



PALO ALTO NETWORKS EDU 210

Lab 5: Configuring Security Policy Rules and NAT Rules

Document Version: **2022-07-18**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology.....	4
Theoretical Lab Topology.....	4
Lab Settings.....	5
1 Configuring Security Policy and NAT Rules.....	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Create a Security Policy Rule	10
1.3 Modify Security Policy Table Columns	15
1.4 Test New Security Policy Rule	17
1.5 Examine and Reset the Rule Hit Count.....	19
1.6 Examine the Traffic Log	22
1.7 Create Security Rules for Internet Access	27
1.8 Ping Internet Host from Client	36
1.9 Create a Source NAT Policy	37
1.10 Create a Destination NAT Policy.....	44

Introduction

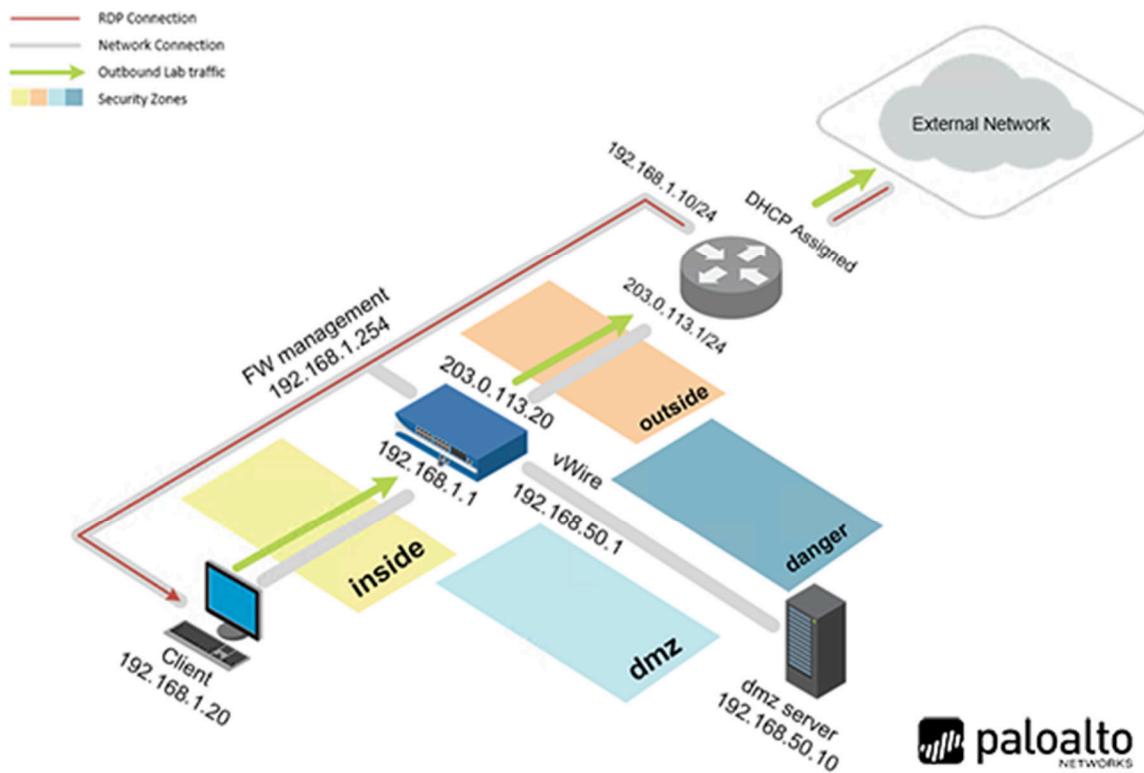
In this lab, you will allow network traffic from the Users_Net security zone to the Extranet security zone so that employees can access various business applications. You will create, modify, and test a security policy rule to allow access between these two zones. Once your rule is successfully in place, you will examine hit counters in the security policy rule table and examine the Traffic Log. Next, you will create security policy rules to allow hosts in your network to access the internet. You will then create source and destination NAT policy rules.

Objective

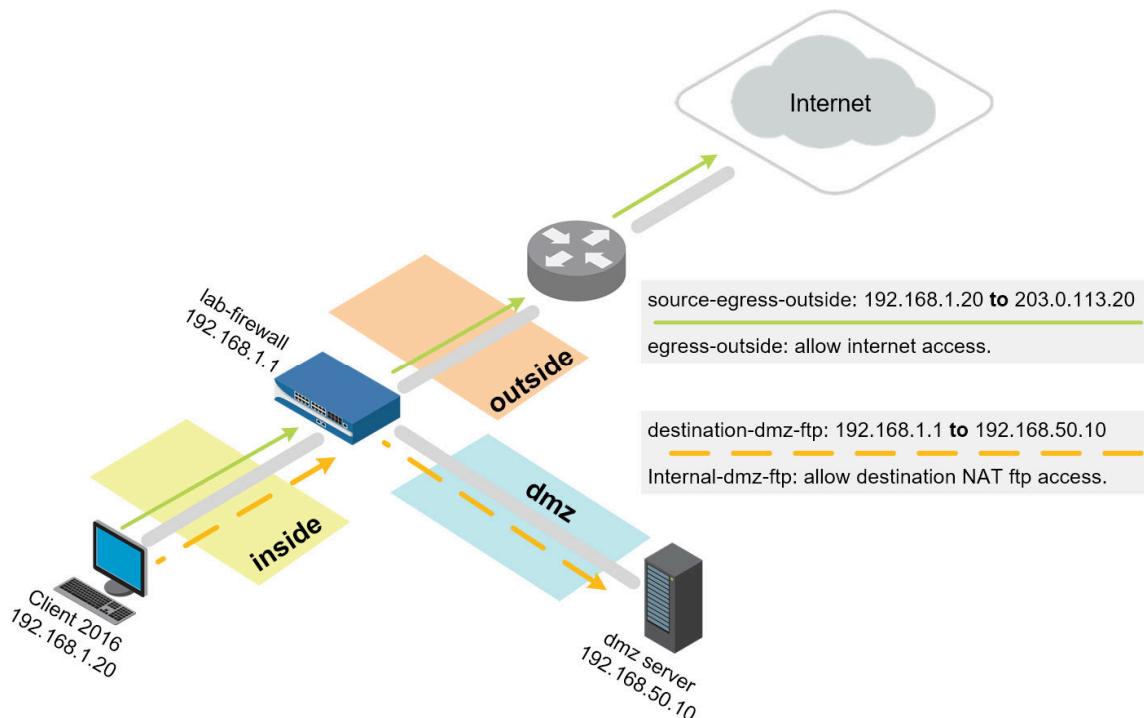
In this lab, you will perform the following tasks:

- Apply a baseline configuration to the firewall
- Create and test a security policy rule
- Modify security policy table columns
- Examine and reset the Rule Hit Count
- Examine the Traffic Log
- Create security rules for internet access
- Ping the internet host from the client
- Create source and destination NAT Policies

Lab Topology



Theoretical Lab Topology



Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

1 Configuring Security Policy and NAT Rules

1.1 Apply a Baseline Configuration to the Firewall

In this section, you will load the firewall configuration file.

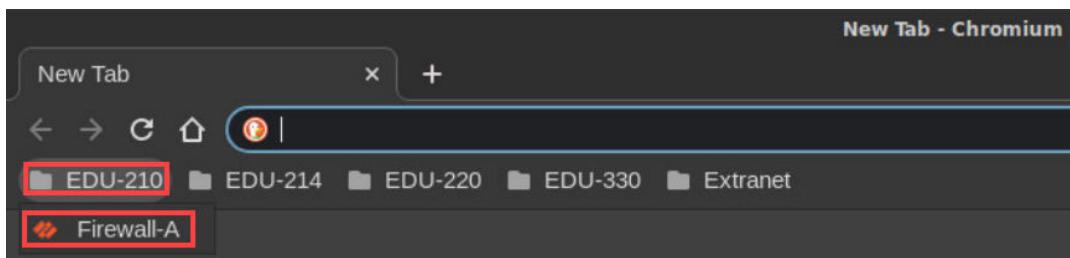
1. Click on the **Client** tab to access the Client PC.



2. Double-click the **Chromium Web Browser** icon located on the desktop.



3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.



4. You will see a "Your connection is not private" message. Next, click on the **ADVANCED** link.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Advanced](#)

[Back to safety](#)



If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

5. Click on **Proceed to 192.168.1.254 (unsafe)**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Hide advanced](#)

[Back to safety](#)

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.254 \(unsafe\)](#)

6. Log in to the firewall web interface as username **admin**, password **PaloAlto!**.

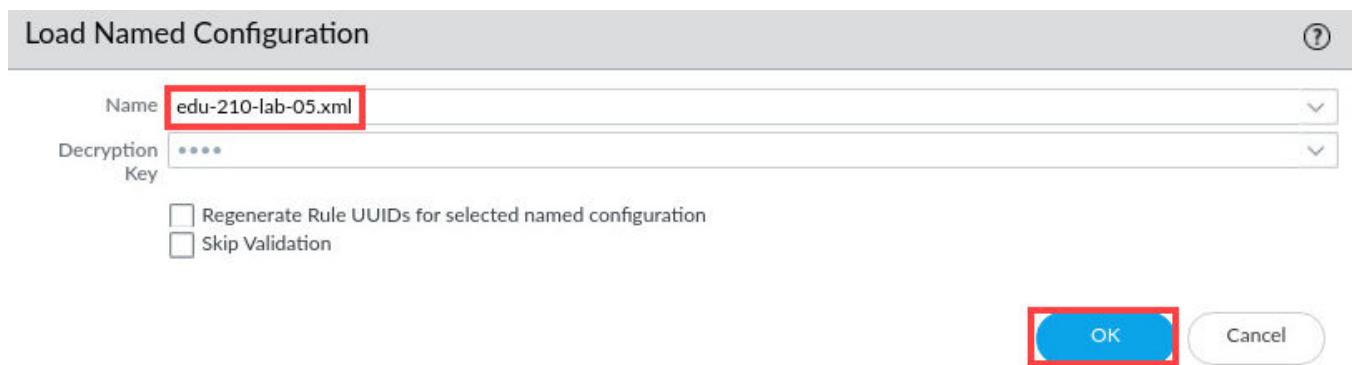


The screenshot shows the login interface for a Palo Alto Networks device. The URL in the address bar is `http://192.168.1.254`. The page features a yellow header bar with the text "Palo Alto Networks". Below this is a login form with two fields: a "Username" field containing "admin" and a "Password" field containing redacted text. At the bottom is a blue "Log In" button.

