PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 5: Creating and Managing Security Policy Rules

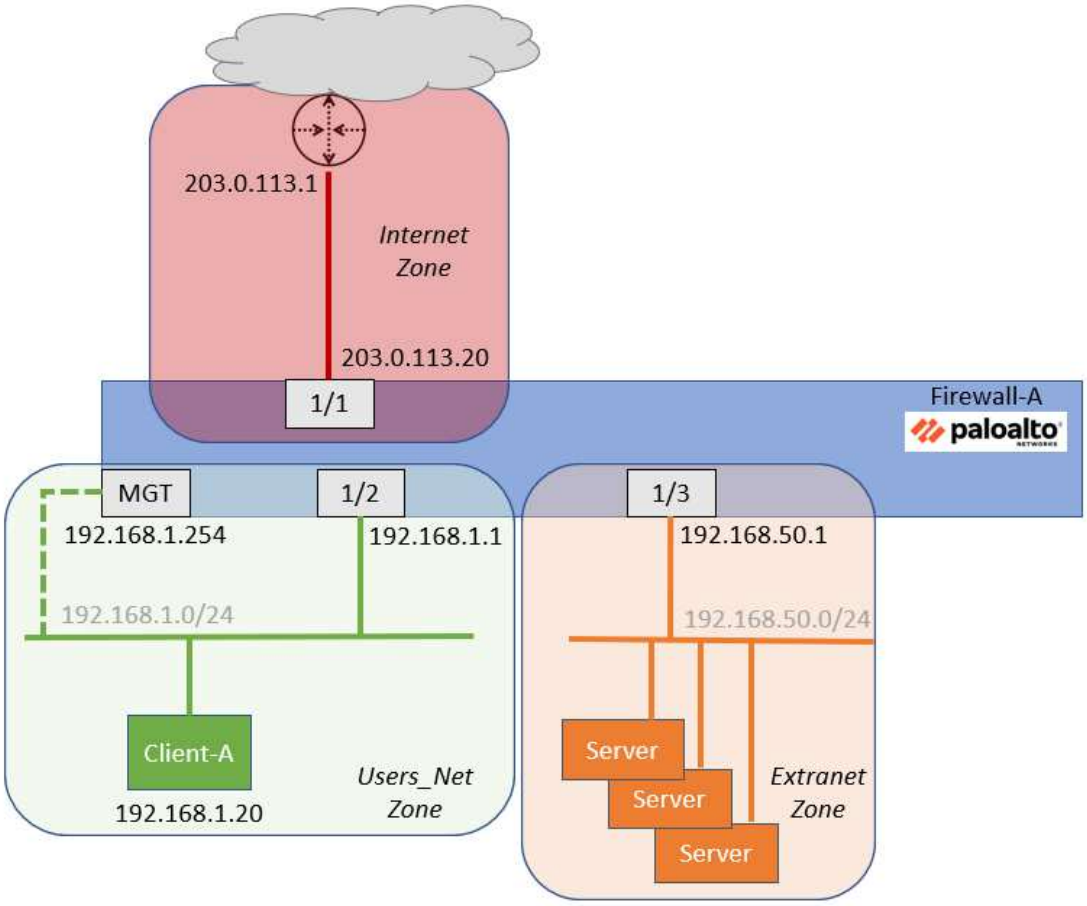
Document Version: 2025-10-13

Contents

Introduction

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.

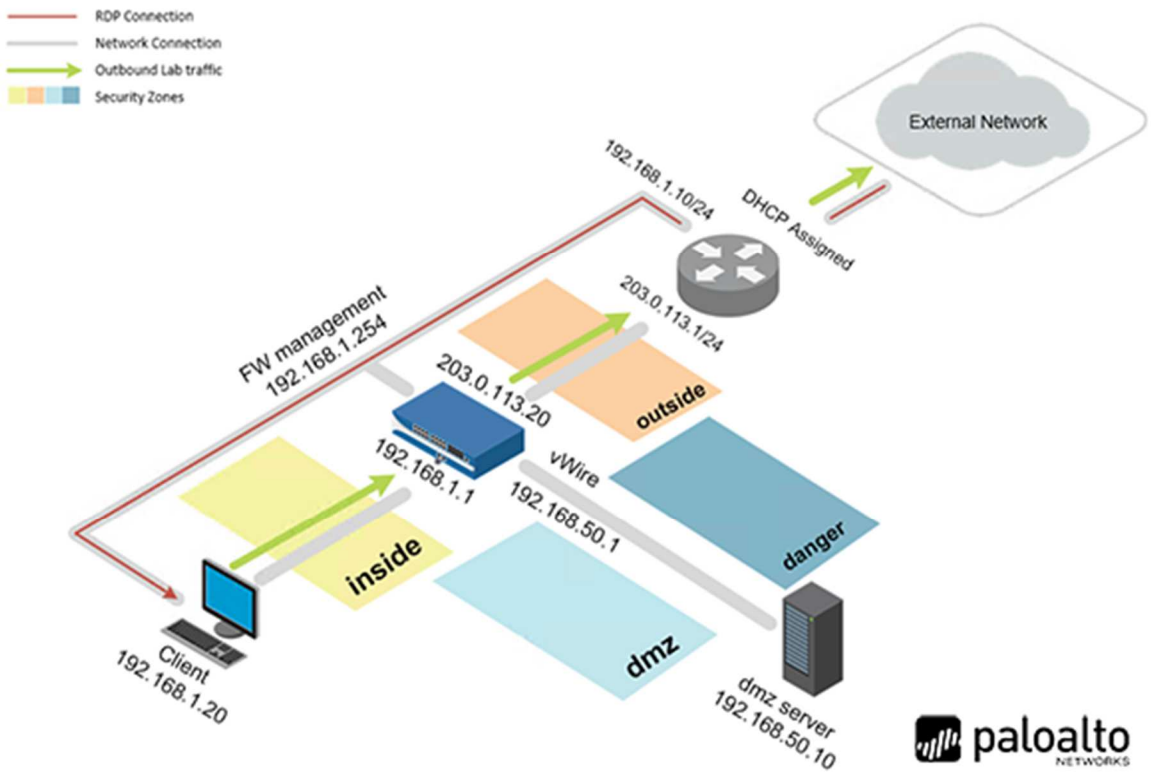


Objective

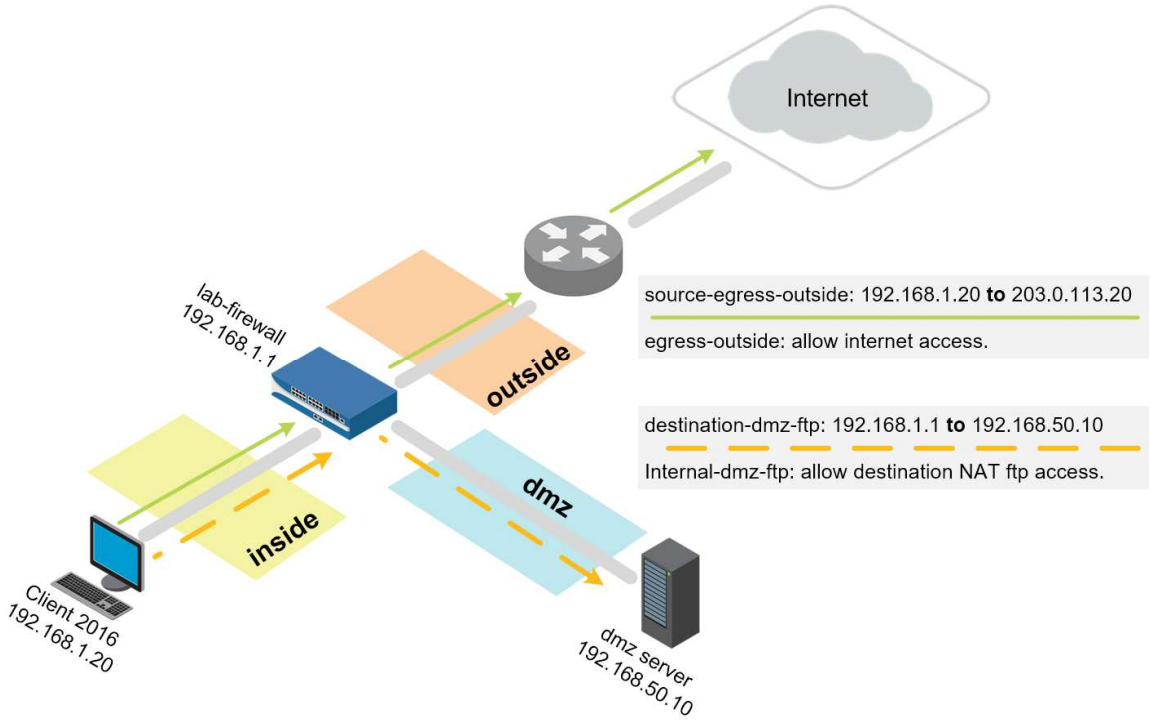
In this lab, you will perform the following tasks:

- 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.

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.

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 Security 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-05.xml** to the Firewall.

1.2 Create Security Policy Rule

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

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**

1.3 Commit the Configuration

- Commit the changes before proceeding.

1.4 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.

1.5 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 Firefox web browser on the Client-A client to connect to the Extranet web page at 192.168.50.80.

1.6 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.

1.7 Reset Rule Hit Counter

- Reset the **Hit Count** for the **Users_to_Extranet** rule.

1.8 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 **not** 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.

1.9 Enable Logging for Default Interzone Rule

- Edit the **Interzone** Security Policy rule and **enable Log at Session End.**

1.10 Commit the Configuration

- Commit the changes before proceeding.

1.11 Ping a Host on the Internet

- 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 interzone-default rule.

1.12 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 *to* 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 *from* 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**

1.14 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**

1.15 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**

1.16 Commit the Configuration

- Commit the changes before proceeding.

1.17 Ping Internet Host from Client A

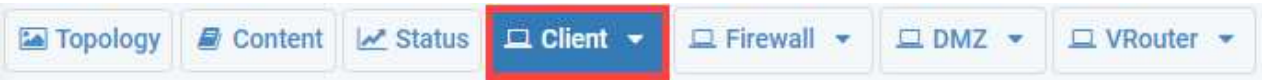
- From the terminal window on the Client-A host, ping 8.8.8.8. You will not get a reply
- Examine the Traffic Log again and use a simple filter to see if there are any entries for this session that failed.
- The entries in the Traffic Log should show you that the ping sessions are hitting the **Users_to_Internet**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

2 Creating and Managing Security Policy Rules – Detailed Lab Steps

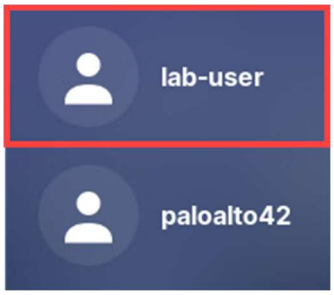
2.1 Apply a Baseline Configuration to the Firewall

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.



