Configure SD-WAN Traffic Steering

For supported software information, click here.

When a Versa Operating System^{TM} (VOS^{TM}) device in a branch has two or more WAN links, you can configure Layer 2 and Layer 3 SD-WAN traffic steering to direct outgoing traffic flows to the desired WAN link. To identify the traffic, you create a policy that matches the desired traffic. Note that you can configure Layer 2 SD-WAN traffic steering for Releases 21.2.1 and later.

To steer the traffic, you do the following:

- Create a forwarding profile that defines the WAN links to which to direct outgoing traffic.
- Create an SLA profile that defines the link-performance parameters to consider when making the final decision which WAN link to use to forward outgoing traffic.
- Associate the forwarding profile and the SLA profile with a Layer 2 or Layer 3 SD-WAN policy.

Creating the forwarding and SLA profiles and associating them with a policy form the basic components of SD-WAN traffic steering.

This article discusses how to create a forwarding profile and associate it with an SD-WAN policy. Configuring an SLA profile is optional and is described in Configure SLA Profiles for SD-WAN Traffic Steering.

When the procedures for creating a forwarding profile and associating it with an SD-WAN policy for Layer 2 and Layer 3 SD-WAN traffic steering are identical, this article presents a single procedure. When they differ slightly, this article presents separate procedures.

To allow an SD-WAN traffic-steering policy to correctly process all traffic in a flow, it uses application detection, which is always running on the VOS device, to inspect the first packet in a flow and to identify the Layer 7 application sending the flow. Application detection maintains a cache that contains entries for all the IP addresses that a domain name resolves to, and for all the applications and URL categories that are known for a domain.

In conjunction with the basic SD-WAN traffic-steering components, you can activate mean opinion score (MOS) score monitoring. The procedures for configuring MOS are described in Configure MOS Score Monitoring.

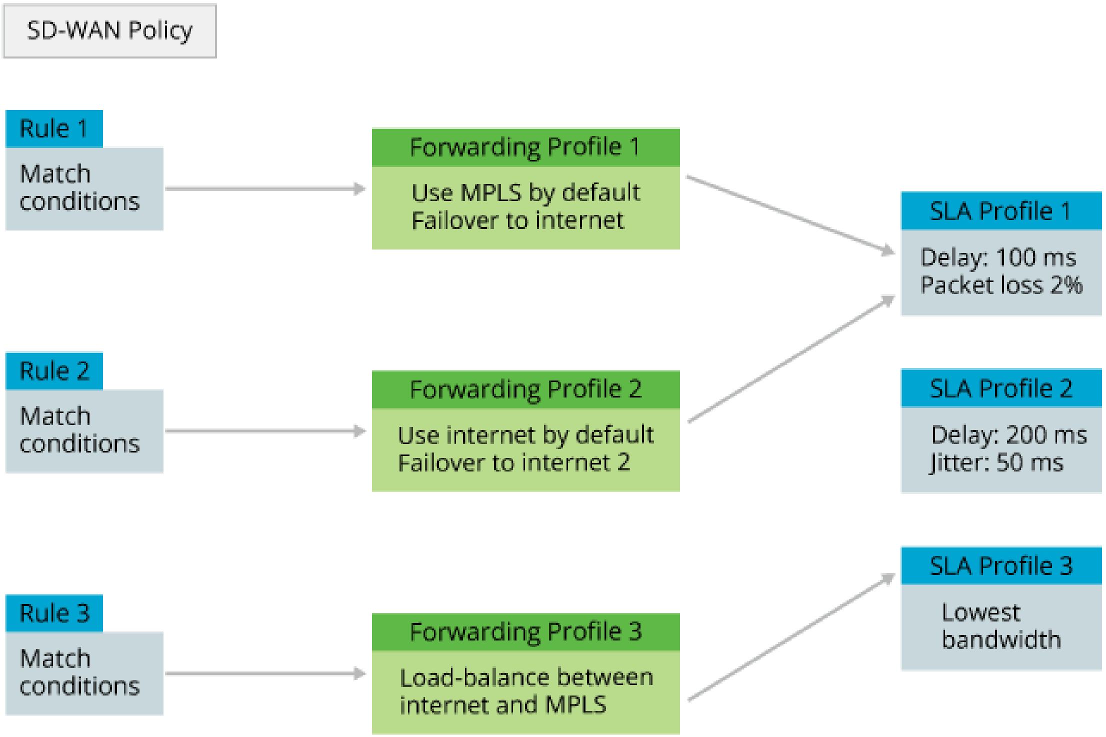
Advanced SD-WAN traffic steering components allow you to handle specific network situations. For Layer 2 SD-WAN traffic steering, the advanced components you can configure are SLA monitoring, data-driven SLA monitoring, forward error correction (FEC), packet replication, and path policies. For Layer 2 SD-WAN traffic steering, they are SLA monitoring, data-driven SLA monitoring, FEC, packet replication, and path policies. The procedures for configuring these features are provided in separate articles, which are listed in Additional Information, at the end of this article.

Traffic-Steering Policy Components

Traffic steering allows you to define how to direct traffic to a particular interface on a VOS device when that device has multiple WAN links. To do this, you create a traffic-steering policy, which consists of the following components:

- Polices and rules—Define criteria for matching packets and application traffic to transmit over one of the WAN links. For an SD-WAN traffic steering policy, you configure a standard SD-WAN policy. A policy consists of policy rules, which define the criteria for matching traffic and applications, and the enforcement action to take when a match does or does not occur. To have the policy apply to SD-WAN traffic steering, you associate a forwarding profile with the policy when you configure a policy rule's enforcement action.
- Forwarding profiles—Define parameters for how to direct matching traffic to the desired WAN link. Parameters include circuit and path priority, connection method, and load balancing. The next section describes some of the forwarding profile parameters.
  Note that in this article and in the VOS software options, WAN links are often referred to as *circuits*. While you configure circuit and path priority together, circuits and paths are different. A circuit is a WAN endpoint on a VOS branch device, and a path runs end to end from a local branch to a remote branch, in the process traversing a local circuit (that is, a local WAN endpoint) and a remote circuit (a remote WAN endpoint). For example, suppose Branch-1 and Branch-2 each have two WAN circuits, called Internet-1 and Internet-2. These circuits allow for four paths between Branch-1 and Branch-2:
    - Branch-1–Internet-1 → Branch-2–Internet-1
    - Branch-1–Internet-1 → Branch-2–Internet-2
    - Branch-1–Internet-2 → Branch-2–Internet-1
    - Branch-1–Internet-2 → Branch-2–Internet-2
- SLA profiles—Define the link-performance parameters to consider when making the final decision about which WAN link to use to forward outgoing traffic. The service-level agreement parameters include link latency, jitter, and packet loss.

The following figure illustrates the traffic steering policy components and how they work together. The left column shows an SD-WAN traffic-steering policy that has three rules. The rules are evaluated in order, from first to last. When the traffic matches a rule, the evaluation process stops, and the traffic is processed by the forwarding profile and then by an SLA profile, if one is configured.



From a configuration perspective, you configure the traffic-steering policy options in the reverse order. That is, first you configure an SLA profile, then a forwarding profile, and finally the SD-WAN traffic steering policy itself. You do this, because when you configure a forwarding profile, you associate an SLA profile with it, and when you configure the traffic-steering policy, you associate a forwarding profile with it.

Each traffic-steering policy is specific to an organization (that is, a tenant). This means that each tenant on a multitenant branch device can control their path selection behavior independently.

Forwarding Profile Parameters

You create forwarding profiles to control the behavior of the traffic passing over SD-WAN links. A forwarding profile defines circuit and path priorities, the connection method, load-balancing, and other capabilities to apply for any traffic that matches the rules you configure in the SD-WAN policy. You can associate a forwarding profile with an entire policy or with an individual rule within a policy. You can associate only one forwarding profile to an individual rule within a policy. You can associate a single forwarding profile with one or more SD-WAN policies or with one or more rules within a policy.

The following list describes some of the basic traffic behavior parameters that you can configure in a Layer 2 or a Layer 3 forwarding profile:

- Circuit priority—Define the preference for each WAN path between the local branch and a remote branch or branches. If the forwarding profile defines SLA requirements, new traffic flows on the circuit are sent on the WAN path with the highest priority that meets the SLA criteria. If a path does not meet the forwarding profile's SLA requirements, it is assigned the SLA-violated priority, which is a system-defined priority level just below the lowest configurable path priority, and the path-selection logic tries to find another path with a higher priority that complies with the SLA. You can configure circuits to avoid. For example, you might want to avoid sending non-critical traffic over a high-cost LTE circuit. You can configure a last-resort priority to select the path to use when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available.

- Encryption—By default, site-to-site traffic is sent over a secure tunnel on a WAN interface, which performs both encryption and authentication on all traffic. Encrypting traffic incurs an overhead that may be undesirable or unnecessary, for example, if the end hosts themselves use SSL to encrypt and authenticate traffic. In this case, you can disable encryption and send the traffic as plain text. To control the WAN access link encryption for an organization, you can modify the default encryption behavior in one of the following ways:
    - Modify the encryption for all traffic on a specific access circuit (path), as described in Configure Encryption on WAN Interfaces.
    - Modify the encryption for specific applications, as part of configuring SD-WAN traffic steering. Application-specific encryption behavior applies to traffic regardless of the path encryption.
- Load-balancing and connection selection method for SD-WAN traffic—By default, traffic is load-balanced per flow using weighted round-robin (WRR), and all packets for a given flow are sent over one path. Flows are load-balanced among the highest-priority SLA-compliant paths. You can configure per-packet load balancing, to load-balance the packets in a flow across all eligible paths. To choose the connection, you can use WRR, which balances flows onto paths proportional to their available bandwidth, or you can use the path that has the most available bandwidth. For Releases 21.2.1 and later, for Layer 3 SD-WAN traffic steering only, you can also configure path weighted round-robin and path high-available bandwidth. For these two methods, the traffic-steering software dynamically monitors and periodically computes the available path bandwidth across all paths towards the remote site, maintaining a historical maximum of the monitored available bandwidth for each path over a period of time, and then it load-balances the traffic across available paths using either WRR or the path that has the most available bandwidth. If you have not configured a bandwidth monitor, the software considers the configured uplink or downlink path bandwidth for traffic steering. Specifically, for the path uplink bandwidth, the software considers the local site's minimum uplink bandwidth and the remote site's minimum downlink bandwidth, and for the path downlink bandwidth, the software considers the local site's minimum downlink bandwidth and the remote site's minimum uplink bandwidth.
- Path evaluation—By default, each branch periodically evaluates its active forwarding profiles to determine which paths comply with the configured parameters. Normally, a traffic path is selected only in two circumstances, when a flow is created and when the path for a flow is determined to be down. For a new flow, the path is SLA-compliant when it is selected, and the path does not change even if it is no longer SLA-compliant. When a path for a traffic flow goes down, a new SLA-compliant path is calculated. This default behavior is recommended for most types of data traffic. For real-time applications, such as voice and video, you can enable continuous evaluation to move an existing flow to a better path when one becomes available. The path switching occurs at a configured recomputation interval. To control the fluctuations between a path being in an SLA-compliant and SLA-non-compliant state, you can configure SLA smoothing and SLA damping. To control how quickly flows are moved from a non-SLA-compliant path to an SLA-compliant path, you can configure gradual migration.
- Symmetric forwarding—Specify which path to use for reverse-direction traffic, that is, whether to send traffic returning from the destination branch to originating branch on the same path on which the traffic was received.

In a Layer 3 forwarding profile, you can also configure the following:

- Packet reordering—Reorder packets in a flow that arrive out of order, which might occur when you configure with per-packet load balancing and packet replication.
- Advanced traffic behavior parameters, including forward error correction (FEC) and packet replication.

Forwarding Profile Policy Evaluation

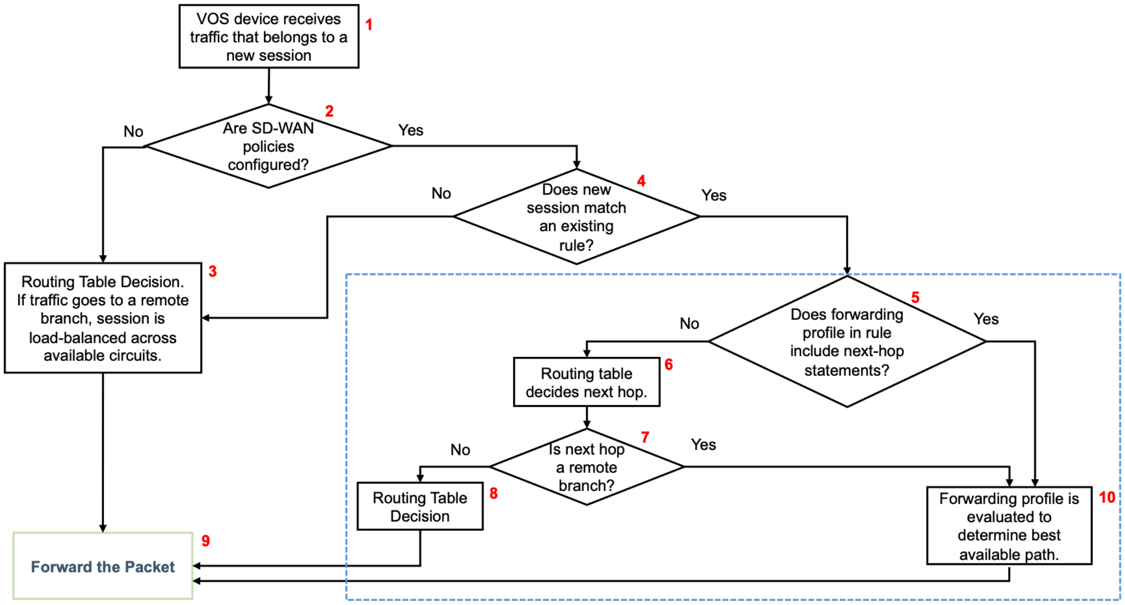
For Releases 20.1 and later.

To determine how to steer SD-WAN traffic, the policy evaluation process on a VOS device evaluates traffic on a per-session basis to determine how to route all traffic for the session. For each session, the policy evaluation process decides whether to use the routing table or to consult a configured SD-WAN policy. At a high level, the traffic-steering decision is straightforward, as illustrated in the flowchart in Figure 1. This flowchart shows the following:

- For traffic that is part of a new session (**1**), if no SD-WAN policies are configured on the VOS device (**2**), the traffic path is determined by consulting the routing table (**3**), and the traffic is forwarded (**9**).
- For traffic that is part of a new session (**1**), if SD-WAN policies are configured on the VOS device (**2**) and if the new session does not match a rule in the SD-WAN policy (**4**), the traffic path is determined by consulting the routing table (**3**), and the packets in the session are forwarded (**9**).
- For traffic that is part of a new session (**1**), if SD-WAN policies are configured on the VOS device (**2**) and if the new session matches a rule in the SD-WAN policy (**4**), how the traffic path is determined depends on the configuration in the forwarding profile (**blue** box). All steps in the blue box are a high-level summary of how the forwarding profile evaluates traffic. Figure 2 details the forwarding profile evaluation.

Forwarding decisions that are made apply to all traffic in a session, and they remain in effect for the duration of the session. The forwarding decisions change only when an event triggers a process to exit the session or when a new session is created.

Figure 1: General SD-WAN Traffic-Steering Flow


VOS device receives traffic that belongs to a new session
1
Are SD-WAN policies configured?
2
No
Yes
Does new session match an existing rule?
4
No
Yes
Routing Table Decision. If traffic goes to a remote branch, session is load-balanced across available circuits.
3
Does forwarding profile in rule include next-hop statements?
5
No
Yes
Routing table decides next hop.
6
Is next hop a remote branch?
7
No
Yes
Routing Table Decision
8
Forwarding profile is evaluated to determine best available path.
10
Forward the Packet
9

In a forwarding profile, the major choice of how to control traffic steering is whether to steer by circuit or by next hop. A circuit is a traffic path identified by media type, such as cable, DSL, Ethernet, LTE, T1, and T3, or a WAN interface, such as WAN1 and WAN2. A next hop is a traffic path identified by an IP address. You assign priority values to circuits and next hops, and in a general sense, the circuit or next hop with the highest priority is selected as the traffic path. The flowcharts in Figures 2, 3, and 4 illustrate how a VOS device makes circuit and next-hop traffic-steering decisions. Note that you can configure a number of other parameters to fine-tune the choice of circuit or next hop, and you can also configure other properties for steering traffic. These options are discussed in the forwarding profile configuration procedure later in this article.

Figure 2 details the traffic processing performed by the steps summarized in the blue box in Figure 1. The flowchart in Figure 2 describes what occurs if evaluation of a forwarding profile is triggered (**1** in Figure 2) because the traffic in a new session matches an existing rule (**4** in Figure 1). The flowchart in Figure 2 shows the following:

- If the forwarding profile configuration includes next hops (**2**), the VOS device checks whether any of the next hops are active.
    - The evaluation begins by looking for next hops whose priority value is 1, and if none are found, continuing with next hops that have lower priority values (**4** and **5** in the **green** box). All steps in the green box are a high-level summary of the next-hop evaluation process, which is detailed in Figure 3.
    - When an active next hop is identified (**5**), the policy evaluation process checks the routing table to determine whether the next hop is a remote branch (**9**).
    - If the next hop is not a remote branch, the session traffic is forwarded using the selected active next hop (**8** and **11**).
    - If the next hop is a remote branch (**9**), the VOS devices initiates the circuit selection process (**blue** box). All steps in the blue box are a high-level summary of the circuit evaluation process, which is detailed in Figure 4.
    - Session traffic is forwarded using the selected circuit or next hop (**11** and **12**).
- If the forwarding profile configuration does not include next hops (**2**), the policy evaluation process consults the routing table (**3**).
    - If the next hop is not a remote branch (**6**), the traffic path is determined from the routing table (**7**), and the packets in the session are forwarded (**11**).
    - If the next hop is a remote branch (**6**), the VOS devices initiates the circuit selection process (**blue** box). All steps in the blue box are a high-level summary of the circuit evaluation process. Figure 4 details this evaluation.
    - Session traffic is forwarded using the selected circuit or next hop (**11** and **12**).

Note that as part of the next-hop or circuit selection process, when multiple circuits or next hops are SLA-compliant and have the same priority (**purple** box), the VOS device load-balances session traffic among them using the load-balancing option in the forwarding profile. (The default option is weighted round-robin.)

