



PALO ALTO NETWORKS EDU 210

Lab 6: Blocking Packet and Protocol Based Attacks

Document Version: **2022-07-18**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Blocking Packet and Protocol Based Attacks	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Generate SYN Flood Traffic	10
1.3 Configure and Test TCP SYN Flood Zone Protection	14
1.4 Reconnaissance Protection	19
1.5 Concurrent Sessions on a Target Host and DoS Protection	30

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.

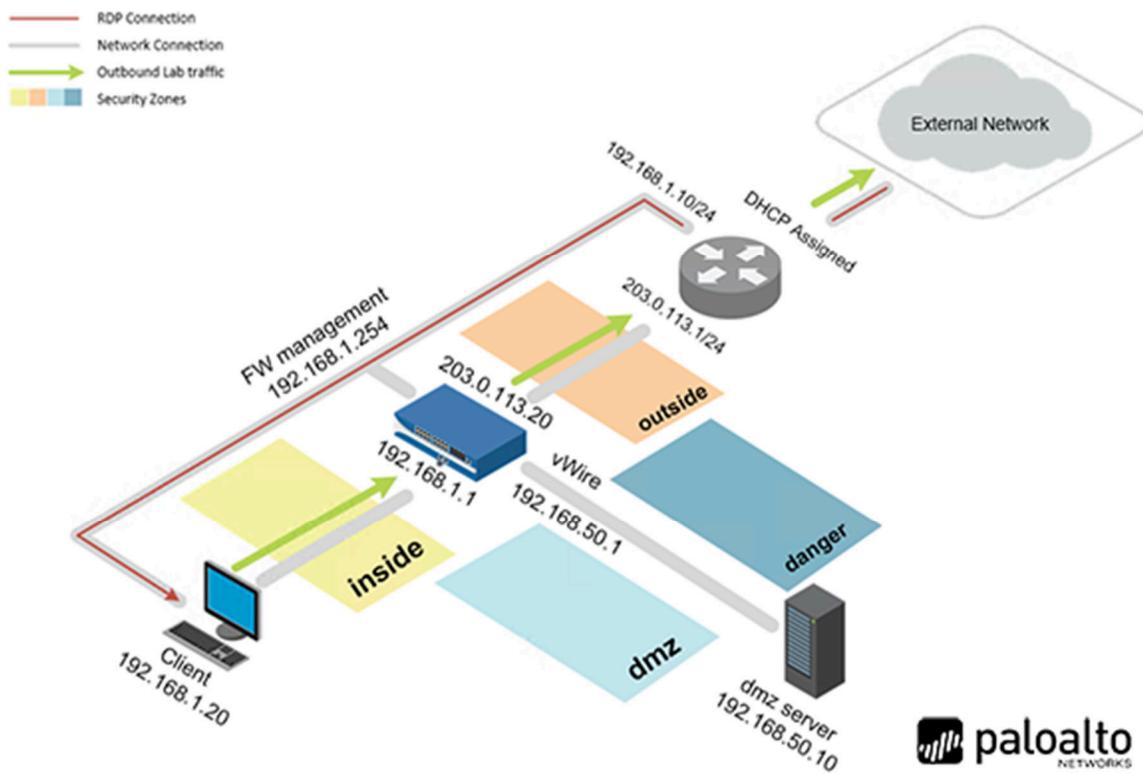
You will create a Zone Protection Profile that you can assign to security zones. You will also create a DoS Protection Profile and DoS policy rules to ensure that you are taking advantage of all the tools that the firewall has available to block packet-based floods and probes.

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	Pa10Alt0!
DMZ	192.168.50.10	root	Pa10Alt0!
Firewall	192.168.1.254	admin	Pa10Alt0!
VRouter	192.168.1.10	root	Pa10Alt0!

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.

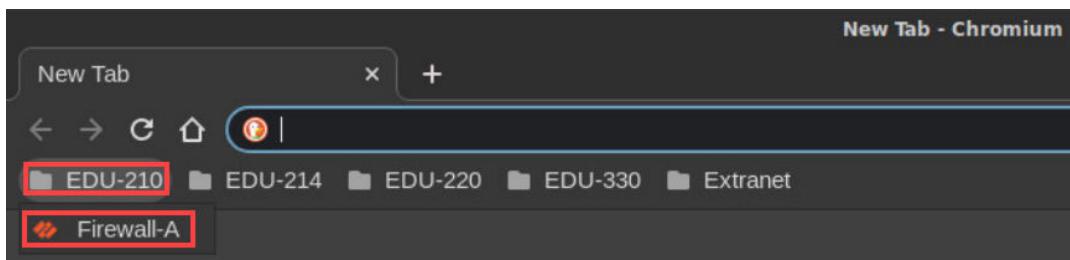
1. Click on the **Client** tab to access the Client PC.



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.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Advanced](#)

[Back to safety](#)



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)**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Hide advanced](#)

[Back to safety](#)

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.1.254 \(unsafe\)](#)

6. Log in to the firewall web interface as username **admin**, password **PaloAlt0!**.



The screenshot shows a login interface for a Palo Alto Networks device. The page has a yellow border. At the top is the Palo Alto Networks logo. Below the logo is a login form with two fields: a 'username' field containing 'admin' and a 'password' field containing redacted dots. At the bottom is a blue 'Log In' button.

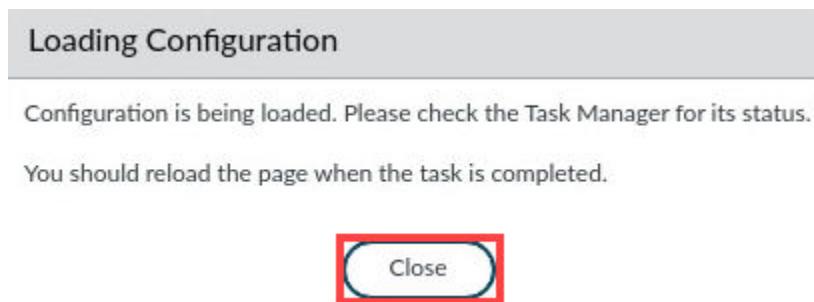
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE link is highlighted with a red box. On the left, a sidebar menu is open, showing options like Setup (highlighted with a red box), High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, and Data Redistribution. The main content area is titled 'Configuration Management'. It contains several buttons: Revert (Revert to last saved configuration, Revert to running configuration), Save (Save named configuration snapshot, Save candidate configuration), Load (Load named configuration snapshot, Load configuration version). The 'Load named configuration snapshot' button is highlighted with a red box.

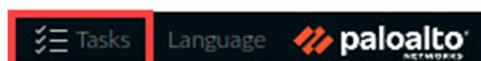
8. In the *Load Named Configuration* window, select **edu-210-lab-06.xml** from the *Name* dropdown box and click **OK**.



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**.

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	08/05/21 00:03:04		
Load	Completed	08/05/21 00:01:59		
EDLRefresh	Completed	08/04/21 23:58:15		
EDLFetch	Completed	08/04/21 23:58:14		
Download	Completed	08/04/21 23:58:04		
Download	Completed	08/04/21 23:54:04		
EDLFetch	Completed	08/04/21 23:53:13		
Auto Commit	Completed	08/04/21 23:52:45		

Show All Tasks | Clear Commit Queue | **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.

COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

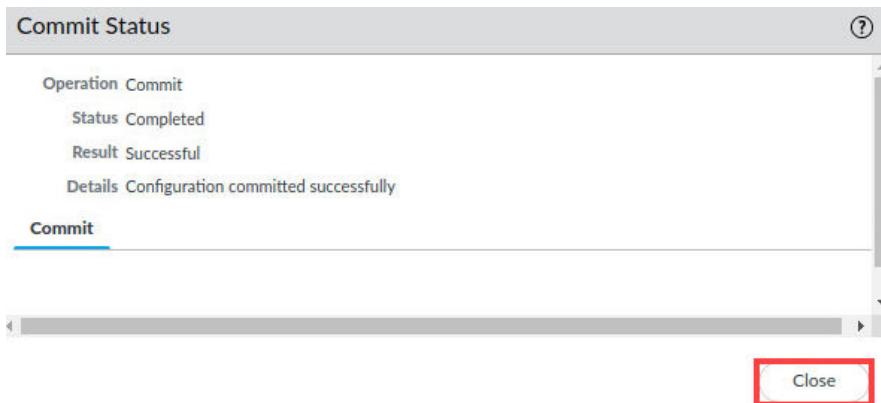
Preview Changes Change Summary Validate Commit Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit **Cancel**

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.

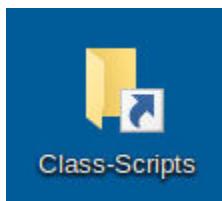
1.2 Generate SYN Flood Traffic

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.

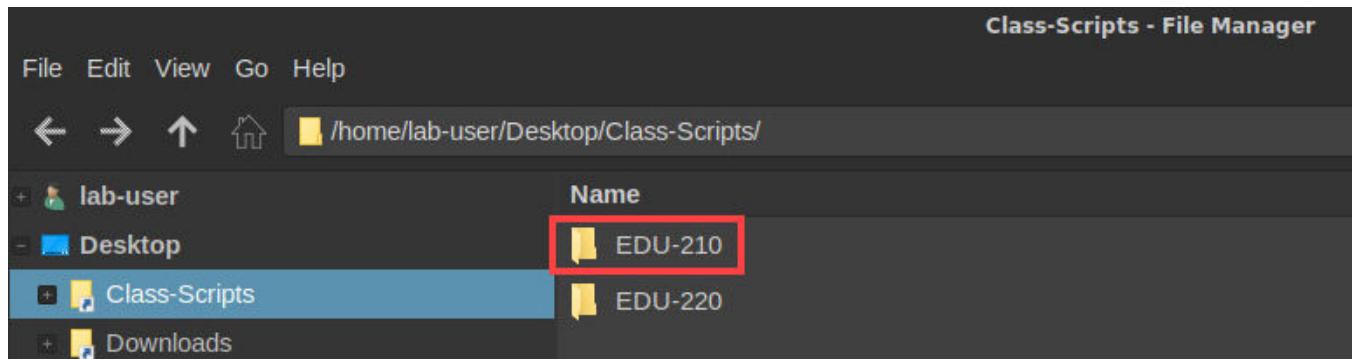
1. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



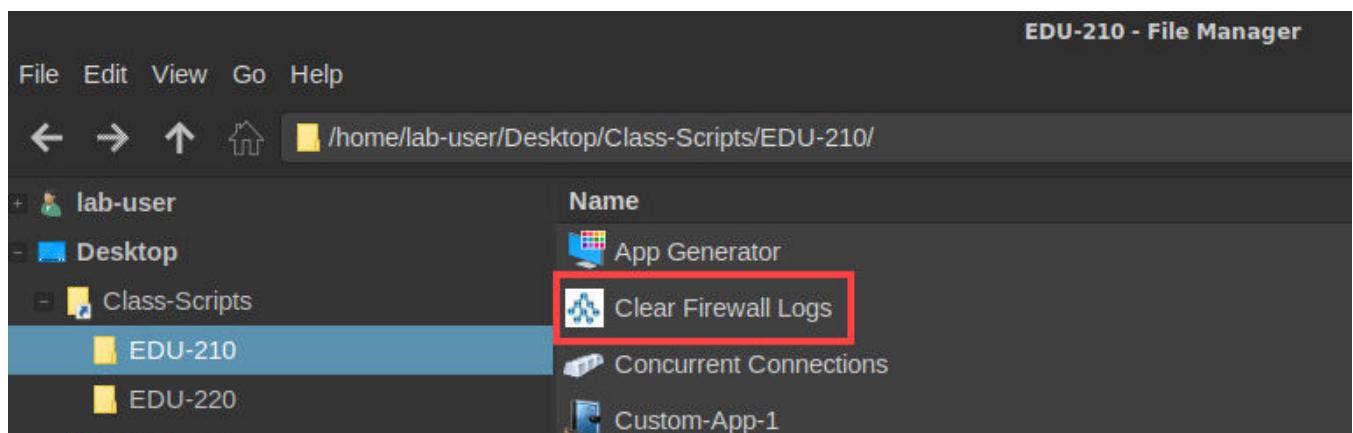
2. On the *client desktop*, double-click the folder for **Class-Scripts**.



