# PALO ALTO NETWORKS EDU 210

# Lab 7: Blocking Threats from Known-Bad Sources

**Document Version: 2021-09-27**

# Contents

## 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.

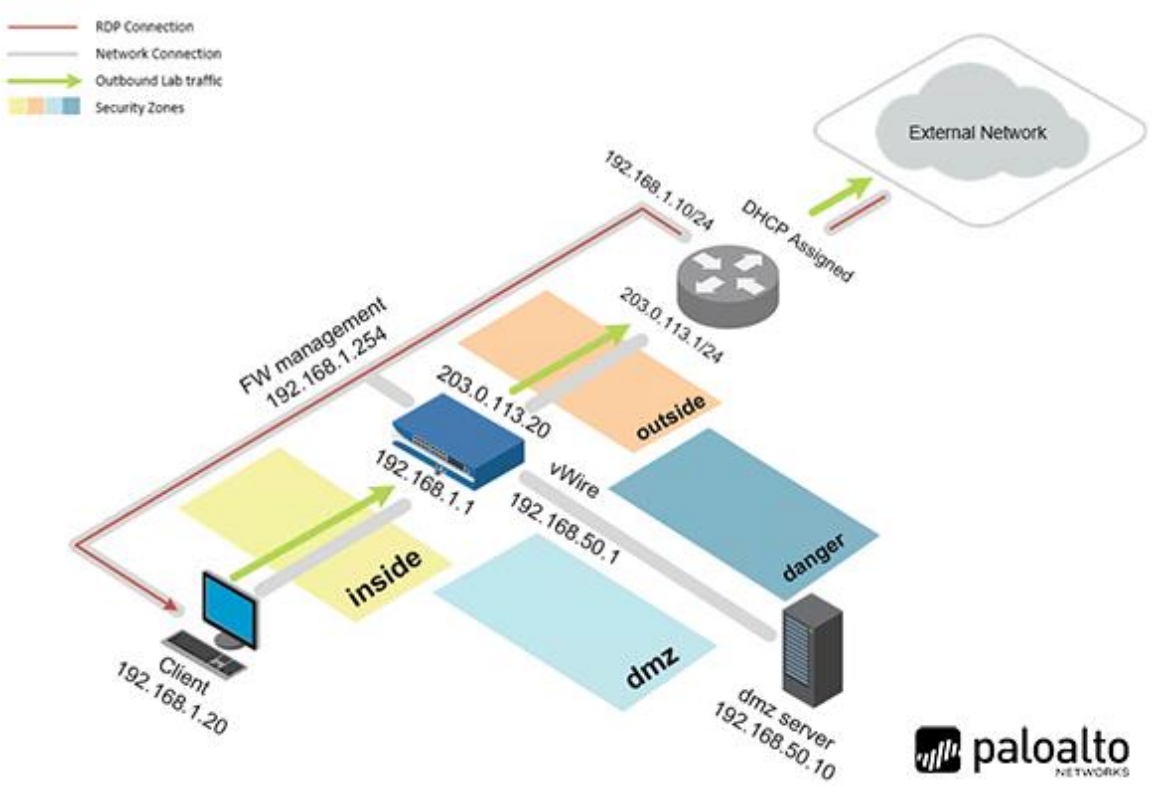
In this section, you will explore the options available on the firewall that allow you to block individual addresses, groups of addresses, and lists of addresses. You will also configure the firewall to block certain categories of websites.

## 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 Topology



## Lab Settings

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

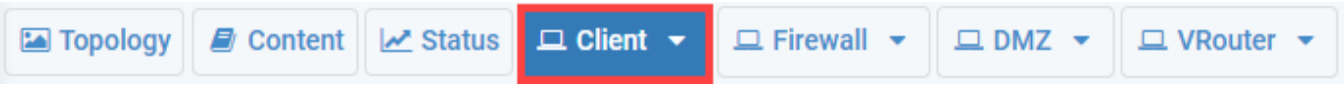
| Virtual Machine | IP Address | Account (if needed) | Password (if needed) |
|---|---|---|---|
| Client | 192.168.1.20 | lab-user | **Pal0Alt0!** |
| DMZ | 192.168.50.10 | root | **Pal0Alt0!** |
| Firewall | 192.168.1.254 | admin | **Pal0Alt0!** |
| VRouter | 192.168.1.10 | root | **Pal0Alt0!** |

# 7 Block Threats from Known-Bad Sources

## 7.1 Apply a Baseline Configuration to the Firewall

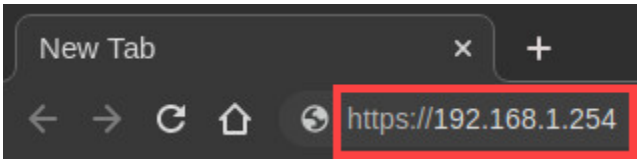
In this section, you will load the firewall configuration file.

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

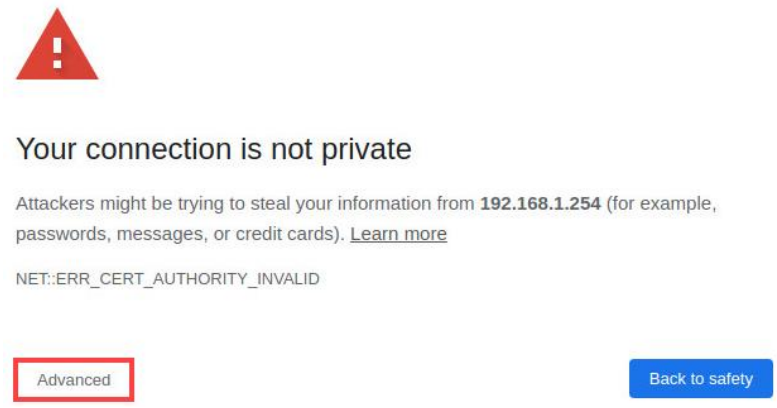



2. Double-click the **Chromium Web Browser** icon located on the *desktop*.


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

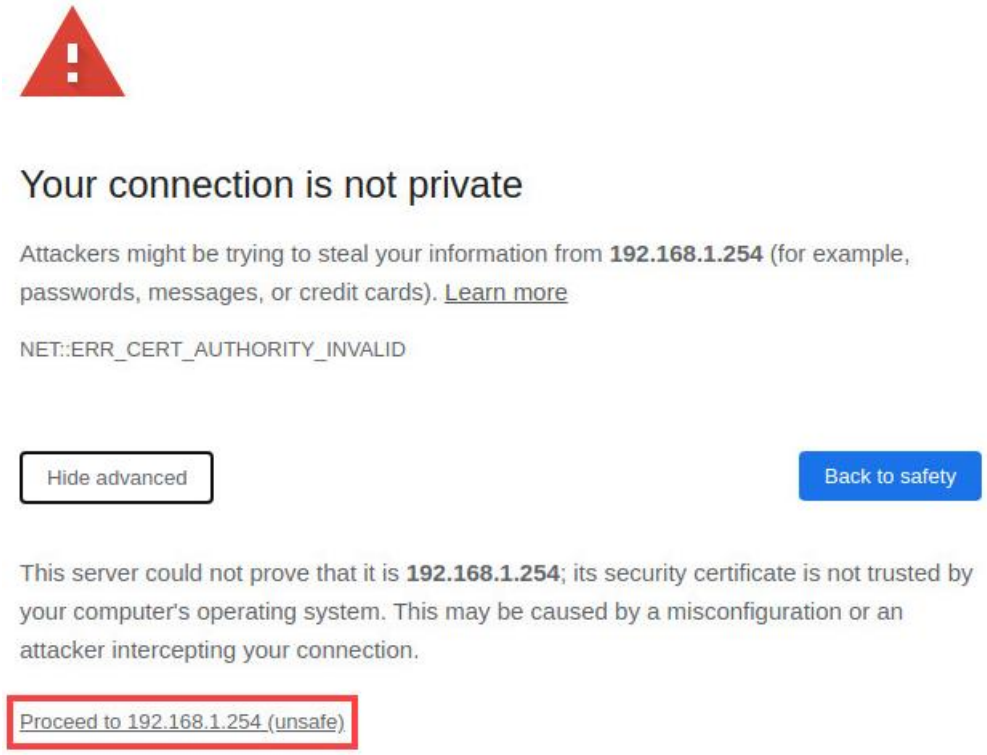



4. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



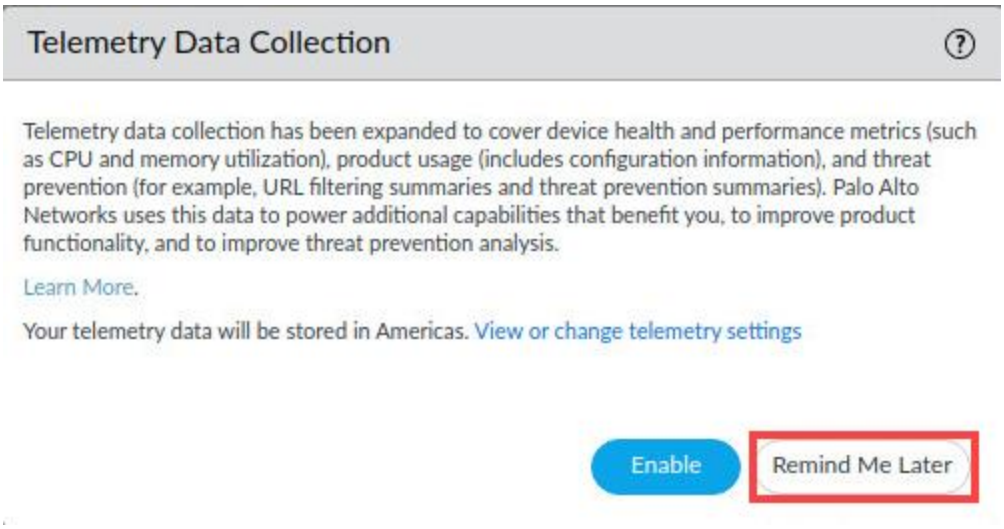

If you experience the "Unable to connect" or "502 Bad Gateway" message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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



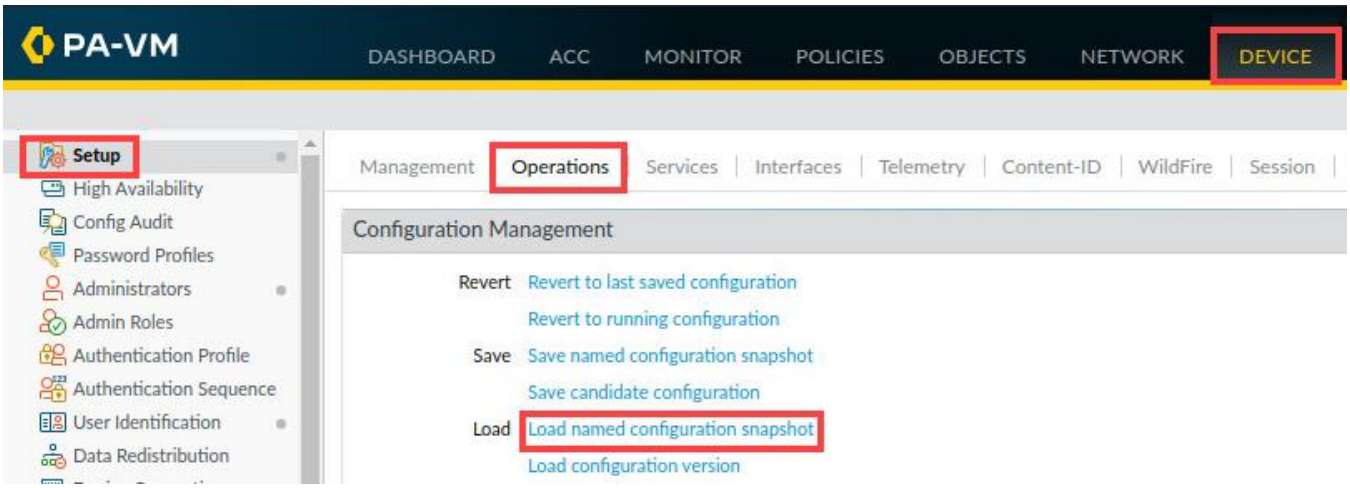

6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

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



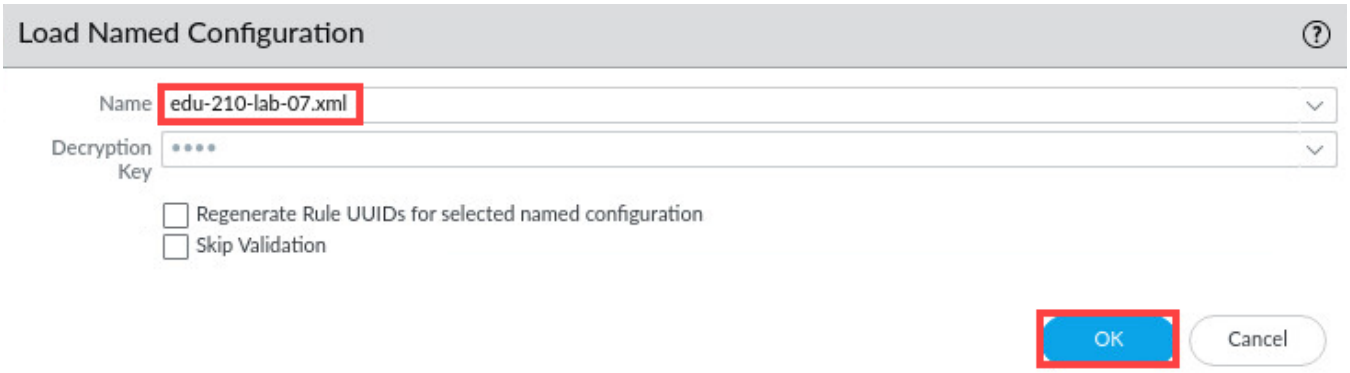

**Please Note** Before you can enable Telemetry Data Collection, you would need to install a device certificate. For this lab, you will not be using Telemetry Data Collection.

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

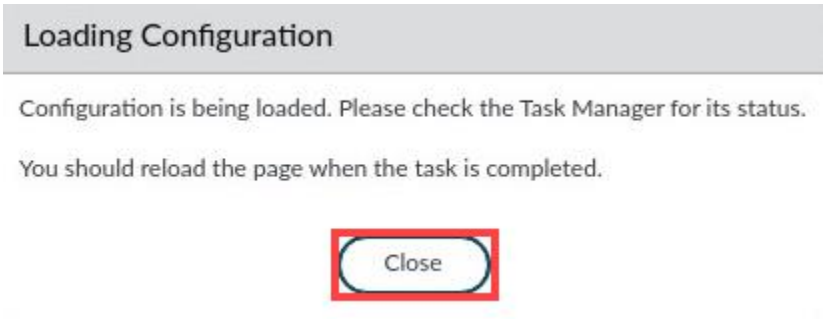


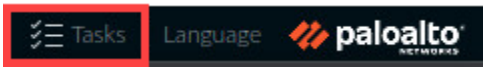
9. In the *Load Named Configuration* window, select **edu-210-lab-07.xml** from the *Name* dropdown box and click **OK**.



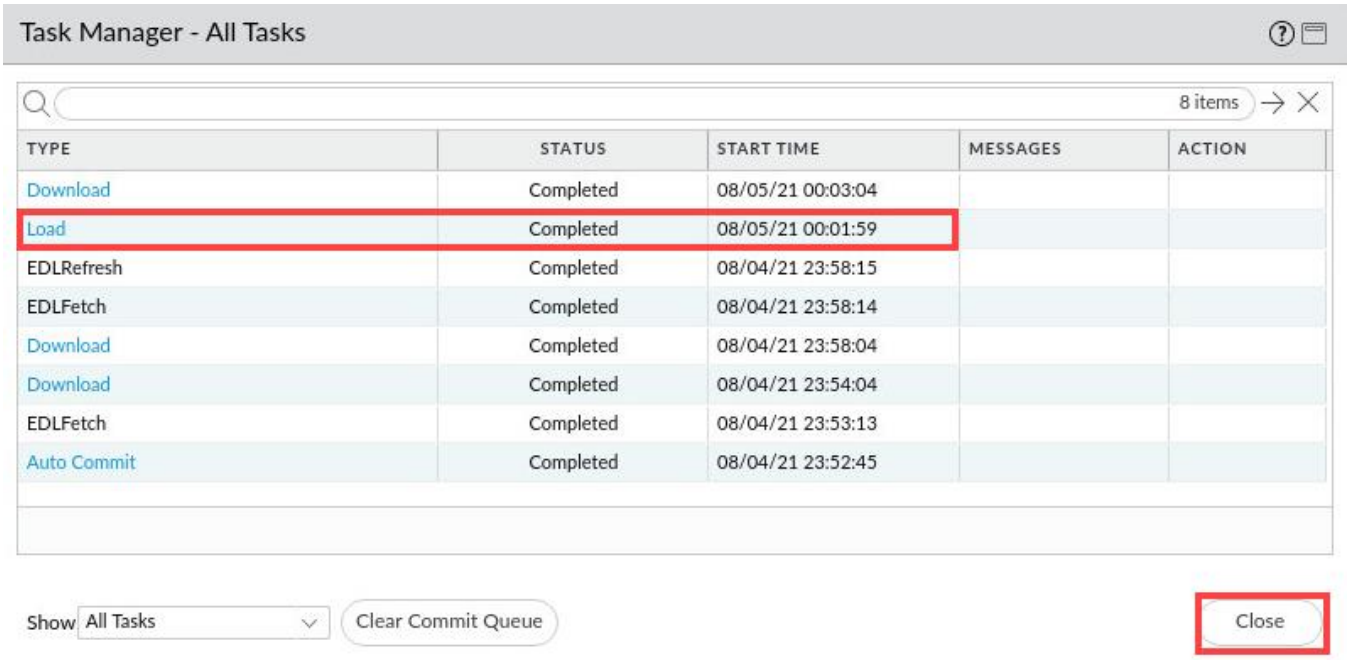

10. In the *Loading Configuration* window, a message will show *Configuration is being loaded*. *Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.




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

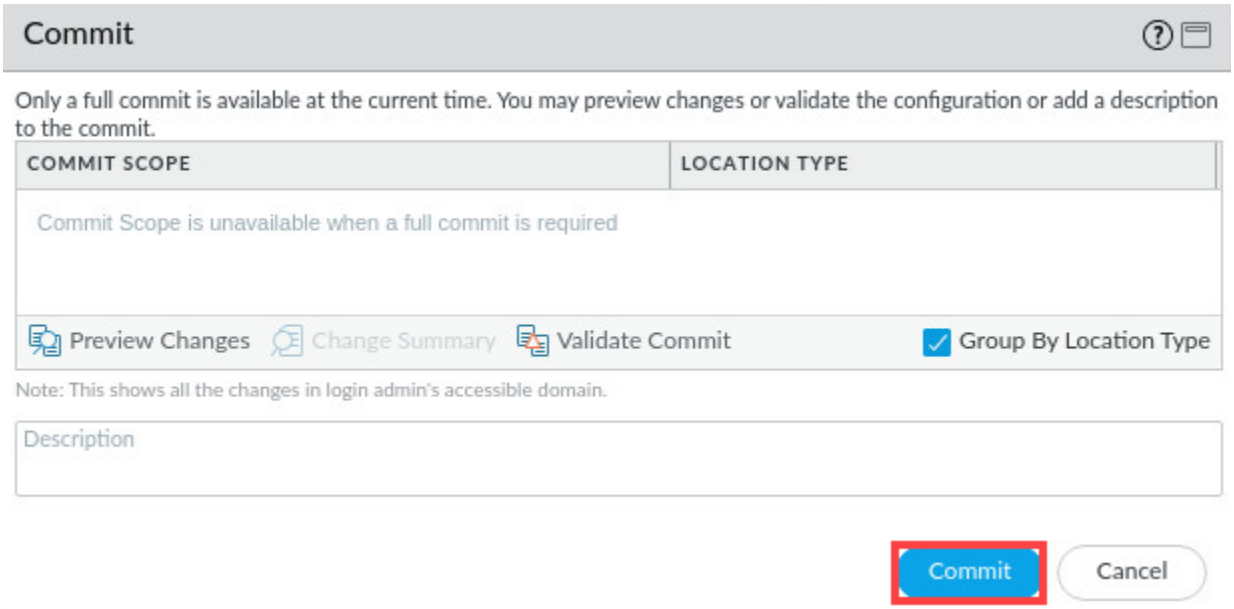


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

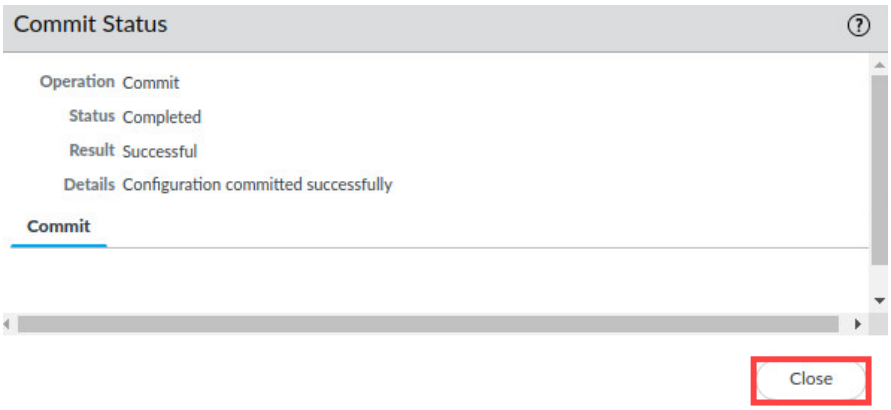



13. Click the **Commit** link located at the top-right of the web interface.


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



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




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.

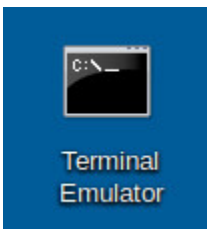
## 7.2 Test Access to Know Malicious IP Addresses

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.


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.

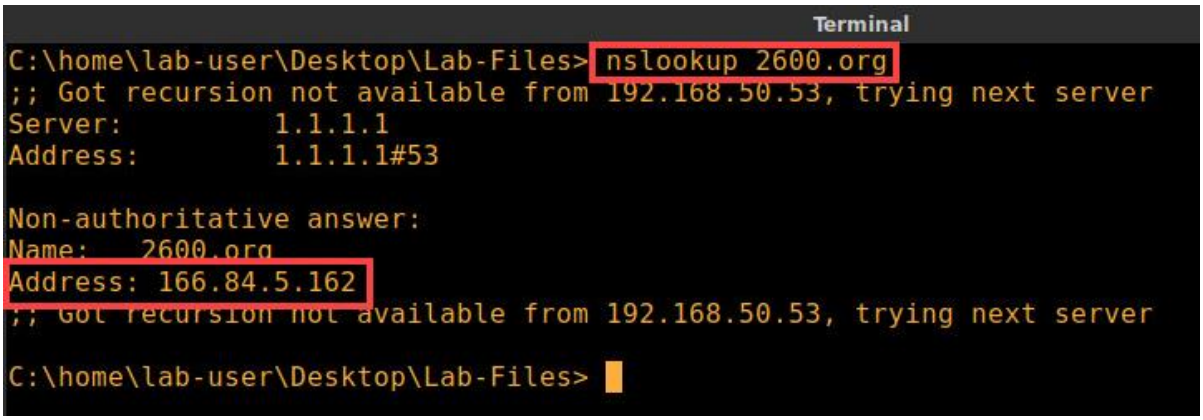

2. On the *client desktop*, open a *terminal* window by double-clicking **Terminal Emulator**.



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
```

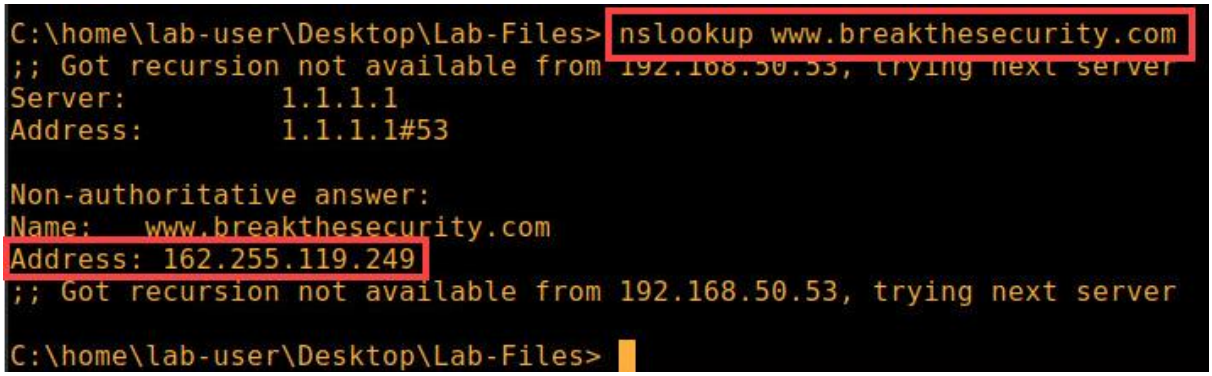



Please Note

This IP address is not malicious.

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
```




Please Note

This IP address is not malicious.

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.
^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>
```

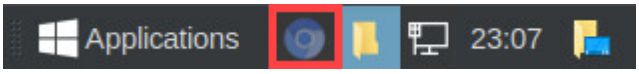
```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=1 ttl=46 time=120 ms
64 bytes from 162.255.119.249 (162.255.119.249): icmp_seq=2 ttl=46 time=124 ms
64 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

Pinging www.breakthesecurity will be successful. That will not be a problem because you will block access in the next task.

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.



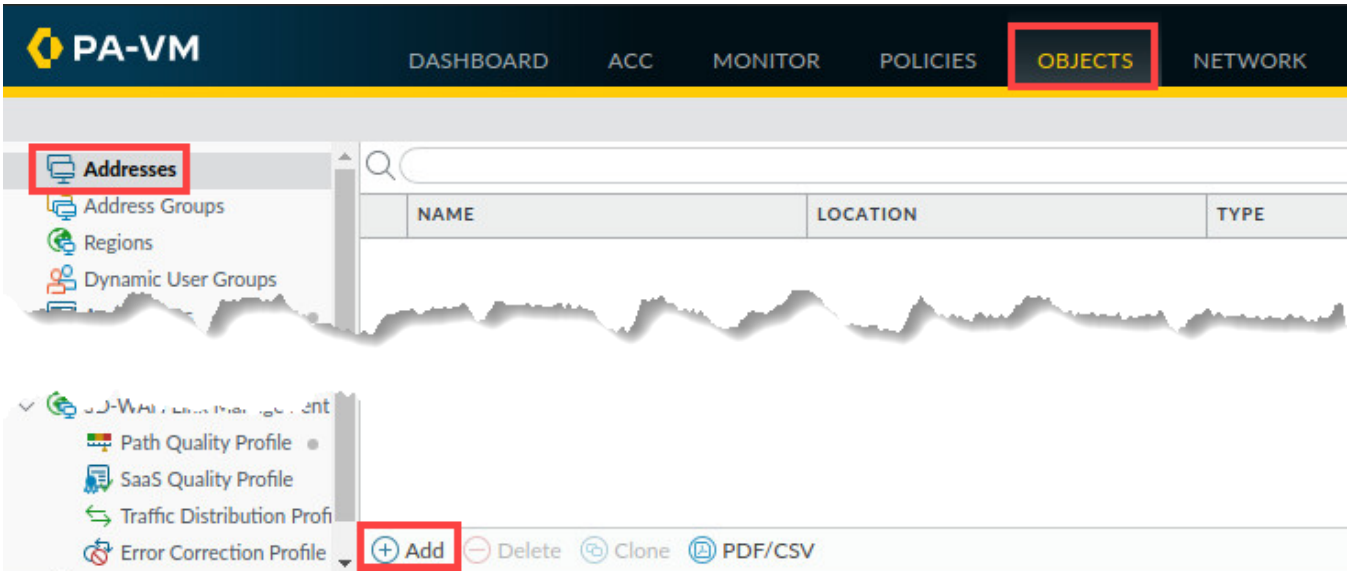
## 7.3 Block Access to Malicious IP Addresses Using Address Objects

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>` |

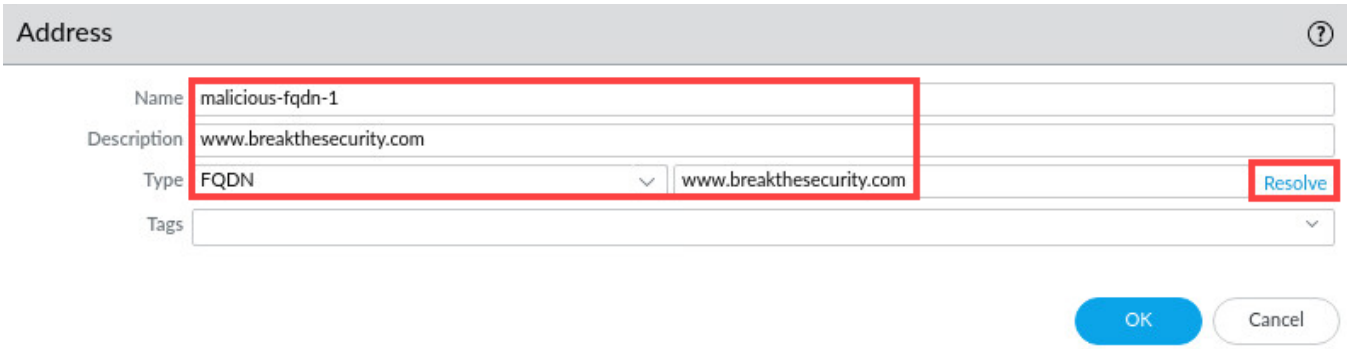

Please Note

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

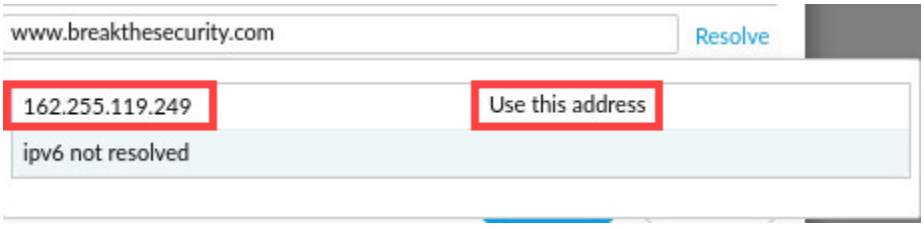
3. In the *Addresses* window, click **Add**.