Figure 2: Forwarding Profile Evaluation

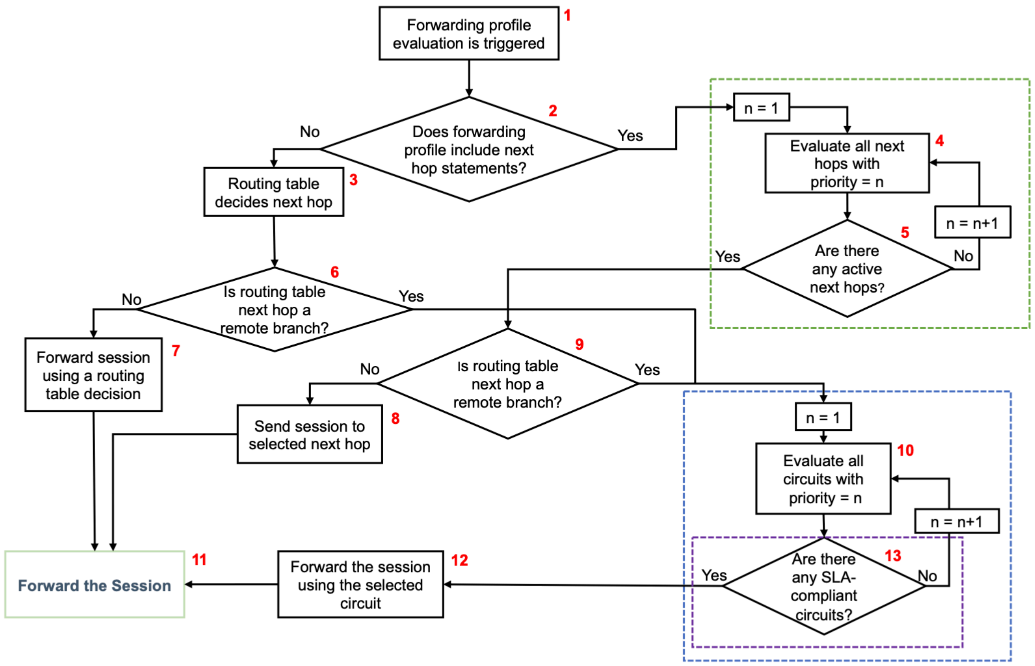

Forwarding profile evaluation is triggered
1
Does forwarding profile include next hop statements?
2
No
Yes
Routing table decides next hop
3
n = 1
Evaluate all next hops with priority = n
4
n = n+1
Are there any active next hops?
5
Yes
No
Is routing table next hop a remote branch?
6
No
Yes
Forward session using a routing table decision
7
Is routing table next hop a remote branch?
9
No
Yes
Send session to selected next hop
8
n = 1
Evaluate all circuits with priority = n
10
n = n+1
Are there any SLA-compliant circuits?
13
Yes
No
Forward the Session
11
Forward the session using the selected circuit
12

Figure 3 details the traffic processing performed by the steps summarized in the green box in Figure 2. The flowchart in Figure 3 describes the process that occurs when two or more next hops have an equal priority and details the next-hop selection process. The flowchart in Figure 3 shows the following:

- When a session matches a forwarding profile in which a next hop is configured (1), the policy evaluation process examines all next hops in the forwarding profile whose priority value is 1 (2).
- If there is no next hop with a priority of 1, the policy evaluation cycles through all possible priority values, up to 15 (for Releases 22.1.1 and later) or up to 8 (for Releases 21.2 and earlier), to determine whether a next hop is up (12, 13, and 2). If no next hop is up, the configured next-hop failure action is taken (14).
- If there is a next hop with a priority value of 1 (or *n* + 1, where *n* ≤ 15 [for Releases 22.1.1 and later], or *n* ≤ 8 [for Releases 21.2 and earlier]) (3), the policy evaluation process checks whether the next hop's SLA profile has a SaaS monitor (4).
- If the SLA profile has a SaaS monitor and the next hop is not a remote branch (5), the policy evaluation process compares the local SaaS monitor to the SLA profile thresholds (6). If the next hop is SLA-compliant (8), the policy evaluation process checks for multiple compliant next hops (9). If not, the policy evaluation process examines the next priority level (12).
- If the SLA profile has a SaaS monitor and the next hop is a remote branch (5), the policy evaluation process compares the local SaaS monitor to the SLA profile thresholds (7). If the next hop is SLA-compliant (8), the policy evaluation process checks for multiple compliant next hops (9). If not, the policy evaluation process examines the next priority level (12).
- If the SLA profile does not have a SaaS monitor (4), or if it does and the next hop determined by comparing the SaaS monitor to the SLA profile thresholds determines that the next hop is SLA-compliant (8), the policy evaluation process determines whether there are multiple compliant next hops (9). If not, the session is forwarded to the next hop (11). If yes, the session is forwarded to the next hop using the configured next-hop selection method (10).

Figure 3: Next-Hop Priority Evaluation

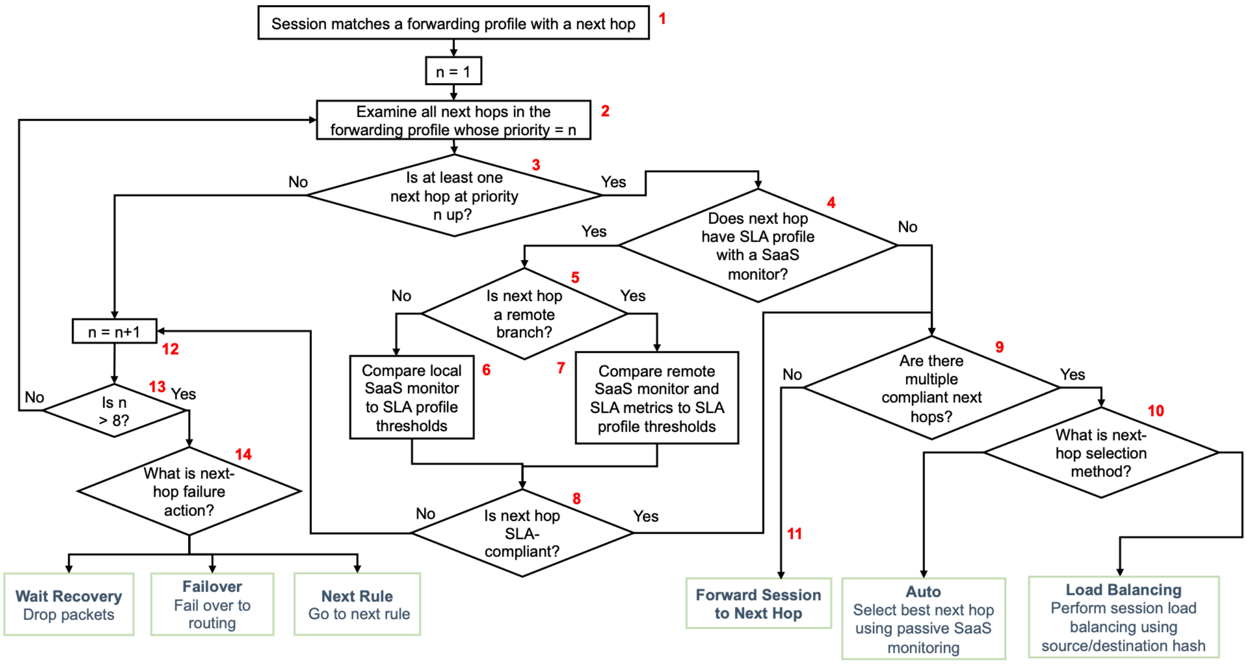

Session matches a forwarding profile with a next hop
1
n = 1
Examine all next hops in the forwarding profile whose priority = n
2
Is at least one next hop at priority n up?
3
No
Yes
Does next hop have SLA profile with a SaaS monitor?
4
Yes
No
Is next hop a remote branch?
5
No
Yes
Compare local SaaS monitor to SLA profile thresholds
6
7
Compare remote SaaS monitor and SLA metrics to SLA profile thresholds
Is next hop SLA-compliant?
8
No
Yes
n = n+1
12
Is n > 8?
13
No
Yes
What is next-hop failure action?
14
Wait Recovery
Drop packets
Failover
Fail over to routing
Next Rule
Go to next rule
Are there multiple compliant next hops?
9
No
Yes
What is next-hop selection method?
10
11
Forward Session to Next Hop
Auto
Select best next hop using passive SaaS monitoring
Load Balancing
Perform session load balancing using source/destination hash

Figure 4 details the traffic processing performed by the steps summarized in the blue box in Figure 2. The flowchart in Figure 4 describes the process that occurs to choose a circuit when the forwarding evaluation process determines that traffic is destined to a remote branch. The flowchart in Figure 4 shows the following:

- When traffic is destined to a remote branch (1), the policy evaluation process examines all SLA paths whose priority value is 1 (2) and compares their SLA metrics with the thresholds configured in the SLA profile. All paths whose SLA is non-compliant are marked as SLA Violated.
- The SLA paths are evaluated to determine whether any of them has a priority value of 1 (3). If not, the policy evaluation process cycles through all possible priority values, up to 15 (for Releases 22.1.1 and later) or up to 8 (for Releases 21.2 and earlier), (4, 2, and 3), and then checks whether a last-resort path is configured (5). The traffic is then dropped (8) or forwarded (9 or 10).
- If there are SLA-compliant paths with a priority of 1, the policy evaluation process determines whether there are multiple SLA-compliant paths (6). If yes, traffic is load-balanced across the available SLA-compliant paths (12). If not, the session is forwarded using the path with priority 1 (11).

Figure 4: Circuit Priority Evaluation

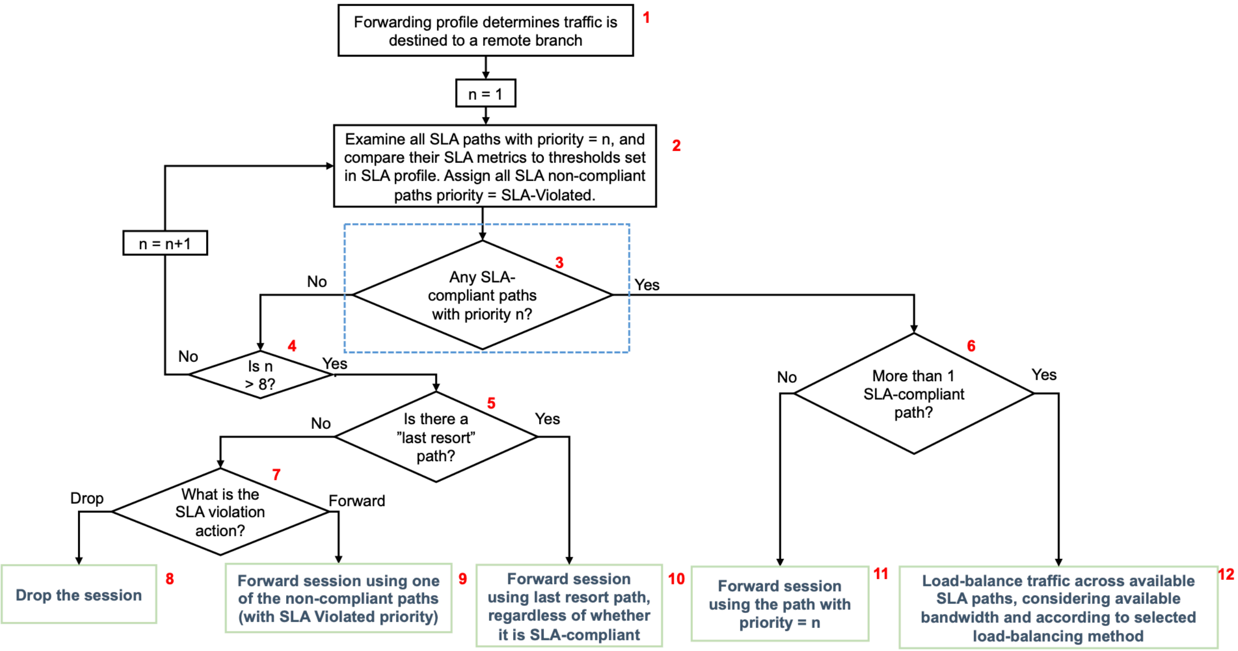
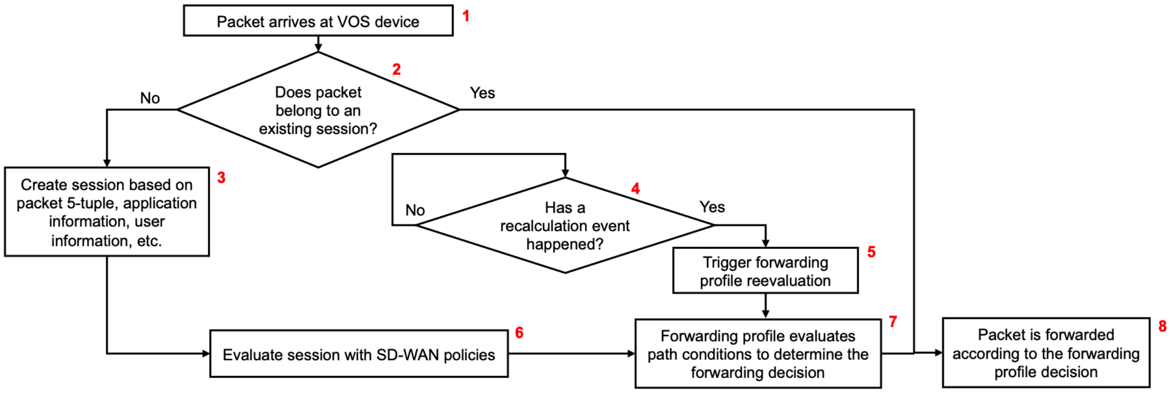

Forwarding profile determines traffic is destined to a remote branch
1
n = 1
Examine all SLA paths with priority = n, and compare their SLA metrics to thresholds set in SLA profile. Assign all SLA non-compliant paths priority = SLA-Violated.
2
n = n+1
Any SLA-compliant paths with priority n?
3
No
Yes
Is n > 8?
4
No
Yes
Is there a "last resort" path?
5
No
Yes
More than 1 SLA-compliant path?
6
No
Yes
What is the SLA violation action?
7
Drop
Forward
Drop the session
8
Forward session using one of the non-compliant paths (with SLA Violated priority)
9
Forward session using last resort path, regardless of whether it is SLA-compliant
10
Forward session using the path with priority = n
11
Load-balance traffic across available SLA paths, considering available bandwidth and according to selected load-balancing method
12

Figure 5 illustrates that for a new session, the circuit and next-hop priorities defined by the SD-WAN policy rule's forwarding profile remain in effect throughout the life of the session. However, reevaluation of the forwarding decision can be triggered by several events, including the following:

- SLA path flaps
- Recalculation timer expires
- A configuration change in the forwarding profile

Figure 5: Evaluation and Re-evaluation


Packet arrives at VOS device
1
Does packet belong to an existing session?
2
No
Yes
Create session based on packet 5-tuple, application information, user information, etc.
3
Has a recalculation event happened?
4
No
Yes
Trigger forwarding profile reevaluation
5
Evaluate session with SD-WAN policies
6
Forwarding profile evaluates path conditions to determine the forwarding decision
7
Packet is forwarded according to the forwarding profile decision
8

Basic SD-WAN Traffic Steering Configuration Overview

To enable Layer 2 or Layer 3 SD-WAN traffic steering, you create a traffic-steering forwarding profile and then apply the profile in a policy enforcement action.

The default SD-WAN traffic-steering profile defines the following traffic-steering behaviors:

- Encryption—Optional
- Load balancing—Per flow
- Connection selection method—Weighted round-robin
- SLA parameters
  - Recomputation timer—300 seconds
  - Path reconsideration interval—60 seconds
  - SLA violation action—Forward
- Symmetric forwarding—Enabled
- Path selection—The WAN path for a new flow is assigned when the flow starts and is based on the configured priority and SLA thresholds. The path does not change even if the path goes out of SLA compliance.
- Path evaluation—Each branch periodically evaluates active forwarding profiles to determine which paths comply with the configured parameters.

To use the default traffic-steering behaviors, you can simply apply the default traffic-steering profile in a policy enforcement action, as described in Configure an SD-WAN Traffic-Steering Policy, below.

To change the default behaviors or configure additional behaviors, create another forwarding profile.

To change the default SLA behaviors, configure an SLA profile, as described in Configure SLA Profiles for SD-WAN Traffic Steering.

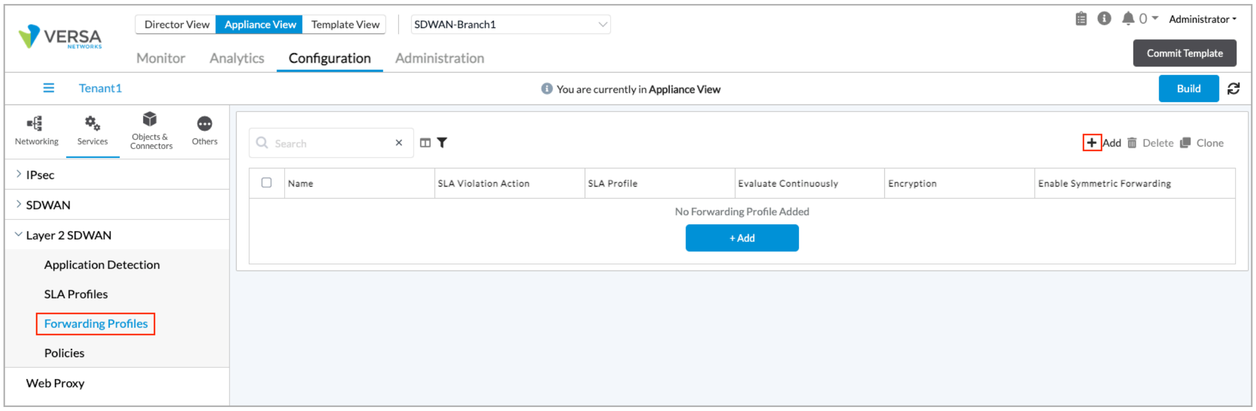
In Layer 3 SD-WAN traffic steering, before a forwarding profile can select the best path for a traffic-steering policy, it must know which paths are eligible to be considered. You can configure path eligibility in one of the following ways:

- Route-based path selection—A route-lookup is performed to determine the set of equal-cost paths, which allows for equal-cost multipath (ECMP) routing.
- Configuration-based path selection—You configure a list of next hops (that is, any combination of WAN circuits and hubs) from which the best one is selected.

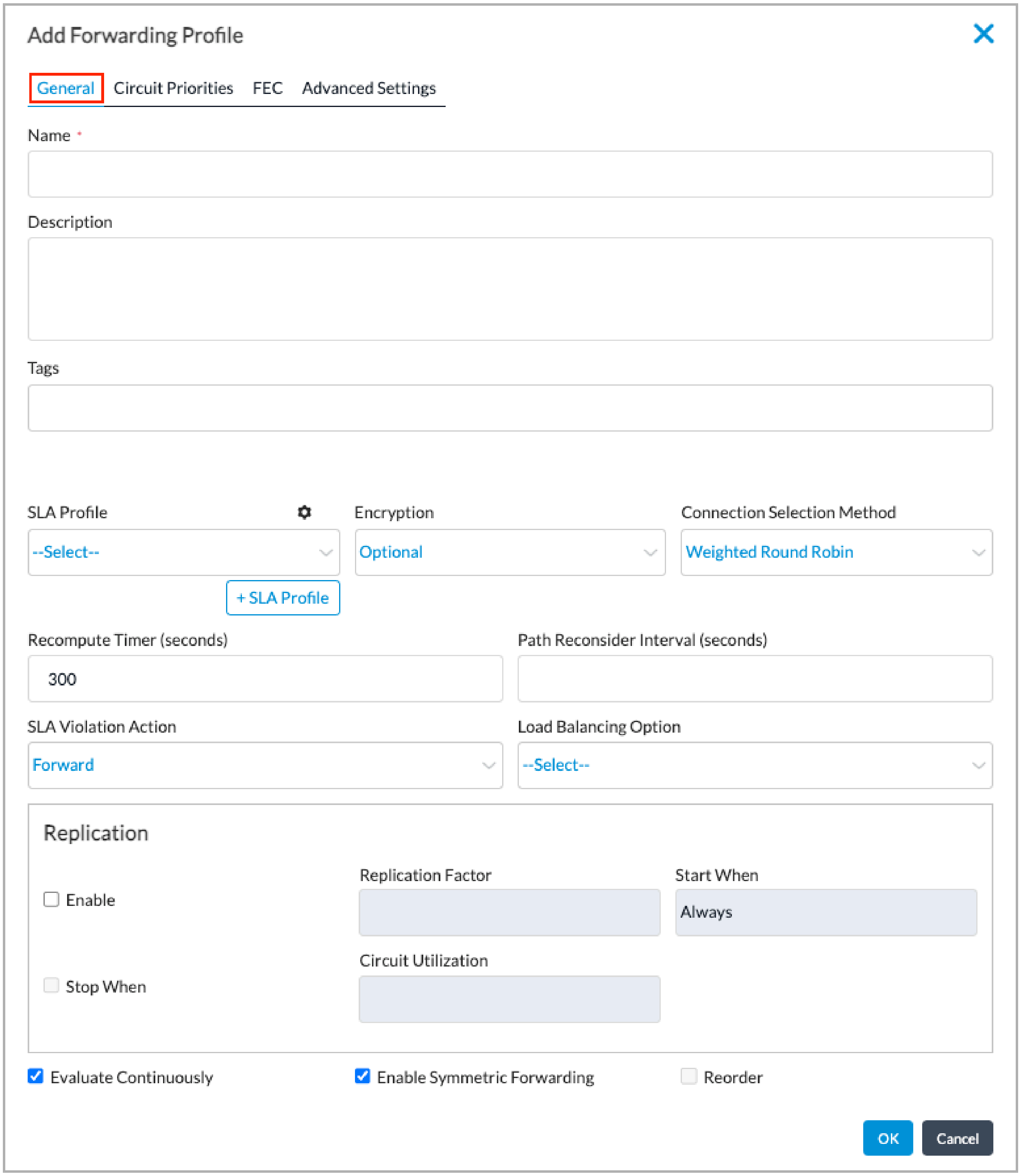
To correctly process all traffic in an application flow, the Layer 2 or Layer 3 SD-WAN traffic-steering policy uses application detection, which is always running on the VOS device, to inspect the first packet in a flow and to identify the Layer 7 application sending the flow. Application detection maintains a cache that contains entries for all the IP addresses that a domain name resolves to, and for all the applications and URL categories that are known for a domain. You can configure the SD-WAN application detection parameters.

