



PALO ALTO NETWORKS - EDU-210

Lab 6: URL Filtering

Document Version: 2017-09-29

Copyright © 2017 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
6 Lab: URL Filtering	6
6.0 Load Lab Configuration	6
6.1 Create a Security Policy Rule with a Custom URL Category	7
6.2 Test Security Policy Rule.....	13
6.3 Review Logs	13
6.4 Configure an External Dynamic List	15
6.5 Test Security Policy Rule.....	17
6.6 Review Logs	18
6.7 Create a Security Policy Rule with URL Filtering Profile.....	19
6.8 Test Security Policy Rule with URL Filtering Profile	22
6.9 Review Logs	23
6.10 Modify Security Profile Group	23

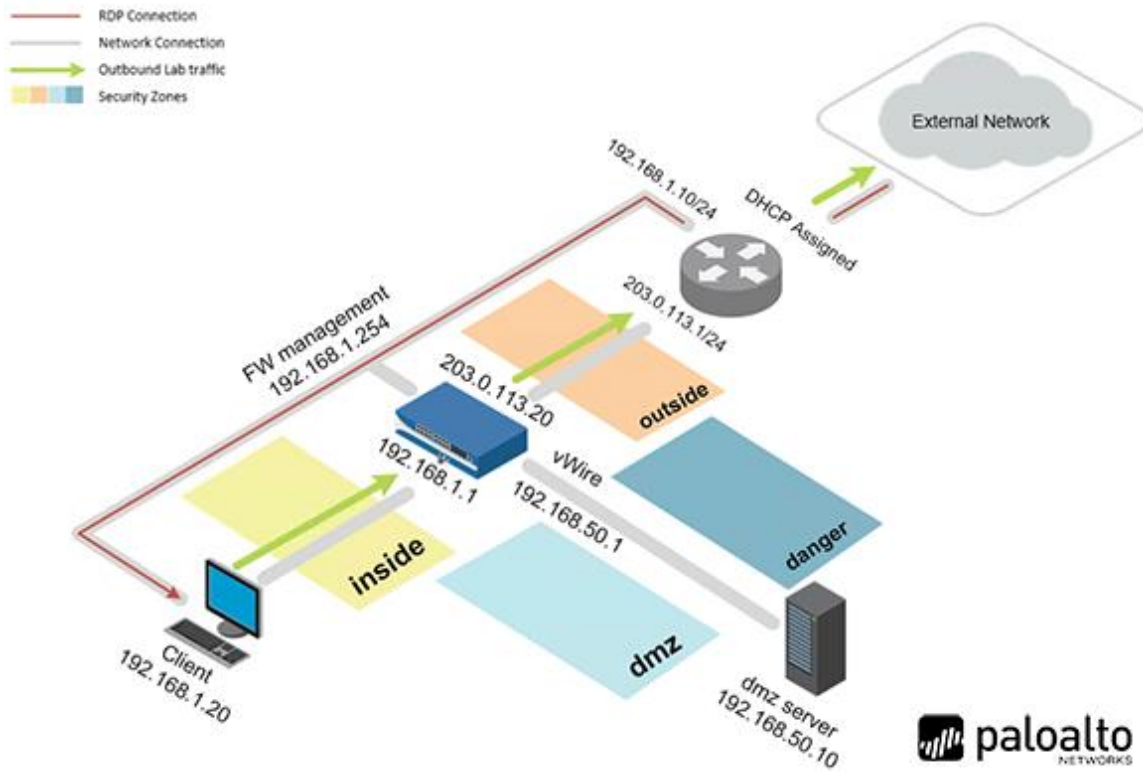
Introduction

The company has security policies in place that scan for spyware, malware, viruses, vulnerabilities, and file blocking. Now the company would like to implement URL filtering. You are needed to create profiles that will meet the requirements of the company's internet usage policy.

Objectives

- Create a custom URL category and use it as a Security policy rule match criterion and as part of a URL Filtering Profile.
- Configure and use an External Dynamic List as a URL block list.
- Create a URL Filtering Profile and observe the difference between using url-categories in a Security policy versus a profile.
- Review firewall log entries to identify all actions and changes.

Lab Topology



Lab Settings

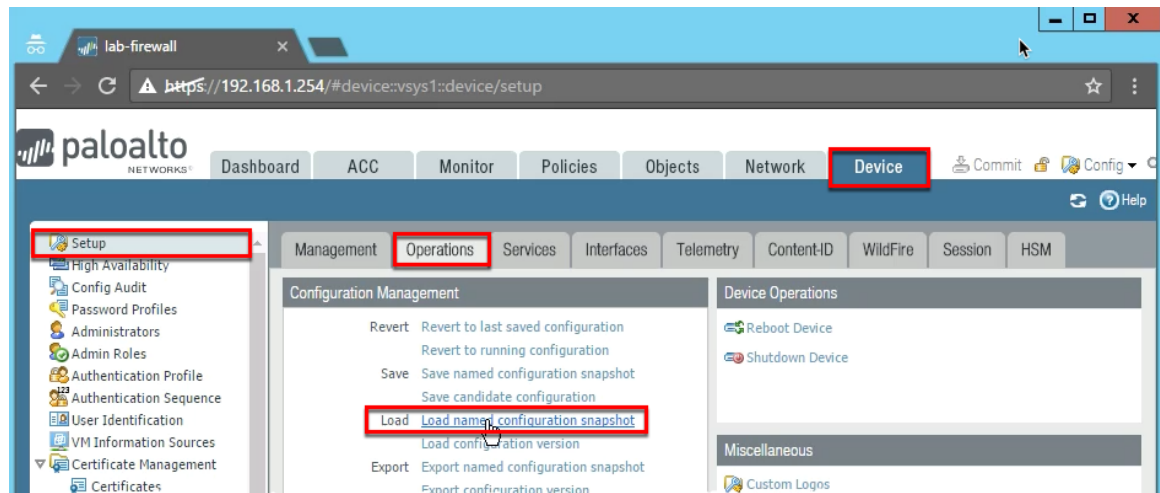
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

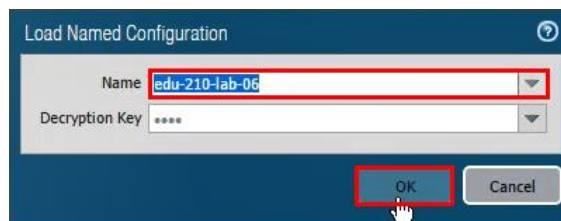
6 Lab: URL Filtering

6.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-06** and click **OK**.

