SECURITY OPERATIONS FUNDAMENTALS

Lab 5: Stopping Reconnaissance Attacks

Document Version: 2021-01-29

Contents

Introduction

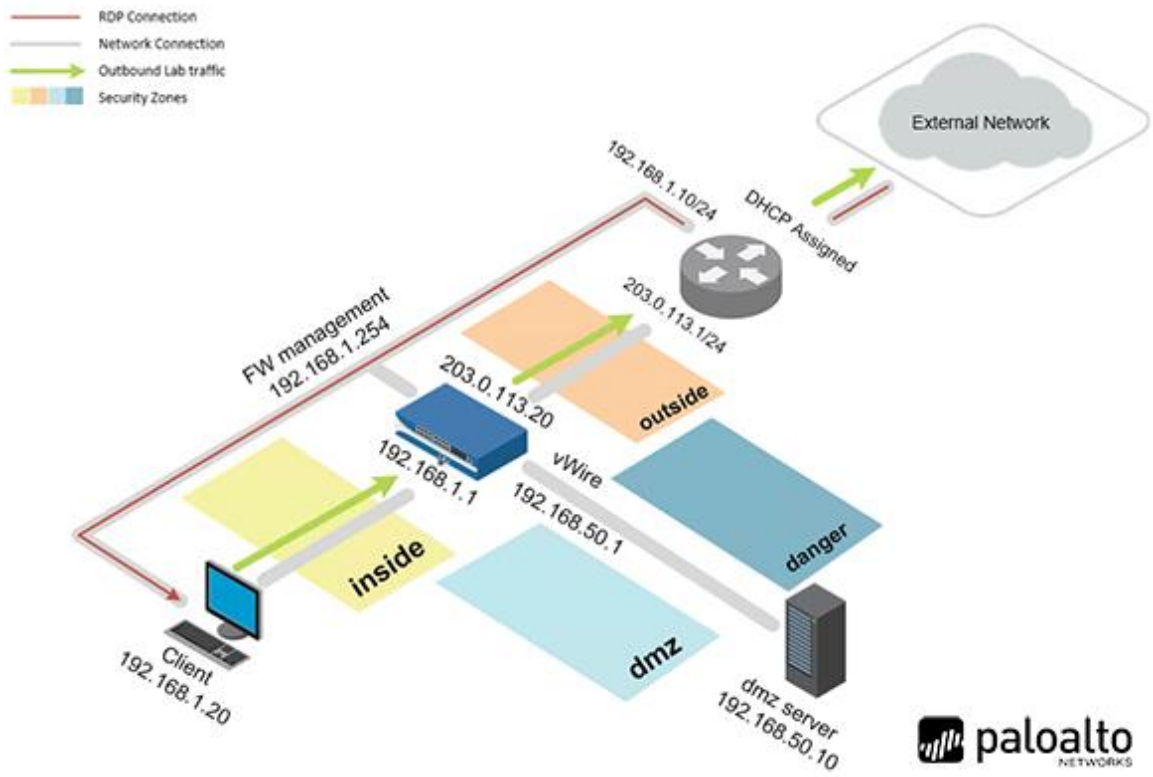
In this lab, you will utilize Zone Protection profiles to provide additional protection for specific network zones to protect the zones from attack. You will use *Nmap* on the client machine to perform a reconnaissance attack. This will test the Zone Protection Profiles of the Palo Alto Networks Firewalls.

Objective

In this lab, you will perform the following tasks:

- Create a Zone Protection Profile
- Apply the Zone Protection Profile to Zones and Commit
- Perform a Reconnaissance Attack on the DMZ Server
- Monitor and Analyze the Threat Logs

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.

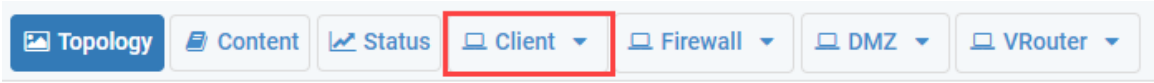
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

5 Stopping Reconnaissance Attacks

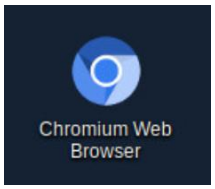
5.0 Load Lab Configuration

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

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

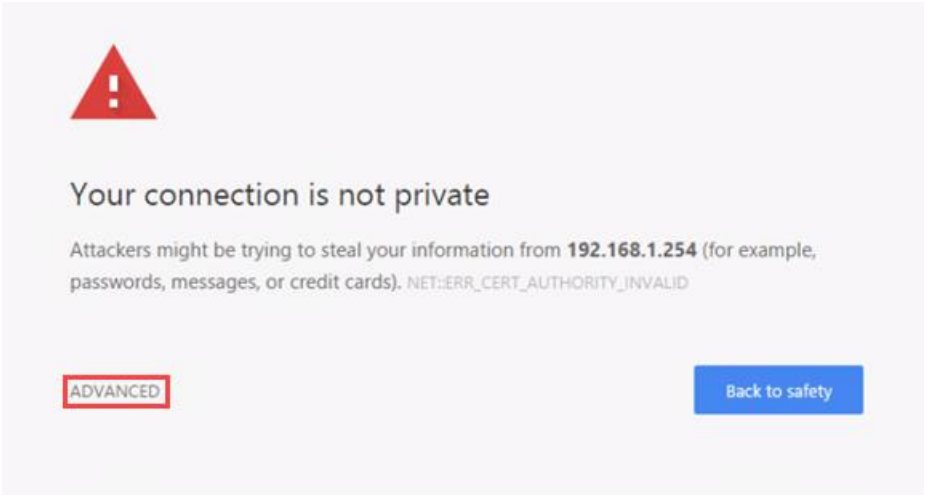


2. Log in to the client PC as username **`lab-user`**, password **`Train1ng$`**.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



