

VERSA 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!

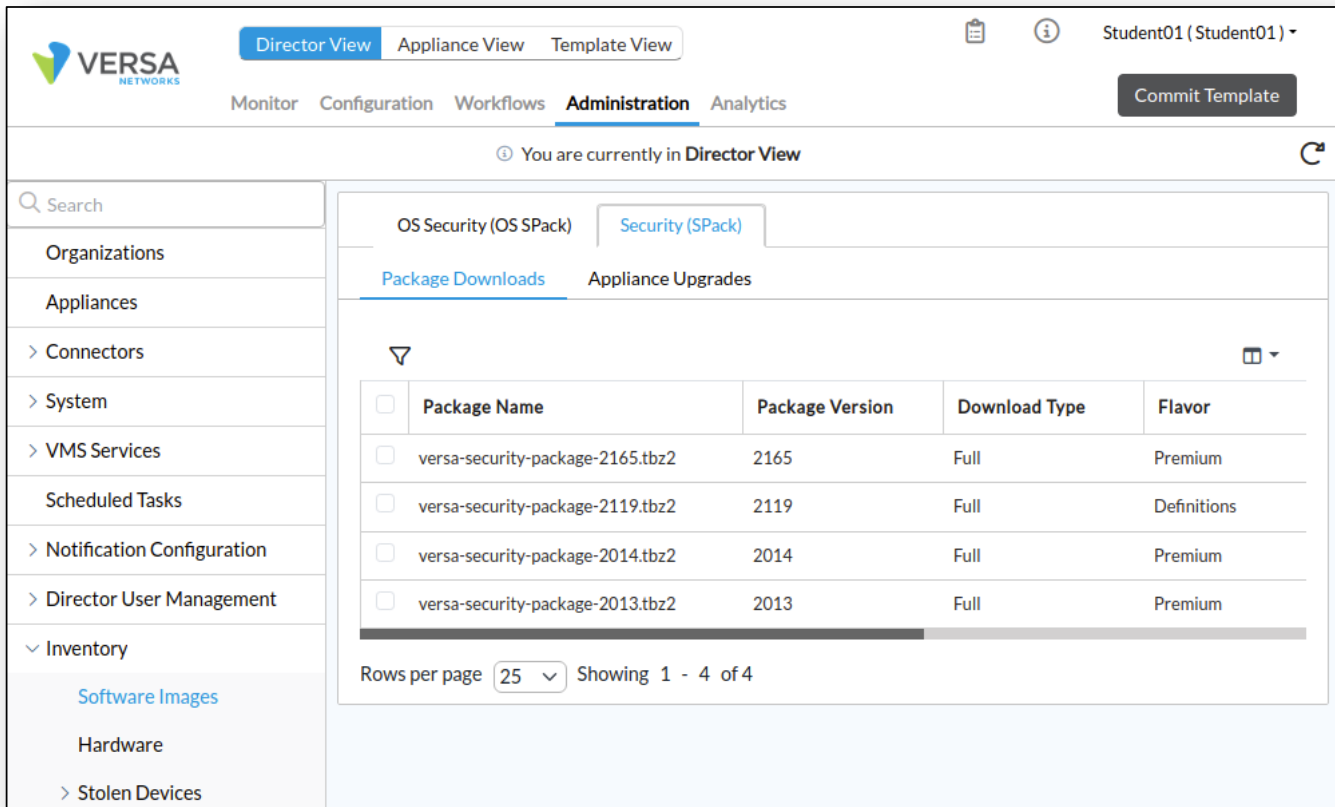
In the following lab exercises, you will:

- 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

- 1.a. 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.



The screenshot shows the Versa Director interface. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The main navigation menu has 'Monitor', 'Configuration', 'Workflows', 'Administration', and 'Analytics'. The 'Administration' section is active, and the 'Inventory' sub-section is selected. The 'Security (SPack)' tab is active, showing a table of security packages. The table has columns for 'Package Name', 'Package Version', 'Download Type', and 'Flavor'. There are four rows of data, each with a checkbox in the first column. The 'Rows per page' is set to 25, and it shows 'Showing 1 - 4 of 4'.

<input type="checkbox"/>	Package Name	Package Version	Download Type	Flavor
<input type="checkbox"/>	versa-security-package-2165.tbz2	2165	Full	Premium
<input type="checkbox"/>	versa-security-package-2119.tbz2	2119	Full	Definitions
<input type="checkbox"/>	versa-security-package-2014.tbz2	2014	Full	Premium
<input type="checkbox"/>	versa-security-package-2013.tbz2	2013	Full	Premium

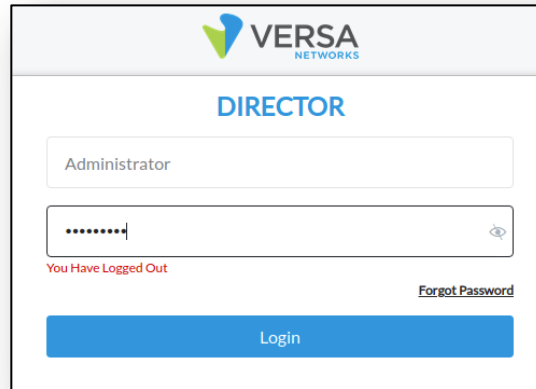
As a tenant in a global system, you do not have access to download security packages to Versa Director, as that can affect the overall system storage space. The Administrator account has access to download security packages.

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.

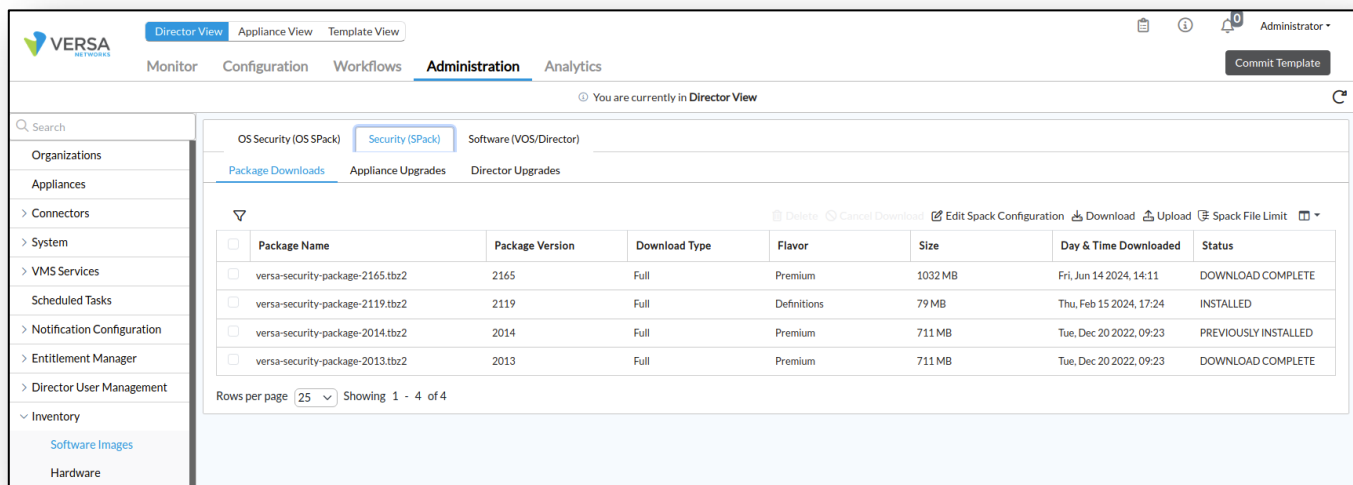
After viewing the Administrator access to the Software Images, you will log out, then log back in as your Studentxx tenant.

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

- 1.b. In the top right corner, click on your user ID and log out of Versa Director.
- 1.c. Log into Versa Director as *Administrator* with password *Versa@123*.



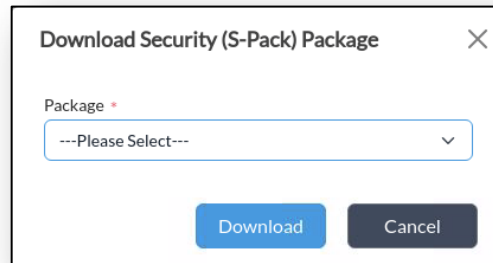
- 1.d. After you log in as Administrator, navigate to *Administration > Inventory > Software Images*.



- 1.e. In the *Software Images* dashboard, select the *Security (SPack)* tab.

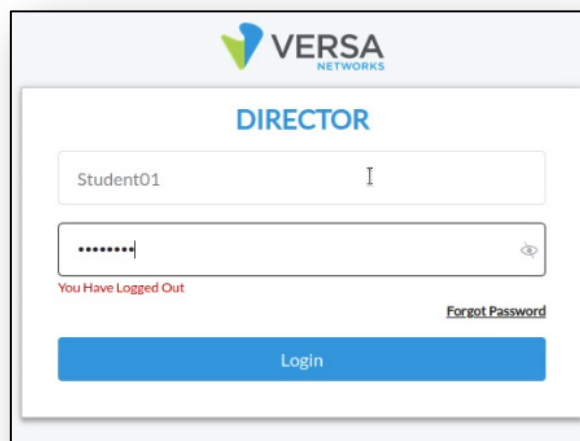
Note the options you have as administrator in the top right of the table (e.g. Download, Upload, Spack File Limit)

- 1.f. 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.
- 1.g. Click the *Download* button to view the download dialog.

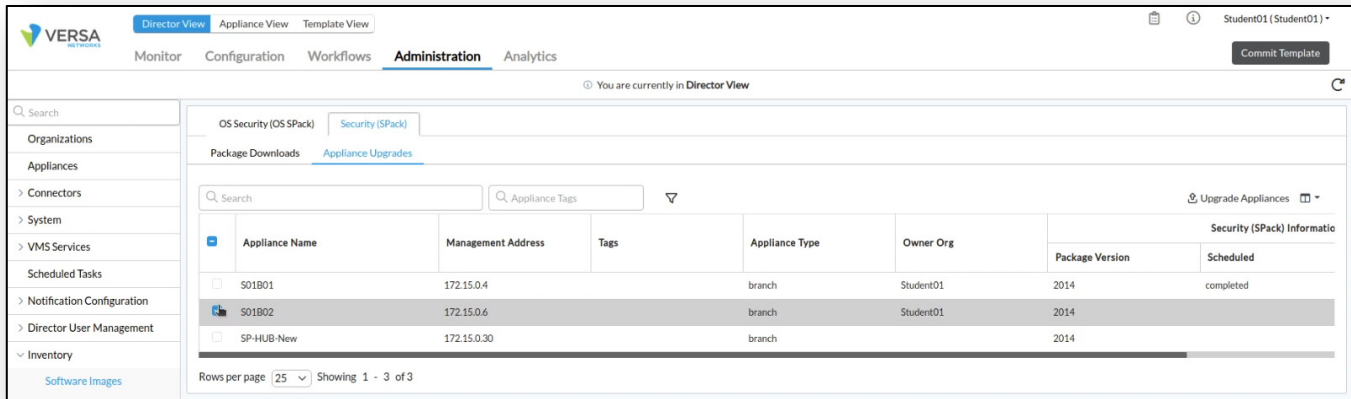


The security package list is automatically populated and when you click the Package drop-down, the latest security packages will be listed.

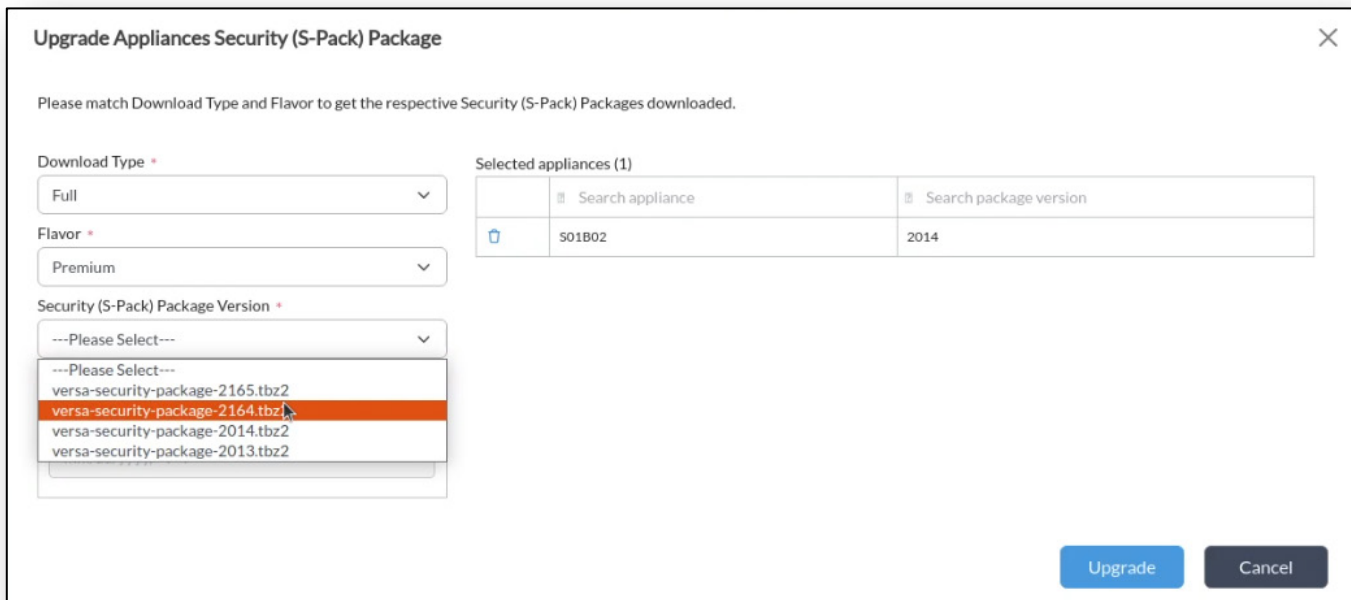
- 1.h. Click the *Cancel* button to exit the dialog.
Examine the list of security packages in the system. This list of packages will be available to the sub-tenants.
- 1.i. Click the *Administrator* user in the top right of the window, and log out as Administrator.
- 1.j. Log back into Versa Director with your assigned student username (Student01, Student02, etc.)



- 1.k. Navigate to *Administration > Inventory > Software Images > Security (SPack) > Appliance Upgrades*.
- 1.l. 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.



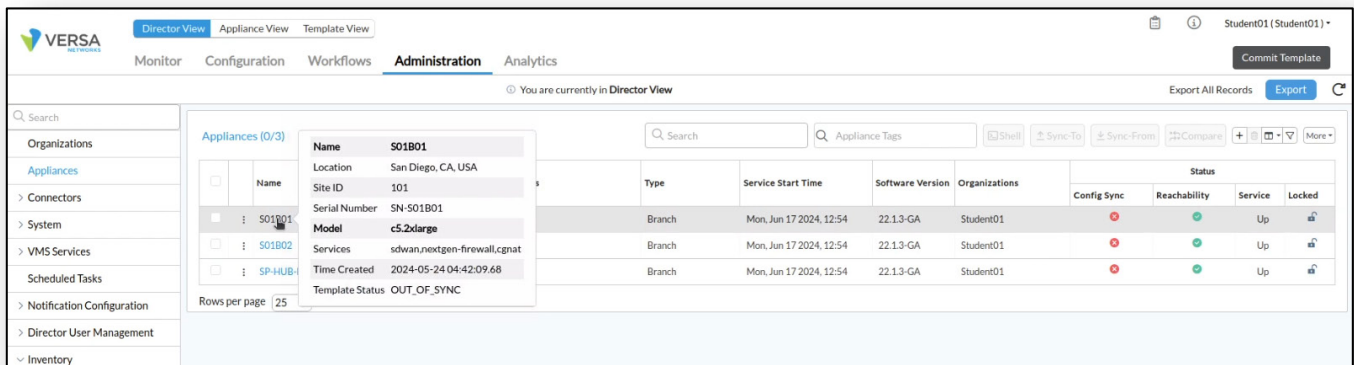
- 1.m. Click the *Upgrade Appliances* button to open the upgrade dialog.
- 1.n. In the *Upgrade Appliances Security (S-Pack) Package* dialog, select one of the newer packages from the list. The download type should be *Full*, and the Flavor *Premium*.



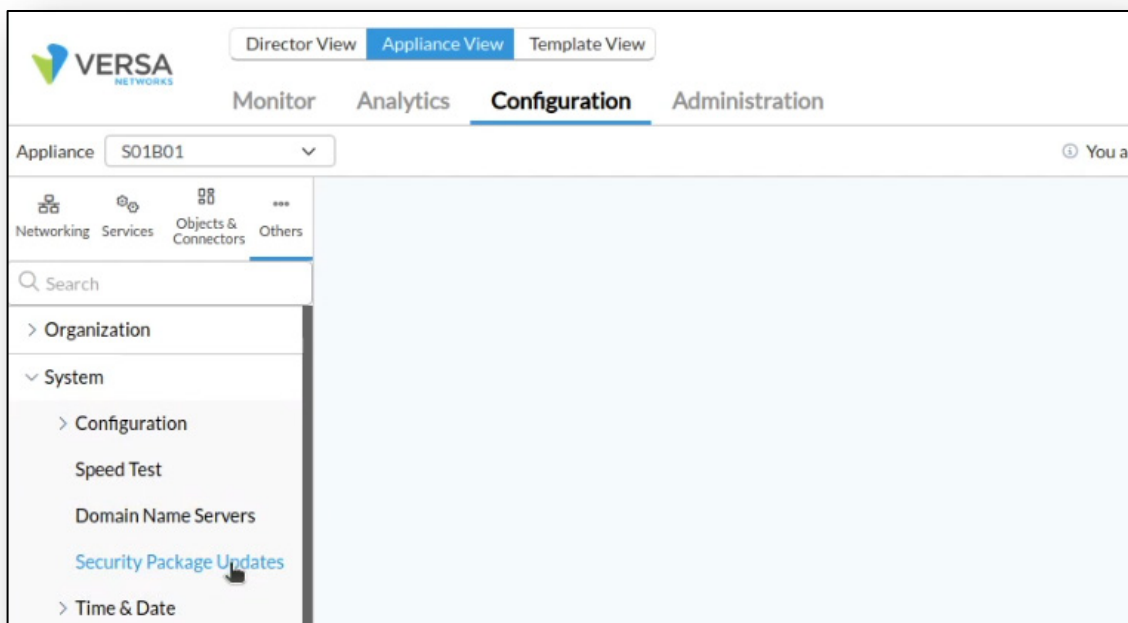
- 1.o. Click the *Upgrade* button to install the security package. This will take a couple of minutes to upload and apply the package to the branch device.

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

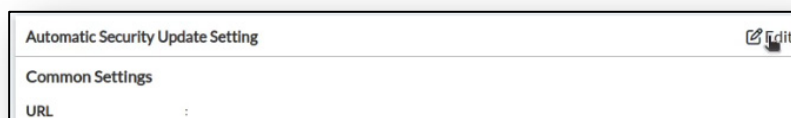
- 1.p. After the update is complete, navigate to *Director View > Administration > Appliances* and locate your B01 appliance in the *Appliances* table.
- 1.q. Click on the *B01* appliance to open it in *Appliance View*.



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



- 1.s. In the *Security Package Updates* dialog, click the *Edit* button to modify the settings.



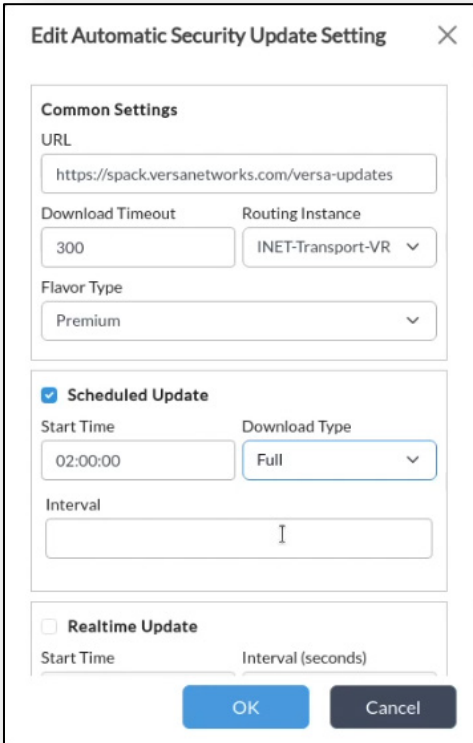
NOTE: Automatic updates may already be configured on the branch device. If this is true, follow the steps to see where this function is enabled.

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: Select the check box to schedule a time
- Start Time: 02:00:00
- Download Type: Full

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

- 1.t. Click *OK* to finish the configuration change.



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

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!

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

- 1.a. In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the workflow to your branch device.
- 1.b. In the *Basic* tab, ensure that the device is assigned to the *DG-Sxx-NGFW* device group, where *Sxx* is the number of your student ID. If you need to change the device group assigned to your branch device, be sure to click *Re-deploy* to apply the changes to the device in Versa Director.
- 1.c. Click the *Commit Template* button in the top-right corner of Versa Director
 - Select your student tenant ID from the Organization drop-down menu
 - Select the *Template-Sxx-NGFW* from the *Select Template* menu, where *Sxx* is your student tenant ID
 - Check the box next to your branch device and click *OK* to overwrite the configuration on the device with the Base-Template configuration.

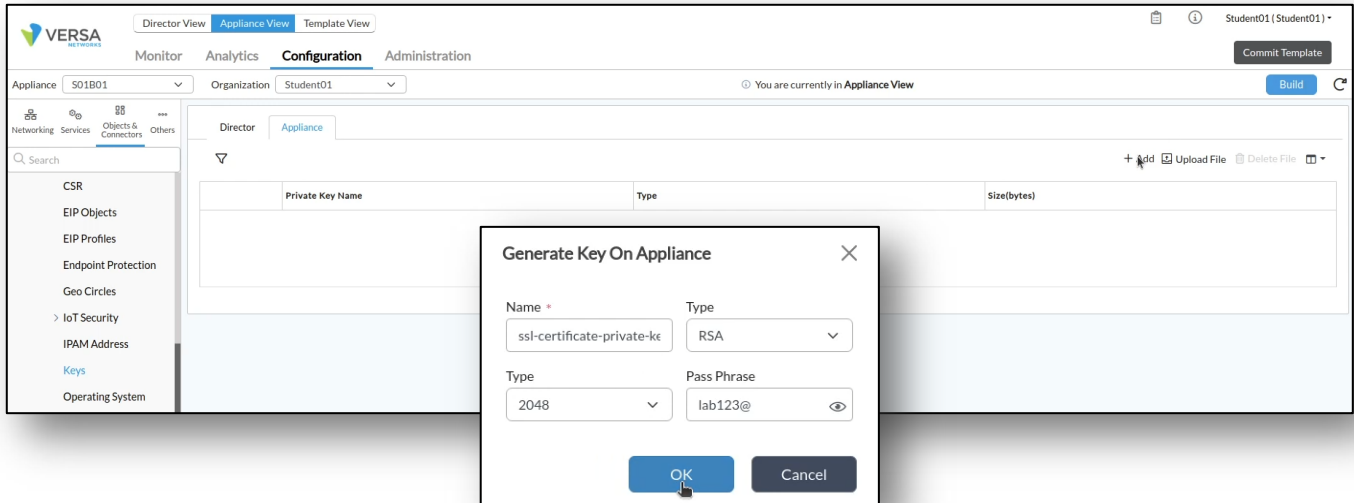
Step 2. Create an SSL encryption key

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 Appliance View mode) and not in the device templates.

- 2.a. 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.
- 2.b. From the Appliance View mode of your B01 device, click on the *Configuration* tab to modify the configuration.

The encryption key is a custom object that is configured under the *Objects & Connectors > Objects > Custom Objects > Keys* hierarchy.

- 2.c. Create an encryption key for the APPLIANCE with the following parameters:
 - Key Name: ssl-certificate-private-key
 - Type: RSA
 - Type: 2048
 - Pass Phrase: lab123@



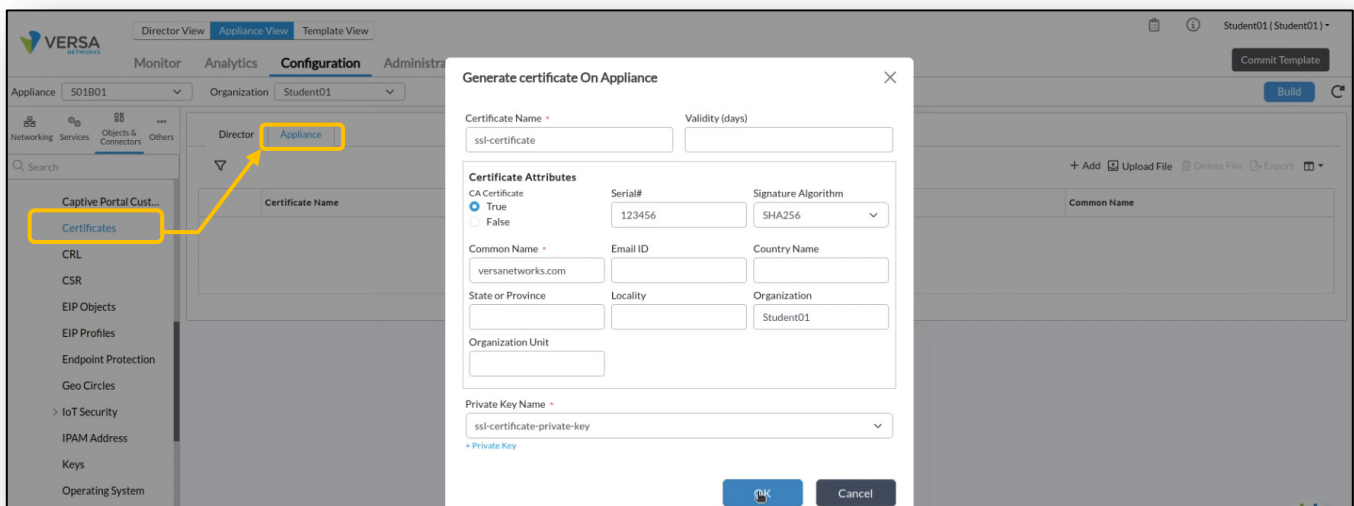
Step 3. Create an appliance certificate

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.

3.a. 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*):

- Certificate Name: ssl-certificate
- CA Certificate: True
- Serial#: 123456
- Signature Algorithm: SHA256
- Common Name: versanetworks.com
- Organization: [your organization]
- Private Key Name: ssl-certificate-private-key

3.b. Click OK to create the certificate.



Step 4. Configure Proxy Profiles

In the next steps you will configure a proxy profile (decryption profile) and a decryption 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 View of your device.