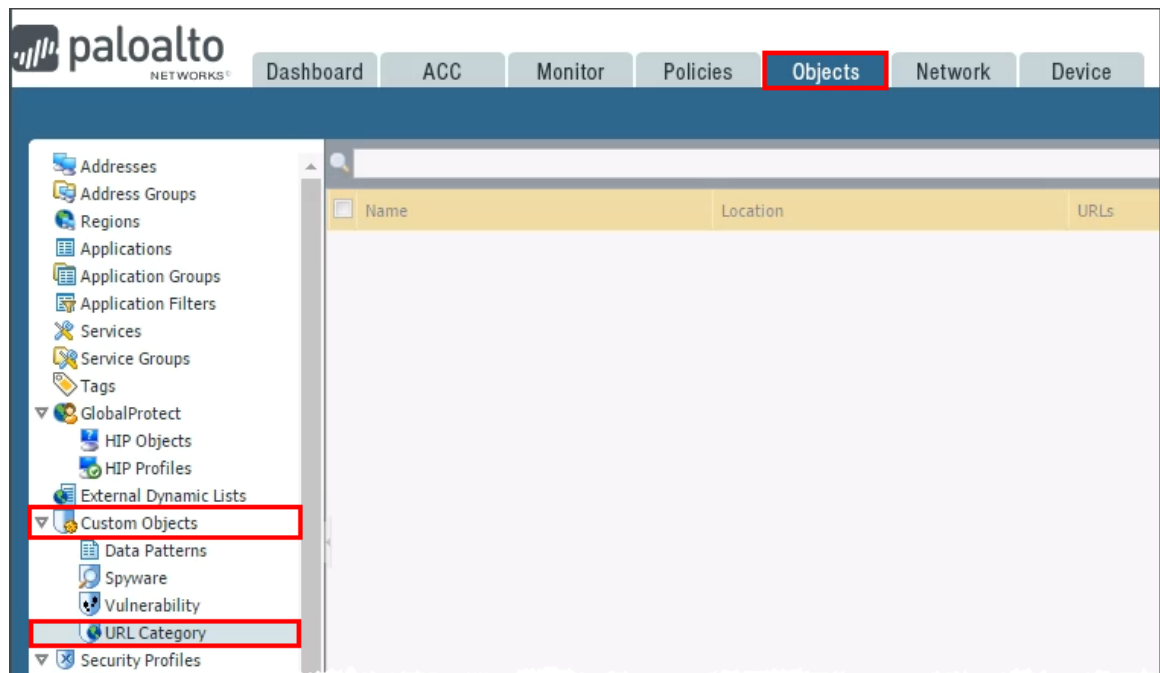


4. Click **Close**.
5. **Commit** all changes.

6.1 Create a Security Policy Rule with a Custom URL Category

Use a custom URL Category object to create your custom list of URLs and use it in a URL Filtering Profile or as match criteria in Security policy rules. In a custom URL Category, you can add URL entries individually, or import a text file that contains a list of URLs.

1. Select **Objects > Custom Objects > URL Category**.



2. Click **Add** to create a custom URL Category.



3. Configure the following:

Parameter	Value
Name	tech-sites
Sites	newegg.com engadget.com techradar.com *.newegg.com *.engadget.com

	*.techradar.com
--	-----------------

Custom URL Category

Name: **tech-sites**

Description:

6 items

Sites

- ☐ newegg.com
- ☐ engadget.com
- ☐ techradar.com
- ☐ *.newegg.com
- ☐ *.engadget.com
- ☒ *.techradar.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.

OK Cancel

- Click **OK** to close the Custom URL Category configuration window.
- Select **Policies > Security**.

paloalto NETWORKS

Dashboard ACC Monitor **Policies** Objects Network Device Commit Config Help

Security

8 items

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
1 internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any
2 egress-outside-app-id	egress	universal	inside	any	any	any	outside	any
3 egress-outside	egress	universal	inside	any	any	any	outside	any
4 internal-dmz-ftp	internal	universal	inside	any	any	any	dmz	any
5 egress-outside-content-id	egress	universal	inside	any	any	any	outside	any
6 danger-simulated-traffic	none	universal	danger	any	any	any	danger	any

Tag Browser

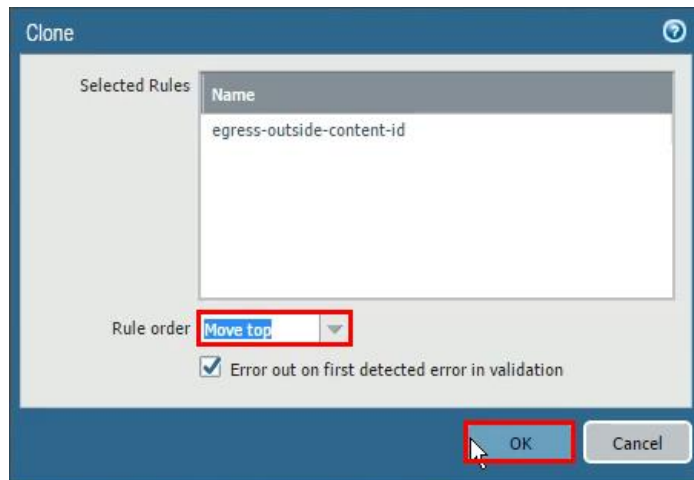
5 items

Tag(#)	Rule
internal (1)	1
egress (2)	2-3
internal (1)	4
egress (1)	5

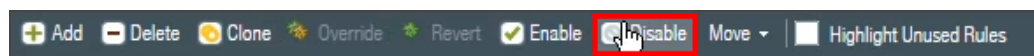
- Select the **egress-outside-content-id** Security policy rule without opening it.
- Click **Clone**. The Clone configuration window opens.

+ Add - Delete **Clone** Override Revert Enable Disable Move Highlight Unused Rules

8. Select **Move top** from the Rule Order drop-down list.



9. Click **OK** to close the Clone configuration window.
10. With the original **egress-outside-content-id** Security policy rule still selected, click **Disable**.

