

Lab Security Packages and Updates

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

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

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

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

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

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

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

Exercise 1:

In the following lab exercises, you will:

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

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

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

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

	r View Appliance View Template View		🗄 🤅 Stu	udent01 (Student01) -
NETWORKS Monitor	Configuration Workflows Administration A	nalytics		Commit Template
	④ You are currently in Direct	ctor View		C
२ Search	OS Security (OS SPack) Security (SPac	:k)		
Organizations	Package Deuploade Appliance Upgra	der		
Appliances	Package Downloads Appliance Opgra	ues		
> Connectors	∇			
> System	Package Name	Package Version	Download Type	Flavor
> VMS Services	versa-security-package-2165.tbz2	2165	Full	Premium
Scheduled Tasks	versa-security-package-2119.tbz2	2119	Full	Definitions
> Notification Configuration	versa-security-package-2014.tbz2	2014	Full	Premium
> Director User Management	versa-security-package-2013.tbz2	2013	Full	Premium
V Inventory				
Software Images	Kowsper page 25 V Showing 1 - 4 0	DT 4		
Hardware				
Stalon Davisos				

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

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

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

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

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

DIRECTOR	
Administrator	
••••••	۲
u Have Logged Out	Forgot Password
Login	

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

	or View 🛛 🖌	Appliance View Temp	plate View						Ê () ⁽ 0	Administrator •
Monit	or Co	nfiguration Wo	orkflows	Administration	Analytics					Сог	mmit Template
					④ You	are currently in Directo	rView				C
Q Search		OS Security (OS SPack)	Security (SPac	k) Software (VO	S/Director)						
Organizations	Par Par	ckage Downloads	Appliance Upgrad	des Director Un	rades						
Appliances		ckage Downloads	Appliance Opgrac	Jes Director op	grades						
> Connectors	7	7						el Download 🕜 Edit Spack C	Configuration 🛓 Download 📤 Uploa	id 🕃 Spack Fi	ile Limit 🛛 🔻
> System		Package Name		Packag	e Version	Download Type	Flavor	Size	Day & Time Downloaded	Status	
> VMS Services		versa-security-packag	e-2165.tbz2	2165		Full	Premium	1032 MB	Fri, Jun 14 2024, 14:11	DOWNLOA	DCOMPLETE
Scheduled Tasks		versa-security-packag	e-2119.tbz2	2119		Full	Definitions	79 MB	Thu, Feb 15 2024, 17:24	INSTALLED	
> Notification Configuration		versa-security-packag	e-2014.tbz2	2014		Full	Premium	711 MB	Tue, Dec 20 2022, 09:23	PREVIOUS	LY INSTALLED
> Entitlement Manager		versa-security-packag	e-2013.tbz2	2013		Full	Premium	711 MB	Tue, Dec 20 2022, 09:23	DOWNLOA	D COMPLETE
> Director User Management	Rows	per page 25 🗸 Sł	howing 1 - 4 c	of 4							
~ Inventory											
Software Images											
Hardware											

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

4

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

Click the Download button to view the download dialog.

Download Security (S-Pack) Package	\times
Package *	
Please Select	~]
Download Cancel	
	_

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

Click the *Cancel* button to exit the dialog.

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

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

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

D	IRECTOR
Student01	Ι
••••••	Ŕ
u Have Logged Out	Forgot Password
	Login

Navigate to Administration > Inventory > Software Images > Security (SPack) > Appliance Upgrades. Check the box next to your BO2 device and identify the Package Version that is currently installed on the device from the Package Version column in the table.

	View Ap	pliance View Template View					1	Student01(Student01) -
Monitor	Conf	iguration Workflows Adr	ministration Analytics					Commit Template
				(i) You are currently in C	Director View			C
2 Search	os	Security (OS SPack) Security (SPack)						
Organizations	Death	Developed and Apple of the second						
Appliances	Pack	Appliance Opgrades						
> Connectors	Q, Se	arch	Q Appliance Tag	55				순 Upgrade Appliances 🔲 🍷
> System								Security (SPack) Informatio
> VMS Services	•	Appliance Name	Management Address	Management Address Tags		Owner Org	Package Version	Scheduled
Scheduled Tasks		501801	172 15 0 4		branch	Student01	2014	completed
Notification Configuration	6	\$01802	172.15.0.6		branch	Student01	2014	completed
Director User Management		SD-HUR-Now	172.15.0.30		branch	JUGGROI	2014	
 Inventory 			11111000		service 1			_
Software Images	Rows p	er page 25 v Showing 1 - 3 of 3						

Click the Upgrade Appliances button to open the upgrade dialog.

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

ownload Type *		Selecte	d appliances (1)		
Full	~		Search appliance	Search package version	
avor *		Û	S01B02	2014	
Please Select	~				
versa-security-package-2165.tbz2					
versa-security-package-2164.tb2 versa-security-package-2014.tb22 versa-security-package-2013.tb22					

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

6

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

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

	Director Vie	w Appl	iance View	Template View										(j)	Student01(S	itudent01) •
	lonitor	Config	uration	Workflows	Administration	Analytics									Commit	Template
						③ You are curre	ntly in Director View							Export All R	ecords [xport C
Q Search							62									
Organizations		Applian	ces (0/3)	Name	S01B01		Q. Search		Q Appli	iance Tags					+ 0 0 •	More *
Appliances				Location	San Diego, CA, USA									Status		
> Connectors			Name	Site ID	101	5	Туре	Service Start T	ime	Software Version	Organizations	Config	g Sync F	teachability	Service	Locked
System			: S01001	Serial Number	SN-S01B01		Branch	Mon, Jun 17 20	024, 12:54	22.1.3-GA	Student01		0	0	Up	ef e
> VAC Consistent			: S01B02	Nodel	c5.2xlarge	cenat	Branch	Mon, Jun 17 20	024, 12:54	22.1.3-GA	Student01		0	0	Up	e a
> VMS Services			SP-HUB-	Time Created	2024-05-24 04:42:09.6	68	Branch	Mon, Jun 1720	024, 12:54	22.1.3-GA	Student01		0	0	Up	aî a
Scheduled Tasks		Pour por	0000	Template Statu	SOUT_OF_SYNC											
> Notification Configuration	n	nows per	page 25													
> Director User Managemen	nt															
~ Inventory																

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

	DCA	Director Vi	iew Appliance	View Template View		
NETWORKS		Monitor	Analytics	Configuration	Administration	
Appliance	S01B01	~				④ You are
Networking S	ତ୍ତ ଅଷ Services Objects Connect	ere Sors Others				
Q Search						
> Organiz	zation					
~ System						
> Con	nfiguration	- 1				
Spe	ed Test	- L				
Dor	main Name Ser	vers				
Sec	urity Package U	Jodates				
> Tim	e & Date					

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

Automatic Security Update Setting	CIdit
Common Settings	
URL :	

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

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

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

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

Click OK to finish the configuration change.

Common Settings	
URL	
https://spack.versanet	tworks.com/versa-updates
Download Timeout	Routing Instance
300	INET-Transport-VR 🗸
Flavor Type	
Premium	~
Scheduled Update	Download Type
Scheduled Update Start Time 02:00:00	Download Type
Scheduled Update Start Time 02:00:00 Interval	Download Type Full Y
Scheduled Update Start Time 02:00:00 Interval	Download Type Full ~
Scheduled Update Start Time 02:00:00 Interval Realtime Update	Download Type Full ~
Scheduled Update Start Time 02:00:00 Interval Realtime Update Start Time	Download Type Full ~ I

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



SSL Inspection and Decryption

Steps:

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

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



SSL Inspection and Decryption

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

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

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

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

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

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

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

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

Exercise 1:

In the following lab exercises, you will:

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

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

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

Step 1: Reset the lab to a base configuration

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

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

Step 2: Open the Device Configuration

In the next steps you will create an SSL encryption key for your branch device. You will then create a selfsigned 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:

10

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

	irector View	Appliance Vi	ew Template View	(Ê	í	Student01 (Student01) •
Metworks	onitor	Analytics	Configuration	Administration							Commit Template
Appliance S01B01	~	Organization	Student01	~		③ You are	currently in Appliance View				Build
문 ৩ ₀ 명립 Networking Services Objects & Connectors C	others	Director	Appliance								
Q Search		∇							+ Add 🗔	Upload F	ile 🝈 Delete File 🔳 🕶
CSR EIP Objects			Private Key Name		Туре			Size(bytes)			
EIP Profiles Endpoint Protection Geo Circles	n				Generate Key On App	pliance Type	×				
> IoT Security					ssl-certificate-private-ke	RSA	~				
Keys					Туре	Pass Phrase					
Operating System					2048 ~	lab123@	۲				
						ok (Cancel				

Step 4: Create an appliance certificate

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

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

VERSA Director Vie	w Appliance View Template View					📋 🤢 Student01(Student01) -
Monitor	Analytics Configuration Administra	Generate certificate On App	oliance		×	Commit Template
Appliance S01B01 V	Organization Student01 ~					Build C
Networking Services Objects & Others	Director Appliance	Certificate Name *	Validity (day	s)		
Q. Search		Certificate Attributes				+ Add 🛄 Upload File 🗇 Delete File 🕒 Export 🔲 •
Captive Portal Cust	Certificate Name	CA Certificate Se	rial#	Signature Algorithm	_	Common Name
Certificates		O False	123456	SHA256	~	
CRL		Common Name • Er	nail ID	Country Name	_	
CSR		versanetworks.com				
EIR Objects		State or Province Lo	cality	Organization		
EIP Objects				Student01		
EIP Promes		Organization Unit				
Endpoint Protection						
Geo Circles		Drivata Kau Nama z			_	
> IoT Security		ssl-certificate-private-key			~	
IPAM Address		+ Private Key				
Keys						
Operating System				®K Can	ncel	

Step 5: Configure Proxy Profiles

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

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

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

	Director Vie	w Appliance V	ew Template View							Ê	(i) Student01	(Student01) •
VERSA	Monitor	Analytics	Configuration	Add Decryption Profile					×		Comm	it Template
Appliance S01B01	~	Organization	Student01	General SSL Inspection SSL Pr	otocol Advanced							Build C ^a
Networking Services Connector	S Others			Name * SSL-INSPECTION-DECRYPTIC	N					+ /	vdd 🗐 Defeta (9)	Classe 🖬 🕶
Q. Search		Name	LEF Pr	Description		Tags			_		Server Certificate	Checks - Actions
CGNAT										Untrusted Issuer	\$	Rei
∨ Next Gen Firewall				Enable Profile	Supp	ort Session Ticket		Use Extended Master Secret				
> DoS				Time	Toustad	Cortificato Database a		CA Costificato a				
> Authentication				SSL Forward Proxy	v default	ertincate Database *	~	ssl-certificate	~			
~ Decryption				(
Policies				LEF Profile					-			
Proxy Profiles	- 11			Default-Logging-Profile								
Server Profiles	- 11			Default Profile								
Settings	- 11			LEF Log Level								
> Security	- 11			Alert				`				
> Security Settings												
> Microsegmentation								OK Cano	el			
> IPsec												(iii)
> SDWAN							_		_			9

OCSP	Response Timeout	Verify	
Enabled Block Unknown Certificate	5	Select	~
CRL Check Fetch issuer using AIA O			
Action for Expired Certificate Action for Untrust	ed Issuers		
Reject ~ Allow	~ 2	Restrict Certificate Extens	sion
Unsupported Mode Checks Action for Unsupported Cipher	Min Supported Key Leng	th	
Allow	512		
Action for Unsupported Key Length	Action for Unsupported	/ersion	
Allow	Alert		~

Min Version		Max Version		
TLS-1.1	~	TLS-1.2		~
Key Exchange Algorithms	Encryption Algorithms AES128-CBC		Authentication SHA	n Algorithms
ECDHE	AES128-GCM		SHA256	
	AES256-CBC		SHA38	If you do not select any specific
	AES256-GCM			and authoriticat
	Camellia-256-CBC			encryption and authentication
	ChaCha20-Poly130	05		algorithms, then all algorithms for
	Seed CBC			the enabled TLS versions are
Cipher Suites				automatically enabled
Oselected	*			

Step 6: Create an SSL Decryption Policy

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

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

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

	w Appliance View Template Vi	/iew		Ē	i	Student01 (Student01) -
Monitor	Analytics Configuration	on Administration				Commit Template
Appliance S01B01 ~	Organization Student01	~	③ You are currently in Appliance View			Build C ^a
Networking Services Objects & Others	Decryption Policies Rules					
Q. Search	Q Search	\bigtriangledown				🗊 Delete 🛛 🗖 🕶
CGNAT	Name		Description			
∨ Next Gen Firewall	Default	It-Policy				
> DoS						J
> Authentication	Rows per page 25 V Showing	ng 1 - 1 of 1				
~ Decryption						
Policies						
Proxy Profiles						
Server Profiles						
Settings						
> Security						

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

.

Next you will create 2 rules with the following parameters:

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

Add Decryption Rule	×
General Source Destination Headers/Schedule URL Users/Groups Enforce	
Name • 15/127	
Inspection-Rule	
Description	
Tags	
	Disable Rule
	OK

Inspect traffic from the Intf-Student_LAN-Zone

Source Zone		+ Ne	w Zone + 📋 💅	Source Address			+ New Address + New Address Group + 📋
Intf-Student_LAN-Zone			۲			Source Address Not Configure	1
Source Address Negate							
Region + 🗊	2 ²⁰	State			a ⊡ +	City	+ 🗊
Region Not Configured			State Not C	Configured			City Not Configured
Source Location Negate							
Custom Geo Circle	+ 🗊 🕫			EIP Profiles			+ Add EIP Profile + 📋
Custom Gen Circle Not Configured						FIP Profiles Not Configured	

Match the HTTPS service

Add Decryption Rule General Source Destination Headers/Schedule URL Use	rs/Groups Enforce			;
IP IP Version	IP Flags		Others Schedules	
Select V	Select	~)	Select	~
DSCP		+	+ Schedule	
TTL			Services	+New Service + 💼 💅
Condition	Value (Max 255)		https	۲
Greater than or equal to 🗸 🗸				
				ок

Match URLs that are in the financial_services category

Add Decryption Rule			×
General Source Destination Headers/Schedule URL Users/Groups Enforce			
URL Category	+ New URL Category + 📋 💅	URL Reputations	a ^α ⊞ +
financial_services	۲	Prede	efined Reputations Not Configured
			OK Cancel

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

eneral Source Destination Header	rs/Schedule URL Users	/Groups Enforce			
Action Setting		Action Override		Decryption Profile*	
Action *		URL Filtering		SSL-INSPECTION-DECRYPTION	~
no-decrypt	~	Select	~	View Decryption Profile	

.

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

Add Decryption Rule		×
General Source Destination Headers/Schedule URL Users/Groups Enforce		
Name - 15/127		
Decryption-Rule		
Description		
Tags		
	Disable Rule	
		OK Cancel

Set the source zone to Intf-Student_LAN-Zone.

Source Zone	+ New Zone + 📋 a ^p	Source Address		+ New Address + New Address Group + 📋 👩	
Intf-Student_LAN-Zone	۲		Source Address Not Configured		
Source Address Negate					
Region + 🗇 💅	State	+ 🗇 e ^p	City	+ 🗇 🕫	
Region Not Configured	State Not 0	Configured	City No	t Configured	
Source Location Negate					
Custom Geo Circle	age ≘ +	EIP Profiles	+ Add EIP Profile		
Custom Geo Circle Not Configured		EIP Profiles Not Configured			

Set the service to https.

