PALO ALTO NETWORKS EDU 210

Lab 6: Blocking Packet and Protocol Based Attacks

Document Version: 2022-07-18

Contents

Introduction

You want to make certain that the Palo Alto Networks firewall provides protection against Layer 3 and Layer 4 attacks and network probes such as port scans.

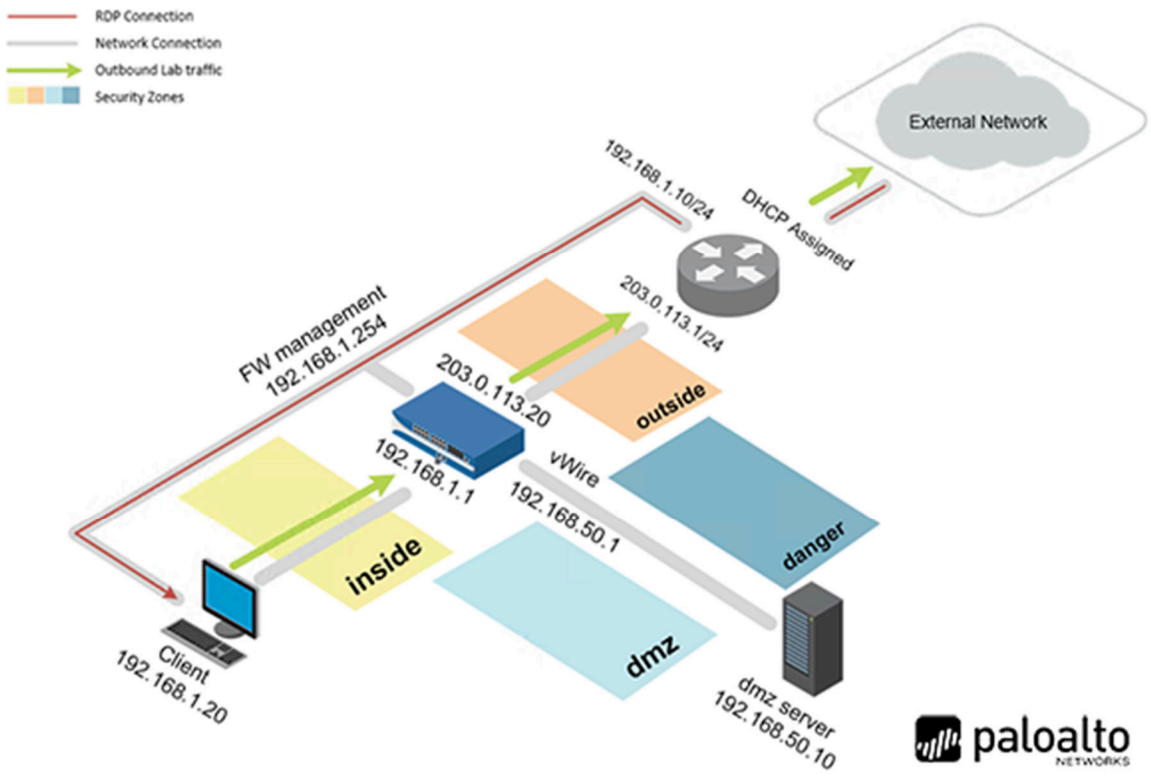
You will create a Zone Protection Profile that you can assign to security zones. You will also create a DoS Protection Profile and DoS policy rules to ensure that you are taking advantage of all the tools that the firewall has available to block packet-based floods and probes.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Configure a Zone Protection Profile to detect and control SYN floods
- Configure a Zone Protection Profile to detect and control reconnaissance scans
- Configure a Zone Protection Profile to detect and control specific IP header options
- Configure a Zone Protection Profile to perform spoofed IP address checking
- Configure a DoS Protection Profile to protect firewall and node resource consumption
- Configure a DoS Protection Profile to detect and control SYN floods

Lab Topology



Lab Settings

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

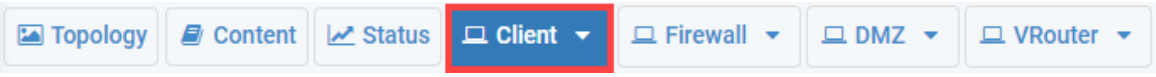
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Blocking Packet and Protocol Based Attacks

1.1 Apply a Baseline Configuration to the Firewall

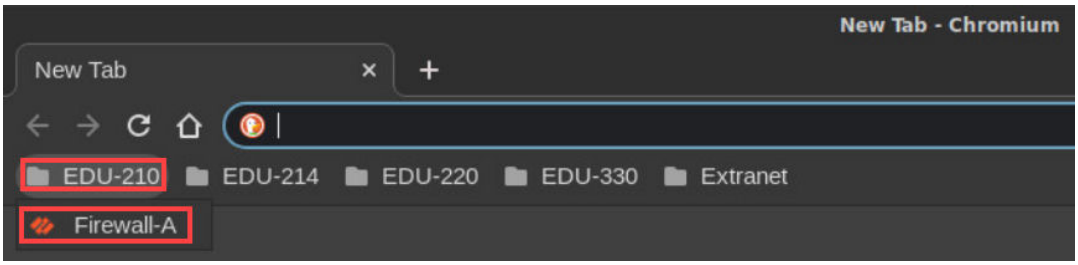
In this section, you will load the firewall configuration file.

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

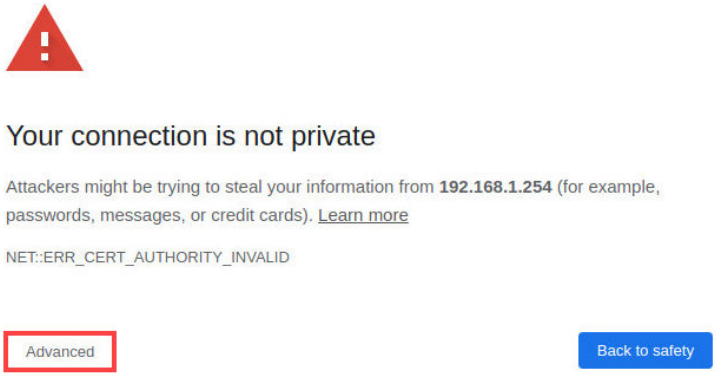


2. Double-click the **Chromium Web Browser** icon located on the desktop.

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

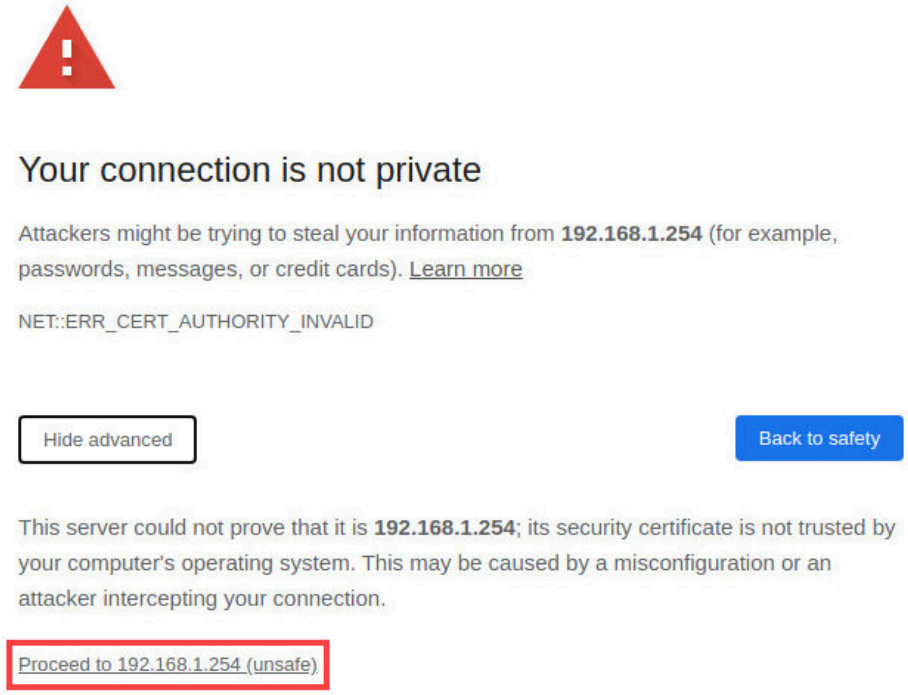


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



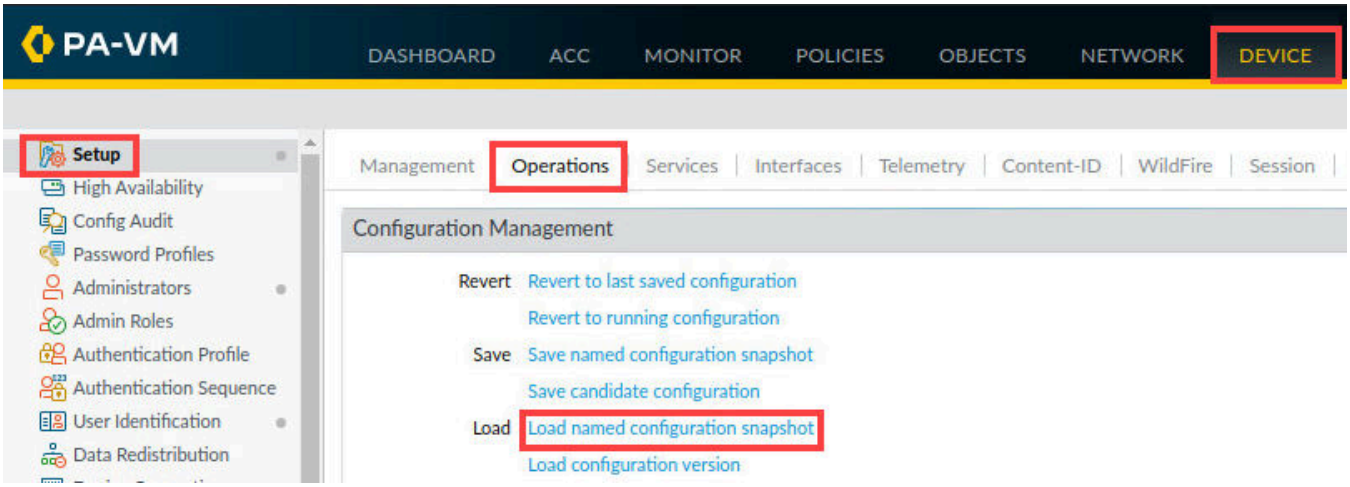
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

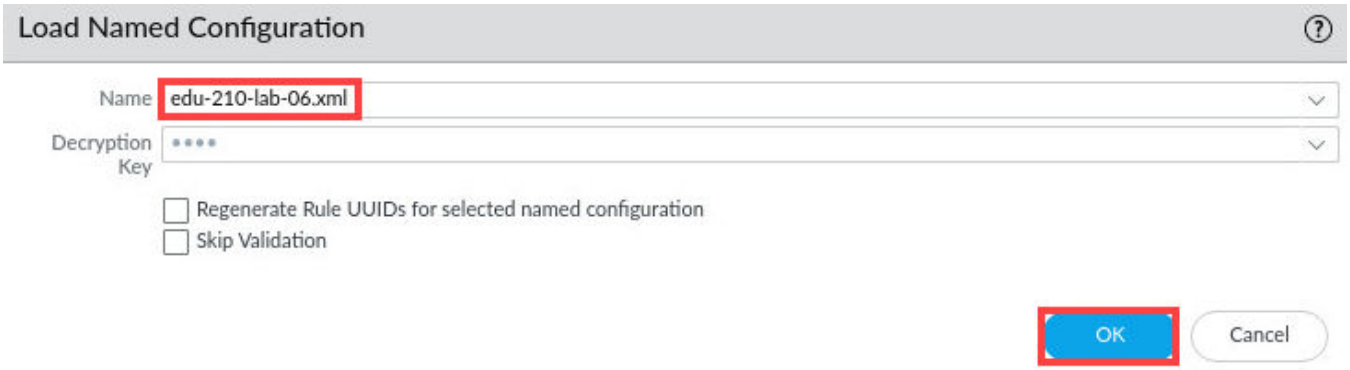


6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

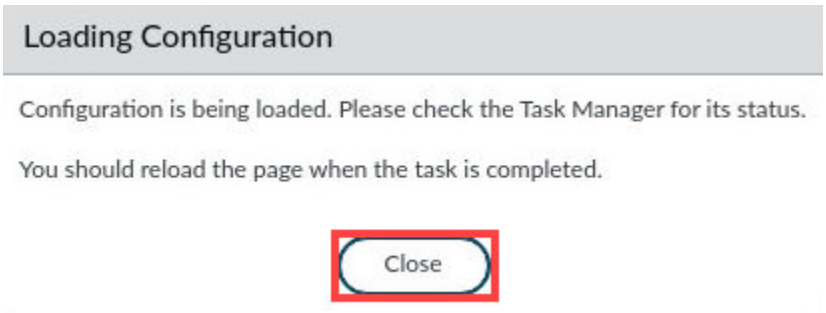
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



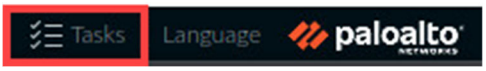
8. In the *Load Named Configuration* window, select **edu-210-lab-06.xml** from the *Name* dropdown box and click **OK**.



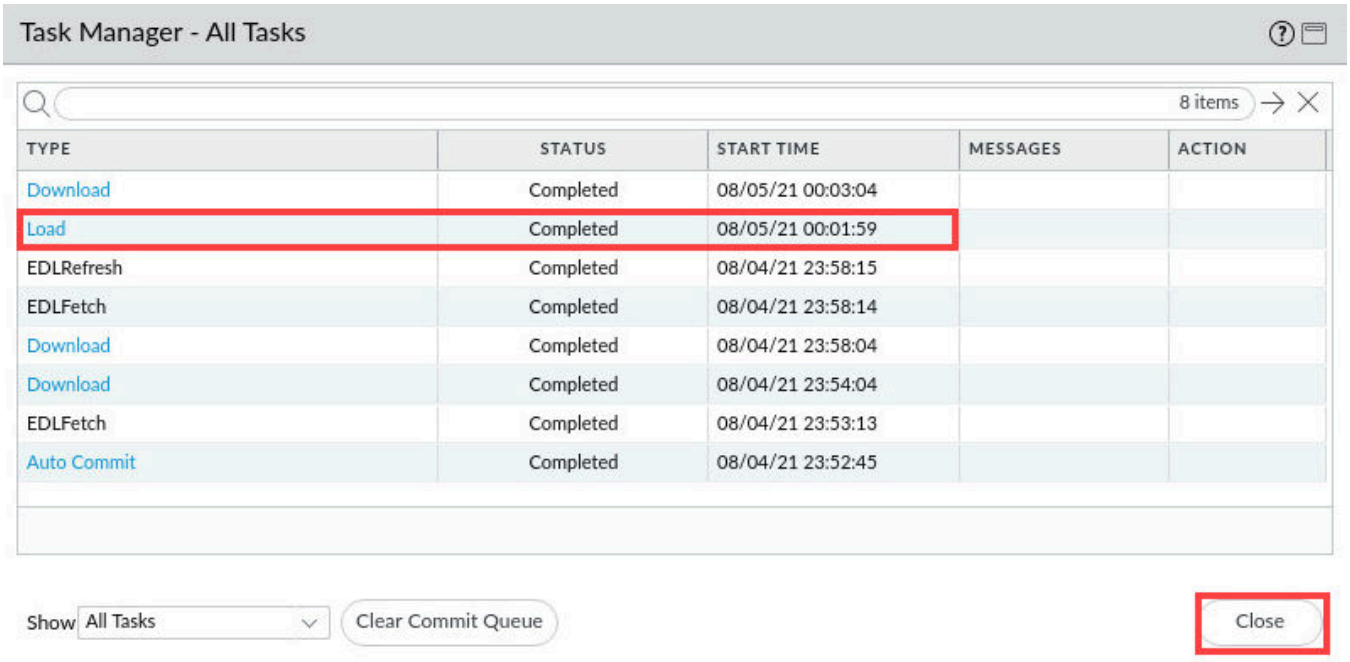
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



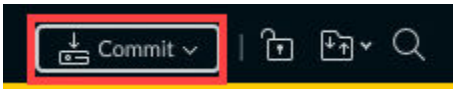
10. Click the **Tasks** icon located at the bottom-right of the web interface.



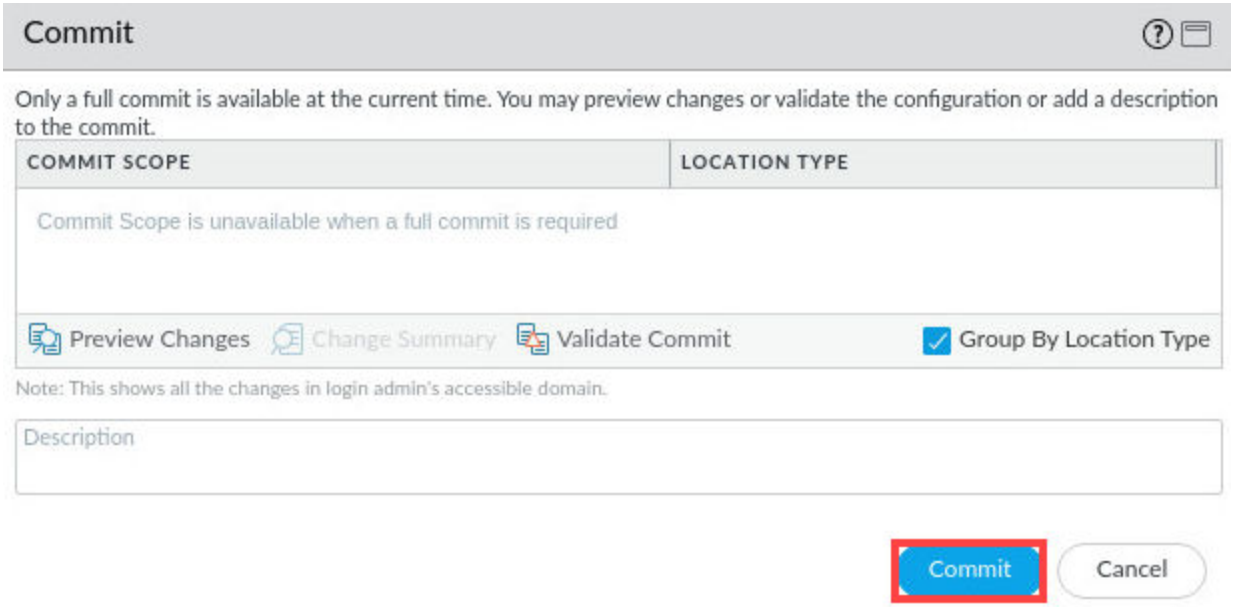
11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



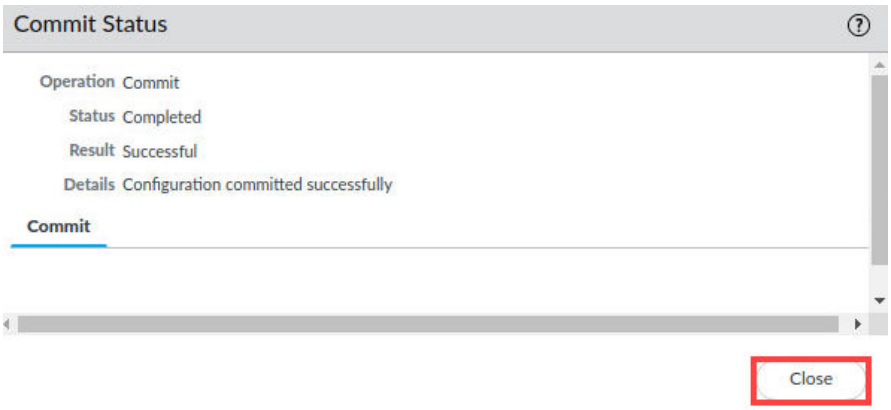
12. Click the **Commit** link located at the top-right of the web interface.



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



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



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

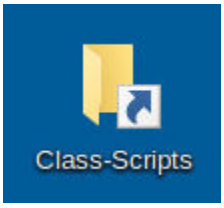
16. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.2 Generate SYN Flood Traffic

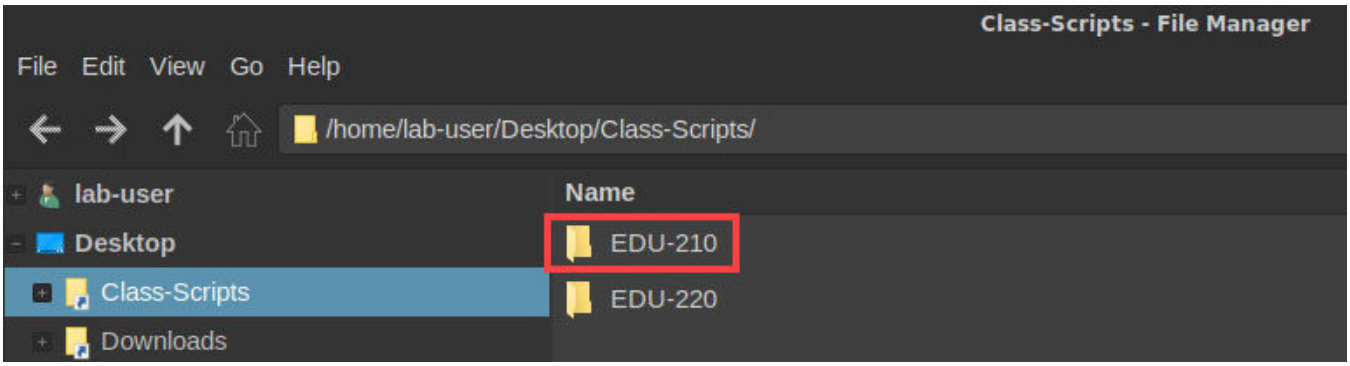
You will use a script on the client host in the Users_Net zone to send numerous TCP SYN packets to a target server in the Extranet zone.

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

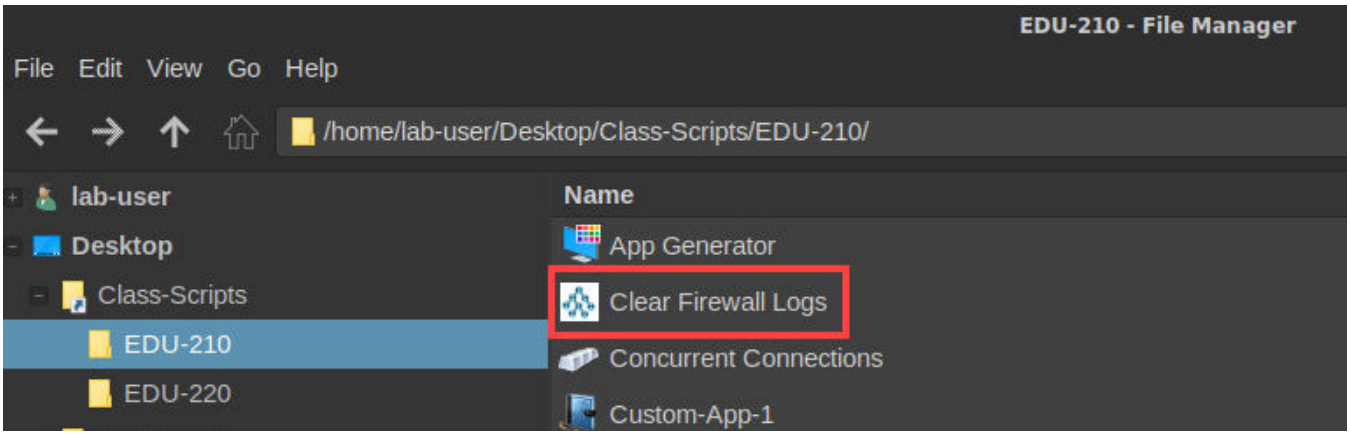
2. On the *client desktop*, double-click the folder for **Class-Scripts**.



