CYBERSECURITY FOUNDATION V2

Lab 3: Creating a Zero Trust Environment

Document Version: 2022-12-22

Contents

Introduction

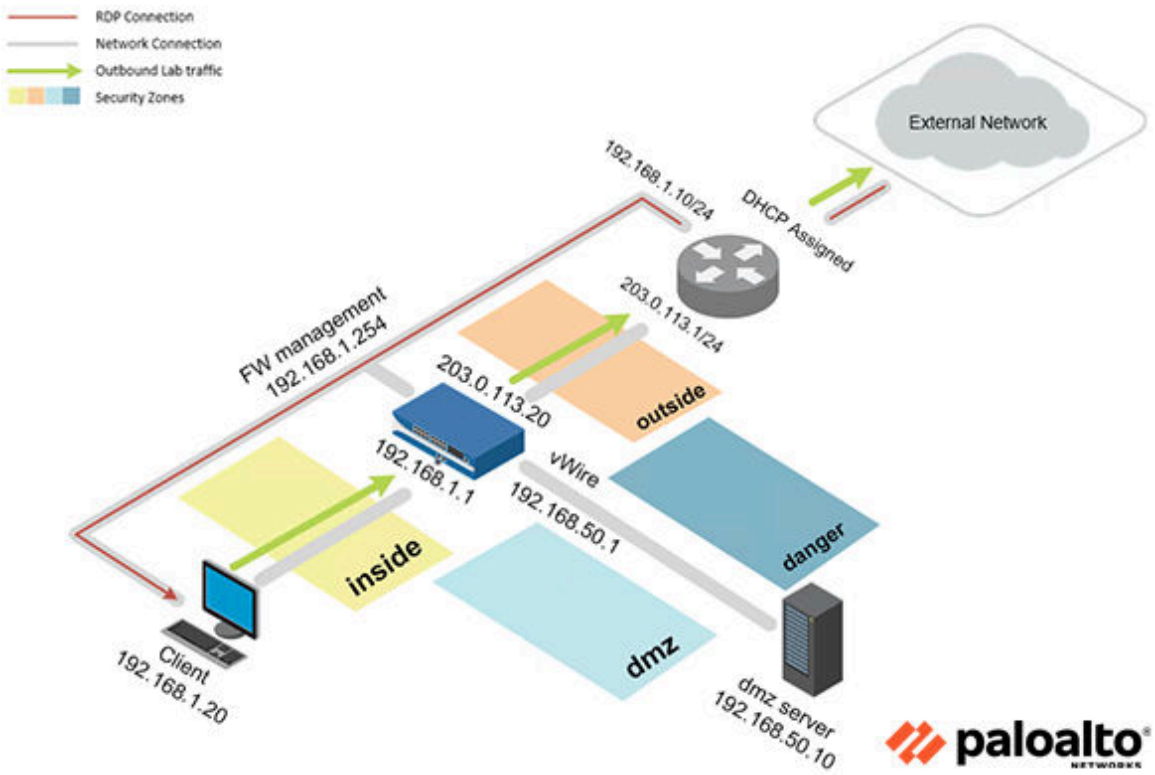
In this lab, you will configure the Firewall with three zones: **inside**, **outside**, and **dmz**. Then, you will apply security policies to these zones to ensure all traffic between zones is being monitored by the Firewall.

Objective

In this lab, you will perform the following tasks:

- Create Zones and Associate the Zones to Interfaces
- Create a Security Policy Rule
- Create a NAT Policy
- Commit and Test the Rules and Policies

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.

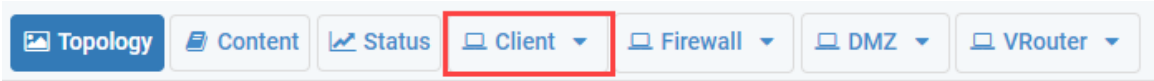
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Creating a Zero Trust Environment

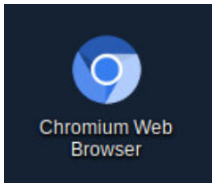
1.0 Load Lab Configuration

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

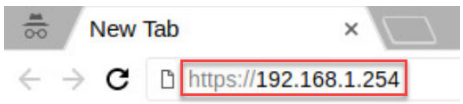
1. Click on the **Client** tab to access the Client PC.



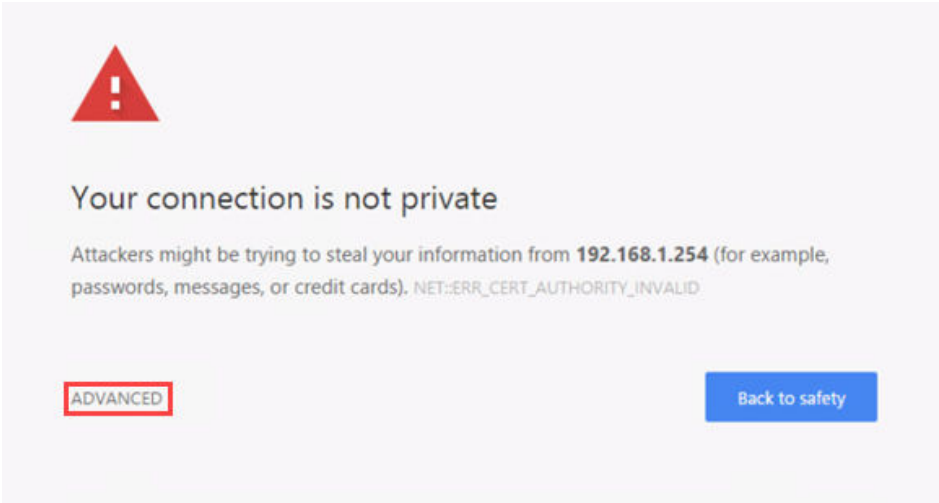
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

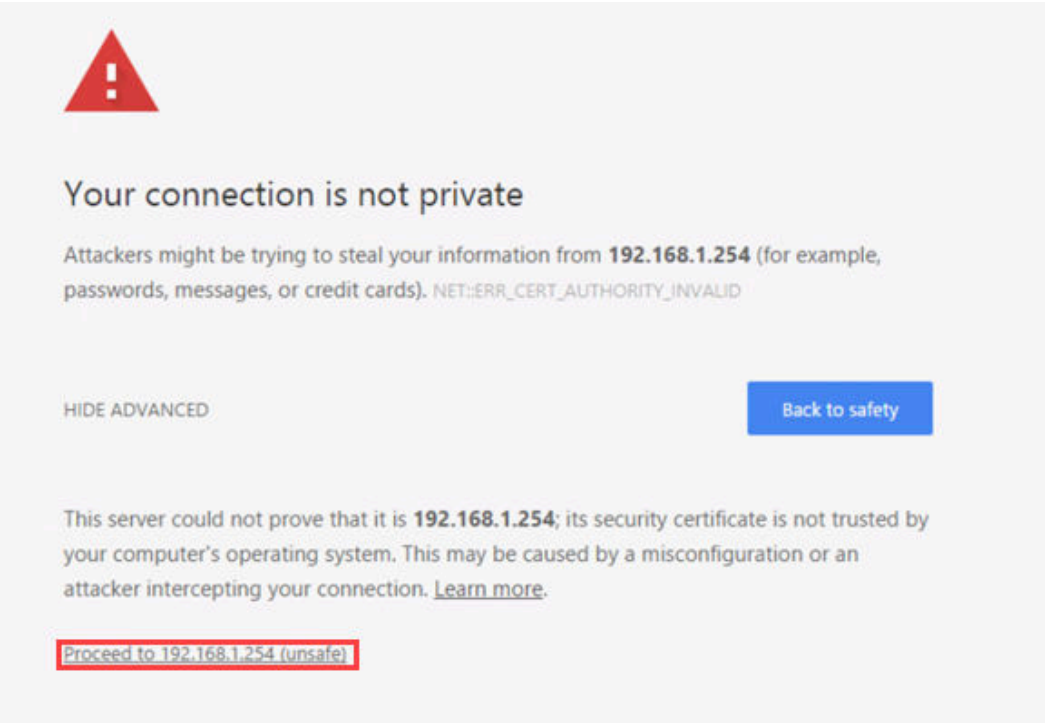


5. You will see a *"Your connection is not private"* message. Click on the **ADVANCED** link.



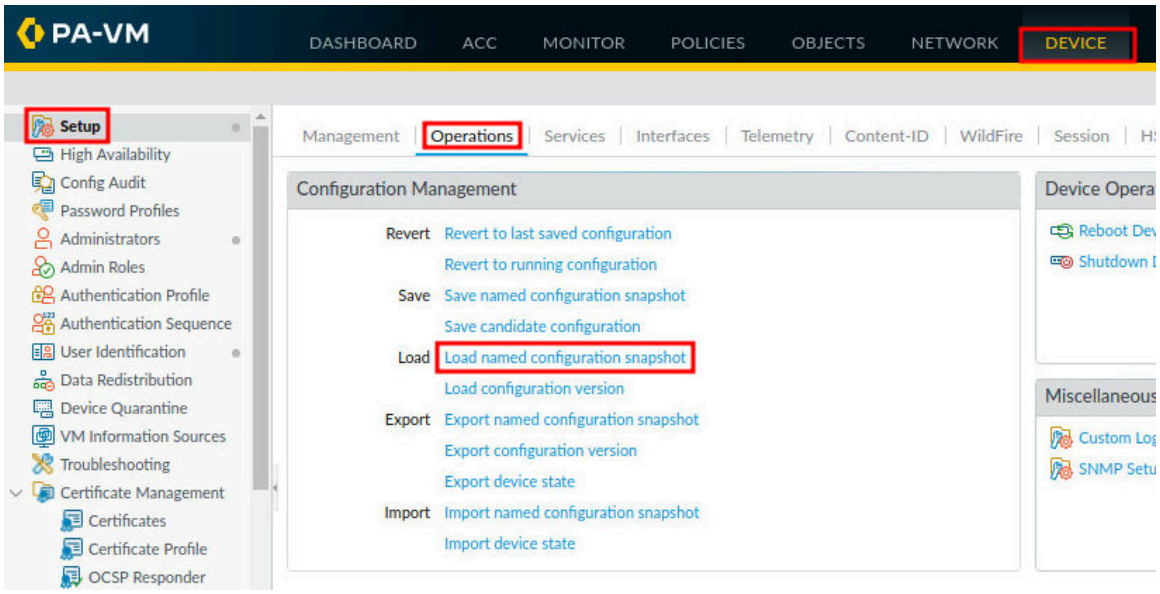
> If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

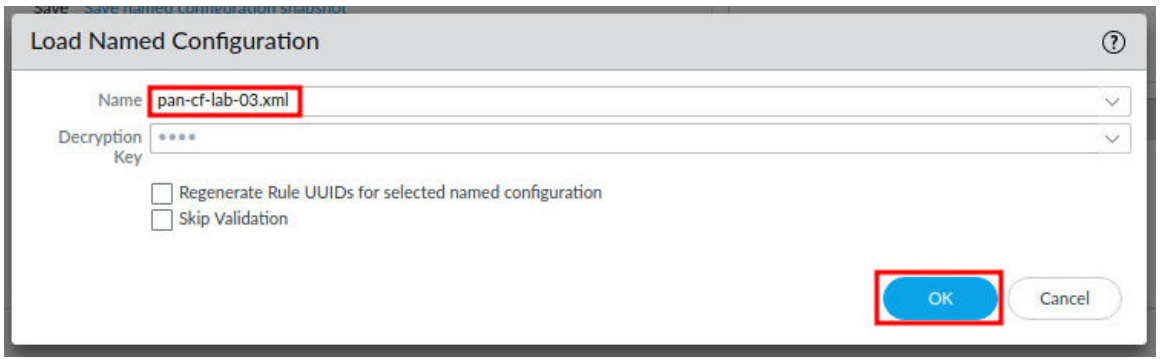


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

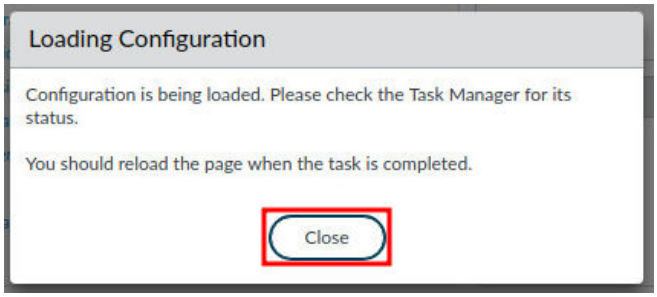
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-cf-lab-03.xml** from the *Name* dropdown box and click **OK**.

