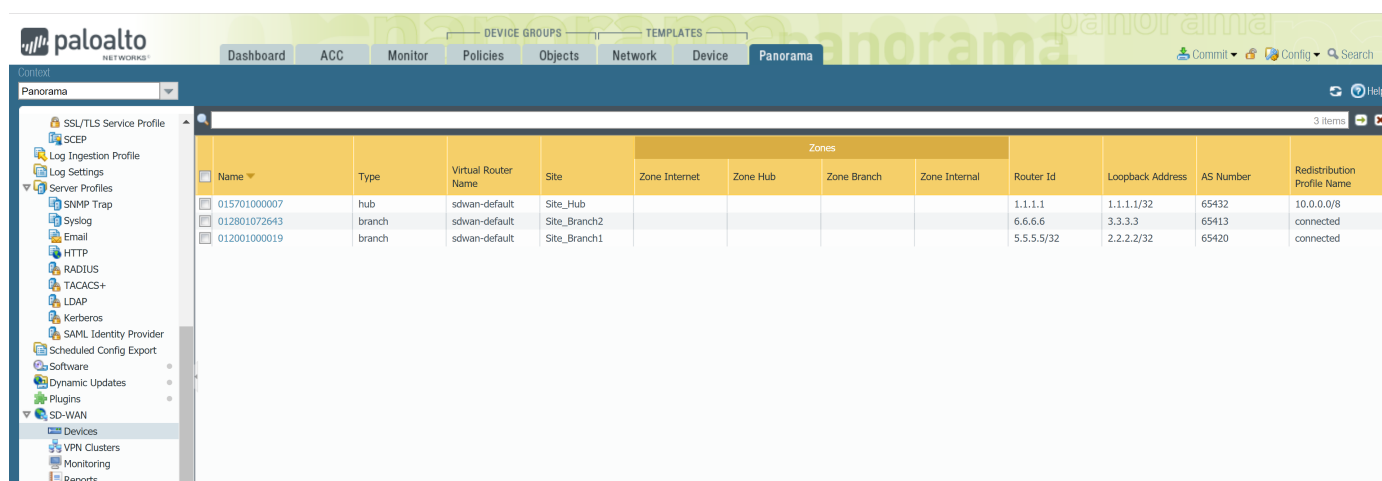
	A	B	C	D	E	F	G	H	I	J	K
1	device-serial	type	site	zone-internet	zone-branch	zone-hub	zone-internal	loopback-address	prefixes redistrib	as-number	router-id
2	12001000019	branch	Site_Branch1					2.2.2.2/32		65420	5.5.5.5/32
3	12801072643	branch	Site_Branch2					3.3.3.3		65413	6.6.6.6
4	15710000007	hub	Site_Hub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

STEP 4 | Import the SD-WAN device CSV into Panorama.

Verify that there are no pending commits on Panorama or the import fails.

1. On Panorama, Select **Panorama > SD-WAN > Devices > Device CSV** and **Import** the CSV you edited in the previous step.
2. **Browse** and select the SD-WAN device CSV.
3. Click **OK** to import the SD-WAN devices.

STEP 5 | Verify that your SD-WAN devices were successfully added.



Name	Type	Virtual Router Name	Site	Zone Internet	Zone Hub	Zone Branch	Zone Internal	Router Id	Loopback Address	AS Number	Redistribution Profile Name
015701000007	hub	sdwan-default	Site_Hub					1.1.1.1	1.1.1.1/32	65432	10.0.0.0/8
012801072643	branch	sdwan-default	Site_Branch2					6.6.6.6	3.3.3.3	65413	connected
012001000019	branch	sdwan-default	Site_Branch1					5.5.5.5/32	2.2.2.2/32	65420	connected

STEP 6 | Commit your configuration changes.

STEP 7 | Select **Push to Devices** to push your configuration changes to your managed firewalls.

Configure HA Devices for SD-WAN

You can configure two branches or two hubs in active/passive HA mode to be part of your SD-WAN environment. In this case, Panorama™ needs to push the same configuration to the active peer and the passive peer, rather than treat the two firewalls individually. To make that happen, you configure active/passive HA before adding the devices for SD-WAN, so that Panorama is aware the devices are HA peers and pushes the same configuration to them.



Read through the following procedure before you begin so you don't Commit after adding your HA peers as SD-WAN devices.

- STEP 1** | Before you enable SD-WAN on your HA peers, [configure Active/Passive HA](#) on two firewall models that support SD-WAN.
- STEP 2** | Add the HA peers as [SD-WAN devices](#), but don't perform the last step to Commit.
- STEP 3** | In Panorama, select **Panorama > Managed Devices > Summary**.
- STEP 4** | At the bottom of the screen, select **Group HA Peers**. Confirm that under the Status display, the HA Status column includes the two firewalls, one Active and one Passive. Panorama is aware of the HA status and will push the same SD-WAN configuration to the two HA peers when you commit.
- STEP 5** | **Commit** and **Commit and Push**.

Create a VPN Cluster

In your SD-WAN configuration, you must configure one or more VPN clusters to determine which branches communicate with which hubs and creates a secure connection between the branch and hub devices. VPN clusters are logical groupings of devices, so consider things such as geographical location or function when logically grouping your devices.

PAN-OS® 9.1.0 supports only Hub-Spoke SD-WAN VPN topology. In a Hub Spoke topology, a centralized firewall hub at a primary office or location acts as the gateway between branch devices. The hub to branch connection is a VPN tunnel. In this configuration, traffic between branches must pass through the hub.



Full Mesh SD-WAN VPN topology is not supported in PAN-OS 9.1.0.

The first time you [Configure a Virtual SD-WAN Interface](#) with direct internet access (DIA) links for an SD-WAN hub or branch firewall, a VPN cluster called `autogen_hubs_cluster` is automatically created and the SD-WAN firewall is automatically added to the VPN cluster. This allows the Panorama™ management server to [Monitor SD-WAN Application and Link Performance](#) for devices that are protected by the SD-WAN firewall and accessing resources outside of your corporate network. Additionally, any SD-WAN firewall with DIA links that you configure in the future are automatically added to the `autogen_hubs_cluster` VPN cluster containing all hubs and branches with DIA links to allow Panorama to monitor application and link performance. The `autogen_hubs_cluster` is purely for monitoring application and link health, and not to create VPN tunnels between the hubs and branches with DIA links. If you need to connect hubs and branches together with VPN tunnels, you need to create a new VPN cluster and add all the required hubs and branches to that cluster.

STEP 1 | Plan your branch and hub VPN topology to determine which branches communicate with each of your hubs. For more information, see [Plan Your SD-WAN Configuration](#).

STEP 2 | Log in to the [Panorama Web Interface](#).

STEP 3 | Configure the VPN cluster. Repeat this step to create VPN clusters as needed.

1. Select **Panorama > SD-WAN > VPN Clusters** and **Add** a VPN cluster.
2. Enter a descriptive name for the VPN cluster.



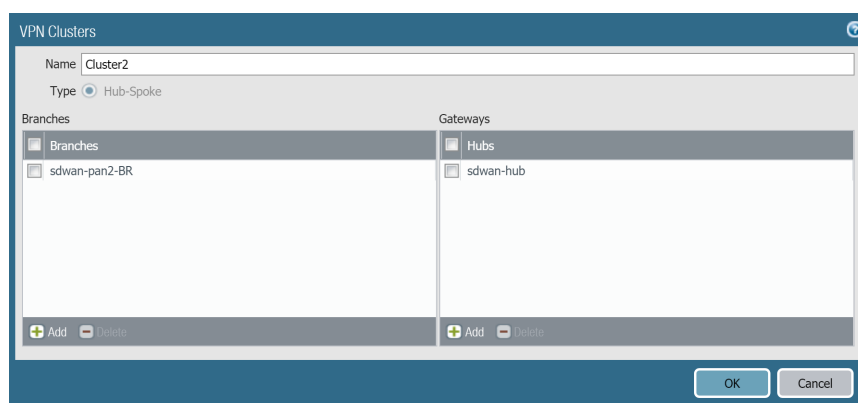
Underscores are not supported in the VPN cluster name. Choose the name of the VPN cluster carefully so you do not need to change the name in the future. SD-WAN monitoring data is generated based on the old cluster name and cannot be reconciled to a new cluster name, and will cause issues with the number of reported clusters when monitoring your VPN clusters or generating reports.