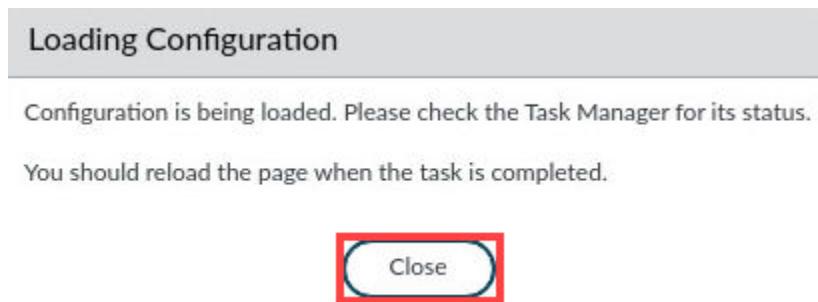
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE link is highlighted with a red box. On the left, a sidebar menu is open, showing options like Setup (highlighted with a red box), High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area is titled 'Configuration Management'. It contains several buttons: 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). The 'Load named configuration snapshot' button is highlighted with a red box.

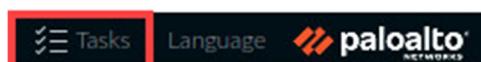
8. In the *Load Named Configuration* window, select **edu-210-lab-05.xml** from the *Name* dropdown box and click **OK**.



9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



10. Click the **Tasks** icon located at the bottom-right of the web interface.



11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show **All Tasks** Clear Commit Queue **Close**

12. Click the **Commit** link located at the top-right of the web interface.



13. In the *Commit* window, click **Commit** to proceed with committing the changes.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

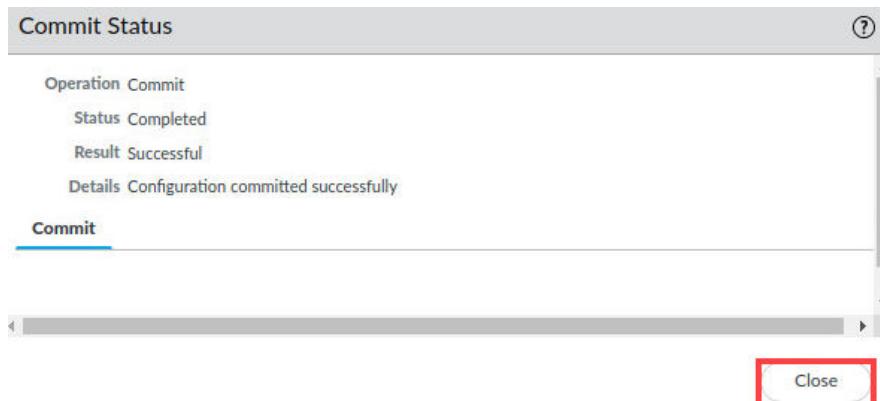
Preview Changes **Change Summary** **Validate Commit** Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

14. When the *Commit* operation successfully completes, click **Close** to continue.



 The commit process takes changes made to the firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 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

1. In the web interface, select **Policies > Security**. Click **Add**.

The screenshot shows the 'Security' tab selected in the left sidebar. The main area displays two security policy rules:

NAME	TAGS	TYPE	Source				Destination				APPLI
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
1 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	
2 interzone-default	none	interzone	any	any	any	any	any	any	any	any	

At the bottom of the table, there is a toolbar with buttons for Object : Addresses, + Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, View Rulebase as Groups, and Reset Rule Hit Counter.

2. In the *Security Policy Rule* window, on the *General* tab. Type **Users-to-Extranet** for the *Name*. For *Description*, enter **Allows hosts in Users_Net zone to access servers in Extranet zone.**

Security Policy Rule

General Source | Destination | Application | Service/URL Category | Actions | Usage

Name	Users-to-Extranet
Rule Type	universal (default)
Description	Allows hosts in Users_Net zone to access servers in the Extranet zone.

3. Select the **Source** tab. Under the *Source Zone* section, click **Add**, and select **Users_Net**.

Security Policy Rule

General **Source** Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/>  Users_Net	
+ Add	- Delete

4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add** and select **Extranet**.

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions

select	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> DESTINATION ZONE	<input type="checkbox"/> DESTINATION ADDRESS
<input checked="" type="checkbox"/> Extranet	
+ Add	- Delete
+ Add	- Delete

5. Select the **Application** tab. Verify **Any** is selected for *Applications*.

Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions

<input checked="" type="checkbox"/> Any
<input type="checkbox"/> APPLICATIONS

6. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service*, and **Any** is selected for *URL Category*.

Security Policy Rule

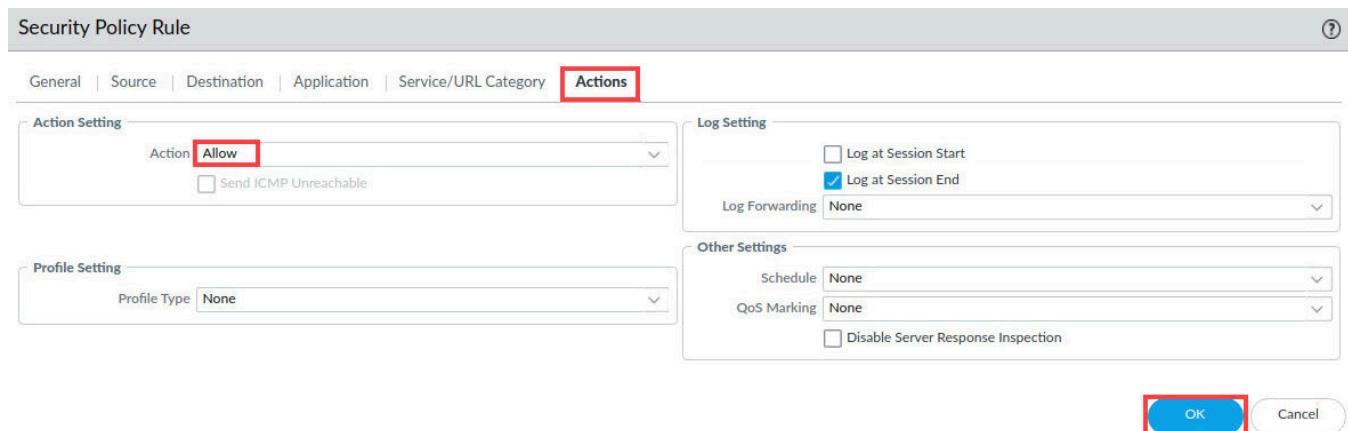
General | Source | Destination | Application | **Service/URL Category** | Actions

application-default	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SERVICE	<input type="checkbox"/> URL CATEGORY



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.

7. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default. Click **OK**.

**Please Note**

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.

8. Verify the *Users to Extranet* security policy rule appears in the *Security Policies* window.

NAME	TAGS	Source			Destination	
		ZONE	ADDRESS	USER	ADDRESS	ZONE
1 Users-to-Extranet	none	Users_Net	any	any	any	Extranet
2 intrazone-default	none	any	any	any	any	(intrazone)
3 interzone-default	none	any	any	any	any	any

Please Note

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

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



10. In the *Commit* window, click **Commit**.

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

Preview Changes Change Summary Validate Commit Group By Location Type

Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit.

Description

Commit **Cancel**

11. Wait until the *Commit* process is complete. Click **Close**.

Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

Commit

Close

12. Leave the web interface open and continue to the next task.

1.3 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.

- In the *Security Policy* window, click the **small dropdown** icon next to the *Name* column in the *Security Policy* table. You may need to hover your pointer over the icon for it to appear.

	NAME	TAGS
1	Users-to-Extranet	none
2	intrazone-default	none
3	interzone-default	none

Please Note

This icon is available next to all column headers.

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

	NAME	TAGS	TYPE	ZONE	ADDRESS
1	Users-to-Extranet				
2	intrazone-default	none	interzone		
3	interzone-default	none	interzone		

Columns

Adjust Columns

- Name
- Tags
- Group
- Type
- Source Zone
- Source Address
- Source User
- Source Device
- Destination Address
- Destination Device
- Destination Zone
- Application
- Service
- URL Category
- Action
- Profile
- Options
- Rule UUID
- Rule Usage Description
- Rule Usage Hit Count
- Rule Usage Last Hit
- Rule Usage First Hit
- Rule Usage Apps Seen
- Days with No New Apps
- Modified
- Created

Please Note

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

3. In the *Columns*, uncheck **Type**, **Source Device**, **Destination Device**, and **Options**.

1	Users-to-Extranet	Columns >		Adjust Columns									
2	intrazone-default			<input checked="" type="checkbox"/> Name <input checked="" type="checkbox"/> Tags <input type="checkbox"/> Group <input type="checkbox"/> Type <input checked="" type="checkbox"/> Source Zone <input checked="" type="checkbox"/> Source Address <input checked="" type="checkbox"/> Source User <input type="checkbox"/> Source Device <input checked="" type="checkbox"/> Destination Address <input type="checkbox"/> Destination Device <input checked="" type="checkbox"/> Destination Zone <input checked="" type="checkbox"/> Application <input checked="" type="checkbox"/> Service <input type="checkbox"/> URL Category <input checked="" type="checkbox"/> Action <input checked="" type="checkbox"/> Profile <input type="checkbox"/> Options <input type="checkbox"/> Rule UUID									
3	interzone-default	none	any										

Please 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.

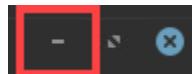
4. At the top of the *Name* column, click the **dropdown** icon again and choose **Adjust Columns**.

NAME	TAGS	ZONE	Source			Destination			APPLICATION	SERVICE
			ADDRESS	USER	ADDRESS	ZONE				
1 Users-to-Extranet			Net	any	any	any	Extranet	any	application-default	
2 intrazone-default				any	any	(intrazone)	any	any		
3 interzone-default	none	any		any	any	any	any	any		

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

NAME	TAGS	Source			Destination			APPLICATION...	SERVICE	ACTION	PROFILE	Rule Usage		
		ZONE	ADDRESS	USER	ADDRESS	ZONE	APPLICATION...					HIT COUNT	LAST HIT	FIRST HIT
1 Users-to-Extranet	none	Users_Net	any	any	any	Extranet	any	application-default	Allow	none	1166	2021-08-06 23:14:...	2021-08-06 22:49:...	
2 intrazone-default	⊗	any	any	any	any	(intrazone)	any	any	Allow	none	2702	2021-08-06 23:11:...	2020-02-27 02:30:...	
3 interzone-default	⊗	any	any	any	any	any	any	Deny	none	10594	2021-08-06 23:14:...	2020-02-27 19:18:...		

