



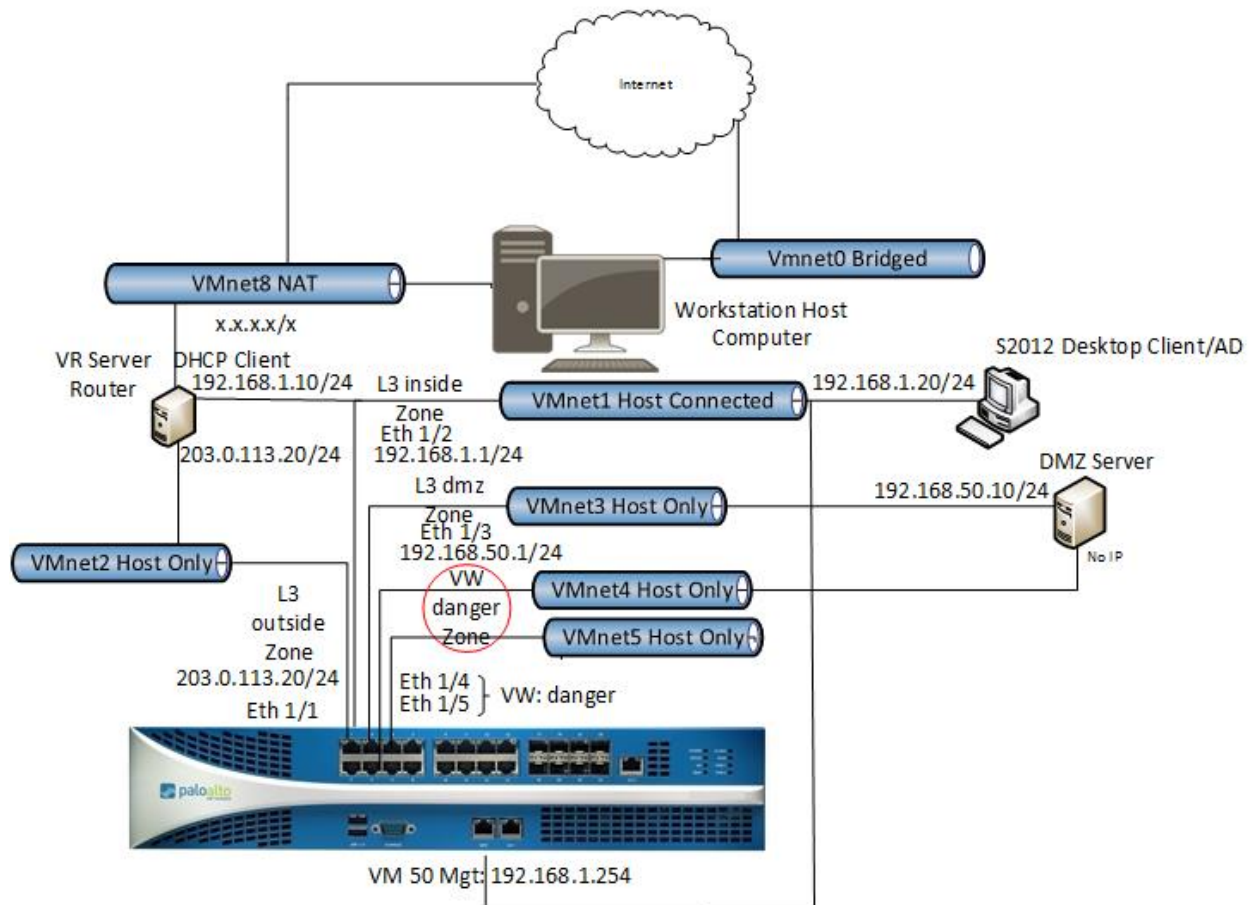
# **Palo Alto Networks Academy Labs Lab 6 URL Filtering**

