

Versa Class of Service

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the structure of the Class of Service configuration hierarchy
- Configure Class of Service services

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these hints to help you in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Exercise 1: Examine the Class of Service Hierarchy

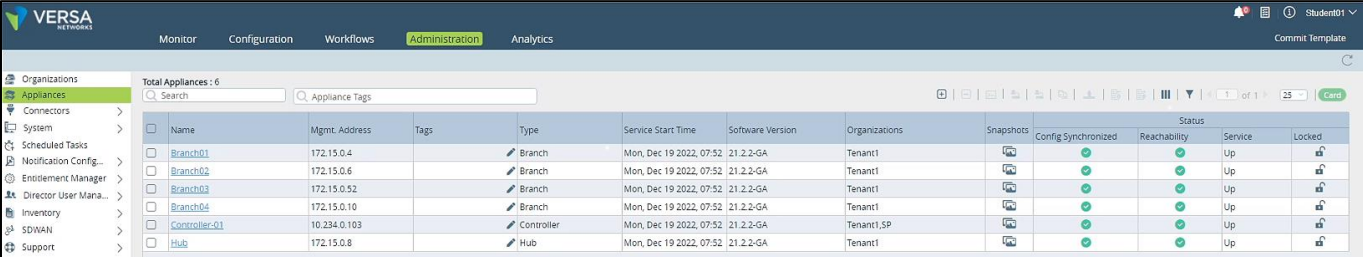
In the following lab exercises, you will:

- Locate the Class of Service configuration parameters
- Identify the components required to implement class of service
- Identify the components that are optional to implement class of service

Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

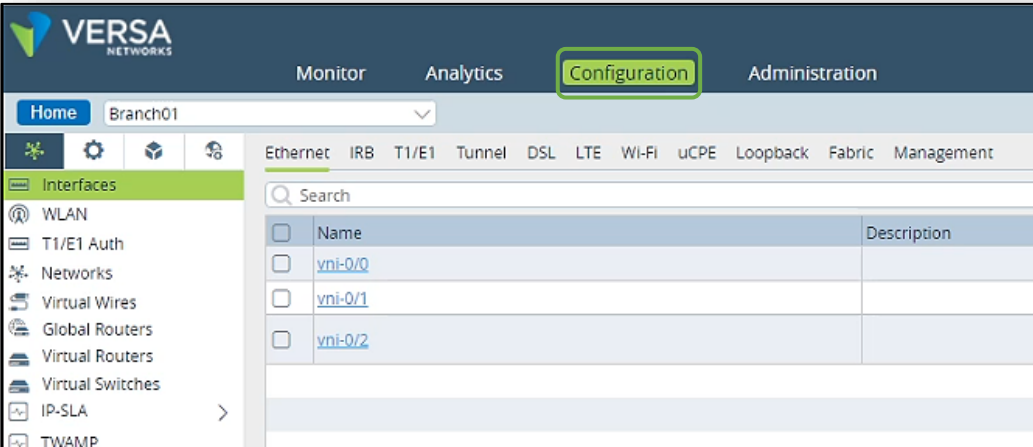
Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

From Versa Director, open the **Administration > Appliances** dashboard to display the deployed devices. Locate your device in the list and click on the link to your device. This will open the Appliance Context of your device so that changes that are made take effect immediately on your appliance.



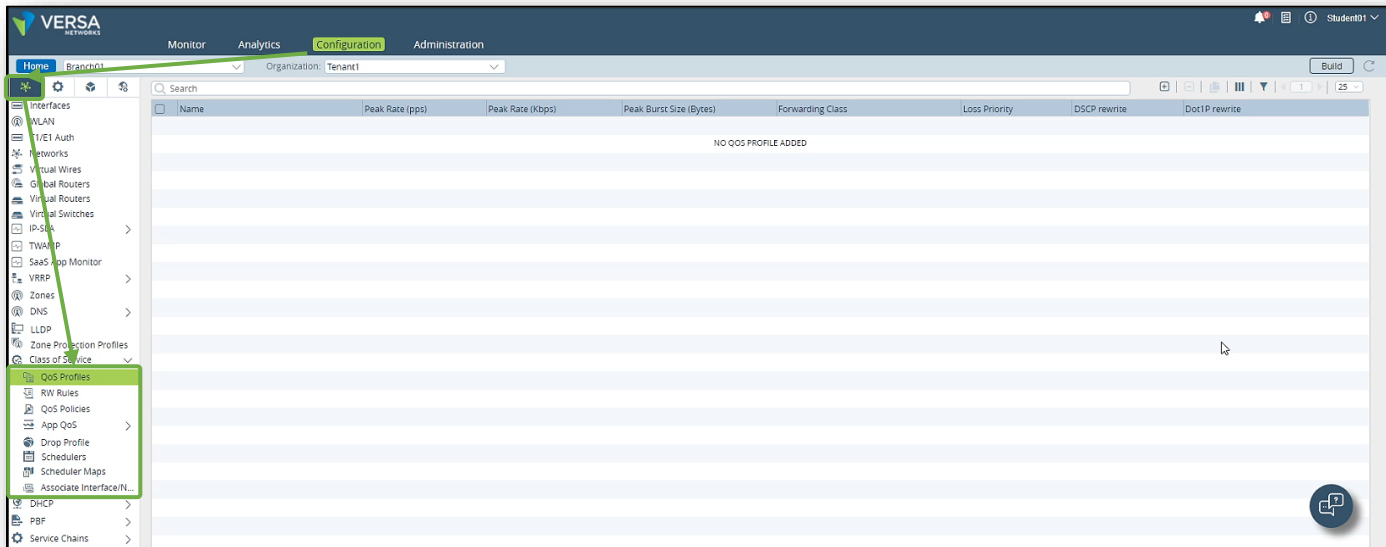
Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Snapshots	Config Synchronized	Reachability	Service	Locked
Branch01	172.15.0.4		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch02	172.15.0.6		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch03	172.15.0.52		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch04	172.15.0.10		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Controller-01	10.234.0.103		Controller	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1.SP				Up	
Hub	172.15.0.8		Hub	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	

From the Appliance Context mode of your device, select the Configuration tab to access the device-specific configuration.



Name	Description
vni-0/0	
vni-0/1	
vni-0/2	

The Class of Service configuration components are located in the Networking tab of the configuration dashboard. Ensure that the Networking tab is selected, locate the Class of Service components, and expand the Class of Service configuration.



The following components are REQUIRED for a Class of Service configuration:

- QoS Profile
- Policy (QoS or AppQoS)
- Scheduler
- Scheduler Maps
- Associate Interface

The following components are OPTIONAL for a Class of Service configuration:

- RW Rules
- Drop Profile

Exercise 2: Configure Basic Class of Service

In the following exercise you will:

- Configure QoS Profiles
- Configure an AppQoS policy with rules to identify different types of traffic
- Configure 4 Schedulers (1 for each major traffic class)
- Create a Scheduler Map to bundle the schedulers together in a set
- Apply the Scheduler Map to the WAN facing ports (MPLS and INET) of your node

QoS Profiles

A QoS Profile defines how traffic will be treated that is mapped to that profile. A QoS or AppQoS policy uses the QoS Profile as an enforce action for matching traffic, and therefore the QoS profile must be created before the policy.

In this lab part you will create the following QoS profiles:

- Common-Internet
- Drop-Sensitive-Apps
- External-Business-Apps
- Internal-Business-Apps
- Internet-Streaming
- Realtime-Critical
- Realtime-Non-Critical

The parameters for each profile are shown below.

Add QoS Profile

Name*
Common-Internet

Description

Ingress Policing

Peak Rate (pps) Peak Rate (Kbps) Peak Burst Size (Bytes)

2000

Forwarding Class Per User Policer

Forwarding Class* Loss Priority*

Forwarding Class 12 (Best-Effort) High

☒ DSCP Rewrite ☐ Dot 1P Rewrite

OK Cancel

Add QoS Profile

Name *

Drop-Sensitive-Apps

Description

Profile for drop-sensitive applications

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

Forwarding Class

Per User Policer

Forwarding Class *

Forwarding Class 10

Loss Priority *

Low

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

Add QoS Profile

Name *

External-Business-Apps

Description

Profile for External business apps (cloud apps)

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

Forwarding Class

Per User Policer

Forwarding Class *

Forwarding Class 9

Loss Priority *

Low

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

Add QoS Profile

Name*

Realtime-Non-Critical

Description

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

5000

Forwarding Class

Per User Policer

Forwarding Class*

Forwarding Class 4 (Expedited-Forwar...

Loss Priority*

High

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

Add QoS Profile

Name*

Internal-Business-Apps

Description

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

10000

Forwarding Class

Per User Policer

Forwarding Class*

Forwarding Class 8 (Assured-Forwardi...

Loss Priority*

Low

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

Add QoS Profile

Name*

Realtime-Critical

Description

Profile for critical real-time voice and video

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

Forwarding Class

Per User Policer

Forwarding Class*

Forwarding Class 4 (Expedited-Forwar...

Loss Priority*

Low

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

Add QoS Profile

Name*

Internet-Streaming

Description

Ingress Policing

Peak Rate (pps)

Peak Rate (Kbps)

Peak Burst Size (Bytes)

Forwarding Class

Per User Policer

Forwarding Class*

Forwarding Class 13

Loss Priority*

Low

☒ DSCP Rewrite

☐ Dot 1P Rewrite

OK

Cancel

When finished, your configuration should resemble the example below.

<input type="checkbox"/>	Name	Peak Rate (pps)	Peak Rate (kbps)	Peak Burst Size (Bytes)	Forwarding Class	Loss Priority	DSCP rewrite	Dot1P rewrite
<input type="checkbox"/>	Common-Internet		2000		Forwarding Class 12 (Best-Effort)	high	Yes	No
<input type="checkbox"/>	Drop-Sensitive-Appls				Forwarding Class 10	low	Yes	No
<input type="checkbox"/>	External-Business-Appls		10000		Forwarding Class 9	low	Yes	No
<input type="checkbox"/>	Internal-Business-Appls		10000		Forwarding Class 8 (Assured-Forwarding)	low	Yes	No
<input type="checkbox"/>	Internet-Streaming		2000		Forwarding Class 13	low	Yes	No
<input type="checkbox"/>	Realtime-Critical				Forwarding Class 4 (Expedited-Forwarding)	low	Yes	No
<input type="checkbox"/>	Realtime-Non-Critical		5000		Forwarding Class 4 (Expedited-Forwarding)	high	Yes	No

AppQoS Policy and Rules

You have created the profiles that associate traffic to input rates (inbound policing) and forwarding classes (which are associated with outbound queues). Next you will create policy rules to identify traffic and direct the traffic to the corresponding QoS profile. To perform this task you will create App QoS policy rules so that you can take advantage of the application identification capabilities of Versa Operating System.

Expand the App QoS configuration hierarchy and select Policies from the App QoS dropdown. There should be a pre-created Default-Policy that does not have any rules.

Ensure that the Rules tab is open and add the following rules to the policy:

Rule 1

General Tab	
Rule Name:	Find-Real-time-Critical
Source/Destination Tab	
Source Zone:	Tenatn1-LAN-Zone
Destination Zone:	Leave Blank
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Leave all fields empty	

Applications/URL Tab	
Applications:	MS_TEAMS, RTP, SIP, SIP_SOAP, ZOOM
URL Categories:	Leave Empty
Enforce Tab	
QoS Profile:	Realtime-Critical

Rule 2

General Tab	
Rule Name:	Find-Real-time-Non-Critical
Source/Destination Tab	
Source Zone:	Tenant1-LAN-Zone
Destination Zone:	Leave Blank
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Leave all fields empty	
Applications/URL Tab	
Applications:	FACEBOOK_AUDIO, FACEBOOK_MESSENGER, FACEBOOK_VIDEO, SKYPE
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	Realtime-Non-Critical

Rule 3

General Tab	
Rule Name:	Find-Internet-Business-Apps
Source/Destination Tab	
Source Zone:	Tenant1-LAN-Zone
Destination Site Name:	Hub
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Service List:	http, https
Applications/URL Tab	
Applications:	Leave Empty
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	Internal-Business-Apps

Rule 4

General Tab	
Rule Name:	Find-External-Business-Apps
Source/Destination Tabs	
Source Zone:	Tenant1-LAN-Zone
Destination Zone:	W-ST-Tenatn1-LAN-VR-INET
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Service List:	Leave Blank
Applications/URL Tab	
Applications:	Amazon-Apps; Google-Apps
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	External-Business-Apps

Rule 5

General Tab	
Rule Name:	Drop-Sensitive-Apps
Source/Destination Tabs	
Source Zone:	Tenant1-LAN-Zone
Destination Zone:	Leave Blank
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Service List:	Leave Blank
Applications/URL Tab	
Applications:	AMAZON_CLOUD_DRIVE
URL Categories:	Leave empty
Enforce Tab	
QoS Profile:	Drop-Sensitive-Apps

Rule 6

General Tab	
Rule Name:	Internet-Streaming
Source/Destination Tabs	
Source Zone:	Tenant1-LAN-Zone
Destination Zone:	W-ST-Tenant1-LAN-VR-INET
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Service List:	Leave Blank
Applications/URL Tab	
Applications:	PANDORA; SPOTIFY; YOUTUBE
URL Categories:	Music; streaming_media
Enforce Tab	
QoS Profile:	Internet-Streaming

Rule 7

General Tab	
Rule Name:	Common-Internet
Source/Destination Tabs	
Source Zone:	Tenant1-LAN-Zone
Destination Zone:	W-ST-Tenant1-LAN-VR-INET
Source Address:	Leave Blank
Destination Address:	Leave Blank
Headers/Schedule Tab	
Service List:	Leave Blank
Applications/URL Tab	
Applications:	Leave Blank
URL Categories:	Leave Blank
Enforce Tab	
QoS Profile:	Common-Internet

When finished your configuration should look similar to this:

Policies Rules												
Default-Policy												
<input type="checkbox"/>	Rule Nu...	Name	Rule Disabled	Action	Enforce	Services	Applications	URL Categories	Source			
					QoS Profiles				Zone	Region	Address	Add
<input type="checkbox"/>	1	Find-Real-Time-Critical	False	Allow	Realtime-Critical		Predefined: MS_TEAMS, RTF		Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	2	Find-Real-Time-Non-Criti...	False	Allow	Realtime-Non-Critical		Predefined: FACEBOOK_AUI		Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	3	Find-Internet-Business-A...	False	Allow	Internal-Business-Apps	Predefined: http, https			Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	4	Find-External-Business-A...	False	Allow	External-Business-Apps		Predefined Groups: Amazon		Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	5	Drop-Sensitive-Apps	False	Allow	Drop-Sensitive-Apps		Predefined: AMAZON_CLOUD		Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	6	Internet-Streaming	False	Allow	Internet-Streaming		Predefined: PANDORA, SPO	Predefined: music, streami	Intf-Tenant1-LAN-Zone			
<input type="checkbox"/>	7	Common-Internet	False	Allow	Common-Internet				Intf-Tenant1-LAN-Zone			

Drop Profiles

There are default drop profiles enabled to manage congestion in queues and interfaces. You will add additional drop profiles that can be used to replace the default drop profiles.

Create 4 drop profiles:

- Deep-Queue-Aggressive
- Deep-Queue-Conservative
- Shallow-Queue-Aggressive
- Shallow-Queue-Conservative

Create the profiles with the following parameters:

Add Drop Profile

Name *

Deep-Queue-Aggressive

Description

Tags

Weighted Random Early Drop

Max *

70

Min *

10

Weight

Inverse-mask Probability

OK

Cancel

Add Drop Profile

Name *

Deep-Queue-Conservative

Description

Tags

Weighted Random Early Drop

Max *

70

Min *

40

Weight

Inverse-mask Probability

OK

Cancel

Add Drop Profile

Name *

Shallow-Queue-Conservative

Description

Tags

Weighted Random Early Drop

Max *

35

Min *

20

Weight

Inverse-mask Probability

OK

Cancel

Add Drop Profile

Name *

Shallow-Queue-Aggressive

Description

Tags

Weighted Random Early Drop

Max *

35

Min *

10

Weight

Inverse-mask Probability

OK

Cancel

When finished, your configuration should look similar to this:

Search									
<input type="checkbox"/>	Name	Min	Max	Weight	Inverse-mask Probability				
<input type="checkbox"/>	Deep-Queue-Aggressive	10	70						
<input type="checkbox"/>	Deep-Queue-Conservative	40	70						
<input type="checkbox"/>	Shallow-Queue-Conservative	20	35						
<input type="checkbox"/>	Shallow-Queue-Aggressive	10	35						

Schedulers

Your device needs to be configured to remove packets from the queues and to forward them out the interface. There are 4 major traffic classes: Network Control, Expedited Forwarding, Assured Forwarding, and Best Effort. Each of these traffic classes has 4 queues. You will create a scheduler for each major traffic class that:

- Defines how much interface bandwidth each traffic class will have for transmitting traffic; and
- Defines which queues to pull traffic from when the traffic class is granted access to the interface.