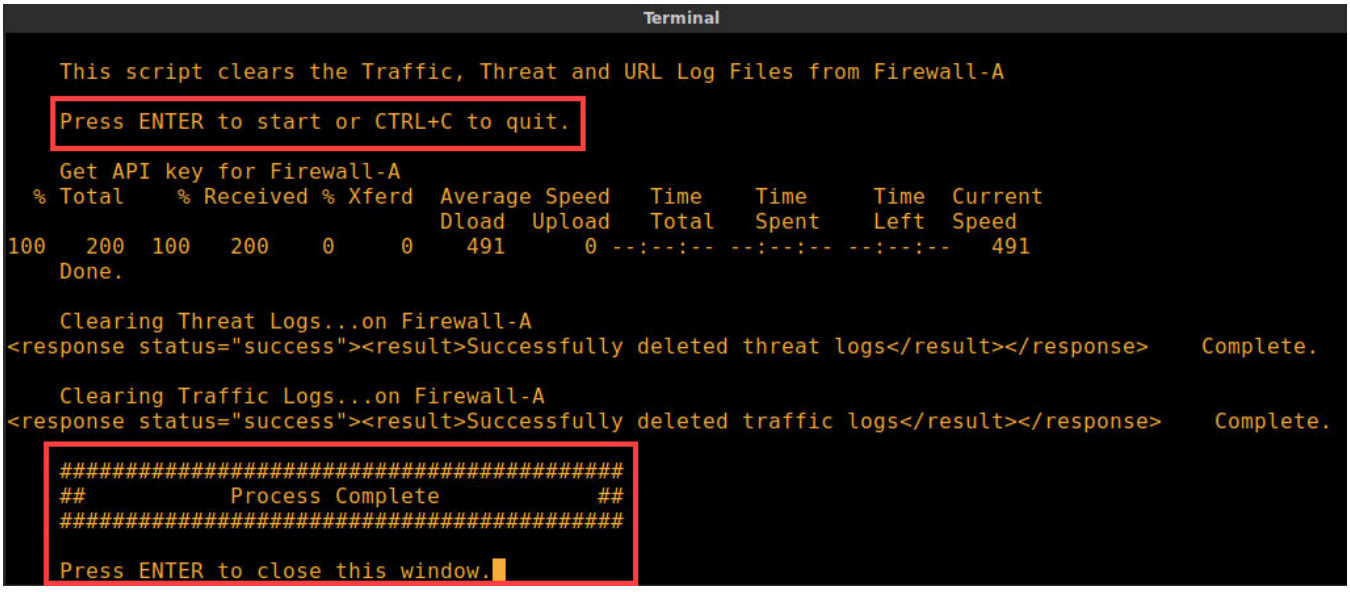
3. Open the **EDU-210** folder.



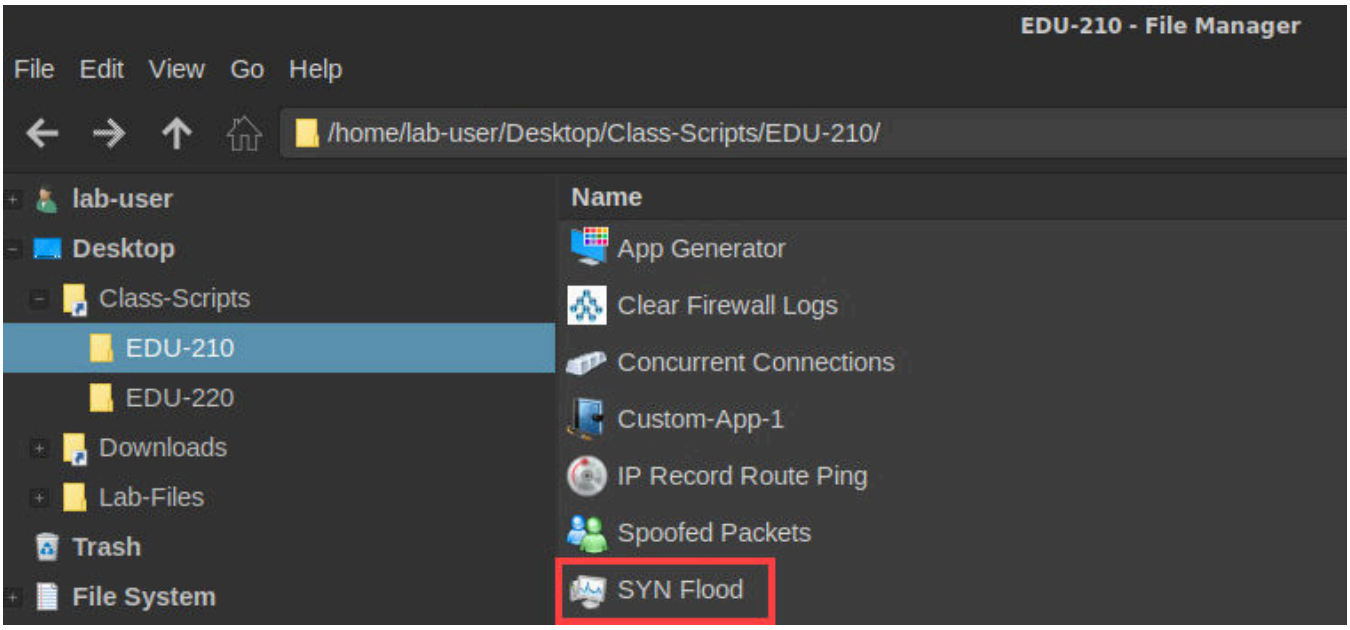
4. Double-click the icon for **Clear Firewall Logs.**



5. Press **Enter** to start the *Clear Firewall Logs* script. Allow the script to complete. Once the *Clear Firewall Logs* script completes, press **Enter**. Leave the *EDU-210 – File Manager* window open.



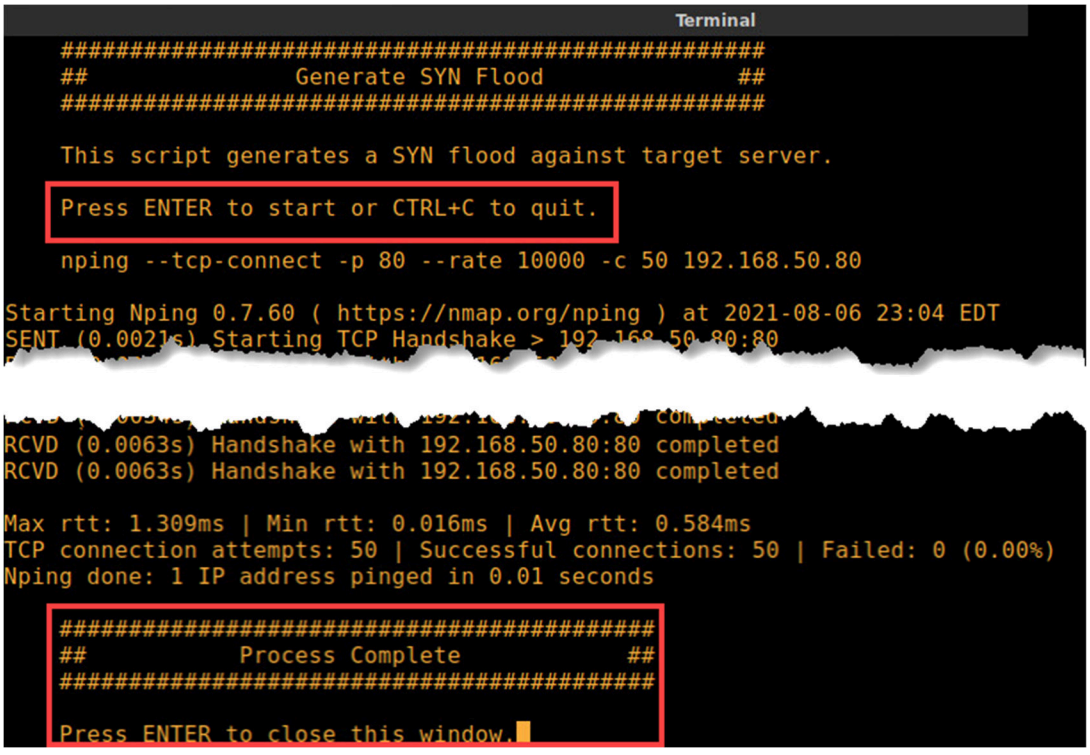
6. Double-click the icon for **SYN Flood**.



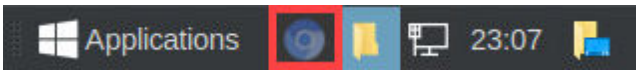
Please Note

This script uses the nmap tool to send multiple SYN packets to a server in the Extranet zone.
nping --tcp-connect -p 80 --rate 10000 -c 50 -1 192.168.50.80

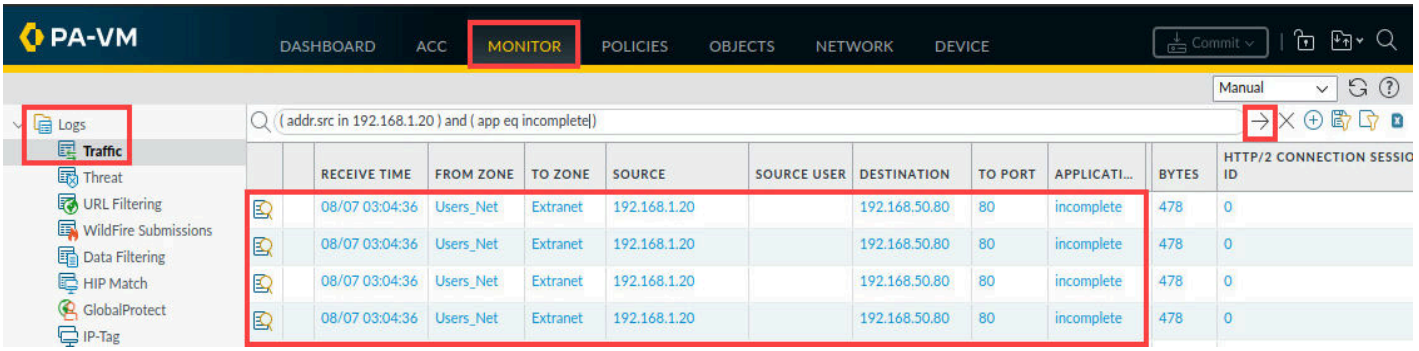
7. Press **Enter** to start the *SYN Flood* script. Allow the script to complete. Once the SYN Flood script completes, press **Enter**. Leave the *EDU-210 – File Manager* window open.



8. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*



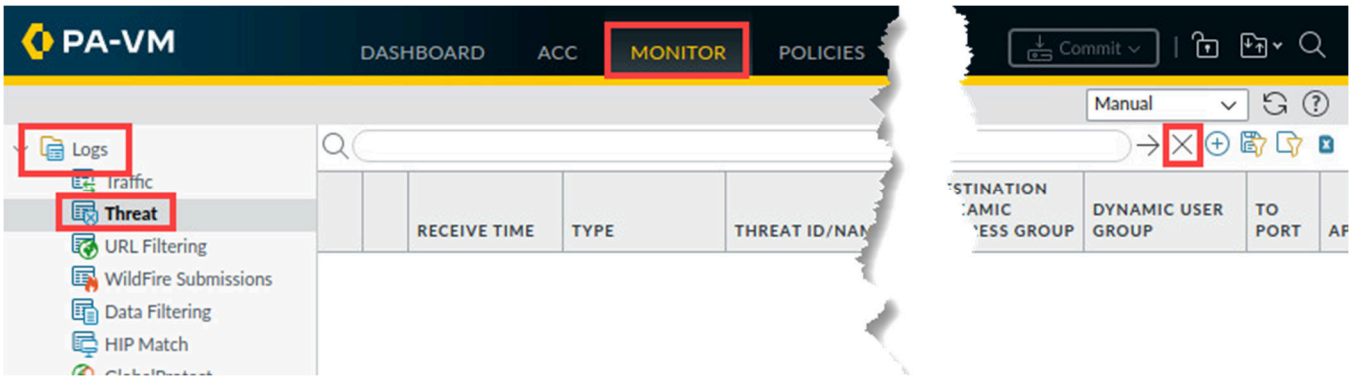
9. Navigate to **Monitor > Logs > Traffic**. Type **`( addr.src in 192.168.1.20 ) and ( app eq incomplete )`** in the filter builder. Press **Enter** or click the **Apply Filter** icon, and you should see incomplete connection attempts from *192.168.1.20* to *192.168.50.80* and port *80* in the Traffic log.



Please Note

Note that in the previous example image, several default columns have been moved or hidden. You may also find that there are certain columns that you scan frequently, and you can move those to locations by dragging and dropping to make easier to see.

10. Navigate to **Monitor > Logs > Threat**. Click the **X** icon to clear any filters. Nothing should be logged to the Threat log because no threat protections have been configured on the firewall.



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

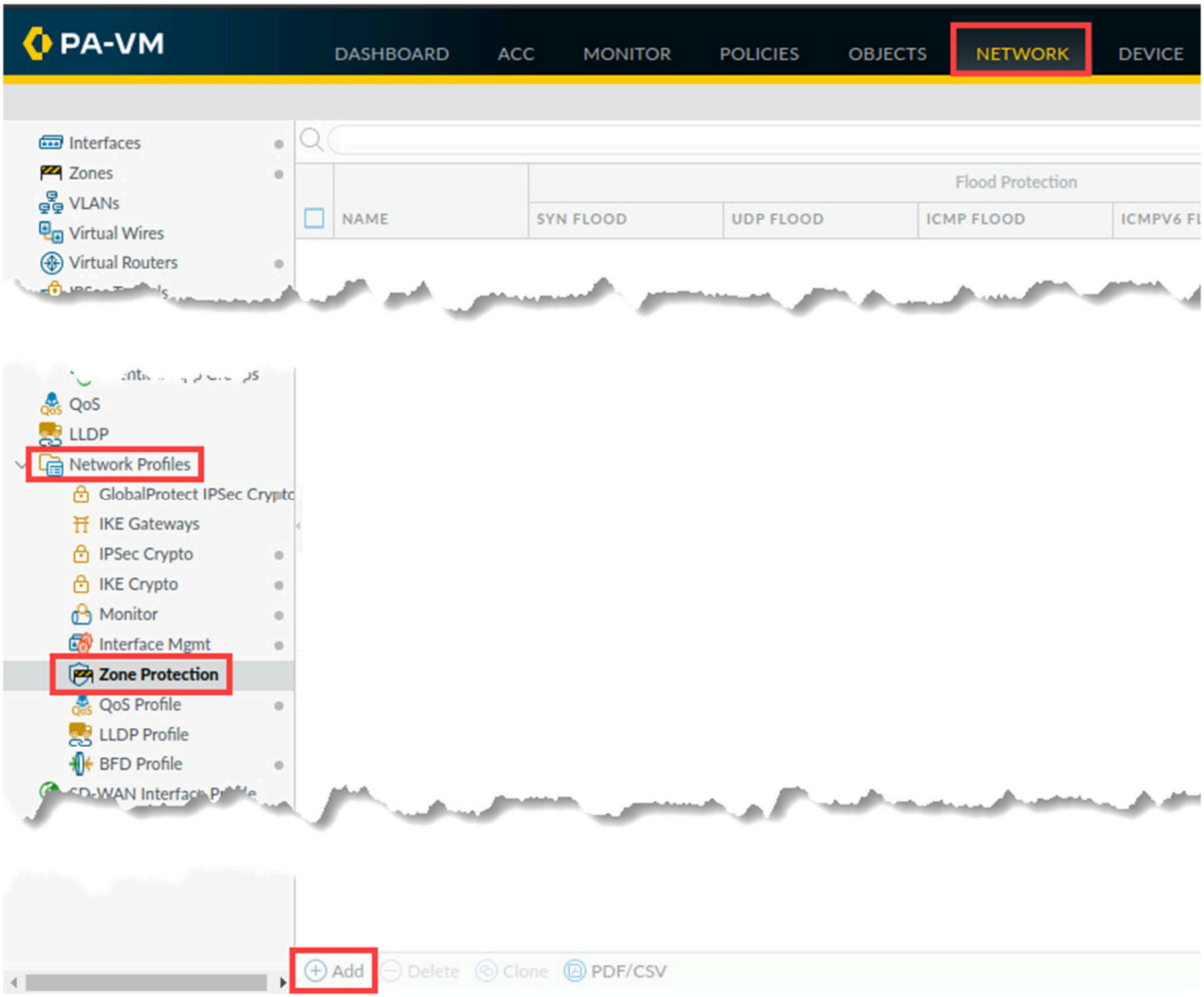
1.3 Configure and Test TCP SYN Flood Zone Protection

A Zone Protection Profile can detect and block flood attacks, including a TCP SYN flood. You will configure a very low SYN flood protection threshold that quickly will trigger flood events, even with a limited amount of traffic. You will see how flood protection operates.

After you define the settings for a Zone Protection Profile, you must apply it to the security zone.

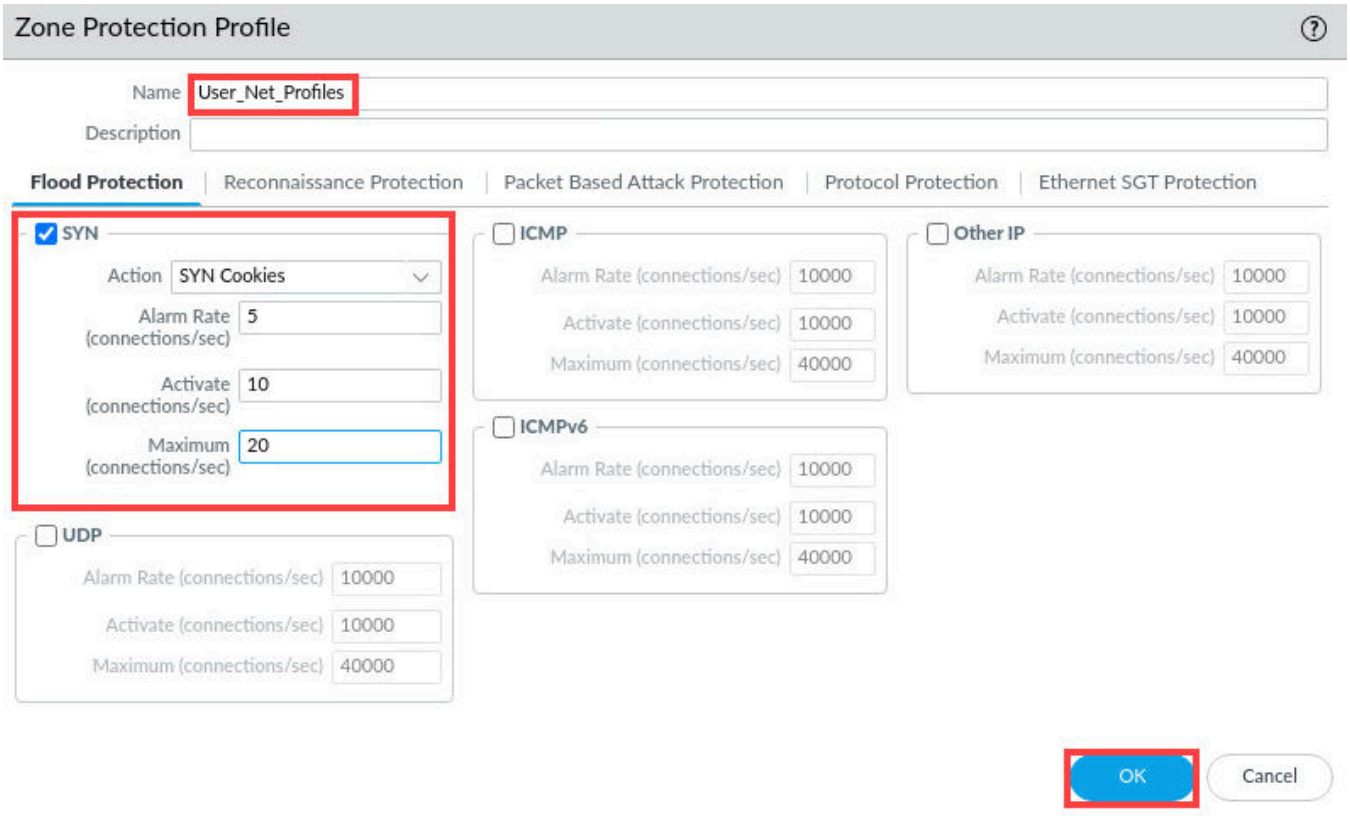
Lastly, you will Generate TCP SYN flood traffic again to determine how the flood threshold settings in the Zone Protection Profile operate. The flood packets will arrive at the firewall's inside zone, which is protected by the Zone Protection Profile.

1. In the web interface, select **Network > Network Profiles > Zone Protection**. Click **Add** to create a new Zone Protection Profile.



