PAN9 CYBERSECURITY ESSENTIALS

Lab 10: Using Dynamic Block Lists

Document Version: 2020-06-08

Contents

Introduction

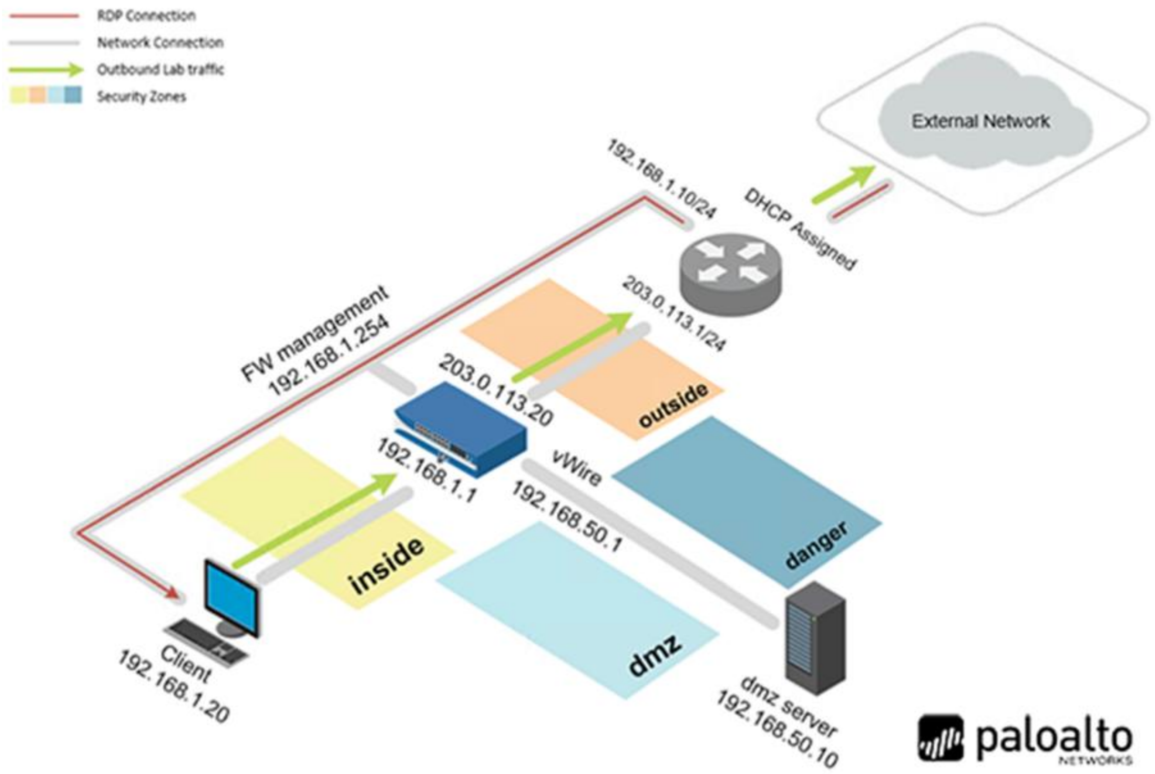
In this lab, you will configure a security policy to use a dynamic block list.

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.

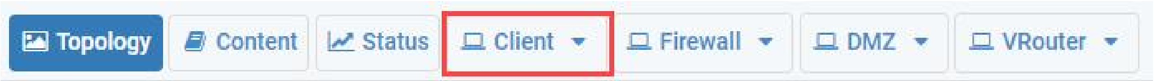
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

10 Lab: Using Dynamic Block Lists

10.0 Load Lab Configuration

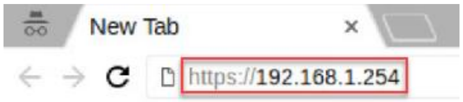
In this section, you will load the Firewall configuration file.

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

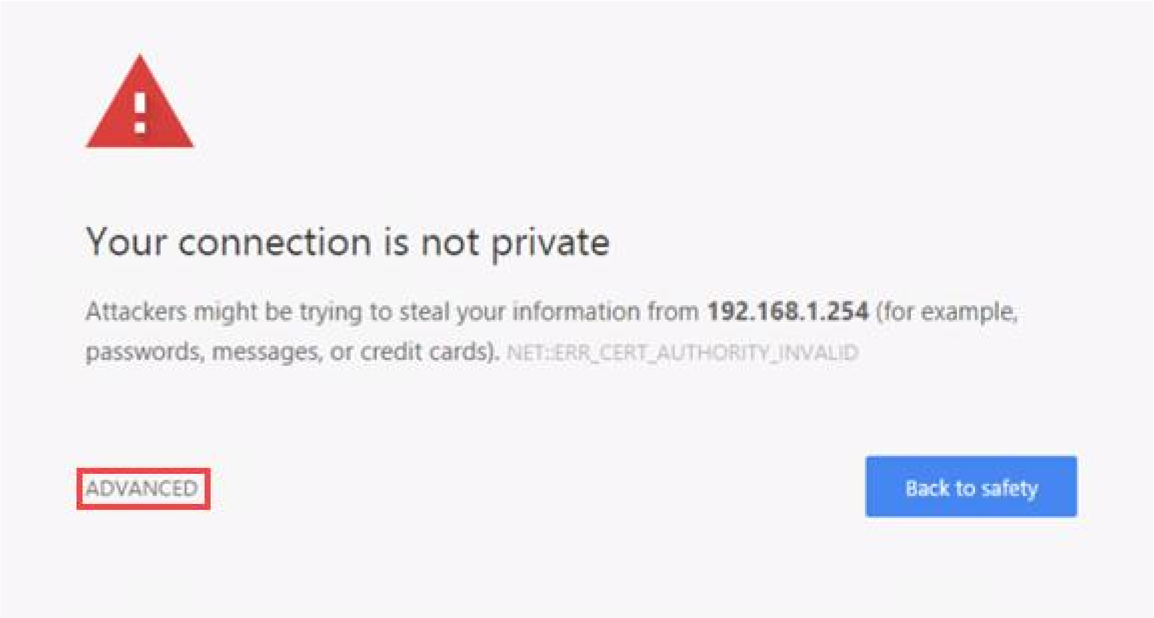


2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.

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.

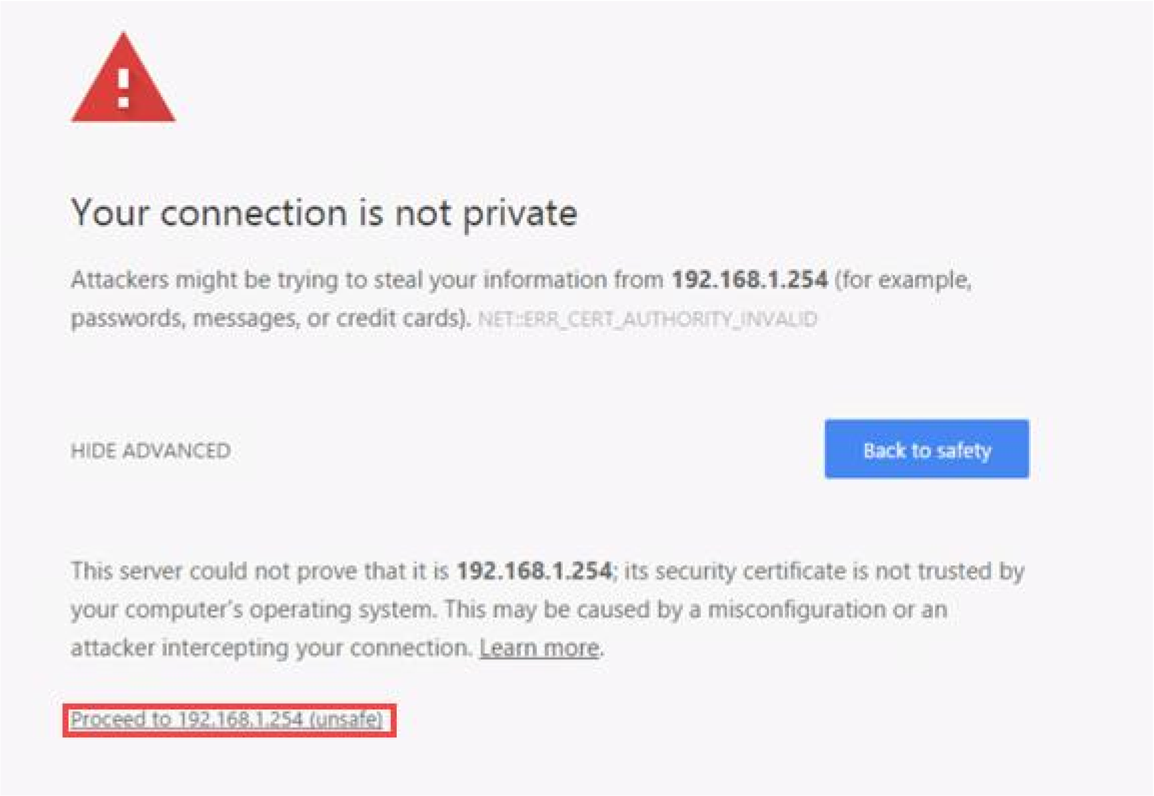


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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.

