



## PALO ALTO NETWORKS EDU 210

### Lab 7: Blocking Threats from Known-Bad Sources

Document Version: **2022-08-29**

Copyright © 2022 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

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

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

## Contents

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

## Introduction

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

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

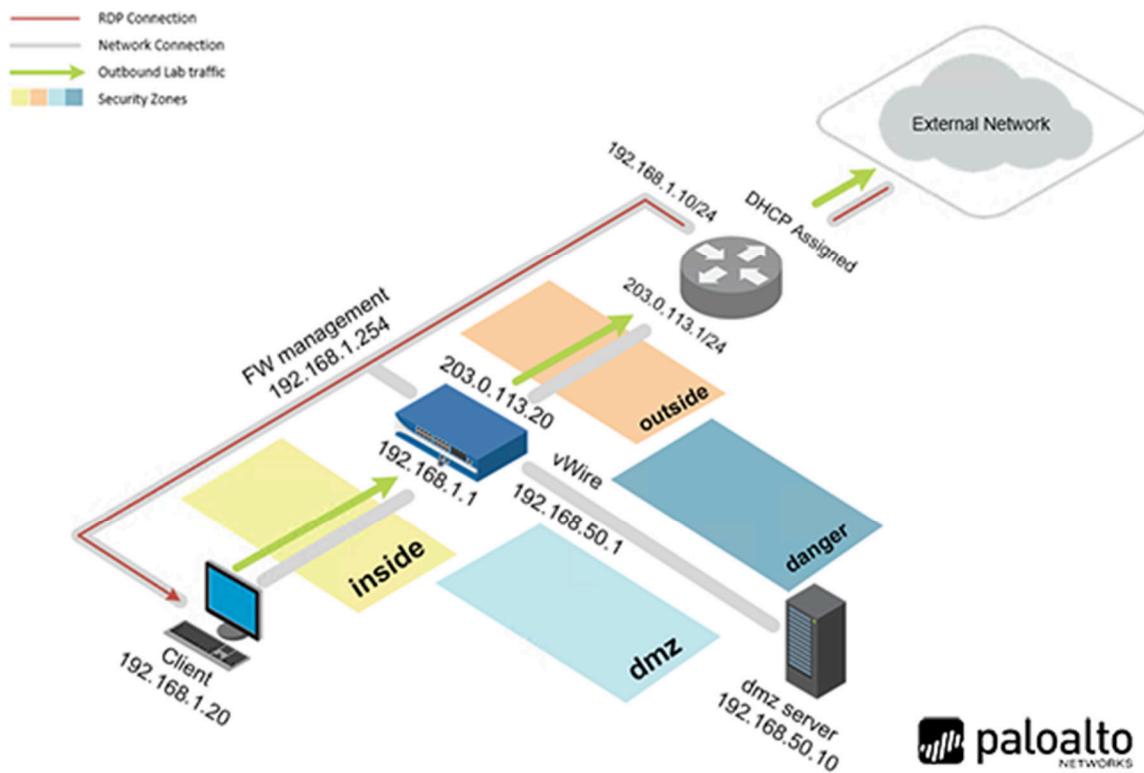
In this section, you will explore the options available on the firewall that allow you to block individual addresses, groups of addresses, and lists of addresses. You will also configure the firewall to block certain categories of websites.

## Objective

In this lab, you will perform the following tasks:

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

## Lab 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.

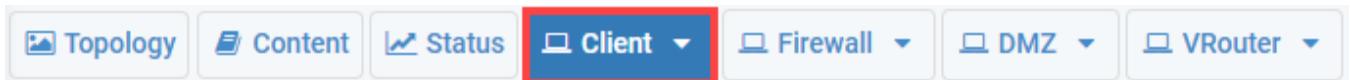
| Virtual Machine | IP Address    | Account<br>(if needed) | Password<br>(if needed) |
|-----------------|---------------|------------------------|-------------------------|
| Client          | 192.168.1.20  | lab-user               | <b>Pa10Alt0!</b>        |
| DMZ             | 192.168.50.10 | root                   | <b>Pa10Alt0!</b>        |
| Firewall        | 192.168.1.254 | admin                  | <b>Pa10Alt0!</b>        |
| VRouter         | 192.168.1.10  | root                   | <b>Pa10Alt0!</b>        |

## 7 Block Threats from Known-Bad Sources

### 7.1 Apply a Baseline Configuration to the Firewall

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

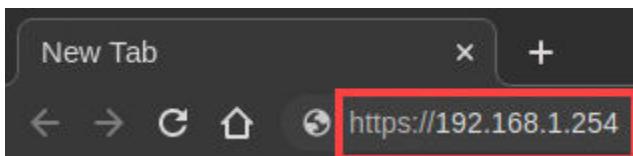
1. Click on the **Client** tab to access the *Client PC*.



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



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



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



Your connection is not private

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

NET::ERR\_CERT\_AUTHORITY\_INVALID

[Advanced](#)

[Back to safety](#)



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

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



## Your connection is not private

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

NET::ERR\_CERT\_AUTHORITY\_INVALID

[Hide advanced](#)

[Back to safety](#)

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

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

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



The screenshot shows a login interface for a Palo Alto Networks device. The page has a yellow border. At the top is the Palo Alto Networks logo. Below it is a form with two input fields: one for the username 'admin' and one for the password, which is currently redacted with dots. At the bottom is a blue 'Log In' button. All three elements—the input fields and the button—are highlighted with red boxes.

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.

The screenshot shows the PA-VM web interface with the following navigation path: PA-VM > DEVICE > Setup > Operations. The 'Operations' tab is selected. Under the 'Configuration Management' section, there is a 'Load' dropdown menu. The 'Load named configuration snapshot' option is highlighted with a red box.

Management Operations Services Interfaces Telemetry Content-ID WildFire Session

Configuration Management

Revert: [Revert to last saved configuration](#)  
[Revert to running configuration](#)

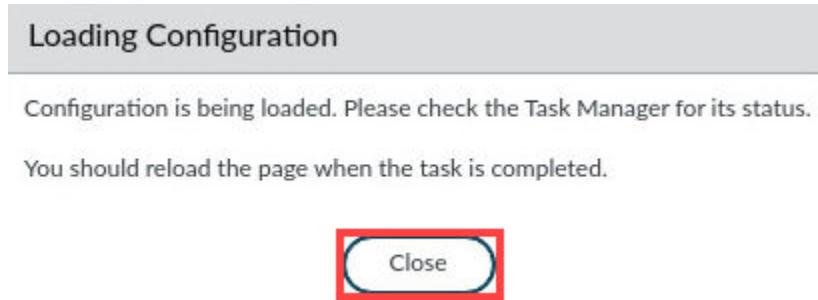
Save: [Save named configuration snapshot](#)  
[Save candidate configuration](#)

Load: **Load named configuration snapshot** [Load configuration version](#)

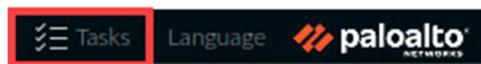
9. In the *Load Named Configuration* window, select **edu-210-lab-07.xml** from the *Name* dropdown box and click **OK**.



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**.

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

Show **All Tasks** Clear Commit Queue **Close**

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



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

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

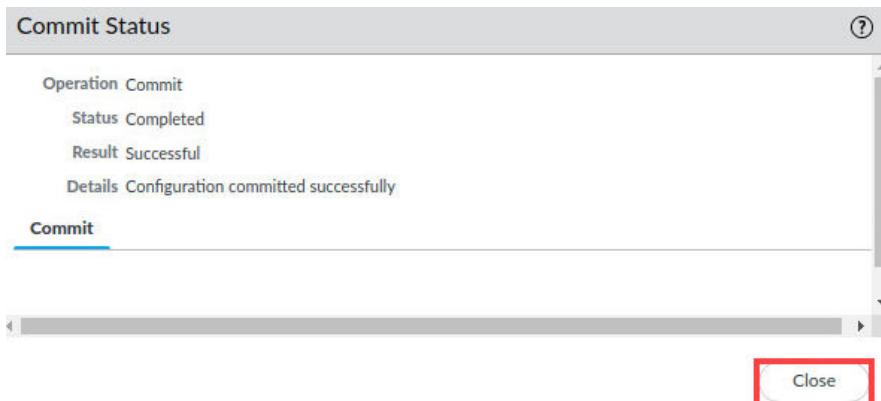
**Preview Changes** **Change Summary** **Validate Commit**  Group By Location Type

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

Description

**Commit** **Cancel**

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



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

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

## 7.2 Test Access to Known Malicious IP Addresses

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

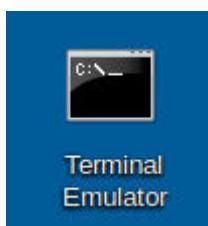
Please Note

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

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



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



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

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

```
Terminal  
C:\home\lab-user\Desktop\Lab-Files> nslookup 2600.org  
;; Got recursion not available from 192.168.50.53, trying next server  
Server:      1.1.1.1  
Address:     1.1.1.1#53  
  
Non-authoritative answer:  
Name:   2600.org  
Address: 166.84.5.162  
;; Got recursion not available from 192.168.50.53, trying next server  
C:\home\lab-user\Desktop\Lab-Files>
```

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

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

```
C:\home\lab-user\Desktop\Lab-Files> nslookup www.breakthesecurity.com  
;; Got recursion not available from 192.168.50.53, trying next server  
Server:      1.1.1.1  
Address:     1.1.1.1#53  
  
Non-authoritative answer:  
Name:   www.breakthesecurity.com  
Address: 162.255.119.249  
;; Got recursion not available from 192.168.50.53, trying next server  
C:\home\lab-user\Desktop\Lab-Files>
```

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

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

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

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

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

Please  
Note

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

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



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



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

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

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

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

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

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. Under the 'Addresses' tab, there is a search bar and a table with columns for NAME, LOCATION, and TYPE. Below the table, there is a dropdown menu for 'PA-VM / Local Profile' containing options like Path Quality Profile, SaaS Quality Profile, Traffic Distribution Profile, and Error Correction Profile. At the bottom of the screen, there are buttons for '+ Add', 'Delete', 'Clone', and 'PDF/CSV'.

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

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

Address

Name: malicious-ip-address-1

Description: 2600.org IP address

Type: IP Netmask

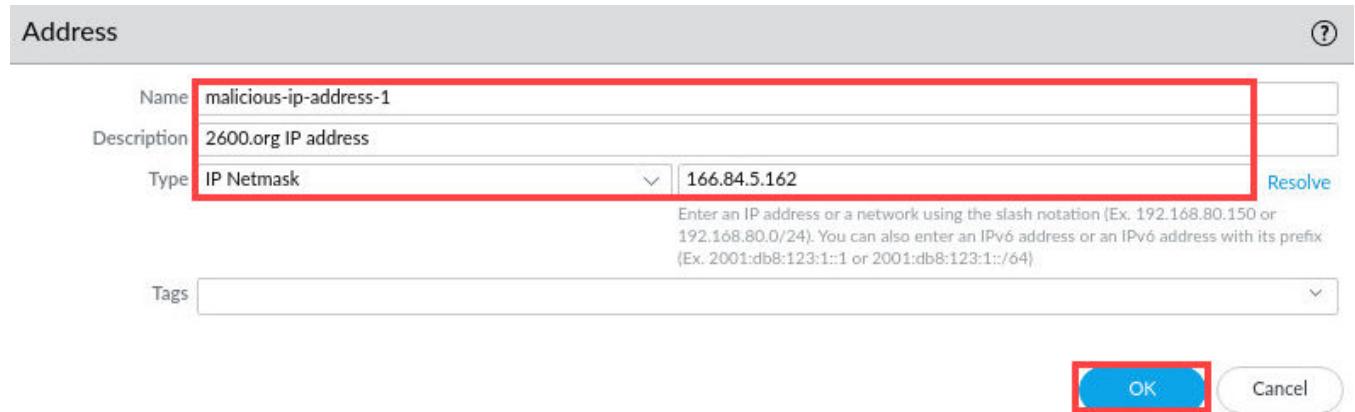
166.84.5.162

Resolve

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

Tags

OK Cancel



Please Note

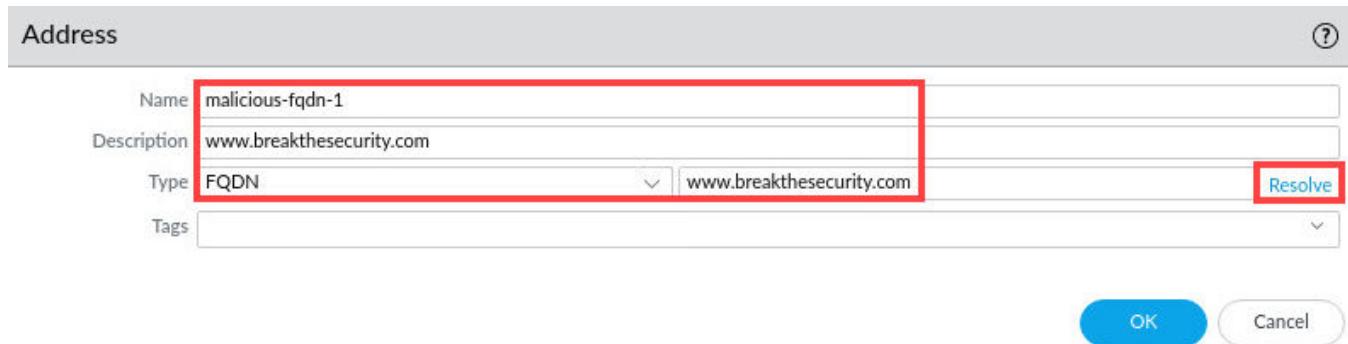
Note that the IP address you enter may be different from the previous example.

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

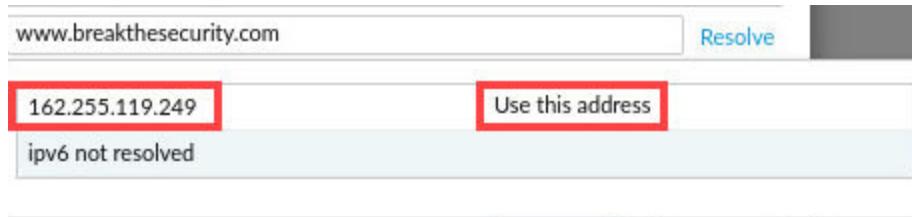


4. In the *Address* window, configure the following. Click **Resolve**.

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



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.

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

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

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

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**.

| General     |   | Source | Destination | Application | Service/URL Category | Actions |
|-------------|---|--------|-------------|-------------|----------------------|---------|
| Name        | block-known-Bad-IPs                         |        |             |             |                      |         |
| Rule Type   | universal (default)                         |        |             |             |                      |         |
| Description | Blocks traffic to malicious address objects |        |             |             |                      |         |

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

| Parameter      | Value                                    |
|----------------|--|
| Source Zone    | Add <b>Users_Net</b> and <b>Extranet</b> |
| Source Address | <b>Any</b>                               |

**Security Policy Rule**

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

Any

SOURCE ZONE ^

- Users\_Net**
- Extranet**

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

Any

SOURCE ADDRESS ^

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

Negate

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

| Parameter           | Value   |
|---------------------|---|
| Destination Zone    | Add <b>Internet</b>   |
| Destination Address | Add <b>malicious-fqdn-1</b> and <b>malicious-ip-address-1</b> |

**Security Policy Rule**

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

select

DESTINATION ZONE ^

- Internet**

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

Any

DESTINATION ADDRESS ^

- malicious-fqdn-1**
- malicious-ip-address-1**

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

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

The screenshot shows the 'Security Policy Rule' configuration interface. The top navigation bar has tabs: General, Source, Destination, Application (which is highlighted with a red box), Service/URL Category, and Actions. Below the tabs, there is a section for selecting applications. A checkbox labeled 'Any' is checked and highlighted with a red box. Below it is a dropdown menu labeled 'APPLICATIONS' with an upward arrow icon.

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

The screenshot shows the 'Security Policy Rule' configuration interface. The top navigation bar has tabs: General, Source, Destination, Application, Service/URL Category (which is highlighted with a red box), and Actions. Below the tabs, there is a section for selecting service URL categories. A dropdown menu labeled 'application-default' is selected and highlighted with a red box. To the right, there is another section for selecting URL categories, which also has a 'Any' checkbox checked and highlighted with a red box. Below these sections are dropdown menus labeled 'SERVICE' and 'URL CATEGORY' with upward arrow icons.