2. On the *Flood Protection* tab, configure the following. Click **OK**.

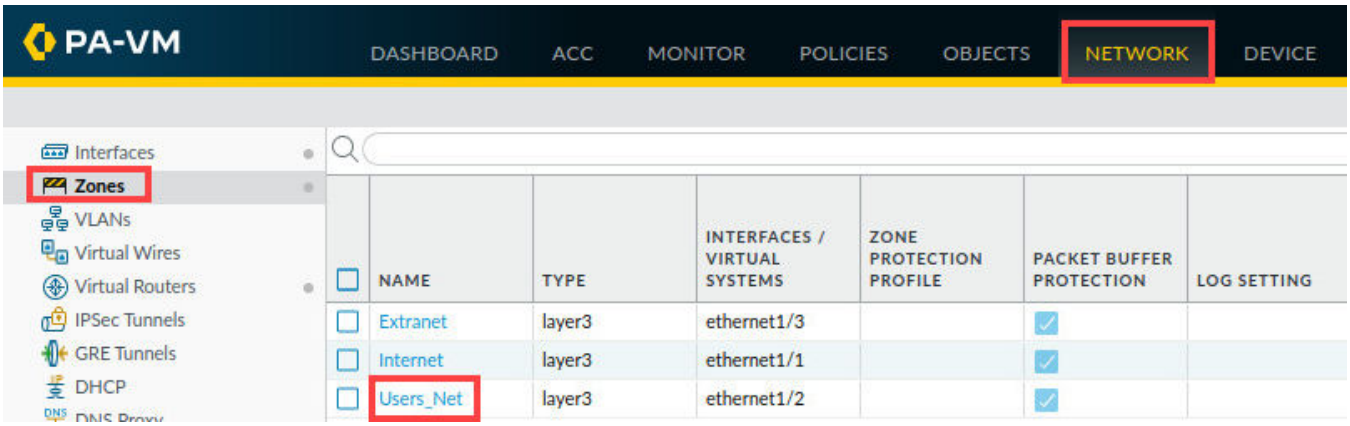
Parameter	Value
Name	**User_Net_Profiles**
SYN	Select **check box**
Action	**SYN Cookies**
Alarm Rate	**5**
Activate	**10**
Maximum	**20**



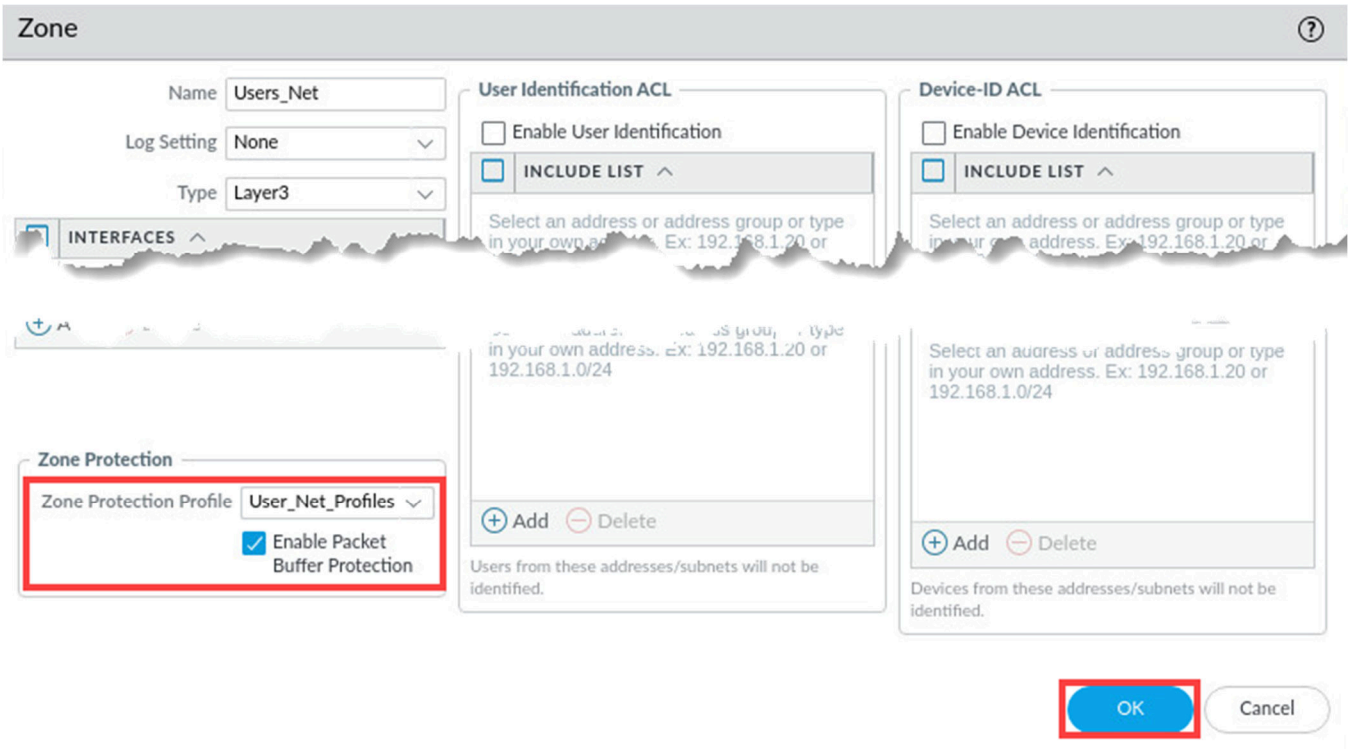
Please Note

These settings are artificially low so that the firewall will implement Zone Protection during the testing part of the lab.

3. In the web interface, select **Network > Zones**. Click **Users_net**.

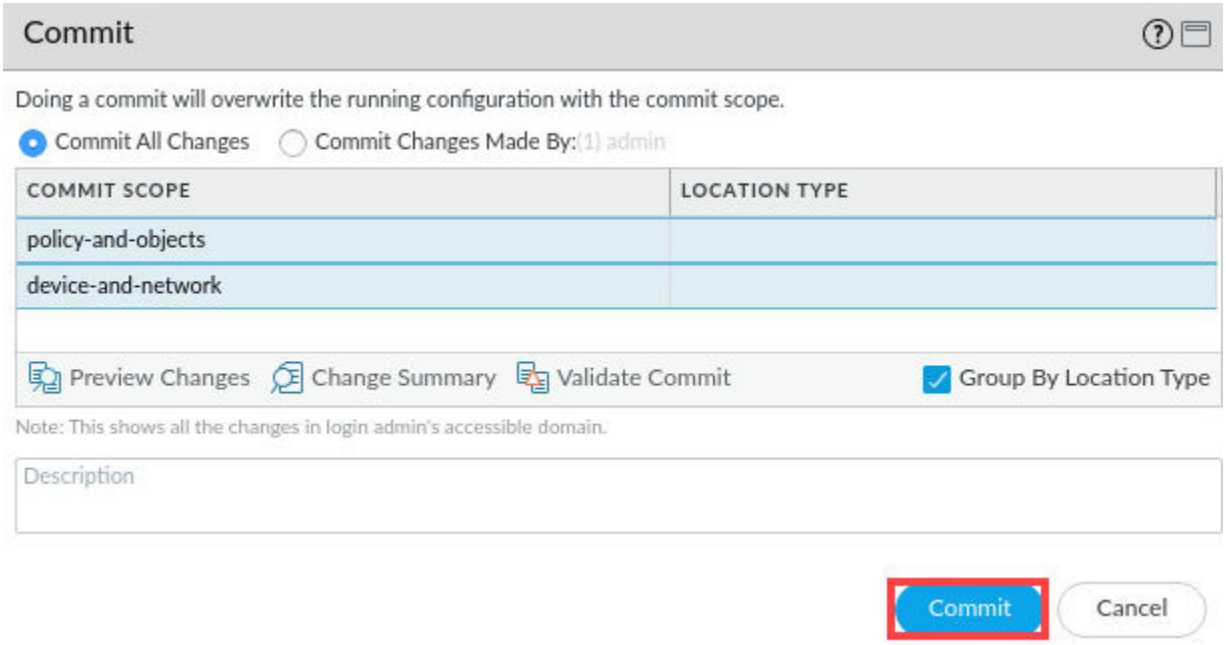


4. In the *Zone* window, in the bottom-left corner, select **User_Net_Profiles** under the *Zone Protection Profile* dropdown list. Verify **Enable Packet Buffer Protection** is checked. Click **OK**.

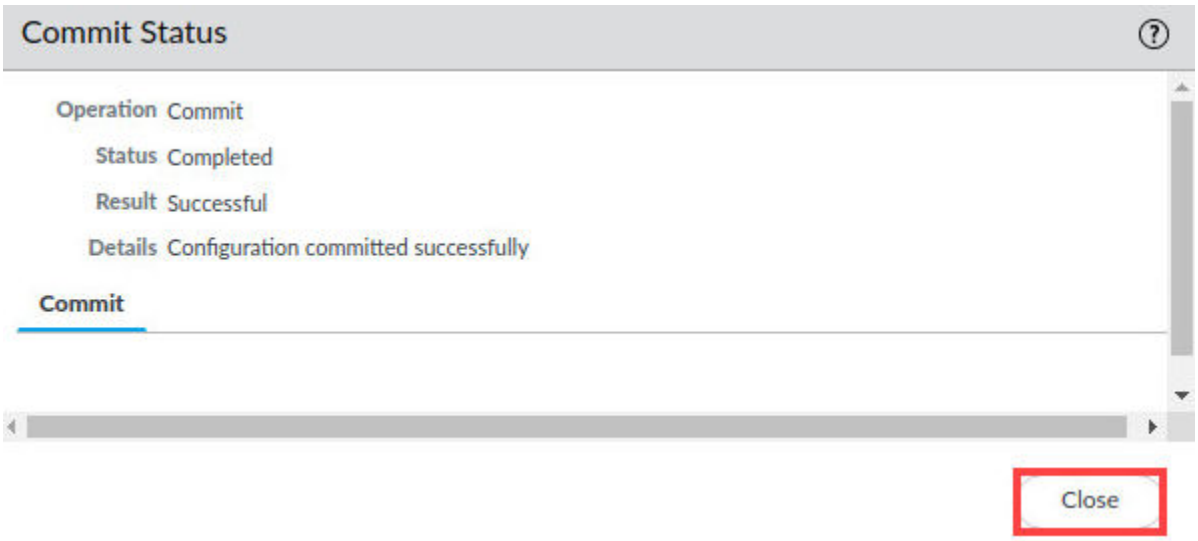


5. Click the **Commit** button at the upper-right of the web interface.

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

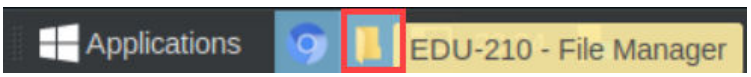


7. Wait until the *Commit* process is complete. Click **Close**.

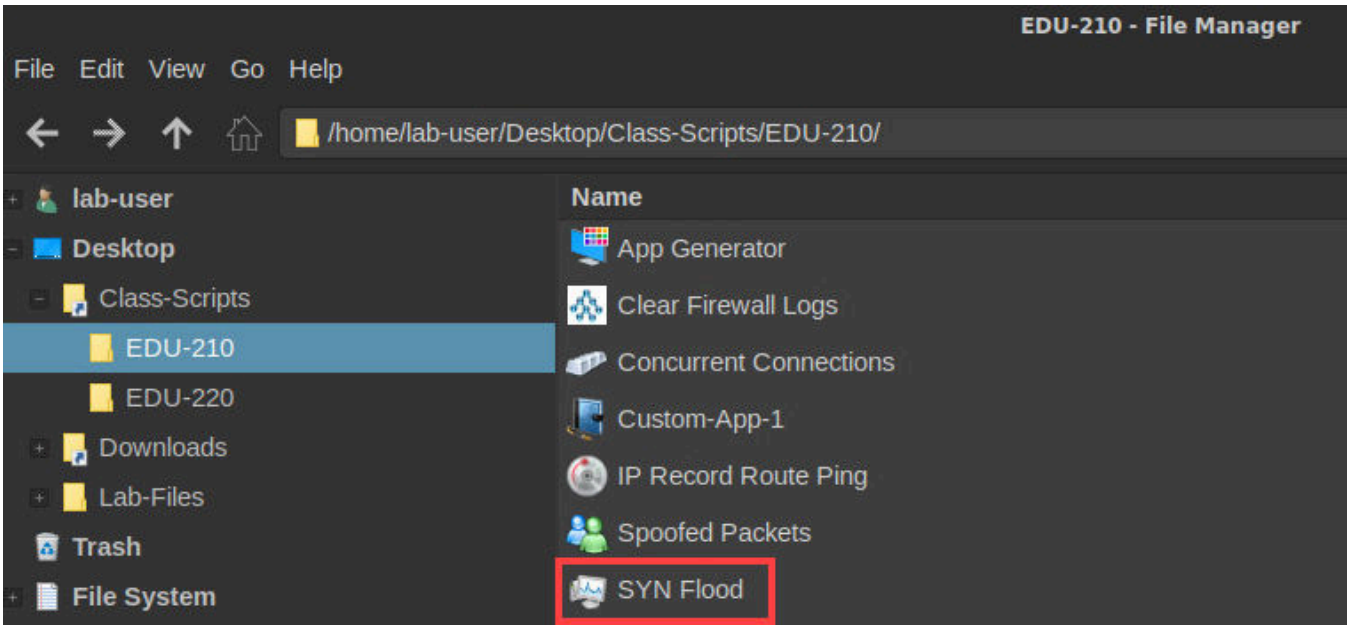


8. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

9. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.



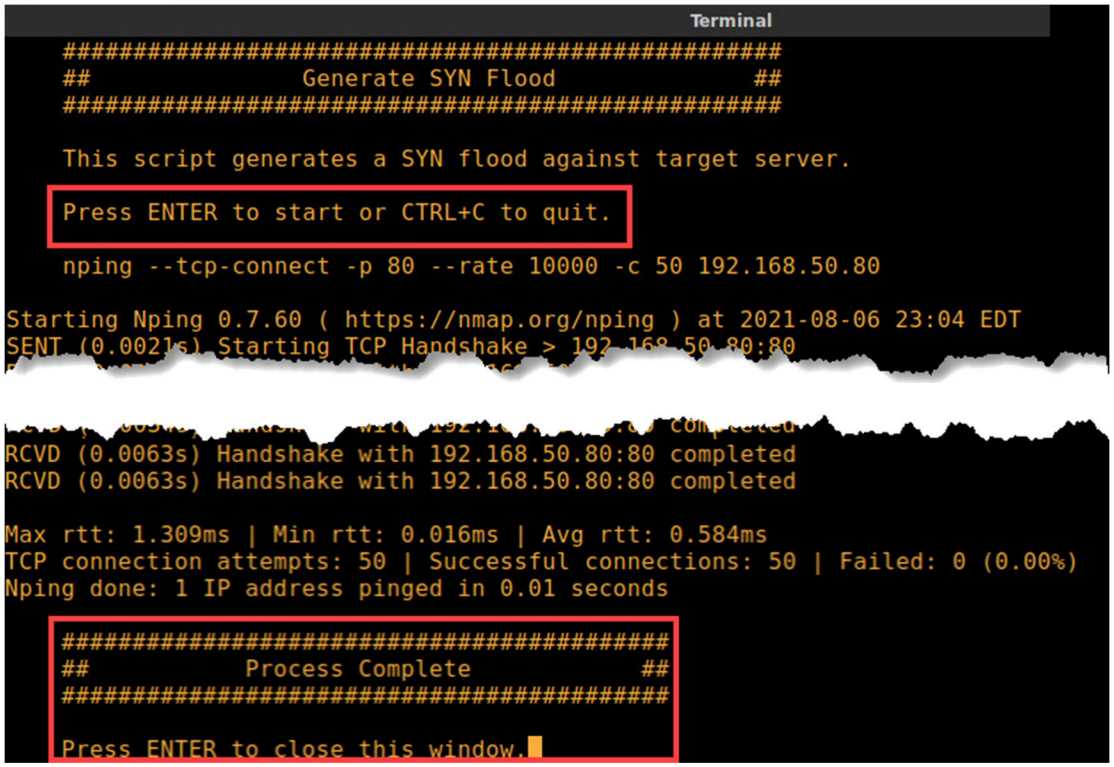
10. Double-click the icon for **SYN Flood**.



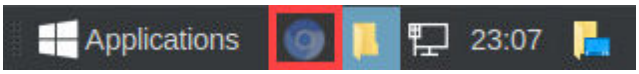
Please Note

This script uses the nmap tool to send multiple SYN packets to a server in the Extranet zone.
nping --tcp-connect -p 80 --rate 10000 -c 50 -1 192.168.50.80

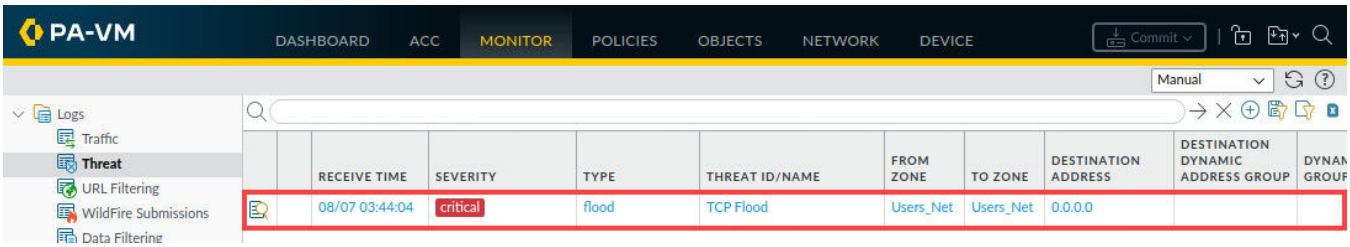
11. Press **Enter** to start the *SYN Flood* script. Allow the script to complete. Once the *SYN Flood* script completes, press **Enter**.



12. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*



13. Navigate to **Monitor > Logs > Threat**. Click the **X** icon to clear any filters. You should see entries for **TCP Flood** threat recorded in the log.



Please Note

Note that in the previous example image, the Severity column has been moved and several other default columns have been hidden. You may also find that there are certain columns that you scan frequently, and you can move those to locations by dragging and dropping to make it easier to see.

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

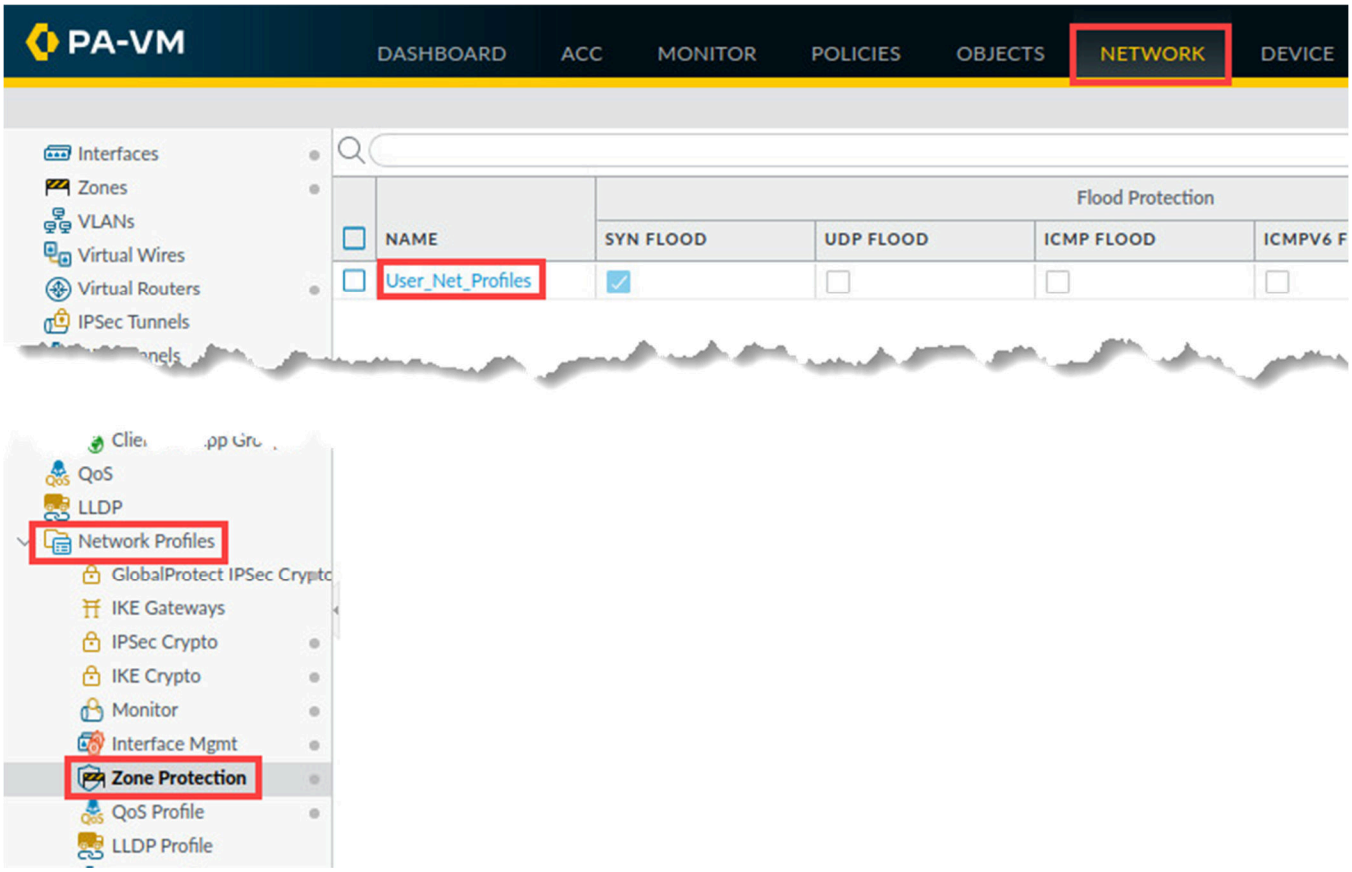
1.4 Reconnaissance Protection

In this section, you will modify the existing Zone Protection Profile to include protection against port scans and ping sweeps. An attacker often will use these techniques against hosts to determine open ports, the version of the services running on the open ports, or the host's operating system. The attacker can use this information to plan further attacks.

An attacker often will probe a host to determine its open ports, the version of the services running on the open ports, or the host's operating system. The attacker can use this information to plan attacks. Once you add reconnaissance to a zone protection profile, you will generate a reconnaissance port scan.

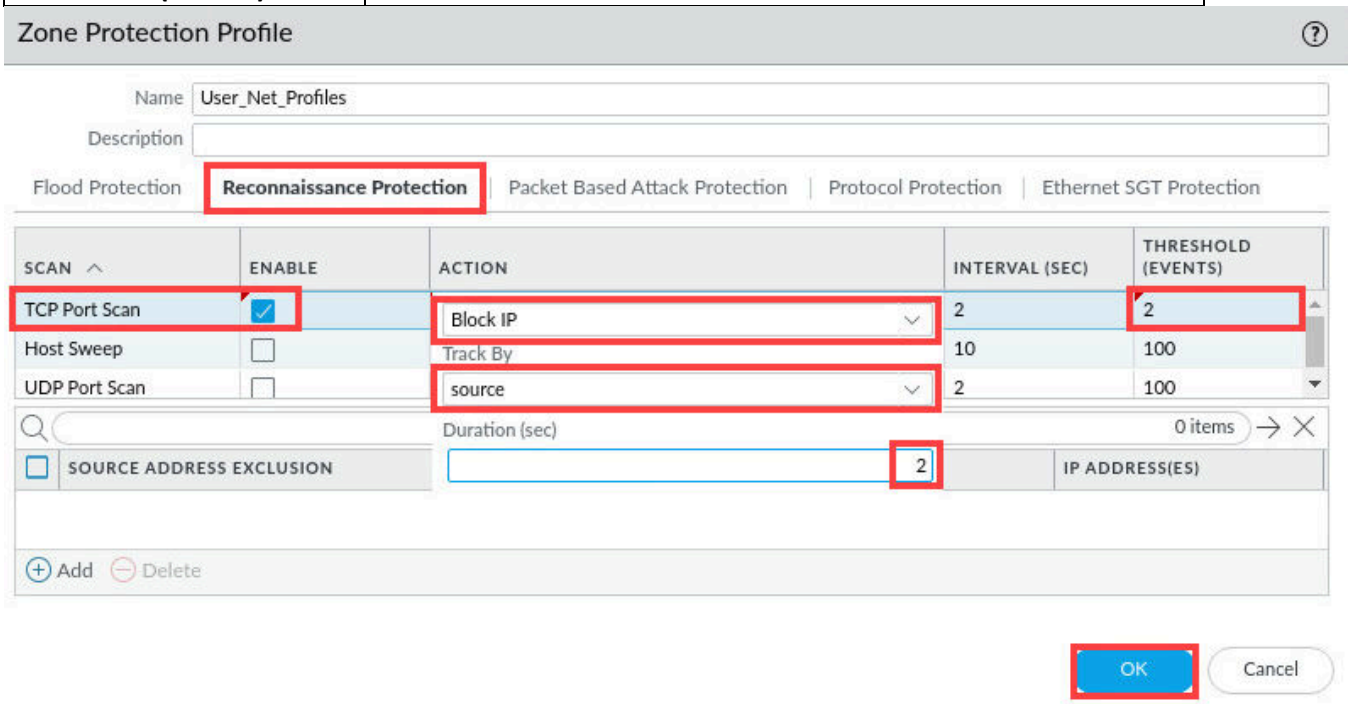
Lastly, a Zone Protection Profile can detect and block packet-based attacks, including the use of specific IP header options such as *Record Route.* An attacker sometimes can use specific IP header options to perform reconnaissance as a precursor to an attack. The firewall can be configured to detect and drop IP packets with specific header options. You will update a zone protection profile to include traceroute protection and test the zone protection profile by generating Traceroute traffic.