3. Select the VPN cluster Type.



Only Hub Spoke VPN cluster type is supported in PAN-OS 9.1.0.

4. **Add** one or more branch devices that you determined need to communicate with each other.
5. **Add** one or more hub devices that you determined need to communicate with the branch devices. If more than one hub device is added, you must use route metrics to control which hub is the primary and which is the secondary.
6. Click **OK** to save your configuration changes.



STEP 4 | Commit your configuration changes.

STEP 5 | Select Push to Devices to push your configuration changes to your managed firewalls.



*When Panorama creates virtual SD-WAN interfaces for hubs, Panorama doesn't necessarily create the interfaces using contiguous interface numbers. It might randomly skip an interface number, for example, sdwan.921, sdwan.922, sdwan.924, sdwan.925. Despite the discontinuous numbering, Panorama creates the correct number of SD-WAN interfaces. Use the operational CLI command **show interface sdwan?** to see the SD-WAN interfaces.*

Create a Static Route for SD-WAN

In addition to (or as an alternative to) BGP routing, you can create static routes to route your SD-WAN traffic.

You can configure static routes either using Panorama™ or directly on the firewall hub or branch. If you are going to use Panorama, you should be familiar with the process to [Configure a Template or Template Stack Variable](#). You will create a variable to use as the destination in your static route, as shown in the following procedure. You will push a static route (that goes to the hub) to the branch. You will push a static route (that goes to the branch) to the hub.

STEP 1 | [Log in to the Panorama Web Interface](#).

STEP 2 | [Configure a Template or Template Stack Variable](#) and enter the variable **Name** in the following format: **\$*peerhostname*_*clustername*.*customname***. For example, **\$branchsanjose_clusterca.10** or **\$DIA_cluster2.location3**. After the dollar sign (\$), the elements in the variable are:

- *peerhostname*—Hostname of the destination hub or branch to which the static route goes. For a static route to the internet, the peerhostname must be **DIA**. An alternative to the peer's hostname is to use the peer's serial number. If the peer is part of an HA pair, you can use the hostname or serial number of either one of the two HA firewalls.
- *clustername*—Name of the VPN cluster to which the destination hub or branch belongs.
- *customname*—Text string of your choice; you cannot use a period (.) in the customname.

You can have more than one static route going to the same peer, which means the variables will have the same peerhostname and clustername; you differentiate the variables by using a different customname.

STEP 3 | Select the variable **Type** to be **Interface**.

STEP 4 | Click **OK** to save the variable.

STEP 5 | Select **Network > Virtual Routers** and select a virtual router.

STEP 6 | Select **Static Routes > IPv4** and **Add a Name** for the static route.

STEP 7 | For **Destination**, select the variable you created.

STEP 8 | For **Interface**, select **sd_wan**.

STEP 9 | For **Next Hop**, select **IP Address** and enter the IP address of the next hop for the static route (the hub or branch to which the static route goes).

STEP 10 | Click **OK**.

STEP 11 | **Commit** and **Commit and Push** your changes.

Auto VPN configuration replaces the **sd_wan** keyword in the Interface field of the static route with the egress virtual SD-WAN interface that it determines based on the Destination variable. Thus, the static route in the routing table indicates that traffic going to the peer host in the identified VPN cluster will egress the virtual SD-WAN interface to reach the specified next hop.

STEP 12 | Configure a static route for the return traffic.

Monitoring and Reporting

Monitor and generate reports of the application and link health status in your VPN clusters to identify and resolve issues. In order for Panorama to display SD-WAN application and link health information, you must enable the SD-WAN firewalls to push device monitoring data to Panorama and configure log forwarding to Panorama when you Add Your SD-WAN Firewalls as Managed Devices. If you have not configured your SD-WAN firewalls to forward logs to Panorama, the SD-WAN **Monitoring** displays no application or link health information.

- > Monitor SD-WAN Application and Link Performance
- > Troubleshoot App Performance
- > Troubleshoot Link Performance
- > Generate an SD-WAN Report

Monitor SD-WAN Application and Link Performance

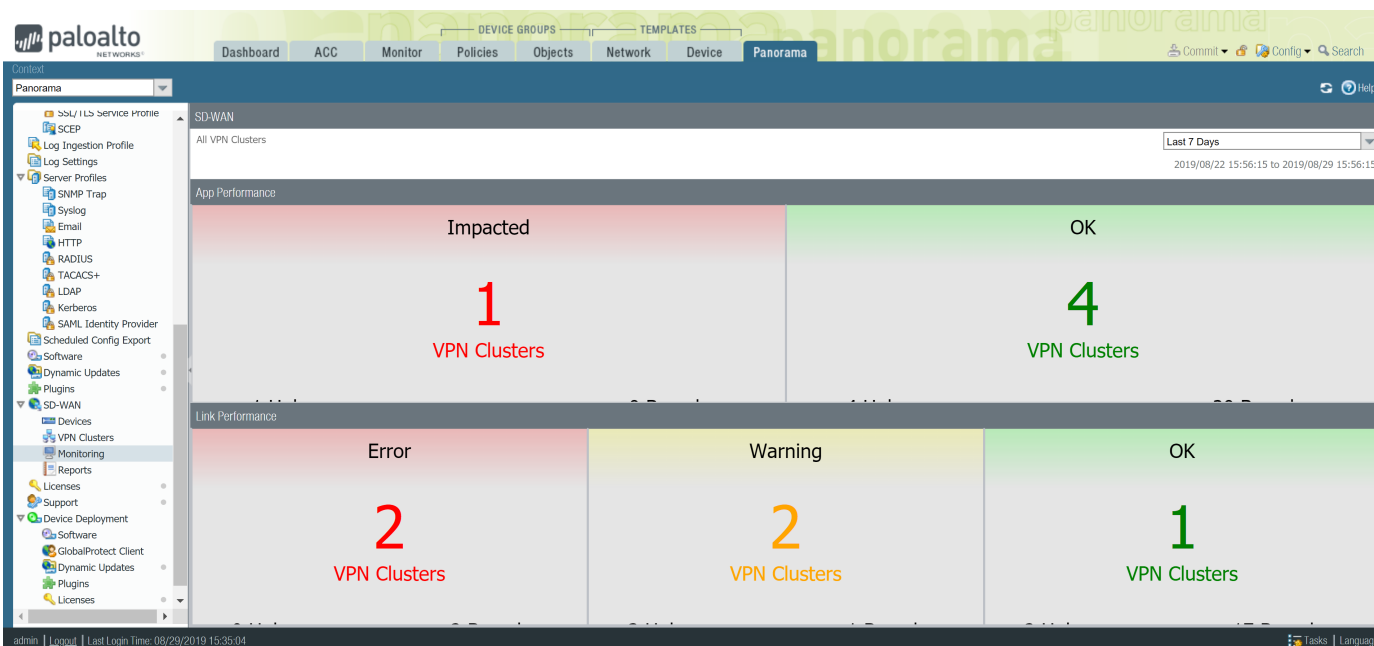
Monitor the application and link performance in your VPN clusters to troubleshoot issues by viewing summary information across all VPN clusters and then successively drilling down to isolate the issues to affected sites, applications, and links. The landing dashboard displays:

- App Performance
 - **Impacted**—One or more applications in the VPN cluster for which none of the paths have jitter, latency, or packet loss performance that meet the specified thresholds in the Path Quality Profile in the list of paths from which the firewall can choose.
 - **OK**—Number of VPN clusters, hubs, and branches that are experiencing no jitter, latency, or packet loss performance issues.
- Link Performance
 - **Error**—One or more sites in the VPN cluster have connectivity issues such as when a tunnel or a virtual interface (VIF) is down.
 - **Warning**—Number of VPN clusters, hubs, and branches that have links with jitter, latency, or packet loss performance measurements that exceed the moving seven-day average value of the metric.
 - **OK**—Number of VPN clusters, hubs, and branches that are experiencing no jitter, latency, or packet loss performance issues.

