Versa Basic Security Services

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

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

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

The lab environment is accessed through a remote desktop connection. 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 5 other students in the environment. Each student has their own remote desktop, but the Versa Director is shared. Because of the shared environment, you may see configuration templates, device groups, workflows, and devices that other students have created, or that have been pre-provisioned within Versa Director. It is important that you only modify the configuration components that are assigned to you by your instructor.

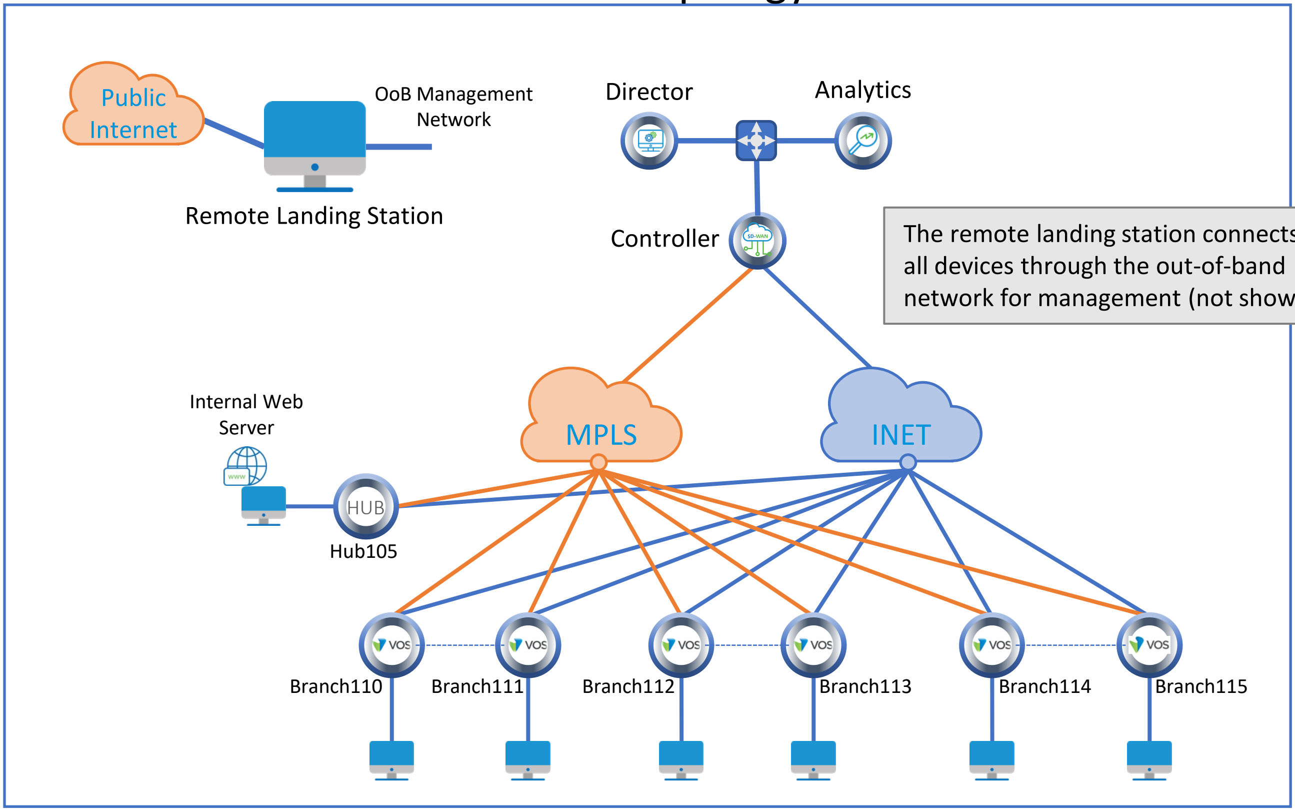
During certain lab parts, the lab guide will present sample output from the GUI or the CLI. The sample outputs are SAMPLES and represent the information as it appeared during the lab guide creation. Your output may vary in some ways (some devices may or may not be present, some routes may or may not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

This lab guide will step you through a set of exercises, and you will be asked to perform some basic tasks that will allow you to become more familiar with the the lab goals. If you cannot accomplish the task, ask your instructor for assistance.