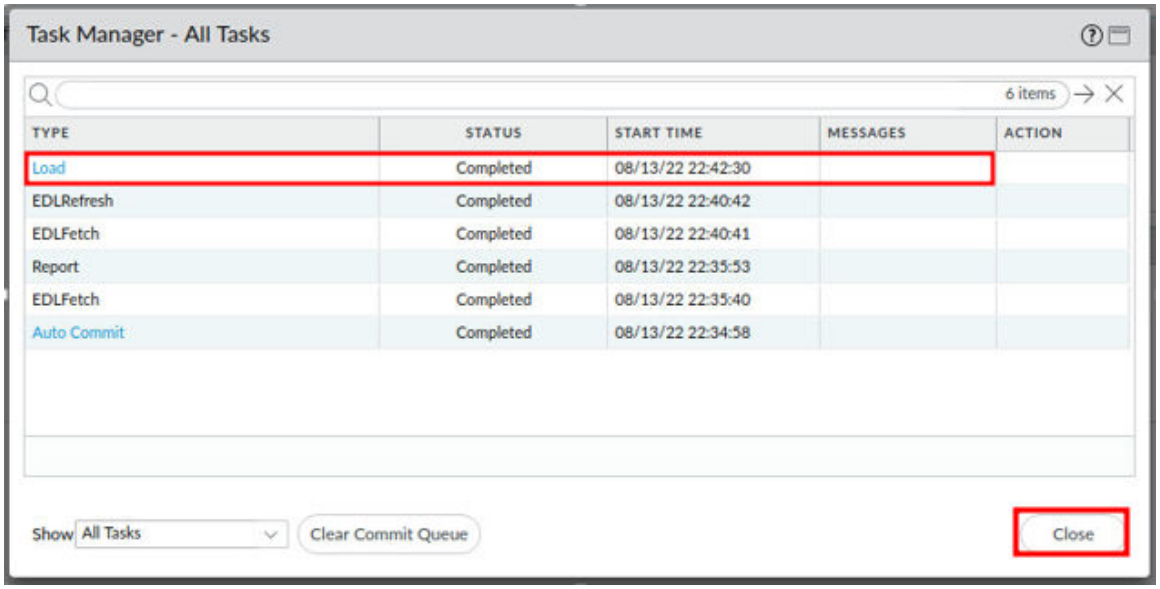


10. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

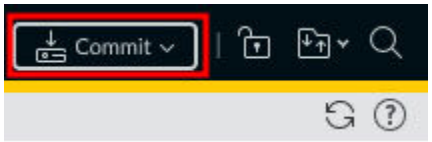


11. Click the **Tasks** icon located at the bottom-right of the web interface.

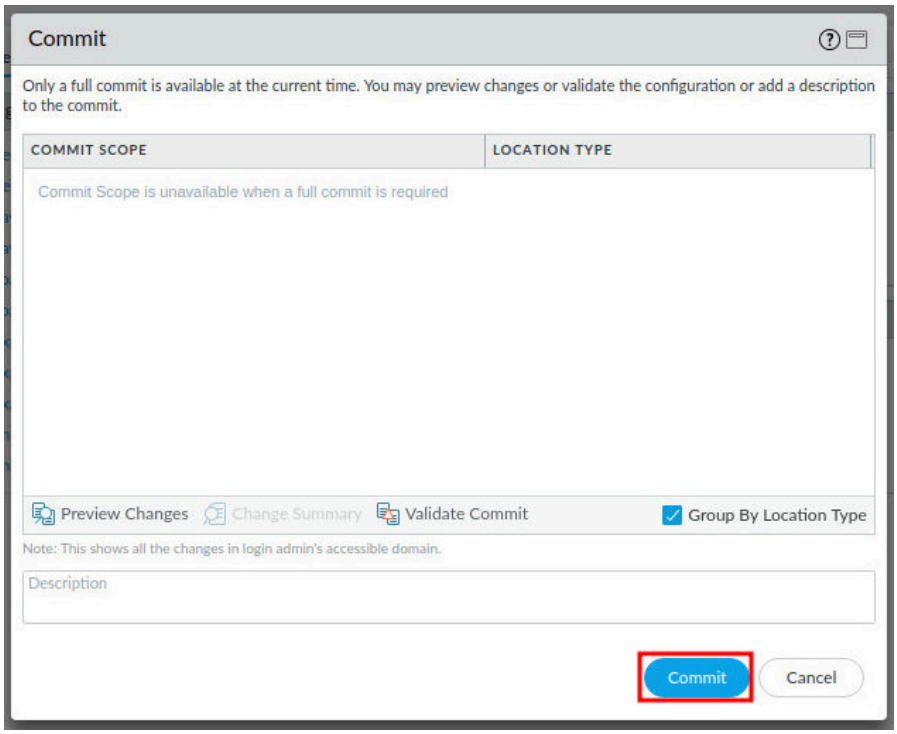
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**



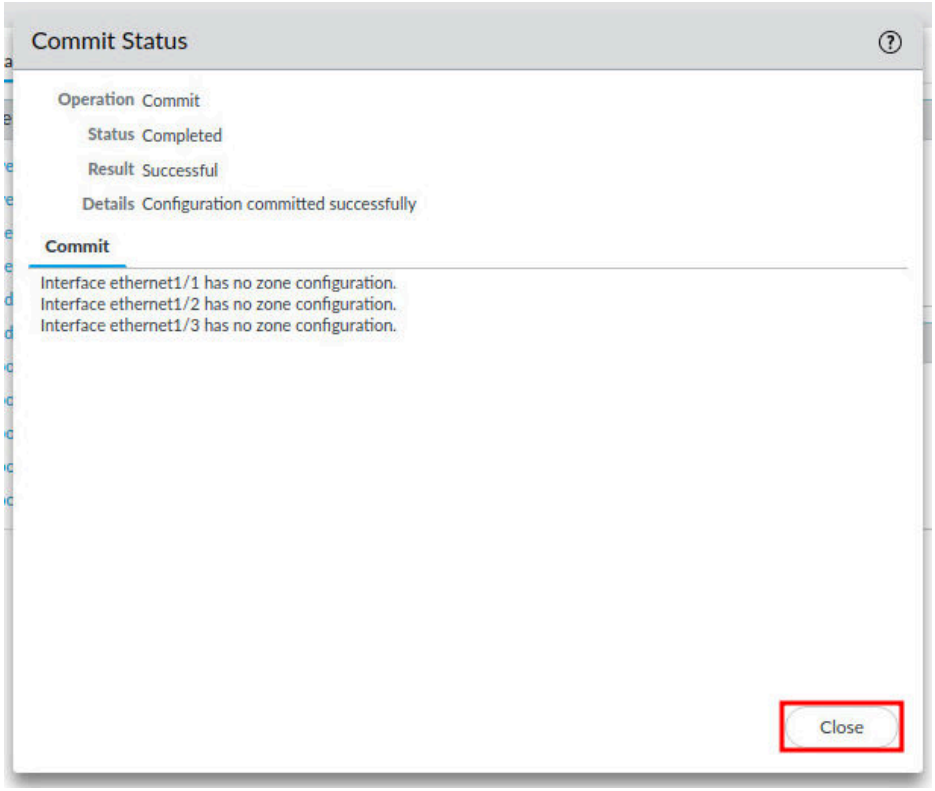
13. Click the **Commit** link located at the top-right of the web interface.



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



15. When the commit operation successfully completes, click **Close** to continue.



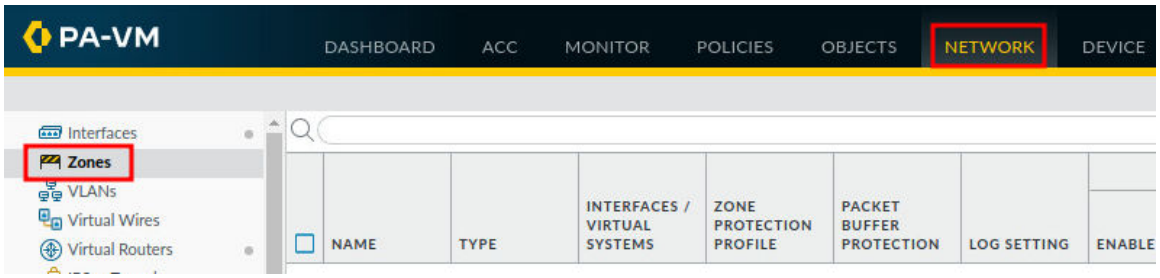
Notice the warnings in the **Commit** section. You will resolve those during this lab.

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.