- 4.a. From your Appliance View, navigate to *Services > Next Gen Firewall > Decryption > Proxy Profiles* hierarchy.
- 4.b. Create a new decryption profile with the following parameters:

General Tab

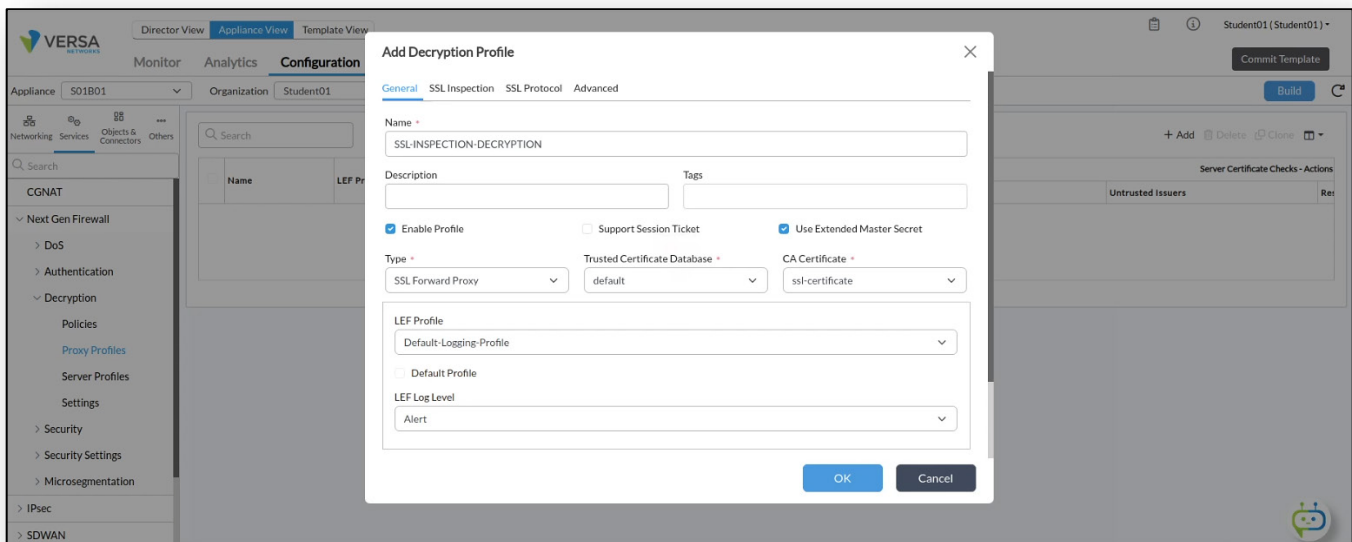
- Name: SSL-INSPECTION-DECRYPTION
- Enable Profile: Checked
- Use Extended Master Secret: Checked
- Type: SSL Forward Proxy
- Trusted Certificate Database: default
- CA Certificate: ssl-certificate
- LEF Profile: Default-Logging-Profile
- LEF Log Level: Alert

SSL Inspection Tab

- Action for Expired Certificate: Reject
- Action for Untrusted Issuers: Allow
- Restrict Certificate Extension: Checked
- Action for Unsupported Cipher: Allow
- Min Supported Key Length: 512
- Action for Unsupported Key Length: Allow
- Action for Unsupported Version: Alert

SSL Protocol Tab

- Leave all values default



Add Decryption Profile [X]

General **SSL Inspection** SSL Protocol Advanced

OCSF

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 [X]

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

OK Cancel

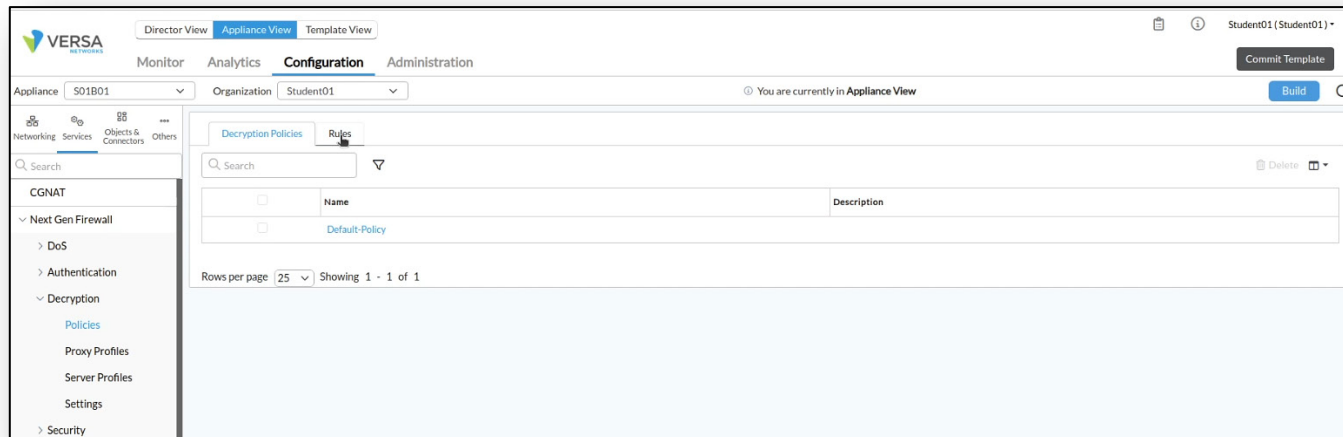
If you do not select any specific encryption and authentication algorithms, then all algorithms for the enabled TLS versions are automatically enabled

Step 5. 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

5.a. In the SSL Decryption configuration hierarchy, open the *Policies* window. Versa Director will automatically create a Default-Policy when you open the dialog.



5.b. Click on the *Rules* tab to add rules to the policy.

5.c. Add a rule named *Inspection-Rule* with the following properties:

General Tab

- Rule Name: Inspection-Rule

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Headers/Schedule Tab

- Services: https

URL Tab

- URL Category: financial_services

Enforce Tab

- Action: no-decrypt
- Decryption Profile: SSL-INSPECTION-DECRYPTION

5.d. Add a rule named *Decryption-Rule* with the following properties:

General Tab

- Rule Name: Decryption-Rule

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Headers/Schedule Tab

- Services: https

URL Tab

- URL Category:
 - sports
 - social_network
 - news_and_media

Enforce Tab

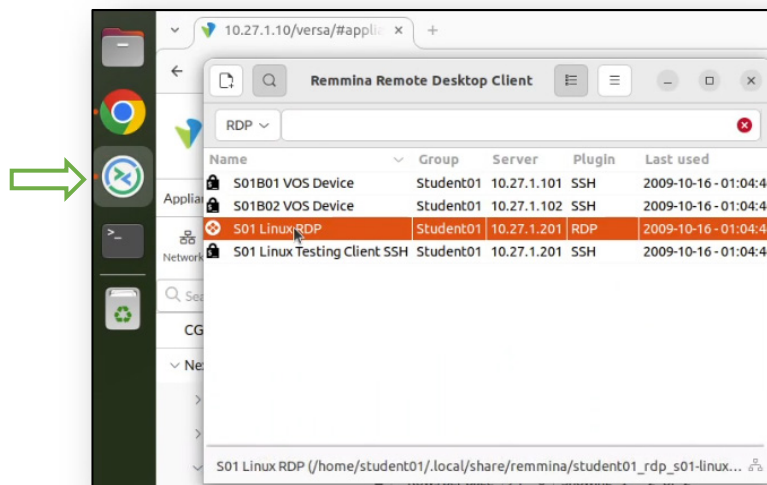
- Action: decrypt
- Decryption Profile: SSL-INSPECTION-DECRYPTION

Step 6. 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.

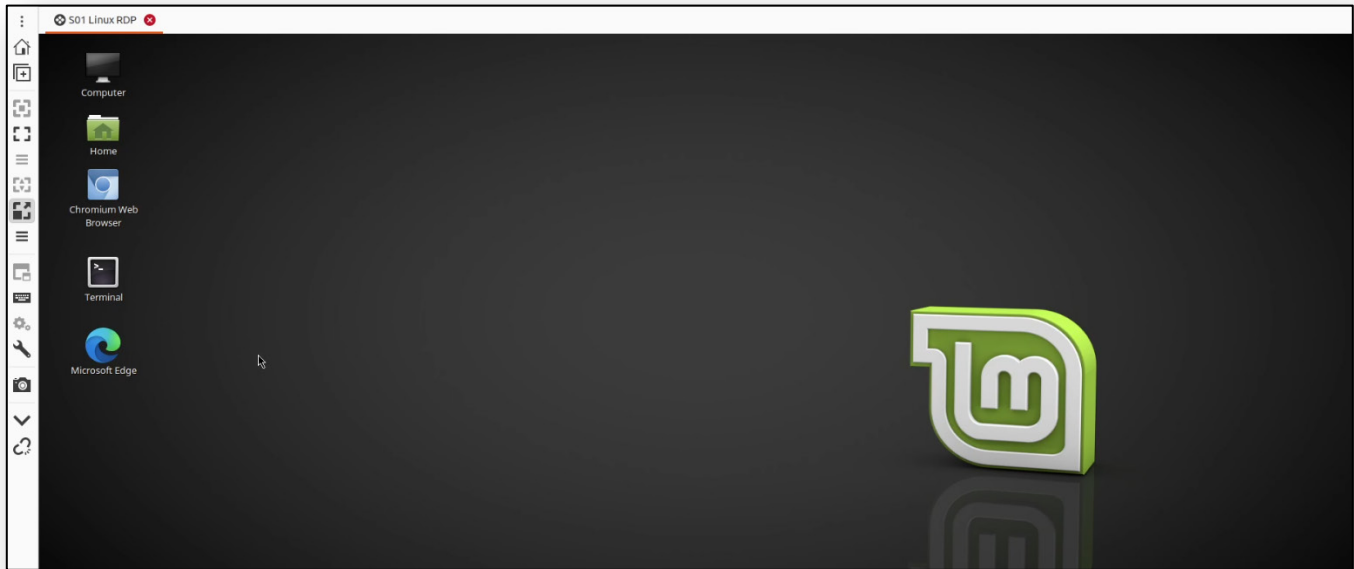
Steps in this exercise:

- 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
- 6.a. Locate and open the *Remmina Remote Desktop Client* icon in the left application bar.
- 6.b. 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*.



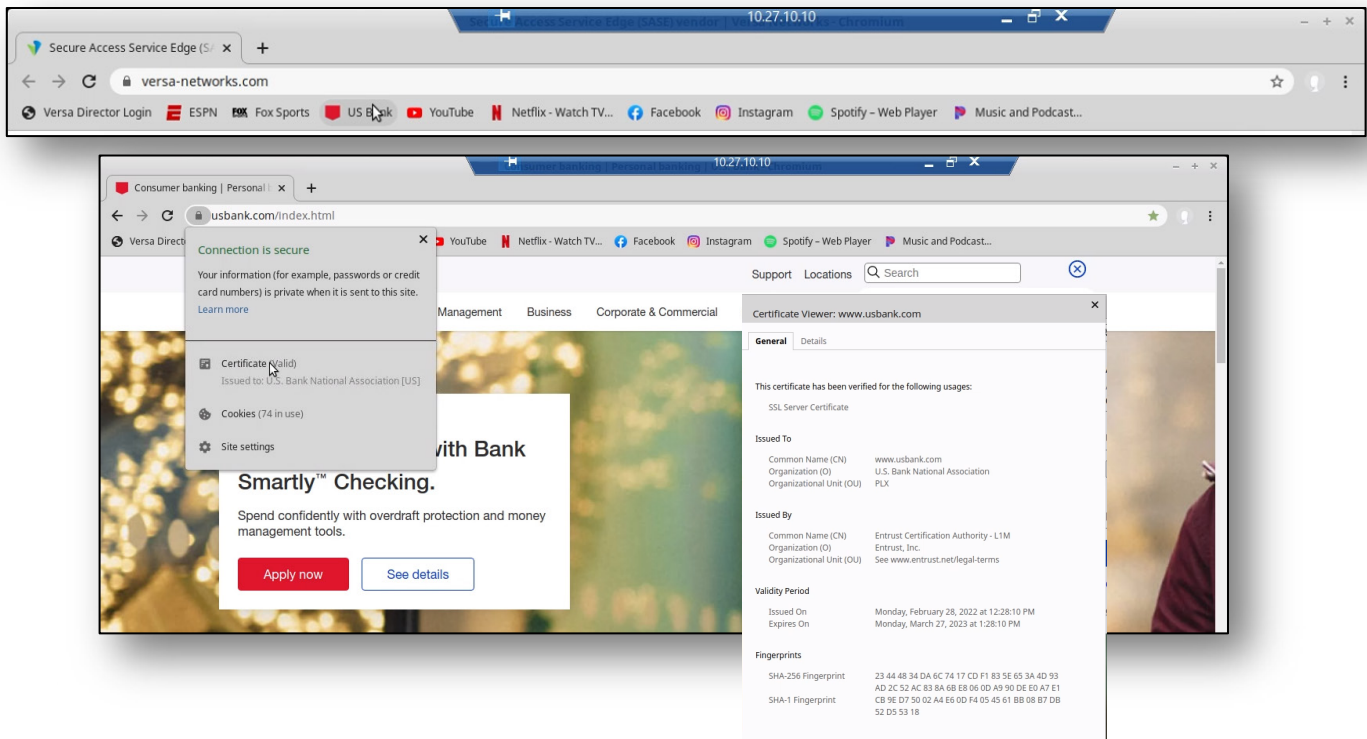
Note: The remote desktop resolution is set to the size of the Remmina application window when the RDP session is started. If the resolution is too small, you can increase the size of the RDP session main window, then close and re-open the RDP session to reset the remote desktop resolution.

You should be presented with the remote desktop below.



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

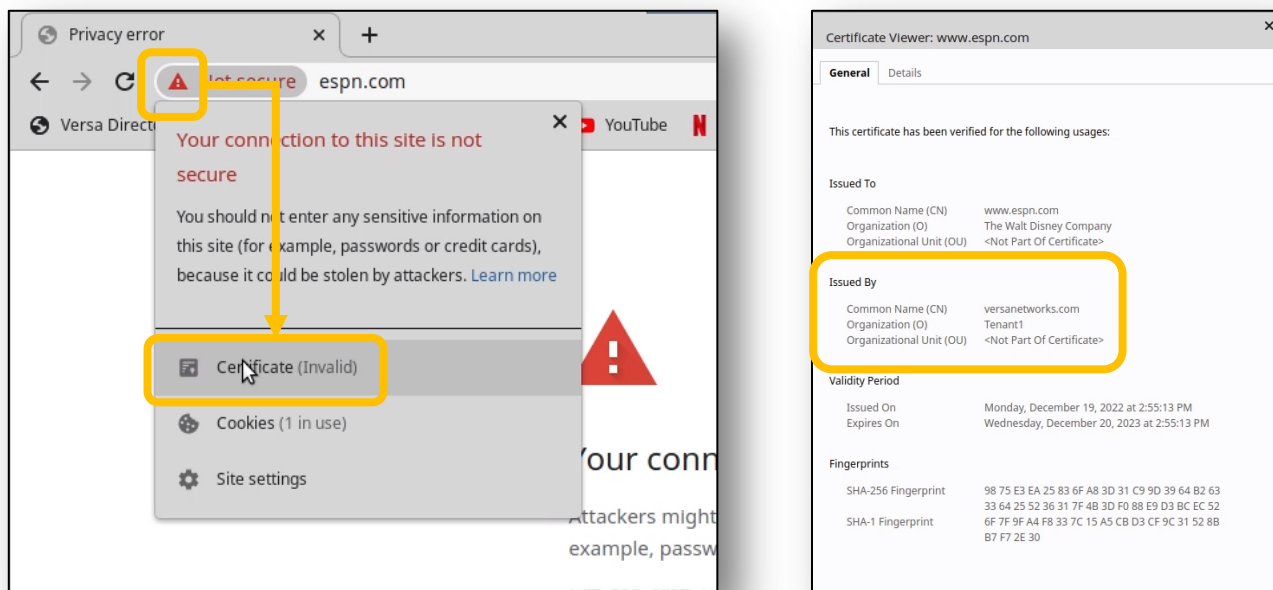
- 6.c. Open the Chromium browser on the remote desktop.
- 6.d. Navigate to *www.usbank.com*. You can use the bookmark in the bookmark bar.



- 6.e. After the page loads, click the icon next to the address 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).
- 6.f. Next, enter the address *www.espn.com* in the address bar or use the bookmark. You should see an alert indicating that there is a problem with the certificate for the ESPN site.

You should receive a warning of a potential security risk. Click the lock icon to view the site certificate information.

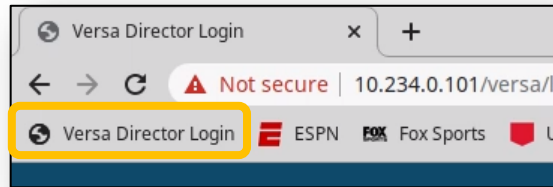
Follow the steps below to view the provider of the certificate used on the site.



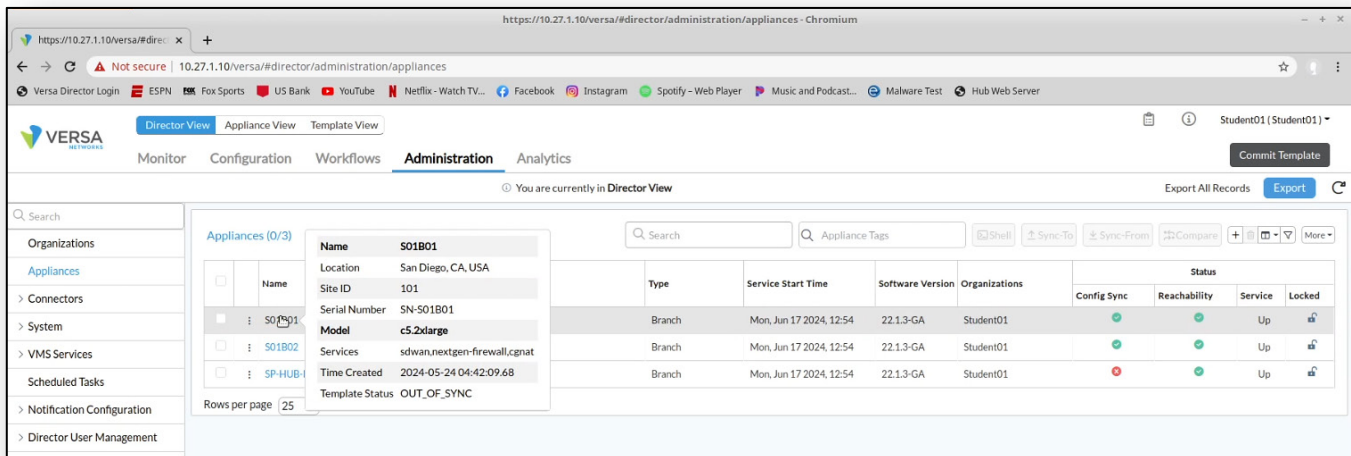
The certificate for the sports site was provided by your organization. This is because the branch device intercepted the SSL session and is acting as a proxy for the SSL tunnel.

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

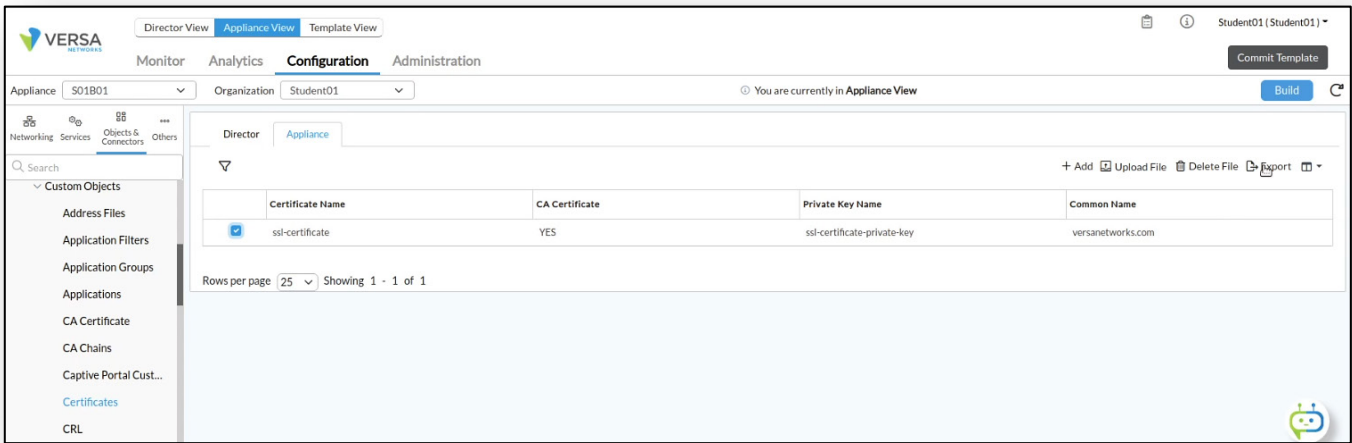
- 6.g. Close the certificate information windows and return to the main browser window.
- 6.h. In the remote desktop Chromium browser, click the *Versa Director* bookmark to open Versa Director (the remote host has an out-of-band management network connection to Versa Director).



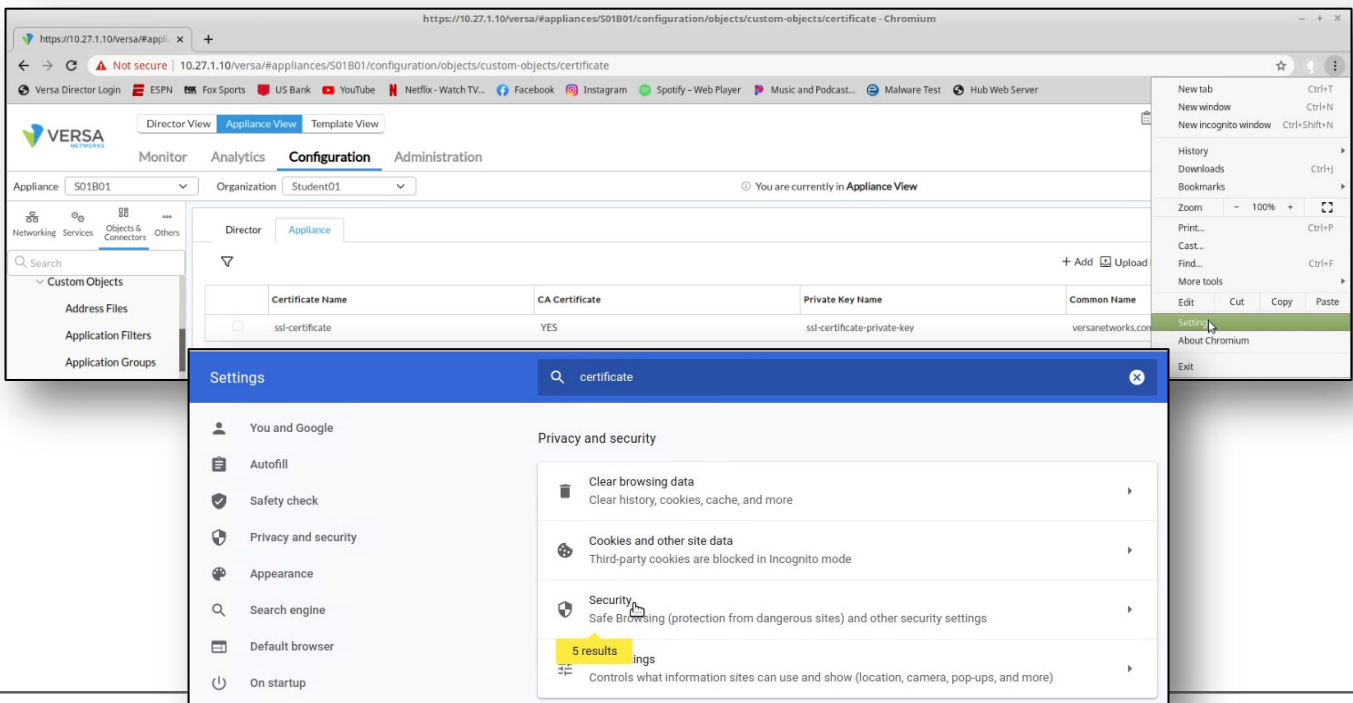
- 6.i. In Versa Director, navigate to the *Administration > Appliances* dashboard and locate your appliance in the appliance table.
- 6.j. Click your appliance to open your appliance configuration.



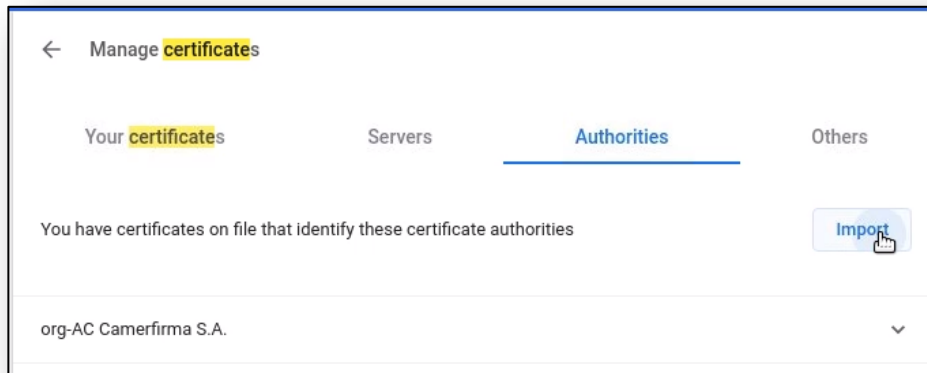
- 6.k. In your appliance configuration, navigate to *Objects & Connectors > Objects > Custom Objects > Certificates*.
- 6.l. Select the *Appliance* tab in the *Certificates* window.
- 6.m. Locate your certificate in the Appliance certificate table.
- 6.n. Check the box next to the certificate so that the *Export* button becomes active.
- 6.o. Click the *Export* button to download the certificate to the remote desktop *Downloads* folder.



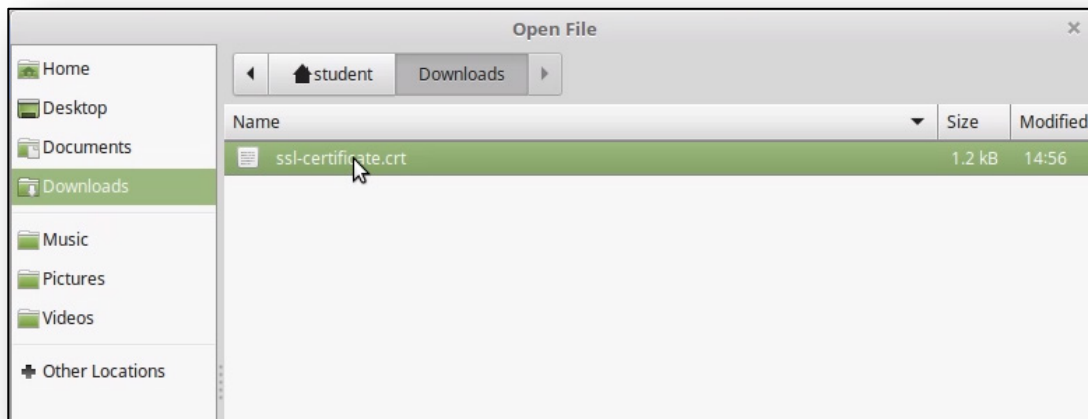
- 6.p. After you have downloaded the certificate, click the *Settings* button in the remote browser.
- 6.q. Open the browser *Preferences*.
- 6.r. In the preferences window, type the word *certificate* in the search window. This will display the *View Certificates* button.
- 6.s. Click the *View Certificates* button to open the certificate manager.



