PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 6: Creating and Managing NAT Policy Rules

Document Version: 2025-10-13

Contents

Introduction

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.

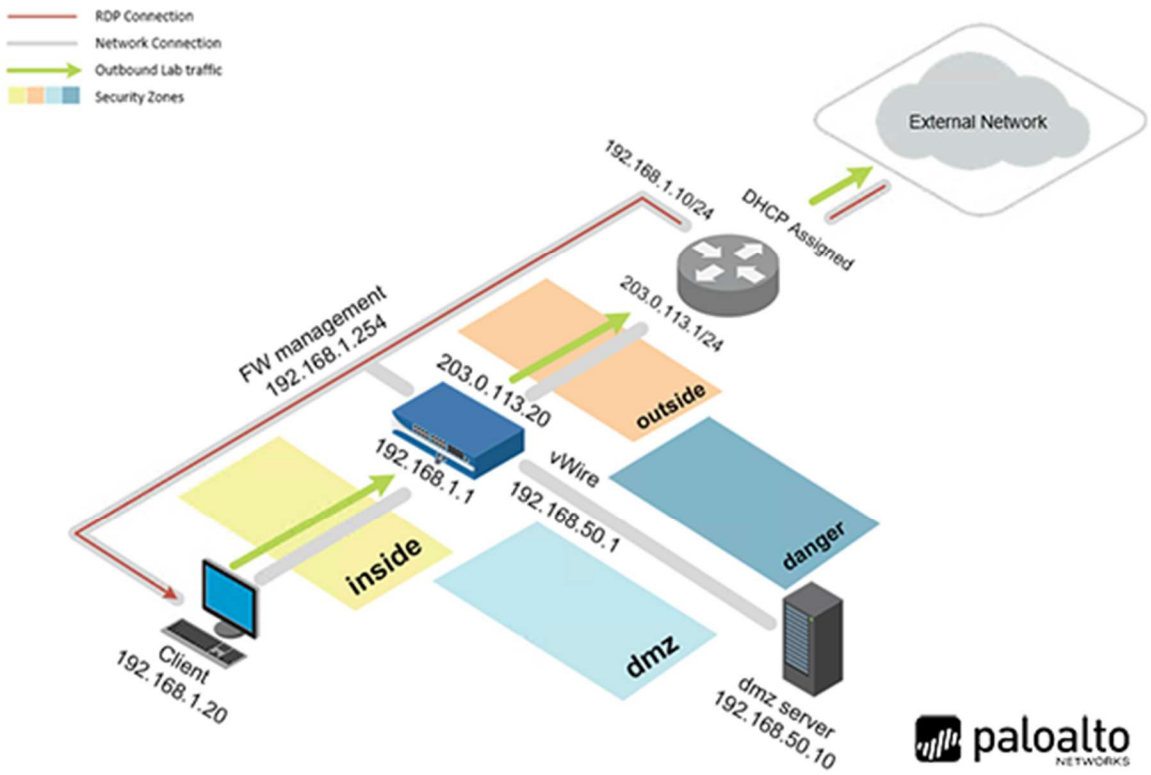
After you have all these components in place, you will generate test traffic and examine firewall logs.

Objective

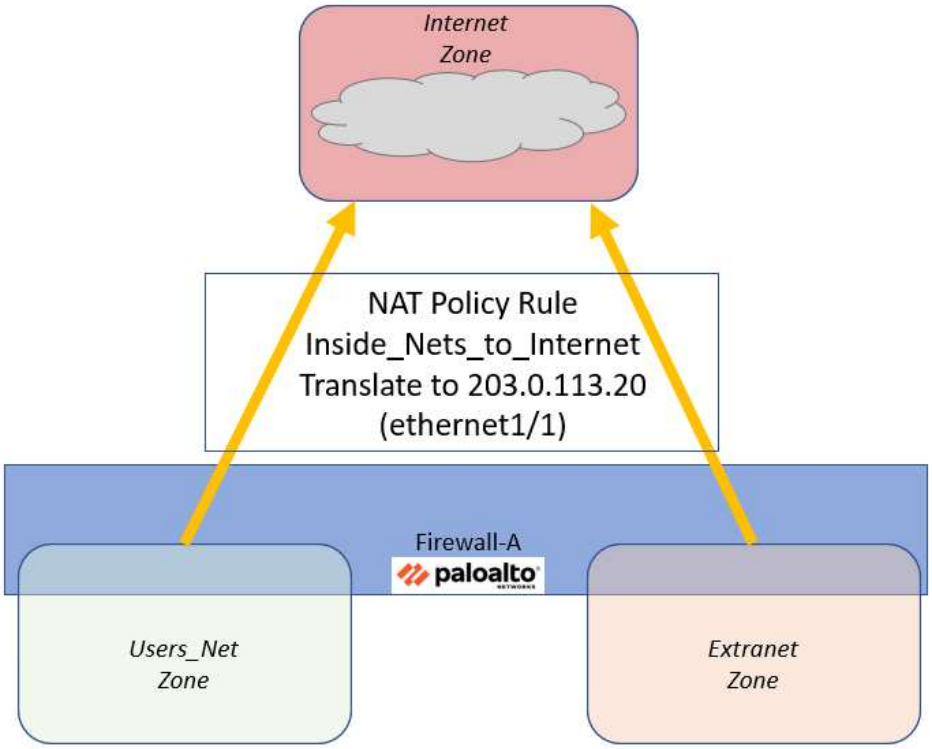
In this lab, you will perform the following tasks:

- Configure source NAT.
- Configure destination NAT.

Lab Topology



Theoretical Lab Topology



Lab Settings

The information in the table below will be needed in order 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`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

Lab Guidance

There are two sections in this lab 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.

Please Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Creating and Managing NAT Policy Rules - High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-06.xml** to the Firewall.

1.2 Create a Source NAT Policy Rule

- Use the Information in the tables below to create a new Source NAT Rule.

General tab

Parameter	Value
Name	**Inside_Nets_to_Internet**
NAT Type	**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**

1.3 Commit the Configuration

- Commit the changes before proceeding.

1.4 Verify Internet Connectivity

- From the Terminal window on the client desktop, ping 8.8.8.8 and you should now receive a reply.
- Use the *Firefox* 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**.

1.5 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 Type	**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**

1.6 Commit the Configuration

- Commit the changes before proceeding.

1.7 Test the Destination NAT Rule

- Use the *Firefox* 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.

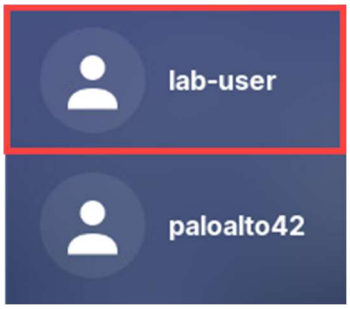
2 Creating and Managing NAT Policy Rules – Detailed Lab Steps

2.1 Apply a Baseline Configuration to the Firewall

In this section, you will connect to the Firewall and load the Firewall configuration file.