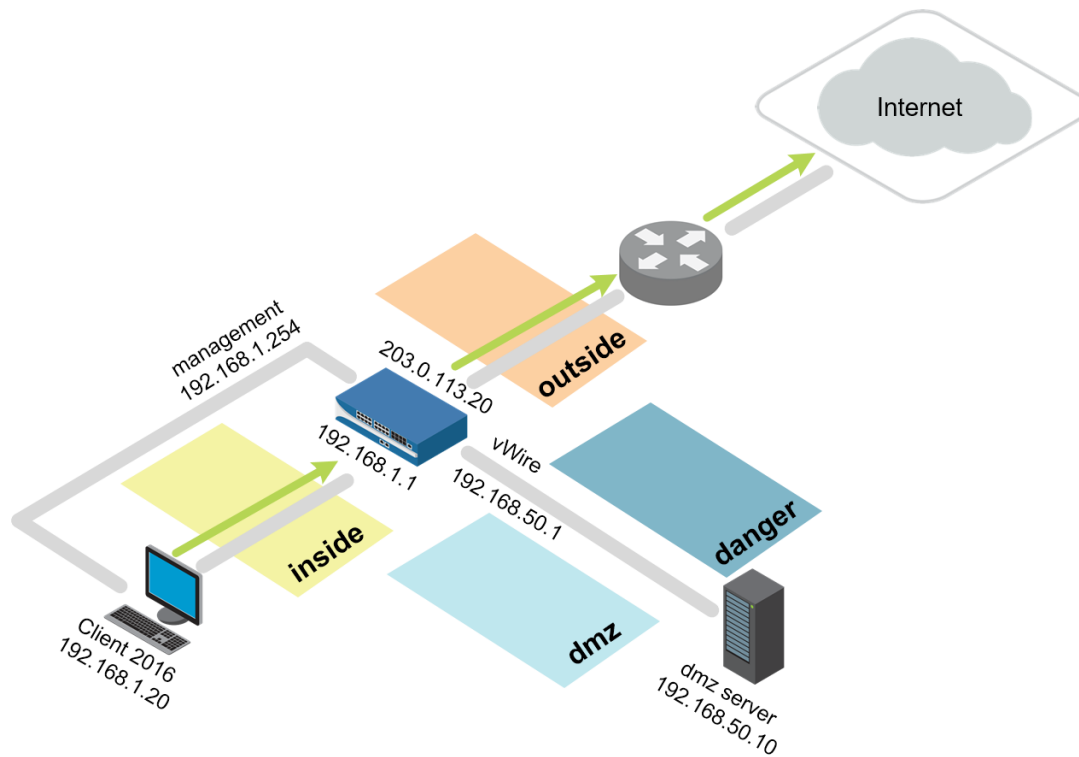
**Document Version: 2018-11-10**

Copyright © 2018 Palo Alto Networks, Inc.

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

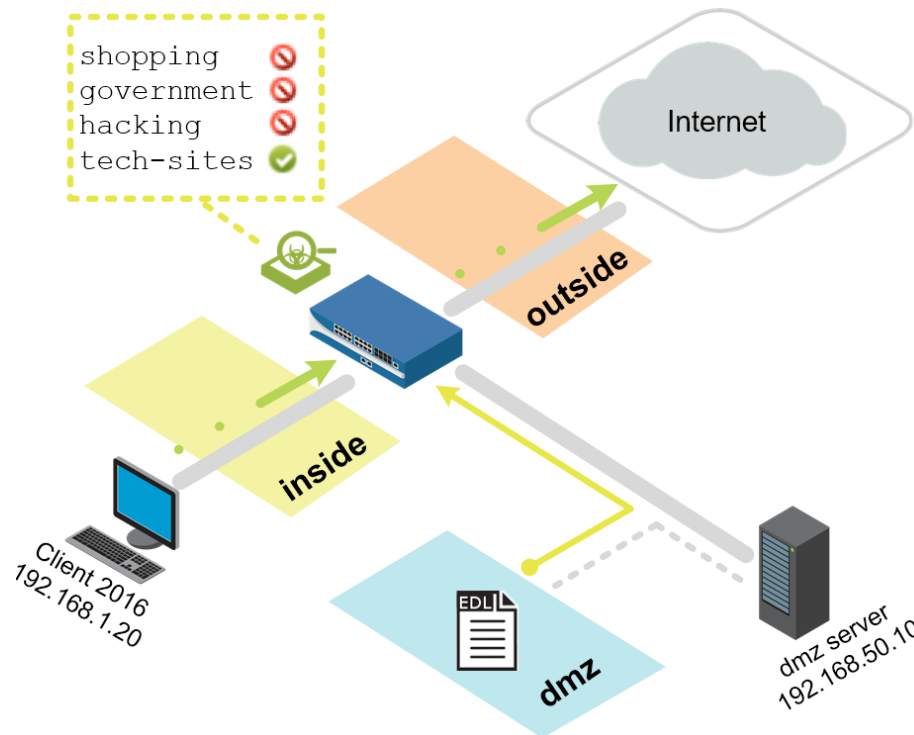
# Lab Topology





Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pa10Alt0
Centos AAC DMZ	root	Pa10Alt0
Centos Virtual Router	root	Pa10Alt0