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

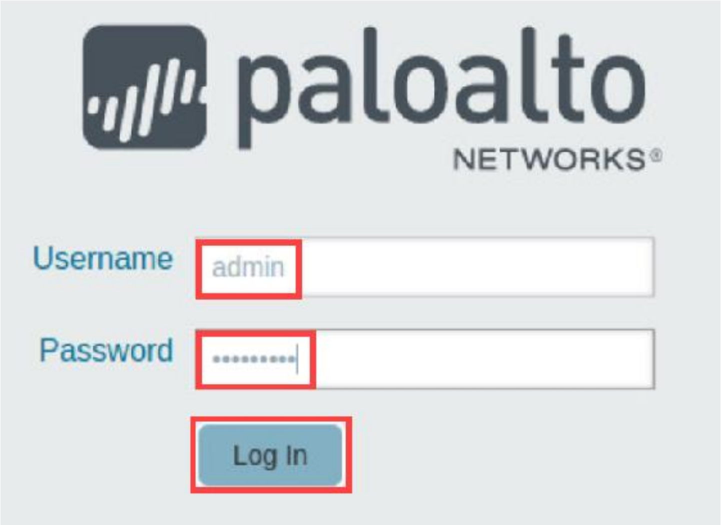


Your connection is not private

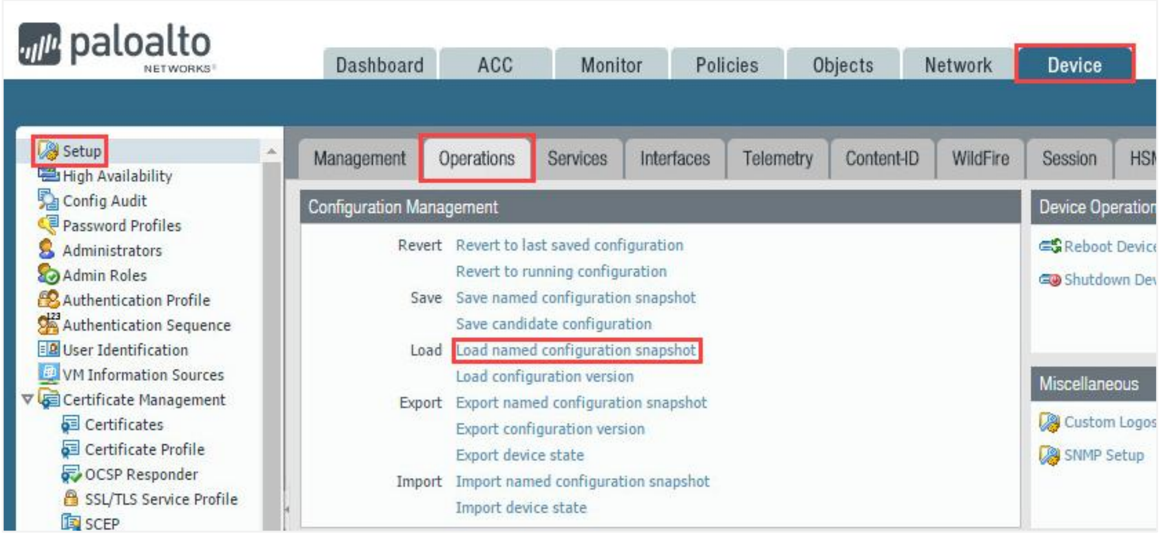
Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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. Learn more.

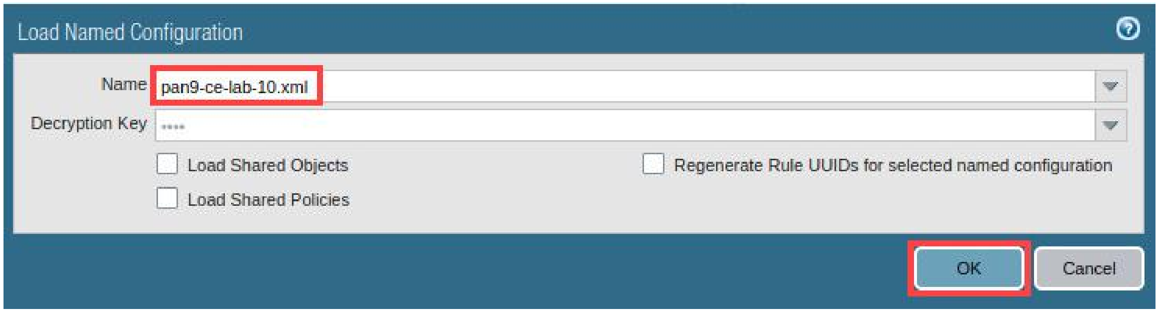
7. Log in to the Firewall web interface as username `admin`, password `Train1ng$`.



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



9. In the *Load Named Configuration* window, select **pan9-ce-lab-10.xml** from the *Name* dropdown box and click **OK**.



Load Named Configuration

Name: pan9-ce-lab-10.xml

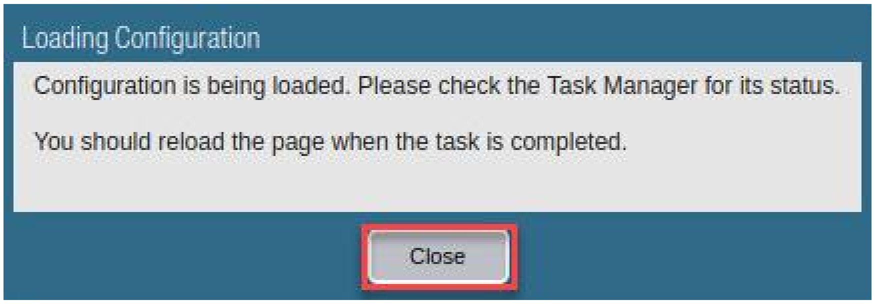
Decryption Key: ••••

□ Load Shared Objects

□ Load Shared Policies

□ Regenerate Rule UUIDs for selected named configuration

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.

