



NETLAB+



PALO ALTO NETWORKS EDU 210

Lab 7: Blocking Threats from Known-Bad Sources

Document Version: 2022-08-29

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
7 Block Threats from Known-Bad Sources	6
7.1 Apply a Baseline Configuration to the Firewall	6
7.2 Test Access to Know Malicious IP Addresses	11
7.3 Block Access to Malicious IP Addresses Using Address Objects	14
7.4 Block Access to Malicious IP Addresses Using Address Groups	23
7.5 Block Access to Malicious IP Addresses by Geographic Region	29
7.6 Block Access to Malicious IP Addresses Using EDLs	33
7.7 Block Access to Malicious Domains Using an EDL	44
7.8 Add the Domain List EDL to an Anti-Spyware Profile	48
7.9 Add the Anti-Spyware Profile to a Security Policy Rule	51
7.10 Block Access to Malicious URLs Using the Security Policy	55
7.11 Create a Custom URL Category	64
7.12 Create an EDL to Block Malicious URL Access	70
7.13 Block Access to a Malicious URL Using a URL Filtering Profile	78

Introduction

You need to make certain that the firewall blocks traffic, both to and from known malicious IP addresses, hostnames, and domain names. There are numerous external blocklists that you may want to implement on the Palo Alto Networks firewall. You also need to implement your own custom lists of IP addresses, hostnames, and domain names to block traffic based on various corporate policies. Upper management is also concerned that some users have been accessing inappropriate web content from their corporate devices. You need to configure the firewall to block browsing to certain categories of web traffic, including adult and nudity.

You are concerned about users accessing websites that are often the source of malicious files and content, such as viruses and spyware.

In this section, you will explore the options available on the firewall that allow you to block individual addresses, groups of addresses, and lists of addresses. You will also configure the firewall to block certain categories of websites.

Objective

In this lab, you will perform the following tasks:

- Load a baseline configuration
- Block access to malicious IP addresses using address objects
- Block access to malicious IP addresses using address Groups
- Block access to malicious IP addresses using geographic regions
- Block access to malicious IP addresses using an External Dynamic List (EDL)
- Block access to malicious domains using an EDL
- Block access to malicious URLs using the security policy
- Block access to a malicious URL using a URL filtering profile

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!

7 Block Threats from Known-Bad Sources

7.1 Apply a Baseline Configuration to the Firewall

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

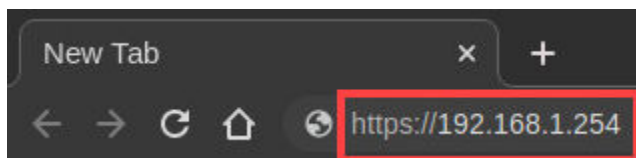
1. Click on the **Client** tab to access the *Client PC*.



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



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



4. You will see a “*Your connection is not private*” message. 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.

- 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.

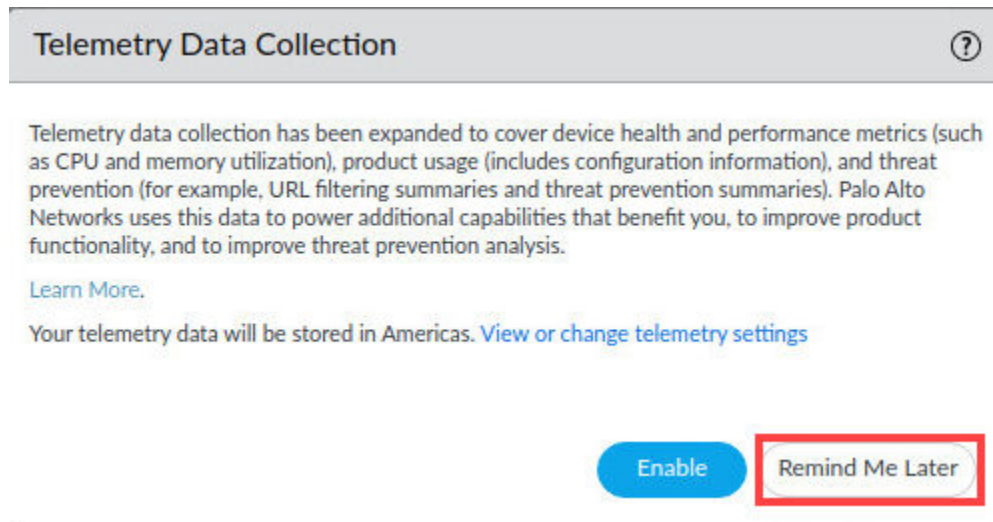
[Proceed to 192.168.1.254 \(unsafe\)](#)

- Log in to the firewall web interface as username **admin**, password **Pa10Alt0!**.



The image shows the Palo Alto Networks login interface. It features the Palo Alto Networks logo at the top. Below the logo, there are two input fields: the first is for the username, which contains the text "admin", and the second is for the password, which is masked with dots. A blue "Log In" button is positioned below the password field. The entire login area is enclosed in a yellow border.

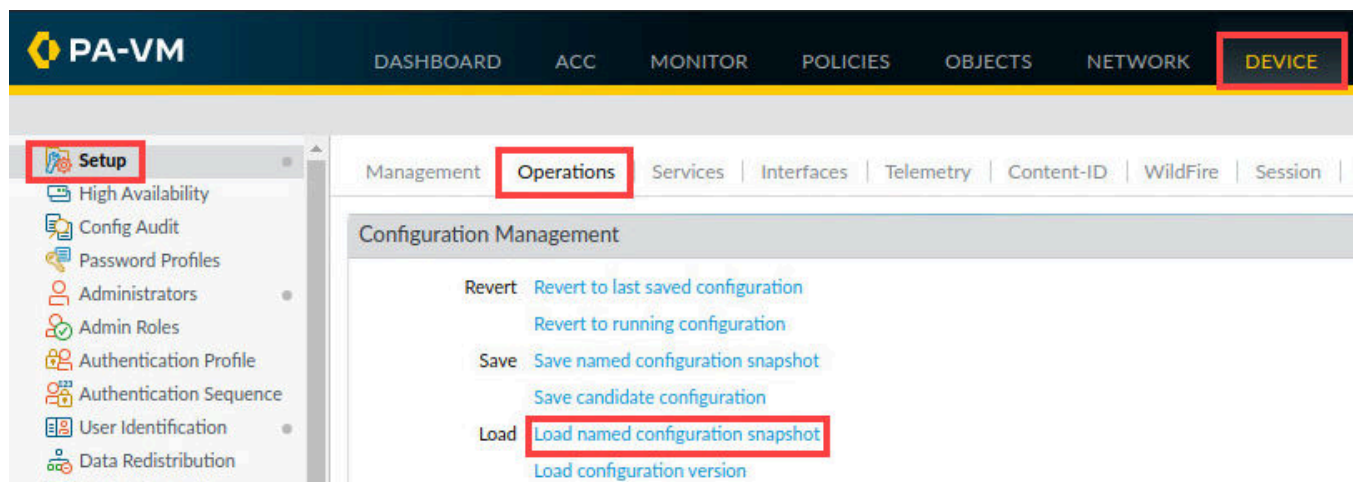
7. In the *Telemetry Data Collection* pop-up, click **Remind Me Later**.



Please Note

Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

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

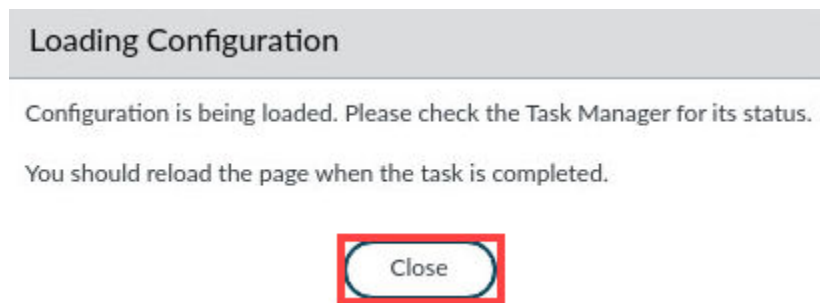


9. In the *Load Named Configuration* window, select **edu-210-lab-07.xml** from the *Name* dropdown box and click **OK**.



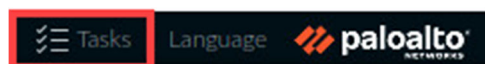
The 'Load Named Configuration' dialog box has a title bar with a question mark icon. It contains a 'Name' dropdown menu with 'edu-210-lab-07.xml' selected, a 'Decryption Key' dropdown menu with four asterisks, and two checkboxes: 'Regenerate Rule UUIDs for selected named configuration' and 'Skip Validation'. At the bottom right are 'OK' and 'Cancel' buttons.

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



The 'Loading Configuration' dialog box has a title bar. The main text reads: 'Configuration is being loaded. Please check the Task Manager for its status.' and 'You should reload the page when the task is completed.' At the bottom center is a 'Close' button.

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



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

Task Manager - All Tasks

8 items

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

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



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

Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

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

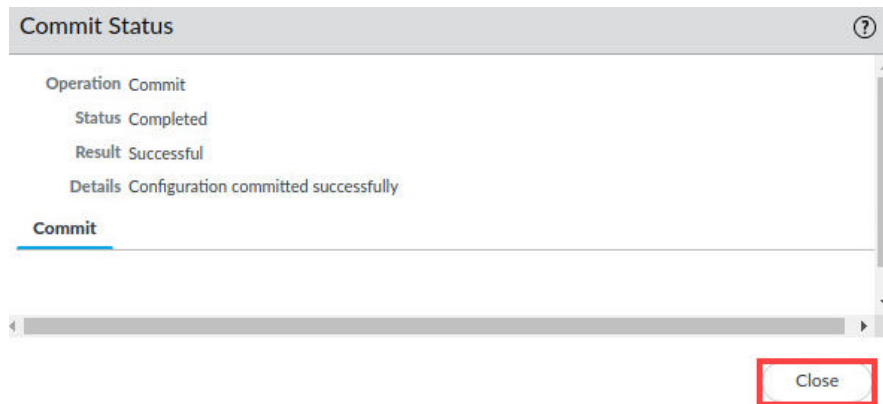
[Preview Changes](#)
[Change Summary](#)
[Validate Commit](#)
☒ Group By Location Type

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

Description

Commit Cancel

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



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

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

7.2 Test Access to Known Malicious IP Addresses

You can use security policy rules to block access to known malicious IP addresses. Because the list of malicious IP addresses can quickly change, you will treat two legitimate IP addresses as though they are malicious and block access to them.

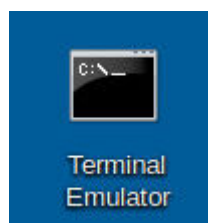
Please Note

Although you can block access to specific IP addresses, Palo Alto Networks recommends that you use a positive enforcement model whenever possible. Use of a positive enforcement model means that you configure a security policy to pass what is allowed rather than what should be blocked, with the assumption that anything not specifically allowed is blocked by default.

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

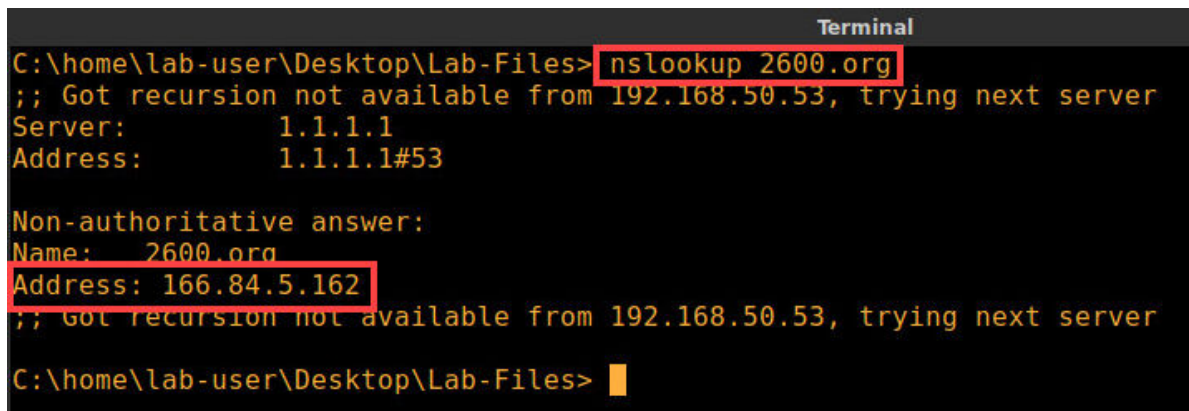


2. On the *client desktop*, open a *terminal* window by double-clicking **Terminal Emulator**.



3. Enter the command below to obtain the IP Address of 2600.org. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup 2600.org
```



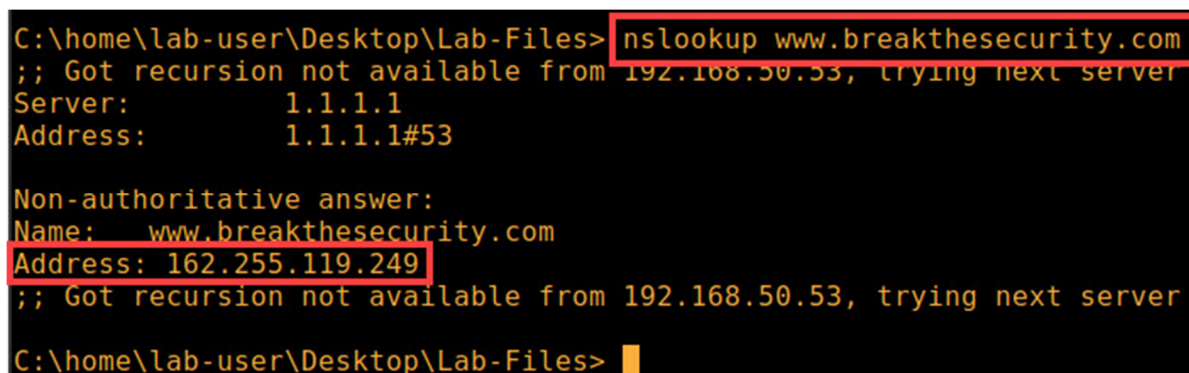
```
Terminal
C:\home\lab-user\Desktop\Lab-Files> nslookup 2600.org
;; Got recursion not available from 192.168.50.53, trying next server
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
Name:   2600.org
Address: 166.84.5.162
;; Got recursion not available from 192.168.50.53, trying next server

C:\home\lab-user\Desktop\Lab-Files> █
```

4. In the same **CMD** window, enter the command below. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup www.breakthesecurity.com
```



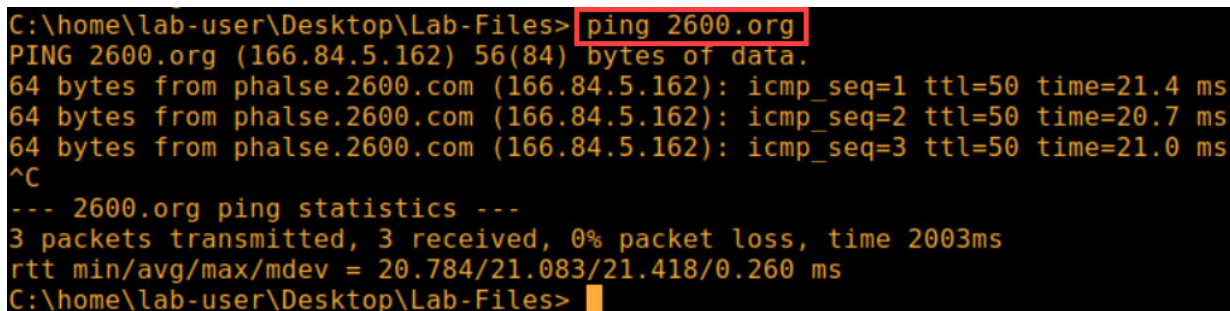
```
C:\home\lab-user\Desktop\Lab-Files> nslookup www.breakthesecurity.com
;; Got recursion not available from 192.168.50.53, trying next server
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
Name:   www.breakthesecurity.com
Address: 162.255.119.249
;; Got recursion not available from 192.168.50.53, trying next server

C:\home\lab-user\Desktop\Lab-Files> █
```

5. In the same **CMD** window, verify connectivity to the websites by entering the commands below. You will **ping** two IP Addresses. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```



```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org
PING 2600.org (166.84.5.162) 56(84) bytes of data:
64 bytes from phalse.2600.com (166.84.5.162): icmp_seq=1 ttl=50 time=21.4 ms
64 bytes from phalse.2600.com (166.84.5.162): icmp_seq=2 ttl=50 time=20.7 ms
64 bytes from phalse.2600.com (166.84.5.162): icmp_seq=3 ttl=50 time=21.0 ms
^C
--- 2600.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 20.784/21.083/21.418/0.260 ms
C:\home\lab-user\Desktop\Lab-Files> █
```



```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=1 ttl=46 time=120 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=2 ttl=46 time=124 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=3 ttl=46 time=133 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=4 ttl=46 time=128 ms
^C
--- www.breakthesecurity.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 120.138/126.615/133.107/4.823 ms
C:\home\lab-user\Desktop\Lab-Files>
```

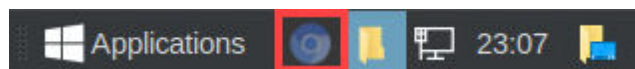
**Please
Note**

Here, pinging *2600.org* and *breakthesecurity.com* will be successful.
Access will be blocked in the next tasks.

6. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.



7. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.



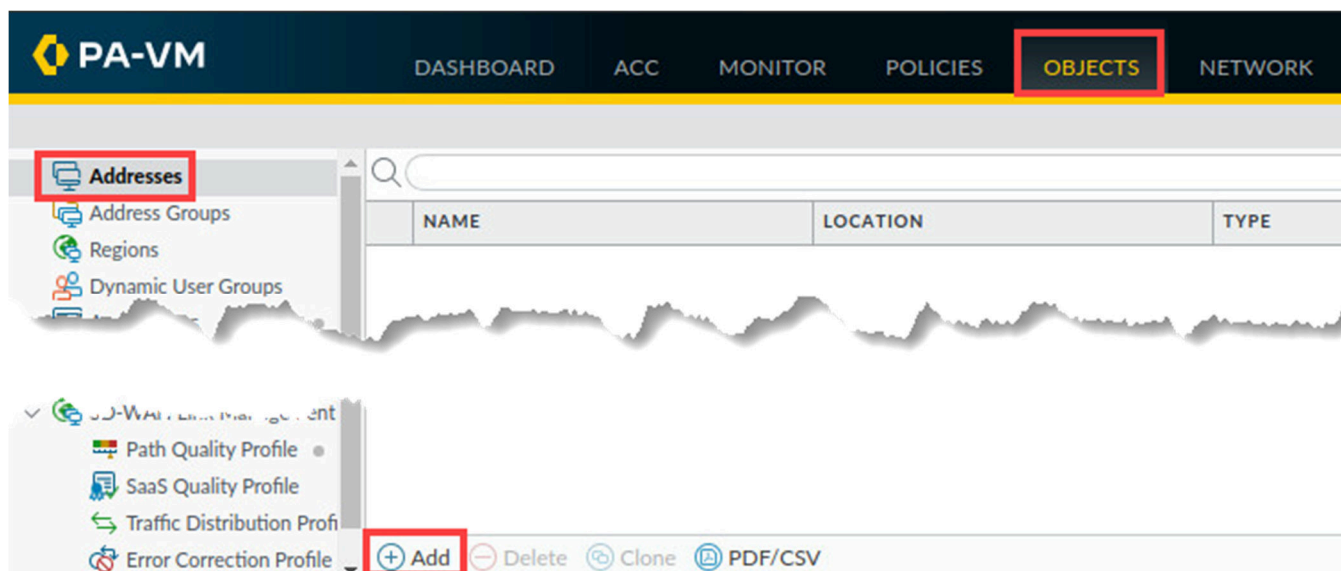
7.3 Block Access to Malicious IP Addresses Using Address Objects

Be aware that the list of malicious IP addresses quickly changes, so keeping your Address objects current could be problematic. For this reason, later lab exercises will illustrate more automated methods to block the current list of malicious IP addresses.

In this section, you will create an Address object that contains a list of malicious IP addresses. You will use this Address object in the security policy to block access to the malicious IP addresses.

Lastly, you will test access to the IP Addresses contained in the Address Objects.

1. In the *PA-VM* interface, select **Objects > Addresses**. Click **Add**.



2. In the *Address* window, configure the following. Click **OK**.

Parameter	Value
Name	malicious-ip-address-1
Description	2600.org IP address
Type	IP Netmask
(address text box)	<IP_address_of_2600.org>

Address

Name

malicious-ip-address-1

Description

2600.org IP address

Type

IP Netmask

166.84.5.162

Resolve

Tags

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

OK

Cancel

Please
Note

Note that the IP address you enter may be different from the previous example.

3. In the *Addresses* window, click **Add**.



4. In the *Address* window, configure the following. Click **Resolve**.

Parameter	Value
Name	malicious-fqdn-1
Description	www.breakthesecurity.com
Type	FQDN
(FQDN text box)	www.breakthesecurity.com

Address ⓘ

Name: malicious-fqdn-1

Description: www.breakthesecurity.com

Type: FQDN (dropdown) | www.breakthesecurity.com (text box) **Resolve**

Tags: (dropdown)

OK **Cancel**

5. Once you click **Resolve**, you will be prompted to select **Use this Address**.

www.breakthesecurity.com **Resolve**

162.255.119.249 **Use this address**

ipv6 not resolved

6. In the *Address* window, click **OK**.

Address ⓘ

Name: malicious-fqdn-1

Description: www.breakthesecurity.com

Type: IP Netmask (dropdown) | 162.255.119.249 (text box) **Resolve**

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

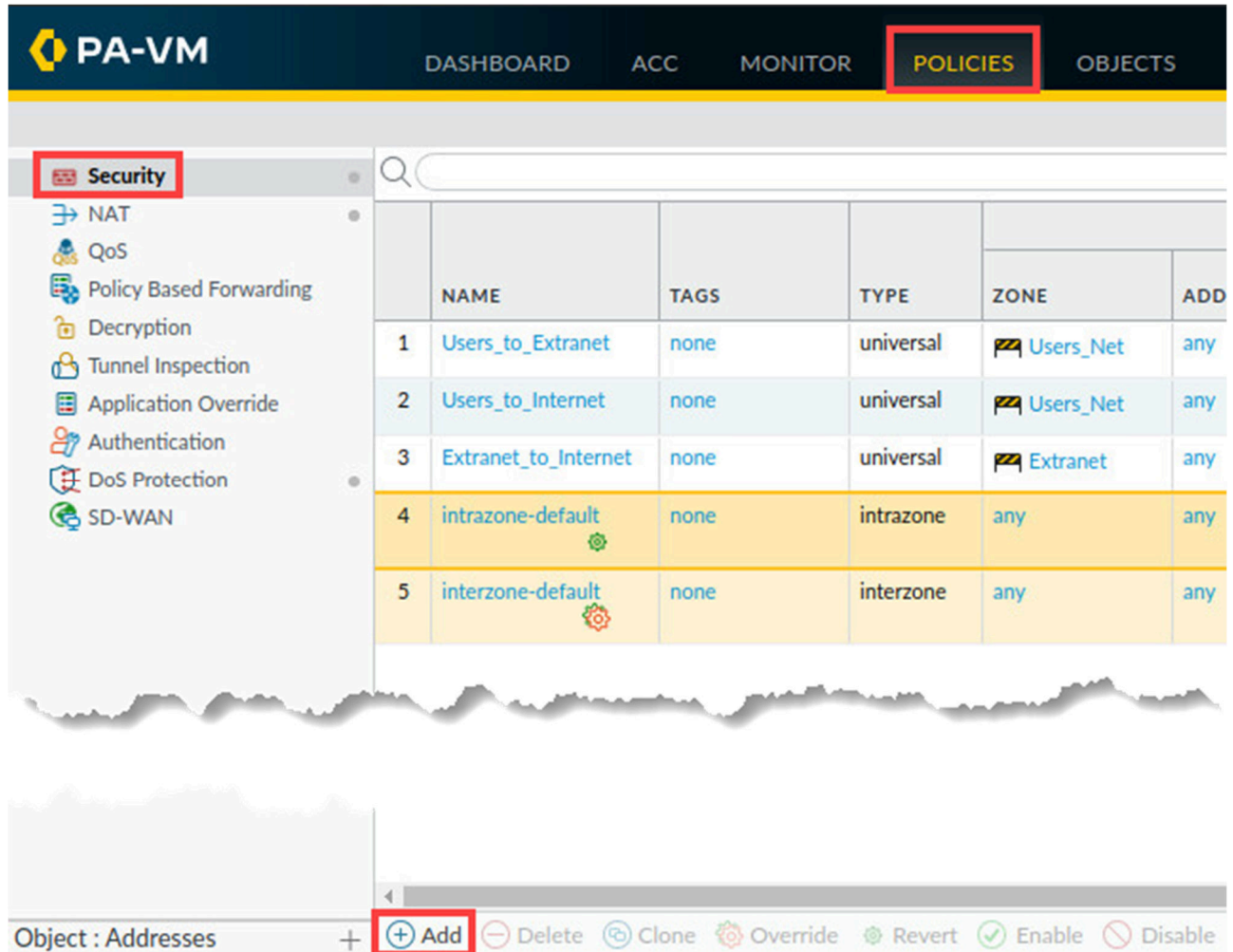
Tags: (dropdown)

OK **Cancel**

7. Confirm the *address* objects appear in the *Addresses* window.

	NAME	LOCATION	TYPE	ADDRESS
<input type="checkbox"/>	malicious-fqdn-1		IP Netmask	162.255.119.249
<input type="checkbox"/>	malicious-ip-address-1		IP Netmask	166.84.5.162

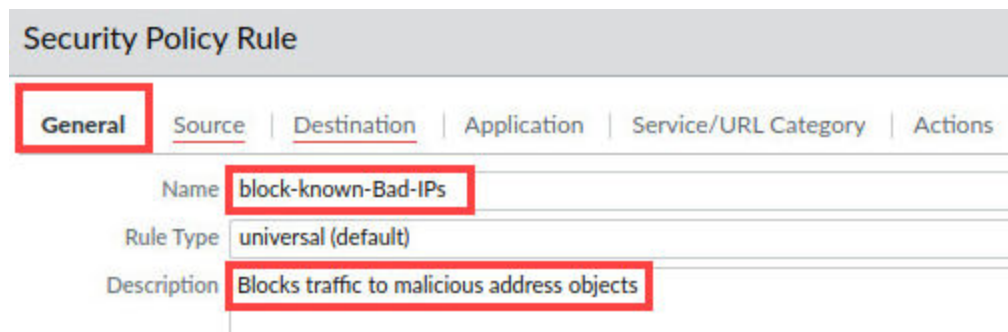
8. Select **Policies > Security**. Click **Add** to create a new security policy rule.



	NAME	TAGS	TYPE	ZONE	ADD
1	Users_to_Extranet	none	universal	Users_Net	any
2	Users_to_Internet	none	universal	Users_Net	any
3	Extranet_to_Internet	none	universal	Extranet	any
4	intrazone-default	none	intrazone	any	any
5	interzone-default	none	interzone	any	any

Object : Addresses + **Add** Delete Clone Override Revert Enable Disable

9. In the *Security Policy Rule* window, on the *General* tab, type **Block-Known-Bad-IPs** as the *Name*. For *Description*, enter **Blocks traffic to malicious address objects**.



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Name: **block-known-Bad-IPs**

Rule Type: universal (default)

Description: **Blocks traffic to malicious address objects**

10. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	Add Users_Net and Extranet
Source Address	Any

Security Policy Rule

General **Source** Destination Application Service/URL Category Actions

☐ Any

☐ SOURCE ZONE ^

☐ Users_Net

☒ Extranet

☐ SOURCE ADDRESS ^

☒ Any

☐ Add

☐ Negate

11. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	Add Internet
Destination Address	Add malicious-fqdn-1 and malicious-ip-address-1

Security Policy Rule

General Source **Destination** Application Service/URL Category Actions

☐ DESTINATION ZONE ^

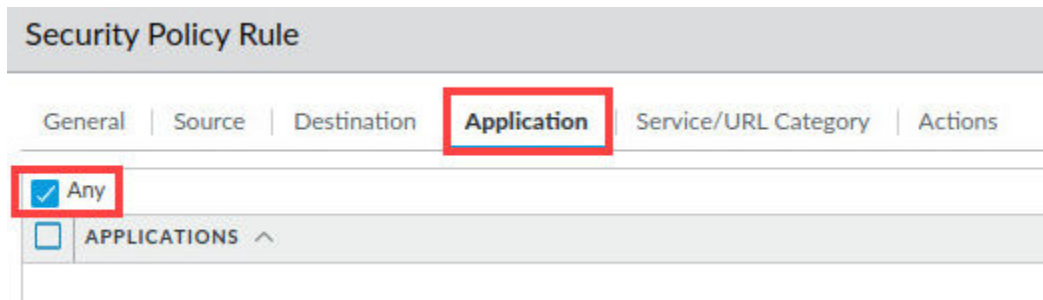
☒ Internet

☐ DESTINATION ADDRESS ^

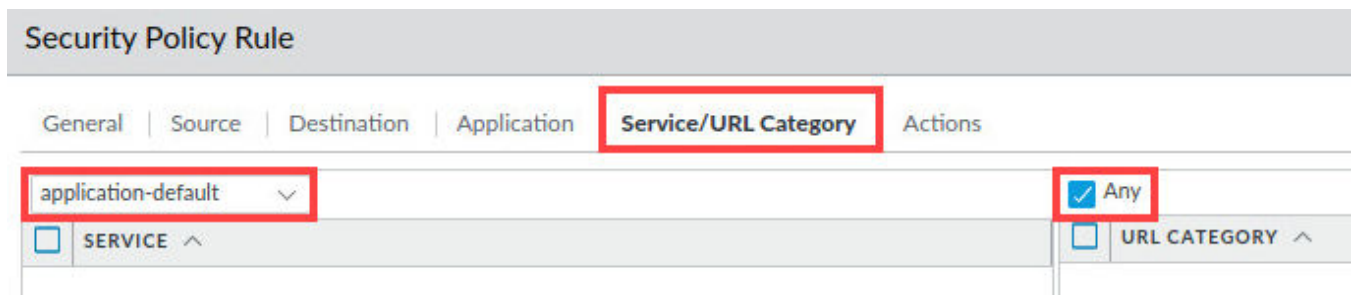
☐ malicious-fqdn-1

☒ malicious-ip-address-1

12. Click the **Application** tab and verify that **Any** is selected.

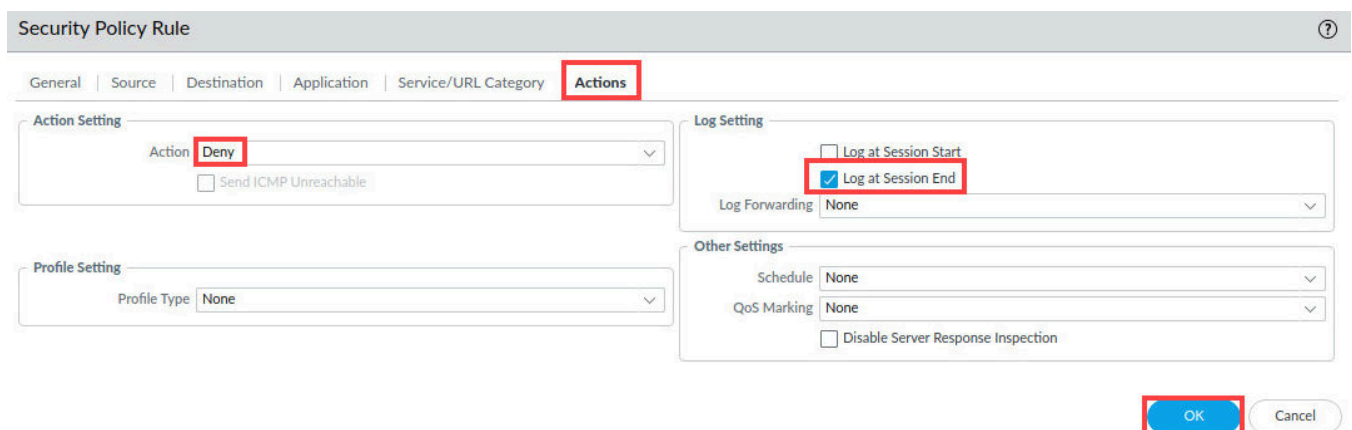


13. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.










