



SECURITY OPERATIONS FUNDAMENTALS V2

Lab 8: Using Dynamic Block Lists

Document Version: **2022-12-23**

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

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

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

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
1 Using Dynamic Block Lists	6
1.0 Load Lab Configuration	6
1.1 Create a List of Blocked Sites and Upload to DMZ Server	11
1.2 Create an External Dynamic List Object	15
1.3 Create a Security Policy	20
1.4 Commit and Test	25

Introduction

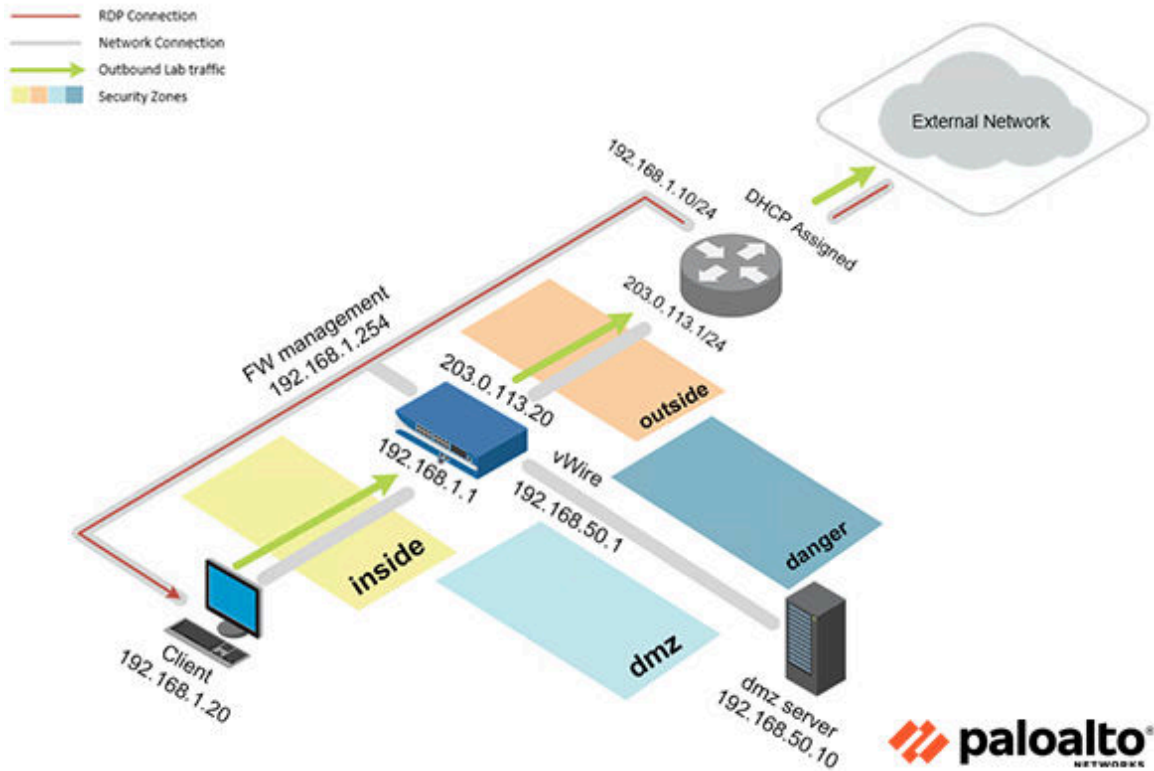
In this lab, you will configure a Security Policy to use a Dynamic Block List.

Objective

In this lab, you will perform the following tasks:

- Create a List of Blocked Sites and Upload to DMZ Server
- Create an External Dynamic List Object
- Commit and Test

Lab Topology



Lab Settings

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

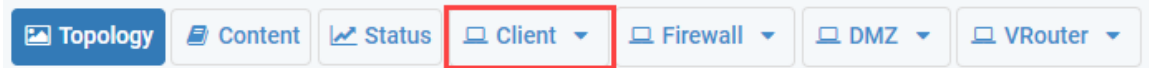
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Using Dynamic Block Lists

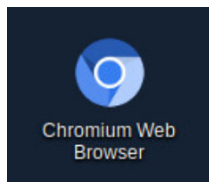
1.0 Load Lab Configuration

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

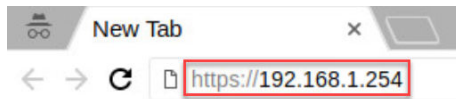
1. Click on the **Client** tab to access the client PC.



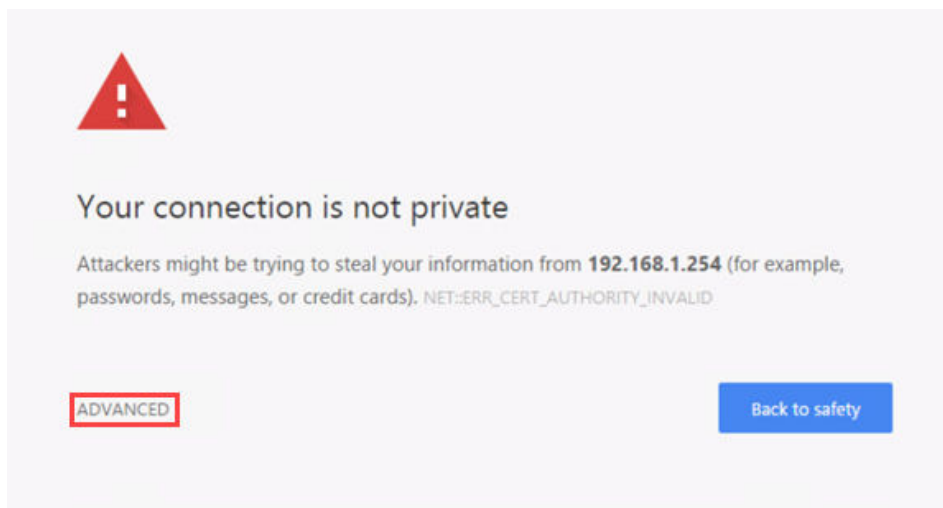
2. Log in to the client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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

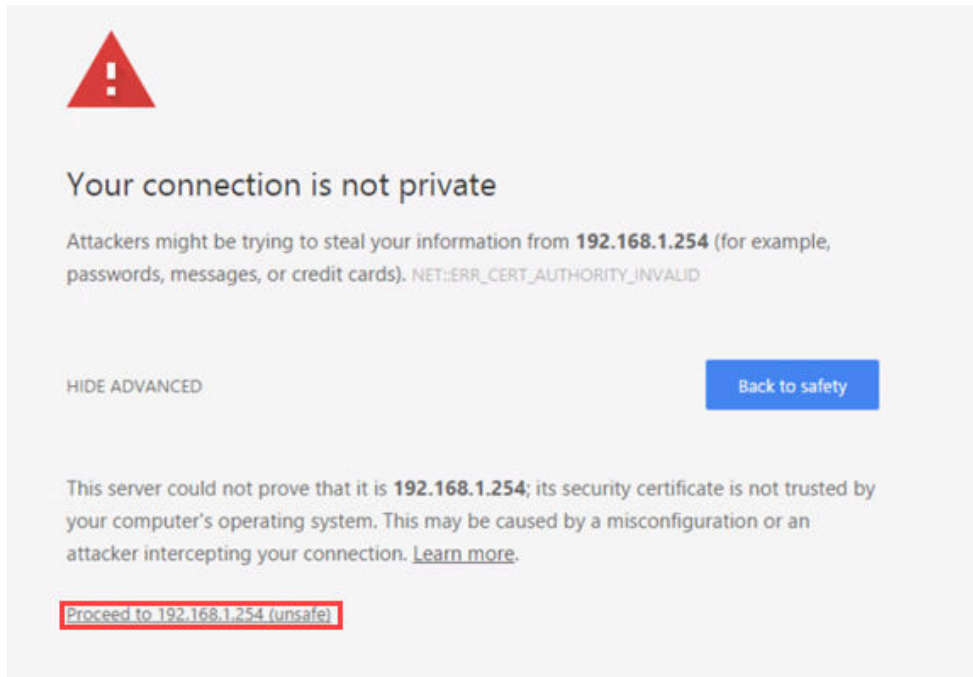


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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

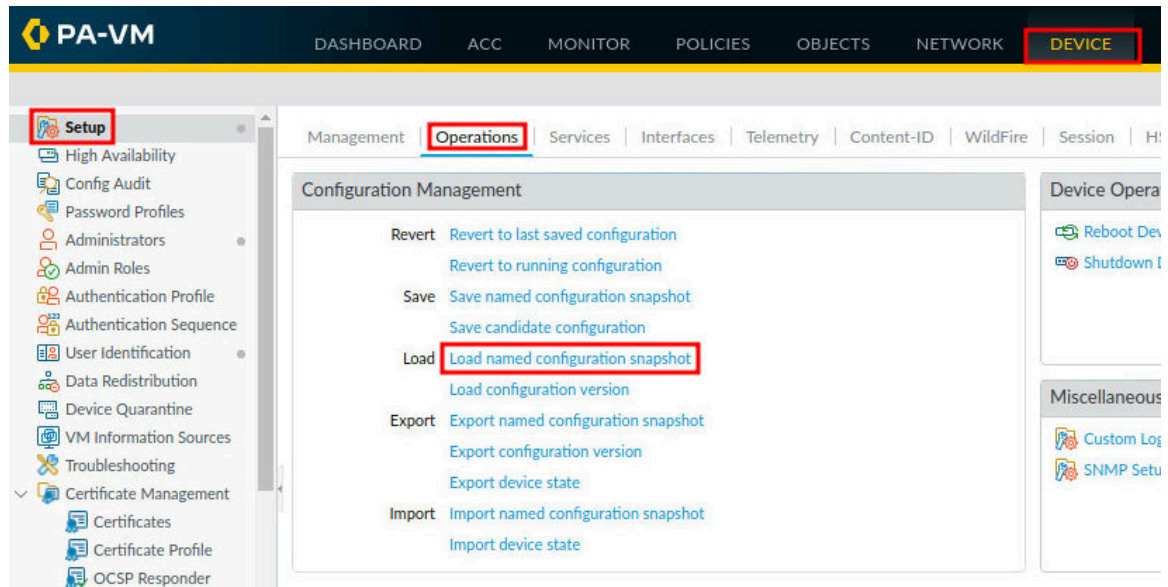
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