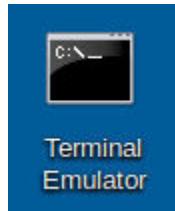
6. Minimize the PA-VM firewall by clicking the **minimize** icon in the upper-right of the web interface and continue to the next task.



1.4 Test New Security Policy Rule

In this section, you will test the new security policy rule you created in a previous task.

1. Open the **Terminal Emulator** on the *client desktop*.



2. Issue the following command below to ensure your security policy rule is functioning correctly.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80
```

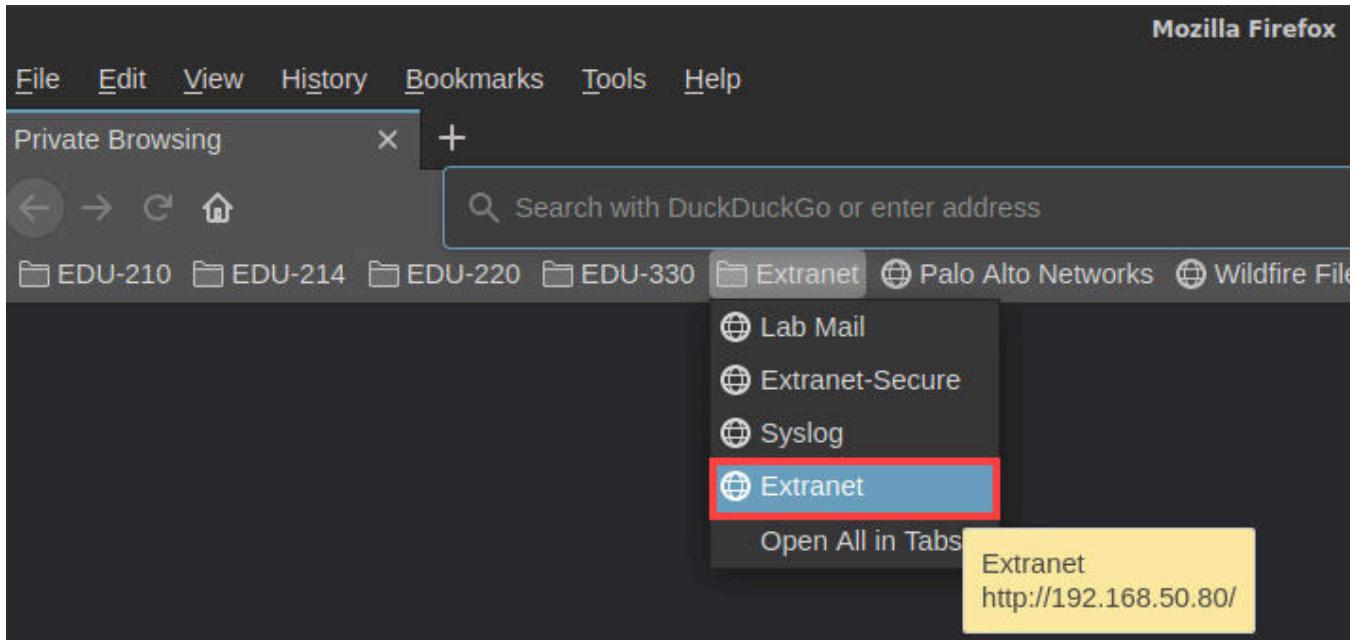
3. Wait a few seconds and use **Ctrl+C** to stop the command. If you see a reply from 192.168.50.80, then your security policy rule is configured correctly! If not, review the previous steps and try this test again.

```
PING 192.168.50.80 (192.168.50.80) 56(84) bytes of data.  
64 bytes from 192.168.50.80: icmp_seq=2 ttl=63 time=0.691 ms  
64 bytes from 192.168.50.80: icmp_seq=3 ttl=63 time=0.703 ms  
64 bytes from 192.168.50.80: icmp_seq=4 ttl=63 time=0.583 ms  
^C  
--- 192.168.50.80 ping statistics ---  
4 packets transmitted, 3 received, 25% packet loss, time 3058ms  
rtt min/avg/max/mdev = 0.583/0.659/0.703/0.053 ms  
C:\home\lab-user\Desktop\Lab-Files>
```

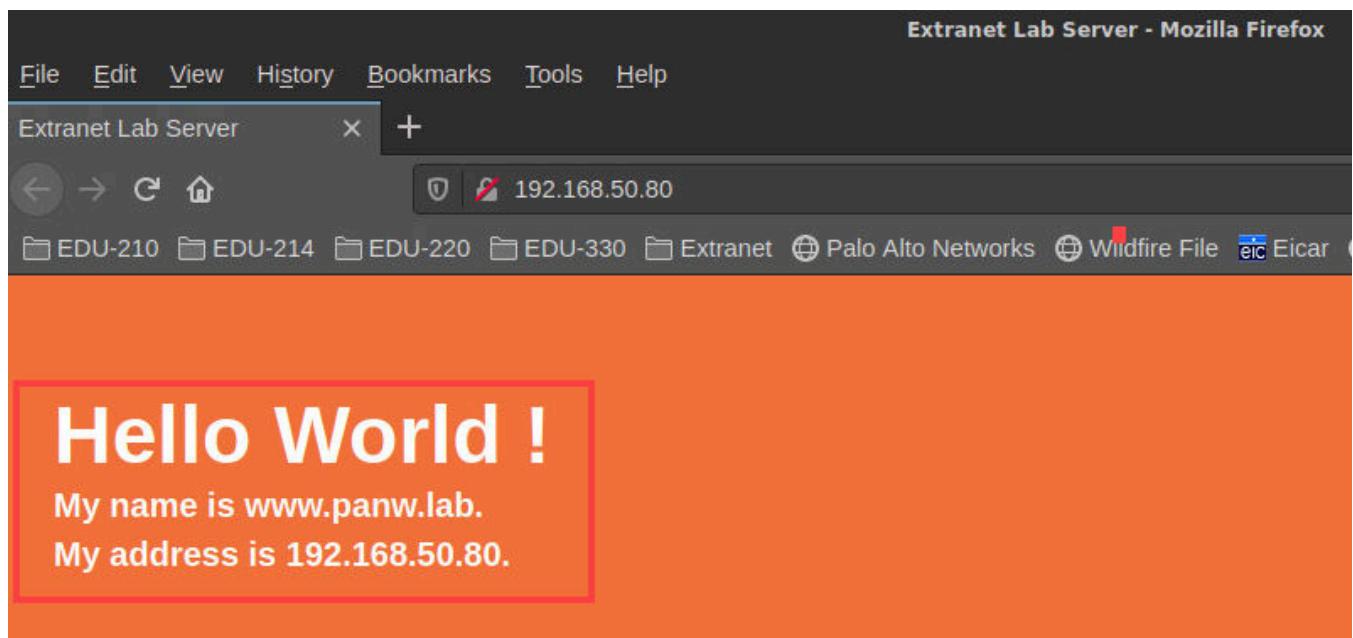
4. On the *client desktop*, double-click the **Firefox** browser to open it.



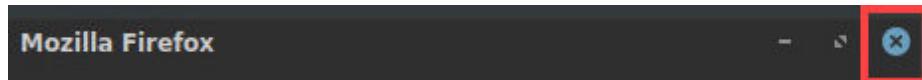
5. Use the *Bookmark bar* and select **Extranet > Extranet**.



6. You should see a *webpage* displayed by the server. If you are seeing **Hello World !**, you have properly configured the security policy.



7. Close the *Firefox* browser. Click the **close** icon in the upper-right.



8. Reopen the *PA-VM firewall* interface by clicking the **Chromium** icon in the taskbar.



9. Leave the terminal and firewall web interface open and continue to the next task.

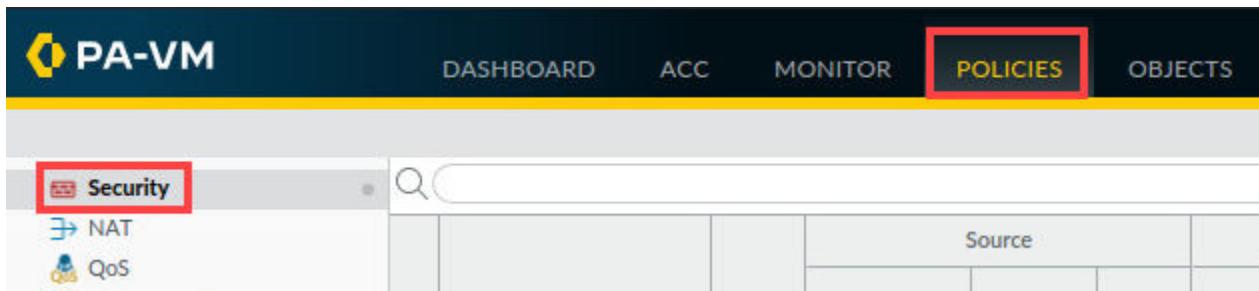
1.5 Examine and Reset the Rule Hit Count

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.

Rule hit counts are very useful to track whether 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 examine and reset the counters for the **Users_to_Extranet** rule.

- In the firewall interface, select **Policies > Security**.



- In the *Security Policies* window, scroll to the right and locate the column for **Hit Count**. Note the number of hits on the Users to Extranet Rule. For this lab, there were **1166** hits. You may get different results, but the conclusion will be the same.

NAME	TAGS	ZONE	Rule Usage			
			ACTION	PROFILE	HIT COUNT	LAST HIT
1 Users-to-Extranet	none	Users_Extranet	Allow	none	1166	2021-08-06 23:14:...
2 intrazone-default	none	any	Allow	none	2702	2021-08-06 23:11:...
3 interzone-default	none	any	Deny	none	10594	2021-08-06 23:14:...

- Return to the terminal window by clicking on the **terminal** icon in the taskbar of your *client desktop*.



- In the CLI connection to the firewall, use the **ping** command to check network connectivity to the panw.lab server. Notice the ping was successful. Wait a few seconds and use **Ctrl+C** to stop the command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80 <Enter>
```

```
Terminal
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.80
PING 192.168.50.80 (192.168.50.80) 56(84) bytes of data.
64 bytes from 192.168.50.80: icmp_seq=1 ttl=63 time=0.566 ms
64 bytes from 192.168.50.80: icmp_seq=2 ttl=63 time=0.721 ms
64 bytes from 192.168.50.80: icmp_seq=3 ttl=63 time=0.669 ms
^C
--- 192.168.50.80 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.566/0.652/0.721/0.064 ms
C:\home\lab-user\Desktop\Lab-Files>
```

5. Return to the *PA-VM firewall* interface and update the security policy rules table by clicking the **Refresh** button in the upper-right corner of the window. Notice the increase in the *Hit Count* for the **Users to Extranet** security policy rule has increased.