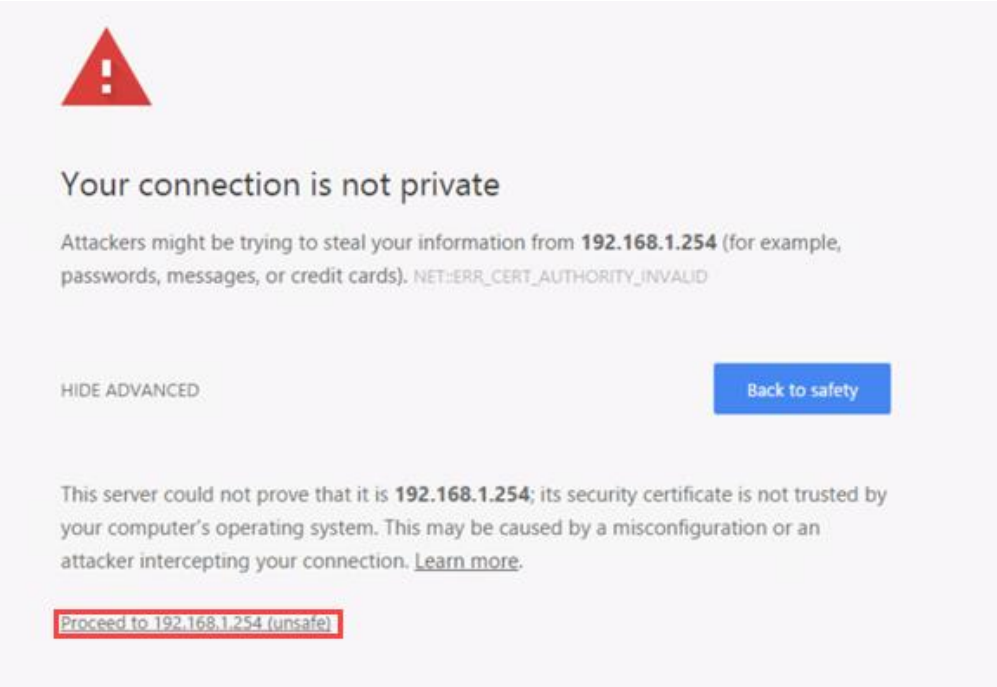
4. In the *Chromium address* field, type **`https://192.168.1.254`** and press **Enter**.

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



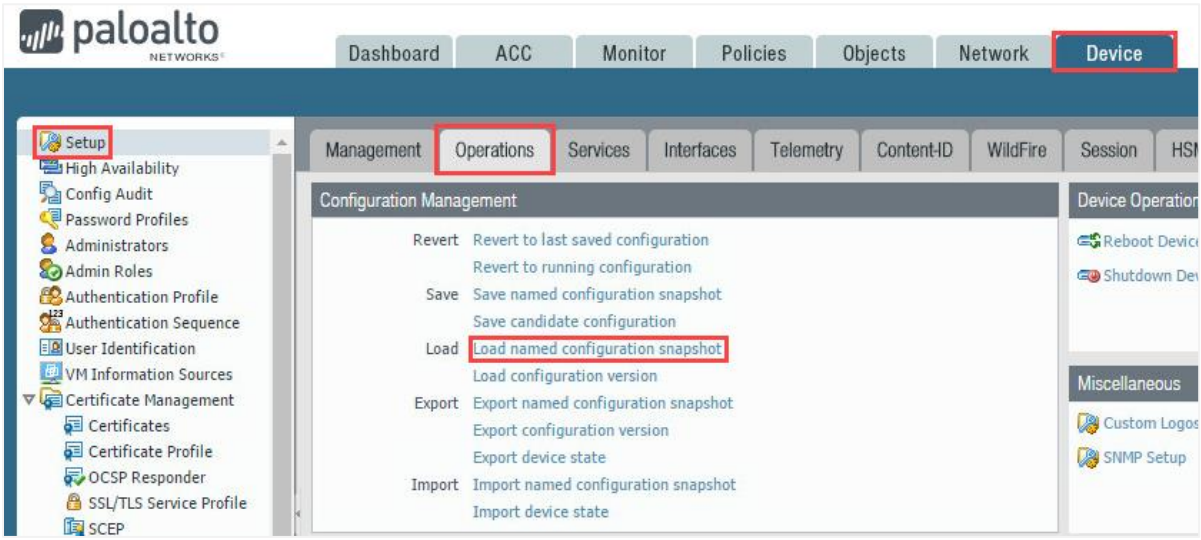
If you encounter the *"Unable to connect"* or *"502 Bad Gateway"* message while attempting to connect to the IP specified above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

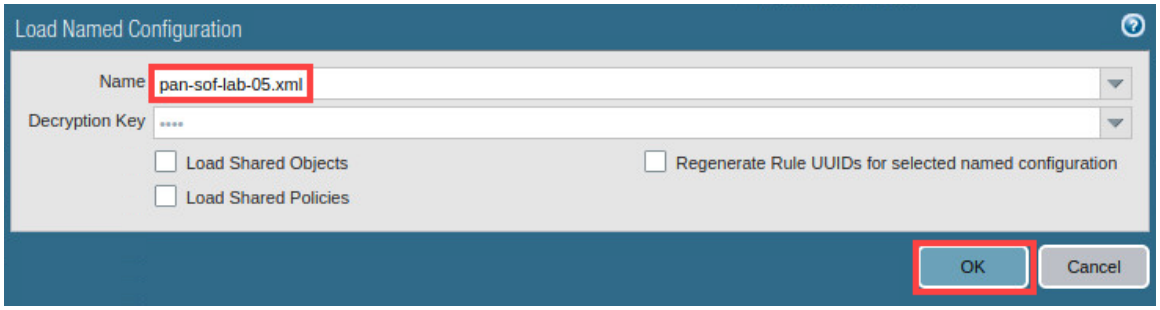


7. Log in to the Firewall web interface with username **`admin`**, password **`Train1ng$.`**

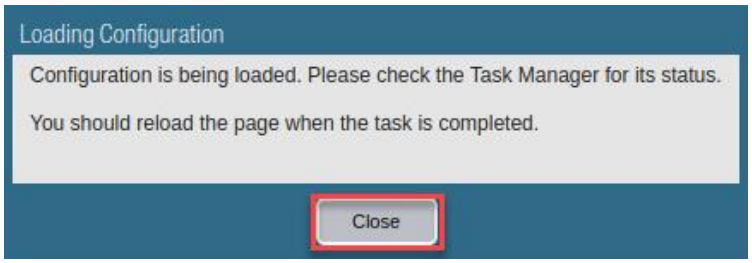
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



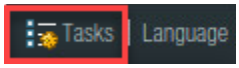
9. In the *Load Named Configuration* window, select **pan-sof-lab-05.xml** from the *Name* dropdown box and click **OK**.