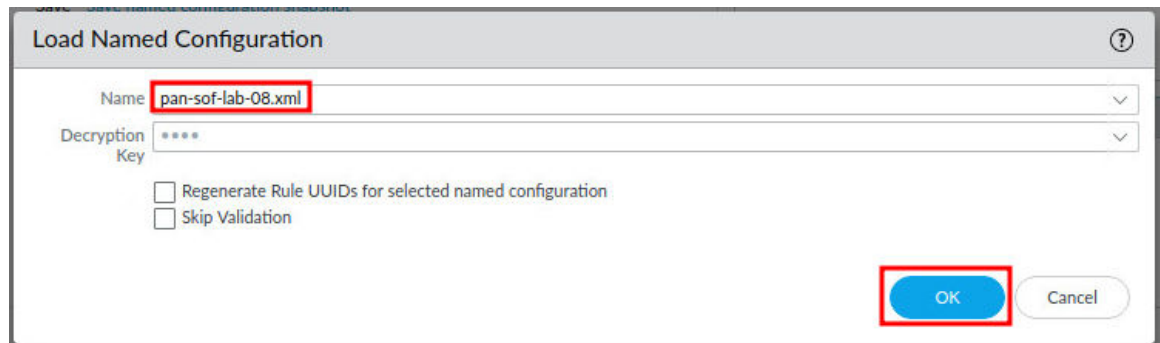
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



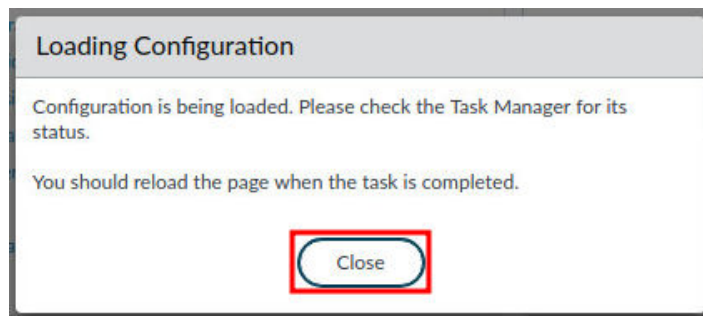
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** in the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-sof-lab-08.xml** from the *Name* dropdown box and click **OK**.



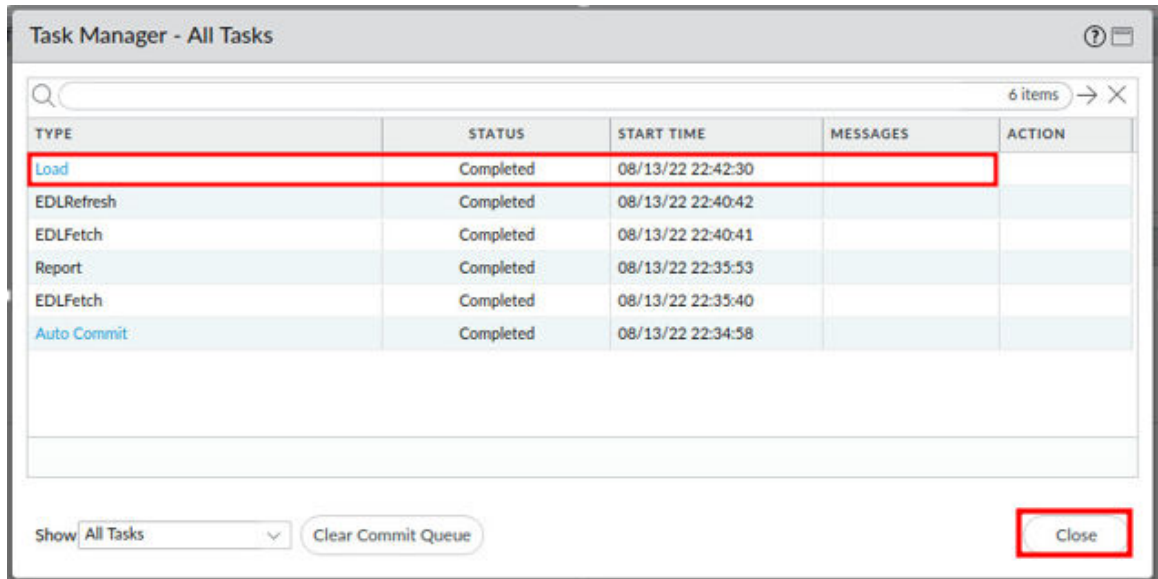
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



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



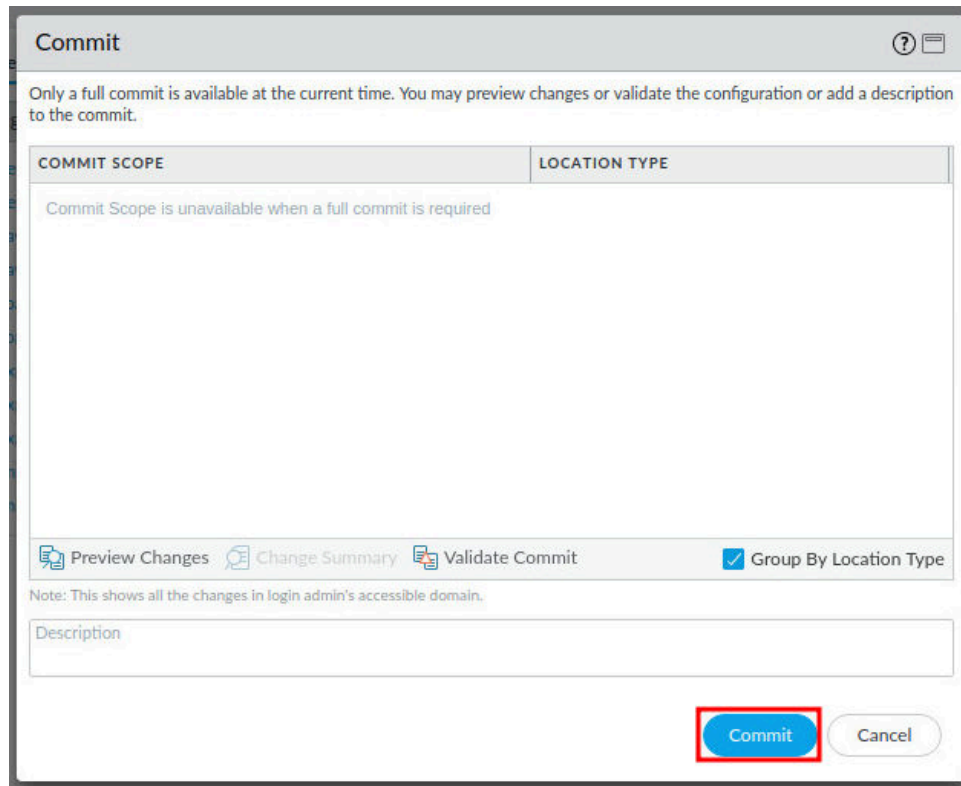
12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.



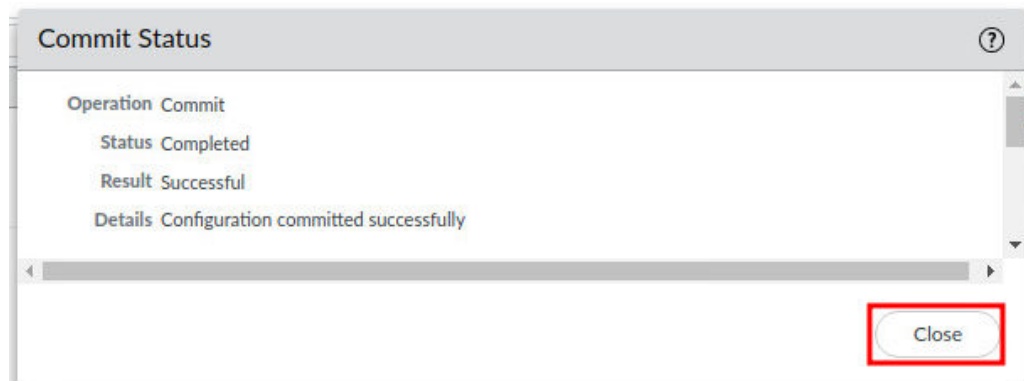
13. Click the **Commit** link located at the top-right of the web interface.



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



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



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

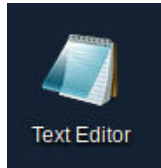
1.1 Create a List of Blocked Sites and Upload to DMZ Server

In this section, you will create a text file with a list of blocked sites.

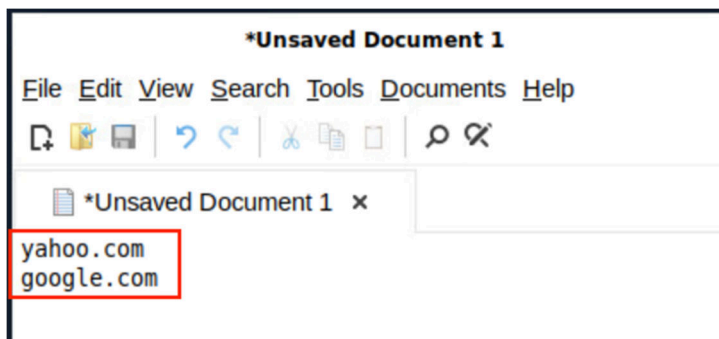
1. Minimize *Chromium* in the upper-right corner.



