SD-WAN Traffic Optimization

For supported software information, click here.

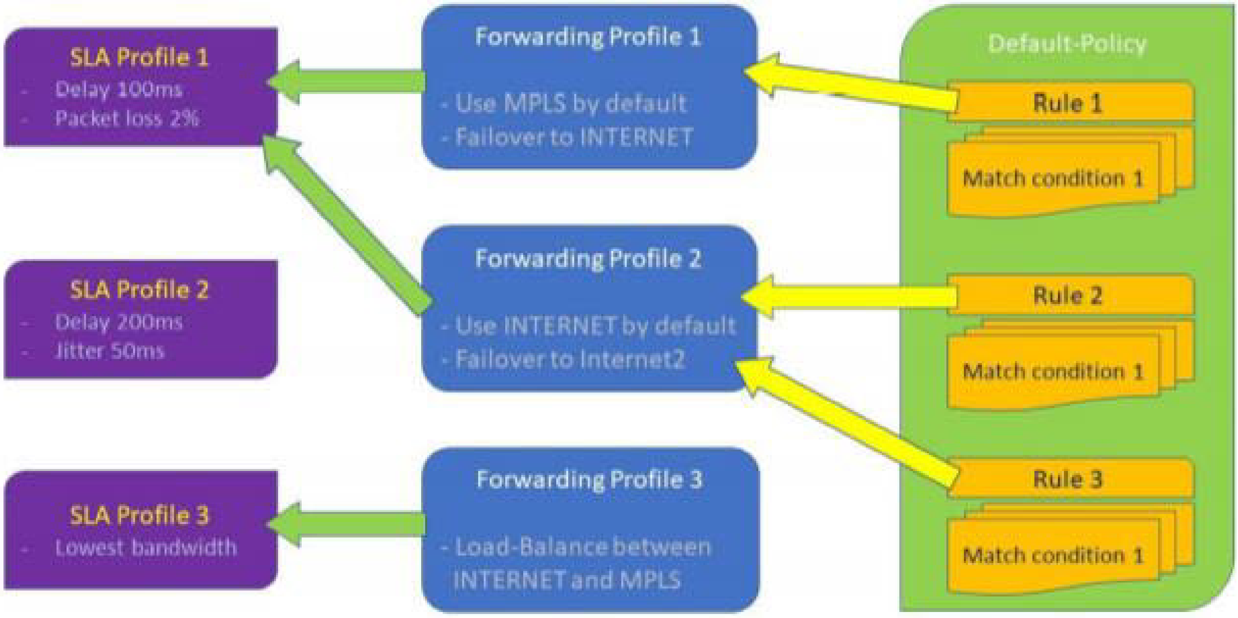
This article discusses how to use traffic steering, traffic conditioning, and SD-WAN path policies to optimize SD-WAN traffic flow.

Traffic Steering

An SD-WAN optimizes traffic over available underlays—MPLS, broadband, and LTE—to deliver traffic across the network in an optimal way. Versa Networks VOS edge devices use SLA monitoring to gather performance metrics about all paths towards all peer branches (assuming a full-mesh topology). The metrics include latency, jitter, and packet loss, and they are used to determine whether a path is up, and if so, whether it meets the user-defined SLAs for an application or a set of applications. The Versa Networks SD-WAN can dynamically steer traffic to the best available link, and if the available links show any transmission issues, the SD-WAN immediately applies remediation for the delay, jitter, and packet loss based on policies, to ensure the continued performance of high-priority applications. The Versa Networks SD-WAN platform provides powerful and flexible policy-based mechanisms for a wide variety of WAN path selection behavior.

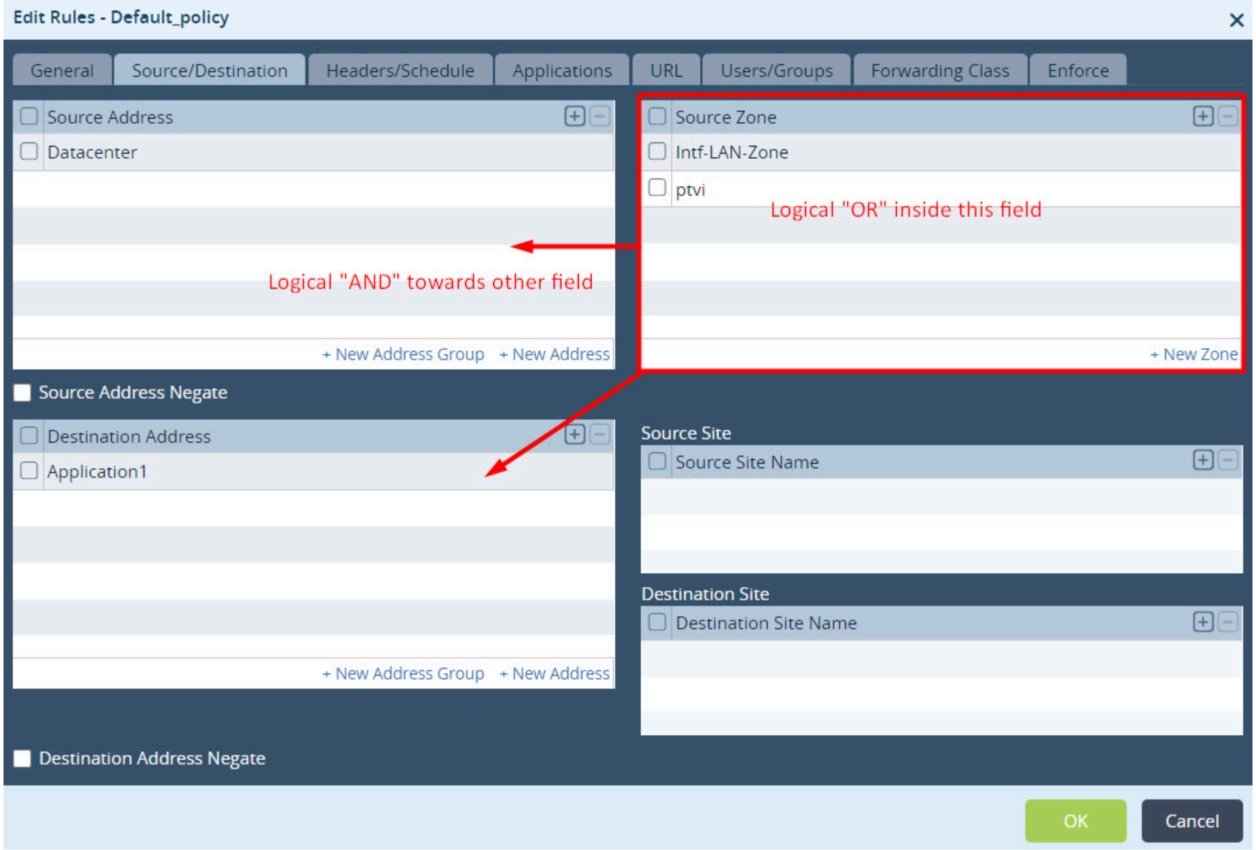
Traffic steering configuration consists of three major components, which are illustrated in the following figure:

- Policy rules—A VOS SD-WAN policy consists of one or more rules. A rule identifies traffic for which you want to specify path selection behavior. Traffic that does not match a specific rule is subject to default behavior. You associate traffic-matching rules with a forwarding profile.
- Forwarding profiles—Forwarding profiles define circuit or path priorities, connection methods, and load-balancing capabilities for traffic that matches the policy associated the forwarding profile.
- SLA profiles—SLA profiles, which are optional and which you associate with a forwarding profile, define application or network thresholds for a path to meet SLA compliance.



The following are best practices related to SD-WAN traffic-steering policy:

- Ensure that the match conditions in the SD-WAN policy match the correct traffic. For SD-WAN policy, and also for all policy configurations on VOS edge devices, all rule values that you configure on the same GUI tab are processed as a logical OR function, and rule values that you configure on different GUI tabs are processed as a logical AND function. For example, if you include multiple addresses in the source address field, any one of the addresses can fulfill the match criteria for that field. If you include multiple source addresses and if you also configure a source zone, the traffic must match one of the source addresses AND one of the source zone parameters. See the screenshot below. Note that the VOS device supports IPv4 and IPv6 addresses. For more information, see Configure SD-WAN Policy.


Edit Rules - Default_policy

□ Source Address
□ Datacenter

□ Source Zone
□ Intf-LAN-Zone
□ ptvi

Logical "OR" inside this field

Logical "AND" towards other field

□ Source Address Negate

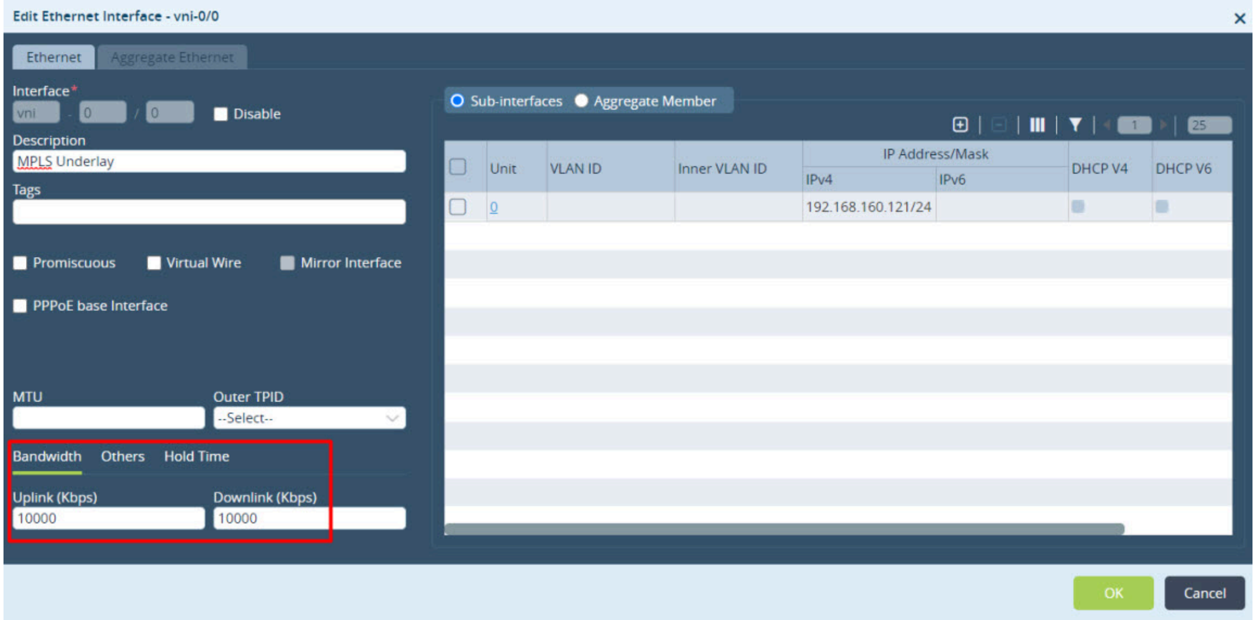
□ Destination Address
□ Application1

Source Site
□ Source Site Name

Destination Site
□ Destination Site Name

□ Destination Address Negate

- SD-WAN policy rules are evaluated in the order that you include them in the policy. Policy rules are processed starting with the first (top) rule, and the rule evaluation is exited at the first match. So make sure that you configure the matching criteria for critical traffic in one of the initial rules.
- When you want to apply the same forwarding profile to different applications because the applications have similar characteristics because because you want the application traffic to be handled similarly, design and configure the SD-WAN policies so that you can associate the them with the same forwarding profile.
- As a rule of thumb, log only on SLA Violated to reduce the number of logsx. Another possibility is to limit the rate of the log messages.
- Always set the bandwidth on the interface. This parameter is used as the main input for the SD-WAN bandwidth-related profiles.