Configure Layer 2 SD-WAN Traffic-Steering Forwarding Profiles

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Layer 2 SD-WAN > Forwarding Profiles in the left menu bar.



4. Click the + Add icon or the + Add Add button. The Add Forwarding Profile popup window displays.



Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings

Name *

Description

Tags

SLA Profile: --Select--

+ SLA Profile

Encryption: Optional

Connection Selection Method: Weighted Round Robin

Recompute Timer (seconds): 300

Path Reconsider Interval (seconds):

SLA Violation Action: Forward

Load Balancing Option: --Select--

Replication

□ Enable

Replication Factor:

Start When: Always

□ Stop When

Circuit Utilization:

☑ Evaluate Continuously

☑ Enable Symmetric Forwarding

□ Reorder

5. Select the General tab, and then enter information for the following fields.

Field	Description
Name	Enter a name for the forwarding profile. This is a text string from 1 to 63 characters long.
Description	Enter a text description for the forwarding profile.
Tags	Enter a keyword or phrase that allows you to filter the forwarding profile name. This is useful when you have many profile names and want to view those that are tagged with a particular keyword.
SLA Profile	Select the SLA profile to associate with the forwarding profile. Selecting an SLA profile is not required to create and activate a forwarding profile. For more information, see Configure SLA Profiles for SD-WAN Traffic Steering. *Default:* If you do not associate an SLA profile with the forwarding profile, all traffic is allowed.
+ SLA Profile	Click to configure a new SLA profile. For more information, see Configure SLA Profiles for SD-WAN Traffic Steering.
Encryption	To control the WAN access link encryption for an organization, you can modify the default encryption behavior in one of the following ways: ◦ Modify the encryption for all traffic on a specific access circuit (path), as described in Configure Encryption on WAN Interfaces. ◦ Modify the encryption for specific applications by selecting the encryption type in the traffic-steering forwarding profile. Application-specific encryption behavior applies to traffic regardless of the path encryption. It is recommended that you configure encryption in a traffic-steering forwarding profile so that the encryption applies to specific application traffic rather than to all traffic transiting a WAN access link. To select the encryption in the traffic-steering profile, select one of the following options: ◦ Always—Always encrypt all traffic regardless of

	the path encryption mode. ◦ Never—Do not encrypt any traffic regardless of the path encryption mode. Select this option to avoid the encryption overhead when end-to-end traffic is already encrypted (for example, secure RTP and SSL traffic). ◦ Optional—Defer to the path encryption mode that is enabled on the WAN link that is used as the Layer 2 SD-WAN transport. This is the default. *Default:* Optional
Connection Selection Method	Select how to forward a traffic flow when multiple available WAN paths have the highest priority. For example, if there are two paths at priority 1 and one path at priority 2, one of the priority 1 paths is chosen. ◦ Weighted round-robin—Use WRR, which balances flows across paths proportional to their available bandwidth. This is the default connection selection method. To determine a circuit's available bandwidth, the bandwidth consumption of each logical interface is measured periodically. To calculate the remaining bandwidth on each access circuit, the VOS traffic-steering software uses a reference bandwidth. For the reference bandwidth, the VOS software considers the CoS shaper rate. If no shaper rate is present, the VOS software considers the interface's uplink and downlink bandwidths (for a logical interface, these are the physical interface's uplink and downlink bandwidths). Then the VOS software assigns a weight to each path based on the bandwidth available on the access circuit. For information about configuring the uplink and downlink bandwidth values, see Configure Interfaces. Here's two examples of how WRR works. First, let's say that two circuits, WAN1 and WAN2, are both the highest-priority SLA-compliant paths. WAN1 is a 10-Mbps link that is currently using 8 Mbps, and WAN2 is a 5-Mbps link using 1 Mbps. WAN1 has 2 Mbps of available capacity, and WAN 2 has 4 Mbps, so load balancing would be performed between the WAN1 and WAN2 circuits in the ratio of 2:4, or 1:2. In a second example, which considers logical interfaces, let's say we have two logical WAN interfaces, WAN1 on vni-0/0.100 and WAN2 on

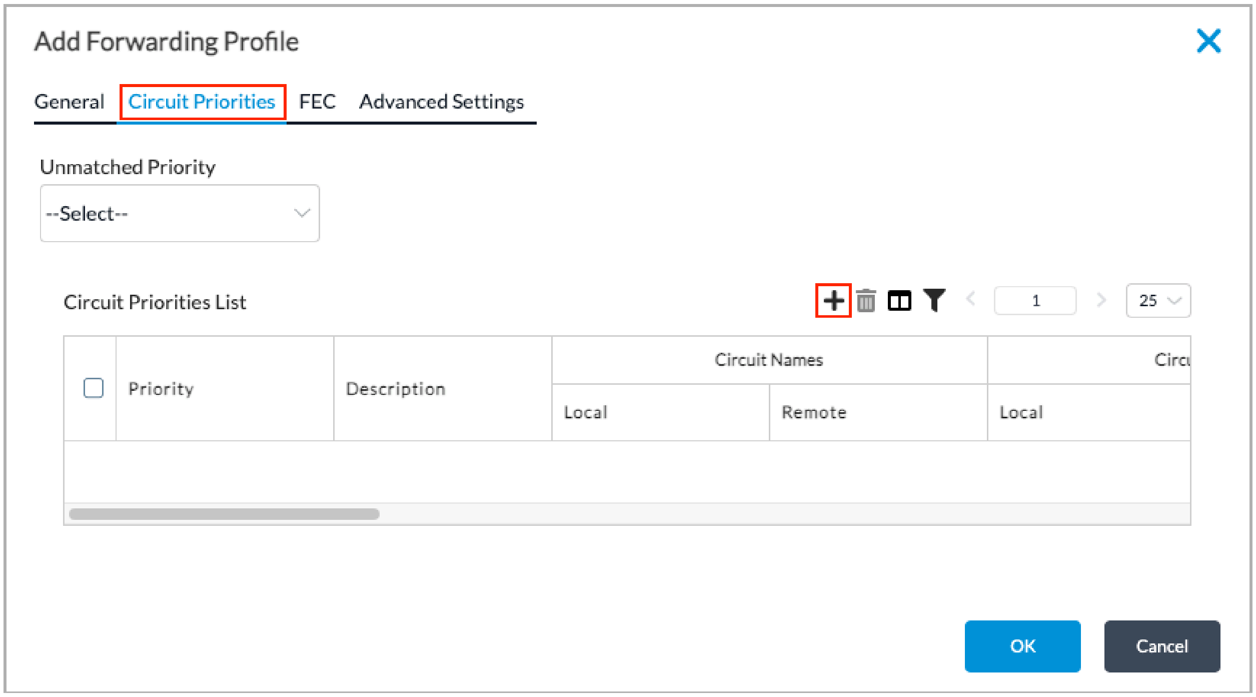
	vni-0/0.200. The WAN1 vni-0/0.100 logical interface has a configured shaping rate of 100 Mbps, and the WAN2 vni-0/0.200 logical interface has a configured shaping rate of 150 Mbps. If the current circuit utilization of vni-0/0.100 is 60 Mbps and of vni-0/0.200 is 70 Mbps, the remaining capacity is 40 Mbps and 80 Mbps, respectively. So load balancing would be performed between the vni-0/0.100 and vni-0/0.200 logical interfaces in the ratio of 40:80, or 1:2. ◦ High available bandwidth—Use the circuit with the highest available bandwidth. Continuing with the example in the previous bullet, because the available bandwidth on WAN2 is higher, this link would be used. ◦ Low cost—This option is not used. It provides backward compatibility with earlier software versions. *Default:* Weighted round-robin
Recompute Timer	Enter how often to re-evaluate the SLA-compliance state of all paths. If the re-evaluation identifies an SLA violation on a circuit, the traffic is switched to a different circuit. *Range:* 5 through 1800 seconds *Default:* 300 seconds
Path Reconsider Interval	Enter a time after which an SLA-violated link is reconsidered for forwarding audio, video, and voice packets that are being steered based on a MOS score. *Range:* 60 through 1800 seconds *Default:* 60 seconds
SLA Violation Action	Select the action to take if no paths towards the destination branch meet the SLA requirements associated with the forwarding profile: ◦ Drop—Drop the traffic. Forwarding resumes only when an SLA-compliant path becomes available. ◦ Forward—Continue to forward traffic on SLA-

	violated paths. This is the default. ◦ Throttle Low Priority Traffic—This option is not used. *Default:* Forward
Load Balancing Option	Select how to load-balance a flow of traffic when two or more paths have the same highest priority. All packets in a flow are directed to the same path. ◦ Per Flow—Load-balance the traffic flows across all eligible paths. This is the default. Per-flow load-balancing can increase the total throughput for an application when multiple paths of the same type are present. ◦ Per Packet—Load-balance the packets in a traffic flow among the paths at the current highest priority level. *Default:* Per Flow
Replication (Group of Fields)	Replication is an advanced SD-WAN traffic-steering feature. For more information, see Configure Replication for SD-WAN Traffic Steering.
◦ Enable	Click to enable packet replication. *Default:* Replication is disabled
◦ Replication Factor	For each ingress packet, define the number of egress packets to send. *Range:* 2 through 4
◦ Start When	Select when to start replication automatically: ◦ Always ◦ SLA violated—When all available paths do not meet configured SLA threshold
◦ Stop When	Click to enable using a circuit utilization threshold value to stop packet replication.
◦ Circuit Utilization	When you enable Stop When, enter the circuit

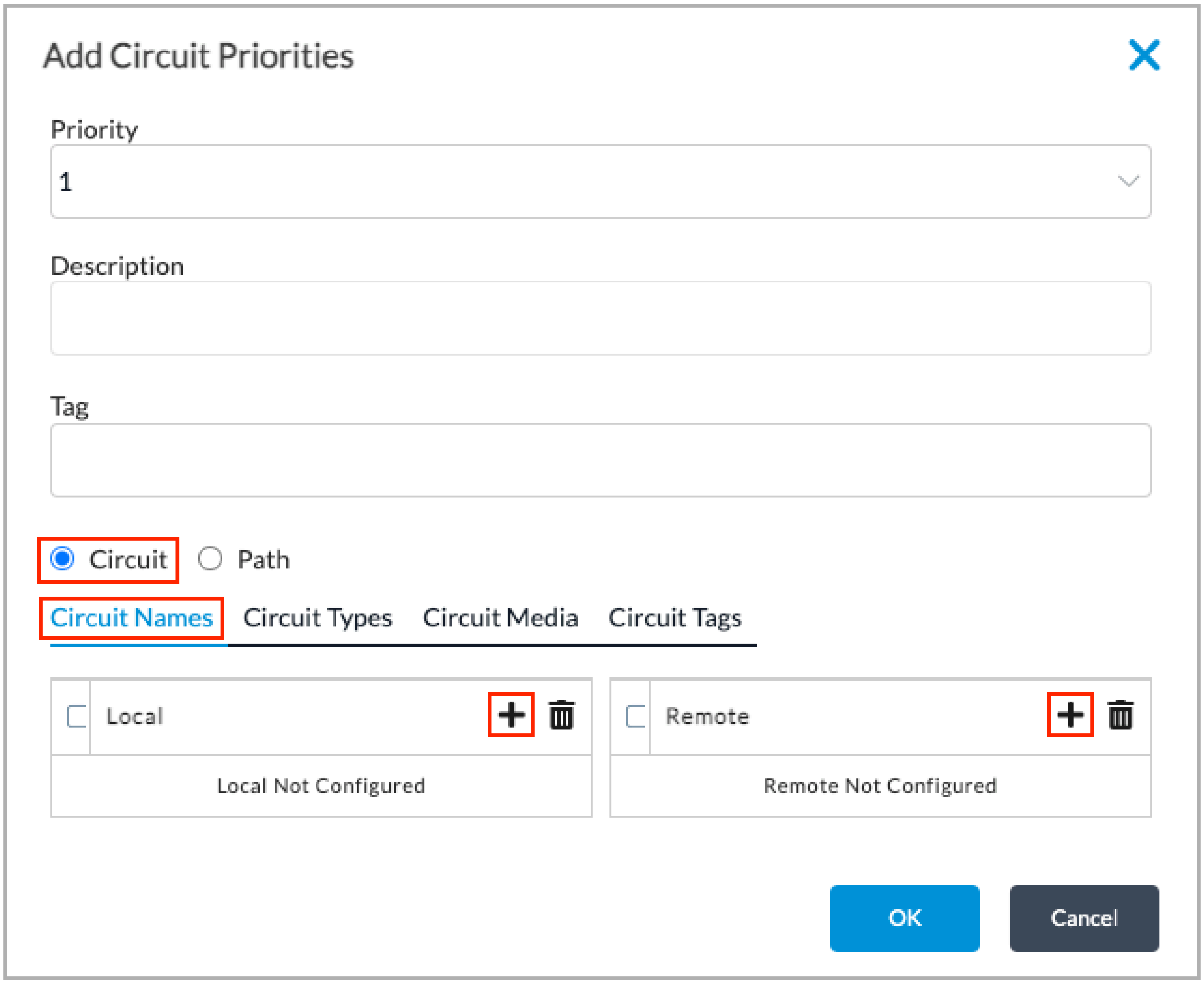
	utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization exceeds this threshold value, packet replication stops automatically. Packet replication stops when the transmit circuit utilization of any link that is used for replicating packets exceeds the configured threshold. *Range:* 1 through 100 percent
Evaluate Continuously	Click to to move a traffic flow off a non-compliant path at the recompute timer interval (by default, 300 seconds). (By default, an existing traffic flow remains on the same path until the flow ends, even if the path becomes SLA non-compliant.) Enabling this option is recommended for real-time applications, such as voice and video, to allow a traffic flow to change to a better path if the original path is no longer SLA-compliant. When traffic is moved off an SLA-non-compliant path, it can lead to a thundering-herd effect in which the moved traffic causes the second path to go out of compliance, and then the traffic is moved back to the first path. To avoid this problem, enable both Evaluate Continuously and Gradual Migration (on the Advanced Settings tab). Doing this allows traffic flows to move gradually from the original path to the new path over multiple recomputation timer cycles. Gradually moving the flows reduces the load on the original path, mitigating the SLA degradation, so that other flows do not have to move. Flows that move to a new path remain on that path as long as it is SLA-compliant. *Default*: Disabled
Enable Symmetric Forwarding	Click to enable symmetric traffic forwarding, which determines the path to use for reverse-direction traffic, that is, for traffic returning from the destination branch to originating branch. By default, the return traffic is forwarded symmetrically, that is, on the same path on

	which the traffic was received. You might want to disable symmetric forwarding for applications where it is beneficial to independently choose the best path in either direction. *Default:* Enabled; that is, return traffic is forwarded symmetrically
Reorder	Click to reorder packets in a flow that arrive out of order. Packets might arrive out of order when you configure per-packet load balancing or packet replication. *Default*: Enabled

6. Select the Circuit Priorities tab to configure circuit properties for local and remote clients.



7. Click the + Add icon. In the Add Circuit Priorities popup window, enter information for the following fields.



Add Circuit Priorities

Priority: 1

Description:

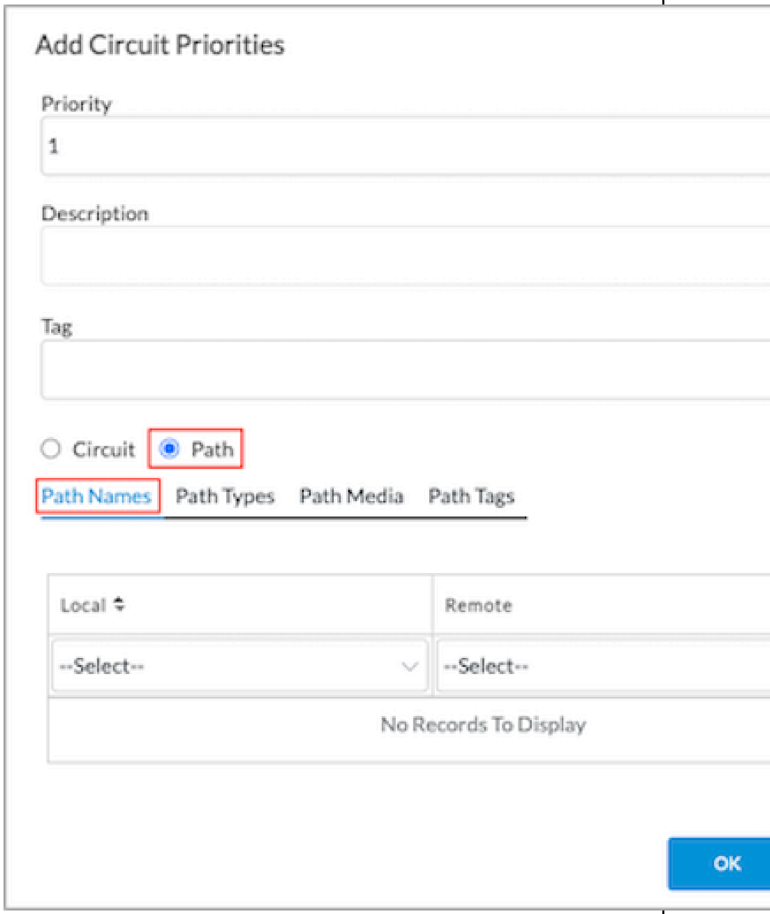
Tag:

● Circuit ○ Path

Field	Description
Priority	Select the priority level to assign to circuits. This value defines the preference for WAN paths between the local branch and a remote branch or branches. For Releases 22.1.1 and later, 17 circuit priority levels are available: 1 through 15, Avoid, and Last Resort. For Releases 21.2 and earlier, 10 circuit priority levels are available: 1 through 8, Avoid, and Last Resort. For the numeric priorities, priority 1 is the most preferred and priority 15 is the least preferred. If you assign the same circuit priority value to two or more WAN paths, traffic is load-balanced among the paths. For example, on a VOS device that has WAN links to MPLS and to the internet, to direct all Layer 2 SD-WAN traffic to the MPLS link, you set a higher priority for the MPLS circuit and a lower priority for the internet link. If you do not configure a circuit priority value for a path, the path is assigned to the lowest priority level and so becomes the least preferred path. If the forwarding profile defines SLA requirements, new traffic flows on the circuit are sent on the WAN path with the highest priority that meets the SLA criteria. If a path does not meet the SLA requirements, it is demoted to the SLA-violated priority. The path-selection logic then tries to find other paths that have a higher priority and that comply with the SLA. At any given time, a path can be assigned one of the following priorities, which are listed in priority order from most preferred to least preferred: ◦ 1 through 15 (for Releases 22.1.1 and later); 1 through 8 (for Releases 21.2 and earlier)—The path is SLA compliant, and its run-time priority is the same as its configured priority. ◦ If a path is not assigned to any priority and an unmatched priority is not selected, the path is assigned a priority of 15 (for Releases 22.1.1 and later) or 8 (for Releases 21.2 and earlier), which is the default priority. ◦ SLA-Violated—The path fails to meet the SLA

	compliance metrics. ◦ Last Resort—A path to use when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available. ◦ Avoid—The circuit is configured as one to be avoided. An avoided circuit is not used even if it is the only available path. If the only available paths are configured as avoid, traffic is dropped. ◦ 15—All unused circuits have this priority, which is the lowest priority. The SLA for these circuits uses low delay, low loss, low jitter, low forwarding loss, and low reverse loss, and the path score is calculated based on loss, delay, and jitter on the circuits with lower latency or loss. *Values:* 1 through 15, Avoid, Last Resort (for Releases 22.1.1 and later); 1 through 8, Avoid, Last Resort (for Releases 21.2 and earlier)
Description	Enter a text description for the circuit priority level.
Tag	Enter a keyword or phrase that allows you to filter the priority level. This is useful when you have many levels and want to view those that are tagged with a particular keyword.
Circuit	Select to configure circuit priorities for local and remote clients.
Circuit Names (Tab)	Configure the WAN circuits, by circuit name, to assign the priority level. For each WAN circuit, you specify a local name and a remote name for the path between two branches. Circuits typically have names such as WAN1 and WAN2. If you specify a name only for the local branch, the name for the remote branch is treated as a wildcard. The same is true if you specify a circuit name only for the remote branch.
◦ Local	Click the + Add icon, and then select a WAN circuit name on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit name on the remote branch.
Circuit Types (Tab)	Configure the circuits, by circuit type, to assign the priority level. For each WAN circuit, you specify a local