1. Navigate to **Network > Network Profiles > Zone Protection**. Select **User_Net_Profiles**.



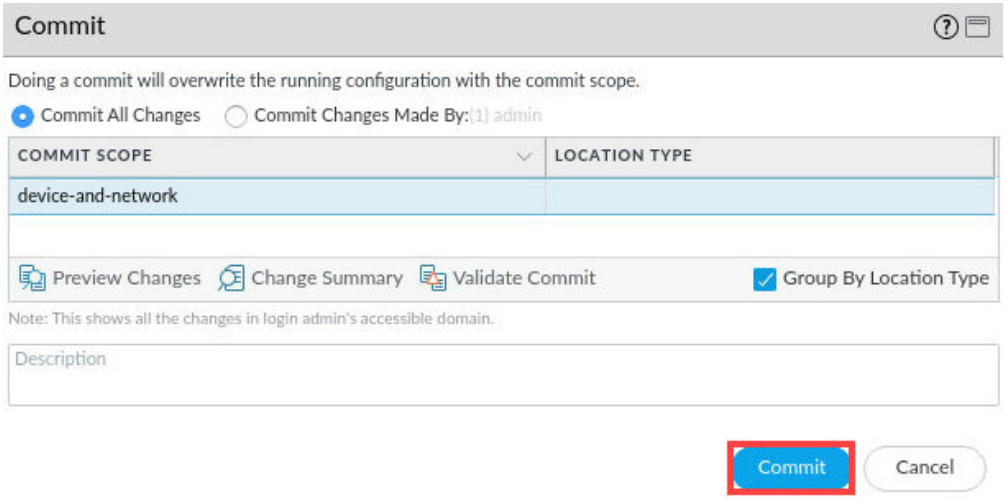
2. Select the tab for **Reconnaissance Protection.** Modify the **TCP Port Scan** with the following settings. Click **OK**.

Parameter	Value
Enable	Select **check box**
Action	Select **Block-IP** Note that when you select block-IP as the action, you will see an overlay menu that allows you to select Track By and Duration. For **Track By**, select **source** For **Duration**, type **2**
Interval (sec)	**2**
Threshold (events)	**2**

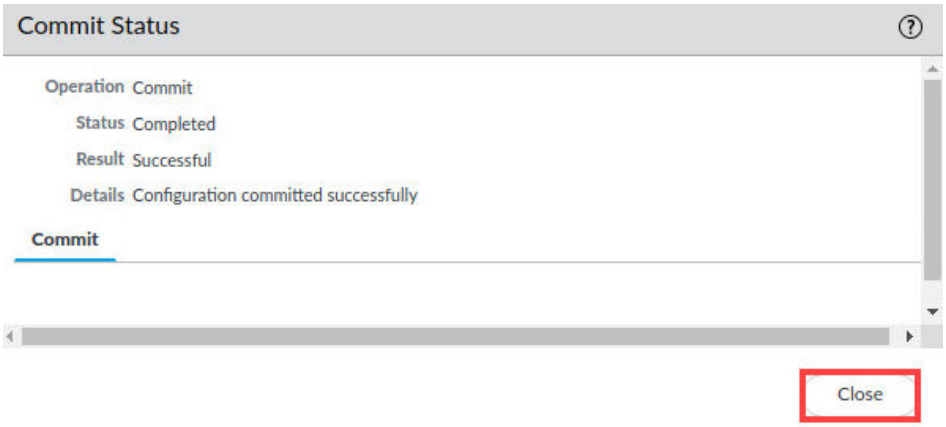


3. Click the **Commit** button at the upper-right of the web interface.

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



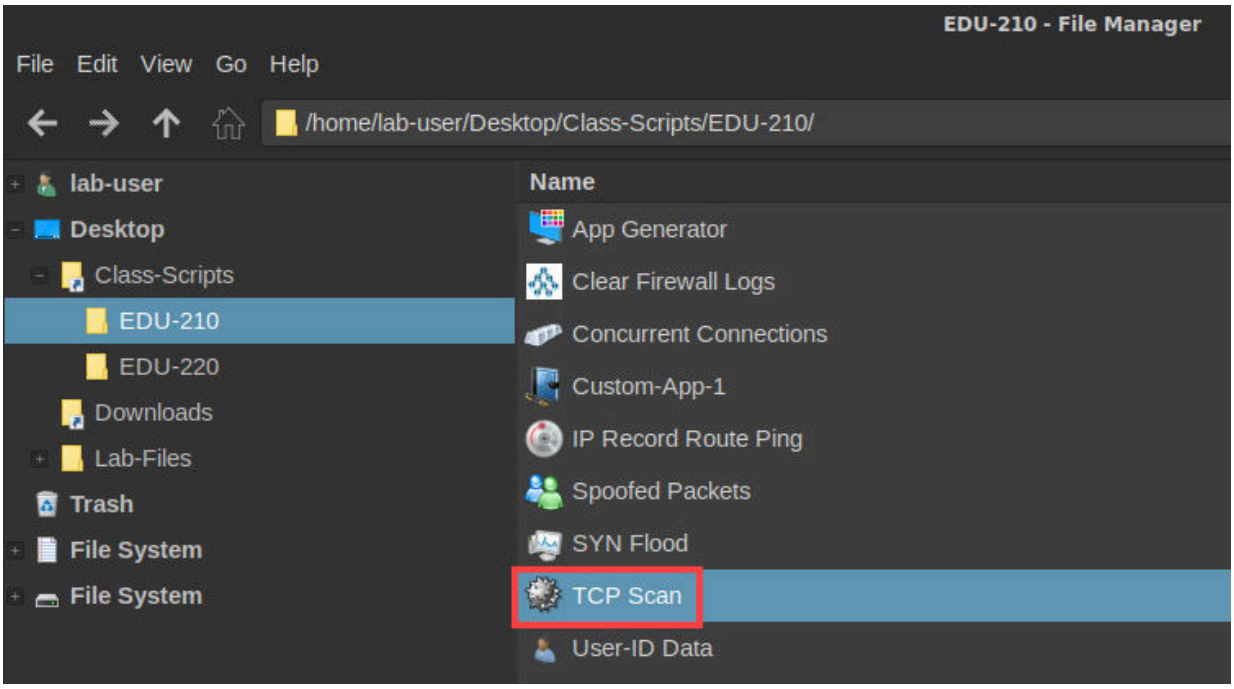
5. Wait until the *Commit* process is complete. Click **Close**.



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

7. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

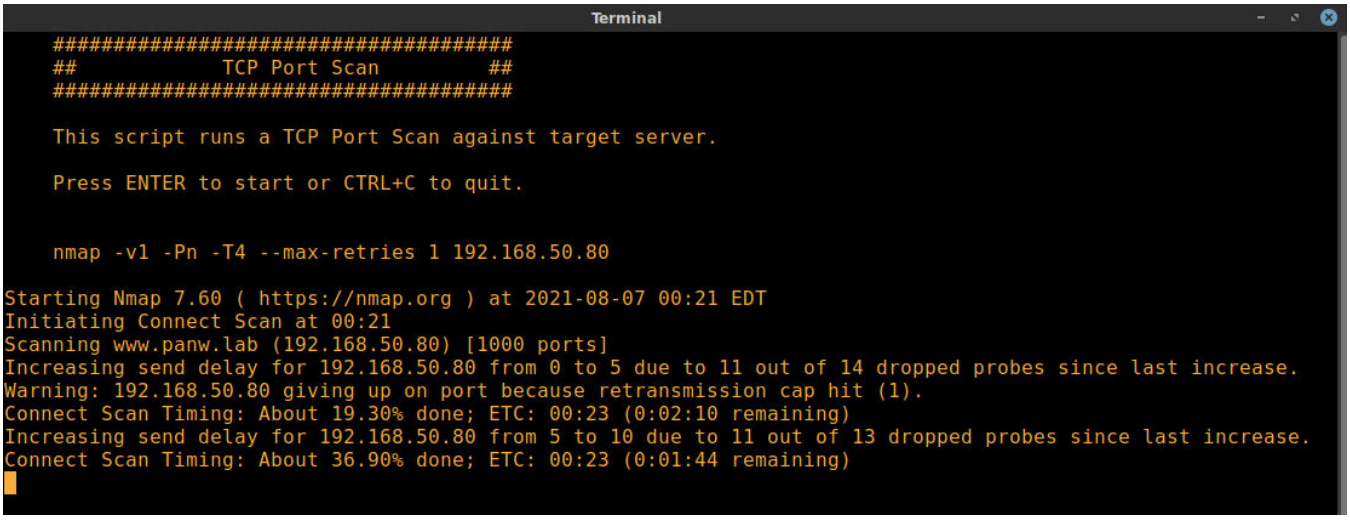
8. Double-click the icon for **TCP Scan**.



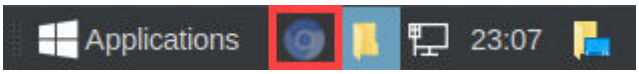
Please Note

This script runs the nmap command to scan 192.168.50.80 for open ports.
The exact syntax for the command is:
`nmap -v1 -Pn -T4 --max-retries 1 192.168.50.80`

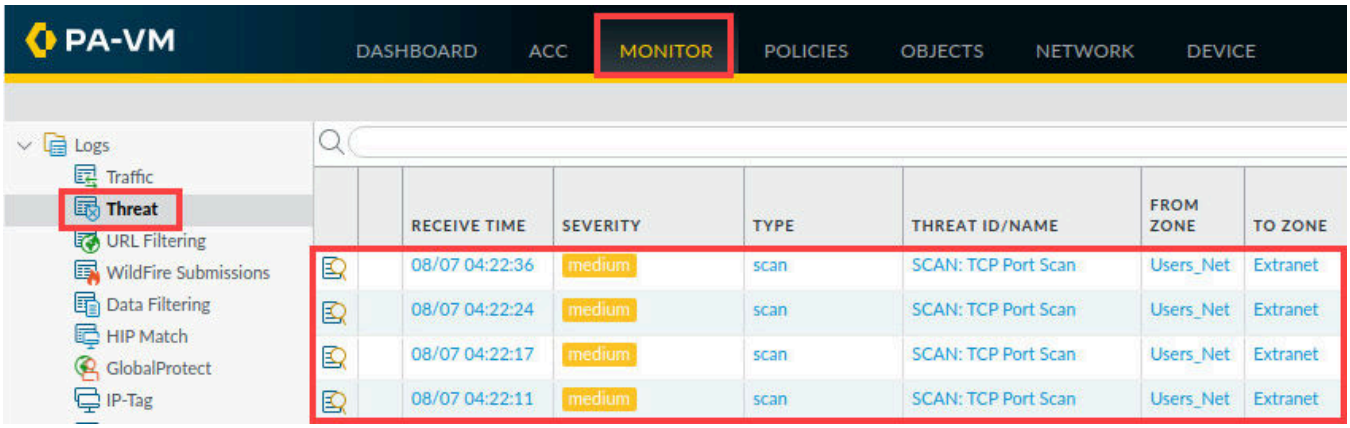
9. Press **Enter** to start the *TCP Scan*. This script runs the nmap command to scan **192.168.50.80** for open ports. After 30 seconds, use **Ctrl+C** to stop the scan script.



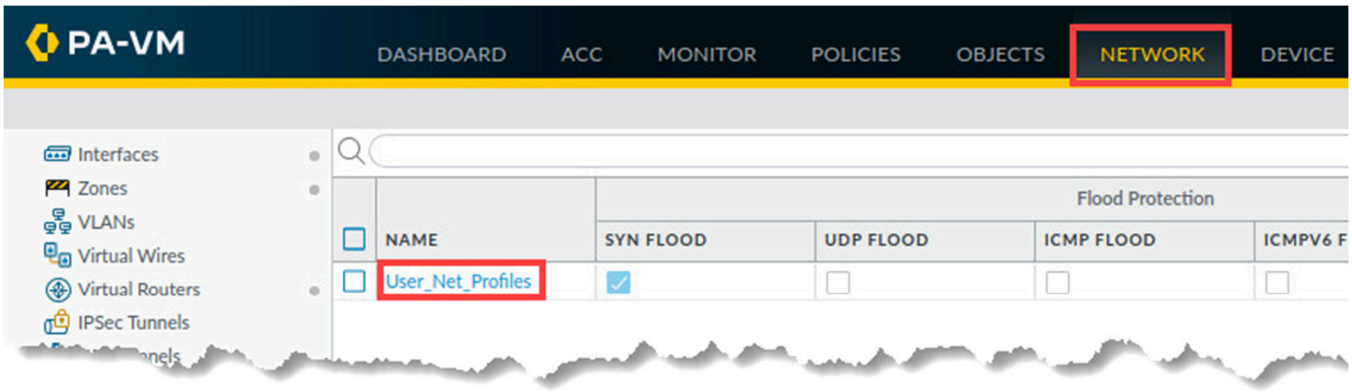
10. Open the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*

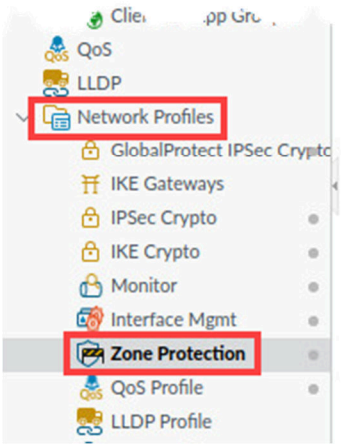


11. Select **Monitor > Logs > Threat**. You should see several **SCAN: TCP Port Scan** records populated. If you do not, wait about **30** seconds and refresh the threat logs by clicking the **Refresh** icon.

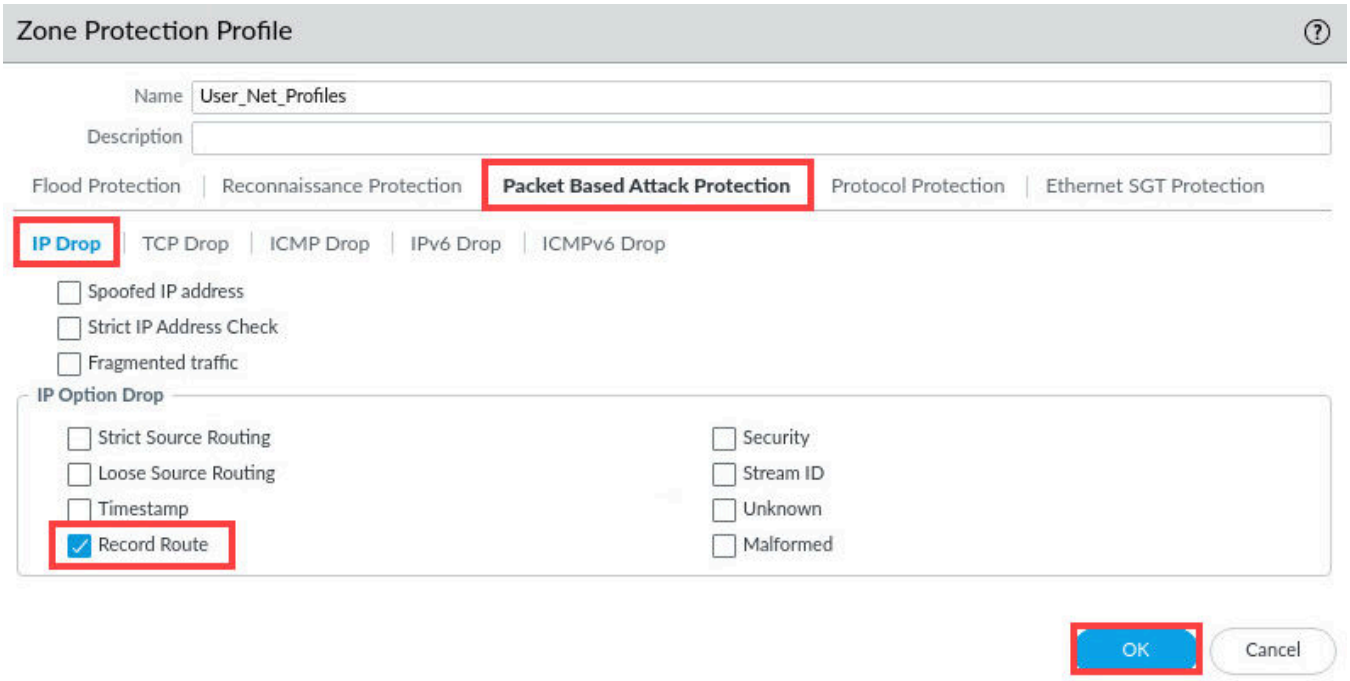


12. Select **Network > Network Profiles > Zone Protection**. Click the **User_Net_Profiles** to open the profile.



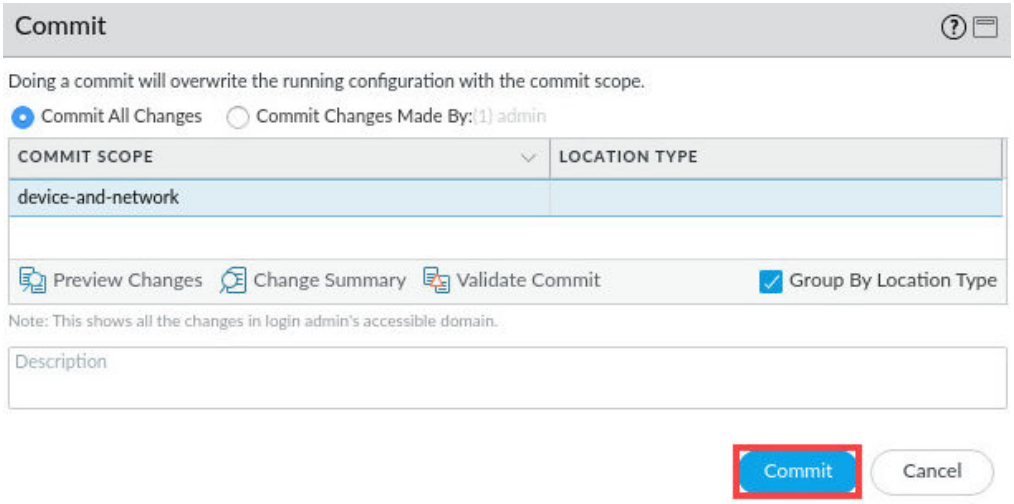


13. Click the **Packet Based Attack Protection** tab. If necessary, you may need to click the **IP Drop** tab. Select the **Record Route** option on the *IP Option Drop* panel. Click **OK**.

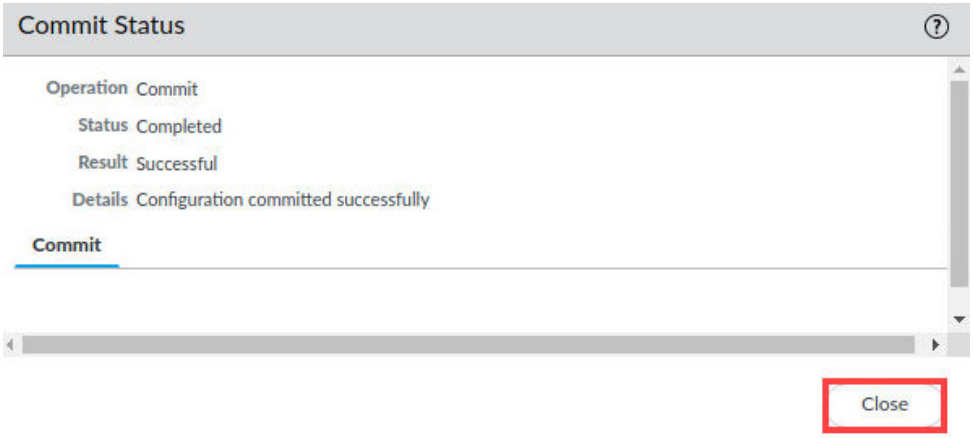


14. Click the **Commit** button at the upper-right of the web interface.

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



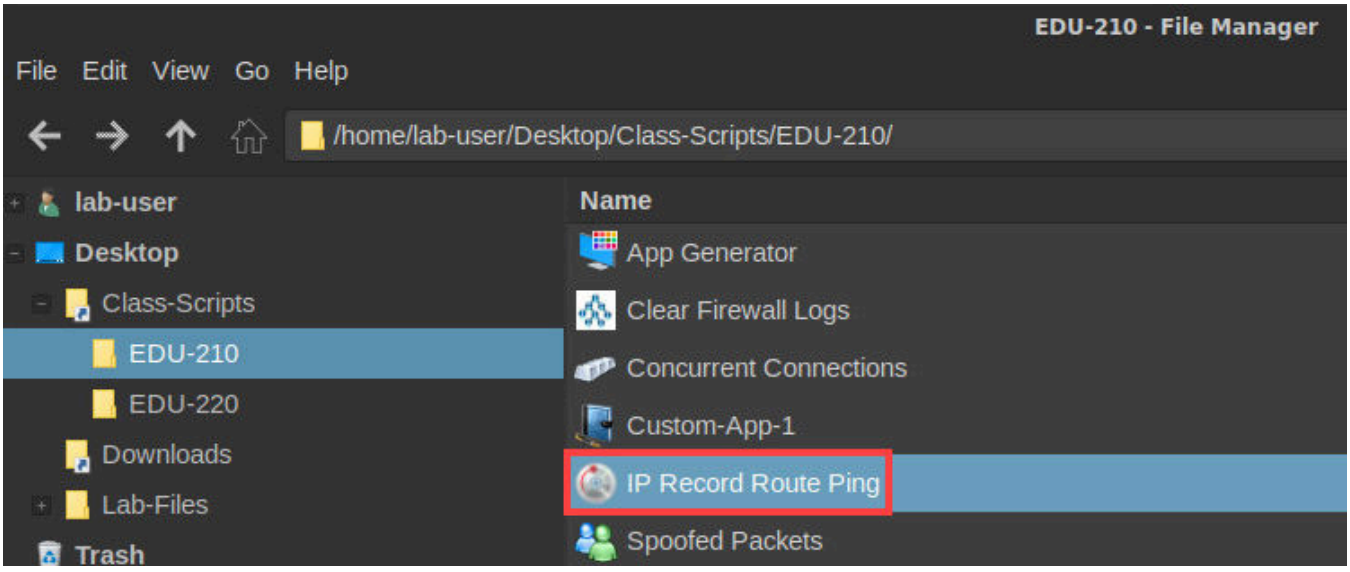
16. Wait until the *Commit* process is complete. Click **Close**.



17. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next step.

18. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

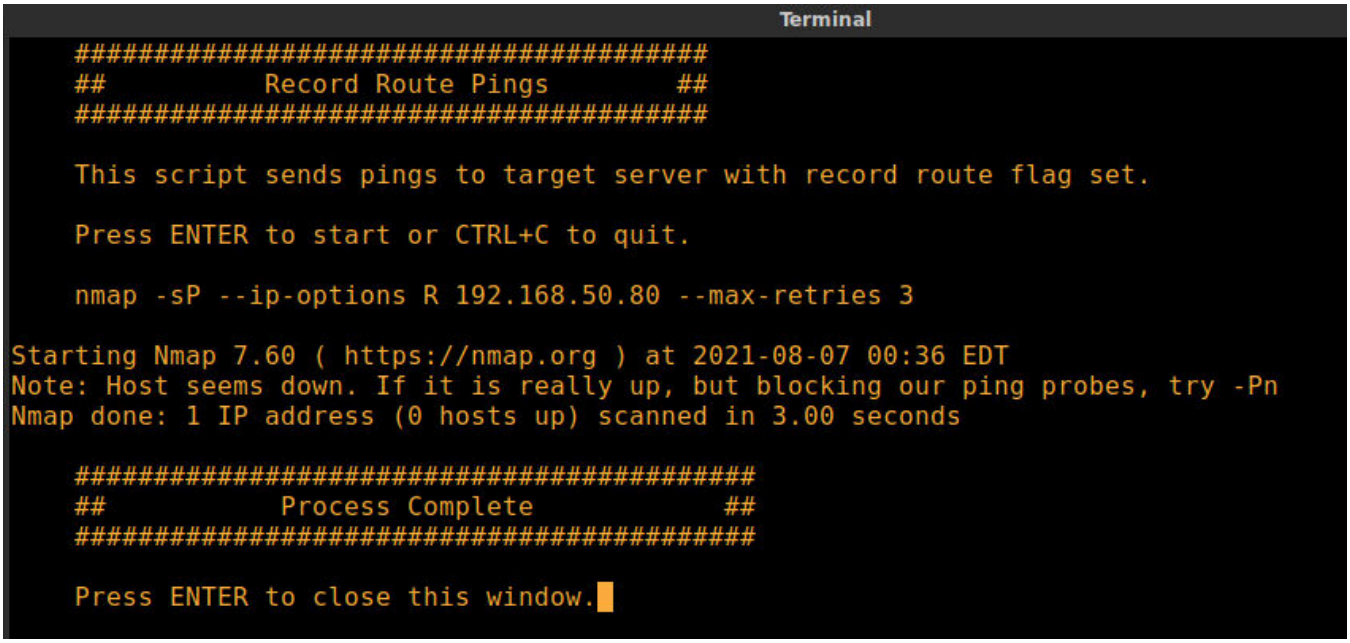
19. Double-click the icon for **IP Record Route Ping**.



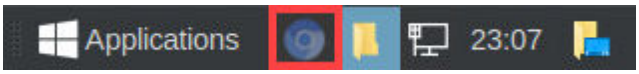
Please Note

This option in the IP header records the network path from the source host to the destination host. The Record Route option is not commonly used, and an attacker could use such information for network reconnaissance.

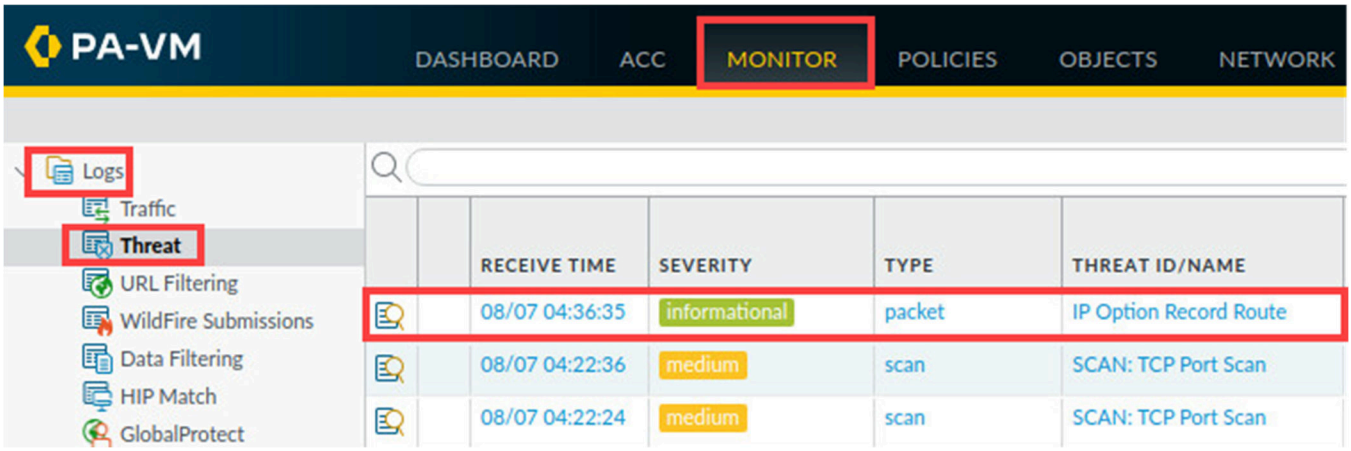
20. Press **Enter** to start the *IP Record Route Ping* script. Allow the script to complete. Once the *IP Record Route Ping* script completes, press **Enter**. The script will stall with **100%** packet loss.



21. In the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*



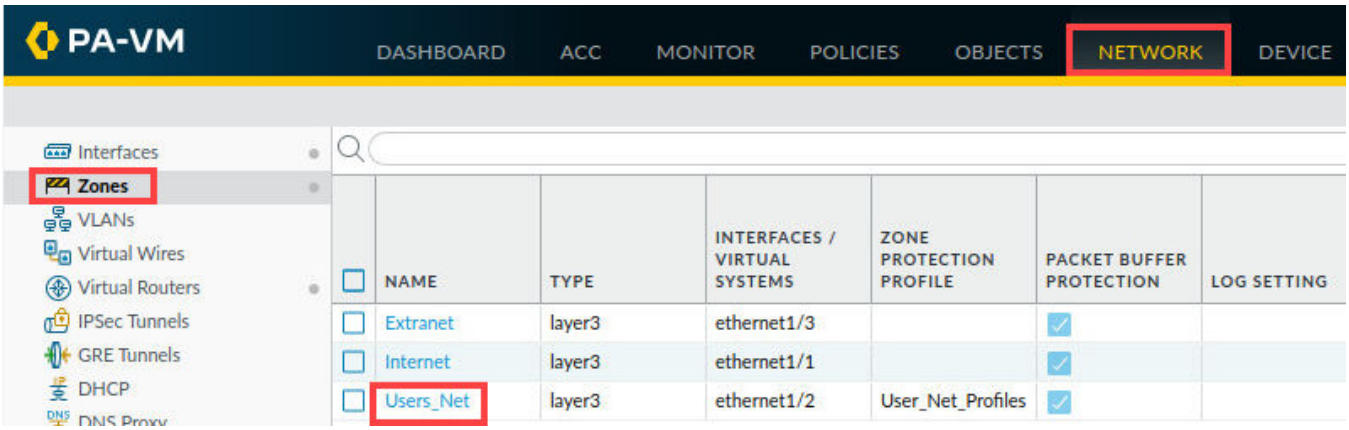
22. Select **Monitor > Logs > Threat**. You should now see an informational message with a threat named *IP Option Record Route*.



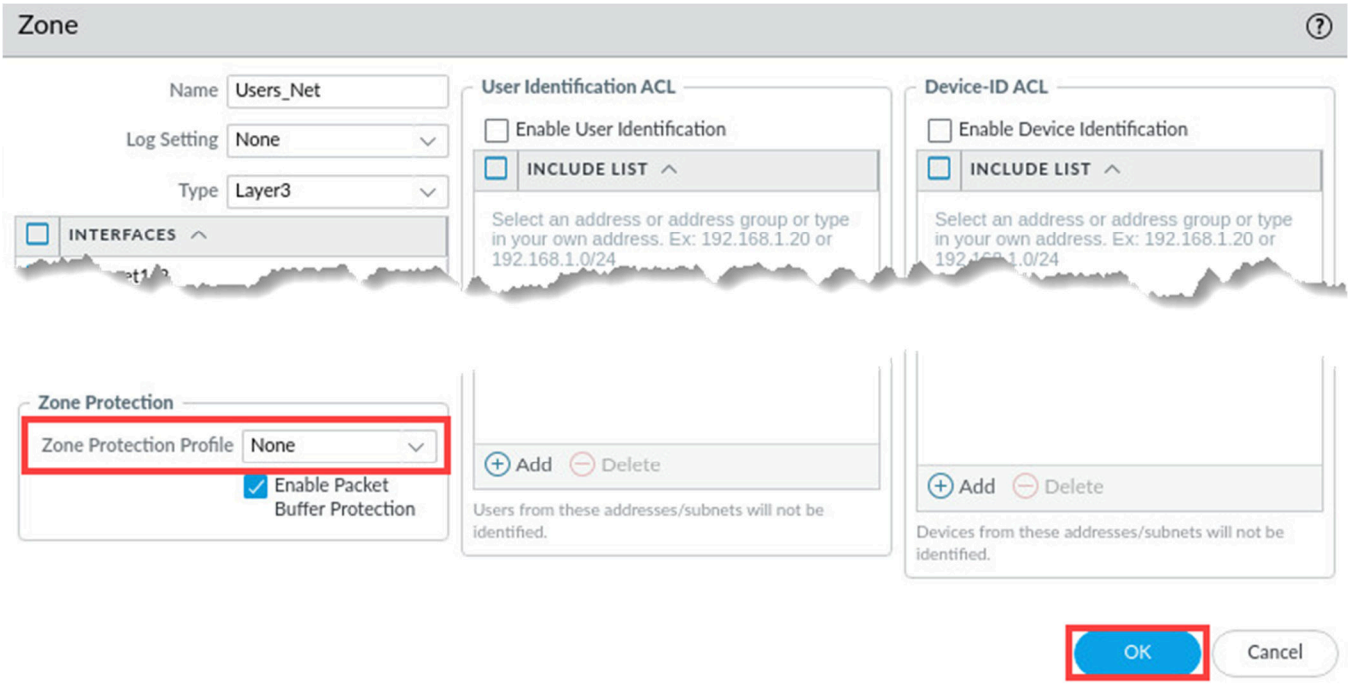
Please Note

To move forward in this lab, you will need to remove your Zone Protection Profile configuration to ensure that it does not interfere while you test a DoS Protection policy and profile

23. Select **Network > Zones**. Click **Users_Net** to edit the zone.

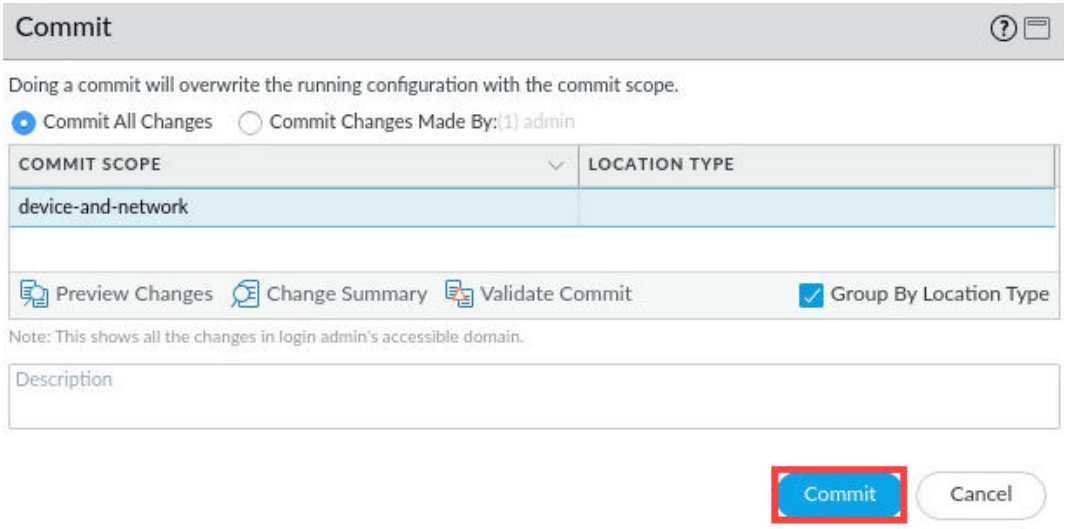


24. In the *Zone* window, select **None** for the *Zone Protection Profile*. Click **OK**.

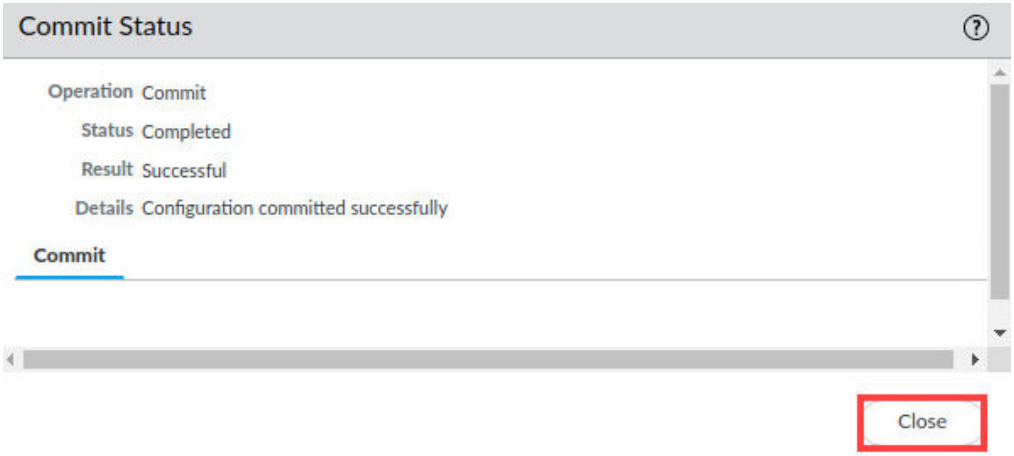


25. Click the **Commit** button at the upper-right of the web interface.

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



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



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

1.5 Concurrent Sessions on a Target Host and DoS Protection

In this section, you will run a script that uses **nmap** to open multiple concurrent sessions from the client host in the Users_Net zone to a target server in the Extranet zone. The script will test whether the firewall will allow 10 concurrent sessions to the target host. You will monitor the results using the Traffic and Threat logs.

A DoS Protection policy and profile can detect when the number of concurrent sessions to a host has exceeded a specified limit. You will configure a maximum concurrent session limit for a host in the Extranet zone.

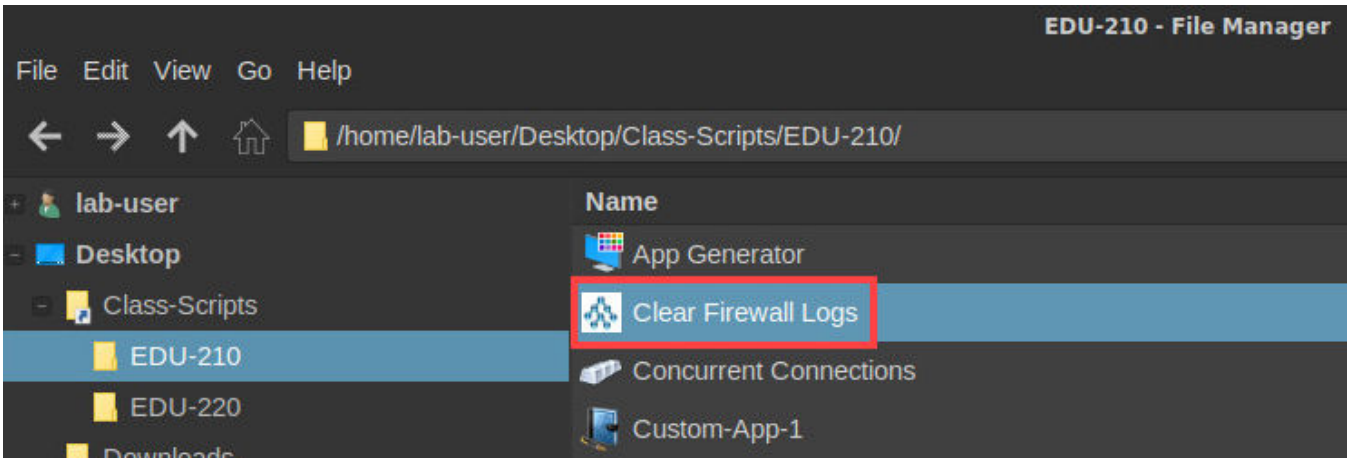
You will use the **Concurrent Connections** script again to generate multiple concurrent sessions to the Linux host in the dmz zone. The host is protected by a DoS Protection policy rule and profile that should drop any connection requests that exceed the configured maximum number of nine concurrent sessions to the Linux host.

A DoS Protection Profile can detect and block flood attacks to a zone, to a subset of hosts in a zone, or to a specific host in a zone. You will configure flood protection in both a Zone Protection Profile and a DoS Protection Profile so that you can see how they interact. You will configure a higher TCP SYN flood protection threshold in a Zone Protection Profile and a lower TCP SYN flood protection threshold in the DoS Protection Profile.

Lastly, you will use the **Concurrent Connections** script to generate multiple concurrent sessions to the target server in the Extranet zone. The host is protected by both a Zone Protection Profile and a DoS Protection Profile that should drop any connection requests that exceed the lowest configured flood threshold settings. The lower DoS Protection Profile thresholds should be reached first.

1. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

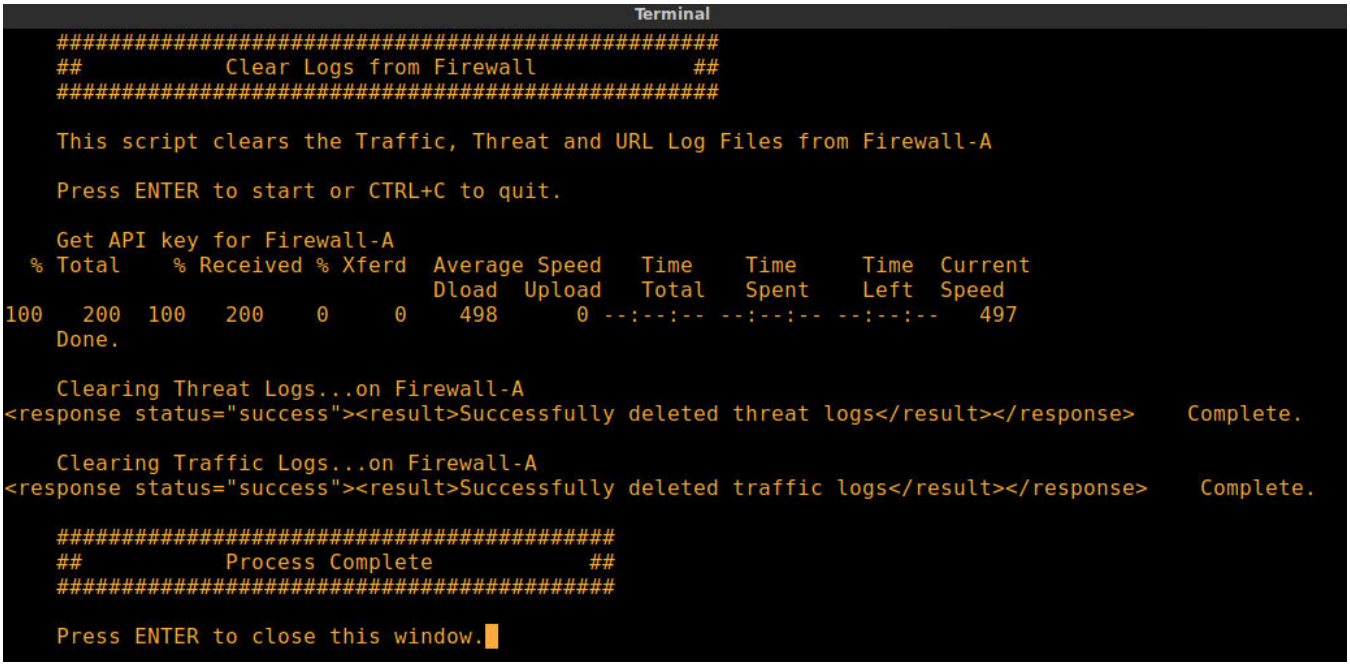
2. Double-click the icon for **Clear Firewall Logs**.



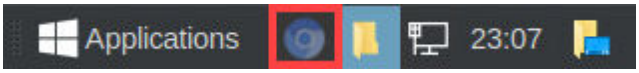
Please Note

This script uses the XML API to clear the Threat, Traffic and URL Filtering log files. We are clearing the log files to make it easier to identify traffic and threats blocked by DoS Protection.

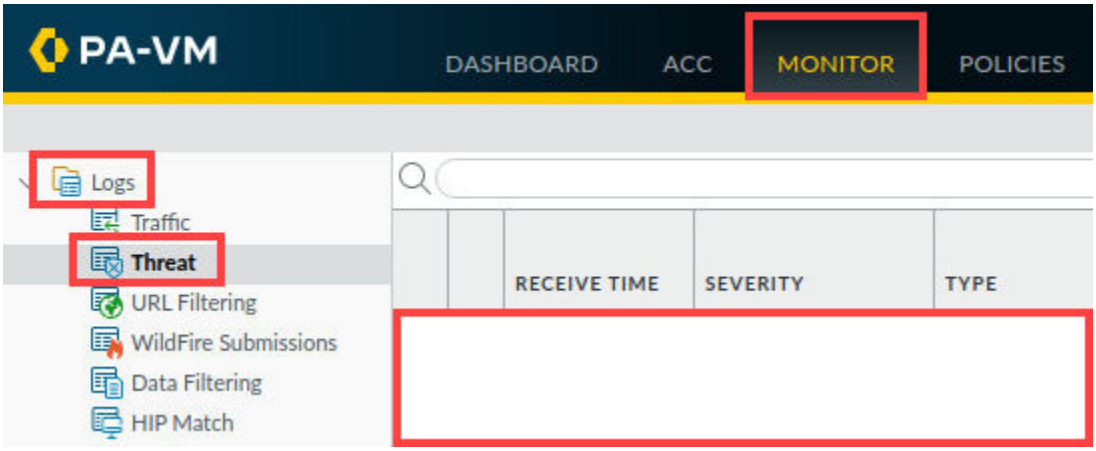
3. Press **Enter** to start the *Clear Firewall Logs* script. Allow the script to complete. Once the *Clear Firewall Logs* script completes, press **Enter**.



4. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop*.