Edit Ethernet Interface - vni-0/0

Interface* vni - 0 / 0 □ Disable

Description: MPLS Underlay

Tags:

□ Promiscuous □ Virtual Wire □ Mirror Interface

□ PPPoE base Interface

MTU:

Outer TPID: --Select--

Uplink (Kbps): 10000

Downlink (Kbps): 10000

● Sub-interfaces ○ Aggregate Member

□	Unit	VLAN ID	Inner VLAN ID	IP Address/Mask		DHCP V4	DHCP V6
				IPv4	IPv6		
□	0			192.168.160.121/24		□	□

- To enable load balancing between paths across the WAN circuits, set the WAN circuit priority to the same value:
  - If you want to do load balancing for specific traffic, configure at least two circuits with equal priority.
  - If you specify no circuits, all circuits are assumed to have the same priority.
- With the weighted round-robin (WRR) connection selection method, weights are assigned to each path based on the available bandwidth on the access circuit. It is recommended that you use WRR if paths with equal priorities are provisioned with different bandwidths.
- An elephant flow, which is a single large volume session such as FTP downloads or file copy, presents peculiar challenges for SD-WAN traffic steering. The following are best practices to optimize these flows:
  - Use per-packet load balancing if the traffic is not sensitive to jitter or loss.
  - Enable the Gradual Migration option in the traffic-steering forwarding profile, to prevent a thundering herd of flows when a previously violated path becomes good again.
  - Set up a relatively longer recompute timer, to prevent violating the path because of transient impairments.
  - Enable FEC to protect against loss especially where data integrity, such as in file copying, is important . Configure a "stop when" circuit utilization value for when circuit utilization reaches hits a high watermark value, to prevent FEC overhead from congesting the network.
- Enable reordering globally on all branches in the network.
- The following are best practices when configuring real-time traffic, such as voice and video UDP streams:
  - Enable the Evaluate Continuously option, to allow real-time flows to react better to changing network conditions.
  - Enable the Gradual Migration option in the traffic-steering forwarding profile.
  - Enable replication to mitigate against loss and jitter. Set the start to be SLA Violated and set the stop to Stop When circuit utilization hits a high watermark value (75% is recommended) to prevent replication overhead from congesting the network.
- The recomputation timer determines the number of SLA reports to access before a violation decision is made. It is recommended that you not shorten the default recompute timer, which is 300 seconds. (However, it might be convenient to lower the value during lab testing.) Rather, enable the Evaluate Continuously option in the forwarding profile. However, you can set a longer recompute timer for relatively high-quality underlay networks, as well as for

flows that can survive transient network conditions.

- SLA smoothing and SLA violation damping are disabled by default, and if you choose to enable them, you should do so only after an in-depth analysis. If the circuits or paths do not often most between the compliant and noncompliant states, you should use the default configuration
- If you enable SLA smoothing, configure the recomputation timer to a value that is less than the SLA smoothing interval.

Traffic Conditioning

Real-time applications have more stringent delay requirements than normal data transmissions. As a result, retransmission of lost packets is generally not a valid option for these types applications. In these cases, better methods to use when attempting to recover information from packet loss are packet replication and forward error correction (FEC).

Packet Replication

Packet replication is the most effective option for applications that are sensitive to latency and packet loss. Packet replication, which is primarily used for real-time applications, takes an identified type of application traffic and sends a copy of each packet across multiple paths. This mechanism prevents inherent latency anomalies and packet losses from negatively impacting the applications.

One drawback of packet replication is that it can have a significant impact on the bandwidth utilization of WAN circuits. Therefore, you should use this feature mainly for low-volume UDP traffic that is sensitive to packet loss, such as VoIP traffic. Also, it is recommended that you configure both Start When SLA Violated and Stop When options in the forwarding profile that you associate with packet replication.

Packet replication works as follows: If a transmitted packet is lost in transit, a copy of the packet is forwarded to the receiver. The receiving branch discards the copies of the packet and forwards only one packet to the receiver. You must enable reordering on all branches to ensure that the receiving branch reorders packets before forwarding them to the receiver.

Packet replication is suitable for branches with multiple SD-WAN paths between branches, while FEC is also effective on a branch that has only a single access links. Packet replication works well when the amount of critical traffic that is being duplicated across the networks is far less than the capacity of the network.

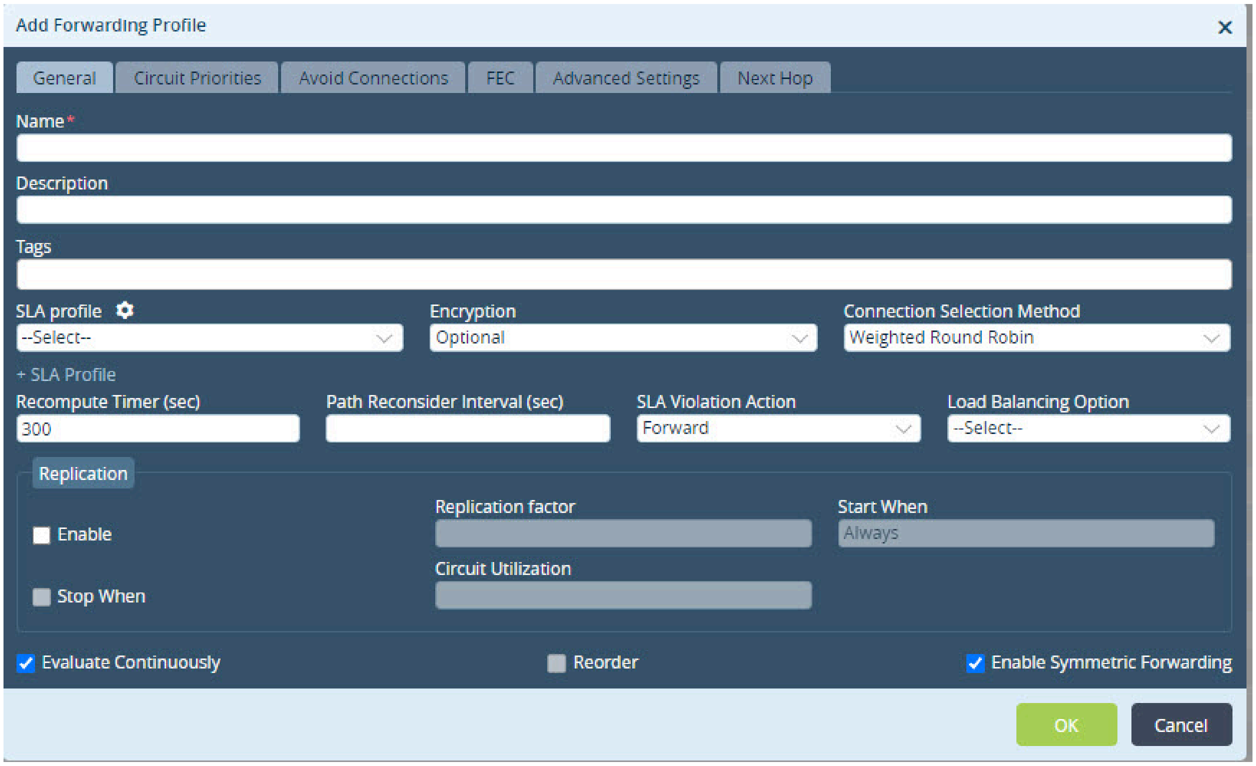
By default, packet replication is disabled. To enable replication, you configure it when you configure an SD-WAN traffic-steering forwarding profile:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template 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. The Add Forwarding Profile popup window displays. Enter the following information in the Replication group of fields. For more information, see [Configure Replication for SD-WAN Traffic Steering]().