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

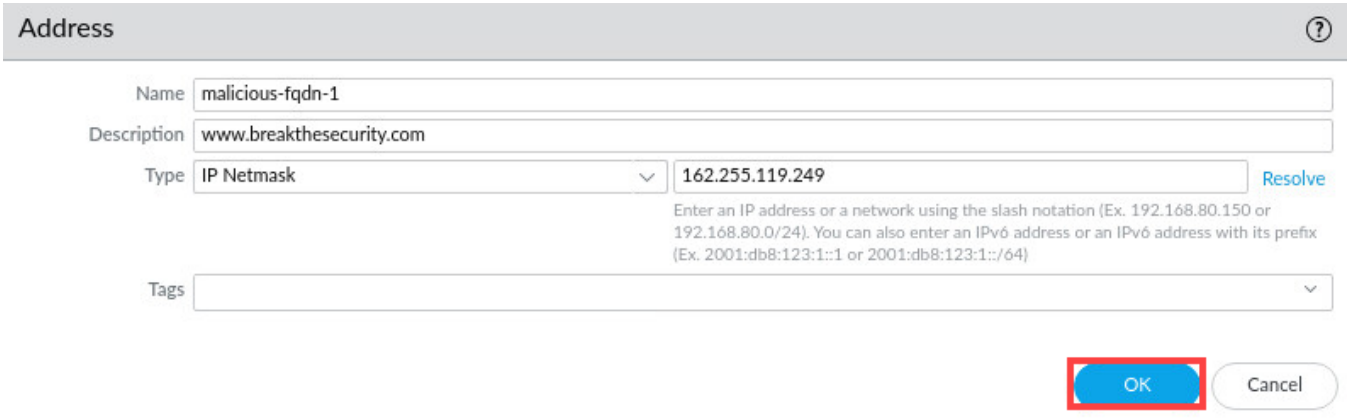
| Parameter | Value |
|---|---|
| **Name** | **malicious-fqdn-1** |
| **Description** | **www.breakthesecurity.com** |
| **Type** | **FQDN** |
| (FQDN text box) | **www.breakthesecurity.com** |




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

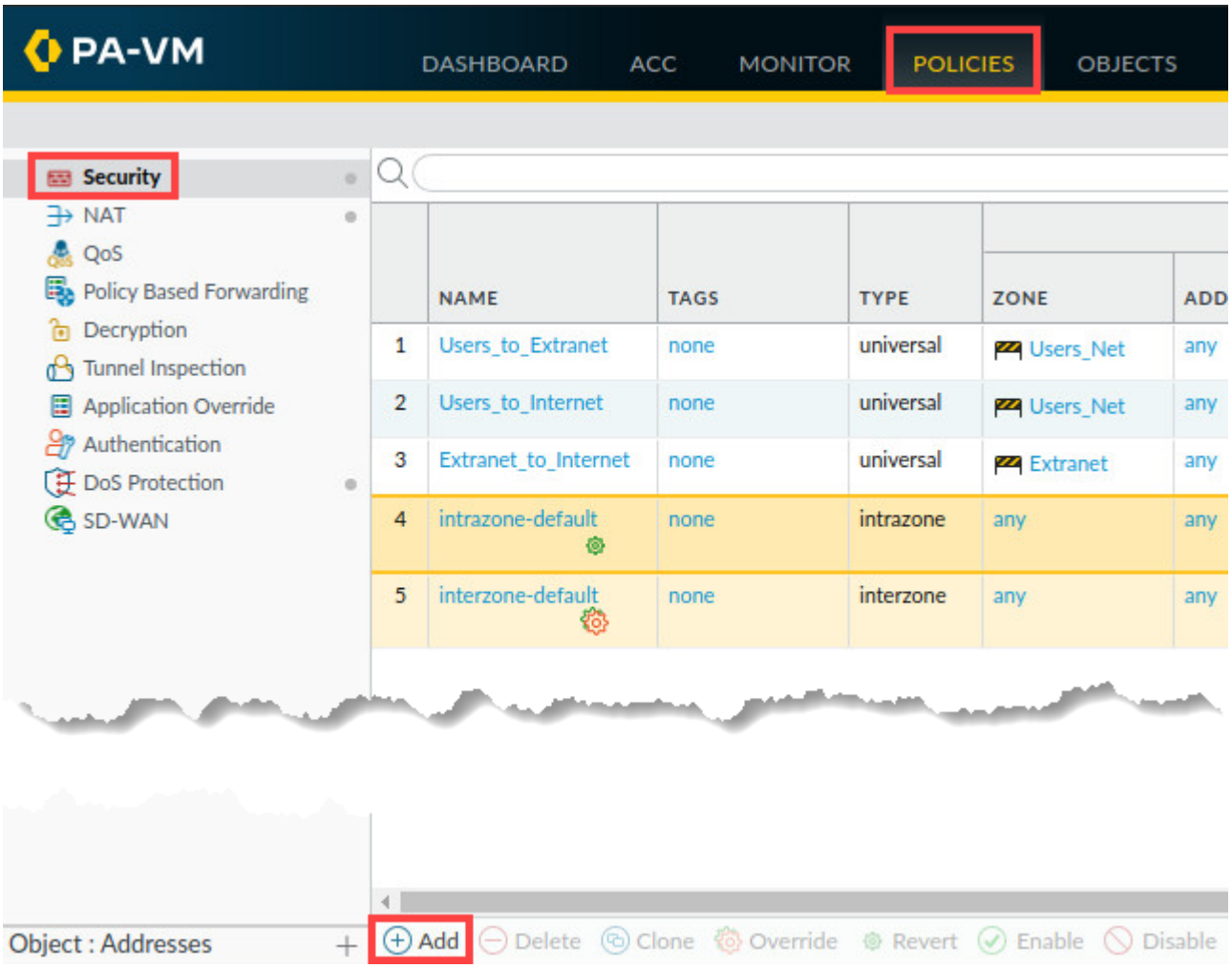



6. In the *Address* window, click **OK**.

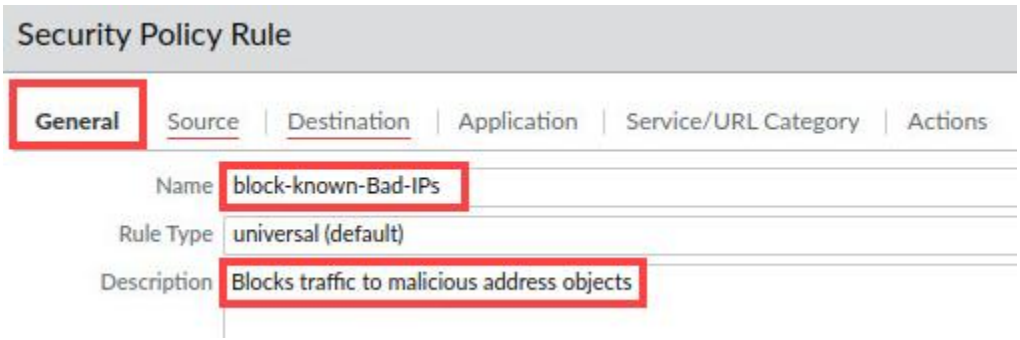



7. Confirm the *address* objects appear in the *Addresses* window.

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

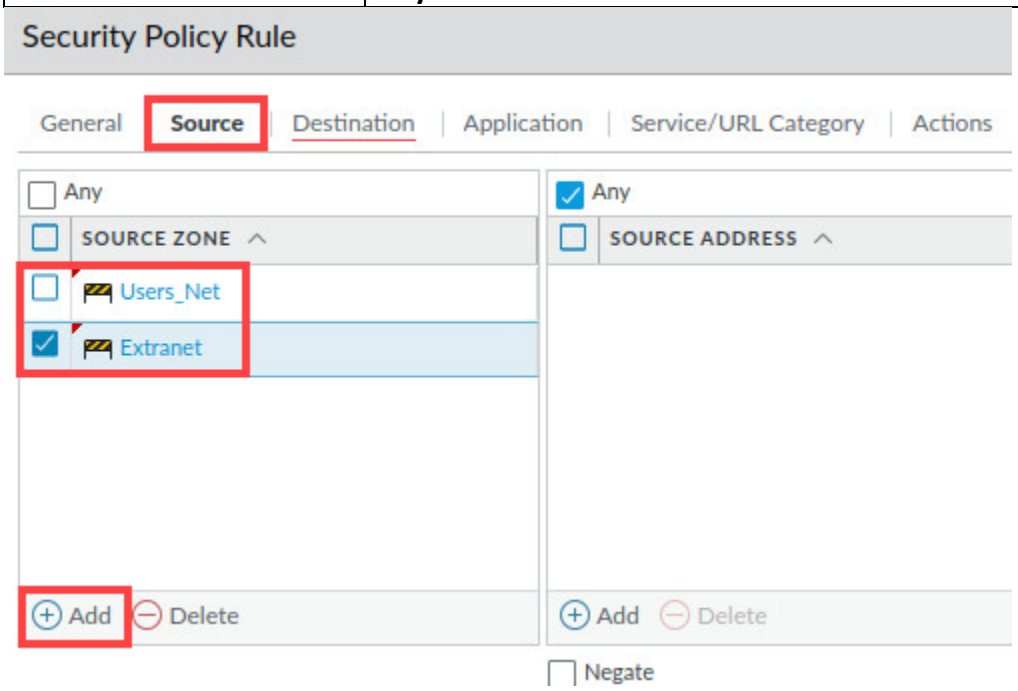



9. In the *Security Policy Rule* window, on the *General* tab, type **`Block-Known-Bad-IPs`** as the *Name*. For *Description*, enter **`Blocks traffic to malicious address objects`**.



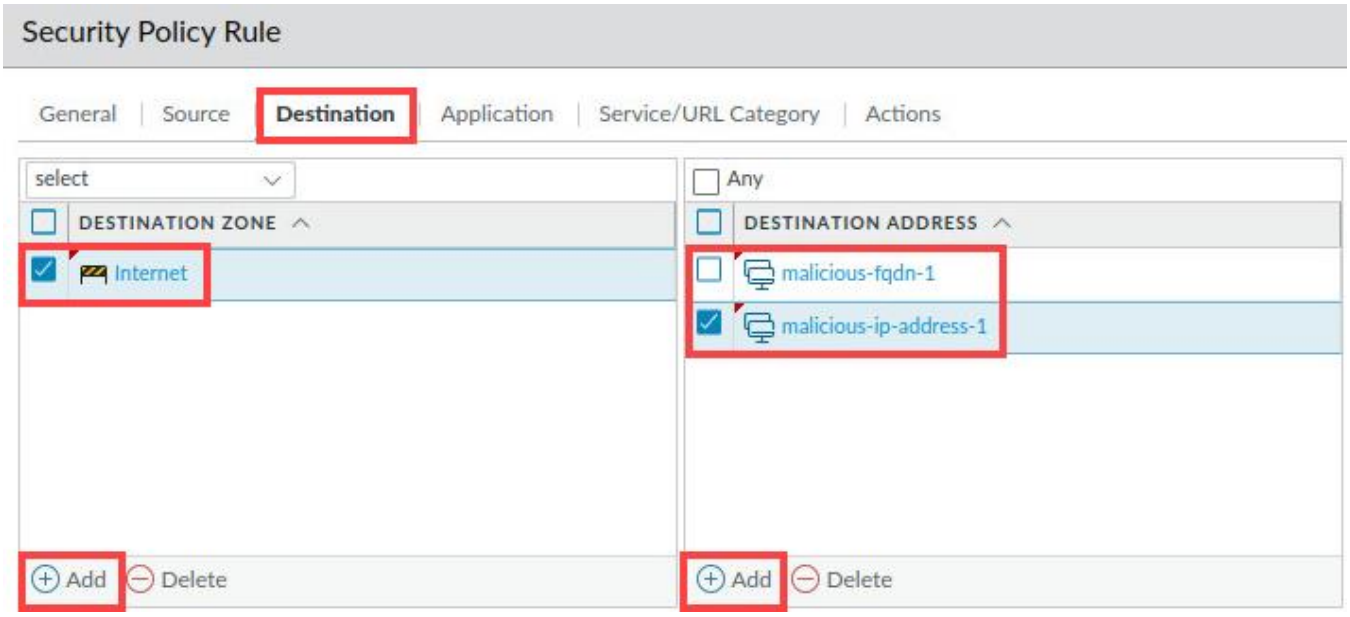
10. Click the **Source** tab and configure the following.

| Parameter | Value |
|---|---|
| **Source Zone** | Add **Users_Net** and **Extranet** |
| **Source Address** | **Any** |

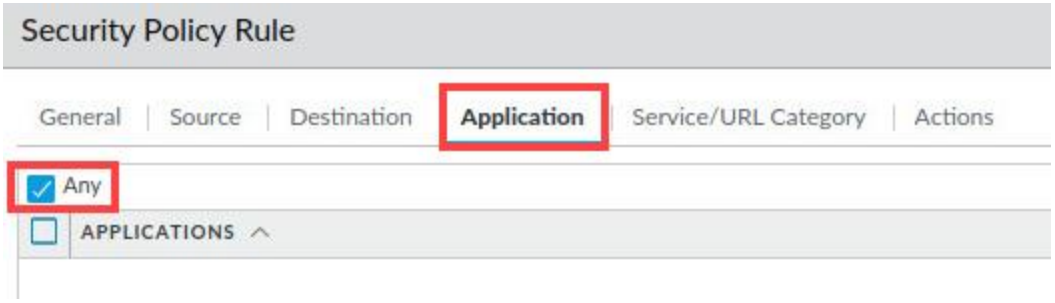



11. Click the **Destination** tab and configure the following.

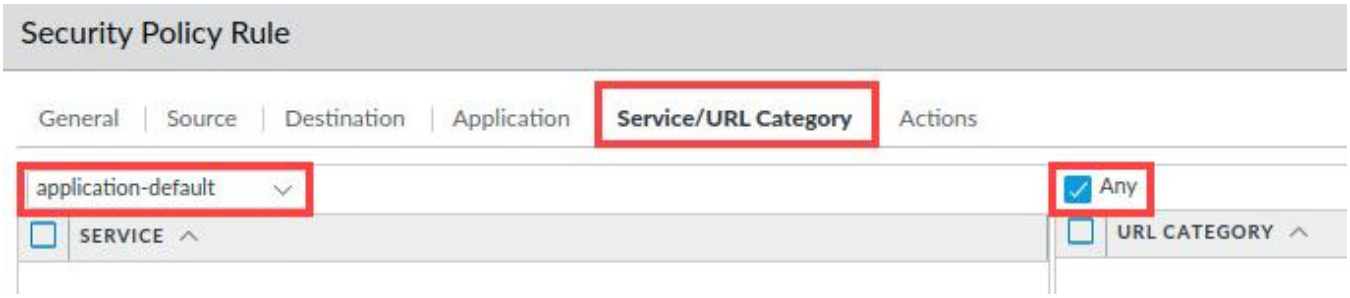
| Parameter | Value |
|---|---|
| **Destination Zone** | Add **Internet** |
| **Destination Address** | Add **malicious-fqdn-1** and **malicious-ip-address-1** |



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

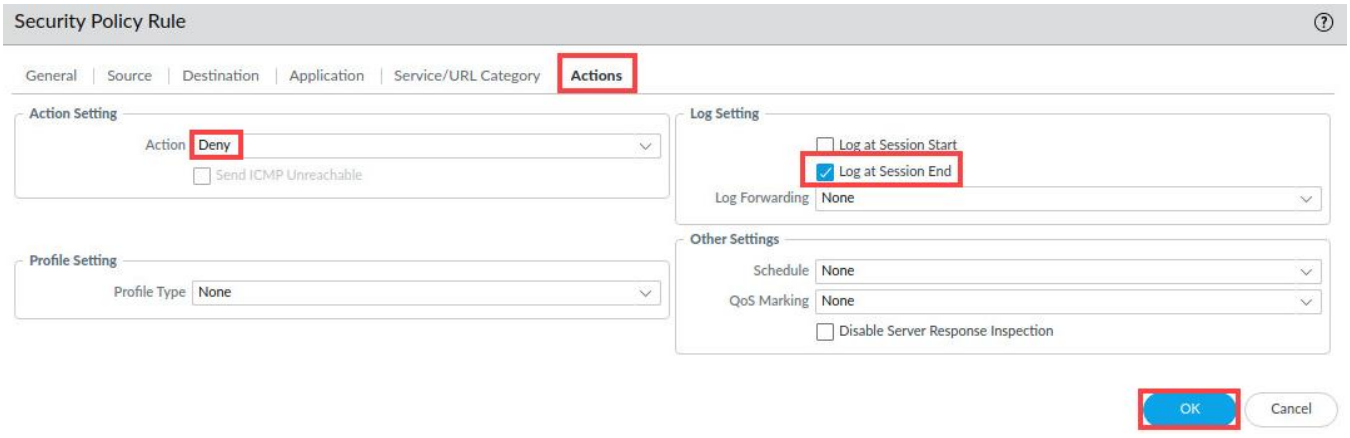



13. Click the **Service/URL Category** tab and verify that **application-default** and **Any** are selected.

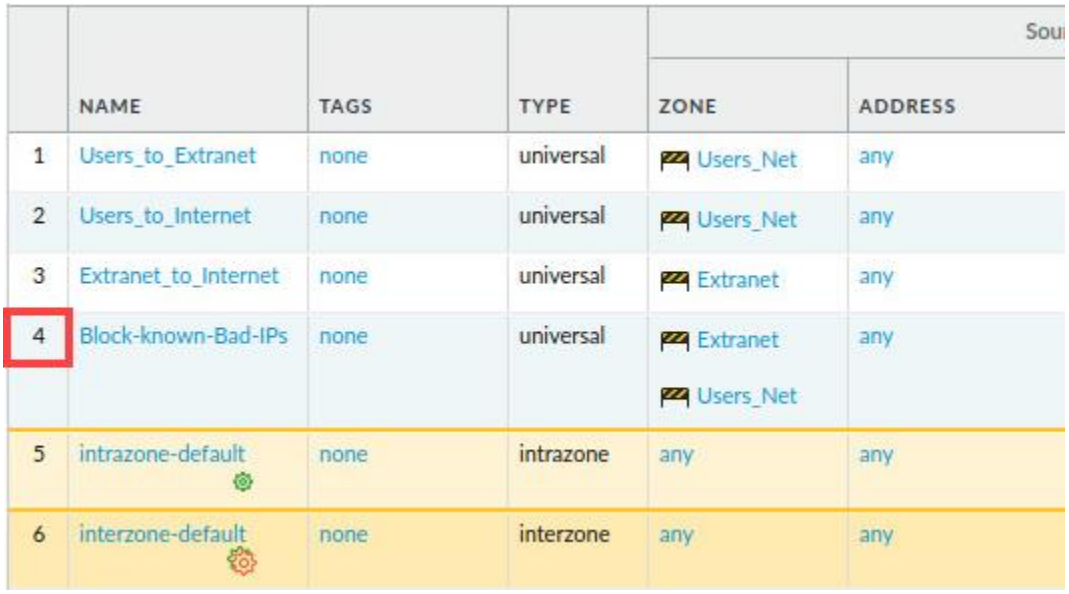



14. Click the **Actions** tab and configure the following. Click **OK**.

| Parameter | Value |
|---|---|
| **Action** | **Deny** |
| **Log Setting** | **Log at Session End** |

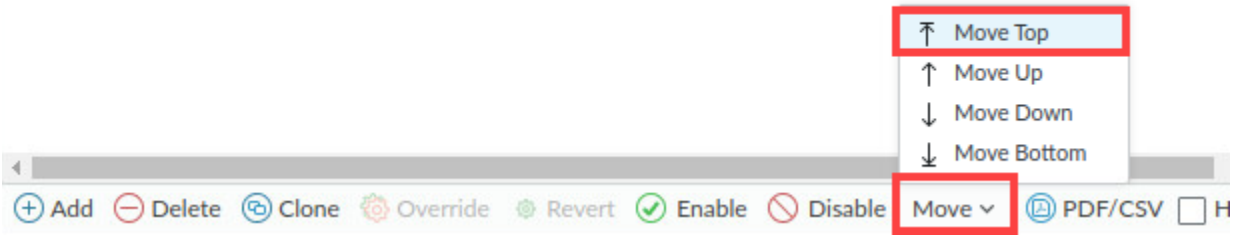


15. Select, but do not open, the **Block-Known-Bad-IPs** rule in the security policy.



| | NAME | TAGS | TYPE | Sou 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<br>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.

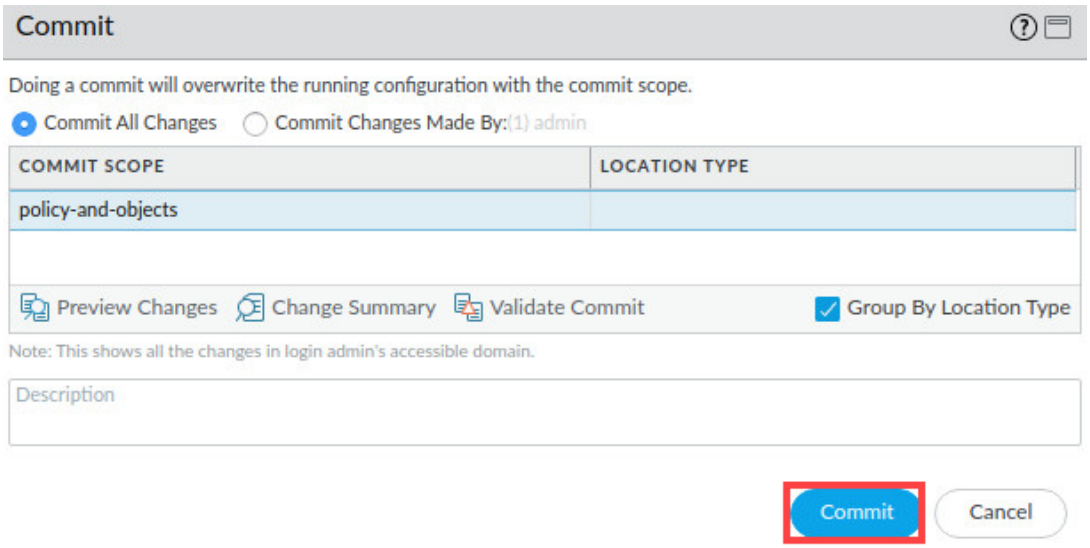



17. Verify that the **Block-Known-Bad-IPs** rule is rule number *1*.

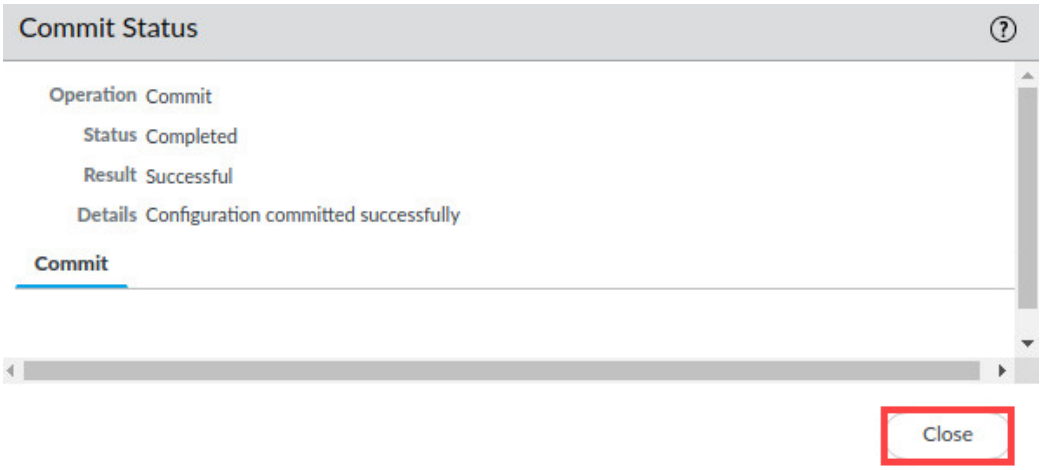
| | NAME | TAGS | TYPE | Sour ZONE | ADDRESS |
|---|---|---|---|---|---|
| 1 | Block-known-Bad-IPs | none | universal | Extranet<br>Users_Net | any |
| 2 | Users_to_Extranet | none | universal | Users_Net | any |
| 3 | Users_to_Internet | none | universal | Users_Net | any |
| 4 | Extranet_to_Internet | 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**.

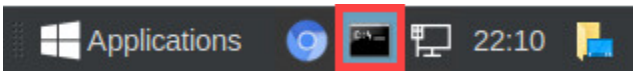



20. Wait until the C*ommit* process is complete. Click **Close**.




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>
```

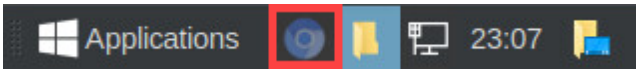
```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
^C
--- www.breakthesecurity.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

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

Please Note

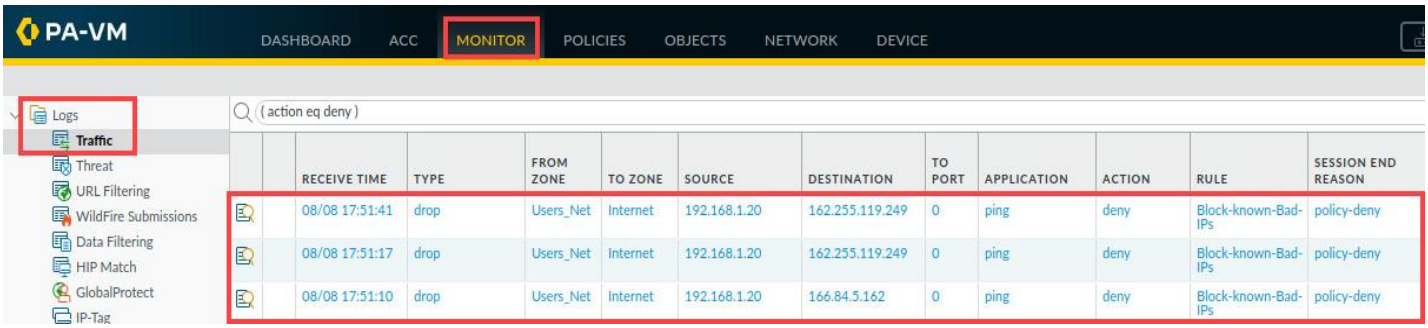
Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the Address objects in the Security policy.

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.




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.

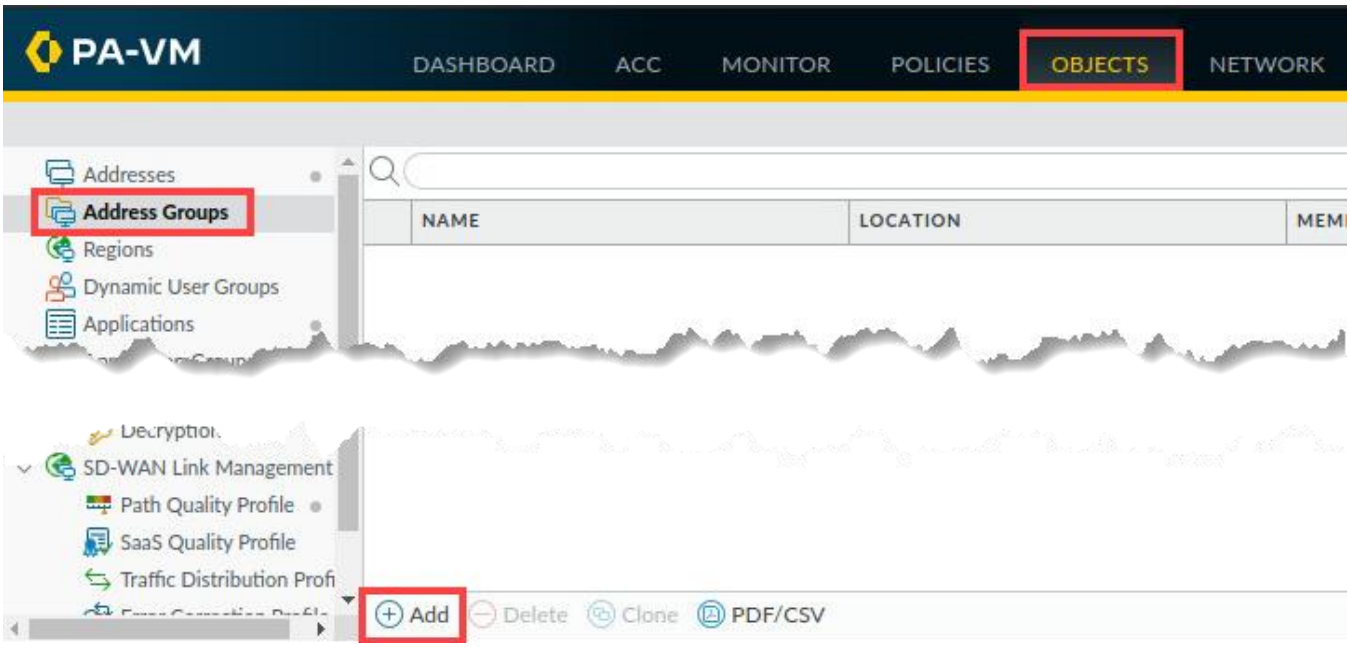
## 7.4 Block Access to Malicious IP Addresses Using Address Groups

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.

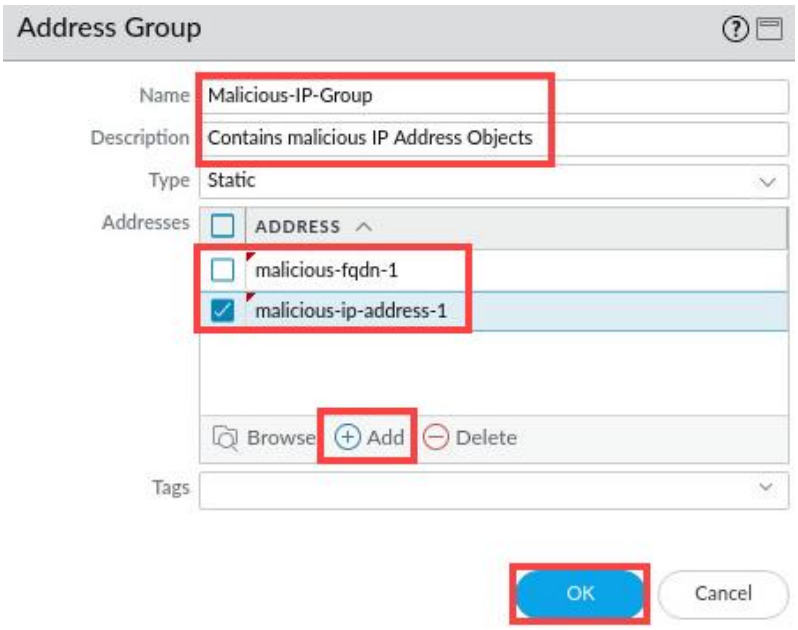
Lastly, you will test access to the IP addresses contained in the Address objects.

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

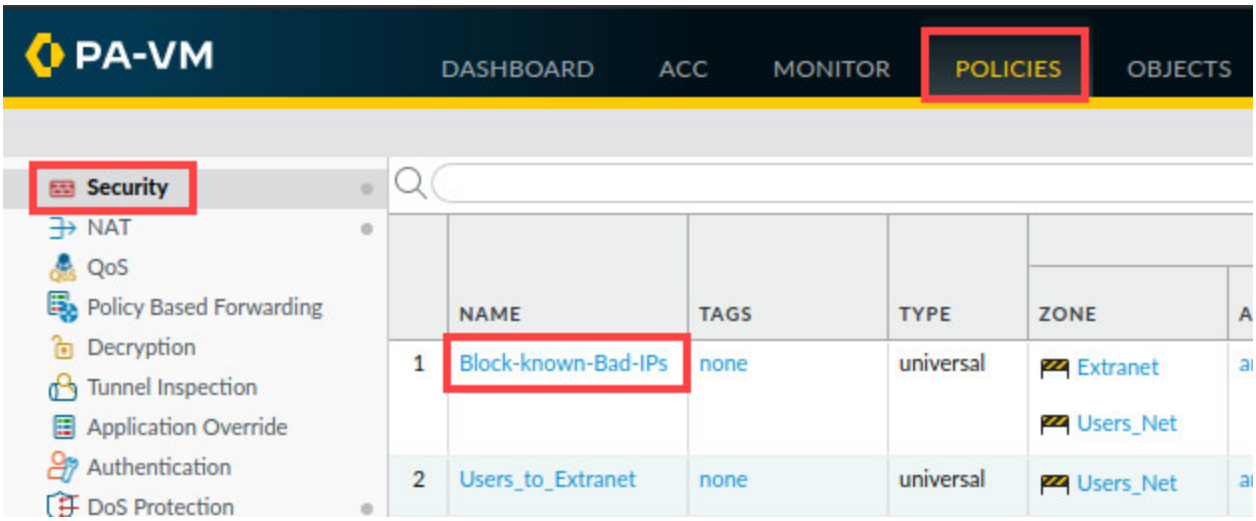



2. In the *Address Group* window, configure the following. Click **OK**.

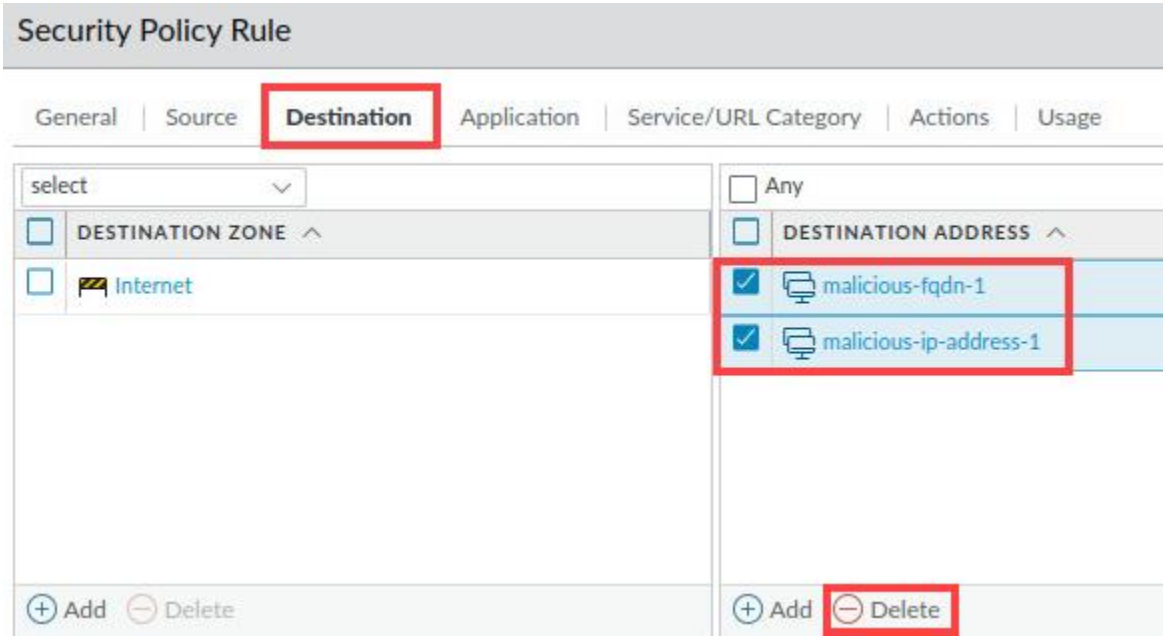
| Parameter | Value |
|---|---|
| **Name** | **`Malicious-IP-Group`** |
| **Description** | **`Contains malicious IP address objects`** |
| **Type** | **Static** |
| **Addresses** | Add **malicious-fqdn-1** and **malicious-ip-address-1** |



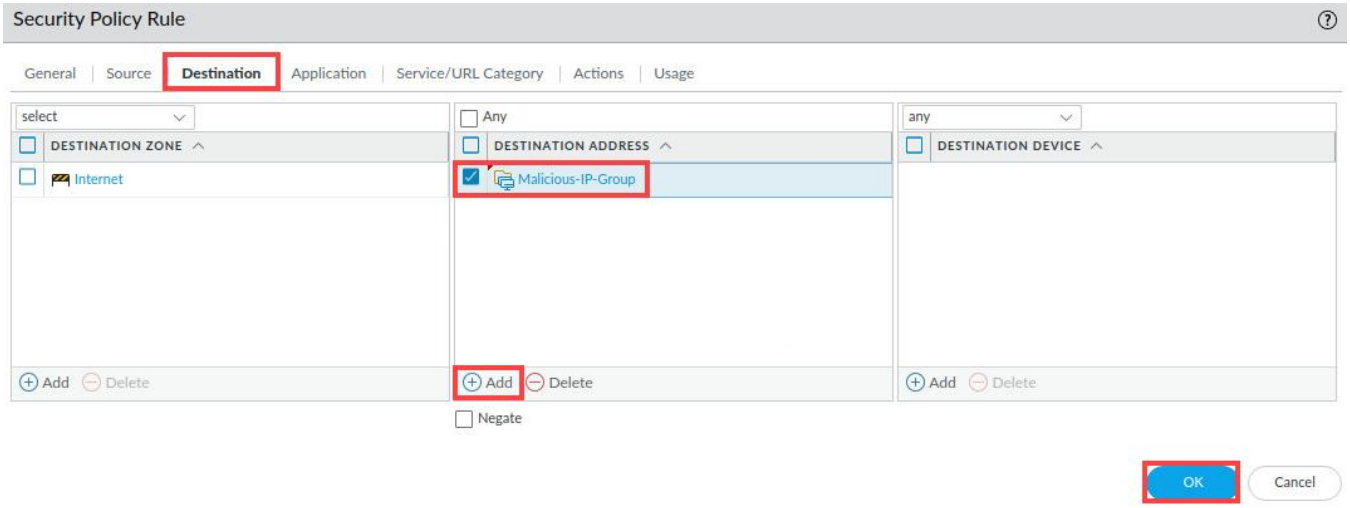
3. Select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.