From the landing dashboard, narrow the view to impacted applications or links that have the Error or Warning status. Then select an affected site to view site-level details. From the site, view application-level or link-level details.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Panorama > SD-WAN > Monitoring** to view at-a-glance health status summaries of your VPN clusters, hubs, and branches.



STEP 3 | Click an App Performance or Link Performance summary that indicates Impacted, Error, or Warning counts to view a detailed list of sites and their status based on latency, jitter, and packet loss.

The screenshot displays the Palo Alto Networks SD-WAN Administrator's Guide interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, Device, and Panorama. The left sidebar contains a list of configuration and monitoring options. The main content area shows the SD-WAN configuration page, specifically the Link Performance - Error summary for VPN Clusters. The table below lists the sites and their status based on latency, jitter, and packet loss.

Sites	VPN Cluster	Profile	Links	Link Notifications	Latency	Jitter	Packet Loss	Apps	Impacted Apps
cluster-1-site-4	cluster-1	branch	4	0	OK	OK	OK	13	0
cluster-1-site-5	cluster-1	branch	4	0	OK	OK	OK	13	0
cluster-3-site-1	cluster-3	hub	4	0	OK	Warning	OK	13	0
cluster-1-site-2	cluster-1	branch	4	338	OK	OK	OK	13	0
cluster-1-site-3	cluster-1	branch	4	0	OK	OK	OK	13	0
cluster-1-site-1	cluster-1	hub	4	0	OK	OK	OK	13	13
cluster-3-site-4	cluster-3	branch	4	0	OK	OK	OK	13	0
cluster-3-site-5	cluster-3	branch	4	0	OK	OK	OK	13	0
cluster-3-site-2	cluster-3	branch	4	310	OK	Warning	OK	13	0
cluster-3-site-3	cluster-3	branch	4	0	OK	OK	OK	13	0

STEP 4 | Click a site that displays Warning or Error to see one VPN cluster. The site data display App Performance and Link Performance, including the impacted applications. Additionally, use the Sites filter to view VPN clusters based on link notifications, latency deviations, jitter deviations, packet loss deviations, or impacted applications.

STEP 5 | On the App Performance or Link Performance window, click **PDF/CSV** to export the detailed health information for the application or link in the VPN cluster in PDF or CSV format.

STEP 6 | Click the branch or hub that has an application that needs attention.

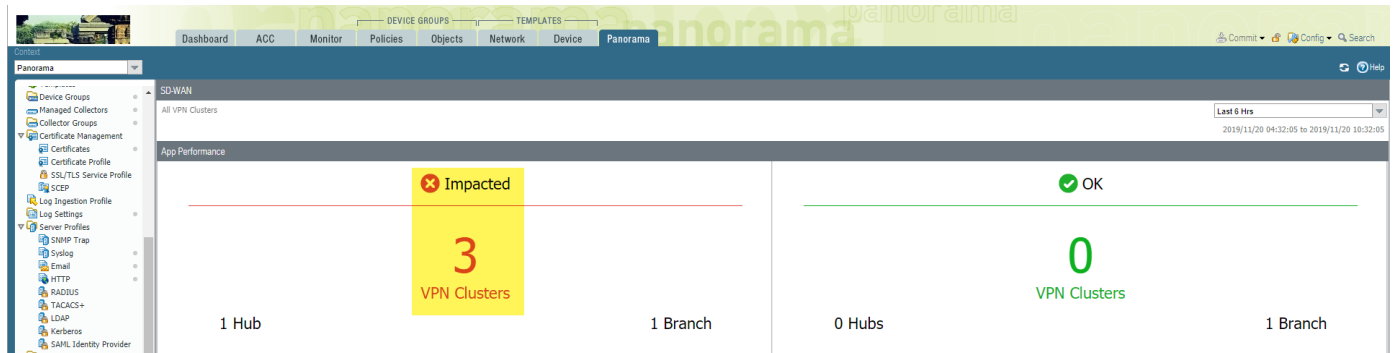
STEP 7 | Click an impacted application to view application-level or link-level details.

Troubleshoot App Performance

Understanding what is causing degraded performance for your apps and services is integral to ensuring the user experience is not impacted. Understanding why your VPN clusters are impacted and application traffic failed over to different links helps in fine tuning your SD-WAN configuration.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Panorama > SD-WAN > Monitoring** and view the **Impacted VPN** clusters.



STEP 3 | Filter the VPN clusters based on your preferred metric from the **Site** drop-down and select time frame. In this example, we are viewing **All Sites** containing impacted VPN clusters in the last 12 hours.

The screenshot shows the Panorama SD-WAN Monitoring interface with a table of impacted VPN clusters. The table is filtered by 'All Sites' and 'Last 12 Hrs'. The table has columns for Sites, VPN Cluster, Profile, Links, Link Notifications, Latency, Jitter, Packet Loss, Apps, and Impacted Apps. The data is as follows:

Sites	VPN Cluster	Profile	Links	Link Notifications	Latency	Jitter	Packet Loss	Apps	Impacted Apps
Hub1	Cluster2	hub	3	6	Warning	Warning	Warning	2	1
Hub1	Cluster1	hub	3	5	Warning	Warning	Warning	1	1
branch2	Cluster2	branch	6	2	Warning	Warning	Warning	4	1
Branch1	Cluster1	branch	6	6	Warning	Warning	Warning	249	190
Hub1	autogen_hubs_cluster	hub	1	No Data	Warning	Warning	Warning	246	246

STEP 4 | In the Sites column, select the impacted hub or branch firewall to view the impacted apps and the corresponding link performance.

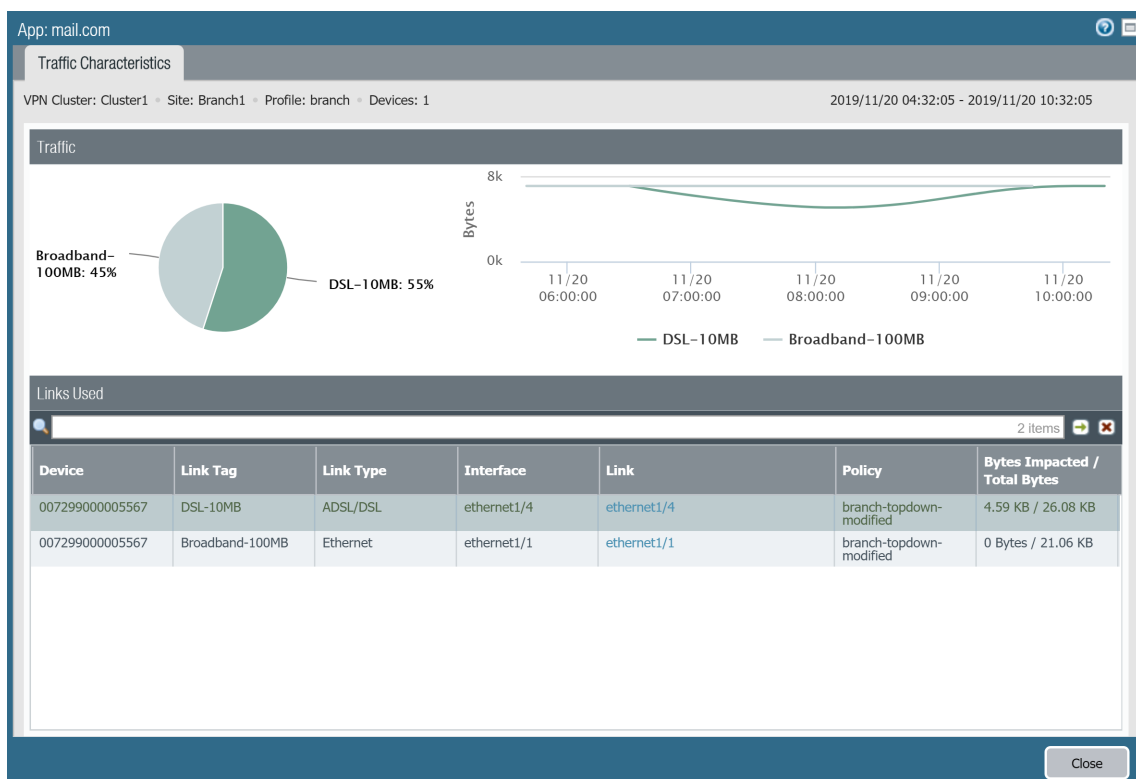
The screenshot displays the Palo Alto Networks Panorama interface, specifically the SD-WAN App Performance section. The left sidebar contains navigation options like Device Groups, Policies, Objects, Network, and Device. The main content area shows a table of application performance metrics for various apps. Below this is a Link Performance table showing details for different links and interfaces.