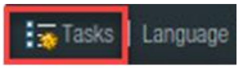


Loading Configuration

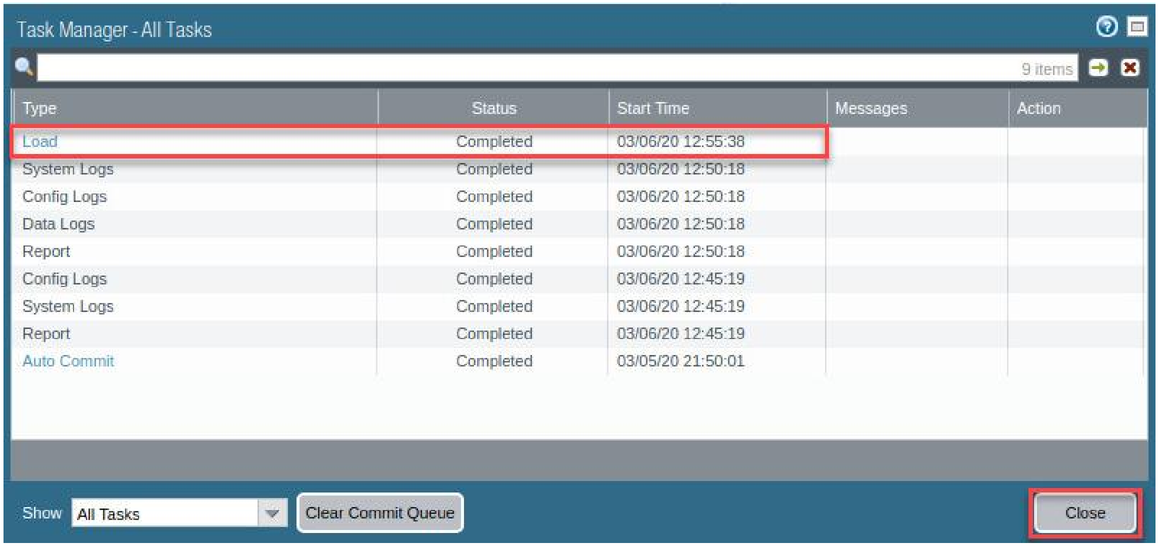
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



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



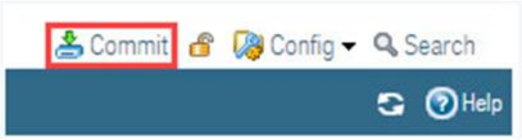
Task Manager - All Tasks

9 items

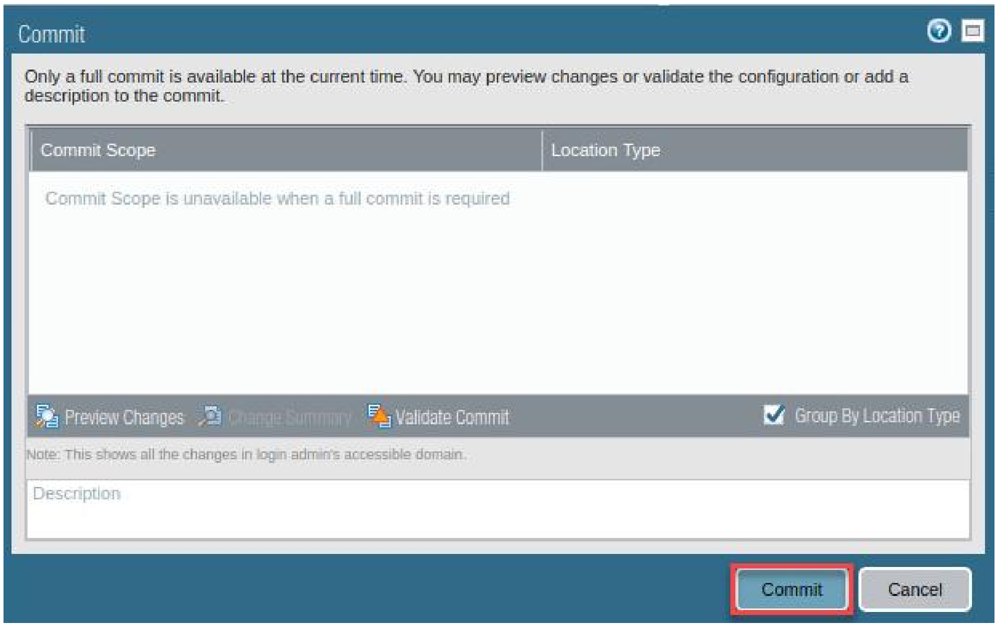
Type	Status	Start Time	Messages	Action
Load	Completed	03/06/20 12:55:38		
System Logs	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:50:18		
Data Logs	Completed	03/06/20 12:50:18		
Report	Completed	03/06/20 12:50:18		
Config Logs	Completed	03/06/20 12:45:19		
System Logs	Completed	03/06/20 12:45:19		
Report	Completed	03/06/20 12:45:19		
Auto Commit	Completed	03/05/20 21:50:01		

Show: All Tasks

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



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

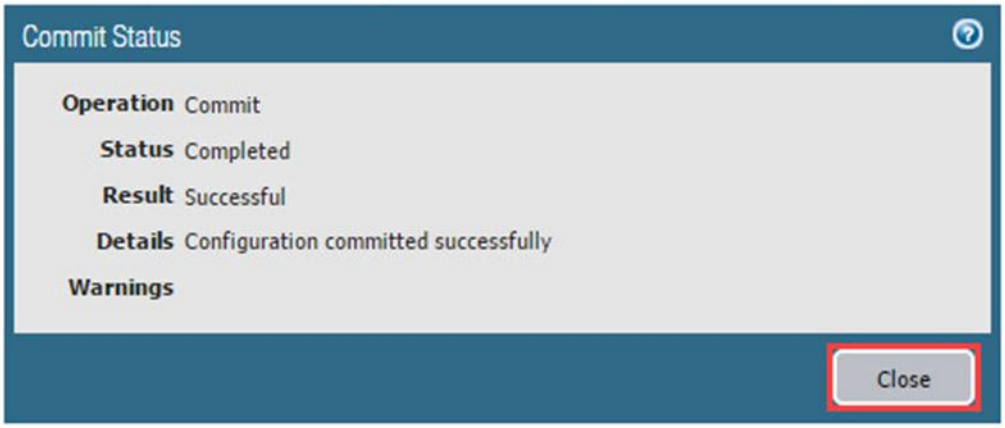

Commit

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

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

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

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


Commit Status

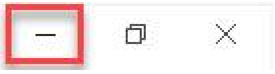
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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.

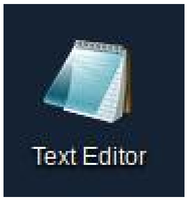
10.1 Create a List of Blocked Sites and Upload to DMZ Server

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

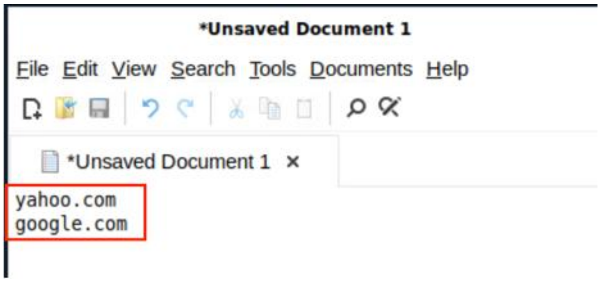
1. Minimize **Chromium** in the upper-right.



