



## **PALO ALTO NETWORKS EDU-210**



### **Lab 6: URL Filtering**

**Document Version: 2019-11-12**

Copyright © 2019 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

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

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
1 Content-ID.....	5
1.0 Load Lab Configuration .....	6
1.1 Create a Security Policy Rule with a Custom URL Category .....	8
1.2 Test Security Policy Rule.....	14
1.3 Review the Logs.....	15
1.4 Configure an External Dynamic List .....	17
1.5 Test the Security Policy Rule .....	21
1.6 Review the Logs.....	22
1.7 Create a Security Policy Rule with a URL Filtering Profile .....	23
1.8 Test Security Policy Rule with a URL Filtering Profile .....	28
1.9 Review Logs .....	29

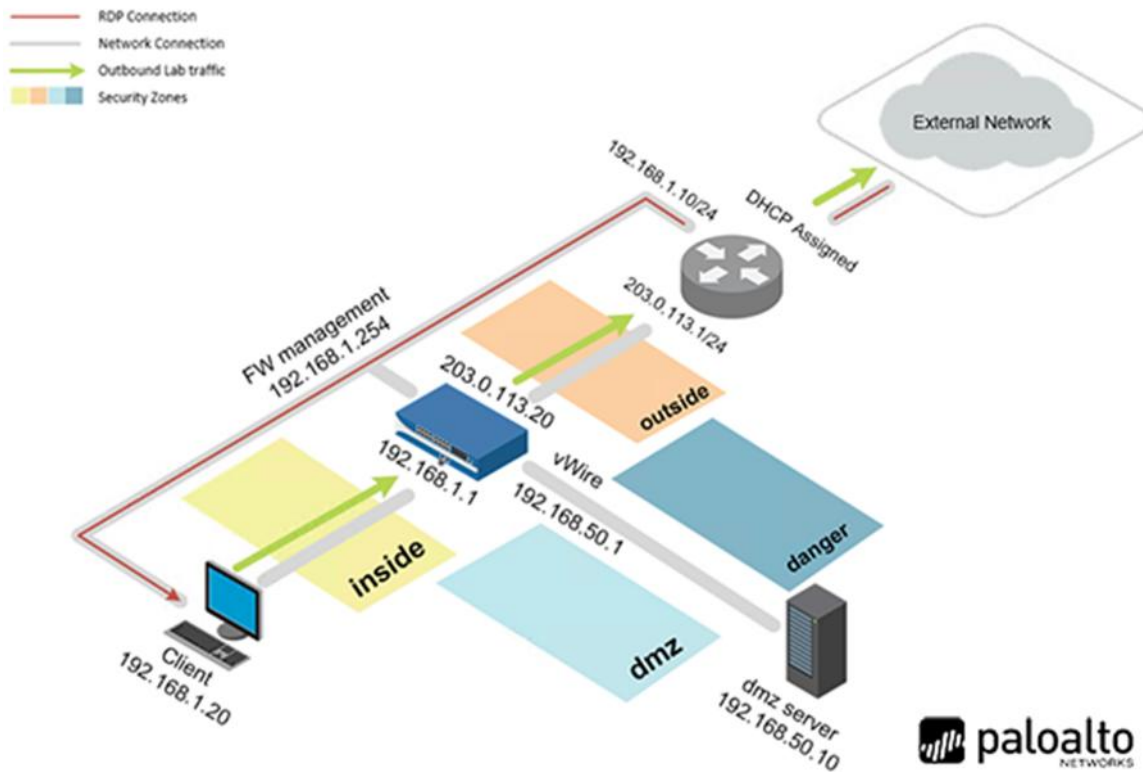
## Introduction

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.

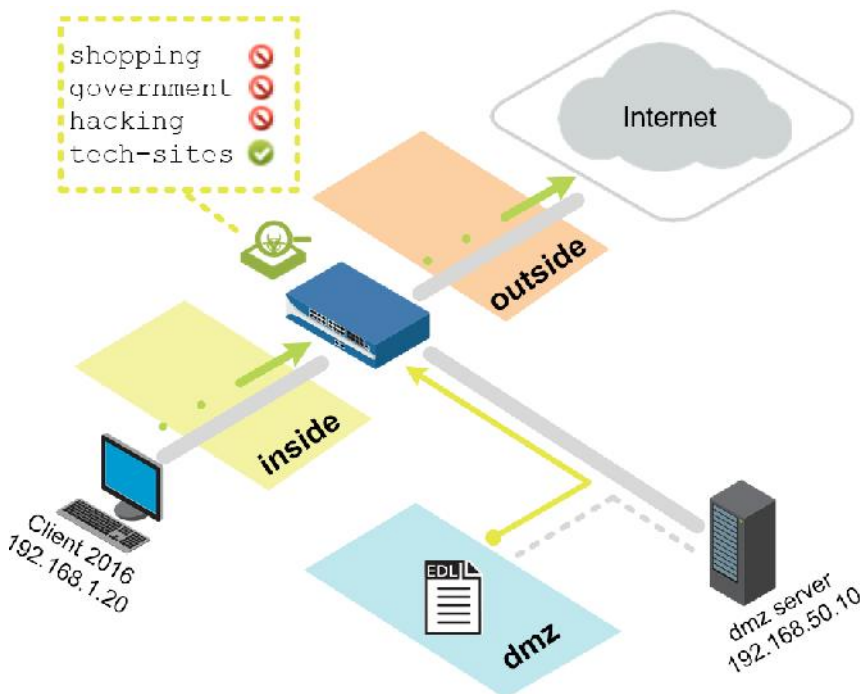
## Objectives

- ) 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



## Theoretical 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	Pa10A1t0
Firewall	192.168.1.254	admin	admin

## 1 Content-ID

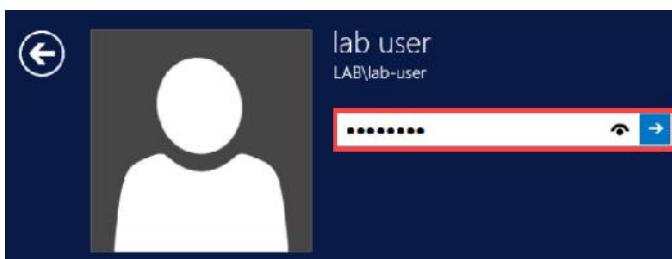
### 1.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Click within the splash screen to bring up the login screen. Log in as **lab-user** using the password **Pa10A1t0**.



