



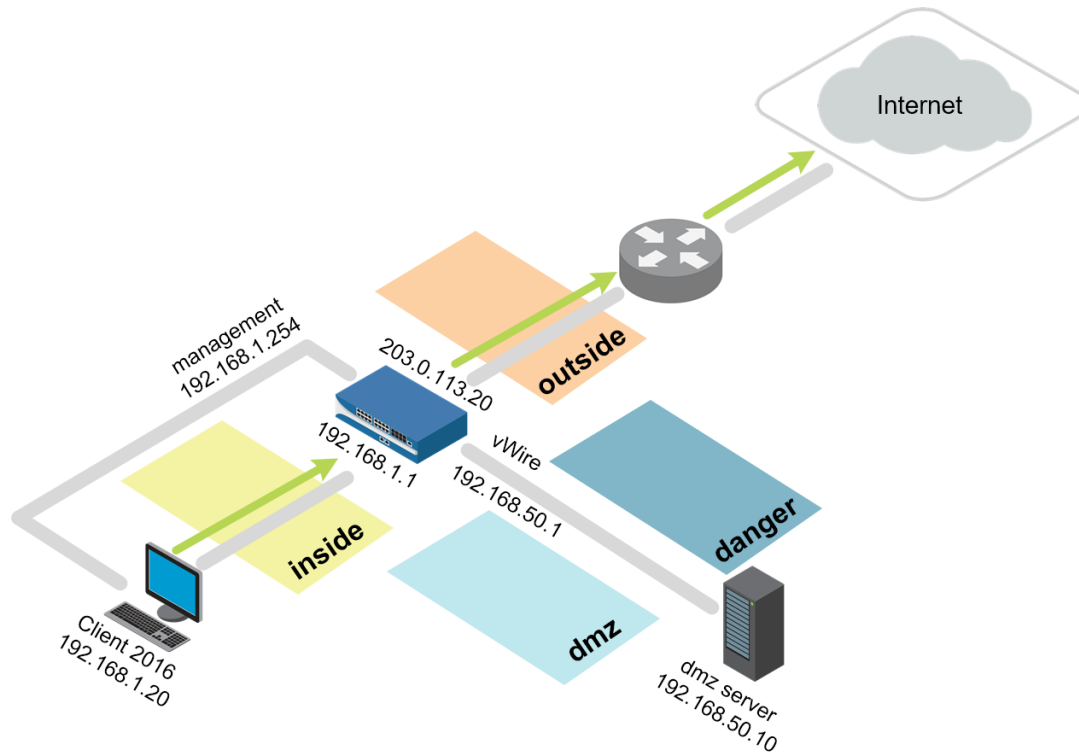
# **Palo Alto Networks Academy Labs Lab URL Filtering**

**Document Version: 10-Dec-19**

Copyright © 2018 Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

## Lab Topology

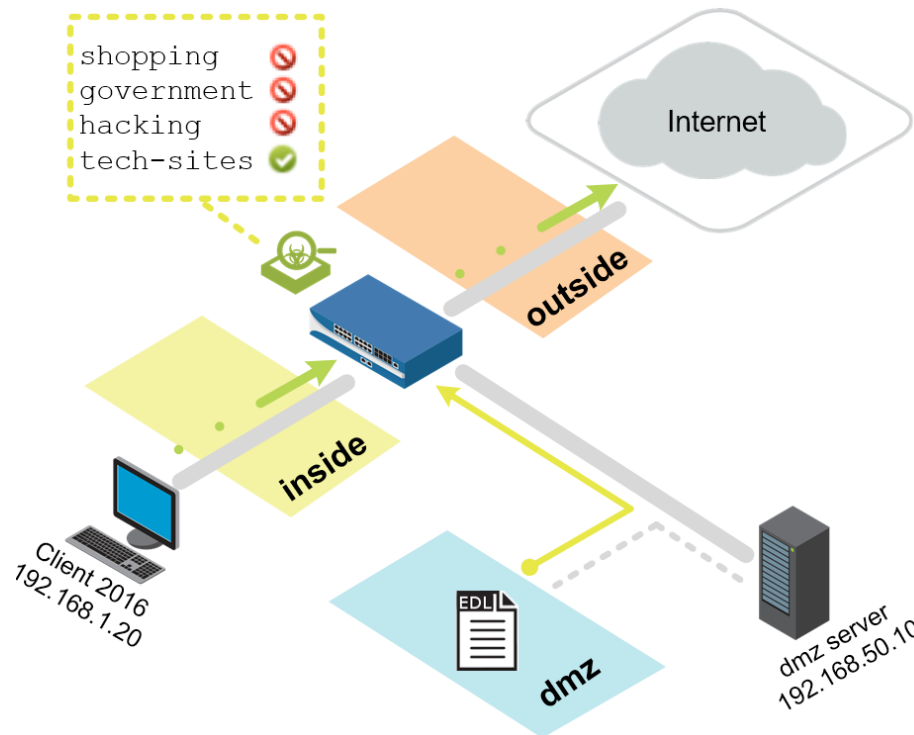


Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pal0Alt0
Centos AAC DMZ	root	Pal0Alt0
Centos Virtual Router	root	Pal0Alt0