General Source Destination Head	ers/Schedule URL User	s/Groups Enforce			
IP		10.5		Others	
IP version		IP Flags		Schedules	
Select	~	Select	× _	Select	~
DSCP				+ Schedule	
TTL			+	Services	+New Service + 🗊 💋
Condition		Value (Max 255)		https	۲
Greater than or equal to	~				

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

Add Decryption Rule			×
General Source Destination Headers/Schedule URL Users/	Groups Enforce		
URL Category	+ New URL Category +	URL Reputations	+ 🔟 🕫
sports	۲	Predefined Reputations N	ot Configured
social_network	۲		
news_and_media	۲		
			OK Cancel
			Cancer

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

Add Decryption Rule			×
General Source Destination Headers/Se	hedule URL Users/Groups Enforce		
Action Setting	Action Override	Decryption Profile "	
Action •	URL Filtering	SSL-INSPECTION-DECRYPTION	~
decrypt	✓Select	View Decryption Profile	
			OK Cancel

Exercise 2: Test the Decryption Policy

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

Steps in this exercise:

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

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

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

In the Remmina application, open the Sxx Linux RDP session, where Sxx is your

Student ID. If prompted, the RDP credentials for the remote session are: username: *student*; password: *versa123*.



©Copyright 2022 Versa Networks

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

You should be presented with the remote desktop below.



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

Open the Chromium browser on the remote desktop and navigate to <u>www.usbank.com</u>. 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.

9 Privacy error × +		
→ C A Not secure gespn.com		* 0 1
Versa Director Login 🚪 ESPN 🛤 Fox Sp	iorts 📕 US Bank 💶 YouTube 🛔 Netflix - Watch TV 😚 Facebook 🔞 Instagram 🥥 Spotify - Web Player 🌗 Music and Podcast	
	A	
	Your connection is not private	
	Attackers might be trying to steal your information from www.espn.com (for	
	example, passwords, messages, or credit cards). Learn more	
	NET::ERR_CERT_AUTHORITY_INVALID	
	Q To get Chrome's highest level of security, <u>turn on enhanced protection</u>	
	Advanced Back to safety	
	@Convright 2022 Versa Networks	

.

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).

🛇 Versa Director Login	× +
← → C A Not secure	10.234.0.101/versa/lo
🕥 Versa Director Login 🧮 ESPN	l 🛤 Fox Sports 📕 U

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.

					https://10.27.	1.10/versa/#d	irector/administration	n/appliances	- Chromium						- +
https://10.27.1.10/versa/#c	direct ×	+													
← → C 🔺 Not sec	ture 10.21	7.1.10/\	ersa/#directo	r/administration	/appliances										*
🗿 Versa Director Login 🛛 🧮	ESPN KSK	Fox Spor	ts 📕 US Ban	k 🖸 YouTube	Netflix - Watch TV 😝 Facebook	🔘 Instagram	Spotify - Web Player	r 👂 Music	and Podcast	Malware Test	Hub Web Server				
	Director Vie	w Ap	pliance View	Template View								1	i	Student01(S	student01) -
VERSA	lonitor	Conf	iguration	Workflows	Administration Analytic	s								Commit	Template
					④ You are cut	rently in Direc	tor View						Export All Re	cords	Export (
l Search															
Organizations		Applia	inces (0/3)	Name	S01B01		Q. Search		Q Appliance	Tags	Shell 1 Sync-			+ 8 -	• 🛛 More •
Appliances				Location	San Diego, CA, USA								Status		
Connectors			Name	Site ID	101		Туре	Service Sta	rt Time	Software Version	Organizations	Config Sync	Reachability	Service	Locked
System			: S01901	Serial Number	SN-S01B01		Branch	Mon, Jun 1	7 2024, 12:54	22.1.3-GA	Student01	0	0	Up	af i
VMS Services			: S01B02	Services	cs.zxiarge		Branch	Mon, Jun 1	7 2024, 12:54	22.1.3-GA	Student01	٥	٥	Up	ъ.
Chadded Tarla			: SP-HUB-I	Time Created	2024-05-24 04:42:09.68		Branch	Mon, Jun 1	7 2024, 12:54	22.1.3-GA	Student01	0	0	Up	ŝ
Scheduled lasks		Power	01 0000 05	Template Statu	s OUT_OF_SYNC										
Notification Configuration	n	Rowsp	er page 25												
Director User Managemen	nt														

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.

VEDSA	Director Vie	ew Appliance	e View Template View)				1	(j)	Student01 (Student0)	1)-
VERSA	Monitor	Analytics	Configuration	Administration						Commit Templat	te
Appliance S01B01	~	Organizatio	on Student01	~]		④ You are of the second sec	currently in Appliance View			Build	C
Retworking Services Objects & Connector	ere Sors Others	Director	Appliance								
Q. Search		∇						+ Add 🔝 Upload File	Dele	teFile 🕒 fixport 🖽	1 -
✓ Custom Objects Address Files			Certificate Name		CA Certificate		Private Key Name	Common Name			
Application Filte	ers		ssl-certificate		YES		ssl-certificate-private-key	versanetworks.com			
Application Gro	oups	Rows per pag	e 25 v Showing 1	- 1 of 1							
CA Certificate	- 1										
CA Chains											
Captive Portal C	Cust										
Certificates										2	-
CRL										ç	ני

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.

$e \rightarrow G$ A Not secure [1]	0.27.1.10/versa/#appliances/S01B01/configuration/objects/ci	istom-objects/certificate			☆ ()
Versa Director Login 📄 ESPN I	Sex Fox Sports 📕 US Bank 💿 YouTube 🕌 Netflix - Watch TV View Appliance View Template View	😯 Facebook 🔞 Instagram 🥥 Spotify – Web Pl	eyer 🐌 Music and Podcast 🤤 Malware Test 🔇 Hub W	leb Server	New tab Ctr New window Ctr New incognito window Ctrl+Shift
Monitor	Analytics Configuration Administration		O You are currently in Appliance View		History Downloads Ct Bookmarks
Se 0.0 BB working Services Connectors Others	Director Appliance				Zoom - 100% + Print Ctr
Search V Custom Objects	V			+ Add 👤 Upload	Cast Find Ctr More tools
Address Files	Certificate Name	CA Certificate	Private Key Name	Common Name	Edit Cut Copy P
Application Filters	ssI-certificate	YES	ssl-certificate-private-key	versanetworks.con	Setting
	You and Google	Privacy and security			_
	Safety check	Clear browsing data Clear history, cookies, cac	he, and more	•	
	 Privacy and security Appearance 	Cookies and other site da Third-party cookies are bl	a ocked in Incognito mode	•	
	Q Search engine	Safe Browsing (protection	from dangerous sites) and other security settings	,	
	Default hereinen				

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.

← Manage <mark>certificate</mark> s								
Your <mark>certificate</mark> s	Servers	Authorities	Others					
You have certificates on file that in	You have certificates on file that identify these certificate authorities							
org-AC Camerfirma S.A.			~					

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

	Open File			×
n Home	▲ student Downloads ▶			
Desktop	Name	•	Size	Modified
Documents	ssl-certificate.crt		1.2 kB	14:56
👕 Downloads	N N			
Music 📄				
Pictures				
Videos				
Other Locations				

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

Trust settings	
_	
 Trust this certificate for identifying websites 	
 Trust this certificate for identifying email users 	
Trust this certificate for identifying software makers	;

.

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



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.

Privacy error X	+		
← → C ▲ Not secure ex	pired.badssl.com		I
🔇 Versa Director Login 🧧 ESPN 😰	🕱 Fox Sports 🛛 📕 US Bank	🖸 YouTube 🚶 Netflix - Watch TV 😝 Facebook	🛛 💿 Instagram 🏾 🥥 Spotify – Web Player 🛛 Ҏ Music and Podcast
		Your connection is not priva	te
		Attackers might be trying to steal your inform example, passwords, messages, or credit car	nation from expired.badssl.com (for 'ds). <u>Learn more</u>
		NET::ERR_CERT_DATE_INVALID	
1 Contraction of the local distance of the l			

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.

Add Decryption Rule	×
General Source Destination Headers/Schedule URL Users/Groups Enforce	
Name • 11/127	
Inspect-All	
Description	
Tags	
	Disable Rule
	OK Cancel

.

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

General Source Destination Headers/Schedule URL Users/Groups Enforce				
Source Zone	+ New Zone + 📋 💅	Source Address		+ New Address + New Address Group + 📋 😰
Intf-Student_LAN-Zone	۲		Source Address Not Configured	
Source Address Negate				
Region + 🗇 💅	State	a ≘ +	City	+ 🗈 s
Region Not Configured	State Not C	onfigured		City Not Configured
Source Location Negate				
Custom Geo Circle	+ 🗎 a ^p	EIP Profiles		+ Add EIP Profile 🕂 📋 🖬
Custom Geo Circle Not Configured			EIP Profiles Not Configured	
Custom Geo Circle Not Configured	т 🛛 в		EIP Profiles Not Configured	OK.

Match the HTTPS service.

Seneral Source Destination Headers/S	chedule URL Users	/Groups Enforce			
IP IP Version		IP Elags		Others	
C-last		C-lt		Schedules	
select		Select	•	Select	×
DSCP				+ Schedule	
			+	Services	+ New Service + 10 2
TTL					
Condition		Value (Max 255)		https	۲
Greater than or equal to	~				
					OK Cancel

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

Add Decryption Rule				X
General Source Destination Headers/Schedule URL U	sers/Groups Enforce			
Action Setting	Action Override		Decryption Profile*	
Action •	URL Filtering		SSL-INSPECTION-DECRYPTION	~
no-decrypt	Select	~	View Decryption Profile	
				K Cancel

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

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



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

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

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

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

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

VEPSA Director View Appliance View Template View	🖺 🔅 Student01 (Student01) •
Monitor Analytics Configuration Administration	Commit Template
Organization Student01 V Ov are currently in Appli	lance View Build
Summary Devices Cloud Workload	
Total Appliances 3 S01B01 X	
S01B01 San Diego, CA, USA Mgmt, Address: 172,15.0,4 System Bridge Address: 0A-CB-AA:FC-CB:00	Reachable SYNC: IN_SYNC: Up since: Mon Jun 17 12:54:31 2024
Summary Services Networking System Tools	Configuration Shell Config Status* Upgrade Subscription
SDWAN NGRW CGNAT SDLAN IPsec Sessions SCI Secure Access APM	
Antivirus ATP Authentication Policies CASB Cloud File Export Decryption DLP DNS Filtering DoS Policies File Filtering IP Filterin	ng Microsegmentation Policies Microsegmentation Statistics Persistent Action Policie < >
Please select ✓ Please select ✓ Global Profile Profile Histoffy Profile Status	

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.

SDWAN NGFW CGNAT SDLAN IPsec	Sessions SCI Secure Access APM		
Antivirus ATP Authentication Policies CASB	Cloud File Export Decryption DLP DNS Filtering DoS Policies	File Filtering IP Filtering Microsegmentation Policies Microsegmentation Statistics	Persistent Action Polic < >
Policy	Default-Policy ~		
			Search C 🖬 🗸 Clear
Name 🕈		Hit Count	
Inspection-Rule		7	
Decryption-Rule	*	81	
Inspect-All		50	

Click the Director View button to exit Appliance View.

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

) sc	WAN >	Configuration	WORKHOU	vs Aunimistra	Analytics	
xoard	Student01	All sites	8.	Last day	•	
gs			3 Total Sites Si	0 tes with Low Availability	O Sites with Dataplane Downtime	Sites with Criti
•	Top sites by band	width				
rting					Top 5	: =

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.

1.0	SSL Decr	yption Logs >											America/D	Denver	•
	Studer	nt01 👻 all		✓ Last day		•									
	SSL	logs													
	Sho	ow Domain Names													
	Set fi	lters here		- Apply	Clear Copy	/ Filter								Show	10 🗸 entries
	Set fi	Iters here	Appliance	Apply Client Address	Client Port	Proxy Address	Proxy Port	Server Address	Server Port	Domain Name	Protocol	Туре	Action Type	Show SSL Action	0 v entries Proxy Typ
	Set fi	Receive Time	Appliance S01B01	Apply Client Address 10.27.101.20	Client Port	Proxy Address	Proxy Port	Server Address 104.154.89.105	Server Port	Domain Name	Protocol tcp	Type	Action Type SSL certificate expired	Show SSL Action reject	Proxy Typ
C	Set fi	Iters here 11 Receive Time 11 Jun 17th 2024, 2:53:19 PM MDT Jun 17th 2024, 2:53:19 PM MDT	Appliance S01B01 S01B01	Apply Client Address 10.27.101.20 10.27.101.20	Client Port	Proxy Address	Proxy Port	Server Address 104.154.89.105 104.154.89.105	Server Port 443 443	Domain Name expired.badssl.com expired.badssl.com	Protocol i tcp tcp	Type end end	Action Type SSL certificate expired SSL certificate expired	Show Show SSL Action reject	Proxy Typ forward forward
	Set fi	Iters here 11 Receive Time 11 Jun 17th 2024, 2:53:19 PM MDT Jun 17th 2024, 2:53:19 PM MDT Jun 17th 2024, 2:53:19 PM MDT	Appliance 501801 501801 501801	 Apply Client Address 10.27.101.20 10.27.101.20 10.27.101.20 	Client Port	Proxy Address	Proxy Port	Server Address 104.154.89.105 104.154.89.105 104.154.89.105	Server Port 443 443 443	Domain Name expired.badssl.com expired.badssl.com expired.badssl.com	Protocol tcp tcp tcp	Type end end end	Action Type SSL certificate expired SSL certificate expired SSL certificate expired	Show SSL Action reject reject	Proxy Typ forward forward forward

Related SSL logs (0x6670	a2220100020003d8)
	Show 10 v entries
Receive Time	Log
Jun 17th 2024, 2:53:19 PM MDT	2024-06-17T20.53:19Z ssl5essionLog, tenant-Student01, applianceName=501B01, srcPort=50318, destPort=443, inglf=vni-0/20, egrlf=vni-0/00, protocolld=6, fromZone=Intf-Student_LAN-Zone, fromUser=Unknown, toZone=Intf-INETZone, srcAddr=1027.101.20, destAddr=104.154.89.105, obsTime=2024-06-17T20.53:182, tb9tes=94, tb9tks=94, tb9tks=94
Showing 1 to 1 of 1 entries	Previous 1 Next
Showing 1 to 1 of 1 entries	Previous 1 N

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



Stateful Firewall

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

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

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

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

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

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

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

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

Exercise 1:

In the following lab exercises, you will:

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

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

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

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

Step 2.1: Reset the lab to a base configuration

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

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

Exercise 2:

Step 2.1:

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

				④ You are currently in	Director View			
λ Search								
Organizations	F	Select Appliance						
Appliances		Organization						
Connectors	-	Select Option						~
System								
VMS Services		Q Search		∇				□ -
Scheduled Tasks		Name	Туре	Management Address	Software Version	Config Sync	Reachability	Locked
Notification Configuration	R	S01B01	branch	172.15.0.4	22.1.3-GA	0	0	ъ£
Director User Management		501B02	branch	172.15.0.6	22.1.3-GA	0	0	ef all a second a sec
Inventory		SP-HUB-New	branch	172.15.0.30	22.1.3-GA	0	0	ъ£
Support		Rows per page 25	Showing 1 - 3 of 3					
Files and Folders								
Files and Folders								Cancel

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

	ew Appliance	View Template View)							Ê	(j)	Student01(Student01) •
Monitor	Analytics	Configuration	Administration									Commit Template
Appliance S01B01 ~	Organization	Student01	~			④ You an	e currently in Appliance Vie	ew .				Build
문 00 88 *** etworking Services Objects & Connectors Others	Access Poli	cies Rules										
Q Search	Default-Polic	y Y Q 5	earch	∇						+ Add 📋		Clone 🗏 Move 🗖 🗸
CGNAT						Source				Destination		
∨ Stateful Firewall	Rule Nun	Name	Rule Disabled	Zone	Region	Address	Address Group	Zone	Region	Addre	\$5	Address Group
> DoS	1	Allow_From_Trust	False	Intf-Student_LAN-Zo W-ST-Student01-LAN	19 I							
> Security Settings	2	Allow_From_SDWAN	False	ptvi								
> IPsec	Rows per page	25 V Showing 1	- 2 of 2									

In the following lab steps you will:

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

.