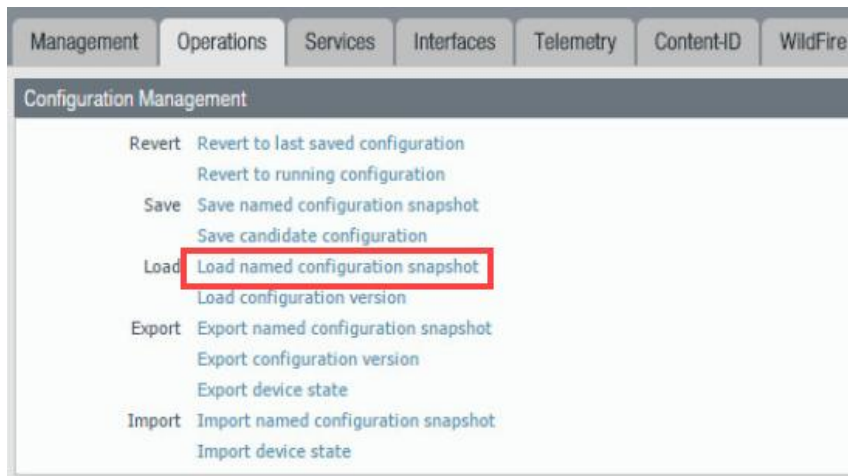
3. Launch the **Chrome** browser and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

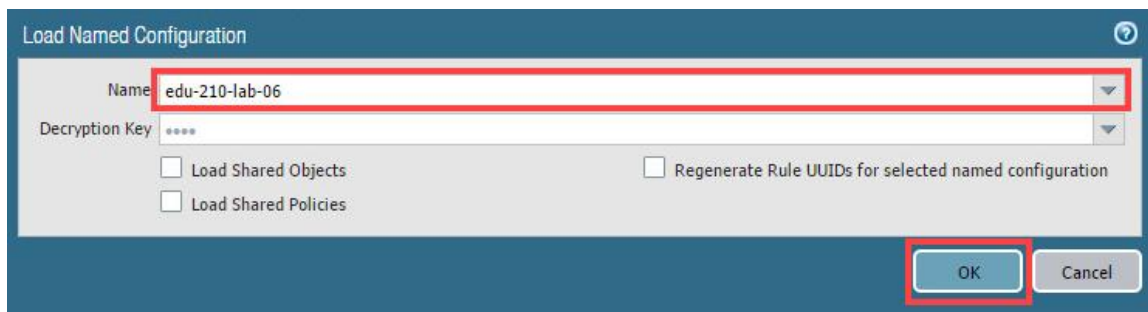
6. In the web interface, navigate to **Device > Setup > Operations**.



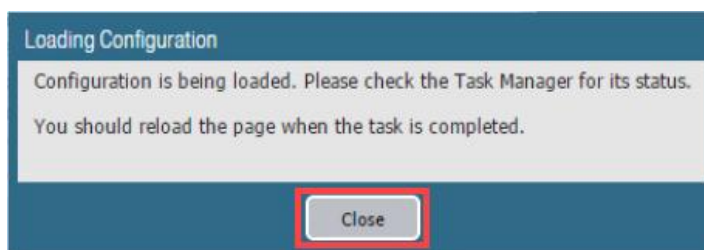
7. Click **Load named configuration snapshot**:



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



9. Click **Close**.

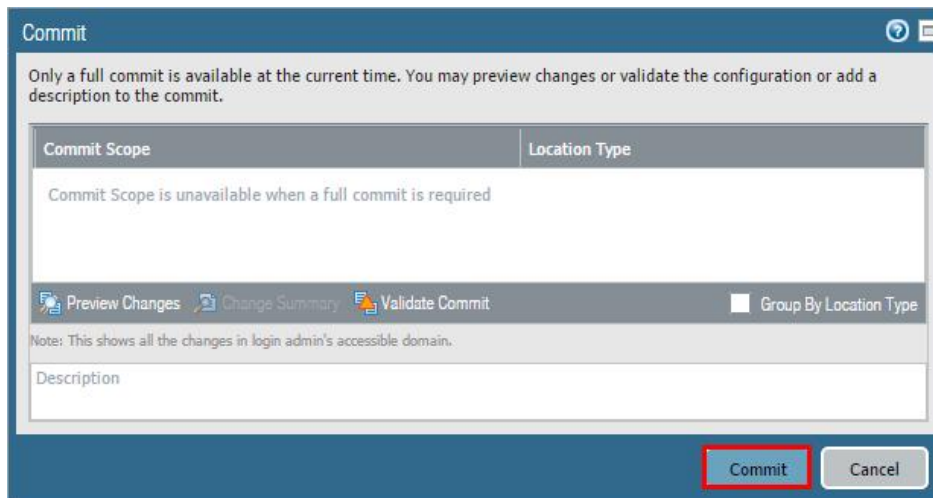


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

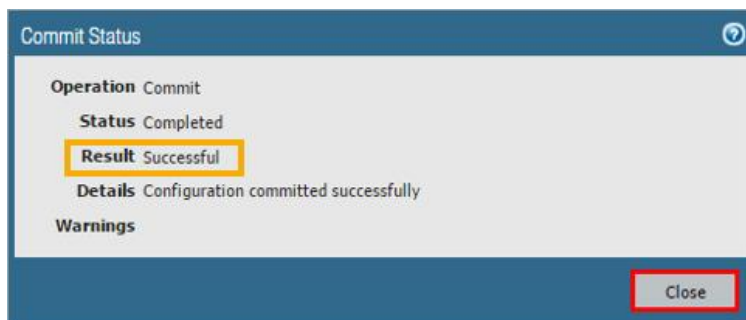
10. Click the **Commit** link at the top-right of the web interface.