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.

```
Terminal
This script clears the Traffic, Threat and URL Log Files from Firewall-A
Press ENTER to start or CTRL+C to quit.

Get API key for Firewall-A
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent    Left  Speed
100  200  100  200    0      0  491      0  --::--  --::--  -:-::--  491
Done.

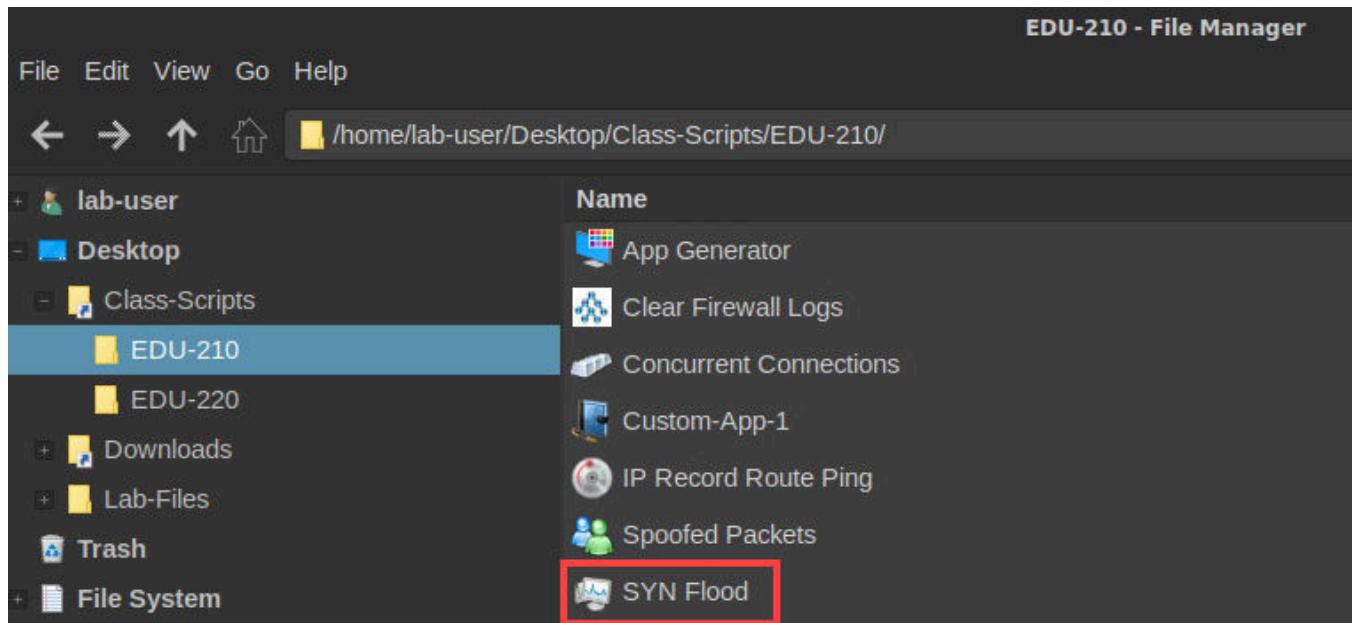
Clearing Threat Logs...on Firewall-A
<response status="success"><result>Successfully deleted threat logs</result></response> Complete.

Clearing Traffic Logs...on Firewall-A
<response status="success"><result>Successfully deleted traffic logs</result></response> Complete.

#####
##      Process Complete      ##
#####

Press ENTER to close this window.
```

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.

```
Terminal
#####
##          Generate SYN Flood      ##
#####

This script generates a SYN flood against target server.

Press ENTER to start or CTRL+C to quit.

nping --tcp-connect -p 80 --rate 10000 -c 50 192.168.50.80

Starting Nping 0.7.60 ( https://nmap.org/nping ) at 2021-08-06 23:04 EDT
SENT (0.0021s) Starting TCP Handshake > 192.168.50.80:80
RCVD (0.0063s) Handshake with 192.168.50.80:80 completed
RCVD (0.0063s) Handshake with 192.168.50.80:80 completed

Max rtt: 1.309ms | Min rtt: 0.016ms | Avg rtt: 0.584ms
TCP connection attempts: 50 | Successful connections: 50 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 0.01 seconds

#####
##          Process Complete      ##
#####

Press ENTER to close this window.
```

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.

	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	BYTES	HTTP/2 CONNECTION SESSION ID
	08/07 03:04:36	Users_Net	Extranet	192.168.1.20		192.168.50.80	80	incomplete	478	0
	08/07 03:04:36	Users_Net	Extranet	192.168.1.20		192.168.50.80	80	incomplete	478	0
	08/07 03:04:36	Users_Net	Extranet	192.168.1.20		192.168.50.80	80	incomplete	478	0
	08/07 03:04:36	Users_Net	Extranet	192.168.1.20		192.168.50.80	80	incomplete	478	0

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.

DESTINATION	DYNAMIC USER GROUP	TO PORT	APPLICATION

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

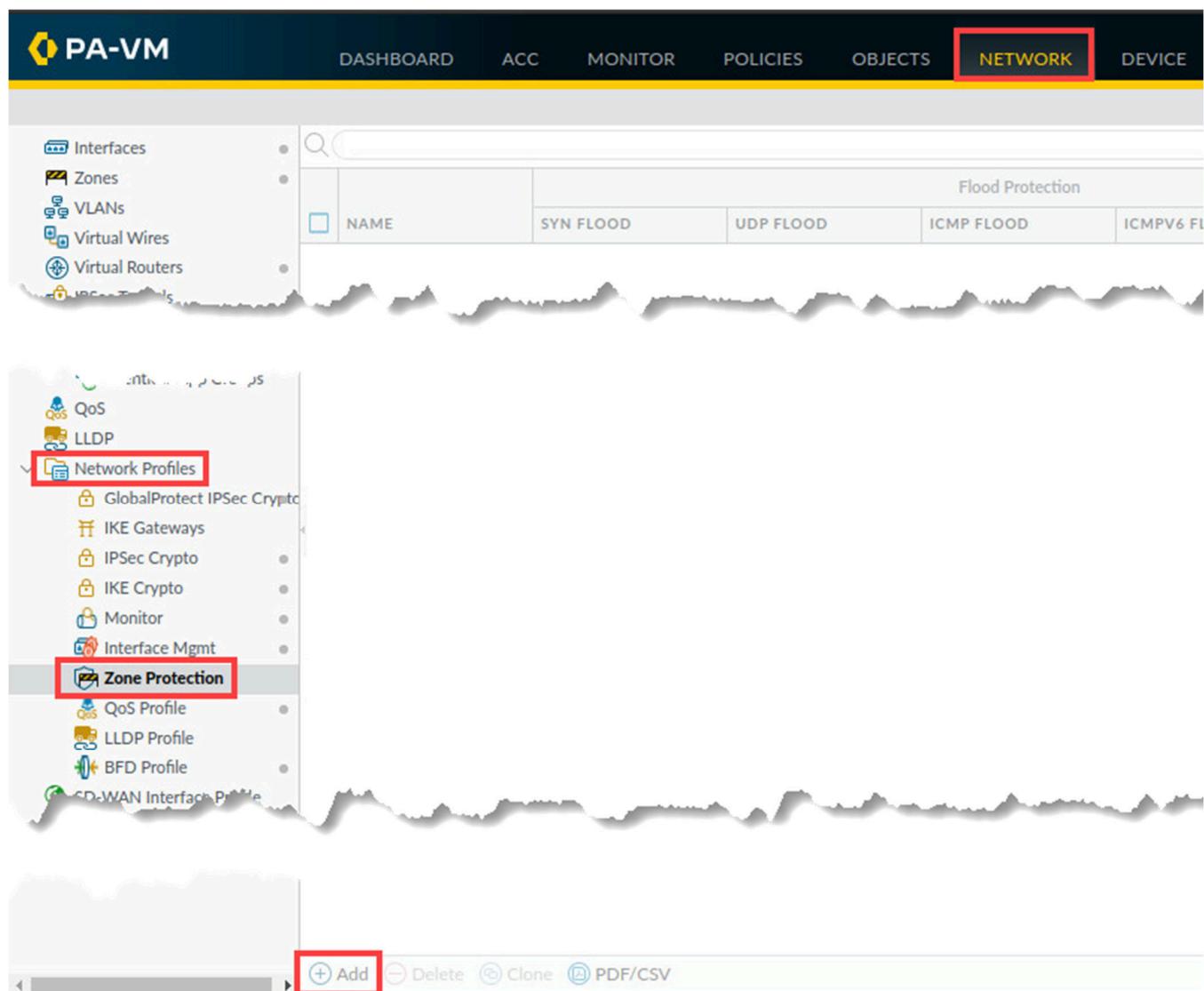
1.3 Configure and Test TCP SYN Flood Zone Protection

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

Zone Protection Profile

Name **User_Net_Profiles**

Description

Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Protection

SYN

Action: SYN Cookies

Alarm Rate (connections/sec): 5

Activate (connections/sec): 10

Maximum (connections/sec): 20

ICMP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

Other IP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

ICMPv6

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

UDP

Alarm Rate (connections/sec): 10000

Activate (connections/sec): 10000

Maximum (connections/sec): 40000

OK **Cancel**

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**.