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

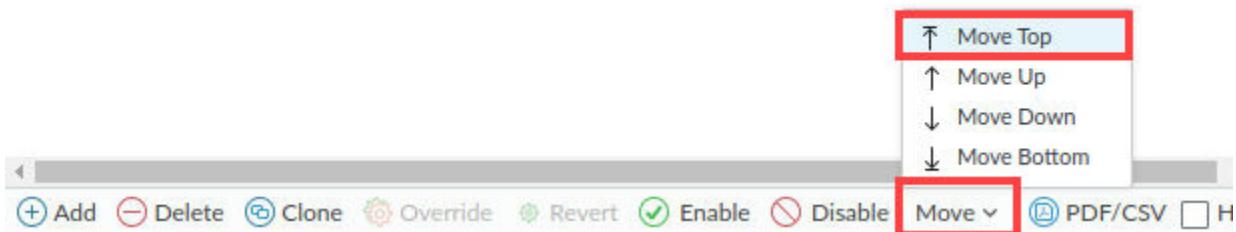
| Parameter   | Value              |
|-------------|--------------------|
| Action      | Deny               |
| Log Setting | Log at Session End |

The screenshot shows the 'Security Policy Rule' configuration interface. The top navigation bar has tabs: General, Source, Destination, Application, Service/URL Category, and Actions (which is highlighted with a red box). Below the tabs, there are several configuration sections. In the 'Action Setting' section, the 'Action' dropdown is set to 'Deny' and highlighted with a red box. In the 'Log Setting' section, the 'Log at Session End' checkbox is checked and highlighted with a red box. In the bottom right corner, there are 'OK' and 'Cancel' buttons, with the 'OK' button highlighted with a red box.

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

|   | NAME                 | TAGS | TYPE      | 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  | any     |
|   |                      |      |           | Users_Net |         |
| 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.



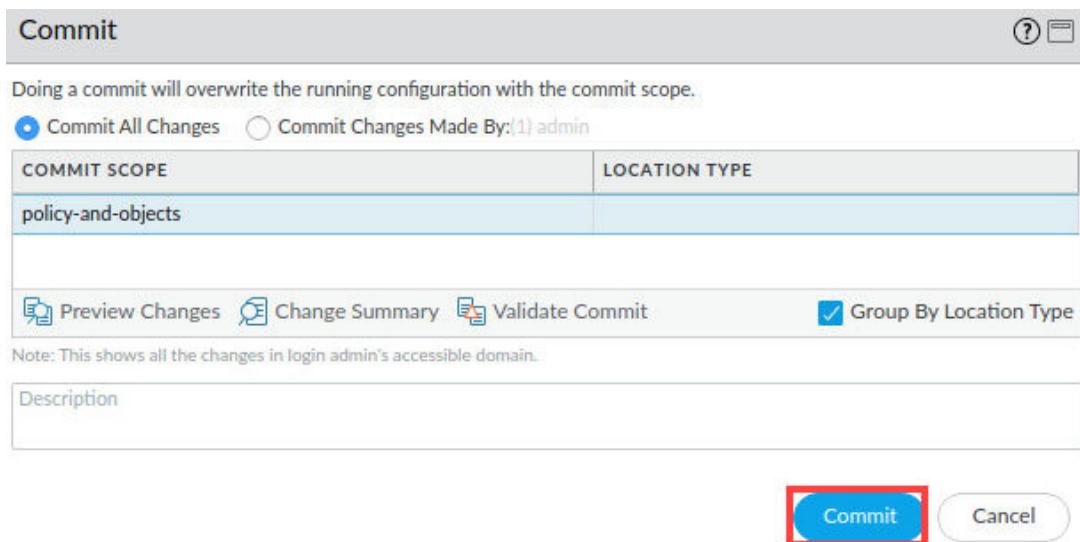
17. Verify that the **Block-Known-Bad-IPs** rule is rule number 1.

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

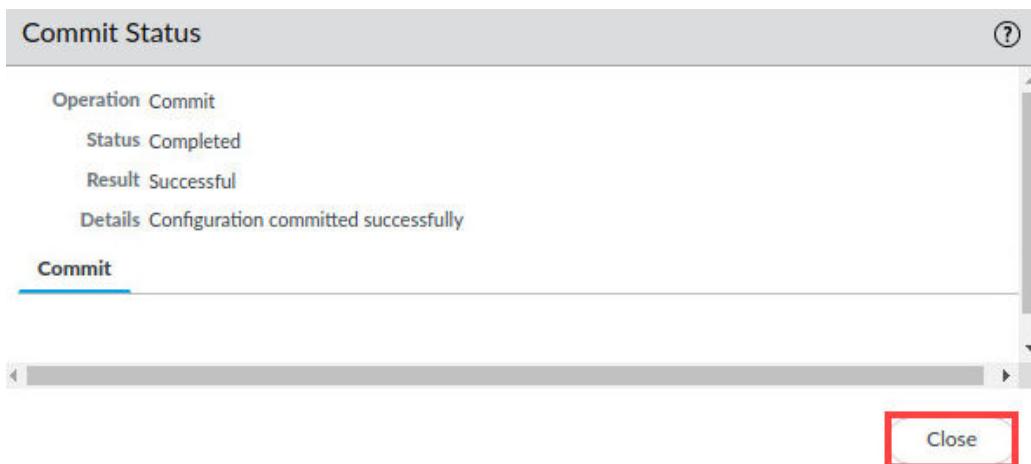
18. Click the **Commit** button at the upper-right of the web interface.



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



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



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



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



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

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

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

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

Please  
Note

Pinging 2600.org will fail.

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

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

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

Please  
Note

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

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



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



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

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

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.

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

The screenshot shows the PA-VM firewall interface. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted with a red box), and NETWORK. On the left, there's a sidebar with icons for Addresses, Address Groups (which is selected and highlighted with a red box), Regions, Dynamic User Groups, and Applications. Below the sidebar is a search bar and a table with columns for NAME, LOCATION, and MEM. At the bottom of the page, there's a toolbar with icons for Decryption, SD-WAN Link Management, Path Quality Profile, SaaS Quality Profile, Traffic Distribution Profile, and Firewall Configuration Profile. A red box highlights the '+ Add' button in the bottom right corner of the main content area.

- 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 |

The screenshot shows the 'Address Group' configuration dialog. It has fields for Name (Malicious-IP-Group), Description (Contains malicious IP Address Objects), Type (Static), and Addresses. Under Addresses, there's a list with 'malicious-fqdn-1' and 'malicious-ip-address-1'. The 'malicious-ip-address-1' entry is checked. The bottom toolbar has 'Browse', '+ Add' (highlighted with a red box), and 'Delete' buttons. The 'OK' button is highlighted with a red box at the bottom right.

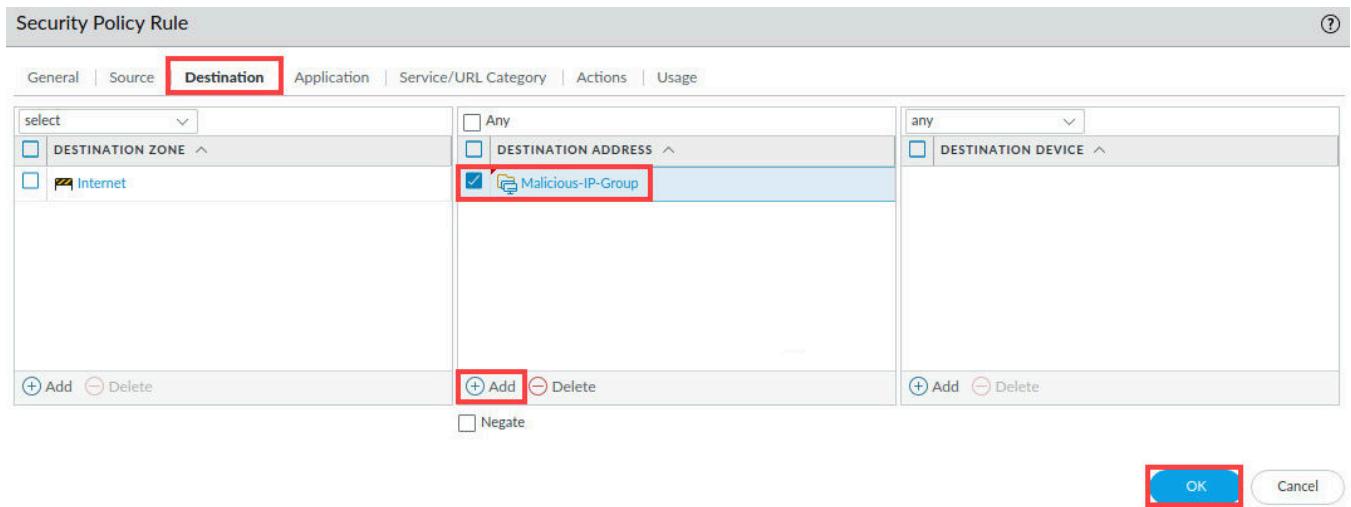
3. Select **Policies > Security**. Click **Block-Known-Bad-IPs** to edit the rule.

| NAME                  | TAGS | TYPE      | ZONE                  |
|-----------------------|------|-----------|-----------------------|
| 1 Block-known-Bad-IPs | none | universal | Extranet<br>Users_Net |
| 2 Users_to_Extranet   | none | universal | Users_Net             |

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

| DESTINATION ZONE | DESTINATION ADDRESS  |
|------------------|--|
| Internet         | <input checked="" type="checkbox"/> malicious-fqdn-1<br><input checked="" type="checkbox"/> malicious-ip-address-1 |

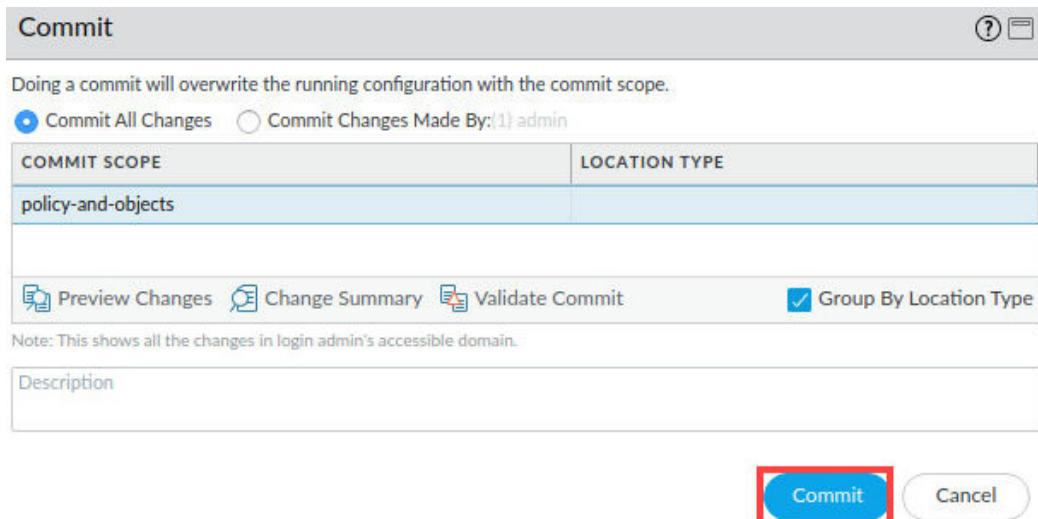
5. In the *Destination Address* window, click **Add**. Select **Malicious-IP-Group**. Click **OK**.



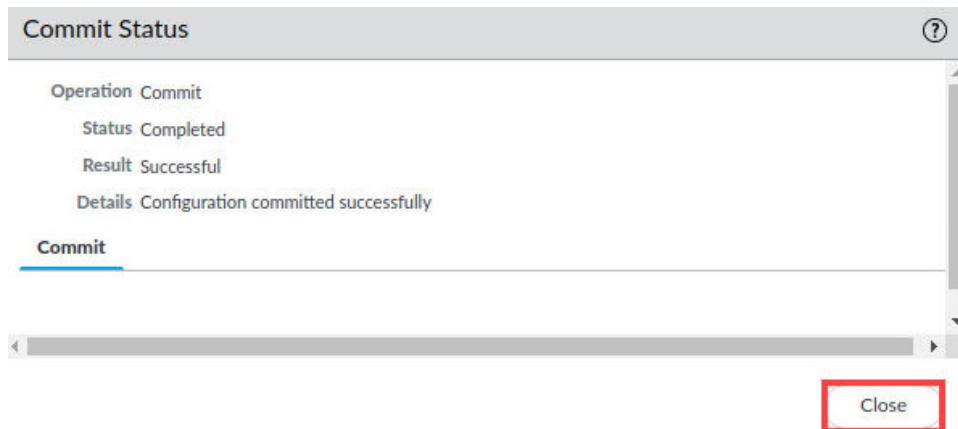
6. Click the **Commit** button at the upper-right of the web interface.