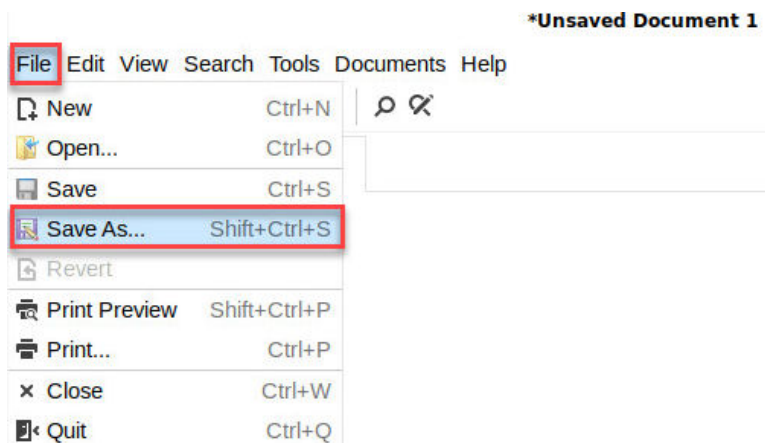
2. Double-click the **Text Editor** icon located on the desktop.



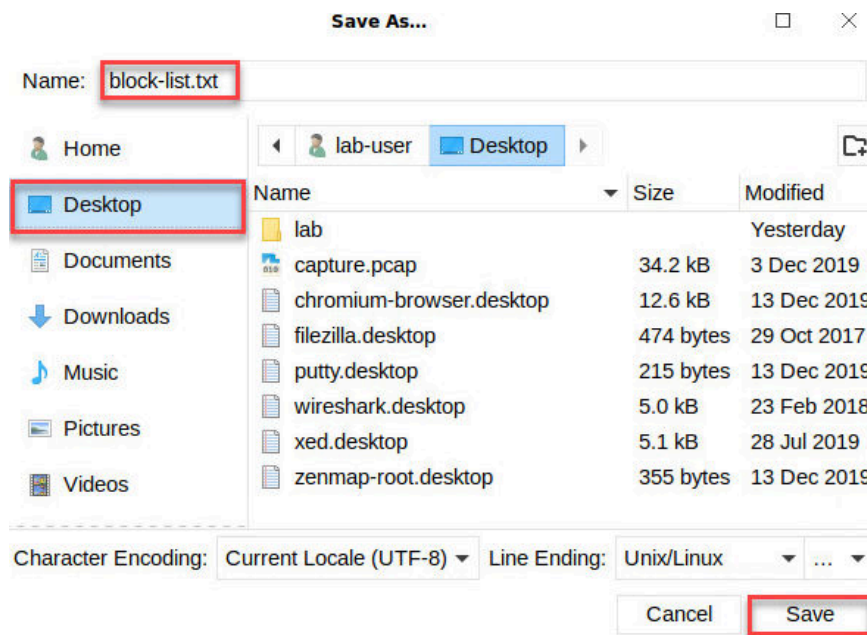
3. In the *Text Editor* window, type `yahoo.com` and `google.com`, each on a separate line.



4. In the *Text Editor* window, click on **File > Save As....**



- In the *Save As...* window, click on **Desktop** on the left. Then, type `block-list.txt` in the *Name* field. Next, click the **Save** button.

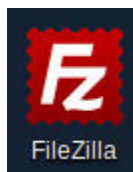


You will upload this file to the DMZ server. This file will be used by the Firewall to block the sites you listed.

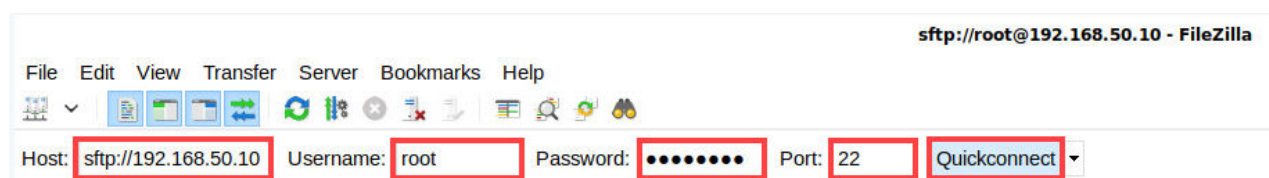
- Click the **X** in the upper-right corner to close the *Text Editor*.



- Double-click the **FileZilla** icon located on the desktop.



- In the *FileZilla* window, type `sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pa10A1t0!` for the *Password*. Lastly, type `22` for the *Port*. Then, click the **Quickconnect** button.



9. In the *Remember passwords?* window, select **Do not save passwords** and click **OK**.

Remember passwords?

Would you like FileZilla to remember passwords?

When allowing FileZilla to remember passwords, you can reconnect without having to re-enter a password after restarting FileZilla.

☐ Save passwords

☒ **Do not save passwords**

☐ Save passwords protected by a master password

Master password:

Repeat password:

A lost master password cannot be recovered! Please thoroughly memorize your password.

10. In the *FileZilla* window, from the dropdown menu, select **/<root>**, **home**, **lab-user**, and finally **Desktop**. Verify that **/home/lab-user/Desktop/** is correct in the *Local site* field.

Local site:

Local site:

▼

▼

▼

▶

11. In the *Remote site* window, navigate to **/var/www/html**. Lastly, verify that **/var/www/html** is in the *Remote site* field.

Remote site:

▼

▼

▼

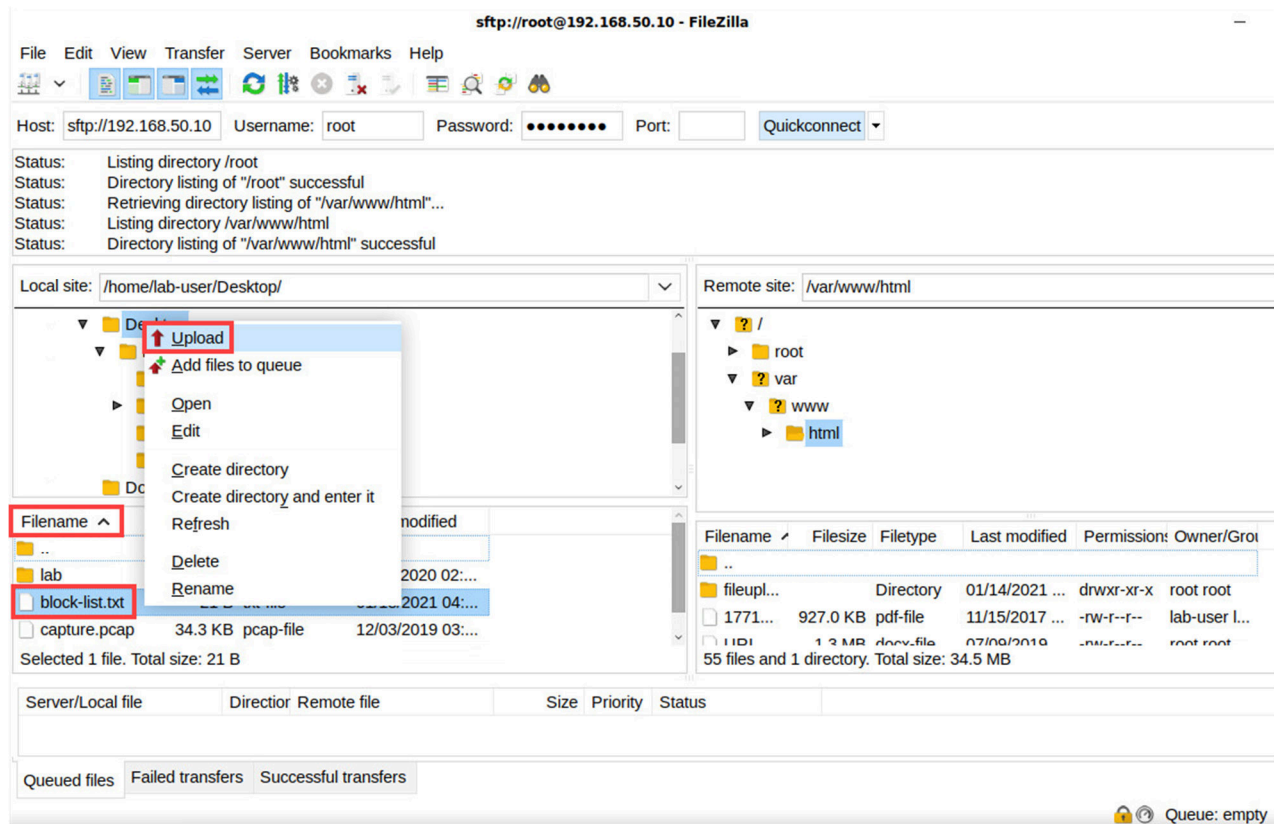
▼

▼

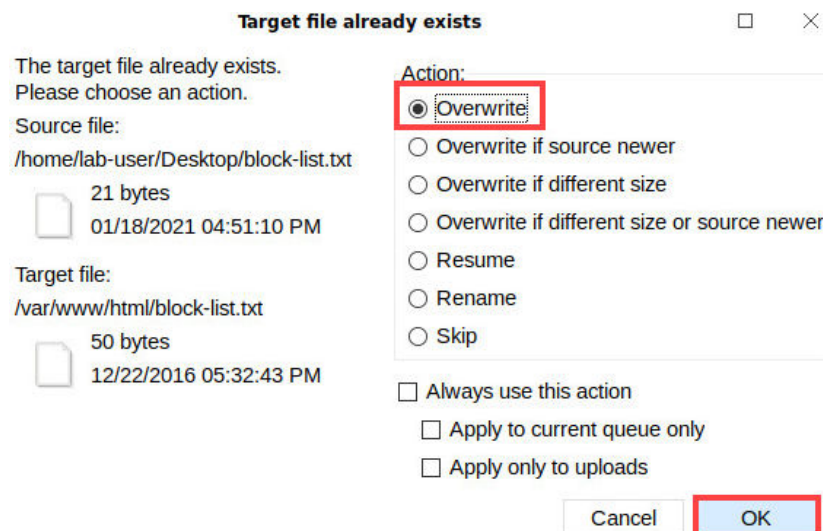
▼

▼

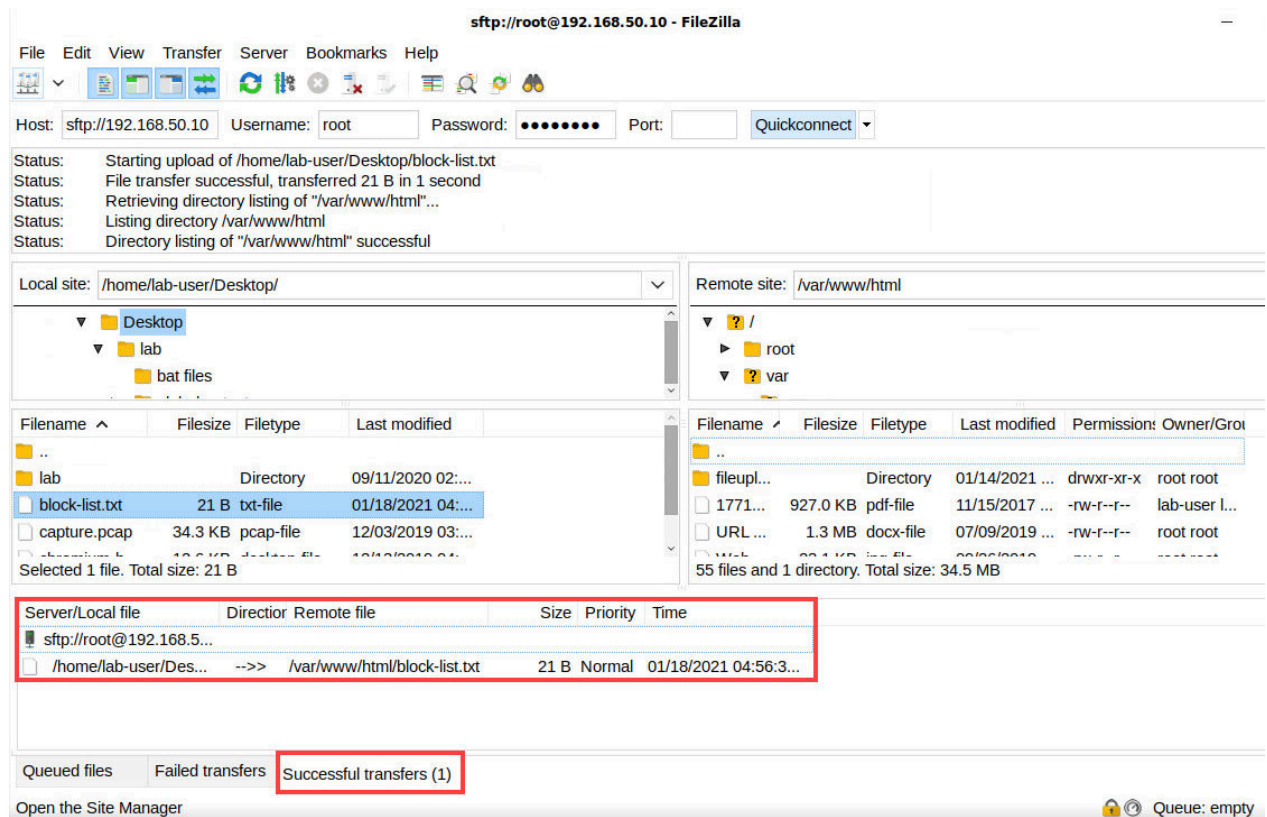
12. In the *Filename* tree, right-click the **block-list.txt** file. Click **Upload**.



13. In the *Target file already exists* window, ensure that **Overwrite** is selected and click **OK**.



- Click on the **Successful transfers** tab and verify that the transfers were successfully downloaded.



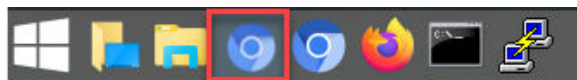
- Minimize *FileZilla* in the upper-right corner.



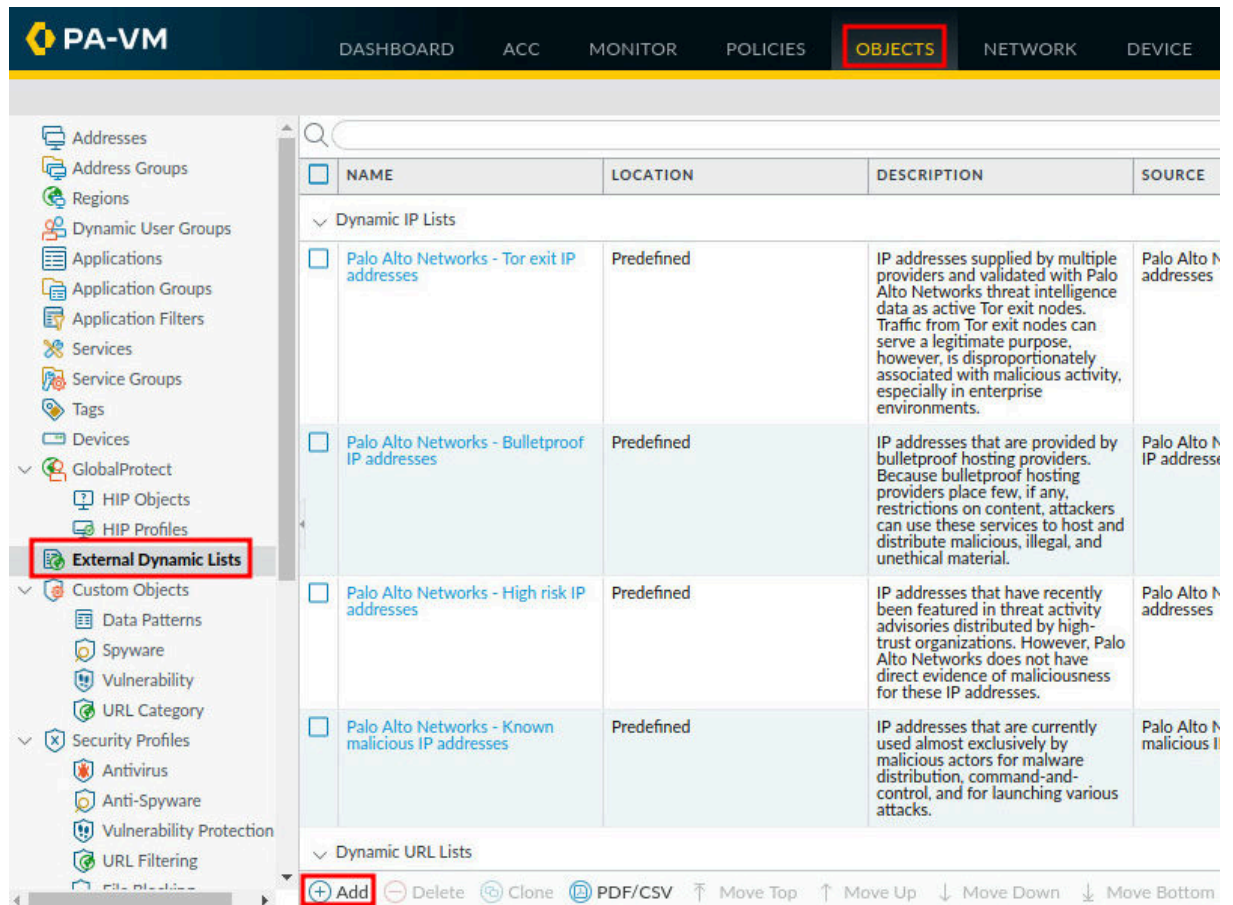
1.2 Create an External Dynamic List Object

In this section, you will create an External Dynamic List. An External Dynamic List is a text file (like the *block-list.txt* file you created) that is hosted on an external web server so that the Firewall can import objects such as IP addresses, URLs, and domains, to enforce policy.

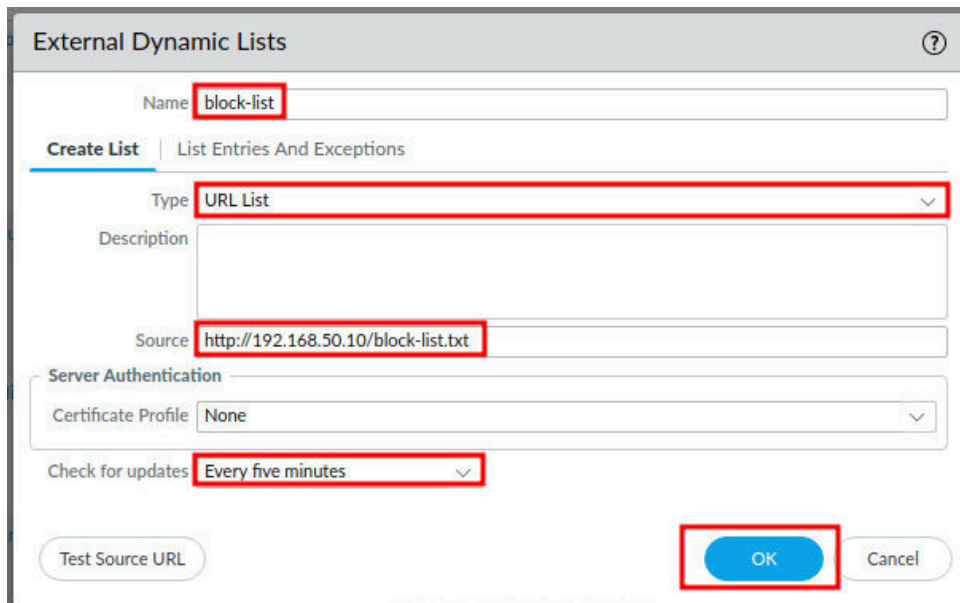
- Click on the **Chromium** icon from the taskbar to maximize the Firewall management interface.



2. Navigate to **Objects > External Dynamic Lists** and then click **Add**.



3. In the *External Dynamic Lists* window, type `block-list` for the *Name* field. Then, select **URL List** in the *Type* dropdown. Next, type `http://192.168.50.10/block-list.txt` in the *Source* field. Then, select **Every Five Minutes** from the *Check for updates* dropdown. Finally, click the **OK** button.