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

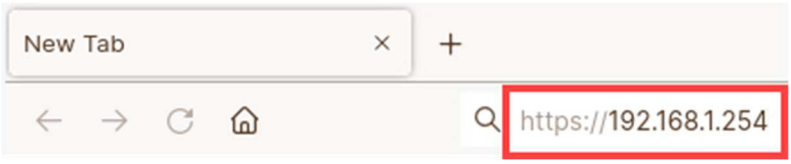
2. On the *Zorin* desktop, click **lab-user.**



3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.

4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.

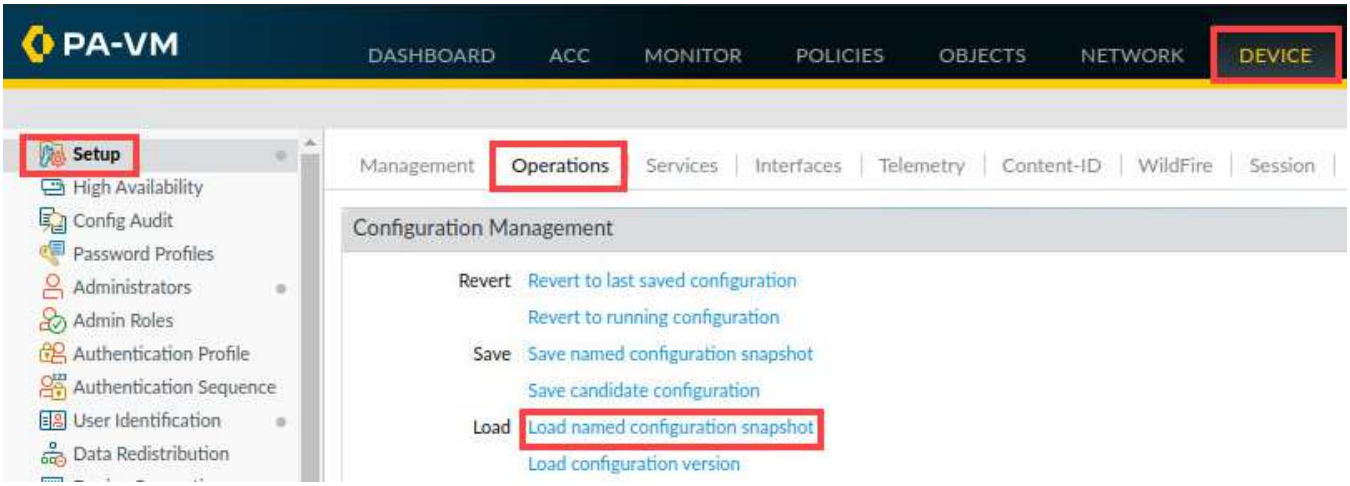
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



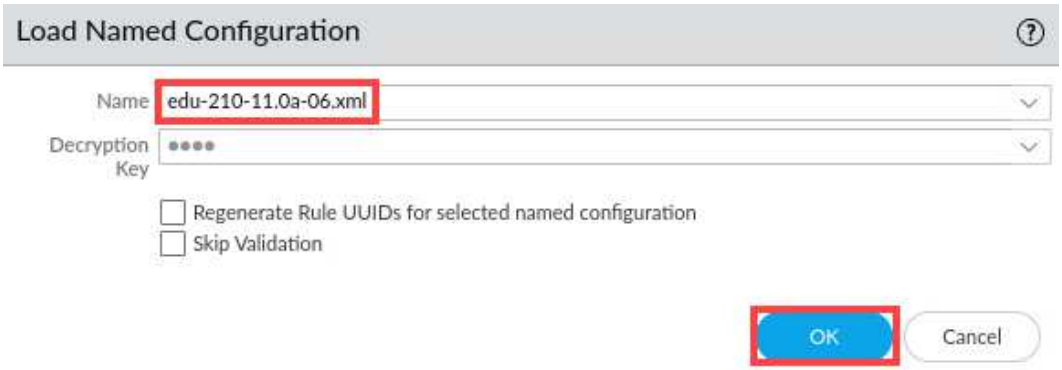
6. Log in to the Firewall web interface as username **admin**, password **`Pal0Alt0!.`**

If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

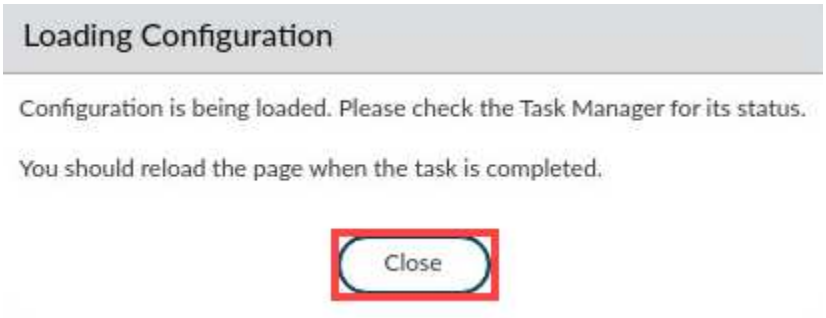
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



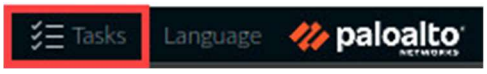
8. In the *Load Named Configuration* window, select **edu-210-11.0a-06.xml** from the *Name* drop-down box and click **OK**.



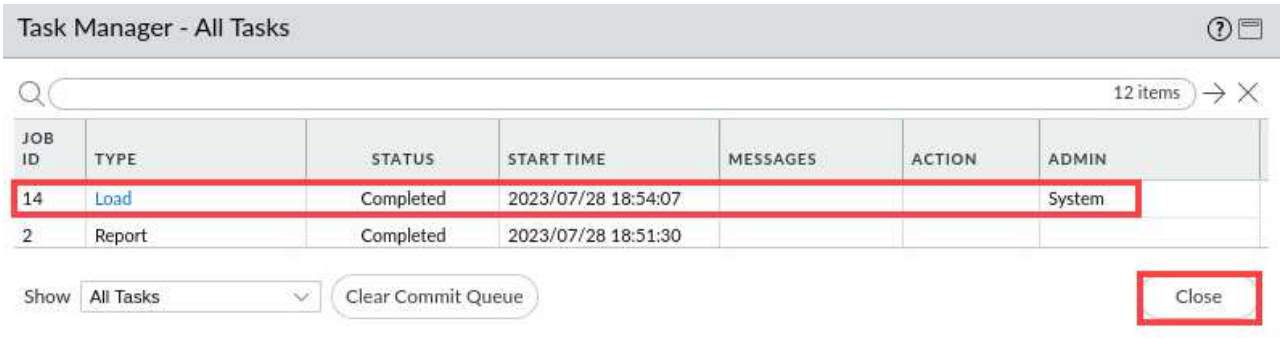
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