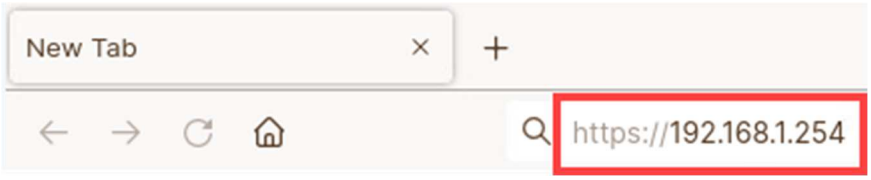
2. On the *Zorin* desktop, click **lab-user.**



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

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

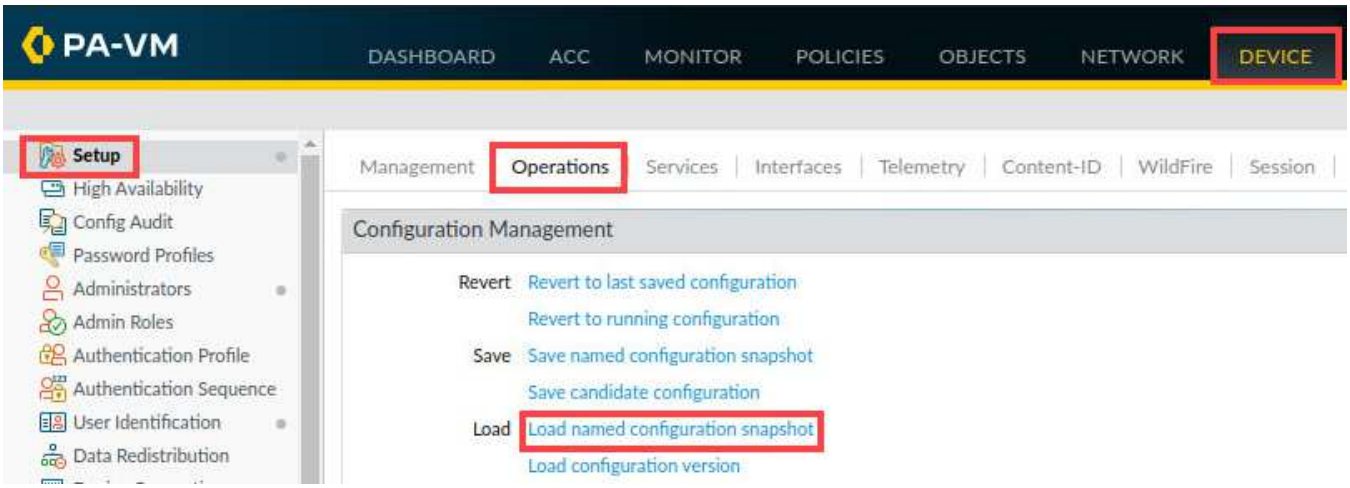
5. In the *Firefox* address field, type **`https://192.168.1.254`** and press **Enter**.



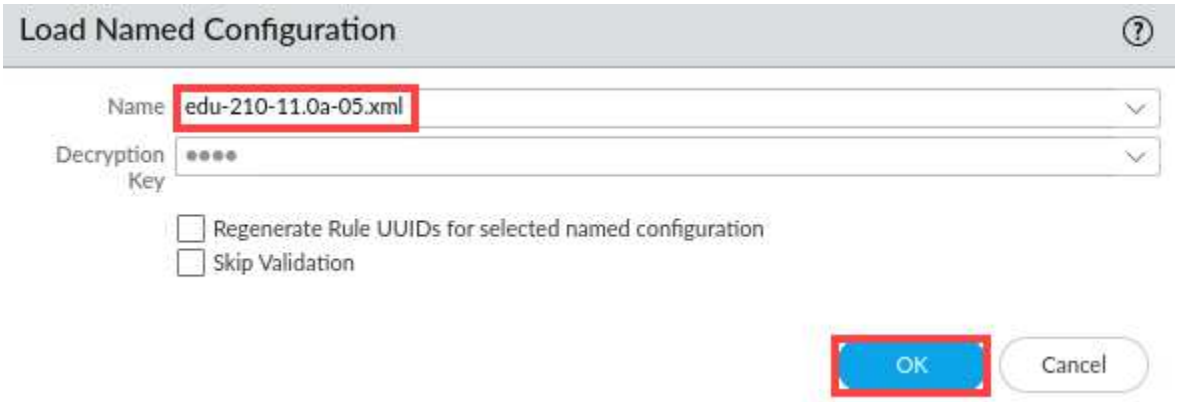
6. Log in to the Firewall web interface as username **admin**, password **`Pal0Alt0!.`**

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.

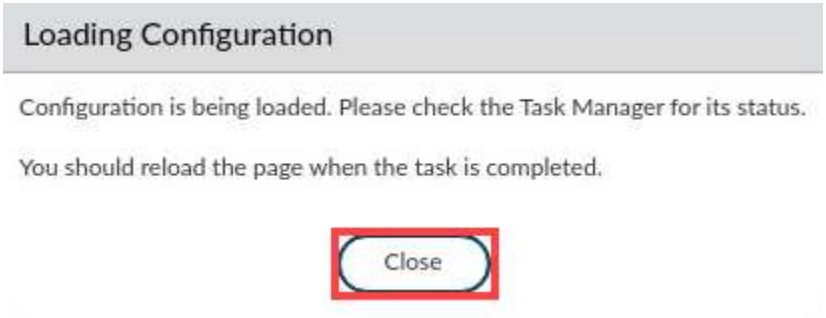
7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



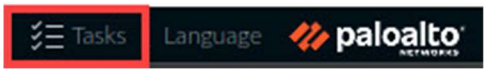
8. In the *Load Named Configuration* window, select **edu-210-11.0a-05.xml** from the *Name* drop-down box and click **OK**.



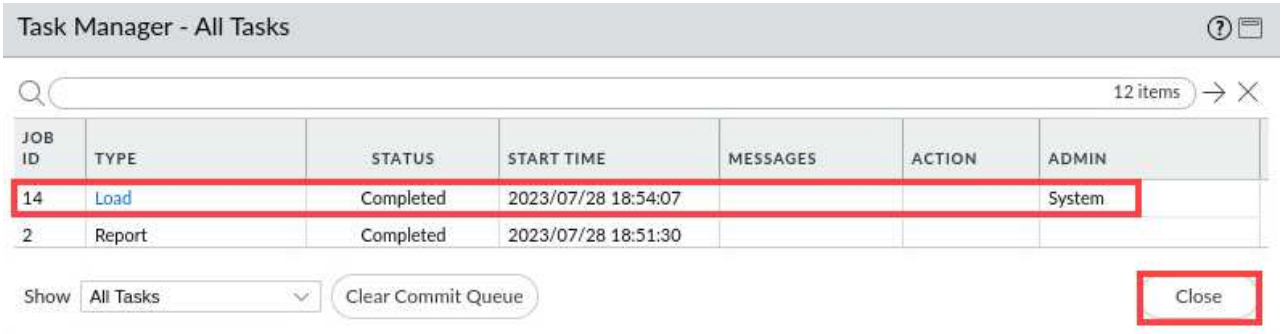
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

