Palo Alto Networks Firewall 11.1 Essentials: Configuration and Management

Lab Guide

PAN-OS[®] 11.1 EDU-210 Courseware Version A

Palo Alto Networks, Inc.

https://www.paloaltonetworks.com

© 2024, Palo Alto Networks, Inc.

Palo Alto Networks, PAN-OS, WildFire, RedLock, and Demisto are registered trademarks of Palo Alto Networks, Inc. All other marks mentioned herein may be trademarks of their respective companies.

Table of Contents

Table of Contents	4
Typographical Conventions	
Lab Guidance	
Browsers	
Lab 1: Palo Alto Networks Portfolio and Architecture	
Lab 2: Configuring Initial Firewall Settings	
Lab Objectives	
High-Level Lab Steps	
Connect to Your Student Firewall	25
Apply a Baseline configuration to the Firewall	25
Configure the DNS and NTP Servers	25
Configure General Settings	25
Modify Management Interface	25
Commit the configuration	25
Check for New PAN-OS Software	25
Detailed Lab Steps	
Connect to Your Student Firewall	26
Apply a Baseline configuration to the Firewall	26
Configure the DNS and NTP Servers	29
Configure General Settings	30
Modify Management Interface	31
Check for New PAN-OS Software	
Commit the configuration	34
Lab 3: Managing Firewall Configurations	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	37

Save a Named configuration Snapshot	
Export a Named configuration Snapshot	
Revert Ongoing configuration Changes	
Preview configuration Changes	
Modify System Log File Columns	
Create a System Log File Filter	
Use the Filter Builder	
Detailed Lab Steps	39
Apply a Baseline configuration to the Firewall	
Save a Named configuration Snapshot	
Export a Named configuration Snapshot	40
Revert Ongoing configuration Changes	42
Preview configuration Changes	45
Modify System Log File Columns	47
Create a System Log File Filter	49
Use the Filter Builder	51
Lab 4: Managing Firewall Administrator Accounts	56
Lab Objectives	56
High-Level Lab Steps	57
Apply a Baseline configuration to the Firewall	57
Create a Local Database Authentication Profile	57
Create a Local User Database Account	57
Create an Administrator Account	57
Commit the configuration	57
Log in With New Admin Account	57
Configure LDAP Authentication	57
Commit the configuration	58
Log in With New Admin Account	58
Configure RADIUS Authentication	58

Commit the configuration	59
Log in With New Admin Account	59
Configure an Authentication Sequence	59
Commit the configuration	59
Detailed Lab Steps	60
Apply a Baseline configuration to the Firewall	60
Create a Local Database Authentication Profile	60
Create a Local User Database Account	62
Create an Administrator Account	63
Commit the configuration	64
Log in With New Admin Account	64
Configure LDAP Authentication	65
Commit the configuration	69
Log in With New Admin Account	69
Configure RADIUS Authentication	70
Configure an Authentication Sequence	74
Commit the configuration	75
Lab 5: Connecting the Firewall to Production Networks with Security Zones	77
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	78
Create Layer 3 Network Interfaces	78
Create a Layer 3 Interface on ethernet1/1	78
Create a Layer 3 Interface on ethernet1/2	78
Create a Layer 3 Interface on ethernet1/3	79
Create a Logical Router	79
Segment Your Production Network Using Security Zones	79
Commit the configuration	80
Test Connectivity to Each Zone	80

	Test Interface Access before Management Profiles	80
	Define Interface Management Profiles	80
	Apply Allow-ping to ethernet1/1	81
	Apply Allow-mgt to ethernet 1/2	81
	Apply Allow-mgt to ethernet 1/3	81
	Commit the configuration	81
	Test Interface Access after Management Profiles	81
D	etailed Lab Steps	82
	Apply a Baseline configuration to the Firewall	82
	Create Layer 3 Network Interfaces	82
	Create a Layer 3 Interface on ethernet1/1	83
	Create a Layer 3 Interface on ethernet1/2	85
	Create a Layer 3 Interface on ethernet1/3	87
	Create a Logical Router	90
	Segment Your Production Network Using Security Zones	93
	Commit the configuration	96
	Test Connectivity to Each Zone	97
	Create Interface Management Profiles	.100
	Test Interface Access before Management Profiles	.101
	Define Interface Management Profiles	.102
	Apply Allow-ping to ethernet1/1	.103
	Apply Allow-mgt to ethernet 1/2	.104
	Apply Allow-mgt to ethernet 1/3	.105
	Commit the configuration	.106
	Test Interface Access after Management Profiles	.106
Lab	6: Creating and Managing Security Policy Rules	109
L	ab Objectives	110
Η	igh-Level Lab Steps	110
	Apply a Baseline configuration to the Firewall	.110

	Create Security Policy Rule	110
	Commit the configuration	110
	Modify Security Policy Table Columns	111
	Test New Security Policy Rule	111
	Examine Rule Hit Count	111
	Reset the Rule Hit Counter	111
	Examine the Traffic Log	111
	Enable Logging for Default Interzone Rule	112
	Commit the configuration	112
	Ping a Host on the Internet	112
	Create Block Rules for Known-Bad IP Addresses	112
	Create Security Rules for Internet Access	113
	Create Users to Internet Security Policy Rule	113
	Create Extranet to Internet Security Policy Rule	114
	Commit the configuration	114
	Ping Internet Host from Client A	114
D	Detailed Lab Steps	115
	Apply a Baseline configuration to the Firewall	115
	Create a Security Policy Rule	115
	Commit the configuration	120
	Modify Security Policy Table Columns	120
	Test New Security Policy Rule	122
	Examine Rule Hit Count	124
	Reset the Rule Hit Counter	125
	Examine the Traffic Log	126
	Enable Logging for Default Interzone Rule	129
	Commit the configuration	130
	Ping a Host on the Internet	130
	Create Block Rules for Known-Bad IP Addresses	132

Create Security Policy Rules for Internet Access	136
Create Users to Internet Security Policy Rule	136
Create Extranet to Internet Security Policy Rule	
Commit the configuration	144
Ping Internet Host from Client A	144
Lab 7: Creating and Managing NAT Policy Rules	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	147
Create a Source NAT Policy Rule	147
Commit the configuration	148
Verify Internet Connectivity	148
Create a Destination NAT Policy	148
Commit the configuration	149
Test the Destination NAT Rule	149
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	
Create a Source NAT Policy Rule	
Commit the configuration	153
Verify Internet Connectivity	154
Create a Destination NAT Policy	155
Commit the configuration	158
Test the Destination NAT Rule	158
Lab 8: Controlling Application Usage with App-ID	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	
Configure an Application Group	
Configure a Security Policy Rule to Allow Update Traffic	

	Commit the configuration	163
	Test the Allow-PANW-Apps Security Policy Rule	163
	Identify Shadowed Rules	164
	Modify the Security Policy to Function Properly	164
	Commit the configuration	164
	Test the Modified Security Policy Rule	164
	Generate Application Traffic	164
	Research Applications	165
	Update Security Policy Rules	165
	Commit the configuration	166
	Test the Updated Security Policy Rules	166
	Enable the Application Block Page	166
	Commit the configuration	166
	Test the Application Block Page	166
D	etailed Lab Steps	. 167
	Apply a Baseline configuration to the Firewall	167
	Configure an Application Group	167
	Configure a Security Policy Rule to Allow Firewall Update Traffic	168
	Commit the configuration	171
	Test the Allow-PANW-Apps Security Policy Rule	172
	Identify Shadowed Rules	173
	Modify the Security Policy to Function Properly	174
	Commit the configuration	175
	Test the Modified Security Policy	175
	Generate Application Traffic	176
	Research Applications	178
	Update Security Policy Rules	181
	Commit the configuration	185
	Test the Updated Security Policy Rules	185

Enable the Application Block Page	
Commit the configuration	
Test the Application Block Page	
Lab 9: Blocking Known Threats Using Security Profiles	190
Lab Objectives	
High-Level Lab Steps	191
Apply a Baseline configuration to the Firewall	191
Generate Traffic Without Security Profiles	
Create a Corporate Antivirus Profile	191
Create A Corporate Vulnerability Security Profile	
Create a Corporate File Blocking Profile	
Create a Corporate Data Filtering Profile	
Create a Corporate Anti-Spyware Security Profile	
Create an External Dynamic List for Malicious Domains	
Update the Anti-Spyware Profile with EDL	
Commit the configuration	
Create a Security Profile Group	
Apply the Corp-Profiles-Group to Security Policy Rules	
Commit the configuration	
Generate Attack Traffic to Test Security Profiles	
Lab Clean-Up	195
Detailed Lab Steps	196
Apply a Baseline configuration to the Firewall	196
Generate Traffic Without Security Profiles	196
Create a Corporate Antivirus Profile	
Create A Corporate Vulnerability Security Profile	
Create a Corporate File Blocking Profile	
Create a Corporate Data Filtering Profile	
Create a Corporate Anti Spyware Profile	

Create an External Dynamic List for Malicious Domains	206
Update the Anti-Spyware Profile with EDL	209
Commit the configuration	209
Create a Security Profile Group	210
Apply the Corp-Profiles-Group to Security Policy Rules	211
Commit the configuration	212
Generate Attack Traffic to Test Security Profiles	212
Lab Clean-Up	216
Lab 10: Blocking Inappropriate Web Traffic with Advanced URL Filtering	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	217
Test Access to Inappropriate Web Content	217
Create a Security Policy Rule to Block Categories	217
Commit the configuration	218
Test Access to URLs Blocked by the Security Policy	218
Block Access to Inappropriate Web Content Using Security Profile	218
Add the URL Profile to the Corp-Profiles-Group	219
Disable Block-Bad-URLs Rule	219
Commit the configuration	219
Test Access to URLs Blocked by a URL Filtering Profile	219
Create a Custom URL Category	
Use Custom Category to Block URL Access in Security Policy Rule	
Commit the configuration	
Test Access to Custom URLs Blocked by the Security Policy	220
Add Custom URL Category to URL Filtering Profile	220
Commit the configuration	220
Test Access to Custom URLs Blocked by the URL Filtering Profile	221
Create an EDL to Block Malicious URL Access	221

Block Access to the the URL List with a Security Policy Rule	221
Commit the configuration	221
Test Access to URLs Blocked by the EDL in the Security Policy	221
Commit the configuration	221
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	222
Test Access to Inappropriate Web Content	222
Create a Security Policy Rule to Block Categories	223
Commit the configuration	225
Test Access to URLs Blocked by the Security Policy	226
Block Access to Inappropriate Web Content Using A Security Profile	228
Add the URL Profile to the Corp-Profiles-Group	230
Disable Block-Bad-URLs Rule	230
Commit the configuration	231
Test Access to URLs Blocked by a URL Filtering Profile	231
Create a Custom URL Category	233
Use Custom Category to Block URL Access in Security Policy Rule	235
Commit the configuration	235
Test Access to Custom URLs Blocked by the Security Policy	236
Add Custom URL Category to URL Filtering Profile	236
Commit the configuration	237
Test Access to Custom URLs Blocked by the URL Filtering Profile	237
Create an EDL to Block Malicious URL Access	238
Block Access to the URL List with a Security Policy Rule	240
Commit the configuration	240
Test Access to URLs Blocked by the EDL in the Security Policy	241
Commit the configuration	241
Lab 11: Blocking Unknown Threats with WildFire	
Lab Objectives	

High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	244
Create a WildFire Analysis Profile	244
Modify Security Profile Group	244
Update WildFire Settings	245
Set Monitor Log Interval	245
Commit the configuration	245
Test the WildFire Analysis Profile	245
Examine WildFire Analysis Details	245
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	246
Create a WildFire Analysis Profile	246
Modify Security Profile Group	247
Update WildFire Settings	
Set Monitor Log Interval	249
Commit the configuration	
Test the WildFire Analysis Profile	
Examine WildFire Analysis Details	251
Lab 12: Controlling Access to Network Resources with User-ID	
Lab Objecti	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	
Examine Firewall configuration	256
Generate Traffic from the Acquisition Zone	257
Enable User-ID on the Acquisition Zone	257
Modify the Acquisition-Allow-All Security Policy Rule	258
Create Marketing Apps Rule	
Create Deny Rule	
Commit the configuration	259

Generate Traffic from the Acquisition Zone	
Examine User-ID Logs	
Examine Firewall Traffic Log	
Examine Firewall Traffic Log	
Clean Up the Desktop	
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	
Examine Firewall Configuration	
Generate Traffic from the Acquisition Zone	
Enable User-ID on the Acquisition Zone	
Modify the Acquisition-Allow-All Security Policy Rule	
Create Marketing Apps Rule	
Create Deny Rule	
Commit the configuration	
Generate Traffic from the Acquisition Zone	
Examine User-ID Logs	
Examine Firewall Traffic Log	
Clean Up the Desktop	
Lab 13: Using Decryption to Block Threats in Encrypted Traffic	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	277
Test the Firewall Behavior Without Decryption	
Create a Self-Signed Certificate for Trusted Connections	
Create a Decryption Policy Rule for Outbound Traffic	
Commit the configuration	
Test Outbound Decryption Policy	
Export the Firewall Certificate	
Import the Firewall Certificate to configuration browser	

Test Outbound Decryption Policy Again	279
Review Firewall Logs	279
Exclude URL Categories from Decryption	
Commit the configuration	
Test the No-Decryption Rule	
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	
Test the Firewall Behavior Without Decryption	
Create Certificate for Trusted Connections	
Create a Certificate for Untrusted Connections	
Create a Decryption Policy Rule for Outbound Traffic	
Commit the configuration	
Test Outbound Decryption Policy	
Export the Firewall Certificate	
Import the Firewall Certificate	
Test Forward Untrust Certificate	
Test Outbound Decryption Policy Again	
Review Firewall Logs	
Exclude URL Categories from Decryption	
Commit the configuration	
Test the No-Decryption Rule	
Lab 14: Locating Valuable Information Using Logs and Reports	
Lab Objectives	
High-Level Lab Steps	
Apply a Baseline configuration to the Firewall	
Generate Traffic	
Display Recent Threat Information in the Dashboard	
Display Recent Application Information in the Dashboard	
View Threat Information in the ACC	

View Application Information in the ACC	
View Threat Information in the Threat Log	
View Application Information in the Traffic Log	
View Threats Using App Scope Reports	
View Threat Information Using Predefined Reports	
View Application Information Using Predefined Reports	
View Threat and Application Information Using Custom Reports	
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	
Generate Traffic	
Display Recent Threat Information in the Dashboard	
Display Recent Application Information in the Dashboard	
View Threat Information in the ACC	
View Application Information in the ACC	
View Threat Information in the Threat Log	
View Application Information in the Traffic Log	
View Threats Using App Scope Reports	
View Threat Information Using Predefined Reports	
View Application Information Using Predefined Reports	
View Threat and Application Information Using Custom Reports	
Lab 15: Capstone	
Load a Lab configuration	
Configure Networking	
Configure Security Zones	
Configure NAT Policy Rules	
Configure Security Policy Rules	
Create and Apply Security Profiles	
Solutions	
Firewall Interfaces	

Logical Router	
Firewall Default Route	358
Allow-ping Interface Management Profile	358
Allow-ping Interface Management Profile Assigned to ethernet1/2	
Security Zones	
NAT Policy Rules	
Security Policy Rules	
Security Profiles	
Bonus Lab	
Lab Objectives	
Detailed Lab Steps	
Apply a Baseline configuration to the Firewall	
Modify Authentication Settings	
Save the Configuration	
Commit Your Changes and Verify Fix	
Appendix A - GlobalProtect	
Lab Objectives	
11.0 Load the Lab Configuration	
11.1 Configure a Loopback interface	
11.2 Generate Self-Signed Certificates	
11.3 Configure the SSL/TLS Service Profile	
11.4 LDAP Server Profile Configuration	
11.5 Authentication Profile Configuration	
11.6 Configure the Tunnel Interface	
11.7 Configure the Internal Gateway	
11.8 Configure the External Gateway	
11.9 Configure the Portal	
11.10 Host the GlobalProtect Agent on the Portal	
11.11 Create a Security Policy Rule	400
11.12 Create a No-NAT Rule	

Appendix B - Active/Passive High Availability	
Lab Objectives	
14.0 Load a Lab Configuration	
14.1 Display the HA Widget	
14.2 Configure the HA Interface	
14.3 Configure Active/Passive HA	
14.4 Configure HA Monitoring	
14.5 Observe the Behavior of the HA Widget	
Appendix C - Site-to-Site VPN	
Appendix C - Site-to-Site VPN Lab Objectives	
Appendix C - Site-to-Site VPN Lab Objectives 12.0 Load a Lab Configuration	
Appendix C - Site-to-Site VPN Lab Objectives 12.0 Load a Lab Configuration 12.1 Configure the Tunnel Interface	
Appendix C - Site-to-Site VPN Lab Objectives 12.0 Load a Lab Configuration 12.1 Configure the Tunnel Interface 12.2 Configure the IKE Gateway	
Appendix C - Site-to-Site VPN Lab Objectives 12.0 Load a Lab Configuration	
Appendix C - Site-to-Site VPN Lab Objectives 12.0 Load a Lab Configuration	

Typographical Conventions

Convention	Meaning	Example
Bolding	Names of selectable items in the web interface	Click Security to open the Security Rule Page
Consolas font	Text that you enter and coding	Enter the following command:
	examples	a:\setup
		The show arp all command yields this output:
		username@hostname> show arp
		<output></output>
Calibri 11 pt. gray font	Lab step results and explanations	A new zone should appear in the web interface.
Click	Click the left mouse button	Click Administrators under the Device tab
Right-click	Click the right mouse button	Right-click the number of a rule you want to copy, and select Clone Rule
<> (text enclosed in angle brackets)	Denotes a variable parameter. Actual value to use is defined in the Lab Guide document.	Click Add again and select <internal interface=""></internal>

This guide uses the following typographical conventions for special terms and instructions.

How to Use This Lab Guide

The Lab Guide contains exercises that correspond to modules in the Student Guide. Each lab exercise consists of step-by-step, task-based labs. The final lab is based on a scenario that you will interpret and use to configure a comprehensive firewall solution.

The following diagram provides a basic overview of the lab environment:



Lab Guidance

There are two sections for each lab in this guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

You do not need to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Use either one or the other.

Browsers

You will use two different browsers for these lab exercises:

- Configuration Browser use this application to configure the firewall.
- Testing Browser use this application to test features once you have configured the firewall.

There are three browsers available in the lab environment:

- Chromium
- Firefox

Note: For all lab exercises, we recommend always using the Chromium browser as the configuration browser when accessing the FireWall WebUI and Firefox as the testing browser. Chromium has been shown to produce fewer errors than other browsers like Firefox when navigating the FireWall WebUI. Please note that the FireWall WebUI requires a lot of memory, and having more than three browser windows or tabs open at the same time can consume the client's entire memory and consequently slow down the lab. We also recommend you restart your browser at least once a day.

The detailed lab guide sections will let you know which browser to use for each task. In some tasks it instruct you to use a specific browser if necessary.

Lab 1: Palo Alto Networks Portfolio and Architecture

No lab exercise is associated with this module.

Lab 2: Configuring Initial Firewall Settings

Your organization has just received a new Palo Alto Networks firewall, and you have been tasked with deploying it. The first steps will be to connect to the firewall's management interface address and configure basic settings to provide the firewall with network access.



Lab Objectives

- Connect to the firewall web interface
- Load a starting lab configuration
- Set DNS servers for the firewall
- Set NTP servers for the firewall
- Configure a login banner for the firewall
- Set Latitude and Longitude for the firewall
- Configure permitted IP addresses for firewall management

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Connect to Your Student Firewall

• Use the configuration browser to connect to the firewall web interface

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-02.xml** - to the Firewall

Configure the DNS and NTP Servers

- Set the **Primary DNS** Server to **8.8.8.8** and the **Secondary DNS Server** to **192.168.50.53**
- Set the **Primary NTP Server** to **0.pool.ntp.org** and the **Secondary NTP Server** to **1.pool.ntp.org**

Configure General Settings

- Set the **Domain** to **panw.lab**
- Create a Login Banner that says Authorized Access Only
- Set the Latitude and Longitude to reflect the firewall's geographical location in Santa Clara, CA, USA

Modify Management Interface

- Verify that the default gateway for the firewall management interface is set to **192.168.1.1**
- Allow access to the management interface only from the **192.168.0.0/16** network

Commit the configuration

• Commit the changes to the firewall before proceeding

Check for New PAN-OS Software

• Check for new PAN-OS software (but do not upgrade the firewall)

Detailed Lab Steps

Use this section if you prefer detailed guidance to complete the objectives for this lab. We strongly recommend that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Connect to Your Student Firewall

- 1. Launch the configuration browser and connect to https://192.168.1.254. Move past any security warnings until you see the web interface login window.
- 2. Log in to the Palo Alto Networks firewall using the following credentials:

Parameter	Value
Username	admin
Password	Pal0Alt0!

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 3. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 4. Click Load named configuration snapshot:

🚯 PA-VM	DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK	
B		
Setup	Management Operations Services Interfaces Telemetry Content-ID WildFi	re Session HSM
Config Audit	Configuration Management	Device Operations
Administrators	Revert to last saved configuration	Reboot Device
Authentication Profile	Save Save named configuration snapshot	
User Identification	Load Load named configuration snapshot	
Data Redistribution	Load configuration version Export Export named configuration snapshot	Miscellaneous
VM Information Sources X Troubleshooting	Export configuration version	Custom Logos
 Certificate Management Certificates 	Import Import amed configuration snapshot	
Certificate Profile	Import device state	

A Load Named configuration dialog box opens.

5. Click the drop-down arrow next to the Name field and select edu-210-11.1a-02.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

Load Name	d Configuration	?
Name	edu-210-11.1a-02.xml	~
Decryption Key	••••	\sim
	Regenerate Rule UUIDs for selected named configuration Skip Validation	
	ок	Cancel

6. Click **OK** to close the **Load Named configuration** window.

A window should open that confirms that the configuration is being loaded.

7. Click **Close** to close the **Loading configuration** window.

Loading Configuration		
Configuration is being loaded. Please check the Task Manager for its status.		
You should reload the page when the task is completed.		
Close		

8. Click the **Commit** button at the upper right corner of the web interface:



A **Commit** window should open.

9. Leave the remaining settings unchanged and click **Commit**.

Commit			0 🗆	
Only a full commit is avail to the commit.	able at the current t	ime. You may	preview changes or validate the	configuration or add a description
 Commit All Changes 	O Commit All Changes O Commit Changes Made By:(1) admin			
COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
Preview Changes	De Change Sumi	mary 🛃 V	alidate Commit	
Note: This shows all the cha Description	nges in login admin's a	ccessible doma	in.	
			ſ	Commit Cancel

10. Wait until the Commit process is complete.

A **Commit Status** window should open that confirms the configuration was committed successfully.



If you receive a message regarding the deprecated algorithm used to generate the API KeyGen, ignore it. This message will have no effect on the labs.

There is a Bonus Lab at the end of this guide that will show you how to address this issue.

Commit Status

Operation	Commit
Status	Completed
Result	Successful
Details	Configuration committed successfully Local configuration size: 10 KB Predefined configuration size: 16 MB Merged configuration size(local, panorama pushed, predefined): 17 MB Maximum recommended merged configuration size: 17 MB (100% configured)
Commit	

The latest API KeyGen was executed on Mon Oct 16 13:44:22 2023 with the deprecated algorithm. You are advised to configure the more secure API key infrastructure by web interface: Setup -> Management -> Authentiation Settings -> API Key Certificate, or by CLI: set deviceconfig setting management api key certificate

Close

?

11. Click **Close** to continue.

Configure the DNS and NTP Servers

The DNS server configuration settings are used for all DNS queries that the firewall initiates in support of FQDN Address objects, logging, and firewall management.

- 12. In the web interface, select **Device > Setup > Services**.
- 13. Click the **Services** gear icon to open the **Services** window.
- 14. Verify that the **Primary DNS Server** is set to **8.8.8.8**.
- 15. Set the Secondary DNS Server to 192.168.50.53.
- 16. Verify that the Update Server is set to **updates.paloaltonetworks.com**.

Services			
Services NTP			
Update Server updates.paloaltonetworks.com			
Verify Update Server Identity ONS Settings			
DNS	 Servers ONS Proxy Object 		
Primary DNS Server	8.8.8.8		
Secondary DNS Server	192.168.50.53		
Minimum FQDN Refresh Time (sec)	30		
FQDN Stale Entry Timeout (min)	1440		
Proxy Server			



The DNS server settings that you configure do not have to be public servers, but the firewall needs to be able to resolve hostnames such as updates.paloaltonetworks.com and wildfire.paloaltonetworks.com to provide various services such as WildFire® or URL filtering.

- 17. Select the **NTP** tab.
- 18. Set the **Primary NTP Server** to **0.pool.ntp.org**.
- 19. Set the Secondary NTP Server to 1.pool.ntp.org.

Services	(?)
Services NTP	
Primary NTP Server NTP Server Address 0.pool.ntp.org	Secondary NTP Server NTP Server Address 1.pool.ntp.org
Authentication Type None ~	Authentication Type None V
Fridary 1995 Server 4,2,2,2 Servedary 544, Server 192,1,68,50	OK Cours
	OK Cancel

20. Leave the remaining settings unchanged and click **OK** to close the **Services** window.

Configure General Settings

21. Select **Device > Setup > Management**.

- 22. Click the **General Settings** gear icon to open the **General Settings** window.
- 23. In the **Domain** field, enter **panw.lab**.
- 24. In the Login Banner area, enter Authorized Access Only.
- 25. In the Latitude field, enter **37.00**.
- 26. In the **Longitude** field, enter **122.00**.

General Settings		?
Hostname	firewall-a	
Domain	panw.lab	
	Accept DHCP server provided Hostname	
	Accept DHCP server provided Domain	
Login Banner	Authorized Access Only	
	Force Admins to Acknowledge Login Banner	
SSL/TLS Service Profile	None	\sim
Time Zone	UTC	\sim
Locale	en	\sim
Date	2023/10/19	\sim
Time	16:26:00	~
Latitude	37.00	
Longitude	122.00	
	Automatically Acquire Commit Lock	



These coordinates are for Santa Clara, California – headquarters of Palo Alto Networks, Inc.

27. Leave the remaining settings unchanged and click **OK** to close the **General Settings** window.

Modify Management Interface

- 28. Select **Device > Setup > Interfaces**.
- 29. Click the link for **Management**.

🚺 PA-VM	DASHBOARD	ACC MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE
Setup	Management Op	perations Services I	interfaces Telem	ietry Conte	ent-ID WildFire	Session HSM
Config Audit	INTERFACE NAME	ENABLED	SPEE	D	IP ADDRESS	SERVICES ENABLED
Password Profiles	Management		auto-	negotiate	192.168.1.254	Ping,HTTPS,SSH

- 30. Set the **Default Gateway** to **192.168.1.1**.
- 31. Leave the remaining settings unchanged.

Management Interface Settings						
Speed	auto-negotiate \lor					
MTU	1500					
IPV4 IPV6						
ID Address	192 168 1 254					
IF Address	172.100.1.2.54					
Netmask	255.255.255.0					
Default Gateway	192.168.1.1					
Administrative Management Services						

- 32. At the bottom of the **Permitted IP Addresses** area, click **Add**.
- 33. In the **Permitted IP Addresses** field, enter **192.168.0.0/16**.
- 34. In the **Description** field, enter Mgt access from these hosts only.





Verify that you have entered the correct address range in the Permitted IP Addresses field. If you make a mistake and enter the wrong information, you can lose network connectivity to your firewall.

- 35. Leave the remaining settings unchanged.
- 36. Click OK.

Check for New PAN-OS Software

37. Select **Device > Software**.

🚺 PA-VM	DASH	IBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	C DEVI	CE 🖆 Commi
 Certificate Management Response Pages 									
Log Settings Or Server Profiles El Local User Database	11.0.0	1037 MB	2022/11	/17 08:45:28	Downloaded	CURRENTLY ✓	INSTALLED	ACTION Validate Export Install Reinstall	Release Notes
Construction Scheduled Log Export	9.1.15	402 MB	2022/10	0/21 11:47:55				Validate Download	Release Notes
GlobalProtect Client Protect Client Protect Client	10.1.8	461 MB	2022/10)/20 12:52:05				Validate Download	Release Notes

38. Uncheck Preferred Releases and Base Releases to see all available softwares.



39. Select Yes on the following Warning:

Warning



Your choice of Release Type directly impacts your experience in terms of performance, stability, and security.

Preferred releases undergo rigorous testing to ensure stability and optimal performance. By using software versions that are not **Preferred**, you may miss out on the latest and most advanced capabilities, and potentially have a subpar software experience.

Your satisfaction and security of your systems are our top priorities. We appreciate your cooperation in adhering to our recommendations. By doing so, you can fully enjoy the range of capabilities, stability, and security that our software has to offer.

Do you want to Continue?



40. At the bottom of the window, click the **Check Now** button.



41. The firewall will perform a software check with the Palo Alto Networks update servers:



42. When the process is complete, the firewall displays an updated list of available software versions:

11.1.3	728 MB	e58427b247e5db9c10a6a	2024/05/14 15:14:08	Downloaded	~	Validate Export Reinstall	Release Notes
11.1.2	586 MB	4faaee165e2f79190c796	2024/02/25 22:54:18			Validate Download	Release Notes
11.1.2-h12	677 MB	3b22796e5232e358db93	2024/09/05 09:07:23			Validate Download	Release Notes
11.1.2-h9	677 MB	f5f6b106b6f7e6b0a38e2	2024/07/31 08:34:44			Validate Download	Release Notes
11.1.2-h4	586 MB	91deabf4ee40b0f868fd3f	2024/05/09 05:24:26			Validate Download	Release Notes
11.1.2-h3	585 MB	c88b08469c28103acd98c	2024/04/14 08:09:19			Validate Download	Release Notes
11.1.2-h1	586 MB	ae21da966c0f075a479ce	2024/03/13 07:07:45			Validate Download	Release Notes
11.1.1	559 MB	456b1bfb38f7e3b713f56	2023/12/26 10:10:40			Validate Download	Release Notes
11.1.1-h1	565 MB	76bb8a6f821baff5ff6368	2024/04/16 06:17:10			Validate Download	Release Notes
11.1.0-h3	446 MB	40cedfebaadfdf070f1ccb7	2024/04/16 08:51:59			Validate Download	Release Notes
11.1.0-h2	439 MB	ae868344e90941f6cb386	2024/01/07 16:52:41			Validate Download	Release Notes
11.1.0	1179 MB	c504e70e41209f35711a4	2023/11/02 12:02:59	Downloaded 🔀		Validate Export	Release Notes

The list you see will vary from this example. Also, no newer versions of PAN-OS software may be available at the time you carry out these steps.



Do not upgrade your firewall!

Commit the configuration

- 43. Click the **Commit** button at the upper right of the web interface.
- 44. Leave the settings unchanged and click **Commit**.
- 45. Wait until the **Commit** process is complete.
- 46. Click **Close** to continue.



Stop. This is the end of the lab.

Lab 3: Managing Firewall Configurations

Now that you have set up the firewall to allow management access, you need to make certain that you can save, load, and restore configurations to the device. You also need to familiarize yourself with the log files available, and with searching through the logs to find specific events.

Because the firewall is not scheduled to be deployed for a few days, you can spend some time on these tasks without worrying about affecting your production networks.



Lab Objectives

- Load a baseline configuration
- Save a named configuration snapshot
- Export a named configuration snapshot
- Save ongoing configuration changes before a commit
- Revert ongoing configuration changes
- Preview configuration changes
- Examine System and configuration log files
- Create a log file filter
- Use the Filter Builder
High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-03.xml** - to the Firewall

Save a Named configuration Snapshot

• Save the firewall's current configuration file as **firewall-a-<Today's Date>**.

Export a Named configuration Snapshot

• Export the **firewall-a-<Today's Date>** configuration file to the lab host's Downloads folder.

Revert Ongoing configuration Changes

- Change the value for the **Primary DNS Server** to **88.8.8.8** (an easy mistake to make).
- Verify the mistake in the **Services** section
- Use the Revert Changes option to restore the Primary DNS Server to its original setting (8.8.8.8)

Preview configuration Changes

- Modify the SNMP configuration with the following settings:
 - Set the Physical Location to Santa Clara, CA, USA.
 - Set the **Contact** to **Sherlock Holmes**.
 - Set the **SNMP Community String** to **paloalto42**.
- Use the **Preview Changes** option to compare the **Running** configuration to the **Candidate** configuration
- Do not commit changes at this stage

Modify System Log File Columns

- Hide the **Object** column in the System Log display
- Move the **Severity** column to the far left side of the System Log display

Create a System Log File Filter

• Create and apply a filter in the System Log that displays only entries with a **Severity** level of **informational**

Use the Filter Builder

• Use the Filter Builder to create a filter that will display all entries in the **System** log that have occurred in the last 60 minutes

Detailed Lab Steps

Use this section if you prefer detailed guidance to complete the objectives for this lab. We strongly recommend that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-03.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK** to close the **Load Named configuration** window.
- 5. Click **Close** to close the **Loading configuration** window.
- 6. Click the **Commit** button at the upper right of the web interface.
- 7. Leave the remaining settings unchanged and click Commit.
- 8. Wait until the **Commit** process is complete.
- 9. Click **Close** to continue.

Save a Named configuration Snapshot

In this section, you will save the firewall configuration with a specific filename.

- 10. Select **Device > Setup > Operations**.
- 11. Click Save named configuration snapshot.



12. In the Save Named configuration window, enter firewall-a-<Today's Date>.xml

Save N	Name	d Configuration		?
	Name	firewall-a-September-6-2023.xml		\sim
			ок	Cancel

- 13. Click **OK**.
- 14. Click **Close** in the confirmation window.

Save Named Configuration						
Config saved to firewall-a-September-6-2023.xml						
Close						



This process saves the configuration file to a location on the firewall itself.

Export a Named configuration Snapshot

You will now export the saved configuration file **firewall-a-<Today's Date>.xml** from the firewall to your workstation.

15. Under **Device > Setup > Operations > Configuration Management**, click the link for **Export named configuration snapshot**.

Configuration Ma	anagement
Revert	Revert to last saved configuration
	Revert to running configuration
Save	Save named configuration snapshot
	Save candidate configuration
Load	Load named configuration snapshot
	Load configuration version
Export	Export named configuration snapshot
	Export configuration version
	Export device state
Import	Import named configuration snapshot
	Import device state

16. In the Export Named configuration window, use the drop-down list to locate the **firewall-a-<Today's Date>.xml** configuration file.

Export Named Configuration							
	Name	firewall-a-September-6-2023.xml		~			
			OK Cancel	$\mathbf{)}$			

- 17. Click OK.
- 18. The workstation will prompt you to save the file to the Downloads folder.
- 19. On the workstation desktop, open the **Downloads** folder:



- A Home Q :: ← \rightarrow ≡ e, × Name Size Modified Star Recent
 Recent
 firewall-a-September-6-2023.xml 12.2 kB 09:32 ★ Starred * A Home Desktop Documents
- 20. The saved file **firewall-a-<Today's Date>.xml** appears in the folder.

21. Close the **Downloads** folder on the workstation.

Revert Ongoing configuration Changes

As you work on a firewall configuration, it is theoretically possible to make a mistake. In such a situation, you may not remember exactly which changes you have made or where the mistake exists in the configuration, particularly if you have made multiple changes (or multiple mistakes).

Fortunately, you can revert the firewall to the current running configuration. This process essentially erases any of the changes you have made to the working candidate configuration and puts the firewall back at the starting point before you made changes.

In this section, you will change the IP address for one of the firewall's DNS servers. You will then use **Revert Changes** to reset the firewall to the running configuration and remove the mistake.

22. In the firewall web interface, select **Device > Setup > Services**.

23. Edit the **Services** section by clicking the gear icon.

Services		
Services	NTP	
	Update Server updates.	paloaltonetworks.com
	Verify	Update Server Identity
DNS Setti	ngs	
	DNS	• Servers ONS Proxy Object
	Primary DNS Server	88.8.8.8
	Secondary DNS Server	192.168.50.53
Minimum	FQDN Refresh Time (sec)	30
FQDN	Stale Entry Timeout (min)	1440

- 24. Change the value for the **Primary DNS Server** to **88.8.8.8** (an easy mistake to make).
- 25. Click **OK** to close the **Services** window.
- 26. You can see the mistake in place under the Services section:



27. In the upper right corner of the web interface, click the **Changes** button and select **Revert Changes**:



28. In the **Revert Changes** window, leave the settings unchanged:

Changes will be reverted from candidate configuration.								
Revert All Changes Revert Changes Made By:(1) admin								
COMMIT SCOPE TYPE ENTITIES ADMINS								
device-and-network Device and Network Configuration								
Preview Changes D Change Summary								



The **Revert Changes** window allows you to select specific elements of the configuration that you can revert. In this case, because you only made a single change, the **Commit Scope** shows **device-and-network** (which is the portion of the configuration that contains the changes to the DNS server).

- 29. Click Revert.
- 30. Click Close in the Message window:



31. In the **Services** window, notice that the **Primary DNS Server** has been reset to the original value before you mistakenly changed it.



Preview configuration Changes

Before you commit changes to the firewall, you can compare the impending changes with the current configuration settings. This process can be useful to make certain you have the right changes in place before they are implemented on the firewall.

In this section, you will make a minor modification to the firewall and use **Preview Changes** to compare the candidate config to the running config.

32. Modify the SNMP configuration by going to **Device > Setup > Operations** and clicking **SNMP Setup** under the **Miscellaneous** section:



- 33. In the SNMP Setup window, set the Physical Location to Santa Clara, CA, USA.
- 34. For **Contact**, enter **Sherlock Holmes**.
- 35. For SNMP Community String, enter paloalto42.
- 36. Leave the remaining settings unchanged:

SNMP Setup	(Ð
Physical Location	Santa Clara, CA]
Contact	Sherlock Holmes Use Event-specific Trap Definitions	
Version	• V2c ○ V3	_
SNMP Community String	paloalto42	
	OK Cancel)

- 37. Click **OK**.
- 38. Click the **Commit** button.
- 39. In the **Commit** window, click **Preview Changes**:



40. In the Preview Changes window, leave the Lines of Context set to 10:

Preview Chang	ges		?
Lines of Context	10	~	
		OK Cance	

ſ	-6	
	_	✓.
	-	~
	=	- 1
l		_

The **Lines of Context** setting determines how many lines are displayed before and after a change in the configuration file.

- 41. Click **OK**.
- 42. A new browser window appears that displays a side-by-side comparison of the current running configuration (on the left) and the proposed changes in the candidate configuration (on the right):

Dev	evice Config Audit (firewall-a)										
Tue	Tue Sep 6 15:53:49 UTC 2022										
					I						
Leg	end: Added	Modified		Deleted	I						
Loc	al Device Changes				I						
	Running Configuration			Candidate Configuration	I						
264	secondary 192.168.50.5	;3;	264	secondary 192.168.50.53;	I						
265	}		265	5 }	I						
266	}		266	3 }	I						
267	domain panw.lab;		267	domain panw.lab;	1						
268	login-banner "Authorized A	ccess Only";	268	login-banner "Authorized Access Only";							
269	permitted-ip {		269	permitted-ip {							
270	192.168.0.0/16 {			192.168.0.0/16 {							
271	description "Mgt access from these hosts only.";			description "Mgt access from these hosts onl							
272	}		272	2 }							
273	}		273	3							
			274	snmp-setting {							
			275	access-setting {							
			276	version {							
			277	7 v2c {							
			278	snmp-community-string paloalto42;							
			279	}							
			280	}							
	0										



Changes are color coded. Green indicates new elements that have been added. Yellow indicates existing elements that have been modified. Red indicates existing elements that have been deleted.

- 43. Close the configuration comparison window by clicking the \mathbf{X} in the upper right corner.
- 44. Click **Cancel** in the **Commit** window.

Modify System Log File Columns

Although the information in log files varies, the process of examining and searching log files on the firewall is the same. In this section, you will examine and navigate the firewall **System** log. You can later apply the same tasks and techniques while examining any other log file on the firewall, such as the Traffic or Threat logs.

45. Select **Monitor > Logs > System**:

🔶 PA-VM	DASHBOAF	RD AC		POLICIES	OBJ	ECTS NETWORK DEVICE
∽ 🔓 Logs	Q					
🖳 Traffic	RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
时 Threat	09/06 15:57:10	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed
📮 System						succession, initiated by 172.106.1.234
式 Alarms	09/06 15:57:00	general	informational	general		User admin accessed tab: monitor

- 46. Hide the **Object** column by clicking the small **drop-down arrow** in the right portion of any column header.
- 47. Choose Columns.
- 48. Uncheck **Object**:



49. The **Object** column is now hidden:

🚺 PA-VM	DASHBOAF	RD AC		POLICIES	OBJECTS	NETWORK	DEVICE
🗸 🔓 Logs	Q						
ा Traffic	RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION		
📷 Threat 🐼 URL Filtering	09/06 15:57:10	general	informational	general	Connection to Upda updates.paloaltone	ate server: tworks.com complet	ted
🖳 System					successfully, Initiate	ed by 172.168.1.25	4
式 Alarms	09/06 15:57:00	general	informational	general	User admin accessed tab: monitor		



Hiding and displaying log columns is optional but quite useful. Each log file contains different columns, some of which you may not need so you can hide them. There may be columns in certain log tables that are not shown by default, and you can use this process to display hidden columns that you want to view.

50. Drag and drop the **Severity** column to the left-most position in the table:

RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION
	general	informational	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
09/06 15:57:00	general	informational	general	User admin accessed tab: monitor
09/06 15:56:42	general	informational	general	User admin logged in via Web from 192.168.1.20

51. The table now displays **Severity** as the first column:

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	09/06 15:57:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	09/06 15:57:00	general	general	User admin accessed tab: monitor
informational	09/06 15:56:42	general	general	User admin logged in via Web from 192.168.1.20 using https



Reordering columns is also optional; however, you may discover that the information in a specific log file is easier for you to analyze after you customize the columns.

Create a System Log File Filter

Scanning through log files row-by-row is tedious. If you are looking for specific information, you can create filters quickly to display only entries that match certain criteria. All log files support filters.

52. In the **System** log file, click any entry under the **Severity** column that contains **informational**:

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	09/06 15:57:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	Click Here	ral	general	User admin accessed tab: monitor
informational	09/06 15:56:42	general	general	User admin logged in via Web from 192.168.1.20 using https

53. The web interface will automatically build a filter statement with the appropriate syntax to search for all entries that contain **informational** in the **Severity** field:

Q (severity eq inf	formational)	Filter St		
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	09/06 15:57:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	09/06 15:57:00	general	general	User admin accessed tab: monitor
informational	09/06 15:56:42	general	general	User admin logged in via Web from 192.168.1.20 using https

54. Click the Apply Filter button in the upper right corner of the window:



55. The System log display will update to show only those entries that contain **informational** as the **Severity** level.

Note that your firewall may only have informational entries in the System log at this point.

56. Under the **Type** column, click any entry that contains the word **general**:

Q (severity eq informational)					
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION	
informational	09/06 16:12:29	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	
informational	09/06 16:08:01	general	general	Auto update agent found no new IoT updates	
informational	09/06 16:08:01	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254	
informational	09/06 16:02:11	ntpd	restart	NTP restart synchronization performed	

57. The interface will update the syntax to create a combined filter:

SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	09/06 16:12:29	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	09/06 16:08:01	general	general	Auto update agent found no new IoT updates
informational	09/06 16:08:01	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254
informational	09/06 16:02:11	ntpd	restart	NTP restart synchronization performed

58. Click the **Apply Filter** button in the upper right corner of the window:



59. The interface will update the log file to display only those entries that match both conditions:

Q (severity eq informational) and (subtype eq general)						
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION		
informational	09/06 16:12:29	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254		
informational	09/06 16:08:01	general	general	Auto update agent found no new IoT updates		
informational	09/06 16:08:01	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254		
informational	09/06 15:57:10	general	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.254		
informational	09/06 15:57:00	general	general	User admin accessed tab: monitor		

60. Remove the filter by clicking the **Clear Filter** button in the upper right corner of the window:





A good practice is to clear any filters from log file displays before you move to other portions of the web interface. The next time you examine the same log, it will display all results instead of only ones you have previously filtered.

Use the Filter Builder

Clicking the link for a specific entry in a log file will automatically create a simple filter. You can create more complex filters by clicking multiple conditions; however, there are some situations in which this process will not provide you with the kind of criteria you need to complete a search. For long or sophisticated searches, you can use the Filter Builder.

In this section, you will use the Filter Builder to search the **System** log for all entries that have occurred in the last 60 minutes.

- 61. Note the current time on the firewall by selecting the **Dashboard** tab.
- 62. Under the General Information section, scroll to the bottom and locate the Time:

Time Tue Sep 6 16:17:03 2022

Uptime 4 days, 1:37:32

In this example, the firewall time is 16:17:03.

- 63. Write the current time down so you do not forget it.
- 64. Select **Monitor** > **Logs** > **System**.
- 65. Clear any filters you may have in place by clicking the **Clear Filter** button in the upper right corner of the window:



66. Click the **Add Filter** button in the upper right corner of the window:



- 67. In the Add Log Filter window:
 - A. Under the **Connector** column, click **and**.
 - B. Under the Attribute column, click Severity.
 - C. Under the **Operator** column, click **equal**.
 - D. Under the Value column, click informational.
 - E. Click Add.
 - F. Note that the filter field at the top of the window updates to display the correct syntax for this filter:





Do not close this window yet!

- 68. With the same window open, build the second part of the filter:
 - A. Under the **Connector** column, select **and**.
 - B. Under the Attribute column, select Time Generated.
 - C. Under Operator, select greater than or equal to.
 - D. Under the **Value** column, use the first drop-down list to select today.
 - E. Under the **Value** column, use the second drop-down list to select a time approximately sixty minutes ago (round up or down if you need to).
 - F. Click Add.

G. Note that the filter is updated to reflect the additional syntax:



- 69. In the Add Log Filter window, click Apply.
- 70. Your filter will appear in the System log syntax field:

Constant) of mile			q ====; =; , == ===; , =; , =; , =; ,	
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION
informational	09/06 16:17:59	general	general	User admin accessed tab: monitor
high	09/06 16:17:42	url- filtering	url-cloud-connection- failure	CURL ERROR: Could not resolve host: s0000.urlcloud.paloaltonetworks.com
informational	09/06 16:17:11	ntpd	restart	NTP restart synchronization performed

The time and date for your filter will differ from the example shown here.

71. Click the **Apply Filter** button in the upper right corner of the window:



72. The System log display will update to show you only entries that have been generated after the time you specified.



Although you used the System log as the basis for this exercise, the process of creating filters is the same throughout all Palo Alto Networks firewall log databases. The Filter Builder is available to use in all log tables.

73. Clear the filter by clicking the **Clear Filter** button in the upper right corner of the window:



74. Click the **Commit** button at the upper right of the web interface



Stop. This is the end of the lab.

Lab 4: Managing Firewall Administrator Accounts

When you deploy the firewall into your production network, you need to make sure that other members of your team have administrative access to the device. You want to leverage an existing LDAP server that maintains account and password information for members of your team. However, your organization recently merged with another company whose administrative accounts are maintained in a RADIUS database.

No one has had time yet to migrate all the accounts from RADIUS into LDAP, so you need to configure the firewall to check both LDAP and RADIUS to authenticate an account when an administrator logs in.



Lab Objectives

- Load a baseline configuration
- Create a local firewall administrator account
- Configure an LDAP Server Profile
- Configure a RADIUS Server Profile
- Configure an LDAP Authentication Profile
- Configure a RADIUS Authentication Profile
- Configure an Authentication Sequence
- Create non-local firewall administrator accounts

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - edu-210-11.1a-04.xml to the Firewall

Create a Local Database Authentication Profile

- Create a Local Database Authentication Profile called Local-database
- Set the Allow List for the Local-database Profile to all

Create a Local User Database Account

• Create an entry in the Local User Database called adminBob with Pal0Alt0! as the Password

Create an Administrator Account

- Create an Administrator account using the Local Database entry for adminBob
- Set the Authentication Profile to Local-database

Commit the configuration

• Commit the changes to the firewall before proceeding

Log in With New Admin Account

- Log out of the firewall web interface and log back into the firewall with **adminBob** as the **Username** and **Pal0Alt0!** as the **Password**.
- Use the System log to verify that the adminBob account was authenticated by the localdatabase
- Log out of the firewall and log back into the firewall with the **admin/Pal0Alt0!** credentials.

Configure LDAP Authentication

• Use the information in the table below to configure an LDAP Server Profile

Profile Name	LDAP-Server-Profile
Server Name	ldap.panw.lab

LDAP Server IP Address	192.168.50.89
Port field	389
Server Settings Type	Other
Base DN	dc=panw,dc=lab
Bind DN	cn=admin,dc=panw,dc=lab
Password / Confirm Password	Pal0Alt0!
Require SSL/TLS secured connection	unchecked

• Use the information in the table below to create an LDAP Authentication Profile.

Name	LDAP-Auth-Profile
Туре	LDAP
Server Profile	LDAP-Server-Profile
Allow List (Advanced Tab)	all

• Use the information in the table below to create a new administrator account that will be authenticated by LDAP

Name	adminSally
Authentication Profile	LDAP-Auth-Profile

Commit the configuration

• Commit the changes to the firewall before proceeding

Log in With New Admin Account

- Test LDAP Authentication by logging in with the adminSally/Pal0Alt0! credentials
- Use the System log to verify that the **adminSally** account was authenticated using LDAP

Configure RADIUS Authentication

• Use the information in the table below to configure a RADIUS Server Profile

Profile Name	RADIUS-Server-Profile
Authentication Protocol	СНАР
Server Name	radius.panw.lab

RADIUS Server	192.168.50.150
Secret / Confirm Secret	Pal0Alt0!
Port	1812

• Use the information in the table below to create an RADIUS Authentication Profile

Name	RADIUS-Auth-Profile
Туре	RADIUS
Server Profile	RADIUS-Server-Profile
Allow List (Advanced Tab)	all

• Use the information in the table below to create a new administrator account that will be authenticated by RADIUS

Name	adminHelga
Authentication Profile	RADIUS-Auth-Profile

Commit the configuration

• Commit the changes to the firewall before proceeding

Log in With New Admin Account

- Test RADIUS Authentication by logging in with the adminHelga/Pal0Alt0! credentials
- Use the System log to verify that the **adminHelga** account was authenticated using RADIUS

Configure an Authentication Sequence

• Create an authentication sequence called LDAP-then-RADIUS that uses the LDAP-Auth-Profile first and the RADIUS-Auth-Profile second.

Commit the configuration

Commit the changes to the firewall before proceeding

Detailed Lab Steps

Use this section if you prefer detailed guidance to complete the objectives for this lab. We strongly recommend that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-04.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK** to close the **Load Named configuration** window.
- 5. Click **Close** to close the **Loading configuration** window.
- 6. Click the **Commit** button at the upper right of the web interface.
- 7. Leave the remaining settings unchanged and click Commit.
- 8. Wait until the **Commit** process is complete.
- 9. Click **Close** to continue.

Create a Local Database Authentication Profile

- Create a Local Database Authentication Profile by selecting Device > Authentication Profile.
- 11. Click **Add** at the bottom of the window.
- 12. Under the Authentication tab, enter Local-database for the Name.
- 13. For **Type**, use the drop-down list to select **Local Database**.

	(?)
ical-database	
Advanced	
Local Database	~
%USERINPUT%	~
Click "Import" to configure this field X Import	rt
]
	Cancel
	cal-database Advanced Local Database %USERINPUT% Click "Import" to configure this field X Impo

- 15. Select the tab for **Advanced**.
- 16. In the Allow List section, click Add.
- 17. Select all.

Authentication Profile	?
Name Local-database	
Authentication Factors Advanced	
Allow List	
e S all	
1	
+ Add Oelete	
Account Lockout	
Failed Attempts [0 - 10]	
Lockout Time (min) 0	
OK Cance	el



The **Allow List** entries let you to select individual members of the local database if you wish to limit access to the firewall by specific administrators. By selecting **all**, you allow any administrator accounts in the local database to access the firewall.