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>
```

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

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

Please  
Note

Pinging 2600.org will fail.

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

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

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

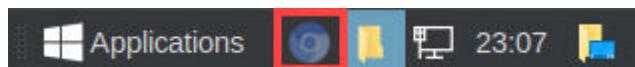
**Please Note**

Pinging `www.breakthesecurity` 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.

 A screenshot of the Palo Alto Networks PA-VM interface. The 'MONITOR' tab is selected. In the left sidebar, 'Logs' is expanded, and 'Traffic' is selected, both with red boxes around them. The main area shows a table of logs with the following columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, DESTINATION, TO PORT, APPLICATION, ACTION, RULE, and SESSION END REASON. There are four rows of data, all of which are highlighted with red boxes:
 

| RECEIVE TIME   | TYPE | FROM ZONE | TO ZONE  | SOURCE       | DESTINATION     | TO PORT | APPLICATION | ACTION | RULE                | SESSION END REASON |
|----------------|------|-----------|----------|--------------|-----------------|---------|-------------|--------|---------------------|--------------------|
| 08/08 18:48    | drop | Users_Net | Internet | 192.168.1.20 | 162.255.119.249 | 0       | ping        | deny   | Block-known-Bad-IPs | policy-deny        |
| 08/08 18:37    | drop | Users_Net | Internet | 192.168.1.20 | 166.84.5.162    | 0       | ping        | deny   | Block-known-Bad-IPs | policy-deny        |
| 08/08 17:51:41 | drop | Users_Net | Internet | 192.168.1.20 | 162.255.119.249 | 0       | ping        | deny   | Block-known-Bad-IPs | policy-deny        |
| 08/08 17:51:17 | drop | Users_Net | Internet | 192.168.1.20 | 162.255.119.249 | 0       | ping        | deny   | Block-known-Bad-IPs | policy-deny        |

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

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

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

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

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



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



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

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

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

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

Please  
Note

The nic.ir domain is in Iran.

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.



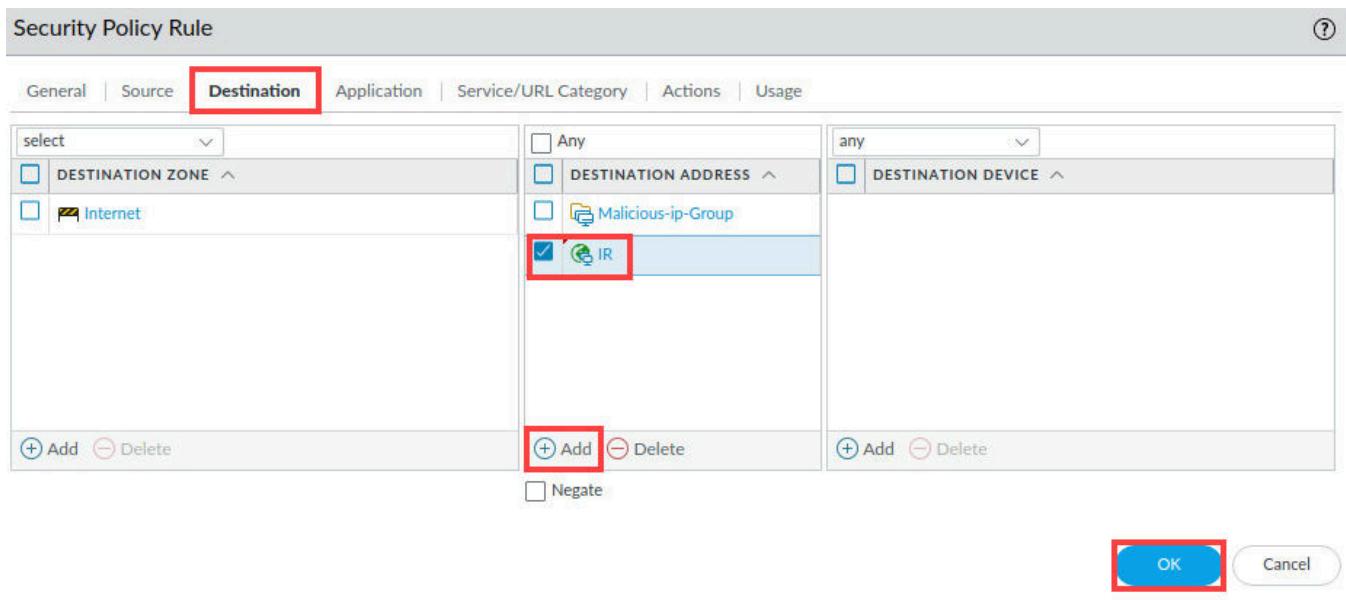
6. If you minimized the *Firewall*, reopen the *Firewall* interface by clicking on the **Chromium** tab in the taskbar.



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

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

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



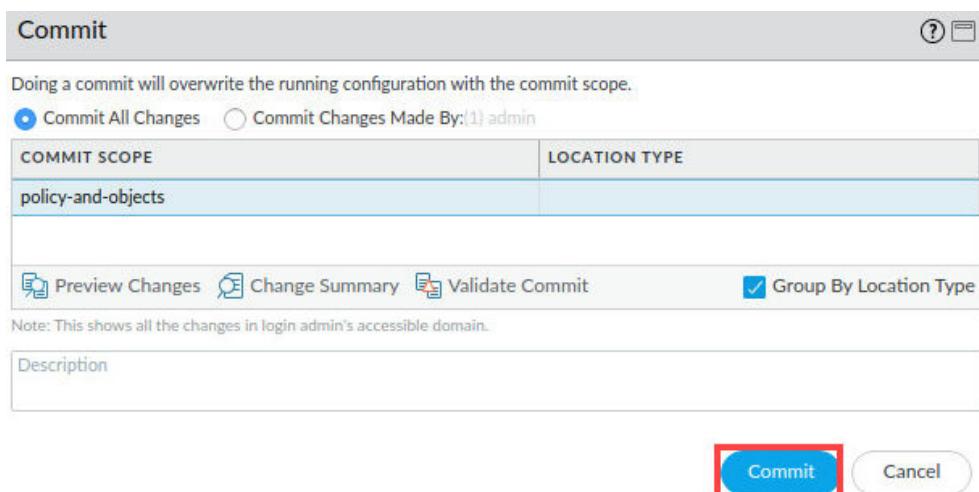
**Please Note**

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

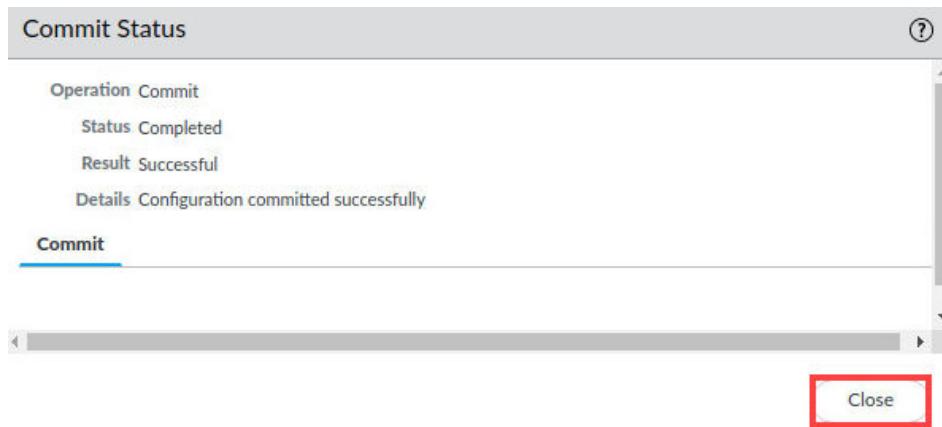
16. Click the **Commit** button at the upper-right of the web interface.



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>
```

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

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

Please  
Note

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

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



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



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

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

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

## 7.6 Block Access to Malicious IP Addresses Using EDLs

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

- 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**.

The screenshot shows the 'External Dynamic Lists' page in the Palo Alto VM firewall interface. The 'OBJECTS' tab is highlighted. On the left, a sidebar lists various object types, with 'External Dynamic Lists' selected and highlighted by a red box. The main area displays a table of predefined dynamic IP lists:

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

Please  
Note

Palo Alto Networks maintains and provides these lists.

- Read the description of the list.

The screenshot shows the 'External Dynamic Lists (Read Only)' dialog box. The 'List Entries And Exceptions' tab is selected. The form fields include:

- Name: Palo Alto Networks - High risk IP addresses
- Type: Predefined IP List
- Description: IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.
- Source: Palo Alto Networks - High risk IP addresses
- Server Authentication: (empty field)

At the bottom are 'OK' and 'Cancel' buttons.

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**.

The screenshot shows the 'External Dynamic Lists (Read Only)' interface. The 'Name' field is set to 'Palo Alto Networks - High risk IP addresses'. The 'List Entries And Exceptions' tab is selected. In the 'List Entries' section, there is a search bar and a table with 312 items. The first three entries (IP addresses) are highlighted with a red box: 89.37.192.194, 80.211.52.246, and 185.232.64.32. The 'Manual Exceptions' section has a search bar and a table with 0 items. At the bottom, there are 'OK' and 'Cancel' buttons, with 'Cancel' highlighted by a red box.

**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            | <a href="http://192.168.50.80/malicious-ips.txt">http://192.168.50.80/malicious-ips.txt</a><br>(The EDL contains only the IP address 192.168.50.11.) |
| Check for updates | Five Minute  |

External Dynamic Lists

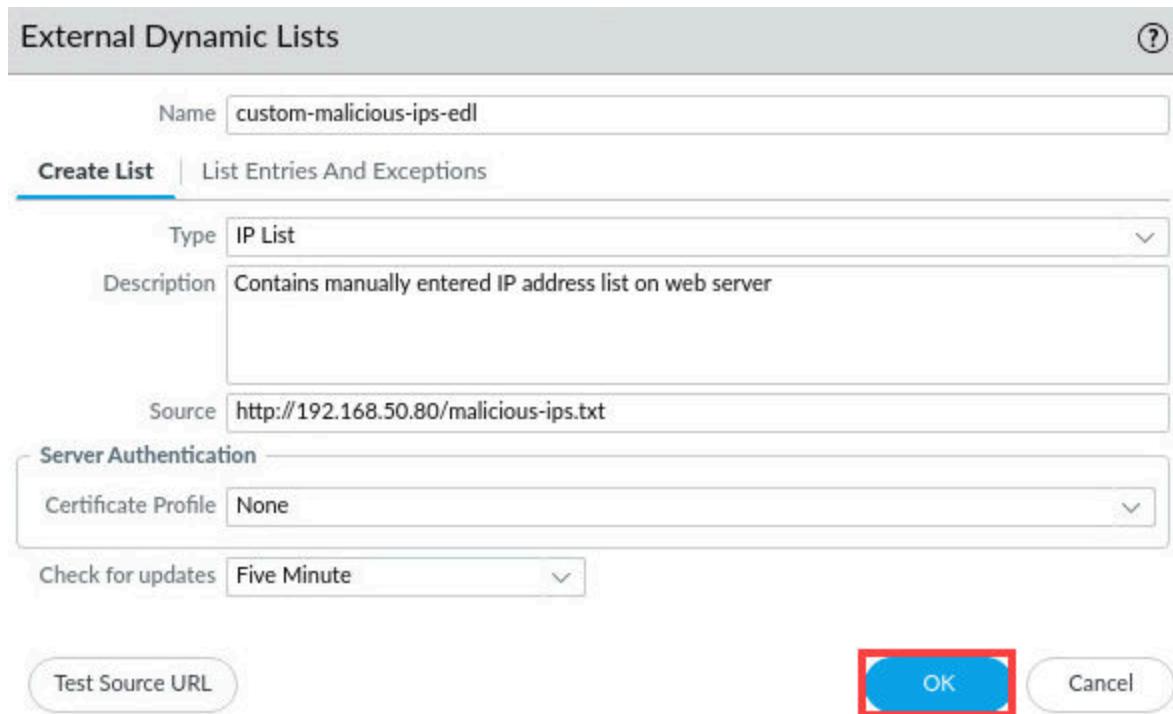
|   |   |
|---|---|
| Name  | custom-malicious-ips-edl  |
| <a href="#">Create List</a>   <a href="#">List Entries And Exceptions</a>   |   |
| Type  | IP List   |
| Description   | Contains manually entered IP address list on web server                                     |
| Source  | <a href="http://192.168.50.80/malicious-ips.txt">http://192.168.50.80/malicious-ips.txt</a> |
| <b>Server Authentication</b>  |   |
| Certificate Profile   | None  |
| Check for updates   | Five Minute   |
| <input type="button" value="Test Source URL"/> <span style="float: right;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></span> |   |

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

Test Source URL

Source URL is accessible.

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.

The screenshot shows the PA-VM interface with the 'Policies' tab selected. The 'Security' section is highlighted with a red box. A table lists two policies: 'Block-known-Bad-IPs' and 'Users\_to\_Extranet'. The 'Block-known-Bad-IPs' row is also highlighted with a red box. The columns in the table are NAME, TAGS, TYPE, ZONE, and AD.

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

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

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

Security Policy Rule

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 |
|------------------------|------|-----------|-----------------------|---------|
|                        |      |           | 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 screenshot shows the 'Security Policy Rule' configuration window. The 'Destination' tab is selected. Under 'DESTINATION ZONE', 'Extranet' is selected. Under 'DESTINATION ADDRESS', 'custom-malicious-ips-edl' is selected. A red box highlights the 'Negate' checkbox at the bottom of the destination section. The 'OK' button is also highlighted with a red box.

**Please Note**

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

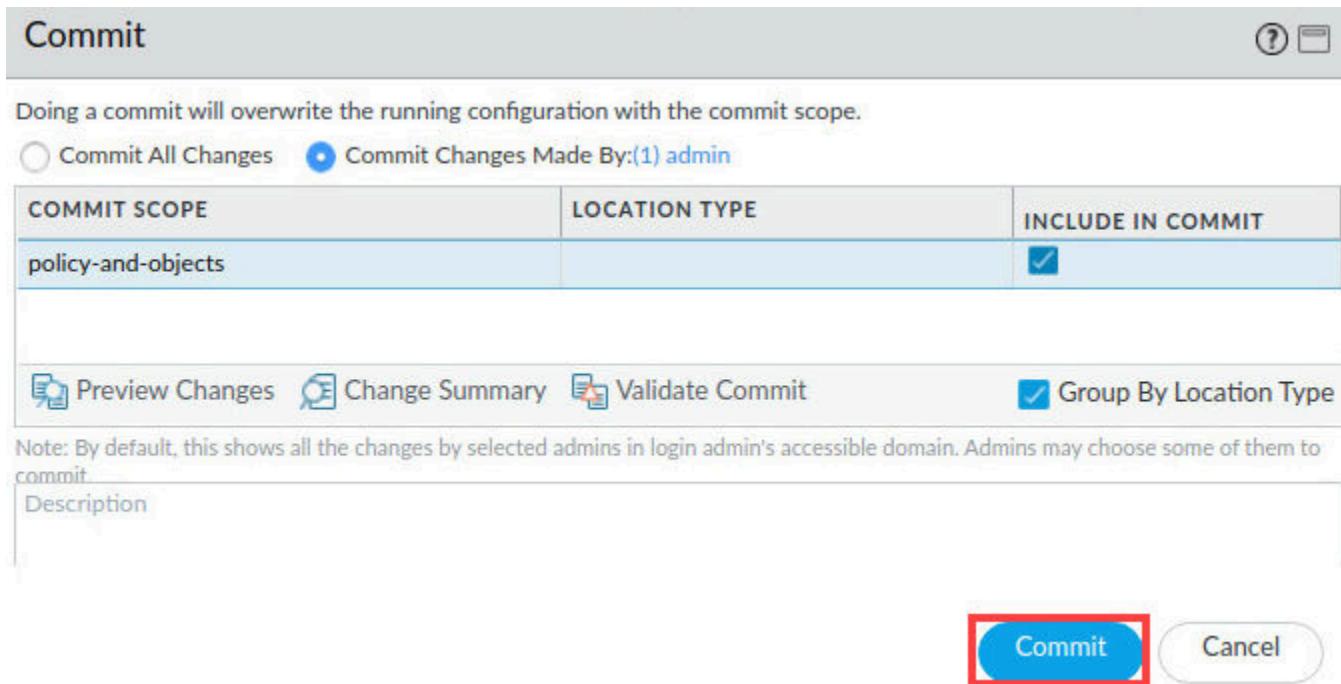
12. Notice in the *Users\_to\_Extranet* rule that *custom-malicious-ips-edl* has a line through it. This line indicates that the **Negate** option has been employed for addresses in the list.

| NAME | TAGS                | TYPE | Source    |   |      |        | Destination |  |
|------|---------------------|------|-----------|---|------|--------|-------------|--|
|      |                     |      | ZONE      | ADDRESS   | USER | DEVICE | ZONE        | ADDRESS  |
| 1    | Block-known-Bad-IPs | none | universal | <input type="checkbox"/> Extranet<br><input type="checkbox"/> Users_Net | any  | any    | any         | <input type="checkbox"/> Internet<br><input checked="" type="checkbox"/> IR<br><input checked="" type="checkbox"/> Malicious-IP-Group<br><input checked="" type="checkbox"/> Palo Alto Networks - Bulletproof IP ...<br><input checked="" type="checkbox"/> Palo Alto Networks - High risk IP ad...<br><input checked="" type="checkbox"/> Palo Alto Networks - Known malicio... |
| 2    | Users_to_Extranet   | none | universal | <input type="checkbox"/> Users_Net                                      | any  | any    | any         | <input type="checkbox"/> Extranet<br><input checked="" type="checkbox"/> custom-malicious-ips-edl  |
| 3    | Users_to_Internet   | none | universal | <input type="checkbox"/> Users_Net                                      | any  | any    | any         | <input type="checkbox"/> Internet<br>any   |

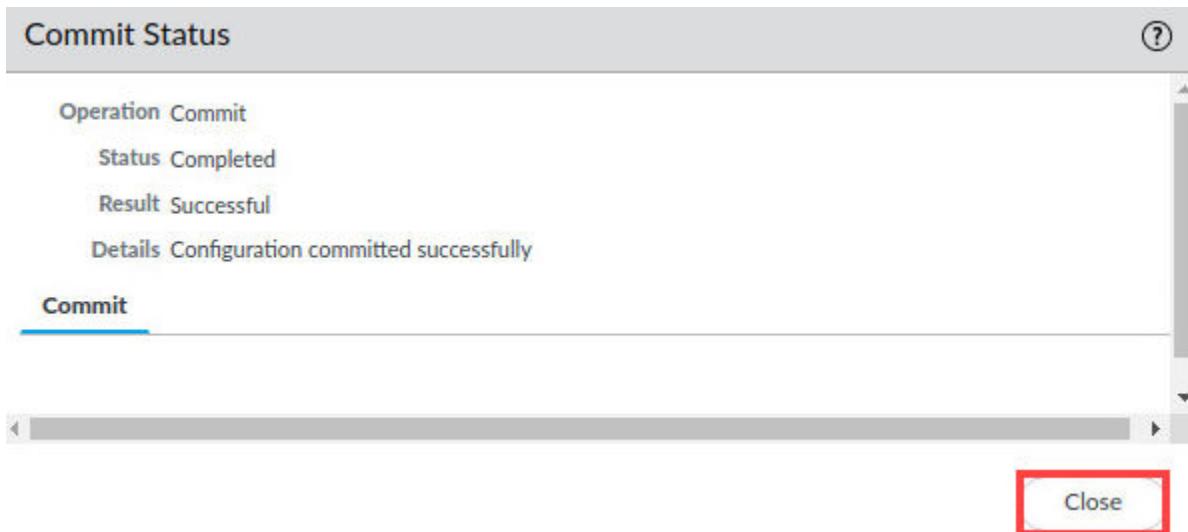
13. Click the **Commit** button at the upper-right of the web interface.