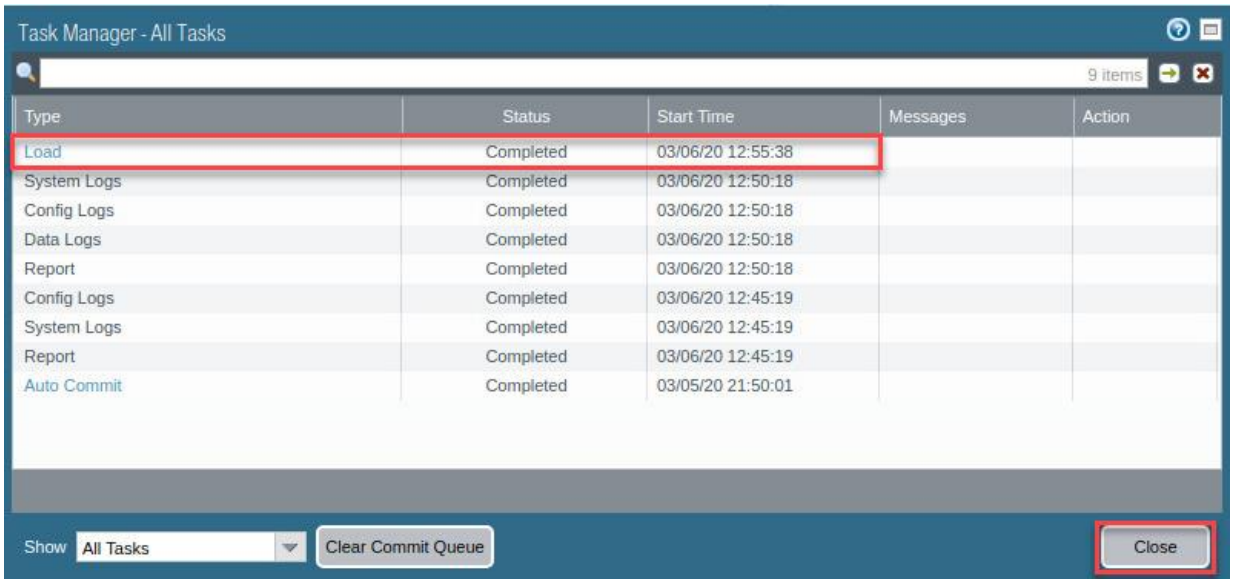
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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