14. Click the **Actions** tab and configure the following. Click **OK**.

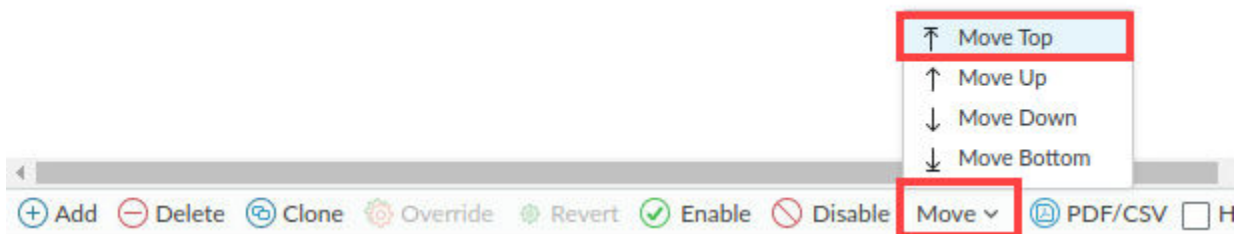
Parameter	Value
Action	Deny
Log Setting	Log at Session End










15. Select, but do not open, the **Block-Known-Bad-IPs** rule in the security policy.

	NAME	TAGS	TYPE	Source	
				ZONE	ADDRESS
1	Users_to_Extranet	none	universal	 Users_Net	any
2	Users_to_Internet	none	universal	 Users_Net	any
3	Extranet_to_Internet	none	universal	 Extranet	any
4	Block-known-Bad-IPs	none	universal	 Extranet  Users_Net	any
5	intrazone-default 	none	intrazone	any	any
6	interzone-default 	none	interzone	any	any

16. At the bottom of the window, select **Move > Move Top** to move the rule to the top of the security policy.



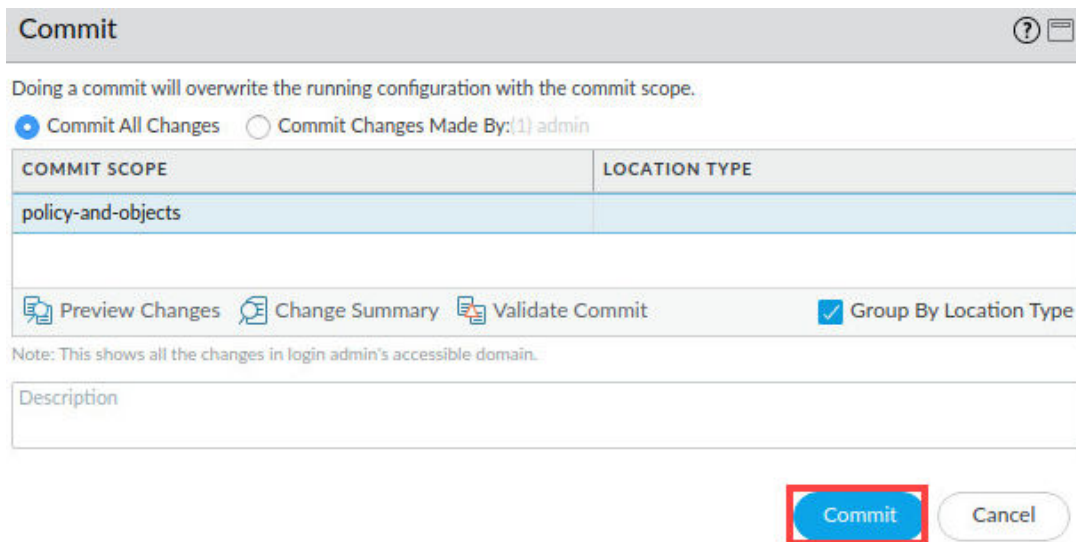
17. Verify that the **Block-Known-Bad-IPs** rule is rule number 1.

	NAME	TAGS	TYPE	Source	
				ZONE	ADDRESS
1	Block-known-Bad-IPs	none	universal	 Extranet  Users_Net	any
2	Users_to_Extranet	none	universal	 Users_Net	any
3	Users_to_Internet	none	universal	 Users_Net	any
4	Extranet_to_Internet	none	universal	 Extranet	any
5	intrazone-default 	none	intrazone	any	any
6	interzone-default 	none	interzone	any	any

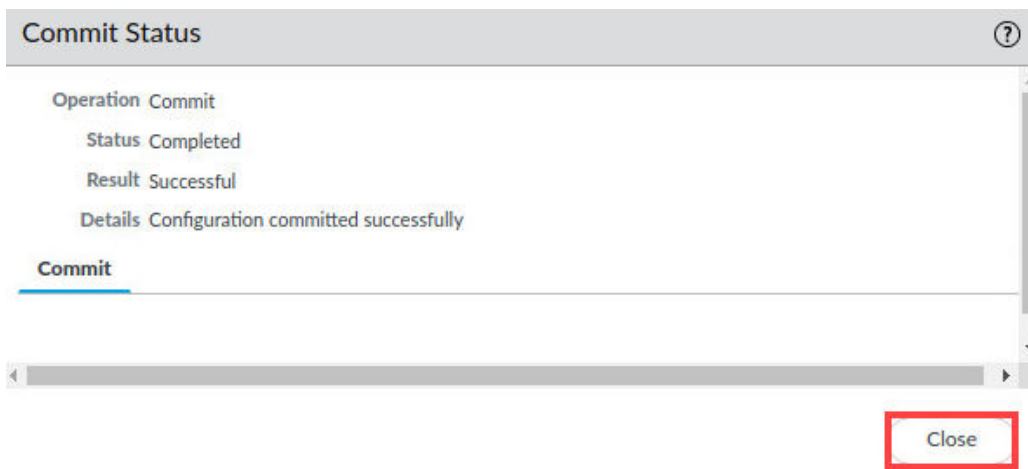
18. Click the **Commit** button at the upper-right of the web interface.



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



23. From the *terminal* window on the *desktop*, enter the following commands. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org
PING 2600.org (166.84.5.162) 56(84) bytes of data.
^C
--- 2600.org ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10227ms
C:\home\lab-user\Desktop\Lab-Files>
```

Please
Note

Pinging 2600.org will fail.

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
^C
--- www.breakthesecurity.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms
C:\home\lab-user\Desktop\Lab-Files>
```

Please
Note

Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the Address objects in the Security policy.

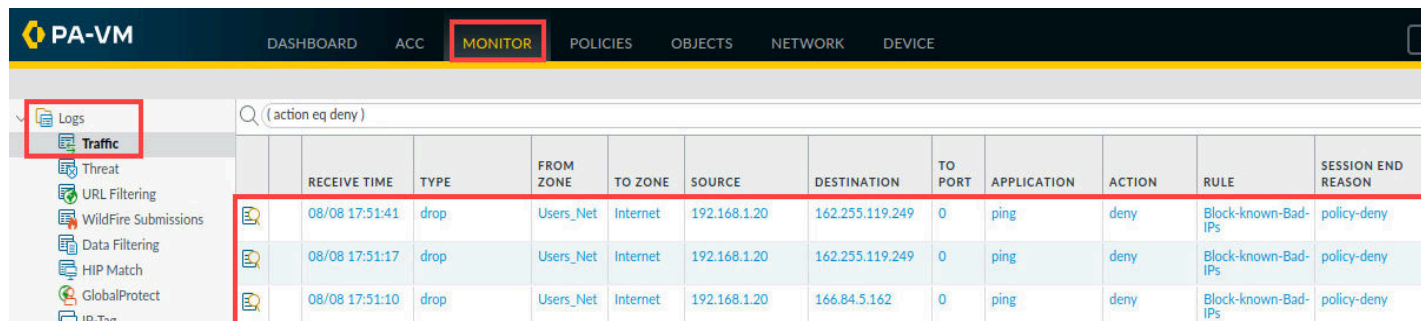
24. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.



25. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.



26. Navigate to **Monitor > Logs > Traffic**. Enter the filter (**action eq deny**) in the *Filter builder* to look for traffic that has been denied. You should see entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.



	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	08/08 17:51:41	drop	Users_Net	Internet	192.168.1.20	162.255.119.249	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 17:51:17	drop	Users_Net	Internet	192.168.1.20	162.255.119.249	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 17:51:10	drop	Users_Net	Internet	192.168.1.20	166.84.5.162	0	ping	deny	Block-known-Bad-IPs	policy-deny

Please Note

Note some columns have been adjusted to view the information shown in the screen shot.

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

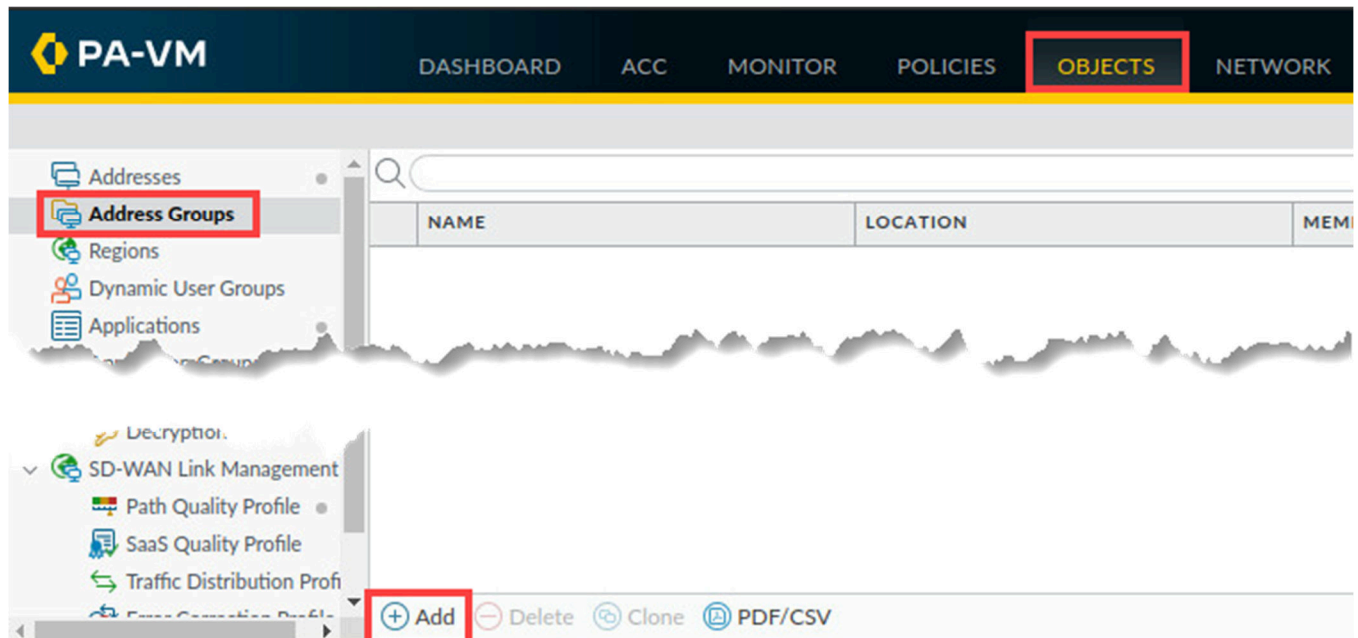
7.4 Block Access to Malicious IP Addresses Using Address Groups

You can use Address Groups in security policy rules to control access to IP addresses. You can group multiple Address objects in an Address Group and then use just the Address Group in your security policy rules. Address Groups are used to shorten and simplify a policy or a policy rule.

You will create a static Address Group, add two Address objects to the group, and then modify the security policy to use the Address Group.

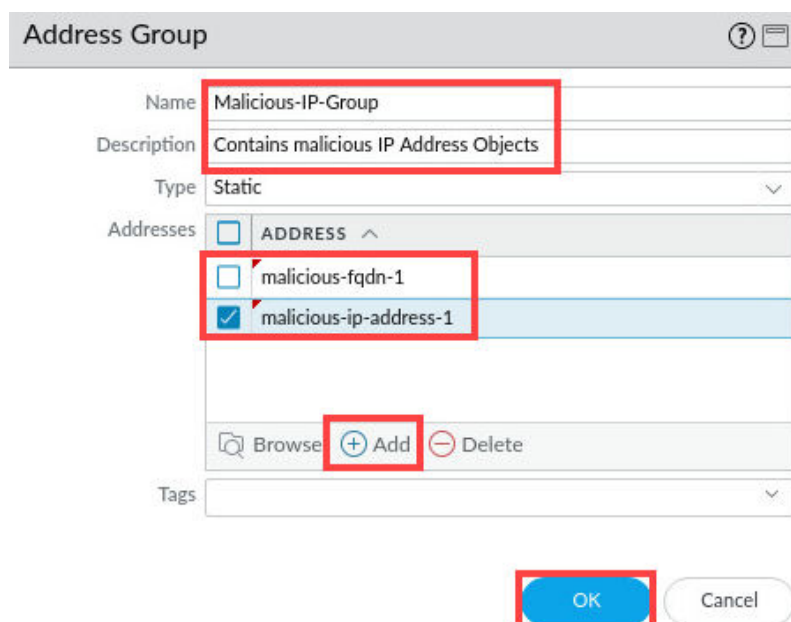
Lastly, you will test access to the IP addresses contained in the Address objects.

1. In the *firewall* interface, select **Objects > Address Groups**. Click **Add**.

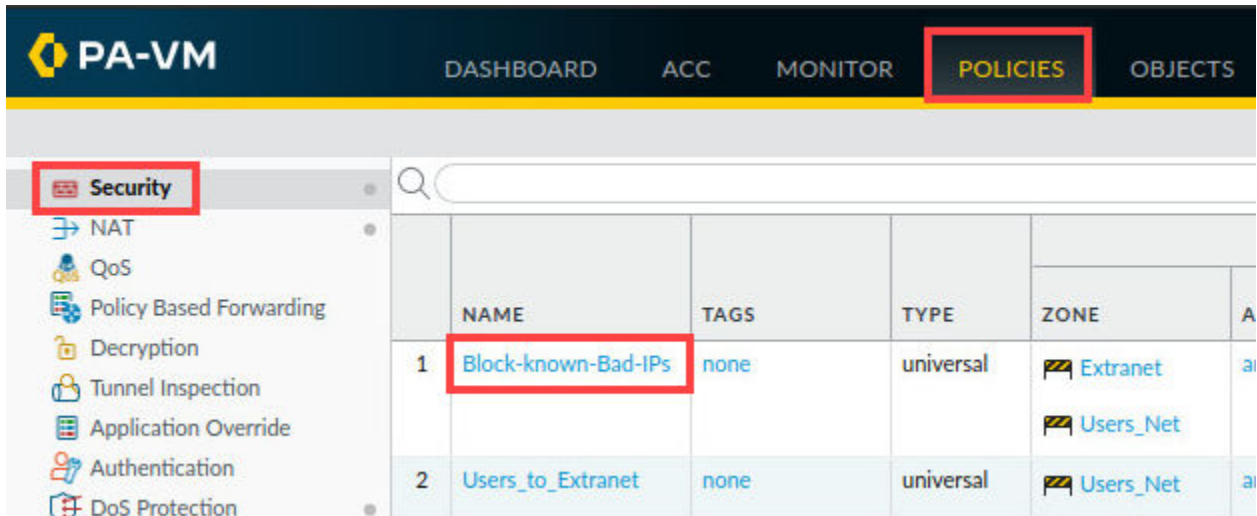


2. In the *Address Group* window, configure the following. Click **OK**.

Parameter	Value
Name	Malicious-IP-Group
Description	Contains malicious IP address objects
Type	Static
Addresses	Add malicious-fqdn-1 and malicious-ip-address-1

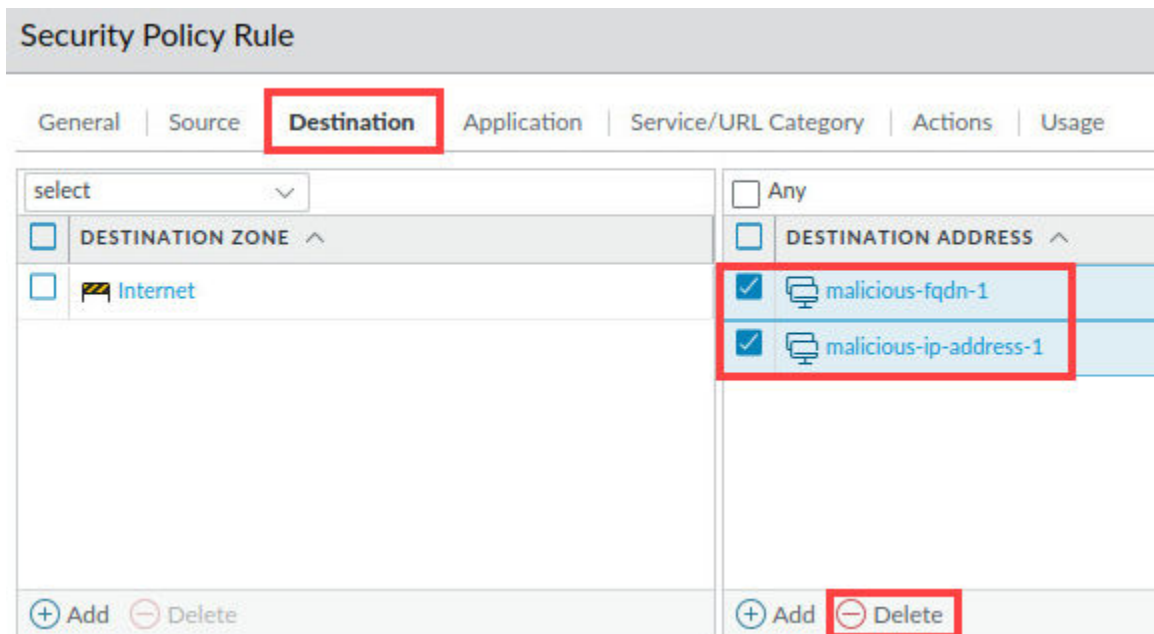


3. Select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.



	NAME	TAGS	TYPE	ZONE	A
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	al
2	Users_to_Extranet	none	universal	Users_Net	al

4. In the *Security Policy Rule* window, **Destination** tab, select the **malicious-fqdn-1** and **malicious-ip-address-1** checkboxes. Click **Delete**.



Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

☐ DESTINATION ZONE ^

☐ Internet

☐ Any

☒ DESTINATION ADDRESS ^

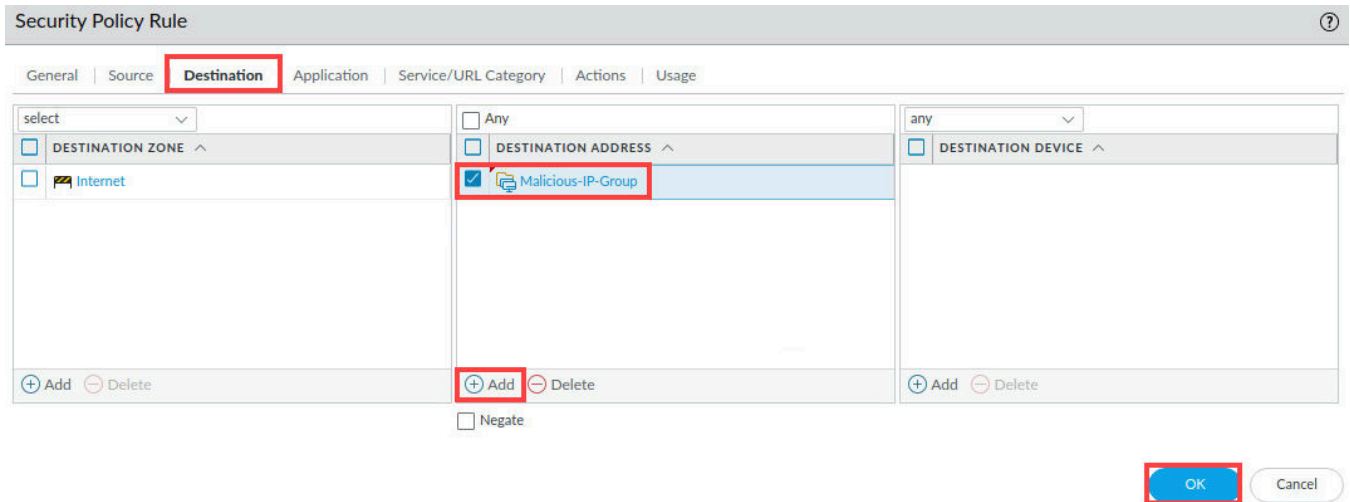
☒ malicious-fqdn-1

☒ malicious-ip-address-1

(+) Add (-) Delete

(+) Add (-) Delete

5. In the *Destination Address* window, click **Add**. Select **Malicious-IP-Group**. Click **OK**.



Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

DESTINATION ZONE ^

Internet

DESTINATION ADDRESS ^

Any

Malicious-IP-Group

DESTINATION DEVICE ^

any

+ Add - Delete

+ Add - Delete

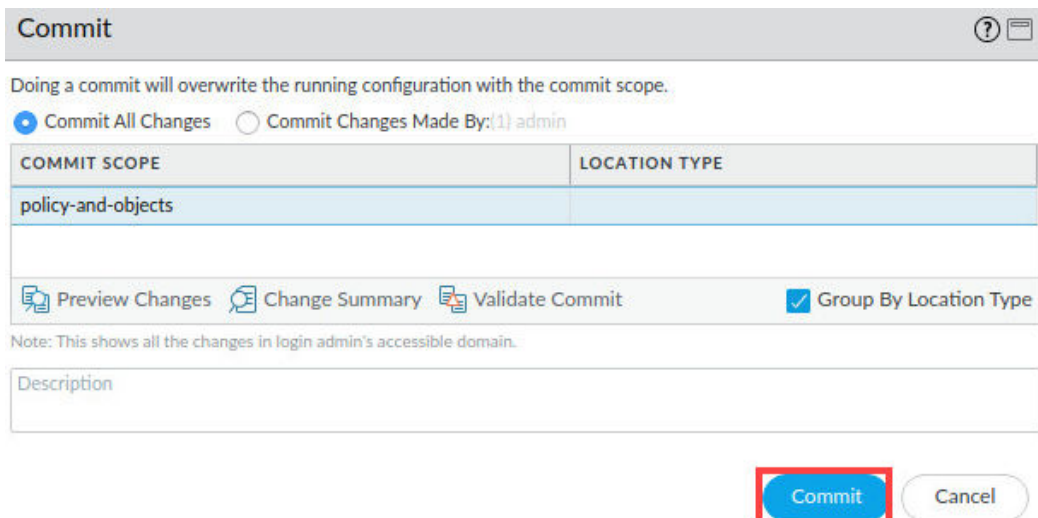
Negate

OK Cancel

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



7. 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
policy-and-objects	

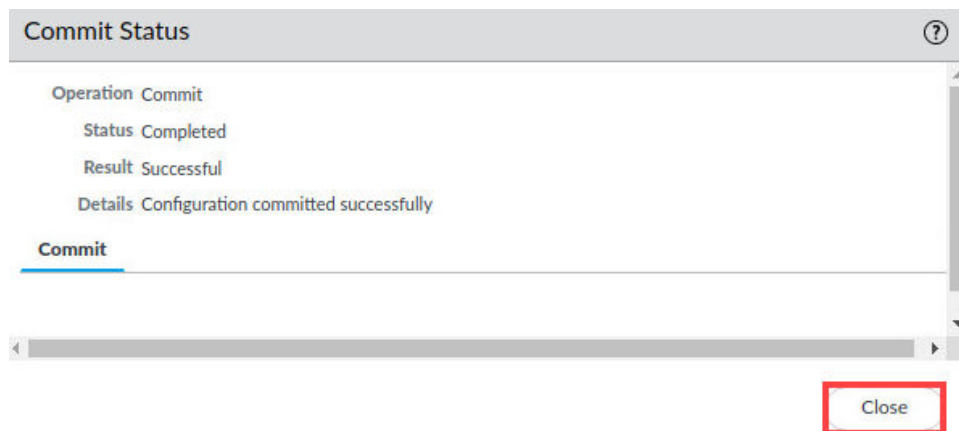
Preview Changes Change Summary Validate Commit ☒ Group By Location Type

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

Description

Commit Cancel

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



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



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



11. From the *terminal* window on the *desktop*, enter the commands below. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 2600.org
PING 2600.org (166.84.5.162) 56(84) bytes of data.
^C
--- 2600.org ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10227ms
C:\home\lab-user\Desktop\Lab-Files>
```

Please
Note

Pinging 2600.org will fail.

```
C:\home\lab-user\
```



```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
^C
--- www.breakthesecurity.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

C:\home\lab-user\Desktop\Lab-Files> █
```

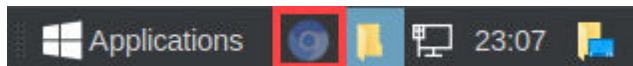
**Please
Note**

Pinging `www.breakthesecurity.com` will fail because access to the IP addresses was blocked by the address objects in the security policy.

12. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.



13. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar. Leave the *firewall* interface open and continue to the next task.



14. Navigate to **Monitor > Logs > Traffic**. Enter the filter (`action eq deny`) in the *filter builder* to look for traffic that has been denied. You should see *additional* entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.

PA-VM												
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE												
Logs	Q ((action eq deny))											
Traffic												
Threat												
URL Filtering												
WildFire Submissions												
Data Filtering												
HIP Match												
GlobalProtect												
IP-Tag												
User-ID												
Device												
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	
	08/08 18:18:48	drop	Users_Net	Internet	192.168.1.20	162.255.119.249	0	ping	deny	Block-known-Bad-IPs	policy-deny	
	08/08 18:18:37	drop	Users_Net	Internet	192.168.1.20	166.84.5.162	0	ping	deny	Block-known-Bad-IPs	policy-deny	
	08/08 17:51:41	drop	Users_Net	Internet	192.168.1.20	162.255.119.249	0	ping	deny	Block-known-Bad-IPs	policy-deny	
	08/08 17:51:17	drop	Users_Net	Internet	192.168.1.20	162.255.119.249	0	ping	deny	Block-known-Bad-IPs	policy-deny	

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

7.5 Block Access to Malicious IP Addresses by Geographic Region

You can block access to IP addresses associated with specific geographic regions. This ability is useful for reducing your attack surface by prohibiting traffic from countries where you have no legitimate business contacts.

In this section, you will configure and test access to the blocked geographic region. After you have tested access, you will restore access to the blocked region.

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



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



3. From the *terminal* window on the *desktop*, enter the command below to obtain the IP Address of 2600.org. Write down the **IP address** or **copy** and paste it into a text document on the *desktop*.

```
C:\home\lab-user\Desktop\Lab-Files> nslookup nic.ir <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> nslookup nic.ir
;; Got recursion not available from 192.168.50.53, trying next server
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
Name:   nic.ir
Address: 194.225.70.16
;; Got recursion not available from 192.168.50.53, trying next server
C:\home\lab-user\Desktop\Lab-Files> █
```

Please
Note

The nic.ir domain is in Iran.

- In the same **CMD** window, verify connectivity to *nic.ir* by entering the command below. Use **Ctrl+C** to stop the ping after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir
PING nic.ir (194.225.70.16) 56(84) bytes of data.
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=1 ttl=45 time=230 ms
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=2 ttl=45 time=228 ms
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=3 ttl=45 time=230 ms
^C
--- nic.ir ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2117ms
rtt min/avg/max/mdev = 228.879/229.995/230.702/0.798 ms
C:\home\lab-user\Desktop\Lab-Files>
```

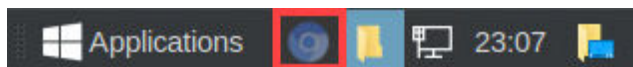
Please
Note

You may not get a response to the ping but that will not affect this lab.

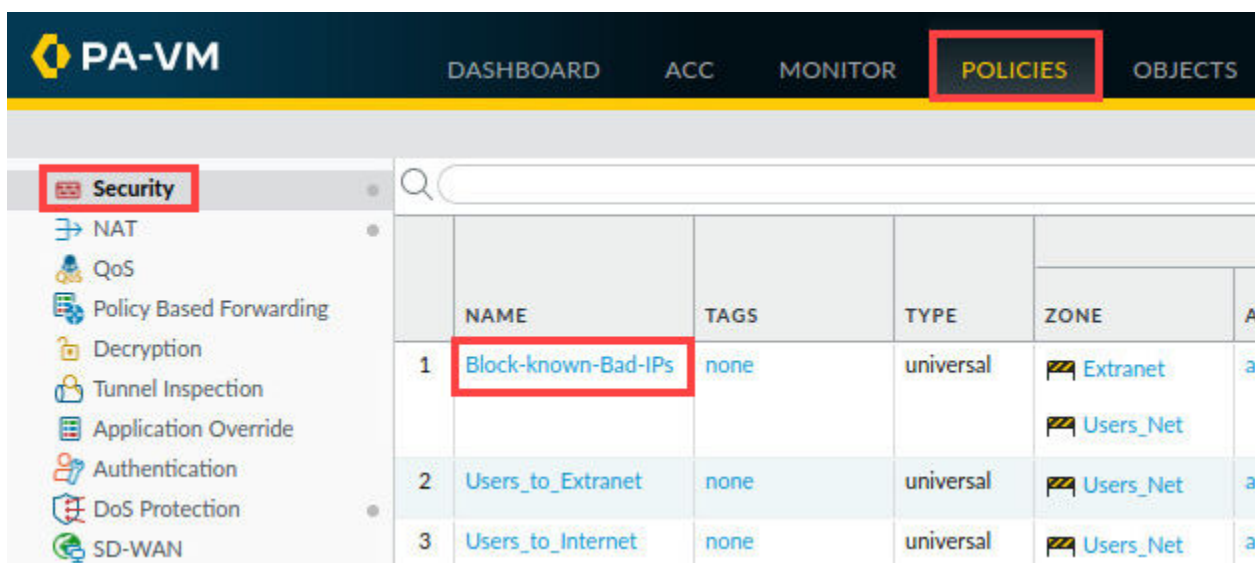
- Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.



- If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.

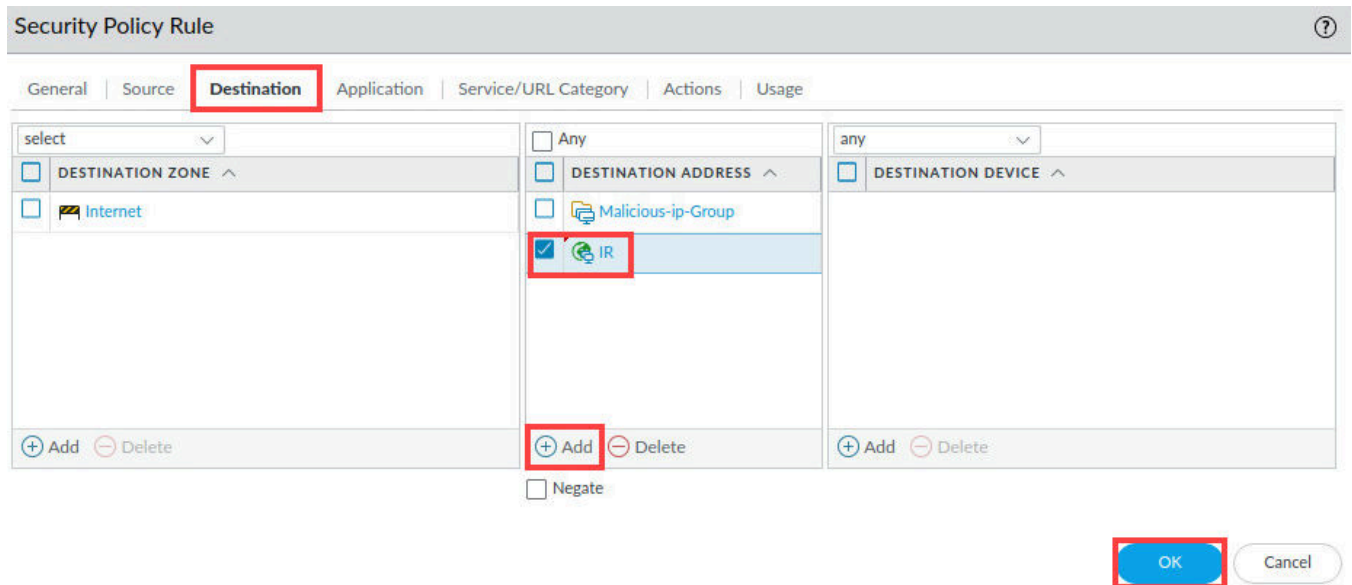


- In the web interface, select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.