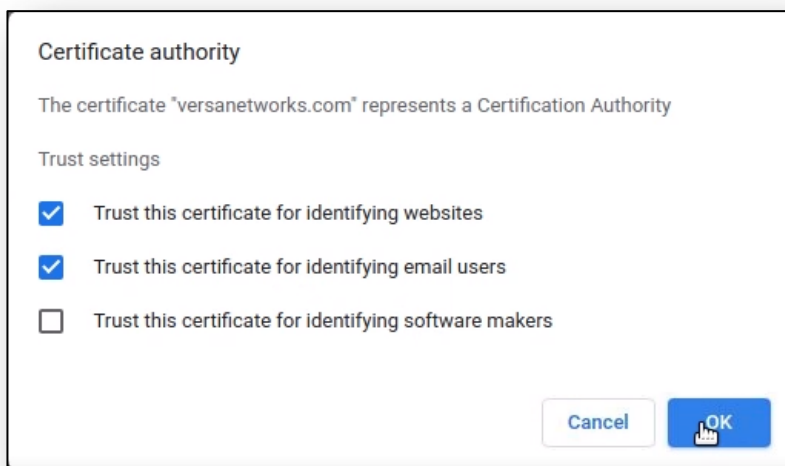
- 6.t. In the *Certificate Manager* window, select *Authorities* from the top menu bar.
- 6.u. Scroll down in the *Authorities* window until you see the *Import* button at the bottom.
- 6.v. Click the *Import* button.



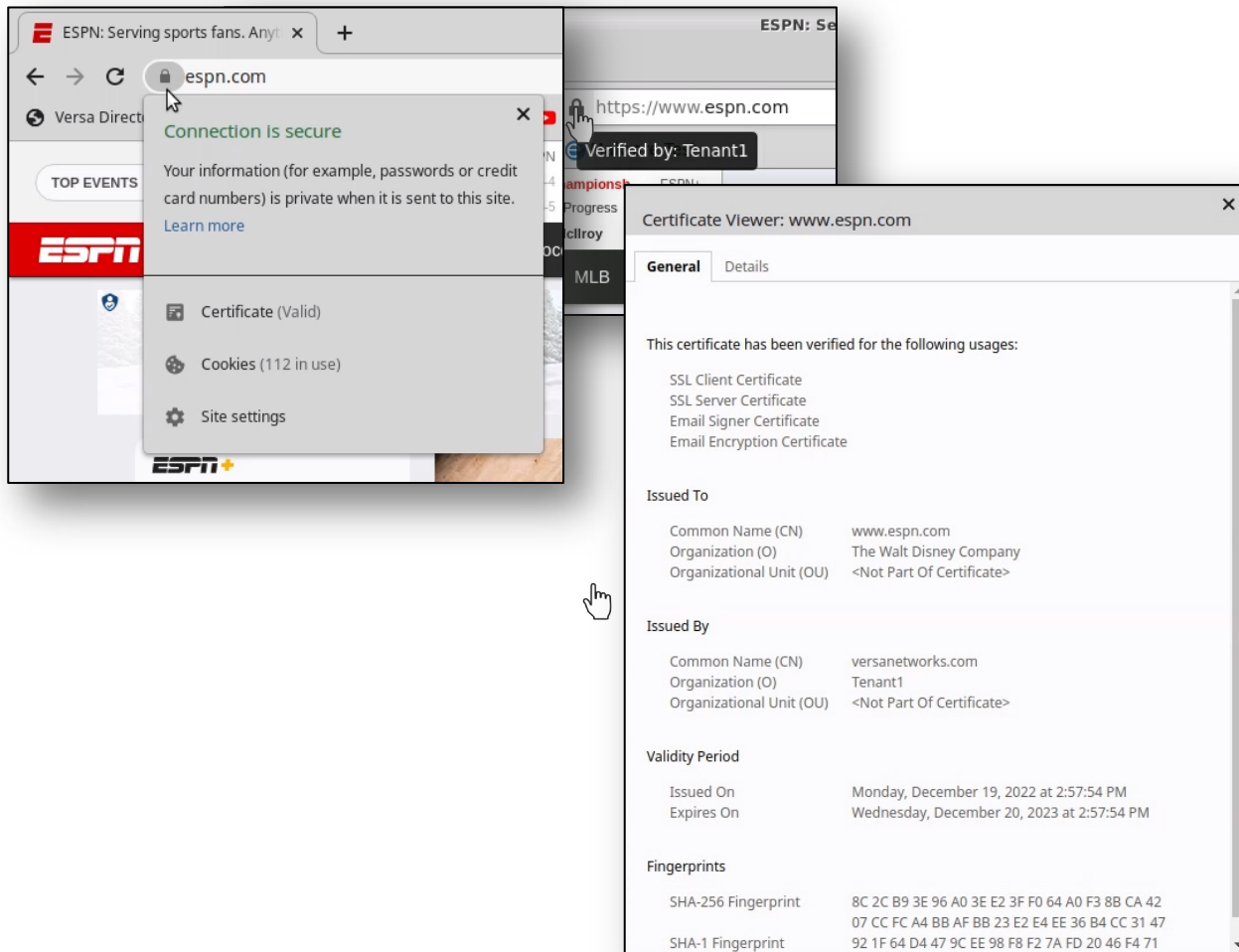
- 6.w. Open the *Downloads* folder and locate the new SSL certificate. Note that there may be a duplicate certificate because a certificate was already present. Choose the newer certificate (based on the date) and click the *Open* button to import the certificate.



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

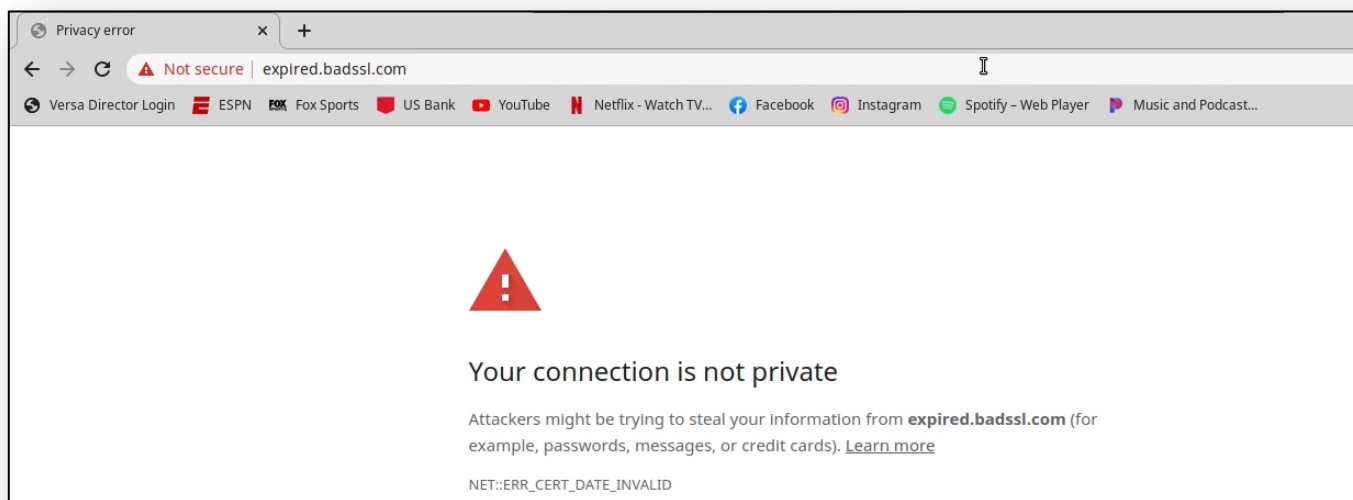


- 6.y. Close the properties windows and return to the testing client browser window.
- 6.z. In the testing client browser window, enter the address *www.espn.com* in the remote browser address bar again. The web site should now open properly.



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

6.aa. 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.



6.ab. Return to the Versa Director session on your remote desktop.

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

6.ad. 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.

General Tab

- Rule Name: Inspect-All

Source Tab

- Source Zone: Intf-Student_LAN-Zone

Headers/Schedule Tab

- Services: https

Enforce Tab

- Action: no-decrypt
- Decryption Profile: SSL-INSPECTION-DECRYPTION

Add Decryption Rule

General Source Destination Headers/Schedule URL Users/Groups Enforce

Name 11/127

Description

Tags
 Disable Rule

Add Decryption Rule

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

Source Zone + New Zone + [trash] [lock]
 Intf-Student_LAN-Zone

Source Address + New Address + New Address Group + [trash] [lock]
 Source Address Not Configured

Source Address Negate

Region + [trash] [lock]
 Region Not Configured

State + [trash] [lock]
 State Not Configured

City + [trash] [lock]
 City Not Configured

Source Location Negate

Custom Geo Circle + [trash] [lock]
 Custom Geo Circle Not Configured

EIP Profiles + Add EIP Profile + [trash] [lock]
 EIP Profiles Not Configured

Add Decryption Rule

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

IP
 IP Version: IP Flags:

DSCP:

TTL
 Condition: Value (Max 255):

Others
 Schedules:

Services + New Service + [trash] [lock]
 https

Add Decryption Rule

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

Action Setting
 Action:

Action Override
 URL Filtering:

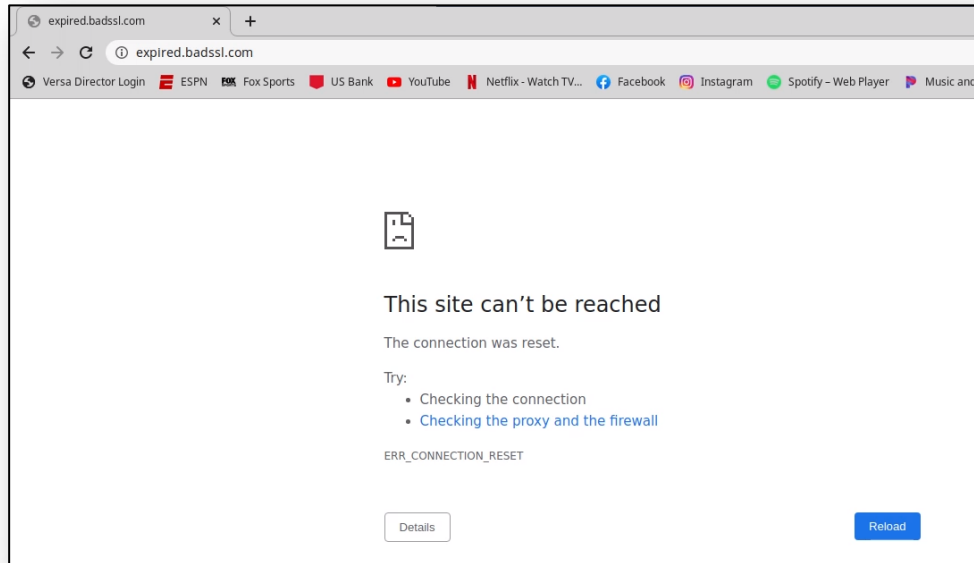
Decryption Profile*

View Decryption Profile

6.ae. Return to the remote desktop client (Remmina Linux RDP).

6.af. In the Linux testing client, navigate to the site *expired.badssl.com* to view the inspection results.

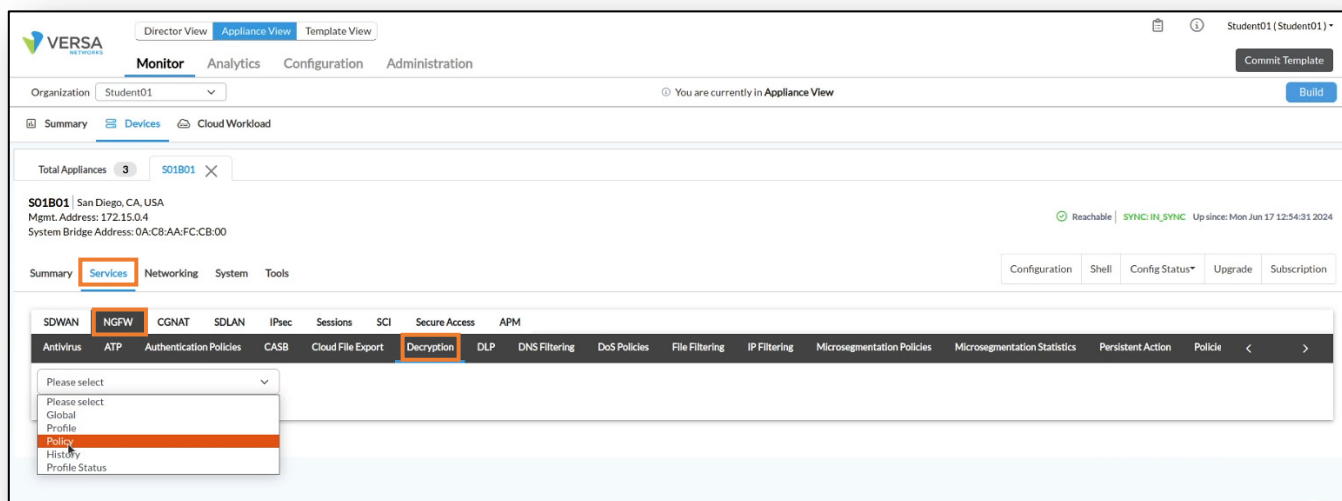
Note: The web page may be cached, so it will not be re-inspected. To force the inspection of the web site, navigate to one of the other sites in the bookmark bar (e.g. ESPN), then enter the *expired.badssl.com* URL in the browser again. The site should now be blocked.



Step 7. 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.

- 7.a. Close the remote browser connection to the testing host and return to your remote desktop.
- 7.b. In your remote desktop, navigate to the *Monitor* tab of your appliance.
- 7.c. In the *Monitor* tab of your appliance, select the *Service > NGFW > Decryption*.
- 7.d. In the *Services* dashboard, select *NGFW* to display the *Next Generation Firewall* statistics.
- 7.e. In the *Decryption* table, select *Policy > Default-Policy* from the drop-down menu.

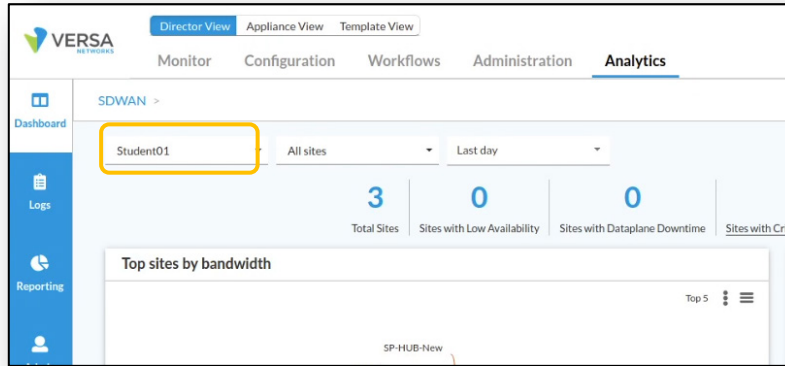


You should see non-zero counters in all of the rules. The rules display how many sessions have matched each of the rules.

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

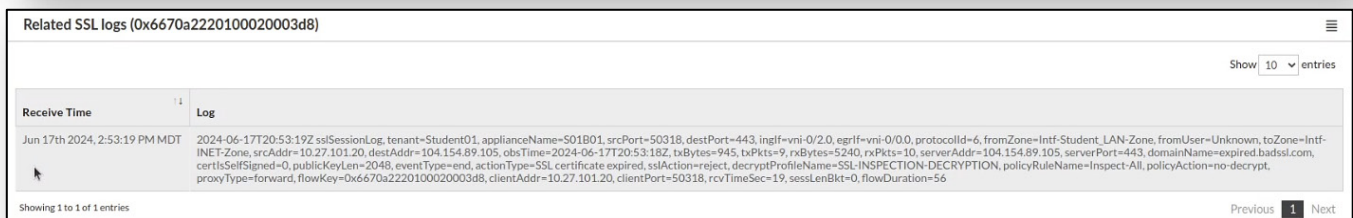
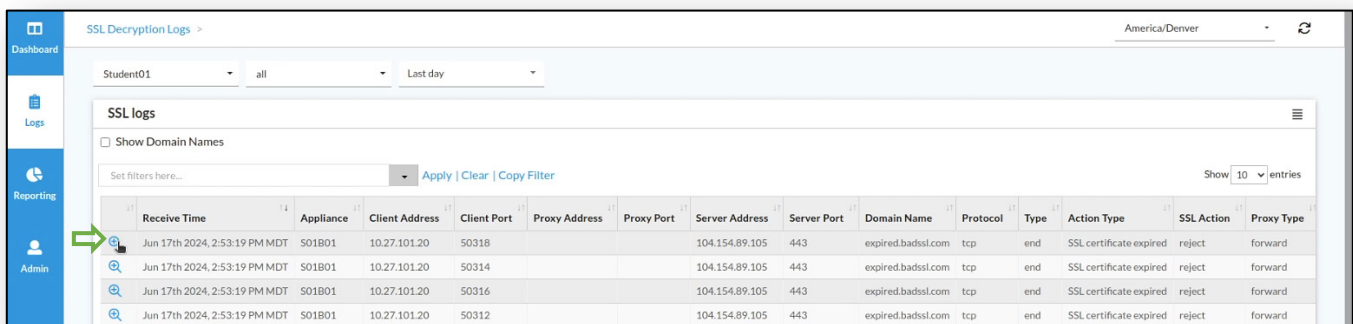
- 7.f. Select *Profile* from the left drop-down menu to display the profile statistics. This will display the number of packets that have been inspected, decrypted, and dropped by the encryption profile.

- 7.g. Click the *Director View* button to exit *Appliance View*.
- 7.h. 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.



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



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!

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.

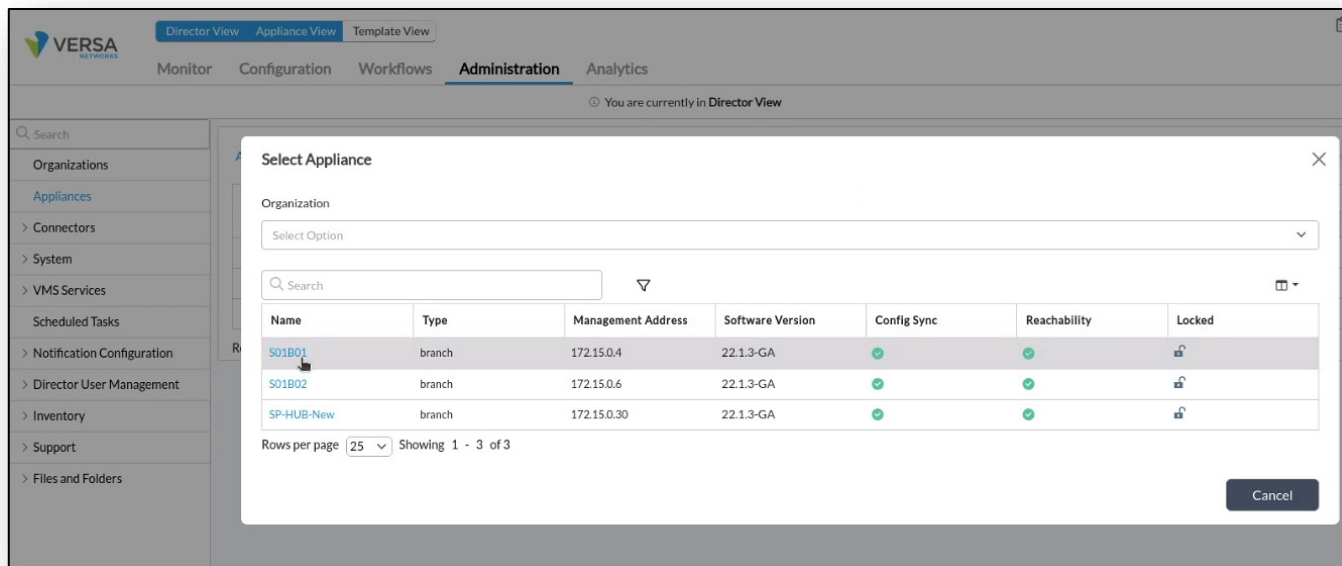
Refer to the Lab Access lab guide for instructions on how to connect to the lab environment and access Versa Director.

- 7.a. Reset the lab to a base configuration.
- 7.b. Open a remote desktop connection to the lab environment.
- 7.c. In the remote desktop, open Google Chrome, then click on the web bookmark to open Versa Director (or navigate to 10.27.1.10 in the browser address bar).
- 7.d. In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the device workflow to your SxxB01 device. In the *Basic* tab, ensure that the device is assigned to the *DG-Sxx-SFW* device group, where *Sxx* is your organization/student ID. 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.
- 7.e. Click the *Commit Template* button in the top-right corner of Versa Director.
- 7.f. Select your student ID as the tenant from the organization drop-down menu, select the *Template-Sxx-SFW* from the *Select Template* menu, then click the *Fetch Devices* button to display devices associated with the template.
- 7.g. Check the box next to your *B01* branch device, and click *Review*.
- 7.h. In the *Review* dashboard, click *Commit* to reconfigure the device with the SFW configuration.

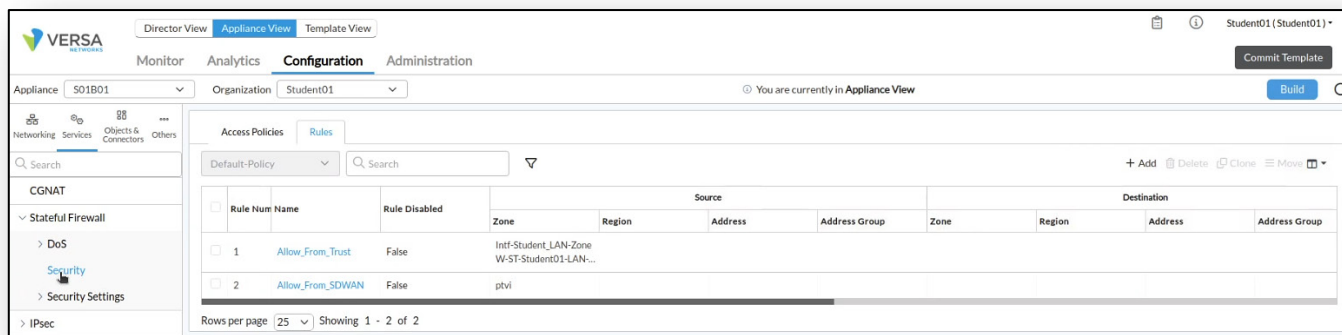
Step 1. Create Stateful Firewall Rules

In the following steps you will:

- Create 5 Stateful Firewall Rules in Appliance View; and
- Verify that the Stateful Firewall rules are applied.
 - 1.a. In *Director View*, navigate to the *Administration > Appliances* dashboard.
 - 1.b. Locate your device in the appliance table and click your device name to open the *Appliance View* of your branch device.



- 1.c. In the *Appliance View* of your device, select the *Services* configuration tab to view the available services. You should see *Stateful Firewall* services in the configuration tab.
- 1.d. Select *Security* under the *Stateful Firewall* service.



1.e. Click the + *Add* button to add a new security rule with the following properties:

<p>General Tab</p> <ul style="list-style-type: none"> Block-Outbound-SSH-INT 	<p>Source Tab</p> <ul style="list-style-type: none"> Source Zone: Click + and add Intf-Student_LAN-Zone
<p>Destination Tab</p> <ul style="list-style-type: none"> Destination Zone: Click + and add Intf-INET-Zone 	<p>Headers/Schedule Tab</p> <ul style="list-style-type: none"> Services: Click + and add ssh
<p>Enforce Tab</p> <ul style="list-style-type: none"> Action: Deny Log: Both; check the Default Profile box 	

Add Rule [Close]

General | Source | Destination | Headers/Schedule | Enforce

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

Description Tags

Disable Rule

OK **Cancel**

Add Rule [Close]

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

<input type="checkbox"/> Source Zone + New Zone + [trash] [refresh]	<input type="checkbox"/> Source Address + New Address + New Address Group + [trash] [refresh]
<input type="checkbox"/> Intf-Student_LAN-Zone [eye]	Source Address Not Configured
<input type="checkbox"/> Custom Geo Circle + [trash] [refresh]	<input type="checkbox"/> Region + [trash] [refresh]
Custom Geo Circle Not Configured	Region Not Configured

Add Rule

General Source **Destination** Headers/Schedule Enforce

<input type="checkbox"/> Destination Zone + New Zone + [trash] [lock]	<input type="checkbox"/> Destination Address + New Address + New Address Group + [trash] [lock]
<input type="checkbox"/> Intf-INET-Zone [eye]	Destination Address Not Configured
<input type="checkbox"/> Custom Geo Circle + [trash] [lock]	<input type="checkbox"/> Region + [trash] [lock]
Custom Geo Circle Not Configured	Region Not Configured

Add Rule

General Source Destination **Headers/Schedule** Enforce

IP IP Version: --Select-- IP Flags: --Select-- DSCP: [input] +	Others Schedules: --Select-- + Schedule
TTL Condition: Greater than or equal to Value (Max 255): [input]	Services Service List: + New Service + [trash] [lock] ssh [eye]

OK Cancel

Add Rule

General Source Destination Headers/Schedule **Enforce**

Log <input type="radio"/> Start <input type="radio"/> End <input checked="" type="radio"/> Both <input type="radio"/> Never LEF Profile: --Select-- Default Profile [checked]	Action <input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Reject
	Synced Flow Synced Flow: --Select--

OK Cancel

Step 2. Create 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.

2.a. Click the + Add button to add another stateful firewall rule with the following properties.