### Powering Down Your VMware Workstation VM-50 firewall appliance:

If after powering off your VM-50 firewall appliance via VMware Workstation it remains powered on, please shut it down by accessing the CLI via SSH and entering the following command: "request shutdown system". You can access the firewall appliance via ssh from the Windows 2016 client virtual machine using PuTTY and 192.168.1.254 as the destination IP address or from your host computer using PuTTY and the Centos VR virtual machine's external interface's (ens160) IP address as the destination ssh address.

# Lab: URL Filtering



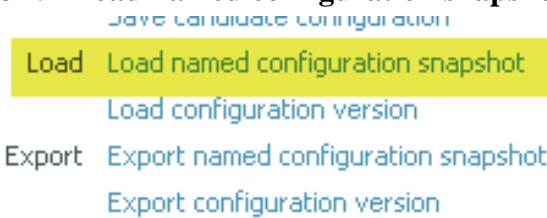
## Lab Objectives

- 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 (EDL) 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.

## 7.0 Load a Lab Configuration

To start this lab exercise, you will load a preconfigured firewall configuration file.

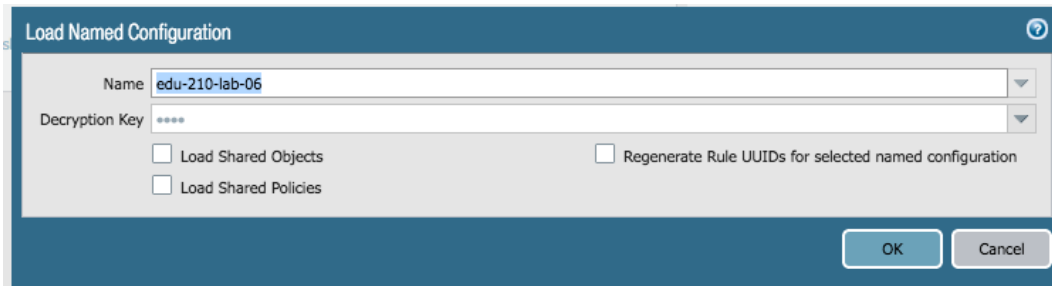
1. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



A Load Named Configuration dialog box appears.

- Click the drop-down list next to the **Name** text box and select **edu-210-lab-06**.

**Note:** Look for **edu-210** in the filename because the drop-down list might contain lab configuration files for other course numbers:



- Click **OK** to close the **Load Named Configuration** window.  
A window should appear that confirms that the configuration is being loaded.
- Click **Close** to close the **Loading Configuration** window.
- Click the **Commit** link at the upper right of the web interface:



A **Commit** window should appear.

- Click **Commit** and wait until the commit process is complete.  
A **Commit Status** window should appear that confirms the configuration was committed successfully.
- Click **Close** to continue.

## 1.1 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.

- In the web interface, select **Objects > Custom Objects > URL Category**.
- Click **Add** to create a **Custom URL Category**.

The **Custom URL Category** configuration window should appear.

- Configure the following:

Parameter	Value
Name	Type news-sites
Description	Type Blocked news sites
Sites	Click Add and type the following news sites:

Parameter	Value
	foxnews.com bbc.com msnbc.com *.foxnews.com *.bbc.com *.msnbc.com

Custom URL Category

Name: news-sites

Description: Blocked news sites

Type: URL List

Matches any of the following URLs, domains or host names

6 items

- foxnews.com
- bbc.com
- msnbc.com
- \*.foxnews.com
- \*.bbc.com
- \*.msnbc.com

- Click **OK** to close the **Custom URL Category** configuration window.

The new Custom URL Category should appear in the web interface.

- In the web interface, select **Policies > Security**.

- Select the **egress-outside-content-id** Security policy rule.

The **Security Policy Rule** configuration window should appear.