The screenshot shows the 'External Dynamic Lists' configuration window. The 'Name' field is set to 'block-list', 'Type' is 'URL List', 'Source' is 'http://192.168.50.10/block-list.txt', and 'Check for updates' is 'Every five minutes'. The 'OK' button is highlighted with a red box.



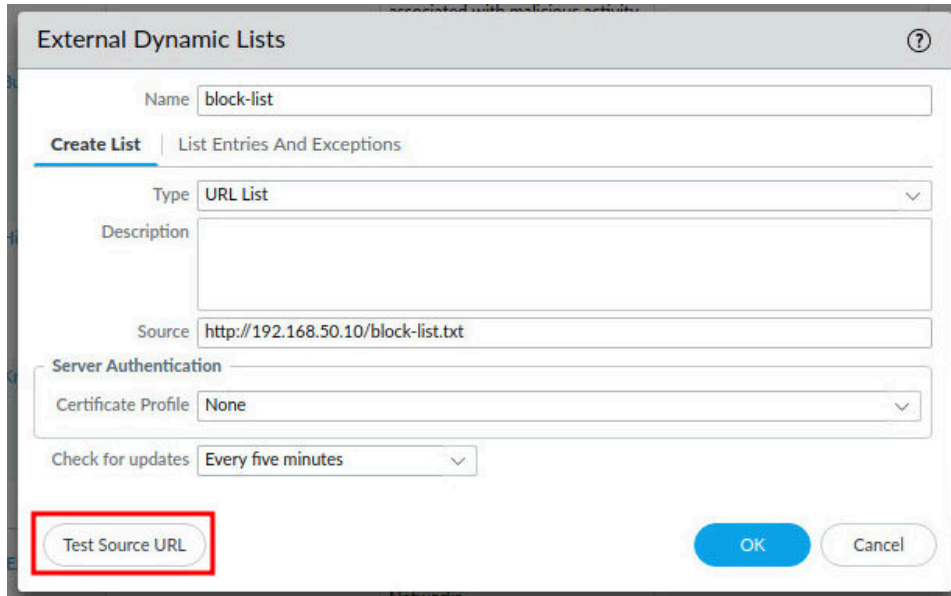
The IP address, **192.168.50.10**, refers to the DMZ server you uploaded the file to earlier. If the list is modified, the Firewall dynamically imports the list at the configured interval, in this case **Every Five Minutes**, and enforces policy without the need to make a configuration change or a commit on the Firewall. This is beneficial as the list could be changed by an administrator manually or, in some cases, by an automated script.

If you click **Test Source URL** in this step it will fail. You need to finish the External Dynamic List by clicking **OK** and proceeding to the next step.

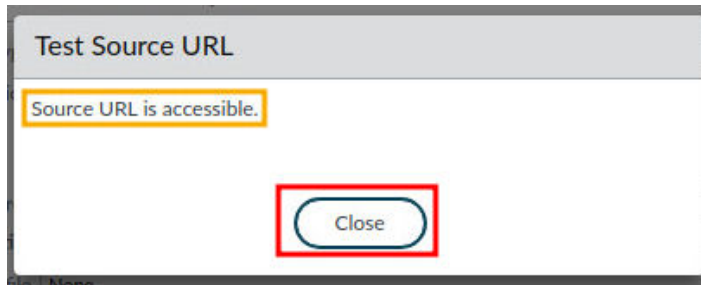
4. Click on the **block-list** object.

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	SOURCE
<input type="checkbox"/>			serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.	
<input type="checkbox"/>	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
<input type="checkbox"/>	Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
<input type="checkbox"/>	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
Dynamic URL Lists				
<input type="checkbox"/>	Palo Alto Networks - Authentication Portal Exclude List	Predefined	Domains and URLs to exclude from Authentication Policy. This list is managed by Palo Alto Networks.	Palo Alto Networks - Authentication Portal Exclude List
<input type="checkbox"/>	block-list			http://192.168.50.10/block-list.txt

5. In the *External Dynamic Lists* window, click on the **Test Source URL** button to test the URL source.

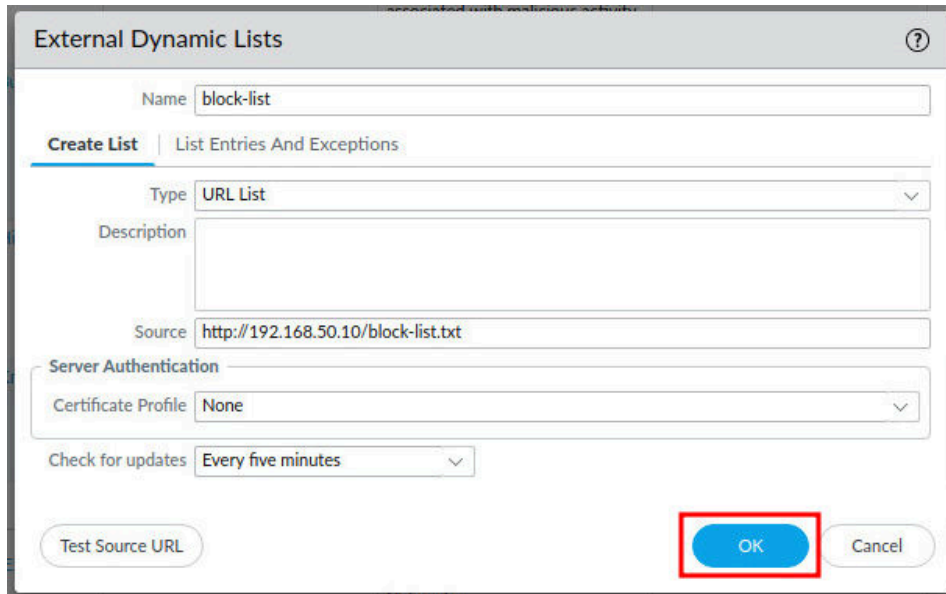


6. In the *Test Source URL* window, click the **Close** button. Verify that the **Source URL is accessible**.



This is an important step to verify that the Firewall can reach the URL. If the web server is unreachable, the Firewall will use the last successfully-retrieved list for enforcing policy until the connection is restored with the web server.

7. In the *External Dynamic Lists* window, click the **OK** button.



External Dynamic Lists

Name

Create List | List Entries And Exceptions

Type

Description

Source

Server Authentication

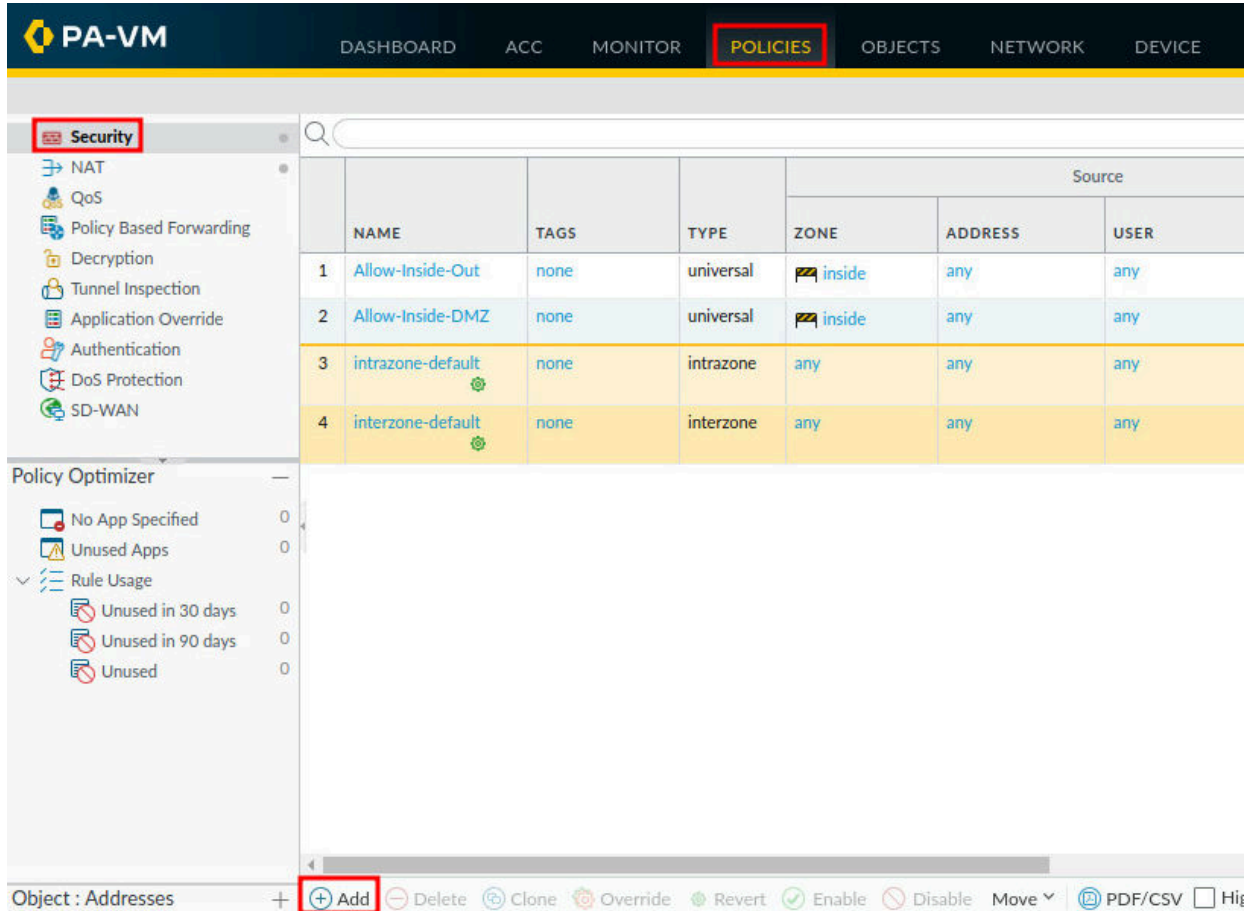
Certificate Profile

Check for updates

1.3 Create a Security Policy

In this section, you will create a new Security Policy that utilizes the External Dynamic List you created to filter traffic.