App	SD-WAN Policies	App Health	Bytes	Impacted Sessions / Total Sessions	Link Tags
lotuslive-base	branch-topdown-modified	Impacted	793.41 KB	16 / 157	Broadband-100MB
mail.com	branch-topdown-modified	Impacted	47.77 KB	1 / 14	DSL-10MB
mail.ru-base	branch-topdown-modified	Impacted	392.03 KB	10 / 117	Broadband-100MB
mail.ru-moimir	branch-topdown-modified	OK	5.71 KB	0 / 4	DSL-10MB
meetup-base	branch-topdown-modified	Impacted	106.72 KB	4 / 22	Broadband-100MB
megaproxy	branch-topdown-modified	Impacted	115.42 KB	2 / 14	DSL-10MB

Device	Link Tag	Link Type	Interface	Link	Link Notifications	Latency	Jitter	Packet Loss
sdwan-branch	LTE-50MB	Fiber	ethernet1/3	t_0103_007299000005568_0101	2	OK	Warning	OK
sdwan-branch	DSL-10MB	ADSL/DSL	ethernet1/4	ethernet1/4	No Data	Warning	Warning	OK
sdwan-branch	Broadband-100MB	Ethernet	ethernet1/1	ethernet1/1	No Data	OK	OK	OK
sdwan-branch	LTE-50MB	Fiber	ethernet1/3	ethernet1/3	No Data	OK	Warning	OK
sdwan-branch	Broadband-100MB	Ethernet	ethernet1/1	t_0101_007299000005568_0101	2	OK	OK	OK
sdwan-branch	DSL-10MB	ADSL/DSL	ethernet1/4	t_0104_007299000005568_0101	2	Warning	Warning	OK

STEP 5 | In the App Performance section, click an app to view detailed Traffic Characteristic information about the app traffic such as the internet service(s) and links used:

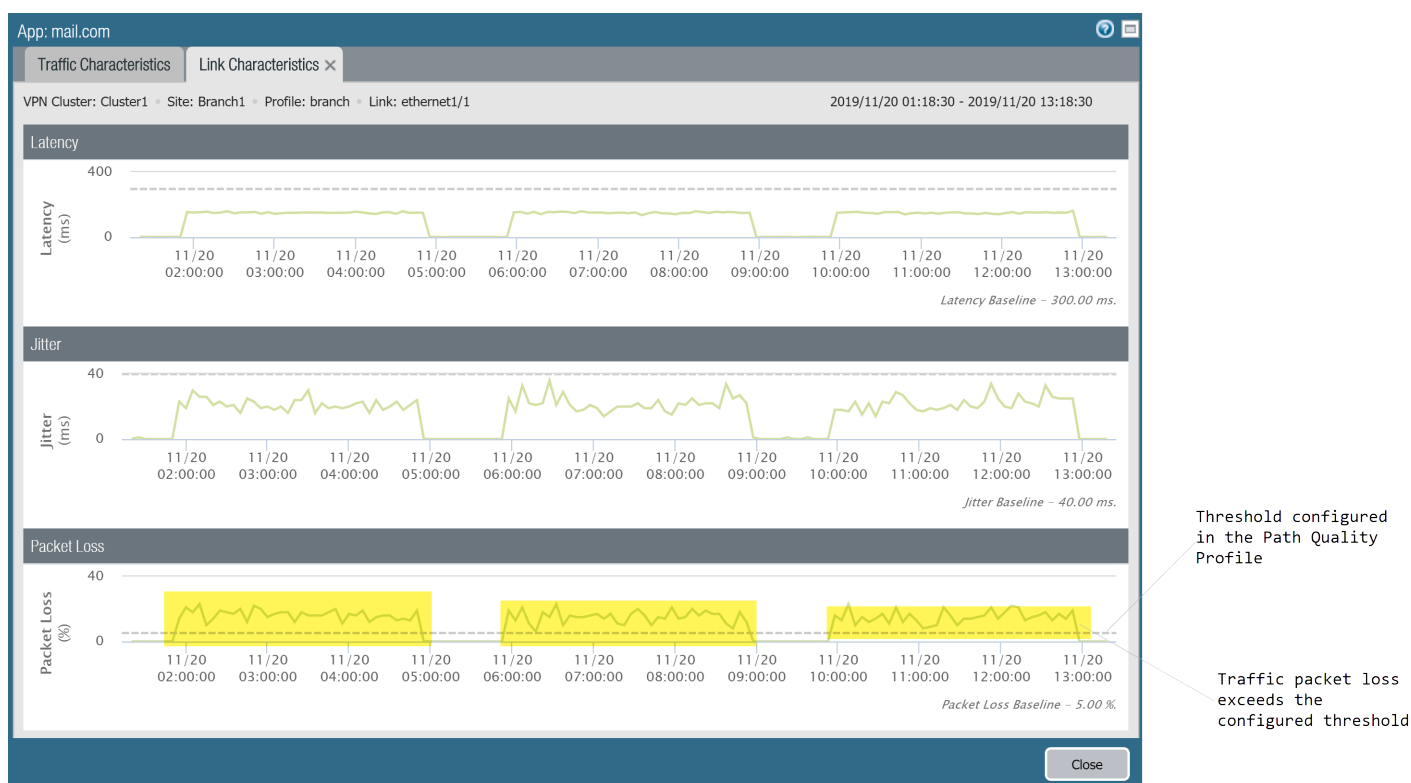
- Review the pie chart to understand the breakdown of app traffic across the your internet services.
- Review the linegraph to understand how many bytes of data were transferred over each internet service over time.
- Review the Links Used section to understand which links the app traffic used and to understand how many of the bytes were impacted out of the total bytes in the selected time frame.



STEP 6 | Investigate which health metric caused the app to swap links.