19. Click OK.

Create a Local User Database Account

In this section, you will create a new entry in the Local User Database on the firewall. This entry will be for a new team member, **adminBob**.

- 20. Select **Device > Local User Database > Users**.
- 21. In the bottom left corner of the window, click Add.
- 22. For **Name**, enter **adminBob**.
- 23. Enter Pal0Alt0! for Password and Confirm Password.

Local User				?
Name	adminBob			
Mode	 Password 	Password Hash		
Password	•••••		Pa1041+01	
Confirm Password	•••••		THIORICO.	
	Enable			
			OK Cancel	\bigcirc

25. Click OK.

Create an Administrator Account

In this section, you will create an administrator account for **adminBob**. The **adminBob** account will use the **Local-database** Authentication Profile.

- 26. Create an Administrator Account from a Local Database user by selecting **Device** > **Administrators**.
- 27. Click **Add** at the bottom of the window.
- 28. For Name, enter adminBob.
- 29. For **Description**, enter **Bob F. superuser admin**.
- 30. For Authentication Profile, use the drop-down list to select Local-database.
- 31. Leave the remaining settings unchanged.

Administrator			(?)
Name	adminBob		
Description	Bob F. superuser admin		
Authentication Profile	Local-database		~
Administrator Type	Use only client certificate au Use Public Key Authenticati Opnamic Role Based	uthentication (Web) on (SSH)	
	Superuser		OK Cancel



When you select Local-database for the Authentication Profile, there is no option to enter a Password for the administrator. The password information for this account is maintained in the Local-database on the firewall.

32. Click **OK**.

Commit the configuration

- 33. Click the **Commit** button at the upper right of the web interface.
- 34. Leave the settings unchanged and click **Commit**.
- 35. Wait until the **Commit** process is complete.
- 36. Click **Close** to continue.

Log in With New Admin Account

37. Log out of the firewall web interface by clicking the **Logout** button in the bottom left corner of the window.



- 38. Log back into the firewall with **adminBob** as the **Username** and **Pal0Alt0!** as the **Password**.
- 39. Close any Welcome windows that appear.
- 40. Select **Monitor > System**.
- 41. Look for an entry with **Type auth**.

RECEIVE TIME	TYPE	SEVERITY	EVENT	DESCRIPTION
09/06 16:42:48	general	informational	general	User adminBob logged in via Web from 192.168.1.20 using https
09/06 16:42:48	auth	informational	auth-success	authenticated for user 'adminBob'. auth profile 'Local-database', vsys 'shared', From: 192.168.1.20.



If you do not see an entry in the System log indicating a successful authentication for adminBob, you can create and apply a filter with (**subtype eq auth**) as the syntax.

- 42. Note that the entry in the firewall system log indicates that adminBob was successfully authenticated against the **Local-database**.
- 43. Log out of the firewall.

44. Log back into the firewall with the **admin/Pal0Alt0!** credentials.

Configure LDAP Authentication

Your organization uses an LDAP server to maintain a database of users, including network administrators. Your team of security personnel is growing each month and you want to leverage the existing LDAP server to authenticate administrators when they attempt to log into the firewall.

The first step in this process is to define an LDAP Server Profile that contains specific information that the firewall can use when sending queries for authentication.

45. Select **Device > Server Profiles > LDAP**.

- 46. At the bottom of the window, click **Add**.
- 47. For **Profile Name**, enter LDAP-Server-Profile.
- 48. Under the **Server List** section, click **Add**.
- 49. In the **Name** field, enter **ldap.panw.lab**.
- 50. In the LDAP Server field, enter **192.168.50.89**.
- 51. Leave the **Port** field set to **389**.
- 52. Under the Server Settings section, verify that the Type is set to other.
- 53. Enter dc=panw, dc=lab for Base DN.
- 54. Enter cn=admin,dc=panw,dc=lab for Bind DN.
- 55. Enter Pal0Alt0! for Password and Confirm Password.
- 56. Uncheck the option for Require SSL/TLS secured connection.
- 57. Leave the remaining settings unchanged.

LDAP Serv	er Profile				?
Profile N	lame LDAP-Server-Profile	;			
	Administrator Use	e Only			
Server List -			Server Settings —		
NAME	LDAP SERVER	PORT	Туре	other	~
Idap.panw.lab	192.168.50.89	389	Base DN	dc=panw,dc=lab	\sim
			Bind DN	cn=admin,dc=panw,dc=lab	
			Password		1011+01
0			Confirm Password	······	ATOATCO:
🕂 Add (-	Delete		Bind Timeout	30	
Enter the IP add	Iress or FQDN of the LDAP se	erver	Search Timeout	30	
			Retry Interval	60	
				Require SSL/TLS secured con	nection
				Verify Server Certificate for S	SL sessions
				ОК	Cancel

Note that there are no spaces between values in the Base DN and Bind DN fields.

58. Click **OK** to create the LDAP Server Profile.

With your LDAP Server Profile in place, you will now create an Authentication Profile and reference the LDAP Server Profile you just created.

- 59. Select **Device > Authentication Profile**.
- 60. Click the **Add** button at the bottom of the window.
- 61. For Name, enter LDAP-Auth-Profile.
- 62. Under the Authentication tab, use the Type drop-down list to select LDAP.

Authentication Profile		?
Name L	DAP-Auth-Profile	
Authentication Factors	Advanced	
Туре	LDAP	~
Server Profile	LDAP-Server-Profile	~
Password Expiry Warning	7	
User Domain	Number of days prior to warning a user about password expiry.	
Username Modifier	%USERINPUT%	\sim
Single Sign On Kerberos Realm	n	
Kerberos Keytal	Click "Import" to configure this field X Import	
	OK Cance	

63. Under Server Profile, use the drop-down list to select LDAP-Server-Profile.

- 64. Select the **Advanced** tab.
- 65. Under the Allow List section, click Add.
- 66. Select all.

Authentication Profile	?
Name LDAP-Auth-Profile	
Authentication Factors Advanced	
Allow List	
S all	
$\overline{\sum}$	
↔ Add ⊖ Delete	
Account Lockout	
Failed Attempts [0 - 10]	
Lockout Time (min) 0	
OK Cance	1

- 68. Click **OK**.
- 69. Create a new administrator by selecting **Device > Administrators**.
- 70. Click Add.
- 71. For **Name**, enter **adminSally**.
- 72. For **Description**, enter Sally C superuser admin.
- 73. For Authentication Profile, use the drop-down list to select LDAP-Auth-Profile.
- 74. Leave the remaining settings unchanged.

Administrator					
(Name	adminSally]
	Description	Sally C superuser admin]
	Authentication Profile	LDAP-Auth-Profile		\sim]
		Use only client certificate	authentication (Web)		
		Use Public Key Authentica	ation (SSH)		
	Administrator Type	 Dynamic O Role Base 	d		
		Superuser		~]
				ОК Cancel	



The adminSally account is one that exists in the LDAP server.

75. Click OK.

Commit the configuration

- 76. Click the **Commit** button at the upper right of the web interface.
- 77. Leave the settings unchanged and click Commit.
- 78. Wait until the **Commit** process is complete.
- 79. Click **Close** to continue.

Log in With New Admin Account

- 80. Log out of the firewall by clicking the **Logout** button in the bottom left corner of the window.
- 81. Log back into the firewall with adminSally as the Username and Pal0Alt0! as the Password.
- 82. Close any Welcome windows that appear.
- 83. Select **Monitor > System**.
- 84. Look for an entry with **Type auth**.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
09/06 16:52:38	general	informational	general		User adminSally logged in via Web from 192.168.1.20 using https
09/06 16:52:38	auth	informational	auth-success	LDAP-Auth- Profile	authenticated for user 'adminSally'. auth profile 'LDAP-Auth-Profile', vsys 'shared', server profile 'LDAP-Server-Profile', server address '192.168.50.89', From: 192.168.1.20.
09/06 16:52:38	auth	medium	auth-server-up		LDAP auth server 192.168.50.89 is up !!!



If you do not see an entry in the System log indicating a successful authentication for adminSally, you can use a filter (**subtype eq auth**) as the syntax.

- 85. Note that the entry in the firewall system log indicates that **adminSally** was successfully authenticated against the **LDAP-Auth-Profile**.
- 86. Log out of the firewall.
- 87. Log back into the firewall with the **admin/Pal0Alt0!** credentials.

Configure RADIUS Authentication

Your organization has recently acquired another company. The newly acquired company maintains all network administrator accounts in a RADIUS server. You need to incorporate RADIUS authentication for the firewall so the new network administrators who have joined your team can access the firewall for management purposes.

- 88. Create a RADIUS Server Profile by selecting **Device > Server Profiles > RADIUS**.
- 89. Click Add.
- 90. For Name, enter RADIUS-Server-Profile.
- 91. For Authentication Protocol, use the drop-down list to select CHAP.



Note: Never use CHAP in a production environment because it is not secure. We are using it in the lab for the sake of simplicity.

- 92. Under the **Servers** section, click **Add**.
- 93. For the server **Name** field, enter **radius.panw.lab**.
- 94. For the **RADIUS Server** field, enter **192.168.50.150**.
- 95. Enter Pal0Alt0! for Secret and Confirm Secret.
- 96. Leave the **Port** set to **1812**.
- 97. Leave the remaining settings unchanged.

RADIUS Server Profile						
Profile Name RADIUS-Server-Profile						
	Administrator Use Only					
Server Settings	Server Settings					
Timeout (sec) 3					
Retrie	s 3					
Authentication Protoco	СНАР		~			
Servers	Servers					
NAME	RADIUS SERVER	SECRET	PORT			
radius.panw.lab	192.168.50.150	•••••	1812			
Add Delete Enter the IP address or FQDN of the RADIUS server						
	(ОК	Cancel			

- 98. Click **OK**.
- 99. Create a **RADIUS Authentication Profile** by selecting **Device > Authentication Profile**.
- 100. Click Add.
- 101. For **Name**, enter **RADIUS-Auth-Profile**.
- 102. For **Type**, select **RADIUS**.
- 103. For Server Profile, select RADIUS-Server-Profile.
- 104. Leave the remaining settings unchanged.

Authentication Profile		
Name RADIUS-Auth-Profile		
Authentication Factors	Advanced	
Туре	RADIUS	~
Server Profile	RADIUS-Server-Profile	~
	Retrieve user group from RADIUS	
User Domain		
Username Modifier Single Sign On	%USERINPUT%	~
Kerberos Realm	1	
Kerberos Keytal	Click "Import" to configure this field X	Import

- 105. Select the **Advanced** tab.
- 106. Under the Allow List section, click Add.
- 107. Select all.

Authentication Profile	?
Name RADIUS-Auth-Profile	
Authentication Factors Advanced	
Allow List	_
🖵 🥵 all	
1	
Account Lockout	
Failed Attempts [0 - 10]	
Lockout Time (min) 0	
OK Cancel	\sum
109. Click OK.

- 110. Create an administrator account for adminHelga (who has recently joined your team from the acquired company) by selecting **Device** > **Administrators**.
- 111.Click **Add**.
- 112. For **Name**, enter **adminHelga**.
- 113. For Description, enter Helga R superuser admin.
- 114. For Authentication Profile, select RADIUS-Auth-Profile.
- 115. Leave the remaining settings unchanged.

Administrator		(?)
Name	adminHelga	
Authentication Profile	RADIUS-Auth-Profile	~
Administrator Type	Use only client certificate authentication (Web) Use Public Key Authentication (SSH) Opynamic ORole Based	
	Superuser	Cancel

116.Click OK.

117. Click the **Commit** button at the upper right of the web interface:



A **Commit** window should open.

- 118. Leave the settings unchanged and click **Commit**.
- 119. Wait until the **Commit** process is complete.
- 120.Log out of the firewall by clicking the **Logout** button in the bottom left corner of the window.
- 121.Log back into the firewall with **adminHelga** as the **Username** and **Pal0Alt0!** as the **Password**.
- 122. Close any Welcome windows that appear.
- 123. Select Monitor > System.
- 124. Look for an entry with **Type auth**.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
09/06 17:01:09	general	informational	general		User adminHelga logged in via Web from 192.168.1.20 using https
09/06 17:01:09	auth	informational	auth-success	RADIUS-Auth- Profile	authenticated for user 'adminHelga'. auth profile 'RADIUS-Auth-Profile', vsys 'shared', server profile 'RADIUS-Server-Profile', server address '192.168.50.150'. auth protocol 'CHAP'. From:
					192.168.1.20.
09/06 17:01:09	auth	informational	auth-success	RADIUS-Auth-	When authenticating user 'adminHelga' from



If you do not see an entry in the System log indicating a successful authentication for adminHelga, you can use a filter (**subtype eq auth**) as the syntax.

- 125. Note that the entry in the firewall system log indicates that **adminHelga** was successfully authenticated against the **RADIUS-Auth-Profile**.
- 126. Log out of the firewall.
- 127.Log back into the firewall with the **admin/Pal0Alt0!** credentials.

Configure an Authentication Sequence

Since the acquisition, some administrator accounts exist in LDAP and other accounts exist in RADIUS. With administrator accounts in these two different systems, you need to configure the firewall so that it can check both external databases when an administrator attempts to log in.

You will accomplish this by creating an Authentication Sequence. The sequence will instruct the firewall to check an account against LDAP first and then against RADIUS if the account does not exist in LDAP (or if the LDAP server is unavailable).

128. Select **Device > Authentication Sequence**.

129. Click Add.

- 130. For Name, enter LDAP-then-RADIUS.
- 131. Under the Authentication Profiles section, click Add.
- 132. Select LDAP-Auth-Profile.
- 133. Click Add again.
- 134. Select RADIUS-Auth-Profile.
- 135. Leave the remaining settings unchanged.

Authentication Sequence	(?)
Name LDAP-then-RADIUS	
Exit the sequence on failed authentication Vise domain to determine authentication profile Use User-ID domain to determine authentication profile	
AUTHENTICATION PROFILES LDAP-Auth-Profile	
RADIUS-Auth-Profile	
<u>1</u>	
(→ Add) Delete ↑ Move Up ↓ Move Down	
ок	Cancel



Note the **Move Up** and **Move Down** buttons. These allow you to change the order of the Authentication Profiles if necessary. In this example, the firewall will use the LDAP-Auth-Profile first when an administrator logs in to attempt authentication; if the user account does not exist in LDAP (or if the LDAP server is unavailable), the firewall will use the RADIUS-Auth-Profile to attempt authentication.

136. Click OK.

Commit the configuration

- 137. Click the **Commit** button at the upper right of the web interface.
- 138. Leave the settings unchanged and click Commit.
- 139. Wait until the **Commit** process is complete.
- 140. Click **Close** to continue.



Stop. This is the end of the lab.

Lab 5: Connecting the Firewall to Production Networks with Security Zones

In preparation for deployment, you need to connect the firewall to the appropriate production networks. You already have cabled the firewall interfaces to the appropriate switch ports in the data center. In this section, you will configure the firewall with Layer 3 IP addresses and a logical router. You also will create security zones that divide your network into separate logical areas so that you have more control over traffic from one segment to another.

When you have the configuration in place on the firewall, you will use ping from different devices to verify connectivity between all the segments.



Lab Objectives

- Load a baseline configuration
- Create Layer 3 interfaces
- Create a Logical router
- Segment your production network using security zones
- Test connectivity from firewall to hosts in each security zone
- Create Interface Management Profiles

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-05.xml** to the Firewall

Create Layer 3 Network Interfaces

Use the information in the tables below to create Layer 3 network interfaces.

Create a Layer 3 Interface on ethernet1/1

Ethernet Interface	ethernet1/1
Comment	Internet connection
Туре	Layer 3
IPv4 Type	Static
IP	203.0.113.20/24

Create a Layer 3 Interface on ethernet1/2

Ethernet Interface	ethernet1/2
Comment	Users network connection
Туре	Layer 3
IPv4 Туре	Static
IP	192.168.1.1/24

Create a Layer 3 Interface on ethernet1/3

Ethernet Interface	ethernet1/3
Comment	Extranet servers connection
Туре	Layer 3
IPv4 Type	Static
IP	192.168.50.1/24

Create a Logical Router

Use the information in the table below to create a Logical Router and a firewall default gateway.

Name	LR-1
Interfaces (General Tab)	ethernet1/1
	ethernet1/2
	ethernet1/3
IPv4 Static Route Name	Firewall-Default-Gateway
Destination	0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
Next Hop IP	203.0.113.1

Segment Your Production Network Using Security Zones

Use the information in the tables below to create three Security Zones with the appropriate interface in each Zone.

Zone Name	Internet
Туре	Layer 3
Interface	ethernet1/1

Zone Name	Users_Net
Туре	Layer 3
Interface	ethernet1/2

Zone Name Extranet	
--------------------	--

Туре	Layer 3
Interface	ethernet1/3

Commit the configuration

• Commit the changes to the firewall before proceeding

Test Connectivity to Each Zone

- Use the Remmina SSH application on the Client-A desktop to connect to Firewall-A
- In the firewall CLI, use the **ping** command to check network connectivity from the firewall to a host in each Security Zone.
 - From **192.168.1.1** (ethernet1/2) to **192.168.1.20**
 - From **192.168.50.1** (ethernet1/3) to **192.168.50.150**
 - From **203.0.113.20** (ethernet1/1) to **8.8.8.8**

Test Interface Access before Management Profiles

- Ping the firewall interface on ethernet1/2 from a terminal connection on Client-A. You will not get a response.
- Attempt to connect to the firewall for CLI management through an SSH connection from Client-A. The firewall will not accept the connection.

Define Interface Management Profiles

Use the information below to create two Interface Management Profiles

Name	Allow-ping
Enabled Administrative Management Services	None
Enabled Network Services	Ping

Name	Allow-mgt
Enabled Administrative Management Services	нттрѕ
	SSH
Enabled Network Services	Ping
	SNMP
	Response Pages

Apply Allow-ping to ethernet1/1

• Apply the **Allow-ping** Interface Management Profile to **ethernet1/1**

Apply Allow-mgt to ethernet1/2

• Apply the **Allow-mgt** Interface Management Profile to **ethernet1**/2

Apply Allow-mgt to ethernet1/3

• Apply the Allow-mgt Interface Management Profile to ethernet1/3

Commit the configuration

• Commit the changes before testing Interface Management Profiles

Test Interface Access after Management Profiles

- Ping the firewall interface on ethernet1/2 from a terminal connection on Client-A. You should now get a response.
- Attempt to connect to the firewall for CLI management through an SSH connection from Client-A. The firewall will now accept the connection.

Detailed Lab Steps

Use this section if you prefer detailed guidance to complete the objectives for this lab. We strongly recommend that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-05.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK** to close the **Load Named configuration** window.
- 5. Click **Close** to close the **Loading configuration** window.
- 6. Click the **Commit** button at the upper right of the web interface.
- 7. Leave the remaining settings unchanged and click Commit.
- 8. Wait until the **Commit** process is complete.
- 9. Click **Close** to continue.

Create Layer 3 Network Interfaces

In the following sections, you will create Layer 3 interfaces on the firewall that will provide basic network connectivity to your production networks. You have a network with users (192.168.1.0/24), a network with production servers (192.168.50.0/24) and a network connecting the firewall to an upstream internet router (203.0.113.0/24). The following diagram provides details.



Create a Layer 3 Interface on ethernet1/1

This interface will provide network connectivity to the Internet.

- 10. Select **Network > Interfaces > Ethernet**.
- 11. Click the link for **ethernet1/1**.

🚺 PA-VM	DASHBOARD	ACC MO	NITOR POLICIE	s obje		NORK DEV	'ICE
🖽 Interfaces	Ethernet VLAN	Loopback	Funnel SD-WAN				
Zones Class VIANs Virtual Wires	Q				1		
> 🛞 Routing	INTERFACE	INTERFACE 1	YPE PROFILE	LINK STATE	IP ADDRESS	LOGICAL ROUTER	тя
Hefer GRE Tunnels	ethernet1/1			m	none	none	U
DNS Proxy	ethernet1/2				none	none	U

- 12. For **Comment**, enter **Internet** connection.
- 13. For **Interface Type**, select **Layer3**.

14. Leave the other settings unchanged but do not close this window.

Ethernet Interf	Ethernet Interface				
Interface Name	ethernet1/1				
Comment	Internet connection.				
Interface Type	Layer3				
Netflow Profile	None				
Config IPv4	IPv6 SD-WAN	Advanced			
Assign Interface To)				
Virtual Route	r None				
Security Zone	e None				

- 15. Select the tab for **IPv4**.
- 16. Leave the **Type** set to **Static**.
- 17. Under the **IP** heading, click **Add**.
- 18. Enter 203.0.113.20/24

invention runne	ethernet1/1
Comment	Internet connection.
Interface Type	Layer3
Netflow Profile	None
Туре	Static PPPoE DHCP Client



Be sure to include /24 in the address!

20. Click OK.

Create a Layer 3 Interface on ethernet1/2

This interface will provide network connectivity to the Users network.

- 21. Select **Network > Interfaces > Ethernet**.
- 22. Click the link for **ethernet1/2**.

🔶 PA-VM	DASHBOARD	ACC	ΜΟΝΙΤΟ	R POLICIES	OBJ	ECTS	NETWORK	DEVICE
Interfaces	Ethernet VLAN	Loopb	ack Tunne	el SD-WAN				
Part Zones	Q				1	1		
> 🛞 Routing	INTERFACE	INTE	RFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDR	ESS R	OGICAL OUTER
GRE Tunnels	ethernet1/1	Laye	r3		6	203.0.11	3.20/24 n	one
👮 DNS Proxy 🚅 Proxy	ethernet1/2					none	n	one

- 23. For **Comment**, enter **Users** network connection.
- 24. For Interface Type, select Layer3.
- 25. Leave the other settings unchanged but do not close this window.

Ethernet Interf	Ethernet Interface				
Interface Name	ethernet1/2				
Comment	Users network connection.				
Interface Type	Layer3				
Netflow Profile	None				
Config IPv4	IPv6 SD-WAN Advanced				
Assign Interface To					
Virtual Route	None				
Security Zon	None				

- 26. Select the tab for **IPv4**.
- 27. Leave the **Type** set to **Static**.
- 28. Under the **IP** heading, click **Add**.
- 29. Enter **192.168.1.1/24**

Ethernet Interf	ace					
Interface Name	ethernet1/2					
Comment	Users network connection.					
Interface Type	Layer3					
Netflow Profile	ow Profile None					
Config IPv4 IPv6 SD-WAN Advanced						
<u> </u>	Enable SD-WAN					
Type 💿 Static 🔿 PPPoE 🔿 DHCP Client						
IP IP						
192.168.1.1/24	4					
← Add ← Delete ← Move Up ↓ Move Down IP address/netmask. Ex. 192.168.2.254/24						



Be sure to include /24 in the address!

31. Click **OK**.

Create a Layer 3 Interface on ethernet1/3

This interface will provide network connectivity to the Extranet network.

- 32. Select Network > Interfaces > Ethernet.
- 33. Click the link for **ethernet1/3**.

🔶 PA-VM	DASHBOARD	ACC MONITO	R POLICIES	OBJE	ECTS NETWO	ORK DEVICE
🚥 Interfaces	Ethernet VLAN	Loopback Tunne	el SD-WAN			
Zones .						
VLANs	Q					
🛃 Virtual Wires						
> 🛞 Routing			MANAGEMENT	LINK		LOGICAL
🔨 IPSec Tunnels	INTERFACE	INTERFACE TYPE	PROFILE	STATE	IP ADDRESS	ROUTER
-{}+ GRE Tunnels	ethernet1/1	Layer3		m	203.0.113.20/24	none
불 DHCP				_		
DNS Proxy	ethernet1/2	Layer3		m	192.168.1.1/24	none
🚝 Proxy				_		
√ 😤 GlobalProtect	ethernet1/3			Ē.	none	none
Rortals	Contenternet1/4			atta	none	none

- 34. For **Comment**, enter **Extranet** servers connection.
- 35. For Interface Type, select Layer3.
- 36. Leave the other settings unchanged but do not close this window.

Ethernet Interf	Ethernet Interface					
Interface Name	ethernet1/3					
Comment	Extranet servers connection.					
Interface Type	Layer3					
Netflow Profile	None					
Config IPv4	IPv6 SD-WAN Advanced					
Assign Interface To)					
Virtual Route	r None					
Security Zone	e None					

- 37. Select the tab for **IPv4**.
- 38. Leave the **Type** set to **Static**.
- 39. Under the **IP** heading, click **Add**.
- 40. Enter **192.168.50.1/24**

Ethernet Interf	ace
Interface Name	ethernet1/3
Comment	Extranet servers connection.
Interface Type	Layer3
Netflow Profile	None
Config IPv4	IPv6 SD-WAN Advanced
Туре	Enable SD-WAN O Static PPPoE ODHCP Client
IP IP	
192.168.50.1/2	24
1	
Add (-) Delet	e 🌴 Move Up 👃 Move Down
IP address/netmask. Ex.	192.168.2.254/24



Be sure to include /24 in the address!

- 42. Click **OK**.
- 43. When complete, your Ethernet table will have three entries:

🔶 PA-VM	DASHBOARD	ACC MONITO	R POLICIES	OBJ	ECTS NETWO	RK DEVICE	
෩ Interfaces	Ethernet VLAN	Loopback Tunn	el SD-WAN				
Zones							
Q VLANs	Q						
Virtual Wires							
> 🛞 Routing			MANAGEMENT	LINK		LOGICAL	
🔁 IPSec Tunnels	INTERFACE	INTERFACE TYPE	PROFILE	STATE	IP ADDRESS	ROUTER	TAC
-{€ GRE Tunnels	ethernet1/1	Layer3		m	203.0.113.20/24	none	Unt
뿣 DHCP							
💥 DNS Proxy	ethernet1/2	Layer3		m	192.168.1.1/24	none	Unt
🚍 Proxy							
V 🚱 GlobalProtect	ethernet1/3	Layer3		Ē	192.168.50.1/24	none	Unt
🚯 Portals							



Note that the Link State indicator icons will remain gray until you commit the configuration.

Create a Logical Router

In this section, you will create a logical router and connect your Layer 3 interfaces to it. You also will define a default gateway for the logical router itself.

- 44. Select **Network > Routing > Logical Routers**.
- 45. Click Add.
- 46. For **Name**, enter **LR-1**.
- 47. Under the **Interface** section, click the **Add** button at the bottom.
- 48. Select ethernet1/1.

Logical Rou	iter
General	Name LR-1
Static	Interface Administrative Distances EC
OSPF	
OSPFv3	
RIPv2	
BGP	ethernet1/1
Multicast	ethernet1/3
	loopback
	sdwan
	tunnel
	vlan
	⊕ Add ⊖ Delete

49. Click Add again.

- 50. Select ethernet1/2.
- 51. Click **Add** again.
- 52. Select ethernet1/3.
- 53. Leave this window open.
- 54. When complete all three interfaces should be listed under the **Interface** tab:

Logical Router					
General	Name LR-1				
Static	Interface Administrative Distance				
OSPF					
OSPFv3	INTERFACE A				
RIPv2	ethernet1/1				
0.00	ethernet1/2				
BGP	ethernet1/3				
Multicast					



The order in which you add these interfaces to the list is not important. You could start by adding ethernet1/3 and the result will be the same. You are simply adding the appropriate interfaces to this logical router.

55. In the Logical Router window, click the link on the side for Static.

Logical Router							
General		IPv4 IPv6					
Static							
OSPF		Q					
OSPFv3							
RIPv2							
BGP			DESTINATION	INTERFACE			
Multicast							
		+ Add De	elete 💿 Clone				

56. Under the tab for **IPv4**, click **Add** at the bottom of the window.

- 57. For Name, enter Firewall-Default-Gateway.
- 58. For **Destination**, enter **0.0.0/0**.
- 59. For Interface, select ethernet1/1.
- 60. Set the Next Hop field to IP Address.
- 61. Below the Next Hop field, enter 203.0.113.1.
- 62. Leave the remaining settings unchanged.

Log	Logical Router - Static Route					
	Name	Firewall-Default-Gateway				
	Destination	0.0.0/0				
	Interface	ethernet1/1				
	Next Hop	IP Address				
		203.0.113.1				
	Admin Dist	[10 - 240]				



This entry is the default route for the firewall. Like all other network hosts, the firewall needs a default gateway in order to send traffic to unknown networks. The firewall has local connections to 192.168.1.0, 192.168.50.0 and 203.0.113.0 networks, so it can forward packets to hosts on those networks directly. However, for any other destination IP addresses (such as 8.8.8.8 for DNS), this route

statement instructs the firewall to forward packets to 203.0.113.1, which is the internet router.

- 63. Click **OK** on the **Logical Router Static Route** window.
- 64. Click **OK** on the **Logical Router** window.

Segment Your Production Network Using Security Zones

With your network interfaces and logical router in place, you can now create security zones. You will create three security zones:



65. Create the **Internet Zone** by selecting **Network > Zones**.

🚺 PA-VM		DASHBOARD	ACC N	MONITOR	POLICIES O	BJECTS	ETWORK [DEVICE
Interfaces	• ^ (I	1	1	1	T	1
VICANS VICANS Victual Wires Victual Wires		NAME	түре	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	ENABLE HEADER INSPECTION	PACKET BUFFER PROTECTION	LOG SETTI
Logical Routers A general content of the second s	•							

- 66. At the bottom of the window, click the **Add** button.
- 67. For **Name**, enter **Internet**.
- 68. For **Type**, select **Layer3**.
- 69. Under the Interfaces section, click Add.
- 70. Select ethernet1/1.
- 71. Leave the remaining settings unchanged.

Zone	
Name Internet	User l
Log Setting None 🗸	Er
Type Layer3 🗸	
ethernet1/1	Selec in yo 192.:
+ Add Delete	(+) Ar



Zone names are case-sensitive! Make sure you are consistent throughout your configuration process.

- 72. Click OK.
- 73. In the **Zones** window, create the Users_Net Zone by clicking **Add**.
- 74. At the bottom of the window, click the **Add** button.
- 75. For **Name**, enter **Users_Net**.
- 76. For **Type**, select **Layer3**.
- 77. Under the **Interfaces** section, click **Add**.
- 78. Select ethernet1/2.



Notice that ethernet1/1 is no longer listed in the available interfaces. You have assigned ethernet1/1 to another zone so the firewall will not allow you to assign the same interface to any other zone.

79. Leave the remaining settings unchanged.



- 80. Click OK.
- 81. In the **Zones** window, create the Extranet Zone by clicking **Add**.
- 82. At the bottom of the window, click the **Add** button.
- 83. For Name, enter Extranet.
- 84. For **Type**, select **Layer3**.
- 85. Under the **Interfaces** section, click **Add**.
- 86. Select ethernet1/3.



All other Layer 3 interfaces have been assigned to zones so you can choose only ethernet1/3.

87. Leave the remaining settings unchanged.

Zone	
Name Extranet	User Ider
Log Setting None ~	Enab
Type Layer3 🗸	
	in your
ethernet1/3	192.168
1	
↔ Add ↔ Delete	Add Users from

- 88. Click OK.
- 89. You should now have three security zones:

🚺 PA-VM			DASHBOARD	ACC	MON	ITOR	POLICI	ES OBJECTS	NETWORK	DEVICE	
🚥 Interfaces		Q									
Image: Second			NAME	TYPE		INTERFACE VIRTUAL SYSTEMS	ES /	ZONE PROTECTION PROFILE	ENABLE HEADER	PACKET BUFFER PROTECTION	LOG
 ⊕ Logical Routers > ⊕ Routing Profiles 	•		Internet Users_Net Extranet	layer3 layer3 layer3		ethernet1/ ethernet1/ ethernet1/	1 2 3				

Commit the configuration

- 90. Click the **Commit** button at the upper right of the web interface.
- 91. Leave the settings unchanged and click **Commit**.
- 92. Wait until the **Commit** process is complete.

93. Click Close to continue.

Test Connectivity to Each Zone

To verify network connectivity from the firewall to hosts in each zone, you will use an SSH connection and ping hosts on each network.

94. On the client **desktop**, open the **Remmina** application:



95. Double-click the entry for **Firewall-A**:

D Q				Remm	Ina Remote Desktop Client Remote Desktop Client
	S	SH 🕶			
Name	-	Group	Server	Plugin	Last used
Berlin-Cl	lent		192.168.1.25	SSH	2022-09-02 - 07:04:25
🔒 Firewall-	A		192.168.1.254	SSH	2022-08-30 - 06:22:24
Firewall-	В		192.168.1.253	SSH	2022-08-01 - 10:40:43
Panoram	a		192.168.1.252	SSH	2022-08-30 - 07:00:17
Server-E	xtranet		192.168.50.10	SSH	2022-06-22 - 12:39:06



The Firewall-A connection in Remmina has been pre-configured to provide login credentials to the firewall so that you do not have to log in each time. This is for convenience in the lab only.

96. In the CLI connection to the firewall, use the **ping** command to check network connectivity to a host in the Users_Net Security Zone by using the following command at the admin@firewall-a> prompt:

admin@firewall-a> ping source 192.168.1.1 host 192.168.1.20



Note the syntax for this command. 192.168.1.1 is the IP address of ethernet1/2 on the firewall. The command instructs the firewall to use that IP address on ethernet1/2 to ping the host 192.168.1.20. If you do not use the source option, the firewall uses its management interface address as the source IP.

97. Allow the ping to continue for three or four seconds and then use **Ctrl+C** to interrupt the command:



98. Use the ping command to check connectivity to a host in the Extranet zone by using the following command at the **admin@firewall-a>** prompt :

admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150



192.168.50.1 is the IP address on ethernet1/3 that is assigned to the Extranet security zone. 192.168.50.150 is a server in the Extranet zone.

99. Allow the ping to continue for three or four seconds and then use **Ctrl+C** to interrupt the command:

	Firewall-A –
s	Firewall-A ×
	admin@firewall-a> ping source 192.168.50.1 host 192.168.50.150 PING 192.168.50.150 (192.168.50.150) from 192.168.50.1 : 56(84) bytes of data. 64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=2.72 ms 64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=2.26 ms 64 bytes from 192.168.50.150: icmp_seq=3 ttl=64 time=2.99 ms ^c
	192.168.50.150 ping statistics 3 packets transmitted, 3 received, 0% packet loss, time 5ms rtt min/avg/max/mdev = 2.263/2.657/2.988/0.302 ms admin@firewall-a>
1 <u>111</u> 1	

100. Use the ping command to check connectivity to a host on the Internet by using the following command at the admin@firewall-a> prompt:

admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8



203.0.113.20 is the IP address on ethernet1/1 that is assigned to the Internet security zone. 8.8.8.8 is a DNS server on the Internet zone.

101. Allow the ping to continue for three or four seconds and then use **Ctrl+C** to interrupt the command:

	Firewall-A
\otimes	🔒 Firewall-A 🗙
	admin@firewall-a> ping source 203.0.113.20 host 8.8.8.8 PING 8.8.8.8 (8.8.8.8) from 203.0.113.20 : 56(84) bytes of data. 64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=5.84 ms 64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=3.100 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=4.04 ms ^C
	8.8.8.8 ping statistics 3 packets transmitted, 3 received, 0% packet loss, time 5ms rtt min/avg/max/mdev = 3.995/4.625/5.837/0.858 ms admin@firewall-a>
Ф.	

- 102. After you have successfully tested network access from the firewall to each network segment, close the Remmina SSH connection to the firewall by typing **exit** <**Enter**>.
- 103. Close the Remmina Remote Desktop Client application window.

Create Interface Management Profiles

Management Interface Profiles allow you to enable specific network services on individual firewall interfaces.

Often, your team members need to manage the firewall but do not always have network connectivity to the management network. In this exercise, you will define two Management Interface Profiles. One Profile, named "allow-ping," will be applied to the Internet interface so that your SecOps team members can ping the external firewall interface for troubleshooting from outside your organization's network.

You will create a second Interface Management Profile called "Allow-mgt" that allows both ping and secure management traffic including SSH and HTTPS. You will apply this Profile to the Users_Net interface and to the Extranet interface. This Profile will allow your SecOps team to manage the firewall from those networks if they need to.



Test Interface Access before Management Profiles

To illustrate the default behavior of firewall interfaces, you will ping 192.168.1.1 from the client workstation. You will also attempt to access the firewall CLI by SSH through 192.168.1.1.

Without any Interface Management Profiles in place, both ping and SSH will fail.

104. Open the Terminal application on the client **desktop**.



105. Issue the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 192.168.1.1 <Enter>

106. You will not get a response.

107. Wait a few seconds and use Ctrl+C to stop the command.



108. Attempt to open an SSH connection to the firewall through 192.168.1.1 by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ssh admin@192.168.1.1 <Enter>

109. After a few seconds, use Ctrl+C to stop the connection because it will not succeed.



110. Leave the Terminal window open on the client because you will perform these same tests after applying an Interface Management Profile to ethernet1/2.

Define Interface Management Profiles

111. In the firewall web interface, select **Network > Network Profiles > Interface Mgmt**.

- 112. Click **Add** at the bottom of the window.
- 113. For Name, enter Allow-ping.
- 114. Under the Network Services section, check the box for Ping.
- 115. Leave the remaining settings unchanged.

Interface Management Profile
Name Allow-ping
Administrative Management Services
□ HTTP
HTTPS
Telnet
SSH SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP

- 116. Click **OK**.
- 117. In the Interface Management section, click Add again to create another entry.
- 118. For **Name**, enter **Allow-mgt**.
- 119. Under the Administrative Management Services section, check the boxes for HTTPS and SSH.
- 120. Under the section for Network Services, check Ping, SNMP and Response Pages.

Interface Management Profile
Name Allow-mgt
HTTPS
Telnet SSH
Network Services
Ping
Response Pages
User-ID
User-ID Syslog Listener-SSL

122. Click OK.

Apply Allow-ping to ethernet1/1

- 123. Select **Network > Interfaces > Ethernet**.
- 124. Edit the entry for ethernet1/1.
- 125. Select the tab for Advanced.
- 126. Under the **Other Info** section, use the drop-down list for **Management Profile** to select **Allow-ping**.

127. Leave the other settings unchanged.

Ethernet Interface					
Interface Name	ethernet1/1				
Comment	Internet connection.				
Interface Type	Layer3				
Netflow Profile	None				
Config IPv4 IPv6 SD-WAN Advanced					
C Link Settings					
Link Speed auto		Link Duplex auto			
Other Info ARP Entries ND Entries NDP Proxy LLDP					
Management Profile Allow-ping					
N	TU [576 - 1500]				
C Adjust TCP MS	S				



This action applies the **Allow-ping** interface management Profile to ethernet1/1. As a result, ethernet1/1 will answer **ping** requests.



Note that in a production environment, you may not want an Internet-facing interface to reply to any type of traffic. Applying this Profile in the lab allows you to see how different Profiles can be applied to different interfaces.

128. Click OK.

Apply Allow-mgt to ethernet1/2

- 129. Select **Network > Interfaces > Ethernet**.
- 130. Edit the entry for ethernet 1/2.
- 131. Select the tab for **Advanced**.
- 132. Under the **Other Info** section, use the drop-down list for **Management Profile** to select **Allow-mgt**.

133. Leave the other settings unchanged.

Ethernet Interface							
Interface Name	ethernet1/2						
Comment	Users network connection.						
Interface Type	Layer3						
Netflow Profile	None						
Config IPv4	IPv6 SD-WAN	Advanced					
Link Settings							
Link Speed auto		Link Duplex auto					
Other Info AR	RP Entries ND Entries	NDP Proxy LLDP DE					
Management Pr	ofile Allow-mgt						
N	MTU [576 - 1500]						

134. Click OK.

135. Read the Warning message and click Yes.

Warning	
By attaching this interface administrative interface to	management profile to this interface, you are potentially exposing the firewall's any party that can reach this interface.
Would you like to continue	with this change?
	Yes No



Managing the firewall by applying a management profile on a network interface has risks and therefore should only be used if there is no other option due to the network topology. In a production environment you should avoid this practice when possible.

Apply Allow-mgt to ethernet1/3

- 136. Select **Network > Interfaces > Ethernet**.
- 137. Edit the entry for ethernet 1/3.
- 138. Select the tab for Advanced.
- 139. Under the **Other Info** section, use the drop-down list for **Management Profile** to select **Allow-mgt**.

- 140. Leave the other settings unchanged.
- 141.Click **OK**.
- 142. Click **Yes** on the Warning message.

143. When you complete these steps, your interface table should have an entry under the Management Profile column for each interface.

🚺 PA-VM		DASHBOARD	ACC	ΜΟΝΙΤΟ	R POLICIES	OBJ	ECTS	NETWOR		:
interfaces		Ethernet VLAN Loopback Tunnel SD-WAN								
Zones 2										
몇 VLANs		0								
Virtual Wires		~		(
✓ ⊕ Routing					MANAGEMENT	LINK			OGICAL	
Logical Routers	- H	INTERFACE	INTERF	ACE TYFE	PROFILE	STATE	IP ADD	RESS	ROUTER	1
> 🛞 Routing Profiles		methernet1/1	Laver3		Allow-ping		203.0.1	13.20/24	LR-1	1
1 IPSec Tunnels		and concerner 1								
GRE Tunnels		ethernet1/2	Layer3		Allow-mgt	m	192.16	8.1.1/24	LR-1	
± рнср										
🕂 DNS Proxy		ethernet1/3	Layer3		Allow-mgt		192.16	8.50.1/24	LR-1	
🚝 Proxy										
V K GlobalProtect		-								

Commit the configuration

- 144. Click the **Commit** button at the upper right of the web interface.
- 145. Leave the settings unchanged and click **Commit**.
- 146. Wait until the **Commit** process is complete.
- 147. Click **Close** to continue.

Test Interface Access after Management Profiles

With the **Allow-mgt** Interface Management Profile in place on ethernet1/2, both ping and SSH will succeed.

148. From the Terminal Emulator on the client desktop, issue the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 192.168.1.1 <Enter>

149. The interface will now respond.

150. Wait a few seconds and use **Ctrl+C** to stop the command.

lab-user@client-a: ~/Desktop/Lab-Files
lab-user@client-a: ~/Desktop/Lab-Files\$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.929 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.88 ms
^c
--- 192.168.1.1 ping statistics --3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.929/1.423/1.884/0.390 ms
lab-user@client-a:~/Desktop/Lab-Files\$

151. Attempt to open an SSH connection to the firewall through 192.168.1.1 by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ssh admin@192.168.1.1 <Enter>

If you are prompted to accept an RSA key fingerprint, type **yes** <**ENTER**>.

152. For password, enter Pal0Alt0! <Enter>.

153. The firewall will present the CLI interface.



154. Close the SSH connection to the firewall by typing exit <Enter>.

155. Close the Terminal window by typing exit <Enter>.



Stop. This is the end of the lab.
Lab 6: Creating and Managing Security Policy Rules

You have the firewall deployed and connected to all the appropriate networks. The next step is to begin creating Security Policy rules. You will start by creating rules that allow hosts in the Users_Net zone to communicate with hosts in the Extranet zone. You will then create Security Policy rules to allow hosts in the Users_Net zone to connect to hosts in the Internet zone.

You also need to allow hosts in the Extranet zone to communicate with hosts in the Internet zone.



Lab Objectives

- Configure a Security Policy rule to allow access from Users_Net to Extranet
- Test access from client to Extranet servers
- View the Traffic log
- Examine Policy Rule Hit Count
- Reset rule hit counts
- Customize Policy tables
- Enable intrazone and interzone logging
- Create Security Policy rules to Internet Zone

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-06.xml** to the Firewall

Create Security Policy Rule

• Use the information below to create a Security Policy rule that will allow traffic from the Users_Net zone to the Extranet zone.

Rule Name	Users_to_Extranet
Description	Allows hosts in Users_Net zone to access servers in Extranet zone
Source Zone	Users_Net
Destination Zone	Extranet
Application	Any
Service	application-default
URL Category	Any
Action	Allow

Commit the configuration

• Commit the changes before proceeding.

Modify Security Policy Table Columns

- Hide the following columns in the **Security Policy** table to create more area to view helpful information
 - Type
 - Source Device
 - Destination Device
 - Options
- Drag and drop the **Action** column from its current location so that it appears between the **Name** column and the **Tag** column

Test New Security Policy Rule

- From the Client-A host, ping 192.168.50.80, which is the IP address of a web server in the Extranet zone.
- Use the web browser on the Client-A client to connect to the Extranet web page at 192.168.50.80.

Examine Rule Hit Count

- In the **Security Policy** rule table, locate the column for **Hit Count**, and note the number of **Hits** on this **Users_to_Extranet** rule.
- From the Client-A host, ping the Extranet web server 192.168.50.80.
- Refresh the **Hit Count** and note any increase in the value for the **Users_to_Extranet** Security Policy rule.

Reset the Rule Hit Counter

• Reset the **Hit Count** for the **Users_to_Extranet** rule

Examine the Traffic Log

- Hide the following columns in the Traffic Log.
 - Type
 - Source Dynamic Address Group
 - Destination Dynamic Address Group
 - Dynamic User Group
- From the terminal window on the Client-A host, ping 8.8.8.8

You will <u>not</u> get a reply

- Examine the traffic log again and use a simple filter to see if there are any entries for the ping session that failed
- Answer the following question:

Why there are no entries in the Traffic log for your ping session to 8.8.8.8?

• Write down your answer in the field shown or on notepaper in class.

Enable Logging for Default Interzone Rule

• Edit the Interzone Security Policy rule and enable Log at Session End

Commit the configuration

• Commit the changes before proceeding

Ping a Host on the Internet

• From the terminal window on the Client-A host, ping 8.8.8.8

You will <u>not</u> get a reply

- Examine the Traffic Log again and use a simple filter to see if there are any entries for this session that failed
- The entries in the Traffic Log should show you that the ping sessions are hitting the interzone-default rule

Create Block Rules for Known-Bad IP Addresses

• Use the information below to create a rule at top of the Security Policy to block traffic <u>to</u> known bad IP addresses provided by Palo Alto Networks.

Rule Name	Block-to-Known-Bad-Addresses	
Description	Blocks traffic from Users and Extranet to known bad IP addresses	
Source Zone	Users_Net Extranet	
Destination Zone	Internet	
Destination Address	 Palo Alto Networks - Bulletproof IP addresses Palo Alto Networks - High risk IP addresses Palo Alto Networks - Known malicious IP addresses 	
Application	Any	

Service	any
URL Category	Any
Action	Deny

• Use the information below to create another Security Policy rule to block traffic <u>from</u> known bad IP addresses provided by Palo Alto Networks. Place this rule at the top of the Security Policy, just below the Block-to-Known-Bad-Addresses rule.

Rule Name	Block-from-Known-Bad-Addresses	
Description	Blocks traffic from known bad IP addresses to Users and Extranet	
Source Zone	Internet	
Source Address	 Palo Alto Networks - Bulletproof IP addresses Palo Alto Networks - High risk IP addresses Palo Alto Networks - Known malicious IP addresses 	
Destination Zone	Users_Net Extranet	
Application	Any	
Service	application-default	
URL Category	Any	
Action	Deny	

Create Security Rules for Internet Access

• Use the information in the tables below to create Security Policy rules.

Create Users to Internet Security Policy Rule

• Use the information below to create a Security Policy rule that will allow traffic from the Users_Net zone to the Internet zone.

Rule Name	Users_to_Internet
Description	Allows hosts in Users_Net zone to access Internet zone
Source Zone	Users_Net
Destination Zone	Internet
Application	Any

Service	application-default
URL Category	Any
Action	Allow

Create Extranet to Internet Security Policy Rule

Use the information below to create a Security Policy rule that will allow traffic from the **Extranet** zone to the **Internet** zone.

Rule Name	Extranet_to_Internet
Description	Allows hosts in Extranet zone to access Internet zone
Source Zone	Extranet
Destination Zone	Internet
Application	Any
Service	application-default
URL Category	Any
Action	Allow

Commit the configuration

• Commit the changes before proceeding

Ping Internet Host from Client A

- From the terminal window on the Client-A host, ping 8.8.8.8
- You will not get a reply
- Examine the Traffic Log again and use a simple filter to see if there are any entries for this session that failed
- The entries in the Traffic Log should show you that the ping sessions are hitting the Users_to_Internet rule.
- Answer the following question:

Can you explain why your ping session from the client to the Internet host did not get a reply even though the firewall is allowing the traffic?

• Write down your answer in the field shown or on notepaper in class.

Detailed Lab Steps

Use this section if you prefer detailed guidance to complete the objectives for this lab. We strongly recommend that you use this section if you do not have extensive experience working with Palo Alto Networks firewalls.

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-06.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK** to close the **Load Named configuration** window.
- 5. Click **Close** to close the **Loading configuration** window.
- 6. Click the **Commit** button at the upper right of the web interface.
- 7. Leave the remaining settings unchanged and click **Commit**.
- 8. Wait until the **Commit** process is complete.
- 9. Click **Close** to continue.

Create a Security Policy Rule

You need to allow network traffic from the Users_Net security zone to the Extranet security zone so that employees can access various business applications. In this section, you will create a Security Policy rule to allow access between these two zones.



- 10. Select **Policies > Security**.
- 11. Click **Add** at the bottom of the window.
- 12. Under the tab for **General**, in the **Name** field, enter **Users_to_Extranet**.
- 13. For **Description**, enter **Allows hosts in Users_Net zone to access** servers in Extranet zone.
- 14. Leave the other settings unchanged:

General	Source Destination Application Service/URL Category Actions
[h	Jame Users_to_Extranet
Rule	Type universal (default)
Descri	ption Allows hosts in User_Net zone to access servers in Extranet zone.
	Tags

Õ

Descriptions are optional but highly recommended. It may take you a few extra moments to enter an accurate Description during these labs, but if you adhere to the practice in the labs, you will be more likely to carry out this best practice when you return to work.

- 15. Select the tab for **Source**.
- 16. Under the **Source Zone** section, click **Add**.
- 17. Select Users_Net.
- 18. Leave the remaining settings unchanged.

Security Policy Rule			
General Source Dest	ination Application Servic	ce/URL Category Actions	
Any	🗾 Any	any 🗸	any
SOURCE ZONE	SOURCE ADDRESS	SOURCE USER	
Users_Net	Pelete	Add 🕞 Delete	€Add
🕂 Add 🕞 Delete	🕂 Add 😑 Delete	🕂 Add 🕞 Delete	🕂 Add — Dele
	Negate		

- 19. Select the tab for **Destination**.
- 20. Under the section for **Destination Zone**, click **Add**.
- 21. Select Extranet.
- 22. Leave the other settings unchanged.

Security Policy Rule		
General Source Destination Application Service/URL Category Actions		
select	Any DESTINATION ADDRESS	any V DESTINATION DEVICE
🕀 Add 🕞 Delete		

- 23. Select the tab for **Application**.
- 24. Do not make any changes to these settings but note that the **Any** box is checked.

Security Policy Rule	
General Source Destination Application Service/URL Category Actions	



Later in this course, we will cover Applications and how to use them in Security Policy rules.

- 25. Select the tab for Service/URL Category.
- 26. Do not make any changes to the settings in this tab but note that the **Service** is set to **application-default**.

Service/URL Category Actions
Any
URL CATEGORY A

	_	
	_	~
	Ξ	~
	=	-
•		

The application-default setting instructs the firewall to allow an application such as web-browsing as long as that application is using the predefined service (or destination port). For an application like web-browsing, the application default service is TCP 80; for an application such as SSL, the application default service is TCP 443. We will spend a great deal of time later in the course discussing Applications and the application-default setting.

27. Select the tab for Actions.

28. You do not need to make any changes in this section but note that the **Action** is set to **Allow** by default.

Security Policy Rule	C
General Source Destination Application Service/U	L Category Actions
Action Setting	Log Setting
Action Allow ~	Log at Session Start
Send ICMP Unreachable	🔽 Log at Session End
	Log Forwarding None ~
	Other Settings
Profile Setting	Schedule None
Profile Type None ~	QoS Marking None
	Disable Server Response Inspection
	OK Cancel



When you create a new Security Policy rule, the **Action** is automatically set to **Allow**. If you are creating a rule to block traffic, make sure you select the **Actions** tab and change the **Action** before you commit the rule.