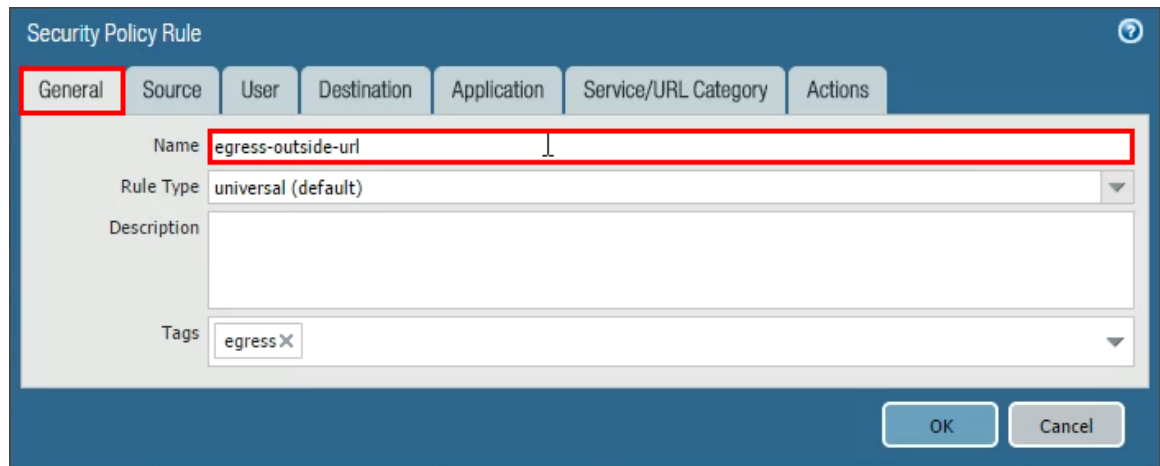


11. Notice that the **egress-outside-content-id** is now grayed out and in italic font:



12. Click **egress-outside-content-id-1** to open the cloned Security policy rule named egress-outside-content-id-1.
13. Configure the following under the General tab:

Parameter	Value
Name	egress-outside-url



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: egress-outside-url

Rule Type: universal (default)

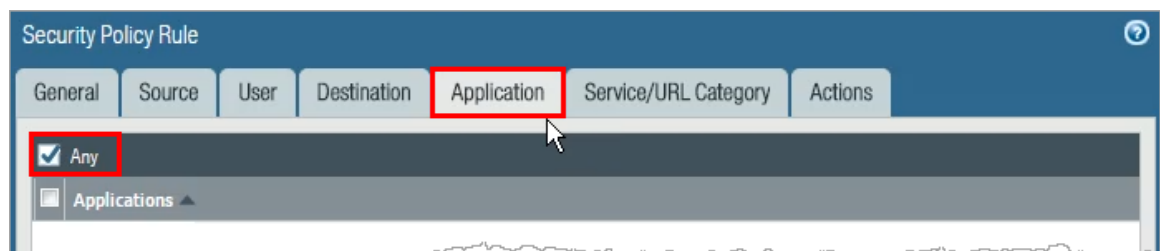
Description:

Tags: egress

OK Cancel

14. Click the **Application** tab and configure the following:

Parameter	Value
Applications	<input checked="" type="checkbox"/> Any



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

☒ Any

☐ Applications

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

Parameter	Value
URL Category	<input checked="" type="checkbox"/> tech-sites



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

application-default

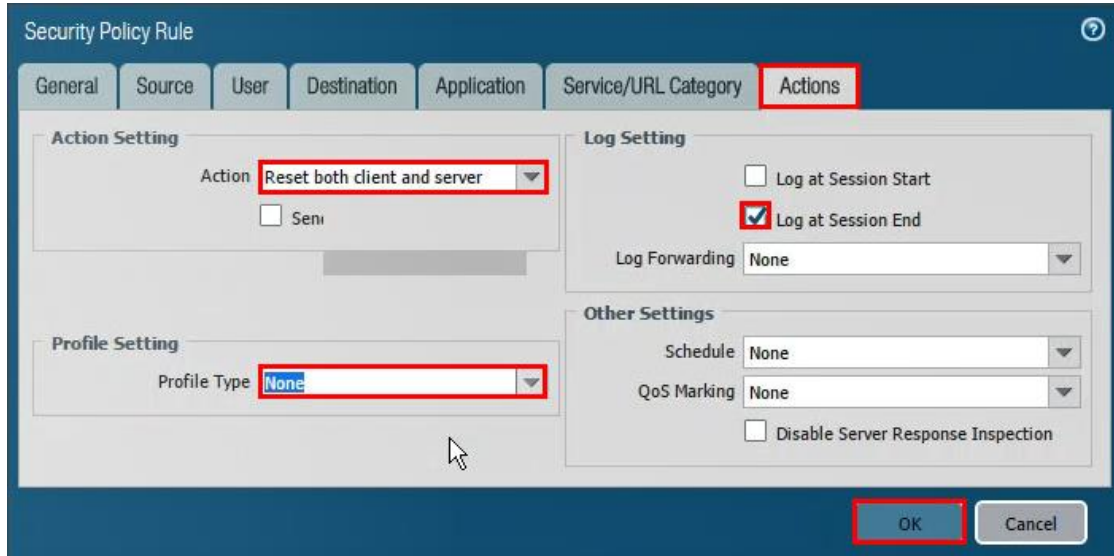
☐ Any

☒ URL Category

☒ tech-sites

16. Click the **Actions** tab and configure the following:

Parameter	Value
Action Setting	Reset both client and server
Log Setting	<input type="checkbox"/> Log at Session Start <input checked="" type="checkbox"/> Log at Session End
Profile Setting	Profile Setting Profile Type None