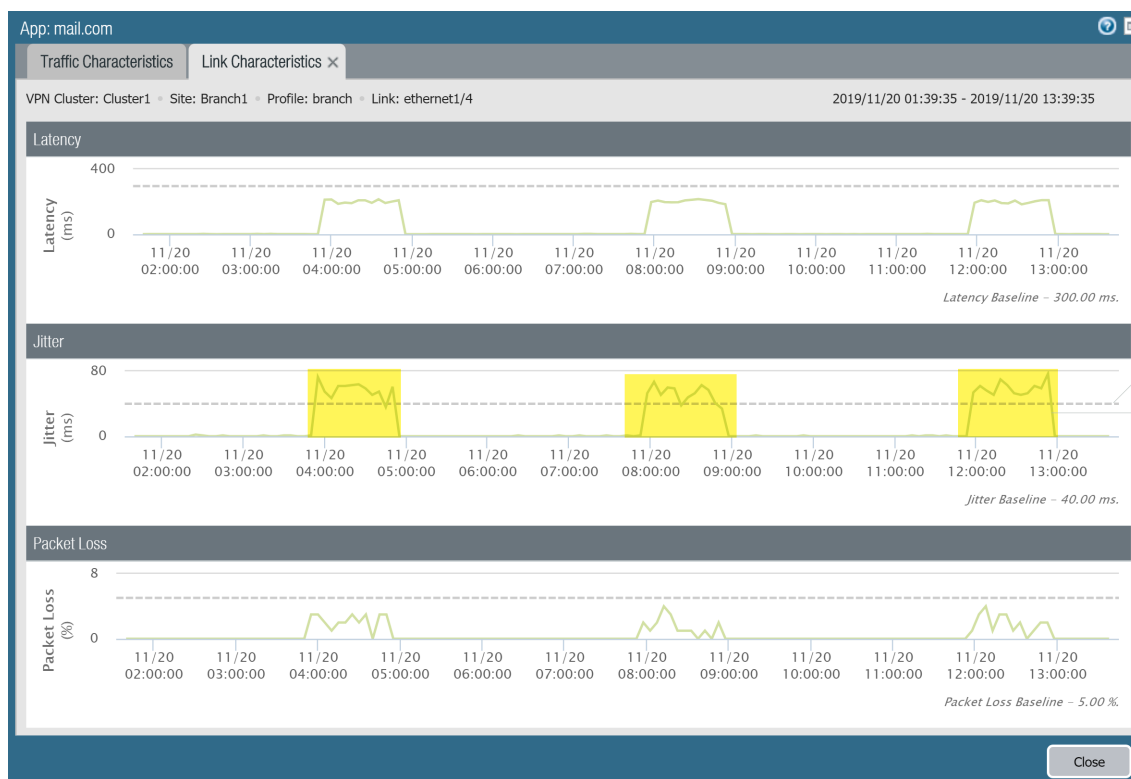
The dotted line indicates the threshold you configure when you [Create a Path Quality Profile](#).

1. In the Links Used section of the Traffic Characteristics tab, click an ethernet Link to view detailed Link Characteristics (latency, jitter, and packet loss) over the time frame specified in Step 2 to investigate what health metric caused the app to swap links. In this example, we are viewing ethernet 1/1 and can see that the percentage of packets lost regularly exceeded the configured threshold in the Path Quality Profile for the app and can conclude that this is the reason the app traffic failed over to the next best link.



2. In the **Traffic Characteristics** tab, select another link to view the Link Characteristics. In this example, we are viewing ethernet 1/4 and can see that after the app traffic failed over, ethernet 1/4 experienced jitter for the app that exceeded the configured threshold. This forced the app traffic to fail over back to ethernet 1/1.

Since both links had health metrics that were exceeded, the app traffic had no healthy link to fail over to resulting in the VPN cluster becoming impacted.



STEP 7 | After you have identified why the app traffic is impacted, consider the following to resolve the issue:

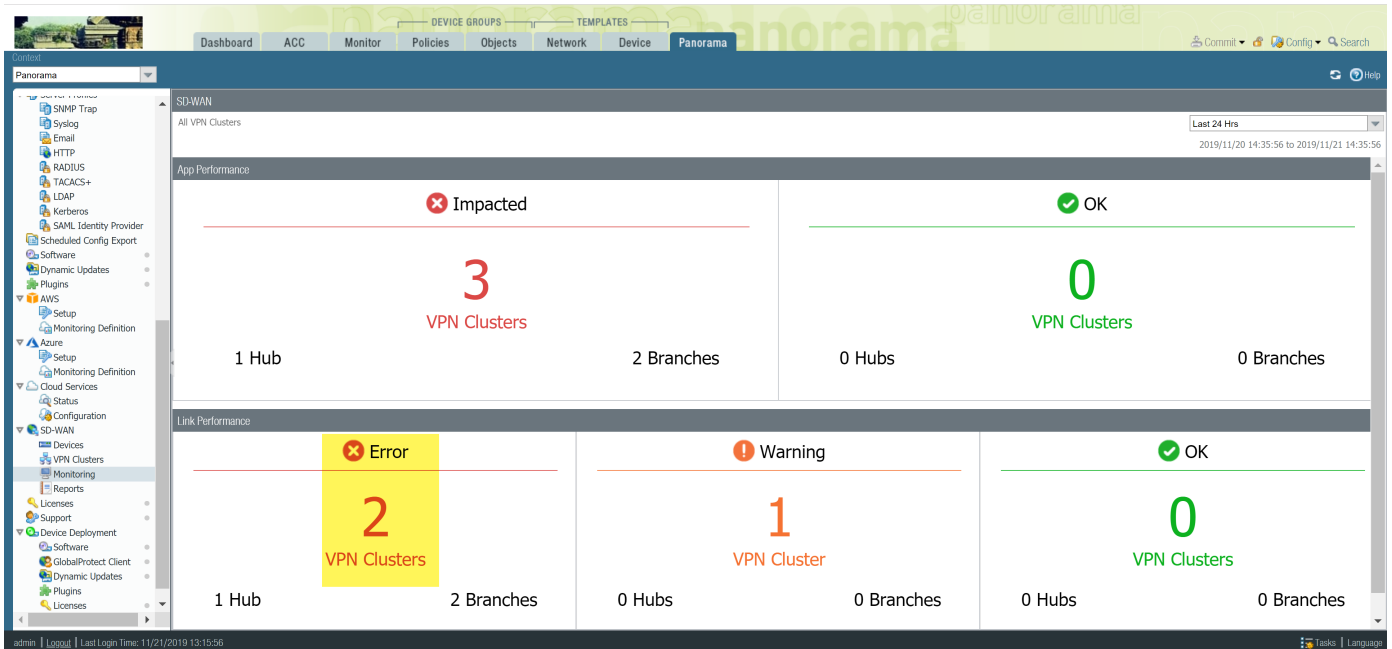
- Consider adding additional links to the [Traffic Distribution Profile](#). By adding additional links for app traffic to fail over to, you help ensure that the app traffic and user experience are not impacted by links with degraded health.
- Reconfigure the health thresholds in your [Path Quality Profile](#). It may be that the health thresholds are too strict, resulting in unnecessary link fail over. For example, if you have an app that can experience up to 18% packet loss before user experience is impacted, having a 10% packet loss threshold would result in the app failing over to a different link without a need to.
- Consult your internet service provider (ISP) to determine if there are impacts to your network outside of your control that they can resolve.

Troubleshoot Link Performance

Understanding what is causing degraded link performance is integral for ensuring the user experience when using apps and services is not impacted. Understanding why your VPN clusters have links that are impacted helps in fine tuning your SD-WAN configuration to ensure that the user experiences when using apps and services are not affected by links with degraded health.

STEP 1 | Log in to the Panorama Web Interface.

STEP 2 | Select **Panorama > SD-WAN > Monitoring** and view the **Impacted VPN** clusters.



