



PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 9: Blocking Inappropriate Web Traffic with Advanced URL Filtering

Document Version: **2025-10-13**

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
Lab Guidance.....	5
1 Blocking Inappropriate Web Traffic with Advanced URL Filtering - High Level Lab Steps	6
1.1 Apply a Baseline Configuration to the Firewall	6
1.2 Test Access to Inappropriate Web Content.....	6
1.3 Create a Security Policy Rule to Block Categories	6
1.4 Commit the Configuration	7
1.5 Test Access to URLs Blocked by the Security Policy	7
1.6 Block Access to Inappropriate Web Content Using Security Profile	7
1.7 Add the URL Profile to the Corp-Profiles-Group.....	8
1.8 Disable Block-Bad-URLs Rule	8
1.9 Commit the Configuration	8
1.10 Test Access to URLs Blocked by a URL Filtering Profile	8
1.11 Create a Custom URL Category.....	8
1.12 Use Custom Category to Block URL Access in Security Policy Rule	8
1.13 Commit the Configuration	8
1.14 Test Access to Custom URLs Blocked by the Security Policy	8
1.15 Add Custom URL Category to URL Filtering Profile	9
1.16 Commit the Configuration	9
1.17 Test Access to Custom URLs Blocked by the URL Filtering Profile	9
1.18 Create an EDL to Block Malicious URL Access	9
1.19 Block Access to the URL List with a Security Policy Rule	9
1.20 Commit the Configuration	9
1.21 Test Access to URLs Blocked by the EDL in the Security Policy	9
1.22 Commit the Configuration	9
2 Blocking Inappropriate Web Traffic with Advanced URL Filtering – Detailed Lab Steps	10
2.1 Apply a Baseline Configuration to the Firewall.....	10
2.2 Generate Traffic Without Security Profiles	14
2.3 Create a Security Policy Rule to Block Categories	16
2.4 Test Access to URLs Blocked by the Security Policy	21
2.5 Block Access to Inappropriate Web Content Using Security Profile	24
2.6 Add the URL Profile to the Corp-Profiles-Group.....	27
2.7 Create a Custom URL Category.....	30
2.8 Test Access to Custom URLs Blocked by Security Policy	36
2.9 Add Custom URL Category to URL Filtering Profile	38
2.10 Test Access to Custom URLs Blocked by the URL Filtering Profile	41
2.11 Create an External Dynamic List to Block Malicious URL Access.....	43
2.12 Block Access to the URL List with a Security Policy Rule	46
2.13 Test Access to a URL in the EDL added to the Security Policy Rule.....	48

Introduction

Access restrictions for potentially malicious or inappropriate websites can be achieved through two distinct approaches.

The first method involves the creation of Security Policy rules with a "Deny" action, incorporating URL categories as part of the rule criteria. This approach allows for granular control over web access by specifying which categories of websites should be blocked.

The second method entails the development of a dedicated URL Filtering Profile that encompasses blocked website categories. This Profile is subsequently applied to a specific Security Policy rule that permits the use of web-browsing and SSL applications.

This strategy offers a balanced approach, granting users access to web resources while ensuring that they conform to predefined security and content filtering guidelines.

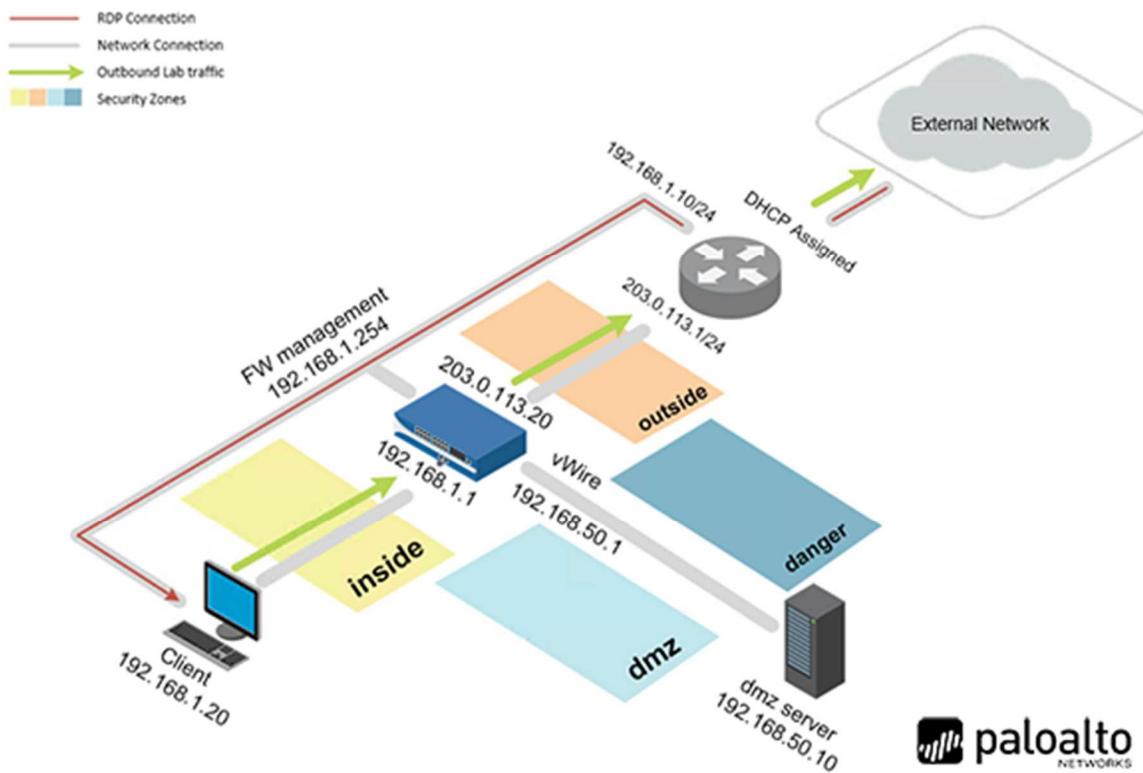
In this lab, you will use both methods so that you can see the differences in how they are configured and in the kind of detail available through the logs when you use one method compared to the other.

Objective

In this lab, you will perform the following tasks:

- Test access to inappropriate web content without URL blocking in place.
- Create a Security Policy rule to block inappropriate web content using the URL Category.
- Test the Security Policy rule and examine the results.
- Disable the Security Policy rule.
- Create and apply a URL Filtering Profile to block access to a malicious URL.
- Test the Security Profile and examine the results.

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	PaloAlt0!
DMZ	192.168.50.10	root	PaloAlt0!
Firewall	192.168.1.254	admin	PaloAlt0!
vRouter	192.168.1.10	root	PaloAlt0

Lab Guidance

There are two sections in this lab guide:

- High-Level Lab Steps
- Detailed Lab Steps

The High-Level Lab Steps section provides only general guidance and information about how to accomplish the lab objectives. This section is more challenging and is suited for students who have a working knowledge of Palo Alto Networks firewalls. If you have never worked with a Palo Alto Networks firewall, we strongly encourage you to use the Detailed Lab Steps section.

The instructions in the Detailed Lab Steps section provide guided, detailed steps and screenshots to accomplish the lab objectives.

If you decide to use the High-Level Lab Guide and get stuck, switch to the Detailed Lab Guide for guidance.

Please
Note

You are not required to complete both the High-Level Lab Guide and the Detailed Lab Guide for each lab. Instead, please select the appropriate section based on your familiarity with Palo Alto Networks Firewalls.

1 Blocking Inappropriate Web Traffic with Advanced URL Filtering - High Level Lab Steps

It is recommended to use this section if you possess significant experience in working with Palo Alto Networks firewalls. In case you require more comprehensive instructions to achieve the objectives, please utilize the Detailed-Lab Steps section in Task 2.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-09.xml** to the Firewall.

1.2 Test Access to Inappropriate Web Content

- Run the **Clear Firewall Logs** script on the *client* desktop.
- Use Firefox to browse to **hacker9.com** and **hidester.com** and verify that both sites are available.

1.3 Create a Security Policy Rule to Block Categories

- Use the information in the tables below to create a Security Policy rule to block traffic to certain URL Categories:

Rule Name	Block-Bad-URLs
Description	Blocks bad URLs based on categories
Source Zone	Users_Net
Destination Zone	Internet
Application	Any
Service	application-default
URL Category	Add the following: adult command-and-control extremism hacking high-risk malware nudity parked peer-to-peer phishing proxy-avoidance-and-anonymizers questionable

Action	Deny
--------	------

- Move the **Block-Bad-URLs** rule to the top of the Security Policy.

1.4 Commit the Configuration

- Commit the changes before proceeding.

1.5 Test Access to URLs Blocked by the Security Policy

- Use Firefox and attempt to connect to **hacker9.com** and **hidester.com**.
- Note the message displayed by browser.
- Examine the **Traffic** log and use a filter to locate entries that have been blocked by the **Block-Bad-URLs**.
- Examine the **URL Filtering** log and use a filter to locate entries that have been blocked by the firewall.

1.6 Block Access to Inappropriate Web Content Using Security Profile

- Create a URL Filtering Profile using the information in the table below:

Name	Corp-URL-Profile
Description	Standard corporate URL profile for all security policy rules
Site Access All Categories (except those below)	Alert
Site Access Block	adult command-and-control copyright-infringement extremism hacking high-risk malware nudity parked peer-to-peer phishing proxy-avoidance-and-anonymizers questionable unknown

1.7 Add the URL Profile to the Corp-Profiles-Group

- Edit the **Corp-Security-Group** and add the URL Filtering Profile **Corp-URL-Filtering**.

1.8 Disable Block-Bad-URLs Rule

- Disable the **Block-Bad-URLs** in the Security Policy so that it does not interfere with your URL Filtering Profile testing.

1.9 Commit the Configuration

- Commit the changes before proceeding.

1.10 Test Access to URLs Blocked by a URL Filtering Profile

- Use Firefox and browse to **hidester.com** and **hacker9.com**.
- Note the difference between this error page and the one you received when using a Security Policy rule to block categories.
- Examine the **Traffic** log and use a filter to display entries that fall in the URL Category of **hacking**.
- Examine the **URL Filtering** Log and use a filter to display entries that fall in the URL Category of **hacking**.

1.11 Create a Custom URL Category

- Use the information in the table below to create a **Custom URL Category**:

Parameter	Value
Name	Block-Per-Company-Policy
Description	URLs that are blocked by company policy.
Sites	Add the following: *.nbcnews.com *.theguardian.com

1.12 Use Custom Category to Block URL Access in Security Policy Rule

- Enable the Security Policy Rule **Block-Bad-URLs**.
- Add the **Block-Per-Company-Policy** custom URL category to the rule.