- Configure the following:

Parameter	Value
Name	Rename the policy to egress-outside-url
Audit Comment	Type Created URL Security policy on <date> by <Your-Role>

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

Name: egress-outside-url

Rule Type: universal (default)

Description:

Tags: egress

Group Rules By Tag: egress

Audit Comment: Created URL Security policy on <date> by admin

[Audit Comment Archive](#)

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

Parameter	Value
Applications	Verify that the <b>Any</b> check box is selected

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

☒ Any

☐ Applications ▲

[Add](#) [Delete](#)

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

Parameter	Value
URL Category	Click <b>Add</b> and select <b>news-sites</b> from the drop-down list

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

application-default

Service

Any

URL Category

new-sites

+ Add - Delete

+ Add - Delete

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

Parameter	Value
Action Setting	Select <b>Reset both client and server</b> from the drop-down list
Log Setting	Verify that <b>Log at Session end</b> is selected
Profile Type	Select <b>None</b> from the drop-down list

Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

Action Setting

Action: Reset both client and server

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

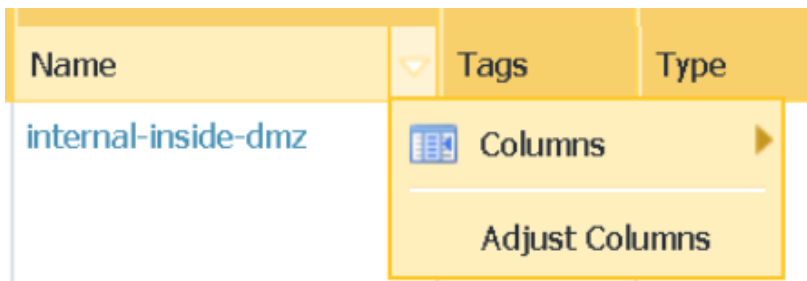
QoS Marking: None

☐ Disable Server Response Inspection

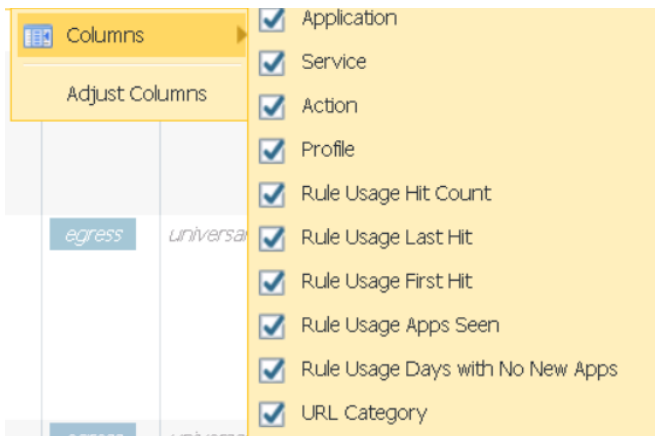
19. Click **OK** to close the **Security Policy Rule** configuration window.

The **egress-outside-url** rule should be listed as the first Security policy rule to ensure that the next sections of the lab work properly. If it is not listed as the first Security policy rule, then highlight it and move the rule to the top of the list.

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



21. Expand the **Columns** list using the right-arrow and verify that the **URL Category** check box is selected:



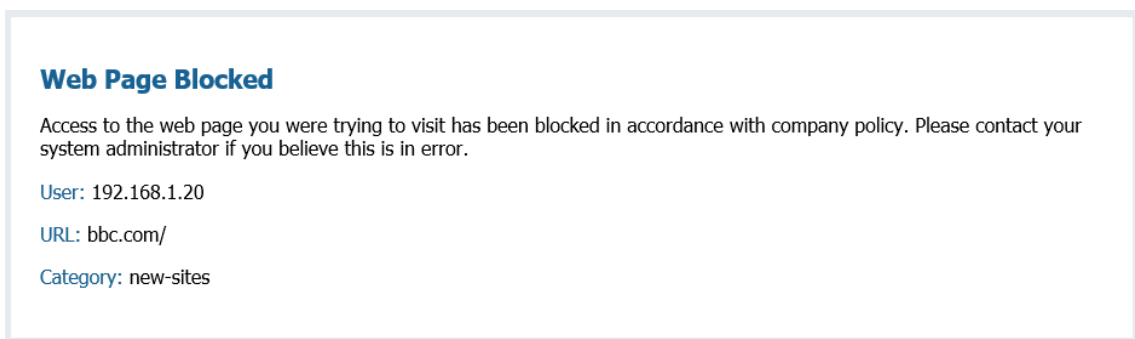
22. Select the **egress-outside** Security policy rule without opening it.  
23. Click **Enable**.

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

24. **Commit** all changes.