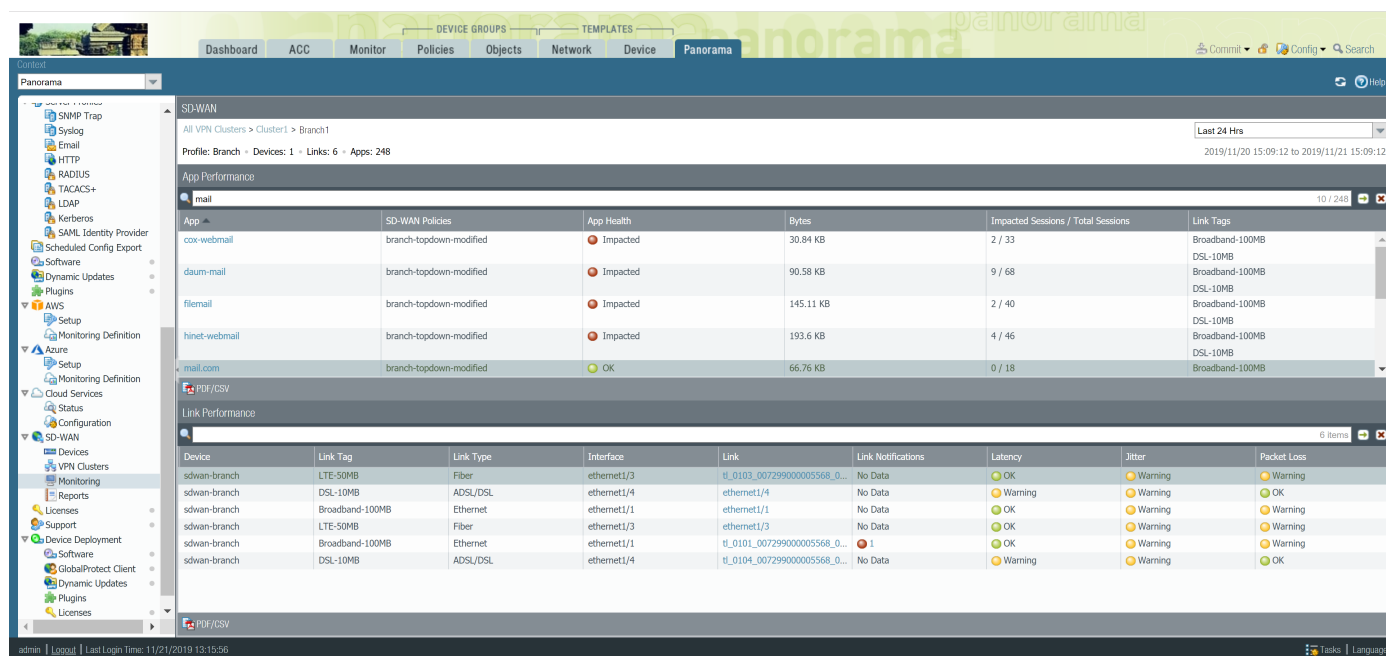
STEP 3 | Filter the VPN clusters based on your preferred metric from the **Site** drop-down and select time frame. In the Sites column, select the impacted hub or branch firewall to view the impacted apps and the corresponding link performance.

In this example, we are viewing **All Sites** containing impacted VPN clusters in the last 24 hours.

The screenshot shows the Panorama SD-WAN Monitoring interface with a table of impacted VPN clusters. The table has columns for Sites, VPN Cluster, Profile, Links, Link Notifications, Latency, Jitter, Packet Loss, Apps, and Impacted Apps. The data is filtered by 'Link Performance - Error' and 'All Sites'.

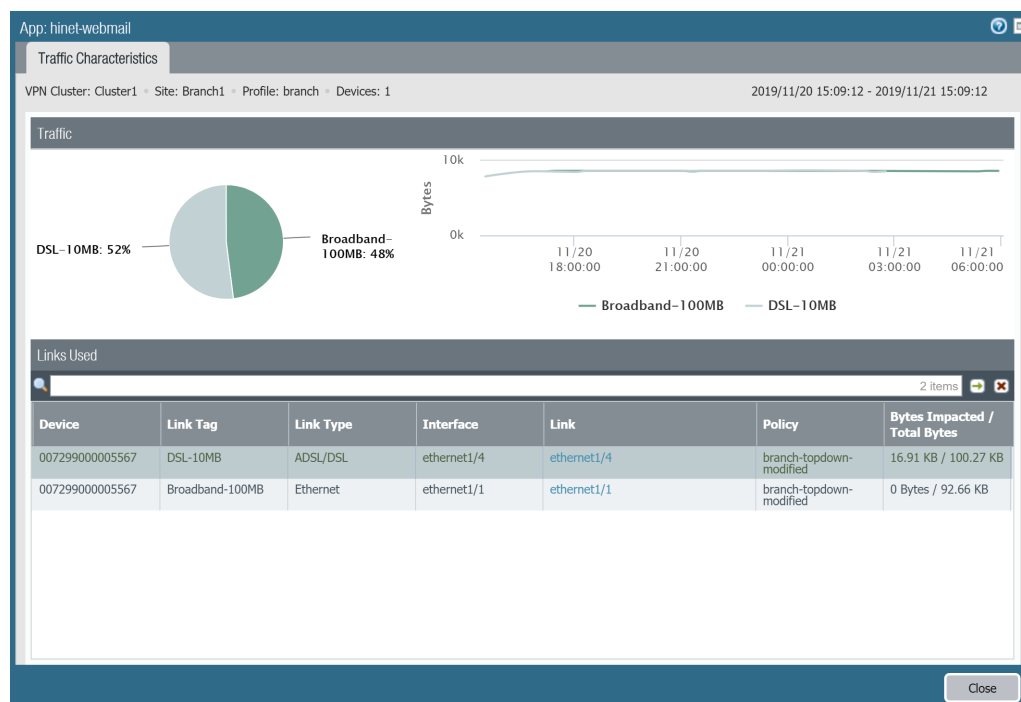
Sites	VPN Cluster	Profile	Links	Link Notifications	Latency	Jitter	Packet Loss	Apps	Impacted Apps
Hub1	Cluster2	hub	3	4	Warning	Warning	Warning	1	1
branch2	Cluster2	branch	6	4	Warning	Warning	Warning	3	1
Branch1	Cluster1	branch	6	1	Warning	Warning	Warning	248	212
Hub1	Cluster1	hub	3	2	Warning	Warning	Warning	1	1

STEP 4 | In the Sites column, select the impacted hub or branch firewall to view the impacted apps and the corresponding link performance.



STEP 5 | In the App Performance section, click an app to view detailed Traffic Characteristic information about the app traffic such as the internet service(s) and links used:

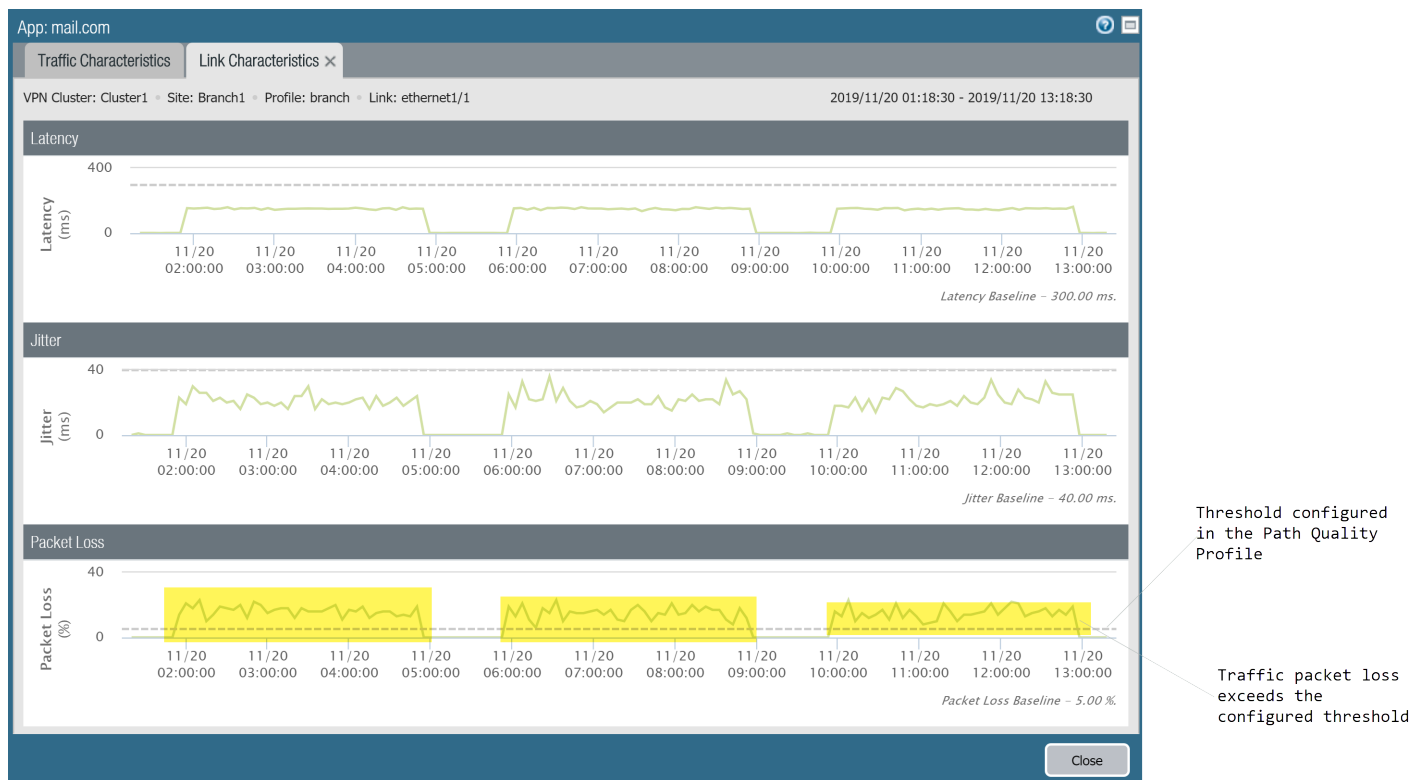
- Review the pie chart to understand the breakdown of app traffic across the your internet services.
- Review the linegraph to understand how many bytes of data were transferred over each internet service over time.
- Review the Links Used section to understand which links the app traffic used and to understand how many of the bytes were impacted out of the total bytes in the selected time frame.



STEP 6 | Investigate which health metric caused the app to swap links.

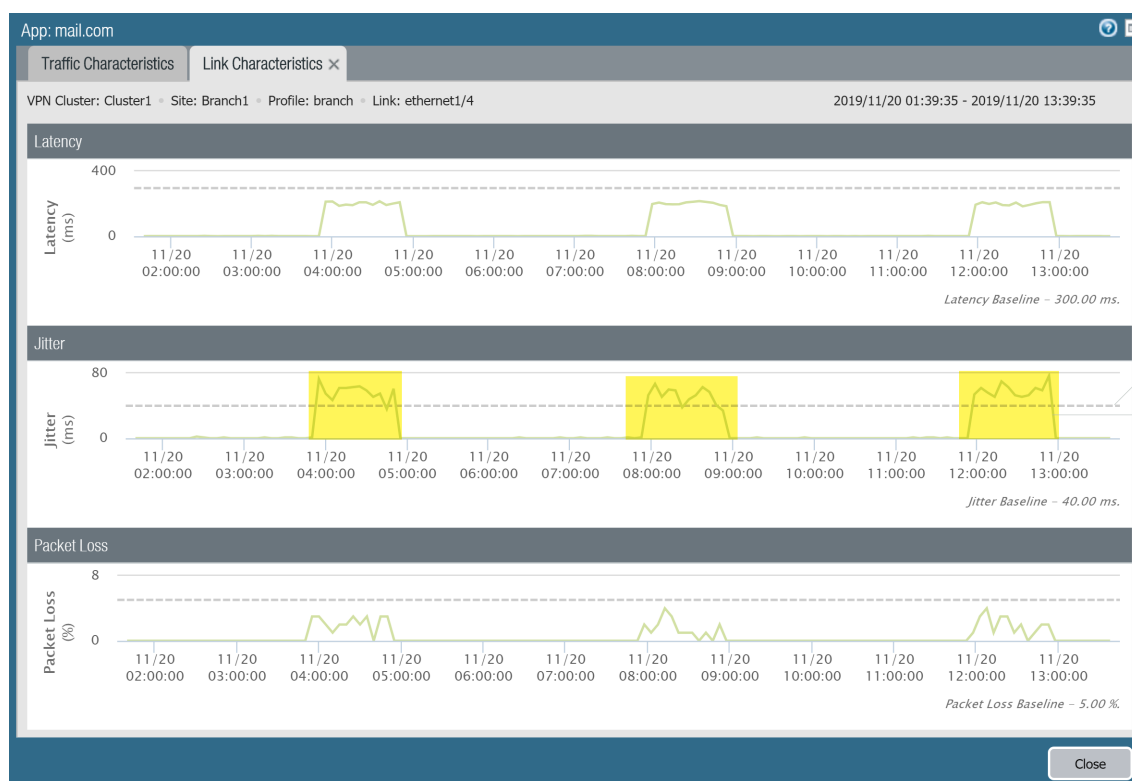
The dotted line indicates the threshold you configure when you [Create a Path Quality Profile](#).

1. In the Links Used section of the Traffic Characteristics tab, click an ethernet Link to view detailed Link Characteristics (latency, jitter, and packet loss) over the time frame specified in Step 2 to investigate what health metric caused the app to swap links. In this example, we are viewing ethernet 1/1 and can see that the percentage of packets lost regularly exceeded the configured threshold in the Path Quality Profile for the app and can conclude that this is the reason the app traffic failed over to the next best link.



2. In the **Traffic Characteristics** tab, select another link to view the Link Characteristics. In this example, we are viewing ethernet 1/4 and can see that after the app traffic failed over, ethernet 1/4 experienced jitter for the app that exceeded the configured threshold. This forced the app traffic to fail over back to ethernet 1/1.

Since both links had health metrics that were exceeded, the app traffic had no healthy link to fail over to resulting in the VPN cluster becoming impacted.



STEP 7 | After you have identified why the app traffic is impacted, consider the following to resolve the issue:

- Consider adding additional links to the [Traffic Distribution Profile](#). By adding additional links for app traffic to fail over to, you help ensure that the app traffic and user experience are not impacted by links with degraded health.
- Reconfigure the health thresholds in your [Path Quality Profile](#). It may be that the health thresholds are too strict, resulting in unnecessary link fail over. For example, if you have an app that can experience up to 18% packet loss before user experience is impacted, having a 10% packet loss threshold would result in the app failing over to a different link without a need to.
- Consult your internet service provider (ISP) to determine if there are impacts to your network outside of your control that they can resolve.

Generate an SD-WAN Report

Configure and generate an SD-WAN report detailing the top applications or links with the highest frequency of path quality degradation. The order application or links appear in a report is based on the amount of data impacted; the more data is impacted, the higher the application or link appears in the report. SD-WAN reports are generated as needed and cannot be scheduled. Use the SD-WAN reports to verify the correct application or link throughput, or ensure that application or link impact is not noticed by users. For example, if your ISP guaranteed a certain amount of throughput on a link, generate a Link Performance report for that link to verify that the guaranteed bandwidth is honored.

From the Panorama™ management server, you can only generate reports for applications or links across all SD-WAN enabled firewalls. To generate a report for applications or links processed by an individual firewall, you must create and generate the report locally on the firewall.

STEP 1 | Log in to the [Panorama web interface](#).

STEP 2 | Select **Panorama > SD-WAN > Reports** and **Add** a new report.

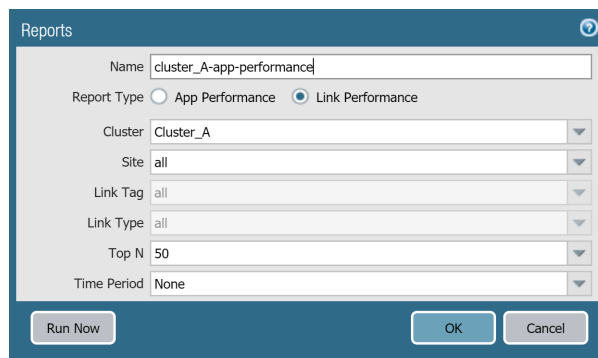
STEP 3 | Configure the SD-WAN report parameters.