1.13 Commit the Configuration

- Commit the changes before proceeding.

1.14 Test Access to Custom URLs Blocked by the Security Policy

- Use the Firefox browser and connect to **www.nbcnews.com** and **www.theguardian.com**.
- Note the **Application Blocked** page message presented by the firewall.
- Examine the **URL Filtering** log and use it to locate entries with an **Action of block-url**.

1.15 Add Custom URL Category to URL Filtering Profile

- Edit the **Corp-URL-Profile** and set the **Site Access** for **Block-Per-Company-Policy** to **block**.
- Disable the Security Policy rule **Block-Bad-URLs** so that it does not interfere with the URL Filtering Profile.

1.16 Commit the Configuration

- Commit the changes before proceeding.

1.17 Test Access to Custom URLs Blocked by the URL Filtering Profile

- Use Firefox and browse to www.nbcnews.com and www.theguardian.com.
- Note the Block page presented by the firewall.

1.18 Create an EDL to Block Malicious URL Access

- Use the information in the table below to create an **External Dynamic List**:

Parameter	Value
Name	malicious-urls-edl
Type	URL List
Description	List of malicious URLs maintained on Extranet server
Source	http://192.168.50.80/malicious-urls.txt (The EDL contains only the URL www.popurls.com)
Check for updates	Every Five Minutes

1.19 Block Access to the URL List with a Security Policy Rule

- Add the **malicious-urls-edl** to the URL Category of the **Block-Bad-URLs** Security Policy rule.
- Enable the **Block-Bad-URLs** Security Policy rule.

1.20 Commit the Configuration

- Commit the changes before proceeding.

1.21 Test Access to URLs Blocked by the EDL in the Security Policy

- Use Firefox and browse to <http://www.popurls.com>.
- Note the Application Blocked that the firewall displays.
- Examine the **URL Filtering** log.
- Use a filter that will display entries that have an action of **block-url**.
- Disable the Security Policy rule **Block-Bad-URLs**.

1.22 Commit the Configuration

- Commit the changes before proceeding.

2 Blocking Inappropriate Web Traffic with Advanced URL Filtering – Detailed Lab Steps

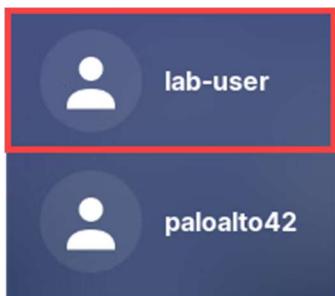
2.1 Apply a Baseline Configuration to the Firewall

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

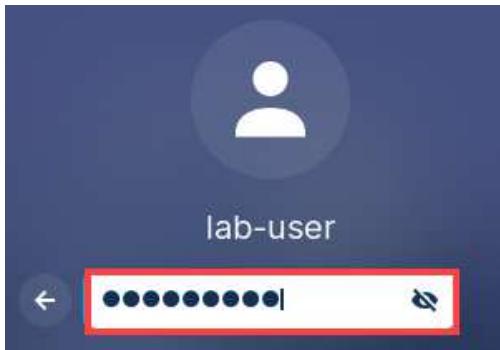
1. Click on the **Client** tab to access the Client PC.



2. On the *Zorin* desktop, click **lab-user**.



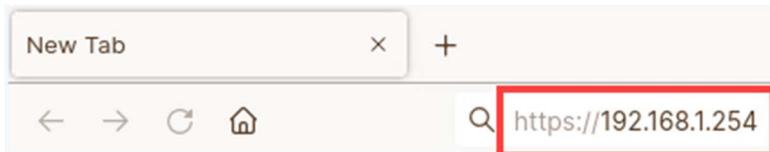
3. For the *lab-user* password, enter **Pal0Alt0!** and press **Enter**.



4. Double-click the **Firefox Web Browser** icon located on the *Desktop*.



5. In the *Firefox* address field, type **<https://192.168.1.254>** and press **Enter**.



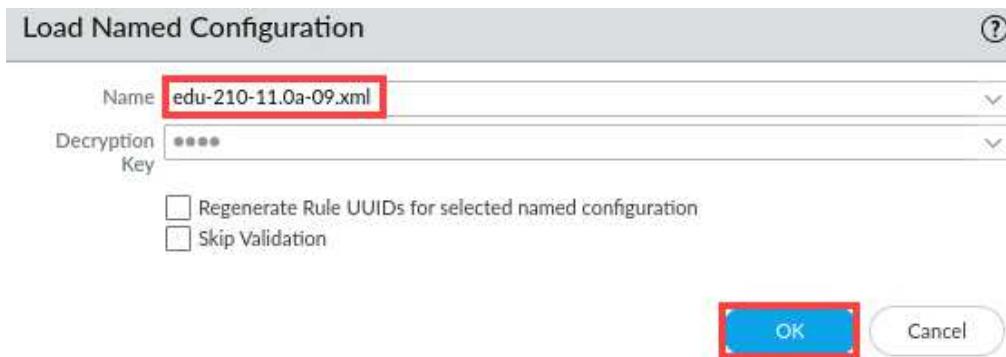
6. Log in to the Firewall web interface as username **admin**, password **Pa10Alt0!**.



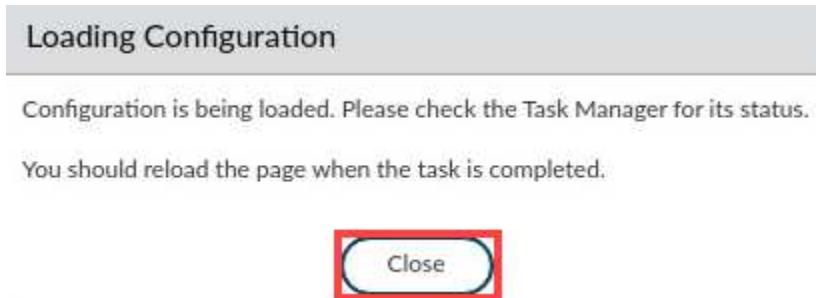
If you do not immediately see the login page, please wait an additional 1-3 minutes for the *Firewall* to fully initialize. If needed, refresh the page.

7. Navigate to **Device > Setup > Operations** in the web interface and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

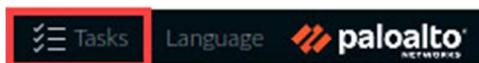
8. In the *Load Named Configuration* window, select **edu-210-11.0a-09.xml** from the *Name* drop-down box and click **OK**.



9. 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.



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



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

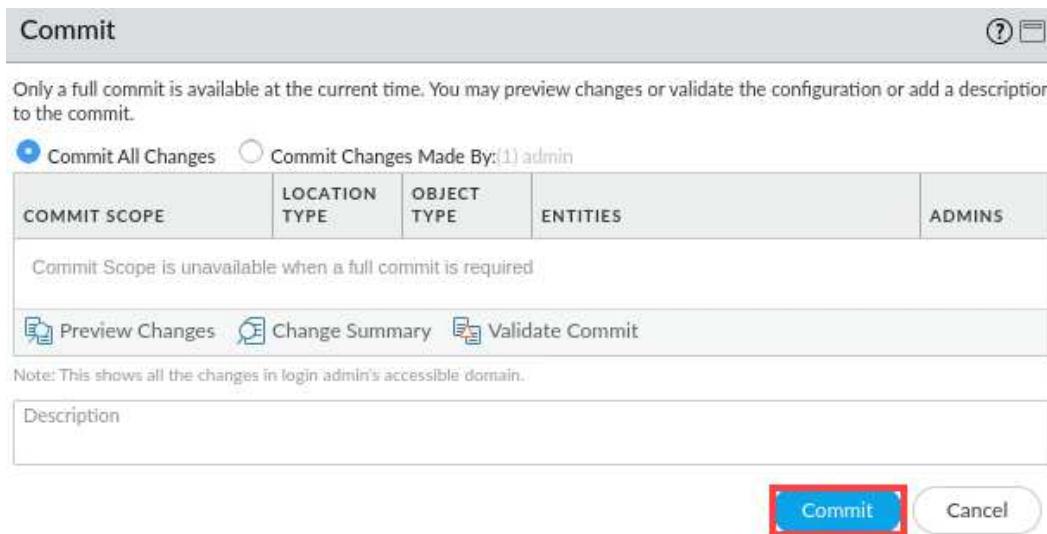
Task Manager - All Tasks						
<input type="text"/> 12 items → X						
JOB ID	TYPE	STATUS	START TIME	MESSAGES	ACTION	ADMIN
14	Load	Completed	2023/07/28 18:54:07			System
2	Report	Completed	2023/07/28 18:51:30			

Show Clear Commit Queue

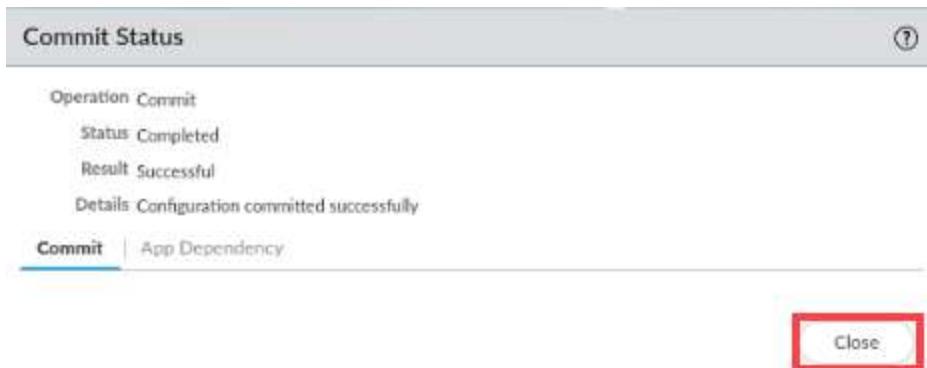
12. Click the **Commit** link located at the top-right of the web interface.



