Lab Security Packages and Updates

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.

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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:

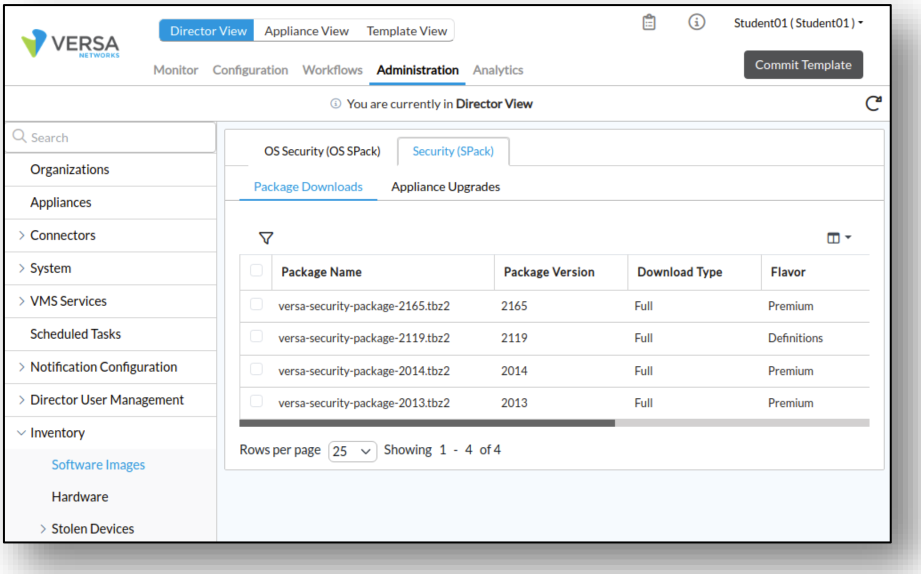
In the following lab exercises, you will:

- Identify where Security Packages are stored in Versa Director
- Learn how to download a security package to Versa Director
- Update your branch device security package

Refer to the Lab Access Guide for instructions on how to connect to the remote lab environment. Once you have connected to the remote lab environment, log into Versa Director on your remote desktop workstation.

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

Security packages are stored in the *Administration > Inventory* dashboard of Versa Director.



You are currently in Director View

☐	Package Name	Package Version	Download Type	Flavor
☐	versa-security-package-2165.tbz2	2165	Full	Premium
☐	versa-security-package-2119.tbz2	2119	Full	Definitions
☐	versa-security-package-2014.tbz2	2014	Full	Premium
☐	versa-security-package-2013.tbz2	2013	Full	Premium

Rows per page 25 Showing 1 - 4 of 4

As a tenant in a global system, you do not have access to download security packages to Versa Director, as that can affect the overall system storage space. The Administrator account has access to download security packages.

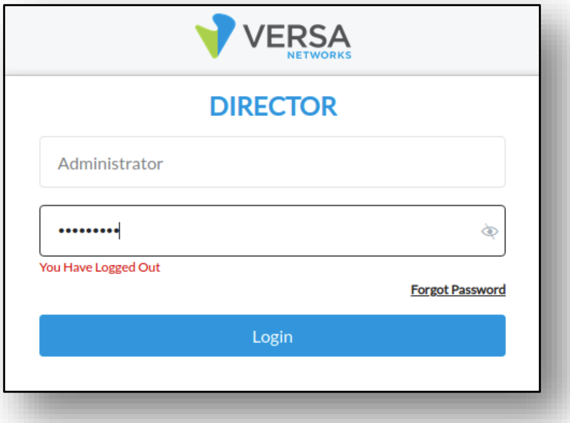
To demonstrate where and how to download security packages, you will TEMPORARILY log into Versa Director as the Administrator, examine the Software Images dialog, and view where packages are uploaded to Versa Director.

After viewing the Administrator access to the Software Images, you will log out, then log back in as your Studentxx tenant.

DO NOT MAKE ANY CHANGES TO THE SYSTEM AS THE ADMINISTRATOR!

In the top right corner, click on your user ID and log out of Versa Director.

Log into Versa Director as *Administrator*, with password *Versa@123.*

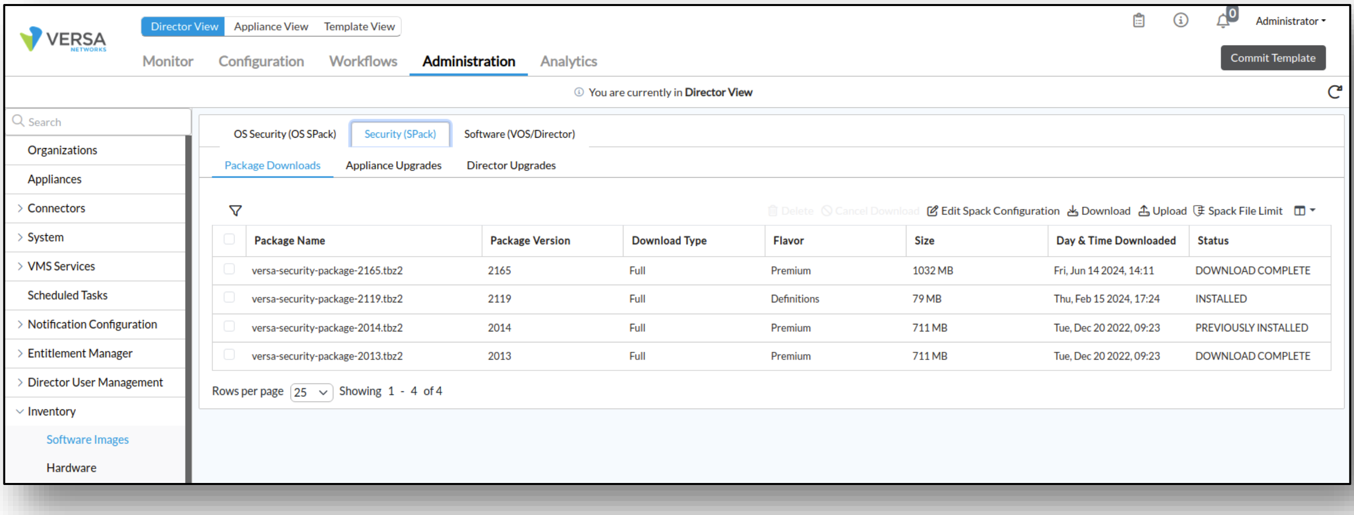


Administrator

•••••••••

You Have Logged Out

After you log in as Administrator, navigate to *Administration > Inventory > Software Images*.



You are currently in Director View

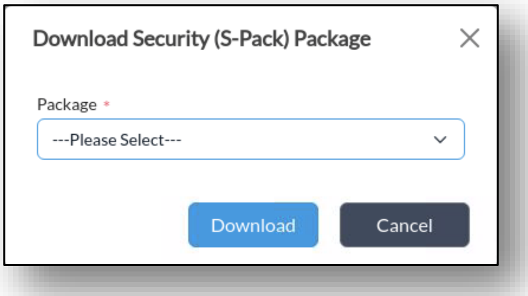
Package Name	Package Version	Download Type	Flavor	Size	Day & Time Downloaded	Status
versa-security-package-2165.tbz2	2165	Full	Premium	1032 MB	Fri, Jun 14 2024, 14:11	DOWNLOAD COMPLETE
versa-security-package-2119.tbz2	2119	Full	Definitions	79 MB	Thu, Feb 15 2024, 17:24	INSTALLED
versa-security-package-2014.tbz2	2014	Full	Premium	711 MB	Tue, Dec 20 2022, 09:23	PREVIOUSLY INSTALLED
versa-security-package-2013.tbz2	2013	Full	Premium	711 MB	Tue, Dec 20 2022, 09:23	DOWNLOAD COMPLETE

Rows per page 25 Showing 1 - 4 of 4

In the Software Images dashboard, select the Security (SPack) tab. Note the options you have as administrator in the top right of the table (e.g. Download, Upload, Spack File Limit)

In the Software Images dashboard, select the Security (SPack) tab. Note the different options you have as administrator in the top right of the table.

Click the Download button to view the download dialog.



Download Security (S-Pack) Package

Package *

---Please Select---

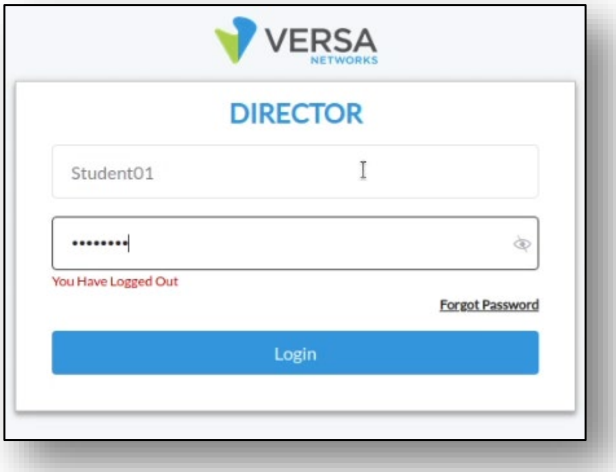
The security package list is automatically populated and when you click the Package drop-down, the latest security packages will be listed.

Click the *Cancel* button to exit the dialog.

Examine the list of security packages in the system. This list of packages will be available to the sub-tenants.

Click the Administrator user in the top right of the window, and log out as Administrator.

Log back into Versa Director with your assigned student username (Student01, Student02, etc.)



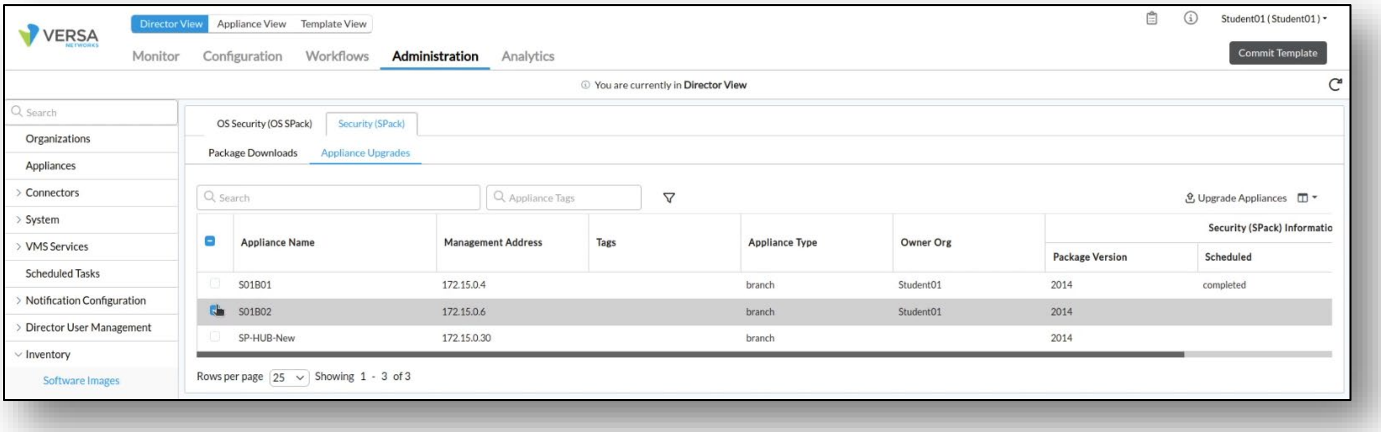
DIRECTOR

Student01

••••••••

You Have Logged Out

Navigate to *Administration > Inventory > Software Images > Security (SPack) > Appliance Upgrades*. Check the box next to your *B02* device and identify the Package Version that is currently installed on the device from the Package Version column in the table.



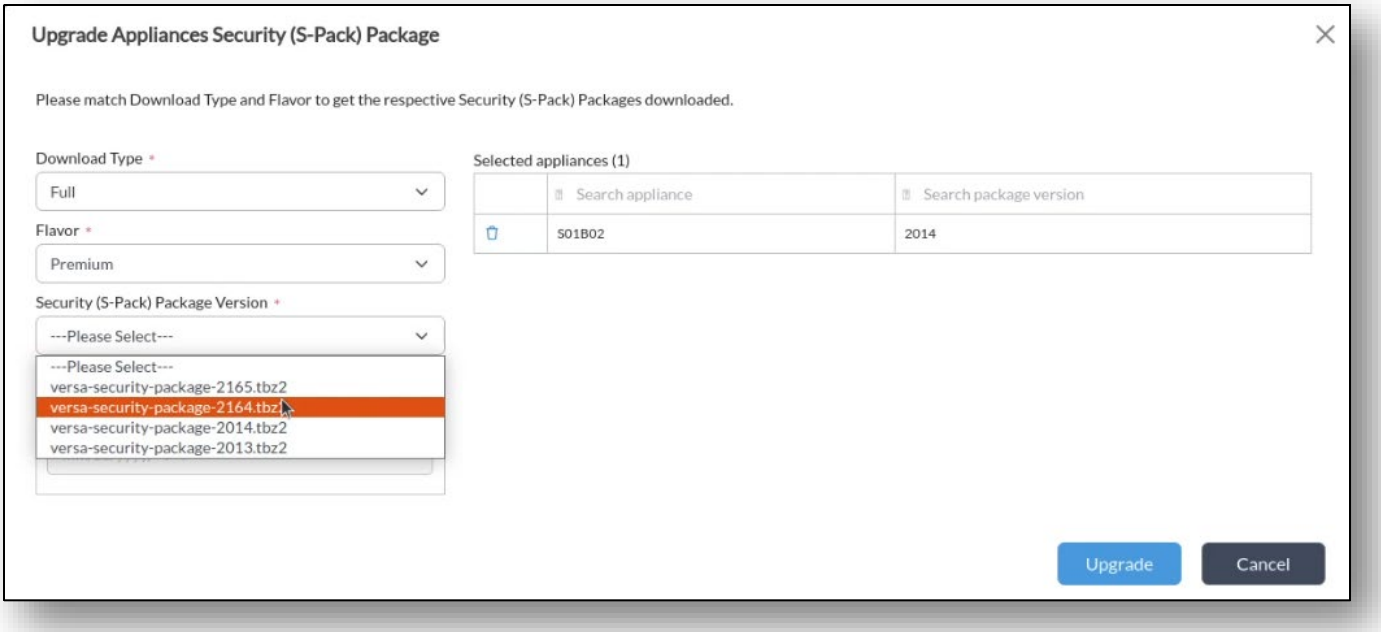
You are currently in Director View

	Appliance Name	Management Address	Tags	Appliance Type	Owner Org	Security (SPack) Informatio	
						Package Version	Scheduled
☐	S01B01	172.15.0.4		branch	Student01	2014	completed
☑	S01B02	172.15.0.6		branch	Student01	2014	
☐	SP-HUB-New	172.15.0.30		branch		2014	

Rows per page 25 Showing 1 - 3 of 3

Click the *Upgrade Appliances* button to open the upgrade dialog.

In the Upgrade Appliances Security (S-Pack) Package dialog, select one of the newer packages from the list. The download type should be Full, and the Flavor Premium.



Upgrade Appliances Security (S-Pack) Package

Please match Download Type and Flavor to get the respective Security (S-Pack) Packages downloaded.

Download Type *: Full

Flavor *: Premium

Security (S-Pack) Package Version *: ---Please Select---

- ---Please Select---
- versa-security-package-2165.tbz2
- versa-security-package-2164.tbz2
- versa-security-package-2014.tbz2
- versa-security-package-2013.tbz2

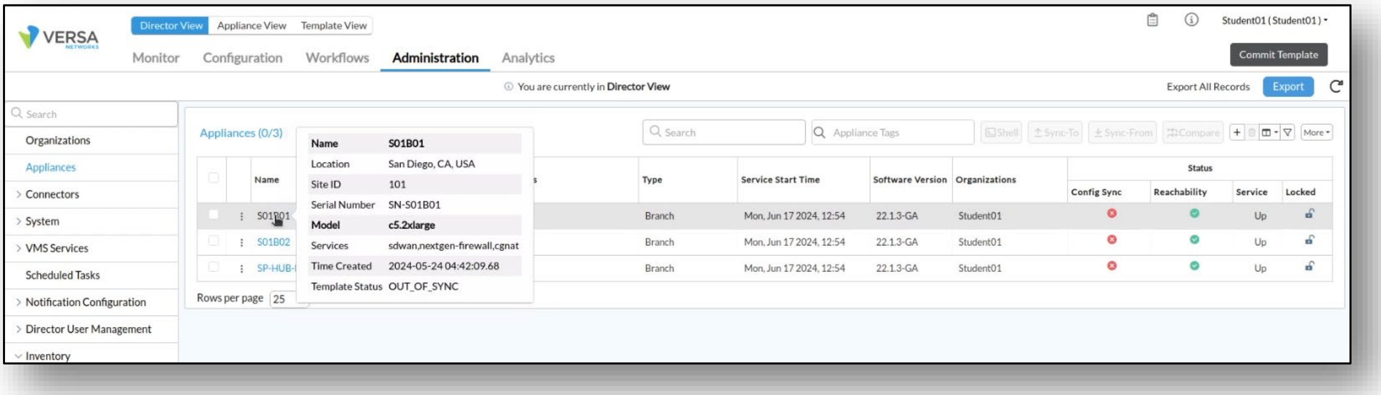
Selected appliances (1)

	Search appliance	Search package version
🗑	S01B02	2014

Click the Upgrade button to install the security package. This will take a couple of minutes to upload and apply the package to the branch device.

In the next part of the lab you will configure the B01 device to automatically download and install security packages when they are released.

After the update is complete, navigate to *Director View > Administration > Appliances* and locate your B01 appliance in the Appliances table. Click on the B01 appliance to open it in Appliance View.



You are currently in **Director View**

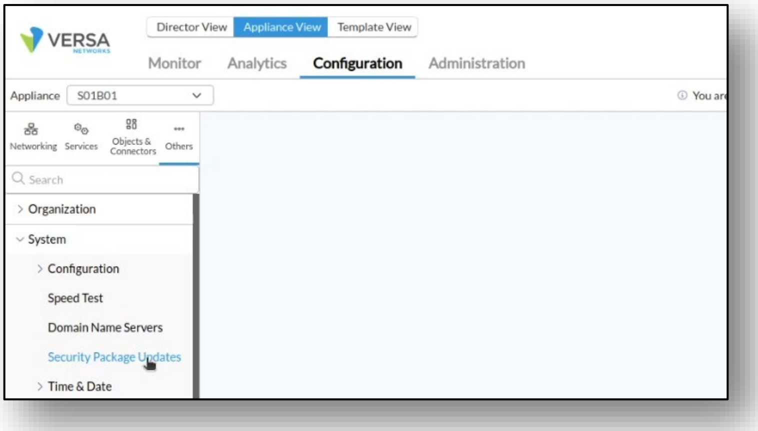
Appliances (0/3)

Name	**S01B01**
Location	San Diego, CA, USA
Site ID	101
Serial Number	SN-S01B01
Model	**c5.2xlarge**
Services	sdwan,nextgen-firewall,cgnat
Time Created	2024-05-24 04:42:09.68
Template Status	OUT_OF_SYNC

Name	Type	Service Start Time	Software Version	Organizations	Status			
					Config Sync	Reachability	Service	Locked
S01B01	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✗	✓	Up	🔓
S01B02	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✗	✓	Up	🔓
SP-HUB-(	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✗	✓	Up	🔓

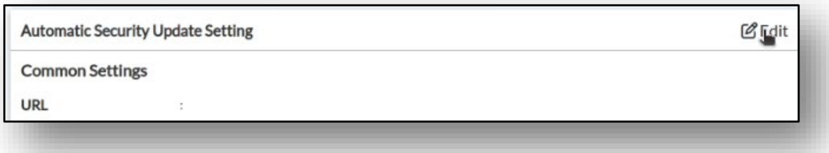
Rows per page 25

In the *Appliance View* of your B01 device, navigate to *Configuration > Others > System > Security Package Updates*.



Appliance S01B01

In the Security Package Updates dialog, click the Edit button to modify the settings.



Automatic Security Update Setting

Common Settings

URL :

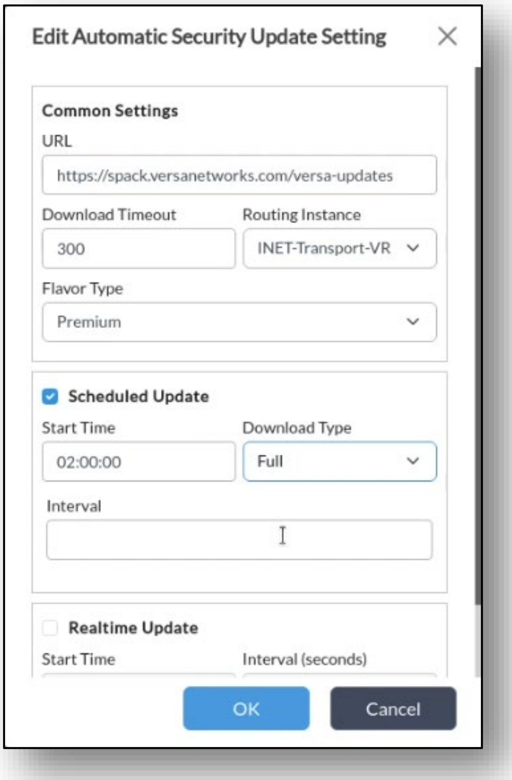
NOTE: Automatic updates may already be configured on the branch device. If this is true, follow the steps to see where this function is enabled.

If you are enabling automatic security updates for the first time, enter the following information in the dialog:

- URL: https://spack.versanetworks.com/versa-updates
- Download timeout: 300
- Routing Instance: INET-Transport-VR
- Flavor Type: Premium
- Schedule Update:
- Start Time: 02:00:00
- Download time: Full

When finished, your device should look similar to the example image.

Click OK to finish the configuration change.



Edit Automatic Security Update Setting

Common Settings

URL: https://spack.versanetworks.com/versa-updates

Download Timeout: 300

Routing Instance: INET-Transport-VR

Flavor Type: Premium

☑ Scheduled Update

Start Time: 02:00:00

Download Type: Full

Interval:

□ Realtime Update

Start Time

Interval (seconds)

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

SSL Inspection and Decryption

Steps:
Navigate to object > others and create a key
Create an appliance cert
Create a decryption profile
Create 2 decryption rules – one for decrypt, one for n-decrypt
Decrypt for shopping, news, sports
No-decrypt for health, banking

Go to VLC RDP
Open browser
Browse to Banking
View cert information
Go to health
View cert information
Go to ESPN
View cert information
Open connection to Versa Director on Linux testing client
Go to objects > others > and download the cert
Install the cert in the browser on the Linux client
View the ESPN site again
Examine the certificate information to verify the cert provider
Go to to ***https://expired.badssl.com***. And see the action taken with expired SSL certs

SSL Inspection and Decryption

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:

- Create an SSL encryption key
- Create an appliance certificate that uses the encryption key
- Create a decryption profile that:
    - has rules that inspect certificates without decrypting the payload
    - has rules that decrypt and inspect traffic from specific URL categories
- Install an appliance certificate in the web browser
- Verify SSL inspection and SSL decryption

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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:

In the following lab exercises, you will:

- Create an SSL key on your appliance
- Create an SSL certificate on your appliance
- Configure an SSL Decryption Profile
- Configure rules for the SSL decryption profile that:
    - Perform SSL inspection on banking and financial web sites
    - Block sessions to sites with bad SSL certificates
    - Decrypt and inspect traffic to sports, news_and_media, and social_networking URL categories.

> **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.

Step 1: Reset the lab to a base configuration

In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the workflow to your branch device. In the Basic tab, ensure that the device is assigned to the DG-NGFW device group. If you need to change the device group assigned to your branch device, be sure to click Redeploy to apply the changes to the device in Versa Director.

Click the *Commit Template* link in the top-right corner of Versa Director, select Tenant1 from the organization drop-down menu, select the *Template-NGFW* from the *Select Template* menu, check the box next to your branch device, and click *OK* to overwrite the configuration on the device with the Base-Template configuration.

Step 2: Open the Device Configuration

In the next steps you will create an SSL encryption key for your branch device. You will then create a self-signed SSL certificate for the device. **The certificates and keys must be created on the appliance (in Device Context mode) and not in the device templates.**

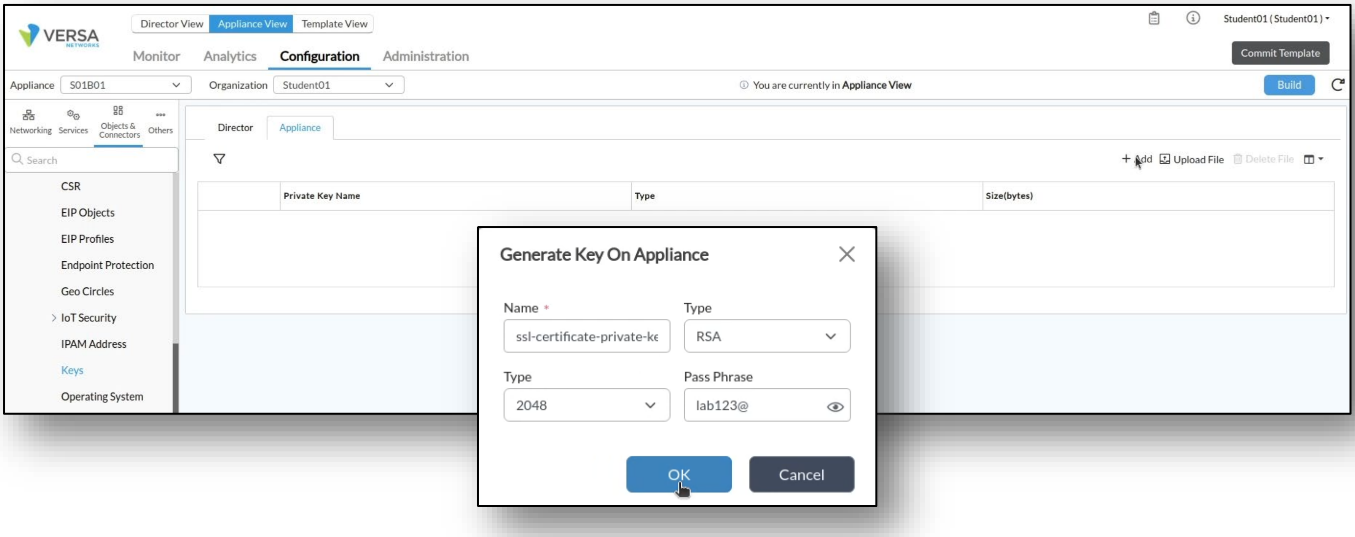
Step 3: Create an SSL encryption key

Open your branch appliance configuration. to open the appliance configuration in device context mode, navigate to the *Administration > Appliances* dashboard and locate your branch in the appliance list. Click on your appliance name to open device context mode for that device.

From the appliance context mode, click on the Configuration tab to modify the configuration.

The encryption key is a custom object that is configured under the *Objects & Connectors > Custom Objects > Keys* hierarchy. Create an encryption key for the APPLIANCE with the following parameters:

Key Name: ssl-certificate-private-key
Type: RSA
Type: 2048
Pass Phrase: lab123@



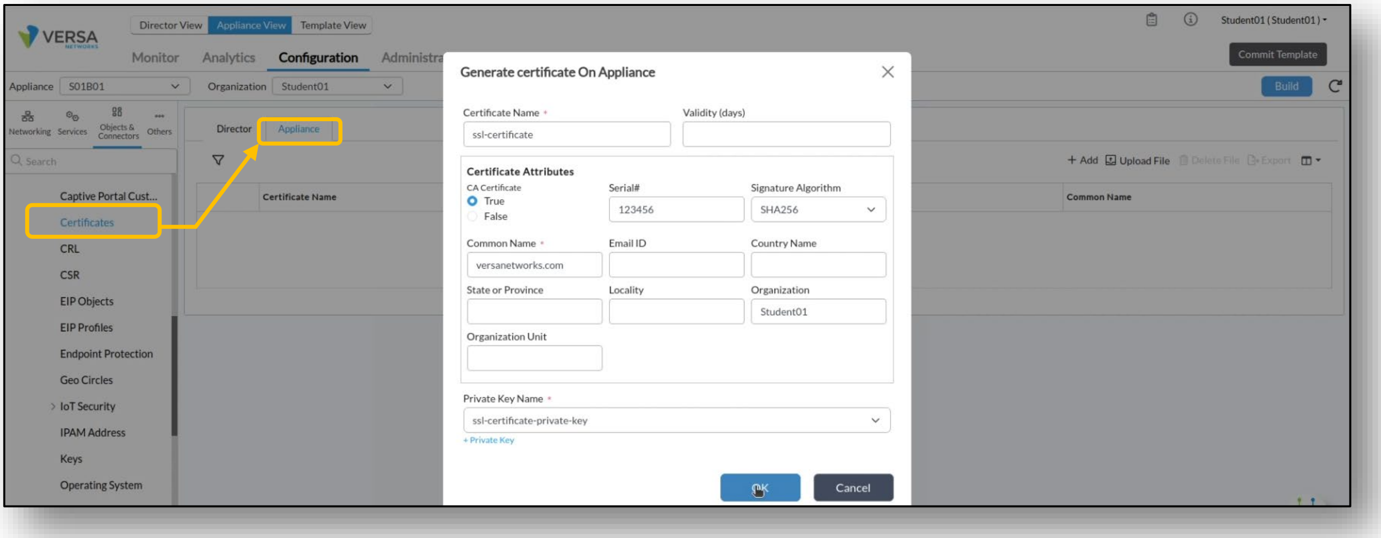
Generate Key On Appliance

Name *: ssl-certificate-private-ke
Type: RSA
Type: 2048
Pass Phrase: lab123@

Step 4: Create an appliance certificate

Next you will create an appliance certificate that uses the appliance key. Appliance certificates are objects that are created under the *Objects & Connectors > Objects > Custom Objects > Certificates* hierarchy.

Create an APPLIANCE certificate with the following parameters (ensure your student ID is in the Organization setting, and ensure that the CA Certificate is set to True):



Generate certificate On Appliance

Certificate Name *: ssl-certificate
Validity (days):

Certificate Attributes

CA Certificate: ● True ○ False
Serial#: 123456
Signature Algorithm: SHA256
Common Name *: versanetworks.com
Email ID:
Country Name:
State or Province:
Locality:
Organization: Student01
Organization Unit:

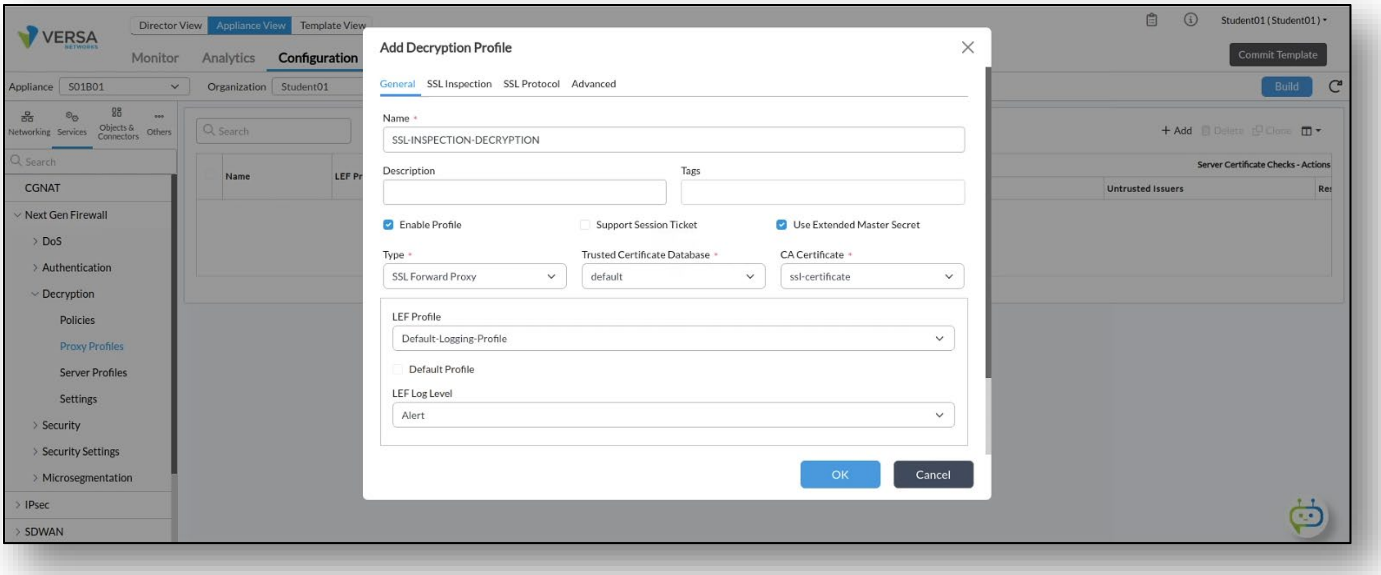
Private Key Name *: ssl-certificate-private-key

Step 5: Configure Proxy Profiles

In the next steps you will configure a proxy profile (decryption profile) and a decryption policy policy to perform SSL inspection or decryption on specified web traffic.

Decryption profiles are configured under the Next Gen Firewall services. You will configure the Next Gen Firewall parameters in the appliance context mode of your device.

From your appliance context mode, navigate to *Services > Next Gen Firewall > Decryption > Proxy Profiles* hierarchy. Create a new decryption profile with the following parameters:



Add Decryption Profile

General | SSL Inspection | SSL Protocol | Advanced

Name *: SSL-INSPECTION-DECRYPTION

Description:

Tags:

☑ Enable Profile □ Support Session Ticket ☑ Use Extended Master Secret

Type *: SSL Forward Proxy

Trusted Certificate Database *: default

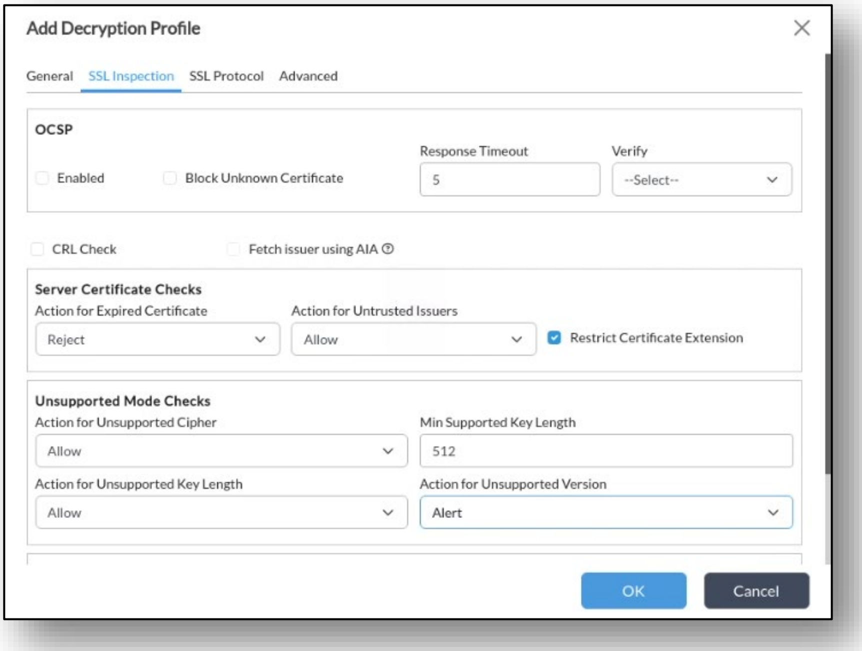
CA Certificate *: ssl-certificate

LEF Profile: Default-Logging-Profile

□ Default Profile

LEF Log Level: Alert

OK Cancel



Add Decryption Profile

General | SSL Inspection | SSL Protocol | Advanced

OCSP

□ Enabled □ Block Unknown Certificate

Response Timeout: 5

Verify: --Select--

□ CRL Check □ Fetch issuer using AIA ⓘ

Server Certificate Checks

Action for Expired Certificate: Reject

Action for Untrusted Issuers: Allow

☑ Restrict Certificate Extension

Unsupported Mode Checks

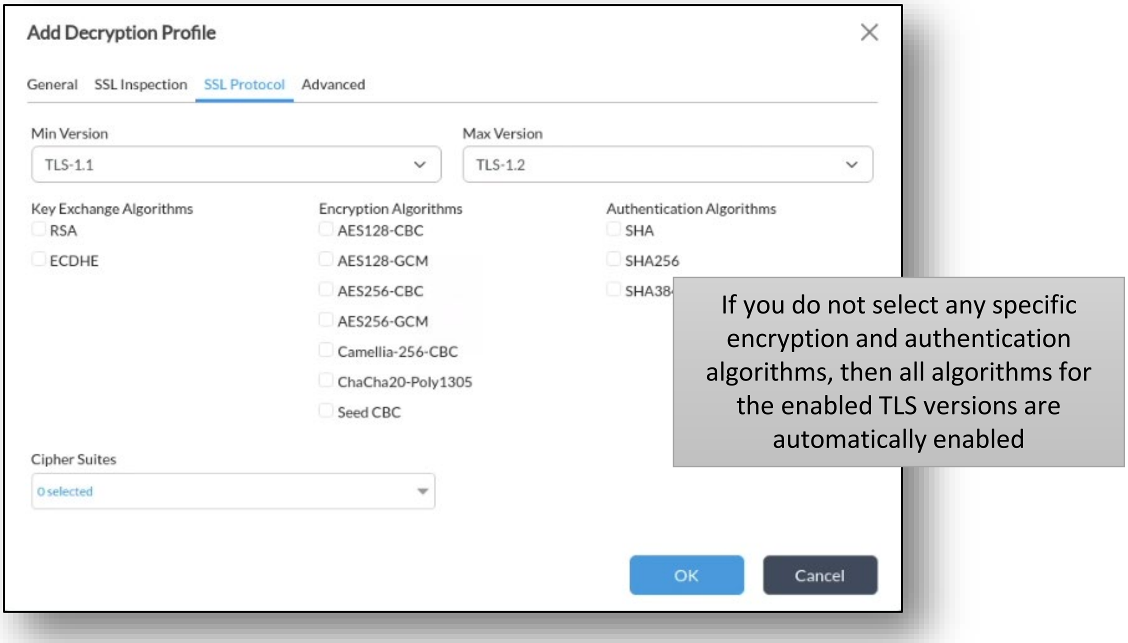
Action for Unsupported Cipher: Allow

Min Supported Key Length: 512

Action for Unsupported Key Length: Allow

Action for Unsupported Version: Alert

OK Cancel



Add Decryption Profile

General | SSL Inspection | SSL Protocol | Advanced

Min Version: TLS-1.1

Max Version: TLS-1.2

Key Exchange Algorithms
- □ RSA
- □ ECDHE

Encryption Algorithms
- □ AES128-CBC
- □ AES128-GCM
- □ AES256-CBC
- □ AES256-GCM
- □ Camellia-256-CBC
- □ ChaCha20-Poly1305
- □ Seed CBC

Authentication Algorithms
- □ SHA
- □ SHA256
- □ SHA384

Cipher Suites: 0 selected

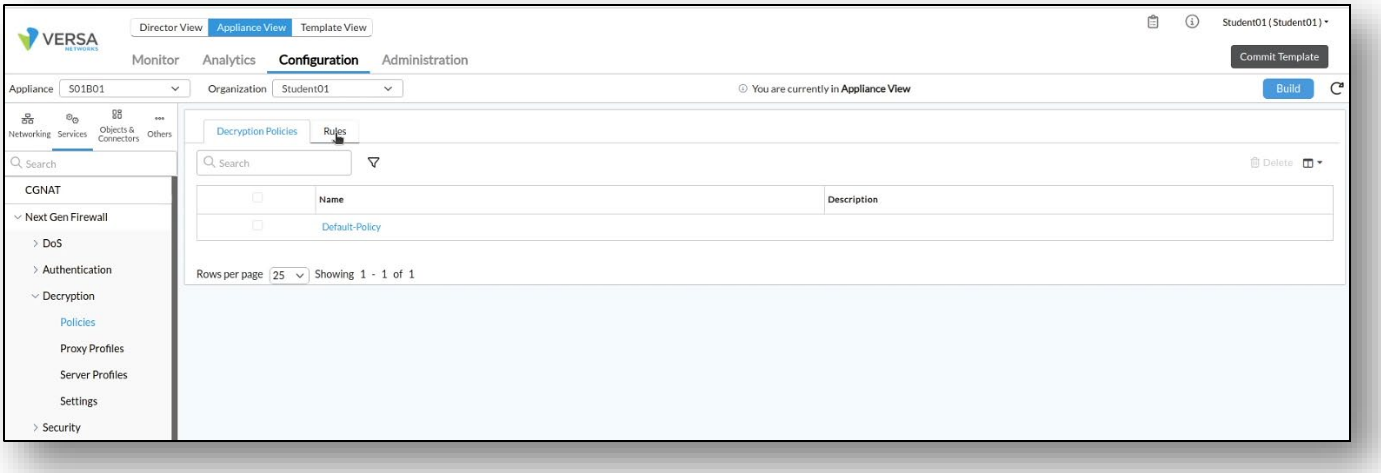
If you do not select any specific encryption and authentication algorithms, then all algorithms for the enabled TLS versions are automatically enabled

Step 6: Create an SSL Decryption Policy

In the next steps you will create an SSL decryption policy that has multiple rules.

- Rule 1 will identify traffic from Financial-Services web sites and will NOT decrypt the traffic (inspection only)
- Rule 2 will identify traffic from sports, news_and_media, and social_networking URL categories and will decrypt

Open the Policies window. Versa Director will automatically create a Default-Policy when you open the dialog.



Appliance: S01B01 | Organization: Student01

You are currently in Appliance View

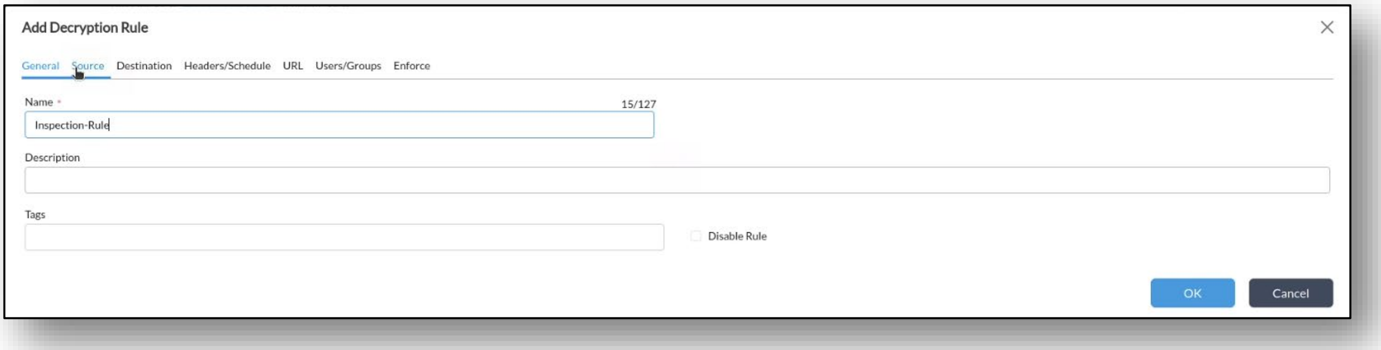
	Name	Description
□	Default-Policy	

Rows per page 25 | Showing 1 - 1 of 1

Click on the Rules tab to add rules to the policy.

Next you will create 2 rules with the following parameters:

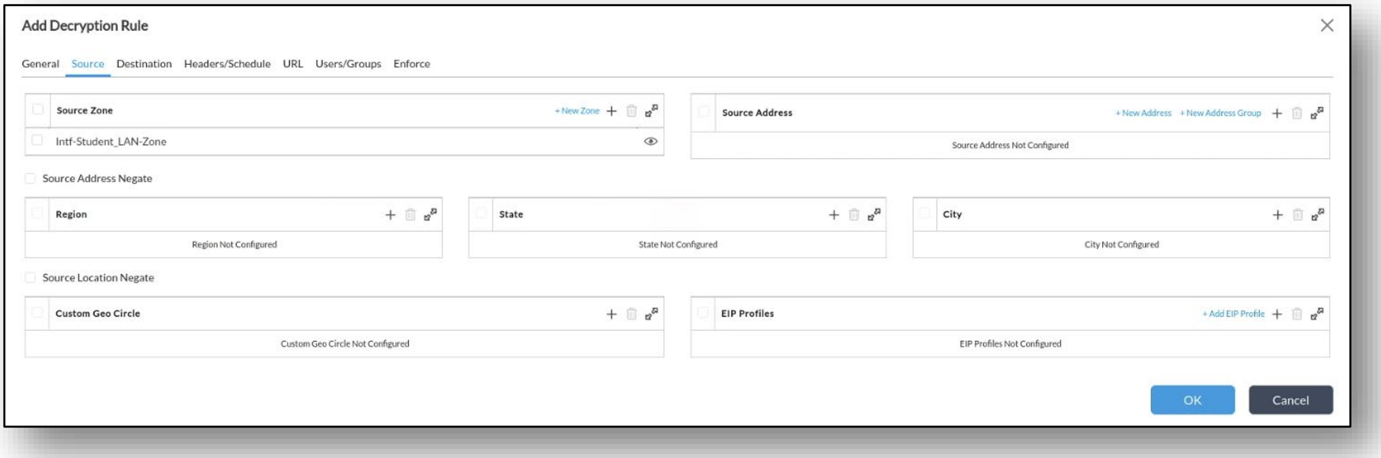
Rule 1: Inspection Rule. This rule will be used to inspect SSL certificates only (will not decrypt traffic).



Add Decryption Rule

Name * 15/127
Inspection-Rule
Description
Tags
□ Disable Rule

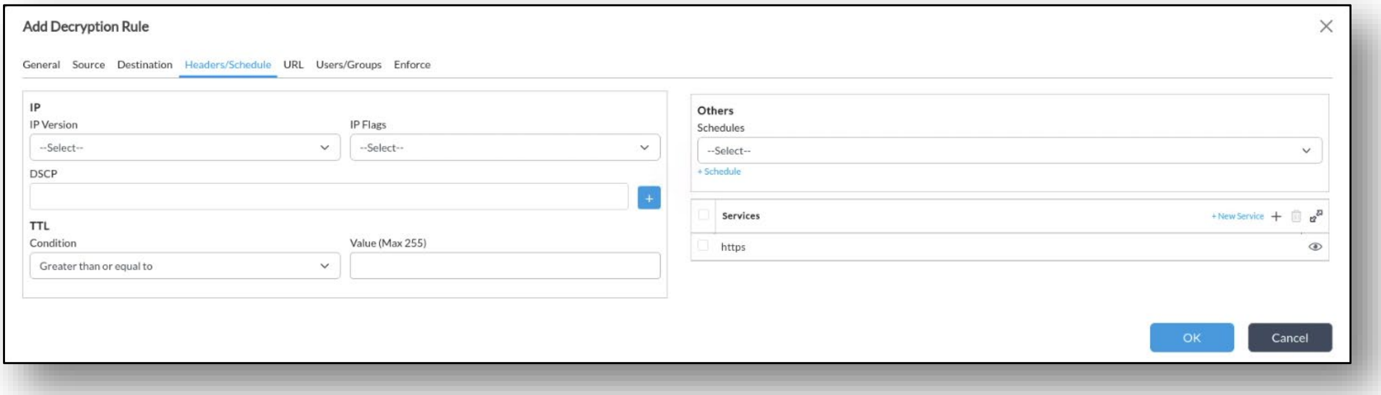
Inspect traffic from the Intf-Student_LAN-Zone



Add Decryption Rule

Source Zone: Intf-Student_LAN-Zone
Source Address: Source Address Not Configured
□ Source Address Negate
Region: Region Not Configured
State: State Not Configured
City: City Not Configured
□ Source Location Negate
Custom Geo Circle: Custom Geo Circle Not Configured
EIP Profiles: EIP Profiles Not Configured

Match the HTTPS service



IP

IP Version: --Select--

IP Flags: --Select--

DSCP

TTL

Condition: Greater than or equal to

Value (Max 255)

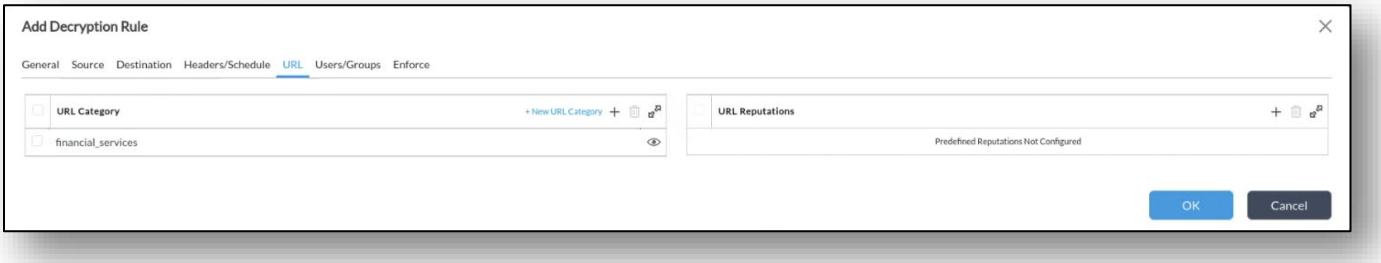
Others

Schedules: --Select--

+ Schedule

Services: https

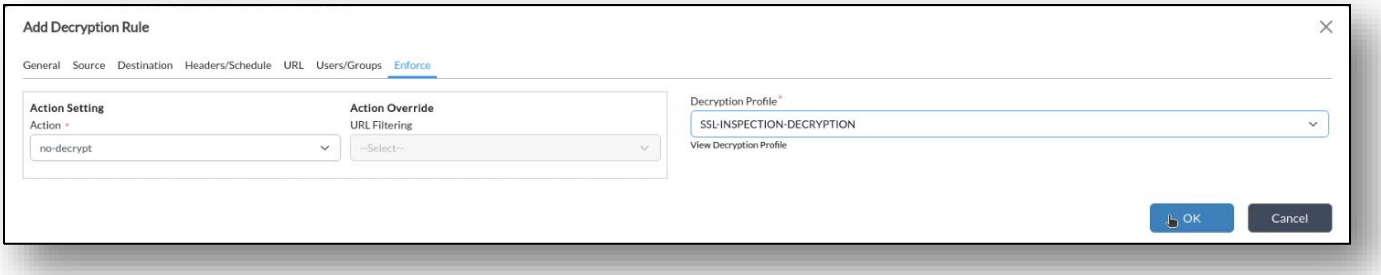
Match URLs that are in the financial_services category



URL Category: financial_services

URL Reputations: Predefined Reputations Not Configured

In the Enforce tab, set the action to no-decrypt, and the Decryption Profile to the SSL-INSPECTION-DECRYPTION profile. This will apply the SSL inspection rules in the profile to the sessions without decrypting the traffic.



Action Setting

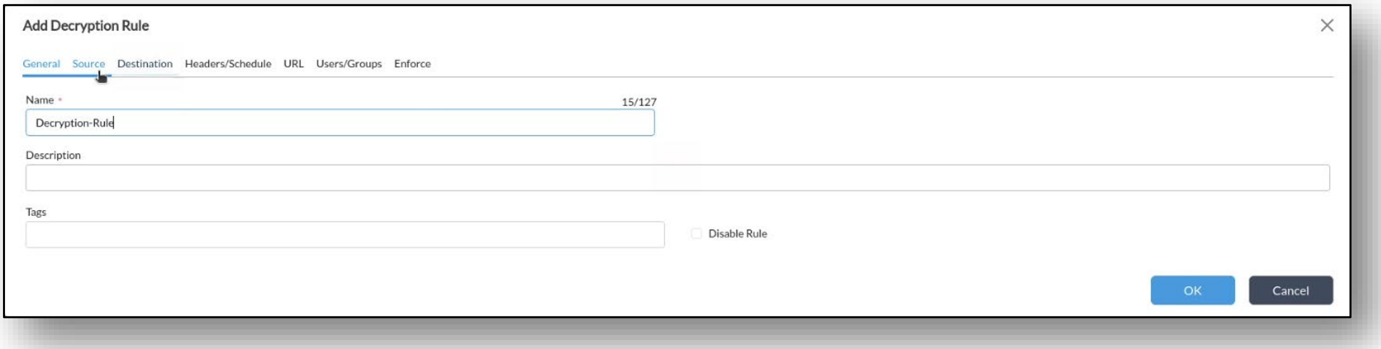
Action *: no-decrypt

Action Override

URL Filtering: --Select--

Decryption Profile *: SSL-INSPECTION-DECRYPTION

Rule 2: Decryption Rule. This rule will perform SSL Forward Proxy to matching traffic and will decrypt the data stream for security inspection.



Add Decryption Rule

General Source Destination Headers/Schedule URL Users/Groups Enforce

Name * 15/127

Decryption-Rule

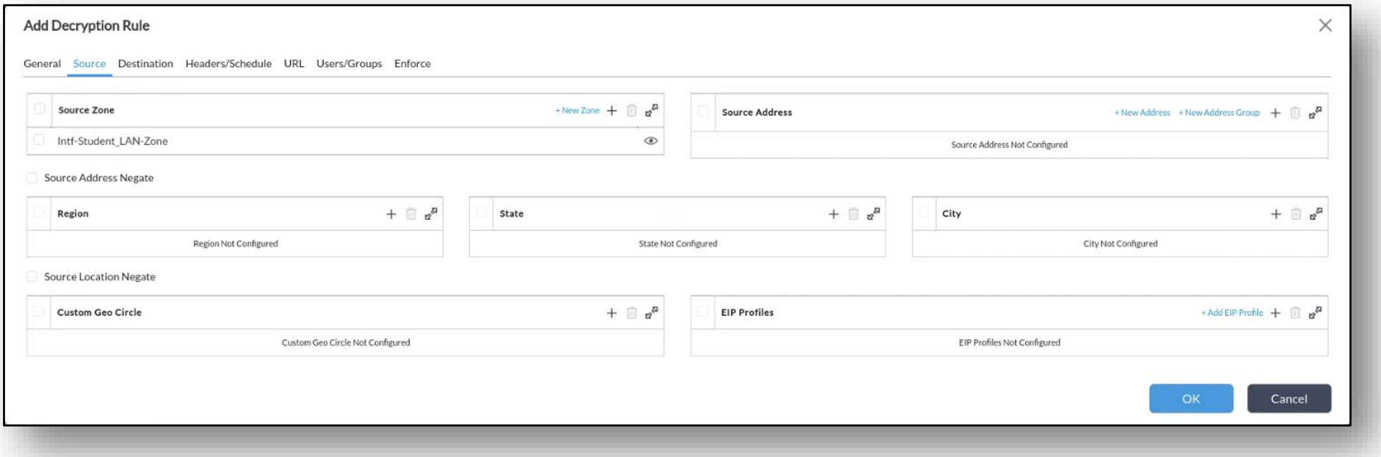
Description

Tags

□ Disable Rule

OK Cancel

Set the source zone to Intf-Student_LAN-Zone.