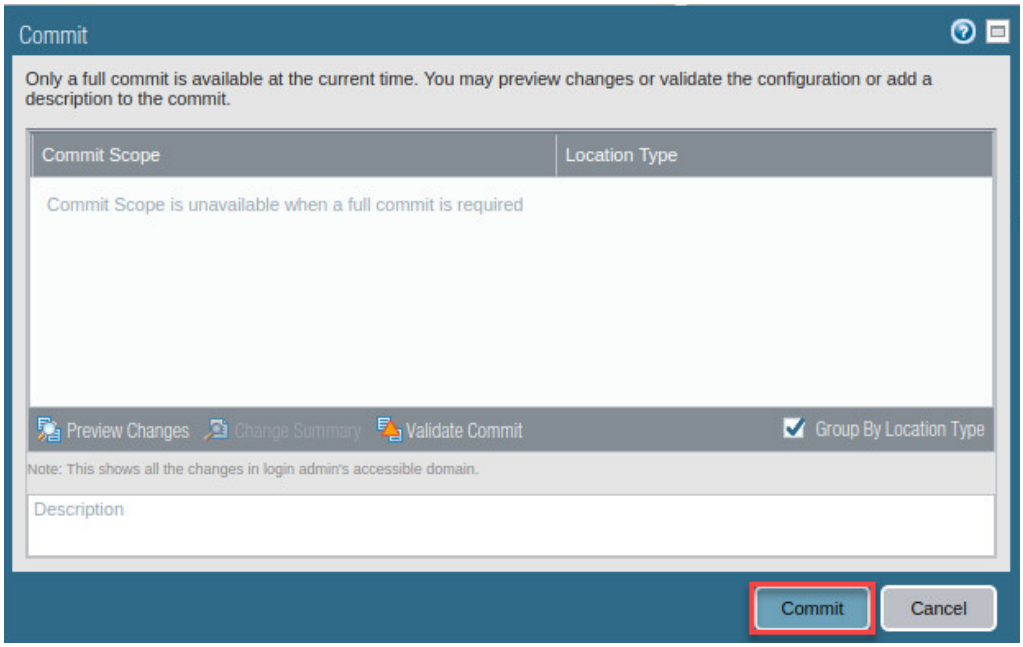


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**

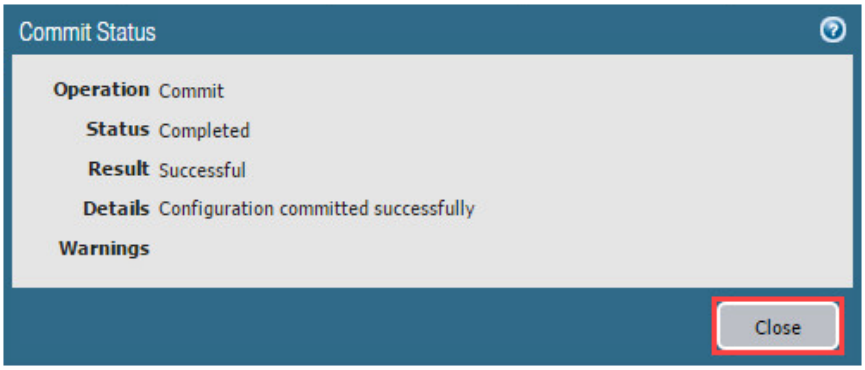


13. Click the **Commit** link located at the top-right of the web interface.

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



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

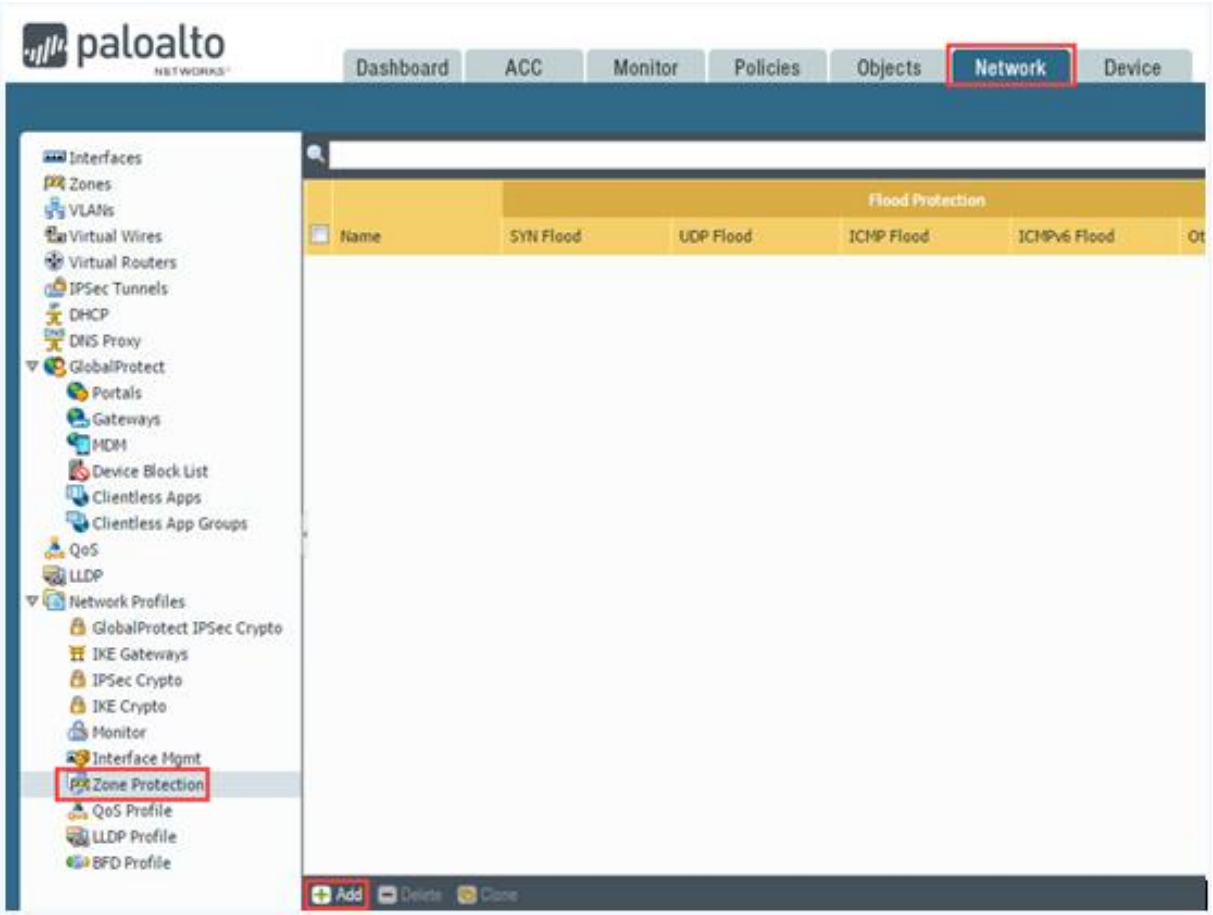


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

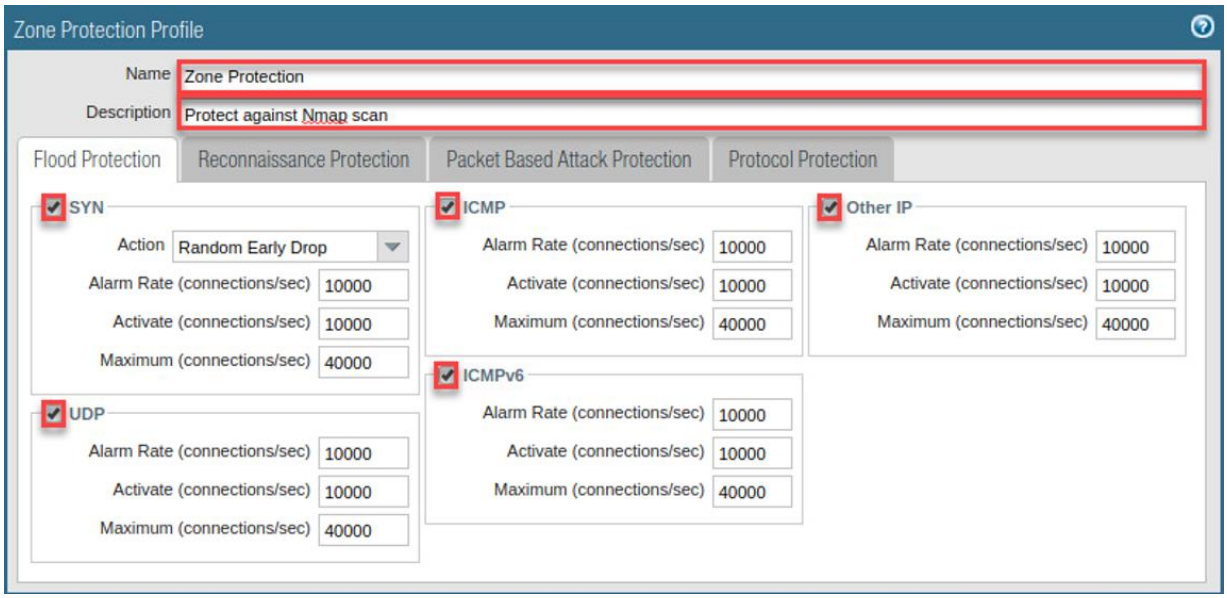
5.1 Create a Zone Protection Profile

In this section, you will create a Zone Protection Profile. Zone Protection Profiles supplement additional protection between determined zones to protect the zones against attacks**.**