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



14. When the commit operation is complete, 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.

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

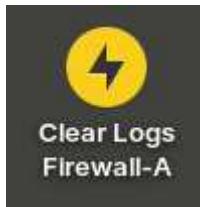


2.2 Generate Traffic Without Security Profiles

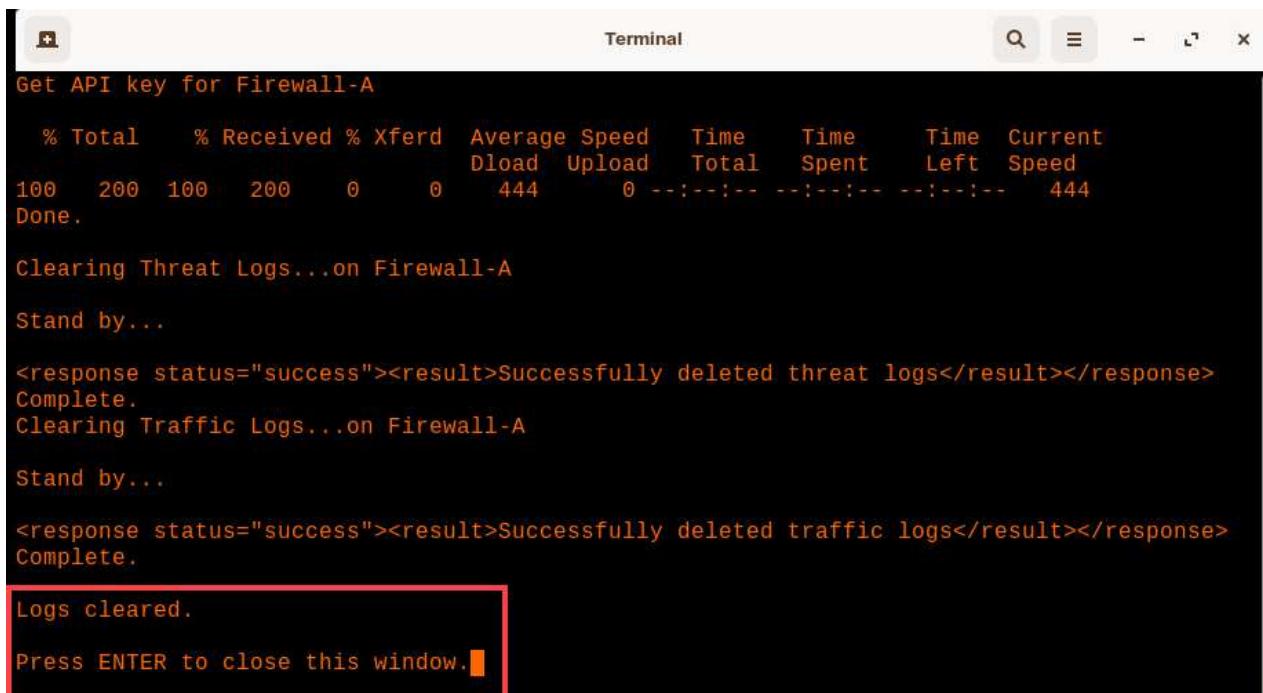
You can block access to inappropriate or malicious URLs by creating rules in the Security Policy. In this section, you will create a rule that blocks access to several URL categories.

Before you create the rule, you will clear the log file entries on the firewall (to make it easier to see new entries generated during this lab). You will also test access to two websites to verify that they are not being blocked.

1. On the client desktop, double-click the **Clear Logs Firewall-A** application.



2. Verify the *Clear Logs* script has cleared the logs. Press **Enter**.



A screenshot of a terminal window titled 'Terminal'. The window shows the output of a script used to clear logs on a device named 'Firewall-A'. The output includes:

```
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  444      0  --::--  --::--  --::--  444
Done.

Clearing Threat Logs...on Firewall-A
Stand by...

<response status="success"><result>Successfully deleted threat logs</result></response>
Complete.

Clearing Traffic Logs...on Firewall-A
Stand by...

<response status="success"><result>Successfully deleted traffic logs</result></response>
Complete.

Logs cleared.

Press ENTER to close this window.
```

3. On the client desktop, open another **Firefox Web Browser** application.



4. Type **http://www.hacker9.com**, which belongs to the URL category *hacking*.



The browser should display a valid webpage.

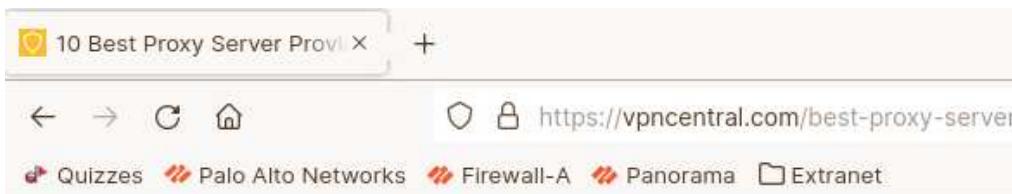
Please Note

5. Type **http://www.hidester.com/proxy**, which belongs to the URL category *proxy-avoidance-and-anonymizers*.



The browser should display a valid webpage. Notice the redirect to vpncentral.com.

Please Note



The browser should display a valid webpage.

Please Note

6. Close the *Firefox browser*.



7. Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



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

2.3 Create a Security Policy Rule to Block Categories

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.

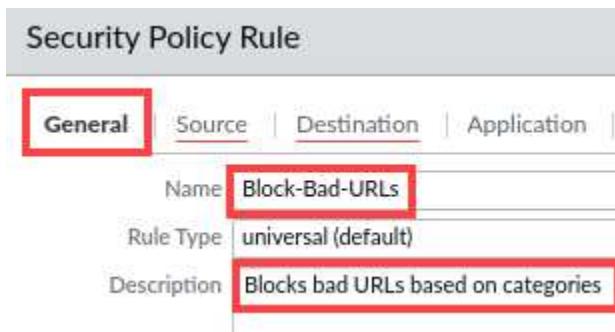
1. In the web interface, select **Policies > Security**. If the **URL Category** column is not displayed, click the **down-arrow** menu that appears next to any column header (hover your pointer over a header to see the **Down arrow**) and select **Columns > URL Category**.

NAME	TAGS	TYPE	ZONE	ADDRESS
Block-from-Known...	none	<input type="button" value="Columns"/>	universal	
4	User ..._extranet	Zone	universal	Universal

Add **Delete** **Clone** **Override**

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

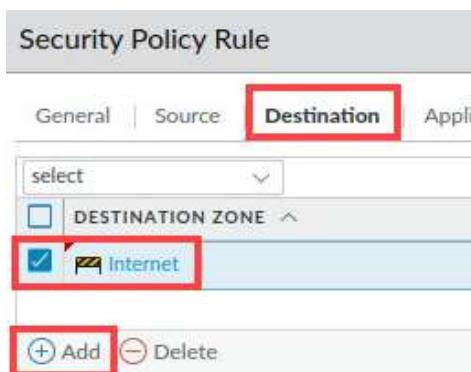
3. In the *Security Policy Rule* window, on the *General* tab, type **Block-Bad-URLs** as the **Name**. For **Description**, enter **Blocks bad URLs based on categories**.



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



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



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



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

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

Please
Note

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

Security Policy Rule

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

application-default ▾

SERVICE ▾

Add **Delete**

Any

URL CATEGORY ▾

- malware
- nudity
- parked
- peer-to-peer
- phishing
- proxy-avoidance-and-anonymizers
- questionable

Add **Delete**

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

Security Policy Rule

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

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** Disable Server Response Inspection

QoS Marking **None**

OK **Cancel**

9. Select, but do not open, the **Block-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.

	NAME	TAGS	TYPE	Source			
				ZONE	ADDRESS	USER	DEV
6	Extranet_to_Internet	none	universal	Extranet	any	any	any
7	Extranet_to_User_Net	none	universal	Extranet	any	any	any
8	Acquisition-Allow-All	none	universal	Acquisition	any	any	any
9	Block-Bad-URLs	none	universal	Users_Net	any	any	any

↑ Move Top
↑ Move Up
↓ Move Down
↓ Move Bottom

⊕ Add ⊖ Delete ⟳ Clone ⚙ Override ⟲ Revert ✓ Enable ✗ Disable Move ▾ PDF/CSV Highli

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



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

Commit

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

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

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			

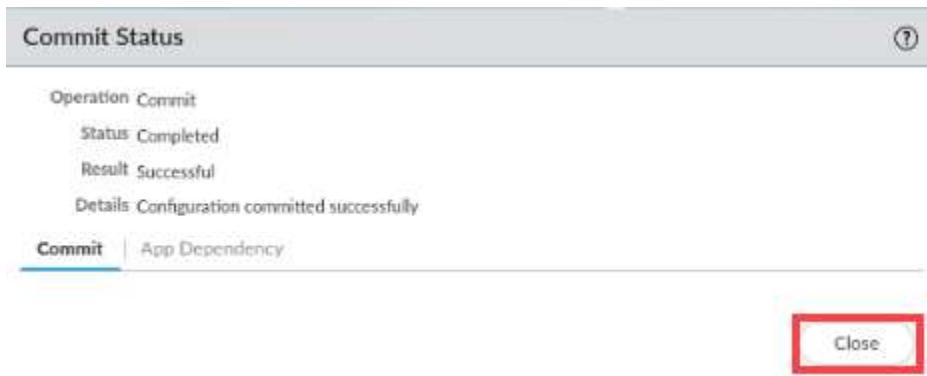
☰ Preview Changes ☰ Change Summary ☰ Validate Commit

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

Description

Commit Cancel

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



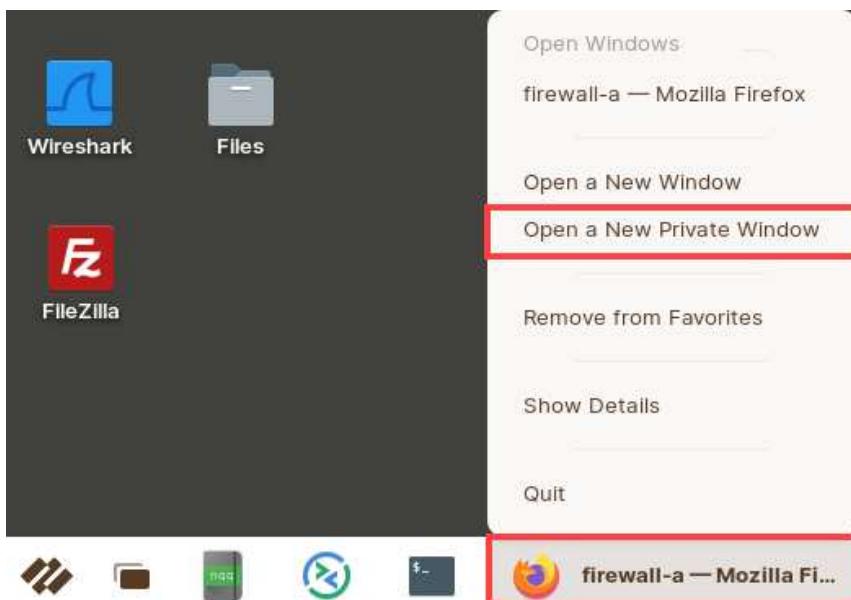
13. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.



2.4 Test Access to URLs Blocked by the Security Policy

In this section, you will test access to URLs that belong to URL categories prohibited by the Security Policy.

