Lab Security Packages and Updates

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

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

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

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

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

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

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

Look for these hints to help you in the labs

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

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

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

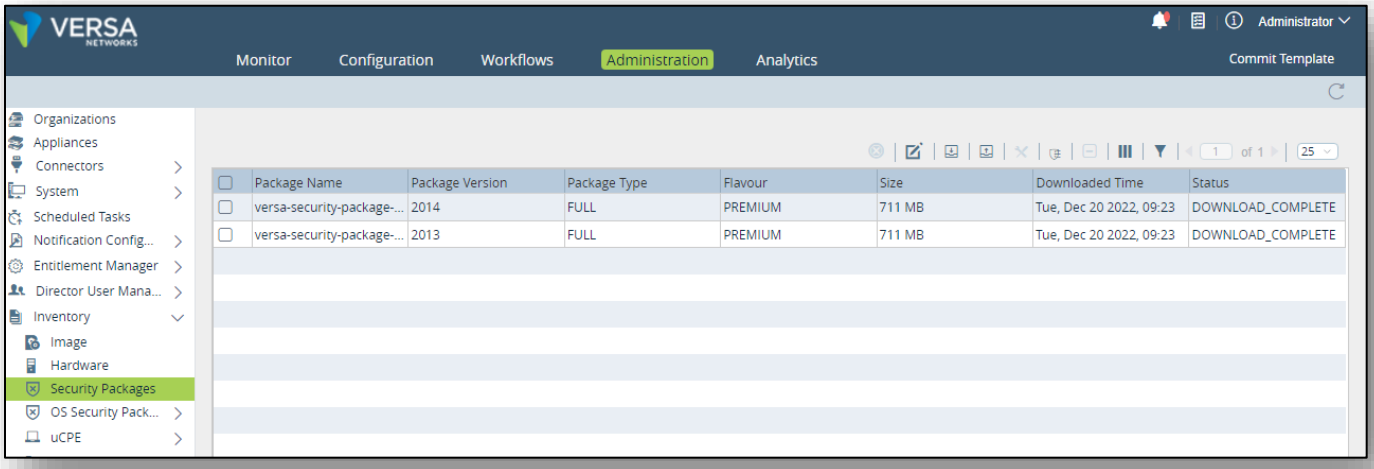
Exercise 1:

In the following lab exercises, you will:

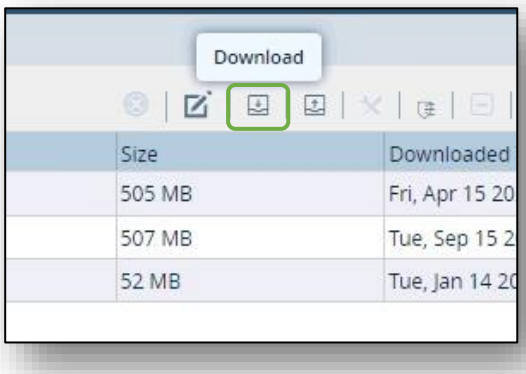
- Identify where Security Packages are stored in Versa Director
- Learn how to download a security package to Versa Director
- Update your branch device security package

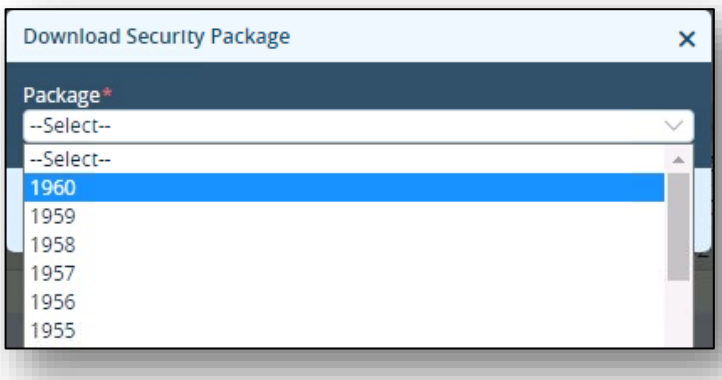
Refer to the Lab Access Guide for instructions on how to connect to the remote lab environment. Once you have connected to the remote lab environment, log into Versa Director on your remote desktop workstation.

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



Click the Download button to open the SPACK download dialog. Versa Director will automatically check the SPACK repository and list the available security packages.

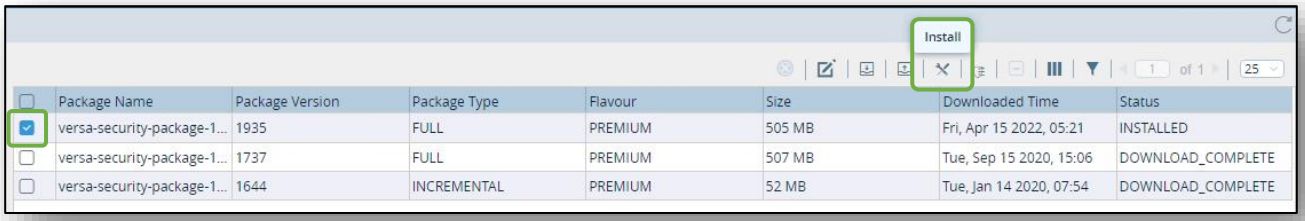




Note: DO NOT DOWNLOAD A SECURITY PACKAGE. The Versa Director is a shared environment. Please do not perform the security package download as it will create multiple processes, as multiple students may perform the same task.

Click the Cancel button to cancel the download process.

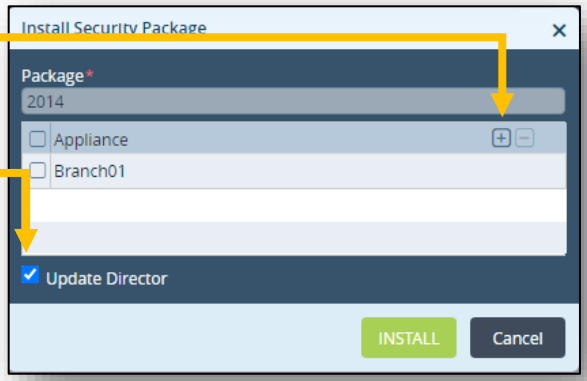
Locate the latest security package version in the database. Check the box next to the latest security package and click the Install button.



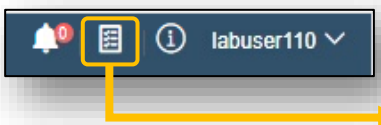
In the Install Security Package dialog, click the + button and add your device to the appliance list.

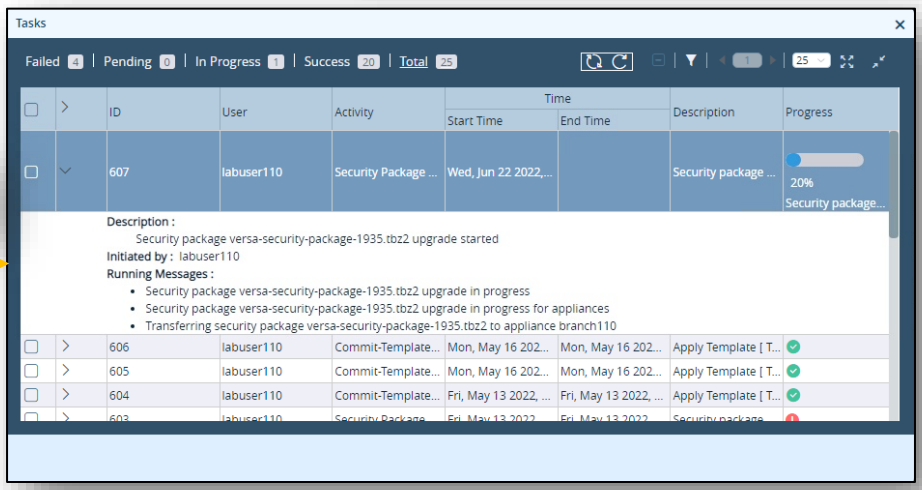
Uncheck the Update Director box.

Click the Install button to install the security package to your appliance.



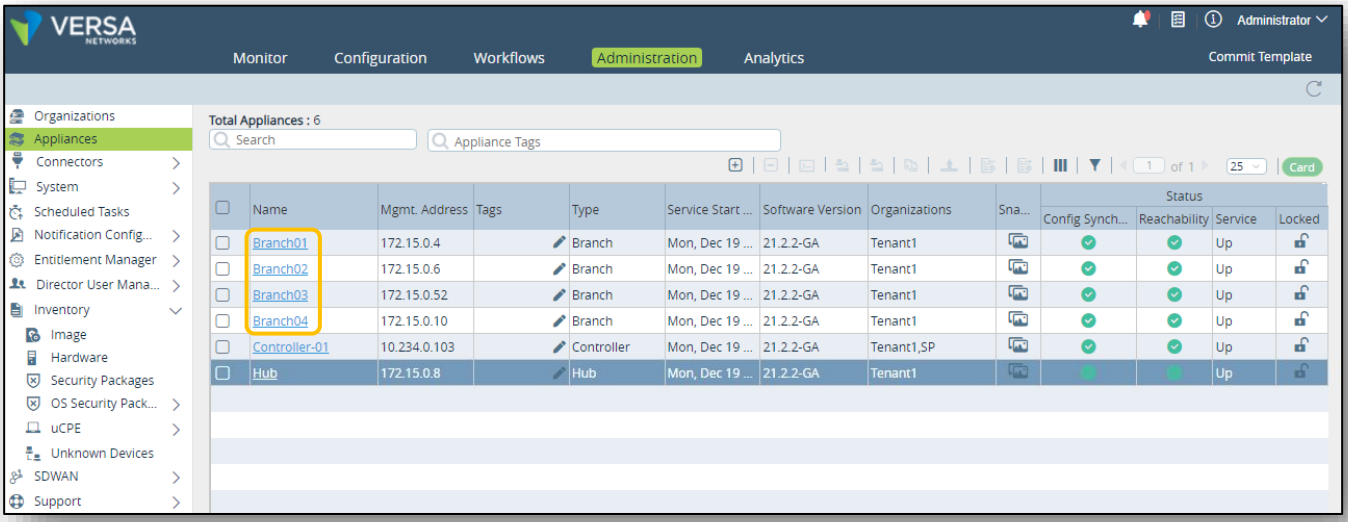
You can monitor the progress of the security package update through the Tasks panel



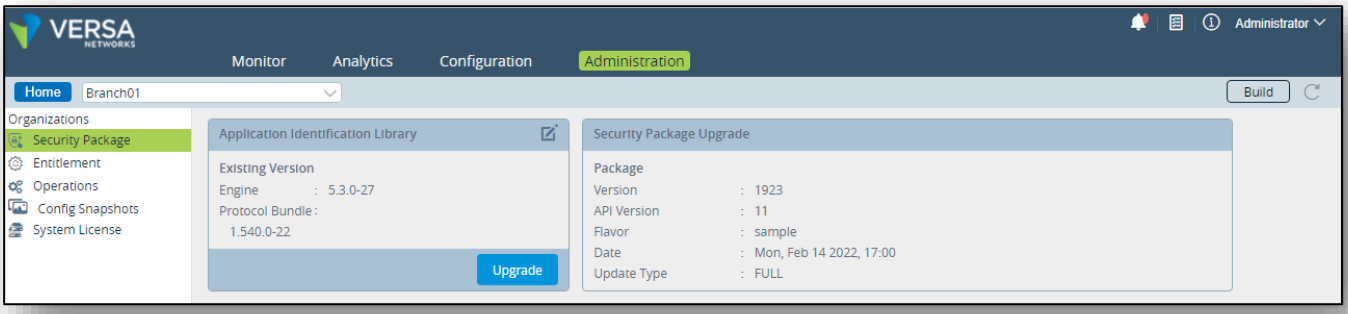


Before you continue, take note of the package version that was just installed on your device. In the example, the package version was 1935.

In the Administration dashboard, navigate to Appliances to display the appliance table. Locate your appliance in the table and click on your appliance name to open the appliance context mode. This will allow you to view, configure, and monitor the appliance directly.



In your branch Appliance Context mode, select the Administration tab. You should see the Security Package menu item on the left-side menu. Select Security Package in the left menu.



Take note of the currently installed security package. It should match the package that you installed from Versa Director. Note the date of the security package (Mon, Apr 11, 2022). This is not a current security package.

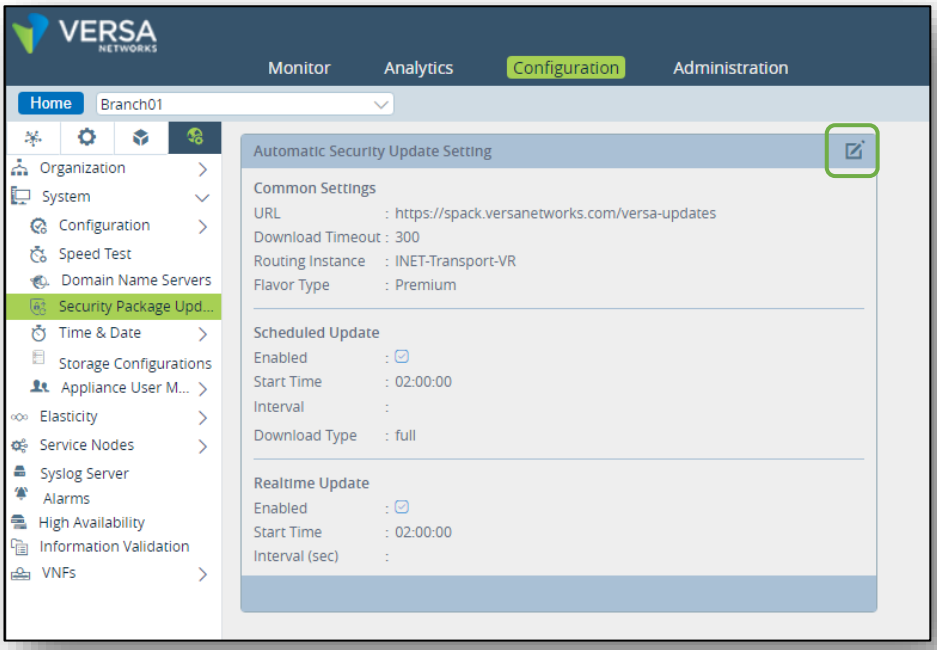
In the next steps you will configure your appliance to perform auto-updates of the security packages.

Exercise 2

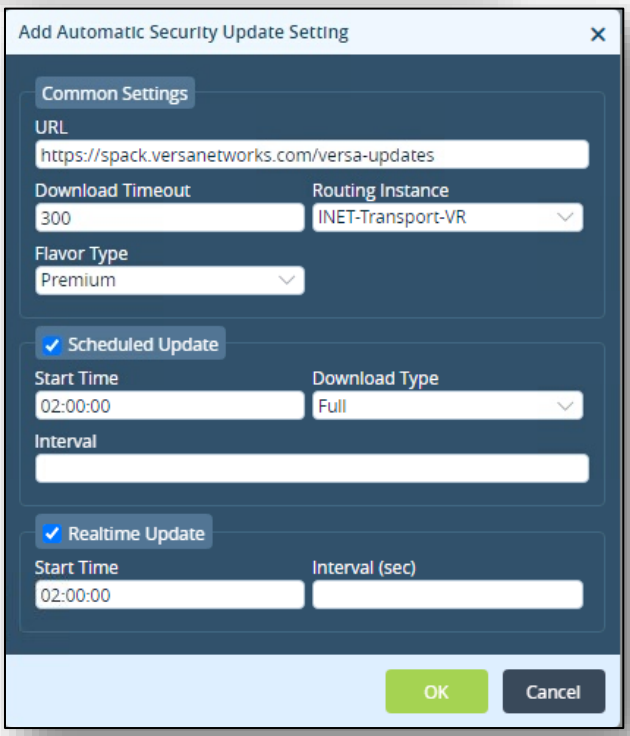
In the next exercise you will configure your appliance to perform automatic security package updates.

In Appliance Context mode, navigate to *Configuration > Others > System > Security Package Updates*.

Click on the Edit icon in the top right to edit the settings.



Fill in the form with the information in the example: Click OK when finished. Your device is now configured to automatically update the security packages when they are released.



Your appliance is now ready for the advanced security lab exercises.

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 single CPE device (Branch device) for configuration and monitoring.

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

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

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

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

Look for these hints to help you in the labs

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.

Exercise 1:

In the following lab exercises, you will:

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

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

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

Step 1: Reset the lab to a base configuration

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

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

Step 2: Open the Device Configuration

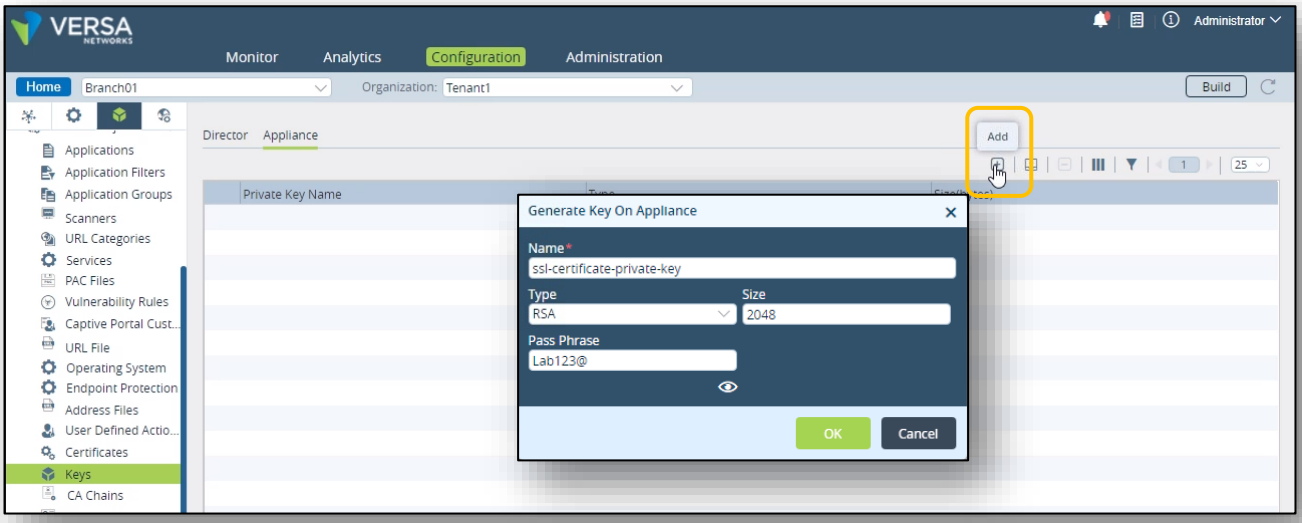
In the next steps you will create an SSL encryption key for your branch device. You will then create a self-signed SSL certificate for the device. **The certificates and keys must be created on the appliance (in Device Context mode) and not in the device templates.**

Step 3: Create an SSL encryption key

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

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

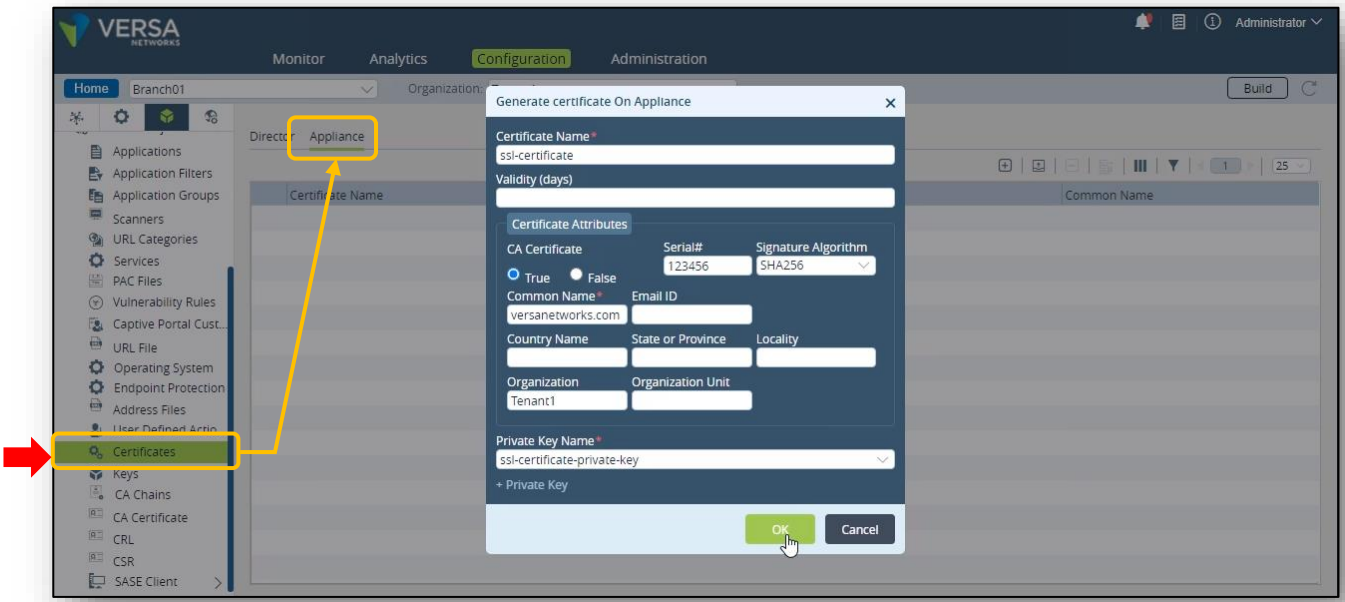
The encryption key is a custom object that is configured under the *Objects & Connectors > Custom Objects > Keys* hierarchy. Create an encryption key for the APPLIANCE with the following parameters:



Step 4: Create an appliance certificate

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

Create an APPLIANCE certificate with the following parameters:

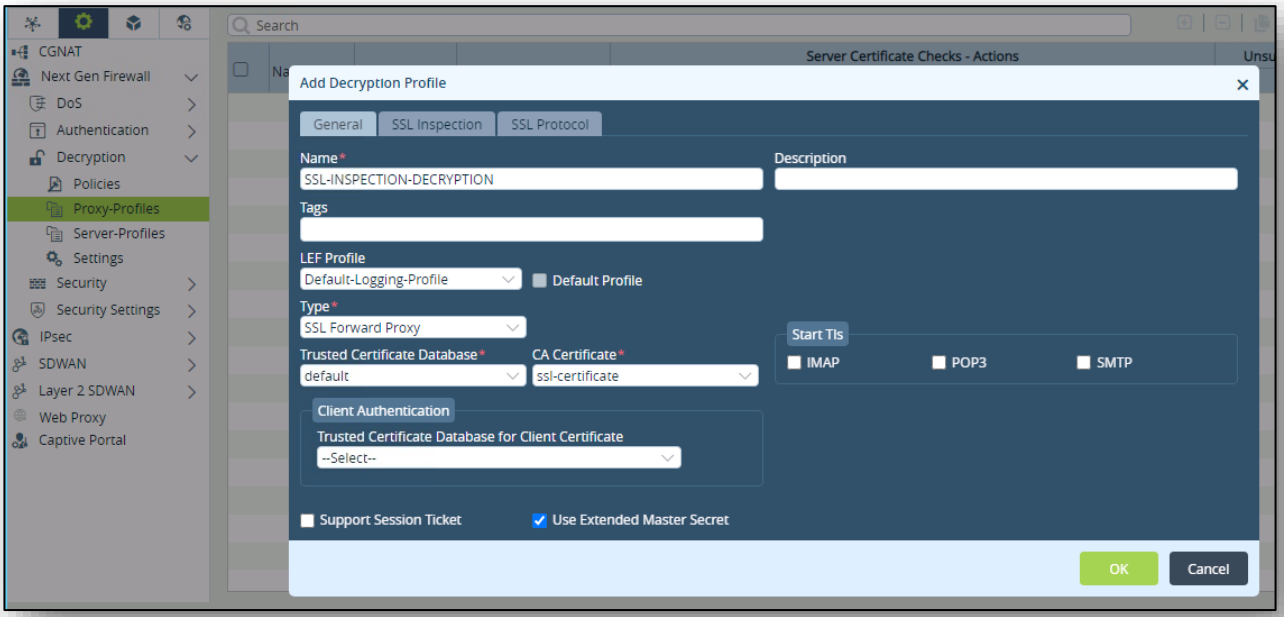


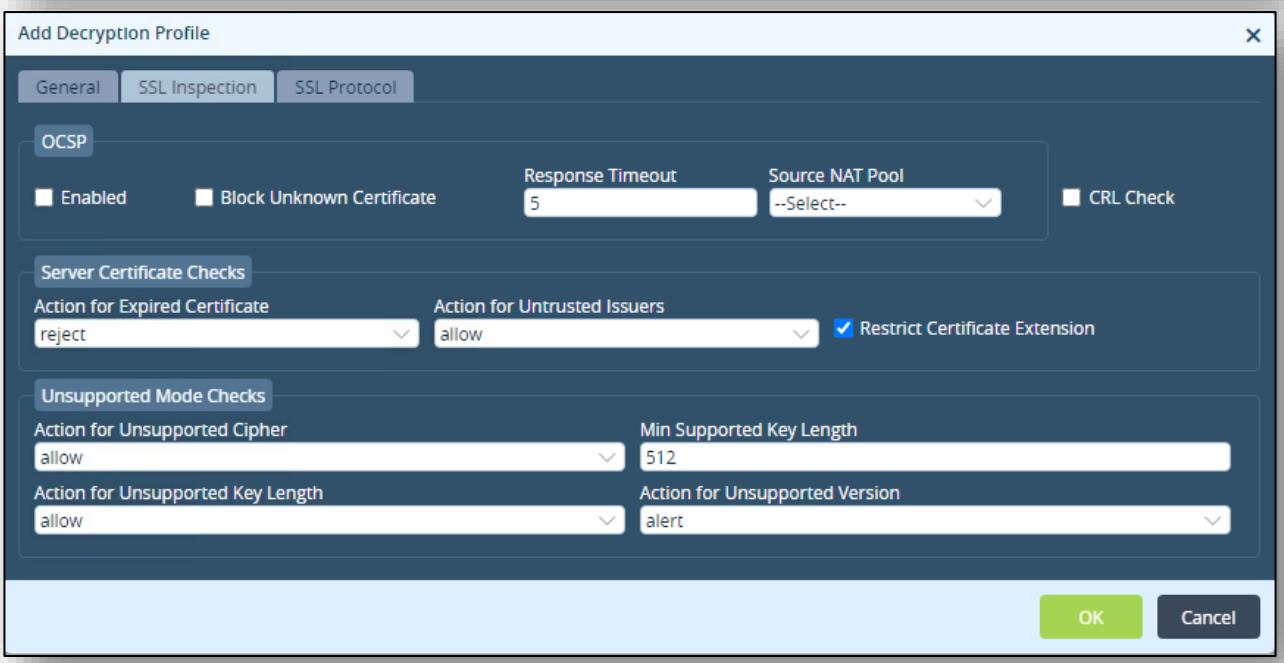
Step 5: Configure Proxy Profiles

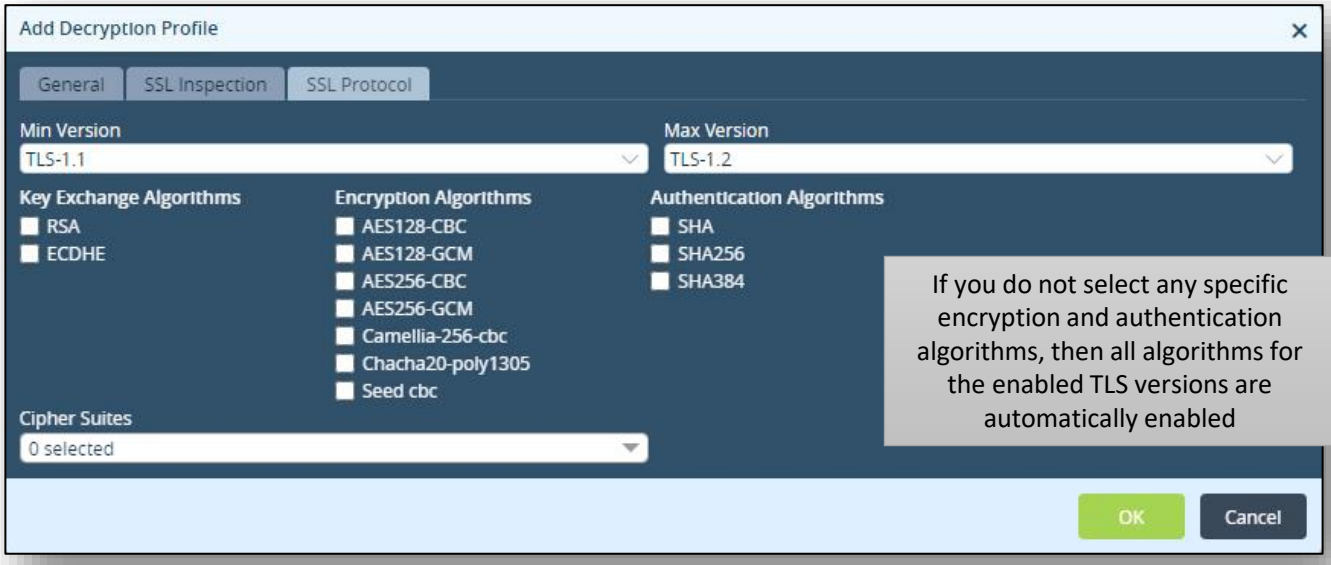
In the next steps you will configure a proxy profile (decryption profile) and a decryption policy policy to perform SSL inspection or decryption on specified web traffic.