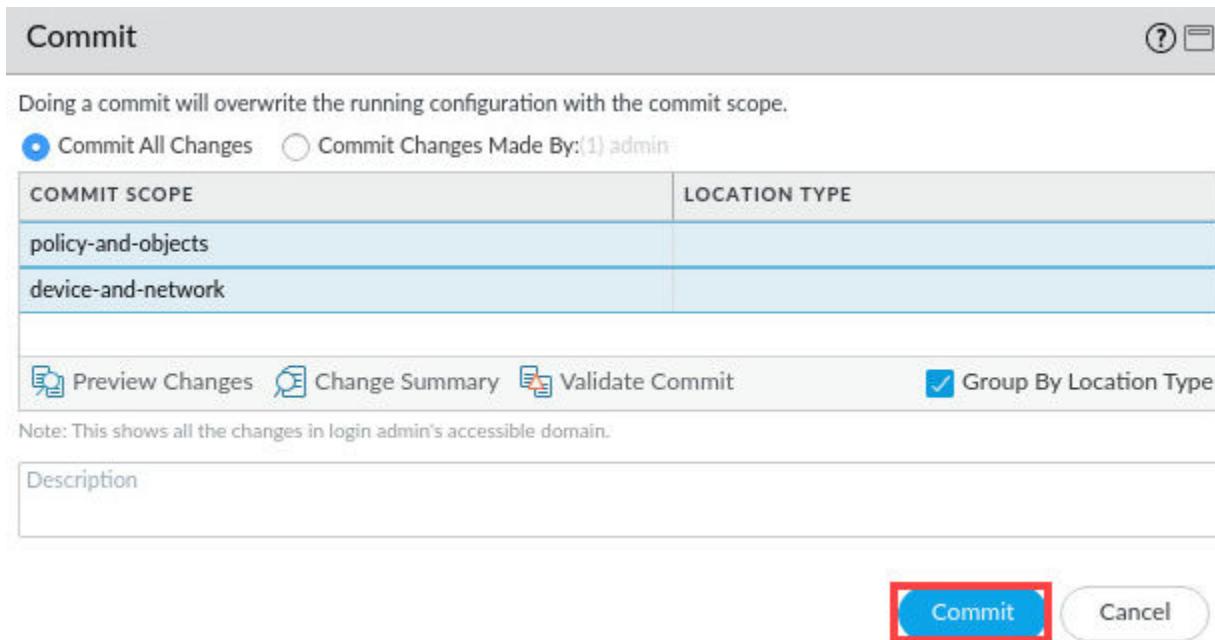
NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING
Extranet	layer3	ethernet1/3		<input checked="" type="checkbox"/>	
Internet	layer3	ethernet1/1		<input checked="" type="checkbox"/>	
Users_Net	layer3	ethernet1/2		<input checked="" type="checkbox"/>	

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**.

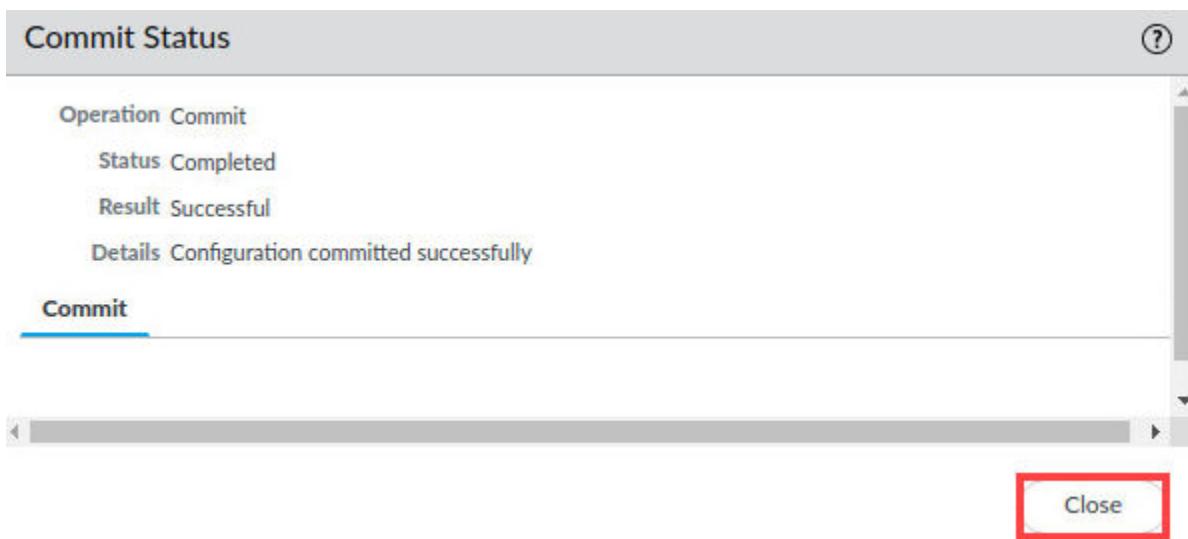
5. Click the **Commit** button at the upper-right of the web interface.



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



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



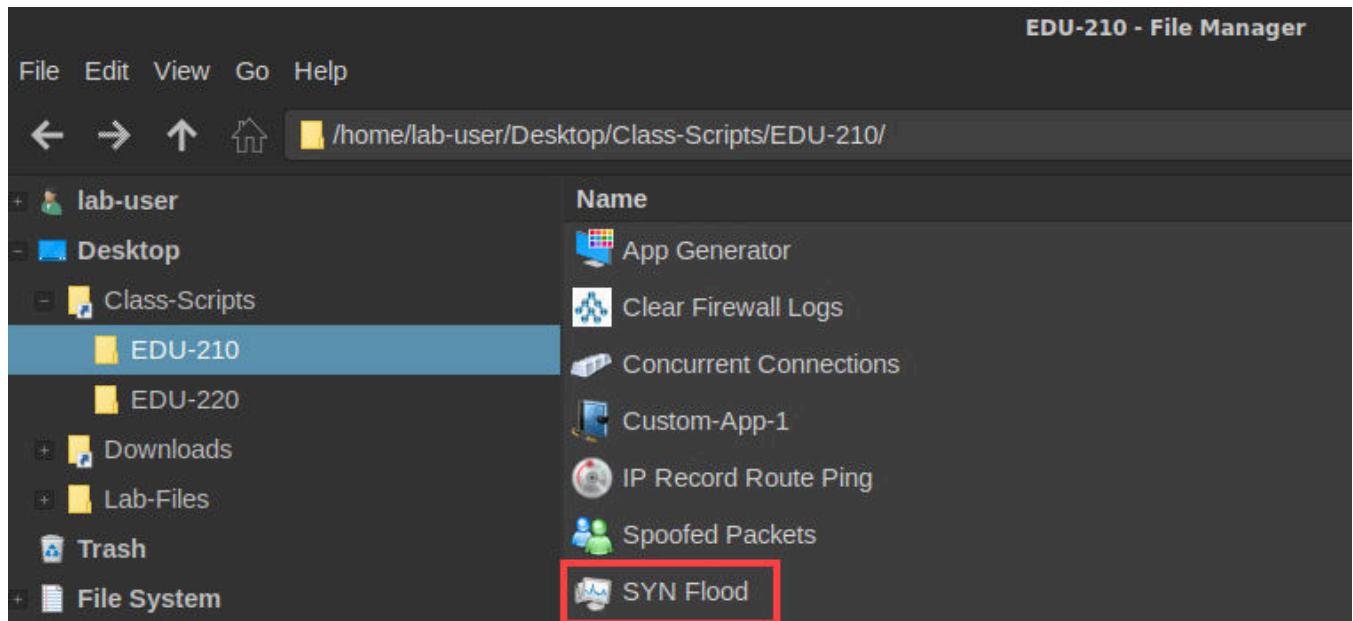
8. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



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**.

```
Terminal
#####
##      Generate SYN Flood      ##
#####

This script generates a SYN flood against target server.

Press ENTER to start or CTRL+C to quit.

nping --tcp-connect -p 80 --rate 10000 -c 50 192.168.50.80

Starting Nping 0.7.60 ( https://nmap.org/nping ) at 2021-08-06 23:04 EDT
SENT (0.0021s) Starting TCP Handshake > 192.168.50.80:80
RCVD (0.0031s) Handshake with 192.168.50.80:80 completed
RCVD (0.0031s) Handshake with 192.168.50.80:80 completed

Max rtt: 1.309ms | Min rtt: 0.016ms | Avg rtt: 0.584ms
TCP connection attempts: 50 | Successful connections: 50 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 0.01 seconds

#####
##      Process Complete      ##
#####

Press ENTER to close this window.
```

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.

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC GROUP
	08/07 03:44:04	critical	flood	TCP Flood	Users_Net	Users_Net	0.0.0.0		

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.

The screenshot shows the PA-VM interface with the following details:

- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, **NETWORK** (highlighted with a red box), DEVICE.
- Left Sidebar:** Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, and Networks. The "Network Profiles" item under "Network" is highlighted with a red box.
- Central Content Area:** A table titled "Flood Protection" with columns: NAME, SYN FLOOD, UDP FLOOD, ICMP FLOOD, ICMPV6 FLOOD. A row for "User_Net_Profiles" is shown, with the "NAME" column and the "SYN FLOOD" checkbox being highlighted with a red box.
- Bottom Sidebar:** Client Groups, QoS, LLDP, and Network Profiles. The "Zone Protection" item under "Network Profiles" is highlighted with a red box.

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

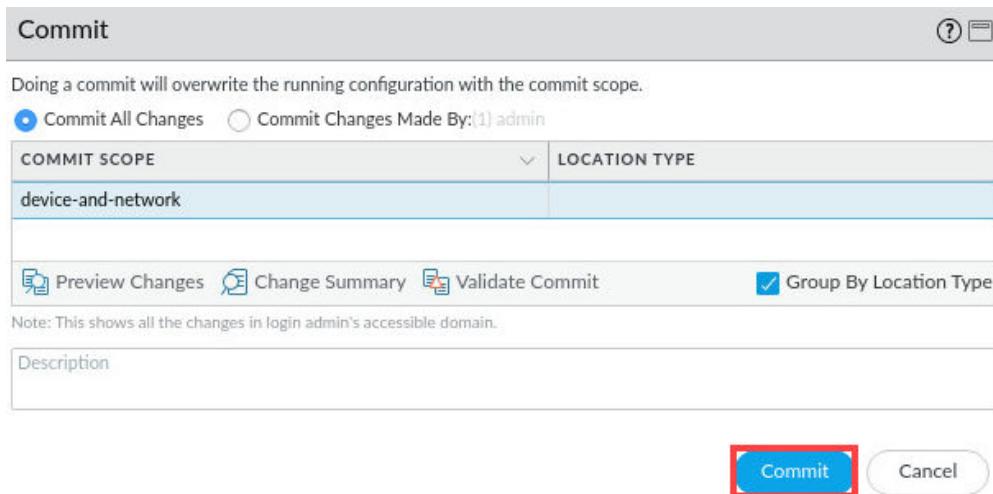
Zone Protection Profile (?)