Define the following 4 schedulers:

Add Scheduler

Name *

NC-Scheduler

Description

Scheduler for network control traffic

Tags

Loss Priority

Drop Profile

High

--Select--

Low

--Select--

Transmit Rate

Guaranteed Rate

Rate (Kbps)

Rate (%)

Rate(Kbps)

Rate (Kbps)

Rate (%)

Rate(Kbps)

500

Queue

Weight

0

--Select--

1

--Select--

2

--Select--

3

--Select--

OK

Cancel

Add Scheduler

Name *

EF-Schedule

Description

Scheduler for expedited forwarding traffic (short term buffering)

Tags

Loss Priority

Drop Profile

High

Shallow-Queue-Aggressive

Low

Shallow-Queue-Conservative

Transmit Rate

Guaranteed Rate

Rate (Kbps)

Rate (%)

Rate(Kbps)

Rate (Kbps)

Rate (%)

Rate(Kbps)

10000

Queue

Weight

0

--Select--

1

--Select--

2

--Select--

3

--Select--

OK

Cancel

Edit Scheduler - AF-Scheduler

Name *

AF-Scheduler

Description

Scheduler for Assured Forwarding Traffic

Tags

Loss Priority

Drop Profile

High

Deep-Queue-Aggressive

Low

Deep-Queue-Conservative

Transmit Rate

Guaranteed Rate

☒ Rate (Kbps)
 ☐ Rate (%)

☒ Rate (Kbps)
 ☐ Rate (%)

Rate(Kbps)

15000

Queue

Weight

0

1

1

3

2

--Select--

3

--Select--

OK

Cancel

Add Scheduler

Name *

BE-Scheduler

Description

Tags

Loss Priority

Drop Profile

High

Shallow-Queue-Aggressive

Low

Shallow-Queue-Conservative

Transmit Rate

Guaranteed Rate

☒ Rate (Kbps)
 ☐ Rate (%)

☒ Rate (Kbps)
 ☐ Rate (%)

Rate(Kbps)

Queue

Weight

0

1

1

2

2

--Select--

3

--Select--

OK

Cancel

When finished your configuration should look similar to this:

Name	Loss Priority	Drop Profile	Transmit Rate	Guaranteed Rate	Queue	Weight
NC-Scheduler	low	Shallow-Queue-Conservative		500 (Kbps)		
EF-Scheduler	high	Shallow-Queue-Aggressive		10000 (Kbps)		
AF-Scheduler	low	Deep-Queue-Conservative		15000 (Kbps)	0	1
	high	Deep-Queue-Aggressive			1	3
BE-Scheduler	low	Shallow-Queue-Conservative			0	1
	high	Shallow-Queue-Aggressive			1	2

Scheduler Map

You have created 4 schedulers that can be used to manage the queues on interfaces. Next you will need to assign a scheduler to each traffic class by using a scheduler map.

Create a scheduler map that will be used to map schedulers to the traffic classes. The same map will be used on all interfaces so that all interfaces receive the same queuing and scheduling parameters.

Traffic Class	Scheduler
Traffic Class 0	NC-Scheduler
Traffic Class 1	EF-Schedule
Traffic Class 2	AF-Scheduler
Traffic Class 3	BE-Scheduler

When finished your configuration should look similar to this:

Scheduler Map Name	Traffic Class - Schedulers
Map-to-WAN-Links	Traffic Class 0 : NC-Scheduler
	Traffic Class 1 : EF-Schedule
	Traffic Class 2 : AF-Scheduler
	Traffic Class 3 : BE-Scheduler

Associating the parameters to the interfaces

You have defined the class of service parameters that will be applied to your network. Now you need to associate those parameters to the interfaces, or assign those parameters to the interfaces.

Assign the following shaping and scheduler map parameters to the physical interfaces (vni-0/0 and vni-0/1) as follows:

Associate Interface/Network

☒ Interface ☐ Network

Name ^{*}
vni-0/0

Description

Tags

Shaping

Burst Size (Bytes) Rate (Kbps)
50000

DSCP Rewrite Rule --Select-- DSCP6 Rewrite Rule --Select--

802.1p Rewrite Rule --Select-- Scheduler Map Map-to-WAN-Links

Logging Interval (Secs) Bandwidth Sharing Off

OK Cancel

Associate Interface/Network

☒ Interface ☐ Network

Name ^{*}
vni-0/1

Description

Tags

Shaping

Burst Size (Bytes) Rate (Kbps)
30000

DSCP Rewrite Rule --Select-- DSCP6 Rewrite Rule --Select--

802.1p Rewrite Rule --Select-- Scheduler Map Map-to-WAN-Links

Logging Interval (Secs) Bandwidth Sharing Off

OK Cancel

Once finished your configuration should look similar to this:

Search							
	Name	Description	Tag	Shaping		Logging Interval (Secs)	Scheduler Map
				Burst Size (Bytes)	Rate (Kbps)		
<input type="checkbox"/>	vni-0/0				50000		Map-to-WAN-Links
<input type="checkbox"/>	vni-0/1				30000		Map-to-WAN-Links

Verify the Class of Service Parameters

You have configured class of service on the device and applied the configuration parameters to the interface. Next we will verify that the class-of-service parameters have been applied by using the Versa Director Monitor dashboard and the VOS CLI.

In the Versa Director **Monitor** dashboard for your device, navigate to **Services > COS**

The screenshot shows the Versa Director Monitor dashboard. The 'Monitor' tab is selected in the top navigation bar. Below it, the 'Services' tab is selected in the sub-navigation bar. In the 'Services' section, the 'COS' (Class of Service) icon is highlighted. A green arrow points from the 'COS' icon to a table of App QoS Policies. The table has the following columns: Rule Name, APP QoS Hit Count, APP QoS Drop Packet Count, APP QoS Drop Byte Count, APP QoS Forward Packet Count, APP QoS Forward Byte Count, and Dropped Sessions By Per User Policer. The rules listed are: Find-Real-Time-Critical, Find-Real-Time-Non-Critical, Find-Internet-Business-Appl, Find-External-Business-Appl, Drop-Sensitive-Appl, Internet-Streaming, and Common-Internet. All counters are currently at 0.

Rule Name	APP QoS Hit Count	APP QoS Drop Packet Count	APP QoS Drop Byte Count	APP QoS Forward Packet Count	APP QoS Forward Byte Count	Dropped Sessions By Per User Policer
Find-Real-Time-Critical	0	0	0	0	0	0
Find-Real-Time-Non-Critical	0	0	0	0	0	0
Find-Internet-Business-Appl	0	0	0	0	0	0
Find-External-Business-Appl	0	0	0	0	0	0
Drop-Sensitive-Appl	0	0	0	0	0	0
Internet-Streaming	0	0	0	0	0	0
Common-Internet	0	0	0	0	0	0

In the COS window, select the App QoS Policies tab, then select Default-Policy. The rules from the Default Policy will be listed, along with their counters. Note that because this is a lab environment and no live data is transiting the devices, the counters are listed at 0.

Next select the Interfaces tab. There will be packets listed under the interface that have been processed by the CoS processes. However, the packets listed didn't match the specific policies created, so they were processed with default CoS behavior.

App QoS Policies			Interfaces			Per User Policer			QoS Policies		
Search			Search			Search			Search		
Tx BPS	Tx Bytes Dropped	Queue Len	Dropped	Tx Bytes	Tx BPS	Tx Bytes Dropped	Queue Len				
19464	0	0		932465	40800	0	0				
0	0	0		131534	2680	0	0				

Open the MTPuTTY application. In the MTPuTTY application, open an SSH session to your branch device. If prompted for a username or password, the login is **student** and password is **versa123**.

Type **cli** at the shell prompt to start the CLI process. From the CLI, issue the command **show class-of-service interfaces detail** to view the configured class of services properties. The output shows the traffic sent in each traffic class and on each interface.

```
admin@branch1110-cli> show class-of-services interfaces detail
```

```
Interface: vni-0/0
```

```
Traffic Stats:
```

```
TX Packets      : 3438
TX PPS          : 0
TX Packets Dropped : 0
TX Bytes        : 1328159
TX bps          : 1056
TX Bytes Dropped : 0
```

```
Port Stats :
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	2402	0	1118887	0
tc1	expedited-fwd	1036	0	209272	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

```
Pipe Stat:
```

```
Pipe ID : 0
Users   : [ vni-0/0.0 ]
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	2402	0	1118887	0
tc1	expedited-fwd	1036	0	209272	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

```
Interface: vni-0/1
```

```
Traffic Stats:
```

```
TX Packets      : 1276
TX PPS          : 0
TX Packets Dropped : 0
TX Bytes        : 254188
TX bps          : 528
TX Bytes Dropped : 0
```

```
Port Stats :
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	268	0	50572	0
tc1	expedited-fwd	1008	0	203616	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

```
Pipe Stat:
```

```
Pipe ID : 0
Users   : [ vni-0/1.0 ]
```

	Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0	network-control	268	0	50572	0
tc1	expedited-fwd	1008	0	203616	0
tc2	assured-fwd	0	0	0	0
tc3	best-effort	0	0	0	0

Use the command **show class-of-services interfaces extensive** to see the shaping parameters in the output.

```
admin@branch110-ctl> show class-of-services interfaces extensive
```

```
Interface: vni-0/0
```

```
Configuration:
```

```
Burst Size : 125000 bytes
Rate       : 50000 kbps
TC0: Network-Control      : 500-50000 kbps
TC1: Expedited-Forwarding : 50000-50000 kbps
TC2: Assured-Forwarding   : 15000-50000 kbps
TC3: Best-Effort          : 50000-50000 kbps
```

```
Traffic Stats:
```

```
TX Packets      : 4360
TX PPS          : 1
TX Packets Dropped : 0
TX Bytes        : 1661446
TX bps          : 1760
TX Bytes Dropped : 0
```

```
Port Stats :
```

Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0 network-control	2985	0	1383696	0
tc1 expedited-fwd	1375	0	277750	0
tc2 assured-fwd	0	0	0	0
tc3 best-effort	0	0	0	0

```
Pipe Stat:
```

```
Pipe ID       : 0
Users         : [ vni-0/0.0 ]
Type          : Access circuit
Configuration :
Burst Size    : 125000 bytes
Rate          : 50000 kbps
TC0: Network-Control      : 500-50000 kbps
TC1: Expedited-Forwarding : 50000-50000 kbps
TC2: Assured-Forwarding   : 15000-50000 kbps
TC3: Best-Effort          : 50000-50000 kbps
```

Queues	Cfg	Inferred	TX	TX	Bytes	Qlen	Avg	Avg Drop
Wt		BW kbps	Pkts	Dropped	Bytes	Dropped	Rate bps	rate bps
tc0 network-control:								
q0: fc_nc	1	125-50000	2985	0	1383696	0 0	1760	0
q1: fc1	1	125-50000	0	0	0	0 0	0	0
q2: fc2	1	125-50000	0	0	0	0 0	0	0
q3: fc3	1	125-50000	0	0	0	0 0	0	0
tc1 expedited-fwd:								
q0: fc_ef	1	12500-50000	1375	0	277750	0 0	0	0
q1: fc5	1	12500-50000	0	0	0	0 0	0	0
q2: fc6	1	12500-50000	0	0	0	0 0	0	0
q3: fc7	1	12500-50000	0	0	0	0 0	0	0
tc2 assured-fwd:								
q0: fc_af	1	2500-50000	0	0	0	0 0	0	0
q1: fc9	3	7500-50000	0	0	0	0 0	0	0
q2: fc10	1	2500-50000	0	0	0	0 0	0	0
q3: fc11	1	2500-50000	0	0	0	0 0	0	0
tc3 best-effort:								
q0: fc_be	1	10000-50000	0	0	0	0 0	0	0
q1: fc13	2	20000-50000	0	0	0	0 0	0	0
q2: fc14	1	10000-50000	0	0	0	0 0	0	0
q3: fc15	1	10000-50000	0	0	0	0 0	0	0

```
Interface: vni-0/1
```

```
Configuration:
```

```
Burst Size : 125000 bytes
Rate       : 30000 kbps
TC0: Network-Control      : 500-30000 kbps
TC1: Expedited-Forwarding : 30000-30000 kbps
TC2: Assured-Forwarding   : 15000-30000 kbps
TC3: Best-Effort          : 30000-30000 kbps
```

```
Traffic Stats:
```

```
TX Packets      : 1708
TX PPS          : 2
TX Packets Dropped : 0
TX Bytes        : 340234
TX bps          : 3736
TX Bytes Dropped : 0
```

```
Port Stats :
```

Traffic Class	TX Pkts	TX Dropped	TX Bytes	Bytes Dropped
tc0 network-control	358	0	67534	0
tc1 expedited-fwd	1350	0	272700	0
tc2 assured-fwd	0	0	0	0
tc3 best-effort	0	0	0	0