1. On the client toolbar, right-click the **firewall-a – Mozilla Firefox Web Browser** application. Select **Open a New Private Window**.



2. Type **http://www.hacker9.com**, which belongs to the URL category *hacking*. The browser should display an error message similar to the following example because the URL category hacking is blocked in the Security Policy.

The application you are trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.1.20

Application: web-browsing

Please Note

Although this page says the Application web-browsing has been blocked, the firewall is actually blocking the site based on its category – hacking. The firewall uses this page to inform users that the firewall has blocked a web page deliberately. You will see a different message when the firewall blocks a page using a URL Filtering Profile.

3. Type **http://www.hidester.com/proxy**, which belongs to the URL category *proxy-avoidance-and-anonymizers*. The browser should display the same kind of block page.

The application you are trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error.

User: 192.168.1.20

Application: web-browsing

4. Close the *Firefox browser*.



5. Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



6. In the *firewall* web interface, select **Monitor > Logs > URL Filtering**.

RECEIVE TIME	CATEGORY	URL C
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-

7. Although this page says the Application web-browsing has been blocked, the firewall is actually blocking the site based on its category – hacking. The firewall uses this page to inform users that the firewall has blocked a web page deliberately. You will see a different message when the firewall blocks a page using a URL Filtering Profile.

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/favicon.ico	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/login/css/latofonts.css	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:26:06	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	www.hidester.com/	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/favicon.ico	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/login/css/latofonts.css	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet	192.168.1.20
09/20 18:24:01	hacking	hacking,low-risk	www.hacker9.com/	Users_Net	Internet	192.168.1.20

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.

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

2.5 Block Access to Inappropriate Web Content Using Security Profile

You can use a Security Policy rule to control access to web site categories or you can use a URL Filtering Profile to accomplish the same task. One significant difference between the two is that you can configure a URL Filtering Profile to log access to all websites and categories; not just to websites that have been blocked by a Security Policy rule.

In this section, you will create a URL Filtering Profile that blocks certain categories of web content.

1. 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, and Applications. The main content area has a search bar and a table with columns: NAME, LOCATION, and SITE ACCESS. One row in the table is for a profile named "default" located in "Predefined" with "Allow Categories (58)" and "Alert Categories (5)". On the left side, there is a vertical tree view of security profiles. The "Security Profiles" node is expanded, and its child node "URL Filtering" is also expanded and highlighted with a red box. Under "URL Filtering", other items like File Blocking and WildFire Analysis are listed. At the bottom of the page, there is a toolbar with buttons for Add, Delete, Clone, PDF/CSV, and a note: "(* indicates custom URL category, + indicates".

2. 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 screen. It has a title bar "URL Filtering Profile". Below it, there are two input fields: "Name" containing "Corp-URL-Profile" and "Description" containing "Company URL Filtering profile", both of which are highlighted with a red box. At the bottom of the screen, there are three tabs: "Categories" (which is underlined and highlighted with a red box), "URL Filtering Settings", and "User Credential Detection".

3. In the **Site Access** column, click the small triangle. Choose **Set All Actions > alert**.

The screenshot shows a table with columns: CATEGORY, SITE ACCESS, and USER CREDENTIAL SUBMISSION. A context menu is open over the 'adult' row in the SITE ACCESS column. The menu includes options like Sort Ascending, Sort Descending, Columns, Set All Actions (which is expanded), Set Selected Actions, Adjust Columns, and a list of actions: allow, alert, block, continue, and override. The 'alert' option is highlighted with a red box.

Please Note

This shortcut allows you to change the setting for all categories in the list rather than changing each one entry at a time. Setting the action to alert instructs the firewall to allow access to the category and to write an entry to the URL Filtering log. When the action is set to allow, the firewall allows access but does not write an entry to the URL Filtering log.

4. 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. Click **OK**.

Parameter	Value
Site Access	<p>Configure the block action for the following URL categories:</p> <p>adult command-and-control copyright-infringement extremism hacking high-risk malware nudity parked peer-to-peer phishing proxy-avoidance-and-anonymizers questionable unknown</p>

URL Filtering Profile

Name		Corp-URL-Profile																												
Description		Company URL Filtering profile																												
Categories URL Filtering Settings User Credential Detection HTTP Header Insertion Inline Categorization																														
<table border="1"> <thead> <tr> <th colspan="2">77 items</th> <th>→</th> <th>X</th> </tr> <tr> <th>CATEGORY</th> <th>SITE ACCESS</th> <th>USER CREDENTIAL SUBMISSION</th> </tr> </thead> <tbody> <tr> <td>nudity</td> <td>block</td> <td>block</td> </tr> <tr> <td>online-storage-and-backup</td> <td>alert</td> <td>allow</td> </tr> <tr> <td>parked</td> <td>block</td> <td>block</td> </tr> <tr> <td>peer-to-peer</td> <td>block</td> <td>block</td> </tr> <tr> <td>personal-sites-and-blogs</td> <td>alert</td> <td>allow</td> </tr> <tr> <td>philosophy-and-political-advocacy</td> <td>alert</td> <td>allow</td> </tr> <tr> <td>phishing</td> <td>block</td> <td>block</td> </tr> </tbody> </table>			77 items		→	X	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION	nudity	block	block	online-storage-and-backup	alert	allow	parked	block	block	peer-to-peer	block	block	personal-sites-and-blogs	alert	allow	philosophy-and-political-advocacy	alert	allow	phishing	block	block
77 items		→	X																											
CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION																												
nudity	block	block																												
online-storage-and-backup	alert	allow																												
parked	block	block																												
peer-to-peer	block	block																												
personal-sites-and-blogs	alert	allow																												
philosophy-and-political-advocacy	alert	allow																												
phishing	block	block																												
<small>* indicates a custom URL category, + indicates external dynamic list</small> Check URL Category																														
<input type="button" value="OK"/> <input type="button" value="Cancel"/>																														

Please Note

For this step, the screen shot only shows the block access to four categories. Ensure you have blocked all the categories for this step before continuing.

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

2.6 Add the URL Profile to the Corp-Profiles-Group

In this section, you will add the URL Filtering Profile **Corp-URL-Filtering** to the existing Security Profile Group and disable the rule that blocks URLs based on categories so that it does not interfere with the URL Filtering Profile.

1. Select **Objects > Security Profile Groups**. Click the entry for **Corp-Profiles-Group** to edit it.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. On the left, there's a sidebar with various options like Addresses, Address Groups, Regions, etc. Below that is a dropdown menu with Data Filtering, DoS Protection, Security Profile Groups (which is selected and highlighted with a red box), and Log Forwarding. The main area displays a table with columns: NAME, LOCATION, ANTIVIRUS PROFILE, ANTI-SPYWARE PROFILE, and VULN PRO PRO. A single row is visible for 'Corp-Profiles-Group'.

	NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULN PRO PRO
<input type="checkbox"/>	Corp-Profiles-Group		Corp-AV	Corp-AS	Corp

2. Use the drop-down list for **URL Filtering Profile** to select **Corp-URL-Profile**. Click OK.

The screenshot shows the 'Security Profile Group' configuration dialog. It has fields for Name (Corp-Profiles-Group), Antivirus Profile (Corp-AV), Anti-Spyware Profile (Corp-AS), Vulnerability Protection Profile (Corp-Vuln), URL Filtering Profile (Corp-URL-Profile, highlighted with a red box), File Blocking Profile (Corp-FileBlock), Data Filtering Profile (Corp-DataFilter), and WildFire Analysis Profile (None). At the bottom are 'OK' and 'Cancel' buttons, with 'OK' highlighted with a red box.

Name	Corp-Profiles-Group
Antivirus Profile	Corp-AV
Anti-Spyware Profile	Corp-AS
Vulnerability Protection Profile	Corp-Vuln
URL Filtering Profile	Corp-URL-Profile
File Blocking Profile	Corp-FileBlock
Data Filtering Profile	Corp-DataFilter
WildFire Analysis Profile	None

3. In the firewall web interface, navigate to **Policies > Security**. Highlight the entry for **Block-Bad-URLs** but do not open it and click **Disable**.

NAME	TAGS	TYPE	ZONE	ADDRESS
1 Block-Bad-URLs	none	universal	inside	any

Object : Addresses + + Add - Delete Clone Override Revert Enable Disable Move ▾

4. The entry will change to *italics* to indicate that the rule is now **Disabled**.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1 Block-Bad-URLs	none	universal	Users-Net	any	any

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



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

Commit

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

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

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			

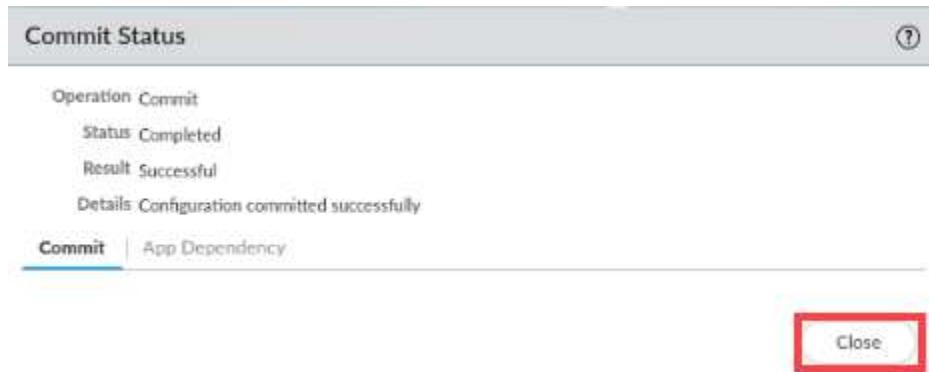
Preview Changes Change Summary Validate Commit

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

Description

Commit Cancel

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



8. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.