Name: User_Net_Profiles	Description:																								
Flood Protection Reconnaissance Protection Packet Based Attack Protection Protocol Protection Ethernet SGT Protection																									
<table border="1"> <thead> <tr> <th>SCAN ^</th> <th>ENABLE</th> <th>ACTION</th> <th>INTERVAL (SEC)</th> <th>THRESHOLD (EVENTS)</th> </tr> </thead> <tbody> <tr> <td>TCP Port Scan</td> <td><input checked="" type="checkbox"/></td> <td>Block IP</td> <td>2</td> <td>2</td> </tr> <tr> <td>Host Sweep</td> <td><input type="checkbox"/></td> <td>Track By</td> <td>10</td> <td>100</td> </tr> <tr> <td>UDP Port Scan</td> <td><input type="checkbox"/></td> <td>source</td> <td>2</td> <td>100</td> </tr> <tr> <td colspan="2"> <input type="text"/> Duration (sec) 0 items → X <input type="checkbox"/> SOURCE ADDRESS EXCLUSION <input type="text"/> 2 IP ADDRESS(ES) </td> </tr> <tr> <td colspan="2"> (+) Add (-) Delete </td> </tr> </tbody> </table>		SCAN ^	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)	TCP Port Scan	<input checked="" type="checkbox"/>	Block IP	2	2	Host Sweep	<input type="checkbox"/>	Track By	10	100	UDP Port Scan	<input type="checkbox"/>	source	2	100	<input type="text"/> Duration (sec) 0 items → X <input type="checkbox"/> SOURCE ADDRESS EXCLUSION <input type="text"/> 2 IP ADDRESS(ES)		(+) Add (-) Delete	
SCAN ^	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)																					
TCP Port Scan	<input checked="" type="checkbox"/>	Block IP	2	2																					
Host Sweep	<input type="checkbox"/>	Track By	10	100																					
UDP Port Scan	<input type="checkbox"/>	source	2	100																					
<input type="text"/> Duration (sec) 0 items → X <input type="checkbox"/> SOURCE ADDRESS EXCLUSION <input type="text"/> 2 IP ADDRESS(ES)																									
(+) Add (-) Delete																									
OK Cancel																									

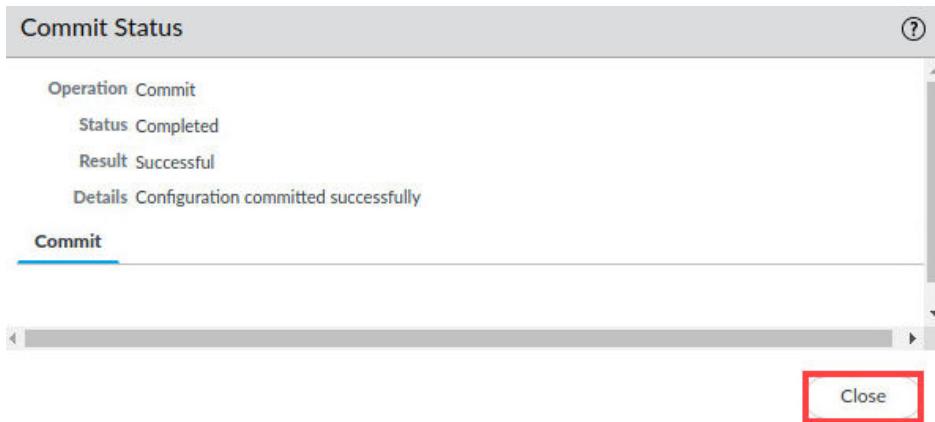
3. Click the **Commit** button at the upper-right of the web interface.



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



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



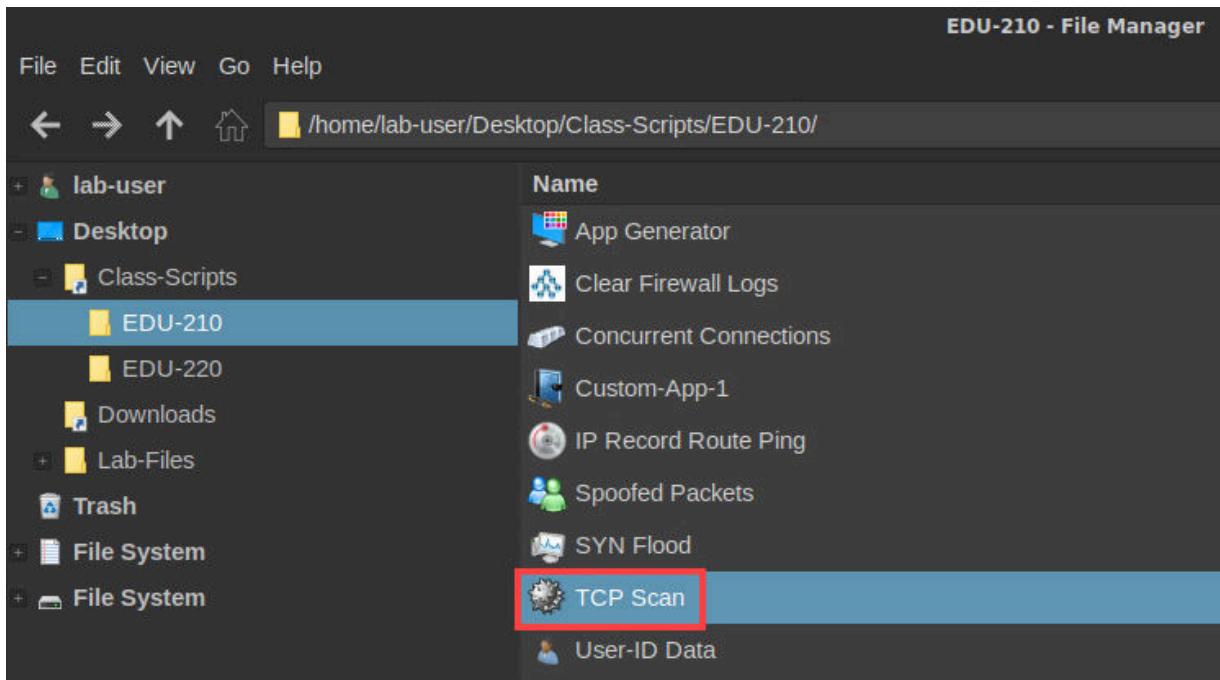
6. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



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.

```
#####
##      TCP Port Scan      ##
#####

This script runs a TCP Port Scan against target server.

Press ENTER to start or CTRL+C to quit.

nmap -v1 -Pn -T4 --max-retries 1 192.168.50.80

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-07 00:21 EDT
Initiating Connect Scan at 00:21
Scanning www.panw.lab (192.168.50.80) [1000 ports]
Increasing send delay for 192.168.50.80 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Warning: 192.168.50.80 giving up on port because retransmission cap hit (1).
Connect Scan Timing: About 19.30% done; ETC: 00:23 (0:02:10 remaining)
Increasing send delay for 192.168.50.80 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Connect Scan Timing: About 36.90% done; ETC: 00:23 (0:01:44 remaining)
```

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.

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE
	08/07 04:22:36	medium	scan	SCAN: TCP Port Scan	Users_Net	Extranet
	08/07 04:22:24	medium	scan	SCAN: TCP Port Scan	Users_Net	Extranet
	08/07 04:22:17	medium	scan	SCAN: TCP Port Scan	Users_Net	Extranet
	08/07 04:22:11	medium	scan	SCAN: TCP Port Scan	Users_Net	Extranet

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

NAME	SYN FLOOD	UDP FLOOD	ICMP FLOOD	ICMPV6 F
User_Net_Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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**.

Zone Protection Profile

Name: User_Net_Profiles

Description:

Flood Protection | Reconnaissance Protection | **Packet Based Attack Protection** | Protocol Protection | Ethernet SGT Protection

IP Drop | TCP Drop | ICMP Drop | IPv6 Drop | ICMPv6 Drop

- Spoofed IP address
- Strict IP Address Check
- Fragmented traffic

IP Option Drop

<input type="checkbox"/> Strict Source Routing	<input type="checkbox"/> Security
<input type="checkbox"/> Loose Source Routing	<input type="checkbox"/> Stream ID
<input type="checkbox"/> Timestamp	<input type="checkbox"/> Unknown
<input checked="" type="checkbox"/> Record Route	<input type="checkbox"/> Malformed

OK | Cancel

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



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

Commit

Doing a commit will overwrite the running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
device-and-network	

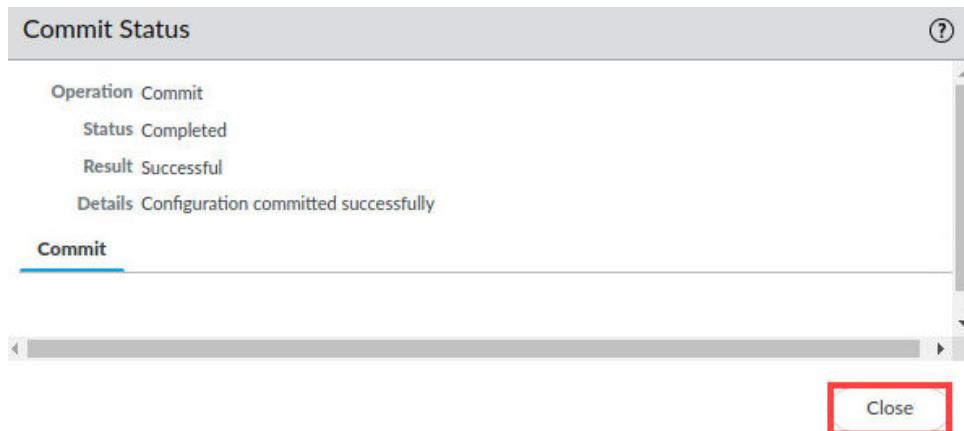
Preview Changes Change Summary Validate Commit Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description:

Commit | Cancel

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



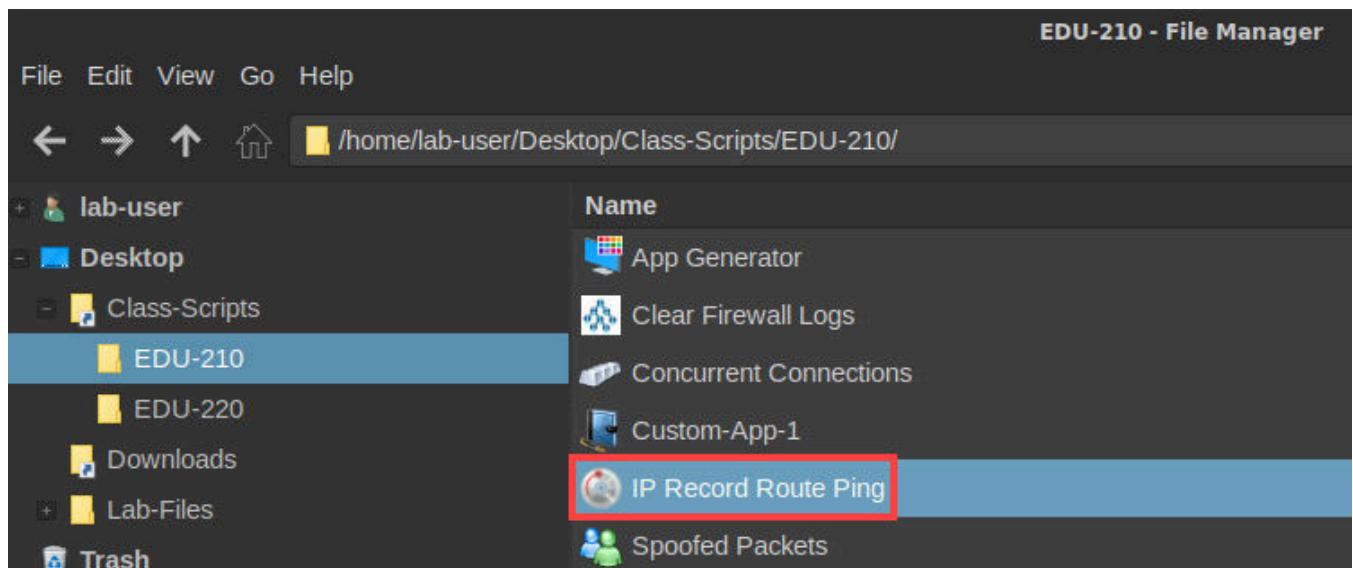
17. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next step.