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

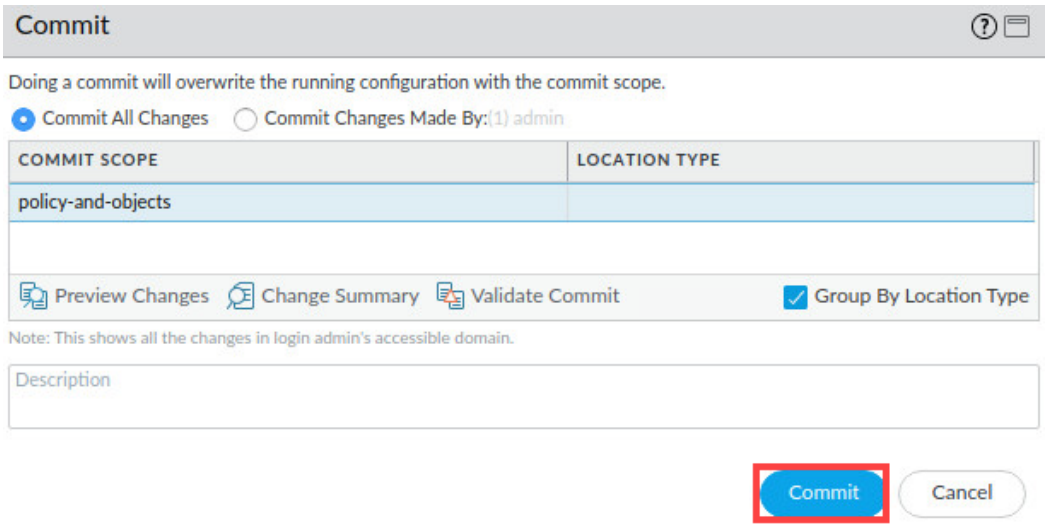


5. In the *Destination Address* window, click **Add**. Select **Malicious-IP-Group**. Click **OK**.

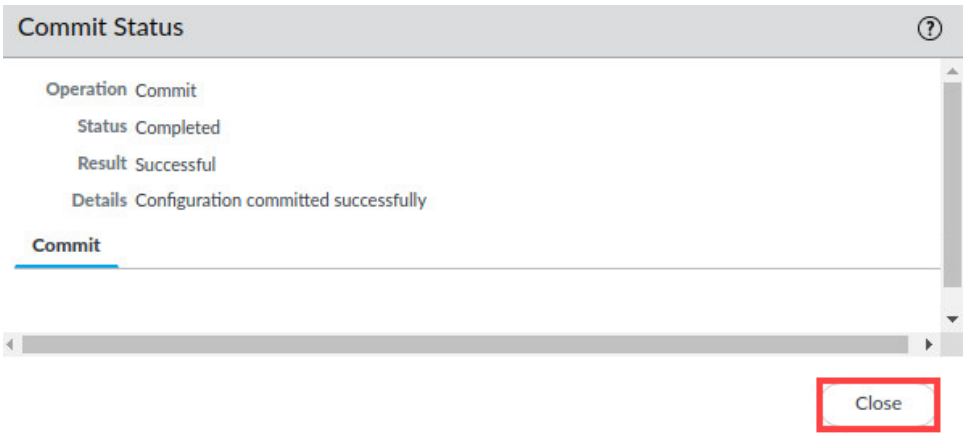



6. Click the **Commit** button at the upper-right of the web interface.


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

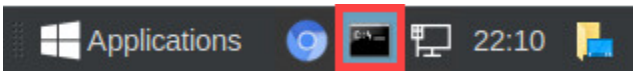


8. Wait until the *Commit* process is complete. Click **Close**.



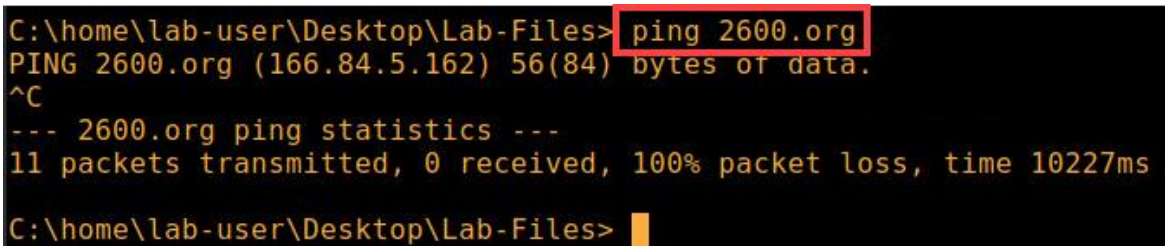

9. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.


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>
```




Please Note

Pinging 2600.org will fail.

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

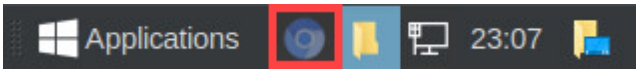
```
C:\home\lab-user\Desktop\Lab-Files> ping www.breakthesecurity.com
PING www.breakthesecurity.com (162.255.119.249) 56(84) bytes of data.
^C
--- www.breakthesecurity.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

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

**Please Note**

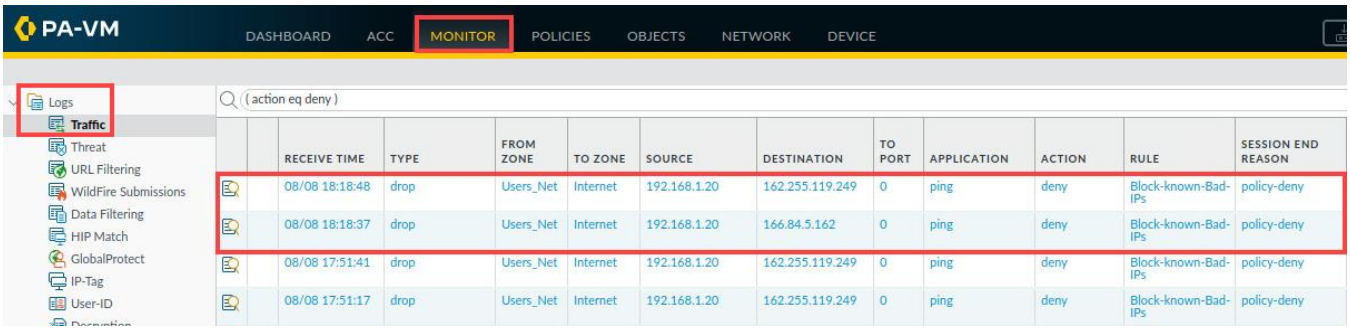
Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the address objects in the security policy.

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.




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

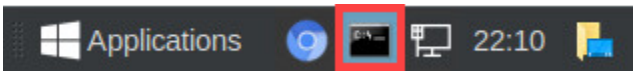
## 7.5 Block Access to Malicious IP Addresses by Geographic Region

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.

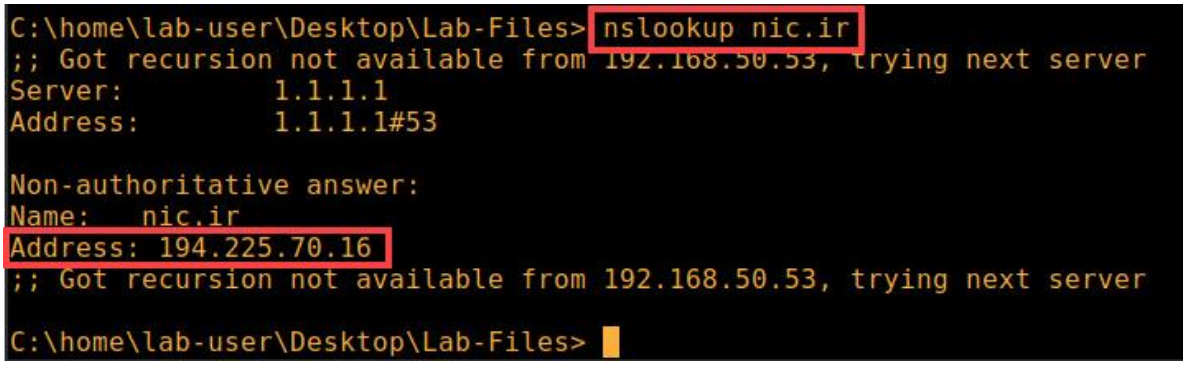
1. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.


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>
```




Please Note

The nic.ir domain is in Iran.

4. 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>
```

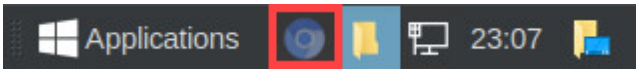
```
C:\home\lab-user\Desktop\Lab-Files> ping nic.ir
PING nic.ir (194.225.70.16) 56(84) bytes of data.
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=1 ttl=45 time=230 ms
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=2 ttl=45 time=228 ms
64 bytes from 194.225.70.16 (194.225.70.16): icmp_seq=3 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

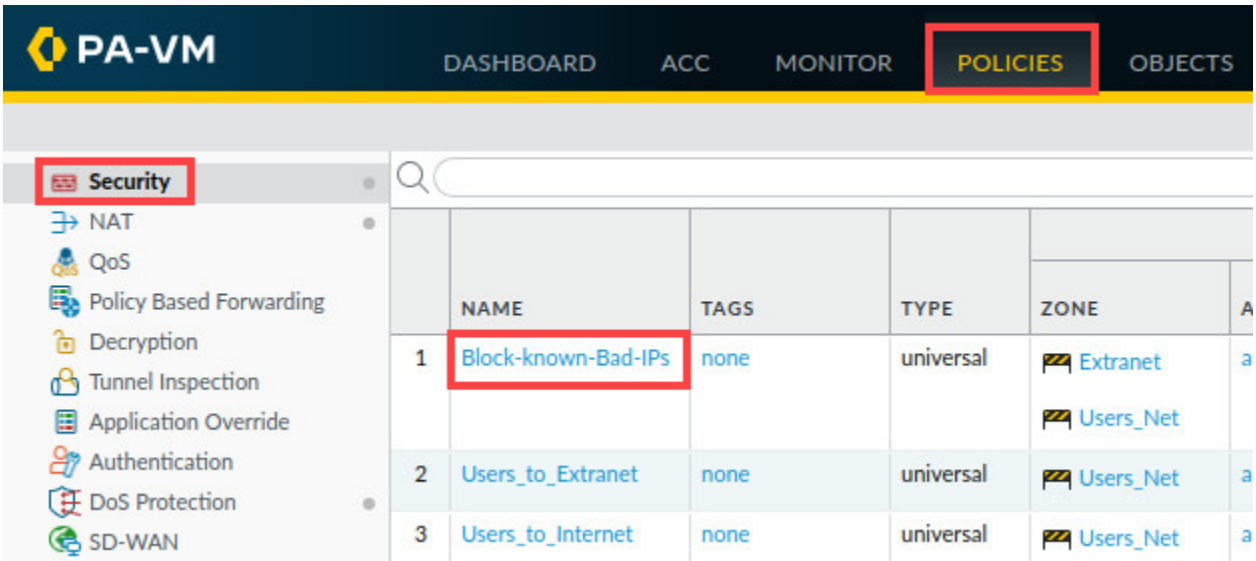
You may not get a response to the ping but that will not affect this lab.

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

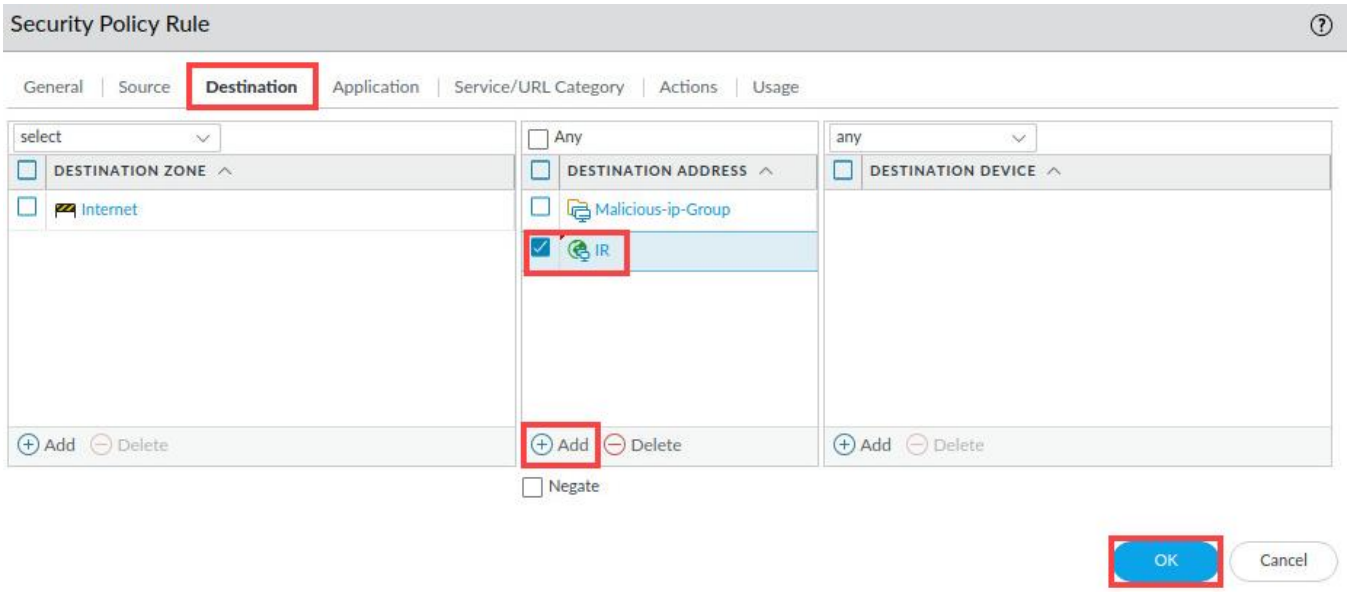

6. If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.




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



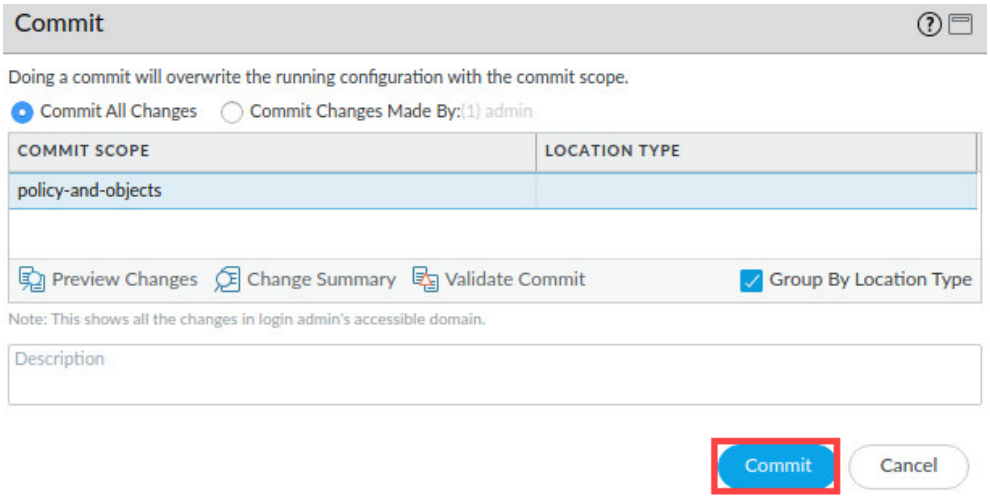
8. In the *Security Policy Rule* window, click the **Destination** tab and Add **IR** to the *Destination Address* list. Click **OK**.



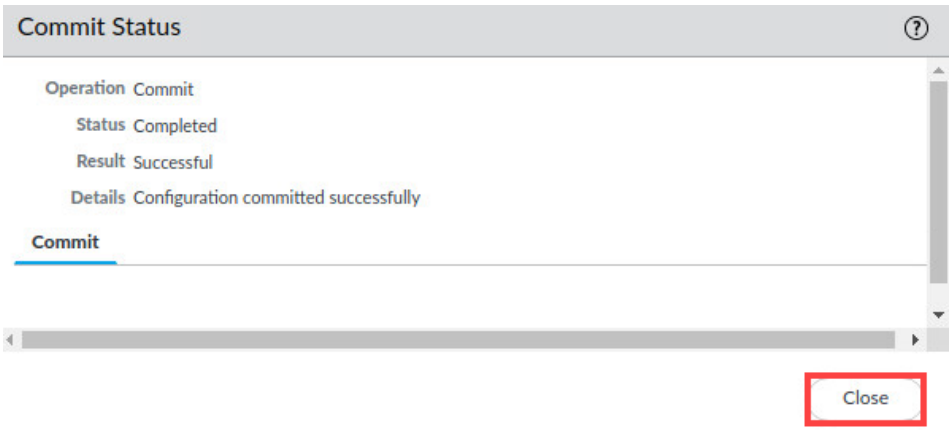

**Please Note** You will need to scroll down the list of available addresses to locate the entry for IR.

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


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

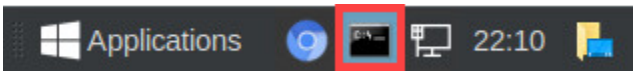


18. Wait until the *Commit* process is complete. Click **Close**.



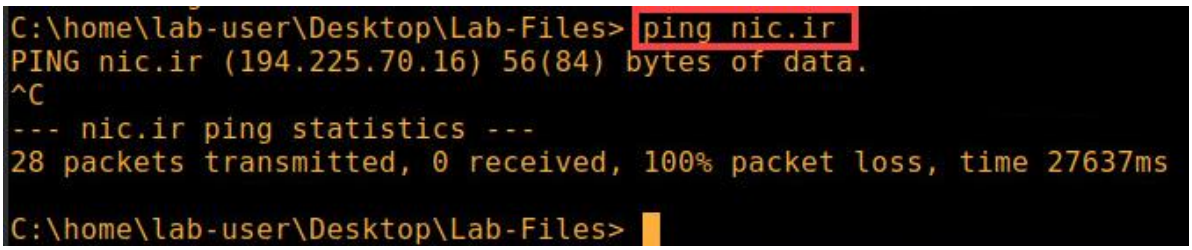

19. Minimize the *Chromium* browser by clicking the **minimize** icon and continue to the next task.


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>
```

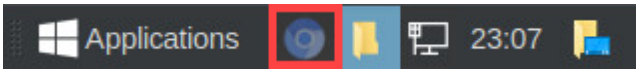



Please Note

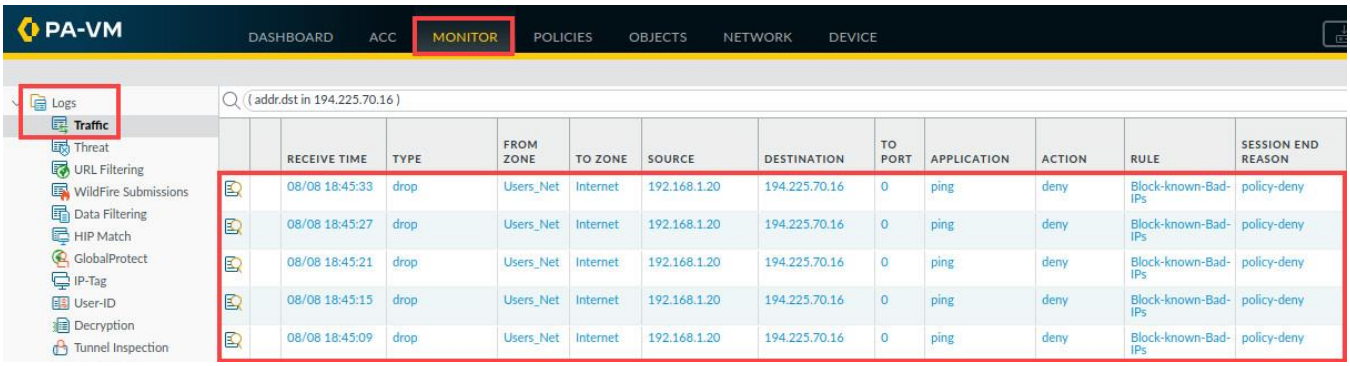
The ping will fail because you blocked the region of IR.

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.

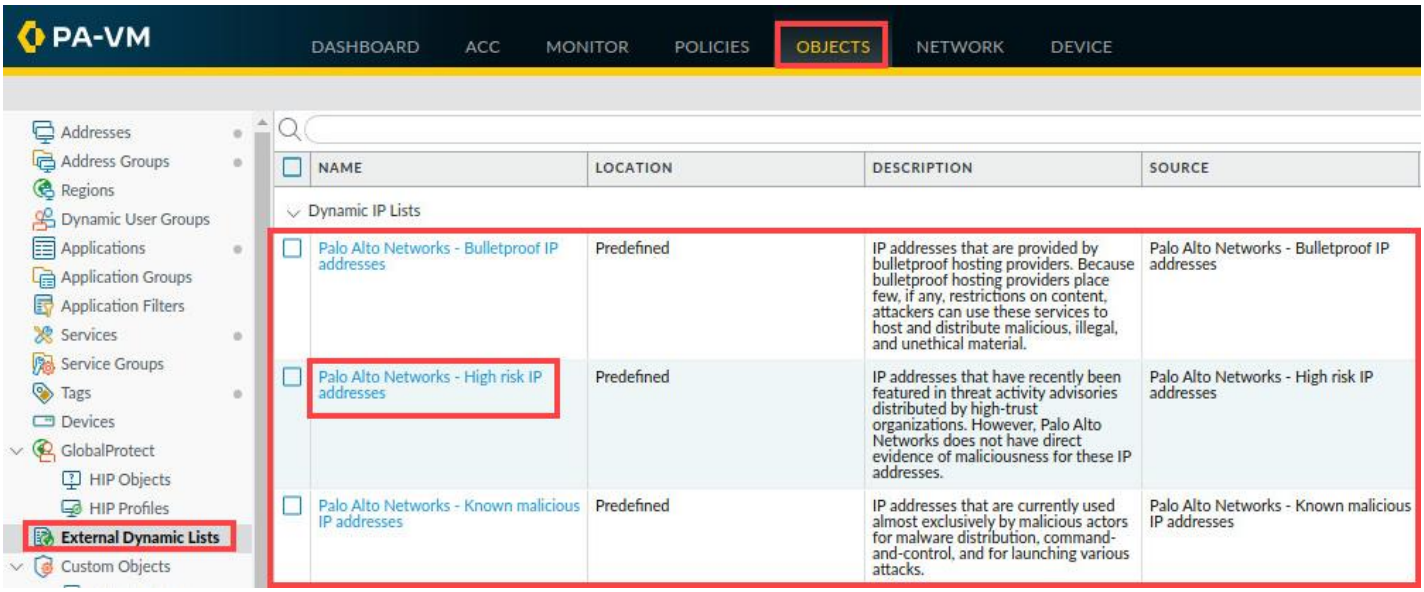



25. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

## 7.6 Block Access to Malicious IP Addresses Using EDLs

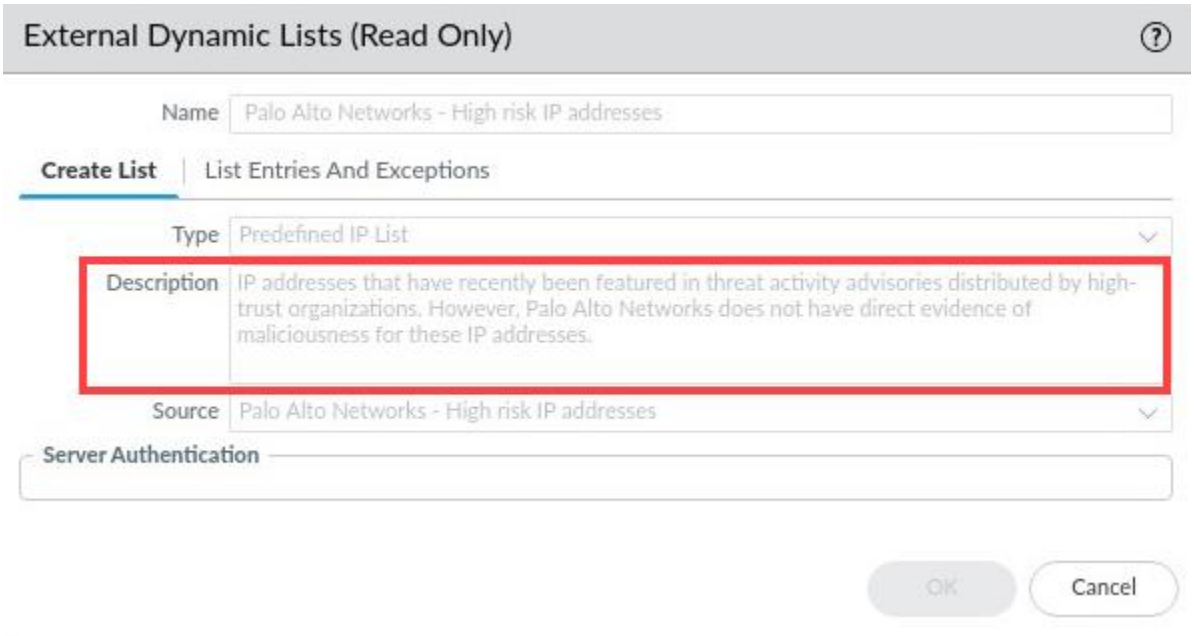
You can add a list of malicious IP addresses to a file on an external web server and configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious IP address list can be regularly updated without the need to recommit the firewall configuration, as you would 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**.



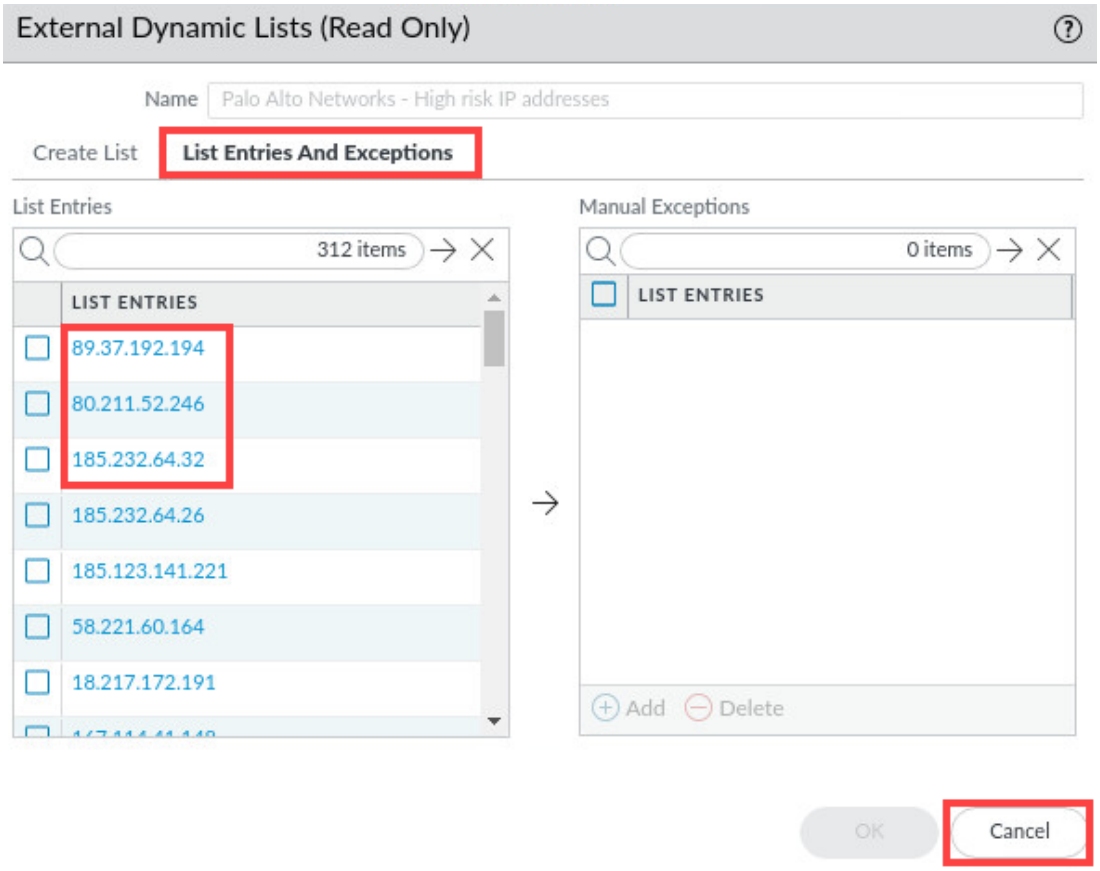

**Please Note** Palo Alto Networks maintains and provides these lists.

2. Read the description of the list.



3. 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**.

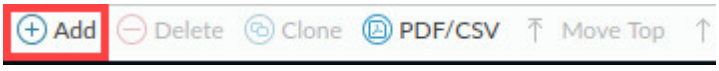



**Please Note**

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.

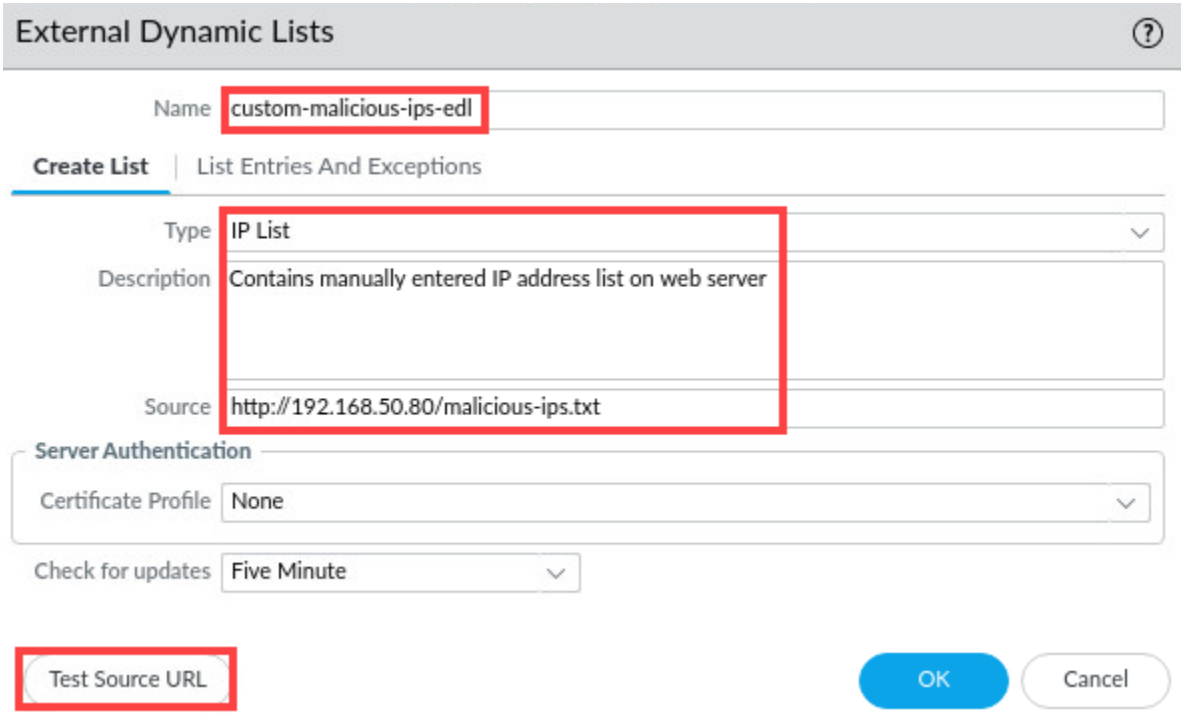
Note that you can also copy and paste these addresses into a text file on the client desktop.

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

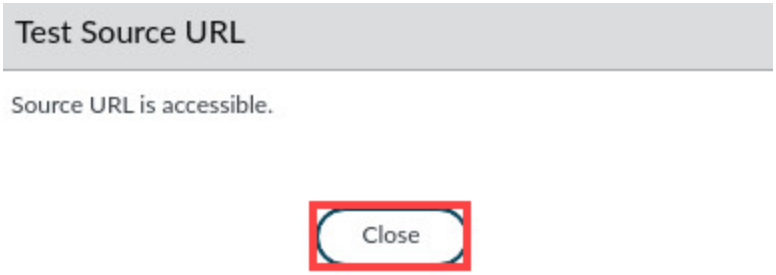


5. In the *External Dynamic Lists* window, create another **EDL** and configure the following. Click **Test Source URL**.