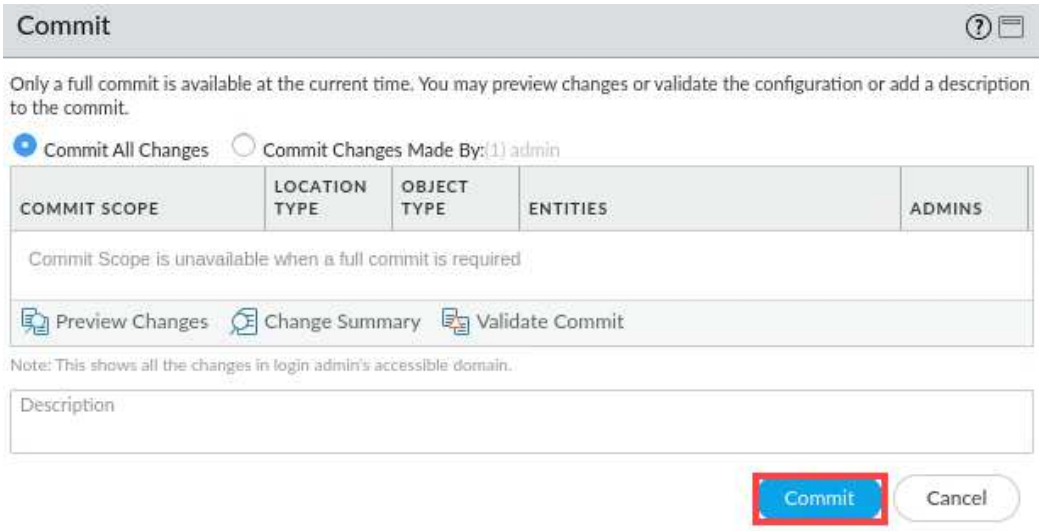


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

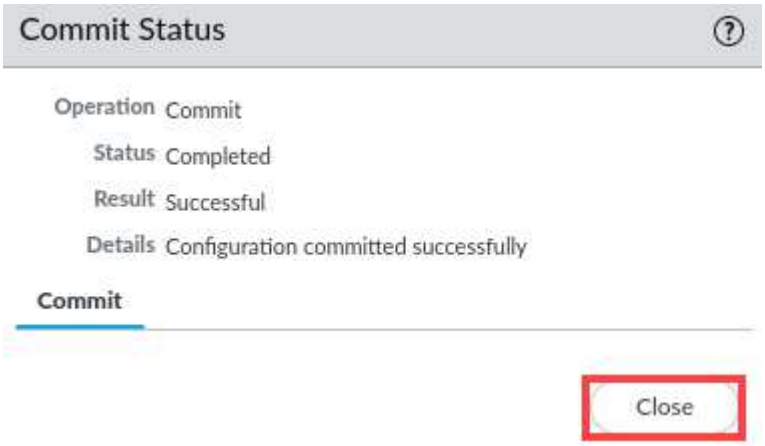


12. Click the **Commit** link located at the top-right of the web interface.

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



14. When the commit operation is complete, 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.

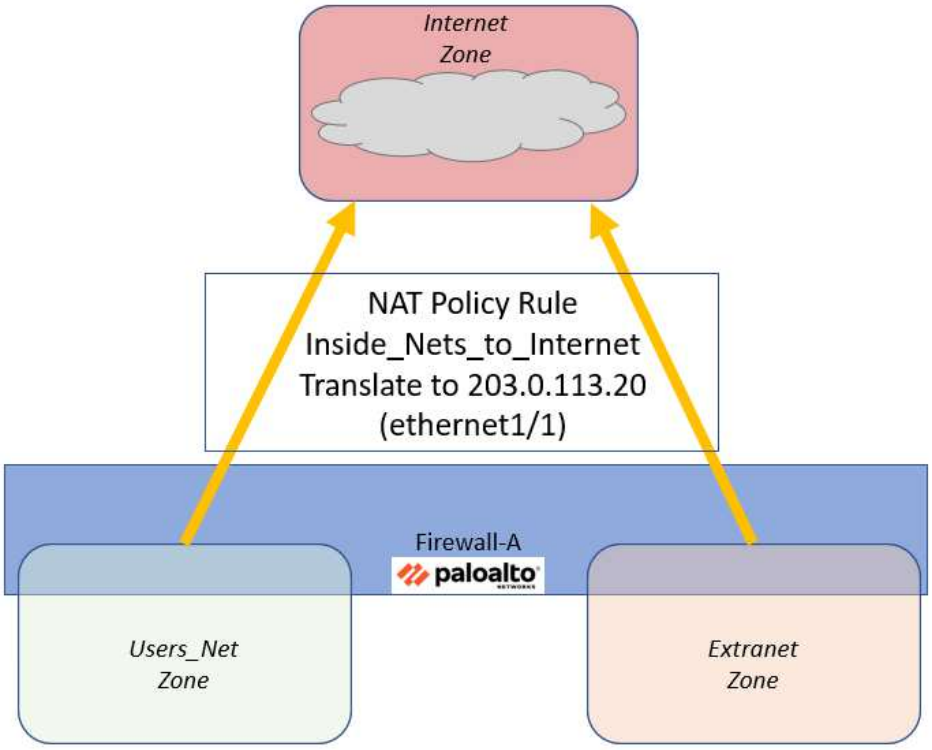
15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.2 Create a Source NAT Policy

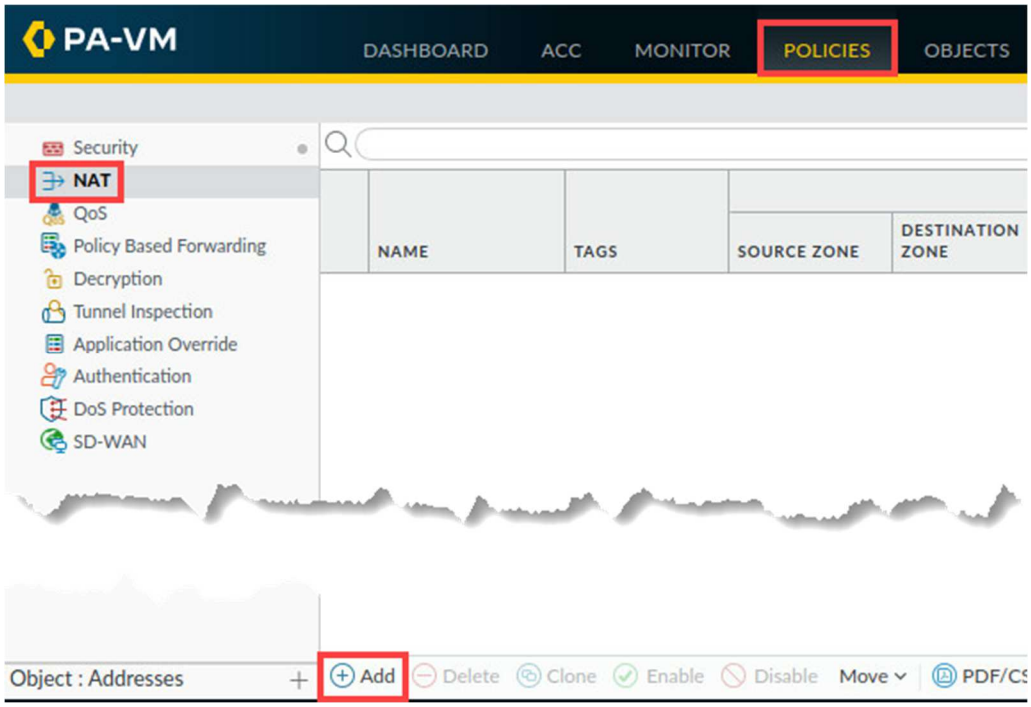
You must create entries in the firewall's NAT Policy table to translate traffic from internal hosts (often on private networks) to a public, routable address (often an interface on the firewall itself). NAT rules provide address translation and are different from Security policy rules, which allow and 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.