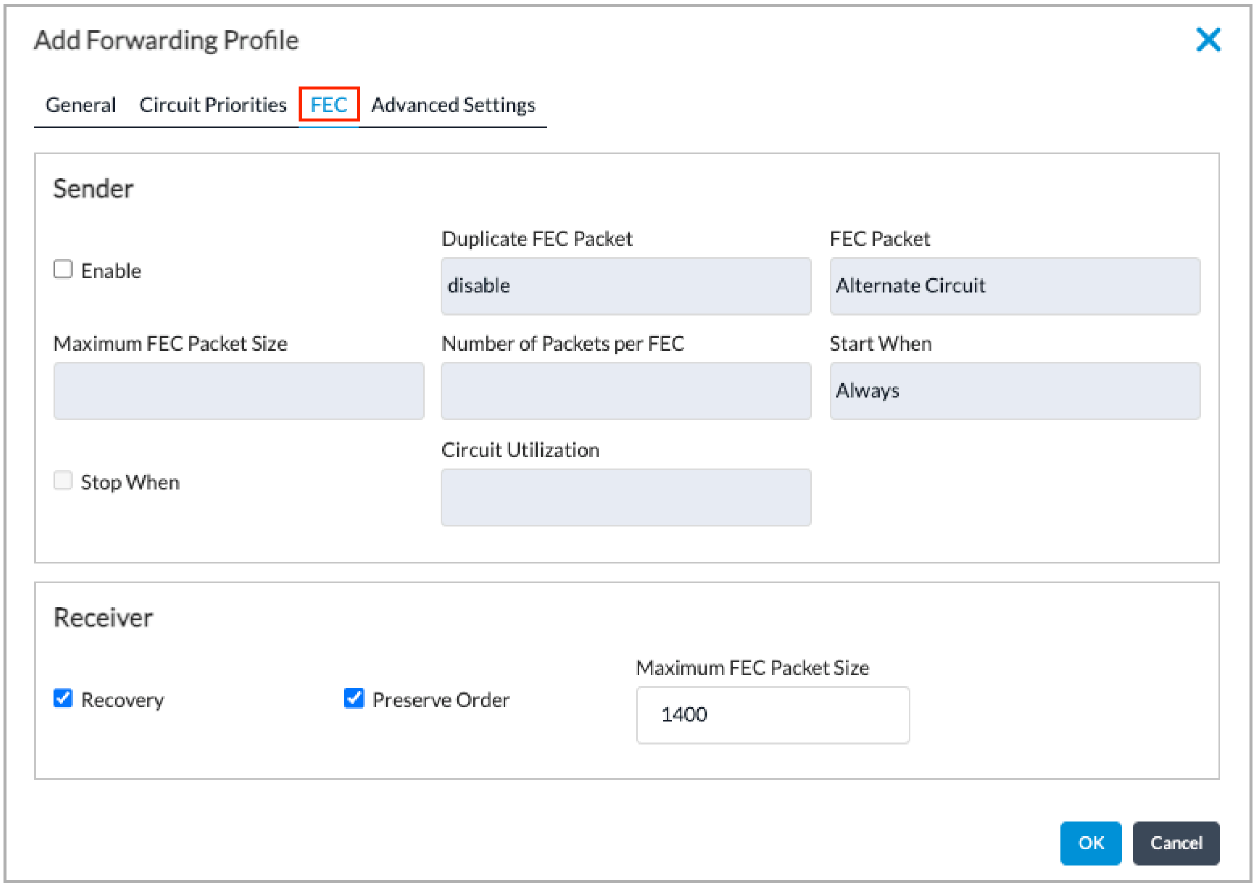
	type and a remote type for the path between two branches. Circuits typically have types such as broadband, IP, and MPLS. If you specify a type only for the local branch, the type for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the + Add icon, and then select a WAN circuit type on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit type on the remote branch.
Circuit Media (Tab)	Configure the circuits, by circuit media, to assign the priority level. For each WAN circuit, you specify a local media and a remote media for the path between two branches. Circuits typically have media such as cable, DSL, Ethernet, LTE, T1, and T3. If you specify a media only for the local branch, the media for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the + Add icon, and then select a WAN media on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit media on the remote branch.
Circuit Tags (Tab)	Configure the circuits, by circuit tags, to assign the priority level. For each WAN circuit, you specify a local tag and a remote tag for the path between two branches. Circuit tags are text strings. If you specify a tag only for the local branch, the tag for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the + Add icon, and then select a WAN circuit tag on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit tag on the remote branch.
Path	Select to configure path-based circuit priorities for local and remote clients.

	 Add Circuit Priorities Priority 1 Description Tag ○ Circuit ● Path Path Names · Path Types · Path Media · Path Tags Local ≑ · Remote --Select-- · --Select-- No Records To Display OK
Path Names (Tab)	Configure the WAN circuits, by path name, to assign the priority level. For each WAN circuit, you specify a local name and a remote name for the path between two branches. Circuits typically have names such as WAN1 and WAN2. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Select a WAN circuit name on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit name on the remote branch, and then click the + Add icon.
Path Types (Tab)	Configure the circuits, by path type, to assign the priority level. For each WAN circuit, you specify a local type and a remote type for the path between two branches. Circuits typically have types such as broadband, IP, and MPLS. You cannot leave either field empty. To specify a wildcard for a field, select

	Any.
◦ Local	Select a WAN circuit type on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit type on the remote branch, and then click the +Add icon.
Path Media (Tab)	Configure the circuits, by path media, to assign the priority level. For each WAN circuit, you specify a local media and a remote media for the path between two branches. Circuits typically have media such as cable, DSL, Ethernet, LTE, T1, and T3. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Select a WAN media on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit media on the remote branch, and then click the + Add icon.
Path Tags (Tab)	Configure the circuits, by path tag, to assign the priority level. For each WAN circuit, you specify a local tag and a remote tag for the path between two branches. Path tags are text strings. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Select a WAN circuit tag on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit tag on the remote branch, and then click the + Add icon.

8. (For Releases 22.1.1 and later.) Select the FEC tab to configure forward error correct. Enter information for the following fields. FEC is an advanced SD-WAN traffic-steering feature. For more information, see Configure Forward Error Correction for SD-WAN Traffic Steering.

   Note that FEC is available to Network Flow Processor (NFP)-capable Layer 2 unicast traffic only.



Add Forwarding Profile

Sender

☐ Enable

Duplicate FEC Packet: disable

FEC Packet: Alternate Circuit

Maximum FEC Packet Size:

Number of Packets per FEC:

Start When: Always

☐ Stop When

Circuit Utilization:

Receiver

☑ Recovery

☑ Preserve Order

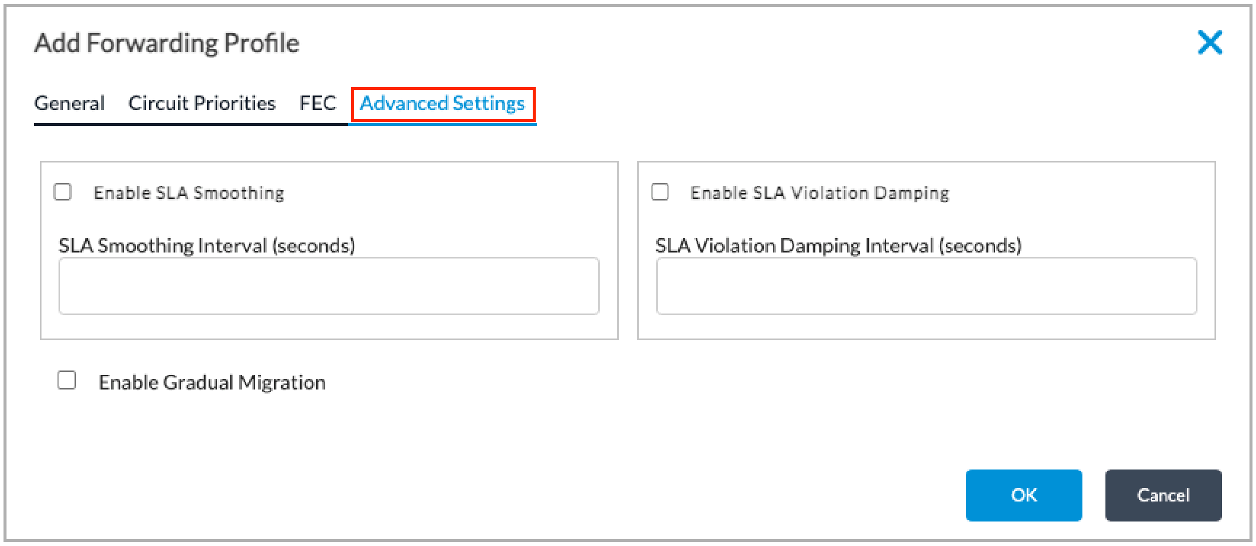
Maximum FEC Packet Size: 1400

Field	Description
Sender (Group of Fields)	
◦ Enable	Click to enable FEC. *Default:* Disabled
◦ Duplicate FEC Packet	Select how to duplicate FEC parity packets: ◦ Alternate circuit—Duplicate FEC parity packets and send them on a WAN interface that is not an interface on which data packets are transmitted. ◦ Disabled—Do not duplicate FEC parity packets. This is the default. ◦ Same circuit—Duplicate FEC parity packets and send them on the same WAN interface used to transmit data packets. *Default:* Disabled
◦ FEC Packet	Select the circuit on which to send FEC parity packets: • Alternate circuit—Send FEC parity packets on a WAN interface that is not an interface on which data packets are transmitted. This is the default. If an alternate circuit is unavailable, FEC parity packets are sent on the same circuit as data packets. • Same circuit—Send FEC parity packets on the same WAN interface used to transmit data packets. *Default:* Alternate circuit
◦ Maximum FEC Packet Size	Enter the maximum packet size of FEC parity packet that the sender can send. This value is used to recover lost packets. If the maximum packet size you configure (referred to as *n*) is less than or equal to the data packet size, the recovered packet contains the first *n* bytes of the original packet. *Range:* 100 through 10000 bytes *Default:* 1400 bytes

◦ Number of Packets per FEC	Enter the number of data packets after which an FEC packet is generated and sent to the peer branch. The generated FEC parity packet can recover a packet on the peer branch only if there is one lost packet in the specified number of packets per FEC. *Range:* 1 through 32 *Default:* 4
◦ Start When	Select when to start sending FEC parity packets: ◦ Always ◦ SLA violated—When all available paths are SLA violated
◦ Stop When	Click to set the circuit utilization threshold at which to stop sending FEC parity packets.
◦ Circuit Utilization	Enter the utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization of the links used for data packets or FEC parity packet transmission exceeds this threshold, FEC stops. FEC stops when the transmit circuit utilization of any link that is used for replicating the packet exceeds the configured threshold. For example, if you configure the circuit utilization threshold as 80 percent and there are two WAN links—broadband and MPLS—then at any given time if the transmit circuit utilization threshold on either the broadband or MPLS circuit exceeds 80 percent, FEC stops on both circuits. *Range:* 1 through 100 percent *Default:* None
Receiver (Group of Fields)	
◦ Recovery	Click to enable packet recovery after receiving FEC packets.

	Default: Receiver packet recovery is enabled.
◦ Preserve Order	Click to reorder out-of-order packets and forward them in their original order. *Default:* Packet reordering is enabled.
◦ Maximum FEC Packet Size	Enter the maximum packet size of FEC parity packet that the receiver can receive. This value is used to recover lost packets. If the maximum packet size you configure (referred to as *n*) is less than or equal to the data packet size, the recovered packet contains the first *n* bytes of the original packet. *Range:* 100 through 10000 bytes *Default:* 1400 bytes

9. Select the Advanced Settings tab to define values for SLA smoothing, damping, and migration. Enter information for the following fields.



Add Forwarding Profile

□ Enable SLA Smoothing

SLA Smoothing Interval (seconds)

□ Enable SLA Violation Damping

SLA Violation Damping Interval (seconds)

□ Enable Gradual Migration

Field	Description
Enable SLA Smoothing	Click to average the SLA metrics over the smoothing interval instead of the recompute interval. If you do not enable SLA smoothing, the SLA compliance of a path is checked every recompute interval. The SLA for a path is recomputed regularly to determine whether a path is SLA compliant. SLA smoothing is a mechanism to prevent a path from frequently oscillating between an SLA-compliant and an SLA-non-compliant state each time the SLA is recomputed. Configuring SLA smoothing is useful for loss-based SLAs, where the loss measurement accuracy depends on the number of packet samples. When you configure SLA smoothing, you define a smoothing interval that is used to minimize the oscillations. The SLA smoothing interval is used in conjunction with the path recomputation interval to determine a path's SLA compliance. For a path that is currently SLA-compliant, the average metrics over the last recompute interval are used to determine compliance. For a path that is currently non-compliant, the average metrics over the last smoothing interval are used. This scheme allows a fast reaction to a network impairment, which can occur in one recompute interval, and it provides a slow and cautious return to the compliant state because the metrics smoothed over the last smoothing interval are used. The default SLA recomputation interval is 300 seconds, which is a conservative interval that is large enough so that you likely would not want or need to configure smoothing. However, if you want to configure an aggressive recomputation interval, you might change the recomputation interval to a value between 5 and 20 seconds. Then, if you configure SLA smoothing and use the default smoothing interval, smoothing is done every 120 seconds. If you change the smoothing interval, it must be larger than

	the recomputation interval. For example, consider a case where the recomputation interval is 10 seconds and the smoothing interval is 60 seconds. If a path is SLA-compliant, the SLA metrics are averaged over the last 10 seconds to determine SLA compliance. If a path is SLA non-compliant, the SLA metrics are averaged over the last 60 seconds to determine SLA compliance. Here, the SLA smoothing allows 50 additional seconds for network conditions to improve before the branch device has to recompute an SLA-compliant path. *Default:* Disabled
SLA Smoothing Interval	Enter the SLA smoothing interval, in seconds. Range: 10 through 300 seconds Default: 120 seconds
Enable SLA Violation Damping	Select to associate the recompute interval value with the damping interval value. If you do not enable SLA violation damping, the SLA compliance of a path is checked every recompute interval. Damping is another mechanism to prevent a path from frequently oscillating between an SLA-compliant and an SLA-non-compliant state each time the SLA is recomputed. The damping interval defaults to 3 times the path recomputation interval. If you change the default damping value, it must be larger than the recomputation interval. With damping, a path moves from an SLA-compliant and an SLA-non-compliant state based on the average SLA metrics over the last recompute interval. If the path is in an SLA-non-compliant state, it is forcibly held in that state for the damping interval even if network conditions have improved and the path is otherwise SLA-compliant. For example, if the

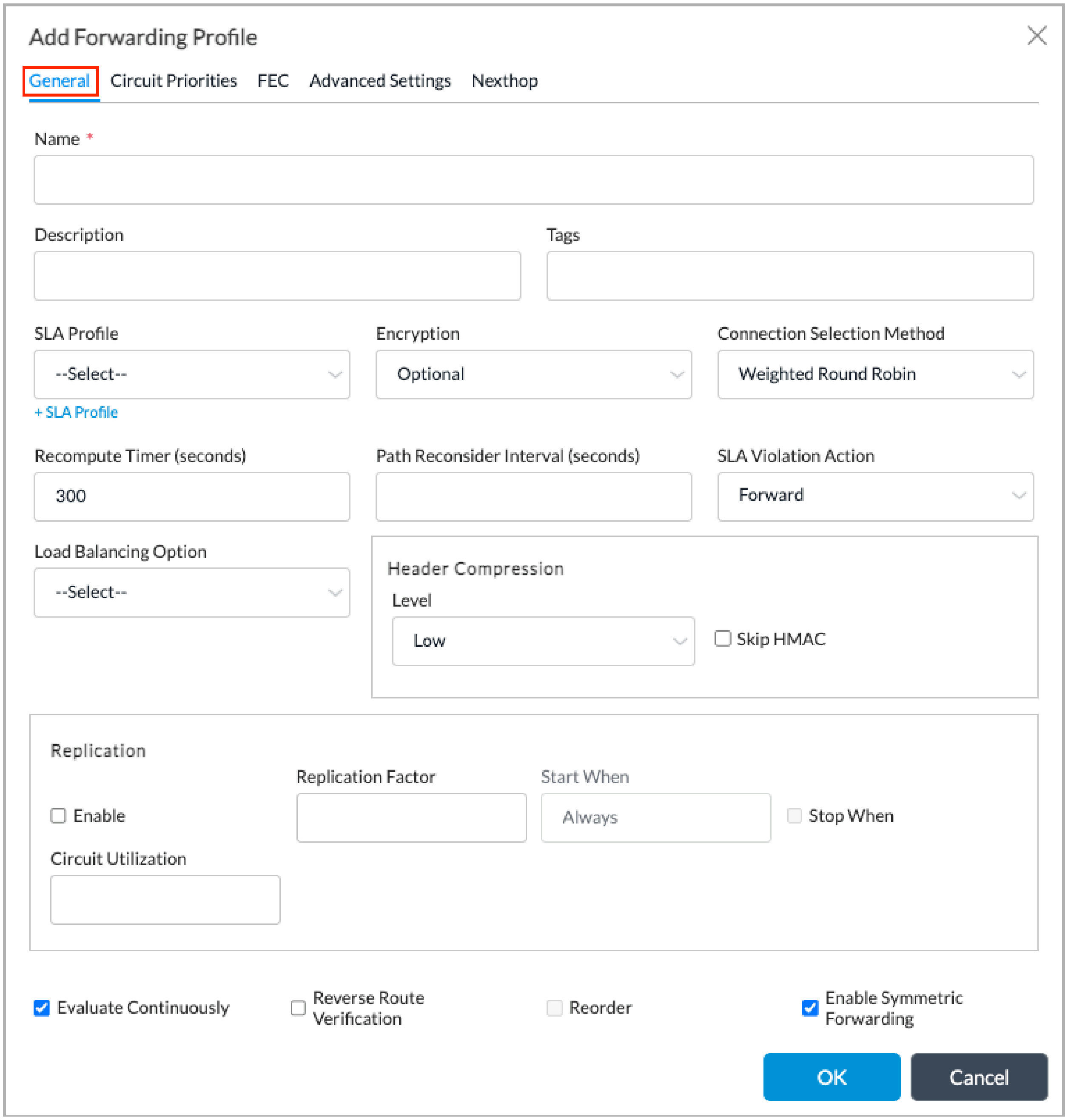
	recomputation interval is 10 seconds, a non-damped path can oscillate between compliant and non-compliant state every 10 seconds. However, if you enable damping and set the damping interval to 60 seconds, the path moves to non-compliant state 10 seconds after network conditions degrade, and remains in that state for at least 60 seconds. Only after 60 seconds are the path metrics evaluated again to determine whether the path is once again SLA-compliant. Note that if both SLA violation damping and SLA smoothing are enabled, the timers both start when a path enters an SLA-non-compliant state. For example, if the recompute interval is 10 seconds, and the dampening interval and smoothing interval are both 60 seconds, dampening ensures that in the 60 seconds, the path will not be put back into the compliant state, even though the metrics are below the violation thresholds through 6 recomputation intervals. The smoothing interval ensures that the last 60 seconds of metrics instead of the last 10 seconds of metrics are used to determine the path's SLA compliance. *Default:* Disabled
SLA Violation Damping Interval	Enter the SLA violation damping interval, in seconds. *Default:* 3 times the recompute interval
Enable Gradual Migration	Click to enable gradual migration. When traffic is moved off an SLA-non-compliant path, it can lead to a thundering-herd effect in which the moved traffic causes the second path to go out of compliance, and then the traffic is moved back to the first path. To avoid this problem, enable both Evaluate Continuously (on the General tab) and Gradual Migration. Doing this allows traffic flows to move gradually from the original path to the new path over

	multiple recomputation timer cycles. Gradually moving the flows reduces the load on the original path, mitigating the SLA degradation, so that other flows do not have to move. Flows that move to a new path remain on that path as long as it is SLA-compliant. *Default:* Disabled

10. Click OK.

Configure Layer 3 SD-WAN Traffic-Steering Forwarding Profiles

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Forwarding Profiles in the left menu bar.
4. Click the + Add icon or the + Add Add button. The Add Forwarding Profile popup window displays.



Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Nexthop

Name *

Description

Tags

SLA Profile: --Select--

+ SLA Profile

Encryption: Optional

Connection Selection Method: Weighted Round Robin

Recompute Timer (seconds): 300

Path Reconsider Interval (seconds)

SLA Violation Action: Forward

Load Balancing Option: --Select--

Header Compression

Level: Low

□ Skip HMAC

Replication

□ Enable

Replication Factor

Start When: Always

□ Stop When

Circuit Utilization

☑ Evaluate Continuously

□ Reverse Route Verification

□ Reorder

☑ Enable Symmetric Forwarding

5. In the General tab, enter information for the following fields.

Field	Description
Name	Enter a name for the forwarding profile. This is a text string from 1 to 63 characters long.
Description	Enter a text description for the forwarding profile.
Tags	Enter a keyword or phrase that allows you to filter the forwarding profile name. This is useful when you have many profile names and want to view those that are tagged with a particular keyword.
SLA Profile	Select the SLA profile to associate with the forwarding profile. Selecting an SLA profile is not required to create and activate a forwarding profile. For more information, see Configure SLA Profiles for SD-WAN Traffic Steering. *Default:* If you do not associate an SLA profile with the forwarding profile, all traffic is allowed.
+ SLA Profile	Click to configure a new SLA profile. For more information, see Configure SLA Profiles for SD-WAN Traffic Steering.
Encryption	To control the WAN access link encryption for an organization, you can modify the default encryption behavior in one of the following ways: ◦ Modify the encryption for all traffic on a specific access circuit (path), as described in Configure Encryption on WAN Interfaces. ◦ Modify the encryption for specific applications by selecting the encryption type in the traffic-steering forwarding profile. Application-specific encryption behavior applies to traffic regardless of the path encryption. It is recommended that you configure encryption in a traffic-steering forwarding profile so that the encryption applies to specific application traffic rather than to all traffic transiting a WAN access link. To select the encryption in the traffic-steering profile, select one of the following options: ◦ Always—Always encrypt all traffic regardless of

	the path encryption mode. ◦ Never—Do not encrypt any traffic regardless of the path encryption mode. Select this option to avoid the encryption overhead when end-to-end traffic is already encrypted (for example, secure RTP and SSL traffic). ◦ Optional—Defer to the path encryption mode that is enabled on the WAN link that is used as the SD-WAN transport. This is the default. *Default:* Optional
Connection Selection Method	Select how to forward a traffic flow when multiple available WAN paths have the highest priority. For example, if there are two paths at priority 1 and one path at priority 2, one of the priority 1 paths is chosen. ◦ Weighted round-robin—Use WRR, which balances flows across paths proportional to their available bandwidth. This is the default connection selection method. To determine a circuit's available bandwidth, the bandwidth consumption of each logical interface is measured periodically. In order to calculate the remaining bandwidth on each access circuit, the VOS traffic-steering software uses a reference bandwidth. For the reference bandwidth, the VOS software considers the CoS shaper rate. If no shaper rate is present, the VOS software considers the interface's uplink and downlink bandwidths (for a logical interface, these are the physical interface's uplink and downlink bandwidths). Then the VOS software assigns a weight to each path based on the bandwidth available on the access circuit. Here are two examples of how WRR works. First, let's say that two circuits, WAN1 and WAN2, are both the highest-priority SLA-compliant paths. WAN1 is a 10-Mbps link that is currently using 8 Mbps, and WAN2 is a 5-Mbps link using 1 Mbps. WAN1 has 2 Mbps of available capacity, and WAN 2 has 4 Mbps, so load balancing would be performed between the WAN1 and WAN2 circuits in the ratio of 2:4, or 1:2. In a second example, which considers logical interfaces, let's say we have two logical WAN interfaces, WAN1 on vni-0/0.100 and WAN2 on vni-0/0.200. The WAN1 vni-0/0.100 logical interface has a configured shaping rate of 100

	Mbps, and the WAN2 vni-0/0.200 logical interface has a configured shaping rate of 150 Mbps. If the current circuit utilization of vni-0/0.100 is 60 Mbps and of vni-0/0.200 is 70 Mbps, the remaining capacity is 40 Mbps and 80 Mbps, respectively. So load balancing would be performed between the vni-0/0.100 and vni-0/0.200 logical interfaces in the ratio of 40:80, or 1:2. ◦ High-available bandwidth—Use the circuit with the highest available bandwidth. Continuing with the example in the previous bullet, because the available bandwidth on WAN2 is higher, this link would be used. ◦ Path weighted round-robin—(For Releases 21.2.1 and later.) Use the monitored available bandwidth as the reference bandwidth for the WRR connection selection method. To determine the reference bandwidth, the traffic-steering software dynamically monitors and periodically computes the available path bandwidth across all paths towards the remote site, and it maintains a historical maximum of the monitored available bandwidth for each path over a period of time. Then the traffic-steering software load-balances the traffic across available paths using either WRR or the path that has the most available bandwidth. If you have not configured a bandwidth monitor, the software considers the configured uplink or downlink path bandwidth for traffic steering. Specifically, for the path uplink bandwidth, the software considers the local site's minimum uplink bandwidth and the remote site's minimum downlink bandwidth, and for the path downlink bandwidth, the software considers the local site's minimum downlink bandwidth and the remote site's minimum uplink bandwidth. To enable dynamic monitoring, you configure a speed-test server. Note that you should use this connection selection method only in hub-and-spoke topologies. Do not use it for full-mesh topologies. For more information, see [Configure Layer 3 SD-WAN Traffic Steering Based on Available Bandwidth](). ◦ Path high-available bandwidth—(For Releases 21.2.1 and later.) Use the monitored available bandwidth as the reference bandwidth for the high-available bandwidth connection selection method. To determine the reference bandwidth, the traffic-steering software dynamically monitors and periodically computes the available path

	bandwidth across all paths towards the remote site, and it maintains a historical maximum of the monitored available bandwidth for each path over a period of time. Then the traffic-steering software load-balances the traffic across available paths using either WRR or the path that has the most available bandwidth. If you have not configured a bandwidth monitor, the software considers the configured uplink or downlink path bandwidth for traffic steering. Specifically, for the path uplink bandwidth, the software considers the local site's minimum uplink bandwidth and the remote site's minimum downlink bandwidth, and for the path downlink bandwidth, the software considers the local site's minimum downlink bandwidth and the remote site's minimum uplink bandwidth. To enable dynamic monitoring, you configure a speed-test server. Note that you should use this connection selection method only in hub-and-spoke topologies. Do not use it for full-mesh topologies. For more information, see Configure Layer 3 SD-WAN Traffic Steering Based on Available Bandwidth. *Default:* Weighted round-robin
Recompute Timer	Enter how often to re-evaluate the SLA-compliance state of all paths. If the re-evaluation identifies an SLA violation on a circuit, the traffic is switched to a different circuit. *Range:* 5 through 1800 seconds *Default:* 300 seconds
Path Reconsider Interval	Enter a time after which an SLA-violated link is reconsidered for forwarding audio, video, and voice packets that are being steered based on a MOS score. *Range:* 60 through 1800 seconds *Default:* 60 seconds
SLA Violation Action	Select the action to take if no paths towards the destination branch meet the SLA requirements associated with the forwarding profile:

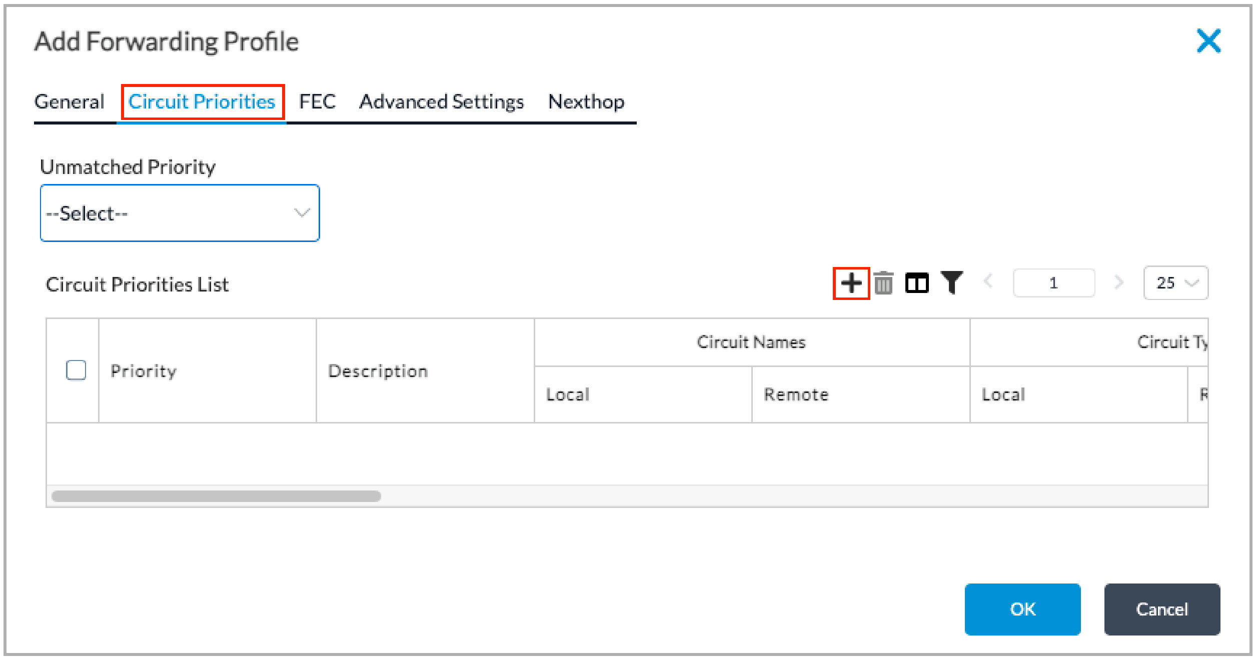
	◦ Drop—Drop the traffic. Forwarding resumes only when an SLA-compliant path becomes available. ◦ Forward—Continue to forward traffic on SLA-violated paths. This is the default. ◦ Throttle Low Priority Traffic—This option is not used. *Default:* Forward
Load Balancing Option	Select how to load-balance a flow of traffic when two or more paths have the same highest priority. All packets in a flow are directed to the same path. ◦ Per Flow—Load-balance the traffic flows across all eligible paths. This is the default. Per-flow load-balancing can increase the total throughput for an application when multiple paths of the same type are present. ◦ Per Packet—Load-balance the packets in a traffic flow among the paths at the current highest priority level. *Default:* Per Flow
Header Compression (Group of Fields)	Header compression provides a tunnel-free bandwidth-saving method by omitting portions of the inner-IPv4/v6, UDP/TCP, ESP, GRE, and VXLAN headers that remain static during a flow's lifetime.
◦ Level	Select the compression level: ◦ Low—Low can be used in cases where both CPU performance and bandwidth usage is minimal ◦ High—High can be used in cases where bandwidth usage is more important than CPU performance
◦ Skip HMAC	Click this option to skip hash-based message authentication code (HMAC). You can skip HMAC in selected in cases in which the traffic is directed towards an external encryption device, such as a High Assurance Internet Protocol Encryptor (HAIPE) device.
Replication (Group of Fields)	Replication is an advanced SD-WAN traffic-steering feature. For more information, see Configure Replication for SD-WAN Traffic Steering.

◦ Enable	Click to enable packet replication. *Default:* Replication is disabled
◦ Replication Factor	For each ingress packet, define the number of egress packets to send. *Range:* 2 through 4
◦ Start When	Select when to start replication automatically: ◦ Always ◦ SLA violated—When all available paths do not meet configured SLA threshold
◦ Stop When	Click to enable using a circuit utilization threshold value to stop packet replication.
◦ Circuit Utilization	When you enable Stop When, enter the circuit utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization exceeds this threshold value, packet replication stops automatically. For Releases 20.2.1 and later, packet replication stops when the transmit circuit utilization of any link that is used for replicating packets exceeds the configured threshold. *Range:* 1 through 100 percent
Evaluate Continuously	Click to to move a traffic flow off a non-compliant path at the recompute timer interval (by default, 300 seconds). (By default, an existing traffic flow remains on the same path until the flow ends, even if the path becomes SLA non-compliant.) Enabling this option is recommended for real-time applications, such as voice and video, to allow a traffic flow to change to a better path if the original path is no longer SLA-compliant. When traffic is moved off an SLA-non-compliant path, it can lead to a thundering-herd effect in which the

	moved traffic causes the second path to go out of compliance, and then the traffic is moved back to the first path. To avoid this problem, enable both Evaluate Continuously and Gradual Migration (on the Advanced Settings tab). Doing this allows traffic flows to move gradually from the original path to the new path over multiple recomputation timer cycles. Gradually moving the flows reduces the load on the original path, mitigating the SLA degradation, so that other flows do not have to move. Flows that move to a new path remain on that path as long as it is SLA-compliant. *Default:* Disabled
Reverse Route Verification	Click to have reverse direction traffic follow routing. By default, VOS devices send reverse-direction SD-WAN traffic back to the same site from which it came (that is, to the source SD-WAN tunnel), even if there is no route to the end host via that tunnel. This reverse path is used as long as the tunnel is up, that is, as long as there is at least one path whose SLA status is Up. For example, consider traffic originating from a client at Site A to a server at Site B. The VOS device at Site B sends reverse direction traffic (Site B to Site A) over the tunnel to Site A,even if the route to the client is not via Site A. Sometimes, however, it may be preferable to have the reverse direction traffic follow routing instead. For this to happen, enable reverse route verification. With this option, the VOS device first verifies that a route exists via the source tunnel before sending reverse-direction traffic over that tunnel. If the route does not exist, the VOS device sends the traffic over the tunnel to which the route points.Continuing with the previous example, if the route to the client via Site A is withdrawn and the route instead points to Site C, Site B sends reverse-direction traffic towards the client via the tunnel to Site C.

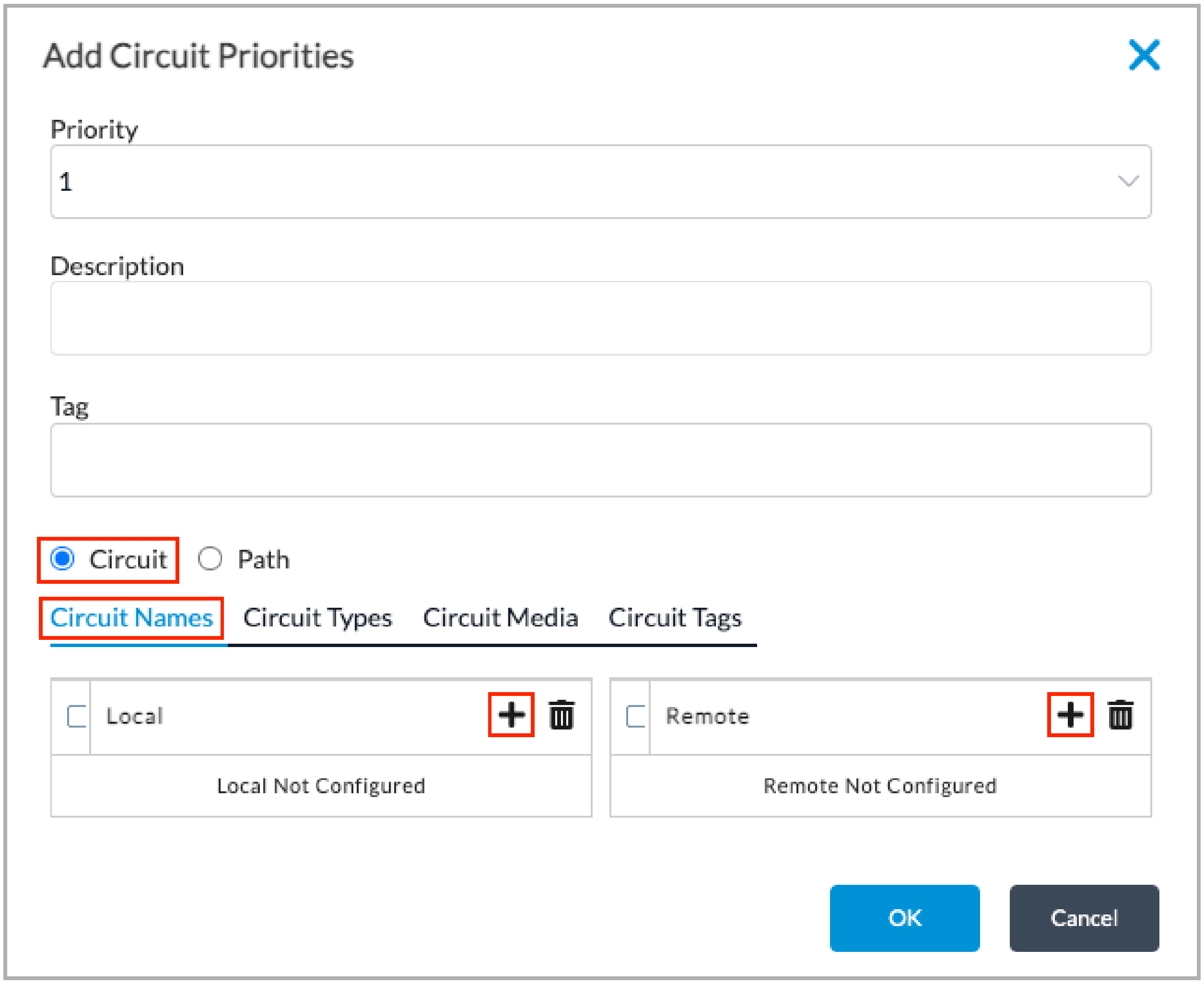
Reorder	Click to reorder packets in a flow that arrive out of order. Packets might arrive out of order when you configure per-packet load balancing or packet replication. *Default:* Enabled
Enable Symmetric Forwarding	Click to enable symmetric traffic forwarding, which determines the path to use for reverse-direction traffic, that is, for traffic returning from the destination branch to originating branch. By default, the return traffic is forwarded symmetrically, that is, on the same path on which the traffic was received. You might want to disable symmetric forwarding for applications where it is beneficial to independently choose the best path in either direction. *Default:* Enabled; that is, return traffic is forwarded symmetrically

6. Select the Circuit Priorities tab to configure circuit properties for local and remote clients and enter the following information.



Field	Description
Unmatched Priority	Assign to paths that are not configured explicitly. The options are: ◦ A value from 1 through 14. For example, if you select the value 2, any path that is not configured in the forwarding profile has a priority of 2. ◦ Avoid—The circuit is configured as one to be avoided. An avoided circuit is not used even if it is the only available path. If the only available paths are configured as avoid, traffic is dropped. ◦ Last Resort—A path to use when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available.
Circuit Priorities List (Table)	Displays the circuit priorities that are already configured.

7. Click the ✚ Add icon to add new circuit properties. In the Add Circuit Priorities popup window, enter information for the following fields.