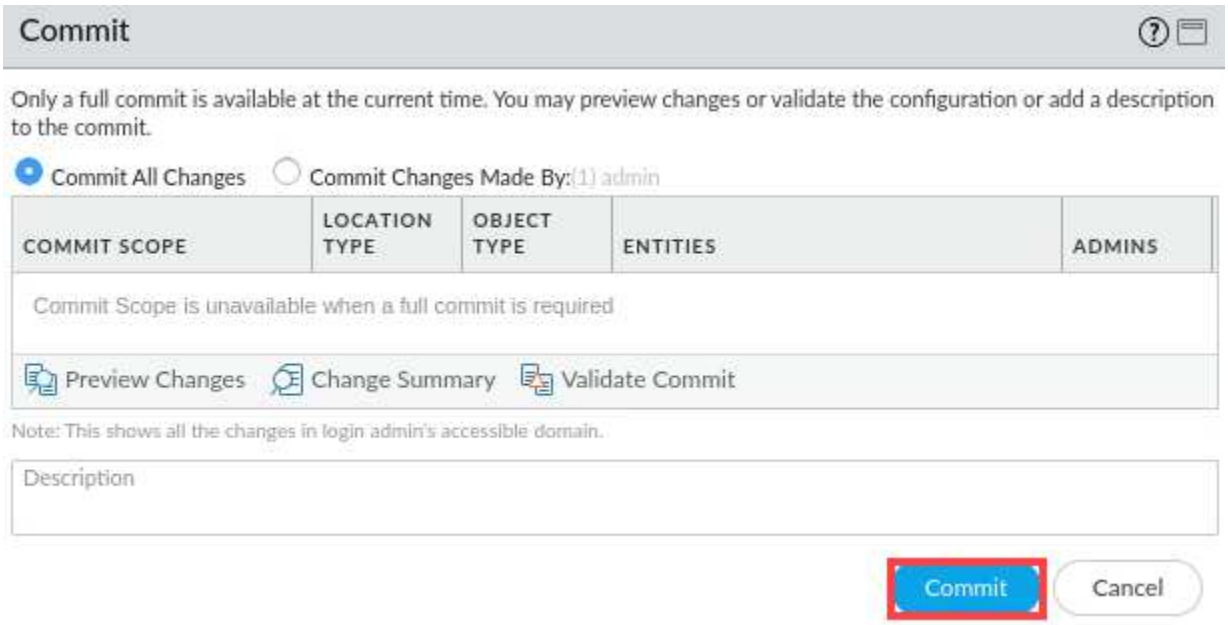


11. In the *Task Manager – All Tasks* window, verify the *Load* type has been completed. Click **Close**

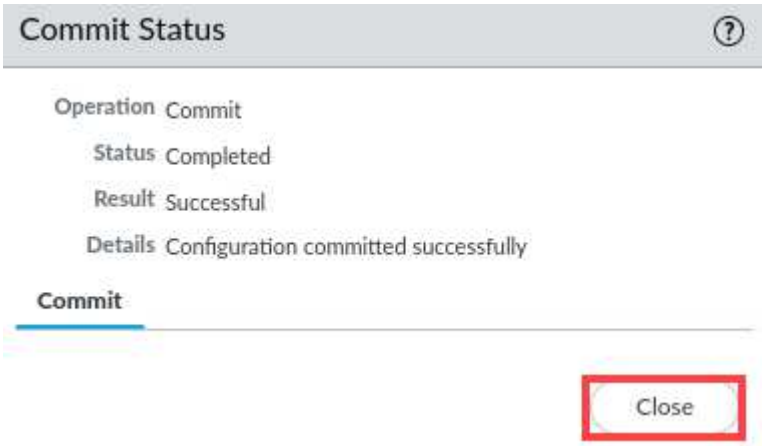


12. Click the **Commit** link located at the top-right of the web interface.

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



14. When the commit operation is complete, click **Close** to continue.

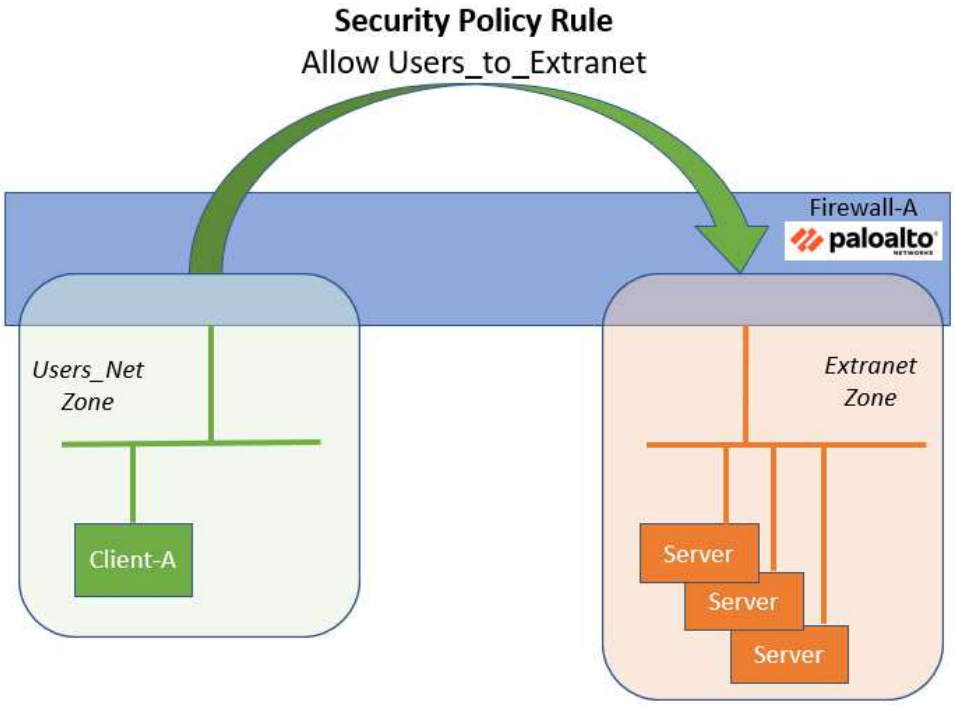


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

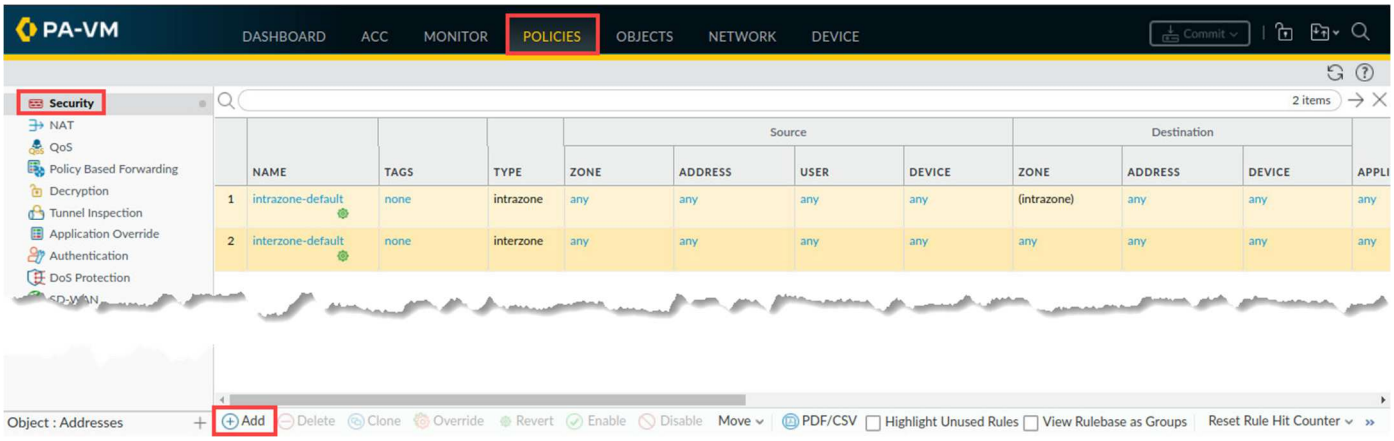
15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

2.2 Create a Security Policy Rule

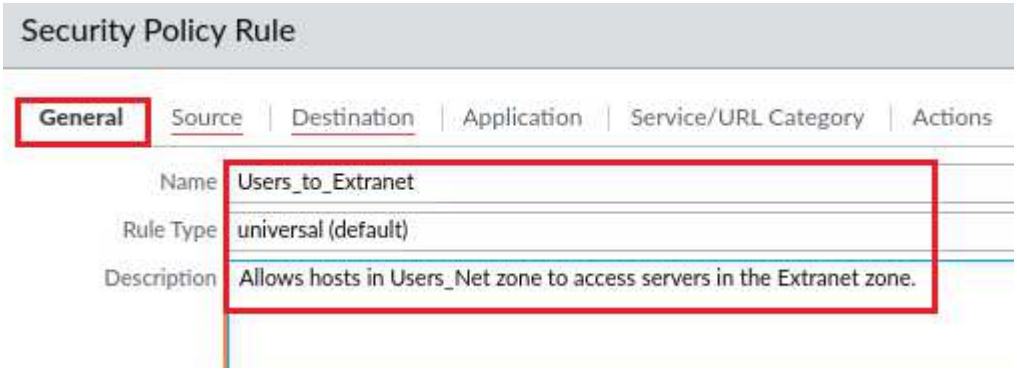
You need to allow network traffic from the Users_Net security zone to the Extranet security zone so that employees can access various business applications. In this section, you will create a Security Policy rule to allow access between these two zones.



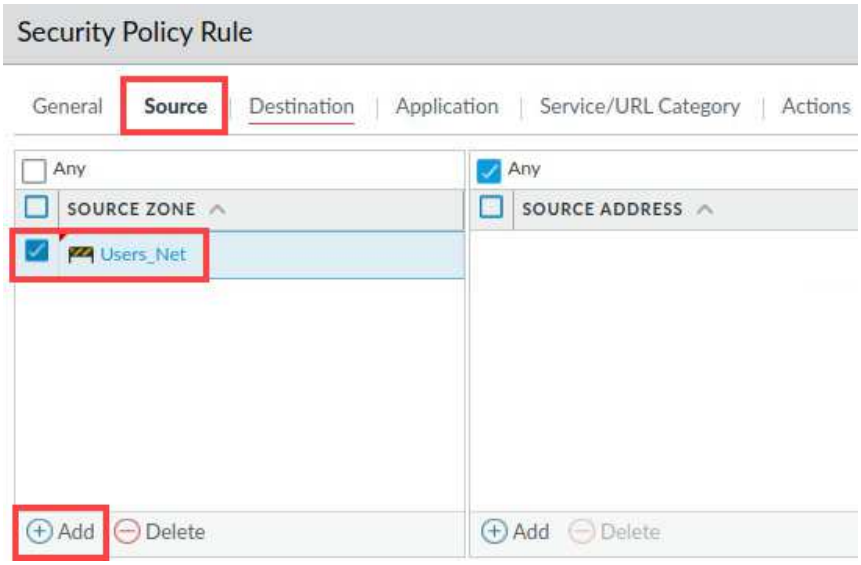
1. In the web interface, select **Policies > Security**. Click **Add**.



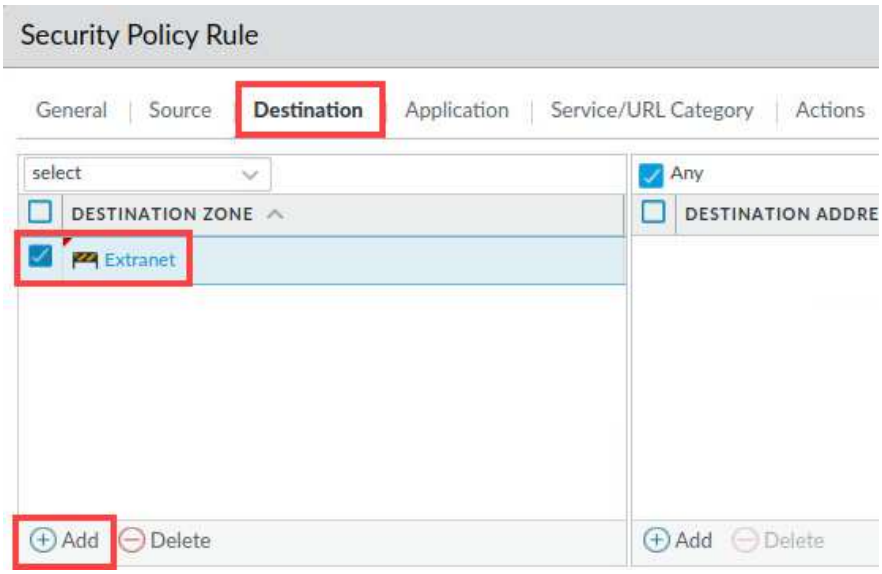
2. In the *Security Policy Rule* window, on the *General* tab. Type **`Users_to_Extranet`** for the N*ame*. For *Description*, enter **`Allows hosts in Users_Net zone to access servers in Extranet zone`**.



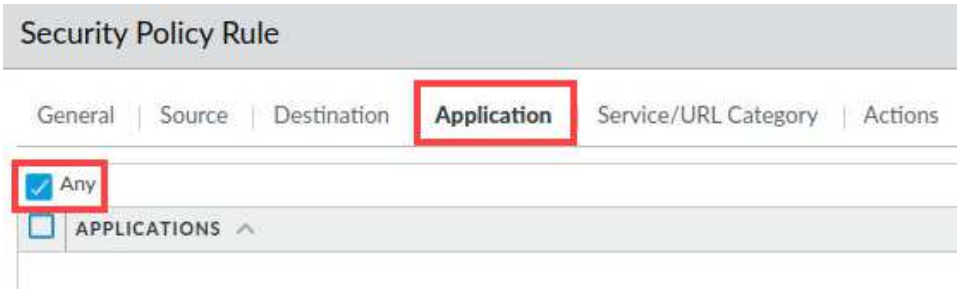
3. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users_Net**.



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



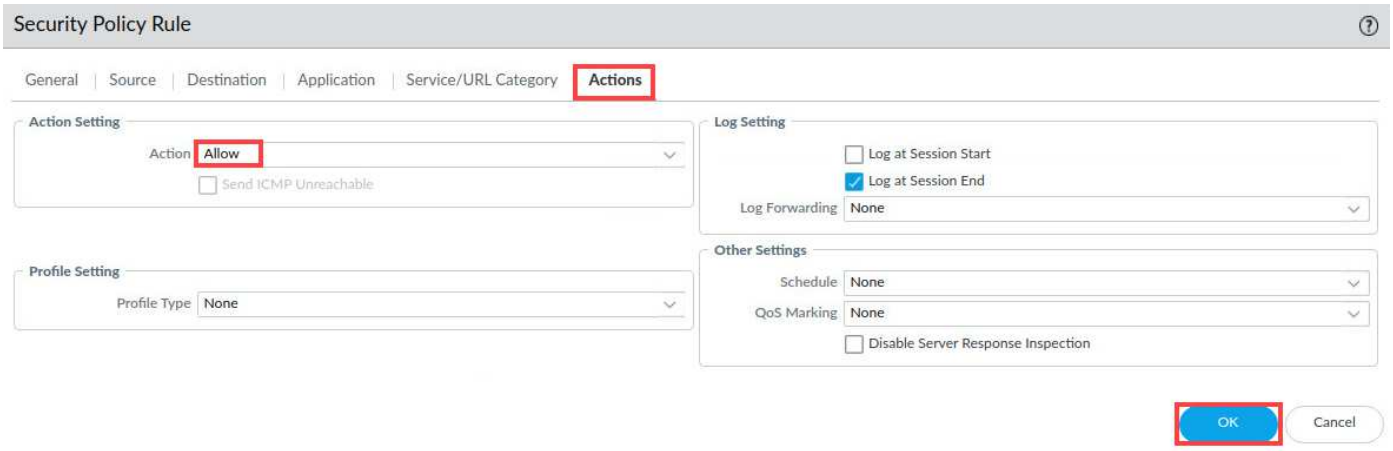
5. Select the **Application** tab. Verify **Any** is selected for *Applications*.