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

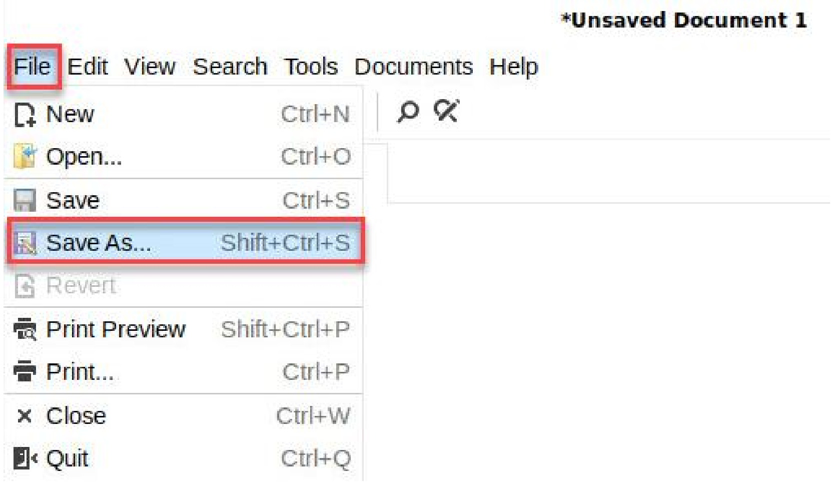


3. In the *Text Editor* window, type `yahoo.com` and `google.com`, each on a separate line.

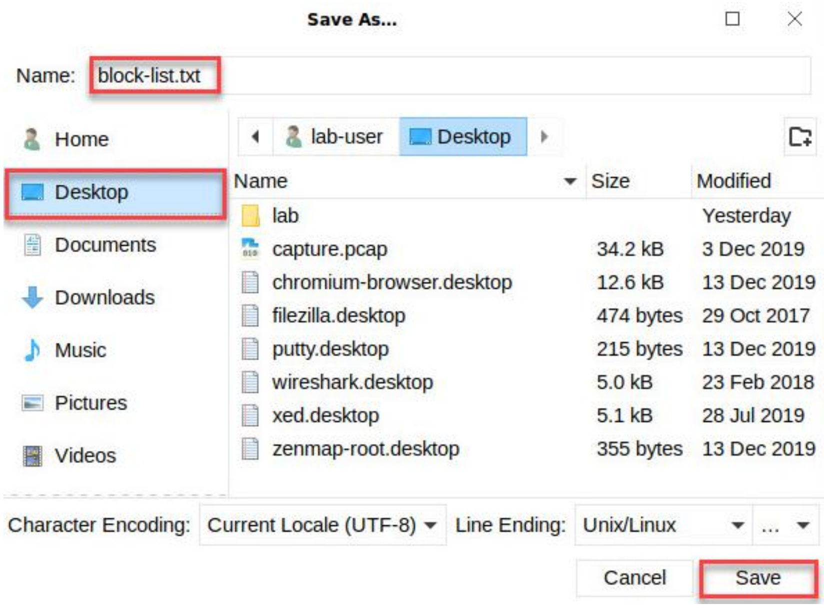


```
yahoo.com
google.com
```

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



5. 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.



Save As...

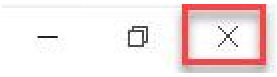
Name: block-list.txt

Name	Size	Modified
lab		Yesterday
capture.pcap	34.2 kB	3 Dec 2019
chromium-browser.desktop	12.6 kB	13 Dec 2019
filezilla.desktop	474 bytes	29 Oct 2017
putty.desktop	215 bytes	13 Dec 2019
wireshark.desktop	5.0 kB	23 Feb 2018
xed.desktop	5.1 kB	28 Jul 2019
zenmap-root.desktop	355 bytes	13 Dec 2019

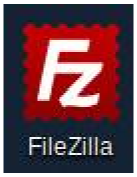
Character Encoding: Current Locale (UTF-8) Line Ending: Unix/Linux

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

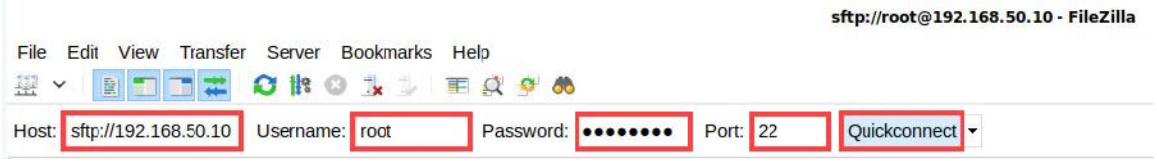
6. Click the **X** in the upper-right to close the *Text Editor*.



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



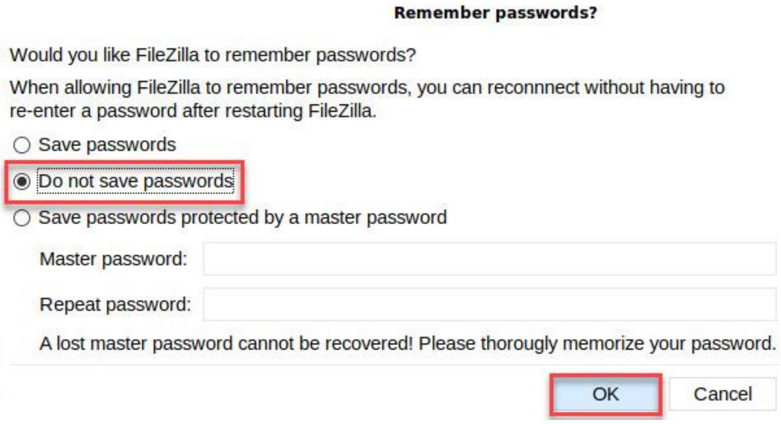
8. In the *FileZilla* window, `type sftp://192.168.50.10` for the *Host*, type `root` for the *Username*, type `Pal0Alt0` for the *Password*. Lastly, type 22 for the *Port*. Then, click the **Quickconnect** button.



sftp://root@192.168.50.10 - FileZilla

Host: sftp://192.168.50.10 Username: root Password: •••••••• Port: 22

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 reconnnect without having to re-enter a password after restarting FileZilla.

○ Save passwords

● Do not save passwords

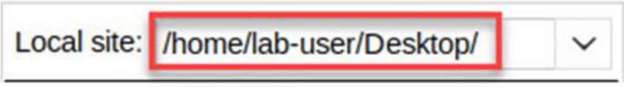
○ Save passwords protected by a master password

Master password:

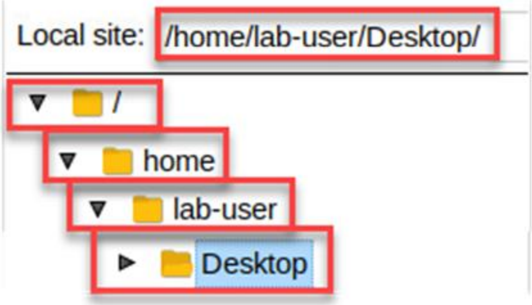
Repeat password:

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

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

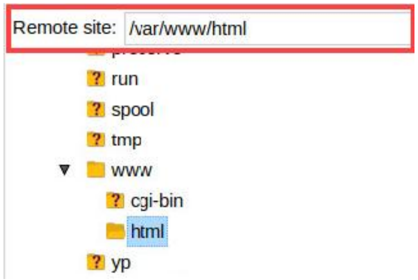


Local site: /home/lab-user/Desktop/



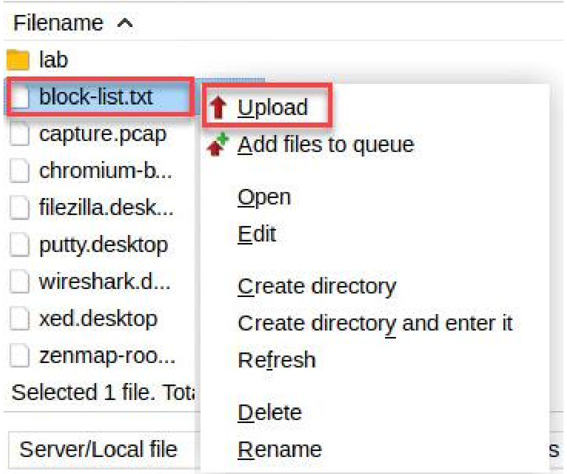
Local site: /home/lab-user/Desktop/

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

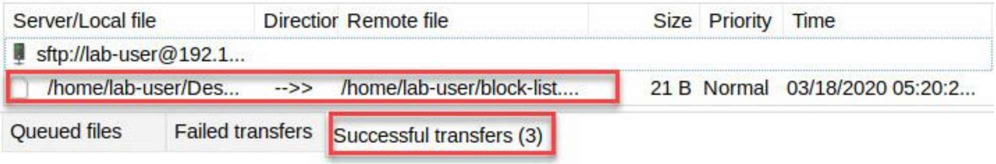


Remote site: /var/www/html

12. Right-click on the **block-list.txt** file in the *Filename* tree and lastly, click **Upload**.

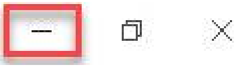


13. Click on the **Successful transfers** tab and verify the transfers were successfully downloaded.



Server/Local file	Directior	Remote file	Size	Priority	Time
sftp://lab-user@192.1...					
/home/lab-user/Des...	-->>	/home/lab-user/block-list....	21 B	Normal	03/18/2020 05:20:2...