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.

```
Terminal
#####
##          Record Route Pings      ##
#####

This script sends pings to target server with record route flag set.

Press ENTER to start or CTRL+C to quit.

nmap -sP --ip-options R 192.168.50.80 --max-retries 3

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-07 00:36 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.00 seconds

#####
##          Process Complete      ##
#####

Press ENTER to close this window.
```

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*.

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME
	08/07 04:36:35	informational	packet	IP Option Record Route
	08/07 04:22:36	medium	scan	SCAN: TCP Port Scan
	08/07 04:22:24	medium	scan	SCAN: TCP Port Scan

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.

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING
Extranet	layer3	ethernet1/3		<input checked="" type="checkbox"/>	
Internet	layer3	ethernet1/1		<input checked="" type="checkbox"/>	
Users_Net	layer3	ethernet1/2	User_Net_Profiles	<input checked="" type="checkbox"/>	

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

Zone

Name: Users_Net

Log Setting: None

Type: Layer3

INTERFACES:

User Identification ACL:

- Enable User Identification:
- INCLUDE LIST: **INCLUDE LIST**
- Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Device-ID ACL:

- Enable Device Identification:
- INCLUDE LIST: **INCLUDE LIST**
- Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Zone Protection:

Zone Protection Profile: **None**

Enable Packet Buffer Protection:

Add Delete

Users from these addresses/subnets will not be identified.

Add Delete

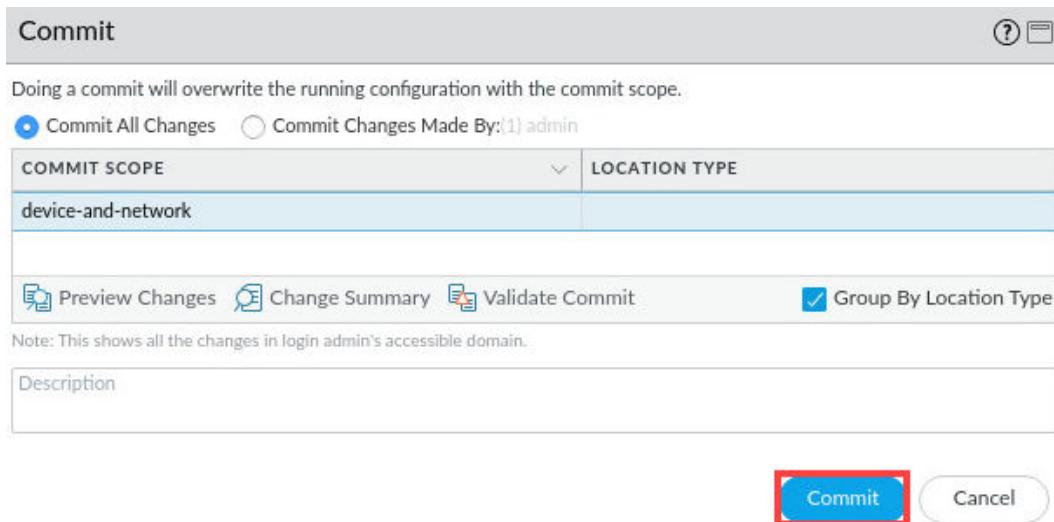
Devices from these addresses/subnets will not be identified.

OK Cancel

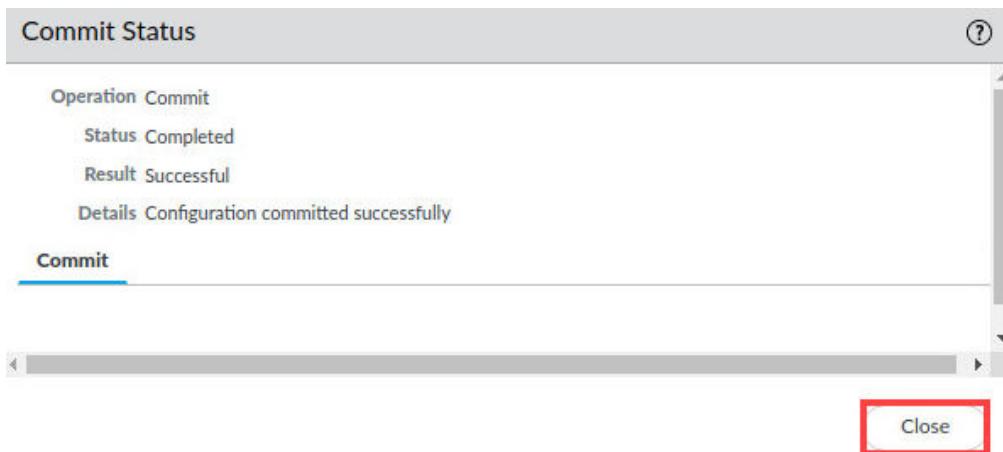
25. Click the **Commit** button at the upper-right of the web interface.



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.

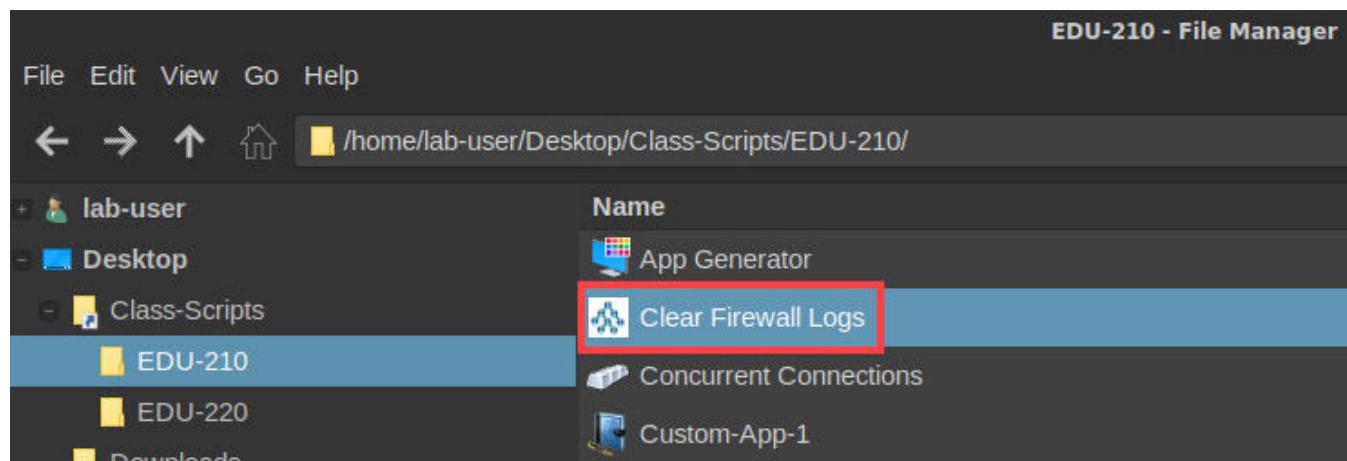
A DoS Protection Profile can detect and block flood attacks to a zone, to a subset of hosts in a zone, or to a specific host in a zone. You will configure flood protection in both a Zone Protection Profile and a DoS Protection Profile so that you can see how they interact. You will configure a higher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

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

```

Terminal
#####
##      Clear Logs from Firewall      ##
#####

This script clears the Traffic, Threat and URL Log Files from Firewall-A

Press ENTER to start or CTRL+C to quit.

Get API key for Firewall-A
% Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
          Dload  Upload   Total Spent  Left Speed
100  200  100  200    0       0  498      0 --:--:-- --:--:-- --:--:-- 497
Done.

Clearing Threat Logs...on Firewall-A
<response status="success"><result>Successfully deleted threat logs</result></response> Complete.

Clearing Traffic Logs...on Firewall-A
<response status="success"><result>Successfully deleted traffic logs</result></response> Complete.

#####
##      Process Complete      ##
#####

Press ENTER to close this window.■

```

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



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

The screenshot shows the PA-VM Firewall web interface. The top navigation bar has tabs for DASHBOARD, ACC, MONITOR (which is highlighted with a red box), and POLICIES. On the left, there's a sidebar with links for Logs, Traffic, Threat (which is highlighted with a red box), URL Filtering, WildFire Submissions, Data Filtering, and HIP Match. The main content area shows a table with columns RECEIVE TIME, SEVERITY, and TYPE, all of which are currently empty. A search bar is also present above the table.

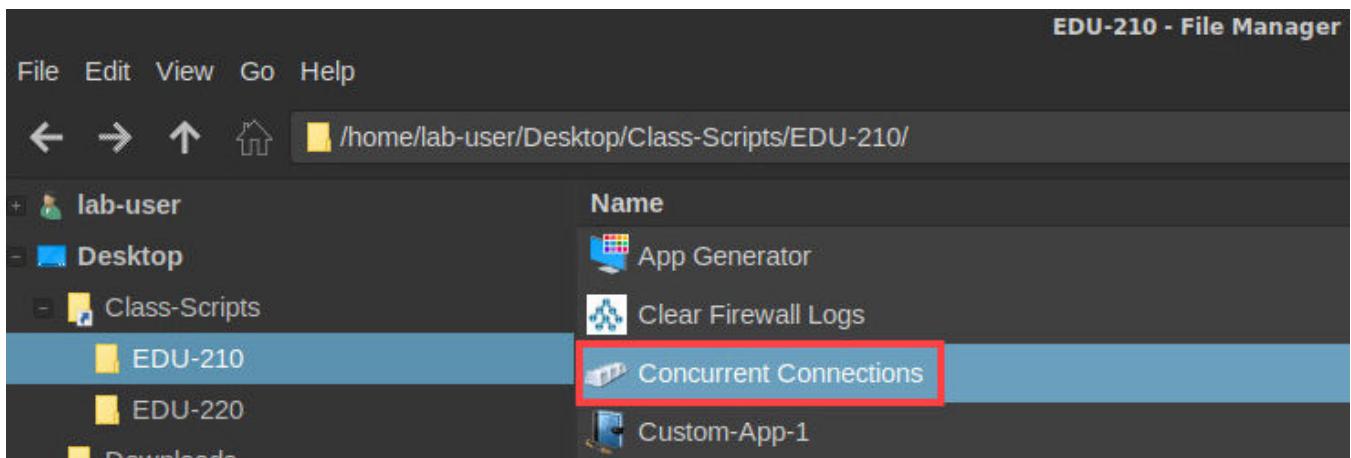
6. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



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.

```

Terminal
#####
## Generate Multiple Connections to Target ##
#####

This script opens multiple TCP connections to the target server.

Press ENTER to start or CTRL+C to quit.

#####
## Allow this script to run for about three minutes ##
#####

Then use CTRL+C to stop the process.

=====
sudo nmap --script http-slowloris --max-parallelism 10 192.168.50.80
Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-07 11:25 EDT
[

```

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.