Add Decryption Rule

General Source Destination Headers/Schedule URL Users/Groups Enforce

Source Zone: Intf-Student_LAN-Zone

Source Address: Source Address Not Configured

□ Source Address Negate

Region: Region Not Configured

State: State Not Configured

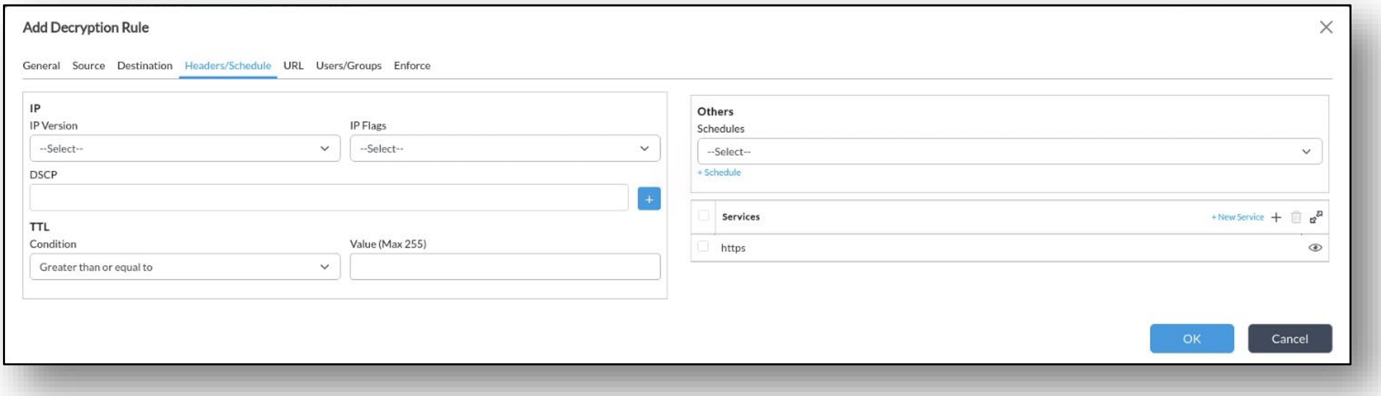
City: City Not Configured

□ Source Location Negate

Custom Geo Circle: Custom Geo Circle Not Configured

EIP Profiles: EIP Profiles Not Configured

Set the service to https.


Add Decryption Rule

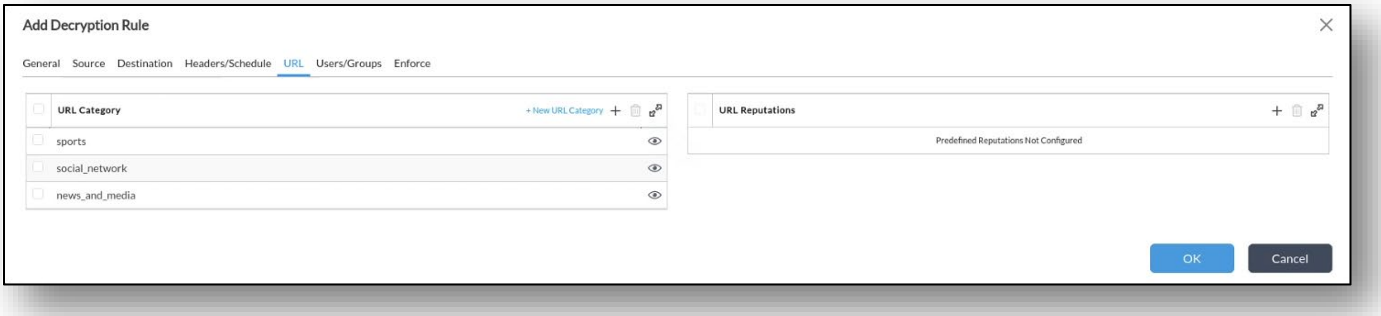
General | Source | Destination | Headers/Schedule | URL | Users/Groups | Enforce

IP
IP Version: --Select--
IP Flags: --Select--
DSCP:
TTL
Condition: Greater than or equal to
Value (Max 255):

Others
Schedules: --Select--
+ Schedule

□	Services
□	https

Set the rule to match URL categories of sports, social_network, and news_and_media.

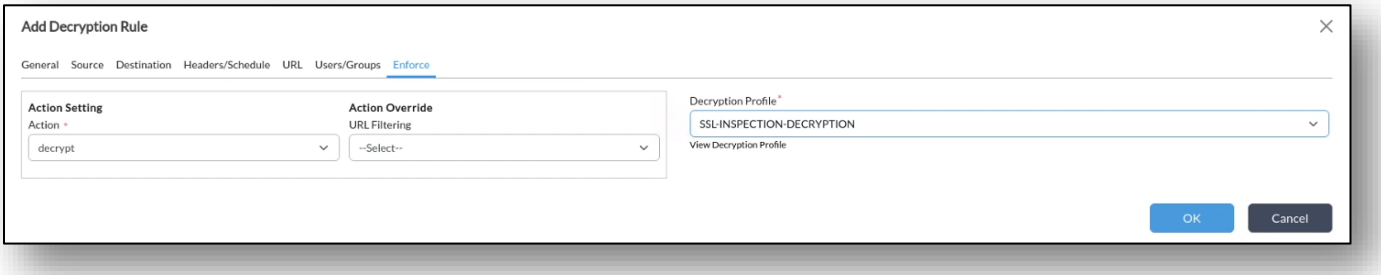

Add Decryption Rule

General | Source | Destination | Headers/Schedule | URL | Users/Groups | Enforce

□	URL Category
□	sports
□	social_network
□	news_and_media

□	URL Reputations
	Predefined Reputations Not Configured

Set the Enforce action to decrypt the traffic using the SSL-INSPECTION-DECRYPTION profile settings.


Add Decryption Rule

General | Source | Destination | Headers/Schedule | URL | Users/Groups | Enforce

Action Setting
Action *: decrypt

Action Override
URL Filtering: --Select--

Decryption Profile *: SSL-INSPECTION-DECRYPTION
View Decryption Profile

Exercise 2: Test the Decryption Policy

In this exercise you will test the decryption policy. To test the policy you will open a remote desktop session to the testing host (from the remote desktop) and use the Chromium web browser to visit sites that will be processed by the proxy profile.

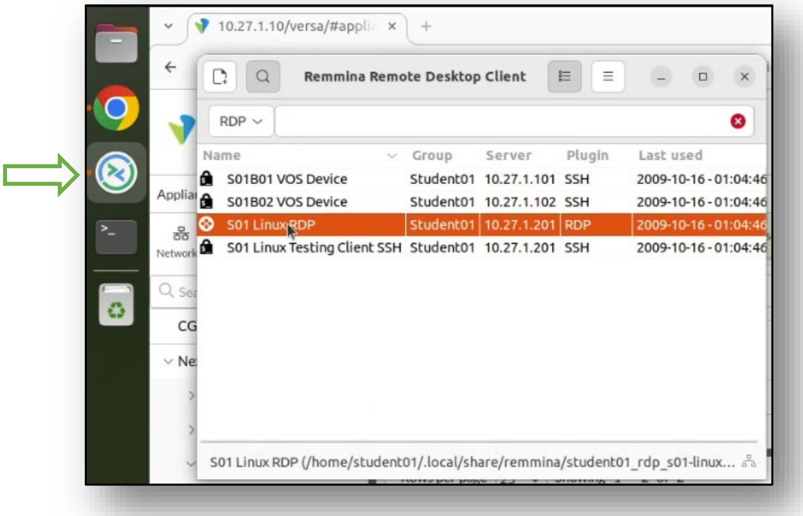
Steps in this exercise:

- Open a remote session to the testing host connected to your branch device
- Open the Chromium web browser
- Navigate to a financial institution web site
- Check the certificate validation
- Attempt to navigate to a sports web site
- Check the certificate validation
- Connect to the Versa Director (from the testing host), download and install the certificate from your appliance in Chromium
- Attempt to navigate to a sports web site
- Attempt to navigate to a news site
- Attempt to navigate to a social network site
- Attempt to navigate to a shopping site
- Attempt to navigate to a site that has a bad SSL certificate
- Analyze the results of the browsing sessions in Versa Director
- Analyze the results of the browsing sessions in Versa Analytics

Step 1: Open a remote desktop session to the testing host

Locate and open the Remmina Remote Desktop Client icon in the left application bar.

In the Remmina application, open the Sxx Linux RDP session, where Sxx is your Student ID. If prompted, the RDP credentials for the remote session are: username: *student*; password: *versa123*.

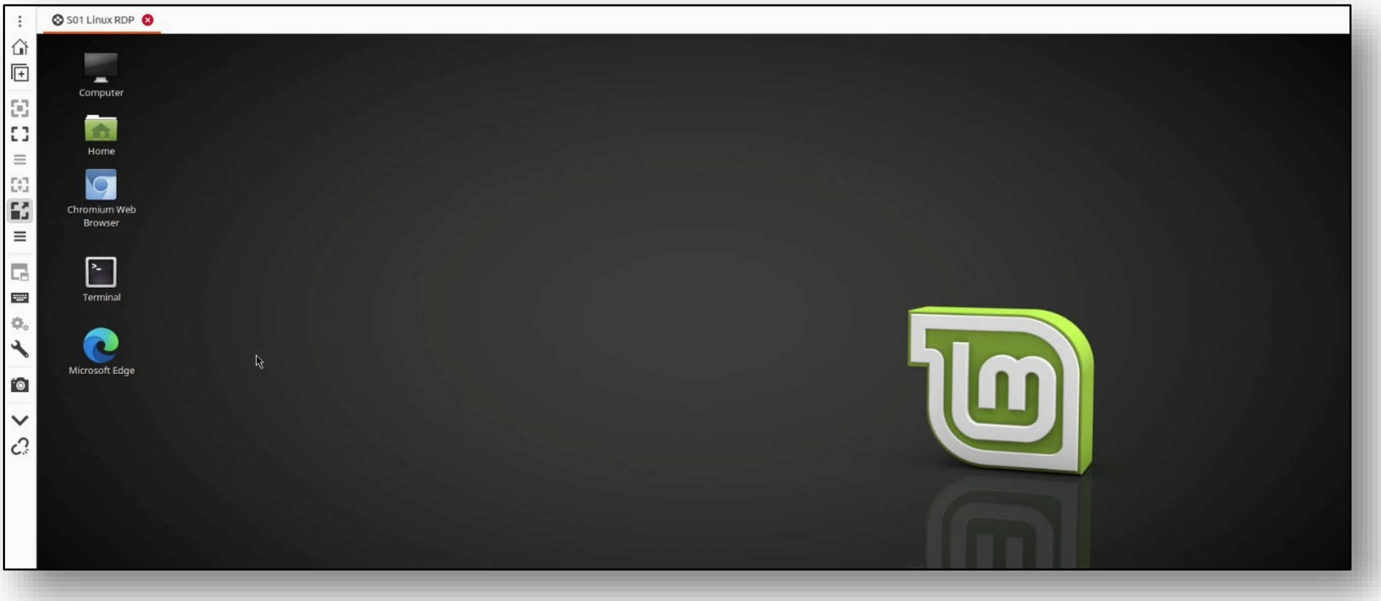


Name	Group	Server	Plugin	Last used
S01B01 VOS Device	Student01	10.27.1.101	SSH	2009-10-16 - 01:04:46
S01B02 VOS Device	Student01	10.27.1.102	SSH	2009-10-16 - 01:04:46
S01 Linux RDP	Student01	10.27.1.201	RDP	2009-10-16 - 01:04:46
S01 Linux Testing Client SSH	Student01	10.27.1.201	SSH	2009-10-16 - 01:04:46

S01 Linux RDP (/home/student01/.local/share/remmina/student01_rdp_s01-linux...

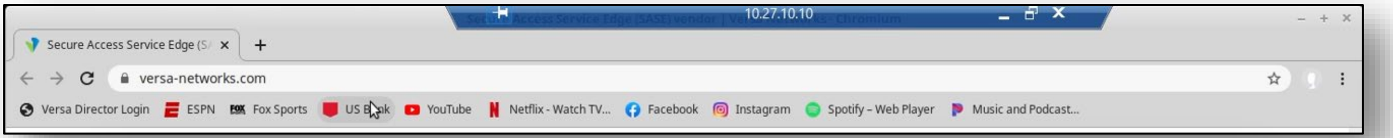
Note: The remote desktop resolution is set to the size of the Remmina application window when the RDP session is started. If the resolution is too small, you can increase the size of the RDP session main window, then close and re-open the RDP session to reset the remote desktop resolution.

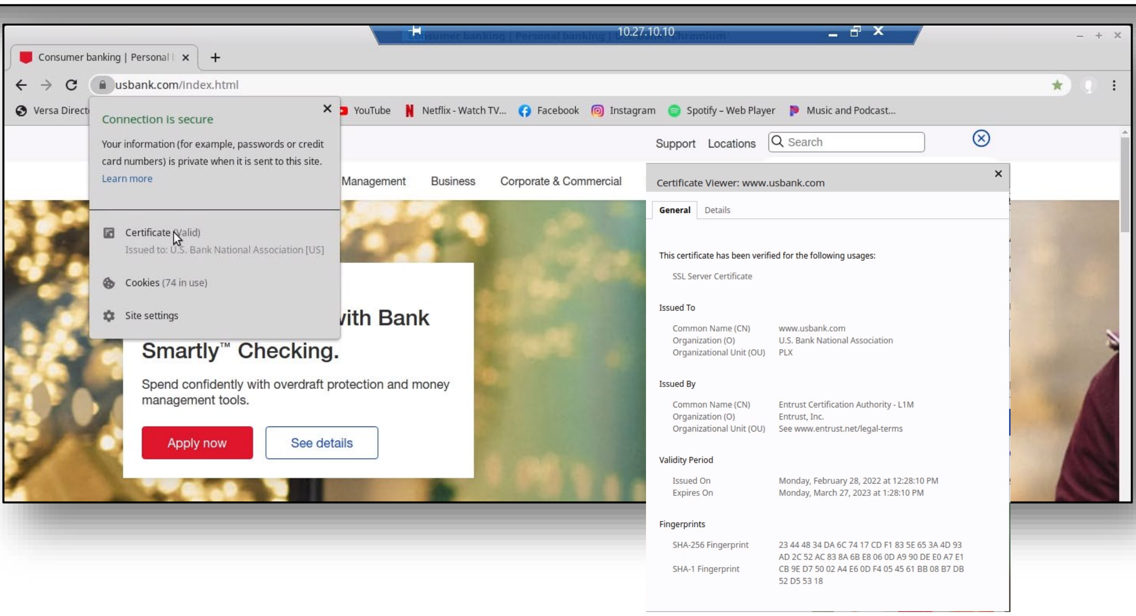
You should be presented with the remote desktop below.



For this exercise use the Chromium Web Browser for proper performance.

Open the Chromium browser on the remote desktop and navigate to ***www.usbank.com***. You can use the bookmark in the bookmark bar.





Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)
Issued to: U.S. Bank National Association [US]

Cookies (74 in use)

Site settings

...vith Bank Smartly™ Checking.

Spend confidently with overdraft protection and money management tools.

Certificate Viewer: www.usbank.com

General | Details

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)	www.usbank.com
Organization (O)	U.S. Bank National Association
Organizational Unit (OU)	PLX

Issued By

Common Name (CN)	Entrust Certification Authority - L1M
Organization (O)	Entrust, Inc.
Organizational Unit (OU)	See www.entrust.net/legal-terms

Validity Period

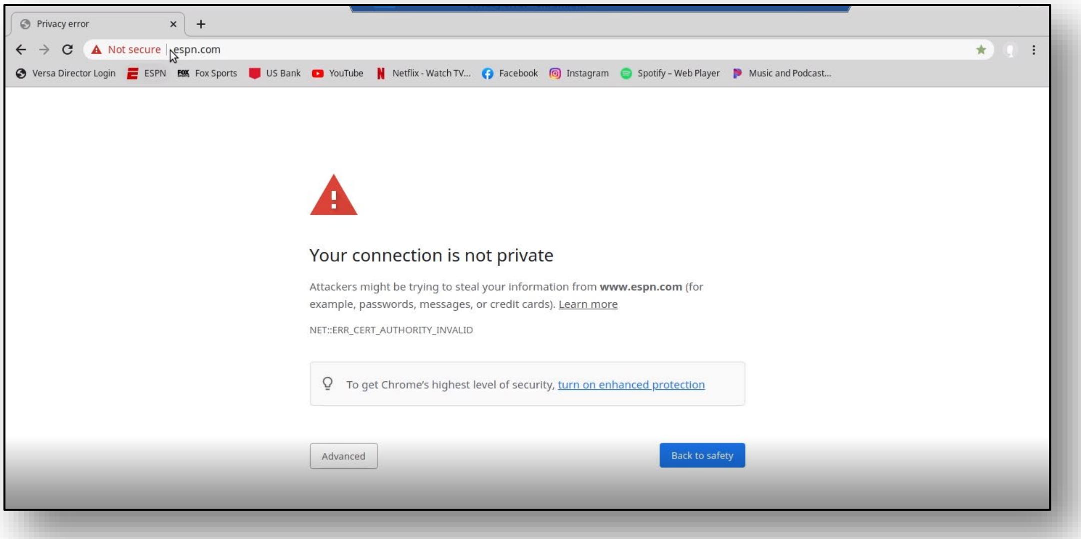
Issued On	Monday, February 28, 2022 at 12:28:10 PM
Expires On	Monday, March 27, 2023 at 1:28:10 PM

Fingerprints

SHA-256 Fingerprint	23 44 48 34 DA 6C 74 17 CD F1 83 5E 65 3A 4D 93 AD 2C 52 AC 83 8A 6B E8 06 0D A9 90 DE E0 A7 E1
SHA-1 Fingerprint	CB 9E D7 50 02 A4 E6 0D F4 05 45 61 BB 08 B7 DB 52 D5 53 18

After the page loads, click Lock icon in the address bar. You should see a popup that indicates that the certificate (and site) is valid. If you click the Certificate button, you will see that the certificate was verified by Entrust, Inc. (a registered certificate authority).

Next, enter the address ***www.espn.com*** in the address bar. You should see an alert indicating that there is a problem with the certificate for the ESPN site.



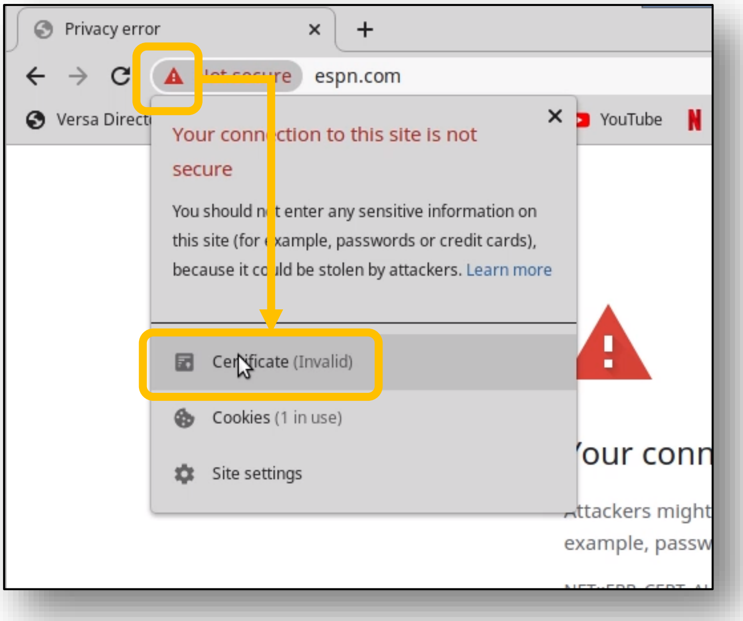
Your connection is not private

Attackers might be trying to steal your information from **www.espn.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

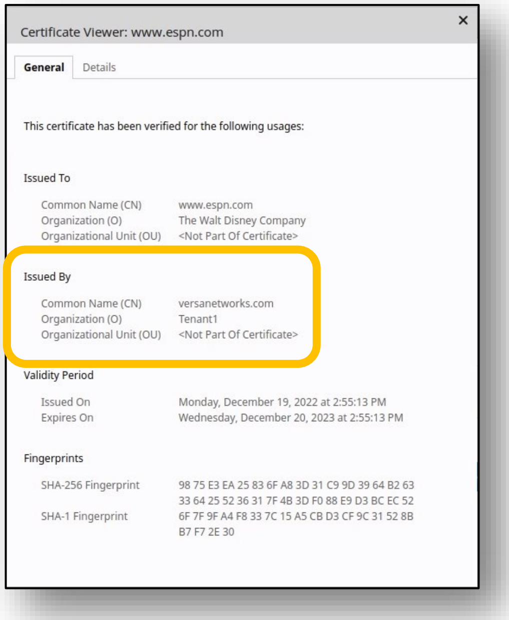
To get Chrome's highest level of security, turn on enhanced protection

Follow the steps below to view the provider of the certificate used on the site.



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more



Certificate Viewer: www.espn.com

This certificate has been verified for the following usages:

Issued To

Common Name (CN)	www.espn.com
Organization (O)	The Walt Disney Company
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	versanetworks.com
Organization (O)	Tenant1
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, December 19, 2022 at 2:55:13 PM
Expires On	Wednesday, December 20, 2023 at 2:55:13 PM

Fingerprints

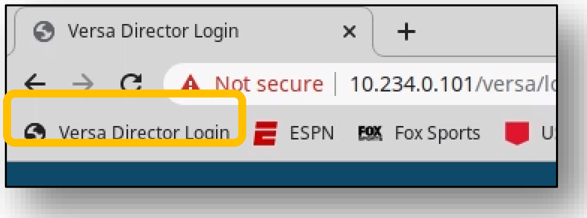
SHA-256 Fingerprint	98 75 E3 EA 25 83 6F A8 3D 31 C9 9D 39 64 B2 63 33 64 25 52 36 31 7F 4B 3D F0 88 E9 D3 BC EC 52
SHA-1 Fingerprint	6F 7F 9F A4 F8 33 7C 15 A5 CB D3 CF 9C 31 52 8B B7 F7 2E 30

The certificate for the sports site was provided by Tenant1. This is because the branch device intercepted the SSL session and is acting as a proxy for the SSL tunnel.

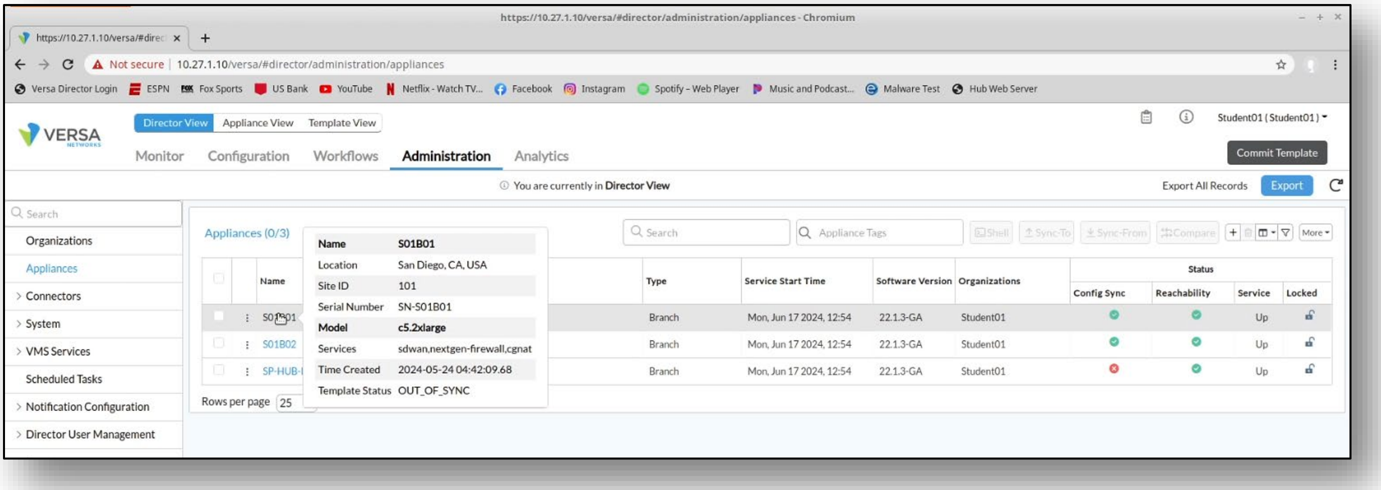
To allow the browser to trust the Tenant1 certificate, you must download the certificate to the host machine and add it to the trusted certificate provider list.

Close the certificate information windows and return to the main browser window.

In the remote desktop Chromium browser, click the Versa Director bookmark to open Versa Director (the remote host has an out-of-band management network connection to Versa Director).



In Versa Director, navigate to the *Administration > Appliances* dashboard and locate your appliance in the appliance table. Click your appliance to open your appliance configuration.



You are currently in **Director View**

Appliances (0/3)

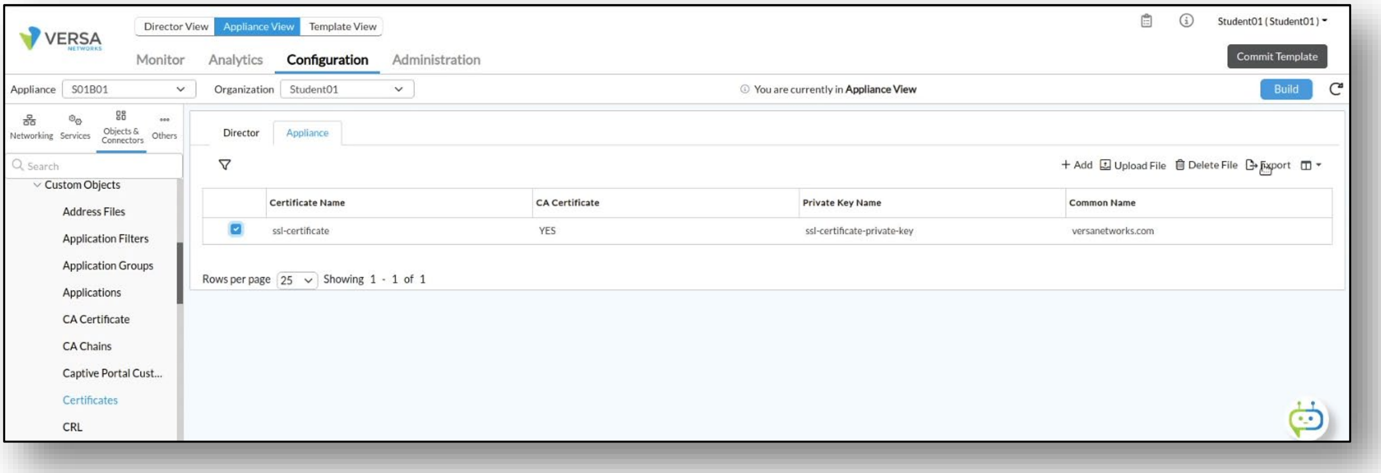
Name	S01B01
Location	San Diego, CA, USA
Site ID	101
Serial Number	SN-S01B01
Model	c5.2xlarge
Services	sdwan,nextgen-firewall,cgnat
Time Created	2024-05-24 04:42:09.68
Template Status	OUT_OF_SYNC

Name	Type	Service Start Time	Software Version	Organizations	Status			
					Config Sync	Reachability	Service	Locked
S01B01	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✓	✓	Up	🔓
S01B02	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✓	✓	Up	🔓
SP-HUB-[illegible]	Branch	Mon, Jun 17 2024, 12:54	22.1.3-GA	Student01	✗	✓	Up	🔓

Rows per page 25

In your appliance configuration, navigate to ***Objects & Connectors > Custom Objects > Certificate***s, then select the Appliance tab in the Certificates window.

Locate your certificate in the Appliance certificate table. Check the box next to the certificate so that the Export button becomes active. Click the *Export* button to download the certificate to the remote desktop Downloads folder.

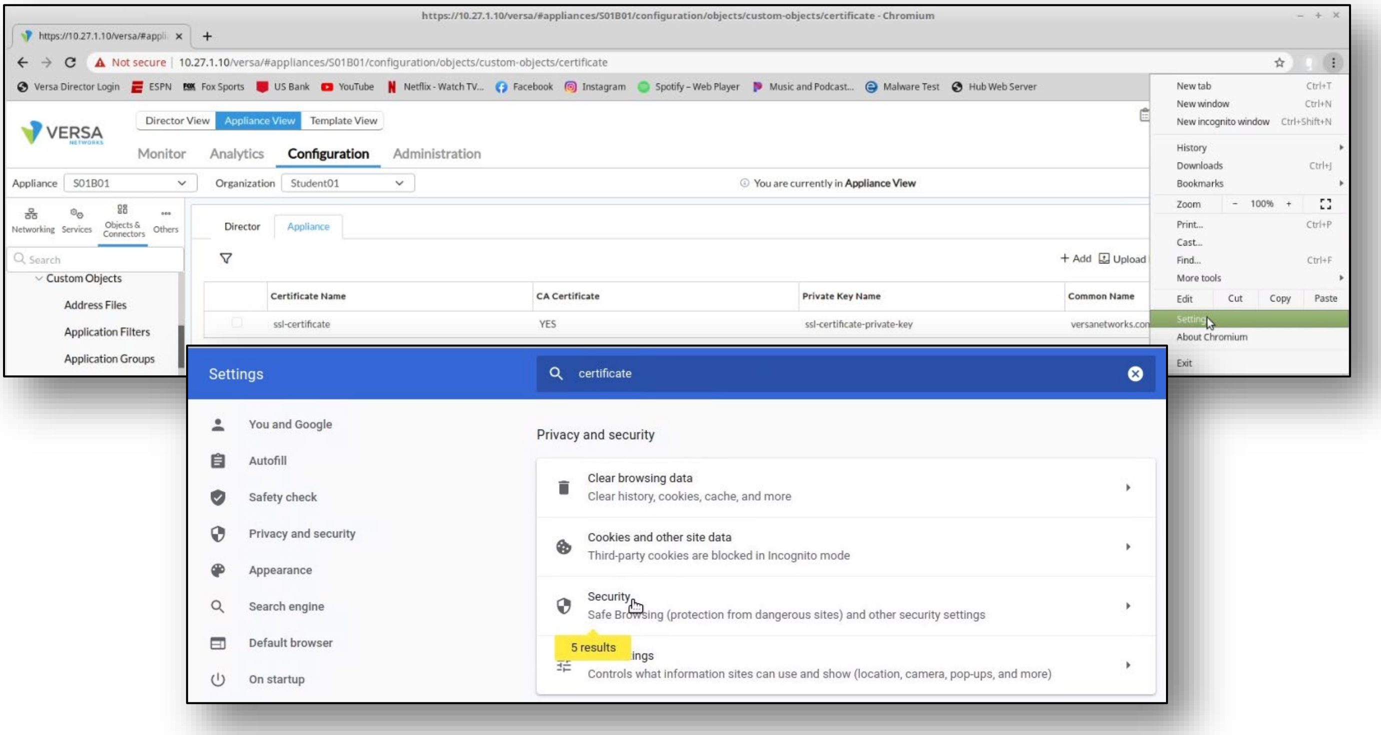


Appliance: S01B01
Organization: Student01
You are currently in Appliance View

	Certificate Name	CA Certificate	Private Key Name	Common Name
☑	ssl-certificate	YES	ssl-certificate-private-key	versanetworks.com

Rows per page 25 Showing 1 - 1 of 1

After you have downloaded the certificate, click the Settings button in the remote browser and open the browser Preferences. In the preferences window, type the word certificate in the search window. This will display the View Certificates button. Click the View Certificates button to open the certificate manager.



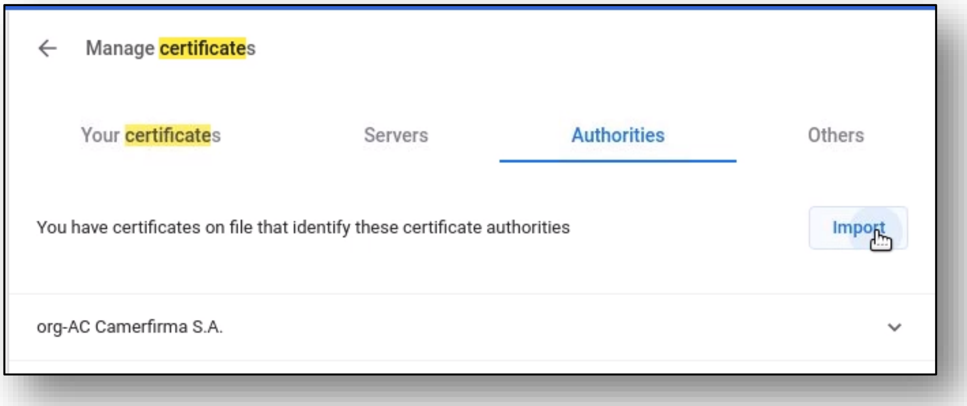
https://10.27.1.10/versa/#appliances/S01B01/configuration/objects/custom-objects/certificate - Chromium

Not secure | 10.27.1.10/versa/#appliances/S01B01/configuration/objects/custom-objects/certificate

	Certificate Name	CA Certificate	Private Key Name	Common Name
□	ssl-certificate	YES	ssl-certificate-private-key	versanetworks.com

Settings search: certificate

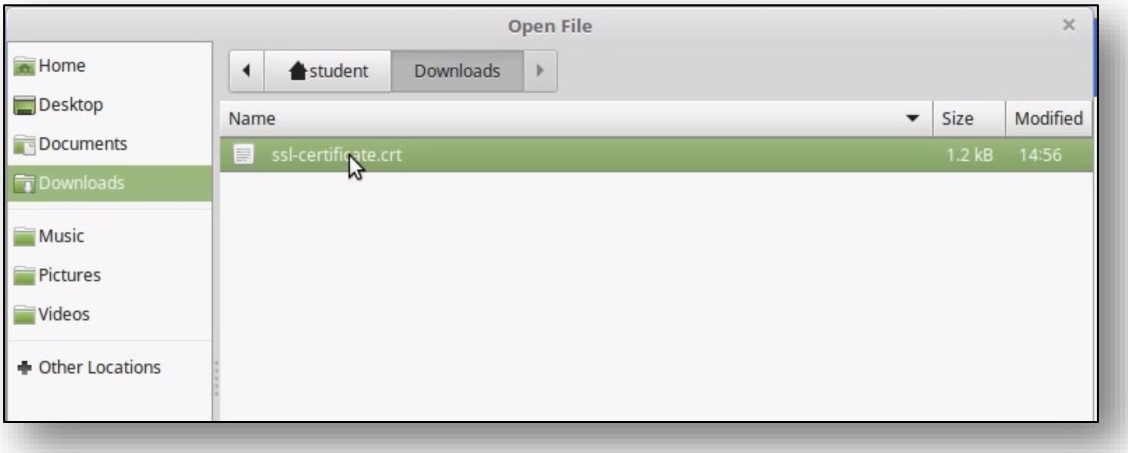
In the Certificate Manager window, select Authorities from the top menu bar. Scroll down in the Authorities window until you see the Import button at the bottom.



You have certificates on file that identify these certificate authorities

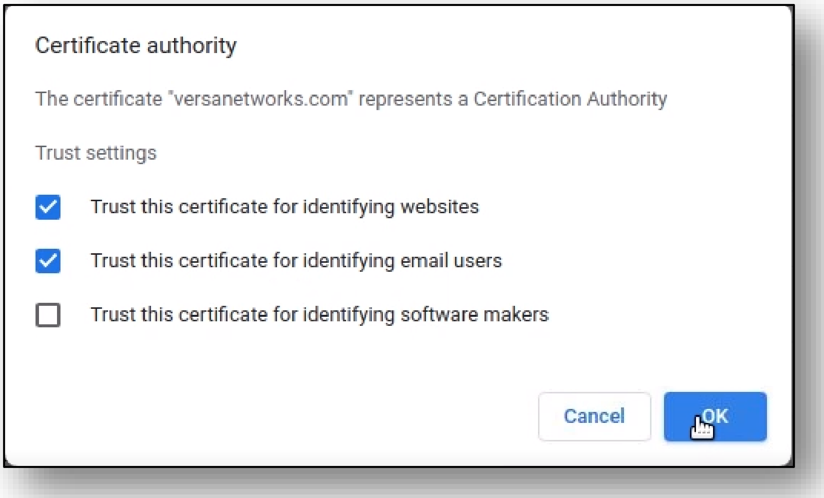
org-AC Camerfirma S.A.

Open the Downloads folder and locate the new SSL certificate. Note that there will be a duplicate certificate because a certificate was already present. Choose the newer certificate (based on the date) and click the Open button to import the certificate.



Name	Size	Modified
ssl-certificate.crt	1.2 kB	14:56

Select the option to trust the CA to identify websites, then click OK.



Certificate authority

The certificate "versanetworks.com" represents a Certification Authority

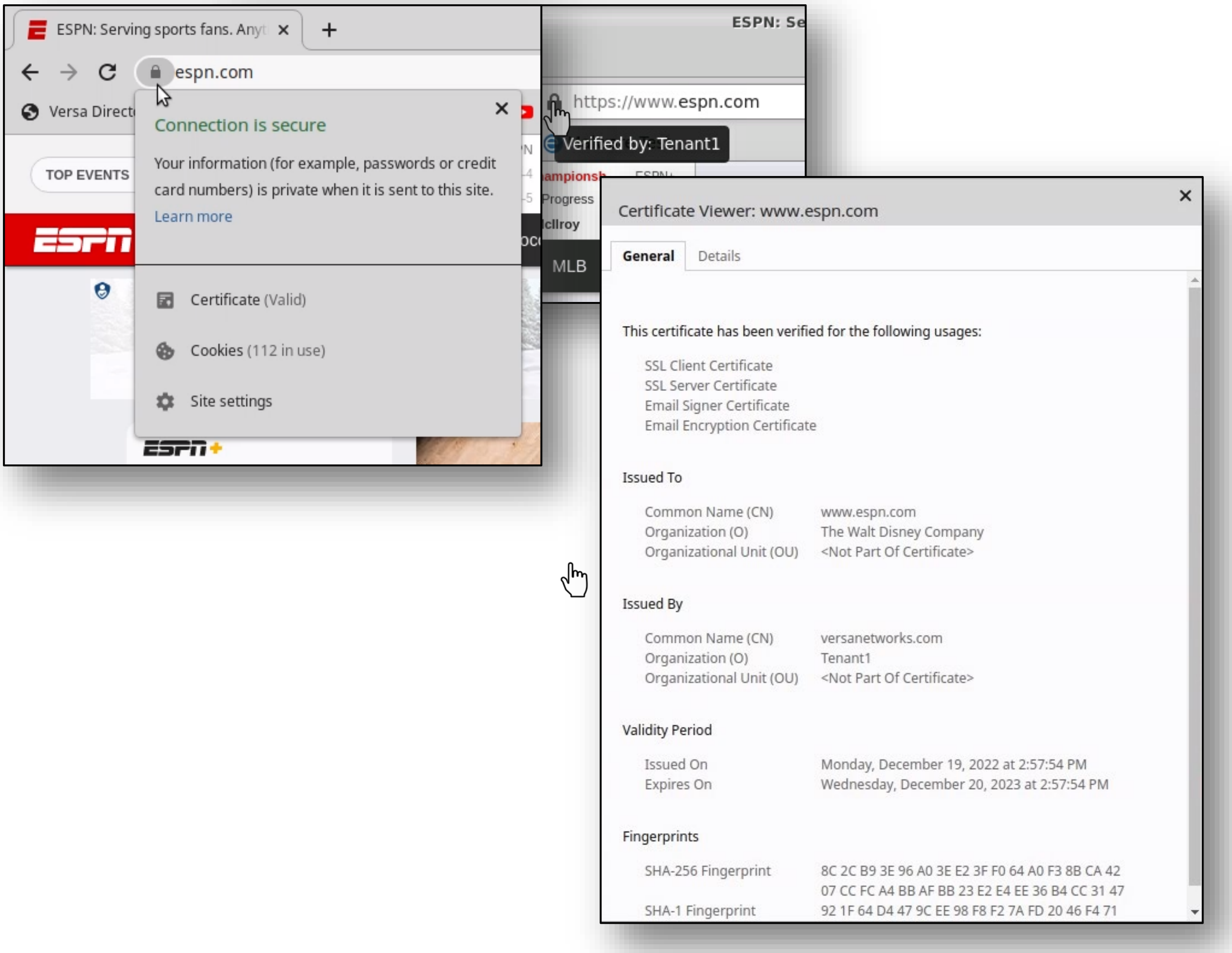
Trust settings

☑ Trust this certificate for identifying websites

☑ Trust this certificate for identifying email users

□ Trust this certificate for identifying software makers

Enter the address ***www.espn.com*** in the remote browser address bar again. The web site should now open properly.



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Cookies (112 in use)

Site settings

Certificate Viewer: www.espn.com

This certificate has been verified for the following usages:

SSL Client Certificate
SSL Server Certificate
Email Signer Certificate
Email Encryption Certificate

Issued To

Common Name (CN)	www.espn.com
Organization (O)	The Walt Disney Company
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	versanetworks.com
Organization (O)	Tenant1
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

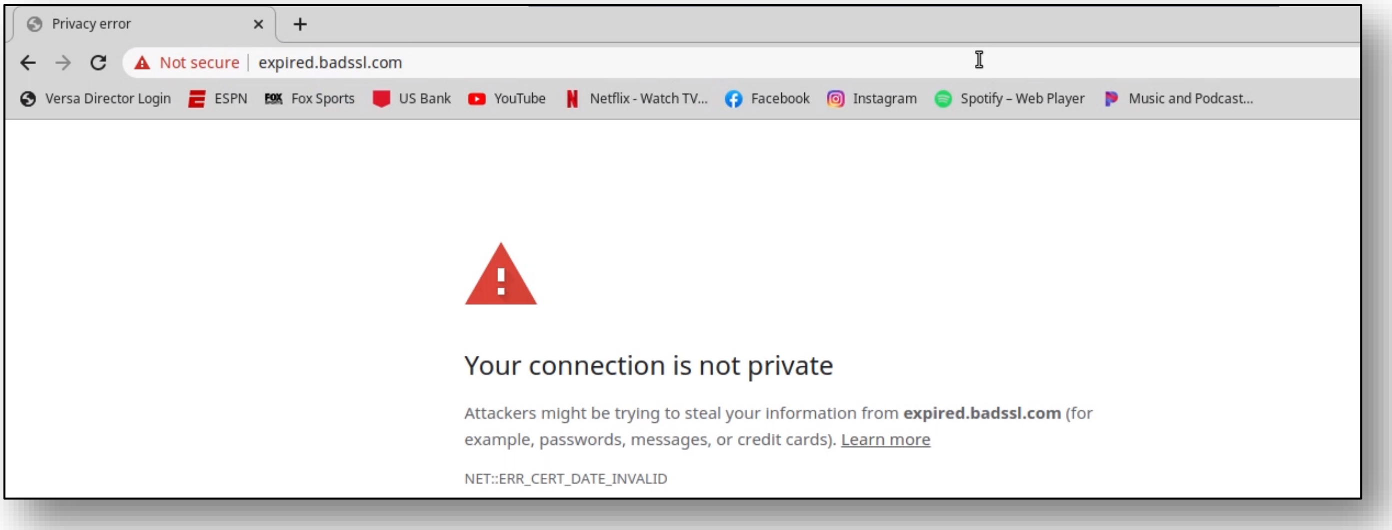
Issued On	Monday, December 19, 2022 at 2:57:54 PM
Expires On	Wednesday, December 20, 2023 at 2:57:54 PM

Fingerprints

SHA-256 Fingerprint	8C 2C B9 3E 96 A0 3E E2 3F F0 64 A0 F3 8B CA 42 07 CC FC A4 BB AF BB 23 E2 E4 EE 36 B4 CC 31 47
SHA-1 Fingerprint	92 1F 64 D4 47 9C EE 98 F8 F2 7A FD 20 46 F4 71

The URLs that are matched by the decryption rule are proxied. The URLs that are not matched by the decryption rule are not proxied.

In the remote browser, navigate to ***https://expired.badssl.com***. You should receive a browser warning that the certificate has an issue. Currently the proxy policy rules do not match the site, so the bad certificate is loaded by the browser and the browser provides the warning.



Your connection is not private

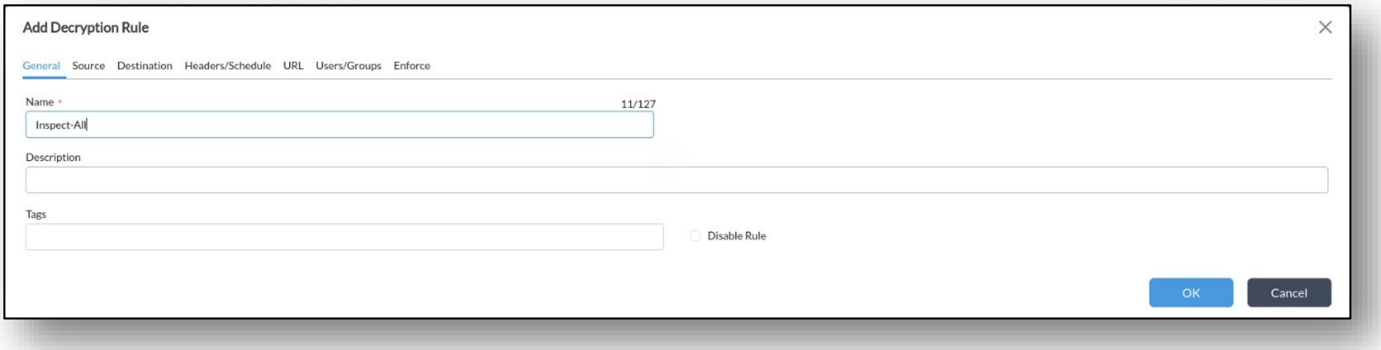
Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

Return to the Versa Director session on your remote desktop.

In Versa Director, navigate to your device configuration and open the *Services > Next Gen Firewall > Decryption > Policies* configuration.

Add a new rule to the policy that matches all HTTP and HTTPS traffic sourced from the local LAN and applies the no-decrypt action. The new rule should be at the end of the rule list so that it doesn't interfere with the existing rules.



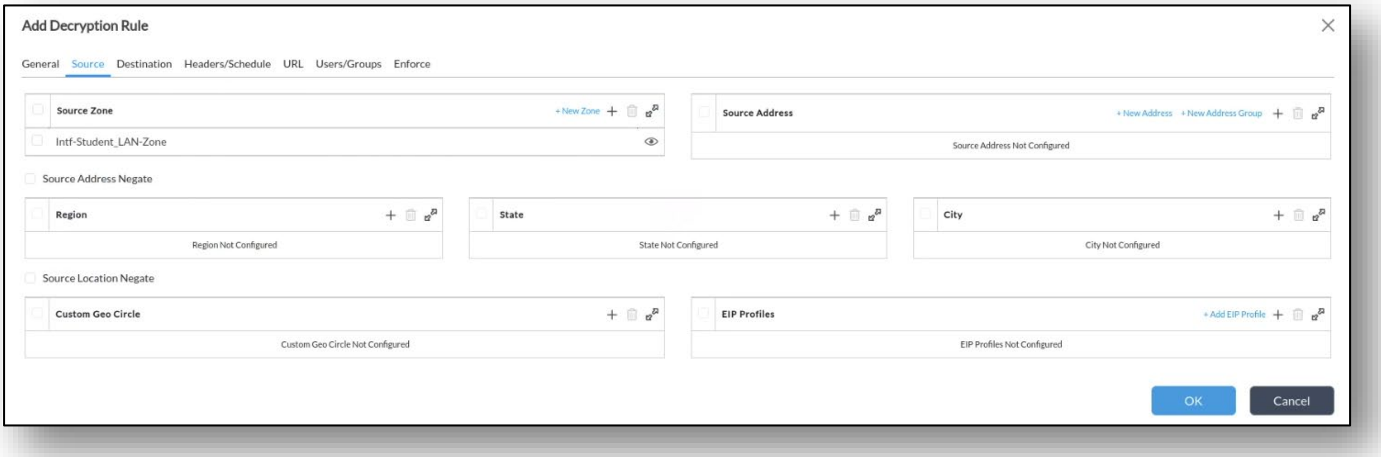
Name * 11/127
Inspect-All

Description

Tags

□ Disable Rule

Match traffic from the Intf-Student_LAN-Zone source zone.



Add Decryption Rule

Source Zone: Intf-Student_LAN-Zone

Source Address: Source Address Not Configured

□ Source Address Negate

Region: Region Not Configured

State: State Not Configured

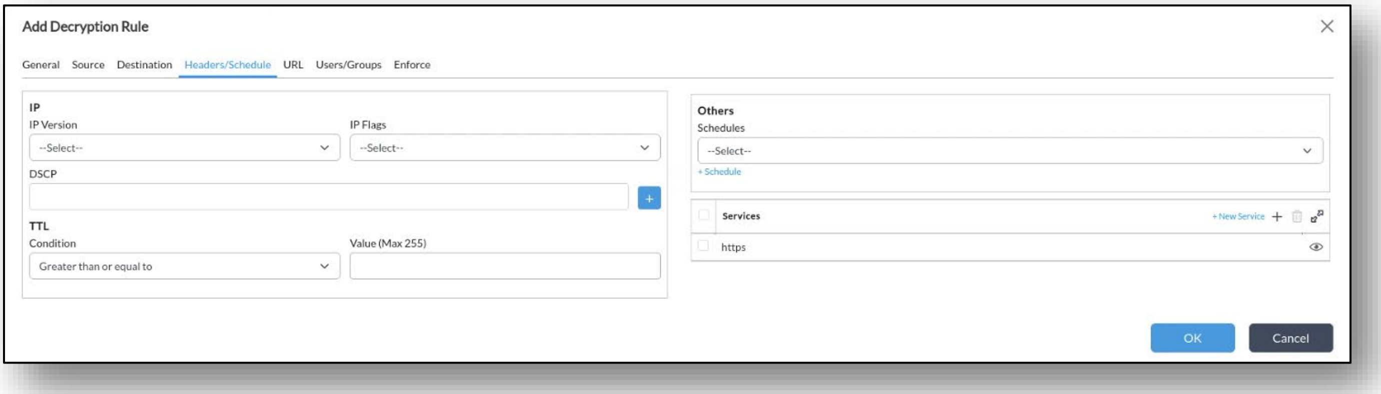
City: City Not Configured

□ Source Location Negate

Custom Geo Circle: Custom Geo Circle Not Configured

EIP Profiles: EIP Profiles Not Configured

Match the HTTPS service.



Add Decryption Rule

IP

IP Version: --Select--

IP Flags: --Select--

DSCP:

TTL

Condition: Greater than or equal to

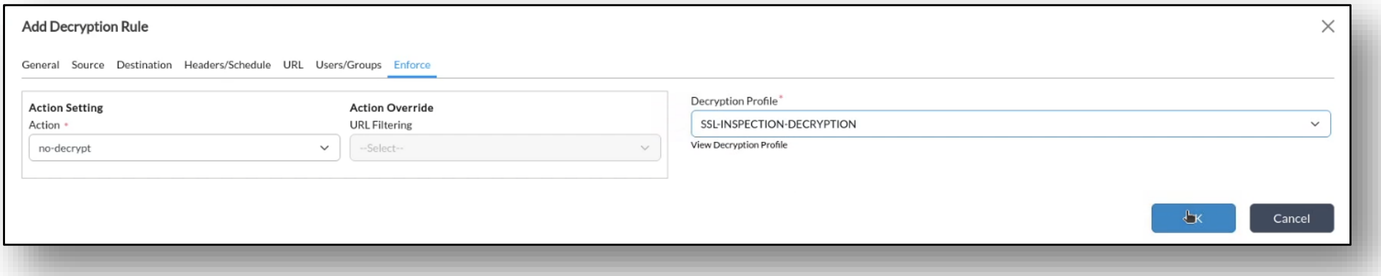
Value (Max 255):

Others

Schedules: --Select--

Services: https

Set the Enforce action to no-decrypt and use the SSL-INSPECTION-DECRYPTION profile for SSL inspection.