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

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





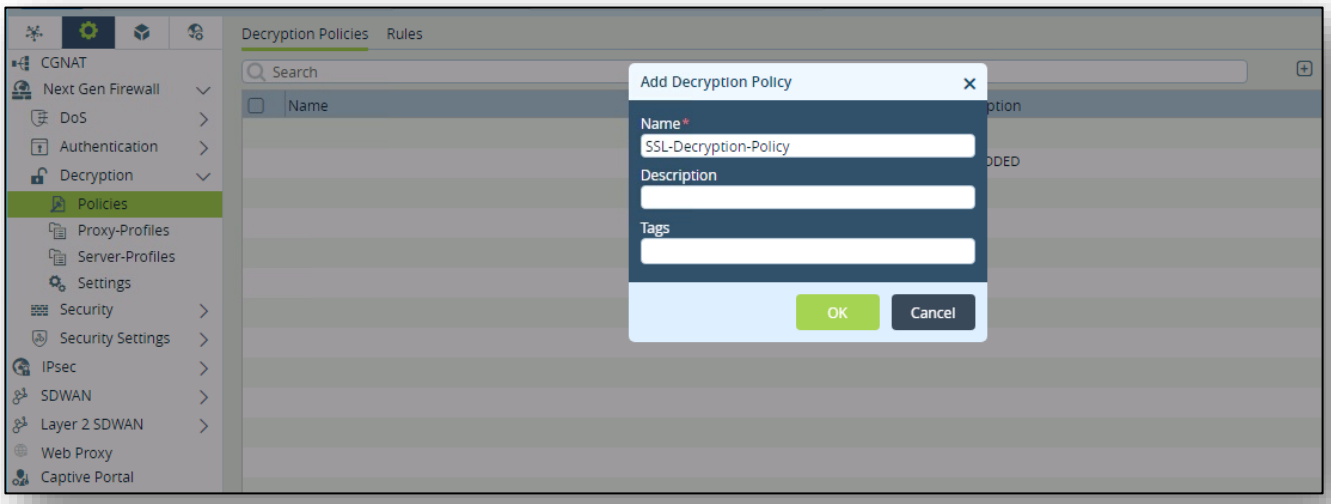


Step 6: Create an SSL Decryption Policy

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

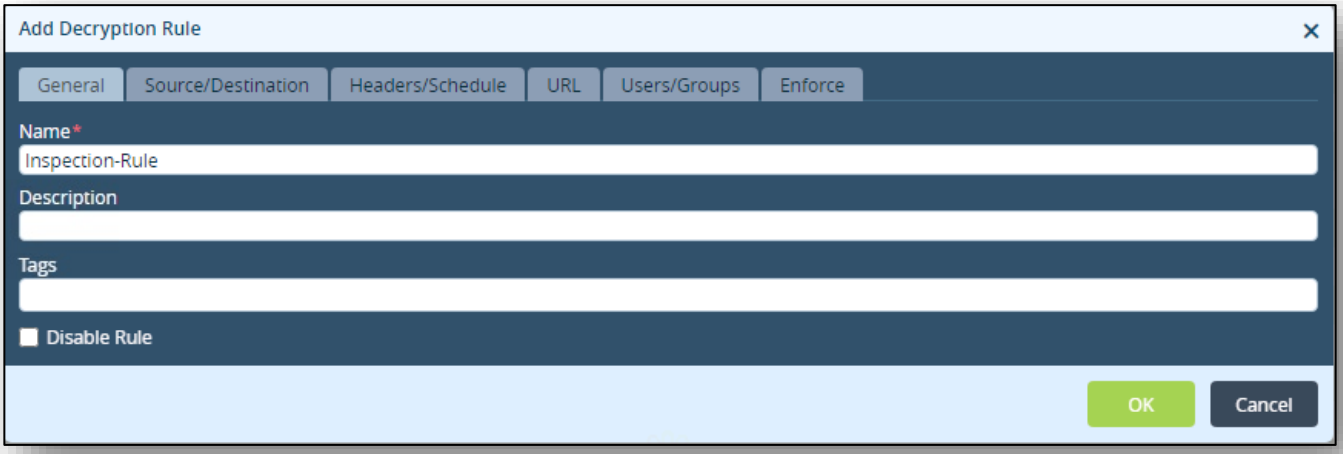
- Rule 1 will identify traffic from Financial-Services web sites and will NOT decrypt the traffic (inspection only)
- Rule 2 will identify traffic from sports, news_and_media, and social_networking URL categories and will decrypt

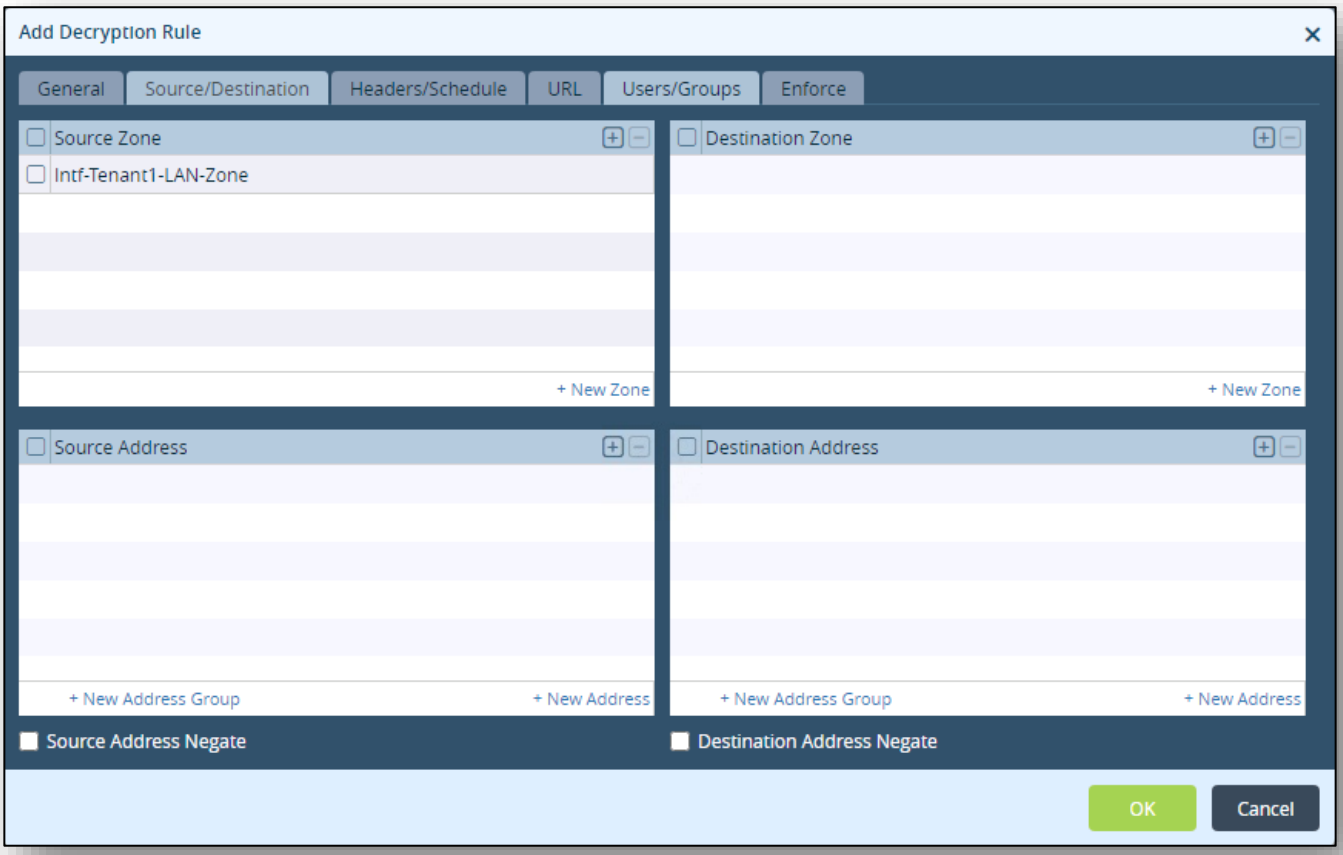
Begin the process by creating a decryption policy, as a decryption policy is not created by default.

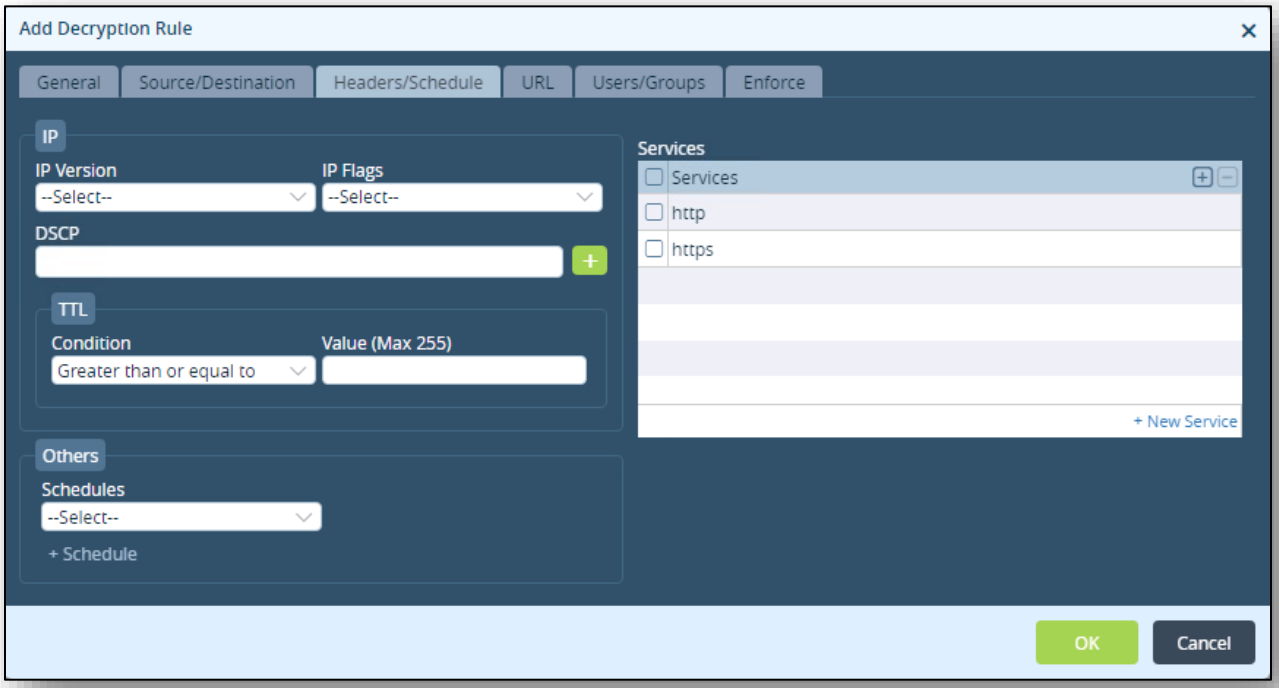


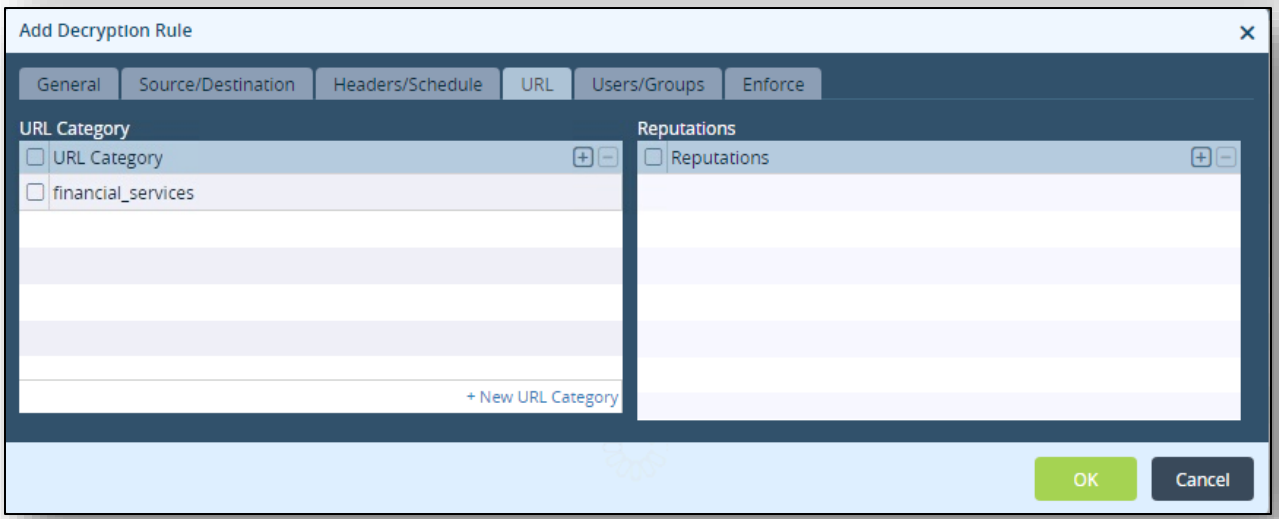
Next you will create 2 rules with the following parameters:

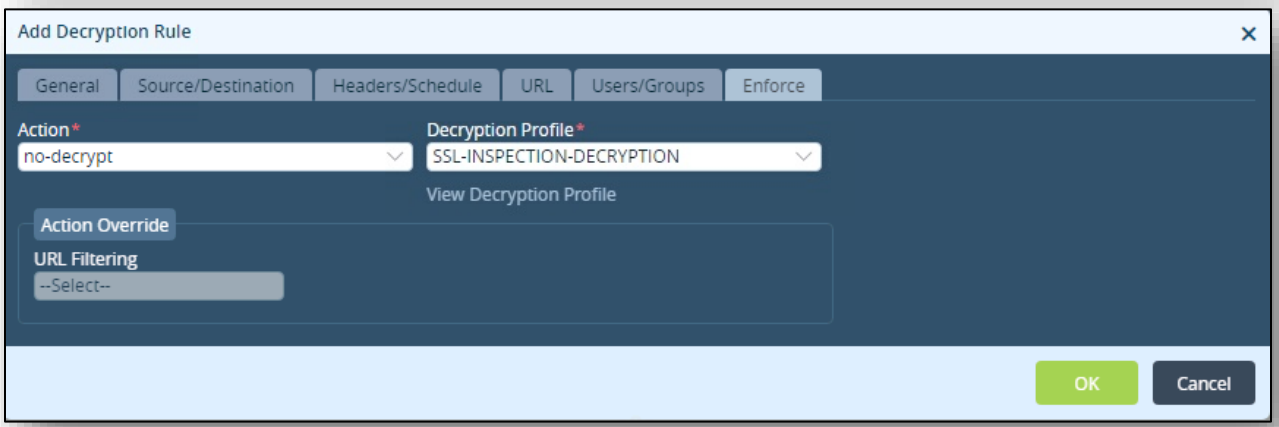
Rule 1: Inspection Rule



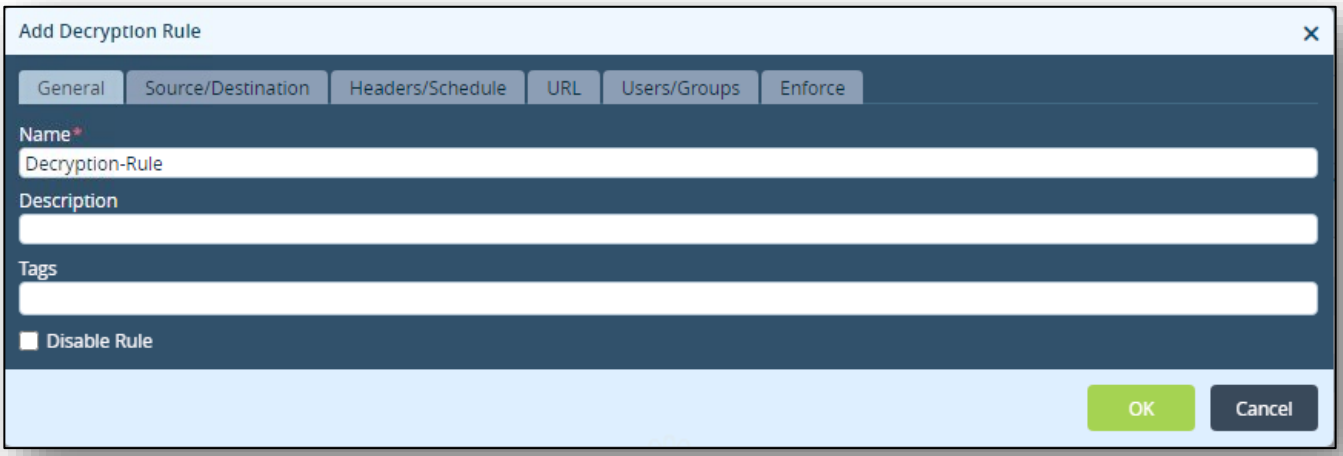


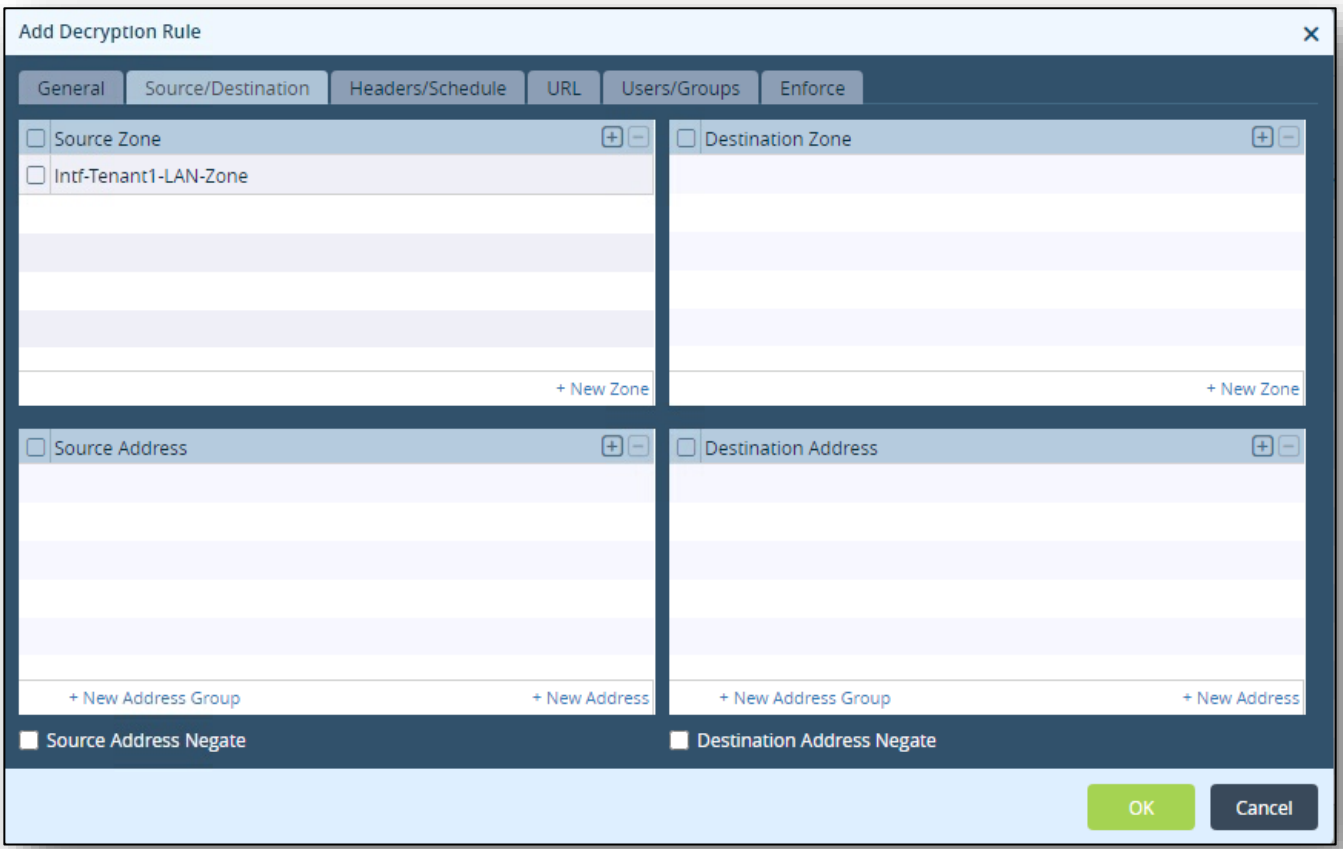


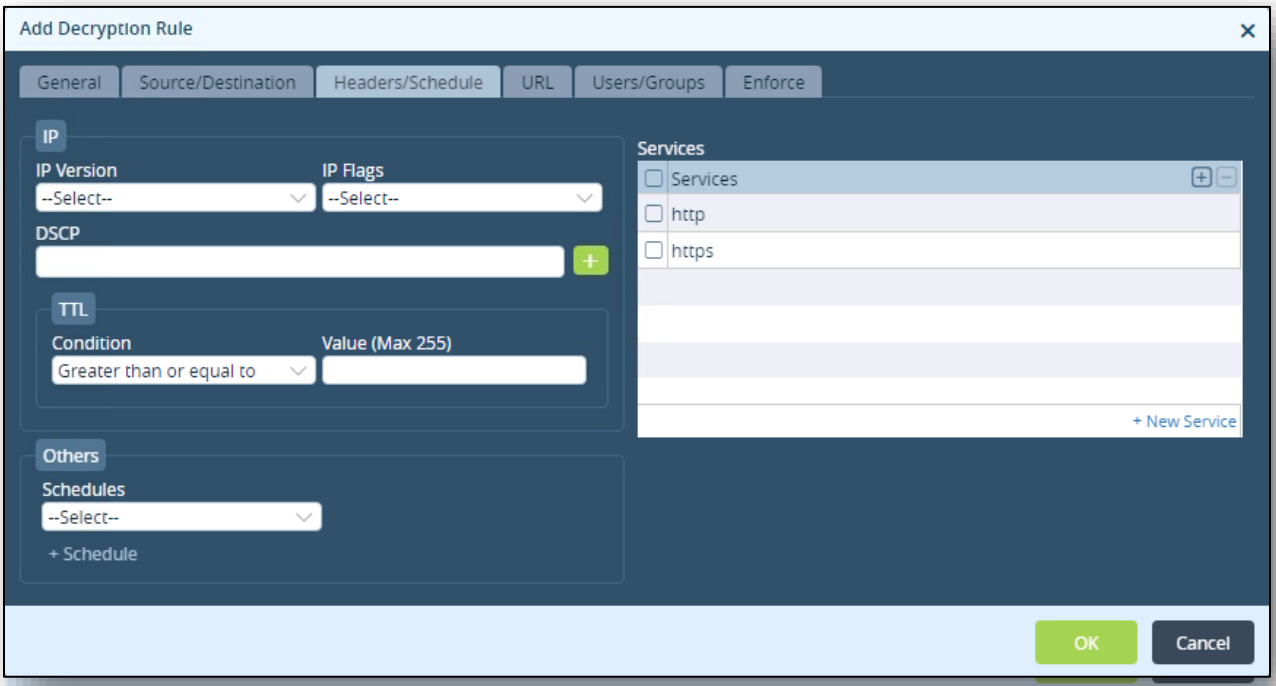


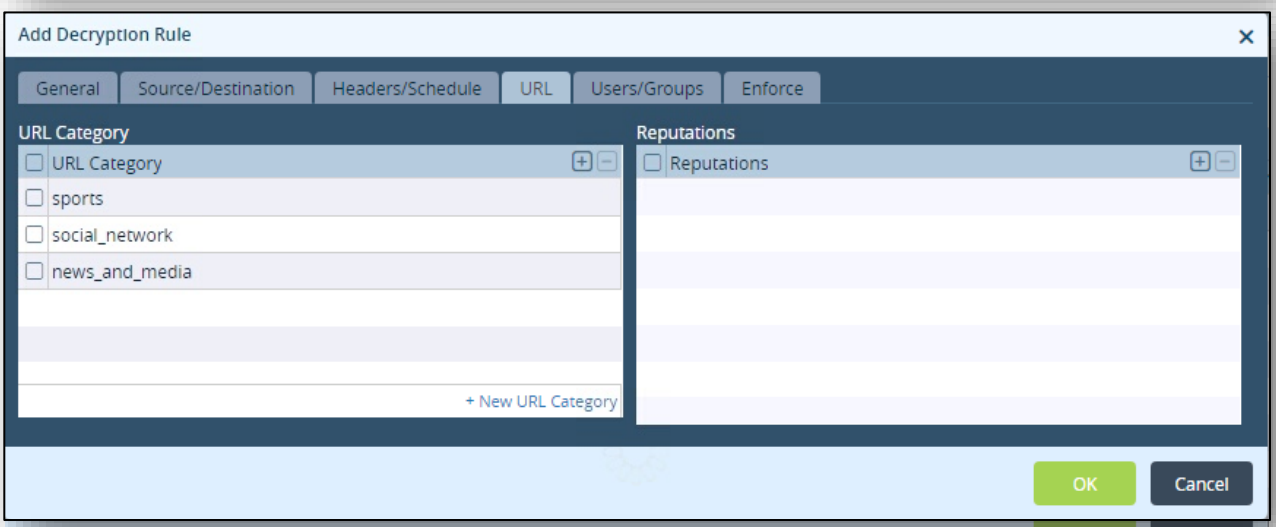


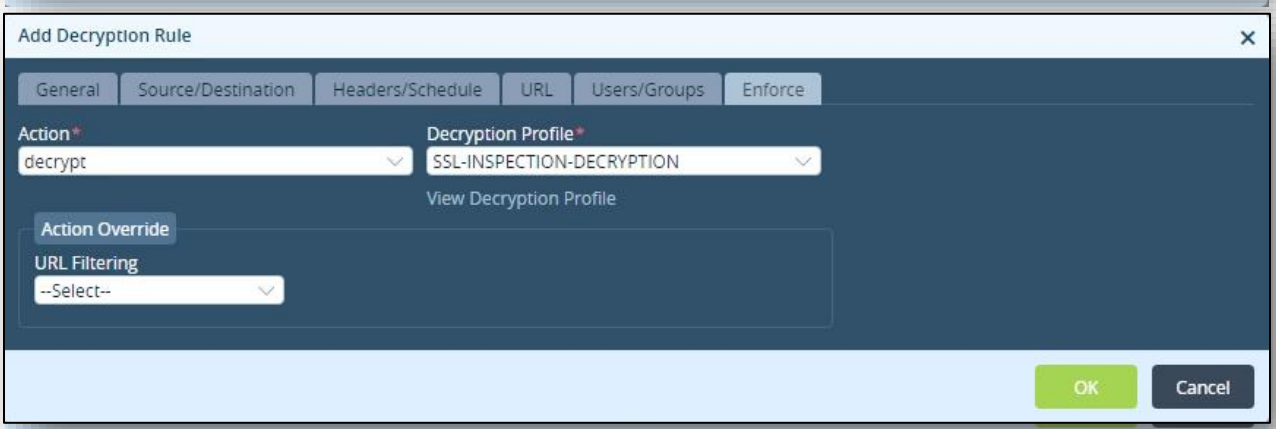
Rule 2: Decryption Rule











Exercise 2: Test the Decryption Policy

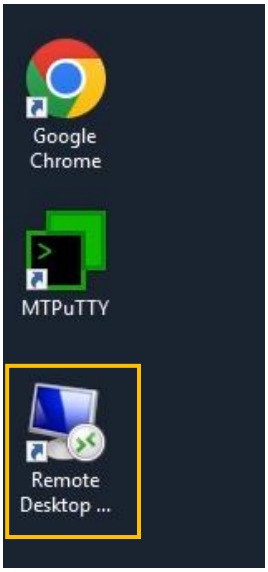
In this exercise you will test the decryption policy. To test the policy you will open a remote desktop session to the testing host (from the remote desktop) and use the Chromium web browser to visit sites that will be processed by the proxy profile.