- 29. Click **OK** on the Security Policy Rule window.
- 30. The new Security Policy rule appears in the table:

🚺 PA-VM		DASHBOARD	ACC	MONITOR	POLICIES
🖽 Security 🌑	Q(
→ NAT & QoS Policy Based Forwarding		NAME	_	TAGS	Source
 Decryption Tunnel Inspection 	1	Users_to_Extranet	J	none	🞮 Users_Net
 Application Override Authentication DoS Protection 	2 3	intrazone-default	©	none	any any



The rule appears above the two preconfigured entries intrazone-default and interzone-default. These two rules always appear at the bottom of the ruleset.

Commit the configuration

- 31. Click the **Commit** button at the upper right of the web interface.
- 32. Leave the settings unchanged and click **Commit**.
- 33. Wait until the **Commit** process is complete.
- 34. Click **Close** to continue.

Modify Security Policy Table Columns

You can customize the information presented in the Security Policy table to fit your needs. In this section, you will hide some of the columns and display others that may be of more interest. You will also move columns around and use the **Adjust Column** feature.

35. Click the small drop-down icon next to the Name column in the Security Policy table.



This icon is available next to all column headers.

36. Choose **Columns** and note the available columns that you can hide or display in this table.

NAME TAGS TYPE ZONE Columns Columns Columns Rule UUID 1 Users_to_Extranet none Columns Source Zone Rule Usage Description 2 intrazone-default none Adjust Columns Source Device Rule Usage First Hit 3 interzone-default none interzone any Destination Zone Profile	Q (Name	Ľ		ţ
1 Users_to_Extranet none Columns Image: Source 2 one Image: Rule Usage Hit Count 2 intrazone-default none Adjust Columns Image: Source User Rule Usage First Hit 3 interzone-default none interzone any Destination Zone		NAME	TAGS	V TYPE	ZONE		Tags Group Type			Profile Options Rule UUID Rule Usage Description
2 intrazone-default none Adjust Columns Image: Source User Image: Source User 3 interzone-default none interzone any Image: Source User Image: Source User 3 interzone-default none interzone any Image: Destination Zone Image: Destination Zone	1	Users_to_Extranet	none	Colur	mns >	Ž	Source Address	ł	~	Rule Usage Hit Count Rule Usage Last Hit
3 interzone-default 💿 none interzone any 🔽 Destination Zone	2	intrazone-default 👩	none	Adjus	st Columns	V	Source User Source Device			Rule Usage First Hit
	3	interzone-default 👩	none	interz	one any	~	Destination Zone	i	~	Rule Usage Apps Seen Days with No New Apps
 Destination Address Destination Device Application Service Action URL Category 	×					X X X X X X	Destination Address Destination Device Application Service Action URL Category		v	Modified Created

Note that the column list in this image has been cropped and wrapped to make it clearer in the lab guide.

- 37. **Uncheck** the following item:
 - Type
 - Source Device
 - Destination Device
 - Options
- 38. Drag and drop the **Action** column from its current location so that it appears between the **Name** column and the **Tag** column.

				Source	Destination	
	NAME	ACTION	TAGS	ZONE	ZONE	APPLICATION
1	Users_to_Extranet	⊘ Allow	none	थ Users_Net	🞮 Extranet	any
2	intrazone-default 👩	⊘ Allow	none	any	(intrazone)	any
3	interzone-default 👩	O Deny	none	any	any	any



Note: These changes are optional. You do not have to show or hide columns or rearrange items in any of the firewall tables. However, you may find that there are certain columns in certain tables that you never use, and you can hide them to provide more room in the table. You may also find that there are certain columns that you scan frequently, and you can move those to locations that are easier to

see. You can use these same steps to show, hide or move columns in all firewall tables.

39. At the top of the **Name** column, click the drop-down icon again and choose **Adjust Columns**.



40. This action will resize the displayed columns to best fit in the browser window.

Test New Security Policy Rule

41. To make certain that your Security Policy rule functions, open a terminal window on the client host.



42. Use the following command to ping 192.168.50.80, which is the IP address of a web server in the Extranet zone.

lab-user@client-a:~/Desktop/Lab-Files\$ ping 192.168.50.80 <Enter>

43. After several replies, use **Ctrl+C** to stop the ping.





If you see a reply from 192.168.50.80, then your Security Policy rule is configured correctly! If not, review the previous steps and try this test again.

44. On the client workstation, open the Firefox testing browser.

45. Use the bookmark bar to choose **Extranet > Extranet**:



Extranet (Secure)

Open All in Tabs

46. You should see a webpage displayed by the server.



47. Close the testing browser.

Examine Rule Hit Count

With your rule successfully in place, you can now examine hit counters in the Security Policy rule table. These counters can be useful for troubleshooting. If a rule is not being hit, you may need to modify it.

- 48. In the firewall web interface, select **Policies > Security**.
- 49. Scroll to the right and locate the column for Hit Count.

🚺 PA-VM	1	DASHBOARD	ACC	MONITOR	POLICIES
🖼 Security	Q(
 → NAT & QoS Policy Based Forwarding 		NAME		ACTION	HIT COUNT
🚡 Decryption 🔂 Tunnel Inspection	1	Users_to_Extranet		⊘ Allow	697
 Application Override Authentication 	2 3	intrazone-default interzone-default	@ @	⊘ Allow	51584 43446
CH Dos Protection					\rangle

Note: This image has been cropped to fit better on the page.



The Hit Count column in your firewall Security Policy rule list will be further to the right than is displayed here and the numbers displayed will differ from those shown.

- 50. Note the number of **Hits** on this rule.
- 51. Return to the terminal window on the desktop of your client.
- 52. Ping the server again by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 192.168.50.80 <Enter>

53. After several replies, use **Ctrl+C** to stop the ping.



54. Return to the firewall web interface and update the Security Policy rules table by clicking the **Refresh** button in the upper right corner of the window.



55. Note the increase in the Hit Count for your Security Policy rule.

Reset the Rule Hit Counter

Rule hit counts are very useful to track whether or not a rule is configured correctly. You can reset the counters for all Security Policy rules or for a single rule. In this section, you will reset the counters for the **Users_to_Extranet** rule.

56. Select **Policies > Security**.

- 57. Highlight the entry for Users_to_Extranet but do not open it.
- 58. At the bottom of the window, select **Reset Rule Hit Counter > Selected rules**.





59. The Rule Usage Hit Count is set to 0.

Examine the Traffic Log

The Traffic Log contains information about sessions that the firewall allows or blocks. In this section, you will examine the Traffic Log to locate entries for sessions between the Users_Net zone and the Extranet zone.

60. Select **Monitor > Logs > Traffic**.

🚺 PA-VM	DAS	SHBOARD A	сс	MONITOR	POLIC	cies c
∼ 🕞 Logs	^ Q					
Threat		RECEIVE TIME	TYPE	:	FROM ZONE	TO ZONE
WildFire Submissions	EQ.	03/03 16:47:49	end		Users_Net	Extranet
Data Filtering	R	03/03 16:47:49	end		Users_Net	Extranet
		00/004/.47.44	and		Linese Niek	Estrenat

- 61. Click the drop-down icon next to **Receive** time and choose **Columns**.
- 62. Uncheck the following items to hide their columns:
 - Type
 - Source Dynamic Address Group
 - Destination Dynamic Address Group

• Dynamic User Group

DA	ASHBOARD AC	с мо		 Receive Time Type From Zone To Zone
	RECEIVE TIME	FROM ZONE	то до	 Source Source User Source Dynamic Address Group
	07/07 18:02:4	Columns	>	Z Destination
	07/07 18:02:4	Adjust Colu	imns	Destination Dynamic Address Group
	07/07 18:02:23	Users_Net	Extrant	To Port
	07/07 18:02:22	Users_Net	Extrant	Application
	07/07 18:02:17	Users_Net	Extrane	Action Rule
	07/07 18:02:16	Users_Net	Extrant	Session End Reason
	07/07 18:02:12	Licers Net	Extrant	Bytes



This is not a requirement, but we will not be using information from these columns in any lab for this course.

63. From the terminal window on the desktop, ping an address on the internet by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 8.8.8.8<Enter>

64. You will not get a reply, so after several seconds, use Ctrl+C to stop the ping.

n	lab-user@client-a: ~/Desktop/Lab-Files
lab-user@client-a:~/D PING 8.8.8.8 (8.8.8.8 ^C	esktop/Lab-Files \$ ping 8.8.8.8) 56(84) bytes of data.
8.8.8.8 ping stat 4 packets transmitted	istics , 0 received, 100% packet loss, time 3052ms
lab-user@client-a:~/D	esktop/Lab-Files\$

- 65. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed.
- 66. Select **Monitor > Logs > Traffic**.
- 67. In the filter field, enter the following text exactly as it appears here:
- (addr.dst eq 8.8.8.8)

🔷 PA-VM	DA	SHBOARD	ACC	ΜΟΝΙΊ	OR
🗸 🔓 Logs		dr.dst eq 8.8.8.8)	1		
🖳 Traffic		RECEIVE TIM	1E FR	OM ZONE	то zo
🛛 URL Filtering	F	11/04 18.56	·46 Us	ers Net	Extran



Filters are case sensitive so be precise! Also, note that there is a space after the first parentheses mark and right before the last parentheses mark.

68. Click the **Apply filter** button in the upper right corner of the window (or you can press the **Enter** key).



69. The Traffic log will update the display but there are no matching entries.

🚺 PA-VM	C	DASHBOARD	AC	C	MONIT	OR	PC	DLICIES
🗸 📑 Logs		addr.dst eq 8.8.8.8	3)					
🖳 Traffic								
取 Threat		RECEIVE T	IME	FRO	M ZONE	TO ZO	DNE	SOURCE
🐼 URL Filtering								
🖏 WildFire Submissions								
🛅 Data Filtering								
📑 HIP Match								
Q GlobalProtect								

70. Answer the following question:

• Why are there no entries in the Traffic log for your ping session to 8.8.8.8?

Write down your answer in the field shown or on notepaper in class.

Enable Logging for Default Interzone Rule

If you were unable to explain why the firewall did not log your ping session to an external address, you are not alone. Most of the students in class probably did not figure it out either.

There are two reasons:

- First, you do not have a Security Policy rule in place to allow traffic from the Users_Net zone to the Internet zone. As the firewall examines the ping session, the only rule that matches is the interzone-default, which denies any traffic from one zone to another. The ping session matches this rule; however, there are no entries in the Traffic log indicating the match.
- Second, remember that traffic that hits the interzone-default rule is not automatically logged. You must manually change a setting on this rule to see entries in the Traffic log. You will enable this setting now and perform the test again.
- 71. Select **Policies > Security**.
- 72. Highlight the interzone-default entry in the Policy list but do not open it.
- 73. Click the **Override** button at the bottom of the window.

🍪 Override

- 74. Select the **Actions** tab.
- 75. Place a check in the box for **Log at session end**.

76. Leave the remaining s ettings unchanged.

Security Policy Rule	- predefined			?
General Actions				
Action Setting Action	Deny Send ICMP Unreachable	~	Log Setting	
Profile Setting Profile Type	None	~	Log Forwarding None	~
			OK Can	cel

77. Click OK.

Commit the configuration

- 78. Click the **Commit** button at the upper right of the web interface.
- 79. Leave the settings unchanged and click **Commit**.
- 80. Wait until the **Commit** process is complete.
- 81. Click **Close** to continue.

Ping a Host on the Internet

- 82. Now that you have enabled Log at session end for the default Security Policy rules, ping a host on the internet and examine the Traffic log to see the results.
- 83. From the Terminal window on the client desktop, ping an address on the Internet by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 8.8.8.8 <Enter>

84. You will not get a reply, so after several seconds, use **Ctrl+C** to stop the ping.



85. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed.

- 86. Select **Monitor > Logs > Traffic**.
- 87. In the filter field, enter the following text exactly as it appears here:
- (addr.dst eq 8.8.8.8)

🔷 PA-VM	DA	SHBOARD	ACC	ΜΟΝΙΤ	TOR
🗸 🔓 Logs	Î Q ((ac	ldr.dst eq 8.8.8.8)			
🖳 Traffic		RECEIVE TIM	IE FR	OM ZONE	TO ZO
URL Filtering	F	11/04 18.56	46 Us	ers Net	Extran



Your filter may already be in place from early.

88. Click the **Apply Filter** button in the upper right corner of the window (or you can press the **Enter** key).



- 89. The Traffic log will update the display and you should see entries matching the filter.
- 90. You can see that the sessions are hitting the interzone-default rule.

🚯 PA-VM		DASHBOARD		NITOR	POLICIES	OBJECTS	NETWORK	DEVIC	E	
∨ 🔓 Logs	^ Q	(addr.dst in 8.8.8.8)								
Traffic		RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI	APPLICATIO	ACTION	RULE	SESSION END REASON
URL Filtering		03/03 16:57:58	Users_Net	Internet	192.168.1.254	8.8.8	not-applicable	deny	interzone-default	policy-deny
WildFire Submissions		03/03 16:57:58	Users_Net	Internet	192.168.1.254	8.8.8	not-applicable	deny	interzone-default	policy-deny
HIP Match	Ð	03/03 16:57:58	Users_Net	Internet	192.168.1.254	8.8.8	not-applicable	deny	interzone-default	policy-deny
GlobalProtect		02/02 14:57-50	Linear Mat	Internet	100 140 1 054	0000	not applicable	dome	interrone default	notice doou



With Log at session end enabled, the firewall records hits on the internet-default rule so that you can see information about sessions that miss all previous rules.

91. Click the \mathbf{X} icon to clear the filter from the log filter text box.

Create Block Rules for Known-Bad IP Addresses

Palo Alto Networks provides several lists of IP addresses that are known to be malicious. As a good practice, you should create Security Policy rules to block traffic to and from these known addresses.

- 92. Under **Policies > Security**, click **Add** at the bottom of the window.
- 93. For Name, enter Block-to-Known-Bad-Addresses.
- 94. For **Description**, enter **Blocks traffic from users and Extranet to known bad IP addresses**.
- 95. Select the **Source** tab.
- 96. Under the **Source Zone** section, click **Add**.
- 97. Select the **Users_Net** zone.
- 98. Under the **Source Zone** section, click **Add** again.
- 99. Select the **Extranet** zone.



Note that you are adding both internal zones to the Source Zone section of the rule.

- 100. Select the **Destination** tab.
- 101. Under the **Destination Zone**, click **Add**.
- 102. Select the **Internet** zone.
- 103. Under the **Destination Address** section of the **Destination** tab, click Add.
- 104. Select Palo Alto Networks Bulletproof IP addresses.
- 105. Click Add again under the Destination Address section.
- 106. Select Palo Alto Networks High risk IP addresses.
- 107. Click Add again under the Destination Address section.
- 108. Select Palo Alto Networks Known malicious IP addresses.

When complete, you should have three Palo Alto Networks IP address lists in the Destination Address section of the rule.

- 109. Select the **Application** tab.
- 110. Leave the **Application** set to **any**.

111. Under the **Service/URL Category** tab, change the **Service** from **application-default** to **any**.

Security Policy Rule						
General Source Destination Application Service/URL Category Actions						
application-default 🗸						
application-default						
any						
select						



When creating deny rules, Palo Alto Networks recommends setting the **Service** to **any** instead of using **application-default**.

- 112. Select the **Actions** tab.
- 113. Change the **Action** to **Deny**.

Security Policy Rule							
General Source D	General Source Destination Application Service/URL Category Actions						
Action Setting							
Action	Deny						
	Deny						
	Allow						
	Drop						
Profile Setting	Reset client						
Profile Type	Reset server						
	Reset both client and server						

114. Click OK.

The new rule appears in the Security Policy table.

- 115. Move this new rule to the top of the Security Policy, by highlighting the entry for **Block-to-Known-Bad-Addresses** (do not open it).
- 116. At the bottom of the window, choose **Move** and select **Move Top**.



			Source				
	NAME	ACTION	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION
1	Block-to-Known-Bad-Addresses	O Deny	Z Extranet	any	Mainternet	 Palo Alto Networks - Bulletproof IP Palo Alto Networks - High risk IP a Palo Alto Networks - Known malici 	any
2	Users_to_Extranet	⊘ Allow	Mage Stress Vet	any	🚧 Extranet	any	any
3	intrazone-default 🛛 🚳	⊘ Allow	any	any	(intrazone)	any	any
4	interzone-default 👸	O Deny	any	any	any	any	any

- 117. Create another rule to block traffic *from* known bad IP addresses.
- 118. In the Security Policy window, click Add.
- 119. For Name, enter Block-from-Known-Bad-Addresses.
- 120. For **Description**, enter **Blocks traffic from known bad IP addresses to Users and Extranet**.
- 121. Select the **Source** tab.
- 122. Under the Source Zone section, click Add.
- 123. Select the **Internet** zone.
- 124. Under the Source Address section, click Add
- 125. Select Palo Alto Networks Bulletproof IP addresses.
- 126. Click Add again under the Source Address section.
- 127. Select Palo Alto Networks High risk IP addresses.

- 128. Click Add again under the Source Address section.
- 129. Select Palo Alto Networks Known malicious IP addresses.

When complete, you should have three Palo Alto Networks IP address lists in the **Source Address** section of the rule.

- 130. Select the **Destination** tab.
- 131. Under the **Destination Zone**, click Add.
- 132. Select the **Users_Net** zone.
- 133. Click Add again under Destination Zone.
- 134. Select Extranet.



Note that you are adding both internal zones to the Destination Zone section of the rule.

- 135. Select the **Application** tab.
- 136. Leave the **Application** set to **any**.
- 137. Under the Service/URL Category tab, set the Service to any.
- 138. Select the Actions tab.
- 139. Change the **Action** to **Deny**.
- 140. Click OK.
- 141. The new rule appears in the Security Policy table.
- 142. Move the Block-to-Known-Bad-Addresses rule to the top of the Security Policy.
- 143. Highlight the entry for Block-from-Known-Bad-Addresses but do not open it.
- 144. At the bottom of the window, choose **Move** and select **Move Top**.
- 145. Both of the rules to block traffic to or from known bad IP addresses should be at the top of the Security Policy.

				Source		Destination	
	NAME	ACTION	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION
1	Block-from-Known-Bad-Addresses	O Deny	Mainternet	 Palo Alto Networks - Bulletproo Palo Alto Networks - High risk I Palo Alto Networks - Known ma 	 Extranet Users_Net 	any	any
2	Block-to-Known-Bad-Addresses	O Deny	Y Extranet	any	Mainternet	 Palo Alto Networks - Bulletproo Palo Alto Networks - High risk I Palo Alto Networks - Known ma 	any
3	Users_to_Extranet	⊘ Allow	🚧 Users_Net	any	🞮 Extranet	any	any
4	intrazone-default 💩	⊘ Allow	any	any	(intrazone)	any	any
5	interzone-default 🚳	O Deny	any	any	any	any	any

Create Security Policy Rules for Internet Access

In this section, you will create Security Policy rules to allow hosts in your network to access the Internet. You need to create a rule for hosts in the Users_Net security zone to access hosts in the Internet security zone. You also need to create a rule to allow hosts in the Extranet security zone to access hosts in the Internet security zone.



Create Users to Internet Security Policy Rule

- 146. Select **Policies > Security**.
- 147. Click **Add** at the bottom of the window.
- 148. Under the tab for **General**, in the **Name** field, enter **Users_to_Internet**.
- 149. For **Description**, enter **Allows hosts in Users_Net zone to access Internet zone**.

150. Leave the other settings unchanged:

Security	Policy	Rule
General	Sourc	e Destination Application Service/URL Category Actions
	Name	Users_to_Internet
Ru	le Type	universal (default)
Desc	ription	Allows hosts in Users_Net zone to access Internet zone.
	Tags	
Group Rules	By Tag	None

- 151. Select the tab for **Source**.
- 152. Under the **Source Zone** section, click **Add**.
- 153. Select Users_Net.
- 154. Leave the remaining settings unchanged.

Security Policy Rule	Security Policy Rule							
General Source Des	General Destination Application Service/URL Category Actions							
Any	🔽 Any	any 🗸	any 🗸					
	SOURCE ADDRESS	SOURCE USER	SOURCE DEVICE					
Users_Net								
+ Add Delete	🕀 Add 😑 Delete	+ Add - Delete	🕂 Add 😑 Delete					
Negate								

- 155. Select the tab for **Destination**.
- 156. Under the section for **Destination Zone**, click **Add**.
- 157. Select Internet.

158. Leave the other settings unchanged.

Security Policy Rule				
General Source Destination	Application Service/URL Category	Actions		
select ~	🔽 Any	any 🗸		
DESTINATION ZONE	DESTINATION ADDRESS	DESTINATION DEVICE		
Internet				
(+) Add (+) Delete	🛨 Add 😑 Delete	🛨 Add 😑 Delete		
	Negate			

159. Select the tab for **Application**.

160. Do not make any changes to these settings but note that the **Any** box is checked.

Security Policy Rule	
General Source Destination Application Service/URL Category Actions	
Any	Q
APPLICATIONS A	DEI

161. Select the tab for **Service/URL Category**.

162. Do not make any changes to the settings in this tab but note that the **Service** is set to **application-default**.

Service/URL Category Actions
Any
URL CATEGORY A

163. Select the tab for Actions.

164. Make certain that the **Action** is set to **Allow**.

Security Policy Rule	(
General Source Destination Application Service/U	RL Category Actions
Action Setting	Log Setting
Action Allow ~	Log at Session Start
Send ICMP Unreachable	🔽 Log at Session End
	Log Forwarding None V
	Other Settings
Profile Setting	Schedule None 🗸
Profile Type None ~	QoS Marking None
	Disable Server Response Inspection
	OK Cancel

165. Click **OK** on the Security Policy Rule window.

166. The new Security Policy rule appears in the table.

167. Highlight the new rule and use the **Move > Move Bottom** option to place this rule at the end of the Security Policy.

	NAME	ACTION	ZONE	ADDRESS	ZONE	
1	Block-from-Known-Bad-Addresses	O Deny	Mainternet	 Palo Alto Networks - Bulletproo Palo Alto Networks - High risk I Palo Alto Networks - Known ma 	 Extranet Users_Net 	
2	Block-to-Known-Bad-Addresses	O Deny	 Extranet Users_Net 	any	थ Internet	
3	Users_to_Extranet	⊘ Allow	🛛 Users_Net	any	🚧 Extranet	
4	Users_to_Internet	O Allow	🛛 Users_Net	any	Mainternet	
5	intrazone-default 👳	⊘ Allow	any	any 🕂 Move Top	"htrazone)	
6	interzone-default 🚳	O Deny	any	any ↑ Move Up ↓ Move Down ↓ Move Bottom	v]	
(+) Add \ominus Delete 🐵 Clone 🝥 Override 💿 Revert 🥑 Enable 🚫 Disable Move 🗸 💿 PDF/CSV 🗌 Highligh						

Create Extranet to Internet Security Policy Rule

You also need to create a Security Policy rule to allow servers in the Extranet security zone to access hosts in the Internet security zone.

- 168. Select **Policies > Security**.
- 169. Click **Add** at the bottom of the window.
- 170. Under the tab for **General**, in the **Name** field, enter **Extranet_to_Internet**.
- 171.For **Description**, enter **Allows hosts in Extranet zone to access Internet zone**.

172. Leave the other settings unchanged:

General	Sourc	Destination Application Service/URL Category Actions
	Name	Extranet_to_Internet
R	ule Type	universal (default)
Des	cription	Allows hosts in the Extranet zone to access Internet zone.
	Ŧ	
	lags	
Group Rule	c Ry Tag	None

- 173. Select the tab for **Source**.
- 174. Under the **Source Zone** section, click **Add**.
- 175. Select Extranet.

176. Leave the remaining settings unchanged.

Security Policy Rule	
General Source Destination Applic	ation Service/URL Category A
Any	🔽 Any
	SOURCE ADDRESS
E Extranet	
(+) Add (+) Delete	🕀 Add — Delete
	Negate

- 177. Select the tab for **Destination**.
- 178. Under the section for **Destination Zone**, click **Add**.
- 179. Select Internet.

180. Leave the other settings unchanged.

Security Policy Rule				
General Source Destination	Application Service/URL Category	Actions		
select 🗸	Any	any		
	DESTINATION ADDRESS	DESTINAT		
Internet				
1				
+ Add Delete	+ Add - Delete	↔ Add ⊖ □		
	Negate Negate			

181. Select the tab for **Application**.

182. Do not make any changes to these settings but note that the **Any** box is checked.

Security Policy Rule	
General Source Destination Application Service/URL Category Actions	
Any	Q
APPLICATIONS A	DEI

183. Select the tab for **Service/URL Category**.

184. Do not make any changes to the settings in this tab but note that the **Service** is set to **application-default**.

Security Policy Rule					
Service/URL Category Actions					
Any					
URL CATEGORY					

185. Select the tab for Actions.

186. Make certain that the **Action** is set to **Allow**.

Security Policy Rule	C
General Source Destination Application Service/U	L Category Actions
Action Setting	- Log Setting
Action Allow ~	Log at Session Start
Send ICMP Unreachable	🔽 Log at Session End
	Log Forwarding None
	- Other Settings
Profile Setting	Schedule None 🗸
Profile Type None ~	QoS Marking None
	Disable Server Response Inspection
	OK Cancel

187. Click **OK** on the Security Policy Rule window.

188. The new Security Policy rule appears in the table.

189. Place the rule at the bottom of the Security Policy rule by using **Move > Move Bottom**.

			Source		Desti	
	NAME	ACTION	ZONE	ADDRESS	ZONE	ADDRESS
1	Block-from-Known-Bad-Addresses	O Deny	Manual Internet	Palo Alto Netw Palo Alto Netw Palo Alto Netw Palo Alto Netw	Z Extranet	any
2	Block-to-Known-Bad-Addresses	O Deny	🛛 Extranet	any	M Internet	Palo Alto Netv
3	Users_to_Extranet	O Allow	W Users_Net	any	Z Extranet	any
4	Users_to_Internet	⊘ Allow	W Users_Net	any	M Internet	any
5	Extranet_to_Internet	O Allow	M Extranet	any T Mov	e Top	any
6	intrazone-default 💩	O Allow	any	any J Mov	e Op re Down	any
7	interzone-default 🍈	O Deny	any	any 🛓 Mov	e Bottom e To Position	any
< (+)	Add 🕞 Delete 🌀 Clone 🍈 Over	rride 🛛 🚳 Re	vert 🧭 Enable	🚫 Disable Move 🗸	DF/CSV	Highlight Unuse

Commit the configuration

- 190. Click the **Commit** button at the upper right of the web interface.
- 191. Leave the settings unchanged and click Commit.
- 192. Wait until the **Commit** process is complete.
- 193. Click Close to continue.

Ping Internet Host from Client A

- 194. To verify that your Security Policy rule is allowing traffic, you will ping an Internet host from the client workstation and examine the Traffic log to see the results.
- 195. From the Terminal window on the client desktop, ping an address on the internet by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 8.8.8.8 <Enter>

196. You will not get a reply, so after several seconds, use Ctrl+C to stop the ping.
| lab-user@client-a:~/Desktop/Lak
PING 8.8.8.8 (8.8.8.8) 56(84) k
^C | b-Files \$ ping 8.8.8.8
bytes of data. |
|---|--|
| 8.8.8.8 ping statistics
4 packets transmitted, 0 receiv | -
ved, 100% packet loss, time 3061ms |

- 197.Examine the traffic log again and use a filter to see if there are any entries for this session that failed.
- 198. Select **Monitor** > **Logs** > **Traffic**.

199. In the filter field, update the syntax to include the application ping:

```
( addr.dst in 8.8.8.8 ) and ( app eq ping )
```

🔷 PA-VM	DA	SHBOARD	ACC	ΜΟΝΙ	TOR
√ ີ Logs	ÂQ (ad	ldr.dst in 8.8.8.8)	and (app e	eq ping)	
Traffic		RECEIVE TIM	E FRO	M ZONE	TO ZONE
URL Filtering		11/04 19:32:4	6 Use	rs Net	Internet

200. Click the **Apply filter** button in the upper right corner of the window (or you can press the **Enter** key).



201. The Traffic log will update the display and you should see entries matching the filter.

202. You can see that the sessions are hitting the Users_to_Internet rule.

Q	Q ((addr.dst in 8.8.8.8) and (app eq ping)										
		RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
		09/08 13:59:16	Users_Net	Internet	192.168.1.20	8.8.8.8	0	ping	allow	Users_to_Internet	aged-out

203. Answer the following question:

• Can you explain why your ping session from the client to the Internet host did not get a reply even though the firewall is allowing the traffic?



For a hint, look at the title of the next module.

204. Write down your answer in the field shown or on notepaper in class.



Stop. This is the end of the lab.

Lab 7: Creating and Managing NAT Policy Rules

You need to create Network Address Translation rules to allow hosts in the private network spaces (192.168.1.0/24 and 192.168.50.0/24) to reach hosts on the internet. You will use an interface IP address on the firewall as the source for outbound NAT.

You will also create a static NAT address on the firewall that represents one of the application servers in the Extranet. When traffic reaches the static NAT address the firewall will translate and forward packets to the web server in the Extranet zone.

After you have all these components in place, you will generate test traffic and examine firewall logs.

Lab Objectives

- Configure source NAT
- Configure destination NAT

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-07.xml** to the Firewall

Create a Source NAT Policy Rule

• Use the Information in the tables below to create a new Destination NAT Rule.

General tab

Parameter	Value
Name	Inside_Nets_to_Internet
NAT Туре	ipv4
Description	Translates traffic from Users_Net and Extranet to 203.0.113.20 outbound to Internet

Original Packet tab

Parameter	Value
Source Zone	Users_Net
	Extranet
Destination Zone	Internet
Destination Interface	ethernet1/1
Service	any
Source Address	Any
Destination Address	Any

Translated Packet tab (Source Address Translation section)

Parameter	Value
Translation Type	Dynamic IP And Port
Address Type	Interface Address
Interface	ethernet1/1
IP Address	203.0.113.20/24

Commit the configuration

• Commit the changes before proceeding

Verify Internet Connectivity

- From the Terminal window on the client desktop, ping 8.8.8.8
- You should now receive a reply
- Use the testing browser to connect to www.paloaltonetworks.com
- Browse to several other websites to verify that you can establish connectivity to the Internet security zone
- Examine the firewall **Traffic Log** to verify that there is allowed traffic that matches the Security Policy rule **Users_to_Internet**

Create a Destination NAT Policy

Use the information in the tables below to create a Destination NAT address on the firewall using an IP address on the Users_Net network. The firewall will translate traffic that hits this address to the destination IP address of the web server in the Extranet Zone.

General tab

Parameter	Value
Name	Dest_NAT_To_Webserver
NAT Туре	ipv4

Original Packet tab

Parameter	Value
Source Zone	Users_Net
Destination Zone	Users_Net
Destination Interface	ethernet1/2
Service	any
Destination Address	192.168.1.80

Translated Packet tab (Destination Address Translation section)

Parameter	Value
Destination Address Translation Translation Type	Static IP
Translated Address	192.168.50.80

Commit the configuration

• Commit the changes before proceeding

Test the Destination NAT Rule

- Use the testing browser and connect to http://192.168.1.80 to verify access to the web page for the Extranet server
- Search the Traffic Log to locate entries with a Destination IP of 192.168.1.80
- In the **Security Policy** window, use the **Log Viewer** option for the **Users_to_Extranet** to jump to entries in the Traffic Log that match the rule

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-07.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK** to close the **Load Named configuration** window.
- 5. Click **Close** to close the **Loading configuration** window.
- 6. Click the **Commit** button at the upper right of the web interface.
- 7. Leave the remaining settings unchanged and click **Commit**.
- 8. Wait until the **Commit** process is complete.
- 9. Click **Close** to continue.

Create a Source NAT Policy Rule

You must create entries in the firewall's NAT Policy table in order to translate traffic from internal hosts (often on private networks) to a public, routable address (often an interface on the firewall itself). NAT rules provide address translation and are different from Security Policy rules, which allow and deny packets. You can configure a NAT Policy rule to match a packet's source and destination zone, destination interface, source and destination address, and service.

In your previous ping test to an Internet host, the ping traffic from your client is allowed by the Security Policy rule, but the packets leave the firewall with a non-routable source IP address from the private network of 192.168.1.0/24.

In this section, you will create a NAT Policy rule to translate traffic from the private networks in the Users_Net and Extranet security zones to a routable address. You will use the same interface IP address on the firewall (203.0.113.20) as the source IP for outbound traffic from both Users_Net and Extranet hosts.



10. In the web interface, select **Policies > NAT**.

11. Click **Add** to define a new source NAT Policy.

The **NAT Policy Rule** configuration window should open.

12. Configure the following:

Parameter	Value
Name	Inside_Nets_to_Internet
NAT Type	Verify that ipv4 is selected
Description	Translates traffic from Users_Net and Extranet to 203.0.113.20 outbound to Internet

NAT	NAT Policy Rule					
Gene	eral	Origi	nal Packet Translated Packet			
		Name	Inside_Nets_To_Internet			
	Desc	ription	Translates traffic from Users_Net and Extranet to 203.0.113.20 outbound to Internet			

Parameter	Value
Source Zone	Click Add and select the Users_Net zone
	Click Add and select the Extranet zone
Destination Zone	Select Internet from the drop-down list
Destination Interface	Select ethernet1/1 from the drop-down list
Service	Verify that the any is selected
Source Address	Verify that the Any check box is selected
Destination Address	Verify that the Any check box is selected

13. Click the **Original Packet** tab and configure the following:





This section defines what the packet will look like when it reaches the firewall. Note that we are using a single NAT rule to translate both source zones to the same interface on the firewall. You could accomplish this same task by creating two separate rules – one for each source zone – and using the same external firewall interface.

14. Click the **Translated Packet** tab and configure the following under the section for **Source Address Translation**:

Parameter	Value
Translation Type	Select Dynamic IP And Port from the drop-down list

Parameter	Value				
Address Type	Select Interface Address from the drop-down list				
Interface	Select ethernet1/1 from the drop-down list				
IP Address	Select 203.0.113.20/24 from the drop-down list. (Make sure that you select the interface IP address from the drop-down list and <i>do not type it</i> .)				

NAT Policy Rule	•					?
General Origina	I Packer Translated	Packet				
Source Address Tran	slation		Destination Address T	Translatio	on	
Translation Type	Dynamic IP And Port	\sim	Translati	on Type	None	\sim
Address Type	Interface Address	~				
Interface	ethernet1/1	\sim				
IP Address	203.0.113.20/24	\sim				
				OK	Can	cel



This section defines how the firewall will translate the packet.

Note: You are configuring *only* the **Source Address Translation** part of this window. Leave the destination address translation **Translation Type** set to **None**.

15. Click **OK** to close the **NAT Policy Rule** configuration window.

16. Verify that your configuration matches the following:

		Original P	Translated Packet			
NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE TRANSLATION	DESTINATION TRANSLATION
Inside_Nets_To_Internet	🚧 Extranet	🚧 Internet	any	any	dynamic-ip-and-port	none
	🚧 Users_Net				ethernet1/1	
					203.0.113.20/24	

Note that some columns have been hidden in the image.

Commit the configuration

- 17. Click the **Commit** button at the upper right of the web interface.
- 18. Leave the settings unchanged and click **Commit**.

- 19. Wait until the **Commit** process is complete.
- 20. Click **Close** to continue.

Verify Internet Connectivity

In this section, you will test the configuration of your NAT and Security policies.

21. From the Terminal window on the client desktop, ping an address on the internet by issuing the following command:

lab-user@client-a:~/Desktop/Lab-Files\$ ping 8.8.8.8 <Enter>

You should now receive a reply:

n	lab-user@client-a: ~/Desktop/Lab-Files					
lab-user@client-a:~/Des	sktop/Lab-Files\$ ping 8.8.8.8					
PING 8.8.8.8 (8.8.8.8)	56(84) bytes of data.					
64 bytes from 8.8.8.8:	<pre>icmp_seq=1 ttl=57 time=9.26 ms</pre>					
64 bytes from 8.8.8.8:	<pre>icmp_seq=2 ttl=57 time=2.86 ms</pre>					
64 bytes from 8.8.8.8:	<pre>icmp_seq=3 ttl=57 time=2.53 ms</pre>					
64 bytes from 8.8.8.8:	<pre>icmp_seq=4 ttl=57 time=2.57 ms</pre>					
^C						
8.8.8.8 ping statis	stics					
4 packets transmitted,	4 received, 0% packet loss, time 3005ms					
rtt min/avg/max/mdev =	2.528/4.301/9.256/2.863 ms					
lab-user@client-a:~/Des	sktop/Lab-Files					

- 22. After several seconds, use Ctrl+C to stop the ping.
- 23. Open the testing browser and connect to www.paloaltonetworks.com.
- 24. Browse to several other websites to verify that you can establish connectivity to the Internet security zone.
- 25. Close the testing browser.
- 26. In the configuration browser, examine the firewall Traffic log by selecting **Monitor** > **Logs** > **Traffic**.

27. Clear any filters you have in place by clicking the **Clear Filter** button in the upper right corner of the window.



28. Verify that there is allowed traffic that matches the Security Policy rule Users_to_Internet:

RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
03/03 18:36:29	Users_Net	Internet	192.168.1.254	8.8.8	53	dns	allow	Users_to_Internet
03/03 18:36:19	Users_Net	Extranet	192.168.1.25	192.168.50.53	53	dns	allow	Users_to_Extranet
03/03 18:36:19	Users_Net	Extranet	192.168.1.25	192.168.50.53	53	dns	allow	Users_to_Extranet
03/03 18:36:19	Users_Net	Internet	192.168.1.254	8.8.8	53	dns	allow	Users_to_Internet

Traffic log entries should be present based on the internet test. A minute or two may elapse for the log files to be updated. If the entries are not present, click the **refresh** icon:





Create a Destination NAT Policy

In this section, you will create a NAT address on the firewall using an IP address on the Users_Net network. The firewall will translate traffic that hits this address to the destination IP address of the web server in the Extranet Zone.

You will connect from the client host (192.168.1.20) to the NAT IP address on the firewall (192.168.1.80). The firewall will translate this connection to the DMZ server at 192.168.50.10.

This exercise will help you see how to configure Destination NAT rules.



- 29. In the web interface, select **Policies > NAT**.
- 30. Click **Add** to define a new destination NAT Policy rule.

The **NAT Policy Rule** configuration window should open.

31. Configure the following:

Parameter	Value
Name	Dest_NAT_To_Webserver
Description	Translates traffic to web server at 192.168.50.80
NAT Туре	Verify that ipv4 is selected





32. Click the **Original Packet** tab and configure the following:

Parameter	Value			
Source Zone	Click Add and select Users_Net			
Destination Zone	Select Users_Net from the drop-down list			
Destination Interface	Select ethernet1/2 from the drop-down list			
Service	Select any from the drop-down list			
Destination Address	Click Add and manually enter 192.168.1.80			

NAT Policy Rule	
General Original Packet Translated Pa	cket
Any Destination Zone	Any Any
SOURCE ZONE Users_Net	Source address A Destination address A
Users_Net	192.168.1.80
Destination Interfa	
Service any	Manually enter
(+) Add (-) Delete	↔ Add



The **Original Packet** tab defines how the packet will look when it reaches the firewall. When selecting the Destination Zone, remember that the IP address we are using (192.168.1.80) is one that resides on the firewall in the Users_Net security zone.

33. Click the **Translated Packet** tab and configure the following:

Parameter	Value
Destination Address Translation Translation Type	Select Static IP from the drop-down list
Translated Address	Type 192.168.50.80 (address of the Extranet web server)

NAT Policy Rule				?
General Original Packet	Translated Packet)		
Source Address Translation —	Destination	n Address Translatio	n —	
Translation Type None	~	Translation Type	Static IP	~
	·	Translated Address	192.168.50.80	~
		Translated Port	[1 65535]	
	C Enable	DNS Rewrite		
		Direction	reverse	\sim



The **Translated Packet** tab defines how the firewall will translate a matching packet. Leave the **Source Address Translation** section set to **None** because we are performing only destination translation in this exercise.

34. Click **OK** to close the **NAT Policy Rule** configuration window.

A new NAT Policy rule should display in the web interface.

			Original Packet				Translated Packet	
	NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE TRANSLATION	DESTINATION TRANSLATION	
1	Inside_Nets_to_Internet	🚧 Extranet 🚧 Users_Net	Mainternet	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none	
2	Dest_NAT_To_Webserver	Users_Net	🛛 Users_Net	any	192.168.1.80	none	destination-translation address: 192.168.50.80	

35. Verify that your configuration matches the following:

Commit the configuration

- 36. Click the **Commit** button at the upper right of the web interface.
- 37. Leave the settings unchanged and click **Commit**.
- 38. Wait until the **Commit** process is complete.
- 39. Click **Close** to continue.

Test the Destination NAT Rule

In this section you will test the destination NAT Policy rule by opening a browser connection to the NAT IP address 192.168.1.80.

- 40. Open the testing browser and connect to http://192.168.1.80.
- 41. Verify that you can view the web page for the Extranet server:



- 42. Close the testing browser window.
- 43. In the web interface, select **Monitor > Logs > Traffic**.
- 44. Use a filter to locate the entry for Destination IP 192.168.1.80:
- (addr.dst in 192.168.1.80)

Q (addr.dst in 192.168.1.80)

	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
	03/03 18:41:34	Users_Net	Extranet	192.168.1.20	192.168.1.80	80	web-browsing	allow	Users_to_Extranet

- 45. Note the Security Policy rule that was matched: Users_to_Extranet.
- 46. As an alternate method to access the Traffic log in the web interface, select **Policies** > **Security**.



47. Select the drop-down icon next to the rule entry for Users_to_Extranet and choose Log Viewer:



This process opens the Traffic log and applies a filter automatically to display only those entries that match the Security Policy rule "Users_to_Extranet."

🔷 PA-VM	DA	SHBOARD	ACC	MONITOR	POLICIES
∼ ີ Logs		e eq 'Users_to_Extra	anet')		
Traffic		RECEIVE TIME	FROM	TO ZONE	SOURCE
	E	07/07 19:39:02	2 Users	Net Extranet	192.168.1.25

48. Click the \mathbf{X} icon to clear the filter from the log filter text box.



Stop. This is the end of the lab.

Lab 8: Controlling Application Usage with App-ID

The old firewalls in your network only allowed you to block or allow traffic using Layer 3 and Layer 4 characteristics. With the deployment of the new Palo Alto Networks firewall, your control over traffic now includes which applications are allowed or blocked into and out of your network.

The list of applications that Palo Alto Networks maintains is long, but you already know some of the applications that you must allow from and to your security zones. You will create an Application Group and include individual applications that the Palo Alto Networks devices use. You will then use this Application Group as part of a Security Policy rule. This process will give you practice in creating Security Policy rules that take advantage of applications instead of simply Layer 3 and Layer 4 traffic characteristics.

Lab Objectives

- Load a baseline configuration
- Generate application traffic
- Configure an application group
- Configure a Security Policy to allow update traffic
- Test the Allow-PANW-Apps Security Policy rule
- Identify shadowed rules
- Modify the Security Policy to function properly
- Test the modified Security Policy rule

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-08.xml** to the Firewall.

Configure an Application Group

• Use the information below to create an Application Group

Parameter	Value
Name	paloalto-apps
Applications	paloalto-dns-security

Parameter	Value
	paloalto-updates
	paloalto-wildfire-cloud
	pan-db-cloud

Configure a Security Policy Rule to Allow Update Traffic

• Use the information below to create a Security Policy rule to allow Palo Alto Networks update traffic.

Parameter	Value
Name	Allow-PANW-Apps
Description	Allows PANW apps for firewall
Source Zone	Users_Net
Source Address	192.168.1.254
Destination Zone	Internet
Destination Address	Any
Applications	paloalto-apps
Service	application-default
URL Category	Any
Action	Allow
Log At Session End	Enabled

Commit the configuration

• Commit the changes before proceeding

Test the Allow-PANW-Apps Security Policy Rule

- On the firewall, use the **Check Now** option for Dynamic Updates to test the Security Policy rule **Allow-PANW-Apps**.
- Create and apply a filter to search for log entries that contain the application **paloalto-updates**
- Note which rule allowed the application traffic to pass through the firewall
- Determine why the firewall traffic did not hit the Allow-PANW-Apps rule

Identify Shadowed Rules

- Use the **Tasks Manager All Tasks** window to locate the most recent entry for **Commit** under **Type**
- Use the information in the **Rule Shadow** tab to determine why firewall traffic did not hit the **Allow-PANW-Apps** rule

Modify the Security Policy to Function Properly

• Use the information below to update the **Users_to_Internet** Security Policy rule to allow only specific applications (instead of any).

Parameter	Value
Applications	dns
	ping
	ssl
	web-browsing

Commit the configuration

• Commit the changes before proceeding and verify that you do not get any commit warnings about **Rule Shadowing**

Test the Modified Security Policy Rule

- On the firewall, use the **Check Now** option for Dynamic Updates to test the Security Policy rule **Allow-PANW-Apps**.
- Create and apply a filter to search for log entries that contain the application **paloalto-updates**
- Note which rule allowed the application traffic to pass through the firewall

Generate Application Traffic

- Generate application traffic by double-clicking on the icon for **App Generator** on the Client-A desktop
- Allow the script to complete
- Examine the **Traffic Log** and note the entries under the **Application** column for the Client-A host
- Use the information in the columns for **Application**, **Action** and **Rule** to answer the following questions.
 - Are there any applications that you should not allow from the Users_Net zone to the Extranet zone?

• Are there any applications being denied from the Users_Net zone that you should allow?

Research Applications

- Use the Application database on the firewall to research one of the three applications below:
 - dailymotion
 - yammer-base
 - scribd-base
- Answer the following questions about the application you have chosen to research:
 - What category does the application fall into?
 - What risk level has Palo Alto Networks assigned to the application?
 - What are some of the characteristics of this application that might make you want to block its use on your network?
 - Should you allow this application on your company's production network?

Update Security Policy Rules

- Edit the Users_to_Extranet Security Policy rule and allow only the following applications:
 - web-browsing
 - ssl
 - ssh
 - ping
 - dns
 - ldap
 - radius
- Edit the Users_to_Internet Security Policy rule and allow only the following applications and their dependencies.
 - dns
 - ping
 - ssl
 - web-browsing
 - yelp
 - dropbox

• ms-office365

Commit the configuration

• Commit the changes before proceeding

Test the Updated Security Policy Rules

- Run the Traffic Generator script again on the Client-A desktop (App Generator)
- Create and apply a filter in the **Traffic** log to display sessions that the firewall has blocked
- Note the applications that are now being blocked.

Enable the Application Block Page

- To see the kind of behavior a user will experience without the **Application Block Page** enabled, open the testing browser and attempt to connect to **http://www.shutterfly.com**.
- Note how the browser responds.
- Enable the **Application Block Page** under **Device** > **Response Pages**.

Commit the configuration

• Commit the changes before proceeding

Test the Application Block Page

- To see the kind of behavior a user will experience with the **Application Block Page** enabled, open the testing browser and attempt to connect to **http://www.shutterfly.com**.
- Note how the browser responds.

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-08.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click OK.
- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.

Configure an Application Group

In this section, you will configure an application group called **paloalto-apps** that includes some Palo Alto Networks applications. The firewall uses these applications to label and control access to the content update network and other Palo Alto Networks products and features. You will add the application group to a Security Policy rule later in this lab exercise.



10. In the web interface, select **Objects > Application Groups**.

11. Click **Add** and configure the following:

Parameter	Value
Name	paloalto-apps
Applications	paloalto-dns-security
	paloalto-updates
	paloalto-wildfire-cloud
	pan-db-cloud

?

Application Group

Name paloalto-apps	
Q	$_{4\text{items}}$ \rightarrow \times
APPLICATIONS	
paloalto-dns-security	
paloalto-updates	
paloalto-wildfire-cloud	
pan-db-cloud	
☐ Browse ⊕ Add ─ Delete	

Õ

Note that we are only adding a few of the Palo Alto Networks entries to this group as an example of how to create an Application Group. The list you are building here is not necessarily inclusive of all Palo Alto Networks applications that you might need to allow in a production environment.

Cancel

You can also use the **Browse** button in the Application Group window to add these entries.

12. Click **OK** to close the **Application Group** window.

Configure a Security Policy Rule to Allow Firewall Update Traffic

In this section, you will create a specific Security Policy rule to allow the firewall to use Palo Alto Networks applications, including content updates.

- 13. Select **Policies > Security**.
- 14. Click **Add** to create a new Security Policy rule.
- 15. On the **General** tab, type **Allow-PANW-Apps** as the **Name**.
- 16. For **Description**, enter **Allows PANW** apps for firewall.
- 17. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	Users_Net
Source Address	192.168.1.254



Note that 192.168.1.254 is the IP address of the management interface on the firewall.

18. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Internet
Destination Address	Any

19. Click the **Application** tab and configure the following:

Parameter	Value
Applications	paloalto-apps



To locate your **paloalto-apps** Application Group, start typing in the first few letters of the group name, and the interface will display only those entries that match. Application Groups appear at the very end of the Application list.

Security Policy Rule
General Source Destination Application Service/URL Cate
Any
APPLICATIONS A
Paloalto-apps
(+) Add (-) Delete

- 20. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.
- 21. Click the **Actions** tab and verify the following:

Parameter	Value
Action	Allow
Log Setting	Log at Session End

22. Click **OK** to close the **Security Policy Rule** window.

The "Allow-PANW-Apps" rule should be listed just above the "intrazone-default" rule in the Security Policy rule list.

			Source	Destination			
	NAME	ACTION	ZONE	ZONE	APPLICATION	URL CATEGORY	PROFILE
1	Block-Known-Bad-IPs	O Deny	🚧 Extranet	Mage Internet	any	any	none
			Mage Street Street				
2	migrated-ftp-rule-port-based	⊘ Allow	🛛 Users_Net	🞮 Extranet	any	any	none
3	Users_to_Extranet	⊘ Allow	Mage Stress Vet	Mage Extranet	any	any	none
4	Users_to_Internet	⊘ Allow	🛛 Users_Net	M Internet	any	any	A@
5	Extranet_to_Internet	⊘ Allow	🚧 Extranet	Mainternet	any	any	none
6	Allow-PANW-Apps	⊘ Allow	🛛 Users_Net	Magnetic Internet	Paloalto-apps	any	none
7	intrazone-default 👩	⊘ Allow	any	(intrazone)	any	any	none
8	interzone-default 🛛 🏀	O Deny	any	any	any	any	none

Some of the columns in the Security Policy table shown here have been hidden or rearranged.

Commit the configuration

- 23. Click the **Commit** button at the upper right of the web interface.
- 24. Leave the settings unchanged and click Commit.
- 25. Wait until the **Commit** process is complete.
- 26. When the commit process completes, notice that there is an additional tab available for **Rule Shadow**.





This tab only appears when you have a rule that shadows other rules. You will fix the rule shadow issue in a later section of the lab.

27. Close the **Commit** window.

Test the Allow-PANW-Apps Security Policy Rule

In this section, you will test the new Security Policy rule for **Allow-PANW-Apps** to see how it is working.

- 28. In the web interface, select **Device > Software**.
- 29. Click Check Now:



This action instructs the firewall to check for new versions of the PAN-OS software. The application used for this task by the firewall is called paloalto-updates and is one that you included in the Application Group called paloalto-apps.

- 30. Select **Monitor > Logs > Traffic**.
- 31. Clear any filters you have in place.
- 32. Create and apply a filter to search for log entries that contain the application paloaltoupdates:
- (app eq paloalto-updates)

Q(i	Q ((app eq paloalto-updates)								
	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
R	03/04 13:52:56	Users_Net	Internet	192.168.1.254	34.96.84.34	443	paloalto-updates	allow	Users_to_Internet
R	03/04 13:50:26	Users_Net	Internet	192.168.1.254	107.178.249.2	443	paloalto-updates	allow	Users_to_Internet
	03/04 13:45:26	Users_Net	Internet	192.168.1.254	107.178.249.2	443	paloalto-updates	allow	Users_to_Internet
	03/04 13:40:26	Users_Net	Internet	192.168.1.254	107.178.249.2	443	paloalto-updates	allow	Users_to_Internet

Leave this filter in place for later testing in this lab.