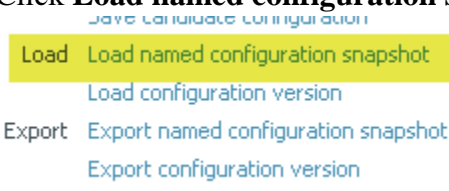

## Lab 6: URL Filtering



### 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.


### 6.0 Load Lab Configuration

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

  - Save candidate configuration
  - Load** Load named configuration snapshot
  - Load configuration version
  - Export Export named configuration snapshot
  - Export configuration version
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.


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

7. Click  to create a custom URL Category.

8. Configure the following:

Parameter	Value
Name	news-sites
Sites	foxnews.com bbc.com msnbc.com *.foxnews.com *.bbc.com *.msnbc.com

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

10. Select **Policies > Security**. 

11. Select the **egress-outside-content-id** Security policy rule without opening it:

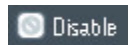


12. Click . The **Clone** configuration window opens.

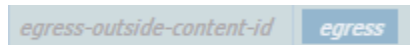
13. Verify that **Move top** is selected from the **Rule** order drop-down list.

14. Click **OK** to close the **Clone** configuration window.

15. With the original egress-outside-content-id Security policy rule still selected, click



16. Notice that the egress-outside-content-id is now grayed out and in italics:



17. Click to open the cloned Security policy rule named **egress-outside-content-id-1**.

18. Configure the following:

Parameter	Value
Name	egress-outside-url

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

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

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

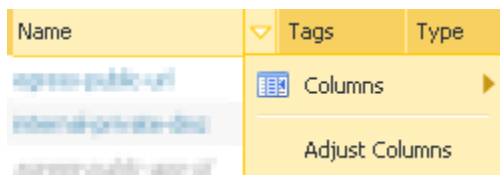
Parameter	Value
URL Category	<input checked="" type="checkbox"/> news-sites

21. 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	<b>Profile Setting</b> Profile Type <span>None</span>

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

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



24. Expand the **Columns** menu using the right-arrow and verify that the **URL Category** check box is selected.

25. Enable the rule **egress-outside**.

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

26.  **Commit** all changes.

## 6.2 Test Security Policy Rule

27. Open a browser in private/incognito mode and browse to **bbc.com**:

### Web Page Blocked

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

User: 192.168.1.20

URL: www.bbc.com/

Category: news-sites

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

28. In the same browser window verify that **foxnews.com** is blocked.
29. 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.

## 6.3 Review Logs

30. In the web interface select **Polices > Security** and hover over the **egress-outside-url** Security policy rule, click the down-arrow, and select **Log Viewer** to open the Traffic log:



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

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	08/27 18:00:49	deny	inside	outside	192.168.1.20		23.207.17.30	443	ssl	reset-both	egress-outside-url	policy-deny	440
	08/27 18:00:44	deny	inside	outside	192.168.1.20		23.207.17.30	443	ssl	reset-both	egress-outside-url	policy-deny	440
	08/27 18:00:43	deny	inside	outside	192.168.1.20		23.207.17.30	443	ssl	reset-both	egress-outside-url	policy-deny	440
	08/27 17:59:58	deny	inside	outside	192.168.1.20		23.45.196.175	80	web-browsing	reset-both	egress-outside-url	threat	687
	08/27 17:59:58	deny	inside	outside	192.168.1.20		23.45.196.175	80	web-browsing	reset-both	egress-outside-url	threat	743
	08/27 17:59:57	deny	inside	outside	192.168.1.20		23.45.196.175	80	web-browsing	reset-both	egress-outside-url	policy-deny	567