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

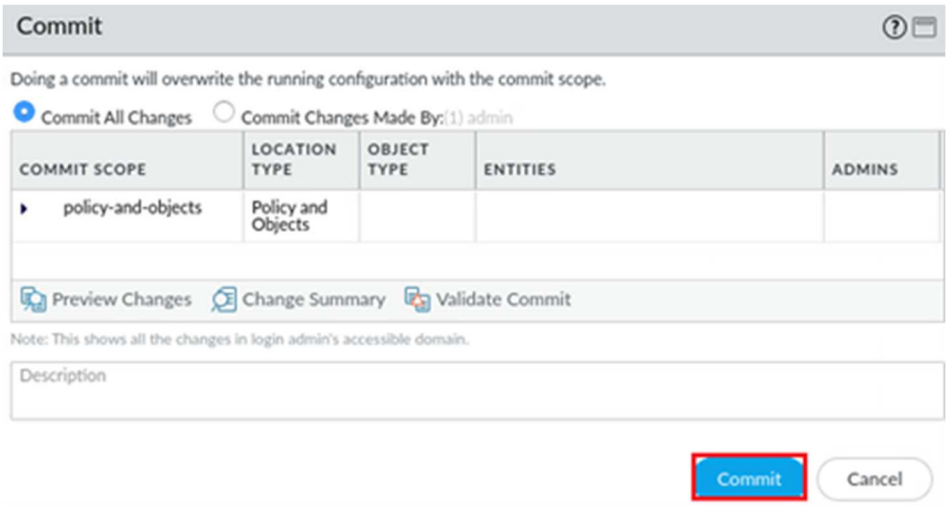
8. Verify the *Users_to_Extranet* security policy rule appears in the Security policies window.

Please Note

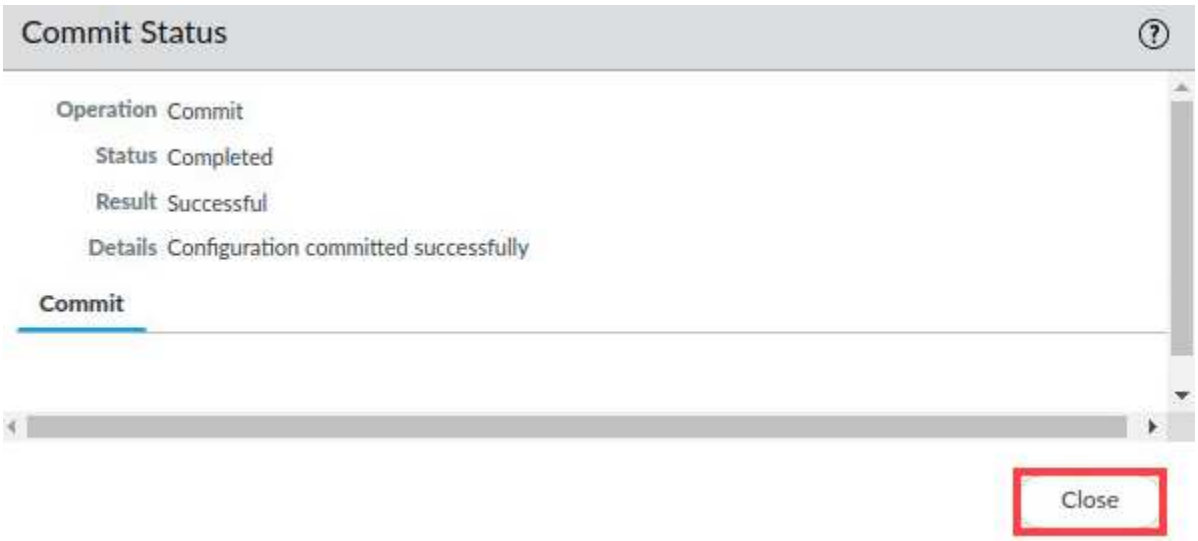
The rule appears above the two preconfigured entries intrazone-default and interzone-default. These two rules always appear at the bottom of the ruleset.

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

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



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

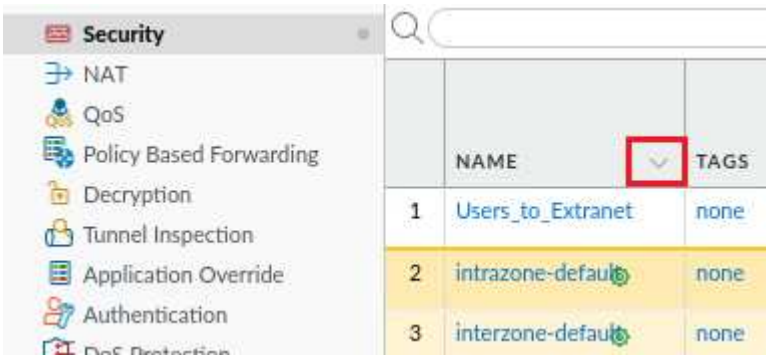


12. Leave the web interface open and continue to the next task.

2.3 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.

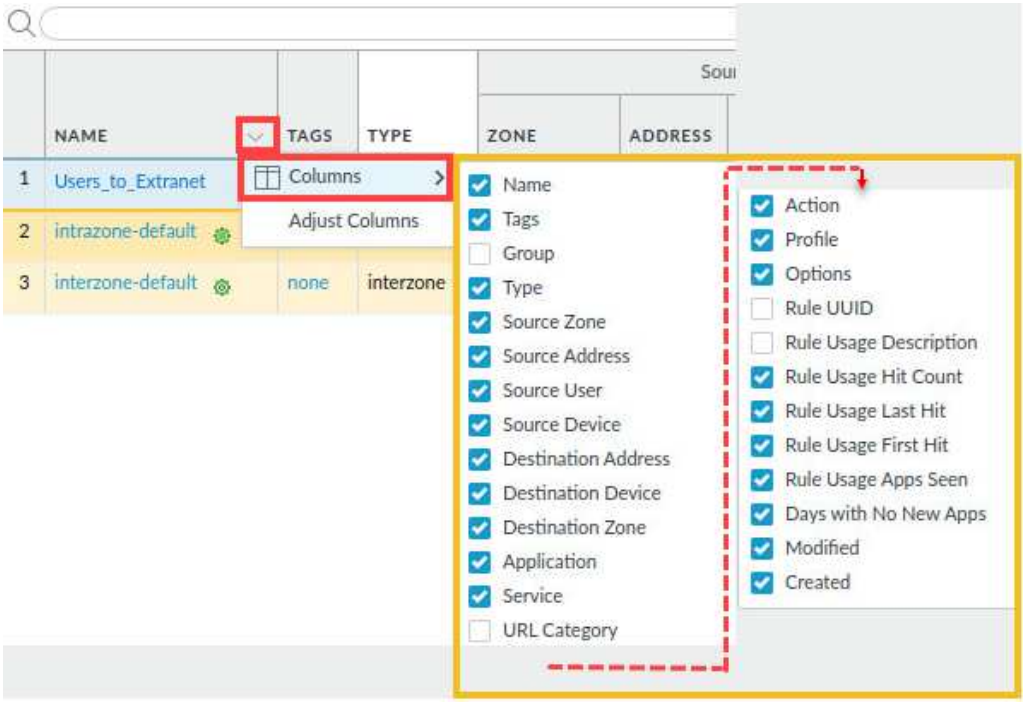
1. In the *Security Policy* window, click the small drop-down icon next to the **Name** column in the Security Policy table. You may need to hover your pointer over the icon for it to appear.



Please Note

This icon is available next to all column headers.

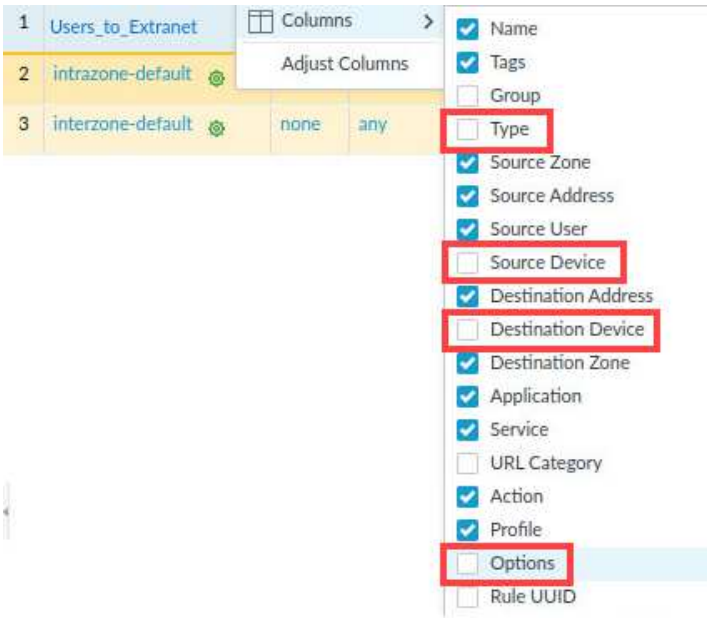
2. Choose **Columns** and note the available columns that you can hide or display in this table.



Please Note

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

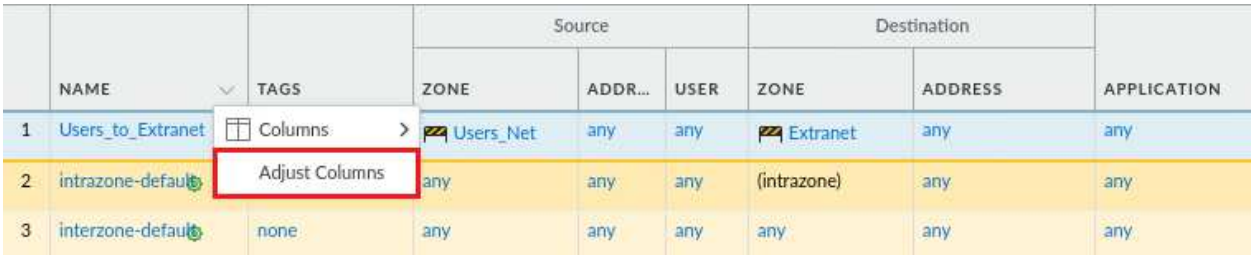
3. In the *Column*, uncheck **Type**, **Source Device**, **Destination Device** and **Options**.



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 drop-down icon again and choose **Adjust Columns**.



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

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.

2.4 Test New Security Policy Rule

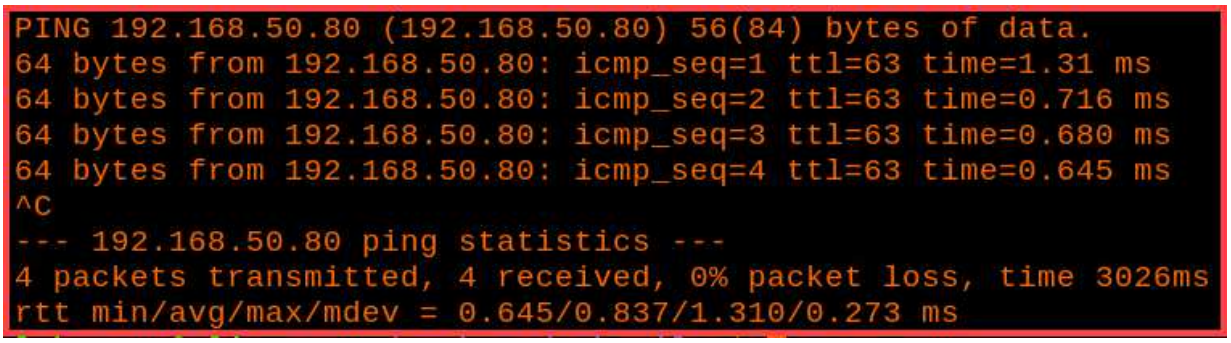
In this section, you will test the new security policy rule you created in a previous task.