	NAME	TAGS	ZONE	Rule Usage				
				ACTION	PROFILE	HIT COUNT	LAST HIT	FIRST HIT
1	Users-to-Extranet	none	Users	<input checked="" type="checkbox"/> Allow	none	1757	2021-08-06 23:28:...	2021-08-06 22:49:...
2	intrazone-default	none	any	<input checked="" type="checkbox"/> Allow	none	2724	2021-08-06 23:23:...	2020-02-27 02:30:...
3	interzone-default	none	any	<input type="checkbox"/> Deny	none	11260	2021-08-06 23:29:...	2020-02-27 19:18:...

6. Highlight the **Users to Extranet** security policy rule. But do not open it.

	NAME	TAGS	ZONE	Source			Destination		APPLICATI...
					ADDRESS	USER	ADDRESS	ZONE	
1	Users-to-Extranet	none	Users_Net	any	any	any	any	Extranet	any
2	intrazone-default	none	any	any	any	any	any	(intrazone)	any
3	interzone-default	none	any	any	any	any	any	any	any

7. At the bottom of the *security policy* rules window, select **Reset Rule Hit Counter > Selected rules**.

NAME	TAGS	Source			Destination			APPLICATION...	SERVICE	ACTION	PROFILE	HIT COUNT	LAST HIT	FIRST HIT	APPS SEE
		ZONE	ADDRESS	USER	ADDRESS	ZONE									
1	Users-to-Extranet	none	Users_Net	any	any	any	Extranet	any	application-default	<input checked="" type="checkbox"/> Allow	none	1757	2021-08-06 23:28:...	2021-08-06 22:49:...	3
2	intrazone-default	none	any	any	any	any	(intrazone)	any	any	<input checked="" type="checkbox"/> Allow	none	2724	2021-08-06 23:23:...	2020-02-27 02:30:...	-
3	interzone-default	none	any	any	any	any	any	any	any	<input type="checkbox"/> Deny	none	11260	2021-08-06 23:29:...	2020-02-27 19:18:...	-

8. Notice the *Hit Count* for *Users to Extranet* has been reset to **0**.

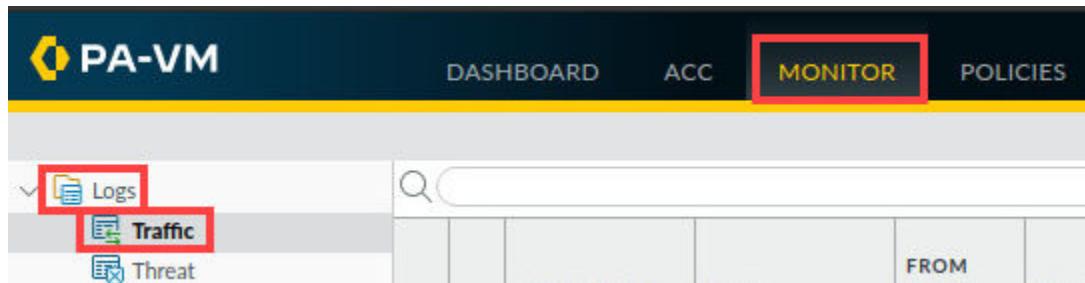
	NAME	TAGS	ZONE	Rule Usage				
				ACTION	PROFILE	HIT COUNT	LAST HIT	FIRST HIT
1	Users-to-Extranet	none	Users_Net	<input checked="" type="checkbox"/> Allow	none	0	-	-
2	intrazone-default	none	any	<input checked="" type="checkbox"/> Allow	none	2724	2021-08-06 23:23:...	2020-02-27 02:30:...
3	interzone-default	none	any	<input type="checkbox"/> Deny	none	11260	2021-08-06 23:29:...	2020-02-27 19:18:...

9. Leave the firewall interface open and continue to the next task.

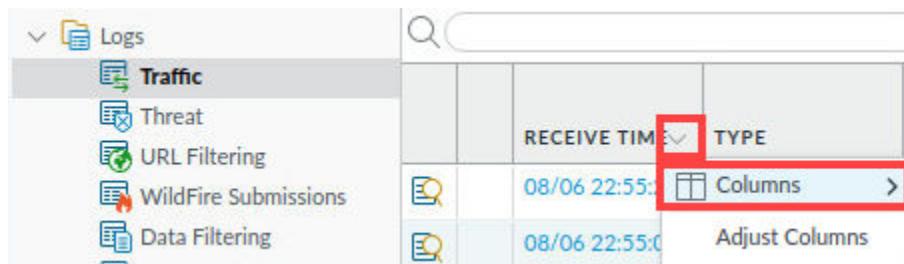
1.6 Examine the Traffic Log

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.

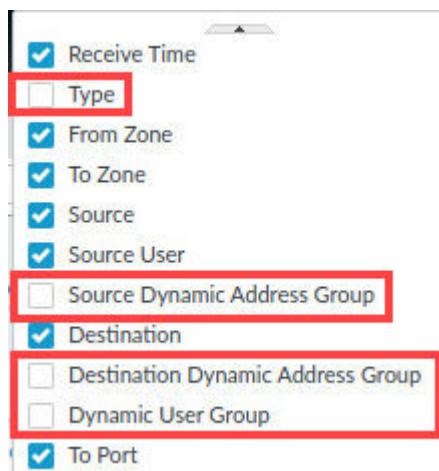
1. In the *firewall* interface, select **Monitor > Logs > Traffic**.



2. Click the dropdown icon next to **Receive Time** and choose **Columns**.



3. Uncheck **Type**, **Source Dynamic Address Group**, **Destination Dynamic Address Group**, and **Dynamic User Group** to hide their columns.



Please Note

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

4. Return to the terminal window by clicking on the terminal icon in the taskbar of your *client desktop*.



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

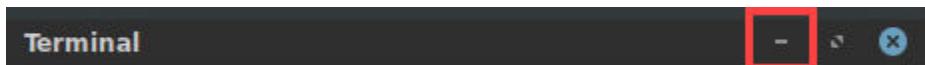
```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8
```