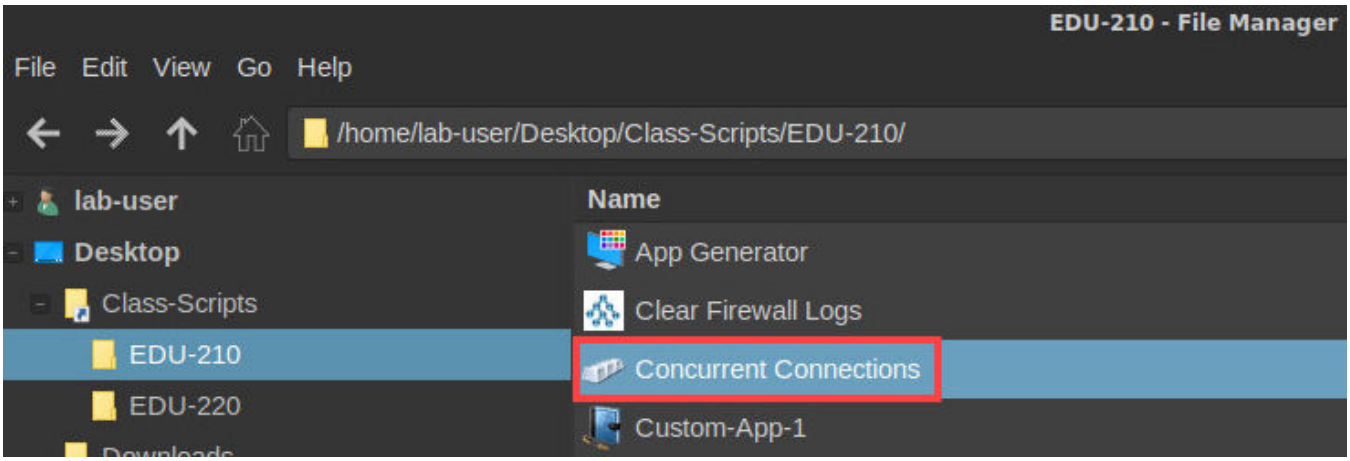
5. Navigate to **Monitor > Logs > Threat** and verify the logs have been cleared.



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

7. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.

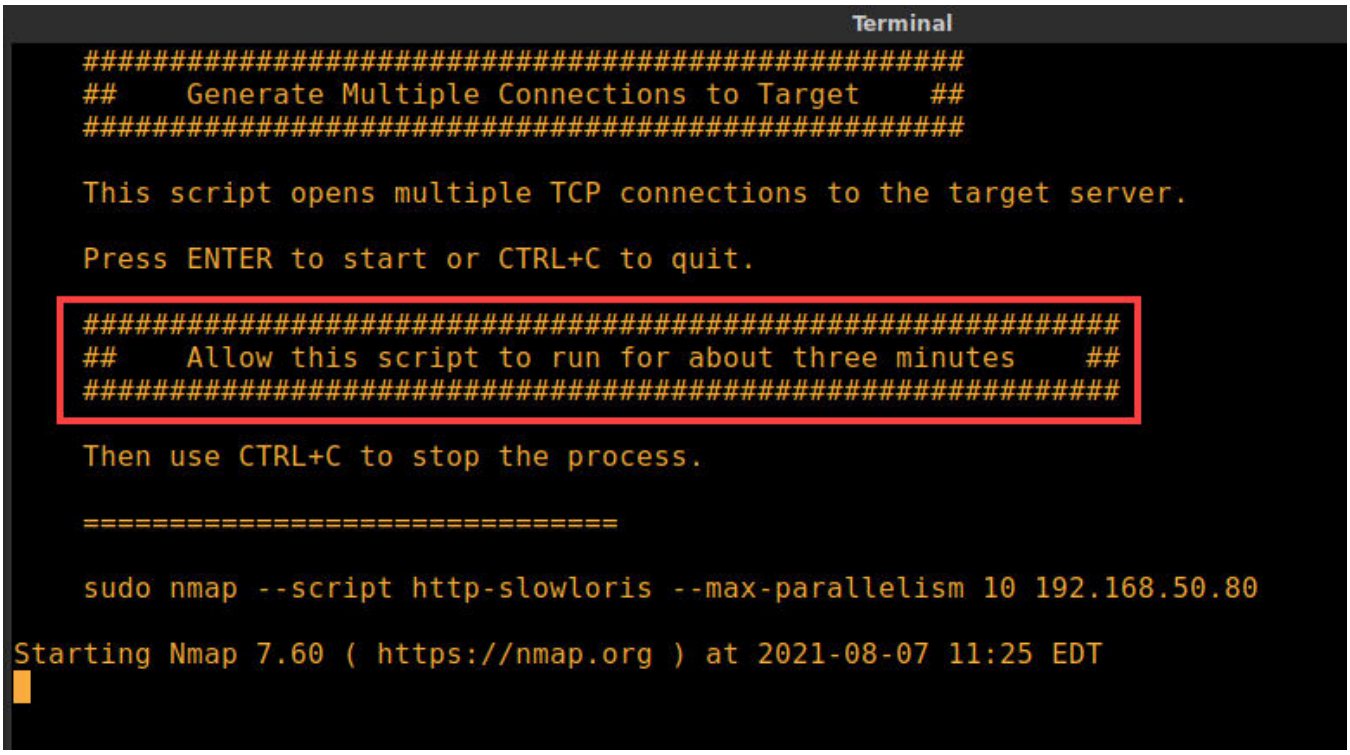
8. Double-click the icon for **Concurrent Connections**.



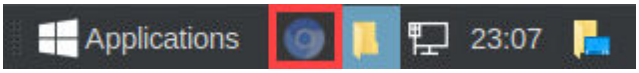
Please Note

The exact syntax for this command is:
nmap --script http-slowloris --max-parallelism 10 192.168.50.80

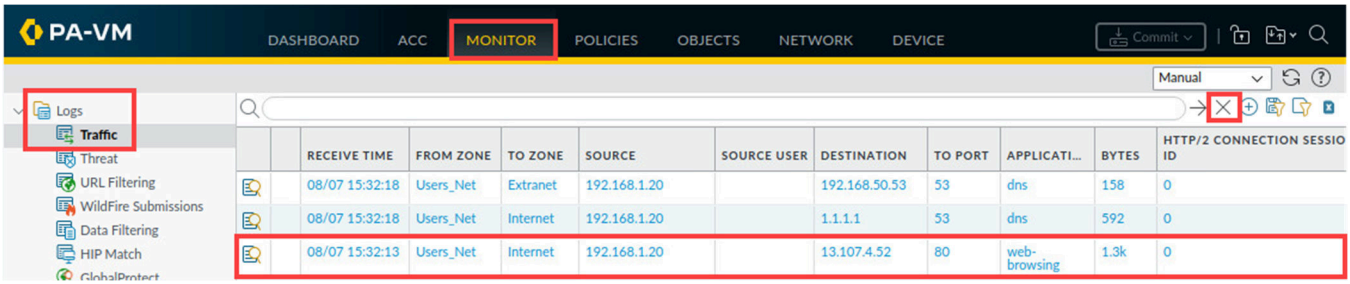
9. Press **Enter** to start the *Concurrent Connections* script. The command can take 30 minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least 3 minutes and then press **Ctrl+C** to stop command execution**.**



10. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the client desktop.



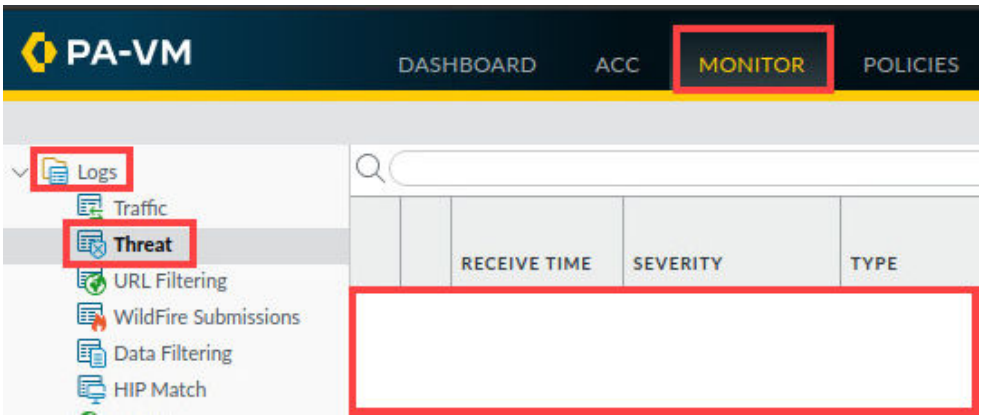
11. Select **Monitor >Logs > Traffic**. Clear any filters you have in place by clicking the **Clear Filter** button.



Please Note

As the command execution progressed, you should see multiple web-browsing log entries for traffic to multiple ports, but especially to port 80 and 443. The traffic was not blocked by any Security Profiles or Security policy rules.

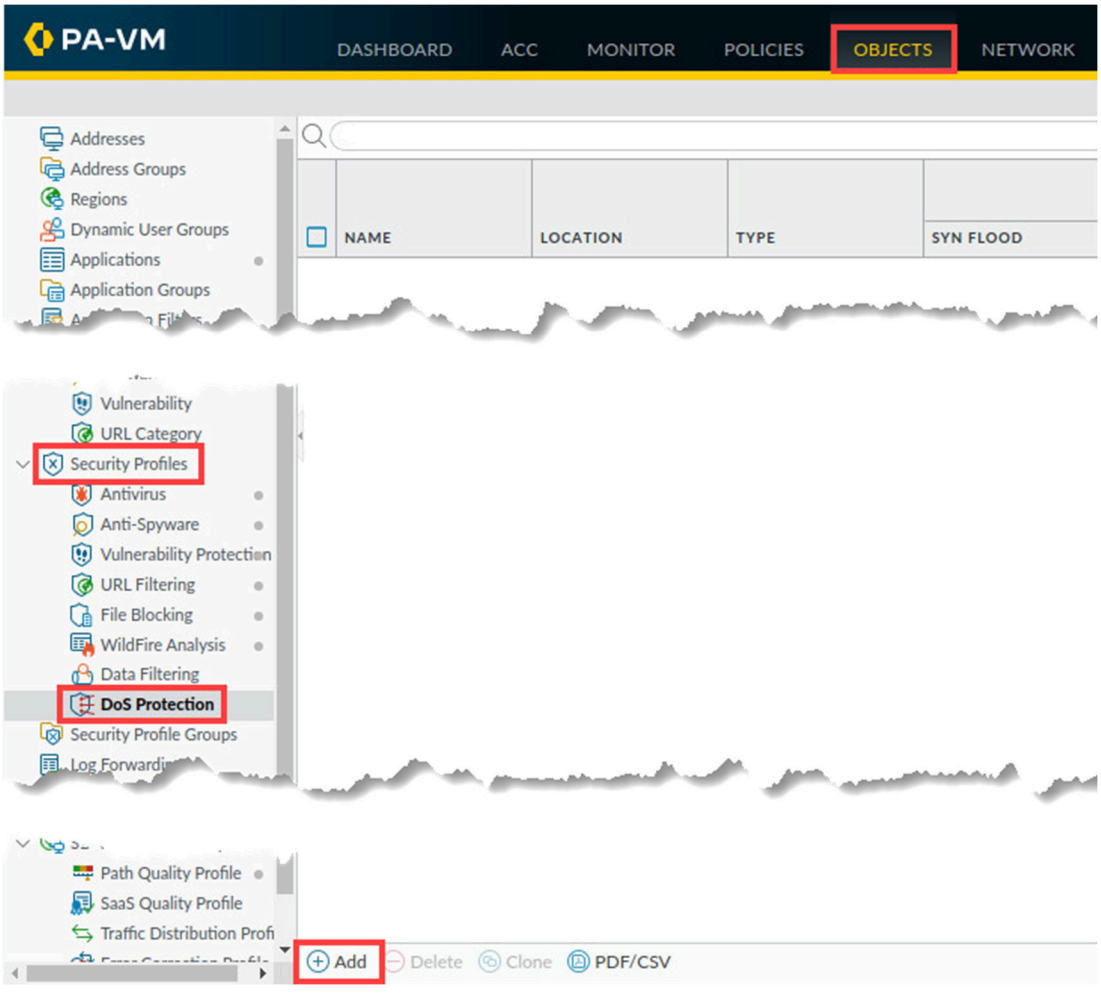
12. Navigate to **Monitor > Logs > Threat**. Notice there are no logs present.



Please Note

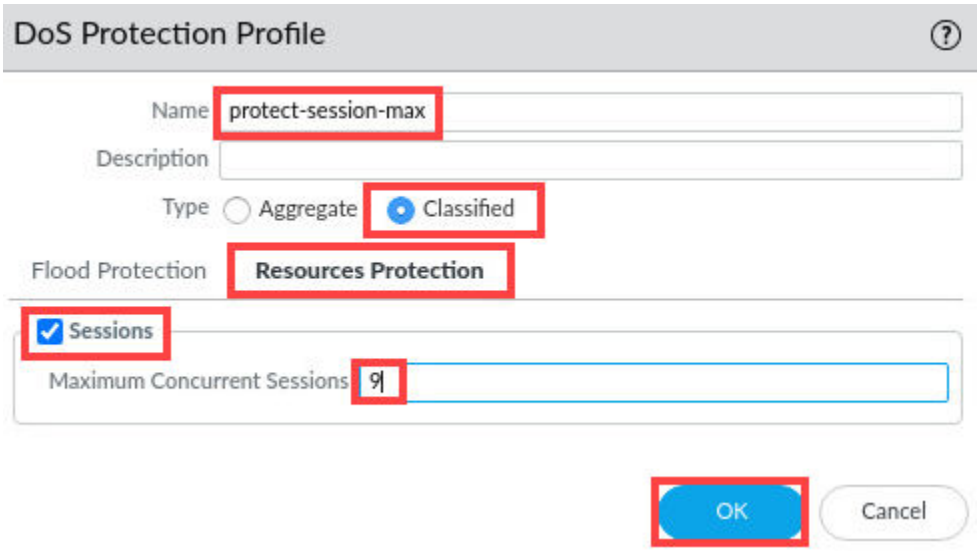
There should be *no* Threat log entries because nothing has been configured to monitor traffic for the number of concurrent sessions to a specific target host

13. Configure maximum concurrent sessions with DoS protection by selecting **Objects > Security Profiles > DoS Protection**. Click **Add** in the lower-left of the window.

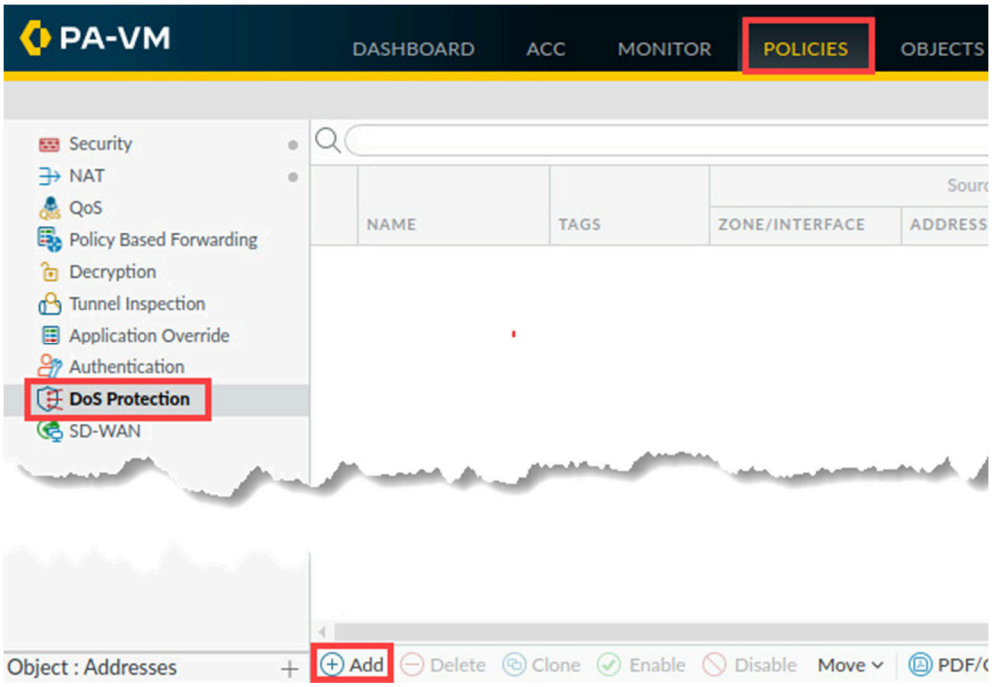


14. In the *DoS Protection Profile* window, configure the following. Click **OK**.

Parameter	Value
Name	**protect-session-max**
Classified	Select it
Resources Protection tab	Click it
Sessions	Select **check box**
Maximum Concurrent Sessions	**9**

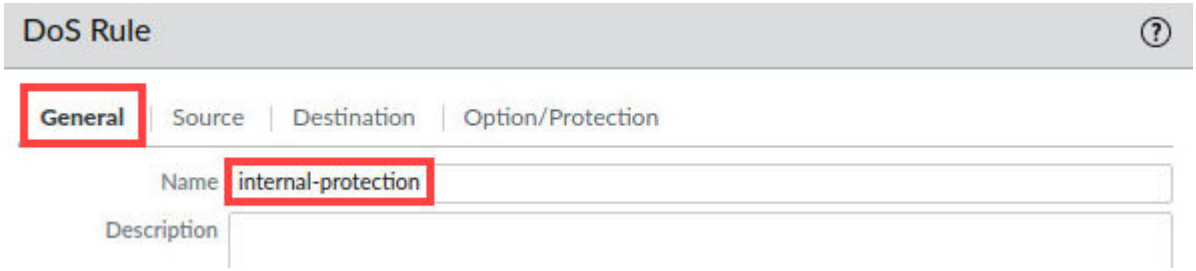


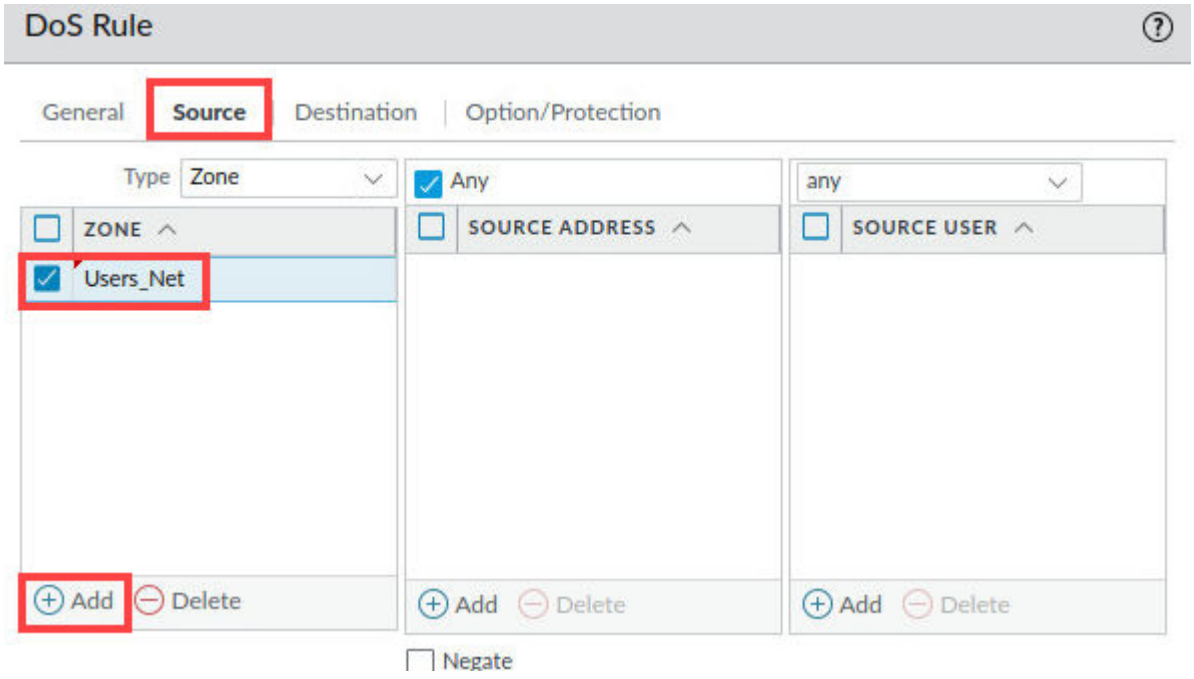
15. Navigate to **Polices > DoS Protection**. Click **Add**.