	RECEIVE TIME	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	BYTES	HTTP/2 CONNECTION SESSION ID
	08/07 15:32:18	Users_Net	Extranet	192.168.1.20		192.168.50.53	53	dns	158	0
	08/07 15:32:18	Users_Net	Internet	192.168.1.20		1.1.1	53	dns	592	0
	08/07 15:32:13	Users_Net	Internet	192.168.1.20		13.107.4.52	80	web-browsing	1.3k	0

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.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. In the left sidebar, under 'Logs', the 'Threat' option is selected and highlighted with a red box. The main area displays a table with columns: RECEIVE TIME, SEVERITY, and TYPE. A large red box highlights the entire content area of the table.

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.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. In the left sidebar, under 'Security Profiles', the 'DoS Protection' option is selected and highlighted with a red box. At the bottom left of the main content area, the '+ Add' button is highlighted with a red box.

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

DoS Protection Profile

Name: **protect-session-max**

Description:

Type: Aggregate Classified

Flood Protection: **Resources Protection**

Sessions

Maximum Concurrent Sessions: **9**

Buttons: **OK** (highlighted with red box) and **Cancel**

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

PA-VM

DASHBOARD ACC MONITOR **POLICIES** OBJECTS

Security NAT QoS Policy Based Forwarding Decryption Tunnel Inspection Application Override Authentication **DoS Protection** SD-WAN

Object : Addresses + **Add** Delete Clone Enable Disable Move PDF/C

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

The screenshot shows two instances of the 'DoS Rule' configuration window. The top instance is the 'General' tab, where the 'Name' field is set to 'internal-protection'. The bottom instance is the 'Source' tab, where the 'Type' dropdown is set to 'Zone' and the 'ZONE' dropdown contains 'Users_Net' selected. The 'Add' button at the bottom left of the source tab is highlighted with a red box.

DoS Rule

General | Source | **Destination** | Option/Protection

Type: Zone

Any

DESTINATION ADDRESS

Extranet

+ Add | - Delete

+ Add | - Delete

Negate

DoS Rule

General | Source | Destination | **Option/Protection**

Any

SERVICE

Action: Protect

Schedule: None

Log Forwarding: None

Aggregate: None

Classified

Profile: protect-session-max

Address: destination-ip-only

+ Add | - Delete

OK | Cancel

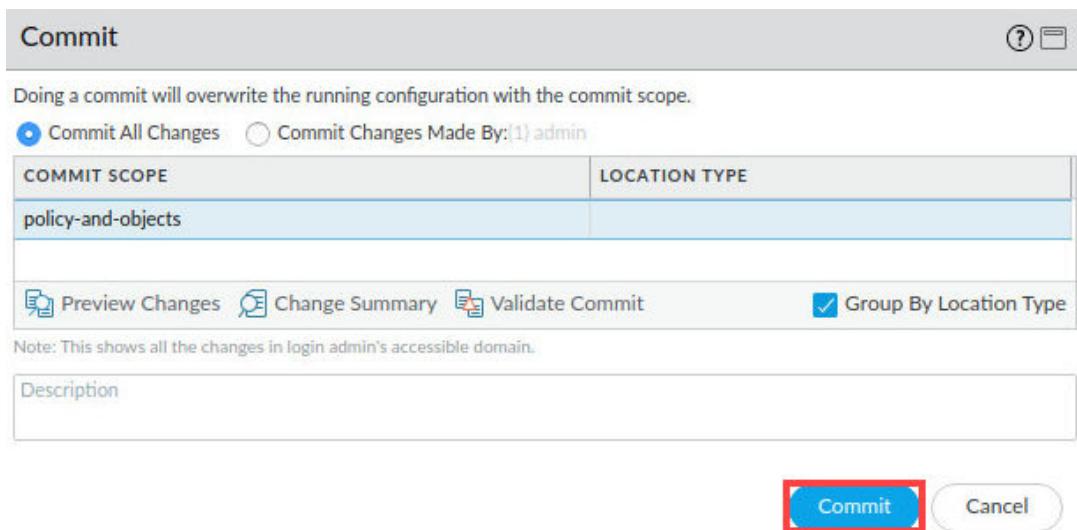
17. Verify the *internal-protection* rule is present in the DoS Protection policies.

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

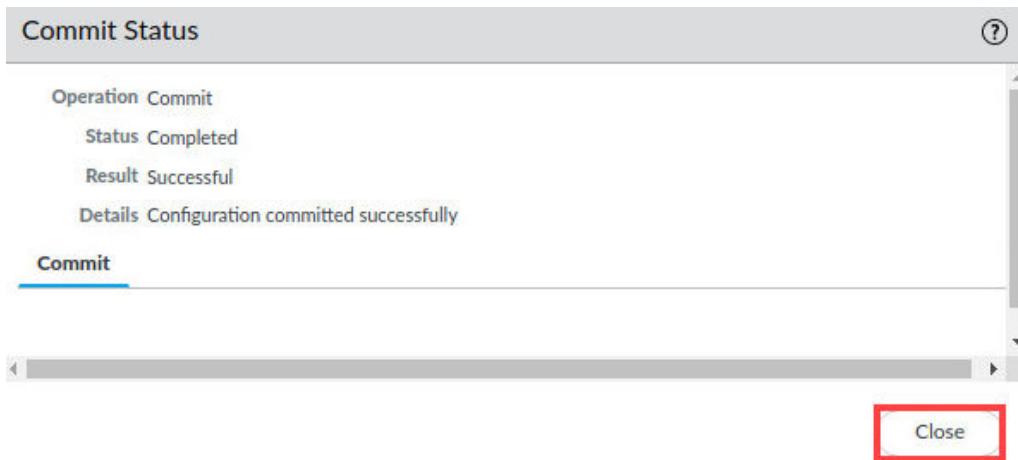
18. Click the **Commit** button at the upper-right of the web interface.



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



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



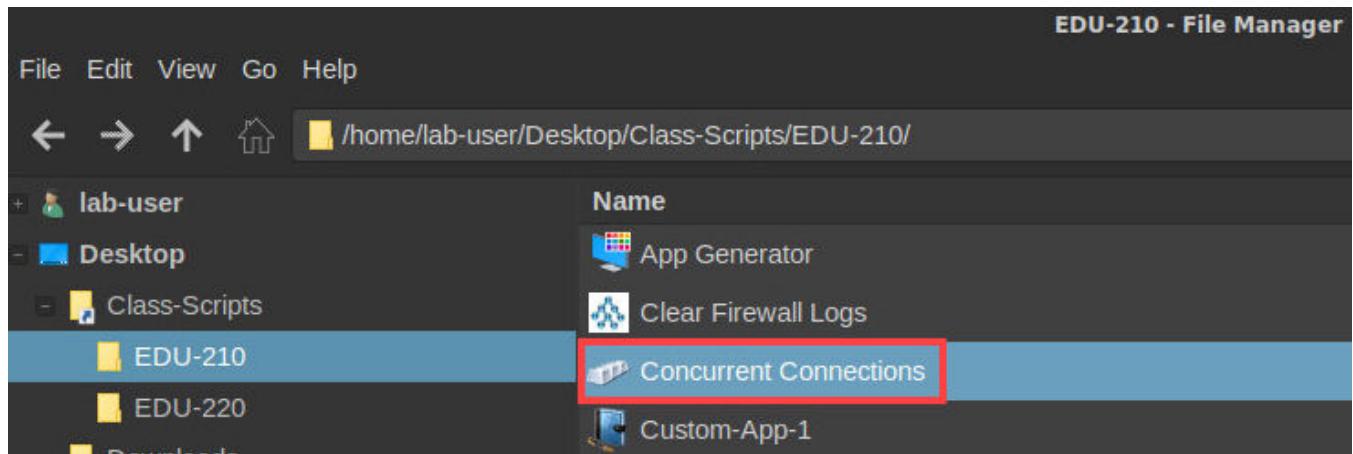
21. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



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.

The terminal window is titled "Terminal". It displays the following text:

```
#####
## Generate Multiple Connections to Target ##
#####

This script opens multiple TCP connections to the target server.

Press ENTER to start or CTRL+C to quit.

#####
## Allow this script to run for about three minutes ##
#####
```

Then use CTRL+C to stop the process.

```
=====
sudo nmap --script http-slowloris --max-parallelism 10 192.168.50.80
Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-07 11:25 EDT
```

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*.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. In the left sidebar, 'Logs' is expanded, and 'Threat' is selected, both highlighted with red boxes. The main area displays a table of threat logs with the following columns: RECEIVE TIME, SEVERITY, TYPE, THREAT ID/NAME, SOURCE ADDRESS, and DESTINATION ADDRESS. Seven entries are listed, all categorized as 'flood' with 'critical' severity and 'Session Limit Event' as the threat type. The destination address for all entries is 192.168.50.80.

	RECEIVE TIME	SEVERITY	TYPE	THREAT ID/NAME	SOURCE ADDRESS	DESTINATION ADDRESS
	08/07 16:01:13	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80
	08/07 16:01:04	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80
	08/07 16:00:48	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80
	08/07 16:00:32	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80
	08/07 16:00:30	critical	flood	Session Limit Event	0.0.0.0	192.168.50.53
	08/07 16:00:23	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80
	08/07 16:00:07	critical	flood	Session Limit Event	0.0.0.0	192.168.50.80

Please Note

Several columns have been hidden in this example.

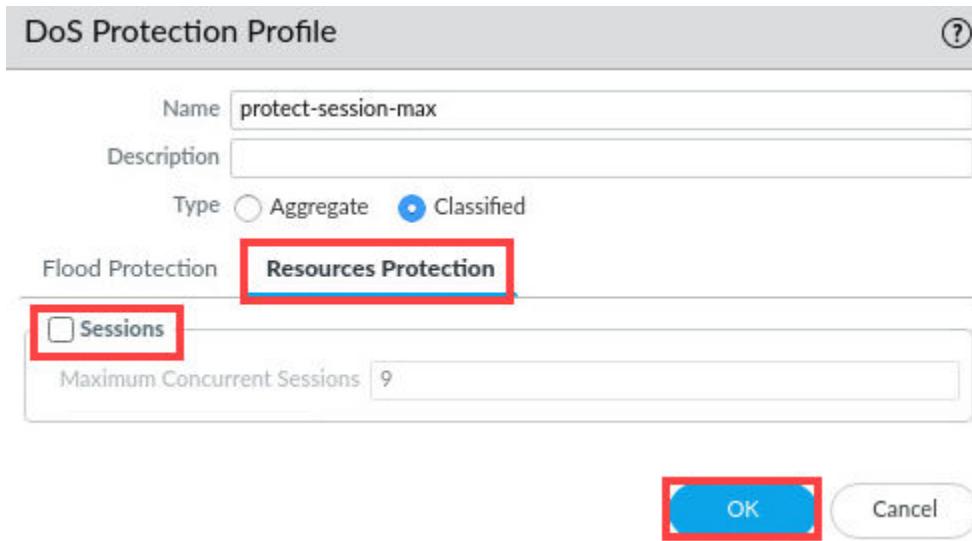
You should see **Session Limit Event** entries in the Threat log because the number of concurrent connection requests to the protected host has exceeded the configured session maximum limit.