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>
```

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

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

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

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

Please  
Note

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

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

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

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

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

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

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

Please  
Note

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

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



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



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

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

Please Note

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

24. In the firewall web interface, select **Policies > Security**. Click **Users\_to\_Extranet** to edit the rule.

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

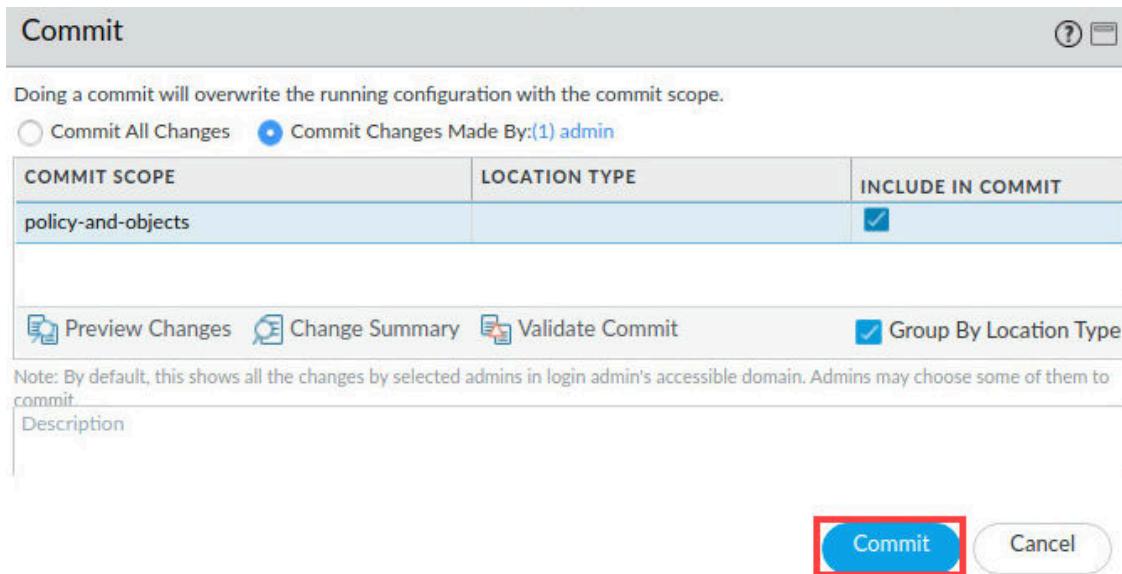
25. In the **Security Policy Rule** window, click the **Destination** tab and configure the following. Click **OK**.

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

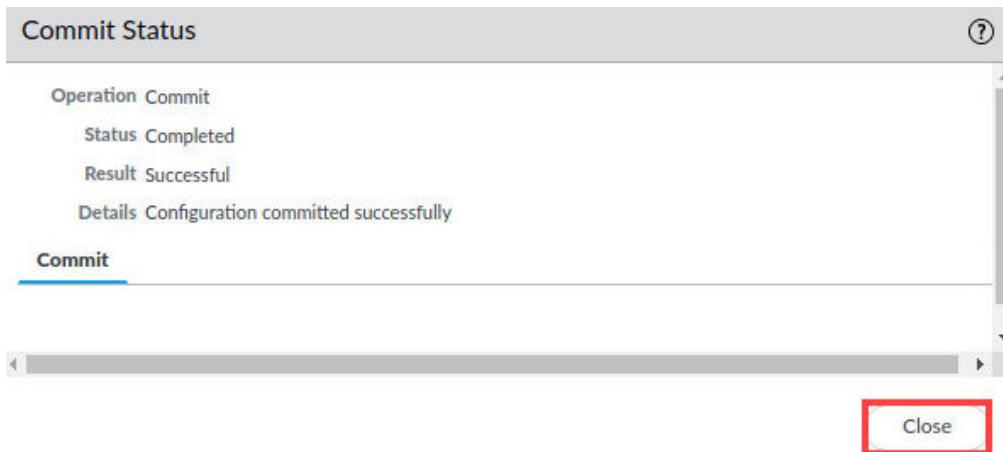
26. Click the **Commit** button at the upper-right of the web interface.



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



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



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

## 7.7 Block Access to Malicious Domains Using an EDL

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

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

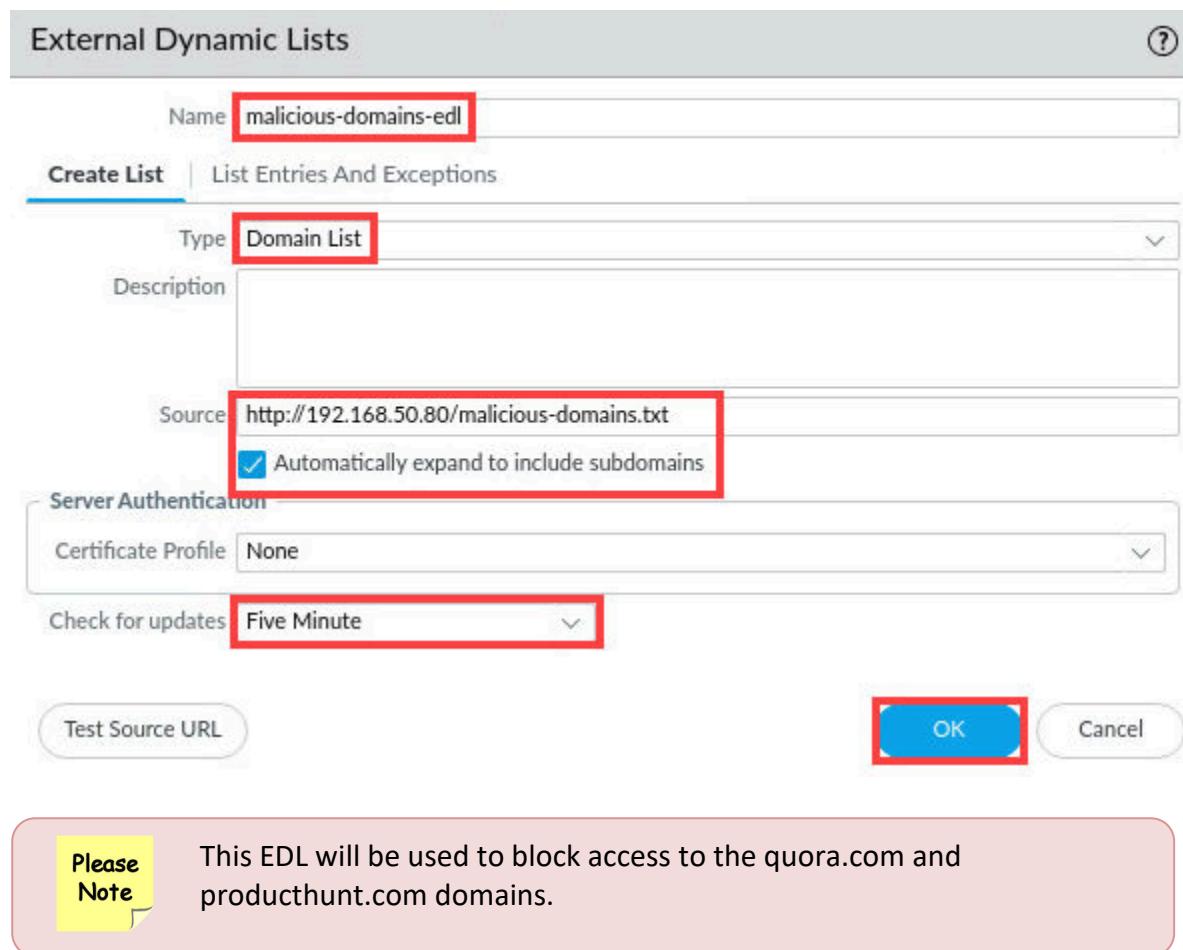
1. In the *PA-VM firewall* web interface, navigate to **Objects > External Dynamic Lists**. Click **Add** at the bottom of the window.

The screenshot shows the PA-VM firewall's web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted with a red box), and NETWORK. The main content area is titled "External Dynamic Lists". On the left, there is a sidebar with various object types: Addresses, Address Groups, Regions, Dynamic User Groups, GlobalProtocols, HIP Objects, HIP Profiles, External Dynamic Lists (which is also highlighted with a red box), Custom Objects, Data Patterns, and Spyware. Below the sidebar is a table with two rows. The first row contains "Palo Alto Networks - Known malicious IP addresses" and is labeled "Predefined". The second row contains "custom-malicious-ips-edl" and has a note to its right stating "Contains manually entered list on web server". At the bottom of the page, there is a footer with links for Decryption Profile, SD-WAN Link Management, Path Quality Profile, SaaS Quality Profile, Traffic Distribution Profile, and Error Correction Profile. The "+ Add" button is highlighted with a red box.

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

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

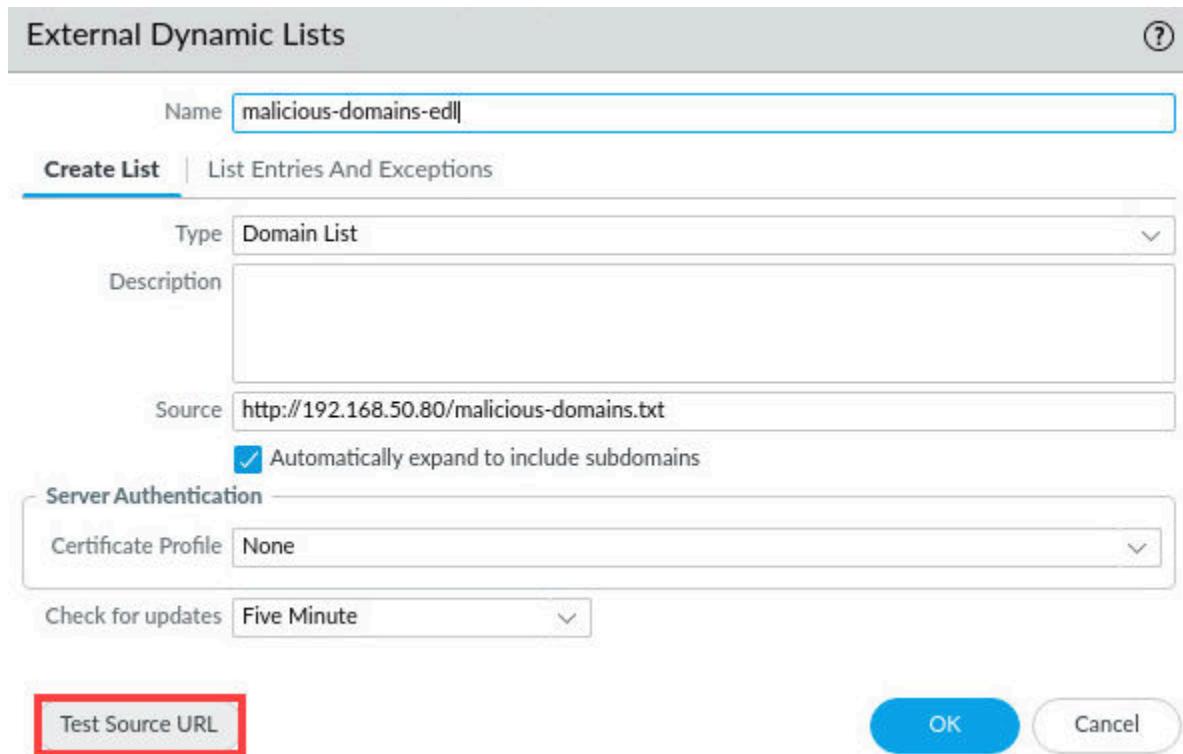
| Parameter                                  | Value  |
|--|--|
| Name                                       | malicious-domains-edl  |
| Type                                       | Domain List  |
| Source                                     | <a href="http://192.168.50.80/malicious-domains.txt">http://192.168.50.80/malicious-domains.txt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



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



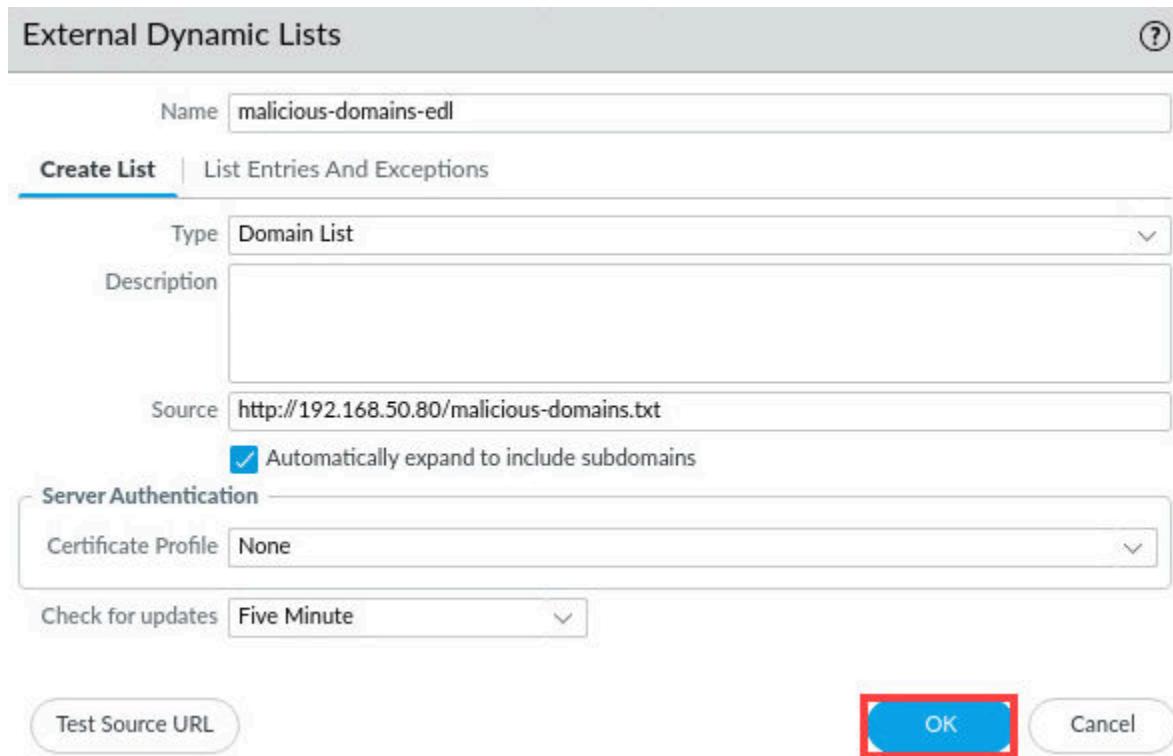
4. In the *External Dynamic Lists* window, click **Test Source URL**.



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.

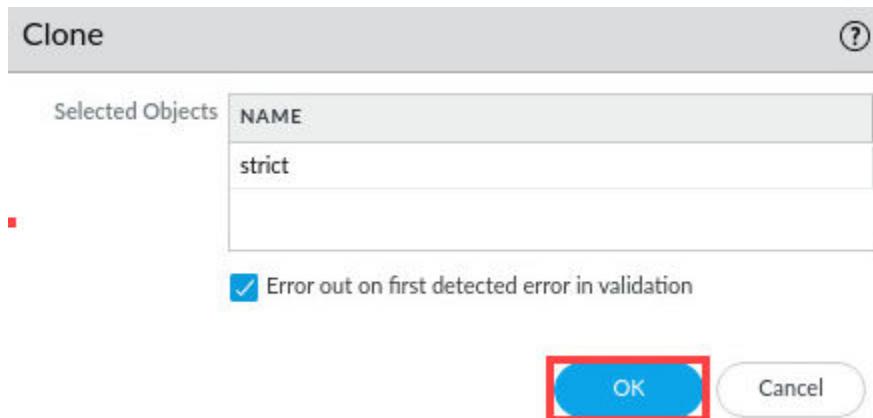
In this section, you will add a domain list EDL to an anti-spyware profile.

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

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

- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS** (highlighted with a red box), NETWORK.
- Left Sidebar:** Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, Devices, GlobalProtect, HIP Objects.
- Table View:** Shows security profiles. The "strict" profile is selected (indicated by a checked checkbox in the first column). The table has columns: NAME, LOCATION, COUNT, POLICY NAME, and THREAT NAME. The "strict" profile has a COUNT of 5 and includes policies: simple-critical, simple-high, simple-medium, simple-low, and simple-informational, all targeting "any".
- Left Panel:** A tree view of security profiles. The "Security Profiles" node is expanded, showing "Anti-Spyware" (which is also highlighted with a red box).
- Bottom Action Bar:** Contains buttons for Add, Delete, **Clone** (highlighted with a red box), and PDF/CSV.

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.

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

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**.

| SIGNATURE SOURCE      | LOG SEVERITY | POLICY ACTION | PACKET CAPTURE |
|-----------------------|--------------|---------------|----------------|
| malicious-domains-edl |              | block         | disable        |

**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.

| ID | Name                 | Action | Scope     | Profile   | Target |
|----|----------------------|--------|-----------|-----------|--------|
| 2  | Users_to_Extranet    | none   | universal | Users_Net | any    |
| 3  | Users_to_Internet    | none   | universal | Users_Net | any    |
| 4  | Extranet_to_Internet | none   | universal | Extranet  | any    |

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

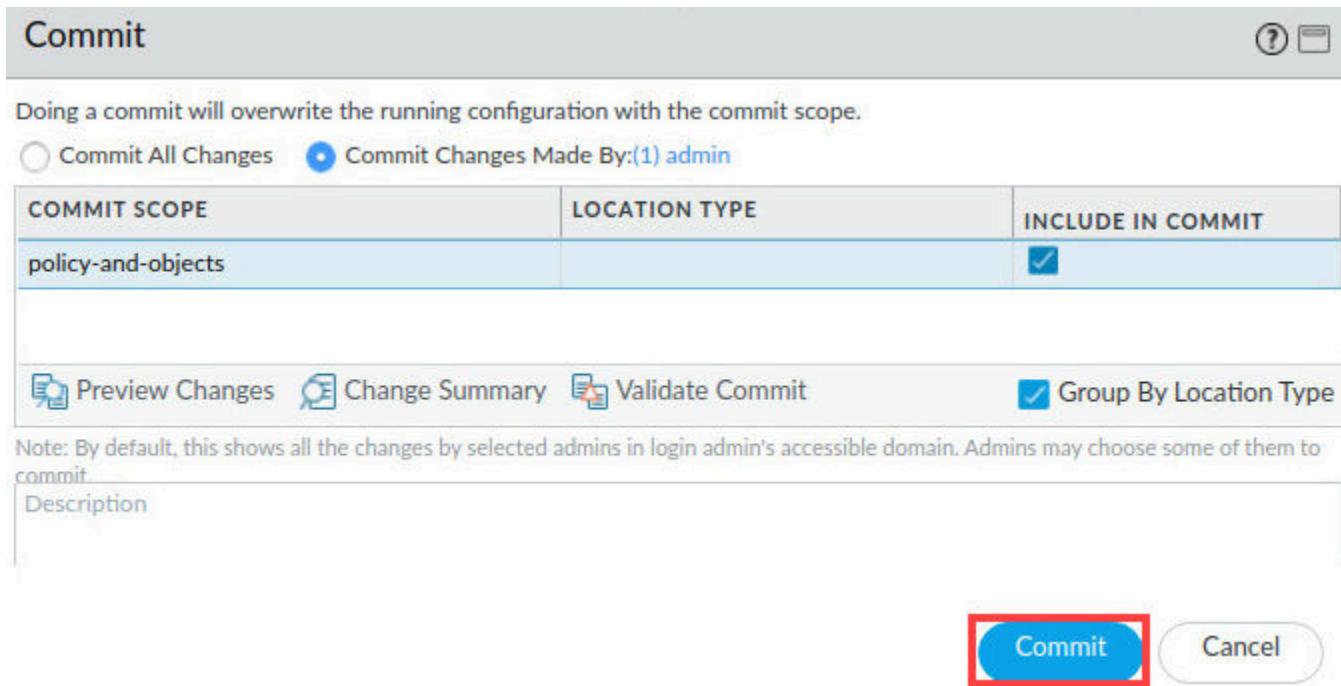
| Parameter    | Value       |
|--------------|-------------|
| Profile Type | Profiles    |
| Anti-Spyware | outbound-as |

The screenshot shows the 'Security Policy Rule' configuration window. The 'Actions' tab is selected. Under 'Action Setting', the 'Action' dropdown is set to 'Allow'. Under 'Profile Setting', the 'Profile Type' is set to 'Profiles'. The 'Anti-Spyware' setting is highlighted with a red box and is set to 'outbound-as'. At the bottom right, the 'OK' button is highlighted with a red box.

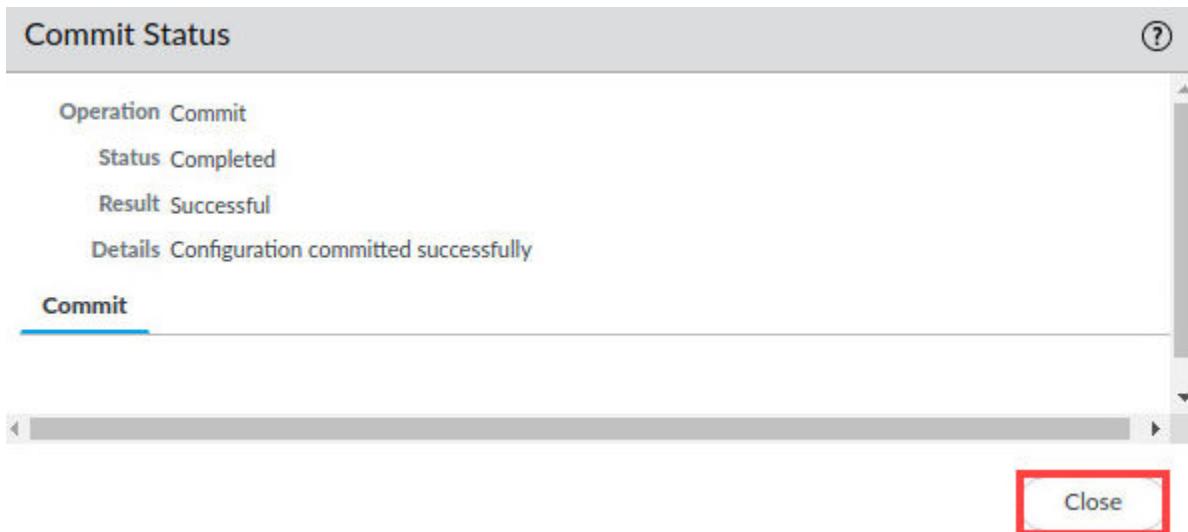
3. Click the **Commit** button at the upper-right of the web interface.



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



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



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



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



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

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

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

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

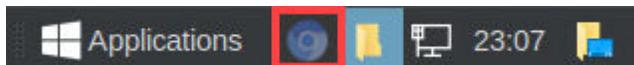
Please  
Note

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

9. Minimize the *Terminal* window.



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



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

| RECEIVE TIME   | TYPE    | THREAT ID/NAME        | FROM ZONE | TO ZONE  | SOURCE ADDRESS | DESTINATION ADDRESS | TO PORT | APPLICATION | ACTION | SEVERITY | URL             |
|----------------|---------|-----------------------|-----------|----------|----------------|---------------------|---------|-------------|--------|----------|-----------------|
| 08/08 20:53:02 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 8.8.8.8             | 53      | dns         | drop   | medium   | quora.com       |
| 08/08 20:52:59 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 1.1.1.1             | 53      | dns         | drop   | medium   | quora.com       |
| 08/08 20:52:40 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 8.8.8.8             | 53      | dns         | drop   | medium   | producthunt.com |
| 08/08 20:52:37 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 1.1.1.1             | 53      | dns         | drop   | medium   | producthunt.com |
| 08/08 20:46:23 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 8.8.8.8             | 53      | dns         | drop   | medium   | producthunt.com |
| 08/08 20:46:20 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 1.1.1.1             | 53      | dns         | drop   | medium   | producthunt.com |
| 08/08 20:46:03 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 8.8.8.8             | 53      | dns         | drop   | medium   | quora.com       |
| 08/08 20:46:00 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 1.1.1.1             | 53      | dns         | drop   | medium   | quora.com       |
| 08/08 20:45:56 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 8.8.8.8             | 53      | dns         | drop   | medium   | quora.com       |
| 08/08 20:45:53 | spyware | malicious-domains-edl | Users_Net | Internet | 192.168.1.20   | 1.1.1.1             | 53      | dns         | drop   | medium   | quora.com       |

**Please Note**

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

- 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.

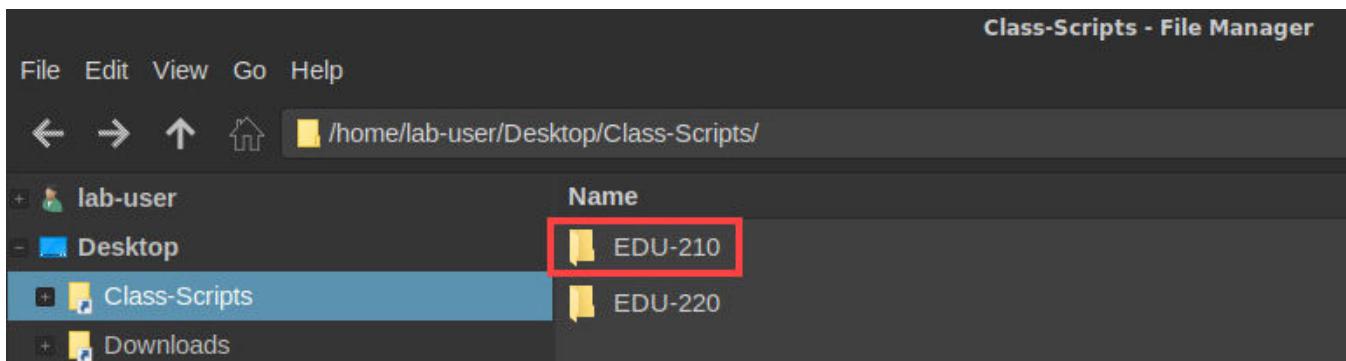
**Please Note**

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.

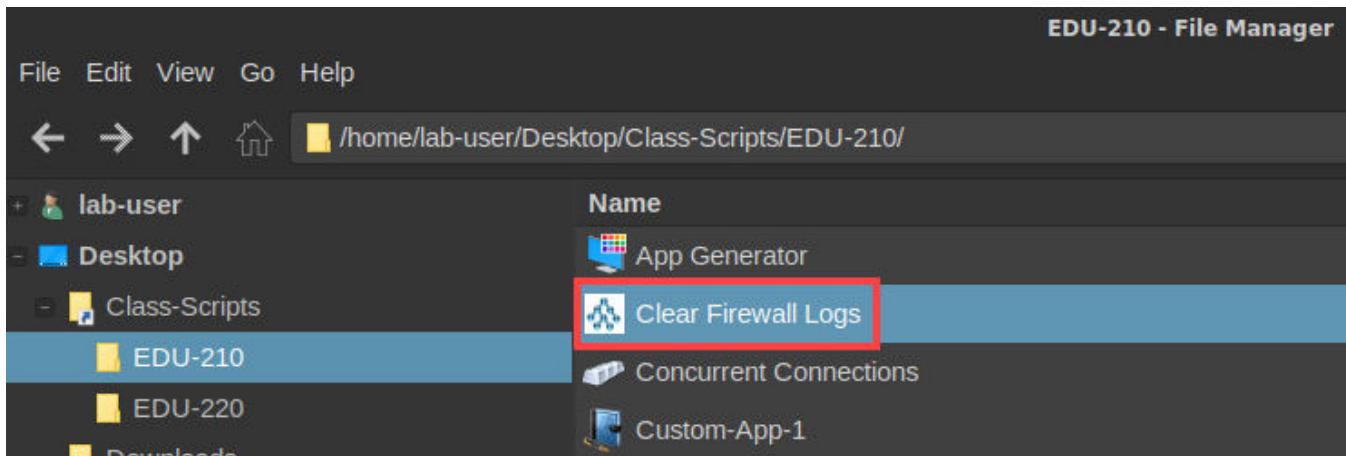
- On the *client desktop*, double-click the folder for **Class-Scripts**.



- 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**.

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

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

Press ENTER to start or CTRL+C to quit.

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

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

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

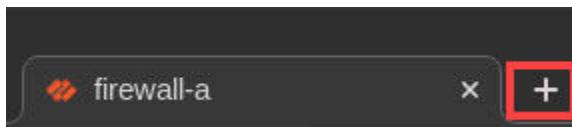
#####
##      Process Complete      ##
#####

Press ENTER to close this window.■
```