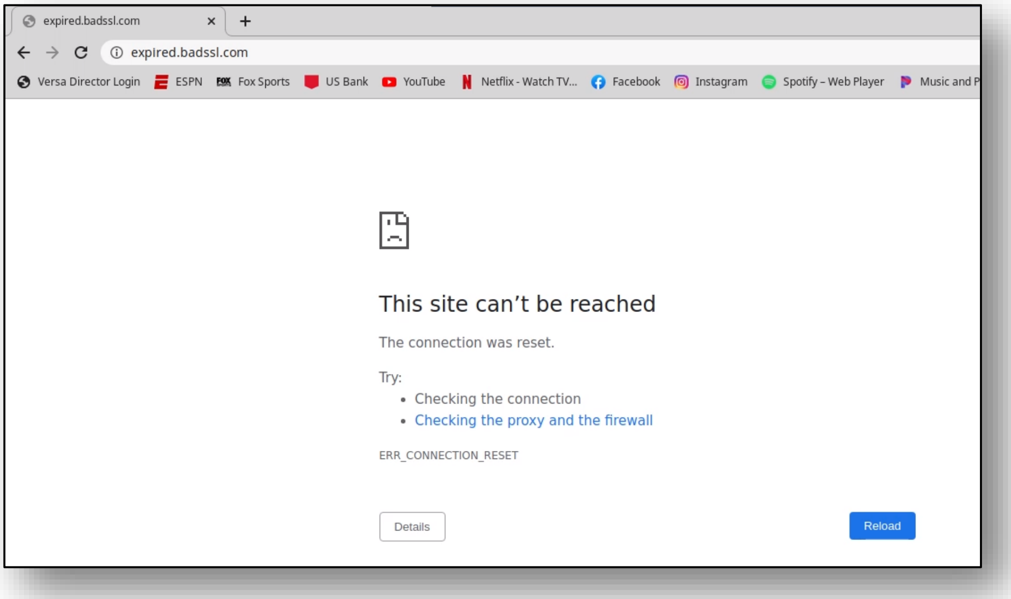
Action Setting
Action *: no-decrypt

Action Override
URL Filtering: --Select--

Decryption Profile *: SSL-INSPECTION-DECRYPTION

Return to the remote desktop client (Remmina Linux RDP). In the Linux testing client, navigate to the site expired.badssl.com to view the inspection results.

Note: The web page may be cached, so it will not be re-inspected. To force the inspection of the web site, navigate to one of the other sites in the bookmark bar (e.g. ESPN), then enter the expired.badssl.com URL in the browser again. The site should now be blocked.



This site can’t be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

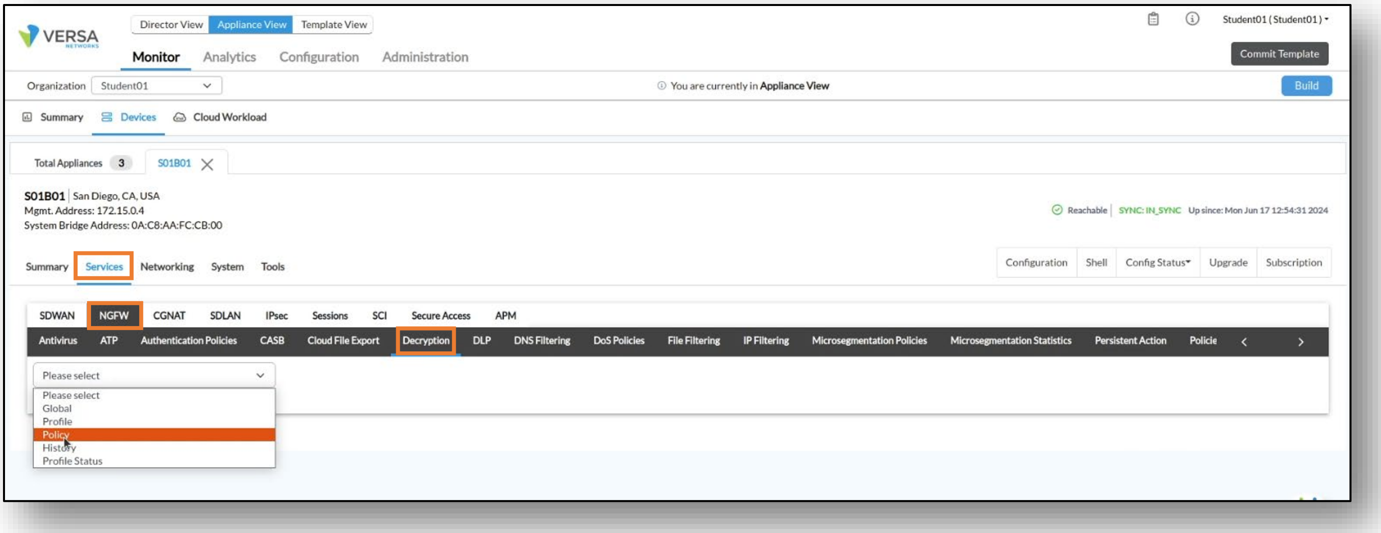
Exercise 3: Verify the Decryption Process in Versa Director and Versa Analytics

In the next steps you will verify the SSL Decryption and Inspection functions in Versa Director and Versa Analytics.

Close the remote browser connection to the testing host and return to your remote desktop. In your remote desktop, navigate to the Monitor tab of your appliance. In the Monitor tab of your appliance, select the *Service > NGFW > Decryption*.

In the Services dashboard, select NGFW to display the Next Generation Firewall statistics.

In the Decryption table, select *Policy > Default-Policy* from the drop-down menu.

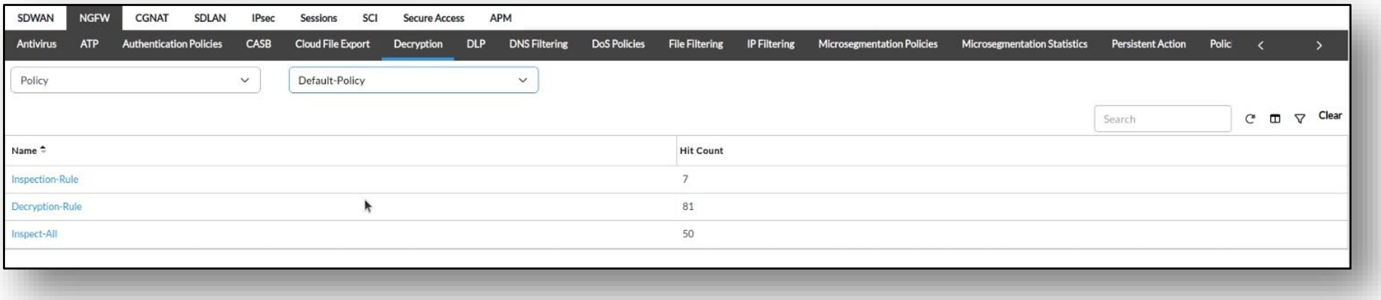


S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:C8:AA:FC:CB:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 17 12:54:31 2024

You should see non-zero counters in all of the rules The rules display how many sessions have matched each of the rules.

Select Profile from the left drop-down menu to display the profile statistics. This will display the number of packets that have been inspected, decrypted, and dropped by the encryption profile.

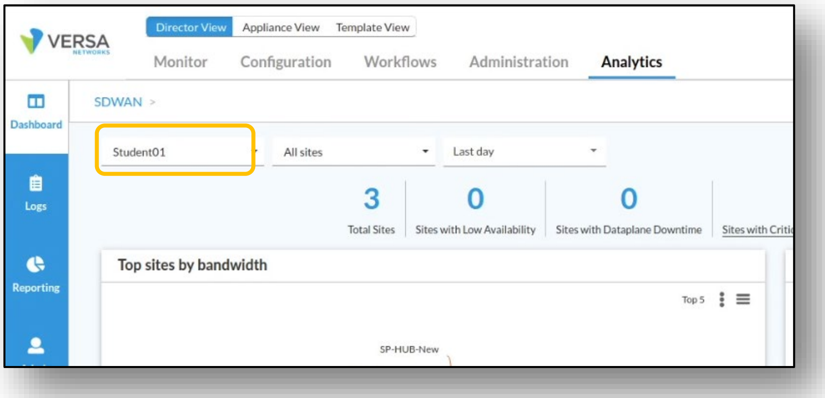


Policy
Default-Policy

Name	Hit Count
Inspection-Rule	7
Decryption-Rule	81
Inspect-All	50

Click the *Director View* button to exit Appliance View.

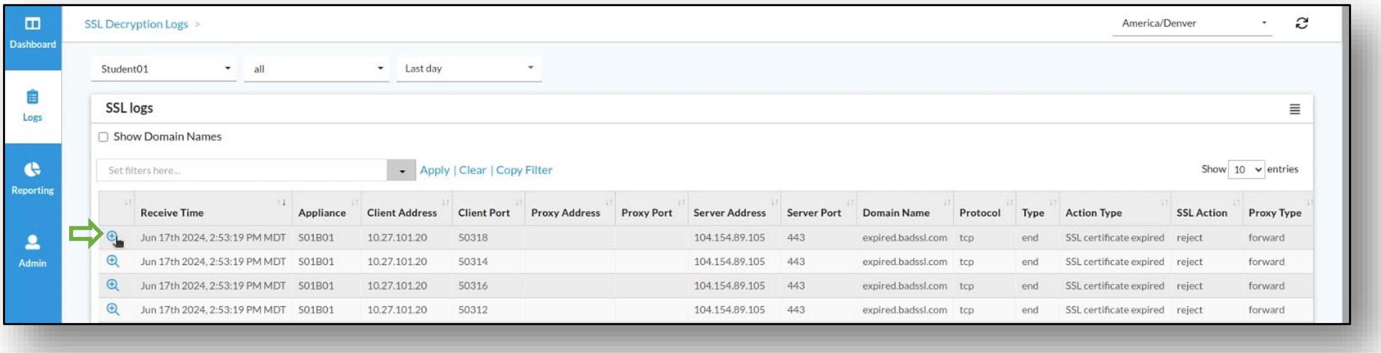
From the Director View dashboard, click the Analytics tab to open Versa Analytics. Ensure that your student ID is selected in the organization drop-down menu.



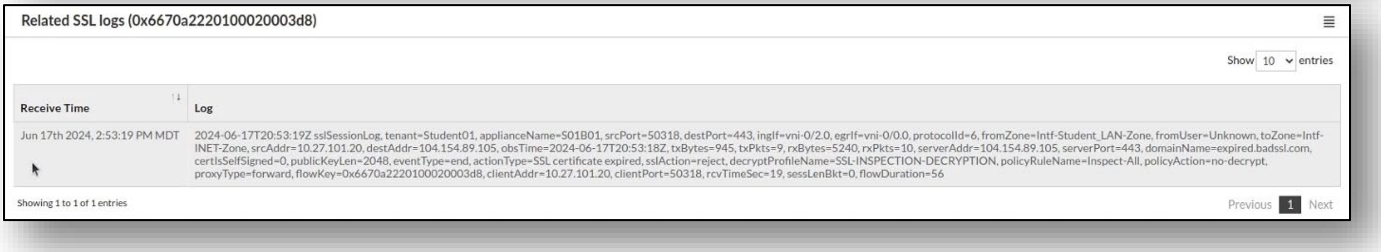
In the left side menu, navigate to *Logs > SSL Decryption* to view the SSL decryption logs. You should see entries in the logs.

Locate a log entry with the Action Type of SSL certificate expired. Click the magnifying glass next to the log entry to view more details.

> Note: You can filter the log entries by selecting your device in the top device filter. This will allow you to remove log entries from other devices from the log list.



	Receive Time	Appliance	Client Address	Client Port	Proxy Address	Proxy Port	Server Address	Server Port	Domain Name	Protocol	Type	Action Type	SSL Action	Proxy Type
🔍	Jun 17th 2024, 2:53:19 PM MDT	S01B01	10.27.101.20	50318			104.154.89.105	443	expired.badssl.com	tcp	end	SSL certificate expired	reject	forward
🔍	Jun 17th 2024, 2:53:19 PM MDT	S01B01	10.27.101.20	50314			104.154.89.105	443	expired.badssl.com	tcp	end	SSL certificate expired	reject	forward
🔍	Jun 17th 2024, 2:53:19 PM MDT	S01B01	10.27.101.20	50316			104.154.89.105	443	expired.badssl.com	tcp	end	SSL certificate expired	reject	forward
🔍	Jun 17th 2024, 2:53:19 PM MDT	S01B01	10.27.101.20	50312			104.154.89.105	443	expired.badssl.com	tcp	end	SSL certificate expired	reject	forward



Receive Time	Log
Jun 17th 2024, 2:53:19 PM MDT	2024-06-17T20:53:19Z sslSessionLog, tenant=Student01, applianceName=S01B01, srcPort=50318, destPort=443, inglf=vni-0/2.0, egrlf=vni-0/0.0, protocolId=6, fromZone=Intf-Student_LAN-Zone, fromUser=Unknown, toZone=Intf-INET-Zone, srcAddr=10.27.101.20, destAddr=104.154.89.105, obsTime=2024-06-17T20:53:18Z, txBytes=945, txPkts=9, rxBytes=5240, rxPkts=10, serverAddr=104.154.89.105, serverPort=443, domainName=expired.badssl.com, certIsSelfSigned=0, publicKeyLen=2048, eventType=end, actionType=SSL certificate expired, sslAction=reject, decryptProfileName=SSL-INSPECTION-DECRYPTION, policyRuleName=Inspect-All, policyAction=no-decrypt, proxyType=forward, flowKey=0x6670a2220100020003d8, clientAddr=10.27.101.20, clientPort=50318, rcvTimeSec=19, sessLenBkt=0, flowDuration=56

Showing 1 to 1 of 1 entries

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

Stateful Firewall

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:

- Configure standard stateful firewall policies
- Monitor and analyze stateful firewall features and functions

In this lab, you will be assigned a student ID (Student01, Student02, etc.) Each student environment is a tenant on Versa Director and has access to 2 VOS devices and a shared hub. You will perform your operations on the VOS devices.

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.

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:

In the following lab exercises, you will:

- Create stateful firewall rules that:
    - Block SSH sessions to public addresses
    - Block web sessions (http) to servers behind the hub site
    - Allow SSH sessions between LAN networks
    - Allow Internet access to LAN networks

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.

Refer to the Lab Access lab guide for instructions on how to connect to the lab environment and access Versa Director.

Step 2.1: Reset the lab to a base configuration

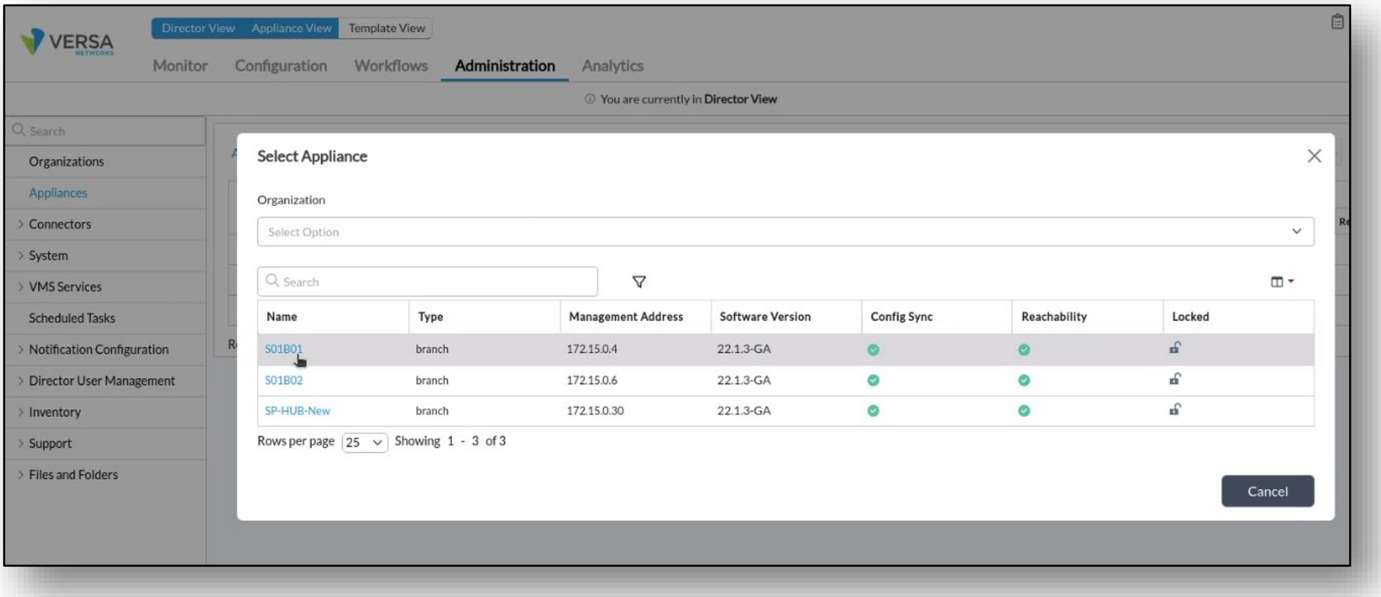
In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the workflow to your branch device. In the Basic tab, ensure that the device is assigned to the DG-SFW device group. If you need to change the device group assigned to your branch device, be sure to click Redeploy to apply the changes to the device in Versa Director.

Click the *Commit Template* link in the top-right corner of Versa Director, select your student ID as the tenant from the organization drop-down menu, select the *Template-SFW* from the *Select Template* menu, then click the Fetch Devices button to display devices associated with the template. Check the box next to your B01 branch device, and click *Review and then Deploy* to overwrite the configuration on the device with the SFW configuration.

Exercise 2:

Step 2.1:

Navigate to the Administration dashboard and open Appliances. Locate your device in the appliance table and click your device name to open the Appliance Context mode of your branch device.



You are currently in Director View

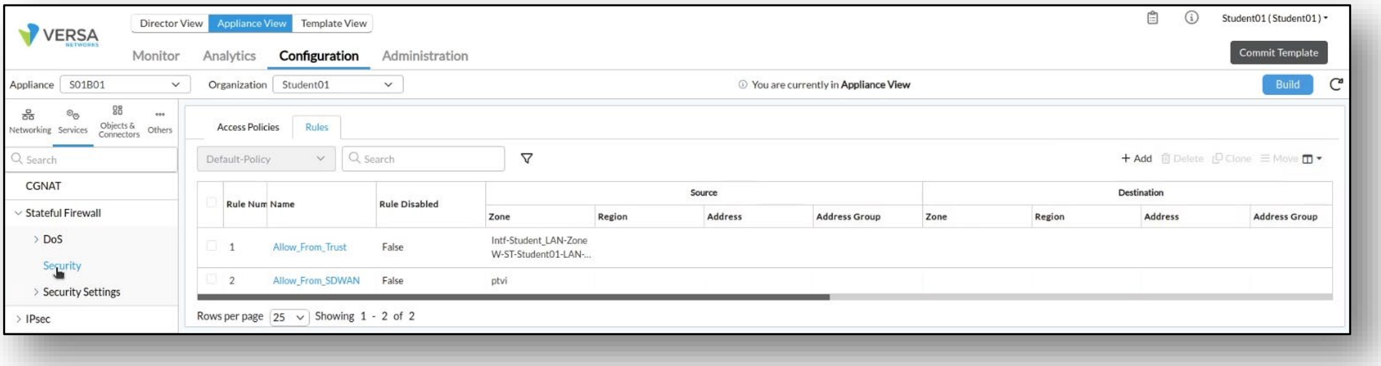
Select Appliance

Organization: Select Option

Name	Type	Management Address	Software Version	Config Sync	Reachability	Locked
S01B01	branch	172.15.0.4	22.1.3-GA	✓	✓	🔓
S01B02	branch	172.15.0.6	22.1.3-GA	✓	✓	🔓
SP-HUB-New	branch	172.15.0.30	22.1.3-GA	✓	✓	🔓

Rows per page 25 Showing 1 - 3 of 3

In the Appliance Context mode of your device, select the *Services* configuration tab to view the available services. You should see *Stateful Firewall* services in the configuration tab. Select *Security* under the Stateful Firewall service.



Appliance: S01B01 Organization: Student01

You are currently in Appliance View

Default-Policy

	Rule Num	Name	Rule Disabled	Source				Destination			
				Zone	Region	Address	Address Group	Zone	Region	Address	Address Group
□	1	Allow_From_Trust	False	Intf-Student_LAN-Zone W-ST-Student01-LAN-...							
□	2	Allow_From_SDWAN	False	ptvi							

Rows per page 25 Showing 1 - 2 of 2

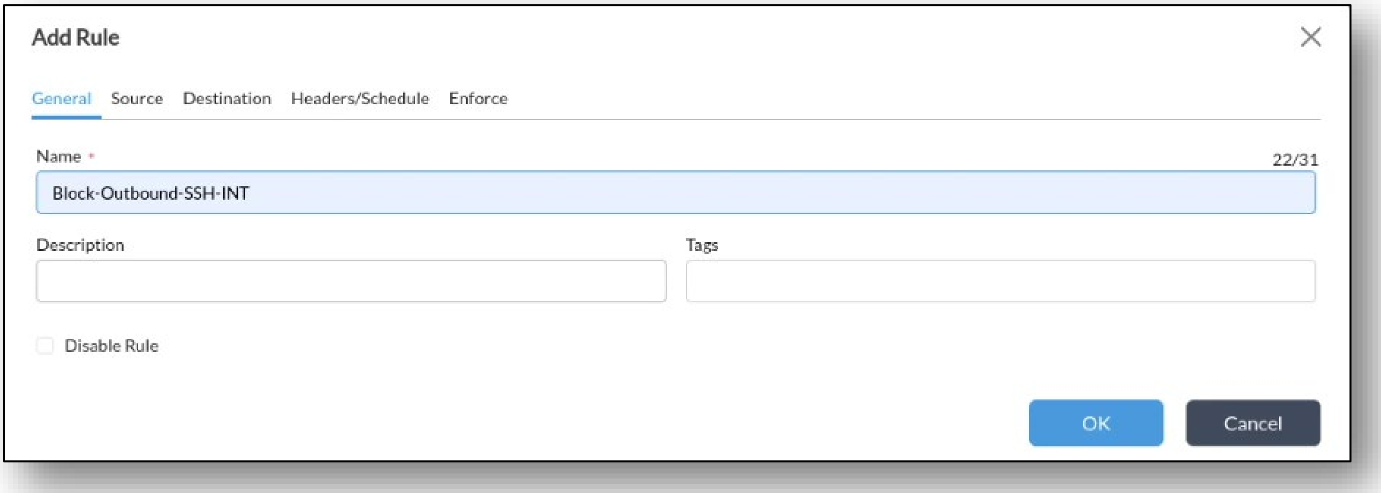
In the following lab steps you will:

- Create 5 Stateful Firewall rules in Appliance Context mode
- Verify that the stateful firewall rules are applied

Click the + button to add a new security rule that matches the following example:

Rule 1:

Security Rule 1 will block outbound SSH sessions from the Tenant LAN network to the Internet, and will log attempted sessions.

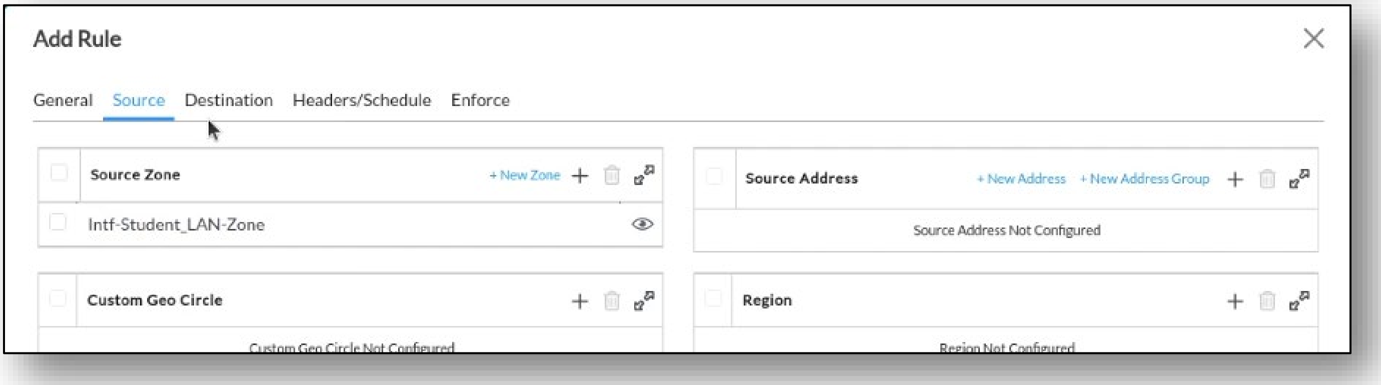


Name * 22/31
Block-Outbound-SSH-INT

Description

Tags

□ Disable Rule

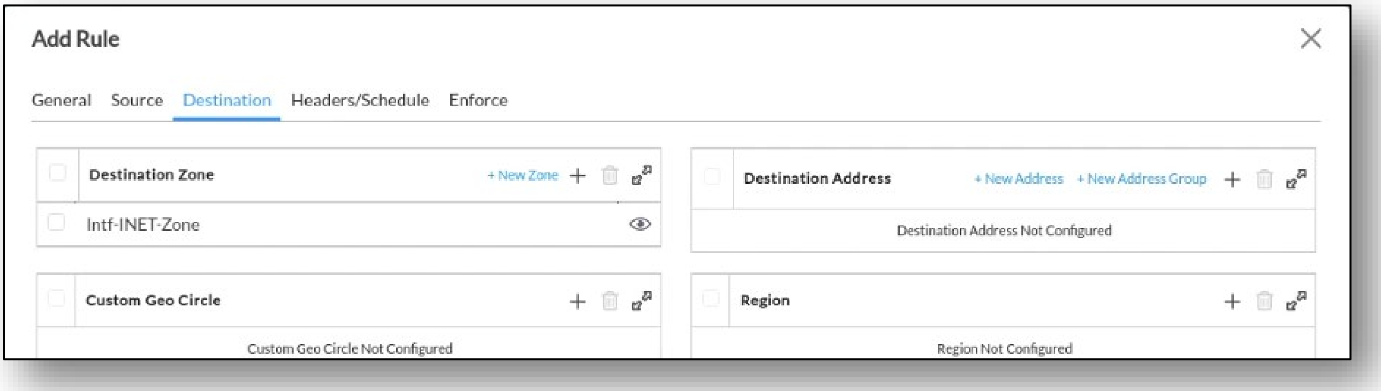


Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Custom Geo Circle
Custom Geo Circle Not Configured

Region
Region Not Configured

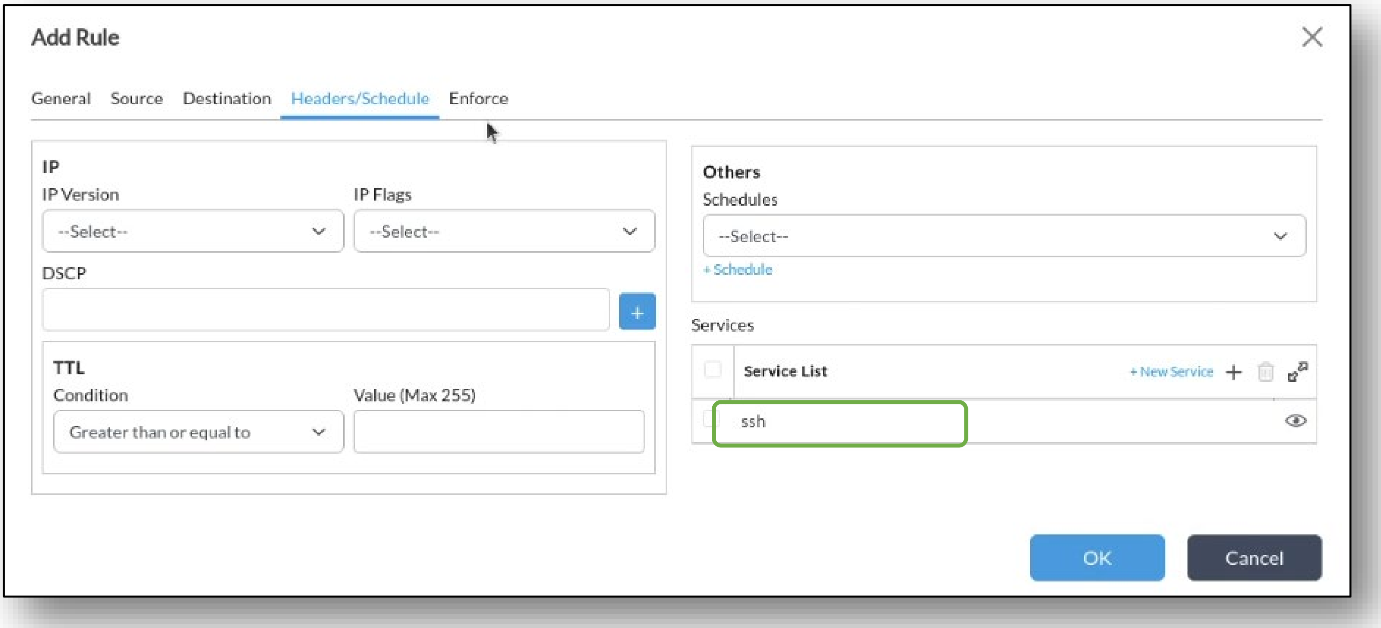


Destination Zone
Intf-INET-Zone

Destination Address
Destination Address Not Configured

Custom Geo Circle
Custom Geo Circle Not Configured

Region
Region Not Configured



Add Rule

General | Source | Destination | Headers/Schedule | Enforce

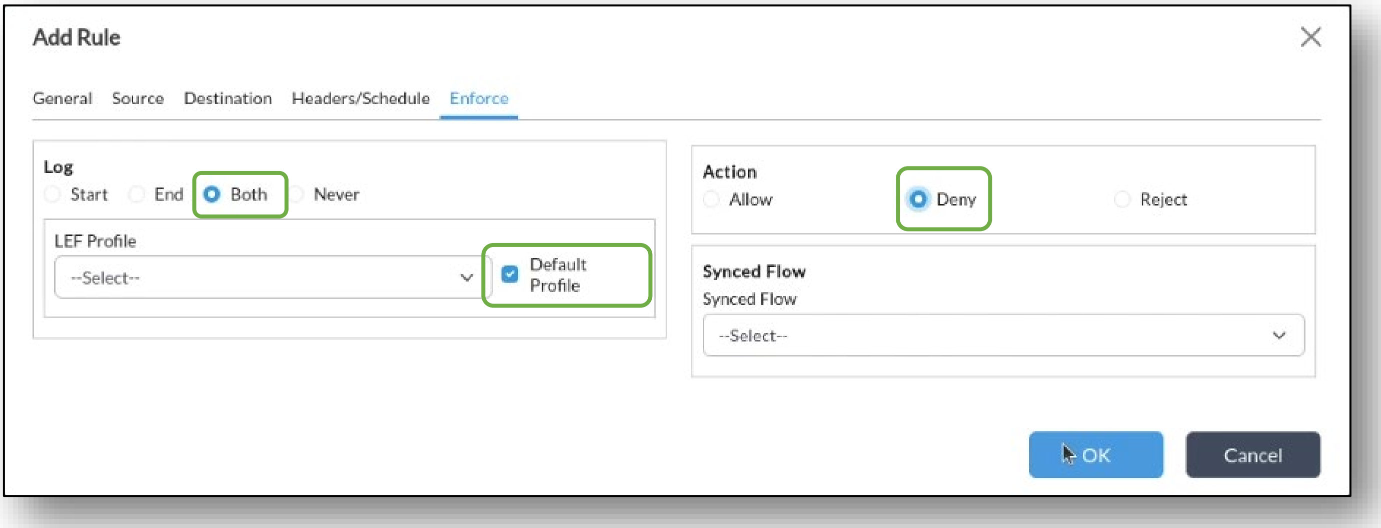
IP
IP Version: --Select--
IP Flags: --Select--
DSCP:

TTL
Condition: Greater than or equal to
Value (Max 255):

Others
Schedules: --Select--
+ Schedule

Services
□ Service List + New Service
□ ssh

OK | Cancel



Add Rule

General | Source | Destination | Headers/Schedule | Enforce

Log
○ Start ○ End ● Both ○ Never

LEF Profile: --Select--
☑ Default Profile

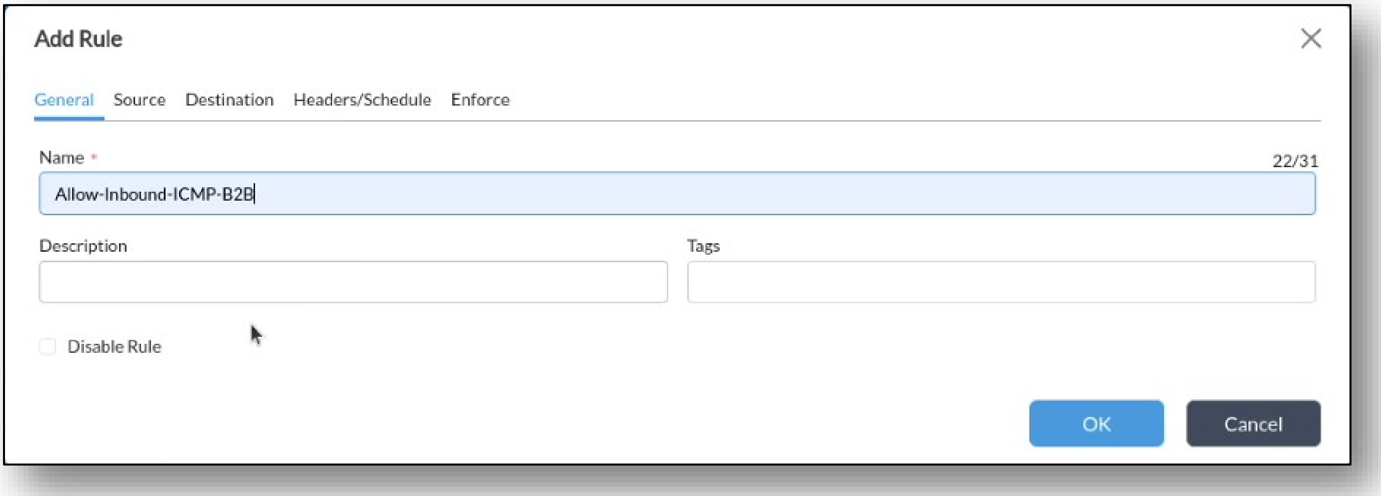
Action
○ Allow ● Deny ○ Reject

Synced Flow
Synced Flow: --Select--

OK | Cancel

Rule 2

Security Rule 2 will allow inbound branch-to-branch ICMP communication. It does this by allowing ICMP traffic received on the ptvi zone (SD-WAN tunnels) to the local LAN zone.



Add Rule

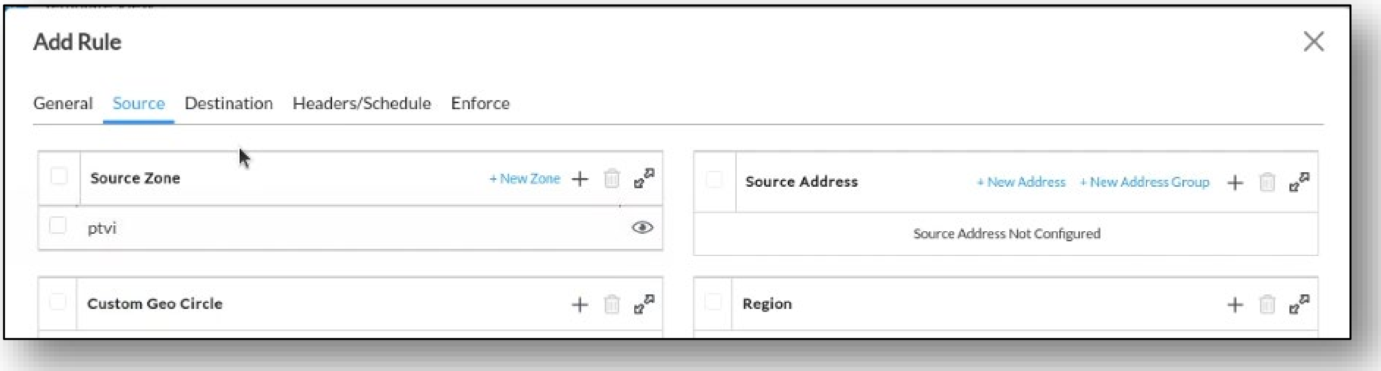
General | Source | Destination | Headers/Schedule | Enforce

Name * 22/31
Allow-Inbound-ICMP-B2B

Description

Tags

□ Disable Rule

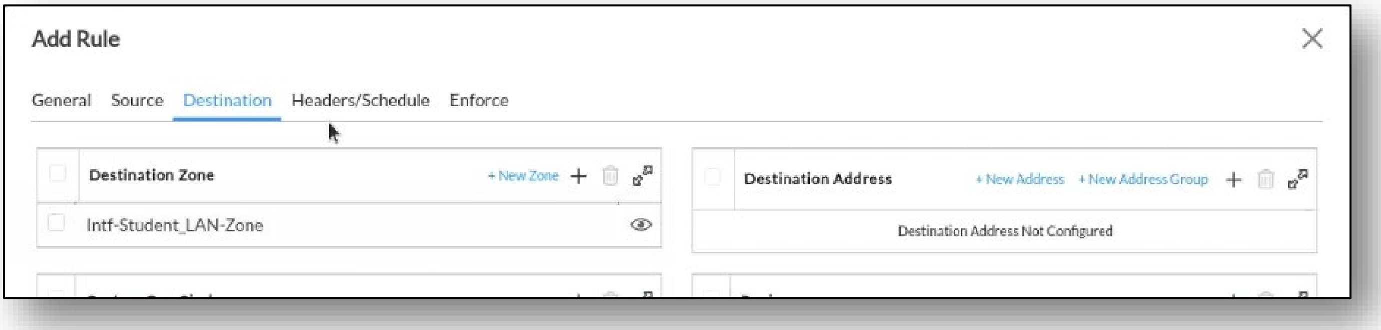


Add Rule

General | Source | Destination | Headers/Schedule | Enforce

Source Zone
ptvi

Source Address
Source Address Not Configured

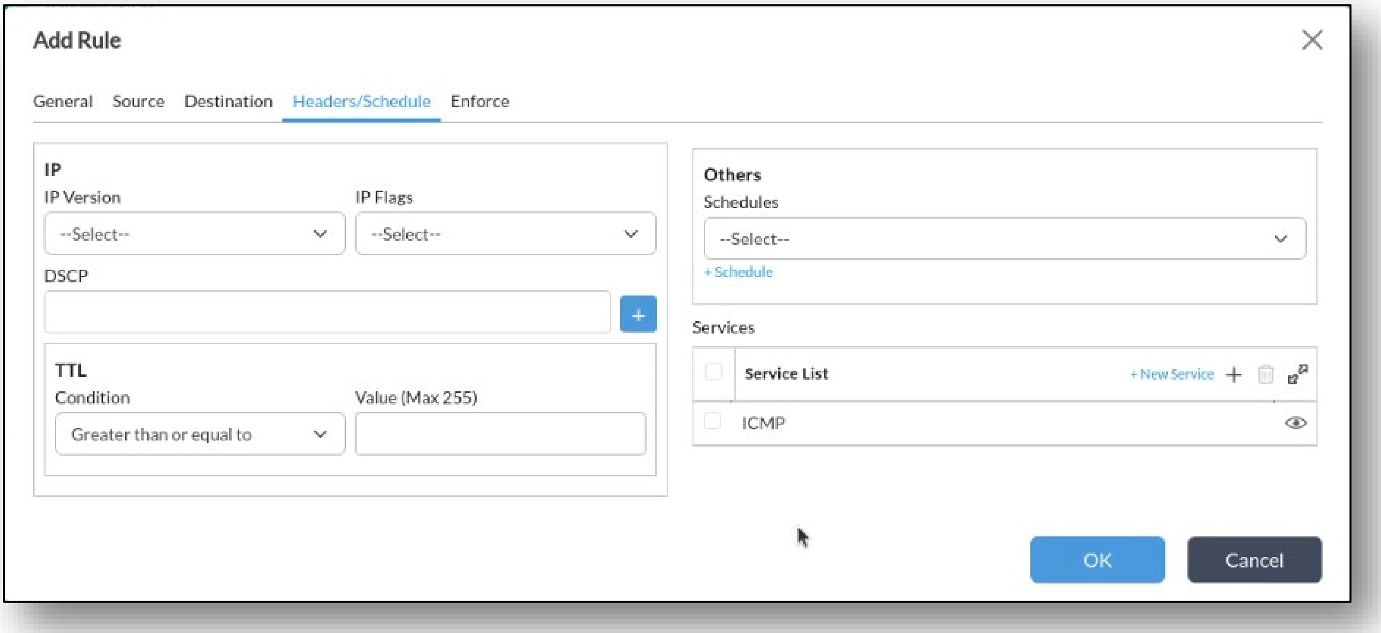


Add Rule

General | Source | Destination | Headers/Schedule | Enforce

Destination Zone
Intf-Student_LAN-Zone

Destination Address
Destination Address Not Configured



Add Rule

General | Source | Destination | Headers/Schedule | Enforce

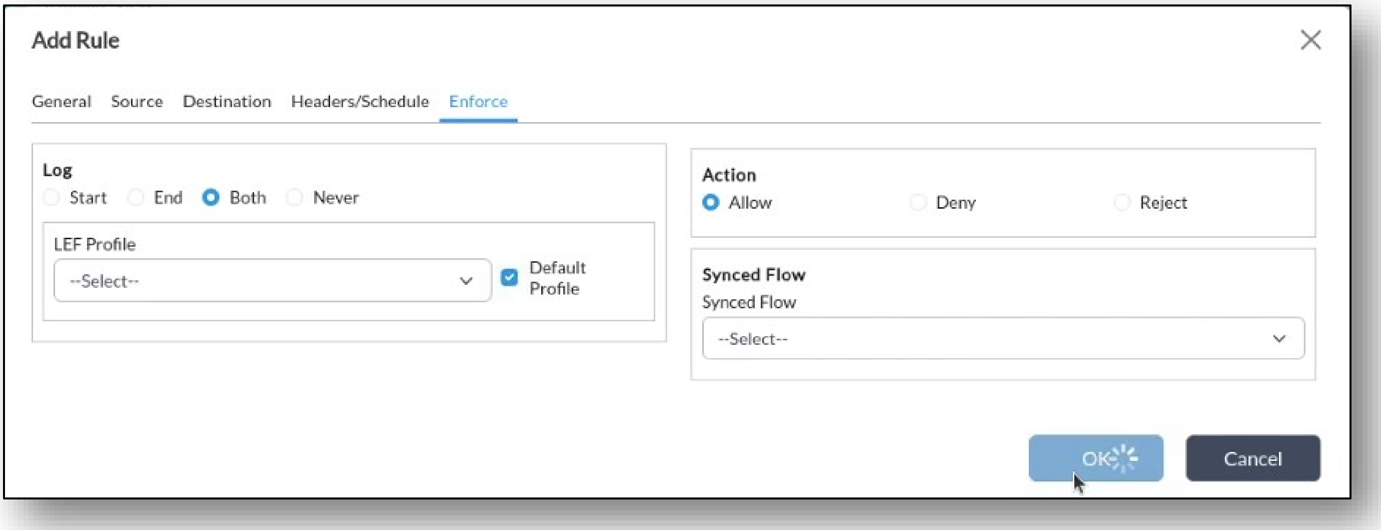
IP
IP Version: --Select--
IP Flags: --Select--
DSCP:

TTL
Condition: Greater than or equal to
Value (Max 255):

Others
Schedules: --Select--
+ Schedule

Services

□	Service List
□	ICMP



Add Rule

General | Source | Destination | Headers/Schedule | Enforce

Log
○ Start ○ End ● Both ○ Never

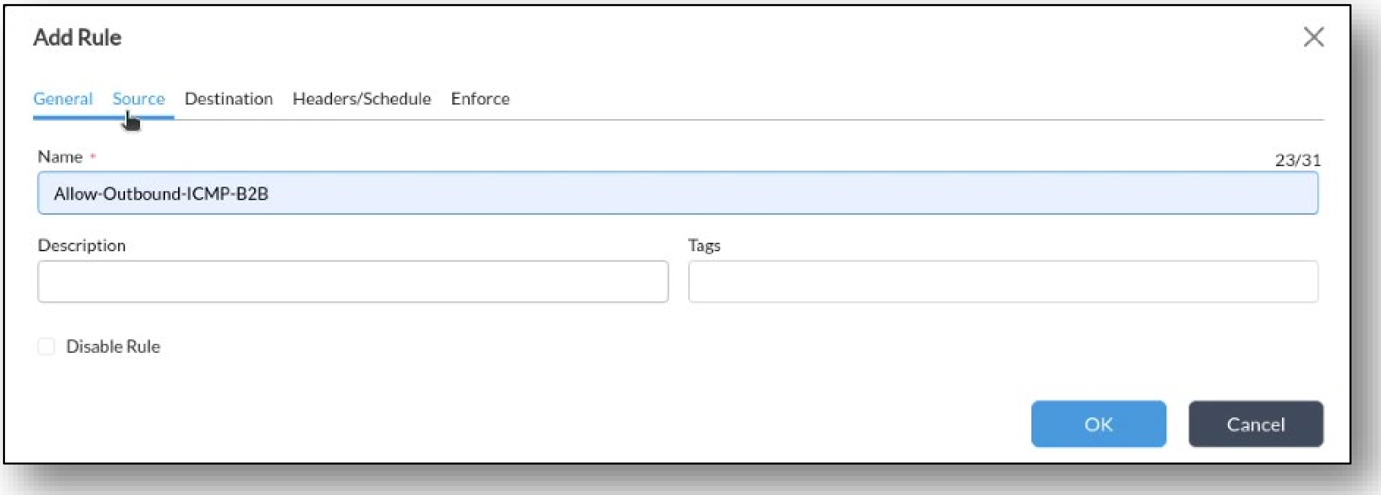
LEF Profile: --Select--
☑ Default Profile

Action
● Allow ○ Deny ○ Reject

Synced Flow
Synced Flow: --Select--

Rule 3

Security Rule 3 will allow outbound branch-to-branch ICMP communication. It does this by allowing ICMP traffic received on the local LAN zone to exit the ptvi (SD-WAN tunnels) zone.



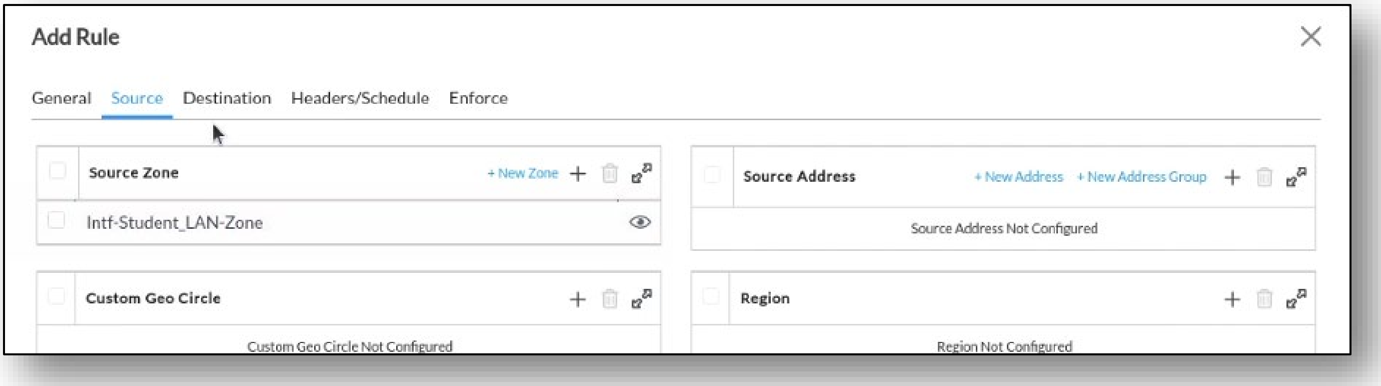
Add Rule

Name * 23/31
Allow-Outbound-ICMP-B2B

Description

Tags

□ Disable Rule



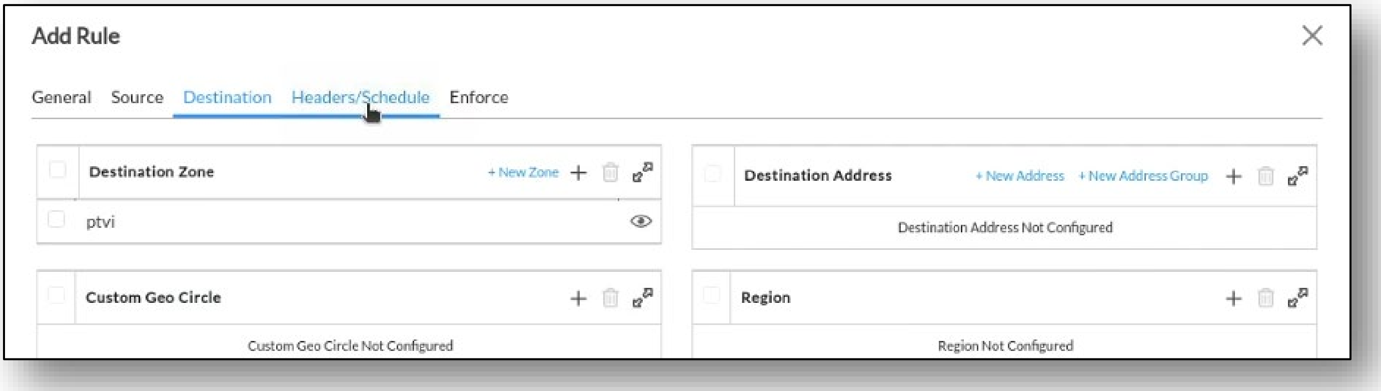
Add Rule

Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Custom Geo Circle
Custom Geo Circle Not Configured

Region
Region Not Configured



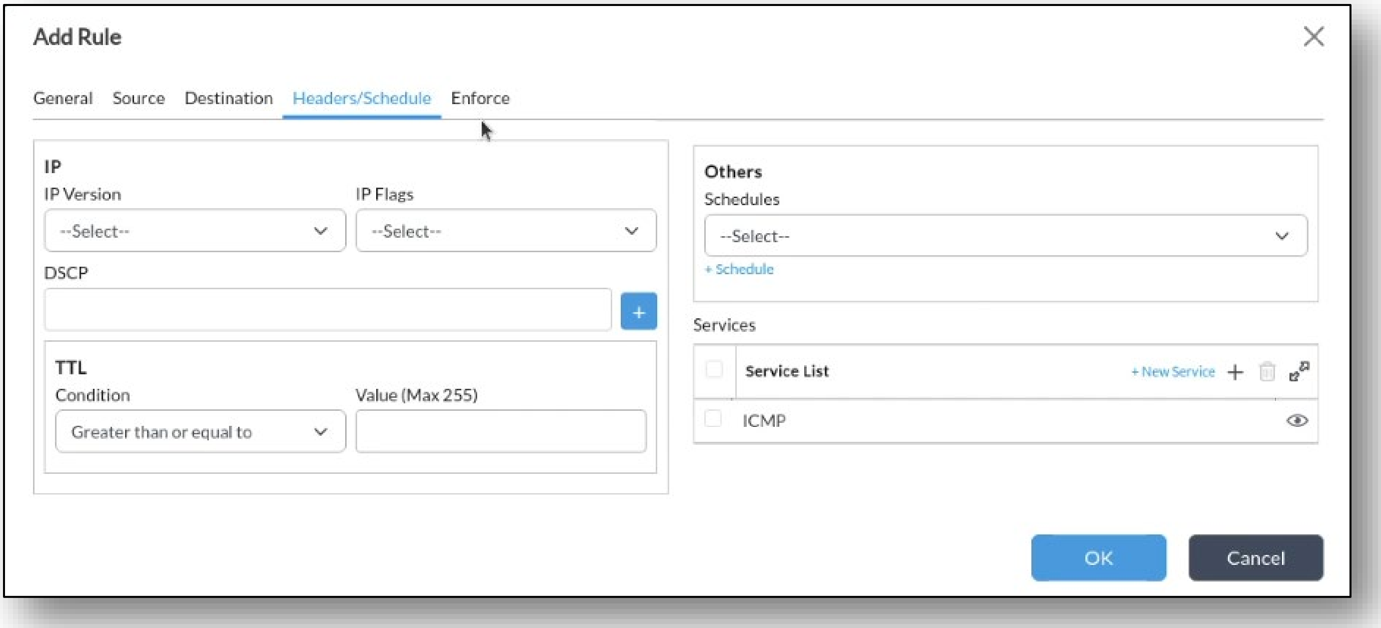
Add Rule

Destination Zone
ptvi

Destination Address
Destination Address Not Configured

Custom Geo Circle
Custom Geo Circle Not Configured

Region
Region Not Configured



Add Rule

IP

IP Version: --Select--

IP Flags: --Select--

DSCP:

TTL

Condition: Greater than or equal to

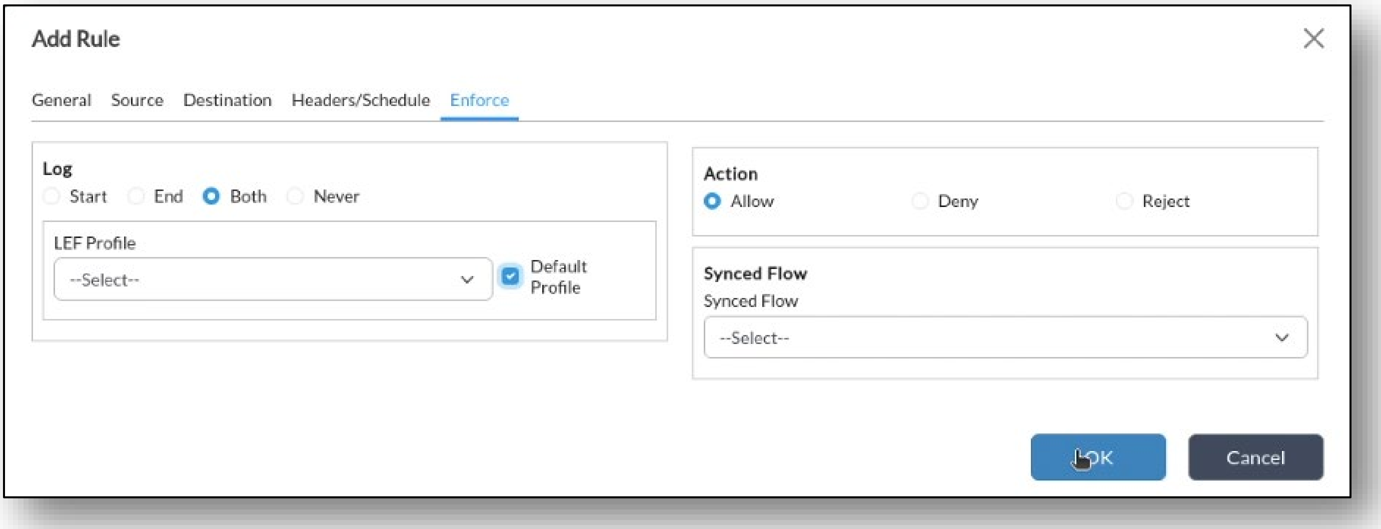
Value (Max 255):

Others

Schedules: --Select--

Services

□ Service List
□ ICMP



Add Rule

Log

○ Start ○ End ● Both ○ Never

LEF Profile: --Select-- ☑ Default Profile

Action

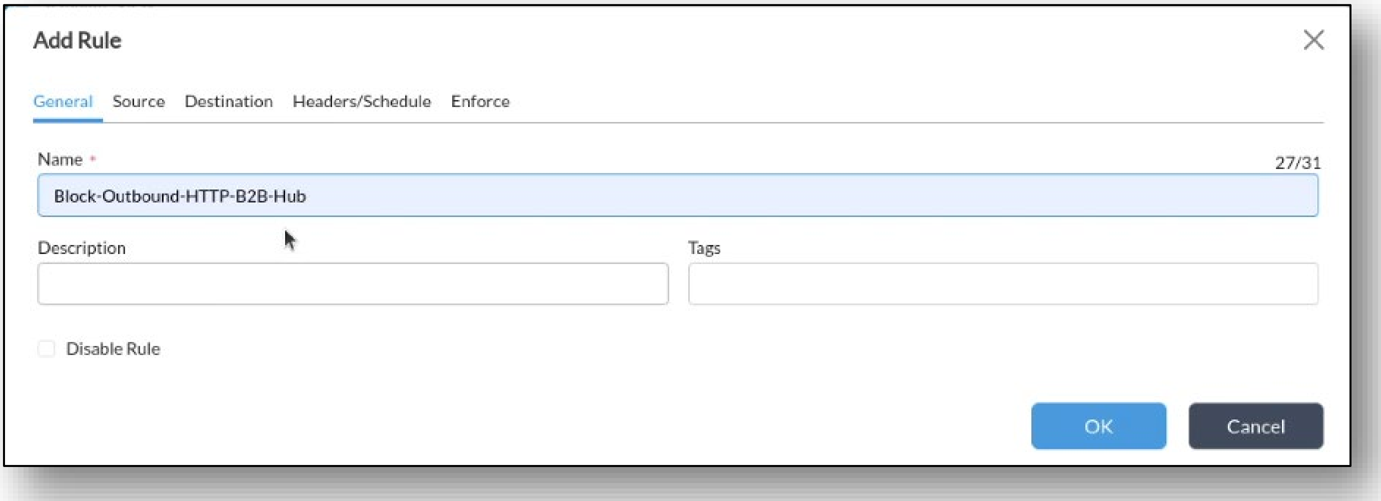
● Allow ○ Deny ○ Reject

Synced Flow

Synced Flow: --Select--

Rule 4

Security Rule 4 will block port 80 web traffic from the Local LAN to the web server connected to the hub site. To perform this task you will create a new address that matches the host device that is connected to the hub site and you will create a custom service to port 80.