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

Rule 1:

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

General Source Destination Headers/Schedule Enforce Name 22/3: Block-Outbound-SSH-INT Description Tags Image:
General Source Destination Headers/Schedule Enforce Name • 22/3: Block-Outbound-SSH-INT Description Tags Image: I
Name * 22/3 Block-Outbound-SSH-INT
Block-Outbound-SSH-INT Description Disable Rule
Description Tags
Disable Rule
Disable Rule
OK Cancel
Add Bule
General Source Destination Headers/Schedule Enforce
Source Address + New Address + New Address Group + 2
IntT-Student_LAN-Zone Source Address Not Configured
Custom Geo Circle + 🖹 🖉 Region + 🗎 🖉
Custom Geo Circle Not Configured Region Not Configured
Add Rule >
Canaral Source Destination Headers/Schedule Enforce
Destination Zone + New Zone + 🗊 g ²⁰ Destination Address + New Address Group + 🗊 g ²⁰
Intf-INET-Zone Destination Address Not Configured
Custom Geo Circle + a 2 ²⁰ Region + a 2 ²⁰
Custom Geo Circle Not Configured Region Not Configured

A

•

IP P Version	IP Flags	Others Schedules	
Select	✓	✓Select	~
DSCP		+ Schedule Services	
TTL	Value (Max 255)	Service List	+ New Service + 🗊 💅
Greater than or equal to	Ville (1.101 200)	ssh	۲

Start End Both Never	Action Allow	Deny Reject
EF Profile Select	✓ ✓ Default Profile Synced Flow Synced Flow	
	Select	~

Rule 2

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

Add Rule		×
General Source Destination Headers/Schedule Enforce		
Name *		22/31
Allow-Inbound-ICMP-B2B		
Description	Tags	
Disable Rule		
		OK Cancel

+ 🗊 💅

h				
	Destination Zone + New Zone +	2 ²²	Destination Address + New Address Group + 🗊 👷	
	Intf-Student_LAN-Zone	۲	Destination Address Not Configured	
ĥ				
A

P Version	IP Flags	Others Schedules	
Select V	Select V	Select	~
DSCP		+ Schedule	
TTL	Value (May 255)	Service List	+ New Service + 🔟 💅
Greater than or equal to V			٢

og	Action	
Start End O Both Never	O Allow O Deny	Reject
LEF Profile Default		
Select V Profile	Synced Flow Synced Flow	
	Select	~

Rule 3

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

eneral Source Destination Headers/Schedule Enforce	
Name *	2
Allow-Outbound-ICMP-B2B	
Description	Tags
Disable Rule	
	OK Cancel
	OK Cancel
	OK Cancel
	OK
ld Rule	OK
dd Rule	OK Cancel
dd Rule neral Source Destination Headers/Schedule Enforce	Cancel
dd Rule neral Source Destination Headers/Schedule Enforce Source Zone + New Zone + 1 g ²	Cancel Cancel Source Address + New Address Group +
dd Rule neral Source Destination Headers/Schedule Enforce Source Zone + New Zone + 1 g ² Intf-Student_LAN-Zone	OK Cancel Image: Source Address + New Address Image: Source Address + New Address Image: Source Address Not Configured
dd Rule neral Source Destination Headers/Schedule Enforce Source Zone +New Zone + g ^Z Intf-Student_LAN-Zone Custom Geo Circle + g ^Z	OK Cancel Source Address + New Address Source Address + New Address Group Source Address Not Configured
dd Rule ineral Source Source Zone + New Zone Intf-Student_LAN-Zone Intf-Student_LAN-Zone Custom Geo Circle + @ g ²	OK Cancel Image: Source Address + New Address Image: Source Address + New Address

Add Rule			>
General Source Destination Heade	rs/Schedule Enforce		
Destination Zone	+ New Zone + 🔟 💅	Destination Address	+ New Address + New Address Group + 📋 💅
🗆 ptvi	۲		Destination Address Not Configured
Custom Geo Circle	as ⊕ 10 +	Region	+ © ₂ ²
Custom Geo Cir	cle Not Configured		Region Not Configured

A

•

	k.		
Р		Others	
P Version	IP Flags	Schedules	
Select V	Select V	Select	~
DSCP		+ Schedule	
	+	Services	
TTL		Service List	+ New Service + 🗊 🖬
Greater than or equal to ~	Value (Max 255)		4

	Action	
Start End O Both Never	Allow Deny	Reject
LEF Profile		
Select V Profile	Synced Flow Synced Flow	
	Select	~

Rule 4

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

Add Rule	×
General Source Destination Headers/Schedule Enforce	
Name *	27/31
Block-Outbound-HTTP-B2B-Hub	
Description	Tags
Disable Rule	
	OK Cancel
Add Rule	×
General Source Destination Headers/Schedule Enforce	
Source Zone + New Zone + 🗎 🕫	Source Address + New Address Group +
Intf-Student_LAN-Zone ③	Source Address Not Configured
Add Rule	×
General Source Destination Headers/Schedule Enforce	
Destination Zone + New Zone + 🗎 💅	Destination Address + New Address Group + i 2
🔹 ptvi 💿	Destination Address Not Configured
Add Address ×	
Name * Hub-HTTP-80	
Description Tags	Create a New Address
Add at ag	Name: Hub-HTTP-80 Type: IPv4
Pv4 v 1027.1320/32	Address: 10.27.13.20/32
L OK Cancel	

A

.

P Version IP Flags	Others Schedules
Select	Schedules
	Select V
JSCP	
	+ Services
TTL Condition Value (Max 255)	Service List + New Service + a 2
Greater than or equal to V	Service List Not Configured Add a new Service
	OK Cancel
Service	×
1e *	
istom-HTTP-80	
cription Tags	
	New Service: Custom-HTTP-80
Protocol O Protocol Value	Protocol: TCP
ocol * Protocol Value	Port Range (Port): 80
CP ~ 0255	
Port Range Osource/Destination Port ICMP	
: O Source Port ICMP Type	
Use ,/- for values/r	angos
Destination Port ICMP Code	
	anges
Oli	Cancel
Rule - Block-Outbound-HTTP-B2B-Hub	×
al Source Destination Headers/Schedule Enforce	
	Action
itart 🖉 End 🧿 Both 🖉 Never	O Allow O Deny O Reject
F Profile	
F Profile -Select V Default Profile	Synced Flow Synced Flow





.

Rule 5

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

Add Rule		>
General Source Destination Headers/Schedule Enforce		
Name • Allow-Local-Outbound-Internet		29/3
Description	Tags	
Disable Rule		
		OK Cancel

ieneral Source	Destination Headers,	/Schedule E	nforce							×
Source Zon	e		+ New Zone +	a ²¹	Source Address	+ New /	Address + New Add	ress Group	+ 1	27
Intf-Studen	t LAN-Zone			۲		Source Address N	ot Configured			
introducen										
	-		_	-		_				
Add Rule	Destination Headers	/Schedule E	inforce							>
Add Rule	Destination Headers, Zone	/Schedule E	nforce + New Zone +	€ a ²	Destination Addre	155 + New/	Address + New Add	fress Group	+ 1	>

•

P Version	IP Flags	Others Schedules	
Select V	Select V	Select	~
TTL	+	Services Service List	+New Service + 💼 🕫
Greater than or equal to V	Value (Max 255)	domain	(3
		http	(
		https	(

Edit Rule - Allow-Local-Outbound-Internet			×
General Source Destination Headers/Schedule Enforce			
Log	Action		
Start End O Both Never	O Allow	Openy	O Reject
LEF Profile			
Select V Default	Synced Flow		
	Synced Flow		
	Select		~
			OK Cancel

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 hostbound 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.



working Services Objects & Others	Q Sear	ch	∇						+ Add 🍈	
Search			Name	Log Profile	Zone Protection Profile	Interface List	Routing Instance	Networks	Org	
Interfaces		:	Intf-INET-Zone					INET		
WLAN		:	Intf-MPLS-Zone					MPLS		
Γ1/E1 Auth		;	Intf-Student LAN-Zone					Student LAN		
Vetworks										
/irtual Wires		1	E-ST-Student01-LAN-VR-INET			tvi-0/603.0				
Global Routers		:	L-ST-Student01-LAN-VR-MPLS							
/irtual Routers		:	RTI-INET-Zone				INET-Transport-VR			
firtual Switches		:	RTI-MPLS-Zone				MPLS-Transport-VR			
P-SLA		:	W-ST-Student01-LAN-VR-INET			tvi-0/602.0				
WAMP		1	W-ST-Student01-LAN-VR-MPLS							
aaS App Monitor			host							
RRP										

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

Networking Services Objects & Objects &	Q, Search		∇		+ Add 🗐 Delete 🔲 🗸
Q Search			Name	Network Type	Interfaces
Interfaces		ı	INET		vni-0/0.0
WLAN		1	MPLS		vni-0/1.0
T1/E1 Auth		1	Student_LAN		vni-0/2.0
Virtual Wires	Rows per page	25 🗸 Show	ving 1 - 3 of 3		

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

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

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

Networking Services Objects & Objects &	Pools Rules							
Q, Search	Q, Search	V						+ Add 🗿 Delete 🖓 Clone 🔲 -
CGNAT	Name	IP Addresses	Source Port	Routing Instance	Provider Org	Destination Port	Egress Network	Egress Interface
> Stateful Firewall	DIA-Pool-INET			INET-Transport-VR			INET	
> IPsec	Pool-INET		AUTOMATIC				INET	
> SDWAN	Pool-MPLS		AUTOMATIC				MPLS	
> Layer 2 SDWAN	Damage (05	Den 1 0 4 0						
State State <th< th=""><th>Pools Rules</th><th>V</th><th></th><th></th><th></th><th></th><th></th><th>+ Add 🔋 Delete 🖓 Clone 🔳 🗸</th></th<>	Pools Rules	V						+ Add 🔋 Delete 🖓 Clone 🔳 🗸
CGNAT	Name	Precedence	NAT Mode	Source IP	Destination IP	Source Pool	Destination Pool	LEF Profile
> Stateful Firewall	DIA-Rule-Stude	nt01-LAN-VR	napt-44			DIA-Pool-INET		
> IPsec				10.0.0/8	10.0.0/8			
> SDWAN	RFC_1918_NoTi	ranslate 100		172.16.0.0/12 192.168.0.0/16	172.16.0.0/12 192.168.0.0/16			
> Layer 2 SDWAN	Speed-Test-INE	r.	napt-44			Pool-INET		
Web Proxy	Speed-Test-MPL	S	napt-44			Pool-MPLS		

©Copyright 2022 Versa Networks

Exercise 5: Test the Security Rules

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

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

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

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

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

Rule 1 Test

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

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



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

VEDGA	ector View Appliance View	Template View						Ë (i) Stude	nt01 (Stude
Mon	nitor Analytics C	onfiguration Administr	ration						C	ommit Tem
ganization Student01	~			③ You are curr	rently in Appliance View					
Summary B Devices	Cloud Workload									
otal Appliances 3	501B01 ×									
1B01 San Diego, CA, USA mt. Address: 172.15.0.4 .tem Bridge Address: 0A:6E	A D:DC:C8:25:00						© Reachable	SYNC: IN_SYNC	Up since: Fri Ju	n 21 05:40:21
mmary Services Net	working System Tools					Cor	nfiguration Shell	Config Status*	Upgrade	Subscrip
SFW SDWAN CG	NAT SDLAN IPsec	Sessions SCI Secure A	APM							
oos Policies Policies	Sessions Zone Protectio	n								
Default-Policy	~)									
							Searc	h	C	
ile Name 🗢	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	L	ist Hit Time	
ck-Outbound-SSH-INT	3	3	180	0	0	3	Fri Jun 21 11:30:	18 2024 F	ri Jun 21 11:30	37 2024
	0	0	0	0	0	0	Fri Jun 21 08:46:	55 2024 F	ri Jun 21 08:46	5:55 2024
llow-Inbound-ICMP-B2B	0									

Rule 2 and Rule 3 Test

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

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

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

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

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

SFW SDWAN CGN	AT SDLAN IPsec Se	essions SCI Secure Acce	ss APM					
DoS Policies Policies	Sessions Zone Protection							
Default-Policy	~							
							Search	C" 🖬 🔻 Clear
Rule Name 🕈	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-Outbound-SSH-INT	3	3	180	0	0	3	Fri Jun 21 11:30:18 2024	Fri Jun 21 11:30:37 2024
Allow-Inbound-ICMP-B2B	0	0	0	0	0	0	Fri Jun 21 08:46:55 2024	Fri Jun 21 08:46:55 2024
Allow-Outbound-ICMP-B2B	1	0	0	0	0	0	Fri Jun 21 11:31:13 2024	Fri Jun 21 11:31:13 2024
Block-Outbound-HTTP-B2B-Hut	b 0	0	0	0	0	0	Fri Jun 21 08:59:23 2024	Fri Jun 21 09:00:26 2024

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

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

The ping command should succeed.

Next you will verify the rule success using Versa Analytics.

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

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

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

Rule 4 Test

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

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

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

Monitor tab verification

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

Analytics Tab Verification

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

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

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

Rule 5 Test

Rule Name: Allow-Local-Outbound-Internet

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

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

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

Monitor Tab Verification

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

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

Versa Analytics Verification

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

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

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



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



DoS Protection

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

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

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

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

Look for these hints to help you in the labs

Exercise 2:

In the following lab exercises, you will:

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

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

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

Step 2.1: Reset the lab to a base configuration

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

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

	Direct	or View Appliance Vi	ew Template View							Ê (3) Student01(Student01) -
V LR.	Monit	or Configuratio	n Workflow	Administration	Analytics						Commit Template
Commit Te	mplate To Selec	t Devices									×
O All the A	Associated Template	s Only	Selected Templates	Ø							Hide Filters
Organizati Student0	lon • 01		~				Auto Merge	Overwrite	•		
Select Devi	rices By 📲		~	Template-S01-NGFW		~	Reboot after commit				Fetch Devices
Select Dev	vices (1) Q Sear	ch		V						>	Remove Selection 🔲 🖛
•	Devices	Device	Туре	Appliance Tags	Te	mplate State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
🗆 s	501B02	branch			4		4	REACHABLE	No	۲	S
😰 s	501B01	branch			4		4	REACHABLE	Yes	۲	B
		٠									
					c	ancel	Review				

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.