General Tab

- Allow-Inbound-ICMP-B2B

Source Tab

- Click + and add Source Zone: ptvi

Destination Tab

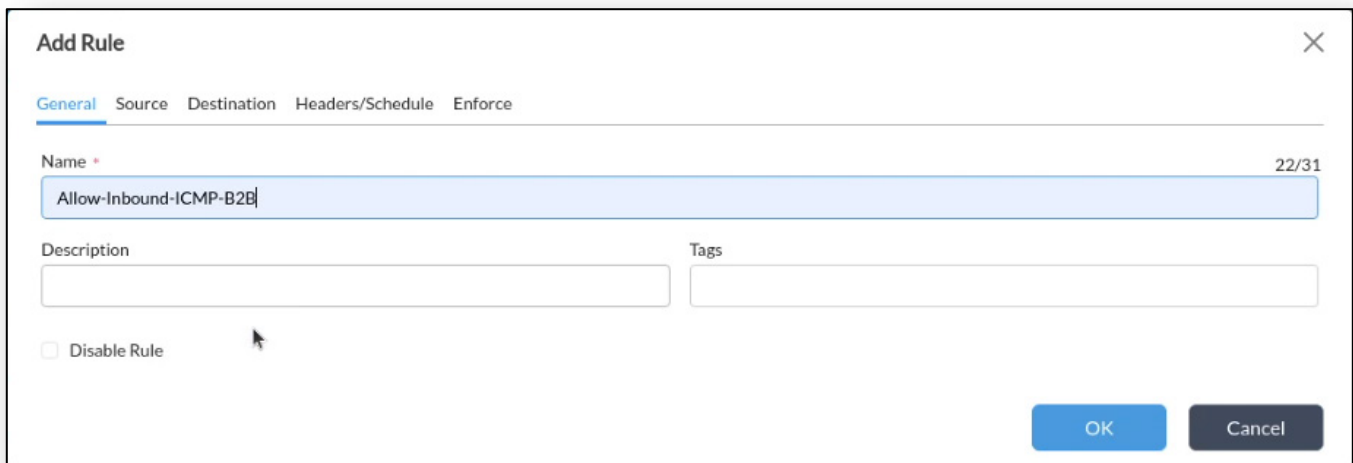
- Destination Zone: Click + and add Intf-Student_LAN-Zone

Headers/Schedule Tab

- Services: Click + and add ICMP

Enforce Tab

- Action: Allow
- Log: Both; check the Default Profile box



Add Rule [Close]

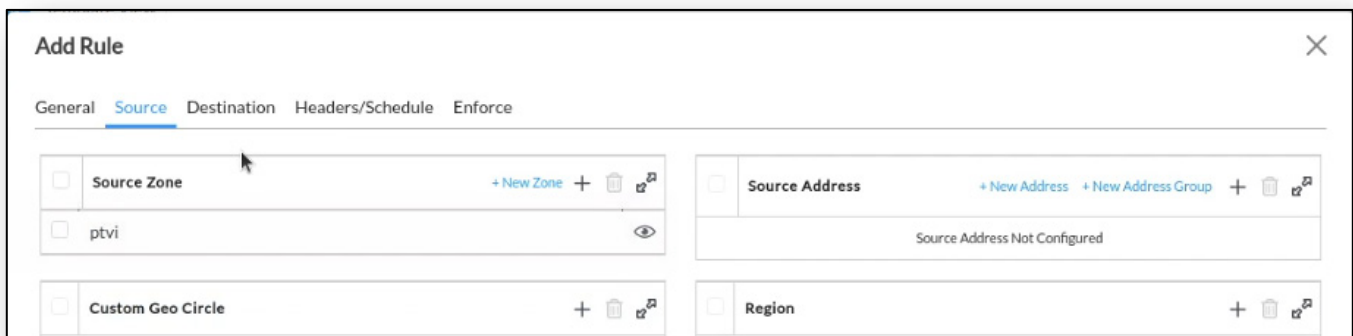
General | Source | Destination | Headers/Schedule | Enforce

Name * 22/31

Description

Tags

Disable Rule



Add Rule [Close]

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

<input type="checkbox"/> Source Zone + New Zone + [trash] [help]	<input type="checkbox"/> Source Address + New Address + New Address Group + [trash] [help]
<input type="checkbox"/> ptvi [eye]	Source Address Not Configured
<input type="checkbox"/> Custom Geo Circle + [trash] [help]	<input type="checkbox"/> Region + [trash] [help]

Add Rule

General Source **Destination** Headers/Schedule Enforce

Destination Zone + New Zone + + -

Intf-Student_LAN-Zone

Destination Address + New Address + New Address Group + + -

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 + New Service + + -
 ICMP

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--

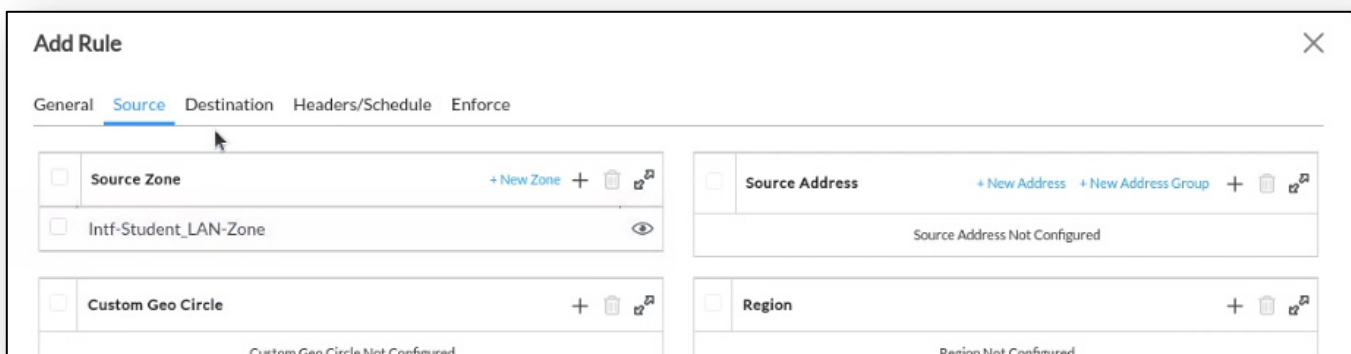
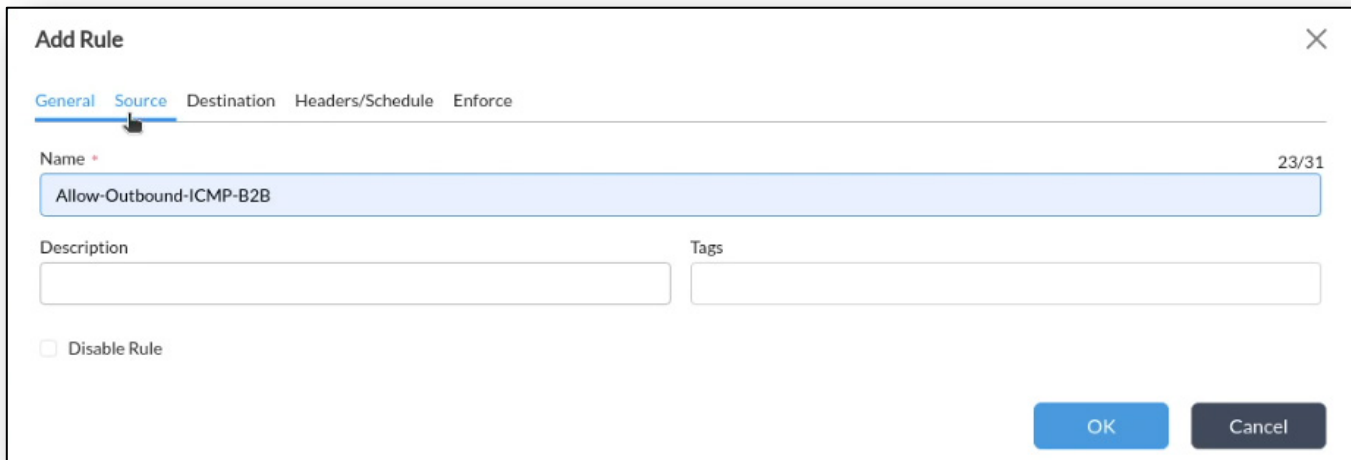
OK Cancel

Step 3. Create 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.

3.a. Click the + Add button to add another stateful firewall rule with the following properties.

<p>General Tab</p> <ul style="list-style-type: none"> • Allow-Outbound-ICMP-B2B 	<p>Source Tab</p> <ul style="list-style-type: none"> • Source Zone: Click + and add Intf-Student_LAN-Zone
<p>Destination Tab</p> <ul style="list-style-type: none"> • Destination Zone: Click + and add ptvi 	<p>Headers/Schedule Tab</p> <ul style="list-style-type: none"> • Services: Click + and add ICMP
<p>Enforce Tab</p> <ul style="list-style-type: none"> • Action: Allow • Log: Both; check the Default Profile box 	



Add Rule

General Source **Destination** Headers/Schedule Enforce

<input type="checkbox"/> Destination Zone + New Zone + [trash] [help]	<input type="checkbox"/> Destination Address + New Address + New Address Group + [trash] [help]
<input type="checkbox"/> ptvi [eye]	Destination Address Not Configured
<input type="checkbox"/> Custom Geo Circle + [trash] [help]	<input type="checkbox"/> Region + [trash] [help]
Custom Geo Circle Not Configured	Region Not Configured

Add Rule

General Source Destination **Headers/Schedule** Enforce

IP IP Version: --Select-- IP Flags: --Select-- DSCP: [input] +	Others Schedules: --Select-- + Schedule
TTL Condition: Greater than or equal to Value (Max 255): [input]	Services <input type="checkbox"/> Service List + New Service + [trash] [help] <input type="checkbox"/> ICMP [eye]

OK Cancel

Add Rule

General Source Destination Headers/Schedule **Enforce**

Log <input type="radio"/> Start <input type="radio"/> End <input checked="" type="radio"/> Both <input type="radio"/> Never LEF Profile: --Select-- [checkbox] Default Profile	Action <input checked="" type="radio"/> Allow <input type="radio"/> Deny <input type="radio"/> Reject
	Synced Flow Synced Flow: --Select--

OK Cancel

Step 4. Create 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.

4.a. Click the + Add button to add another stateful firewall rule with the following properties.

General Tab <ul style="list-style-type: none"> Block-Outbound-HTTP-B2B-Hub 	Source Tab <ul style="list-style-type: none"> Source Zone: Click + and add Intf-Student_LAN-Zone
Destination Tab <ul style="list-style-type: none"> Destination Zone: Click + and add ptvi Destination Address: Click + New Address <ul style="list-style-type: none"> New Address: <ul style="list-style-type: none"> Name: Hub-HTTP-80 Type: IPv4 Address: 10.27.13.20/32 	Headers/Schedule Tab <ul style="list-style-type: none"> Services: Click + New Service <ul style="list-style-type: none"> New Service properties: <ul style="list-style-type: none"> Name: Custom-HTTP-80 Protocol: TCP Port Range (Port): 80
Enforce Tab <ul style="list-style-type: none"> Action: Deny Log: Both; check the Default Profile box 	

Add Rule [Close]

General | Source | Destination | Headers/Schedule | Enforce

Name ^{*} 27/31
Block-Outbound-HTTP-B2B-Hub

Description Tags

Disable Rule

Add Rule [Close]

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

Source Zone + New Zone + [trash] [refresh]

Intf-Student_LAN-Zone [eye]

Source Address + New Address + New Address Group + [trash] [refresh]

Source Address Not Configured

Add Rule

General Source **Destination** Headers/Schedule Enforce

<input type="checkbox"/> Destination Zone	+ New Zone +	<input type="checkbox"/> Destination Address	+ New Address + New Address Group +
<input type="checkbox"/> ptvi		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

OK Cancel

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
--	--

OK Cancel

Add a new Service

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

General Source Destination Headers/Schedule **Enforce**

Log <input type="radio"/> Start <input type="radio"/> End <input checked="" type="radio"/> Both <input type="radio"/> Never LEF Profile: --Select-- <input checked="" type="checkbox"/> Default Profile	Action <input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Reject Synced Flow Synced Flow: --Select--
--	--

OK Cancel

Step 5. Create Rule 5

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

5.a. Click the + Add button to add another stateful firewall rule with the following properties.

<p>General Tab</p> <ul style="list-style-type: none"> • Allow-Local-Outbound-Internet 	<p>Source Tab</p> <ul style="list-style-type: none"> • Source Zone: Click + and add Intf-Student_LAN-Zone
<p>Destination Tab</p> <ul style="list-style-type: none"> • Click + and add zone Intf-INET-Zone 	<p>Headers/Schedule Tab</p> <ul style="list-style-type: none"> • Services: Click + and add: <ul style="list-style-type: none"> • http • https • domain
<p>Enforce Tab</p> <ul style="list-style-type: none"> • Action: Allow • Log: Both; check the Default Profile box 	

Add Rule

General Source Destination Headers/Schedule Enforce

Name * 29/31

Allow-Local-Outbound-Internet

Description Tags

Disable Rule

OK **Cancel**

Add Rule

General **Source** Destination Headers/Schedule Enforce

<input type="checkbox"/> Source Zone + New Zone +	<input type="checkbox"/> Source Address + New Address + New Address Group +
<input type="checkbox"/> Intf-Student_LAN-Zone	Source Address Not Configured

Add Rule

General Source **Destination** Headers/Schedule Enforce

<input type="checkbox"/>	Destination Zone	+ New Zone +	🗑️	👁️
<input type="checkbox"/>	Intf-INET-Zone			👁️

<input type="checkbox"/>	Destination Address	+ New Address + New Address Group +	🗑️	👁️
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

<input type="checkbox"/>	Service List	+ New Service +	🗑️	👁️
<input type="checkbox"/>	domain			👁️
<input type="checkbox"/>	http			👁️
<input type="checkbox"/>	https			👁️

OK Cancel

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--

OK Cancel

Step 6. Place the rules in the proper order.

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

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

6.a. In the rule list, click and drag the rules so that they appear in the list according to the above order.

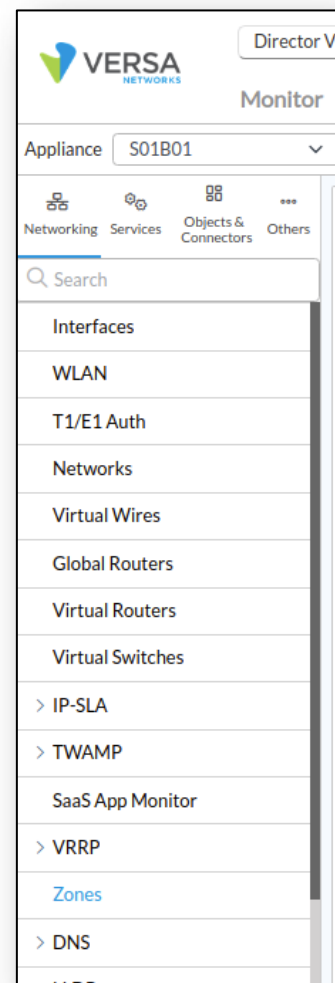
EXPLORE NETWORK ZONES

Step 1. Locate and explore the zone configurations.

1.a. 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						

1.b. 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

Step 2. Verify the automatic NAT configuration.

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.

2.a. 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		10.0.0/8 172.16.0/12 192.168.0/16	10.0.0/8 172.16.0/12 192.168.0/16			
Speed-Test-INET		napt-44			Pool-INET		
Speed-Test-MPLS		napt-44			Pool-MPLS		

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 testing host shell to run the test commands.

Step 1. Open an SSH session from the remote desktop to the Linux testing client

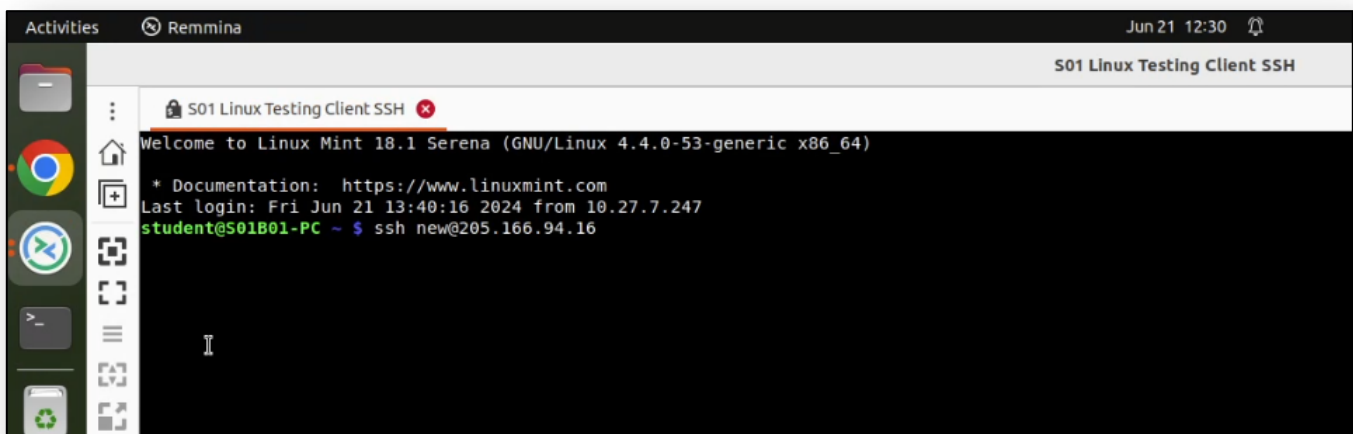
- 1.a. On your remote desktop, open the *Remmina* application.
- 1.b. Use the *Remmina* application to open an SSH session to the Linux Testing Client associated with your branch. Use the username *student* and password *versa123* if prompted.
- 1.c. From the shell prompt on the Linux Testing Client, 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.

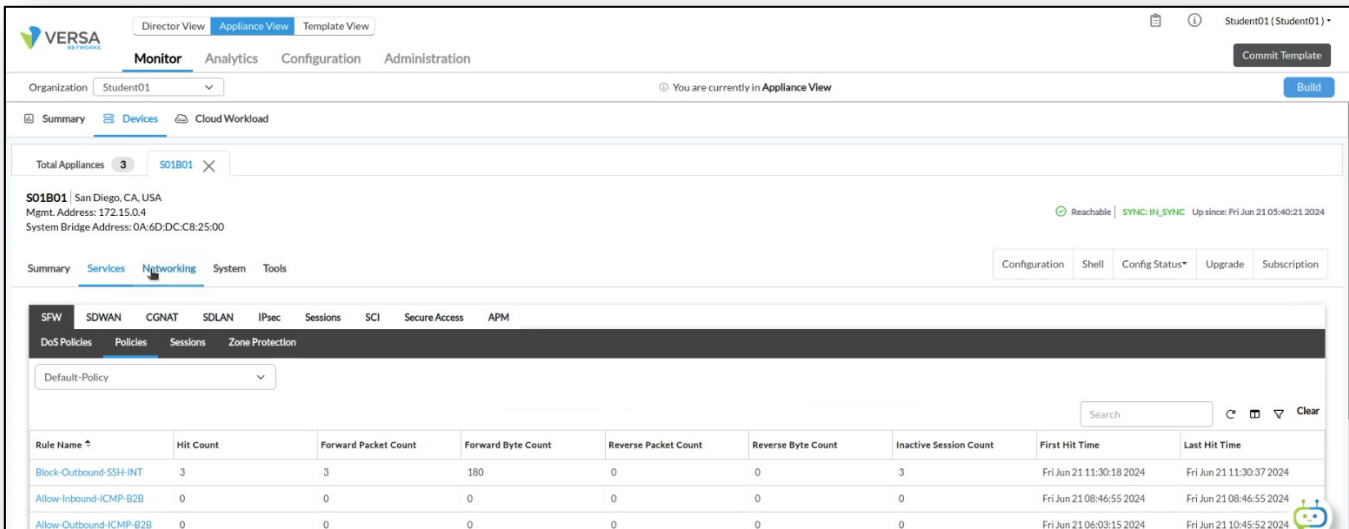
Note: If you don't see log entries in Versa Analytics, ensure that you enabled the logging action in the Enforce tab of your security rules.

Step 2. Test the Block-Outbound-SSH-INT rule

- 2.a. From the shell in the testing linux host, run the command `ssh new@205.166.94.16`. This command should fail.



- 2.b. To verify that the session failed due to the security rule, return to the Versa Director user interface.
- 2.c. From the Versa Director user interface, click the *Appliance View* tab at the top of the interface.
- 2.d. Locate your *B01* device in the device list, then click on the device to open the *Appliance View* of your *B01* device.
- 2.e. From *Appliance View* of your *B01* device, navigate to the *Monitor > Services > SFW > Policies* dashboard.
- 2.f. From the *Policies* dashboard, select the *Default-Policy* from the drop-down menu. This should display the list of rules that you created.
- 2.g. Verify that the *Block-Outbound-SSH-INT* rule has a non-zero value in the *Hit Count* table.



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

Step 3. Test Rules 2 and 3

In this step you will test the Allow-Inbound-ICMP-B2B and Allow-Outbound-ICMP-B2B firewall 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.

- 3.a. Return to the SSH session to the Linux testing client.
- 3.b. From the shell prompt on the testing PC, run the command: **ping 10.27.13.20 -c 5** to initiate ICMP traffic towards the hub LAN network. The command should be successful.
- 3.c. To verify the security rule, return to *Versa Director* and navigate to the *Appliance View* of your device.
- 3.d. In the *Monitor* tab navigate to *Services > SFW > Policies* and select the *Default-Policy*.
- 3.e. 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

- 3.f. Using the Remmina application, open an SSH session to your B02 VOS device.
- 3.g. On your B02 VOS device, type *cli* to start the command line interface.
- 3.h. 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/Student	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.

- 3.i. Return to the *Versa Director* user interface.
- 3.j. Click on *Director View* at the top of the user interface.

- 3.k. From the *Director View*, click on the *Analytics* tab to open the Versa Analytics dashboards.
- 3.l. 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.
- 3.m. 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.

Step 4. Verify the Block-Outbound-HTTP-B2B-Hub rule

- 4.a. On the remote landing station, use the *Remmina* application to open an RDP session to your Linux Testing Host.
- 4.b. Use the username *student* and password *versa123* if prompted.
- 4.c. From the test host, open the *Chromium* web browser.
- 4.d. From the Chromium browser on the testing client, enter the address *http://10.27.13.20*. The policy in the VOS device should still intercept the attempt and block it.

Monitor tab verification

- 4.e. Return to the *Versa Director* user interface.
- 4.f. From *Versa Director*, open the *Appliance View* of your B01 device.
- 4.g. In the *Appliance View* of your B01 device, navigate to the *Monitor* dashboard.
- 4.h. From the *Monitor* dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created in previous steps should be listed.
- 4.i. 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

- 4.j. Click the *Director View* icon to return to the main Versa Director UI.
- 4.k. Click on the *Analytics* tab to open the Versa Analytics dashboards.
- 4.l. 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.
- 4.m. 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*.

Step 5. Verify the Allow-Local-Outbound-Internet rule

- 5.a. Return to the Remmina remote desktop session to the Linux testing client.
- 5.b. Use the username *student* and password *versa123* if prompted.
- 5.c. From the test host, open the *Chromium* web browser.
- 5.d. From the *Chromium* browser on the testing linux client, navigate to the address *https://google.com*. The web page should open.

Monitor Tab Verification

- 5.e. Return to the *Versa Director* user interface.
- 5.f. From *Versa Director*, navigate to the *Appliance View* and select your *B01* appliance from the list.
- 5.g. 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.
- 5.h. 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

- 5.i. Click the *Director View* button to return to the main *Versa Director* UI.
- 5.j. Click on the *Analytics* tab to open the *Versa Analytics* dashboards.
- 5.k. 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.
- 5.l. 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! 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.

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 1. Reset the lab to a base configuration

You will begin by loading a baseline configuration on your branch devices.

- 1.a. Connect to the lab environment using the steps provided by your instructor.
- 1.b. In the remote desktop, open the Google Chrome browser.
- 1.c. In the Google Chrome browser on the remote desktop, open the link to *Versa Director* (bookmark bar) or use the address 10.27.1.10. Login using the username and password provided by your instructor.
- 1.d. In Versa Director, navigate to *Workflows > Devices > Devices*.
- 1.e. Open the workflow to your *SxxB01* device.
- 1.f. In the *Basic* tab, ensure that the device is assigned to the *DG-Sxx-NGFW* device group. If you need to change the device group assigned to your branch device, be sure to click *Re-deploy* to apply the changes to the device in *Versa Director*.
- 1.g. Click the *Commit Template* button in the top-right corner of Versa Director.
- 1.h. Select your student ID (tenant name) from the organization drop-down menu.
- 1.i. Select the *Template-Sxx-NGFW* from the Select Template menu.
- 1.j. Click *Fetch Devices*. Your B01 device should be displayed.
- 1.k. Check the box next to your B01 branch device, and click *Review*
- 1.l. Click *Commit* to overwrite the configuration on the device with the base configuration.

Step 2. Configure DoS Profiles

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.

- 2.a. In Versa Director, click *Appliance View* at the top of the dashboard. This will open a table of your devices.
- 2.b. From the devices table, click your *B01* device. This will open the Appliance View of the B01 device.
- 2.c. In the *Appliance View* of your appliance, click on the *Configuration* tab to open the device configuration.
- 2.d. From the left-side menu, navigate to *Services > Next Gen Firewall > DoS > Profiles*.
- 2.e. In the *DoS Profiles* dashboard click on the + button to create a new DoS profile.
- 2.f. In the *DoS Profile* dialog, enter the following parameters:

DOS Profile 1	
Profile Name:	Classified-DoS-Profile
ProtectionOptions:	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 Maximum Rate Packets/sec: 10 Drop Period Seconds: 30

- 2.g. Click *OK* to create the DoS profile when finished.

Add DoS Profile ✕

Name * 22/31

Description Tags

Type
 Aggregate Profile Classified Profile

Classification Key Max Sessions

Flood Protection

Protocol	Enable	Alarm Rate Packets (seconds)	Activate Rate Packets (seconds)	Maximum Rate Packets (seconds)	Drop Period (seconds)	Actions
TCP	<input checked="" type="checkbox"/>	<input type="text" value="5"/>	<input type="text" value="7"/>	<input type="text" value="10"/>	<input type="text" value="30"/>	SYN Cox ▾
UDP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	
ICMP	<input checked="" type="checkbox"/>	<input type="text" value="5"/>	<input type="text" value="7"/>	<input type="text" value="10"/>	<input type="text" value="30"/>	
Other IP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	

Step 3. Create DoS Policy Rules

You will now create rules in a DoS 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

3.a. In your device configuration (Appliance View), navigate to *Services > Next Gen Firewall > DoS > Policies*.

3.b. Navigate to the *Rules* tab to add rules to the *Default-Policy* policy. Add the following rule:

<p>General Tab:</p> <ul style="list-style-type: none"> • Name: DoS-Classified-Hub-Rule 	<p>Source Tab:</p> <ul style="list-style-type: none"> • Source Zone: Click + and add Intf-Student_LAN-Zone
<p>Destination Tab:</p> <ul style="list-style-type: none"> • Destination Address: Click + and add: <ul style="list-style-type: none"> • Address Name: HUB-HTTP-80 • Type: IPv4 • IPv4 Address/Prefix: 10.27.13.20/32 Intf-Student_LAN-Zone 	<p>Headers/Schedule Tab:</p> <ul style="list-style-type: none"> • Service List: Click + and add: <ul style="list-style-type: none"> • http • ICMP
<p>Enforce Tab</p> <ul style="list-style-type: none"> • Action: Protect • Logging Setting: Check the Default Profile box 	

3.c. Click OK to finish creating the policy.