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

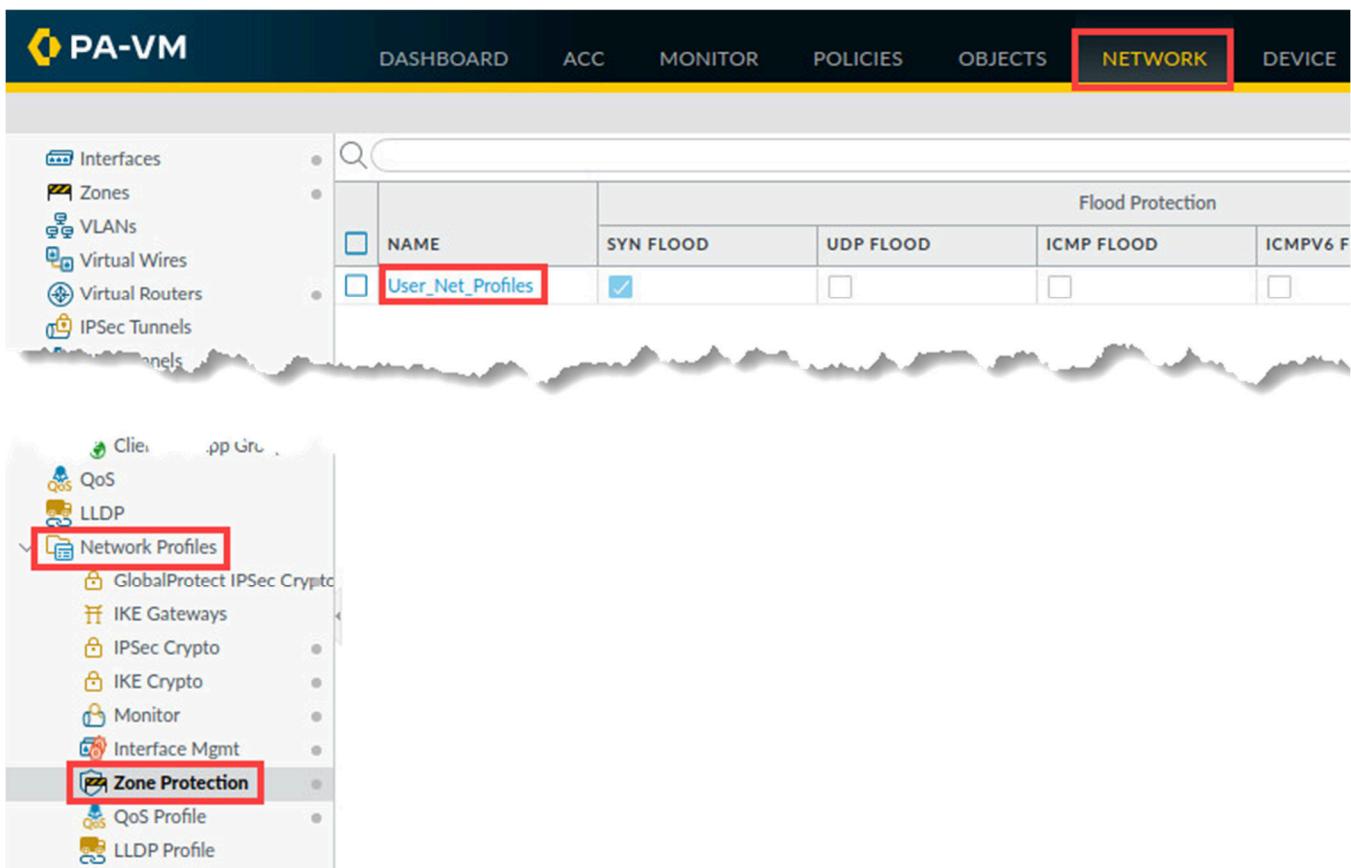
The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. In the left sidebar, 'Security Profiles' is expanded, and 'DoS Protection' is selected, both highlighted with red boxes. The main area displays a table with columns: NAME, LOCATION, TYPE, and SYN FLOOD. One entry named 'protect-session-max' is listed, categorized as 'classified'. There is also a checkbox next to the entry.

	NAME	LOCATION	TYPE	SYN FLOOD
<input type="checkbox"/>	protect-session-max		classified	<input type="checkbox"/>

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

Zone Protection Profile (?)

Name: User_Net_Profiles
Description:
<input checked="" type="checkbox"/> Flood Protection <input type="checkbox"/> Reconnaissance Protection <input type="checkbox"/> Packet Based Attack Protection <input type="checkbox"/> Protocol Protection <input type="checkbox"/> Ethernet SGT Protection
<div style="border: 1px solid #ccc; padding: 5px;"> <input checked="" type="checkbox"/> SYN <div style="margin-top: 5px;"> Action: SYN Cookies Alarm Rate (connections/sec): 1000 Activate (connections/sec): 1100 Maximum (connections/sec): 1300 </div> </div> <div style="margin-top: 10px;"> <input type="checkbox"/> ICMP <div style="margin-top: 5px;"> Alarm Rate (connections/sec): 10000 Activate (connections/sec): 10000 Maximum (connections/sec): 40000 </div> </div> <div style="margin-top: 10px;"> <input type="checkbox"/> Other IP <div style="margin-top: 5px;"> Alarm Rate (connections/sec): 10000 Activate (connections/sec): 10000 Maximum (connections/sec): 40000 </div> </div> <div style="margin-top: 10px;"> <input type="checkbox"/> ICMPv6 <div style="margin-top: 5px;"> Alarm Rate (connections/sec): 10000 Activate (connections/sec): 10000 </div> </div>

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**.

Zone Protection Profile

Name		User_Net_Profiles	Description	
Flood Protection		Reconnaissance Protection	Packet Based Attack Protection Protocol Protection Ethernet SGT Protection	
SCAN	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)
TCP Port Scan	<input type="checkbox"/>	block-ip	2	2
Host Sweep	<input type="checkbox"/>	alert	10	100
UDP Port Scan	<input type="checkbox"/>	alert	2	100

0 items X

SOURCE ADDRESS EXCLUSION ADDRESS TYPE IP ADDRESS(ES)

Add Delete

OK Cancel

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

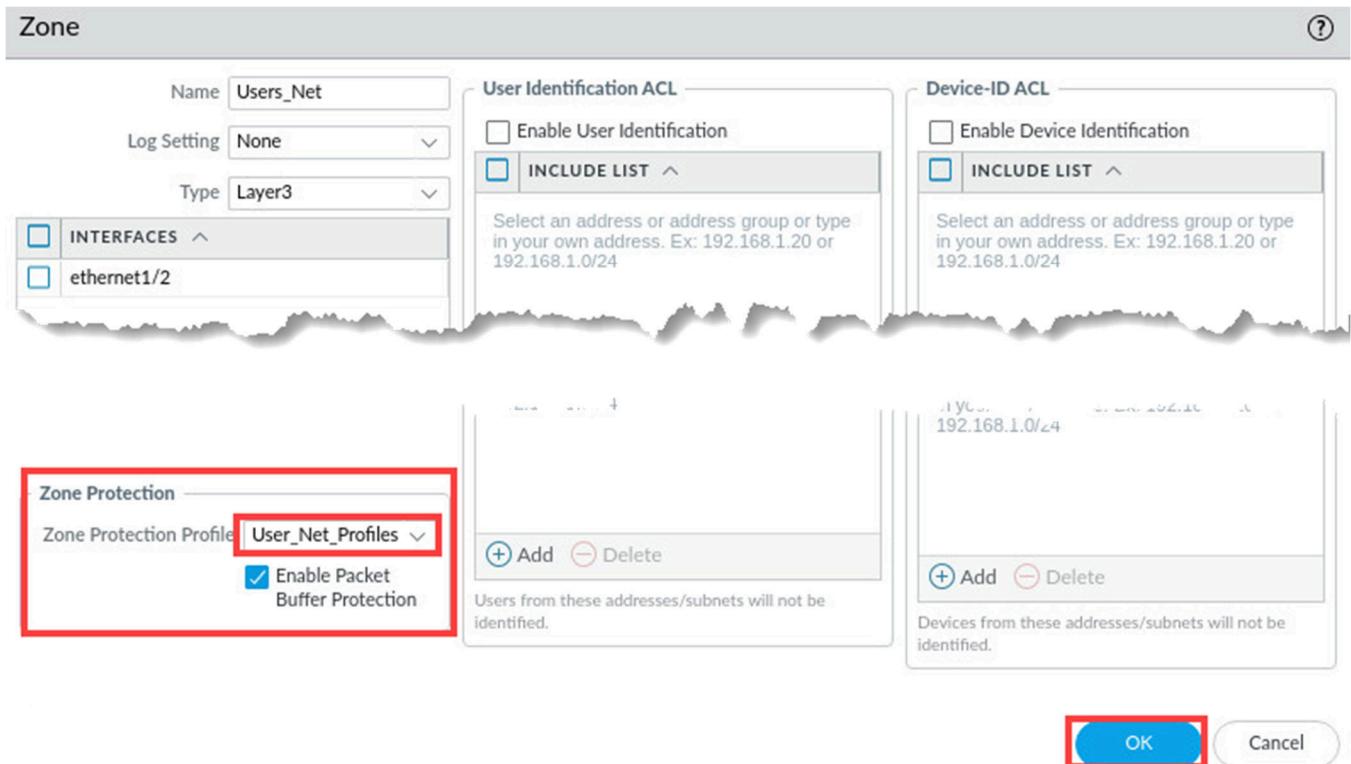
PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE