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

33. Select the **URL Filtering** log. 

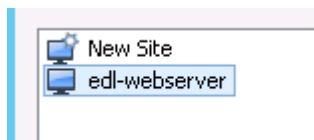
34. Notice that the URL Filtering log includes the **Category** and **URL** columns by default:

	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
	08/27 18:00:49	news-sites	www.msnbc.com/	inside	outside	192.168.1.20		23.207.17.30	ssl	block-url
	08/27 18:00:44	news-sites	www.msnbc.com/	inside	outside	192.168.1.20		23.207.17.30	ssl	block-url
	08/27 18:00:43	news-sites	www.msnbc.com/	inside	outside	192.168.1.20		23.207.17.30	ssl	block-url
	08/27 17:59:58	news-sites	www.foxnews.com...	inside	outside	192.168.1.20		23.45.196.175	web-browsing	block-url
	08/27 17:59:58	news-sites	www.foxnews.com/	inside	outside	192.168.1.20		23.45.196.175	web-browsing	block-url
	08/27 17:59:57	news-sites	www.foxnews.com...	inside	outside	192.168.1.20		23.45.196.175	web-browsing	block-url
	08/27 17:59:57	news-sites	www.foxnews.com/	inside	outside	192.168.1.20		23.45.196.175	web-browsing	block-url
	08/27 17:53:52	news-sites	www.bbc.com/favi...	inside	outside	192.168.1.20		151.101.48.81	web-browsing	block-url
	08/27 17:53:52	news-sites	www.bbc.com/	inside	outside	192.168.1.20		151.101.48.81	web-browsing	block-url

## 6.4 Configure an External Dynamic List

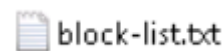
An External Dynamic List is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules.

35. Open WinSCP on the Windows desktop.



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

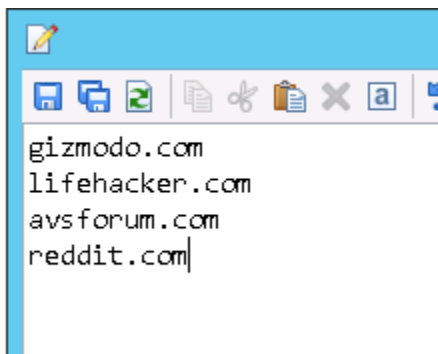
37. Locate the text file in the right window pane named **block-list.txt**.



38. Right-click the **block-list.txt** file and select **Edit**.

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

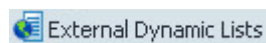
```
gizmodo.com
lifehacker.com
avsforum.com
reddit.com
```



40. **Save** the file if you made modifications, and **Close** the file.