```
Pipe Stat:
```

```
Pipe ID       : 0
Users         : [ vni-0/1.0 ]
Type          : Access circuit
Configuration :
Burst Size    : 125000 bytes
Rate          : 30000 kbps
TC0: Network-Control      : 500-30000 kbps
TC1: Expedited-Forwarding : 30000-30000 kbps
TC2: Assured-Forwarding   : 15000-30000 kbps
TC3: Best-Effort          : 30000-30000 kbps
[snip]
```



STOP! Notify your instructor that you have completed this section of the lab.

Versa Adaptive Shaping

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the structure of the Class of Service configuration hierarchy
- Configure Class of Service services

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

Look for these
hints to help you
in the labs

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Exercise 1: Configure Adaptive Shaping

In the following lab exercises, you will:

- Locate the Adaptive Services configuration parameters
- Configure Adaptive Shaping
- Verify Adaptive Shaping

Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

In this lab part you will identify the configuration components required that will allow your device to advertise its local interface speed to the remote devices. Testing of the changes you make on your device will be verified by logging into the Hub device, as changes made on your device will advertise your link rates to the hub, and the hub will apply dynamic shapers towards your device.

The following components are required for a complete adaptive shaping configuration:

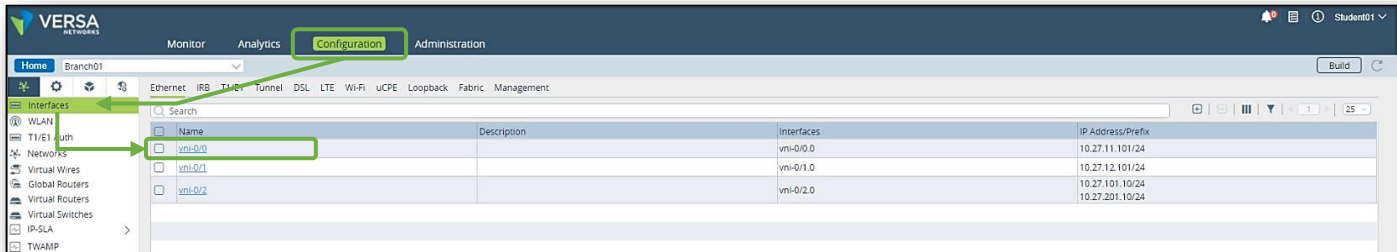
- Shaping configured on the local interfaces (in order to apply dynamic shapers towards remote sites)
- The local circuit speeds must be defined (this provides the value that will be used to trigger Advertised Link Rate adjustments)
- Adaptive Shaping function: This adds the Advertised Link Rate value to remote sites using MP-BGP (Versa-Private Route), and defines the circumstances that will trigger an update
- Inbound Shaper: This defines the Advertised Link Rate value that is advertised by the device

The hub already has shaping configured on its WAN interfaces, and therefore will respond to advertised link rate information sent from your site. In this lab you will begin by configuring the local site circuit bandwidth. You will configure a different bandwidth for the MPLS and INET links.

You will perform the lab configuration from the Appliance Context mode and not through device templates. To open the Appliance Context mode for your device, navigate to *Administration > Appliances* and locate your device in the appliances list. Click on your device to open your appliance.

From your Appliance Context mode, click the *Configuration* tab to access your device configuration.

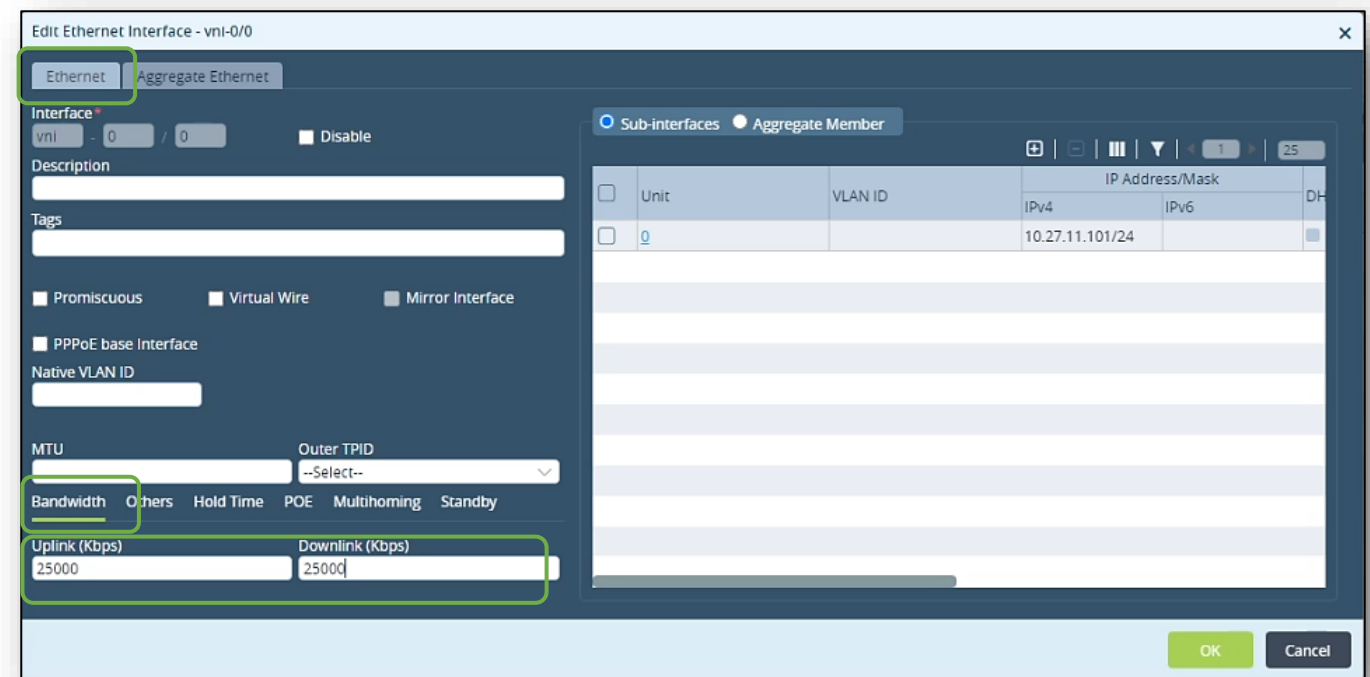
The circuit speeds are configured under the *Networking > Interfaces* configuration. Open the Interfaces configuration dashboard:



The WAN interfaces are vni-0/0 (INET link) and vni-0/1 (MPLS link).

Click on the vni-0/0 interface to open the interface configuration. In the Ethernet tab, locate the Bandwidth setting. It should be blank.

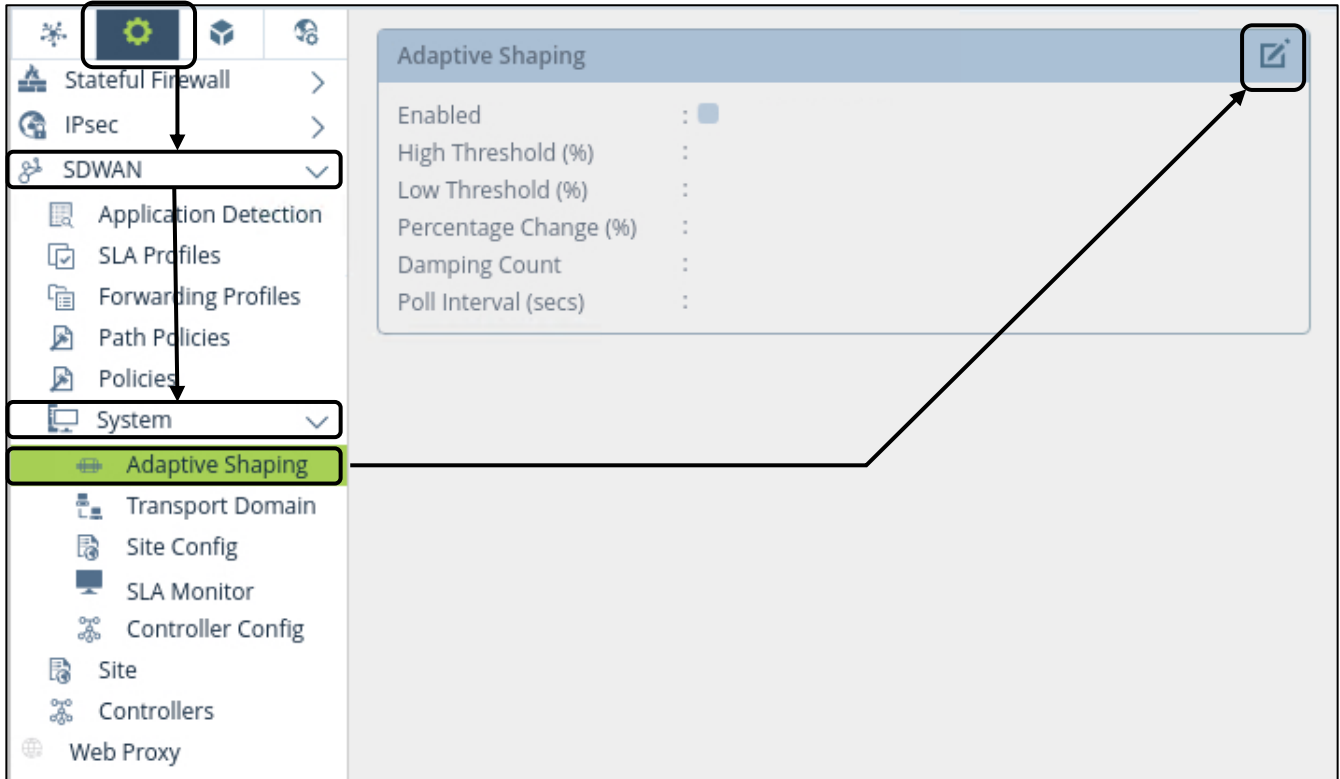
Set the Uplink and Downlink bandwidth to 25000Kbps (25mbps), then click OK to apply the setting.



Repeat the process on the vni-0/1 interface.

After you have configured the Uplink and Downlink speeds on the interface you need to enable Adaptive Shaping.

To enable Adaptive Shaping, navigate to Services > SDWAN > System > Adaptive Shaping. The Adaptive Shaping function is a system function. Click on the edit (Pencil) button to open the Adaptive Shaping configuration dialog.



When the Edit Adaptive Shaping dialog appears, the Enable setting will automatically be checked. The default settings are shown. For our lab exercise, the default settings will work. Click the OK button to apply the changes and enable the Adaptive Shaping function. The parameters from the dialog should now appear in the Adaptive Shaping information on the main Adaptive Shaping dashboard.

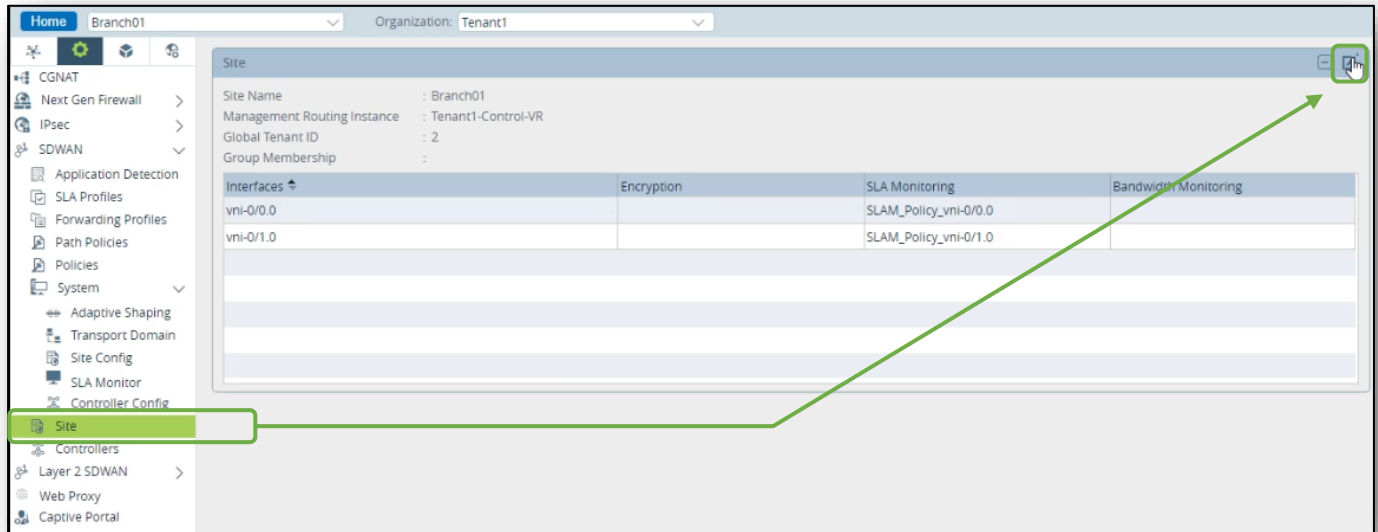
The 'Edit Adaptive Shaping' dialog box is shown. It has a title bar with a close button (X). The 'Enable' checkbox is checked. The settings are as follows:

High Threshold (%)	Low Threshold (%)
85	10
Percentage Change (%)	Damping Count
10	1
Poll Interval (secs)	
10	

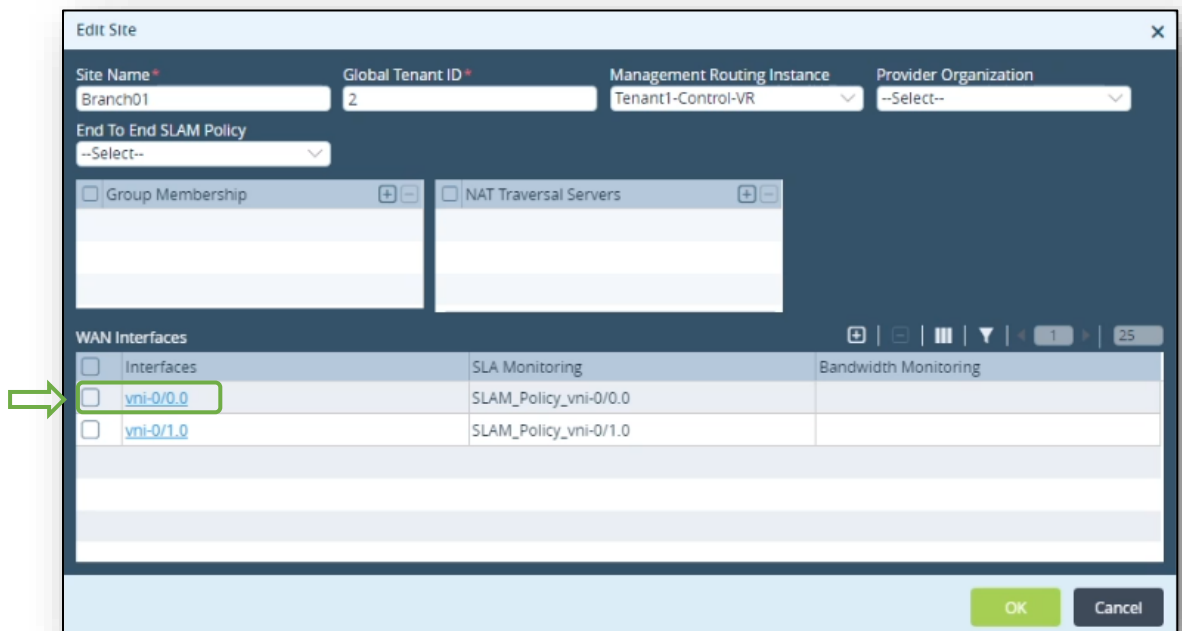
At the bottom right, there are two buttons: 'OK' (green) and 'Cancel' (grey).

The final step to complete the Adaptive Shaping configuration is to configure the inbound shaping value. This is the value that will be advertised to the remote sites and it is found under the *Services > SDWAN > Site* parameters.

Navigate to the Services > SDWAN > Site hierarchy and click on the pencil icon to edit the site properties:



In the Edit Site dialog, locate the WAN interfaces. Click on the vni-0/0.0 interface to modify the interface settings.



The WAN Interfaces configuration dialog allows you to configure an Input Rate and Minimum Input Rate. The Input rate is the default rate that will be advertised to remote sites. The Minimum Input Rate is the lowest value that will be advertised to remote sites (the lowest value the Adaptive Shaping algorithm can advertise.)

Set the Shaping Input rate of your device according the table below. Each site will have a unique rate configured, which will assist in verifying the advertised rate.

vni-0/0.0

Branch Device	Input Rate	Minimum Input Rate
Branch01	10001	1001
Branch02	10002	1002
Branch03	10003	1003
Branch04	10004	1004
Branch05	10005	1005
...Branch24	10024	1024

vni-0/1.0

Branch Device	Input Rate	Minimum Input Rate
Branch01	11101	1101
Branch02	11102	1102
Branch03	11103	1103
Branch04	11104	1104
Branch05	11105	1105
...Branch24	11124	1124

Edit WAN Interfaces

Interfaces * vni-0/0.0 Encryption --Select--

Shaping Rate

☒ Rate (Kbps) Input Rate(Kbps) 10001 Minimum Input Rate(Kbps) 1001

☐ Rate (%)

Management Traffic

Priority 0

SLA Monitoring Policy

SLA Monitoring SLAM_Policy_vni-0/0.0

Bandwidth Monitoring Policy

Bandwidth Monitoring --Select--

OK Cancel

Example of vni-0/0.0

You have finished configuring Adaptive Shaping on your branch device.

Exercise 2: Verify the Advertised Link Rate and dynamic shapers on the Hub device

Your device should now be advertising its local link rates to the other devices in the network. You will verify your advertised link rate by logging in to the hub device. On the hub device you will verify that your advertised link rate has been received, and that the hub device has applied dynamic shapers on the tunnels to your branch device.

Locate the MT-Putty shortcut on your remote desktop task bar. Open the MT-Putty application and open an SSH session to the hub device.

On the hub device, enter the command **cli** to start the command line interface. From the CLI on the hub device, enter the command **show class-of-services**. You will see output from all of the interfaces and for all of the tunnels. You will need to look for a Pipe ID that has a rate that matches your sites configured Input Shaping rate. To help you find your sites Pipe (tunnel), you can use the following command: *show class-of-services | find [your site's bandwidth setting]:e.g. **show class-of-services | find 10001***

You should see output that reflects the configured inbound shaping parameter that you configured on your device in an earlier step.

```
dmin@Hub-cli> show class-of-services | find 10001
```

```
Rate : 10001 kbps
```

Traffic Stats:

Queues	Tx Pkts	Tx Dropped	Tx Bytes	Bytes Dropped	Qlen
tc0 network-control:					
q0: fc_nc	0	0	0	0	0
q1: fc1	0	0	0	0	0
q2: fc2	0	0	0	0	0
q3: fc3	0	0	0	0	0
tc1 expedited-fwd:					
q0: fc_ef	0	0	0	0	0
q1: fc5	0	0	0	0	0
q2: fc6	0	0	0	0	0
q3: fc7	0	0	0	0	0
tc2 assured-fwd:					
q0: fc_af	0	0	0	0	0
q1: fc9	0	0	0	0	0
q2: fc10	0	0	0	0	0
q3: fc11	0	0	0	0	0
tc3 best-effort:					
q0: fc_be	0	0	0	0	0
q1: fc13	0	0	0	0	0
q2: fc14	0	0	0	0	0
q3: fc15	0	0	0	0	0

Pipe ID : 2

Users : [WAN-103:17:2:secure]

Type : SDWAN

Configuration :

```
Rate : 10001 kbps
```

Traffic Stats:

Queues	Tx Pkts	Tx Dropped	Tx Bytes	Bytes Dropped	Qlen
tc0 network-control:					
q0: fc_nc	0	0	0	0	0
q1: fc1	0	0	0	0	0
q2: fc2	0	0	0	0	0
q3: fc3	0	0	0	0	0

You can use the same command to display the dynamic shaper on the hub's INET interface by issuing the same command, but substitute the INET inbound shaping rate configured on your site (e.g. 11110)

```
admin@Hub-cli> show class-of-services | find 11110
Rate : 11101 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes        Dropped
tc0 network-control:
  q0: fc_nc        0           0           0           0      0
  q1: fc1          0           0           0           0      0
  q2: fc2          0           0           0           0      0
  q3: fc3          0           0           0           0      0
tc1 expedited-fwd:
  q0: fc_ef        0           0           0           0      0
  q1: fc5          0           0           0           0      0
  q2: fc6          0           0           0           0      0
  q3: fc7          0           0           0           0      0
tc2 assured-fwd:
  q0: fc_af        0           0           0           0      0
  q1: fc9          0           0           0           0      0
  q2: fc10         0           0           0           0      0
  q3: fc11         0           0           0           0      0
tc3 best-effort:
  q0: fc_be        0           0           0           0      0
  q1: fc13         0           0           0           0      0
  q2: fc14         0           0           0           0      0
  q3: fc15         0           0           0           0      0