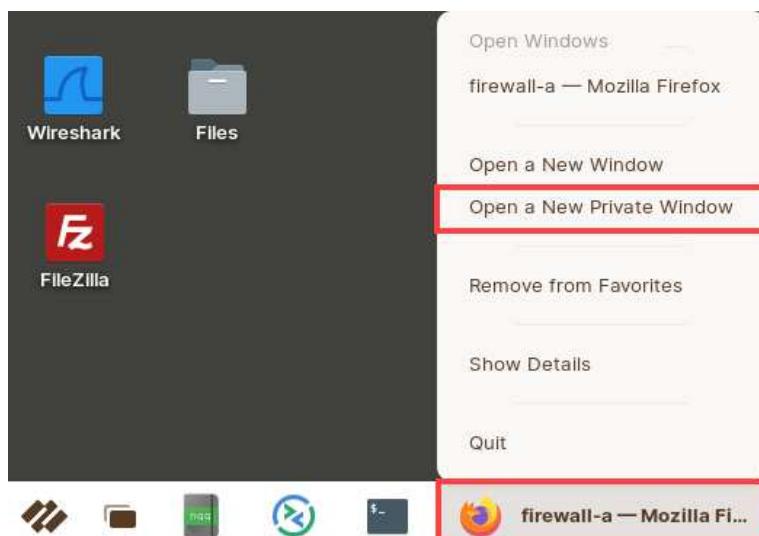


2.7 Create a Custom URL Category

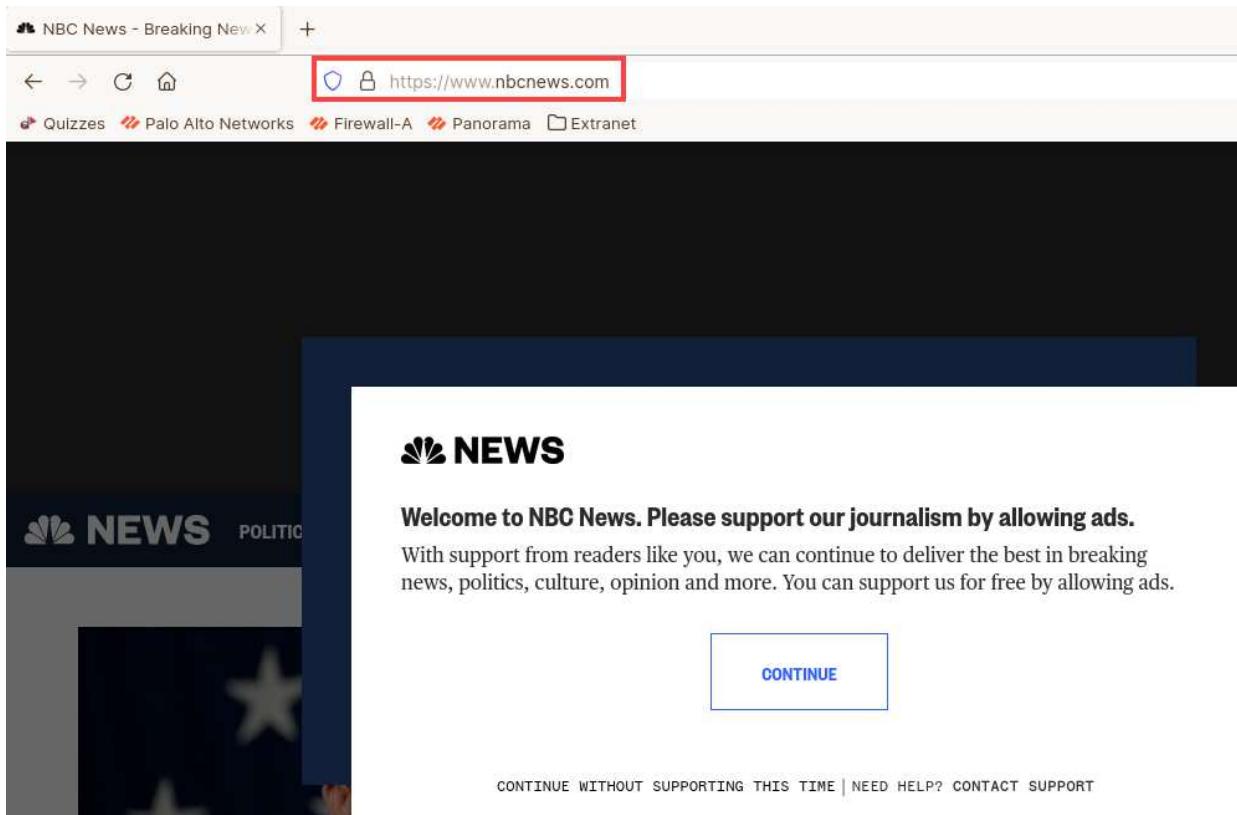
In some situations, you may want to block only a few websites in a particular category, but you do not want to block the entire category itself. You can accomplish this by creating a Custom URL Category. Adding individual URLs to the Custom URL Category allows you to then block the Custom URL Category within a Security Policy rule or within a URL Filtering Profile.

In this section, you will test access to a URL and then create a Custom URL Category that includes that URL along with a few others.

1. On the client toolbar, right-click the **firewall-a – Mozilla Firefox Web Browser** application. Select **Open a New Private Window**.



2. Type **http://www.nbcnews.com**, you should get a valid webpage displayed.



3. Close the *Firefox browser*.



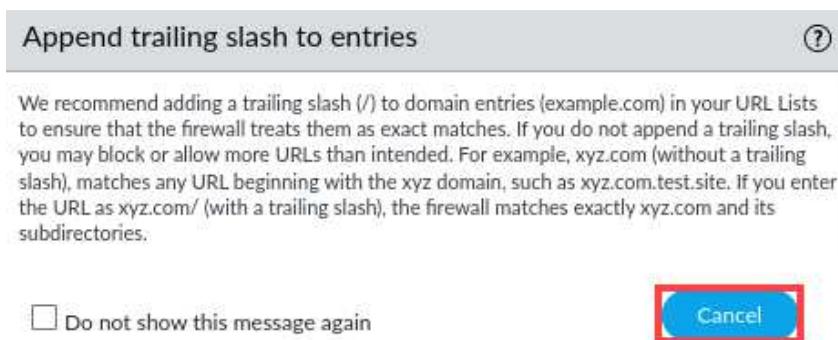
4. Re-open the *PA-VM firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



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

The screenshot shows the PA-VM web interface. The top navigation bar has tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is highlighted with a red box), and NETWORK. On the left, a sidebar menu is open under 'Custom Objects'. The 'URL Category' option is highlighted with a red box. At the bottom of the page, there is a toolbar with buttons: '+ Add' (highlighted with a red box), Delete, Clone, and PDF/CSV.

6. Click **Cancel** on the message about *Append trailing slash to entries*.



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

Parameter	Value
Name	Block-Per-Company-Policy
Description	URLs that are blocked by company policy.
Type	URL List
Sites	Add the following: *.nbcnews.com *.theguardian.com

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 X <input type="checkbox"/> SITES <input type="checkbox"/> *.nbcnews.com <input type="checkbox"/> *.theguardian.com	
+ Add Delete Import Export	
Enter one entry per row. Each entry may be of the form www.example.com or it could have wildcards like www.*.com. To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: xyz.com/ matches only xyz.com. For more info, see URL Category Exceptions	
OK Cancel	

8. Confirm the *Block-Per-Company-Policy* Custom URL is showing in the URL Category window.

	NAME	LOCATION
<input checked="" type="checkbox"/>	Block-Per-Company-Policy	

9. Add your *Custom URL Category* to a Security policy rule that has a “**deny**” action. Select **Policies > Security**. Click **Block-Bad-URLs** to edit the rule.

NAME	TAGS	TYPE	ZONE
1 Block-Bad-URLs	none	universal	Users_Net

10. Select the **Service/URL Category** tab and click **Add**. Add **Block-Per-Company-Policy** to the list. Click **OK**.

Security Policy Rule

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

application-default

SERVICE

Any

URL CATEGORY

- nudity
- parked
- peer-to-peer
- phishing
- proxy-avoidance-and-anonymizers
- questionable
- Block-Per-Company-Policy**

+ Add | - Delete

OK | Cancel

11. Highlight the rule for **Block-Bad-URLs** but do not open it. Click the **Enable** button at the bottom of the window.

	NAME	TAGS	TYPE	Source		
				ZONE	ADDRESS	USER
1	Block-Bad-URLs	none	universal	Users_Net	any	any
2	Block-from-Known...	none	universal	Internet	Palo Alto Netw... Palo Alto Netw... Palo Alto Netw...	any
3	Block-to-Known-Ba...	none	universal	Extranet Users_Net	any	any
4	Allow-PANW-Apps	none	universal	Users_Net	192.168.1.254	any
5	Users_to_Extranet	none	universal	Users_Net	any	any

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



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

Commit

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

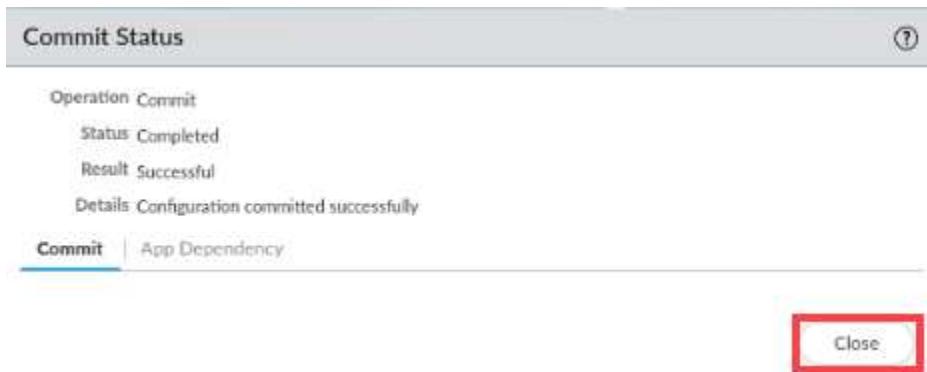
Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			

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

Description

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



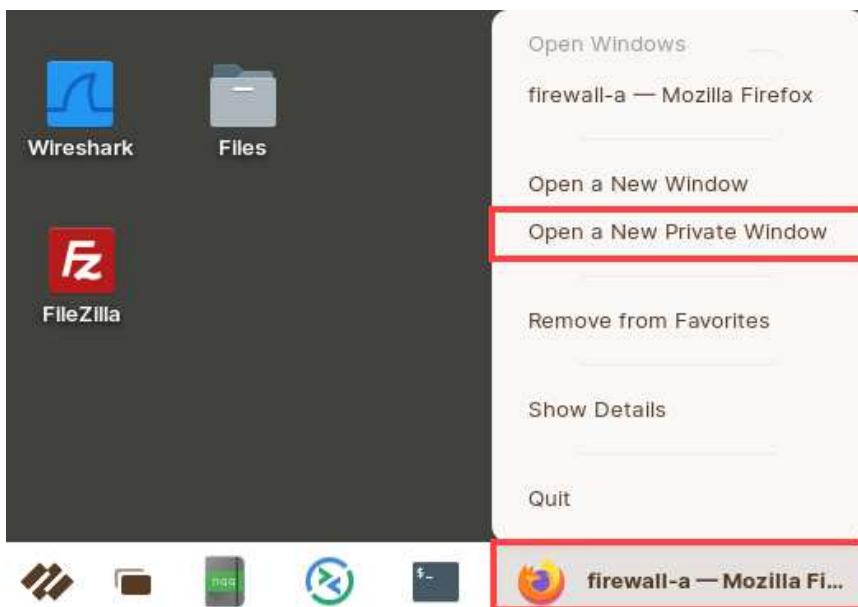
15. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.