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

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4081ms  
^C:C:\home\lab-user\Desktop\Lab-Files>
```

7. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.



8. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Ensure you are still viewing the *traffic logs*. In the filter field, enter **(addr.dst eq 8.8.8.8) and (zone.src eq Users_Net)**. Click the **Apply Filter** button in the upper-right corner of the window. You will notice the firewall did not log your ping session to an external address. Notice the last successful log was on 09/02 from the *Users_net* to *Internet*. You should not see any entries on the date you complete this lab in this step.

	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	RULE	SESSION END REASON	BYTES
	09/02 22:33:37	Users_Net	Internet	192.168.1	Users_to_Internet	aged-out	203
	09/02 22:33:37	Users_Net	Internet	192.168.1	Users_to_Internet	aged-out	241

Please Note

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.



There are two reasons why the firewall did not log the ping session.

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.

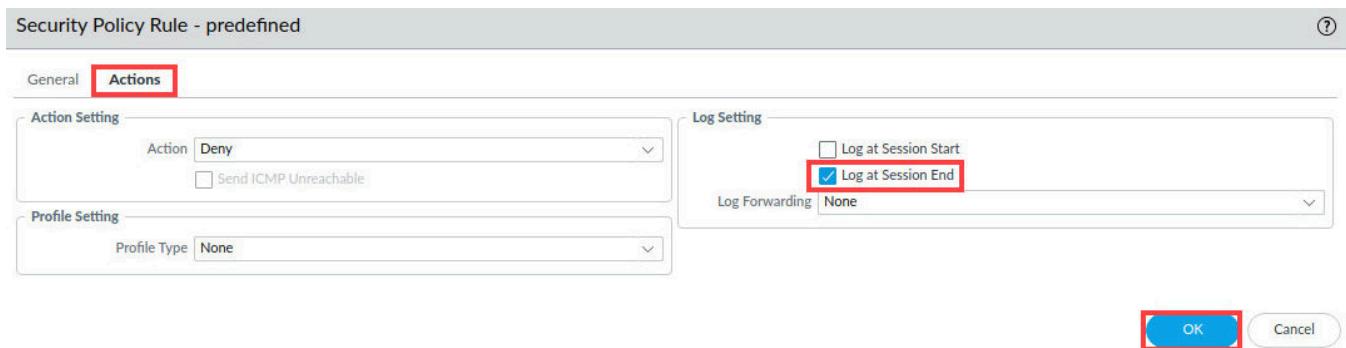
- For the firewall to see the entries in the Traffic log, enable *Log at Session End* in the *interzone-default* rule. Navigate to **Policies > Security**. Highlight the **interzone-default** rule but do not open it.

NAME	TAGS	Source				ADDR
		ZONE	ADDRESS	USER		
1 Users-to-Extranet	none	Users_Net	any	any	any	
2 intrazone-default	none	any	any	any	any	
3 interzone-default	none	any	any	any	any	

- Click the **Override** button at the bottom of the window.



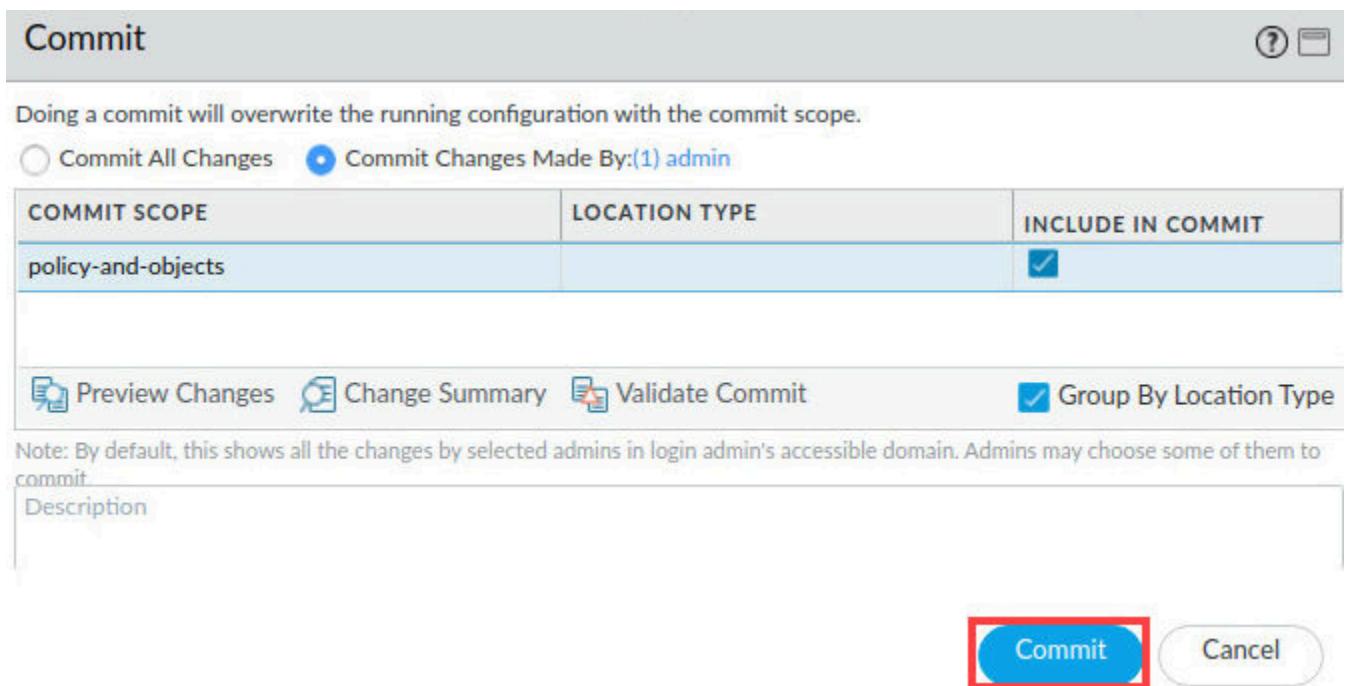
11. In the *Security Policy Rule – predefined* window, click the **Actions** tab. Select **Log at Session End** and click **OK**.



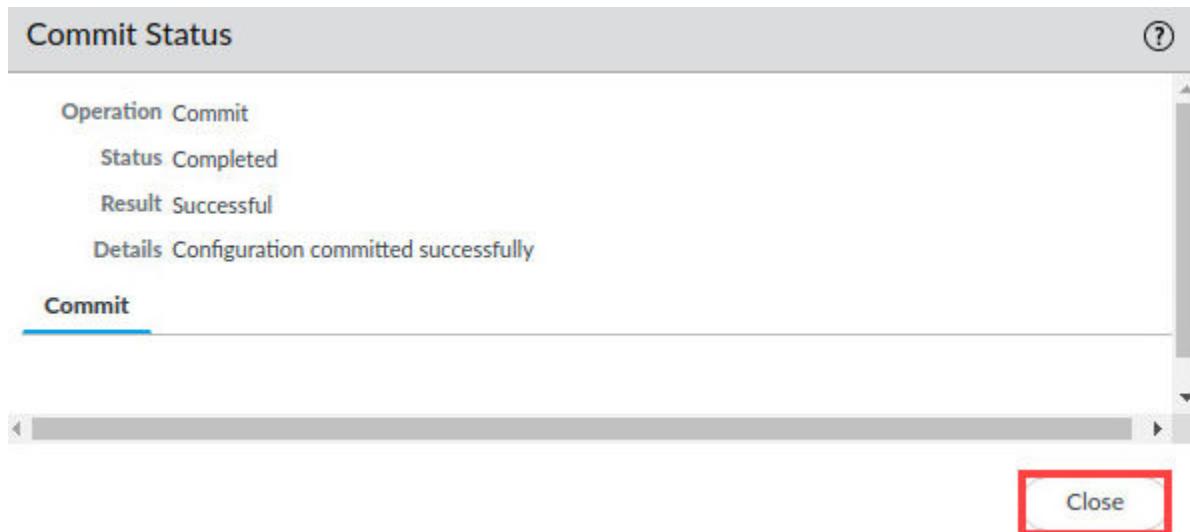
12. Click the **Commit** button at the upper-right of the web interface.



13. In the *Commit* window, click **Commit**.



14. Wait until the *Commit* process is complete. Click **Close**.



15. Return to the terminal window by clicking on the *terminal* icon in the taskbar of your *client desktop*.



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

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8
```

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

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4081ms  
^C:C:\home\lab-user\Desktop\Lab-Files>
```

18. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.



19. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter (`addr.dst eq 8.8.8.8`) and (`zone.src eq Users_Net`). Click the **Apply Filter** button in the upper right corner of the window. You will notice the firewall is now logging entries on the date you complete this step matching your filter.

RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE
09/16 22:47:08	Users_Net	Internet	192.168.1.254
09/16 22:47:07	Users_Net	Internet	192.168.1.20
09/16 22:47:01	Users_Net	Internet	192.168.1.20

RULE	SESSION END REASON	BYTES
interzone-default	policy-denry	0
interzone-default	policy-denry	0
interzone-default	policy-denry	0

20. Leave the web interface open and continue to the next task.

1.7 Create Security 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.

- In the *PA-VM firewall* web interface, navigate to **Policies > Security**. Click **Add** at the bottom of the window.

The screenshot shows the PA-VM firewall's web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), and OBJECTS. On the left, a sidebar menu under the Security section lists various policy types: NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below this is an 'Unused' section showing a count of 0. The main content area displays a table of security policies:

NAME	TAGS	Source				ADDRESS	USER	ADDRESS
		ZONE	ANY	ANY	ANY			
1 Users-to-Extranet	none	Users_Net	any	any	any	any		
2 intrazone-default	none	any	any	any	any	any		
3 interzone-default	none	any	any	any	any	any		

At the bottom of the table, there is a toolbar with buttons for Object : Addresses, + Add, Delete, Clone, Override, Revert, Enable, and Disable. The '+ Add' button is highlighted with a red box.

- In the *Security Policy Rule* window, on the *General* tab. Type **Users-to-Internet** for the *Name*. For *Description*, enter **Allows hosts in Users_Net zone to access Internet zone**.

The screenshot shows the 'Security Policy Rule' configuration window. The 'General' tab is selected (highlighted with a red box). The configuration fields are:

- Name:** Users-To-Internet
- Rule Type:** universal (default)
- Description:** Allows hosts in Users_Net zone to access Internet Zone

3. Select the **Source** tab. Under the *Source Zone* section, click **Add**, and select **Users_Net**.

Security Policy Rule

General **Source** Destination Application Service/URL Category Actions

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> Users_Net	
(+ Add) (- Delete)	(+ Add) (- Delete)

4. Select the **Destination** tab. Under the *Destination Zone* section, click **Add**, and select **Internet**.

Security Policy Rule

General Source **Destination** Application Service/URL Category Actions

select	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> DESTINATION ZONE ^	<input type="checkbox"/> DESTINATION ADDRESS ^