## 1.2 Test a Security Policy Rule

25. On your desktop, open a new browser window in private/incognito mode and browse to **bbc.com**:



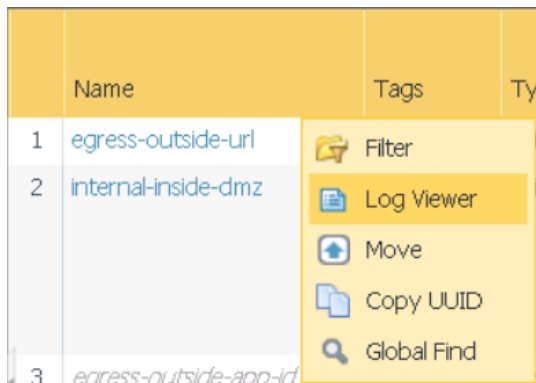
The URL is blocked by the Security policy rule named “egress-outside-url.”



26. In the same browser window, verify that **foxnews.com** is blocked.
27. In the same browser window, determine if **https://www.msnbc.com** also is blocked.  
Note that this is an SSL connection. Because the firewall is not decrypting traffic, the firewall resets the connection but does not generate a URL block page. If the firewall intercepted this connection and generated a URL block page, the browser (depending on the type) would assume and possibly report a man-in-the-middle attack.
28. Close the browser window.

## 1.3 Review the Logs

29. In the web interface, select **Policies > Security**.
30. Hover the pointer over the **egress-outside-url** Security policy rule, click the Down arrow, and select **Log Viewer** to open the Traffic log:



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

(rule eq 'egress-outside-url')												
	Receive Time	Type	From Zone	To Zone	Source	Destination	To P...	Application	Action	Rule	Session End Reason	
	02/21 03:21:20	deny	inside	outside	192.168.1.20	23.67.232...	443	ssl	reset-both	egress-outside-url	policy-deny	
	02/21 03:21:20	deny	inside	outside	192.168.1.20	23.67.232...	443	ssl	reset-both	egress-outside-url	policy-deny	
	02/21 03:21:20	deny	inside	outside	192.168.1.20	23.67.232...	443	ssl	reset-both	egress-outside-url	policy-deny	

31. Click the down-arrow on any column header to add the **URL Category** column to the Traffic log display:

Receive Time	URL Category	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason
12/18 00:04:43	news-sites	deny	inside	outside	192.168.1.20	23.49.15.167	80	web-browsing	reset-both	egress-outside-url	policy-deny
12/18 00:04:43	news-sites	deny	inside	outside	192.168.1.20	23.76.192.83	80	web-browsing	reset-both	egress-outside-url	policy-deny
12/18 00:04:43	news-sites	deny	inside	outside	192.168.1.20	151.101.0.81	80	web-browsing	reset-both	egress-outside-url	policy-deny

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

Notice that the URL Filtering log includes the **Category** and **URL** columns by default:

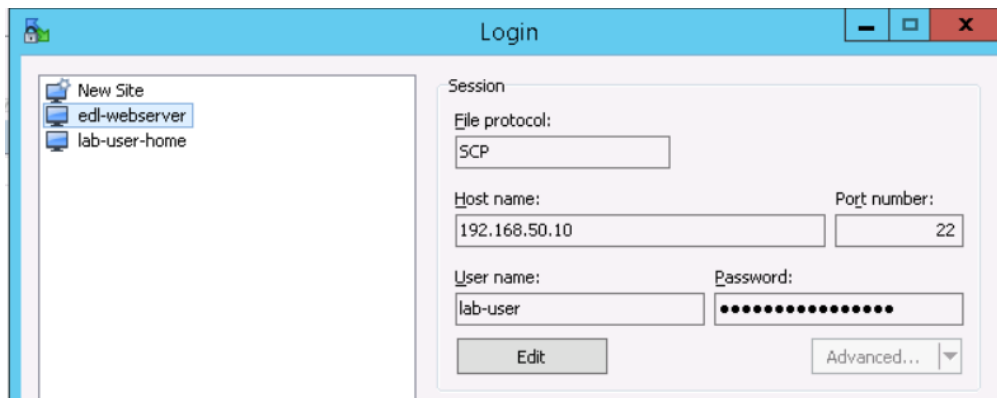
Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Destination	Application	Action
02/21 04:05:54	news-sites	news-sites,news,low-risk	msnbc.com/	inside	outside	192.168.1.20	23.49.15.167	web-browsing	block-url
02/21 04:05:46	news-sites	news-sites,news,low-risk	foxnews.com/	inside	outside	192.168.1.20	23.76.192.83	web-browsing	block-url
02/21 04:05:39	news-sites	news-sites,news,low-risk	bbc.com/	inside	outside	192.168.1.20	151.101.0.81	web-browsing	block-url