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**.

The screenshot shows a Chromium browser window with the title bar "HACKER9 - The Unruly Hacking & Security channel - Chromium". The address bar contains "hacker9.com", which is also highlighted by a red box. Below the address bar, there are navigation icons and a list of recent tabs: "firewall-a", "9 HACKER9 - The Unruly H...". The main content area displays the Hacker9 website, featuring a large banner image and several menu links: FACEBOOK, SECURITY, HACKS, SCAMS, PRIVACY, MOBILE, and CRYPTOCURREN.

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**.

The screenshot shows a web-based interface for managing network policies. At the top, there is a table header with columns: TYPE, ZONE, and ADDRESS. Below the header, there is a "Columns" dropdown menu with a red box around it, showing options: Name, Tags, Group, and Type. A sub-menu "Adjust Columns" is also visible. The main table body contains three rows: one row with "universal" in the ZONE column and "any" in the ADDRESS column; another row with "intrazone" in the ZONE column and "any" in the ADDRESS column; and a third row with "interzone" in the ZONE column and "any" in the ADDRESS column. To the right of the table, there is a list of checked items: Destination L...ce, Application, Service, URL Category, and Action.

|           |     |                    |
|-----------|-----|--------------------|
| universal | Ex  | Destination L...ce |
| intrazone | any | Application        |
| interzone | any | Service            |

The screenshot shows a table with three rows. The first row has "universal" in the first column and "Ex" in the second column. The second row has "intrazone" in the first column and "any" in the second column. The third row has "interzone" in the first column and "any" in the second column. To the right of the table, there is a list of checked items: Destination L...ce, Application, Service, URL Category, and Action. The "URL Category" item is highlighted with a red box.

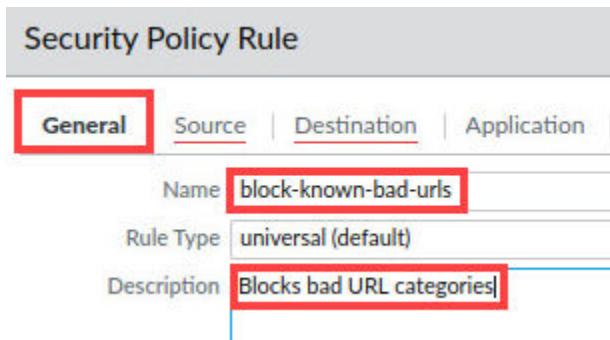
**Please Note**

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

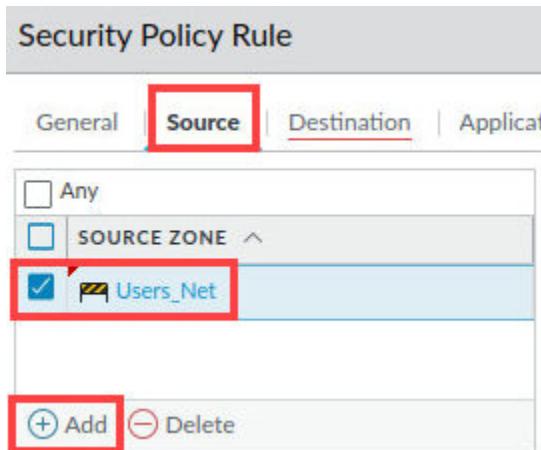
10. In the *Security Policies* window, click **Add** to create a new security policy rule.



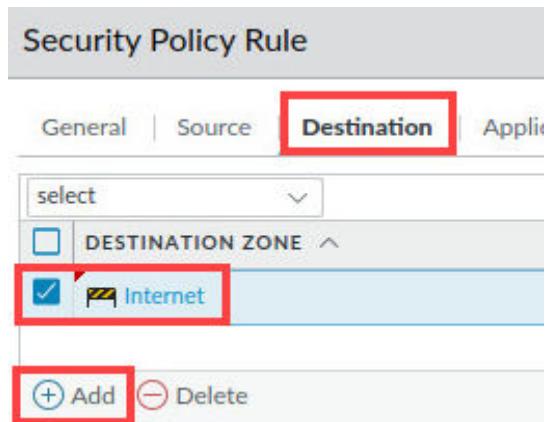
11. In the *Security Policy Rule* window, on the *General* tab, type **block-known-bad-urls** as the *Name*. For *Description*, enter **Blocks bad URL categories**.