Add Circuit Priorities

Priority: 1

Description:

Tag:

● Circuit ○ Path

□ Local
Local Not Configured

□ Remote
Remote Not Configured

Field	Description
Priority	Select the priority level to assign to circuits. This value defines the preference for WAN paths between the local branch and a remote branch or branches. For Releases 22.1.1 and later, 17 circuit priority levels are available, 1 through 15, Avoid, and Last Resort. For Releases 21.2 and earlier, 10 circuit priority levels are available, 1 through 8, Avoid, and Last Resort. For the numeric priorities, priority 1 is the most preferred and priority 15 is the least preferred. If you assign the same circuit priority value to two or more WAN paths, traffic is load-balanced among the paths. For example, on a VOS device that has WAN links to MPLS and to the internet, to direct all SD-WAN traffic to the MPLS link, you set a higher priority for the MPLS circuit and a lower priority for the internet link. If you do not configure a circuit priority value for a path, the path is assigned to the lowest priority level and so becomes the least preferred path. If the forwarding profile defines SLA requirements, new traffic flows on the circuit are sent on the WAN path with the highest priority that meets the SLA criteria. If a path does not meet the SLA requirements, it is demoted to the SLA-violated priority. The path-selection logic then tries to find other paths that have a higher priority and that comply with the SLA. At any given time, a path can be assigned one of the following priorities, which are listed in priority order from most preferred to least preferred: ◦ 1 through 15 (for Releases 22.1.1 and later); 1 through 8 (for Releases 21.2 and earlier)—The path is SLA compliant, and its run-time priority is the same as its configured priority. ◦ If a path is not assigned to any priority and an unmatched priority is not selected, the path is assigned a priority of 15 (for Releases 22.1.1 and later) or 8 (for Releases 21.2 and earlier), which is the default priority. ◦ SLA-Violated—The path fails to meet the SLA

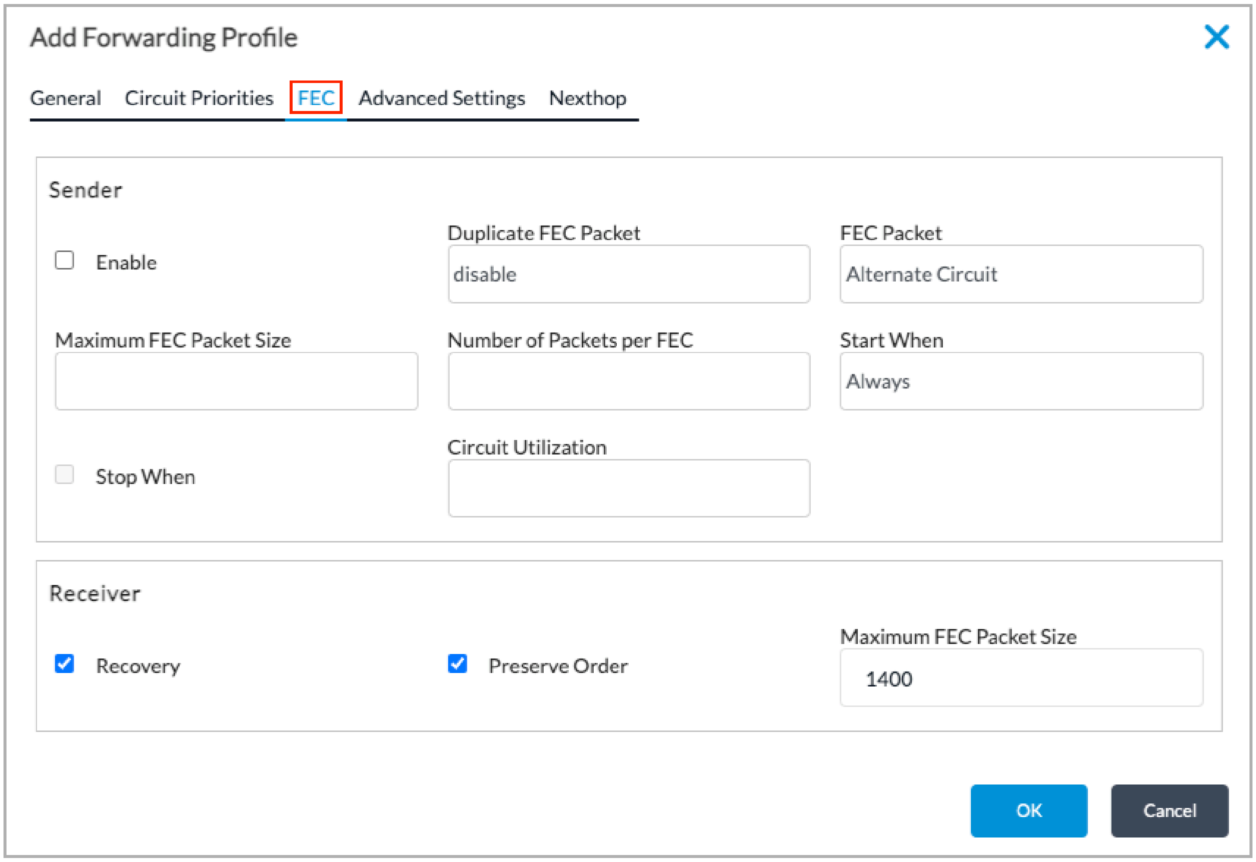
	compliance metrics. ◦ Last Resort—A path to use when all other paths are down. As an example, you can configure a last resort so as not to use LTE paths when other paths are available. ◦ Avoid—The circuit is configured as one to be avoided. An avoided circuit is not used even if it is the only available path. If the only available paths are configured as avoid, traffic is dropped. ◦ 15—All unused circuits have this priority, which is the lowest priority. The SLA for these circuits uses low delay, low loss, low jitter, low forwarding loss, and low reverse loss, and the path score is calculated based on loss, delay, and jitter on the circuits with lower latency or loss. *Values:* 1 through 15, Avoid, Last Resort (for Releases 22.1.1 and later); 1 through 8, Avoid, Last Resort (for Releases 21.2 and earlier)
Description	Enter a text description for the circuit priority level.
Tag	Enter a keyword or phrase that allows you to filter the priority level. This is useful when you have many levels and want to view those that are tagged with a particular keyword.
Circuit	Select to configure circuit priorities for local and remote clients.
Circuit Names (Tab)	Configure the WAN circuits, by circuit name, to assign the priority level. For each WAN circuit, you specify a local name and a remote name for the path between two branches. Circuits typically have names such as WAN1 and WAN2. If you specify a name only for the local branch, the name for the remote branch is treated as a wildcard. The same is true if you specify a circuit name only for the remote branch.
◦ Local	Click the + Add icon, and then select a WAN circuit name on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit name on the remote branch.
Circuit Types (Tab)	Configure the circuits, by circuit type, to assign the priority level. For each WAN circuit, you specify a local

	type and a remote type for the path between two branches. Circuits typically have types such as broadband, IP, and MPLS. If you specify a type only for the local branch, the type for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the +Add icon, and then select a WAN circuit type on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit type on the remote branch.
Circuit Media (Tab)	Configure the circuits, by circuit media, to assign the priority level. For each WAN circuit, you specify a local media and a remote media for the path between two branches. Circuits typically have media such as cable, DSL, Ethernet, LTE, T1, and T3. If you specify a media only for the local branch, the media for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the + Add icon, and then select a WAN media on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit media on the remote branch.
Circuit Tags (Tab)	Configure the circuits, by circuit tags, to assign the priority level. For each WAN circuit, you specify a local tag and a remote tag for the path between two branches. Circuit tags are text strings. If you specify a tag only for the local branch, the tag for the remote branch is treated as a wildcard, and vice versa.
◦ Local	Click the + Add icon, and then select a WAN circuit tag on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit tag on the remote branch.
Path	Select to configure path-based circuit priorities for local and remote clients.
Path Names (Tab)	Configure the WAN circuits, by path name, to assign the priority level. For each WAN circuit, you specify a local name and a remote name for the path between

	two branches. Circuits typically have names such as WAN1 and WAN2. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Click the + Add icon, and then select a WAN circuit name on the local branch.
◦ Remote	Click the + Add icon, and then select a WAN circuit name on the remote branch.
Path Types (Tab)	Configure the circuits, by path type, to assign the priority level. For each WAN circuit, you specify a local type and a remote type for the path between two branches. Circuits typically have types such as broadband, IP, and MPLS. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Select a WAN circuit type on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit type on the remote branch, and then click the + Add icon.
Path Media (Tab)	Configure the circuits, by path media, to assign the priority level. For each WAN circuit, you specify a local media and a remote media for the path between two branches. Circuits typically have media such as cable, DSL, Ethernet, LTE, T1, and T3. You cannot leave either field empty. To specify a wildcard for a field, select Any.
◦ Local	Select a WAN media on the local branch , and then click the + Add icon.
◦ Remote	Select a WAN circuit media on the remote branch, and then click the + Add icon.
Path Tags (Tab)	Configure the circuits, by path tag, to assign the priority level. For each WAN circuit, you specify a local tag and a remote tag for the path between two branches. Path tags are text strings. You cannot leave either field empty. To specify a wildcard for a field, select Any.

◦ Local	Select a WAN circuit tag on the local branch, and then click the + Add icon.
◦ Remote	Select a WAN circuit tag on the remote branch, and then click the + Add icon.

8. Select the FEC tab to configure forward error correction. Enter information for the following fields. Note that FEC is an advanced SD-WAN traffic-steering feature. For more information, see Configure Forward Error Correction for SD-WAN Traffic Steering.



Sender

☐ Enable

Duplicate FEC Packet: disable

FEC Packet: Alternate Circuit

Maximum FEC Packet Size:

Number of Packets per FEC:

Start When: Always

☐ Stop When

Circuit Utilization:

Receiver

☑ Recovery

☑ Preserve Order

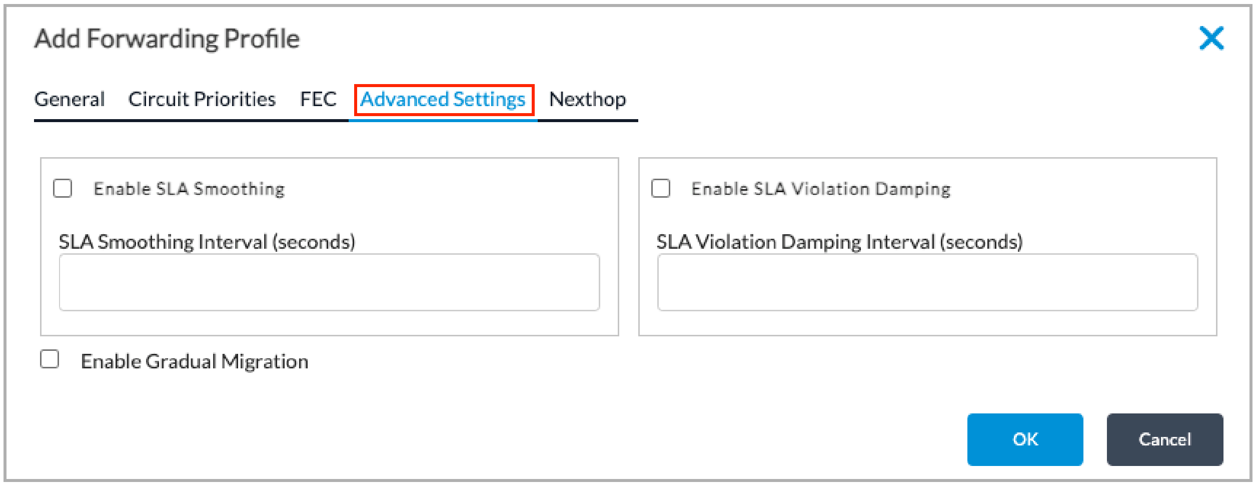
Maximum FEC Packet Size: 1400

Field	Description
Sender (Group of Fields)	
◦ Enable	Click to enable FEC. *Default:* Disabled
◦ Duplicate FEC Packet	Select how to duplicate FEC parity packets: ◦ Alternate circuit—Duplicate FEC parity packets and send them on a WAN interface that is not an interface on which data packets are transmitted. ◦ Disabled—Do not duplicate FEC parity packets. This is the default. ◦ Same circuit—Duplicate FEC parity packets and send them on the same WAN interface used to transmit data packets. *Default:* Disabled
◦ FEC Packet	Select the circuit on which to send FEC parity packets: • Alternate circuit—Send FEC parity packets on a WAN interface that is not an interface on which data packets are transmitted. This is the default. If an alternate circuit is unavailable, FEC parity packets are sent on the same circuit as data packets. • Same circuit—Send FEC parity packets on the same WAN interface used to transmit data packets. *Default:* Alternate circuit
◦ Maximum FEC Packet Size	Enter the maximum packet size of FEC parity packet that the sender can send. This value is used to recover lost packets. If the maximum packet size you configure (referred to as *n*) is less than or equal to the data packet size, the recovered packet contains the first *n* bytes of the original packet. *Range:* 100 through 10000 bytes *Default:* 1400 bytes

◦ Number of Packets per FEC	Enter the number of data packets after which an FEC packet is generated and sent to the peer branch. The generated FEC parity packet can recover a packet on the peer branch only if there is one lost packet in the specified number of packets per FEC. *Range:* 1 through 32 *Default:* 4
◦ Start When	Select when to start sending FEC parity packets: ◦ Always ◦ SLA violated—When all available paths are SLA violated
◦ Stop When	Click to set the circuit utilization threshold at which to stop sending FEC parity packets.
◦ Circuit Utilization	Enter the utilization threshold at which replication stops automatically. Specify this as a percentage of the total circuit bandwidth. When the circuit utilization of the links used for data packets or FEC parity packet transmission exceeds this threshold, FEC stops. For Releases 20.2.1 and later, FEC stops when the transmit circuit utilization of any link that is used for replicating the packet exceeds the configured threshold. For example, if you configure the circuit utilization threshold as 80 percent and there are two WAN links—broadband and MPLS—then at any given time if the transmit circuit utilization threshold on either the broadband or MPLS circuit exceeds 80 percent, FEC stops on both circuits. *Range:* 1 through 100 percent *Default:* None
Receiver (Group of Fields)	
◦ Recovery	Click to enable packet recovery after receiving FEC packets.

	Default: Receiver packet recovery is enabled.
◦ Preserve Order	Click to reorder out-of-order packets and forward them in their original order. *Default:* Packet reordering is enabled.
◦ Maximum FEC Packet Size	Enter the maximum packet size of FEC parity packet that the receiver can receive. This value is used to recover lost packets. If the maximum packet size you configure (referred to as *n*) is less than or equal to the data packet size, the recovered packet contains the first *n* bytes of the original packet. *Range:* 100 through 10000 bytes *Default:* 1400 bytes

9. Select the Advanced Settings tab to define values for SLA smoothing, damping, and migration. Enter information for the following fields.


Add Forwarding Profile
General
Circuit Priorities
FEC
Advanced Settings
Nexthop
□ Enable SLA Smoothing
SLA Smoothing Interval (seconds)
□ Enable SLA Violation Damping
SLA Violation Damping Interval (seconds)
□ Enable Gradual Migration
OK
Cancel

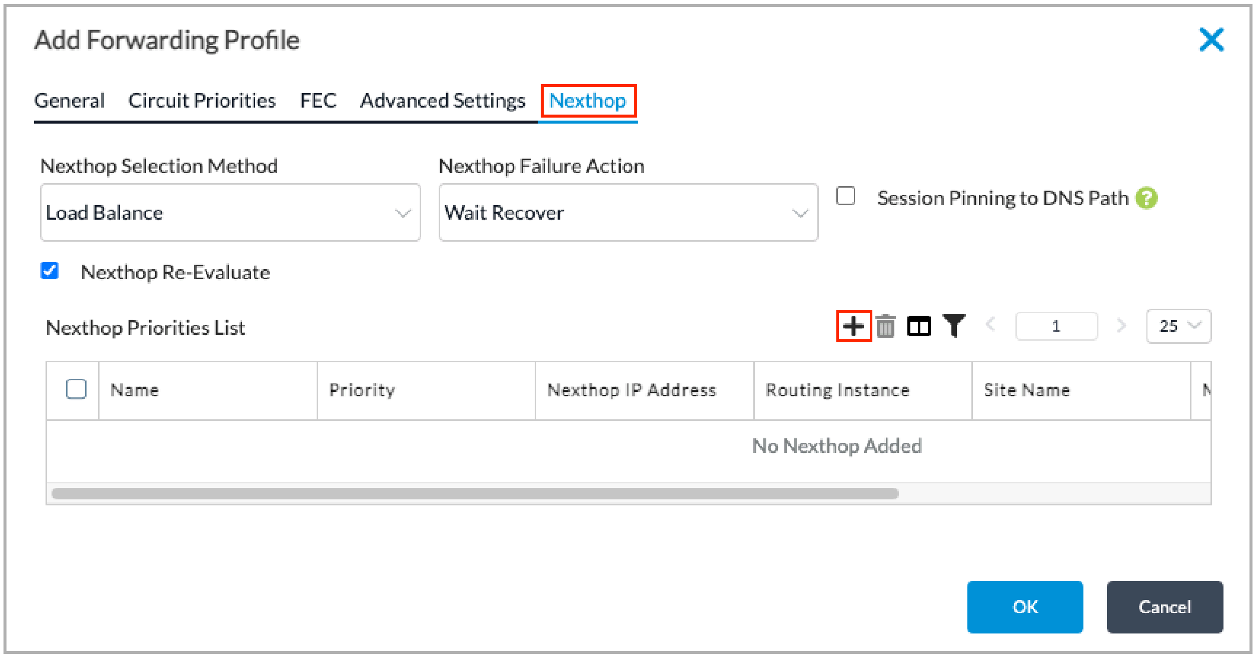
Field	Description
Enable SLA Smoothing	Click to average the SLA metrics over the smoothing interval instead of the recompute interval. If you do not enable SLA smoothing, the SLA compliance of a path is checked every recompute interval. The SLA for a path is recomputed regularly to determine whether a path is SLA compliant. SLA smoothing is a mechanism to prevent a path from frequently oscillating between an SLA-compliant and an SLA-non-compliant state each time the SLA is recomputed. Configuring SLA smoothing is useful for loss-based SLAs, where the loss measurement accuracy depends on the number of packet samples. When you configure SLA smoothing, you define a smoothing interval that is used to minimize the oscillations. The SLA smoothing interval is used in conjunction with the path recomputation interval to determine a path's SLA compliance. For a path that is currently SLA-compliant, the average metrics over the last recompute interval are used to determine compliance. For a path that is currently non-compliant, the average metrics over the last smoothing interval are used. This scheme allows a fast reaction to a network impairment, which can occur in one recompute interval, and it provides a slow and cautious return to the compliant state because the metrics smoothed over the last smoothing interval are used. The default SLA recomputation interval is 300 seconds, which is a conservative interval that is large enough so that you likely would not want or need to configure smoothing. However, if you want to configure an aggressive recomputation interval, you might change the recomputation interval to a value between 5 and 20 seconds. Then, if you configure SLA smoothing and use the default smoothing interval, smoothing is done every 120 seconds. If you change the smoothing interval, it must be larger than

	the recomputation interval. For example, consider a case where the recomputation interval is 10 seconds and the smoothing interval is 60 seconds. If a path is SLA-compliant, the SLA metrics are averaged over the last 10 seconds to determine SLA compliance. If a path is SLA non-compliant, the SLA metrics are averaged over the last 60 seconds to determine SLA compliance. Here, the SLA smoothing allows 50 additional seconds for network conditions to improve before the branch device has to recompute an SLA-compliant path. *Default:* Disabled
SLA Smoothing Interval	Enter the SLA smoothing interval, in seconds. Range: 10 through 300 seconds Default: 120 seconds
Enable SLA Violation Damping	Select to associate the recompute interval value with the damping interval value. If you do not enable SLA violation damping, the SLA compliance of a path is checked every recompute interval. Damping is another mechanism to prevent a path from frequently oscillating between an SLA-compliant and an SLA-non-compliant state each time the SLA is recomputed. The damping interval defaults to 3 times the path recomputation interval. If you change the default damping value, it must be larger than the recomputation interval. With damping, a path moves from an SLA-compliant and an SLA-non-compliant state based on the average SLA metrics over the last recompute interval. If the path is in an SLA-non-compliant state, it is forcibly held in that state for the damping interval even if network conditions have improved and the path is otherwise SLA-compliant. For example, if the

	recomputation interval is 10 seconds, a non-damped path can oscillate between compliant and non-compliant state every 10 seconds. However, if you enable damping and set the damping interval to 60 seconds, the path moves to non-compliant state 10 seconds after network conditions degrade, and remains in that state for at least 60 seconds. Only after 60 seconds are the path metrics evaluated again to determine whether the path is once again SLA-compliant. *Default:* Disabled
SLA Violation Damping Interval	Enter the SLA violation damping interval, in seconds. *Default:* 3 times the recompute interval
Enable Gradual Migration	Click to enable gradual migration. When traffic is moved off an SLA-non-compliant path, it can lead to a thundering-herd effect in which the moved traffic causes the second path to go out of compliance, and then the traffic is moved back to the first path. To avoid this problem, enable both Evaluate Continuously (on the General tab) and Gradual Migration. Doing this allows traffic flows to move gradually from the original path to the new path over multiple recomputation timer cycles. Gradually moving the flows reduces the load on the original path, mitigating the SLA degradation, so that other flows do not have to move. Flows that move to a new path remain on that path as long as it is SLA-compliant. *Default:* Disabled

10. Select the Next Hop tab to define next-hop parameters and priorities for DIA traffic. The next hop does not need to be an SD-WAN interface. Enter information for the following fields.