11. Click **Commit** and wait until the commit process is complete.



12. Once completed successfully, click **Close** to continue.



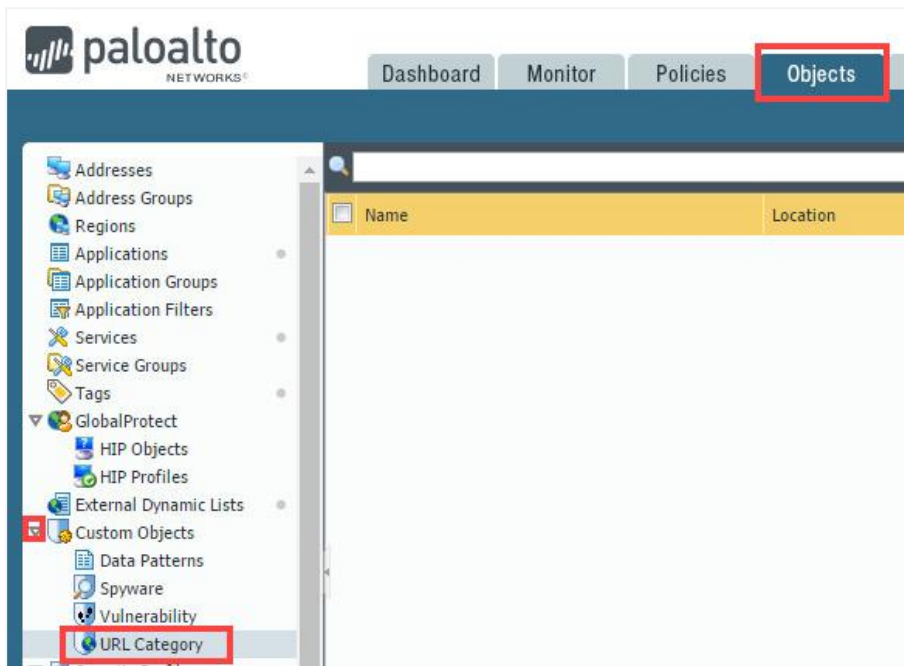
13. Leave the firewall web interface open to continue with the next task.

## 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.



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



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



3. In the *Custom URL Category* window, configure the following and click **OK**.

Parameter	Value
Name	Type <code>news-sites</code>
Description	Type <code>Blocked news sites</code>
Sites	<p>Click <b>Add</b> and type the following news sites:</p> <p><code>foxnews.com</code></p> <p><code>bbc.com</code></p> <p><code>msnbc.com</code></p> <p><code>*.foxnews.com</code></p> <p><code>*.bbc.com</code></p> <p><code>*.msnbc.com</code></p>

## Lab 6: URL Filtering

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

Sites

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

- In the web interface, navigate to **Policies > Security**.

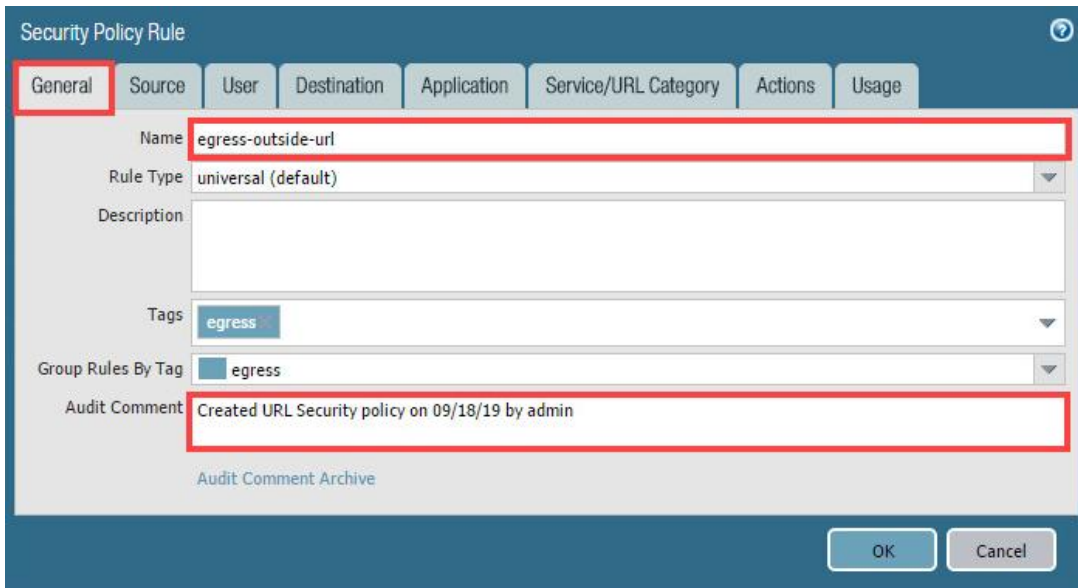


- Click on the **egress-outside-content-id** security policy rule.

	Name	Tags	Type	Zo
1	internal-inside-dmz	internal	universal	po
2	<b>egress-outside-content-id</b>	egress	universal	po
3	egress-outside	egress	universal	po
4	danger-simulated-traffic	none	universal	po
5	intrazone-default	none	intrazone	po