	NAME	TAGS	TYPE	ZONE	A
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	a
2	Users_to_Extranet	none	universal	Users_Net	a
3	Users_to_Internet	none	universal	Users_Net	a

8. In the *Security Policy Rule* window, click the **Destination** tab and Add IR to the *Destination Address* list. Click **OK**.



Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

DESTINATION ZONE

Internet

DESTINATION ADDRESS

Any

Malicious-ip-Group

☒ IR

+ Add - Delete

+ Add - Delete

☐ Negate

any

DESTINATION DEVICE

+ Add - Delete

OK Cancel

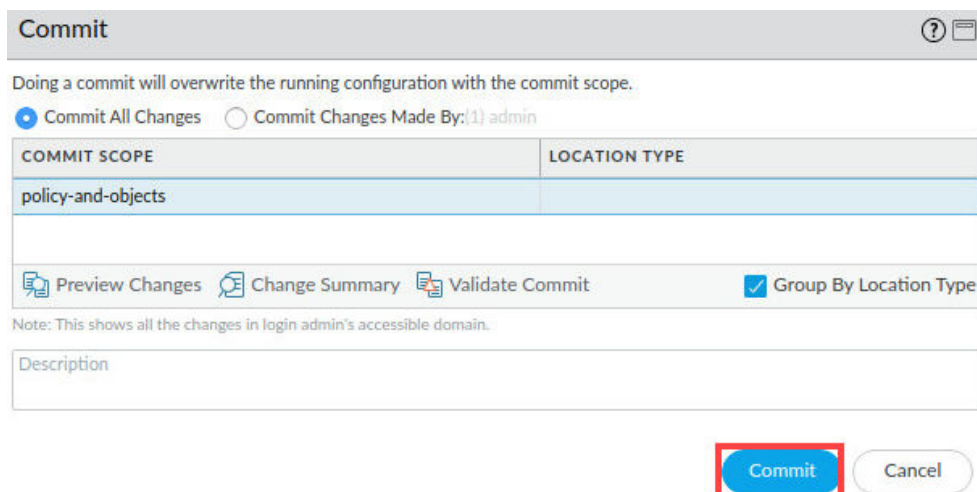
Please Note

You will need to scroll down the list of available addresses to locate the entry for IR.

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



17. 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
policy-and-objects	

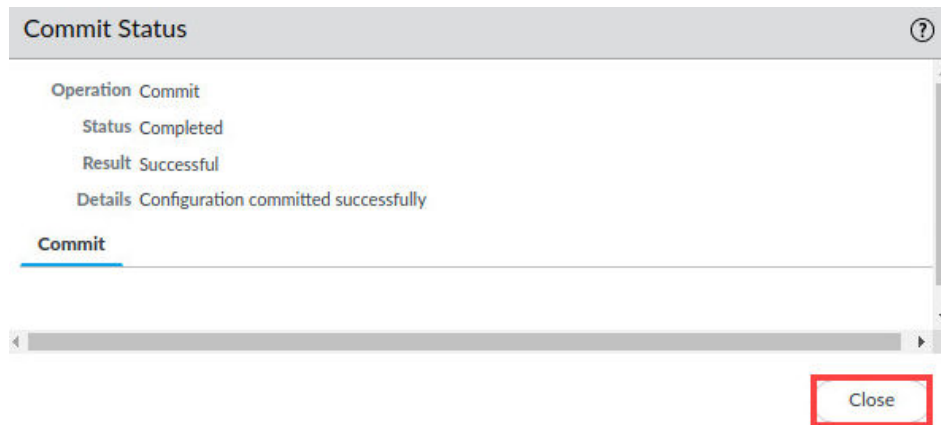
Preview Changes Change Summary Validate Commit ☒ Group By Location Type

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

Description

Commit Cancel

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



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



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



21. From the *terminal* window on the *desktop*, verify connectivity to *nic.ir* by entering the command below. Use **Ctrl+C** to stop the ping after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir
PING nic.ir (194.225.70.16) 56(84) bytes of data.
^C
--- nic.ir ping statistics ---
28 packets transmitted, 0 received, 100% packet loss, time 27637ms
C:\home\lab-user\Desktop\Lab-Files>
```

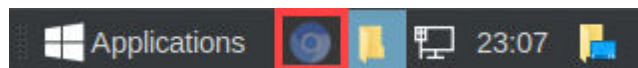
Please
Note

The ping will fail because you blocked the region of IR.

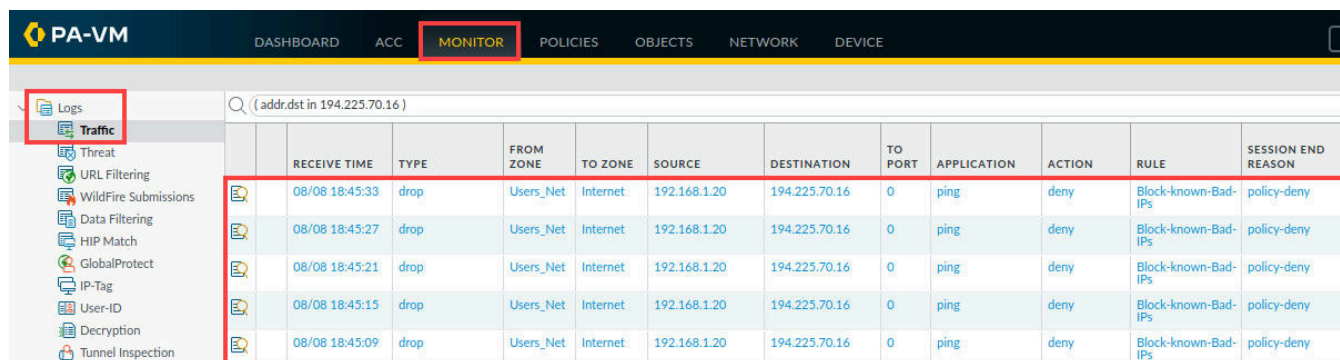
22. Minimize the *Terminal* window by clicking the **minimize** icon in the upper-right.



23. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



24. Navigate to **Monitor > Logs > Traffic**. Enter the filter (`addr.dst in 194.225.70.16`) in the *filter builder* to look for traffic that has been denied. You should see entries indicating that your **Block-Known-Bad-IPs** security policy rule has denied traffic to each host.



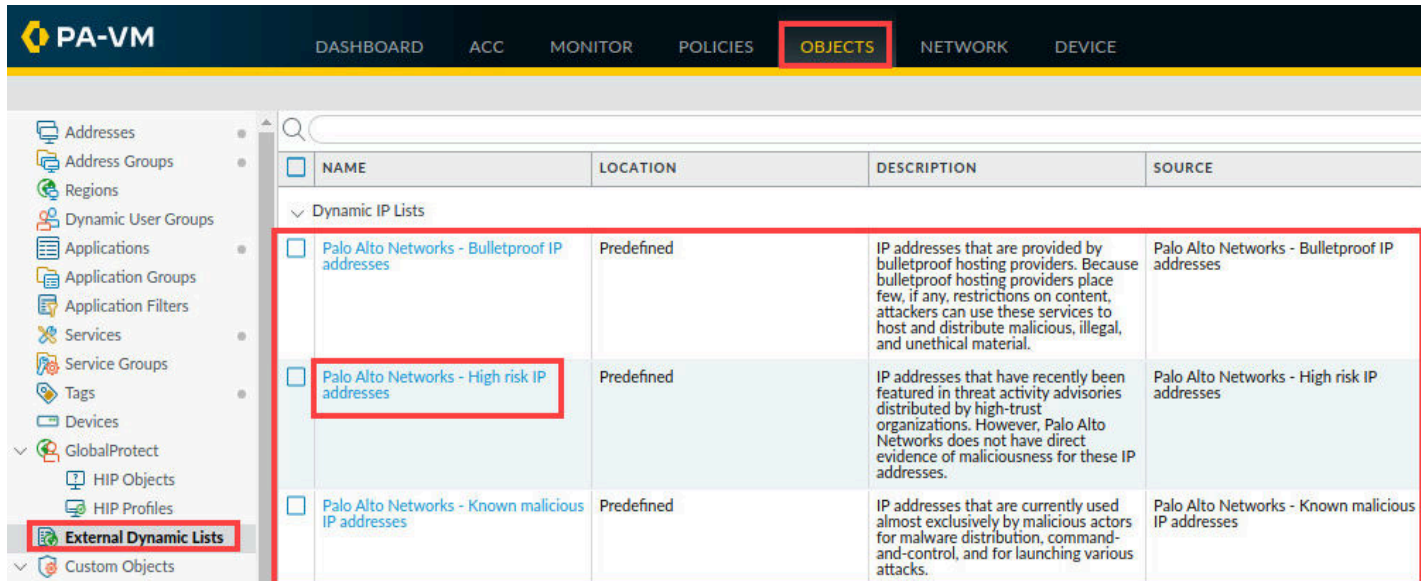
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	08/08 18:45:33	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 18:45:27	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 18:45:21	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 18:45:15	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 18:45:09	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny

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

7.6 Block Access to Malicious IP Addresses Using EDLs

You can add a list of malicious IP addresses to a file on an external web server and configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious IP address list can be regularly updated without the need to recommit the firewall configuration, as you would have to do if you updated an Address object or Address Group. EDLs simplify the maintenance of a current list of IP addresses.

1. In the *firewall* interface, select **Objects > External Dynamic Lists**. Note the three predefined EDLs contain known malicious and high-risk IP address lists. Click **Palo Alto Networks – High risk IP addresses**.

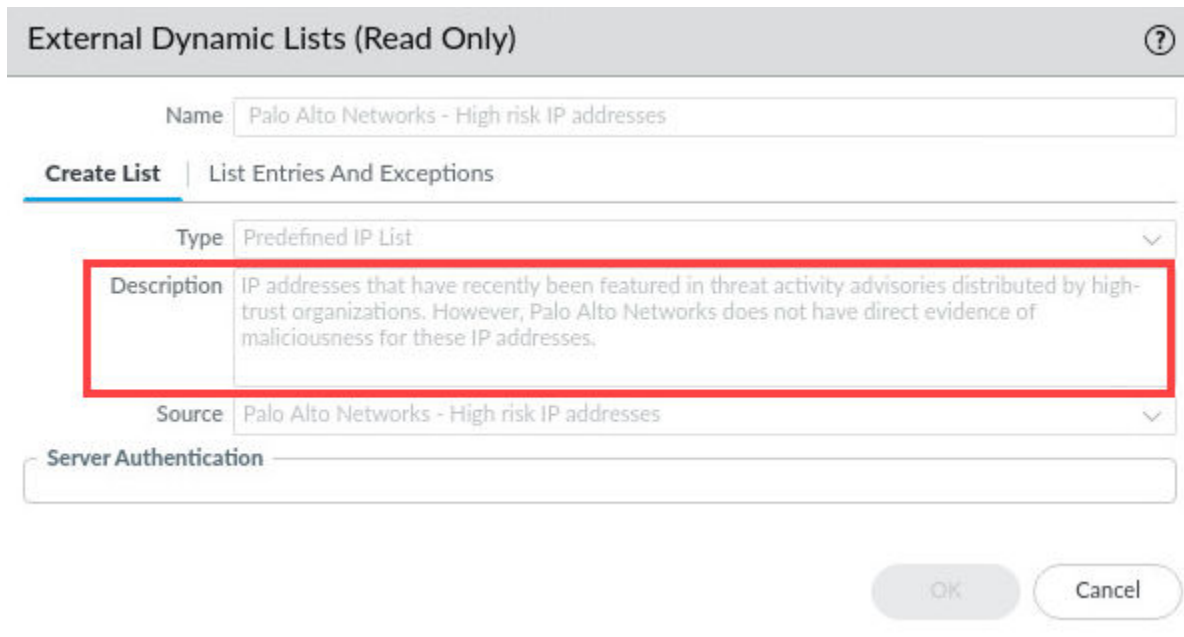


NAME	LOCATION	DESCRIPTION	SOURCE
Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	Palo Alto Networks - Known malicious IP addresses

Please Note

Palo Alto Networks maintains and provides these lists.

2. Read the description of the list.



External Dynamic Lists (Read Only) ⓘ

Name:

Create List | List Entries And Exceptions

Type:

Description:

Source:

Server Authentication:

OK Cancel

- Click the **List Entries And Exceptions** tab. Write down *three IP addresses* on the current list of IP addresses. You will try to **ping** these addresses later in this lab exercise. Click **Cancel**.

External Dynamic Lists (Read Only) ?

Name: Palo Alto Networks - High risk IP addresses

Create List **List Entries And Exceptions**

List Entries 312 items → ×

	LIST ENTRIES
<input type="checkbox"/>	89.37.192.194
<input type="checkbox"/>	80.211.52.246
<input type="checkbox"/>	185.232.64.32
<input type="checkbox"/>	185.232.64.26
<input type="checkbox"/>	185.123.141.221
<input type="checkbox"/>	58.221.60.164
<input type="checkbox"/>	18.217.172.191
<input type="checkbox"/>	117.111.111.111

Manual Exceptions 0 items → ×

	LIST ENTRIES
--	--------------

+ Add - Delete

→

OK Cancel

Please Note

For this step, we chose the first three IP Addresses on the list. You may choose any IP Addresses you would like however, it is important to write down the IP Address to complete this task.

Note that you can also copy and paste these addresses into a text file on the client desktop.

- At the bottom of the *External Dynamic Lists* window, click **Add**.

+ Add - Delete Clone PDF/CSV Move Top ↑

5. In the *External Dynamic Lists* window, create another **EDL** and configure the following. Click **Test Source URL**.

Parameter	Value
Name	custom-malicious-ips-edl
Type	IP List
Description	Contains manually entered IP address list on web server.
Source	http://192.168.50.80/malicious-ips.txt (The EDL contains only the IP address 192.168.50.11.)
Check for updates	Five Minute

External Dynamic Lists ?

Name

Create List | List Entries And Exceptions

Type

Description

Source

Server Authentication

Certificate Profile

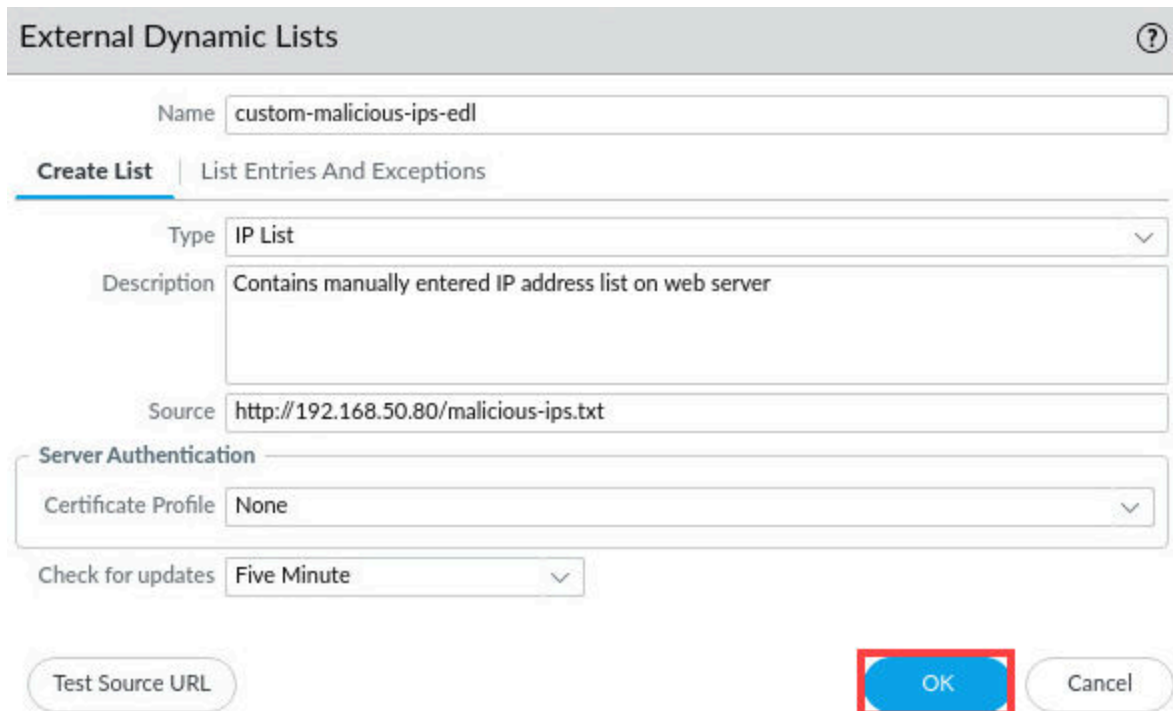
Check for updates

6. The firewall should present a *Test Source URL* window indicating that it can access the URL. Click **Close**.

Test Source URL

Source URL is accessible.

- Click **OK** in the *External Dynamic Lists* window.



External Dynamic Lists ⓘ

Name: custom-malicious-ips-edl

Create List | List Entries And Exceptions

Type: IP List

Description: Contains manually entered IP address list on web server

Source: http://192.168.50.80/malicious-ips.txt

Server Authentication

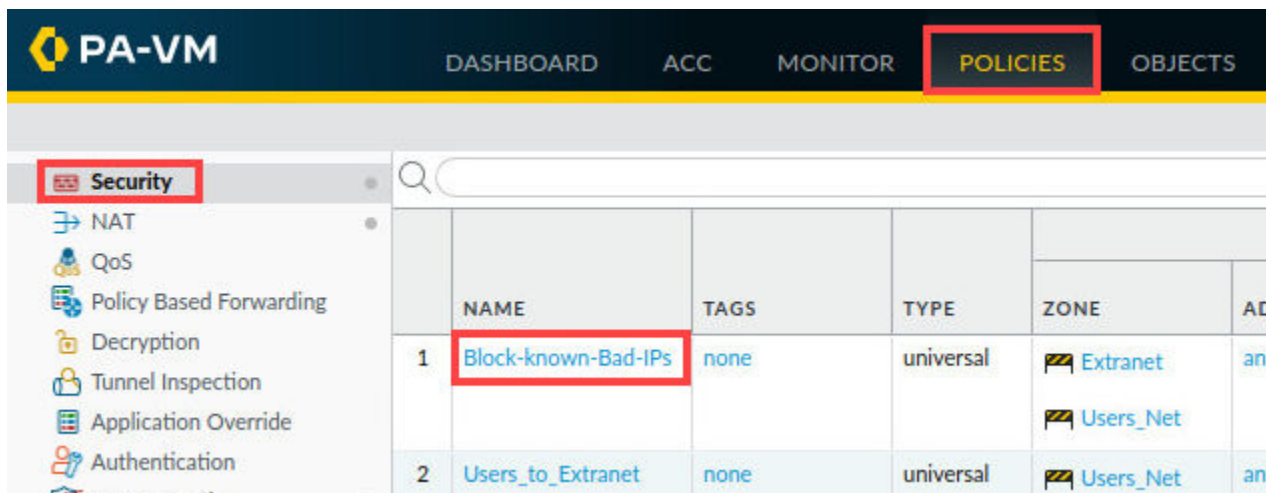
Certificate Profile: None

Check for updates: Five Minute

Test Source URL

OK Cancel

- Update the security policy to include *External Dynamic Lists*. Navigate to **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.



PA-VM DASHBOARD ACC MONITOR **POLICIES** OBJECTS

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection
- Application Override
- Authentication


	NAME	TAGS	TYPE	ZONE	AD
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	an
2	Users_to_Extranet	none	universal	Users_Net	an

9. Click the **Destination** tab and configure the following. Click **OK**.

Parameter	Value
Destination Zone	Internet
Destination Address	Add the following to the list: Palo Alto Networks – Bulletproof IP addresses Palo Alto Networks – High risk IP addresses Palo Alto Networks – Known malicious IP addresses

Security Policy Rule ?

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select ▼
☐ DESTINATION ZONE ^
☒  Internet

☐ Any
☐ DESTINATION ADDRESS ^
☐ IR
☐ Malicious-IP-Group
☒ Palo Alto Networks - Bulletproof IP addresses
☒ Palo Alto Networks - High risk IP addresses
☒ Palo Alto Networks - Known malicious IP addresses

any ▼
☐ DESTINATION DEVICE ^






+ Add - Delete + Add - Delete + Add - Delete

☐ Negate

Please Note

The “Block-Known-Bad-IPs” rule now is configured to block access to the three IP addresses you wrote down in lab Step 3.

10. Click **Users_to_Extranet** to edit the rule.

	NAME	TAGS	TYPE	ZONE	ADDRESS
1	Block-known-Bad-IPs	none	universal	 Extranet  Users_Net	any
2	Users_to_Extranet	none	universal	 Users_Net	any
3	Users_to_Internet	none	universal	 Users_Net	any
4	Extranet_to_Internet	none	universal	 Extranet	any

11. In the *Security Policy Rule* window, click the **Destination** tab and configure the following. Click **OK**.

Parameter	Value
Destination Zone	Extranet
Destination Address	custom-malicious-ips-edl
Negate	Select check box

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

☐ DESTINATION ZONE ^

☒ Extranet

☐ DESTINATION ADDRESS ^

☒ custom-malicious-ips-edl

☐ DESTINATION DEVICE ^

☐ Any

☐ any

+ Add - Delete

+ Add - Delete

+ Add - Delete

☒ Negate

OK Cancel

Please Note

The malicious-ips-edl EDL contains the IP address of a host in the Extranet zone (192.168.50.11). When the destination address is used in conjunction with the Negate option, the rule matches and allows any address in the Extranet zone except the address listed in the EDL.

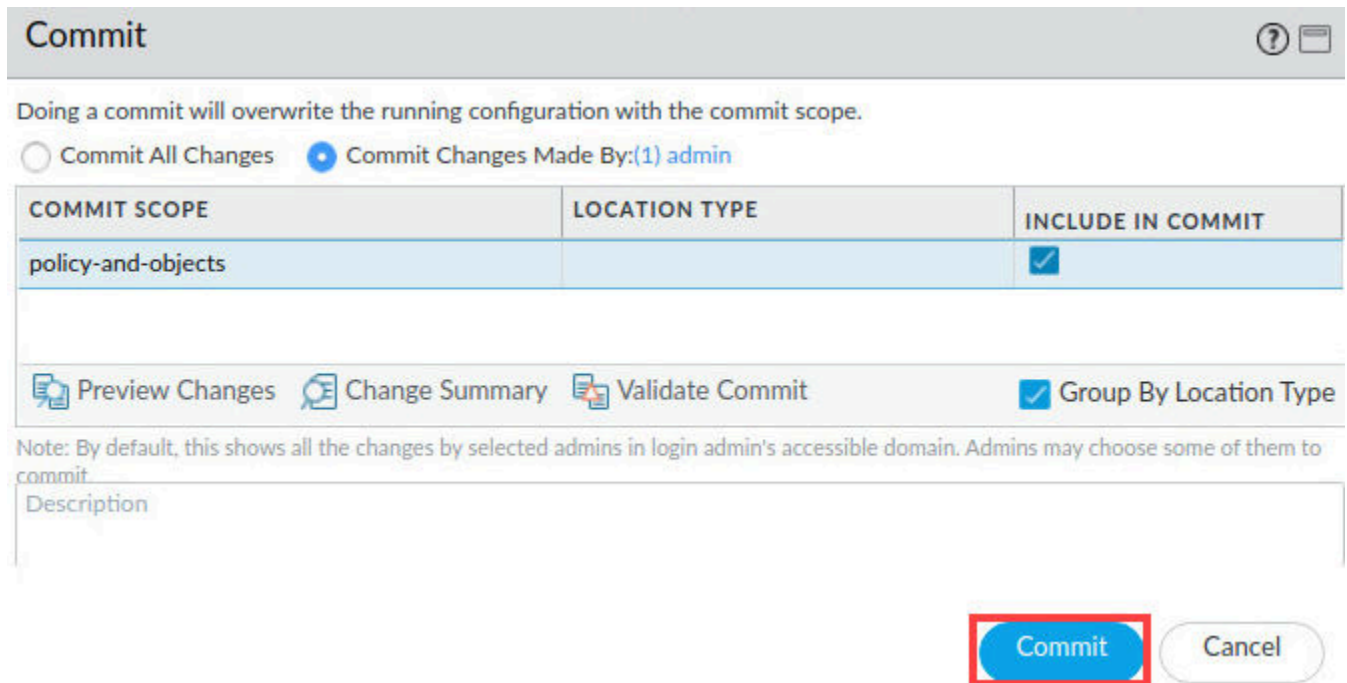
12. Notice in the *Users_to_Extranet* rule that *custom-malicious-ips-edl* has a line through it. This line indicates that the **Negate** option has been employed for addresses in the list.

	NAME	TAGS	TYPE	Source				Destination	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	Block-known-Bad-IPs	none	universal	Extranet Users_Net	any	any	any	Internet	IR Malicious-IP-Group Palo Alto Networks - Bulletproof IP ... Palo Alto Networks - High risk IP ad... Palo Alto Networks - Known malicio...
2	Users_to_Extranet	none	universal	Users_Net	any	any	any	Extranet	custom-malicious-ips-edl
3	Users_to_Internet	none	universal	Users_Net	any	any	any	Internet	any

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



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

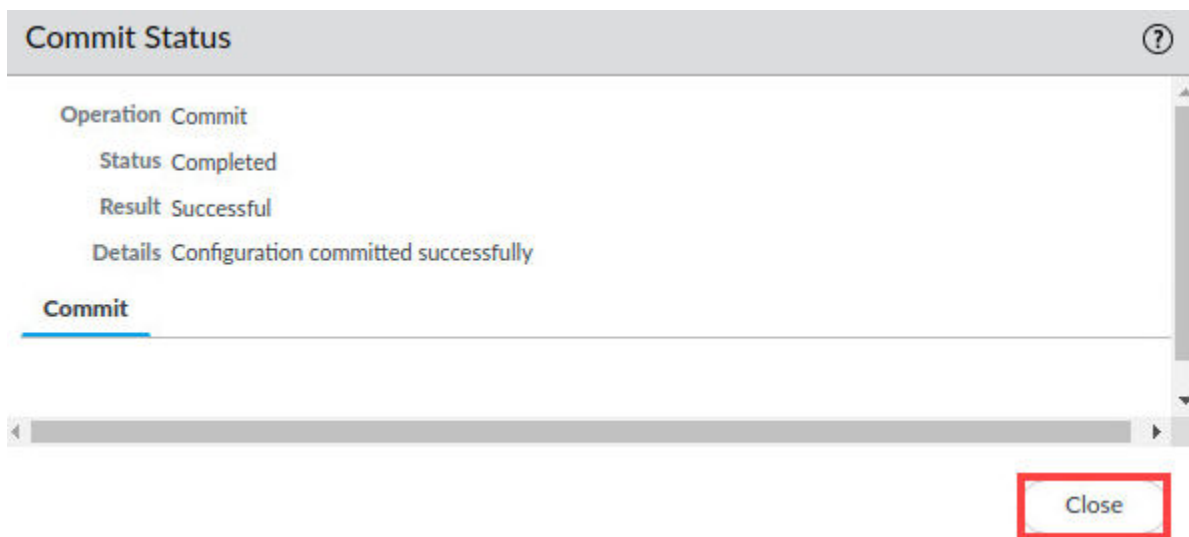


The **Commit** window shows a confirmation dialog. At the top, it states: "Doing a commit will overwrite the running configuration with the commit scope." Below this, there are two radio buttons: "Commit All Changes" (unselected) and "Commit Changes Made By:(1) admin" (selected). A table lists the commit scope and location type:

COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

Below the table, there are three icons with labels: "Preview Changes", "Change Summary", and "Validate Commit". To the right, there is a checkbox labeled "Group By Location Type" which is checked. A note at the bottom states: "Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit." At the bottom right, there are two buttons: "Commit" (highlighted with a red box) and "Cancel".

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



The **Commit Status** window displays the results of the commit operation. It shows:

- Operation: Commit
- Status: Completed
- Result: Successful
- Details: Configuration committed successfully

Below this information, there is a tab labeled "Commit" which is selected. At the bottom right, there is a button labeled "Close" (highlighted with a red box).

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



17. From the *terminal* window on the *desktop*, ping an address on the internet by issuing the following command.

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11
```

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

```
C:\home\lab-user\Desktop\Lab-Files> ping 192.168.50.11
PING 192.168.50.11 (192.168.50.11) 56(84) bytes of data.
^C
--- 192.168.50.11 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
C:\home\lab-user\Desktop\Lab-Files>
```

Please
Note

The **ping** should fail because the IP address is listed in the custom EDL.

19. From the *terminal* window, use **ping** again, but this time try one of the three IP addresses that you wrote down earlier in lab step 3.