<input checked="" type="checkbox"/> Internet	
(+ Add) (- Delete)	(+ Add) (- Delete)
<input type="checkbox"/> Negate	

5. Select the **Application** tab. Verify **Any** is selected for *Applications*.

Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions

Any

APPLICATIONS ▾

6. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service*, and **Any** is selected for *URL Category*.

Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions

application-default ▾

SERVICE ▾

Any

URL CATEGORY ▾



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.

7. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default. Click **OK**.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action **Allow**

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None

Profile Setting

Profile Type None

Other Settings

Schedule None

QoS Marking None

Disable Server Response Inspection

OK Cancel

Please Note

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.

- Verify the *Users-to-Internet* security policy rule appears in the *Security Policies* window.

NAME	TAGS	Source			Destination	
		ZONE	ADDRESS	USER	ADDRESS	ZONE
1 Users-to-Extranet	none	Users_Net	any	any	any	Extranet
2 Users-To-Internet	none	Users_Net	any	any	any	Internet
3 intrazone-default		any	any	any	any	(intrazone)
4 interzone-default		any	any	any	any	any

- Click **Add** at the bottom of the *Security Policies* window.

NAME	TAGS	Source			Destination	
		ZONE	ADDRESS	USER	ADDRESS	ZONE
1 Users-to-Extranet	none	Users_Net	any	any	any	Extranet
2 Users-To-Internet	none	Users_Net	any	any	any	Internet
3 intrazone-default		any	any	any	any	(intrazone)

Object : Addresses + **+ Add**

10. In the *Security Policy Rule* window, on the *General* tab. Type **Extranet-to-Internet** for the *Name*. For *Description*, enter **Allows hosts in Extranet zone to access Internet zone.**

Security Policy Rule

General Source | Destination | Application | Service/URL Category | Actions

Name	Extranet-to-Internet
Rule Type	universal (default)
Description	Allows host in the Extranet zone to access the Internet zone.

11. Select the **Source** tab. Under the *Source Zone* section, click **Add**, and select **Extranet**.

Security Policy Rule

General Source Destination | Application | Service/URL Category | Actions

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input checked="" type="checkbox"/> Extranet	

(+ Add) (- Delete) (+ Add) (- Delete)

12. Select the **Destination** tab. Under the *Destination Zone* section, click **Add**, and select **Internet**.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. In the 'DESTINATION ZONE' dropdown, the 'Internet' option is highlighted with a red box and checked. Below the dropdown, there are 'Add' and 'Delete' buttons, with 'Add' also highlighted with a red box. To the right, there are sections for 'Any' and 'DESTINATION ADDRESS', both currently empty.

13. Select the **Application** tab. Verify **Any** is selected for *Applications*.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Application' tab selected. The 'Any' checkbox under the 'APPLICATIONS' dropdown is checked and highlighted with a red box. Below the dropdown, there are 'Add' and 'Delete' buttons.

14. Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service*, and **Any** is selected for *URL Category*.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Service/URL Category' tab selected. The 'application-default' dropdown is selected and highlighted with a red box. The 'SERVICE' dropdown below it is empty. To the right, the 'Any' checkbox under the 'URL CATEGORY' dropdown is checked and highlighted with a red box.



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.

15. Select the **Actions** tab. Do not make any changes in this section but notice that the Action is set to **Allow** by default. Click **OK**.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action **Allow**

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None

Profile Setting

Profile Type None

Other Settings

Schedule 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.

16. Verify the *Extranet-to-Internet* security policy rule appears in the Security policies window.

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

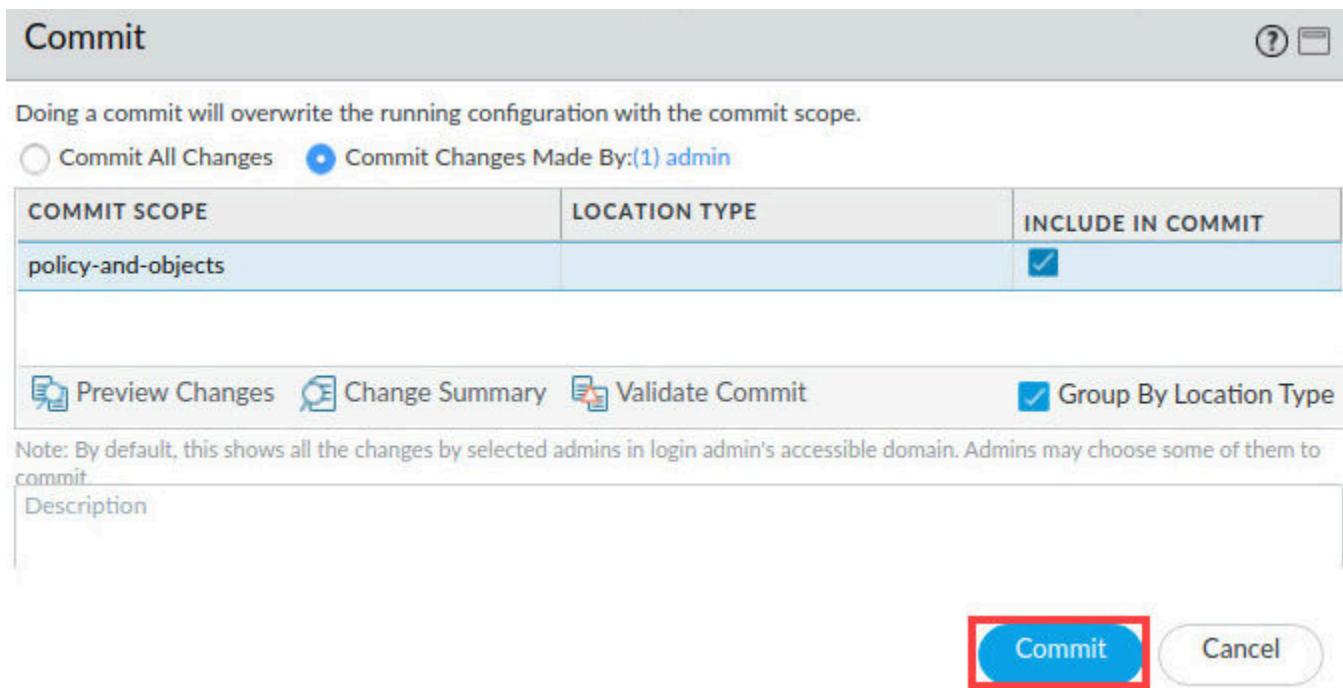
Security

NAME	TAGS	Source			Destination	
		ZONE	ADDRESS	USER	ADDRESS	ZONE
1 Users-to-Extranet	none	Users_Net	any	any	any	Extranet
2 Users-To-Internet	none	Users_Net	any	any	any	Internet
3 Extranet-to-Internet	none	Extranet	any	any	any	Internet
4 intrazone-default	none	any	any	any	any	(intrazone)
5 interzone-default	none	any	any	any	any	any

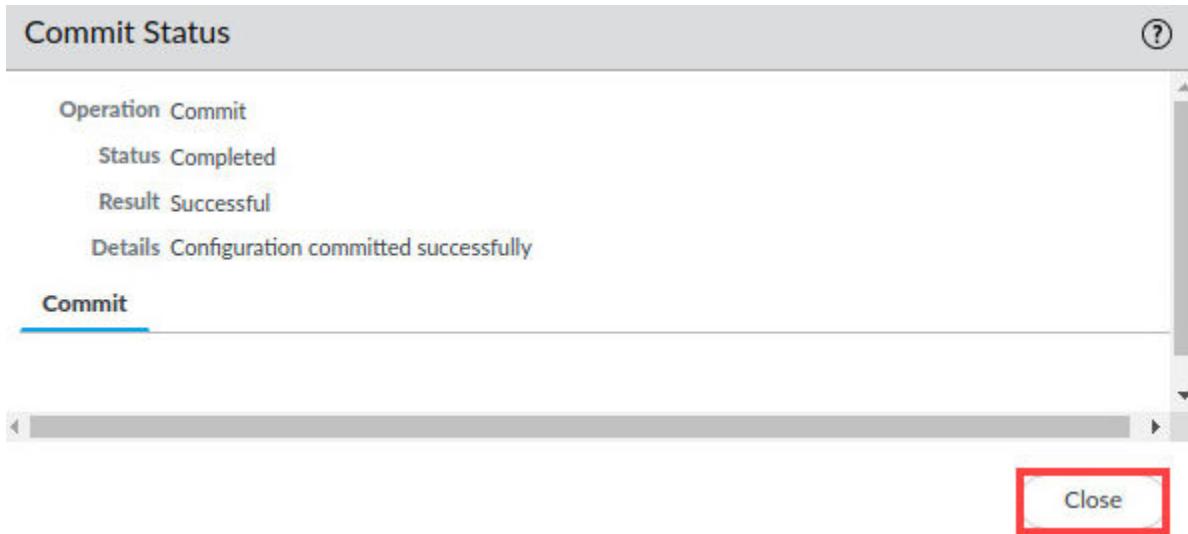
17. Click the **Commit** button at the upper right of the web interface.



18. In the *Commit* window, click **Commit**.



19. Wait until the Commit process is complete. Click **Close**.



20. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



1.8 Ping Internet Host from Client

In this section, you 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.

1. Return to the *terminal* window by clicking on the **terminal** icon in the taskbar of your *client desktop*.



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

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8
```