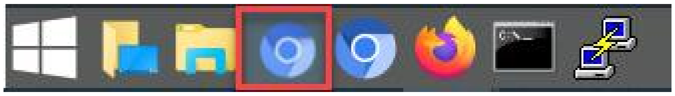
14. Minimize **FileZilla** in the upper-right.



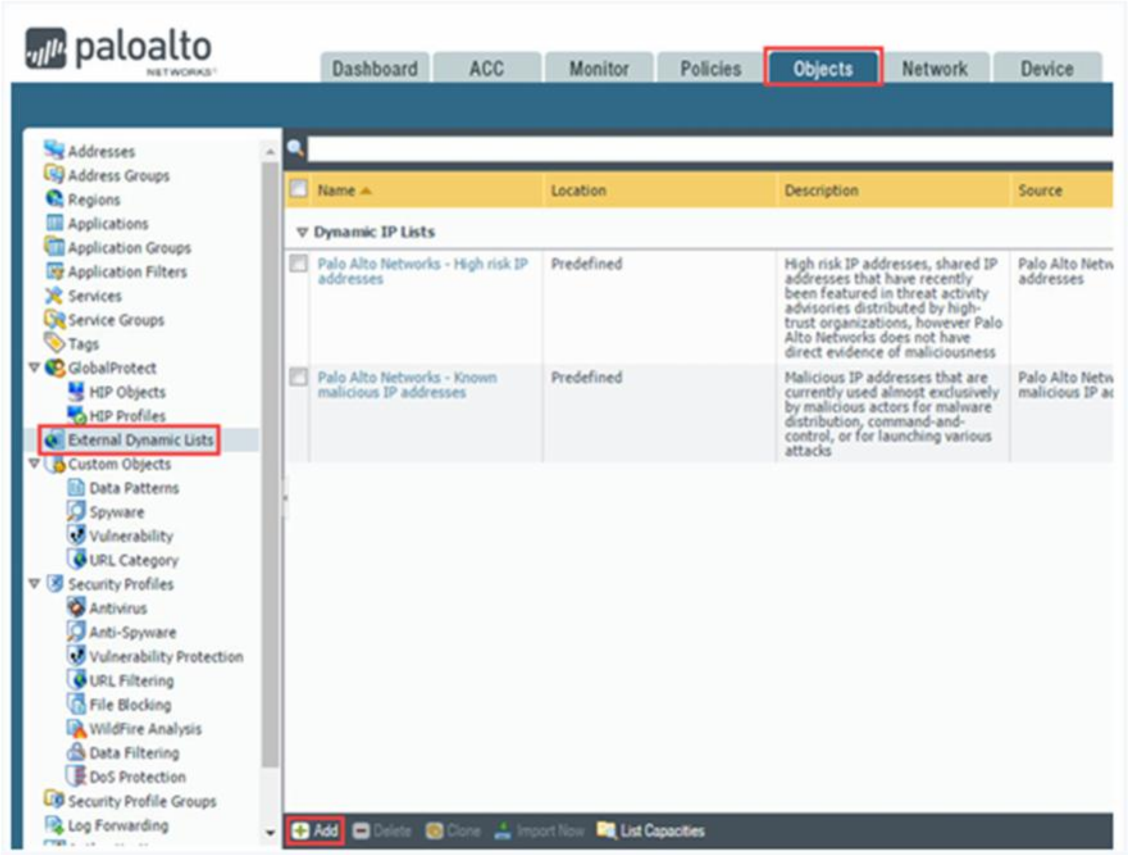
10.2 Create an External Dynamic List Object

In this section, you will create an External Dynamic List. An External Dynamic List is a text file, such as 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.

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

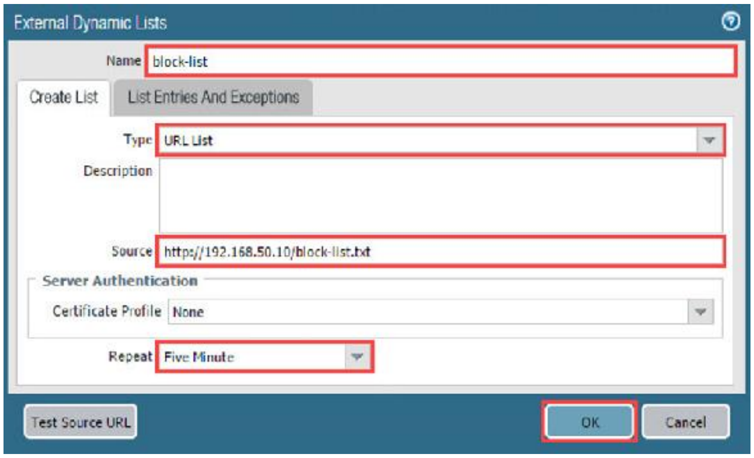


2. Navigate to **Objects > External Dynamic Lists > Add**.



Name	Location	Description	Source
Dynamic IP Lists			
Palo Alto Networks - High risk IP addresses	Predefined	High risk IP addresses, shared 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	Palo Alto Netw addresses
Palo Alto Networks - Known malicious IP addresses	Predefined	Malicious IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, or for launching various attacks	Palo Alto Netw malicious IP ad

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 **Five Minute** on the *Repeat* dropdown. Finally, click the **OK** button.



Name: block-list

Type: URL List

Description:

Source: https://192.168.50.10/block-list.txt

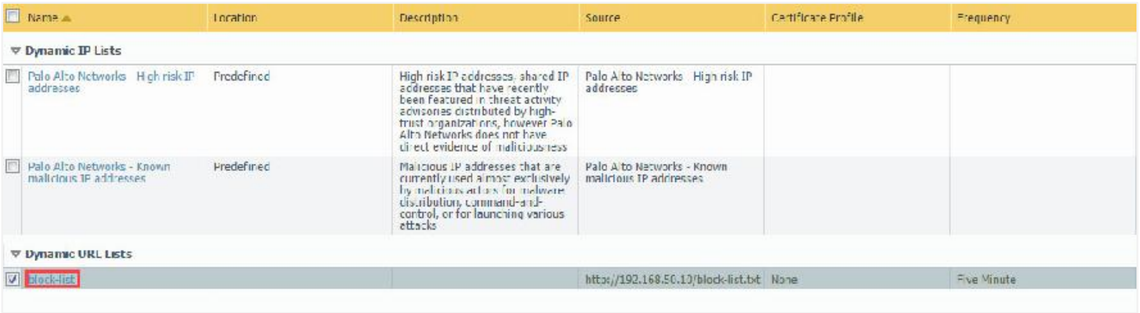
Certificate Profile: None

Repeat: Five Minute

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 **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 changing by an administrator manually or, in some cases, an automated script.

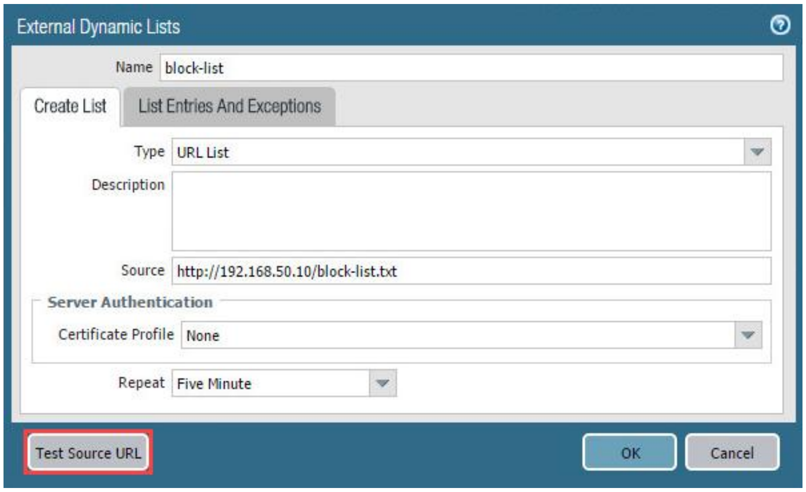
If you click **Test Source URL** in this step it will fail. You need to finish the External Dynamic List by clicking ok and proceeding to the next step.