## 1.4 Configure an External Dynamic List

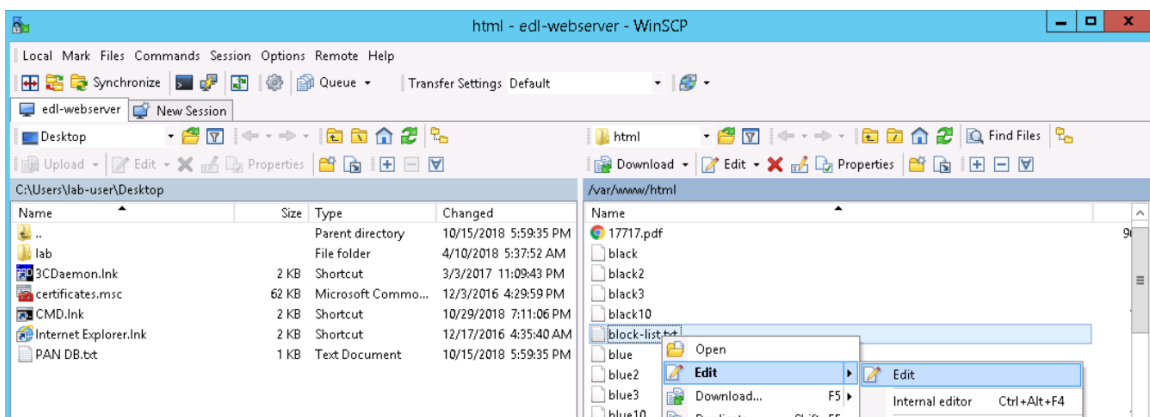
An EDL is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules.

33. On the Windows desktop, double-click the **WinSCP** icon.

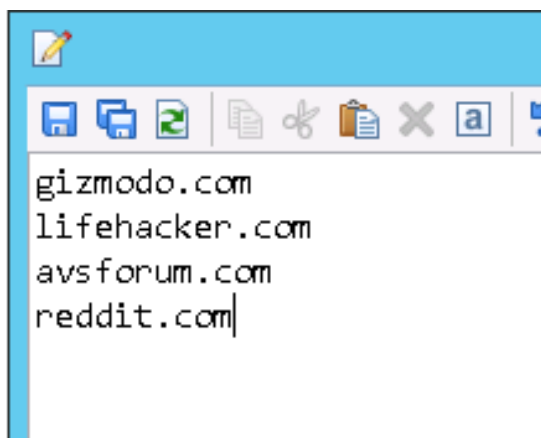
34. Double-click the list menu item **edl-webserver**:





35. Locate the text file named **block-list.txt** in the right window pane.  
36. Right-click the **block-list.txt** file and select **Edit**.



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



38. Click **Save**  to save any modifications to the file that you might have made.  
39. Click  to close the file.  
40. Close the **WinSCP** window.  
41. In the web interface, select **Objects > External Dynamic Lists**.

42. Click **Add** to configure a new EDL.

The **External Dynamic Lists** configuration window should appear.

43. Configure the following:

Parameter	Value
Name	Type url-block-list
Type	Select <b>URL List</b> from the drop-down list
Source	Type <b>http://192.168.50.10/block-list.txt</b>
Check for updates	Select <b>Five Minute</b> from the drop-down list