Add DoS Rule

General **Source** Destination Headers/Schedule Enforce

Source Zone + New Zone + [trash] [refresh]

Intf-Student_LAN-Zone [eye]

Source Address + New Address + New Address Group + [trash] [refresh]

Source Address Not Configured

Source Address Negate

Region + [trash] [refresh]

Region Not Configured

State + [trash] [refresh]

State Not Configured

City + [trash] [refresh]

City Not Configured

Source Location Negate

Custom Geo Circle + [trash] [refresh]

Custom Geo Circle Not Configured

OK **Cancel**

Add DoS Rule

General Source **Destination** Headers/Schedule Enforce

Destination Zone + New Zone + [trash] [refresh]

Destination Address + New Address + New Address Group + [trash] [refresh]

Destination

Region + [trash] [refresh]

Destination

Custom

Add Address

Name *

HUB-HTTP-80

Description

Tags

Add a tag

Type *

IPv4

IPv4 Address/Prefix *

10.27.13.20/32

OK **Cancel**

OK **Cancel**

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--
+ Schedule

Service List + New Service + [] []
 http []
 ICMP []

OK Cancel

Add DoS Rule

General Source Destination Headers/Schedule Enforce

Action Setting
 Allow Deny Protect

Logging Setting
LEF Profile: --Select-- Default Profile

DDoS Profile
Aggregate Profile: --Select--
Classified Profile: Classified-DoS-Profile
View Profile

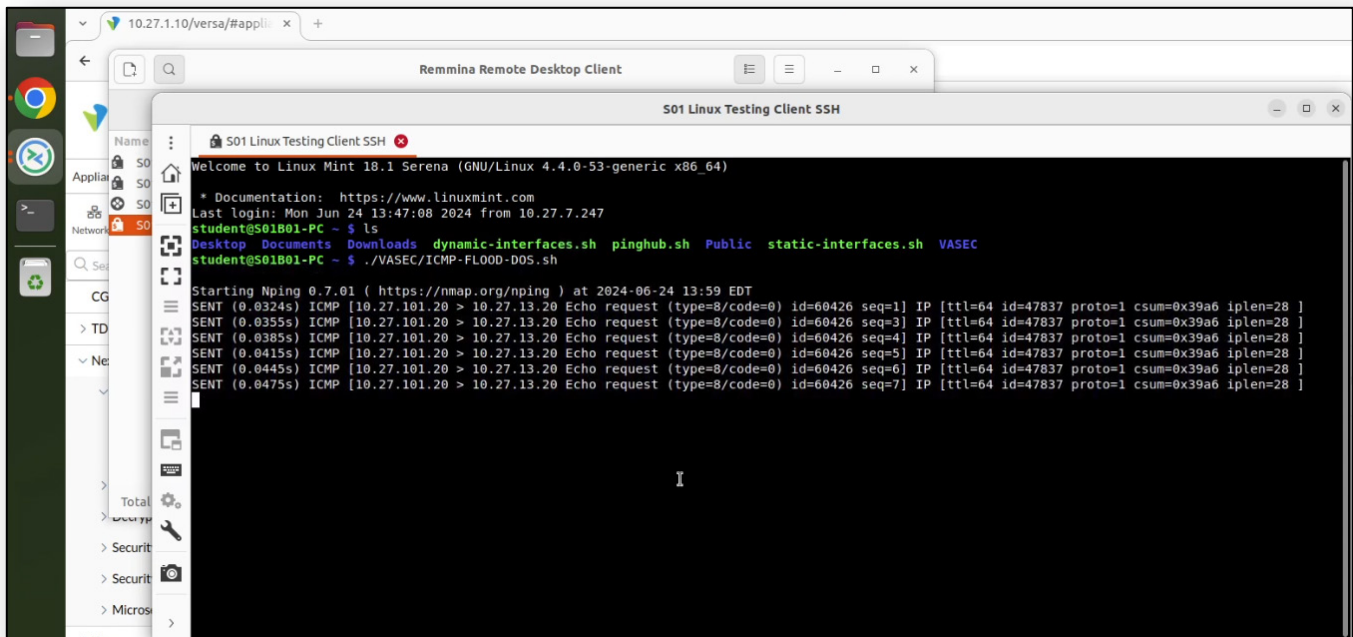
OK Cancel

Step 4. Verify the DoS Policy Protection

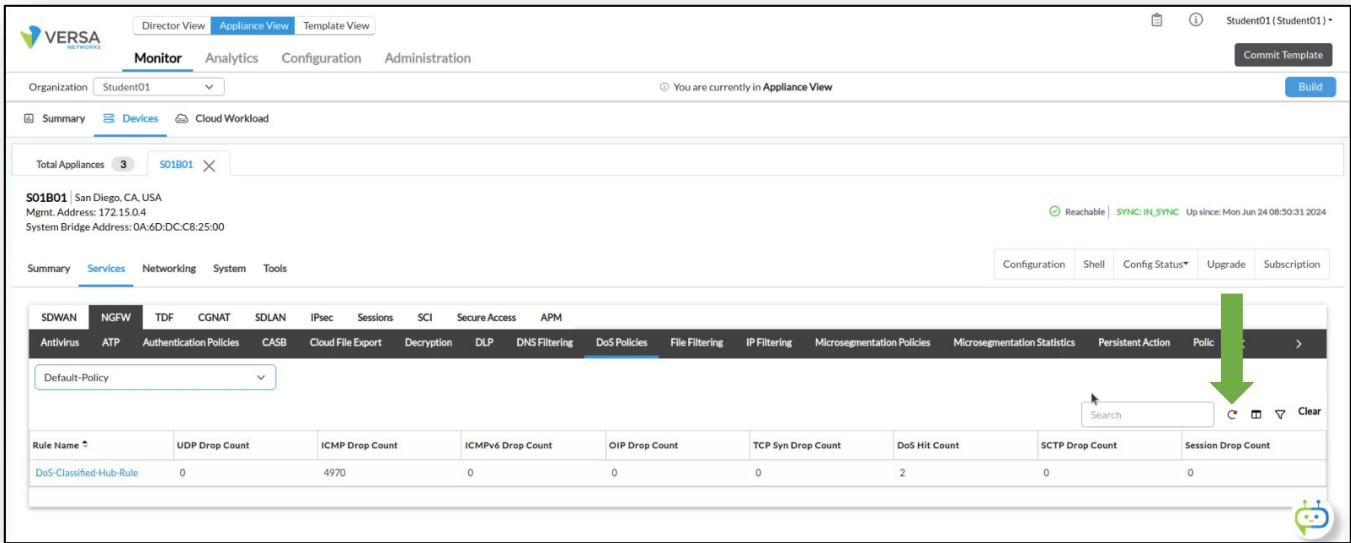
In the next steps you will verify that the DoS Protection rules and profile are functioning. To do this you will log into the test host connected to your B01 device and running traffic simulation scripts, then you will verify the behavior of the policies.

- 4.a. In the remote desktop, open the *Remmina* application.
- 4.b. From the Remmina application, open an ssh session to the Linux testing host device that is connected to your branch device. Use the username *student* and password *versa123*.
- 4.c. From the command prompt on the Linux testing station, perform the following tasks:

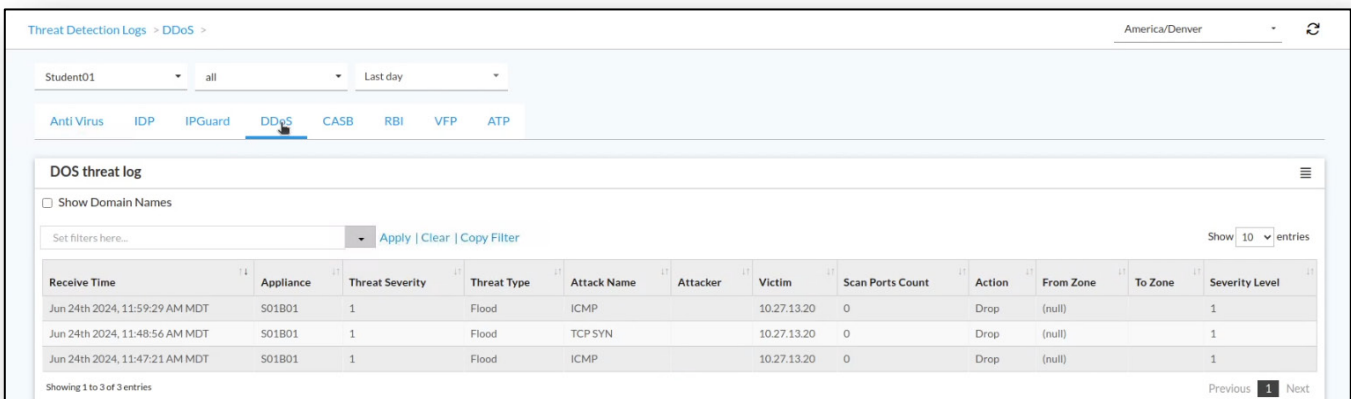
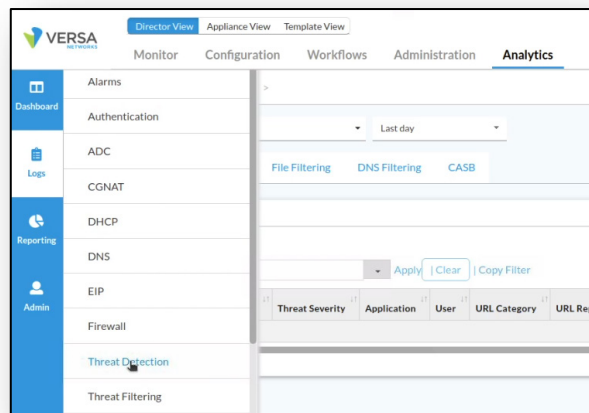
Verification Step 1	
Name:	ICMP Flood
Command to run:	From the command line on the testing host, run the command <code>./VASEC/ICMP-FLOOD-DOS.sh</code> Enter the password <i>versa123</i> if prompted.
Monitor Tab Verification:	<ul style="list-style-type: none"> Navigate to <i>Appliance View > SxxB01 > Monitor</i>. In the branch <i>Monitor</i> window, navigate to <i>Servcies > NGFW > DoS Policies</i> Verify that the <i>ICMP Drop Count</i> counter is incrementing.
Analytics Verification:	<ul style="list-style-type: none"> Click on the <i>Director View</i> button at the top of Versa Director. Click on the <i>Analytics</i> tab to open Versa Analytics In Versa Analytics, navigate to <i>Logs > Threat Detection</i> In the <i>Logs > Threat Detection</i> dashboard, open the <i>DDOS</i> tab. Verify that the ICMP flood logs with an action of <i>Drop</i> are displayed for your device.



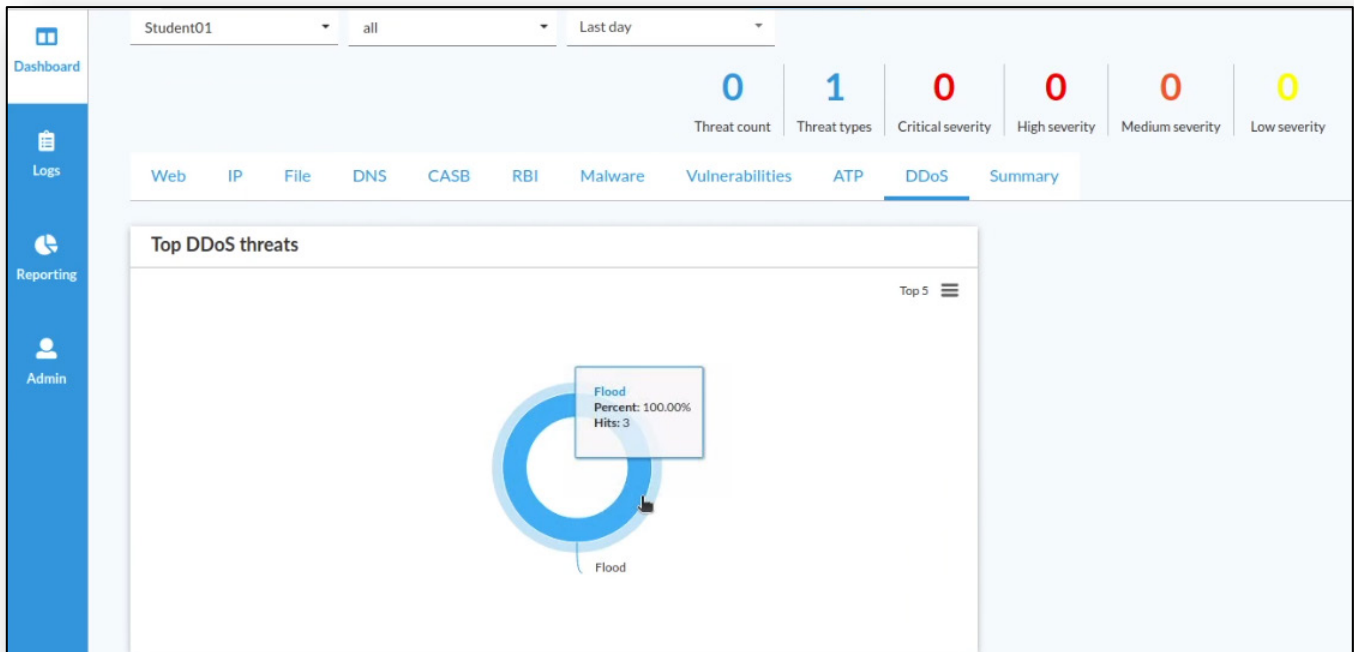
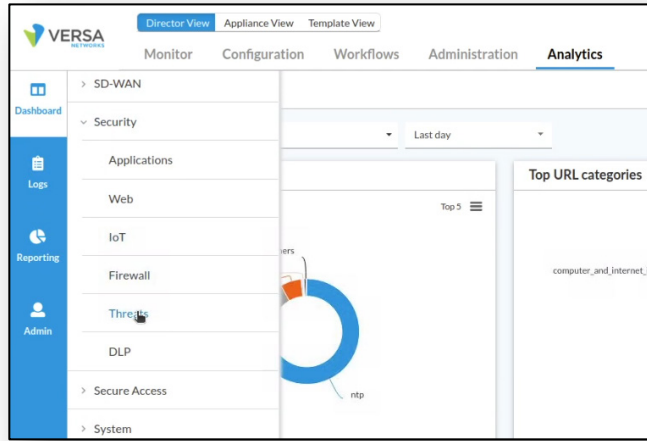
In the Monitor dashboard you can click the refresh button while the attack is in progress to see the drop counter increase.



Analytics logs record the log messages triggered by the event.



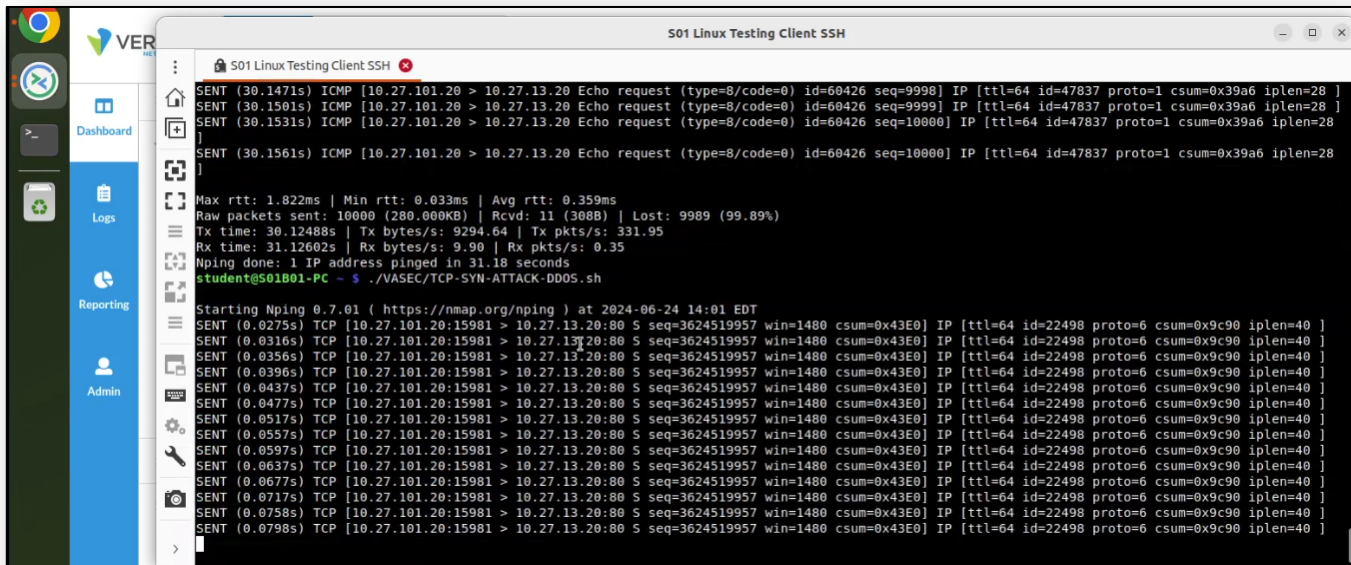
Analytics Dashboards provide a quick view of the event and history.



This screenshot shows a detailed view of 'DOS Threats (Flood)'. At the top, a bar chart shows the session count over time. Below the chart is a table with the following data:

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

Verification Step 2	
Name:	TCP SYN Flood
Command to run:	<ul style="list-style-type: none"> Return to the SSH session on the testing host. From the command line on the testing host, press <i>CTRL + C</i> to stop the flood attack. Run the command <code>./VASEC/TCP-SYN-ATTACK-DDOS.sh</code> 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:	<ul style="list-style-type: none"> Navigate to <i>Appliance View > SxxB01 > Monitor</i>. In the branch <i>Monitor</i> window, navigate to <i>Servcies > NGFW > DoS Policies</i> Select the <i>Default-Policy</i>. Verify that the <i>TCP-SYN Drop Count</i> counter is incrementing.
Analytics Verification:	<ul style="list-style-type: none"> Click on the <i>Director View</i> button at the top of Versa Director. Click on the <i>Analytics</i> tab to open Versa Analytics In Versa Analytics, navigate to <i>Logs > Threat Detection</i> In the <i>Logs > Threat Detection</i> dashboard, open the <i>DDOS</i> tab. Verify that the TCP SYN flood logs with an action of <i>Drop</i> are displayed for your device.



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

The screenshot shows the Versa Networks GUI in the 'Appliance View' for organization 'Student01'. The 'DoS Policies' section is active, showing a table of policies. The 'Default-Policy' is selected, and the 'DoS-Classified-Hub-Rule' is highlighted. The table shows the following counts:

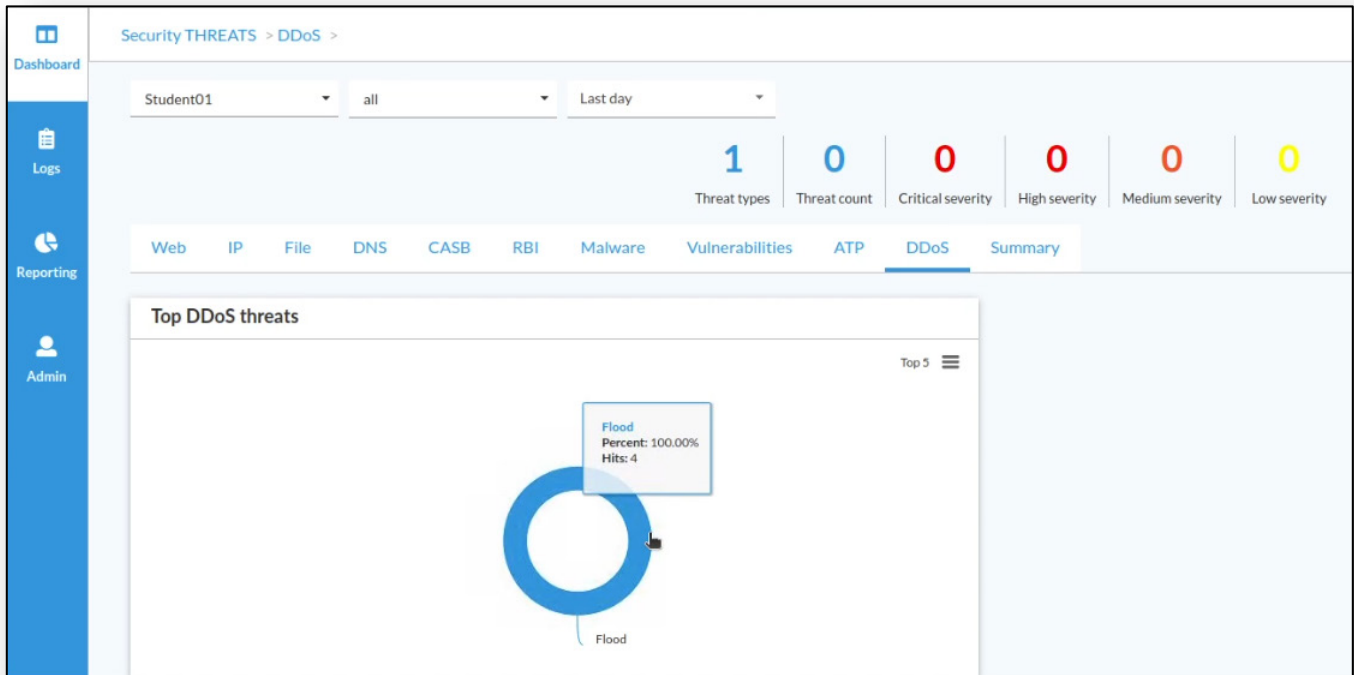
Rule Name	UDP Drop Count	ICMP Drop Count	ICMPv6 Drop Count	OIP Drop Count	TCP Syn Drop Count	DoS Hit Count	SCTP Drop Count	Session Drop Count
DoS-Classified-Hub-Rule	0	9989	0	0	3730	4	0	0

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

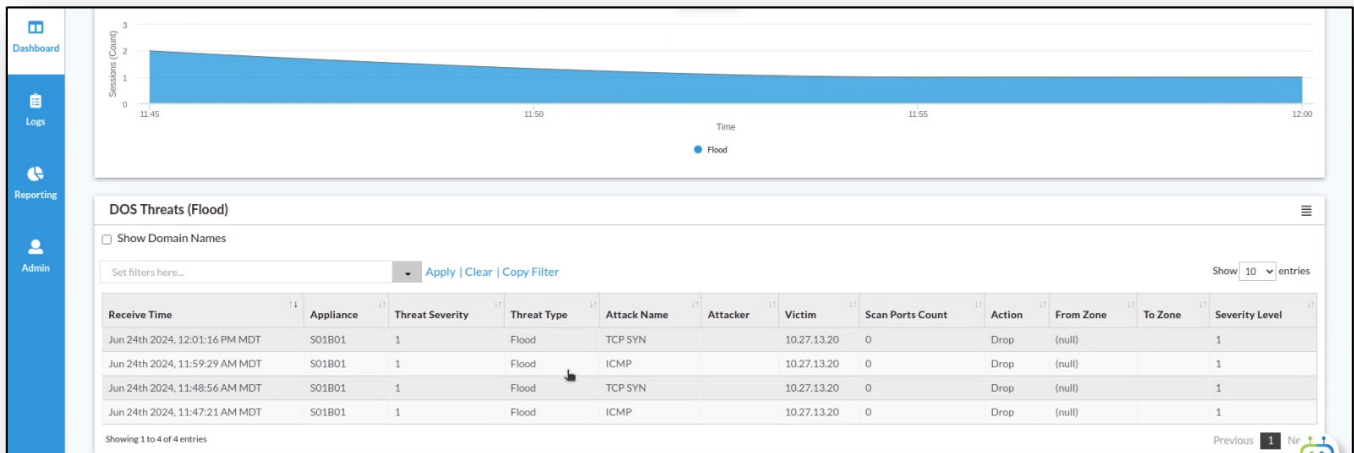
The screenshot shows the Versa Networks GUI in the 'Analytics' section, specifically the 'Threat Detection Logs > DDoS' view. The 'DOS threat log' is displayed, showing a table of attack entries. The table has the following columns: Receive Time, Appliance, Threat Severity, Threat Type, Attack Name, Attacker, Victim, Scan Ports Count, Action, From Zone, To Zone, and Severity Level. The entries are as follows:

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

Flood Hits increases in the DDoS Threats dashboard.



Click on the chart to view details.



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

APPLICATION FILTERING

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 custom application group 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 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.

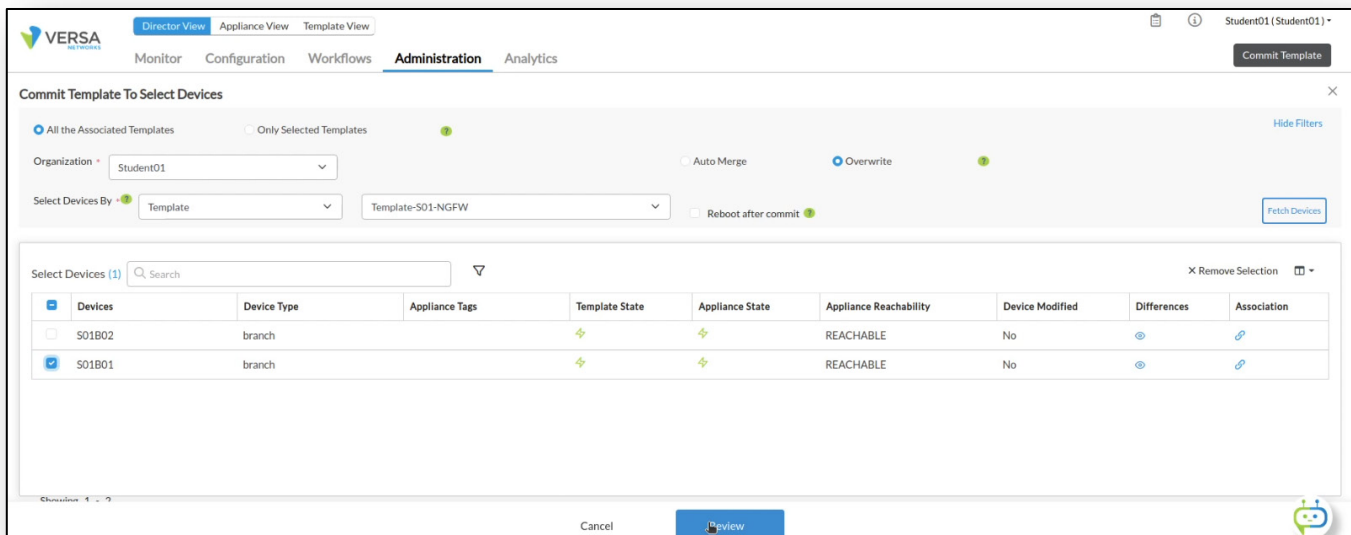
Note: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.

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 Environment

The first step of this lab is to reset your device to the base Next Generation Firewall configuration. To do so, perform the following tasks:

- 1.a. Log into Versa Director with your assigned username and password.
- 1.b. Click the *Commit Template* button in the top right corner of the Versa Director interface.
- 1.c. 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.
- 1.d. Click *Fetch Devices*. Your branch devices should be displayed.
- 1.e. From the *Select Devices* table, mark the box next to the *SxxB01* device, then click *Review*.
- 1.f. In the *Review* window, click *Commit* to apply the base configuration to your branch device.



The screenshot displays the 'Commit Template To Select Devices' dialog in the Versa Director interface. The 'Administration' tab is active, and the 'Commit Template' button is visible in the top right corner. The dialog includes the following elements:

- Organization:** Student01
- Select Devices By:** Template
- Template:** Template-S01-NGFW
- Fetch Devices:** A button to refresh the device list.
- Select Devices Table:**

Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
<input type="checkbox"/> S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗
- Buttons:** Cancel, Review

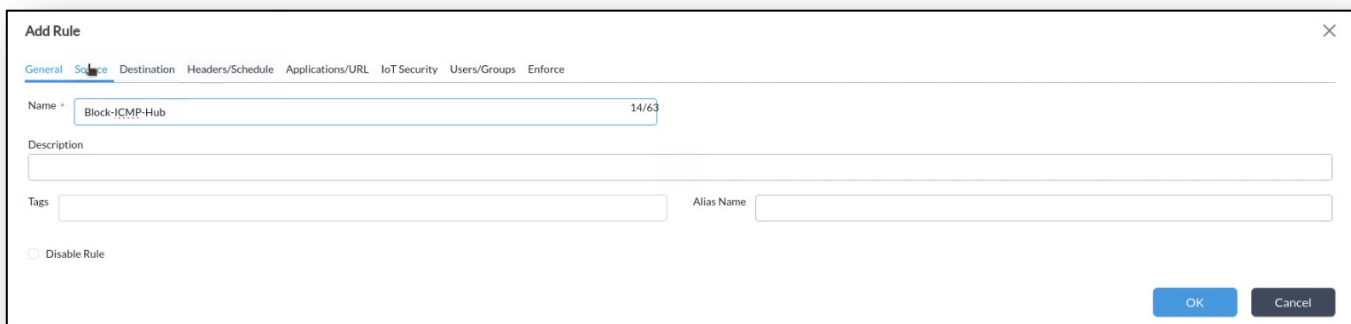
Step 2. Configure a rule to block ICMP traffic

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

- 2.a. In Versa Director, navigate to the *Appliance View* in Versa Director..
- 2.b. Click on your B01 appliance in the appliance table to open your appliance context mode. You will perform the configuration changes directly on your device.
- 2.c. In your B01 device configuration window, navigate to *Services > Next Gen Firewall > Security > Policies*. In the *Rules* tab you should see the 2 access rules generated by the template workflow.
- 2.d. In the *Rules* tab, click the + button to create a new rule with the following parameters.