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



□	Name	Location	Description	Source	Certificate Profile	Frequency
	Dynamic IP Lists					
□	Palo Alto Networks High risk IP addresses	Predefined	High risk IP addresses, shared 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	Palo Alto Networks High risk IP addresses		
□	Palo Alto Networks - Known malicious IP addresses	Predefined	Malicious IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, or for launching various attacks	Palo Alto Networks - Known malicious IP addresses		
	Dynamic URL Lists					
☑	block-list			http://192.168.50.10/block-list.txt	None	Five Minute

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



External Dynamic Lists

Name: block-list

Type: URL List

Description:

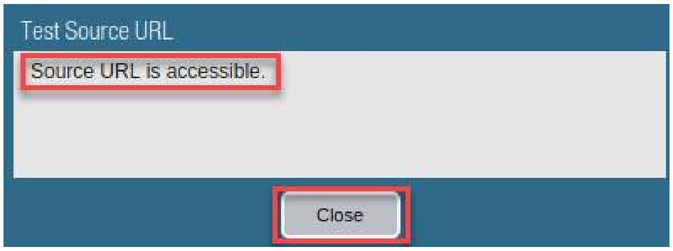
Source: http://192.168.50.10/block-list.txt

Server Authentication

Certificate Profile: None

Repeat: Five Minute

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

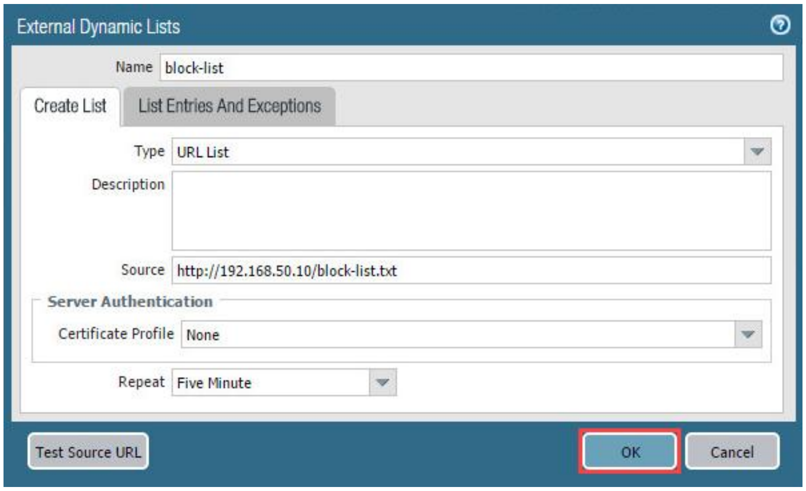


Test Source URL

Source URL is accessible.

This is an important step to verify 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: block-list

Create List | List Entries And Exceptions

Type: URL List

Description:

Source: http://192.168.50.10/block-list.txt

Server Authentication

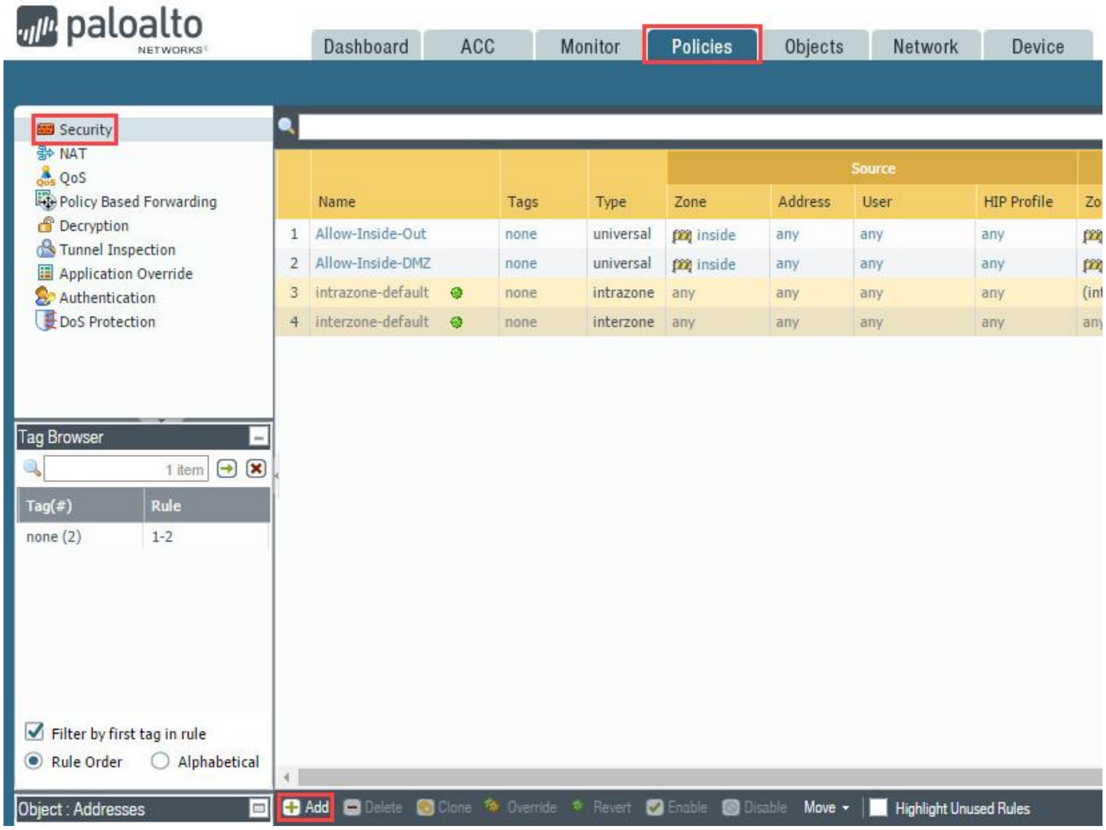
Certificate Profile: None

Repeat: Five Minute

10.3 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.

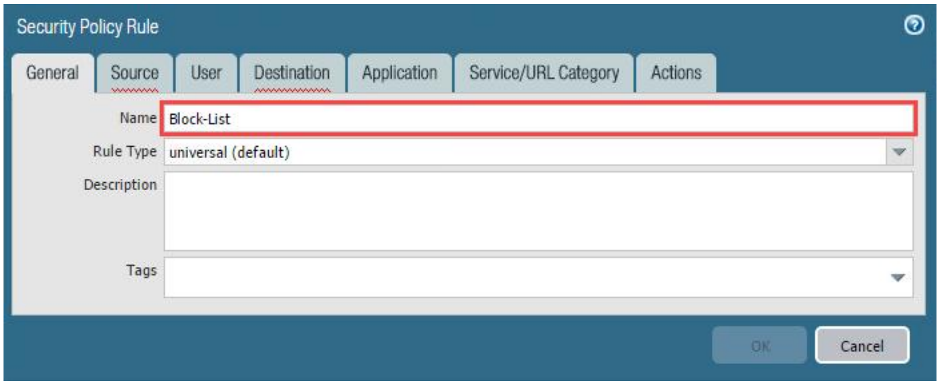
1. Navigate to **Policies > Security > Add**.