Security Policy Rule

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

Action Setting

Action Reset both client and server

☐ Send

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding None

Profile Setting

Profile Type None

Other Settings

Schedule None

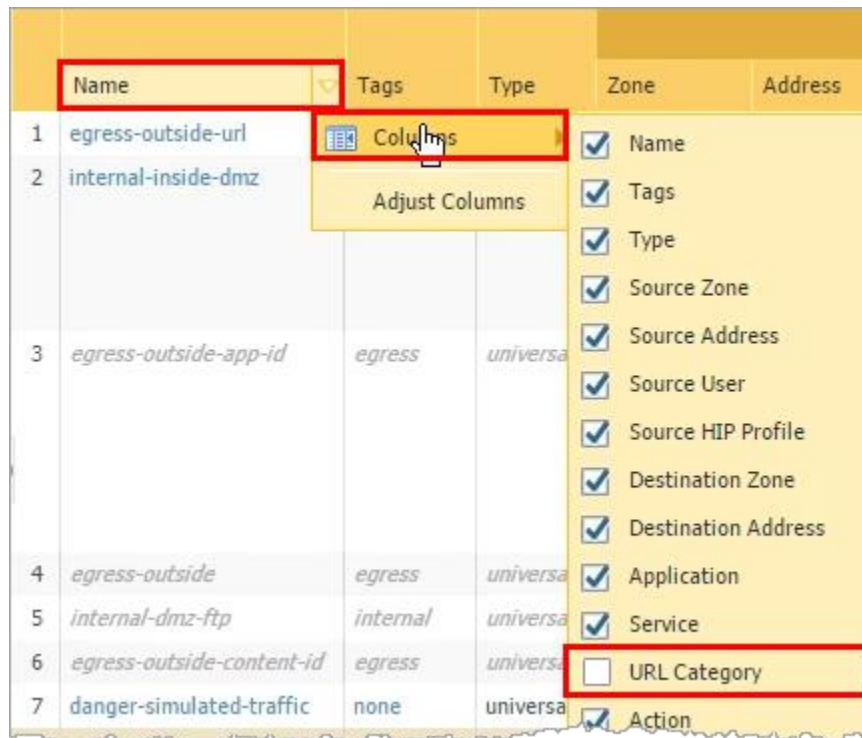
QoS Marking None

☐ Disable Server Response Inspection

OK Cancel

17. Click **OK** to close the Security Policy Rule configuration window.

18. Hover over the **Name** column and click the **down-arrow**:



19. Expand the **Columns** menu using the right-arrow and select the **URL Category** check box. The URL Category column is displayed.
20. Enable the rule **egress-outside**.

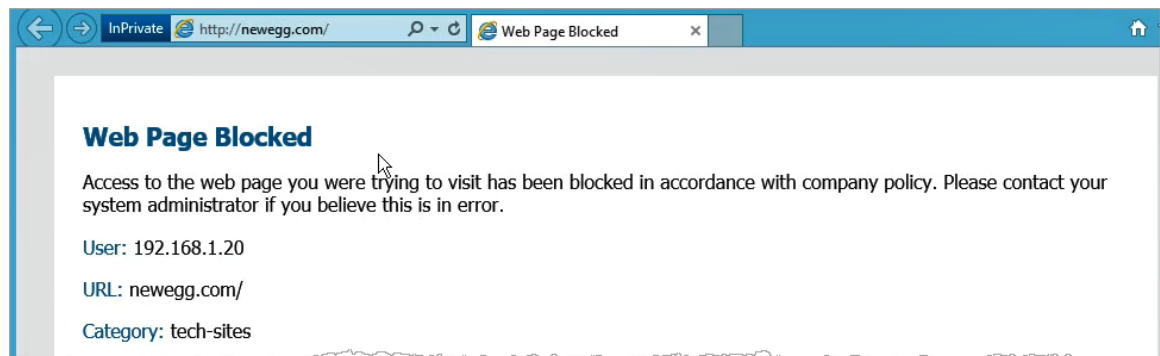


21. **Commit** all changes.

Note: Because you created a rule that resets traffic, you need to enable the egress-outside rule to allow everything else.

6.2 Test Security Policy Rule

1. Open a browser in private/incognito mode and browse to **newegg.com**:



The URL is blocked by the Security policy rule named **egress-outside-url**.

2. In the same browser window verify that **techradar.com** is blocked.
3. In the same browser window, check if **https://www.engadget.com** also is blocked.

Note that this was an SSL connection. Because the firewall is not decrypting traffic, the connection is reset without a URL block page. If the firewall intercepted this connection and displayed the URL block page, the browser would assume a man-in-the-middle attack might be in progress.

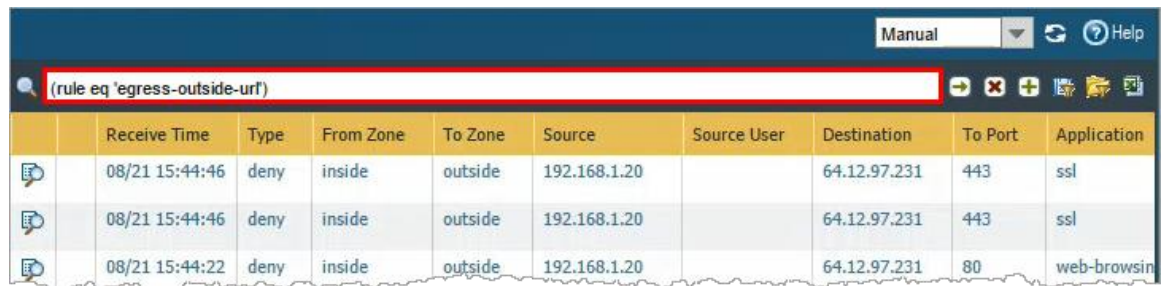
6.3 Review Logs

1. Hover over the **egress-outside-url** Security policy rule, click the down-arrow, and select **Log Viewer** to open the Traffic log:

	Name	Tags	Type	Source				Destination	
				Zone	Address	User	HIP Profile	Zone	Address
1	egress-outside-url	Filter	Universal	any	inside	any	any	any	outside
2	internal-inside-dmz	Log Viewer	Universal	any	inside	any	any	any	dmz

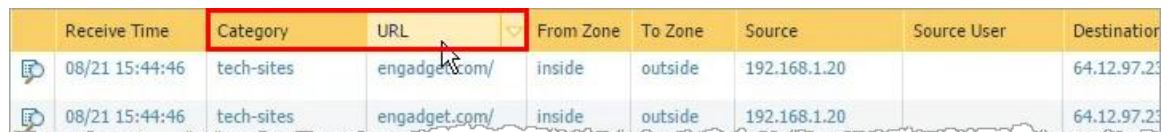
2. Notice that the firewall adds (`rule eq 'egress-outside-url'`) to the Traffic log filter text box:

Lab 6: URL Filtering



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
	08/21 15:44:46	deny	inside	outside	192.168.1.20		64.12.97.231	443	ssl
	08/21 15:44:46	deny	inside	outside	192.168.1.20		64.12.97.231	443	ssl
	08/21 15:44:22	deny	inside	outside	192.168.1.20		64.12.97.231	80	web-browsin

3. The **URL Category** column can be added to the Traffic log to provide additional information.
4. Select the **URL Filtering** log.
5. Notice that URL Filtering log includes the **Category** and **URL** columns by default:



	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination
	08/21 15:44:46	tech-sites	engadget.com/	inside	outside	192.168.1.20		64.12.97.231
	08/21 15:44:46	tech-sites	engadget.com/	inside	outside	192.168.1.20		64.12.97.231

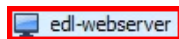
6.4 Configure an External Dynamic List

An External Dynamic List is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules.