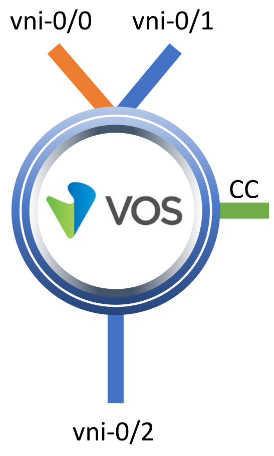
The goal of this and all lab exercises is to help you gain additional skills and knowledge. Because of this, the lab guide contains additional instruction to supplement the student guides.

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

Lab Topology



The remote landing station connects to all devices through the out-of-band network for management (not shown).



Each branch device connects to the MPLS transport and to the INET Transport

- MPLS: vni-0/0
- INET: vni-0/1

Each branch connects to a local LAN

- vni-0/2

Each branch pair has a cross-connect (used in HA labs only)

- vni-0/3

Versa Director Login: **labuserXYZ** (e.g. **labuser110**, **labuser111**, etc.)
Versa Director Password: **Versa@123**

Branch OoB Login: **versa**
Branch OoB Password: **versa123**

Testing Host Login: **labuserXYZ** (e.g. **labuser110**, **labuser111**, etc.)
Testing Host Password: **versa123**

Remember this! You will use it a lot!

Interface Addresses

CPE	vni-0/0	vni-0/1	vni-0/2
Branch110	192.168.19.110/24	192.168.20.110/24	172.16.110.1/24
Branch111	192.168.19.111/24	192.168.20.111/24	172.16.111.1/24
Branch112	192.168.19.112/24	192.168.20.112/24	172.16.112.1/24
Branch113	192.168.19.113/24	192.168.20.113/24	172.16.113.1/24
Branch114	192.168.19.114/24	192.168.20.114/24	172.16.114.1/24
Branch115	192.168.19.115/24	192.168.20.115/24	172.16.115.1/24
MPLS Gateway	192.168.19.3		
INET Gateway		192.168.20.3	

Controller Addresses

MPLS	MPLS Gateway	INET	INET Gateway
192.168.17.3/24	192.168.17.1	192.168.18.3/24	192.168.18.1

Exercise 1: Connect to the remote lab environment

The first lab exercise is to become familiar with how to connect to the remote lab environment. Your instructor should have reviewed the following information with you prior to starting:

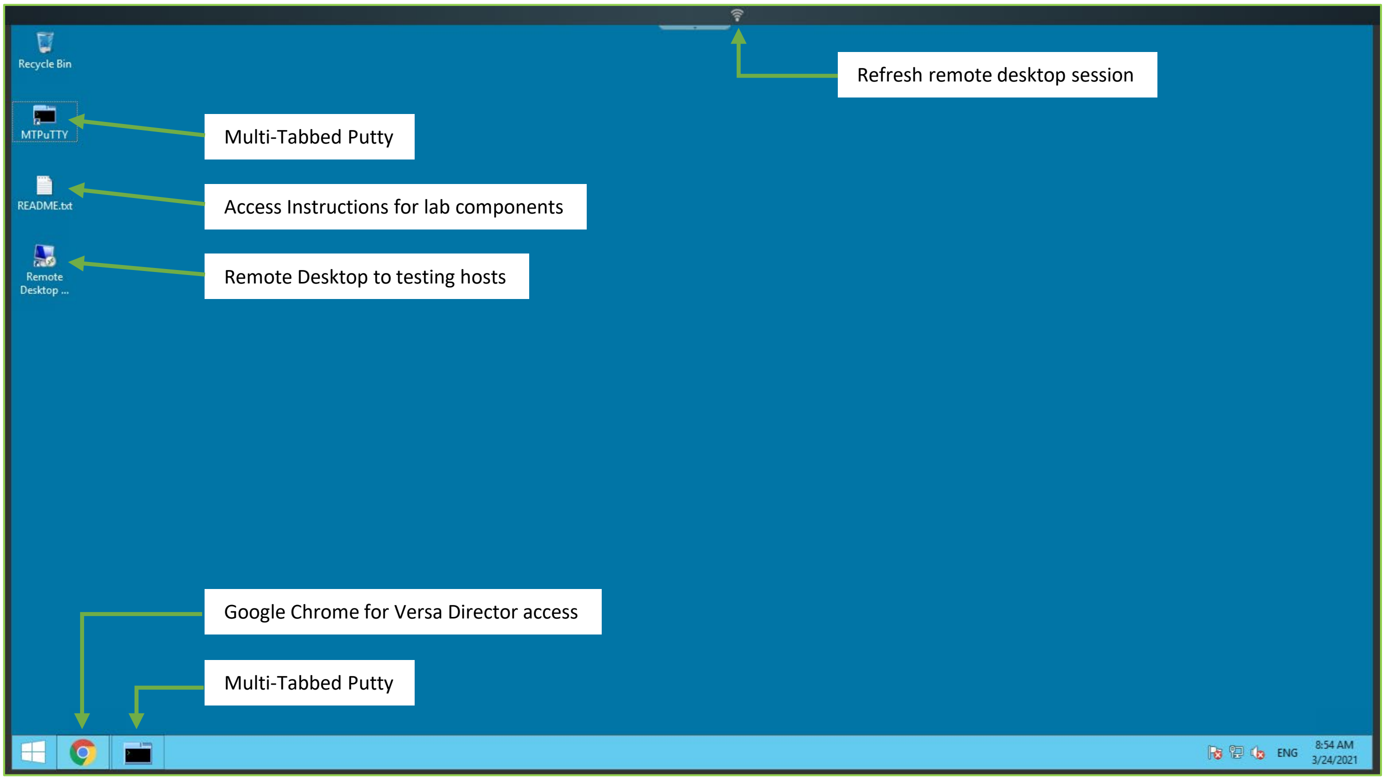
- Branch/Node/CPE Assignment
- Remote Lab Access