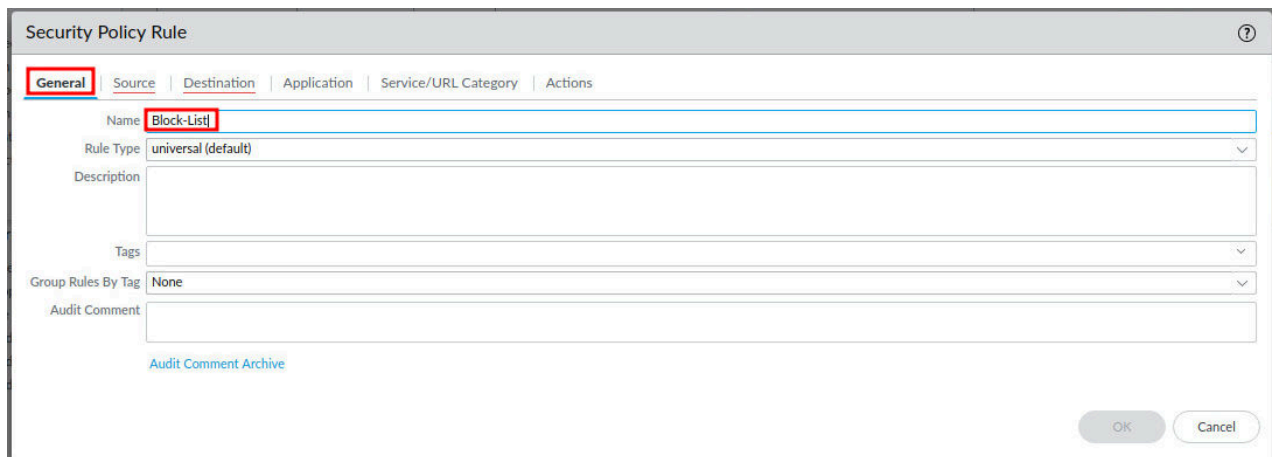
1. Navigate to **Policies > Security** and click **Add**.



	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	Allow-Inside-Out	none	universal	inside	any	any
2	Allow-Inside-DMZ	none	universal	inside	any	any
3	intrazone-default	none	intrazone	any	any	any
4	interzone-default	none	interzone	any	any	any

Object : Addresses + **Add** Delete Clone Override Revert Enable Disable Move PDF/CSV Hig

2. In the *Security Policy Rule* window, type **Block-List** in the *Name* field.



Security Policy Rule

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

Name: **Block-List**

Rule Type: universal (default)

Description:

Tags:

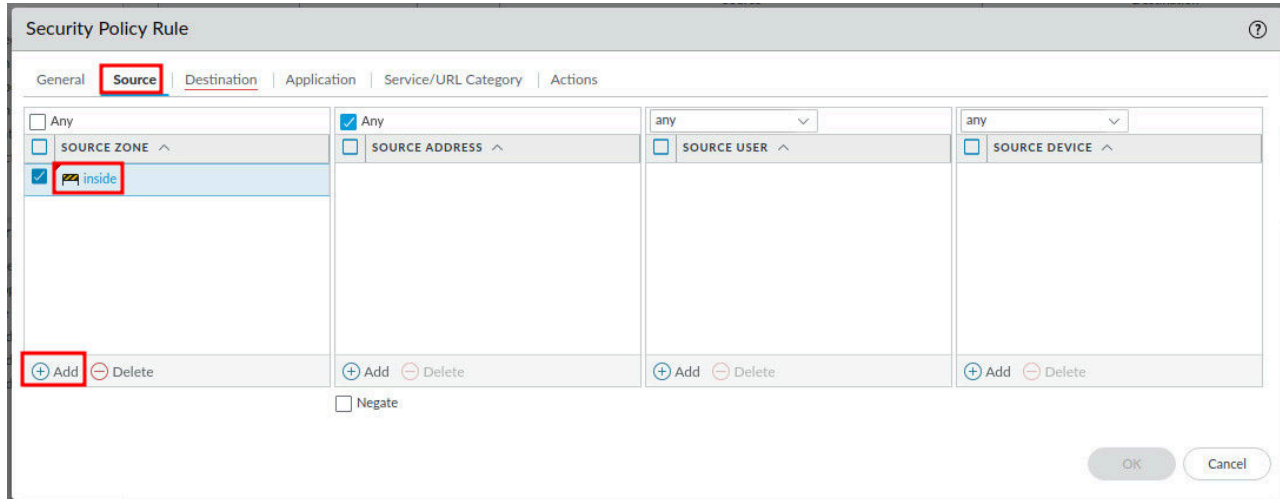
Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

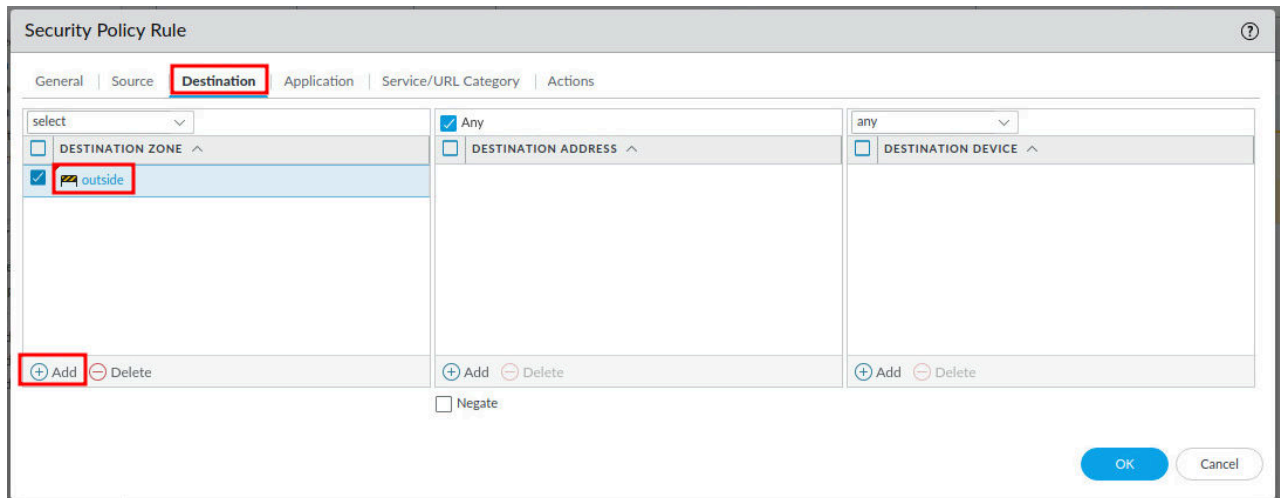
OK Cancel

3. In the *Security Policy Rule* window, click the **Source** tab. Then, click the **Add** button in the *Source Zone* section. Next, select **inside** in the *Source Zone* column.



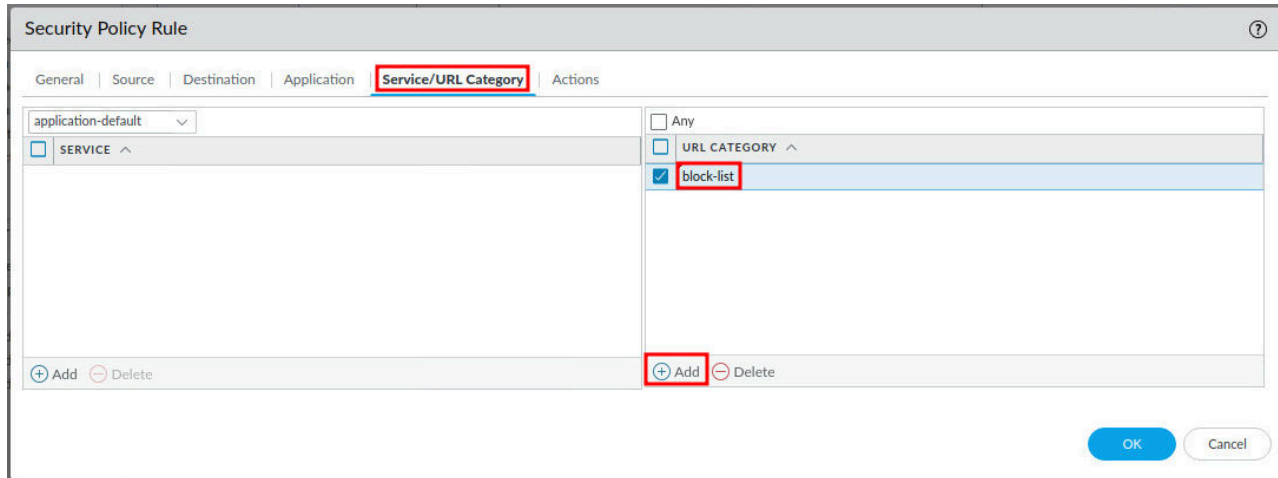
The screenshot shows the 'Security Policy Rule' window with the 'Source' tab selected. The 'SOURCE ZONE' section has a red box around the 'Add' button and another red box around the 'inside' option in the dropdown menu. The 'SOURCE ADDRESS', 'SOURCE USER', and 'SOURCE DEVICE' sections are empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

4. In the *Security Policy Rule* window, click the **Destination** tab. Then, click the **Add** button in the *Destination Zone* section. Next, select **outside** in the *Destination Zone* column.