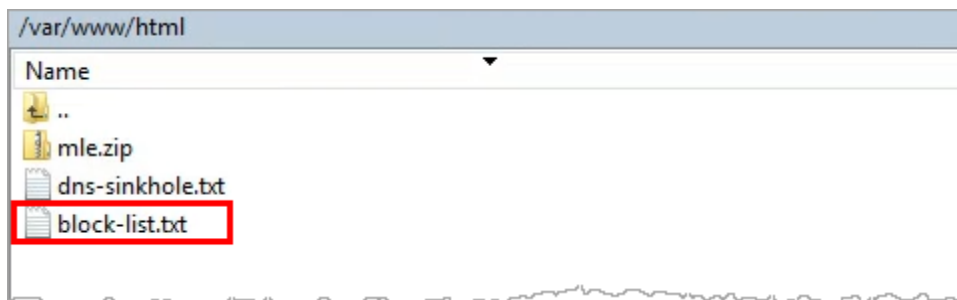
1. Open WinSCP on the Windows desktop.



2. Double-click the list item **edl-webserver**.

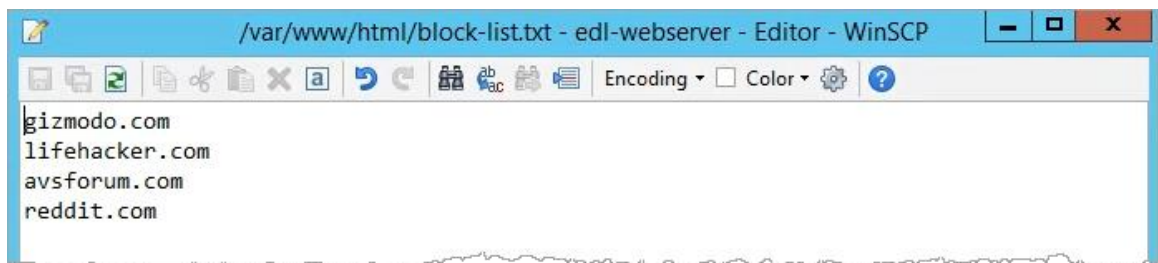


3. Locate the text file in the right window pane named **block-list.txt** and double-click on it to edit it.



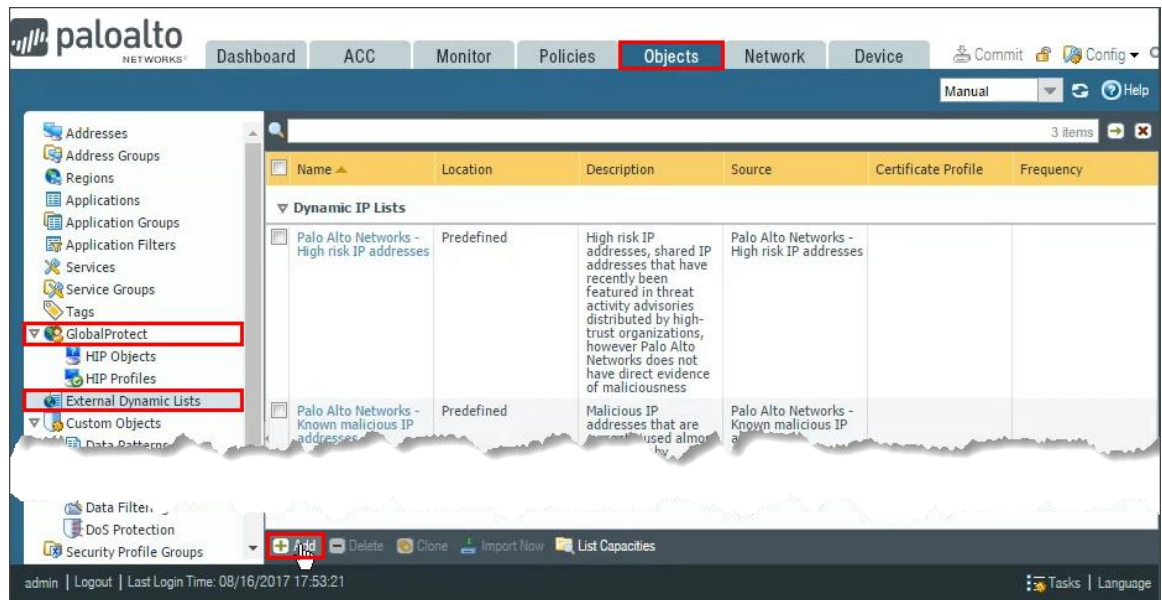
4. Verify that the following URLs exist, each followed by a line break:

```
gizmodo.com
lifehacker.com
avsforum.com
reddit.com
```



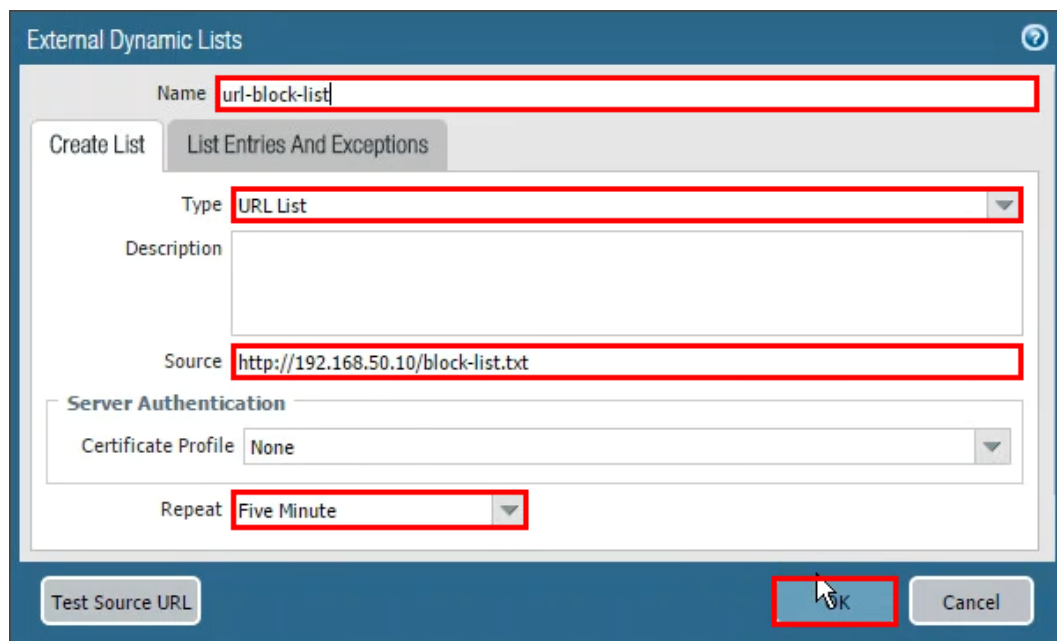
5. **Save** and **Close** the file.
6. **Close** the WinSCP window.