    Note: These parameters and priorities do not apply to SD-WAN traffic.



Add Forwarding Profile

Nexthop Selection Method: Load Balance

Nexthop Failure Action: Wait Recover

☐ Session Pinning to DNS Path

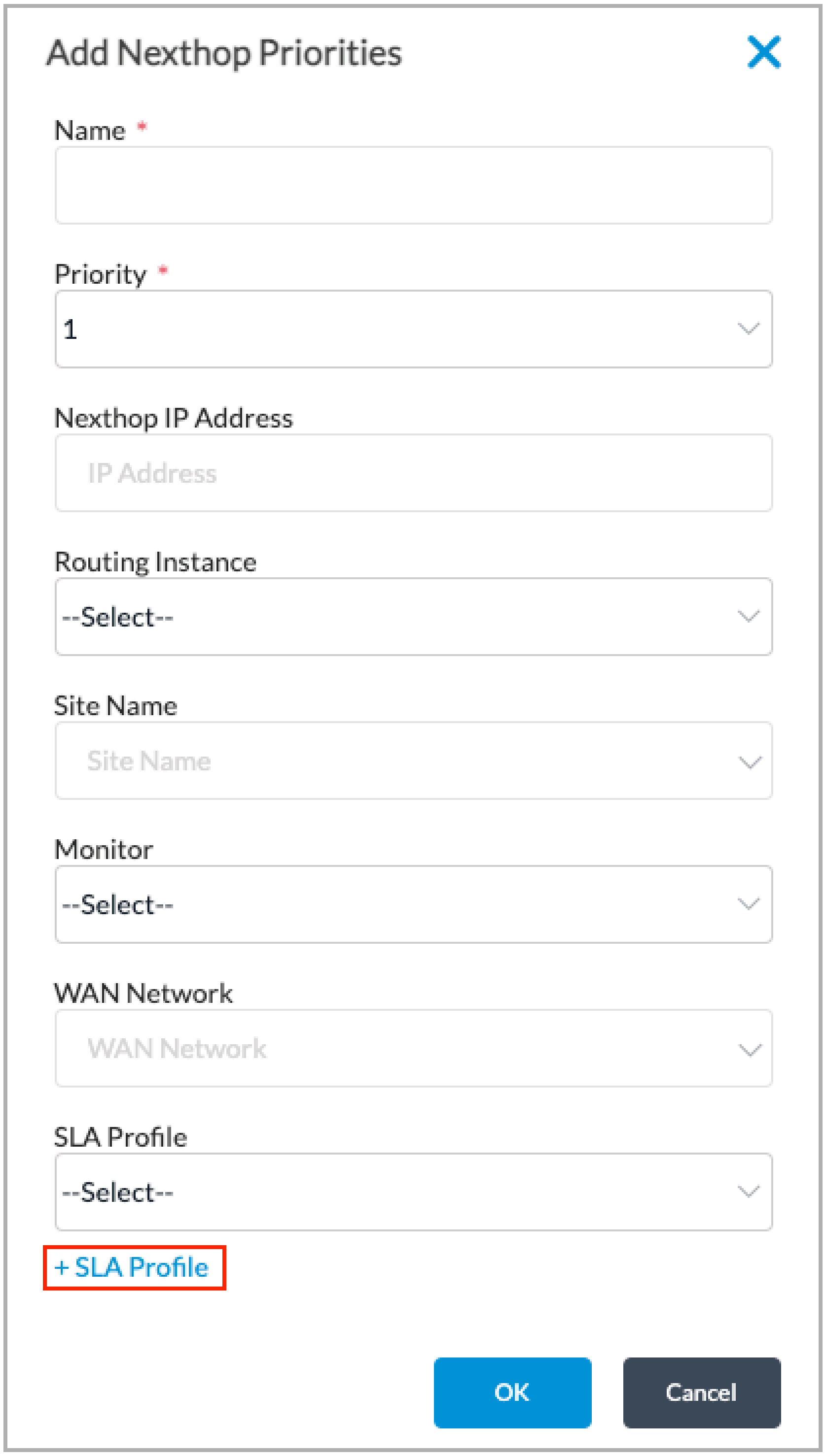
☑ Nexthop Re-Evaluate

Nexthop Priorities List

☐	Name	Priority	Nexthop IP Address	Routing Instance	Site Name	N
			No Nexthop Added			

Field	Description
Next-Hop Selection Method	Select the method for choosing the next hop for DIA traffic: ◦ Automatic—Choose the next hop that provides the best performance based on passively collected performance metrics. ◦ High-Available Bandwidth—(For Releases 21.2.1 and later.) Use high-available bandwidth to load-balance DIA traffic among equal priority next hops. If any one of the next hops is not an outgoing WAN Network type (as specified in the WAN Network field of the Add Next Hop Priorities screen below), equal-cost load balancing is used as the selection method. ◦ Load Balance—Perform equal-cost load balancing between all active next hops at the highest priority level using SLA monitoring and SLA-based path selection metrics. ◦ Weighted Round-Robin—(For Releases 21.2.1 and later.) Use WRR to load-balance DIA traffic between equal priority next-hops. If any one of the next hops is not an outgoing WAN Network type (as specified in the WAN Network field of the Add Next Hop Priorities screen below), equal-cost load balancing is used as the selection method.
Next-Hop Failure Action	Select the action to take when none of the configured next hops is deemed reachable: ◦ Failover—Fall back to routing-based path selection. ◦ Next rule—Fail over to the next matching rule. ◦ Wait recover—Wait for this rule to recover at least one next hop.
Session Pinning to DNS Path	Select to pin all sessions between a client and server to the path of the DNS query that resolved the server
Nexthop Re-Evaluate	Select to enable nexthop re-evaluation.

11. In the Next-Hop Priorities List table, click the ✚ Add icon to define the path priority levels for paths to the next hop. In the Add Next-Hop Priorities popup window, enter information for the following fields.



Add Nexthop Priorities

Name *

Priority * 1

Nexthop IP Address: IP Address

Routing Instance: --Select--

Site Name: Site Name

Monitor: --Select--

WAN Network: WAN Network

SLA Profile: --Select--

Field	Description
Name	Enter a name for the next-hop priority level.
Priority	Select a priority value. *Values:* 1 through 15 (for Releases 22.1.1 and later); 1 through 8 (for Releases 21.2.1 and later); 1 through 4 (in earlier releases)
Next-Hop IP Address	Enter the IP address of the next hop.
Routing Instance	Select the routing instance to use to reach the next hop.
Site Name	Select the name of the next-hop site to use to reach the next hop.
Monitor	Select the monitor type.
WAN Network	Select the type of WAN network to use to reach the next hop.
SLA profile	Select the SLA profile to use for the path. Click + SLA Profile to add a new SLA profile.
+ SLA Profile	Click to add an SLA profile. For more information, see Configure SLA Profiles for SD-WAN Traffic Steering.

12. Click OK.

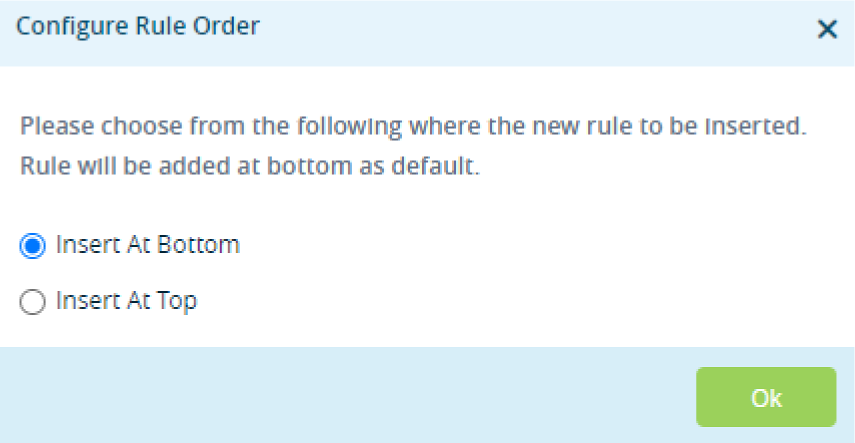
Configure Layer 2 or Layer 3 SD-WAN Traffic Steering Policy

To enable a Layer 2 or Layer 3 SD-WAN traffic-steering forwarding profile, you associate the forwarding profile with an SD-WAN policy rule when you configure the enforcement action for the rule.

To associate an SD-WAN traffic-steering forwarding profile with a policy rule:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. To configure a policy rule for a Layer 2 SD-WAN policy, select Configuration > Services > Layer 2 SD-WAN > Policies > Rules. Or, to configure a policy rule for a Layer 3 SD-WAN policy, select Configuration > Services > SD-WAN > Policies > Rules.
3. Click the + Add icon to add a rule.

4. If you have already added one or more rules, the Configure Rule Order popup window displays.
    a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

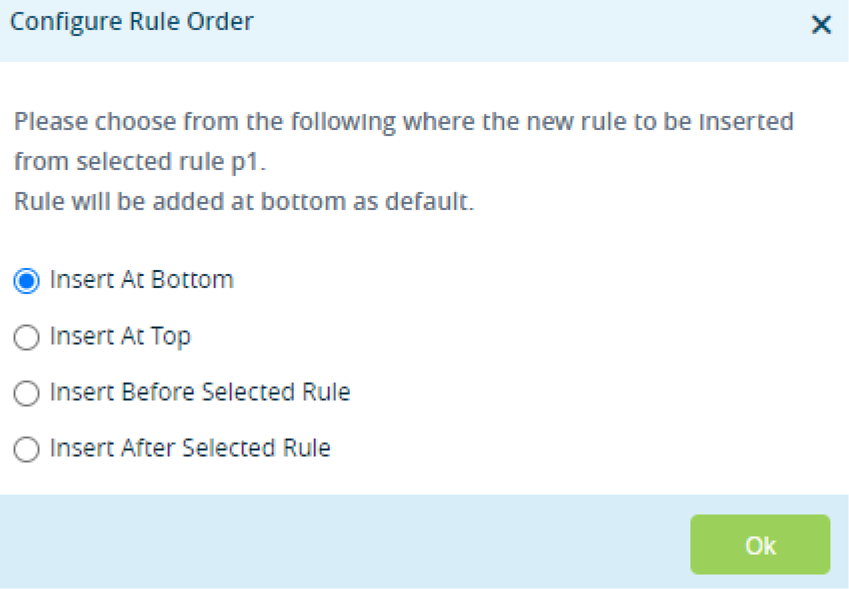


Please choose from the following where the new rule to be inserted.
Rule will be added at bottom as default.

● Insert At Bottom

○ Insert At Top

    b. If you select a rule and then click the + Add icon, the Configure Rule Order popup window displays the following options:



Please choose from the following where the new rule to be inserted from selected rule p1.
Rule will be added at bottom as default.

● Insert At Bottom

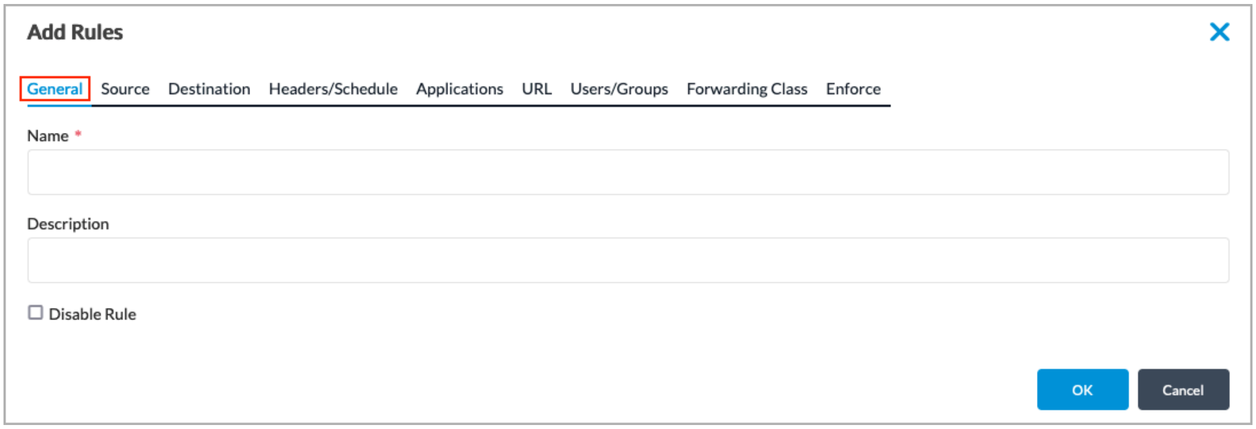
○ Insert At Top

○ Insert Before Selected Rule

○ Insert After Selected Rule

    c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
    d. Click OK.

5. The Add Rules popup window displays.



Add Rules

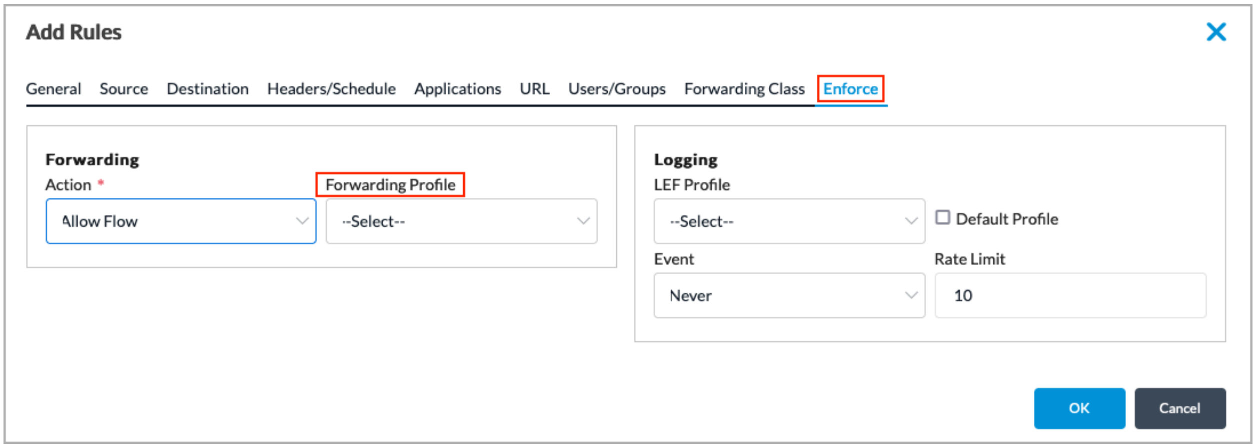
General | Source | Destination | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | Enforce

Name *

Description

☐ Disable Rule

6. Configure the policy rule parameters, as described in Configure SD-WAN Policy.
7. Select the Enforce tab.



Add Rules

General | Source | Destination | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | Enforce

Forwarding

Action *: Allow Flow

Forwarding Profile: --Select--

Logging

LEF Profile: --Select--

☐ Default Profile

Event: Never

Rate Limit: 10

8. In the Forwarding Profile field, select the SD-WAN traffic-steering forwarding profile to apply to traffic that matches the rule.
9. Configure other enforcement parameters, as described in Configure SD-WAN Policy.
10. Click OK.

Configure Application Identification Properties for Traffic Sent over Layer 2

For Releases 21.2.1 and later.

Application identification (AppID), which is always running on VOS devices, inspects the Layer 7 (application) payload of the traffic in a flow to determine the application so that it can then apply a Layer 2 application-specific policy to the flow. Application identification can identify most applications other than basic ones, such as ICMP and DNS, only after a few packets for the session have been received. The result is that policy, which is often used to override route table–based routing and divert the traffic to a different path, is not applied to the first few packets in a flow, and so a non-optimal path may be selected for the flow.

To correctly identify the application from the first packet and thus to have policy apply to all packets in a flow, you configure a property of application identification called application detection. Application detection allows rapid identification of a flow's application by creating an application cache, which is used to identify the application in the first packet, instead of waiting for the application identification software to do so.

The VOS application cache maps IP address–port pairs to applications and URL categories.

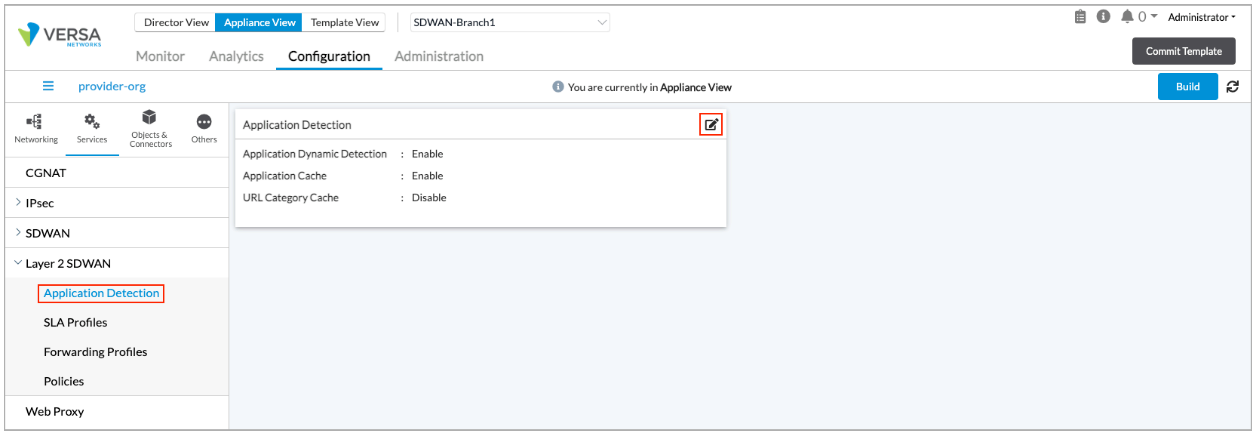
The domain name application cache times out after 5 days (7200 minutes). You cannot change this value.

Entries are not added to the application cache when the client is connecting to a proxy or when the session is being processed by an HTTP/HTTPS web proxy. Application caching is enabled by default, and URL category caching is disabled by default.

You configure application detection globally for each tenant. You cannot configure them for individual applications.