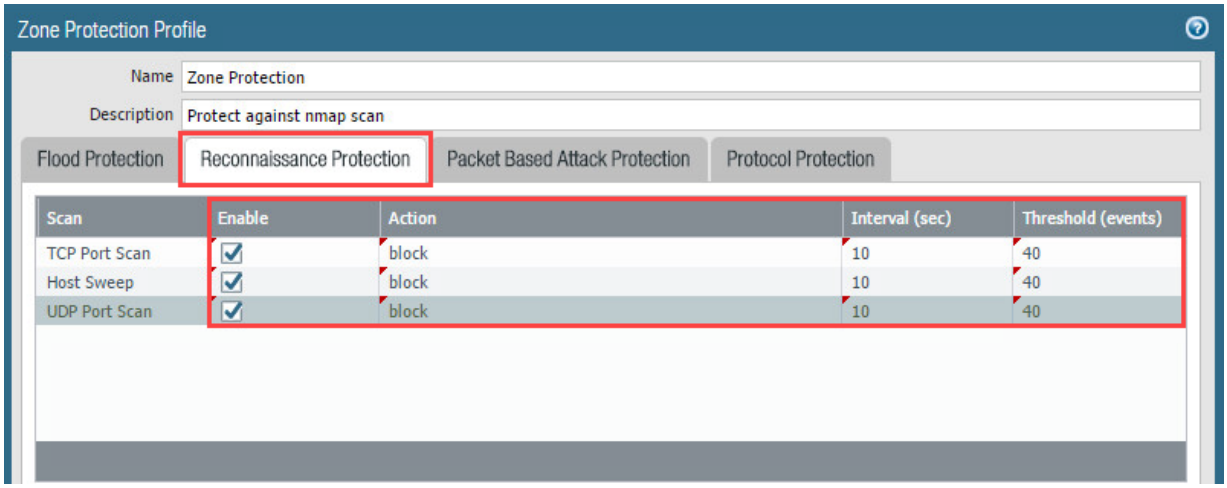
1. Navigate to **Network > Network Profiles > Zone Protection > Add**.



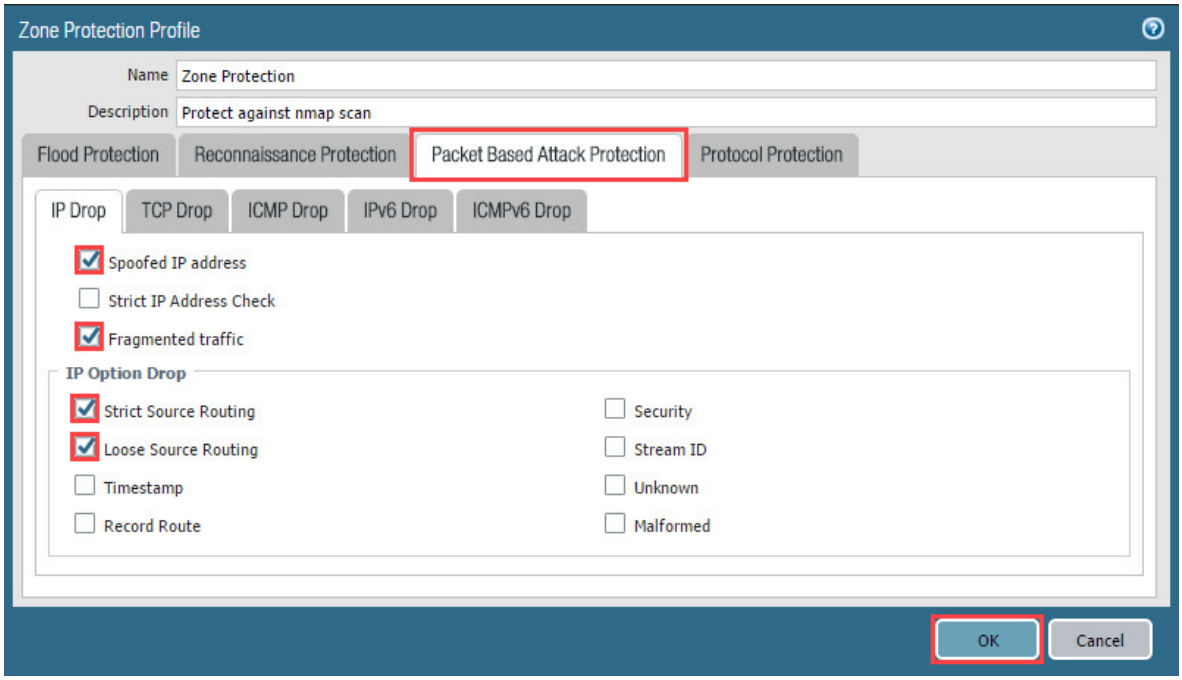
2. In the *Zone Protection Profile* window, type **`Zone Protection`** for the *Name* field. Then, type **`Protect against Nmap scan`** in the *Description* field. Next, click the checkboxes for **SYN, ICMP, Other IP, UDP**, and **ICMP6.**



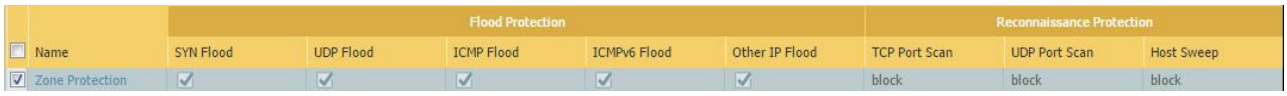
3. In the *Zone Protection Profile* window, click on the **Reconnaissance Protection** tab. Then, click the **Enable** checkboxes for **TCP Port Scan**, **Host Sweep**, and **UDP Port Scan**. Next, select **Block** for the *Action* column for all scans. Then, type **10** for the *Interval (sec)* column for all scans. Finally, type **40** for the *Threshold (events)* column for all scans.



4. In the *Zone Protection Profile* window, click on the **Packet Based Attack Protection** tab. Then, click the checkboxes for **Spoofed IP address**, **Fragmented traffic**, **Strict Source Routing**, and **Loose Source Routing**. Next, click the **OK** button.