Steps in this exercise:

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

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

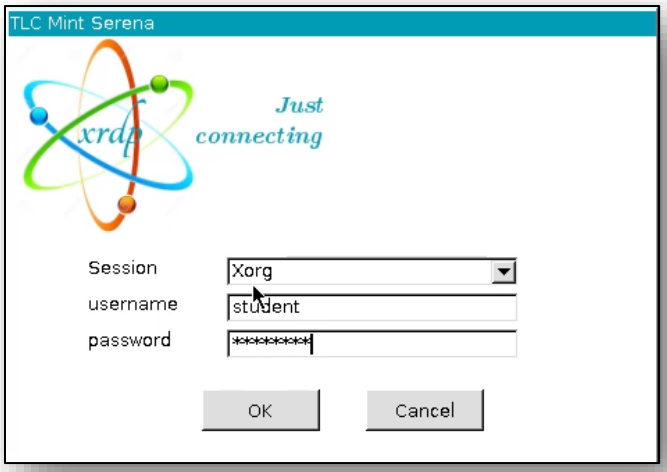
Locate the Remote Desktop Session icon on the remote desktop:

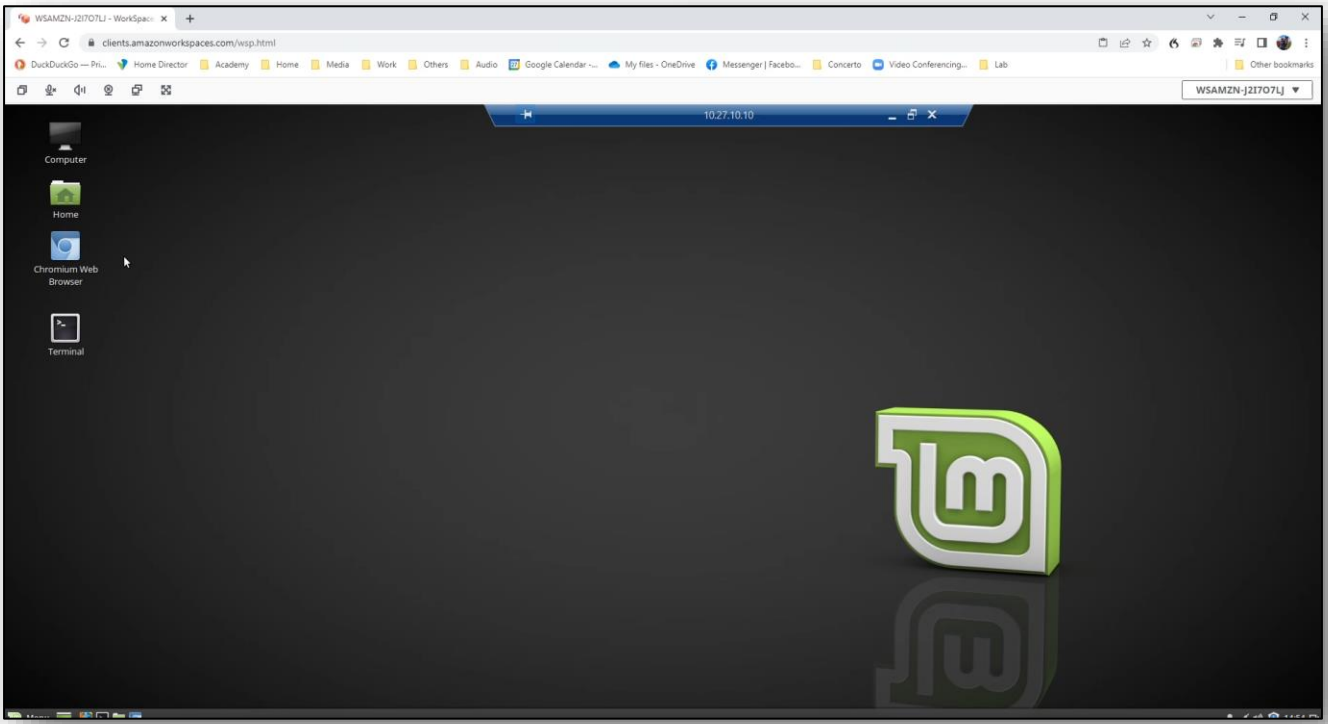


Double-click the icon to open the remote desktop application and start a remote desktop to your testing host based on the IP addresses listed in the Lab access guide.

When presented with the identity warning, click Yes to continue with the connection.

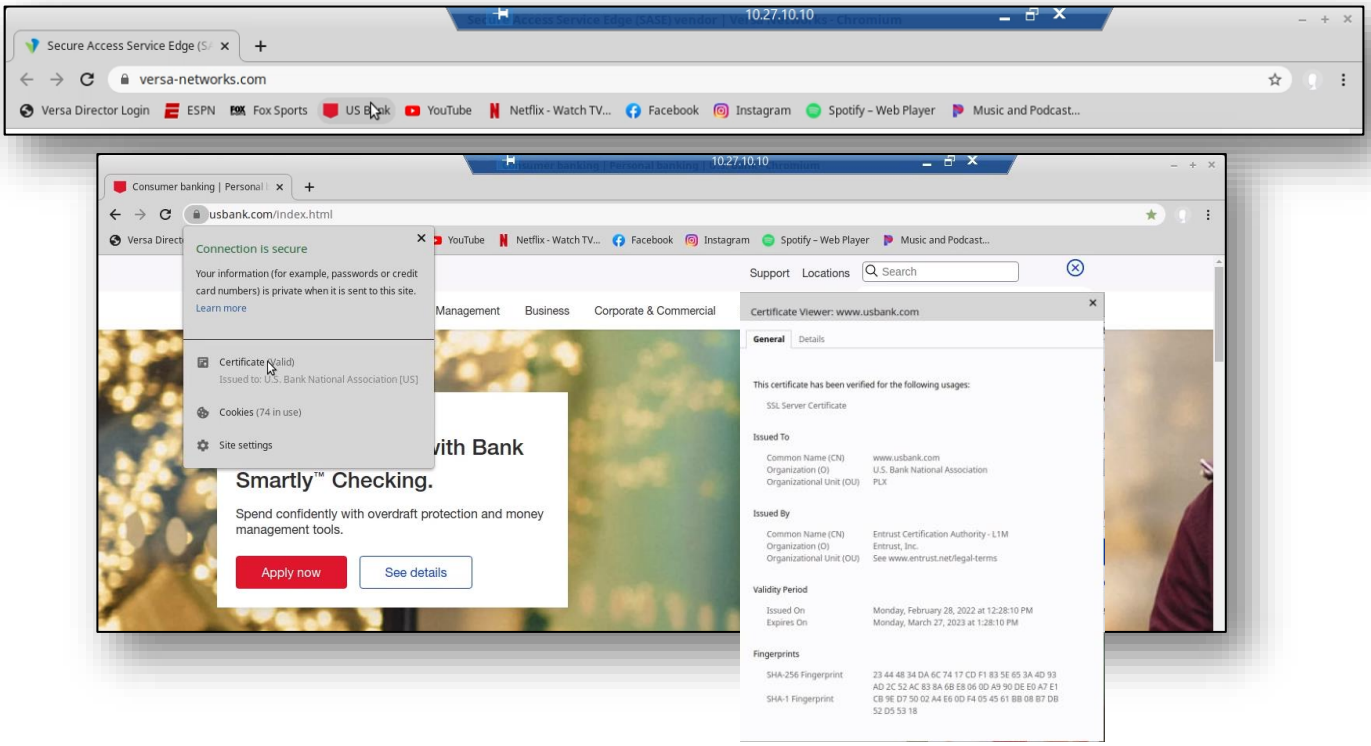
When presented with the remote desktop login window use the username ***student*** and password ***versa123***.





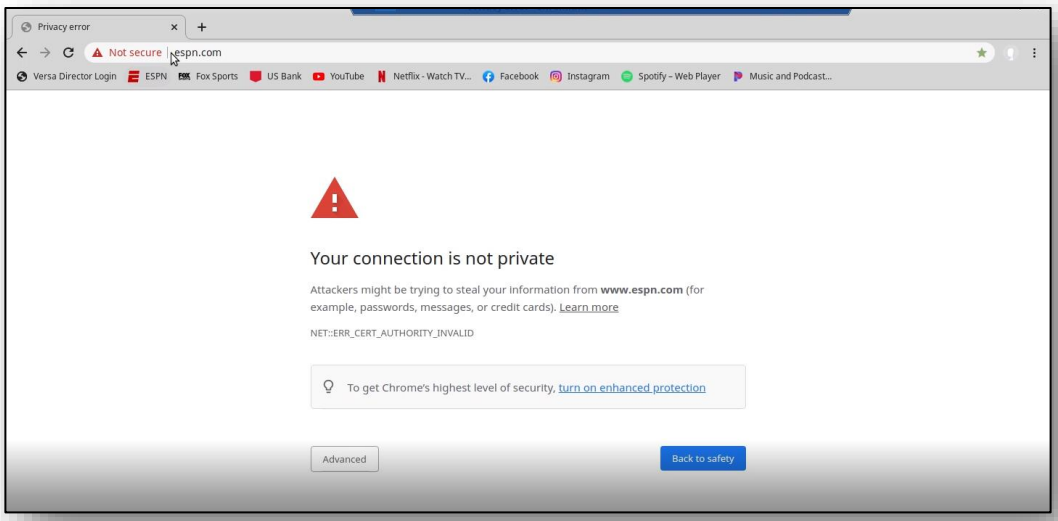
For this exercise use the Chromium Web Browser for proper performance.

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

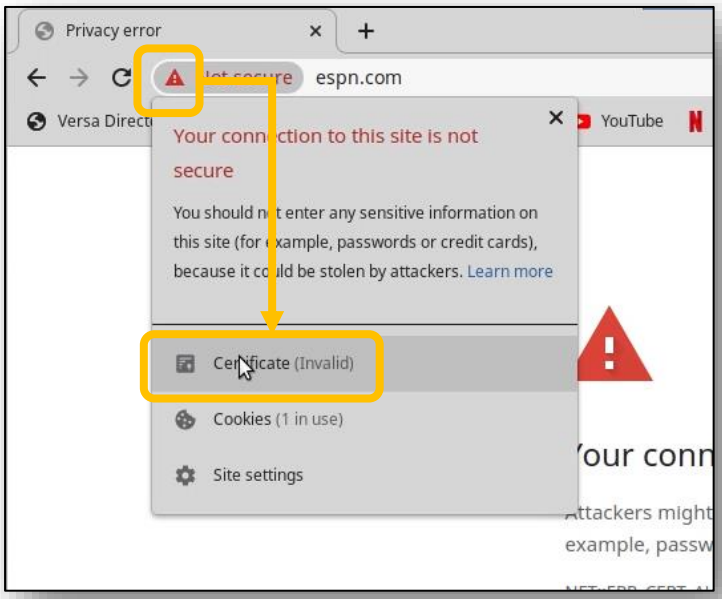


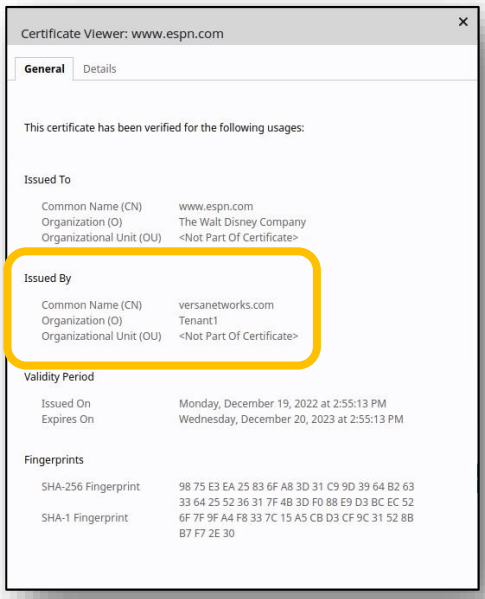
After the page loads, click Lock icon in the address bar. You should see a popup that indicates that the certificate (and site) is valid. If you click the Certificate button, you will see that the certificate was verified by Entrust, Inc. (a registered certificate authority).

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



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



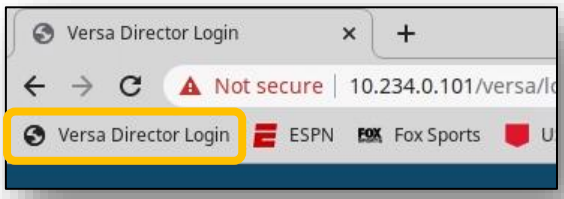


The certificate for the sports site was provided by Tenant1. This is because the branch device intercepted the SSL session and is acting as a proxy for the SSL tunnel.

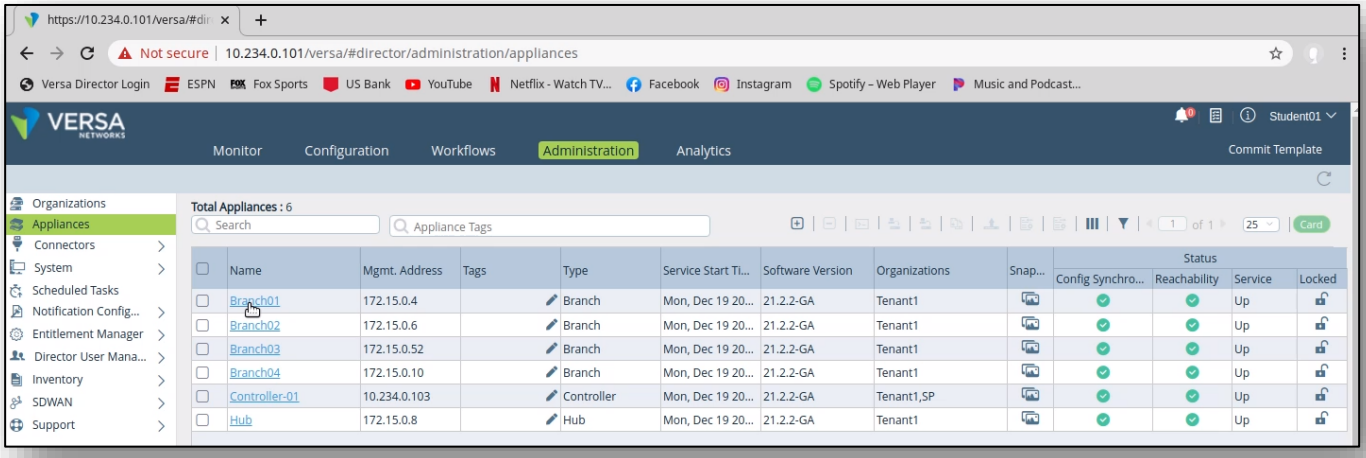
To allow the browser to trust the Tenant1 certificate, you must download the certificate to the host machine and add it to the trusted certificate provider list.

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

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

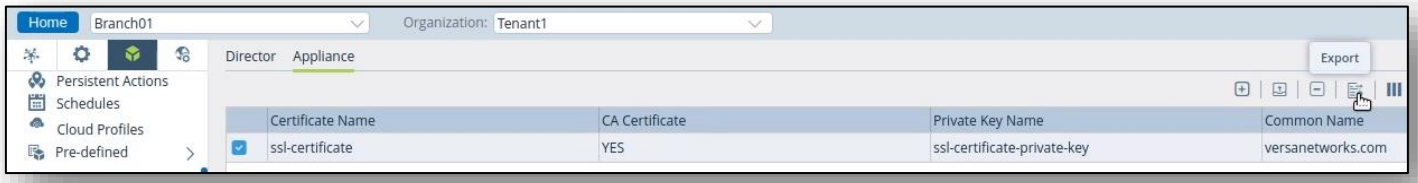


In Versa Director, navigate to the Administration > Appliances dashboard and locate your appliance in the appliance table. Click your appliance to open your appliance configuration.

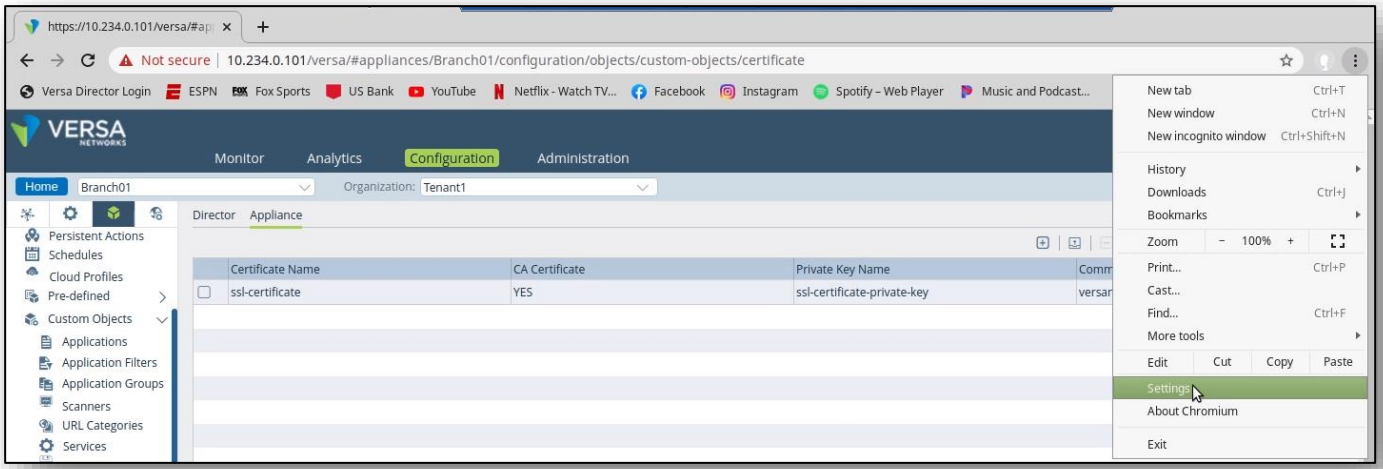


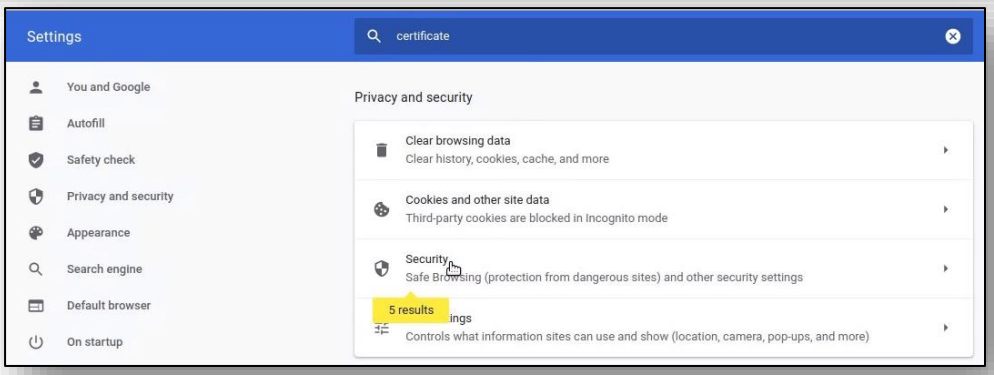
In your appliance configuration, navigate to ***Objects & Connectors > Custom Objects > Certificate***s, then select the Appliance tab in the Certificates window.

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

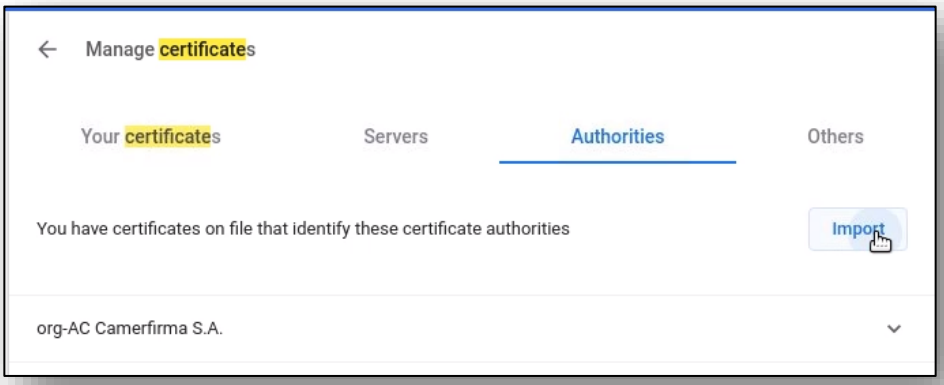


After you have downloaded the certificate, click the Settings button in the remote browser and open the browser Preferences. In the preferences window, type the word certificate in the search window. This will display the View Certificates button. Click the View Certificates button to open the certificate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

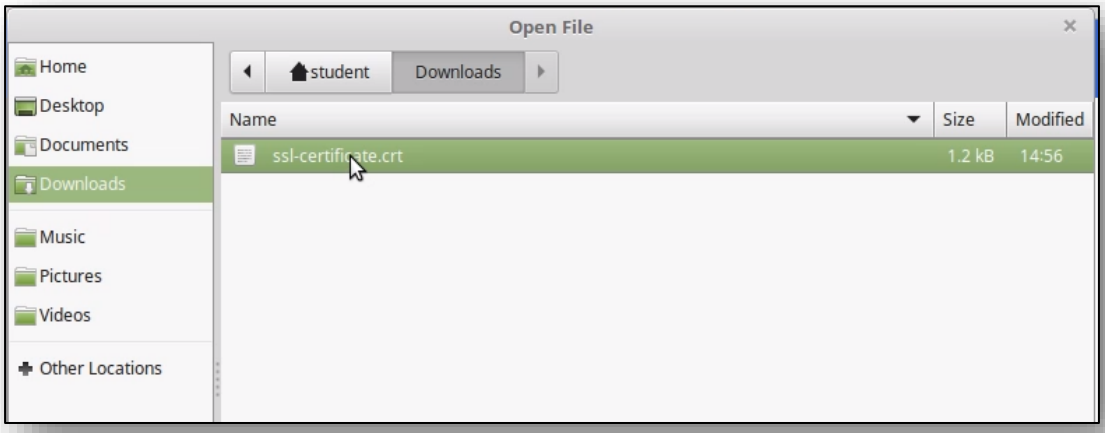




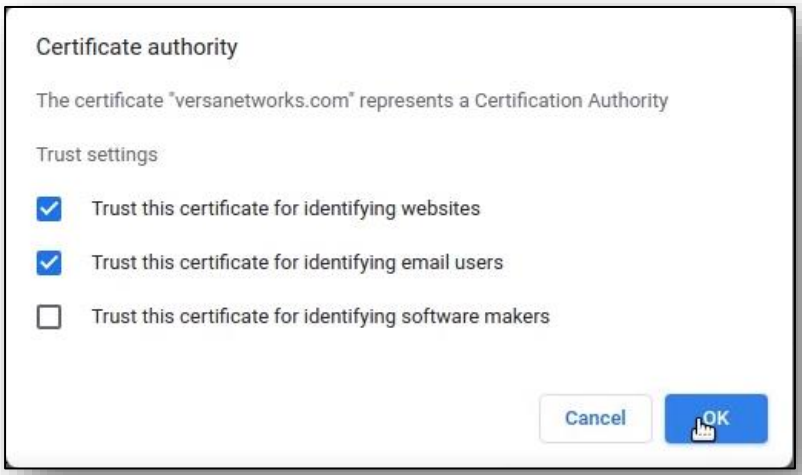
In the Certificate Manager window, select Authorities from the top menu bar. Scroll down in the Authorities window until you see the Import button at the bottom.



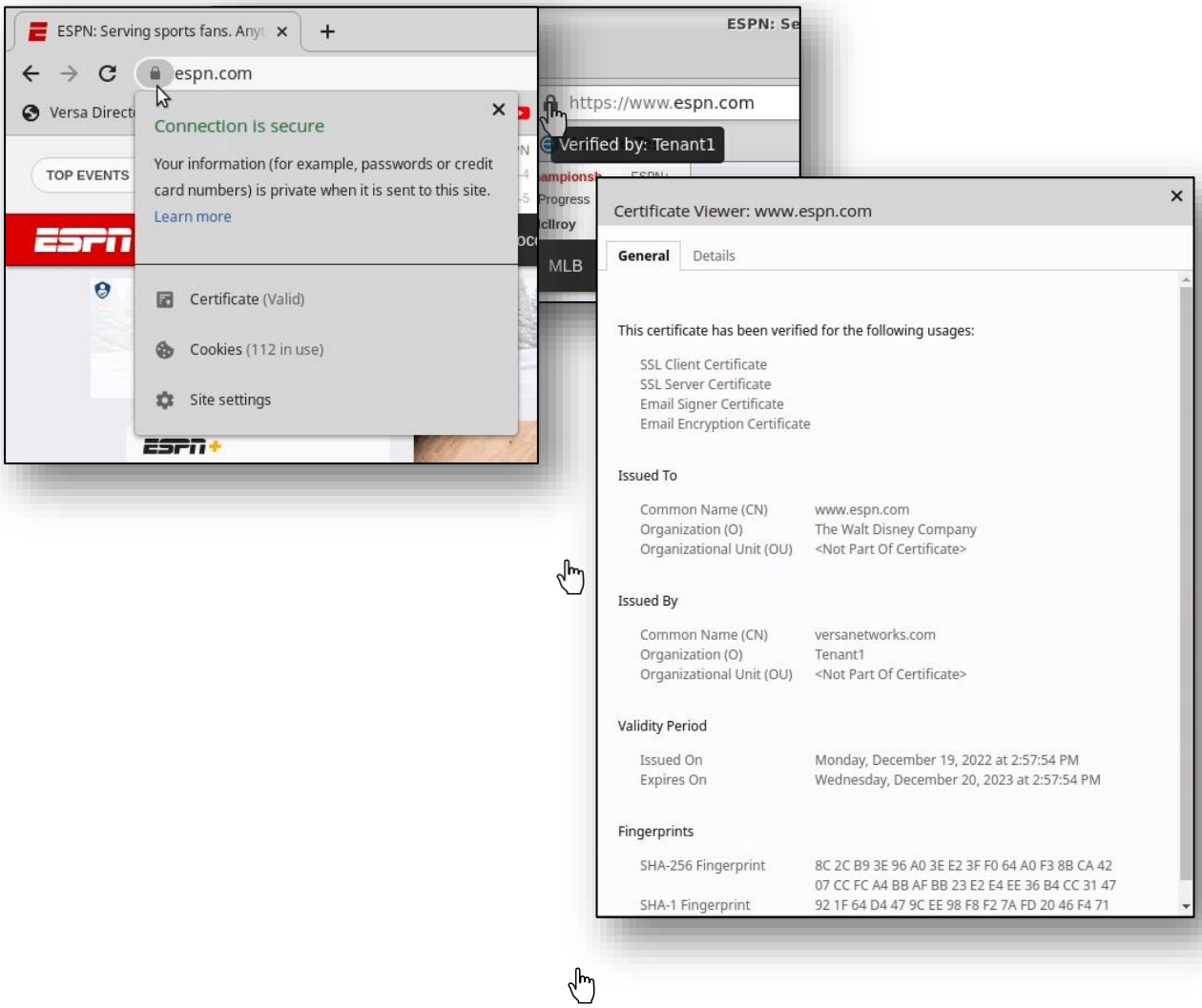
Open the Downloads folder and locate the new SSL certificate. Note that there will be a duplicate certificate because a certificate was already present. Choose the newer certificate (based on the date) and click the Open button to import the certificate.