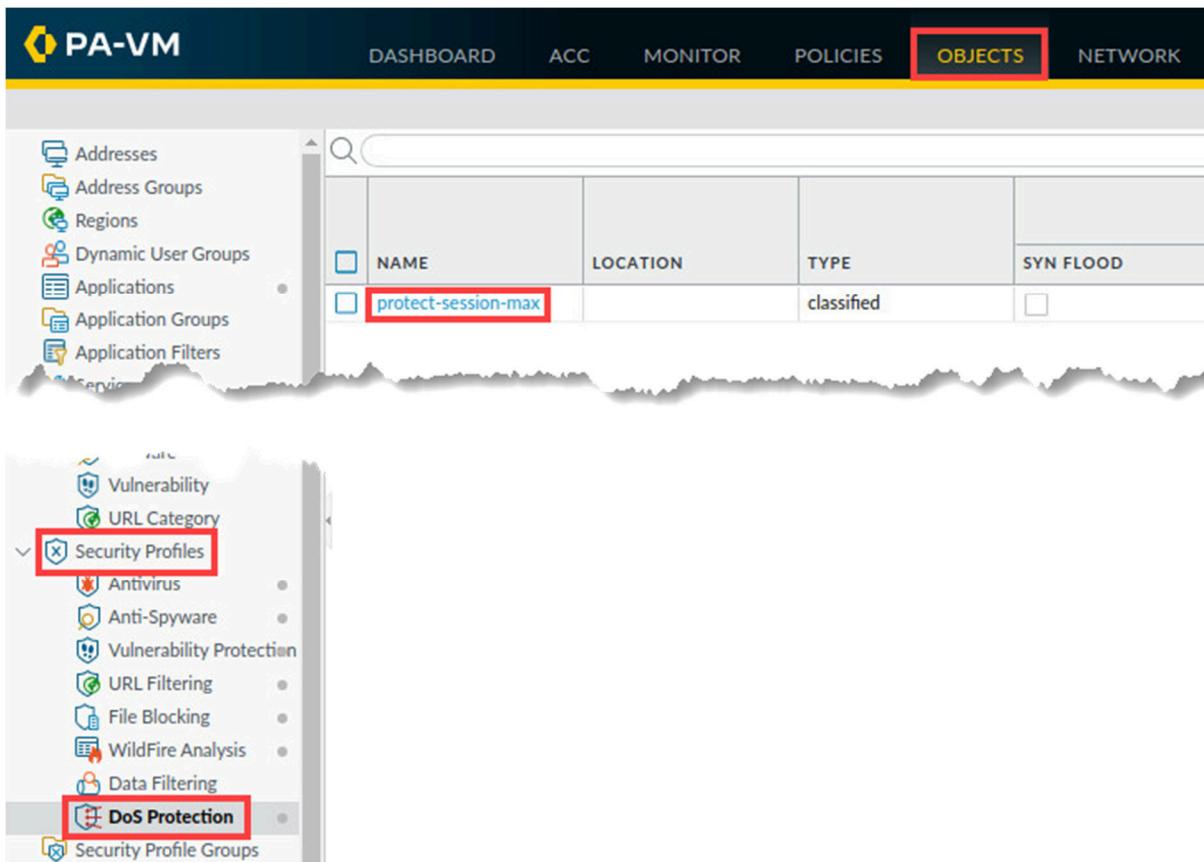
Interfaces Zones VLANs Virtual Wires Virtual Routers IPSec Tunnels GRE Tunnels DHCP DNS Proxy

<input type="checkbox"/> NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING
<input type="checkbox"/> Extranet	layer3	ethernet1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> Internet	layer3	ethernet1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> Users_Net	layer3	ethernet1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

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

DoS Protection Profile (?)

Name Description

Type Aggregate Classified

Flood Protection Resources Protection

SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

SYN Flood

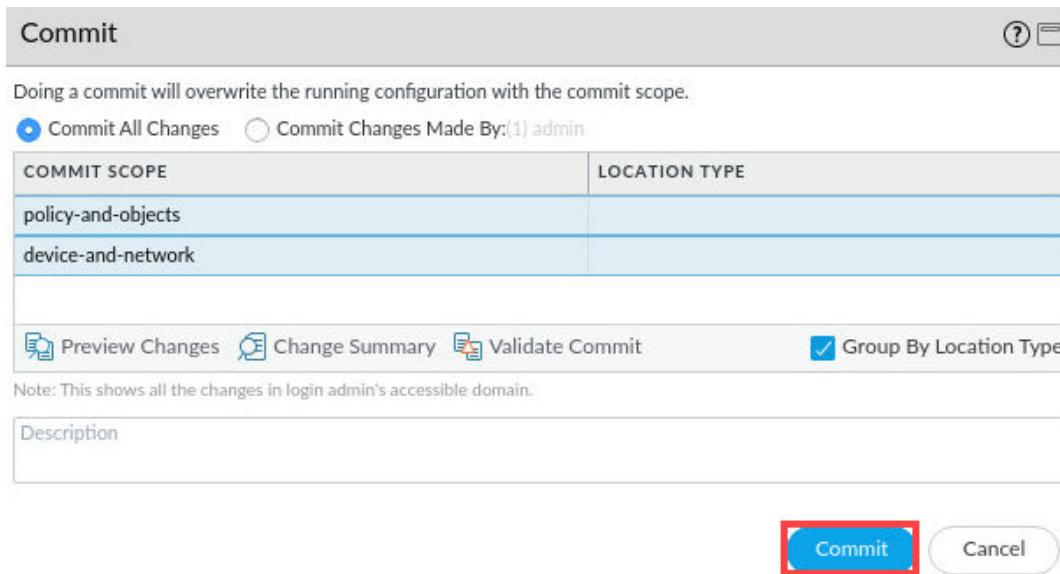
Action	SYN Cookies
Alarm Rate (connections/s)	5
Activate Rate (connections/s)	10
Max Rate (connections/s)	20
Block Duration (s)	300

OK **Cancel**

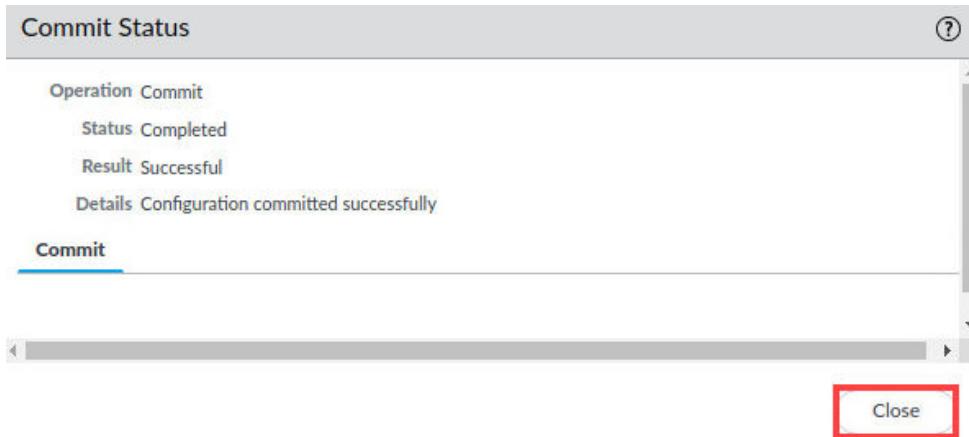
36. Click the **Commit** button at the upper-right of the web interface.



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



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



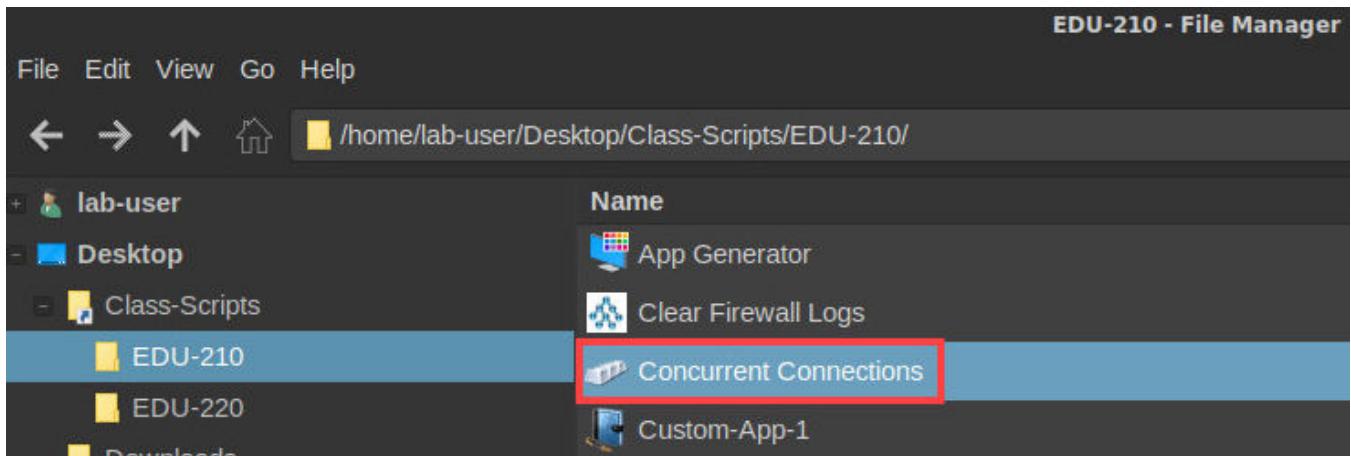
39. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.



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

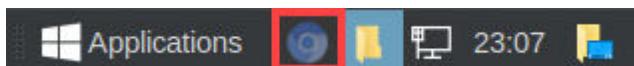
The exact syntax for this command is:

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.

The screenshot shows a terminal window titled "Terminal". It displays the following text:
"#####
Generate Multiple Connections to Target ##
#####"
"This script opens multiple TCP connections to the target server.
Press ENTER to start or CTRL+C to quit."
A red box highlights the text "## Allow this script to run for about three minutes ##".
The text "Then use CTRL+C to stop the process." is below the red box.
"===== "
"sudo nmap --script http-slowloris --max-parallelism 10 192.168.50.80
Starting Nmap 7.60 (https://nmap.org) at 2021-08-07 11:25 EDT
[
[

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*.

The screenshot shows the PA-VM interface with the MONITOR tab selected. On the left, a sidebar lists various monitoring categories: Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, and Decryption. The Threat category is highlighted with a red box. The main area displays a table of threat logs. The columns are: RECEIVE TIME, SEVERITY, FROM ZONE, TO ZONE, TYPE, THREAT ID/NAME, SOURCE ADDRESS, DESTINATION ADDRESS, and ACTION. There are five entries in the table, all categorized as 'flood' type threats with 'critical' severity, originating from 'Users_Net' and targeting 'Extranet'. The destination address is '192.168.50.80' and the action taken is 'drop'.

	RECEIVE TIME	SEVERITY	FROM ZONE	TO ZONE	TYPE	THREAT ID/NAME	SOURCE ADDRESS	DESTINATION ADDRESS	ACTION
	08/08 02:35:58	critical	Users_Net	Extranet	flood	TCP Flood	0.0.0	192.168.50.80	drop
	08/08 02:35:52	critical	Users_Net	Extranet	flood	TCP Flood	0.0.0	192.168.50.80	drop
	08/08 02:35:46	critical	Users_Net	Extranet	flood	TCP Flood	0.0.0	192.168.50.80	drop
	08/08 02:35:40	critical	Users_Net	Extranet	flood	TCP Flood	0.0.0	192.168.50.80	drop
	08/08 02:35:34	critical	Users_Net	Extranet	flood	TCP Flood	0.0.0	192.168.50.80	drop

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.