1.1 Create Zones and Associate the Zones to Interfaces

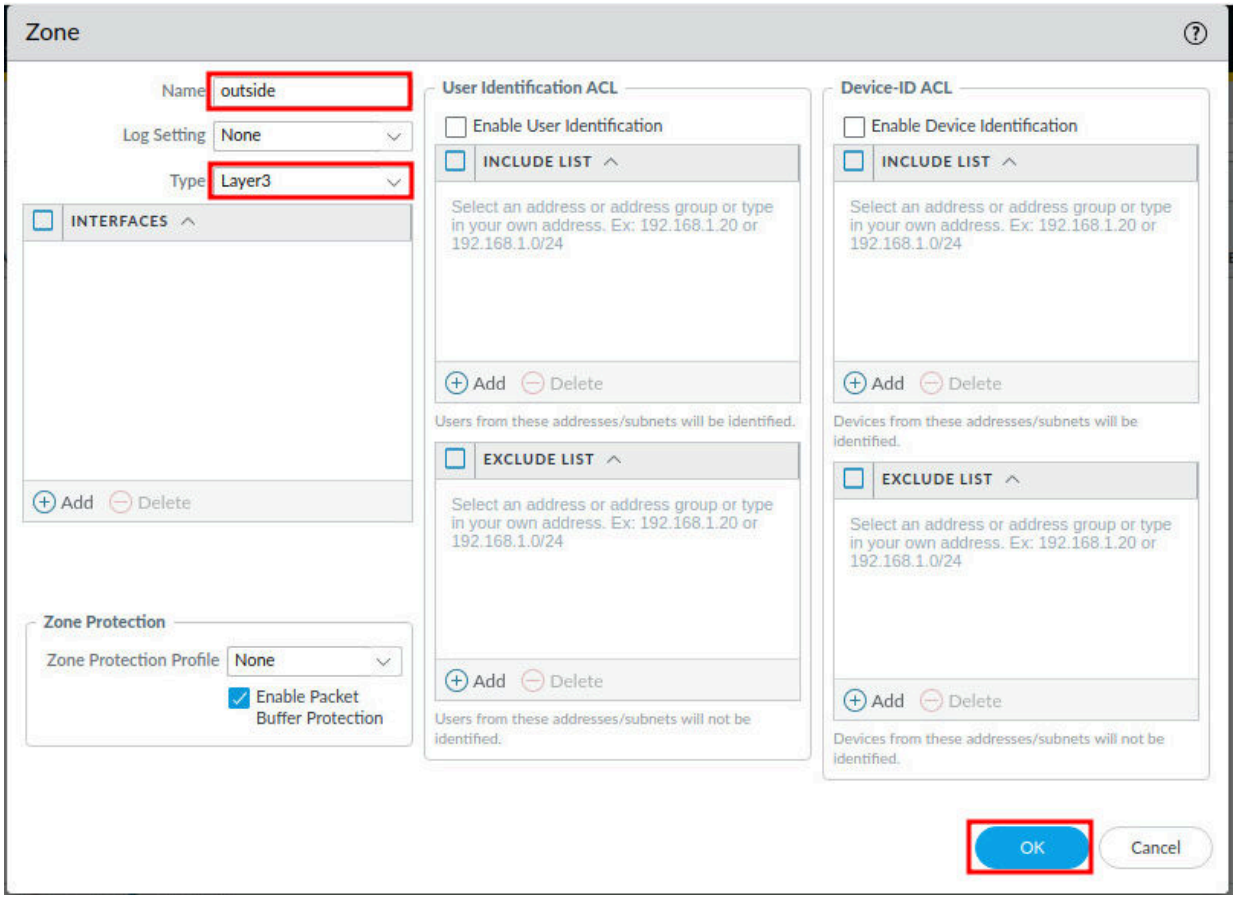
In this section, you will create three basic zones: **inside**, **outside**, and **dmz**. A security zone allows you to segregate traffic in the Firewall so that you can apply security policies later to limit the traffic between zones. Next, you will associate them with the appropriate interfaces.

1. Navigate to **Network > Zones.**



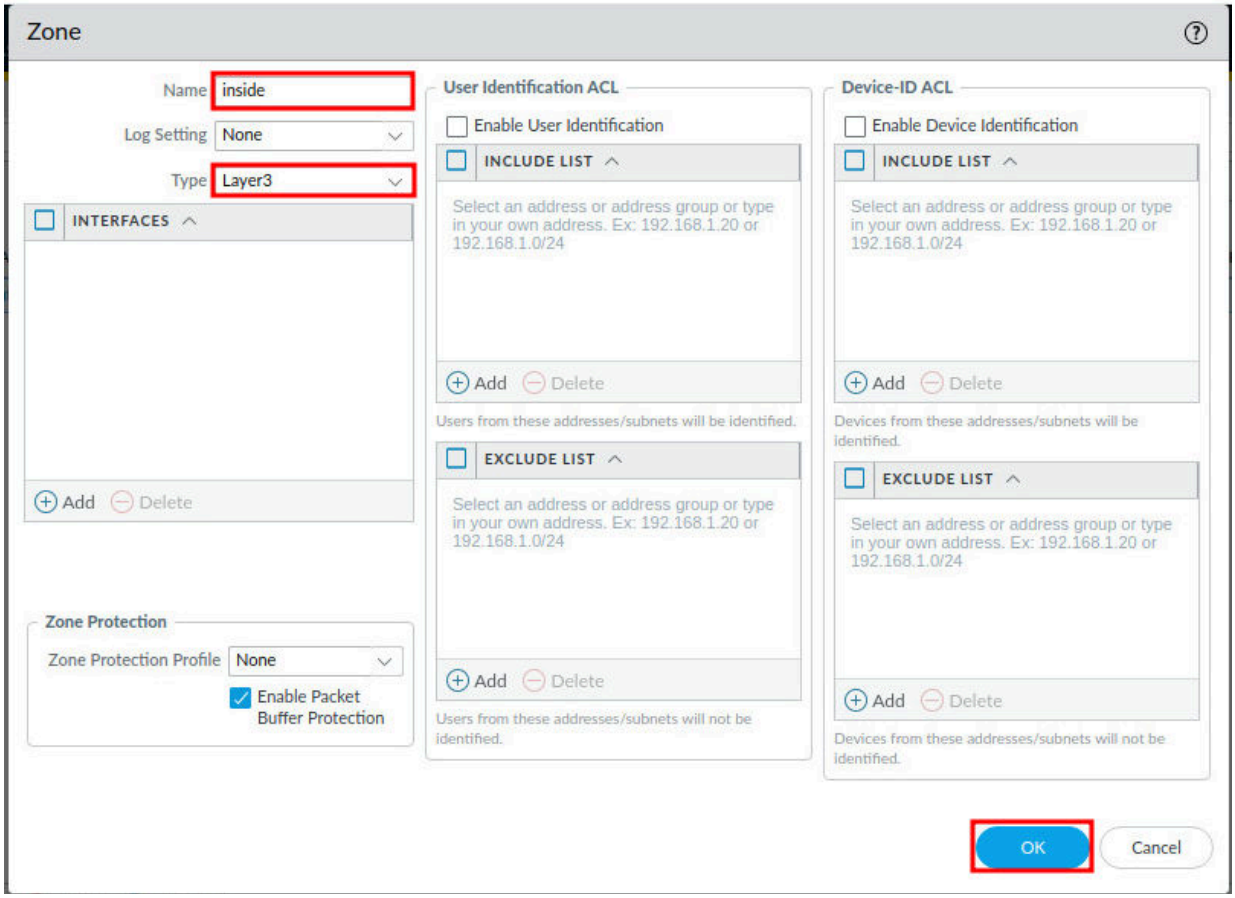
2. Click on the **Add** button at the bottom-left of the center section.

3. In the *Zone* window, type `outside` in the *Name* field. Change *Type* to **Layer3**. Then, click the **OK** button.



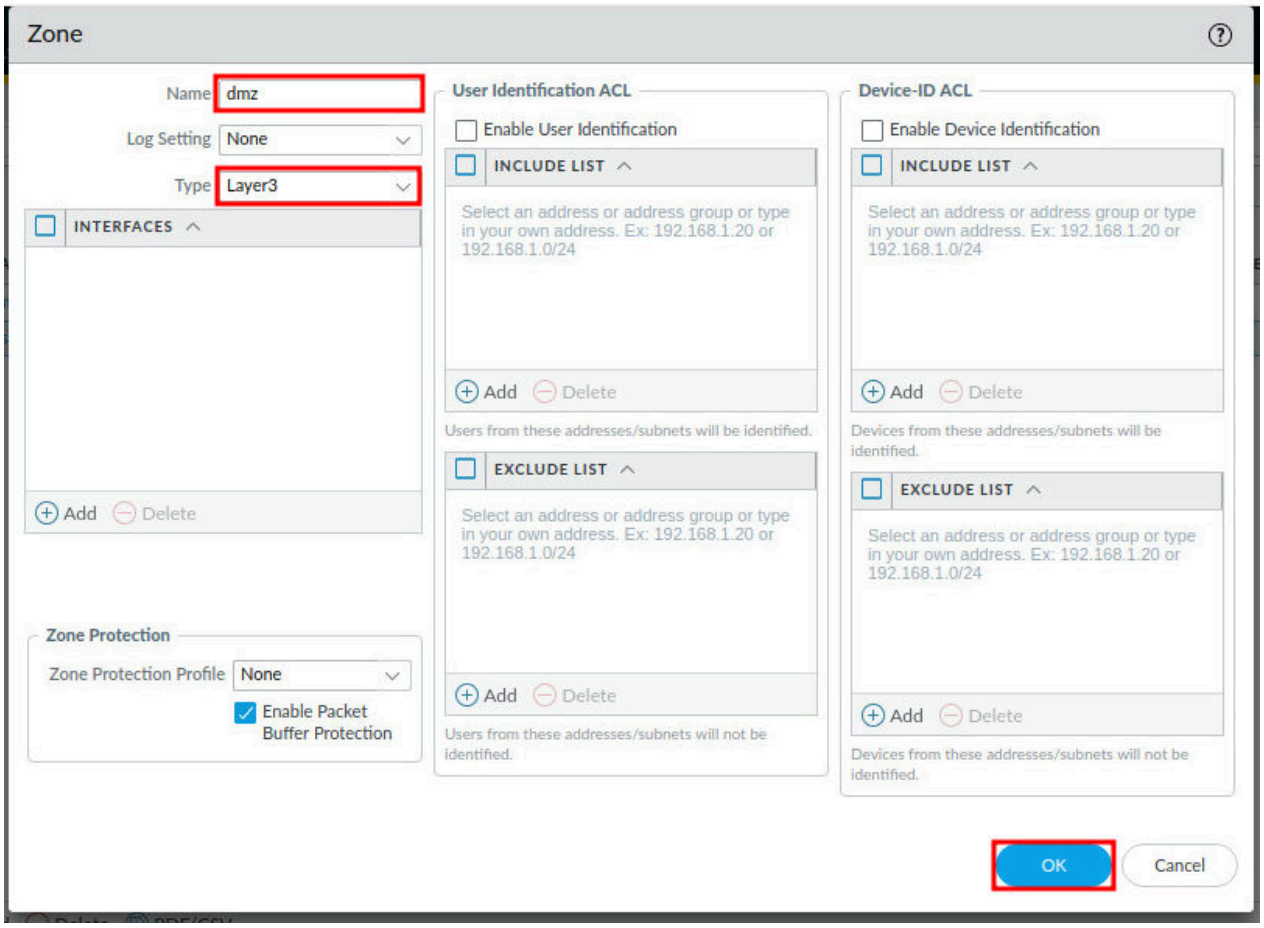
4. Click on the **Add** button at the bottom-left of the center section.

5. In the *Zone* window, type `inside` in the *Name* field. Change *Type* to **Layer3**. Then, click the **OK** button.



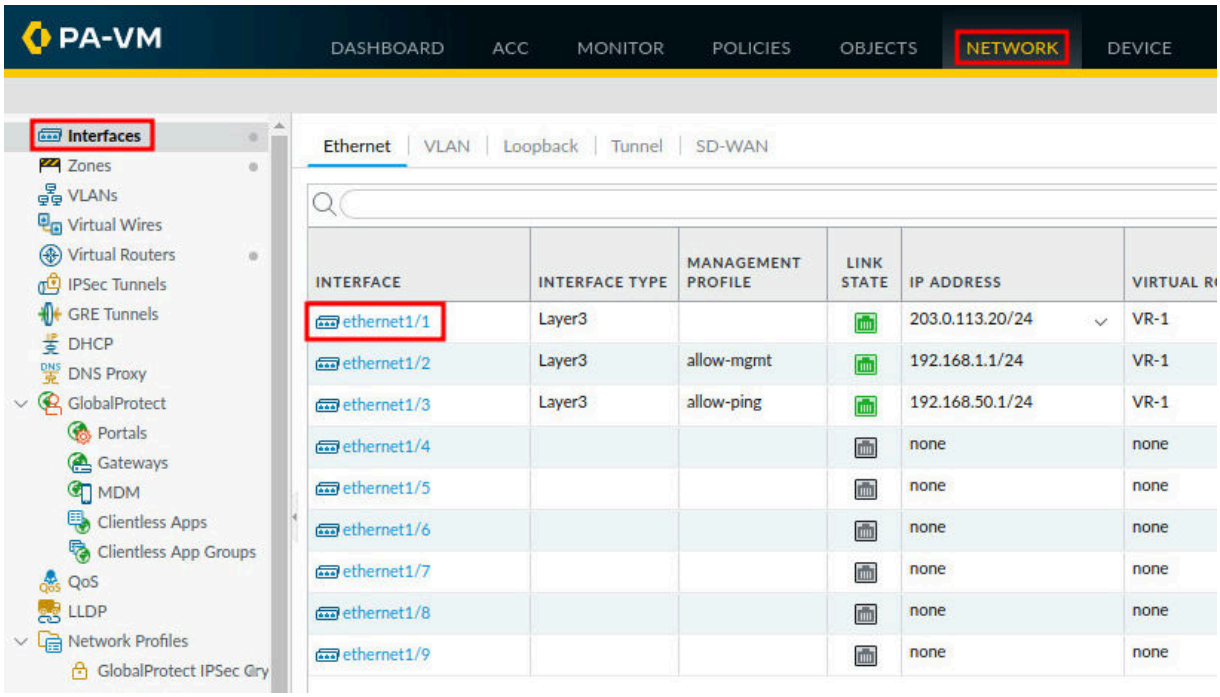
6. Click the **Add** button at the bottom-left of the center section.