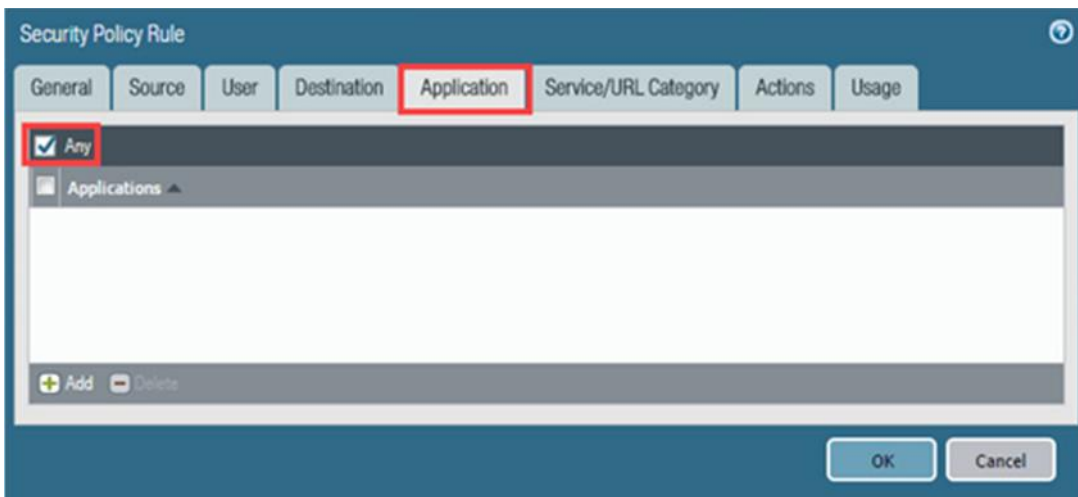
6. In the *Security Policy Rule* window, configure the following under the *General* tab:

Parameter	Value
Name	Rename the policy to <b>egress-outside-url</b>
Audit Comment	Type <b>Created URL Security policy on &lt;date&gt; by admin</b>



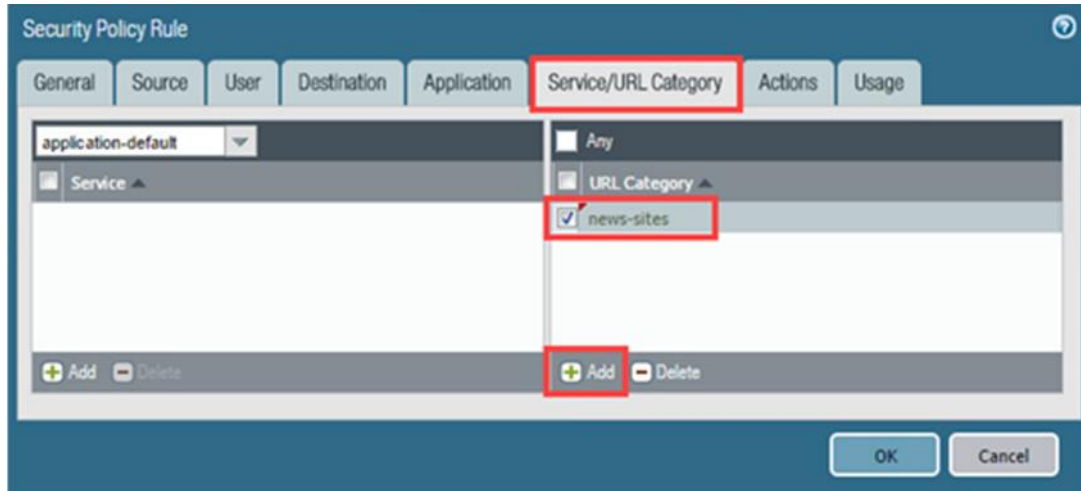
7. Click the **Application** tab and configure the following:

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



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

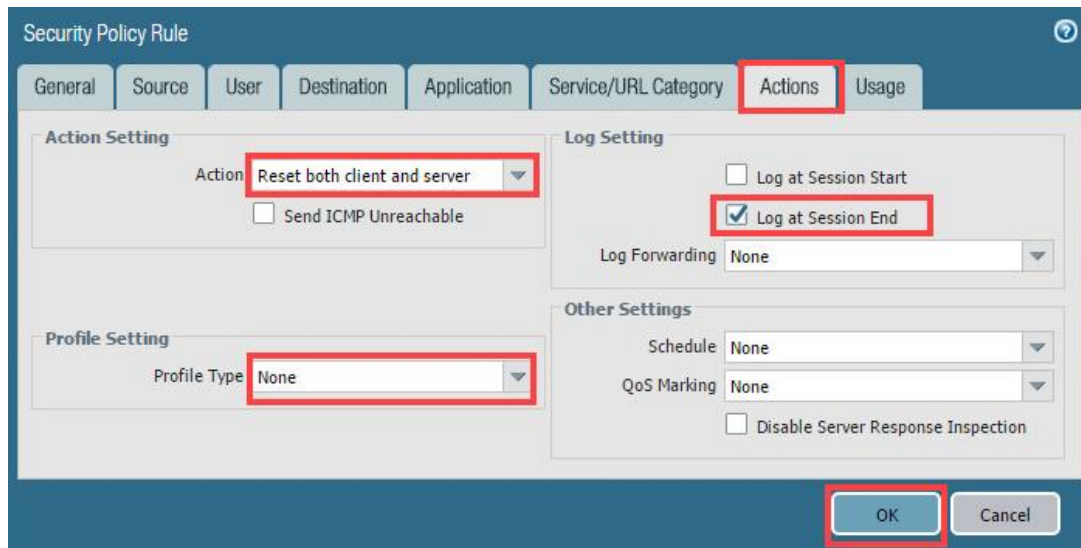
Parameter	Value
URL Category	Click <b>Add</b> and select <b>news-sites</b> from the drop-down list



The screenshot shows the 'Security Policy Rule' configuration window with the 'Service/URL Category' tab selected. The 'URL Category' dropdown is set to 'news-sites'. The 'Add' button is highlighted with a red box.

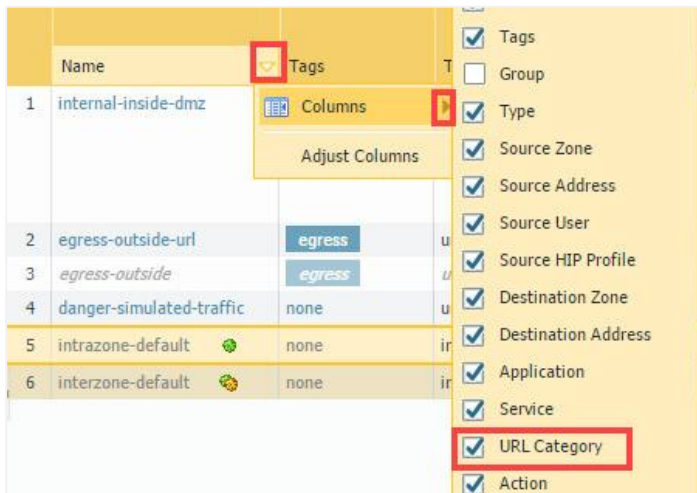
9. Click the **Actions** tab and configure the following; once finished, click **OK**.