5. Verify that your **Zone Protection Profile** is configured as shown.

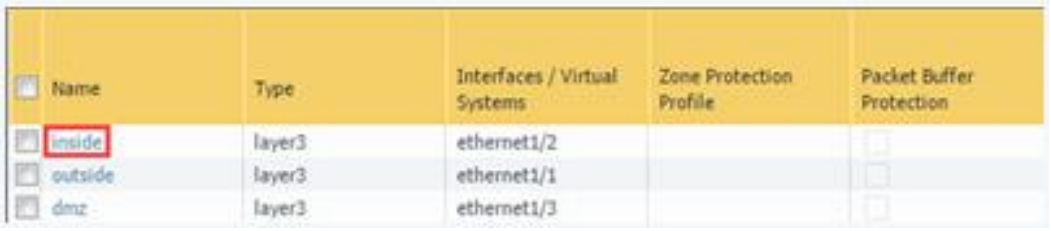


5.2 Apply the Zone Protection Profile to Zones and Commit

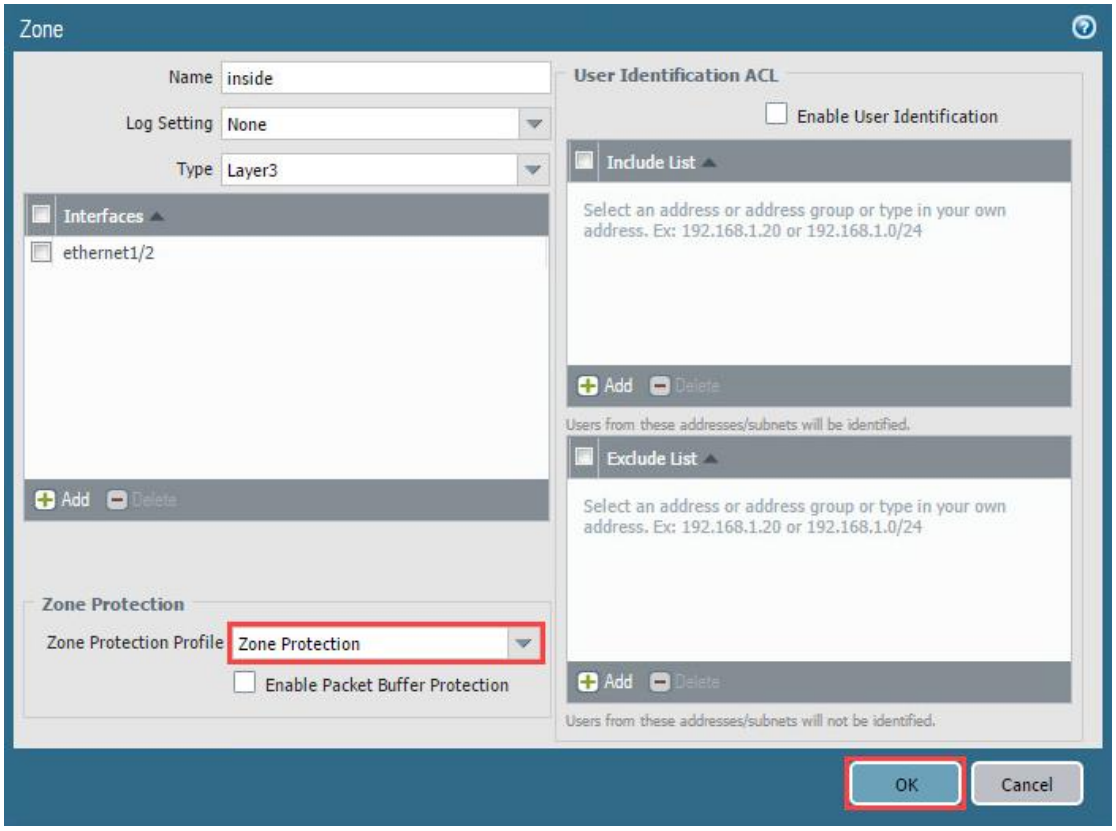
In this section, you will apply the Zone Protection Profile you created to the **inside, outside,** and **dmz** security zones. This will help control against network floods, reconnaissance, and other packet-based related attacks. Then, you will commit your changes to the Firewall.

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

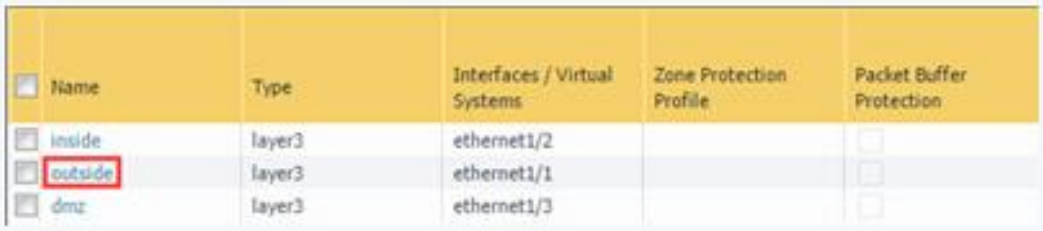
2. Click on the **inside** zone.



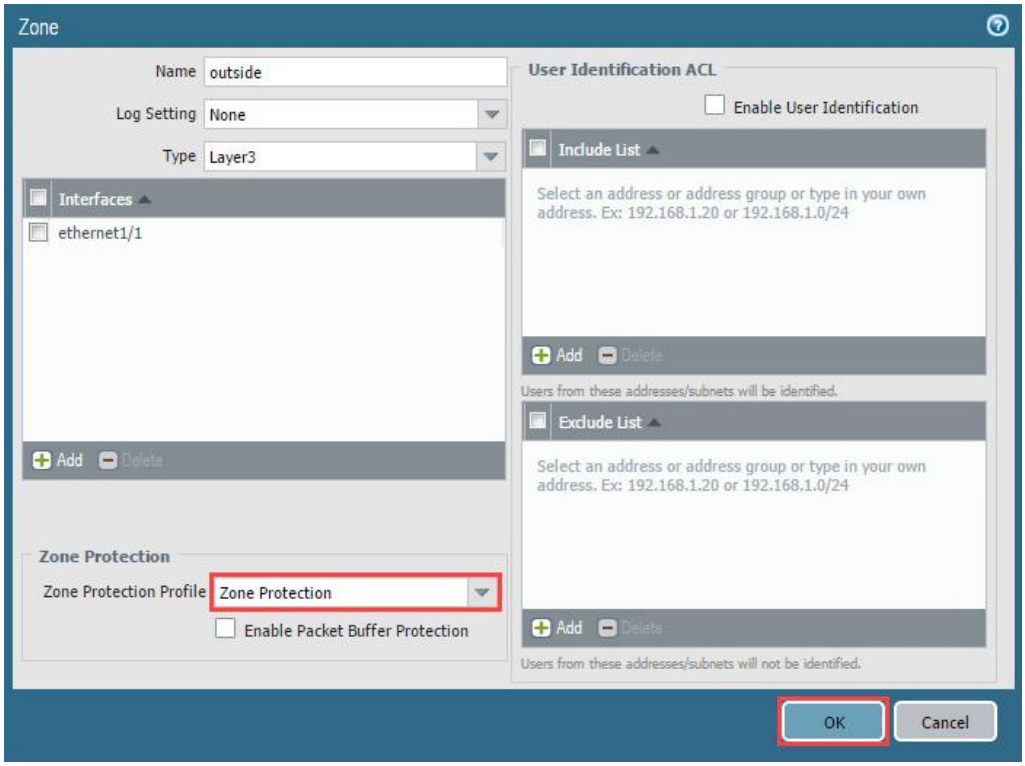
3. In the *Zone* window, select **Zone Protection** in the *Zone Protection Profile* field. Then, click the **OK** button.