ICMP Access Rule	
General Tab:	Name: Block-ICMP-Hub
Source/Destination Tabs:	Source Zone: Intf-Student_LAN-Zone Destination Zone: ptvi Destination Address: Click + New Address and add the following address: <ul style="list-style-type: none"> • Name: Hub • Type: IPv4 • IPv4 Address/Prefix: 10.27.13.20/32
Application/URL Tab:	Application: ICMP
Enforce Tab:	Action: Deny Log Events: Select both; check the Default Logging Profile box

- 2.e. Click OK to finish creating the rule.
- 2.f. Click and drag the rule so that it is at the top of the rule list.




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

Add Rule

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

Destination Zone: + New Zone + pvtl

Destination Address: + New Address + New Address Group + Destination Site Name: + Destination Site Name Not Configured

Region: Region 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

OK Cancel

OK Cancel

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

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Appliance: S01B01 Organization: Student01

Access Policies **Rules**

Default-Policy Search

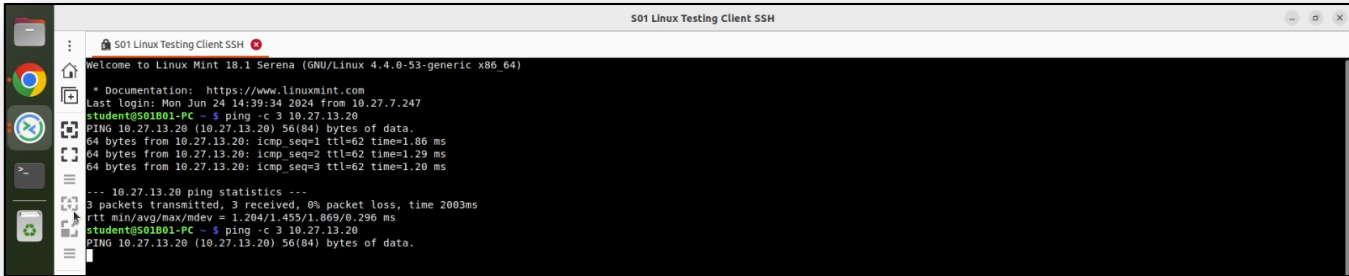
Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	Source
1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone					User Defined Devices
2	Allow_From_Trust	False		Intf-Student_LAN-Zone					W-ST-Student01-LAN...
3	Allow_From_SDWAN	False		pvtl					

Rows per page: 25 Showing 1 - 3 of 3

Step 3. Verify the Block-ICMP-Hub 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.