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194 <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194
```

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

```
C:\home\lab-user\Desktop\Lab-Files> ping 89.37.192.194
PING 89.37.192.194 (89.37.192.194) 56(84) bytes of data.
^C
--- 89.37.192.194 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2036ms
C:\home\lab-user\Desktop\Lab-Files>
```

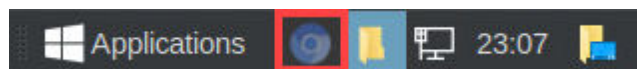
Please
Note

These IP addresses were in one of the EDLs predefined by Palo Alto Networks.

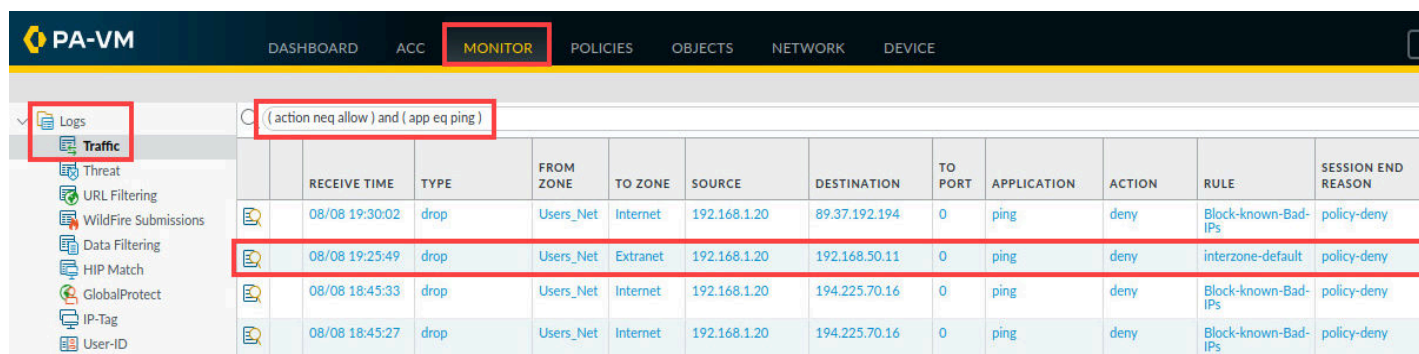
21. Minimize the *Terminal* window open on the client because you will perform this same task in a later step.



22. If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.



23. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter (**action neq allow**) and (**app eq ping**). Click the **Apply Filter** button in the upper-right corner of the window. You will notice the firewall is now logging entries matching your filter.

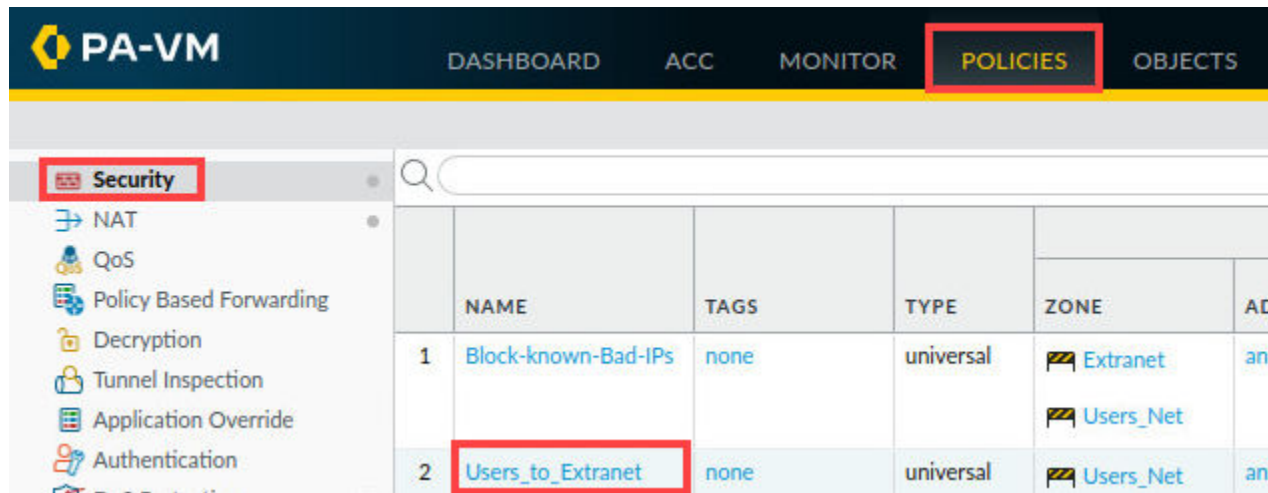


	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	08/08 19:30:02	drop	Users_Net	Internet	192.168.1.20	89.37.192.194	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 19:25:49	drop	Users_Net	Extranet	192.168.1.20	192.168.50.11	0	ping	deny	interzone-default	policy-deny
	08/08 18:45:33	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny
	08/08 18:45:27	drop	Users_Net	Internet	192.168.1.20	194.225.70.16	0	ping	deny	Block-known-Bad-IPs	policy-deny

Please Note

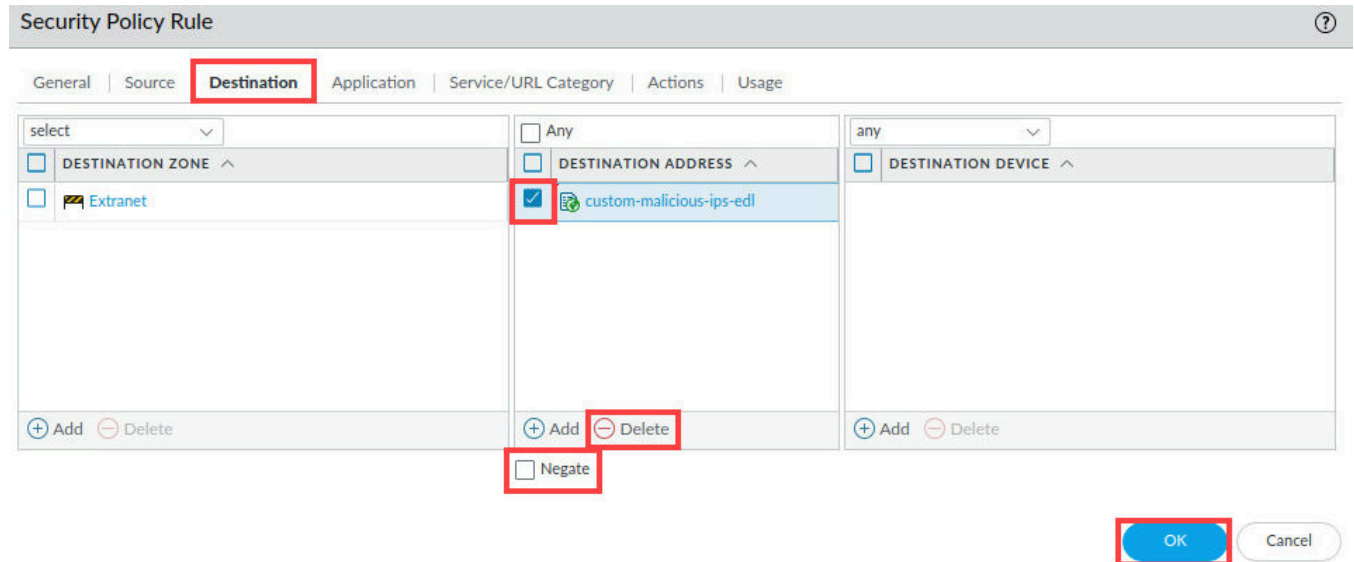
Note that ping to 192.168.50.11 hit the **interzone-default** rule and not the **Users_to_Extranet** rule. The **Users_to_Extranet** rule is set to allow traffic (with the exception of the IP address 192.168.50.11). Traffic to the 192.168.50.11 address does not match the rule because of the negate setting you applied in the Destination Address section. However, that traffic does match the interzone-default rule which denies traffic.

24. In the firewall web interface, select **Policies > Security**. Click **Users_to_Extranet** to edit the rule.



25. In the *Security Policy Rule* window, click the **Destination** tab and configure the following. Click **OK**.

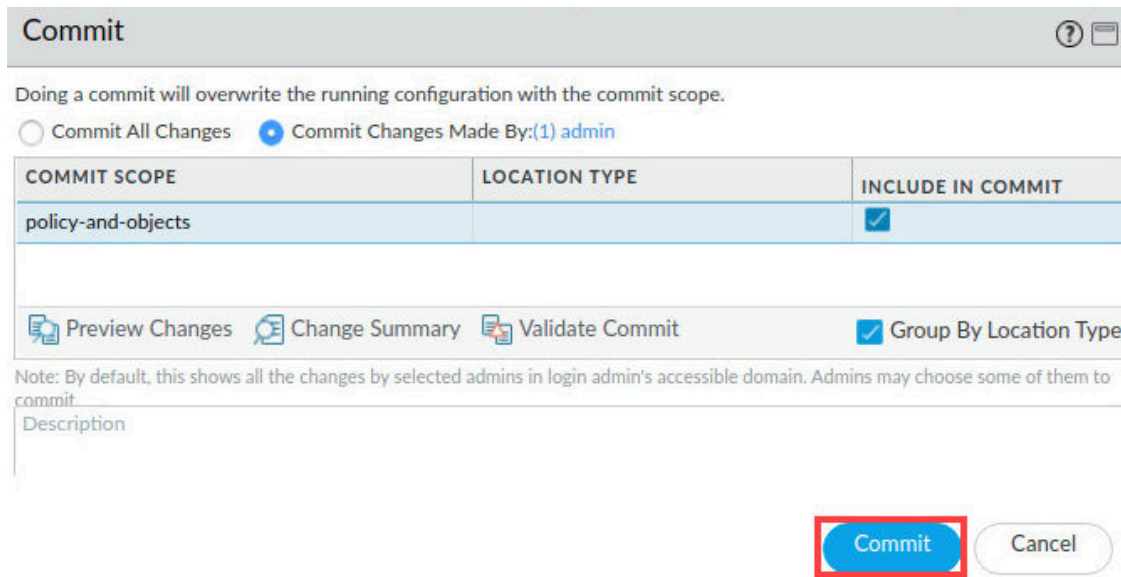
Parameter	Value
Destination Zone	Extranet
Destination Address	Delete custom-malicious-ips-edl
Negate check box	Deselect it



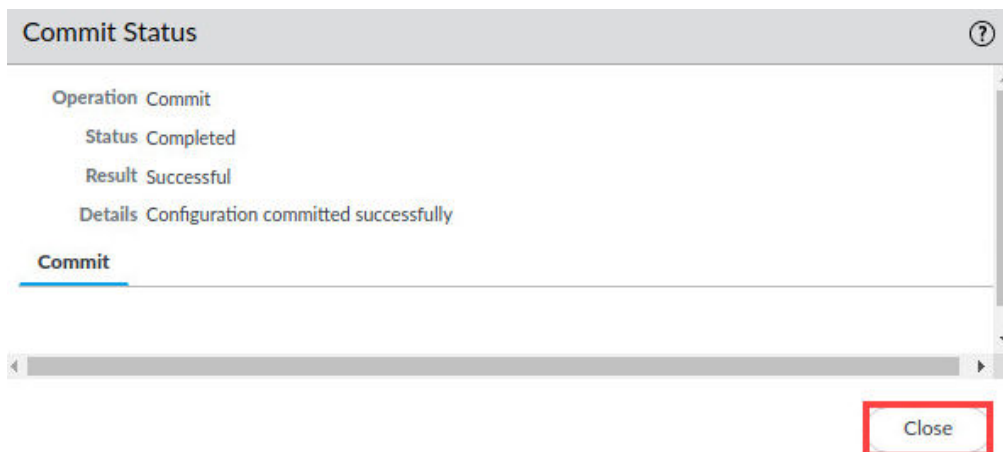
26. Click the **Commit** button at the upper-right of the web interface.



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



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



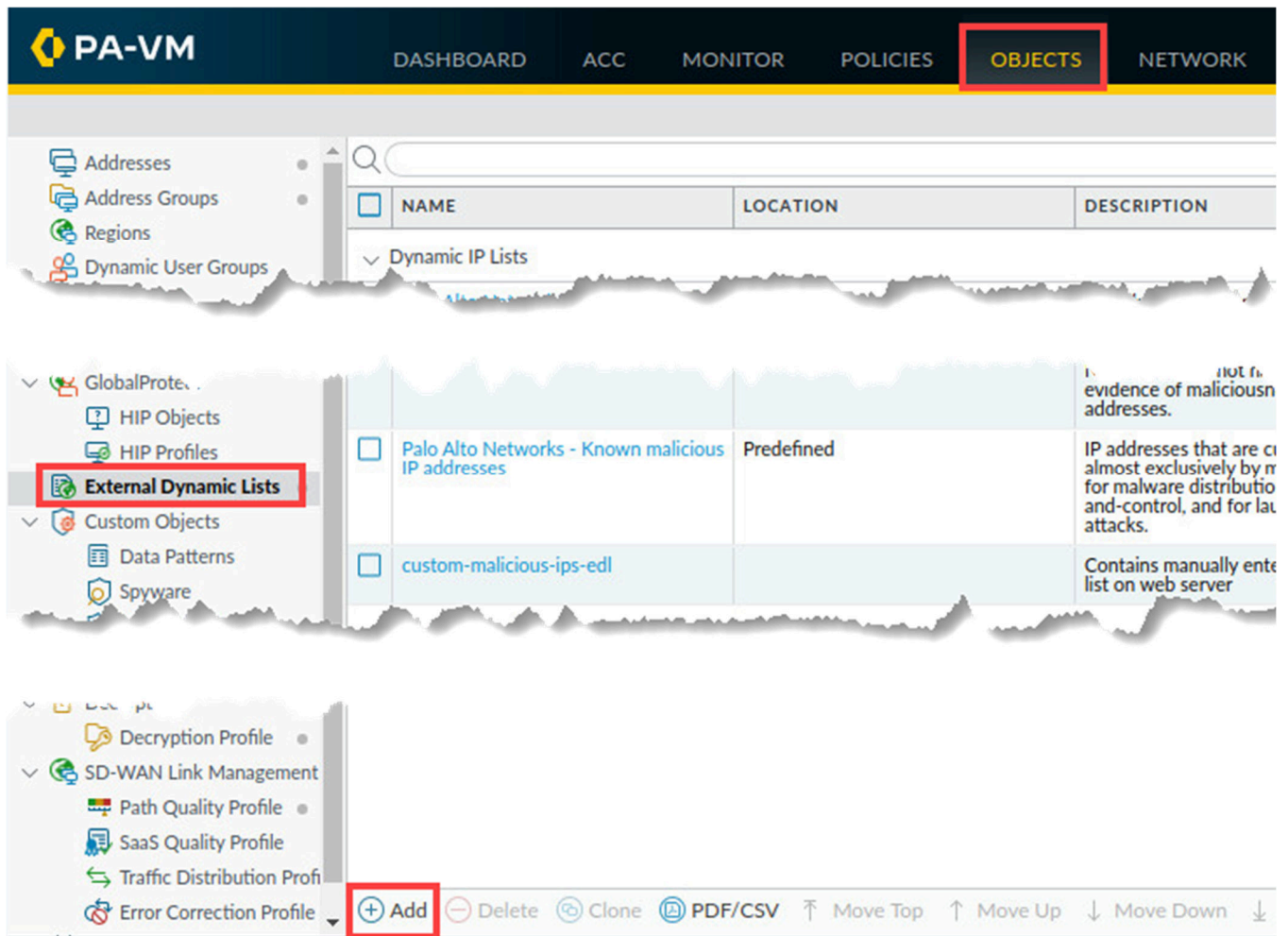
29. Leave the web interface open and continue to the next task.

7.7 Block Access to Malicious Domains Using an EDL

You can add a list of malicious domains to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious domain list can be updated regularly without the need to recommit the firewall configuration.

In this section, you will block access to malicious domains using an External Dynamic List.

1. In the *PA-VM firewall* web interface, navigate to **Objects > External Dynamic Lists**. Click **Add** at the bottom of the window.



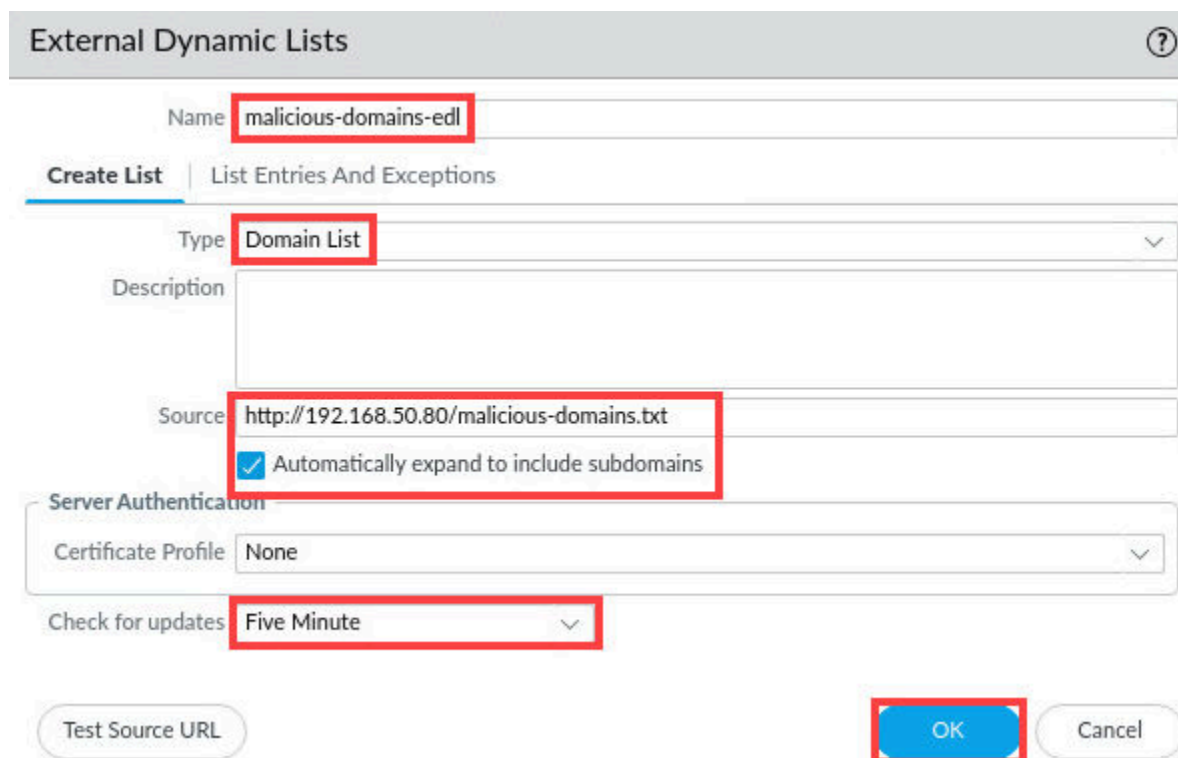
The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (highlighted with a red box), and 'NETWORK'. The left sidebar contains a tree view with 'Addresses', 'Address Groups', 'Regions', 'Dynamic User Groups', 'GlobalProtect', 'HIP Objects', 'HIP Profiles', 'External Dynamic Lists' (highlighted with a red box), 'Custom Objects', 'Data Patterns', 'Spyware', 'Decryption Profile', 'SD-WAN Link Management', 'Path Quality Profile', 'SaaS Quality Profile', 'Traffic Distribution Profile', and 'Error Correction Profile'. The main content area displays a table of Dynamic IP Lists. The table has columns for 'NAME', 'LOCATION', and 'DESCRIPTION'. The table lists two entries: 'Palo Alto Networks - Known malicious IP addresses' (Predefined) and 'custom-malicious-ips-edl' (Custom). The 'Add' button at the bottom left is highlighted with a red box.

NAME	LOCATION	DESCRIPTION
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are almost exclusively by IP for malware distribution and-control, and for later attacks.
custom-malicious-ips-edl		Contains manually entered list on web server

At the bottom of the interface, there is a toolbar with buttons: '+ Add', '- Delete', 'Clone', 'PDF/CSV', 'Move Top', 'Move Up', 'Move Down', and a dropdown arrow.

2. In the *External Dynamic Lists* window, configure the following. Click **OK**.

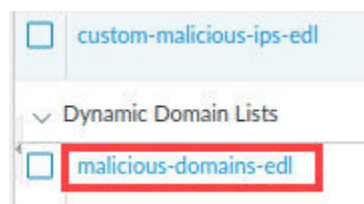
Parameter	Value
Name	malicious-domains-edl
Type	Domain List
Source	http://192.168.50.80/malicious-domains.txt (The EDL contains the domains quora.com and producthunt.com.)
Automatically expand to include subdomains	Select it
Check for updates	Five Minute



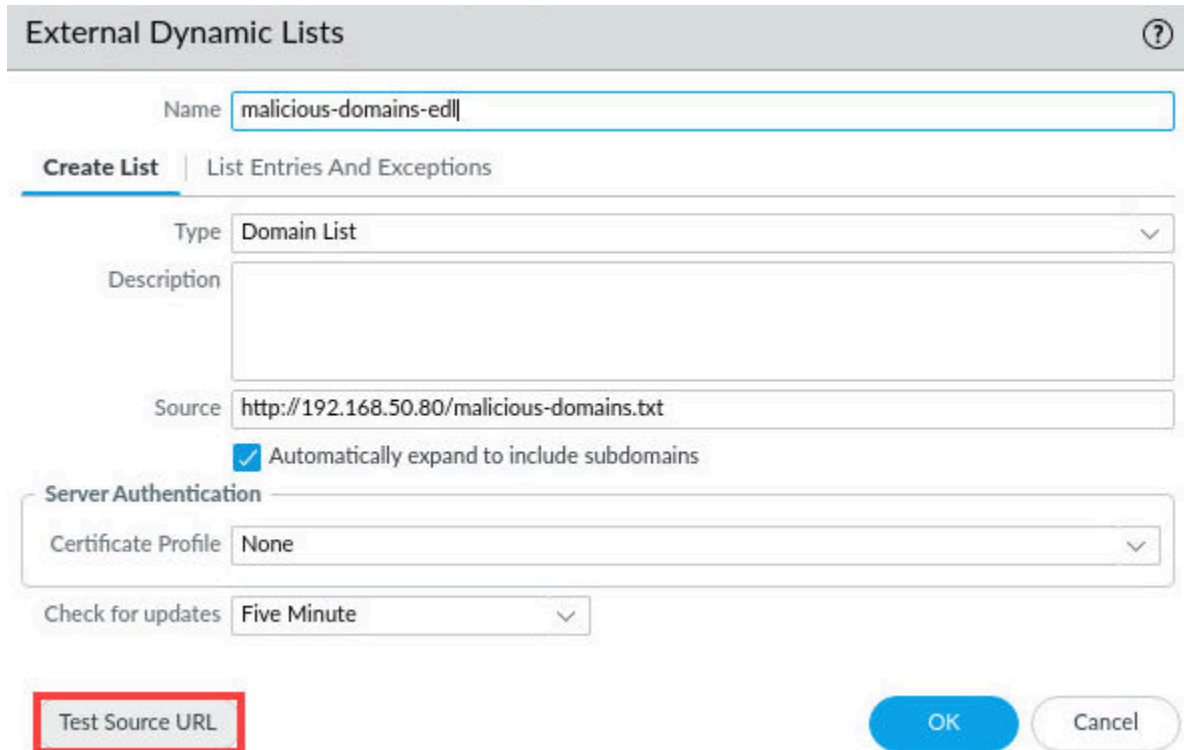
Please Note

This EDL will be used to block access to the quora.com and producthunt.com domains.

3. Click to reopen the **malicious-domains-edl**.

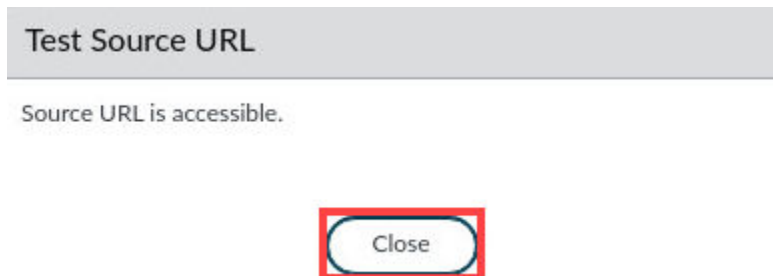


4. In the *External Dynamic Lists* window, click **Test Source URL**.



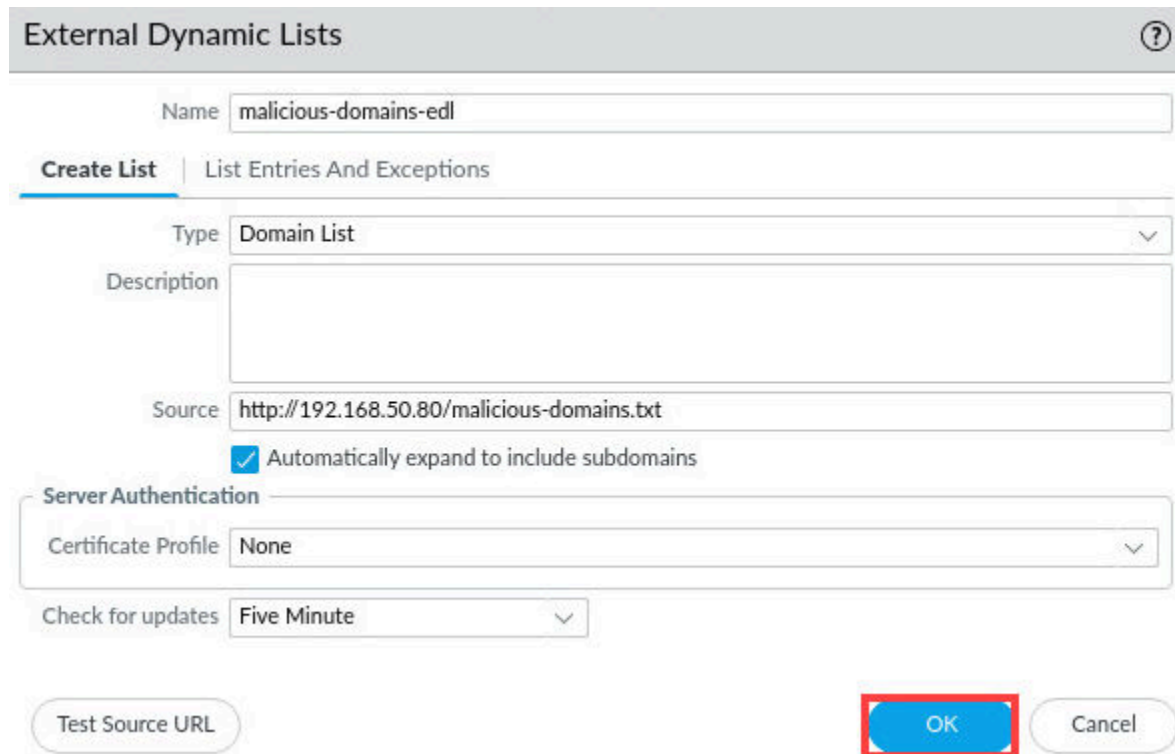
The **External Dynamic Lists** window is shown. The **Name** field contains "malicious-domains-edl". The **Create List** tab is selected, and the **Type** is set to "Domain List". The **Source** field contains "http://192.168.50.80/malicious-domains.txt". The checkbox **Automatically expand to include subdomains** is checked. The **Server Authentication** section shows **Certificate Profile** set to "None". The **Check for updates** dropdown is set to "Five Minute". At the bottom, the **Test Source URL** button is highlighted with a red box. Other buttons include **OK** and **Cancel**.

5. The firewall should present a **Test Source URL** window indicating that it can access the URL. Click **Close**.



The **Test Source URL** window is shown. It displays the message "Source URL is accessible." At the bottom, the **Close** button is highlighted with a red box.

6. Click **OK** in the *External Dynamic Lists* window.



The screenshot shows the 'External Dynamic Lists' window. The title bar is 'External Dynamic Lists' with a help icon. The 'Name' field contains 'malicious-domains-edl'. There are two tabs: 'Create List' (selected) and 'List Entries And Exceptions'. Under 'Create List', the 'Type' is 'Domain List', the 'Description' field is empty, and the 'Source' is 'http://192.168.50.80/malicious-domains.txt'. A checkbox 'Automatically expand to include subdomains' is checked. The 'Server Authentication' section has a 'Certificate Profile' dropdown set to 'None'. The 'Check for updates' dropdown is set to 'Five Minute'. At the bottom, there is a 'Test Source URL' button, a blue 'OK' button (highlighted with a red rectangle), and a 'Cancel' button.

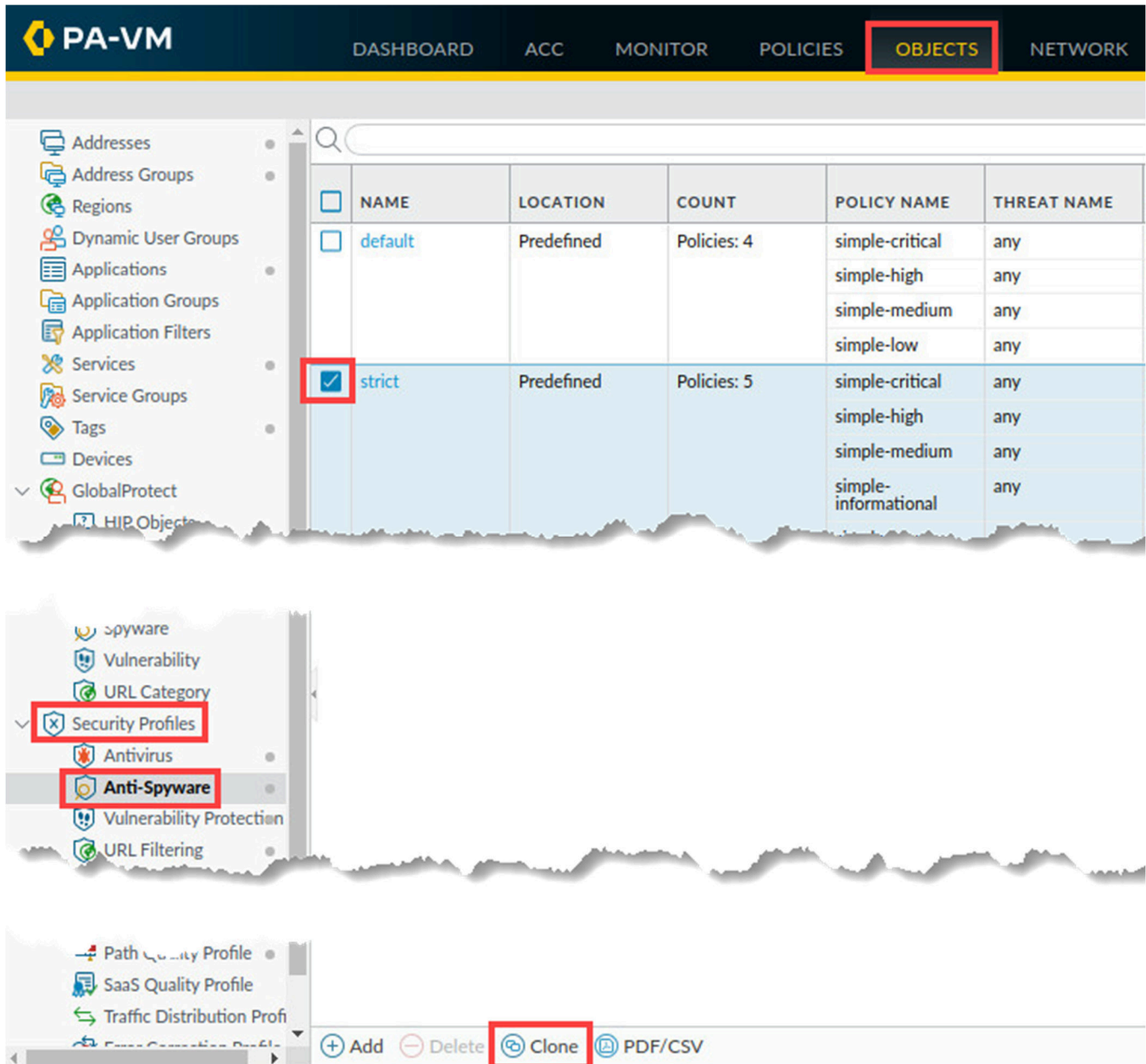
7. Leave the firewall open and continue to the next task.

7.8 Add the Domain List EDL to an Anti-Spyware Profile

You can add an EDL containing a domain list to an Anti-Spyware Profile to block access to malicious domains. You must attach the Anti-Spyware Profile to a security policy rule that allows network access. Although the security policy rule might allow the traffic, the attached Anti-Spyware Profile will block access to any domains listed in the EDL.

In this section, you will add a domain list EDL to an anti-spyware profile.

1. In the web interface, select **Objects > Security Profiles > Anti-Spyware**. Select the checkbox next to the **strict** Anti-Spyware Profile. Click **Clone**.

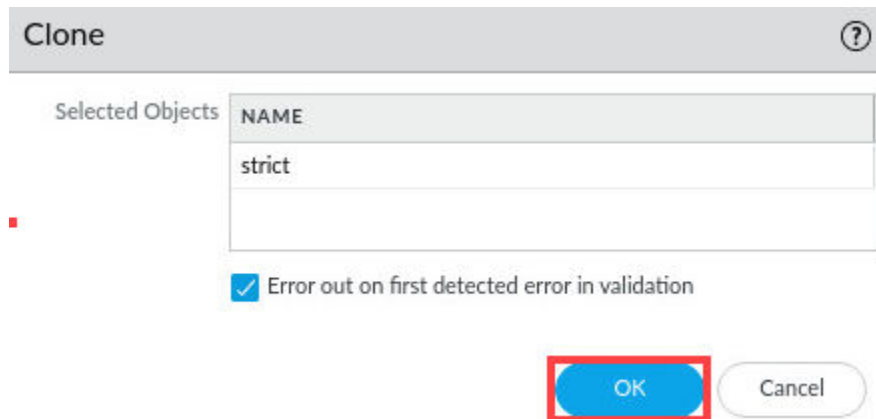


The screenshot displays the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (highlighted with a red box), and 'NETWORK'. The left sidebar lists various categories: Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, Devices, GlobalProtect, and HIP Objects. The main content area shows a table of Security Profiles under the 'Anti-Spyware' category. The 'strict' profile is selected, indicated by a red box around its checkbox. The table lists the following profiles:

NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME
default	Predefined	Policies: 4	simple-critical	any
			simple-high	any
			simple-medium	any
			simple-low	any
strict	Predefined	Policies: 5	simple-critical	any
			simple-high	any
			simple-medium	any
			simple-informational	any

Below the table, the left sidebar shows the 'Security Profiles' category expanded, with 'Anti-Spyware' highlighted. The bottom of the interface shows a toolbar with 'Add', 'Delete', 'Clone' (highlighted with a red box), and 'PDF/CSV' buttons.

- In the *Clone* window, click **OK**.



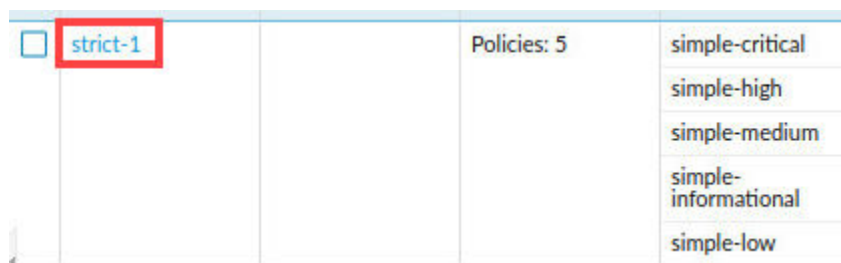
The **Clone** window shows a table with the following data:

Selected Objects	NAME
<input checked="" type="checkbox"/>	strict

Below the table, the checkbox **Error out on first detected error in validation** is checked.

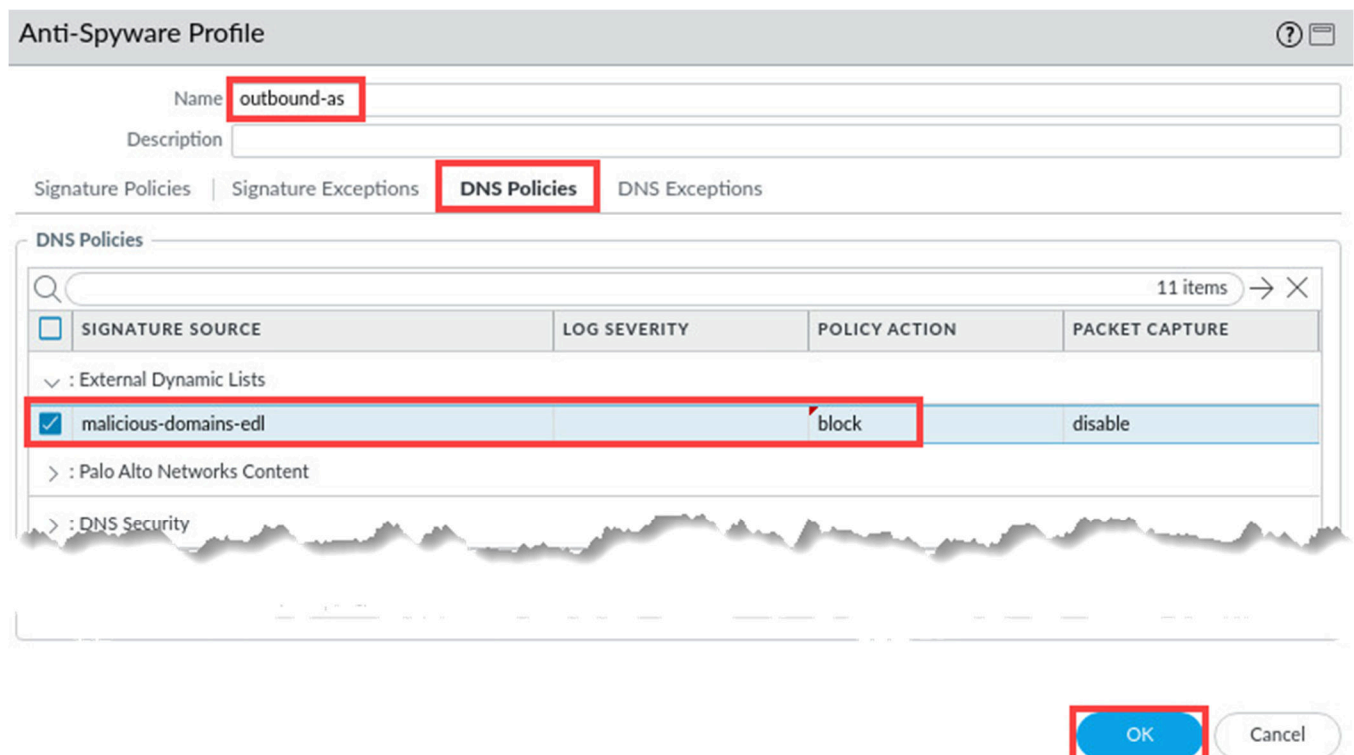
At the bottom, the **OK** button is highlighted with a red box.

- A new **strict-1** Anti-Spyware Profile should have been created. Click **strict-1** to edit the profile.



<input checked="" type="checkbox"/>	strict-1	Policies: 5	simple-critical simple-high simple-medium simple-informational simple-low
-------------------------------------	----------	-------------	---

- Rename the profile **outbound-as**. Click the **DNS Policies** tab. Under the *External Dynamic Lists* section, change the **Policy Action** dropdown list to **block**. Click **OK**.



The **Anti-Spyware Profile** window shows the following configuration:

- Name:** outbound-as
- Description:** (empty)
- Tabs:** Signature Policies, Signature Exceptions, **DNS Policies** (selected), DNS Exceptions

Under the **DNS Policies** tab, the **External Dynamic Lists** section is expanded, showing a table with 11 items:

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
<input checked="" type="checkbox"/> malicious-domains-edl		block	disable

The **malicious-domains-edl** row is highlighted with a red box, and the **block** value in the **POLICY ACTION** column is also highlighted with a red box.

At the bottom, the **OK** button is highlighted with a red box.

Please Note

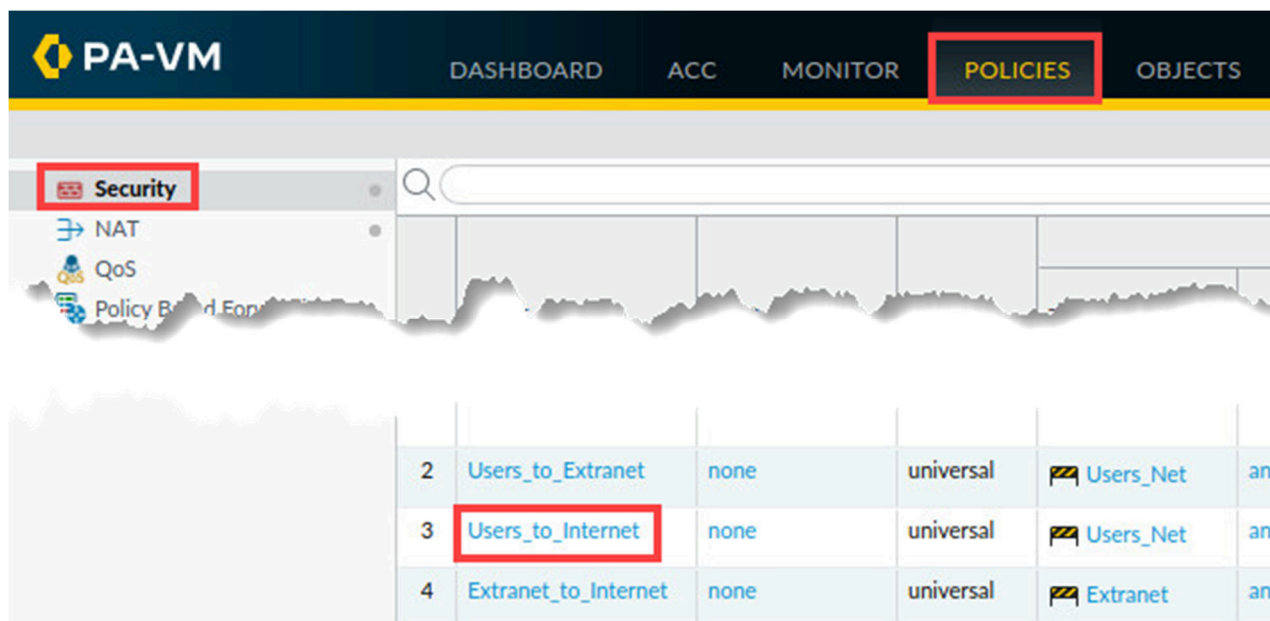
Palo Alto Networks typically recommends the “sinkhole” action, which will be discussed and used in another lab exercise.

5. Leave the firewall open and continue to the next task.

7.9 Add the Anti-Spyware Profile to a Security Policy Rule

In this section, you will add the **outbound-as** Anti-Spyware Profile to the security policy. The configuration of the profile will enable the firewall to use malicious domain signatures to block access to malicious domains.

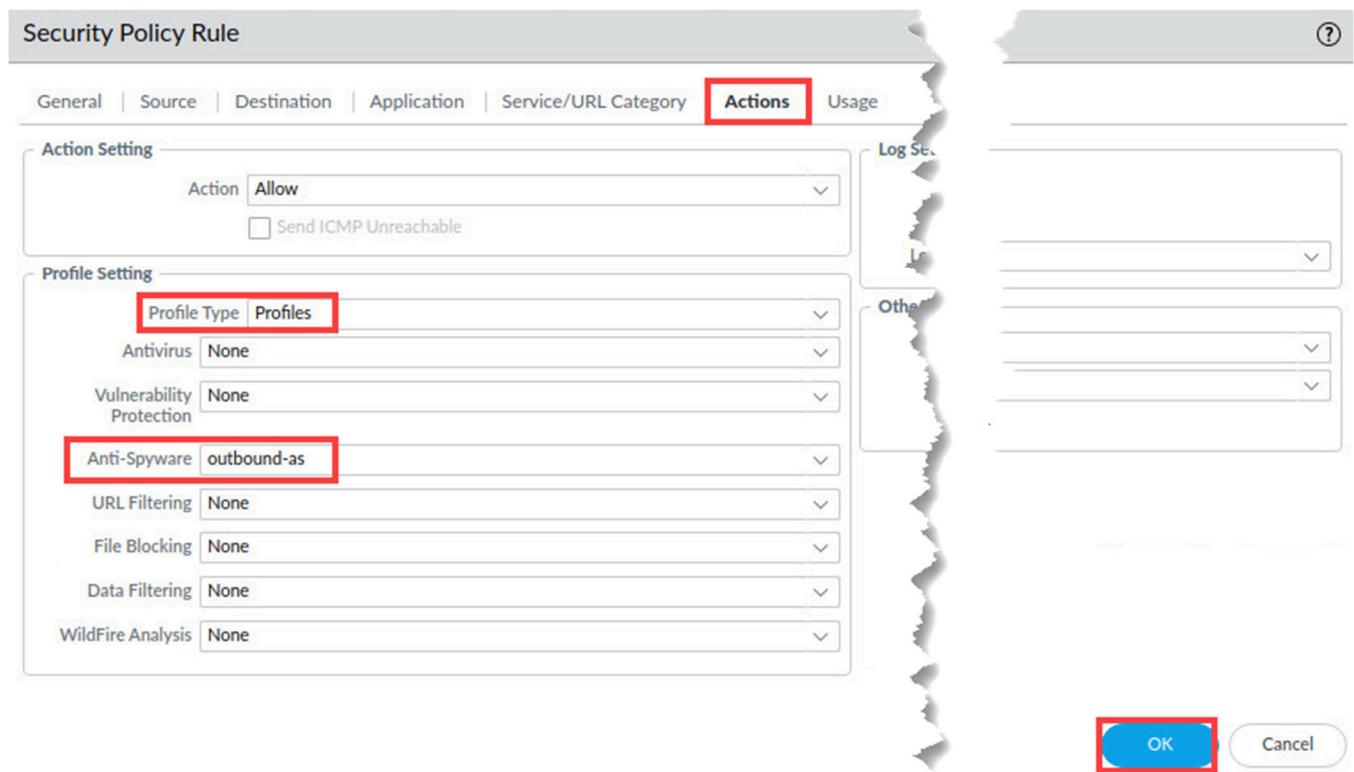
1. In the web interface, navigate to **Policies > Security**. Click **Users_to_Internet** to edit the rule.



Rule ID	Rule Name	Action	Profile	Source Object	Destination Object
2	Users_to_Extranet	none	universal	Users_Net	any
3	Users_to_Internet	none	universal	Users_Net	any
4	Extranet_to_Internet	none	universal	Extranet	any

2. In the *Security Policy Rule* window, configure the following on the **Actions** tab. Click **OK**.

Parameter	Value
Profile Type	Profiles
Anti-Spyware	outbound-as



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: **Allow** (v)

☐ Send ICMP Unreachable

Profile Setting

Profile Type: **Profiles** (v)

Antivirus: None (v)

Vulnerability Protection: None (v)

Anti-Spyware: **outbound-as** (v)

URL Filtering: None (v)

File Blocking: None (v)

Data Filtering: None (v)

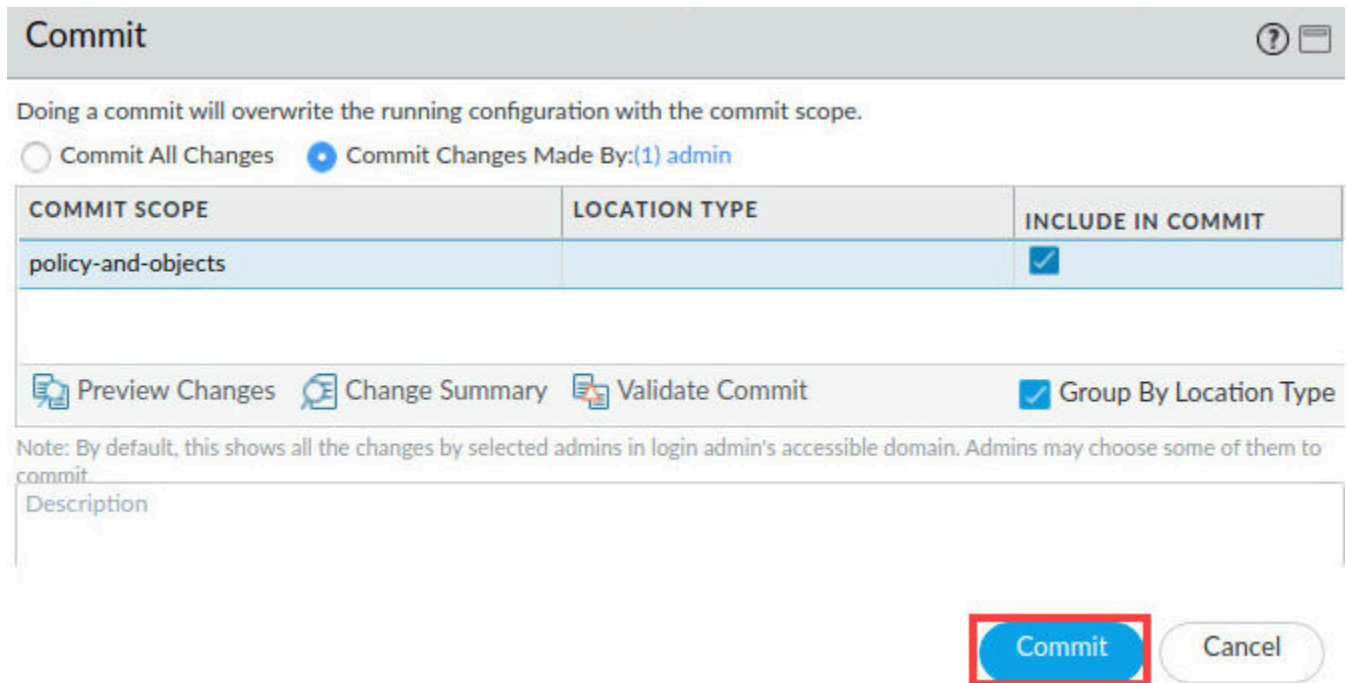
WildFire Analysis: None (v)

OK Cancel

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



4. 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	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

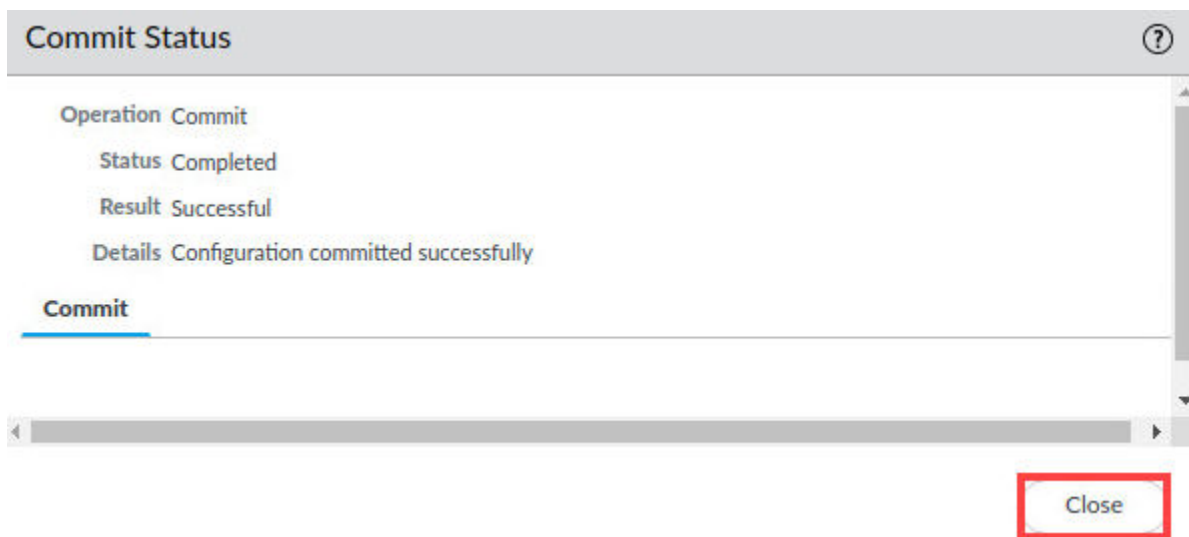
[Preview Changes](#)
[Change Summary](#)
[Validate Commit](#)
☒ Group By Location Type

Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit.

Description

Commit Cancel

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



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

Commit

Close

6. Minimize the *Chromium* browser by clicking the **minimize** icon.



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



8. From the *terminal* window on the *desktop*, ping two addresses on the internet by issuing the following commands. Use **Ctrl+C** to stop the ping for the two commands after a few seconds.