				Source				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zo
1	Allow-Inside-Out	none	universal	inside	any	any	any	
2	Allow-Inside-DMZ	none	universal	inside	any	any	any	
3	intrazone-default	none	intrazone	any	any	any	any	(int
4	interzone-default	none	interzone	any	any	any	any	any

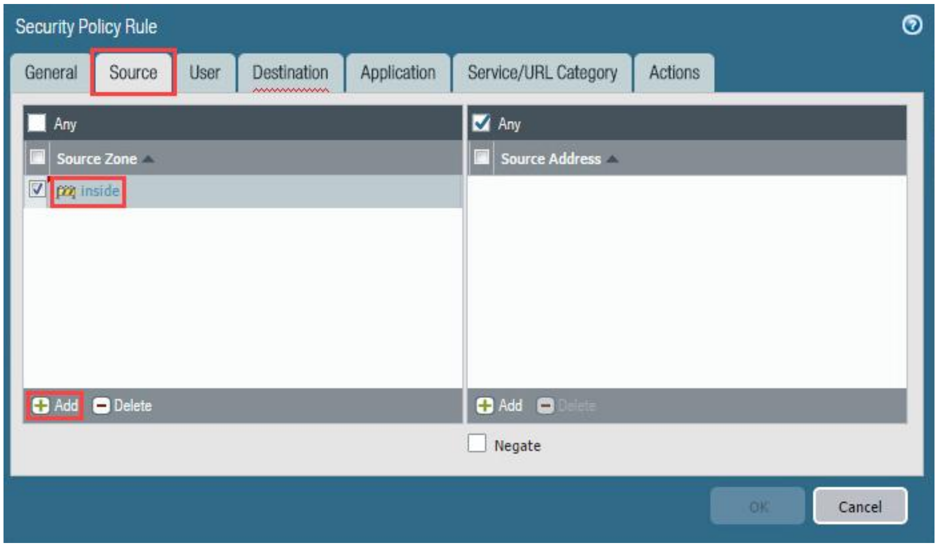
Tag(#)	Rule
none (2)	1-2

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

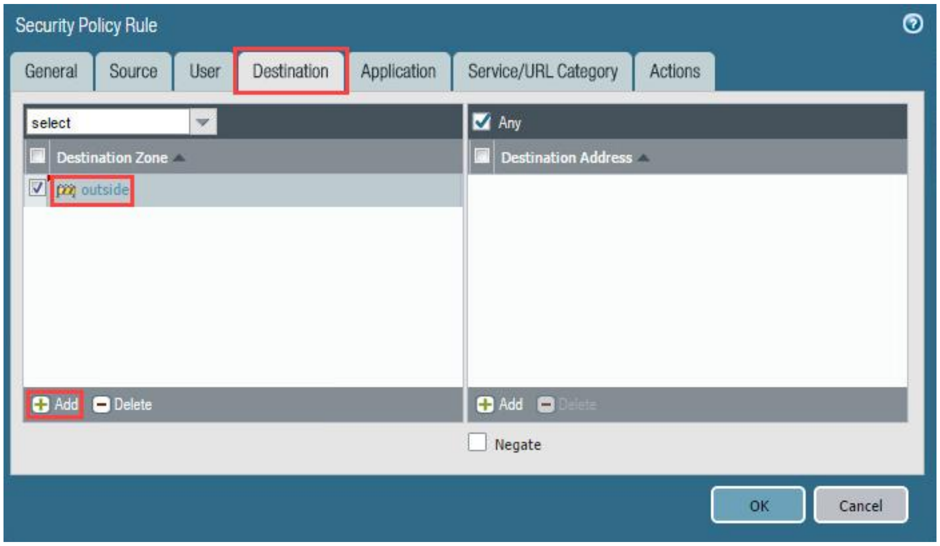


Name: Block-List
Rule Type: universal (default)
Description:
Tags:

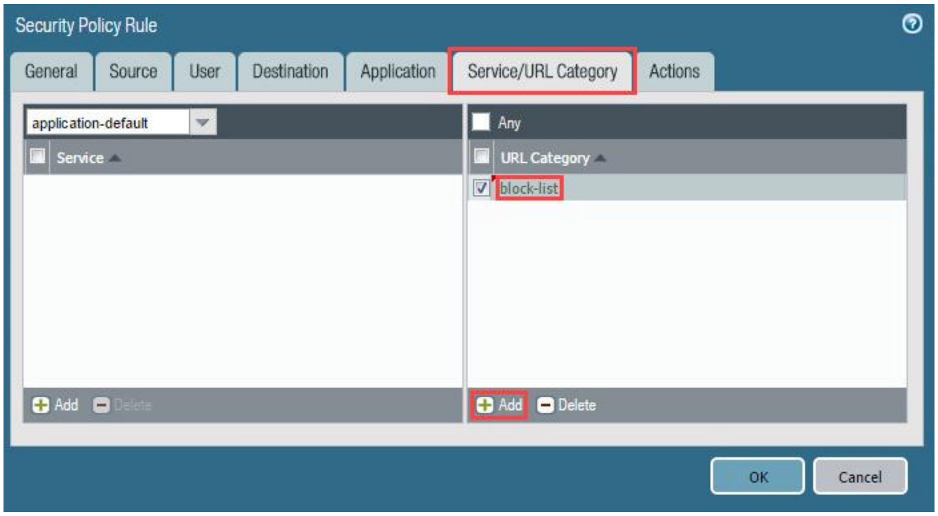
3. In the *Security Policy Rule* window, click the **Source** tab. Then, click the **Add** button in the *Source Zone* section. Next, select **inside** in the *Source Zone* column.



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.



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** under the *External Dynamic* Lists.

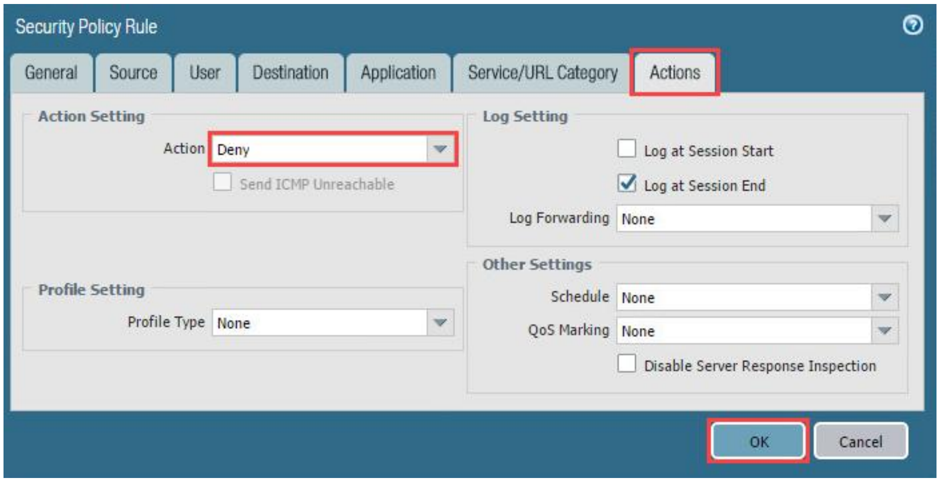


application-default

□ Service

□ Any
□ URL Category
☑ block-list

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



Action Setting

Action: Deny

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

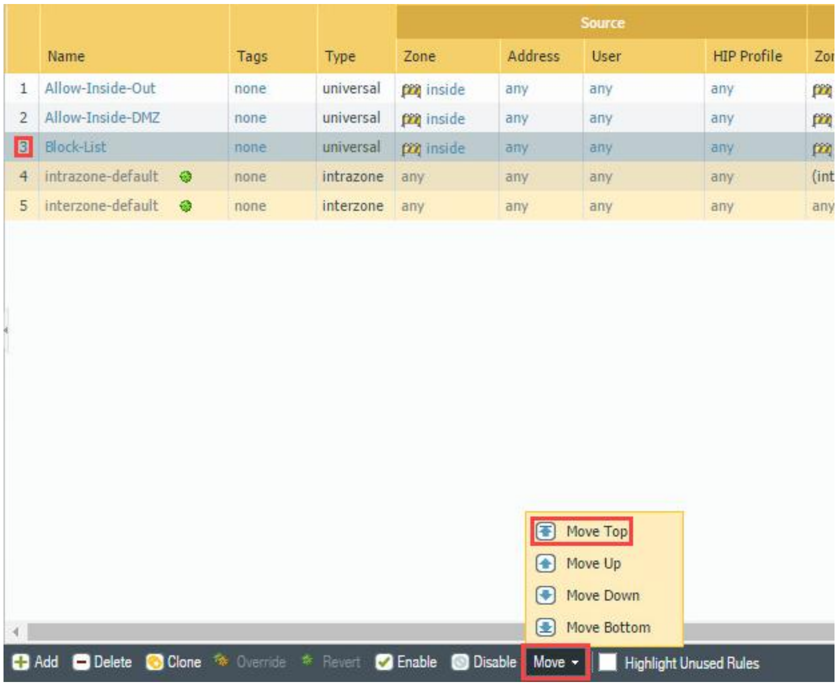
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

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



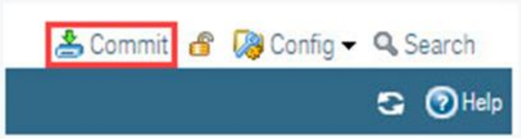
				Source				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zor
1	Allow-Inside-Out	none	universal	inside	any	any	any	
2	Allow-Inside-DMZ	none	universal	inside	any	any	any	
3	Block-List	none	universal	inside	any	any	any	
4	intrazone-default	none	intrazone	any	any	any	any	(int
5	interzone-default	none	interzone	any	any	any	any	any

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.