7. In the *Zone* window, type `dmz` in the *Name* field. Change *Type* to **Layer3**. Then, click the **OK** button.

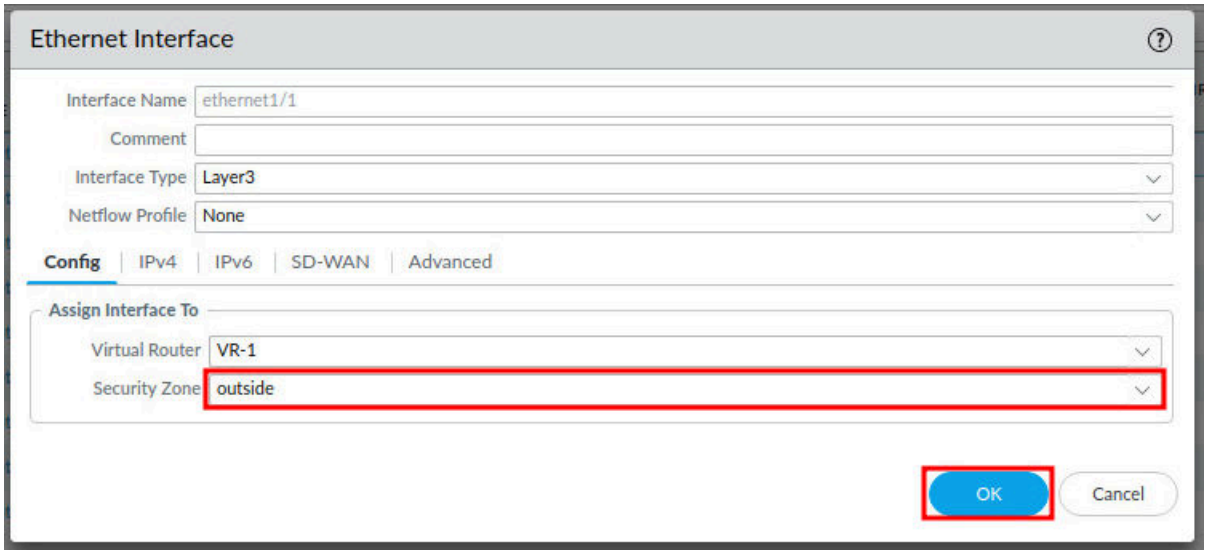


You have now created a zone for each interface. This will keep the traffic between each interface in each zone. Next, you will associate each zone with an interface.

8. Navigate to **Network > Interfaces**, and click on the **ethernet1/1** interface.



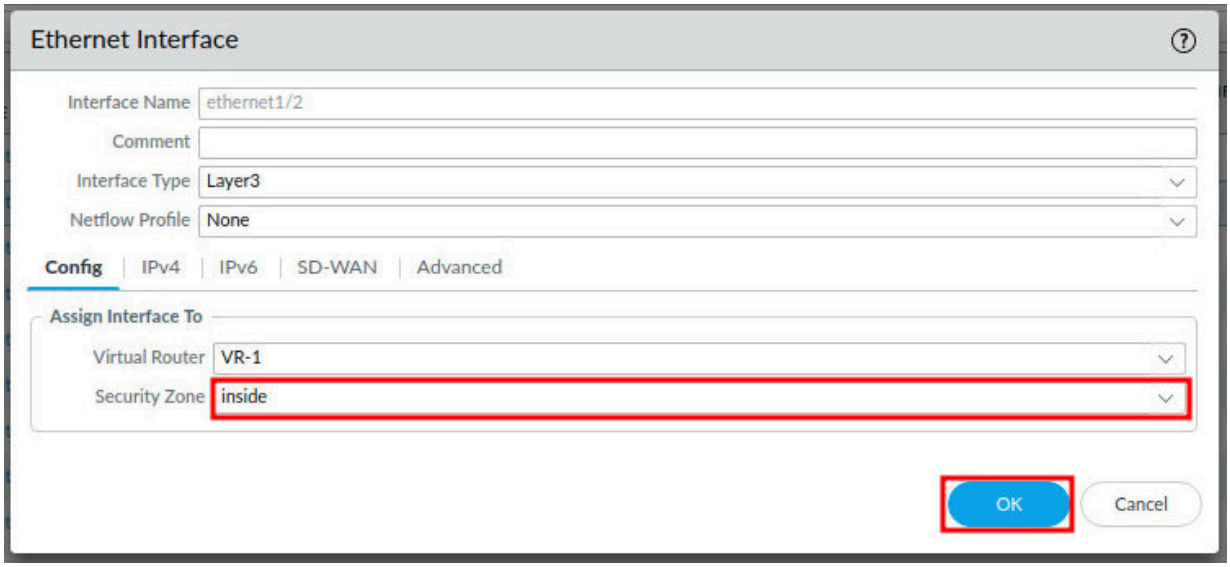
9. In the *Ethernet Interface* window, select **outside** from the *Security Zone* dropdown. Then, click on the **OK** button.



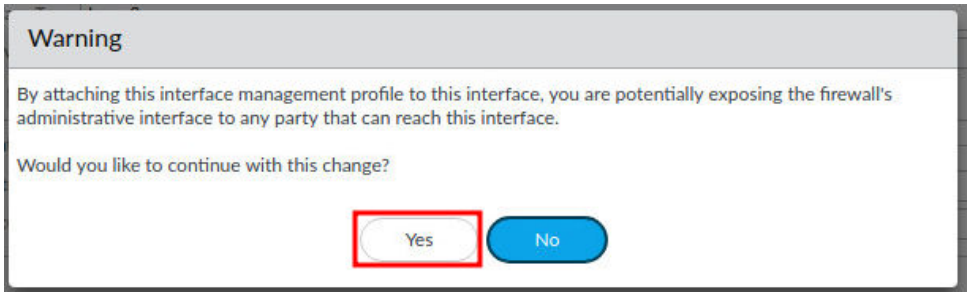
10. Click on the **ethernet1/2** interface.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER
ethernet1/1	Layer3			203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24	VR-1
ethernet1/3	Layer3	allow-ping		192.168.50.1/24	VR-1

11. In the *Ethernet Interface* window, select **inside** from the *Security Zone* dropdown. Then, click on the **OK** button.



12. In the *Warning* window, click **Yes**.

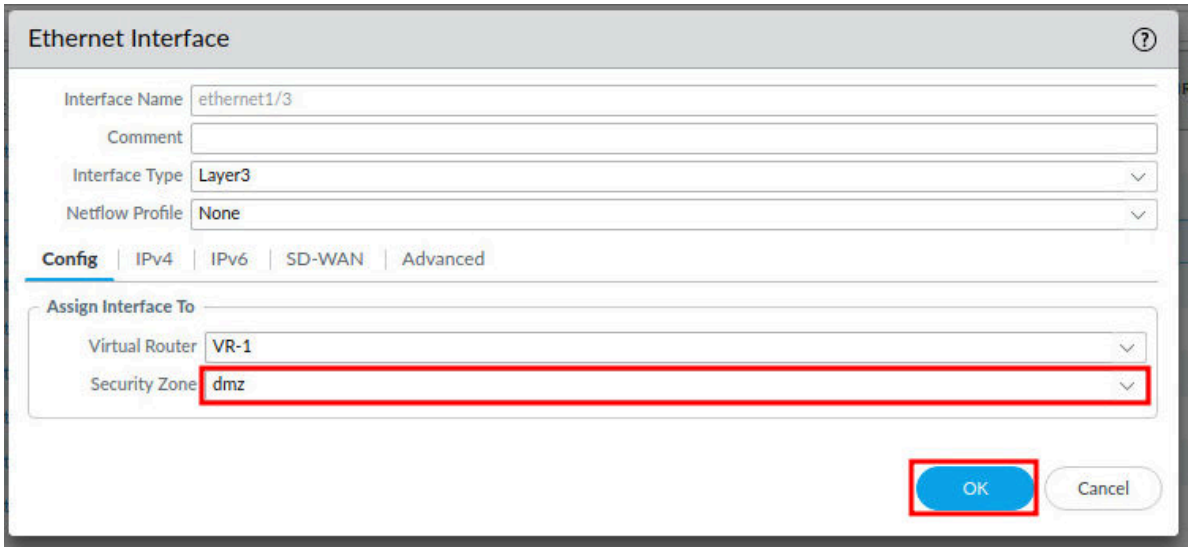


The *Warning* advises that if you attach this interface management profile to this interface, you are potentially exposing the firewall's administrative interface to any party that can reach this interface. For the purpose of this lab, you will bypass this warning knowing that it is not good practice to attach a management profile to a production interface.