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

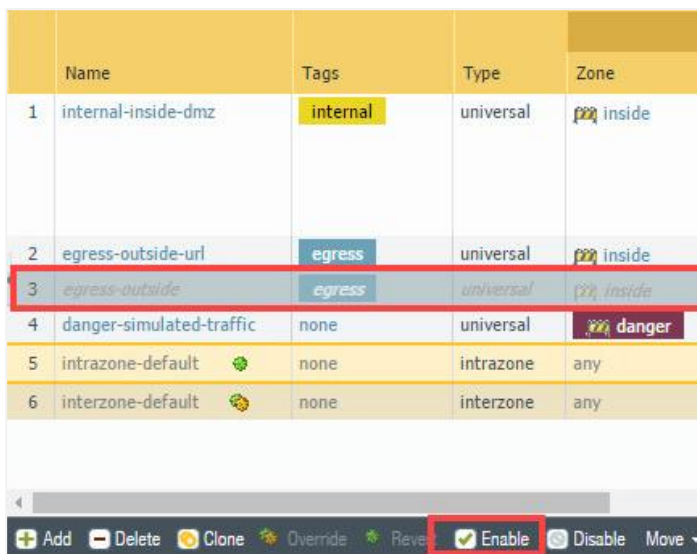


The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action' is set to 'Reset both client and server', 'Log at Session End' is checked, and 'Profile Type' is set to 'None'. The 'OK' button is highlighted with a red box.

10. Hover over the **Name** column and click the **down-arrow**. Expand the **Columns** menu using the right-arrow and select the **URL Category** checkbox. The URL Category column is displayed.



11. Select the **egress-outside** security policy rule without opening it and click **Enable**.

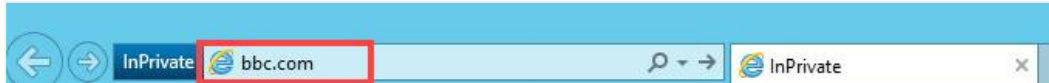


Because you created a rule that resets traffic, you need to enable the egress-outside rule to allow everything else.

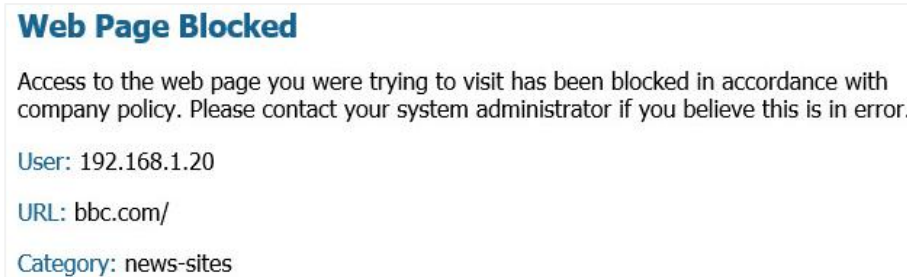
12. **Commit** all changes.

## 1.2 Test Security Policy Rule

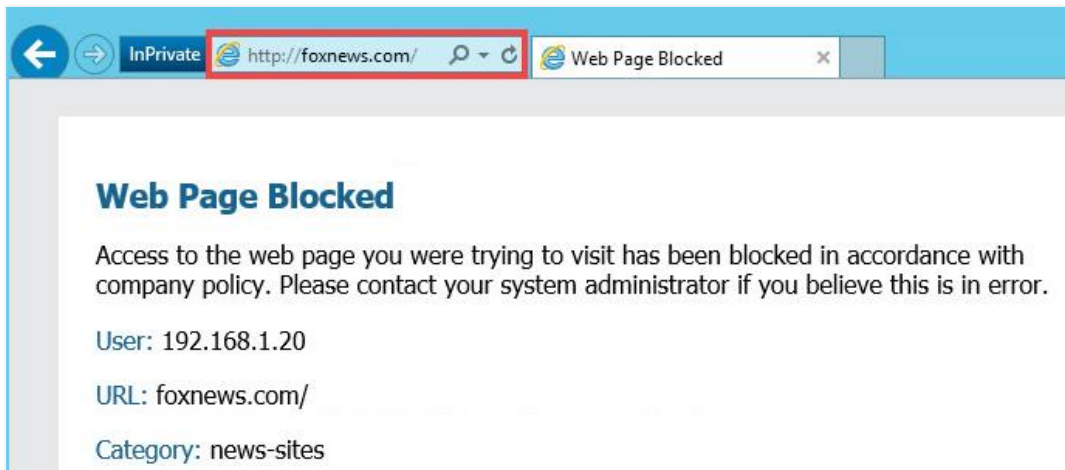
1. Open the **Internet Explorer** browser in **private/incognito mode** and browse to **bbc.com**.