Name*

Description

Tags

SLA profile: --Select--

Encryption: Optional

Connection Selection Method: Weighted Round Robin

Recompute Timer (sec): 300

Path Reconsider Interval (sec):

SLA Violation Action: Forward

Load Balancing Option: --Select--

Replication

☐ Enable

☐ Stop When

Replication factor:

Start When: Always

Circuit Utilization:

☑ Evaluate Continuously

☐ Reorder

☑ Enable Symmetric Forwarding

5. To enable packet replication, click Enable. By default, replication is disabled.
6. In the Replication Factor field, enter the number of egress packets to send for each ingress packet. For example, if you configure a replication factor of 2, for each ingress packet, two egress packets (the original and one copy) are forwarded to the next hop. The default replication factor is 2. If there are more than two paths between branches, you can increase the value.
7. In the Start When field, select SLA Violation, to enable packet replication only when all available paths have violated the SLA. Otherwise, replication is enabled on all flows that use the forwarding profile. It is recommended that when you enable packet replication, you always select the SLA Violation option.
8. Optionally, click Stop When to set a circuit utilization threshold value to use to stop packet replication and thus prevent oversubscription of links. When the utilization of any of the links used for replication reaches the percentage set in the Circuit Utilization option, replication stops, and the flow passes using only one available link, as was the case before you enabled replication.
9. When you click Stop When, in the Circuit Utilization field, enter the circuit utilization threshold at which replication stops automatically if all the device's WAN circuits exceed this threshold. Specify this as a percentage of the total circuit bandwidth. This threshold applies to all circuits, even those that are set as to be avoided.
10. Click OK.

The following are best practices for packet replication:

- Use packet replication only for specific traffic, such as VoIP. Avoid enabling replication on wildcard traffic.
- Enable replication only when Start When is SLA Violated, and always set the Stop When and Circuit Utilization. For the circuit utilization calculations to be accurate, ensure that the bandwidth values are set correctly on the interface.
- A replication factor of 2 is adequate for most cases. However, you can increase the value to match the available paths for the flows that are protected. For example, four paths can benefit from a replication factor of 3.
- Bandwidth utilization increases by 100% for each unit increment in the replication factor. That is, a replication factor of 2 equates to a 100% increase in bandwidth, a factor of 3 equates to a 200% increase, and so on.
- Enable replication for real-time traffic and other business-critical traffic for which jitter and loss are important.

Forward Error Correction

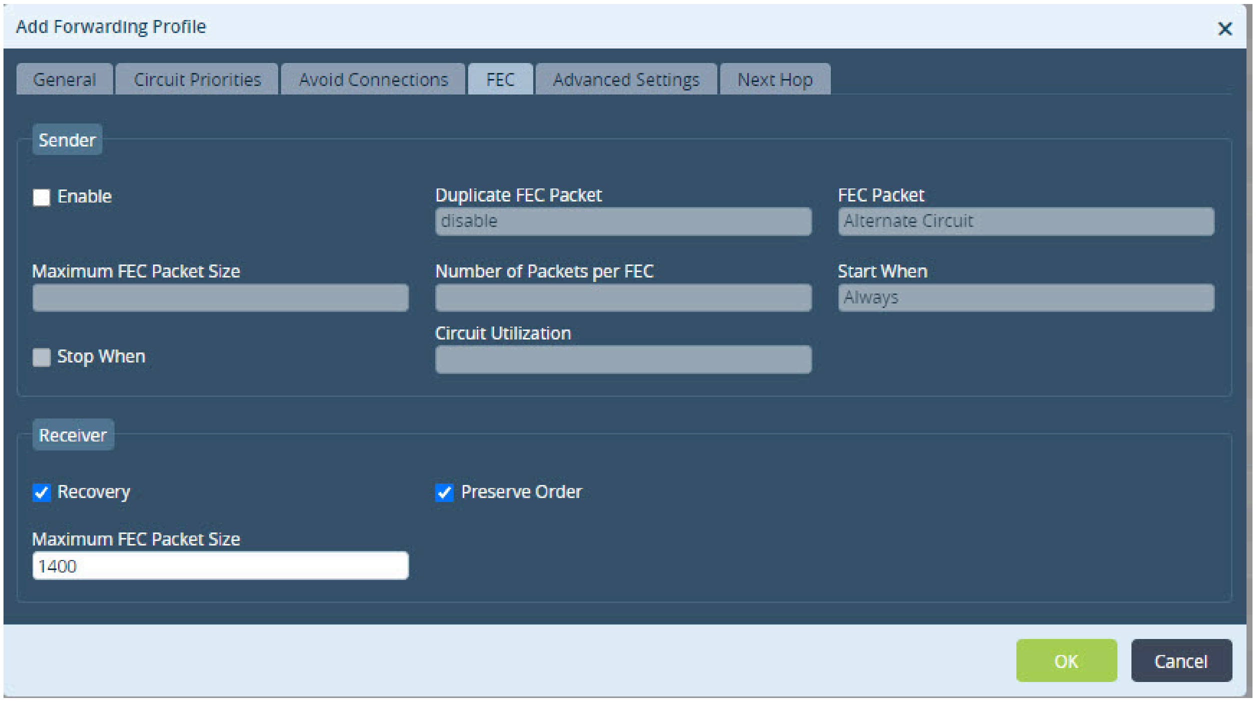
FEC is a mechanism to correct bit errors at the physical layer. While FEC has traditionally been used for this purpose, it has been adapted so that it can be used to recover from packet loss at the network level.