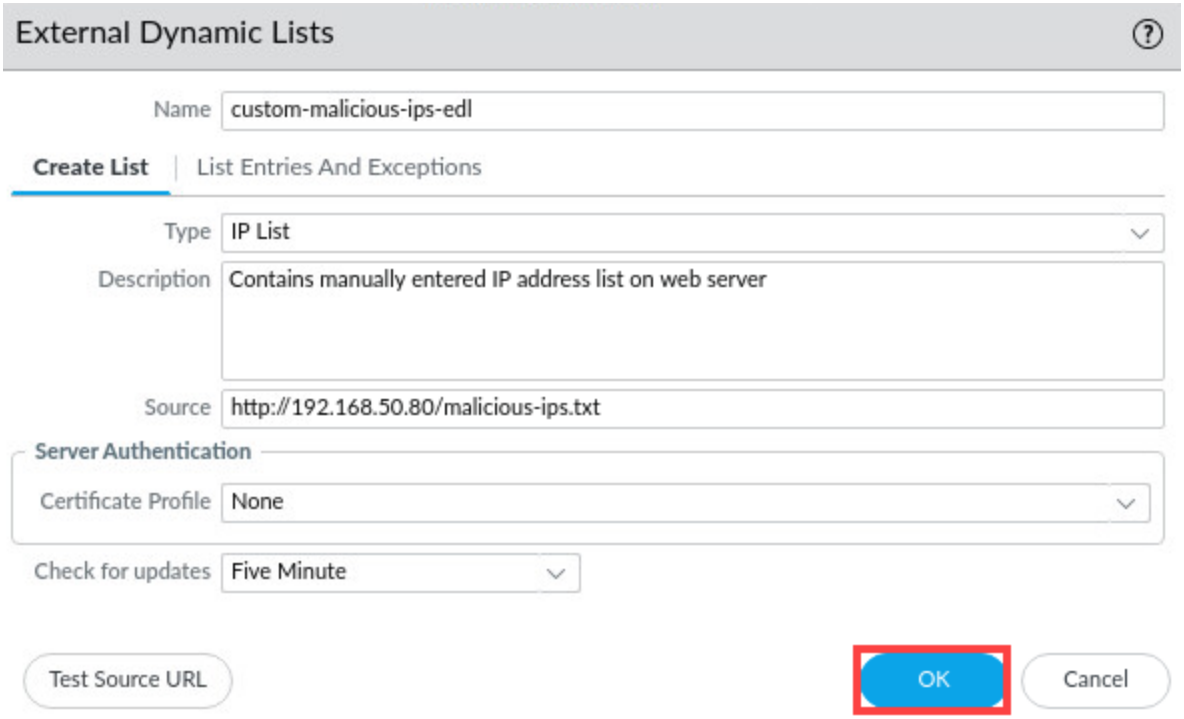
| Parameter | Value |
|---|---|
| **Name** | **`custom-malicious-ips-edl`** |
| **Type** | **IP List** |
| **Description** | **`Contains manually entered IP address list on web server.`** |
| **Source** | **`http://192.168.50.80/malicious-ips.txt`**<br>(The EDL contains only the IP address 192.168.50.11.)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



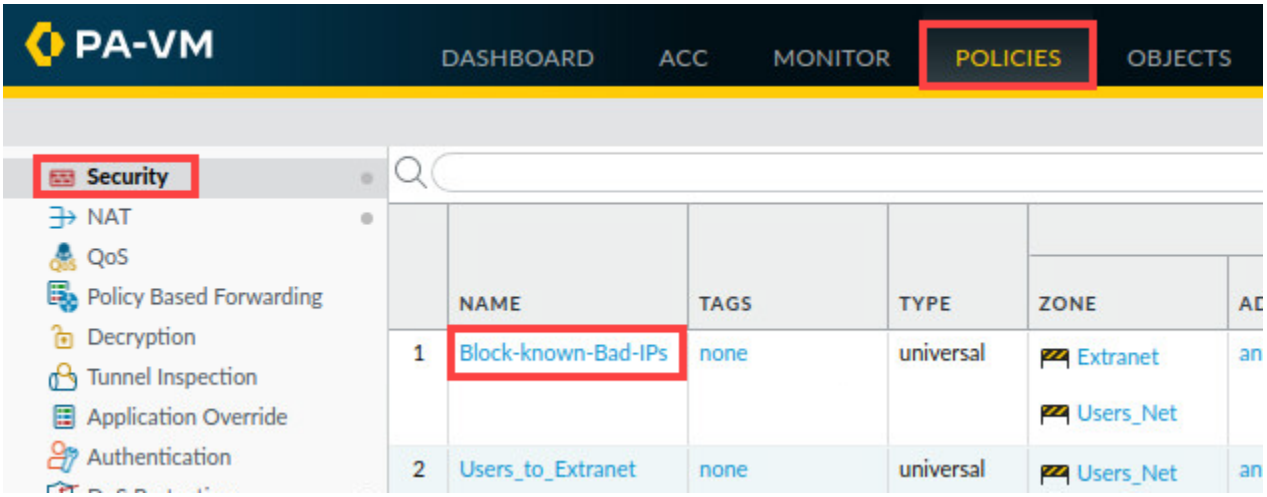

6. The firewall should present a *Test Source URL* window indicating that it can access the URL. Click **Close**.



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

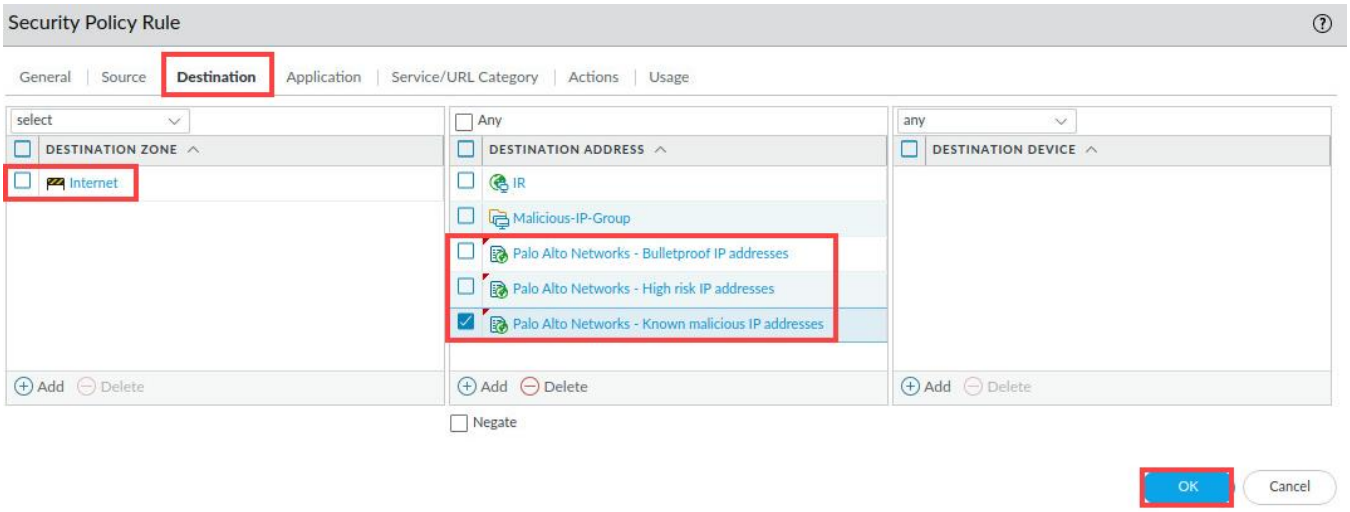



8. Update the security policy to include *External Dynamic Lists*. Navigate to **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.



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

| Parameter | Value |
|---|---|
| **Destination Zone** | **Internet** |
| **Destination Address** | Add the following to the list:<br>**Palo Alto Networks – Bulletproof IP addresses**<br>**Palo Alto Networks – High risk IP addresses**<br>**Palo Alto Networks – Known malicious IP addresses** |




Please Note

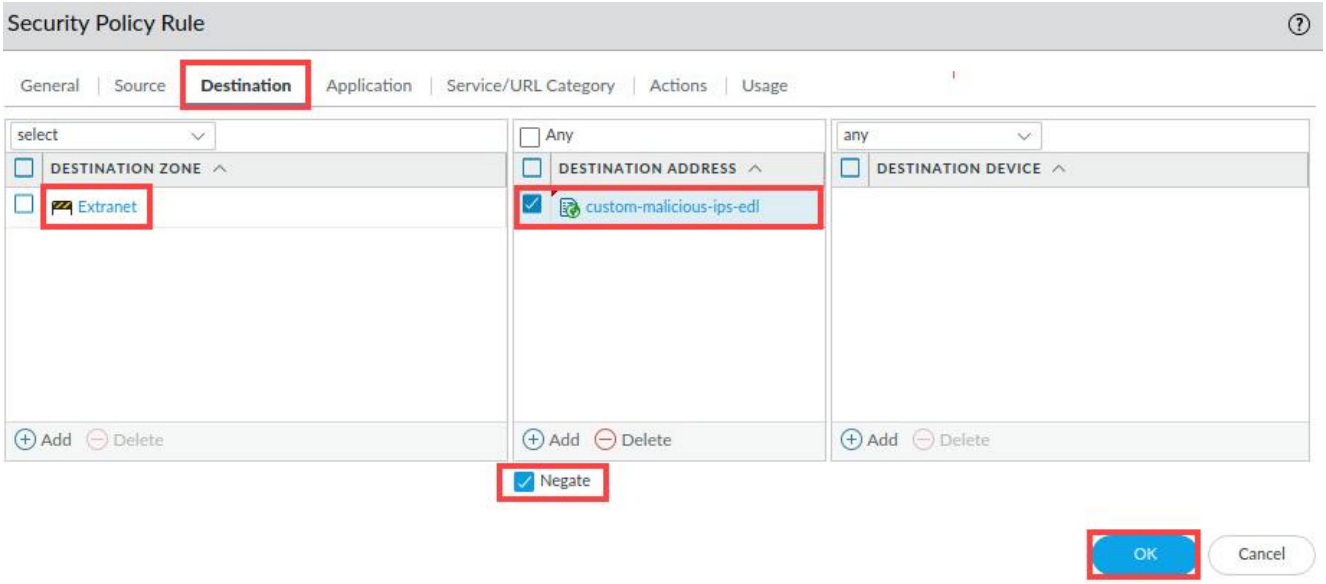
The "Block-Known-Bad-IPs" rule now is configured to block access to the three IP addresses you wrote down in lab Step 3.

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

| | NAME | TAGS | TYPE | ZONE | ADDRESS |
|---|---|---|---|---|---|
| 1 | Block-known-Bad-IPs | none | universal | Extranet<br>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** |





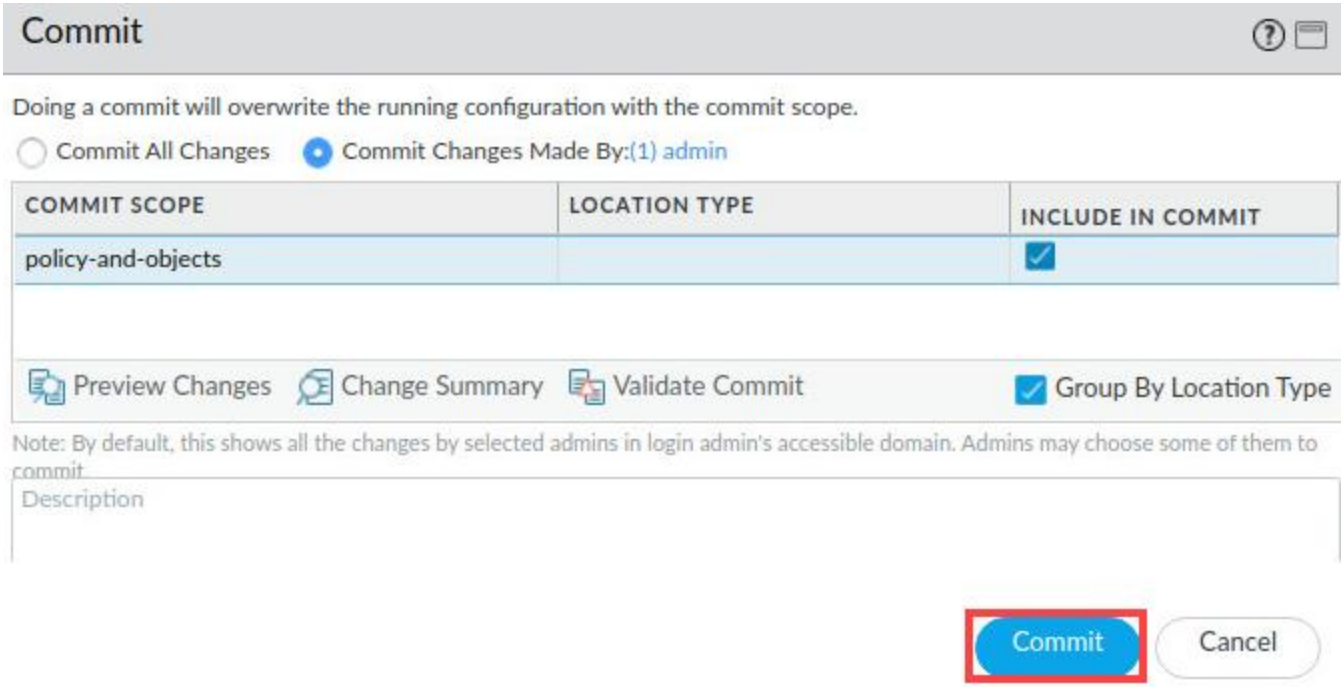
The malicious-ips-edl EDL contains the IP address of a host in the Extranet zone (192.168.50.11). When the destination address is used in conjunction with the Negate option, the rule matches and allows any address in the Extranet zone except the address listed in the EDL.

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.

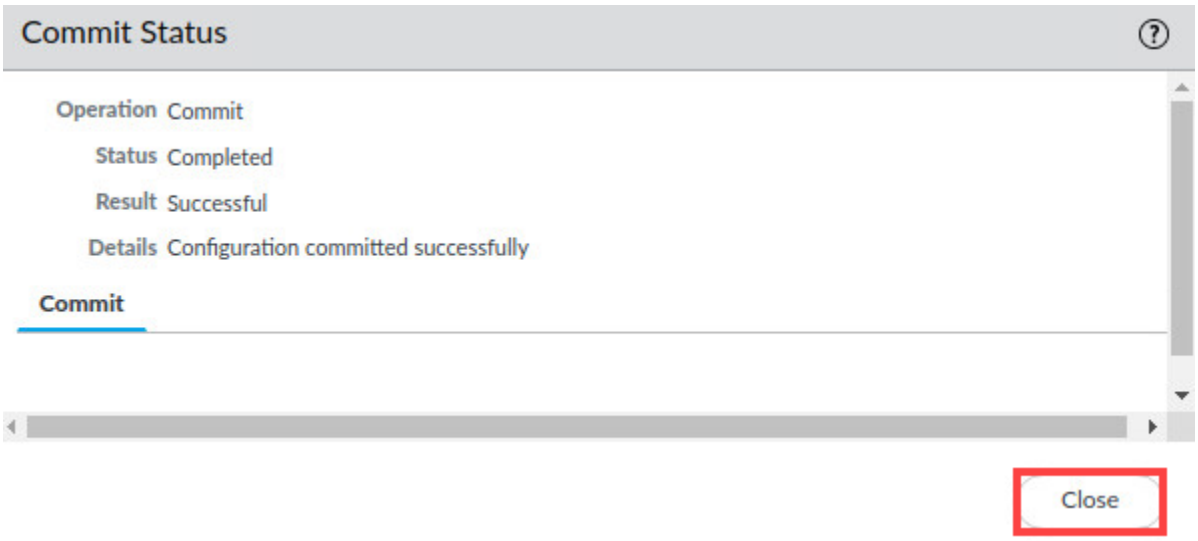
| | | | | Source | | | | Destination | |
|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 1 | Block-known-Bad-IPs | none | universal | Extranet<br>Users_Net | any | any | any | Internet | IR<br>Malicious-IP-Group<br>Palo Alto Networks - Bulletproof IP ...<br>Palo Alto Networks - High risk IP ad...<br>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.

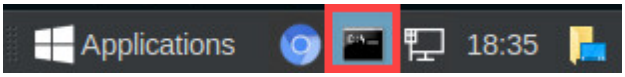
14. In the *Commit* window, click **Commit**.




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



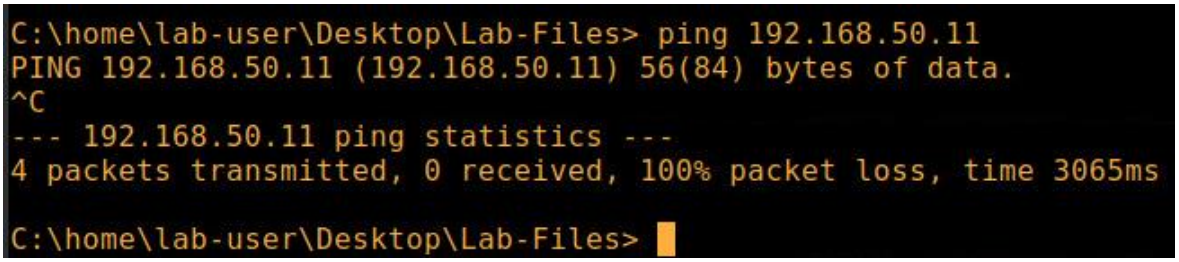

16. Return to the *terminal* window by clicking on the **Terminal** icon in the taskbar of your *client desktop*.



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>
```


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



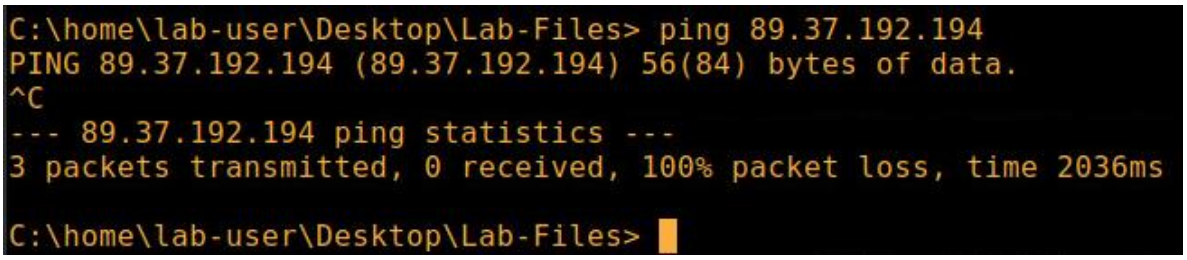

Please Note

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>
```


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

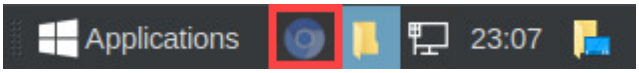



Please Note

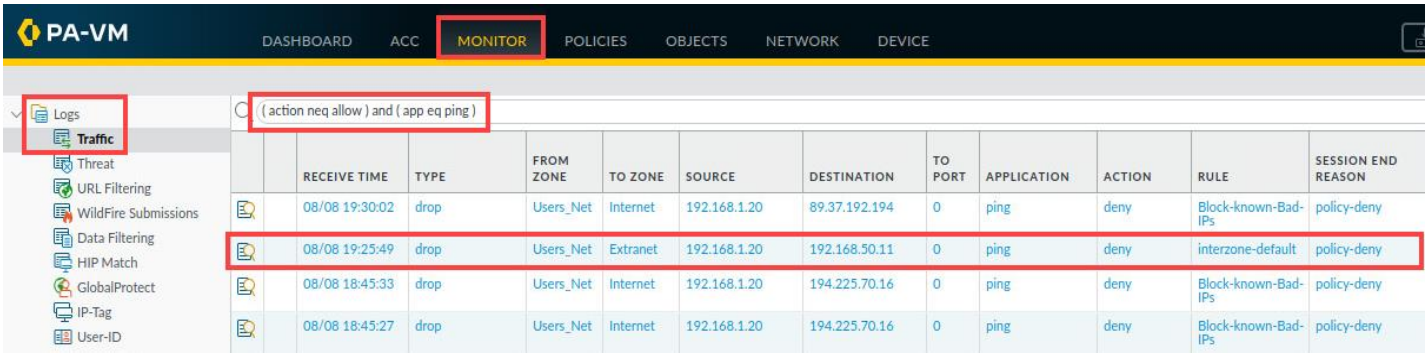
These IP addresses were in one of the EDLs predefined by Palo Alto Networks.

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.



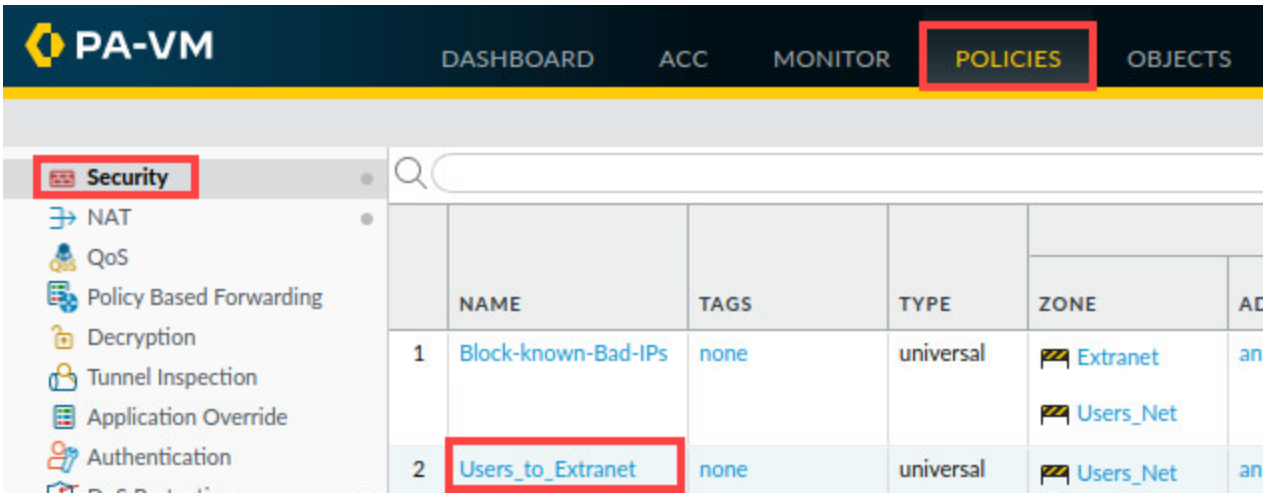

23. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to **Monitor > Logs > Traffic**. In the filter field, enter **`( action neq allow ) and ( app eq ping )`.** Click the **Apply Filter** button in the upper-right corner of the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




**Please Note**

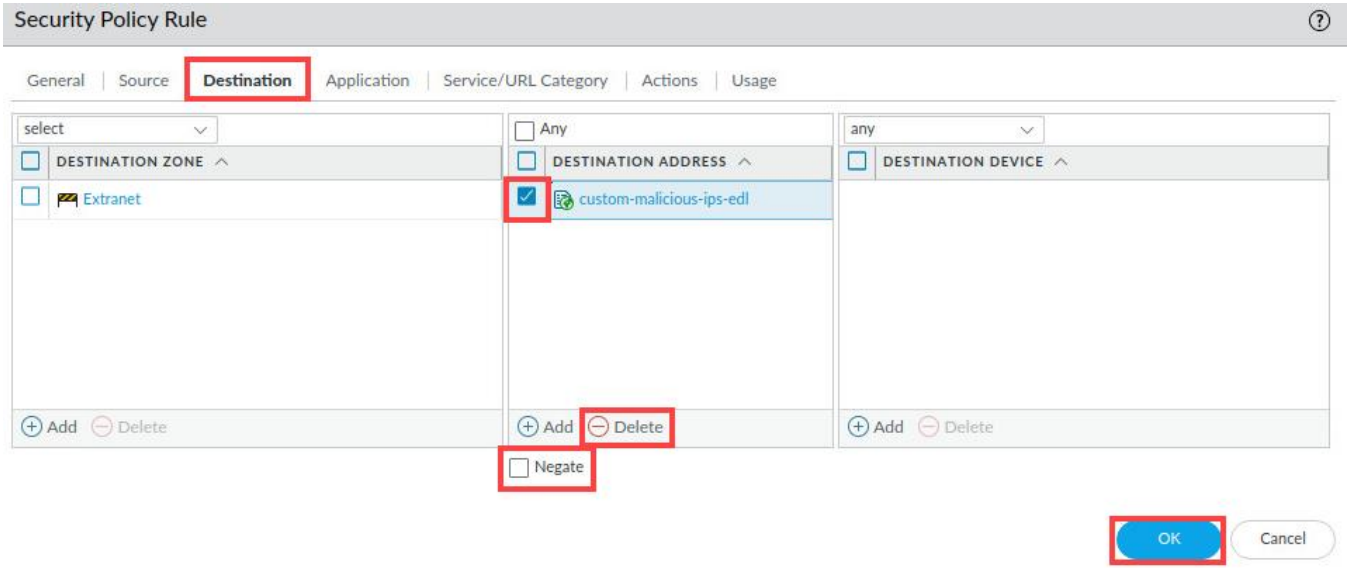
Note that ping to 192.168.50.11 hit the **interzone-default** rule and not the **Users_to_Extranet** rule. The Users_to_Extranet rule is set to allow traffic (with the exception of the IP address 192.168.50.11). Traffic to the 192.168.50.11 address does not match the rule because of the negate setting 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.



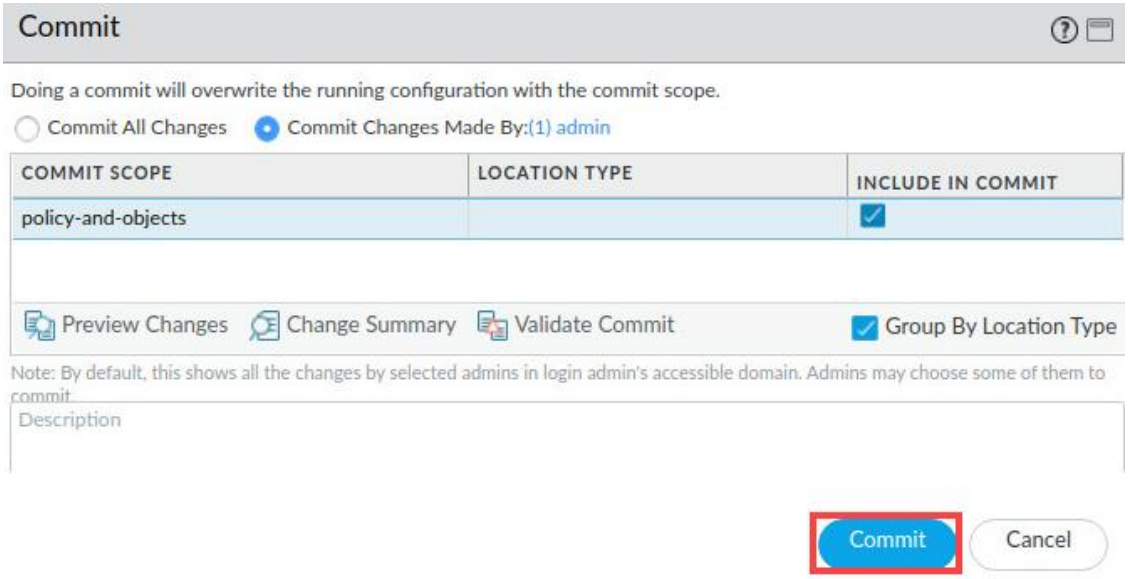

25. In the *Security Policy Rule* window, click the **Destination** tab and configure the following. Click **OK**.

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

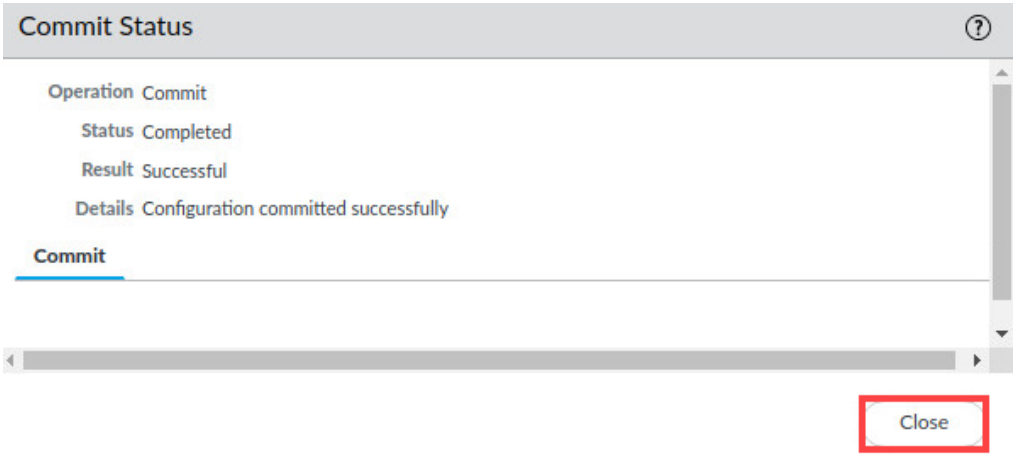



26. Click the **Commit** button at the upper-right of the web interface.

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




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



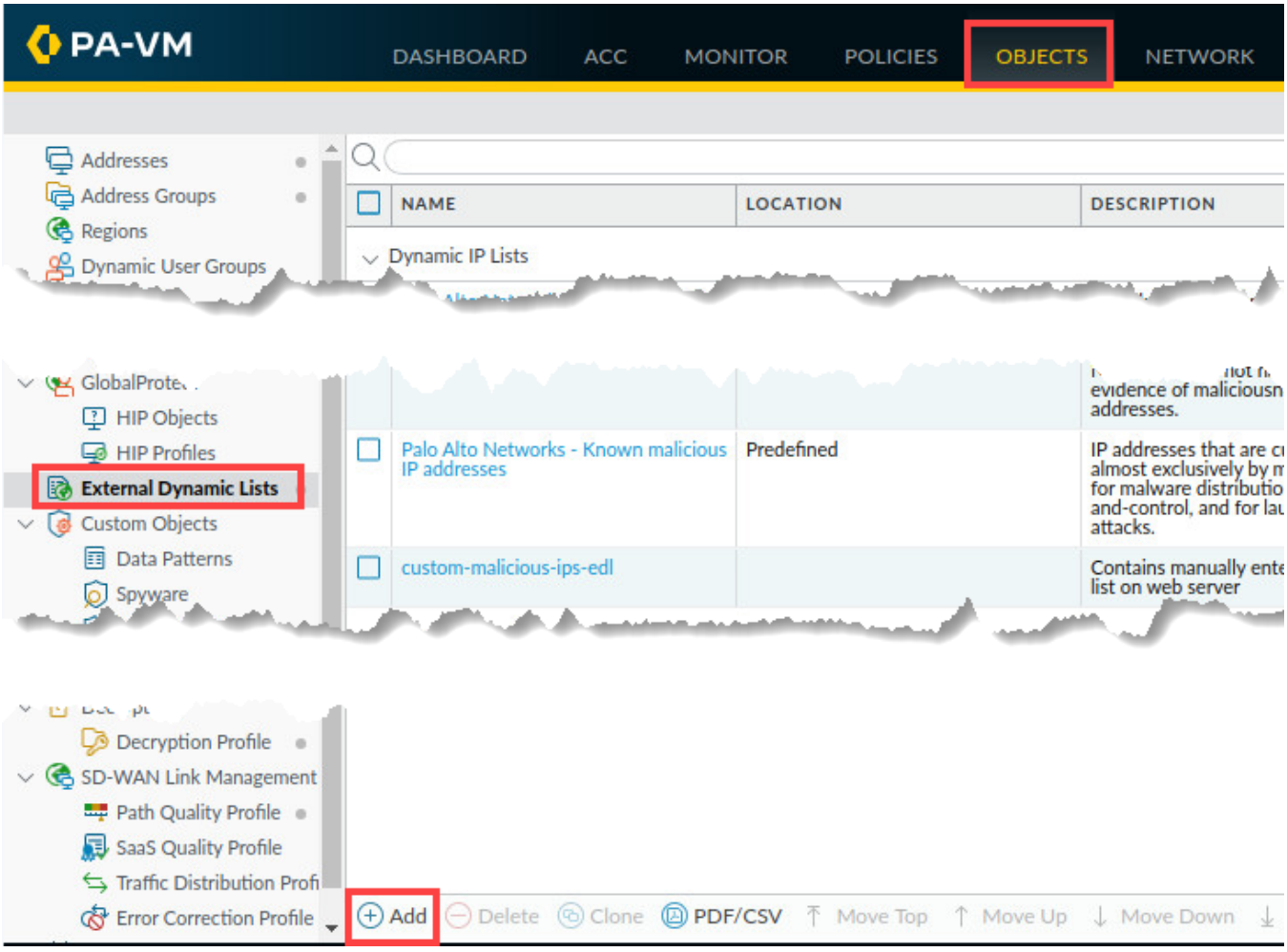

29. Leave the web interface open and continue to the next task.

## 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.

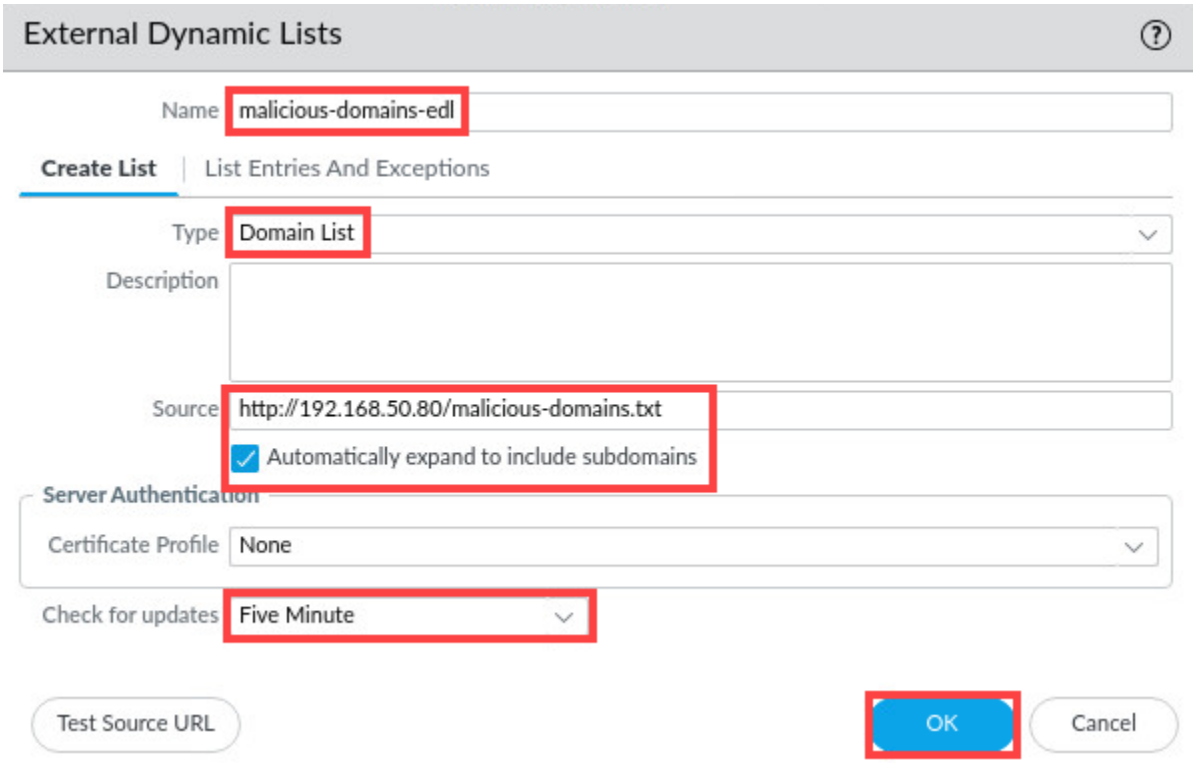
1. In the *PA-VM firewall* web interface, navigate to **Objects > External Dynamic Lists**. Click **Add** at the bottom of the window.