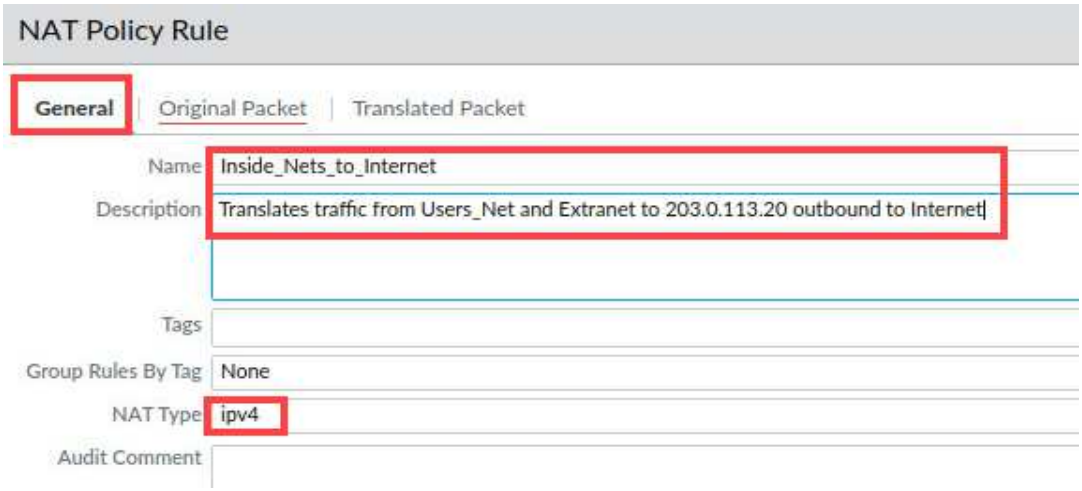


1. In the web interface, navigate to **Policies > NAT**. Click **Add** to define a new *source NAT policy*.



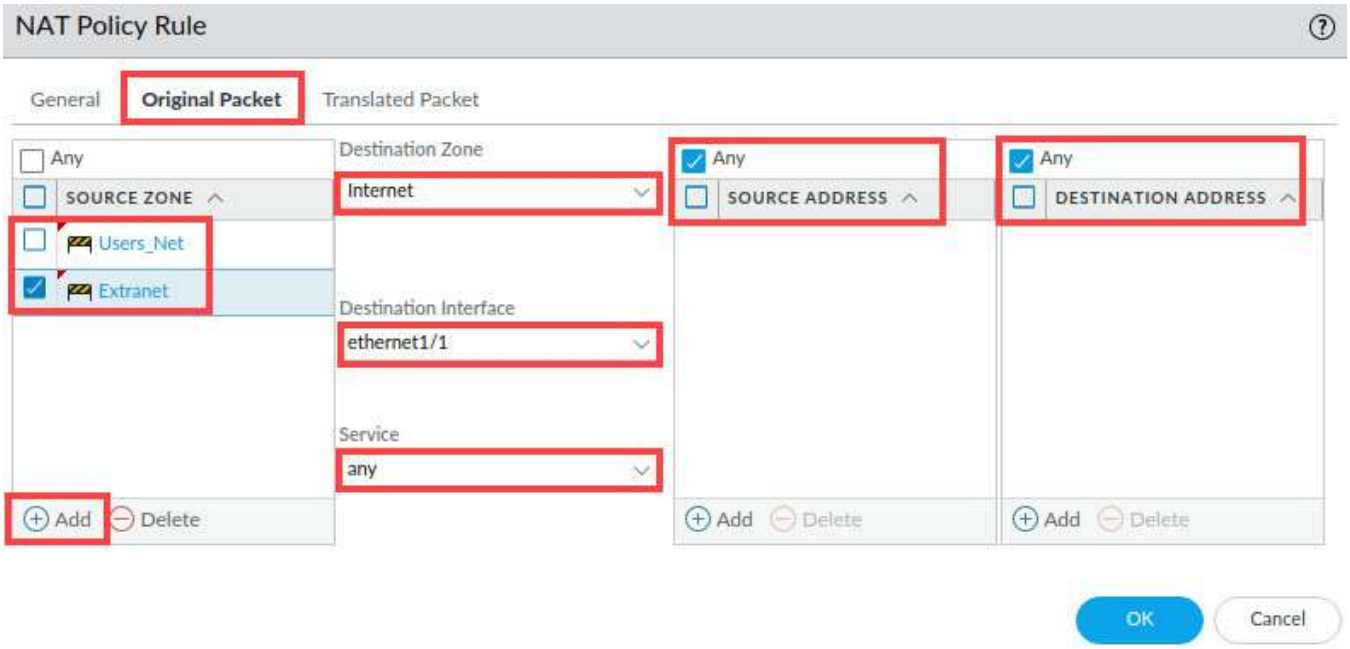
2. In the *NAT Policy Rule* window, configure the following on the *General* tab:

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`



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 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



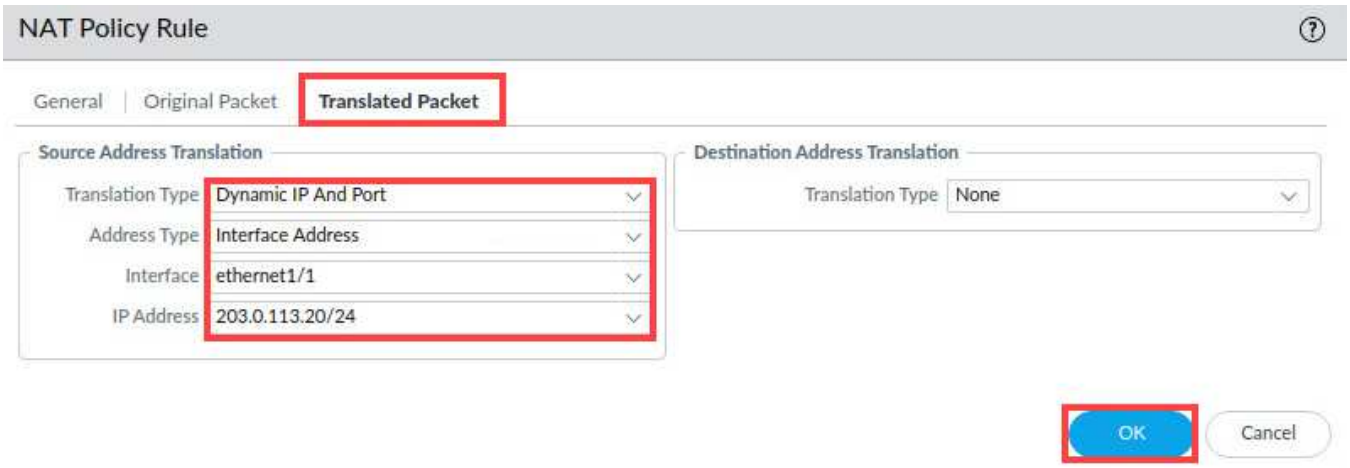
Please Note

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 drop-down list
Address Type	Select **Interface Address** from the drop-down list
Interface	Select **ethernet1/1** from the drop-down list

Parameter	Value
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 ***do not type it***.)