Cancel

Ŀ

Sample DoS Profile

Add DoS	Profile					
Name *			22/31			
Classifie	d- <u>DoS</u> -Prof	ile				
Descriptio	n			Tags		
Туре			٨			
O Aggreg	ate Profile			Classified Profil	e	
Classificat	ion Key			Max Sessions		
Select-	-		~			
Flood Prot	ection					
Protocol	Enable	Alarm Rate Packets (seconds)	Activate Rate Packets (seconds)	Maximum Rate Packets (seconds)	Drop Period (seconds)	Actions
ТСР		5	7	10	30	SYN Coc 🗸
UDP		100000	100000	100000	300]
ICMP		5	7	10	30]
Other		100000	100000	100000	300	

VERSA NETWORKS LAB GUIDE

2.3 Create a DoS Policy

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

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

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

2.4 Create Rules in the DoS Policy

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

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

Click OK to finish creating the policy.

.

Sample DoS-Classified-Hub-Rule

neral Source Destination Headers/Schedule I	Enforce			
ame *	23/63			
DoS-Classified-Hub-Rule I				
scription				
35				
		Disable Rule		
			ок	Cancel
d DoS Rule	Enforce			
d DoS Rule eral Source Destination Headers/Schedule E	+NewZone + 🗊 💅	Source Address	+ New Address + New Address Group	+ 🗈 e
d DoS Rule heral Source Destination Headers/Schedule E Source Zone Intf-Student_LAN-Zone	+NewZone + 💼 e ^a	Source Address	+ New Address + New Address Group Source Address Not Configured	+ 🗈 e
d DoS Rule Peral Source Destination Headers/Schedule E Source Zone Source Address Negate	+ New Zone + 🗐 💅	Source Address	+ New Address + New Address Group Source Address Not Configured	+ 0.
d DoS Rule heral Source Destination Headers/Schedule E Source Zone Intf-Student_LAN-Zone Source Address Negate Region +	Enforce + New Zone + 🖻 🕫 💿	Source Address	+ New Address + New Address Group Source Address Not Configured City	+ 0 ,
Id DoS Rule neral Source Source Zone Intf-Student_LAN-Zone Source Address Negate Region +	Enforce + NewZone + 2 ^a State State Not Con	Source Address	+ New Address + New Address Group Source Address Not Configured City City Not Configured	+ 🗈 a
d DoS Rule Terral Source Destination Headers/Schedule E Source Zone Intf-Student_LAN-Zone Source Address Negate Region + 2 Region Not Configured Source Location Negate	Enforce + NewZone + 2 2 ² 3 3 State State Not Con	Source Address	+ New Address + New Address Group Source Address Not Configured City City Not Configured	+ 🗈 a
d DoS Rule heral Source Destination Headers/Schedule E Source Zone Intf-Student_LAN-Zone Source Address Negate Region + g ² Region Not Configured Source Location Negate Custom Geo Circle	Enforce + New Zone + 2 2010	Source Address	+ New Address + New Address Group Source Address Not Configured City City Not Configured	+ 0 :
Id DoS Rule heral Source Source Zone Intf-Student_LAN-Zone Source Address Negate Region + @ Region Not Configured Source Location Negate Custom Geo Circle	Enforce + New Zone + 2 2 3 3 3 3 4 3 4 3 4 4 4 4 5 4 5 4 5 4 5 4	Source Address	+ New Address + New Address Group Source Address Not Configured City City Not Configured	+ 0 :
Introduction Source Zone Intf-Student_LAN-Zone Source Address Negate Region Region Not Configured Source Location Negate Custom Geo Circle	Enforce + New Zone + 2 2% State State State Not Con Custom Geo Circle N	Source Address + a ² a ² ifigured	+ New Address + New Address Group Source Address Not Configured City City Not Configured	+ 0 a

VERSA NETWORKS LAB GUIDE

•

		lew Zone + 🔟 💅	Destination Address	+ NEW MULLIESS + NEW MULLIESS G	roup + 🔟 💅
Add	Address			×	()
Destination					
Region	B-HTTP-80				+ 🗊 🕫
Descr	intion	Т	arc		
Destination	prior.		Add a tag		
Custom Type	*		10 27 13 20/32]	+ 🗉 🖬
			_		
				OK Cancel	Cancel
dd DoS Rule neral Source Desti	nation Headers/Schedule Enforce		Others	OK Cancel	Cancel
Id DoS Rule	nation Headers/Schedule Enforce	,	Others Schedules	OK Cancel	Cancel
Id DoS Rule neral Source Dest	IP Flags	•	Others Schedules Select + Schedule	OK Cancel	Cancel
d DoS Rule neral Source Desti Version Select SCP	IP Flags	•	Others Schedules Select + Schedule	OK Cancel	Cancel
Id DoS Rule neral Source Desti Version Select SCP TL	IP Flags	•	Others Schedules Select + Schedule Service List	OK Cancel	Cancel
Id DoS Rule neral Source Desti Version Select SCP TL ondition	IP Flags	•	Others Schedules Select + Schedule Service List	OK Cancel	Cancel

A

Action Setting Allow Deny O Protect	Aggregate Profile	
Logging Sotting	Select	~
LEF Profile	Classified Profile	
Select V V Default Profile	Classified-DoS-Profile	~
	View Profile	

1.6 Verify the DoS Policy Protection

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

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

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



VERSA NETWORKS LAB GUIDE

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

VEDSA	ector View Appliance View	Template View							(i) Stude	ent01 (Student0
Mo	nitor Analytics Cor	nfiguration Administrat	ion							Commit Templa
Organization Student01	~			④ You are currently and a c	ntly in Appliance View					Bui
Summary 😑 Devices	s 🖂 Cloud Workload									
Total Appliances 3	501B01 ×									
91B01 San Diego, CA, US, gmt. Address: 172.15.0.4 stem Bridge Address: 0A:60	A D:DC:C8:25:00						⊘ Read	chable SYNC: IN_SYNC	Up since: Mon Ju	un 24 08:50:31 2
ummary Services Ne	tworking System Tools						Configuration	Shell Config Statu	• Upgrade	Subscriptic
SDWAN NGFW	TDF CGNAT SDLAN thentication Policies CASB	IPsec Sessions SCI Cloud File Export Decryption	Secure Access APM DLP DNS Filtering	DoS Policies File Filtering	IP Filtering Microsegmer	tation Policies Microse	gmentation Statistics	Persistent Action	Polic	>
SDWAN NGFW Antivirus ATP Aut Default-Policy	TDF CGNAT SDLAN thentication Policies CASB	IPsec Sessions SCI Cloud File Export Decryption	Secure Access APM DLP DNS Filtering	DoS Policies File Filtering	IP Filtering Microsegmer	tation Policies Microse	gmentation Statistics	Persistent Action	Polic	
SDWAN NGFW Authors ATP Authors ATP Authors ATP Authors ATP Authors Attack Attac	TDF CGNAT SDLAN thentication Policies CASB	IPsec Sessions SCI Cloud File Export Decryption	Secure Access APM DLP DNS Filtering	DoS Policies File Filtering OIP Drop Count	IP Filtering Microsegmer	tation Policies Microse DoS Hit Count	gmentation Statistics SCTP Dro	Persistent Action	Polic C	> ⊡ ⊽ Cle Count

Analytics logs record the log messages triggered by the event.

	Monitor	Configuration Workflows Administration Analytics
•	Alarms	>
Dashboard	Authentication	▼ Last day ▼
Ê	ADC	Eile Eiltering DNS Eiltering CASE
Logs	CGNAT	
G	DHCP	
Reporting	DNS	Apply I Clear I Conv Filter
2	EIP	
Admin	Firewall	Threat Severity Application User URL Category URL Repu
	Threat Detection	
	71	

sat Detection Loga > DD03 >										America/Denv	er •
Student01 • all		Last day									
Anti Virus IDP IPGuard	DDoS (CASB RBI VF	P ATP								
DOS threat log											
Show Domain Names											
Set filters here		+ Apply Clear	r Copy Filter								Show 10 🗸 entr
Set filters here	Appliance	Apply Clear Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Show 10 v entr
Set filters here 11 Receive Time 11 Jun 24th 2024, 11:59:29 AM MDT	Appliance S01B01	Apply Clear	Threat Type Flood	Attack Name	Attacker 1	Victim 10.27.13.20	Scan Ports Count	Action Drop	From Zone	To Zone	Show 10 v entr
Set filters here 11 Receive Time 11 Jun 24th 2024, 11:59:29 AM MDT Jun 24th 2024, 11:48:56 AM MDT	Appliance S01B01 S01B01	Apply Clean Threat Severity 1 1	Threat Type Flood Flood	Attack Name ICMP TCP SYN	Attacker 17 V	Victim 10.27.13.20 10.27.13.20	Scan Ports Count 0 0	Action Drop Drop	From Zone (null) (null)	To Zone	Show 10 v entr
Set filters here 11 Receive Time 11 Jun 24th 2024, 11:59:29 AM MDT Jun 24th 2024, 11:48:56 AM MDT Jun 24th 2024, 11:47:21 AM MDT Jun 24th 2024, 11:47:21 AM MDT	Appliance \$01801 \$01801 \$01801 \$01801	Apply Clean Threat Severity 1 1 1	Threat Type Flood Flood Flood Flood	Attack Name ICMP ICP SYN ICMP	Attacker it V	Victim 10.27.13.20 10.27.13.20 10.27.13.20	Scan Ports Count 0 0 0 0	Action Drop Drop Drop	From Zone (null) (null) (null)	To Zone	Show 10 v entr

m

VERSA NETWORKS LAB GUIDE

.

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





.

TCP SYN Flood Verification

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

		_			
	VER		S01 Linux Testing Client SSH	- •	×
	NE	:	🔒 S01 Linux Testing Client SSH 💈		
		۲ آ	SENT (30.14715) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=9998] IP [ttl=64 id=47837 proto=1 csum=0x39a6 SENT (30.15015) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=9999] IP [ttl=64 id=47837 proto=1 csum=0x39a6 SENT (30.15315) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=19000] IP [ttl=64 id=47837 proto=1 csum=0x39a6	iplen=28 iplen=28 iplen=28]] 8
<u>^_</u>	Dashboard	8] SENT (30.1561s) ICMP [10.27.101.20 > 10.27.13.20 Echo request (type=8/code=0) id=60426 seq=10000] IP [ttl=64 id=47837 proto=1 csum=0x39a6]	iplen=28	8
	Ê	53	Max rtt: 1.822ms Min rtt: 0.033ms Avg rtt: 0.359ms		
	Logs	≡	Raw packets sent: 10000 (280.000KB) Rcvd: 11 (308B) Lost: 9989 (99.89%) Tx time: 30.12488s Tx bytes/s: 9294.64 Tx pkts/s: 331.95		
	¢	63	Rx time: 31.12602s Rx bytes/s: 9.90 Rx pkts/s: 0.35 Nping done: 1 IP address pinged in 31.18 seconds student@s01B01-PC - \$./VASEC/TCP-SYN-ATTACK-DD05.sh		
	Reporting	L.	Starting Nping 0.7.01 (https://nmap.org/nping) at 2024-06-24 14:01 EDT		
		=	SENT (0.0275s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0316s) TCP [10.27.101.20:15981 > 10.27.13f20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
		G	SENT (0.0356s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0396s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
	Admin		SENT (0.0437s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0477s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
		Ф.	SENT (0.0517s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0557s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
		٦	SENT (0.0597s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0637s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
		0	SENT (0.0677s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0717s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	
			SENT (0.0758s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip SENT (0.0798s) TCP [10.27.101.20:15981 > 10.27.13.20:80 S seq=3624519957 win=1480 csum=0x43E0] IP [ttl=64 id=22498 proto=6 csum=0x9c90 ip	len=40] len=40]	-
		>			

VERSA NETWORKS LAB GUIDE

.

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

Dir	ector View Appliance View	Template View					Ê	 Student01 (Student0
Mor	nitor Analytics Co	nfiguration Administrat	tion					Commit Templa
ganization Student01	~			③ You are currently and the second	ntly in Appliance View			Bui
Summary 😁 Devices	Cloud Workload							
otal Appliances 3	501B01 ×							
1B01 San Diego, CA, US, mt. Address: 172.15.0.4 tem Bridge Address: 0A:61	A D:DC:C8:25:00						Reachable SYNC: IN_SY	NC Up since: Mon Jun 24 08:50:31 20
mmary Services Net	tworking System Tools					c	onfiguration Shell Config Sta	atus* Upgrade Subscriptio
SDWAN NGFW	TDF CGNAT SDLAN	IPsec Sessions SCI	Secure Access APM					
Antivirus ATP Aut	hentication Policies CASB	Cloud File Export Decryption	DLP DNS Filtering	DoS Policies File Filtering	IP Filtering Microsegmen	ation Policies Microsegment	tation Statistics Persistent Action	n Polic < >
Default-Policy	~							
							Search	C III V Clea
ule Name 🕈	UDP Drop Count	ICMP Drop Count	ICMPv6 Drop Count	OIP Drop Count	TCP Syn Drop Count	DoS Hit Count	SCTP Drop Count	Session Drop Count
	0	9989	0	0	3730	4	0	0
loS-Classified-Hub-Rule	•							
DoS-Classified-Hub-Rule	·							

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

/ERS	A Director View Appliance View Monitor Configuration	v Template View	ows Administra	ation Analyti	cs						i (i)	Student01 (Stude
1	Threat Detection Logs > DDoS >										America/Denve	r *
	Student01 • all		Last day	•								
	Anti Virus IDP IPGuard	DDoS C	ASB RBI VI	FP ATP								
	DOS threat log											
	Show Domain Names											
	Set filters here		Apply Clear	r Copy Filter								Show 10 v entr
	Receive Time	11 Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
	Jun 24th 2024, 12:01:16 PM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(nuli)		1
	Jun 24th 2024, 11:59:29 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1
	Jun 24th 2024, 11:48:56 AM MDT	S01B01	1	Flood	TCP SYN		10.27.13.20	0	Drop	(null)		1
	Jun 24th 2024, 11:47:21 AM MDT	S01B01	1	Flood	ICMP		10.27.13.20	0	Drop	(null)		1

The Flood Hits increases in the DDoS Threats dashboard.

StudentO	1	•	all		•	Last day	-				
							1 Threat types	O Threat count	O Critical severity	O High severity	O Medium severity
Web	IP	File	DNS	CASB	RBI	Malware	Vulnerabilities	ATP	DDoS S	ummary	
						Flood			1005		
						Flood Percent: 100 Hits: 4	0.00%				
)					

Click on the chart to view details.