Pipe ID      : 2
Users       : [ WAN-103:34:2:secure ]
Type        : SDWAN
Configuration:
Rate : 11101 kbps
Traffic Stats:
  Queues          TX          TX          TX          Bytes  Qlen
                  Pkts        Dropped      Bytes        Dropped
tc0 network-control:
  q0: fc_nc        0           0           0           0      0
  q1: fc1          0           0           0           0      0
  q2: fc2          0           0           0           0      0
  q3: fc3          0           0           0           0      0
```



STOP! Notify your instructor that you have completed this lab.

Versa Application Steering and SLA

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the components required to enable traffic steering using SD-WAN Policy
- Identify the components used to measure and monitor transport path statistics
- Configure SD-WAN Profiles to define how application traffic should be treated
- Configure SD-WAN Policy to assign traffic flows to SD-WAN Profiles

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Exercise 1: Create SLA Profiles to Track Link Statistics

In the following lab exercises, you will:

- Configure a set of SLA profiles that can be used to monitor the performance of links between sites

Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

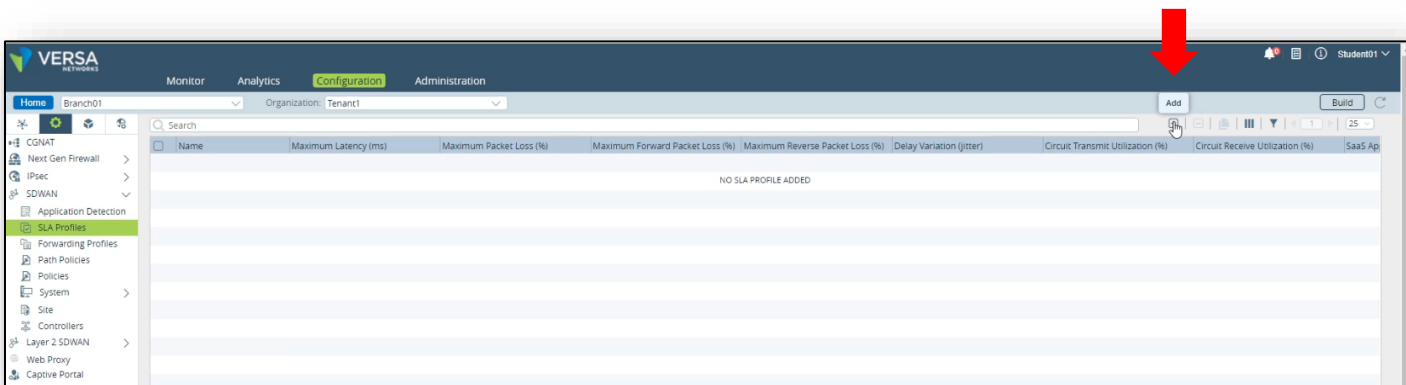
Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

The SLA Monitoring process is constantly running on Versa Operating System. Each device sends probes to other devices on all available transport networks (paths) to determine the path performance, and the statistics that are gathered are automatically sent to Versa Analytics.

You can configure your device to use the statistics that are gathered to determine whether a transport path is suitable for different types of applications, based on administrative rules. To configure your device to track SLA statistics you configure SLA profiles.

SLA profiles are configured under the Configuration > Services > SLA Profiles hierarchy.

Navigate to the Configuration > Services > SLA Profiles hierarchy. Click the Add button to create SLA profiles.



Add SLA Profile

General SaaS App Monitor

Name* 2-percent-loss

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 30ms-Delay

General SaaS App Monitor

Name* 30ms-Delay

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 30ms-Delay-20ms-Jitter

General SaaS App Monitor

Name* 30ms-Delay-20ms-Jitter

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Add SLA Profile

General SaaS App Monitor

Name* 5-percent-loss

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - 60ms-Delay

General SaaS App Monitor

Name* 60ms-Delay

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Low-Delay-Low-Packet-Loss

General SaaS App Monitor

Name* Low-Delay-Low-Packet-Loss

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☒ Low Delay Variation ☐ Low Latency ☒ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Low-Delay-Only

General SaaS App Monitor

Name* Low-Delay-Only

Description

Tags

Packet Delay-variation (jitter) Circuit Transmit Utilization (%) Circuit Receive Utilization (%)

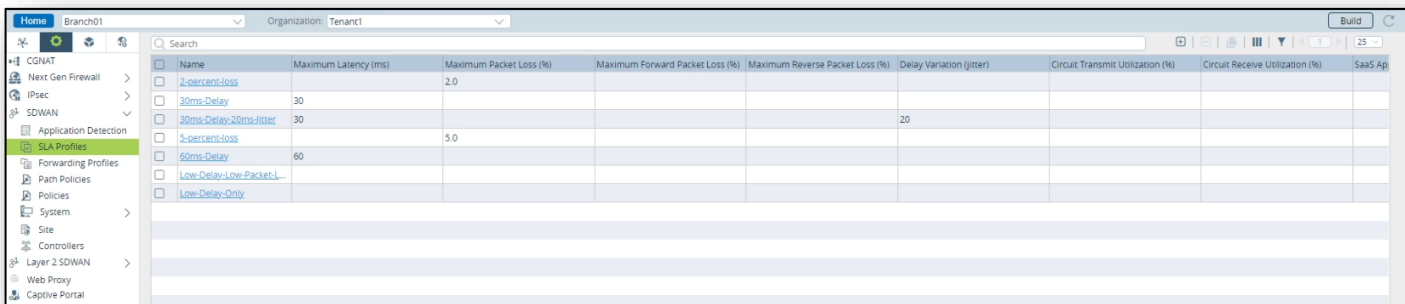
Maximum Packet Loss (%) Maximum Forward Packet Loss (%) Maximum Reverse Packet Loss (%)

Maximum Latency (ms) MOS Score

☒ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel


When finished, your SLA profiles should look similar to the result below.



Name	Maximum Latency (ms)	Maximum Packet Loss (%)	Maximum Forward Packet Loss (%)	Maximum Reverse Packet Loss (%)	Delay Variation (Jitter)	Circuit Transmit Utilization (%)	Circuit Receive Utilization (%)	SaaS Ap
2-percent-loss		2.0						
30ms-Delay	30							
30ms-Delay-20ms-Jitter	30				20			
5-percent-loss		5.0						
60ms-Delay	60							
Low-Delay-Low-Packet-Loss								
Low-Delay-Only								

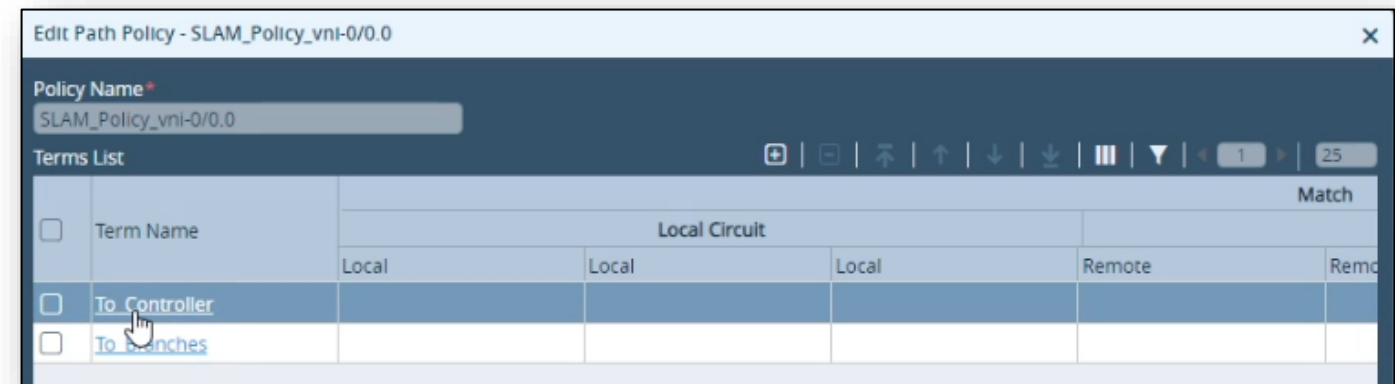
Next you will adjust the SLA probe frequency on your links. This is done with two steps. The first step is to modify the Path Policies. The path policies determine the properties of the SLA probe system. The second step is to ensure that the policies are applied to the interfaces. Because the default policies are already applied to the interfaces, you will only verify that the policies are applied.

Navigate to Configuration > Services > SD-WAN > Path Policies and locate the 2 default path policies. Click on the SLAM_Policy-vni-0/0.0 name to open the policy for editing.



Name	Terms
SLAM_Policy-vni-0/0.0	To_Controller To_Branches
SLAM_Policy-vni-0/1.0	To_Controller To_Branches

In the SLAM_Policy-vni-0/0.0, click the To_Controller term to open the term.



Edit Path Policy - SLAM_Policy-vni-0/0.0						
Policy Name *						
SLAM_Policy-vni-0/0.0						
Terms List						
	Term Name	Local Circuit			Match	
		Local	Local	Local	Remote	Remote
<input type="checkbox"/>	To_Controller					
<input type="checkbox"/>	To_Branches					

In the To_Controller term, select the Action tab and locate the forwarding class specific configuration. There should be a ForwardingClass 0 setting configured by default. Open the ForwardingClass 0 entry.

Edit Terms

Term Name *

Match **Action**

SLA Monitoring

Interval (milliseconds)

Logging Interval (secs)

Loss Threshold

☐ **Adaptive SLA Monitoring**

Inactivity Interval (secs)

Suspend Interval (secs)

☐ Data Driven

Forwarding Class

FC General Config

☐ Forwarding Class

FC Specific Config

		SLA Monitoring		
		Interval	Logging Interval	Loss T
<input type="checkbox"/>	Forwarding Class			
<input type="checkbox"/>	Forwarding Class 0 (Net...			

Bandwidth Monitoring

Interval (mins)

OK **Cancel**

The default timers are built into the system, so they don't appear in the configuration explicitly. Modify the SLA Monitoring interval and set it to 20 seconds (20000ms).

Click OK to accept the new settings, then click OK in the Edit Terms window to finish editing the To_Controller term.

Edit Terms Edit Forwarding Class Specific Config

Forwarding Class*
Forwarding Class 0 (Network-Control)

SLA Monitoring

Interval (milliseconds)
20000

Logging Interval (secs)

Loss Threshold

☐ **Adaptive SLA Monitoring**

Inactivity Interval (secs)

Suspend Interval (secs)

OK **Cancel**

Click the To_Branches term to open and modify the term.

Edit Path Policy - SLAM_Policy_vni-0/0.0

Policy Name*
SLAM_Policy_vni-0/0.0

Terms List

	Term Name	Local Circuit					Match
		Local	Local	Local	Remote	Remo	
<input type="checkbox"/>	To_Controller						
<input type="checkbox"/>	To_Branches						

In the Action tab of the To_Branches term, select the Forwarding Class 4 SLA probe option and change the interval to 4 seconds (4000ms).

Edit Terms Edit Forwarding Class Specific Config

Forwarding Class *
 Forwarding Class 4 (Expedited-Forwarding)

SLA Monitoring

Interval (milliseconds)
 4000

Logging Interval (secs)
 [Empty]

Loss Threshold
 [Empty]

☒ Adaptive SLA Monitoring

Inactivity Interval * (secs)
 300

Suspend Interval * (secs)
 30

OK Cancel

Uncheck and re-check this box to populate the form fields.

Click OK to accept the parameter change, then click OK in the Edit Terms dialog to finish editing the To_Branches term. Click OK on the Edit Path Policy dialog to apply the changes.

[illegible]

Exercise 2: Analyze and Verify SLA Probe Information

In the following lab exercise you will locate and analyze the SLA probe statistics in the Versa Director Monitor tab for your appliance.

In Versa Director, navigate to the Monitor tab of your device. In your device Monitor tab, navigate to **Services > SDWAN > SLA Metrics**. Select the Hub device from the drop-down to view the SLA statistics between your branch device and the hub device.

The screenshot shows the Versa Director interface with the Monitor tab selected. The left sidebar shows the navigation menu with 'Monitor' highlighted. The main content area displays 'Branch01 : 172.15.0.4' with a location of 'San Jose, CA, USA' and a status of 'Reachable'. Below this, there are two main sections: 'Services' and 'Networking'. The 'Services' section includes icons for SDWAN, NGFW, CGNAT, SDLAN, IPSEC, Sessions, SCI, and Secure Access. The 'Networking' section includes icons for Interfaces, Routes, BGP, OSPF, OSPFv3, BFD, DHCP, DNS Stats, COS, VRRP, LDP, ARP, IP-SLA, PIM, IGMP, doctx, and RIP. Below these sections, there is a table titled 'SLA Metrics' with columns for Path Handle, Fwd Class, Local WAN Link, Remote WAN Link, Local WAN Link ID, Remote WAN Link ID, Two Way Delay, Fwd Delay Vari, Rev Delay Vari, PDU Loss Ratio, Fwd Loss Ratio, Rev Loss Ratio, Fwd Loss, Rev Loss, PDU Sent, and PDU Rcvd. The table shows two rows of data for paths 6754564 and 6758916.

Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Two Way Delay	Fwd Delay Vari	Rev Delay Vari	PDU Loss Ratio	Fwd Loss Ratio	Rev Loss Ratio	Fwd Loss	Rev Loss	PDU Sent	PDU Rcvd
6754564	fc_ef	INET	INET	1	1	5	5	0	0.0	0.0	0.0	0	0	2	2
6758916	fc_ef	MPLS	MPLS	2	2	0	0	0	0.0	0.0	0.0	0	0	5	5

Select the SLA Paths tab to view the SLA probe status between sites. In the SLA Paths dialog, select the Hub site from the dropdown menu to view the SLA probe status between your branch and the hub device.

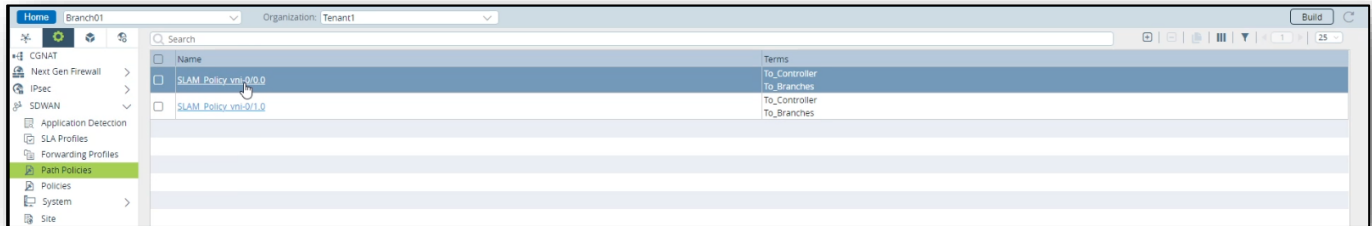
The screenshot shows the Versa Director interface with the Monitor tab selected. The left sidebar shows the navigation menu with 'Monitor' highlighted. The main content area displays 'Branch01 : 172.15.0.4' with a location of 'San Jose, CA, USA' and a status of 'Reachable'. Below this, there are two main sections: 'Services' and 'Networking'. The 'Services' section includes icons for SDWAN, NGFW, CGNAT, SDLAN, IPSEC, Sessions, SCI, and Secure Access. The 'Networking' section includes icons for Interfaces, Routes, BGP, OSPF, OSPFv3, BFD, DHCP, DNS Stats, COS, VRRP, LDP, ARP, IP-SLA, PIM, IGMP, doctx, and RIP. Below these sections, there is a table titled 'SLA Paths' with columns for Path Handle, Fwd Class, Local WAN Link, Remote WAN Link, Local WAN Link ID, Remote WAN Link ID, Adaptive Monitoring, Damp State, Damp Flaps, Conn State, Flaps, and Last Flapped. The table shows two rows of data for paths 6754564 and 6758916.

Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State	Damp Flaps	Conn State	Flaps	Last Flapped
6754564	fc_ef	INET	INET	1	1	active	disable	0	up	1	00:41:40
6758916	fc_ef	MPLS	MPLS	2	2	active	disable	0	up	1	00:40:43

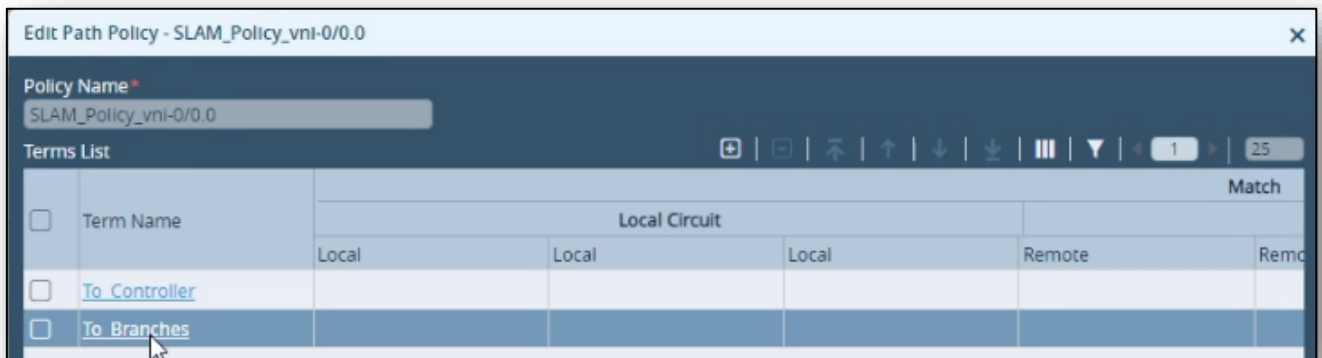
Note that the Adaptive Monitoring status should be active, meaning the probes are actively being sent between sites.

Return to the Configuration > Services > SDWAN > Path Policies hierarchy so that you can modify the adaptive SLA parameters on one of the WAN links.

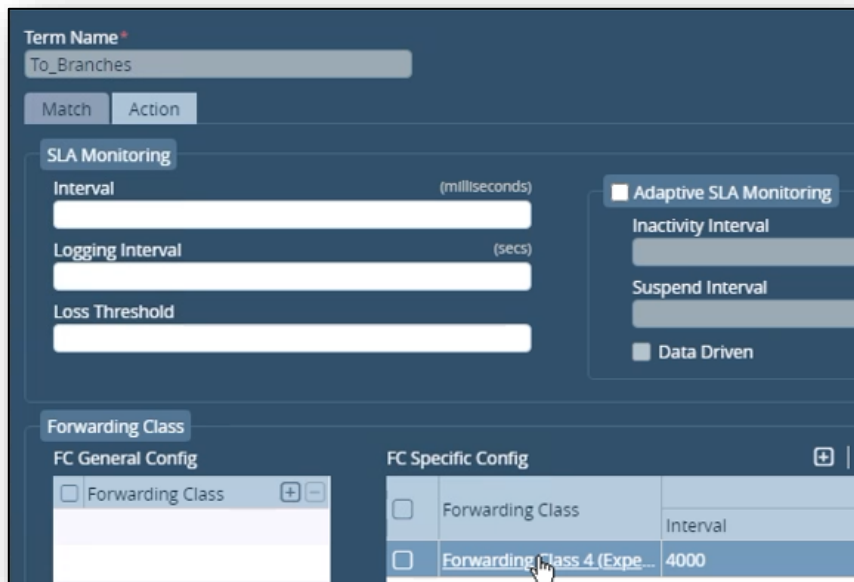
In the Path Policies table, click the SLAM_Policy_vni-0/0.0 policy to open the policy for editing.



Open the To_Branches term.



Select the Action tab, then select the Forwarding Class 4 options.



In the Forwarding Class 4 options, enable Adaptive SLA Monitoring and enter a 30 second interval and 300 second suspend interval.

Click OK on the dialog boxes until you have finished applying the configuration changes.

Once you have applied the adaptive SLA monitoring parameters, return to the Monitor > Services > SDWAN > SLA Paths dialog to view the Adaptive Monitoring status.

Path Handle	Field Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State	Damp Flaps	Conn State	Flaps	Last Flapped
6754564	ft_ef	INET	INET	1	1	suspend	disable	0	up	1	00:43:52
6758916	ft_ef	MPLS	MPLS	2	2	suspend	disable	0	up	1	00:00:12

If the status for the MPLS circuit is NOT in suspend mode, wait 10 seconds and then refresh the window. If you refresh the window more than 2 times and the status does not change to suspend, verify that the Adaptive SLA configuration parameters are properly configured.

Open the MT-PuTTY application and start an SSH session to your testing host device (Branch01-PC, Branch02-PC, etc.)

From the command line on the testing PC, issue the **ping 10.27.130.99 -c 5** command to send 5 ICMP packets to the address 172.16.105.1 (the LAN gateway address on the hub site).

Return to the Versa Director SLA Paths monitoring window. Refresh the table by selecting a different site from the site dropdown menu, then select the Hub site again. The Adaptive Monitoring status should have changed to active because you sent data packets between the sites with the Ping utility.

Aggregate Traffic Application Metrics Forwarding Profiles MOS Policies Sessions Sites SLA End To End Paths SLA Metrics SLA Paths Transport Paths Web Proxy								
Hub105								
Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State	Damp Flaps
6623492	fc_ef	MPLS	MPLS	1	1	active	disable	0
6627844	fc_ef	INET	INET	2	2	active	disable	0

Wait 30 seconds, then refresh the table (select a different remote site, then select Hub again). The MPLS link Adaptive Monitoring status should return to suspend state.

Aggregate Traffic Application Metrics Forwarding Profiles MOS Policies Sessions Sites SLA End To End Paths SLA Metrics SLA Paths Transport Paths Web Proxy								
Hub105								
Path Handle	Fwd Class	Local WAN Link	Remote WAN Link	Local WAN Link ID	Remote WAN Link ID	Adaptive Monitoring	Damp State	Damp Flaps
6623492	fc_ef	MPLS	MPLS	1	1	suspend	disable	
6627844	fc_ef	INET	INET	2	2	active	disable	

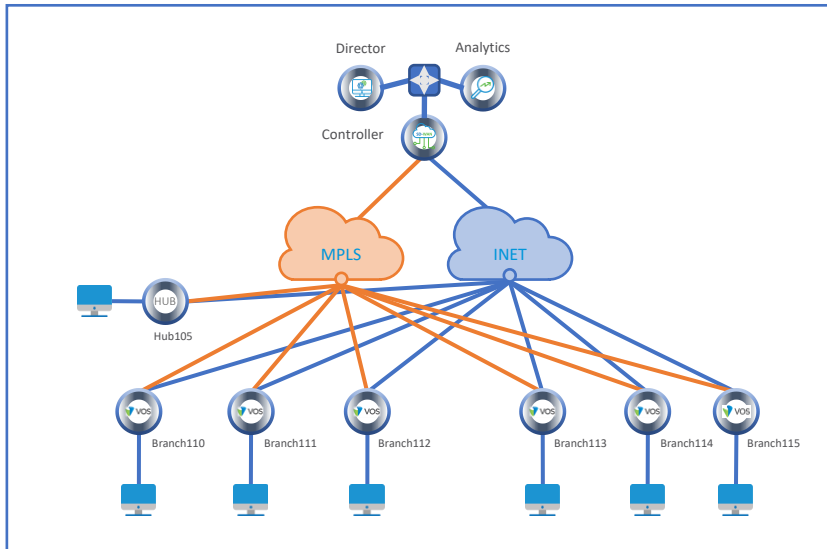


STOP! Notify your instructor that you have completed this lab.

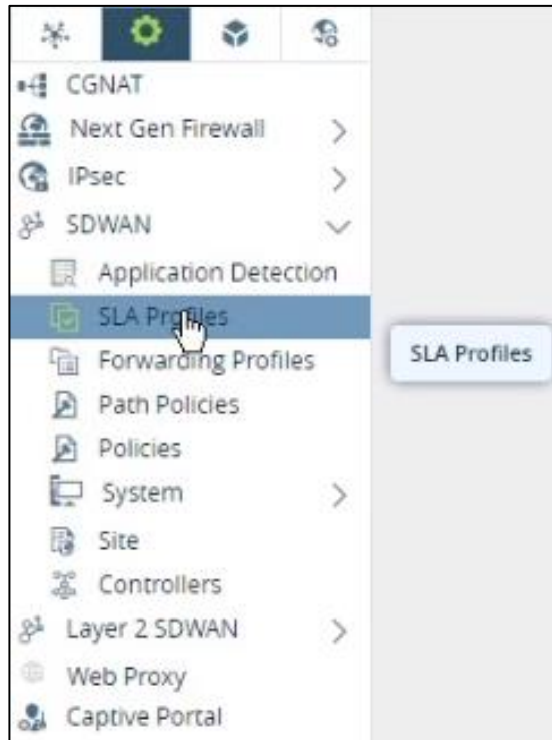
Description of the Environment

VERSA NETWORKS LAB GUIDE

- The topology for this example:



- To begin, if you plan to use path statistics to help determine forwarding paths, create SLA profiles that analyze the desired performance statistics



Name	Maximum Latency (ms)	Maximum Packet Loss (%)	Maximum Forward Packet Loss (%)	Maximum Reverse Packet Loss (%)	Delay Variation (Jitter)	Circuit Transmit Utilization (%)	Circuit Receive Utilization (%)	SaaS Ap
Latency-30ms	30							
Latency-50-Jitter-20	50				20			
Packet-Loss-5-Percent		5						
Packet-Loss-3-Percent		3						

Name	Maximum Latency (ms)	Maximum Packet Loss (%)	Maximum Forward Packet Loss (%)	Maximum Reverse Packet Loss (%)	Delay Variation (jitter)	Circuit Transmit Utilization (%)	Circuit Receive Utilization (%)	SaaS Ap
Latency-30ms	30							
Latency-50-jitter-20	50				20			
Packet-Loss-5-Percent		5						
Packet-Loss-3-Percent		3						

Add SLA Profile

General SaaS App Monitor

Name*
Latency-30ms

Description

Tags

Packet Delay-variation (jitter) * Circuit Transmit Utilization (%) * Circuit Receive Utilization (%) *

Maximum Packet Loss (%) * Maximum Forward Packet Loss (%) * Maximum Reverse Packet Loss (%) *

Maximum Latency (ms) * MOS Score *

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Add SLA Profile

General SaaS App Monitor

Name*
Latency-50-jitter-20

Description

Tags

Packet Delay-variation (jitter) * Circuit Transmit Utilization (%) * Circuit Receive Utilization (%) *

20

Maximum Packet Loss (%) * Maximum Forward Packet Loss (%) * Maximum Reverse Packet Loss (%) *

Maximum Latency (ms) * MOS Score *

50

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Packet-Loss-5-Percent

General SaaS App Monitor

Name*
Packet-Loss-5-Percent

Description

Tags

Packet Delay-variation (jitter) * Circuit Transmit Utilization (%) * Circuit Receive Utilization (%) *

Maximum Packet Loss (%) * Maximum Forward Packet Loss (%) * Maximum Reverse Packet Loss (%) *

5

Maximum Latency (ms) * MOS Score *

☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

Edit SLA Profile - Packet-Loss-3-Percent

General SaaS App Monitor

Name*
Packet-Loss-3-Percent

Description

Tags

Packet Delay-variation (jitter) * Circuit Transmit Utilization (%) * Circuit Receive Utilization (%) *

Maximum Packet Loss (%) * Maximum Forward Packet Loss (%) * Maximum Reverse Packet Loss (%) *

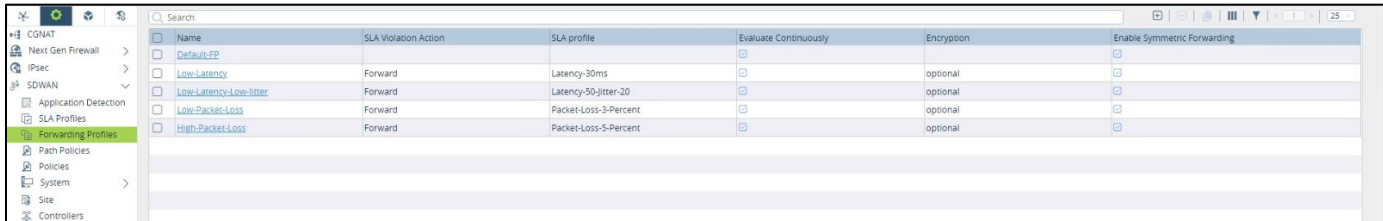
3

Maximum Latency (ms) * MOS Score *

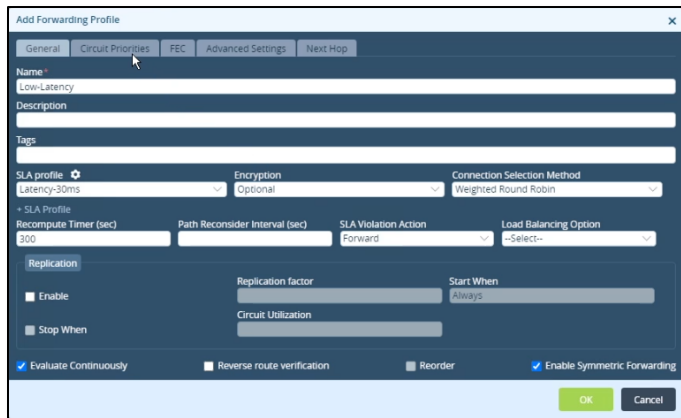