```
C:\home\lab-user\Desktop\Lab-Files> ping quora.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping producthunt.com <Enter>
```

```
C:\home\lab-user\Desktop\Lab-Files> ping quora.com
^C
C:\home\lab-user\Desktop\Lab-Files> ping producthunt.com
^C
C:\home\lab-user\Desktop\Lab-Files>
```

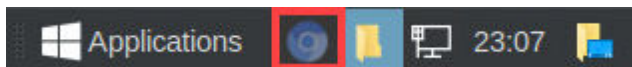
Please Note

The ping commands should fail because the domains are listed in the custom EDL and the custom EDL was added to the outbound-as Anti-Spyware Profile and configured with the “block” action.

9. Minimize the *Terminal* window.



10. If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



11. Examine the firewall traffic log by ensuring you are at **Monitor > Logs > Threat**. Clear any *filters* in filter builder. You should see several entries indicating that the firewall has blocked DNS queries for the hosts listed in the **malicious-domains-edl**.

PA-VM

DASHBOARDACC**MONITOR**POLICIESOBJECTSNETWORKDEVICE

Commit

Logs

Traffic

Threat

URL Filtering

WildFire Submissions

Data Filtering

HIP Match

GlobalProtect

IP-Tag

User-ID

Decryption

Tunnel Inspection

Configuration

System

Alarms

Authentication

Unified

<

Please Note

The order of columns has been rearranged and several columns have been hidden in the example above.

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



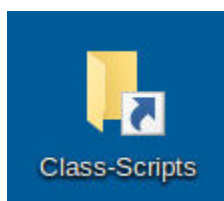
7.10 Block Access to Malicious URLs Using the Security Policy

In this section, you will block access to known-malicious URLs by configuring the firewall's URL Filtering feature. You will add URL categories to a security policy rule configured to block traffic.

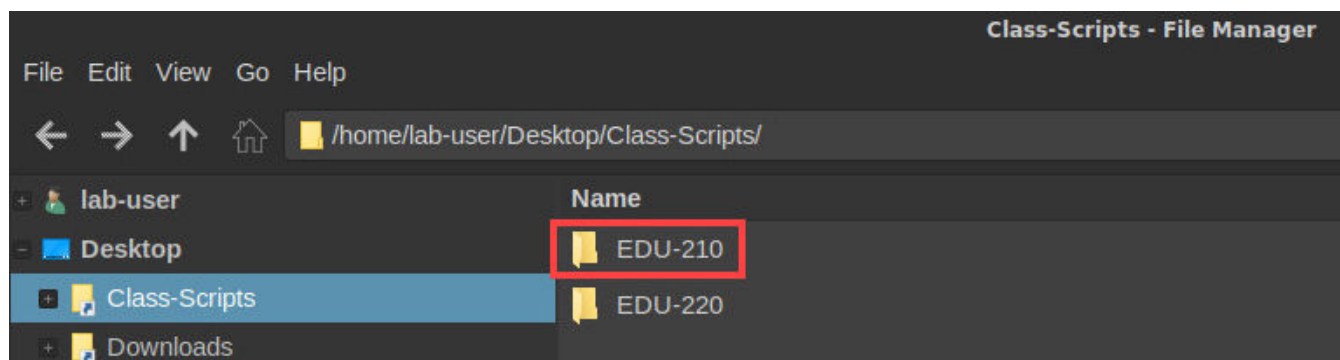
Please Note

Although you can configure the security policy to control access to URLs, the URL Filtering Profile more commonly is used to configure the action that a firewall should take when it detects a URL. You will configure a URL Filtering Profile in a later lab section.

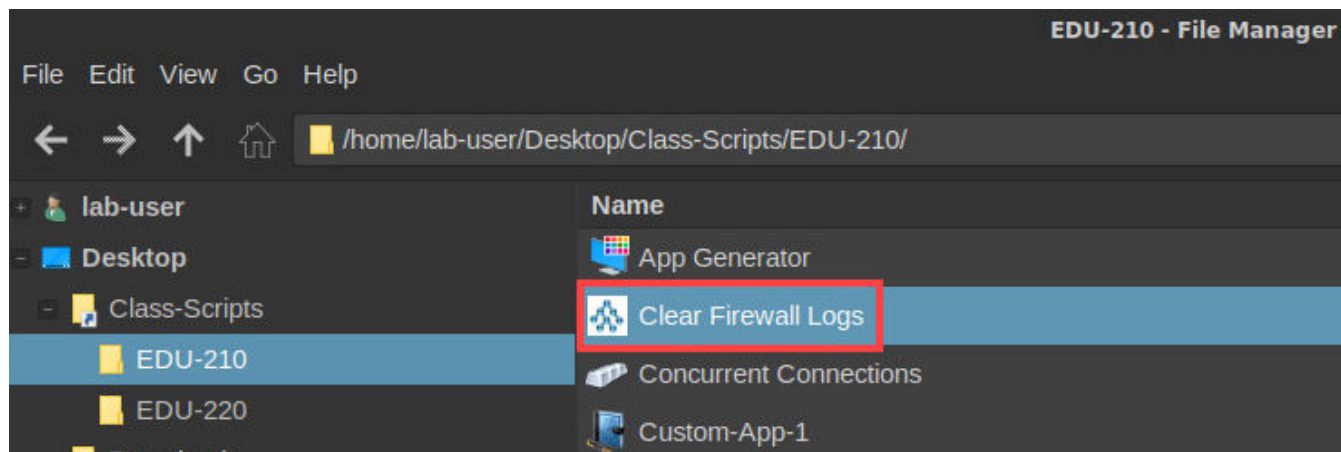
1. On the *client desktop*, double-click the folder for **Class-Scripts**.



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



- 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      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      ##
#####

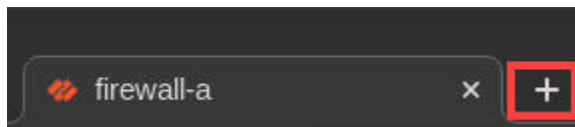
Press ENTER to close this window.

```

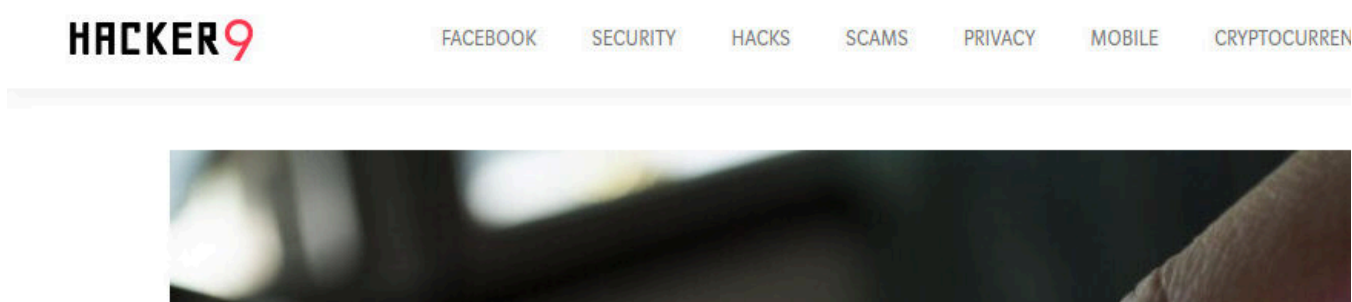
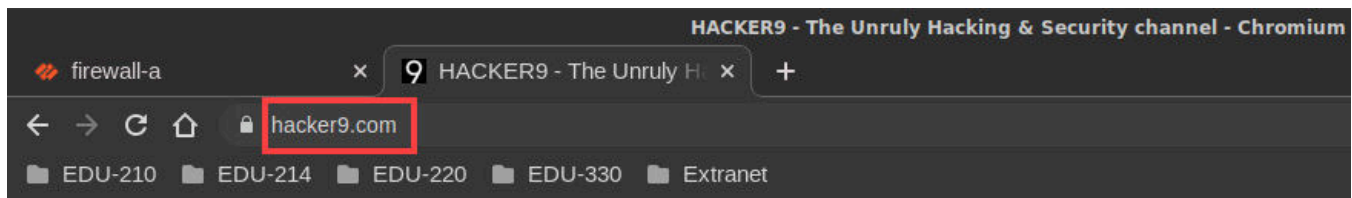
- If you minimized the *firewall*, reopen the *firewall* interface by clicking on the **Chromium** tab in the taskbar.



6. Open a new tab in **Chromium**.



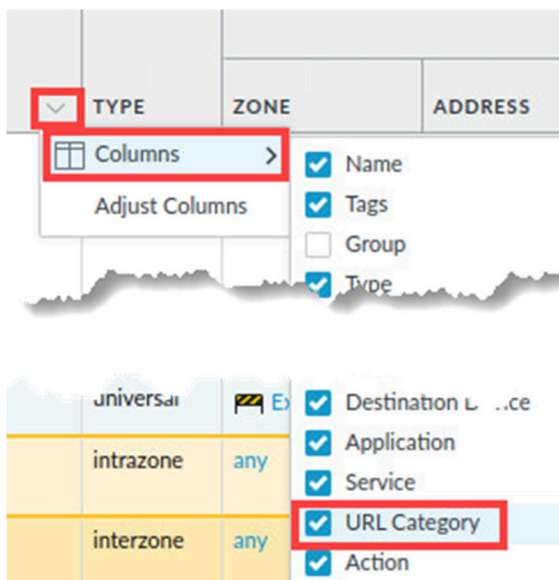
7. Type **hacker9.com** which belongs to the *URL category hacking* in the address bar, and press **Enter**.



8. Close the *hacker9.com* tab by clicking the **X** icon.



9. In the web interface, select **Policies > Security**. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category**.



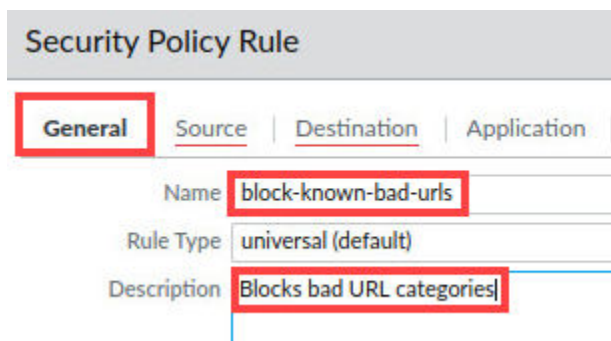
**Please
Note**

You may need to scroll through the Security Policies to find the URL Category once you have selected to display it.

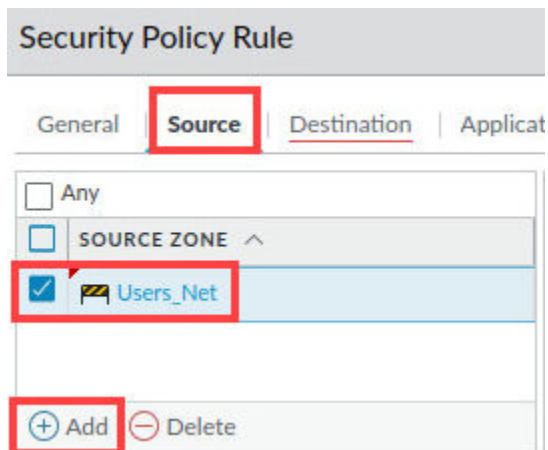
10. In the *Security Policies* window, click **Add** to create a new security policy rule.



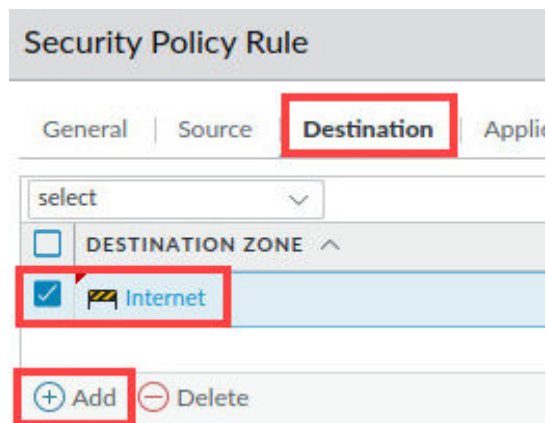
11. In the *Security Policy Rule* window, on the *General* tab, type **block-known-bad-urls** as the *Name*. For *Description*, enter **Blocks bad URL categories**.



12. Click the **Source** tab and for the *Source Zone*, select **Users_Net**.



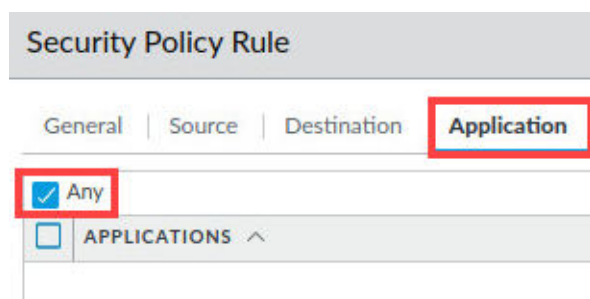
13. Click the **Destination** tab, and for the *Destination Zone*, select **Internet**.



The screenshot shows the 'Security Policy Rule' configuration page with the 'Destination' tab selected. The 'DESTINATION ZONE' section is expanded, and the 'Internet' option is selected with a checkmark. The 'Add' button is also highlighted.

General	Source	Destination	Application
select ▼			
<input type="checkbox"/> DESTINATION ZONE ^			
<input checked="" type="checkbox"/> Internet			
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>			

14. Click the **Application** tab and verify that **Any** is selected.



The screenshot shows the 'Security Policy Rule' configuration page with the 'Application' tab selected. The 'Any' option is selected with a checkmark.

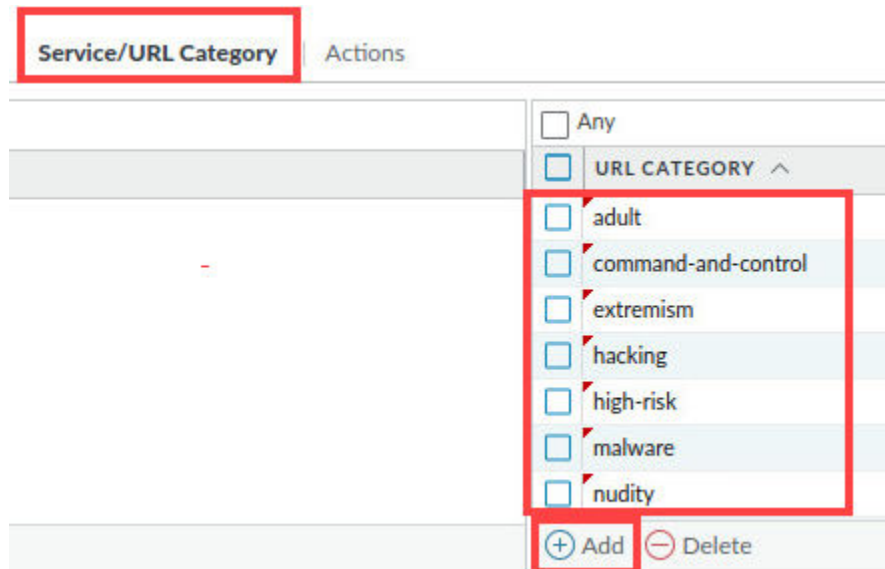
General	Source	Destination	Application
<input checked="" type="checkbox"/> Any			
<input type="checkbox"/> APPLICATIONS ^			

15. Click the **Service/URL Category** tab and configure the following.

Parameter	Value
Service	application-default
URL Category	Add the following: adult command-and-control extremism hacking high-risk malware nudity parked peer-to-peer phishing proxy-avoidance-and-anonymizers questionable

Please Note

You can type in the first few letters of each category to locate each one more quickly.