2 Count											
Seese											
0 11:45			11:50		Time		11:55				
					Flood						
DOS Threats (Flood)											
Show Domain Names											
Set filters here		Apply Clear	r Copy Filter								Show 10 🗸 e
Receive Time	Appliance	Threat Severity	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Receive Time Jun 24th 2024, 12:01:16 PM MDT	Appliance S01B01	Threat Severity	Threat Type Flood	Attack Name TCP SYN	Attacker	Victim 10.27.13.20	Scan Ports Count	Action Drop	From Zone	To Zone	Severity Level
Receive Time Jun 24th 2024, 12:01:16 PM MDT Jun 24th 2024, 11:59:29 AM MDT	Appliance S01B01 S01B01	Threat Severity 1 1	Threat Type Flood Flood	Attack Name TCP SYN ICMP	Attacker	Victim 10.27.13.20 10.27.13.20	Scan Ports Count 0 0	Action Drop Drop	From Zone (null) (null)	To Zone	Severity Level
Receive Time Jun 24th 2024, 12:01:16 PM MDT Jun 24th 2024, 11:59:29 AM MDT Jun 24th 2024, 11:48:56 AM MDT	Appliance S01B01 S01B01 S01B01	Threat Severity 1 1 1 1 1 1	Threat Type Flood Flood Flood	Attack Name TCP SYN ICMP TCP SYN	Attacker	 Victim 10.27.13.20 10.27.13.20 10.27.13.20 	Scan Ports Count O O O O	Action Drop Drop Drop	From Zone (null) (null) (null) (null)	To Zone	Severity Level
Receive Time Jun 24th 2024, 12:01:16 PM MDT Jun 24th 2024, 11:59:29 AM MDT Jun 24th 2024, 11:48:56 AM MDT Jun 24th 2024, 11:47:21 AM MDT	Appliance S01B01 S01B01 S01B01 S01B01 S01B01	Threat Severity 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Threat Type Flood Flood Flood Flood Flood	Attack Name TCP SYN ICMP TCP SYN ICMP	Attacker	Victim 10.27.13.20 10.27.13.20 10.27.13.20 10.27.13.20 10.27.13.20	Scan Ports Count 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Action Drop Drop Drop Drop Drop	From Zone (null) (null) (null) (null) (null)	To Zone	Severity Level 1 1 1 1 1 1 1



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



Application Filtering

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

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

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

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

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

- **Note**: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.
- **Note:** The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

Application Filtering and Control

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

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

Lab Objective

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

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

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

Reset the Lab Environment

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

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

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

	DCA	Director Vie	Appliance View	Template Viev	v							i (j	Student01 (Student01)
	NE TWORKS	Monitor	Configuration	Workflow	s Adr	ministration	Analytics						Commit Template
Commit	Template	To Select De	vices										
O All th	e Associated	Templates	Only Se	elected Templates	5	•							Hide Filters
Organiz	ation * S	tudent01		~					Auto Merge	Overwrite	۰		
Select D	Devices By	Template		~	Template	-S01-NGFW		×	Reboot after commi	t 🕐			Fetch Devices
Select [Devices (1)	Q Search				V						×F	emove Selection 🔲 🕇
•	Devices		Device Ty	pe	A	Appliance Tags		Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
	S01B02		branch					4	47	REACHABLE	No	۲	8
	S01B01		branch					4	4	REACHABLE	No	0	8
Chourin	nor 1 . 7							Cancel	Peview				Ċ

- **Note**: Configuration modifications in this lab will be performed in Appliance Context mode (directly on your device) and will not be performed through device templates.
- **Note:** The images in this lab are for demonstration purposes only. Your lab experience may differ from the images provided in the lab guide.

Step 2.1: Configure a rule to block ICMP traffic

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

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

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

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

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

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

VERSA NETWORKS LAB GUIDE

.

Example ICMP Access Rule

Add Rule	×
General Solare Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Name * Block-ICMP-Hub 14/63 14/63 14/63	
Tars	Alias Name
Disable Rule	
	OK Cancel

Add Rule					×
General Source Destination Headers/Sche	dule Applications/URL IoT Security Use	rs/Groups Enforce			
Source Zone	+ New Zone + 💼 💅	Source Address	* New Address + New Address Group + 💼 💅	Source Site Name	a ₈ ⊞ +
Intf-Student_LAN-Zone	۲	Sou	arce Address Not Configured	Source Site Name Not	Configured
Source Address Negate					

Add Rule	×
General Source Destination Headers/Schedule Applications/URL IoTSecurity Users/Groups	
Actions Log Events Start End O Both Never	Profile
	Select V Default Profile

Add Rule			×
General Source Destination Headers/Schedule Applicatio	ns/URL IoT Security Users/Groups Enforce		
Destination Zone	• New Zone + 📋 💅 Destination Address	+ New Address + New Address Group + 💼 🧬 Destination Site	Name + 🗇 🕫
D ptvi	Add Address	×	Destination Site Name Not Configured
Destination Address Negate	Name *		
Region	Hub		+ 🔟 a ⁿ
Region Not Configured	Description	Tags	City Not Configured
Destination Location Negate		Add a tag	
Custom Geo Circle	Туре -	IPv4 Address/Prefix *	
Custom Geo Circle Not Configured	IPv4 ~	10.27.13.20/32	
		ÖK Cancel	OK Cancel

Example ICMP Access Rule

Add Rule				×
General Source Destination Headers/Schedule Applications/URL IoTSecurity Users/Groups Enforce				
Application List + New Application + New Applica	un URL	Category List		+New URL Category + 🗊 💅
C ICMP			URL Category List Not Configured	
URL Reputations +	2.22			
Predefined Reputations Not Configured				
				OK Cancel
Add Rule				×
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce				

General Source Destination Headers/Sc	hedule Applications/URL IoT Security Users/Groups Enforce		
Actions Log			
Actions Allow O Deny Reject Apply	Security Profile	Set-Type Private None	
Synced Flow	Session Timeout (secs)		
Select	~	Send TCP Keep Alive at Session Timeout	

	Appliance View Template View]							🗄 🤅 Stud	ent01(Student01) •
Monitor	Analytics Configuration	Administration								Commit Template
Appliance S01B01 V	Organization Student01	~			④ You a	re currently in Appliance	View			Build
Band Services Objects & Connectors Others	Access Policies Rules									
Q Search	Default-Policy V Q S	earch	∇						+ Add 🗇 Delete 🖓 Clor	ne 🗏 Move 🖬 🕶
CGNAT									Source	
> TDF Rule Num Name Rule Disabled	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	User Defined Devices	Discovered Device	
∨ Next Gen Firewall	1 Block-ICMP-Hub	False		Intf-Student_LAN-Zone						
> DoS	2 Allow_From_Trust	False		Intf-Student_LAN-Zone W-ST-Student01-LAN-						
Decryption	3 Allow_From_SDWAN	False		ptvi						
~ Security	Rows per page 25 v Showing 1	- 3 of 3								

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

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

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

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

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


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

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

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

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

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

	Director View Appliance View	W Template View								L	Stud	entor(Studentor)*
WETWORKS	Monitor Analytics	Configuration Admin	istration									Commit Template
Organization Stu	udent01 V				④ You are currently i	in Appliance View						Build
🖪 Summary 🚍	Devices 🗁 Cloud Workload											
Total Appliances	3 S01B01 ×											
SO1BO1 San Diego Mgmt. Address: 172. System Bridge Addre	30, CA, USA 2.15.0.4 ress: 0A:6D:DC:C8:25:00								Reachable	ble SYNC: IN	SYNC Up since: Mon.	lun 24 08:50:31 2024
Summary Service	ces Networking System Too	ls						Configur	ration Sh	ell Config	Status Upgrade	Subscription
-	_											
SDWAN NGF	GFW TDF CGNAT SDLA	N IPsec Sessions S	SCI Secure Access APM	g DoS Policies	File Filtering IP	Filtering Microsegmentat	ion Policies Micro	segmentation S	Statistics	Persistent Act	tion Polic d	
Default-Policy											_	
Default-Policy	h											Chur
									S	Search	e	
Rule Name 🤤	Hit Count	Forward Packet Count	Forward Byte Count	Reverse P	acket Count	Reverse Byte Count	Inactive Session Co	unt	First Hit Tim	10 00 00 000 1	Last Hit Time	0000004
Block-ICMP-Hub	1	1	84	0		0	1		Mon Jun 24 :	13:02:09 2024	Mon Jun 24 1	3:02:09 2024
							1000		Mon Jun 241	08-53-20 2024	Marc 1	3:01:58 2024
Allow_From_Trust	1200	40775	2859482	18146		18803008	1200		HUIJUITZH	00.33.27 2024	Mon Jun 24 1	
Allow_From_Trust	1200 AN 0	40775 0	2859482 0	18146 0		0	0			00.33.27 2024	- Mon Jun 24 1	$\overline{\mathbf{O}}$
Allow_From_Trust Allow_From_SDWAN	1200 N 0 Director View Appliance Vie Monitor Configurat	40775 0 w Template View ion Workflows	2859482 0 Administration Anal	18146 0 ytics		0	0		-	60.30.272024		ent01 (Student01) • Commit Template
Allow, From_Trust Allow, From_SDWAY	1200 NN 0 Director View Appliance Vie Monitor Configural rall > Logs >	40775 0 w Template View ion Workflows	0 Administration	18146 0 ytics		0	0		-	Americ	- - (i) Stud	ent01 (Student01) • Commit Template
Allow, From_Trust Allow, From_SDWAP VERSA skibboard Stue	1200 NN 0 Director View Appliance Vie Monitor Configural rall > Logs > udent01 • all	40775 0 w Template View ion Workflows	2859482 0 Administration Anal	18146 0 ytics		0	0		-	Americ	- Mon Jun 24 1 	ent01 (Student01)+ Commit Template
Allow, From, Trust Allow, From, SDWA VERSA staboard E	1200 NN 0 Monitor Configural vall > Logs > udent01 • all	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal thour •	18146 0 ytics	0 2	0	0		-			ent01(Student01)+ Commit Template
Allow, From, Trust Allow, From, SDWA' VERSA ushboard Logs	1200 NN 0 Director View Applance Vie Monitor Configurat vall > Logs > udent01 • all	40775 0 w Template View ion Workflows Las	0 Administration Anal thour •	18146 0 ytics	0 2 Data Allowed Total De	0 o	0			Americ	. Mon Jun 24 1	ent01 (Student01)+ - Commit Template - 2
Allow, From, Trust Allow, From, SDWA' VERSA athoused Logs	1200 NN 0 Director View Appliance Vie Monitor Configurat vall > Logs > udent01 • all	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal thour •	18146 0 ytics	0 2 Dtal Allowed Total De	18903008	0			Americ	ca/Denver	ent01(Student01)+ Commit Template
Allow, From, Trust Allow, From, SDWA' VERSA ashboard Logs sporting	1200 NN 0 Director View Appliance Vie Monitor Configural nall > Logs > udent01 • all ogs_Charts Maps	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal	18146 0 ytics	0 2 Dtal Allowed Total De	18903008	0		-	Americ	mon Jun 24 1	ent01(Student01)+
Allow, From, Trust Allow, From, SDWA' Allow, From, SDWA' Contemport astroboard Logs eporting Engenting	1200 NN 0 Director View Appliance Vie Monitor Configural vall > Logs > udent01 • all ogs Charts Maps Firewall logs	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal	18146 0 ytics	0 2 Dtal Allowed Total De	18903008	0			Americ	Ca/Denver	ent01(Student01)+ commit Template
Allow, From, Trust Allow, From, SDWAJ VERSA Version Logs Control Stud Logs Logs Log Log Log Log Log Log Log Log Log Log	1200 NN 0 Director View Appliance Vie Monitor Configural vall > Logs > udent01 • all all ogs Charts Maps Firewall logs Show Domain Names	40775 0 ion Workflows Las	2859482 0 Administration Anal	18146 0 ytics	0 2 Dtal Allowed Total De	18903008	0			Americ	Car/Denver	ent01(Student01)+ commit Template
Allow, From, Trust Allow, From, SDWA' VERSA Allow, From, SDWA' VERSA Provident Studies Studies Admin File Second Studies Second Studies Second Studies	1200 NN 0 Plinctor View Applance Vie Monitor Configural vall > Logs > udent01 • all ogs Charts Maps Firewall logs Show Domain Names Set filters here	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal thour * Apply Clear Copy Filter	18146 0 ytics	0 2 Ital Allowed Total De	18903008	0				Ca/Denver	ent01 (Student01)+ commit Template Commit Template
Allow, From, Trust Allow, From, SDWA' VERSA Institution Institution Logs Exporting Admin	1200 NN 0 Chrector View Applance Vie Monitor Configural all > Logs > udent01 • all ogs Charts Maps Firewall logs Show Domain Names Siet filters here	40775 0 w Template View ion Workflows Las	2859482 0 Administration Anal thour • Apply Clear Copy Filter Iress Destination Address	18146 0 ytics To Source Port	0 2 otal Allowed Total De	Application ¹¹ User	0 URL Category	Protocol	Action	Americ Type ¹ Rul	mon Jul 24 1 .	ent01(Student01)+ commit Template
Allow, From, Trust Allow, From, SDWA' VERSA Institution Studies Logs Logs Logs Logs Log Admin	1200 NN 0 CDirector View Applance Vie Monitor Configurat call > Logs > udent01 • all ogs Charts Maps Grewall logs Show Domain Names Stef fitters here	40775 0 w Template View ion Workflows Las Las Appliance Source Add	Administration Anal Administration Administration Administratio Administration Administration A	18146 0 ytics To Source Port 1 5453	0 2 Dtal Allowed Total De Destination Port 5453	Application User	0 URL Category	Protocol	Action deny	Americ Type ¹⁵ Rul start Bio	Car/Denver Car/Denver Car/Denver Car/Denver Car/Denver	ent01(Student01)+ commit Template Commit Temp
Allow, From, Trust Allow, From, SDWA' VERSA Loss Keportine Admin	1200 N 0 Clirector View Applance Vie Monitor Configurat all > Logs > udent01 all ogs Charts Maps Grewall logs Show Domain Names Stef filters here	40775 0 w Template View ion Workflows Las 4 4 40775 Las 5 4 4 4 4 7 501801 1027.1012 7 501801 1027.1012	Administration Anal thour Administration Anal Anal Comparison	18146 0 ytics TC 5453 5453	0 2 Ital Allowed Total De Destination Port 5 5453 5453	Application ¹³ User ¹³ imp Unknown imp Unknown	0 URL Category	Protocol ¹¹ Icmp	Action 4	Americ Type ¹⁵ Rul start Blo end Blo	Moon Juli 24 1 Car/Denver Car/Denver Show 1 te cck-ICMP-Hub cck-ICMP-Hub	ent01 (Student01)+ commit Template Commit Template Commit Template Commit Template Commit Template E
Allow, From, Trust Allow, From, SDWA' VERSA Loss Loss Admin Admin	1200 N 0 Applance Vie Monitor Configurat all > Logs > udent01 all ogs Charts Maps Grewall logs Show Domain Names fir Reveau Time Jun 24th 2024, 20208 PM MM Jun 24th 2024, 20208 PM MM Jun 24th 2024, 2106-58 PM MM	40775 0 w Template View Ion Workflows Las 40775 Las 40775 Las 501801 10.27.10.12 501801 501801 10.27.10.12 501801 50180000000000	2859482 0 Administration Analysis thour • thour • Apply Clear Copy Filter Instruction • In	18146 0 ytics TC 5453 5453 35650	0 2 tal Allowed Total De Destination Port 5 5453 5453 5453 5453	Application Issociation Initial User Initial User	0 0 URL Category 4 streaming_media	Protocol 1 kmp tcp	Action ²¹ deny deny reject	Type ¹⁵ Rul start Blo start Blo	Moon Juli 24 1 Car/Denver Car/Denver Car/Denver Car/Denver Car/Denver Car/Denver Car/Denver	ent01 (Student01) • commit Template Commit Template Co
Allow, From, Trust Allow, From, SDWA' VERSA Logs Logs Logs Logs Logs Logs Logs Logs	1200 N 0 Applance Vie Monitor Configural all > Logs > udent01 all ogs Charts Maps Greewall logs Show Domain Names firewall logs Jun 24th 2024, 2:02:08 PM MI Jun 24th 2024, 1:06:58 PM MI Jun 24th 2024, 1:06:58 PM MI Jun 24th 2024, 1:06:58 PM MI	40775 0	2859482 0 Administration Analy Athour * Analy * Administration Analy Athour * Apply Clear Copy Filter * Apply Clear Copy Filter * 0 0.27.13.20 0 0.27.13.20 0 bc-in-f93.1e100.net 10 bc-in-f93.1e100.net	18146 0 ytics TC Source Port 5 5453 35650 35650	0 2 tal Allowed Total De 5453 5453 5453 443 443	Application ¹ User inied User <u>fama</u> Unknown yzoutube Unknown yzoutube Unknown	0 0 URL Category streaming, media streaming, media	Protocol icmp icmp itcp itcp	Action ²¹ deny reject	Type ¹³ Ruf start Bio end Bio start Bio end Bio	Moon Juli 24 1 Car/Denver Car/Denver Car/Denver Car/Denver Cch-ICMP-Hub cck-ICMP-Hub cck-APP-Group-Yout cck-APP-Group-Yout cck-APP-Group-Yout	ent01 (Student01) + commit Template

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 predefined applications that are built into the Versa Operating System.