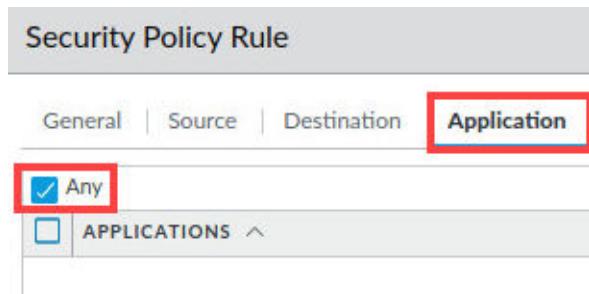
12. Click the **Source** tab and for the *Source Zone*, select **Users\_Net**.



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



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

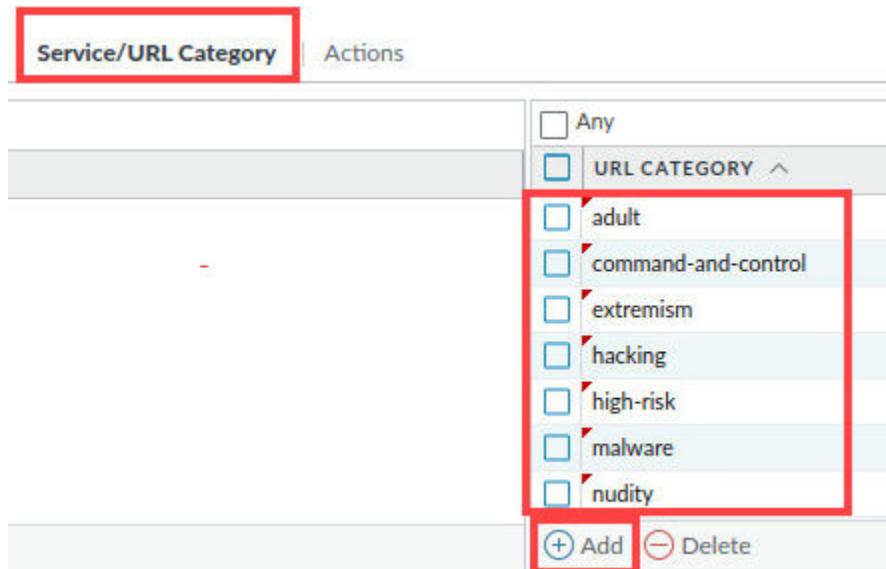


15. Click the **Service/URL Category** tab and configure the following.

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

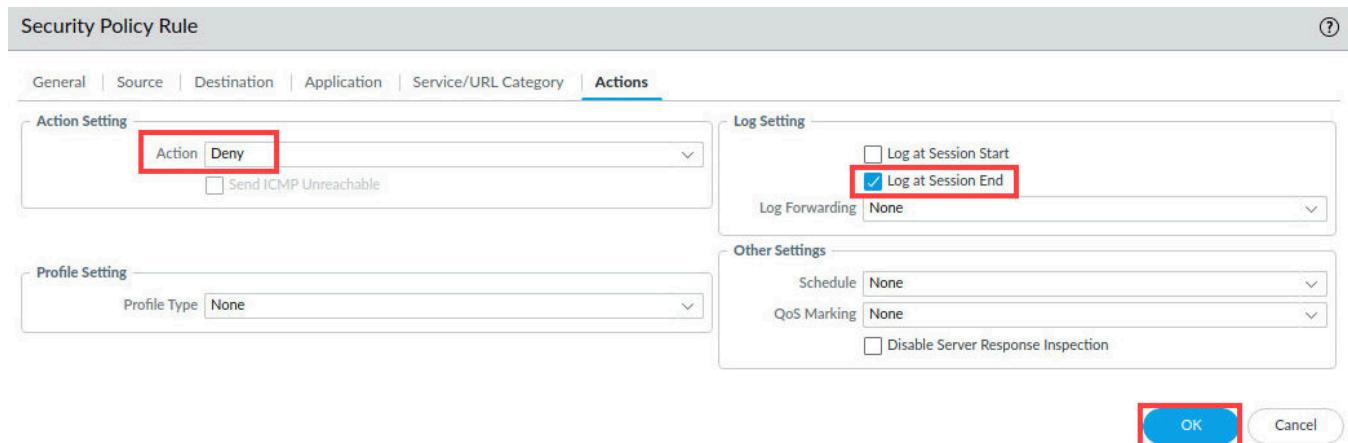
Please  
Note

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



The screenshot shows a user interface for managing service and URL categories. The top navigation bar has two tabs: "Service/URL Category" (which is active and highlighted with a red box) and "Actions". Below the tabs is a search bar with placeholder text "Search for a category or service". A dropdown menu titled "URL CATEGORY" is open, showing a list of categories. The categories listed are: adult, command-and-control, extremism, hacking, high-risk, malware, and nudity. Each category name is preceded by a small blue square icon with a white checkmark. At the bottom of the dropdown menu, there are two buttons: a blue "Add" button with a plus sign and a red "Delete" button with a minus sign. The entire dropdown menu is also highlighted with a red box.

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

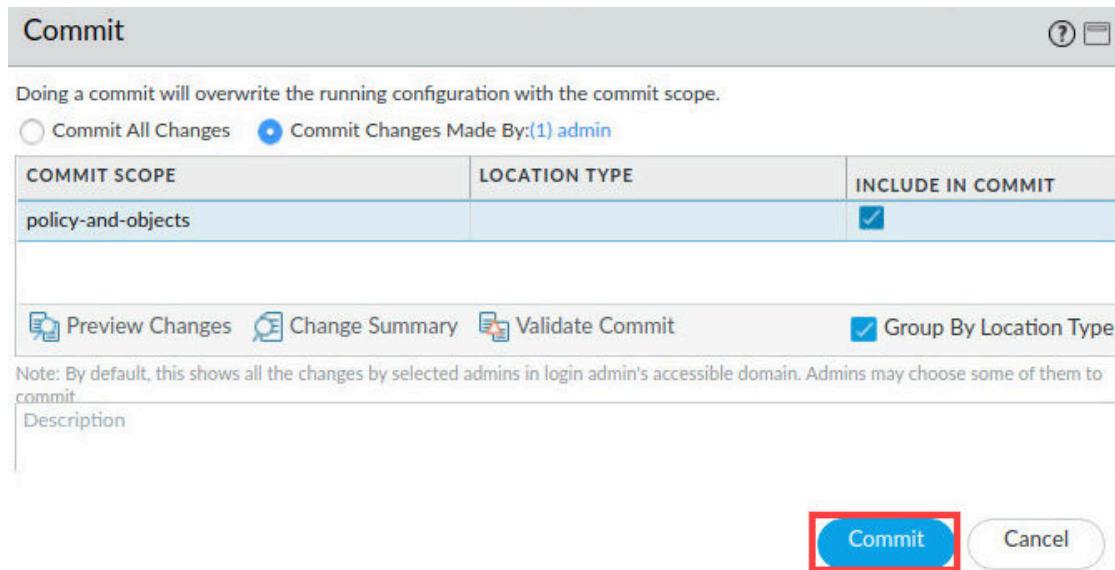


17. Select, but do not open, the **block-known-bad-urls** rule in the security policy. Select **Move > Move Top** to move the *block-known-bad-urls* rule to the top of the security policy.

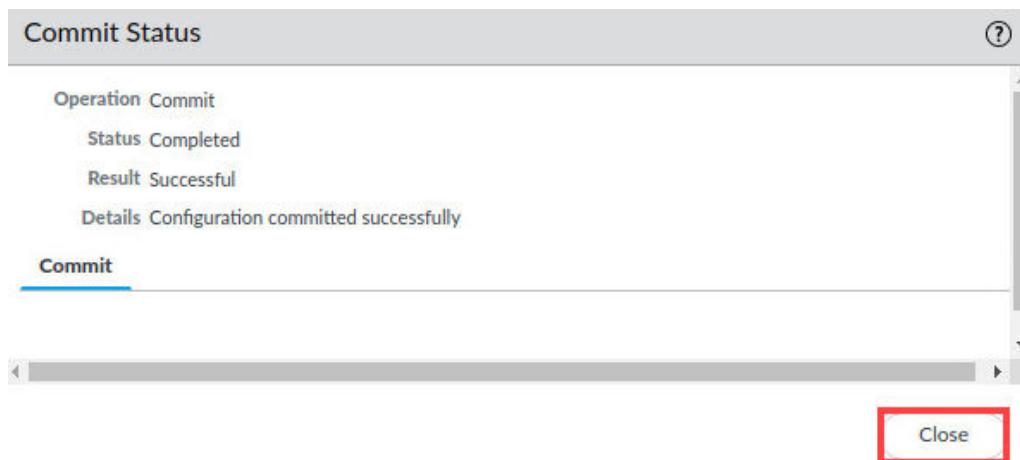
18. Click the **Commit** button at the upper-right of the web interface.



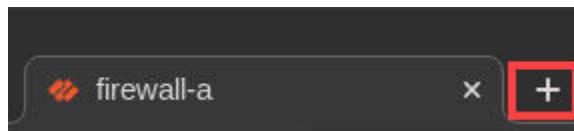
19. In the *Commit* window, click **Commit**.



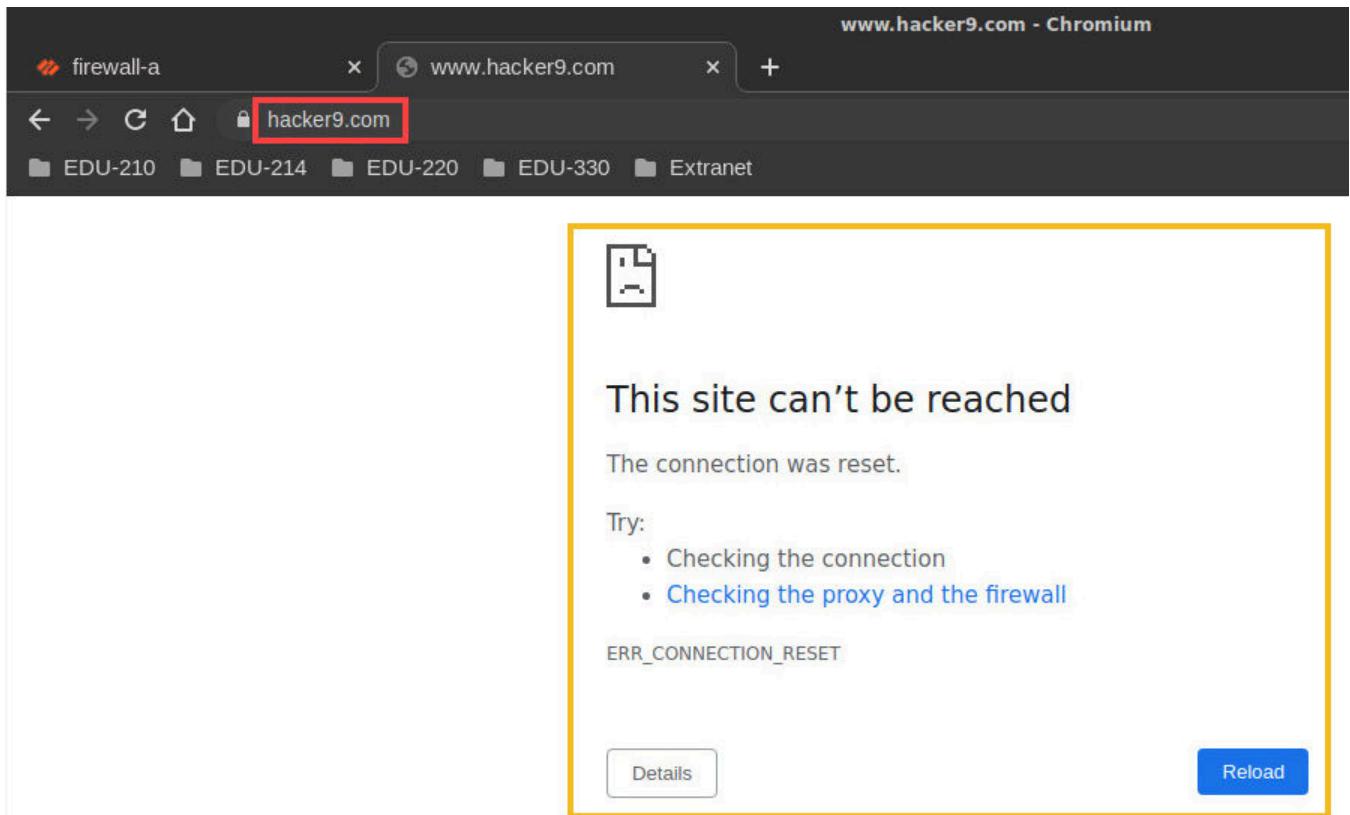
20. Wait until the *Commit* process is complete. Click **Close**.



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**.

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

**Please Note**

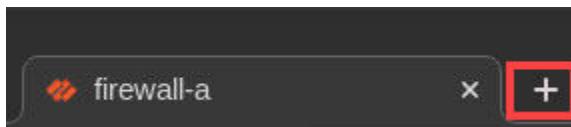
You should see multiple entries that have been blocked. Several default columns have been hidden in the example URL Filtering log file shown here.

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

### 7.11 Create a Custom URL Category

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

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



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

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



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

The screenshot shows the PA-VM web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted in yellow), and NETWORK. On the left, there's a sidebar with icons for Addresses, Address Groups, Regions, Dynamic User Groups, Help Objects, HIP Profiles, External Dynamic Lists, Custom Objects (which is expanded and has URL Category selected), Data Patterns, Spyware, Vulnerability, and SD-WAN Link Management. At the bottom of the interface, there are several buttons: + Add (highlighted with a red box), Delete, Clone, and PDF/CSV.

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

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

Custom URL Category

|             |   |
|-------------|---|
| Name        | block-per-company-policy                |
| Description | URLs that are blocked by company policy |
| Type        | URL List                                |

Matches any of the following URLs, domains or host names

|  |         |                        |                        |
|--|---------|------------------------|------------------------|
| <input type="text"/>   | 2 items | <input type="button"/> | <input type="button"/> |
| <input type="checkbox"/> SITES<br><input type="checkbox"/> *.nbcnews.com<br><input checked="" type="checkbox"/> *theguardian.com |         |                        |                        |
| <input type="button"/> Add   <input type="button"/> Delete   <input type="button"/> Import   <input type="button"/> Export       |         |                        |                        |

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

OK  Cancel

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

PA-VM

DASHBOARD ACC MONITOR POLICIES OBJECTS

Addresses Address Groups Regions Dynamic User Groups

| NAME   | LOCATION |
|--|----------|
| <input checked="" type="checkbox"/> block-per-company-policy |          |

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.