External Dynamic Lists

Name

Create List List Entries And Exceptions

Type

Description

Source

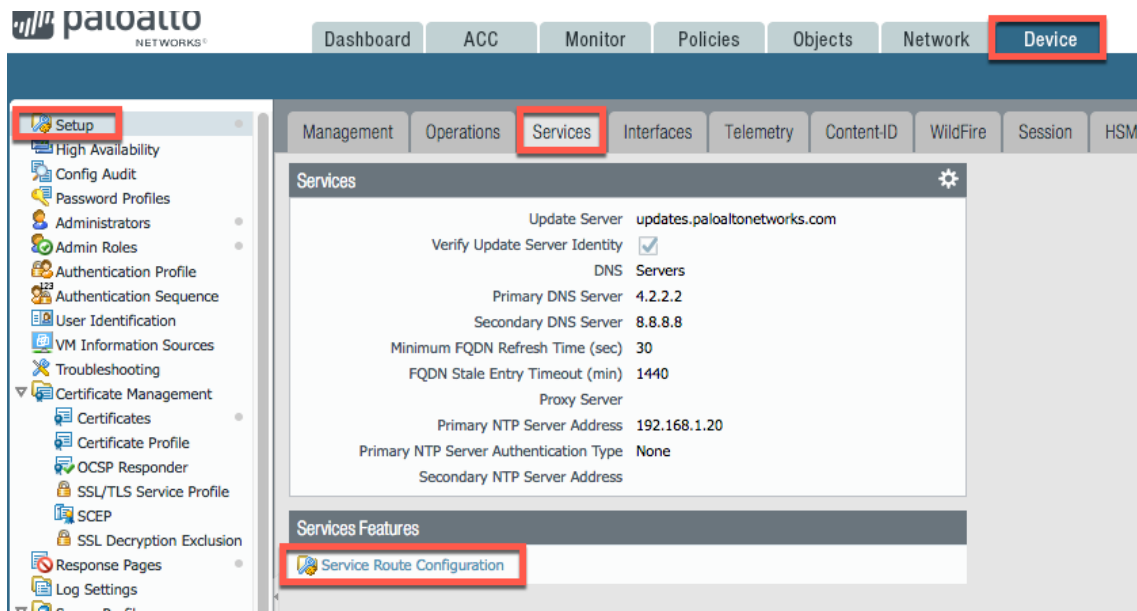
Server Authentication

Certificate Profile

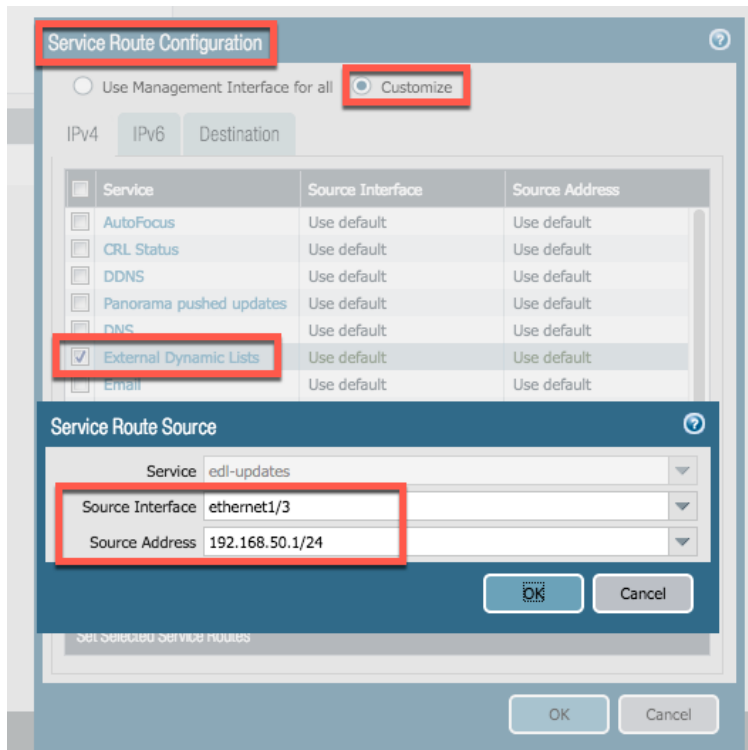
Check for updates

44. Click **OK** to close the **External Dynamic Lists** configuration window.

45. In the Web-UI, navigate to Device tab>Setup>Services tab and under Service Features click **Service Route Configuration**.



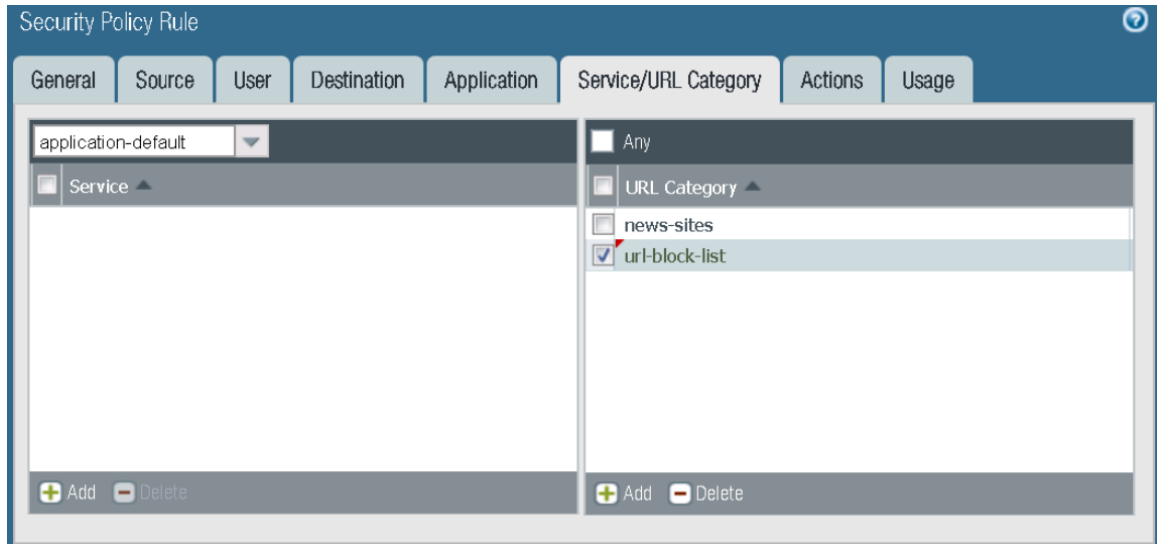
46. In the **Service Route Configuration** dialog box, select radial dial for **Customize**, select **External Dynamic Lists**. In the **Service Route Source** dialog box select **Source Interface** ethernet1/3 and **Source Address** 192.168.50.1/24.