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

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

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

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

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

•

Sample Block-Bit-Torrent Rule

1

Add Rule	×
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	
Name *17//3	
Block-Bit-Torrent	
Description	
lags	Alias Name
Disable Rule	
	OK Cancel
Add Dule	×
	^
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	
Source Zone + New Zone + 💼 👷	*New Address + New Address Group + 💼 👷
Intf-Student_LAN-Zone © Source Addres	Not Configured Source Site Name Not Configured
Source Address Negate	
Add Rule	X
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	
Destination Zone	+ New Address + Hew Address Group +
Intf-INET-Zone (D) Destination Add	ess Not Configured Destination Site Name Not Configured
Destination Address Negate Destination Address Anycast	
Add Rule	
	X
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	X
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	UBL Category List
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	URL Category List + New URL Category + @ g ^p
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application +New Filter +New Group + a a ^B BITTORRENT BITTORRENT APPLICATION	URL Category List + New URL Category + g g ² URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +NewApplication +NewFilter +NewGroup + (i) g ^a BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE	URL Category List + New URL Category + g g ^p URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +hewApplication +hewFilter + hewGroup + @ g ^B BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE	URL Category List +New URL Category + a g ^p URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filter + New Group + BITTORRENT BITTORRENT_BUNDLE URL Reputations	URL Category List +New URL Category List uRL Category Ust Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filter + New Group + @ g ^B BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE VRL Reputations Predefined Reputations: Not Configured	URL Category List +New URL Category + g g ^B URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filter + New Group + in g ^B BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE uRL Reputations VIRL Reputations + in g ^B Predefined Reputations Not Configured	URL Category List +New URL Category + g ^p URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application +New Filter +New Group + and BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE URL Reputations Predefined Reputations Not Configured	URL Category List + New URL Category + g g ^p URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application +New Group +	URL Category List +New URL Category + a a ^p URL Category List Not Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filter + New Group + @ g ^B BITTORRENT BITTORRENT, APPLICATION BITTORRENT, BUNDLE + @ g ^B VRL Reputations + @ g ^B Predefined Reputations Not Configured	VIRL Category List +New URL Category + 2 2 ⁸ URL Category List Configured OK Cancel
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +NewApplication +NewFilter +NewGroup + @ g ^R BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE VRL Reputations Predefined Reputations Not Configured	VIRL Category List URL Category List URL Category List Not Configured OK Caricel
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +NewApplication +NewFiler +NewGroup + @ g ^R BITTORRENT BITTORRENT_BUNDLE URL Reputations Predefined Reputations Not Configured	VIRL Category List + New URL Category List URL Category List Net Configured
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filter + New Group + :::::::::::::::::::::::::::::::::::	VIRL Category List URL Category List URL Category List Not Configured CK Cancel X Set-Tune
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application +New Filer +New Group + BITTORRENT_APPLICATION BITTORRENT_BUNDLE URL Reputations Prodefined Reputations Not Configured	URL Category List +New URL Category + e ^p URL Category List Not Configured OK Cancel Set-Type Public Private: None
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application +New Filter +New Group + g ^{ag} BITTORRENT BITTORRENT APPLICATION BITTORRENT_BUNDLE + URL Reputations + Predefined Reputations Not Configured	URL Category List +New URL Category + g ^p URL Category List URL Category List Not Configured CK Cancel Set-Type Public Private None
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List BITTORRENT BITTORRENT_BUNDLE URL Reputations Predefined Reputations Not Configured	URL Category List +New URL Category + a ⁰ URL Category List +New URL Category + a ⁰ OK Cancel Set-Type Public Private None
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +HewAppRation +HewFilter +He	URL Category List + New URL Category + * *********************************
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Filer + New Group + in g ^R BITTORRENT BITTORRENT_APPLICATION BITTORRENT_BUNDLE + in g ^R VIRL Reputations + in g ^R Prodefined Reputations Not Configured + in g ^R Add Rule	URL Category List + New URL Category + * *********************************
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +New Application + New Group + • • • • • • • • • • • • • • • • • •	URL Category List + New URL Category + * *********************************
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +tex-Application + theor Filter + theor Group + • • • • • • • • • • • • • • • • • •	URL Category List +New URL Category + ***********************************
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce Application List +tex Application +there Filter +there Group + • • • • • • • • • • • • • • • • • •	UBL Category List +New UBL Category + e ² UBL Category List Not Configered OK Cancel OK Cancel X Set-Type • Public Private None

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

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

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

Į										S01 Lir	ux Tes	ting C	lient S
	:	C	2 Q			Rer	nmina Rei	mote Desktop Client	E	=	-		×
.0	÷			RD	P ~				8				
		Nar	me	~	Group	Server	Plugin	Last used					
	83 J	â	S01B01 VOS Device		Student01	10.27.1.101	SSH	2024-06-21 - 11:41:06					
	5.3	â	S01B02 VOS Device		Student01	10.27.1.102	SSH	2024-06-21 - 12:31:42					
>_		8	S01 Linux RDP		Student01	10.27.1.201	RDP	2024-06-24 - 14:01:44					
	=	ŝ	S01 Linux Testing Client	SSH	Student01	10.27.1.201	SSH	2024-06-24 - 14:01:48					
	53												
	2.2												
		F											
	=												
	1												
	Là												
	-	4 <mark>.</mark> 0											
	8												
	100												
	*												
	-												
	0	so	11 Linux PDP (/home/stur	lent	1/local/sh	ace/remmina	/student0	1 rdp s01-linux-rdp 10-27-1-201 remmin	(er				2
	- 1	50	T LINGX RDF (TIOINE/SCOC	rentu	rr.tocatysni	arenennina	Jacobenico	10p_301-000x+0p_10-27-1-201.1e0000		_	_	_	0.0

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

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

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

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

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



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.

Monitor Analytics Configuration Administration Commentation		ector View Appliance View	Template View						Ê	i) Studer	nt01(Student01) •
Organization Studentiti I I I I I I I I I I I I I I I I I I	Mor	itor Analytics Cor	figuration Administrat	ion						C	ommit Template
Summary © Devices © Cloud Workload Total Applances © Silbol × Sollapiances © Reschable SPICEIRESPIC Up since: How Jun 2408:503.512024 Sollapiances © Reschable SPICEIRESPIC Up since: How Jun 2408:503.512024 Soummary Services Networking System Total Configuration Shell Configuration Shell Configuration Shell Configuration Shell Shell Up grade Subscription Soummary Services Networking System Total Source Applance Services Applance Up grade Subscription Source Total Applances NGRW Tof Config Status Up grade Subscription Source Total Applances Config Status Up grade Subscription Source Total Applances Config Status Up grade Subscription Source Total Applances Config Status Dot Policies File Filtering IP Filtering Microsogmentation Policies Microsogmentation Policies Microsogmentation Policies Neon Amplalaplace Subscription	Organization Student01	~			① You are curre	ntly in Appliance View					Build
Total Appliances 3 \$01801 × SOIB01 Sam Diego CA USA Mgmt. Address: 172.151.04 System Bridge Address: 00A GD-DC-C82.500 © Reachable \$VRC: INL, WIC Up since: Mon. Jun. 24 08:50:31.2024 Summary Services Networking \$ystem Tools Configuration Shell Configuration Shell Configuration Subscription SOWAN NGFW TDF GONAT SDLAN Presc Sectores APM Artivirus ATP Authentication Puicles CASB Cloud File Export Decryption D/P DNS Filtering D/S Filtering IP Filtering Microsegmentation Puicles Microsegmentation Statistics Persistent Action Polic > Explanate Hit Count Forward Packet Count Reverse Packet Count Reverse Packet Count Reverse Packet Count First Hit Time Last Hit Time Block-Bit-Torrent 6 18 9672 6 Mon.Jun.241305:22024 Mon.Jun.241305:22024 Mon.Jun.241305:20204 Mon.Jun.241305:20204 Mon.Jun.241305:20204 Mon.Jun.241305:20204 Mon.Jun.241305:20204 Mon.Jun.241305:20204 Mon.Jun.241305:302:002	Summary Devices	Cloud Workload									
SDB01 SnDlego CAUSA Merrit 721504 System Bridge Address: VAGDDCCR32500 Smethall Sindlego CAUSA Merrit 721504 Merrit 721504 Smethall Sindlego Causa Merrit 721504 Merrit 721504 Smethall Sindlego Causa Merrit 721504 Smethall Sindle	Total Appliances 3	S01B01 X									
Services Networking System Totis Upgrade Subscription SDWAN NGPW TDF GGNAT SDLAN Presc Secure Access APM Artivirus AT Authentication Policies CASB Cloud File Export Decryption D/P DNS Filtering D/S Filtering IP Filtering Microsegmentation Policies Microsegmentation Statistics Persiterit Accion Polic< > Default-Policy v <t< th=""><th>S01B01 San Diego, CA, USA Mgmt. Address: 172.15.0.4 System Bridge Address: 0A:60</th><th>0:DC:C8:25:00</th><th></th><th></th><th></th><th></th><th></th><th>🕝 Reachabl</th><th>e SYNC: IN_SYNC U</th><th>Ip since: Mon Ju</th><th>24 08:50:31 2024</th></t<>	S01B01 San Diego, CA, USA Mgmt. Address: 172.15.0.4 System Bridge Address: 0A:60	0:DC:C8:25:00						🕝 Reachabl	e SYNC: IN_SYNC U	Ip since: Mon Ju	24 08:50:31 2024
SDWAN NGFW TDF CGNAT SDLAN IPsec Session SCI Secure Access APM Arthvirus AT Authentication Policies CASB Cloud File Export Decryption DLP DNS Filtering DOS Policies File Filtering Microsegmentation Policies Microsegmentation Statistics Persistent Action Polic > Default-Policy v	Summary Services Net	working System Tools					Co	onfiguration She	Config Status	Upgrade	Subscription
Arthivins ATP Authentication Policies CASB CASB Decryption DLP DNS Filtering DoS Policies Filtering Microsegmentation Policies Microsegmentations Statistics Persistent Action Polic > Default-Policy	SDWAN NGFW 1	DF CGNAT SDLAN	IPsec Sessions SCI	Secure Access APM							
Cefault-Policy ✓ Search C □ ▼ Clear Rule Name * Nit Count Forward Packet Count Reverse Packet Count Reverse Dyte Count Inactive Session Count First Nit Time Last Hit Time Block ICMP Hub 1 84 0 0 1 Mon Jun 241302:09 2024 Mon Jun 241302:09 2024 Block Bit-Torrent 6 18 9672 6 Mon Jun 241305:29 2024 Mon Jun 241305:29 2024 Allow From Trust 1286 40775 2859482 18146 18803008 1200 Mon Jun 241305:33 2020 PM	Antivirus ATP Aut	hentication Policies CASB	Cloud File Export Decryption	DLP DNS Filtering	DoS Policies File Filtering	IP Filtering Microsegmer	ntation Policies Microsegment	ation Statistics	Persistent Action	Polic <	>
Rule Name * Mit Count Forward Packet Count Reverse Packet Count Reverse Packet Count Reverse Packet Count Inactive Session Count First Hit Time Last Hit Time Block-HCMPHub 1 1 84 0 0 1 Mon.Jun.2413.002.092.0024 Mon.Jun.2413.002.092.0024 Block-Bit-Torrent 6 18 9672 6 Mon.Jun.2413.052.2024 Mon.Jun.2413.052.2024 Allow From.Trust 1286 40775 2859482 18146 1800308 1200 Mon.Jun.2413.053.2024 Mon.Jun.2413.053.2024	Default-Policy	~									
Rule Hame 4 Hit Count Ferward Packet Count Reverse Packet Count Reverse Packet Count Inatileve Session Count First Hit Time Last Hit Time Block-HCMP-Hab 1 4 6 0 0 1 Mon Jun 241302:092024 Mon Jun 241302:092024 Block-Hit-Forment 6 18 4066 18 9672 6 Mon Jun 241305:292024 Mon Jun 241305:292024 Allow_Form_Trust 126 40775 265942 18146 1803008 1200 Mon Jun 241305:392024 Mon Jun 241305:392024								Se	arch	C	🗉 🗸 Clear
Block ICMP Hub 1 84 0 0 1 Mon Jun 24 1302:09 2024 Mon Jun 24 1302:09 2024 Block Bit-Torrent 6 1% 4086 18 9672 6 Mon Jun 24 1305:29 2024 Mon Jun 24 1305:29 2024 Allow From, Trust 1286 40775 2859482 18146 1803008 1200 Mon Jun 24 1305:32 2024 Mon Jun 24 1305:33 2024	Rule Name 🕈	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	L	ast Hit Time	
Block-Bit-Forment 6 1% 4086 18 9672 6 Mon Jun 24 1305:22 2024 Mon Jun 24 1305:22 2024 Allow From, Trust 1286 40775 2859482 18146 18803008 1200 Mon Jun 24 0853:22 2024 Mon Jun 24 1305:32 2024	Block-ICMP-Hub	1	1	84	0	0	1	Mon Jun 24 1	3:02:09 2024	Mon Jun 24 13:	02:09 2024
Allow From Trust 1286 40775 2859482 18146 18803008 1200 Mon Jun 24 08.53.29 2024 Mon Jun 24 13.05.33 202	Block-Bit-Torrent	6	18	4086	18	9672	6	Mon Jun 24 1	3:05:22 2024	Mon Jun 24 13:	05:29 2024
	Allow_From_Trust	1286	40775	2859482	18146	18803008	1200	Mon Jun 24 0	3:53:29 2024	Mon Jun 24 13:	05:33 202