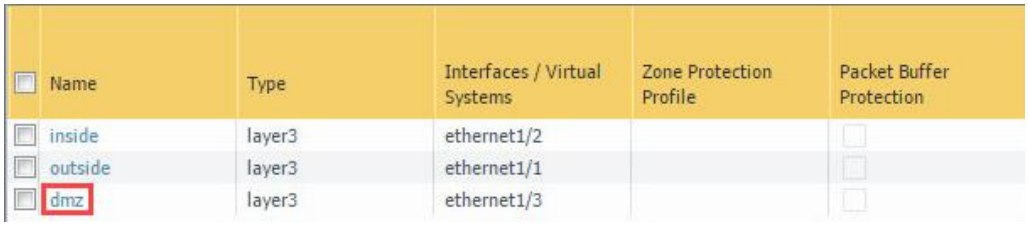
4. Click on the **outside** zone.



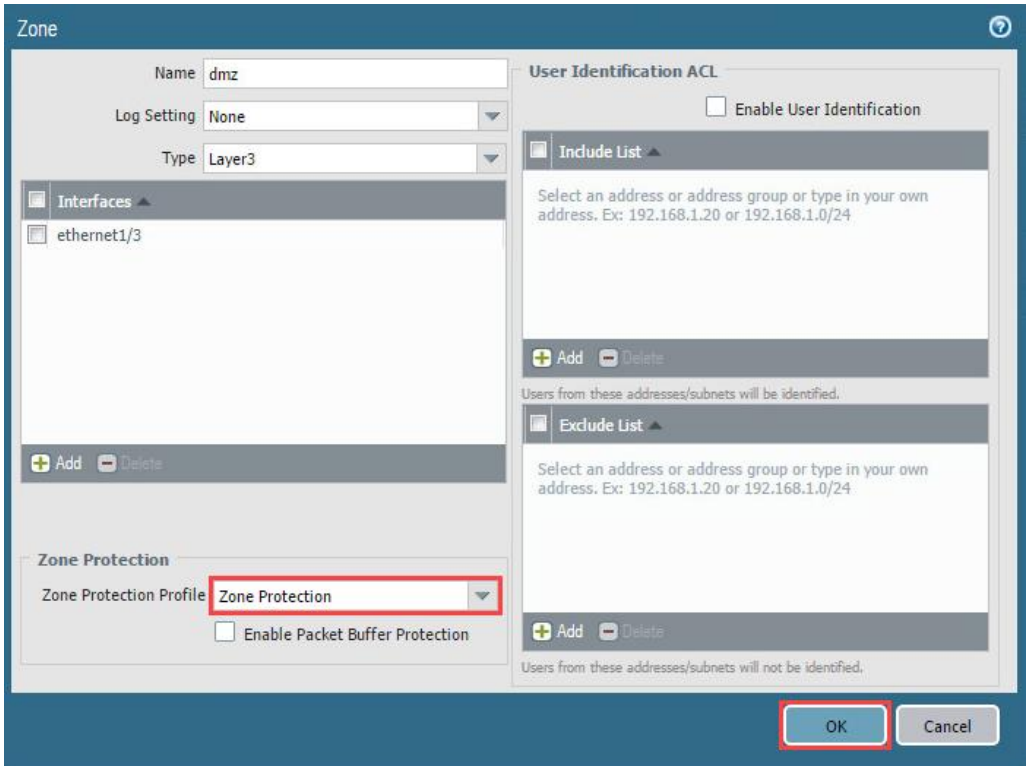
5. In the *Zone* window, select **Zone Protection** in the *Zone Protection Profile* field. Then, click the **OK** button.



6. Click on the **dmz** zone.

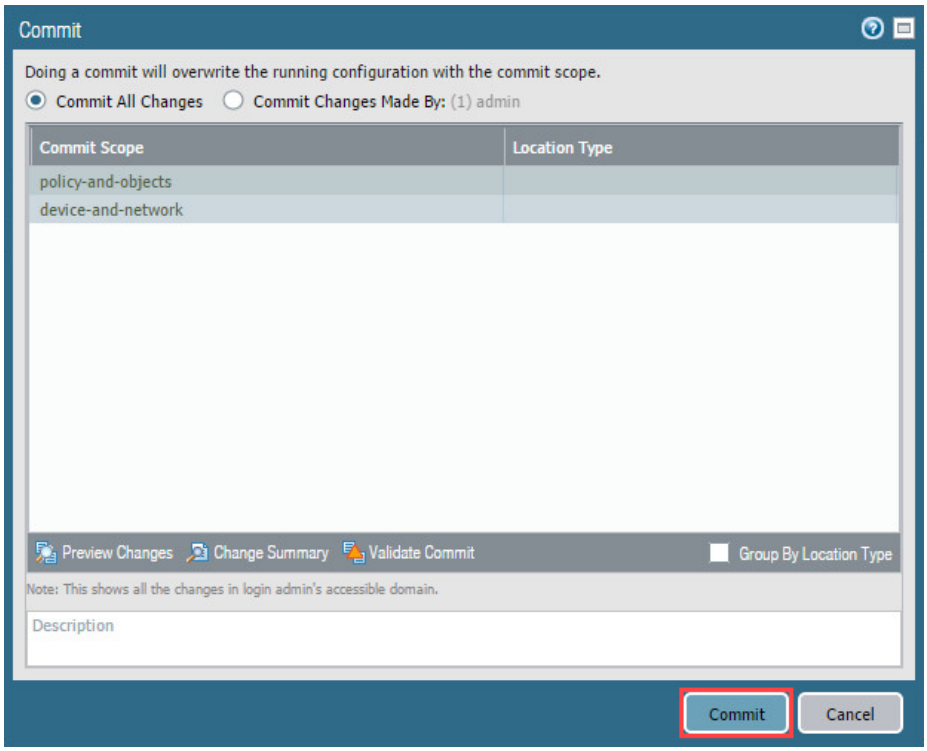


7. In the *Zone* window, select **Zone Protection** in the *Zone Protection Profile* field. Then, click the **OK** button.