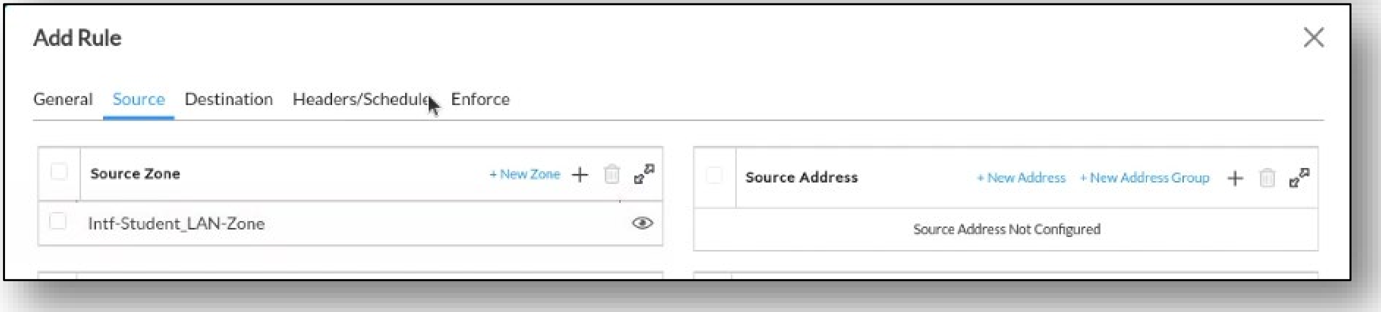
Add Rule

Name * 27/31
Block-Outbound-HTTP-B2B-Hub

Description

Tags

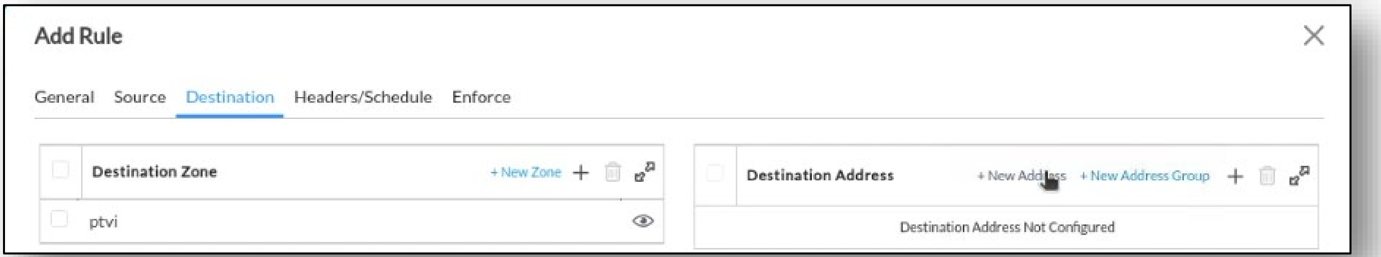
□ Disable Rule



Add Rule

□	Source Zone
□	Intf-Student_LAN-Zone

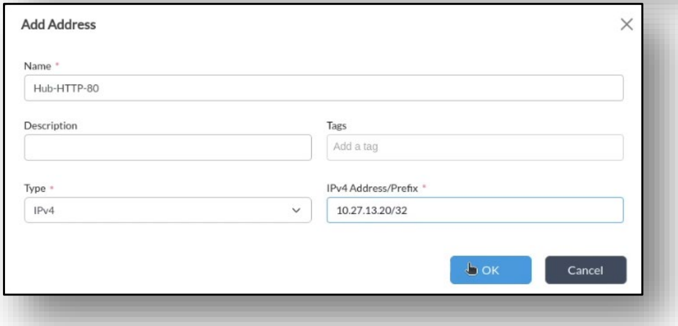
□	Source Address
	Source Address Not Configured



Add Rule

□	Destination Zone
□	ptvi

□	Destination Address
	Destination Address Not Configured



Add Address

Name *
Hub-HTTP-80

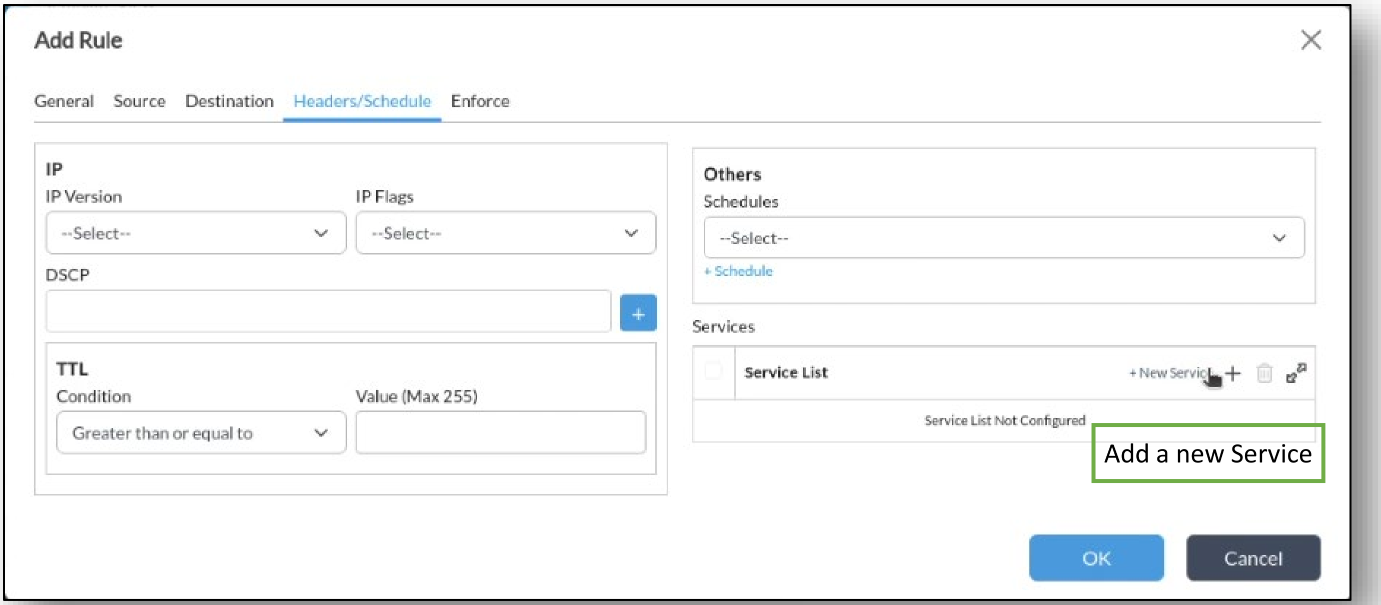
Description

Tags
Add a tag

Type *
IPv4

IPv4 Address/Prefix *
10.27.13.20/32

Create a New Address
Name: Hub-HTTP-80
Type: IPv4
Address: 10.27.13.20/32



Add Rule

General | Source | Destination | **Headers/Schedule** | Enforce

IP
IP Version: --Select--
IP Flags: --Select--
DSCP: +

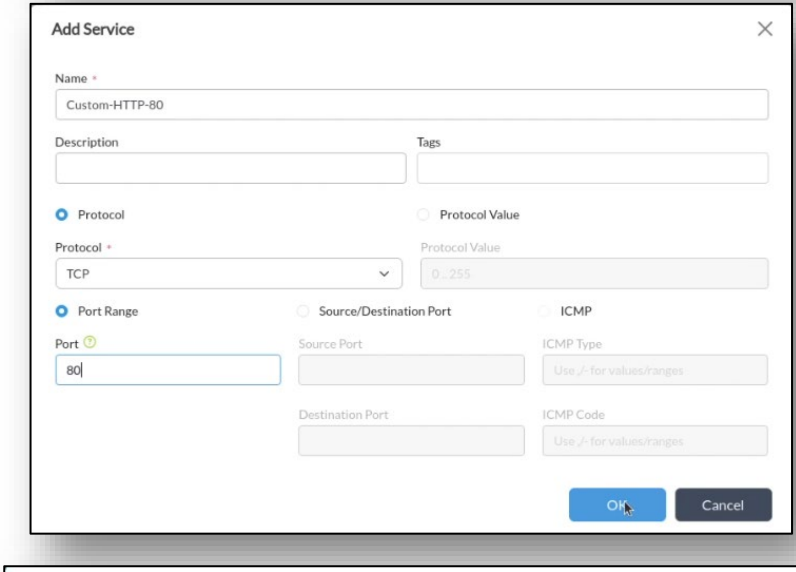
TTL
Condition: Greater than or equal to
Value (Max 255):

Others
Schedules: --Select--
+ Schedule

Services
Service List | + New Service
Service List Not Configured

Add a new Service

OK | Cancel



Add Service

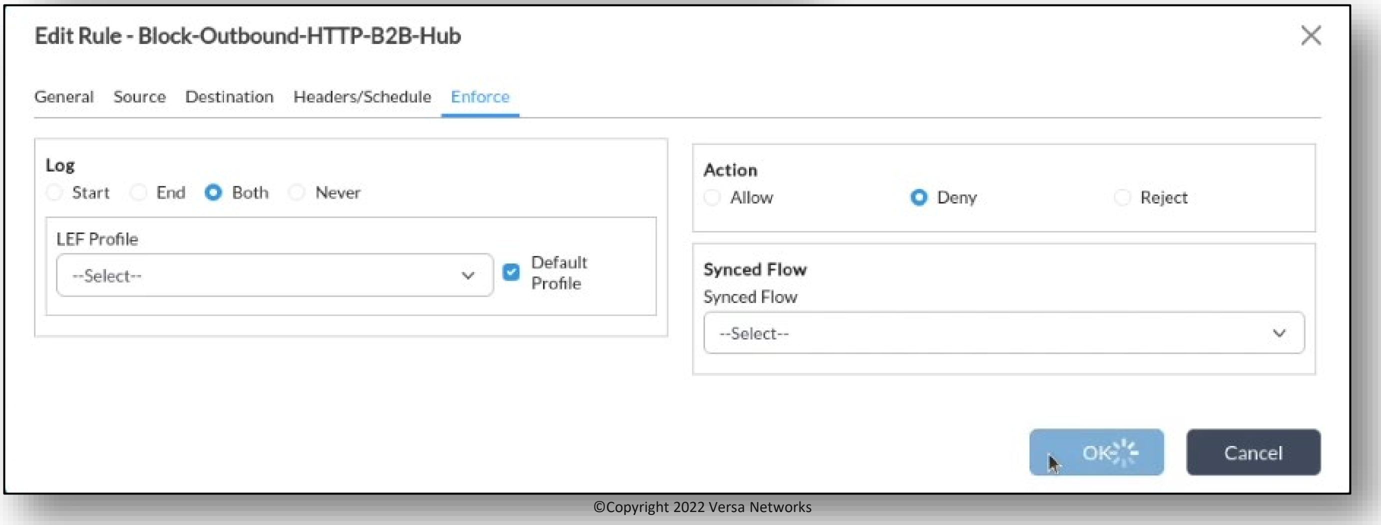
Name *: Custom-HTTP-80
Description:
Tags:

● Protocol ○ Protocol Value
Protocol *: TCP
Protocol Value: 0..255

● Port Range ○ Source/Destination Port ○ ICMP
Port: 80
Source Port:
ICMP Type: Use ,/- for values/ranges
Destination Port:
ICMP Code: Use ,/- for values/ranges

OK | Cancel

New Service: Custom-HTTP-80
Protocol: TCP
Port Range (Port): 80



Edit Rule - Block-Outbound-HTTP-B2B-Hub

General | Source | Destination | Headers/Schedule | **Enforce**

Log
○ Start ○ End ● Both ○ Never

LEF Profile: --Select--
☑ Default Profile

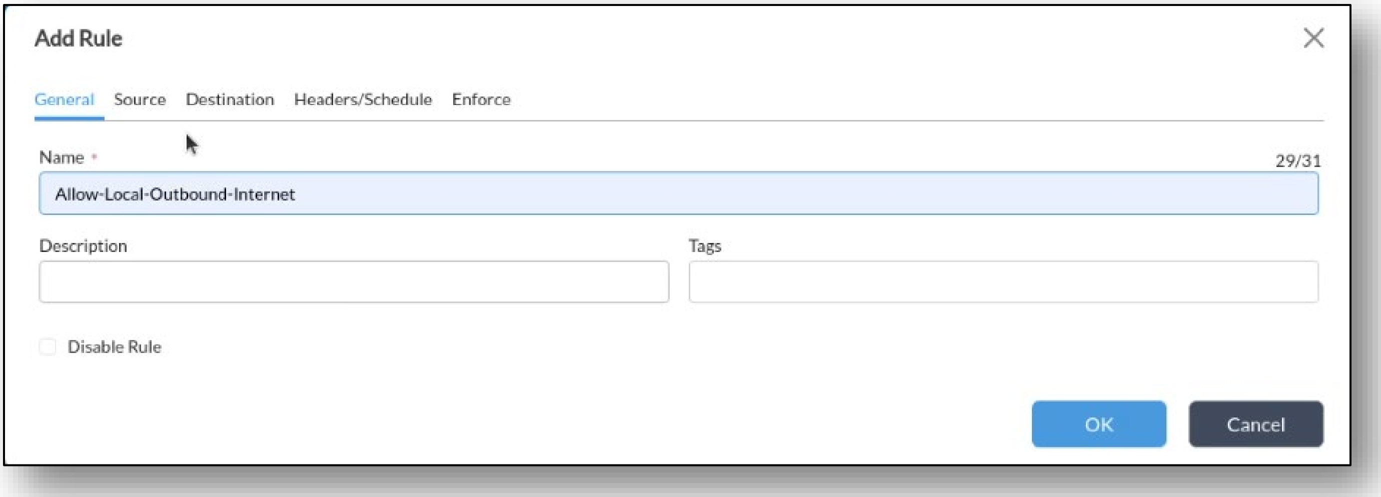
Action
○ Allow ● Deny ○ Reject

Synced Flow
Synced Flow: --Select--

OK | Cancel

Rule 5

Security Rule 5 will allow Internet access from the local LAN to the INET zone.

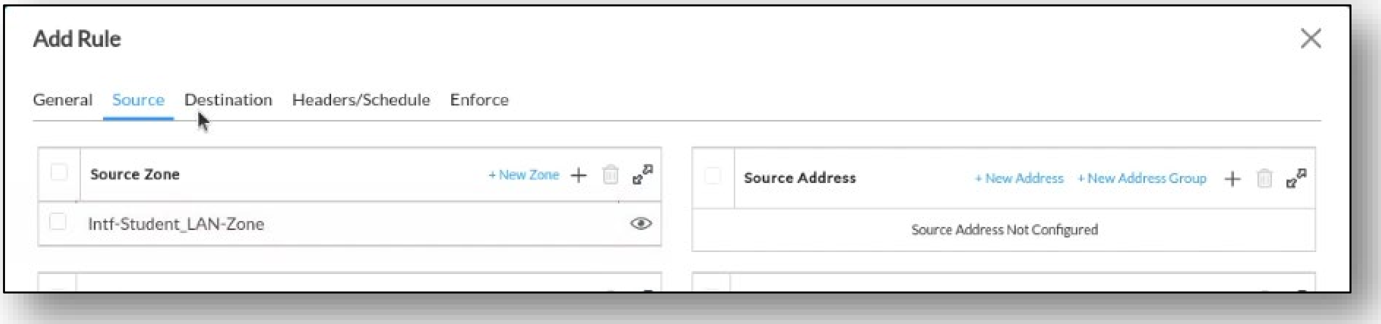


Name * 29/31
Allow-Local-Outbound-Internet

Description

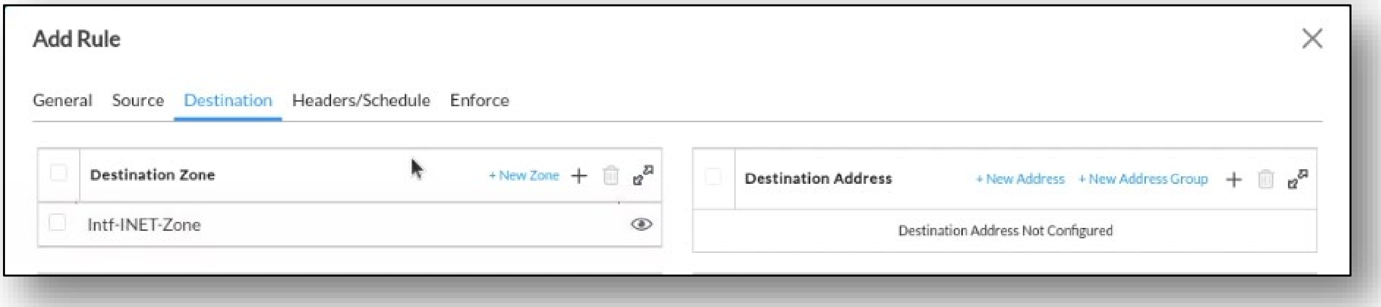
Tags

□ Disable Rule



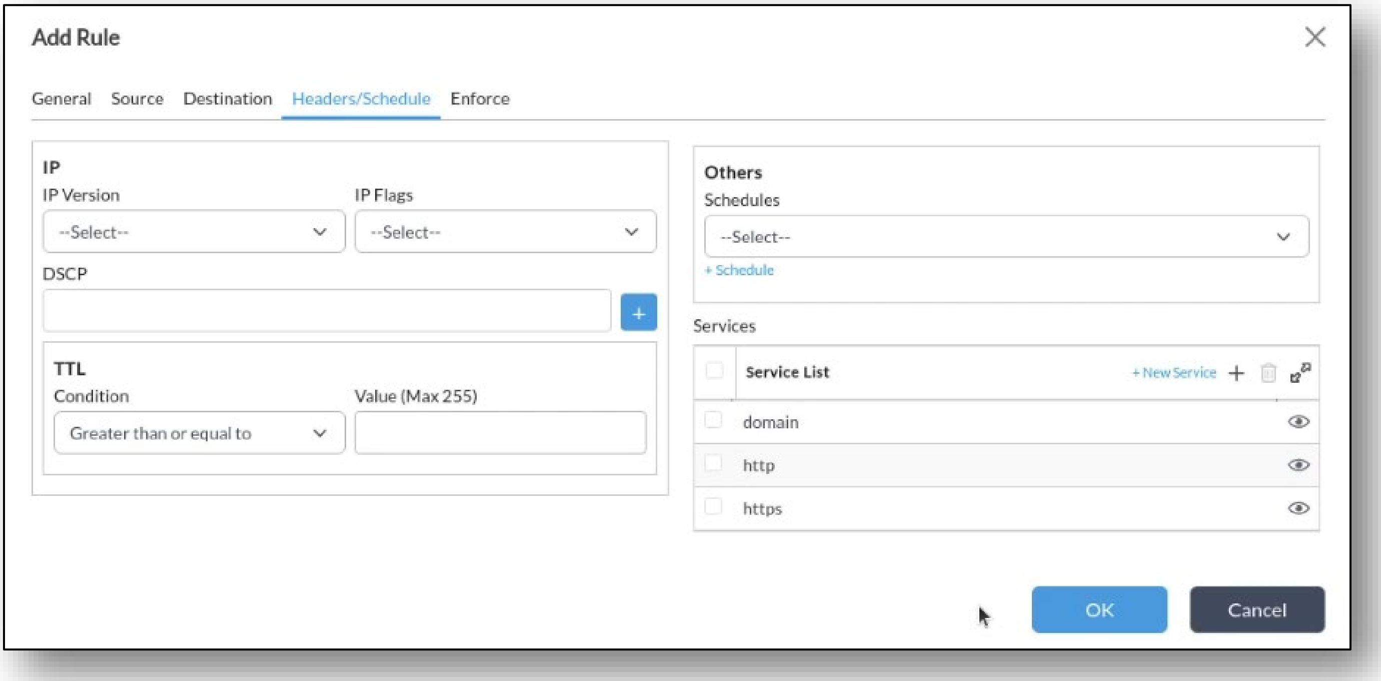
Source Zone
□ Intf-Student_LAN-Zone

Source Address
Source Address Not Configured



Destination Zone
□ Intf-INET-Zone

Destination Address
Destination Address Not Configured



Add Rule

General | Source | Destination | Headers/Schedule | Enforce

IP

IP Version: --Select--

IP Flags: --Select--

DSCP:

TTL

Condition: Greater than or equal to

Value (Max 255):

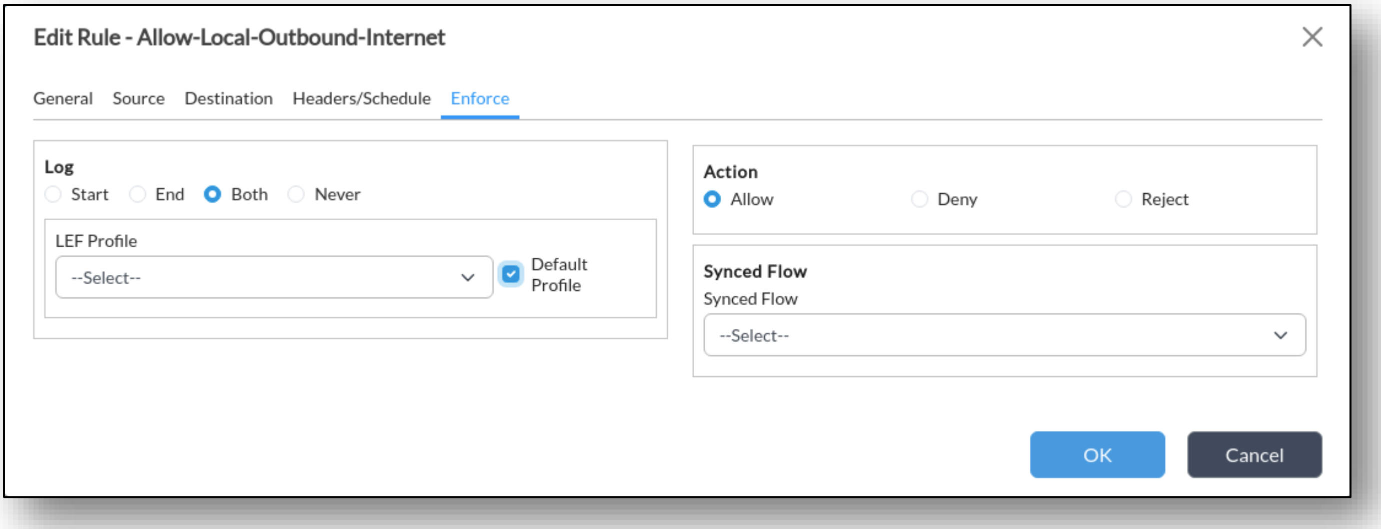
Others

Schedules: --Select--

+ Schedule

Services

□	Service List
□	domain
□	http
□	https



Edit Rule - Allow-Local-Outbound-Internet

General | Source | Destination | Headers/Schedule | Enforce

Log

○ Start ○ End ● Both ○ Never

LEF Profile: --Select-- ☑ Default Profile

Action

● Allow ○ Deny ○ Reject

Synced Flow

Synced Flow: --Select--

Next you will re-order the firewall rules. The rules should be applied in the following order:

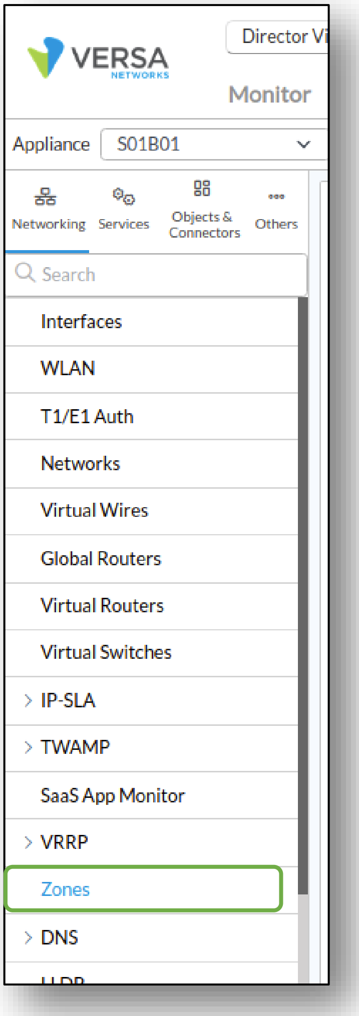
- Block-Outbond-SSH-INT
- Allow-Inbound-ICMP-B2B
- Allow-Outbound-ICMP-B2B
- Block-Outbound-HTTP-B2B
- Allow-Local-Outbound-Internet
- Allow_From_Trust
- Allow_From_SDWAN

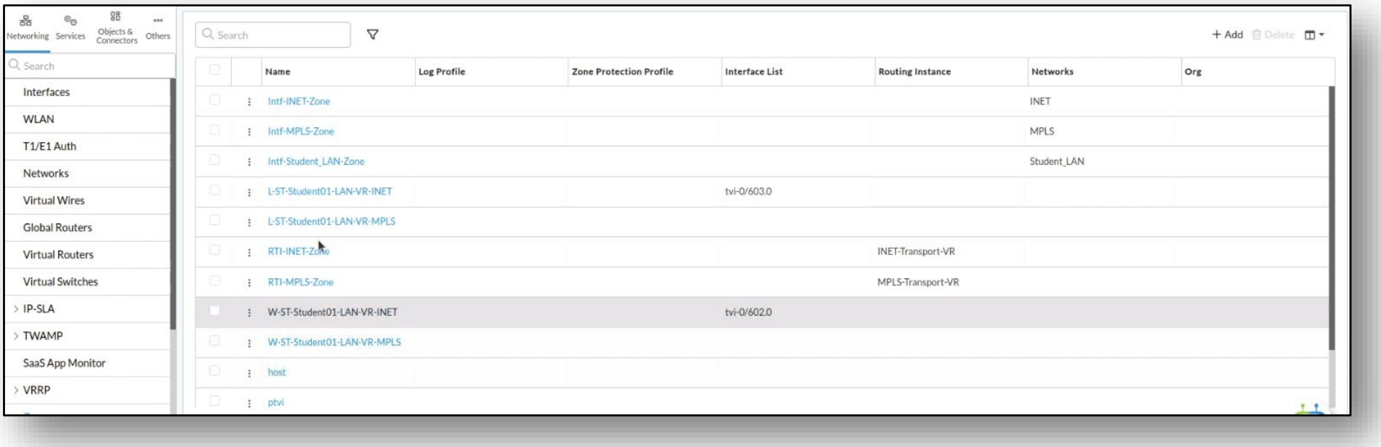
Exercise 2: Explore Network Zones

In the device configuration, navigate to the *Networking* > *Zones* hierarchy of your branch device.

The ptvi zones are default zones that are used for identifying traffic that is sent and received over SD-WAN tunnels. Because the tunnels are dynamically created and don't have the same interface name after reboots or interface flaps, the Versa Networks architecture uses the ptvi zone to identify all dynamic tunnels between branches and hubs. This zone does not include the host-bound traffic to head-end devices and no separate rule is required for head-end operations.

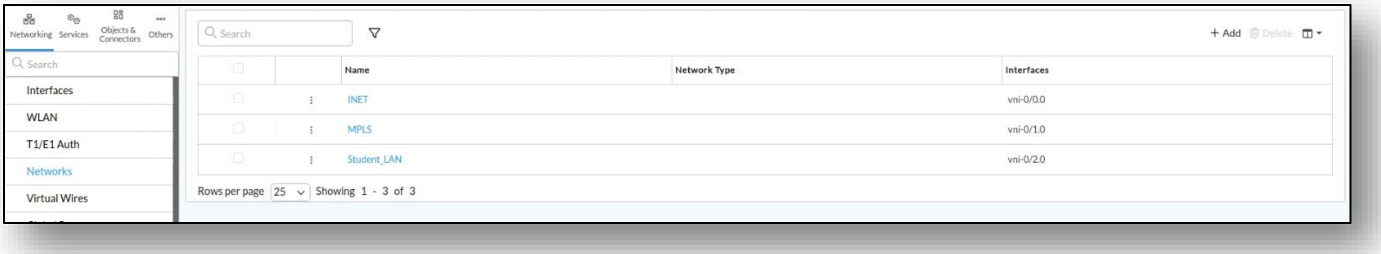
The Tenant LAN zone is associated with the local LAN assigned to a tenant. The Intf-INET-Zone and Intf-MPLS-Zone are associated with the INET network and MPLS network.





	Name	Log Profile	Zone Protection Profile	Interface List	Routing Instance	Networks	Org
☐	Intf-INET-Zone					INET	
☐	Intf-MPLS-Zone					MPLS	
☐	Intf-Student_LAN-Zone					Student_LAN	
☐	L-ST-Student01-LAN-VR-INET			tvi-0/603.0			
☐	L-ST-Student01-LAN-VR-MPLS						
☐	RTI-INET-Zone				INET-Transport-VR		
☐	RTI-MPLS-Zone				MPLS-Transport-VR		
☐	W-ST-Student01-LAN-VR-INET			tvi-0/602.0			
☐	W-ST-Student01-LAN-VR-MPLS						
☐	host						
☐	ptvi						

Click on Networks on the left to view the logical network and interface associations.



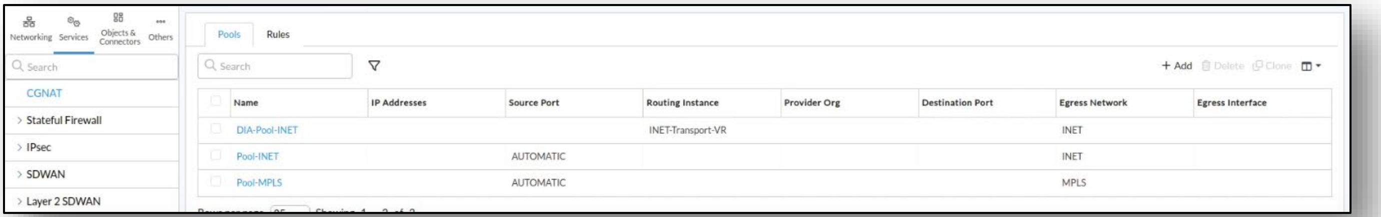
	Name	Network Type	Interfaces
☐	INET		vni-0/0.0
☐	MPLS		vni-0/1.0
☐	Student_LAN		vni-0/2.0

Rows per page 25 Showing 1 - 3 of 3

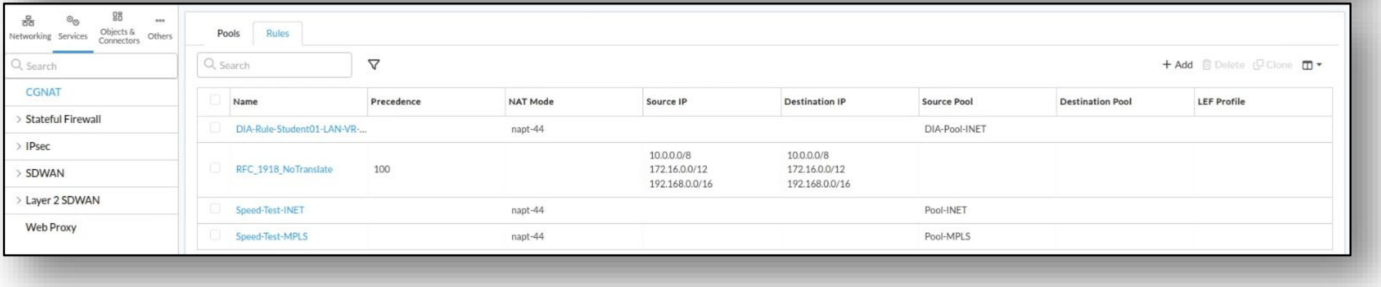
Next you will verify the NAT configuration that is automatically created when Direct Internet Access is enabled in the template workflow. The DIA function creates a logical link between the virtual routers specified in the DIA configuration. A BGP session is automatically configured between the two virtual routers, and a default route is advertised from the transport VR to the LAN VR for non-SD-WAN destinations.

To view the NAT configuration navigate to the *Services > CGNAT* configuration hierarchy.

You should see 3 NAT pools and 4 NAT rules. One of the NAT rules is associated with the DIA connection and was automatically created when DIA is configured in the template workflow.



	Name	IP Addresses	Source Port	Routing Instance	Provider Org	Destination Port	Egress Network	Egress Interface
☐	DIA-Pool-INET			INET-Transport-VR			INET	
☐	Pool-INET		AUTOMATIC				INET	
☐	Pool-MPLS		AUTOMATIC				MPLS	



	Name	Precedence	NAT Mode	Source IP	Destination IP	Source Pool	Destination Pool	LEF Profile
☐	DIA-Rule-Student01-LAN-VR-...		napt-44			DIA-Pool-INET		
☐	RFC_1918_NoTranslate	100		10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16			
☐	Speed-Test-INET		napt-44			Pool-INET		
☐	Speed-Test-MPLS		napt-44			Pool-MPLS		

Exercise 5: Test the Security Rules

In this lab part you will generate traffic from the host device that is connected to your branch device. You will use the branch shell to run the test commands.

On your remote desktop, open the Remmina application. Use the Remmina application to open an SSH session to the Linux Testing Client associated with your branch. Use the username `student` and password `versa123` if prompted.

From the shell prompt on the Linux Testing Client, run the following tests for each security rule.

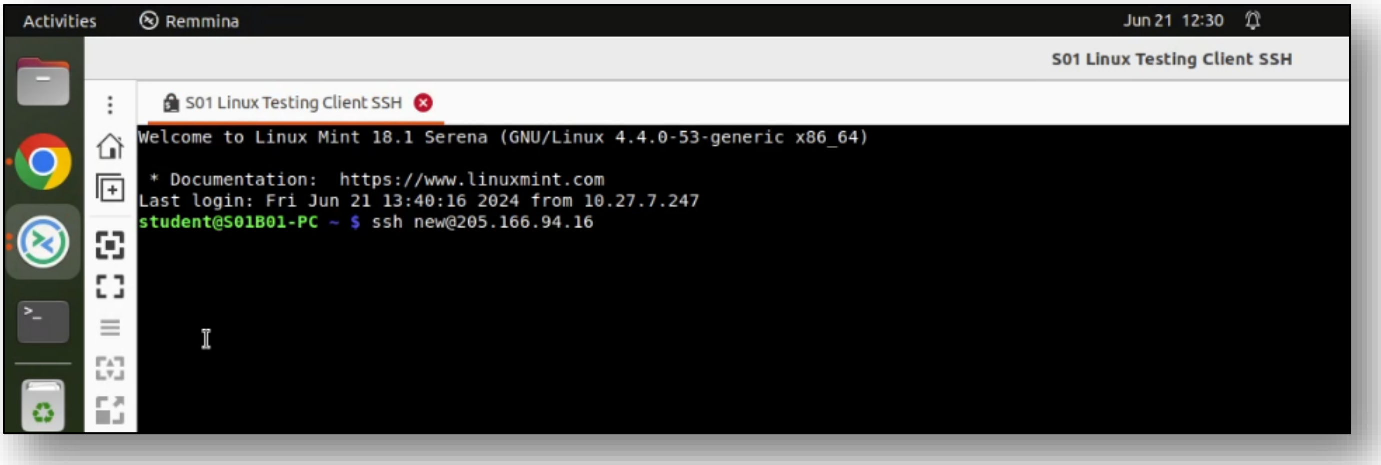
> **Note**: It can take several seconds for the counters to update during testing. To refresh the table counters, navigate to a different tab in the dashboard, then return to the tab where you are viewing the counters.

> **Note**: If you don't see log entries in Versa Analytics, ensure that you enabled the logging action in the Enforce tab of your security rules.

Rule 1 Test

Rule Name: Block-Outbound-SSH-INT
Actions: Deny

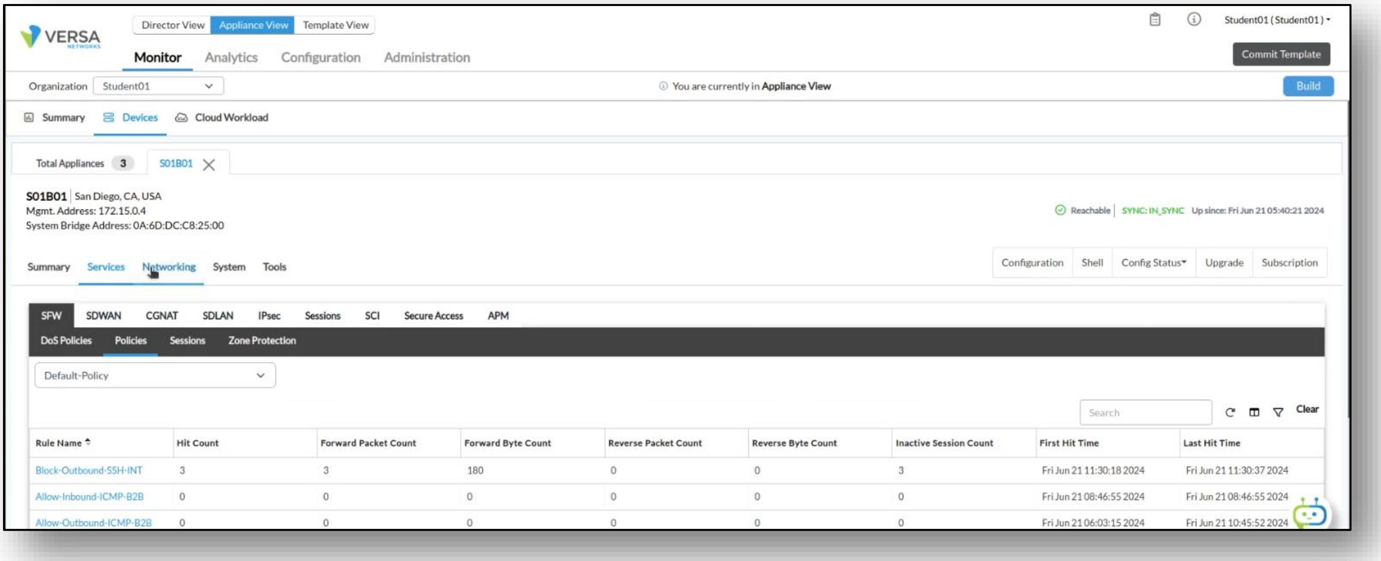
Test Procedure: From the Linux shell of the test PC issue the command **`ssh new@205.166.94.16`**
The command should fail.



```
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

 * Documentation:  https://www.linuxmint.com
Last login: Fri Jun 21 13:40:16 2024 from 10.27.7.247
student@S01B01-PC ~ $ ssh new@205.166.94.16
```

Monitor tab verification: From Versa Director, navigate to *Appliance View* and select your B01 appliance to open Appliance View. From the Appliance View Monitor dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created should be listed.



S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-Outbound-SSH-INT	3	3	180	0	0	3	Fri Jun 21 11:30:18 2024	Fri Jun 21 11:30:37 2024
Allow-Inbound-ICMP-B2B	0	0	0	0	0	0	Fri Jun 21 08:46:55 2024	Fri Jun 21 08:46:55 2024
Allow-Outbound-ICMP-B2B	0	0	0	0	0	0	Fri Jun 21 06:03:15 2024	Fri Jun 21 10:45:52 2024

Rule 2 and Rule 3 Test

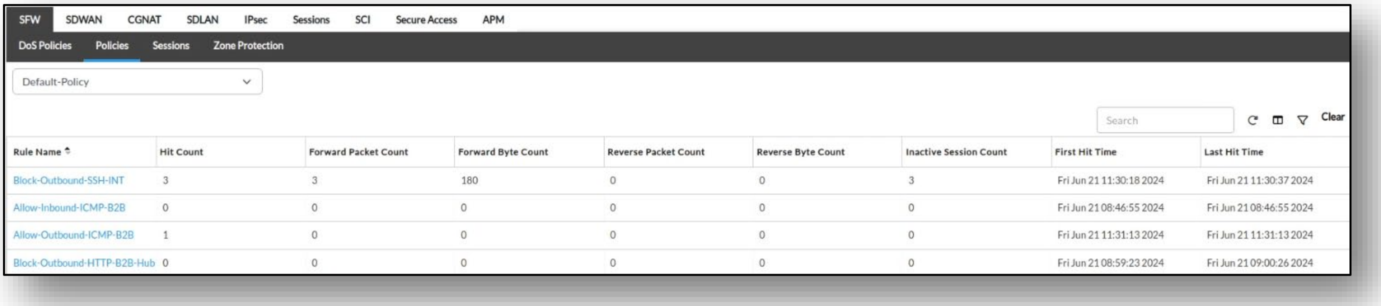
Rule Name: Allow-Inbound-ICMP-B2B and Allow-Outbound-ICMP-B2B

In this lab part you will generate traffic from the host device that is connected to your branch device. You will use the branch shell to run the test commands.

On your remote desktop, open the Remmina application. Use the Remmina application to open an SSH session to the test PC associated with your branch. If prompted, use the username *`student`* and password *`versa123`* to login. From the shell prompt on the testing PC, run the following command: **`ping 10.27.13.20 –c 5`** to initiate ICMP traffic towards the hub LAN network. The command should be successful.

To verify the security rule, return to Versa Director and navigate to the appliance context mode of your device. In the *Monitor* tab of the appliance context mode select *Services > SFW > Policies* and select the *Default-Policy*.

Check the counters for the *Allow-Inbound-ICMP-B2B* rule. The counters should not increment. However, the *Allow-Outbound-ICMP-B2B* counters should increase.



Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-Outbound-SSH-INT	3	3	180	0	0	3	Fri Jun 21 11:30:18 2024	Fri Jun 21 11:30:37 2024
Allow-Inbound-ICMP-B2B	0	0	0	0	0	0	Fri Jun 21 08:46:55 2024	Fri Jun 21 08:46:55 2024
Allow-Outbound-ICMP-B2B	1	0	0	0	0	0	Fri Jun 21 11:31:13 2024	Fri Jun 21 11:31:13 2024
Block-Outbound-HTTP-B2B-Hub	0	0	0	0	0	0	Fri Jun 21 08:59:23 2024	Fri Jun 21 09:00:26 2024

Using the Remmina application, open an SSH session to your B02 VOS device. On the B02 device, type *cli* to start the command line interface. From the B02 VOS device CLI, run the command in the table below that is associated with your branch to generate packets from the B02 branch to the B01 branch:

Branch	Command
01	ping 10.27.101.20 routing-instance Student01-LAN-VR count 5
02	ping 10.27.103.20 routing-instance Student02-LAN-VR count 5
03	ping 10.27.105.20 routing-instance Student03-LAN-VR count 5
04	ping 10.27.107.20 routing-instance Student04-LAN-VR count 5
05	ping 10.27.109.20 routing-instance Student05-LAN-VR count 5
06	ping 10.27.111.20 routing-instance Student06-LAN-VR count 5
07	ping 10.27.113.20 routing-instance Student07-LAN-VR count 5
08	ping 10.27.115.20 routing-instance Student08-LAN-VR count 5
09	ping 10.27.117.20 routing-instance Student09-LAN-VR count 5
10	ping 10.27.119.20 routing-instance Student10-LAN-VR count 5
11	ping 10.27.121.20 routing-instance Student11-LAN-VR count 5
12	ping 10.27.123.20 routing-instance Student12-LAN-VR count 5
13	ping 10.27.125.20 routing-instance Student13-LAN-VR count 5
14	ping 10.27.127.20 routing-instance Student14-LAN-VR count 5
15	ping 10.27.129.20 routing-instance Student15-LAN-VR count 5
16	ping 10.27.131.20 routing-instance Student16-LAN-VR count 5
17	ping 10.27.133.20 routing-instance Student17-LAN-VR count 5
18	ping 10.27.135.20 routing-instance Student18-LAN-VR count 5
19	ping 10.27.137.20 routing-instance Student19-LAN-VR count 5
20	ping 10.27.139.20 routing-instance Student20-LAN-VR count 5

The ping command should succeed.

Next you will verify the rule success using Versa Analytics.

Return to the Versa Director user interface. From the *Director View*, click on the *Analytics* tab to open the Versa Analytics dashboards.

From the left-side menu, select *Logs > Firewall*. You can filter more specific log entries by selecting the branch name from the drop-down menu as well.

Enter a filter based on the rule name and with the value Allow-Outbound-ICMP-B2B in the filter window. Verify that the action for the rule matches is allow.

Rule 4 Test

Rule Name: Block-Outbound-HTTP-B2B-Hub

On the remote landing station, use the Remmina application to open an RDP session to your Linux Testing Host.

Use the username *student* and password *versa123* if prompted. From the test host open the Chromium web Browser to open the browser window and enter the address **http://10.27.13.20**. The web page will not open because there is not a web server at that address. However, the policy in the VOS device should still intercept the attempt and block it.

Monitor tab verification

From Versa Director, navigate to the *Monitor* dashboard for your B01 appliance. From your appliance monitor dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created in previous steps should be listed. Check the counters for the Block-Outbound-HTTP-Hub rule. The counters should increment each time you attempt to establish the HTTP session.

Analytics Tab Verification

Click the Director View icon to return to the main Versa Director UI.

Click on the Analytics tab to open the Versa Analytics dashboards. From the left-side menu, select *Logs > Firewall*. You can filter more specific log entries by selecting the branch name from the dropdown menu as well.

Enter a filter based on the rule and with the value Block-Outbound-HTTP-B2B-HUB in the filter window. Verify that the action for the rule matches is Deny.

Rule 5 Test

Rule Name: Allow-Local-Outbound-Internet

On the remote landing station, return to the Remmina remote desktop session to the Linux testing client.

Use the username *student* and password *versa123* if prompted.

From the test host, open the Chromium web browser and navigate to the address https://google.com. The web page should open.

Monitor Tab Verification

Return to the Versa Director user interface. From Versa Director, navigate to the *Appliance View* and select your B01 appliance from the list. From your appliance monitor dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created in previous steps should be listed.

Check the counters for the Allow-Local-Outbound-Internet rule. The counters should increase when you access the web site. Apply a filter to search for the rule if necessary, as several log entries will have been created.

Versa Analytics Verification

Click the Director View icon to return to the main Versa Director UI.

Click on the Analytics tab to open the Versa Analytics dashboards. From the left-side menu, select *Logs > Firewall*. You can filter more specific log entries by selecting your branch name from the drop-down menu.

Enter a filter based on the rule and with the value Allow-Local-Outbound-Internet in the filter window. Verify that the action for the rule matches is Allow.

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

DoS Protection

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.

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!

Look for these hints to help you in the labs

Exercise 2:

In the following lab exercises, you will:

- Create baseline Denial of Service protection rules
- Test the Denial of Service protection rules

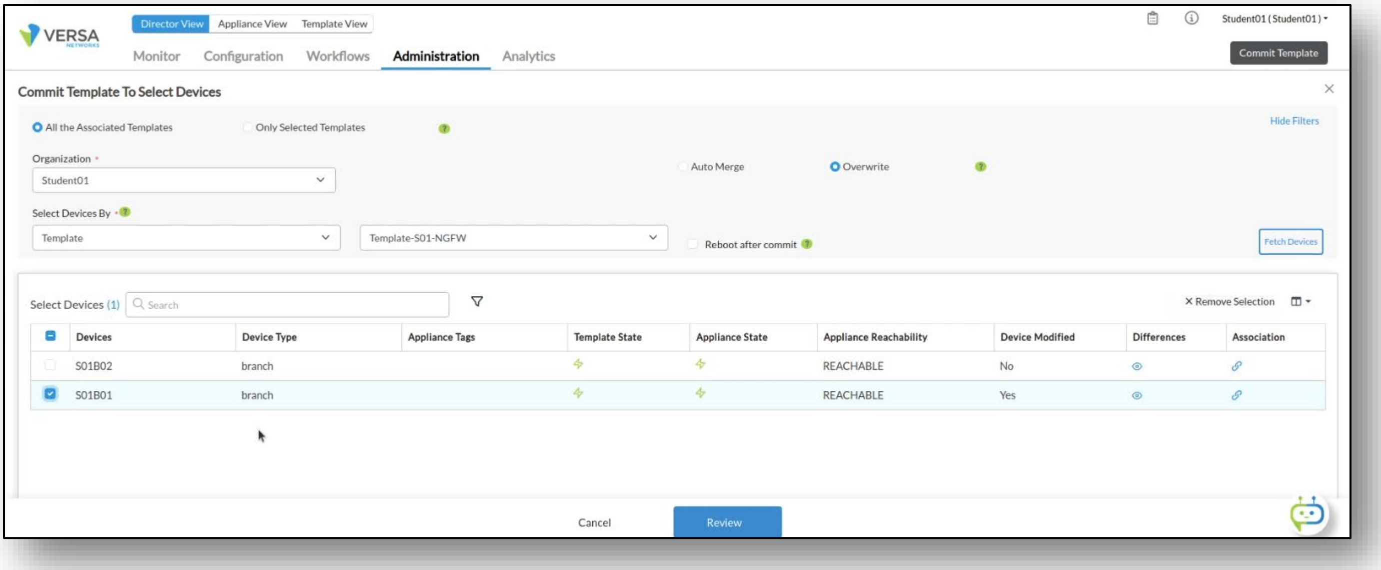
> **Note**: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

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

Step 2.1: Reset the lab to a base configuration

In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the workflow to your branch device. In the Basic tab, ensure that the device is assigned to the DG-NGFW device group. If you need to change the device group assigned to your branch device, be sure to click Redeploy to apply the changes to the device in Versa Director.

Click the *Commit Template* link in the top-right corner of Versa Director, select your student ID (tenant name) from the organization drop-down menu, select the *Template-Sxx-NGFW* from the *Select Template* menu, then click *Fetch Devices*. Check the box next to your B01 branch device, and click *Review,* then *Commit* to overwrite the configuration on the device with the Base-Template configuration.



Commit Template To Select Devices

● All the Associated Templates ○ Only Selected Templates

Organization *: Student01

○ Auto Merge ● Overwrite

Select Devices By *: Template | Template-S01-NGFW

□ Reboot after commit

Select Devices (1) Search

	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
□	S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
☑	S01B01	branch		⚡	⚡	REACHABLE	Yes	👁	🔗

Exercise 2:

2.1 Open the Device Template for Configuration

In the next steps you will configure thresholds for different protocols using DoS profiles. The DoS profiles will then be applied by assigning them as an action to a policy in later steps. This allows you to choose what DoS profile limits are applied to different types of traffic.

Navigate to the Configuration > Appliances workspace and locate your appliance in the table. Click on your appliance to open the Appliance Context mode for your appliance.