47. Click “OK” twice to close all the windows.
48. In the web interface, select **Policies > Security**.
49. Click the **egress-outside-url** Security policy rule to configure the policy.
- The **Security Policy Rule** configuration window should appear.

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

Parameter	Value
URL Category	Click <b>Add</b> and select <b>url-block-list</b> from the drop-down list

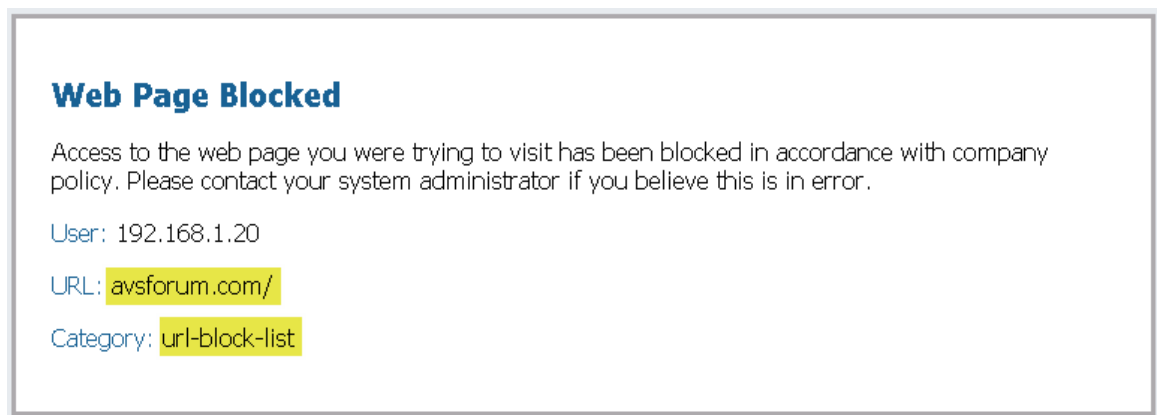


51. Click **OK** to close the **Security Policy Rule** configuration window.

52. **Commit** all changes.

## 1.5 Test a Security Policy Rule

53. On your desktop, open a new browser window in private/incognito mode and browse to **avsforum.com**:



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






54. In the same browser window, verify that **gizmodo.com** and **lifehacker.com** also are blocked.

55. Close the browser window.

## 1.6 Review the Logs

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

Notice that the **Category** column should display the name of the EDL you created and that the **Action** column shows that the URL is blocked:

	Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Destination	Application	Action
	02/21 03:57:24	url-block-list	url-block-list,computer-and-internet-info,low-risk	lifehacker.com/	inside	outside	192.168.1.20	151.101.130...	web-browsing	block-url
	02/21 03:57:22	url-block-list	url-block-list	lifehacker.com/	inside	outside	192.168.1.20	151.101.130...	web-browsing	block-url
	02/21 03:57:14	url-block-list	url-block-list,computer-and-internet-info,low-risk	gizmodo.com/	inside	outside	192.168.1.20	151.101.2.166	web-browsing	block-url
	02/21 03:57:14	url-block-list	url-block-list	gizmodo.com/	inside	outside	192.168.1.20	151.101.2.166	web-browsing	block-url
	02/21 03:57:00	url-block-list	url-block-list,personal-sites-and-blogs,low-risk	avsforum.com/	inside	outside	192.168.1.20	35.227.203.50	web-browsing	block-url
	02/21 03:57:00	url-block-list	url-block-list	avsforum.com/	inside	outside	192.168.1.20	35.227.203.50	web-browsing	block-url