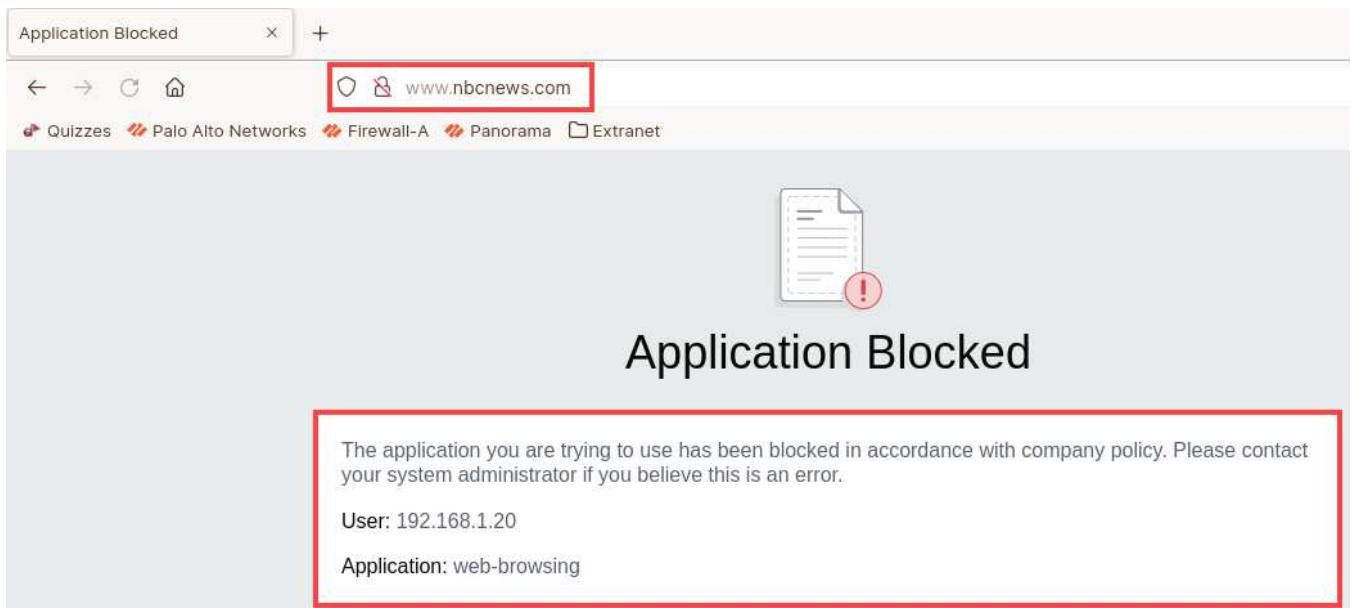
2.8 Test Access to Custom URLs Blocked by Security Policy

In this section, you will test access to URLs that belong to the Custom URL Category that you added to a Security Policy deny rule.

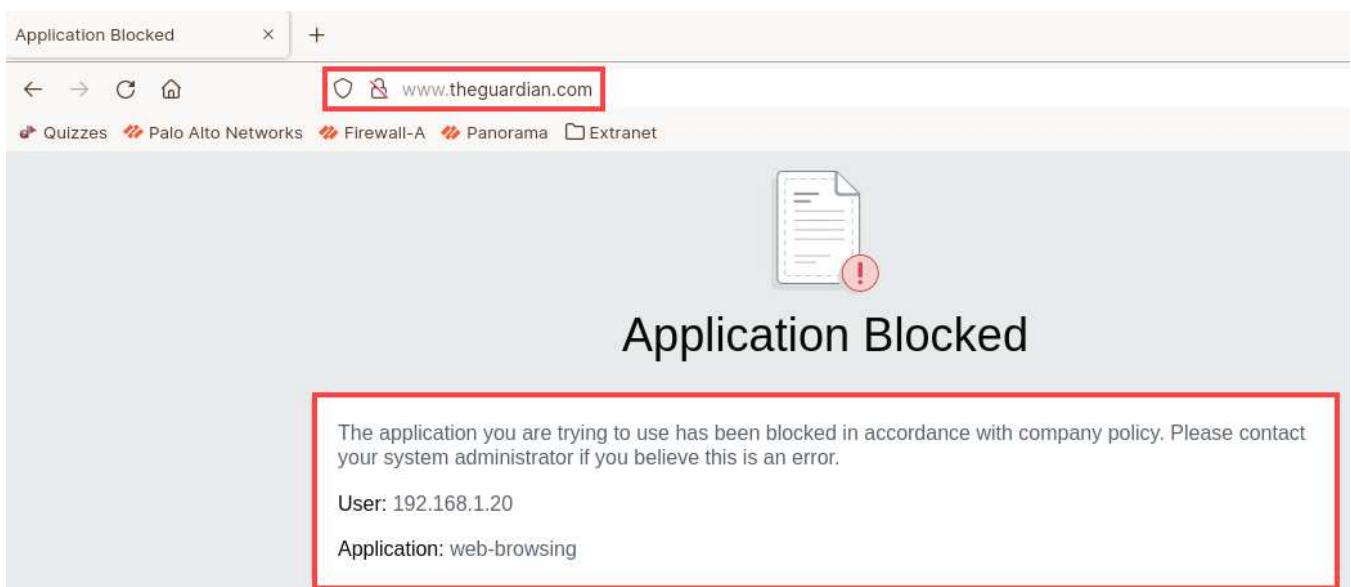
1. On the client taskbar, right-click the **firewall-a – Mozilla Firefox Web Browser** application. Select **Open a New Private Window**.



2. Type **www.nbcnews.com**, the browser should display an Application Blocked page message because the Custom URL Category in the Security Policy blocks access to the webpage.



3. Type **www.theguardian.com**, the browser should display the Application Blocked page again.



4. Close the *Firefox browser*.



5. Re-open the PA-VM *firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



6. In the **firewall** web interface, navigate to **Monitor > Logs > URL Filtering**. Create and apply the filter (**action eq block-url**). You should see multiple entries for sessions to www.nbcnews.com and www.theguardian.com that the firewall has blocked.

Please
Note

Note that several default columns have been hidden in the example URL Filtering log file shown here.

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

2.9 Add Custom URL Category to URL Filtering Profile

In this section, you will set the **Block-Per-Company-Policy** category to **block** in the **Corp-URL-Profile** URL Filtering Profile.

1. Select **Objects > Security Profiles > URL Filtering**. Click the **Corp-URL-Profile** entry.

The screenshot shows the PA-VM interface with the following navigation path: PA-VM > DASHBOARD > MONITOR > POLICIES > OBJECTS > Security Profiles > URL Filtering. The 'Corp-URL-Profile' entry is selected and highlighted with a red box. The main table displays various URL profiles with their details under 'NAME', 'LOCATION', and 'SITE ACCESS' columns.

NAME	LOCATION	SITE ACCESS
default	Predefined	Allow Categories (59) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (0)
Corp-URL-Profile		Allow Categories (63) Alert Categories (0) Continue Categories (0) Block Categories (14) Override Categories (0)

2. Under the **Custom URL Categories** section, set the **Site Access** for **Block-Per-Company-Policy** to **block**. Click **OK**.

The screenshot shows the 'URL Filtering Profile' configuration dialog with the 'Categories' tab selected. The 'Custom URL Categories' section lists 'Block-Per-Company-Policy *' with 'Site Access' set to 'block'. The 'OK' button at the bottom right is highlighted with a red box.

3. Navigate to **Policies > Security**. Highlight the entry for **Block-Bad-URLs** but do not open it. Click **Disable** at the bottom of the window.

NAME	TAGS	TYPE	ZONE	ADDRESS
1 Block-Bad-URLs	none	universal	inside	any

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



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

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

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

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			

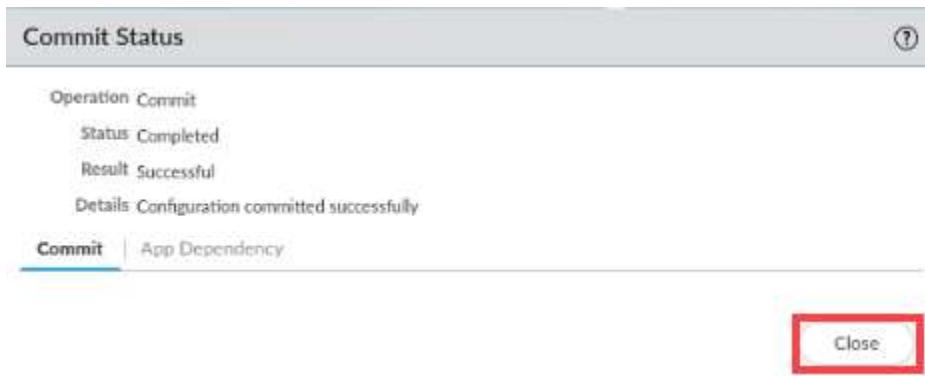
[Preview Changes](#) [Change Summary](#) [Validate Commit](#)

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

Description

Commit **Cancel**

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



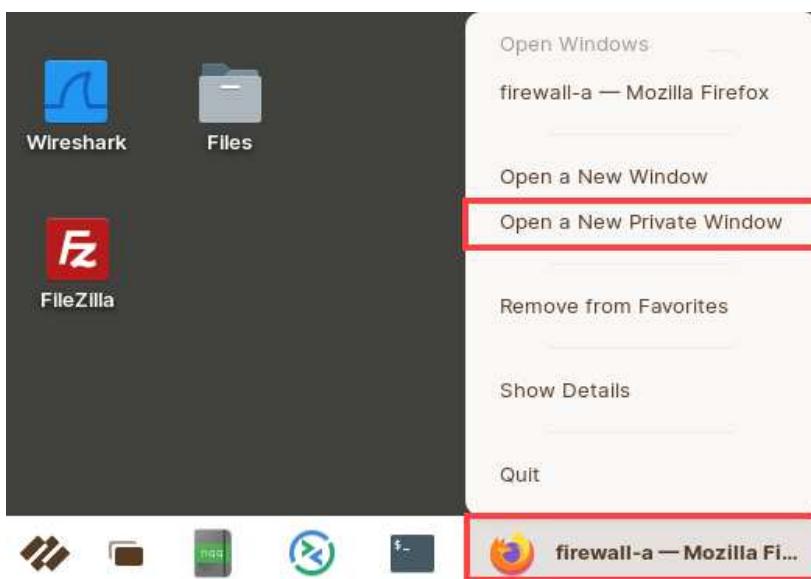
7. Minimize the *Palo Alto Networks Firewall* and continue to the next task.