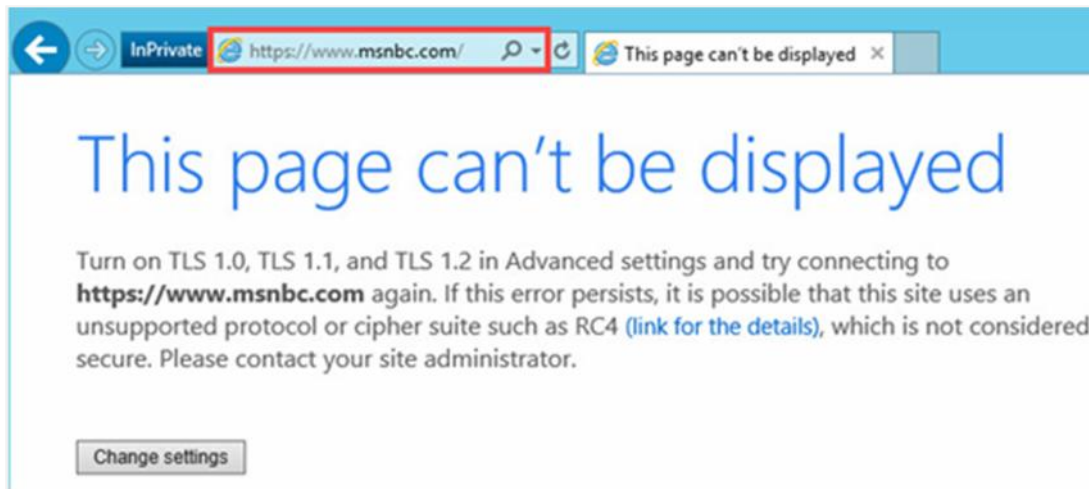
2. Notice that the URL is blocked by the Security Policy Rule.



3. In the same browser window, verify that **foxnews.com** is blocked.



4. In the same browser window, determine if `https://www.msnbc.com` also is blocked.



Notice 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.

5. Close the IE browser window.

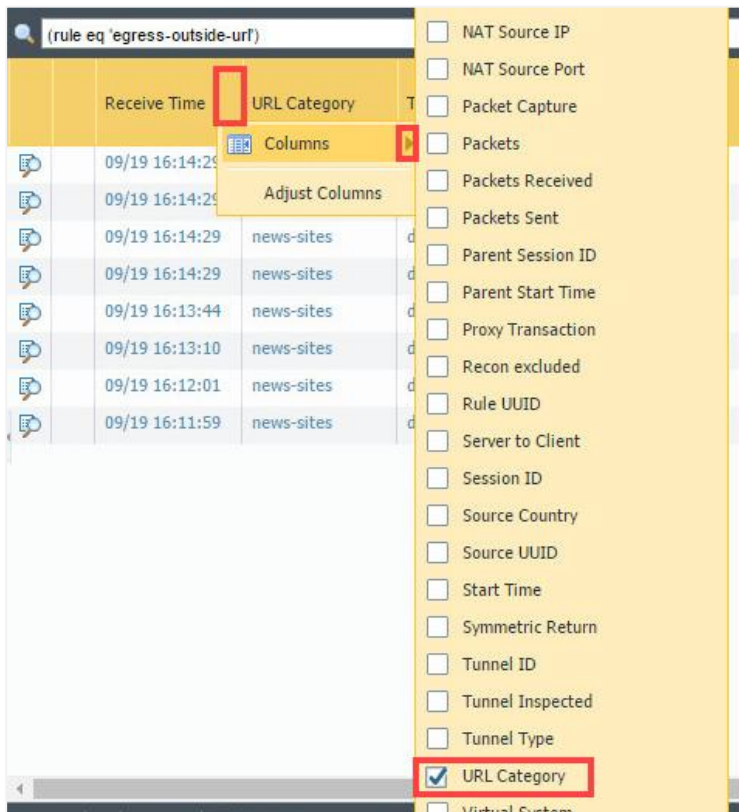
### 1.3 Review the Logs

1. In the web interface, navigate to **Policies > Security**.
2. 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	Zone
1	internal-inside-dmz	internal	universal	inside
2	egress-outside-url		universal	inside
3	egress-outside		universal	inside
4	danger-simulated-traff		universal	danger
5	intrazone-default		intrazone	any
6	interzone-default		interzone	any



- Notice that the firewall adds (*rule eq 'egress-outside-url'*) to the Traffic log filter text box. Click the down-arrow on any column header to add the **URL Category** column to the Traffic log display (when the list appears, scroll down to locate *URL Category*).



- Notice that the *URL Category* header now appears.

	Receive Time	URL Category	Type	From Zone
	09/19 16:14:29	news-sites	deny	inside
	09/19 16:14:29	news-sites	deny	inside
	09/19 16:14:29	news-sites	deny	inside
	09/19 16:14:29	news-sites	deny	inside
	09/19 16:13:44	news-sites	deny	inside
	09/19 16:13:10	news-sites	deny	inside
	09/19 16:12:01	news-sites	deny	inside
	09/19 16:11:59	news-sites	deny	inside



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



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

	Receive Time	Category	URL Category List	URL	From Zone
	09/19 16:14:29	news-sites	news-sites	www.msnbc.com/	inside
	09/19 16:14:29	news-sites	news-sites	www.msnbc.com/	inside
	09/19 16:14:29	news-sites	news-sites	www.msnbc.com/	inside
	09/19 16:14:29	news-sites	news-sites	www.msnbc.com/	inside
	09/19 16:13:44	news-sites	news-sites	foxnews.com/	inside
	09/19 16:13:10	news-sites	news-sites	foxnews.com/	inside
	09/19 16:12:01	news-sites	news-sites,not-resolved	bbc.com/	inside
	09/19 16:11:59	news-sites	news-sites	bbc.com/	inside