13. Click on the **ethernet1/3** interface.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER
ethernet1/1	Layer3			203.0.113.20/24	VR-1
ethernet1/2	Layer3	allow-mgmt		192.168.1.1/24	VR-1
ethernet1/3	Layer3	allow-ping		192.168.50.1/24	VR-1

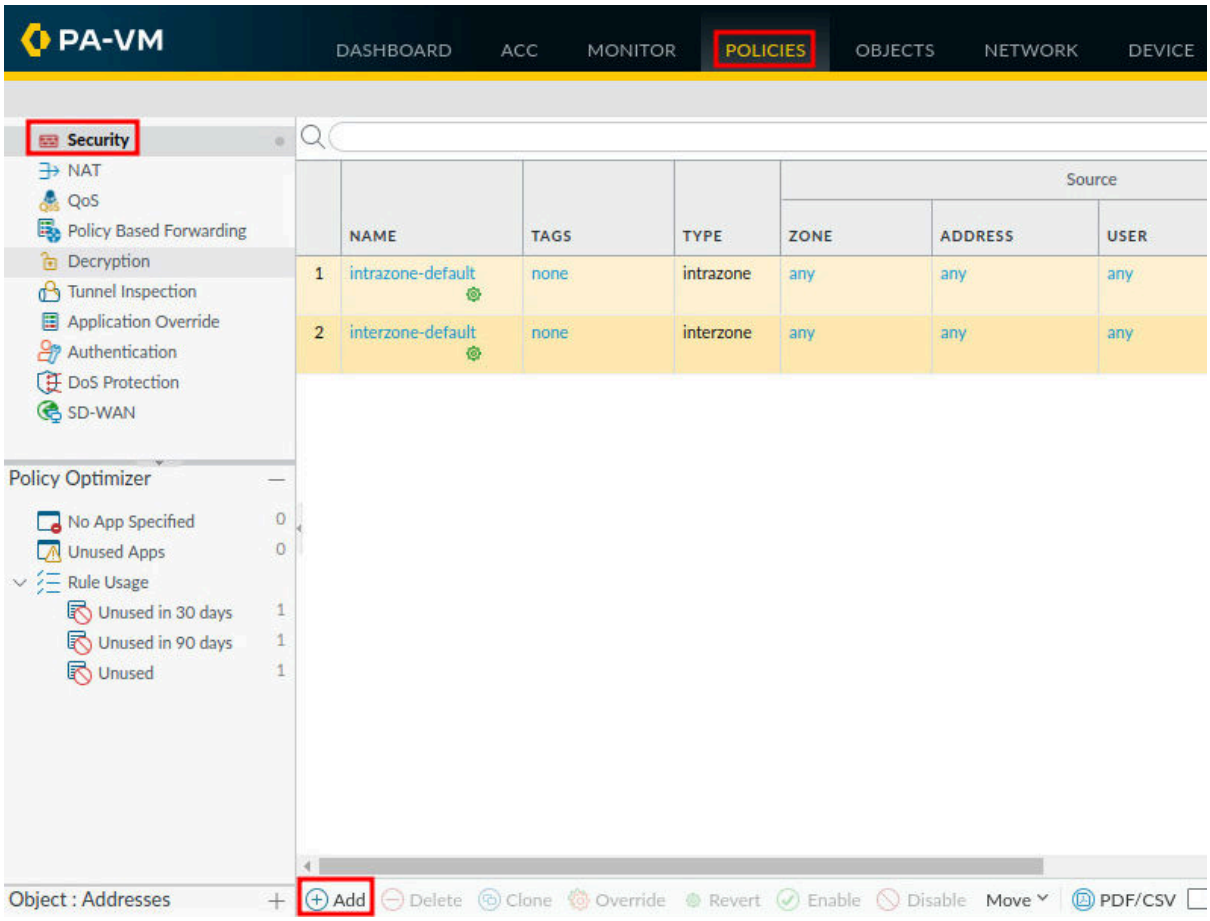
14. In the *Ethernet Interface* window, select the **dmz** in the *Security Zone* dropdown. Then, click on the **OK** button.



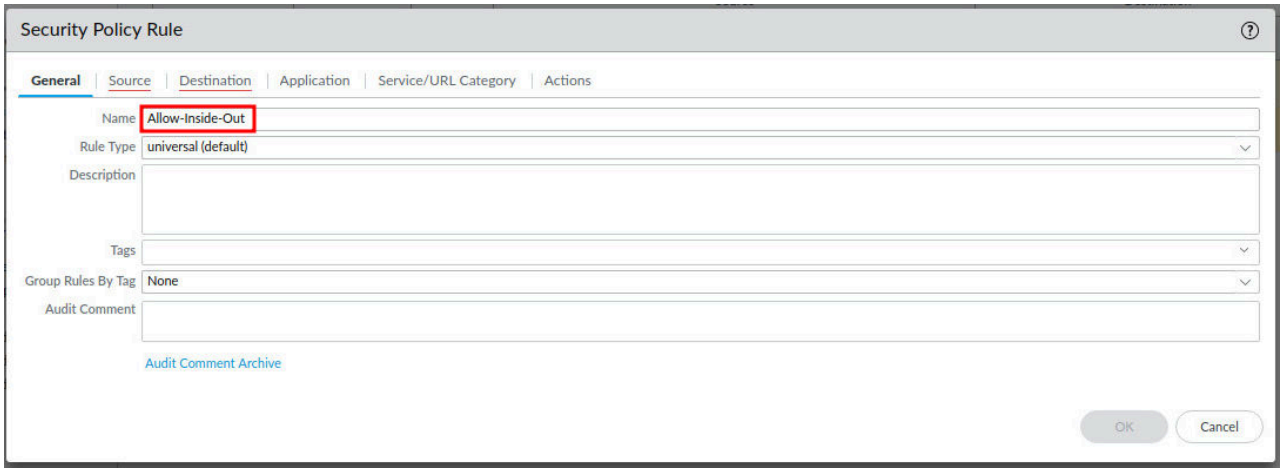
1.2 Create a Security Policy Rule

In this section, you will create a security policy rule that allows traffic from the inside zone to the outside zone.

1. Navigate to **Policies > Security > Add.**

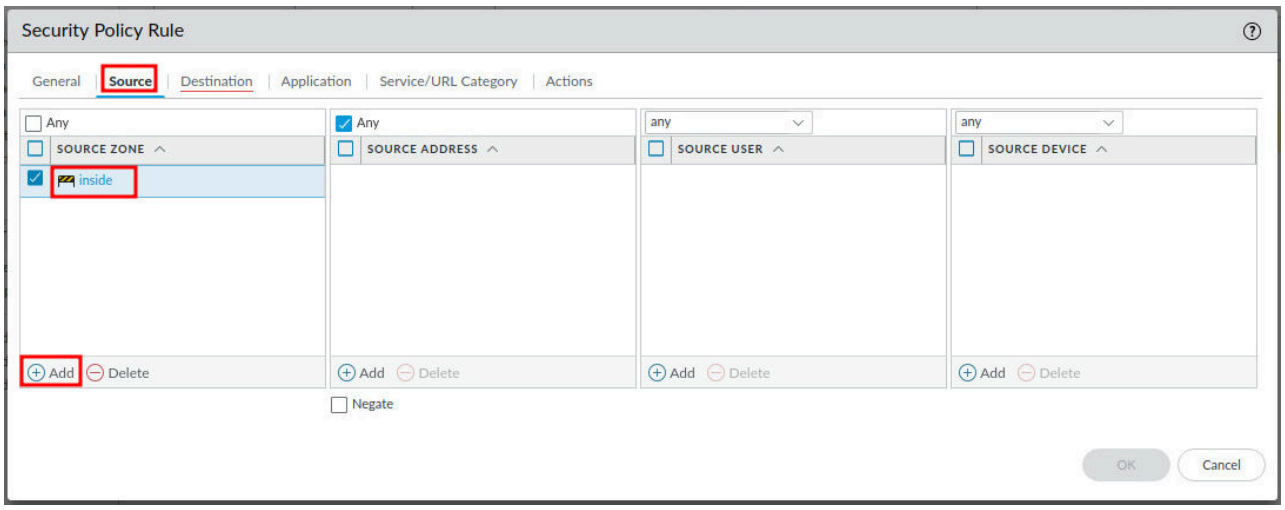


2. In the *Security Policy Rule* window, type `Allow-Inside-Out` in the *Name* field.



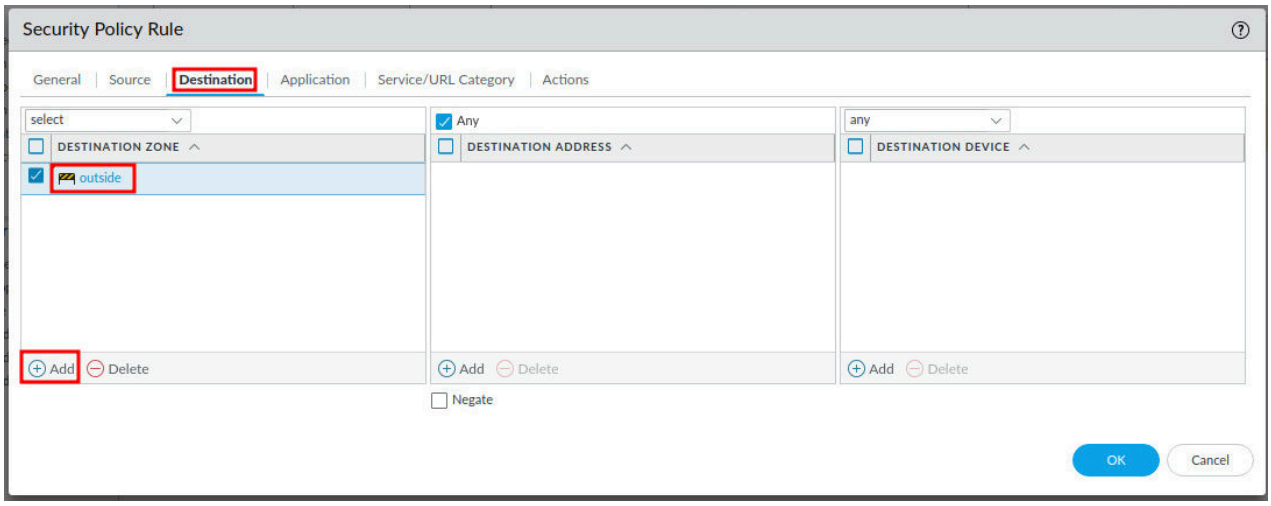
In a Security Policy Rule, there are three required sections. Note the initial red squiggle lines under General, Source, and Destination. These will go away as you fill out the required information.

3. In the *Security Policy Rule* window, click on the **Source** tab. Then, click the **Add** button in the *Source Zone* section. Next, select **inside** from the dropdown in the *Source Zone* column.



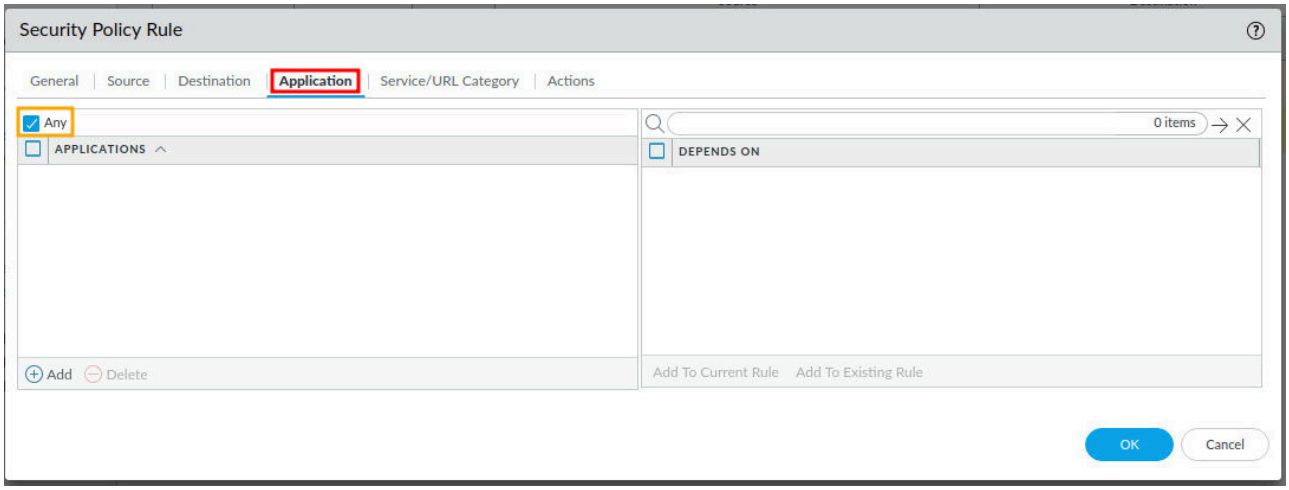
The **Source** tab allows you to select where traffic is coming from. In this rule, you select traffic coming from the *inside* zone. Note that you leave the default setting of *any* source address. This allows any address in the *inside* zone to pass through.