1. Enter a descriptive **Name** for the report.
2. Choose the **Report Type** to generate:
 - Select **App Performance** to generate a report detailing only application health performance.
 - Select **Link Performance** to generate a report detailing only the link health performance.
3. Select the **VPN Cluster** for which to generate the report. By default, **all** is selected.
4. Select a **Site** within the selected VPN cluster for which to generate the report. By default, **all** is selected.

If you selected **all** Clusters then this field is grayed out and a Site cannot be selected.
5. (**App Performance only**) Select the **Application** for which to generate the report.

If you selected **all** Clusters and Sites then this field is grayed out and an individual application cannot be selected.
6. (**Link Performance only**) Select the **Link Tag** for which to generate the report. Selecting a link tag generates a report for all links in grouped using the tag in the cluster or site. By default, **all** is selected.
7. (**Link Performance only**) Select the **Link Type** for which to generate the report. Selecting a link type generates a report for all links of the specified type in the cluster or site. By default, **all** is selected.
8. Select the **Top N** applications or links to include in the report. This setting determines the number of applications or links experiencing health degradation to include in the report. By default, the report includes the top 5 applications or links experiencing health degradation.
9. Specify the **Time Period** within which to generate the report. By default, **None** is selected and queries the entire health status history of the applications or links.

STEP 4 | Click **Run Now** to generate the report.



The 'Reports' dialog box is shown with the following configuration:

- Name: cluster_A-app-performance
- Report Type: ☐ App Performance, ☒ Link Performance
- Cluster: Cluster_A
- Site: all
- Link Tag: all
- Link Type: all
- Top N: 50
- Time Period: None

Buttons at the bottom: Run Now, OK, Cancel.

STEP 5 | View the generated report and **Export XML** to export the report in XML format to your local device. When ready, click **Close**.



The 'Ad-hoc Link Report' window displays a table with the following structure:

Cluster	Site	Link Tag	Link Name	App			Time Under-performing (min)
				Name	Impacted/Total Data	Per App/Total %	
0 items							

Buttons at the bottom right: Export XML, Close.

STEP 6 | In the Reports pop-up, click **OK** to save your configured report.

STEP 7 | **Commit** > **Commit to Panorama** and **Commit** your changes.

Use the CLI

Use the Panorama™ management server Command Line Interface (CLI) to view SD-WAN information and perform operations.

- > Use CLI Commands for SD-WAN Tasks

Use CLI Commands for SD-WAN Tasks

Use the following CLI commands to view and clear SD-WAN information and view SD-WAN global counters. You can also view VPN tunnel information, BGP information, and SD-WAN interface information.

If you want to ...	Use ...
View or Clear SD-WAN Information	
<ul style="list-style-type: none">View path names and IDs for an SD-WAN interface, their state, local and peer IP addresses, and tunnel interface number.	<pre>> show sdwan connection all <sdwan-interface></pre>
<ul style="list-style-type: none">View the number and percentage of sessions distributed to each tunnel member of a virtual SD-WAN interface.	<pre>> show sdwan session distribution policy-name <sdwan-policy-name></pre>
<ul style="list-style-type: none">View the names of SD-WAN policy rules that send traffic to the specified virtual SD-WAN interface, along with the traffic distribution method, configured latency, jitter, and packet loss thresholds, link tags identified for the rule, and member tunnel interfaces.	<pre>> show sdwan rule interface sdwan.x</pre>
<ul style="list-style-type: none">View SD-WAN events such as path selection and path quality measurements.	<pre>> show sdwan event</pre>
<ul style="list-style-type: none">Clear SD-WAN events.	<pre>> clear sdwan event</pre>
<ul style="list-style-type: none">View latency, jitter, and packet loss on a virtual SD-WAN interface (specify interface number or name). Latency, jitter, and packet loss measurements are taken and averaged over three timeframes. Each timeframe has a health version, which increments when a health parameter value (that exceeds the threshold) changes. In addition to the real time measurement, there is a current use measurement, which displays the value of the parameter the last time the real-time value change exceeded the threshold.	<pre>> show sdwan path-monitor stats vif <sdwan.x></pre> <pre>> show sdwan path-monitor stats vif <sdwan-interface-name></pre>
<ul style="list-style-type: none">View the name of the SD-WAN policy rule that the specified session matches, the source and destination tunnel interfaces, the configured	<pre>> show sdwan session path-select session-id <session-id></pre>

If you want to ...	Use ...
latency, jitter, and packet loss percentage for the rule, and the traffic distribution method.	
<ul style="list-style-type: none"> View monitoring mode for the virtual SD-WAN link (Aggressive or Relaxed) and update intervals. 	<pre>> show sdwan path-monitor parameter path-name <sdwan-path-name></pre>
<ul style="list-style-type: none"> View monitoring mode for the virtual SD-WAN interface (Aggressive or Relaxed), update intervals, and probe statistics. 	<pre>> show sdwan path-monitor parameter vif <sdwan.x></pre>

View Global Counters to Troubleshoot SD-WAN

<ul style="list-style-type: none"> On a branch, verify that the number of SD-WAN probe Request packets transmitted equals the number of probe Reply packets received. On a branch firewall, most SD-WAN tunnels are the initiator, which means the tunnel will have SD-WAN path-monitor probing enabled. 	<pre>> show counter global filter delta yes</pre> <p>flow_sdwan_prob_req_tx flow_sdwan_prob_reply_rx</p>
<ul style="list-style-type: none"> On a hub, verify that the number of SD-WAN probe Request packets received equals the number of probe Reply packets transmitted. On a hub firewall, most SD-WAN tunnels are the responder, which means the tunnel will have SD-WAN path-monitor probing disabled. 	<pre>> show counter global filter delta yes</pre> <p>flow_sdwan_prob_req_rx flow_sdwan_prob_reply_tx</p>

View VPN Tunnel Information

<ul style="list-style-type: none"> View all tunnels created on firewall. 	<pre>> show vpn flow</pre>
<ul style="list-style-type: none"> View details of individual tunnels identified by name. 	<pre>> show vpn flow name <name></pre>
<ul style="list-style-type: none"> View details of individual tunnels identified by ID. 	<pre>> show vpn flow tunnel-id <tunnel-id></pre>
<ul style="list-style-type: none"> View Internet Key Exchange (IKE) Phase 1 and Phase 2 details for all tunnels. 	<pre>> show vpn ike-sa</pre>
<ul style="list-style-type: none"> View IKEv2 security associations (SAs) and IKEv2 IPSec child SAs of a specific gateway. 	<pre>> show vpn ike-sa gateway <gateway></pre>

If you want to ...	Use ...
<ul style="list-style-type: none"> View tunnel details. 	<pre>> show vpn tunnel</pre>
View BGP Information	
<ul style="list-style-type: none"> View BGP summary for a virtual router. 	<pre>> show routing protocol bgp summary virtual-router <virtual-router></pre>
<ul style="list-style-type: none"> View BGP peer summary. 	<pre>> show routing protocol bgp peer peer-name <peer-name> virtual-router <virtual-router></pre>
<ul style="list-style-type: none"> View summary of local routing information base (RIB). 	<pre>> show routing protocol bgp loc-rib</pre>
View SD-WAN Interface Information among RIB and FIB	
<ul style="list-style-type: none"> View new SD-WAN egress interface. 	<pre>> show routing route</pre>
<ul style="list-style-type: none"> View SD-WAN interfaces in forwarding information base (FIB). 	<pre>> show routing fib</pre>