- 33. Which rule allowed the application traffic to pass through the firewall? It should be the **Users_to_Internet** rule.
- 34. Why did the firewall traffic not use the Allow-PANW-Apps rule?

Because the Users_to_Internet rule 'shadows' the Allow-PANW-Apps rule. Traffic matched the Users_to_Internet rule and the firewall carried out the allow action. There is no reason for the

firewall to continue comparing packet characteristics to any following rules after it has found a match. Remember: Rule order is important!

Identify Shadowed Rules

The firewall provides notification when you have a rule shadowing one or more other rules. The **Rule Shadow** tab appears at the end of the Commit process.

However, you might not always notice the **Rule Shadow** tab, so in this section, you will use the **Task** list to examine your earlier Commit messages.

35. In the bottom right corner of the web browser, click the **Tasks** button.



- 36. In the **Tasks Manager All Tasks** window, scroll down to locate the most recent entry for **Commit** under **Type**.
- 37. Click the link for **Commit**.

Task Manager - All Tasks						
Q			33	$items$ \rightarrow \times		
ТҮРЕ	STATUS	START TIME	MESSAGES	ACTION		
Commit	Completed	09/08/22 17:57:04	Commit Processing By: admin Start Time (Dequeued Time): 09/08/22 17:57:04			
Commit	Completed	09/08/22 17:51:31	Commit Processing By: admin Start Time (Dequeued Time):			

38. Select the **Rule Shadow** tab.

The interface shows you which rule is shadowing other rules.

39. Click the number under **Count** (in this example, the value is 1).

Job Status	- Commit	- Job ID - 58				0	
Operation	Commit						
Status	Completed						
Result	t Successful						
Details	Details Configuration committed successfully Local configuration size: 32 KB Predefined configuration size: 16 MB Merged configuration size(local, panorama pushed, predefined): 17 MB Maximum recommended merged configuration size: 17 MB (100% configured)						
Commit	Rule Shadow	K					
Q		\sim	1 iten	$\rightarrow \times$	Q	1 item $ ightarrow$ $ ightarrow$	
RULE		ТҮРЕ	ςοι	INT V	SHADOWED RULE	^	
Users_to_I	nternet	security-rule	1	\rightarrow	Rule 'Users_to_Intern PANW-Apps'.	net' shadows rule 'Allow-	

Ē

The value under the **Count** column indicates the number of rules that are shadowed. The **Shadowed Rule** column shows you details about which rule is shadowed.

You can use this detailed information to modify your Security Policy rule order to make certain traffic hits rules in the correct manner.

- 40. Close the Job Status Commit window.
- 41. Close the **Task Manager All Tasks** window.

Modify the Security Policy to Function Properly

In this section, you will modify your Security Policy to ensure that firewall update traffic hits the **Allow-PANW-Apps** rule.

- 42. In the web interface, select **Policies > Security**.
- 43. Highlight the entry for Allow-PANW-Apps but do not open it.
- 44. Move the entry to the third row of the Policy just below the two Block rules for known bad IP addresses.



You may drag and drop the **Allow-PANW-Apps** entry to the correct location, or you can use the **Move** button at the bottom to place the rule in the right spot.

		DASHBOARD ACC MC	ONITOR	POLICIES	OBJECTS NETWORK	DEVICE	(
	۵						
1					Source		Destination
		NAME	ACTION	ZONE	ADDRESS	ZONE	ADDRESS
	1	Block-from-Known-Bad-Addresses	O Deny	Mainternet	 Palo Alto Networks - Bulle Palo Alto Networks - High Palo Alto Networks - Kno 	Z Extranet	any
	2	Block-to-Known-Bad-Addresses	O Deny	 Extranet Users_Net 	any	Market Internet	 Palo Alto Networks Palo Alto Networks Palo Alto Networks Palo Alto Networks
	3	Allow-PANW-Apps	⊘ Allow	🛛 Users_Net	192.168.1.254	Mage Internet	any
	4	Users_to_Extranet	⊘ Allow	Mage Stress Vet	any	🞮 Extranet	any
	5	Users_to_Internet	⊘ Allow	Mage Stress Vet	any	Mainternet	any
	6	Extranet_to_Internet	⊘ Allow	🚧 Extranet	any	Mainternet	any

Note that several columns have been hidden or rearranged in the example shown here.

Commit the configuration

- 45. Click the **Commit** button at the upper right of the web interface.
- 46. Leave the settings unchanged and click **Commit**.
- 47. Wait until the **Commit** process is complete.
- 48. Did you get any commit warnings on a **Rule Shadow** tab about one rule shadowing another rule?

You should not receive any commit warnings.

49. Click Close.

Test the Modified Security Policy

In this section, you will test the modified Security Policy to verify that it is working as expected. You want to verify that Dynamic Update traffic from the firewall uses the **Allow-PANW-Apps** rule and not the **Users_to_Internet** rule.

- 50. In the web interface, select **Device > Software**.
- 51. Click **Check Now**:



- 52. Select **Monitor > Logs > Traffic**.
- 53. If your filter is still in place, click the **Apply Filter** button, or create a filter to search for update traffic:

(app eq paloalto-updates)

54. Look for the log entries for the application paloalto-updates. Which rule allowed the application traffic to pass through the firewall?

Q (app eq paloalto-updates) ACTION RECEIVE TIME FROM ZONE SOURCE DESTINATION TO PORT APPLICATION RULE TO ZONE 03/04 14:02:56 192.168.1.254 34.96.84.34 Allow-PANW-Users_Net Internet 443 paloalto-updates allow Apps 03/04 14:02:56 Users Net 192.168.1.254 34.96.84.34 443 paloalto-updates allow Allow-PANW-Internet Apps 03/04 14:02:56 192.168.1.254 34.96.84.34 443 Allow-PANW-Users_Net Internet paloalto-updates allow Apps 03/04 14:02:56 Users_Net Internet 192.168.1.254 34.96.84.34 443 paloalto-updates allow Allow-PANW-Apps

It should be the "Allow-PANW-Apps" rule.

Generate Application Traffic

In this section, you will run a short script that generates application traffic from your client workstation to hosts in the Internet and Extranet security zones.

55. On the client desktop, generate application traffic by double-clicking the icon for **App Generator**:



- 56. Press ENTER in the opened window to start the script.
- 57. Allow the script to complete and then press **ENTER** to close the window.
- 58. Examine the Traffic log by selecting **Monitor > Logs > Traffic**.
- 59. Clear any filters you may have in place.
- 60. Create and apply a filter to display sessions from your client workstation (192.168.1.20) that do not include the application dns:
- (addr.src in 192.168.1.20) and (app neq dns)



Excluding the dns application from the display will make it easier for you to see other applications in use on the network.

61. Note the information under the **Application**, **Action** and **Rule** columns.



You should see entries for a variety of applications. Some of the entries will be recognizable and others will be for applications you may never have heard of.

62. Use the information in the columns for **Application**, **Action** and **Rule** to answer the following questions. You can also use filters to help you find the answers from the Traffic log.

-								
RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
03/08 17:24:20	Users_Net	Internet	192.168.1.20	151.101.0.116	443	yelp-base	allow	Users_to_Internet
03/08 17:24:12	Users_Net	Internet	192.168.1.20	23.221.22.170	443	gotomeeting	allow	Users_to_Internet
03/08 17:24:07	Users_Net	Extranet	192.168.1.20	192.168.50.80	80	web-browsing	allow	Users_to_Extranet
03/08 17:24:04	Users_Net	Internet	192.168.1.20	13.107.6.159	443	yammer-base	allow	Users_to_Internet
03/08 17:24:04	Users_Net	Internet	192.168.1.20	23.216.68.169	443	webex-base	allow	Users_to_Internet
03/08 17:24:04	Users_Net	Internet	192.168.1.20	203.205.251.1	443	wechat-base	allow	Users_to_Internet
03/08 17:24:03	Users_Net	Extranet	192.168.1.20	192.168.50.150	0	ping	allow	Users_to_Extranet
03/08 17:24:03	Users_Net	Internet	192.168.1.20	184.84.66.128	443	viber-base	allow	Users_to_Internet
03/08 17:24:03	Users_Net	Internet	192.168.1.20	216.239.36.21	443	ssl	allow	Users_to_Internet
03/08 17:24:02	Users_Net	Internet	192.168.1.20	104.244.42.193	443	twitter-base	allow	Users_to_Internet
03/08 17:24:02	Users_Net	Internet	192.168.1.20	18.195.149.18	443	teamdrive-base	allow	Users_to_Internet

• Are there any applications that you should not allow from the Users_Net zone to the Extranet zone?

There is no right or wrong answer to this question.

Whether the list of allowed applications is 'correct' or not depends on your environment and the applications and services running on the destination servers.

FTP is an insecure application, and you might be tempted to deny it. However, your organization may have an old process in place that relies on FTP to transfer files. Denying FTP would break that process, so be careful.

You can use the output of the Traffic log to identify the kinds of applications in use in your network. You can then research the applications in question to make an informed decision about them. You can also use the source and destination information to find out more about why an application is in use.

• Are there any applications being denied from the Users_Net zone that you should allow?

Another trick question!

The answer depends on your organization and the applications that are necessary for employees to do their jobs. Although you may not think it appropriate to use social media applications during work, organizations like sales and marketing often use those types of applications to drive awareness and branding. Your company may rely on Dropbox as the sanctioned cloud storage application, so should you be concerned that someone is using boxnet? Or sharefile? What is dailymotion and who uses it?

You cannot answer these kinds of questions intelligently without additional information. Fortunately, Palo Alto Networks provides that kind of information within the firewall itself.

Research Applications

Now that you have access to detailed information about the applications in use in the network, you can use tools available from Palo Alto Networks to help answer the questions at the end of the last section. In this section, you will locate one application and find out more information about it so you can make an informed decision about whether to allow it onto your network or not.

63. In the **Traffic** log, locate the entry for one of the three applications listed below:

- dailymotion
- yammer-base
- scribd-base



Note that you can use the navigation buttons at the bottom of the window, or you can create and apply a filter to locate the application entries.

- 64. Use the **Applications** database to find details about the application you have chosen to research.
- 65. Select **Objects > Applications**.
- 66. In the **Search** field, enter the name of the application as it appears in the Traffic log.
- 67. Click the magnifying glass icon to search.

🚯 PA-VM	DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS
Addresses	Search dailymotion				
Regions	CATEGORY A 1350 business-systems			SUBCA	audio-streaming
Applications	648 collaboration 511 general-internet	23 a 39 d	auth-service latabase		
L Application Groups	324 media	86 €	email		

The previous example shows searching for the **dailymotion** application.

- 68. The **Applications** database will display all entries that match the Search.
- 69. Click directly on the entry for application below the **Name** column.

CATEGORY A	SUBCATEGORY A	RISK	^	TAGS A	
1 media	1 photo-video	1	4	1 Web App	

The previous example shows selecting the **dailymotion** entry.

70. The Applications database entry will display detailed information about the application:

Application		(7
Name: dailyme Standard Ports: tcp/80 Depends on: ssl, wel Implicitly Uses: Deny Action: drop-re Additional Information: Wikipe	otion ,443 b-browsing eset edia Google Yahoo!	Description: Dailymotion is a video hosting service website, based in Paris, France. Its domain name was registered one month after YouTube (but the site opened one month earlier) with gandi.net, a French internet domain name provider, and at least one name server is based in France with th .fr name extension.
Characteristics Evasive: yes T Excessive Bandwidth Use: yes Used by Malware: no Capable of File Transfer: yes Has Known Vulnerabilities: yes Classification Category: media Subcategory: photo-video Risk: 4 Customize	unnels Other Applications: Prone to Misuse: Widely Used:	Options TCP Timeout (seconds): 3600 Customize TCP Half Closed (seconds): 120 Customize TCP Time Wait (seconds): 15 Customize App-ID Enabled: yes

71. Answer the following questions about the application you have chosen to research.

• What category does the application fall into?

In the bottom left corner of the window under the Classification section, you can see the entry for Category.

• What risk level has Palo Alto Networks assigned to the application?

The Risk level will be listed under the Classification section on a scale of 1 (Safe) to 5 (Very Risky).

• What are some of the characteristics of this application that might make you want to block its use on your network?

Under the Characteristics section of the window you can see a list of traits for the application. A Yes answer for a characteristic increases the risk rating of that application.

• Should you allow this application on your company's production network?

Note that this last question does not have a right or wrong answer. Whether you allow an application on your network depends on numerous factors. Even if the application presents some risk, your organization may need to use it ("I can't do my job without it!"), or there may be lots of employees that prefer the application over safer alternatives ("We've always used this application!"). Part of your job as a security professional is to identify network risks and to
mitigate them when possible. You can use the detailed information about applications on your network to advocate for safer alternatives when possible.

72. Click **Close** in the Application window.

Update Security Policy Rules

When you created the **Users_to_Extranet** and the **Users_to_Internet** Security Policy rules in an earlier lab, you set the **Application** to **Any**.

After your research, you can now update both rules to allow only applications that are necessary for your organization.

- 73. Navigate to **Policies > Security**.
- 74. Edit the entry for **Users_to_Extranet**.
- 75. Select the tab for **Application**.
- 76. **Uncheck** the option for **Any**.
- 77. Click Add under the Applications section.
- 78. Type in the first few letters of **web-browsing** and allow the list to update with the available selection.

Sec	Security Policy Rule				
Ge	eneral Source Destination Application Service/URL Cate				
	Any				
	APPLICATIONS				
	web-bro				
	Application				
	web-browsing				
	New 🛃 Application Filter 🛛 🕞 Application Group				

79. Select the entry for **web-browsing** to add it to the list.

Security Policy Rule			
General Source Destination	Application Service/UI		
Any			
web-browsing			
🕀 Add 😑 Delete			

- 80. Click Add again.
- 81. Enter **ssl** and choose it from the list.
- 82. Repeat this process and add the following applications to this Security Policy rule:
 - ssh
 - ping
 - dns
 - ldap
 - radius
- 83. When complete, your list of applications should look like the following:

	Sec	urity Policy Rule	
	Ge	neral Source Destination Application Service/UR	LC
	A	Any	
		APPLICATIONS	
(🖽 dns	
		🔝 ldap	
		i ping	
		🗊 radius	
		≣ ssh	
		≣ ssl	
l		I web-browsing	
	÷	Add 🕞 Delete	

- 84. Click **OK** to close the Security Policy rule.
- 85. In the Security Policy table, click the entry for **Users_to_Internet** to edit it.
- 86. Select the tab for **Application**.
- 87. Uncheck the box for **Any**.
- 88. Add the following applications to this Security Policy rule:
- dns
- ping
- ssl
- web-browsing
- yelp
- dropbox



Note – when you add the **dropbox** application, the web interface adds an entry to the **Depends On column** for the **google-base** application.

• ms-office365



Note – when you add **ms-office365**, the web interface adds additional applications to the Depends On list.

89. When complete, the **Applications** list should have seven entries and the **Depends On** list should have multiple entries.

Security Policy Rule (?)					
General Source Destination Applicat	tion Service/URL Category Actions	Usage			
Any	QC	12 items \rightarrow \times			
	DEPENDS ON A				
L 🗊 dropbox	google-base	A			
🔲 📰 ms-office365	hotmail	Automatically			
imping	http-audio	added			
	http-video				
	office365-consumer-access				
iii web-browsing	office365-enterprise-access				
U jij yelp	- rtcp	-			
	Add To Current Rule Add To Exi	sting Rule			



Note that the list of applications in the **Depends On** column may differ from the example shown here. Palo Alto Networks updates application definitions frequently, and in many cases an existing application will require additional applications to work correctly.

- 90. Place the check box next to **Depends On** to select all items in that column.
- 91. Click Add to Current Rule.

Security Policy Rule (?)				
General Source Destination Applicat	ion Service/URL Category Actions Usage			
Any	$\bigcirc \qquad 12 \text{ items} \rightarrow \times$			
	DEPENDS ON A			
🔲 🗐 dns	google-base			
Generation of the second secon	hotmail			
ms-office365	http-audio			
	http-video			
	office365-consumer-access			
	office365-enterprise-access			
web-browsing	▼ V rtcp ▼			
🛨 Add 😑 Delete	Add To Current Rule Add To Existing Rule			
	OK Cancel			

- 92. Scan through the list of **Applications** on the left side of the window and note that the dependent applications have been added.
- 93. Click **OK.**

Commit the configuration

- 94. Click the **Commit** button at the upper right of the web interface.
- 95. Leave the settings unchanged and click **Commit**.
- 96. Wait until the **Commit** process is complete.
- 97. Click **Close** to continue.

Test the Updated Security Policy Rules

Run the application script again and examine the results.

98. On the client desktop, generate application traffic by double-clicking the icon for **App Generator**:



99. Press ENTER in the opened window to start the script.

100. Allow the script to complete and then press ENTER to close the window.



Ignore any errors that the script generates – these occur because the firewall is blocking various application traffic types. The script may also pause at different points while applications time out because they are being blocked by the firewall.

- 101. When the script is complete, press **ENTER** to close the window.
- 102. Examine the Traffic log by selecting **Monitor > Logs > Traffic**.
- 103. Clear any filters you may have in place.
- 104. Create and apply a filter to display sessions that the firewall has blocked:
 - (action neq allow)



This filter will allow you to see the applications that have been blocked.

105. Note the entries under the **Application** column:

Q ((action neq allow)									
RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
09/08 18:34:31	Users_Net	Internet	192.168.1.20	13.107.6.159	443	yammer-base	reset-both	interzone-default	policy-deny
09/08 18:34:31	Users_Net	Internet	192.168.1.20	23.64.139.64	443	webex-base	deny	interzone-default	policy-deny
09/08 18:34:31	Users_Net	Internet	192.168.1.20	23.211.76.194	443	viber-base	deny	interzone-default	policy-deny
09/08 18:34:31	Users_Net	Internet	192.168.1.20	104.244.42.129	443	twitter-base	reset-both	interzone-default	policy-deny
09/08 18:34:31	Users_Net	Internet	192.168.1.20	18.195.149.18	443	teamdrive-base	reset-both	interzone-default	policy-deny
09/08 18:34:31	Users_Net	Internet	192.168.1.20	192.0.77.40	443	tumblr-base	reset-both	interzone-default	policy-deny

Many of the applications are now being blocked by the interzone-default rule. Remember that any application that is not explicitly allowed in a Security Policy rule will be blocked by the interzone-default rule.

The entries you see will differ from the example shown here.

106. Clear the filter in the Traffic log.

Enable the Application Block Page

When the firewall denies traffic to a web-based application, many users may assume that the Internet is down or slow or that there is something wrong with their browser settings.

To reduce the number of potential calls to the help desk, you can enable the **Application Block Page** on the firewall. This setting presents a web page that informs users when the firewall has blocked a web-based application.

By default, the **Application Block Page** is not enabled.

- 107. To see the kind of behavior a user will experience without the Application Block page enabled, open the testing browser.
- 108. Attempt to connect to http://www.shutterfly.com.



Note: Be sure to type in the URL as shown above – include **http** as the protocol for the request.

- 109. The browser will not be able to connect and will eventually time out (note that you do not have to wait until you receive the time out message before continuing to the next step).
- 110. Close the testing browser.
- 111. In the firewall web interface, select **Device > Response Pages**.
- 112. Under the Action column in the row for Application Block Page, click the link for Disabled.



113. Place a check in the box for **Enable Application Block Page**.

Applicati	on Block Page	?
	Enable Application Block Page	
	ОК	Cancel

114. Click **OK**.

Commit the configuration

- 115. Click the **Commit** button at the upper right of the web interface.
- 116. Leave the settings unchanged and click **Commit**.
- 117. Wait until the **Commit** process is complete.

118. Click **Close** to continue.

Test the Application Block Page

119. To see the kind of behavior a user will experience with the Application Block page enabled, open the testing browser.

120. Attempt to connect to http://www.shutterfly.com.

Be sure to use http in the request and be sure to use the configuration browser for this test.



The number of websites which still support HTTP is dwindling. And, some browsers automatically send requests using HTTPS even if you specify HTTP.

This test is only to show you how to enable the block page. In order for the firewall to determine an application inside encrypted web traffic (HTTPS), you need to enable decryption which is covered in a later section of this course.

121. The firewall will present a web page indicating that the application has been blocked.



You can customize this page to include additional information if necessary. This is the default page that the firewall presents.



Note: Response Pages must also be enabled on the Interface Management Profile assigned to the firewalls interface that is required to respond. This was completed in an earlier lab.

122. Close the testing browser.

Note that there are limitations to the Application Block Page. The firewall cannot present the page to a user when the browser session is encrypted using HTTPS. Doing so would interrupt the secure communication between the client and the destination server and violate the rules of encryption.



However, you can configure and enable decryption on the firewall (which we cover in a later module). With decryption enabled, the firewall can present the Application Block Page to a web browser when a user attempts to access a blocked application.



Stop. This is the end of the lab.

Lab 9: Blocking Known Threats Using Security Profiles

Your organization recently acquired another company. Over the weekend one of your coworkers configured the firewall with a new security zone called Acquisition that contains all the users from this new company.

The coworker also configured the firewall with a Virtual Wire that allows traffic to the Internet from the users in the Acquisition security zone.

Traffic is now being forwarded from users in the acquisition company through the firewall.



The firewall has a Security Policy rule that allows users in the Acquisition zone to access any application on the Internet.

In this lab, you will build and apply a set of Security Profiles that will watch for and block known threats from the users in this Acquisition zone.

Lab Objectives

- Load a baseline configuration
- Generate traffic without Security Profiles and examine logs
- Create Security Profiles
- Create a Security Profile Group
- Apply the Security Profile Group to existing Security Policy rules

• Generate traffic with Security Profiles and examine logs

High-Level Lab Steps

Use the information in the sections below to complete the objectives for this lab. We suggest that you use this section only if you have extensive experience working with Palo Alto Networks firewalls.

If you need more detailed guidance for the objectives, use the Detailed-Lab Steps section.

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-09.xml** - to the Firewall

Generate Traffic Without Security Profiles

- Use Remmina to connect to the Server-Extranet host
- Change to the working directory

cd pcaps92019/attack.pcaps/ <Enter>

• Run the simulated attacks script

./malwareattacks.sh <Enter>

This script takes about 6 minutes to complete

- Allow the script to run uninterrupted
- Use testing browser on the Client-A workstation to connect to the following URI: http://192.168.50.80/badtarfile.tar
- Save the file to the **Downloads** folder when prompted
- From a new tab in testing browser, browse to the following URI:

http://192.168.50.80/companyssns.txt

Note that the browser will displays a file with employees and their Social Security Numbers.

• From a **Terminal** window on the Client-A host, use the following command to generate a DNS query using **dig** to resolve a URL to an IP address:

dig @8.8.8.8 www.quora.com

The command should return a public IP address, indicating that the URL is accessible.

- Leave the Terminal Emulator window open because you will use it again later in this lab
- In the firewall web interface, examine the **Threat Log**
- You should have <u>no</u> significant entries in the Threat Log

Create a Corporate Antivirus Profile

• Clone the **default** Antivirus Profile

- Rename the clone to **Corp-AV**
- For the Corp-AV **Description**, enter **Standard antivirus profile for all** security policy rules

Create A Corporate Vulnerability Security Profile

- Clone the **strict** Vulnerability Profile
- Rename the clone to **Corp-Vuln**
- For the Corp-Vuln **Description**, enter **Standard vulnerability profile for** all security policy rules

Create a Corporate File Blocking Profile

- Clone the **strict file blocking** Profile
- Rename the clone to **Corp-FileBlock**.
- For the Corp-FileBlock **Description**, enter **Standard file blocking profile** for all security policy rules.

Create a Corporate Data Filtering Profile

• Use the information below to create a Data Filtering Pattern that will identify US Social Security numbers with and without dash separators

Parameter	Value
Name	US-SSNs
Description	US Social Security Numbers
Pattern Type	Predefined Pattern
First Pattern	Social Security Numbers
Second Pattern	Social Security Numbers (without dash separator)

• Use the information below to create a **Data Filtering** Profile

Parameter	Value
Name	Corp-DataFilter
Description	Standard data filtering profile for all security rules
Data Pattern	US-SSNs
Alert Threshold	1

Parameter	Value
Block Threshold	3
Log Severity	critical

Create a Corporate Anti-Spyware Security Profile

- Clone the **strict** Anti-Spyware Profile
- Rename the clone **Corp-AS**
- For the Corp-AS **Description**, enter **Standard anti-spyware profile for all** security policy rules

Create an External Dynamic List for Malicious Domains

Parameter	Value
Name	malicious-domains-edl
Туре	Domain List
Description	Custom list of bad domains maintained on Extranet server
Source	http://192.168.50.80/malicious-domains.txt
	(The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	Checked
Check for updates	Every Five Minutes

• Use the information below to create an External Dynamic List

Update the Anti-Spyware Profile with EDL

• Edit the **Corp-AS** Security profile and apply the DNS **sinkhole** action to the entry for **malicious-domains-edl**

Commit the configuration

• Commit the changes before proceeding

Create a Security Profile Group

• Use the information below to create a Security Profile Group

Parameter	Value
Name	Corp-Profiles Group
Antivirus Profile	Corp-AV
Anti-Spyware Profile	Corp-AS
Vulnerability Protection Profile	Corp-Vuln
URL Filtering Profile	none
File Blocking Profile	Corp-FileBlock
Data Filtering Profile	Corp-DataFilter
Wildfire Analysis Profile	none



Leave the URL Filtering Profile and the WildFire Analysis Profile set to **none** for this lab. We will examine both of those Security Profiles in more detail later in the course.

Apply the Corp-Profiles-Group to Security Policy Rules

- Individually edit each Security Policy rule that allows traffic and change the **Profile Setting** under the **Action** tab to use the **Corp-Profiles Group**
 - Allow-PANW-Apps
 - Users_to_Extranet
 - Users_to_Internet
 - Extranet_to_Internet
 - Extranet_to_Users_Net
 - Acquisition-Allow-All

Commit the configuration

• Commit the changes before proceeding

Generate Attack Traffic to Test Security Profiles

- Use Remmina to connect to the **Server-Extranet** host
- Change to the working directory
 - cd pcaps92019/attack.pcaps/ <Enter>

• Run the simulated attacks script

./malwareattacks.sh <Enter>

This script takes about 6 minutes to complete

- Allow the script to run uninterrupted
- Use testing browser on the Client-A workstation to connect to the following URI:

http://192.168.50.80/badtarfile.tar

- You should receive a File Transfer Blocked page from the firewall.
- From a new tab in testing browser, browse to the following URI:

http://192.168.50.80/companyssns.txt

- You should receive a **Data Transfer Blocked** page from the firewall
- From a **Terminal** window on the Client-A host, use the following command to generate a DNS query using **dig** to resolve a URL to an IP address:

dig @8.8.8.8 www.quora.com

This time, the command returns **sinkhole.paloaltonetworks.com** instead of an IP address for the domain.

• In the firewall web interface, examine the **Threat Log** and note the numerous entries for spyware and vulnerabilities

Lab Clean-Up

- Close the SSH connection to the firewall
- Close the Remmina desktop application window
- Close the Terminal Emulator window on the workstation desktop

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-9.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

4. Click OK.

- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.



Note that you may receive messages in the **Commit** window about **App Dependencies**. In a production environment, you should examine the messages and use the information provided to add the missing applications to the appropriate rules. These dependencies result from changes in Application definitions that are released each month.

Generate Traffic Without Security Profiles

In this section, you will generate traffic that contains threats and malicious content. You will do so from the client workstation and from the Extranet server. Because you have not yet configured Security Profiles for your Security Policy, the firewall will allow this harmful traffic.

After the testing, you will examine the Threat Log to verify that this traffic was passed.

10. On the client desktop, open the Remmina application by double-clicking the icon:



11. In the Remmina Remote Desktop Client window, double-click the entry for **Server-Extranet**:

				Remm	ina Remote Desktop Client Remote Desktop Client	=
	R	DP 🔻 🗌				
Name	Ŧ	Group	Server	Plugin	Last used	
🔒 Berlin-Cl	ient		192.168.1.25	SSH	2022-09-02 - 07:04:25	
🔒 Firewall-	A		192.168.1.254	SSH	2022-09-07 - 07:51:44	
🔒 Firewall-	в		192.168.1.253	SSH	2022-08-01 - 10:40:43	
Panoram	a		192.168.1.252	SSH	2022-08-30 - 07:00:17	
Server-E	xtranet	1	192.168.50.10	SSH	2022-06-22 - 12:39:06	

This action will open an SSH connection to the server and automatically log you in with appropriate credentials.

12. Enter the following command to change the working directory:

cd pcaps92019/attack.pcaps/ <Enter>

13. Run the simulated attacks:

./malwareattacks.sh <Enter>

This script takes about 6 minutes to complete.

- 14. Allow the script to run uninterrupted.
- 15. Minimize the Remmina connection window and move to the next step.
- 16. On the client workstation, open the testing browser.
- 17. Connect to the following URI:
- 18. http://192.168.50.80/badtarfile.tar



The download should succeed. This filetype is one that you will block when you configure the firewall with a File Blocking Profile.

19. When prompted, select **Save** and click **OK**.

Cancel	Name badtarfile.tar			٩	Save
🔒 Home	▲ lab-user Downloads >				E
Desktop	Name	▲ \$	Size	Туре	Modified
Documents					
Downloads ■					
Music					
Pictures					
Videos					
+ Other Locations					
				.ta	r,.TAR 🔻

This action saves the malicious tar file to the client Downloads folder.

- 20. In the testing browser, open a new tab.
- 21. Browse to the following URI:

http://192.168.50.80/companyssns.txt

22. The browser will display the file:



- 23. Close the testing browser.
- 24. On the client workstation, open a Terminal Emulator window.
- 25. Enter the following command to generate a DNS query using **dig** to resolve a URL to an IP address:
- dig @8.8.8.8 www.quora.com <Enter>



Quora.com is one of the entries included in an external dynamic list of malicious domains. You will configure this type of list later in the lab.

The **dig** tool is similar to **nslookup** but provides more detailed information.

26. The command returns a public IP address, indicating that the URL is accessible.



Note that the IP address you see may differ from this example.

- 27. Leave the Terminal Emulator window open because you will use it again later in this lab.
- 28. In the firewall web interface, select **Monitor** > **Logs** > **Threat**.
- 29. You should have <u>no</u> significant entries in the Threat Log.

🚺 PA-VM	DAS	HBOARD	ACC	MONIT	OR PC	DLICIES	OBJECTS	NETWC	ORK DEVICE	
V 🕞 Logs	Q									
Traffic							FROM			
📆 Threat		RECEIVE TI	ME TYP	E TI	HREAT ID/N	AME	ZONE	TO ZONE	SOURCE ADDRESS	SOURCE US
🐼 URL Filtering										
🙀 WildFire Submissions										
🛅 Data Filtering										
🛱 HIP Match										
ClobalProtect										
P ID-Tog										

Create a Corporate Antivirus Profile

In this section, you will create the first of several Security Profiles. The Antivirus Profile you create will use signatures provided by Palo Alto Networks to watch for and block known threats from viruses.

- 30. In the web interface, select **Objects > Security Profiles > Antivirus**.
- 31. Place a check in the box next to the **default** entry.

🚺 PA-VM		DASHBO	ARD ACC	: MON	IITOR	POLICIES	OBJECTS N	IETWORK DEVICE	E
V 👩 Custom Objects				Ī				Decoders	
Spyware Ulnerability C URL Category Security Profiles		NAME	LOCATION	PACKET CAPTURE	HOLD MODE	PROTOCOL	SIGNATURE ACTIO	WILDFIRE N SIGNATURE ACTION	WILDFIR
Antivirus		default I	Predefined			http	default (reset-both)	default (reset-both)	default (re
Anti-Spyware						http2	default (reset-both)	default (reset-both)	default (re

- 32. At the bottom of the window, click the **Clone** button.
- 33. In the **Clone** window that appears, leave the settings unchanged.

Clone		?
Selected Objects	NAME	
	default	
	Error out on first detected error in validation	
	OK Cance	el

- 34. Click OK.
- 35. A new entry called **default-1** will appear in the Antivirus list.
- 36. Click the entry for **default-1** to edit it.
- 37. Change the **Name** to **Corp-AV**.
- 38. For **Description**, enter **Standard corporate antivirus profile for all** security policy rules.
- 39. Leave the remaining settings unchanged.

Antivirus Profi	antivirus Profile						
Name Description	Corp-Av Standard corporate	e antivirus profile for all security	y policy rules.				
Action Signat	ure Exceptions	WildFire Inline ML					
PROTOCOL		SIGNATURE ACTION	WILDFIR				
http		default (reset-both)	default (r				
http2 default (reset-both) defa							

40. Click **OK**.

Create A Corporate Vulnerability Security Profile

In this section, you will create a vulnerability Security Profile. Palo Alto Networks provides two Vulnerability Profiles that you can use as the basis for your own – strict and default.

You will clone the strict Profile and modify it to function as your Corp-Vuln Profile.

- 41. Select **Objects > Security Profiles > Vulnerability Protection**.
- 42. Place a check in the box beside **strict**.
- 43. At the bottom of the window, click **Clone**.
- 44. In the Clone window that appears, leave the settings unchanged and click OK.
- 45. A new Vulnerability Protection Profile appears called strict-1.
- 46. Click the entry for **strict-1** to open it.
- 47. Change the **Name** to **Corp-Vuln**.

48. For **Description**, enter **Standard vulnerability profile for all security policy rules**.



49. Leave the remaining settings unchanged and click **OK**.

Create a Corporate File Blocking Profile

In this section, you will configure a File Blocking Security Profile that the firewall will use to help detect, report, and block attempts to download potentially harmful filetypes. Palo Alto Networks provides two File Blocking Profiles that you can use as the basis for your own – basic file blocking and strict file blocking.

You will clone the strict file blocking Profile and modify it to function as your Corp-FileBlock Profile.

- 50. Select **Objects > Security Profiles > File Blocking**.
- 51. Place a check beside the entry for **strict file blocking**.
- 52. At the bottom of the window, click the **Clone** button.
- 53. In the Clone window that appears, leave the settings unchanged and click OK.
- 54. A new File Blocking Profile appears called **strict file blocking-1**.
- 55. Click the entry for strict file blocking-1 to open it.
- 56. Change the **Name** to **Corp-FileBlock**.

57. For **Description**, enter **Standard file blocking profile for all security policy rules**.

File Blocking Profile								
	Name	Corp	Corp-FileBlock					
	Description	Stand	Standard file blocking profile for all security policy rules.					
Q(
	NAME		APPLICATIONS	FILE TYPES				
	Block all risky file types		any	7z				

58. Leave the remaining settings unchanged and click **OK**.

Create a Corporate Data Filtering Profile

Create a Data Filtering Profile to detect and block the transfer of files that contain more than three US social security numbers. Data Filtering Profiles are based on one or more Data Patterns, so you will need to first configure a Data Pattern that matches variations of US social security numbers.

- 59. Select **Objects > Custom Objects > Data Patterns**.
- 60. Click Add.
- 61. For **Name**, enter **US-SSNs**.
- 62. For **Description**, enter US Social Security Numbers.
- 63. Change the **Pattern Type** to **Predefined Pattern**.
- 64. Click Add.
- 65. Scroll down the available list and select **Social Security Numbers**.
- 66. Click **Add** again.

Nar Descripti Pattern Ty	De Predefined P	curity Numbers attern		
		DESCRIPTION	2 iten	ns)→
 Social Security Numbers Social Security Numbers (without dash separator) 		US Social Security Numbers pattern US Social Security Numbers pattern without dash	Any Any	
🕂 Add				

67. Scroll down the list and select Social Security Numbers (without dash separator).

- 68. Leave the remaining settings unchanged and click OK.
- 69. Select **Objects > Security Profiles > Data Filtering**.
- 70. Click Add.
- 71. For Name, enter Corp-DataFilter.
- 72. For **Description**, enter **Standard data filtering profile for all** security policy rules.
- 73. Click Add and select the US-SSNs data pattern that you defined.
- 74. Click in the Alert Threshold field and change the value to **1**.
- 75. Click in the **Block Threshold** field and change the value to **3**.
- 76. Change the **Log Severity** to **critical**.

77. Leave the remaining settings unchanged.

Data Filtering F	Data Filtering Profile					
Name	Corp-DataFilter					
Description	Standard data filtering	g profile for all sec	curity policy rules	5.		
	Data Capture					
Q				\frown		1 item \rightarrow \times
DATA PATTERN	APPLICATIONS	FILE TYPE	DIRECTION	ALERT THRESHOLD	BLOCK THRESHOLD	LOG SEVERITY
US-SSNs	any	Any	both	1	3	critical
+ Add Delete	e alues: (0-65535)				ОК	Cancel

78. Click OK.

Create a Corporate Anti Spyware Profile

In this section, you will create a Security Profile that will watch for and block known spyware.

- 79. In the web interface, select **Objects > Security Profiles > Anti-Spyware**.
- 80. Select the check box next to the **strict** Anti-Spyware Profile. The Profile should be highlighted after it has been selected.
- 81. Click **Clone** to clone the Profile.

_					
ſ	strict	Policies: 5	simple-critical	any	critical
L			simple-high	any	high
			simple-medium	any	medium
			simple- informational	any	informationa
	4		simple-low	any	low
Ŧ		Clone DF/	CSV		

- 82. A **Clone** window should open.
- 83. Click **OK** to close the **Clone** window.

A new **strict-1** Anti-Spyware Profile should have been created.

84. Click **strict-1** to edit the Profile.

The Anti-Spyware Profile window should open.

- 85. Rename the Profile **Corp-AS**.
- 86. For **Description**, enter **Standard anti-spyware profile for all security policy rules**.
- 87. Click **OK** to close the **Anti-Spyware Profile** window.

Create an External Dynamic List for Malicious Domains

You need to configure the firewall to ingest an external dynamic list that contains entries for several malicious domains that users should not access due to company restrictions. You have a list available on a local server that you can import to the firewall.

In this section, you will configure the firewall to import an External Dynamic List (EDL) from a server in the DMZ.

With the list configured on the firewall, you will update the Corporate-AS Anti-Spyware Profile to sinkhole entries in the EDL.

- 88. In the web interface, select **Objects > External Dynamic Lists**.
- 89. Click Add.
- 90. The firewall presents a notice about using trailing slashes for entries:



91. Read the notice and then click **Cancel**.

92. In the External Dynamic Lists window, configure the following:

Parameter	Value
Name	malicious-domains-edl
Туре	Domain List

Parameter	Value
Description	Custom list of bad domains maintained on Extranet server
Source	http://192.168.50.80/malicious-domains.txt (The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	Checked
Check for updates	Every five minutes

External Dynamic Lists	?
Name malicious-domains-edl	
Create List List Entries And Exceptions	
Type Domain List	\sim
Description Custom list of bad domains maintained on Extranet server	
Source http://192.168.50.80/malicious-domains.txt	
Automatically expand to include subdomains	
Server Authentication	
Certificate Profile None	\sim
Check for updates Every five minutes	
Test Source URL OK Cano	:el

93. Click **OK** to close the **External Dynamic Lists** window.

94. Click malicious-domains-edl.

The External Dynamic Lists window should open again.

- 95. Click Cancel on the Append trailing slash to entries window.
- 96. Click **Test Source URL** to verify that the firewall can access the EDL URL.

A message window should open and state that the source URL is accessible.

External Dyna	mic Lists	?
Name	malicious-domains-edl	
Create List	st Entries And Exceptions	
Туре	Domain List	\sim
Description	Custom list of bad domains maintained on Extranet server	
Source	http://192.168.50.80/malicious-domains.txt	
	✓ Automatically expand to include subdomains	
Server Authenticat	ion	
Certificate Profile	None	\sim
Check for updates	Every five minutes	
Test Source URL	ОК Сал	cel

97. Click Close to close the Test Source URL window.

Test Source URL	
Source URL is accessible.	
	Close
	Close

98. Click **OK** to close the **External Dynamic Lists** window.

Update the Anti-Spyware Profile with EDL

Now that you have configured the firewall with the External Dynamic List for custom malicious domains, you can update the Anti-Spyware Profile to use the list for sinkholing.

99. In the web interface, select **Objects > Security Profiles > Anti-Spyware**.

100. Click **Corp-AS** to edit the Profile.

The Anti-Spyware Profile window should open.

- 101. Click the **DNS Policies** tab.
- 102. Under the **External Dynamic Lists** section, change the **Policy Action** drop-down list to **sinkhole** for the **malicious-domains-edl** entry.

nu-spyware Pro	file			(?
Name	Corp-AS			
Description	Standard anti-spyware for all security p	oolicy rules		
Signature Policies	Signature Exceptions DNS Polici	DNS Exceptions	Inline Cloud Analysis	
DNS Policies				
Q.(10 items) \rightarrow)
SIGNATURE SOU	RCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
 External Dynamic 	Lists			
Malicious-domains-edl		medium	sinkhole	disable
🗸 : Palo Alto Network	s Content			
default-paloalto-d	ns		sinkhole	disable
✓ : DNS Security				
	ntrol Domains	default (high)	default (block)	disable
Command and Co	Dynamic DNS Hosted Domains			
Command and Co Dynamic DNS Ho	sted Domains	default (informational)	default (allow)	disable
Command and Co Dynamic DNS Ho Grayware Domain	sted Domains	default (informational) default (low)	default (allow) default (block)	disable disable

103. Leave the remaining settings unchanged.

104. Click **OK** to close the **Anti-Spyware Profile** window.

Commit the configuration

105. Click the **Commit** button at the upper right of the web interface.

106. Leave the settings unchanged and click **Commit**.

- 107. Wait until the **Commit** process is complete.
- 108. Click Close.

Create a Security Profile Group

In order to simplify the process of applying Security Profiles to Security Policy rules, you can create a Security Profile Group that contains individual Security Profiles.

You can then apply the Security Profile Group to a Security Policy rule, rather than individually selecting each Profile for each rule.

In this section, you will create a Security Profile Group called Corp-Profiles-Group. You will add each of your Corp-* Security Profiles to the group.



- 109. Select **Objects > Security Profile Groups**.
- 110. Click **Add**.
- 111. For Name, enter Corp-Profiles-Group.
- 112. For each of the available **Profiles**, use the drop-down list to select the **Corp-*** entry you have created.

Security Profile Group	(?)	
Name	Corp-Profiles-Group	
Antivirus Profile	Corp-Av	~
Anti-Spyware Profile	Corp-AS	~
Vulnerability Protection Profile	Corp-Vuln	~
URL Filtering Profile	None	~
File Blocking Profile	Corp-FileBlock	~
Data Filtering Profile	Corp-DataFilter	~
WildFire Analysis Profile	None	~



Leave the URL Filtering Profile and the WildFire Analysis Profile set to None for this lab. We will examine both of those Security Profiles in more detail later in the course.

113. Click OK.

Apply the Corp-Profiles-Group to Security Policy Rules

With the Security Profiles in place, you can modify your Security Policy rules to use these protections.

114. Select **Policies > Security**.

115. Individually edit each Security Policy rule that <u>*allows*</u> traffic and change the **Profile Setting** under the **Action** tab to use the **Corp-Profiles Group**:

Security Policy Rule	
General Source Destination Application Service/URL Category Actions	Usage
Action Setting	Log S
Action Allow	~
Send ICMP Unreachable	
	L
Profile Setting	Othe
Profile Type Group	\sim
Group Profile Corp-Profiles-Group	\sim

116. Be sure to edit and modify each of these rules:

- Allow-PANW-Apps
- Users_to_Extranet
- Users_to_Internet
- Extranet_to_Internet
- Extranet_to_Users_Net
- Acquisition-Allow-All

Commit the configuration

117. Click the **Commit** button at the upper right of the web interface.

118. Leave the settings unchanged and click **Commit**.

- 119. Wait until the **Commit** process is complete.
- 120. Click Close.

Generate Attack Traffic to Test Security Profiles

121. On the client desktop, locate the Remmina SSH connection to Server-Extranet.

122. Enter the following command to change the working directory:

cd /home/paloalto42/pcaps92019/attack.pcaps/ <Enter>

123. Run the simulated attacks script again:

./malwareattacks.sh <Enter>

This script takes about 6 minutes to complete.

- 124. Allow the script to run uninterrupted.
- 125. Minimize the Remmina connection window and move to the next step.
- 126. On the client workstation, open the testing browser.

127. Connect to the following URI:

http://192.168.50.80/badtarfile.tar

128. You should receive a File Transfer Blocked page from the firewall.



This page indicates that the firewall has blocked the file using the File Blocking Profile you defined.



If testing browser prompts you to save the file, clear the browser cache (Settings > Privacy and Security > Clear browsing data and click Clear Data). Close testing browser and try the test again.

You can also use CTRL + Shift + Delete as a shortcut to invoke the **Clear Recent History** window in Firefox. The same key sequence invokes the **Clear browsing data** window in Chromium.

129. In testing browser, open a new tab.130. Browse to the following URI:http://192.168.50.80/companyssns.txt







If you see the companyssns.txt file, **clear the browser cache and try again**. Often browsers will display content from earlier sessions so you want to make certain your request is actually sent to the server so that the firewall can intercept and block the reply which contains Social Security Numbers.

1	-6		
	_	\checkmark	
	_	~	
	_	- 1	
	_	- 1	
•			

This page indicates that the firewall has blocked the transfer using the Data Filtering Profile and Data Pattern you defined for Social Security Numbers.

- 132. Close the testing browser.
- 133. On the client workstation, locate the open Terminal Emulator window you used earlier in this lab.
- 134. Run the **dig** command again to resolve a URL to an IP address:
- dig @8.8.8.8 www.quora.com <Enter>

135. This time, the command returns **sinkhole.paloaltonetworks.com** instead of an IP address for the domain.





This indicates that the firewall has intercepted and sinkholed the DNS query using the DNS Sinkholing function in your Anti-Spyware Profile.

136. In the firewall web interface, select **Monitor > Logs > Threat**.

137. The Threat Log should contain numerous entries for spyware and vulnerabilities:

	~	RECEIVE TIME	SEVERITY	ТҮРЕ	THREAT ID/NAME	TO ZONE	DESTINATION ADDRESS	ACTION
R		07/09 17:50:14	high	spyware	DGA:wodjfdhhe	Acquisition	192.168.56.17	drop- packet
R		07/09 17:50:14	medium	spyware	malicious- domains-edl	Internet	4.2.2.2	sinkhole
R		07/09 17:50:13	high	spyware	generic:paleorant	Acquisition	192.168.56.17	drop- packet
R		07/09 17:50:12	high	spyware	Trojan.yakes:afro	Acquisition	5.135.183.146	reset- both
R		07/09 17:50:10	high	spyware	Trojan.yakes:afro	Acquisition	31.3.135.232	reset- both
R		07/09 17:50:10	high	spyware	Trojan.yakes:afro	Acquisition	58.251.121.110	reset- both
R		07/09 17:50:10	high	spyware	Trojan.yakes:afro	Acquisition	188.165.200.156	reset- both
R		07/09 17:50:06	high	spyware	Trojan.yakes:afro	Acquisition	5.135.183.146	reset- both

These entries indicate that the firewall has blocked malicious traffic using the Vulnerability and Anti-Spyware Profiles that you defined. Note that the entries you see in the Threat Log may

differ from the example shown here. Also, several Threat Log columns have been hidden in this example.



The table may not contain very many entries until the malwareattacks script is finished. Use the refresh button periodically to update the table.

Lab Clean-Up

- 138. On the workstation desktop, locate the Remmina SSH connection to the Extranet server.
- 139. Type **exit <Enter>** to close the session.
- 140. Close the Remmina desktop application window.
- 141. Locate the open Terminal Emulator window on the workstation desktop.
- 142. Type **exit <Enter>** to close the window.



Stop. This is the end of the lab.
Lab 10: Blocking Inappropriate Web Traffic with Advanced URL Filtering

You can block access to malicious or inappropriate websites in two ways.

- Create Security Policy rules with a Deny Action and use URL categories as part of the rule criteria
- Create a URL Filtering Profile that includes blocked categories and apply the Profile to a Security Policy rule that allows the web-browsing and ssl applications.

In this lab, you will use both methods so that you can see the differences in how they are configured and in the kind of detail available through the logs when you use one method compared to the other.

Lab Objectives

- Test access to inappropriate web content without URL blocking in place
- Create a Security Policy rule to block inappropriate web content using the URL Category
- Test the Security Policy rule and examine the results
- Disable the Security Policy rule
- Create and apply a URL Filtering Profile to block access to a malicious URL
- Test the Security Profile and examine the results

High-Level Lab Steps

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-10.xml** - to the Firewall

Test Access to Inappropriate Web Content

- Run the Clear Logs Firewall-A script from the /home/lab-user/Desktop/
- Use testing browser to browse to **hacker9.com** and **hidester.com** and verify that both sites are available

Create a Security Policy Rule to Block Categories

• Use the information in the tables below to create a Security Policy rule to block traffic to certain URL Categories:

Rule Name	Block-Bad-URLs
Description	Blocks bad URLs based on categories

Source Zone	Users_Net			
Destination Zone	Internet			
Application	Any			
Service	application-default			
URL Category	Add the following:			
	adult			
	command-and-control			
	extremism			
	hacking			
	high-risk			
	malware			
	nudity			
	parked			
	peer-to-peer			
	phishing			
	proxy-avoidance-and-anonymizers			
	questionable			
Action	Deny			

• Move the **Block-Bad-URLs** rule to the top of the Security Policy.

Commit the configuration

• Commit the changes before proceeding.

Test Access to URLs Blocked by the Security Policy

- Use testing browser and attempt to connect to hacker9.com and hidester.com
- Note the message displayed by browser
- Examine the **Traffic** log and use a filter to locate entries that have been blocked by the **Block-Bad-URLs**
- Examine the **URL Filtering** log and use a filter to locate entries that have been blocked by the firewall

Block Access to Inappropriate Web Content Using Security Profile

• Create a URL Filtering Profile using the information in the table below:

Name	Corp-URL-Profile
Description	Standard corporate URL profile for all
	security policy rules
Site Access All Categories (except those below)	Alert
Site Access Block	adult
	command-and-control
	copyright-infringement
	extremism
	hacking
	high-risk
	malware
	nudity
	parked
	peer-to-peer
	phishing
	proxy-avoidance-and-anonymizers
	questionable
	unknown

Add the URL Profile to the Corp-Profiles-Group

• Edit the **Corp-Security-Group** and add the URL Filtering Profile **Corp-URL-Profile**.

Disable Block-Bad-URLs Rule

• Disable the **Block-Bad-URLs** in the Security Policy so that it does not interfere with your URL Filtering Profile testing.

Commit the configuration

• Commit the changes before proceeding.

Test Access to URLs Blocked by a URL Filtering Profile

- Use testing browser and browse to hidester.com and hacker9.com
- Note the difference between this error page and the one you received when using a Security Policy rule to block categories

- Examine the **Traffic** log and use a filter to display entries that fall in the URL Category of **hacking**
- Examine the **URL Filtering** Log and use a filter to display entries that fall in the URL Category of **hacking**

Create a Custom URL Category

• Use the information in the table below to create a **Custom URL Category**:

Parameter	Value
Name	Block-Per-Company-Policy
Description	URLs that are blocked by company policy.
Sites	Add the following:
	*.nbcnews.com
	*.theguardian.com

Use Custom Category to Block URL Access in Security Policy Rule

- Enable the Security Policy Rule Block-Bad-URLs
- Add the **Block-Per-Company-Policy** custom URL category to the rule

Commit the configuration

• Commit the changes before proceeding.