Please Note

This section defines how the firewall will translate the packet.

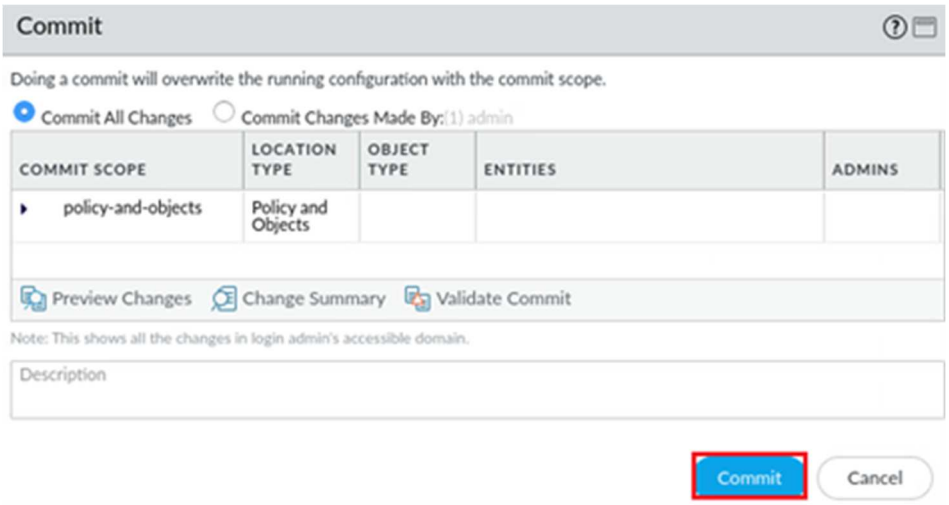
You are configuring *only* the **Source Address Translation** part of this window. Leave the destination address translation **Translation Type** set to **None**.

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

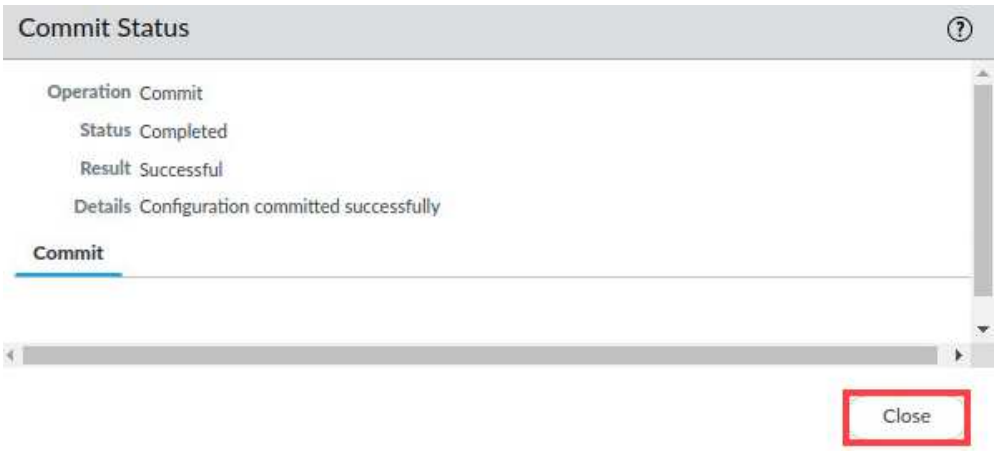
	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION
1	Inside_Nets_to_Inter...	none	Extranet Users_Net	Internet	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 203.0.113.20/24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



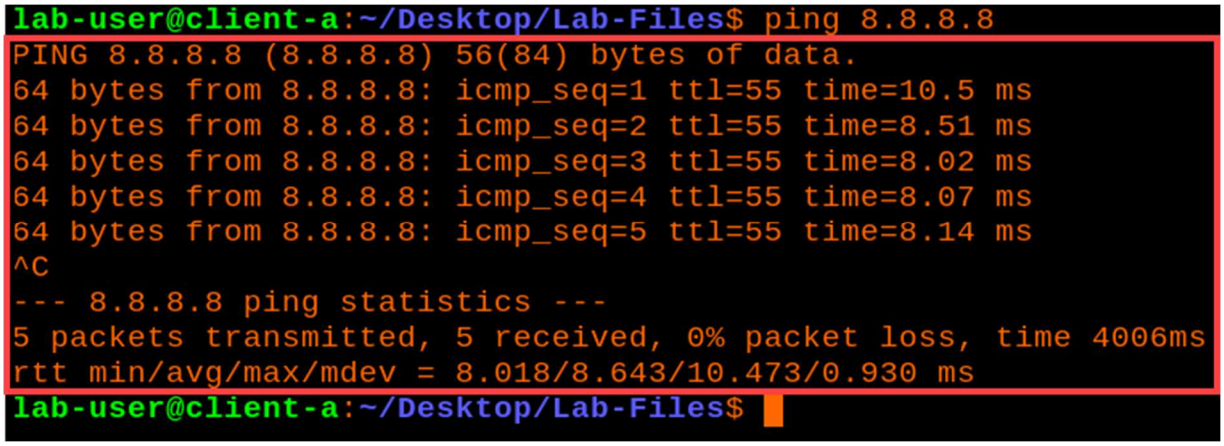
9. Minimize the *Firefox* browser by clicking the **minimize** icon and continue to the next task.