7. In the WebUI select **Objects > External Dynamic Lists**.



8. Click **Add** to configure a new External Dynamic List.
9. Configure the following:

Parameter	Value
Name	url-block-list
Type	URL List
Source	http://192.168.50.10/block-list.txt
Repeat	Five Minute

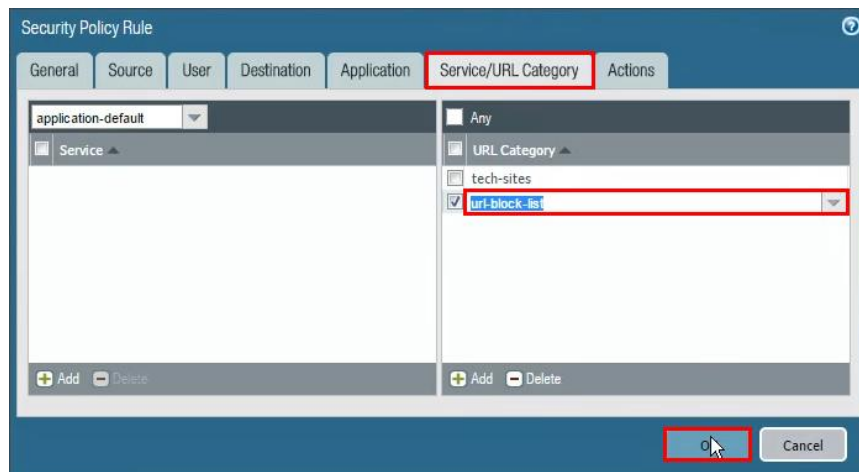


The screenshot shows the 'External Dynamic Lists' configuration form. The 'Name' field is 'url-block-list'. The 'Type' dropdown is set to 'URL List'. The 'Source' field is 'http://192.168.50.10/block-list.txt'. The 'Repeat' dropdown is set to 'Five Minute'. The 'Add' button at the bottom right is highlighted with a red box.

10. Click **OK** to close the External Dynamic Lists configuration window.
11. Go to **Policies > Security**.



12. Click to open the Security policy rule named **egress-outside-url**.
13. Click the **Service/URL Category** tab.
14. Add the newly created External Dynamic List to the **URL Category** list:



15. Click **OK** to close the Security Policy Rule configuration window.
16. **Commit** all changes.

6.5 Test Security Policy Rule

1. Open a browser in private/incognito mode and browse to **avsforum.com**:



The URL is blocked by the Security policy rule named egress-outside-url.

2. In the same browser window verify that gizmodo.com and lifehacker.com also are blocked.

6.6 Review Logs

1. In the WebUI select **Monitor > Logs > URL Filtering**.
2. Notice the new entries in the category and action columns:

	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
	12/02 12:59:42	url-block-list	avsforum.com/f...	private	public	192.168.1.20		173.192.76.217	web-browsing	block-ur
	12/02 12:59:42	url-block-list	avsforum.com/f...	private	public	192.168.1.20		173.192.76.217	web-browsing	block-ur
	12/02 12:59:42	url-block-list	avsforum.com/	private	public	192.168.1.20		173.192.76.217	web-browsing	block-ur

6.7 Create a Security Policy Rule with URL Filtering Profile

1. Select **Objects > Security Profiles > URL Filtering**. Click **Add** to define a URL Filtering Profile.

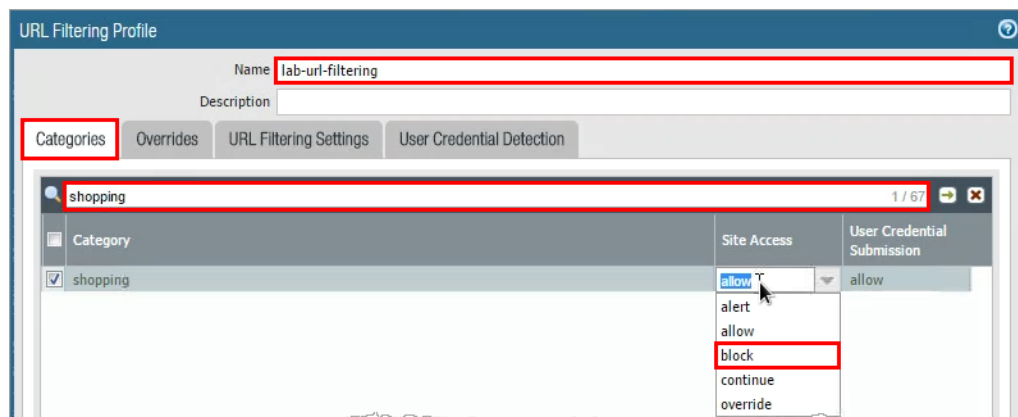


2. Configure the following:

Parameter	Value
Name	egress-outside-url

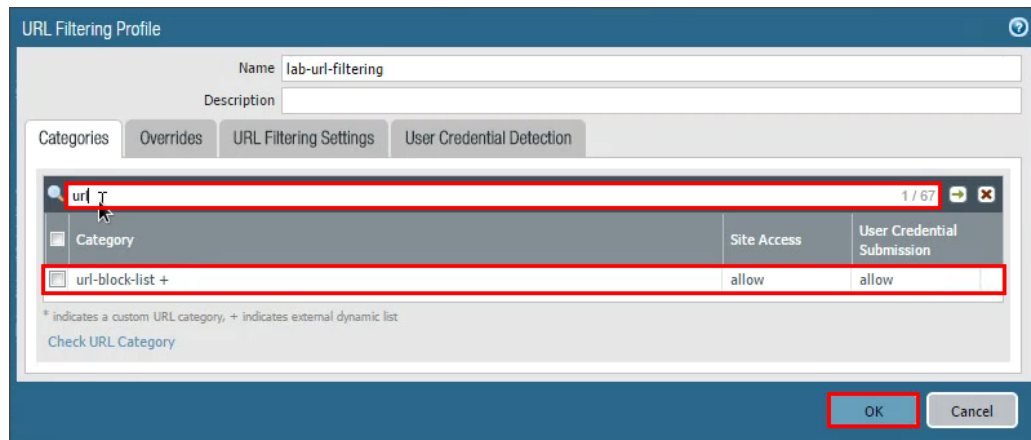
3. Click the **Categories** tab.
4. Search the Category field for the following three categories and set the **Site Access** to block:

shopping
government
hacking

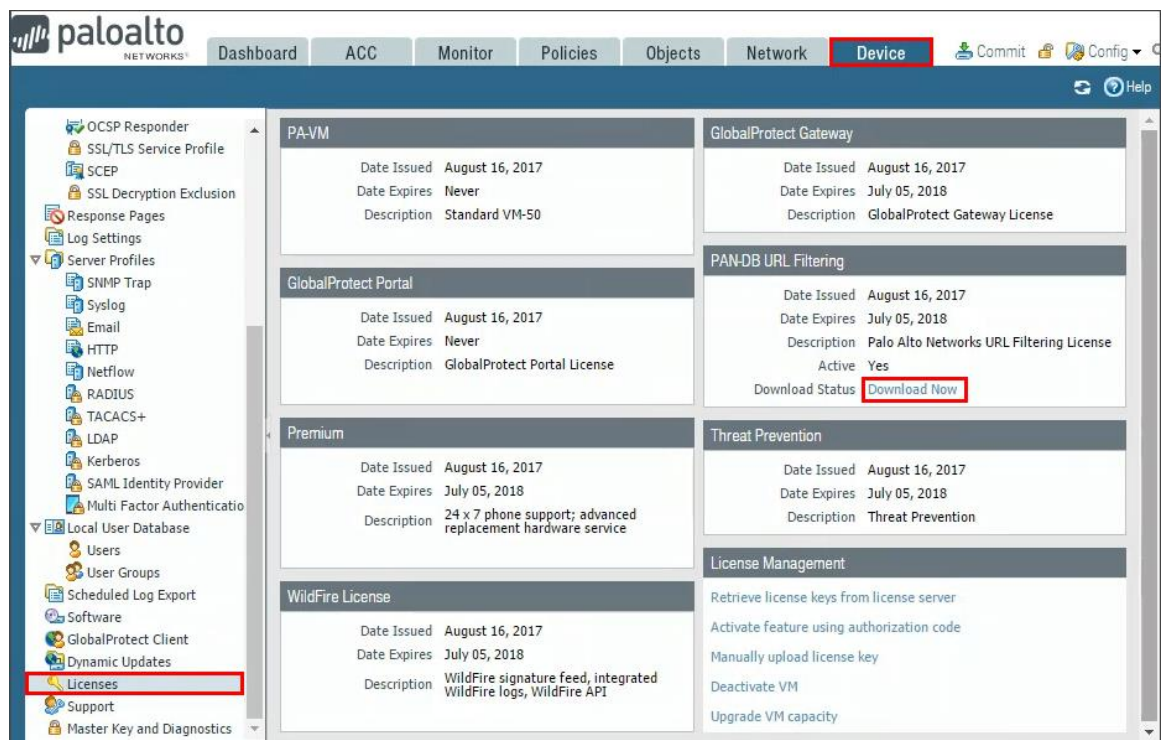


Lab 6: URL Filtering

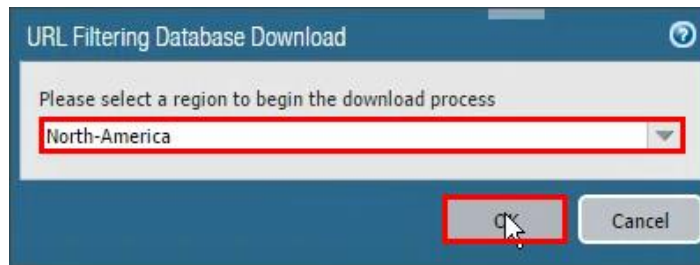
5. Search for url-block-list and tech-sites. Notice that your custom URL categories are also listed and they are set to a Site Access of “allow.” Leave them set to “allow.”



6. Click **OK** to close the URL Filtering Profile window.
7. Select **Device > Licenses**.



8. Under the PAN-DB URL Filtering header, click **Download Now** (or **Re-Download**). A warning might appear; click **Yes**.
9. Select the region nearest the location of your firewall and click **OK**.



After the download completes, a Download Successful window appears.

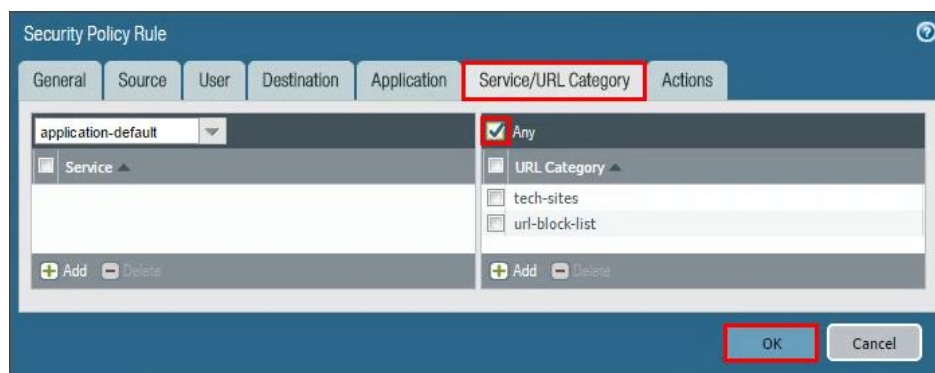
- Click **Close** to close the download status window. The WebUI should now show a message similar to the following:



- Select **Policies > Security**.