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

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

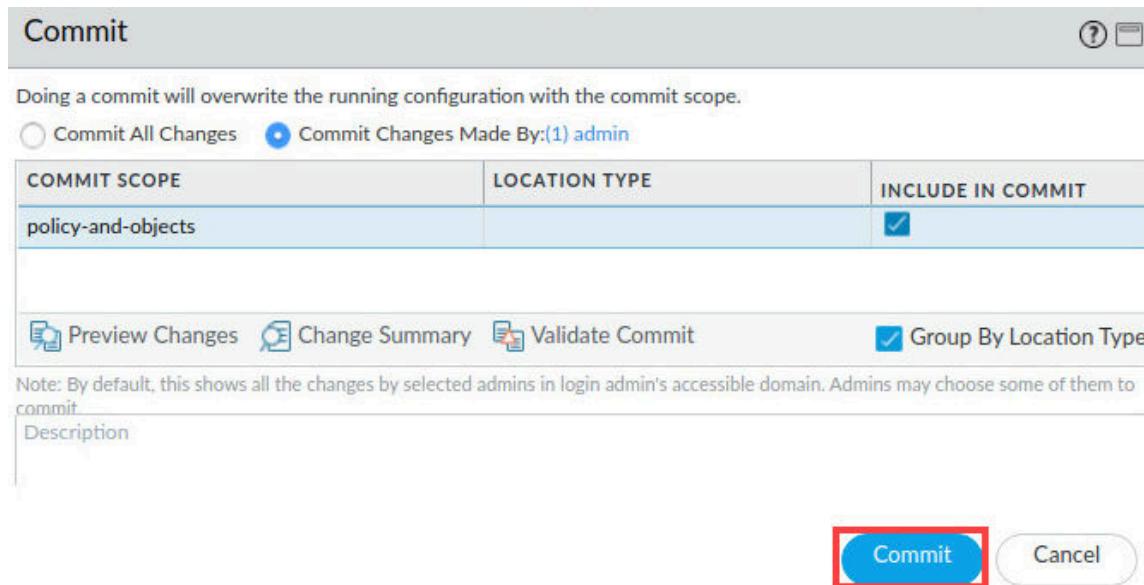
| application-default                                      | SERVICE  |
|--|--|
| <input type="checkbox"/> Any                             | <input type="checkbox"/> URL CATEGORY                        |
| <input type="checkbox"/> nudity                          | <input type="checkbox"/> parked                              |
| <input type="checkbox"/> parked                          | <input type="checkbox"/> peer-to-peer                        |
| <input type="checkbox"/> peer-to-peer                    | <input type="checkbox"/> phishing                            |
| <input type="checkbox"/> phishing                        | <input type="checkbox"/> proxy-avoidance-and-anonymizers     |
| <input type="checkbox"/> proxy-avoidance-and-anonymizers | <input type="checkbox"/> questionable                        |
| <input type="checkbox"/> questionable                    | <input checked="" type="checkbox"/> block-per-company-policy |

**+ Add** **- Delete** **OK** **Cancel**

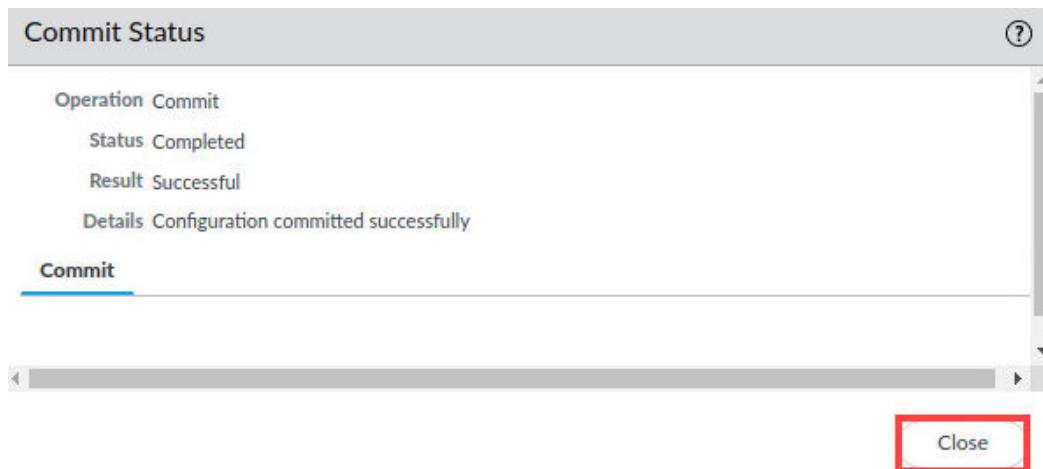
9. Click the **Commit** button at the upper-right of the web interface.



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](http://www.nbcnews.com) on the first tab and press **Enter**. Type [www.theguardian.com](http://www.theguardian.com) on the second tab and press **Enter**.



This site can't be reached

The connection was reset.

Try:

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

[ERR\\_CONNECTION\\_RESET](#)

[Details](#)

[Reload](#)

Please  
Note

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

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



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

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

**Please Note**

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

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

## 7.12 Create an EDL to Block Malicious URL Access

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

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

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

The screenshot shows the PA-VM web interface with the 'OBJECTS' tab selected. In the left sidebar, under 'External Dynamic Lists', the 'External Dynamic Lists' option is highlighted with a red box. At the bottom of the main content area, there is a table with columns: NAME, LOCATION, and DESCRIPTION. Two entries are listed:

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

At the bottom of the table, there is a row of buttons: '+ Add' (highlighted with a red box), Delete, Clone, PDF/CSV, Move Top, Move Up, Move Down, and Move Bottom.

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

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

External Dynamic Lists

Name **malicious-urls-edl**

Create List | List Entries And Exceptions

Type **URL List**

Description

Source **http://192.168.50.80/malicious-urls.txt**

Server Authentication

Certificate Profile **None**

Check for updates **Five Minute**

Test Source URL OK Cancel

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

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

Dynamic URL Lists

- Palo Alto Networks - Authentication Portal Exclude List
- malicious-urls-edl**

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

External Dynamic Lists

Name

Create List | List Entries And Exceptions

Type

Description

Source

Server Authentication

Certificate Profile

Check for updates

**Test Source URL**  OK Cancel



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

Test Source URL

Source URL is accessible.

**Close**



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

External Dynamic Lists

Name: malicious-urls-edl

Create List | List Entries And Exceptions

Type: URL List

Description:

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

Server Authentication

Certificate Profile: None

Check for updates: Five Minute

Test Source URL

OK (highlighted)

Cancel

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.

PA-VM

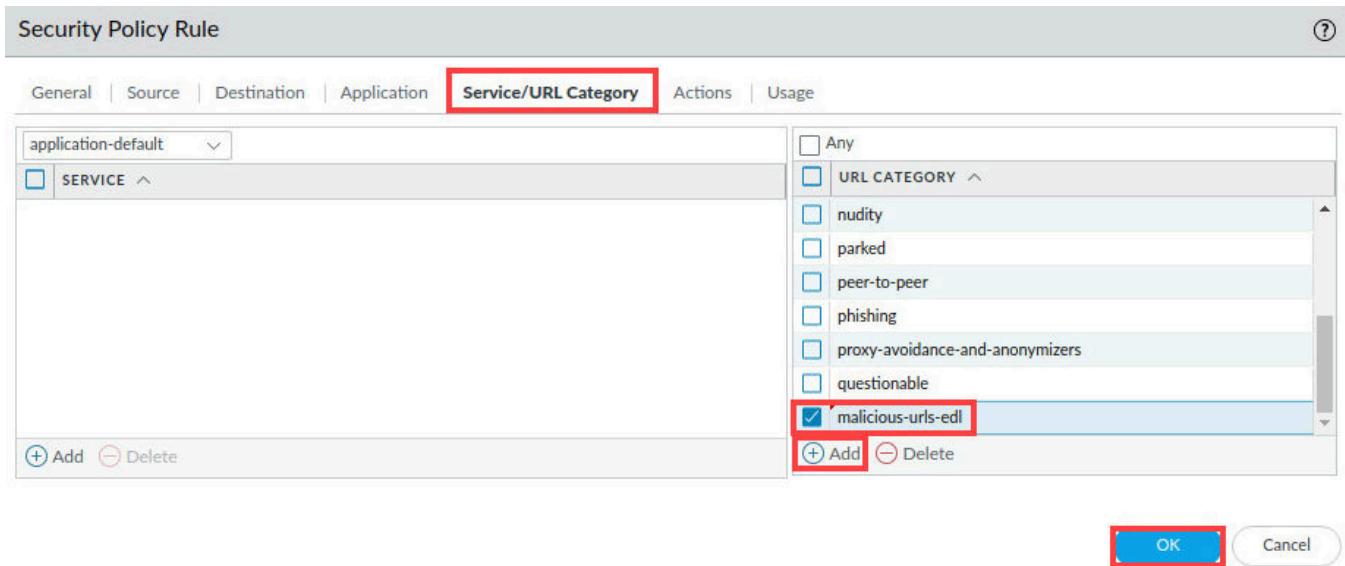
DASHBOARD ACC MONITOR POLICIES (highlighted)

Security (highlighted)

NAT QoS Policy Based Forwarding Decryption Tunnel Inspection

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

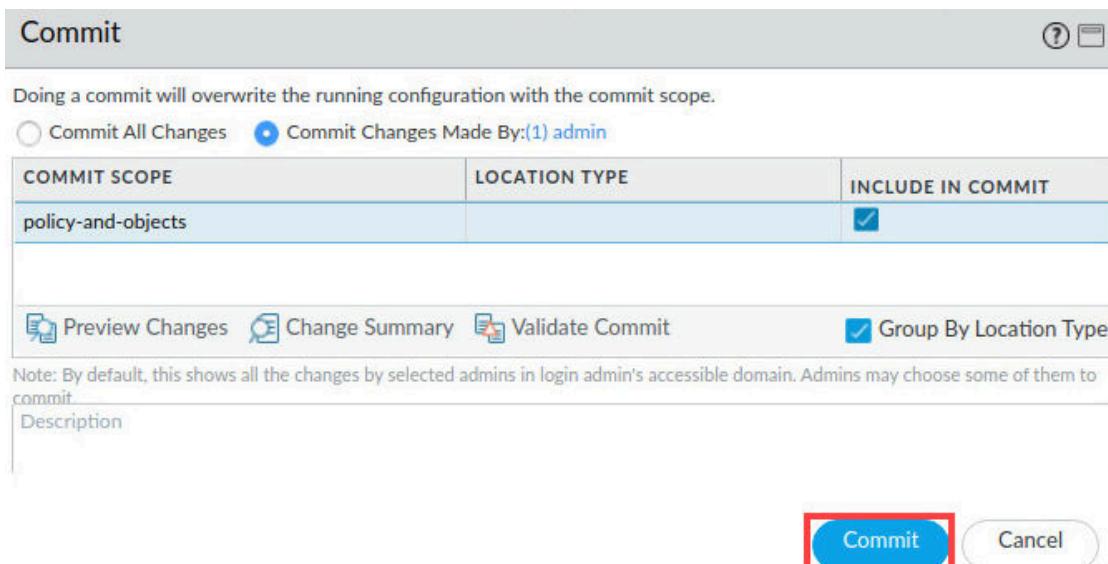
8. In the **Security Policy Rule** window, click the **Service/URL Category** tab. Add **malicious-urls-edl** to the list. Click **OK**.



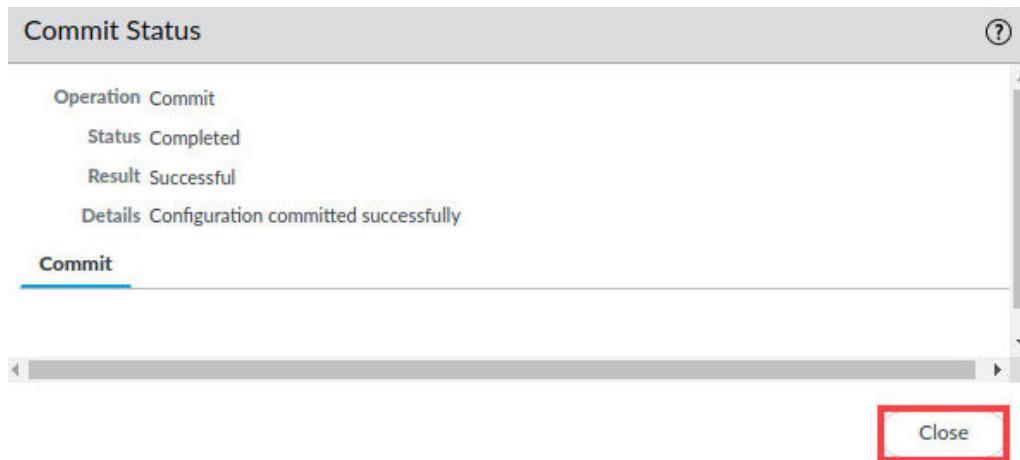
9. Click the **Commit** button at the upper-right of the web interface.



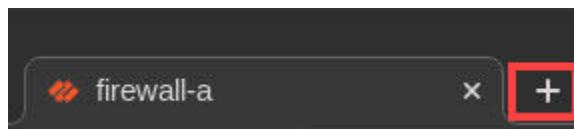
10. In the **Commit** window, click **Commit**.



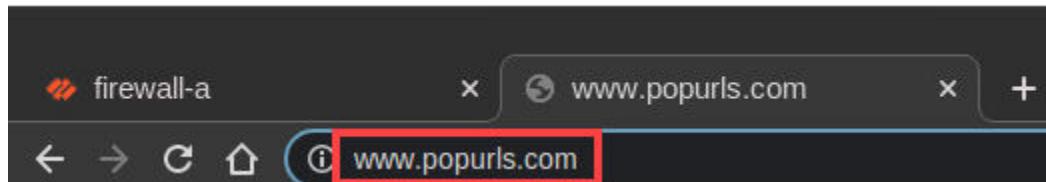
11. Wait until the *Commit* process is complete. Click **Close**.



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.



## This site can't be reached

The connection was reset.

Try:

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

ERR\_CONNECTION\_RESET

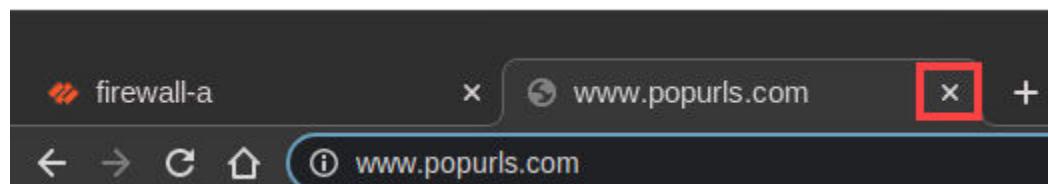
Details

Reload

Please  
Note

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

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



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

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

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

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

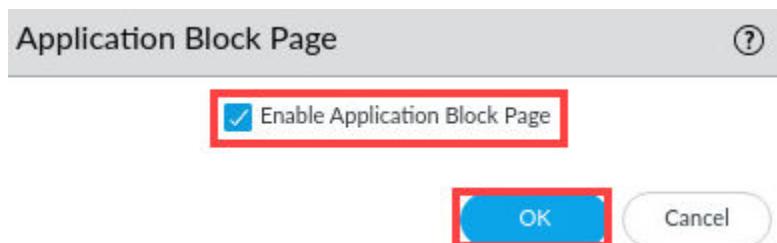
Now you will configure a URL Filtering Profile to control access to URLs. You must add the URL Filtering Profile to a security policy rule with an “allow” action. The use of a URL Filtering Profile to block access to URLs typically is easier to maintain over time compared to the addition of URLs to a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

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

- 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.

| TYPE  | ACTION   | LOCATION |
|---|----------|----------|
| Antivirus / Anti-spyware Block Page         |          | Default  |
| Application Block Page                      | Disabled | Default  |
| Captive Portal Comfort Page                 |          | Default  |
| Data Filtering Block Page                   |          | Default  |
| URL Filtering and Category Match Block Page |          | Default  |
| URL Filtering Continue and Override Page    |          | Default  |
| URL Filtering Safe Search Block Page        |          | Default  |
| Anti Phishing Block Page                    |          | Default  |

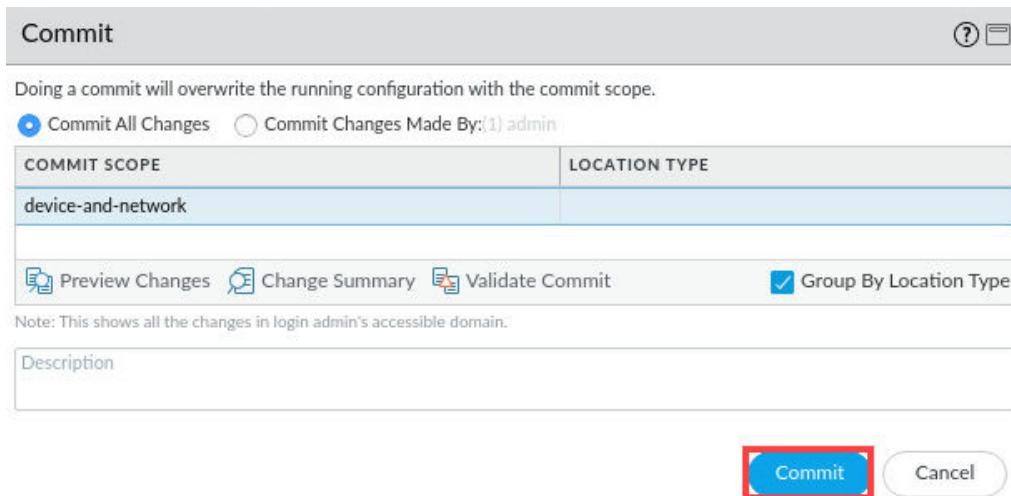
- In the **Application Block Page** window, place a **check** in the box for **Enable Application Block Page**. Click **OK**.