☐ Low Delay Variation ☐ Low Latency ☐ Low Packet Loss ☐ Low Forward Packet Loss ☐ Low Reverse Packet Loss

OK Cancel

- Next you define the forwarding profiles. These determine how to treat traffic that is sent to the profile.



Name	SLA Violation Action	SLA profile	Evaluate Continuously	Encryption	Enable Symmetric Forwarding
<input type="checkbox"/> Default-FP			<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/> Low-Latency	Forward	Latency-30ms	<input type="checkbox"/>	optional	<input type="checkbox"/>
<input type="checkbox"/> Low-Latency-Low-Jitter	Forward	Latency-50-jitter-20	<input type="checkbox"/>	optional	<input type="checkbox"/>
<input type="checkbox"/> Low-Packet-Loss	Forward	Packet-Loss-3-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>
<input type="checkbox"/> High-Packet-Loss	Forward	Packet-Loss-5-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>



Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Name: Low-Latency

Description:

Tags:

SLA profile: Latency-30ms | Encryption: Optional | Connection Selection Method: Weighted Round Robin

SLA Profile Details:

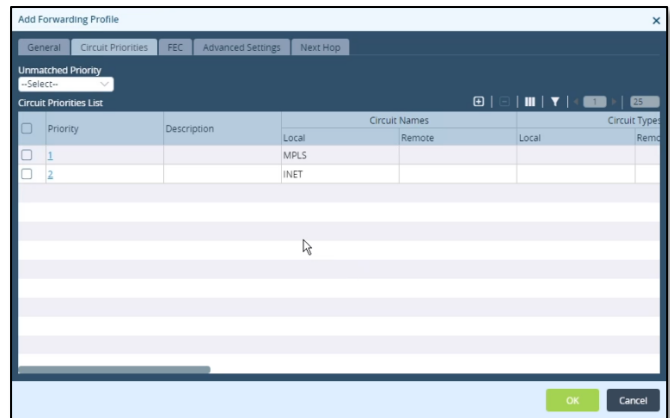
- Recompute Timer (sec): 300
- Path Reconsider Interval (sec):
- SLA Violation Action: Forward
- Load Balancing Option: --Select--

Replication:

- ☐ Enable
- ☐ Stop When
- Replication factor:
- Start When: Always
- Circuit Utilization:

☒ Evaluate Continuously | ☐ Reverse route verification | ☐ Reorder | ☒ Enable Symmetric Forwarding

OK Cancel



Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Unmatched Priority: --Select--

Circuit Priorities List:

Priority	Description	Local	Remote	Circuit Names	Local	Remote	Circuit Types
<input type="checkbox"/> 1				MPLS			
<input type="checkbox"/> 2				INET			

OK Cancel

- Next you define the forwarding profiles. These determine how to treat traffic that is sent to the profile.

Name	SLA Violation Action	SLA profile	Evaluate Continuously	Encryption	Enable Symmetric Forwarding
Default-FP			<input type="checkbox"/>		<input type="checkbox"/>
Low-Latency	Forward	Latency-30ms	<input type="checkbox"/>	optional	<input type="checkbox"/>
Low-Latency-Low-Jitter	Forward	Latency-50-Jitter-20	<input type="checkbox"/>	optional	<input type="checkbox"/>
Low-Packet-Loss	Forward	Packet-Loss-3-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>
High-Packet-Loss	Forward	Packet-Loss-5-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>

Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Name: Low-Latency-Low-Jitter

Description:

Tags:

SLA profile: --Select--
 --Select--
 Latency-30ms
 Latency-50-Jitter-20
 Packet-Loss-3-Percent
 Packet-Loss-5-Percent

Encryption: Optional

Connection Selection Method: Weighted Round Robin

SLA Violation Action: Forward

Load Balancing Option: --Select--

Replication factor:

Start When: Always

Circuit Utilization:

☒ Evaluate Continuously ☐ Reverse route verification ☐ Reorder ☒ Enable Symmetric Forwarding

OK Cancel

Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Unmatched Priority: --Select--

Circuit Priorities List

Priority	Description	Local	Remote	Local	Remote
1	MPLS INET				

OK Cancel

- Next you define the forwarding profiles. These determine how to treat traffic that is sent to the profile.

Name	SLA Violation Action	SLA profile	Evaluate Continuously	Encryption	Enable Symmetric Forwarding
Default-FP			<input type="checkbox"/>		<input type="checkbox"/>
Low-Latency	Forward	Latency-30ms	<input type="checkbox"/>	optional	<input type="checkbox"/>
Low-Latency-Low-Jitter	Forward	Latency-50-Jitter-20	<input type="checkbox"/>	optional	<input type="checkbox"/>
Low-Packet-Loss	Forward	Packet-Loss-3-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>
High-Packet-Loss	Forward	Packet-Loss-5-Percent	<input type="checkbox"/>	optional	<input type="checkbox"/>

Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Name: Low-Packet-Loss

Description:

Tags:

SLA profile: **Packet-Loss-3-Percent**

Encryption: Optional

Connection Selection Method: Weighted Round Robin

Slider Interval (sec):

SLA Violation Action: Forward

Load Balancing Option: --Select--

Replication factor:

Start When: Always

Circuit Utilization:

☒ Evaluate Continuously ☐ Reverse route verification ☐ Reorder ☒ Enable Symmetric Forwarding

OK Cancel

Add Forwarding Profile

General | Circuit Priorities | FEC | Advanced Settings | Next Hop

Unmatched Priority: --Select--

Circuit Priorities List:

Priority	Description	Local	Remote	Local	Remote
1		MPLS			
2		INET			

OK Cancel

- Next you define the forwarding profiles. These determine how to treat traffic that is sent to the profile.

Name	SLA Violation Action	SLA profile	Evaluate Continuously	Encryption	Enable Symmetric Forwarding
<input type="checkbox"/> Default-FP			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
<input type="checkbox"/> Low-Latency	Forward	Latency-30ms	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/> Low-Latency-Low-Jitter	Forward	Latency-50-jitter-20	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/> Low-Packet-Loss	Forward	Packet-Loss-3-Percent	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>
<input type="checkbox"/> High-Packet-Loss	Forward	Packet-Loss-5-Percent	<input checked="" type="checkbox"/>	optional	<input checked="" type="checkbox"/>

Add Forwarding Profile

General Circuit Priorities FEC Advanced Settings Next Hop

Name: High-Packet-Loss

Description:

Tags:

SLA profile: Packet-Loss-3-Percent 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 Replication factor: 2 Start When: Always

☒ Stop When: 80

☒ Evaluate Continuously ☐ Reverse route verification ☐ Reorder ☒ Enable Symmetric Forwarding

OK Cancel

Add Forwarding Profile

General Circuit Priorities FEC Advanced Settings Next Hop

Unmatched Priority: --Select--

Circuit Priorities List

Priority	Description	Local	Remote	Local	Remote
<input type="checkbox"/> 1		INET	MPLS		

OK Cancel

Add Forwarding Profile

General Circuit Priorities FEC Advanced Settings Next Hop

Sender

☒ Enable Duplicate FEC Packet: disable FEC Packet: Alternate Circuit

Maximum FEC Packet Size: 1400 Number of Packets per FEC: 4 Start When: Always

☒ Stop When: 80 Circuit Utilization: 80

Receiver

☒ Recovery ☒ Preserve Order

Maximum FEC Packet Size: 1400

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule No.	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-LowJitter				Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency				Predefined Filters: VOIP		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Packet-Loss				Predefined: ZOOM, YOU...			
4	Non-Critical-Apps	False	Allow	High-Packet-Loss				SaaS groups: Office365-A...	Predefined: social_netwo...		

Add Rules

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

Name: Critical-Voice

Description: 15/63

☐ Disable Rule

OK Cancel

Add Rules

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

☐ Source Zone ☐ Destination Zone ☐ Source Site Name ☐ Destination Site Name

☐ Source Address ☐ Destination Address

☐ Source Address Negate ☐ Destination Address Negate

Routing Instance: --Select--

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule No.	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-Low-jitter				Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency				Predefined Filters: VOIP		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Packet-Loss				Predefined Filters: Audio...			
4	Non-Critical-Appls	False	Allow	High-Packet-Loss				SaaS groups: Office365-A...			

Add Rules

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

Applications

☐ Application List

☐ VOIP

☐ SKYPE

☐ MS_TEAMS

☐ SIP

☐ SIP_SOAP

+ New Group + New Filter + New Application

SaaS Application Groups

☐ SaaS Application Group List

OK Cancel

Add Rules

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

Forwarding

Action: Allow Flow

Forwarding Profile: --Select--

Next Hop IP address: --Select--

IP Address: --Select--

Enable Symmetric Forwarding of Return Traffic: ☐

Monitor: ☐

Address: --Select--

IP Address: --Select--

Action: --Select--

Threshold (Events):

Routing Instance: --Select--

Interval (sec):

Forwarding Profile: Low-Latency-Low-jitter

Logging: ☐ Default Profile

LEF Profile: --Select--

Event: Never

Rate Limit: 10

TCP Optimization: ☐

Bypass Latency Threshold (msec):

Mode: --Select--

Lan Profile: --Select--

Wan Profile: --Select--

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule No.	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-Low-Jitter				Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency				Predefined Filters: VOIP...		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Latency				Predefined: ZOOM, YOU...		Tenant1-LAN-Zone	
4	Non-Critical-Appls	False	Allow	High-Packet-Loss				Predefined Filters: Audio...		Predefined: social_netwo...	

Add Rules

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

Name *
Non-Critical-Voice-Video

Description
24/63

☐ Disable Rule

OK Cancel

Add Rules

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

☐ Source Zone
☐ Tenant1-LAN-Zone
+ New Zone

☐ Destination Zone
+ New Zone

☐ Source Site Name
+ New Site

☐ Destination Site Name
+ New Site

☐ Source Address
+ New Address Group + New Address

☐ Destination Address
+ New Address Group + New Address

☐ Source Address Negate
Routing Instance
--Select--

☐ Destination Address Negate

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule No.	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone
1	Critical-Voice	False	Allow	Low-Latency-Low-jitter				Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone
2	Non-Critical-Voice-Video	False	Allow	Low-Latency				Predefined Filters: VOIP		Tenant1-LAN-Zone
3	Business-Applications	False	Allow	Low-Packet-Loss				Predefined Filters: Audio...		
4	Non-Critical-Apps	False	Allow	High-Packet-Loss				SaaS groups: Office365-A...	Predefined: social_netwo...	

Add Rules

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

Applications

- ☐ Application List
- ☐ ZOOM
- ☐ YOUTUBE
- ☐ stream
 - Application Filter
 - Pre-defined Filters
 - Audio-Video-Streaming
 - Applications
 - Pre-defined
 - ADNSTREAM
 - APPSTREAM
 - LIGHTSTREAMER
 - MS_STREAM

SaaS Application Groups

- ☐ SaaS Application Group List

OK Cancel

Add Rules

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

Forwarding

Action: Allow Flow | Forwarding Profile: --Select--

Next Hop IP address: IP Address | --Select--

☐ Enable Symmetric Forwarding of Return Traffic

Monitor

Address: IP Address | --Select--

Action: --Select-- | Interval(sec):

Threshold(Event):

Logging

LEF Profile: --Select-- | Default Profile: ☐

Event: Never | Rate Limit: 10

TCP Optimization

Bypass Latency Threshold (msec): --Select-- | Mode: --Select--

Lan Profile: --Select-- | Wan Profile: --Select--

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule Num...	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Enforce	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-Low-jitter					Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency					Predefined Filters: VOIP		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Packet-Loss					Predefined Filters: Audio...			
4	Non-Critical-Apps	False	Allow	High-Packet-Loss					Saas groups: Office365-A...	Predefined: social_netwo...		

Add Rules

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

Name: Business-Applications

Description: 21/63

☐ Disable Rule

OK Cancel

Add Rules

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

Applications

☐ Application List

+ New Group + New Filter + New Application

Saas Application Groups

☐ Saas Application Group List

- ☐ Office365-Apps
- ☐ GotoMeeting-Apps
- ☐ Concur-Apps
- ☐ ADP-Apps
- ☐ Amazon-Apps
- ☐ Box-Apps
- ☐ Citrix-Apps
- ☐ Docusign-Apps
- ☐ Dropbox-Apps
- ☐ Google-Apps
- ☐ IBM-Apps
- ☐ Intuit-Apps

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule No.	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Enforce	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone
1	Critical-Voice	False	Allow	Low-Latency-Low-Jitter					Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone
2	Non-Critical-Voice-Video	False	Allow	Low-Latency					Predefined Filters: VOIP...		Tenant1-LAN-Zone
3	Business-Applications	False	Allow	Low-Packet-Loss					Predefined Filters: Audio...		
4	Non-Critical-Apps	False	Allow	High-Packet-Loss					SaaS groups: Office365-A...	Predefined: social_newwo...	

Add Rules

Forwarding

Action: Allow Flow

Forwarding Profile: --Select--

Nexthop IP address: IP Address

Enable Symmetric Forwarding of Return Traffic: ☐

Monitor

Address: IP Address

Routing Instance: --Select--

Action: --Select--

Interval(sec):

Threshold(Events):

Logging

LEF Profile: --Select--

Event: Never

Rate Limit: 10

Default Profile: ☐

TCP Optimization

Bypass Latency Threshold (msec):

Mode: --Select--

Lan Profile: --Select--

Wan Profile: --Select--

OK Cancel

- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

Rule Num...	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Enforce	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-Low-jitter					Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency					Predefined: VOIP		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Packet-Loss					Predefined: ZOOM, YOU...			
4	Non-Critical-Apps	False	Allow	High-Packet-Loss					Predefined: Audio...			

Add Rules

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

Name *
Non-Critical-Apps

Description
17/63

☐ Disable Rule

OK Cancel

Add Rules

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

URL Categories

☐ URL Category List

☐ social_network

☐ entertainment_and_arts

☐ sports

☐ news

Pre-defined

news_and_media

+ New URL Category

OK Cancel

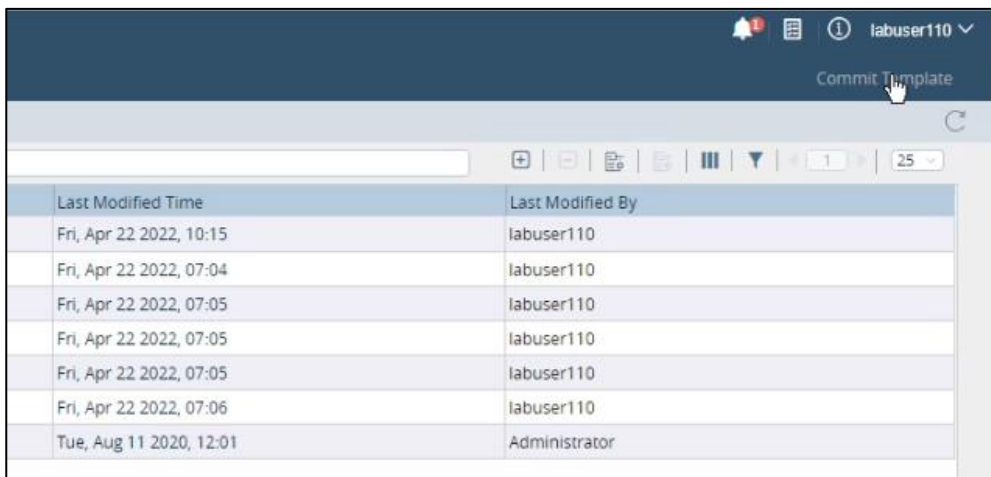
- Next you define the SD-WAN Rules. These analyze new sessions and assign them to one of the forwarding profiles based on the traffic requirements.

The screenshot shows the 'Policies > Rules' configuration page. A table lists four rules with their names, disabled status, forwarding actions, and profiles. Rule 1 is 'Critical-Voice' with 'Low-Latency-Low-Jitter' profile. Rule 2 is 'Non-Critical-Voice-Video' with 'Low-Latency' profile. Rule 3 is 'Business-Applications' with 'Low-Packet-Loss' profile. Rule 4 is 'Non-Critical-Apps' with 'High-Packet-Loss' profile.

Rule No...	Name	Rule Disabled	Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action	Services	Applications	URL Categories	Zone	Add
1	Critical-Voice	False	Allow	Low-Latency-Low-Jitter				Predefined: SKYPE, MS_T...		Tenant1-LAN-Zone	
2	Non-Critical-Voice-Video	False	Allow	Low-Latency				Predefined Filters: VOIP		Tenant1-LAN-Zone	
3	Business-Applications	False	Allow	Low-Packet-Loss				Predefined: ZOOM, YOU...			
4	Non-Critical-Apps	False	Allow	High-Packet-Loss				Predefined Filters: Audio...			

The 'Add Rules' dialog box is shown with the 'Forwarding' tab active. It contains fields for 'Action' (set to 'Allow Flow'), 'Nexthop IP address' (with a gear icon), 'Enable Symmetric Forwarding of Return Traffic' (checked), 'Forwarding Profile' (a dropdown menu with 'High-Packet-Loss' selected), 'Logging' (with 'LEF Profile' and 'Event' set to 'Never'), and 'TCP Optimization' (with 'Bypass Latency Threshold (msec)' and 'Mode' set to 'Never').

- Once the SD-WAN SLA Profiles, Forwarding Profiles, and Policy Rules have been created:
 - If the changes were made in a template, commit the template to rebuild the device configurations and copy the configurations to the appliances
 - If the changes were made in Appliance Context mode, the changes take effect immediately



Last Modified Time	Last Modified By
Fri, Apr 22 2022, 10:15	labuser110
Fri, Apr 22 2022, 07:04	labuser110
Fri, Apr 22 2022, 07:05	labuser110
Fri, Apr 22 2022, 07:05	labuser110
Fri, Apr 22 2022, 07:05	labuser110
Fri, Apr 22 2022, 07:06	labuser110
Tue, Aug 11 2020, 12:01	Administrator

- You can view the path statistics in the Monitor tab, or through the CLI on each device:

```
user@device-cli> show orgs org-services org-name sd-wan path path-metrics
```

REMOTE BRANCH	LOCAL CIRCUIT	REMOTE CIRCUIT	TWO WAY DELAY	FWD DELAY VAR	REV DELAY VAR	FWD LOSS PERCENTAGE	REV LOSS PERCENTAGE	PDU LOSS PERCENTAGE	RX BYTES	TX BYTES	VOICE MOS	AUDIO MOS	VIDEO MOS
Controller01	INET	INET	2	1	0	0.00	0.00	0.00	12626696	16967856	0.00	0.00	0.00
	MPLS	MPLS	2	0	0	0.00	0.00	0.00	157877844	306469548	0.00	0.00	0.00
Hub105	INET	INET	0	0	0	0.00	0.00	0.00	12919004	12919004	0.00	0.00	0.00
	MPLS	MPLS	0	2	0	0.00	0.00	0.00	12921460	12921452	0.00	0.00	0.00
branch111	INET	INET	0	0	0	0.00	0.00	0.00	11127852	11128596	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11129524	11128796	0.00	0.00	0.00
branch112	INET	INET	0	0	0	0.00	0.00	0.00	11129244	11130236	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11132096	11131120	0.00	0.00	0.00
branch113	INET	INET	1	0	0	0.00	0.00	0.00	11126700	11126036	0.00	0.00	0.00
	MPLS	MPLS	0	0	0	0.00	0.00	0.00	11127256	11128264	0.00	0.00	0.00
branch114	INET	INET	0	0	0	0.00	0.00	0.00	11127924	11128668	0.00	0.00	0.00
	MPLS	MPLS	1	0	0	0.00	0.00	0.00	11130348	11129604	0.00	0.00	0.00
branch115	INET	INET	0	0	0	0.00	0.00	0.00	11124408	11124956	0.00	0.00	0.00
	MPLS	MPLS	0	0	0	0.00	0.00	0.00	11126472	11126816	0.00	0.00	0.00

- Path Policy mapping can be displayed from the CLI