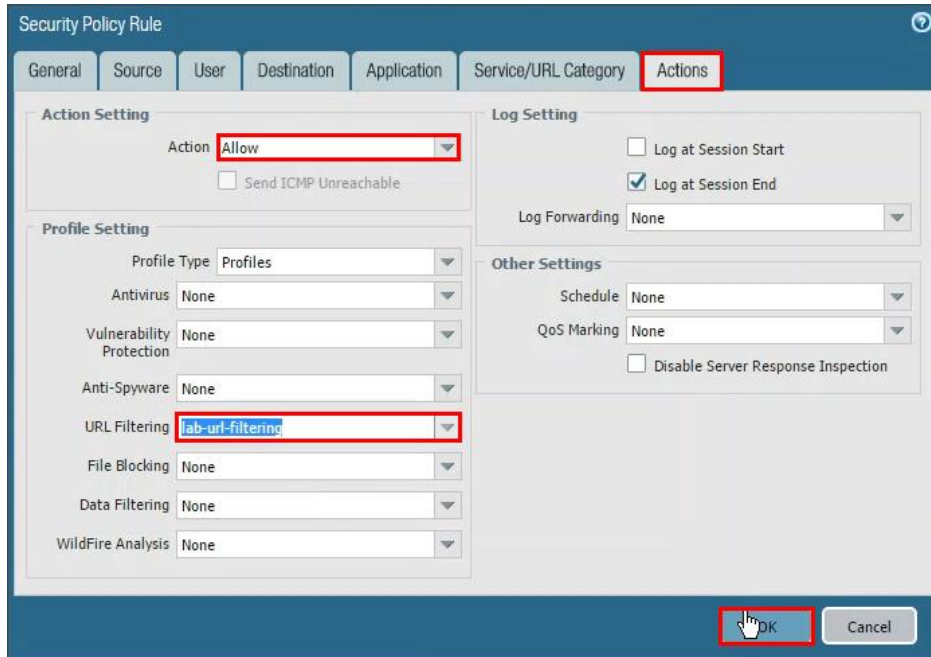


- Click to open the Security policy rule named **egress-outside-url**.
- Click the **Service/URL Category** tab then select **Any** above the **URL Category** list.



- Click the **Actions** tab and configure the following.

Parameter	Value
Action	Allow
Profile Setting – URL Filtering	lab-url-filtering



15. Click **OK** to close the Security Policy Rule configuration window.

16. **Disable** the egress-outside rule.

Note: You can disable the **egress-outside** rule because the URL Filtering Profile is being used and the **egress-outside-url** Security policy rule now allows traffic.

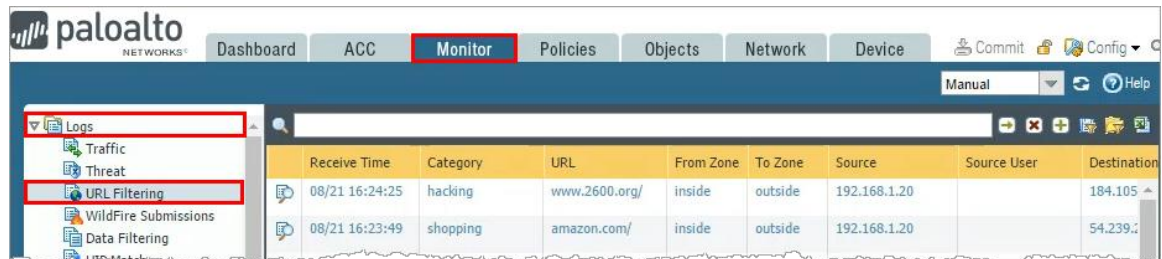
17. **Commit** all changes.

6.8 Test Security Policy Rule with URL Filtering Profile

1. Open a different browser (not a new tab) in private/incognito mode and browse to www.newegg.com. The URL www.newegg.com belongs to the shopping URL category. Based on the Security policy rule named egress-outside-url, the URL is now allowed even though you chose to block the shopping category because your custom URL category has newegg.com listed and is set to “allow,” and your custom category is evaluated before the Palo Alto Networks URL categories.
2. In the same browser window verify that <http://www.transportation.gov> (government), <http://www.amazon.com> (Shopping), and <http://www.2600.org> (hacking) are blocked.
3. Close all browser windows except for the firewall WebUI.

6.9 Review Logs

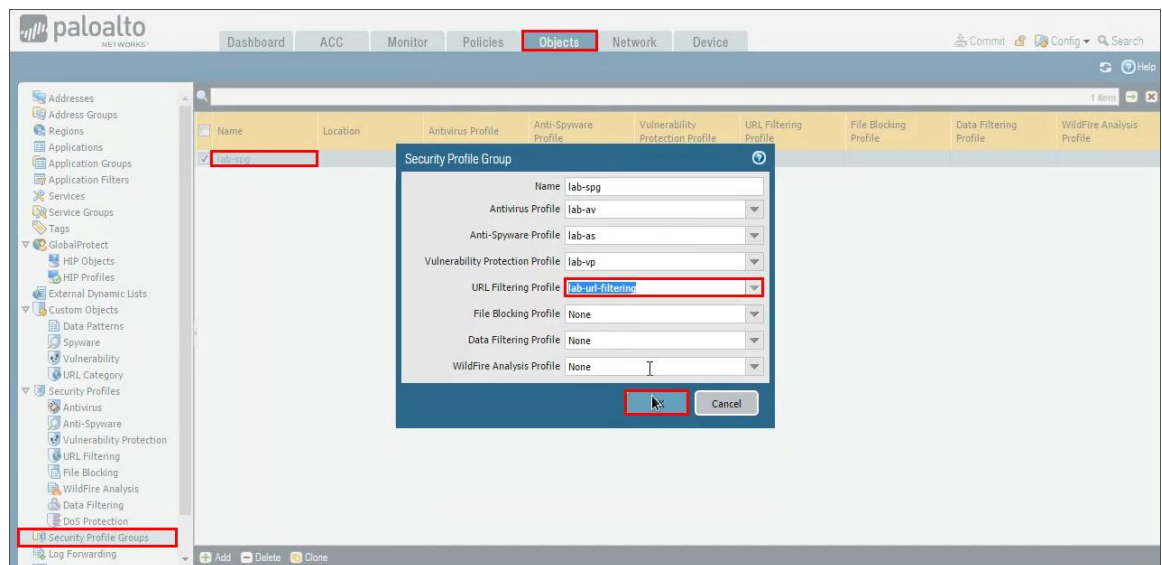
1. Select **Monitor > Logs > URL Filtering**.
2. Review the actions taken on the following entries:



Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination
08/21 16:24:25	hacking	www.2600.org/	inside	outside	192.168.1.20		184.105
08/21 16:23:49	shopping	amazon.com/	inside	outside	192.168.1.20		54.239.2

6.10 Modify Security Profile Group

1. In the WebUI select **Objects > Security Profile Groups** then click **lab-spg** Security Profile Group.



2. Select the newly created URL Filtering Profile: **lab-url-filtering** then click **OK**.
3. Select **Policies > Security**.
4. Select the **egress-outside-content-id** Security policy rule without opening it.
5. Click **Enable**.
6. Select the **egress-outside-url** Security policy rule without opening it.
7. Click **Delete**.
8. **Commit** all changes.

Stop. This is the end of the URL Filtering lab.