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

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

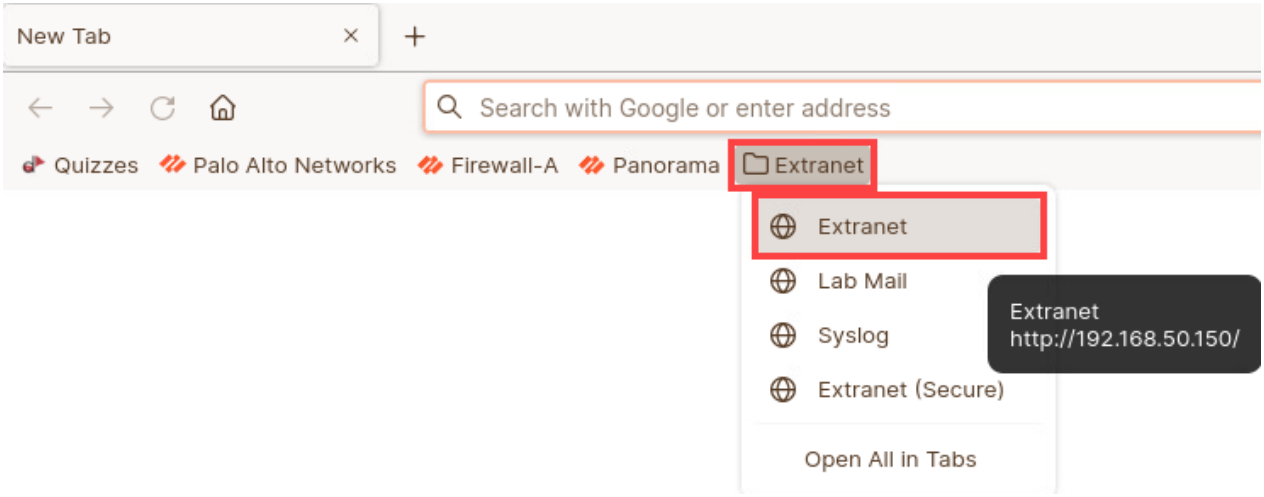
```
lab-user@client-a:~/Desktop/Lab-Files$ ping 192.168.50.80 <Enter>
```

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.



4. On the *client* desktop, open a new **Firefox Web Browser** window.

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. Re-open the *PA-VM firewall* interface by clicking the **firewall-a – Mozilla Firefox** icon in the taskbar.

9. Leave the Terminal and Firewall web interface open and continue to the next task.

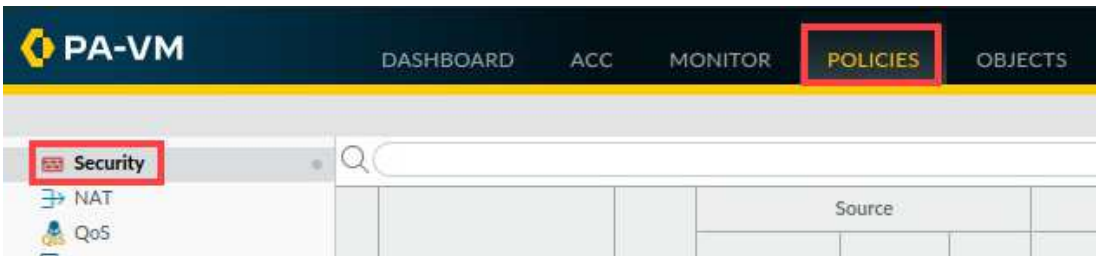
2.5 Examine and Reset the Rule Hit Count

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.

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



2. 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 **1263** hits. You may get different results, but the conclusion will be the same.

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

4. In the terminal window, 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.

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



```
lab-user@client-a:~/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=1.31 ms
64 bytes from 192.168.50.80: icmp_seq=2 ttl=63 time=0.716 ms
64 bytes from 192.168.50.80: icmp_seq=3 ttl=63 time=0.680 ms
64 bytes from 192.168.50.80: icmp_seq=4 ttl=63 time=0.645 ms
^C
--- 192.168.50.80 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3026ms
rtt min/avg/max/mdev = 0.645/0.837/1.310/0.273 ms
```

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.

6. Highlight the **Users_to_Extranet** Security policy rule. But do not open it.

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

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

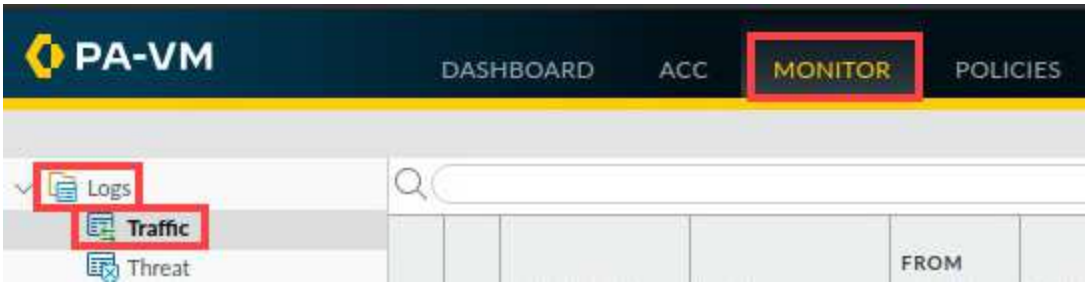
8. Notice the *Hit Count* for *Users_to_Extranet* has been reset to **0**.

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

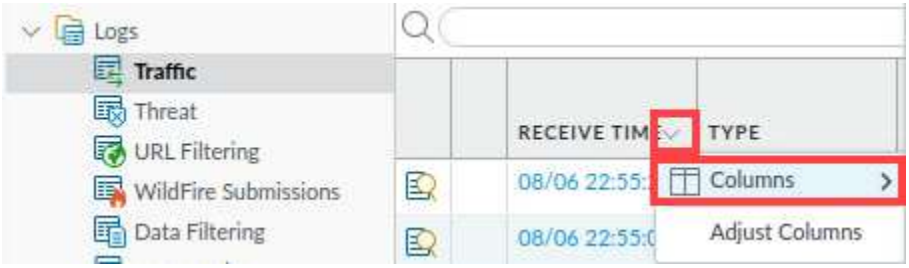
2.6 Examine the Traffic Log

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.

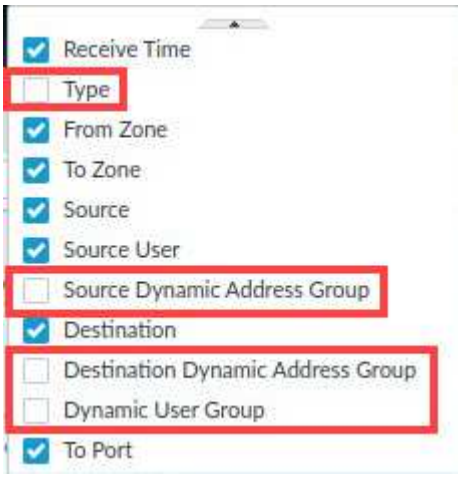
1. In the *Firewall* interface, select **Monitor > Logs > Traffic**.



2. Click the drop-down 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.

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


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.
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7164ms