4. In the *Security Policy Rule* window, click on the **Destination** tab. Then, click the **Add** button in the *Destination Zone* section. Next, select **outside** from the dropdown in the *Destination Zone* column.



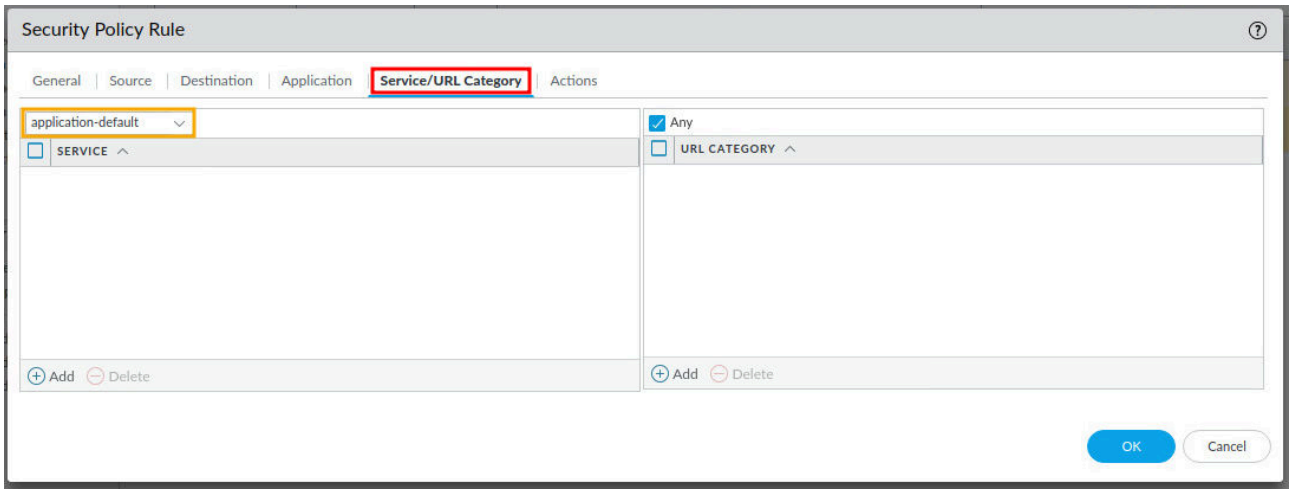
The **Destination** tab allows you to select where traffic is going to. In this rule, you select traffic destined to the *outside* zone. Note that you leave the default setting of *any* destination address. This allows the source traffic to communicate with any address in the destination zone.

5. In the *Security Policy Rule* window, click on the **Application** tab. Then, make sure that the **Any** checkbox is checked.



The **Application** tab allows you to select predefined applications to allow through the Firewall. The Palo Alto Networks Firewall can be very precise on the traffic it allows. The **Any** checkbox allows any application through. In a real-world deployment, you may use a similar rule for testing traffic without any restrictions.

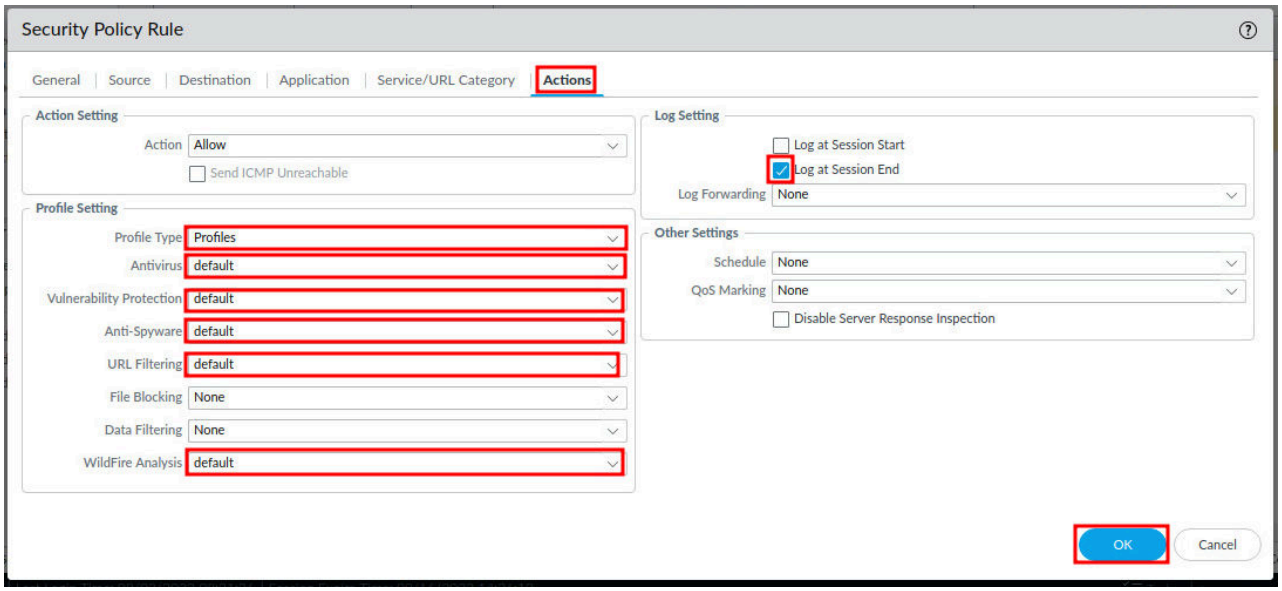
6. In the *Security Policy Rule* window, click on the **Service/URL Category** tab. Then, make sure **application-default** is selected in the dropdown above the *Service* section.



The **Service/URL Category** tab allows you to select predefined services or preset groups to allow through the Firewall. The **application-default** selection means that the selected applications are allowed or denied only on their default ports defined by Palo Alto Networks. This option is recommended for allowing policies because it prevents applications from running on unusual ports and protocols, which if not intentional, can be a sign of undesired application behavior and usage. When you use this option, the device still checks for all applications on all ports, but with this configuration, applications are only allowed on their default ports/protocols.

For example, if a web server is running on the standard port 80, traffic will be allowed to pass. However, if the web server is running on a non-standard port such as 5000, traffic will be blocked.

7. In the *Security Policy Rule* window, click on the **Actions** tab. Then, make sure **Log at Session End** is checked under the *Log Setting* section. Next, select **Profiles** from the dropdown under the *Profile Setting* section. Then, select **default** for the *Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering,* and *WildFire Analysis* fields. Finally, click the **OK** button.



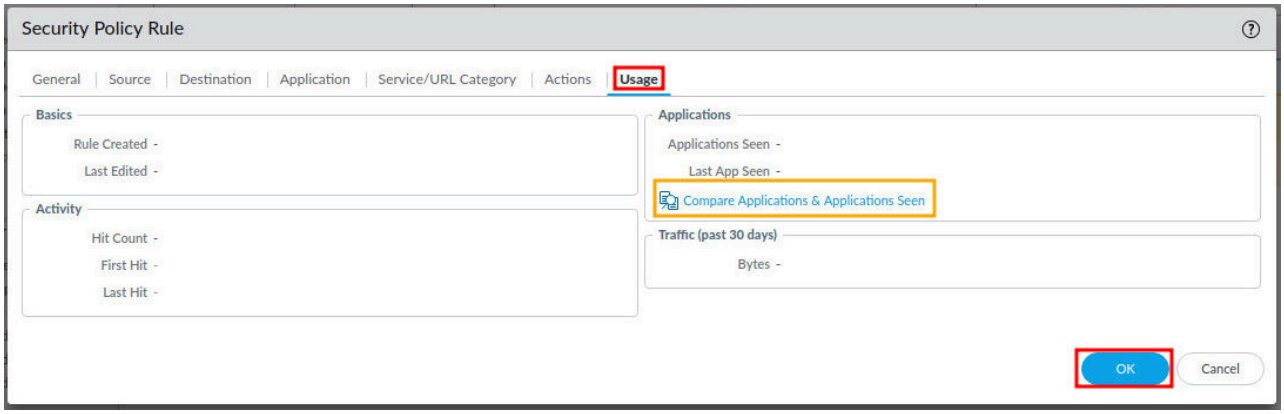
The **Actions** tab allows you to decide what to do with the traffic you have defined. In this rule, you use the default *Allow* action setting to permit traffic. Selecting *Log at Session End* is considered best practice as applications are likely to change throughout the lifespan of the session. Facebook, for example, will start as *web-browsing* and change to *Facebook-base* after the firewall recognized the application.

The various profile settings allow for predefined signatures and threats to be assessed by the Firewall. At a minimum it is best practice to select the *default* profiles. There are additional best practices for each individual profile defined in the technical documentation available at Palo Alto Networks.

8. Click on the **Allow-Inside-Out** to reopen the *Security Policy Rule*.

	NAME	TAGS	TYPE	Source			
				ZONE	ADDRESS	USER	DEVICE
1	Allow-Inside-Out	none	universal	inside	any	any	any
2	intrazone-default	none	intrazone	any	any	any	any
3	interzone-default	none	interzone	any	any	any	any

9. In the *Security Policy Rule* window, an additional tab named *Usage* will be displayed. Click on the **Usage** tab. You can now **Compare Applications & Applications Seen**. Because there is nothing to see right now, click **OK** to exit the *Security Policy Rule* window.



The **Usage** tab allows you to evaluate the rule's usage, number of applications seen on the rule, when the last application was seen on the rule, hit count, traffic over the past 30 days, and when the rule was created and last edited.

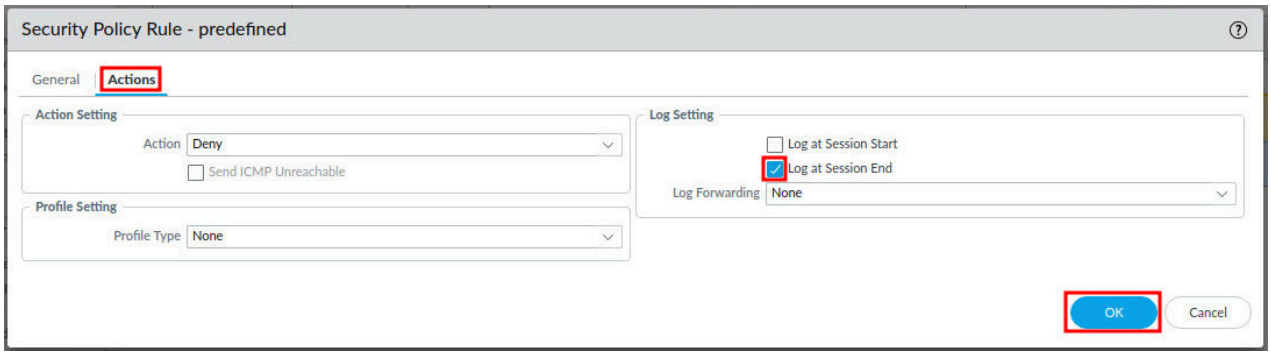
The **Compare Applications & Applications seen** allows you to access the tools to help you mitigate from port-based security policy rules to application-based security policy rules. This also allows you to exclude unused applications from in *Applications & Usage*.