Service/URL Category Actions

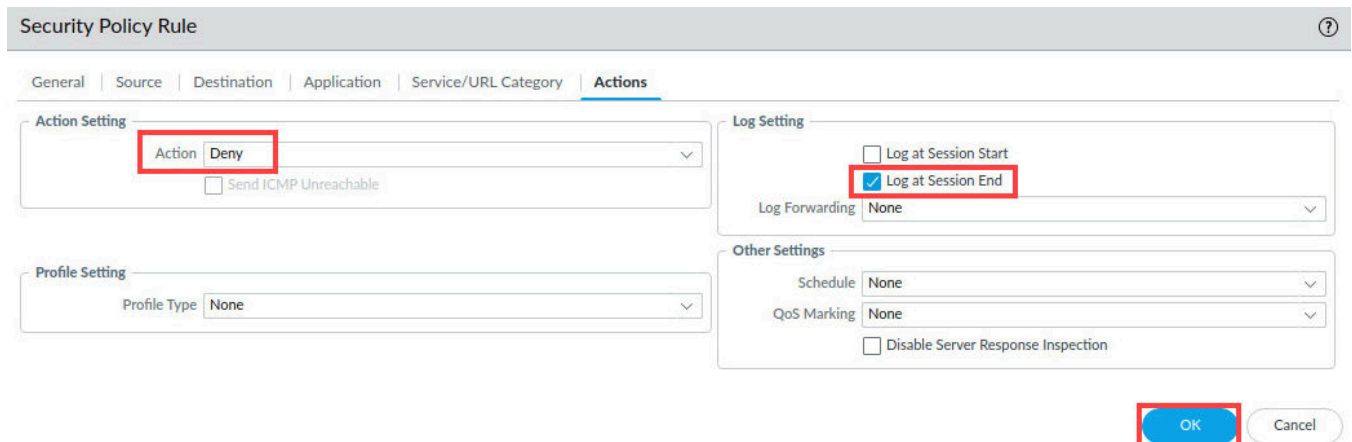
☐ Any

☐ URL CATEGORY ^

- ☐ adult
- ☐ command-and-control
- ☐ extremism
- ☐ hacking
- ☐ high-risk
- ☐ malware
- ☐ nudity

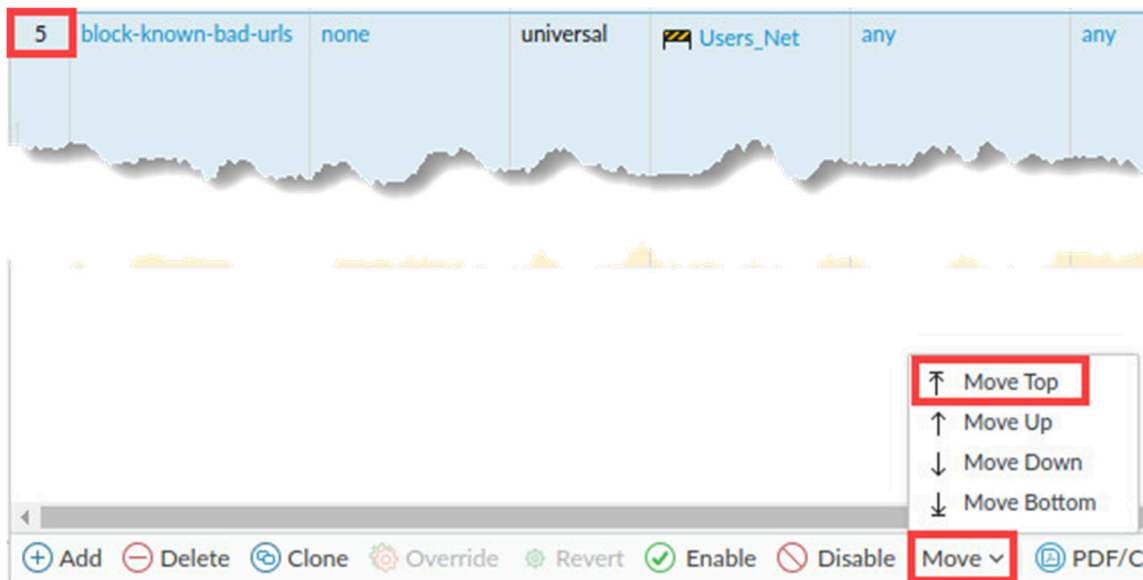
+ Add - Delete

16. Click the **Actions** tab and for the action, select **Deny**. Verify *Log at Session End* is checked. Click **OK**.



The image shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. In the 'Action Setting' section, the 'Action' dropdown is set to 'Deny'. In the 'Log Setting' section, the 'Log at Session End' checkbox is checked. The 'Log Forwarding' dropdown is set to 'None'. In the 'Profile Setting' section, the 'Profile Type' dropdown is set to 'None'. In the 'Other Settings' section, the 'Schedule' and 'QoS Marking' dropdowns are set to 'None', and the 'Disable Server Response Inspection' checkbox is unchecked. At the bottom right, the 'OK' button is highlighted with a red box.

17. Select, but do not open, the **block-known-bad-urls** rule in the security policy. Select **Move > Move Top** to move the *block-known-bad-urls* rule to the top of the security policy.



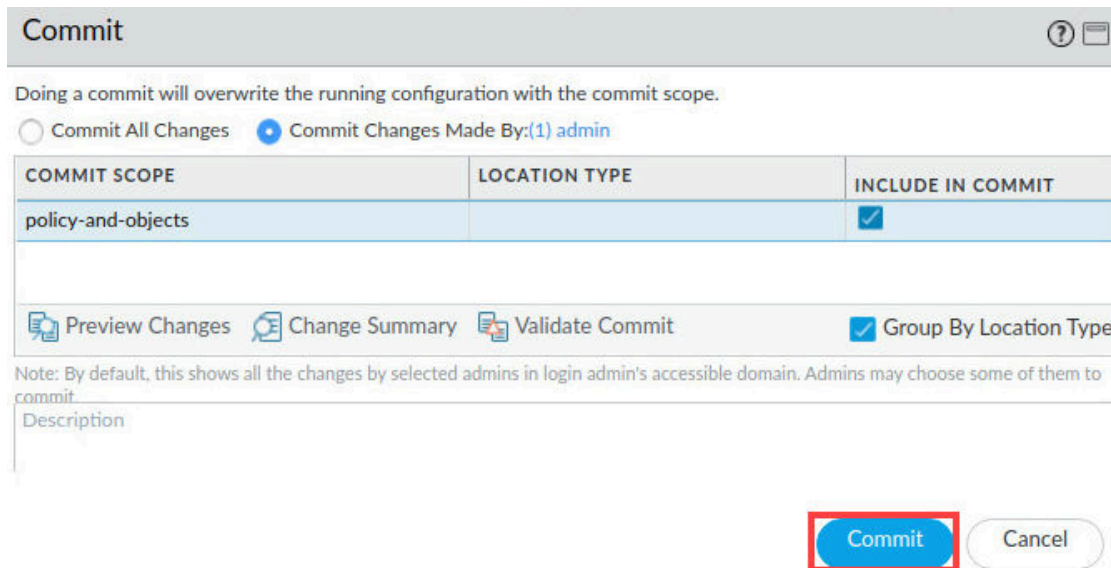
The image shows a list of security policy rules. The first rule, 'block-known-bad-urls', is highlighted with a red box around its index '5'. Below the list, a context menu is open, showing options: 'Move Top', 'Move Up', 'Move Down', 'Move Bottom', and 'Move'. The 'Move Top' option is highlighted with a red box. At the bottom of the interface, there are buttons for 'Add', 'Delete', 'Clone', 'Override', 'Revert', 'Enable', 'Disable', and 'Move'. The 'Move' button is highlighted with a red box.

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



The image shows a 'Commit' button with a dropdown arrow, highlighted with a red box. It is located in the upper-right corner of the web interface.

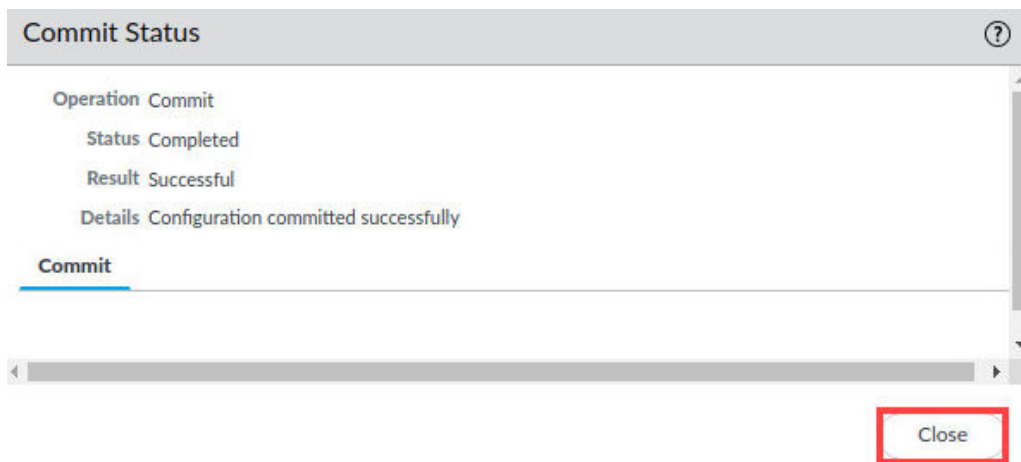
19. In the *Commit* window, click **Commit**.



The **Commit** window shows a confirmation dialog. At the top, it states: "Doing a commit will overwrite the running configuration with the commit scope." Below this, there are two radio buttons: "Commit All Changes" (unselected) and "Commit Changes Made By:(1) admin" (selected). A table lists the commit scope and location type, with a checkbox to include it in the commit. The table has three columns: COMMIT SCOPE, LOCATION TYPE, and INCLUDE IN COMMIT. The first row shows "policy-and-objects" under COMMIT SCOPE, an empty cell under LOCATION TYPE, and a checked checkbox under INCLUDE IN COMMIT. Below the table, there are three tabs: "Preview Changes", "Change Summary", and "Validate Commit". The "Change Summary" tab is active, showing a "Group By Location Type" checkbox which is checked. A note at the bottom states: "Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit." At the bottom right, there are two buttons: "Commit" (highlighted with a red box) and "Cancel".

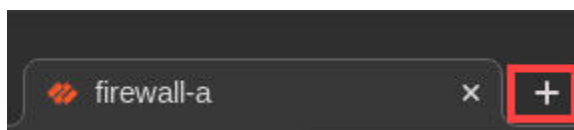
COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

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

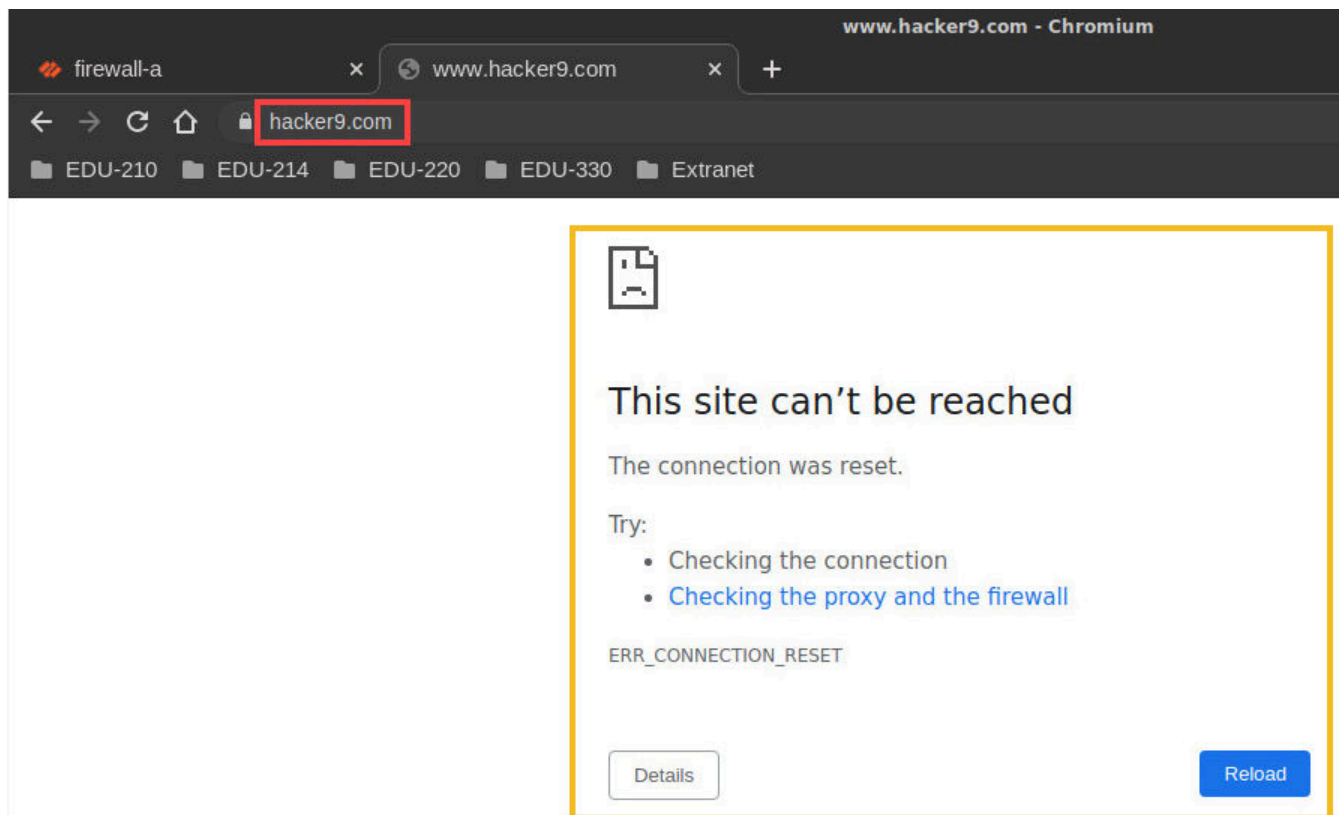


The **Commit Status** window displays the results of the commit operation. It shows the following information: Operation: Commit, Status: Completed, Result: Successful, and Details: Configuration committed successfully. Below this information, there is a tab labeled "Commit" which is currently selected. At the bottom right, there is a "Close" button (highlighted with a red box).

21. Open a new tab in **Chromium**.



22. Type **hacker9.com** which belongs to the *URL category hacking* in the address bar, and press **Enter**.



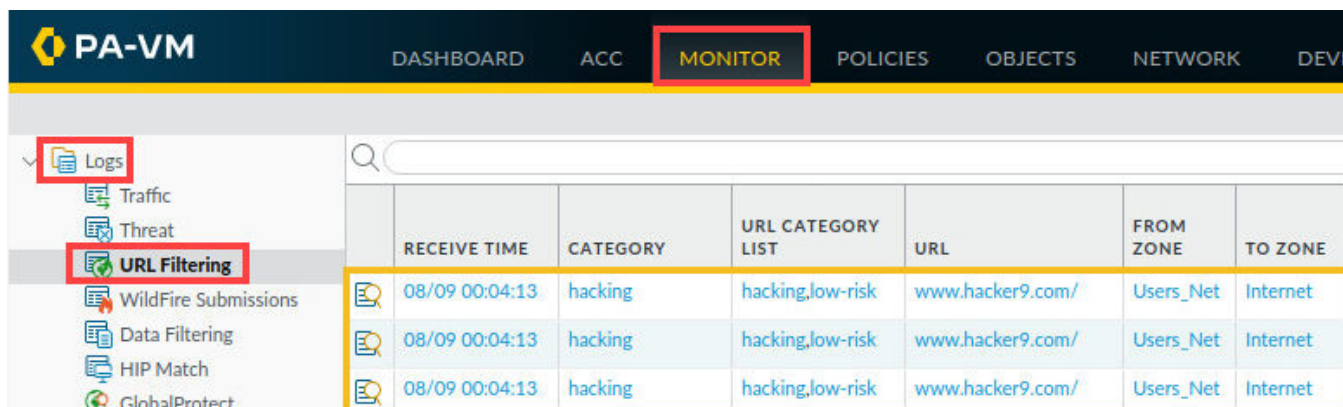
Please Note

The browser should display an error message similar to the following example because the URL category *hacking* is blocked in the security policy. If you get a browser window, it was likely a version cached locally by the browser. Refresh the browser window and access should be blocked.

23. Close the *hacker9.com* tab by clicking the **X** icon.



24. In the web interface, select **Monitor > Logs > URL Filtering**. If the **URL Category List** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category List**.



	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE
	08/09 00:04:13	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet
	08/09 00:04:13	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet
	08/09 00:04:13	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet

Please Note

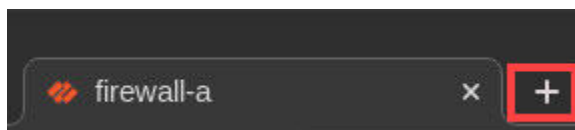
You should see multiple entries that have been blocked. Several default columns have been hidden in the example URL Filtering log file shown here.

25. Leave the firewall open and continue to the next task.

7.11 Create a Custom URL Category

In this section, you will add your Custom URL Category to a security policy rule that has a “deny” action.

1. Open a new tab in **Chromium**.



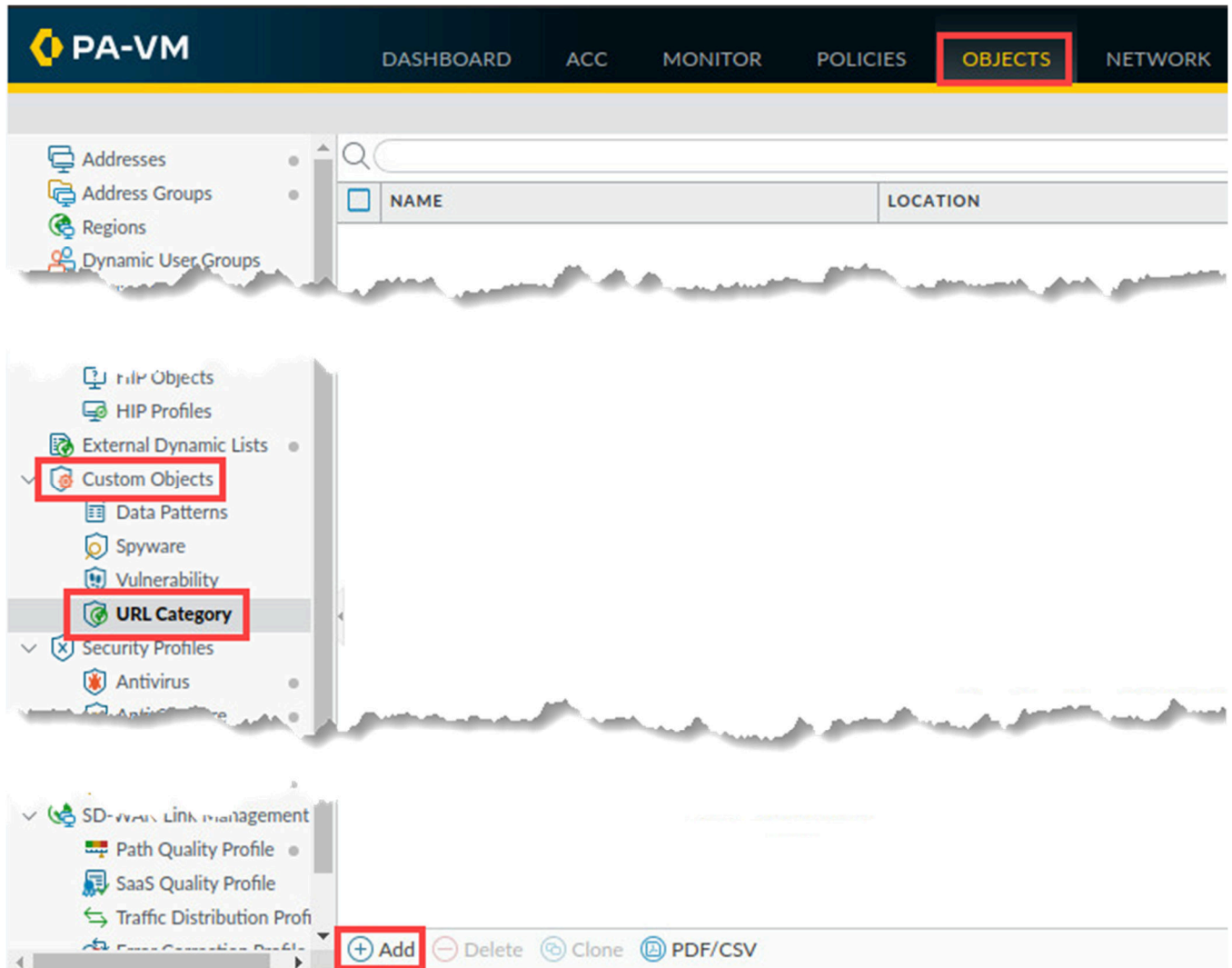
2. Type **www.nbcnews.com** and press **Enter**. The browser should display a valid webpage.



3. Close the *nbcnews.com* tab by clicking the **X** icon.

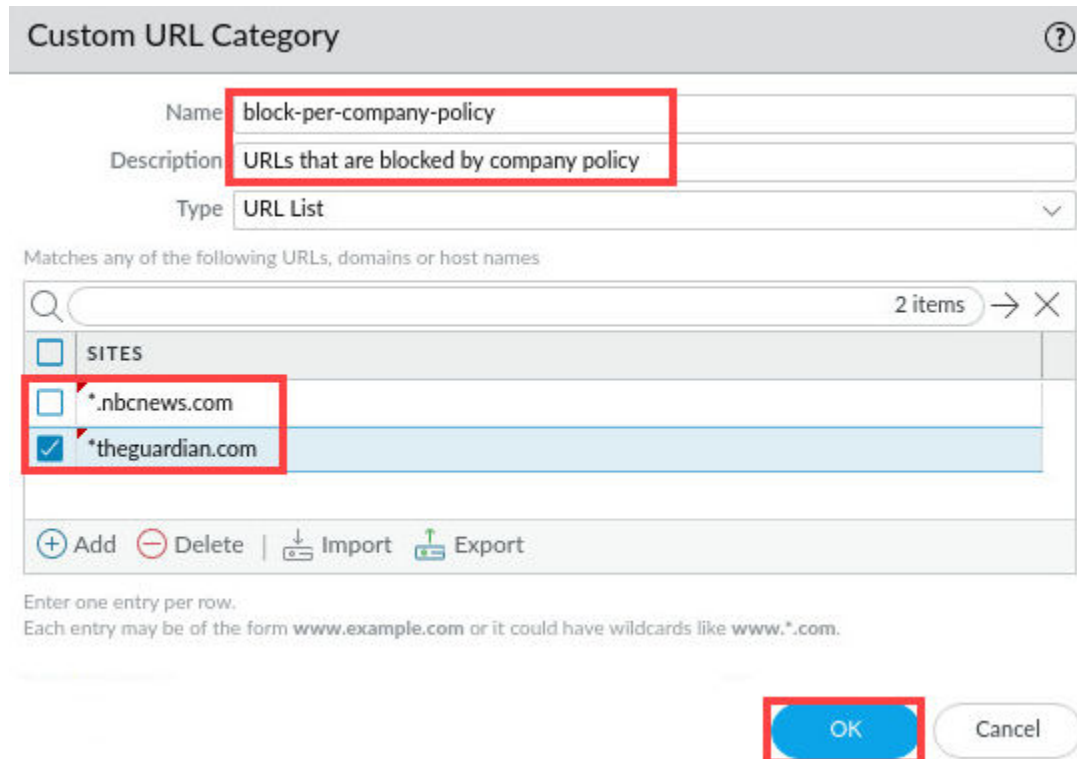


4. In the web interface, select **Objects > Custom Objects > URL Category**. Click **Add**.



5. In the *Custom URL Category* window, configure the following. Click **OK**.

Parameter	Value
Name	block-per-company-policy
Description	URLs that are blocked by company policy.
Sites	Add the following: *.nbcnews.com *.theguardian.com



Custom URL Category ⓘ

Name:

Description:

Type:

Matches any of the following URLs, domains or host names

2 items → ×

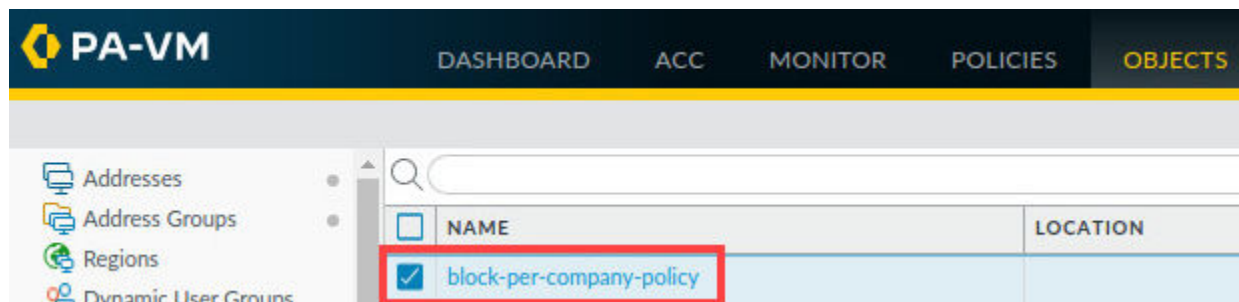
<input type="checkbox"/>	SITES
<input type="checkbox"/>	*.nbcnews.com
<input checked="" type="checkbox"/>	*.theguardian.com

⊕ Add ⊖ Delete | 📁 Import 📄 Export

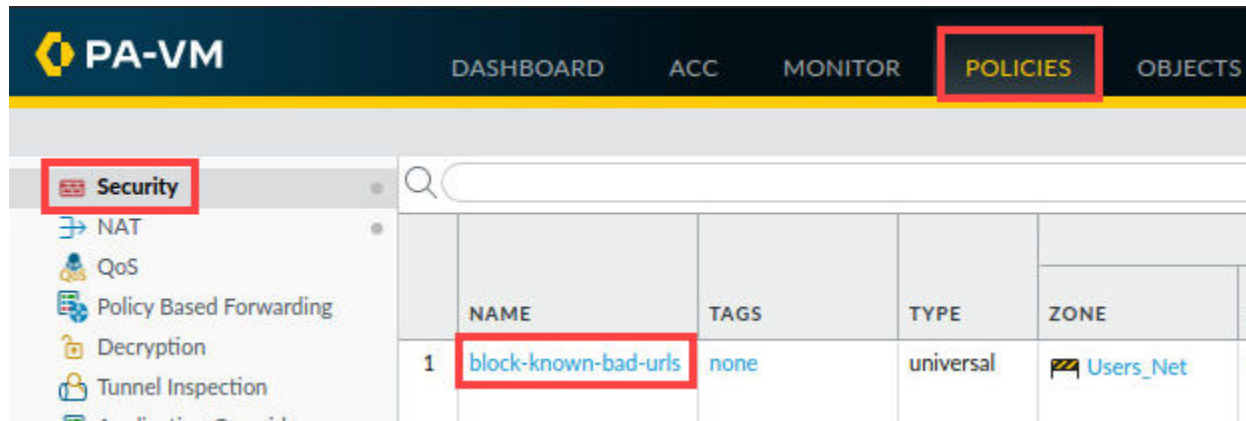
Enter one entry per row.
Each entry may be of the form `www.example.com` or it could have wildcards like `www.*.com`.

OK Cancel

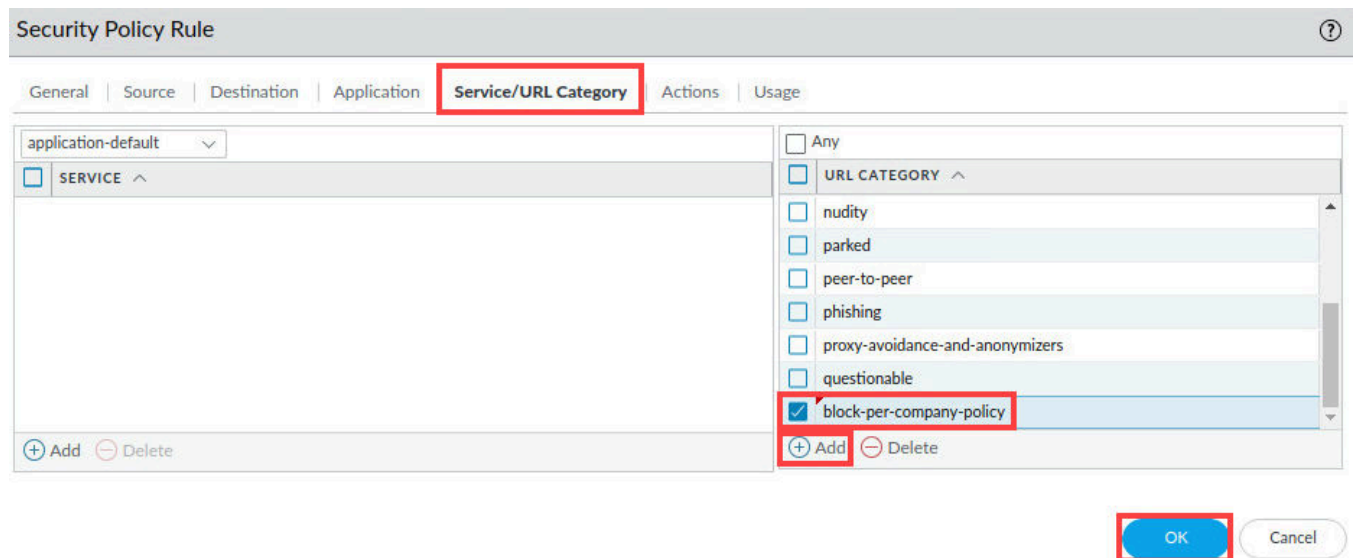
6. Confirm the *block-per-company-policy* Custom URL is showing in the *URL Category* window.



7. Add your *Custom URL Category* to a security policy rule that has a **deny** action. Select **Policies > Security**. Click **block-known-bad-urls** to edit the rule.



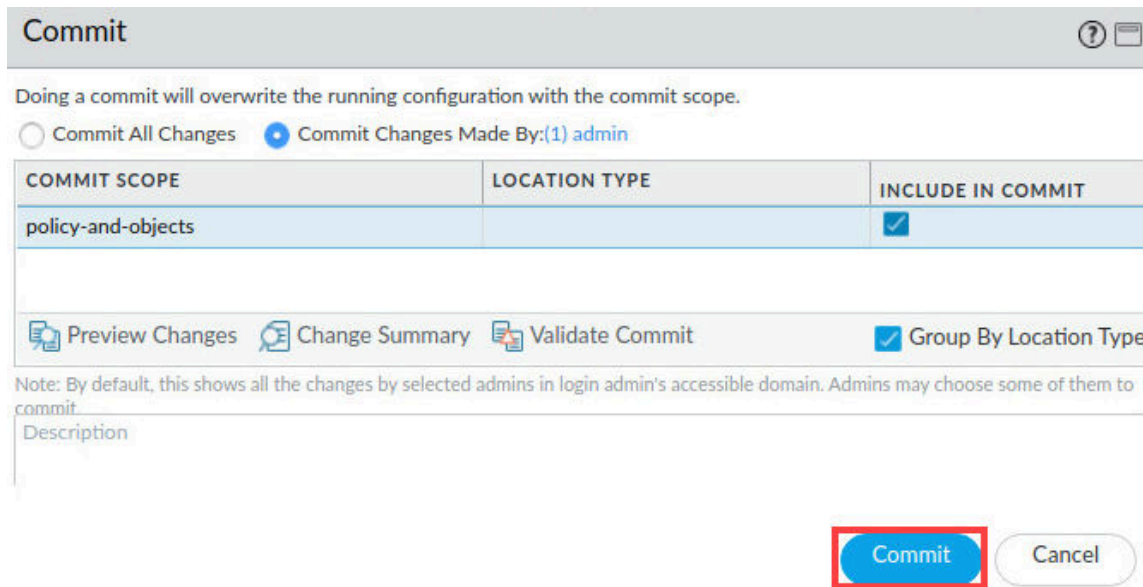
8. Select the **Service/URL Category** tab and click **Add**. Add **block-per-company-policy** to the list. Click **OK**.



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



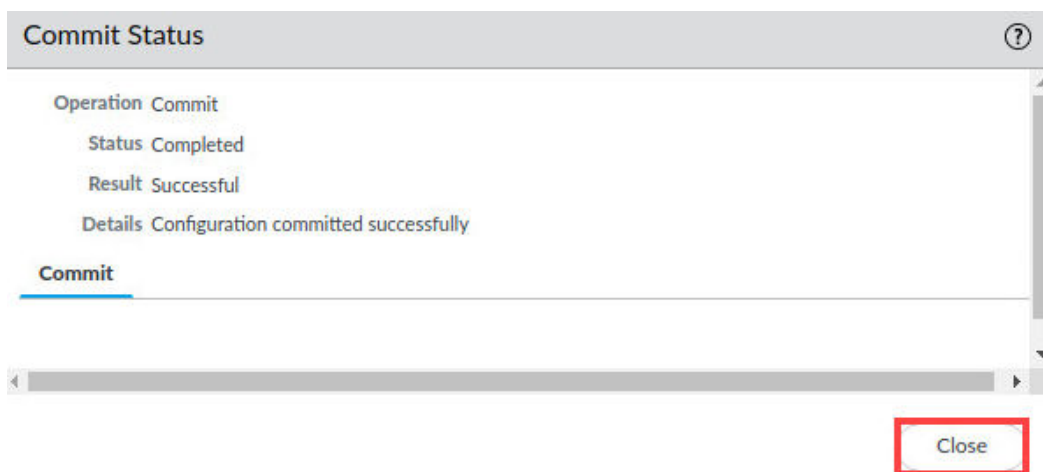
10. In the *Commit* window, click **Commit**.