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

11. 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>
```

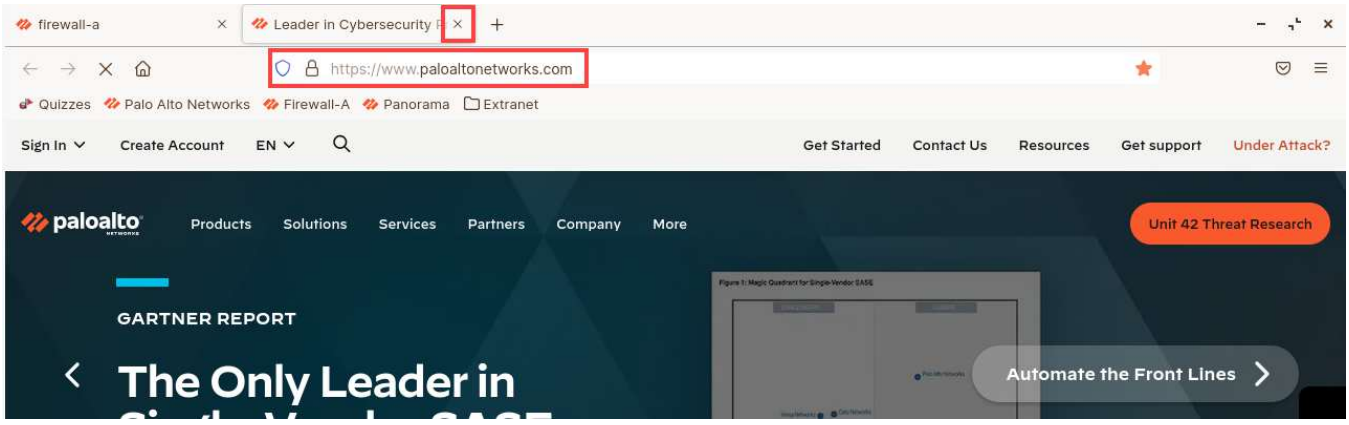
12. After a few seconds, use **Ctrl+C** to stop the connection. You should now receive a successful reply.



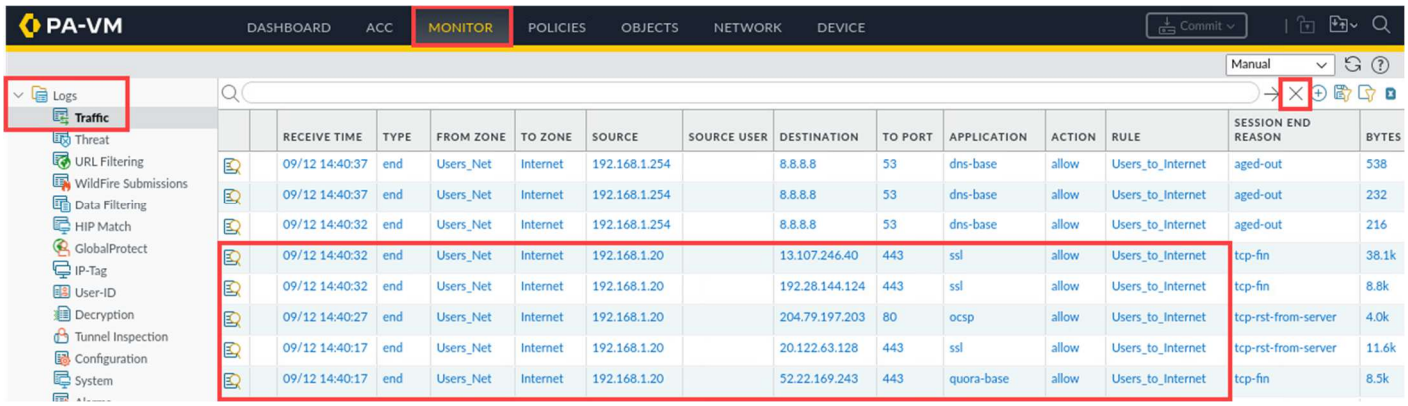
13. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.

14. Return to the *firewall-a – Mozilla Firefox* window by clicking on the **Firefox** icon in the taskbar of your client desktop.

15. Open a new tab on the *Firefox* tab. Type **`www.paloaltonetworks.com`** and verify connectivity. Close the newly opened tab by clicking the **X** icon.



16. 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	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
09/12 14:40:37	end	Users_Net	Internet	192.168.1.254		8.8.8.8	53	dns-base	allow	Users_to_Internet	aged-out	538
09/12 14:40:37	end	Users_Net	Internet	192.168.1.254		8.8.8.8	53	dns-base	allow	Users_to_Internet	aged-out	232
09/12 14:40:32	end	Users_Net	Internet	192.168.1.254		8.8.8.8	53	dns-base	allow	Users_to_Internet	aged-out	216
09/12 14:40:32	end	Users_Net	Internet	192.168.1.20		13.107.246.40	443	ssl	allow	Users_to_Internet	tcp-fin	38.1k
09/12 14:40:32	end	Users_Net	Internet	192.168.1.20		192.28.144.124	443	ssl	allow	Users_to_Internet	tcp-fin	8.8k
09/12 14:40:27	end	Users_Net	Internet	192.168.1.20		204.79.197.203	80	ocsp	allow	Users_to_Internet	tcp-rst-from-server	4.0k