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

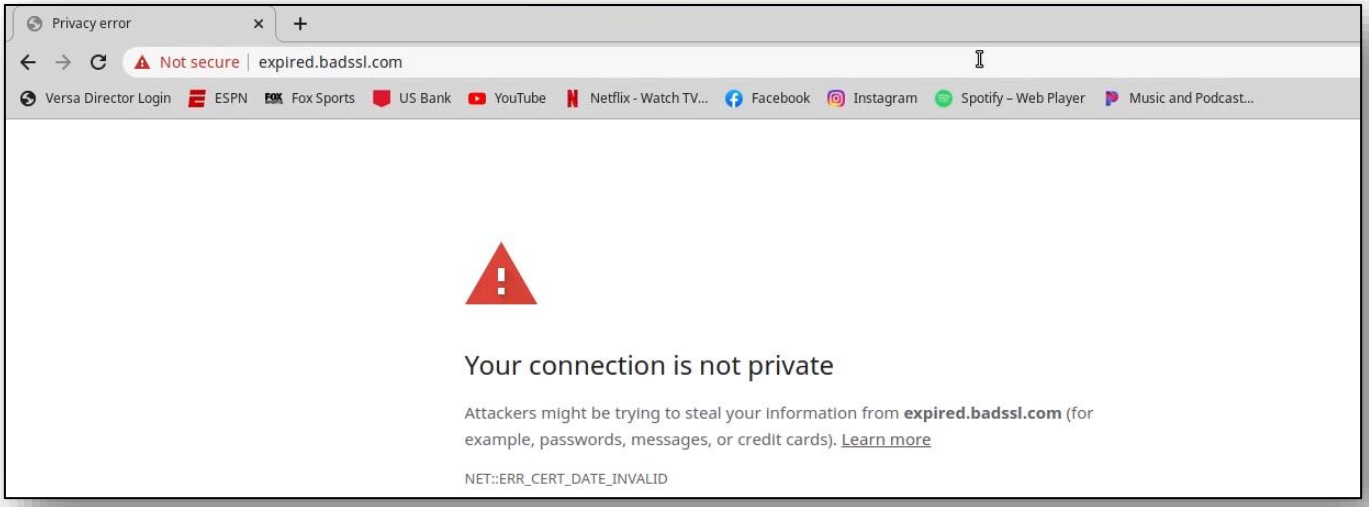


Enter the address ***www.espn.com*** in the remote browser address bar again. The web site should now open properly.



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

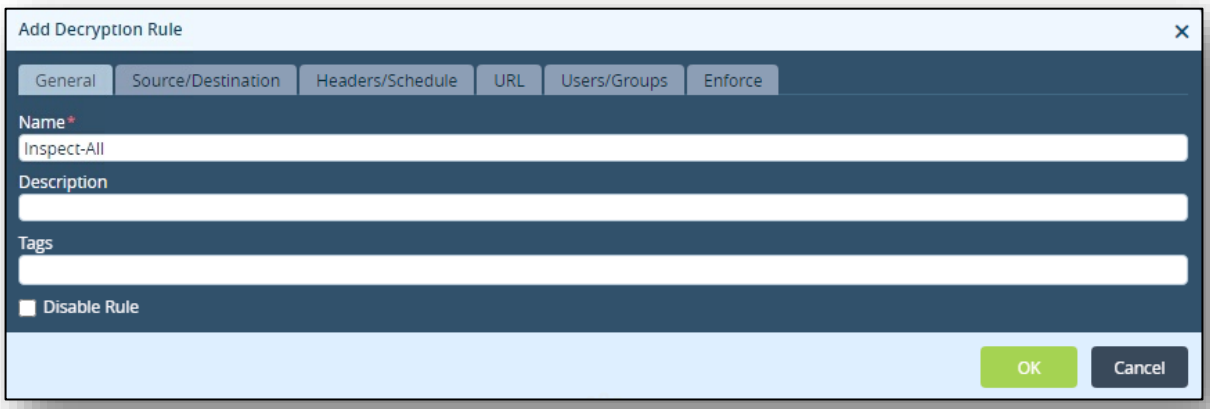
In the remote browser, navigate to ***https://expired.badssl.com***. You should receive a browser warning that the certificate has an issue. Currently the proxy policy rules do not match the site, so the bad certificate is loaded by the browser and the browser provides the warning.

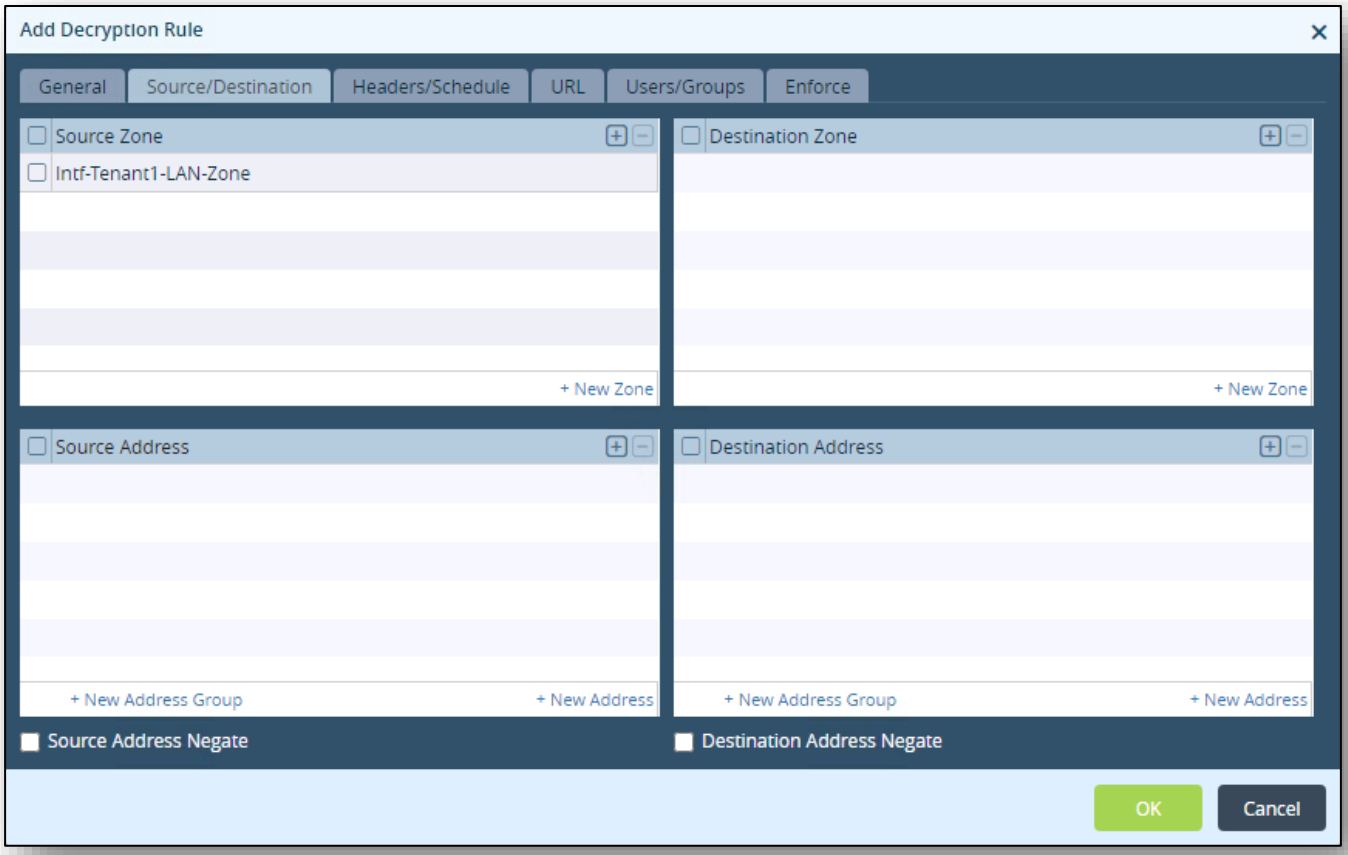


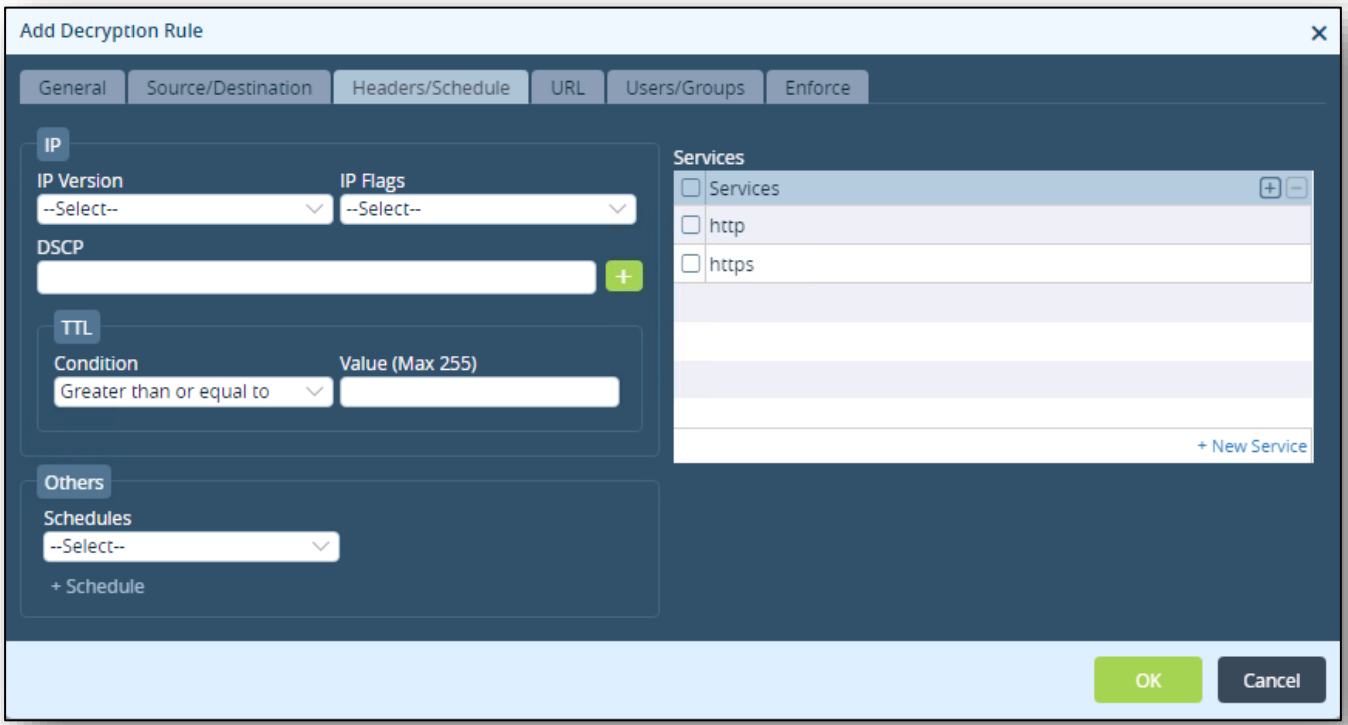
Return to the Versa Director session on your remote desktop.

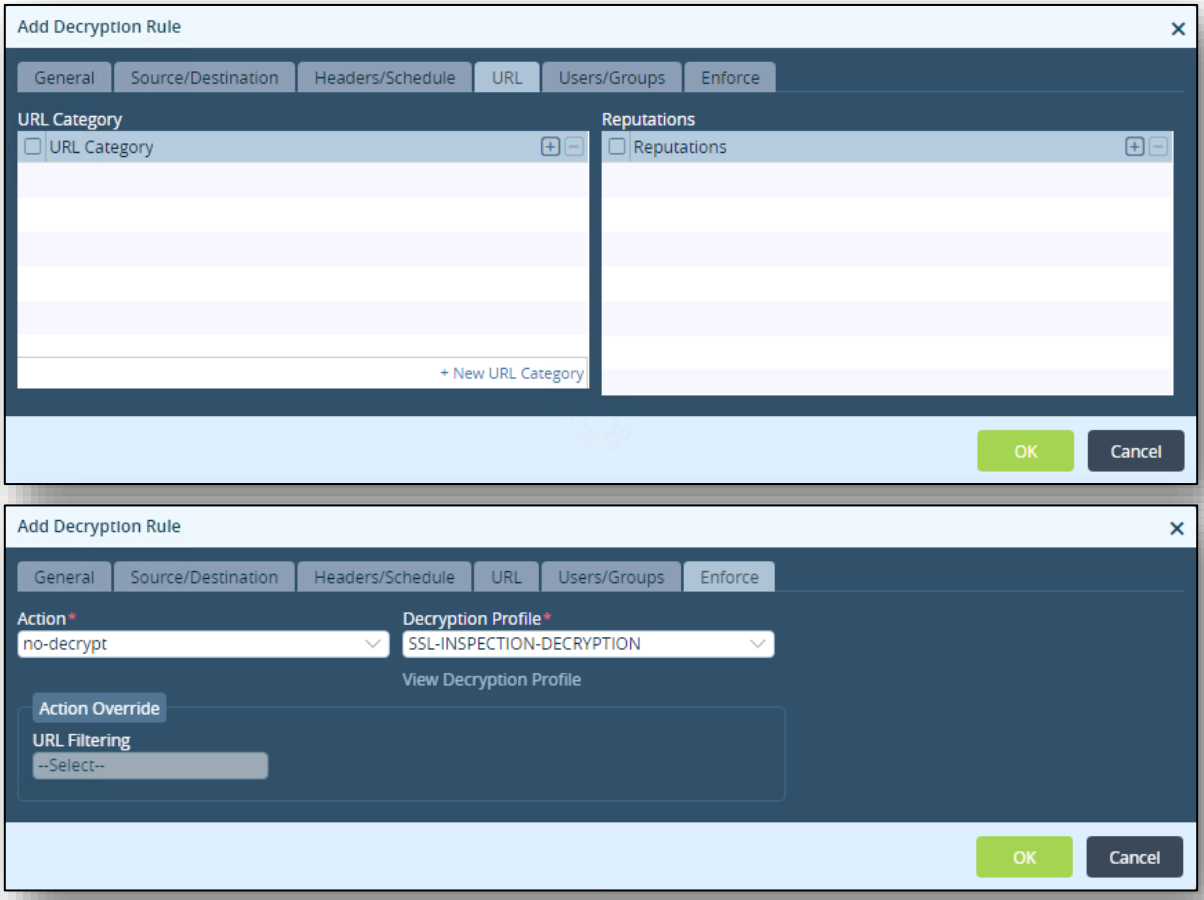
In Versa Director, navigate to your device configuration and open the *Services > Next Gen Firewall > Decryption > Policies* configuration.

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

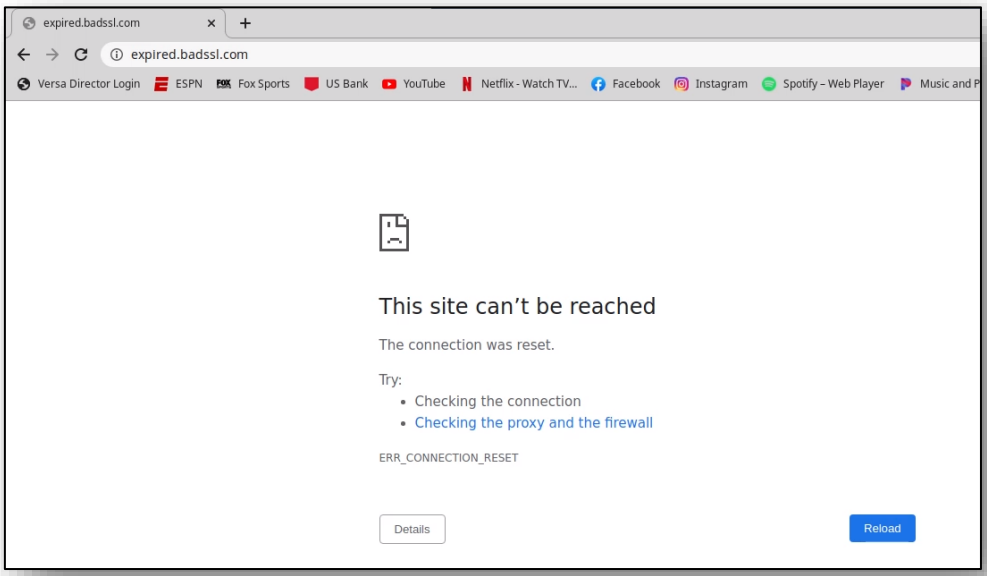








After the rule has been created, return to the remote desktop session to the testing host. In the remote browser session, click the refresh button to reload the https://expired.badssl.com site. You should receive a Secure Connection Failed error. The VOS appliance reset the connection because the certificate was invalid.



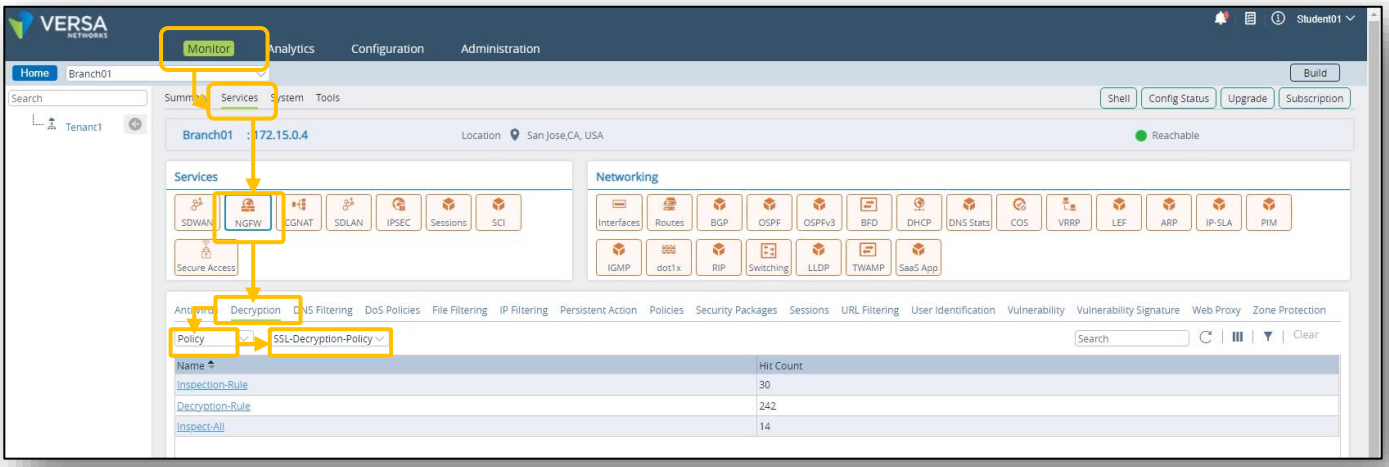
Exercise 3: Verify the Decryption Process in Versa Director and Versa Analytics

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

Close the remote browser connection to the testing host and return to your remote desktop. In your remote desktop, navigate to the Monitor tab of your appliance. In the Monitor tab of your appliance, select the Services tab to display the Services dashboard.

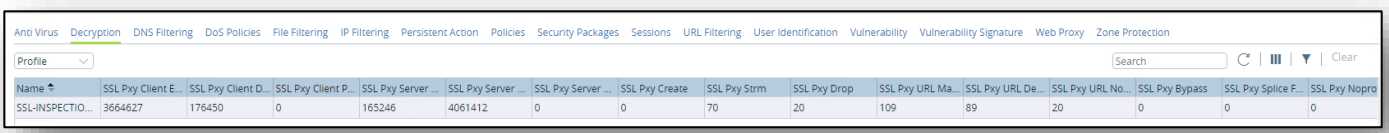
In the Services dashboard, select NGFW to display the Next Generation Firewall statistics.

In the Next Generation Firewall statistics, select the Decryption tab to display the Decryption information. In the Decryption window, select Policy and SSL-Decryption-Policy from the drop-down menus to display the SSL-Decryption-Policy statistics.



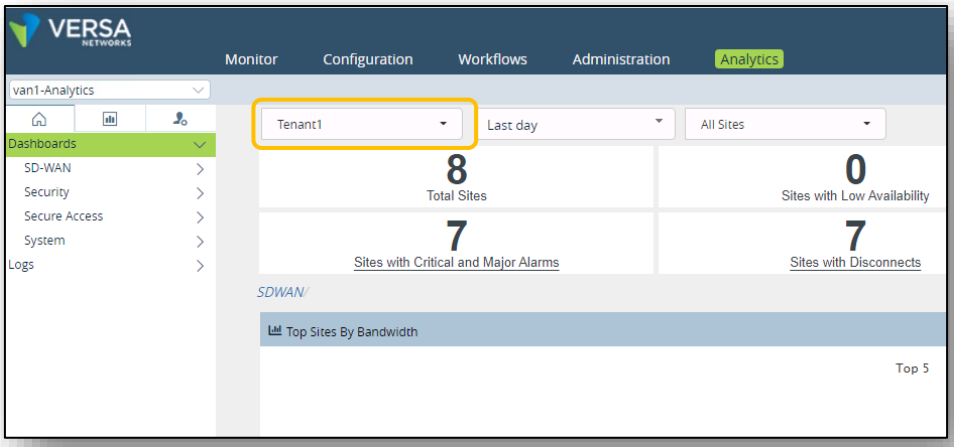
You should see non-zero counters in all of the rules The rules display how many sessions have matched each of the rules.

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



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

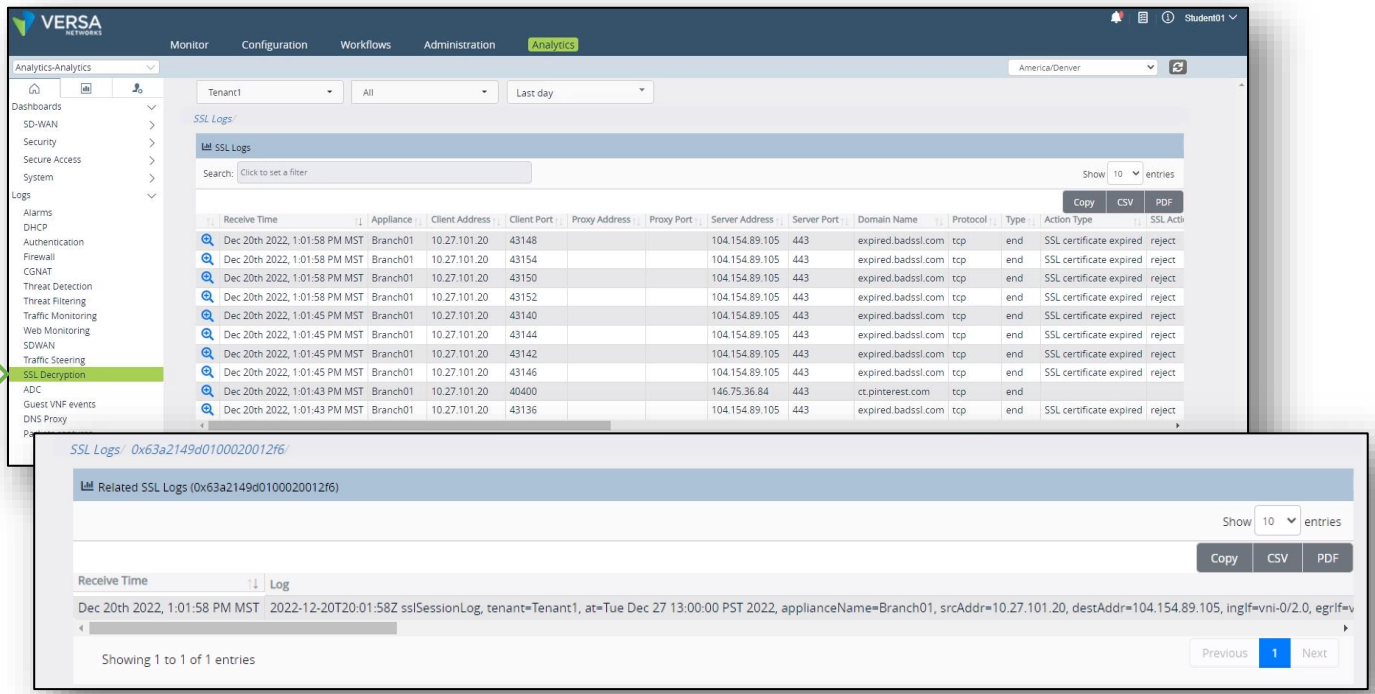
From the main Versa Director dashboard, click the Analytics tab to open Versa Analytics. Ensure that Tenant1 is selected from the top filter menu.



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

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

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



You can click the PDF button on the right to download a PDF of the log entry. This can help to make the entry more readable. You can then click the downloaded PDF to open the file in the PDF reader.

Related SSL logs (0x63a2149d0100020012f6)

Receive Time	Log
Dec 20th 2022, 1:01:58 PM MST	2022-12-20T20:01:58Z sslSessionLog, tenant=Tenant1, at=Tue Dec 27 13:00:00 PST 2022, applianceName=Branch01, srcAddr=10.27.101.20, destAddr=104.154.89.105, inglf=vni-0/2.0, egrIf=vni-0/0.0, toCountry=United States, protocolId=6, fromZone=Intf-Tenant1-LAN-Zone, fromUser=Unknown, toZone=Intf-INET-Zone, toLatLon=38.0,-97.0, toGeoHash=9yg00t, txBytes=945, txPkts=9, rxBytes=5240, rxPkts=10, serverAddr=104.154.89.105, serverPort=443, domainName=expired.badssl.com, certIsSelfSigned=0, publicKeyLen=2048, eventType=end, actionType=SSL certificate expired, sslAction=reject, decryptProfileName=SSL-INSPECTION, policyRuleName=Inspect-All, policyAction=no-decrypt, proxyType=forward, srcPort=43148, destPort=443, flowKey=0x63a2149d0100020012f6, clientAddr=10.27.101.20, clientPort=43148, rcvTimeSec=58, sessLenBkt=0, flowDuration=60

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 single CPE device (Branch device) for configuration and monitoring.