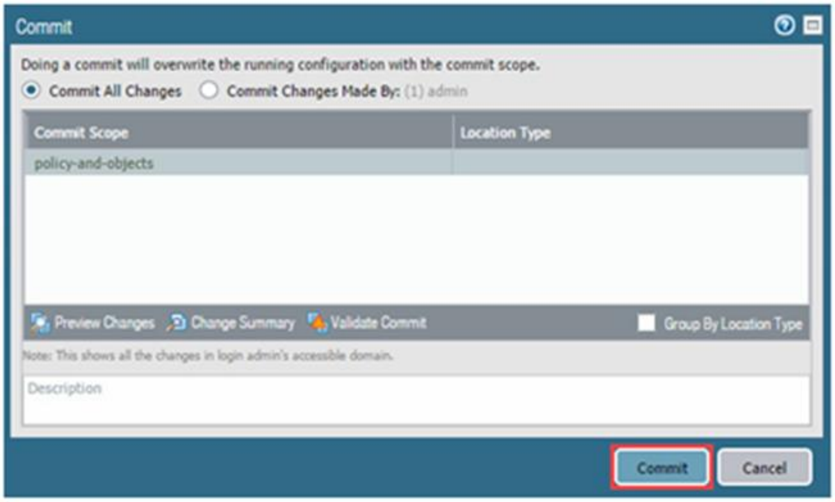
10.4 Commit and Test

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.



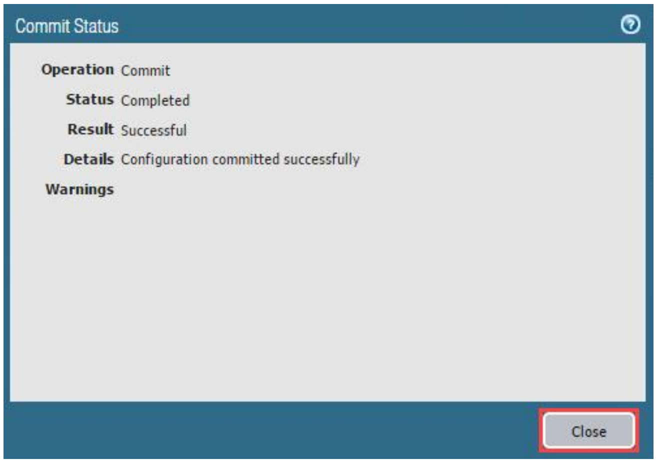
Doing a commit will overwrite the running configuration with the commit scope.

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

Commit Scope	Location Type
policy-and-objects	

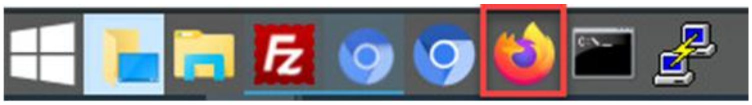
Note: This shows all the changes in login admin's accessible domain.

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

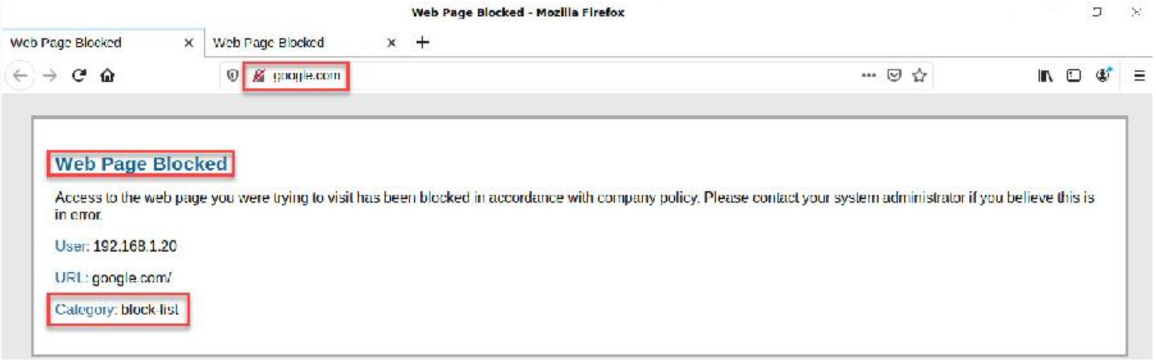


Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

4. Open *Firefox* from the taskbar.



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



Web Page Blocked

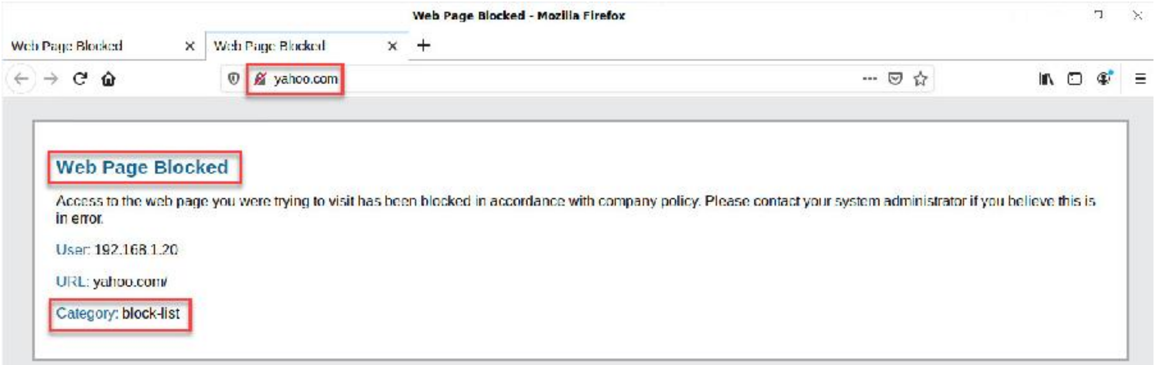
Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 192.168.1.20

URL: google.com/

Category: block-list

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



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

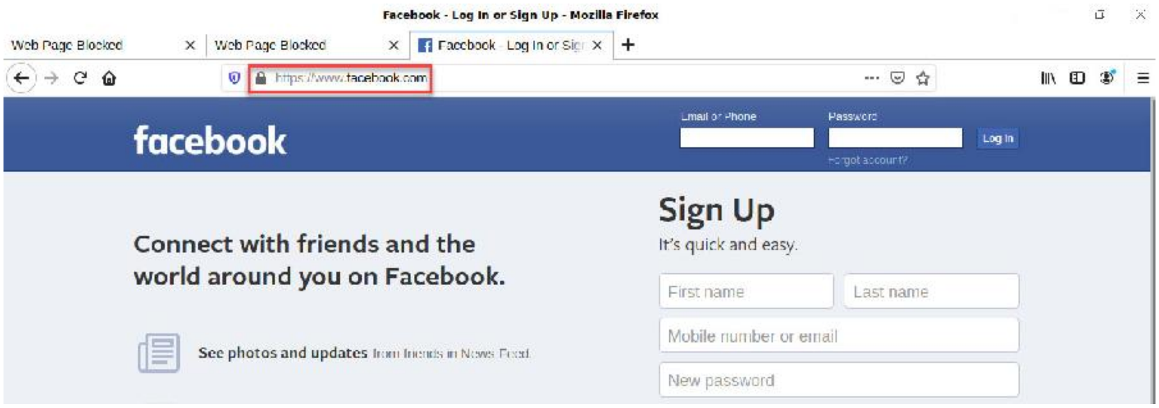
User: 192.168.1.20

URL: yahoo.com/

Category: block-list

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**.



Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

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.