lab-user@client-a:~/Desktop/Lab-Files$
```

7. Minimize the *Terminal* window 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.

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.

Q1. Have any entries been recorded in the Traffic log for the filter (addr.dst eq 8.8.8.8) and (zone.src eq Users_Net)?

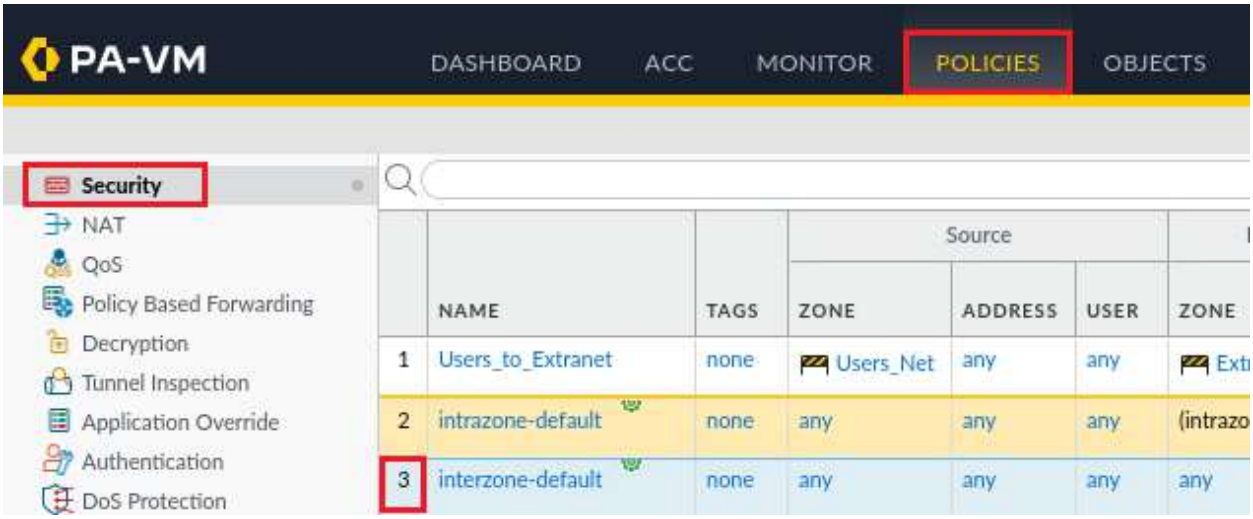
a. Yes
b. No

There are two reasons why the firewall did not log any traffic logs with the filter you applied.

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.

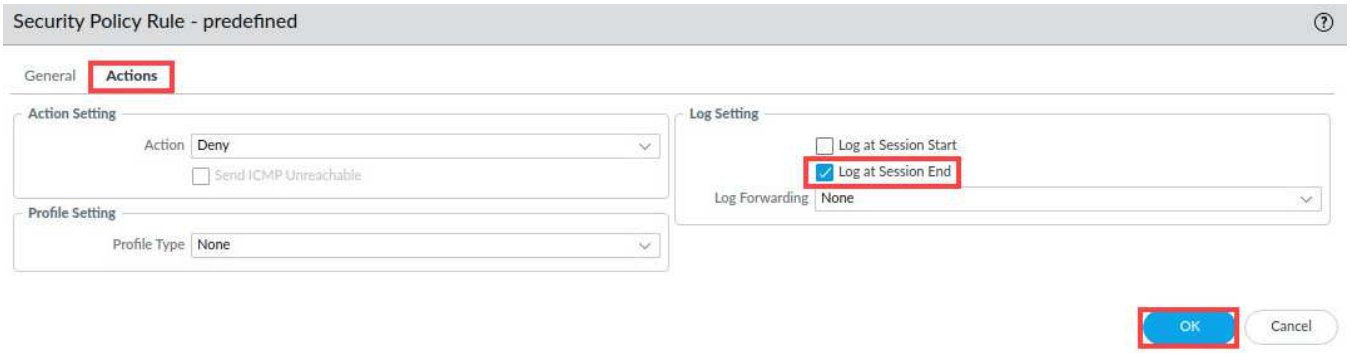
Second, remember that traffic that hits the interzone-default rule is not automatically logged. You must manually change a setting on this rule to see entries in the Traffic log. You will enable this setting

9. 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.



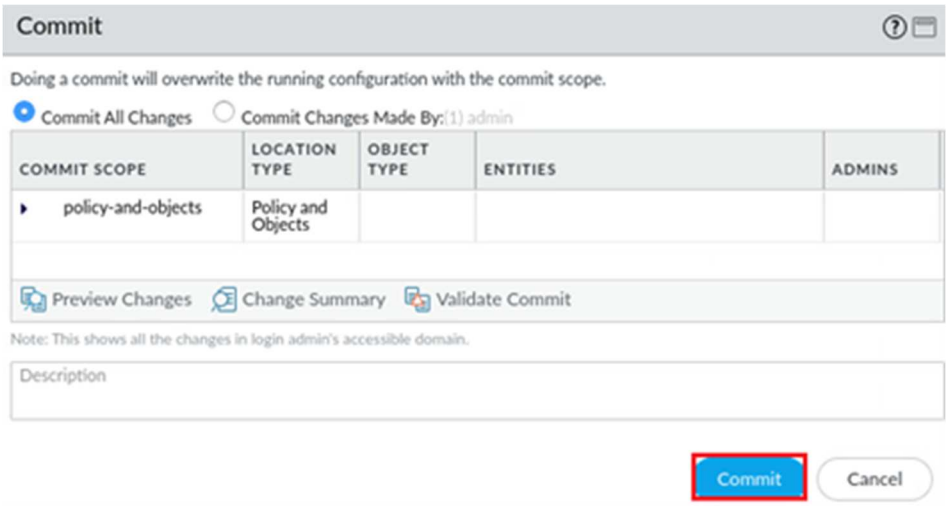
10. Click the **Override** button at the bottom of the window.

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

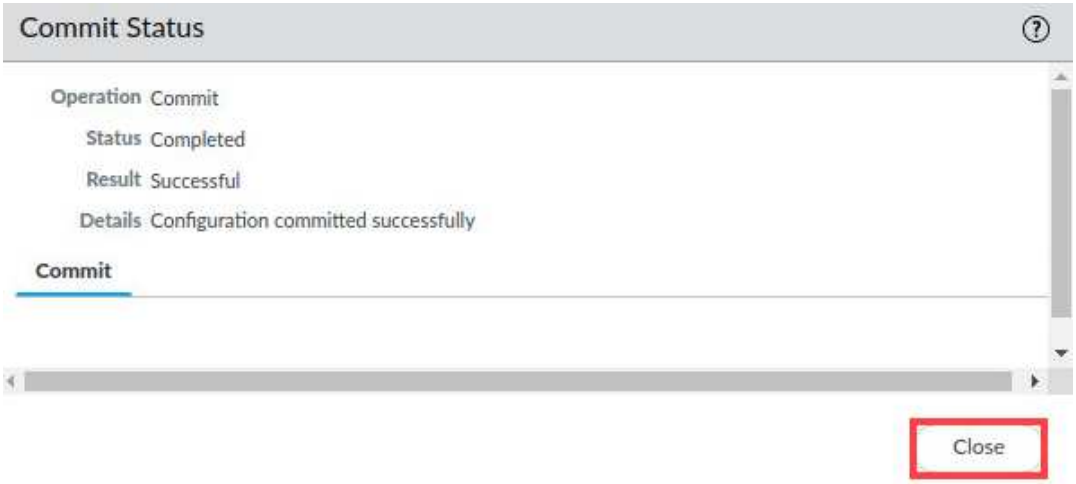


12. Click the **Commit** button at the upper right of the web interface.

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.

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

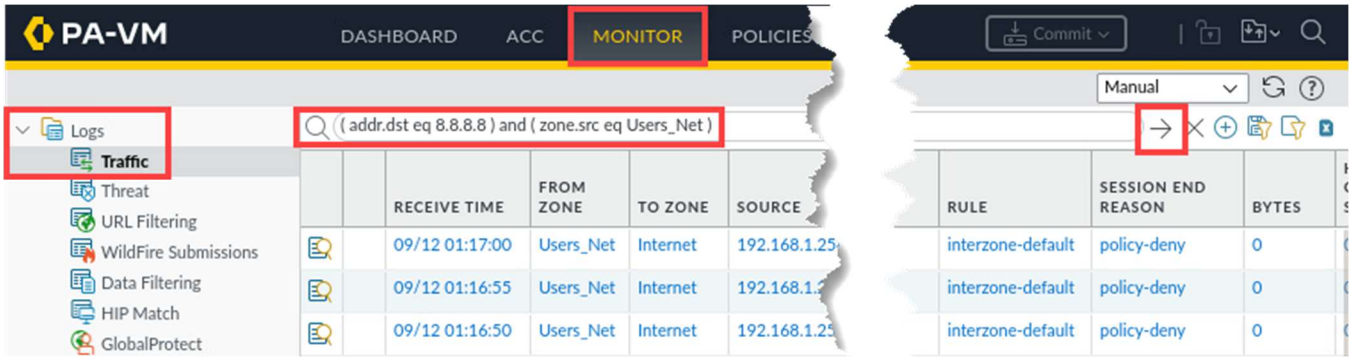
17. After a few seconds, use **Ctrl+C** to stop the connection because it will not succeed.

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7164ms

lab-user@client-a:~/Desktop/Lab-Files$
```

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

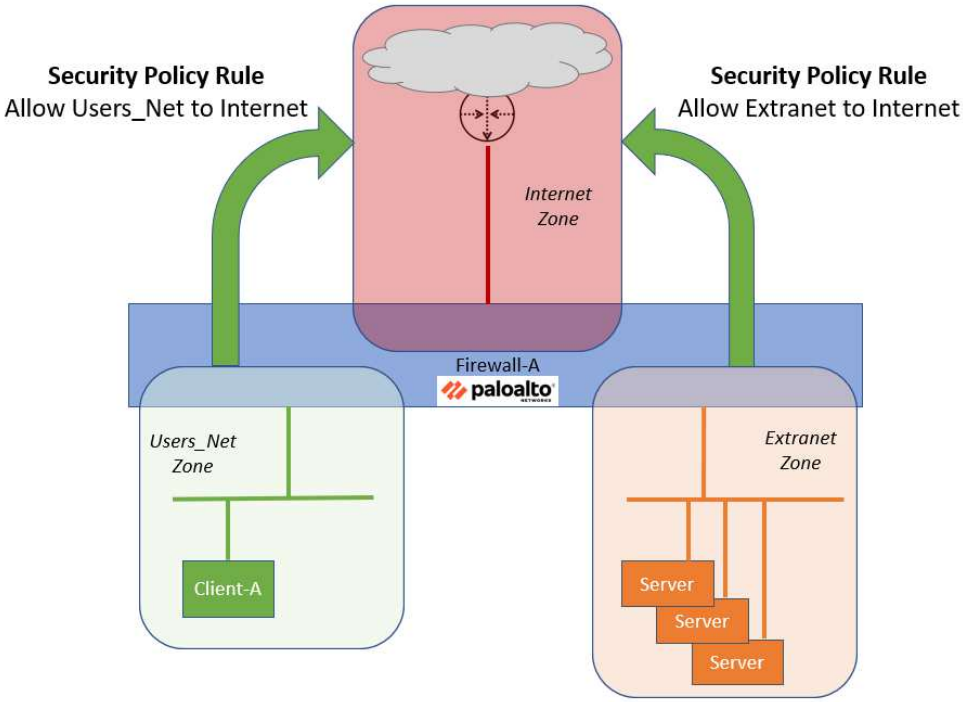
19. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter **`( addr.dst eq 8.8.8.8 ) and ( zone.src eq Users_Net )`.** Click the **Apply Filter** button in the upper right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



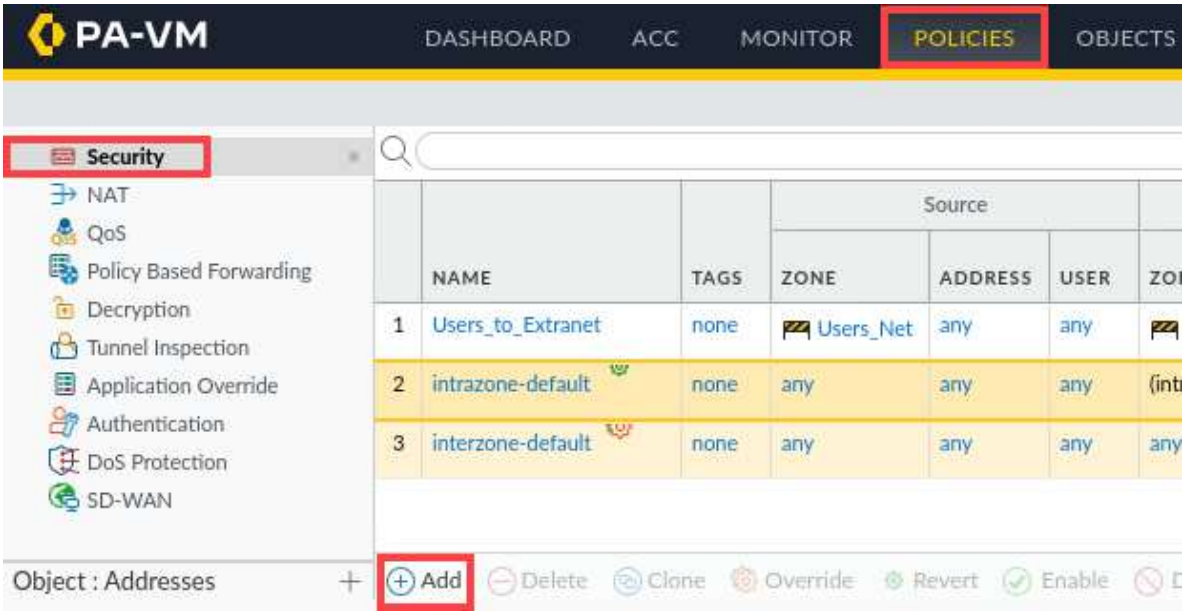
20. Leave the web interface open and continue to the next task.