Test Access to Custom URLs Blocked by the Security Policy

- Use the testing browser and connect to www.nbcnews.com and www.theguardian.com
- Note the **Application Blocked** page message presented by the firewall
- Examine the URL Filtering log and use it to locate entries with an Action of block-url

Add Custom URL Category to URL Filtering Profile

- Edit the Corp-URL-Profile and set the Site Access for Block-Per-Company-Policy to block.
- Disable the Security Policy rule **Block-Bad-URLs** so that it does not interfere with the URL Filtering Profile.

Commit the configuration

• Commit the changes before proceeding.

Test Access to Custom URLs Blocked by the URL Filtering Profile

- Use testing browser and browse to www.nbcnews.com and www.theguardian.com
- Note the Block page presented by the firewall

Create an EDL to Block Malicious URL Access

Use the information in the table below to create an **External Dynamic Lists**:

Parameter	Value	
Name	malicious-urls-edl	
Туре	URL List	
Description	List of malicious URLs maintained on Extranet server	
Source	http://192.168.50.80/malicious-urls.txt	
	(The EDL contains only the URL duckduckgo.com)	
Check for updates	Every Five Minutes	

Block Access to the the URL List with a Security Policy Rule

- Add the **malicious-urls-edl** to the URL Category of the **Block-Bad-URLs** Security Policy rule.
- Enable the **Block-Bad-URLs** Security Policy rule

Commit the configuration

• Commit the changes before proceeding.

Test Access to URLs Blocked by the EDL in the Security Policy

- Use testing browser and browse to http://duckduckgo.com.
- Note the Application Blocked that the firewall displays
- Examine the **URL Filtering** log
- Use a filter that will display entries that have an action of block-url
- Disable the Security Policy rule **Block-Bad-URLs**

Commit the configuration

• Commit the changes before proceeding.

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-10.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

4. Click OK.

- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.

Test Access to Inappropriate Web Content

You can block access to inappropriate or malicious URLs by creating rules in the Security Policy. In this section, you will create a rule that blocks access to several URL categories.

Before you create the rule, you will clear the log file entries on the firewall (to make it easier to see new entries generated during this lab). You will also test access to two websites to verify that they are not being blocked.

Throughout this lab, use the Chromium browser to test access to various websites.

Different browsers react in different ways, and Chromium provides consistent and predictable responses to the firewall's blocking messages. Other browsers may display messages about reset connections or page not available. These responses do indicate that the firewall is blocking inappropriate web requests, but Chromium will usually display the response pages correctly.

If you do not see the appropriate block page in Chromium, clear the browser cache (Settings > Privacy & Security > Clear browsing data > Clear data). Close and reopen Chromium and try the test again.

You can also use CTRL + Shift + Delete to invoke the Clear browsing data window.



10. Clear the firewall log files by double-clicking on the Desktop icon for **Clear Logs Firewall-A**:



- 11. On the client desktop, open Chromium and browse to http://www.hacker9.com, which belongs to the URL category *hacking*.
- 12. In Chromium, browse to **http://kproxy.com**, which belongs to the URL category *proxy-avoidance-and-anonymizers*.

The browser should display a valid webpage.

13. Close the Chromium browser.

Create a Security Policy Rule to Block Categories

- 14. In the web interface, select **Policies > Security**.
- 15. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **Down arrow**) and select **Columns > URL Category**.

The **URL Category** column should appear in the web interface.



- 16. Click Add to create a new Security Policy rule.
- 17. On the General tab, type Block-Bad-URLs as the Name.
- 18. For **Description**, enter **Blocks bad URLs based on categories**.
- 19. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	Users_Net
Source Address	Any

20. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Internet
Destination Address	Any

- 21. Click the **Application** tab and verify that **Any** is selected.
- 22. Click the Service/URL Category tab and configure the following:

Parameter	Value	
Service	application-default	
URL Category	Add the following:	
	adult	
	command-and-control	
	extremism	
	hacking	
	high-risk	
	malware	
	nudity	
	parked	
	peer-to-peer	
	phishing	
	proxy-avoidance-and-anonymizers	
	questionable	



Note: you can type in the first few letters of a category to locate each one more quickly.



The categories you add to the Security Policy rule in this exercise are only some of the ones that you may need to add in a production environment. For more information on recommended categories to block, search the Live Community for "URL Filtering Category Recommendations."

23. Click the **Actions** tab and configure the following:

Parameter	Value
Action	Deny
Log Setting	Log at Session End

24. Click **OK** to close the Security Policy Rule window.

The new **Block-Bad-URLs** rule should be added to the Security Policy.

25. Select, but do not open, the Block-Bad-URLs rule in the Security Policy.

The rule should be highlighted after it has been selected.

			So	ource	Destination			
	NAME	ACTION	ZONE	ADDRESS	ZONE	APPLICATION	URL CATEGORY	PROFILE
6	Extranet_to_Internet	⊘ Allow	🚧 Extranet	any	Mainternet	any	any	₽
7	Extranet_to_User_Net	⊘ Allow	🚧 Extranet	any	🚧 Users_Net	📰 ssl	any	₽
8	Acquisition-Allow-All	⊘ Allow	Acquisition	any	any	any	any	Ŀ⊗i
9	Block-Bad-URLs	O Deny	Vsers_Net	any	Market Internet	any	adult command-and-control extremism hacking high-risk malware nudity more	none
10	intrazone-default 🚓	Allow	any	any	(intrazone)	any	any	none

26. Select **Move > Move Top** to move the **Block-Bad-URLs** rule to the top of the Security Policy:



•

Commit the configuration

- 27. Click the **Commit** button at the upper right of the web interface.
- 28. Leave the settings unchanged and click **Commit**.
- 29. Wait until the **Commit** process is complete.

30. Click Close.

Test Access to URLs Blocked by the Security Policy

In this section, you will test access to URLs that belong to URL categories prohibited by the Security Policy.

- 31. On the client desktop, open Chromium (or open a new tab if you are using Chromium as the configuration browser).
- 32. Connect to http://www.hacker9.com, which belongs to the URL category hacking. The browser should display an error message similar to the following example because the URL category hacking is blocked in the Security Policy.





Although this page says the Application web-browsing has been blocked, the firewall is actually blocking the site based on its category – hacking. The firewall uses this page to inform users that the firewall has blocked a web page deliberately. You will see a different message when the firewall blocks a page using a URL Filtering Profile.

33. In Chromium, open a new tab and connect to http://www.kproxy.com, which belongs to the URL category *proxy-avoidance-and-anonymizers*.

The browser should display the same kind of block page.

- 34. Close the Chromium browser.
- 35. In the firewall web interface, navigate to Monitor > Logs > Traffic.
- 36. Add the **URL Category** column to the display by clicking the small arrow next to the **Application** column heading and choosing **URL Category**:



37. Create and apply a filter to locate entries that have been blocked by the **Block-Bad-URLs** rule:

```
( rule eq 'Block-Bad-URLs' )
```

- 38. Note the entries you see in the Traffic Log that have been blocked by the Block-Bad-URLs Security Policy rule.
- 39. Clear the filter entry from the Traffic Log.
- 40. Navigate to **Monitor > Logs > URL Filtering**.
- 41. Create and apply a filter to locate entries that have been blocked by the firewall:

(action eq block-url)

- 42. You should see multiple entries for web-browsing sessions that have been blocked.
- 43. Note that the URL Filtering table contains the actual URL that was blocked as well as the category of the site.

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	SOURCE	APPLICATION	ACTION
Q	10/24 13:49:16	hacking	hacking,low-risk	www.hacker9.com/favicon.ico	192.168.1.20	web-browsing	block-url
Q	10/24 13:49:16	hacking	hacking,low-risk	www.hacker9.com/login/css/la	192.168.1.20	web-browsing	block-url
Q	10/24 13:49:16	hacking	hacking,low-risk	www.hacker9.com/	192.168.1.20	web-browsing	block-url
Q	10/24 13:46:51	proxy-avoidance- and-anonymizers	proxy-avoidance- and- anonymizers,low- risk	www.kproxy.com/favicon.ico	192.168.1.20	web-browsing	block-url
	10/24 13:46:51	proxy-avoidance- and-anonymizers	proxy-avoidance- and- anonymizers,low- risk	www.kproxy.com/login/css/lat	192.168.1.20	web-browsing	block-url



The Traffic log does not list the specific URL that a user attempted to visit; however, the URL filtering log does. Note that the default columns for the URL Filtering log table have been rearranged in this example.

44. Clear the filter from the URL Filtering Log.

Block Access to Inappropriate Web Content Using A Security Profile

You can use a Security Policy rule to control access to web site categories or you can use a URL Filtering Profile to accomplish the same task. One significant difference between the two is that you can configure a URL Filtering Profile to log access to all websites and categories; not just to websites that have been blocked by a Security Policy rule.

In this section, you will create a URL Filtering Profile that blocks certain categories of web content.

- 45. In the firewall web interface, select **Objects > Security Profiles > URL Filtering**.
- 46. Click Add to create a new Profile.A URL Filtering Profile window should open.
- 47. Type **Corp-URL-Profile** as the **Name** of the Profile.
- 48. For **Description**, enter **Standard corporate URL profile for all security policy rules**.
- 49. In the **Site Access** column, click the small triangle.
- 50. Choose **Set All Actions > alert**.



Õ

This shortcut allows you to change the setting for all categories in the list rather than changing each one entry at a time. Setting the action to alert instructs the firewall to allow access to the category and to write an entry to the URL Filtering log. When the action is set to allow, the firewall allows access but does not write an entry to the URL Filtering log.

Parameter	Value
Site Access	Configure the block action for the following URL categories:
	adult
	command-and-control
	copyright-infringement
	extremism
	hacking
	high-risk
	malware
	nudity
	parked
	peer-to-peer
	phishing
	proxy-avoidance-and-anonymizers
	questionable
	ransomware
	unknown

51. Under the **Categories** tab, configure the following:

The categories you are blocking here are only some of the ones that you should consider blocking in production environments. The choices you make about the types of categories to block in production may often be influenced by company policies and other factors. Also, Palo Alto Networks continuously updates the categories used in URL filtering, so you should re-evaluate the list of allowed and blocked URLs frequently to make certain the firewall carries out the appropriate actions for your environment.

For more information on recommended categories to block, search the Live Community for "URL Filtering Category Recommendations."

52. Click **OK** to close the **URL Filtering Profile** window.

Add the URL Profile to the Corp-Profiles-Group

In this section, you will add the URL Filtering Profile **Corp-URL-Filtering** to the existing Security Profile Group you created in an earlier lab.

- 53. In the firewall web interface, select **Objects > Security Profile Groups**.
- 54. Click the entry for **Corp-Profiles-Group** to edit it.
- 55. Use the drop-down list for **URL Filtering Profile** to select **Corp-URL-Profile**.

Security Profile Group		?
Name	Corp-Profiles-Group	
Antivirus Profile	Corp-Av	\sim
Anti-Spyware Profile	Corp-AS	\sim
Vulnerability Protection Profile	Corp-Vuln	\sim
URL Filtering Profile	Corp-URL-Profile	~
File Blocking Profile	Corp-FileBlock	\sim
Data Filtering Profile	Corp-DataFilter	\sim
WildFire Analysis Profile	None	\sim
	OK Cance	2

Ĝ

Because you have already applied this Security Profile group to the rules in your Security Policy, you will not need to modify any of the rules themselves. Each rule will now also include this Corp-URL-Profile as part of the inspection process.

56. Leave the remaining settings unchanged and click **OK**.

Disable Block-Bad-URLs Rule

In this section, you will disable the rule that blocks URLs based on categories so that it does not interfere with the URL Filtering Profile.

- 57. In the firewall web interface, navigate to **Policies > Security**.
- 58. Highlight the entry for **Block-Bad-URLs** but do not open it.
- 59. At the bottom of the window, click the **Disable** button.

			So	ource	Destination	
	NAME	ACTION	ZONE	ADDRESS	ZONE	APPLICATI
1	Block-Bad-URLs	O Deny	थ Users_Net	any	Market Internet	any
2	Block-from-Known-Bad-Addr	O Deny	Mainternet	Palo Alto N Palo Alto N Palo Alto N	Y Extranet	any
3	Block-to-Known-Bad-Address	O Deny	ExtranetUsers_Net	any	Market Internet	any
< (+)	Add 😑 Delete 💿 Clone 《	Override	💿 Revert 🥑	Enable 🚫 Disa	ble Move 🗸 🛛 🕼	PDF/CSV

Note that several columns have been hidden or rearranged in the example shown here.

60. The entry will change to *italics* to indicate that the rule is now **Disabled**.

			Sc	ource	Destination		
	NAME 🗸	ACTION	ZONE	ADDRESS	ZONE	APPLICATION	URL CA
1	Block-Bad-URLs	🚫 Deny	🚧 Users_Net	any	🚧 Internet	any	adult comman

Note that several columns have been hidden or rearranged in the example shown here.

Commit the configuration

- 61. Click the **Commit** button at the upper right of the web interface.
- 62. Leave the settings unchanged and click **Commit**.
- 63. Wait until the **Commit** process is complete.
- 64. Click Close.

Test Access to URLs Blocked by a URL Filtering Profile

In this section, you will perform tests to ensure that access to malicious URLs is blocked by the firewall using the URL Filtering Profile.

65. Open Chromium and browse to http://www.kproxy.com.

66. You should get a block page because you do not have access to this website. It belongs to the URL category *proxy-avoidance-and-anonymizers*, which is blocked by the URL Filtering Profile.





Notice that the information provided in this page provides more details than what the firewall displayed when it blocked the same website using the Block-Bad-URLs Security Policy rule.

This block page includes the actual URL and the Category that the site belongs to.

67. In the same tab, browse to http://www.hacker9.com.



- 68. Close the Chromium browser.
- 69. Select Monitor > Logs > Traffic.
- 70. Clear any filters you have in place.

- 71. Create and apply a filter that will display entries that fall in the URL Category of hacking:
- (category eq hacking)

(category eq hacking)								
RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	URL CATEGORY	ACTION	RULE
03/10 20:39:00	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	hacking	allow	Users_to_Internet
03/10 20:39:00	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	hacking	allow	Users_to_Internet
03/10 20:39:00	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	hacking	allow	Users_to_Internet
03/10 20:28:34	Users_Net	Internet	192.168.1.20	159.89.148.144	web-browsing	hacking	allow	Users_to_Internet



Notice that the Security Policy rule listed is **Users_to_Internet** and that the **Action** for each entry is **allow**.

The Security Policy rule is not blocking the URL category of hacking. The blocking process happens as part of the URL Filtering Profile inspection.

- 72. Clear the filter from the Traffic Log.
- 73. Examine the URL Filtering Log under **Monitor > Logs > URL Filtering**.
- 74. Clear any filters you have in place.
- 75. Create and apply a filter to show entries in which the URL Category is hacking:

```
( category eq hacking )
```

 \mathbb{Q} (category eq hacking)

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	SOURCE	APPLICATION	ACTION
Q	03/10 20:38:45	hacking	hacking,low-risk	hacker9.com/favicon.ico	192.168.1.20	web-browsing	block-url
R	03/10 20:38:45	hacking	hacking,low-risk	hacker9.com/login/css/latofonts	192.168.1.20	web-browsing	block-url
R	03/10 20:38:45	hacking	hacking,low-risk	hacker9.com/	192.168.1.20	web-browsing	block-url

Note that several columns have been hidden or rearranged in the example shown here.

- 76. Note that the action for these sessions is **block-url**, which is carried out by the URL Filtering Profile.
- 77. Clear the filter in the URL Filtering log.

Create a Custom URL Category

In some situations, you may want to block only a few websites in a particular category, but you do not want to block the entire category itself. You can accomplish this by creating a Custom URL Category. Adding individual URLs to the Custom URL Category allows you to then block the Custom URL Category within a Security Policy rule or within a URL Filtering Profile. In this section, you will test access to a URL and then create a Custom URL Category that includes that URL along with a few others.

- 78. Open Chromium (or a new tab) and connect to www.nbcnews.com. The browser should display a valid webpage.
- 79. Close the Chromium tab for nbcnew.com.
- 80. In the firewall web interface, select **Objects > Custom Objects > URL Category**.
- 81. Click Add.
- 82. Click **Cancel** on the message about **Append trailing slash to entries**.
- 83. Configure the following for the Custom URL Category:

Parameter	Value
Name	Block-Per-Company-Policy
Description	URLs that are blocked by company policy.
Туре	URL List
Sites	Add the following:
	*.nbcnews.com/

Custom URL (Category	()
Name	Block-Per-Company-Policy	
Description	ULRs that are blocked by company policy	
Туре	URL List	× 1
Matches any of the fol	owing URLs, domains or host names	
Q		1 item \rightarrow \times
	_	
*.nbcnews.com	n/	
+ Add O Dele	ete 🛛 🛶 Import 📑 Export	
Enter one entry per m		
Each entry may be of t	*. he form www.example.com or it could have wildcards li	ke www.*.com.
T		Formalis and formalistic and
xyz.com. For more info	ry match, use a forward slash (/) at the end of your entry , see URL Category Exceptions	. Example: xyz.com/ matches only
		OK Cancel

84. Click **OK** to close the **Custom URL Category** window.

Use Custom Category to Block URL Access in Security Policy Rule

In this section, you will add your Custom URL Category to a Security Policy rule that has a "deny" action.

- 85. In the web interface, select **Policies > Security**.
- 86. Highlight the rule for **Block-Bad-URLs** but do not open it.
- 87. Click the **Enable** button at the bottom of the window.

✓ Enable

- 88. Click **Block-Bad-URLs** to edit the rule.
- 89. Click the Service/URL Category tab.
- 90. Under the URL Category, configure the following:

Parameter	Value
URL Category	Add the following to the list:
	Block-Per-Company-Policy

General Source Destination App	lication Service/URL Category Actions Us
application-default 🗸	Any
SERVICE A	URL CATEGORY A
· ·	nudity
	parked
	peer-to-peer
	phishing
	proxy-avoidance-and-anonymizers
	questionable
	Block-Per-Company-Policy

91. Click **OK** to close the **Security Policy Rule** window.

Commit the configuration

- 92. Click the **Commit** button at the upper right of the web interface.
- 93. Leave the settings unchanged and click **Commit**.

- 94. Wait until the **Commit** process is complete.
- 95. Click Close.

Test Access to Custom URLs Blocked by the Security Policy

Now you will test access to URLs that belong to the Custom URL Category that you added to a Security Policy deny rule.

- 96. On the client desktop, open Chromium and browse to http://www.nbcnews.com. The browser should display an Application Blocked page message because the Custom URL Category in the Security Policy blocks access to the webpage.
- 97. In the firewall web interface, navigate to **Monitor** > **Logs** > **URL Filtering**.
- 98. Create and the apply a filter to display blocked URLs:

(action eq block-url)

99. You should see multiple entries for sessions to www.nbcnews.com that the firewall has blocked:

Q ((action eq 'block-url')						
CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	ACTION
Block-Per- Company-Policy	Block-Per- Company- Policy,news,low- risk	www.nbcnews.com/favicon.ico	Users_Net	Internet	192.168.1.20	block-url
Block-Per- Company-Policy	Block-Per- Company- Policy,news,low- risk	www.nbcnews.com/login/css/l	Users_Net	Internet	192.168.1.20	block-url
Block-Per- Company-Policy	Block-Per- Company- Policy,news,low-	www.nbcnews.com/	Users_Net	Internet	192.168.1.20	block-url

Note that several default columns have been hidden in the example URL Filtering log file shown here.

100. Notice that the **Category** listed for each of the entries is the **Block-Per-Company-Policy**.

Add Custom URL Category to URL Filtering Profile

In this section, you will set the **Block-Per-Company-Policy** category to **block** in the **Corp-URL-Profile** URL Filtering Profile.

- 101. In the firewall web interface, navigate to **Objects > Security Profiles > URL Filtering**.
- 102. Edit the **Corp-URL-Profile** entry.
- 103. Under the **Custom URL Categories** section, set the **Site Access** for **Block-Per-Company-Policy** to **block**.

URL Filtering Profile			(?		
Name Corp-URL-Profile					
Description	Standard corporate URL profile for all security policy rules				
Categories URL Filtering Setting	s User Credential Detection HTTP Header Insertion In	ine Categorization			
			75 items \rightarrow \times		
CATEGORY	CATEGORY USER CREDENTIAL SITE ACCESS SUBMISSION				
Block-Per-Company-Policy* block					
abortion alert allow					
abused-drugs		alert	allow		
		1.1	1.11-		

104. Leave the remaining settings unchanged.

105. Click OK.

106. In the web interface, select **Policies > Security**.

107. Highlight the entry for **Block-Bad-URLs** but do not open it.

108. Click **Disable** at the bottom of the window.



Note that you are disabling this rule so that it does not interfere with the Users_to_Internet rule which allows traffic but applies the URL Filtering Profile.

Commit the configuration

109. Click the **Commit** button at the upper right of the web interface.

- 110. Leave the settings unchanged and click **Commit**.
- 111. Wait until the **Commit** process is complete.
- 112. Click Close.

Test Access to Custom URLs Blocked by the URL Filtering Profile

Now you will test access to URLs that belong to the Custom URL Category that you added to the URL Filtering Profile.

113. On the client desktop, open Chromium and browse to www.nbcnews.com.

114. The browser should display a **Web Page Blocked** message.



115. Close the Chromium browser.

Create an EDL to Block Malicious URL Access

You can add a list of malicious URLs to a file on an external web server, and then configure the firewall to access the list as an External Dynamic List (EDL). The advantage of this approach is that you can regularly update the malicious URL list without the need to recommit the firewall configuration each time, as you would have to do if you updated a Security Policy rule with a new URL.

116. In the firewall web interface, select **Objects > External Dynamic Lists**.

- 117.Click Add.
- 118. Click **Cancel** on the message about **Append trailing slash to entries**.
- 119. Configure the following:

Parameter	Value
Name	malicious-urls-edl
Туре	URL List
Description	List of malicious URLs maintained on Extranet server
Source	http://192.168.50.80/malicious-urls.txt (The EDL contains several URL for testing purposes - duckduckgo.com is one of them)
Check for updates	Every Five Minutes

External Dynami	mic Lists (?
Name	malicious-urls-edl	
Create List	si Entres And Exceptions	
Туре	URL List	~
Description	List of malicious URLs maintained on Extranet server	
Source	http://192.168.50.80/malicious-urls.txt	Ī
Server Authenticat	tion	
Certificate Profile	None]
Check for updates	Every five minutes	
Test Source URL	OK Cancel)

The malicious-urls.txt file contains entries for duckduckgo.com.

120. Click **OK** to close the **External Dynamic Lists** window.

121. Click malicious-urls-edl.

The External Dynamic Lists window should open again.

- 122. Click Cancel on the message about Append trailing slash to entries.
- 123. Click Test Source URL to verify that the firewall can access the EDL URL.
- 124. A message window should open and state that the source URL is accessible.

Test Source URL

Source URL is accessible.

C	Close)

125. Click **Close** to close the message window.

126. Click **OK** to close the **External Dynamic Lists** window.

Block Access to the URL List with a Security Policy Rule

Now you will add the EDL containing the malicious URL list to a Security Policy rule with a "deny" action.

127. In the web interface, select **Policies > Security**.

128. Click **Block-Bad-URLs** to edit the rule.

129. Click the Service/URL Category tab and configure the following:

Parameter	Value	
URL Category	Add malicious-urls-edl to the list.	
	This EDL will block access to duckduckgo.com.	

Security Policy Rule				
General Source Destination Application	Service/URL Category Actions Usage			
application-default \checkmark	Any			
SERVICE A	URL CATEGORY A			
	nudity			
	parked			
	peer-to-peer			
	phishing			
	proxy-avoidance-and-anonymizers			
	questionable			
	Malicious-urls-edl			
+ Add - Delete	(+) Add (-) Delete			

- 130. Click **OK** to close the **Security Policy Rule** window.
- 131. With the **Block-Bad-URLs** Security Policy rule highlighted, click **Enable** at the bottom of the window.

Commit the configuration

- 132. Click the **Commit** button at the upper right of the web interface.
- 133. Leave the settings unchanged and click **Commit**.
- 134. Wait until the **Commit** process is complete.
- 135. Click Close.

Test Access to URLs Blocked by the EDL in the Security Policy

In this section, you will test access to a URL that is contained in the EDL that you added to a Security Policy rule with a "deny" action.

136. Open Chromium and browse to http://duckduckgo.com.

The browser will display an Application Blocked page because the EDL in the Security Policy blocks access to the duckduckgo.com webpage. If you do not see the response page from the FireWall, then please ensure you are using http and not https. If the browser switches to https automatically then please access the link using incognito mode. To open Chromium in incognito mode, please right click the Chromium icon and select **Open a New Window in incognito mode**

- 137. Close Chromium.
- 138. In the firewall web interface, navigate to **Monitor > Logs > URL Filtering**.
- 139. Clear any filters you have in place.
- 140. Create and apply a filter that will display entries that have an action of block-url: (action eq block-url)
- 141. You should see multiple entries for sessions to duckduckgo.com that the firewall has blocked:

Q (action eq block-url)						
CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	ACTION
malicious-urls-edl	malicious-urls- edl,search- engines,low-risk	duckduckgo.com	Users_Net	Internet	192.168.1.20	block-url
malicious-urls-edl	malicious-urls- edl,search- engines,low-risk	duckduckgo.com	Users_Net	Internet	192.168.1.20	block-url
malicious-urls-edl	malicious-urls- edl,search- engines,low-risk	duckduckgo.com/	Users_Net	Internet	192.168.1.20	block-url

Note that several default columns have been hidden in the example URL Filtering log file shown here.

- 142. In the web interface, select **Policies > Security**.
- 143. Highlight the entry for Block-Bad-URLs but do not open it.
- 144. Click **Disable** at the bottom of the window.

Commit the configuration

- 145. Click the **Commit** button at the upper right of the web interface.
- 146. Leave the settings unchanged and click **Commit**.
- 147. Wait until the **Commit** process is complete.
- 148. Click Close.



Stop. This is the end of the lab.

Lab 11: Blocking Unknown Threats with WildFire

Your company has recently seen an increase in malicious files that users are downloading. You have sent out informational emails explaining how much damage these types of files can do, and you have told people not to download files from questionable sources.

Fortunately, you have deployed the Palo Alto Networks firewall, and you can set up a Security Profile that will send any unknown files to the WildFire cloud for analysis.

To test the Security Profile after you have configured it, you will download a test file provided by Palo Alto Networks. This test file is not actually malicious, but WildFire will identify it as such.

You will then examine a detailed report from WildFire with information about the file that was analyzed.



Lab Objectives

- Create a WildFire Analysis Profile
- Apply WildFire Profile to security rules
- Test the WildFire Analysis Profile
- Examine WildFire analysis details

High-Level Lab Steps

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-11.xml** - to the Firewall

Create a WildFire Analysis Profile

• Use the information in the tables below to create a WildFire Analysis Security Profile that you can attach to Security Policy rules to test files and URLs for malware.

Parameter	Value
Name	Corp-WF
Description	WildFire profile for Corp security rules.

• Click **Add** in the bottom left corner and configure the following:

Profile Details	Value
Name	All_Files
Applications	any
File Types	any
Direction	Both
Analysis	public-cloud

Modify Security Profile Group

- Add the **Corp-WF** Profile to the **Corp-Profiles-Group**.
- **Disable** all but the **Corp-WF** Security Profile.

Doing this ensures that the firewall will only use WildFire and no other Security Profiles such as Anti-Virus or Machine Learning for this lab.

Update WildFire Settings

• Enable the options for **Report Benign Files** and **Report Grayware Files** under the **General Settings** for Wildfire.

Set Monitor Log Interval

• Change the **Interval** setting from the default **20** minutes to **1** minute by issuing the following command:

debug wildfire monitor-log interval 1

Commit the configuration

• Commit the changes before proceeding.

Test the WildFire Analysis Profile

• Use the testing browser and connect to:

http://192.168.50.80/wildfire-test-pe-file.exe

- Save the file when prompted
- Use the **Remmina** application and connect to **Firewall-A**
- Use the command **debug wildfire upload-log show** to verify that the test file was uploaded

Examine WildFire Analysis Details

- Examine the **WildFire Submissions** log file and periodically use the **Refresh** until you see a new entry for the wildfire-test-pe-file.exe.
- Examine the **Detailed Log View** for the entry.
- Note the **Verdict** of the file.
- Click the link for **Download PDF** and examine the report to view detailed information about the Wildfire analysis of the file.

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-11.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

4. Click OK.

- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.

Create a WildFire Analysis Profile

In this section you will create a WildFire Analysis Security Profile that you can attach to Security Policy rules to test files and URLs for malware.

- 10. In the web interface, select **Objects > Security Profiles > WildFire Analysis**.
- 11. Click **Add** to create a new Profile.

A WildFire Analysis Profile window should open.

12. Configure the following:

Parameter	Value
Name	Corp-WF
Description	WildFire profile for Corp security rules.

13. Click **Add** in the bottom left corner and configure the following:

Parameter	Value
Name	All_Files
Applications	Verify that any is selected
File Types	Verify that any is selected
Direction	Verify that both is selected

Parameter	Value
Analysis	Verify that public-cloud is selected

WildFire Analy	ysis Profile				?
Name	Corp-WF				
Description	Description WildFire profile for Corp security rules.				
	Cloud Analysis			1 item	→ ×
NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS	
All_Files	any	any	both	public-cloud	

14. Click **OK** to close the window.

The new WildFire Analysis Profile now should be listed.

Modify Security Profile Group

- 15. Select **Objects > Security Profile Groups**.
- 16. Edit the entry for **Corp-Profiles-Group**.
- 17. Use the drop-down list for Wildfire Analysis Profile to select Corp-WF.
- 18. Set the other **Profiles** to **None**:

Security Profile Group	(?)
Name	Corp-Profiles-Group
Antivirus Profile	None
Anti-Spyware Profile	None
Vulnerability Protection Profile	None
URL Filtering Profile	None
File Blocking Profile	None
Data Filtering Profile	None
WildFire Analysis Profile	Corp-WF 🗸
	OK Cancel

Doing this ensures that the firewall will only use Wildfire and no other Security Profiles such as Anti-Virus or Inline Machine Learning.



In a production environment, you definitely want to apply all the Security Profiles for your Group. In this lab, we only want to test WildFire to see how it operates alone.

19. Click **OK**.

Update WildFire Settings

- 20. Select **Device > Setup > WildFire**.
- 21. Click the gear icon to edit the **General Settings**.
- 22. Check the boxes for **Report Benign Files** and **Report Grayware Files**.
- 23. Leave the remaining settings unchanged.

WildFire Public Cloud	wildfire.paloaltonetworks.com						
WildFire Private Cloud	Lice Draves Settings for Drivete Cloud						
File Size Limits							
	pe (MB)	16 (default)					
	apk (MB)	10 (default)					
	pdf (KB)	3072 (default)					
	ms-office (KB)	16384 (default)					
	jar (MB)	5 (default)					
	flash (MB)	5 (default)					
	MacOSX (MB)	10 (default)					
	archive (MB)	50 (default)					
	linux (MB)	50 (default)					
	script (KB)	20 (default)					

24. Click OK.

Set Monitor Log Interval

In this section, you will connect to the firewall through the CLI and modify a setting that determines how long the firewall waits before writing information to the WildFire upload log. The default value is 20 minutes. You will set this value to 1 minute only for this test (so you don't have to wait as long to see information in the log). When testing is complete, you will set the value back to the default 20 minutes.

- 25. Open the Remmina Remote Desktop Client.
- 26. Double-click the entry for **Firewall-A** to connect.
- 27. Issue the following command to see the current monitor log settings:

```
debug wildfire monitor-log settings <ENTER>
```

```
G Firewall-A ×
admin@firewall-a> debug wildfire monitor-log settings
Monitor log write to disk is enabled. Max file size is 25.000 MB. Interval is 20 minutes.
```

28. Change the **Interval** setting from the default **20** minutes to **1** minute by issuing the following command:

```
debug wildfire monitor-log interval 1 <ENTER>
```

```
Firewall-A ×
admin@firewall-a> debug wildfire monitor-log interval 1
Monitor log write to disk is enabled. Max file size is 25.000 MB. Interval is 1 minutes.
```



The monitor log interval determines how long the firewall waits to

29. Leave the Remmina connection to Firewall-A open because you will use it a bit later in this lab.

Commit the configuration

- 30. In the web interface, click the **Commit** button at the upper right of the web interface.
- 31. Leave the settings unchanged and click **Commit**.
- 32. Wait until the **Commit** process is complete.
- 33. Click Close.

Test the WildFire Analysis Profile

34. Open the testing browser and connect to:

http://192.168.50.80/wildfire-test-pe-file.exe

35. When the testing browser prompts you, select **Save**.

Cancel Name w	ildfire-test-pe-file.exe	Q Save
🔒 Home	A lab-user Downloads	D
Desktop	Name	▼ Size Type Modifi€
Documents		
🛃 Downloads		
🖻 thinclient_drives 📥		
Music		
Pictures		
Videos		
		DOS/Windows executable -

This site generates an attack file with a unique signature that simulates a zero-day attack.

- 36. Close the testing browser.
- 37. On the client desktop, select the **Remmina** connection to Firewall-A.

38. From the CLI, enter the command **debug wildfire upload-log show.**

The command should display the output **log: 0**, **filename: wildfire-test-pefile.exe processed...**. This output verifies that the file was uploaded to the WildFire public cloud. The message might take a minute or two to display.



Note that the details of the entry you see will differ from the example shown here.

If you do not see any entries in the wildfire upload log, clear the cache in the testing browser and repeat the file download steps.

39. Change the Monitor Log Interval back to the default setting by issuing the following command:

debug wildfire monitor-log interval 20 <ENTER>

- 40. Type **exit <Enter>** to close the SSH session to the firewall.
- 41. Close the Remmina application window.

Examine WildFire Analysis Details

42. In the firewall web interface, select **Monitor** > **Logs** > **WildFire Submissions**:

Analysis takes 5 to 15 minutes, and the table will remain empty until WildFire has reached a verdict about the file.

43. Periodically use the **Refresh** button in the upper right corner of the window until you see a new entry for the wildfire-test-pe-file.exe.

	RECEIVE TIME~	FILE NAME	SOURCE ZONE	DESTINA ZONE	SOURCE ADDRESS	APPLICATION	RULE	VERDICT	SEVERITY
R	09/12 15:48:44	wildfire-test-pe-file.exe	Users_Net	Extranet	192.168.1.20	web-browsing	Users_to_Extranet	malicious	high

Note that in this example several default columns have been hidden, and the details of the entry you see will differ.

44. Click the **magnifying glass** icon next to the entry to open the **Detailed Log View** of the entry.

Detailed Log View										? 🗆			
Log Info WildFire Analysis Report													
General				Source				Destination					
	Session ID Action Application Rule Rule UUID Verdict Device SN IP Protocol Log Action	16165 allow web-browsir Users_to_Ex f811ebab-44 a104-8ac890 malicious 0070510000 tcp	ng tranet 33c-48c6- 621e837 055975	Source User Source 192.168.1.20 Source DAG Port 53944 Zone Users_Net Interface ethernet1/2 Details				Destination User Destination 192.168.50.80 Destination DAG Port 80 Zone Extranet Interface ethernet1/3					
PCAP		TYPE	APPLICAT	ACTION	RULE	RULE	BY	SEVERI	CATEG	URL CATEG LIST	VERDI	URL	FILE NAME
	2022/09/12 15:48:44	wildfire	web- browsing	allow	Users	f811eb		high			malicio		wildfir
	2022/09/12 15:48:44	wildfire	web- browsing	allow	Users	f811eb		high			malicio		wildfir
	2022/09/12 15:46:39	end	web- browsing	allow	Users	f811eb	61		any				
	Close												

45. Under the General section, note the **Verdict**:

Note that the details of the entry you see will differ from this example.

46. Click the tab labeled Wildfire Analysis Report at the top of the Detailed Log View.47. Click the link for Download PDF.
| Detailed Log View | | ? | | | | |
|-------------------------|--|----------------------------------|--|--|--|--|
| Log Info WildFire Ana | alysis Report | | | | | |
| WildFire Analysis | Summary | Download PDF | | | | |
| File Information | e e e e e e e e e e e e e e e e e e e | | | | | |
| File Type | PE | | | | | |
| File Signer | | | | | | |
| SHA-256 | 8735487f06936a8fbc87019385be711500e91e73d423b3847f864e9bdc51bf99 | | | | | |
| SHA1 | 5598f46590713156145ff44c714e91c5a606d51e | | | | | |
| MD5 | 65ebc74c8ae85397f1844bb6240dec83 | 65ebc74c8ae85397f1844bb6240dec83 | | | | |
| File Size | 55296 bytes | | | | | |
| First Seen Timestamp | 2020-11-06 16:43:37 UTC | | | | | |
| Verdict | malware | | | | | |
| RECEIVE TIME | RULE | FILE | | | | |

48. This action will open a PDF version of the Wildfire Analysis Report in another tab of the configuration browser.

WildFire Analysis Report

WildFire Analysis Report	1
1 File Information	2
2 Static Analysis	2
2.1. Suspicious File Properties	2
3 Dynamic Analysis	2
3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)	3
3.1.1. Behavioral Summary	3
3.1.2. Network Activity	3
3.1.3. Host Activity	3
Process Activity	3
Process Name - sample.exe	3
Event Timeline	3
3.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)	3
3.2.1. Behavioral Summary	3
3.2.2. Network Activity	4
3.2.3. Host Activity	4
Process Activity	4
Process Name - sample.exe	4
Event Timeline	4

Note that the information you see in your report may vary from the example shown here.

49. Scroll through the report to view detailed information about the Wildfire analysis of the file.

3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Sample removed system files. Sample removed system files.	000000000
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	1000000000
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	010000000

For example, section 3.1 provides details about the kind of environment that WildFire used to test the file along with specific actions that the malware file carried out. Note that the information you see in your report may vary from the example shown here.

- 50. Close the configuration browser tab that contains the PDF version of the WildFire Analysis Report.
- 51. Click **Close** to close the **Detailed Log View** window.



Stop. This is the end of the lab.

Lab 12: Controlling Access to Network Resources with User-ID

Your organization recently acquired another company, and you have been tasked to create appropriate security Policy rules for traffic generated by these new users.

Your firewall has been configured with a virtual wire that allows traffic to the Internet from the users in the newly acquired company. The firewall also has a new security zone in place called Acquisition that contains all new users.

The firewall has an existing Security Policy rule that allows all users in the Acquisition zone to access any application on the internet. Your task is to restrict users in this new organization to approved corporate applications only.



The approved corporate applications include DNS, web-browsing, and SSL.

You also need to ensure that only users in the marketing group are allowed to use social media applications such as Facebook, Instagram, and others.

Another firewall administrator has created the appropriate Application Groups for you.

The firewall receives User-ID and Group membership information about users in this new company from an XML upload sent by network authentication devices. (Note that this is simulated in this lab and outside the scope of this course).



You also need to create a Security Policy rule that explicitly denies any other traffic generated by users in the Acquisition zone. Although the interzone-default rule will deny any traffic not expressly allowed, creating an explicit deny rule will allow you to examine the kinds of applications users in the Acquisition zone are attempting to access.

Lab Objecti

- Examine current configuration
- Enable User-ID technology on the Acquisition zone.
- Generate traffic
- Modify Security Policy to meet requirements

High-Level Lab Steps

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-12.xml** - to the Firewall

Examine Firewall configuration

• Review the settings that another administrator has configured for Application Groups and Security Policy rules, and verify the following settings on the Acquisition-Allow-All Security Policy rule

Parameter	Value
Source Zone	Acquisition
Source Address	Any
Destination Zone	any
Destination IP	Any
Application	Any
Action	Allow

- Clear the counters for all Security Policy rules
- Use the information below to verify that the configuration contains two new **Application Groups**

Name	Applications
Allowed-Corp-Apps	dns
	web-browsing
	ssl
Allowed-Mktg-Apps	facebook-base
	instagram-base
	twitter-base
	myspace-base
	linkedin-base

Generate Traffic from the Acquisition Zone

- Use **Remmina** to connect to the **Server-Extranet** host
- Change to the appropriate directory

cd /home/paloalto42/pcaps92019/app.pcaps <Enter>

• Run the following command to start generating traffic in the Acquisition Zone:

./Appgenerator-2.sh <Enter>

- While the script is running, examine the firewall Traffic log under **Monitor** > **Logs** > **Traffic**.
- Note that almost all traffic is hitting the Acquisition-Allow-All Rule.
- Add the **Source User** column to the Traffic Log

Enable User-ID on the Acquisition Zone

• Edit the Acquisition Security zone and check the box for Enable User Identification

Modify the Acquisition-Allow-All Security Policy Rule

- Change the name of the Security Policy rule **Acquisition-Allow-All** to **Allow-Corp-Apps**
- Change the Description field to Allows only approved apps for Acquisition users.
- Set the Applications to use only the **Allowed-Corp-Apps** Application Group

Create Marketing Apps Rule

• Use the information below to create a Security Policy rule to allow only Marketing users to access the Allowed-Mktg-Applications

Parameter	Value
Name	Allow-Mktg-Apps
Description	Allows only users of marketing group to access Mktg apps
Source Zone	Acquisition
Source User	marketing
Destination Zone	any
Application	Allowed-Mktg-Apps
Dependent Applications	Add to Current Rule
Action	Allow

Create Deny Rule

• Use the information below to create a new Security Policy rule that will deny any other application traffic for users in the Acquisition zone.

Parameter	Value
Name	Deny-All-Others
Description	Denies non-approved applications for users in Acquisition zone
Source Zone	Acquisition
Source User	Any
Destination Zone	any

Parameter	Value
Application	Any
Action	Deny

• Place the **Deny-All-Others** rule at the bottom of the Security Policy.

Commit the configuration

• Commit the changes before proceeding

Generate Traffic from the Acquisition Zone

- Use the Extranet-Server connection in the Remmina application to run the **Appgenerator-2.sh** script again
- While the script is running, move to the next section in which you will examine the firewall logs

Examine User-ID Logs

- Use the firewall CLI and the web interface to examine information about User-ID
- The firewall should have numerous entries with username-to-ip-address mappings in the User-ID log
- Use the Remmina application to connect to the CLI of Firewall-A
- Use the following command to display entries for User-ID:

show user ip-user-mapping all <Enter>

• Close the firewall SSH connection.

Examine Firewall Traffic Log

Examine Firewall Traffic Log

1. Create and apply filters in the Traffic log to answer the questions in this section.

Which rule does the firewall use when it encounters youtube-base traffic?

Which rule does the firewall use when it encounters dns traffic?

Which rule does the firewall use when it encounters facebook-base?

Which users are allowed access to facebook-base?

Is the user sholmes allowed to access instagram-base?

Is the user bbart allowed to access instagram-base?

Clean Up the Desktop

- In the Traffic log window on the firewall, clear any filters you have in place
- In the Remmina application window, close the SSH connections to the firewall and the Server-Extranet
- Close the main Remmina application window

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-12.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

- 4. Click **OK**.
- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.

9. Click **Close** to continue.

Examine Firewall Configuration

In this section, you will review the settings that another administrator has configured for Application Groups and Security Policy rules.

- 10. Select **Policies > Security**.
- 11. Edit the entry for Acquisition-Allow-All.
- 12. Select the **Source** tab.

Any	Any	any
SOURCE ZONE		

- 13. Note that the **Source Zone** is set to **Acquisition**.
- 14. Select the **Destination** tab.
- 15. Note that the **Destination Zone** is set to **any**.

	Security Policy Rule			
	General Source Destination A	Application Service/U	URL (Category Actions Usage
-				
	any 🗸		<u> </u>	Any
Τ	DESTINATION ZONE			DESTINATION ADDRESS

16. Select the **Application** tab.

Security Policy Rule
General Source Destination Application Service/URL Category A
APPLICATIONS A

- 17. Note that the **Application** is set to **Any**.
- 18. Select the **Actions** tab.

Security Polic	y Rule						
General Sou	rce D	Destinatior	Application	Service/URL Categor	Actions	Usage	2
Action Setting -			_				Log S
	Action	Allow				\sim	
		Send I	CMP Unreachable				
							Lo

- 19. Note that the Action is set to Allow.
- 20. Click **OK** to close the **Security Policy Rule** window.

			Source	Destination	
	NAME	ACTION	ZONE	ZONE	APPLICATION
9	Acquisition-Allow-All	⊘ Allow	Acquisition	any	any

This Security Policy rule allows any host in the Acquisition security zone to access any application anywhere.

21. Clear the counters for all Security Policy rules by clicking **Reset Rule Hit Counter** > **All rules** at the bottom of the window.



This action will allow you to see how many times the rules are accessed from this point forward.

- 22. Click **Yes** in the **Reset** window.
- 23. Select **Objects > Application Groups**.
- 24. Note the two new **Application Groups**:

	NAME	LOCATION	MEMBERS	APPLICATIONS
	paloalto-apps		5	paloalto-dns-security
				paloalto-updates
				paloalto-userid-agent
				paloalto-wildfire-cloud
				pan-dh-cloud
	Allowed-Corp-Apps		3	dns
All Users				web-browsing
				ssl
	Allowed-Mktg-Apps		5	facebook-base
				instagram-base
Aarketing Only				twitter-base
				myspace-base
				linkedin-base

You will configure the firewall to allow all users in the Acquisition zone to use the Allowed-Corp-Apps. However, only users in the Marketing group will be able to use applications in the Allowed-Mktg-Apps group.

Generate Traffic from the Acquisition Zone

- 25. On the client workstation, open Remmina.
- 26. Open the connection to the **Server-Extranet**.
- 27. Enter the following command to change directories:

cd /home/paloalto42/pcaps92019/app.pcaps <Enter>

28. Run the following command to start generating traffic in the Acquisition Zone:

./Appgenerator-2.sh <Enter>

- 29. While the script is running, examine the firewall Traffic log under **Monitor** > **Logs** > **Traffic**.
- 30. Clear any filters you may have in place.
- 31. Note that almost all traffic is hitting the Acquisition-Allow-All Rule.
- 32. If the **Source User** column is not already displayed, add it to the table by clicking the small triangle in any header and choosing **Columns** > **Source User**.

	`		Source
rion~	TO PORT	APPLIC	Source User
221 8			Source Dynamic Address Group
2.2		>	Destination
0.5	Adjust Col	umns	Destination Dynamic Address Group
.174	443	youtube	Dynamic User Group
			To Port
0.53	53	dns	Application
	52	doc	Action

33. Drag and drop the Source User column between the Source and Destination columns

	-	*		
	SOURCE	DESTINATION	SOURCE USER	то і
n	192.168.1.24		ISER	443
n	192.168.1.20	192.168.50.53		53
n	192.168.1.20	172.217.9.174		443
	400440400	4004405050		100

This action will make it easier for you to locate Source User information later in this lab. Note that the Source User column will be empty because you have not yet enabled User-ID.

Enable User-ID on the Acquisition Zone

In this section you will enable User-ID on the Acquisition Security zone as part of the process of enabling User-ID on a firewall.

- 34. In the web interface, select **Network > Zones**.
- 35. Click **Acquisition** to open the zone.

The **Zone** configuration window should open.

36. Select the **Enable User Identification** check box:

Zone			
Name	Acquisition		User Identification ACL
Log Setting	None	~	Enable User Identification
Туре	Virtual Wire	~	
			Select an address or address gro in your own address. Ex: 192.168
ethernet1/4			192.168.1.0/24
ethernet1/5			

37. Click **OK** to close the **Zone** configuration window.

Modify the Acquisition-Allow-All Security Policy Rule

You will now change the set of applications that Acquisition users are allowed to access by modifying the existing **Acquisition-Allow-All** rule.

- 38. Select **Policies > Security**.
- 39. Edit the entry for Acquisition-Allow-All.
- 40. Under the General tab, change the Name of this rule to Allow-Corp-Apps.
- 41. For **Description**, change the entry to **Allows only approved apps for Acquisition users**.

Security Policy Rule				
General	Source Destination Application Service/URL Categ	jory		
	Name Allow-Corp-Apps			
Ru	Type universal (default)			
Dese	ption Allows only approved apps for Acquisition users.			

- 42. Select the **Application** tab.
- 43. **Uncheck** the option for **Any**.
- 44. Click **Add** and enter the first few letters of the **Allowed-Corp-Apps** to display the Application Groups available:
- 45. Select Allowed-Corp-Apps.

Sec	curity Policy Rule
Ge	neral Source Destination Application Service/U
	Any
	APPLICATIONS A
	Allowe
	Application Group Allowed-Corp-Apps Allowed-Mktg-Apps
	New 🛃 Application Filter 🕞 Application Group

46. Click **OK** to close this Security Policy Rule window.

Create Marketing Apps Rule

Create a new Security Policy rule to allow only Marketing users to access the Allowed-Mktg-Applications.

- 47. In **Policies > Security**, click **Add**.
- 48. Under the General tab, enter Allow-Mktg-Apps for the Name.
- 49. For **Description**, enter **Allows only users of marketing group to access** Mktg apps.

Security Policy	Rule
General	ce Destination Application Service/URL Category Act
Name	Allow-Mktg-Apps
Rule Type	universal (default)
Description	Allows only users of marketing group access to Mktg apps.
Tags	

- 50. Select the **Source** tab.
- 51. Under Source Zone, click Add.
- 52. Select Acquisition.
- 53. Under the **Source User** column, click **Add** and enter **marketing**.

Security Policy Rule			
General Source De	stination Application Serv	vice/URL Category Actions	
Any	🔽 Any	select ~	
SOURCE ZONE	SOURCE ADDRESS ^		
Acquisition		🗹 🏖 marketing	

- 54. Select the **Destination** tab.
- 55. Use the drop-down list at the top to select **any**.

Security Policy Rule	
General Source Destination	Application
any V DESTINATION ZONE A	

- 56. Select the **Application** tab.
- 57. **Uncheck** the option for **Any**.

58. Click **Add** and enter the first few letters of the **Allowed-Mktg-App**s to display the Application Groups available:

Security Policy Rule		
General Source Destination Application Se		
Any		
Allow		
Application Group		
 Allowed-Corp-Apps 		
- Allowed-Mktg-Apps		
New 🛃 Application Filter 🛛 🕞 Application Group		

59. Select Allowed-Mktg-Apps.

Security Policy Rule
General Source Destination Application Serv
Any
Allowed-Mktg-Apps

60. In the right side of the **Application** window, place a check box beside **DEPENDS ON**:

General Source Destination	Application	Service/URL Category Acti
Any	Q	
	DEPENDS	ON A
Allowed-Mktg-Apps	Z apple-map	s
	google-bas	se
	google-ma	ps
	🗹 ssl	
	web-brows	sing
	Add To Currer	nt Rule Add To Existing Rule

This action will select all the individual applications under the DEPENDS ON column. Note that the list of applications in the Depends On column may differ from the example here.

61. Click Add to Current Rule to add these applications to this Security Policy rule.

Add To Current Rule

- 62. Select the **Action** tab.
- 63. Verify that the Action is set to Allow.

Security Policy Rule	
General Source Destination Application Service/URL Category	tions
Action Setting Action Allow Send ICMP Unreachable	

When you create a new Security Policy rule, the default setting for Action is Allow. However, it is always a good practice to verify this setting before closing the window.

64. Click **OK** to close this Security Policy Rule window.

Create Deny Rule

Create a new Security Policy rule that will deny any other application traffic for users in the Acquisition zone.

- 65. In the Security Policy table, click Add.
- 66. Select the tab for **General**.
- 67. For Name, enter Deny-All-Others.
- 68. For **Description**, enter **Denies non-approved applications for users in Acquisition zone**.

Security Policy Rule				
General	Source Destination Application Service/URL Category Actions			
R	Name Deny-All-Others le Type universal (default)			
Des	ription Denies non-approved applications for users in the Acquisition zone.			

- 69. Select the tab for **Source**.
- 70. Under the Source Zone column, click Add and select Acquisition.



Note that you do not need to specify any users or user groups under the Source User column. Because the drop-down list is set to **any**, this rule will deny traffic to any user, regardless of group membership.

- 71. Select the tab for **Destination**.
- 72. Use the drop-down list at the top to select **any**.