In the Appliance Context mode of your appliance, click on the Configuration tab to open the device configuration.

2.2 Create DoS Profiles

From the left-side menu, navigate to *Services > Next Gen Firewall > DoS > Profiles*.

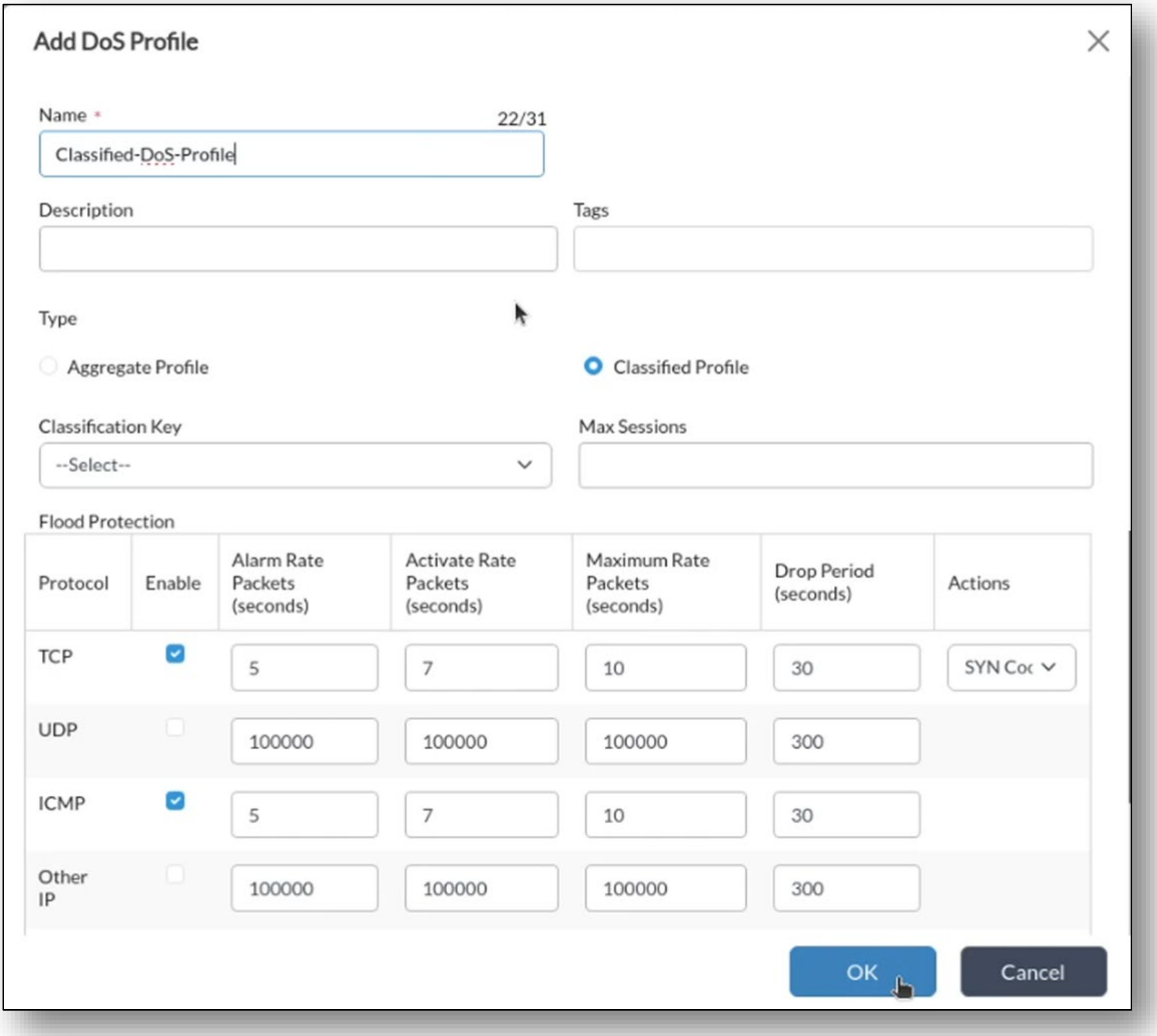
In the DoS Profiles dashboard click on the + button to create a new DoS profile.

In the DoS Profile dialog, enter the following parameters:

DoS Profile 1	
Profile Name:	Classified-DoS-Profile
Protection Options:	Enable ICMP and TCP
TCP Flood Thresholds:	Alarm Rate Packets/sec: 5 Active Rate Packets/sec: 7 Maximum Rate Packets/sec: 10 Drop Period Seconds: 30 Actions: SYN Cookies
ICMP Flood Thresholds:	Alarm Rate Packets/sec: 5 Active Rate Packets/sec: 7 Maximal Rate Packets/sec: 10 Drop Period Seconds: 30

Click OK to create the DoS profile when finished.

Sample DoS Profile



Name * 22/31
Classified-DoS-Profile

Description

Tags

Type

○ Aggregate Profile

● Classified Profile

Classification Key
--Select--

Max Sessions

Flood Protection

Protocol	Enable	Alarm Rate Packets (seconds)	Activate Rate Packets (seconds)	Maximum Rate Packets (seconds)	Drop Period (seconds)	Actions
TCP	☑	5	7	10	30	SYN Coo
UDP	□	100000	100000	100000	300	
ICMP	☑	5	7	10	30	
Other IP	□	100000	100000	100000	300	

2.3 Create a DoS Policy

You will now create a policy to identify traffic to which you want the profile thresholds applied. The policy will have the following rules:

- Restrict ICMP based flood attacks to the hub server 10.27.13.20 using the DoS Profile parameters
- Restrict TCP-SYN based attacks over port 80 to the hub server 10.27.13.20 using the DoS Profile created

In your device configuration (Appliance Context), navigate to *Services > Next Gen Firewall > DoS > Policies*. Unlike with security policies, a default DoS policy is not automatically created when the configuration is built by the workflow. In the Policies tab, click the + button to create a new DoS policy. Name the policy *DoS-Policy* and click *Ok*.

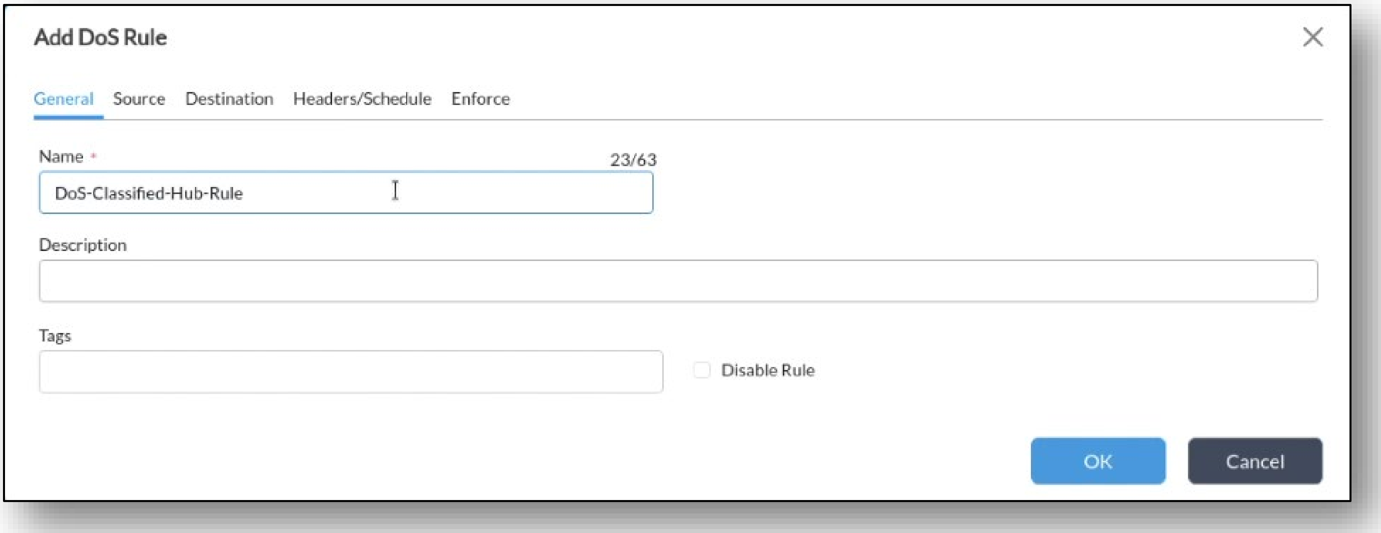
2.4 Create Rules in the DoS Policy

Navigate to the Rules tab to add rules to the DoS-Policy policy. Add the following rules:

Rule 1	
Rule Name:	DoS-Classified-Rule-Hub
Source/Destination Tab:	Source Zone:intf-Student_LAN-Zone Destination Zone: ptvi Add a new destination address: Address Name: HUB-HTTP-80 Address: IPv4 10.27.13.20/32
Headers/Schedule Tab:	Add services http and ICMP
Enforce Tab:	Action: Protect Classified Profile: Classified-DoS-Profile Logging: Default-Logging-Profile

Click *OK* to finish creating the policy.

Sample DoS-Classified-Hub-Rule

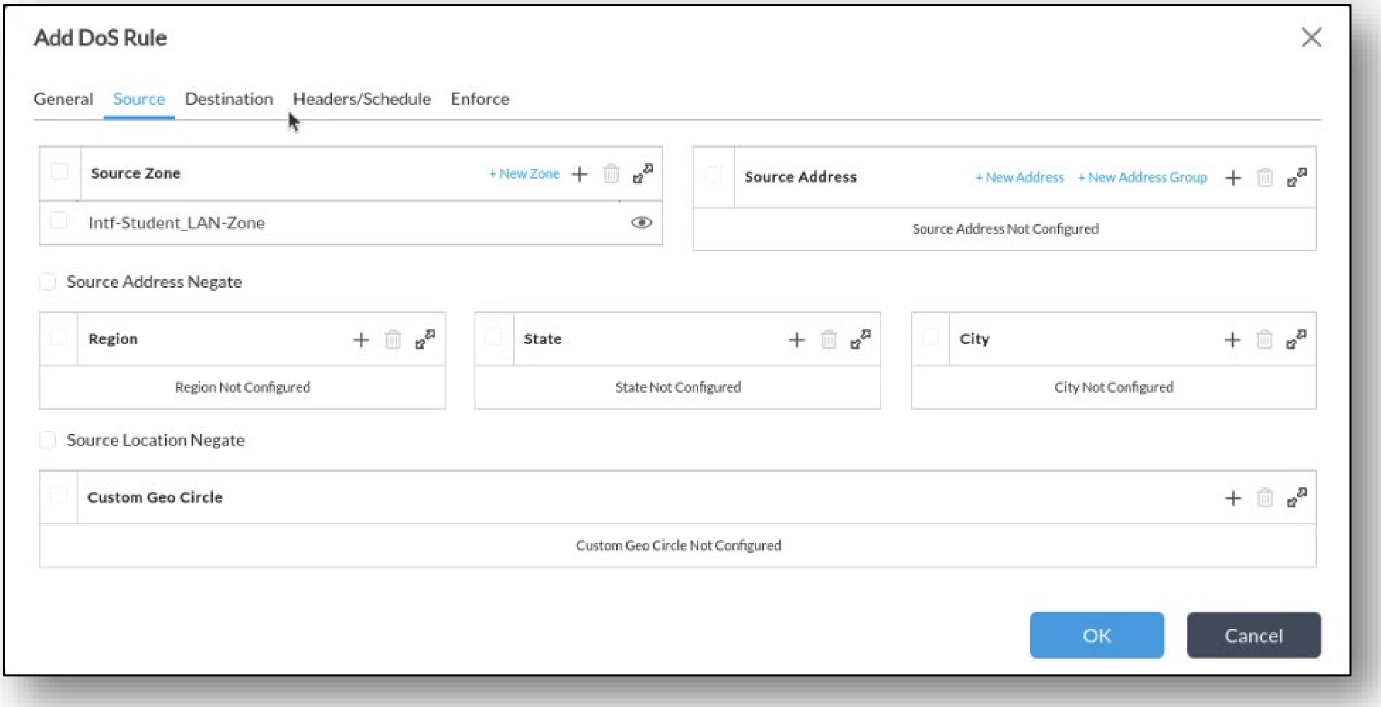

Add DoS Rule

Name * 23/63
DoS-Classified-Hub-Rule

Description

Tags

□ Disable Rule


Add DoS Rule

Source Zone
Intf-Student_LAN-Zone

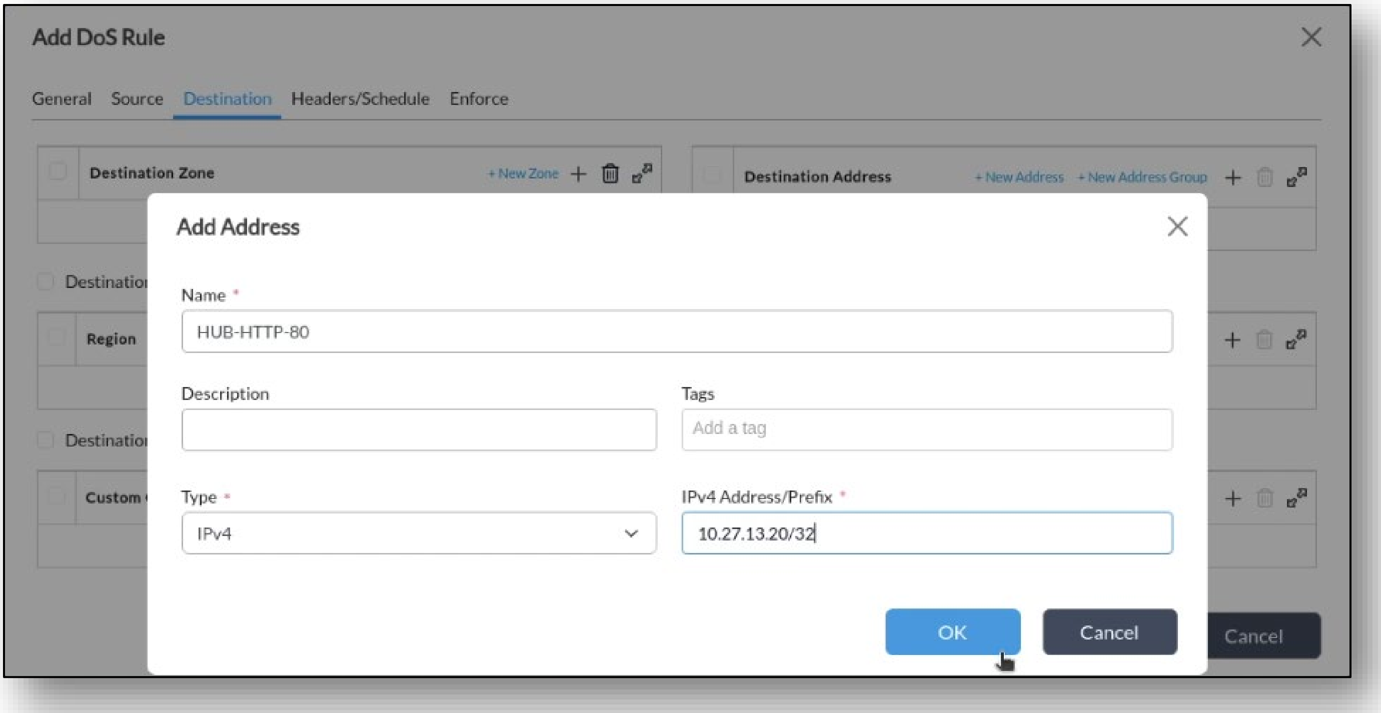
Source Address
Source Address Not Configured

□ Source Address Negate

Region	State	City
Region Not Configured	State Not Configured	City Not Configured

□ Source Location Negate

Custom Geo Circle
Custom Geo Circle Not Configured



Add DoS Rule

General | Source | Destination | Headers/Schedule | Enforce

Add Address

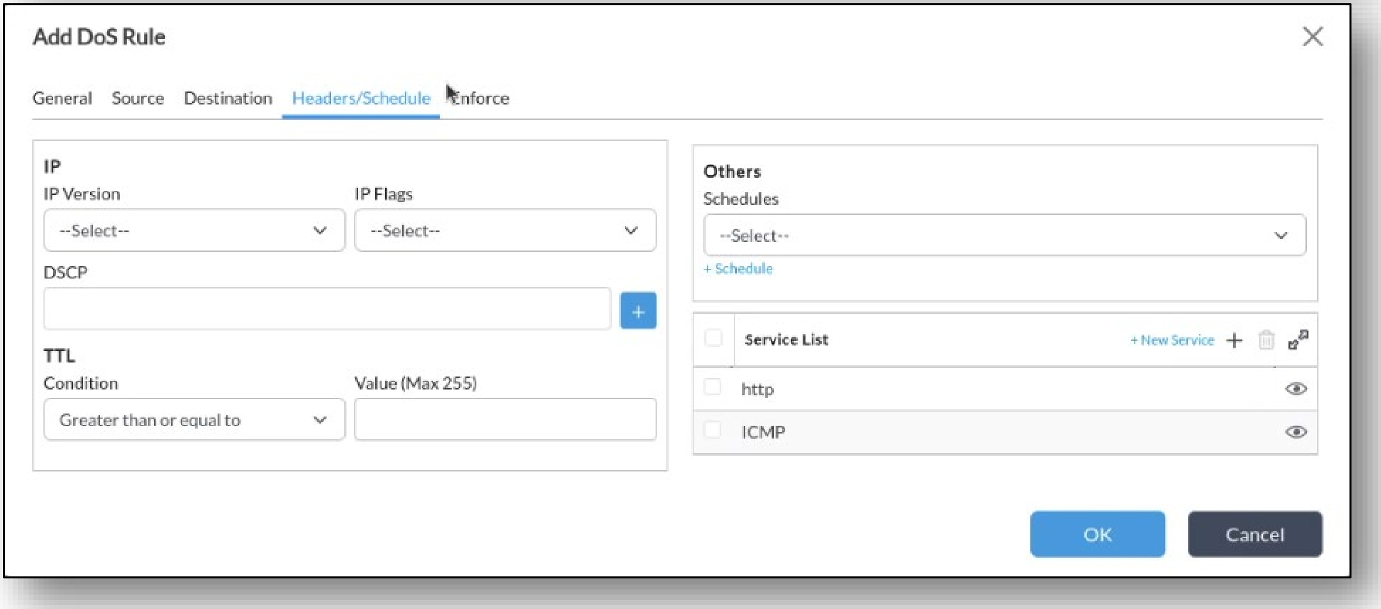
Name *: HUB-HTTP-80

Description:

Tags: Add a tag

Type *: IPv4

IPv4 Address/Prefix *: 10.27.13.20/32



Add DoS Rule

General | Source | Destination | Headers/Schedule | Enforce

IP

IP Version: --Select--

IP Flags: --Select--

DSCP:

TTL

Condition: Greater than or equal to

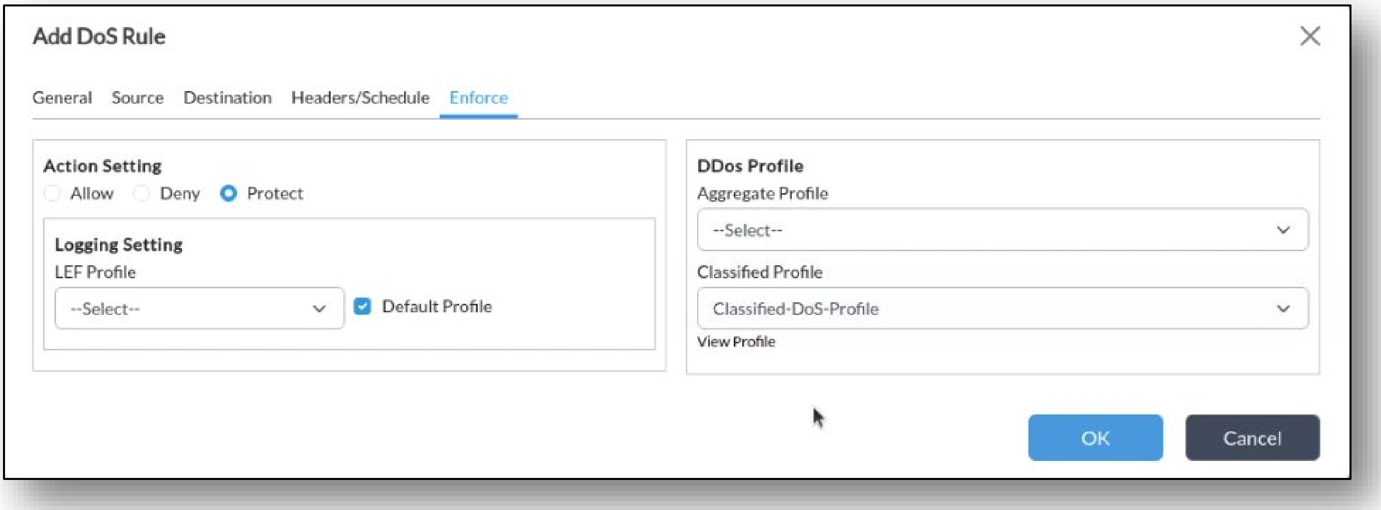
Value (Max 255):

Others

Schedules: --Select--

Service List

- http
- ICMP



Add DoS Rule

Action Setting

○ Allow ○ Deny ● Protect

Logging Setting

LEF Profile: --Select-- ☑ Default Profile

DDos Profile

Aggregate Profile: --Select--

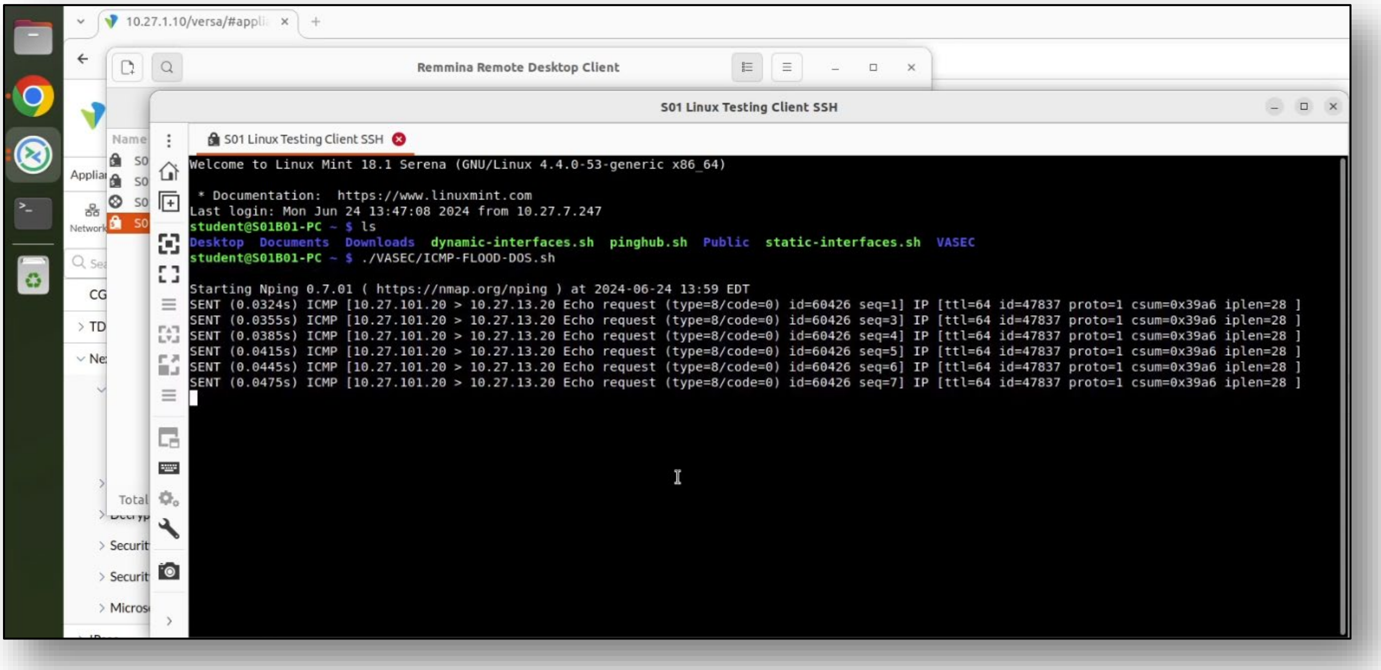
Classified Profile: Classified-DoS-Profile

1.6 Verify the DoS Policy Protection

In the next steps you will verify that the DoS Protection rules and profile are functioning by logging into the test host connected to Branch110 and running traffic simulation scripts, then verifying the behavior of the policies.

Create an ssh session to the testing host device that is connected to your branch device. Use the username ***student*** and password ***versa123***. From a command prompt, perform the following tasks:

Verification Step 1	
Name:	ICMP Flood
Command to run:	From the command line on the testing host, run the ./VASEC/ICMP-FLOOD-DOS.sh command. Enter the password ***versa123*** if prompted.
Monitor Tab Verification:	Navigate to *Appliance View > SxxB01 > Monitor.* In the branch Monitor window navigate to *Services > NGFW > DoS Policies*. Verify that the ICMP Drop Count counter is incrementing.
Analytics Verification:	Return to the main Versa Director dashboard (exit the device context mode.) Navigate to the *Analytics > Logs* dashboard. Ensure that the Tenatn1 organization is selected in the top filter drop-down. Under Logs, select *Threat Detection* and open the DDOS tab in the table. The ICMP flood logs with action Drop should be displayed for your device.

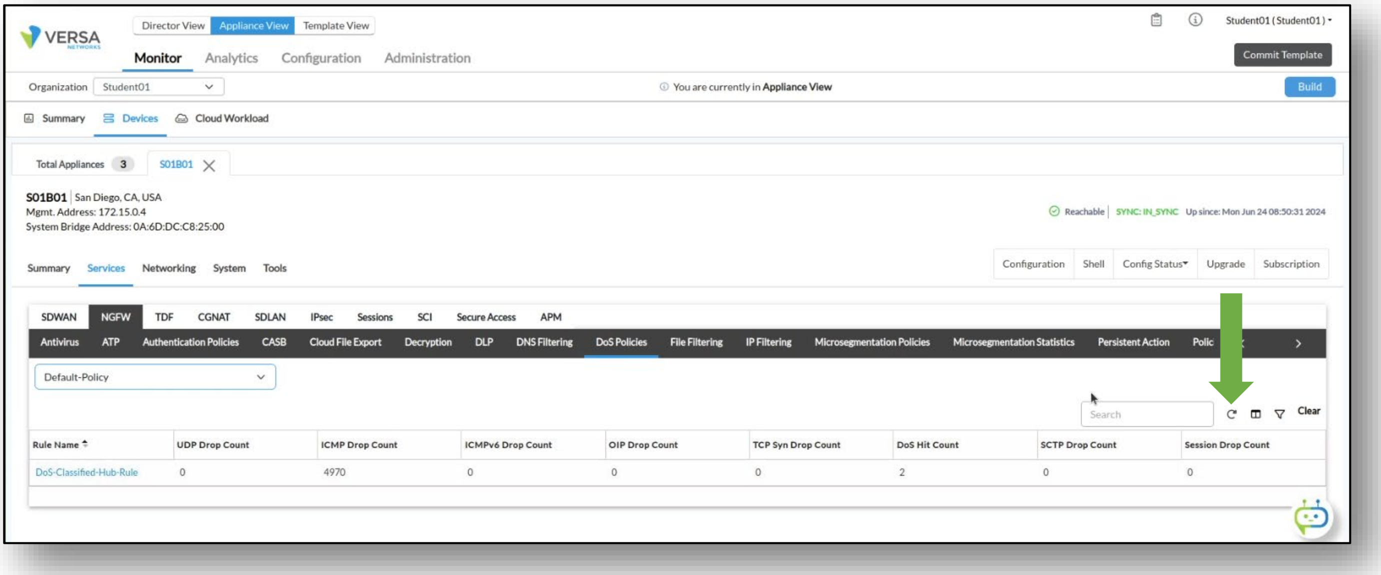

10.27.1.10/versa/#appli
Remmina Remote Desktop Client
S01 Linux Testing Client SSH
S01 Linux Testing Client SSH

```
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

 * Documentation:  https://www.linuxmint.com
Last login: Mon Jun 24 13:47:08 2024 from 10.27.7.247
student@S01B01-PC ~ $ ls
Desktop  Documents  Downloads  dynamic-interfaces.sh  pinghub.sh  Public  static-interfaces.sh  VASEC
student@S01B01-PC ~ $ ./VASEC/ICMP-FLOOD-DOS.sh

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2024-06-24 13:59 EDT
SENT (0.0324s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=1] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (0.0355s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=3] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (0.0385s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=4] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (0.0415s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=5] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (0.0445s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=6] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (0.0475s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=7] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
```

In the Monitor dashboard you can click the refresh button while the attack is in progress to see the drop count increase.



Organization: Student01

You are currently in Appliance View

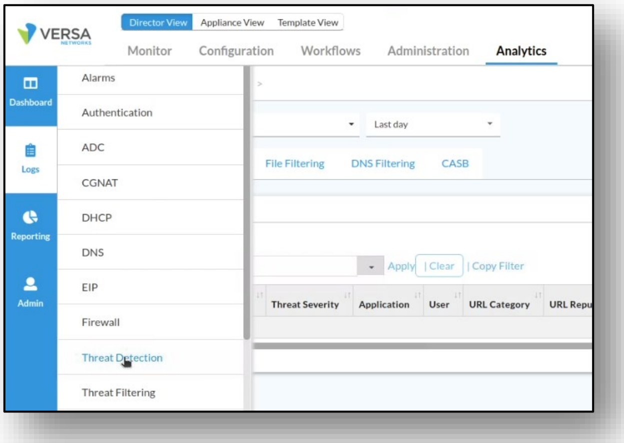
S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

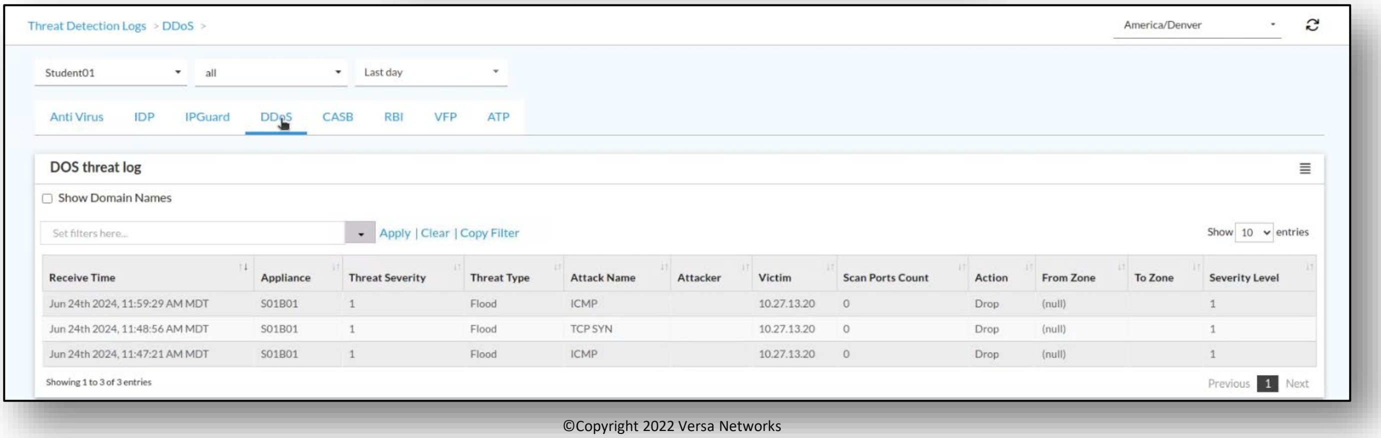
Reachable | SYNC: IN_SYNC Up since: Mon Jun 24 08:50:31 2024

Default-Policy

Rule Name	UDP Drop Count	ICMP Drop Count	ICMPv6 Drop Count	OIP Drop Count	TCP Syn Drop Count	DoS Hit Count	SCTP Drop Count	Session Drop Count
DoS-Classified-Hub-Rule	0	4970	0	0	0	2	0	0

Analytics logs record the log messages triggered by the event.





Student01 | all | Last day

DOS threat log

☐ Show Domain Names

Set filters here... Apply | Clear | Copy Filter

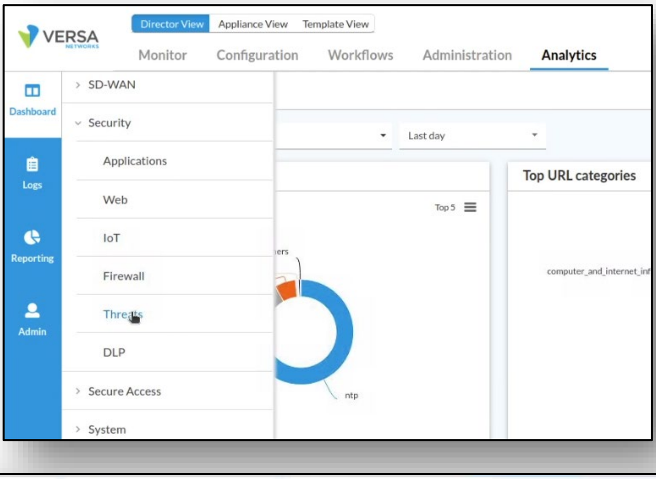
Show 10 entries

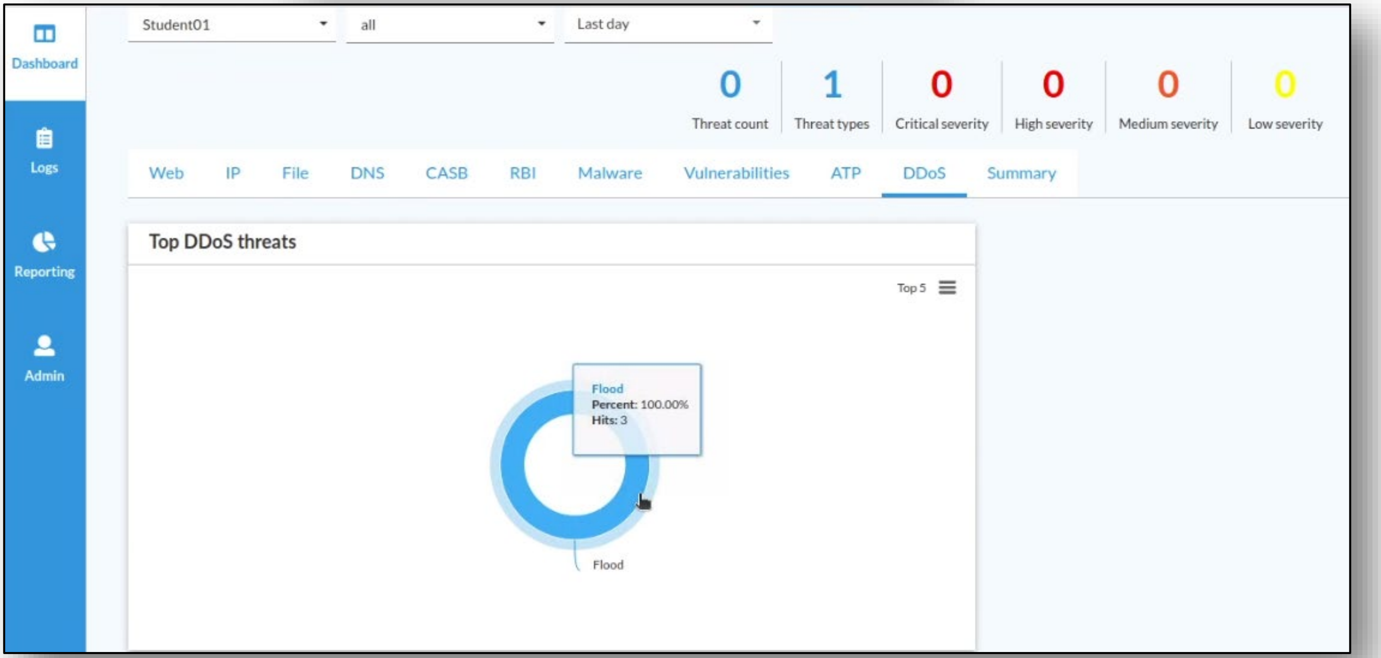
Receive Time	Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Jun 24th 2024, 11:59:29 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:48:56 AM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:47:21 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1

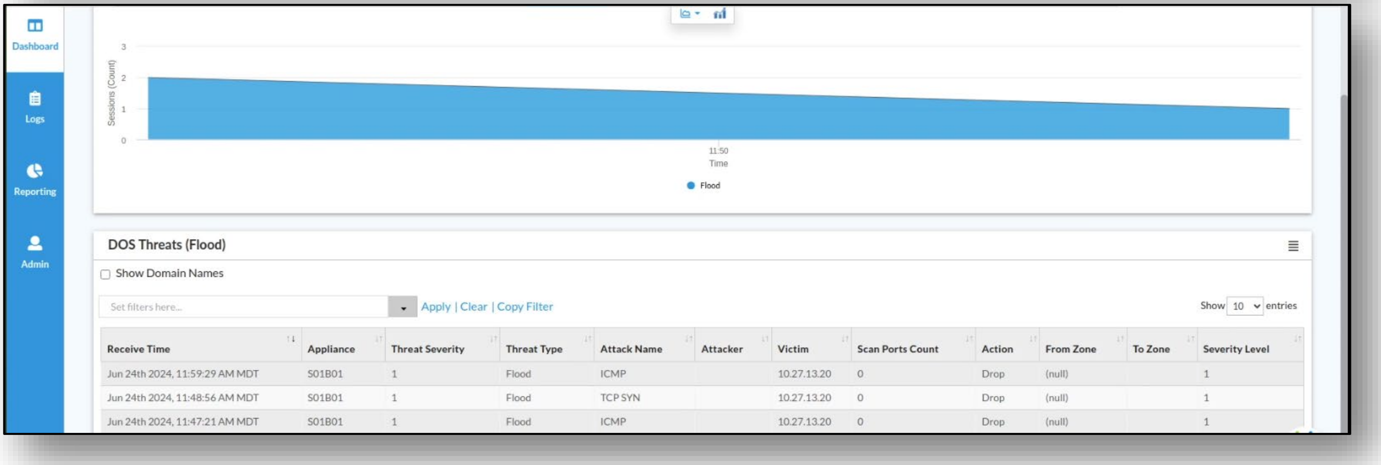
Showing 1 to 3 of 3 entries

Previous 1 Next

Analytics Dashboards provide a quick view of the event and history.







DOS Threats (Flood)

☐ Show Domain Names

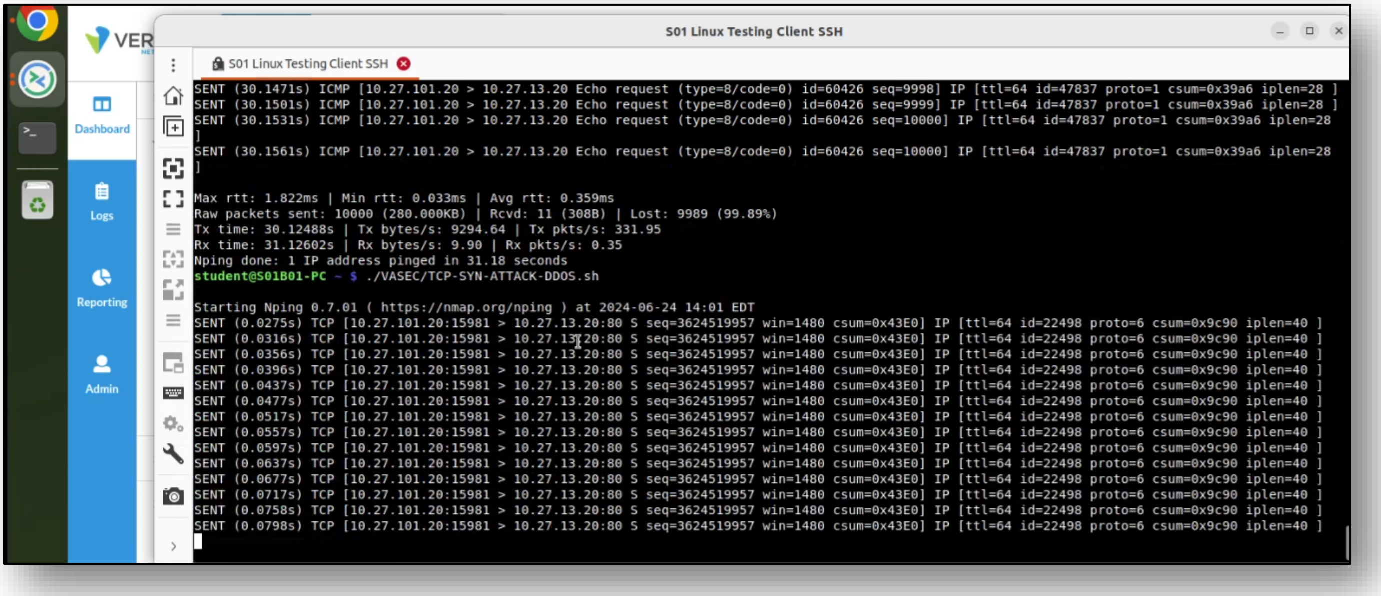
Set filters here... Apply | Clear | Copy Filter

Show 10 entries

Receive Time	Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Jun 24th 2024, 11:59:29 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:48:56 AM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:47:21 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1

TCP SYN Flood Verification

Verification Step 2	
Name:	TCP SYN Flood
Script to run:	Return to the open session on the testing host. From the command line on the testing host, press CTRL + C to stop the flood attack. run the ./VASEC/TCP-SYN-ATTACK-DDOS.sh command. Use the password ***versa123*** if prompted. This will generate a TCP SYN flood to port 80 of the hub host 10.27.13.20.
Monitor Tab Verification:	Navigate to *Monitor* > *Tenant1* > *Devices* and select your branch from the table. In your branch device Monitor window navigate to *Services* > *NGFW* > *DoS Policies*. Select *DoS-Policy* from the drop-down. Verify that the TCP-SYN Drop Count counter is incrementing.
Analytics Verification:	Return to the main Versa Director dashboard (exit the device-context mode). Navigate to the *Analytics* > *Logs* dashboard. Ensure that the Tenant1 Organization is selected in the top filter drop-down. Under Logs, select *Threat Detection* and open the DDOS tab in the table. The TCP SYN flood logs with action Drop should be displayed.

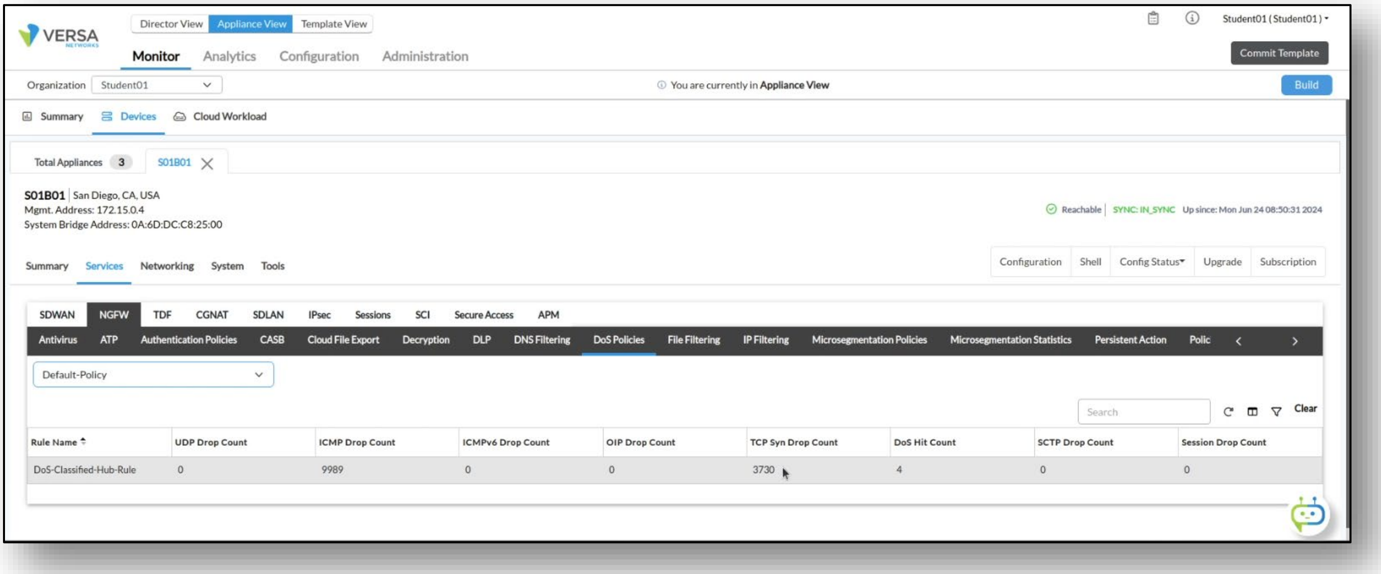


```
SENT (30.1471s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=9998] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (30.1501s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=9999] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28 ]
SENT (30.1531s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=10000] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28
]
SENT (30.1561s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=10000] IP [ttl=64 id=47837 proto=1 csum=0x39a6 iplen=28
]

Max rtt: 1.822ms | Min rtt: 0.033ms | Avg rtt: 0.359ms
Raw packets sent: 10000 (280.000KB) | Rcvd: 11 (308B) | Lost: 9989 (99.89%)
Tx time: 30.12488s | Tx bytes/s: 9294.64 | Tx pkts/s: 331.95
Rx time: 31.12602s | Rx bytes/s: 9.90 | Rx pkts/s: 0.35
Nping done: 1 IP address pinged in 31.18 seconds
student@S01B01-PC ~ $ ./VASEC/TCP-SYN-ATTACK-DDOS.sh

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2024-06-24 14:01 EDT
SENT (0.0275s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0316s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0356s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0396s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0437s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0477s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0517s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0557s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0597s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0637s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0677s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0717s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0758s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
SENT (0.0798s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 iplen=40 ]
```

TCP Syn Drop Count increases, as does DoS Hit Count.



Student01 (Student01)

Organization: Student01

You are currently in **Appliance View**

S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

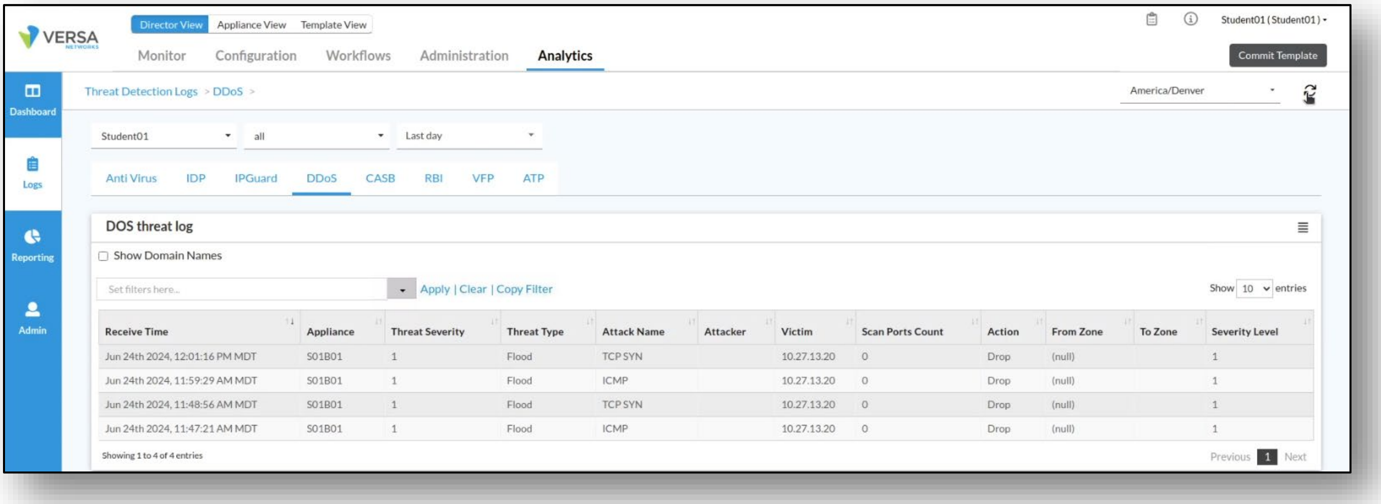
Reachable | SYNC: IN_SYNC Up since: Mon Jun 24 08:50:31 2024

Summary | Services | Networking | System | Tools

Default-Policy

Rule Name	UDP Drop Count	ICMP Drop Count	ICMPv6 Drop Count	OIP Drop Count	TCP Syn Drop Count	DoS Hit Count	SCTP Drop Count	Session Drop Count
DoS-Classified-Hub-Rule	0	9989	0	0	3730	4	0	0

The new attack is recorded in the Analytics logs. You may have to click the Refresh button to update the entries.



Student01 (Student01)

Threat Detection Logs > DDoS >

America/Denver

Student01 | all | Last day

DOS threat log

☐ Show Domain Names

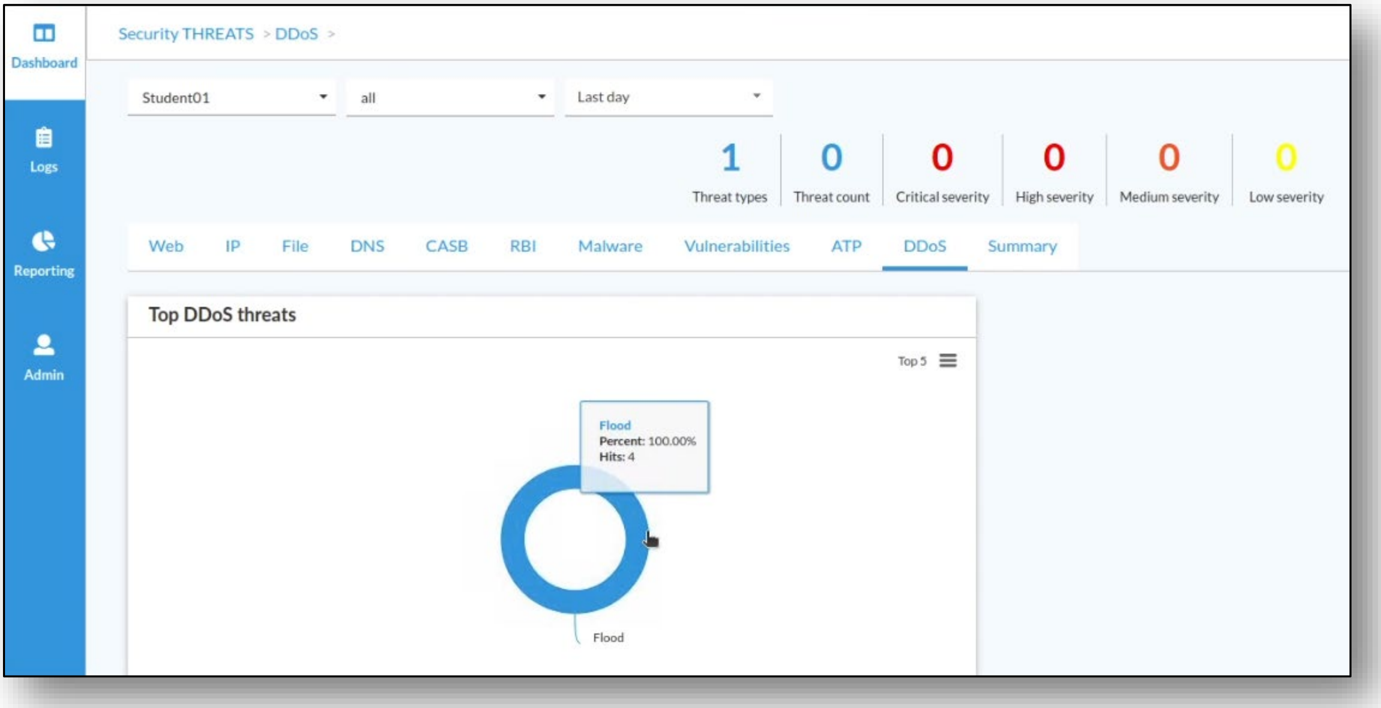
Set filters here...

Show 10 entries

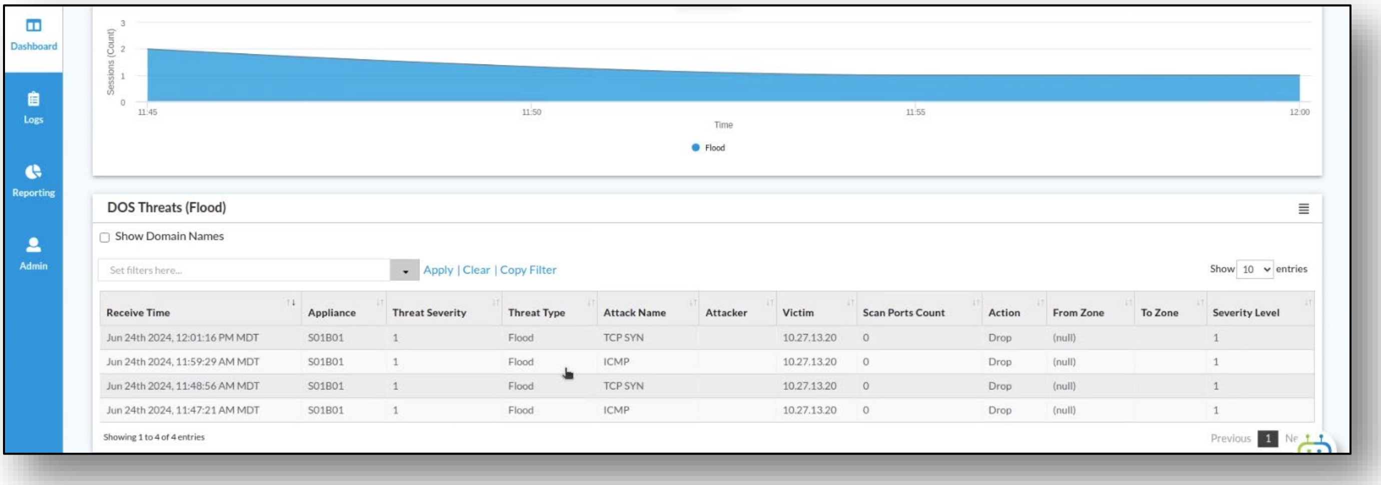
Receive Time	Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Jun 24th 2024, 12:01:16 PM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:59:29 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:48:56 AM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:47:21 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1

Showing 1 to 4 of 4 entries

The Flood Hits increases in the DDoS Threats dashboard.