If you have not yet been assigned a branch device, please contact the instructor as this is a shared environment, and each student will configure and monitor a specific branch node.

Question: What node is assigned to you in the lab topology? ____________________

Follow the instructions provided by your instructor to connect to the remote lab environment.

Once you have started your remote desktop session, you will be presented with the remote desktop:


Recycle Bin
MTPuTTY
README.txt
Remote Desktop ...
Refresh remote desktop session
Multi-Tabbed Putty
Access Instructions for lab components
Remote Desktop to testing hosts
Google Chrome for Versa Director access
Multi-Tabbed Putty
ENG
8:54 AM
3/24/2021

On the remote desktop, open the Google Chrome browser window. The Google Chrome browser window contains a bookmark to the Versa Director. Log into the Versa Director with the username associated with your assigned branch device:

CPE	Username	Password
Branch110	labuser110	Versa@123
Branch111	labuser111	Versa@123
Branch112	labuser112	Versa@123
Branch113	labuser113	Versa@123
Branch114	labuser114	Versa@123
Branch115	labuser115	Versa@123

Exercise 2: Configure Basic Security Services

In the following lab exercises, you will:

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

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

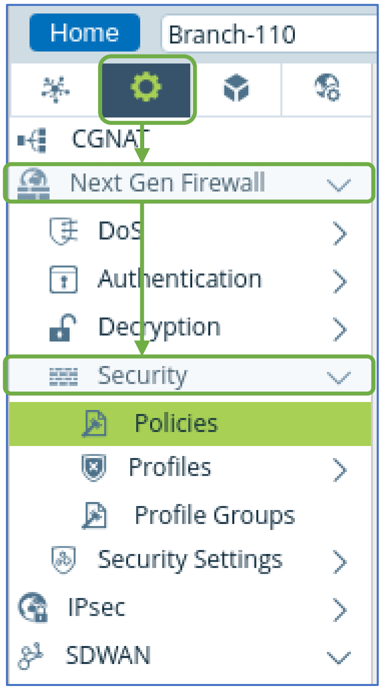
Note: The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