To configure application detection parameters:

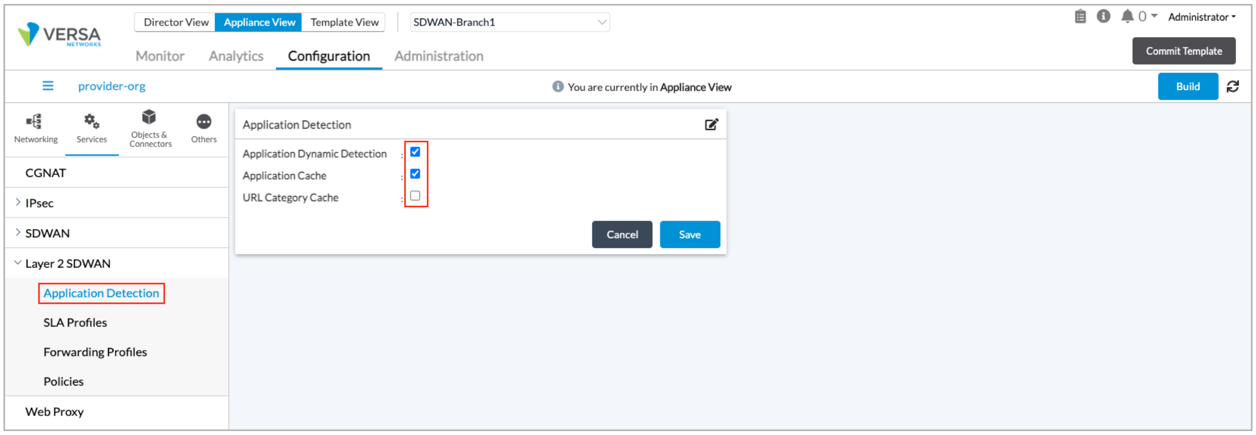
1. In Director view:
    a. Select the Administration in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Layer 2 SD-WAN > Application Detection in the left menu bar. The main pane displays the Application Detection pane.



Application Detection

Application Dynamic Detection : Enable
Application Cache : Enable
URL Category Cache : Disable

4. Click the ✎ Edit icon in the Application Detection pane. In the Application Detection pane, enter information for the following fields.



Application Detection

Application Dynamic Detection ☑

Application Cache ☑

URL Category Cache □

Field	Description
Application Dynamic Detection	Click Enable to dynamically re-evaluate Layer 2 SD-WAN traffic-steering rules when an application or URL category is detected in a traffic flow even if the packet being inspected is not the first packet in the flow. *Default:* Enabled
Application Cache	Click Enable to cache applications associated with server IP address and port numbers. *Default:* Enabled
URL Category Cache	Click Enable to cache URL categories associated with HTTP and HTTPS server IP addresses and port numbers. *Default:* Disabled

5. Click Confirm.

Configure Application Identification Properties for Traffic Sent over Layer 3

Application identification (AppID), which is always running on VOS devices, inspects the Layer 7 (application) payload of the traffic in a flow to determine the application so that it can then apply a Layer 3 application-specific policy to the flow. Application identification can identify most applications other than basic ones, such as ICMP and DNS, only after a few packets for the session have been received. The result is that policy, which is often used to override route table–based routing and divert the traffic to a different path, is not applied to the first few packets in a flow, and so a non-optimal path may be selected for the flow. Additionally, when NAT is involved, the path for the session must be selected on the first packet itself.

To correctly identify the application from the first packet and thus to have policy apply to all packets in a flow, you configure a property of application identification called application detection. Application detection allows rapid identification of a flow's application by creating an application cache, which is used to identify the application and the URL categories in the first packet, instead of waiting for the application identification software to do so. In addition to the application cache, the domain-name application cache is used to identify applications (and URL categories) for domain names.

The VOS application cache maps IP address–port pairs (sometimes referred to as endpoints) and domain names to applications and to predefined and custom URL categories.

By default, dynamic application detection and application caching are enabled. By default, URL category caching is disabled.

You configure application detection and application caching globally for each tenant. You cannot configure them for individual applications. Note, also, that you should never disable application detection.

The previous paragraphs describe the basic application detection features. Releases 20.2 and 21.1 introduce the following enhancements to basic application detection:

- For Releases 20.2 and later, after DNS requests are processed, the application cache maintains entries for all the IP addresses that a domain name resolves to, and for all the applications and URL categories that are known for a domain.
- For Release 20.2 and later 20.*x* releases, entries remain in the application cache for 24 hours, and you cannot change this value. For Releases 21.1 and later, the application cache times out after 5 days (7200 minutes), and you cannot change this value.
- For Releases 21.1 and later, VOS devices automatically perform first-packet identification for SaaS (and other) applications and for DNS requests. No configuration is required. First-packet application identification uses the endpoint information published by the SaaS vendors, which is delivered to the VOS devices via service packages (SPacks). First-packet identification is performed in addition to the using the information application cache, which is gathered when sessions pass through the VOS device. The following paragraphs provide more details about first-packet identification.

For SD-WAN edge devices, detecting applications starting with the first packet is critical for optimum path selection. If an application is not known with the first packet and a non-optimal path is selected for the TCP session, the session's performance is often degraded. For releases prior to Release 21.1, the VOS software uses an application cache to cache the application detected for a session associated with a specific IP address and port. However, the application cache cannot assist in directing the first session to a given destination. Because SaaS vendors now use many IP addresses to serve applications, this limitation has become an issue. First-packet identification addresses this limitation. It allows the SaaS application to be identified starting with the first packet of a session. First-packet identification is also used to identify applications that are making DNS requests, which means that DNS requests can use the same WAN path selection as data sessions.

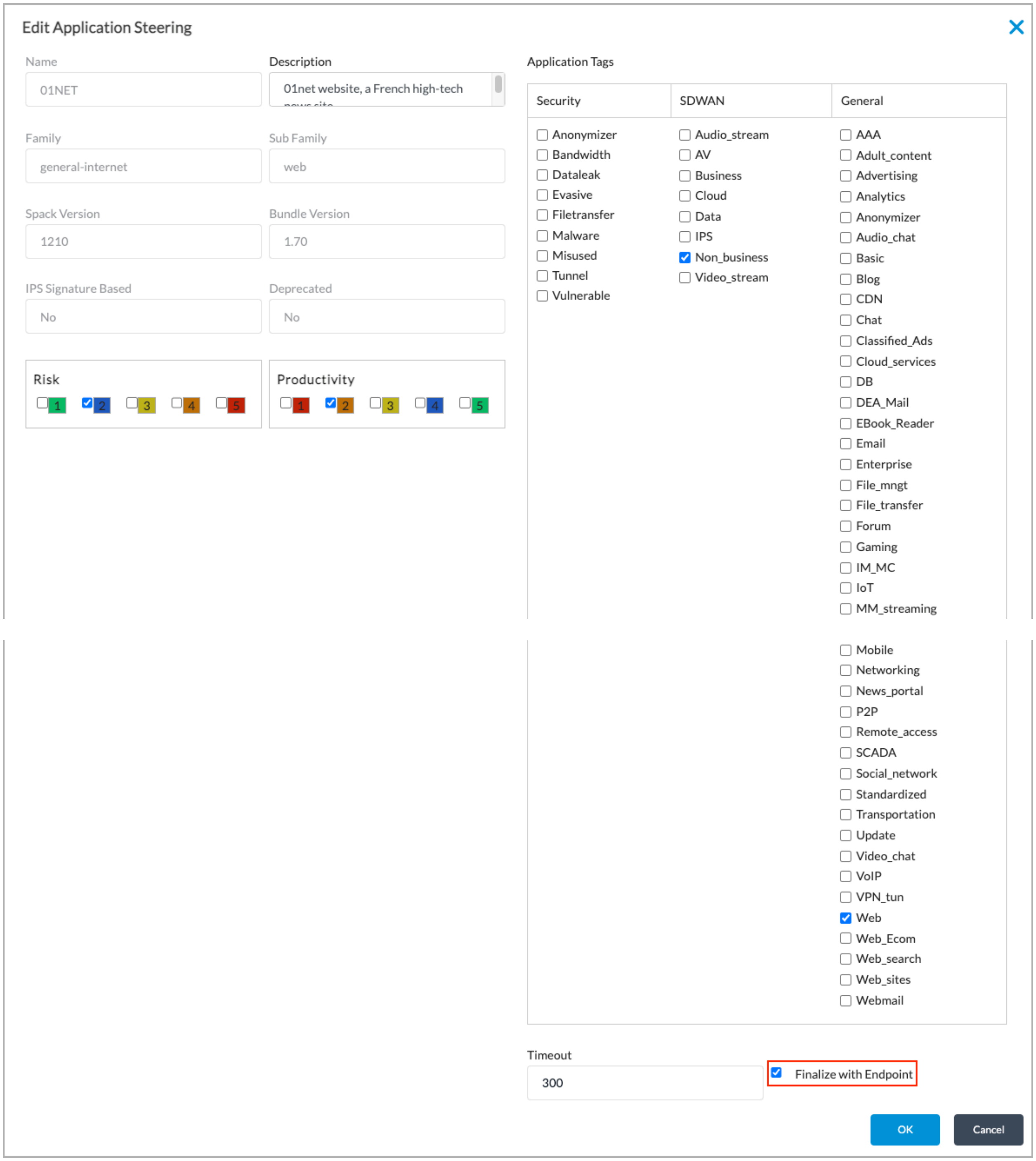
First-packet identification performs WAN path selection for specific applications, both for the DNS sessions and the data sessions, and it allows users to configure firewall rules to create allow lists of SaaS applications using the published IP prefixes and domain names.

Several SaaS providers publish the IP prefixes and domain name patterns for their service endpoints. Examples of endpoint information published by SaaS providers are, for Microsoft Office 365, https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges, and, for Zoom, https://support.zoom.us/hc/en-us/articles/201362683-Network-Firewall-or-Proxy-Server-Settings-for-Zoom. VOS also supports endpoint information published by Okta, Webex, and Salesforce. The latest application endpoint information is included in Versa SPack updates, which are performed dynamically, and so this information is available to VOS devices so that they can identify applications on the first packet. For more information, see Use Security Packages.

VOS devices map the IP prefixes and domain names to the predefined applications for the SaaS application. For example, Microsoft Office 365 endpoints are mapped to the application OFFICE365. The applications are the same predefined applications that you use to configure policies, so you do not need to modify the policy configuration.

The following bullets provide more details about how SaaS application detection using endpoints operates:

- Identify applications for DNS requests and data sessions—For DNS sessions, the database containing the published domain names is used to resolve the domain name, and published IP prefixes are used to identify the application for data sessions. The applications that are identified are the same predefined applications that you use when configuring policies. For example, the published Microsoft Office365 endpoints include the FQDNs outlook.office.com and outlook.office365.com, and the IP addresses13.107.6.152/31, 13.107.18.10/31, and 13.107.128.0/22, with TCP ports 80 and 443. This information allows a DNS request for outlook.office365.com and a TCP session destined to 13.107.128.1 to be mapped to the OFFICE365 application.
- WAN path selection—To select a WAN path for applications, you need to configure SD-WAN policy rules. Because both the DNS requests and the data sessions are mapped to the same applications (on the first packet of session) using the published endpoint information, they both receive the same path selection treatment. To use path selection for DNS requests, you must enable DNS proxy on the VOS device.
- Allow lists for applications using endpoint information—You can create allow lists (sometimes called whitelists) for the SaaS applications using predefined applications. Identifying applications on the first packet of the session helps the VOS software to finalize, or select, the firewall policy to use for the session without having to wait for the deep-packet inspection software to detect the application. For an application for which application identification is to be selected for the firewall policy based on the published endpoint match, you must set the application-specific app-final-with-endpoint option to TRUE. To set this option from the Director GUI, on the Object & Connectors > Predefined > Applications screen for the device, select the application name, and then in the Edit Application Steering popup window, select Finalize with Endpoint.



Edit Application Steering

Name: 01NET

Description: 01net website, a French high-tech news site

Family: general-internet

Sub Family: web

Spack Version: 1210

Bundle Version: 1.70

IPS Signature Based: No

Deprecated: No

Risk: □ 1 ☑ 2 □ 3 □ 4 □ 5

Productivity: □ 1 ☑ 2 □ 3 □ 4 □ 5

Application Tags

Security:

□ Anonymizer
□ Bandwidth
□ Dataleak
□ Evasive
□ Filetransfer
□ Malware
□ Misused
□ Tunnel
□ Vulnerable

SDWAN:

□ Audio_stream
□ AV
□ Business
□ Cloud
□ Data
□ IPS
☑ Non_business
□ Video_stream

General:

□ AAA
□ Adult_content
□ Advertising
□ Analytics
□ Anonymizer
□ Audio_chat
□ Basic
□ Blog
□ CDN
□ Chat
□ Classified_Ads
□ Cloud_services
□ DB
□ DEA_Mail
□ EBook_Reader
□ Email
□ Enterprise
□ File_mngt
□ File_transfer
□ Forum
□ Gaming
□ IM_MC
□ IoT
□ MM_streaming
□ Mobile
□ Networking
□ News_portal
□ P2P
□ Remote_access
□ SCADA
□ Social_network
□ Standardized
□ Transportation
□ Update
□ Video_chat
□ VoIP
□ VPN_tun
☑ Web
□ Web_Ecom
□ Web_search
□ Web_sites
□ Webmail

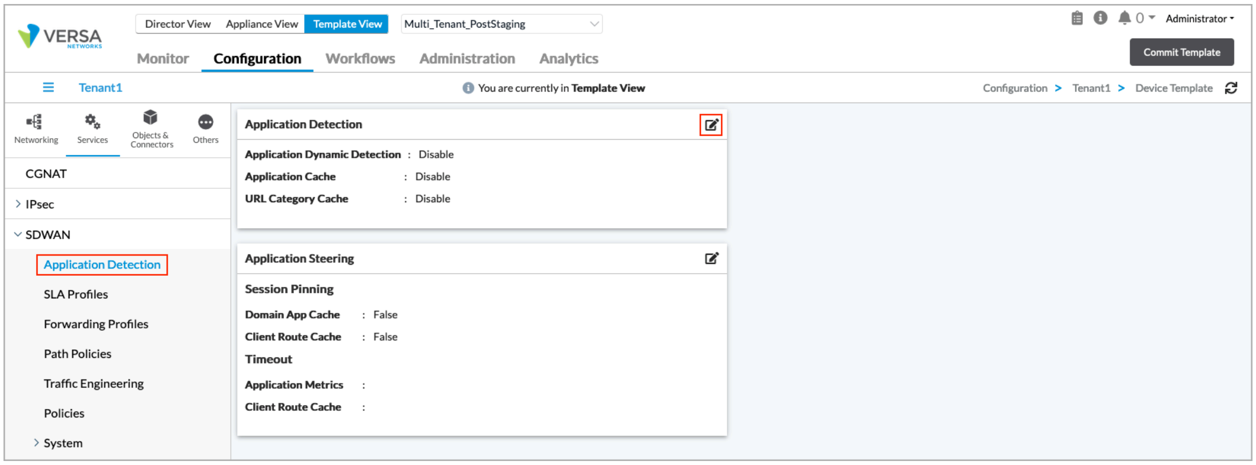
Timeout: 300

☑ Finalize with Endpoint

To configure Layer 3 application detection and application steering parameters:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Application Detection in the left menu bar. The main pane displays the Application Detection and Application Steering panes.



Application Detection

Application Dynamic Detection : Disable
Application Cache : Disable
URL Category Cache : Disable

Application Steering

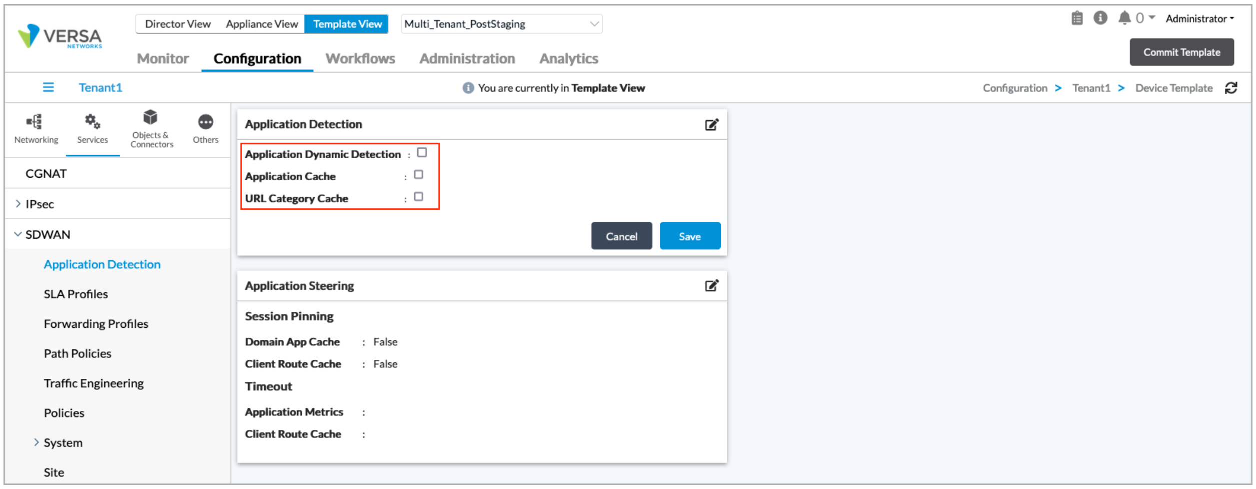
Session Pinning

Domain App Cache : False
Client Route Cache : False

Timeout

Application Metrics :
Client Route Cache :

4. In the Application Detection pane, click the ✎ Edit icon. In the Application Detection pane, enter information for the following fields.



Application Detection

Application Dynamic Detection : □
Application Cache : □
URL Category Cache : □

Application Steering

Session Pinning

Domain App Cache : False
Client Route Cache : False

Timeout

Application Metrics :
Client Route Cache :

Field	Description
Application Dynamic Detection	Click to dynamically re-evaluate SD-WAN traffic-steering rules when an application or URL category is detected in a traffic flow even if the packet being inspected is not the first packet in the flow. *Default:* Enabled
Application Cache	Click to cache applications associated with server IP address and port numbers. *Default:* Enabled
URL Category Cache	Click to cache URL categories associated with HTTP and HTTPS server IP addresses and port numbers. *Default:* Disabled

5. Click Confirm.

6. In the Application Steering pane, click the ✎ Edit icon. In the Application Steering pane, enter information for the following fields.

Field	Description
Session Pinning (Group of Fields)	Configure path affinity.
◦ Domain App Cache	Click to enable strict path affinity, to ensure that all the sessions of an application flow use the same path that was used by the DNS query to resolve the path to the application server. Do not click to use loose path affinity. This is the default. Here, the DNS query and the application sessions follow paths to the same geographic location, but the DNS query and the application traffic may be sent on different links. In general, it is recommended that you use loose path affinity, because it provides the best balance between ensuring optimal performance and ensuring load balancing of traffic among all eligible paths. *Default:* Loose path affinity
◦ Client Route Cache	Click to pin the subsequent consecutive sessions of an application flow between a specific client and server to the same path.
Timeout (Group of Fields)	Configure the session-pinning timeout periods.
◦ Application Metrics	Enter the maximum time, in seconds, that a link with the worst metric must wait before trying again. *Default:* 300 seconds
◦ Client Route Cache	Enter the maximum time, in seconds, that sessions between a host and client remain pinned to the same link. *Default:* 30 seconds

7. Click Confirm.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1.1 adds support for circuit tags, path names, path types, path media, and path tags; add timeout value for domain name application cache.
- Release 21.2.1 increases the next-hop priority value from 4 to 8; adds support for traffic steering based on monitored available bandwidth; adds support for Layer 2 SD-WAN traffic steering.
- Release 22.1.1 increases circuit priority and next-hop priority values from 8 to 15; adds support for replication and FEC in Layer 2 SD-WAN traffic-steering forwarding profiles

Additional Information

Configure Application Performance Monitoring
Configure Automatic Bandwidth Monitoring
Configure Data-Driven SLA Monitoring
Configure Direct Breakout to the Internet
Configure DNS Proxy
Configure DNS Proxy with SD-WAN Traffic Steering for DIA
Configure Encryption on WAN Interfaces
Configure Forward Error Correction for SD-WAN Traffic Steering
Configure HTTP/HTTPS Proxy
Configure Layer 3 SD-WAN Traffic Steering Based on Available Bandwidth
Configure MOS Score Monitoring
Configure Path Policies
Configure Real-Time Monitoring
Configure Replication for SD-WAN Traffic Steering
Configure SaaS Application Monitoring
Configure SD-WAN Policy
Configure SD-WAN Traffic Engineering
Configure SLA Monitoring for SD-WAN Traffic Steering
Configure SLA Profiles for SD-WAN Traffic Steering
Overview of Policy-Based Forwarding in an SD-WAN Network
Run Internet Speed Tests
Troubleshoot Link Bandwidth Issues