09/12 14:40:17	end	Users_Net	Internet	192.168.1.20		20.122.63.128	443	ssl	allow	Users_to_Internet	tcp-rst-from-server	11.6k
09/12 14:40:17	end	Users_Net	Internet	192.168.1.20		52.22.169.243	443	quora-base	allow	Users_to_Internet	tcp-fin	8.5k

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

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

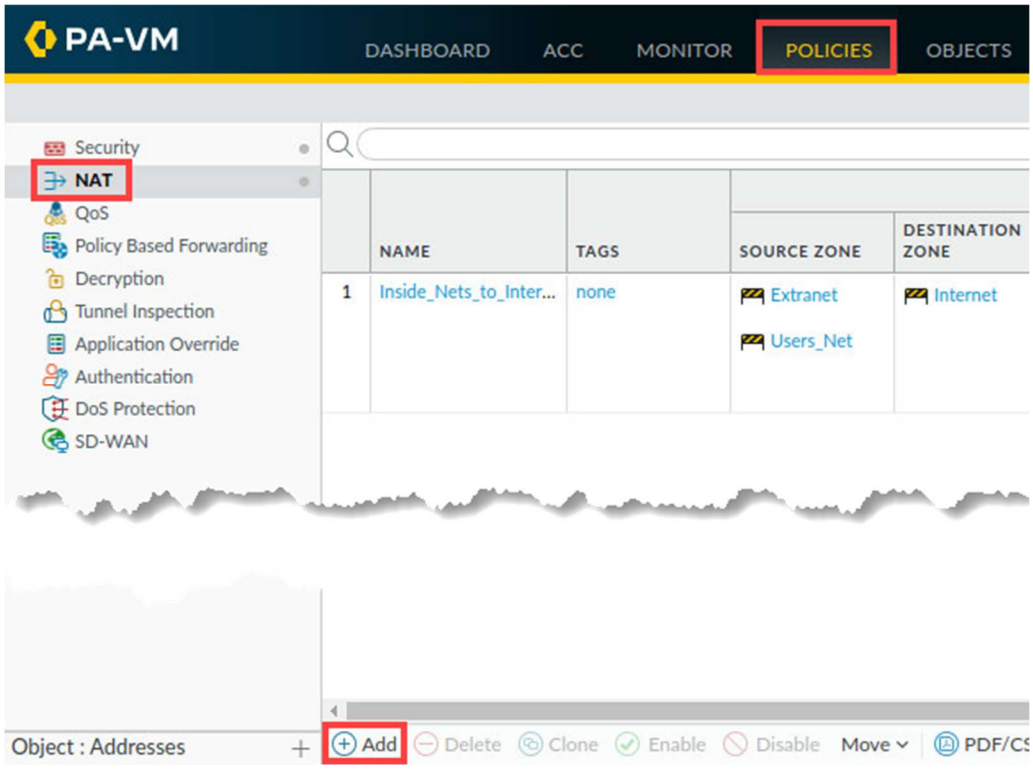
2.3 Create a Destination NAT Policy

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 which 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.

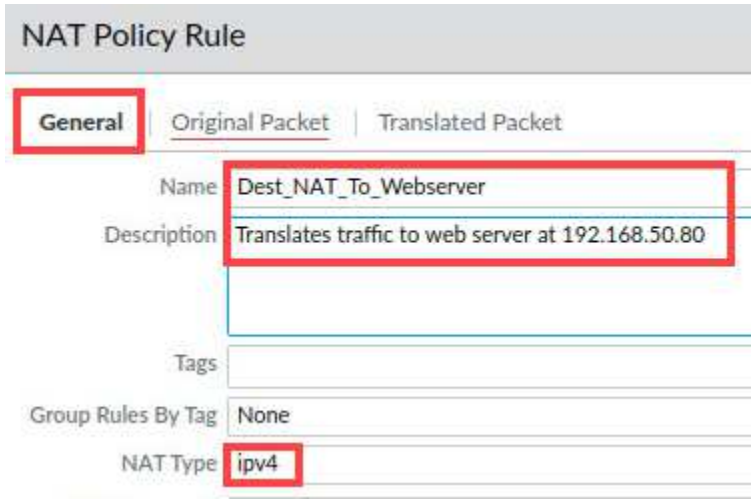
This exercise will help you see how to configure Destination NAT rules.

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



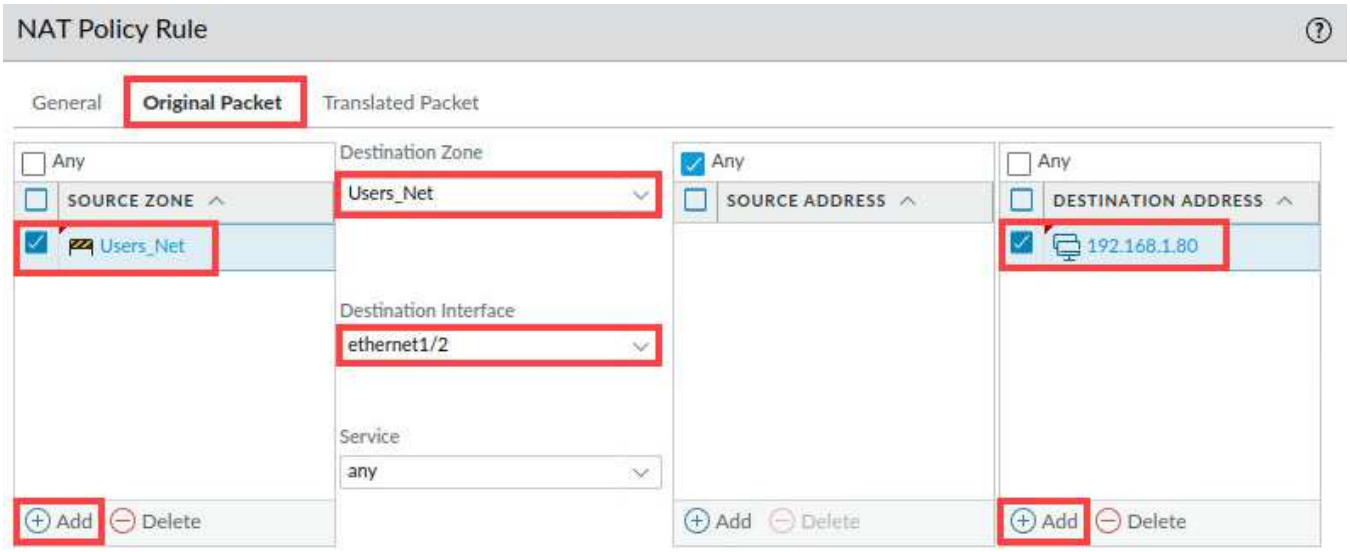
2. In the NAT Policy Rule window, configure the following on the General tab:

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`**



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 drop-down list
Destination Interface	Select **ethernet1/2** from the drop-down 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`**

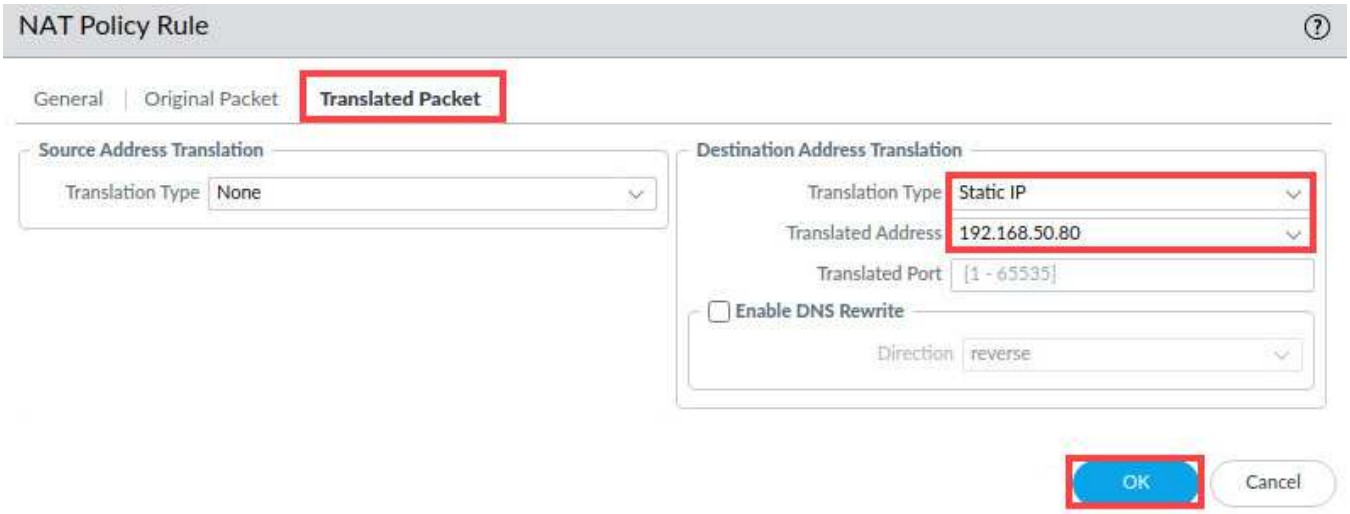


Please Note

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 **Destination Address Translation**. Click **OK**.

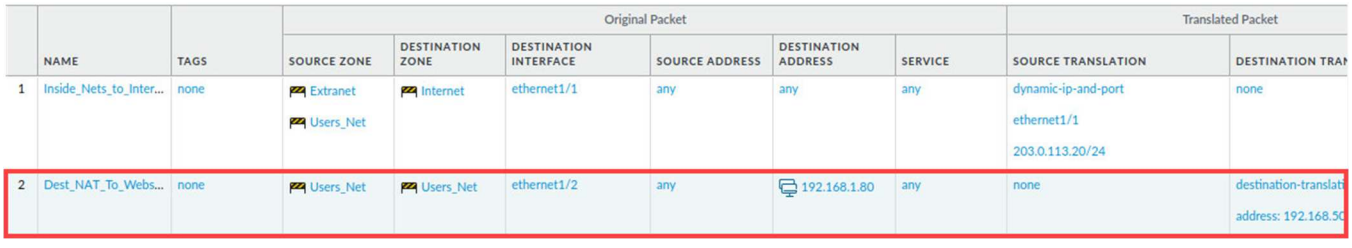
Parameter	Value
Translation Type	Select **Static IP** from the drop-down list