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

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

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

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

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

Look for these hints to help you in the labs

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

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

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

Exercise 1:

In the following lab exercises, you will:

- Create stateful firewall rules that:
- Block SSH sessions to the Hub-connected host
- Permit FTP sessions to the Hub-connected host

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

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

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

Step 2.1: Reset the lab to a base configuration

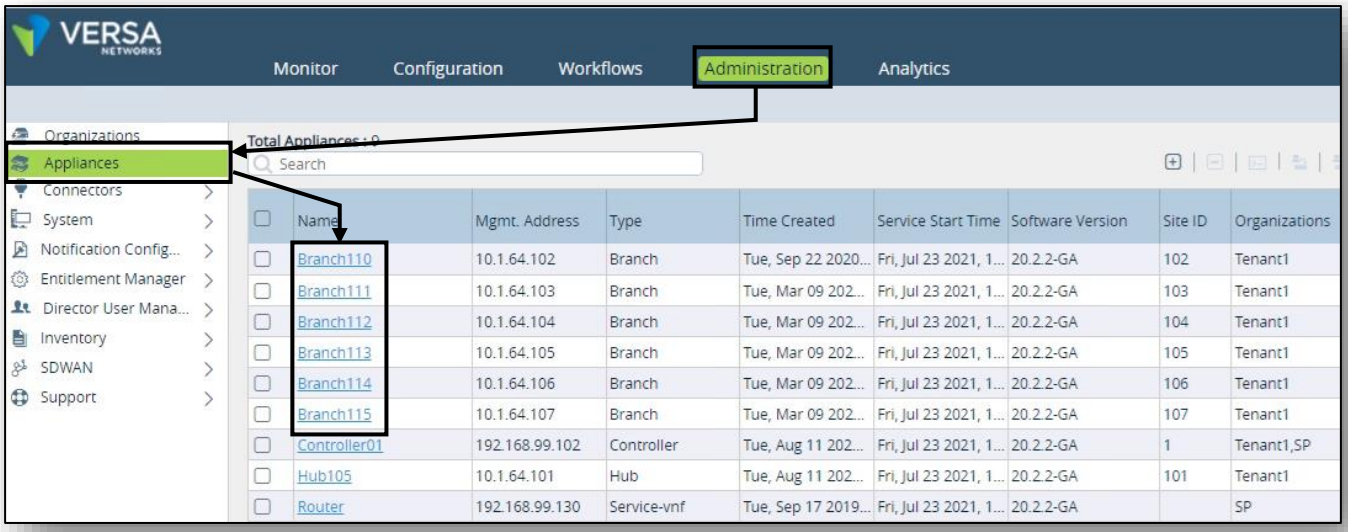
In Versa Director, navigate to the *Workflows > Devices > Devices* hierarchy and open the workflow to your branch device. In the Basic tab, ensure that the device is assigned to the DG-SFW device group. If you need to change the device group assigned to your branch device, be sure to click Redeploy to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

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

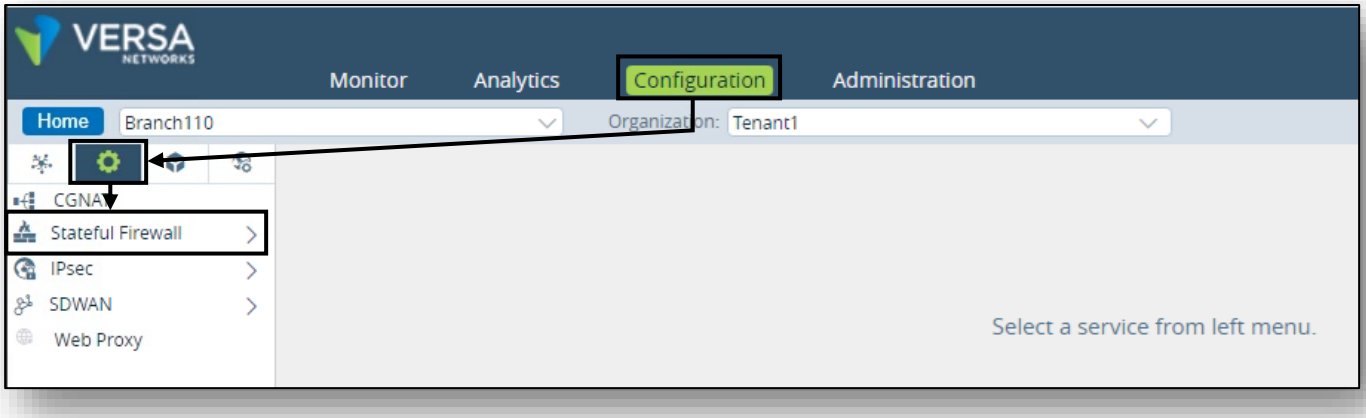
Exercise 2:

Step 2.1:

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



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



In the following lab steps you will:

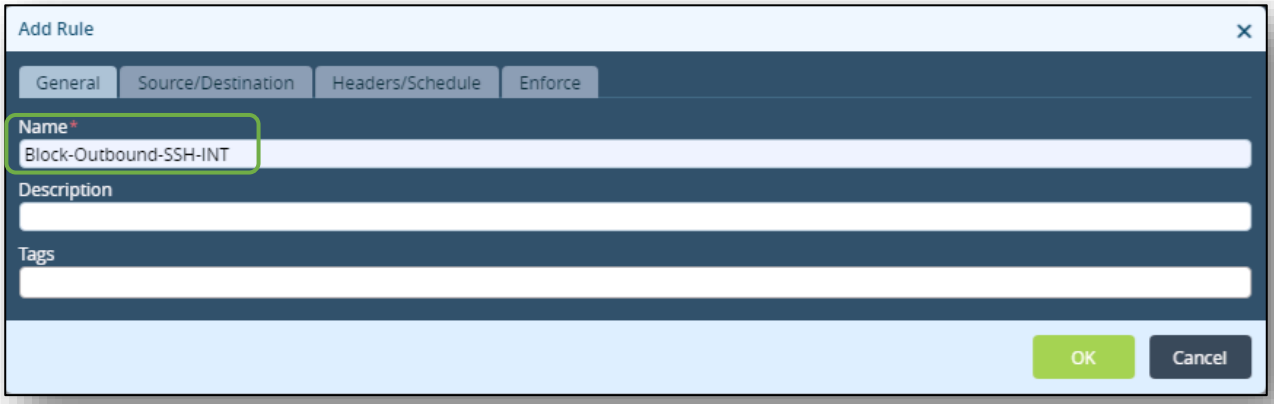
- Create 5 Stateful Firewall rules in Appliance Context mode
- Verify that the stateful firewall rules are applied

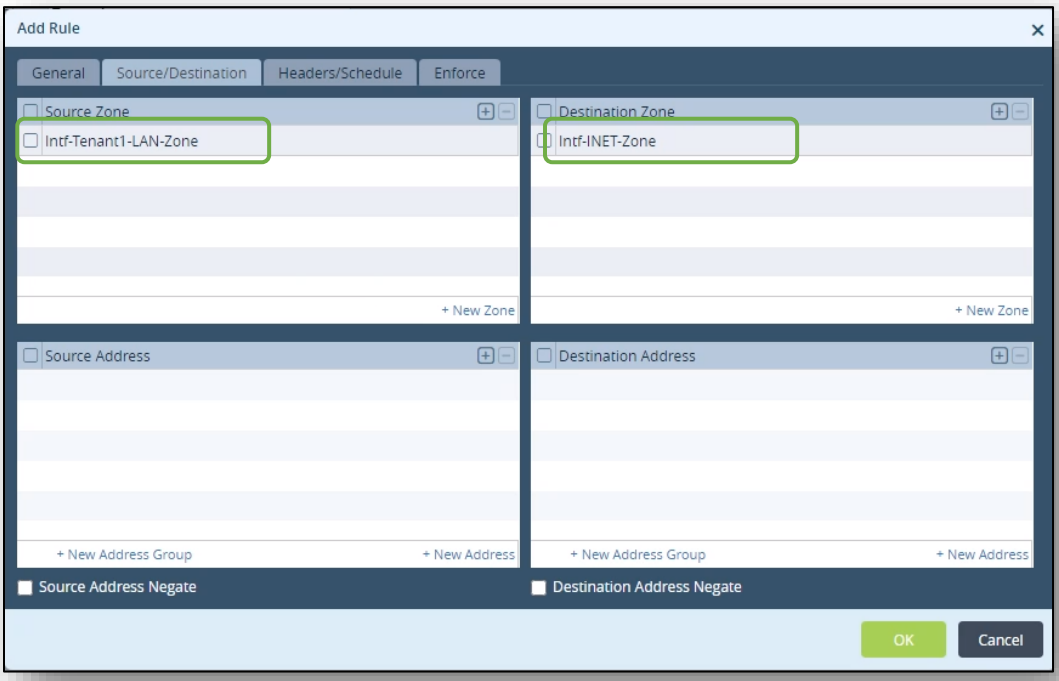
Expand the Stateful Firewall menu option in your device configuration and select the Security menu option to open the Stateful Firewall Security policy dashboard.

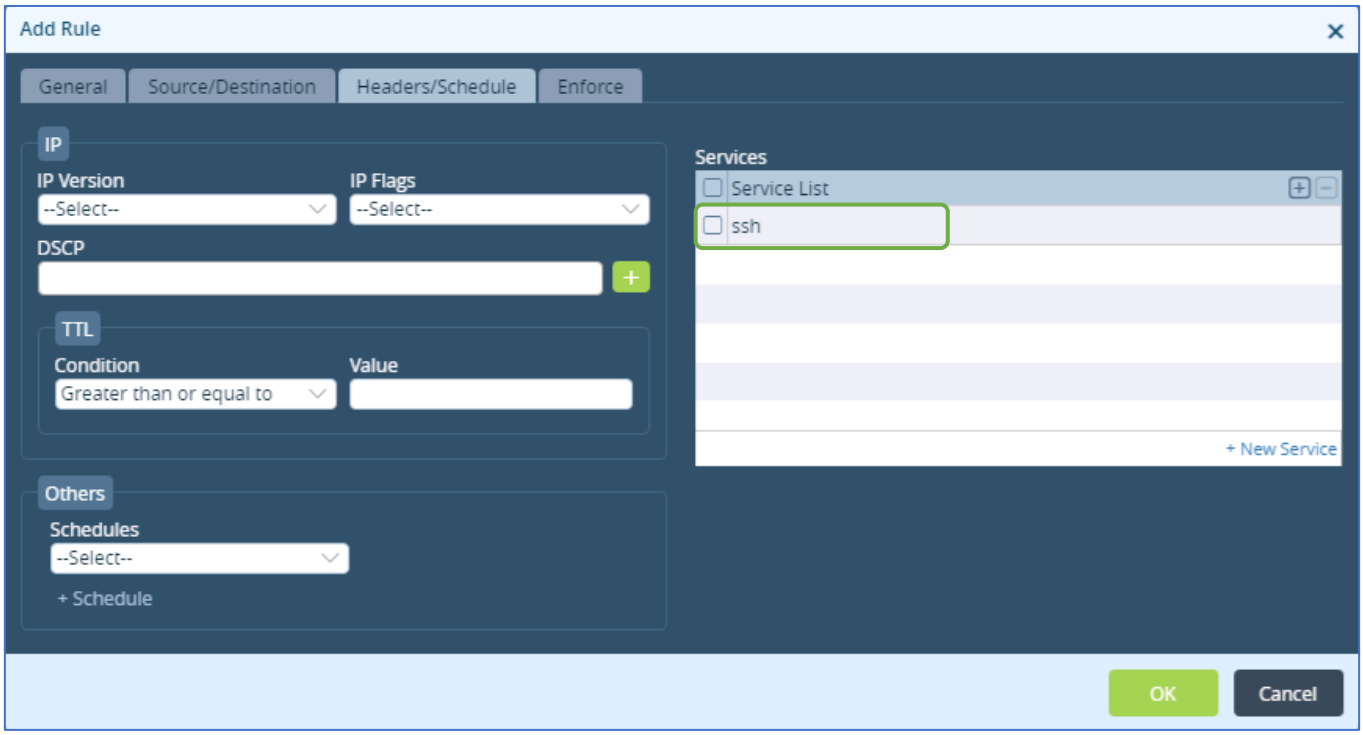
Click the + button to add a new security rule that matches the following example:

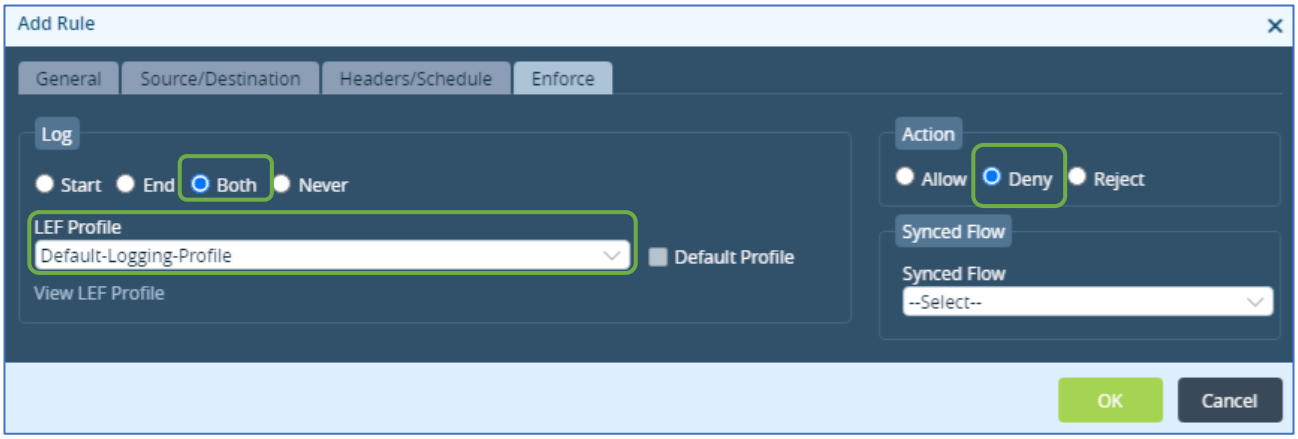
Rule 1:

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



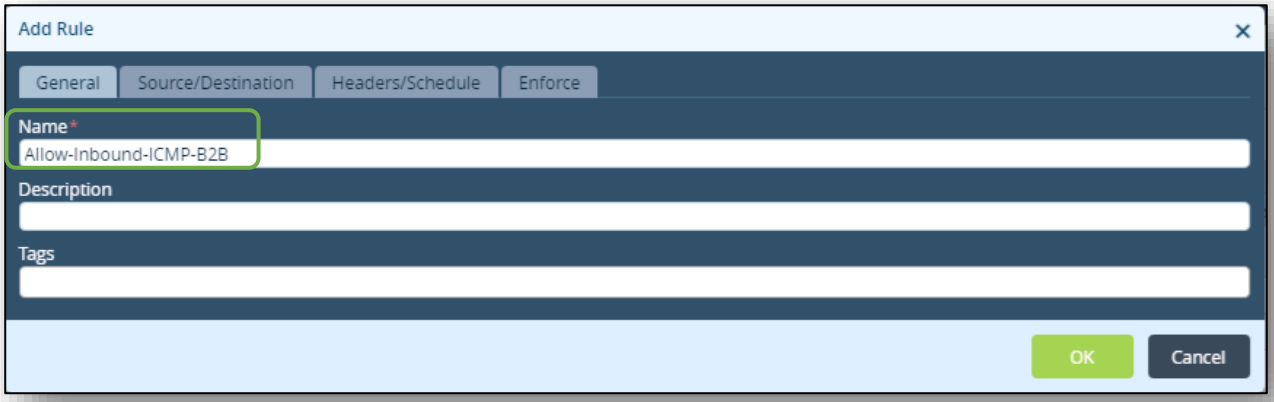


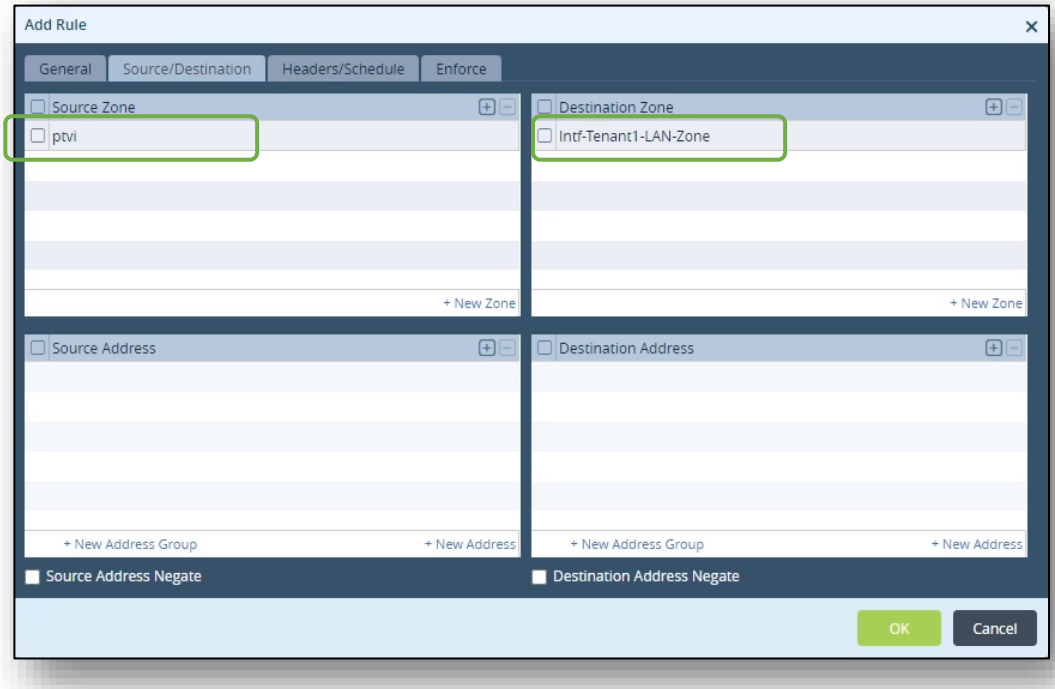


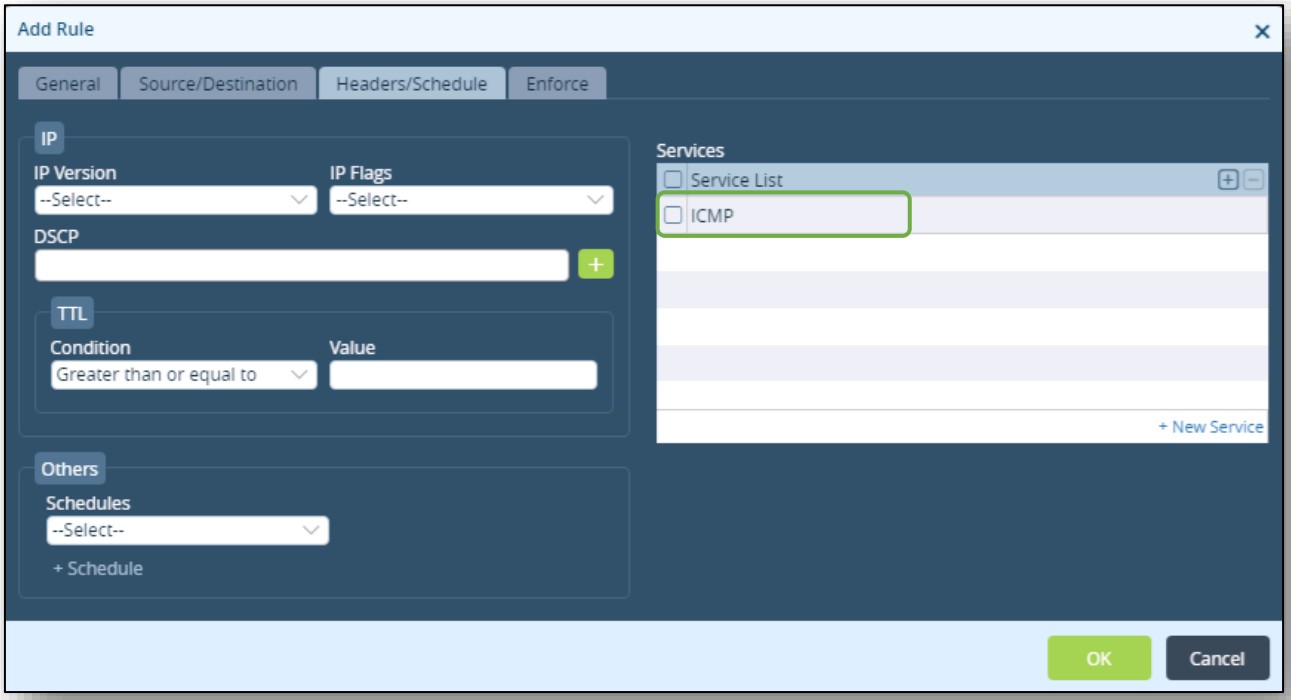


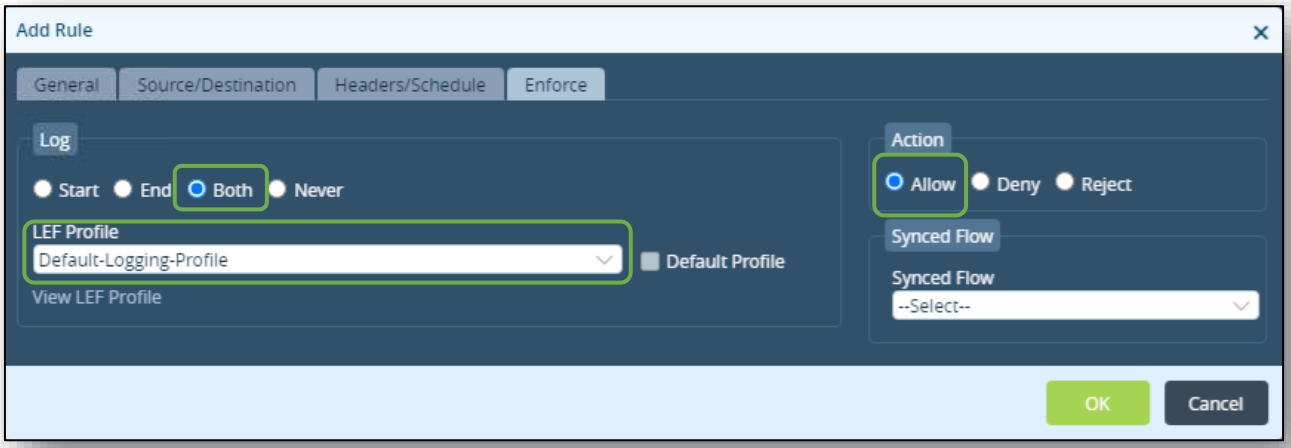
Rule 2

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.



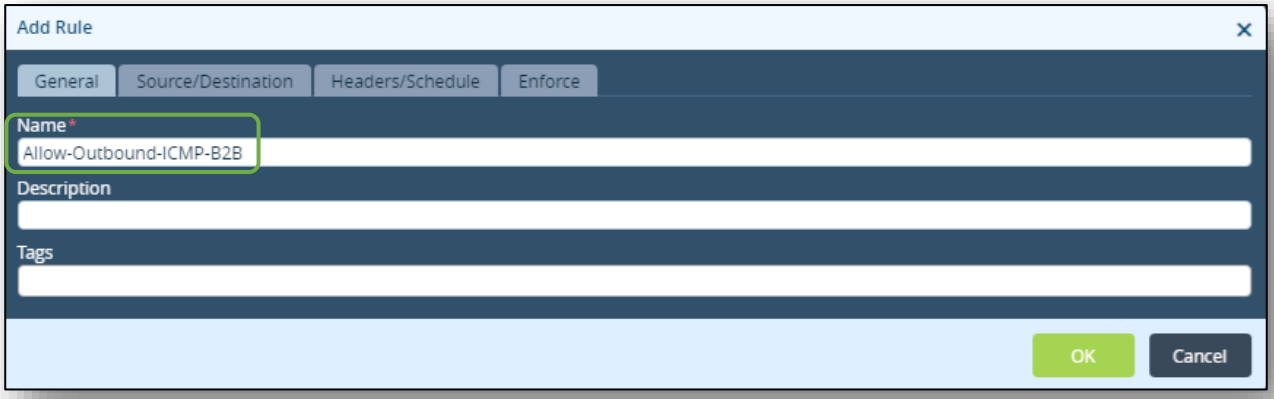


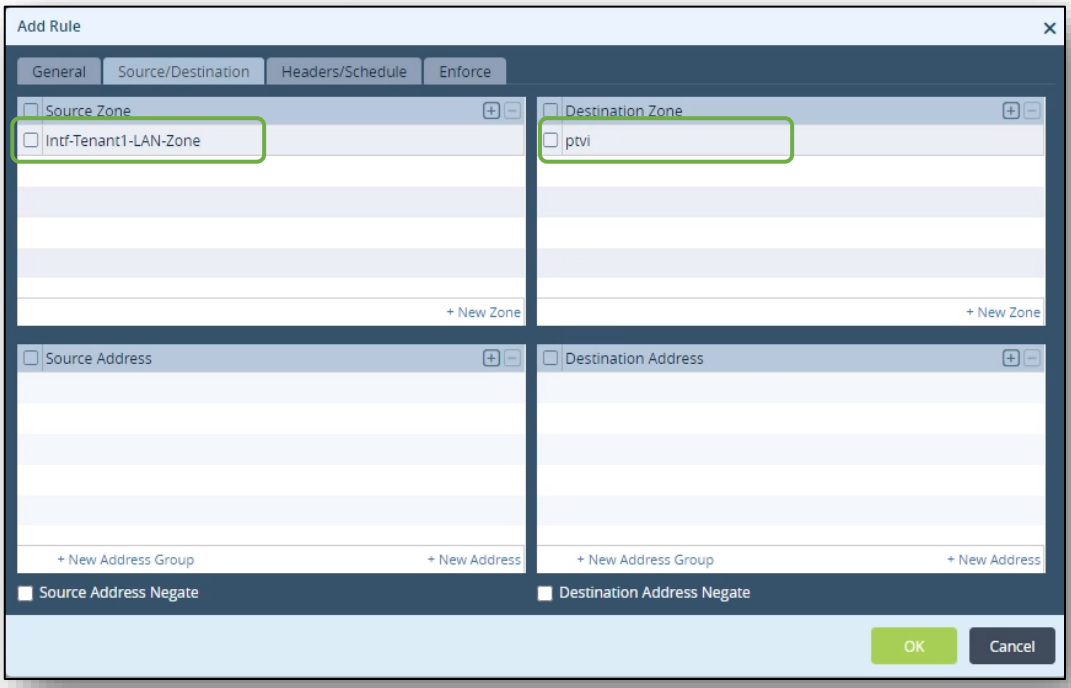


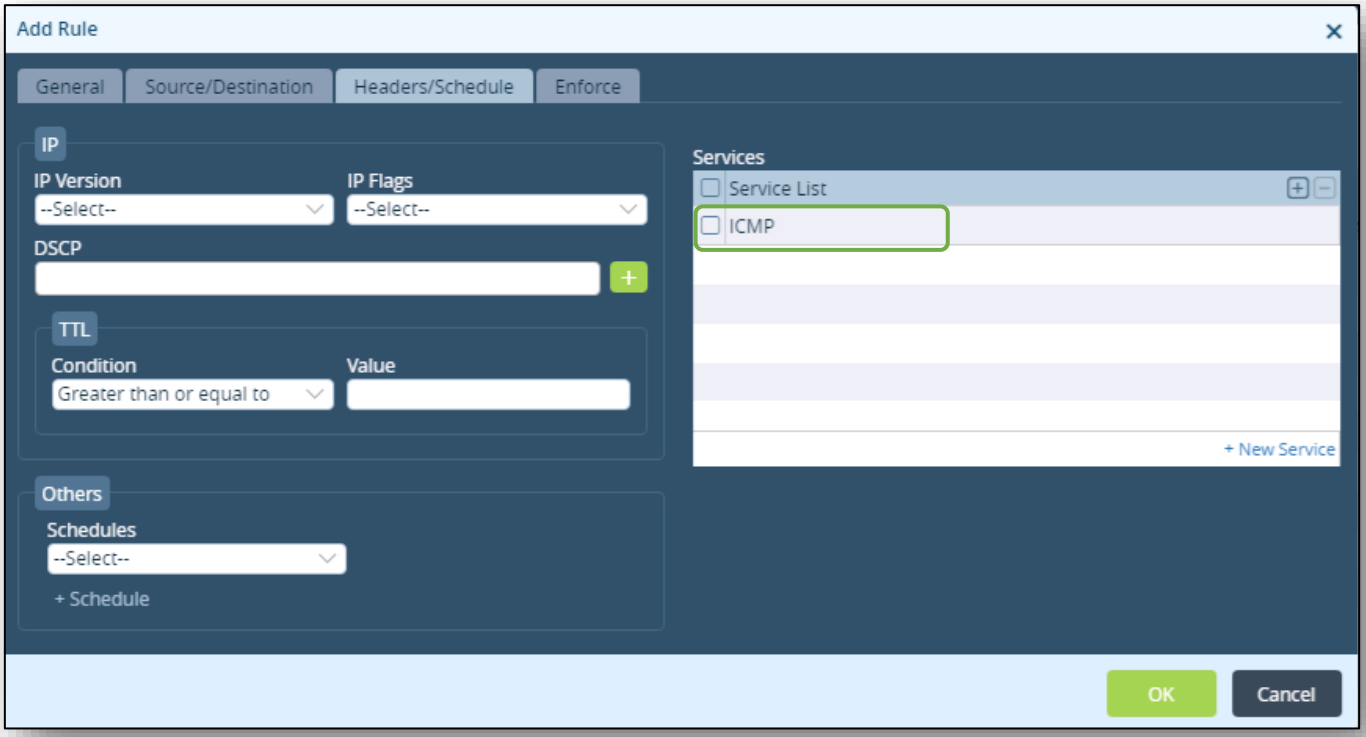


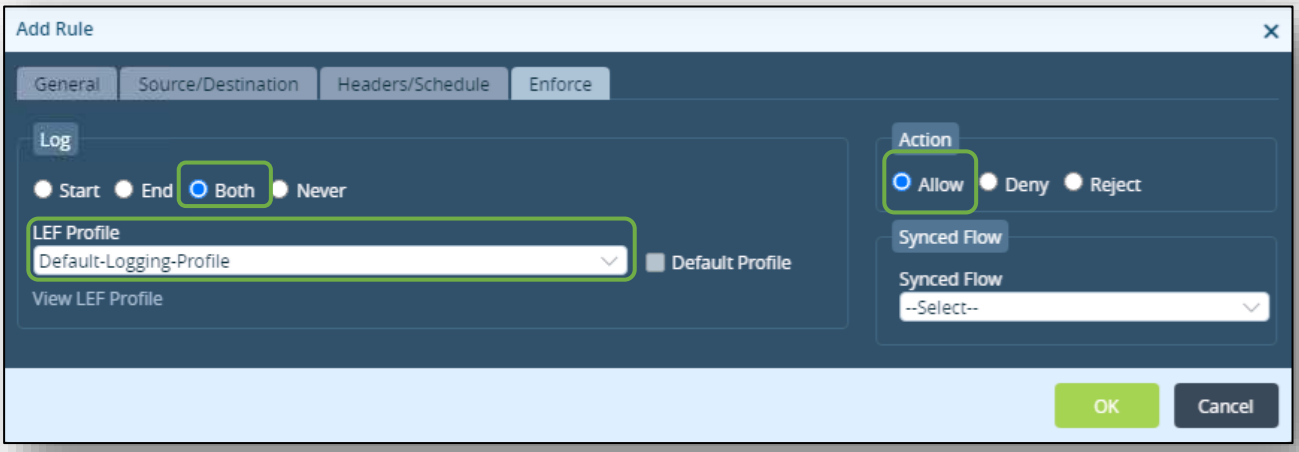
Rule 3

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.