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

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
--- 8.8.8.8 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4081ms  
^CC:\home\lab-user\Desktop\Lab-Files>
```

4. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.



5. Reopen the firewall interface if you minimized it. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter `(addr.dst eq 8.8.8.8) and (app eq ping)`. Click the **Apply Filter** button in the upper right corner of the window. You will notice the firewall is now logging entries hitting the **Users-to-Internet** rule. You may need to refresh the Traffic logs every one to two minutes for the Traffic logs to update.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, under 'Logs', the 'Traffic' tab is selected. A search bar at the top contains the filter: '(addr.dst eq 8.8.8.8) and (app eq ping)'. The main area displays a table of traffic logs with columns: RECEIVE TIME, FROM ZONE, TO ZONE, and SO. Three rows of log entries are shown, all of which have the 'ACTION' column set to 'allow' and the 'RULE' column set to 'Users-To-Internet'. The last three columns show session details: SESSION END REASON (all listed as 'aged-out'), BYTES (294, 588, 588), HTTP/2 CONNECTION SESSION (0, 0, 0), and SDW# (empty). On the right, the 'DEVICE' tab is open, showing a table of sessions with columns: PORT, APPLICATION, ACTION, RULE, SESSION END REASON, BYTES, HTTP/2 CONNECTION SESSION, and SDW#. The first three rows in this table also have 'ACTION' as 'allow' and 'RULE' as 'Users-To-Internet', matching the log entries.



Notice the ping failed. It failed because your ping session from the client to the Internet host did not get a reply even though the firewall is allowing the traffic. For the ping to be successful, you will need to create a NAT policy.

6. Leave the firewall open and continue to the next task.

1.9 Create a Source NAT Policy

You must create entries in the firewall's NAT Policy table 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.

1. In the web interface, navigate to **Policies > NAT**. Click **Add** to define a new *source NAT policy*.

The screenshot shows the PA-VM web interface. At the top, there is a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), and OBJECTS. On the left, a sidebar under the 'Security' heading has a 'NAT' tab highlighted with a red box. Below the sidebar is a search bar. The main area contains a table with columns: NAME, TAGS, SOURCE ZONE, and DESTINATION ZONE. At the bottom of the screen, there is a toolbar with buttons: Object : Addresses, +, Add (highlighted with a red box), Delete, Clone, Enable, Disable, Move, PDF/CS.

2. In the *NAT Policy Rule* window, configure the following on the *General* tab:

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

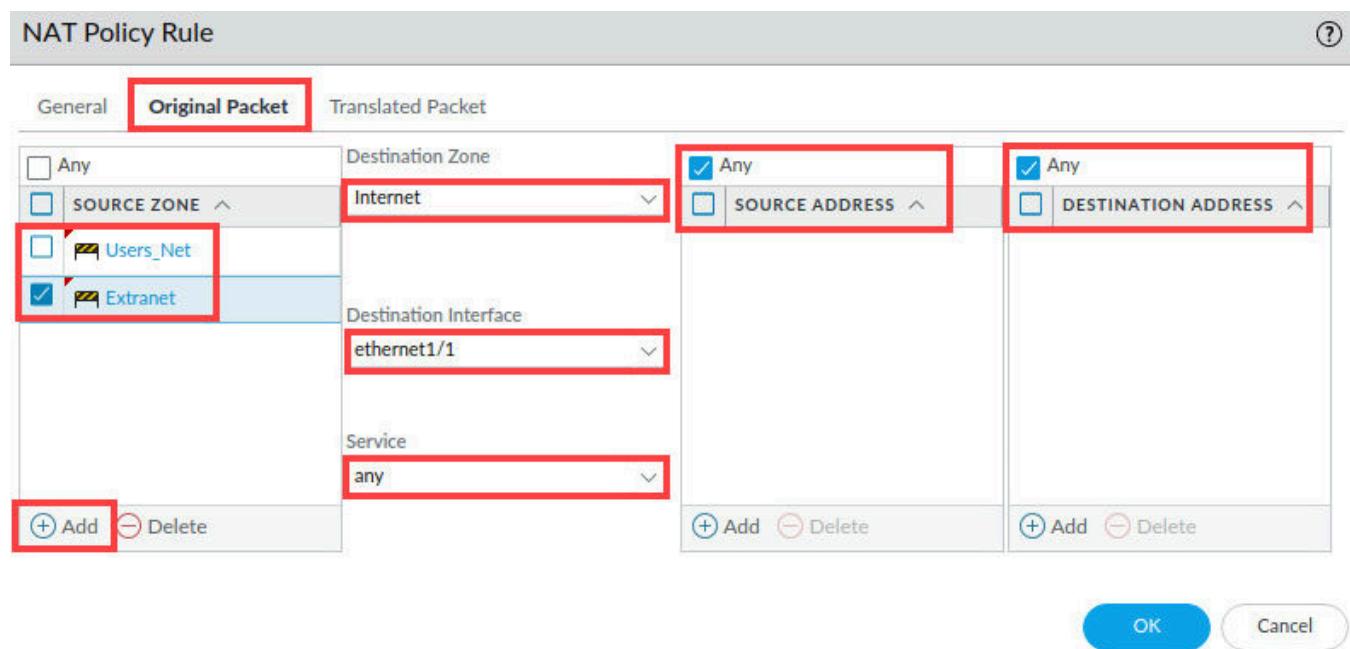
NAT Policy Rule

General | Original Packet | Translated Packet

Name	Inside_Nets_to_Internet
Description	Translates traffic from Users_Net and Extranet to 203.0.113.20 outbound to Internet
Tags	
Group Rules By Tag	None
NAT Type	ipv4
Audit Comment	

3. Click the **Original Packet** tab and configure the following.

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 dropdown list
Destination Interface	Select ethernet1/1 from the dropdown 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



Please Note

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.

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

Parameter	Value
Translation Type	Select Dynamic IP And Port from the dropdown list
Address Type	Select Interface Address from the dropdown list
Interface	Select ethernet1/1 from the dropdown list

Parameter	Value
IP Address	Select 203.0.113.20/24 from the dropdown list. (Make sure that you select the interface IP address from the dropdown list and do not type it.)

NAT Policy Rule

General | Original Packet **Translated Packet**

Source Address Translation

Translation Type: **Dynamic IP And Port**

Address Type: **Interface Address**

Interface: **ethernet1/1**

IP Address: **203.0.113.20/24**

Destination Address Translation

Translation Type: **None**

OK Cancel

Please Note

This section defines how the firewall will translate the packet.

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

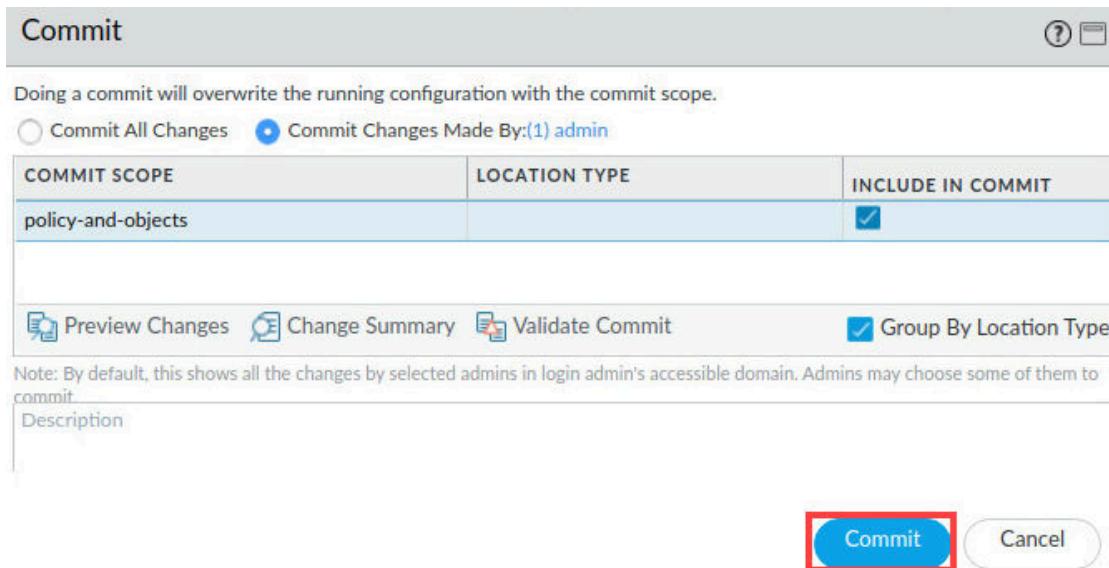
5. Verify that the **Inside_Nets_to_Internet** NAT policy is showing.

NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION
1 Inside_Nets_to_Inter...	none	Extranet Users_Net	Internet	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none

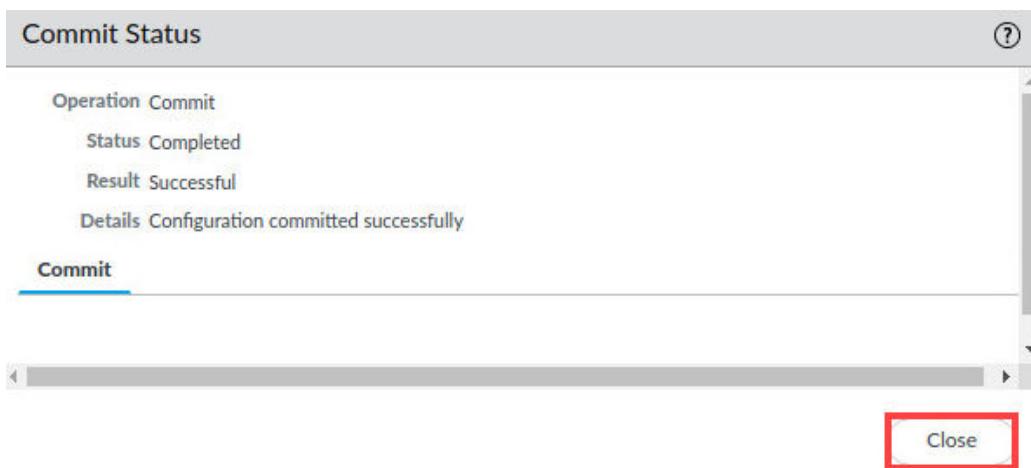
6. Click the **Commit** button at the upper right of the web interface.



7. In the *Commit* window, click **Commit**.



8. Wait until the *Commit* process is complete. Click **Close**.



9. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



10. Return to the terminal window by clicking on the terminal icon in the taskbar of your *client desktop*.



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

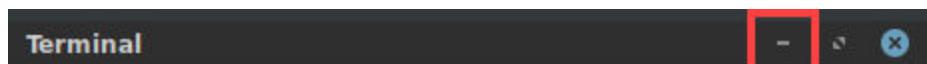
```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 8.8.8.8
```

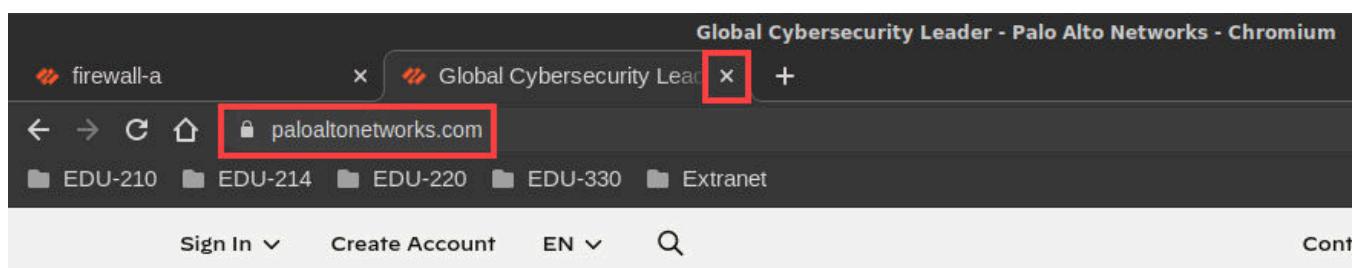
12. After a few seconds, use **Ctrl+C** to stop the connection. You should now receive a successful reply.

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=9.56 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=8.21 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=8.66 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=8.68 ms  
^C  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 8.215/8.782/9.561/0.492 ms
```

13. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.



14. Open a new tab on the *Chromium* web browser. Type www.paloaltonetworks.com and verify connectivity. Close the newly opened tab by clicking the X icon.



15. Examine the firewall Traffic log by ensuring you are at **Monitor > Logs > Traffic**. Clear any filters you have in place by clicking the **Clear Filter** button in the upper right corner of the window. Verify that there is allowed traffic that matches the security policy rule **Users_to_Internet**.

	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATI...	TO PORT	APPLICATI...	ACTION	RULE	HTTP/2 CONNECTION SESSION ID	SDW/
	08/07 01:55:10	Users_Net	Internet	192.168.1....		34.96.84.34	443	paloalto-updates	allow	Users-To-Internet	0	
	08/07 01:55:08	Users_Net	Internet	192.168.1.20		44.194.25.77	443	ssl	allow	Users-To-Internet	0	
	08/07 01:55:00	Users_Net	Extranet	192.168.1.20		192.168.50....	53	dns	allow	Users-to-Extranet	0	
	08/07 01:55:00	Users_Net	Internet	192.168.1.20		1.1.1.1	53	dns	allow	Users-To-Internet	0	
	08/07 01:55:00	Users_Net	Extranet	192.168.1.20		192.168.50....	53	dns	allow	Users-to-Extranet	0	
	08/07 01:55:00	Users_Net	Internet	192.168.1.20		1.1.1.1	53	dns	allow	Users-To-Internet	0	
	08/07 01:55:00	Users_Net	Extranet	192.168.1.20		192.168.50....	53	dns	allow	Users-to-Extranet	0	

Please Note

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

16. Leave the firewall open and continue to the next task.

1.10 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.