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

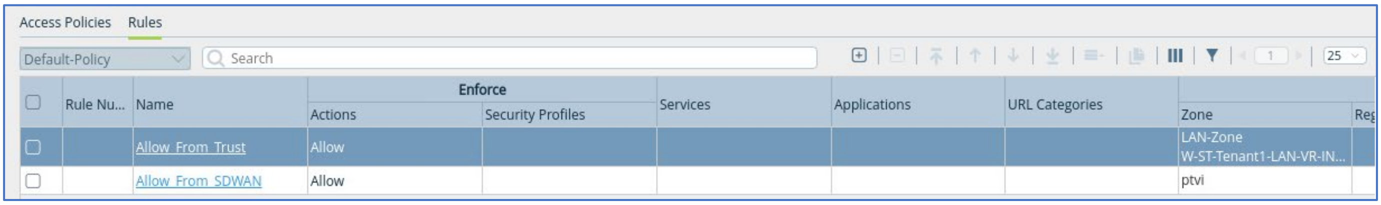
The main configuration components related to security policy are located in the *Services > Stateful Firewall* or *Services > Next Gen Firewall* hierarchy of the configuration, depending on which type of services are enabled in the template workflow.

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

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



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



☐	Rule Nu...	Name	Enforce		Services	Applications	URL Categories		
			Actions	Security Profiles				Zone	Reg
☐		Allow_From_Trust	Allow					LAN-Zone W-ST-Tenant1-LAN-VR-IN...	
☐		Allow_From_SDWAN	Allow					ptvi	

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

Allow access to the following business applications from the branch to the Internet through DIA:

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

Deny the following URL categories from the LAN to any destination. Enable logging for the End of session attempts to these types of URLs. Use the default logging profile:

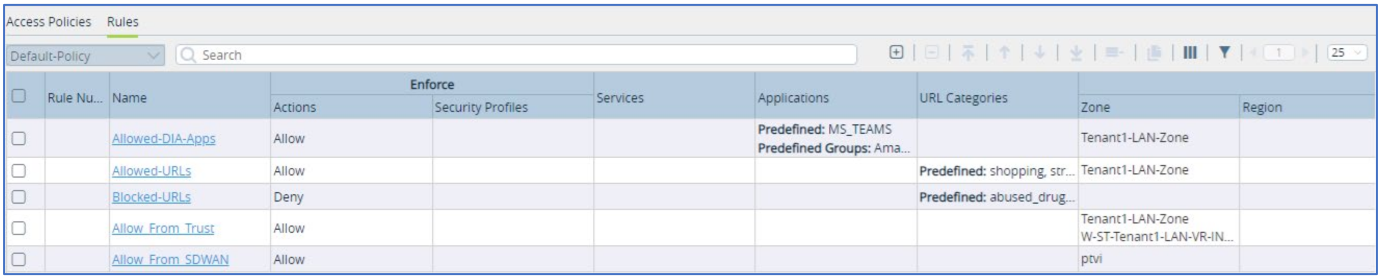
- games
- gambling
- abused_drugs
- dating
- malware_sites
- news_and_media
- streaming_media

Special Note: Many sites are now encrypted with SSL encryption (HTTPS), and therefore security policies cannot decrypt URL categories on HTTPS sites.

For example: a web session to a shopping site may create dozens of sessions, some of which are HTTP and some of which are HTTPS. The HTTPS sessions may not be recognized by a rule that allows the traffic to pass, whereas the HTTP session can be recognized. Because of this, when some security features that rely on analyzing URL information is implemented, some components of a web page may pass the filter and some may not, depending on whether the system can recognize and analyze the embedded components. This can cause some web pages to behave abnormally or to *break*.

To enable full security scanning of HTTPS traffic, SSL proxy can be enabled to decrypt transit traffic. SSL proxy is NOT configured in this lab environment, and therefore the lab is designed to demonstrate how to configure basic security policies, but does not focus on testing and validating those policies.

When finished, your security policies should resemble the below screenshot:



□	Rule Nu...	Name	Enforce		Services	Applications	URL Categories		
			Actions	Security Profiles				Zone	Region
□		Allowed-DIA-Apps	Allow			**Predefined:** MS_TEAMS **Predefined Groups:** Ama...		Tenant1-LAN-Zone	
□		Allowed-URLs	Allow				**Predefined:** shopping, str...	Tenant1-LAN-Zone	
□		Blocked-URLs	Deny				**Predefined:** abused_drug...		
□		Allow_From_Trust	Allow					Tenant1-LAN-Zone W-ST-Tenant1-LAN-VR-IN...	
□		Allow_From_SDWAN	Allow					ptvi	

STOP

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