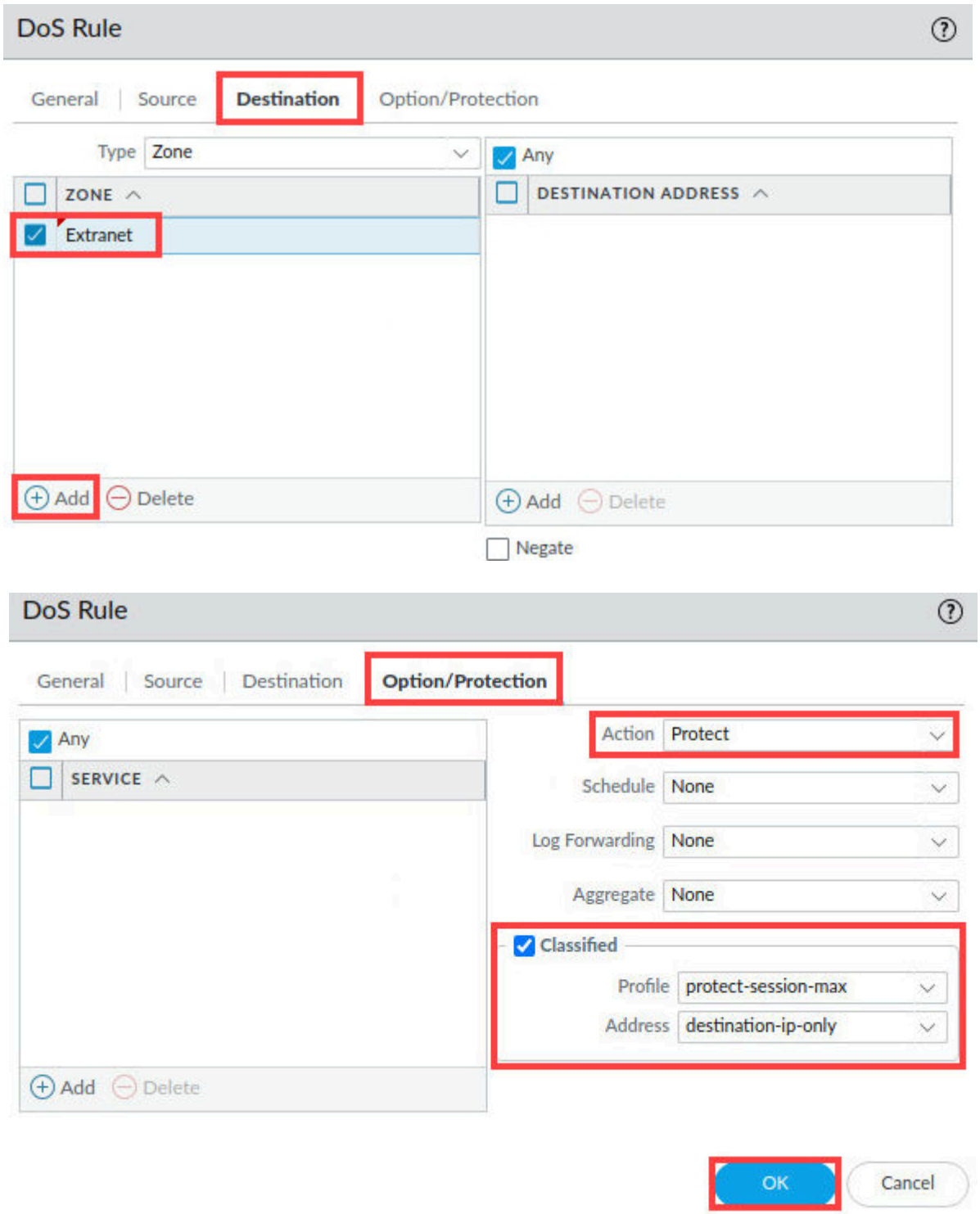


16. In the *DoS Rule* window, configure the following. Click **OK**.

Parameter	Value
General tab	Click it, if necessary
Name	**`internal-protection`**
Source tab	Click it
Zone	Select **Users_Net**
Destination tab	Click it
Zone	Select **Extranet**
Option/Protection tab	Click it
Action	Select **Protect**
Classified	Select **check box**
Profile	Select **protect-session-max**
Address	Select **destination-ip-only**





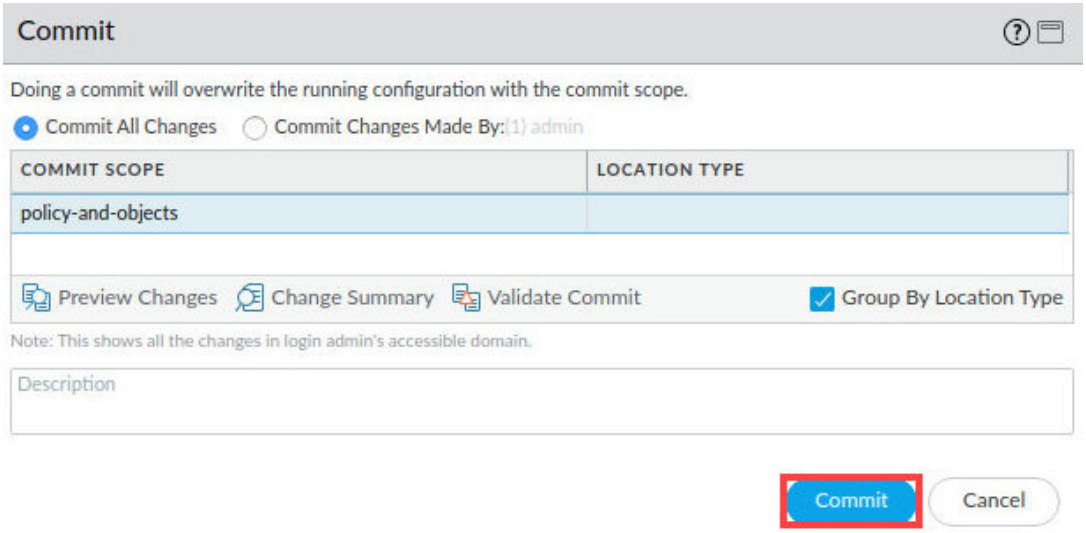


17. Verify the *internal-protection* rule is present in the DoS Protection policies.

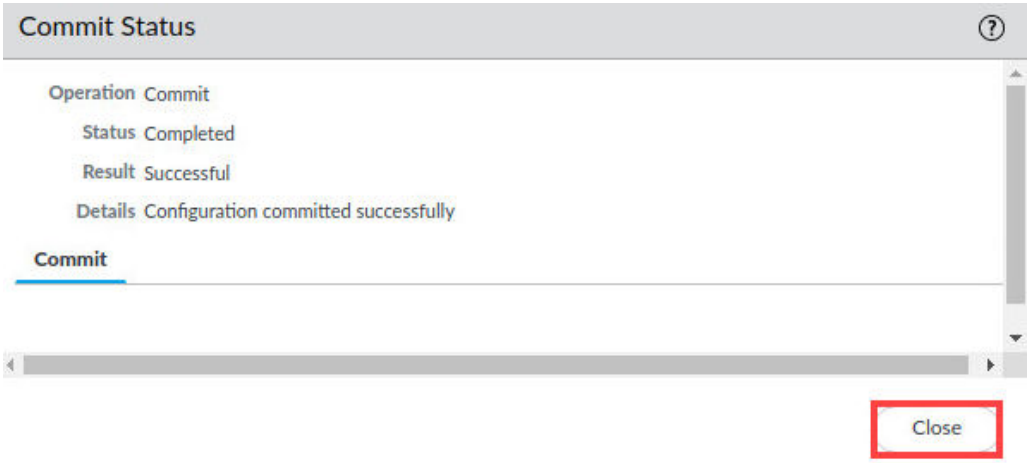
	NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection	
			ZONE/INTERFA...	ADDRESS	USER	ZONE/INTERFA...	ADDRESS			AGGREGATE	CLASSIFIED
1	internal-protection	none	Users_Net	any	any	Extranet	any	any	protect	none	profile: protect-session-max destination-ip-only

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

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

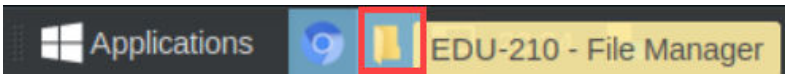


20. Wait until the *Commit* process is complete. Click **Close**.

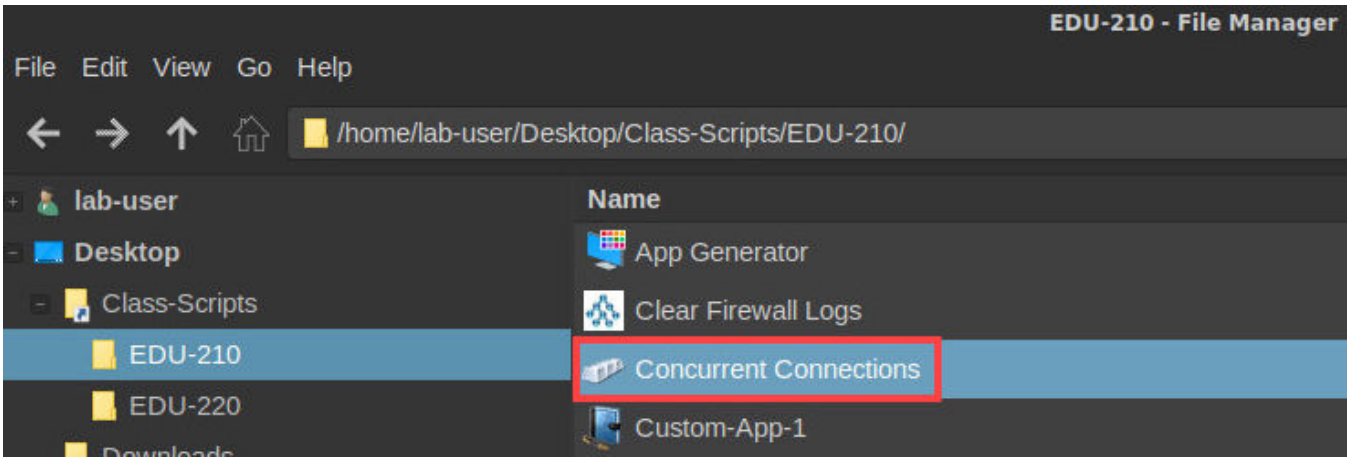


21. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

22. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.



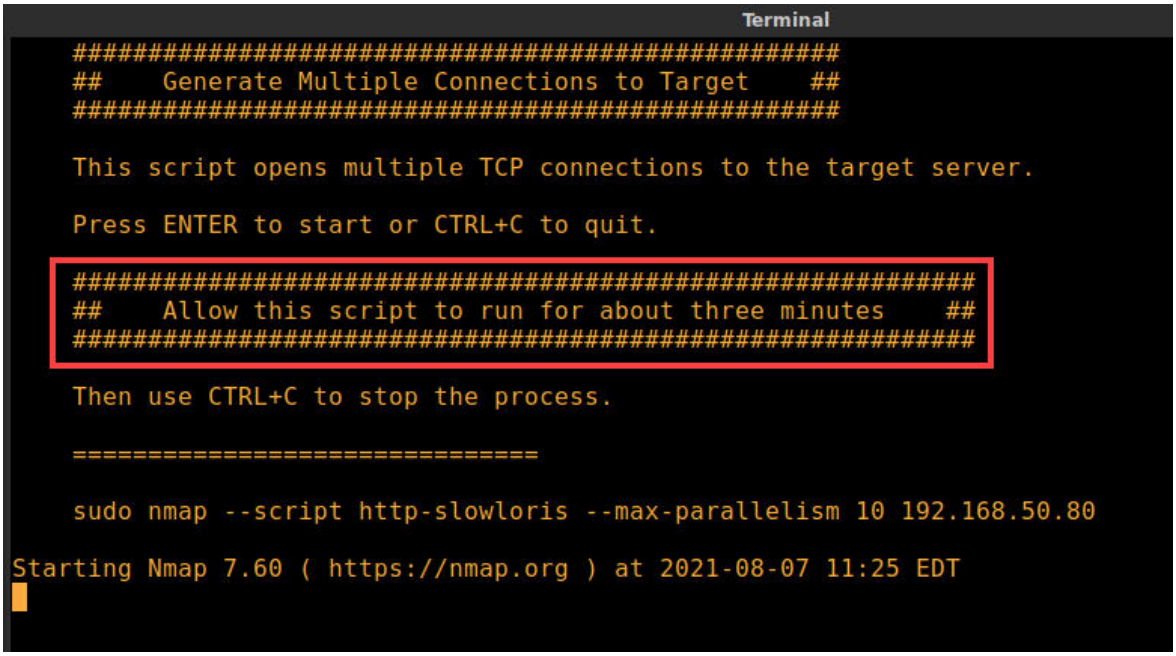
23. Double-click the icon for **Concurrent Connections**.



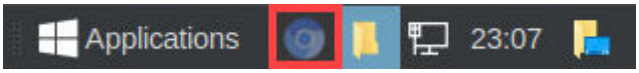
Please Note

The exact syntax for this command is:
nmap --script http-slowloris --max-parallelism 10 192.168.50.80

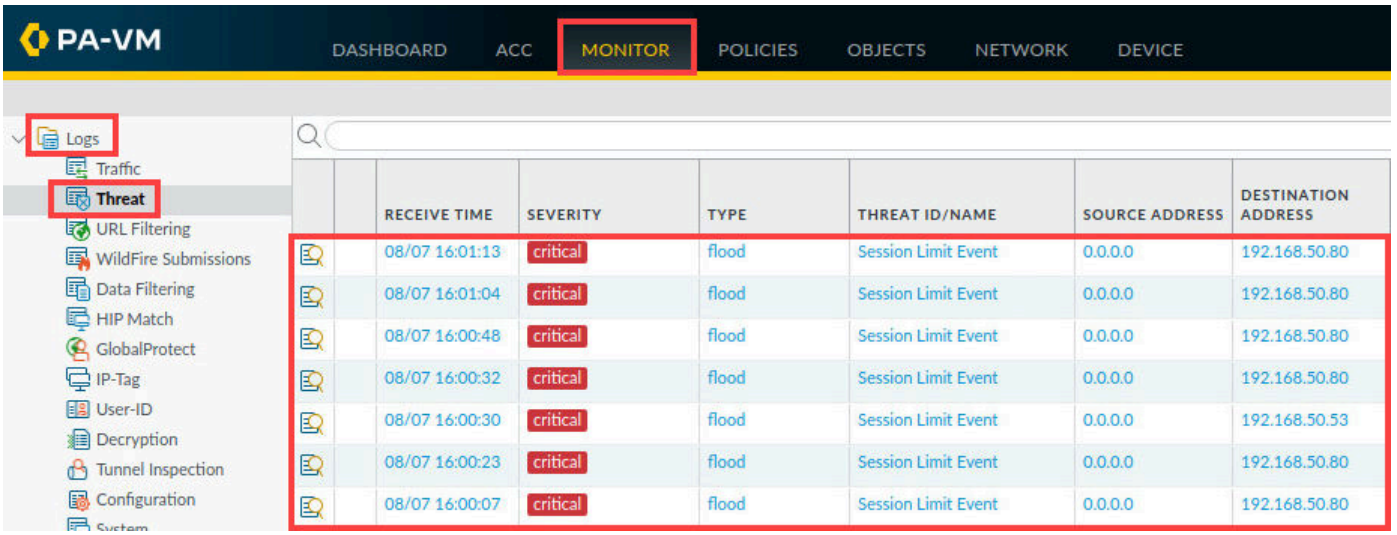
24. Press **Enter** to start the *Concurrent Connections* script. The command can take *30* minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least *3* minutes and then press **Ctrl+C** to stop command execution**.**



25. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*



26. Navigate to **Monitor > Logs > Threat**. Notice the new *Threats*.

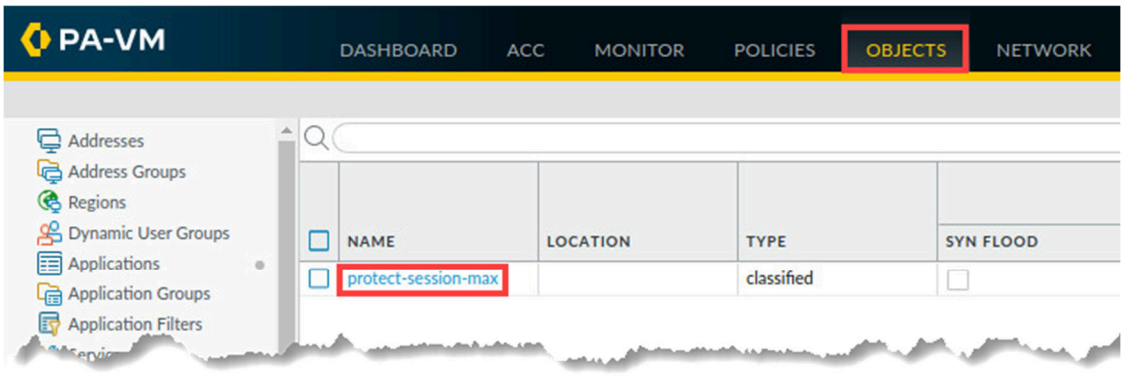


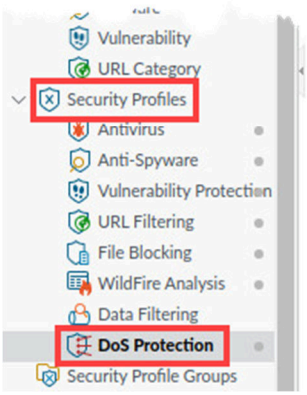
Please Note

Several columns have been hidden in this example.

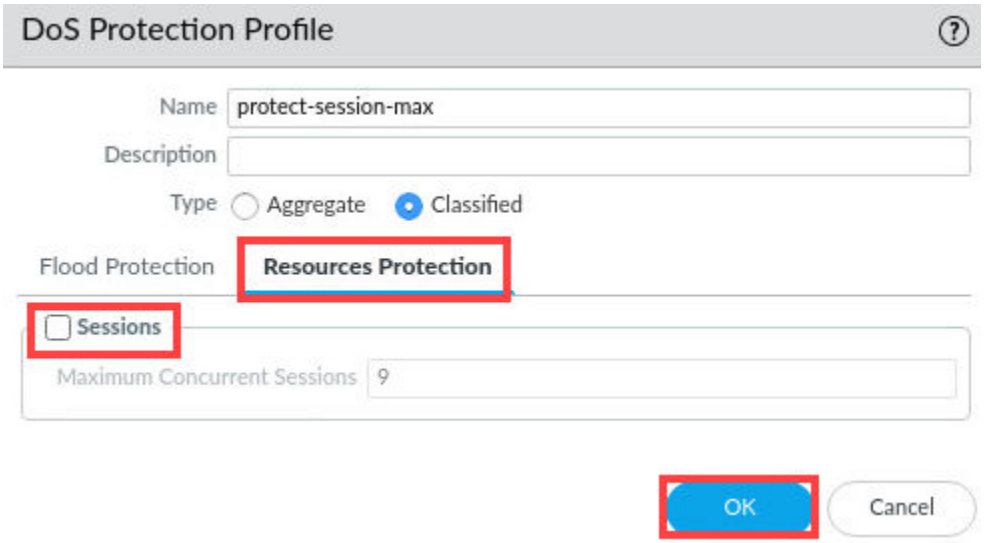
You should see **Session Limit Event** entries in the Threat log because the number of concurrent connection requests to the protected host has exceeded the configured session maximum limit.

27. Navigate to **Objects > Security Profiles > DoS Protection**. Click **protect-session-max** to edit the profile.

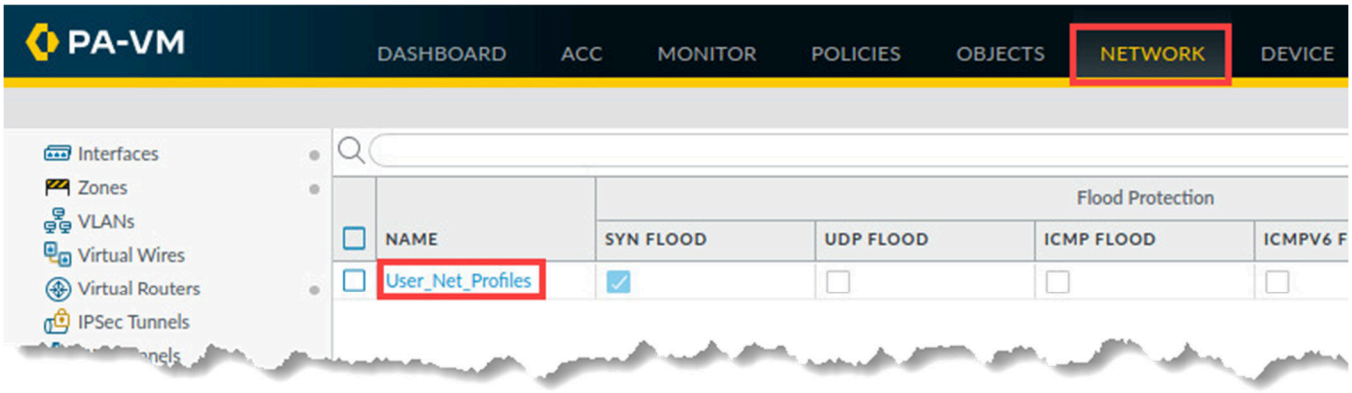


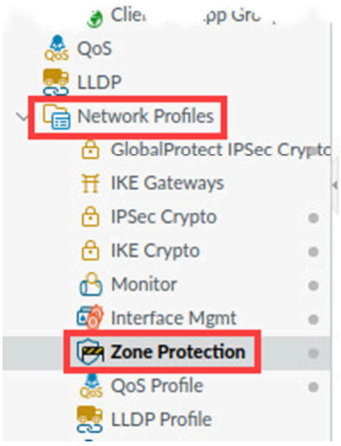


28. In the *DoS Protection Profile* window, click the **Resources Protection** tab. **Deselect** *Sessions*. Click **OK**.



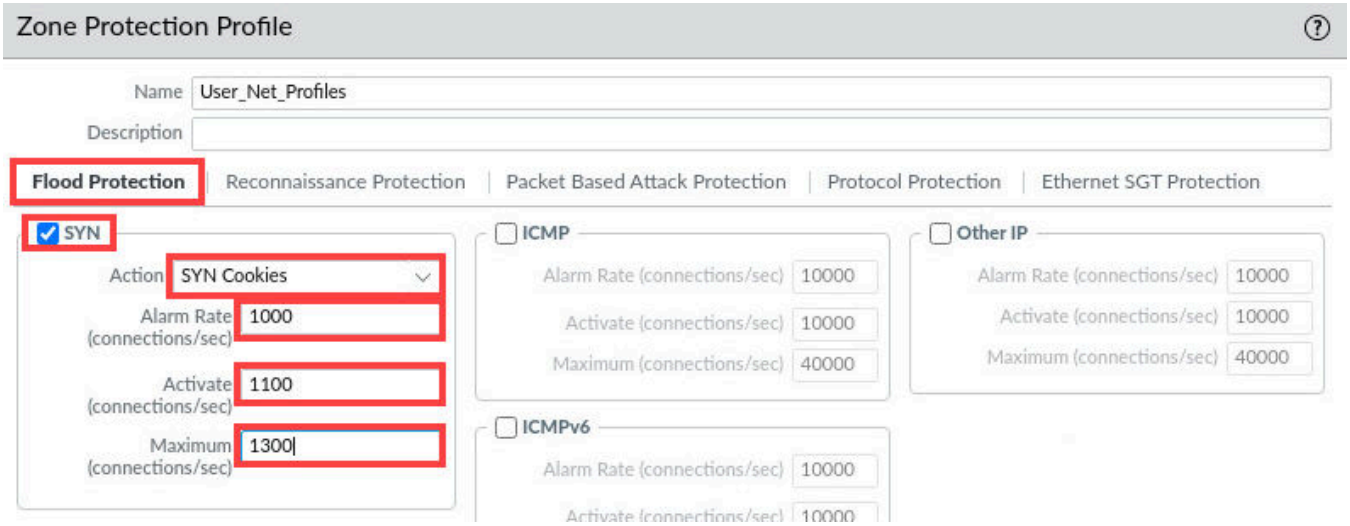
29. Navigate to **Network > Network Profiles > Zone Protection**. Click **User_Net_Profile**.