```
user@device-cli> show orgs org-services org-name sd-wan policies Default-Policy rules path-state brief
```

NAME	REMOTE BRANCH	FORWARDING PROFILE	SLA PROFILE	LOCAL CIRCUIT	REMOTE CIRCUIT	FORWARDING CLASS	PRIORITY
Critical-Voice	Controller01	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_nc	Priority 1
				MPLS	MPLS	fc_nc	Priority 1
	Hub105	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
	branch111	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
	branch112	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
	branch113	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
	branch114	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
	branch115	Low-Latency-Low-Jitter	Latency-50-Jitter-20	INET	INET	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1
Non-Critical-Voice-Video	Controller01	Low-Latency	Latency-30ms	INET	INET	fc_nc	Priority 2
				MPLS	MPLS	fc_nc	Priority 1
	Hub105	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
	branch111	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
	branch112	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
	branch113	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
	branch114	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
	branch115	Low-Latency	Latency-30ms	INET	INET	fc_ef	Priority 2
				MPLS	MPLS	fc_ef	Priority 1
				MPLS	MPLS	fc_ef	Priority 1

--More--

Versa Basic Security Services

The Versa Networks lab environment consists of a fixed, pre-configured topology that will allow you to explore, configure, and manage Versa Networks CPEs by using Versa Director, the central management and orchestration platform for a Versa Secure SD-WAN solution. After completing this lab, you will be able to:

- Identify the components required to enable basic Next Generation firewall and next-generation firewall services
- Configure basic next-generation firewall services

In this lab, you will be assigned a single CPE device (Branch device) for configuration and monitoring.

The lab environment is accessed through Amazon Workspaces. You should have received an email to allow you to register your Amazon Workspaces account and set your password.

NOTE: It is common for the Amazon Workspaces email to be sent to the spam/junk folder. If you have not received the registration email, check those folders.

The remote desktop connection opens a remote workstation, where you will use various tools to navigate and configure the lab environment. The main tool you will use in this lab is Versa Director. Versa Director can be accessed by opening the Google Chrome browser on the Remote Desktop. There is a bookmark to the Versa Director device in the Google Chrome bookmark bar.

This lab environment is a shared environment. There may be up to 24 students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not be the same, etc.) Do not be alarmed if your results vary slightly from the results shown in the lab guide. The important thing is that the lab functions in the desired manner.

This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

Now that we've discussed what is expected, let's get started!

Exercise 1: Configure Basic Security Services

In the following lab exercises, you will:

- Locate the SD-WAN security policy components
- Configure a basic Next-Generation Firewall policy

Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

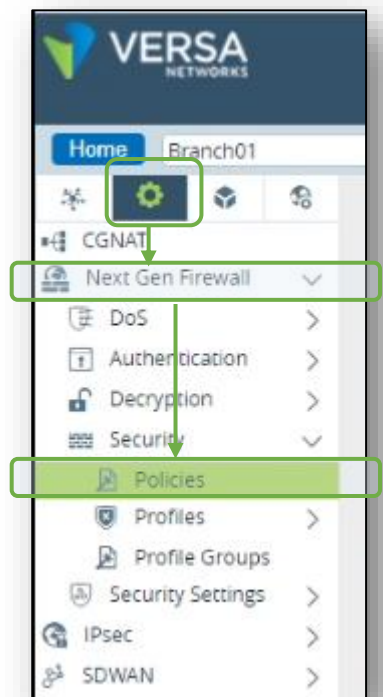
Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

In this lab part you will identify the configuration components required that will allow your device to perform standard next-generation firewall services on transit traffic.

The main configuration components related to security policy are located in the *Services > Stateful Firewall* or *Services > Next Gen Firewall* hierarchy of the configuration, depending on which type of services are enabled in the template workflow.

Navigate to *Administration > Appliances* and locate your appliance in the appliance list. Click your appliance name to open the Appliance Context mode of your device. From the Appliance Context mode of your device, click the *Configuration* tab to open the configuration of your device.

Navigate to the *Services > Next Gen Firewall > Security* hierarchy of the configuration and select Policies.



When security services are enabled in a workflow, 2 default policy rules are created to allow traffic from the local site to remote destinations and to allow SD-WAN traffic from remote sites to enter the local device through the SD-WAN tunnels.

Access Policies Rules									
Default-Policy Search									
<input type="checkbox"/>	Rule Nu...	Name	Enforce		Services	Applications	URL Categories	Zone	Reg
			Actions	Security Profiles					
<input type="checkbox"/>		Allow From Trust	Allow					LAN-Zone	
<input type="checkbox"/>		Allow From SDWAN	Allow					W-ST-Tenant1-LAN-VR-IN...	
<input type="checkbox"/>								ptvi	

In the next lab parts you will create new rules that will manage the types of traffic and applications that can be accessed from the local LAN. The branch device is configured for Direct Internet Access (DIA).

Access Policies Rules												
Default-Policy <input type="text" value="Search"/>												
<input type="checkbox"/>	Rule Nu...	Name	Rule Disabled	Alias Name	Actions	Enforce	Services	Applications	URL Categories	URL Reputations	Zone	Region
						Security Profiles						
<input type="checkbox"/>	1	Allow-Business-Apps	False		Allow		Predefined: http, https	Predefined: MS_TEAMS Predefined Groups: Am...			Intf-Tenant1-LAN-Zone	
<input type="checkbox"/>	2	Scan-Email	False		Allow	Scan Email Traffic		Predefined: GMAIL, LIVE...			Intf-Tenant1-LAN-Zone	
<input type="checkbox"/>	3	Work-Hour-Restrictions	False		Deny				Predefined: dating, gam...		Intf-Tenant1-LAN-Zone	
<input type="checkbox"/>	4	Blocked-Web	False		Deny				Predefined: abused_dru...		Intf-Tenant1-LAN-Zone	
<input type="checkbox"/>	5	Allow From SDWAN	False		Allow						pvti	
<input type="checkbox"/>	6	Allow From Trust	False		Allow						Intf-Tenant1-LAN-Zone	

Allow access to the following business applications from the branch to the Internet through the SD-WAN (Internet access is provided through the Hub device):

- Salesforce-Apps
- MS_TEAMS
- Office365-Apps
- Amazon-Apps

Match the applications GMAIL, LIVE_HOTMAIL, OUTLOOK and direct them to the Antivirus engine for email scanning.

Create a schedule for business hours (8:00 AM to 5:00 PM). Block traffic from the following URL categories during business hours:

- dating
- gambling
- games
- news_and_media

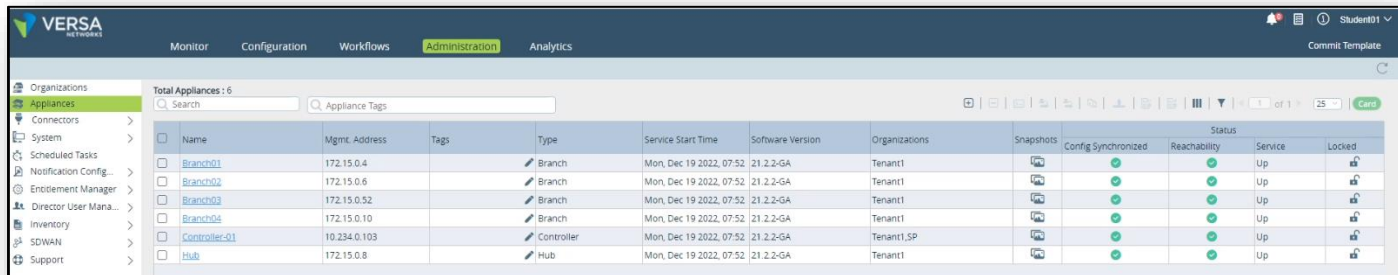
Block traffic to the following URL categories all of the time:

- abused_drugs
- adult_and_pornography
- malware_sites

After creating the rules, arrange the rules in an order that will not allow the default allow rules to permit traffic.

Open the Security Policies on your device.

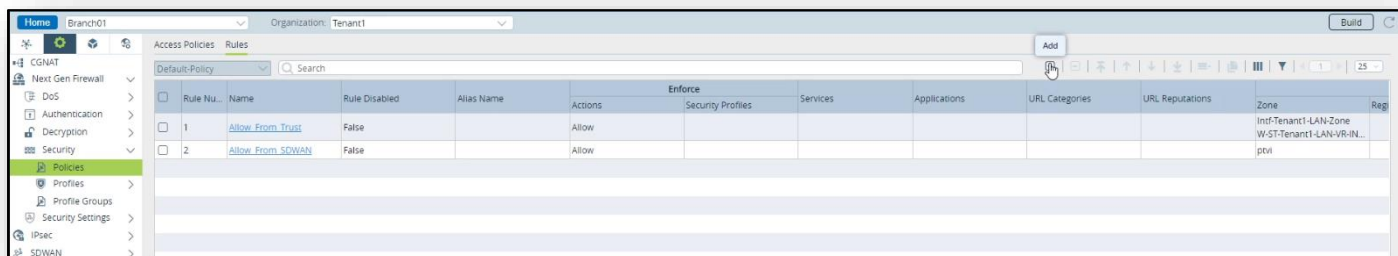
In Versa Director, navigate to Administration > Appliances and locate your appliance in the table. Click on your appliance to open the Appliance Context mode for your device. All of your configuration changes will be made directly on the device (NOT through templates).



The screenshot shows the Versa Director interface with the 'Administration' tab selected. The 'Appliances' section is active, displaying a table of 6 appliances. The table columns include Name, Mgmt. Address, Tags, Type, Service Start Time, Software Version, Organizations, Snapshots, Config Synchronized, Reachability, Service, and Locked. The appliances listed are Branch01, Branch02, Branch03, Branch04, Controller-01, and Hub.

Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Snapshots	Config Synchronized	Reachability	Service	Locked
Branch01	172.15.0.4		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch02	172.15.0.6		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch03	172.15.0.52		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Branch04	172.15.0.10		Branch	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	
Controller-01	10.234.0.103		Controller	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1.SP				Up	
Hub	172.15.0.8		Hub	Mon, Dec 19 2022, 07:52	21.2.2-GA	Tenant1				Up	

In your device Appliance Context mode, navigate to Configuration > Services > Next Gen Firewall > Security > Policies. Click the Add button to create a new rule.



The screenshot shows the Versa Director interface in the device Appliance Context mode. The 'Security' > 'Policies' section is active, displaying a table of rules. The table columns include Rule No., Name, Rule Disabled, Alias Name, Actions, Enforce, Security Profiles, Services, Applications, URL Categories, URL Reputations, Zone, and Reg. Two rules are listed: 'Allow From Trust' and 'Allow From SDWAN'.

Rule No.	Name	Rule Disabled	Alias Name	Actions	Enforce	Security Profiles	Services	Applications	URL Categories	URL Reputations	Zone	Reg
1	Allow From Trust	False		Allow							Intf-Tenant1-LAN-Zone	
2	Allow From SDWAN	False		Allow							W-ST-Tenant1-LAN-VIR-IN...	

Create a new rule called Allow-Business-Apps with the following parameters:

Source Zone: Intf-Tenatn1-LAN-Zone

Applications/URL: Amazon-Apps; Office365-Apps; Salesforce-Apps, MS_TEAMS

Enforce: Allow

Edit Rule - Allow-Business-Apps

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

☐ Source Zone

+

-

☐ Intf-Tenant1-LAN-Zone

+ New Zone

☐ Source Site Name

+

-

☐ Source Address

+

-

+ New Address Group

+ New Address

Ingress Routing Instance

--Select--

Egress Routing Instance

--Select--

☐ Source Address Negate

OK

Cancel

Edit Rule - Allow-Business-Apps

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Applications

☐ Application List

☐ Amazon-Apps

☐ Office365-Apps

☐ Salesforce-Apps

☐ MS_TEAMS

+ New Group

+ New Filter

+ New Application

URL Categories

☐ URL Category List

+ New URL Category

Reputations

☐ Reputations

OK

Cancel

Edit Rule - Allow-Business-Apps

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Actions

Log

Actions

☒ Allow

☐ Deny

☐ Reject

☐ Apply Security Profile

Synced Flow

Session Timeout (secs)

☐ Send TCP Keepalive at Session Timeout

Profiles

Profile Groups

☐ IP Filtering

☐ Anti-Virus

☐ File Filtering

☐ Vulnerability

☐ URL Filtering

☐ DNS Filtering

☐ Predefined Vulnerability Profile Override

OK

Cancel

Source Zone: Intf-Tenant1-LAN-Zone
Application List: GMAIL; LIVE_HOTMAIL; OUTLOOK

- mail

Edit Rule - Scan-Email

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

☐

Source Zone

+ -

☐Intf-Tenant1-LAN-Zone

+ New Zone

☐

Source Site Name

+ -

☐

Source Address

+ -

+ New Address Group

+ New Address

Ingress Routing Instance

Egress Routing Instance

☐ Source Address Negate

--Select--

--Select--

OK

Cancel

Edit Rule - Scan-Email

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Applications

☐ Application List

☐ GMAIL

☐ LIVE_HOTMAIL

☐ OUTLOOK

+ New Group

+ New Filter

+ New Application

URL Categories

☐ URL Category List

+ New URL Category

Reputations

☐ Reputations

OK

Cancel

Edit Rule - Scan-Email

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Actions

Log

Actions

☐ Allow

☐ Deny

☐ Reject

☒ Apply Security Profile

Synced Flow

Session Timeout (secs)

☐ Send TCP Keepalive at Session Timeout

☒ Profiles

☐ Profile Groups

☐ IP Filtering

☒ Anti-Virus

☐ File Filtering

☐ Vulnerability

☐ URL Filtering

☐ DNS Filtering

☐ Predefined Vulnerability Profile Override

OK

Cancel

Create a rule called Work-Hour-Restrictions to block specified URL categories during work ours. To do this you will create a schedule (from within the rule creation process). The rule should have the following parameters:

Source Zone: Intf-Tenant1-LAN-Zone

Headers/Schedule: Create a new schedule (+ Schedule) called Work-Hours

- Recurrence: Daily
- Start time: 8:00
- End time: 1700

URL Categories List: dating; gambling; games; news_and_media

Enforce: Deny

The screenshot shows the 'Edit Rule - Work-Hour-Restrictions' dialog box with the 'General' tab selected. The 'Name' field is filled with 'Work-Hour-Restrictions'. The 'Description' and 'Tags' fields are empty. The 'Alias Name' field is also empty. There is a checkbox for 'Disable Rule' which is currently unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Edit Rule - Work-Hour-Restrictions' dialog box with the 'Headers/Schedule' tab selected. The 'Source Zone' section has a checkbox and a list containing 'Intf-Tenant1-LAN-Zone'. The 'Source Site Name' section has a checkbox and an empty list. The 'Source Address' section has a checkbox and an empty list. At the bottom, there are dropdown menus for 'Ingress Routing Instance' and 'Egress Routing Instance', both set to '--Select--'. There is also a checkbox for 'Source Address Negate' which is unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

Edit Schedule - Work-Hours

Name*

Work-Hours

Description

Tags

Recurrence

Daily

1

Start Time*	End Time*	
00:00	00:00	+
08:00	17:00	🗑

OK

Cancel

Edit Rule - Work-Hour-Restrictions

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Applications

☐ Application List

+ New Group

+ New Filter

+ New Application

URL Categories

☐ URL Category List

☐ dating
 ☐ gambling
 ☐ games
 ☐ news_and_media

+ New URL Category

Reputations

☐ Reputations

OK

Cancel

Edit Rule - Work-Hour-Restrictions

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Actions

Log

Actions

☐ Allow
 ☒ Deny
 ☐ Reject
 ☐ Apply Security Profile

Synced Flow

--Select--

Session Timeout (secs)

☐ Send TCP Keepalive at Session Timeout

Profiles

Profile Groups

☐ IP Filtering

--Select--

☐ Anti-Virus

--Select--

☐ File Filtering

--Select--

☐ Vulnerability

--Select--

☐ URL Filtering

--Select--

☐ DNS Filtering

--Select--

☐ Predefined Vulnerability Profile Override

--Select--

OK

Cancel

Note: You can view the schedule that you created by navigating to Configuration > Objects & Connectors > Objects > Schedules, as schedules are objects that can be used by rules from any service.

Create a rule called Blocked-Web to block specified URL categories at all times with the following parameters:

Source Zone: Intf-Tenant1-LAN-Zone

URL Categories List: abused_drugs; adult_and_pornography; malware_sites

Enforce: Deny; Log End of events to Default-Logging-Profile

Edit Rule - Blocked-Web

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Name*

Blocked-Web

Description

Tags

Alias Name

☐ Disable Rule

OK

Cancel

Edit Rule - Blocked-Web

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

☐ Source Zone

Intf-Tenant1-LAN-Zone

+ New Zone

☐ Source Site Name

☐ Source Address

+ New Address Group

+ New Address

Ingress Routing Instance

--Select--

Egress Routing Instance

--Select--

☐ Source Address Negate

OK

Cancel

Edit Rule - Blocked-Web

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Applications

☐ Application List

+ New Group

+ New Filter

+ New Application

URL Categories

☐ URL Category List

☐ abused_drugs

☐ adult_and_pornography

☐ malware_sites

+ New URL Category

Reputations

☐ Reputations

OK

Cancel

Edit Rule - Blocked-Web