The **Commit** window shows a confirmation dialog. At the top, it states: "Doing a commit will overwrite the running configuration with the commit scope." Below this, there are two radio buttons: "Commit All Changes" (unselected) and "Commit Changes Made By: (1) admin" (selected). A table lists the commit scope and location type, with a checkbox to include it in the commit. The table has three columns: COMMIT SCOPE, LOCATION TYPE, and INCLUDE IN COMMIT. The first row shows "policy-and-objects" under COMMIT SCOPE, which is checked under INCLUDE IN COMMIT. Below the table, there are three tabs: "Preview Changes", "Change Summary", and "Validate Commit". The "Group By Location Type" checkbox is checked. A note at the bottom states: "Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit." Below the note is a text area labeled "Description". At the bottom right, there are two buttons: "Commit" (highlighted with a red box) and "Cancel".

COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

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



The **Commit Status** window displays the results of the commit operation. It shows: "Operation Commit", "Status Completed", "Result Successful", and "Details Configuration committed successfully". Below this, there is a tab labeled "Commit" which is selected. At the bottom right, there is a "Close" button (highlighted with a red box).

12. Test access to URLs that belong to the *Custom URL Category* that you added to a security policy *deny* rule. Open two new tabs in **Chromium**.



13. Type **www.nbcnews.com** on the first tab and press **Enter**. Type **www.theguardian.com** on the second tab and press **Enter**.



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

Details

Reload

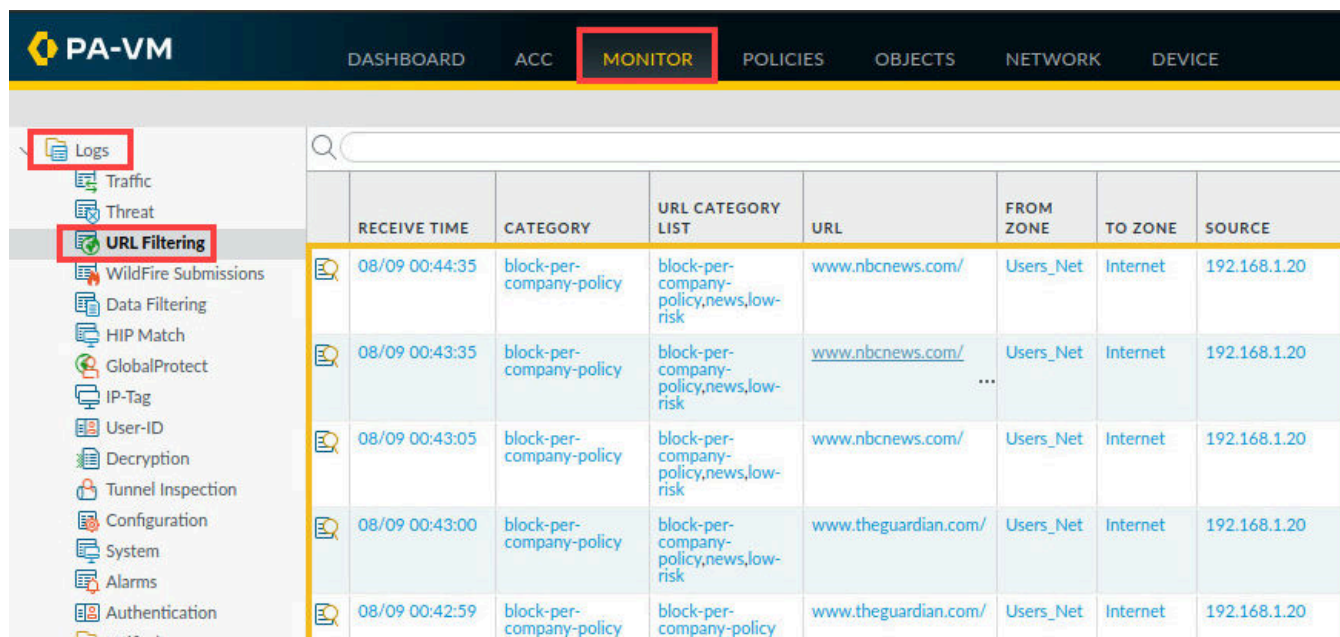
Please
Note

The browser should display an error message because the Custom URL Category in the security policy blocks access to the webpage.

14. Close the *nbcnews* and *theguardian* tabs by clicking the **X** icon.



15. In the web interface, select **Monitor > Logs > URL Filtering**. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **down-arrow**) and select **Columns > URL Category**.



	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE
	08/09 00:44:35	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/	Users_Net	Internet	192.168.1.20
	08/09 00:43:35	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/	Users_Net	Internet	192.168.1.20
	08/09 00:43:05	block-per-company-policy	block-per-company-policy,news,low-risk	www.nbcnews.com/	Users_Net	Internet	192.168.1.20
	08/09 00:43:00	block-per-company-policy	block-per-company-policy,news,low-risk	www.theguardian.com/	Users_Net	Internet	192.168.1.20
	08/09 00:42:59	block-per-company-policy	block-per-company-policy	www.theguardian.com/	Users_Net	Internet	192.168.1.20

Please Note

You should see multiple entries for sessions to www.nbcnews.com and www.theguardian.com that the firewall has blocked.

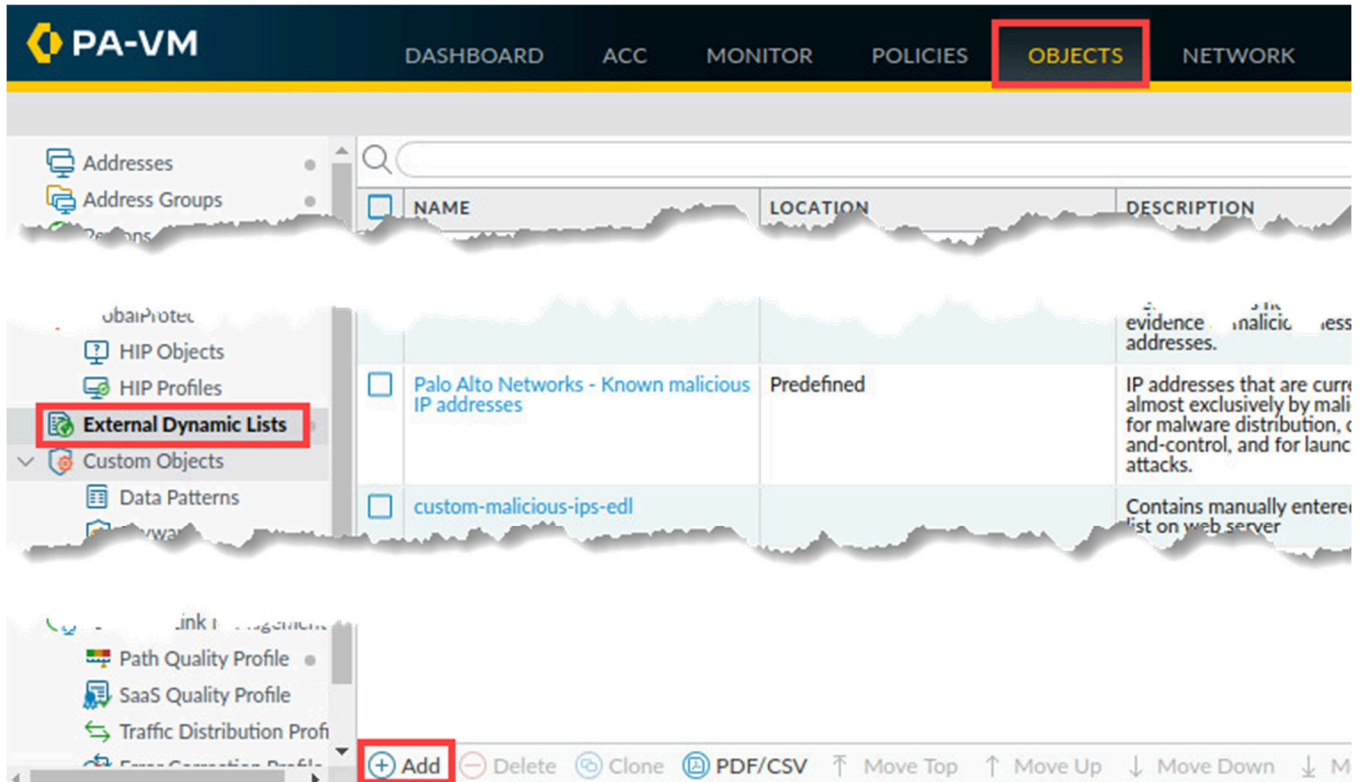
16. Leave the firewall open and continue to the next task.

7.12 Create an EDL to Block Malicious URL Access

You can add a list of malicious URLs to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that you can regularly update the malicious URL list without the need to recommit the firewall configuration each time, as you would have to do if you updated a security policy rule with a new URL.

In this section, you will create an EDL to block malicious URL access.

1. In the web interface, select **Objects > External Dynamic Lists**. Click **Add**.



NAME	LOCATION	DESCRIPTION
<input type="checkbox"/> Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently almost exclusively by malware for malware distribution, command-and-control, and for launch attacks.
<input type="checkbox"/> custom-malicious-ips-edl		Contains manually entered list on web server

Toolbar: **Add** (highlighted), Delete, Clone, PDF/CSV, Move Top, Move Up, Move Down, Move Bottom

2. In the *External Dynamic Lists* window, configure the following. Click **OK**.

Parameter	Value
Name	malicious-urls-edl
Type	URL List
Source	http://192.168.50.80/malicious-urls.txt (The EDL contains only the URL www.popurls.com)
Check for updates	Five Minute

External Dynamic Lists

Name

malicious-urls-edl

Create List

List Entries And Exceptions

Type

URL List

Description

Source

http://192.168.50.80/malicious-urls.txt

Server Authentication

Certificate Profile

None

Check for updates

Five Minute

Test Source URL

OK

Cancel

**Please
Note**

The malicious-urls.txt file contains an entry for popurls.com.

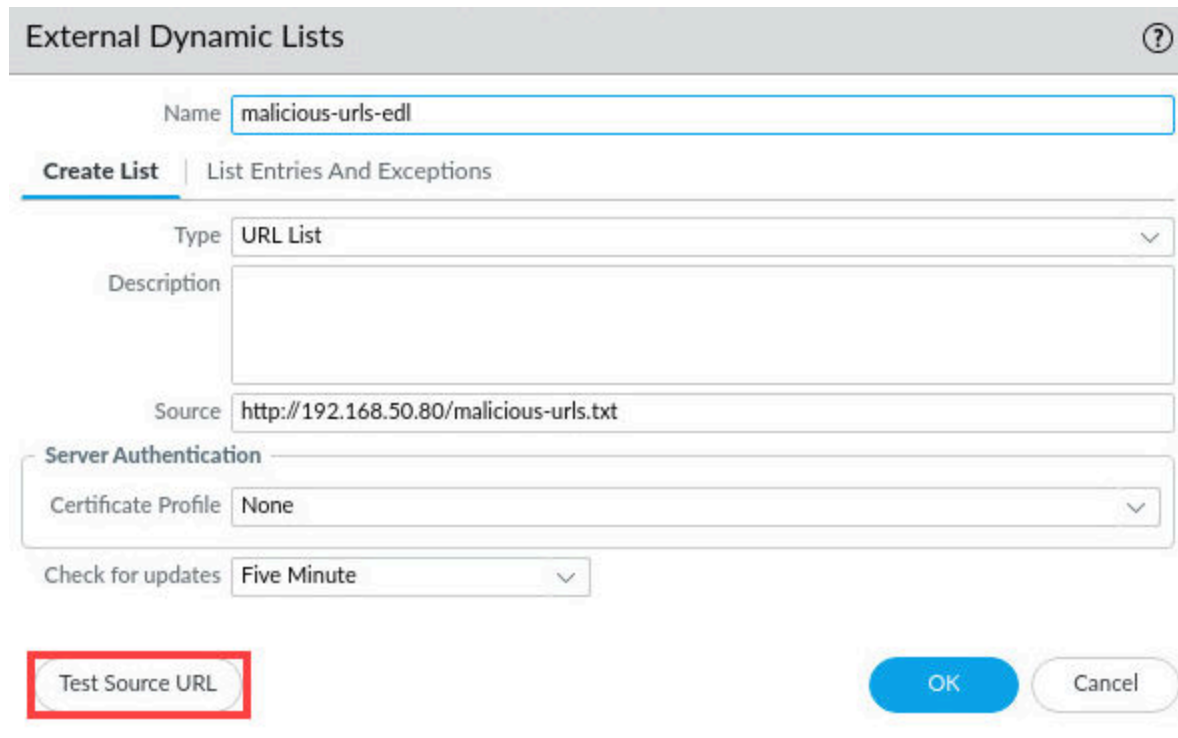
3. In the *External Dynamic Lists* window, click **malicious-urls-edl**.

Dynamic URL Lists

☐
Palo Alto Networks - Authentication Portal Exclude List

☐
malicious-urls-edl

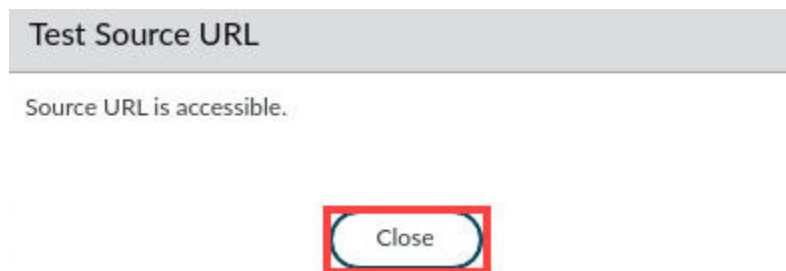
- Click **Test Source URL** and verify the firewall can access the *EDL URL*.



The 'External Dynamic Lists' window is shown with the following configuration:

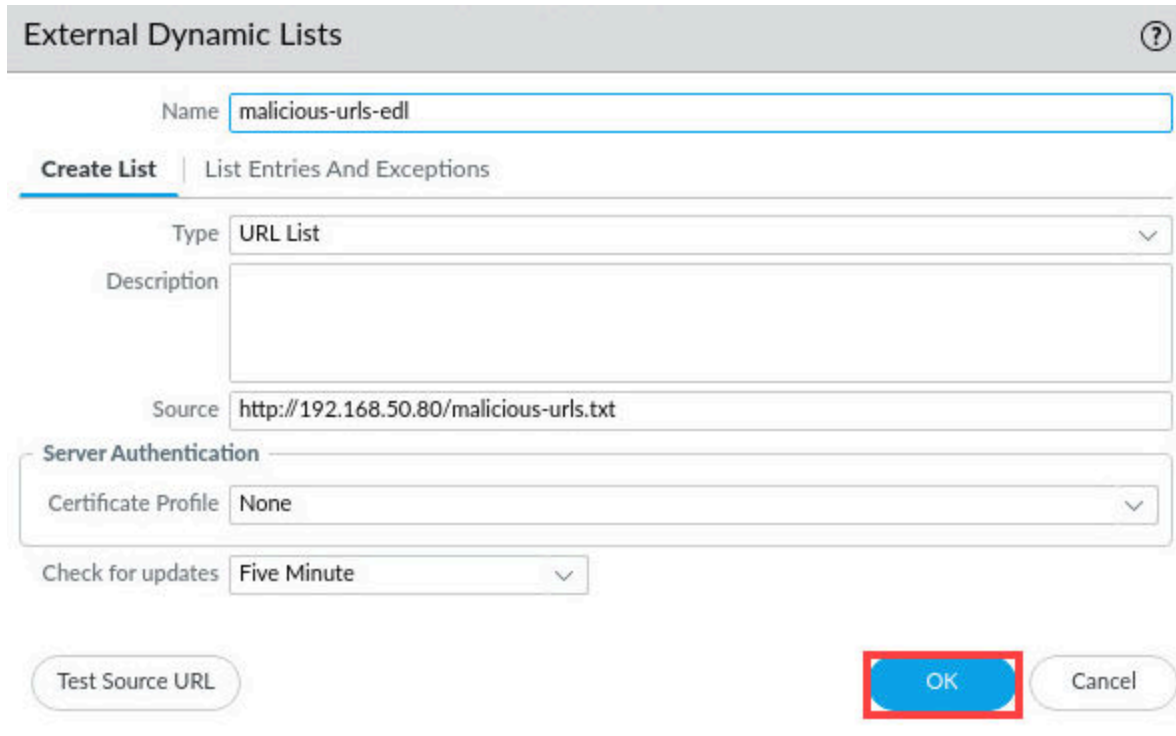
- Name:** malicious-urls-edl
- Tab:** Create List (selected), List Entries And Exceptions
- Type:** URL List
- Description:** (empty text area)
- Source:** http://192.168.50.80/malicious-urls.txt
- Server Authentication:**
 - Certificate Profile:** None
- Check for updates:** Five Minute
- Buttons:** Test Source URL (highlighted with a red box), OK, Cancel

- In the *Test Source URL* window, verify the *Source URL* is accessible. Click **Close**.



The 'Test Source URL' window displays the message 'Source URL is accessible.' and a 'Close' button (highlighted with a red box).

6. In the *External Dynamic List* window, click **OK**.



The screenshot shows the 'External Dynamic Lists' configuration window. The 'Name' field is set to 'malicious-urls-edl'. The 'Type' is 'URL List'. The 'Source' is 'http://192.168.50.80/malicious-urls.txt'. The 'Certificate Profile' is 'None'. The 'Check for updates' is set to 'Five Minute'. The 'OK' button is highlighted with a red box.

External Dynamic Lists ⓘ

Name

Create List | List Entries And Exceptions

Type

Description

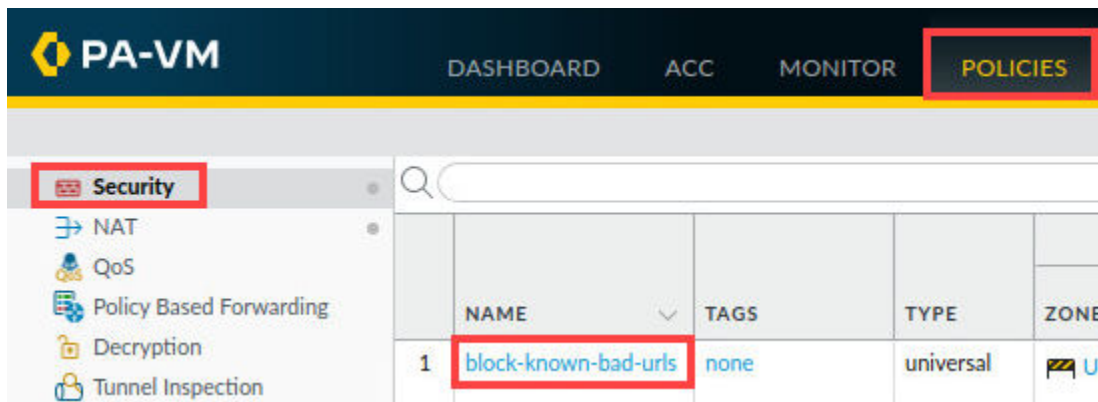
Source

Server Authentication

Certificate Profile

Check for updates

7. Add the *EDL* containing the malicious URL list to a security policy rule with a *deny* action. In the web interface, select **Policies > Security**. Click **block-known-bad-urls** to edit the rule.



The screenshot shows the PA-VM web interface. The 'POLICIES' tab is selected. The 'Security' section is expanded, showing a list of security policy rules. The rule 'block-known-bad-urls' is highlighted with a red box.

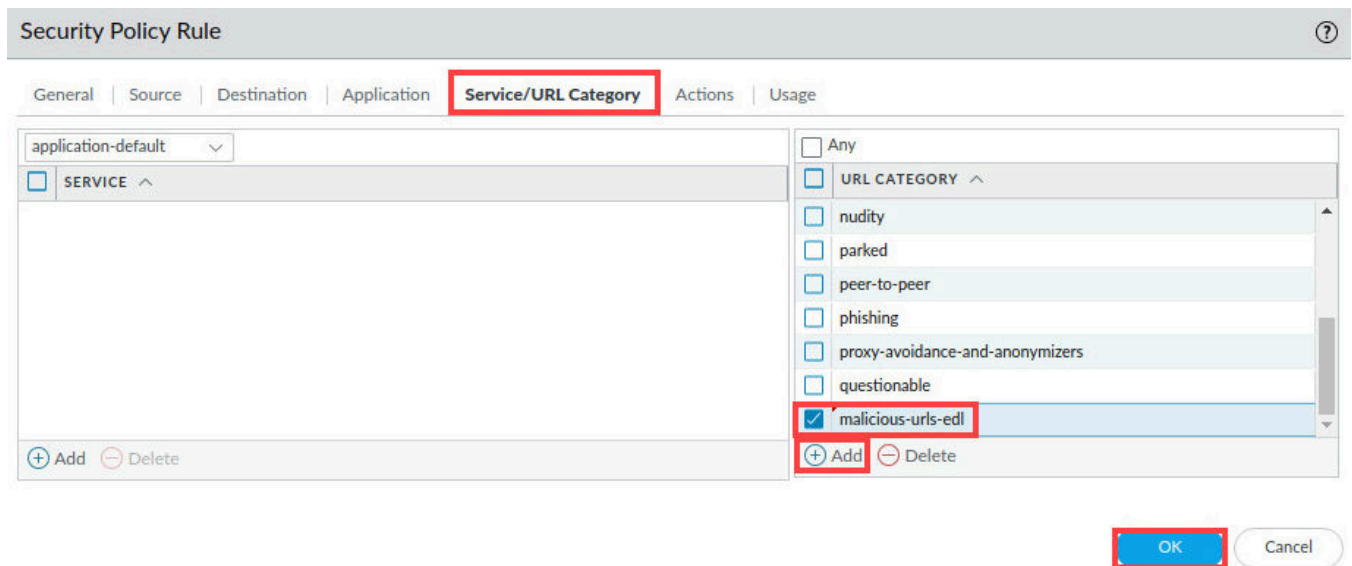
PA-VM DASHBOARD ACC MONITOR **POLICIES**

Security

- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection

	NAME	TAGS	TYPE	ZONE
1	block-known-bad-urls	none	universal	U

8. In the *Security Policy Rule* window, click the **Service/URL Category** tab. Add **malicious-urls-edl** to the list. Click **OK**.



Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

application-default

☐ SERVICE ^

☐ Any

☐ URL CATEGORY ^

☐ nudity

☐ parked

☐ peer-to-peer

☐ phishing

☐ proxy-avoidance-and-anonymizers

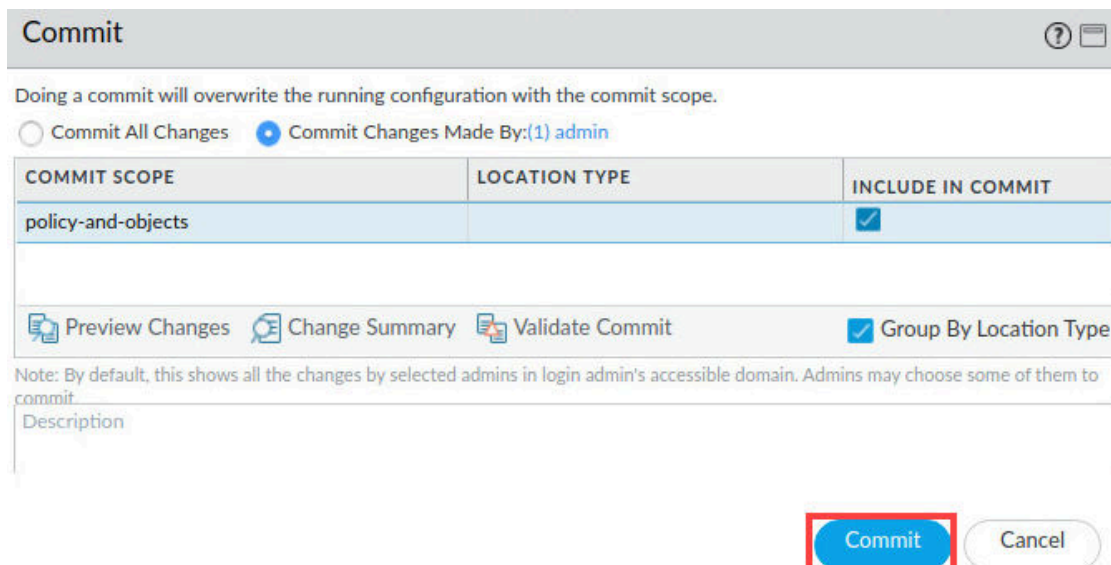
☐ questionable

☒ **malicious-urls-edl**

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



10. 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

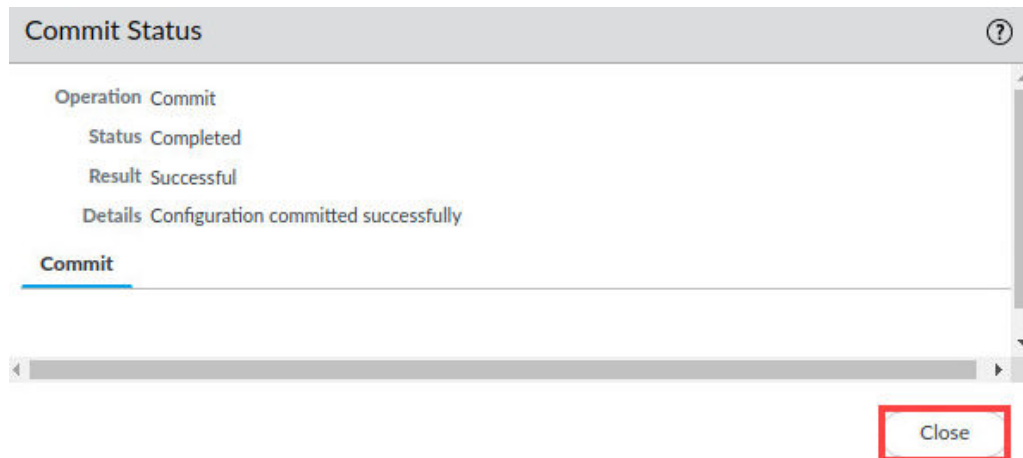
COMMIT SCOPE	LOCATION TYPE	INCLUDE IN COMMIT
policy-and-objects		<input checked="" type="checkbox"/>

☒ Group By Location Type

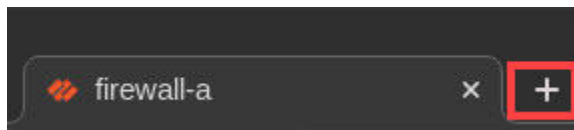
Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit.

Description

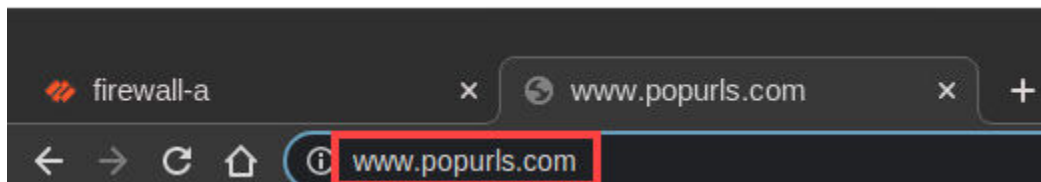
11. Wait until the *Commit* process is complete. Click **Close**.



12. Test access to a URL contained in the EDL that you added to the *block-known-bad-urls* security policy. Open a new tab in **Chromium**.



13. Type **http://www.popurls.com** in the address bar.



14. The browser displays a block page because the EDL in the security policy blocks access to the *popurls.com* webpage.



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

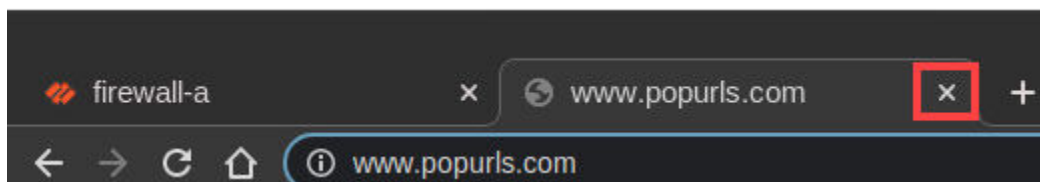
Details

Reload

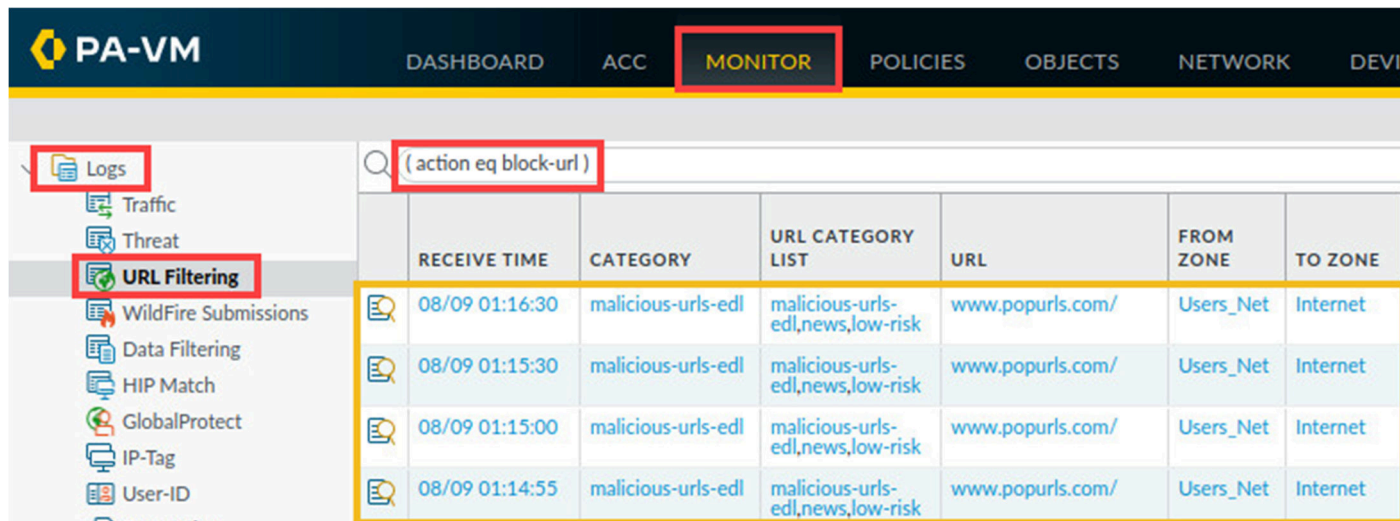
**Please
Note**

The browser should display an error message because the Custom URL Category in the security policy blocks access to the webpage.

15. Close the *popurls.com* tab by clicking the **X** icon.



16. In the web interface, select **Monitor > Logs > URL Filtering**. Type (`action eq block-url`) in the filter builder. You should see multiple entries for sessions to *www.popurls.com* that the firewall has blocked.