1. In the web interface, navigate to **Policies > NAT**. Click **Add** to define a new source NAT policy.

NAME	TAGS	SOURCE ZONE	DESTINATION ZONE
1 Inside_Nets_to_Inter...	none	Extranet Users_Net	Internet

2. In the *NAT Policy Rule* window, configure the following on the **General** tab:

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

NAT Policy Rule

General | Original Packet | Translated Packet

Name	Dest_NAT_To_Webserver
Description	Translates traffic to web server at 192.168.50.80
Tags	
Group Rules By Tag	None
NAT Type	ipv4

3. Click the **Original Packet** tab and configure the following.

Parameter	Value
Source Zone	Click Add and select the Users_Net zone
Destination Zone	Select Users_Net from the dropdown list
Destination Interface	Select ethernet1/2 from the dropdown list
Service	Verify that Any is selected
Source Address	Verify that the Any check box is selected
Destination Address	Click Add and manually enter 192.168.1.80

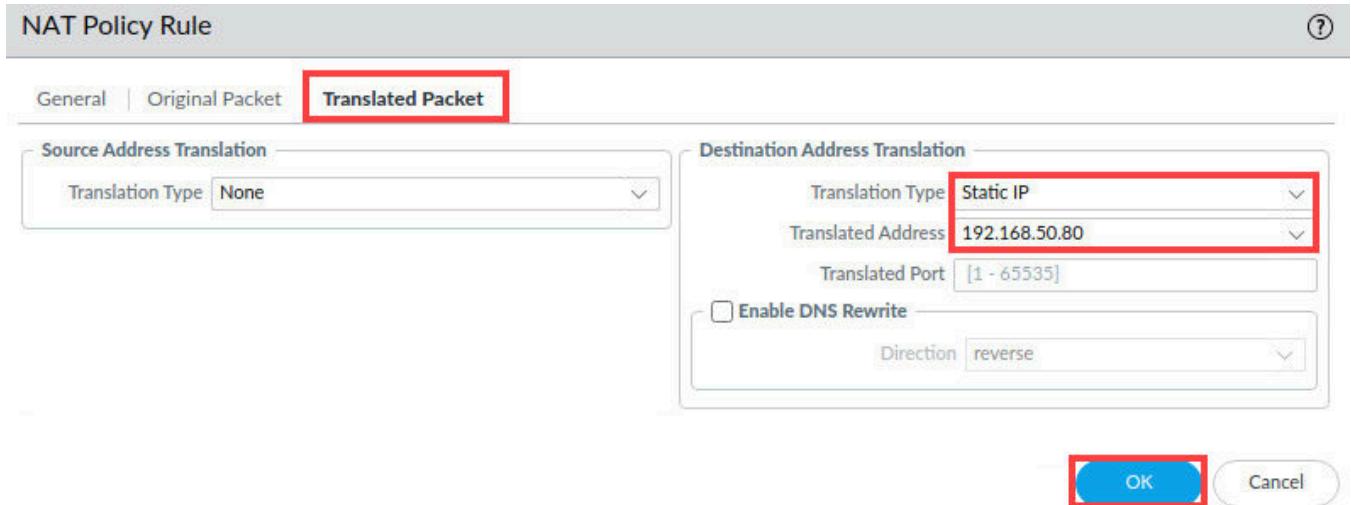
NAT Policy Rule

Please
Note

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.

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

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


Please Note

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.

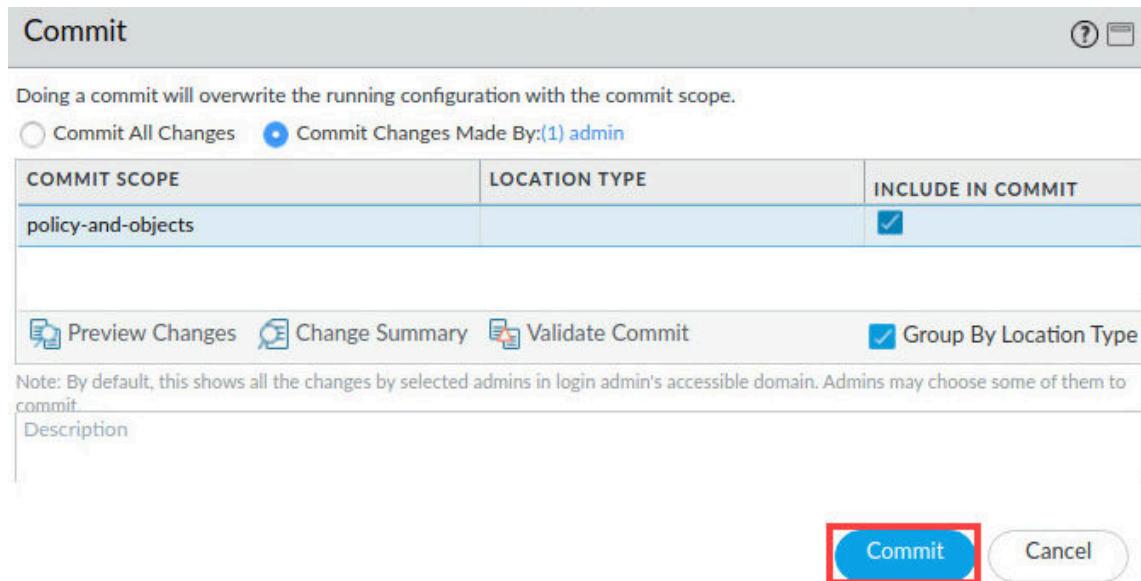
5. Verify that the **Dest_NAT_To_Webserver** NAT policy is showing.

NAME	TAGS	Original Packet						Translated Packet	
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1 Inside_Nets_to_Inter...	none	Extranet Users_Net	Internet	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24	none
2 Dest_NAT_To_Webs...	none	Users_Net	Users_Net	ethernet1/2	any	192.168.1.80	any	none	destination-translat... address: 192.168.50.80

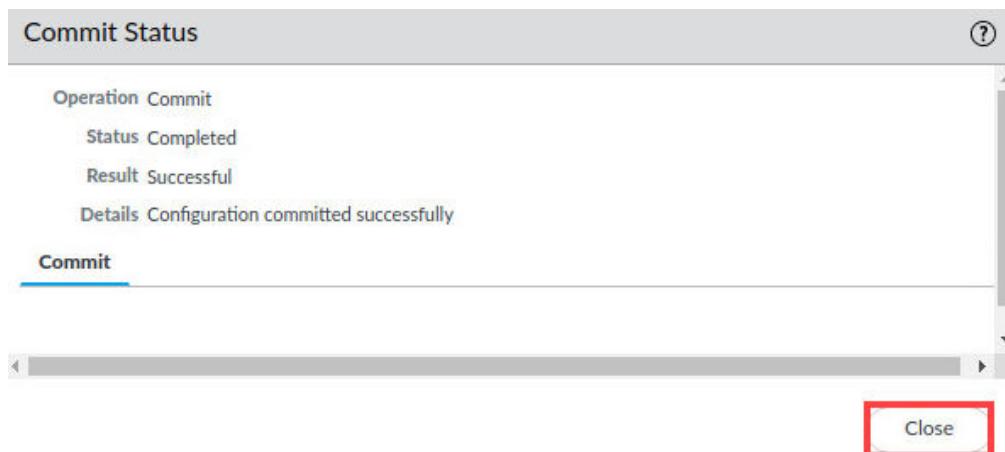
6. Click the **Commit** button at the upper right of the web interface.



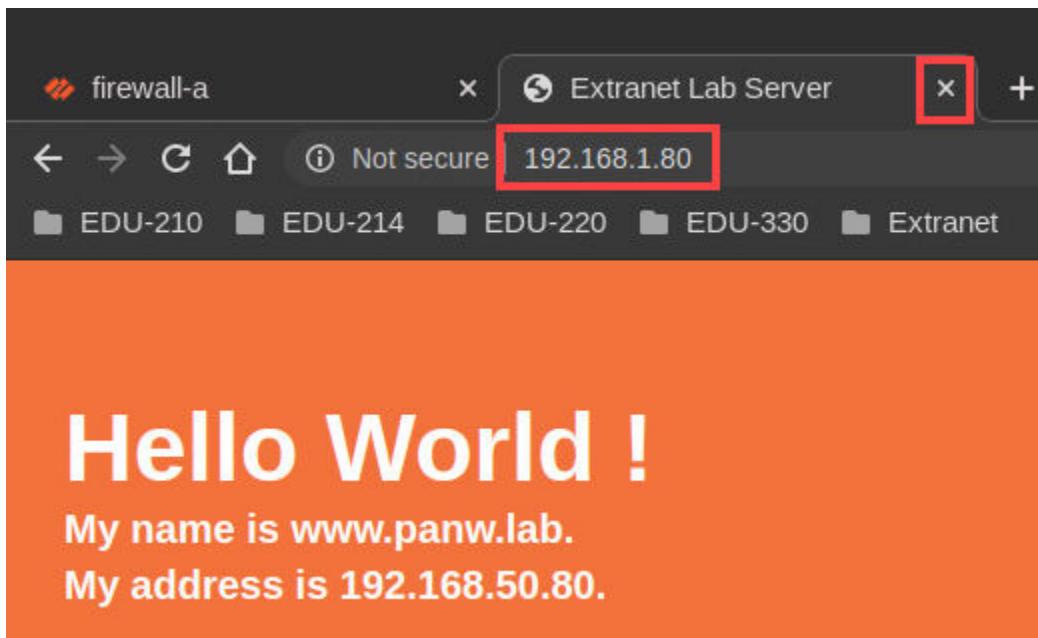
7. In the *Commit* window, click **Commit**.



8. Wait until the *Commit* process is complete. Click **Close**.



9. Open a new tab on the *Chromium* web browser. Type **http://192.168.1.80** and verify connectivity to the *Extranet Server*. Close the newly opened tab by clicking the X icon.



10. Examine the firewall Traffic log by ensuring you are at **Monitor > Logs > Traffic**. Use a filter to locate the entry for Destination IP 192.168.1.80 (`addr.dst in 192.168.1.80`). Verify that there is allowed traffic that matches the security policy rule **Users_to_Internet**.

The screenshot shows the PAN-OS Firewall Traffic Log interface under the "MONITOR" tab. The "Logs" section is selected, and a search filter "(addr.dst in 192.168.1.80)" is applied. The log table displays one entry:

RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATI...	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID
08/07 02:15:11	Users_Net	Extranet	192.168.1.20		192.168.1.80	80	web-browsing	allow	Users-to-Extranet	Tcp-fin	3.0k	0

A yellow callout box on the left is labeled "Please Note" and points to the log entry. The entire screenshot is framed by a red border.

11. As an alternate method to access the Traffic log in the web interface, select **Policies > Security**. Hover to the right of *Users-to-Extranet* to utilize the **dropdown** icon below the *Name* column, select **Log Viewer**.

The screenshot shows the PA-VM web interface with the following details:

- Header:** PA-VM, DASHBOARD, ACC, MONITOR, POLICIES (highlighted in red).
- Left Sidebar (Security tab):** NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, SD-WAN.
- Table:** Shows security policies with columns: NAME, TAGS, ZONE, ADDRESS.
- Row 1:** Users-to-Extranet, none, Users_Net, any. The dropdown icon next to 'none' is highlighted with a red box.
- Row 2:** Users-To-Internet, Filter, Jusers_Net, any.
- Row 3:** Extranet-to-Internet, Log Viewer (highlighted with a red box), Extranet, any. The 'Log Viewer' option is also highlighted with a red box.
- Row 4:** intrazone-default, Copy UUID, any.
- Row 5:** interzone-default, Global Find, any.



When you use the Log Viewer option on a security policy, it opens the Traffic log and applies a filter automatically to display only those entries that match the security policy rule “Users_to_Extranet” that was selected.

12. The lab is now complete; you may end your reservation.