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Actions

Log

Actions

☐ Allow

☒ Deny

☐ Reject

☐ Apply Security Profile

Synced Flow

--Select--

Session Timeout (secs)

☐ Send TCP Keepalive at Session Timeout

☐ Profiles

☐ Profile Groups

☐ IP Filtering

--Select--

☐ Anti-Virus

--Select--

☐ File Filtering

--Select--

☐ Vulnerability

--Select--

☐ URL Filtering

--Select--

☐ DNS Filtering

--Select--

☐ Predefined Vulnerability Profile Override

--Select--

OK

Cancel

The screenshot shows the 'Edit Rule - Blocked-Web' window with the 'Log' tab selected. The 'Events' section has 'End' selected. The 'Profile' dropdown is set to 'Default-Logging-Profile'. The 'Packet Capture' section is expanded, showing 'All' selected. Below this, there are two empty lists for 'Pre-defined Applications' and 'User Defined Applications'. A 'Per session' slider is visible at the bottom of the packet capture section. The window has 'OK' and 'Cancel' buttons at the bottom right.

Next, enable security logging on the device so that session logs can be sent to Versa Analytics (by default only statistics are sent).

Navigate to Configuration > Services > Next Gen Firewall > Security Settings > Logging Control. Click on the Edit button to modify the logging control functions.

The screenshot shows the Versa Networks configuration interface. On the left, the 'Logging Control' option under 'Security Settings' is highlighted with a red box. In the main panel, the 'Logging Control' section is expanded, showing settings for Sessions, PCAP, and All Stats. A red arrow points to the 'Edit' button in the top right corner of the 'Logging Control' section. An 'Edit Logging Control' dialog box is open, showing the 'Sessions' tab with 'All' selected, 'PCAP' settings (Limit: 20000, Timeout: 600), and 'LEF Profile' set to 'Default-Logging-Profile' with 'All Stats' checked. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

Return to the Next Gen Firewall > Security > Policies hierarchy. Re-arrange the rules into this order:

1. Allow-Business-Apps
2. Scan-Email
3. Work-Hour-Restrictions
4. Blocked-Web
5. Allow_From_SDWAN
6. Allow_From_Trust

When finished your rules should resemble the following:



Rule Nu...	Name	Rule Disabled	Alias Name	Actions	Enforce	Services	Applications	URL Categories	URL Reputations	Zone	Reg
1	Allow-Business-Apps	False		Allow	Security Profiles		Predefined: MS_TEAMS			Inst-Tenant1-LAN-Zone	
2	Scan-Email	False		Allow	Scan Email Traffic		Predefined: Gmail_LIVE...			Inst-Tenant1-LAN-Zone	
3	Work-Hour-Restrictions	False		Deny				Predefined: dating_gamb...		Inst-Tenant1-LAN-Zone	
4	Blocked-Web	False		Deny				Predefined: abused_drug...		Inst-Tenant1-LAN-Zone	
5	Allow_From_Trust	False		Allow						Inst-Tenant1-LAN-Zone	
6	Allow_From_SDWAN	False		Allow						W-ST-Tenant1-LAN-VB-INT...	

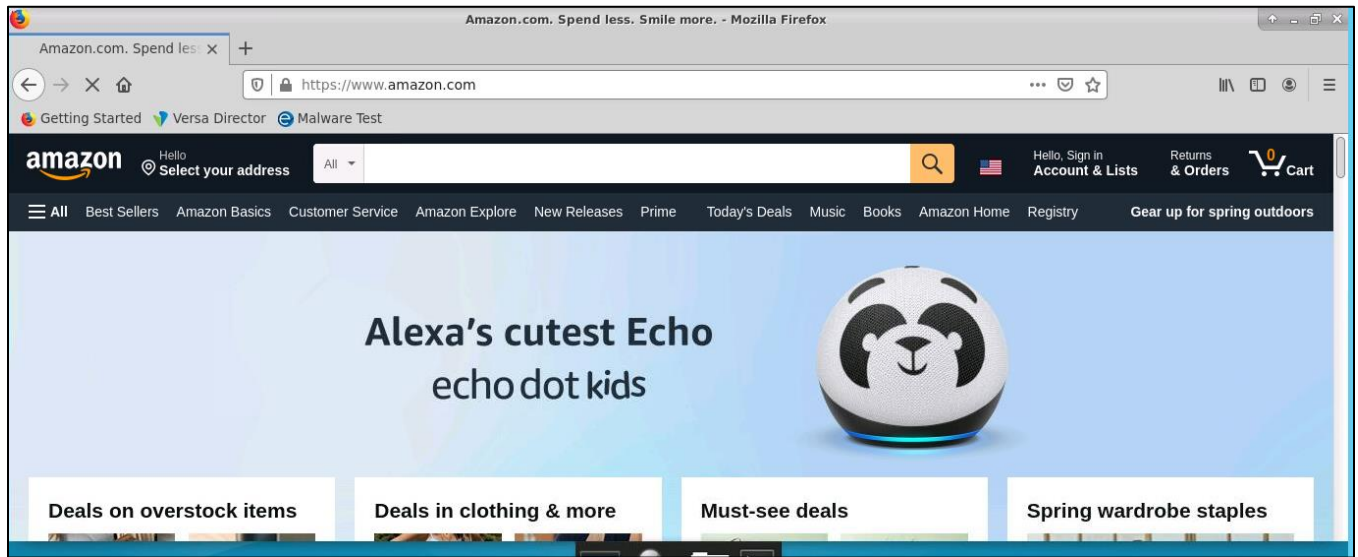
Once you have finished configuring the rules, locate the Remote Desktop icon on the remote landing station desktop. Double-click the Remote Desktop icon and open a remote desktop session to the testing host that is connected to your branch. Use the following IP addresses according to your branch assignment:

Branch01: 10.27.10.10	Branch07: 10.27.10.16	Branch13: 10.27.10.22
Branch02: 10.27.10.11	Branch08: 10.27.10.17	Branch14: 10.27.10.23
Branch03: 10.27.10.12	Branch09: 10.27.10.18	Branch15: 10.27.10.24
Branch04: 10.27.10.13	Branch10: 10.27.10.19	Branch16: 10.27.10.25
Branch05: 10.27.10.14	Branch11: 10.27.10.20	Branch17: 10.27.10.26
Branch06: 10.27.10.15	Branch12: 10.27.10.21	Branch18: 10.27.10.27

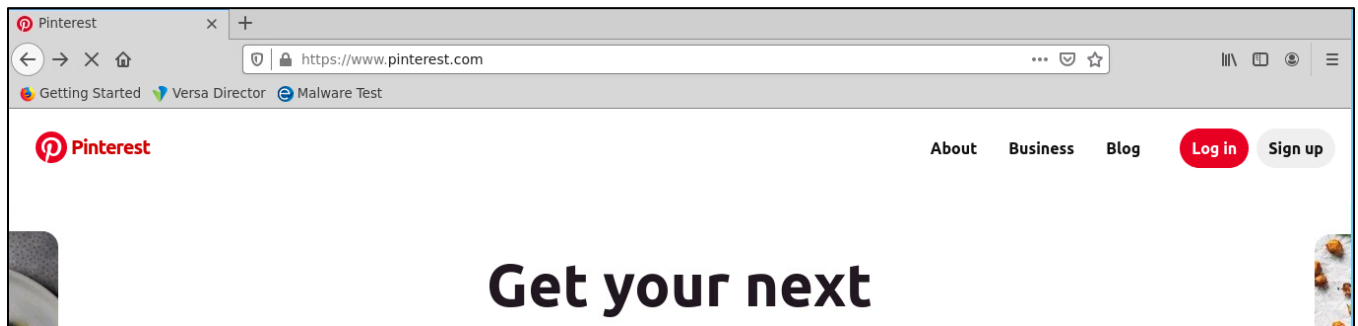
When prompted to connect (the certificate warning), click Yes.

In the remote desktop connection window, enter the session **Xorg**, username **student** and password **versa123**.

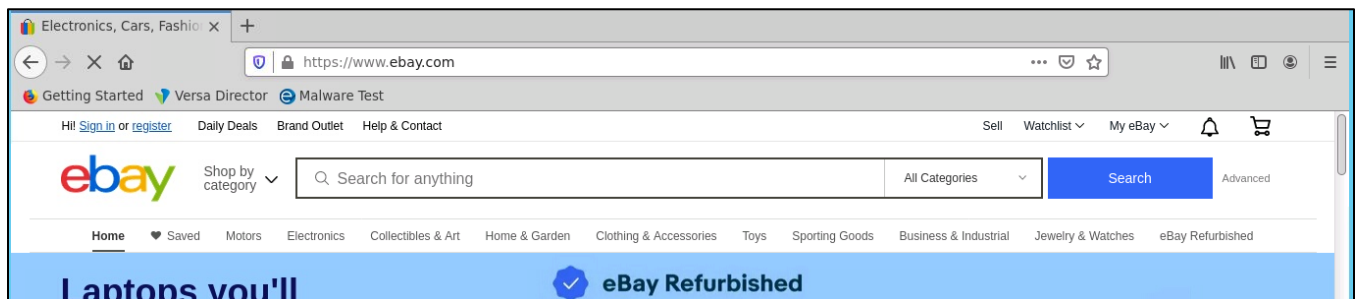
On the testing host, open the Firefox Web Browser. In the Firefox web browser, enter the URL **www.amazon.com** in the address bar.



After the page loads, enter the address www.pinterest.com in the address bar.



After the page loads, enter the address www.ebay.com in the address bar.



Return to your Versa Director session. In Versa Director, navigate to the Monitor > Services > NGFW > Policies dashboard of your device. The Default-Policy should automatically be displayed.

Rule Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count	Hit Rate	Inactive Session Count
Allow-Business-Apps	28	23	2743	24	8186	0	3
Scan-Email	0	0	0	0	0	0	0
Work-Hour-Restrictions	0	0	0	0	0	0	0
Blocked-Web	0	0	0	0	0	0	0
Allow-From-Trust	1999	46181	5641022	137619	172979914	0	1898
Allow-From-SDWAN	1	3	252	3	252	0	1

The hit counter of the Allow-Business-Apps should be a non-zero value.

Return to the remote desktop session of the testing host. In the testing host Firefox browser address bar, enter the address www.Hotmail.com and wait for the page to load. Once the page has loaded, navigate to www.gmail.com and wait for the page to load.

Once you have visited both the Hotmail and Gmail pages, return to your Versa Director dashboard. In the Versa Director dashboard (in the NGFW Policies window), click the Security Packages tab, then the Policies tab to refresh the policy statistics. You should see hit counts increased on the Scan-Email rule.

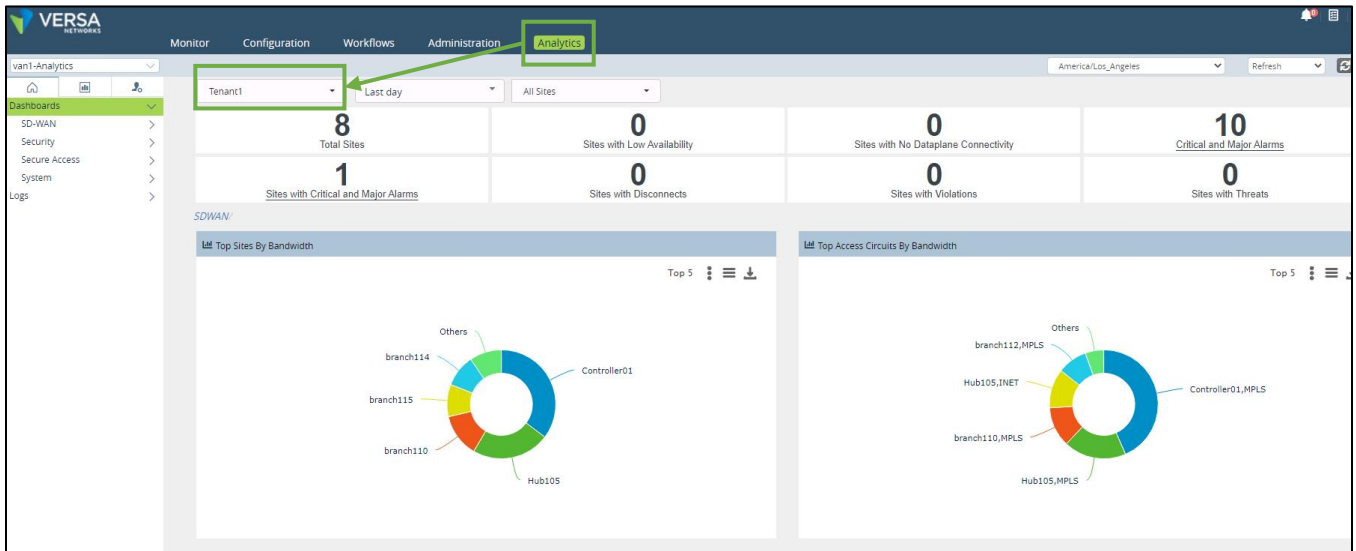
Rule Name	Hit Count	Forward Pkt Count	Forward Byte Count	Reverse Pkt Count	Reverse Byte Count	Hit Rate	Inactive Session Count
Allow-Business-Apps	38	707	329294	598	212360	0	26
Scan-Email	3	0	0	0	0	0	0
Work-Hour-Restrictions	0	0	0	0	0	0	0
Blocked-Web	0	0	0	0	0	0	0
Allow-From-Trust	2057	52640	6374284	156994	197483851	0	1990
Allow-From-SDWAN	1	3	252	3	252	0	1

Note: The statistics on the page are not real-time. They are queried when the page is opened. To refresh the counters and statistics, navigate to any other tab or window, then return. When the table reloads, the statistics will be refreshed.

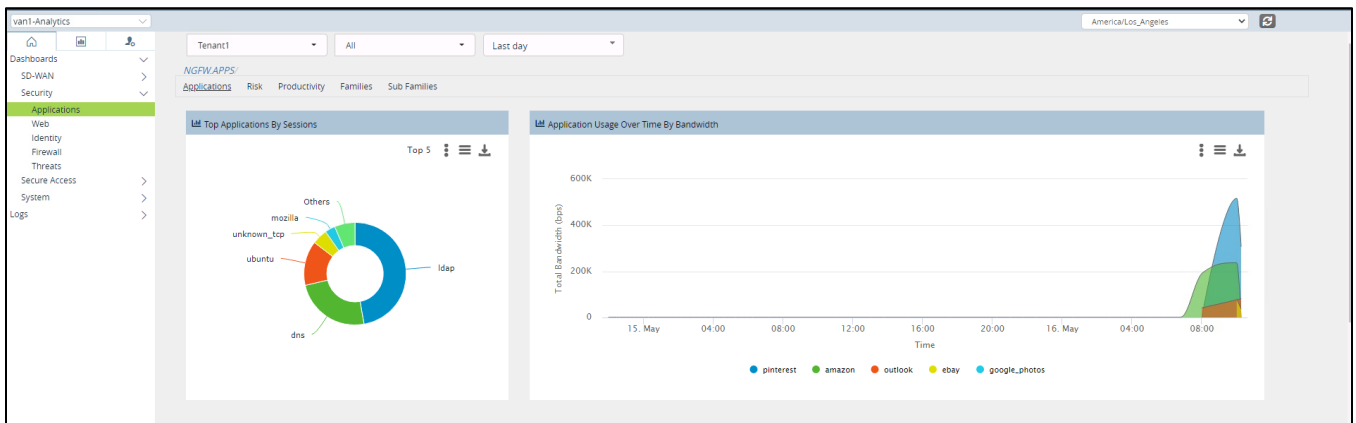
Next you will identify the logged sessions in Versa Analytics.

Click the Home button on the top-left of the Versa Director dashboard to return to the main Versa Director workspace.

From the main Versa Director workspace, open the Analytics workspace. In the Analytics workspace, ensure that the Tenant1 organization is selected (it may default to the SP organization).



Expand the Security > Applications dashboard to view the application activity. You should see some entries for the web sites that you visited.



In the left side menu, expand the Logs section and select the Firewall logs. You should see log entries in the logs list that match the applications you have accessed.

Refresh the entries in the window

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	URL Category	Protocol	Action	Type	Rule	Egress Interface	Ingress Interface
May 16th 2022, 10:20:57 AM PDT	branch110	172.16.110.110	142.250.191.42	42584	443	google_api	computer_and_internet_info	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:20:23 AM PDT	branch110	172.16.110.110	54.189.35.180	41718	443	mozilla	shareware_and_freeware	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:18:45 AM PDT	branch110	172.16.110.110	142.250.191.46	35772	443	google_analytics	computer_and_internet_info	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:18:45 AM PDT	branch110	172.16.110.110	142.250.191.36	52834	443	google	search_engines	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:17:56 AM PDT	branch110	172.16.110.110	64.4.54.254	37312	443	microsoft	business_and_economy	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:17:56 AM PDT	branch110	172.16.110.110	13.107.227.69	33260	443	microsoft	computer_and_internet_info	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:17:56 AM PDT	branch110	172.16.110.110	52.96.64.194	57790	443	outlook	web_based_email	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:17:38 AM PDT	branch110	172.16.110.110	142.250.191.42	42584	443	google_api	computer_and_internet_info	tcp	allow	start	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:17:07 AM PDT	branch110	172.16.110.110	34.122.121.32	46766	80	ubuntu	business_and_economy	tcp	allow	end	Allow_From_Trust	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:16:46 AM PDT	branch110	172.16.110.110	34.122.121.32	46766	80	ubuntu	business_and_economy	tcp	allow	start	Allow_From_Trust	dtvi-0/36	vni-0/2.0

Locate a log entry that matches the application “microsoft” and click the magnifying glass next to the entry. This will open the log entry. To view the log entry in a more readable format, click the PDF button in the top right to download the listed entries to a PDF file. The file will be downloaded to the remote desktop computer. You can open the file by clicking the file name in the Download window (at the bottom of the browser window).

Note: It may take a few minutes before the log entries are saved and parsed on the Versa Analytics platform. Use the refresh icon in the top right corner to refresh the data. If log entries do not appear within a minute or two, ensure that the Log action is specified in ALL of your security rules.

Showing 1 to 2 of 2 entries

Previous 1 Next

Versa Analytics-Rel...pdf

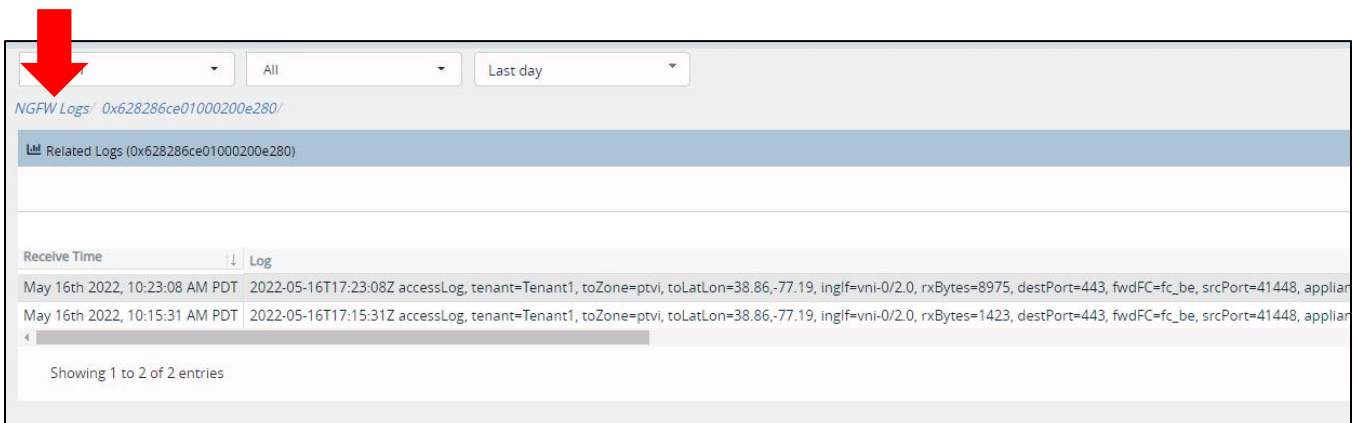
Show all

The Related Logs lists log entries that are related to each other. In this instance, both entries are accessLog entries, and they are sourced and destined to the same locations and have other information that is related or identical.

Related Logs (0x628286ce01000200e280)

Receive Time	Log
May 16th 2022, 10:23:08 AM PDT	2022-05-16T17:23:08Z accessLog, tenant=Tenant1, toZone=ptvi, toLatLon=38.86,-77.19, inglf=vni-0/2.0, rxBytes=8975, destPort=443, fwdFC=fc_be, srcPort=41448, applianceName=branch110, rxPkts=41, revFC=fc_be, action=allow, destAddr=20.75.32.255, flowDuration=418817, urlCat=computer_and_internet_info, rcvTimeSec=8, fromUser=Unknown, toCountry=United States, protocolId=6, flowKey=0x628286ce01000200e280, txPkts=53, eventType=end, egrlf=dtvi-0/36, at=Mon May 23 11:00:00 PDT 2022, txBytes=6764, appld=microsoft, sessLenBkt=4, srcAddr=172.16.110.110, deviceKey=Unknown, toGeoHash=dqcj56, rule=Allow_From_Trust, fromZone=Intf-Tenant1-LAN-Zone
May 16th 2022, 10:15:31 AM PDT	2022-05-16T17:15:31Z accessLog, tenant=Tenant1, toZone=ptvi, toLatLon=38.86,-77.19, inglf=vni-0/2.0, rxBytes=1423, destPort=443, fwdFC=fc_be, srcPort=41448, applianceName=branch110, rxPkts=2, revFC=fc_be, action=allow, destAddr=20.75.32.255, flowDuration=0, urlCat=computer_and_internet_info, rcvTimeSec=31, fromUser=Unknown, toCountry=United States, protocolId=6, flowKey=0x628286ce01000200e280, txPkts=3, eventType=start, egrlf=dtvi-0/36, at=Mon May 23 11:00:00 PDT 2022, txBytes=657, appld=microsoft, sessLenBkt=0, srcAddr=172.16.110.110, deviceKey=Unknown, toGeoHash=dqcj56, rule=Allow_From_Trust, fromZone=Intf-Tenant1-LAN-Zone

Close the browser window that displays the PDF file. In the Versa Analytics dashboard, click the NGFW Logs link to return to the previous window.



NGFW Logs/ 0x628286ce01000200e280/

Related Logs (0x628286ce01000200e280)

Receive Time	Log
May 16th 2022, 10:23:08 AM PDT	2022-05-16T17:23:08Z accessLog, tenant=Tenant1, toZone=ptvi, toLatLon=38.86,-77.19, inglf=vni-0/2.0, rxBytes=8975, destPort=443, fwdFC=fc_be, srcPort=41448, applianceName=branch110, rxPkts=41, revFC=fc_be, action=allow, destAddr=20.75.32.255, flowDuration=418817, urlCat=computer_and_internet_info, rcvTimeSec=8, fromUser=Unknown, toCountry=United States, protocolId=6, flowKey=0x628286ce01000200e280, txPkts=53, eventType=end, egrlf=dtvi-0/36, at=Mon May 23 11:00:00 PDT 2022, txBytes=6764, appld=microsoft, sessLenBkt=4, srcAddr=172.16.110.110, deviceKey=Unknown, toGeoHash=dqcj56, rule=Allow_From_Trust, fromZone=Intf-Tenant1-LAN-Zone
May 16th 2022, 10:15:31 AM PDT	2022-05-16T17:15:31Z accessLog, tenant=Tenant1, toZone=ptvi, toLatLon=38.86,-77.19, inglf=vni-0/2.0, rxBytes=1423, destPort=443, fwdFC=fc_be, srcPort=41448, applianceName=branch110, rxPkts=2, revFC=fc_be, action=allow, destAddr=20.75.32.255, flowDuration=0, urlCat=computer_and_internet_info, rcvTimeSec=31, fromUser=Unknown, toCountry=United States, protocolId=6, flowKey=0x628286ce01000200e280, txPkts=3, eventType=start, egrlf=dtvi-0/36, at=Mon May 23 11:00:00 PDT 2022, txBytes=657, appld=microsoft, sessLenBkt=0, srcAddr=172.16.110.110, deviceKey=Unknown, toGeoHash=dqcj56, rule=Allow_From_Trust, fromZone=Intf-Tenant1-LAN-Zone

Showing 1 to 2 of 2 entries

Locate and click on the Rule title in the table to sort the entries by the rule that takes action on the session. Sort the entries so that the Allow-Business-Apps rules are first.

NGFW Logs /
Logs Charts

Firewall Logs

☐ Show Domain Names

Search:

Copy CSV PDF

Show 10 entries

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	URL Category	Protocol	Action	Type	Rule	Egress Interface	Ingress Interface
May 16th 2022, 8:00:35 AM PDT	branch110	172.16.110.110	52.94.232.195	49768	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 8:04:57 AM PDT	branch110	172.16.110.110	52.94.225.56	37544	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:08:07 AM PDT	branch110	172.16.110.110	3.227.221.25	52794	443	amazon	business_and_economy	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:07:02 AM PDT	branch110	172.16.110.110	13.227.78.100	55614	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:07:02 AM PDT	branch110	172.16.110.110	13.227.78.100	55610	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:07:02 AM PDT	branch110	172.16.110.110	13.227.78.100	55616	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:07:02 AM PDT	branch110	172.16.110.110	13.227.78.100	55620	443	amazon	cdns	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:07:17 AM PDT	branch110	172.16.110.110	52.46.129.152	49626	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:08:23 AM PDT	branch110	172.16.110.110	52.46.155.182	39192	443	amazon	shopping	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0
May 16th 2022, 10:08:59 AM PDT	branch110	172.16.110.110	52.46.141.85	40496	443	amazon	uncategorized	tcp	allow	end	Allow-Business-Apps	dtvi-0/36	vni-0/2.0

Showing 1 to 10 of 911 entries

Previous 1 2 3 4 5 ... 92 Next

View the details of one of the entries, then download and view a PDF version of the log entry. Note the session properties and the rule that took action on the session.

SAMPLE LOG ENTRY

Related Logs (0x6282670a01000200e0a3)

Receive Time	Log
May 16th 2022, 8:00:35 AM PDT	2022-05-16T15:00:35Z accessLog, tenant=Tenant1, toZone=ptvi, toLatLon=39.56,-75.6, ingIf=vni-0/2.0, rxBytes=6627, destPort=443, fwdFC=fc_be, srcPort=49768, applianceName=branch110, rxPkts=12, revFC=fc_be, action=allow, destAddr=52.94.232.195, flowDuration=5954, urlCat=shopping, rcvTimeSec=35, fromUser=Unknown, toCountry=United States, protocolId=6, flowKey=0x6282670a01000200e0a3, txPkts=9, eventType=end, egrIf=dtvi-0/36, at=Mon May 23 09:00:00 PDT 2022, txBytes=1054, appId=amazon, sessLenBkt=1, srcAddr=172.16.110.110, deviceKey=Unknown, toGeoHash=dr41pd, rule=Allow-Business-Apps, fromZone=Intf-Tenant1-LAN-Zone

SAMPLE LOG ENTRY



STOP! Notify your instructor that you have completed this lab.