10. Click on the number **3,** to select but not open the **interzone-default** security policy.

	NAME	TAGS	TYPE	Source			
				ZONE	ADDRESS	USER	DEVICE
1	Allow-Inside-Out	none	universal	inside	any	any	any
2	intrazone-default	none	intrazone	any	any	any	any
3	interzone-default	none	interzone	any	any	any	any

11. With the *interzone-default policy* selected, click on the **Override** button at the bottom of the center section.

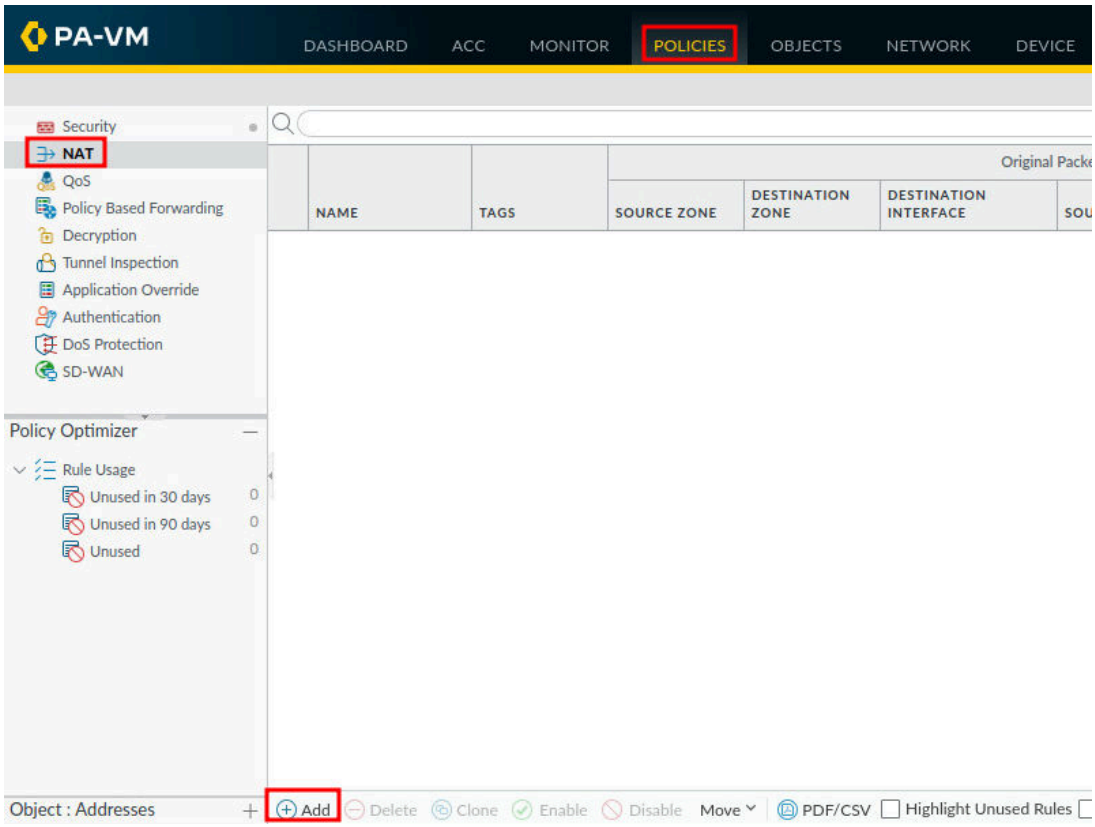
12. In the *Security Policy Rule – predefined* window, click on the **Actions** tab. Then, select the **Log at Session End** checkbox under the *Log Settings* section. Finally, click the **OK** button.



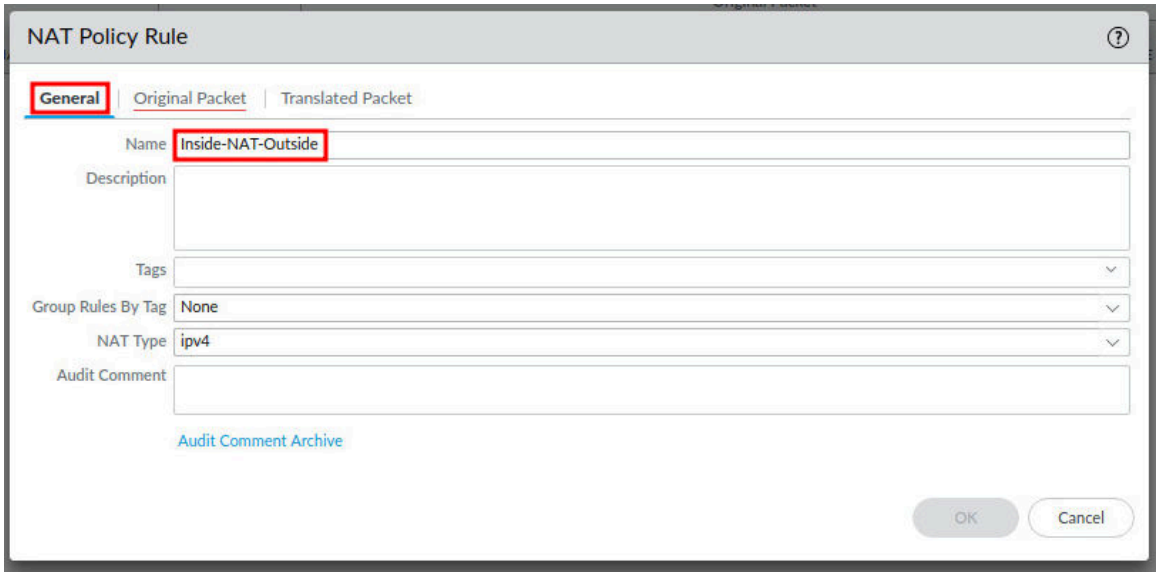
1.3 Create a NAT Policy

In this section, you will create a basic NAT policy to NAT traffic from the inside zone to the outside zone.

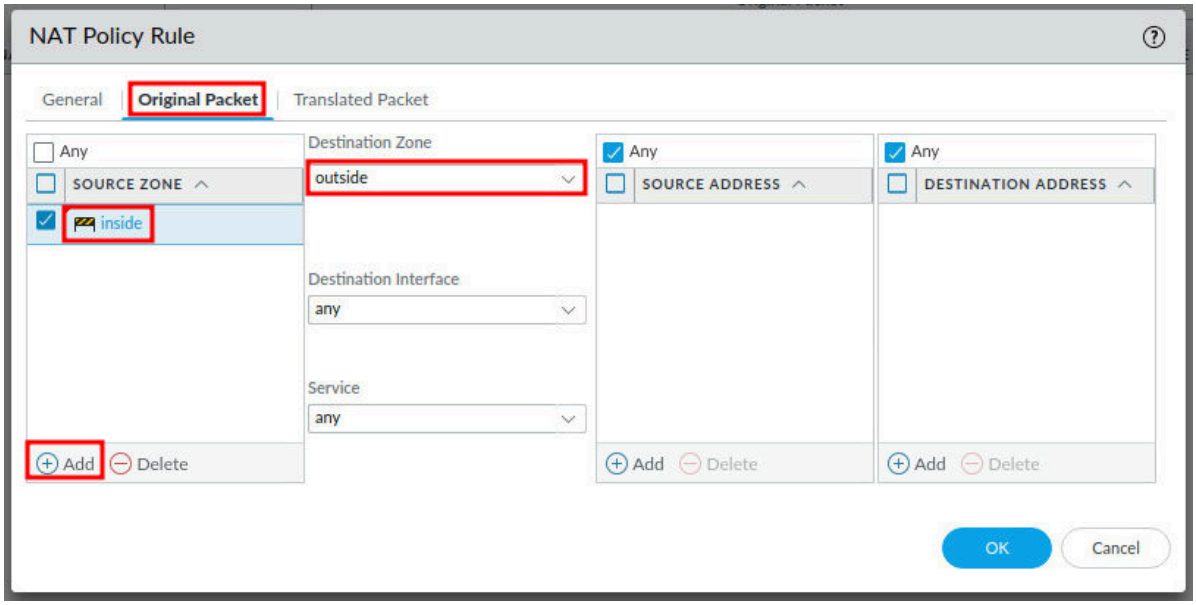
1. Navigate to **Policies > NAT > Add**.



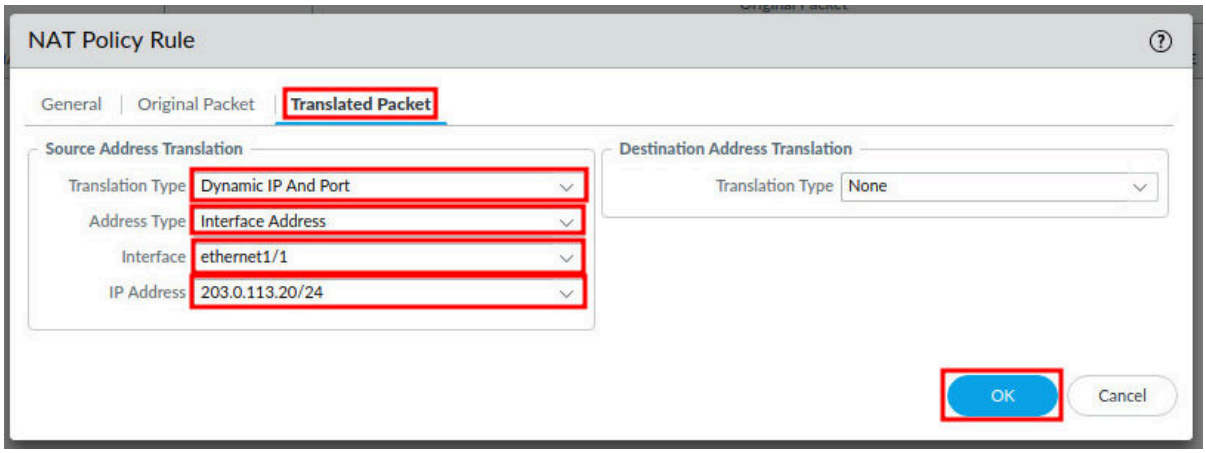
2. In the *NAT Policy Rule* window, type `Inside-NAT-Outside` in the *Name* field.



3. In the *NAT Policy Rule* window, click on the **Original Packet** tab. Then, click the **Add** button at the bottom of the *Source Zone* section. Next, select **inside** in the dropdown of the *Source Zone* column. Finally, select **outside** in the *Destination Zone* dropdown.



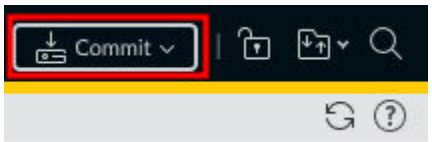
4. In the *NAT Policy Rule* window, click on the **Translated Packet** tab. Then, select **Dynamic IP And Port** on the *Translation Type* dropdown. Next, select **Interface Address** on the *Address Type* dropdown. Then, select **ethernet1/1** for the *Interface* dropdown. Finally, select **203.0.113.20/24** on the *IP Address* dropdown and click the **OK** button.