Security Policy Rule	
General Source Destination	Application
any ~	
DESTINATION ZONE	

73. Select the tab for **Application** and verify that **Any** is checked.

	Security Policy Rule
	General Source Destination Application Service/URL
Γ	Any Any

74. Select Service/URL Category

75. Use the drop-down list at the top to select **any**

Security Policy Rule	
General Source Destination Application	Service/URL Category Actions
any V	

- 76. Select the tab for **Actions**.
- 77. Change the **Action** to **Deny**.

Security Policy Rule	
General Source Destination Application Service/URL Category)
Action Deny Send ICMP Unreachable	~

- 78. Click **OK** to close this Security Policy Rule window.
- 79. Verify that the **Deny-All-Others** rule appears at the bottom of the Security Policy.
- 80. If the "Deny-All-Others" rule does not appear at the bottom of the ruleset, use the **Move Down** button to place the rule just above the "intrazone-default" rule.

Commit the configuration

- 81. Click the **Commit** button at the upper right of the web interface.
- 82. Leave the settings unchanged and click **Commit**.
- 83. Wait until the **Commit** process is complete.
- 84. Click Close.

Generate Traffic from the Acquisition Zone

- 85. On the client workstation, select the window for the Remmina application.
- 86. Select the tab for **Extranet-Server** connection.
- 87. Use the up arrow key to retrieve the previous command:

./Appgenerator-2.sh

- 88. Press Enter to launch the script again.
- 89. While the script is running, move to the next section in which you will examine the firewall logs.

Examine User-ID Logs

You can see information about User-ID through the firewall CLI or in the web interface. In this section, you will use both tools to examine User-ID entries.

- 90. In the firewall web interface, select **Monitor** > **Logs** > **User-ID**.
- 91. The firewall should have numerous entries with username-to-ip-address mappings:

~	RECEIVE TIME	IP	USER	TIMEOUT	GROUP FOUND	DATA SOU
R	07/08 19:56:55	192.168.1.50	chicago\dcrocket	2700	yes	xml-api
R	07/08 19:56:55	172.20.200.20	chicago\dboone	2700	yes	xml-api
R	07/08 19:56:55	10.10.17.102	chicago\wearp	2700	yes	xml-api
R	07/08 19:56:55	192.168.1.47	chicago\wbhickock	2700	yes	xml-api
R	07/08 19:56:55	192.168.1.46	chicago\skid	2700	yes	xml-api
R	07/08 19:56:55	192.168.1.45	chicago\sbull	2700	yes	xml-api
R	07/08 19:56:55	192.168.1.44	chicago\pgarrett	2700	yes	xml-api
F	07/08 19:56:55	192 168 1 43	chicago\iringo	2700	Ves	xml-ani

Note that the entries you see will differ from this example.

- 92. On the client desktop, locate the main window for the Remmina application.
- 93. Double-click the Firewall-A connection.
- 94. This action will open a connection to the firewall CLI.
- 95. In the firewall CLI, enter the following command to display entries for User-ID:

show user ip-user-mapping all <Enter>

96. The firewall will display User-ID information:

IP	Vsys	From	User	<pre>IdleTimeout(s)</pre>	<pre>MaxTimeout(s)</pre>
10.10.24.102	vsysl	XMLAPI	chicago\jcaesar	2558	2558
192.168.1.9	vsys1	XMLAPI	chicago\nnickleby	2558	2558
10.4.5.101	vsys1	XMLAPI	chicago\tsawyer	2558	2558
192.168.1.104	vsys1	XMLAPI	chicago\mrhyde	2558	2558
192.168.1.22	vsys1	XMLAPI	chicago\hpoirot	2558	2558
192.168.1.43	vsys1	XMLAPI	chicago\jringo	2558	2558
192.168.1.36	vsys1	XMLAPI	chicago\bbill	2558	2558
192.168.1.41	vsys1	XMLAPI	chicago\gronimo	2558	2558
192.168.1.2	vsys1	XMLAPI	chicago\drjekyll	2558	2558
192.168.1.13	vsys1	XMLAPI	chicago\jhawkins	2558	2558
192 168 1 102	vsvs1	ΧΜΙ ΔΡΤ	chicago\hfinn	2558	2558

97. When you have finished examining the User-ID information, type **exit** <**Enter**> to close the firewall SSH connection.

Examine Firewall Traffic Log

Create and apply filters in the **Traffic** log to answer the questions in this section.

- 98. In the firewall web interface, select **Monitor** > **Logs** > **Traffic**.
- 99. Write down your answers to the following questions in the space provided or on notepaper:

Question: Which rule does the firewall use when it encounters youtube-base traffic?

Hint: Use the filter (app eq youtube-base)

Answer: Deny-All-Others

Question: Which rule does the firewall use when it encounters dns traffic?

Hint: Use the filter (app eq dns)

Answer: Allow-Corp-Apps (in some cases, you may also see Users_to_Extranet)

Question: Which rule does the firewall use when it encounters facebook-base?

Hint: Use the filter (app eq facebook-base)

Answer: Allow-Mktg-Apps and Deny-All-Others (depending on the Source User)

Question: Which users are allowed access to facebook-base?

Hint: Use the filter (app eq facebook-base) and (action eq allow)

Answer: chicago\hpoirot; chicago\sholmes; chicago\vhelsing

Question: Is the user sholmes allowed to access instagram-base?

Hint: Use the filter (app eq instagram-base) and (user.src eq 'chicago\sholmes')

Answer: Yes

Question: Is the user bbart allowed to access instagram-base?

Hint: Use the filter (app eq instagram-base) and (user.src eq 'chicago\bbart)

Answer: No

Clean Up the Desktop

- 100. In the Traffic log window on the firewall, clear any filters you have in place.
- 101. In the Remmina window on the client workstation, select the tab for the **Server-Extranet**.
- 102. Close the SSH connection by typing **exit <Enter>**.
- 103. Close the main Remmina application window.



Stop. This is the end of the lab.

Lab 13: Using Decryption to Block Threats in Encrypted Traffic

As an astute network security professional, you have noticed the dramatic increase of HTTPS secure traffic over the past few years. Correspondingly, you have noticed that very few websites even use unencrypted HTTP traffic anymore. Virtually all network traffic is now encrypted.

You know that HTTPS protects privacy and sensitive data in transit between hosts, but you have begun to realize that HTTPS also hides potentially damaging data as well. Encrypted traffic into and out of your network might contain viruses, spyware, vulnerability exploits and other damaging types of data.

You need to make certain that the Palo Alto Networks firewall can inspect even encrypted traffic, so you have decided to implement decryption. This process will allow the firewall to decrypt HTTPS traffic, inspect it and then block any sessions that contain malicious content.



Right now, you do not have budget funds available to build a corporate PKI infrastructure to generate a decryption certificate from a CA (certificate authority). However, you can generate a self-signed CA certificate on the Palo Alto Networks firewall and deploy that for decryption

© 2024 Palo Alto Networks, Inc.

HR has also told you that there are certain types of traffic from employees that should not be decrypted because those transactions might contain personally identifiable information (PII). You need to exclude certain categories of websites (such as finance and healthcare) from decryption. You will create a No-Decrypt rule to prevent the firewall from decrypting traffic to and from these kinds of websites.

Lab Objectives

- Load a lab configuration
- Test the firewall without decryption
- Create a self-signed certificate for trusted connections
- Create a self-signed certificate for untrusted connections
- Create and test a Decryption Policy rule for outbound traffic
- Test outbound Decryption Policy rule
- Export the firewall certificate and import it to the Firefox browser
- Test outbound Decryption Policy again
- Review firewall logs
- Exclude URL categories from decryption using a No-Decrypt rule
- Test the No-Decrypt rule



The lab instructions show you how to import a certificate to the Firefox browser, so for this lab, use Firefox for testing and Chromium to configure the firewall. Although the concept of using a firewall-issued certificate for decryption in any client browser is the same, the actual steps to carry out the import process are different.

High-Level Lab Steps

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-13.xml** - to the Firewall

Test the Firewall Behavior Without Decryption

- On the client-A host, use the Firefox browser and browse to the following URI: http://192.168.50.80/eicar.com
- Note the block page that the firewall presents Your Antivirus Security Profile is in place and has blocked this file
- Use Firefox to browse to www.eicar.org.

- In the Eicar website, navigate to Download Anti Malware Testfile > Download area using the secure, SSL enabled protocol HTTPS
- Download the **eicar.com** file
- When prompted to save the file, click **Cancel**.
- Close the configuration browser.

Create a Self-Signed Certificate for Trusted Connections

Use the information in the table below to create a self-signed certificate to use as a Forward Trust Certificate.

Parameter	Value
Certificate Name	Type trusted-cert
Common Name	Type 192.168.1.1
Certificate Authority	Select the Certificate Authority check box
Forward Trust Certificate	Checked

Create a Decryption Policy Rule for Outbound Traffic

Use the information below to create a Decryption Policy rule that will decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

Parameter	Value	
Name	Decrypt_Users_Traffic	
Description	Decrypts web traffic from Users_Net.	
Source Zone	Users_Net	
Source Address	Any	
Source User	Any	
Destination Zone	Internet	
	Extranet	
Destination Address	Any	
Service	any	
URL Category	Any	
Action	Decrypt	

Parameter	Value
Туре	SSL Forward Proxy
Decryption Profile	None

Commit the configuration

• Commit the changes before proceeding.

Test Outbound Decryption Policy

- Use Firefox to browse to https://www.bing.com.
- Use the Advanced > View Certificate buttons to note that the Issuer Name section contains 192.168.1.1
- Close Firefox.

Export the Firewall Certificate

- From the firewall web interface, export the trusted-cert as a Base64 Encoded Certificate (PEM)
- Save the file to the Downloads folder of the Client-A host

Import the Firewall Certificate to configuration browser

- Use the Certificate Manager in Firefox to Import the **cert_trusted-cert.crt** to the **Authorities** section.
- Set Firefox to **Trust this CA to identify websites** and **Trust this CA to identify email** users

Test Outbound Decryption Policy Again

- In Firefox, browse to https://www.eicar.org
- Navigate to Download Anti Malware Testfile > Download
- Attempt to download the **eicar.com** file
- You will receive a warning page from the firewall indicating that it has detected and blocked the malicious file download
- Close Firefox.

Review Firewall Logs

- Add the Decrypted column to the **Traffic Log**
- Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table.

- Create and apply a filter to display entries that have been decrypted from the client workstation and that have been terminated because of a detected threat in the traffic
- Examine the Detailed Log View of a matching entry to see details about the session
- Use the **Threat** Log to locate entries about the eicar.com test file that the firewall detected and blocked

Exclude URL Categories from Decryption

• Use the information below to create an entry in the Decryption Policy that will exclude certain URL categories from decryption

Parameter	Value
Name	No-Decryption
Description	Do not decrypt URLs in gov, shopping and finance
Source Zone	Users_Net
Destination Zone	Internet
Service	any
URL Category	government
	financial-services
	shopping
Action	No Decrypt
Туре	SSL Forward Proxy

Note that in a production environment, the URL Categories which you exclude from decryption will depend on many factors. Company policy, national privacy laws, HR concerns, destination country – all of these can dictate what types of traffic you should or should not decrypt. The examples we use here simple ones to illustrate how to exclude URL categories from decryption.

• Place this rule at the top of the **Decryption** Policy

Commit the configuration

• Commit the changes before proceeding

Test the No-Decryption Rule

- Use Firefox to browse to a website that falls into one of the excluded categories.
- Connect to <u>https://texas.gov</u>
- Examine the certificate issued to the texas.gov website
- Note that the Issuer Name is *not* 192.168.1.1 (the firewall)

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot.
- 3. Click the drop-down list next to the Name text box and select edu-210-11.1a-13.xml.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

4. Click OK.

- 5. A window should open that confirms that the configuration is being loaded.
- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.

Test the Firewall Behavior Without Decryption

For this lab, use Firefox to test and Chromium to configure. The instructions for this lab will walk you through the process of installing a Trusted certificate from the firewall in Firefox. You can install a Trusted certificate in the other browsers as well; however, the lab will only show you how to do so in Firefox to illustrate the process and in order to make sure you have time to complete the tasks.

- 10. On the client desktop, open Firefox and browse to http://192.168.50.80/eicar.com
- 11. You should get a page indicating that the connection was reset:



- 12. In the firewall web interface, navigate to Monitor > Logs > Threat.
- 13. You should see one or more entries for vulnerability indicating that the firewall blocked the Eicar file download:

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	DESTINATION ADDRESS
EQ.	03/07 17:36:13	vulnerability	Eicar File Detected	Users_Net	Extranet	192.168.1.20		192.168.50.80

Because the connection between the client and the server is not encrypted, the firewall is able to examine the traffic and block malicious content.

- 14. In Firefox, open a new tab and browse to https://192.168.50.80/eicar.com.
- 15. If the browser presents a Warning window, click the Advanced button.



16. Click Accept the Risk and Continue.



The web server is using a self-signed SSL certificate, which is why Firefox presents this warning.

17. When you are prompted to save the file, click **Cancel**.

Cancel	Name eicar.com			٩	Save
A Home	▲ lab-user Downloads				D
Desktop	Name	-	Size	Туре	Modifi€
Documents					
👲 Downloads					
🖹 thinclient_drives 🔺					
Music					
Pictures					
Videos					
					*.com 🔻

Notice that the download is *not* blocked because the connection is encrypted, and the virus is hidden. This exercise proves that without Decryption, the firewall is unable to examine the contents of a secure connection and cannot scan for malicious content.

18. Close Firefox.

Create Certificate for Trusted Connections

In this section, you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that have certificates issued by trusted certificate authorities.

The firewall will use this certificate as part of the decryption process between clients and trusted HTTPS websites.

- 19. In the web interface, select **Device > Certificate Management > Certificates**.
- 20. Click Generate at the bottom of the page to create a new CA certificate:

🔜 Generate

21. Configure the following:

Parameter	Value
Certificate Name	trusted-cert
Common Name	192.168.1.1
Certificate Authority	Select the Certificate Authority check box

Gen	erate Certifica	te		?
	Certificate Type	 Local 	◯ SCEP	
	Certificate Name	trusted-cert]	
	Common Name	192.168.1.1]	
		IP or FQDN to app	pear on the certificate	
	Signed By			~
		Certificate A	uthority e Key Export	
	OCSP Responder			\sim
٢ ^	Cryptographic Sett	ings		
	Algorithm	RSA		

22. Leave the remaining settings unchanged and click **Generate** to create the certificate. A **Generate Certificate** status window should open that confirms that the certificate and key

pair were generated successfully.

- 23. Click **OK** to close the **Generate Certificate** success window.
- 24. You should have a new entry in the **Device Certificates** table:

De	Device Certificates Default Trusted Certificate Authorities									
Q										
	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE	
	TLSv1.3_Default	C = US, ST = CA, L = Santa Cla	C = US, ST = CA, L = Santa Cla		\checkmark	Aug 14 15:40:00 2033 GMT	valid	Elliptic Curve DSA		
	🗊 trusted-cert	CN = 192.168.1.1	CN = 192.168.1.1	\checkmark		Oct 25 17:14:25 2024 GMT	valid	RSA		

- 25. Edit the entry for trusted-cert by clicking it.
- 26. Place a **check** in the box for **Forward Trust Certificate**.
- 27. Leave the remaining settings unchanged.

Certificate info	Certificate information (
Name	trusted-cert					
Subject	192.168.1.1					
Issuer	192.168.1.1					
Not Valid Before	Dec 16 15:11:09 2022 GMT					
Not Valid After	Dec 16 15:11:09 2023 GMT					
Algorithm	RSA					
	Certificate Authority					
	V Forward Trust Certificate					
	Forward Untrust Certificate					
	Trusted Root CA					
	ОК	Cancel				

This action instructs the firewall to use this certificate to decrypt traffic between clients and sites which have a trusted HTTPS certificate.

Note that the dates for Not Valid Before and Not Valid After will be different for your certificate.

28. Click OK.

Create a Certificate for Untrusted Connections

In this section, you will generate a certificate on the firewall that will be used when clients connect to HTTPS websites that <u>do not</u> have certificates issued by trusted certificate authorities.

The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

- 29. In the web interface, select **Device > Certificate Management > Certificates**.
- 30. Click Generate at the bottom of the page to create a new CA certificate:

👼 Generate

31. Configure the following:

Parameter	Value
Certificate Name	untrusted-cert

Parameter	Value
Common Name	DO NOT TRUST
Certificate Authority	Select the Certificate Authority check box

Generate Certificate	?
Certificate Type 🧿 Local 🔷 SCEP	
Certificate Name untrusted-cert	
Common Name DO NOT TRUST	
IP or FQDN to appear on the certificate	
Signed By	\sim
Certificate Authority	
OCSP Responder	\sim
Cryptographic Settings	
Algorithm RSA	\sim

- 32. Leave the remaining settings unchanged and click **Generate** to create the certificate. A **Generate Certificate** status window should open that confirms that the certificate and key pair were generated successfully.
- 33. Click **OK** to close the **Generate Certificate** success window.
- 34. You should have a new entry in the **Device Certificates** table.
- 35. Edit the entry for **untrusted-cert** by clicking it.
- 36. Place a **check** in the box for **Forward Untrust Certificate**.

37. Leave the remaining settings unchanged.

Certificate info	ormation	0
Name	untrusted-cert	
Subject	DO NO TRUST	
Issuer	DO NO TRUST	
Not Valid Before	Dec 16 15:14:02 2022 GMT	
Not Valid After	Dec 16 15:14:02 2023 GMT	
Algorithm	RSA	
	Certificate Authority	
	Forward Trust Certificate	
	Forward Untrust Certificate	
	Trusted Root CA	
Revoke		OK Cancel

This action instructs the firewall to use this certificate when it encounters a site that is not trusted – one that has a self-signed certificate, for example.

Note that the dates for Not Valid Before and Not Valid After will be different for your certificate.

- 38. Click OK.
- 39. You should now have two new entries in the **Device Certificates** table:

	Device Certificates Default Trusted Certificate Authorities									
	۹(
		NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
		TI Sv1 3 Default	C = US. ST = CA. L = Santa Cla	C = US. ST = CA. L = Santa Cla			Aug 14 15:40:00 2033 GMT	valid	Elliptic Curve DSA	
		🗊 trusted-cert	CN = 192.168.1.1	CN = 192.168.1.1			Oct 25 17:14:25 2024 GMT	valid	RSA	Forward Trust Certificate
U		🗊 untrusted-cert	CN = DO NOT TRUST	CN = DO NOT TRUST		\checkmark	Oct 25 17:18:02 2024 GMT	valid	RSA	Forward Untrust Certificate

Note that the dates for Expires will be different for your certificates.

Create a Decryption Policy Rule for Outbound Traffic

In this section, you will create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet and Extranet security zones.

- 40. In the firewall web interface, select **Policies > Decryption**.
- 41. Click Add to create a decryption Policy rule.

A Decryption Policy Rule window should open.

42. Configure the following:
| Parameter | Value |
|-------------|-------------------------------------|
| Name | Decrypt_Users_Traffic |
| Description | Decrypts web traffic from Users_Net |

Decryption Policy Rule

Ger	neral	Sourc	ce Destination Service/URL Category Op	otio
	$\left(\right)$	Name	Decrypt_Users_Traffic	
	Desc	ription	Decrypts web traffic from Users_Net	
	Desc	ription	Decrypts web traffic from Users_Net	

43. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	Users_Net
Source Address	Verify that the Any check box is selected
Source User	Verify that any is selected
Source Device	Verify that any is selected

Decryption Po	licy Rule
General Source	e Destination Service/URL Catego
Any SOURCE ZONE	Any SOURCE ADDRESS
Users_Net	

44. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Internet Extranet

Parameter	Value	
Destination Address	Verify that the Any check box is selected	
Destination Device	Verify that the Any check box is selected	

Decryption Policy Rule

General Source	Destination	Service/URL Category Options
Any		🔽 Any
DESTINATION ZO	NE A	DESTINATION ADDRESS
🔲 🎮 Internet		
Z Extranet		

45. Click the **Service/URL Category** tab and verify that the **Service** is set to **Any** and that the box for **Any** above **URL Category** is **checked**:

Decryption Policy Rule	
General Source Destination	Service/URL Category Options
any V	URL CATEGORY

Note that the **Any** setting for URL category instructs the firewall to decrypt all HTTPS traffic, regardless of the type of website users are accessing. Decrypting traffic from users to website categories such as Health and Medicine, Shopping or Government can expose Personally Identifiable Information (PII). In a production environment, you will need to make sure you only decrypt traffic that is appropriate.

Later in this lab, you will exclude several categories of websites as an illustration.

46. Click the **Options** tab and configure the following:

Parameter	Value
Action	Decrypt
Туре	Verify that SSL Forward Proxy is selected

Parameter	Value
Decryption Profile	Select default
Decryption Policy Rule	(?)
General Source Destina	tion Service/URL Category Options
Action O No Decry	ot Oecrypt
Type SSL Forward	Proxy
Decryption Profile default	✓
Log Settings	
Log Succ	essful SSL Handshake
🗸 Log Unsu	ccessful SSL Handshake
Log Forwarding None	✓
	OK Cancel

- 47. Leave the remaining settings unchanged.
- 48. Click **OK** to close the **Decryption Policy Rule** configuration window.
- 49. Verify that your configuration matches the following:

			Source	Destination				
		NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	ТҮРЕ
Γ	1	Decrypt_Users_Traffic~	🚧 Users_Net	🞮 Extranet	any	any	decrypt	ssl-forward-proxy
				Mainternet				

Note that several columns have been hidden or rearranged in the example shown here.

Commit the configuration

- 50. Click the **Commit** button at the upper right of the web interface.
- 51. Leave the settings unchanged and click **Commit**.
- 52. Wait until the **Commit** process is complete.
- 53. Click Close.

Test Outbound Decryption Policy

- 54. Open Firefox and browse to https://www.paloaltonetworks.com.
- 55. The browser presents a Caution message.

Software is Preventing Firefox From Safely Connecting to This Site

www.paloaltonetworks.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **192.168.1.1**, which is either software on your computer or your network.

What can you do about it?

- If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **192.168.1.1**, then this could be an attack and you should not continue to the site.

Learn more...

Go Back (Recommended)

Advanced...

Note: The configuration browser on the client workstation does not trust the certificate generated by the firewall (192.168.1.1).

- 56. Click the button for **Advanced**.
- 57. Click the link for **View Certificate**.

Firefox is b (CA) store.	acked by the non-p The CA store help	profit Mozilla, which administers a co s ensure that certificate authorities	ompletely open certificate authority are following best practices for user
security.			
Firefox use by the user with a secu considered	s the Mozilla CA st 's operating system rity certificate issue unsafe.	ore to verify that a connection is see n. So, if an antivirus program or a ne ed by a CA that is not in the Mozilla	cure, rather than certificates supplied etwork is intercepting a connection CA store, the connection is
Error code:	MOZILLA_PKIX_E	ERROR_MITM_DETECTED	
View Certif	cate		
ALCAR OCTUR	Perto.		

58. Under the section for ***paloaltonetworks.com**, note the **Issuer Name** section contains **192.168.1.1**:

	Certificate				
*.paloalto	networks.com	192.168.1.1			
Subject Name					
State/Province	California				
Locality	Santa Clara				
Organization	Palo Alto Networks, Inc.				
Common Name	*.paloaltonetworks.com				
Issuer Name					
Common Name	192.168.1.1				
Validity					
Not Refore	0/22/2021 8:00:00 DM (Eastern Standard Ti	me)			

This certificate has been issued on behalf of *.paloaltonetworks.com by the firewall (192.168.1.1) using the Trusted Certificate you created earlier. Firefox does not trust this certificate because it is "self-signed" by the firewall. In the next section, you will fix this issue so that Firefox trusts certificates issued by the firewall.

59. Close the Firefox browser.

Export the Firewall Certificate

To make users' web browsing experience seamless while implementing decryption, you will export the trusted certificate from the firewall and import the certificate into Firefox on the Client host.



- 60. In the firewall web interface, select **Device > Certificate Management > Certificates**.
- 61. Highlight but do not open **trusted-cert**.
- 62. At the bottom of the window, click **Export Certificate** to open the **Export Certificate** configuration window.
- 63. Use the drop-down list for File Format to verify that **Base64 Encoded Certificate** (**PEM**) is selected.
- 64. Leave the box for **Export Private Key** unchecked.
- 65. Leave all settings unchanged and click **OK** to export the trusted-cert CA certificate.

Export Private Key	
	Export Private Key

66. Save the file to the workstation's **Downloads** folder:

Cancel	Name cert_trusted-cert.crt			۹	Save
🔒 Home					D
Desktop	Name	-	Size	Туре	Modifi
Documents					
🛋 thinclient_drives 📥					
Music					
Pictures					
Videos					
			plain t	text do	cument 🔻

Import the Firewall Certificate

- 67. Open the Firefox browser.
- 68. In the upper right corner of the browser window, click the "hamburger" button and choose **Settings**:



69. On the left side of the screen, select **Privacy & Security**:



- 70. Scroll to the bottom of the screen and locate the **Certificates** section.
- 71. Click the button for View Certificates.

Certificates		
\mathbf{Q} uery OCSP responder servers to confirm the current validity of	View <u>C</u> ertificates	
certificates	Security <u>D</u> evices	

72. Under the Authorities tab, click Import.

	Certificate	Manager				>
Your Certificates	Authentication Decis	sions Pe	ople	Servers	Authorities	_
You have certificates on	file that identify thes	e certificate a	authorities			
Certificate Name		Security [Device			E,
\sim AC Camerfirma S.A.						
Chambers of Com	merce Root - 2008	Builtin Obje	ect Token			
Global Chambersig	jn Root - 2008	Builtin Obje	ect Token			
✓ AC Camerfirma SA C	IF A82743287					
Camerfirma Cham	bers of Commerce R	. Builtin Obje	ect Token			
Camerfirma Global	Chambersign Root	Builtin Obje	ect Token			
View <u>E</u> dit Tr	ust I <u>m</u> port	Export	Dele	ete or Dist	trust	ĸ

- 73. Select the **Downloads** folder.
- 74. Highlight the entry for **cert_trusted-cert.crt**.
- 75. Click **Open**.

Cancel	Select File containing CA certificate(s) to import
⊘ Recent	A lab-user Downloads
🔒 Home	Name
Desktop	
Documents	
Downloads ■	

76. In **the Downloading Certificate** window, place **checks** in both boxes for **Trust this CA to** ...

	Downloading Certificate		×
You have bee	en asked to trust a new Certificate Authority (CA)).	
Do you want	to trust "192.168.1.1" for the following purposes?		
🗹 Trust this	CA to identify websites.		
🔽 Trust this	CA to identify email users.		
Before trusti procedures (ng this CA for any purpose, you should examine in if available).	ts certificate and i	ts policy and
View	Examine CA certificate		
		Cancel	ОК

77. Click OK.

	Certificate	e Manager		
Your Certificates	Authentication Deci	sions Peopl	e Servers	Authorities
You have certificates or	file that identify thes	e certificate autl	horities	
Certificate Name		Security Dev	vice	
~ 192.168.1.1				
192.168.1.1		Software Seco	urity Device	
~ AC Camerfirma S.A.				
Chambers of Com	imerce Root - 2008	Builtin Object	Token	
Global Chambersi	gn Root - 2008	Builtin Object	Token	
~ AC Camerfirma SA 0	CIF A82743287			
	- (A B	D 10 01 1	T 1	
View Edit T	rust I <u>m</u> port	E <u>x</u> port	Delete or Distr	rust
				0

78. The firewall **trusted-cert** entry appears in the list of certificate authorities:



Note – if you do not see the entry for 192.168.1.1 at the top of the list, click **OK** and then click **View Certificates** again.

The Firefox browser will trust any certificate issued by the entities in this Authorities list. By adding the firewall certificate to this list, Firefox will trust any certificates issued by the firewall. Note that the process of importing certificates to client workstations varies based on the browser type and the operating system. This lab shows you how to add a certificate to Firefox, but the process is similar for other browsers.

- 79. Click **OK** to close the **Certificate Manager** window.
- 80. Close Firefox.
- 81. Open Firefox and browse to https://www.paloaltonetworks.com.
- 82. Notice that you do not get any warning messages about certificates.

Test Forward Untrust Certificate

When a web browser connects to a site that has a self-signed or untrusted certificate, the firewall will present the Forward Untrust Certificate. The web server in the Extranet zone has a self-signed certificate; in this section, you will see how the firewall presents the DO NOT TRUST certificate you created.

- 83. In Firefox, connect to https://192.168.50.80.
- 84. Note the **Warning** message that configuration browser presents:

<mark>.</mark>	Warning: Potential Security Risk Ahead				
	Firefox detected a potential security threat and did not continue to 192.168.50.80. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.				
	What can you do about it?				
	The issue is most likely with the website, and there is nothing you can do to resolve it.				
	If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.				
	Learn more				
	Go Back (Recommended) Advanced				

- 85. Click Advanced.
- 86. Click View Certificate.

Someone could be trying to impersonate the site and you should not continue.					
Websites prove their identity via certificates. Firefox does not trust 192.168.50.80 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.					
Error code: SEC_ERROR_UNKNOWN_ISSUER					
View Certificate					
Go Back (Recommended)	Accept the Risk and Continue				

87. Note the information in the certificate:

	Certificate				
192.168	.50.80			DO NOT TRUST	
Subject Name Country State/Province Common Name	AU New South Wales 192.168.50.80				
Issuer Name Common Name	DO NOT TRUST				
Validity Not Before	9/14/2020, 2:58:48 AM	M (Eastern D	aylight Time)		

You can tell that the firewall has intervened in this connection and presented the Forward Untrust certificate you created.

88. Close the tab for Certificate for 192.168.50.80.

Test Outbound Decryption Policy Again

89. In the Firefox browser warning window, click Accept the Risk and Continue:



90. You will see the default page for the web server in the Extranet:



- 91. Attempt to download the virus file by appending eicar.com to the end of the link https://192.168.50.80/<u>eicar.com</u> <ENTER>
- 92. The connection will not succeed, and you will receive a message from the browser:



Note that the kind of message a client receives will vary depending on the browser.

93. Close Firefox.

Review Firewall Logs

In this section, you will examine information in the firewall Logs to see more details about the decryption process.

- 94. In the firewall web interface, select **Monitor** > **Logs** > **Traffic**.
- 95. Click the small triangle to the right of the Threat ID/Name column header.
- 96. Add the **Decrypted** column to the table by selecting **Columns > Decrypted**.

		App Subcategory
		App Technology
THREAT ID/NAME		ZOI Captive Portal
Eiro Eile Datastad		Content Version
Elcar File Detected		Count
Eicar File Detected	Adjust Columns	Decrypted
		Destination Country
		Destination Device Category
		Destination Device Host

97. Drag and drop the **Session End Reason** column from the right side of the table to the beginning of the table:

		Drag and column h	drop nere		-	
SESSION END REASON	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	DECRYPTED	SOURCE U
aged-out	07/09 15:20:48	Users_Net	Internet	192.168.1.254	no	
aged-out	07/09 15:20:48	Users_Net	Internet	192.168.1.254	no	
aged-out	07/09 15:20:48	Users_Net	Extranet	192.168.1.254	no	

This is not a requirement, but placing this column at the beginning of the table will make it easier for you to locate entries that have ended because of unusual actions taken by the firewall (such as detecting a threat).

98. Create and apply a filter to display entries that have been decrypted from the client workstation and that have been terminated because of a detected threat in the traffic:(flags has proxy)

The filter syntax "flags has proxy" displays entries that have been decrypted (the value will show as **yes** in the **Decrypted** column). Entries that match the filter indicate that the firewall carried out a proxy connection for decryption.

- 99. Click the **magnifying glass** next to the most recent entry listed to see details about the session.
- 100. Scroll down in the upper section of the window until you see the Flags section in the right column.
- 101. Note the **Decrypted** box is checked, indicating that the firewall decrypted this session.

Det	ailed Log Vie	w											? 🗆
Se	ssion End Reason Category	threat private-ip-a	addresses						Flags				
	Device SN			Details					T Tags				
	IP Protocol	tcp			Type	e end				Captive Por	rtal		
	Log Action				Byte	s 3800			Pro	xy Transacti	ion	1	
	Generated Time	2022/09/1	12 17:44:53	By	tes Receivee	d 2140				Decrypt	ted 🔽	J	
	Start Time	2022/09/1	12 17:43:20		Bytes Sen	t 1660			P	acket Capti	ure		
	Receive Time	2022/09/1	12 17:44:53	R	lepeat Coun	t 1			c	lient to Ser	ver		
	Elapsed Time(sec)	0			Packet	s 13			S	erver to Clie	ent		
	Tunnel Type	N/A		Pack	ets Received	d 5			Sym	metric Retu	urn		
	Flow Type	NonProxyT	raffic		Packets Sen	t 8				Mirro	red		
	Cluster Name				Source UUIE)			Tur	nnel Inspect	ted 🗌		
РСАР		ТҮРЕ	APPLICAT	ACTION	RULE	RULE UUID	ВΥ	SEVERI	CATEG	URL CATEG LIST	VERDI	URL	FILE NAME
	2022/09/12	end	web-	allow	Users	de4d44a	5-7ac6-	471a-997f-a	8770c3d9c	3d			

The details you see will differ from the example shown, but you should see similar information.

102. Click **Close** in the Detailed Log View window.

- 103. Select **Monitor > Logs > Threat**.
- 104. Add the **Decrypted** column to the table.
- 105. Create and apply a filter in the Threat Log to show decrypted session:

(flags has proxy)

С	20	flags	has proxy)				
			RECEIVE TIME	ТҮРЕ	DECRYPTED	THREAT ID/NAME	FROM ZONE
E	2		09/12 17:43:28	vulnerability	yes	Eicar File Detected	Users

- 106. Click the magnifying glass icon next to the entry for vulnerability.
- 107. In the top portion of the window, scroll down until you can see the **Details** section in the middle column.
- 108. You can see information about the file that the firewall detected and blocked:



Note the ID number 39040 and the link **View in Threat Vault**. The ID number is a unique value assigned to each threat by Palo Alto Networks. Threat Vault is an online database maintained by Palo Alto Networks with extensive information about each threat. Access to Threat Vault requires a support account.

109. In the bottom of the window, highlight an entry with **Type vulnerability** to see more information about why the firewall terminated this connection.

Detailed	d Log View								
Genera	al			Source			Destination		
	Session ID26004Actionreset-bothHost IDweb-browsingRuleUsers_to_ExtranetRule UUIDde4d44a5-7ac6-471a-997f-a8770c3d9c3dDevice SN007051000055975IP ProtocoltcpLog Action2022/09/12 17:43:28Receive Time2022/09/12 17:43:28Tunnel TypeN/ACluster Name		Source User Source Source DAG Country Port Zone Interface X-Forwarded-For IP	Source User Source 192.168.1.20 Source DAG Country 192.168.0.0-192.168.255.255 Port 53964 Zone Users_Net Interface ethernet1/2 arded-For IP		Destination User Destination Destination DAG Country Port Zone Interface	192.168.50.80 192.168.0.0-192 443 Extranet ethernet1/3	168.255.255	
Ge			Details Threat Type Threat ID/Name ID Category Content Version	vulnerability Eicar File Detected 39040 (View in Thre code-execution AppThreat-8601-74:	at Vault) 87	Flags Captive Portal Proxy Transaction Decrypted Packet Capture Client to Server			
PCAP RE	CEIVE TIME ^	3	TYPE vulnerability	APPLICATION web-browsing	ACTION reset-both	RULE Users_to_Extranet	SEVERITY	CATEGORY private-ip- addresses	FILE NAME eicar.com
20	022/09/12 17:43:28	3	vulnerability	web-browsing	reset-both	Users_to_Extranet	medium	private-ip- addresses	eicar.com
20	22/09/12 17:43:28	3	vulnerability	web-browsing	reset-both High	Users_to_Extranet	or vulnerabil	private-ip- addresses	eicar.com

Note that when you select the row, the information in the top half of the window changes.

- 110. Click **Close** in the **Detailed Log View**.
- 111. Clear the filter you have in place in the Threat log by clicking the **X** in the upper right corner of the window.



Exclude URL Categories from Decryption

The existing Decryption Policy rule you created instructs the firewall to decrypt all traffic, regardless of the URL category. In this section, you will configure a No-Decrypt rule that instructs the firewall to exclude sensitive categories of web traffic from decryption in order to avoid exposing PII (Personally Identifiable Information).



Note that in a production environment, the URL Categories which you exclude from decryption will depend on many factors. Company policy, national privacy laws, HR concerns, destination country – all of these can dictate what types of traffic you should or should not decrypt. The examples we use here are simple ones to illustrate how to exclude URL categories from decryption.

- 112. In the firewall web browser, select **Policies > Decryption**.
- 113. Click Add.
- 114. Under the **General** tab, enter **No-Decryption** for **Name**.

115. For **Description**, enter **Do not decrypt URLs in gov, shopping and finance**.



- 116. Select the tab for **Source**.
- 117. Under the Source Zone section, click Add and select Users_Net.

Decryption Policy Rule						
General Source Destinatio	n Service/URL					
	Any					
Users_Net						

- 118. Select the **Destination** tab.
- 119. Under the Destination Zone section, click Add and select Internet.

Decryption Policy Rule						
General Source	Destination	Service/URL Category O				
Any DESTINATION ZON Printernet	IE A	Any DESTINATION A				

- 120. Select the tab for **Service/URL Category**.
- 121. Leave the **Service** set to **any**.

122. Under the **URL Category**, use the **Add** button to add **government**, **financial-services**, and **shopping**.

Decryption Policy Rule	
General Source Destination	Service/URL Category Options
any 🗸	Any
SERVICE ^	URL CATEGORY
	government
	financial-services
	shopping
	Add Delete

- 123. Select the tab for **Options**.
- 124. Verify that the **Action** is set to **No Decrypt**.
- 125. Set the Decryption Profile to default.

Decryption Policy Rule							
General Source	te Destination Service/URL Category Options						
Action	No Decrypt Decrypt						
Туре	SSL Forward Proxy						
Decryption Profile	default						
Log Settings							
	Log Successful SSL Handshake						

- 126. Leave the remaining settings unchanged.
- 127. Click **OK** to create this entry.
- 128. You should have two entries in the **Decryption** Policy.

		Source	Destination			
~	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION
1	Decrypt_Users_Traffic	🚾 Users_Net	🚧 Extranet	any	any	decrypt
			Mainternet			
2	No-Decryption	Z Users_Net	Mainternet	financial-services	any	no-decrypt
				government		
				shopping		

129. Before you proceed, answer the following question:

Is there anything wrong with these Decryption Policy rules?

The answer is yes. They are in the wrong order. All traffic will match the first rule Decrypt_Users_Traffic because the URL category is set to **any**. The firewall will therefore never proceed beyond the first rule to implement the second rule, which instructs the firewall to exclude financial-services, government and shopping websites from decryption.

130. Highlight the **No-Decryption** rule entry (but do not open it).

131. At the bottom of the window, click **Move > Move Top**.

		Source	Destination				
	NAME	ZONE	ZONE	U	JRL CATEGORY	SERVICE	ACTION
1	Decrypt_User_Traffic	Wers_Net	🚧 Extranet	a	iny	any	decrypt
			2 Internet				
2	No-Decryption	थ Users_Net	Mage Internet	fi	inancial-services	any	no-decrypt
				g	overnment		
				s	hopping		
				M M M M M	love Top love Up love Down love Bottom love To Position		
(+) A	Add 😑 Delete 🔞 Cl	one 🕜 Enable	🚫 Disable	Move	• • DF/C	SV 🗌 Highlig	ht Unused Rules [

132. The rules now should be in the correct order:

		Source	Destination			
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION
1	No-Decryption	🚧 Users_Net	Mainternet	financial-services government shopping	any	no-decrypt
2	Decrypt_Users_Traffic	थ Users_Net	थ Extranet	any	any	decrypt

Always place no-decrypt rules at the beginning of the Decryption Policy table.

Commit the configuration

- 133. Click the **Commit** button at the upper right of the web interface.
- 134. Leave the settings unchanged and click **Commit**.
- 135. Wait until the **Commit** process is complete.
- 136. Click Close.

Test the No-Decryption Rule

With your No-Decryption rule in place, browse to a website that falls into one of the excluded categories.

- 137. Open Firefox.
- 138. Connect to https://texas.gov.

139. Click the **padlock** icon just in front of the URL:



140. Click the **arrow** next to **Connection secure**:



141. Click More information.

8	https://www.texas.gov
<	Connection security for www.texas.gov
6	You are securely connected to this site.
V	erified by: Amazon
N	lore information

The Certificate details you see may vary from this example because we are testing with live websites that may change.

142. Click View Certificate:

Page Info — https://	www.texas.gov	/ – ." ×		
General Media Permissions Security				
Website Identity Website: www.texas.gov Owner: This website does not supply own	nership informat	tion.		
Verified by: Amazon		<u>V</u> iew Certificate		
Privacy & History Have I visited this website prior to today? Is this website storing information on my computer? Have I saved any passwords for this website?	No Yes, <u>C</u> le No	ear Cookies and Site Data		
Technical Details Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3) The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.				

143. Note that the Issuer Name is not 192.168.1.1.

Certificate

www.texas.gov	Amazon RSA 2048 M02	Amazon Root CA 1
Subject Na Common Na	me me www.texas.gov	
Issuer Na Coun	me try US	
Organizat Common Na	ion Amazon me Amazon RSA 2048 M02	

If the firewall had decrypted this website, the Issuer Name would be displayed as 192.168.1.1. Because you excluded government websites from Decryption, the firewall has not decrypted this site.

The issuer name you see may be different from the example shown here.

144. Close Firefox and any certificate windows.



Stop. This is the end of the lab.

Lab 14: Locating Valuable Information Using Logs and Reports

Having worked with the new Palo Alto Networks firewall for almost a week, you have discovered how much information the device provides about traffic that it processes. You have already worked with the Traffic, Threat, URL and System log files and learned how to create filters to locate specific information. But before you roll the firewall into production, you want to spend some time looking at some of the other resources, graphs, reports and tools that are available.

You will also need to show your colleagues where to find different kinds of information in the firewall web interface so that they can assist you in keeping your network as secure as possible.

Lab Objectives

- View threat information using the Dashboard
- View application information using the Dashboard
- View threat information using the ACC
- View application information using the ACC
- View threat information using the Threat log
- View application information using the Traffic log
- View threat information using App Scope reports
- View threat information using predefined reports
- View application information using predefined reports
- View threat and application information using custom reports

High-Level Lab Steps

Apply a Baseline configuration to the Firewall

• Load and commit the configuration file - **edu-210-11.1a-lab-14.xml** - to the Firewall

Generate Traffic

- Use the Remmina application to connect to the Server-Extranet host
- Run the traffic generating script by entering the following commands:

cd ~ <ENTER>

- ./UsingLogs-V1.sh <Enter>
- Allow the script to run uninterrupted

Display Recent Threat Information in the Dashboard

- Add the Threat Logs widget to the Dashboard
- Use the Threat Log widget to determine what threats the firewall has detected within the last hour
- Add the URL Filtering Logs widget to the Dashboard
- Use the URL Filtering Logs widget to examine URL Filtering entries written by the firewall within the last hour
- Add the Data Filtering Logs widget to the Dashboard
- Use the Data Filtering Logs widget to examine Data Filtering entries written by the firewall within the last hour

Display Recent Application Information in the Dashboard

- Add the Top Applications widget to the Dashboard
- Note which applications the firewall has detected within the last hour
- Add the Top High Risk Applications to the Dashboard
- Note which applications the firewall has detected that are considered high-risk

Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks.

View Threat Information in the ACC

- In the ACC, use the Threat Activity tab to view information for the Last 7 Days
- In the Threat Activity widget's table below the graph, click the small arrow icon next to one of the critical severity level entries to add critical severity level as a Global filter for the ACC

Note that the widget's table changes to display only threats that have a critical severity level

- In the Global Filters area, click Clear all to remove the global filter
- On the Threat Activity tab, determine what widgets you would use to see which hosts have either visited or resolved a malicious DNS domain

View Application Information in the ACC

- In the Network Activity tab of the ACC, hide the sidebar to make more room for the widgets
- In the top section of the Application Usage widget, hover your mouse pointer over the web-browsing section in the graph

Note the summary window that appears with information about web-browsing

- In the table below the graph, hover your pointer over the web-browsing application until the global filter Left arrow appears. Then click the Left arrow to promote the web-browsing application to a global filter
- Unhide the sidebar
- In the Network Activity tab, locate the Rule Usage widget and change the display to Bytes

Use the information displayed to determine which Security Policy rules have allowed webbrowsing traffic

- In the Rule Usage widget, use the Jump to Logs button to open the Traffic Log Note the log filters that have been applied automatically to the Traffic log
- Clear the filter in the Traffic log
- In the Global Filters section of the ACC tab, clear all filters

View Threat Information in the Threat Log

- In the Threat Log, clear any filters you may have in place
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	and
Attribute	Severity
Operator	greater than or equal
Value	high

This configuration filters the log to display only critical-severity and high-severity threats

- Apply the filter to the Threat Log
- Use the information from the Action column to determine how these threats have been handled by the firewall.
- Clear the existing filter
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	and
Attribute	Source User
Operator	equal
Value	chicago\escrooge

This configuration filters the log to display threats coming from only this user.

- Apply the filter to the Threat log
- Note what Threats this user has generated

You may need to add the Source User column to the Threat Log display if it is not already present

• Clear the existing filter

Note: URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You also can use filters to view these logs.

View Application Information in the Traffic Log

- In the **Traffic** Log, remove any existing log filters
- Use the Add Log Filter button to build a filter with the following characteristics:

Parameter	Value
Connector	and
Attribute	Source Zone
Operator	equal
Value	Acquisition

This configuration filters the log to display only application traffic that is sourced from the Acquisition zone.

• Apply the filter to the Traffic Log

Note that the Traffic log been filtered to display only traffic sourced from the Acquisition zone

- Use the **Add Log Filter** to modify the existing source zone filter to filter on the Users_Net zone instead of the Acquisition zone.
- Use the Add Log Filter to update the filter to include the following information:

Parameter	Value
Connector	and
Attribute	Application
Operator	equal
Value	web-browsing

• Apply the filter to the Traffic Log

Note that the Traffic log been filtered to display only web-browsing traffic sourced from the Users_Net zone

View Threats Using App Scope Reports

- Select App Scope > Threat Monitor
- Set the time frame to Last 7 days
- Set the list of entries to Top 25
- Filter the list by Source User
- Set the display to Show all threat types
- Hover your pointer over the top section of any bar on the bar chart and note the popup window that shows the threat name and number of detections

View Threat Information Using Predefined Reports

- Under Monitor > Reports, expand the list of Traffic Reports
- Select the entry for Sources
- Note the Sources report that is displayed in the web interface
- In the calendar below the report column, click various dates from the past week to see information about traffic logged by the firewall on other days

Note that days that are grayed out do not have any data available

View Application Information Using Predefined Reports

- Under Monitor > Reports, expand the list of Application Reports
- Select the entry for Applications

Note the Applications report that is displayed in the web interface

• Expand the list of URL Filtering Reports and select the entry for Web Sites Note that you may need to click different dates until you see a report with data

View Threat and Application Information Using Custom Reports

• Select **Monitor > Manage Custom Reports**, and use the following information to create a **Custom Report**:

Parameter	Value
Name	Apps Used by Internal Zones
Database	Traffic Summary
Scheduled check box	Select it
Time Frame	Last 7 Days
Sort By	Select Sessions and Top 100

Parameter	Value
Group By	Select Source Zone and 5 Groups
Selected Columns	In top-down order, select Source Zone, Application, Bytes, and Action

The report will list each internal zone along with the applications seen coming from each zone. Because only four zones are available in the lab environment, grouping of the data into a maximum of five groups is enough to display all zones. Sorting the applications list in each zone by the top 100 sessions should display all applications associated with a source zone.

• Use the Filter Builder button to create a filter with the following characteristics:

Parameter	Value
Connector	and
Attribute	Source Zone
Operator	not equal
Value	Internet

• Apply the filter

• Click **OK** to close the **Custom Report** window and to see a new entry in the list of custom reports

• Open the custom report and use **Run Now** to see report information

Note that the report provides details for applications used by the Extranet and the Acquisition zones

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. Open configuration browser and connect to firewall-a.
- 2. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 3. Click Load named configuration snapshot.
- 4. Click the drop-down list next to the **Name** text box and select **edu-210-11.1a-14.xml**.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

5. Click **OK**.

A window should open that confirms that the configuration is being loaded.

- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Click **Close** to continue.

Generate Traffic

In this section, you will generate simulated attacks, web browsing and application traffic to populate firewall logs.

- 10. On the client workstation, open the Remmina application.
- 11. Double-click the entry for **Server-Extranet**.
- 12. At the prompt, enter the following command:

./UsingLogs-V1.sh <Enter>

- 13. Press Enter again to begin the process.
- 14. Allow the script to run uninterrupted.
- 15. Minimize the Remmina application window.

Display Recent Threat Information in the Dashboard

You will use the **Dashboard** to view threats detected by the firewall in the last hour. Because you can configure the **Dashboard** to periodically refresh, the displayed threats will change, depending on the most recent information available. The **Dashboard** information is sourced from the Threat, URL Filtering, and Data Filtering logs.

- 16. In the web interface, click the **Dashboard** tab.
- 17. Click **Widgets** and select **Logs** > **Threat Logs**:

🔶 PA-VM	DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS
	Layout 3 Columns	~	Widgets 🗸	Last updated	10:54:07
General Information			Application)	>	GΧ
Device Name	firewall-a		E Logs >	Threat Log	gs
MGT IP Address	192.168.1.254			🔞 URL Filter	ing Logs
MGT Netmask	255.255.255.0			🛅 Data Filte	ring Logs
MGT Default Gateway	192.168.1.1			Config Log	gs
MGT IPv6 Address	unknown			System Lo	gs

Note that if Threat Logs is grayed out, it means that the widget is already displayed on the Dashboard.

18. Are any threats displayed in the **Threats Logs** widget? It can display the 10 most recent threats detected by the firewall in the last hour.

Depending on activity in your lab environment in the last hour, you might not see threat entries. This widget is useful for viewing only the most recent threats detected by the firewall. Here is an example:

Threat Logs		G×
Name	Severity	Time
Eicar File Detected	medium	09/19 10:32:24
Eicar File Detected	medium	09/19 10:10:19
Suspicious Domain	medium	09/19 09:58:59
Suspicious Domain	medium	09/19 09:58:59
Suspicious Domain	medium	09/19 09:58:29
Suspicious Domain	medium	09/19 09:58:29
Suspicious Domain	medium	09/19 09:58:04
Suspicious Domain	medium	09/19 09:58:04
Suspicious Domain	medium	09/19 09:57:49
Suspicious Domain	medium	09/19 09:57:49

You can use the refresh button in the upper right corner of any widget to update the displayed items. The entries you see will differ from the examples shown here.

19. Click **Widgets** and select **Logs** > **URL Filtering Logs**.

A **URL Filtering Logs** widget should appear on the **Dashboard**. Note that if URL Filtering Logs is grayed out, it means that the widget is already displayed on the Dashboard.

URL Filtering Logs		G×
URL	Category	Time
www.olj2pojack3m.com/	high-risk	09/19 10:59:09
www.gjb98p0d2b.com/	high-risk	09/19 10:59:09
www.d8o3hk29m3l3fi3age5.com/	high-risk	09/19 10:59:09
www.lni43pkbn9j670def1.com/	high-risk	09/19 10:59:09
www.155714gah09blo.com/	high-risk	09/19 10:59:09
www.0958g0la9ih4074h.com/	high-risk	09/19 10:59:09
www.eon0ph6c5am01ah.com/	high-risk	09/19 10:59:09
www.g7b535g0nc.com/	high-risk	09/19 10:59:09
www.0lmok80g049ci2.com/	high-risk	09/19 10:59:09
www.efoj41d3hepnc0a.com/	high-risk	09/19 10:59:09

You can use the refresh button in the upper right corner of any widget to update the displayed items. The threats you see will differ from the examples shown here.