Packet-level FEC works by adding an additional loss recovery packet for every *n*th packet that is sent. This additional loss recovery packet enables a VOS edge device to reconstitute lost packets at the far end of a WAN link, before the packets are delivered to TCP or other transport layers. This mechanism avoids transport layer retransmission and, in the case of TCP, prevents the TCP congestion avoidance mechanism from lowering the throughput available to the application. For the modest overhead of an additional loss recovery packet, FEC reduces packet loss dramatically, enabling applications to benefit from the maximum throughput that the WAN link can support.

You can turn on FEC along with replication at the sites that have multiple paths, to provide maximum protection and correction. You can also use FEC to recover packets independently when replication might not be useful, for example, at sites with a single path for transport traffic.

To configure FEC:

1. In Appliance view, select the Configuration tab in the top menu bar.
2. Select Services ⚙ > SD-WAN > Forwarding Profiles in the left menu bar.
3. Click the ⊞ Add icon. The Add Forwarding Profile popup window displays. Enter the following information in the FEC tab. For more information, see Configure 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

4. For FEC on the sender, configure the following options in the Sender group of fields:
    a. To enable FEC, click Enable.
    b. In the Duplicate FEC Packet field, if extra protection is required, additional FEC parity data packet can be sent. The FEC parity packets could be transmitted over the same WAN link or over another available WAN circuit. By default, duplicate FEC packets are not sent.
    c. In the FEC Packet field, select the circuit on which to send the FEC packets. The default if the alternate circuit. If you configure Duplicate FEC Packets, select the same circuit that you use for the duplicate packets.
    d. In the Maximum FEC Packet Size field, enter the maximum size of the data in the packet to protect. For example, voice packets are typically less than 100 bytes, so set the maximum size to 100bytes to protect the traffic.
    e. In the Number of Packets per FEC field, nter the number of data packets after which an FECe packet is generated and sent to the peer branch. The default value is 4, which means the system generates FEC parity data after each four packets of actual data transmitted according to this forwarding profile.
    f. In the Start When field, if you do not select any value, the forwarding profile always protects traffic for the defined rule. If you select SLA Violation, the FEC is enabled only when all available paths have a violated SLA.
    g. Click the Stop When field to optionally prevent oversubscription of the links. When the utilization of the link over the FEC data is sent reaches the percentage configured in the Circuit Utilization field, the FEC operations stop.
5. For FEC on the receiver, configure the following options in the Receiver group of fields:
    a. Click the Recovery field to enable packet recovery after the receiver receives FEC packets. By default, receiver packet recovery is enabled.
    b. Click the Preserve Order to reorder out-of-order packets and forward them in their original order. By default, reordering is enabled. Note that this option is independent from Reorder option in the Forwarding Profile.
6. Click OK.

There are multiple ways of configuring Layer 3 FEC, and the following are some recommendations:

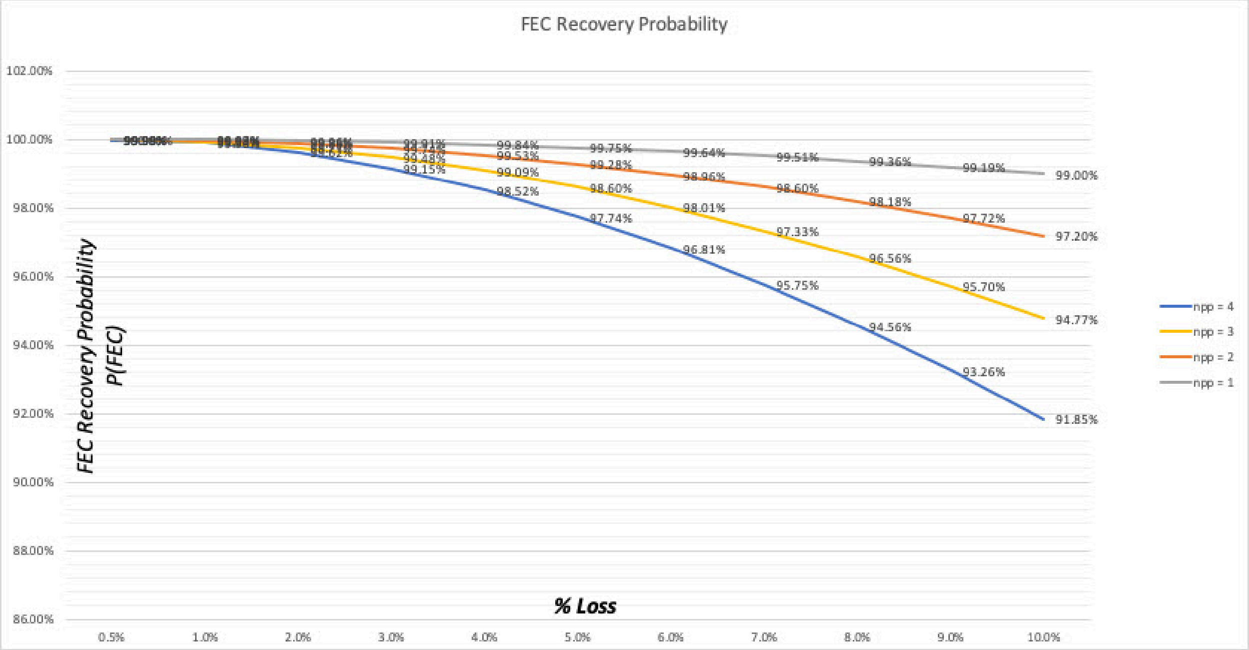
- WAN circuit utilization—When bandwidth is at a premium, FEC is more efficient than packet replication, and it generates only one parity packet for a specified number of data-carrying packets (range 1 through 32, default 4). The generated FEC parity packet can recover a packet on the peer branch only if one packet is lost in the specified number of packets per FEC.
- If packet corruption on a path has a specific pattern (corrupting the *n*th recovery packet and its replica), it is recommended that you replicate the FEC packet on an alternate circuit so that non-corrupted FEC packets can reach the remote site.
- Small versus large packets—Layer 3 FEC works well on flows of small packets, such as voice or point-of-sale transactions. Applications that have large packets, such as video and file transfers, are usually not business-critical applications, and performing forward error correction on fragmented packets is difficult. It is recommended that you use FEC for packets less than 500 bytes.
- LTE and FEC—In most cases, you should not use FEC on LTE interfaces, because FEC increases the amount of traffic on a network that is already limited in capacity. When packets are dropped in a wireless network, it is usually many packets in a row, and FEC is not useful in such a scenario.
- Adaptive codecs versus FEC—Many of the latest voice and video codecs support FEC within the application codec. Usually, these adaptive codecs are more efficient than Layer 3 FEC. For these cases, you must perform tests to find out whether the Layer 3 FEC feature provides any advantage if you use it on top of the voice or video codec FEC feature.
- Versa implements single-dimensional FEC, which is most effective against bit error and single packet loss within a protected block. FEC improves the probability that a stream arrives intact at a receiver. You can calculate the probability with the following formula:

  $$P(FEC = (1 - p_X)^{w+1} = ((w + 1)(1 - p_X)^{w})\mathrm{p}_X$$

  Where:

  - $P(FEC)$ is the FEC recovery probability, as a percentage
  - p_X is the packet loss, as a percentage
  - w is the number of packets per parity (npp)

  This formula indicates that the FEC default settings of 4 (npp) is effective only up about a 5 percent packet loss, as illustrated with the following graph. You should consider replication for higher loss percentages.



- FEC performance increases when the npp is closer to 1. There is, however, a 25 percent increase in the bandwidth utilization value for every unit decrease in *x* – 1, where *x* = npp. For example, if the default npp is 4, reducing it to 3 increases bandwidth utilization by 25 percent. When npp = 1, bandwidth utilization increases by 100 percent.

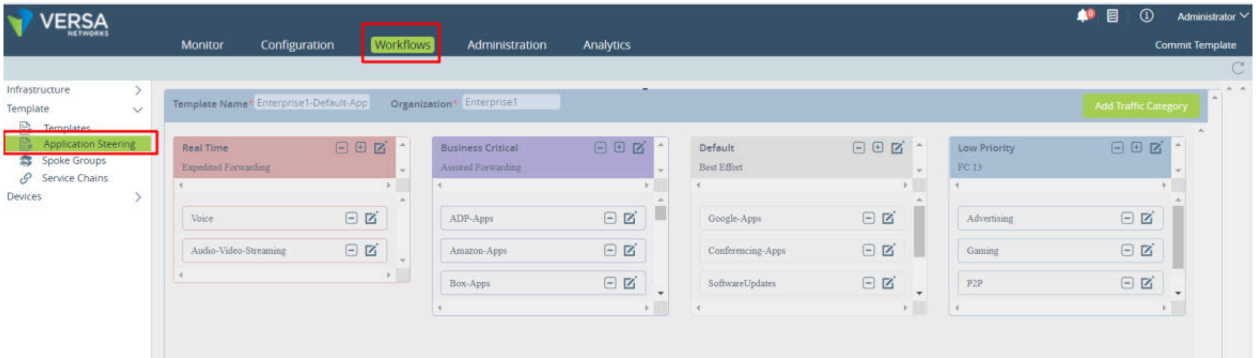
Business-Intent Traffic Steering with Application-Steering Templates

Application-steering templates automate business-intent policies and combine all business applications and network characteristics into a single configuration template. These characteristics include classification, mapping into forwarding classes (QoS), and SD-WAN policies.

Application-steering templates do not add new SD-WAN functionality, but rather they simplify management of business applications in one template. These templates do not configure other QoS parameters other than forwarding class assignment and loss priority, so you still have to define and apply QoS policies and rules to deliver predictable application performance during congestion.

After the initial deployment is complete, you can modify SD-WAN application-steering templates for detailed configurations. The application-steering workflow is retained and is used in similar ways as other Workflow templates, to create complex configuration modifications. For more information, see Create Application-Steering Templates.

A default application-steering template is preconfigured for each organization, with four traffic categories—Real Time, Business Critical, Default and Low Priority, as shown in the screenshot below These categories group applications or family of applications under a particular traffic category. For example, voice applications are grouped under Real Time, and Office 365 applications are grouped under Business Critical. Note that the default application template is an example template that is designed to allow the administrator a quick start in writing application business intents. You can evaluate it and then modify it as needed.