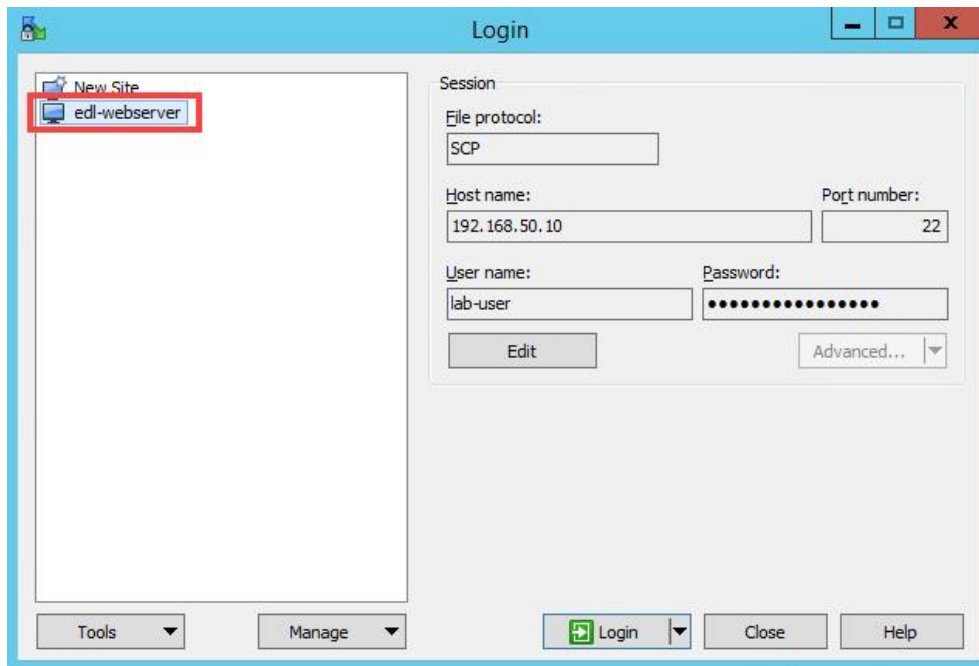
## 1.4 Configure an External Dynamic List

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

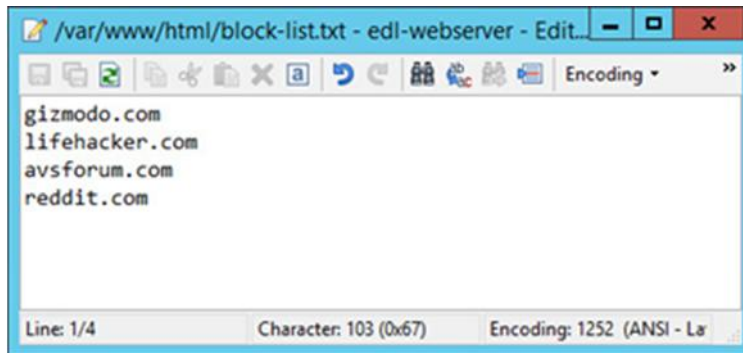
- In the *Login* window, double-click the list menu item **edl-webserver**.



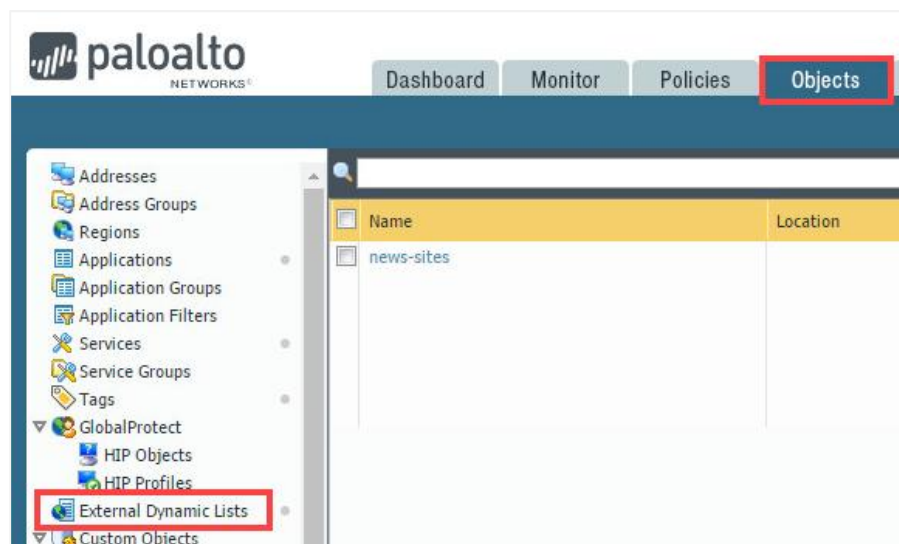
- Locate the text file in the right pane named **block-list.txt**. Right-click on it and select **Edit**.



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



5. **Save** and **Close** the file.
6. Close the **WinSCP** window. If prompted, click **OK**.
7. Change focus back to the firewall's web interface and select **Objects > External Dynamic Lists**.