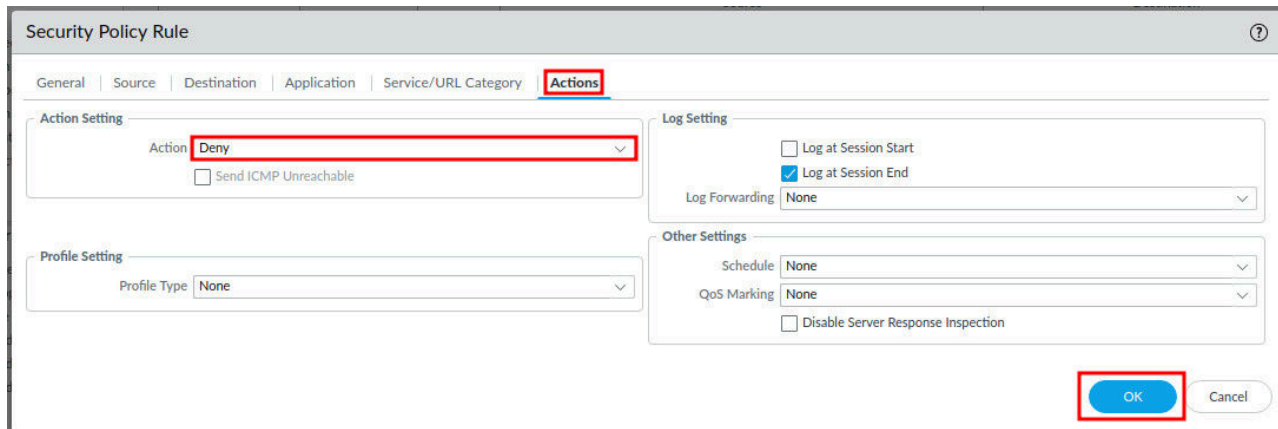
The screenshot shows the 'Security Policy Rule' window with the 'Destination' tab selected. The 'DESTINATION ZONE' section has a red box around the 'Add' button and another red box around the 'outside' option in the dropdown menu. The 'DESTINATION ADDRESS' and 'DESTINATION DEVICE' sections are empty. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

5. In the *Security Policy Rule* window, click the **Service/URL Category** tab. Then, click the **Add** button in the *URL Category* section. Next, select **block-list**.



The screenshot shows the 'Security Policy Rule' window with the 'Service/URL Category' tab selected. The 'URL CATEGORY' section is expanded, and the 'block-list' option is selected. The 'Add' button in the bottom right of the 'URL CATEGORY' section is highlighted with a red box. The 'OK' button is also highlighted with a red box.

6. In the *Security Policy Rule* window, click the **Actions** tab. Then, select **Deny** in the *Action* dropdown. Next, click the **OK** button.







The screenshot shows the 'Security Policy Rule' window with the 'Actions' tab selected. The 'Action' dropdown is set to 'Deny'. The 'Log at Session End' checkbox is checked. The 'OK' button is highlighted with a red box.

7. Click on **3** to select the **Block-List** rule. Then, click the **Move** button at the bottom. Next, select **Move Top**.

Search:

	NAME	TAGS	TYPE	Source			
				ZONE	ADDRESS	USER	DEVICE
1	Allow-Inside-Out	none	universal	inside	any	any	any
2	Allow-Inside-DMZ	none	universal	inside	any	any	any
3	Block-List	none	universal	inside	any	any	any
4	intrazone-default	none	intrazone	any	any	any	any
5	interzone-default	none	interzone	any	any	any	any

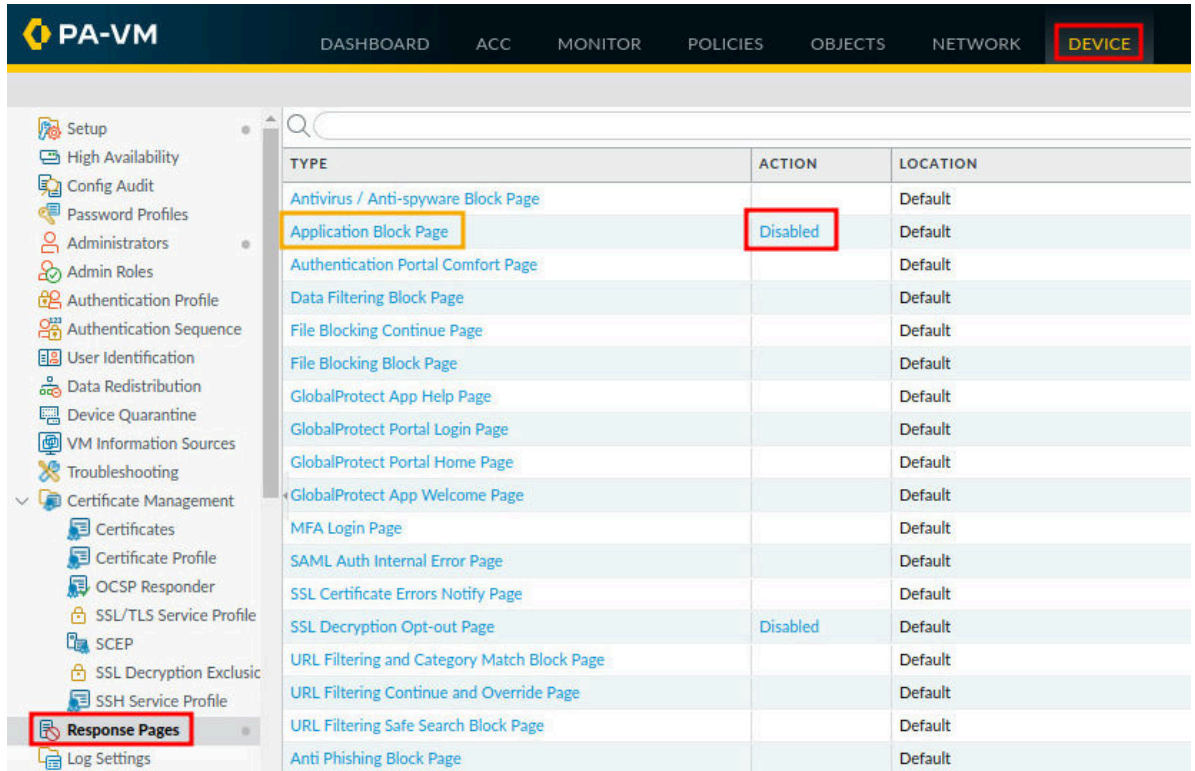
 Move Top
 Move Up
 Move Down
 Move Bottom

+ Add - Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused



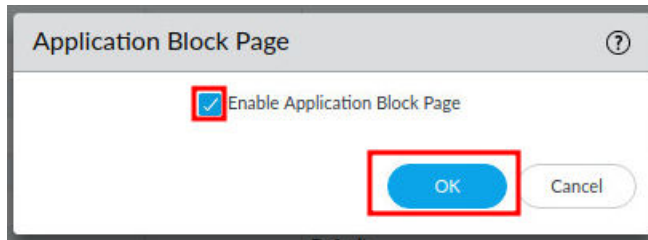
The order of the Security Policies is very important as traffic is matched in order from top to bottom. If **Block-List** were not moved to the top, traffic would have matched the **Allow-Inside-Out** policy first, allowing traffic listed in the **Block-List** to pass.

8. Navigate to **Device > Response Pages** and click **Disabled** in the *Action* column to enable the **Application Block Page**.



TYPE	ACTION	LOCATION
Antivirus / Anti-spyware Block Page		Default
Application Block Page	Disabled	Default
Authentication Portal Comfort Page		Default
Data Filtering Block Page		Default
File Blocking Continue Page		Default
File Blocking Block Page		Default
GlobalProtect App Help Page		Default
GlobalProtect Portal Login Page		Default
GlobalProtect Portal Home Page		Default
GlobalProtect App Welcome Page		Default
MFA Login Page		Default
SAML Auth Internal Error Page		Default
SSL Certificate Errors Notify Page		Default
SSL Decryption Opt-out Page	Disabled	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

9. In the *Application Block Page* window, click **Enable Application Block Page**. Lastly, Click **OK**.



Application Block Page

☒ Enable Application Block Page

OK Cancel

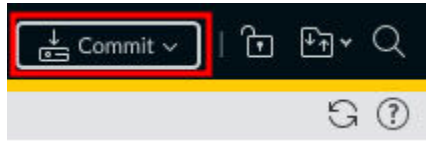
**Please
Note**

Application Block Page is used to block applications by a security policy rule.

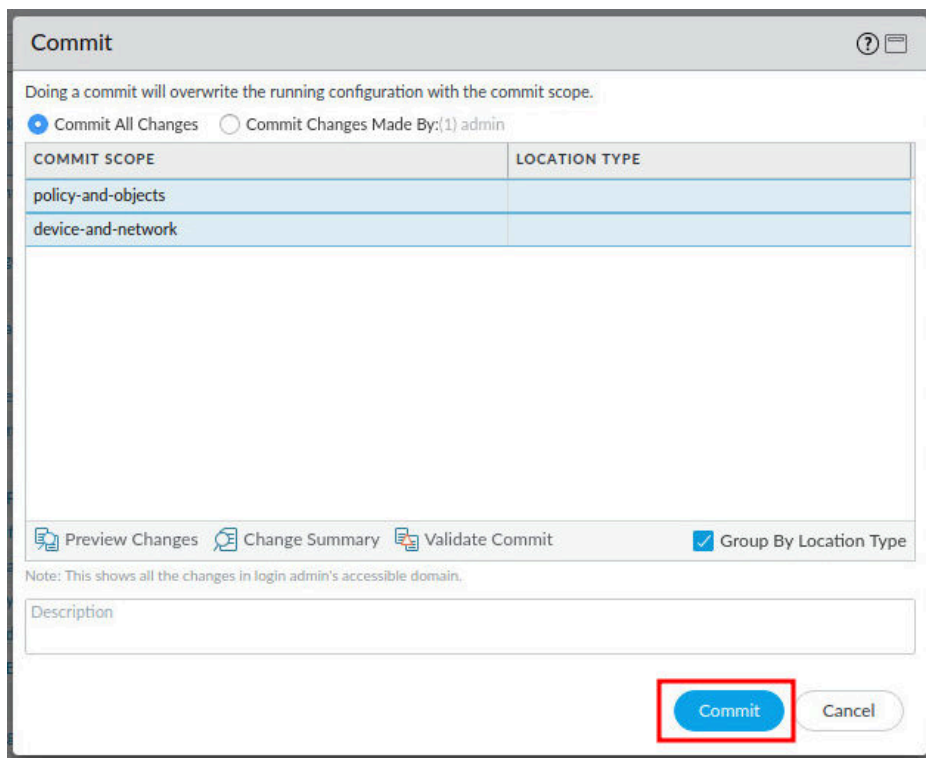
1.4 Commit and Test

In this section, you will commit your changes to the Firewall and test traffic matching the **Block-List** Security Policy.