Translated Address	**`192.168.50.80`** (address of the Extranet web server)



Please Note

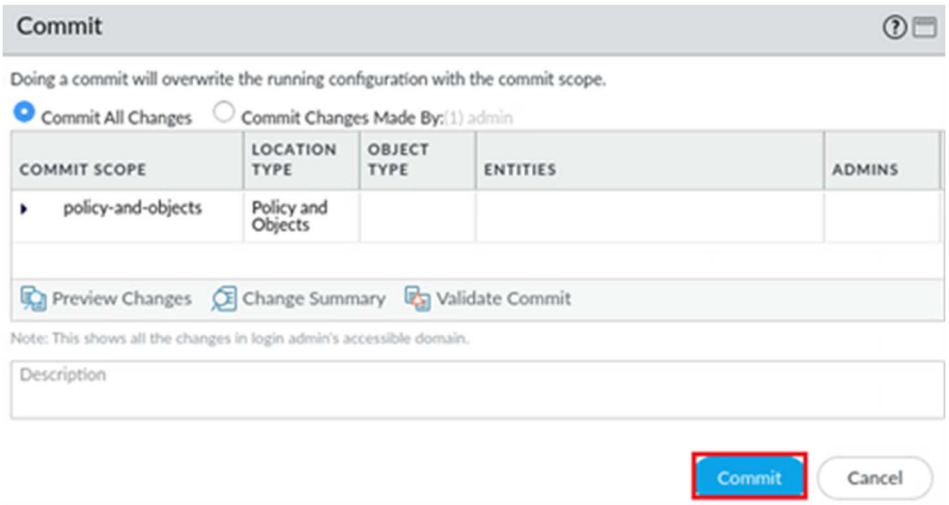
The **Translated Packet** tab defines how the firewall will translate a matching packet. Leave the **Source Address Translation** section set to **None** because we are performing only destination translation in this exercise.

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

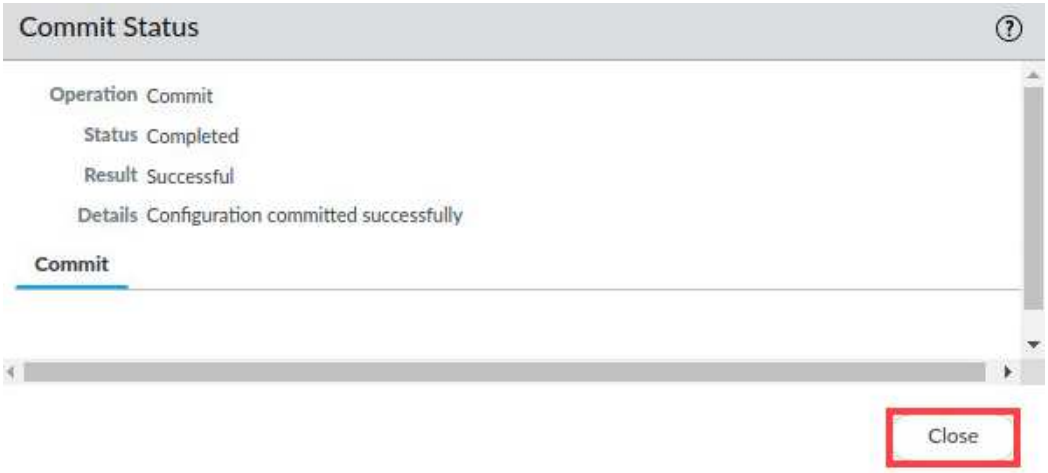


6. Click the **Commit** button at the upper right of the web interface.

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

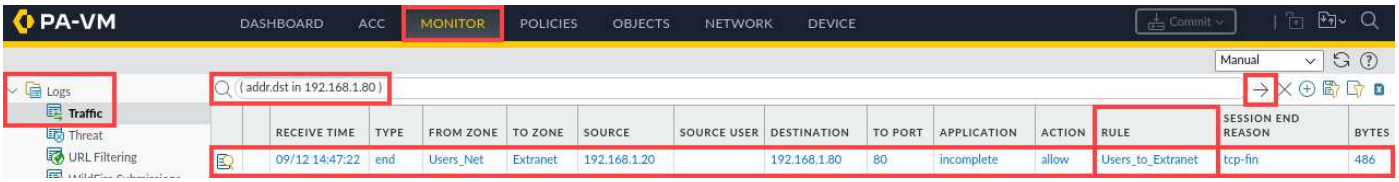


8. Wait until the Commit process is complete. Click **Close**.



9. Open a new tab on the *Firefox* 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.

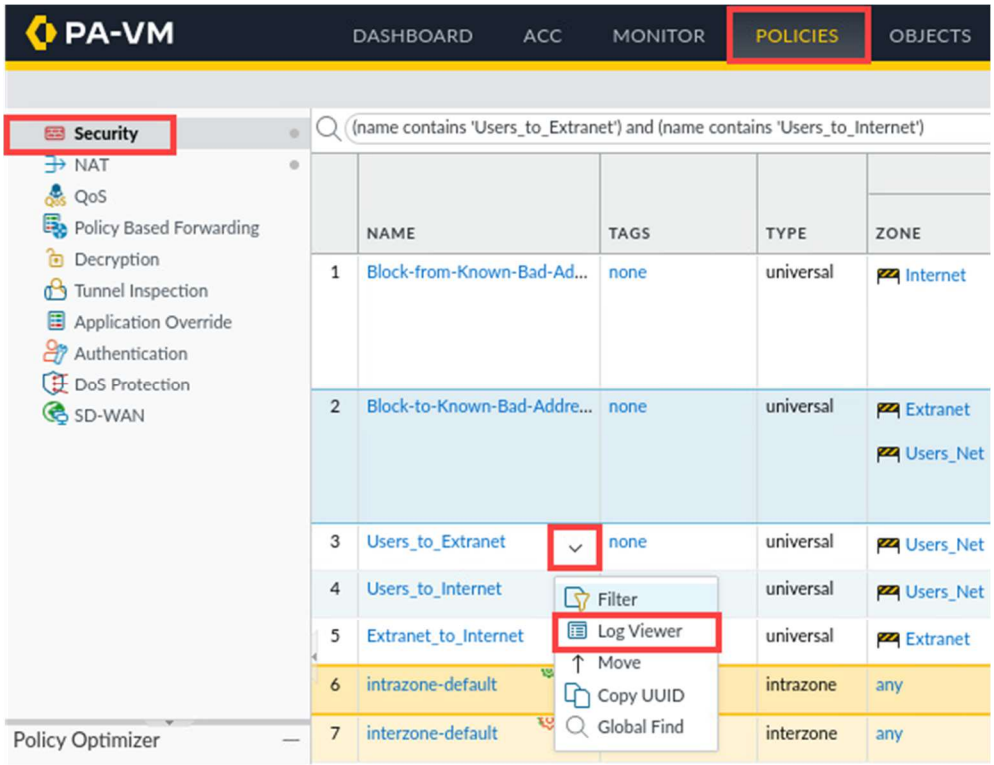
10. Examine the firewall Traffic log by ensuring you are at **Monitor > Logs > Traffic**. Use a filter to locate the entry for Destination IP 192.168.1.80 **(addr.dst in 192.168.1.80).** Verify that there is allowed traffic that matches the Security policy rule **Users_to_Extranet.**



Please Note

Note the Security policy rule that was matched: **Users_to_Extranet**

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 drop-down icon below the **Name** column, select **Log Viewer**.



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.