Click on the chart to view details.



DOS Threats (Flood)

□ Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Show 10 entries

Receive Time	Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Jun 24th 2024, 12:01:16 PM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:59:29 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:48:56 AM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
Jun 24th 2024, 11:47:21 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1

Showing 1 to 4 of 4 entries

Previous 1 Ne

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

Application Filtering

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.

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!

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.

Application Filtering and Control

In the lab you will learn about configuring firewall rules based on applications. This lab will help you understand how traffic through the Versa Operating System device can be controlled based on zones, address, other L3/L4 and Versa's Application Identification engine information.

This lab assumes that you are familiar with the versa Director user interface, the process of creating template and device workflows, the process of onboarding devices, and the configuration and committing of templates to devices. Refer to the lab diagram included with the lab, and the table "IP Addresses of Branch Nodes" to complete this lab.

Lab Objective

Your customer is planning to enable security services and has the following requirements to have more control on the applications that the users are using on the network. The following requirements are to be met:

- Block ICMP traffic destined to 10.27.13.20 in the hub site using the applications field in security access rules.
- Block Bit-Torrent traffic for all users at the local Branches
- Create a customer application groups that includes Youtube and Netflix applications. Use the application group to create security access rules that block Youtube and Netflix.
- Create a custom application definition to identify, and categorize Twitter traffic. Use the application definition in an access rule to block the traffic.
- Allow other the Internet traffic.

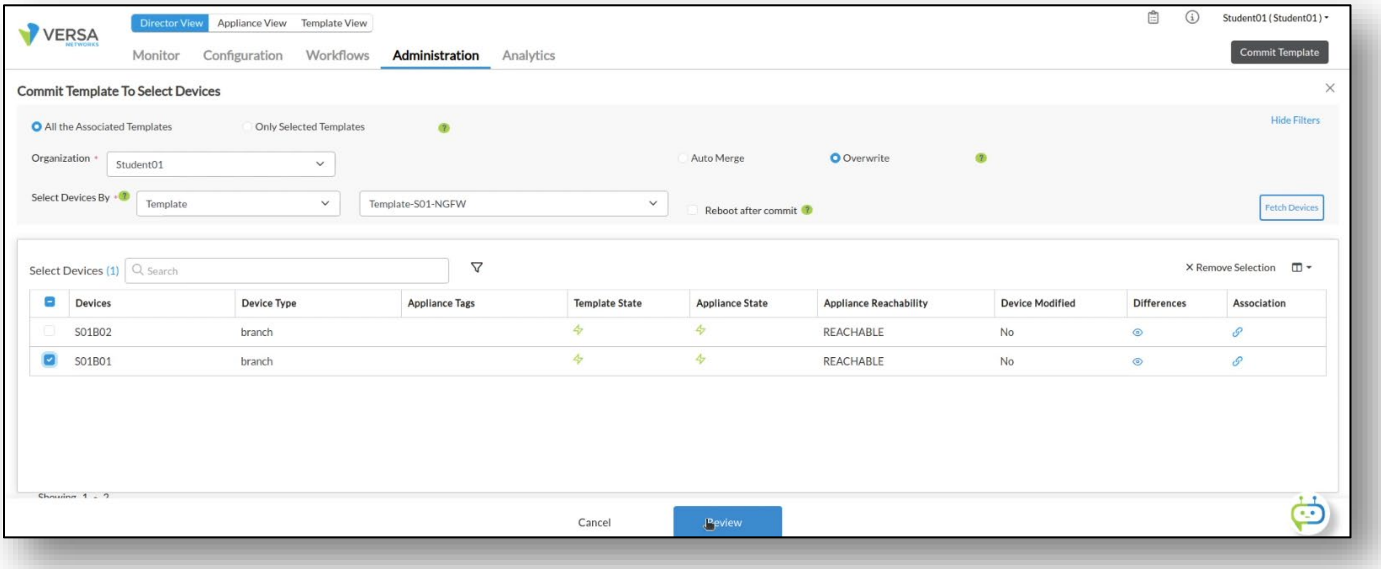
The branch B01 device will be the device configured to perform these functions. Configure the policies in appliance context mode of your assigned branch device.

Reset the Lab Environment

The first step of this lab is to reset your device to the base Next Generation Firewall configuration. To do so, log into Versa Director with your assigned username and password, and click the Commit Template button in the top right corner of the Versa Director interface.

In the Commit Template dialog, select your Student ID in the Organization box, Select Devices By Template, and choose the Template-Sxx-NGFW template from the template drop-down list. Then click Fetch Devices.

From the Select Devices table, mark the box next to the SxxB01 device, then click Review. In the Review window, click Commit to apply the base configuration to your branch device.



Commit Template To Select Devices

● All the Associated Templates ○ Only Selected Templates

Organization * Student01

○ Auto Merge ● Overwrite

Select Devices By * Template Template-S01-NGFW

□ Reboot after commit

Select Devices (1)

	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
□	S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
☑	S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

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.

Step 2.1: Configure a rule to block ICMP traffic

By default, the template workflow created 2 access rules to allow all traffic to and from the SD-WAN environment, and to all ow all sessions initiated from the locally connected branch security zone. You will create additional rules to modify this behavior.

In Versa Director, navigate to *Appliance View* and click on your appliance in the appliance table to open your appliance context mode. You will perform the configuration changes directly on your device.

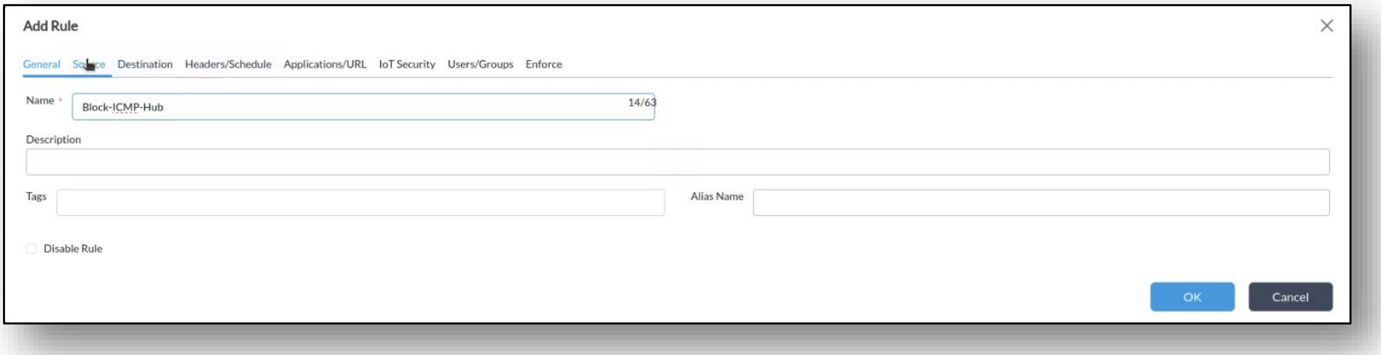
In your device configuration window, navigate to *Services > Next Gen Firewall > Security > Policies*. In the *Rules* tab you should wee the 2 access rules generated by the template workflow.

In the Rules tab, click the + button to create a new rule with the following parameters.

ICMP Access Rule	
Name:	Block-ICMP-Hub
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: ptvi Destination Address: Click + New Address and add the following address: Name: Hub Type: IPv4 IPv4 Address/Prefix: 10.27.13.20/32
Application/URL:	Application: ICMP
Enforce:	Action: Deny Log Events: Both, Default Logging Profile

Click *OK* to create the new access rule, then move the rule to the top of the rule list.

Example ICMP Access Rule



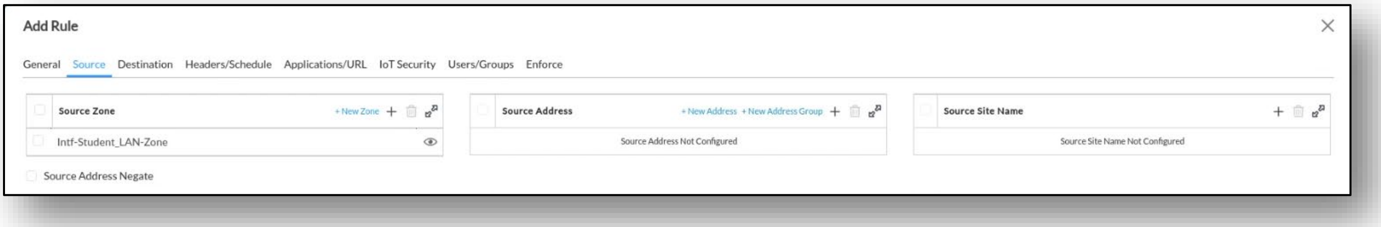
Name * Block-ICMP-Hub 14/63

Description

Tags

Alias Name

□ Disable Rule

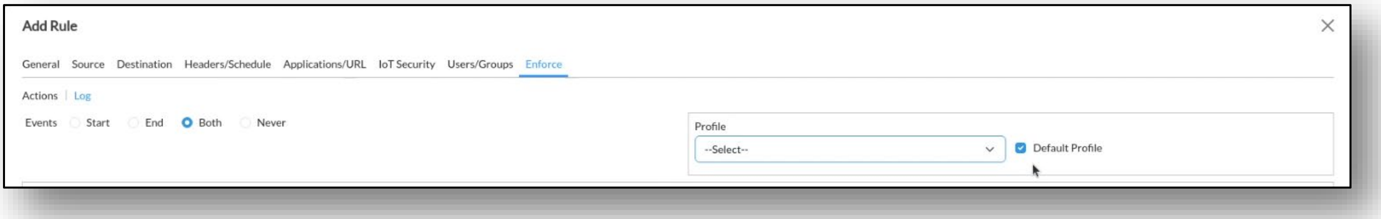


Source Zone: Intf-Student_LAN-Zone

Source Address: Source Address Not Configured

Source Site Name: Source Site Name Not Configured

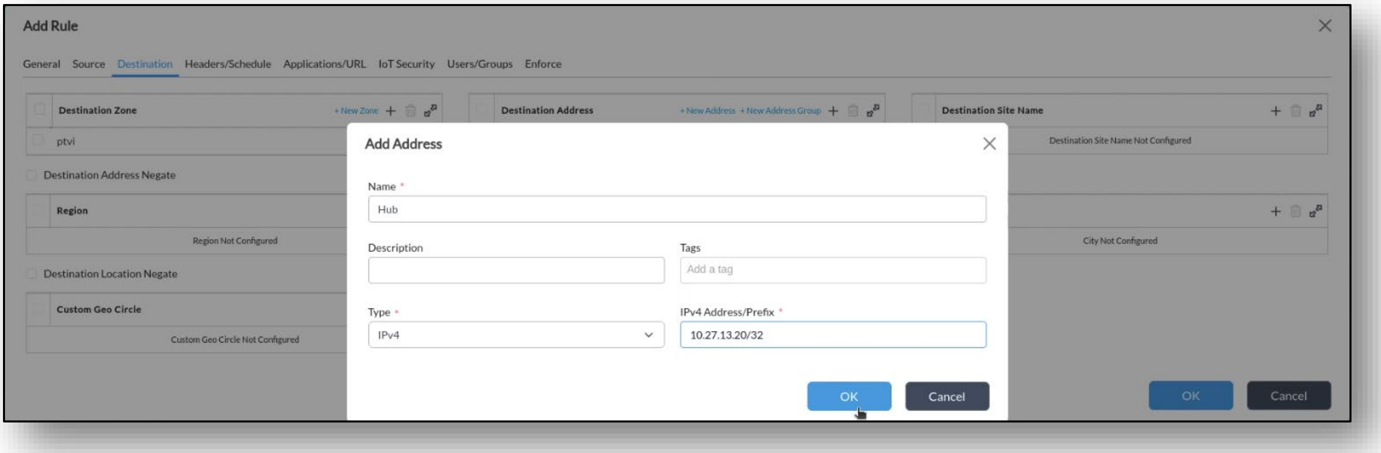
□ Source Address Negate



Events ○ Start ○ End ● Both ○ Never

Profile --Select--

☑ Default Profile



Destination Zone: ptvi

Destination Address

Destination Site Name: Destination Site Name Not Configured

□ Destination Address Negate

Region: Region Not Configured

City Not Configured

□ Destination Location Negate

Custom Geo Circle: Custom Geo Circle Not Configured

Add Address

Name * Hub

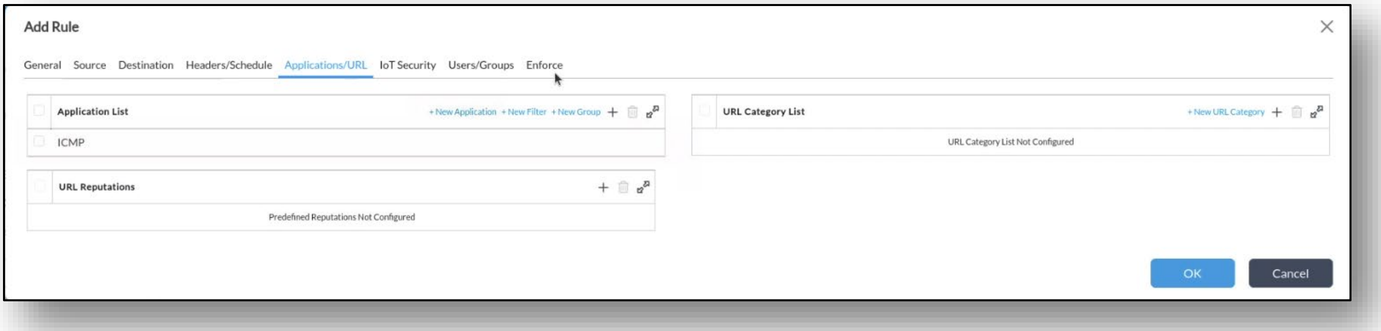
Description

Tags: Add a tag

Type * IPv4

IPv4 Address/Prefix * 10.27.13.20/32

Example ICMP Access Rule



Add Rule

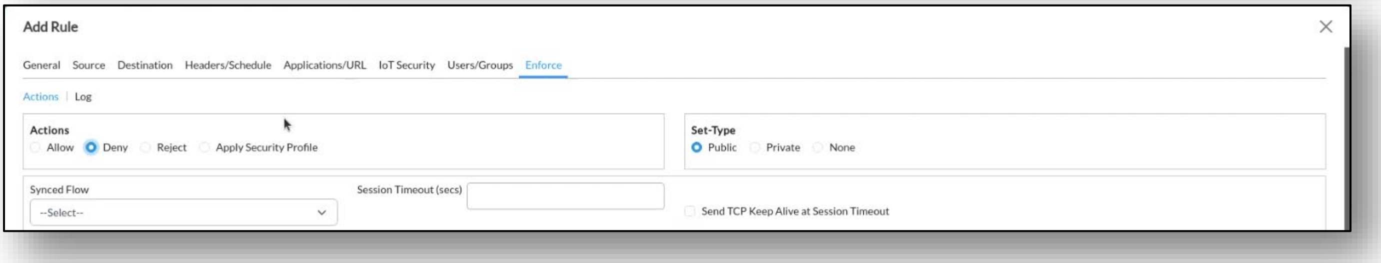
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

□ Application List	+ New Application + New Filter + New Group
□ ICMP	

□ URL Category List	+ New URL Category
URL Category List Not Configured	

□ URL Reputations
Predefined Reputations Not Configured

OK | Cancel



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Actions | Log

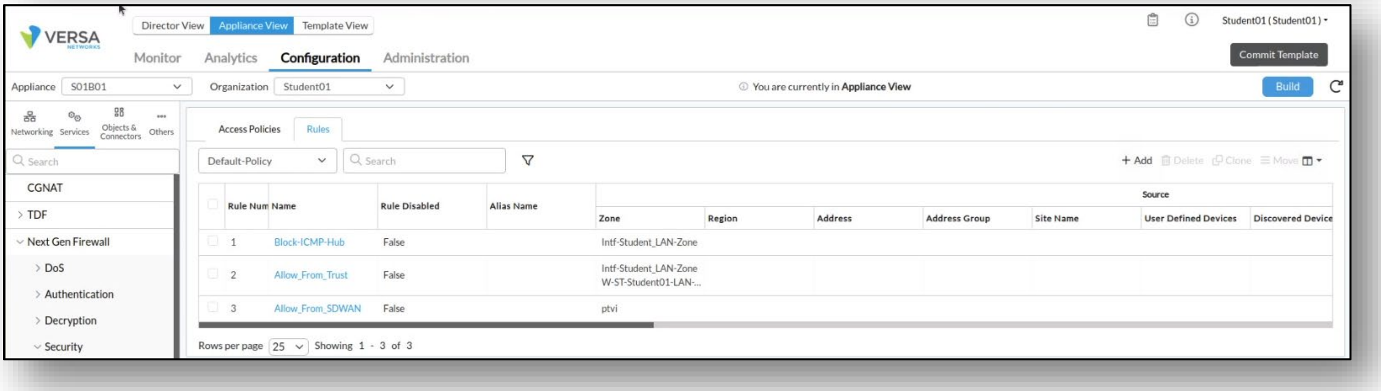
Actions
○ Allow ● Deny ○ Reject ○ Apply Security Profile

Set-Type
● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout



VERSA NETWORKS

Director View | Appliance View | Template View

Monitor | Analytics | Configuration | Administration

Student01 (Student01)

Commit Template

Appliance: S01B01 | Organization: Student01

You are currently in Appliance View

Build

Networking | Services | Objects & Connectors | Others

Search

CGNAT
TDF
Next Gen Firewall
DoS
Authentication
Decryption
Security

Access Policies | Rules

Default-Policy | Search

+ Add | Delete | Clone | Move

□	Rule Num	Name	Rule Disabled	Alias Name	Source						
					Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device
□	1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone						
□	2	Allow_From_Trust	False		Intf-Student_LAN-Zone W-ST-Student01-LAN-...						
□	3	Allow_From_SDWAN	False		ptvi						

Rows per page 25 | Showing 1 - 3 of 3

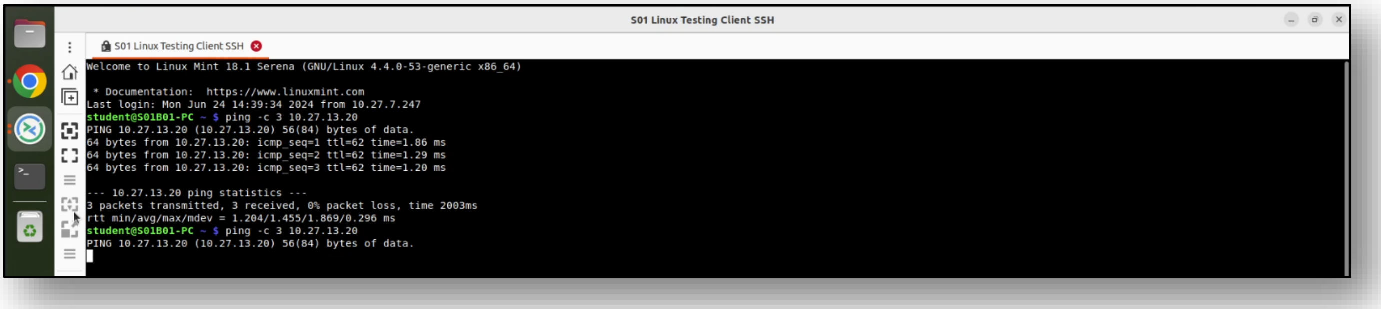
Step 2.2: Verify the Block-ICMP-105-105-Hub access rule

In the next steps you will verify that the access rule you created blocks the ICMP traffic to the hub host. You will do this by logging into the testing host connected to your assigned branch device.

In the remote desktop, click on the *Remmina* application and open the Remote Desktop connection to your Linux testing client. The username for the remote desktop session is ***student*** and password is ***versa123*** if prompted.

From the remote desktop of the Linux testing client, right-click the desktop and open a terminal window.

From the terminal window on the testing station, issue the command **`ping -c 3 10.27.13.20`.** This will send 3 ICMP packets to the host connected to the remote hub. The ICMP messages should fail.



```
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

 * Documentation:  https://www.linuxmint.com
Last login: Mon Jun 24 14:39:34 2024 from 10.27.7.247
student@S01B01-PC ~ $ ping -c 3 10.27.13.20
PING 10.27.13.20 (10.27.13.20) 56(84) bytes of data.
64 bytes from 10.27.13.20: icmp_seq=1 ttl=62 time=1.86 ms
64 bytes from 10.27.13.20: icmp_seq=2 ttl=62 time=1.29 ms
64 bytes from 10.27.13.20: icmp_seq=3 ttl=62 time=1.20 ms

--- 10.27.13.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.204/1.455/1.869/0.296 ms
student@S01B01-PC ~ $ ping -c 3 10.27.13.20
PING 10.27.13.20 (10.27.13.20) 56(84) bytes of data.
```

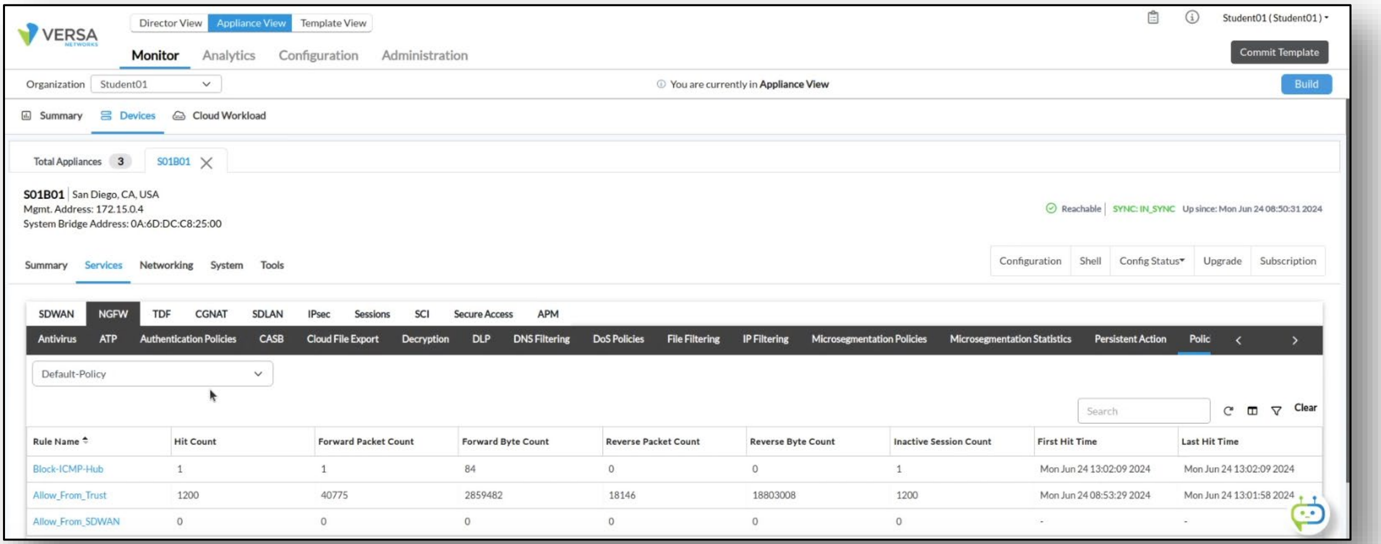
Step 2.3: Analyze the statistics and logs for the Block-ICMP-Hub access rule

Return to the Versa Director user interface. In Versa Director, navigate to the *Monitor* tab for your device. Navigate to *Services* > *NGFW* > *Policies*. This should open the *Monitor* window for your branch appliance. Examine the statistics for the *Block-ICMP-Hub* policy. You should see hit counts. If the hit counts reads 0, return to the previous steps and verify the configuration of the access rule.

Click the *Home* button next to the appliance name to return to the main Versa Director.

From the main Versa Director dashboard, navigate to the *Analytics* > *Logs* > *Firewall* hierarchy. Ensure that the *Tenant1* organization is selected in the organization drop-down at the top of the dashboard.

In the *Firewall Logs* dashboard, add a filter that searches for the rule name *Block-ICMP-Hub.* This should display the entries that match the rule name. You should see entries that indicate that the ICMP packets have been denied. You can check the source address of the entries to determine which packets are sourced from the LAN connected to your branch device. You should see entries that indicate that the ICMP packets have been denied.



Organization: Student01

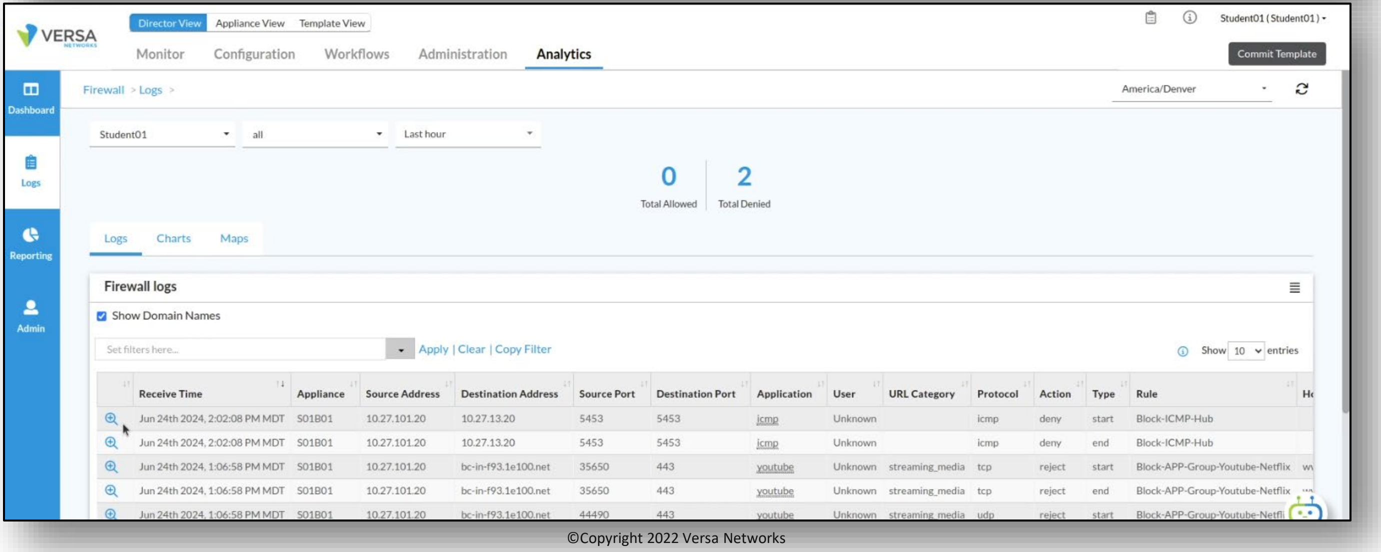
You are currently in Appliance View

S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 24 08:50:31 2024

Default-Policy

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-ICMP-Hub	1	1	84	0	0	1	Mon Jun 24 13:02:09 2024	Mon Jun 24 13:02:09 2024
Allow_From_Trust	1200	40775	2859482	18146	18803008	1200	Mon Jun 24 08:53:29 2024	Mon Jun 24 13:01:58 2024
Allow_From_SDWAN	0	0	0	0	0	0	-	-



Firewall > Logs >

America/Denver

Student01 | all | Last hour

0 Total Allowed | 2 Total Denied

Firewall logs

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	URL Category	Protocol	Action	Type	Rule	Ho
Jun 24th 2024, 2:02:08 PM MDT	S01B01	10.27.101.20	10.27.13.20	5453	5453	icmp	Unknown		icmp	deny	start	Block-ICMP-Hub	
Jun 24th 2024, 2:02:08 PM MDT	S01B01	10.27.101.20	10.27.13.20	5453	5453	icmp	Unknown		icmp	deny	end	Block-ICMP-Hub	
Jun 24th 2024, 1:06:58 PM MDT	S01B01	10.27.101.20	bc-in-f93.1e100.net	35650	443	youtube	Unknown	streaming_media	tcp	reject	start	Block-APP-Group-Youtube-Netflix	wv
Jun 24th 2024, 1:06:58 PM MDT	S01B01	10.27.101.20	bc-in-f93.1e100.net	35650	443	youtube	Unknown	streaming_media	tcp	reject	end	Block-APP-Group-Youtube-Netflix	
Jun 24th 2024, 1:06:58 PM MDT	S01B01	10.27.101.20	bc-in-f93.1e100.net	44490	443	youtube	Unknown	streaming_media	udp	reject	start	Block-APP-Group-Youtube-Netfli	

Step 2.4: Configure a rule to block Bit-Torrent

In the next steps you will create a rule that will block Bit Torrent related traffic by using the pre-defined applications that are built into the Versa Operating System.

Navigate to *Administration > Appliances* and click your branch device in the appliance table to open the appliance context mode for your device. You will perform the configuration steps directly in your device.

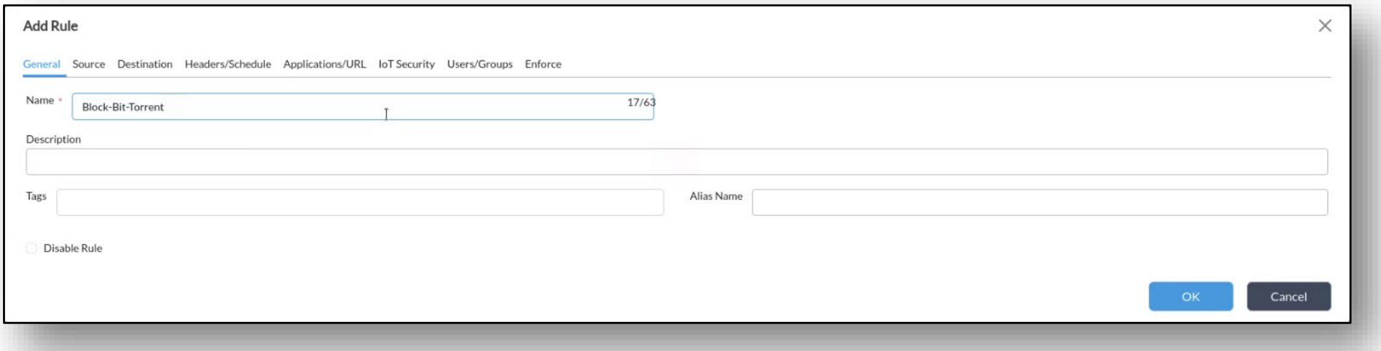
In your device configuration, navigate to *Services > Next Gen Firewall > Security > Policies*. In the Rules tab, click the + button to create a new access rule with the following parameters:

Block-Bit-Torrent Access Rule	
Name:	Block-Bit-Torrent
Source/Destination:	Source Zone:intf-Student_LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Applications: BITTORRENT, BITTORRENT_APPLICATION, BITTORRENT_BUNDLE
Enforce:	Action: Reject Log Events: Both, Default Logging Profile

Click *OK* to create the rule, then move the rule to the 2nd position in the rule list.

NOTE: The Reject action in this lab is to speed up the testing process. The Reject command sends a TCP-Reset back to the browser on the testing host immediately so that you do not have to wait for attempted sessions to time out.

Sample Block-Bit-Torrent Rule



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Name * Block-Bit-Torrent 17/63

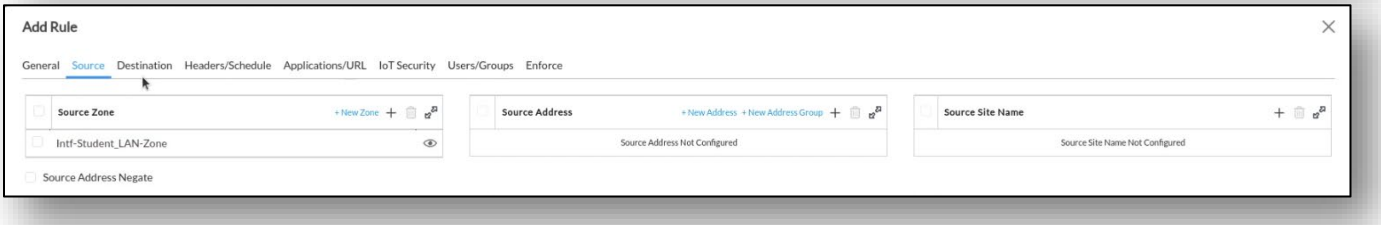
Description

Tags

Alias Name

□ Disable Rule

OK Cancel



Add Rule

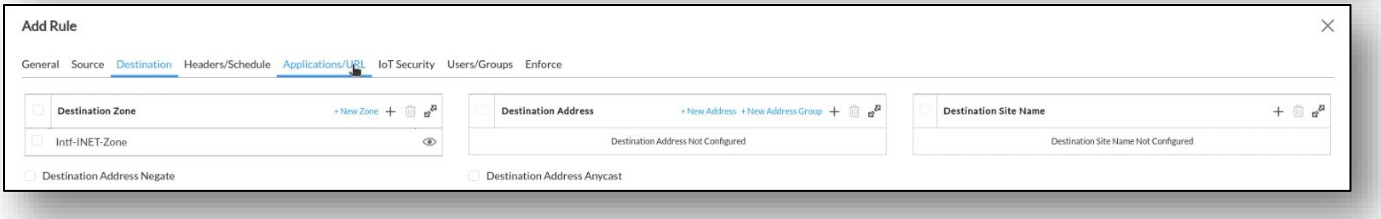
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Source Site Name
Source Site Name Not Configured

□ Source Address Negate



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

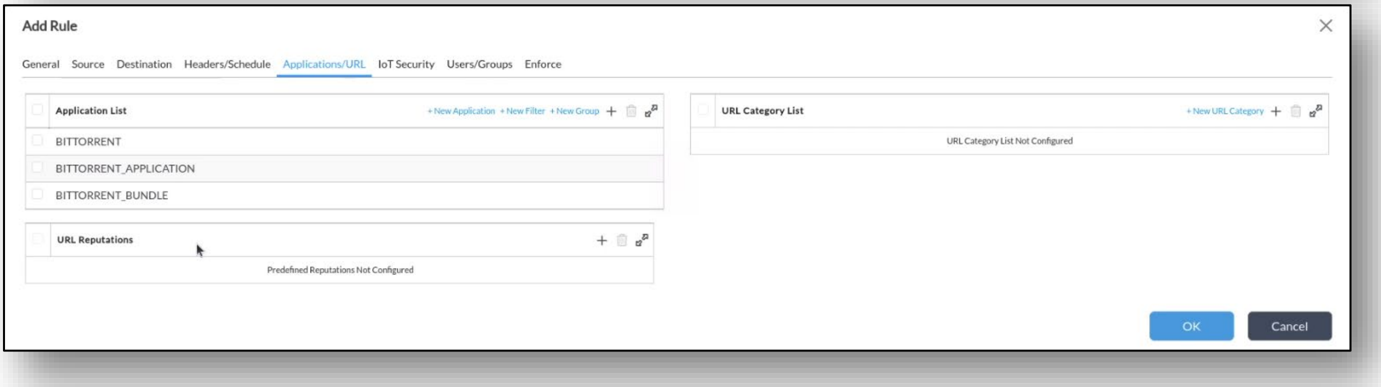
Destination Zone
Intf-INET-Zone

Destination Address
Destination Address Not Configured

Destination Site Name
Destination Site Name Not Configured

□ Destination Address Negate

□ Destination Address Anycast



Add Rule

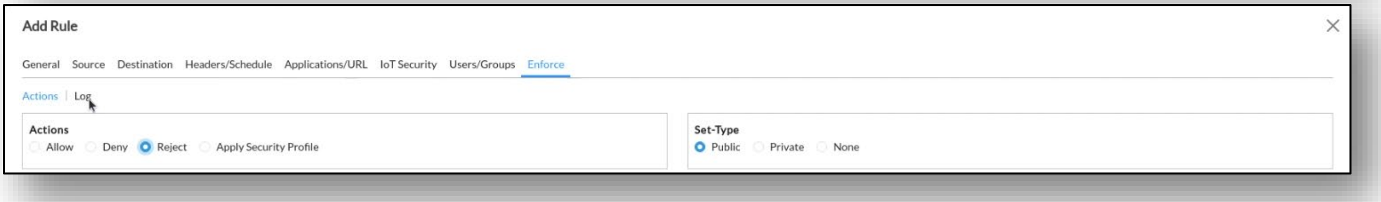
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Application List
BITTORRENT
BITTORRENT_APPLICATION
BITTORRENT_BUNDLE

URL Category List
URL Category List Not Configured

URL Reputations
Predefined Reputations Not Configured

OK Cancel



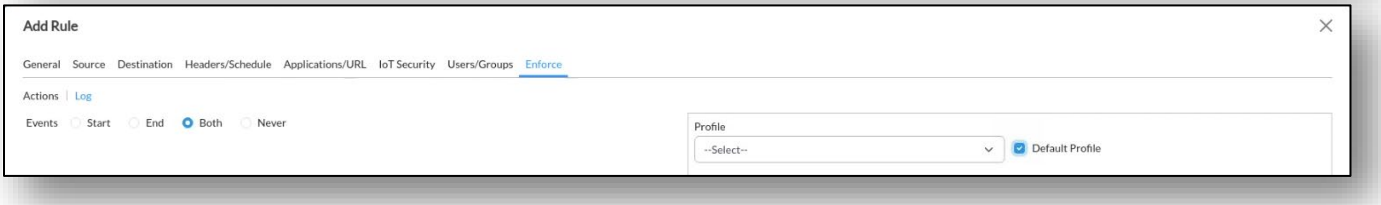
Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Actions | Log

Actions
○ Allow ○ Deny ● Reject ○ Apply Security Profile

Set-Type
● Public ○ Private ○ None



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Actions | Log

Events ○ Start ○ End ● Both ○ Never

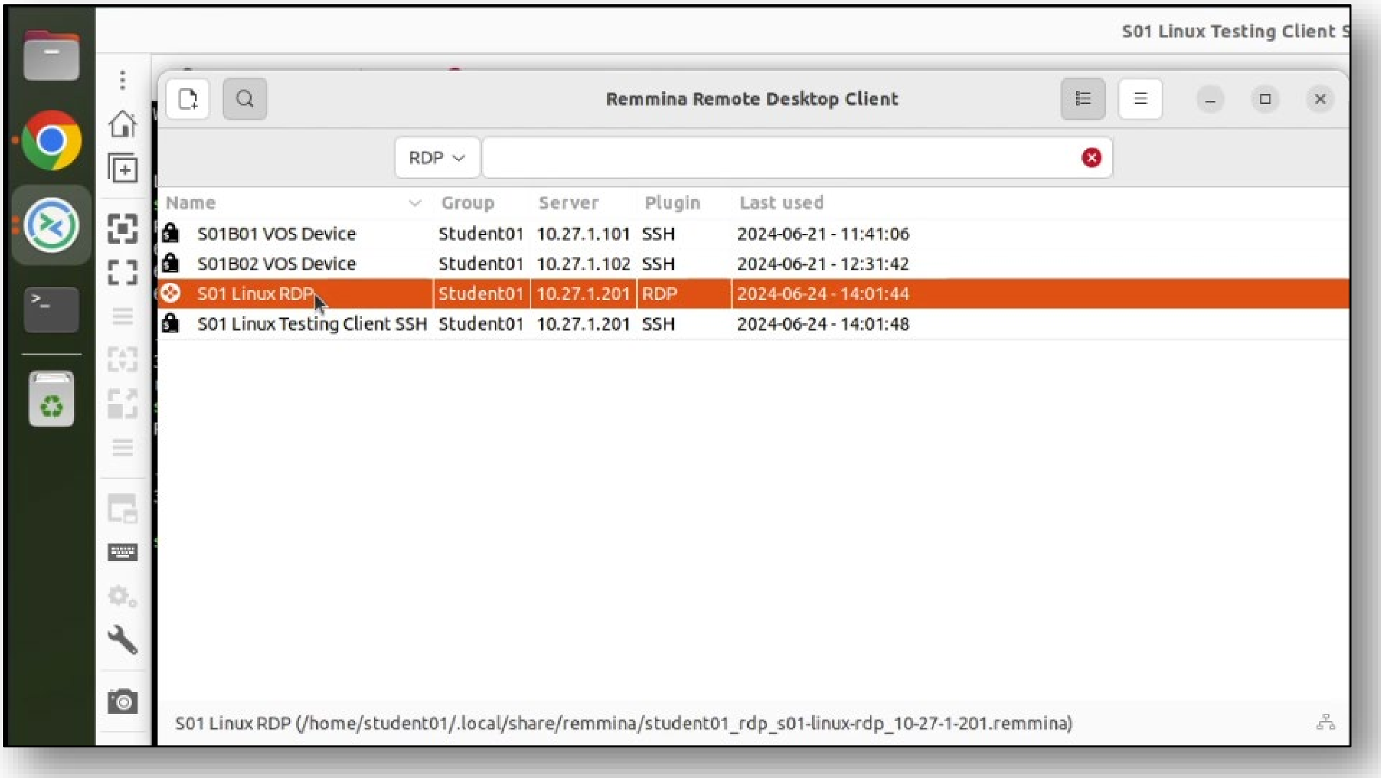
Profile
--Select--

☑ Default Profile

Step 2.5: Verify that the Block-Bit-Torrent rule blocks traffic

In the next steps you will return to the testing host remote desktop, open the Chromium web browser, and attempt to navigate to the *https://bittorent.com* web site.

On the remote landing station, use the Remmina application to open an RDP session to the Linux testing client. The username is ***s tudent*** and the password is ***versa123*** if prompted.



Name	Group	Server	Plugin	Last used
S01B01 VOS Device	Student01	10.27.1.101	SSH	2024-06-21 - 11:41:06
S01B02 VOS Device	Student01	10.27.1.102	SSH	2024-06-21 - 12:31:42
S01 Linux RDP	Student01	10.27.1.201	RDP	2024-06-24 - 14:01:44
S01 Linux Testing Client SSH	Student01	10.27.1.201	SSH	2024-06-24 - 14:01:48

S01 Linux RDP (/home/student01/.local/share/remmina/student01_rdp_s01-linux-rdp_10-27-1-201.remmina)

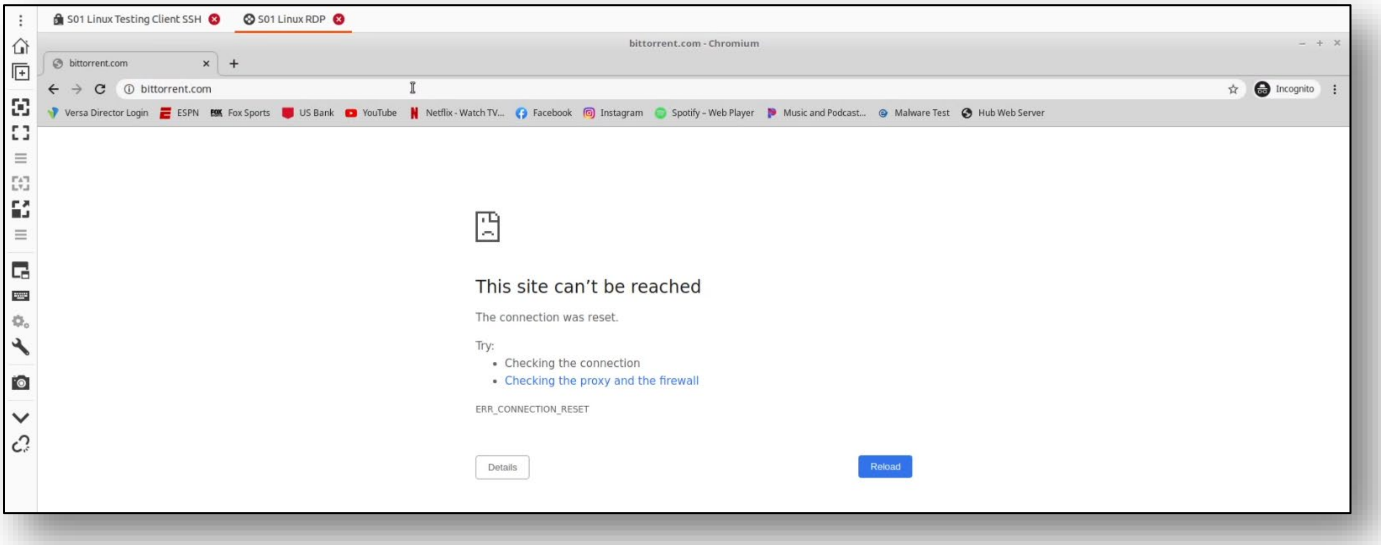
From the desktop of the testing host, open the Chromium web browser.

Click on the three dots in the top right corner of the browser and open an Incognito window (this will help prevent browser caching of sessions).

In the address bar of the web browser, enter the URL *https://bittorrent.com*. The page should not open. Click the *Refresh* button on the browser a couple of times to try to connect.

Step 2.6: Analyze the statistics and logs for the Block-Bit-Torrent access rule in Versa Director

Return to versa Director. In Versa Director, open the appliance *Monitor* tab to view your appliance statistics. In the *Monitor* tab for your appliance, navigate to the *Monitor > Services > NGFW > Policies* dashboard. Examine the hit count on the *Block-Bit-Torrent* access rule. The rule hit count should be a non-zero number.



This site can't be reached

The connection was reset.

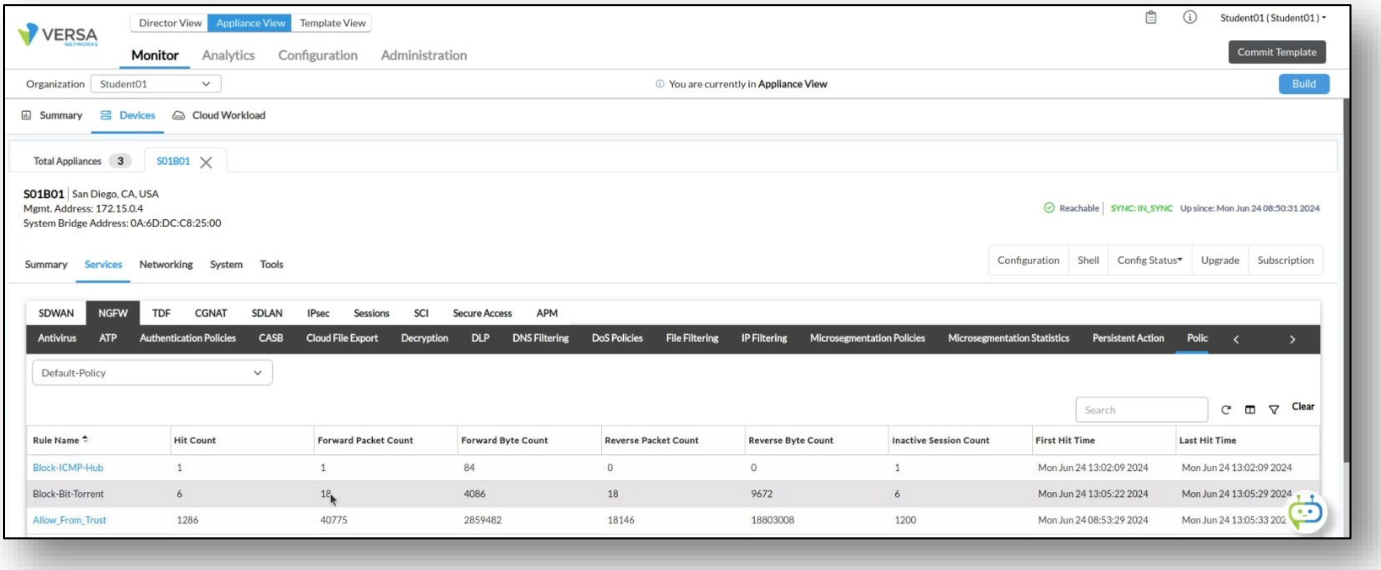
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

Step 2.6: Analyze the statistics and logs for the Block-Bit-Torrent access rule in Versa Director

Return to versa Director. In Versa Director, open the appliance *Monitor* tab to view your appliance statistics. In the *Monitor* tab for your appliance, navigate to the *Monitor > Services > NGFW > Policies* dashboard. Examine the hit count on the *Block-Bit-Torrent* access rule. The rule hit count should be a non-zero number.



Organization Student01

You are currently in **Appliance View**

S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 24 08:50:31 2024

Default-Policy

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-ICMP-Hub	1	1	84	0	0	1	Mon Jun 24 13:02:09 2024	Mon Jun 24 13:02:09 2024
Block-Bit-Torrent	6	18	4086	18	9672	6	Mon Jun 24 13:05:22 2024	Mon Jun 24 13:05:29 2024
Allow_From_Trust	1286	40775	2859482	18146	18803008	1200	Mon Jun 24 08:53:29 2024	Mon Jun 24 13:05:33 202

Configure a custom application group for the Netflix and YouTube applications.

In the next steps you will create a custom application group that contains the applications YouTube and Netflix. You will use this application group to match traffic in an access rule and block the traffic from those two applications.

Step 2.7 Configure and access rule that references the new application group

In the next steps you will create an access rule to block traffic that matches the applications in the application group you just created.

Navigate to *Configuration* > *Services* > *Next Gen Firewall* > *Security* > *Policies*. In the *Rules* tab, click the + button to create a new access rule with the following parameters:

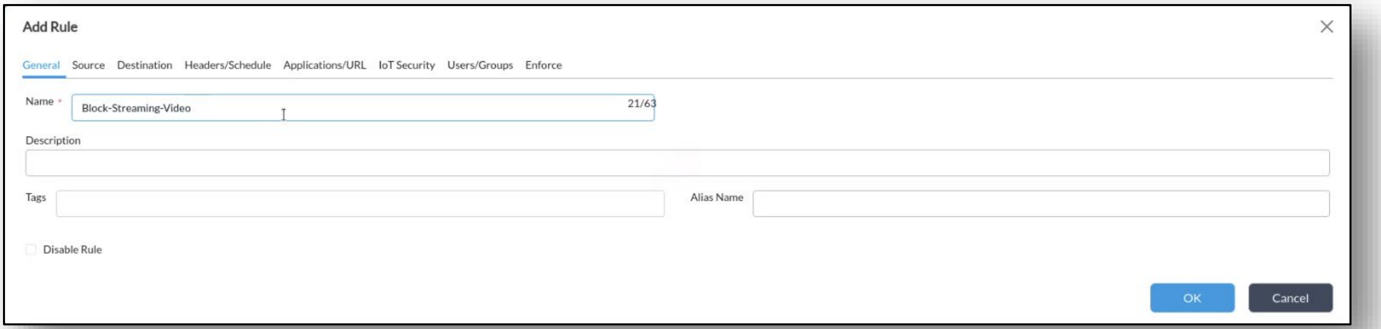
Access Rule	
Name:	Block-Streaming-Video
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Applications List: APP-Group-Youtube-Netflix (create a new application group that includes Netflix and Youtube)
Enforce:	Action: Deny Log Events: Both, Default-Logging-Profile

You can create an application group inline in the policy by clicking the *+ New Group* button, or you can create the application group separately in the *Objects & Connectors > Objects > Custom Objects > Application Groups* hierarchy. If you create the application group inline in the policy, the resulting group is created in the custom objects database.

Custom Application Group	
Name:	APP-Group-Youtube-Netflix
Applications:	Applications; YOUTUBE, NETFLIX

When you are finished creating the rule, place the rule in position 3 (3rd) in the rule list.