## 1.7 Create a Security Policy Rule with a URL Filtering Profile

57. In the web interface, select **Objects > Security Profiles > URL Filtering**.

58. Click **Add** to define a **URL Filtering Profile**.

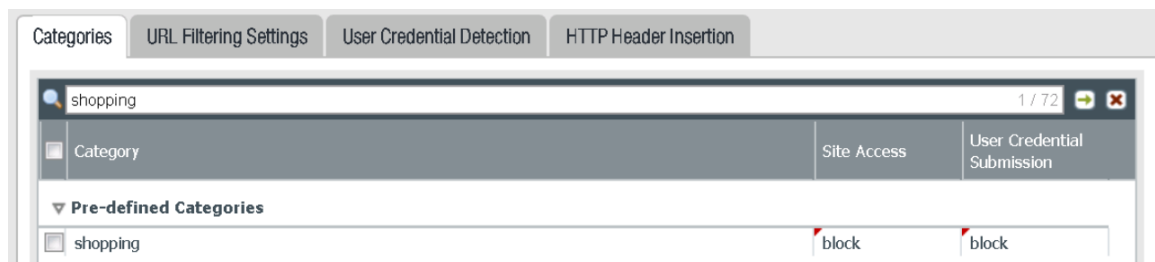
The **URL Filtering Profile** configuration window should appear.

59. Configure the following:

Parameter	Value
<b>Name</b>	<b>Type lab-url-filtering</b>
<b>Description</b>	<b>Type Block shopping, government, and hacking websites</b>

60. Click the **Categories** tab.

61. Search the **Category** field for the following three categories and set the **Site Access** to **block**:



**shopping**

**government**

**hacking**

62. Search for **url-block-list** and **news-sites**.

Notice that your custom URL categories also are listed, and they are set to a **Site Access** of “allow.” Leave them set to “allow.”

63. Click **OK** to close the **URL Filtering Profile** window.

64. In the web interface, select **Policies > Security**.

65. Click **egress-outside-url** to configure the policy.

The **Security Policy Rule** configuration window should appear.

66. Click the **Service/URL Category** tab.

67. Select the **Any** check box above the **URL Category** list.

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

Parameter	Value
Action	Select <b>Allow</b> from the drop-down list
Profile Type	Select <b>Profiles</b> from the drop-down list
URL Filtering	Select <b>lab-url-filtering</b> from the drop-down list

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The window has several tabs: General, Source, User, Destination, Application, Service/URL Category, Actions, and Usage. The 'Actions' tab is active, displaying four main sections: Action Setting, Profile Setting, Log Setting, and Other Settings. In the Action Setting section, the 'Action' dropdown is set to 'Allow' and the 'Send ICMP Unreachable' checkbox is unchecked. In the Profile Setting section, the 'Profile Type' dropdown is set to 'Profiles', and 'Antivirus', 'Vulnerability Protection', and 'Anti-Spyware' are all set to 'None'. The 'URL Filtering' dropdown is set to 'lab-url-filtering'. In the Log Setting section, 'Log at Session Start' is unchecked, 'Log at Session End' is checked, and 'Log Forwarding' is set to 'None'. In the Other Settings section, 'Schedule' and 'QoS Marking' are both set to 'None', and the 'Disable Server Response Inspection' checkbox is unchecked.

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

70. **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.

71. **Commit** all changes.

## 1.8 Test a Security Policy Rule with a URL Filtering Profile

72. Open a different browser (not a new tab) in private/incognito mode and browse to **www.newegg.com**.






The URL [www.newegg.com](http://www.newegg.com) belongs to the shopping URL category. Based on the Security policy rule named “egress-outside-url,” the URL now is 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.

73. In the same browser window, verify that **<http://www.transportation.gov>** (government) and **<http://www.2600.org>** (hacking) are blocked.
74. Close all browser windows except for the firewall web interface.

## 1.9 Review the Logs

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

Review the actions taken on the following log entries:

	Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Destination	Application	Action
	02/21 04:14:18	hacking	hacking,low-risk	<a href="http://www.2600.org/">www.2600.org/</a>	inside	outside	192.168.1.20	184.105.226...	web-browsing	block-url
	02/21 04:14:14	hacking	hacking,low-risk	<a href="http://www.2600.com/">www.2600.com/</a>	inside	outside	192.168.1.20	184.105.226...	web-browsing	block-url
	02/21 04:14:04	governme...	government,low-risk	<a href="http://transportation.gov/">transportation.gov/</a>	inside	outside	192.168.1.20	204.68.196.12	web-browsing	block-url



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