20. Are any URLs displayed in the **URL Filtering Logs** widget? It can display the 10 most recent URLs seen by the firewall in the last hour.

Depending on activity in your lab environment in the last hour, you might see URL entries. This widget is useful for viewing only the most recent URLs seen by the firewall.

21. Click **Widgets** and select **Logs** > **Data Filtering Logs**.

A **Data Logs** widget should appear on the **Dashboard**. Note that if Data Filtering Logs is grayed out, it means that the widget is already displayed on the Dashboard.

Data Logs		G×
File Name	Name	Time
c	US-SSNs	09/19 10:45:29
application2.js	US-SSNs	09/19 10:45:29
tiles	US-SSNs	09/19 10:45:14
threatListUpdates:fetch	Unknown Binary File	09/19 10:45:14
tiles	US-SSNs	09/19 10:32:49
segment0.ts	US-SSNs	09/19 10:31:09
segment0.ts	US-SSNs	09/19 10:30:59
segment0.ts	US-SSNs	09/19 10:30:49
segment0.ts	US-SSNs	09/19 10:30:39
segment0.ts	US-SSNs	09/19 10:30:34

The entries you see will differ from the examples shown here.

22. Are any files displayed in the **Data Logs** widget? It can display the 10 most recent files detected by the firewall in the last hour.

Depending on activity in your lab environment in the last hour, you might not see file entries. This widget is useful for viewing only the most recent file transfers seen by the firewall.

Display Recent Application Information in the Dashboard

In this section, you will display the **Dashboard** and view applications identified by the firewall in the last hour. Because you can configure the **Dashboard** to periodically refresh, the displayed applications will change depending on the most recent information available. You also will use the **Dashboard** to display those applications identified by the firewall in the last hour that have the most risk associated with them.

- 23. In the web interface, click the **Dashboard** tab.
- 24. Click **Widgets** and select **Application > Top Applications**. A **Top Applications** widget should appear on the **Dashboard**.
- 25. Look at the applications displayed in the **Top Applications** widget. It displays the applications seen by the firewall in the last hour.

Some applications should be listed because some "housekeeping" traffic nearly always traverses the network, even in the lab environment. This widget is useful for viewing only the recent application traffic seen in the last hour by the firewall. Here is an example:



The information you see will differ from the examples shown here.

26. Click Widgets and select Application > Top High Risk Applications.

A **Top High Risk Applications** widget should appear on the Dashboard.

27. Notice the applications displayed in the **Top High Risk Applications** widget. It displays the high-risk applications seen by the firewall in the last hour.

Some applications should be listed because some "housekeeping" traffic nearly always traverses the network. This widget is useful for quickly viewing only the recent application traffic seen by the firewall in the last hour. Here is an example:



Applications with a risk level of 4 are shown in orange. Applications with a risk level of 5 are shown in red. These rankings come from Palo Alto Networks. The information you see will differ from the examples shown here.

View Threat Information in the ACC

In this section, you will view a few ACC widgets on the **Threat Activity** tab to become familiar with widgets that display threats against your environment. Spend time examining each widget so that you can determine which information is presented that might be most useful to you back in your environment.

28. In the web interface, click the ACC tab.
29. On the left side of the ACC page, look at **Global Filters** for any configured global filters. If there are filters, click **Clear all**:



30. Click the **Threat Activity** tab:

Network Activity	Threat Activity 🧷	Blocked Activity Tunnel Activity GlobalProtect Activity SSL Activity 🕂
)

31. On the left side of the ACC window, click the Time drop-down menu and select Last 7 Days. This value configures all the widgets to display threat information for the last seven days:

Time	
Last 7 Days	\sim

32. Do you see any threats listed in the Threat Activity widget?

You should see some combination of flood, scan, spyware, packet, vulnerability, and virus threats displayed in a graph. Next to each entry should be the number of occurrences of these threat types that the firewall has seen in the last seven days. More detail about the threats should be displayed in a table below the graph:



The entries you see will differ from the examples shown here.

33. In the **Threat Activity** widget's table below the graph, click the small arrow icon next to one of the **critical** severity level entries.

THREAT NAME	ID	SEVERITY	THREAT TYPE
Eicar File Detected	39040	medium	vulnerability
TrickBot TLS Fingerprint Detection	85331	critical 🗧	 spyware
Trojan.yakes:afroamericanec.bit	209627145	medium	Global
malicious-domains-edl	12000000	medium Filte	er
generic:31.smokemenowhhalala.bit	188290431	high	spyware
Eicar Test File	100000	medium	virus
Malicious Windows Executable	599800	medium	ml-virus
generic:mustardcafeonline.com	318388689	medium	spyware
generic:click.clickanalytics208.com	295864113	medium	spyware
Bredolab.Gen Command and Control Traffic	13024	critical	spyware

This action adds the critical severity level as a Global filter for the ACC. Global filters are applied to every widget on the ACC. Global filters are useful for quickly pivoting your search on a specific piece of information, thus causing all widgets to display only information that is relevant to a specific object or threat.

34. Did the widget's table change to display only threats that have a **critical** severity level?

The widget should have changed to display only critical severity level threats. The graph will also change to display only threats that match the filter.

- 35. Find the global filter on the left side of the **ACC** window.
- 36. Was **critical** added as a global filter condition?





You should see a global filter for critical.

37. Note that the Threat Activity graph and the table of Threat Names are updated to reflect only items with a Severity level of Critical.



The entries you see will differ from the examples shown here.

38. In the Global Filters area, click Clear all to remove the global filter.

The global filter should be removed, and all widgets should be refreshed to include all threats detected in the last seven days.

39. On the **Threat Activity** tab, which widgets would you use to see which hosts have either visited or resolved a malicious DNS domain? Make a guess based on the widget names.

The answer is: Hosts Visiting Malicious URLs and Hosts Resolving Malicious Domains.

View Application Information in the ACC

In this section, you will view two widgets on the **Network Activity** tab. The goal is for you to gain familiarity with some of the widgets available for viewing application and traffic information.

40. In the web interface, click the ACC tab and then the Network Activity tab.

41. Hide the sidebar to make more room for the widgets by clicking the very small arrow shown:



42. Resize the **Application** column to display the entries:

APPLICATION	RISK	BYTES	SESS
not-applicable	1	0	
dns	3	37.0M	35.7
ssl	4	179.0M	1.2
web-browsing	4	50.0M	1.5
smtp	5	23.0k	

43. The top section of the **Application Usage** widget is a graph that illustrates how much of the traffic a specific application represents:

Application Usage		
• bytes • sessions • threats	⊖ content ⊖ URLs ⊖ users ⊖ profil	es 📴 🖄
Application Categories business-systems	general-internet	networking
paloalto-updates	rpan-dweb-browsing	g. ssl
	paloa paloa	infrastructure
	auth	dns unknown unknown

Think of this as a sort of square pie-chart. The entries you see will differ from the examples shown here.

44. Hover your pointer over the section for **web-browsing**.



This action displays a summary window with information about that application. The information you see will differ from the examples shown here.

45. In the table below the graph, hover your pointer over the **web-browsing** application until the global filter **Left arrow** appears. Then click the **Left arrow** to promote the **web-browsing** application to a global filter:



46. Unhide the sidebar by clicking the tiny arrow again:



47. Scroll down in the Network Activity tab until you reach the Rule Usage widget.



48. Select the radio button at the top for **Bytes**.

The entries you see will differ from the examples shown here.

49. Which Security Policy rules have allowed web-browsing traffic?

The widget should display only those rules that have allowed web-browsing traffic in the last seven days because the widget is filtered by the web-browsing application in the global filter and the ACC time range setting.

50. In the upper right corner of the **Rule Usage** widget, click the **Jump to Logs** button and select **Traffic Log** icon to open the logs menu.



51. Which log is displayed in the web interface?

It should be the Traffic log.

52. Which log filters have been applied automatically to the Traffic log?

Q ((receive_time geq '2024/09/12 11:00:00') AND (receive_time leq '2024/09/19 10:59:59') AND ((app eq web-browsing))

There should be a time range filter and an application filter for web-browsing. The time range filter is derived from the time specified in the ACC. The entry you see will differ from the example shown here.

53. Note that the entries displayed in the Traffic log match the filter:

Q (re	Q (receive_time geq '2020/07/02 21:15:00') AND (receive_time leq '2020/07/09 21:14:59') AND ((app eq web-browsing))							
	SESSION END REASON	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	то
R	tcp-fin	07/09 21:05:51	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot	104.92.118.21	80
<mark>ا</mark>	tcp-rst-from- server	07/09 21:05:51	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot	96.17.134.15	80
R	tcp-rst-from- server	07/09 21:05:50	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot	96.17.134.15	80
B	tcp-rst-from- server	07/09 21:05:50	Acquisition	Acquisition	192.168.1.22	chicago\hpoirot	96.17.134.15	80
	tcp-rst-from-	07/09 21:05:50	Acquisition	Acquisition	192 168 1 22	chicago\bnoirot	96 17 134 15	80

Note that several columns have been hidden or rearranged in the example shown here.

- 54. Clear the filter in the Traffic log.
- 55. Click the ACC tab.
- 56. In the Global Filters area, click Clear all to remove the global filter:

Global Filters	
⊕ ~ ⊖	Clear all

View Threat Information in the Threat Log

In this section, you will apply different filters to the Threat log. You will use the filters to determine whether all critical-severity and high-severity threats detected by the firewall have been blocked. You also will use a log filter to determine which detected threats come from a specific security zone.

- 57. In the web interface, select **Monitor > Logs > Threat**.
- 58. In the upper right corner of the window, click the **X** icon in the filter area to remove any existing log filter:



59. Click the + icon in the filter area to open the **Add Log Filter** window:

Commit ~	È ⊬∄× Q
Manual	G 🕐
\longrightarrow	🕀 🖏 🖓 🖻
	Add Filter

The Add Log Filter window should open.

60. In the Add Log Filter window, select the following:

Parameter	Value
Connector	and
Attribute	Severity
Operator	greater than or equal
Value	high

This configuration filters the log to display only critical- and high-severity threats.



61. Click Add to add the in-progress filter to the top pane of the Add Log Filter's window:



The **Add Log Filter** window should close.



As you become more familiar with filter syntax, you can simply type the filter directly into the filter field and forego using the filter builder.

63. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log:



64. Has the Threat log been filtered to display only threats of high severity or greater?

It should be filtered. You can scan the **Action** column to determine how the threats have been handled by the firewall. You could, for example, use this information to help you determine the Security Profile configuration required to control threats found in legitimate traffic.

Q (severity geq high)							
RECEIVE TIME	SEVERITY	ТҮРЕ	THREAT ID/NAME	TO ZONE	DESTINATION ADDRESS	ACTION	
07/09 21:05:38	critical	spyware	Ursnif.Trojan Command and Control Traffic	Acquisition	144.168.95.105	reset- both	
07/09 21:05:37	high	spyware	generic:aplatmes	Acquisition	172.21.169.77	drop- packet	
07/09 21:05:35	high	spyware	generic:teomeng	Acquisition	172.21.169.77	drop- packet	
07/09 21:05:35	critical	spyware	DeepPanda.Gen Command And Control Traffic	Acquisition	172.17.124.171	reset- both	
07/09 21:05:31	critical	vulnerabil	Terror Exploit Kit	Acquisition	159,203,185,4	reset-	

Note that several columns have been hidden or rearranged in the example shown here. The entries you see will differ from the ones shown here.

65. Click the **X** icon in the filter area to remove any existing log filter:



- 66. Click the + icon in the filter area to re-open the **Add Log Filter** window.
- 67. In the Add Log Filter window, select the following:

Parameter	Value
Connector	and
Attribute	Source User
Operator	equal
Value	chicago\escrooge

This configuration filters the log to display threats coming from only this user.



68. Click Add and then click Apply to add the filter to the Threat log filter text box.

The **Add Log Filter** window should close, and the filter should have been added to the Threat log's filter text box.



- 69. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Threat log.
- 70. Has the Threat log been filtered to display only threats coming from the specified user? You may need to add the Source User column to the Threat Log display if it is not already present.

(user.src eq 'chicago\escrooge')							
RECEIVE TIME	SEVERITY	ТҮРЕ	THREAT ID/NAME	TO ZONE	SOURCE USER	DESTINATION ADDRESS	ACTION
07/09 21:05:09	informational	vulnerabil	Non-RFC Compliant SMTP Traffic on Port 25	Acquisition	chicago\escrooge	66.218.85.52	alert
07/09 21:05:06	high	spyware	generic:31.smok	Acquisition	chicago\escrooge	107.161.16.236	drop
07/09 21:05:06	high	spyware	generic:31.smok	Acquisition	chicago\escrooge	10.11.1.1	drop
07/09 21:04:53	high	spyware	generic:31.smok	Acquisition	chicago\escrooge	107.161.16.236	drop
07/09 21:04:53	high	spyware	generic:31.smok	Acquisition	chicago\escrooge	10.11.1.1	drop
07/09 21:04:49	critical	spyware	Lethic.Gen Command And Control Traffic	Acquisition	chicago\escrooge	89.248.174.17	reset- both

Note that several columns have been hidden or rearranged in the example shown here. If you do not see any entries, wait a few moments and click the refresh button to update the Threat Log table.

71. Click the **X** icon to clear the filter from the log filter text box.

Note: URL Filtering, WildFire Submissions, and Data Filtering logs are available to display traffic and threats detected by the firewall but are not shown in this section. You can also use filters to view these logs.

View Application Information in the Traffic Log

In this section, you will apply different filters to the Traffic log. You will use a filter to determine which applications are being seen in a specific zone.

- 72. In the web interface, select **Monitor** > **Logs** > **Traffic**.
- 73. Click the **X** icon in the filter area to remove any existing log filter
- 74. Click the + icon in the filter area to open the **Add Log Filter** window: The **Add Log Filter** window should open.

Parameter	Value
Connector	and
Attribute	Source Zone
Operator	equal
Value	Acquisition

75. In the **Add Log Filter** window, select the following:

This configuration filters the log to display only application traffic that is sourced from the Acquisition zone. You could use this information, for example, to help you to determine how to configure your Security Policy rules. You easily could modify the filter to display application traffic sourced from any zone and use that information to help you improve your Security Policy configuration.



76. Click **Add** and then click **Apply** to add the filter to the Traffic log filter text box. The **Add Log Filter** window should close.



- 77. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Traffic log
- 78. Has the Traffic log been filtered to display only traffic sourced from the Acquisition zone?

It should be. You could use this information to help you determine the Security Policy rules required to control legitimate traffic sourced from devices in the Acquisition zone.

Q (zon	Q (Izone.src eq Acquisition)								
	SESSION END REASON	RECEIVE TIME	FROM ZONE	SOURCE	SOURCE USER	DESTINATION			
R	aged-out	07/09 21:38:07	Acquisition	10.0.0.10		10.0.0.255			
R	aged-out	07/09 21:30:42	Acquisition	10.9.3.101	chicago\aoakley	10.9.3.8			
R	aged-out	07/09 21:30:42	Acquisition	10.9.3.101	chicago\aoakley	10.9.3.8			
R	aged-out	07/09 21:30:41	Acquisition	10.9.3.101	chicago\aoakley	10.9.3.8			
R	aged-out	07/09 21:26:07	Acquisition	10.0.0.10		10.0.0.255			
E	aged-out	07/09 21:14:07	Acquisition	10.0.0.10		10.0.0.255			

Note that several columns have been hidden or rearranged in the example shown here.

- 79. Click the + icon in the filter area to again open the Add Log Filter window. The Acquisition source zone filter still should appear in the open Add Log Filter window.
- 80. In the **Add Log Filter** window in the top pane, modify the existing source zone filter to filter on the Users_Net zone instead of the Acquisition zone. The completed filter should read (zone.src eq Users_Net):

Add Log Filter

(zone.src eq Users_Net)

81. In the Add Log Filter window, also add the following selections:

Parameter	Value
Connector	and
Attribute	Application
Operator	equal
Value	web-browsing



82. Click **Add** and then click **Apply** to add the filter to the Traffic log filter text box. The **Add Log Filter** window should close.



- 83. With the filter string in the log filter text box, click the **right arrow** icon to apply the filter to the Traffic log.
- 84. Has the Traffic log been filtered to display only web-browsing traffic sourced from the Users_Net zone?

It should be filtered.

Q	Q (zone.src eq Users_Net) and (app eq web-browsing)							
REC	EIVE TIME	FROM ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATIO	ACTION
07/0	09 21:47:14	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:47:14	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:42:13	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:42:13	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:37:12	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:37:12	Users_Net	192.168.1.254		192.168.50.80	80	web-browsing	allow
07/0	09 21:35:11	Users_Net	192.168.1.254		199.167.52.141	443	web-browsing	allow

Note that several columns have been hidden or rearranged in the example shown here.

85. Click the \mathbf{X} icon to clear the filter from the log filter text box.

View Threats Using App Scope Reports

In this section, you will view threat information using App Scope's Threat Monitor and Threat Map reports.

86. In the web interface, select **Monitor > App Scope > Threat Monitor**.



87. At the bottom of the window, click Last 7 days:



88. The window should update to display the top 10 threats detected by the firewall in the last seven days.



Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days

Note that the image you see will differ from the example shown here.

89. At the top of the window, click **Top 10** and select **Top 25** from the menu:



This configuration enables you to see the top 25 threats within the selected time range.

90. At the top of the window, click Threat and choose Source User:



91. At the top of the window, hover your pointer over each **Filter** icon to see how to display specific types of threats:



- 92. Select Show all threat types.
- 93. Hover your pointer over the top section of any bar on the bar chart. What appears on the page?

<u>h</u>	Top 25	🗸 🥖 Source User 🗸	Filter 🗵 🔋 🖧	🛛 🕕 🔒 Export: 🕻	🚠 🕰		101	≋
	400						_	
SUC	300							
Sessic	200					[Thu chicago\tsawyer: 140 Total: 341]
1	100					Ĺ		_
	0	Fri	Sat	Sun Mon	Tue	Wed	Thu	
		chicago\tsawyer chicago\drjekyll chicago\aoakley	chicago\es chicago\rcr	crooge chica usoe chicago	go\mrhyde ch \jcaesar chica	nicago\wearp ago\sholmes		

You should see a popup window that shows the threat name and number of detections.

The information you see may differ from the example here.

View Threat Information Using Predefined Reports

In this section, you will open and view three of the more than 40 predefined reports available on the firewall. Your efficient use of the predefined reports depends on your spending time with each report, discovering and determining which information might be useful to you in your own environment. Your familiarity with the reports will help you to find the reports that are most useful to you.

- 94. In the web interface, select **Monitor > Reports**.
- 95. Click Traffic Reports to expand the list of available Traffic Reports:



96. Click **Sources** to view a report.

A Sources report should be displayed in the web interface. The report displays which source IP addresses were detected by your firewall on the previous day. It should have a format like the following example, but your data may be different.

Note: Reports are generated by the firewall each morning at 2 am. Your lab firewall might not show any reports because it was not running at this time. This also applies to the next step 97.

	SOURCE ADDRESS	SOURCE HOST NAME	SOU EDL	SO USER	SOURCE DYNAMIC ADDRESS GROUP	BYTES	SESSIONS
1	192.168.50.1	192.168.50.1				10.8M 🔲	48.6k
2	192.168.50.150	192.168.50.150				14.3M 🔲	11.4k
3	192.168.1.20	192.168.1.20				12.6M 🔲	9.3k 🛄
4	192.168.1.25	192.168.1.25				2.5M	5.4k 🛄
5	192.168.1.254	192.168.1.254				l41.2M	1.4k 🛙
6	192.168.50.14	192.168.50.14				59.7k	110
7	192.168.50.53	192.168.50.53				59.7k	110
8	192,168,50,25	100 140 50 255				59 7L	110

97. In the calendar below the report column, click various dates from the past week to see information about traffic logged by the firewall on other days:

<	December 2022 ~ >								
s	м	т	w	т	F	s			
27	28	29	30	1	2	3			
4	5	6	7	8	9	10			
11	12	13	14	15	16	17			
18	19	20	21	22	23	24			
25	26	27	28	29	30	31			
1	2	3	4	5	6	7			

Note that days that are grayed out do not have any data available.

View Application Information Using Predefined Reports

In this section, you will view reports related to Applications.

- 98. In the web interface, select **Monitor > Reports**.
- 99. Click **Application Reports** to expand the list of available application reports:

Application Reports — Image: Applications Image: Applications Image: Application Categories Image: Application Categories Image: Application Categories Image: Applications Image: Application Categories Image: Applications Image: Application Categories Image: Applications Image: Application Categories Image: Application Categories</t

100. Click **Applications** to view the Applications report.

An **Applications** report should be displayed in the web interface. The report displays the applications that were detected by your firewall on the previous day. It should have a format like the following example, but your application data will be different. You can use this information to update your Security Policy rules, as necessary.

Note: Reports are generated by the firewall each morning at 2 am. Your lab firewall might not show any reports because it was not running at this time. This also applies to the next step 97.

101. Click **URL Filtering Reports** to expand the list of available URL Filtering reports:



102. Click Web Sites to view the report. Click each date until you see a report with data.

A **Web Sites** report should be displayed in the web interface. The report displays the websites that were seen by your firewall on a given day. It should have a format like the following example, but your data will be different. You can use this information to update your Security Policy rules or a URL Filtering Profile, as necessary.

Note: Reports are generated by the firewall each morning at 2 am. Your lab firewall might not show any reports because it was not running at this time. This also applies to the next step 97.

	URL DOMAIN	CATEGORY	COUNT
1	www.amazon.com	shopping	29
2	www.hackthissite.org	hacking	28
3	www.taobao.com	shopping	20
4	www.tmall.com	shopping	20
5	global.jd.com	shopping	20
6	www.aliexpress.com	shopping	20
7	shodan.io	hacking	11
8	www.shutterfly.com	shopping	10

View Threat and Application Information Using Custom Reports

In this section, you will create a custom report. The custom reports feature enables you to build reports that include only the information that you consider useful in your environment. The first custom report will list the applications that the firewall has detected in each of your internal security zones. The second custom report will list the applications that the firewall has detected in the outside zone, which in the lab environment is associated with the internet. Such information can help you to improve the configuration of your Security policies and ultimately improve your security stance.

103. In the web interface, select **Monitor > Manage Custom Reports**.

Parameter	Value
Name	Apps Used by Internal Zones
Database	Traffic Summary
Scheduled box	Checked
Time Frame	Last 7 Days
Sort By	Select Sessions and Top 100
Group By	Select Source Zone and 5 Groups
Selected Columns	In top-down order, select Source Zone, Application, Bytes, and Action

104. Click Add and configure the following in the Custom Report window:

The report will list each internal zone along with the applications seen coming from each zone. Because only four zones are available in the lab environment, grouping of the data into a maximum of five groups is enough to display all zones. Sorting the applications list in each zone by the top 100 sessions should display all applications associated with a source zone.

Custom Report								? 🗆	
Report Setting									
Cal Load Template	ightarrow Run Now								
Name	Apps Used by Internal Zones		Available Columns			Selected Columns			
Description				App Category	-		Source Zone		
Database	Traffic Summary		~	App Container	- 1	Ð	Application		
	Scheduled			App Sub Category		Θ	Bytes		
Time Frame	Last 7 Days		\sim	App Technology			Action		
Sort By	Sessions 🗸	Top 100	~	Apps	-				
Group By	Source Zone	5 Groups	~		ΤŤ	ор	† Up ↓ Down	↓ Bottom	

105. In the bottom right corner of the Custom Report window, click the Filter Builder link:

	Filter Builder
ОК	Cancel

The Add Log Filter window should open.

106. Configure the following:

Parameter	Value
Connector	and
Attribute	Source Zone
Operator	not equal
Value	Internet

Add Log Filter			0
Please type (or) add a filter	using the filter builder		
Connector	Attribute	Operator	Value
and	Source Vendor	equal	Internet
or	Source Zone	not equal	
	Technology		
	Tunnel ID		
	Tunnel Type		
Negate	Zone	- C	•
		(Add Apply Close

107. In the Add Log Filter window, click Add and then Apply.

A filter should be added to the custom report. The Internet zone is outside of your network, and this filter ensures that the custom report does not include applications that are coming from outside your network.



108. Click **OK** to close the **Custom Report** window.

The new custom report should be added to the list of custom reports in the web interface.

NAME	DESCRIPTION	DATABASE	TIME FRAME	ROWS	SORT BY	GROUP BY	SCHEDULED
Apps Used by Internal Zones		Traffic Summary	Last 7 Days	100	Sessions	from	 Image: A set of the set of the

109. Click Apps Used by Internal Zones to open the custom report.

110. Click **Run Now** to run the custom report:

ightarrow Run Now
Apps Used by Internal Zones

The report should run, and the results should be displayed in a tab that is added and opened in the **Custom Report** window.

111. View the results of the custom report.

You can scroll down through the report to see information about the Extranet and the Acquisition zones along with details about the applications that the firewall processed in each one. Note that the entries you see in the report may differ from the example shown here.

Report Setting Apps Used by Internal Zones (100%)							
	SOURCE ZONE	APPLICATION	ACTION		BYTES		
1	Acquisition	ssl	allow	122.1M 🔋			
2		web-browsing	allow	50.4M			
3	3	google-base	allow	3.8M			
4		dns	allow	644.0k			
5		twitter-base	allow	4.8M			
6		web-browsing	block-url	0			
7		netbios-dg	allow	190.7k			
8		facebook-base	allow	2.1M			
9		ssl	block-url	0			

Custom Report

Ensure that you explore all pages of the report, as other zones may be listed on subsequent pages.

112. When you are finished viewing the report, close it by clicking the **X** on the **Apps Used by Internal Zones (100%)** tab:

Custo	m Report		
Report	t Setting App	os Used by Internal Zone	s (100%) 🔀
	SOURCE ZONE	APPLICATION	ACTION
1	Acquisition	ssl	allow

113. Click **Cancel** to close the **Custom Report** window.



Stop. This is the end of the lab.

Lab 15: Capstone

This comprehensive lab is meant to provide you with additional hands-on firewall experience and to enable you to test your new knowledge and skills. You can refer to your student guide and previous lab exercises.

In this scenario, you are a network administrator and recently received a new Palo Alto Networks VM-Series firewall. The firewall's management IP address is 192.168.1.254. You can log in with the username **admin** and **Pal0Alt0!** as the password. Take special care to use the exact spelling and capitalization for the items you are asked to configure.

You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.



Load a Lab configuration

- 1. In the web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot:
- 3. Select edu-210-11.1a-Capstone-start.xml and click OK.
- 4. Click **Close**.
- 5. Commit all changes.

Configure Networking

Complete the following objectives:

- Configure three firewall interfaces using the following values:
 - Ethernet 1/1: 203.0.113.20/24 Layer 3
 - Ethernet 1/2: 192.168.1.1/24 Layer 3
 - Ethernet 1/3: 192.168.50.1/24 Layer 3
- Create a logical router called **LR-1** for all configured firewall interfaces.
- Create a default route for the firewall called **Default-Route**
- Create an Interface Management Profile called Allow-ping that allows ping
- Assign the Allow-ping Interface Management Profile to ethernet1/2

Configure Security Zones

Complete the following objectives:

- Create a **Security Zone** called **Internet** and assign **ethernet1/1** to the zone
- Create a Security Zone called Users and assign ethernet1/2 to the zone:
 - Configure the **Users** zone for User-ID
- Create a **Security Zone** called **Extranet** and assign **ethernet1/3** to the zone

Verify network connectivity from the firewall to other hosts.

- Your internal host can ping **192.168.1.1** and receive a response
- From the firewall CLI, the following commands are successful:
 - ping source 203.0.113.20 host 203.0.113.1
 - ping source 203.0.113.20 host 8.8.8.8
 - ping source 192.168.1.1 host 192.168.1.20
 - ping source 192.168.50.1 host 192.168.50.150

Configure NAT Policy Rules

Create Source NAT rules to meet the following requirements:

- Rule Name = Users_to_Internet
 - From Source Zone Users to Destination Zone Internet
 - Use **ethernet1/1** on the firewall as the source translation address
- Rule Name = Extranet_to_Internet
 - From Source Zone Extranet to Destination Zone Internet
 - Use **ethernet1/1** on the firewall as the source translation address
- All NAT rules must include a helpful Description

Configure Security Policy Rules

Create Security Policy rules to meet the following requirements:

- For all Security Policy rules, enter a helpful **Description**.
- Modify the **interzone-default** Security Policy rule so that traffic is logged at session end.
- Create a Security Policy rule called **Block_Bad_URLs** with the following characteristics:
 - For all outbound traffic, the URL categories **hacking**, **phishing**, **malware**, and **unknown** must be **blocked** by a Security Policy rule match criterion.
- From the User zone to the Extranet zone, create a Security Policy rule called Users_to_Extranet to allow the following applications:
 - ping
 - ssl
 - ssh
 - dns
 - web-browsing
- From the User zone to the Internet zone, create a Security Policy rule called **Users_to_Internet** to allow the following applications:
 - ping
 - dns
 - web-browsing
 - ssl
- From the Extranet zone to the Internet zone, create a Security Policy rule called **Extranet_to_Internet** to allow the following applications:
 - ping
 - dns

- web-browsing
- ssl

You can consider this objective complete when the following tests are successful:

- The client host can **ping 8.8.8.8** and **google.com**
- The client host can access www.paloaltonetworks.com
- The client host can browse to the Extranet web server at http://192.168.50.80
- The client host can use **SSH** to access the Extranet host at **192.168.50.150** using the login name **paloalto42** and the password **Pal0Alt0**!
- The Extranet host can **ping 8.8.8.8** and **google.com**
- The internal host cannot access hacker9.com
- The firewall blocks attempts to download a test virus file using the URL: http://192.168.50.80/eicar.com

Create and Apply Security Profiles

Create Security Profiles and a Security Profile Group to meet the following requirements:

• A Corporate **URL Filtering Security Profile** called **Corp-URL** to log access to all web categories

You can use the existing default Profile as the basis for your own

• A Corporate **File Blocking Security Profile** called **Corp-FB** to block dangerous file types

You can use the existing strict Profile as the basis for your own

- A Corporate Antivirus Security Profile called Corp-AV to block virues You can use the existing default Profile as the basis for your own
- A Corporate Anti-Spyware Security Profile called Corp-AS to block spyware You can use the existing strict Profile as the basis for your own
- A Corporate Vulnerability Protection Security Profile called Corp-Vuln to block vulnerabilities

You can use the existing strict Profile as the basis for your own

• A Corporate **WildFire Profile** called **Corp-WF** to send all file types to the public cloud for inspection

You can use the existing default Profile as the basis for your own

• Create a **Security Profile Group** called **Corp-Profiles** and assign the appropriate Security Profiles to it

Note: You can leave the Data Filtering Profile set to None.

• Apply the **Corp-Profiles Group** to all applicable Security Policy rules

You can consider this objective complete when the following tests are successful:

- The internal host cannot download a test virus file from http://192.168.50.80/eicar.com using HTTP.
- The internal host cannot download the **badtarfile.tar** from http://192.168.50.80/badtarfile.tar
- A URL log file entry appears when the client host browses to https://www.paloaltonetworks.com

Solutions

You can use the following screenshots to determine how to accomplish the requirements for this lab. You are encouraged to attempt meeting the requirements BEFORE you use these screenshots.

Firewall Interfaces

Network > Interfaces > Ethernet

Ethernet VLAN Loopback Tunnel SD-WAN								
Q								
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS				
ethernet1/1	Layer3		[]	203.0.113.20/24				
ethernet1/2	Layer3		m	192.168.1.1/24				
ethernet1/3	Layer3			192.168.50.1/24				
			_					

Logical Router

Network > Routing > Logical Routers

Logical Router - LR-1							
General	Name LR-1						
Static	Interface Administrative Distances						
OSPF							
OSPFv3	INTERFACE ^						
RIPv2	ethernet1/1						
BGP	ethernet1/2						
Multicast	ethernet1/3						
Multicast							

Firewall Default Route

Network > Routing > Logical Routers > LR-1 > Static

Logical Router - LR-1								
General	ID							
Static	_							
OSPF	Q							
OSPFv3					Nex	t Hop		
RIPv2								
BGP		NAME	DESTINATION	INTERFACE	TYPE	VALUE	DISTAN	
Multicast		Default-Route-ipv4-unicast	0.0.0/0	ethernet1/1	ip-address	203.0.113.1		

Allow-ping Interface Management Profile

Network > Network Profiles > Interface Mgmt

NAME	PING	TELNET	SSH	H.
Allow-ping				

Allow-ping Interface Management Profile Assigned to ethernet1/2

Network > Interfaces > Ethernet > ethernet1/2 > Advanced

Ethernet VLAN Loopback Tunnel SD-WAN								
Q								
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS				
ethernet1/1	Layer3		m	203.0.113.20/24				
ethernet1/2	Layer3	Allow-ping	m	192.168.1.1/24				
ethernet1/3	Layer3		[]	192.168.50.1/24				
			_					

Security Zones

Network > Zones

							User-ID
NAME	ТҮРЕ	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS
Extranet	layer3	ethernet1/3		 Image: A set of the set of the			any
Internet	layer3	ethernet1/1					any
Users	layer3	ethernet1/2		×		×	any

NAT Policy Rules

Policies > NAT

		Original Packet				Translated Packet		
	NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE TRANSLATION	DESTINATION TRANSLATION	
1	Users_to_Internet	Musers 🗠	Market Internet	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none	
2	Extranet_to_Internet	थ Extranet	Market Internet	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none	

Security Policy Rules

Policies > Security

			Source	Destination			
	NAME	ACTION	ZONE	ZONE	URL CATEGORY	APPLICATION	PROFILE
1	Block_Bad_URLs	O Deny	🚧 Extranet	Magnet Internet	hacking	any	none
			🚧 Users		malware		
					phishing		
					unknown		
2	Users_to_Extranet	⊘ Allow	🚧 Users	🞮 Extranet	any	🖽 dns	6
						III ping	
						ssh ssh	
						≣ ssl	
						web-browsing	
3	Users_to_Internet	⊘ Allow	🚧 Users	Mainternet	any	📰 dns	6
						i ping	
						≣ ssl	
						web-browsing	
4	Extranet_to_Internet	⊘ Allow	🚧 Extranet	Mainternet	any	⊞ dns	6
1						i ping	
						≣ ssl	
						web-browsing	
5	intrazone-default	⊘ Allow	any	(intrazone)	any	any	none
6	interzone-default	O Deny	any	any	any	any	none

			Source	Destination				
	NAME	ACTION	ZONE	ZONE	URL CATEGORY	APPLICATION	PROFILE	OPTIONS
5	intrazone-default	⊘ Allow	any	(intrazone)	any	any	none	none
• 6	interzone-default	O Deny	any	any	any	any	none Traffic I	og sent at session end
Security Profiles

Objects > Security Profiles

• Corporate URL Filtering Profile

NAME \land	SITE ACCESS
Corp-URL	Allow Categories (0)
	Alert Categories (77)
	Continue Categories (0)
	Block Categories (0)
	Override Categories (0)

• Corporate File Blocking Profile

NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
Corp-FB	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
	Log all other file types	any	any	both	alert

• Corporate Antivirus Profile

					Deco	oders	
	NAME LOCATION CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION		
	Corp-AV		http	default (reset- both)	default (reset- both)	default (reset- both)	
			http2	default (reset- both)	default (reset- both)	default (reset- both)	
			smtp	default (alert)	default (alert)	default (alert)	
				imap	default (alert)	default (alert)	default (alert)
				pop3	default (alert)	default (alert)	default (alert)
				ftp	default (reset- both)	default (reset- both)	default (reset- both)
				smb	default (reset- both)	default (reset- both)	default (reset- both)

• Corporate Anti-Spyware Profile

	NAME 🗸	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
	Corp-AS	Policies: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple- informational	any	informational	default	disable
			simple-low	any	low	default	disable

• Corporate Vulnerability Profile

	NAME	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE	
	Corp- Vuln	Rules: 10	simple-client- critical	any	client	critical	reset-both	disable	
			simple-client-high	any	client	high	reset-both	disable	
		simple-client- medium	any	client	medium	reset-both	disable		
				simple-client- informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable	
			simple-server- critical	any	server	critical	reset-both	disable	
			simple-server-high	any	server	high	reset-both	disable	
			more						

• Corporate WildFire Profile

NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
Corp-Wildfire	default	any	any	both	public-cloud

• Security Profile Group

Security Profile Group		?
Name	Corp-Profiles	
Antivirus Profile	Corp-AV	\sim
Anti-Spyware Profile	Corp-AS	\sim
Vulnerability Protection Profile	Corp-Vuln	\sim
URL Filtering Profile	Corp-URL	\sim
File Blocking Profile	Corp-FB	~
Data Filtering Profile	None	~
WildFire Analysis Profile	Corp-Wildfire	\sim

Cancel

• Security Policy rules with Profile Group

Policies > Security > [Rule] > Actions

Profile Setting	
Profile	Type Group
Group Profile	Corp-Profile-Group



Stop. This is the end of the lab.

Bonus Lab

In this lab, you will create a new API certificate on the firewall. This certificate can then be used to eliminate the API KeyGen warning message you receive when committing a configuration.

Lab Objectives

• Modify the firewall Authentication Settings to use a new API Key Certificate

Detailed Lab Steps

Apply a Baseline configuration to the Firewall

To start this lab exercise, load a preconfigured firewall configuration file.

- 1. Open configuration browser and connect to firewall-a.
- 2. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 3. Click Load named configuration snapshot.
- 4. Click the drop-down list next to the **Name** text box and select **edu-210-11.1a-Capstone-end.xml**.



Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

5. Click OK.

A window should open that confirms that the configuration is being loaded.

- 6. Click Close.
- 7. Click the **Commit** link at the upper right of the web interface:
- 8. Click **Commit** again and wait until the commit process is complete.
- 9. Note the error message you receive regarding the API KeyGen algorithm:

Commit S	tatus
Operation	Commit
Status	Active
Result	: Pending
Progress	55%
Details	i
Commit	
The latest AP more secure a set devicecor	² I KeyGen was executed on Mon Oct 16 13:44:22 2023 with the deprecated algorithm. You are advised to configure the API key infrastructure by web interface: Setup -> Management -> Authentiation Settings -> API Key Certificate, or by CLI: nfig setting management api key certificate
	Cancel Close

10. Click Close to continue.

Modify Authentication Settings

In this section, you will create a certificate that the firewall will use to generate API Keys. Doing so will remove the error message you see when you commit a configuration. With this certificate in place, you will not see the error message when committing any configuration files you save from this point forward. If you load an older configuration file (one you created before applying the API Key certificate), you will receive the error message.

- 11. Go to **Device > Setup > Management**.
- 12. Scroll down and locate the section for Authentication Settings.
- 13. Click the gear icon to edit this section.
- 14. In the field labeled API Key Certificate, use the dropdown box to select Generate.

Authentication Settin	gs	?
Authentication Profile	None	\sim
	Authentication profile to use for non-local admins. Only RADIUS, TACACS+ a SAML methods are supported.	nd
Authentication Profile(Non-UI)	None	\sim
	Authentication Profile to use for non-UI like CLI and API.	
Certificate Profile	None	\sim
Idle Timeout (min)	0	\sim
API Key Lifetime (min)	O (default)	\sim
API Keys Last Expired	Expire All API Keys	
API Key Certificate	None	\sim
Failed Attempts	None	
Lockout Time (min)	New 🕂 Import 😡 Generate	
Max Session Count (number)	0	
Max Session Time (min)	0	
	ОК Сапс	el

- 15. In the Generate Certificate window, enter API-KEY-GEN for Certificate Name.
- 16. For **Common name**, also enter **API-KEY-GEN**.
- 17. Check the box for **Certificate Authority**.
- 18. Under Cryptographic Settings, change the Number of Bits to 4096.
- 19. Leave the remaining settings unchanged.

Generate Certificate	?
Certificate Type 💿 Local 💿 SCEP	
Certificate Name API-KEY-GEN	
Common Name API-KEY-GEN	
IP or FQDN to appear on the certificate	
Signed By	~
Certificate Authority Block Private Key Export	
OCSP Responder	~
 Cryptographic Settings 	
Algorithm RSA	~
Number of Bits 4096	~
Digest sha256	~
Expiration (days) 365	
Certificate Attributes	
TYPE VALUE	
+ Add Oelete	
Generate	Cancel

- 20. Click Generate.
- 21. Click **OK** on the **Generate Certificate** message box.



22. Your Authentication Settings window should now display the API-KEY-GEN certificate in the API Key Certificate field.

Authentication Setting	gs	٢
Authentication Profile	None	V
	Authentication pro SAML methods an	ofile to use for non-local admins. Only RADIUS, TACACS+ and e supported.
Authentication Profile(Non-UI)	None	~
	Authentication Pro	ofile to use for non-UI like CLI and API.
Certificate Profile	None	~
Idle Timeout (min)	0	
API Key Lifetime (min)	0 (default)	~
API Keys Last Expired		Expire All API Keys
API Key Certificate	API-KEY-GEN	· · ·
Failed Attempts	0	
Lockout Time (min)	0	
Max Session Count (number)	0	
Max Session Time (min)	0	
		ОК Сапсе!

- 23. Leave the remaining settings unchanged.
- 24. Click **OK** to close the **Authentication Settings** window.
- 25. Select **YES** on the warning message:

API Key Certificate Change

Changes to the API Key Certificate value will invalidate all existing API keys. Would you like to proceed?



- 26. Click the **Commit** link at the upper right of the web interface:
- 27. Click **Commit** again and wait until the commit process is complete.
- 28. Click **Close** to continue.

Save the Configuration

- 29. Under Device > Setup > Operations > Configuration Management, click Save named configuration snapshot.
- 30. In the Save Named Configuration window, enter API-Key-Config.xml for Name.

Save Name	d Configuration	٢
Name	API-Key-Config.xml	×
		OK Cancel

- 31. Click OK.
- 32. Click Close on the Save Named Configuration message window.
- 33. Under **Device > Setup > Operations**, click **Load named configuration snapshot**.
- 34. For Name, use the drop-down list to select the API-Key-Config.xml file.
- 35. Click **OK** to close the **Load Named Configuration** window.
- 36. Click **OK** to close the **Loading Configuration** message box.

Commit Your Changes and Verify Fix

- 37. Click the **Commit** link at the upper right of the web interface:
- 38. Click **Commit** again and wait until the commit process is complete.
- 39. Note that you no longer receive any error messages regarding the API KeyGen algorithm.

Commit Status		0
Operation Commit		
Status Active		
Result Pending		
Progress	55%	
Details		
Commit		
		Cancel Close

40. Click **Close** when the Commit Status is complete.

Any configuration files you save on this firewall will now use the updated API Key Certificate.

Appendix A - GlobalProtect



Lab Objectives

- Create and configure a Loopback interface.
- Create certificates for the GlobalProtect Portal, internal gateway, and external gateway.
- Attach certificates to an SSL/TLS Service Profile.
- Configure the Server Profile and Authentication Profile to be used when authenticating users.
- Create and configure the tunnel interface to be used with the external gateway.
- Configure the internal gateway, external gateway, and portal.
- Host the GlobalProtect agent on the portal for download.
- Create a No-NAT policy rule to ensure that portal traffic is not subjected to network address translation.
- Test the external gateway and internal gateway.

11.0 Load the Lab Configuration

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot:



A Load Named Configuration dialog box opens.

3. Click the drop-down arrow next to the **Name** field and select **FW-A-11.1a-InternetAccess.xml**

Load Name	d Configuration	?
Name	FW-A-11.1a-InternetAccess.xml	\sim
Decryption Key	****	\sim
	Regenerate Rule UUIDs for selected named configuration Skip Validation	
	OK Cancel	

4. Click **OK** to close the **Load Named Configuration** window.

A window should open that confirms that the configuration is being loaded.

- 5. Click **Close** to close the **Loading Configuration** window.
- 6. Click the **Commit** link at the upper right of the web interface:



A **Commit** window should open.

- Click Commit and wait until the commit process is complete.
 A Commit Status window should open that confirms the configuration was committed successfully.
- 8. Click **Close** to continue.

11.1 Configure a Loopback interface

This Loopback interface will be used for the internal GlobalProtect Gateway.

- 9. In the web interface, select **Network > Interfaces > Loopback**.
- 10. Click **Add**.

The **Loopback Interface** configuration window should open.

11. Configure the following:

Parameter	Value	
Interface Name		
	Interface Name loopback . 1	
Comment	Type Internal gateway	
Logical Router	Select LR-1 from the drop-down list	
Security Zone	ne Select Users_Net from the drop-down list	

oopback Inter	ace		(?
Interface Name	loopback	. 1	
Comment	Internal Gateway		
Netflow Profile	None		~
Config IPv4	IPv6 Advanced		
Assign Interface To			
Assign Interface To Logical Router	LR-1		~



12. Click the **IPv4** tab and configure the following:

Parameter	Value
IP	Click Add and type 192.168.2.1/32

Config IPv4 I	Pv6 Advanc	ed
IP		
192.168.2.1/32		
🕂 Add 😑 Delete	↑ Move Up	↓ Move Down
IP address/netmask. Ex. 192	2.168.2.254/24	

13. Click the Advanced tab and select Allow-Ping for the Management Profile:

Config IPv4 IPv6	Advanced
Other Info	
Management Profile	Allow-Ping
MTU	[576 - 1500]

Addition of a Management Profile is not a requirement for GlobalProtect but can make troubleshooting easier if you need to verify that the IP address on the loopback interface is available.

14. Click **OK** to close the **Layer3 Subinterface** configuration window.

A new loopback interface should display in the web interface.

15. Verify that your configuration looks like the following:

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	LOGICAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
loopback		none	none	none		
loopback.1	Allow-ping	192.168.2.1/32	LR-1	Users_Net		Internal Gateway

11.2 Generate Self-Signed Certificates

GlobalProtect needs three certificates, one each for the portal, external gateway, and internal gateway. These certificates typically are signed by a common CA certificate. This lab creates a CA certificate and internal gateway certificate but combines the portal and external gateway certificates because these GlobalProtect functions are combined on the same IP address. The common CA certificate will be exported and installed on the lab client to make all certificates trusted. In a production environment it is recommended to use a public SSL certificate for the GlobalProtect Portal.

16. In the web interface, select **Device > Certificate Management > Certificates**.

17. Click **Generate** to create a certificate.

👼 Generate

The Generate Certificate window should open.

18. Configure the following:

Parameter	Value
Certificate Name	GlobalProtect
Common Name	GlobalProtect
Signed By	Leave blank
Certificate Authority	Select the check box

Generate Certificate (
Certificate Type	💿 Local 🔷	SCEP
Certificate Name	GlobalProtect	
Common Name	GlobalProtect	
	IP or FQDN to appear on the cer	tificate
Signed By		\sim
	Certificate Authority	
	Block Private Key Export	
OCSP Responder		\sim

You will use this certificate to sign the external and internal gateway certificates.

19. Click Generate.

A status window should open that shows that the **GlobalProtect** certificate and key pair were generated successfully.

20. Click **OK** to close the status window.

A new certificate should display in the web interface.



21. Click Generate and create a certificate for the GlobalProtect external gateway.

The Generate Certificate window should open.

22. Configure the following:

Parameter	Value
Certificate Name	external-gw-portal
Common Name	203.0.113.20
	In a production environment it is recommended to use a public SSL certificate with a public DNS name as the common name
Signed By	Select GlobalProtect from the drop-down list

Generate Certificate

Certificate Type	O Local O SCEP	
Certificate Name	external-gw-portal	
Common Name	203.0.113.20	
	IP or FQDN to appear on the certificate	
Signed By	GlobalProtect	\sim
	Certificate Authority	
	Block Private Key Export	
OCSP Responder		~

Note that you are signing this new certificate with the **GlobalProtect** certificate.

23. Click Generate.

A status window should open that shows the **external-gw-portal** certificate and key pair were generated successfully.

24. Click **OK** to close the status window.

A new certificate should open in the web interface.

- 25. Click **Generate** and create a certificate for the GlobalProtect internal gateway. The **Generate Certificate** window should open.
- 26. Configure the following:

(?)

Parameter	Value	
Certificate Name	internal-gw	
Common Name	192.168.2.1 (the IP address previously assigned to the	
	Loopback interface)	
Signed By	Select GlobalProtect from the drop-down list	

Generate Certifica	te	?
Certificate Type	 Local SCEP 	
Certificate Name	internal-gw	
Common Name	192.168.2.1	
Signed By	IP or FQDN to appear on the certificate	
Signed by	Certificate Authority	<u>``</u>

Again, you are signing this new certificate with the **GlobalProtect** certificate you created earlier.

27. Click Generate.

A status window should open that shows the **internal-gw** certificate and key pair were generated successfully.

28. Click **OK** to close the status window.

A new certificate should display in the web interface.

29. Verify that your configuration looks like the following:

NA	AME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITH
5	TLSv1.3_Default	C = US, ST = CA, L = Santa Clara, O = Palo Alto Networks, CN =	C = US, ST = CA, L = Santa Clara, O = Palo Alto Networks, CN =		\checkmark	Aug 31 11:19:52 2034 GMT	valid	Elliptic Cur
~	GlobalProtect	CN = GlobalProtect	CN = GlobalProtect	<u>~</u>	~	Sep 21 11:50:53 2025 GMT	valid	RSA
	🗊 external-gw-portal	CN = 203.0.113.20	CN = GlobalProtect		\checkmark	Sep 21 11:53:34 2025 GMT	valid	RSA
	🗊 internal-gw	CN = 192.168.2.1	CN = GlobalProtect		\checkmark	Sep 21 11:54:57 2025 GMT	valid	RSA

11.3 Configure the SSL/TLS Service Profile

- 30. In the web interface, select **Device > Certificate Management > SSL/TLS Service Profile**.
- 31. Click **Add** to create a profile.

The **SSL/TLS Service Profile** configuration window should open.

32. Configure the following:

Parameter	Value	
Name	Type external-gw-portal	
Certificate	Select external-gw-portal from the drop-down list	
Min Version	Select TLSv1.2 from the drop-down list	
Max Version	Select TLSv1.3 or the maximum available TLS version	

SSL/TLS Service Profile		
Name	external-gw-portal	
Certificate	external-gw-portal	
Protocol Settings		
Min Version	TLSv1.2	
Max Version	TLSv1.3	

This SSL/TLS Service Profile defines the certificate to present to the GlobalProtect client agent when the agent initially connects to the GlobalProtect Portal. The firewall will present this same certificate when the agent software connects to an external gateway.

33. Click **OK** to close the **SSL/TLS Service Profile** configuration window.

A new SSL/TLS profile should display in the web interface.

34. Click Add to create a second SSL/TLS Service Profile.

The **SSL/TLS Service Profile** configuration window should open.

35. Configure the following:

Parameter	Value	
NameType internal-gw		
Certificate	Select internal-gw from the drop-down list	
Min Version Select TLSv1.2 from the drop-down list		
Max Version	Select TLSv1.3 or the maximum available TLS version	

SSL/TLS Service Profile	
Name	internal-gw
Certificate	internal-gw
Protocol Settings	
Min Version	TLSv1.2
Max Version	TLSv1.3

This SSL/TLS Service Profile defines the certificate to present to the GlobalProtect client agent when the agent connects to an internal GlobalProtect Gateway.

- 36. Click **OK** to close the **SSL/TLS Service Profile** configuration window. A new SSL/TLS profile should display in the web interface.
- 37. Verify that your configuration looks like the following:

external-gw-portal	external-gw-portal	RSA DHE ECDHE	Min Version: TLSv1.2 Max Version: TLSv1.3
internal-gw	internal-gw	RSA DHE ECDHE	Min Version: TLSv1.2 Max Version: TLSv1.3

These entries instruct the firewall to use the appropriate certificate when communicating with the GlobalProtect agent software. You have one certificate to use when the client connects to the portal or to an external gateway; and a second certificate to use when the client connects to an internal gateway.