78

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

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

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

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

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

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

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

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

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

A

Example Rule

Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Name * Block-Streaming-Video 121/63
Description
Terc Alise Name
Disable Rule
OK Cancel
Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Source Zone Terra Zone Terra Zone Terra Zone Terra Zone Terra Zone Zone Zone Zone Zone Zone Zone Zone
Source Address Negate
Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Destination Zone +New Zone + 🖻 🖉 Destination Address +New Address Group + 🗊 g ^B
Intf-INET-Zone Destination Address Not Configured Destination Address Not Configured
Destination Address Negate Destination Address Anycast
Add Rule
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce
Application List + New Application + New Filter + New Group + a g ²
Application List Not Configured URL Category List Not Configured
URL Reputations + 🖹 a ^R
Predefined Reputations Not Configured
Add Application Group X
Name * Anno Graum-Youthube-Notfliv
Approroup-routube-retrix
Description Tags
NEIFLIX
OK

A

Example Rule

Add Rule	×
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	
Actions Log	
Actions Allow Deny OReject Apply Security Profile	Set-Type Public Private None
Synced Flow Session Timeout (secs)Select	Send TCP Keep Alive at Session Timeout
Add Rule	×
General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce	

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce		
Actions Log		
Events Start End O Both Never	ProfileSelect V	Default Profile

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

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

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

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

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



	www.netflix.com - Chromium	- + X
🛇 www.netflix.com x +		
← → C ③ netflix.com	*	😖 Incognito
😗 Versa Director Login 🗧 ESPN 🛤 Fox Sports 📕 US Bank 😰 YouTube 🕌 Netflix - W	Vatch TV 🚯 Facebook 🔞 Instagram 🥥 Spotify - Web Player 🐌 Music and Podcast 🥹 Malware Test 🔇 Hub Web Server	
	μ. L	
	This site can't be reached	
	The connection was reset.	
	Try	
	Checking the connection	
	Checking the proxy and the firewall	
	ERR_CONNECTION_RESET	
	Details	

82

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

Update the application group to include other applications

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

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

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

am	App-Group-Youtube-Netflix		
)esc	ription	Tags	
	Applications .		, p ³ a ₂ ≡ +
	NETFLIX		
	YOUTUBE		
	INSTAGRAM		
	PANDORA		

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

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

Verify access rule statistics in Versa Director

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

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

	Director View Appliance View	Template View						(i) Student01(Student01)*
	fonitor Analytics Co	nfiguration Administra	ation					Commit Template
Organization Student0	11 ~			③ You are currently	ently in Appliance View			Build
SO1BO1 San Diego, CA, U Mgmt. Address: 172.15.0.4 System Bridge Address: 0A	USA 4 4:6D:DC:C8:25:00						Reachable SYNC: IN_SY	NC Up since: Mon Jun 24 08:50:31 2024
Summary Services I	Networking System Tools					Co	onfiguration Shell Config Sta	tus• Upgrade Subscription
Antivirus ATP J	Authentication Policies CASB	Cloud File Export Decryptic	on DLP DNS Filtering	DoS Policies File Filtering	IP Filtering Microsegme	entation Policies Microsegment	ation Statistics Persistent Action	n Polic < > C* Œ ∀ Clear
Rule Name 🕈	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Block-ICMP-Hub	k ¹	1	84	0	0	1	Mon Jun 24 13:02:09 2024	Mon Jun 24 13:02:09 2024
Block-Bit-Torrent	12	36	8172	36	19344	12	Mon Jun 24 13:05:22 2024	Mon Jun 24 13:07:00 2024
Block-Streaming-Video	154	438	113238	426	223168	154	Mon Jun 24 13:08:41 2024	Mon Jun 24 13:11:31 2024
Allow_From_Trust	1714	45/40	4121734	20170				
	1/18	45613	4121/54	271/7	30558627	1529	Mon Jun 24 08:53:29 2024	Mon Jun 24 13:11:34 2024

Configure a custom Twitter application

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

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

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

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

A

ame * Custom-Twi	tter-APP					
escription *						
Custom Twitter Applic	ation					
ecedence * 100		Application	Timeout (seconds)			
tributes Match Info	rmation				Application match ba	ised on IPS signature 🛛 🔘
- 11	C 1 5 1	D: 1	D 1 1 1	Application Tags		
amily	Sub Family	KISK	Productivity	Security	SDWAN	General
Business-system	Antivirus	01	01	Anonymizer	Audio_stream	AAA
General-internet	Audio_video	0 3	0 3	Bandwidth	AV	Adult_content
Media Authentication		Authentication				
Networking	O Behavioral	5	0.5	Dataleak	Business	Advertising
Networking	 Behavioral Compression Database 	ं 5	ं 5	Dataleak	Business	Advertising Analytics
Networking	Behavioral Compression Database Encrypted Encrypted-tunnel		5	Dataleak	Business Cloud Data	 Advertising Analytics Anonymizer OK Cancel
Id Custom Applica	Behavioral Compression Database Encrypted Encrypted-tunnel		5	Dataleak	Business Cloud Data	 Advertising Analytics Anonymizer OK Cancel
Id Custom Applica	Behavioral Compression Database Encrypted Encrypted-tunnel		5	Dataleak	Business Cloud Data	 Advertising Analytics Anonymizer OK Cancel
Id Custom Applications Custom Twitter Applications	Behavioral Compression Database Encrypted Encrypted-tunnel		5	Dataleak	Business Cloud Data	 Advertising Analytics Anonymizer OK Cancel
Id Custom Applica Id Custom Twi Id Custom Twi Id Custom Twi Id Custom Twitter Applica Id Custom Twitter Applica Id Custom Twitter Applica	Behavioral Compression Database Encrypted Encrypted-tunnel tter-APP	Application	Timeout (seconds)	Dataleak Evasive Filetransfer	Business Cloud Data	 Advertising Analytics Anonymizer OK Cancel
Id Custom Applica ame * Custom-Twi escription * Custom Twitter Applica ecedence * 100	Behavioral Compression Database Encrypted Encrypted-tunnel tter-APP	Application	Timeout (seconds)	Dataleak Evasive Filetransfer	Business Cloud Data Application match b	Advertising Analytics Anonymizer OK Cancel Cancel
Media Networking Netwo	Behavioral Compression Database Encrypted Encrypted-tunnel tter-APP ation	Application	Timeout (seconds)	Dataleak Evasive Filetransfer	Business Cloud Data Application match b	Advertising Analytics Anonymizer OK Cancel Cancel
Media Networking	Behavioral Compression Database Encrypted Encrypted-tunnel tter-APP	Application	Timeout (seconds)	Dataleak Evasive Filetransfer	Business Cloud Data Application match b	Advertising Analytics Anonymizer OK Cancel Cancel
Media Networking	Behavioral Compression Database Encrypted Encrypted-tunnel tter-APP ation tter-APP	Application	Timeout (seconds)	ddress	Business Cloud Data Application match b + @ F ↑ ↓ ± 0 Source Port	Advertising Analytics Anonymizer OK Cancel assed on IPS signature
Media Networking	Behavioral Compression Database Encrypted Encrypted-tunnel The second se	Application	Timeout (seconds)	ddress Source Port V	Business Cloud Data Data Application match b + • • • • • ± •	Advertising Analytics Anonymizer OK Cancel Assed on IPS signature

Name * Custom-Gmail		
lost Pattern .*twitter.* 11/63	Protocol Value	
in Address IP Address/Mask	Destination Address	IP Address/Mask
Source Port		
🔾 Value 🗍 Range		
Source Port Value Low	High	
Destination Port		
O Value Range		
	1.0.4	
Destination Port Value Low	High	

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

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

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

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

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

Example Rule

A

Add Rule										×
General Source Destination	Headers/Schedule Applications/URL	IoT Security Users/Gro	oups Enforce							
Name · Block-Custom-Twitter	Т			20/63						
Description										
Add Rule										×
General Source Destination	Headers/Schedule Applications/UPI	InT Security Litears/Gra	upr Enforce							
General Source Destination i	Headers/ schedule Applications/ OKL	ior security Osers/Gro	Jups Enlorce							
Source Zone	+ New Zon	• + 💼 🖉 🗐	Source Address	+ N	ew Address + New Address G	roup + 🗊 💅	Source Site Name			+ © ₂²
Intf-Student_LAN-Zone		۲		Source Address Not	Configured			Source Site Name	Not Configured	
Source Address Negate										
Add Rule										×
General Source Destination	Headers/Schedule Applications/URL	IoT Security Users/Gre	oups Enforce							
Destination Zone			Destination Address		an Address 1 March Address		Destination fit- 11-	me		1 6 8
Intf-INFT-Zone	+ New Zon	<u>۲ ۳ ۳</u>	Destination Address	+ N Destination Address N	lot Configured		Descination site Na	Destination Site Na	me Not Configured	⊤ <u></u> 12 ⁻
Destination Address Negato			estination Address Ame	vcast						
- Provinsion Address negate			Ally	y						
Add Rule										×
		1.70 1. 11 10								~
General Source Destination	Headers/Schedule Applications/URL	IoT Security Users/Gro	oups Enforce							
Application List		+ New Application	n + New Filter + New Group	+ 🖻 a ^p	URL Category List				+ New URL	Category + 📋 🖉
Custom Twitter ADD										
Customerwitter-AFF							URL Category List Not	Configured		
CustonPrwitterAFF							URL Category List Not	Configured		-
Add Rule					-		URL Category List Not	Configured		×
Add Rule General Source Destination	Headers/Schedule Applications/URL	loT Security Users/Gr	oups Enforce				URL Category List Not	Configured		×
Add Rule General Source Destination Actions Lot	Headers/Schedule Applications/URL	loT Security Users/Gr	oups Enforce				URL Category List Not	Configured		×
Add Rule General Source Destination Actions Lot	Headers/Schedule Applications/URL	loT Security Users/Gr	oups Enforce		Set-Type		URL Category List Not	Configured		×
Add Rule General Source Destination Actions Actions Actions Actions Reject	Headers/Schedule Applications/URL	loT Security Users/Gr	oups Enforce		Set-Type O Public O Private	• O None	URL Category List Not	Contigured		×
Add Rule General Source Destination Actions Actions Actions Actions Contemportation Reject	Headers/Schedule Applications/URL	loT Security Users/Gr	oups <u>Enforce</u>		Set-Type ● Public ○ Private	s 🔿 None	URL Category List Not	Configured		×
Add Rule Actions Acti	Headers/Schedule Applications/URL	IoT Security Users/Gr	oups Enforce		Set-Type O Public O Private	t O None	URL Category List Not	Configured		×
Add Rule Actions Compared Com	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL	IoT Security Users/Gr	oups <u>Enforce</u>		Set-Type Public Private	t ONOR	URL Category List Not	Configured		×
Add Rule General Source Destination Actions Actions Actions Add Rule General Source Destination Add Rule General Source Destination Actions Log	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL	IoT Security Users/Gr	oups Enforce		Set-Type Public Private	None	URL Category List Not	Configured		×
Add Rule General Source Destination Actions Allow Deny Reject Add Rule General Source Destination Actions Log Events Start End (Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never	IoT Security Users/Gr	oups <u>Enforce</u>		Set-Type Public Private Profile	i 🕜 None	URL Category List Nor	Configured		×
Add Rule Actions Add Rule Actions Actions Actions Actions Ceneral Source Destination Add Rule Ceneral Source Destination Ceneral Source Central Ceneral Ce	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never	IoT Security Users/Gr	oups Enforce		Set-Type Public Private ProfileSelect	n Onne	URL Category List Not	Default Profile		×
Add Rule General Source Destination Actions Actions Actions Actions Callow Deny Reject Add Rule General Source Destination Actions Log Events Start End	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never	IoT Security Users/Gr	oups <u>Enforce</u>		Set-Type Public Private ProfileSelect	t ONORE	URL Category List Not	Default Profile		×
Add Rule General Source Destination Actions Actions Add Rule General Source Destination Actions Log Events Start Events Start End	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never	IoT Security Users/Gr	oups <u>Enforce</u>		Set-Type Public Private ProfileSelect	s None	URL Category List Not	Default Profile		×
Add Rule General Source Destination Actions Actions Allow Deny Reject Add Rule General Source Destination Actions Log Events Start End	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules	IoT Security Users/Gr	oups Enforce		Set-Type Public Private Profile Select	• None	URL Category List Not	Default Profile	+ AM @ Detes: 100	X
Add Rule General Source Destination Actions Ations Allow Deny Reject Add Rule General Source Destination Actions Log Events Start Events Start Conector Others Conector CGNAT	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy v Q Se	IoT Security Users/Gr	oups Enforce		Set-Type Public Private ProfileSelect	n None	URL Category List Not	Default Profile	+ Add @ Deleter @ C	X
Add Rule General Source Destination Actions Actions Actions Actions Ceneral Source Destination Actions Log Events Start Events Convertis Convertis Convertis Convertis Convertis Convertis Convertis Convertin	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy V Q Se Rule Name	IoT Security Users/Gr IoT Security Users/Gr arch	oups Enforce	Zone	Set-Type Public Private ProfileSelect Region	t None	URL Category List Not	Default Profile Site Name	+ Add @ Deleter @Q Source User Defined Device	X X
Add Rule General Source Destination Actions Log Add Rule General Source Destination Actions Log Events Start End Start End CGNAT > TDF Vext Gen Firewall	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy Security Profile Rule Num Name 1 Block-ICMP-Hub	IoT Security Users/Gr IoT Security Users/Gr IoT Security Users/Gr arch Rule Disabled /	oups Enforce	Zone Zone	Set-Type Public Private ProfileSelect Region e	None	URL Category List Not	Default Profile Site Name	+ Add @ Deleter @ C Source User Defined Devic	X
Add Rule General Source Destination Actions Log Add Rule General Source Destination Actions Log Events Start End General Source Destination Actions Log Events Start End General Source Destination Actions Log Events Start Ones General Source Destination Actions Log Events Start Ones CGNAT > DDF Vex Gen Firevall > DoS > Authoriting Construction	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy V Security Profile Rules Rules Default-Policy V Security V Security Policies Rules Rules Both Default-Policy V Security V Security V Security V Security V V V Security V V V Security V V V V V V V V V V V V V V V V V V V	IoT Security Users/Gr IoT Security Users/Gr IoT Security Users/Gr arch Rule Disabled 4 False 5	oups Enforce	Zone Intf-Student_LAN-Zon Intf-Student_LAN-Zon	Set-Type Public Private ProfileSelect Region e e e	h None	URL Category List Not	Default Profile Site Name	+ Add Delete O Source User Defined Device	Kone = Move - +
Add Rule General Source Destination Actions Log Add Rule General Source Destination Actions Log Events Start End General Source Destination Actions Log Events Start End Start CGNAT > DoS > Authentication > Decryption	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy Security Profile Rule Name 1 Block-ICMP-Hub 2 Block-Bi-Torrent 3 Block-Streaming-Video 4 Block-Custon-Twitter	IoT Security Users/Gr IoT Security Users/Gr arch Rule Disabled / / False False False	oups Enforce	Zone Intf-Student_LAN-Zon Intf-Student_LAN-Zon Intf-Student_LAN-Zon	Set-Type Prublic Private ProfileSelect Region e e e e e e e e e e e e e e e e e e e	None Address	URL Category List Not	Default Profile Site Name	+ Add @ Detete @Q Source User Defined Devic	X X X X X X X X X X X X X X X X X X X
Add Rule General Source Destination Actions Actions Add Rule General Source Destination Actions Add Rule General Source Destination Actions Log Events Start Events Start Events Start Events Converting Others Converting Others Converting Others Converting Others Start Destination Destinat	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy Security Security Security Security Security Profile Both Never Rule Name Biock-ICMP-Hub Biock-Streaming-Video 4 Biock-Streaming-Video 5 Allow, From, Trust	IoT Security Users/Gr IoT Security Users/Gr IoT Security Users/Gr Rule Disabled False	oups Enforce	Zone Inff-Student_LAN-Zon Inff-Student_LAN-Zon Inff-Student_LAN-Zon Inff-Student_LAN-Zon	Set-Type Prublic Private Profile Select Region	Address	URL Category List Not	Default Profile Site Name	+ Add Deters OC Source User Defined Device	
Add Rule General Source Destination Actions Actions Add Rule General Source Destination Actions Add Rule General Source Destination Actions Log Events Start End General Start CGNAT TDF VNext Gen Firewall DDS Authentication Destryption Security Policies	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy V Security Security Security Profile Rule Num Name Both Never Rule Num Name Biock-ICMP-Hub Biock-ICMP-Hub Biock-Streaming-Video Allow From Trust 6 Allow From SDWAN	IoT Security Users/Gr IoT Security Users/Gr IoT Security Users/Gr Rule Disabled 4 False 4 False 4 False 4 False 4 False 4	oups Enforce	Zone Intf-Student, LAN-Zon Intf-Student, LAN-Zon Intf-Student, LAN-Zon Intf-Student, LAN-Zon VST-Student, LAN-ZON	Set-Type Public Private ProfileSelect Region R	t None	URL Category List Not	Default Profile Site Name	+ Add Delse Q C Source User Defined Devic	X
Add Rule General Source Destination Actions Log Add Rule General Source Destination Actions Log Events Start End CGNAT > TDF < Next Gen Firewall > DoS > Authentication > Decryption < Security Policies > Profiles > Profiles	Headers/Schedule Applications/URL t Apply Security Profile Headers/Schedule Applications/URL Both Never Access Policies Rules Default-Policy Security Profile Rule Name Rule Name Biock-ICMP-Hub Biock-CitMP-Hub Biock-CitMP-	IoT Security Users/Gr IoT Security Users/Gr IoT Security Users/Gr Rule Disabled Users/Gr False False False False False False False False V	oups Enforce	Zone Intf-Student_LAN-Zon Intf-Student_LAN-Zon Intf-Student_LAN-Zon Intf-Student_LAN-Zon W-ST-Student01-LAN- Ptvi	Set-Type Public Private ProfileSelect Region Region Point Private Profile Profi	Address	URL Category List Not	Default Profile	+ Add Deleter (PC Source User Defined Devic	X