2.7 Create Security Rules for Internet Access

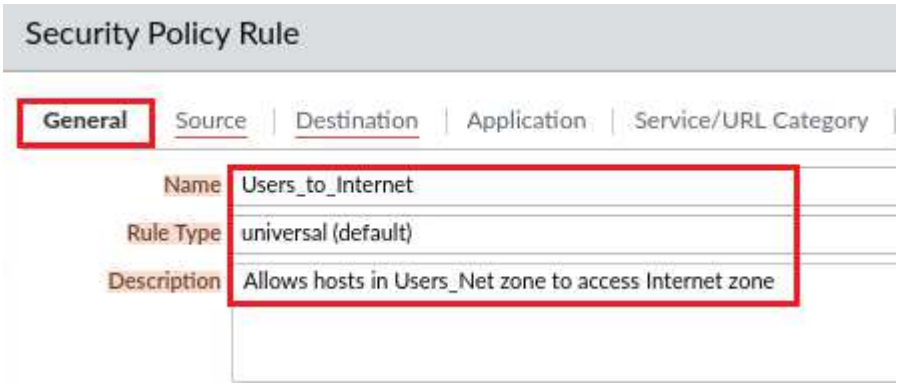
In this section, you will create Security policy rules to allow hosts in your network to access the Internet. You need to create a rule for hosts in the Users_Net security zone to access hosts in the Internet security zone. You also need to create a rule to allow hosts in the Extranet security zone to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



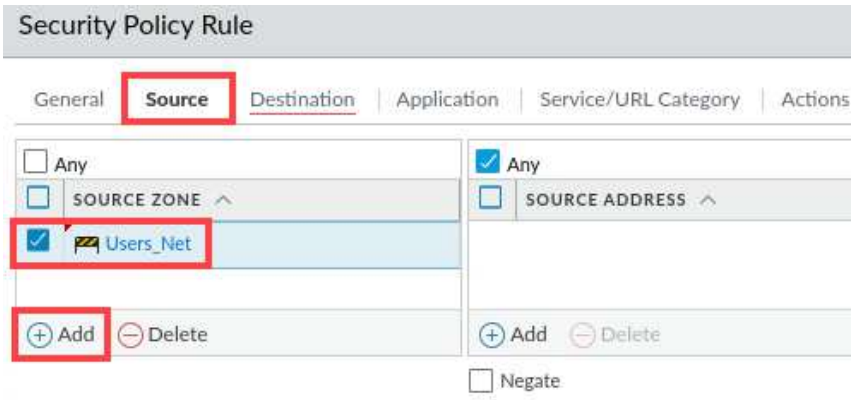
1. In the *PA-VM firewall* web interface, navigate to **Policies > Security**. Click **Add** at the bottom of the window.



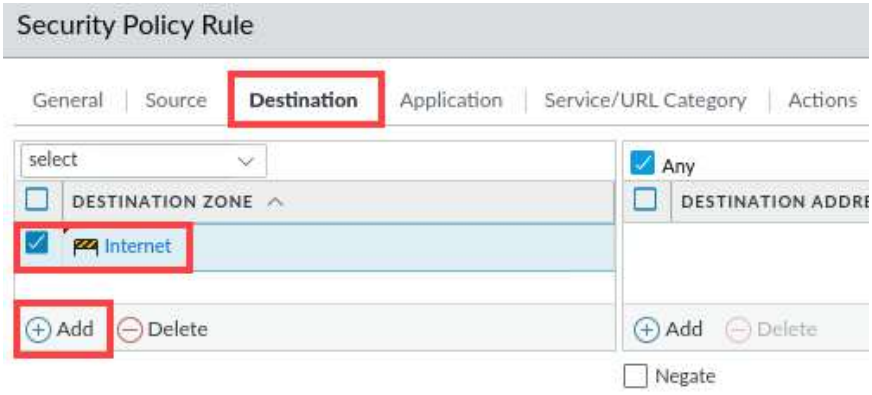
2. In the *Security Policy Rule* window, on the *General* tab. Type **`Users_to_Internet`** for the *Name*. For *Description*, enter **`Allows hosts in Users_Net zone to access Internet zone`**.



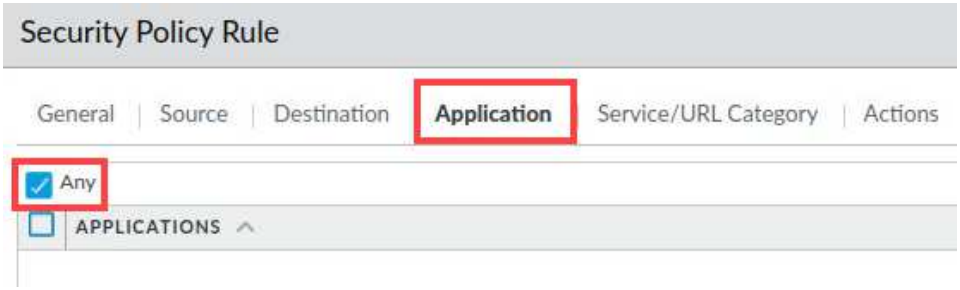
3. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users_Net**.



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



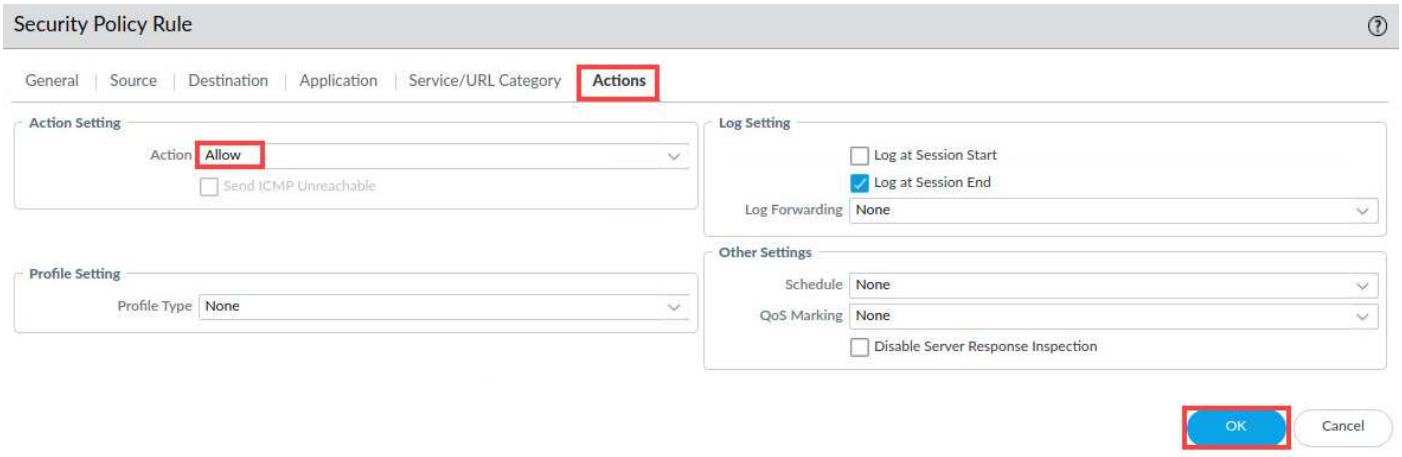
5. Select the **Application** tab. Verify **Any** is selected for *Applications*.



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

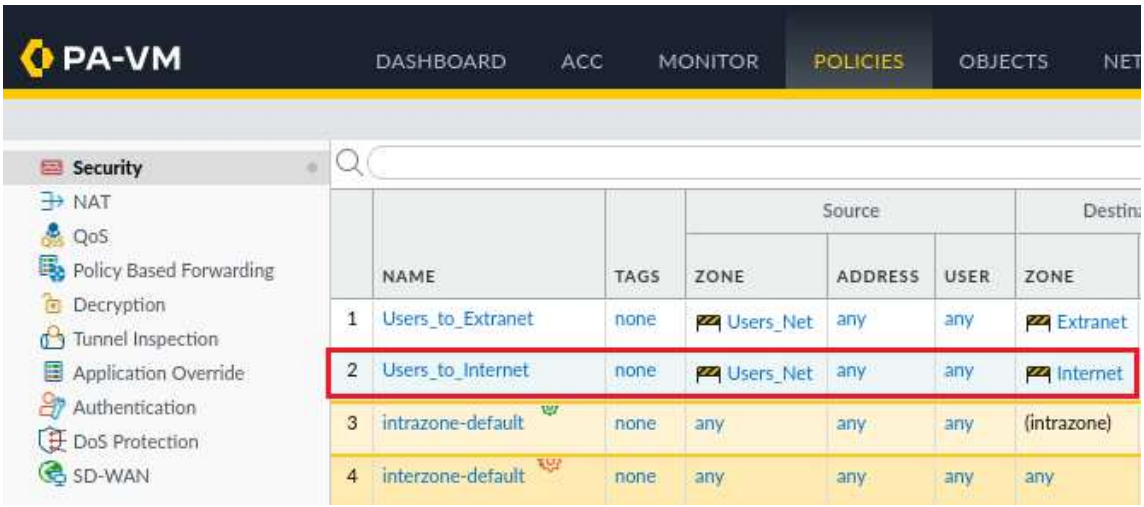
7. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default**.** Click **OK**.



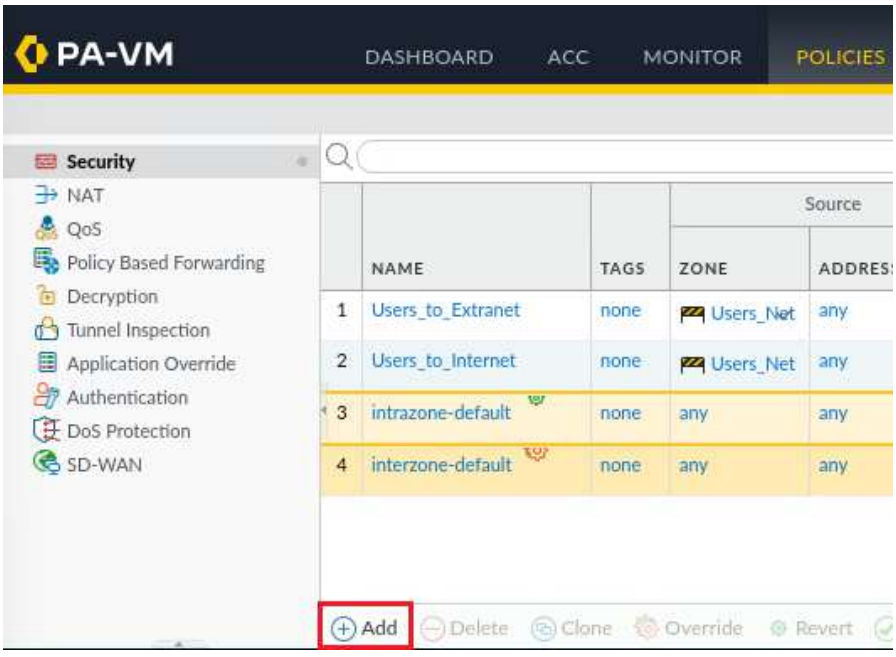
Please Note

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_Internet* security policy rule appears in the Security policies window.