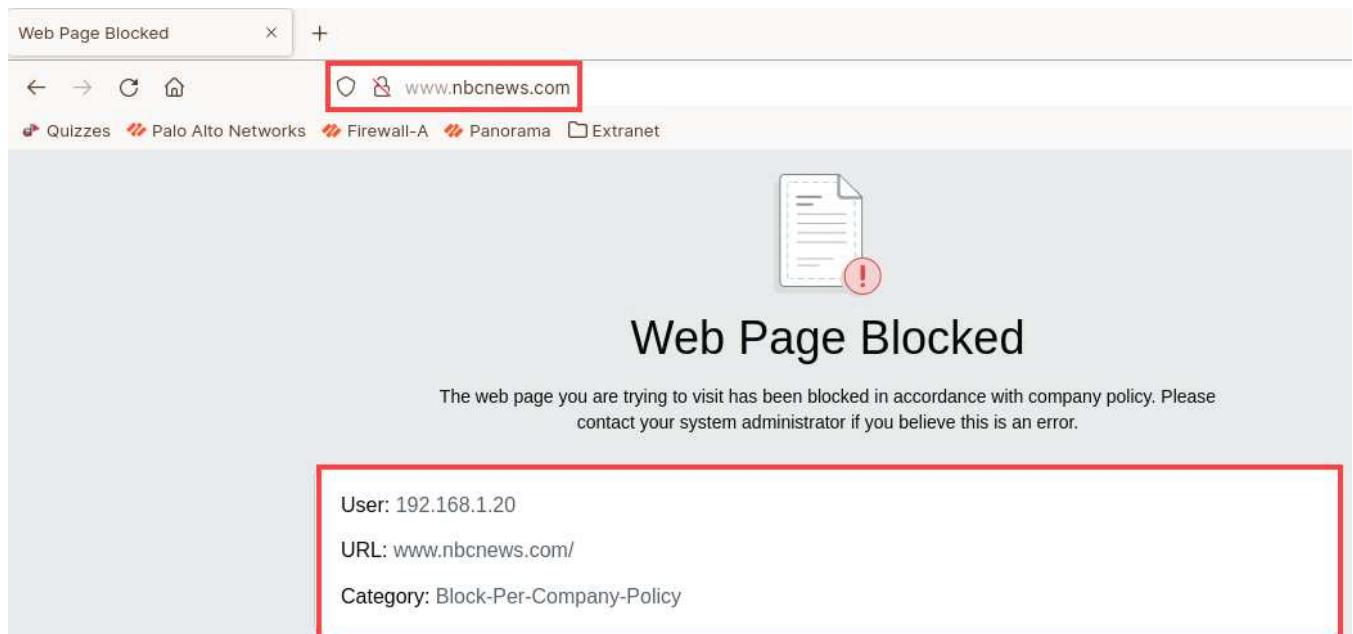
2.10 Test Access to Custom URLs Blocked by the URL Filtering Profile

In this section, you will test access to URLs that belong to the Custom URL Category that you added to the URL Filtering Profile.

1. In the client taskbar, right-click the **firewall-a – Mozilla Firefox Web Browser** application. Select **Open a New Private Window**.

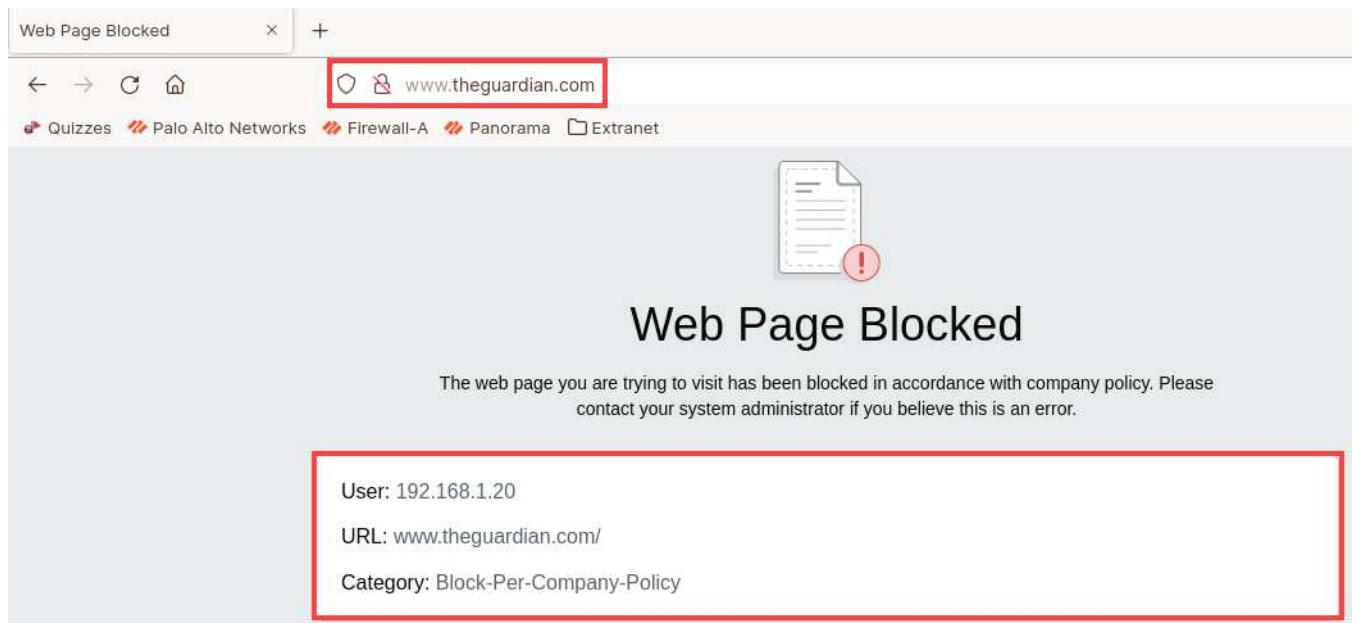


2. Type **www.nbcnews.com**, the browser should display a Web Page Blocked message because the Custom URL Category in the URL Filtering Profile blocks access to the webpage.



The screenshot shows a Firefox browser window with the title "Web Page Blocked". The URL bar contains "www.nbcnews.com". Below the URL bar, there is a message icon (a document with a red exclamation mark) and the text "Web Page Blocked". A message below states: "The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error." At the bottom of the blocked message area, there is a red box highlighting the following information: "User: 192.168.1.20", "URL: www.nbcnews.com/", and "Category: Block-Per-Company-Policy".

3. Type **www.theguardian.com**, the browser should display the Web Page Blocked again.



The screenshot shows a Firefox browser window with the title "Web Page Blocked". The URL bar contains "www.theguardian.com". Below the URL bar, there is a message icon (a document with a red exclamation mark) and the text "Web Page Blocked". A message below states: "The web page you are trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is an error." At the bottom of the blocked message area, there is a red box highlighting the following information: "User: 192.168.1.20", "URL: www.theguardian.com/", and "Category: Block-Per-Company-Policy".

4. Close the *Firefox browser*.



5. Re-open the PA-VM *firewall* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar and continue to the next task.



2.11 Create an External Dynamic List to Block Malicious URL Access

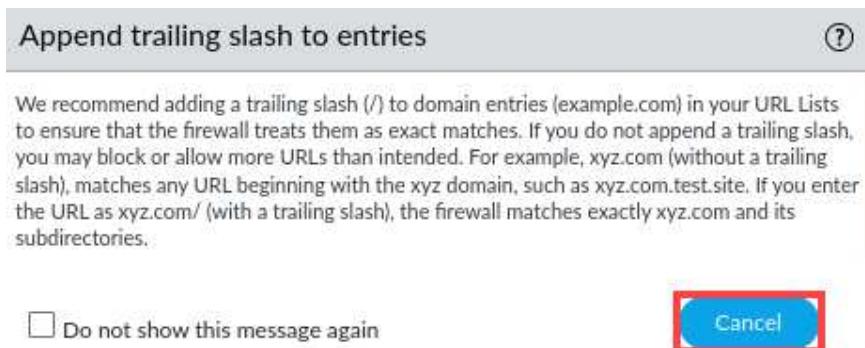
You can add a list of malicious URLs to a file on an external web server, and then configure the firewall to access the list as an External Dynamic List (EDL). The advantage of this approach is that you can regularly update the malicious URL list without the need to recommit the firewall configuration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

1. Select **Objects > External Dynamic Lists**. Click **Add**.

The screenshot shows the PA-VM interface with the 'OBJECTS' tab selected. On the left, there's a sidebar with sections like Global Protect, External Dynamic Lists (which is currently selected and highlighted with a red box), Custom Objects, and others. Below that is a list of security profile groups, log forwarding, authentication, decryption, and decryption profiles. At the bottom of the sidebar, there's an 'Add' button highlighted with a red box. The main area displays a table for 'External Dynamic Lists' with one entry: 'Palo Alto Networks - High risk IP addresses'. The table has columns for 'Name', 'Type', and 'Description'.

Name	Type	Description
Palo Alto Networks - High risk IP addresses	Predefined	IP address been featured in advisories trust organizations because bad providers can use them to distribute unethical

2. The firewall presents a notice about adding a trailing slash for domain entries, read the notice and click **Cancel**.



3. In the *External Dynamic Lists* window, configure the following and click **OK**.

Parameter	Value
Name	malicious-urls-edl
Type	URL List
Description	List of malicious URLs maintained on Extranet server
Source	http://192.168.50.80/malicious-urls.txt (The EDL contains a single URL for testing purposes - www.popurls.com)
Check for updates	Every Five Minutes

Name **malicious-urls-edl**

Type **URL List**

Description **List of malicious URLs maintained on Extranet server**

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

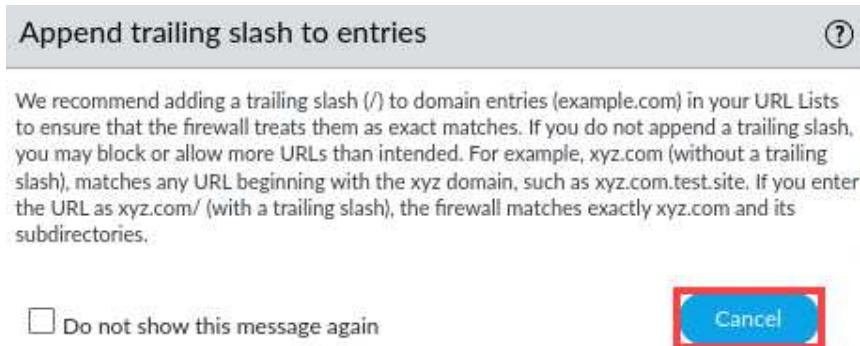
Check for updates **Every five minutes**

OK **Cancel**

4. Click **malicious-urls-edl**.

Dynamic Domain Lists					
<input type="checkbox"/>	malicious-domains-edl	Custom list of bad domains maintained on Extranet server	http://192.168.50.80/malicious-domains.txt	None	Every five minutes

5. The firewall presents a notice about adding a trailing slash for domain entries, read the notice and click **Cancel**.