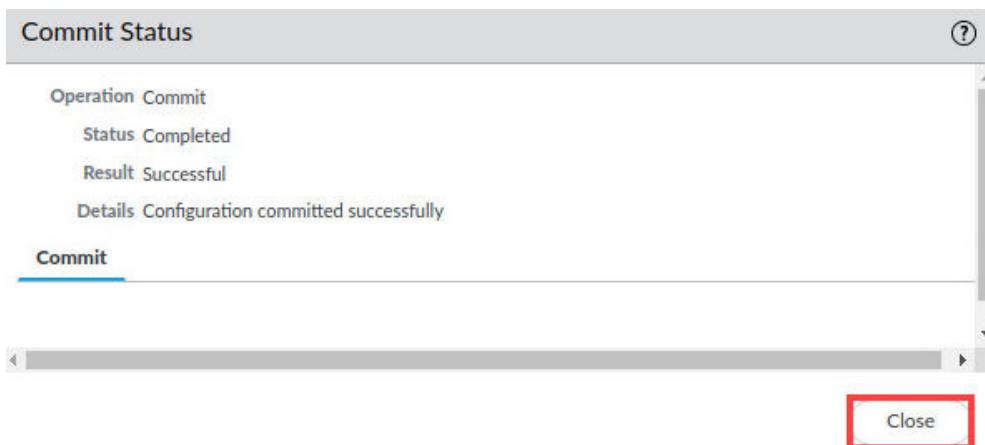
- Click the **Commit** button at the upper-right of the web interface.



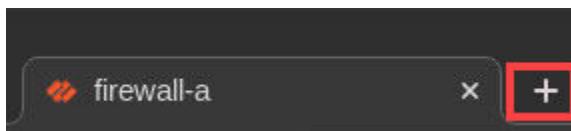
4. In the *Commit* window, click **Commit**.



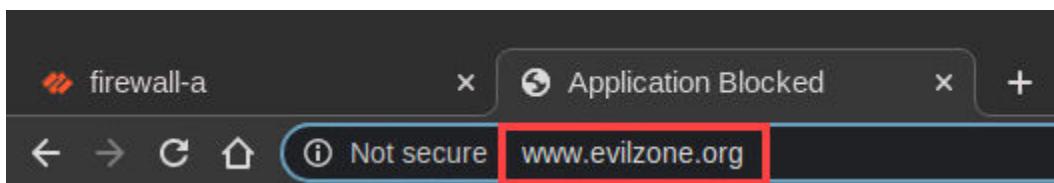
5. Wait until the *Commit* process is complete. Click **Close**.



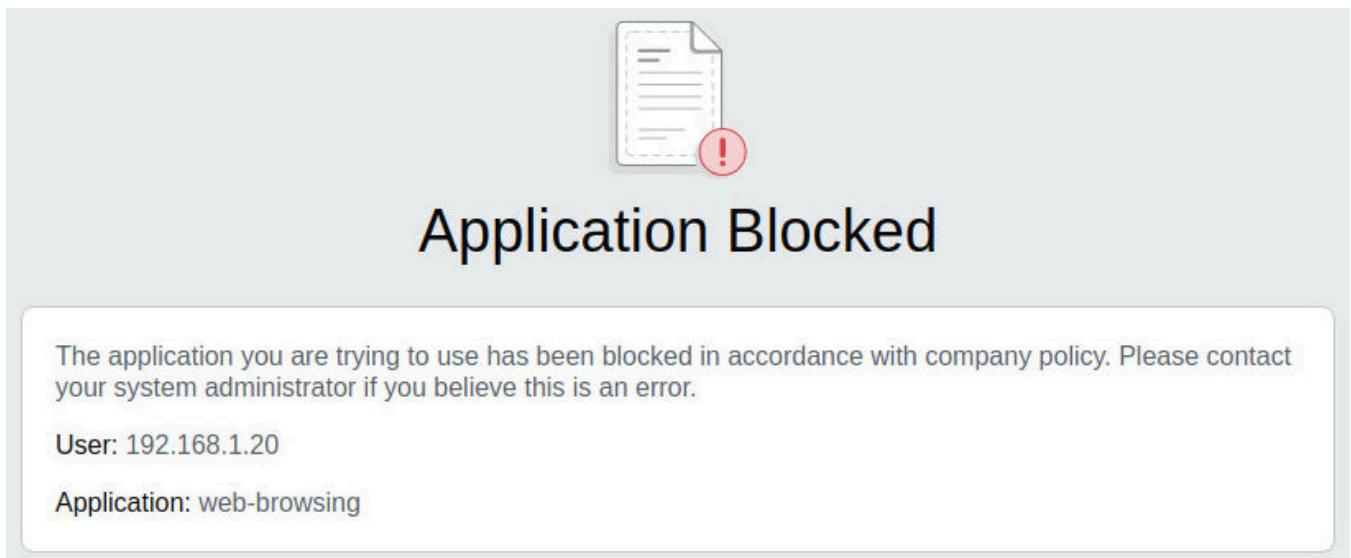
6. Test the *Application Block Page* response. Open a new tab in **Chromium**.



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



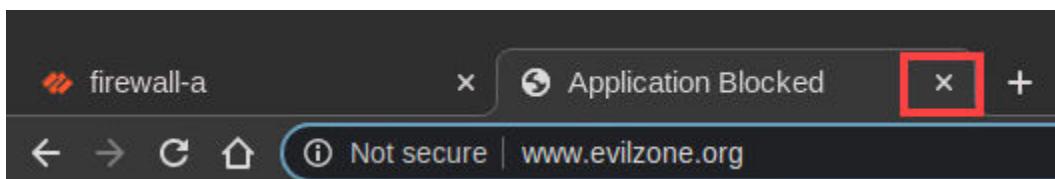
8. The browser displays a block page because the EDL in the security policy blocks access to the [evilzone.org](http://evilzone.org) webpage.



**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](http://evilzone.org) tab by clicking the X icon.



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

The screenshot shows the PA-VM web interface. At the top, there is a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted with a red box), and NETWORK. Below the navigation bar is a sidebar with icons for Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Vulnerability, URL Category, Security Profiles (highlighted with a red box), Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering (highlighted with a red box), File Blocking, WildFire Analysis, SaaS Quality Profile, and Traffic Distribution Profile. The main content area shows a table with columns: NAME, LOCATION, and SITE ACCESS. One row is visible for 'default' with 'Predefined' location and 'Allow Categories (58)' and 'Alert Categories (5)' under SITE ACCESS. At the bottom of the main content area, there is a toolbar with buttons for Add (highlighted with a red box), Delete, Clone, and PDF/CSV, along with a note: "(\* indicates custom URL category, + indicates".

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

The screenshot shows the 'URL Filtering Profile' configuration page. The title is 'URL Filtering Profile'. There are two input fields: 'Name' containing 'Corp-URL-Profile' and 'Description' containing 'Company URL Filtering profile'. Below these fields are three tabs: 'Categories' (underlined), 'URL Filtering Settings', and 'User Credential Detection'. A note at the bottom right says '(\* indicates custom URL category, + indicates'.

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

| SITE ACCESS | USER CREDENTIAL SUBMISSION |
|-------------|----------------------------|
| block       | block                      |
| block       | block                      |
| allow       | allow                      |
| allow       | allow                      |

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**.

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

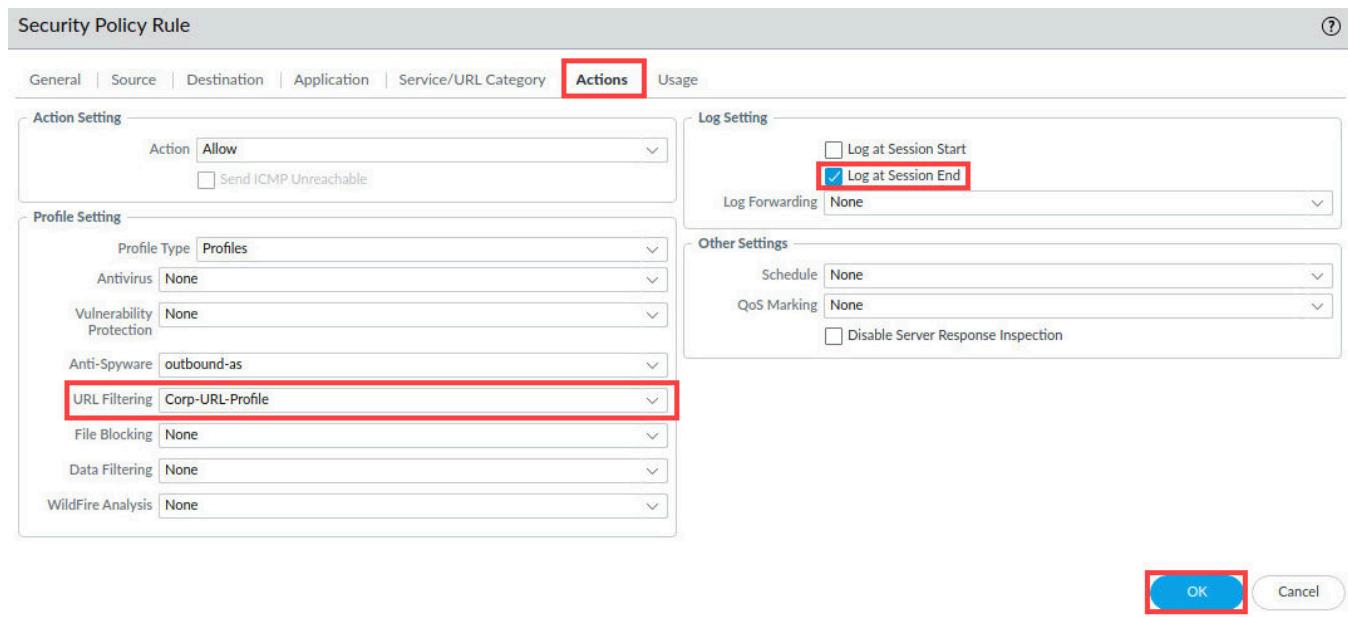
**OK** **Cancel**

14. In the web interface, select **Policies > Security**. Click **Users\_to\_Internet** to edit the rule.

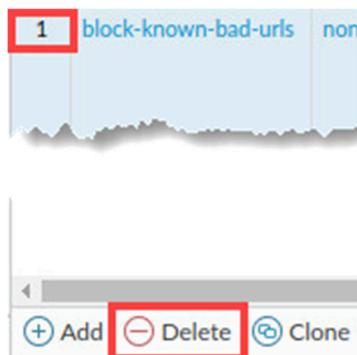
| Order | Name                 | Action | Scope     | Profile   | Target |
|-------|----------------------|--------|-----------|-----------|--------|
| 3     | Users_to_Extranet    | none   | universal | Users_Net | any    |
| 4     | Users_to_Internet    | none   | universal | Users_Net | any    |
| 5     | Extranet_to_Internet | none   | universal | Extranet  | any    |

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

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



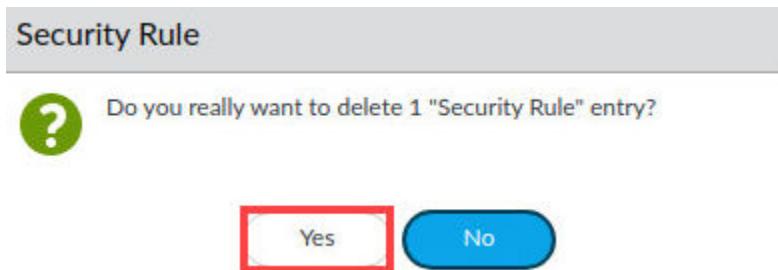
16. Select, but do not open the *block-known-bad-urls* security policy rule. Click **Delete** to remove the *block-known-bad-urls* rule.



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.

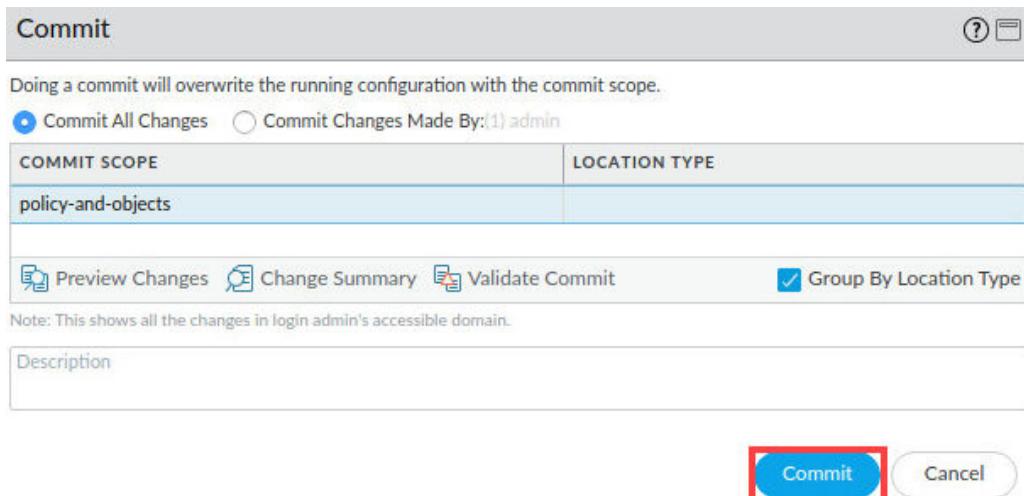
17. In the *Security Rule* window, click **Yes** to confirm the deletion.



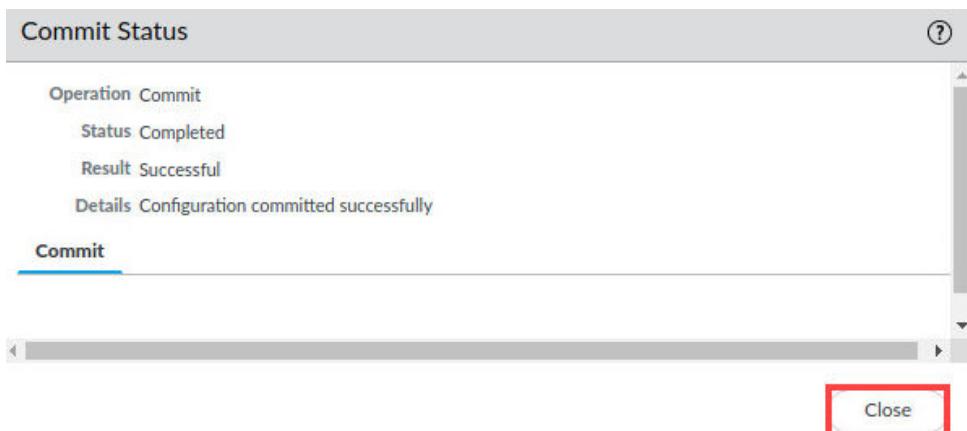
18. Click the **Commit** button at the upper-right of the web interface.



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



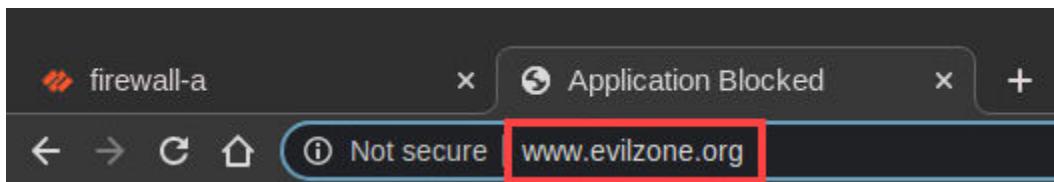
20. Wait until the *Commit* process is complete. Click **Close**.



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



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



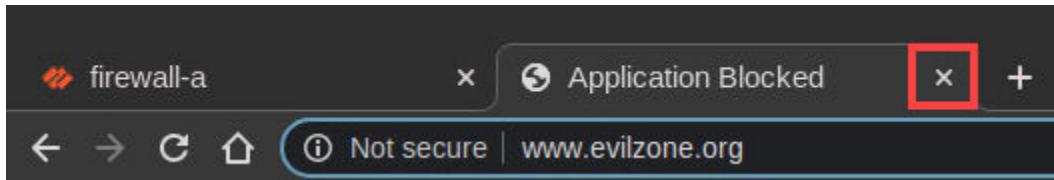
23. The browser displays a block page because the EDL in the security policy blocks access to the *evilzone.org* webpage. If the *Web Page Blocked* message does not appear, allow 1 to 3 minutes for the firewall to process the changes, then refresh the *evilzone.org* tab.

User: 192.168.1.20  
URL: www.evilzone.org/  
Category: hacking

Please  
Note

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

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



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

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

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