	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE
	08/09 01:16:30	malicious-urls-edl	malicious-urls-edl,news,low-risk	www.popurls.com/	Users_Net	Internet
	08/09 01:15:30	malicious-urls-edl	malicious-urls-edl,news,low-risk	www.popurls.com/	Users_Net	Internet
	08/09 01:15:00	malicious-urls-edl	malicious-urls-edl,news,low-risk	www.popurls.com/	Users_Net	Internet
	08/09 01:14:55	malicious-urls-edl	malicious-urls-edl,news,low-risk	www.popurls.com/	Users_Net	Internet

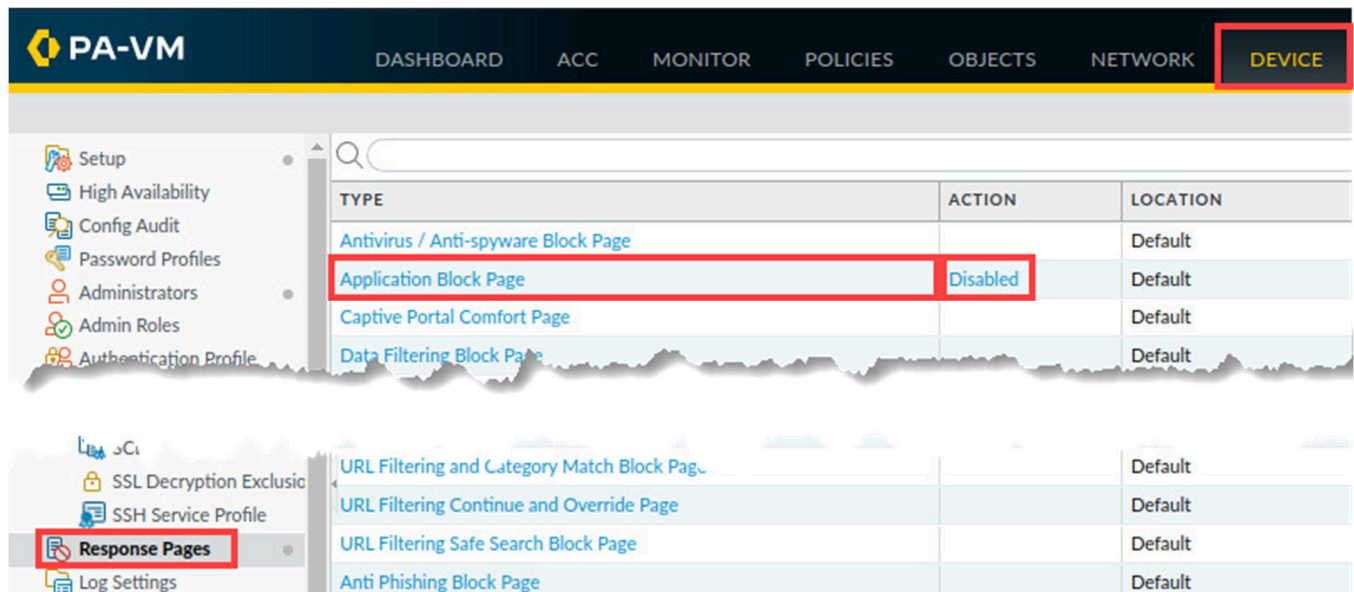
17. Leave the firewall open and continue to the next task.

7.13 Block Access to a Malicious URL Using a URL Filtering Profile

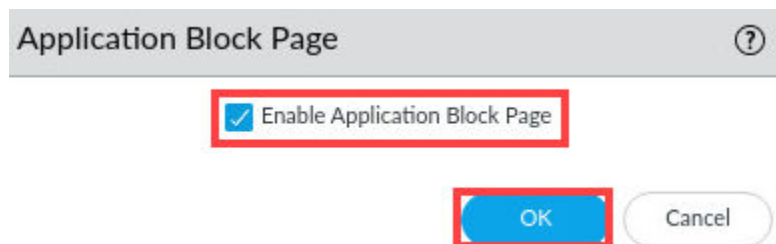
Now you will configure a URL Filtering Profile to control access to URLs. You must add the URL Filtering Profile to a security policy rule with an “allow” action. The use of a URL Filtering Profile to block access to URLs typically is easier to maintain over time compared to the addition of URLs to a security policy block rule. You will also enable the Application Block Page, which instructs the firewall to present a warning page to users when they access websites that have been purposely blocked.

In this section, you will block access to a Malicious URL with a URL Filtering Profile and test the URL Filtering Profile.

1. In the web interface, select **Device > Response Pages**. Locate the entry for **Application Block Page** and click the link for **Disabled** under the *Action* column.



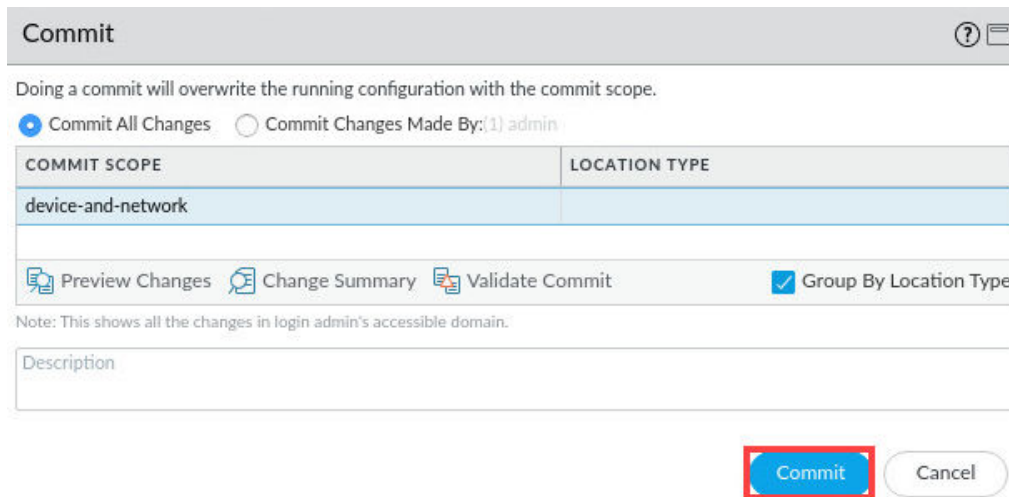
2. In the *Application Block Page* window, place a **check** in the box for **Enable Application Block Page**. Click **OK**.



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



4. 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	

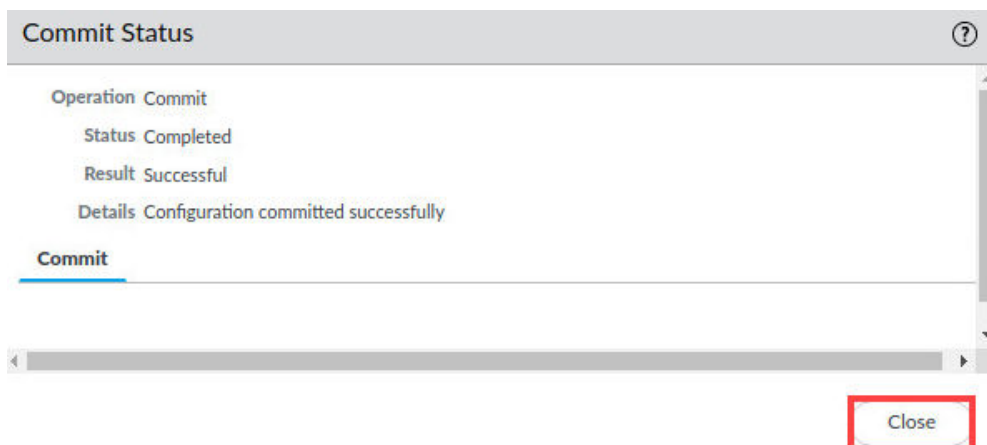
Preview Changes
 Change Summary
 Validate Commit
 ☒ Group By Location Type

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

Description

Commit Cancel

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



Commit Status ⓘ

Operation Commit

Status Completed

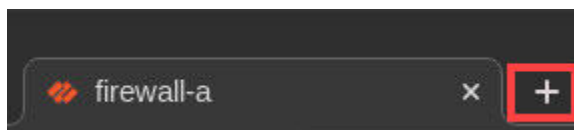
Result Successful

Details Configuration committed successfully

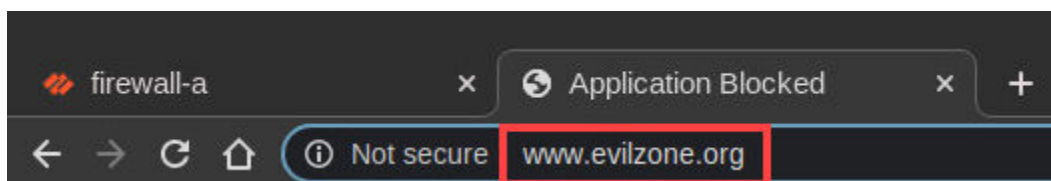
Commit

Close

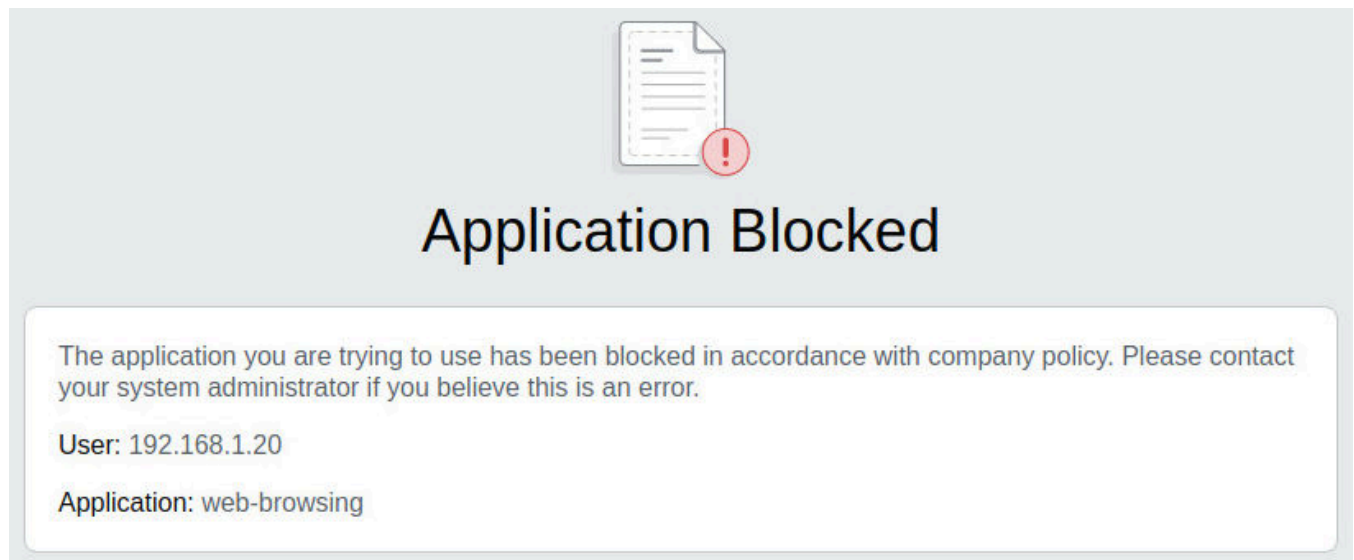
6. Test the *Application Block Page* response. Open a new tab in **Chromium**.



7. Type **www.evilzone.org** in the address bar, press **Enter**.



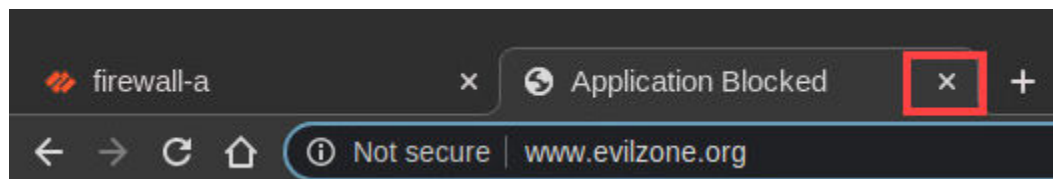
8. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage.



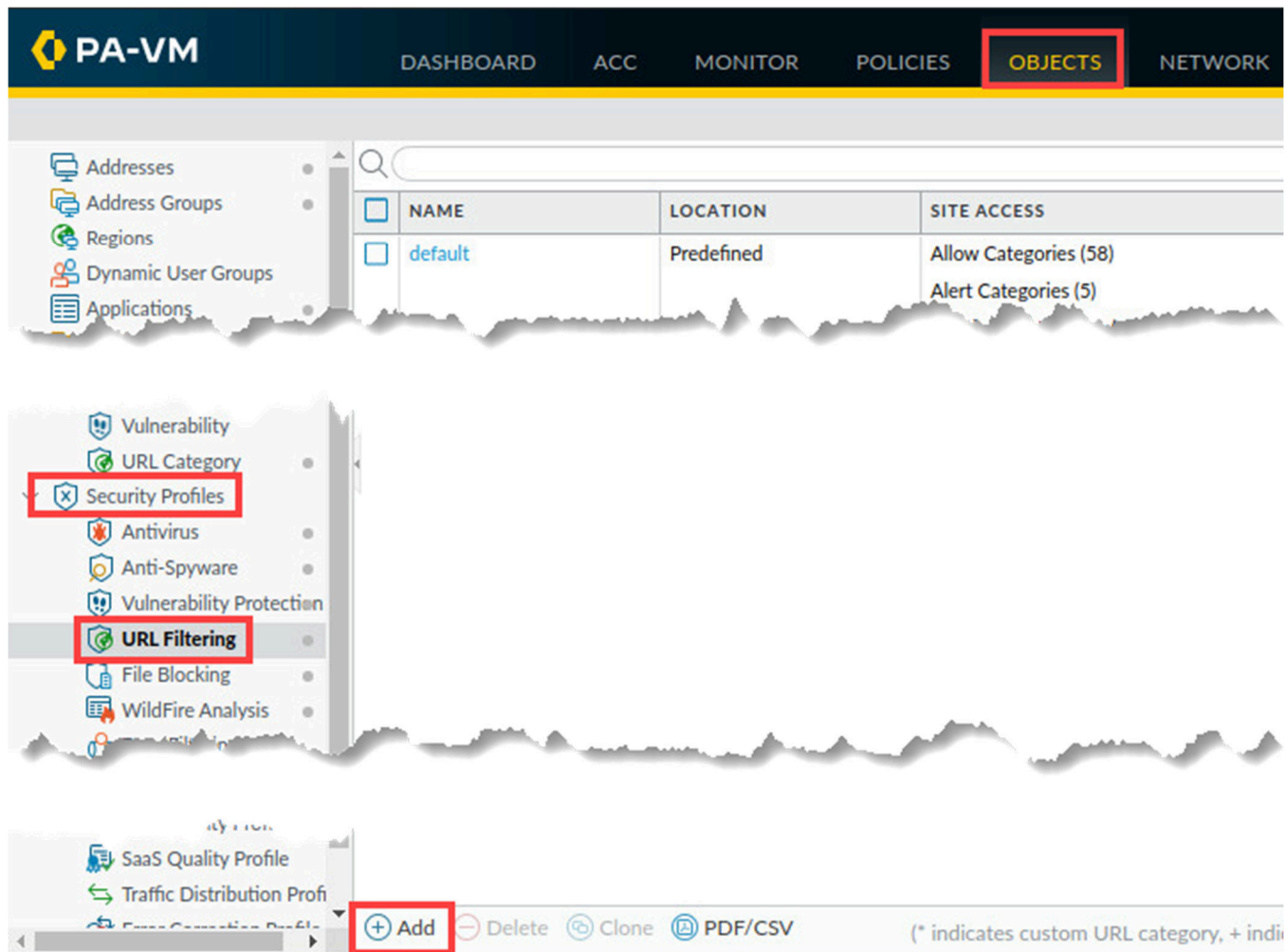
**Please
Note**

The browser should display a block page because the URL belongs to the URL category *hacking*, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

9. Close the *evilzone.org* tab by clicking the **X** icon.

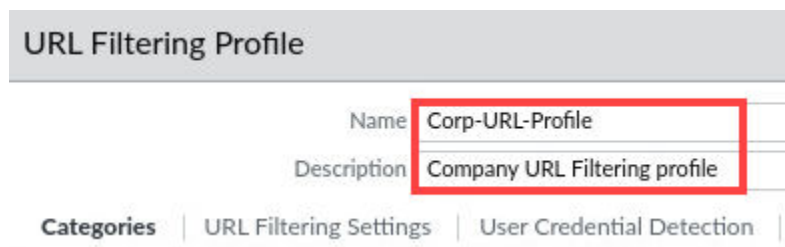


10. In the web interface, select **Objects > Security Profiles > URL Filtering**. Click **Add** to create a new profile.



The screenshot shows the PA-VM web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (highlighted with a red box), and 'NETWORK'. On the left sidebar, under 'Security Profiles', 'URL Filtering' is highlighted with a red box. Below the sidebar, the 'Add' button (a circle with a plus sign) is highlighted with a red box. The main content area shows a table with columns 'NAME', 'LOCATION', and 'SITE ACCESS'. The 'NAME' column contains 'default'. The 'LOCATION' column contains 'Predefined'. The 'SITE ACCESS' column contains 'Allow Categories (58)' and 'Alert Categories (5)'.

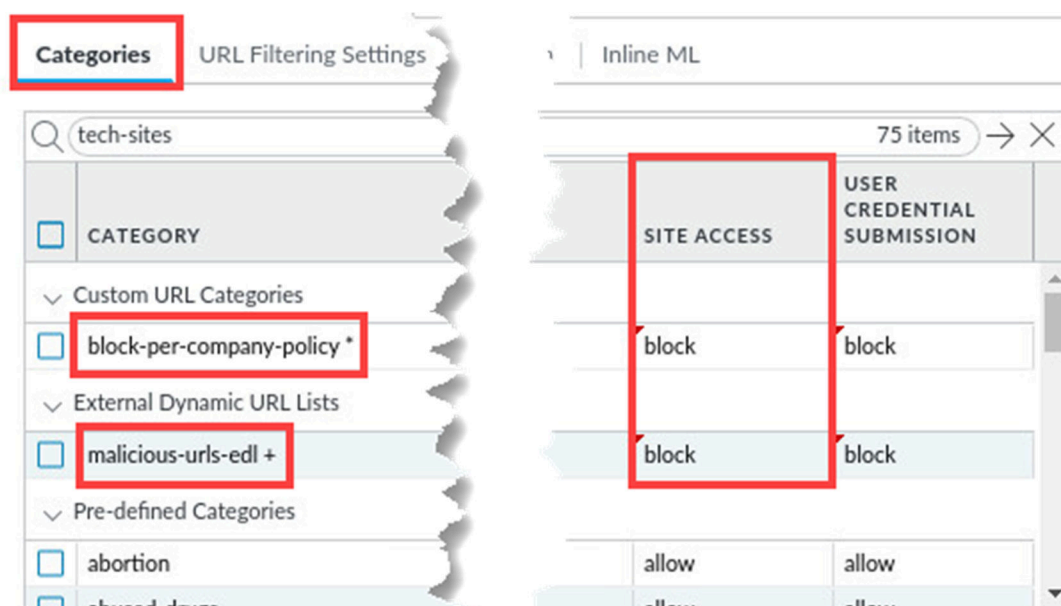
11. In the *URL Filtering Profile*, type **Corp-URL-Profile** as the *Name* of the profile. For *Description*, enter **Company URL Filtering profile**.



The screenshot shows the 'URL Filtering Profile' configuration form. The 'Name' field contains 'Corp-URL-Profile' and the 'Description' field contains 'Company URL Filtering profile', both highlighted with red boxes. Below the fields are three tabs: 'Categories' (selected), 'URL Filtering Settings', and 'User Credential Detection'.

12. On the **Categories** tab, configure the following. You will need to scroll through each *Category* for the value to set it to block the site access.

Parameter	Value
Site Access	Configure the block action for the following URL categories: block-per-company-policy* (your Custom URL Category) malicious-urls-edl+ (your custom URL list) adult command-and-control extremism hacking high-risk malware nudity parked peer-to-peer phishing proxy-avoidance-and-anonymizers questionable



Please Note

These categories are the same ones you set to **block** earlier using the URL Category as part of the security policy rule. In this configuration, the firewall will use the URL Filtering profile to block these categories.

13. Select the tab for **Inline ML**. For **Phishing Detection** and **Javascript Exploit Detection**, set the **Policy Action** to **block**. Click **OK**.

URL Filtering Profile ?

Name: Corp-URL-Profile

Description: Company URL Filtering profile

Categories: URL Filtering Settings | User Credential Detection | HTTP Header Insertion | **Inline ML**

Available Models

MODEL	DESCRIPTION	ACTION ^
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages	block
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block

OK Cancel

14. In the web interface, select **Policies > Security**. Click **Users_to_Internet** to edit the rule.

PA-VM DASHBOARD ACC MONITOR **POLICIES** OBJECTS

Security

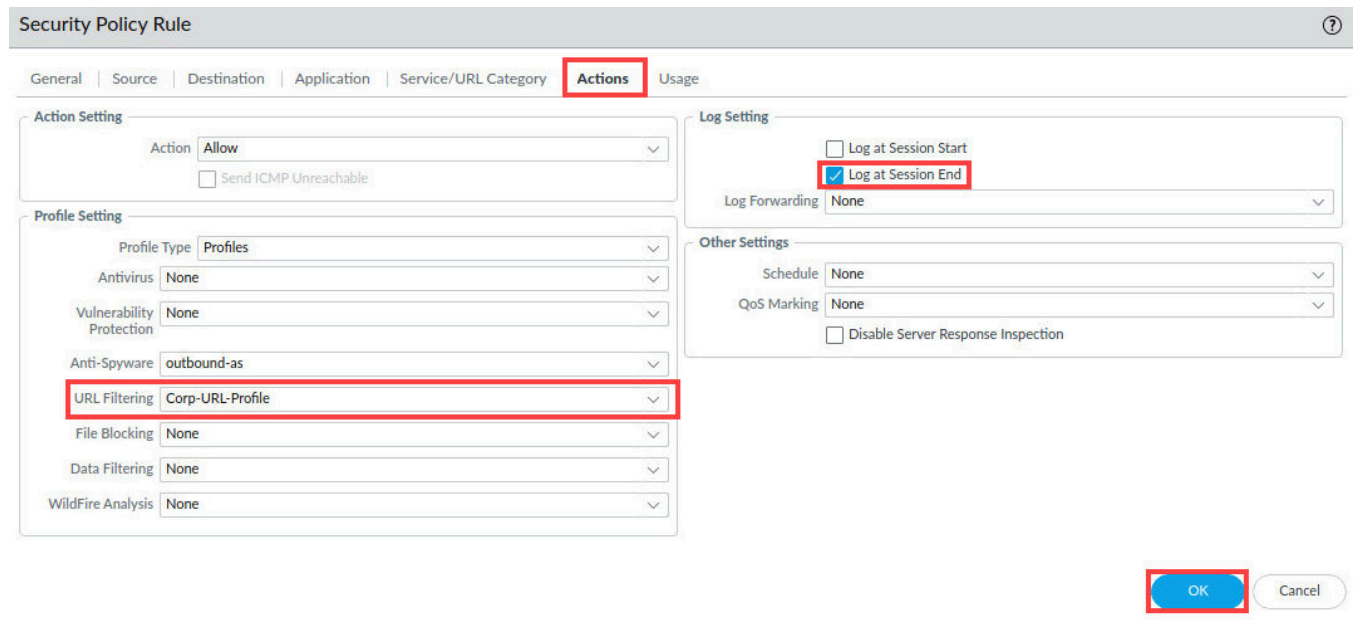
NAT

QoS

3	Users_to_Extranet	none	universal	Users_Net	any
4	Users_to_Internet	none	universal	Users_Net	any
5	Extranet_to_Internet	none	universal	Extranet	any

15. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Click **OK**.

Parameter	Value
Action	Allow
Log Setting	Log at Session End
Profile Type	Profiles
URL Filtering	Corp-URL-Profile



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: outbound-as

URL Filtering: Corp-URL-Profile

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

☐ Log at Session Start

☒ **Log at Session End**

Log Forwarding: None

Other Settings

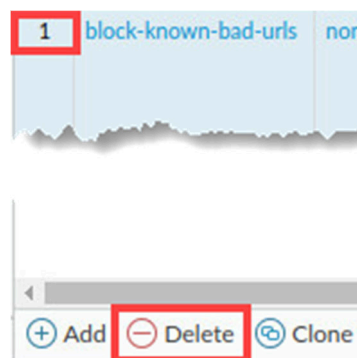
Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

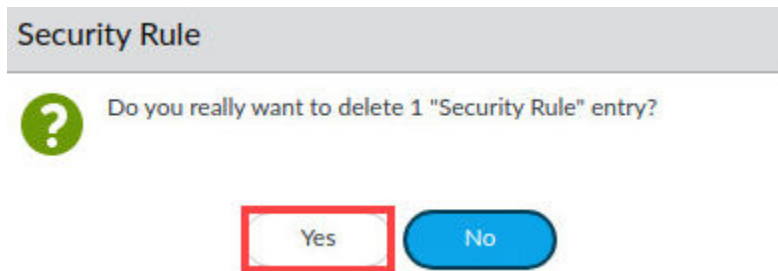
16. Select, but do not open the *block-known-bad-urls* security policy rule. Click **Delete** to remove the *block-known-bad-urls* rule.



Please Note

This rule no longer will be used to block access to the URLs. Instead, the "Users_to_Internet" rule with its attached URL Filtering Profile will control URL access.

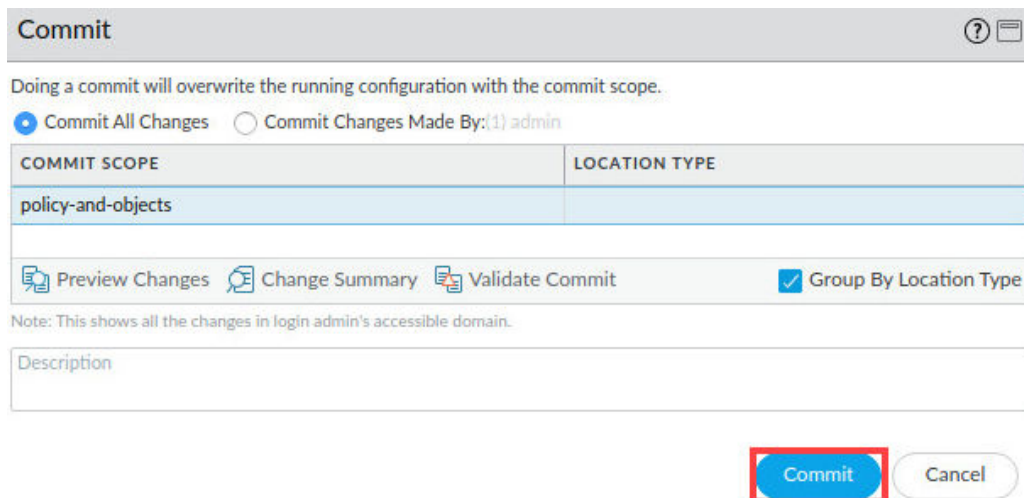
17. In the *Security Rule* window, click **Yes** to confirm the deletion.



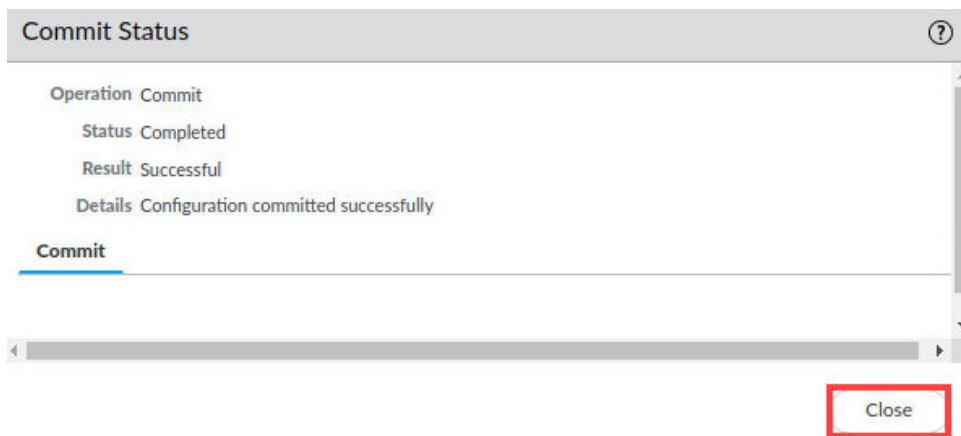
18. Click the **Commit** button at the upper-right of the web interface.



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



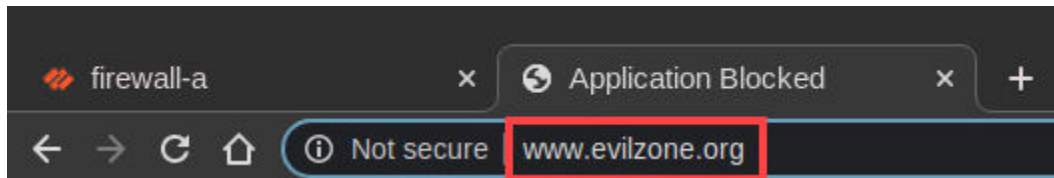
20. Wait until the *Commit* process is complete. Click **Close**.



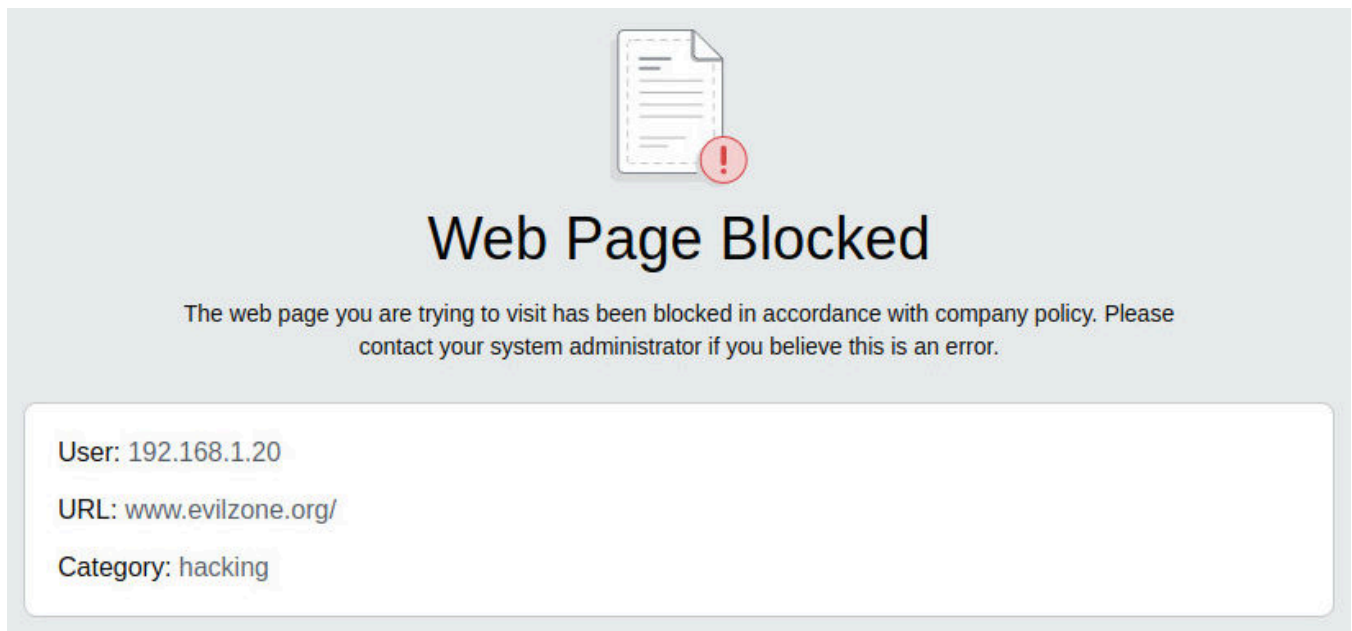
21. Test the *Application Block Page* response. Open a new tab in **Chromium**.



22. Type **www.evilzone.org** and press **Enter**.



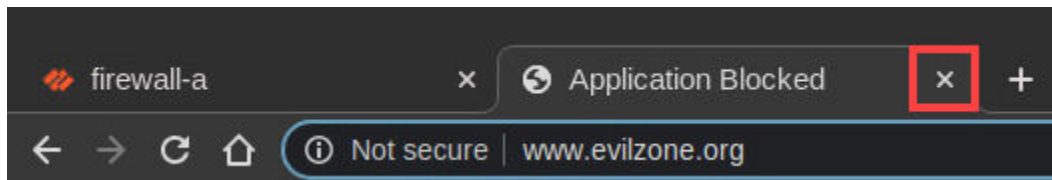
23. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage. If the *Web Page Blocked* message does not appear, allow 1 to 3 minutes for the firewall to process the changes, then refresh the *evilzone.org* tab.



**Please
Note**

The browser should display a block page because the URL belongs to the URL category *hacking*, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

24. Close the *evilzone.com* tab by clicking the **X** icon.



25. Examine the URL Filtering Log under **Monitor > Logs > URL Filtering**.



RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE
08/09 02:38:36	hacking	hacking,low-risk	www.evilzone.org/fav...	Users_Net	Internet	192.168.1.20
08/09 02:38:36	hacking	hacking,low-risk	www.evilzone.org/log...	Users_Net	Internet	192.168.1.20
08/09 02:38:36	hacking	hacking,low-risk	www.evilzone.org/...	Users_Net	Internet	192.168.1.20
08/09 02:07:33	hacking	hacking,low-risk	www.evilzone.org/fav...	Users_Net	Internet	192.168.1.20

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