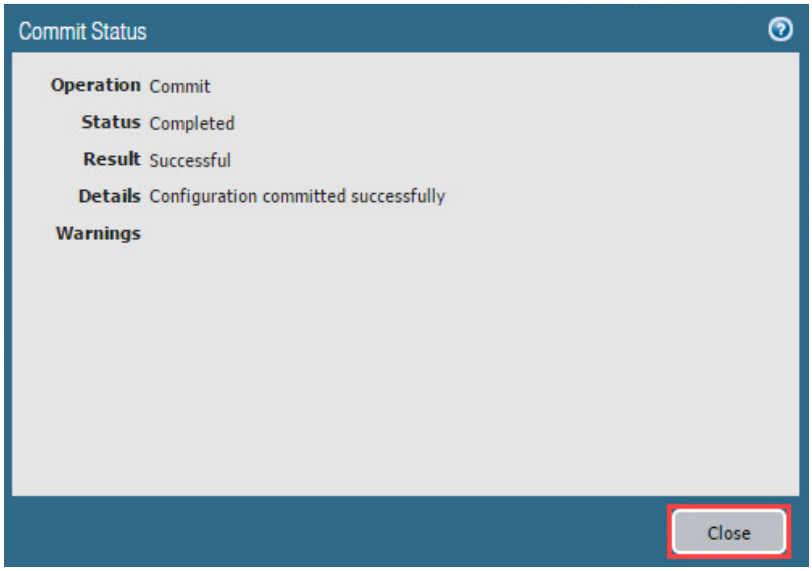


8. Click the **Commit** link located at the top-right of the web interface.

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



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

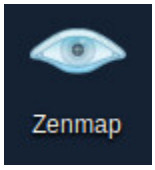


11. Minimize **Chromium** in the upper-right corner.

5.3 Perform a Reconnaissance Attack on the DMZ Server

In this section, you will use *Nmap* to perform a reconnaissance attack on the DMZ server. *Nmap* is used to scan networks as a host detection tool for penetration testing and to visualize network vulnerabilities.

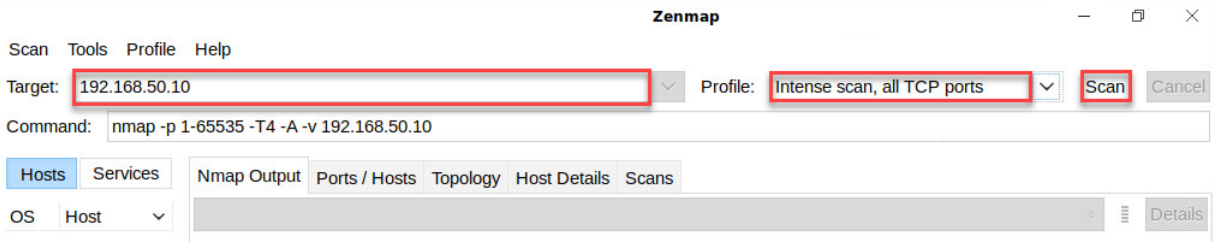
1. Double-click the **Zenmap** icon located on the desktop.



2. In the *Terminal* window, type **`Train1ng$`** for the password.

Zenmap adapts certain techniques to utilize the methods using the privilege level you are working in, that is, if you do not explicitly request something different.

3. In the *Zenmap* window, type **`192.168.50.10`** for the *Target* field. Then, select **Intense scan, all TCP ports** for the *Profile* field. Next, click the **Scan** button.



4. Minimize **Zenmap** in the upper-right corner.

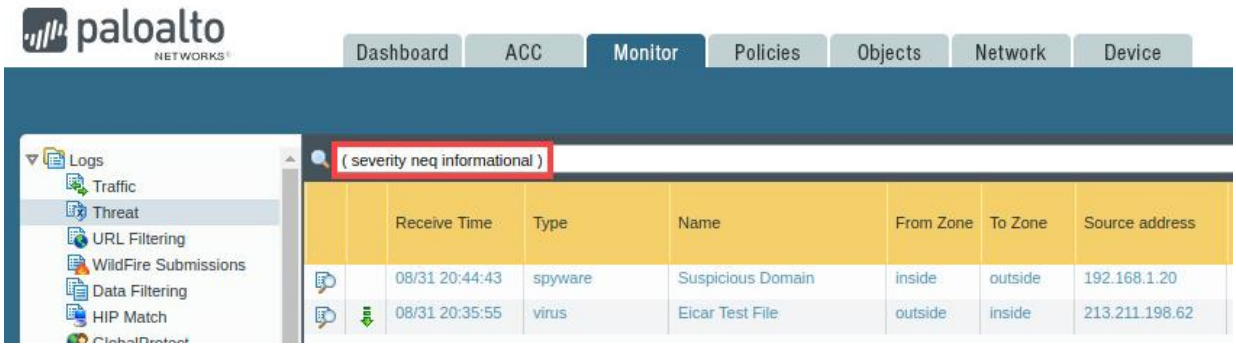
5.4 Monitor and Analyze the Threat Logs

In this section, you will monitor and analyze the Threat Logs in the Palo Alto Networks Firewall.

1. Click on **Chromium** on the taskbar to maximize.

2. Navigate to **Monitor > Logs > Threat**.

3. If **(severity neq informational)** is showing in the search box, delete it and click **Refresh**.



4. Notice the *Type* is **scan**, and the *Name* is **SCAN: TCP Port Scan** from the **inside** zone to the **DMZ** zone. The attacker in this instance is **192.168.1.20,** which is the client machine, and the victim is **192.168.50.10,** which is the DMZ server. You may need to click the **Refresh** icon in the upper-right to see traffic as it flows. You may need to click **Refresh** multiple times for the logs to show.

		Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action
		03/17 13:31:44	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	37954	not-applicable	drop
		03/17 13:31:34	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	44910	not-applicable	drop
		03/17 13:31:24	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	28223	not-applicable	drop
		03/17 13:31:14	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	49849	not-applicable	drop
		03/17 13:31:04	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	11487	not-applicable	drop
		03/17 13:30:54	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	22105	not-applicable	drop
		03/17 13:30:44	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	22988	not-applicable	drop
		03/17 13:30:34	scan	SCAN: TCP Port Scan	inside	dmz	192.168.1.20		192.168.50.10	19811	not-applicable	drop

After an administrator analyzes the logs present on the Firewall from the *Nmap* scan, the port scan activity is clearly visible. If this had been a malicious hacker scanning the network, the threat logs would have alerted the administrator. For the purposes of this lab, the security policy is set to allow all traffic. That security policy setting most likely would not be utilized in a production environment. If the security policy would have been set to deny traffic, an alert would have been triggered by the *Nmap* scan but the scan traffic would not have been allowed between the zones.

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