Template Name* Enterprise1-Default-App
Organization* Enterprise1

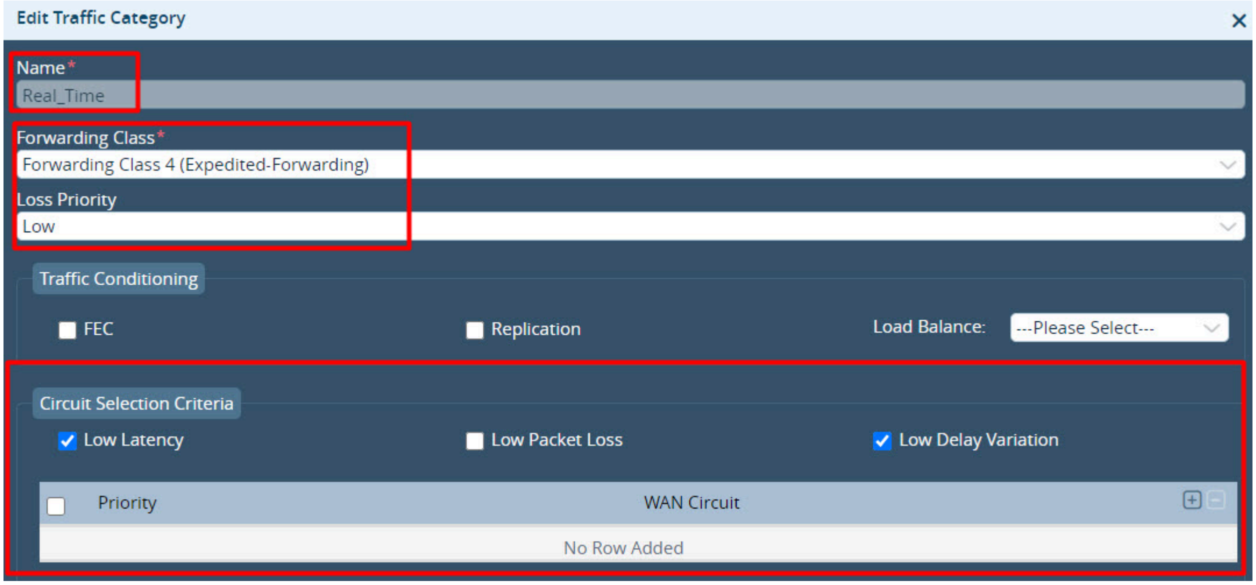
Real Time
Expedited Forwarding
Voice
Audio-Video-Streaming

Business Critical
Assured Forwarding
ADP-Apps
Amazon-Apps
Box-Apps

Default
Best Effort
Google-Apps
Conferencing-Apps
SoftwareUpdates

Low Priority
FC 13
Advertising
Gaming
P2P

For each traffic category, default criteria are applied. For example, for the Real Time category, a default configuration for Forwarding Class and Circuit Selection Criteria is applied, as shown in the following screenshot. For more information, see Add a Traffic Category.


Edit Traffic Category

Name* Real_Time

Forwarding Class* Forwarding Class 4 (Expedited-Forwarding)

Loss Priority Low

Traffic Conditioning

□ FEC □ Replication Load Balance: ---Please Select---

Circuit Selection Criteria

☑ Low Latency □ Low Packet Loss ☑ Low Delay Variation

□	Priority	WAN Circuit
No Row Added		

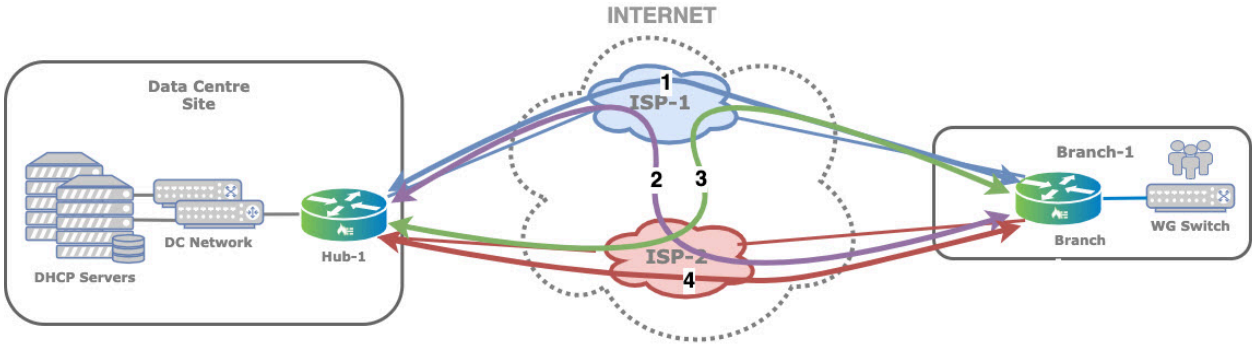
You can modify the values in Forwarding Class and Loss Priority fields and set traffic conditioning parameters (such as FEC and replication), load-balancing algorithm, and dynamic or static circuit path selection criteria that apply to the applications configured for the traffic category. You can create custom traffic categories or modify predefined categories.

The following are best practices for application-steering templates:

- Use application-steering templates to automate the creation of SD-WAN policies. You can customize the service template to suit your requirements.
- Application-steering templates create CoS classifiers and ensure that schedulers are added to the appropriate interfaces.

SD-WAN Path Policies

BOS branches continuously monitor the performance of all paths towards all SD-WAN peer branches and Controller nodes. A path is defined as any valid transport tunnel between the two branches. For example, if two branches have two broadband links each, and each of them is in a single transport domain, there are four paths between the branches, as illustrated in the following. This applies to the paths between branches and Controller nodes as well but is not represented in Figure 9.

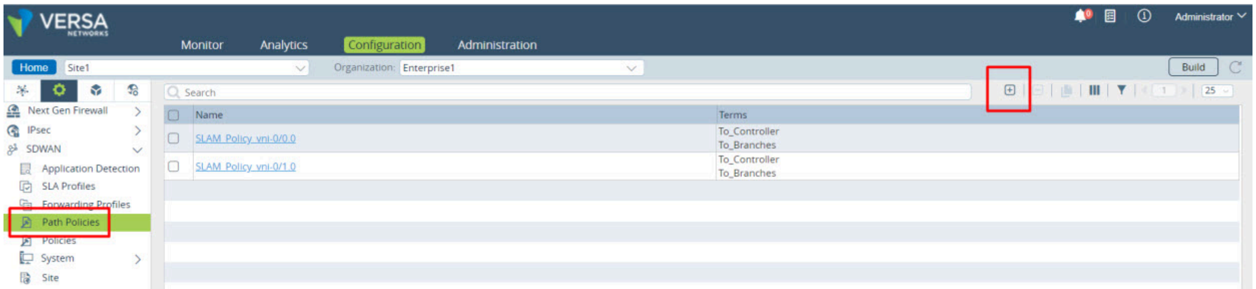


Each path is monitored by sending request-response style SLA probes at a configured interval. Because a network may impose differentiated treatment for different forwarding classes, SLA probes are sent for each forwarding class. The metrics computed are delay, and forward and reverse delay variation and loss (statistical and actual traffic loss in forward and reverse directions).