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

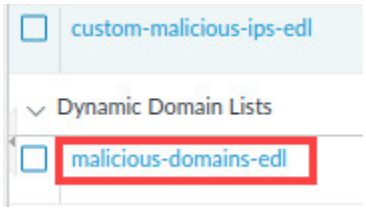
| Parameter | Value |
|---|---|
| **Name** | **malicious-domains-edl** |
| **Type** | **Domain List** |
| **Source** | **http://192.168.50.80/malicious-domains.txt** (The EDL contains the domains quora.com and producthunt.com.) |
| **Automatically expand to include subdomains** | Select it |
| **Check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



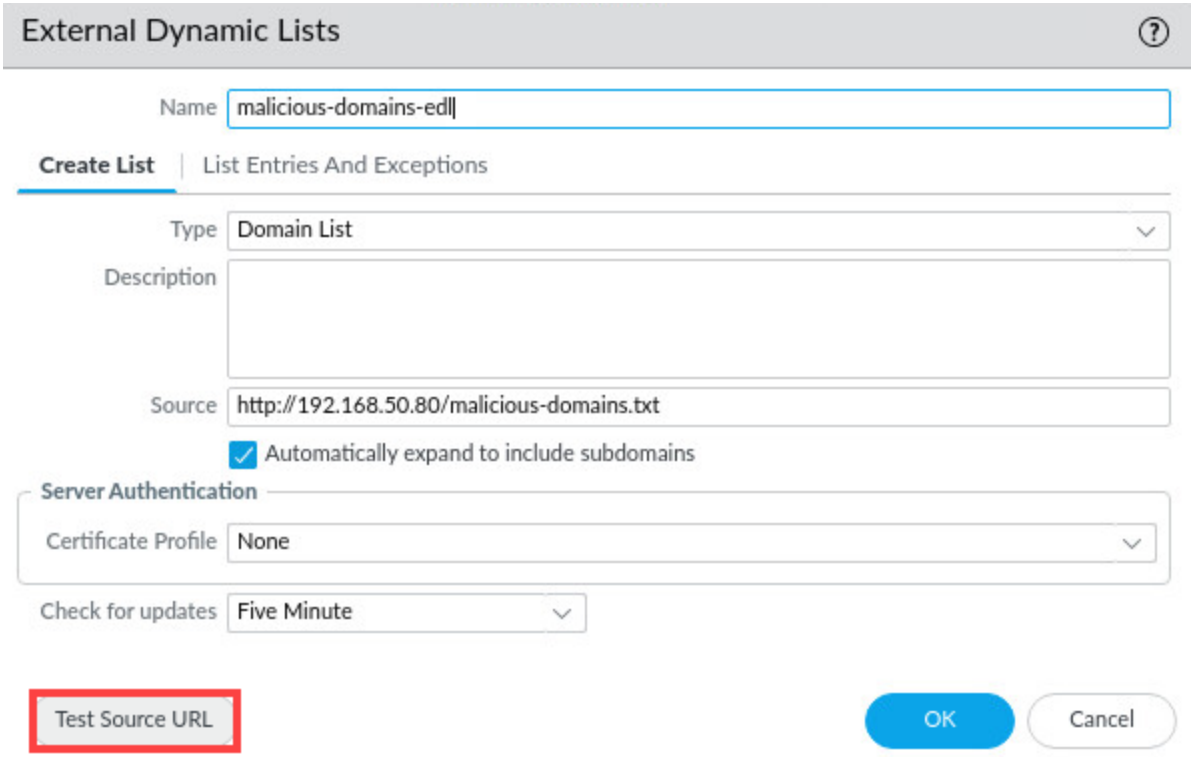

Please Note

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

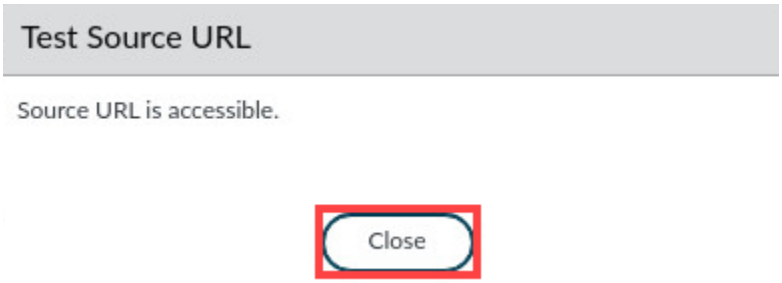
3. Click to reopen the **malicious-domains-edl**.



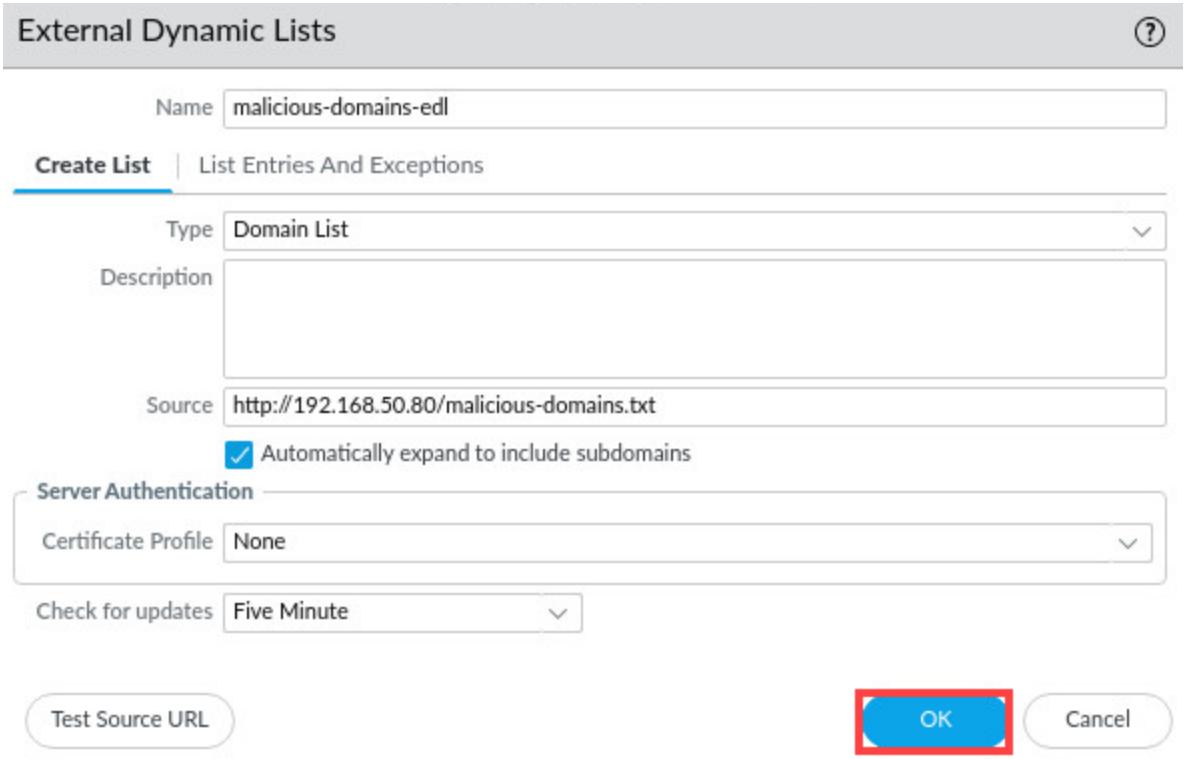
4. In the *External Dynamic Lists* window, click **Test Source URL**.




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



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



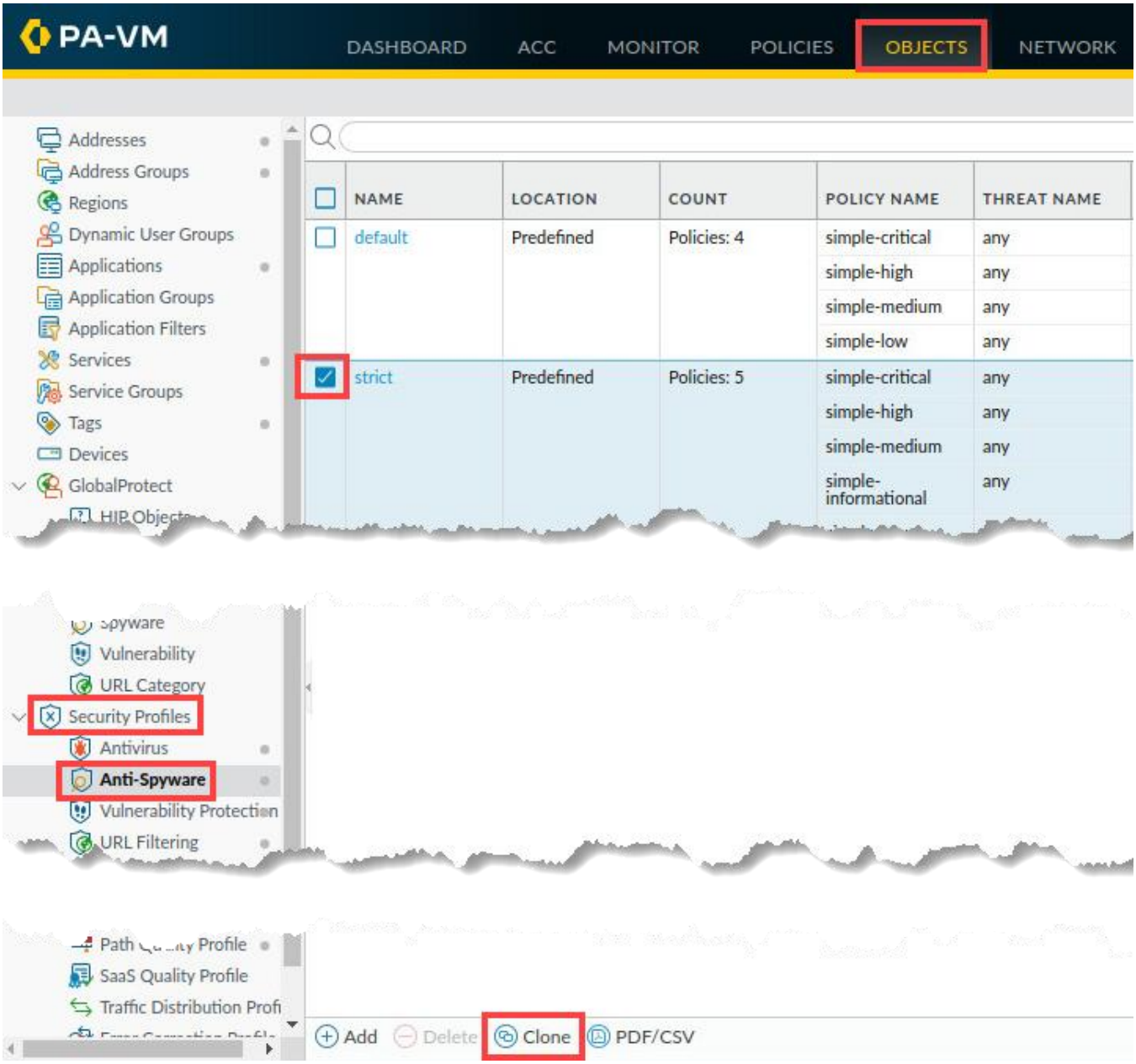

7. Leave the firewall open and continue to the next task.

## 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.

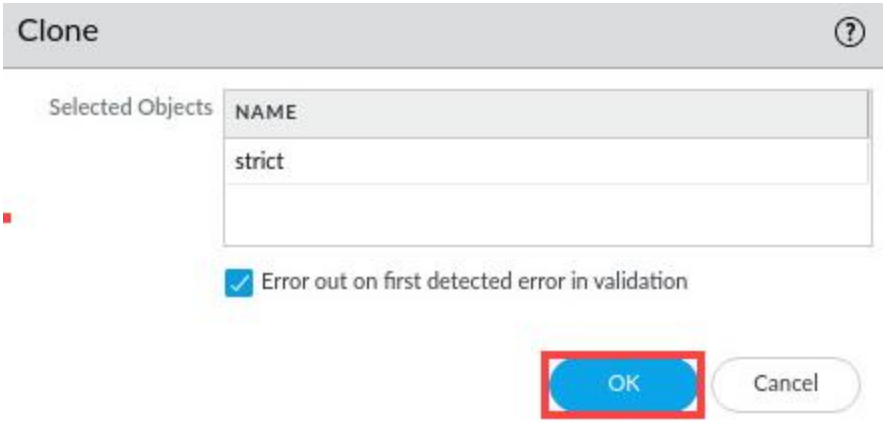
In this section, you will add a domain list EDL to an anti-spyware profile.

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



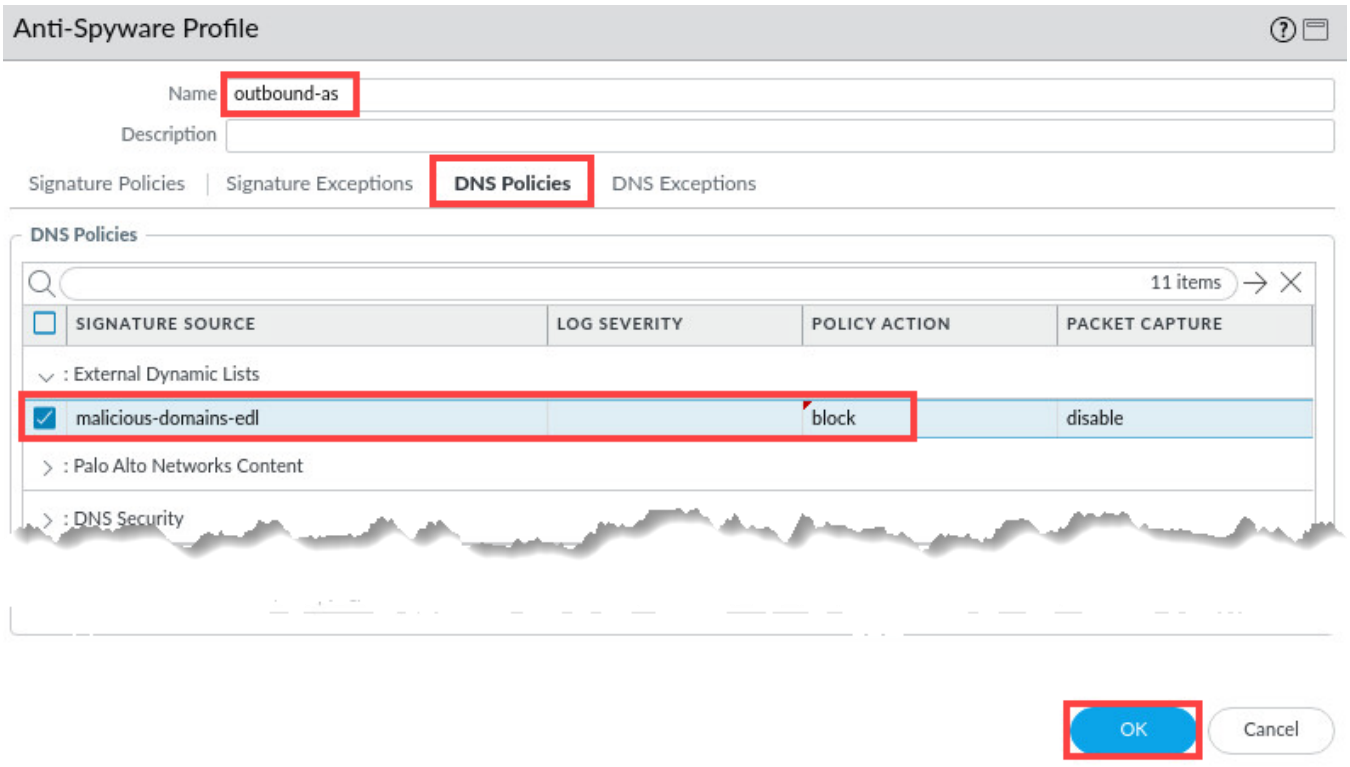

  

2. In the *Clone* window, click **OK**.




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


4. 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.**



Please Note

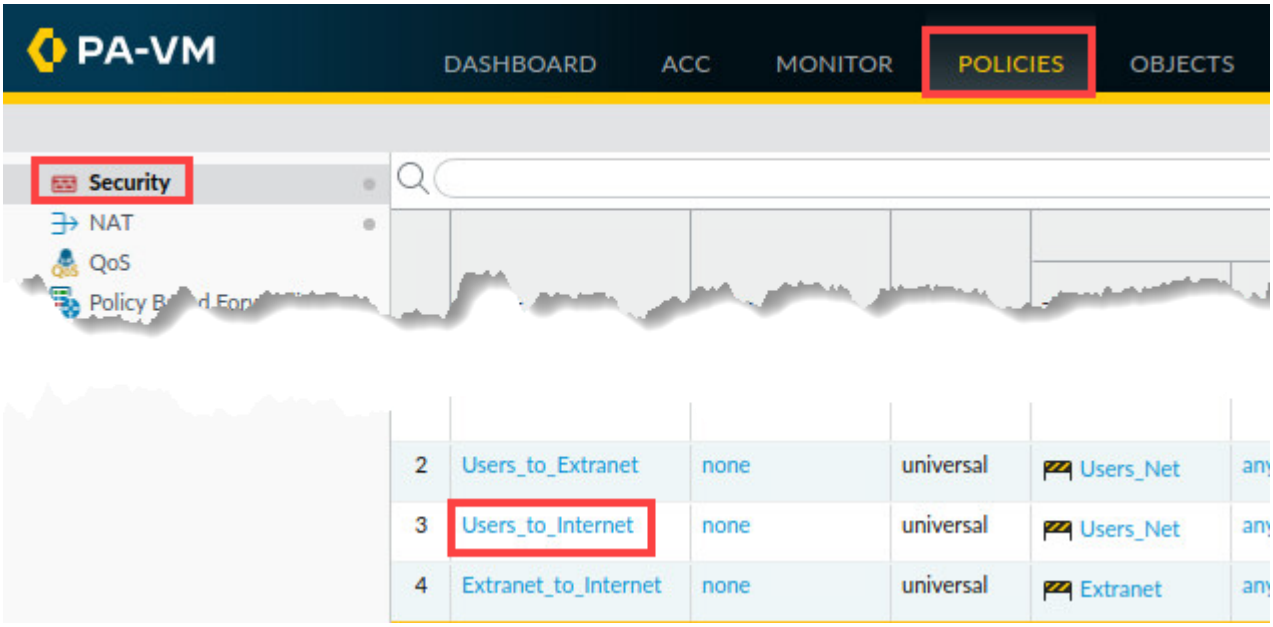
Palo Alto Networks typically recommends the “sinkhole” action, which will be discussed and used in another lab exercise.

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

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

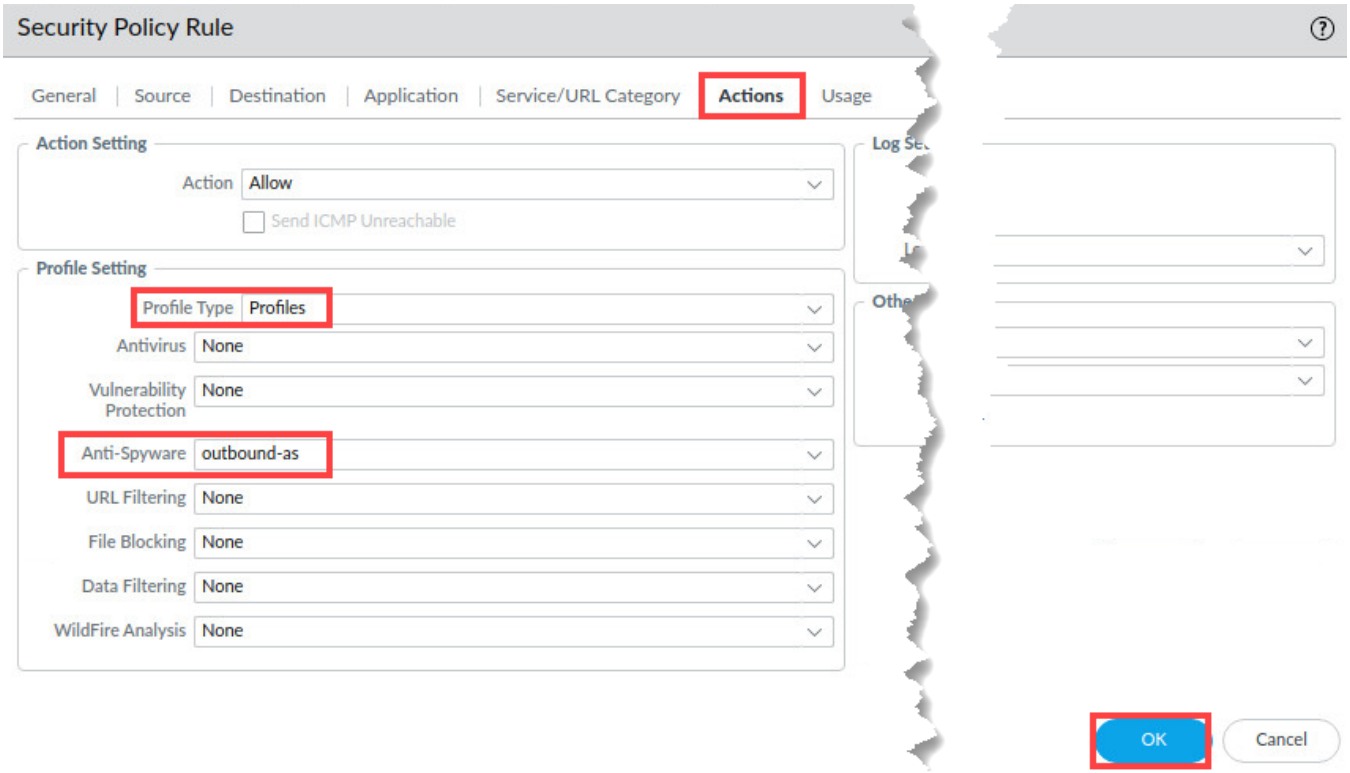
In this section, you will add the **outbound-as** Anti-Spyware Profile to the security policy. The configuration of the profile will enable the firewall to use malicious domain signatures to block access to malicious domains.

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



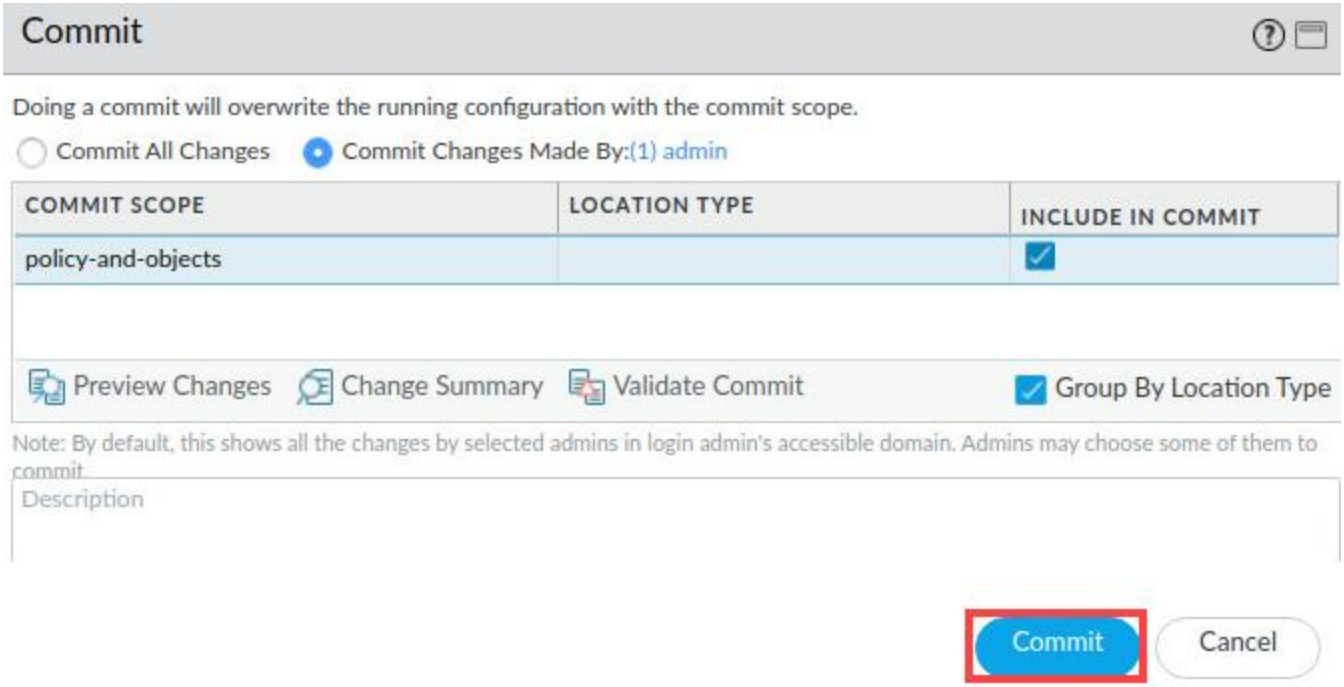
2. In the *Security Policy Rule* window, configure the following on the **Actions** tab. Click **OK**.

| Parameter | Value |
|---|---|
| **Profile Type** | **Profiles** |
| **Anti-Spyware** | **outbound-as** |