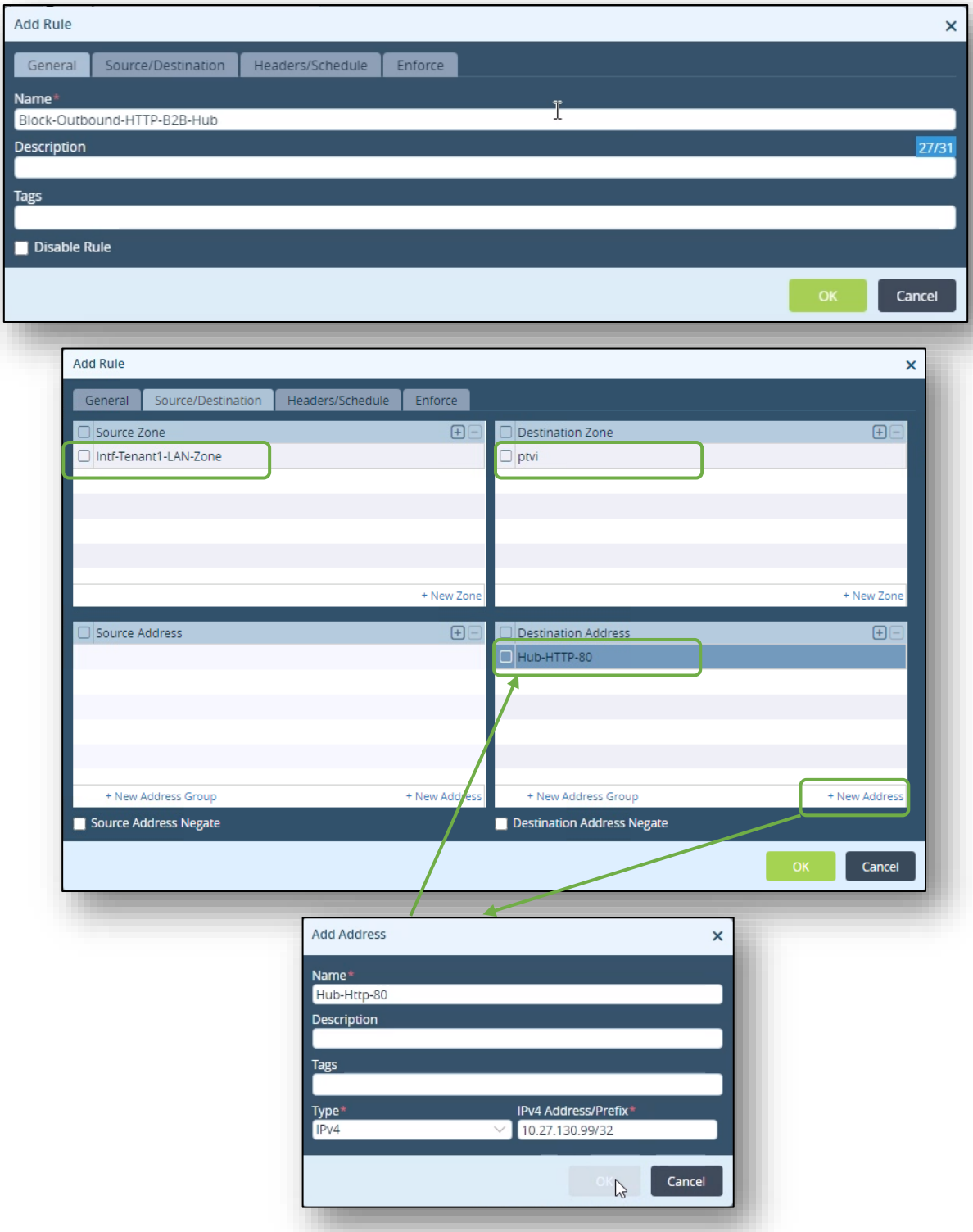


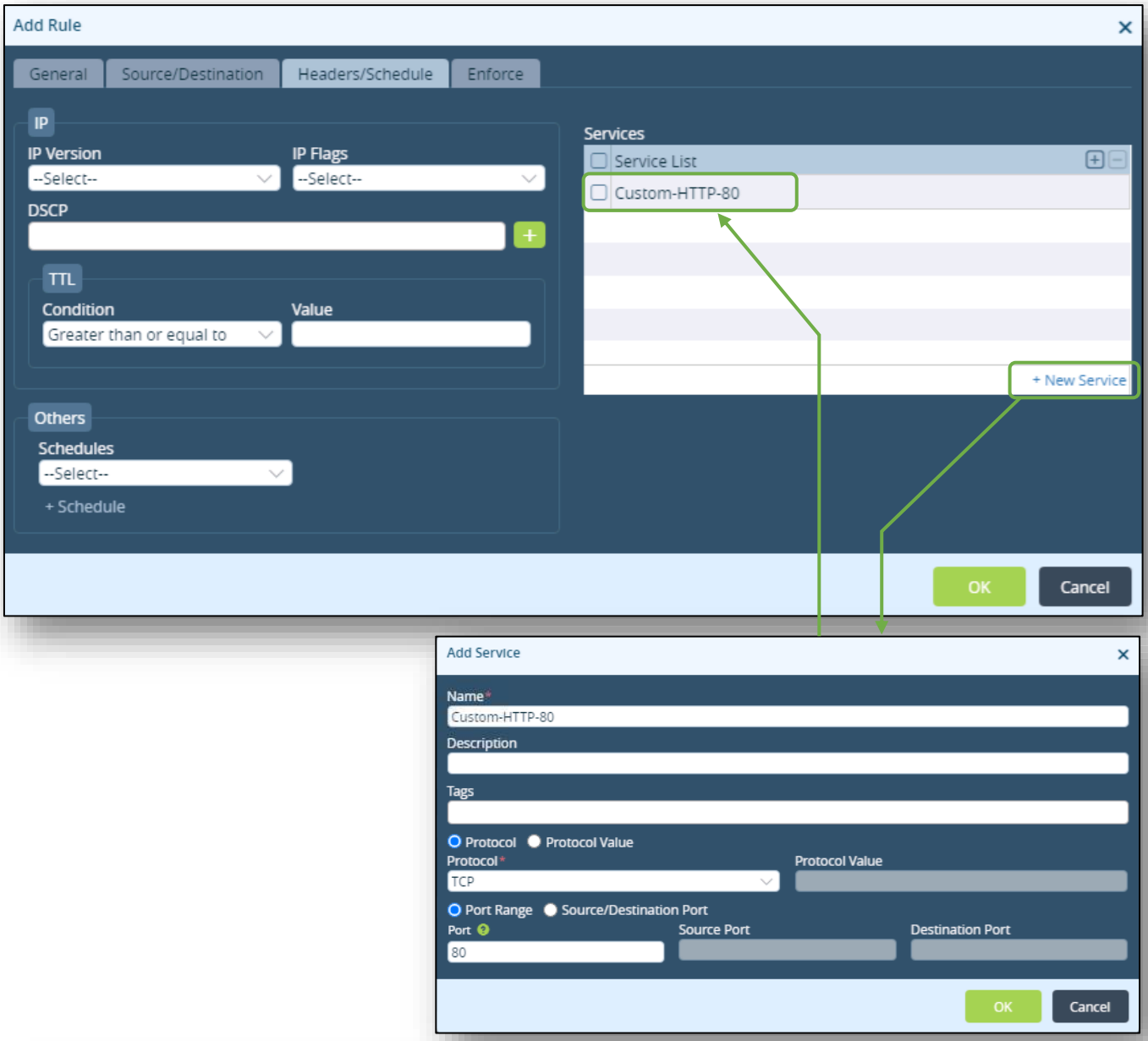


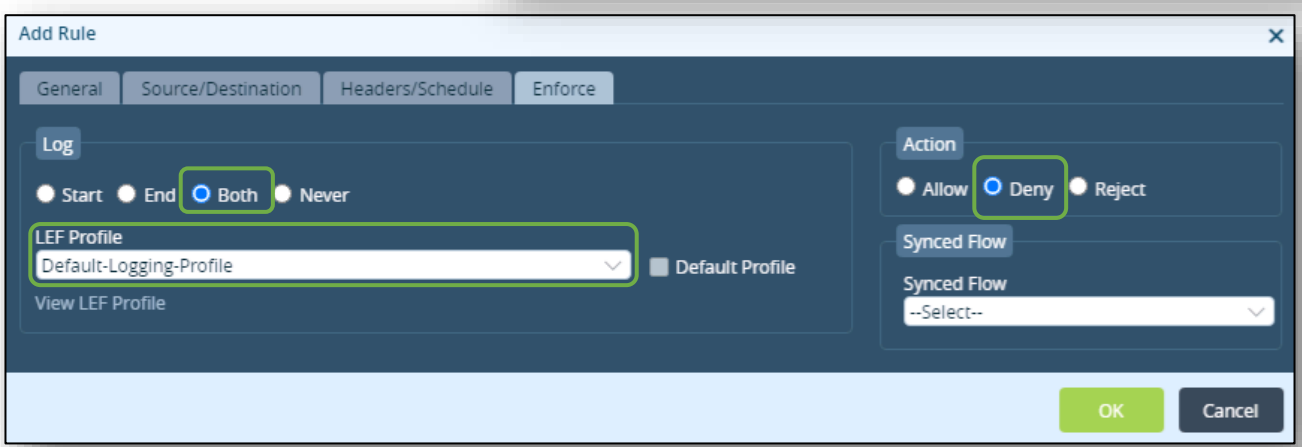


Rule 4

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.

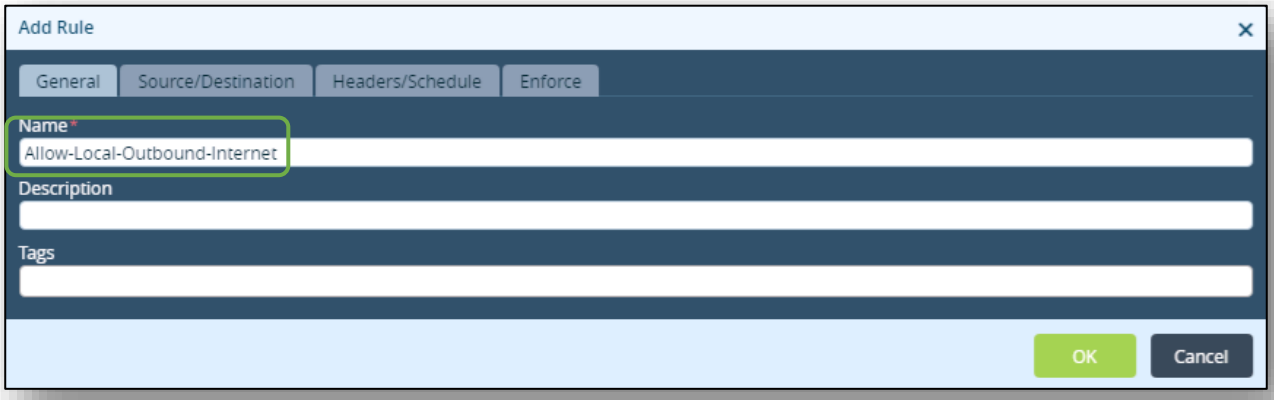


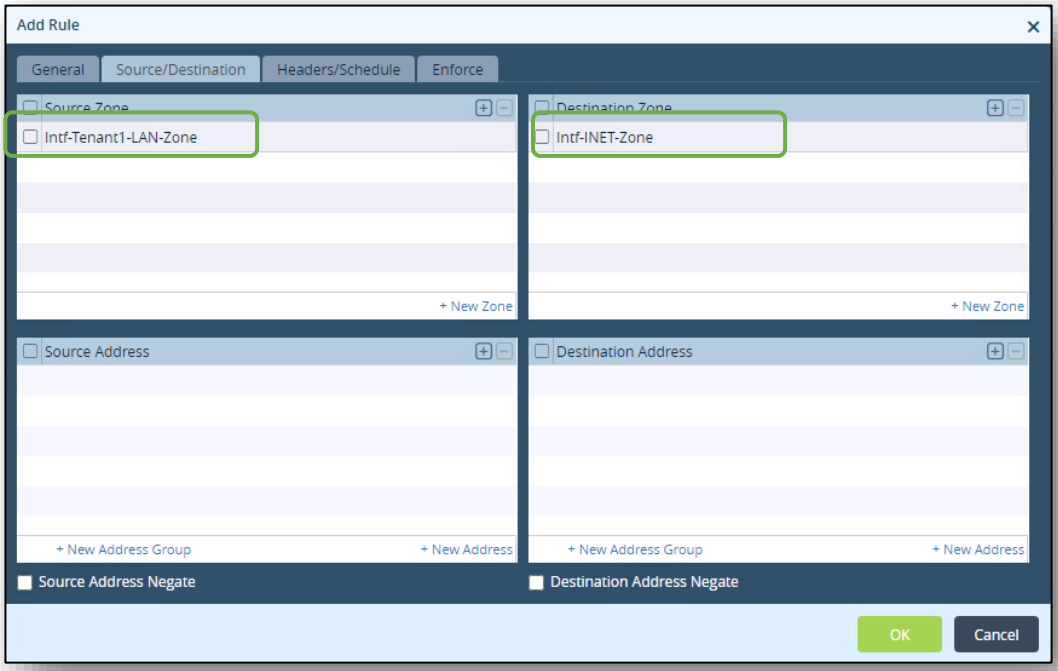


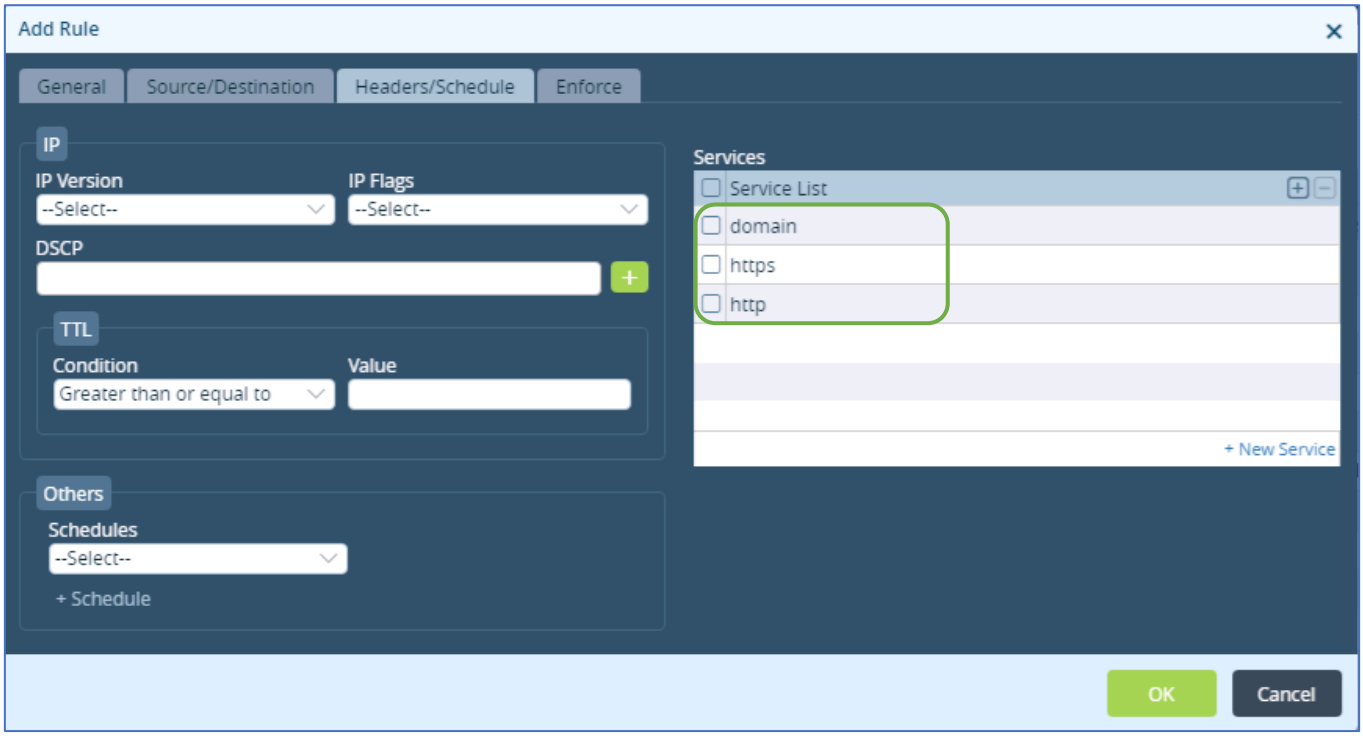


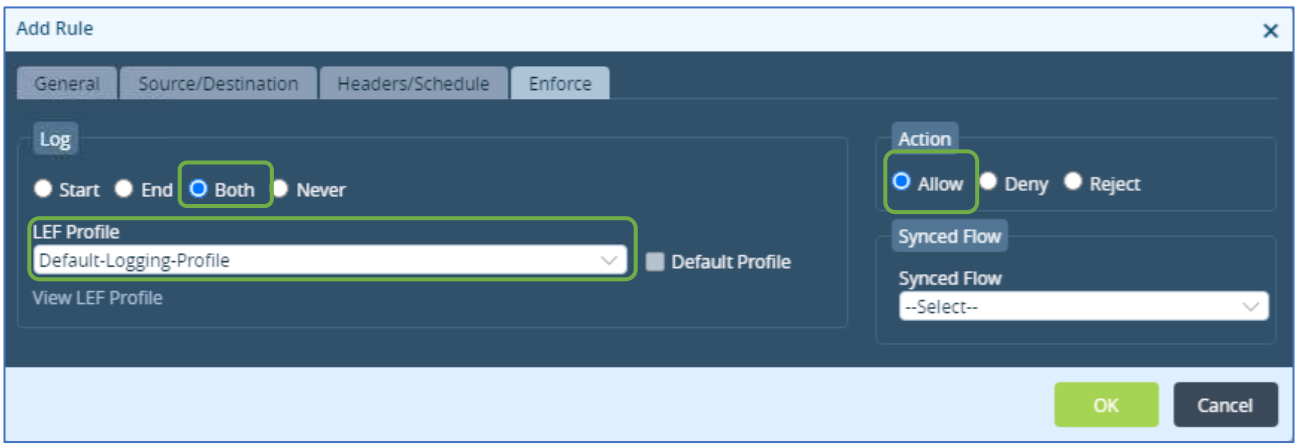
Rule 5

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









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

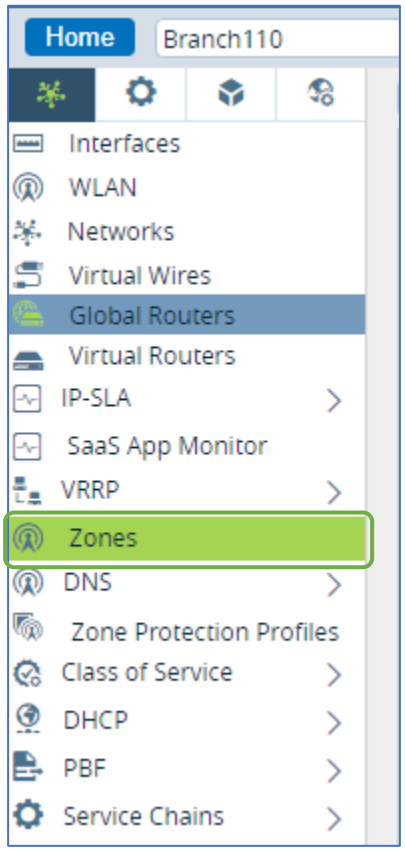
- Block-Outbond-SSH-INT
- Allow-Inbound-ICMP-B2B
- Allow-Outbound-ICMP-B2B
- Block-Outbound-HTTP-B2B
- Allow-Local-Outbound-Internet
- Allow_From_Trust
- Allow_From_SDWAN

Exercise 2: Explore Network Zones

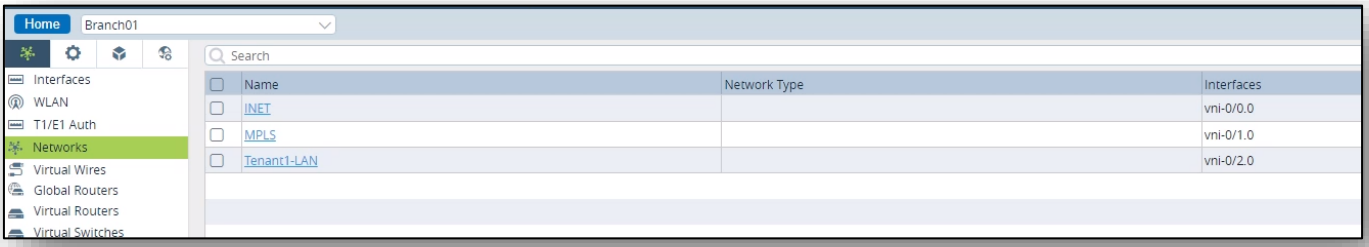
In the device configuration, navigate to the *Networking > Zones* hierarchy of your branch device.

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

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

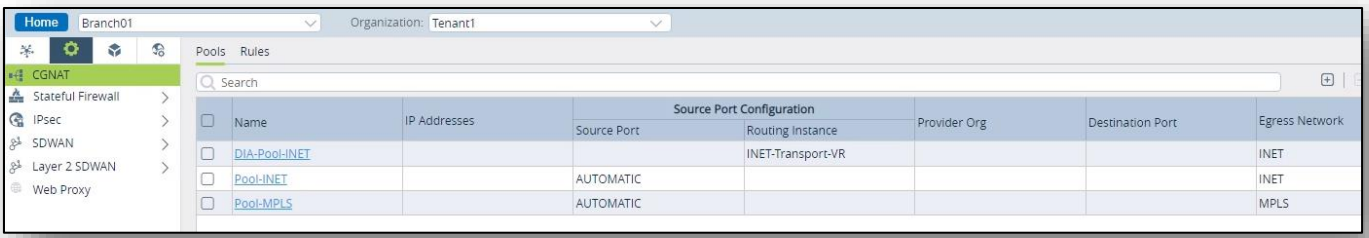


The Intf-INET-Zone contains the INET network. The INET network is associated with the INET transport link (in this example vni-0/1.0). You can view the Network-to-Interface mapping by selecting the Networks configuration section.



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

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



A DIA NAT pool was automatically created by the system. To view the NAT pool parameters, click the pool name.

The pool defines how the NAT rules will be applied, which includes the NAT translation type. The DIA-Pool-INET pool performs Interface NAT on the INET egress network. The port translation is set to source port translation.

The CGNAT Rules define when to perform the NAT operation and identify which pool to use for the NAT process.

Exercise 5: Test the Security Rules

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

On your remote desktop, open the MTPuTTY application. Use the MTPuTTY application to open an SSH session to the test PC associated with your branch (e.g. BR-110-PC, BR-111-PC, etc.) Use the username *student* and password *versa123* if prompted.

From the shell prompt on the testing PC, run the following tests for each security rule.

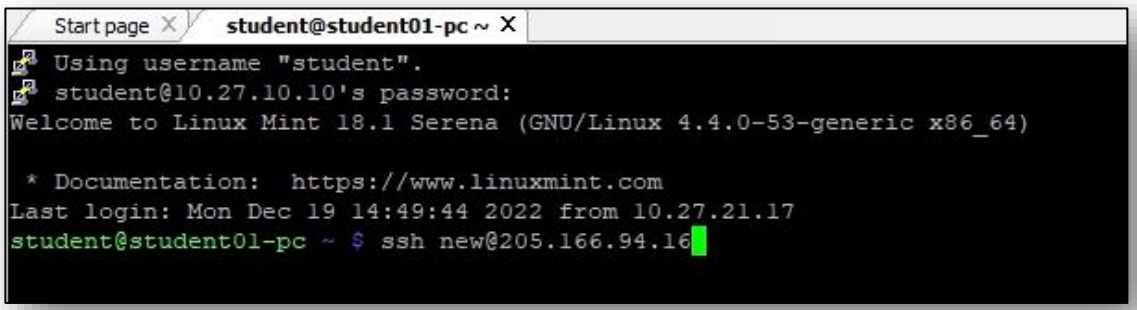
> **Note**: It can take several seconds for the counters to update during testing. To refresh the table counters, navigate to a different tab in the dashboard, then return to the tab where you are viewing the counters.

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

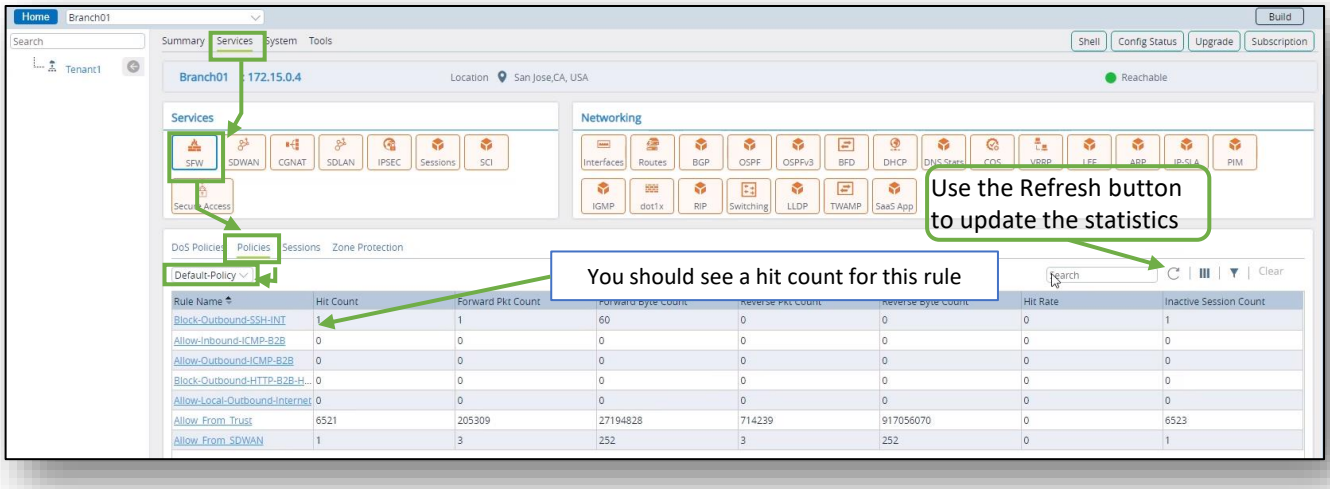
Rule 1 Test

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

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



Monitor tab verification: From Versa Director, navigate to *Monitor > Tenant1 > Devices* and select your branch from the devices table. From your device Monitor dashboard, select *Services > SFW > Policies* and select the Default-Policy. The list of rules you created should be listed.



Rule 2 and Rule 3 Test

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

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

On your remote desktop, open the MTPuTTY application. Use the MTPuTTY application to open an SSH session to the test PC associated with your branch (e.g. BR-110-PC, BR-111-PC, etc.) Use the username *student* and password *versa123* if prompted. From the shell prompt on the testing PC, run the following command: **ping 10.27.130.99 –c 5** to initiate ICMP traffic towards the hub LAN network. The command should be successful.