41. Close the **WinSCP** window.

42. In the web interface select **Objects > External Dynamic Lists**.




43. Click **Add** to configure a new External Dynamic List.

44. Configure the following:



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

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

46. Go to **Policies > Security**.  Security

47. Click to open the Security policy rule named **egress-outside-url**.

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

49. Add the newly created External Dynamic List to the **URL Category** list:

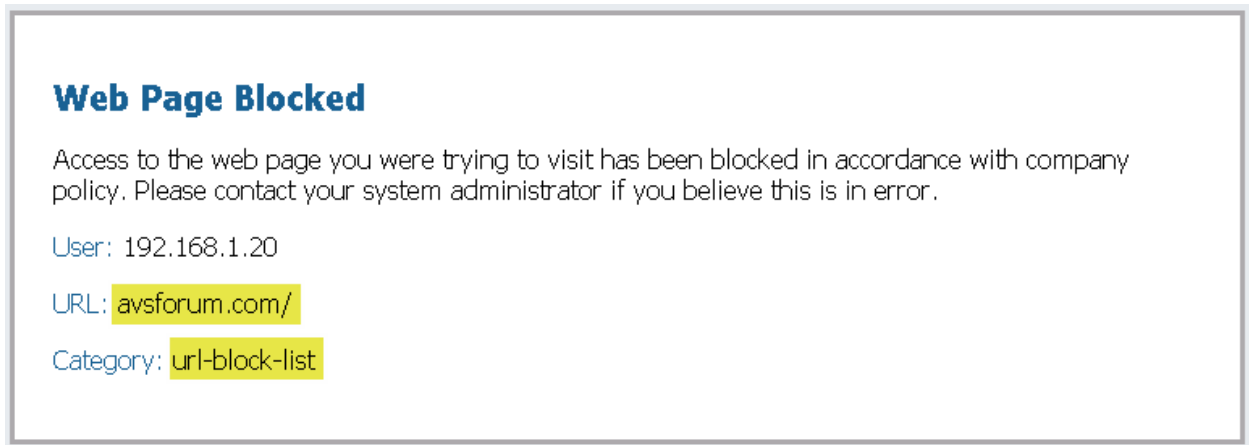


50. Click **OK** to close the **Security Policy Rule** configuration window.

51.  **Commit** all changes.

## 6.5 Test Security Policy Rule


52. 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**.

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

## 6.6 Review Logs

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

55. Notice the new category and action:

	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...	untrust	trust	192.168.1.20		173.192.76.217	web-browsing	block-ur
	12/02 12:59:42	url-block-list	avsforum.com/f...	untrust	trust	192.168.1.20		173.192.76.217	web-browsing	block-ur
	12/02 12:59:42	url-block-list	avsforum.com/f...	untrust	trust	192.168.1.20		173.192.76.217	web-browsing	block-ur

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

56. Select **Objects > Security Profiles > URL Filtering**.

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

58. Configure the following:

Parameter	Value
Name	lab-url-filtering

59. Click the **Categories** tab.

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



shopping

government

hacking

61. Search for url-block-list and tech-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.”

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

63. Select **Device > Licenses**.

64. Under the **PAN-DB URL Filtering** header, click **Download Now** (or **Re-Download**).  
Click **Yes** if a warning appears.

65. Select the region nearest the location of your firewall and click **OK**.  
After the download completes, a **Download Successful** window appears.

66. Click **Close** to close the download status window. The web interface now should show a message similar to the following:

Download Status 2016-11-10 11:30:40 PAN-DB download: Finished successfully. [Re-Download](#)

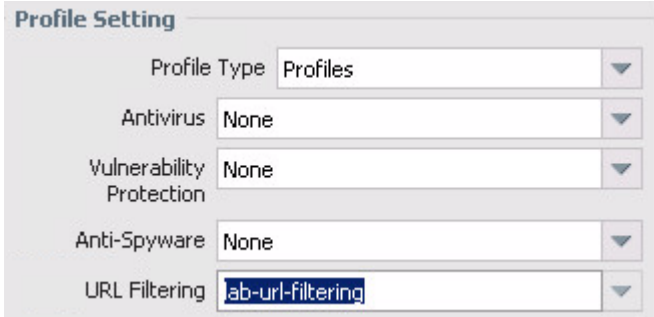
67. Select **Policies > Security**.

68. Click to open the Security policy rule named **egress-outside-url**.




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

70. Select **Any** above the **URL Category** list.

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

Parameter	Value
Action	Allow
Profile Setting	

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

73.  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.

74.  all changes.

## 6.8 Test Security Policy Rule with URL Filtering Profile

75. 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.







76. In the same browser window verify that **http://www.transportation.gov** (government) and **http://www.2600.org** (hacking) are blocked.

77. Close all browser windows except for the firewall web interface.

## 6.9 Review Logs

78. Select **Monitor > Logs > URL Filtering**. 

79. Review the actions taken on the following entries:

	02/07 21:41:11	hacking	www.2600.org/favicon.ico	inside	outside	192.168.1.20		184.105.226.26	web-browsing	block-url
	02/07 21:41:11	hacking	www.2600.org/	inside	outside	192.168.1.20		184.105.226.26	web-browsing	block-url
	02/07 21:40:58	government	www.transportation.gov...	inside	outside	192.168.1.20		23.204.8.230	web-browsing	block-url
	02/07 21:40:58	government	www.transportation.gov/	inside	outside	192.168.1.20		23.204.8.230	web-browsing	block-url
	02/07 21:40:37	shopping	play.google.com/	inside	outside	192.168.1.20		172.217.9.14	google-play	block-url
	02/07 21:40:03	shopping	newegg.needle.com/	inside	outside	192.168.1.20		107.20.202.113	ssl	block-url

You should see entries for 2600.org and newegg.needle.com.



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