Example Rule



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Name * Block-Streaming-Video 21/63

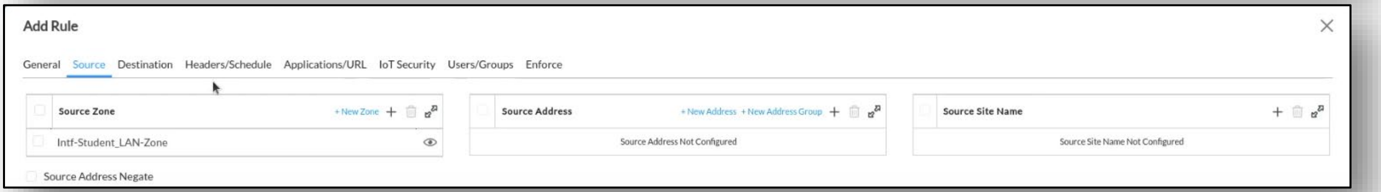
Description

Tags

Alias Name

□ Disable Rule

OK Cancel



Add Rule

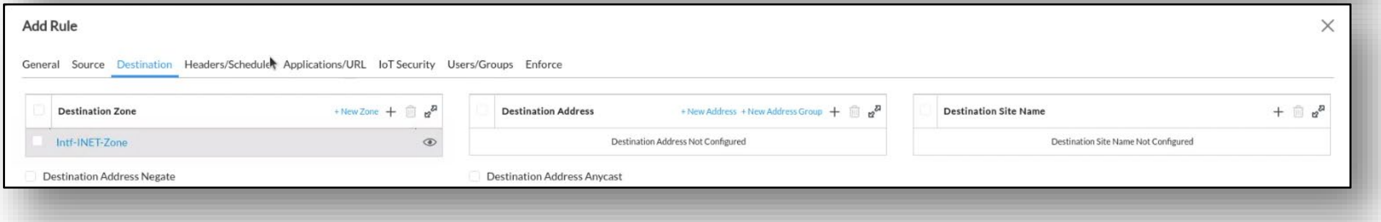
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Source Zone
Intf-Student_LAN-Zone

Source Address
Source Address Not Configured

Source Site Name
Source Site Name Not Configured

□ Source Address Negate



Add Rule

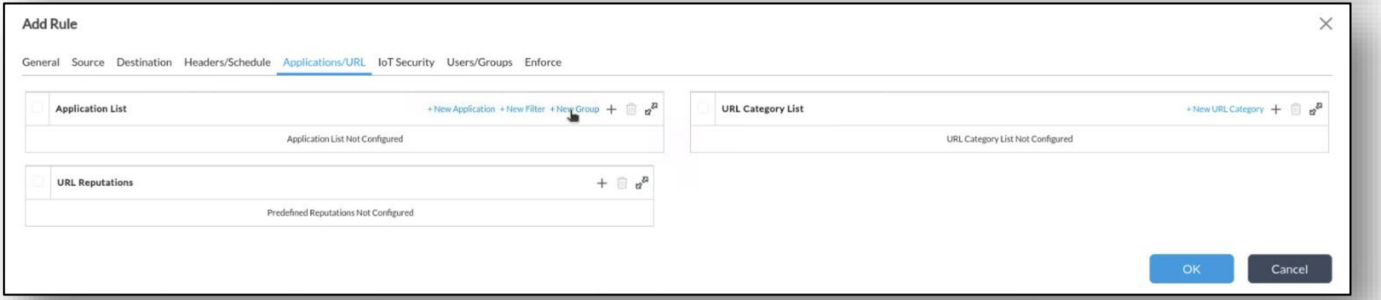
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Destination Zone
Intf-INET-Zone

Destination Address
Destination Address Not Configured

Destination Site Name
Destination Site Name Not Configured

□ Destination Address Negate □ Destination Address Anycast



Add Rule

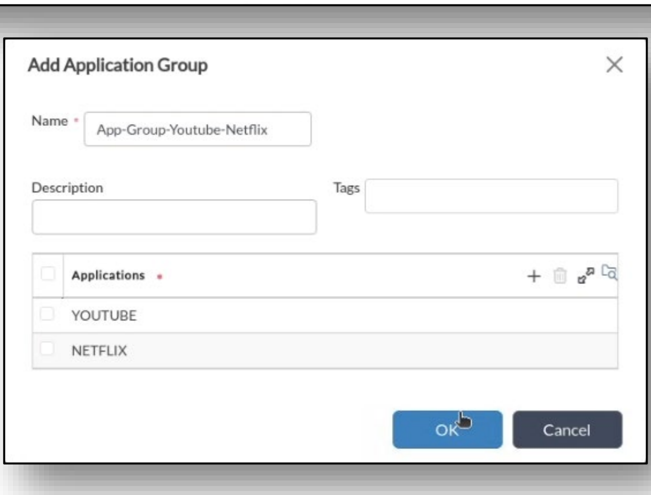
General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Application List
Application List Not Configured

URL Category List
URL Category List Not Configured

URL Reputations
Predefined Reputations Not Configured

OK Cancel



Add Application Group

Name * App-Group-Youtube-Netflix

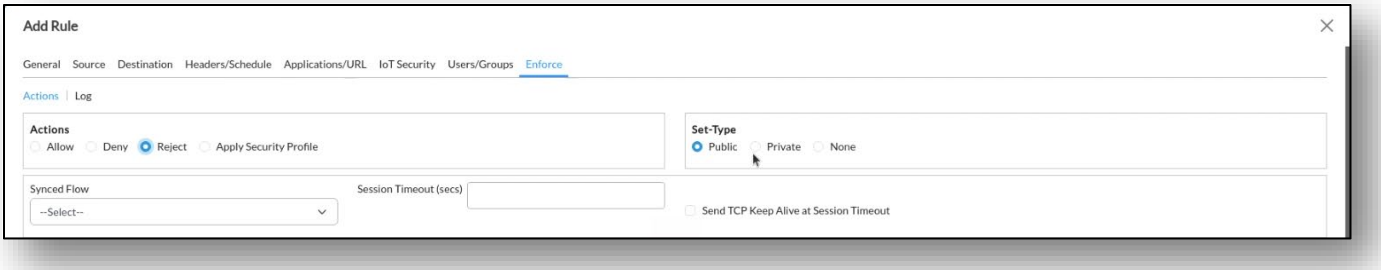
Description

Tags

Applications *
YOUTUBE
NETFLIX

OK Cancel

Example Rule



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Actions | Log

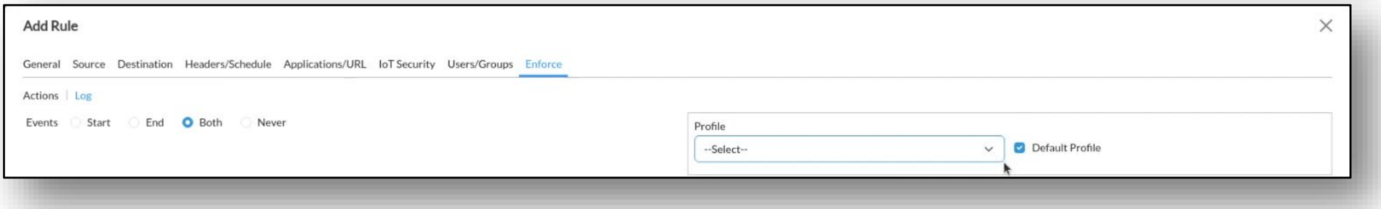
Actions
○ Allow ○ Deny ● Reject ○ Apply Security Profile

Set-Type
● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout



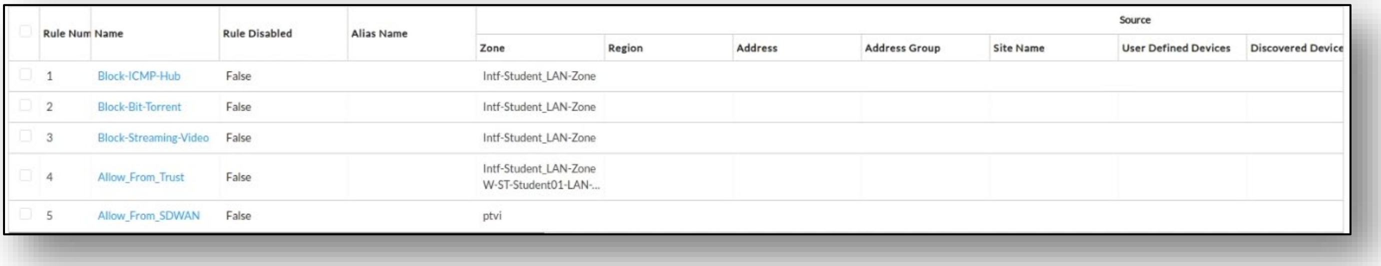
Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Actions | Log

Events ○ Start ○ End ● Both ○ Never

Profile: --Select-- ☑ Default Profile



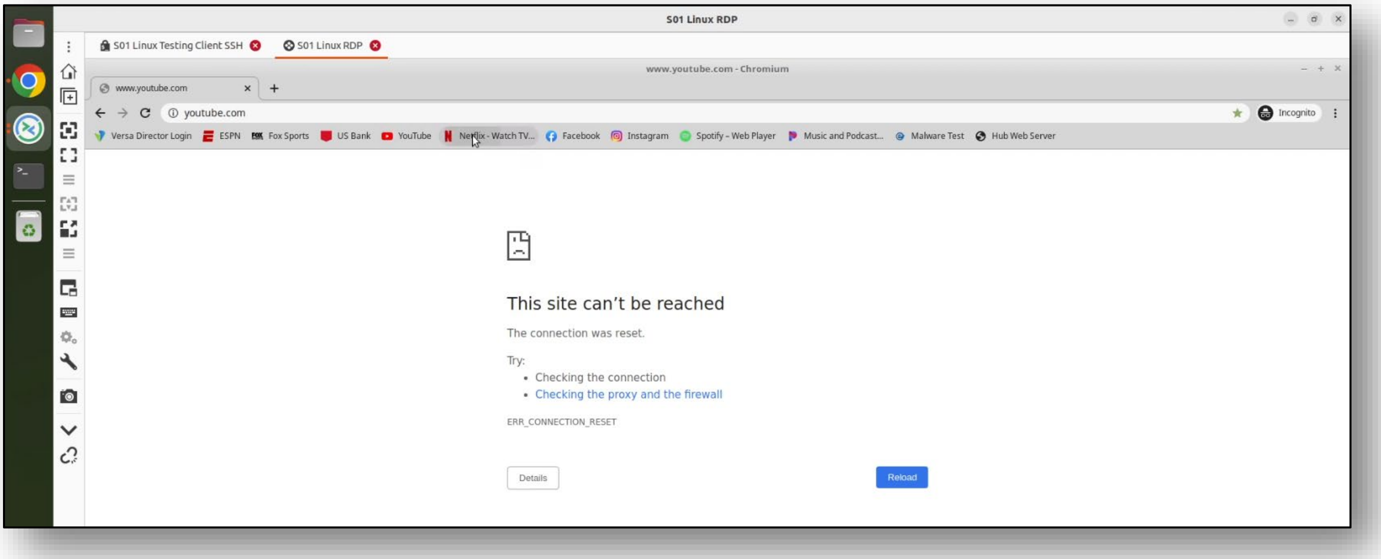
Rule Num	Name	Rule Disabled	Alias Name	Source						
				Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device
1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone						
2	Block-Bit-Torrent	False		Intf-Student_LAN-Zone						
3	Block-Streaming-Video	False		Intf-Student_LAN-Zone						
4	Allow_From_Trust	False		Intf-Student_LAN-Zone W-ST-Student01-LAN-...						
5	Allow_From_SDWAN	False		ptvi						

Step 2.10: Verify that the rule blocks YouTube and Netflix traffic

In the next steps you will verify that the access rule you created blocks the Youtube and Netflix traffic.

Return to the remote desktop session to the testing host. From the testing host, open the Chromium web browser and enter the URL *https://youtube.com* in the address bar. Click on some of the videos in the main window to attempt to watch the videos. The videos should not play.

Enter the URL *https://netflix.com* in the address bar of the browser. The web site should not open.



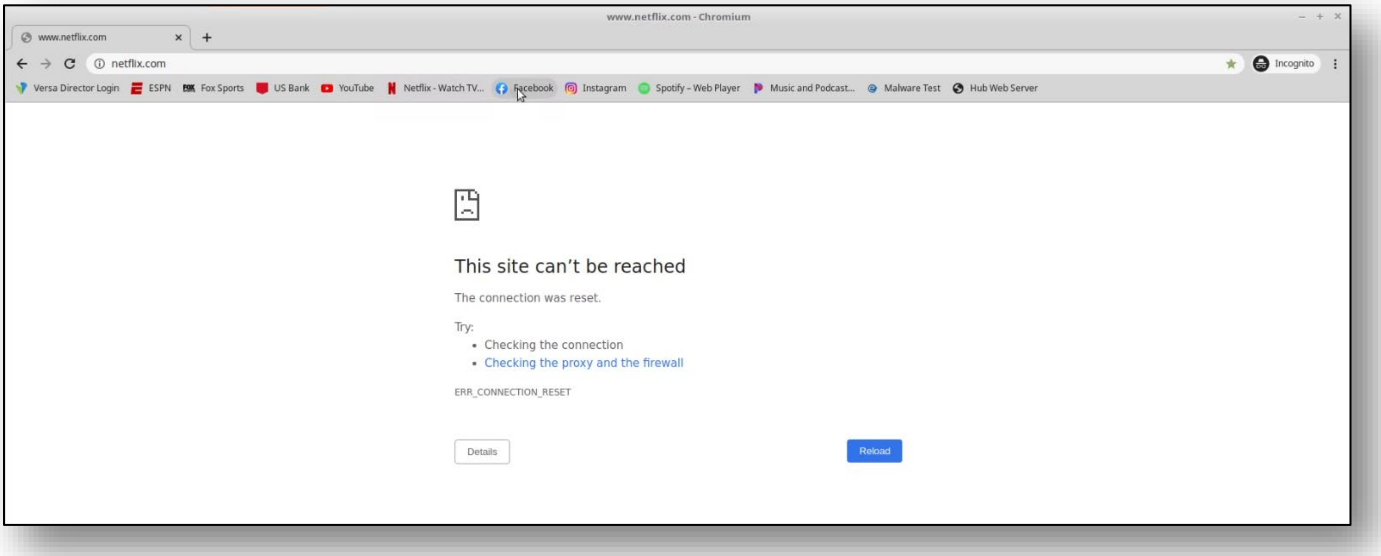
This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

Visit social media sites

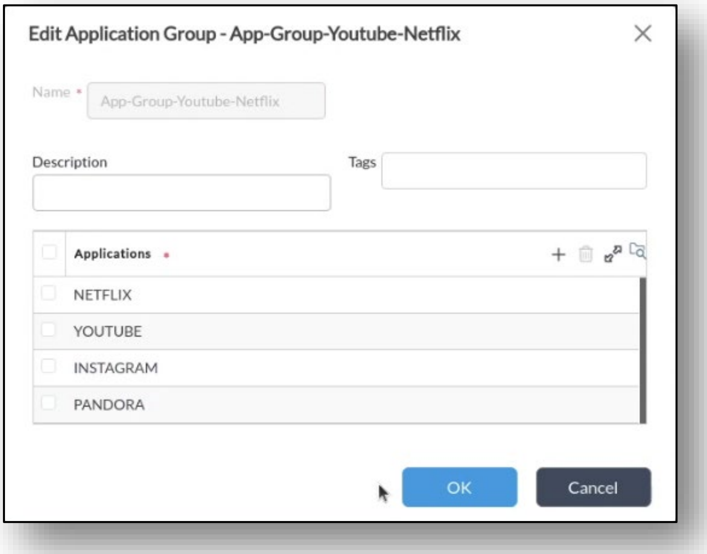
In the browser window, click on the links to a few other sites, including Facebook, Instagram, and Music and Podcast (Pandor). Verify that the pages open in the browser.

Update the application group to include other applications

You can update the application group to add or remove applications to the group. When you modify the application group, you do not need to update the policy or policies that reference the application group.

Navigate to *Objects & Connectors > Objects > Custom Objects > Application Groups* and open the application group you created through your policy.

Add the following applications to the application group: Instagram; Pandora



Edit Application Group - App-Group-Youtube-Netflix

Name * App-Group-Youtube-Netflix

Description

Tags

□	Applications *
□	NETFLIX
□	YOUTUBE
□	INSTAGRAM
□	PANDORA

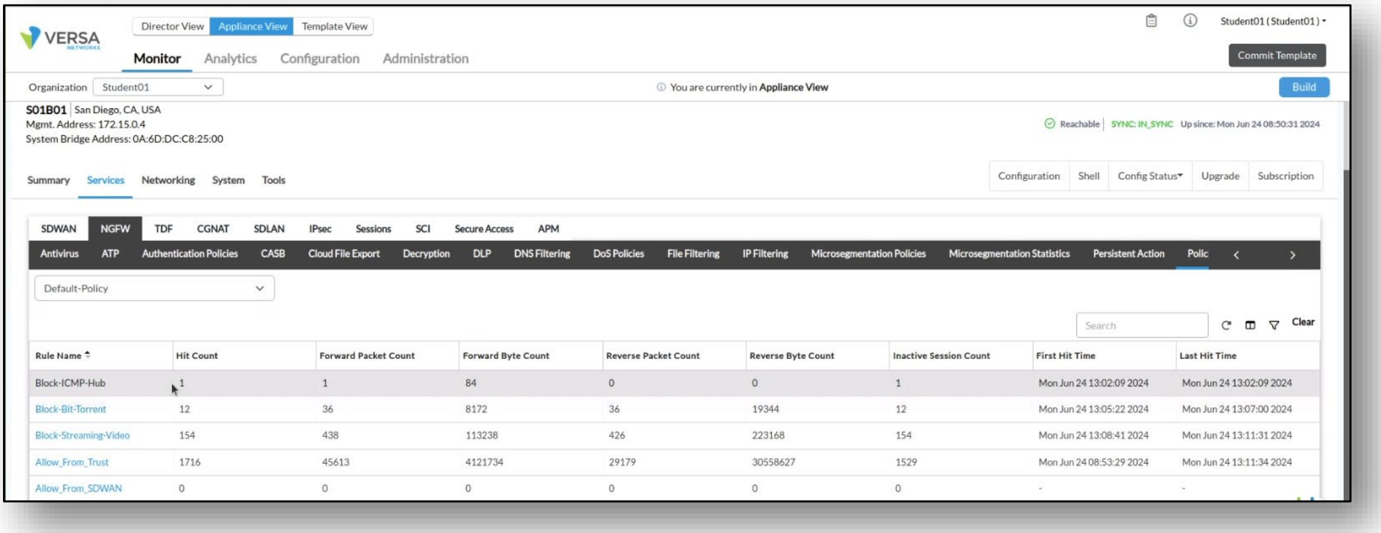
Return to the remote desktop session to the Linux testing client. In the Linux testing client, close the Chromium Web Browser, as the previous visits to the web sites will be cached. Re-open the Chromium web browser.

In the new browser window, click on the Instagram, Spotify, and Pandora (Music and Podcast) links. Only the Spotify site should open. The others should be blocked.

Verify access rule statistics in Versa Director

In the next steps you will verify that the proper access rules blocked the traffic from the previous steps.

Return to Versa Director on the landing workstation. In appliance context mode of your device, navigate to *Monitor > Services > NGFW > Policies*. Examine the statistics for the *Block-App-Group-Youtube-Netfilx* access rule. The hit count and reject count should be non-zero values.



Organization Student01

You are currently in Appliance View

S01B01 | San Diego, CA, USA
Mgmt. Address: 172.15.0.4
System Bridge Address: 0A:6D:DC:C8:25:00

Reachable | SYNC: IN_SYNC Up since: Mon Jun 24 08:50:31 2024

Default-Policy

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-ICMP-Hub	1	1	84	0	0	1	Mon Jun 24 13:02:09 2024	Mon Jun 24 13:02:09 2024
Block-Bit-Torrent	12	36	8172	36	19344	12	Mon Jun 24 13:05:22 2024	Mon Jun 24 13:07:00 2024
Block-Streaming-Video	154	438	113238	426	223168	154	Mon Jun 24 13:08:41 2024	Mon Jun 24 13:11:31 2024
Allow_From_Trust	1716	45613	4121734	29179	30558627	1529	Mon Jun 24 08:53:29 2024	Mon Jun 24 13:11:34 2024
Allow_From_SDWAN	0	0	0	0	0	0	-	-

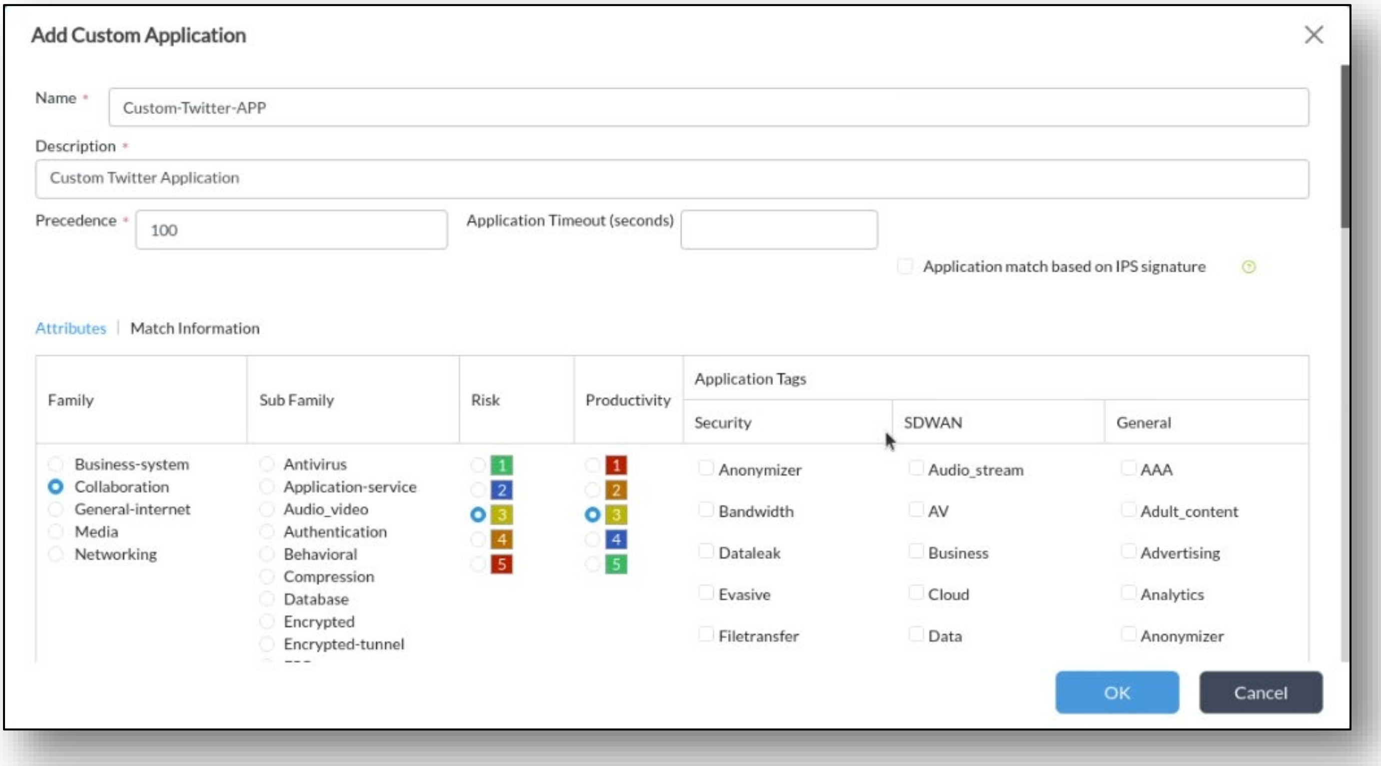
Configure a custom Twitter application

In the next steps you will create a custom application called *Custom-Twitter-APP*, and use the custom application to block the corresponding traffic.

In Versa Director, navigate to the appliance context mode of your appliance to modify the configuration directly.

In the appliance context mode of your device, navigate to *Configuration > Objects & Connectors > Custom Objects > Applications*, then click on the + Add icon or the Add button to create a new custom application with the following parameters:

Custom Application	
Name:	Custom-Twitter-APP
Description:	Custom-Twitter-APP
Precedence	100 (higher precedence makes the DPI use this custom application)
Attributes:	Family: Collaboration Sub-Family: Mail Risk: 3 Productivity: 3 Security: Misused General: File_Transfer, Email
Match Information:	Click + and add: Name: Custom-Gmail Host Pattern: .*twitter.*
Application Timeout:	120secs



Add Custom Application

Name * Custom-Twitter-APP

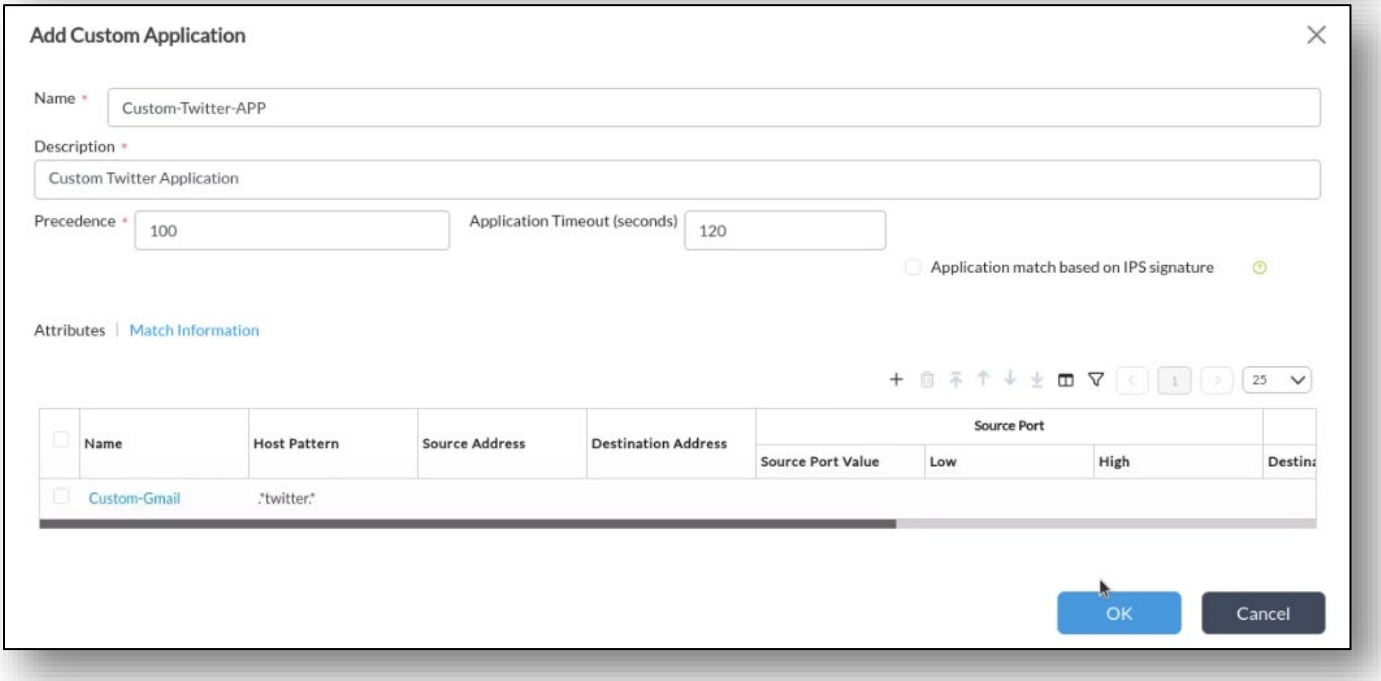
Description * Custom Twitter Application

Precedence * 100 Application Timeout (seconds)

□ Application match based on IPS signature

Attributes | Match Information

Family	Sub Family	Risk	Productivity	Application Tags Security	 SDWAN	 General
○ Business-system	○ Antivirus	○ 1	○ 1	□ Anonymizer	□ Audio_stream	□ AAA
● Collaboration	○ Application-service	○ 2	○ 2	□ Bandwidth	□ AV	□ Adult_content
○ General-internet	○ Audio_video	● 3	● 3	□ Dataleak	□ Business	□ Advertising
○ Media	○ Authentication	○ 4	○ 4	□ Evasive	□ Cloud	□ Analytics
○ Networking	○ Behavioral	○ 5	○ 5	□ Filetransfer	□ Data	□ Anonymizer
	○ Compression					
	○ Database					
	○ Encrypted					
	○ Encrypted-tunnel					



Add Custom Application

Name * Custom-Twitter-APP

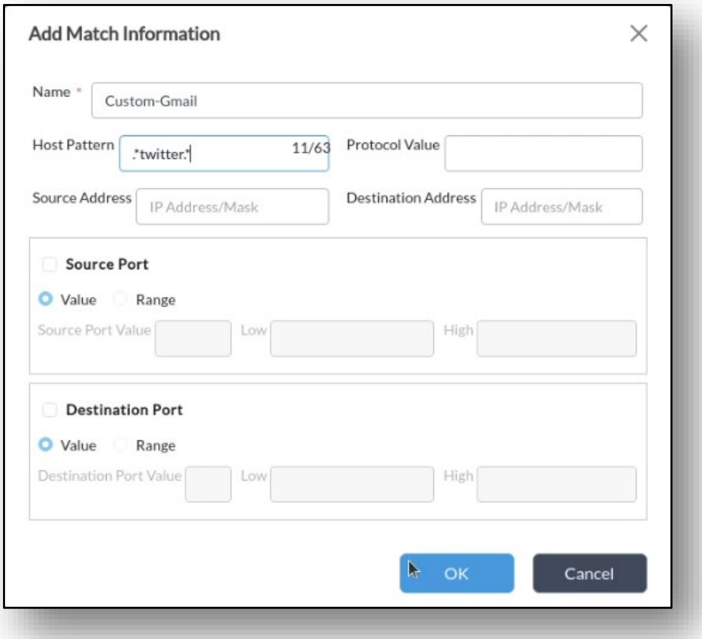
Description * Custom Twitter Application

Precedence * 100 Application Timeout (seconds) 120

□ Application match based on IPS signature

Attributes | Match Information

□	Name	Host Pattern	Source Address	Destination Address	Source Port Source Port Value	 Low	 High	 Destina
□	Custom-Gmail	.*twitter.*						



Add Match Information

Name * Custom-Gmail

Host Pattern .*twitter.* 11/63

Protocol Value

Source Address IP Address/Mask

Destination Address IP Address/Mask

□ Source Port

● Value ○ Range

Source Port Value

Low

High

□ Destination Port

● Value ○ Range

Destination Port Value

Low

High

Step 2.14: Create an access rule to block traffic that matches the custom application

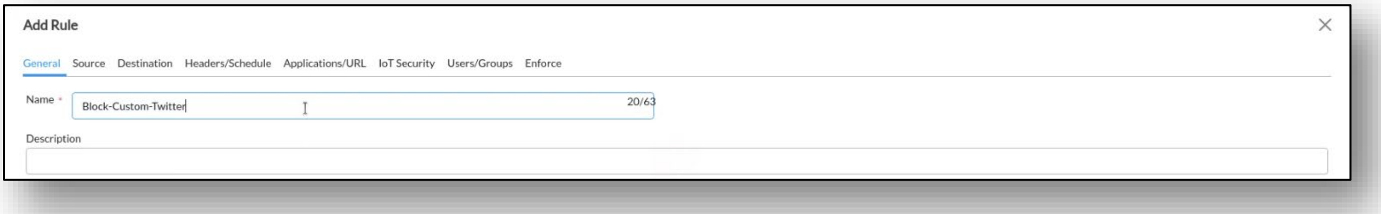
In the next steps you will configure a security access rule that uses the custom application to filter traffic.

In your appliance context, navigate to *Configuration > Services > Next Gen Firewall > Security > Policy*. In the Rules tab, click the + button to crate a new access rule with the following parameters:

Custom Application Security Rule	
Name:	Block-Custom-Twitter
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Application: Custom-Twitter-APP
Enforce:	Action: Deny Log Events: Both, Default Logging Profile

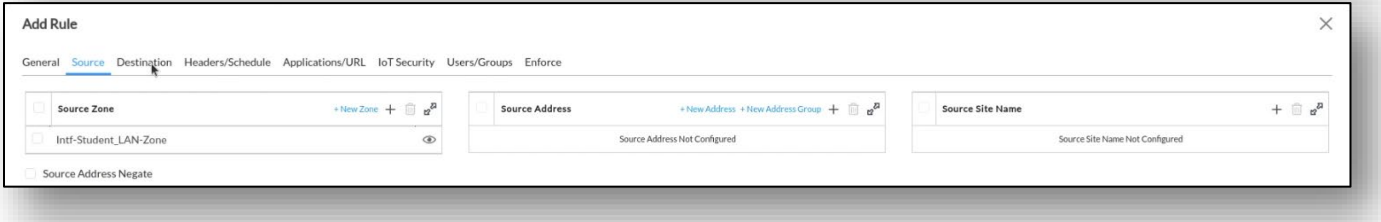
Click *OK* to create the access rule, then move it to the 4th position in the rule list.

Example Rule



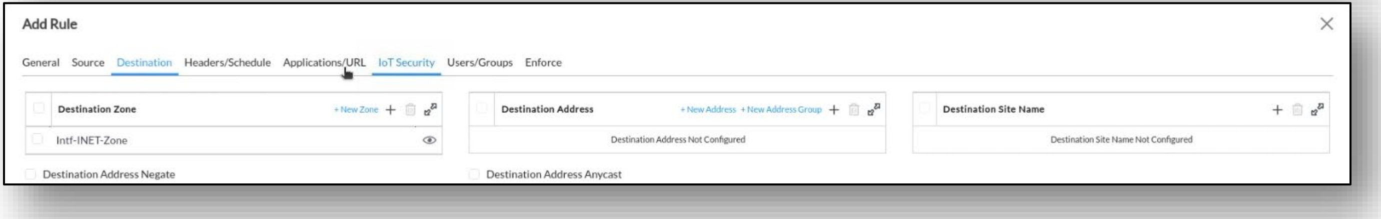
Name *: Block-Custom-Twitter 20/63

Description:



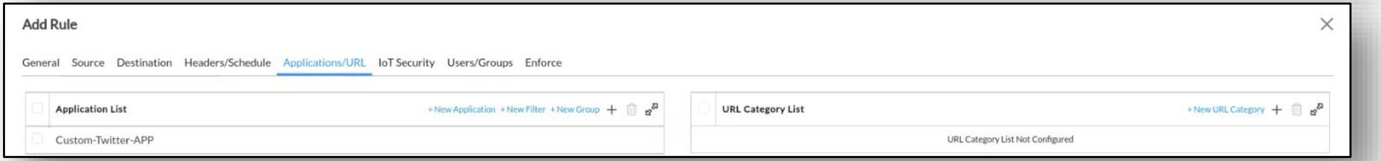
Source Zone	Source Address	Source Site Name
Intf-Student_LAN-Zone	Source Address Not Configured	Source Site Name Not Configured

□ Source Address Negate

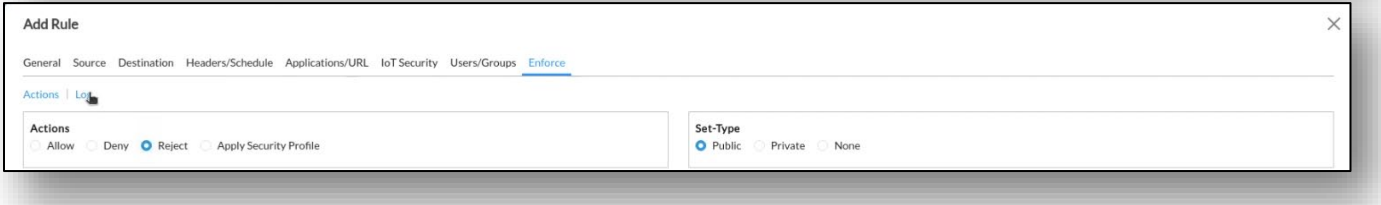


Destination Zone	Destination Address	Destination Site Name
Intf-INET-Zone	Destination Address Not Configured	Destination Site Name Not Configured

□ Destination Address Negate
□ Destination Address Anycast

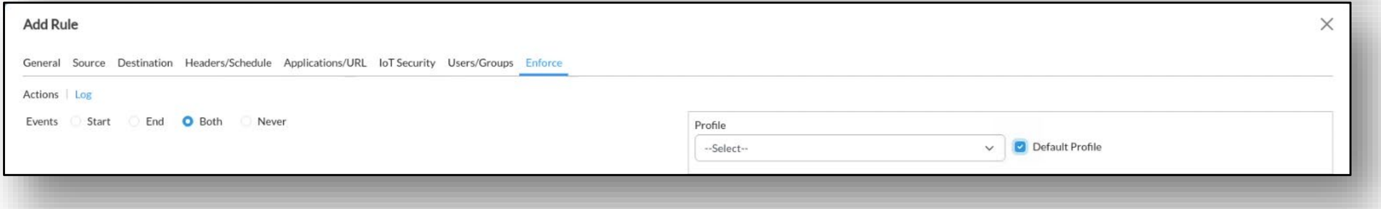


Application List	URL Category List
Custom-Twitter-APP	URL Category List Not Configured



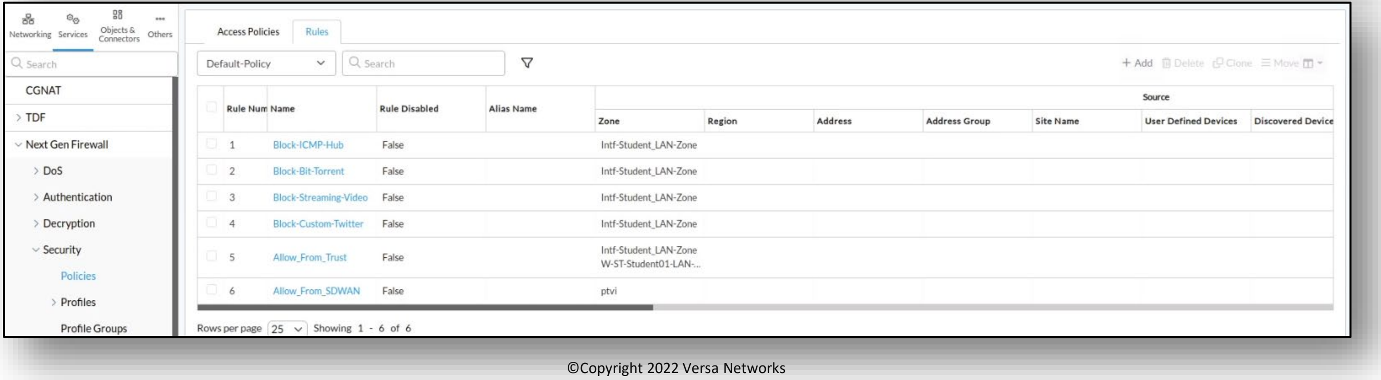
Actions: ○ Allow ○ Deny ● Reject ○ Apply Security Profile

Set-Type: ● Public ○ Private ○ None



Events ○ Start ○ End ● Both ○ Never

Profile: --Select-- ☑ Default Profile



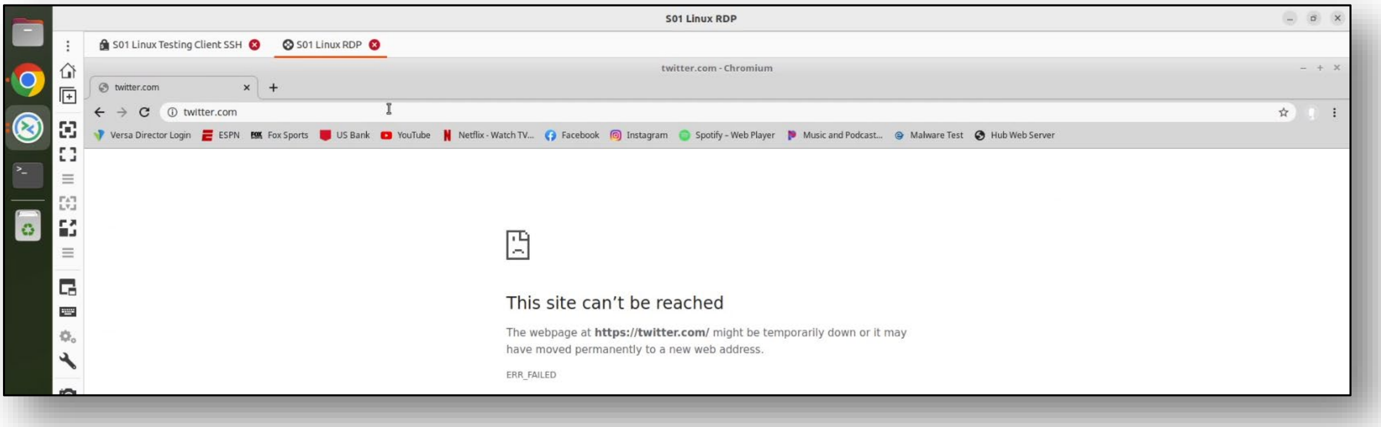
Rule Num	Name	Rule Disabled	Alias Name	Source Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device
1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone						
2	Block-Bit-Torrent	False		Intf-Student_LAN-Zone						
3	Block-Streaming-Video	False		Intf-Student_LAN-Zone						
4	Block-Custom-Twitter	False		Intf-Student_LAN-Zone						
5	Allow_From_Trust	False		Intf-Student_LAN-Zone W-ST-Student01-LAN-...						
6	Allow_From_SDWAN	False		ptvi						

Rows per page 25 Showing 1 - 6 of 6

Verify that the access rule blocks Twitter traffic

In the next steps you will verify that the access rule you created blocks the desired traffic.

In the remote landing station, return to the remote desktop session to the testing host. On the testing host, open the Chromium web browser and enter the URL *https://twitter.com* in the address bar. The page should not open.



This site can't be reached

The webpage at **https://twitter.com/** might be temporarily down or it may have moved permanently to a new web address.

ERR_FAILED

Step 2.16: Verify the access rule statistics in Versa Director

Return to Versa Director. From your appliance context mode, navigate to *Monitor > Services > NGFW > Policies*. Examine the counters for the *Block-Custom-Twitter* access rule. The hit count and deny count should be non-zero values.

Step 2.17: Verify the access rule logs in Versa Analytics

Click the *Home* button next to your appliance name to exit appliance context mode. From the main Versa Director dashboard, navigate to *Analytics > Logs > Firewall*. Ensure that the *Tenant1* organization is selected in the organization filter box at the top of the dashboard.

In the firewall log window, click the *Search* box and enter a filter for the rule *Block-Custom-Twitter*. Only log entries associated with the *Block-Custom-Twitter* access rule should be displayed. Analyze the log entries to verify that the action for the entries is deny, and that the rule *Block-Custom-Twitter* is the rule that applied the action. Look for the source address of the local LAN connected to your branch to verify that traffic from your testing host is listed.

Step 2.18: Finish the lab and exit the lab environment

To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.

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

URL Filtering

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.

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.

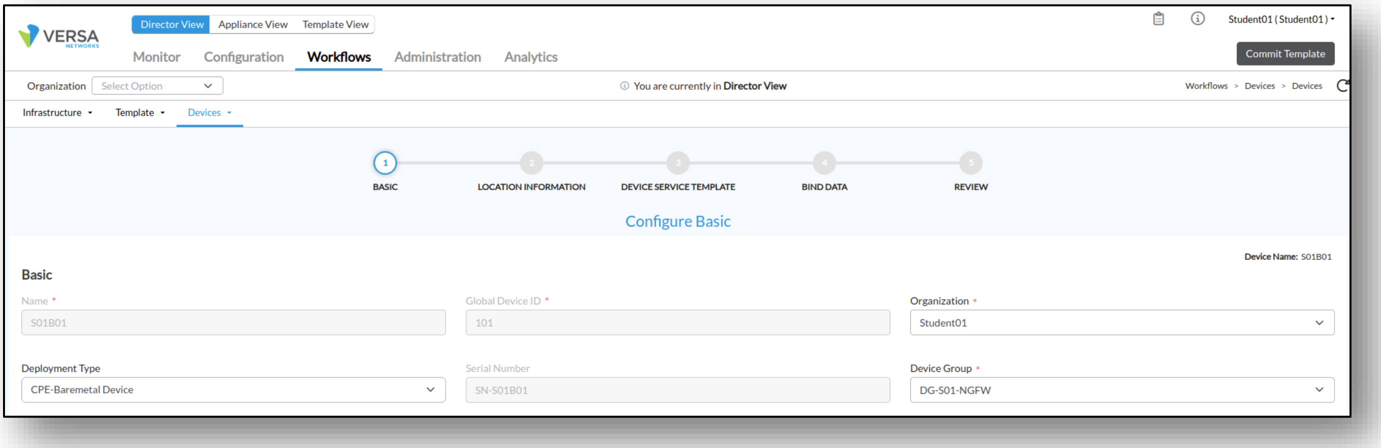
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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!

Step 1.1: Verify that your device is in the base device group

In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Configure Basic

Device Name: S01B01

Basic

Organization: Select Option

Name *: S01B01

Global Device ID *: 101

Organization *: Student01

Deployment Type: CPE-Baremetal Device

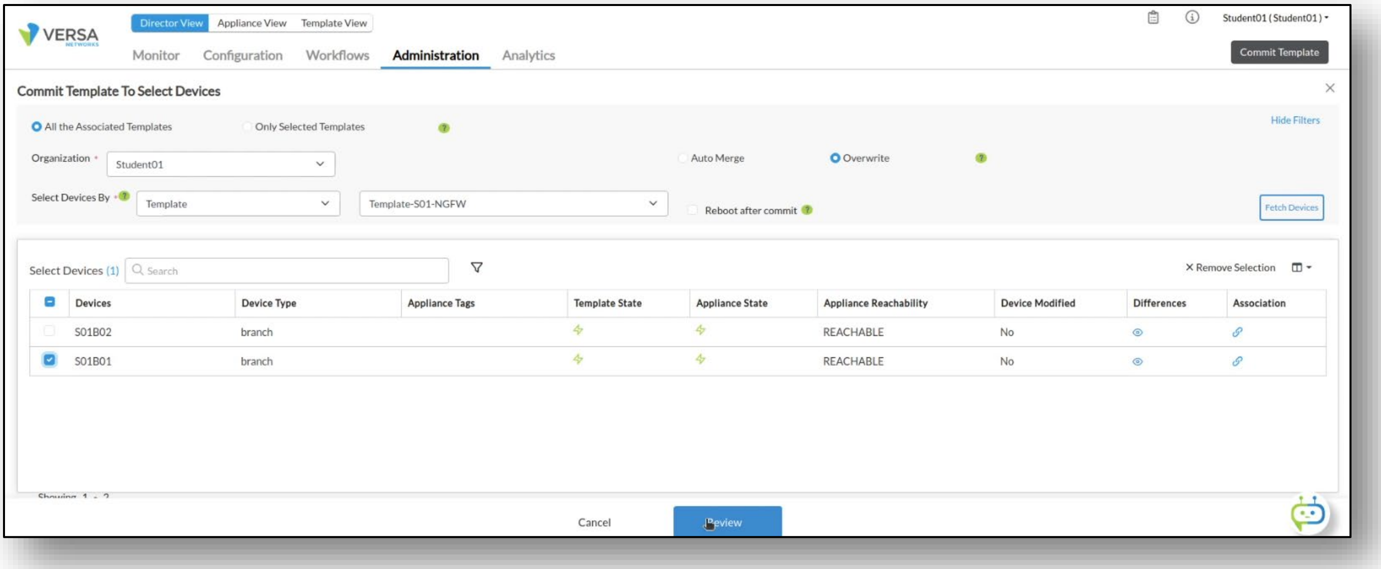
Serial Number: SN-S01B01

Device Group *: DG-S01-NGFW

Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select your student ID as the organization, the template *Template-Sxx-NGFW*, and click Fetch Devices to display your devices.

Select your devices in the device list and click *Review,* then in the Review window click Commit to apply the base configuration to your device.



Commit Template To Select Devices

● All the Associated Templates ○ Only Selected Templates

Organization *: Student01

○ Auto Merge ● Overwrite

Select Devices By *: Template | Template-S01-NGFW

□ Reboot after commit

Select Devices (1)

	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
□	S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
☑	S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

Showing 1 - 2

Step 2.1: Configure cloud lookup for current URL reputations

In the next steps you will configure a URL lookup profile to retrieve current URL categories from the cloud database. You will perform all configuration steps in appliance context mode so that the configuration changes apply only to your device. In a production environment, the same configuration steps would be used with the device templates in order to apply the configuration to multiple devices.

Form the Versa Director main dashboard, navigate to I and locate your B01 appliance in the table. Click your appliance name to open the appliance context mode for the appliance.

In appliance context mode, navigate to *Configuration > Objects & Connectors > Objects > SNAT Pool* to define a NAT pool to allow the device to communicate with the cloud service. Click the + button to create a new NAT pool with the following parameters:

NAT Pool Properties	
Name:	Cloud-NAT-Pool
Routing-Instance:	Tenant1-LAN-VR
Egress Networks:	INET

Click *OK* when finished.

To create the cloud lookup profile, navigate to *Objects & Connectors > Objects > Cloud Profiles* and click on the + button to create a new cloud profile with the following parameters:

Cloud Profile	
Name:	Cloud-URL-Profile
Connection Pool:	100
Source NAT Pool:	Cloud-NAT-Pool
Type:	Urlf-cloud-profile
Activation:	Check the activation button

Click *OK* to finish creating the cloud profile.

Step 2.2: Create a cloud lookup URL profile for use in access rules

In the next steps you will create a URL profile that uses the cloud profile for URL lookups.

In the appliance context configuration window, navigate to *Services > Next Gen Firewall > Security Settings > URL-Filtering* and click the edit button ✎ to modify the settings.

Select the *Cloud Lookup* tab and enter the following parameters:

Cloud Lookup Parameters	
Cloud Lookup Profile:	Cloud-URL-Profile
Cloud Lookup Mode:	Asynchronous
Cache Time To Live:	21600
Timeout:	1000
Cloud Lookup State:	Check the activation button

Click *OK* when finished.

Click I to save the settings. Cloud Lookup for URL categories has been enabled on the appliance.

Step 2.3: Create URL filtering profiles to match URLs and block malware sites

In the next steps you will create a URL filtering profile that defines actions to take on malware sites.

In your appliance context mode, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > URL-Filtering*. Create a URL filtering profile with the following parameters:

URL Filtering Profile Parameters	
Name:	URLF-Profile
Default Action:	Allow
Cloud Lookup State:	Check the Cloud Lookup State box
LEF Profile:	Default-Logging –Profile
Category Based Action:	Click the + button and enter the following details in the pop-up window: Name: BLOCK-CATEGORIES Action: Block Predefined Categories: Click the + button and add the following categories: -malware_sites -sports -news_and_media -social_network

Click the *OK* buttons until you have finished creating the URL filtering profile. The URL filtering profile can now be used by access rules to filter traffic based on the URL category.

Step 2.4: Create access rules to filter the URLs listed in the URL Filtering Profile

In the next steps you will use a security access rule to match web traffic and send it through the URL Filtering profile for additional scanning. The URL Filtering profile will scan the traffic for the specified URL categories. It will allow traffic that does not match the URL categories and block traffic that matches the URL categories defined in the profile.

Navigate to the *Services > Next Gen Firewall > Policies* hierarchy and open the *Rules* tab to add new rules to the default security policy.

In the Rules tab, click the + button to add the following rule to the policy:

Access Rule Parameters	
Name:	URL-IP-Filtering-Rule
Source/Destination:	Source Zone:intf-Student_LAN-Zone Destination Zone: intf-INET-Zone
Headers/Schedule:	Add the following services: domain, http, https
Enforce:	Action: Apply Security Profile Select Profiles > URL Filtering > URLF-Profile Logging: Both, Default-Logging-Profile

Click *OK* to finish configuring the rule, then ***move the rule to the top of the rule list*** so that it is evaluated first.

Step 2.5: Test the URL filtering

In the next steps you will verify the URL filtering profile. You will do this by logging into the testing host connected to your assigned branch device.

In the remote desktop, click on the Remmina icon in the left application bar. In the Remmina application, open the RDP session to the Linux testing host. If prompted, the username is ***student*** and the password is ***versa123***:

On the testing host desktop, open the Chromium Web Browser application.

From within the Chromium web browser, enter the following URL in the address bar:

`https://facebook.com`

The site should be blocked by the VOS device.

Browse to `https://espn.com`

The site should be blocked.

Browse to `https://instagram.com`

The site should be blocked.

Browse to `https://spotify.com`

The site should be allowed.

Step 2.6: Update the URL filter profile to block music sites

The Spotify web site was available, but now it needs to be blocked.

To block the Spotify web site, you will add the URL category *music* to the existing URL profile. To do so, return to Versa Director and navigate to appliance context mode.

From the configuration dashboard in the appliance context mode of your device, navigate to *Services > Next Gen Firewall > Security > Profiles > URL Filtering* to view the URL filtering profile table. Select the *URLF-Profile* profile to modify the profile. Add the music category to the *Category Based Action > BLOCK-CATEGORIES > Predefined Categories* list. The list should now contain malware_sites, sports, news_and_media, social_network, and music categories.

Click the *OK* buttons until you finish updating the URL filter profile.

Step 2.7: Test your changes to the URL Filter profile

Return to the remote desktop connection to the testing host, and if the Chromium web browser is open, close the browser and then re-open the Chromium web browser.

From the Chromium web browser, enter `www.spotify.com` in the address bar to attempt to access the Spotify web site. The site should now be blocked.

Step 2.8: Verify the URL filtering using Versa Director and Versa Analytics

Return to Versa Director.

From Versa Director, navigate to the appliance context mode for your branch appliance.

From the appliance context mode, navigate to *Monitor > Services > NGFW > URL Filtering* and choose *User Defined Profiles* from the drop-down menu. You may have to use the arrows on the Services row to scroll right to find the URL Filtering tab. This will display URL filtering counters and statistics and should show the number of rule hits in the URL filtering. You should see several

In the statistics table you should see many total hits and some Total Default Action hits. You should also see some Total URL Category Actions and some Total URL PreDefined Category Actions.

Click the Director View button to return to the main Versa Director dashboard. From the main Versa Director dashboard, then click the Analytics tab to open the Analytics dashboard.

From the main Analytics dashboard, navigate to *Dashboards > Security > Web*, then select the URL Categories tab. You should see URL category information.

Navigate to the *Logs > Threat Filtering* dashboard to view the Threat Filtering logs. Select the URL Filtering tab from the Threat Filtering window.

Examine the URL Filtering log entries. You should see entries for Spotify and other URLs. Some of the URLs may be to sites that you didn't browse to, but that may have been embedded or linked to in the web pages. Verify that the URL category is one of the categories that you included in the URL profile. You can verify which session originated on your testing LAN by examining the source address of the sessions. You may also see some of the URLs with an "allow" action. This is because the main firewall process (security rule) passed the traffic on to the URL filtering profile, where the URL filtering profile performed the Block action (as indicted in the Threat Filtering Logs).

Note: When you browse the Internet, many sessions are created to linked or embedded web page components, so there may be too many entries in the log files to view on one page. You can view more entries by changing the Show x entries value in the top-right of the table or by adding filter parameters, such as sports or social_media. The keyword in the search filter must be the complete word (the search does not perform partial matches.)

Step 2.9: Finish the lab and exit the lab environment

To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.

Log out of Versa Director.

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

IP Filtering

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.

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.