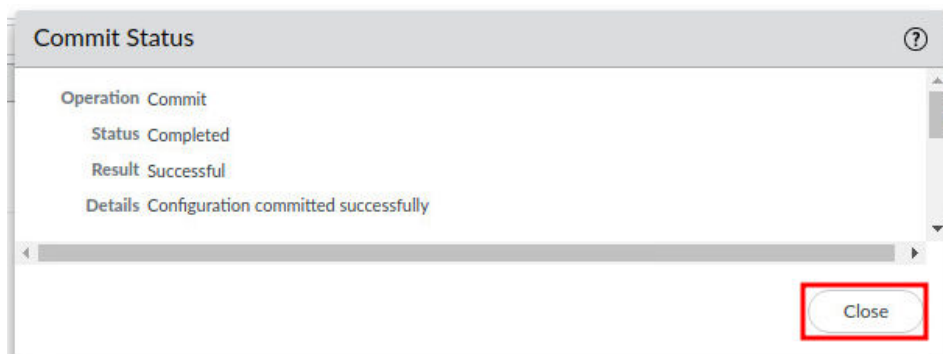
1. Click the **Commit** link located at the top-right of the web interface.



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



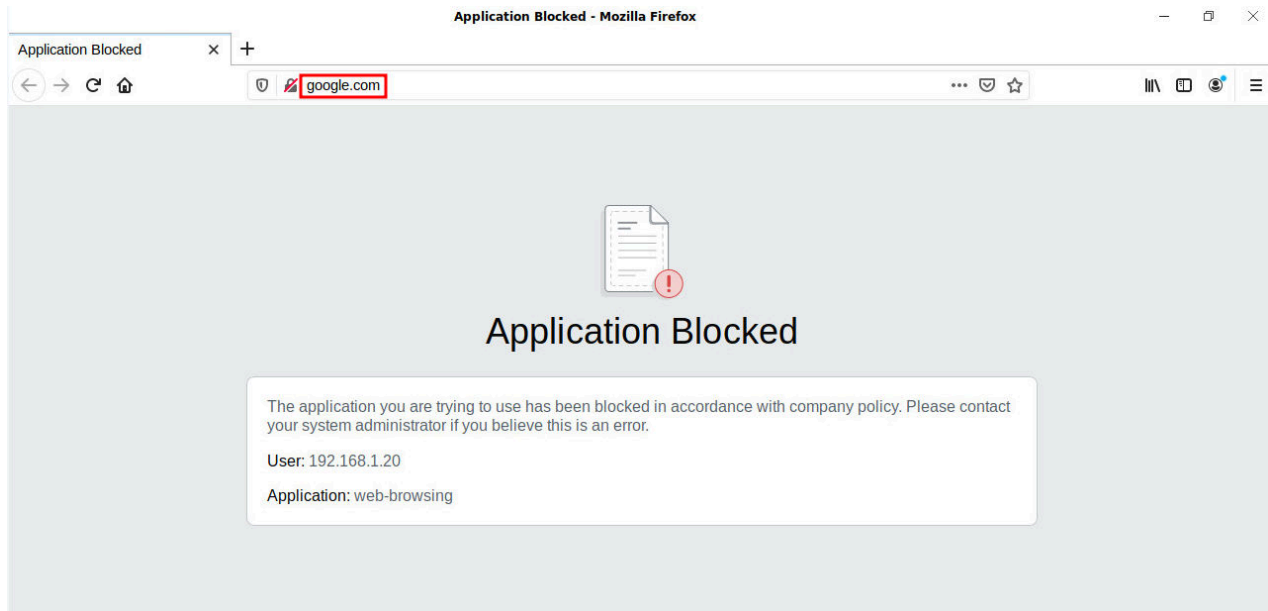
3. When the commit operation successfully completes, click **Close** to continue.



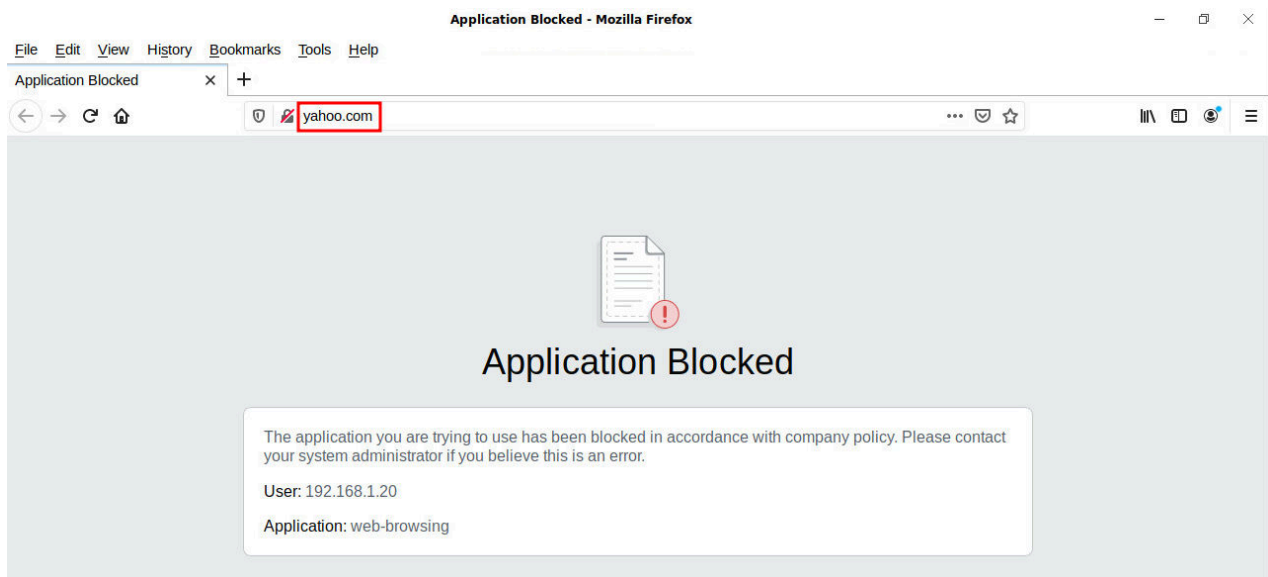
4. Open **Firefox** from the taskbar.



5. In the address bar, type `http://google.com` and press **Enter**.

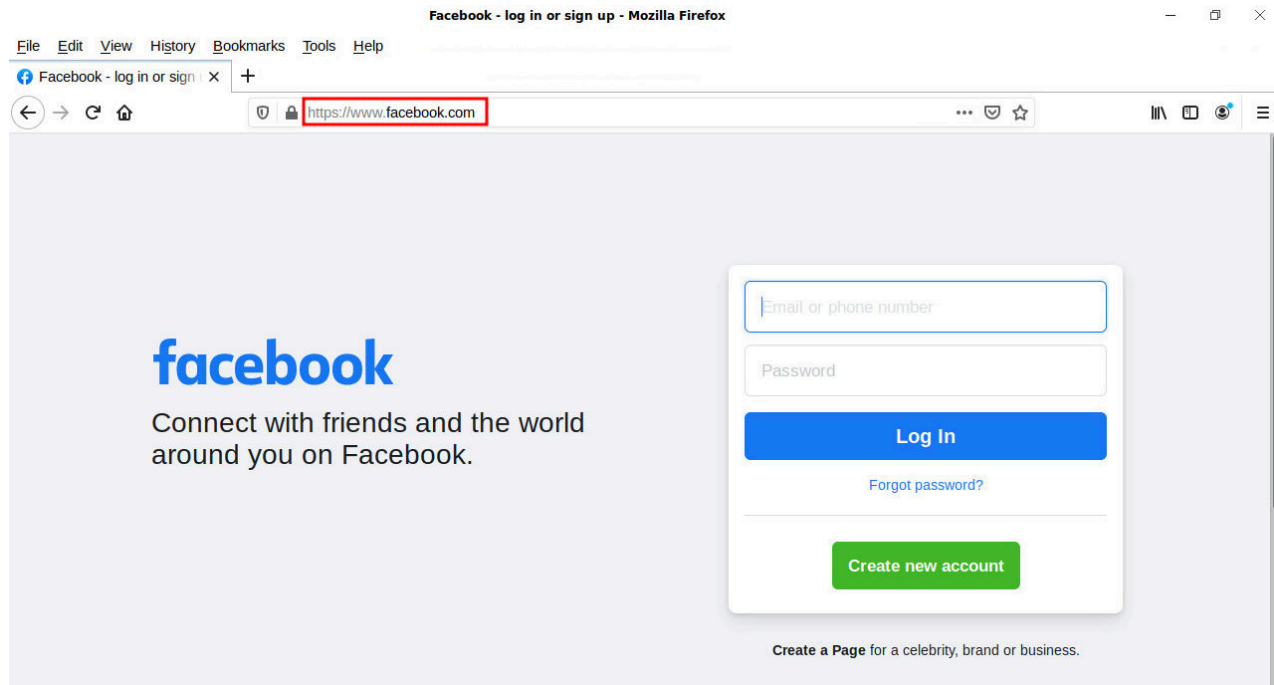


6. In the address bar, type `http://yahoo.com` and press **Enter**.



Due to the *Dynamic Block Lists*, you cannot get to **google.com** or **yahoo.com**.

7. In the address bar, type `https://www.facebook.com` and press **Enter**.



Here, the traffic did not match the Security Policy **Block-List**. Instead, it matched the next policy, **Allow-Inside-Out**.

8. The lab is now complete; you may end the reservation.