30. On the *Flood Protection* tab, configure the following.

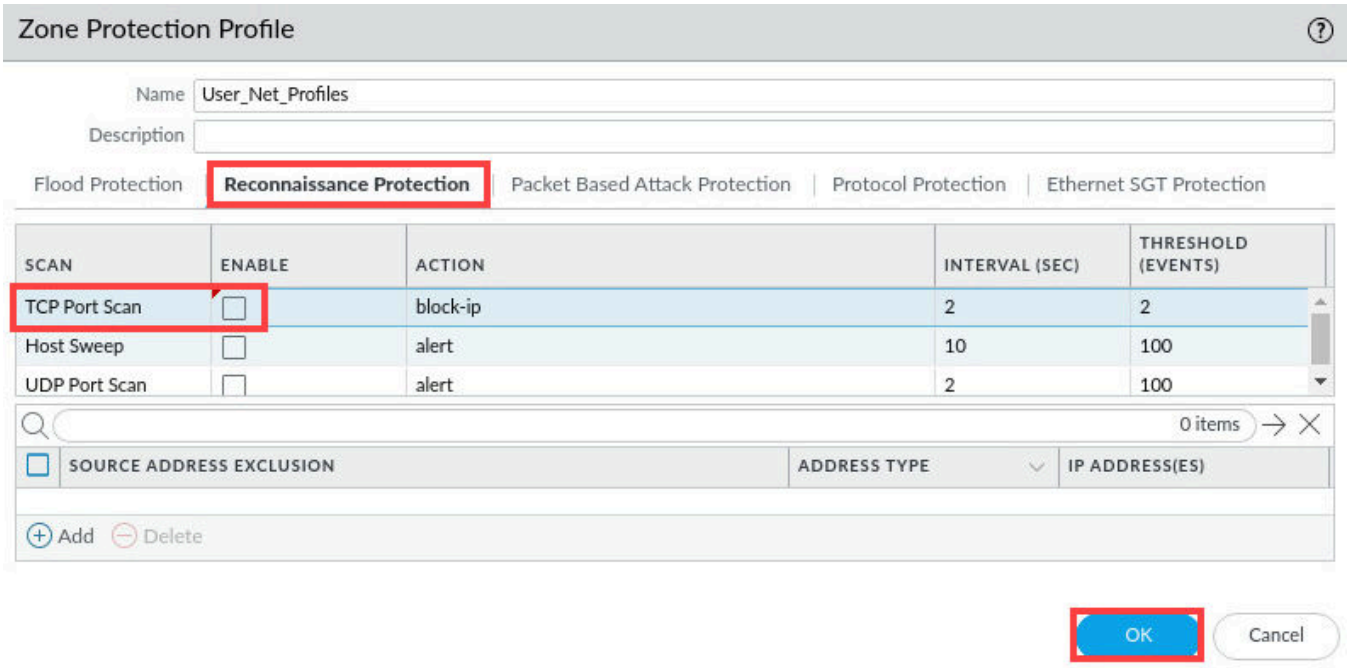
Parameter	Value
SYN	**Verify the check box is selected**
Action	**SYN Cookies**
Alarm Rate	**1000**
Activate	**1100**
Maximum	**1300**



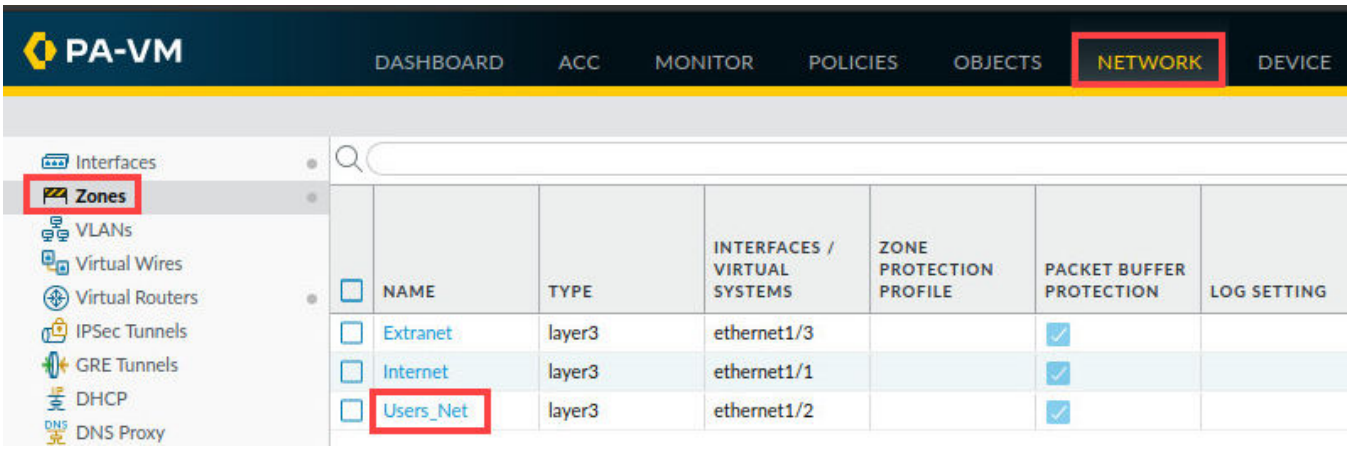
Please Note

The threshold values here are configured with high values to ensure that the lower DoS Protection Profile thresholds are reached first during testing in a later lab section.

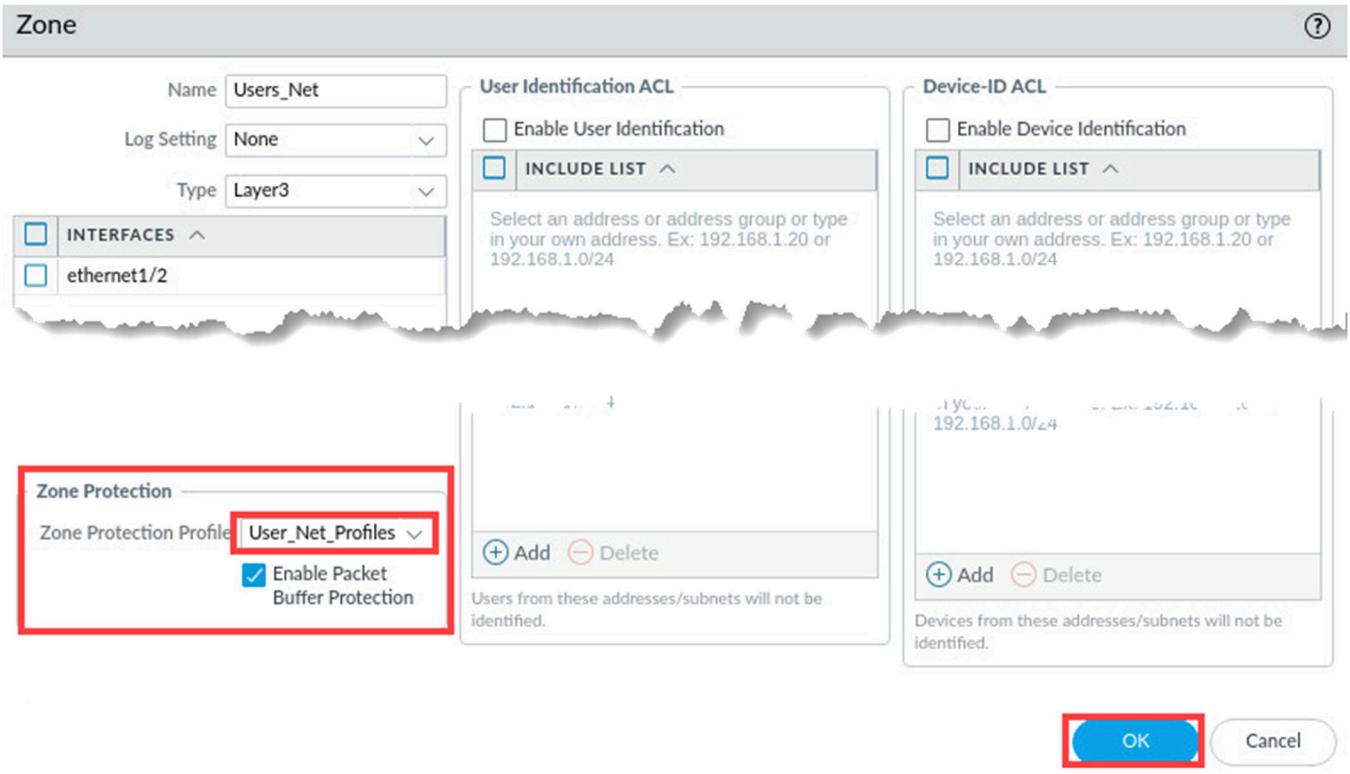
31. Click the **Reconnaissance Protection** tab. For *TCP Port Scan*, deselect the **Enable** checkbox. Click **OK**.



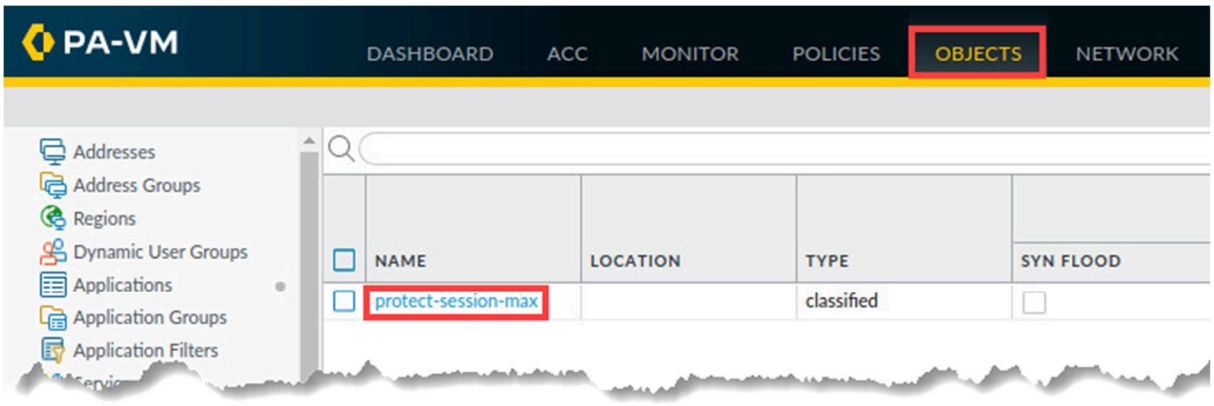
32. Select **Network > Zones**. Click the **Users_Net** zone.

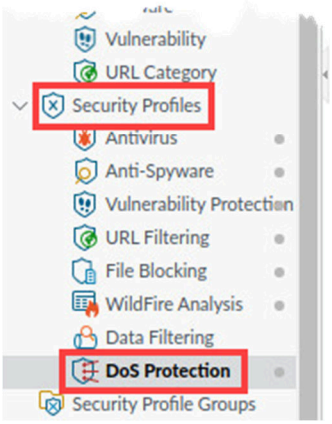


33. In the *Zone* window**,** *Zone Protection Profile* menu, select **User_Net_Profiles**. Click **OK**.



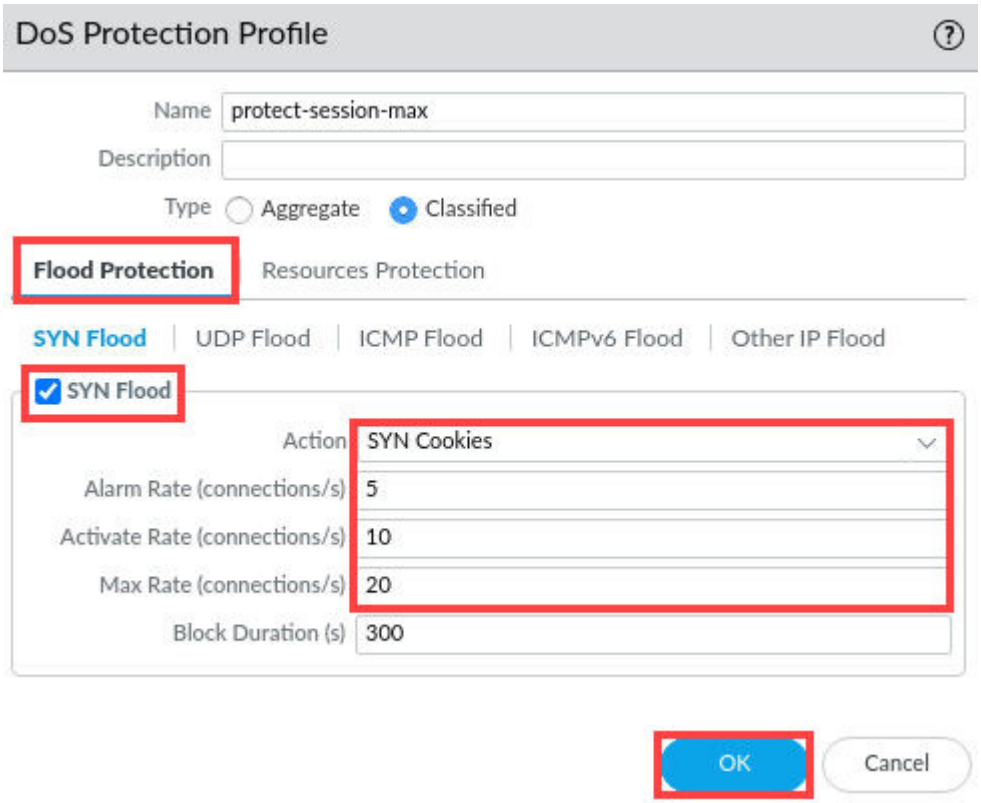
34. Navigate to **Objects > Security Profiles > DoS Protection**. Click **protect-session-max**.





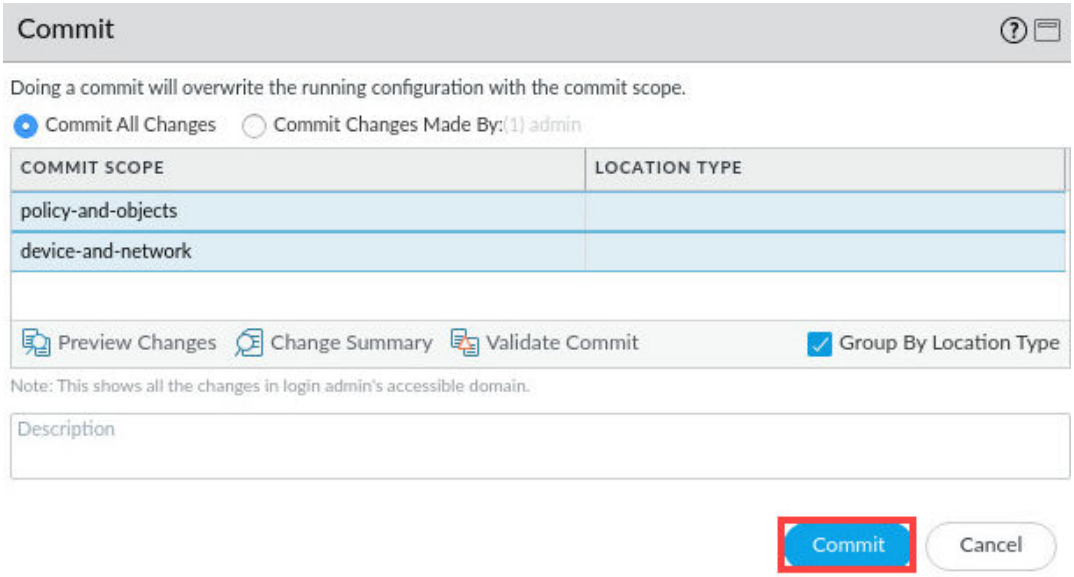
35. In the *DoS Protection Profile* window, configure the following. Click **OK**.

Parameter	Value
Flood Protection tab	**Verify that the tab is selected**
SYN Flood	**Select check box**
Action	**SYN Cookies**
Alarm Rate	**5**
Activate Rate	**10**
Max Rate	**20**

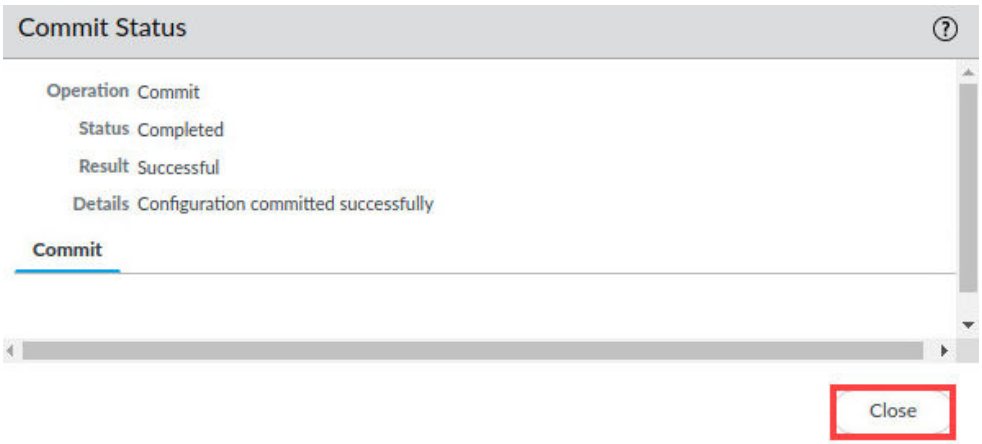


36. Click the **Commit** button at the upper-right of the web interface.

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

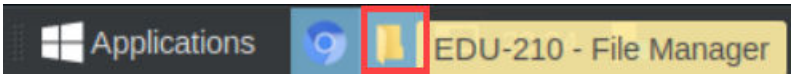


38. Wait until the *Commit* process is complete. Click **Close**.

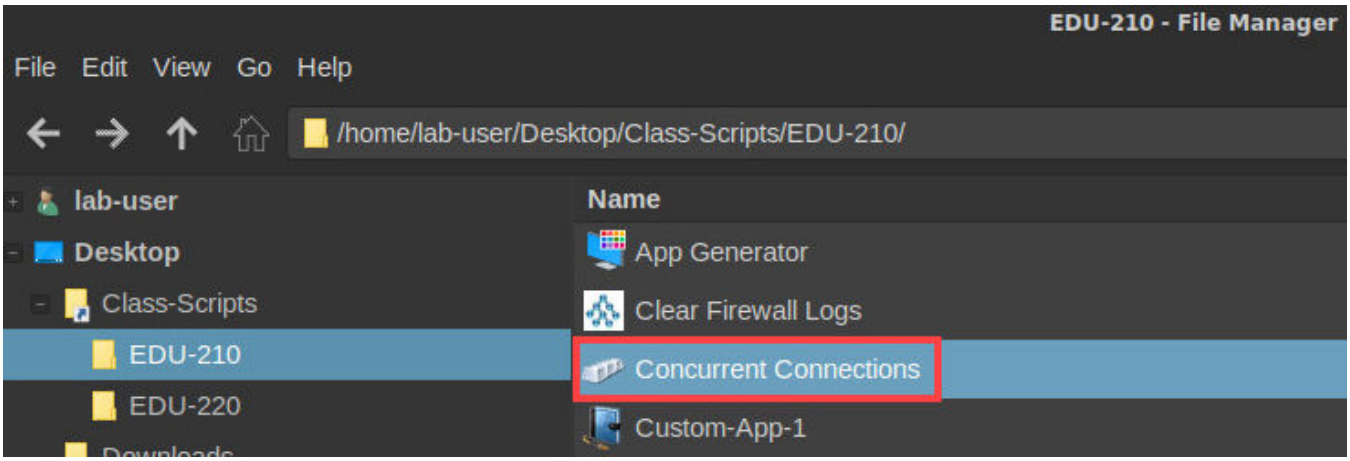


39. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.

40. Open the *EDU-210* folder by clicking on the **EDU-210 – File Manager** tab.



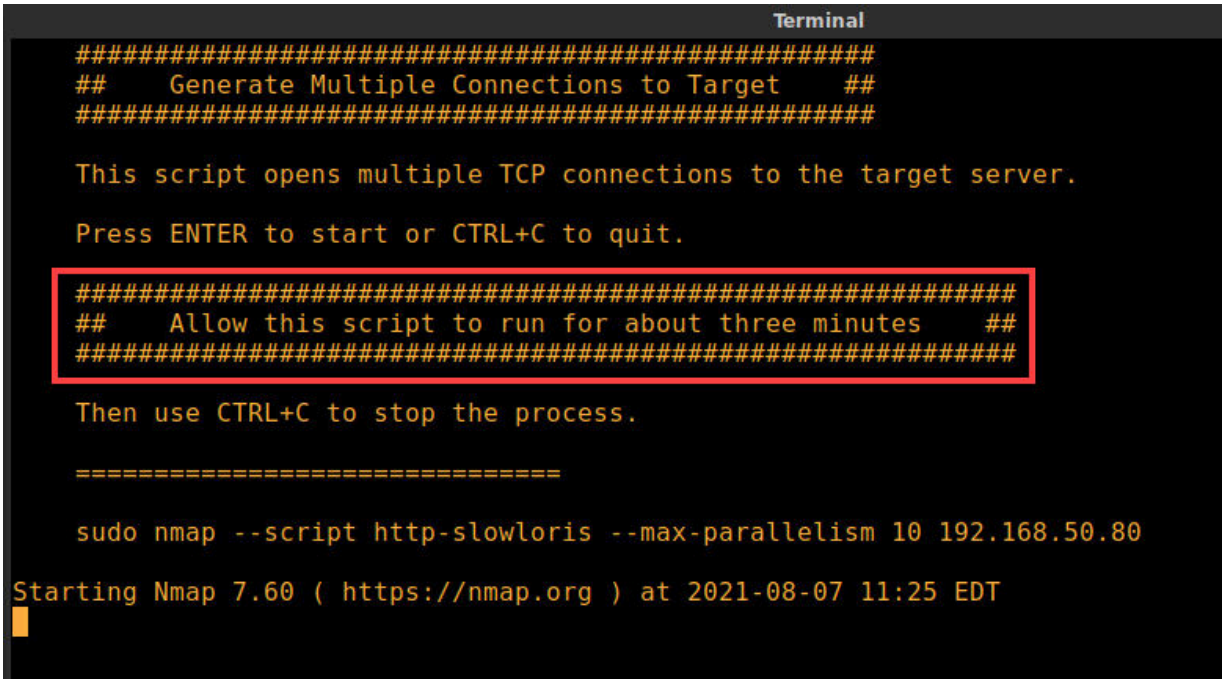
41. Double-click the icon for **Concurrent Connections**.



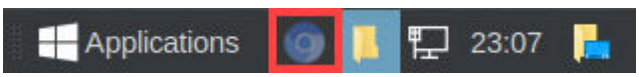
Please Note

The exact syntax for this command is:
nmap --script http-slowloris --max-parallelism 10 192.168.50.80

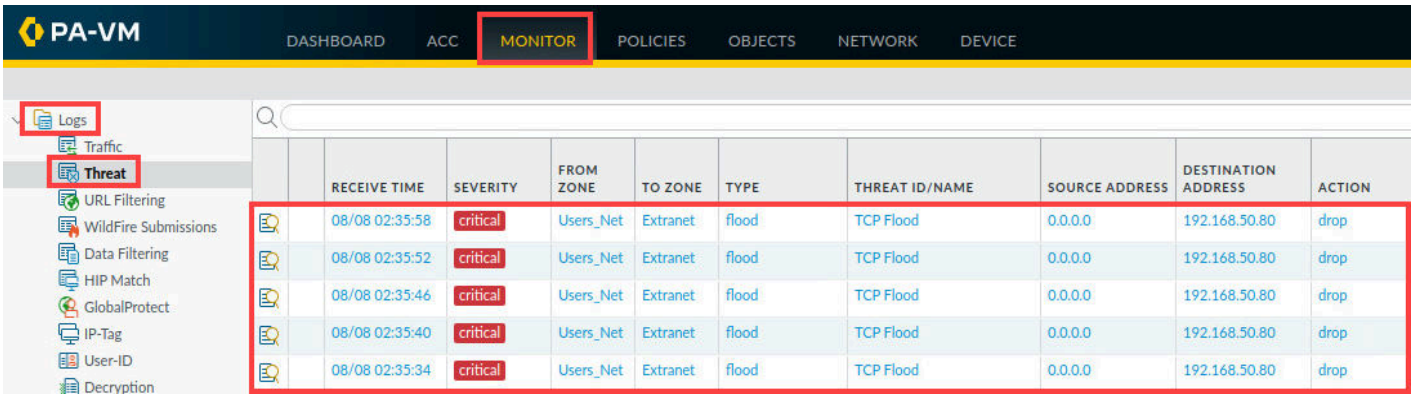
42. Press **Enter** to start the *Concurrent Connections* script. The command can take *30* minutes to complete. You do not need to wait for the script to complete. Allow the command to run for at least *3* minutes and then press **Ctrl+C** to stop command execution**.**



43. Reopen the *PA-VM Firewall* by clicking on the **Chromium** tab in the taskbar on the *client desktop.*



44. Navigate to **Monitor > Logs > Threat**. Notice the new *Threats*.



Please Note

Several columns have been hidden in this example.

You should see **TCP Flood** Threat log entries because the number of connection requests to the target host has exceeded the configured flood threshold maximum in the DoS Protection Profile. The flood threshold in the DoS Protection Profile is lower than the Zone Protection Profile, so it should have been triggered first.

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