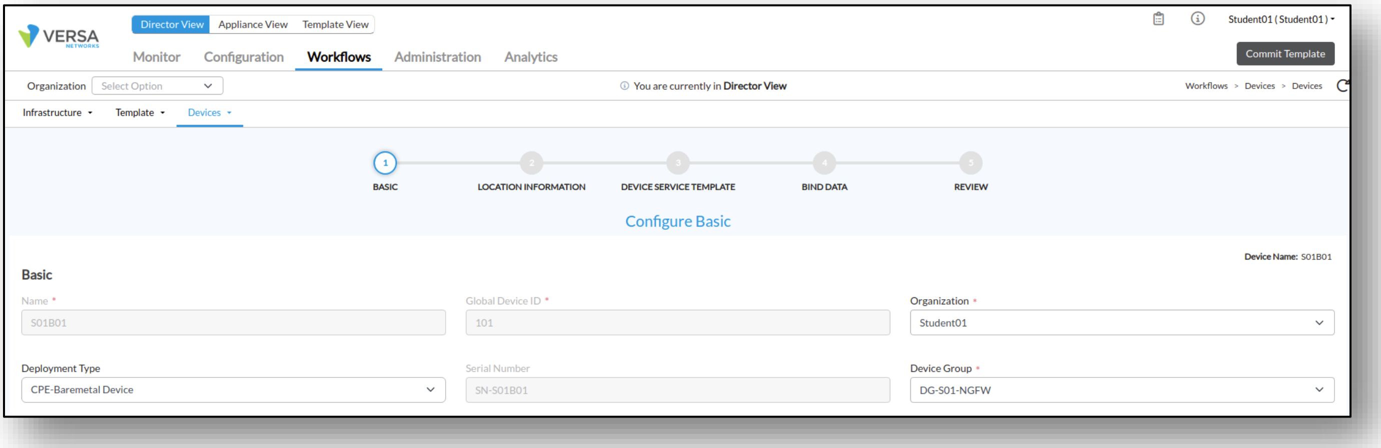
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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!

Step 1.1: Verify that your device is in the base device group

In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Organization: Select Option

Configure Basic

Device Name: S01B01

Basic

Name *: S01B01

Global Device ID *: 101

Organization *: Student01

Deployment Type: CPE-Baremetal Device

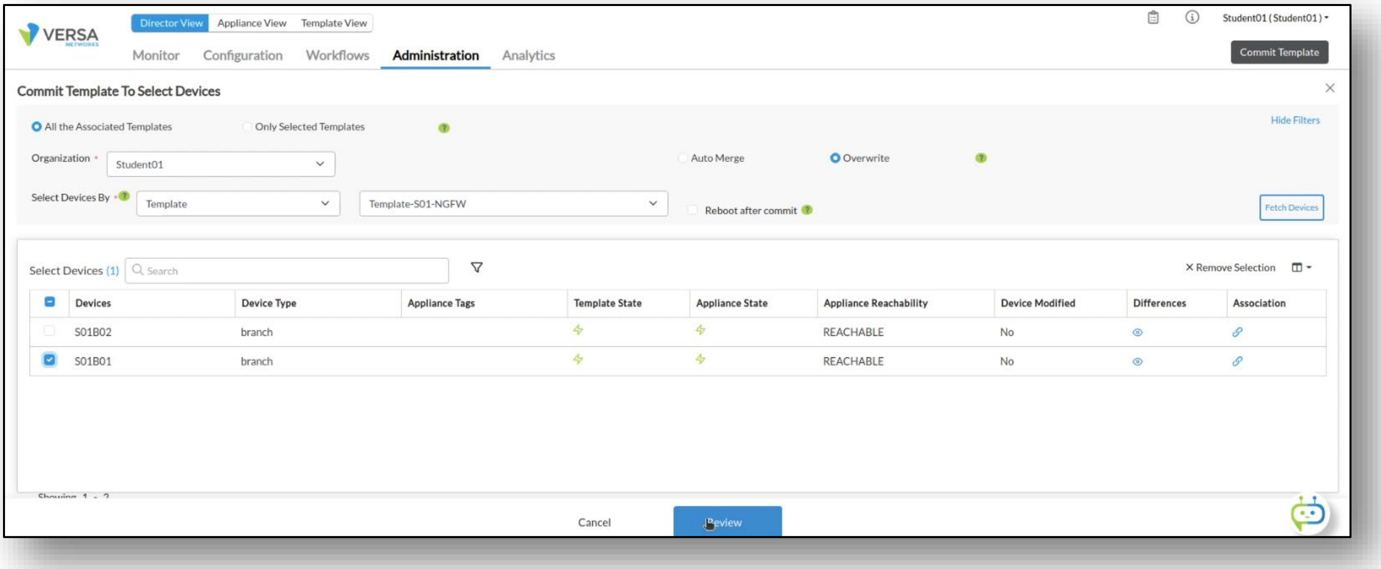
Serial Number: SN-S01B01

Device Group *: DG-S01-NGFW

Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select your student ID as the organization, the template *Template-Sxx-NGFW*, and click Fetch Devices to display your devices.

Select your devices in the device list and click *Review,* then in the Review window click Commit to apply the base configuration to your device.



Commit Template To Select Devices

● All the Associated Templates ○ Only Selected Templates

Organization *: Student01

○ Auto Merge ● Overwrite

Select Devices By *: Template | Template-S01-NGFW

□ Reboot after commit

Select Devices (1) Search

☐	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
☐	S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
☑	S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

Showing 1 - 2

Step 2.1: Check the IP Filtering profiles in the pre-defined database on the branch device

In the next in the steps you will examine the pre-defined IP filtering profiles in the device template. The IP Filtering profiles are located in the *Objects & Connectors > Objects > Pre-defined > IP Filtering Profile* hierarchy of the appliance configuration.

From the Versa Director user interface, click the Appliance View tab. Locate and click on your appliance in the appliance list to open the appliance context mode for your appliance. You will perform the configuration tasks in this lab directly on your appliance. Navigate to *Configuration > Objects & Connectors > Objects > Pre-defined > IP Filtering Profile* hierarchy. You will see a list of pre-defined IP Filtering profiles.

Each IP Filtering profile has a set of match types, reputation based actions, and profile actions. They are displayed le table.

Step 2.2: Create a custom IP Filter profile

In the next steps you will create a custom IP Filter profile for use in a security access policy. The custom IP Filter profiles are defined under the *Services > Next Gen Firewall > Profiles > IP Filtering* hierarchy of the template or device configuration.

Navigate to the *Services > Next Gen Firewall > Security > Profiles > IP Filtering* hierarchy of the template. Click the + button to add a new IP filter profile with the following parameters:

IP Filter Profile	
Name:	IP-Filtering-Profile
Default Action:	Allow
LEF Profile:	Default-Logging-Profile
Prioritize URL Reputation:	Uncheck the box
Deny List Action:	Reject
IP Address:	Click the + New Address button and create a new address in the Deny List with the following properties: Name: deny-list-address Address: 10.27.11.100 The address should be added to the IP address list when finished
Match Type:	Match Source or Destination

Click OK to finish creating the profile.

Step 2.3: Create an access policy that uses the IP Filter profile

In the next steps you will create an access policy rule that matches specified traffic and directs it towards the IP Filter profile for further analysis. The IP Filter profile will determine whether the traffic will be allowed or denied.

Navigate to the *Services > Next Gen Firewall > Security > Policies* hierarchy and ensure that the Rules tab is selected. Click the + button to add a new access rule with the following parameters:

Access Policy Rule Parameters	
Name:	IP-Filtering-Rule
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: Intf-INET-Zone
Headers/Schedule:	Services: domain, http, https, ICMP
Enforce:	Action: Apply Security Profile Select IP Filtering and the IP-Filtering-Profile Logging: Both, select the Default-Logging-Profile

Click OK to create the rule. When you are finished creating the rule, ***move the rule to the top of the rule list*** so that it is processed first.

Step 2.4: Adjust the default NAT rules

When NAT is automatically configured through the DIA configuration, a default rule is put in place that prevents the translation of RFC1918 (private) routes. Because our lab environment uses private routes, you will have to modify the NAT translation rule so that the 10.27.0.0/16 prefixes will match the DIA NAT rule.

Navigate to the Services > CGNAT hierarchy of your appliance configuration. Select the Rules tab from the CGNAT table. Locate the RFC_1918_NoTranslate NAT rule in the table and click on the rule to open and modify the rule.

In the RFC_1918_NoTranslate rule, select the Match tab. In the Match tab, select and delete the 10.0.0.0/8 address from the Source IP Address and Destination IP Address fields, the click OK to finish modifying the rule.

Step 2.5: Test the IP Filter profile

In the next steps you will verify the IP filtering profile. You will do this by logging into the testing host connected to your assigned branch device.

In the remote desktop, click on the Remmina icon on the left application bar to the Remmina. Open the remote desktop session to the Linux testing host assigned to your branch. The login for the remote desktop is username ***student*** and password ***versa123***.

On the testing host, use the Terminal icon on the desktop to open a terminal window.

The scripts for this lab are located in the ./VASEC/ directory. Type cd ./VASEC/ to move to that directory.

From the terminal session, issue the command **./ip-filtering-blacklist.sh** to run the blacklist test script. The script will attempt to initiate different types of traffic sessions to the blacklisted device.

Step 2.6: Verify the IP filter profile in Versa Director

In the next steps you will verify that your branch appliance processed the test traffic and applied an action on the traffic.

Return to the Versa Director dashboard on the remote landing station. From your appliance context mode, navigate to *Monitor > Services > NGFW*. Select the Policies tab.

In the *Policies* tab, ensure that the *Default-Policy* is selected and examine the IP-Filtering-Rule counters. You should see packets in the *Hit Count* field. This indicates that the policy has matched and processed traffic.

Select the *IP Filtering* tab, then choose *User Defined* from the drop-down field to view the user defined IP Filtering-Profile.

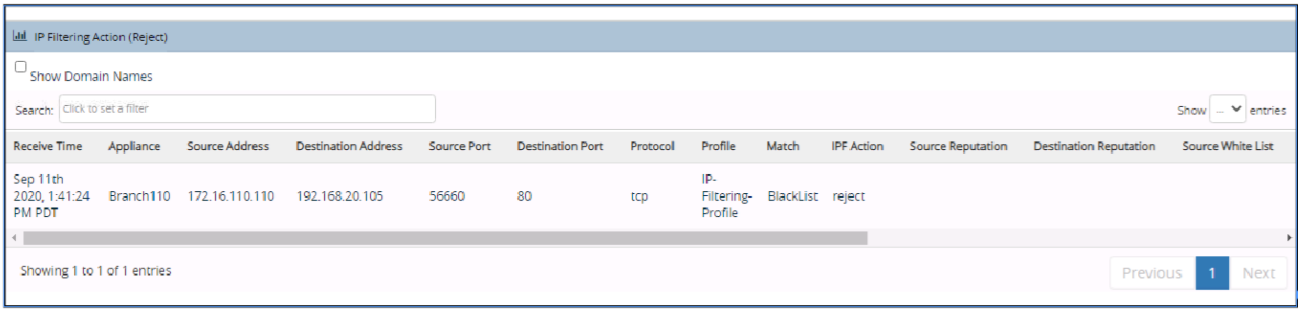
In the *IP-Filtering-Profile* you should see a filter hit count and a *BlackList Hit Count*. Both values should be non-zero. You should also see a non-zero *Drop Count* value.

Step 2.7: Verify the IP Filter profile in Versa Analytics

Click the Director View button to exit device context and return to the main Versa Director dashboard. From the main Versa Director dashboard, navigate to Analytics

In the Versa Analytics dashboard, navigate to *Dashboards > Security > Threats* and select the IP tab. You should see a reject field in the Top IP Filtering Action chart. Click the reject icon in the graphic to open more detailed information.

A new threat window should open that displays a hit count and that has a receive time in the list similar to the graphic below. You can filter this further by using the source address of your LAN.



IP Filtering Action (Reject)

□ Show Domain Names

Search: Click to set a filter

Show ... entries

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action	Source Reputation	Destination Reputation	Source White List
Sep 11th 2020, 1:41:24 PM PDT	Branch110	172.16.110.110	192.168.20.105	56660	80	tcp	IP-Filtering-Profile	BlackList	reject			

Showing 1 to 1 of 1 entries

Navigate to *Logs > Threat Filtering* and open the IP Filtering tab. You should see the IP Filtering log entry. Click the 🔍 icon to expand the log details. You should see multiple entries. The entry types may differ, but the Versa Analytics platform correlates the log entries into multiple entries related to the same flow.

Step 2.8: Add geo-location to the IP Filtering profile

In the next steps you will add geo-location information to the IP Filter profile to filter traffic based on the location of the IP address.

Click on the Appliance View button, then select your B02 appliance from the list. In your appliance context mode, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > IP Filtering*. Open the profile IP-Filtering-Profile and add the following Geo IP Based Actions parameters:

IP-Filtering-Profile Geo IP Based Actions	
Name:	Drop-Region
Action:	Drop-packet
Match Type:	Match Source or Destination
Regions:	Click the + button and select Russia

Click OK to apply the changes.

Step 2.9: Test the geo-location IP Filtering profile

In the next steps you will connect to the testing host, open a shell prompt, and run a testing script to generate traffic, which includes traffic to a registered Canada IP address. Then you will verify that the IP Filter profile identifies and blocks traffic from the Canada geo-location.

On the landing station, return to the remote desktop session to the testing host. If a shell prompt is not already open, open a new shell prompt using the Terminal icon on the desktop.

From the terminal window, issue the command `./ip-filtering-region-block.sh` to run the test script. The script will issue a series of 5 ICMP packets to an IP address registered to the Russia geo-location. The script should time out.

Step 2.10: Verify the Geo-location IP Filter results

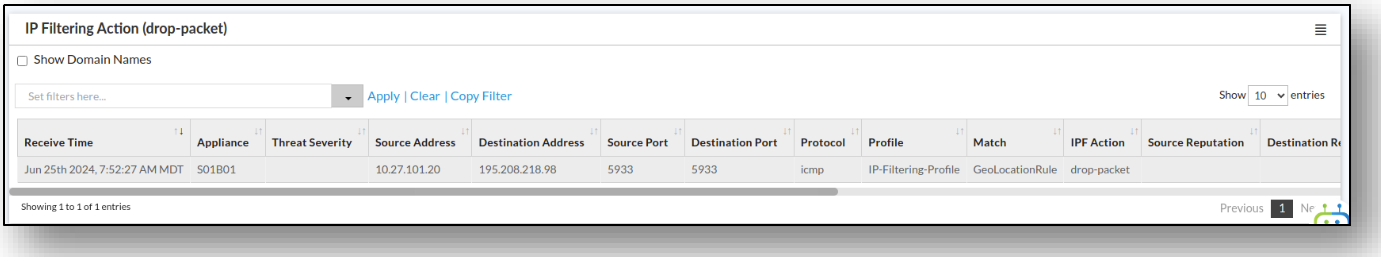
Return to Versa Director. In Versa Director, open the appliance context mode for your appliance.

From your appliance context, navigate to *Monitor > Services > NGFW > IP Filtering* and select *User Defined* in the drop down list. You should see the IP-Filtering-Profile statistics. Verify that the Geoip Rule Hit Count is a non-zero value. This indicates that the Geo-IP parameters were matched in the traffic.

Click the Director View button to return to the main Versa Director dashboard. From the Versa Director dashboard, Navigate to *Analytics > Dashboards > Security > Threats*, then select the IP tab to display the IP threat dashboard.

You should see drop-packet in the Top IP Filtering Action panel. Click the drop-packet graphic to open the details about the top action.

In the Events (Drop-Packet) dashboard, you should see hits. Scroll down in the dashboard until you see the action details.



IP Filtering Action (drop-packet)

□ Show Domain Names

Set filters here... Apply | Clear | Copy Filter Show 10 entries

Receive Time	Appliance	Threat Severity	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action	Source Reputation	Destination Re
Jun 25th 2024, 7:52:27 AM MDT	S01B01		10.27.101.20	195.208.218.98	5933	5933	icmp	IP-Filtering-Profile	GeoLocationRule	drop-packet		

Showing 1 to 1 of 1 entries

Previous 1 Ne

Example Output

You can identify traffic from your appliance by the appliance name or source IP address.

Scroll the panel to the right to view the drop action details. The Match reason should state GeoLocationRule and the Destination Country field should list Russia.

Step 2.11: Add IP Reputation to the IP Filtering profile

In the next steps you will add IP Reputation to the list of rules in the IP filtering profile. You will then run a script on the test host that will attempt to connect to known bad-reputation web sites. You will then verify and monitor the results.

In Versa Director, navigate to your appliance context mode. In your appliance context mode, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > IP Filtering*. Select the IP-Filtering-Profile from the table to open and edit the profile.

You will be adding IP Reputation Based Actions to the filtering profile. Add the following Reputation Based Actions to the profile:

IP-Filtering-Profile Reputation Based Actions	
Name:	Bad-IPs
Predefined Action:	Drop Packet
Match Type:	Match Source or Destination
URL Reputations:	Click the + button and add the following: -Web Attacks -Phishing -Spam Sources -Windows Exploits -BotNets -Denial of Service -Scanners

Click OK to finish updating the profile.

Step 2.12: Test the IP Reputation profile

From the remote landing station, open the remote desktop session to the Linux testing host. From the terminal window in the testing host, issue the command `./ip-filtering-reputation-block.sh` to run the IP reputation test script. Two sessions should be attempted, and both should time out.

Return to the Versa Director dashboard. In the Versa Director dashboard, navigate to your appliance context mode. From your appliance context mode, navigate to *Monitor > Services > NGFW* and select the IP Filtering tab. Select User Defined in the table drop down box to view the IP-Filtering-Profile statistics. You should see that the hit count for the *Reputation Rule* has increased (is non-zero). This indicates that the IP Reputation of traffic crossing the device violated the reputation rules.

Click the *Director View* button to exit appliance context mode and return to the main Versa Director dashboard. From the Versa Director dashboard, navigate to the *Analytics > Dashboards > Security > Threats* dashboard. Select the *IP* tab from the dashboard to view IP filtering statistics.

Mouse over the Top *IP Filtering Action > drop-packet* chart. The popup will display how many rule hits have been counted. Click on the *drop-packet* chart to open the drop-packet details.

Scroll down to the action entries. The most recent entries should indicate a match on *ReputationRule* for your branch device.

Step 2.13: Finish the lab and exit the lab environment

To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.

Log out of Versa Director.

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

Antivirus and IDP

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.

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.

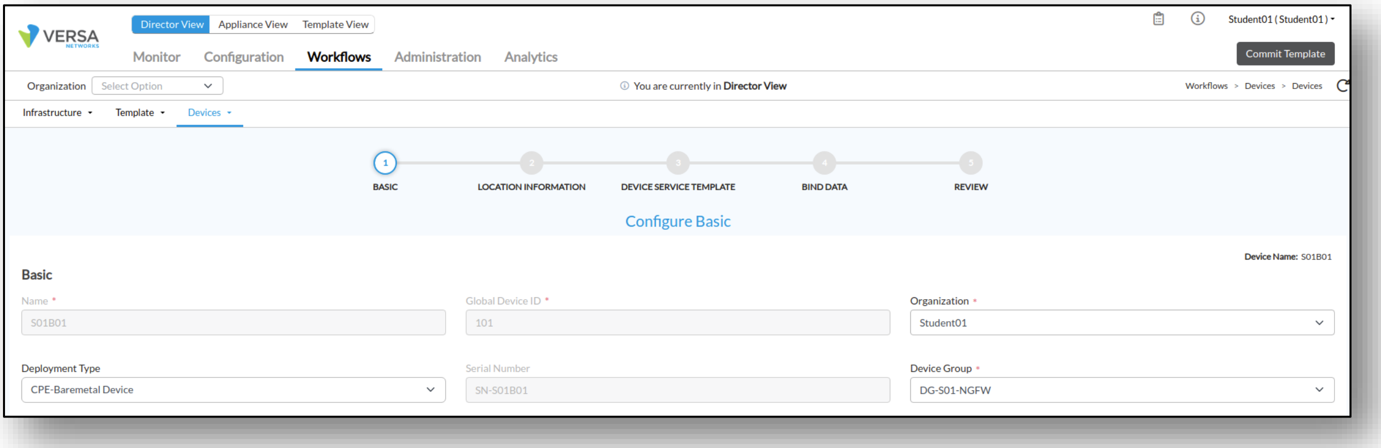
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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!

Step 1.1: Verify that your device is in the base device group

In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Organization: Select Option

You are currently in **Director View**

Configure Basic

Device Name: S01B01

Basic

Name *: S01B01

Global Device ID *: 101

Organization *: Student01

Deployment Type: CPE-Baremetal Device

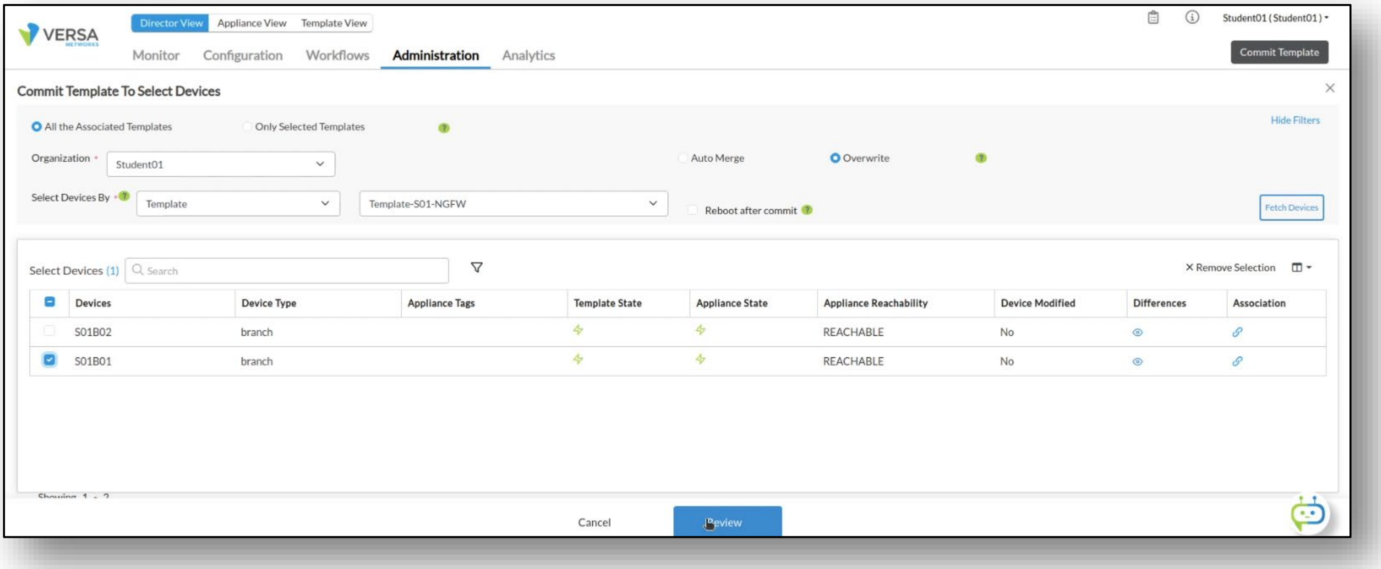
Serial Number: SN-S01B01

Device Group *: DG-S01-NGFW

Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select your student ID as the organization, the template *Template-Sxx-NGFW*, and click Fetch Devices to display your devices.

Select your devices in the device list and click *Review,* then in the Review window click Commit to apply the base configuration to your device.



Commit Template To Select Devices

● All the Associated Templates ○ Only Selected Templates

Organization *: Student01

○ Auto Merge ● Overwrite

Select Devices By *: Template — Template-S01-NGFW

□ Reboot after commit

Select Devices (1)

☐	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
☐	S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
☑	S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

Showing 1 - 2

Step 2.1: Configure SSL Decryption using SSL Forward Proxy

In order to analyze encrypted sessions, SSL Decryption must be enabled on the branch device. In the next steps you will verify that an SSL self-signed certificate is present on your appliance. If the SSL certificate is not present, refer to the lab SSL Encryption and Decryption for instructions on how to generate a self-signed SSL certificate and import the certificate into the testing host web browser.

To verify that an SSL certificate is present on your appliance:

In Versa Director, click on Appliance View and select your B01 appliance from the list.

From your appliance context mode, navigate to *Configuration > Objects & Connectors > Objects > Custom Objects > Certificates*. From the Certificates dashboard, select the *Appliance* tab. If there is not an SSL certificate on the device, perform the following steps to create the certificate:

Navigate to *Keys* in the Custom Objects hierarchy. Create an Appliance Key with the following properties:

- Name: ssl-key
- Type: RSA
- Type: 2048
- Pass Phrase: versa123

Navigate to Certificates in the Custom Objects hierarchy. Create an Appliance certificate with the following properties:

- Certificate Name: ssl-cert
- CA Certificate: True
- Serial#: 123456
- Common Name: versanetworks.com
- Private Key Name: ssl-key

When the time comes to test the security services, you will need to import the certificate into the browser in the Linux testing machine. Instructions will be given at that time.

Step 2.2: Test HTTPS access to an Internet site

On the Linux testing client, open a Chromium web browser window on the testing host.

If you need to import the certificate you just created, click the Versa Director bookmark in the remote browser. Log into Versa Director with your student ID and password.

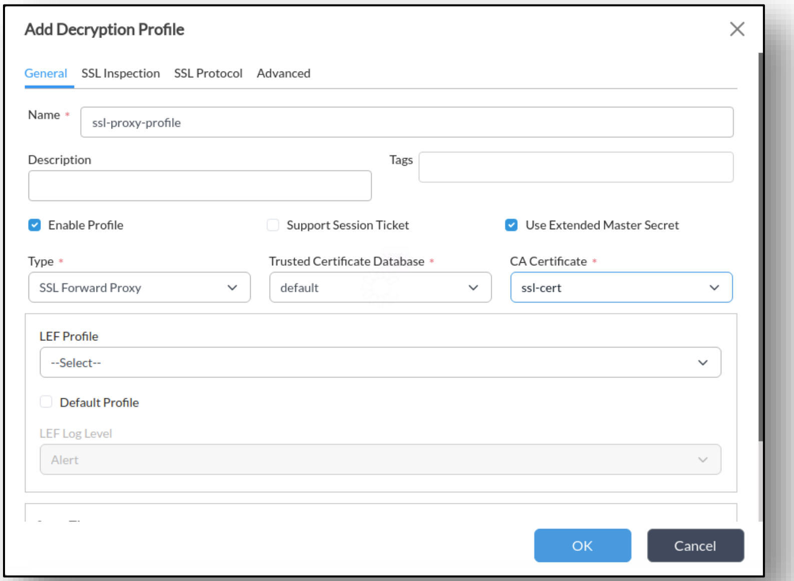
Navigate to the *Objects & Connectors > Custom Objects > Certificates > Appliance* page and export the certificate to the Linux testing client. The certificate will be placed in the Downloads folder of the Linux testing client.

To import the certificate into the browser, click on the 3 dots in the top right corner of the remote browser (on the Linux testing client), select Settings, and enter certificates in the settings search bar. Scroll down to the Manage certificates section.

In the Manage Certificates window, select the Authorities tab, then click Import to import the certificate. Set it to be used to authenticate web sites and email. Once the certificate is imported, you can continue with the lab.

Next you will create an SSL Decryption profile and policy to proxy SSL sessions.

Return to the Versa Director browser window in the main remote desktop. In Versa Director, in the Appliance View of your B01 device, navigate to Service > Next Gen Firewall > Decryption > Proxy Profiles. Create a new proxy profile with the following parameters:



Add Decryption Profile

Name * ssl-proxy-profile

Description

Tags

☑ Enable Profile

□ Support Session Ticket

☑ Use Extended Master Secret

Type * SSL Forward Proxy

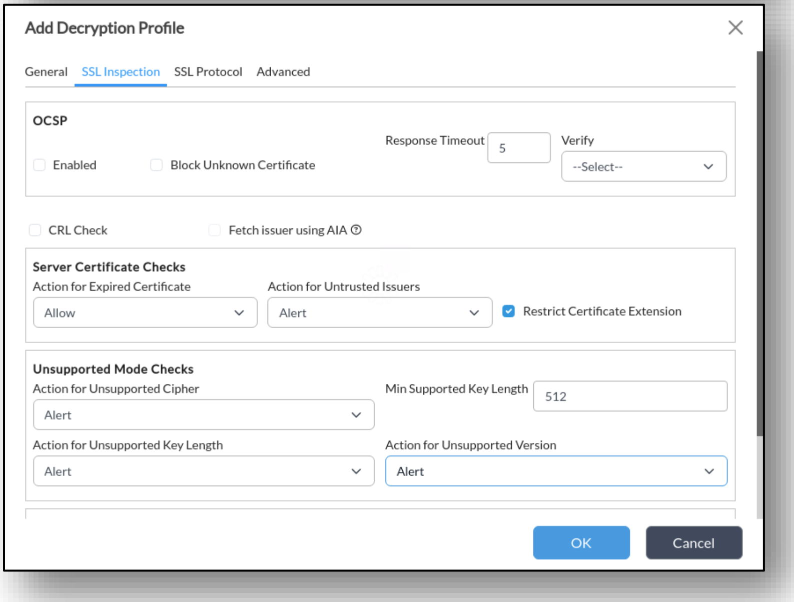
Trusted Certificate Database * default

CA Certificate * ssl-cert

LEF Profile --Select--

□ Default Profile

LEF Log Level Alert



Add Decryption Profile

OCSP

□ Enabled

□ Block Unknown Certificate

Response Timeout 5

Verify --Select--

□ CRL Check

□ Fetch issuer using AIA

Server Certificate Checks

Action for Expired Certificate: Allow

Action for Untrusted Issuers: Alert

☑ Restrict Certificate Extension

Unsupported Mode Checks

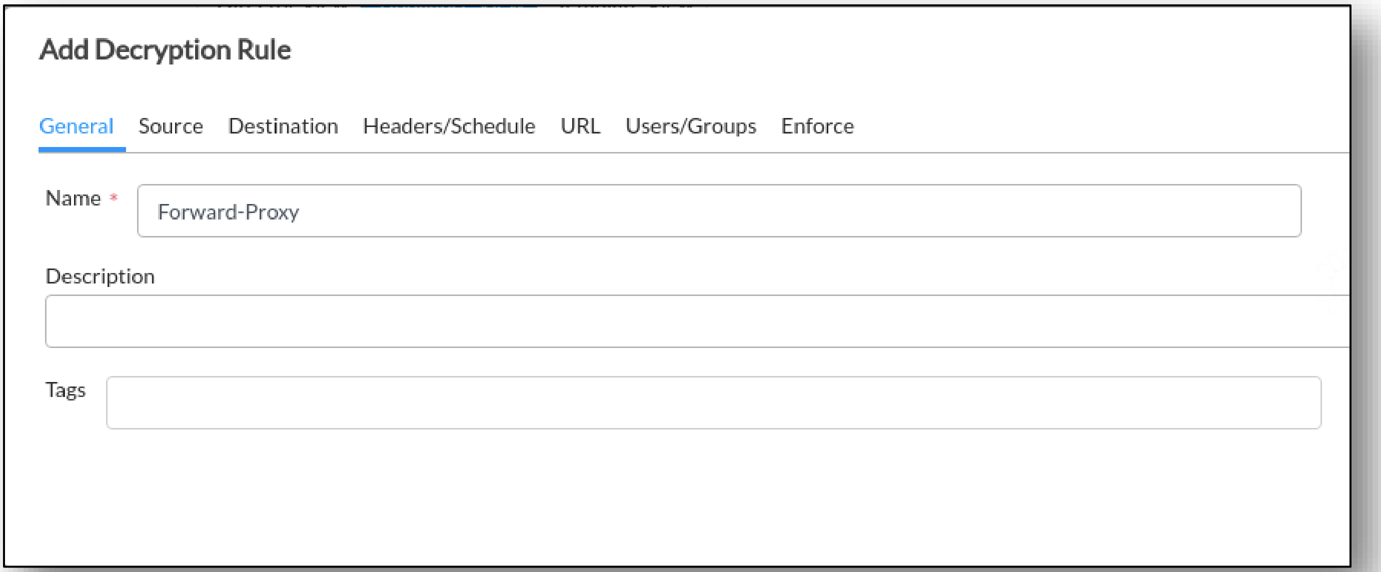
Action for Unsupported Cipher: Alert

Min Supported Key Length: 512

Action for Unsupported Key Length: Alert

Action for Unsupported Version: Alert

Add the following decryption rules to the default decryption policy:

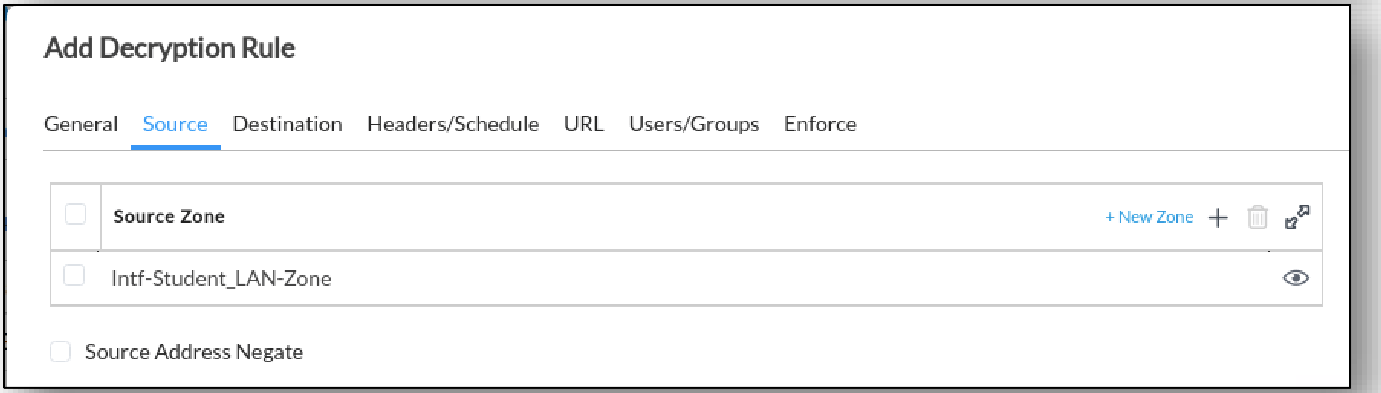


Add Decryption Rule

Name * Forward-Proxy

Description

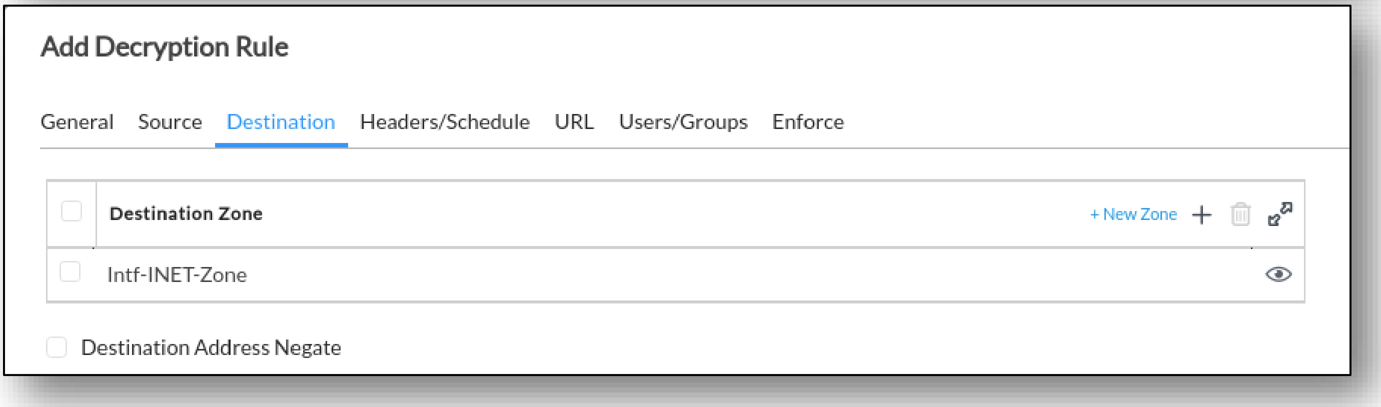
Tags



Add Decryption Rule

□	Source Zone
□	Intf-Student_LAN-Zone

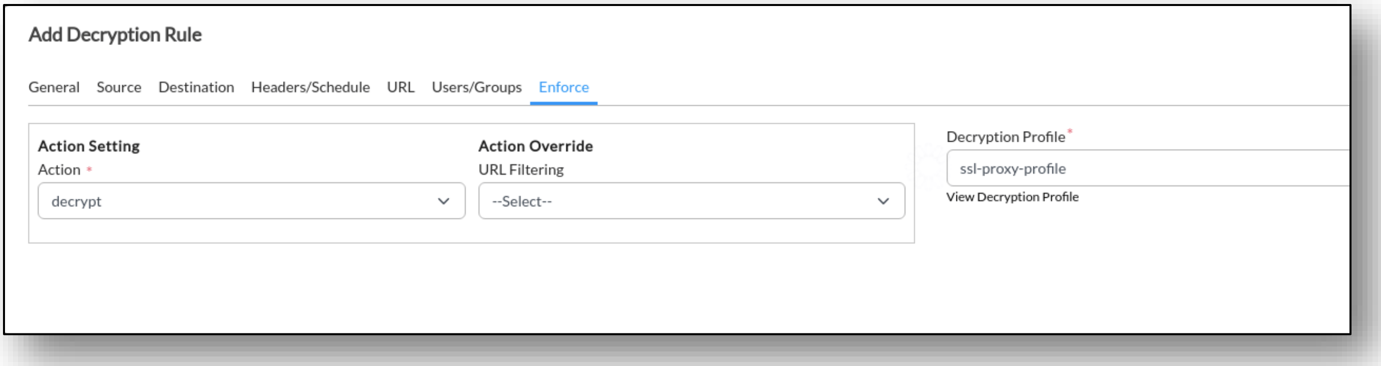
□ Source Address Negate



Add Decryption Rule

□	Destination Zone
□	Intf-INET-Zone

□ Destination Address Negate



Add Decryption Rule

Action Setting

Action * decrypt

Action Override

URL Filtering --Select--

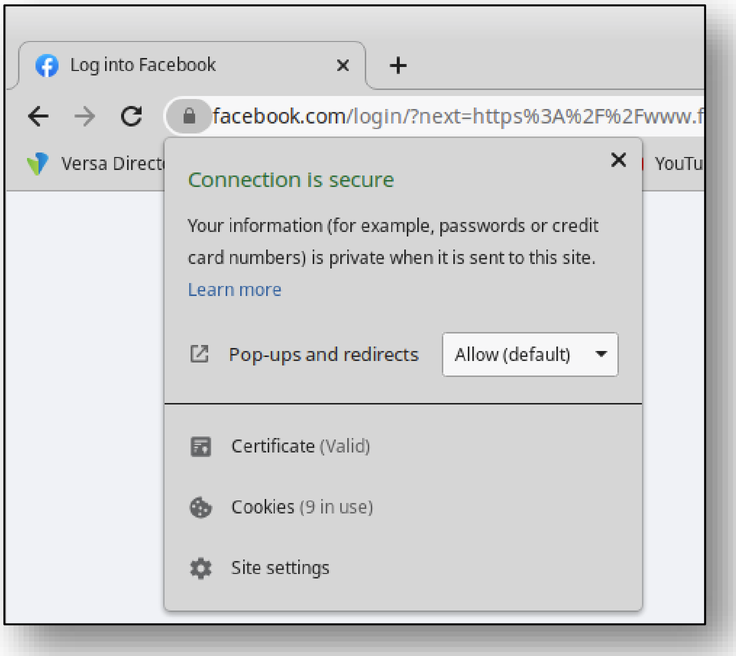
Decryption Profile * ssl-proxy-profile

Return to the remote desktop session to the Linux testing client (Remmina session).

If the Chromium browser is open in the Linux testing client, close the browser and re-open the browser to refresh the browsing sessions.

Enter the `url https://facebook.com` in the address bar to open the Facebook home page.

When the Facebook login page appears, click the padlock icon next to the address in the browser bar to inspect the certificate used for the connection, then click on the Certificate button:



Log into Facebook

facebook.com/login/?next=https%3A%2F%2Fwww.f

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

In the *Certificate Viewer* dialog you can view the certificate information. The Website should be `www.facebook.com`, the certificate should be verified by verasnetworks.com. This indicates that the session with the remote server is proxied by the VOS device.

Configure Antivirus profiles to scan encrypted traffic

In the next steps you'll configure your appliance to scan decrypted traffic for known virus profiles and signatures.

To create an Anti-Virus Profile, return to the Versa Director session on your remote desktop, open your appliance context and navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Anti-Virus*.

Click the + button to create a new anti-virus profile with the following parameters:

Antivirus Profile Settings	
Name:	AV-Profile
Direction:	Both
LEF Profile:	Default-Logging-Profile
Action:	Deny
File Type:	Add the following file types: zip, gzip, txt, 7zip, tar
Protocol:	http
Action on Disk Full:	Deny

The default storage profile will be sued for files that exceed the configured limit because the test files are less than 1MB.

Click *OK* to create the profile.

Step 2.7: Create security access rules to forward traffic to the Antivirus profile

Now that an anti-virus profile has been created, you will create security access rules that will analyze traffic and direct matching traffic to the anti-virus profile for scanning.

Navigate to *Configuration > Services > Next Gen Firewall > Security > Policies*. The *Rules* tab should display the 2 auto-generated rules. Click the + button to add a new rule to the policy. Create the rule with the following parameters:

Antivirus Rule Settings	
Name:	UTM-RULE-AV
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: Intf-INET-Zone
Headers/Schedule:	Add the following services: http, https
Enforce:	Action: Apply Security Profile > AV-Profile Logging: Both, Default-Logging-Profile

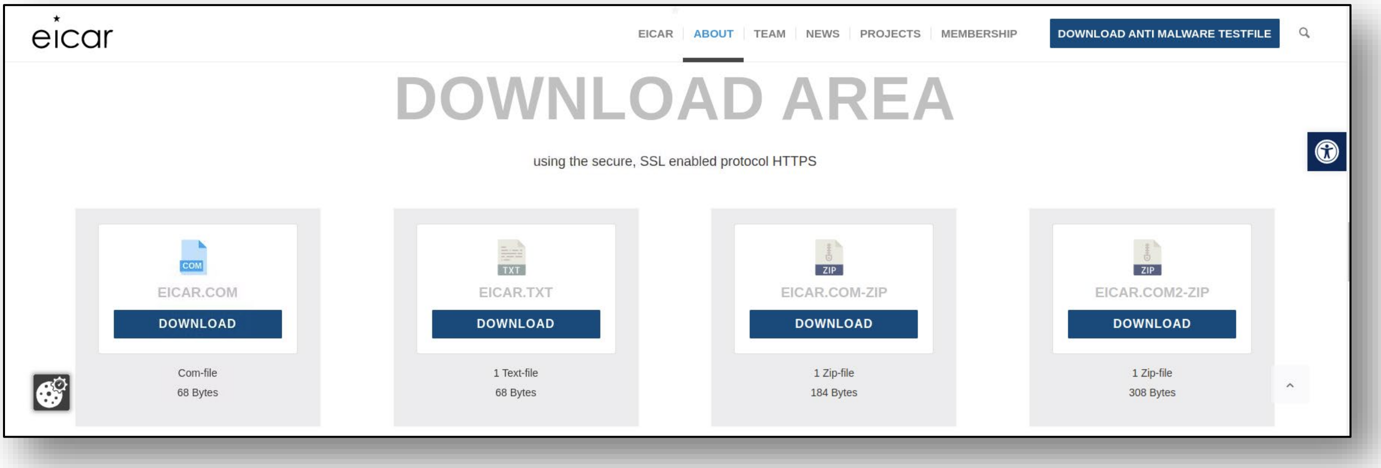
Click *OK* to create the rule. The rule will be placed after the auto-generated rules. Move the rule to the top of the rule list so that it is processed first.

Step 2.8: Verify the SSL decryption and Antivirus scanning

In the next steps you will open a browser window on the Linux testing host and browse to a known testing web site in the Internet. You will attempt to download sample files that appear to contain malicious code. These files are test files used for testing anti-virus systems.

On the landing station, open the remote desktop session to the testing host (Remmina RDP). From the testing host desktop, open the Chromium web browser. Click the *Malware Test* bookmark in the bookmark toolbar to open the testing site.

In the malware testing site, scroll down until you see the download area:



DOWNLOAD AREA

using the secure, SSL enabled protocol HTTPS

EICAR.COM	EICAR.TXT	EICAR.COM-ZIP	EICAR.COM2-ZIP
Com-file	1 Text-file	1 Zip-file	1 Zip-file
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Click the `eicar.txt` file to attempt to download the file. Wait 5 to 10 seconds.

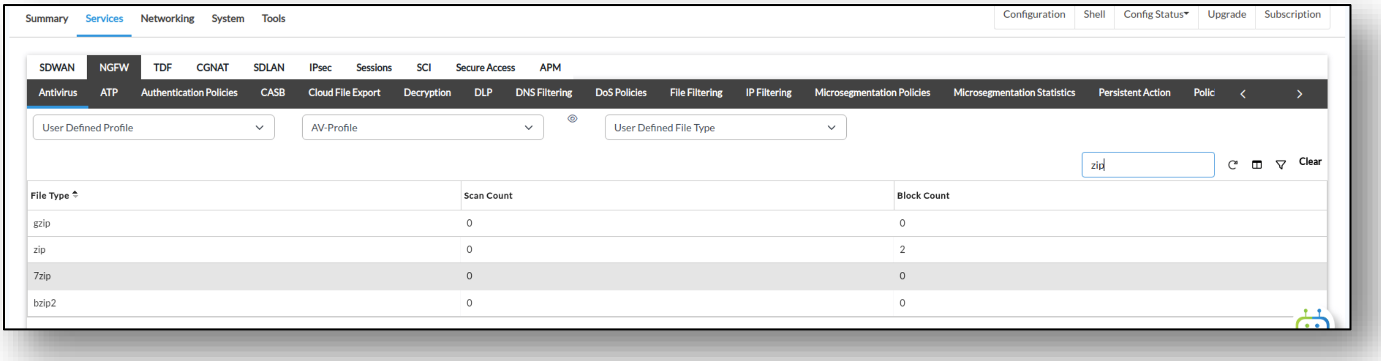
Click the `eicar.com.zip` file to attempt to download the file. Wait 5 to 10 seconds.

Click the `eicar.com2-zip` file to attempt to download the file. Wait 5 to 10 seconds.

The files should not be downloaded and should be blocked.

Note: If the files have been previously downloaded, the files may be pulled from the browser cache and appear to download from the remote site. If this happens, open the browser settings on the testing host and clear the cache.

Return to Versa Director. In Versa Director, open your appliance context *Monitor* dashboard. In the *Monitor* dashboard, navigate to *Services > NGFW > Anti Virus > User Defined Profile > AV-Profile > user-defined-file-type*. Use the search function to search for file types that contain the text `zip` and note the block count. Next search for file types that contain the text `txt` and note the block count. You should see a non-zero block count for both file types.



User Defined Profile | AV-Profile | User Defined File Type

zip

File Type	Scan Count	Block Count
gzip	0	0
zip	0	2
7zip	0	0
bzip2	0	0

In the Versa Analytics dashboard, navigate to *Logs > Threat Detection* and select the *Anti Virus* tab. You should see entries for the different files that were blocked by the anti virus engine.

Step 2.9: Configure IDP profiles for deep packet inspection and vulnerability scans

In the next steps you will configure your appliance to scan for exploits by using the IDP engine. Versa recommends to use the *Versa-Recommended* vulnerability profile in IDP because the profile covers the most up-to-date signatures to protect against threats and vulnerabilities.

You will create an access rule that references the *Versa-Recommended* vulnerability security profile, which is a pre-configured profile.

In Versa Director, navigate to your appliance context. In your appliance context, navigate to *Configuration > Services > Next Gen Firewall > Security > Policies > Rules* and click the + button to add a new access rule with the following parameters:

UTM Rule Parameters	
Name:	UTM-Rule-IDP
Source/Destination:	Source Zone: intf-Student_LAN-Zone Destination Zone: ptvi
Headers/Schedule:	Click + New Service and create a custom service: Name: UTM-Hub Protocol: TCP_OR_UDP Port: 80
Enforce:	Action: Apply Security Profile Select Vulnerability > Versa Recommended Profile Logging: Both, Default-Logging-Profile

Click *OK* to add the rule, then move it to the top of the rule list.

Step 2.10: Verify results using Versa Director

In the next steps you will connect to the testing host and run an exploit script from the terminal window.

In the remote landing session, open the remote desktop session to the testing host. On the testing host, navigate to *Applications > System > Xfce Terminal* to open a new terminal window.

The scripts for this lab are located in the ./VASEC/ directory. Type cd ./VASEC/ to move to that directory.

From within the terminal window, execute the following command

```
./exploitS2-057-cmd.py 10.27.13.20:80 'id'
```

to run the exploit script. This script attempts to run a web exploit on a web server connected to the hub device. At the bottom of the output you should see a "Connection refused" error, which is expected.

Step 2.11: Verify the results using Versa Director

Return to Versa Director on the remote landing station. In Versa Director, open your appliance context and navigate to *Monitor > Services > NGFW > Policies* for your appliance. Examine the Hit Count for the UTM-Rule-IDP rule. It should be a non-zero value, which indicates that the rule matched sessions. The rule enforce action is to forward the session to the Vulnerability security profile.

Navigate to the *Vulnerability* tab and select *Pre Defined* from the drop down list. Scroll down to the *Versa Recommended* profile. It should show a non-zero value in the Total Sessions field.

Step 2.12: Verify results using Versa Analytics

Click the *Director View* button next to your appliance name in the top left to return to the main Versa Director user interface. From the main Versa Director user interface, navigate to *Analytics > Dashboards > Security > Threats*.

Open the *Vulnerabilities* tab in the *Threats* dashboard. You should see charts listing the top threats and top signature IDs. Click on the *attempted-user* chart to open details about the threat.

In the *attempted-user* threat window, scroll down to see the list of events recorded for the attempted-user threat. The action should be *reject*. Examine the *Signature Message* field and *Class Message* field to discover more details about the type of threat.

Navigate to *Logs > Threat Detection* and select the IDP tab. In the IDP tab you should see the log entries for the events.

Step 2.13: Configure Intrusion Detection (alert only)

In the previous lab example, the appliance was used to block the attempted exploits. The IDP engine can be configured to act as a detection engine only that logs flagged sessions but does not block them. This is done by creating a *Vulnerability Profile Override* which overrides the vulnerability profile default action.

In the next steps you will configure a vulnerability profile override action to configure your appliance to act as an intrusion detection device only (not a prevention device).

In Versa Director, open the appliance context of your appliance. In appliance context, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override*.

Click the + button to create a new override profile with the following parameters:

Override Profile Parameters	
Name:	IDP-Override
LEF Profile:	Default-Logging-Profile
Rule:	Action: Alert

Next you will map the Access-Policy rule to the Override Profile.

Navigate to the *Configuration > Services > Next Gen Firewall > Security > Policies > Rules* tab and open the *UTM-Rule-IDP* rule. Navigate to the *Enforce* tab and check the *Predefined Vulnerability Profile Override* box, then select the *IDP-Override* profile from the drop down menu.

Step 2.14: Verify the threat detection without prevention

In the next steps you will verify that the device logs the exploit attempt but does not block it.

Return to the remote desktop session to the Linux testing host (in Remmina). In the terminal window of the testing host, run the script for the exploit. You can use the up arrow to recall the previously run command, or enter the following command manually:

```
./exploit-S2-057-cmd.py 10.27.13.20:80 'id'
```

The attack should present an HTTP Error 400: Bad Request message, which is normal for this lab scenario. However, the session will not be reset by the branch device. The error message is returned by the remote web server, which indicates the remote web server was contacted.

To verify that the device only generated an alert for the attack, return to Versa Director. In Versa Director, navigate to *Analytics > Dashboards > Security > Threats*.

Select the *Vulnerabilities* tab and click on the *attempted-user* graphic in the *Top Threats* chart.

Scroll down to the threat log table. You should see several entries for the attempted-user threat type from your appliance, but the action should be set to alert instead of reject. If you scroll down through the entries you will see the previous exploit attempt with the original reject action. You can also see the new name for the Profile, which indicates that the new sessions were acted upon by the Versa Recommended Profile-IDP-Override profile.

Step 2.15: Configure over-ride profiles to skip processing of selected traffic

In the next steps you will configure the Versa branch appliance to allow specified threat IDs to and from hosts within an exception list.

To perform this task, you will modify the Vulnerability Profile Override created previously and add exceptions to the override rule.

Return to Versa Director. From Versa Director appliance context, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override* hierarchy and click the *IDP-Override* profile to open the profile. Modify the rule with the following parameters:

Exception Parameters	
Name:	IDP-Override
LEF Profile:	Default-Logging-Profile
Rule:	Action: Reject
Exceptions:	You will add 3 exceptions to the rule. Click the + button and add the following: ThreatID: 1111209051; enable Signatures: Search and select the following signatures: 1111209050 1130527060 1111209051 Exception Details: Action: Allow Exempt IP Address 10.27.13.20 Thresholds: Track by Destination

Click *OK* to create the exemption.

Step 2.16: Verify the exemption

Return to the testing host remote desktop session. From the testing host terminal window, run the exploit script again. You can run the exploit script by typing the up arrow on the keyboard to recall the previous instance of the script, or by entering the following in the terminal prompt:

```
./exploitS2-057-cmd.py 10.27.13.20:80 'id'
```

The attack should succeed or end with an HTTP 400 error, which indicates that the exploit reached the remote web server and was not blocked by the B01 device.

Return to Versa Director. In Versa Director, navigate to *Analytics* > *Logs* > *Threat Detection* and select the *IDP* tab.

In the log entries, refer to the time stamp of the latest entry. Note that the latest script did not register in Versa Analytics because the session was exempted and by passed the IDP engine.

Step 2.17: Finish the lab and exit the lab environment

To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.

Log out of Versa Director.

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