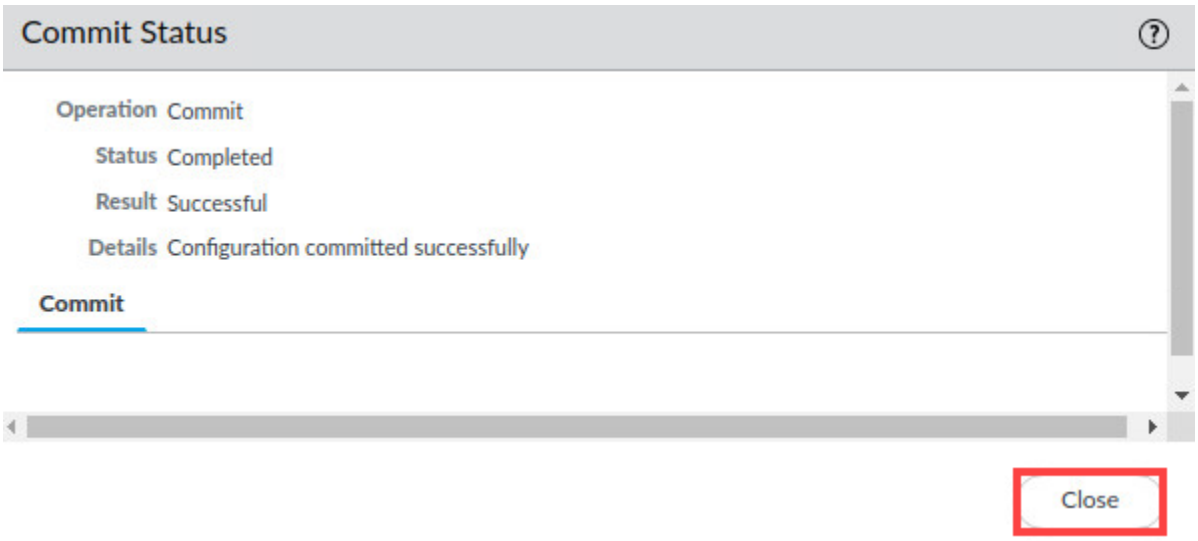



3. Click the **Commit** button at the upper-right of the web interface.

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

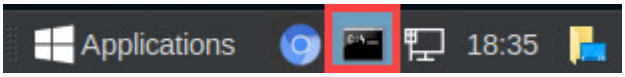



5. Wait until the *Commit* process is complete. Click **Close**.




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

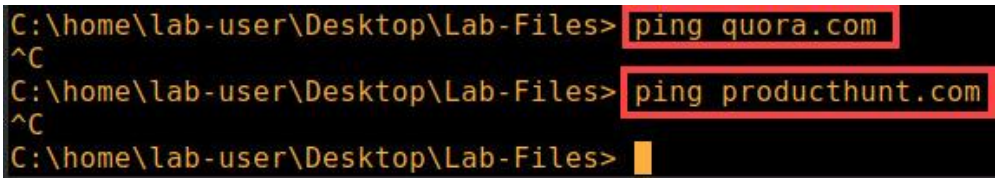

7. Return to the *terminal* window by clicking on the **terminal** icon in the taskbar of your *client desktop*.



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>
```

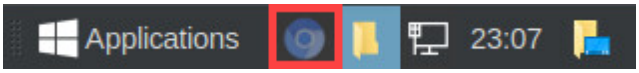



Please Note

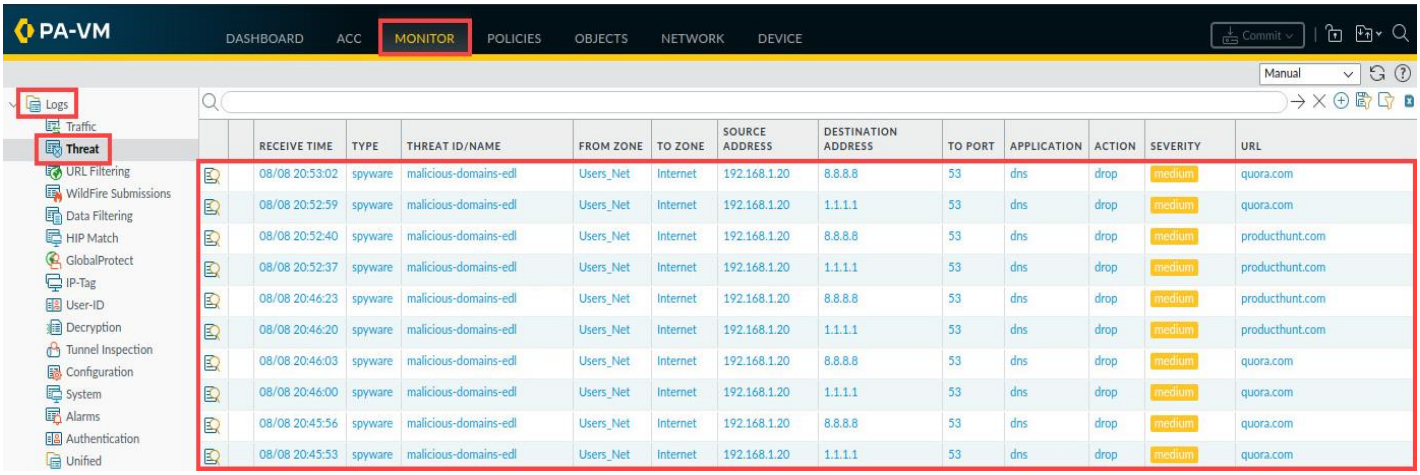
The ping commands should fail because the domains are listed in the custom EDL and the custom EDL was added to the outbound-as Anti-Spyware Profile and configured with the "block" action.

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.**



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.

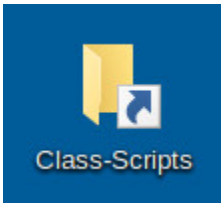

## 7.10 Block Access to Malicious URLs Using the Security Policy

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.

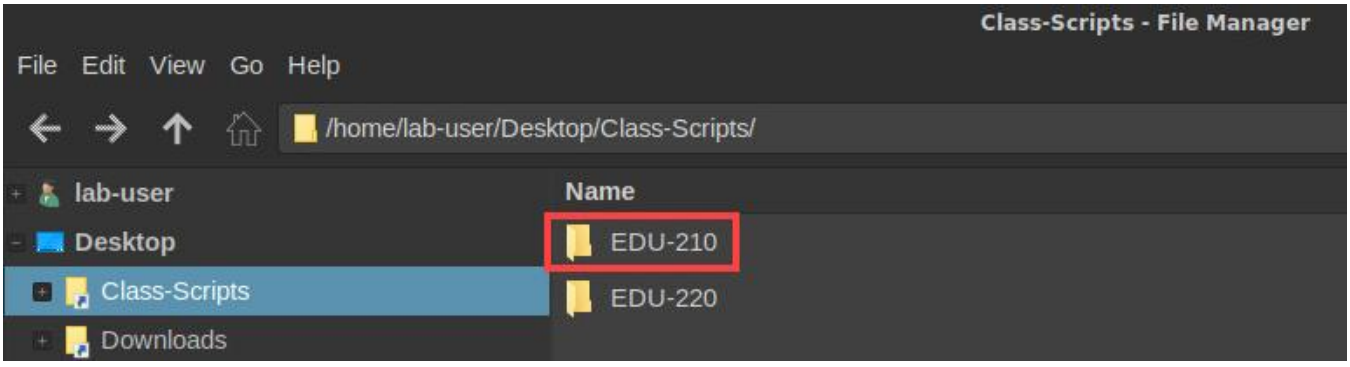
Please Note

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.

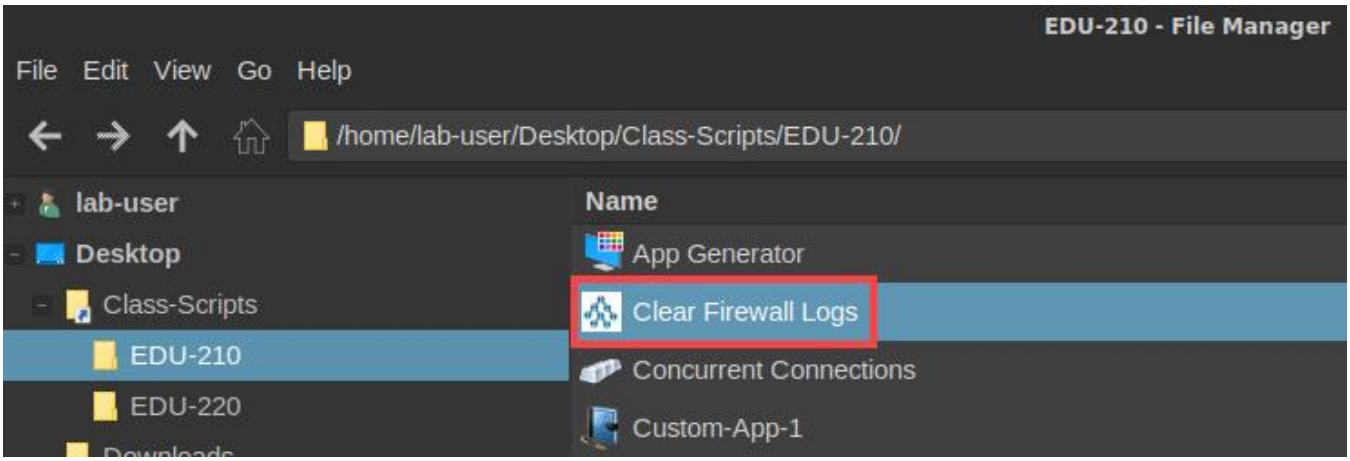
1. On the *client desktop*, double-click the folder for **Class-Scripts**.




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



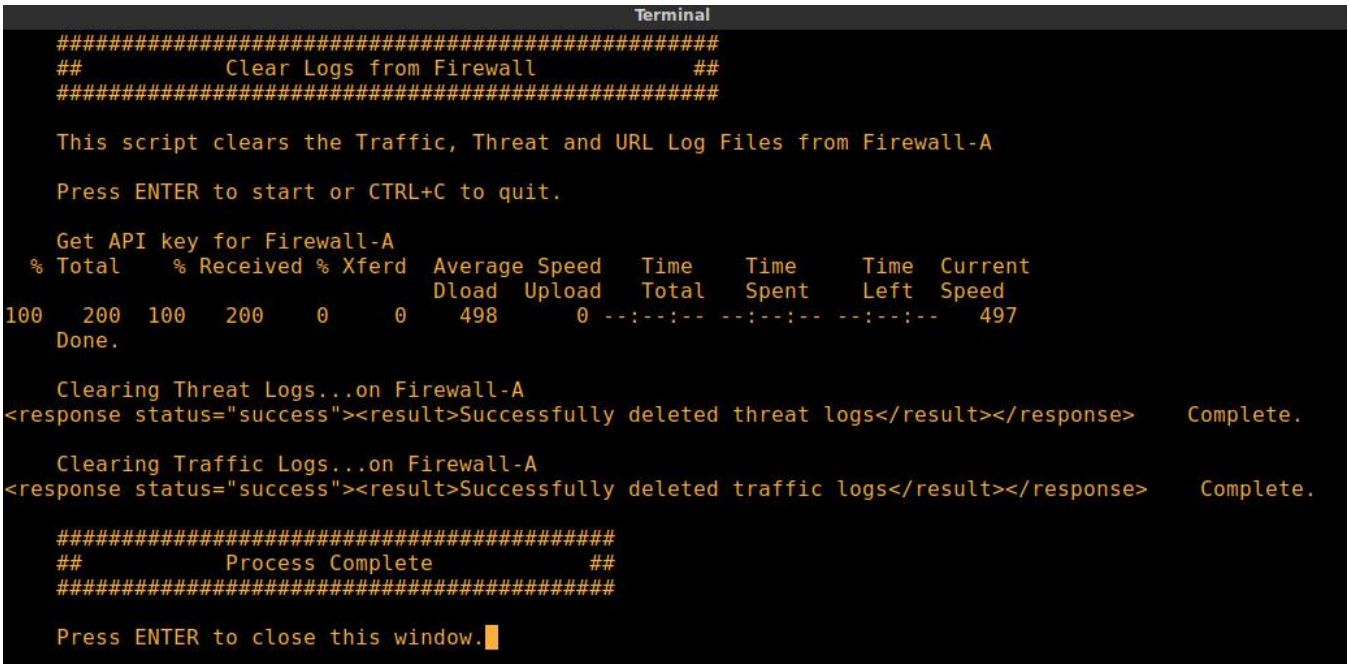
3. Double-click the icon for **Clear Firewall Logs**.



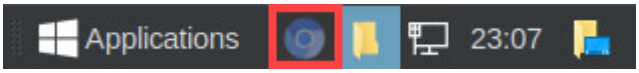

Please Note

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.

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




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



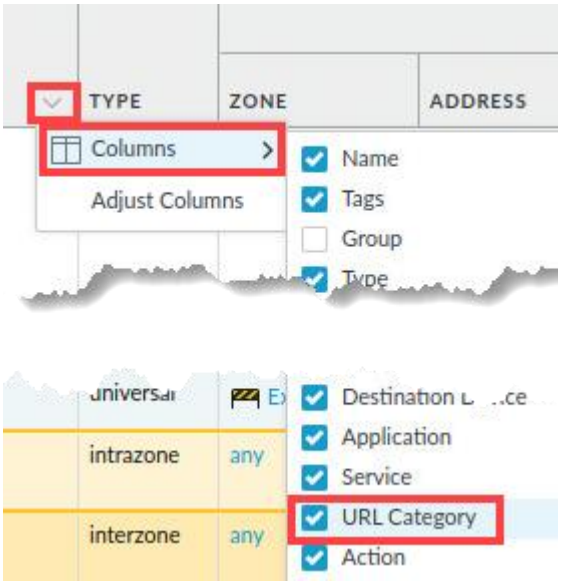

  

6. Open a new tab in **Chromium**.


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.**



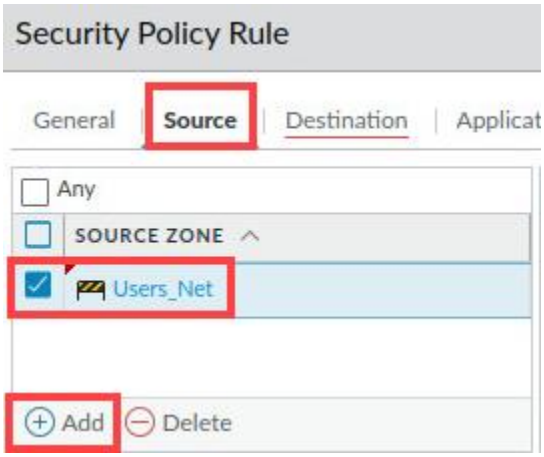
Please Note

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

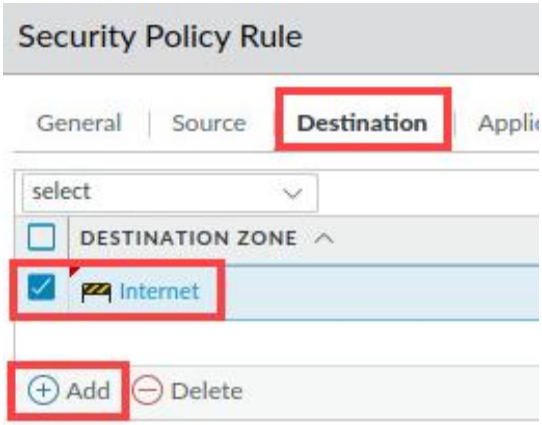
10. In the *Security Policies* window, click **Add** to create a new security policy rule.


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.`**

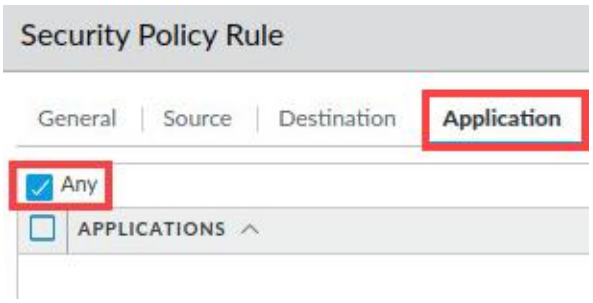

12. Click the **Source** tab and for the *Source Zone*, select **Users_Net**.



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




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

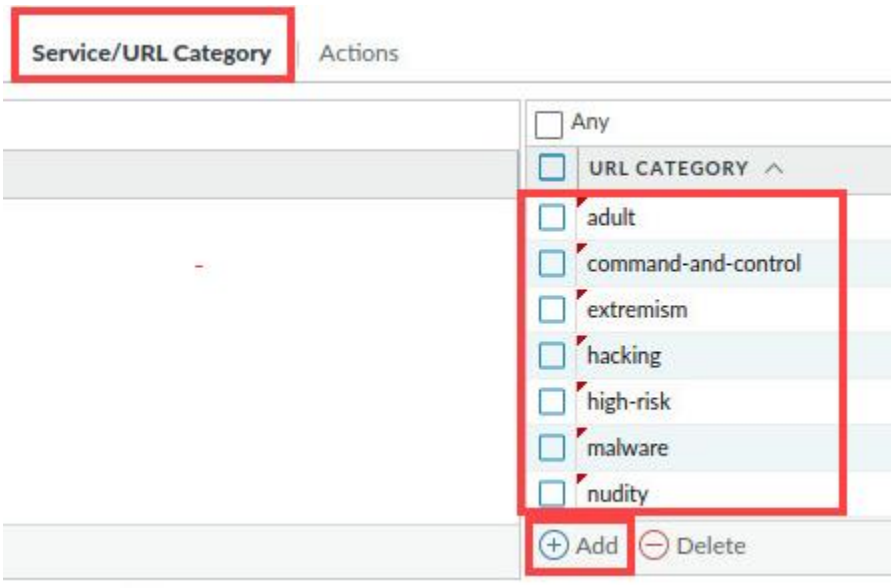


15. Click the **Service/URL Category** tab and configure the following.

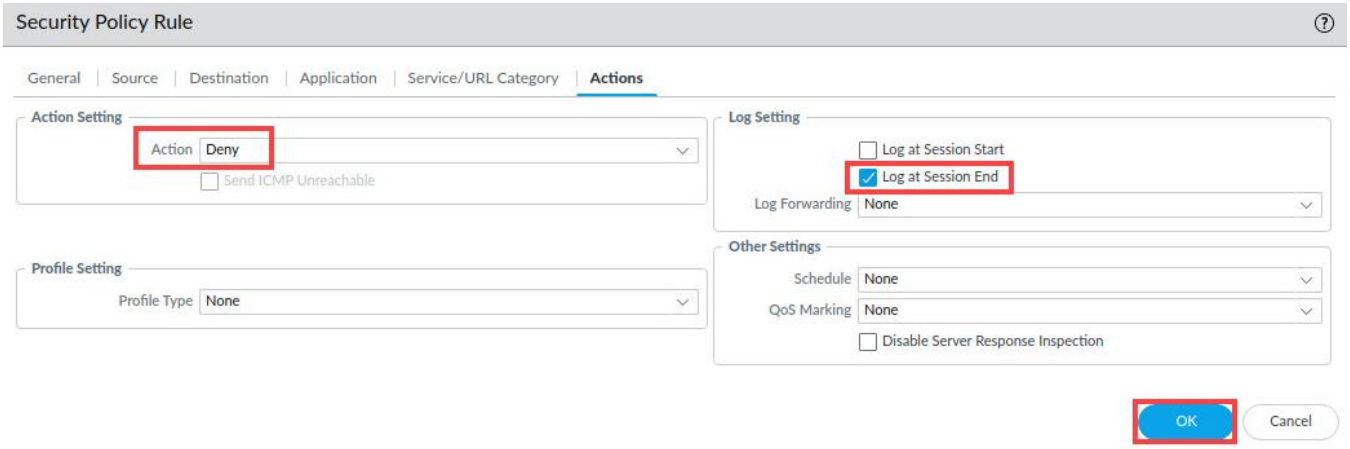
| Parameter | Value |
|---|---|
| **Service** | **application-default** |
| **URL Category** | Add the following:<br>**adult**<br>**command-and-control**<br>**extremism**<br>**hacking**<br>**high-risk**<br>**malware**<br>**nudity**<br>**parked**<br>**peer-to-peer**<br>**phishing**<br>**proxy-avoidance-and-anonymizers**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

Please Note

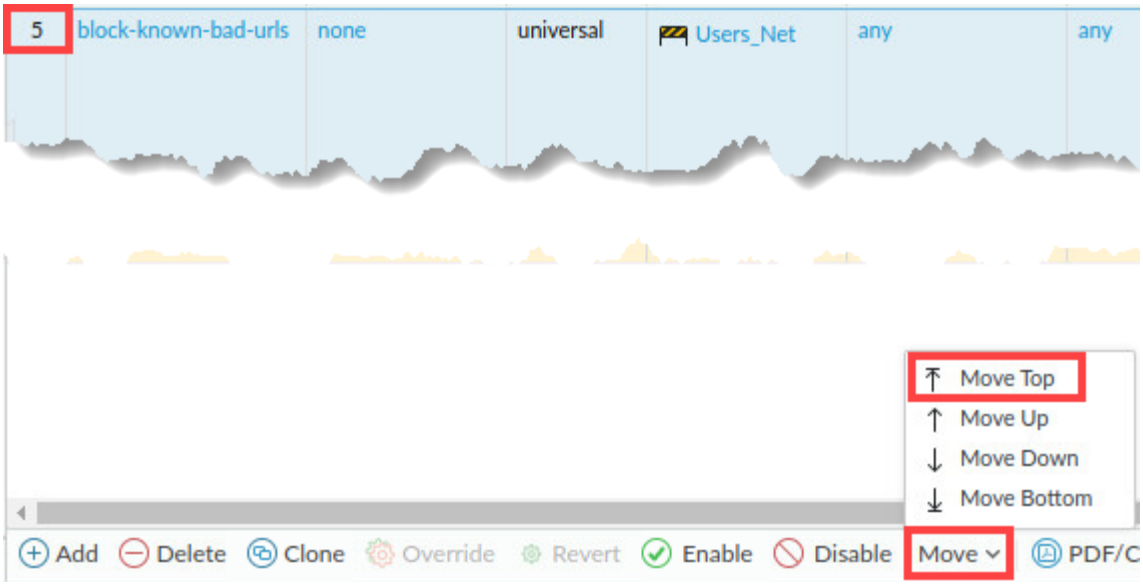
You can type in the first few letters of each category to locate each one more quickly.



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

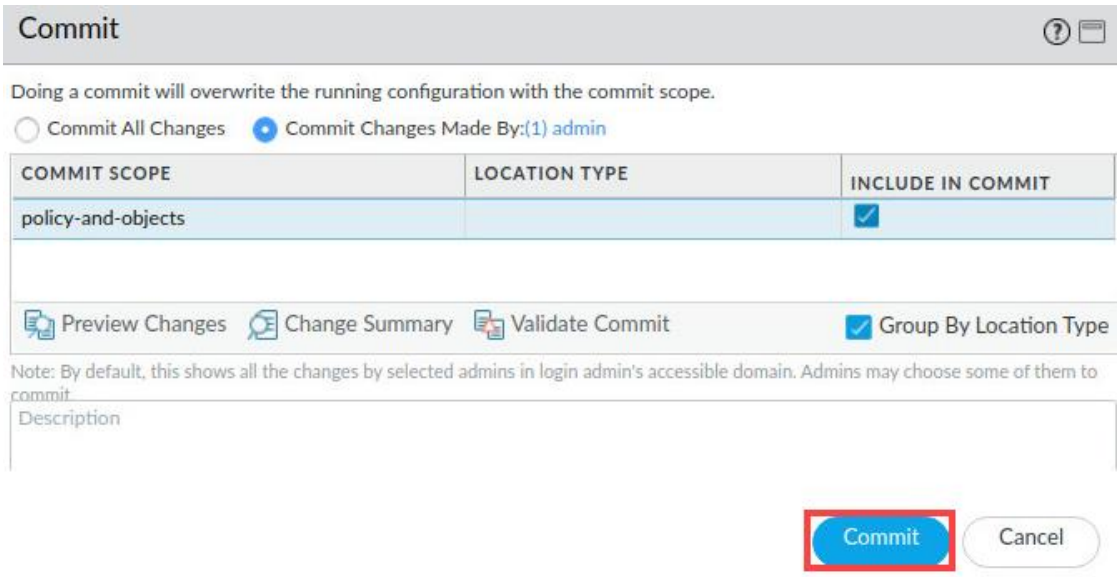



17. Select, but do not open, the **block-known-bad-urls** rule in the security policy. Select **Move > Move Top** to move the *block-known-bad-urls* rule to the top of the security policy.

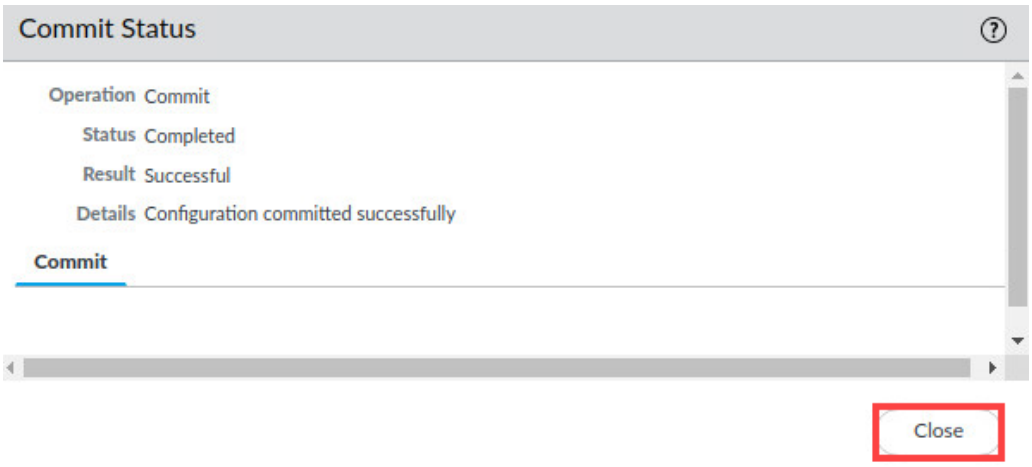



18. Click the **Commit** button at the upper-right of the web interface.

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

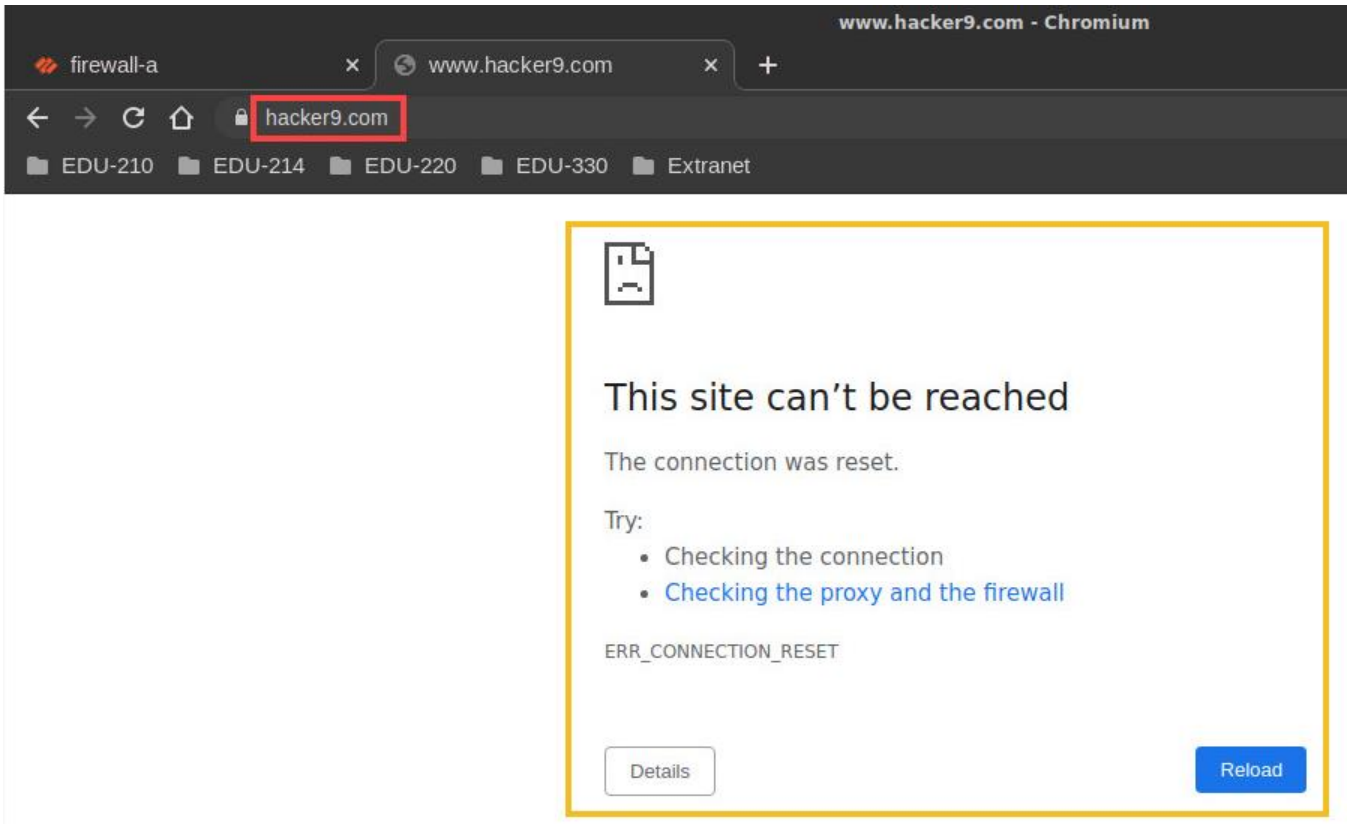



20. Wait until the *Commit* process is complete. Click **Close**.




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

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

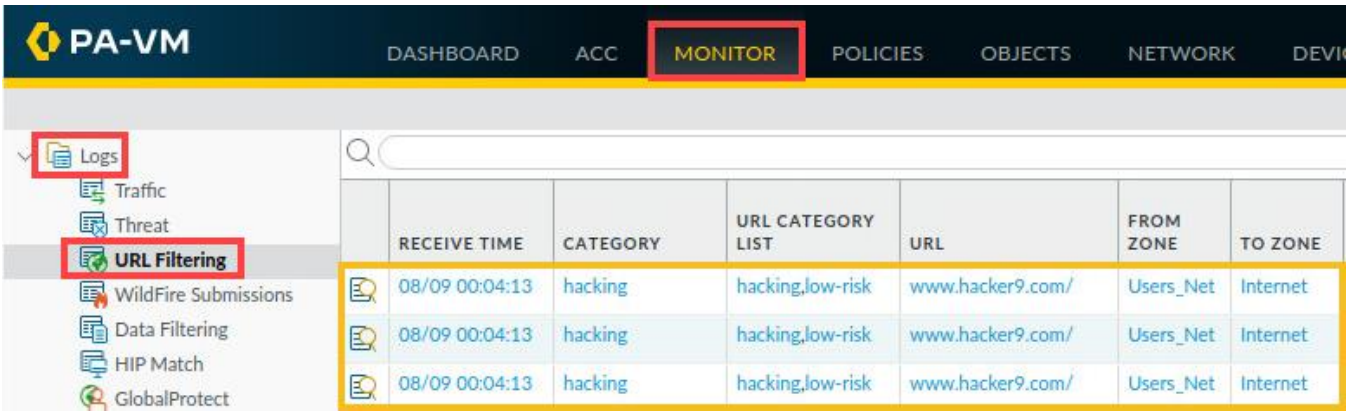



**Please Note**

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**.