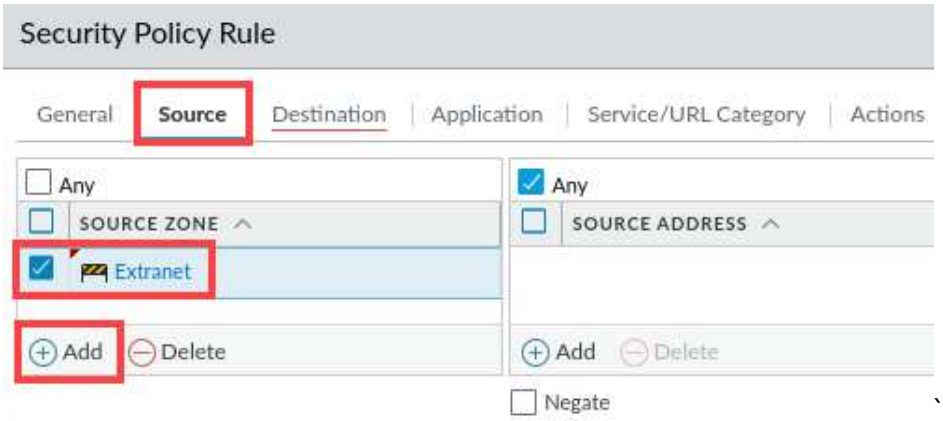


9. Click **Add** at the bottom of the *Security policy* window.

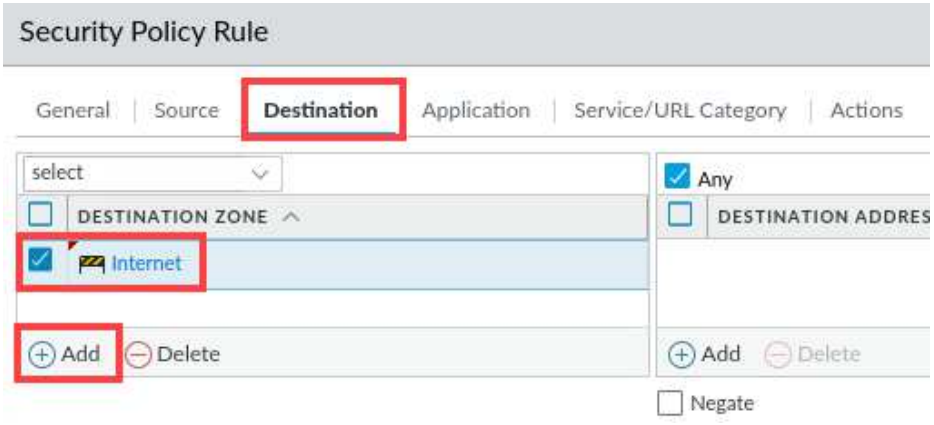


10. In the *Security Policy Rule* window, on the *General* tab. Type **`Extranet_to_Internet`** for the *Name*. For *Description*, enter **`Allows hosts in Extranet zone to access Internet zone`**.

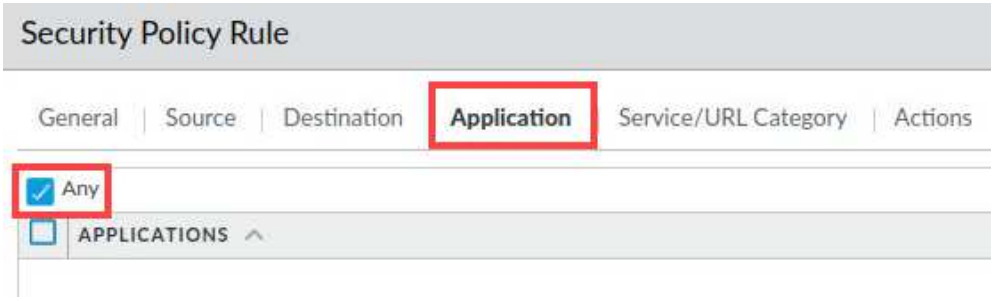
11. Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Extranet**.



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



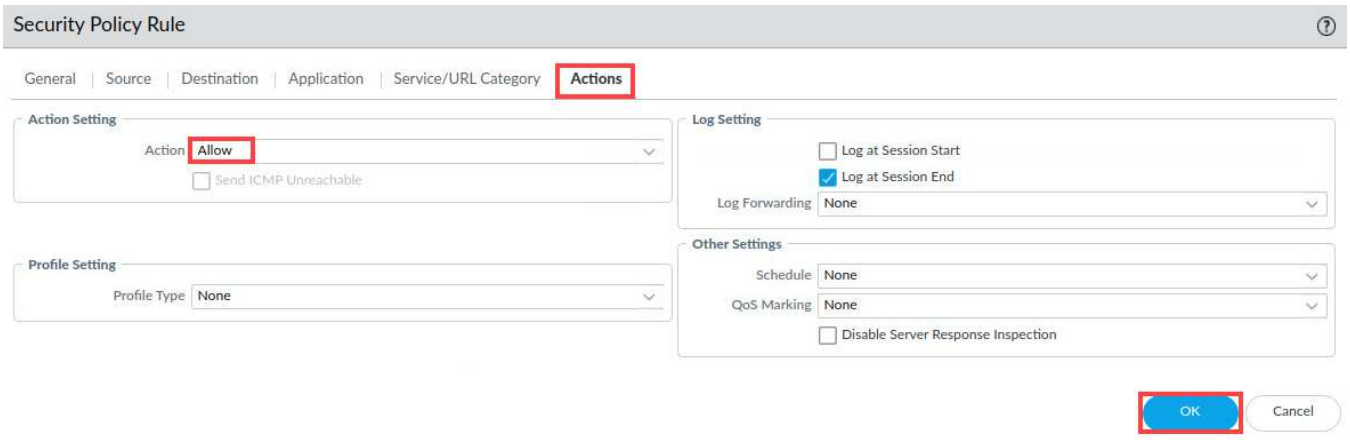
13. Select the **Application** tab. Verify **Any** is selected for *Applications*.



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

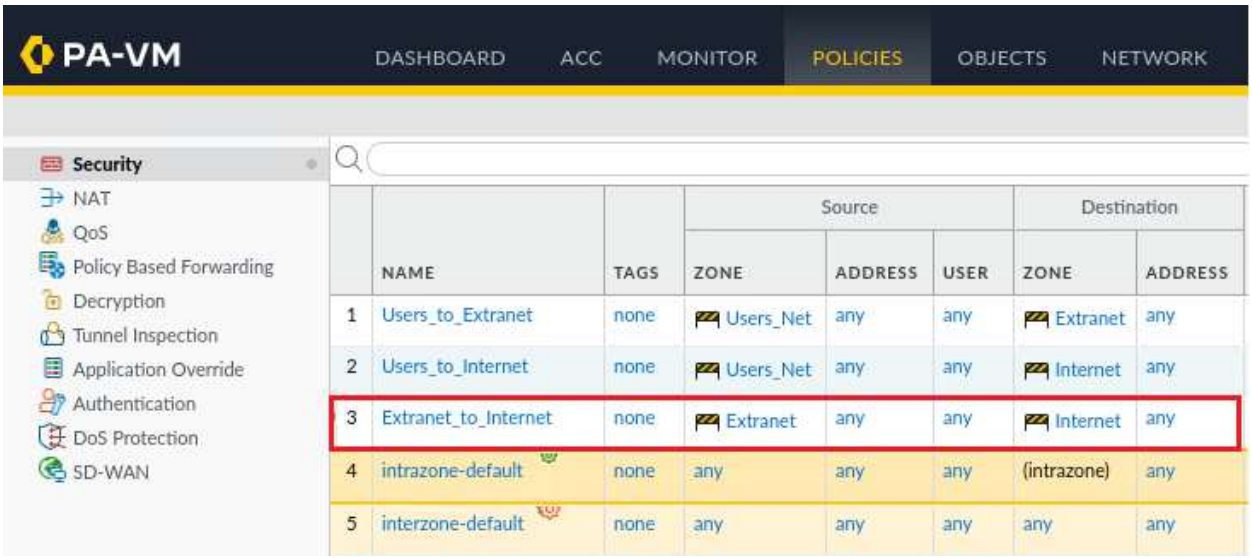
15. Select the **Actions** tab. Do not make any changes in this section but notice that the *Action* is set to **Allow** by default**.** Click **OK**.



Please Note

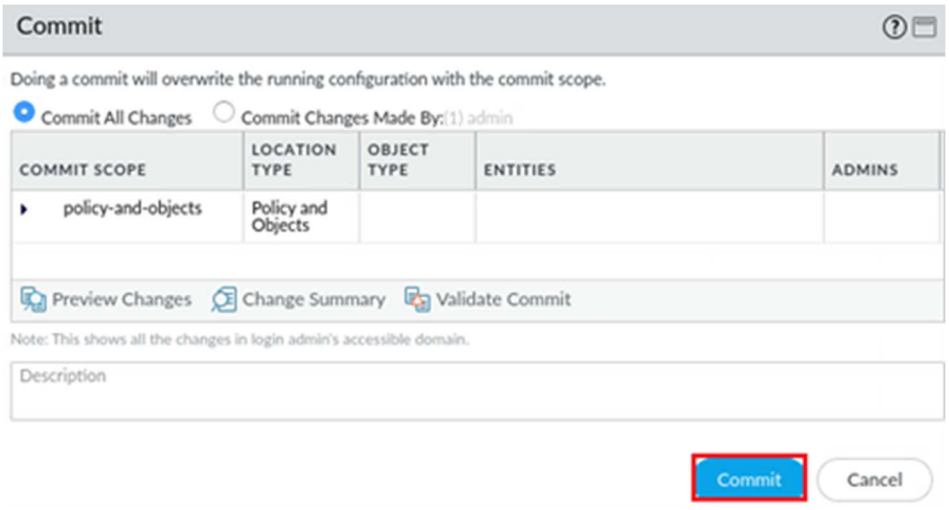
When you create a new Security policy rule, the Action is automatically set to Allow. If you are creating a rule to block traffic, make sure you select the Actions tab and change the Action before you commit the rule.

16. Verify the *Extranet_to_Internet* security policy rule appears in the Security policies window.

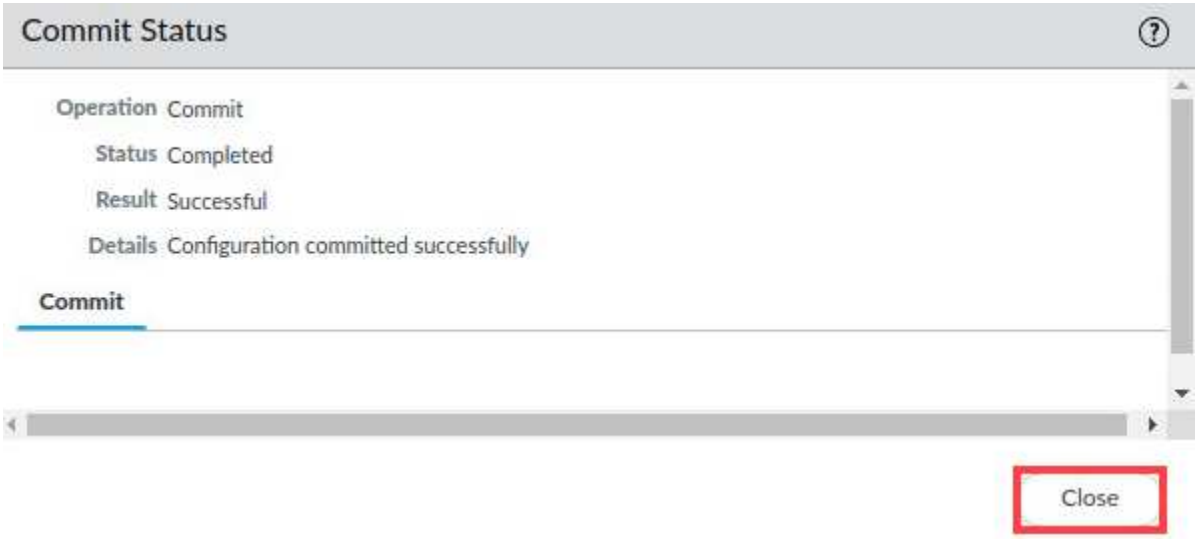


17. Click the **Commit** button at the upper right of the web interface.

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



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



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

2.8 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.

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

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.
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7164ms

lab-user@client-a:~/Desktop/Lab-Files$
```

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

5. Re-open 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.

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. In the next lab, you will need to create a NAT policy so that ping will be successful.

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