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

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

Open an SSH session to the Hub Host device that is connected to the Hub105 branch. Login with the username *student* and the password *versa123*. From the terminal prompt on the host120 device (the host connected to the hub site) issue the ping command below to send ICMP packets to your testing PC:

Branch	Command
01	Ping 10.27.101.20 –c 5
02	Ping 10.27.102.20 –c 5
03	Ping 10.27.103.20 –c 5
04	Ping 10.27.104.20 –c 5
05	Ping 10.27.105.20 –c 5
24	Ping 10.27.124.20 –c 5

The ping command should succeed.

Next you will verify the rule success using Versa Analytics.

Return to the Versa Director user interface. Click the Home button next to your branch name to return to the main Versa Director user interface.

From the main Versa Director UI, click on the Analytics tab to open the Versa Analytics dashboards. Ensure that the Tenant1 organization is in the organization filter at the top of the dashboards.

From the left-side menu, select Logs > Firewall. Ensure that Tenant1 is listed as the organization in the toolbar drop-down menu. You can filter more specific log entries by selecting the branch name from the drop-down menu as well.

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

Rule 4 Test

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

On the remote landing station, click the Remote Desktop icon on the desktop. Open a remote desktop session to your test host according to the table below:

Remote Desktop IP addresses		
Branch01: 10.27.10.10	Branch09: 10.27.10.18	Branch17: 10.27.10.26
Branch02: 10.27.10.11	Branch10: 10.27.10.19	Branch18: 10.27.10.27
Branch03: 10.27.10.12	Branch11: 10.27.10.20	Branch19: 10.27.10.28
Branch04: 10.27.10.13	Branch12: 10.27.10.21	Branch20: 10.27.10.29
Branch05: 10.27.10.14	Branch13: 10.27.10.22	Branch21: 10.27.10.30
Branch06: 10.27.10.15	Branch14: 10.27.10.23	Branch22: 10.27.10.31
Branch07: 10.27.10.16	Branch15: 10.27.10.24	Branch23: 10.27.10.32
Branch08: 10.27.10.17	Branch16: 10.27.10.25	Branch24: 10.27.10.33

Use the username *student* and password *versa123* if prompted. From the test host open the Chromium web Browser to open the browser window and enter the address http://10.27.130.99. The web page will not open because there is not a web server at that address. However, the policy in the VOS device should still intercept the attempt and block it.

Monitor tab verification

From Versa Director, navigate to the *Monitor > Tenant1 > Devices* and select your branch from the device list. From your device monitor dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created in previous steps should be listed. Check the counters for the Block-Outbound-HTTP-B2B-105-105 rule. The counters should increment each time you attempt to establish the HTTP session.

Analytics Tab Verification

Click the Home icon next to the branch name to return to the main Versa Director UI.

Click on the Analytics tab to open the Versa Analytics dashboards. Ensure that the Tenant1 organization is selected in the organization filter at the top of the dashboard. From the left-side menu, select Logs > Firewall. You can filter more specific log entries by selecting the branch name from the dropdown menu as well.

Enter a filter based on the rule and with the value Block-Outbound-HTTP-B2B-105-105 in the filter window. Verify that the action for the rule matches is Deny.

Rule 5 Test

Rule Name: Allow-Local-Outbound-Internet

On the remote landing station, click the Remote Desktop icon on the desktop. Open a remote desktop session to your test host.

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

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

Monitor Tab Verification

From Versa Director, navigate to the *Monitor > Tenant1 > Devices* dashboard and select your device from the devices list. From your device monitor dashboard, select *Services > SFW > Policies* and select the *Default-Policy*. The list of rules you created in previous steps should be listed.

Check the counters for the Allow-Local-Outbound-Internet rule. The counters should when you access the web site.

Versa Analytics Verification

Click the Home icon next to the branch name to return to the main Versa Director UI.

Click on the Analytics tab to open the Versa Analytics dashboards. Ensure that Tenant1 is listed as the organization in the toolbar drop-down menu. From the left-side menu, select *Logs > Firewall*. You can filter more specific log entries by selecting your branch name from the drop-down menu.

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

Question: Which rule allows the DNS resolution?

_____

Answer: DNS resolution allowed by rule Allow-Local-Outbound-Internet because the rule allows the domain service, which is mapped to port 53.

Question: Will port 23 traffic be allowed by the configured rule set?

_____

Answer: No, port 23 will not be allowed.

Question: Can address objects be used under either the source or destination address match fields?

_____

Answer: Yes, an address object can be used by any match field that can match on addresses.

Question: What is the significance of selecting the *both* option under the enforce logging action?

_____

Answer: Selecting Both will log the start and end of the session. Although this option can be useful for troubleshooting, it can also create large amounts of log information and should be used with caution.

Question: What command should be used to check the policy hits using the CLI?

_____

Answer: The CLI command to view the policy rule hits is **`show orgs org-services [tenant-name] security access-policies rules`**.

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.

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

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

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

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

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

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

Look for these hints to help you in the labs

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

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

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

Exercise 2:

In the following lab exercises, you will:

- Create stateful firewall rules that:
- Block SSH sessions to the Hub-connected host
- Permit FTP sessions to the Hub-connected host

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

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

Step 2.1: Reset the lab to a base configuration

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

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

Exercise 2:

2.1 Open the Device Template for Configuration

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

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

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

2.2 Create DoS Profiles

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

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

In the DoS Profile dialog, enter the following parameters:

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

Click OK to create the DoS profile when finished.

2.3 Create a DoS Policy

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

- Restrict ICMP based flood attacks to the hub server 10.27.130.99 using the DoS Profile parameters
- Restrict TCP-SYN based attacks over port 80 to the hub server 10.27.130.99 using the DoS Profile created

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

2.4 Create Rules in the DoS Policy

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

Rule 1	
Rule Name:	DoS-Classified-Rule-Hub
Source/Destination Tab:	Source Zone:intf-Tenant1-LAN-Zone Destination Zone: ptvi Add a new destination address: Address Name: HUB-HTTP-80 Address: IPv4 10.27.130.99/32
Headers/Schedule Tab:	Add services http and ICMP
Enforce Tab:	Action: Protect Classified Profile: Classified-DoS-Profile Logging: Default-Logging-Profile

Click *OK* to finish creating the policy.

Question: What are the 2 types of profiles available in the DoS Module?

_____

Answer: Classified Profile and Aggregate Profile

Question: What are the actions available in the DoS rules?

_____

Answer: The actions for DoS rules are Allow, Deny, and Protect. To enable and enforce the DoS profile parameters you must select the Protect option.

Question: Can DoS policy protect against TCP based attacks like RST, FIN, ACK, or a combination of these attacks?

_____

Answer: No. The DoS mosule can only protect against TCP-SYN based attacks and not other variants of TCP based attacks.

1.6 Verify the DoS Policy Protection

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

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

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

Verification Step 2	
Name:	TCP SYN Flood
Script to run:	Return to the open session on the testing host. From the command line on the testing host, press CTRL + C to stop the flood attack. run the ./VASEC/TCP-SYN-ATTACK-DDOS.sh command. Use the password ***versa123*** if prompted. This will generate a TCP SYN flood to port 80 of the hub host 10.27.130.99.
Monitor Tab Verification:	Navigate to *Monitor > Tenant1 > Devices* and select your branch from the table. In your branch device Monitor window navigate to *Services > NGFW > DoS Policies*. Select *DoS-Policy* from the drop-down. Verify that the TCP-SYN Drop Count counter is incrementing.
Analytics Verification:	Return to the main Versa Director dashboard (exit the device-context mode). Navigate to the *Analytics > Logs* dashboard. Ensure that the Tenant1 Organization is selected in the top filter drop-down. Under Logs, select *Threat Detection* and open the DDOS tab in the table. The TCP SYN flood logs with action Drop should be displayed.

Question: What are the threat types and attack names displayed in Versa Analytics for the traffic simulations?

_____

Answer: Threat type is displayed as Flood. The ICMP attack name is ICMP and the TCP attack name is TCP-SYN.

Question: What will happen if the rate exceeds the “Maximum Rate Packets/sec” value?

_____

Answer: All packets exceeding the maximal rate will be dropped for the defined time period.

Question: What are some differences between Zone Protection and DoS Protection?

_____

Answer: Zone Protection is applied at the interface level before the session processing happens, and is applied to the aggregate traffic for all protocols. DoS protection is applied after the sessions are created and with more granular options to filter and apply protection for different types of traffic. Both profiles help to prevent flood attacks and exhaustion of resources.

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

Application Filtering

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

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

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

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

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

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

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

Look for these hints to help you in the labs

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

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

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

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

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

Application Filtering and Control

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

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

Lab Objective

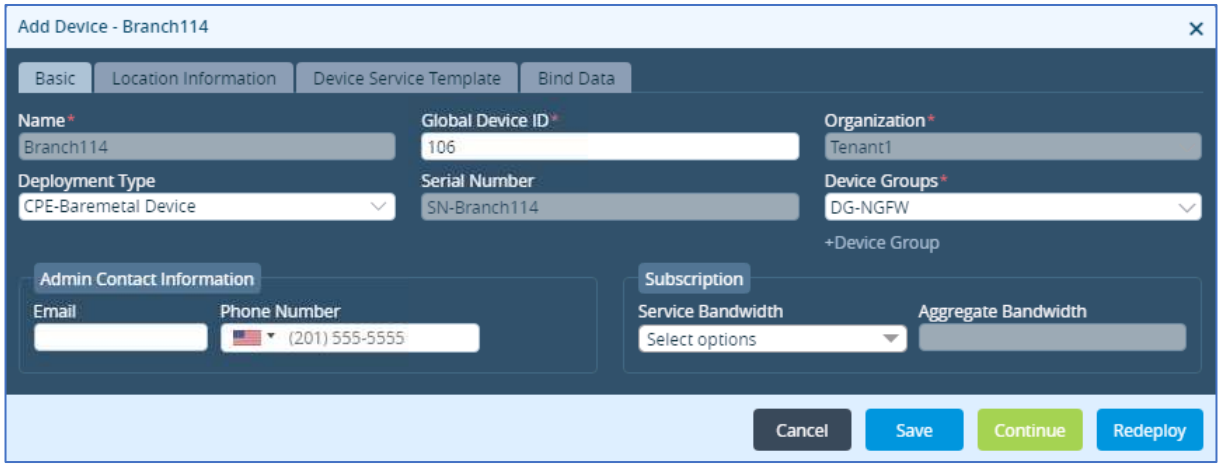
Customer Tenant1 is planning to enable security services and has the following requirements to have more control on the applications that the users are using on the network. The following requirements are to be met:

- Block ICMP traffic destined to 10.27.130.99 in the hub site using the applications field in security access rules.
- Block Bit-Torrent traffic for all users at the local Branches
- Create a customer application groups that includes Youtube and Netflix applications. Use the application group to create security access rules that block Youtube and Netflix.
- Create a custom application definition to identify, and categorize Twitter traffic. Use the application definition in an access rule to block the traffic.
- Allow other the Internet traffic.

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

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

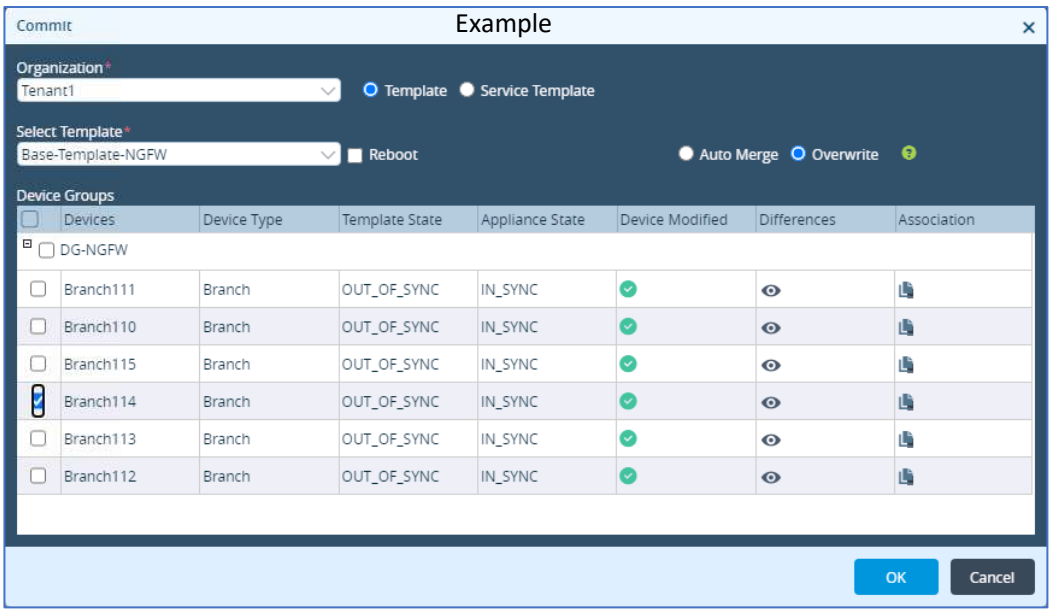
In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select the *Tenant1* organization, the template *Template-NGFW*, and locate your device in the list.

Select your device in the device list and click *OK* to apply the base configuration to your 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 2.1: Configure a rule to block ICMP traffic

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

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

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

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

ICMP Access Rule	
Name:	Block-ICMP-Hub
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: ptvi Destination Address: Click + New Address and add the following address: Name: Hub Type: IPv4 IPv4 Address/Prefix: 10.27.130.99/32
Application/URL:	Application: ICMP
Enforce:	Action: Deny Log Events: Both, Default Logging Profile

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

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

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

In the remote desktop, click on the *Remote Desktop Connection* icon on the desktop to open the Remote Desktop application. Open a remote desktop session to the testing host assigned to your branch. The username for the remote desktop session is ***student*** and password is ***versa123***.

Remote Desktop IP addresses		
Branch01: 10.27.10.10	Branch09: 10.27.10.18	Branch17: 10.27.10.26
Branch02: 10.27.10.11	Branch10: 10.27.10.19	Branch18: 10.27.10.27
Branch03: 10.27.10.12	Branch11: 10.27.10.20	Branch19: 10.27.10.28
Branch04: 10.27.10.13	Branch12: 10.27.10.21	Branch20: 10.27.10.29
Branch05: 10.27.10.14	Branch13: 10.27.10.22	Branch21: 10.27.10.30
Branch06: 10.27.10.15	Branch14: 10.27.10.23	Branch22: 10.27.10.31
Branch07: 10.27.10.16	Branch15: 10.27.10.24	Branch23: 10.27.10.32
Branch08: 10.27.10.17	Branch16: 10.27.10.25	Branch24: 10.27.10.33

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

From the terminal window on the testing station, issue the command **`ping -c 3 10.27.130.99`**. This will send 3 ICMP packets to the host connected to the remote hub. The ICMP messages should fail.

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

Return to the Versa Director user interface. In Versa Director, navigate to the *Monitor* tab for your device. Click the *Services* tab and navigate to *Services > NGFW > Policies*. This should open the *Monitor* window for your branch appliance. Examine the statistics for the *Block-ICMP-105-105-Hub* policy. You should see hit counts. If the hit counts reads 0, return to the previous steps and verify the configuration of the access rule.

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

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

In the *Firewall Logs* dashboard, add a filter that searches for the rule name *Block-ICMP-105-105-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.

Step 2.4: Configure a rule to block Bit-Torrent

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

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

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

ICMP Access Rule	
Name:	Block-Bit-Torrent
Source/Destination:	Source Zone:intf-Tenant1-LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Applications: BITTORRENT, BITTORRENT_APPLICATION, BITTORRENT_BUNDLE
Enforce:	Action: Deny Log Events: Both, Default Logging Profile

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

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

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

On the remote landing station, return to the remote desktop session to the testing host.

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

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

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

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

Step 2.7: Verify the Block-Bit-Torrent rule in Versa Analytics

Click the *Home* button next to your branch device name to exit appliance context mode. From the main Versa Director window, click the *Analytics* tab to open Versa Analytics. Navigate to *Analytics > Logs > Firewall*. Ensure that the *Tenant1* organization is selected in the organization filter at the top of the dashboard. Filter the log entries by clicking on the *Search* tab and select rule. Give the rule name as "Block-Bit-Torrent". This should display only the entries related to the Block-Bit-Torrent rule. You can identify entries from your device by checking the source address, as the source address will be from the LAN connected to your branch appliance.

Check the filter logs to see that the application "bittorrent" has the action deny, and that it is mapped to the rule "Block-Bit-Torrent".

Step 2.8: 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.

In Versa Director, navigate to *Administration > Appliances* and locate your appliance in the appliance list to enter appliance context mode. In appliance context mode, Navigate to *Objects & Connectors > Custom Objects > Application Groups*, then click the + button to create a new application group with the following parameters:

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

Click *OK* to create the application group.

Step 2.9: Configure and access rule that references the new application group

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

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

Access Rule	
Name:	Block-APP-Group-Youtube-Netflix
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Applications List: APP-Group-Youtube-Netflix
Enforce:	Action: Deny Log Events: Both, Default-Logging-Profile

Click *OK* to create the new access rule, then move the rule to the 3rd position in the rule list.

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

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

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

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

Step 2.11: Verify access rule statistics in Versa Director

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

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

Step 2.12: Verify access rule logs in Versa Analytics

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

In the firewall logs field, click the *Search* field and enter a filter to match the rule name *Block-APP-Group-Youtube-Netflix*. This will display only log entries related to the selected rule. You should see entries related to the application YouTube and the application Netflix with an action of deny. Find entries that have a source address of your local LAN to verify that your appliance is sending logs to Versa Analytics.

Step 2.13: 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.

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

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

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

Clock *OK* to create the custom application definition.

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

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

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

Custom Application Security Rule	
Name:	Block-Custom-Twitter
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: Intf-INET-Zone
Applications/URL:	Application: Custom-Twitter-APP
Enforce:	Action: Deny Log Events: Both, Default Logging Profile

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

Step 2.15: Verify that the access rule blocks Twitter traffic

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

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

Step 2.16: Verify the access rule statistics in Versa Director

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

Step 2.17: Verify the access rule logs in Versa Analytics

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

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

Step 2.18: Finish the lab and exit the lab environment

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

Close the MTPuTTY application.

Log out of Versa Director.

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

URL Filtering

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

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

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

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

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

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

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

Look for these hints to help you in the labs

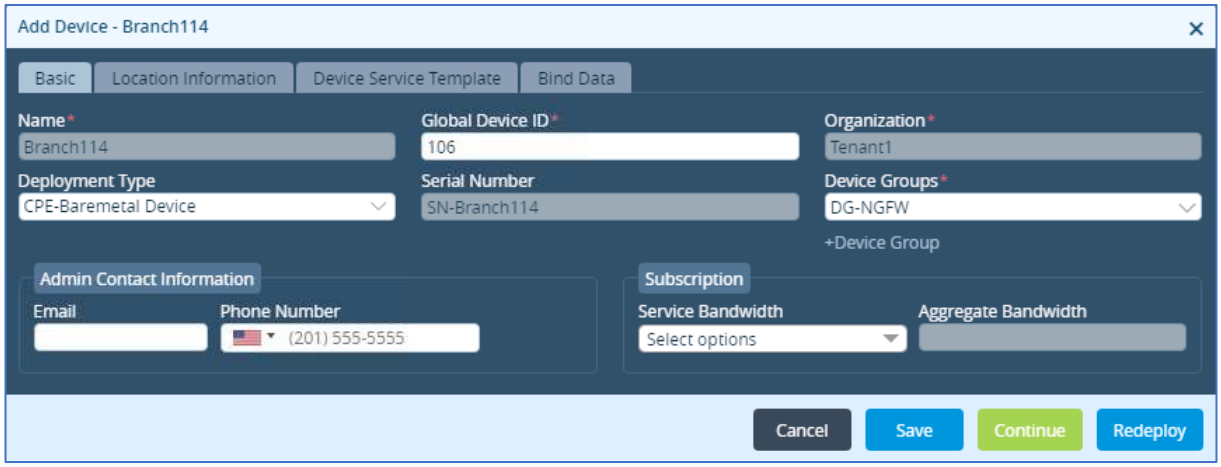
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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

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

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

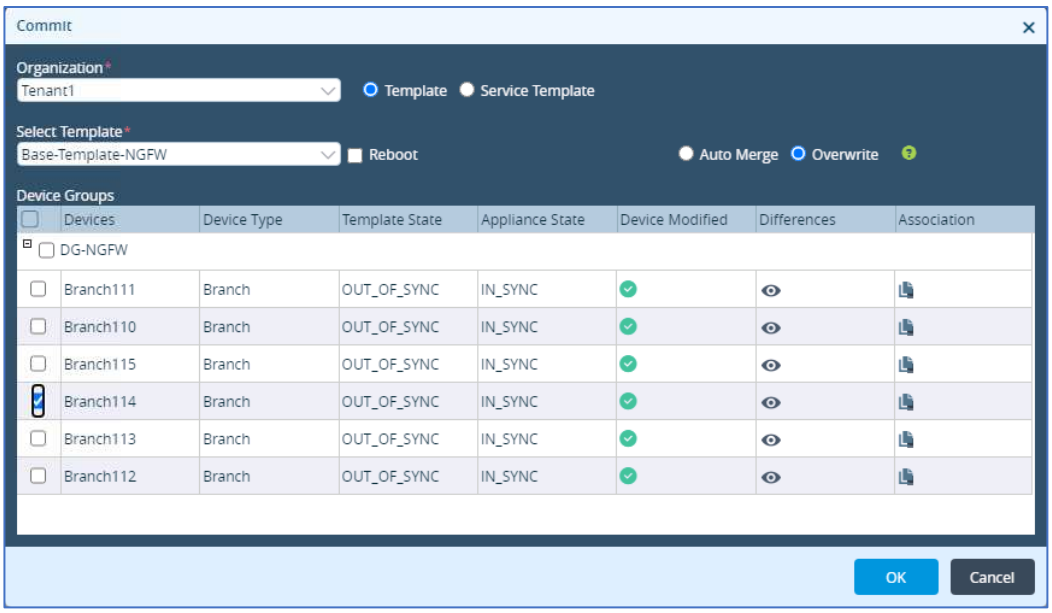
In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select the *Tenant1* organization, the template *Template-NGFW*, and locate your device in the list.

Select your device in the device list and click *OK* to apply the base configuration to your device.



Step 2.1: Configure cloud lookup for current URL reputations

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

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

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

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

Click OK when finished.

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

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

Click OK to finish creating the cloud profile.

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

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

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

Select the Cloud Lookup tab and enter the following parameters:

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

Click OK when finished.

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

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

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

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

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

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

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

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

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

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

Access Rule Parameters	
Name:	URL-IP-Filtering-Rule
Source/Destination:	Source Zone:intf-Tenant1-LAN-Zone Destination Zone: intf-INET-Zone
Headers/Schedule:	Add the following services: domain, http, https
Enforce:	Action: Apply Security Profile Select Profiles > URL Filtering > URLF-Profile Logging: Both, Default-Logging-Profile

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

Step 2.5: Test the URL filtering

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

In the remote desktop, click on the Remote Desktop Connection icon on the desktop to open the Remote Desktop application. Open a remote desktop session to the testing host assigned to your branch. The login for the remote desktop is username ***student*** and password ***versa123***:

Remote Desktop IP addresses		
Branch01: 10.27.10.10	Branch09: 10.27.10.18	Branch17: 10.27.10.26
Branch02: 10.27.10.11	Branch10: 10.27.10.19	Branch18: 10.27.10.27
Branch03: 10.27.10.12	Branch11: 10.27.10.20	Branch19: 10.27.10.28
Branch04: 10.27.10.13	Branch12: 10.27.10.21	Branch20: 10.27.10.29
Branch05: 10.27.10.14	Branch13: 10.27.10.22	Branch21: 10.27.10.30
Branch06: 10.27.10.15	Branch14: 10.27.10.23	Branch22: 10.27.10.31
Branch07: 10.27.10.16	Branch15: 10.27.10.24	Branch23: 10.27.10.32
Branch08: 10.27.10.17	Branch16: 10.27.10.25	Branch24: 10.27.10.33

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

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

`https://facebook.com`

The site should be blocked by the VOS device.

Browse to `https://espn.com`

The site should be blocked.

Browse to `https://instagram.com`

The site should be blocked.

Browse to `https://spotify.com`

The site should be allowed.

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

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

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

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

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

Step 2.7: Test your changes to the URL Filter profile

Return to the remote desktop connection to the testing host, and if the Chromium web browser is not open, open the Chromium web browser.

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

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

Return to Versa Director.

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

From the appliance context mode, navigate to Monitor > Services > NGFW > URL Filtering and choose Profiles from the drop-down menu. This will display URL filtering counters and statistics and should show the number of rule hits in the URL filtering. You should see several

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

Click the Home button in the top-left of Versa Director to return to the main Versa Director dashboard. From the main Versa Director dashboard, click the Analytics tab to open the Analytics dashboard.

From the main Analytics dashboard, ensure that the Tenant1 organization is selected in the Organization drop-down.

Navigate to *Dashboards > Security > Web*, then select the URL Categories tab. You should see URL category information.

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

Examine the URL Filtering log entries. You should see entries for Spotify and other URLs. Some of the URLs may be to sites that you didn't browse to, but that may have been embedded or linked to in the web pages. Verify that the URL category is one of the categories that you included in the URL profile. You can verify which session originated on your testing LAN by examining the source address of the sessions.

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

Step 2.9: Finish the lab and exit the lab environment

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

Close the MTPuTTY application.

Log out of Versa Director.

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

IP Filtering

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

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

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

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

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

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

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

Look for these hints to help you in the labs

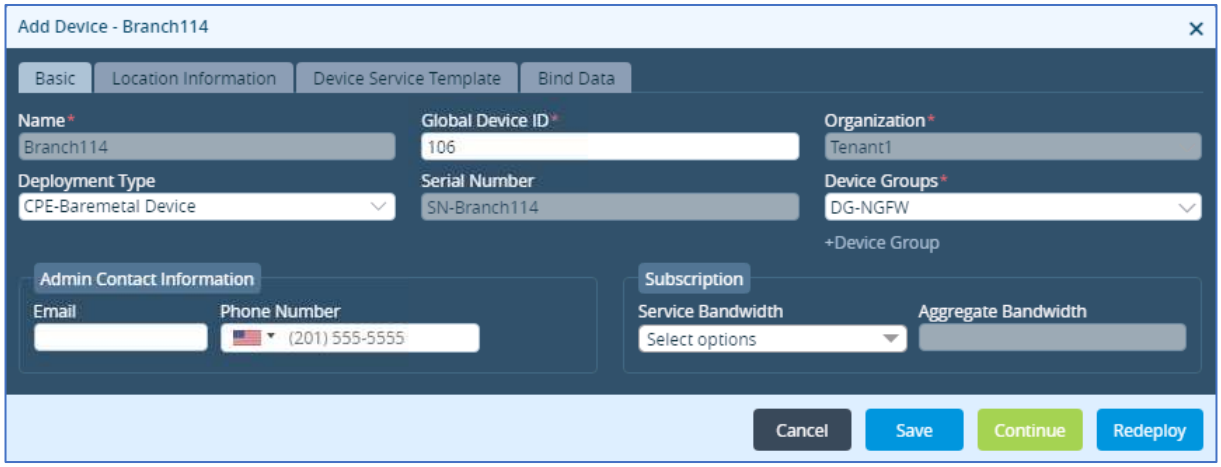
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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

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

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

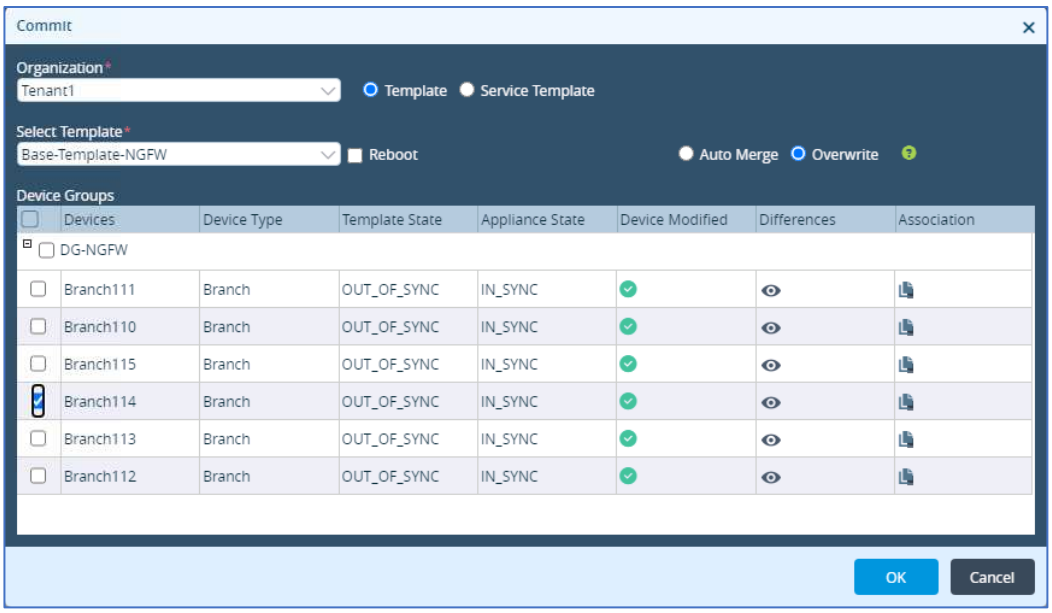
In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select the *Tenant1* organization, the template *Template-NGFW*, and locate your device in the list.