You can configure SLA monitoring (SLAM) for all 16 forwarding classes (network control through FC 15) using SLA path policies. These SLAM path policies are created, by default, on all WAN interfaces using the EF forwarding class at 2-seconds intervals towards remote branches, and using the NC forwarding class at 10-second intervals towards Controller nodes. You can modify these polices or create new one to suit your requirements. Each SLAM path policy has a match condition on the remote site type, that is, whether it is a Controller node or a branch.

To configure a path policy:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the left menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template 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 > Path Policies. The main pane displays a list of the path policies that are already configured.

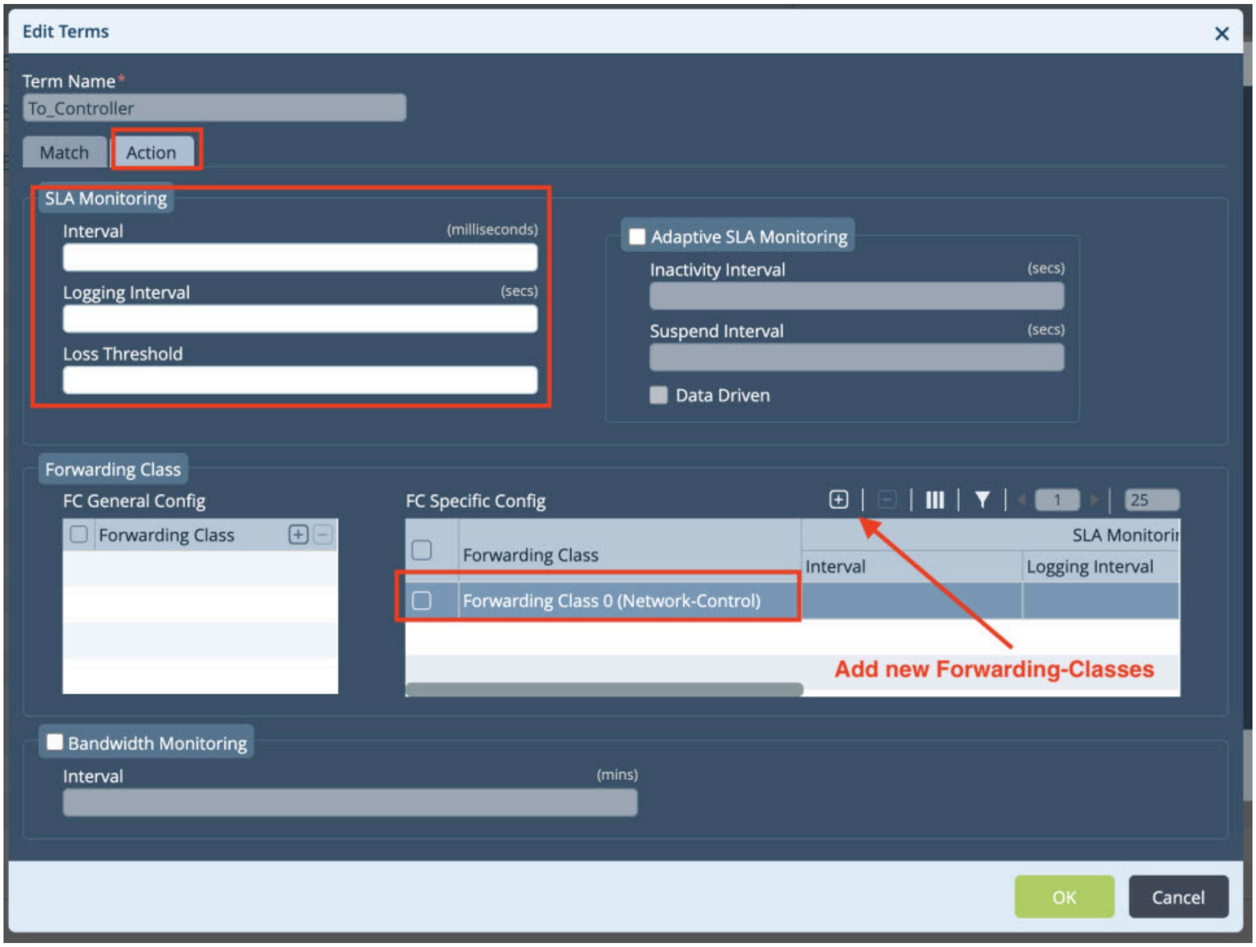


Site1

Organization: Enterprise1

Name	Terms
SLAM_Policy_vni-0/0.0	To_Controller To_Branches
SLAM_Policy_vni-0/1.0	To_Controller To_Branches

4. Click the ⊞ Add icon. The Add Path Policy popup window displays. Select the Action tab and enter the following information fields. For more information, see Configure SD-WAN Path Policies.



Term Name* To_Controller

	Forwarding Class
□	Forwarding Class 0 (Network-Control)

Add new Forwarding-Classes

The following are best practices for path policies:

- The default SLA path policy is generally sufficient for most use cases.
- If you want to configure additional SLA probes, it is recommended that you not have more than one SLA probe for each traffic class.
- For granularity, you can use four probes for the four traffic classes—Network Control, Expedited Forwarding, Assured Forwarding, and Best-Effort. This modification is required only for a branch-to branch-profile. Branch-to-

Controller profiles require probes only for the Network Control class.

- On low-bandwidth circuits, configuring SLA monitoring for several forwarding classes with aggressive timer can use a considerable portion of the available bandwidth. A hub-and-spoke topology is recommended to minimize this overhead, rather than having only SLA probe to the hub.
- You can enable SLA optimization techniques such as adaptive SLA and data-driven SLA to reduce the SLA probe load, especially on low-bandwidth links.
- Gradually introduce topology changes to further optimize the network to prevent a full mesh of SLA probes and the subsequent SLA load. For more information, see SD-WAN Topologies.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure SD-WAN Path Policies
Configure SD-WAN Traffic Steering
Create Application-Steering Templates
SD-WAN Topologies