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.

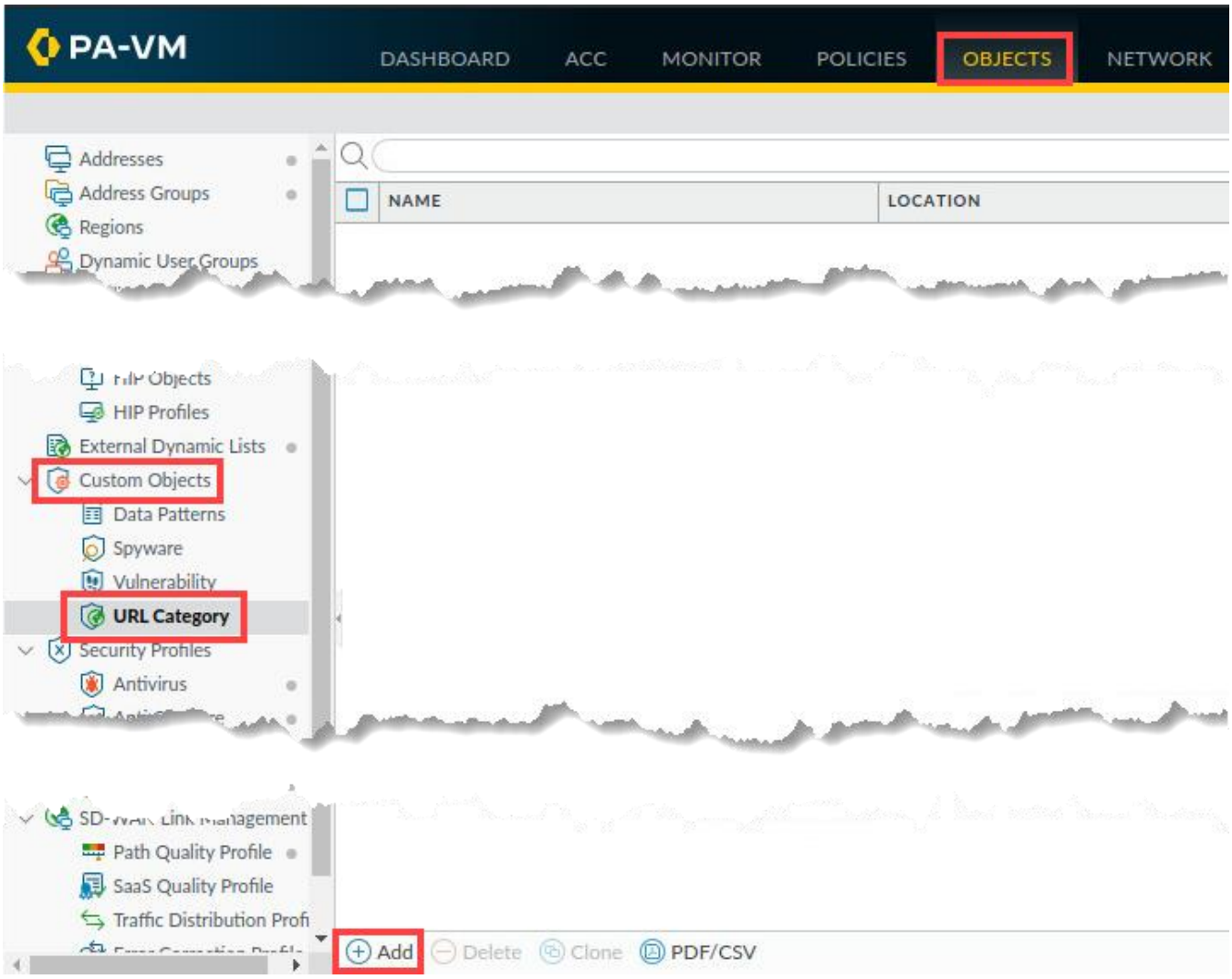
1. Open a new tab in **Chromium**.


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

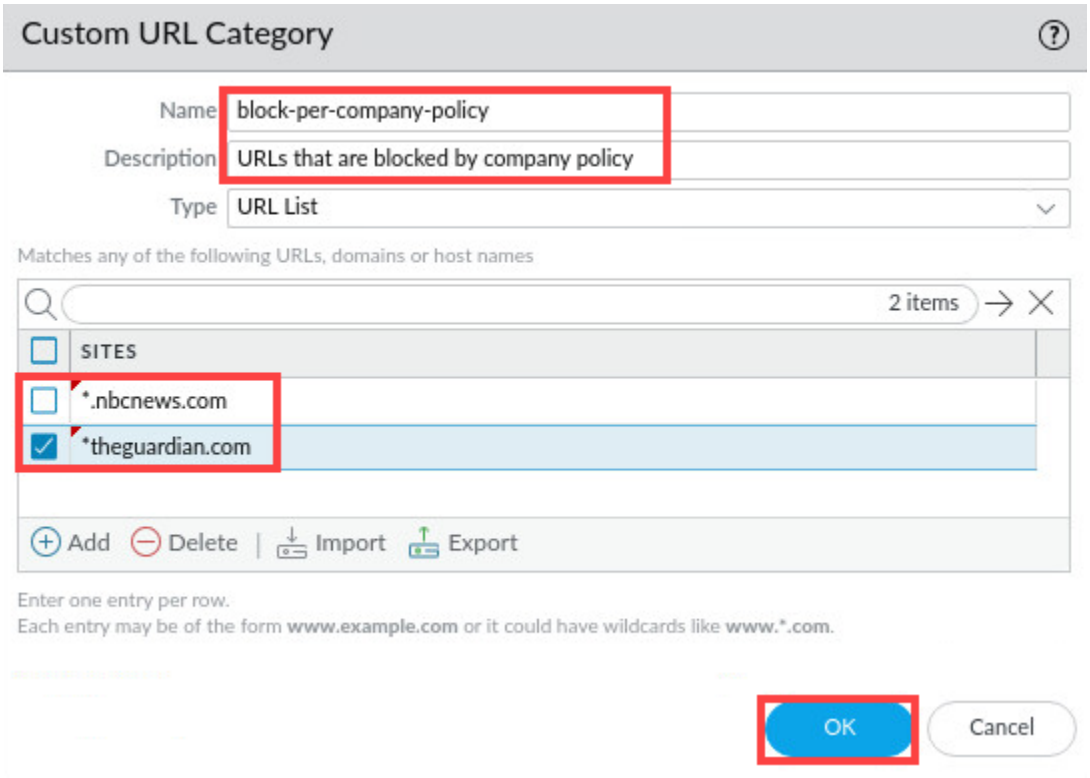
3. Close the *nbcnews.com* tab by clicking the **X** icon.


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

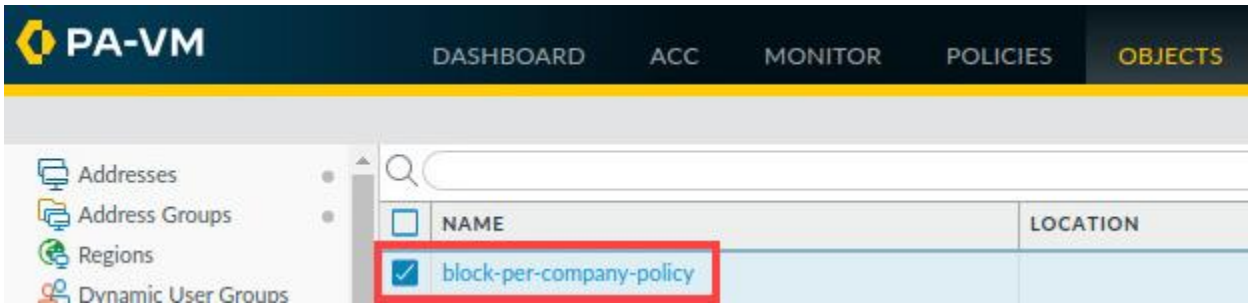


5. In the *Custom URL Category* window, configure the following. Click **OK.**

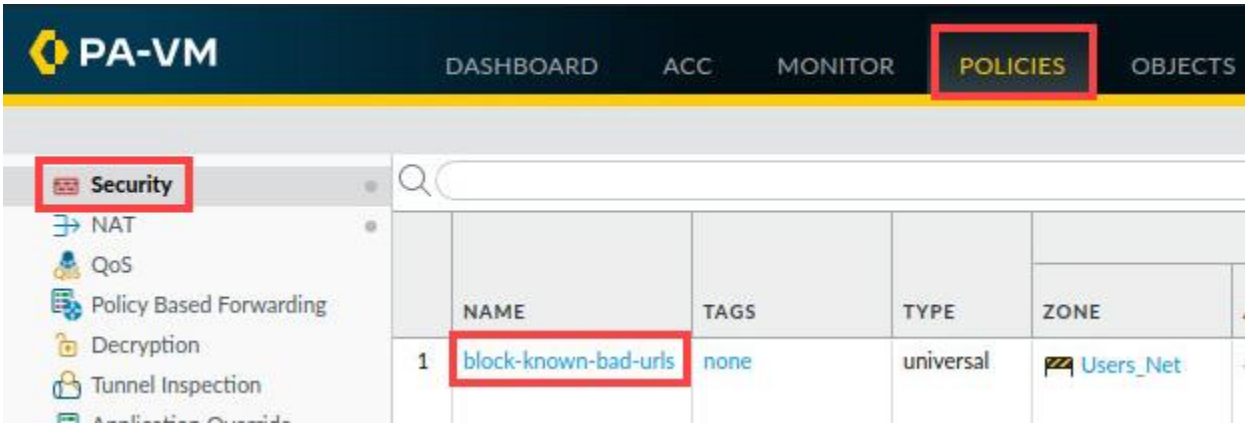
| Parameter | Value |
|---|---|
| **Name** | `block-per-company-policy` |
| **Description** | `URLs that are blocked by company policy.` |
| **Sites** | Add the following:<br>`*.nbcnews.com`<br>`*.theguardian.com` |



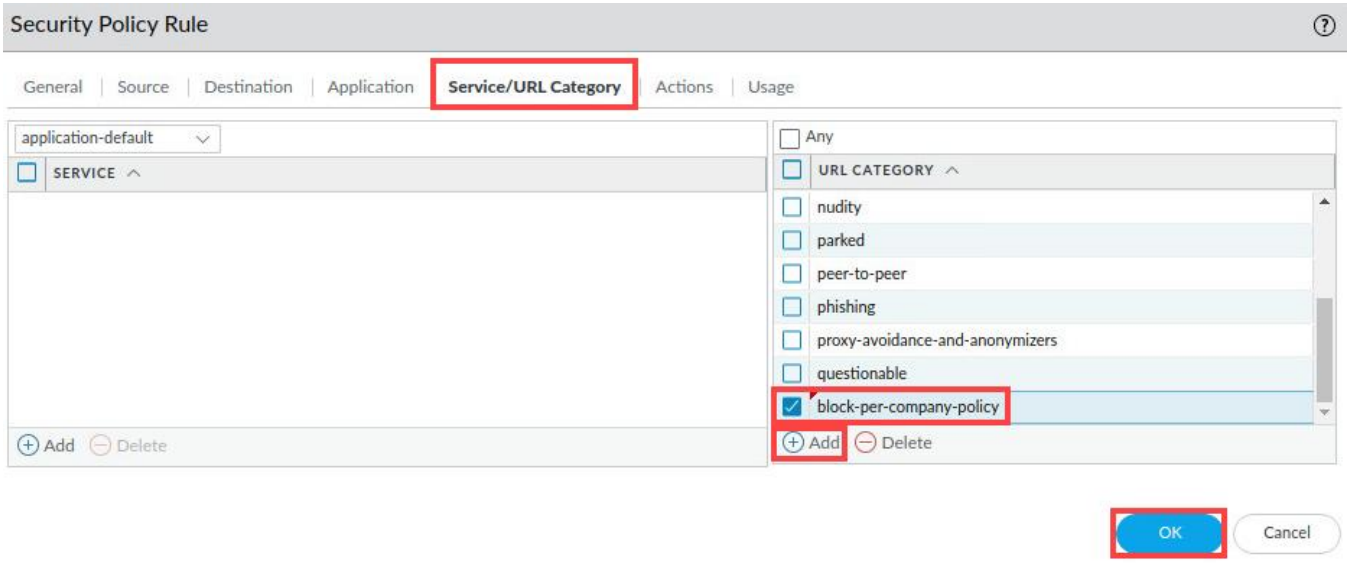

6. Confirm the *block-per-company-policy* Custom URL is showing in the *URL Category* window.



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.

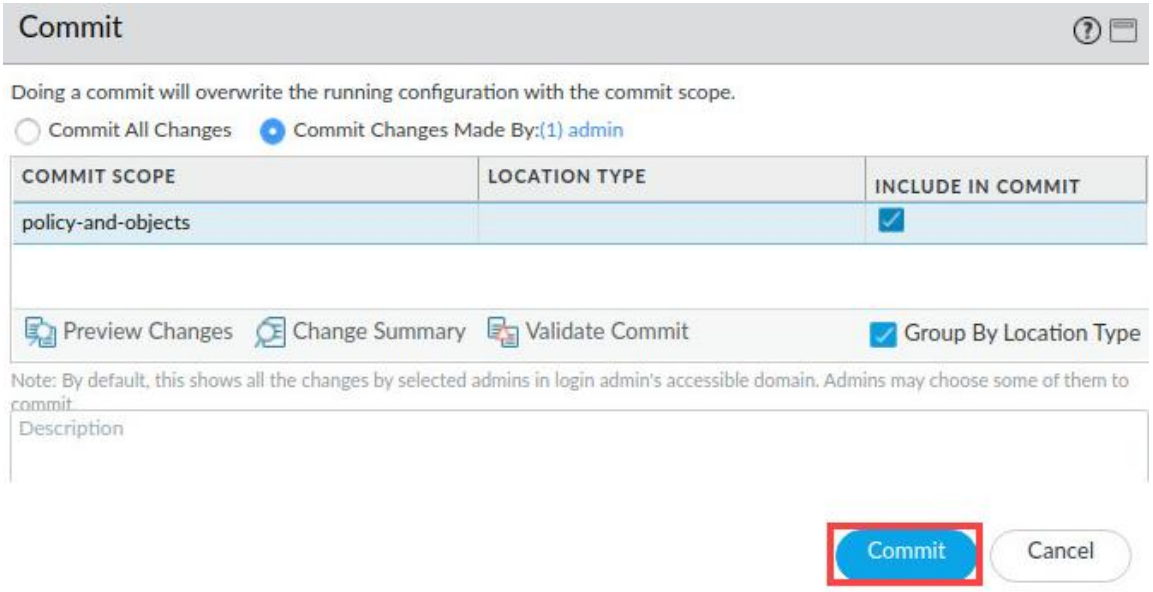



8. Select the **Service/URL Category** tab and click **Add**. Add **block-per-company-policy** to the list. Click **OK**.

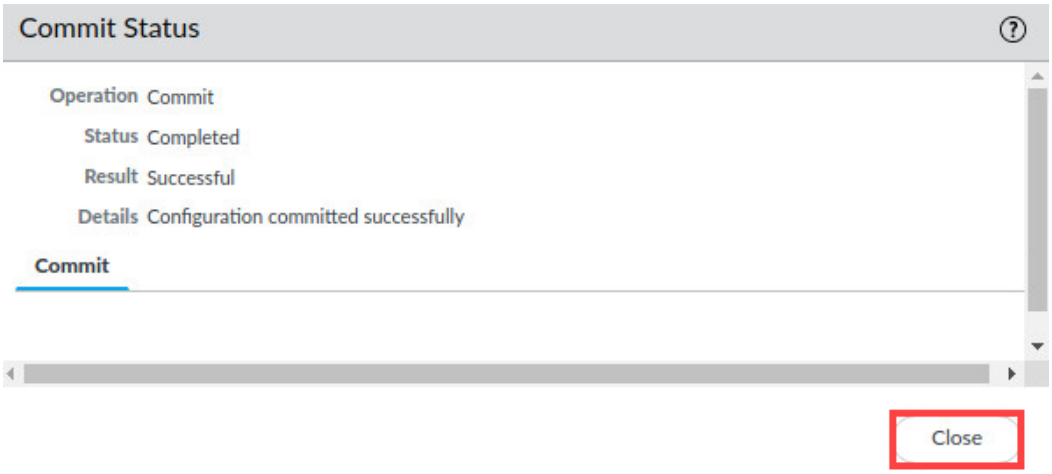



9. Click the **Commit** button at the upper-right of the web interface.

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

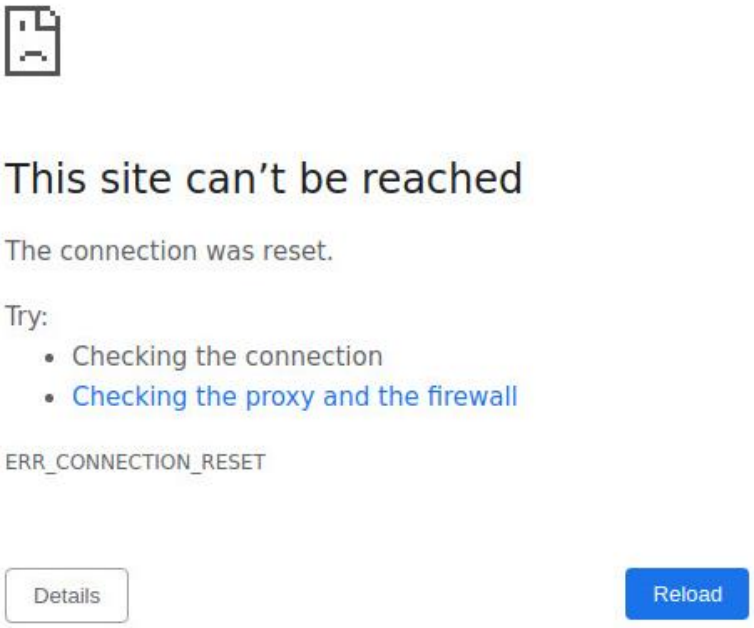



11. Wait until the *Commit* process is complete. Click **Close**.




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**.

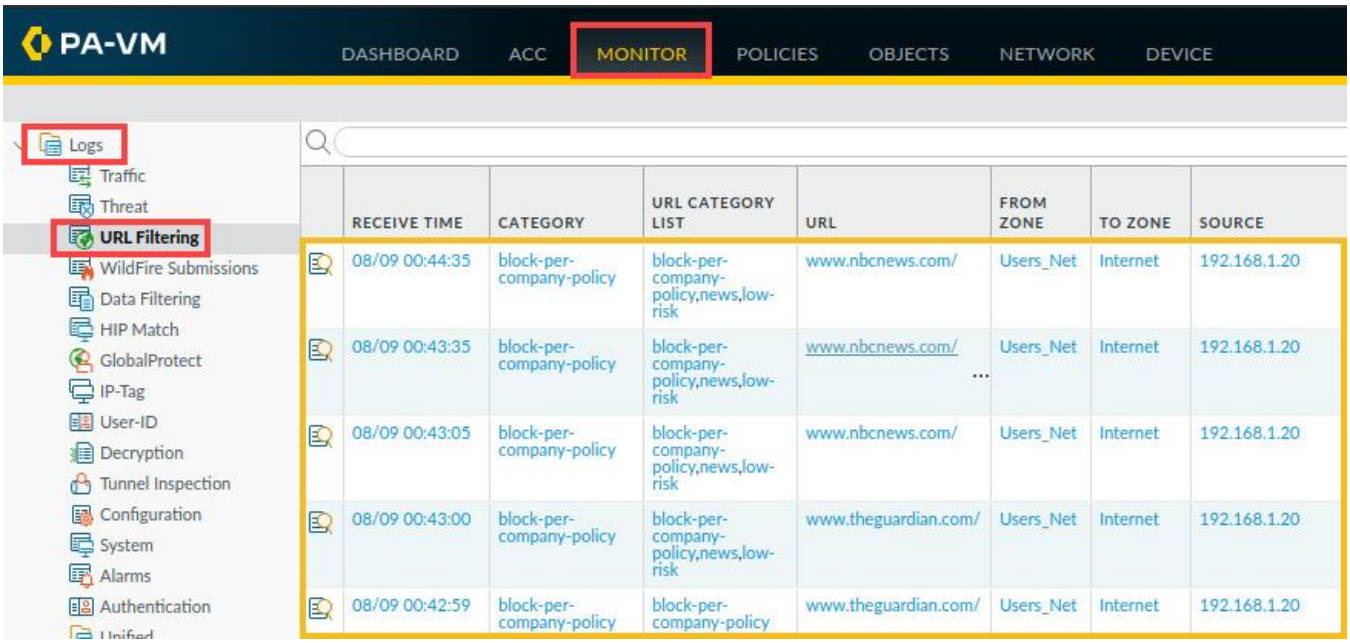



Please Note

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.**




Please Note

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

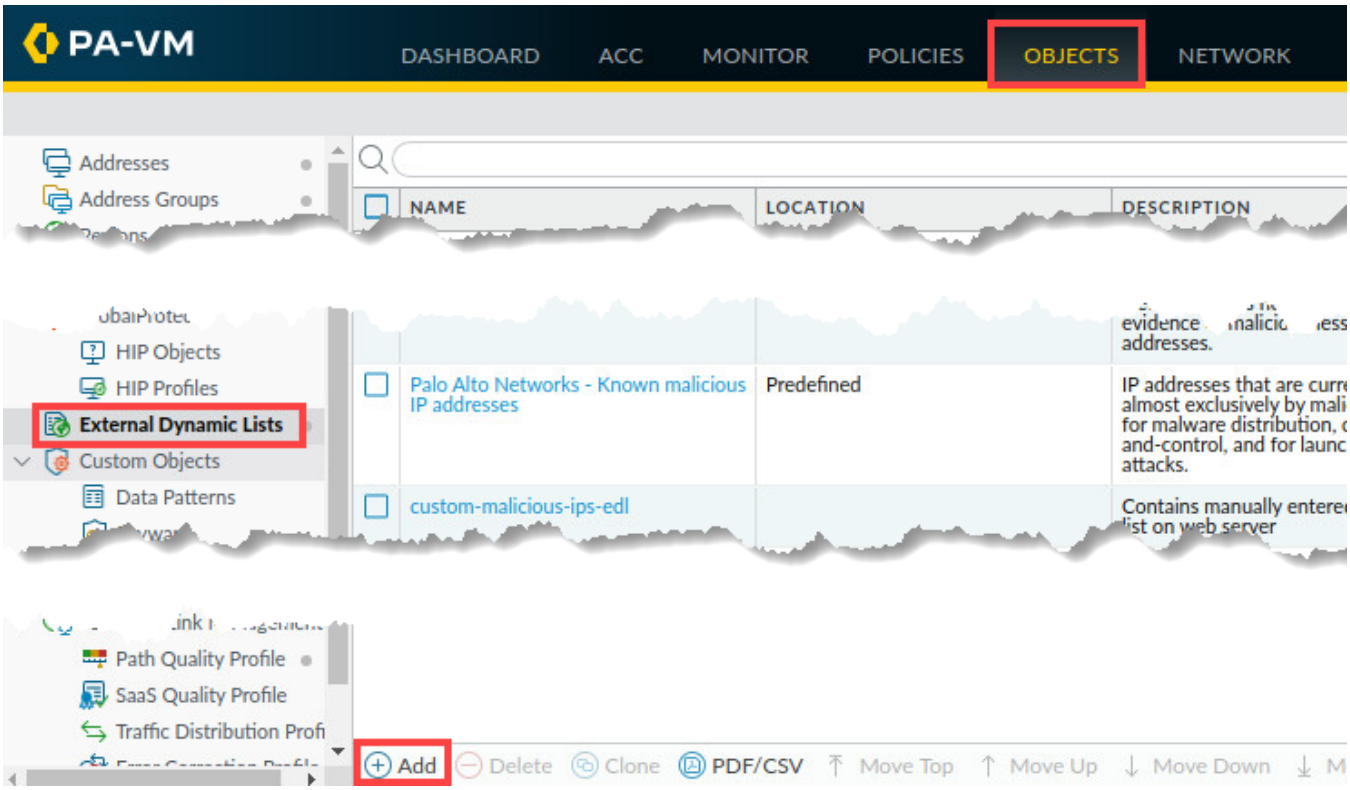
16. Leave the firewall open and continue to the next task.

## 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.

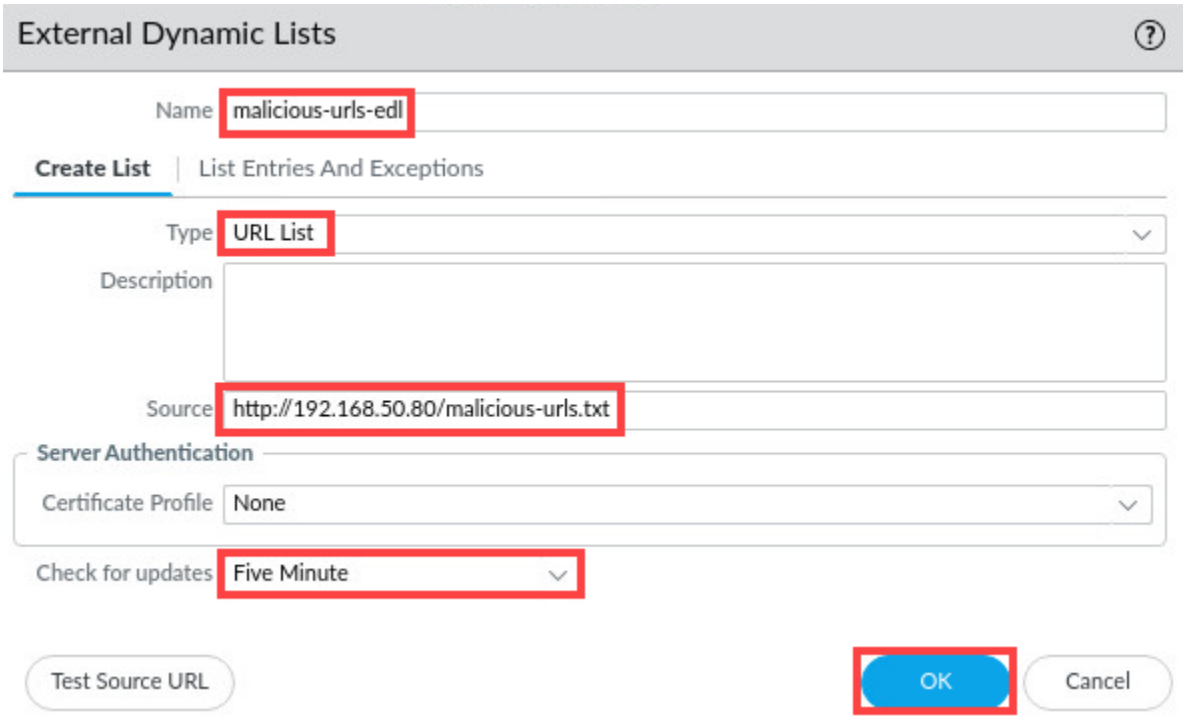
1. In the web interface, select **Objects > External Dynamic Lists.** Click **Add**.



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

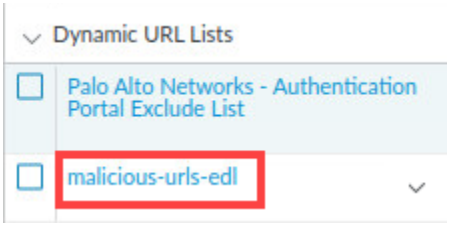
| Parameter | Value |
|---|---|
| **Name** | **malicious-urls-edl** |
| **Type** | **URL List** |
| **Source** | **http://192.168.50.80/malicious-urls.txt**<br>(The EDL contains only the URL www.popurls.com) |
| **Check for updates** | **Five Minute** |



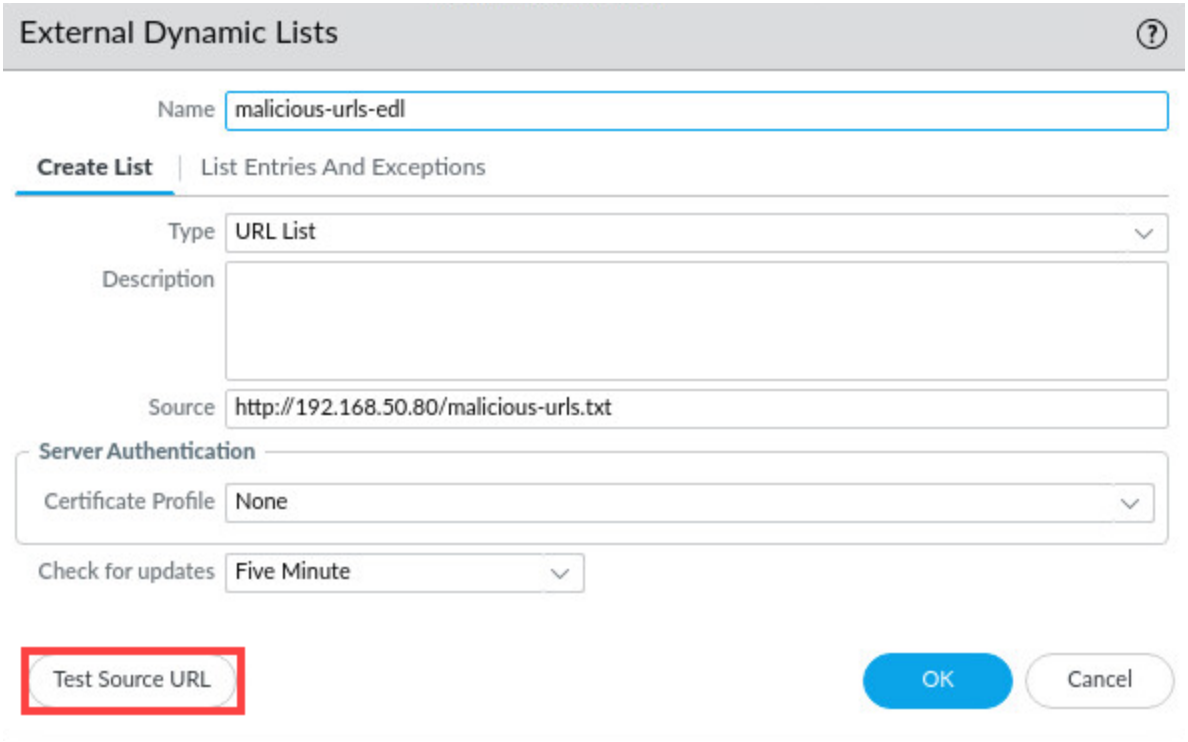

Please Note

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

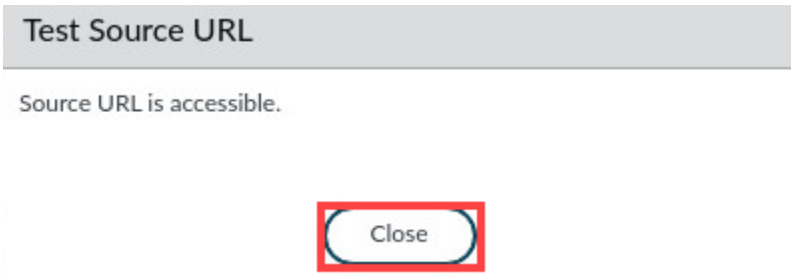
3. In the *External Dynamic Lists* window, click **malicious-urls-edl**.



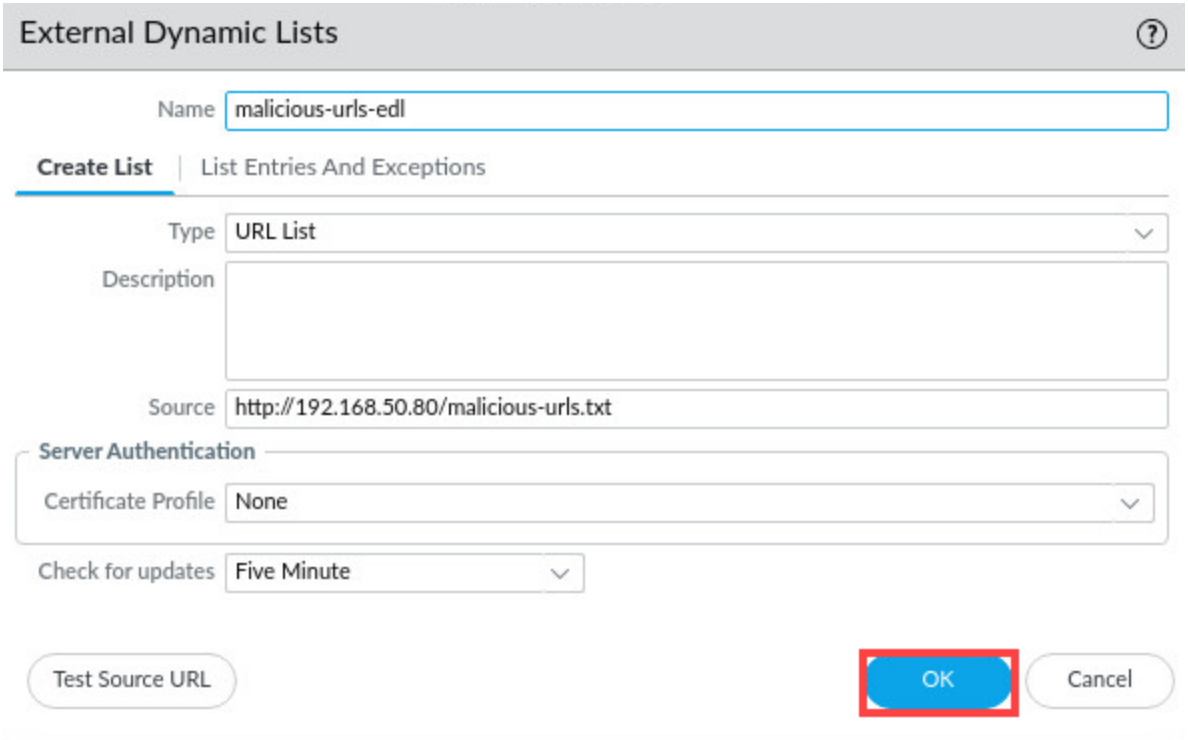
4. Click **Test Source URL** and verify the firewall can access the *EDL URL*.



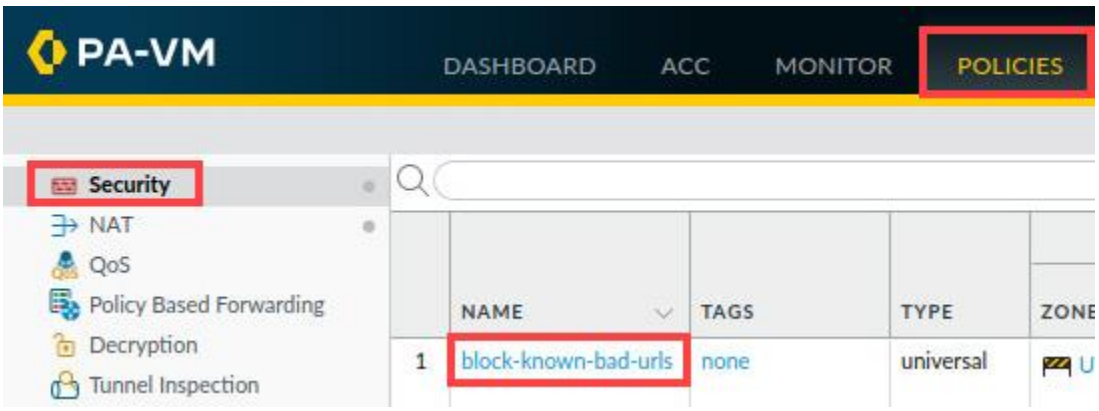

5. In the *Test Source URL* window, verify the *Source URL* is accessible. Click **Close**.



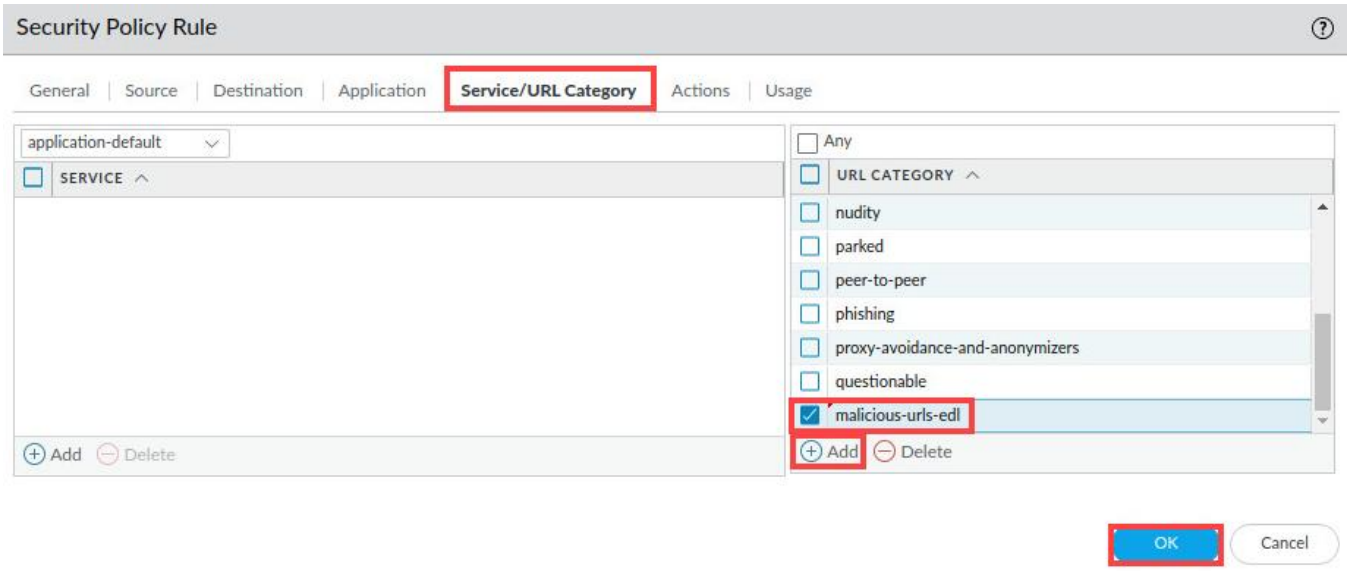
6. In the *External Dynamic List* window, click **OK**.




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**.**

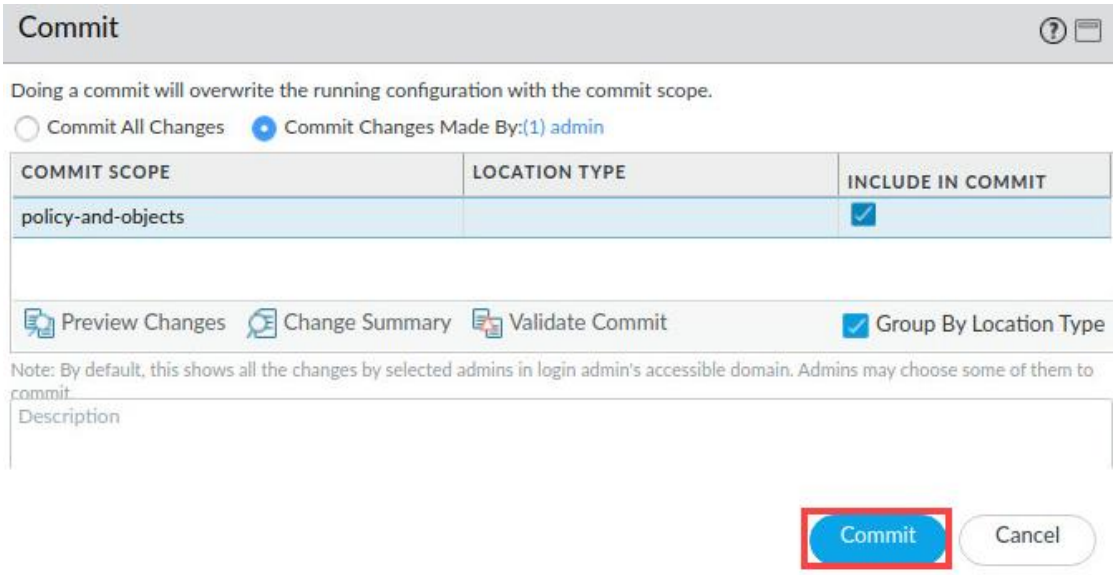


8. In the *Security Policy Rule* window, click the **Service/URL Category** tab. Add **malicious-urls-edl** to the list. Click **OK.**

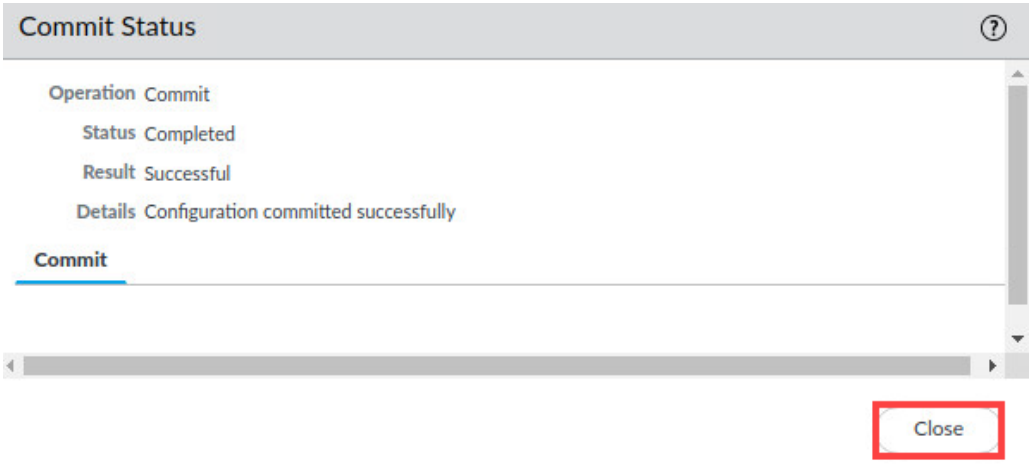



9. Click the **Commit** button at the upper-right of the web interface.


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

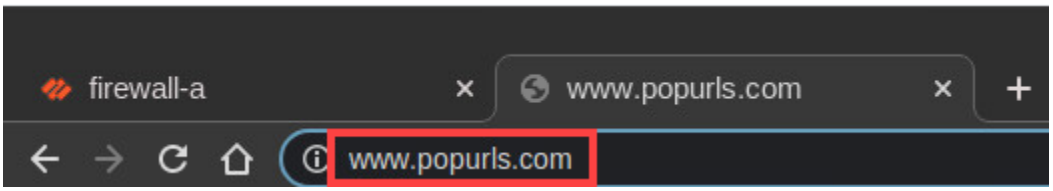


11. Wait until the *Commit* process is complete. Click **Close**.

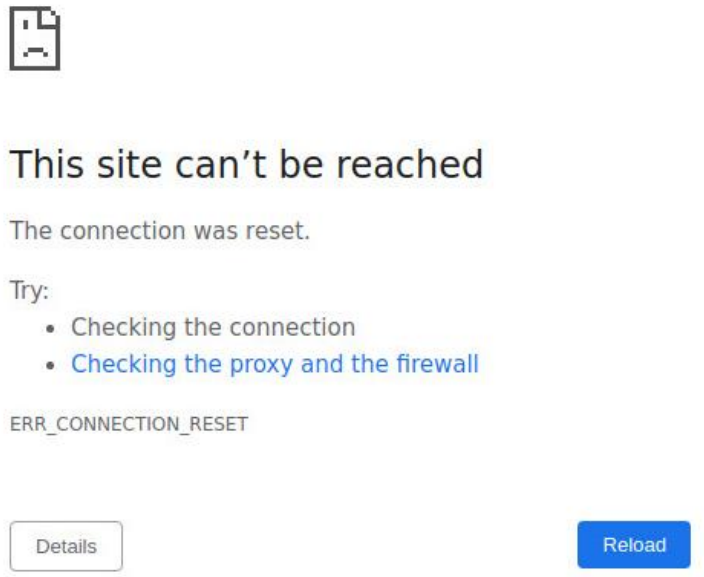



12. Test access to a URL contained in the EDL that you added to the *block-known-bad-urls* security policy. Open a new tab in **Chromium**.


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



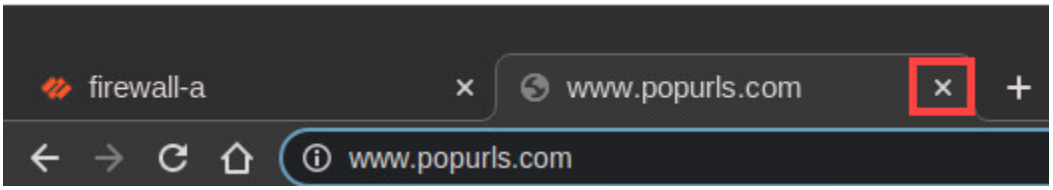
14. The browser displays a block page because the EDL in the security policy blocks access to the *popurls.com* webpage.



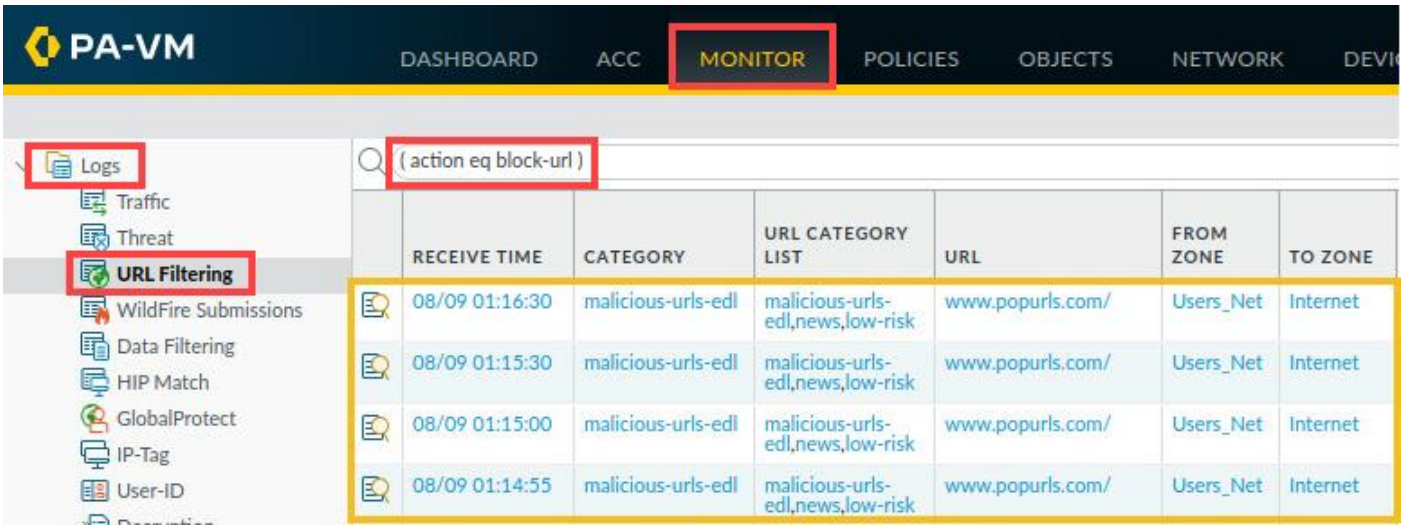

Please Note

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.



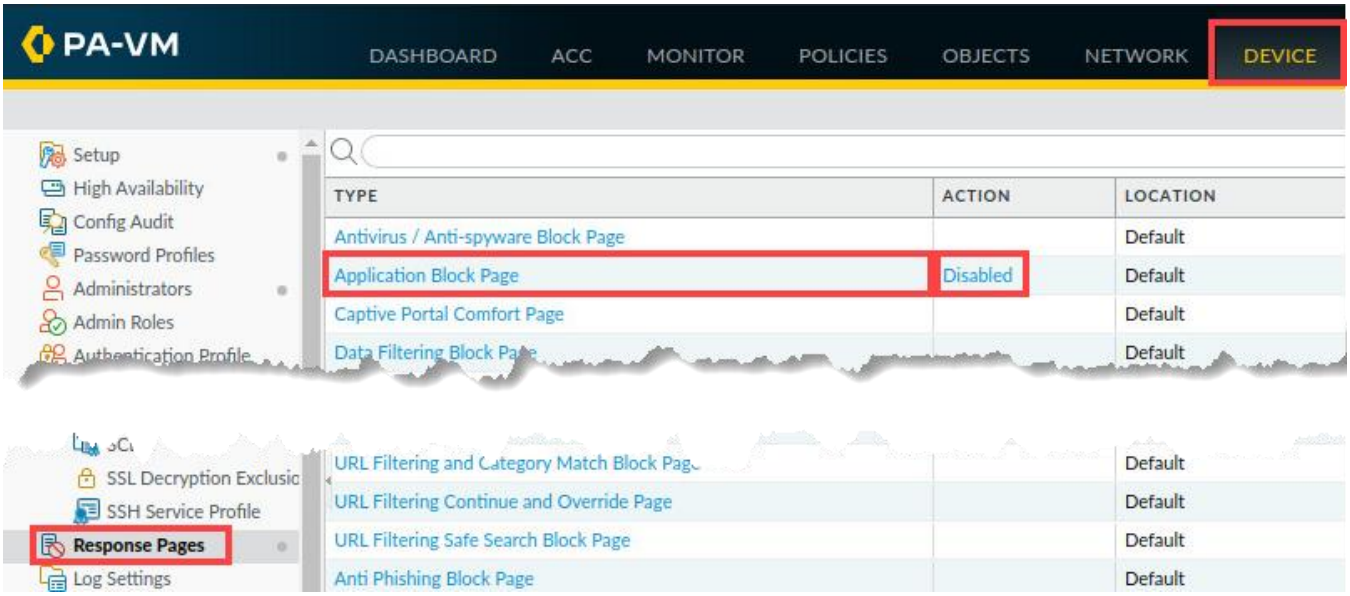