Select your device in the device list and click *OK* to apply the base configuration to your device.



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

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

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

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

Step 2.2: Create a custom IP Filter profile

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

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

IP Filter Profile	
Name:	IP-Filtering-Profile
Default Action:	Allow
LEF Profile:	Default-Logging-Profile
Prioritize URL Reputation:	Uncheck the box
Deny List Action:	Reject
IP Address:	Click the + New Address button and create a new address in the blacklist with the following properties: Name: blacklist-address Address: 10.27.11.130 The address should be added to the IP address list when finished
Match Type:	Match Source or Destination

Click OK to finish creating the profile.

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

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

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

Access Policy Rule Parameters	
Name:	IP-Filtering-Rule
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: Intf-INET-Zone
Headers/Schedule:	Services: domain, http, https, ICMP
Enforce:	Action: Apply Security Profile Select IP Filtering and the IP-Filtering-Profile Logging: Both, select the Default-Logging-Profile

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

Step 2.4: Adjust the default NAT rules

When NAT is automatically configured through the DIA configuration, a default rule is put in place that prevents the translation of RFC1918 (private) routes. Because our lab environment uses private routes, you will have to modify the NAT translation rule so that the 192.168.0.0/16 prefixes will match the DIA NAT rule.

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

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

Step 2.5: Test the IP Filter profile

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

In the remote desktop, click on the Remote Desktop Connection icon on the desktop to open the Remote Desktop application. Open a remote desktop session to the testing host assigned to your branch. The login for the remote desktop is username ***student*** and password ***versa123***.

Remote Desktop IP addresses		
Branch01: 10.27.10.10	Branch09: 10.27.10.18	Branch17: 10.27.10.26
Branch02: 10.27.10.11	Branch10: 10.27.10.19	Branch18: 10.27.10.27
Branch03: 10.27.10.12	Branch11: 10.27.10.20	Branch19: 10.27.10.28
Branch04: 10.27.10.13	Branch12: 10.27.10.21	Branch20: 10.27.10.29
Branch05: 10.27.10.14	Branch13: 10.27.10.22	Branch21: 10.27.10.30
Branch06: 10.27.10.15	Branch14: 10.27.10.23	Branch22: 10.27.10.31
Branch07: 10.27.10.16	Branch15: 10.27.10.24	Branch23: 10.27.10.32
Branch08: 10.27.10.17	Branch16: 10.27.10.25	Branch24: 10.27.10.33

On the testing host, right-click the desktop and open a terminal window.

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

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

Step 2.6: Verify the IP filter profile in Versa Director

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

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

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

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

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

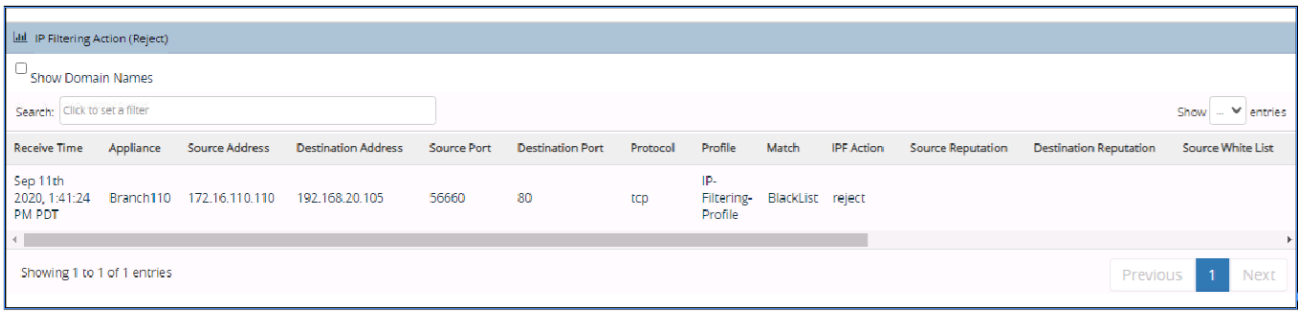
Step 2.7: Verify the IP Filter profile in Versa Analytics

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

In the Versa Analytics dashboard, ensure that the Tenant1 organization is selected in the organization filter drop-down.

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

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



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

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

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

In your appliance context mode, navigate to Configuration > Services > Next Gen Firewall > Security > Profiles > IP Filtering. Open the profile IP-Filtering-Profile and add the following Geo IP Based Actions parameters:

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

Click OK to apply the changes.

Step 2.9: Test the geo-location IP Filtering profile

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

On the landing station, return to the remote desktop session to the testing host. If a shell prompt is not already open, open a new shell prompt by navigating to *Applications > System > Xfce Terminal*.

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 Canada geo-location. The script should time out.

Step 2.10: Verify the Geo-location IP Filter results

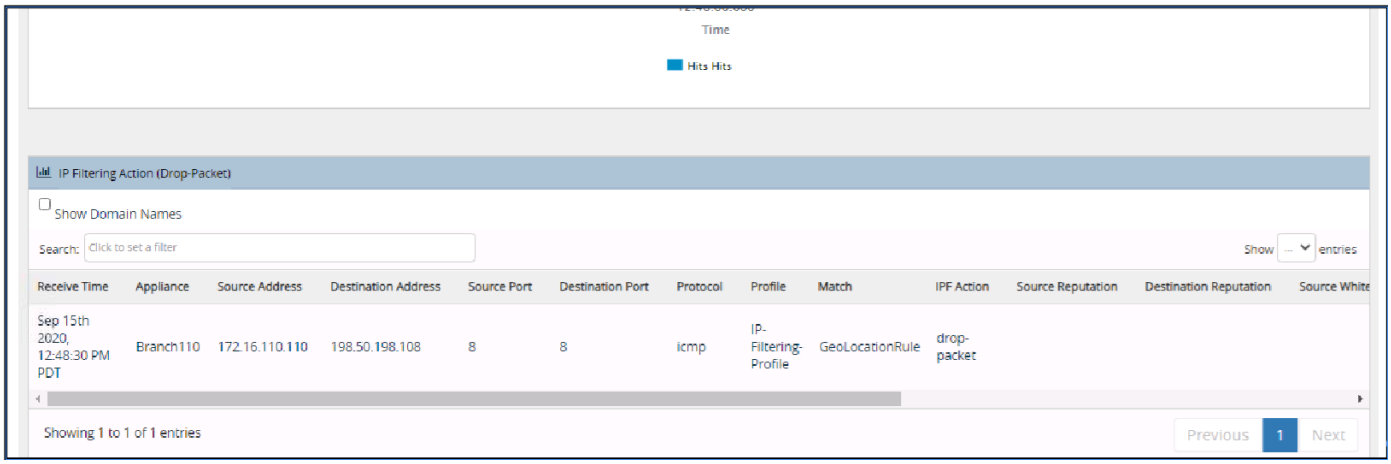
Return to Versa Director. In Versa Director, open the appliance context mode for your appliance.

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

Click the Home button next to your appliance name to return to the main Versa Director dashboard. From the Versa Director dashboard, Navigate to *Analytics > Dashboards > Security > Threats*, then select the IP tab to display the IP threat dashboard. Ensure that the Tenant1 organization is selected in the organization filter drop-down at the top of the dashboard.

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

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



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 Canada.

Step 2.11: Add IP Reputation to the IP Filtering profile

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

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

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

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

Click OK to finish updating the profile.

Step 2.12: Test the IP Reputation profile

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

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

Click the Home button next to your appliance name in the top left to exit appliance context mode and return to the main Versa Director dashboard. From the Versa Director dashboard, navigate to the *Analytics > Dashboards > Security > Threats* dashboard. Ensure that the Tenant1 organization is chosen in the organization filter at the top of the dashboard. Select the IP tab from the dashboard to view IP filtering statistics.

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

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

Step 2.13: Finish the lab and exit the lab environment

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

Close the MTPuTTY application.

Log out of Versa Director.

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

URL Filtering

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

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

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

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

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

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

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

Look for these hints to help you in the labs

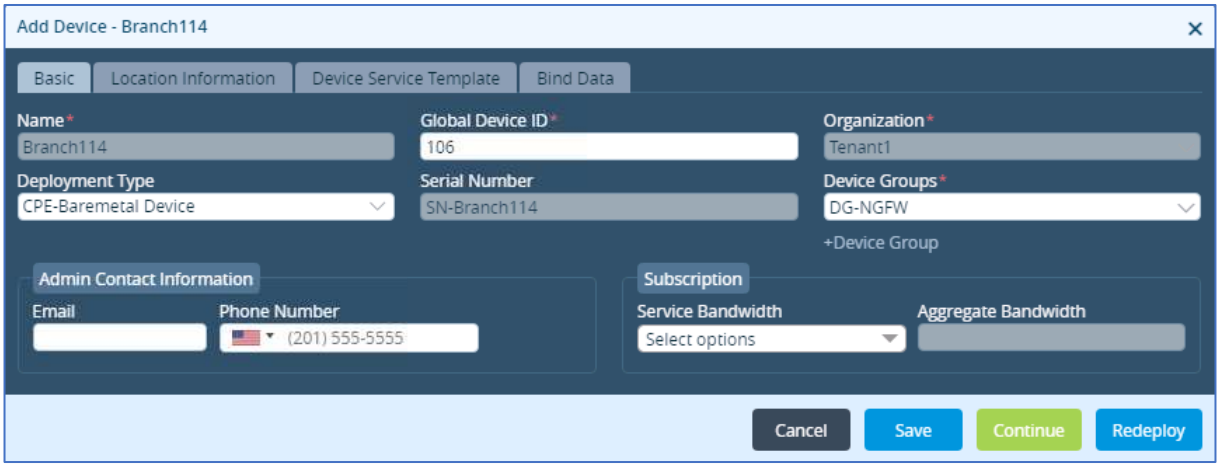
This lab guide will step you through some common tasks that are performed on Versa Director. After an introductory set of exercises, you will be asked to perform some basic tasks that will allow you to become more familiar with the environment.

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

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

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

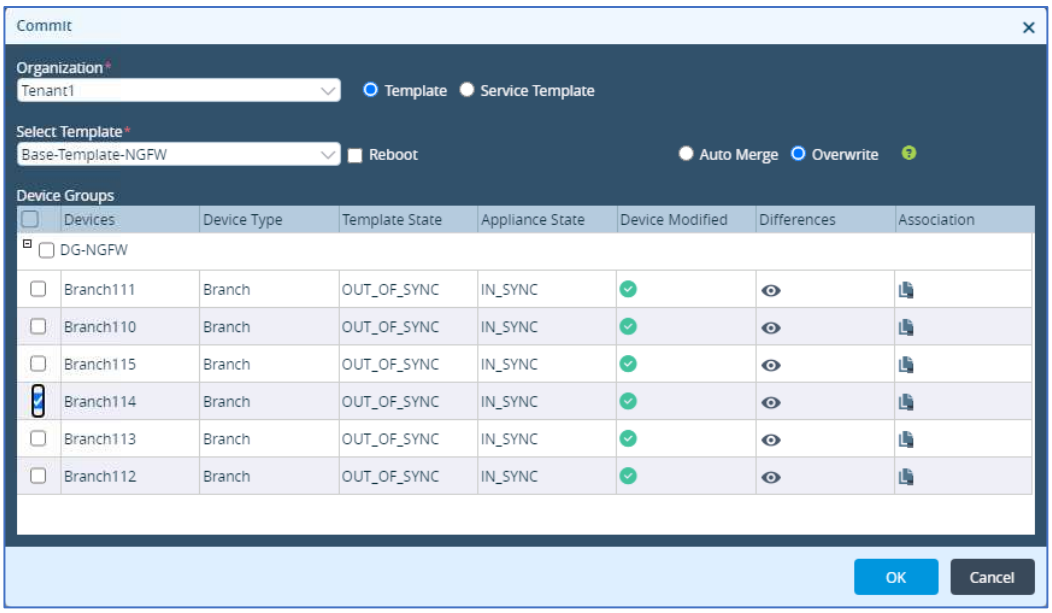
In Versa Director, open the *Workflows > Devices > Devices* dashboard and click on your device workflow. In your device workflow, ensure that the device group *DG-NGFW* is selected, then click Redeploy.



Step 1.2: Commit the default configuration to your device

Click the *Commit Template* button. In the Commit dialog box, select the *Tenant1* organization, the template *Template-NGFW*, and locate your device in the list.

Select your device in the device list and click *OK* to apply the base configuration to your device.



Step 2.1: Configure SSL Decryption using SSL Forward Proxy

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

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

In Versa Director, navigate to *Administration > Appliances*. Click on your appliance in the appliance list to open device context mode for the appliance.

From your appliance context mode, navigate to *Configuration > Objects & Connectors > Objects > Custom Objects > Certificates*. From the Certificates dashboard, select the *Appliance* tab. If there is not an SSL certificate on the device, please refer to the SSL Encryption and Decryption lab for instructions on how to generate a self-signed SSL certificate and import the certificate into the testing host web browser.

If a certificate is present on the appliance you may continue with the lab.

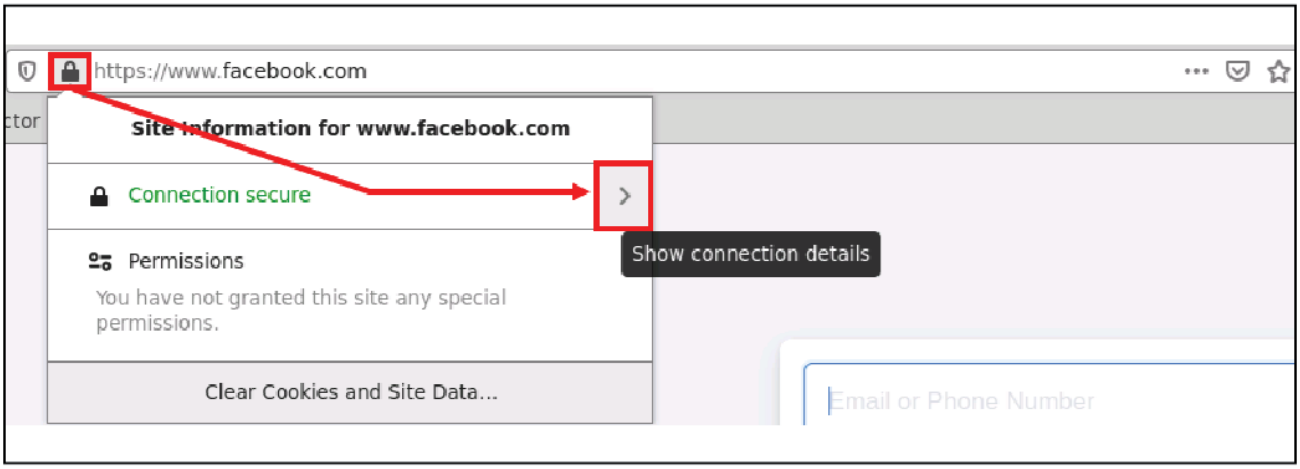
Step 2.2: Test HTTPS access to an Internet site

In the remote desktop, click on the *Remote Desktop Connection* icon on the desktop to open the Remote Desktop application. Open a remote desktop session to the testing host assigned to your branch. The login for the remote desktop is username ***student*** and password ***versa123***.

Remote Desktop IP addresses		
Branch01: 10.27.10.10	Branch09: 10.27.10.18	Branch17: 10.27.10.26
Branch02: 10.27.10.11	Branch10: 10.27.10.19	Branch18: 10.27.10.27
Branch03: 10.27.10.12	Branch11: 10.27.10.20	Branch19: 10.27.10.28
Branch04: 10.27.10.13	Branch12: 10.27.10.21	Branch20: 10.27.10.29
Branch05: 10.27.10.14	Branch13: 10.27.10.22	Branch21: 10.27.10.30
Branch06: 10.27.10.15	Branch14: 10.27.10.23	Branch22: 10.27.10.31
Branch07: 10.27.10.16	Branch15: 10.27.10.24	Branch23: 10.27.10.32
Branch08: 10.27.10.17	Branch16: 10.27.10.25	Branch24: 10.27.10.33

On the testing host, open a Chromium web browser window on the testing host. Enter the `url https://facebook.com` in the address bar to open the Facebook home page.

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



Click the More Information button in the connection details popup.

In the *More Information* dialog you can view the *Website Identify* information in the *Security* tab. The Website should be `www.facebook.com`, the certificate should be verified by DigiCert Inc. Click the *View Certificate* button for more certificate details.

This certificate is the certificate authority certificate for the Facebook web page and is used for validation and encryption of the SSL connection.

Step 2.3: Create a decryption profile

In the next steps you will configure the Versa Operating System device to perform forward proxy to allow the device to decrypt and inspect encrypted payloads for virus and malware payloads.

Close the Chromium web browser and any associated web browser windows on the testing host, then return to Versa Director.

In your appliance context in Versa Director, navigate *Configuration* > *Services* > *Next Gen Firewall* > *Security* > *Decryption* > *Profiles*. Click the + button to create a new decryption profile with the following parameters:

Decryption Profile Settings	
Name:	SSL-INSPECTION-DECRYPTION
CA Certificate:	ssl-certificate
LEF Profile:	Default-Logging-Profile
Decryption Type:	SSL Forward Proxy
Trusted Certificate Database:	default
Min Supported Key Length:	512
SSL Inspection:	Action for Expired Certificate: reject Action for Untrusted Issuers: Drop-packet Action for Unsupported Cipher: allow Action for Unsupported Key Length: allow Action for Unsupported Version: alert
Restrict Certificate Extension:	Enable

Click *OK* to create the decryption profile.

Step 2.4: Create a decryption policy

Next you will create a decryption policy to identify traffic that should be decrypted and to direct the traffic to the decryption profile.

In your appliance context, navigate to *Configuration* > *Next Gen Firewall* > *Security* > *Decryption* > *Decryption Policies*. Click the + button to create a new policy with the following parameters:

Decryption Policy Parameters	
Name:	Decryption-Policy
Description	SSL-INSPECTION-DECRYPTION

Click *OK* to create the policy. Now that the policy has been created you can add rules to the policy.

In the *Decryption Policies* hierarchy, click the *Rules* tab. Click the + button to create a new decryption rule with the following parameters:

Decryption Rule Parameters	
Name:	Inspection-Rule
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: intf-INET-Zone
Headers/Schedule:	Select services: http, https
Enforce:	Action: Decrypt Decryption Profile: SSL-INSPECTION-Decryption

Click *OK* to create the decryption rule.

Step 2.5: Verify the decryption policy and forward proxy functions

Return to the remote desktop session to the testing host. On the testing host remote desktop, open the Chromium web browser.

Enter the address `https://facebook.com` in the address bar to open the Facebook home page. Click on the padlock icon next to the address to inspect the certificate used for the connection.

In the *Certificate* window, expand the *Connection Secure* dialog (> arrow) to view more information about the connection. The connection information should say that the certificate is verified by Tenant1 (the identity in the self-signed certificate). You can click the More Information button to view more detailed information about the certificate. In the certificate details the organization Tenant1 and Common Name Versanetworks.com will be in the Issuer Name field.

This process verifies that the Versa Operating System is intercepting the Facebook connection and acting as a forward proxy for the sessions. Close the Chromium web browser window and any Chromium web browser related windows on the testing host.

Return to the Versa Director user interface.

In your appliance context mode, navigate to *Monitor > Services > NGFW > Decryption > Profile*. Next click on *Service > NGFW > Decryption*. Choose *Profile* from the drop-down box. This will display the SSL decryption statistics. Check for the "SSL Pxy Server Encrypt" & "SSL Pxy Server Decrypt" statistics which indicate that the SSL connections have been encrypted/decrypted as expected.

In the Decryption statistics table, select *Policy* from the drop-down box, then choose *SSL-INSPECTION-DECRYTPION* in the new drop-down box that appears to view the policy statistics. The rule I*nspection-Rule* should show a number of hits. This indicates that the rule was used for transit sessions.

Next you will analyze the the detailed decryption logs using Versa Analytics.

Click the *Home* button next to your appliance name in the top-left corner to exit appliance context mode and return to the main Versa Director user interface.

From Versa Director, click the *Analytics* tab to open the main Versa Analytics dashboard. Select the organization *Tenant1* from the organization drop-down at the top of the dashboard.

From the left-side menu, navigate to *Logs > SSL Decryption*. You should see a list of log entries. In the Search bar, enter a filter to search for domainName `facebook.com`. When applied, you will see the entry for the facebook.com session. Locate an entry from your appliance. Click the magnify button to view the log entry details. Information including the decryption profile used, policy rule that matched the traffic, the forward and reverse interfaces, the addresses and domain name, and zone information is recorded.

Configure Antivirus profiles to scan encrypted traffic

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

To create an Anti-Virus Profile, open your appliance context and navigate to *Configuration > Services > Next Gen Firewall > Security > Profiles > Anti-Virus*.

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

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

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

Click *OK* to create the profile.

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

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

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

Antivirus Rule Settings	
Name:	UTM-RULE-AV
Source/Destination:	Source Zone: Intf-Tenant1-LAN-Zone Destination Zone: Intf-INET-Zone
Headers/Schedule:	Add the following services: http, https
Enforce:	Action: Apply Security Profile > AV-Profile Logging: Both, Default-Logging-Profile

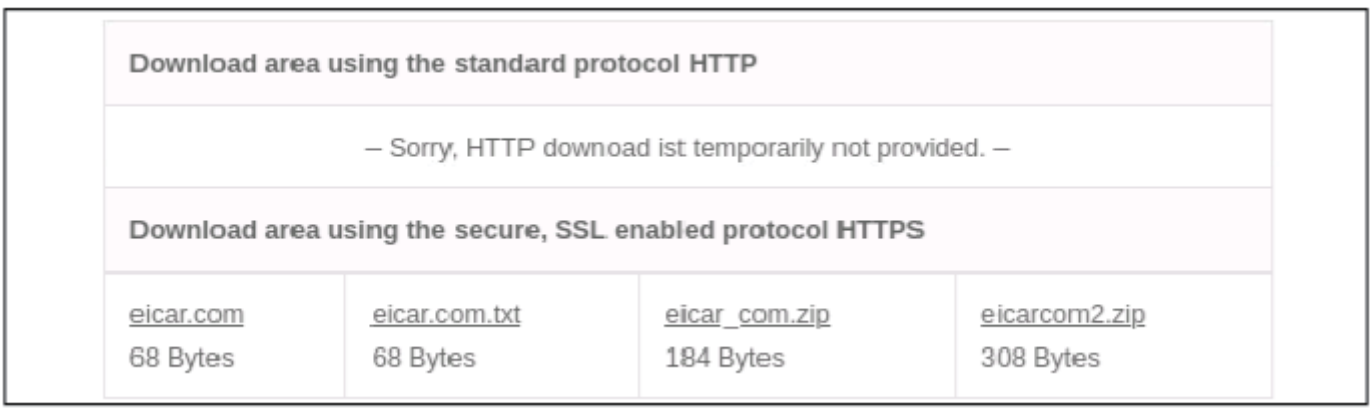
Click *OK* to create the rule. The rule will be placed after the auto-generated rules. Move the rule to the top of the rule list so that it is processed first.

Step 2.8: Verify the SSL decryption and Antivirus scanning

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

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

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



Click the `eicar.com.txt` file to attempt to download the file.

Click the `eicar_com.zip` file to attempt to download the file.

Click the `eicarcom2.zip` file to attempt to download the file.

The files should not be downloaded and should be blocked.

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

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

Click the *Home* button next to your appliance name to exit device context mode and return to the main Versa Director user interface. From the main Versa Director interface, navigate to *Analytics > Logs > Firewall*. Ensure that the *Tenant1* organization is selected in the organization drop-down at the top of the dashboards. In the search dialog, set a filter that matches rule with a name of *UTM-Rule-AV*. Apply the filter. Look for entries from your appliance. You should now only see entries related to the *UTM-Rule-AV* firewall rule. Check to see that the rule has traffic matching port 80 and 443, and with the action set to *allow*. Note that the firewall rule matches and allows the traffic, but the allow action refers to the forwarding of the traffic to the corresponding security profile. The security profile makes the final decision on whether or not to allow the traffic flow.

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

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

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

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

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

UTM Rule Parameters	
Name:	UTM-Rule-IDP
Source/Destination:	Source Zone: intf-Tenant1-LAN-Zone Destination Zone: ptvi
Headers/Schedule:	Click + New Service and create a custom service: Name: UTM-Hub Protocol: TCP_OR_UDP Port: 443
Enforce:	Action: Apply Security Profile Select Vulnerability > Versa Recommended Profile Logging: Both, Default-Logging-Profile

Click *OK* to add the rule.

Step 2.10: Verify results using Versa Director

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

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

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

From within the terminal window, execute the following command

```
./exploitS2-057-cmd.py 10.27.130.99:80 'id'
```

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

Step 2.11: Verify the results using Versa Director

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

Navigate to the *Vulnerability* tab and select *Pre Defined* from the drop down list. Scroll down to the *Versa Recommended* profile. It should show a non-zero value in the Total Sessions field. To view more details about the profile sessions, click the  icon. You should see statistics indicating that there were signature hits and reset actions taken.

Step 2.12: Verify results using Versa Analytics

Click the *Home* button next to your appliance name in the top left to return to the main Versa Director user interface. From the main Versa Director user interface, navigate to *Analytics > Dashboards > Security > Threats*. Ensure that the *Tenant1* organization is listed in the organization drop down at the top of the dashboard.

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

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

Navigate to *Logs > Threat Detection* and select the IDP tab. In the IDP tab you should see the log entries for the events. Click the ⊕ icon to view more details about the session and related log messages. Included in the log entry is information such as Threat type, Signature Message, Class Message, Action, and Signature Identifier.

Step 2.13: Configure Intrusion Detection (alert only)

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

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

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

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

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

Click *OK* to create the profile.

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

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

Step 2.14: Verify the threat detection without prevention

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

Return to the remote desktop session to the testing host. 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-S2057-cmd.py 10.27.130.99:32771 'id'
```

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

To verify that the device only generated an alert for the attack, return to Versa Director. In Versa Director, navigate to *Analytics* > *Dashboards* > *Security* > *Threats*. Ensure that the *Tenant1* organization is selected in the organization drop-down at the to of the dashboard.

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

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

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

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

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

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

Exception Parameters	
Name:	IDP-Override
LEF Profile:	Default-Logging-Profile
Rule:	Action: Reject
Exceptions:	You will add 3 exceptions to the rule. Click the + button and add the following: ThreatID: 1111209051; enable Signatures: Search and select the following signatures: 1111209050 1130527060 1111209051 Exception Details: Action: Allow Exempt IP Address 10.27.130.99 Thresholds: Track by Destination

Click *OK* to create the exemption.

Step 2.16: Verify the exemption

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

```
./exploitS2-057-cmd.py 10.27.130.99:80 'id'
```

The attack should succeed or end with an HTTP 400 error, which indicates that the exploit reached the remote web server and was not blocked by the Branch110 device.

Return to Versa Director. In Versa Director, navigate to *Analytics > Logs > Threat Detection* and select the *IDP* tab. Ensure that the organization filter in the top of the dashboard is set to *Tenant1*.

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

Step 2.17: Finish the lab and exit the lab environment

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

Close the MTPuTTY application.

Log out of Versa Director.

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