11.4 LDAP Server Profile Configuration

When the GlobalProtect agent connects to the portal, the firewall must authenticate the user. In this section, you define the service that the firewall will use to authenticate users when they invoke the GlobalProtect agent. Separately, when the GlobalProtect agent connects to a gateway to establish a VPN, the firewall must authenticate the user.

You should have created an LDAP Server Profile for authentication.

In the web interface, select **Device > Server Profiles > LDAP**.

- 38. Select Add.
- 39. Configure the following parameters:

Parameter	Value
Profile Name	LDAP_Servers

- 40. Locate the **Server list** on the left side of the window.
- 41. Configure the following:

Parameter	Value
Name	LDAP1
LDAP Server	192.168.50.89
Port	389

42. Locate Server Settings on the right side of the window and configure the following:

Parameter	Value
Туре	other
Base DN	dc=panw,dc=lab
Bind DN	cn=admin,dc=panw,dc=lab
Password	Pal0Alt0!
Require SSL/TLS secured connection	Deselected check box

LDAP Server	Profile			(
Profile Name	LDAP_Servers					
Server List	Administrator Use Only		 Server Settings 			
NAME	LDAP SERVER	PORT	Туре	other 🗸		
LDAP1	192.168.50.89	389	Base DN	dc=panw,dc=lab \checkmark		
			Bind DN	cn=admin,dc=panw,dc=lab		
			Password	•••••		
			Confirm Password	•••••		
+ Add - De	elete		Bind Timeout	32		
Enter the IP address	or FQDN of the LDAP server		Search Timeout	30		
			Retry Interval	60		
				Require SSL/TLS secured connection		
				Verify Server Certificate for SSL sessions		
				OK Cancel		

43. Click **OK** to close the **LDAP Server Profile** configuration window.

11.5 Authentication Profile Configuration

You should have create an Authentication Profile that contains the LDAP Server Profile. You will create this profile and authenticate the users accessing the GlobalProtect Portal or the Gateway via it.

44. In the web interface, select **Device > Authentication Profile**.

45. Click Add.

An Authentication Profile configuration window should open.

46. Configure the following parameters:

Parameter	Value
Name	LDAP_Auth
Туре	LDAP
Server Profile	LDAP_Servers

Autonication From	Autł	nenti	cati	on P	rofile	e
-------------------	------	-------	------	------	--------	---

Name LDAP_Auth					
Authentication Factors	Authentication Factors Advanced				
Туре	LDAP	~			
Server Profile	LDAP_Servers	~			
Login Attribute					
Password Expiry Warning	7				
	Number of days prior to warning a user about password expiry.				
User Domain					
Username Modifier	%USERINPUT%	~			

47. Select the Advanced tab then Add under Allow List and configure the following:

Parameter	Value
Allow List	all

Authentication Profile (?		
Name	LDAP_Auth	
Authentication Factors	Advanced	
Allow List		
ALLOW LIST A		
🔲 🥵 all		

48. Click **OK** to close the **Authentication Profile** configuration window.

A new Authentication Profile should display in the web interface.

		Loc	kout			
NAME	LOCATION	FAILED ATTEMPTS (#)	LOCKOUT TIME (MIN)	ALLOW LIST	AUTHENTICATION	SERVER PROFILE
LDAP_Auth			0	🥵 all	LDAP	LDAP_Servers

?

11.6 Configure the Tunnel Interface

The GlobalProtect client agent software uses a VPN tunnel to establish a secure connection to an external gateway. The firewall uses a tunnel interface to encrypt and decrypt traffic with the client.

- 49. In the web interface, select **Network > Interfaces > Tunnel**.
- 50. Click Add to create a new tunnel interface.

A **Tunnel Interface** configuration window should open.

51. Configure the following:

Parameter	Value
Interface Name	
	Interface Name tunnel . 11
Comment	Type VPN Tunnel Interface
Logical Router	Select LR-1 from the drop-down list
Security Zone	Select Users_Net from the drop-down list

Tunnel Interface		(?)	
Interface Name	tunnel . 11		
Comment	VPN_Tunnel_Interface		
Netflow Profile None			
Config IPv4 IF	V6 Advanced		
 Assign Interface To — 			
Logical Route	r LR-1	\sim	
Security Zone	Users_Net	~	

The logical tunnel interface is connected to a logical router and assigned to a security zone just as are other interfaces.

52. Click **OK** to close the **Tunnel Interface** configuration window.

A new tunnel interface should display in the web interface.

Cancel

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	LOGICAL ROUTER	SECURITY ZONE	FEATURES	COMMENT
tunnel		none	none	none		
tunnel.11		none	LR-1	Users_Net		VPN_Tunnel_Interface

11.7 Configure the Internal Gateway

Internal gateways can be used for User-ID deployment and host information profile (HIP) enforcement. They also can be used to encrypt traffic from the client to sensitive internal resources through a VPN gateway.

- 53. In the web interface, select **Network > GlobalProtect > Gateways**.
- 54. Click **Add** to create a gateway.

The **GlobalProtect Gateway Configuration** window should open.

55. Configure the following:

Parameter	Value
Name	Type gp-int-gateway
Interface	Select loopback.1 from the drop-down list
IPv4 Address	Select 192.168.2.1/32 from the drop-down list

GlobalProtect Gateway Configuration					
General	Name gp-int-gateway				
Authentication	Network Settings				
Agent	Interface	loopback.1			
Satellite	IP Address Type	IPv4 Only			
	IPv4 Address	192.168.2.1/32			
	Log Settings				
		Log Successful SSL Handshake			
		Log Unsuccessful SSL Handshake			
	Log Forwarding d	efault			

56. Select the Authentication tab and configure the following:

Parameter	Value
SSL/TLS Service Profile	Select internal-gw from the drop-down list

GlobalProtect Gateway Configuration

General	Server Authentication		
Authentication	SSL/TLS Service Profile	internal-gw	

- 57. Locate the **Client Authentication** list box.
- 58. Click **Add** to configure client authentication settings.

The **Client Authentication** configuration window should open.

59. Configure the following:

Parameter	Value
Name	Type lab-ldap
OS	Verify that Any is selected
Authentication Profile	Select LDAP_Auth from the drop-down list

Client Authentication

		\sim	
Name	lab-ldap		
OS	Any	~	
Authentication Profile	LDAP_Auth	\sim	
	Automatically retrieve passcode from SoftToken application		
GlobalProtect App Login Screen —			
Username Labe	Username		
Password Labe	Password		
Authentication Message	Enter login credentials		
	Authentication message can be up to 256 characters.		
		=	
Allow Authentication with Use	No (User Credentials AND Client Certificate Required)	\sim	
Credentials OR Client Certificate	To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.		

ок	Cancel

 \bigcirc

This area lets you configure different authentication methods for different sets of users based on the operating system in use for the GlobalProtect client agent software.

60. Click **OK** to close the **Client Authentication** configuration window.

GlobalProtect Gateway Configuration (?)									
General	Server Authentication								
Authentication	SSL/TLS Service Profile internal-gw 🗸								
Agent Satellite	Client Authentication								
		AME	OS	AUTHENTICAT PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC MESSAGE	ALLOW AUTHENTIC WITH USER CREDENTIALS OR CLIENT CERTIFICATE
	🔲 lab	o-ldap	Any	LDAP_Auth		Username	Password	Enter login credentials	No
	Block login for quarantined devices								

61. Click **OK** to close the **GlobalProtect Gateway Configuration** window.

A new GlobalProtect Gateway should display in the web interface.

11.8 Configure the External Gateway

In this section you will create the GlobalProtect external gateway.

62. Click **Add** to create a second gateway.

The **GlobalProtect Gateway Configuration** window should open. The external gateway is the VPN gateway that GlobalProtect clients connect to when they are outside the local network.

63. Configure the following:

Parameter	Value
Name	Type gp-ext-gateway
Interface	Select ethernet1/1 from the drop-down list
IPv4 Address	Select 203.0.113.20/24 from the drop-down list

GlobalProtect Gateway Configuration				
General	Name	gp-ext-gateway		
Authentication	Network Settings			
Agent	Interface	e ethernet1/1		
Satellite	IP Address Type	Pv4 Only		
	IPv4 Address	203.0.113.20/24		

64. Select the **Authentication** tab and configure the following:

Parameter	Value
SSL/TLS Service Profile	Select external-gw-portal from the drop-down list

GlobalProtect Gateway Configuration

General	Server Authentication	
Authentication	SSL/TLS Service Profile	external-gw-portal
Agent	Client Authentication	

This setting defines the certificates to present to the client when it connects to the gateway. Remember that you created a single SSL/TLS Service Profile for the portal and for the external gateway.

65. Locate the **Client Authentication** list box.

66. Click Add to configure client authentication settings.

The **Client Authentication** configuration window should open.

67. Configure the following:

Parameter	Value
Name	Type lab-ldap
OS	Verify that Any is selected
Authentication Profile	Select LDAP_Auth from the drop-down list

Client Authentication			
Name	lab-Idap		
OS	Any		
Authentication Profile	LDAP_Auth		

This section allows you to select different authentication methods (Authentication Profiles) based on the operating system of client hosts.

68. Click **OK** to close the **Client Authentication** window:

GlobalProtec	t Gate	eway Config	uration						(?
General	Ser	Server Authentication							
Authentication	ation SSL/TLS Service Profile external-gw-portal						~		
Agent	Client Authentication								
outenice		NAME	os	AUTHENTICAT PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC MESSAGE	ALLOW AUTHENTIC WITH USER CREDENTIALS OR CLIENT CERTIFICATE
		lab-ldap	Any	LDAP_Auth		Username	Password	Enter login credentials	No
	÷	Add 🔵 Dele Certificate	te ⓒ Clone Profile None V Block	↑ Move Up ↓ I	Move Down				~

69. Click the **Agent** tab and configure the following:

Parameter	Value		
Tunnel Mode	Select the check box		
Tunnel Interface	Select tunnel.11 from the drop-down list		
Enable IPSec	Verify that the Enable IPSec check box is selected		

GlobalProtect Gateway Configuration					
General Authentication	Tunnel Settings Client Settings Client IP Pool				
Agent Satellite	Tunnel Interface tunnel.11 Max User [1 - 500]				
	GlobalProtect IPSec Crypto default				

This section tells the firewall how to establish a tunnel with a client and which interface to use.

70. Click the **Client Settings** subtab.

71. Click **Add** to configure client settings.

The **Configs** configuration window should open.

72. Click the **Config Selection Criteria** tab and configure the following:

Parameter	Value
Name	Type gp-client-config

Configs	
Config Selection Criteria	Authentication Override IP Pools
Name gp-client	-config

After a client has been authenticated to establish a VPN with the gateway, these settings define which IP address and other network elements the GlobalProtect client adapter will use.

73. Click the **IP Pools** subtab and configure the following:

Parameter	Value
IP Pools	Click Add and type 192.168.100.200- 192.168.100.210

Configs					
Config Selection Criteria Authentication Override	Is Split Tunnel Network Services				
Retrieve Framed-IP-Address attribute from authentication server					
AUTHENTICATION SERVER IP POOL	IP POOL				
Enter IP subnets or ranges to match the Framed IP attribute of the authentication server. Supports IPv4 private/public addresses (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) or IPv6 unique local/public addresses (e.g. 2001:aa::1-2001:aa::10)	192.168.100.200-192.168.100.210				
⊕ Add ⊖ Delete	Add ⊖ Delete ↑ Move Up ↓ Move Down				

These IPs will be added to the firewall's routing table

These IPs will be added to the firewall's routing table

The firewall will assign an IP address to each GlobalProtect client from this range of addresses.

74. Click **OK** to close the **Configs** window.

The **GlobalProtect Gateway** configuration window still should be open on the **Client Settings** subtab.

75. Click the Network Services subtab and configure the following:

Parameter	Value
Primary DNS	Type 1.1.1.1
Secondary DNS	Type 8.8.8.8

GlobalProtec	t Gateway Confi	guration ()
General Authentication	Tunnel Settings	Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification
Agent	Inheritance Source	None
Satellite		Q Check inheritance source status
	Primary DNS	1111 ~
	Secondary DNS	8.8.8.8
	Primary WINS	None v
	Secondary WINS	None V
		Inherit DNS Suffixes
	DNS Suffix	Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)

The servers used in the lab are public, but in many cases the DNS servers that are assigned to the GlobalProtect client adapter will be private, internal DNS hosts. This setting will enable the client to resolve internal hostnames while connected to the VPN.

- 76. Click **OK** to close the **GlobalProtect Gateway Configuration** window. A new GlobalProtect Gateway should display in the web interface.
- 77. Verify that your configuration looks like the following:

		NAME	LOCATION	LOCAL INTERFACE	LOCAL IP	TUNNEL	MAX USER	INFO
+		gp-int-gateway		loopback.1	192.168.2.1/32			
+	\checkmark	<u>gp-ext-gateway</u>		ethernet1/1	203.0.113.20/24	tunnel.11		Remote Users

11.9 Configure the Portal

The GlobalProtect Portal provides the management functions for the GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives its configuration from the portal, including information about the available GlobalProtect Gateways and any optional client certificates that might be necessary for the client to connect to a gateway.

- 78. In the web interface, select **Network > GlobalProtect > Portals**.
- 79. Click **Add** to create a new portal.

The **GlobalProtect Portal Configuration** window opens.

80. Configure the following:

Parameter	Value		
Name	Type gp-portal		
Interface	Select ethernet1/1 from the drop-down list		
IPv4 Address	Select 203.0.113.20/24 from the drop-down list		

GlobalProtect Portal Configuration					
General	Name	gp-portal			
Authentication	Network Settings				
Portal Data Collection	Interface	ethernet1/1			
Agent	IP Address Type	IPv4 Only			
Clientless VPN	IPv4 Address	203.0.113.20/24			

81. Click the Authentication tab and configure the following:

Parameter	Value
SSL/TLS Service Profile	Select external-gw-portal from the drop-down list

82. Locate the **Client Authentication** list box.

83. Click Add to configure client authentication settings.

The **Client Authentication** configuration window should open.

84. Configure the following:

Parameter	Value	
Name	Type lab-ldap	
OS	Verify that Any is selected	
Authentication Profile	Select LDAP_Auth from the drop-down list	

Client Authentication				
Name	lab-ldap			
OS	Any			
Authentication Profile	LDAP_Auth			

In this section, the portal is being configured to authenticate users against the LDAP_Auth Profile that contains your LDAP server.

- 85. Click **OK** to close the **Client Authentication** list box.
- 86. Click the Agent tab.
- 87. Locate Trusted Root CA in the lower-left corner.
- 88. Click Add and select the GlobalProtect certificate from the drop-down list.
- 89. Check Install in Local Root Certificate Store

	TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE			
	GlobalProtect				
🛨 Add 😑 Delete					

This is the certificate you used to sign the portal certificate and the gateway certificate. By placing it in this section, you can push this signing certificate down to the client's trusted certificate store through the GlobalProtect connection. This CA is at the top of the chain of trust, so the client host will trust any certificate signed by this one, including the portal and gateway certificates.

90. Locate the **Agent** list box:

GlobalProtect Port	GlobalProtect Portal Configuration (?				
General	eneral Agent				
Authentication					CLIENT
Portal Data Collection	CONFIGS	USER/USER GROUP	os	EXTERNAL GATEWAYS	CERTIFICATE
Agent					
Clientless VPN					
Satellite	+ Add - Delete) Clone ↑ Move Up ↓ N	Nove Down		
	TRUSTED ROOT CA	INSTALL IN LOCAL ROO CERTIFICATE STORE	T Conf	Agent User Override Key	
	GlobalProtect			,	
	+ Add - Delete				

91. Click Add to configure Agent.

The **Configs** configuration window should open.

92. Click the Authentication tab and configure the following:

Parameter	Value
Name	Type portal-agent-config

Configs	
Authentication Config Selection	Criteria Internal External App HIP Data Collection
Name	portal-agent-config
Client Certificate	None 🗸

- 93. Click the **Internal** tab.
- 94. Select the Internal Host Detection IPv4 check box.
- 95. Configure the following:

Parameter	Value	
IP Address	Type 192.168.2.1	
Hostname	Type gp-int-gw	

Configs				
Authentication	Config Selection Criteria	Internal	External	
✓ Internal Host Detection IPv4				
IP Address	192.168.2.1			
Hostname	gp-int-gw			

When the client is inside the network, a reverse DNS lookup for 192.168.2.1 will resolve to gp-ingw. If that lookup is successful, the GlobalProtect client will connect to an internal gateway. If that reverse lookup fails (or returns a name other than gp-in-gw), the GlobalProtect client will connect to an external gateway.

96	Locate the Internal	Gateways	list hox and	l click A	ot bb	configure
90.	Locale the milerna	Galeways	list box and	I CHCK A	uu 10	configure.

Configs			
Authentication Con	fig Selection Criteria	xternal App HIP Data Collection	
🗸 🔽 Internal Host Detectio	on IPv4	Internal Host Detection IPv6	
IP Address 192	2.168.2.1	IP Address	
Hostname gp-i	int-gw	Hostname	
Internal Gateways			
NAME	ADDRESS	SOURCE IP	DHCP OPTION 43 CODE
			Specify one or more sub- option codes (in decimal). GlobalProtect Agent will read the gateway address from values defined by the sub-option codes.
🕂 Add 😑 Delete	↑ Move Up 👃 Move Down		🕂 Add 😑 Delete

The Internal Gateway configuration window should open.

97. Configure the following:
Parameter	Value
Name	Type int-gw-1
Address	Select the IP radio button
IPv4	Type 192.168.2.1

nternal Gateway (?)				
Name	int-gw-1			
Address	🔿 FQDN 💿 IP			
IPv4	192.168.2.1			
IPv6				

- 98. Click **OK** to close the **Internal Gateway** configuration window.
- 99. Click the **External** tab.
- 100. Locate the External Gateways list box and click Add to configure.

The **External Gateway** configuration window should open.

101. Configure the following:

Parameter	Value
Name	Type ext-gw-1
Address	Select the IP radio button
IPv4	Type 203.0.113.20

External Gateway		
Name	ext-gw-1	
Address	◯ FQDN 🧿 IP	
IPv4	203.0.113.20	
IPv6		

102. Locate the **Source Region** list box and click **Add** to configure the following:

Parameter	Value
Source Region	Select Any from the drop-down list
Priority	Verify that Highest is selected

External Gatev	vay	?
Name	ext-gw-1	
Address	🔵 FQDN 💿 IP	
IPv4	203.0.113.20	
IPv6		
Q		1 item $ ightarrow$ $ ightarrow$
	ол	PRIORITY
Any		Highest

The **Source Region** options allow you to prioritize that the external gateway that a client connects to be based on the geographic assignment of a client's IP address. You have only a single external gateway, so you are setting **Source Region** to **Any** so that all clients connect to this gateway, regardless of their IP address.

- 103. Click **OK** to close the **External Gateway** configuration window.
- 104. Click **OK** to close the **Configs** configuration window.
- 105. Click **OK** to close the **GlobalProtect Portal Configuration** window.

A new GlobalProtect Gateway should display in the web interface. Click the Plus icon to expand the entry and verify that your configuration looks like the following screenshot:

٢	AME	LOCATIO	N	INTERFACE		IP	SSL/TLS SERVICE PROFILE	AU	JTHENTICATION P	ROFILE	CERTIFICATE PROFILE	INFO
8	p-portal			ethernet1/1		203.0.113.20/24	external-gw-portal	LD	DAP_Auth			
	AGENT CONFIGURATION		USERS		os	OPTIONS			EXTERNAL GWS	INTERN	IAL GWS	CONNECT METHOD
	portal-agent-config		any		any	Internal Host D	etection: gp-int-gw,192.168.2	.1	ext-gw-1	int-gw-	1	User-logon (Always On)

11.10 Host the GlobalProtect Agent on the Portal

To make the process of obtaining and installing the GlobalProtect agent software easier for users, you will download a specific version and activate it on the portal. Activation of the GlobalProtect Agent software allows users to connect to a webpage on the portal and download the appropriate version of the client software for their host operating system.

106. In the web interface, select **Device > GlobalProtect Client**.

107. Click **Check Now** at the bottom of the page.

The Palo Alto Networks firewall checks for the latest version of the GlobalProtect agent.

108. Search for the **6.1.0** version of GlobalProtect.

Even if there is a newer version of the client software, be sure to use the 6.1.0 version.

109. Click **Download** in the **Action** column:

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY ACTIVATED	ACTION	
6.1.0	124 MB	2022/09/01 14:06:19			Validate	Release Notes

A **Download GlobalProtect Client** status window should open. Do not continue until the download has completed successfully. After a new version of the GlobalProtect client software is released, you can download it through this interface and activate it. Any users currently running an older version of the GlobalProtect software will be upgraded to the new version when they connect to the portal.

Download	I GlobalProtect Client
Operation Status	Download Completed
Result	Successful
Details	Successfully downloaded Preloading into software manager Successfully loaded into software manager
Warnings	

110. Clock **Close** to close the status window.

111. Click Activate in the Action column.

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY ACTIVATED	ACTION	
6.1.0	124 MB	2022/09/01 14:06:19	1		Validate Export Activate	Release Notes

112. Click the Yes button to close the Activate GlobalProtect Client version message:



An **Activate GlobalProtect Client** message should display that shows that the client package was activated successfully.

Activate GlobalProtect Client version 6.1.0

Operation Software Install Status Completed Result Successful Details client package activation successfully completed. Warnings

113. Click **Close** to close the **Activate GlobalProtect Client** status message:

114. Verify:

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY ACTIVATED	ACTION	DOCUMENTATION
6.1.0	124 MB	2022/09/01 14:06:19	1	1	Validate Export Reactivate	Release Notes

11.11 Create a Security Policy Rule

- 115. In the web interface, select **Policies > Security**.
- 116. Select the "Users_to_Internet" rule without opening it.
- 117. Click Clone.
- 118. When the cloned security rule appears click on "Users_to_Internet-1" to edit it.

The **Security Policy Rule** configuration window should open.

119. Configure the following:

Parameter	Value
Name	Rename the security policy rule to inside-portal
Audit Comment	Type-Created GlobalProtect inside portal Security policy rule on <date> by <your- Role></your- </date>

Security Policy Rule						
General Source	e Destination Application Service/URL Category Actions Usage					
Name	inside-portal					
Rule Type	universal (default)					
Description	Allows hosts in Users_Net zone to access Internet zone.					
T						
lags						
Group Rules By Tag	None					
Audit Comment	Created GlobalProtect inside portal Security policy rule on 21.09.2024 by Company/Admin					
	Audit Comment Archive					

120. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Address	Click Add and type 203.0.113.20

Security Policy Rule	
General Source Destination Application Service	e/URL Category Actions Usage
select 🗸	Any
DESTINATION ZONE A	DESTINATION ADDRESS ^
Internet	203.0.113.20

121. Click the **Service/URL Category** tab and configure the following:

Parameter	Value
Service	Select any from the drop-down list

Security Policy Rule	0
General Source Destination Application Service/URL Category Actions Us	sage
any v	Any
SERVICE A	URL CATEGORY A
+ Add O Delete	↔ Add

122. Click the Actions tab and configure the following:

Parameter	Value
Profile Type	None

Security Policy Rule					
General Source D	estination Application Service/URL Category Actions	Usa			
Action Setting					
Action	Allow	\sim			
	Send ICMP Unreachable				
L					

Profile Setting			
Profile Type	None	\sim	

123. Click **OK** to close the **Security Policy Rule** configuration window.

11.12 Create a No-NAT Rule

All traffic from the **Users_Net** zone to the **Internet** zone uses source NAT. In this section, you will create a new NAT policy rule so that internal requests for the GlobalProtect Portal (203.0.113.20) will not get their address translated by the "Users_to_Internet" rule. The new NAT policy rule must be matched before the "Users_to_Internet" rule, so you will place it at the top of the NAT policy.

- 124. In the web interface, select **Policies > NAT**.
- 125. Click **Add** to create a rule.

The **NAT Policy Rule** configuration window should open.

126. Configure the following:

Parameter	Value
Name	Type gp-portal-no-nat
NAT Type	Verify that ipv4 is selected
Audit Comment	Type Created GlobalProtect no NAT policy rule on <date> by <your-role></your-role></date>

NAT Policy Rule				
General Original Packet Translated Packet				
gp-portal-no-nat				
None				
ipv4				
Created GlobalPotect no NAT policy rule on 26.01.2023 by CompanyAdmin				

Audit Comment Archive

127. Click the **Original Packet** tab and configure the following:

Parameter	Value		
Source Zone	Click Add and select Users_Netfrom the drop-down list		
Destination Zone	Select Internet from the drop-down list		
Destination Interface	Select ethernet1/1 from the drop-down list		
Destination Address	Click Add and type 203.0.113.20		

NAT Policy Rule				(
General Original Packet	Translated Packet			
Any	Destination Zone		🗸 Any	Any
	Internet	\sim	SOURCE ADDRESS A	DESTINATION ADDRESS A
Users_Net				203.0.113.20
	Destination Interface			
	ethernet1/1	~		
	Service	~		
+ Add Oelete			+ Add O Delete	+ Add O Delete

128. Select the **Translated Packet** tab and verify that the **Translation Type** for **Source Address Translation** and **Destination Address Translation** are set to **None**.

This rule instructs the firewall to *not* perform network address translation of any kind for traffic from the Users_Net zone that has a destination address of 203.0.113.20 in the Internet zone, which is the IP address of the GlobalProtect Portal and of the external gateway.

IAT Policy Rule					(
General Origina	Packet Translated Packet				
Source Address Tran	slation	De	stination Address Translatio	n —	
Translation Type	None	~	Translation Type	None	~

129. Click **OK** to close the **NAT Policy Rule** configuration window.

A new NAT policy rule should display in the web interface.

Cancel

130. Select but do not open **gp-portal-no-nat**.

131. Click **Move** and select **Move Top**:

					Original	Packet			Translate	ed Packet
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	gp-portal-no-nat	none	🚧 Users_Net	Mainternet	ethernet1/1	any	P 203.0.113.20	any	none	none
2	Extranet_to_Internet	none	🚧 Extranet	Mainternet	any	any	any	any	dynamic-ip-and-port	none
									ethernet1/1	
									203.0.113.20/24	
3	Users_to_Internet	none	Mage Stress Net	Mainternet	any	any	any	any	dynamic-ip-and-port	none
									ethernet1/1	
									203.0.113.20/24	
4	Extranet-to-UsersNet	none	🞮 Extranet	Musers_Net	any	any	any	any	dynamic-ip-and-port	none
									ethernet1/2	
									192.168.1.1/24	

Traffic that is not destined for the portal IP address (203.0.113.20) will be translated by the "Users_to_Internet" rule.

132. Commit all changes.

Note: A warning might display about IPv6 not being enabled on the tunnel interface. You can safely ignore it.



Stop. This is the end of the GlobalProtect lab.

Appendix B - Active/Passive High Availability



Lab Objectives

Please note that this is a configuration lab only as the lab has been designed with a single FireWall.

- Display the Dashboard HA widget.
- Configure a dedicated HA interface.
- Configure active/passive HA.
- Configure HA monitoring.
- Observe behavior in the HA widget.

14.0 Load a Lab Configuration

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot:

Configuration	Management
---------------	------------

- Revert Revert to last saved configuration Revert to running configuration
- Save Save named configuration snapshot Save candidate configuration Load Load named configuration snapshot

Load configuration version

Export Export named configuration snapshot Export configuration version Export device state Import Import named configuration snapshot

Import device state

A Load Named Configuration dialog box opens.

3. Click the drop-down arrow next to the **Name** field and select **FW-A-11.1a-InternetAccess.xml**.

Load Name	d Configuration	?
Name	FW-A-11.1a-InternetAccess.xml	\sim
Decryption Key	****	\sim
	Regenerate Rule UUIDs for selected named configuration Skip Validation	
	OK Cancel	

4. Click **OK** to close the **Load Named Configuration** window.

A window should open that confirms that the configuration is being loaded.

- 5. Click **Close** to close the **Loading Configuration** window.
- 6. Click the **Commit** link at the upper right of the web interface:



A **Commit** window should open.

7. Click **Commit** and wait until the commit process is complete.

A **Commit Status** window should open that confirms that the configuration was committed successfully.

8. Click **Close** to continue.

14.1 Display the HA Widget

If high availability (HA) is enabled, the **High Availability** widget on the **Dashboard** indicates the HA status.

- 9. In the web interface, click the **Dashboard** tab to display current firewall information.
- 10. If the **High Availability** panel is not displayed, select **Widgets > System > High Availability** to enable the display:



The High Availability widget now displays on the Dashboard:

High Availability	G	\times
HA not enabled		

14.2 Configure the HA Interface

Each HA interface has a specific function: One interface is for configuration synchronization and heartbeats, and the other interface is for state synchronization.

- 11. In the web interface, select **Network > Interfaces > Ethernet**.
- 12. Click **ethernet1/6** to open the configuration window.

The Ethernet Interface configuration window should open.

13. Configure the following:

Parameter	Value
Interface Type	Select HA from the drop-down list
Comment	HA1

Ethernet Interf	ace	(?)
Interface Name	ethernet1/6	
Comment	HA1	
Interface Type	НА	×
Advanced		
Link Settings		
Link Speed	uto Link Duplex auto	Link State \sim

- OK Cancel
- 14. Click **OK** to close the **Ethernet Interface** configuration window.

15. Click **ethernet1/7** to open the configuration window.

The **Ethernet Interface** configuration window should open.

16. Configure the following:

Parameter	Value
Interface Type	Select HA from the drop-down list
Comment	HA2

thernet Inter	rface		(
Interface Name	e thernet1/7		
Commen	t HA2		
Interface Type	HA		```
Link Settings —			

17. Click **OK** to close the **Ethernet Interface** configuration window.

14.3 Configure Active/Passive HA

In this deployment, the active firewall continuously synchronizes its configuration and session information with the passive firewall over two dedicated interfaces. If a hardware or software disruption occurs on the active firewall, the passive firewall becomes active automatically without loss of service. Active/passive HA deployments are supported by the interface modes Virtual Wire, Layer 2, and Layer 3.

- 18. In the web interface, select **Device > High Availability > General**.
- Click the icon of the Setup panel.
 The Setup configuration window should open.
- 20. Configure the following:

Parameter	Value
Enable HA	Enable HA
Group ID	Type 60 (This field is required, and must be unique, if multiple HA pairs reside on the same broadcast domain.)
Mode	Verify that the Active Passive radio button is selected
Enable Config Sync	Enable Config Sync (Select this option to enable synchronization of configuration settings between the peers.)
Peer HA1 IP Address	Type 172.16.3.11
Backup Peer HA1 IP Address	Type 192.168.1.253

 \bigcirc

Setup

•	Ŭ
	✓ Enable HA
Group ID	60
Description	
Mode	 Active Passive O Active Active
	🗸 Enable Config Sync
Peer HA1 IP Address	172.16.3.11
Backup Peer HA1 IP Address	192.168.1.253

- 21. Click **OK** to close the **Setup** configuration window.
- 22. Click the icon of the **Active/Passive Settings** panel:

The Active/Passive Settings configuration window should open.

23. Configure the following:

Parameter	Value	
Passive Link State	Select the Auto radio	button
Active/Passive Set	tings	(?)
Passive I	ink State 🔵 Shutdown 💿 Au	ito

When **Auto** is selected, the links that have physical connectivity remain physically up but in a disabled state. They do not participate in ARP or packet forwarding. This configuration helps reduce convergence times during failover because no time is required to activate the links. To avoid network loops, do not select this option if the firewall has any Layer 2 interfaces configured.

24. Click **OK** to close the **Active/Passive Settings** configuration window.

Parameter	Value	
Device Priority	Type 80	
	Enter a priority value (range is 0 to 255) to identify the active firewall. The firewall with the lower value (higher priority) becomes the active firewall when the preemptive capability is enabled on both firewalls in the pair.)	
Preemptive	Preemptive	
	Enables the higher priority firewall to resume active operation after recovering from a failure. This parameter must be enabled on both firewalls but is not always a recommended practice.	
Heartbeat Backup	Heartbeat Backup	
	Uses the management ports on the HA firewalls to provide a backup path for heartbeat and hello messages	

25. Click the ⁽¹⁾ icon of the **Election Settings** panel to configure failover behavior:

26. Click **OK** to close the **Election Settings** configuration window.

Election Settings		?
Device Priority	80	
	Preemptive	
	Heartbeat Backup	
HA Timer Settings	Recommended	\sim

27. Open the **HA Communication** tab.

General	HA Communications	Link and Path Monitoring
---------	-------------------	--------------------------

28. Click the icon of the **Control Link (HA1)** configuration window to configure the HA1 link. The firewalls in an HA pair use HA links to synchronize data and maintain state information:

Parameter	Value
Port	Select ethernet1/6 from the drop-down list
IPv4/IPv6 address	Type 172.16.3.10
Netmask	Type 255.255.255.0

Ш	I٨	1
	IA	Т.

		U
Port	ethernet1/6	~
IPv4/IPv6 Address	172.16.3.10	
Netmask	255.255.255.0	
Gateway		
	Encryption Enabled	
Monitor Hold Time (ms)	3000	

- 29. Click **OK** to close the **Control Link (HA1)** configuration window.
- 30. Click the icon of the **Control Link (HA1 Backup)** configuration window to configure the HA1 Backup link. The HA1 Backup link is important to avoid a split brain condition in case the primary HA1 link goes down:

Parameter	Value
Port	Select management

0

HA1 Backup		0
	Port	management (Non-dedicated out of band MGT interface for ha \checkmark
		ОК Сапсе!

- 31. Click **OK** to close the **Control Link** (**HA1 Backup**) configuration window.
- 32. Click the ^(III) icon of the **Data Link (HA2)** configuration window.
- 33. to configure the HA2 link. The firewalls in an HA pair use HA2 links to synchronize session state information:

Parameter	Value	
Port	Select ethernet1/7 from the drop-down list	
Transport	Select ethernet	
	When using ethernet as the transport protocol, it is not necessary to configure any IP addresses on the HA2 link as the state information are transferred between the FireWalls at Layer-2	
HA2 Keep-alive	Check and select Log Only	

HA2

\bigcirc
(?)
\sim

	Enable Session Synchronization	
Port	ethernet1/7	~
IPv4/IPv6 Address		
Netmask		
Gateway		
Transport	ethernet	~
🚽 🖌 HA2 Keep-alive —		
Actio	🛛 📀 Log Only 🛛 Split Datapath	
Threshold (ms) 10000	

34. Click **OK** to close the **Data Link** (**HA2**) configuration window.

14.4 Configure HA Monitoring

35. In the web interface, select **Device > High Availability > Link and Path Monitoring**.

36. Click the ⁽¹⁾ icon of the **Link Monitoring** panel to configure link failure detection.

The Link Monitoring configuration window should open.

Link monitoring enables failover to be triggered when a physical link or group of physical links fails.

37. Configure the following:

Parameter	Value
Enabled	Enabled
Failure Condition	Verify that the Any radio button is selected
Link Monitoring	

	🗸 Enabled	
Failure Condition	💿 Any i 🔿 A	dI

38. Click **OK** to close the **Link Monitoring** configuration window.

39. Click Add in the Link Group panel to configure the traffic links to monitor.

The **Link Group** configuration window should open.

General HA Communicat	tions Link and Path Monitoring	Cluster Config
Link Monitoring		
		Enabled 🔽
	Failur	re Condition any
Link Group		
NAME NAME	ENABLED	GROUP FAILURE CONDITION
+ Add Delete		

40. Configure the following:

Parameter	Value		
Name	Type traffic-links		
Enabled	🗹 Enabled	(Note: not supported on VM-Series firewalls	
	on ESXi)		
Failure Condition	Verify that the Any radio button is selected		

Parameter	Value
Interface	Click Add and select the following from the drop-down list:
	ethernet1/1
	ethernet1/2

Link Group	(?)
Name	traffic-links
	🔽 Enabled
Failure Condition	💿 Any i 🔿 All
INTERFACE A	×
ethernet1/1	
ethernet1/2	
🕂 Add 😑 Delet	te

41. Click **OK** to close the **Link Group** configuration window.

42. Click the ⁽¹⁾ icon of the **Path Monitoring** panel to configure path failure detection.

The **Path Monitoring** configuration window should open. Path monitoring enables the firewall to monitor specified destination IP addresses by sending ICMP ping messages to ensure that they are responsive.

43. Configure the following:

Parameter	Value
Enabled	C Enabled
Failure Condition	Verify that the Any radio button is selected

44. Click **OK** to close the **Path Monitoring** configuration window.

Path Monitoring		©
	Enabled 🔽 Failure Condition any	

45. Find the **Path Group** panel and click **Add Logical Router Path** to configure the path failure condition.

The **HA Logical Router Path** configuration window should open.

Note: Path Monitoring should only be used if both FireWalls have two independent network routes were link-monitoring would not cover all failure conditions. In order to avoid HA flapping, it is important to monitor multiple IP addresses and only trigger a failover if all IPs are not reachable.

Pat	h Group								
	NAME	TYPE \checkmark	ENAB	FAILURE	SOURCE IP	DESTINATION IP GROUP	PING INTERVAL (MS)	PING COUNT	
ŧ	• Add Virtual Wire Path • Add VLAN Path • Add Logical Router Path • Delete • Delete • Operation • Operation								

46. Configure the following:

Parameter	Value		
Name	Select LR-1		
Enabled	C Enabled		
Failure Condition	Select the All radio button		
Destination IP Group	Click Add and create reachable IPs destination IP		
	group		
Destination IP	Click Add and type 8.8.8.8		
	Click Add and type 8.8.4.4		
	Click Add and type 1.1.1.1		
	Click OK		
Ping Interval	Change from 200 to 1000 as a ping every 200ms is quite aggressive		

HA Path Group Logical Router				
Name	LR-1		~	
	Enabled			
Failure Condition	🔾 Any 🛛 O All			
Ping Interval	1000			
Ping Count	10			
Q			1 item \rightarrow \times	
DESTINATION GROUP	IP DESTINATION IP	ENABLED	FAILURE	
reachable IPs	8.8.8.8 8.8.4.4 1.1.1.1		any	

- 47. Click **OK** to close the **HA Path Group Logical Router** configuration window.
- 48. **Commit** all changes.

14.5 Observe the Behavior of the HA Widget

49. In the web interface, click the **Dashboard** tab and view the **High Availability** status widget for the firewall.

Active/passive mode should be enabled, and the local firewall should be active (green). You may need to refresh the **High Availability** pane if the local firewall still shows that it is initializing. However, because there is no peer firewall, the status of most monitored items is unknown (yellow). Because HA1 has no peer, its state is down (red):



50. If a peer was configured and was operating in passive mode, the **High Availability** widget on the **Dashboard** would display as follows:



To avoid overwriting the wrong firewall configuration, the firewalls are not automatically synchronized. You must manually synchronize a firewall to the firewall with the "valid" configuration by clicking **Sync to peer**.



Stop. This is the end of the Active/Passive High Availability lab.

Appendix C - Site-to-Site VPN



Lab Objectives

- Create and configure a tunnel interface to use in the site-to-site VPN connection.
- Configure the IKE gateway and IKE Crypto Profile.
- Configure the IPsec Crypto Profile and IPsec tunnel.
- Test connectivity.

12.0 Load a Lab Configuration

To start this lab exercise, you will load a preconfigured firewall configuration file.

- 1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
- 2. Click Load named configuration snapshot:

Configuration Management

Revert	Revert to last saved configuration
	Revert to running configuration
Save	Save named configuration snapshot
	Save candidate configuration
Load	Load named configuration snapshot
	Load configuration version
Export	Export named configuration snapshot
	Export configuration version
	Export device state
Import	Import named configuration snapshot
	Import device state

A Load Named Configuration dialog box opens.

3. Click the drop-down arrow next to the Name field and select edu-210-11.1a-14.xml.

Note: Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers.

Load Name	ed Configuration	?
Name	edu-210-11.1a-14.xml	\sim
Decryption Key	0000	\sim
	Regenerate Rule UUIDs for selected named configuration Skip Validation	

4. Click **OK** to close the **Load Named Configuration** window.

A window should open that confirms that the configuration is being loaded.

- 5. Click **Close** to close the **Loading Configuration** window.
- 6. Click the **Commit** link at the upper right of the web interface:



A **Commit** window should open.

7. Click **Commit** and wait until the commit process is complete.

Cancel

A **Commit Status** window should open that confirms that the configuration was committed successfully.

8. Click **Close** to continue.

12.1 Configure the Tunnel Interface

- 9. In the web interface, select **Network > Interfaces**.
- 10. Click the **Tunnel** tab.
- 11. Click **Add** to configure a tunnel interface:

Parameter	Value					
Interface Name	In the text box to the right of tunnel , type 15					
Comment	Type Tunnel to DMZ					
Logical Router	Select LR-1 from the drop-down list					
Security Zone	Create and assign a new Layer 3 zone named VPN New Zone					

Tunnel Interface		?
Interface Name	unnel	. 15
Comment	iunnel to DMZ	
Netflow Profile	None	\sim
Config IPv4 IP	6 Advanced	
Logical Router	LR-1	×
Security Zone	VPN	~

- OK Cancel
- 12. Click **OK** to close the **Tunnel Interface** configuration window.

12.2 Configure the IKE Gateway

- 13. In the web interface, select **Network > Network Profiles > IKE Gateways**.
- 14. Click **Add** to create the gateway.

The IKE Gateway configuration window should open.

15. Configure the following:

Parameter	Value
Name	Type dmz-ike-gateway
Version	Verify that IKEv1 only mode is selected
Interface	Select ethernet1/3 from the drop-down list
Local IP Address	Select 192.168.50.1/24 from the drop-down list
Peer IP Address Type	Verify that the IP radio button is selected
Peer Address	Type 192.168.50.10
Pre-shared Key	Type paloalto

IKE Gateway		(D
General Advanced	Options		
Name	dmz-ike-gateway		
Version	IKEv1 only mode	~	
Address Type	o IPv4 ○ IPv6		
Interface	ethernet1/3	~	
Local IP Address	192.168.50.1/24	~	
Peer IP Address Type	💿 IP 🔿 FQDN 📄 Dynamic		
Peer Address	192.168.50.10	~	
Authentication	● Pre-Shared Key ○ Certificate		
Pre-shared Key	•••••		
Confirm Pre-shared Key	•••••		
Local Identification	None 🗸]
Peer Identification	None 🗸]
Comment			ן
		OK Cancel	

16. Click the Advanced Options tab.

17. On the **IKEv1** subtab configure the following:

Parameter	Value
IKE Crypto Profile	Select New 🔒 IKE Crypto Profile

The IKE Crypto Profile configuration window should open.

IKE Gateway		0
General Advanced	Options	
Common Options		
Enable Passive M	lode	
Enable NAT Trave	ersal	
IKEv1		
Exchange Mode	auto	
IKE Crypto Profile	default	~
	default	
🗸 🗸 Dead Peer Detectio	Suite-B-GCM-128	
Interval	Suite-B-GCM-256	
Retry	New 🔒 IKE Crypto Profile	

OK Cancel

18. Configure the following IKE Crypto Profile values:

Parameter	Value
Name	Type AES256-DH2-SHA256
DH Group	Click Add and select group 2 from the drop-down list
Authentication	Click Add and select sha256 from the drop-down list
Encryption	Click Add and select aes-256-cbc from the drop-down list

IKE Crypto Profile	0
Name AES256-DH2-SHA256	
DH GROUP	ENCRYPTION
group2	aes-256-cbc
↔ Add	
AUTHENTICATION	Timers
sha256	Key Lifetime Hours 🗸
	8
	Minimum lifetime = 3 mins
⊖ Add ⊖ Delete ↑ Move Up ↓ Move Down	IKEv2 Authentication 0 Multiple

19. Click **OK** to close the **IKE Crypto Profile** configuration window.

20. Click **OK** to close the **IKE Gateway** configuration window.

A new IKE gateway should display in the web interface.

		Loca	al Address	Pe	eer ID	Lo	cal ID		IKE Advanced Options					
NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION	MODE	PASSIVE MODE	NAT TRAVERSAL	CRYPTO PROFILE	DPD	
dmz-ike-gateway	192.168.50.10	ethernet1/3	192.168.50.1/24					ikev1	auto			AES256-DH2-SHA256	enabled/default/default	

12.3 Create an IPSec Crypto Profile

- 21. In the web interface, select Network > Network Profiles > IPSec Crypto.
- 22. Click **Add** to open the configuration window.

The **IPSec Crypto Profile** configuration window should open.

23. Configure the following:

Parameter	Value
Name	Type AES256-DH2-SHA256
IPSec Protocol	Verify that ESP is selected
Encryption	Click Add and select aes-256-cbc from the drop-down list
Authentication	Click Add and select sha256 from the drop-down list
DH Groups	Verify that group2 is selected

Cancel

IPSec Crypto P	Profile						?
Name	AES256-DH2-SHA256						
IPSec Protocol	ESP 🗸	DH Group	group	2			\sim
ENCRYPTION		Lifetime	Hours		~	1	
aes-256-cbc			Minimur	n lifetime =	3 mi	ins	
		C Enable —					
		Lifesiz	e MB		\sim	[1 - 65535]	
			Recon			is 100MB or greater	
		· · · · · · · · · · · · · · · · · · ·					
🕀 Add 😑 Dele	te ↑ Move Up 👃 Move Down						
	ION						
sha256							
🕂 Add 🖂 Dele	te ↑ Move Up ↓ Move Down						
		1					

OK Cancel

24. Click **OK** to close the **IPSec Crypto Profile** configuration window.

A new IPsec Crypto Profile should display in the web interface.

	NAME	ESP/AH	ENCRYPTION	AUTHENTICATION	DH GROUP	LIFETIME
	default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours
	Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours
	Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours
\checkmark	AES256-DH2-SHA256	ESP	aes-256-cbc	sha256	group2	1 hours

12.4 Configure the IPsec Tunnel

- 25. In the web interface, select **Network > IPSec Tunnels**.
- 26. Click **Add** to define a new tunnel.

The IPSec Tunnel configuration window should open.

27. On the **General** tab configure the following:

Parameter	Value
Name	Type dmz-tunnel
Tunnel Interface	Select tunnel.15 from the drop-down list
Туре	Verify that the Auto Key radio button is selected

Parameter	Value
Address Type	Verify that the IPv4 radio button is selected
IKE Gateway	Select dmz-ike-gateway from the drop-down list
IPSec Crypto Profile	Select AES256-DH2-SHA256 from the drop-down list

IPSec Tunnel		?
General Proxy	y IDs	
Name	dmz-tunnel	
Tunnel Interface	tunnel.15	\sim
Туре	오 Auto Key 🔿 Manual Key 🔿 GlobalProtect Satellite	
Address Type	S IPv4 ○ IPv6	
IKE Gateway	dmz-ike-gateway	\sim
IPSec Crypto Profile	AES256-DH2-SHA256	\sim
	Show Advanced Options	
Comment		



- 28. Click the **Proxy IDs** tab.
- 29. Click **Add** and configure the following:

Parameter	Value
Proxy ID	Type dmz-tunnel-network
Local	Type 192.168.1.0/24
Remote	Type 172.16.2.0/24
Protocol	Verify that Any is selected

Proxy ID		?
Proxy ID	dmz-tunnel-network	
Local	192.168.1.0/24	
	IP Address or IP/netmask, only needed when peer requires it.	
Remote	172.16.2.0/24	
	IP Address or IP/netmask, only needed when peer requires it.	
Protocol	Any	\sim

- 30. Click **OK** to close the **Proxy ID** configuration window.
- 31. Click **OK** to close the **IPSec Tunnel** configuration window:

			IKE Gateway/Satellite				Tunnel Interface				
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	LOGICAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS
dmz-tunnel	Tunnel Info	Auto Key	ethernet1/3	192.168.50.1/24	192.168.50.10	IKE Info	tunnel.15	LR-1 (Show Routes)	vsys1	VPN	

A new IPsec tunnel should display in the web interface.

32. Commit all changes.

12.5 Test the Connectivity

33. In the web interface, select **Network > IPSec Tunnels**:

		IKE Gateway/Satellite				Tunnel Interface					
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	LOGICAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS
dmz-tunnel	Tunnel Info	Auto Key	ethernet1/3	192.168.50.1/24	192.168.50.10	IKE Info	tunnel.15	LR-1 (Show Routes)	vsys1	VPN	m

A red **Status** column indicator on the VPN tunnel means that the VPN tunnel is not connected.

34. Refresh G the **Network > IPSec Tunnels** page.

The **Status** column indicators now are green, which means that the VPN tunnel is connected:

			IKE Gateway/Satellite				Tunnel Interface				
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	LOGICAL ROUTER	VIRTUAL SYSTEM	SECURITY ZONE	STATUS
dmz-tunnel	Tunnel Info	Auto Key	ethernet1/3	192.168.50.1/24	192.168.50.10	IKE Info	tunnel.15	LR-1 (Show Routes)	vsys1	VPN	

35. In the web interface, select **Monitor** > **Logs** > **System**.

36. Review the **VPN** log entries:

To display only VPN entries, you can click **vpn** in the **Type** column to add a filter:

Q (subtype eq 'vpn')								
SEVERITY	RECEIVE TIME	TYPE	EVENT	DESCRIPTION				
informational	09/21 15:57:38	vpn	ipsec-key-install	IPSec key installed. Installed SA: 192.168.50.1[500]-192.168.50.10[500] SPI:0xB4DDB92A/0xC3F33E80 lifetime 3600 Sec lifesize unlimited.				
informational	09/21 15:57:38	vpn	ike-nego-p2-succ	IKE phase-2 negotiation is succeeded as responder, quick mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x697AF75C, SPI:0xB4DDB92A/0xC3F33E80.				
informational	09/21 15:57:38	vpn	ike-nego-p2-start	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 192.168.50.1[500]-192.168.50.10[500] message id:0x697AF75C.				
informational	09/21 15:57:38	vpn	ike-nego-p1-succ	IKE phase-1 negotiation is succeeded as responder, main mode. Established SA: 192.168.50.1[500]-192.168.50.10[500] cookie:06e4ac57823e8d11:96d42d87707a07e9 lifetime 28800 Sec.				
informational	09/21 15:57:38	vpn	ike-nego-p1-start	IKE phase-1 negotiation is started as responder, main mode. Initiated SA: 192.168.50.1[500]-192.168.50.10[500] cookie:06e4ac57823e8d11:96d42d87707a07e9.				
informational	09/21 15:56:44	vpn	ike-config-p2-success	IKE daemon configuration load phase-2 succeeded.				
informational	09/21 15:56:31	vpn	ike-config-p1-success	IKE daemon configuration load phase-1 succeeded.				
informational	09/21 15:38:34	vpn	ike-config-p2-success	IKE daemon configuration load phase-2 succeeded.				

- 37. On the client desktop, open the **Remmina** application.
- 38. Double-click the entry for **Firewall-A**:

			Ren	mina Ren Remote	note Desktop Client Desktop Client
	RDP 🔻				
Name	-	Group	Server	Plugin	Last used
Berlin-Client			192.168.1.25	SSH	2023-02-18 - 15:12:09
BestPractice	Firewall-A		192.168.1.254	SSH	2023-01-14 - 15:04:51
BestPractice	Panorama		192.168.1.252	SSH	2023-01-14 - 18:54:28
Expedition			192.168.1.200	SSH	2023-02-18 - 14:54:37
🔒 Firewall-A			192.168.1.254	SSH	2024-09-21 - 11:25:28
🔒 Firewall-B			192.168.1.253	SSH	2024-08-31 - 15:03:28
🔒 Panorama			192.168.1.252	SSH	2024-08-31 - 17:11:35
🔒 Server-Extranet			192.168.50.10	SSH	2024-09-21 - 12:46:54

39. After the VPN tunnel is connected, type the following CLI commands and observe the output:

show vpn ike-sa
show vpn ipsec-sa tunnel dmz-tunnel:dmz-tunnel-network
show vpn flow name dmz-tunnel:dmz-tunnel-network
show running tunnel flow

- 40. Type exit to close the Remmina connection to the firewall.
- 41. Close the Remmina desktop application window.



Stop. This is the end of the Site-to-Site VPN lab.