- 3.a. In the remote desktop, click on the *Remmina* application.
- 3.b. Open the *Remote Desktop (RDP)* connection to your Linux testing client. The username for the remote desktop session is *student* and password is *versa123* if prompted.
- 3.c. From the remote desktop of the Linux testing client, right-click the desktop and open a terminal window.
- 3.d. 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.



```
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 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 4. Analyze the statistics and logs for the Block-ICMP-Hub access rule

- 4.a. Return to the Versa Director user interface.
- 4.b. In Versa Director, navigate to the *Monitor* tab for your device (Appliance View).
- 4.c. Navigate to *Services > NGFW > Policies*. This should open the Monitor window for your branch appliance.
- 4.d. 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.
- 4.e. Click the *Director View* button at the top of the window.
- 4.f. From the main Versa Director dashboard, navigate to the *Analytics > Logs > Firewall* hierarchy.
- 4.g. 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.

Director View | Appliance View | Template View

Organization: Student01 | You are currently in Appliance View

Summary | **Devices** | Cloud Workload

Total Appliances: 3 | S01B01

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

Configuration | Shell | Config Status | Upgrade | Subscription

SDWAN | NGFW | TDF | CGNAT | SDLAN | IPsec | Sessions | SCI | Secure Access | APM

Antivirus | ATP | Authentication Policies | CASB | Cloud File Export | Decryption | DLP | DNS Filtering | DoS Policies | File Filtering | IP Filtering | Microsegmentation Policies | Microsegmentation Statistics | Persistent Action | **Policy**

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	-	-

Director View | Appliance View | Template View

Monitor | Configuration | Workflows | Administration | **Analytics**

Firewall > Logs > | Student01 | all | Last hour

0 | 2
Total Allowed | Total Denied

Logs | Charts | Maps

Firewall logs

Show Domain Names

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

Show 10 entries

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	URL Category	Protocol	Action	Type	Rule
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
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-Netflix

Step 5. Configure a rule to block Bit-Torrent

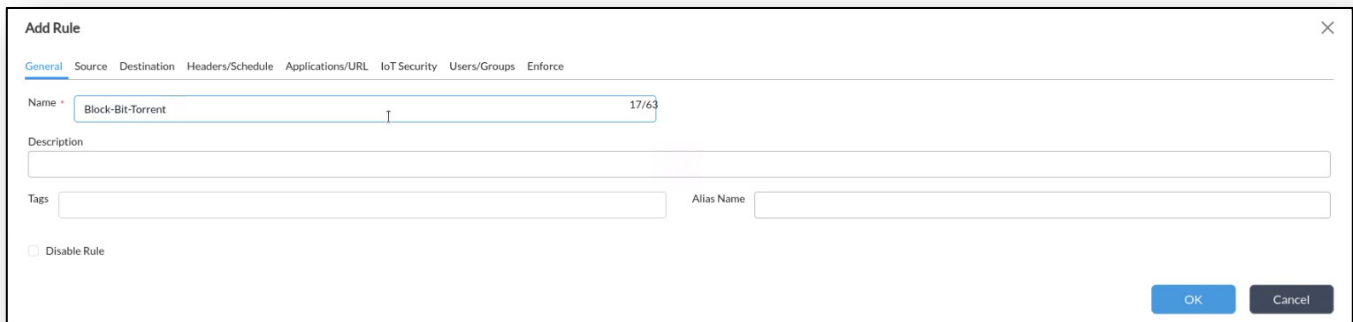
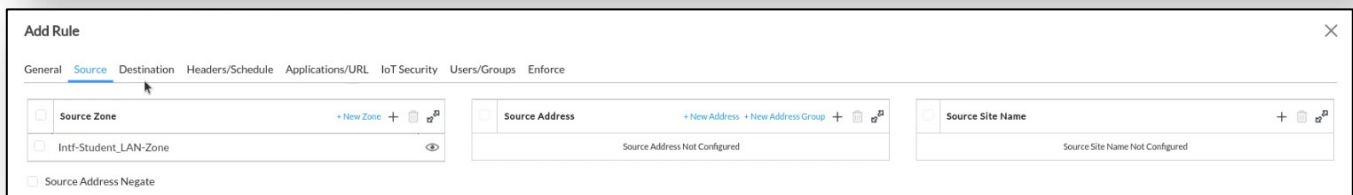
In the next steps you will create a rule that will block Bit Torrent related traffic by using the pre-defined applications that are built into the Versa Operating System.

- 5.a. Navigate to *Administration > Appliances*.
- 5.b. Click your branch *SxxB01* device in the appliance table to open the appliance context mode for your device. You will perform the configuration steps directly in your device.
- 5.c. In your device configuration tab, navigate to *Services > Next Gen Firewall > Security > Policies*.
- 5.d. In the *Rules* tab, click the + button to create a new access rule with the following parameters:

Block-Bit-Torrent Access Rule	
General Tab:	Name: Block-Bit-Torrent
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Intf-INET-Zone
Applications/URL Tab:	Add the following applications (use the + button): <ul style="list-style-type: none"> • BITTORRENT • BITTORRENT_APPLICATION • BITTORRENT_BUNDLE
Enforce Tab:	Action Reject Log Events: Both; check the Default Profile Box

- 5.e. Click OK to create the rule.
- 5.f. Drag and drop 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.

Add Rule [Close]

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

Destination Zone + New Zone + [trash] [lock]

Intf-INET-Zone [eye]

Destination Address + New Address + New Address Group + [trash] [lock]

Destination Address Not Configured

Destination Site Name + [trash] [lock]

Destination Site Name Not Configured

Destination Address Negate Destination Address Anycast

Add Rule [Close]

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

Application List + New Application + New Filter + New Group + [trash] [lock]

BITTORRENT

BITTORRENT_APPLICATION

BITTORRENT_BUNDLE

URL Reputations + [trash] [lock]

Predefined Reputations Not Configured

URL Category List + New URL Category + [trash] [lock]

URL Category List Not Configured

OK **Cancel**

Add Rule [Close]

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 [Close]

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

Actions | Log

Events Start End Both Never

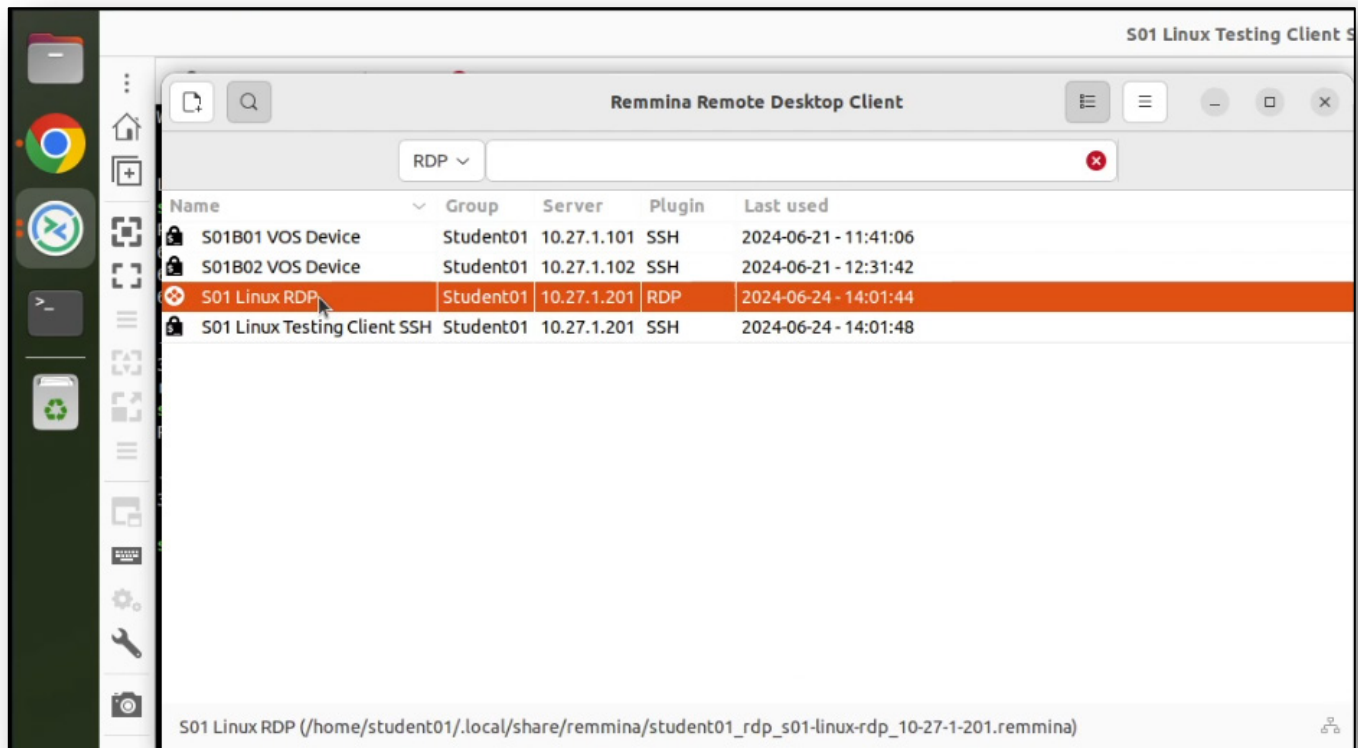
Profile

--Select-- [dropdown] Default Profile

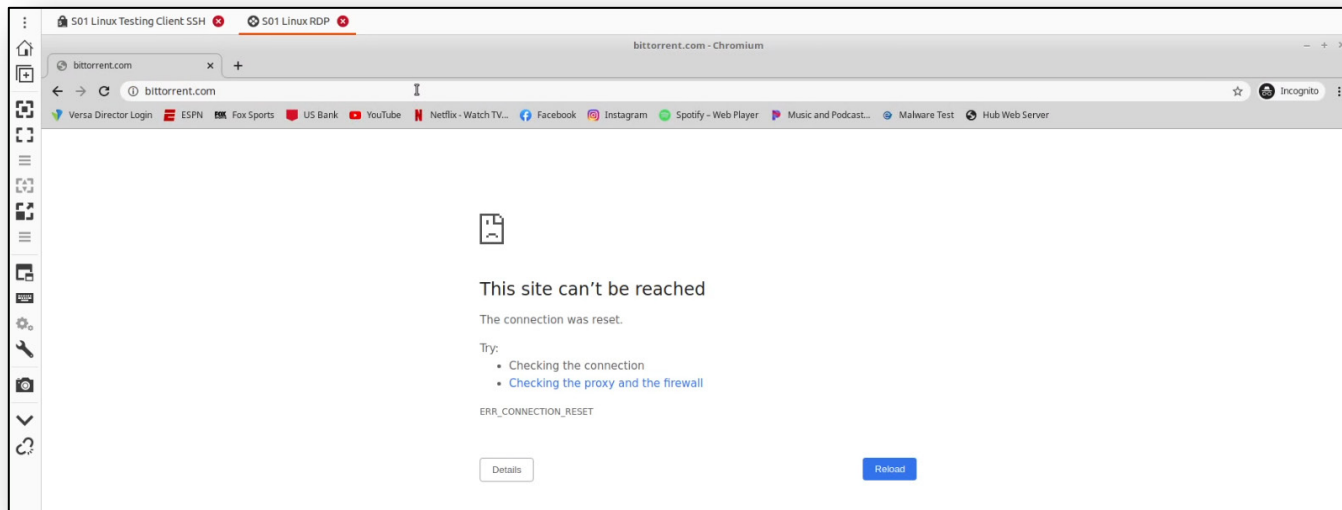
Step 6. Verify the Block-Bit-Torrent rule

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://bittorrent.com> web site.

- 6.a. On the remote landing station, open the Remmina application.
- 6.b. In the Remmina application, open an RDP session to the Linux testing client. The username is *student* and the password is *versa123* if prompted.

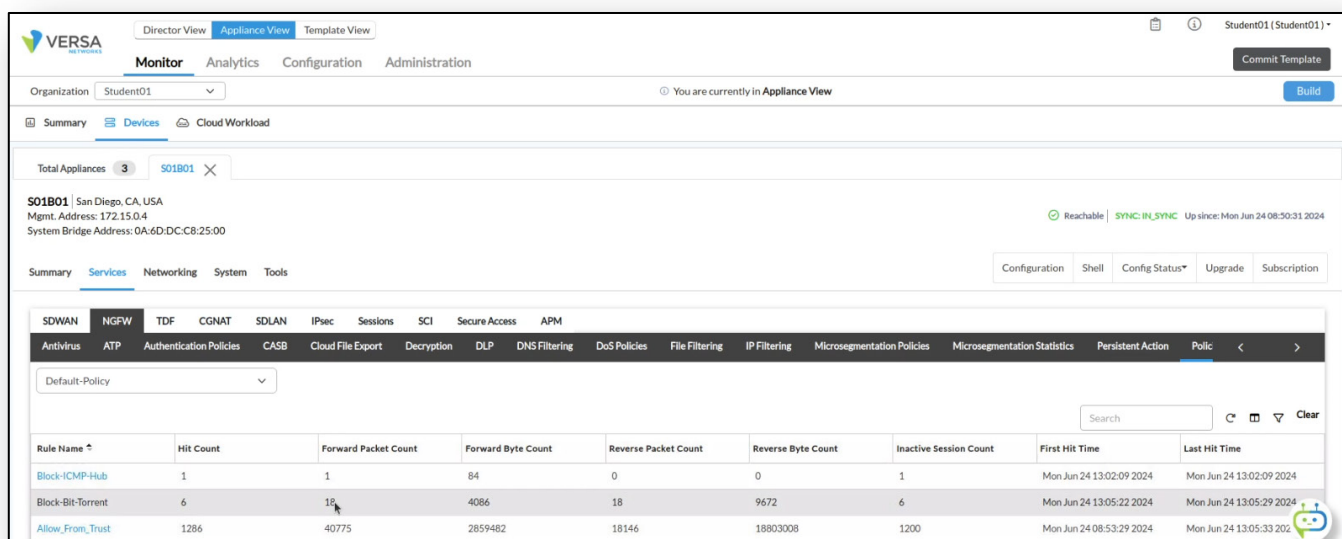


- 6.c. From the desktop of the testing host, open the *Chromium* web browser.
- 6.d. Click on the three dots in the top right corner of the browser and open an *Incognito* window (this will help prevent browser caching of sessions).
- 6.e. In the address bar of the web browser, enter the URL <https://bittorrent.com>. The page should not open.
- 6.f. Click the *Refresh* button on the browser a couple of times to try to connect.



Step 7. Analyze the statistics and logs for the Block-Bit-Torrent access rule in Versa Director

- 7.a. Return to versa Director.
- 7.b. In Versa Director, open the appliance *Monitor* tab to view your appliance statistics (*Appliance View* of your B01 device).
- 7.c. In the *Monitor* tab for your appliance, navigate to the *Monitor > Services > NGFW > Policies* dashboard.
- 7.d. Examine the hit count on the *Block-Bit-Torrent* access rule. The rule hit count should be a non-zero number.



Step 8. 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.

- 8.a. In Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Policies*.
- 8.b. In the *Rules* tab, click the + button to create a new access rule with the following parameters:

Block Streaming Video Rule	
General Tab:	Name: Block-Streaming-Video
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Intf-INET-Zone
Applications/URL Tab:	Click the + New Group link
Add Application Group Properties:	Name: App-Group-Youtube-Netflix Applications (click the + button): <ul style="list-style-type: none"> • YOUTUBE • NETFLIX
Enforce Tab:	Action: Reject Log Events: Both, check the Default Profile box

Add Rule

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

Application List + New Application + New Filter + New Group +
Application List Not Configured

URL Reputations +
Predefined Reputations Not Configured

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

OK Cancel

Add Application Group

Name

Description Tags

Applications +
 YOUTUBE
 NETFLIX

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 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 Default Profile

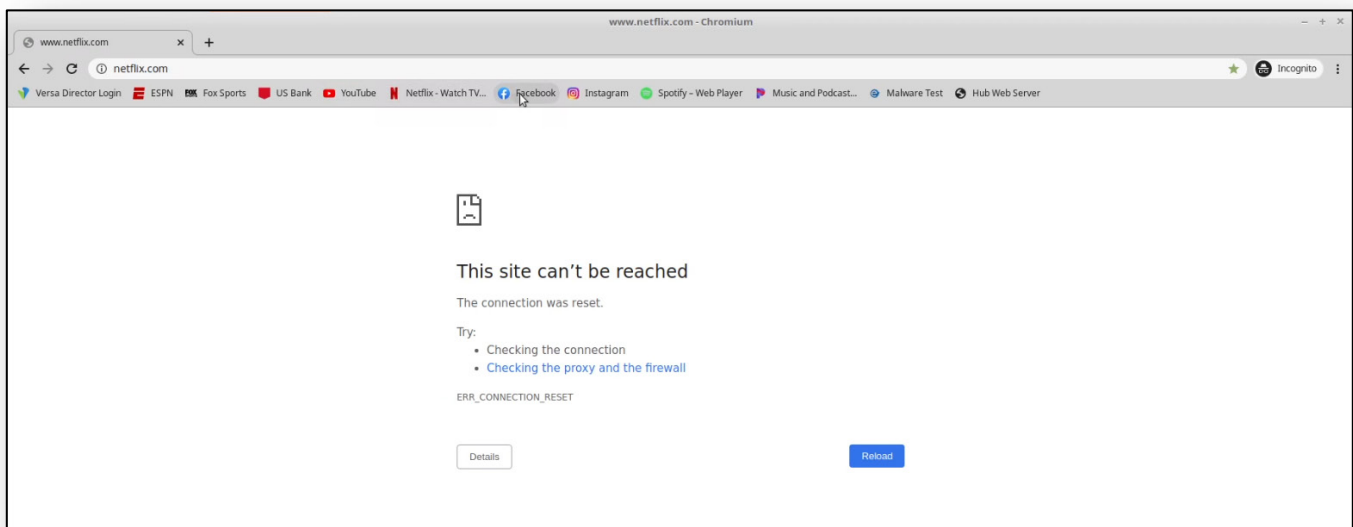
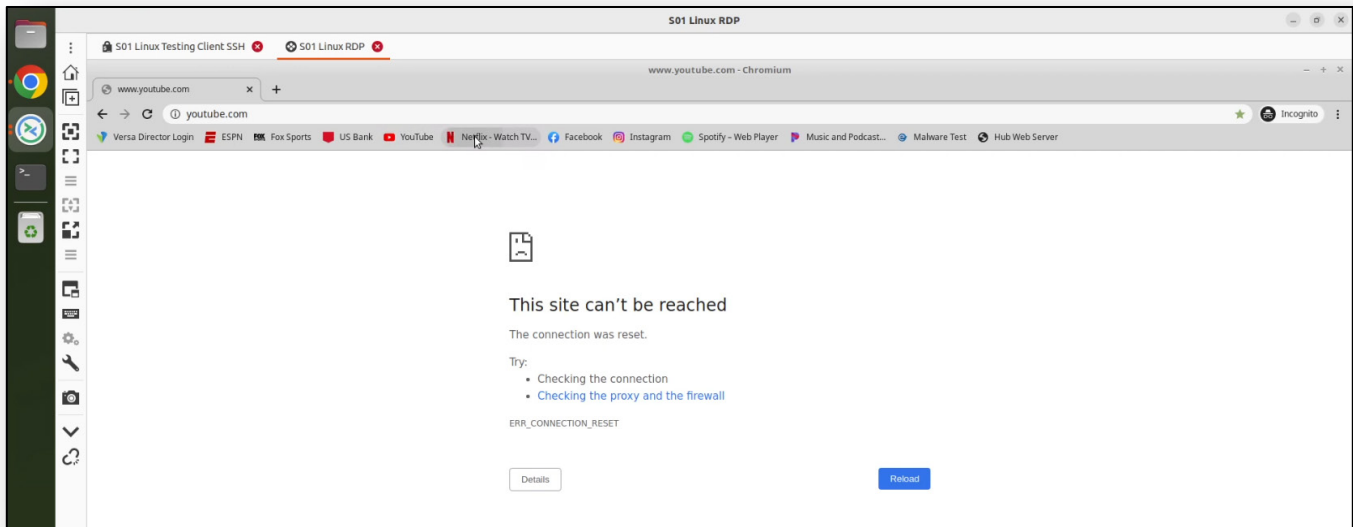
Rule Num	Name	Rule Disabled	Alias Name	Source							
				Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device	
<input type="checkbox"/> 1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone							
<input type="checkbox"/> 2	Block-Bit-Torrent	False		Intf-Student_LAN-Zone							
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

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

Step 9. Verify the Block Streaming Video rule

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

- 9.a. Return to the remote desktop session to the testing host.
- 9.b. From the testing host, open the Chromium web browser.
- 9.c. From the Chromium web browser on the testing host, enter the URL *https://youtube.com* in the address bar.
- 9.d. Click on some of the videos in the main window to attempt to watch the videos. The videos should not play.
- 9.e. Enter the URL *https://netflix.com* in the address bar of the browser. The web site should not open.



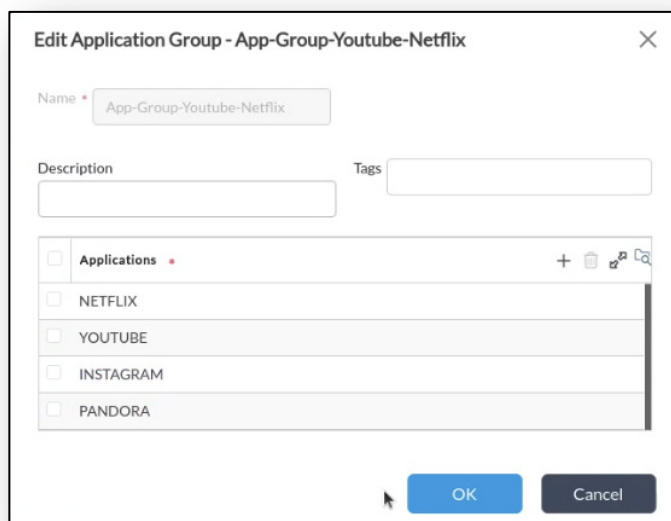
Step 10. Visit Social Media Sites

- 10.a. 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.

Step 11. Update the Application Group

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.

- 11.a. In your Appliance View B01 configuration, navigate to *Objects & Connectors > Objects > Custom Objects > Application Groups*.
- 11.b. Open the application group you created through your policy.
- 11.c. Add the following applications to the application group: Instagram; Pandora



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

Step 12. 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.

- 12.a. Return to Versa Director on the landing workstation.
- 12.b. Navigate to *Appliance View* of your B01 device.
- 12.c. In Appliance View of your B01 device, navigate to *Monitor > Services > NGFW > Policies*.
- 12.d. Examine the statistics for the *Block-App-Group-Youtube-Netflix* access rule. The hit count and reject count should be non-zero values.

The screenshot shows the Versa Director interface in Appliance View for device S01B01. The 'Monitor' tab is active, and the 'Policies' sub-tab is selected under the 'NGFW' service. A table displays the statistics for various access rules. The 'Block-App-Group-Youtube-Netflix' rule is highlighted, showing a hit count of 1 and a reject count of 1.

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	-	-

Step 13. 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.

- 13.a. In Versa Director, navigate to the *Appliance View* of your B01 device to modify the configuration directly.
- 13.b. In the *Appliance View* of your device, navigate to *Configuration > Objects & Connectors > Objects > Custom Objects > Applications*
- 13.c. 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 Application
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:	120 secs

Add Custom Application ✕

Name *

Description *

Precedence * Application Timeout (seconds)

Application match based on IPS signature ○

Attributes | Match Information

Family	Sub Family	Risk	Productivity	Application Tags		
				Security	SDWAN	General
<input type="radio"/> Business-system	<input type="radio"/> Antivirus	<input type="radio"/> 1	<input type="radio"/> 1	<input type="checkbox"/> Anonymizer	<input type="checkbox"/> Audio_stream	<input type="checkbox"/> AAA
<input checked="" type="radio"/> Collaboration	<input type="radio"/> Application-service	<input type="radio"/> 2	<input type="radio"/> 2	<input type="checkbox"/> Bandwidth	<input type="checkbox"/> AV	<input type="checkbox"/> Adult_content
<input type="radio"/> General-internet	<input type="radio"/> Audio_video	<input checked="" type="radio"/> 3	<input checked="" type="radio"/> 3	<input type="checkbox"/> Dataleak	<input type="checkbox"/> Business	<input type="checkbox"/> Advertising
<input type="radio"/> Media	<input type="radio"/> Authentication	<input type="radio"/> 4	<input type="radio"/> 4	<input type="checkbox"/> Evasive	<input type="checkbox"/> Cloud	<input type="checkbox"/> Analytics
<input type="radio"/> Networking	<input type="radio"/> Behavioral	<input type="radio"/> 5	<input type="radio"/> 5	<input type="checkbox"/> Filetransfer	<input type="checkbox"/> Data	<input type="checkbox"/> Anonymizer
	<input type="radio"/> Compression					
	<input type="radio"/> Database					
	<input type="radio"/> Encrypted					
	<input type="radio"/> Encrypted-tunnel					

Add Custom Application

Name *

Description *

Precedence * Application Timeout (seconds)

Application match based on IPS signature

Attributes | [Match Information](#)

Name	Host Pattern	Source Address	Destination Address	Source Port			Destination Port
				Source Port Value	Low	High	
<input type="checkbox"/> Custom-Gmail	*.twitter.*						

Add Match Information

Name *

Host Pattern 11/63 Protocol Value

Source Address Destination Address

Source Port

Value Range

Source Port Value Low High

Destination Port

Value Range

Destination Port Value Low High

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

13.d. In Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Policies*.

13.e. In the *Rules* tab, click the + button to create a new access rule with the following parameters:

Custom Application Security Rule	
Name:	Block-Custom-Twitter
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Intf-INET-Zone
Applications/URL:	Application: Custom-Twitter-APP
Enforce:	Action: Reject Log Events: Both, check the Default Profile box

Add Rule

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

Name: Block-Custom-Twitter 20/63

Description

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

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

Add Rule

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

Application List: Custom-Twitter-APP

URL Category List: URL Category List Not Configured

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

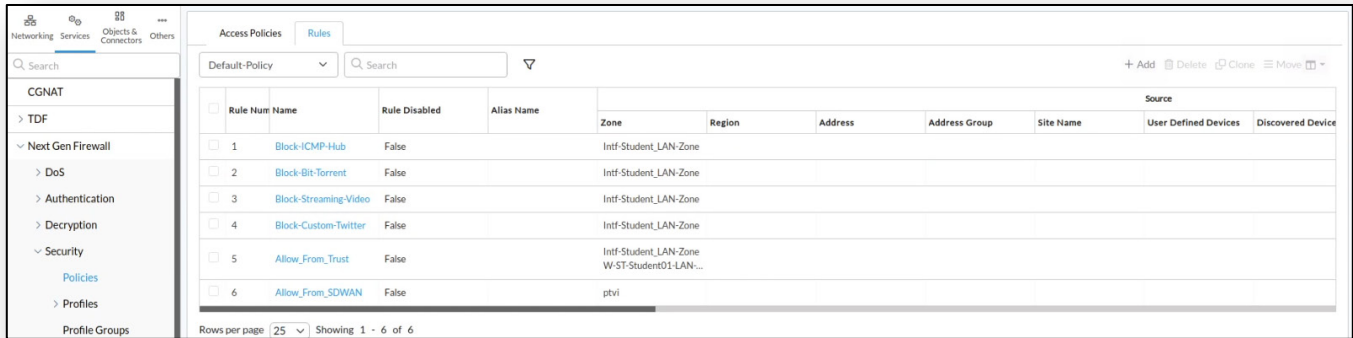
Add Rule

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

Actions | Log

Events: Start End Both Never

Profile: --Select-- Default Profile

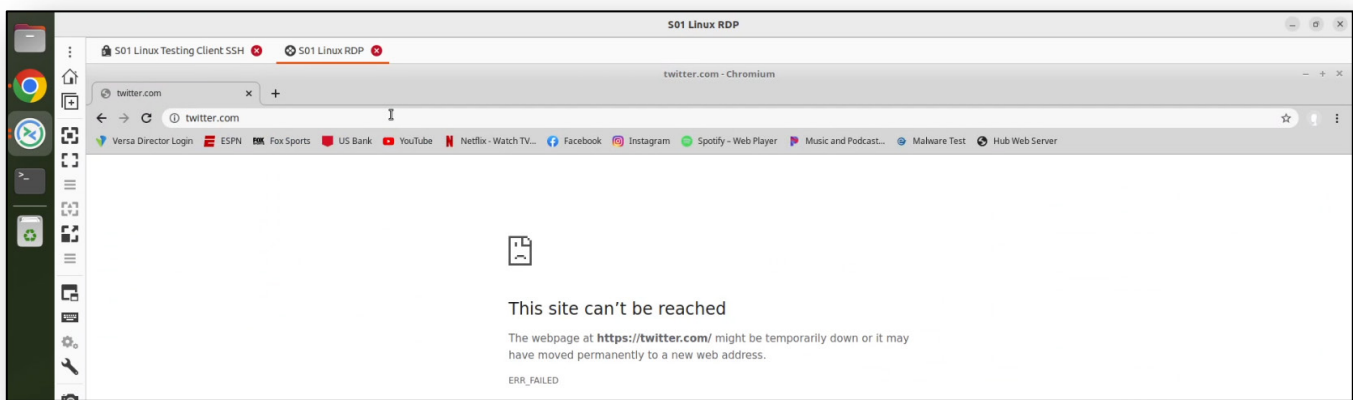


Rule Num	Name	Rule Disabled	Alias Name	Source	Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device
1	Block-ICMP-Hub	False		Intf-Student_LAN-Zone							
2	Block-Bit-Torrent	False		Intf-Student_LAN-Zone							
3	Block-Streaming-Video	False		Intf-Student_LAN-Zone							
4	Block-Custom-Twitter	False		Intf-Student_LAN-Zone							
5	Allow_From_Trust	False		Intf-Student_LAN-Zone W-ST-Student01-LAN...							
6	Allow_From_SDWAN	False		ptv1							

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

13.f. In the remote landing station, return to the remote desktop session to the testing host.

13.g. 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.



13.h. Return to Versa Director.

13.i. Open the Appliance View for your B01 device.

13.j. From Appliance View of your B01 device, *Monitor > Services > NGFW > Policies*.

13.k. Examine the counters for the *Block-Custom-Twitter* access rule. The hit count and deny count should be non-zero values.

13.l. Click the Director View at the top of the dashboard. From the main Versa Director dashboard, navigate to *Analytics > Logs > Firewall*.

13.m. In the firewall log window, click the Search box and enter a filter for the rule name *Block-Custom-Twitter*. Only log entries associated with the Block-Custom-Twitter access rule should be displayed.

- 13.n. 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.



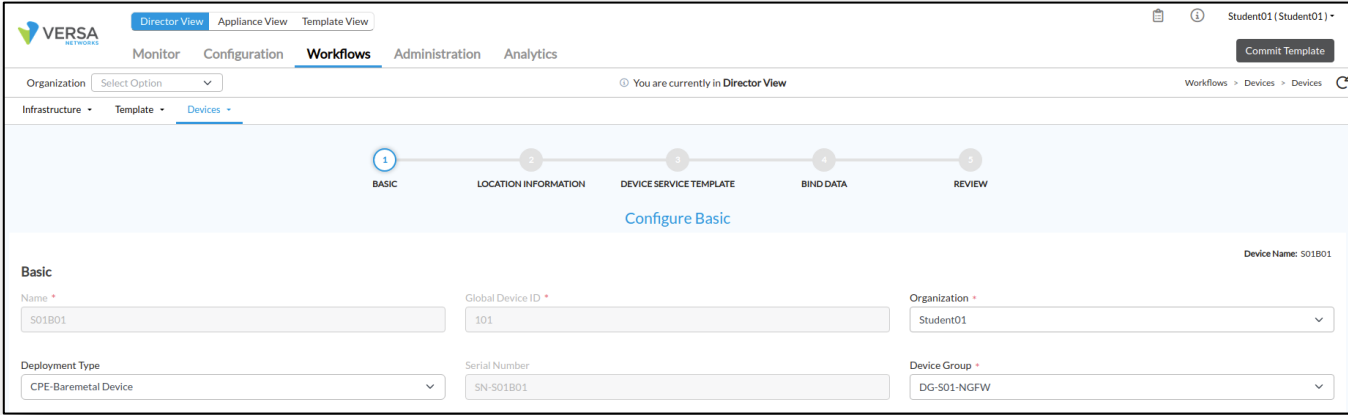
STOP! Notify your instructor that you have completed this lab.

URL FILTERING

In this lab you will configure the URL filtering security rules to filter web based traffic.

Step 1. Verify that your device is in the base device group

- 1.a. Open a connection to the lab environment remote desktop using the instructions provided by our instructor.
- 1.b. In the remote desktop, open the Google Chrome browser.
- 1.c. In the Google Chrome browser on the remote desktop, use the bookmark to open a connection to Versa Director (or navigate to 10.27.1.10).
- 1.d. Log into Versa Director with your student ID (Student01, Student02, etc.) and the password *Versa@123*.
- 1.e. In Versa Director, open the *Workflows > Devices > Devices* dashboard.
- 1.f. Click on your SxxB01 device workflow.
- 1.g. In your B01 device workflow, ensure that the device group *DG-Sxx-NGFW* is selected, where *Sxx* is your student ID, then click *Re-deploy*.



The screenshot shows the Versa Director interface for configuring a device. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The main menu has 'Monitor', 'Configuration', 'Workflows', 'Administration', and 'Analytics'. The breadcrumb trail is 'Workflows > Devices > Devices'. A progress bar at the top indicates five steps: 1. BASIC (highlighted), 2. LOCATION INFORMATION, 3. DEVICE SERVICE TEMPLATE, 4. BIND DATA, and 5. REVIEW. Below the progress bar, the 'Basic' configuration section is visible. It includes the following fields:

- Name: S01B01
- Global Device ID: 101
- Organization: Student01
- Deployment Type: CPE-Baremetal Device
- Serial Number: SN-S01B01
- Device Group: DG-S01-NGFW

A 'Commit Template' button is located in the top right corner of the page.

- 1.h. Click the *Commit Template* button.
- 1.i. 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.
- 1.j. Select your devices in the device list and click *Review*.
- 1.k. In the *Review* window click *Commit* to apply the base configuration to your device.

Director View | Appliance View | Template View

Monitor | Configuration | Workflows | **Administration** | Analytics

Student01 (Student01) | Commit Template

Commit Template To Select Devices

All the Associated Templates
 Only Selected Templates

Organization: Student01
 Auto Merge
 Overwrite

Select Devices By: Template

 Reboot after commit

Fetch Devices

Select Devices (1)

Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
<input type="checkbox"/> S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

Cancel | Review

Step 2. 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.

- 2.a. From the Versa Director main dashboard, navigate to the *Appliance View* and locate your B01 appliance in the table.
- 2.b. Click your appliance name to open the appliance context mode for the appliance.
- 2.c. 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.
- 2.d. Click the + button to create a new NAT pool with the following parameters:

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


- 2.e. Click OK when finished.
- 2.f. To create the cloud lookup profile, navigate to *Objects & Connectors > Objects > Cloud Profiles*.
- 2.g. 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:	Urf-cloud-profile
Activation:	Check the Activate checkbox

- 2.h. Click *OK* to finish creating the cloud profile.

Step 3. 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.

- 3.a. In the *Appliance View* of your B01 device, open the *Configuration* window.
- 3.b. In the *Configuration* window, navigate to *Services > Next Gen Firewall > Security Settings > URL-Filtering* and click the *Edit* button  to modify the settings.
- 3.c. 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:	Click the Enable Cloud Lookup box

- 3.d. Click OK when finished.
- 3.e. Click *OK* to save the settings. Cloud Lookup for URL categories has been enabled on the appliance.

Step 4. 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.

- 4.a. In the *Appliance View* of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > URL Filtering*.
- 4.b. 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:	Select the Default-Logging-Profile
Category Based Action:	Click the + button and enter the following in the pop-up window: Name: BLOCK-CATEGORIES Action: Block Predefined Categories: Click the + button and add the following categories: <ul style="list-style-type: none"> • malware_sites • sports • news_and_media • social network

- 4.c. 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 5. Create URL Filtering Access Rules

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.

- 5.a. In the *Configuration* tab of your B01 branch device, navigate to the *Services > Next Gen Firewall > Security > Policies* hierarchy.
- 5.b. Open the *Rules* tab to add new rules to the default security policy.
- 5.c. In the *Rules* tab, click the + button to add the following rule to the policy:

Access Rule Parameters	
Name:	URL-IP-Filtering-Rule
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Intf-INET-Zone
Headers/Schedule Tab:	Add the following Services: <ul style="list-style-type: none"> • domain • http • https
Enforce	Action: <ul style="list-style-type: none"> • Apply Security Profile <ul style="list-style-type: none"> • Select Profiles > URL Filtering > URLF-Profile • Logging: Both, check the Default Profile box

- 5.d. Click OK to finish configuring the rule.
- 5.e. Click and drag the rule to the top of the rule list so that it is evaluated first.

Step 6. 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.

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

- 6.c. On the testing host desktop, open the Chromium Web Browser application.
- 6.d. 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.
- 6.e. Browse to *https://espn.com*
The site should be blocked.
- 6.f. Browse to *https://instagram.com*
The site should be blocked.
- 6.g. Browse to *https://spotify.com*
The site should be allowed.

Step 7. 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.

- 7.a. Return to the *Configuration* dashboard of your B01 device.
- 7.b. From the *Configuration* dashboard of your B01 device, navigate to *Services > Next Gen Firewall > Security > Profiles > URL Filtering* to view the URL filtering profile table.
- 7.c. Select the *URLF-Profile* profile to modify the profile.
- 7.d. 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.
- 7.e. Click the OK buttons until you finish updating the URL filter profile.

Step 8. Test your changes to the URL Filter profile

- 8.a. Return to the remote desktop connection to the testing host.
- 8.b. If the Chromium web browser is open, close the browser and then re-open the Chromium web browser.
- 8.c. 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 9. Step 2.8: Verify the URL filtering using Versa Director and Versa Analytics

- 9.a. Return to Versa Director.
- 9.b. From Versa Director, navigate to the *Appliance View* for your B01 branch appliance.
- 9.c. From the *Appliance View* of your B01 device, navigate to *Monitor > Services > NGFW > URL Filtering*.
- 9.d. 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. The rule count should be non-zero.

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.

- 9.e. Click *Director View* to return to the main Versa Director dashboard.
- 9.f. From the main Versa Director dashboard, then click the *Analytics* tab to open the Analytics dashboard.
- 9.g. From the main *Analytics* dashboard, navigate to *Dashboards > Security > Web*.
- 9.h. Select the *URL Categories* tab. You should see URL category information.
- 9.i. Navigate to the *Logs > Threat Filtering* dashboard to view the Threat Filtering logs.
- 9.j. Select the *URL Filtering* tab from the *Threat Filtering* window.
- 9.k. 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, 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.)

- 9.l. To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.
- 9.m. Log out of Versa Director.



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

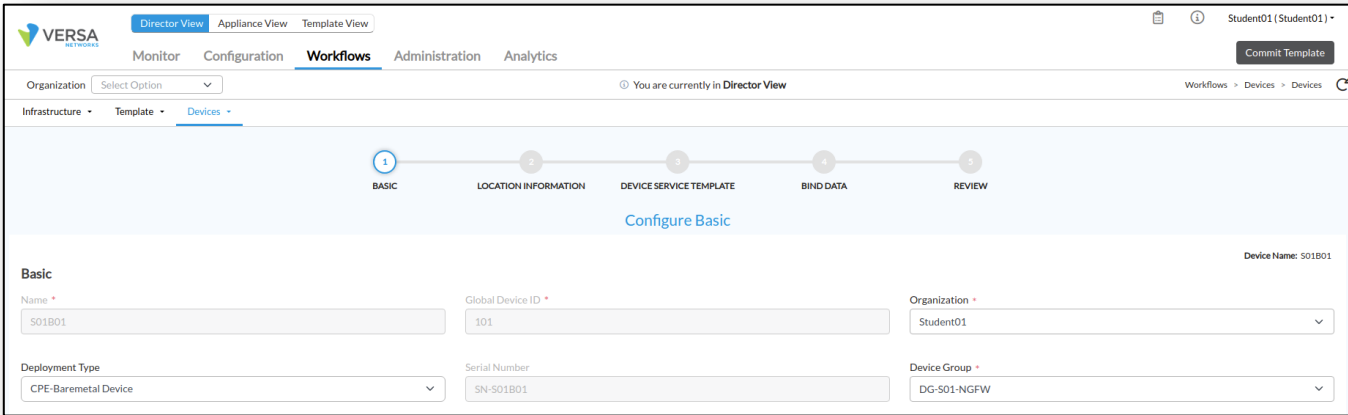
IP FILTERING

In this lab you will use the IP Filtering capability in VOS to create and monitor security access policies.

Step 1. Step 1.1: Verify that your device is in the base device group

You will start by ensuring that your device has a default configuration.

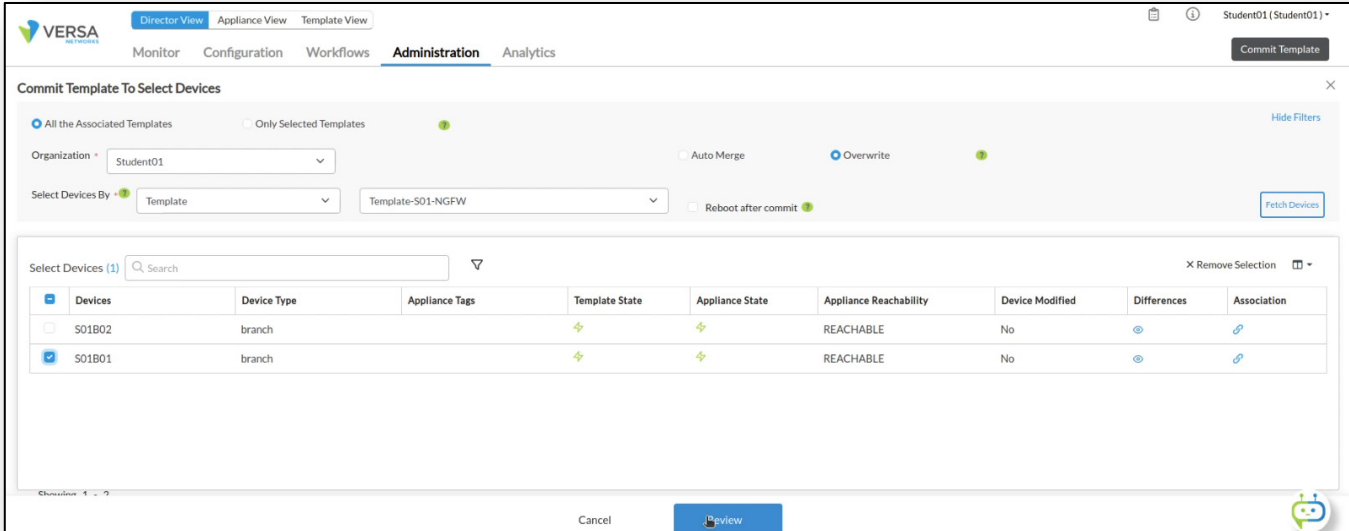
- 1.a. Connect to the lab remote desktop by following the instructions provided by your instructor.
- 1.b. In the remote desktop, open the Google Chrome browser.
- 1.c. In the Google Chrome browser on the remote desktop, open Versa Director by clicking on the Versa Director bookmark (or navigate to IP address 10.27.1.10).
- 1.d. In Versa Director, open the *Workflows > Devices > Devices* dashboard
- 1.e. Click on your *SxxB01* device workflow, where *Sxx* is your student number.
- 1.f. In your B01 device workflow, ensure that the device group *DG-Sxx-NGFW* is selected
- 1.g. Click *Re-deploy*.



The screenshot shows the 'Configure Basic' page in the Versa Director interface. The breadcrumb navigation is 'Workflows > Devices > Devices'. The page title is 'Configure Basic' and the device name is 'S01B01'. The configuration fields are as follows:

Field	Value
Name *	S01B01
Global Device ID *	101
Organization *	Student01
Deployment Type	CPE-Baremetal Device
Serial Number	SN-S01B01
Device Group *	DG-S01-NGFW

- 1.h. Click the *Commit Template* button.
- 1.i. In the *Commit* dialog box, select your student ID as the organization, select the template *Template-Sxx-NGFW*, and click *Fetch Devices* to display your devices.
- 1.j. Select your B01 (and B02 if shown) in the device list and click *Review*.
- 1.k. 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

Fetch Devices

Select Devices (1) Remove Selection

Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
<input type="checkbox"/> S01B02	branch		⚡	⚡	REACHABLE	No	👁	🔗
<input checked="" type="checkbox"/> S01B01	branch		⚡	⚡	REACHABLE	No	👁	🔗

Cancel Review

Step 2. Check the IP Filtering profiles in the pre-defined database on the branch device

In the next 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.

- 2.a. From the Versa Director user interface, click the *Appliance View* tab.
- 2.b. Locate and click on your B01 appliance in the appliance list to open the appliance context mode. You will perform the configuration tasks in this lab directly on your appliance.
- 2.c. Navigate to *Configuration > Objects & Connectors > Objects > Predefined > 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 in the table.

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.

- 2.d. Navigate to the *Configuration > 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
Match Type:	Match source or destination

- 2.e. Click OK to finish creating the profile.

Step 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.

- 3.a. In the *Configuration* dashboard of your B01 device, navigate to the *Services > Next Gen Firewall > Security > Policies* hierarchy.
- 3.b. Open the *Rules* tab.
- 3.c. Click the + button to add a new access rule with the following parameters:

Access Rule Parameters	
Name:	IP-Filtering-Rule
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Intf-INET-Zone
Headers/Schedule Tab:	Add the following services: <ul style="list-style-type: none"> • domain • http • https • ICMP
Enforce Tab:	Action: Apply Security Profile Check the IP Filtering box and select the IP-Filtering-Profile from the drop-down Logging: Both; select Default Profile

- 3.d. Click *OK* to create the rule.
- 3.e. Drag and drop the rule to the top of the rule list.

Step 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 on the emulated public network, you will have to modify the NAT translation rule so that the 10.27.0.0/16 prefixes will match the DIA NAT rule.

- 4.a. Navigate to the *Services > CGNAT* hierarchy of your appliance configuration.
- 4.b. Select the *Rules* tab from the CGNAT table.
- 4.c. Locate the *RFC_1918_NoTranslate* NAT rule in the table and click on the rule to open and modify the rule.
- 4.d. In the *RFC_1918_NoTranslate* rule, select the *Match* tab.
- 4.e. In the *Match* tab, select and delete the *10.0.0.0/8* address from the *Source IP Address* and *Destination IP Address* fields.
- 4.f. Click OK to finish modifying the rule.

Step 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.

- 5.a. In the remote desktop, click on the *Remmina* icon on the left application bar to the Remmina.
- 5.b. 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*.
- 5.c. On the testing host, use the *Terminal* icon on the desktop to open a terminal window.
- 5.d. The scripts for this lab are located in the *./VASEC/* directory. Type `cd ./VASEC/` to move to that directory.
- 5.e. 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 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.

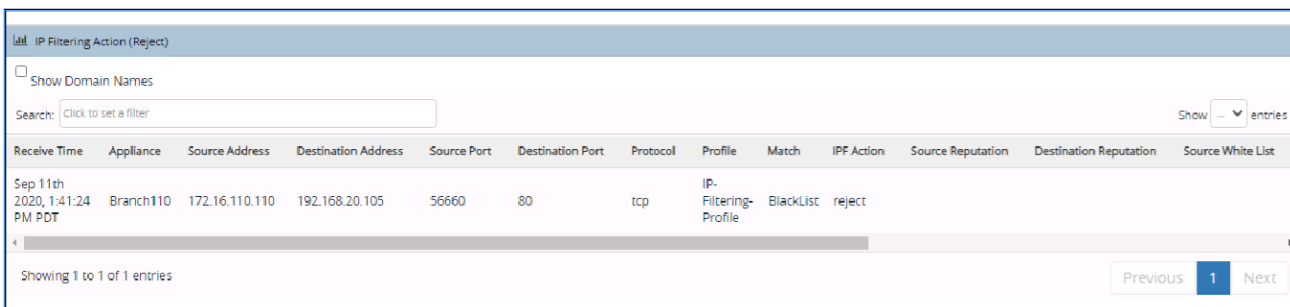
- 6.a. Return to the *Versa Director* dashboard on the remote landing station.
- 6.b. From the *Appliance View* of your B01 device, navigate to *Monitor > Services > NGFW*.
- 6.c. Select the *Policies* tab.
- 6.d. In the *Policies* tab, ensure that the *Default-Policy* is selected and examine the IP-Filtering-Rule counters. You should see packets in the Hit Count field. This indicates that the policy has matched and processed traffic.
- 6.e. 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 7. Verify the IP Filter profile in Versa Analytics

- 7.a. Click the *Director View* button to exit device context and return to the main Versa Director dashboard.
- 7.b. From the main *Versa Director* dashboard, navigate to *Analytics*.
- 7.c. In the *Versa Analytics* dashboard, navigate to *Dashboards > Security > Threats*
- 7.d. Select the *IP* tab. You should see a reject field in the Top IP Filtering Action chart.
- 7.e. 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.



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			

- 7.f. Navigate to *Logs > Threat Filtering* and open the *IP Filtering* tab. You should see the IP Filtering log entry.
- 7.g. Click the magnifying glass icon next to a log entry 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 8. Add Geo-location to the IP Filtering profile

- 8.a. 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.
- 8.b. Click on the Appliance View button, then select your B01 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:

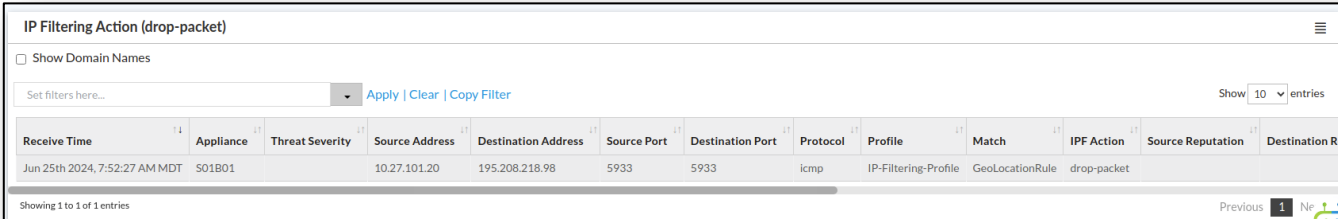
IP-Filtering-Profile Geo IP Based Actions	
Name:	Drop-Region
Action:	Drop Packet
Match Type:	Match source or destination
Regions:	Click the + button and add Russia

- 8.c. Click OK to apply the changes.

Step 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.

- 9.a. On the landing station, return to the remote desktop session to the testing host.
- 9.b. If a shell prompt is not already open, open a new shell prompt using the Terminal icon on the desktop.
- 9.c. 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.
- 9.d. Return to *Versa Director*.
- 9.e. In *Versa Director*, open the Appliance View for your B01 appliance.
- 9.f. From your B01 Appliance View, navigate to *Monitor > Services > NGFW > IP Filtering*.
- 9.g. 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.
- 9.h. Click the *Director View* button to return to the main Versa Director dashboard.
- 9.i. From the *Versa Director* dashboard, navigate to *Analytics > Dashboards > Security > Threats*.
- 9.j. Select the *IP* tab to display the IP threat dashboard. You should see drop-packet in the Top IP Filtering Action panel.
- 9.k. Click the *drop-packet* graphic to open the details about the top action.
- 9.l. In the Events (*Drop-Packet*) dashboard, you should see hits. Scroll down in the dashboard until you see the action details.



Receive Time	Appliance	Threat Severity	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action	Source Reputation	Destination Reputation
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		

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 10. 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.

10.a. In Versa Director, navigate to the Appliance View of your B01 device.

10.b. Navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > IP Filtering*.

10.c. 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.

10.d. Add the following Reputation Based Actions to the profile:

IP-Filtering-Profile Reputation Based Actions	
Name:	Bad-IPs
Default Action:	Drop Packet
Match Type:	Match source or destination
URL Reputations:	Click the + button and add the following: <ul style="list-style-type: none"> • Web Attacks • Phishing • Spam Sources • Windows Exploits • BotNets • Denial of Services • Scanners

10.e. Click *OK* to finish updating the profile.

Step 11. Test the IP Reputation profile

11.a. From the remote desktop, use the Remmina application to open a remote desktop session to the Linux testing host.

11.b. On the Linux testing host, open a terminal window.

11.c. 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.

11.d. Return to the *Versa Director* dashboard.

11.e. In the *Versa Director* dashboard, navigate to your appliance context mode.

11.f. From your appliance context mode, navigate to *Monitor > Services > NGFW* and select the *IP Filtering* tab.

11.g. 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.

- 11.h. Click the *Director View* button to exit appliance context mode and return to the main Versa Director dashboard.
- 11.i. From the *Versa Director* dashboard, navigate to the *Analytics > Dashboards > Security > Threats* dashboard.
- 11.j. Select the *IP* tab from the dashboard to view IP filtering statistics.
- 11.k. Mouse over the *Top IP Filtering Action > drop-packet* chart. The pop-up will display how many rule hits have been counted.
- 11.l. Click on the drop-packet chart to open the drop-packet details.
- 11.m. Scroll down to the action entries. The most recent entries should indicate a match on ReputationRule for your branch device.

Step 12. Finish the lab and exit the lab environment

- 12.a. To finish the lab, close the browser window on the testing host, then close the remote desktop session to the testing host.
- 12.b. Log out of Versa Director.



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

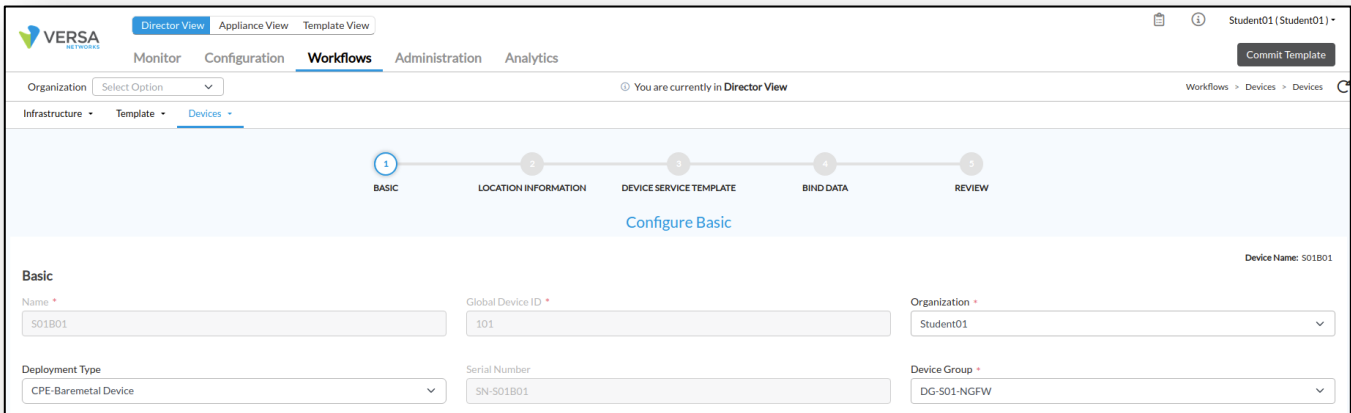
ANTIVIRUS AND IDP

In this lab exercise you will configure antivirus profiles and settings, and configure and apply Intrusion Detection and Prevention profiles.

Step 1. Set device to a default configuration

In this step you will ensure that your B01 device is in the DG-Sxx-NGFW device group and that the NGFW template is configured for your device. This will allow you to configure the Next Generation Firewall features in the lab.

- 1.a. Connect to the lab remote desktop by following the instructions provided by your instructor.
- 1.b. In the remote desktop, click on the Google Chrome icon to open Google Chrome.
- 1.c. In the Google Chrome browser on the remote desktop, click on the Versa Director bookmark to open a connection to Versa Director. The login is your student ID (*Student01*, *Student02*, etc.) and the password is *Versa@123*. Alternatively you can enter the IP address of Versa Director in the browser (10.27.1.10).
- 1.d. In Versa Director, open the *Workflows > Devices > Devices* dashboard.
- 1.e. In the Devices workflow dashboard, click on your *SxxB01* device workflow.
- 1.f. In your B01 device workflow, ensure that the device group *DG-Sxx-NGFW* is selected.
- 1.g. Click *Re-deploy*.

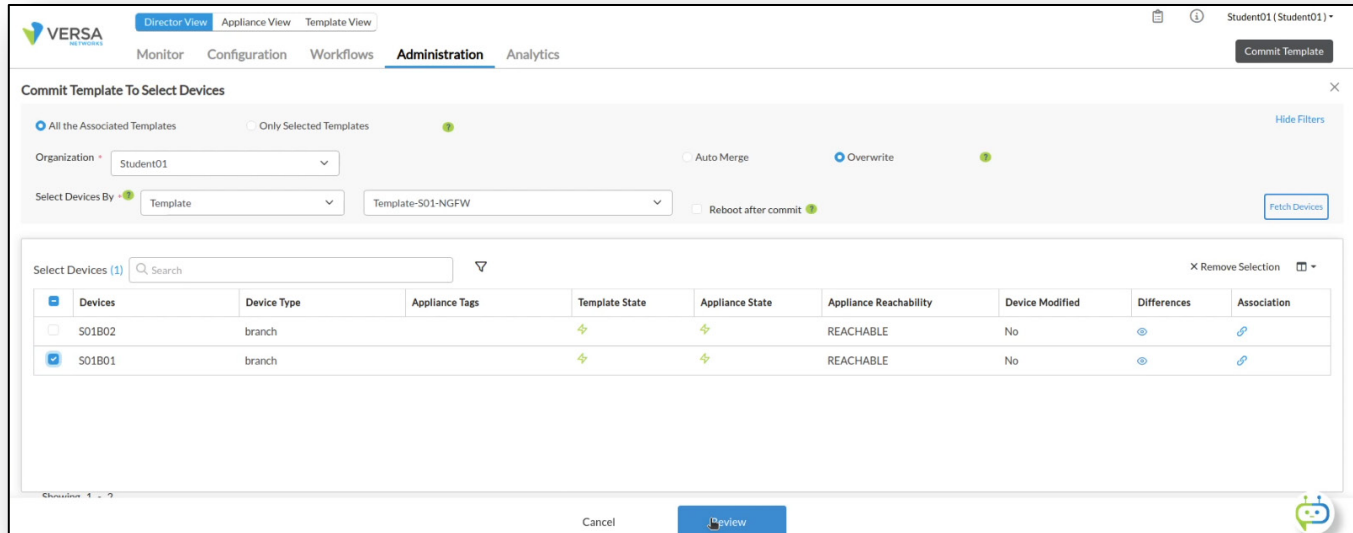


The screenshot shows the Versa Director interface for configuring a device workflow. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The main menu has 'Monitor', 'Configuration', 'Workflows', 'Administration', and 'Analytics'. The current view is 'Workflows > Devices > Devices'. A progress indicator shows five steps: 1. BASIC (selected), 2. LOCATION INFORMATION, 3. DEVICE SERVICE TEMPLATE, 4. BIND DATA, and 5. REVIEW. The 'Configure Basic' section contains the following fields:

Name *	Global Device ID *	Organization *
S01B01	101	Student01
Deployment Type	Serial Number	Device Group *
CPE-Baremetal Device	SN-S01B01	DG-S01-NGFW

Device Name: S01B01

- 1.h. Click the *Commit Template* button at the top right of the Director dashboard.
- 1.i. In the *Commit* dialog, select your student ID as the organization.
- 1.j. Select the *Template-Sxx-NGFW* as the template.
- 1.k. Click *Fetch Devices* to display the devices associated with the template. If your B01 device does not appear in the table, ensure that it is associated with the proper device group (steps 1.d through 1.g).
- 1.l. Click *Review*.
- 1.m. In the *Review* dialog, click *Commit* to apply the base configuration to your device(s).



Step 2. 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:

- 2.a. In Versa Director, click on *Appliance View* and select your *B01* appliance from the list.
- 2.b. From the *Appliance View* of your B01 device, navigate to *Configuration > Objects & Connectors > Objects > Custom Objects > Certificates*.
- 2.c. 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 3. Test HTTPS access to an Internet site

- 3.a. On the remote desktop, open the Remmina application.
- 3.b. In the Remmina applicaiton, open an RDP session to the Linux testing client. There should be a pre-configured session in Remmina. Enter the username *student* and password *versa123* if prompted.
- 3.c. On the Linux testing client, open a Chromium web browser window on the testing host.
- 3.d. 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 > Objects > 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.

Step 4. Create an SSL Decryption Profile to Proxy SSL Sessions

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

Proxy Profile Settings	
General Tab:	Name: ssl-proxy-profile Enable Profile Use Extended Master Secret Type: SSL Forward PROxy Trusted Certificate Database: default CA Certificate: ssl-cert
SSL Inspection Tab:	Server Certificate Checks: <ul style="list-style-type: none"> • Action for Expired Certificate: Allow • Action for Untrusted Issuers: Alert • Restrict Certificate Extension: Checked Unsupported Mode Checks: <ul style="list-style-type: none"> • Action for Unsupported Cipher: Alert • Min Supported Key Length: 512 • Action for Unsupported Key Length: Alert • Acction for Unsupported Version: Alert

Add Decryption Profile

General | **SSL Inspection** | SSL Protocol | Advanced

Name *

Description Tags

Enable Profile Support Session Ticket Use Extended Master Secret

Type * Trusted Certificate Database * CA Certificate *

LEF Profile

Default Profile

LEF Log Level

Add Decryption Profile

General | **SSL Inspection** | SSL Protocol | Advanced

OCSP

Enabled Block Unknown Certificate Response Timeout Verify

CRL Check Fetch issuer using AIA ⓘ

Server Certificate Checks

Action for Expired Certificate Action for Untrusted Issuers Restrict Certificate Extension

Unsupported Mode Checks

Action for Unsupported Cipher Min Supported Key Length

Action for Unsupported Key Length Action for Unsupported Version

Step 5. Create Decryption Rules

5.a. In your Appliance View Configuration dashboard, add the following Decryption Rule:

Decryption Rule Settings	
General Tab:	Name: Forward-Proxy
Source Tab:	Source Zone: Click + and add Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Click + and add Intf-INET-Zone
Enforce Tab:	Action: decrypt Decryption Profile: ssl-proxy-profile

Add Decryption Rule

[General](#)
[Source](#)
[Destination](#)
[Headers/Schedule](#)
[URL](#)
[Users/Groups](#)
[Enforce](#)



Name *

Description

Tags

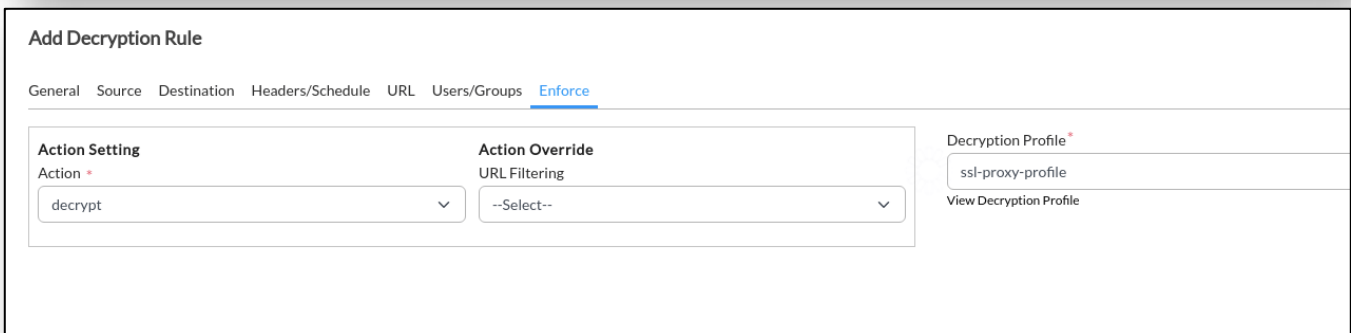
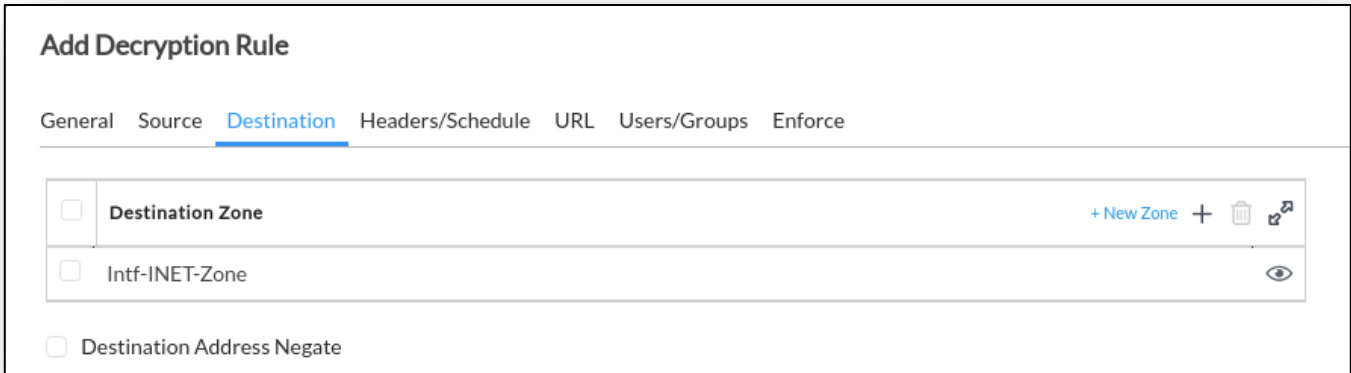
Add Decryption Rule

[General](#)
[Source](#)
[Destination](#)
[Headers/Schedule](#)
[URL](#)
[Users/Groups](#)
[Enforce](#)

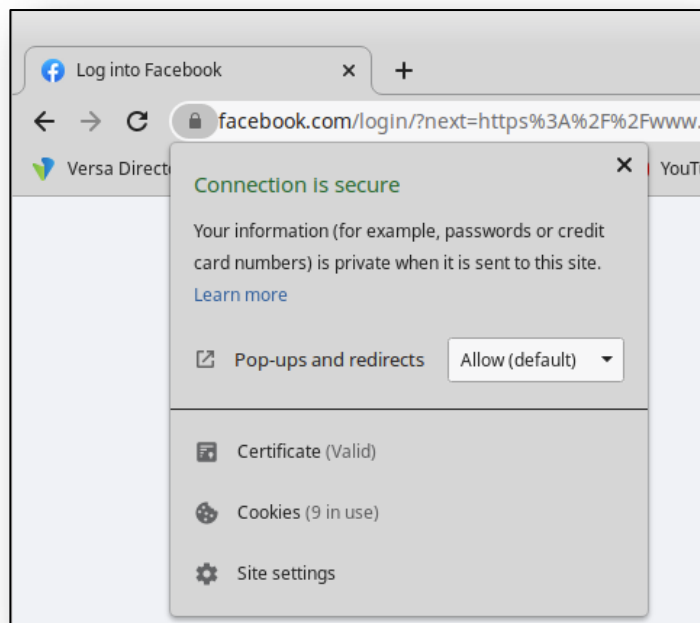
Source Zone + New Zone +  

Intf-Student_LAN-Zone 

Source Address Negate



- 5.b. Return to the remote desktop session to the Linux testing client (Remmina session).
- 5.c. If the Chromium browser is open in the Linux testing client, close the browser and re-open the browser to refresh the browsing sessions.
- 5.d. In the Chromium browser on the testing client, enter the url `https://facebook.com` in the address bar to open the Facebook home page.
- 5.e. 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:



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.

Step 6. 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.

- 6.a. Return to the Versa Director session on your remote desktop
- 6.b. Open the Appliance View of your B01 device.
- 6.c. In Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Antivirus*.
- 6.d. 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: <ul style="list-style-type: none"> • zip • gzip • txt • 7zip • tar
Protocol:	<ul style="list-style-type: none"> • http
Action on Disk Full:	<ul style="list-style-type: none"> • Deny

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

- 6.e. Click *OK* to create the profile.

Step 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.

- 7.a. In Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Policies*. The Rules tab should display the 2 auto-generated rules.
- 7.b. Click the + button to add a new rule to the policy. Create the rule with the following parameters:

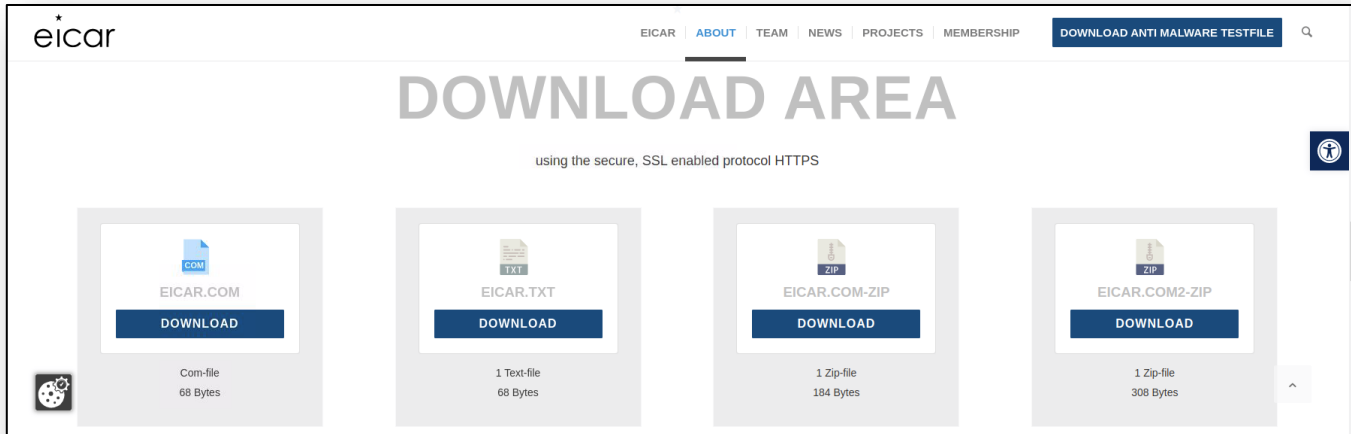
Antivirus Rule Setting	
Name:	UTM-RULE-AV
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: Intf-INET-Zone
Headers/Schedule Tab:	Add the following services: <ul style="list-style-type: none"> • http • https
Enforce Tab:	Action: Apply Security Profile <ul style="list-style-type: none"> • Profile: Antivirus • Logging: Both, select Default Profile

- 7.c. Click *OK* to create the rule. The rule will be placed after the auto-generated rules.
- 7.d. Drag and drop the rule to the top of the rule list so that it is processed first.

Step 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.

- 8.a. On the remote desktop, open the Remmina application and create a remote desktop session to the Linux Testing host (or use the existing session if one is already open). If prompted, the login to the Linux RDP session is username *student* and password *versa123*.
- 8.b. From the testing host desktop, open the Chromium web browser.
- 8.c. Click the *Malware Test* bookmark in the bookmark toolbar to open the testing site.
- 8.d. In the malware testing site, scroll down until you see the download area:



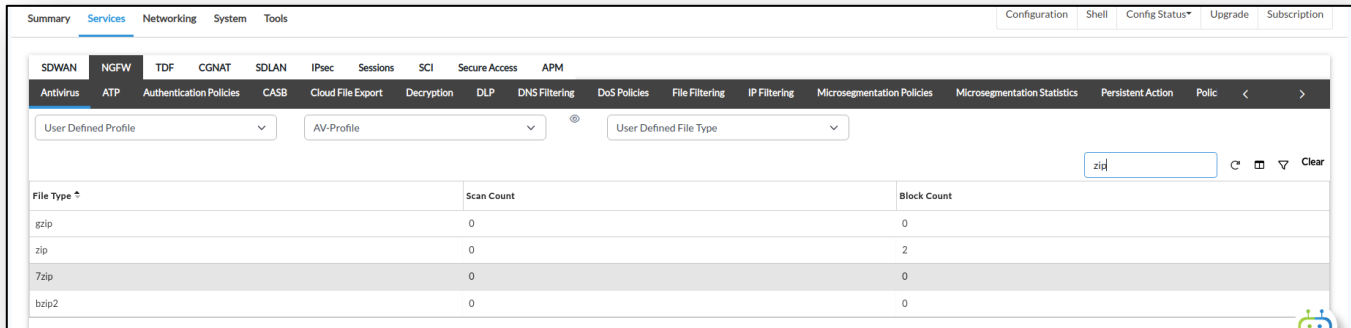
- 8.e. Click the eicar.txt file to attempt to download the file. Wait 5 to 10 seconds.
- 8.f. Click the eicar.com.zip file to attempt to download the file. Wait 5 to 10 seconds.
- 8.g. Click the eicar.com2-zip file to attempt to download the file. Wait 5 to 10 seconds.

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.

Step 9. Verify the policy in the Monitor and Analytics Dashboards

- 9.a. Return to Versa Director.
- 9.b. In Versa Director, open the *Appliance View* of your B01 device.
- 9.c. In the Appliance View of your B01 device, open the *Monitor* dashboard.
- 9.d. In the *Monitor* dashboard, navigate to *Services > NGFW > Anti Virus > User Defined Profile > AV-Profile > User Defined File Type*.
- 9.e. Use the search function to search for file types that contain the text *zip* and note the block count.
- 9.f. 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.



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.

- 9.g. Click the *Director View* button at the top of the Versa Director dashboard.
- 9.h. Click the *Analytics* tab to open Versa Analytics.
- 9.i. 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 10. 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.

10.a. In Versa Director, navigate to the Appliance View of your B01 device.

10.b. In the B01 *Appliance View*, navigate to *Configuration > Services > Next Gen Firewall > Security > Policies > Rules*.

10.c. Click the + button to add a new access rule with the following parameters:

UTM Rule Settings	
Name:	UTM-RULE-IDP
Source Tab:	Source Zone: Intf-Student_LAN-Zone
Destination Tab:	Destination Zone: ptvi
Headers/Schedule Tab:	Click the + New Service link and create a custom service: <ul style="list-style-type: none"> • Name: UTM-Hub • Protocol: TCP OR UDP • Port 80
Enforce Tab:	Action: Apply Security Profile: <ul style="list-style-type: none"> • Select Vulnerability: Versa Recommended Profile Logging: Both, check the Default Profile

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

Step 11. Verify the results using Versa Director

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

11.a. Return to the remote desktop session to the Linux Testing Host.

11.b. On the testing host, launch a Terminal session to open a new terminal window.

The scripts for this lab are located in the `./VASEC/` directory.

11.c. Type `cd ./VASEC/` at the shell prompt to move to that directory.

11.d. From within the terminal window, execute the following command: `./exploitS2-057-cmd.py 10.27.13.20:80 'id'`

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.

11.e. Return to Versa Director.

11.f. In Versa Director, navigate to the *Appliance View* of your B01 device.

- 11.g. In *Appliance View* of your B01 device, navigate to *Monitor > Services > NGFW > Policies*.
- 11.h. 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.
- 11.i. Navigate to the *Vulnerability* tab.
- 11.j. Select *Predefined* from the drop-down list.
- 11.k. Scroll down to the *Versa Recommended* profile. It should show a non-zero value in the Total Sessions field.

Step 12. Verify results using Versa Analytics

- 12.a. Click the *Director View* button at the top of the Versa Director user interface.
- 12.b. From the main Versa Director user interface, navigate to *Analytics > Dashboards > Security > Threats*.
- 12.c. Open the *Vulnerabilities* tab in the *Threats dashboard*. You should see charts listing the top threats and top signature IDs.
- 12.d. Click on the *attempted-user* chart to open details about the threat.
- 12.e. 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.
- 12.f. Navigate to *Logs > Threat Detection*.
- 12.g. Select the *IDP* tab. In the IDP tab you should see the log entries for the events.

Step 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).

13.a. In Versa Director, open the *Appliance View* of your *B01* device.

13.b. In Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override*.

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

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

13.d. Click *OK* to create the profile.

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

13.e. Navigate to the *Configuration > Services > Next Gen Firewall > Security > Policies > Rules* tab.

13.f. Open the *UTM-Rule-IDP* rule.

13.g. 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 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.

14.a. Return to the remote desktop session to the Linux testing host (in Remmina).

14.b. 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.

14.c. To verify that the device only generated an alert for the attack, return to *Versa Director*.

14.d. In Versa Director, navigate to *Analytics > Dashboards > Security > Threats*.

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

- 14.f. 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 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.

15.a. Return to *Versa Director*.

15.b. From Appliance View of your B01 device, navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override* hierarchy.

15.c. Click the *IDP-Override* profile to open the profile. Modify the rule with the following parameters:

Exception Parameters	
Name:	IDP-Override
LEF Profile:	Default-Loggin-Profile
Rule:	Action: Reject
Exceptions:	<p>You will add 3 exceptions to the rule:</p> <p>Click the + button and add the following:</p> <ul style="list-style-type: none"> • ThreatID: 1111209051; enable • Signatures: <ul style="list-style-type: none"> • Search for and add select the following signatures: <ul style="list-style-type: none"> • 1111209050 • 1130527060 • 1111209051 • Exception Details: <ul style="list-style-type: none"> • Action: Allow • Exempt IP Address: 10.27.13.20 • Thresholds: Track by Destination

15.d. Click OK to create the exception.

Step 16. Verify the Exception

16.a. Return to the testing host remote desktop session.

16.b. From the testing host terminal window, run the exploit script again.

16.c. 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 404 error, which indicates that the exploit reached the remote web server and was not blocked by the B01 device.

16.d. Return to Versa Director.

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

16.f. 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 17. Finish the lab and exit the lab environment

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

17.b. Log out of Versa Director.



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