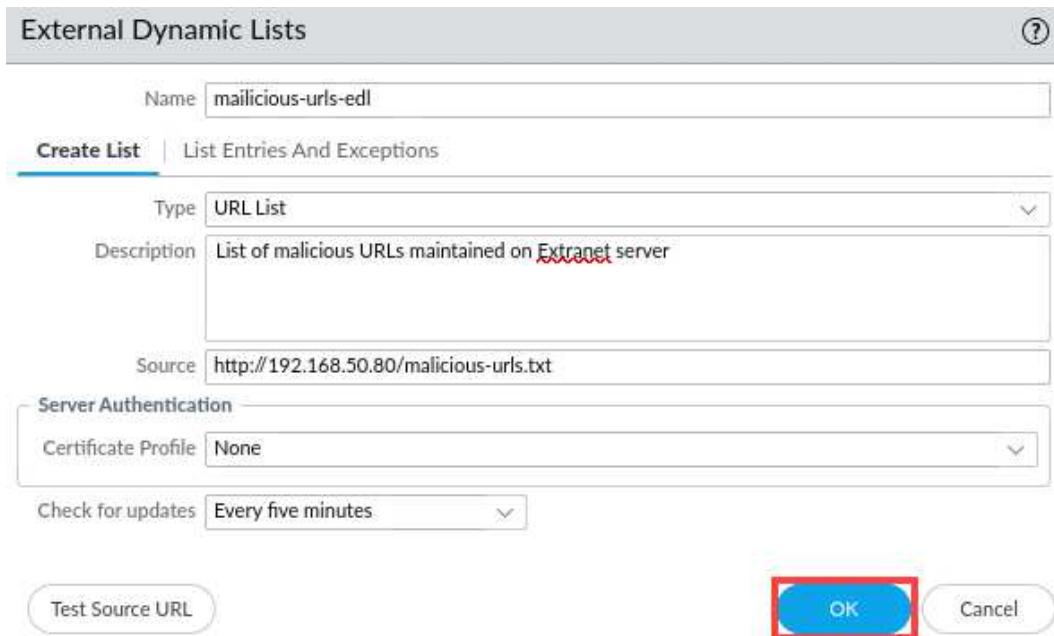
6. Click **Test Source URL** to verify that the firewall can access the EDL URL.



7. A message window should open and state that the source URL is accessible. Click **Close**.



8. Click **OK** to close the **External Dynamic Lists** window.



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

2.12 Block Access to the URL List with a Security Policy Rule

In this section, you will add the EDL containing the malicious URL list to a Security Policy rule with a “deny” action.

1. Select **Policies > Security** and click the **Block-Bad-URLs** policy.

NAME	TAGS	TYPE	ZONE
Block-Bad-URLs	none	universal	Users_Net

2. In the **Security Policy Rule** window, click the **Service/URL Category** tab and configure the following. Click **OK**.

Parameter	Value
URL Category	Add malicious-urls-edl to the list. This EDL will block access to www.popurls.com.

The screenshot shows the 'Service/URL Category' tab selected in the top navigation bar. On the right, a list of categories is displayed, with 'malicious-urls-edl' checked. The 'OK' button at the bottom right is also highlighted with a red box.

3. With the **Block-Bad-URLs** Security Policy rule highlighted, click **Enable** at the bottom of the window.

The screenshot shows a list of security policy rules. The first rule, 'Block-Bad-URLs', is highlighted with a red box. At the bottom of the list, the 'Enable' button is also highlighted with a red box.

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



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

Commit

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

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

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
▶ policy-and-objects	Policy and Objects			

Preview Changes Change Summary Validate Commit

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

Description

Commit **Cancel**

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

Commit Status

Operation Commit
Status Completed
Result Successful
Details: Configuration committed successfully

Commit | App Dependency

Close

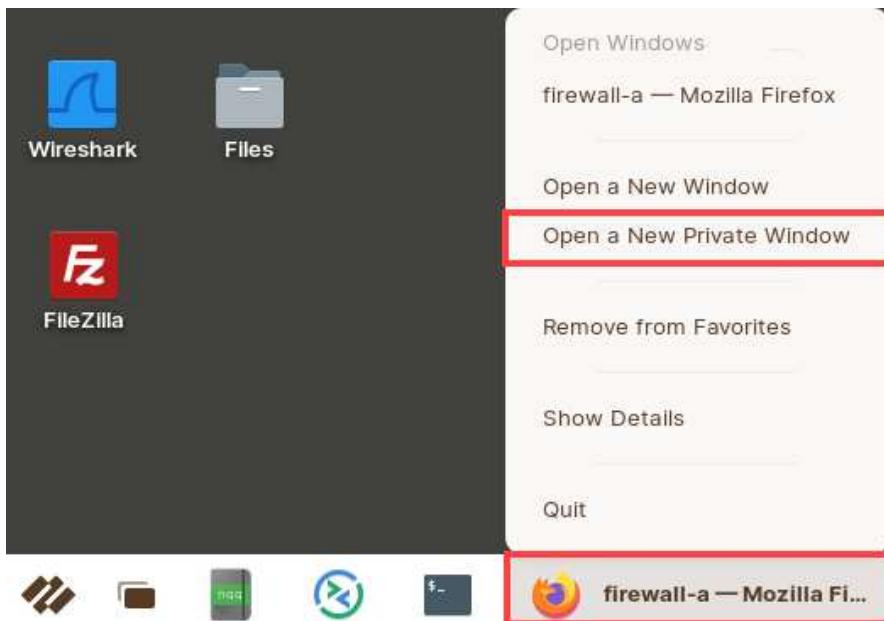
7. Minimize the *Palo Alto Networks Firewall* open and continue to the next task.



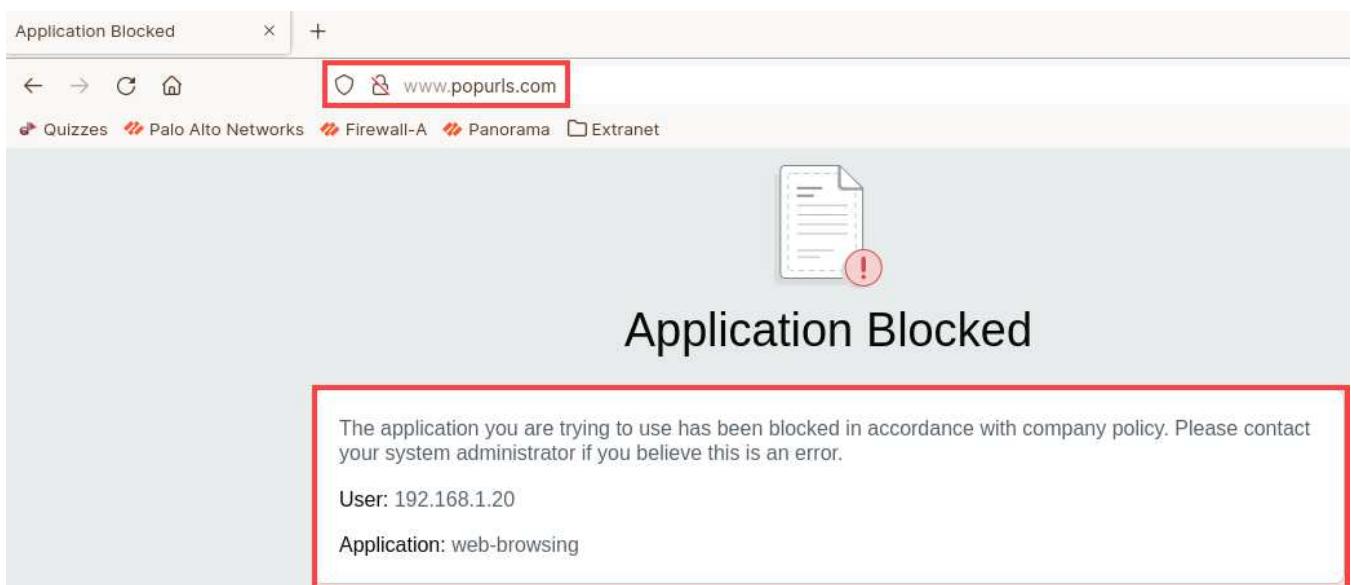
2.13 Test Access to a URL in the EDL added to the Security Policy Rule

In this section, you will test access to a URL that is contained in the EDL that you added to a Security Policy rule with a “deny” action.

1. In the client taskbar, right-click the **firewall-a – Mozilla Firefox Web Browser** application. Select **Open a New Private Window**.



2. Type **www.popurls.com**, the browser should display an Application Blocked because the EDL in the Security Policy blocks access to the popurls.com webpage.



3. Close the *Firefox browser*.



4. Re-open the PA-VM *firewall-a* web interface by clicking on the **firewall-a – Mozilla Firefox** icon in the task bar.



5. Navigate to **Monitor > Logs > URL Filtering** and clear any filters you have in place.

TO ZONE	SOURCE
Internet	192.168.1.20
Internet	192.168.1.20
Internet	192.168.1.20

6. Create and apply the (**action eq block-url**) filter that will display entries that have an action of block-url. You should see multiple entries for sessions to www.popurls.com that the firewall has blocked.

RECEIVE TIME	CATEGORY	URL	ACTION	FROM ZONE	TO ZONE	SOURCE
09/21 02:43:53	malicious-urls-edl	www.popurls.com/favicon.ico	block-url	Users_Net	Internet	192.168.1.20
09/21 02:43:53	malicious-urls-edl	www.popurls.com/login/css/latofonts.css	block-url	Users_Net	Internet	192.168.1.20
09/21 02:43:53	malicious-urls-edl	www.popurls.com/	block-url	Users_Net	Internet	192.168.1.20
09/21 02:43:48	malicious-urls-edl	www.popurls.com/	block-url	Users_Net	Internet	192.168.1.20
09/21 02:43:48	malicious-urls-edl	www.popurls.com/	block-url	Users_Net	Internet	192.168.1.20
09/21 02:43:48	malicious-urls-edl	www.popurls.com/	block-url	Users_Net	Internet	192.168.1.20

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