17. Leave the firewall open and continue to the next task.

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

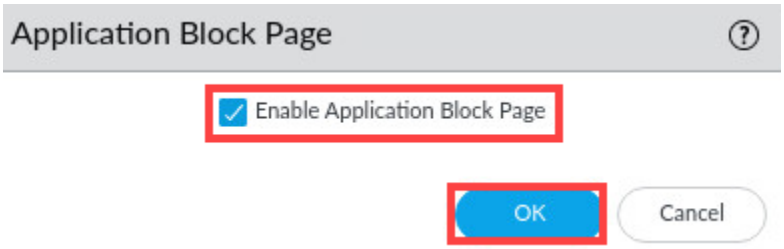
Now you will configure a URL Filtering Profile to control access to URLs. You must add the URL Filtering Profile to a security policy rule with an “allow” action. The use of a URL Filtering Profile to block access to URLs typically is easier to maintain over time compared to the addition of URLs to a 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.

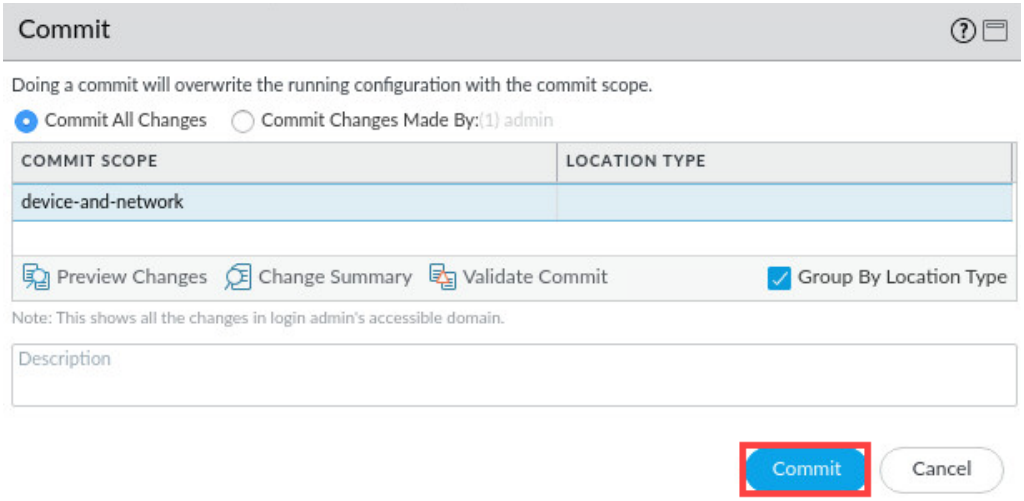



2. In the *Application Block Page* window, place a **check** in the box for **Enable Application Block Page**. Click **OK.**

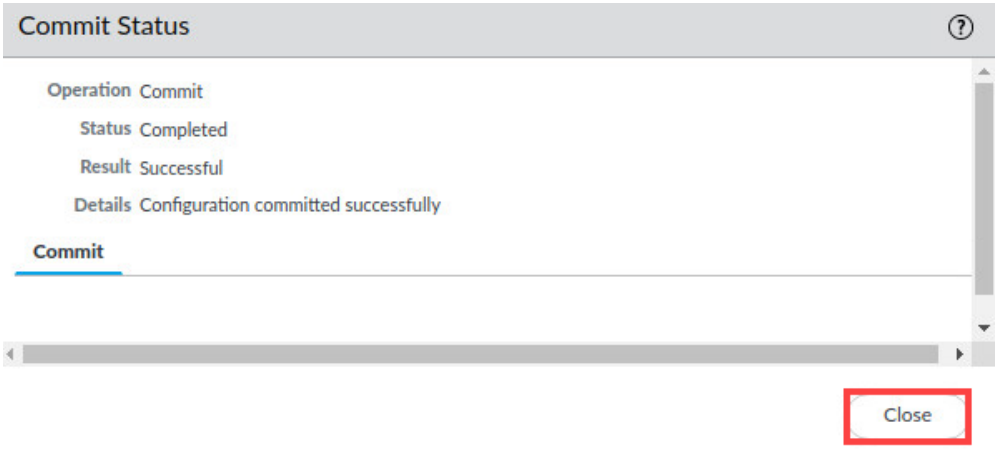



3. Click the **Commit** button at the upper-right of the web interface.

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

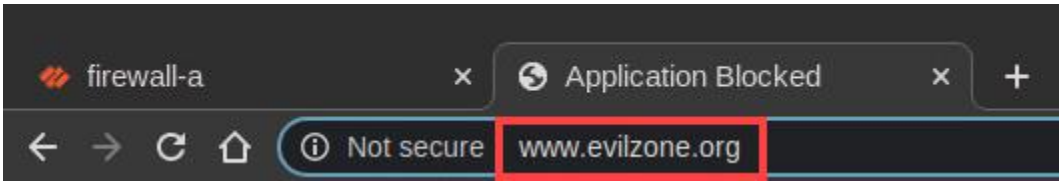



5. Wait until the *Commit* process is complete. Click **Close**.

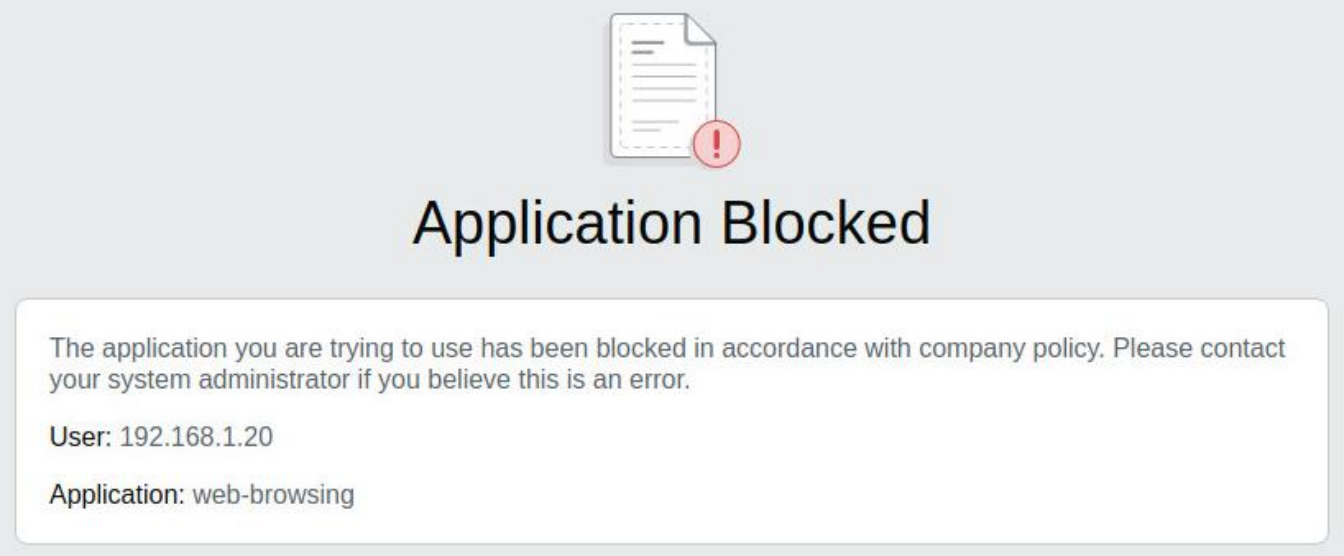



6. Test the *Application Block Page* response. Open a new tab in **Chromium**.


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



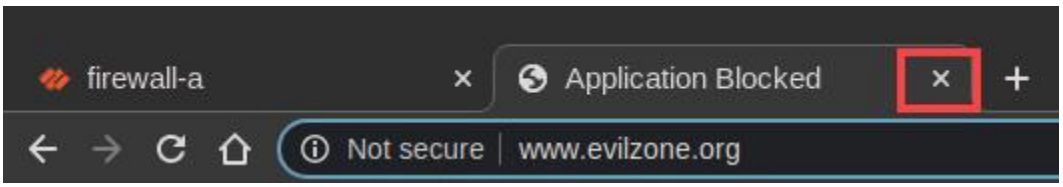
8. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage.



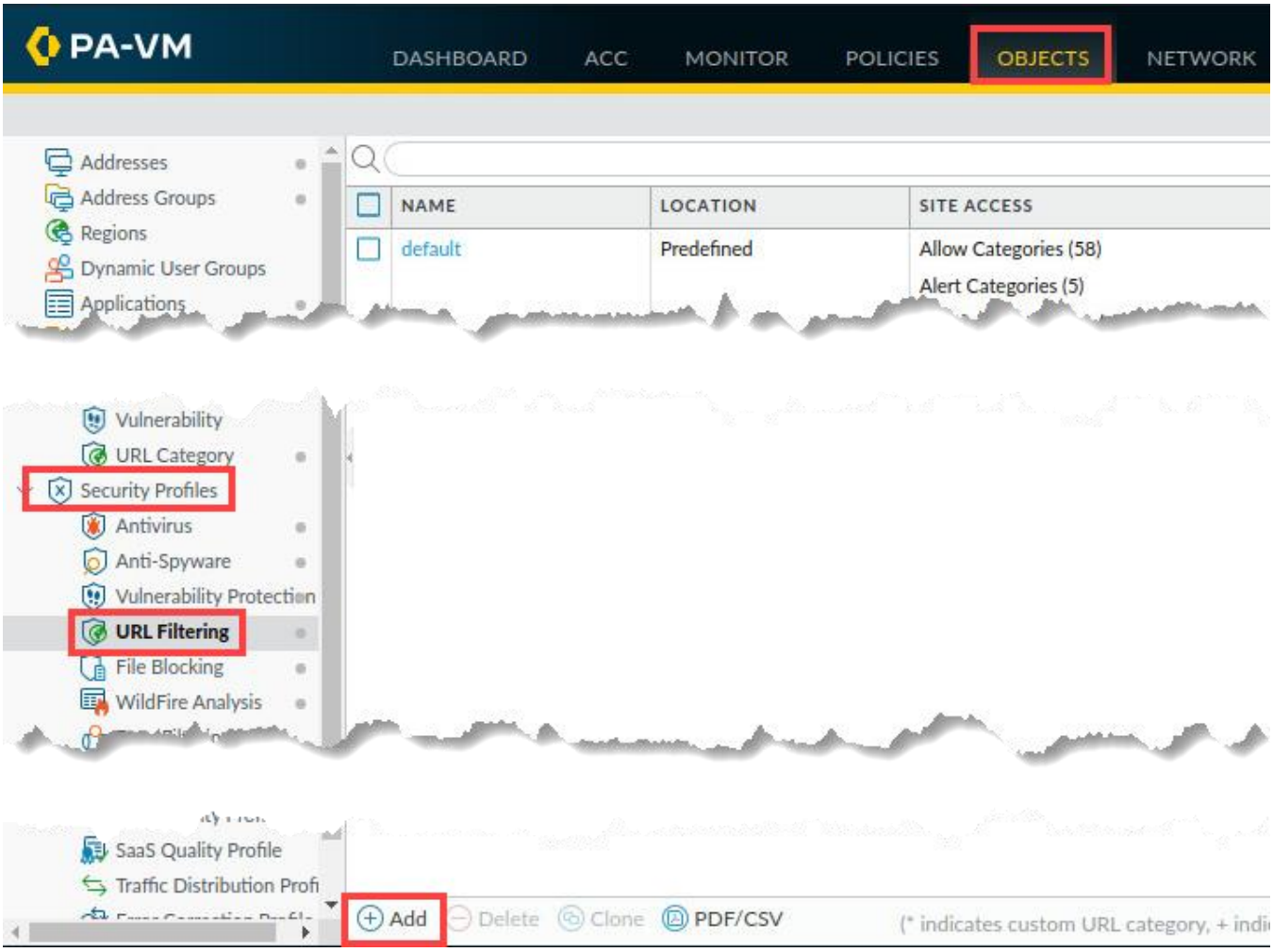

Please Note

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.

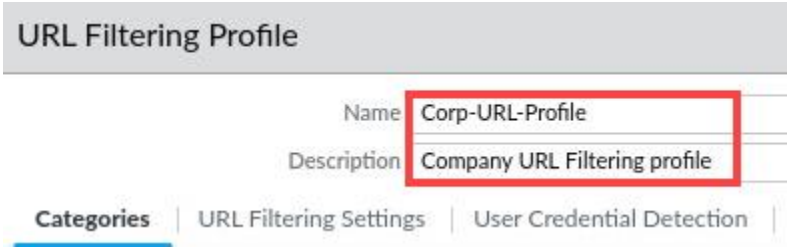
9. Close the *evilzone.org* tab by clicking the **X** icon.



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

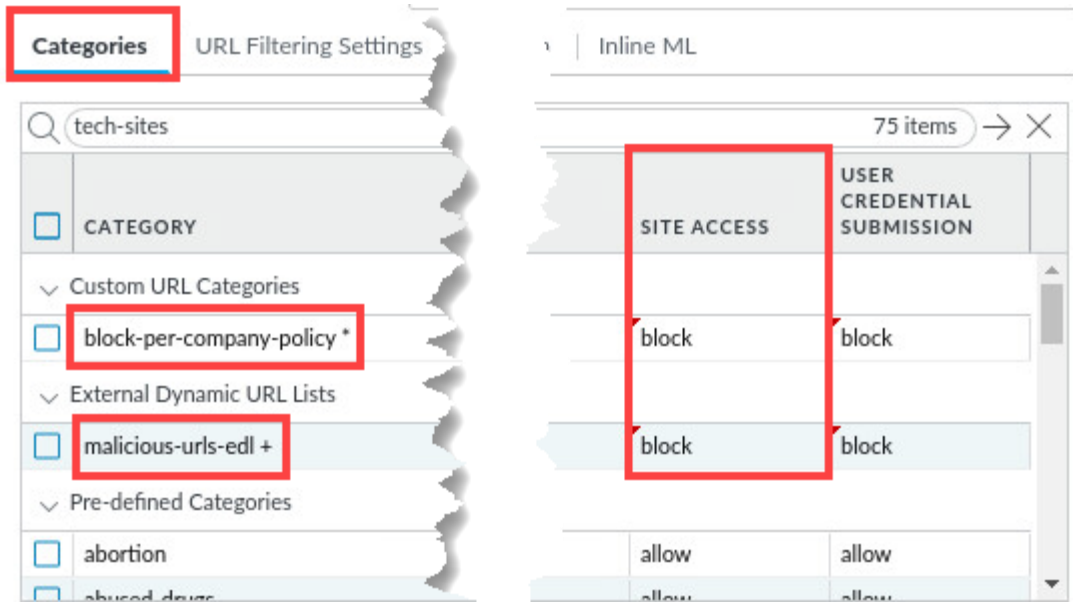



11. In the *URL Filtering Profile*, type **`Corp-URL-Profile`** as the *Name* of the profile. For *Description*, enter **`Company URL Filtering profile`**.



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.

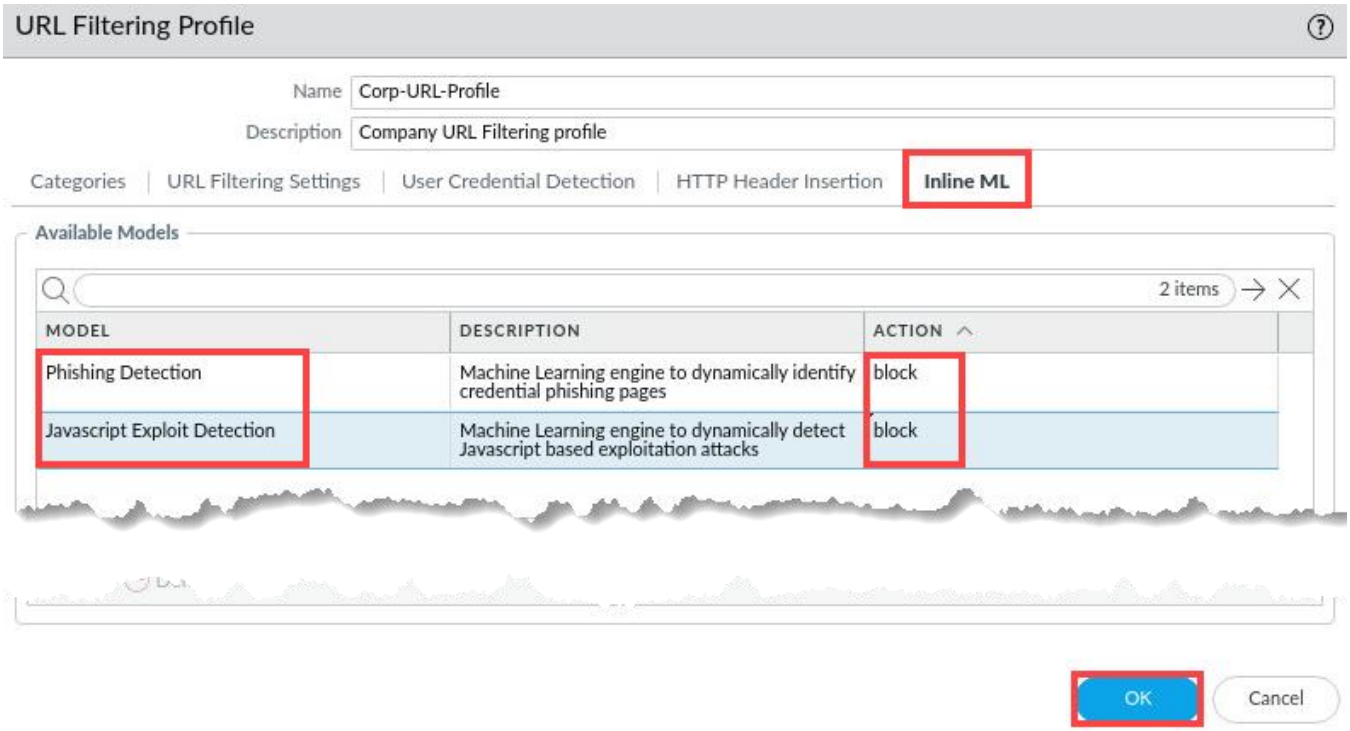
| Parameter | Value |
|---|---|
| **Site Access** | Configure the **block** action for the following URL categories:<br>**block-per-company-policy*** (your Custom URL Category)<br>**malicious-urls-edl+** (your custom URL list)<br>**adult**<br>**command-and-control**<br>**extremism**<br>**hacking**<br>**high-risk**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



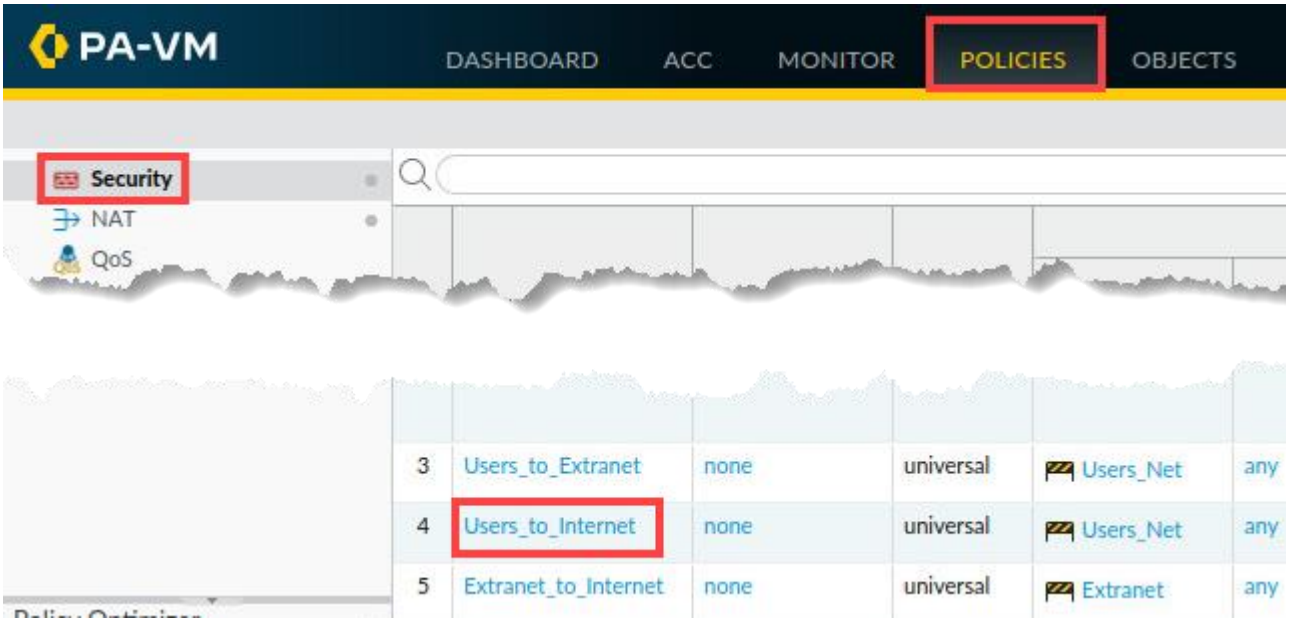

Please Note

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**.

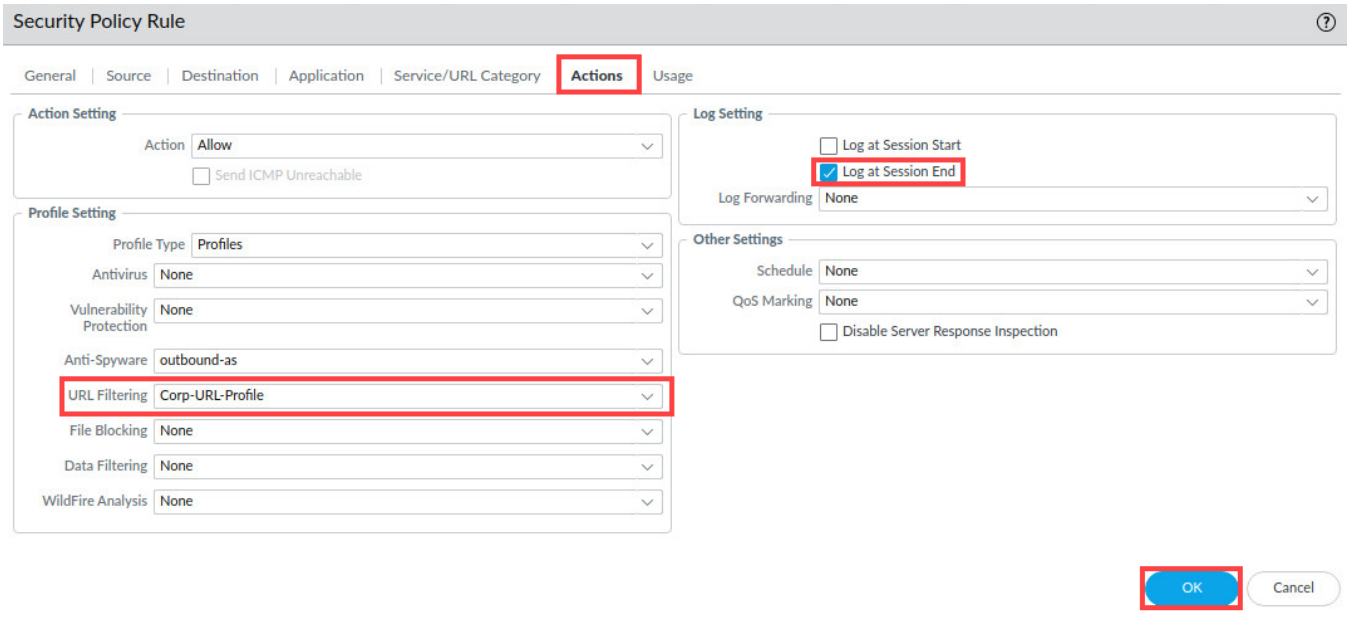



14. In the web interface, select **Policies > Security.** Click **Users_to_Internet** to edit the rule.

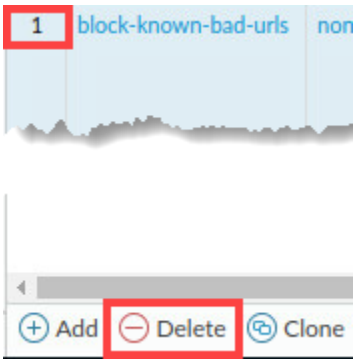


15. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Click **OK**.

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



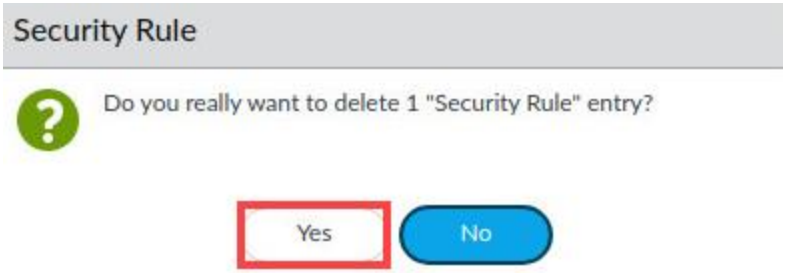

16. Select, but do not open the *block-known-bad-urls* security policy rule. Click **Delete** to remove the *block-known-bad-urls* rule.




Please Note

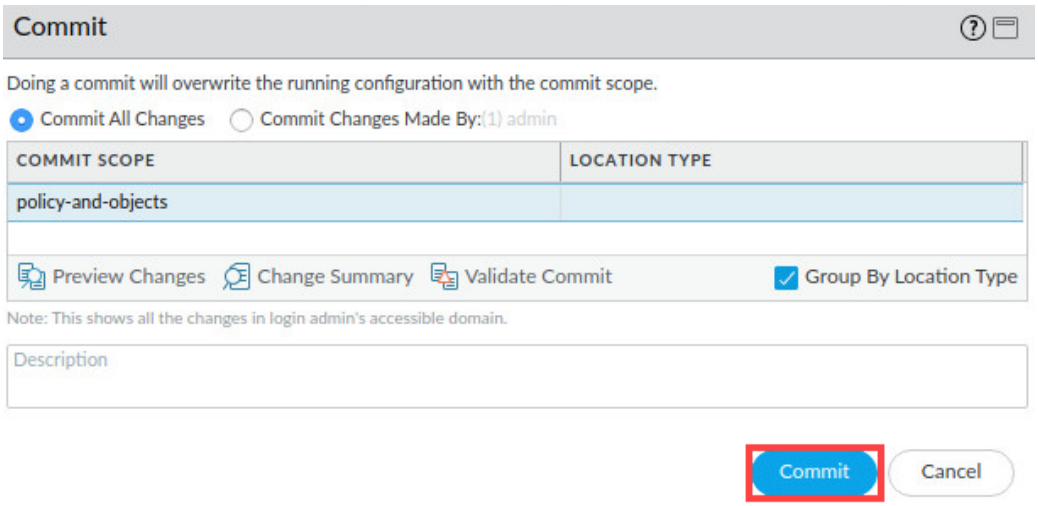
This rule no longer will be used to block access to the URLs. Instead, the "Users_to_Internet" rule with its attached URL Filtering Profile will control URL access.

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

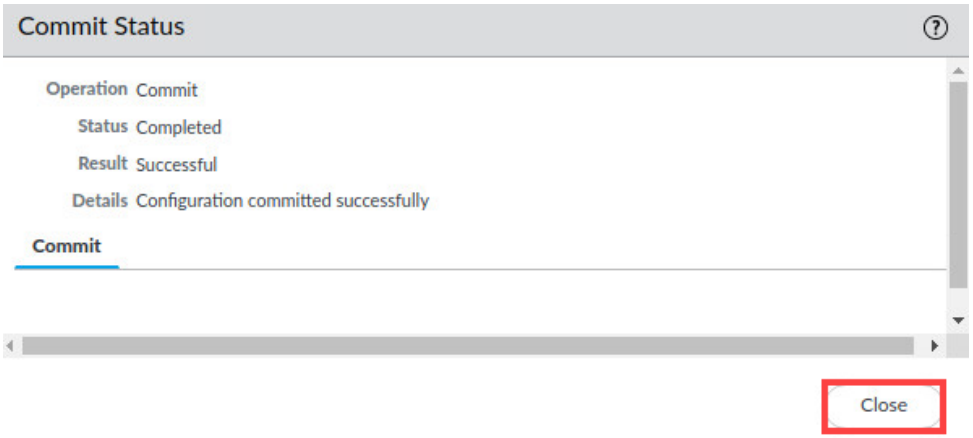



18. Click the **Commit** button at the upper-right of the web interface.


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

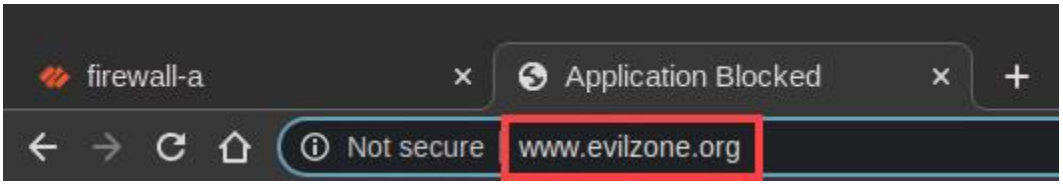



20. Wait until the *Commit* process is complete. Click **Close**.

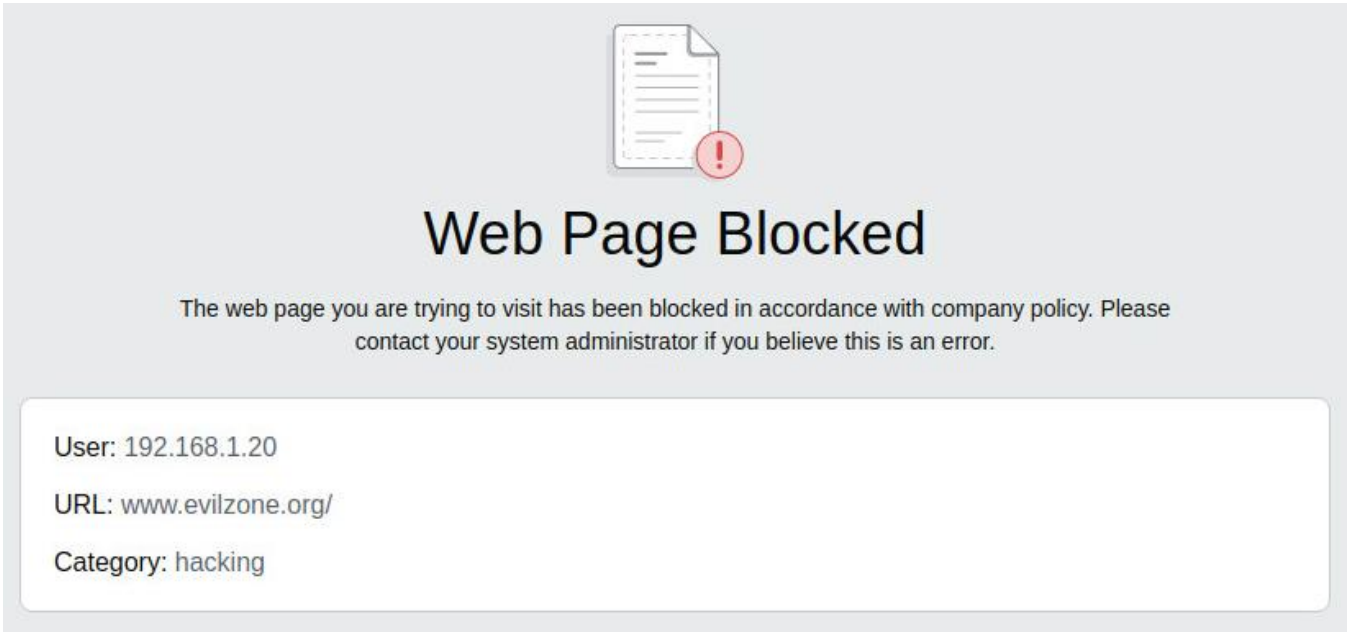


21. Test the *Application Block Page* response. Open a new tab in **Chromium**.


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



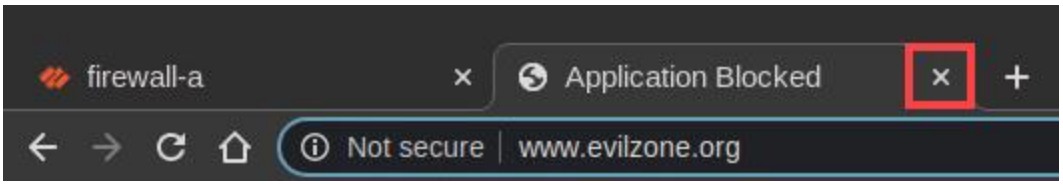

23. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage. If the *Web Page Blocked* message does not appear, allow 1 to 3 minutes for the firewall to process the changes, then refresh the *evilzone.org* tab.




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**.


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