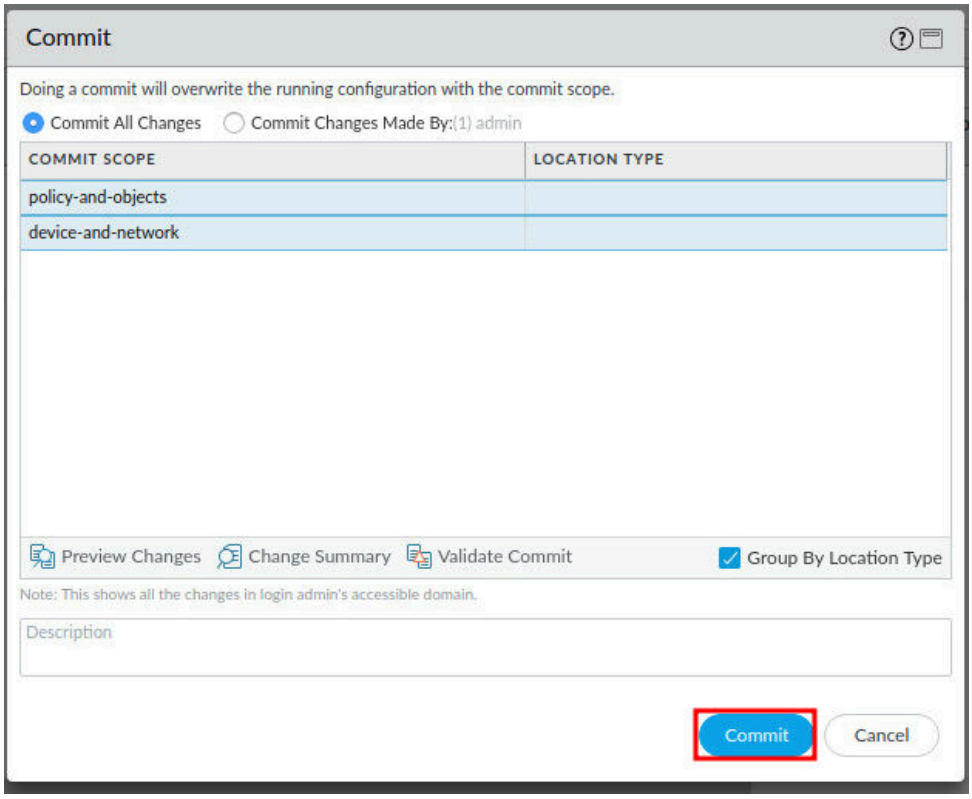
1.4 Commit and Test the Rules and Policies

In this section, you will create a basic NAT policy to NAT traffic from the inside zone to the outside zone.

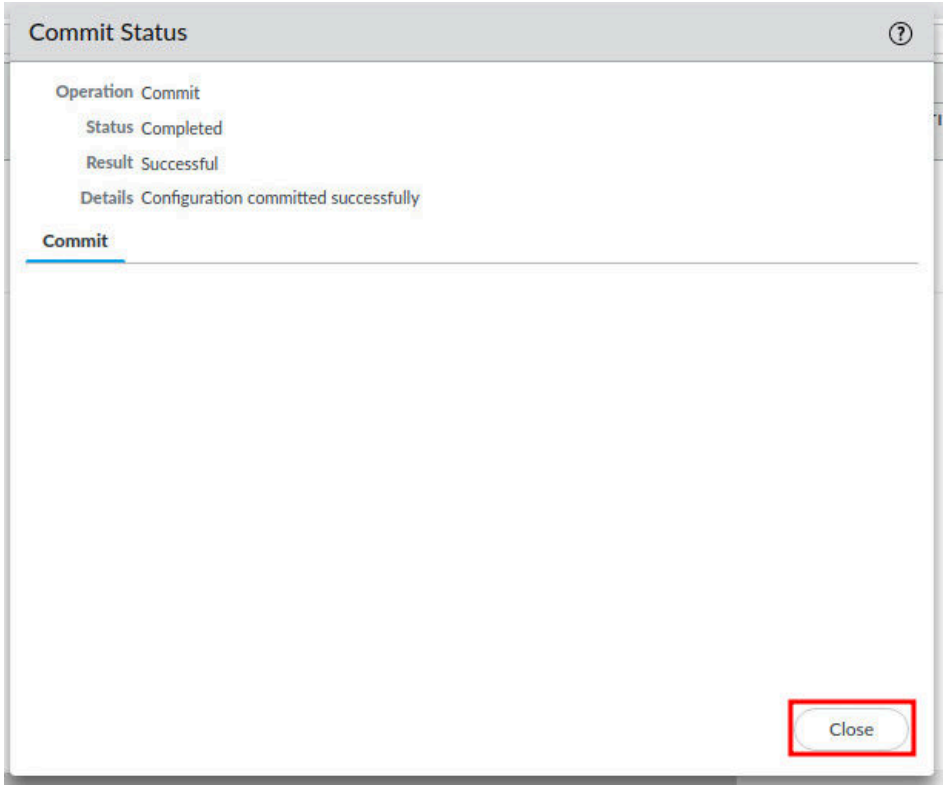
1. Click the **Commit** link located at the top-right of the web interface.



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

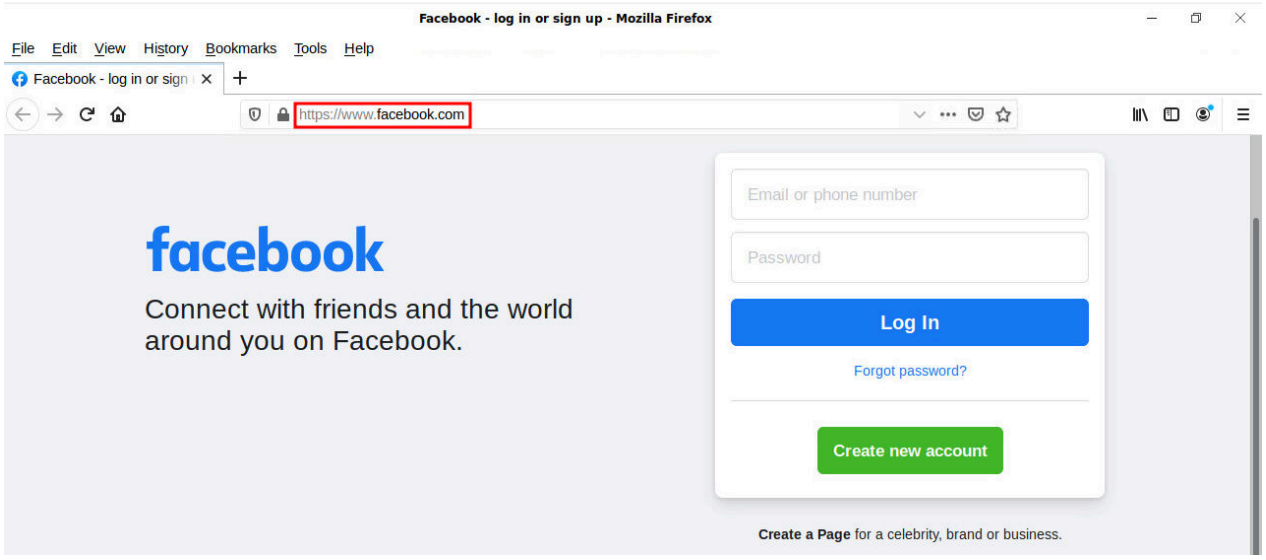


3. When the commit operation successfully completes, verify there are no warnings under the **Commit** section, then click **Close** to continue.

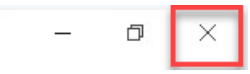


4. Open **Firefox** from the taskbar.

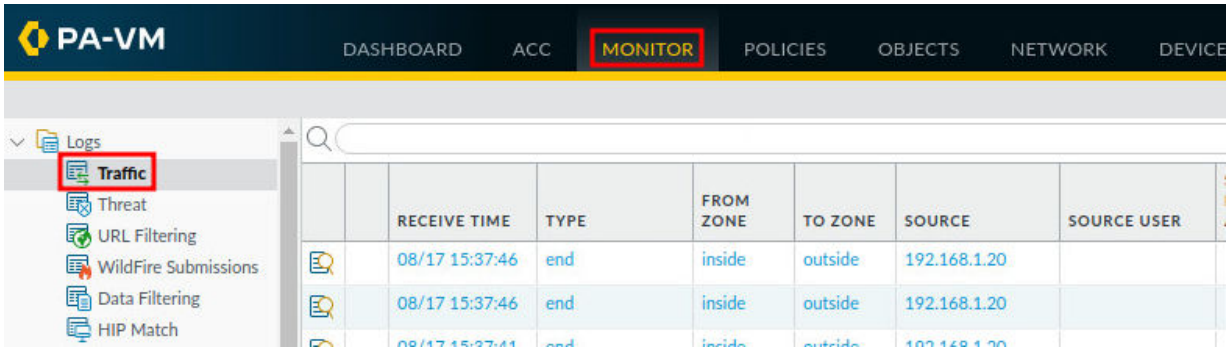
5. In the address bar, type `https://www.facebook.com` and press **Enter**.



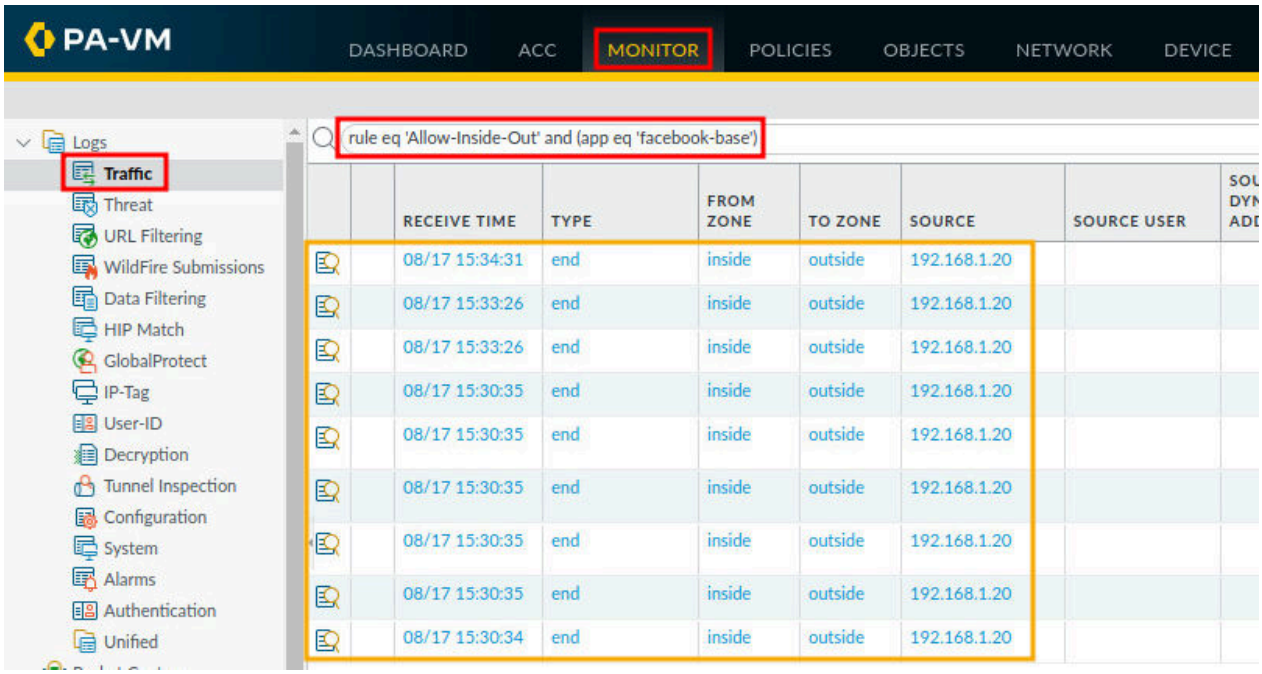
6. Click the **X** in the upper-right to close **Firefox**.



7. Navigate to **Monitor > Logs > Traffic.**



8. In the filter text box, type `rule eq 'Allow-Inside-Out' and (app eq 'facebook-base')` and press **Enter**. You will see log entries allowing the **facebook-base** application.



9. The lab is now complete; you may end the reservation.