.

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.

STOP

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



URL Filtering

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

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

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

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

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

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

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

Director View Appliance View Monitor Configuration	Template View Workflows Administration Analytics	🖹 (i) Student01 (Student01) • Commit Template
Organization Select Option	③ You are currently in Director View	Workflows > Devices > Devices 🤇
Infrastructure • Template • Devices •		
	Image: Service template Bind Data REVIEW	
	Configure Basic	
		Device Name: S01B01
Basic	Global Device ID * Organization *	
501B01	101 Student01	~
Deployment Type CPE-Baremetal Device	Serial Number Device Group + V SN-501801 DG-501-NGFW	~

Step 1.2: Commit the default configuration to your device

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

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

VFI	Director Vie	Appliance View Template Vie	rw.					i (j	Student01(Student01) -
• •	Monitor	Configuration Workflow	ws Administration A	nalytics					Commit Template
Commit	Template To Select De	vices							×
O All th	e Associated Templates	Only Selected Template	es 🕐						Hide Filters
Organiz	sation * Student01	~			Auto Merge	Overwrite	•		
Select D	Devices By + 1 Template	~	Template-S01-NGFW	~	Reboot after comm	nit 💿			Fetch Devices
Select D	Devices (1) Q Search		V					×R	move Selection 🔲 👻
۰	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association
	S01B02	branch		4	47	REACHABLE	No	۲	8
	S01B01	branch		4	4	REACHABLE	No	0	8
Chousie	na 1 - 7								÷
				Cancel	Beview				(D)

Step 2.1: Configure cloud lookup for current URL reputations

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

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

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

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

Click OK when finished.

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

	Cloud Profile
Name:	Cloud-URL-Profile
Connection Pool:	100
Source NAT Pool:	Cloud-NAT-Pool
Туре:	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 \nearrow to modify the settings.

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

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

Click OK when finished.

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

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

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

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

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

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

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

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

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

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

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

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

Step 2.5: Test the URL filtering

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

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

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

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

https://facebook.com

The site should be blocked by the VOS device.

Browse to https://espn.com

The site should be blocked.

Browse to https://instagram.com

The site should be blocked.

Browse to https://spotify.com

The site should be allowed.

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

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

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

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

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

Step 2.7: Test your changes to the URL Filter profile

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

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

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

Return to Versa Director.

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

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

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

97

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

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

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

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

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

Step 2.9: Finish the lab and exit the lab environment

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

Log out of Versa Director.



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



IP Filtering

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

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

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

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

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

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

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

VERSA Monitor Configuration	Template View Workflows Administra	ation Analytics				:::	Student01 (Student01) • Commit Template
Organization Select Option			③ You are currently in Director	View			Workflows > Devices > Devices C
Infrastructure • Template • Devices •							
	1 BASIC	2 LOCATION INFORMATION	3 DEVICE SERVICE TEMPLATE	BIND DATA	3 REVIEW		
			Configure Basic				
							Device Name: S01B01
Basic							
Name *		Global Device ID *			Organization *		
S01B01					Student01		~
Deployment Type		Serial Number			Device Group *		
CPE-Baremetal Device	~	SN-S01B01			DG-S01-NGFW		~

Step 1.2: Commit the default configuration to your device

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

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

											* 0		
VE	RSA 🗧	Director View	Appliance View	Template View								Student01(Student01) -	
V · -	M	onitor (Configuration	Workflows	Administrati	n Analytics						Commit Template	
Commit	Commit Template To Select Devices X												
O All th	O All the Associated Templates Only Selected Templates O												
Organiz	ation * Stude	nt01		~				Auto Merge	Overwrite	Ø			
Select D	levices By +0												
bucctb		Template		× T	Template-S01-NGFW		~	Reboot after commit				Fetch Devices	
Select [Devices (1)	Search				∇					×Re	move Selection 🛛 🛨	
۰	Devices		Device Type	e	Appliance Ta	ţs	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association	
	S01B02		branch				4	47	REACHABLE	No	۲	8	
	S01B01		branch				4	47	REACHABLE	No	0	8	
Chourin	na 1 - 7						Consel	Deview					
	_						Cancer	Genew				-	

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

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

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

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

Step 2.2: Create a custom IP Filter profile

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

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

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

Click OK to finish creating the profile.

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

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

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

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

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

Step 2.4: Adjust the default NAT rules

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

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

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

Step 2.5: Test the IP Filter profile

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

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

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

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

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

Step 2.6: Verify the IP filter profile in Versa Director

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

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

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

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

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

Step 2.7: Verify the IP Filter profile in Versa Analytics

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

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

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

Ltd IP Filtering A	Action (Reject)											
□ Show Doma	ain Names											
Search: Click to	set a filter											Show - 🗸 entries
Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action	Source Reputation	Destination Reputation	Source White List
Sep 11th 2020, 1:41:24 PM PD T	Branch110	172.16.110.110	192.168.20.105	56660	80	tcp	IP- Filtering- Profile	BlackList	reject			
4												•
Showing 1 to	1 of 1 entries										Previo	us 1 Next

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

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

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

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

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

Click OK to apply the changes.

Step 2.9: Test the geo-location IP Filtering profile

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

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

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

Step 2.10: Verify the Geo-location IP Filter results

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

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

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

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

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

IP Filtering Action (drop-p	IP Filtering Action (drop-packet)												
Show Domain Names													
Set filters here Apply Clear Copy Filter Show 10 v entries													
Receive Time	Appliance	Threat Severity	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action	Source Reputation	Destination Re	
Jun 25th 2024, 7:52:27 AM MDT	S01B01		10.27.101.20	195.208.218.98	5933	5933	icmp	IP-Filtering-Profile	GeoLocationRule	drop-packet			
Showing 1 to 1 of 1 entries											Previou	is 1 Ne	

Example Output

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

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

Step 2.11: Add IP Reputation to the IP Filtering profile

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

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

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

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

Click OK to finish updating the profile.

Step 2.12: Test the IP Reputation profile

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

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

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

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

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

Step 2.13: Finish the lab and exit the lab environment

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

Log out of Versa Director.



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



Antivirus and IDP

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

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

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

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

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

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

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

VERSA	Director View	w Appliance View	Template View						 (j)	Student01 (Student01) -
NETWORKS	Monitor	Configuration	Workflows	Administra	ation Analytics					Commit Template
Organization Se	elect Option	~				④ You are currently in Director	View		Workflow	vs > Devices > Devices
Infrastructure •	Template • De	evices 👻								
			ВА	1 ASIC	2 LOCATION INFORMATION	3 DEVICE SERVICE TEMPLATE	BIND DATA	REVIEW		
						Configure Basic				
										Device Name: S01B01
Basic										
Name *					Global Device ID *			Organization *		
S01B01								Student01		~
Deployment Type					Serial Number			Device Group *		
CPE-Baremetal De	evice			~	SN-S01B01			DG-S01-NGFW		~

Step 1.2: Commit the default configuration to your device

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

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

								Ê (j)	Student01 (Student01) -				
VE	RSA Director View	Appliance View Template View						0					
	Monitor Co	nfiguration Workflows	Administration Analytics						Commit Template				
Commit	Commit Template To Select Devices ×												
O All the Associated Templates Only Selected Templates 0													
Organiz	ation * Student01	~			Auto Merge	Overwrite	2						
Select D	evices By + 10												
	Template	Templ	ate-501-NGFW	×	Reboot after commit 🕯	Ð			Fetch Devices				
Select E	Devices (1) Q Search		∇					×F	emove Selection 🔲 🖛				
•	Devices	Device Type	Appliance Tags	Template State	Appliance State	Appliance Reachability	Device Modified	Differences	Association				
	S01B02	branch		4	4	REACHABLE	No	۲	8				
	S01B01	branch		4	4	REACHABLE	No	0	8				
Chourin	ur 1 - '2			Cancel	Porteur								
				Cancer	eview								

Step 2.1: Configure SSL Decryption using SSL Forward Proxy

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

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

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

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

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

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

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

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

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

Step 2.2: Test HTTPS access to an Internet site

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

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

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

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

In the Manage Certificates window, select the Authorities tab, then click Import to import the certificate. Set it to be used to authenticate web sites and email. Once the certificate is imported, you can continue with the lab.
109

VERSA NETWORKS LAB GUIDE

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

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

ame * ssl-proxy-profile	
lescription	Tags
Enable Profile	Ipport Session Ticket 🥑 Use Extended Master Secret
ype • Truste	ed Certificate Database • CA Certificate •
SSL Forward Proxy V defa	ault v ssl-cert v
LEF Profile	
Select	~
Default Profile	
LEF Log Level	
Alert	~
dd Decryption Profile	OK Cancel
dd Decryption Profile eneral SSL Inspection SSL Protocol Advance	OK Cancel
dd Decryption Profile eneral SSL Inspection SSL Protocol Advance OCSP Block Unknown Certification	OK Cancel
dd Decryption Profile eneral SSL Inspection SSL SSL Protocol Advance OCSP Enabled Block Unknown Certifica CRL Check Fetch issuer u	OK Cancel
dd Decryption Profile eneral SSL Inspection SSL Inspection SSL Protocol Advance DCSP Enabled Block Unknown Certificat CRL Check Fetch issuer u Server Certificate Checks Action for Expired Certificate	OK Cancel
dd Decryption Profile eneral SSL Inspection SSL Inspection SSL Protocol Advance OCSP Enabled Block Unknown Certificate CRL Check Fetch issuer u Server Certificate Checks Action for Expired Certificate Action Allow Aler	OK Cancel ed
dd Decryption Profile eneral SSL Inspection SSL Inspection SSL Protocol Advance OCSP Enabled Block Unknown Certificate CRL Check Fetch issuer u Server Certificate Checks Action for Expired Certificate Action JIow Aler Unsupported Mode Checks Action for Unsupported Cipher	OK Cancel ed
	OK Cancel ed
	OK Cancel ed
add Decryption Profile eneral SSL Inspection SSL Protocol Advance OCSP Enabled Block Unknown Certificat CRL Check Fetch issuer u Server Certificate Checks Action for Expired Certificate Allow Unsupported Mode Checks Action for Unsupported Cipher Alert	OK Cancel ed

A

Add the following decryption rules to the default decryption policy:

Add Decryption Rule	
General Source Destination Headers/Schedule URL Users/Groups Enforce	
Name * Forward-Proxy	
Description	8
Tags	
Add Decryption Rule	
General Source Destination Headers/Schedule URL Users/Groups Enforce	
Source Zone	+ New Zone + 💼 💅
Intf-Student_LAN-Zone	۲
Source Address Negate	
Add Decryption Rule	
General Source Destination Headers/Schedule URL Users/Groups Enforce	
Destination Zone	+ New Zone + 🔟 💅
Intf-INET-Zone	۲
Destination Address Negate	

Add Decryption Rule			
General Source Destination Header	s/Schedule URL Users/Groups Enforce		
Action Setting	Action Override		Decryption Profile *
Action *	URL Filtering		ssl-proxy-profile
decrypt	✓Select	~	View Decryption Profile

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

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

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

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



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

Configure Antivirus profiles to scan encrypted traffic

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

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

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

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

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

Click OK to create the profile.

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

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

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

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

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

Step 2.8: Verify the SSL decryption and Antivirus scanning

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

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

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



115

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

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

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

The files should not be downloaded and should be blocked.

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

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

Summary Services Networking System Tools		Configuration Shell Config Status [*] Upgrade Subscription
SDWAN NGFW TDF CGNAT SDLAN IPsec Sessions SCI S	ecure Access APM	- Politica Messacrossicale Postalator - Posta
Antwirus AIP Authentication Policies CASB Cloud Pile Export Decryption	ULP DRSHittering DosPolicies Hile Hittering IP Hittering Microsegnentatio V V User Defined File Type V	n Policies Microsegmentation statistics Persistent Action Polic ()
		zip C III V Clear
File Type 🗢	Scan Count	Block Count
gzip	0	0
zip	0	2
7zip	0	0
bzip2	0	0
j		

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

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

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

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

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

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

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

Step 2.10: Verify results using Versa Director

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

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

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

From within the terminal window, execute the following command

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

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

Step 2.11: Verify the results using Versa Director

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

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

Step 2.12: Verify results using Versa Analytics

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

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

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

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

Step 2.13: Configure Intrusion Detection (alert only)

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

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

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

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

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

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

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

119

Step 2.14: Verify the threat detection without prevention

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

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

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

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

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

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

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

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

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

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

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

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

Click *OK* to create the exemption.

Step 2.16: Verify the exemption

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

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

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

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

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

Step 2.17: Finish the lab and exit the lab environment

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

Log out of Versa Director.



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