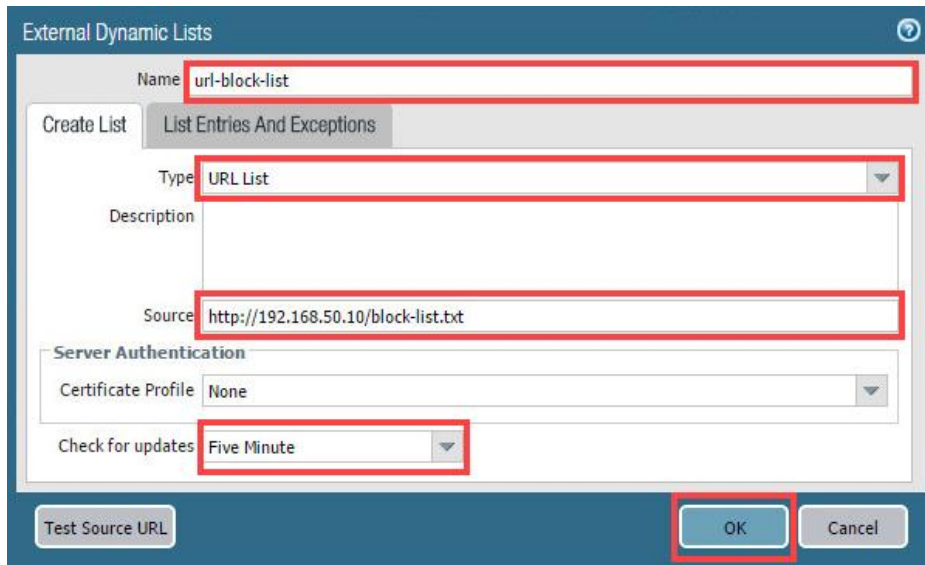


8. Click **Add** to configure a new External Dynamic List.



9. In the *External Dynamic Lists* window, configure the following. Once finished, click **OK**.

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

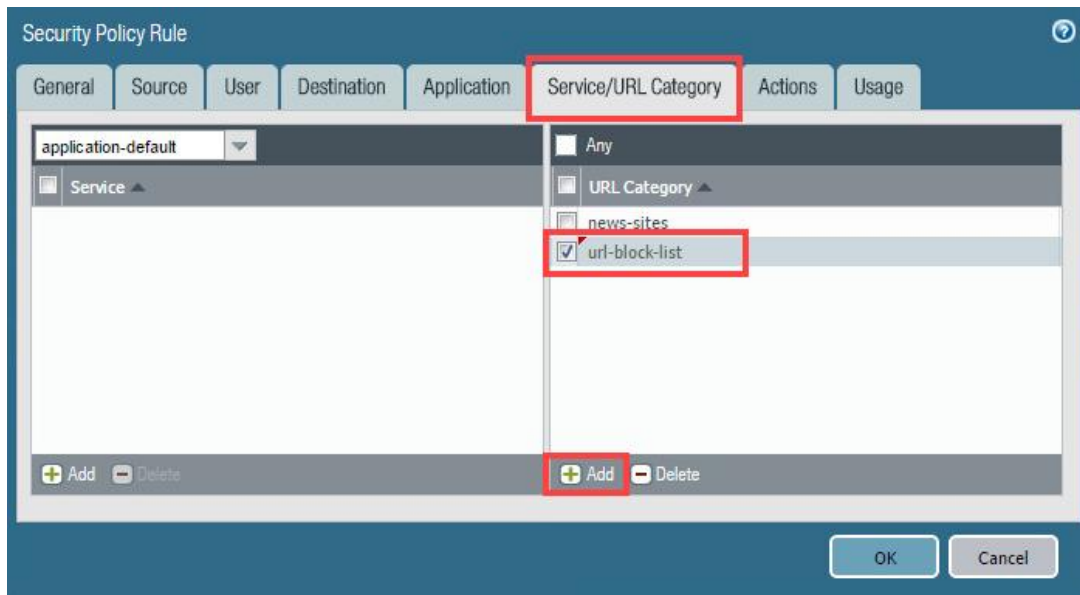


10. In the web interface, navigate to **Policies > Security**.
11. Click on **egress-outside-url** to open the Security policy rule.

	Name	Tags	Type	Zone
1	internal-inside-dmz	internal	universal	inside
2	egress-outside-url	egress	universal	inside
3	egress-outside	egress	universal	inside
4	danger-simulated-traffic	none	universal	dan
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

12. In the *Security Policy Rule* window, click the **Service/URL Category** tab and configure the following. Once finished, click **OK**.

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



13. **Commit** all changes.

## 1.5 Test the Security Policy Rule

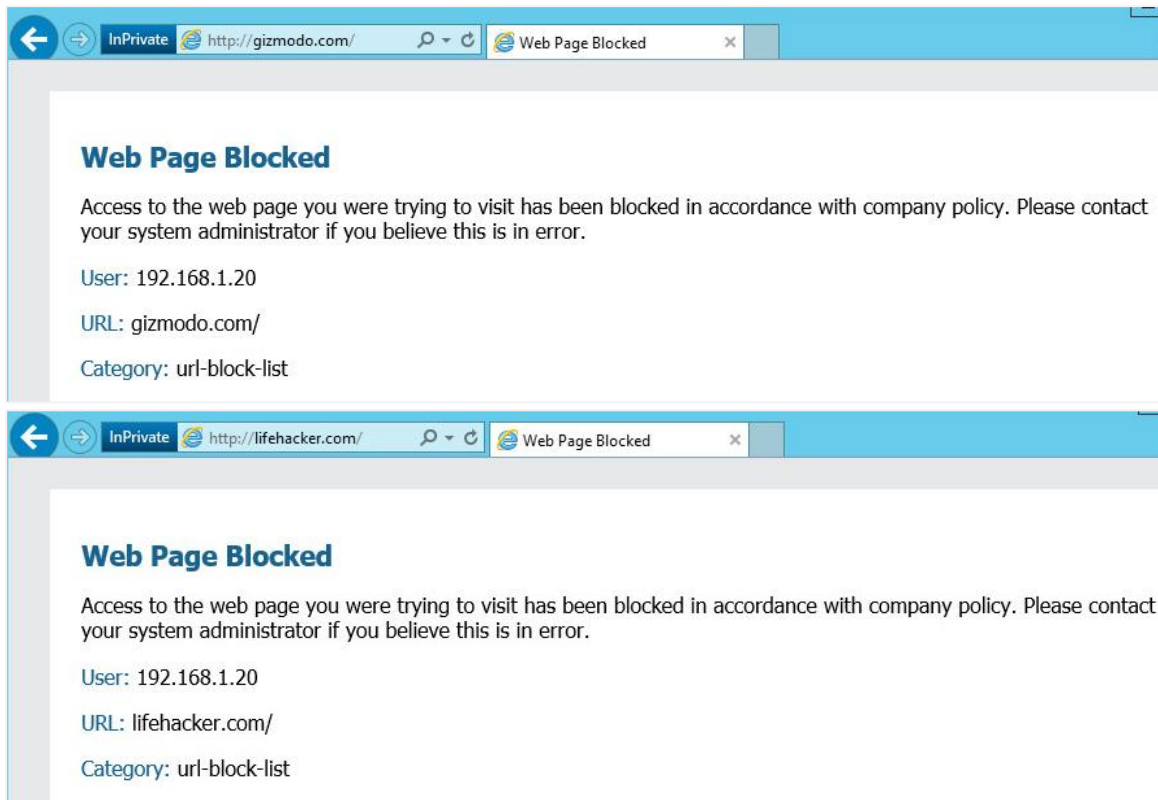
1. Open the **Internet Explorer** browser in **private/incognito mode** and browse to **avsforum.com**.



2. Notice the URL is blocked.



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



4. Close the IE browser.

## 1.6 Review the Logs

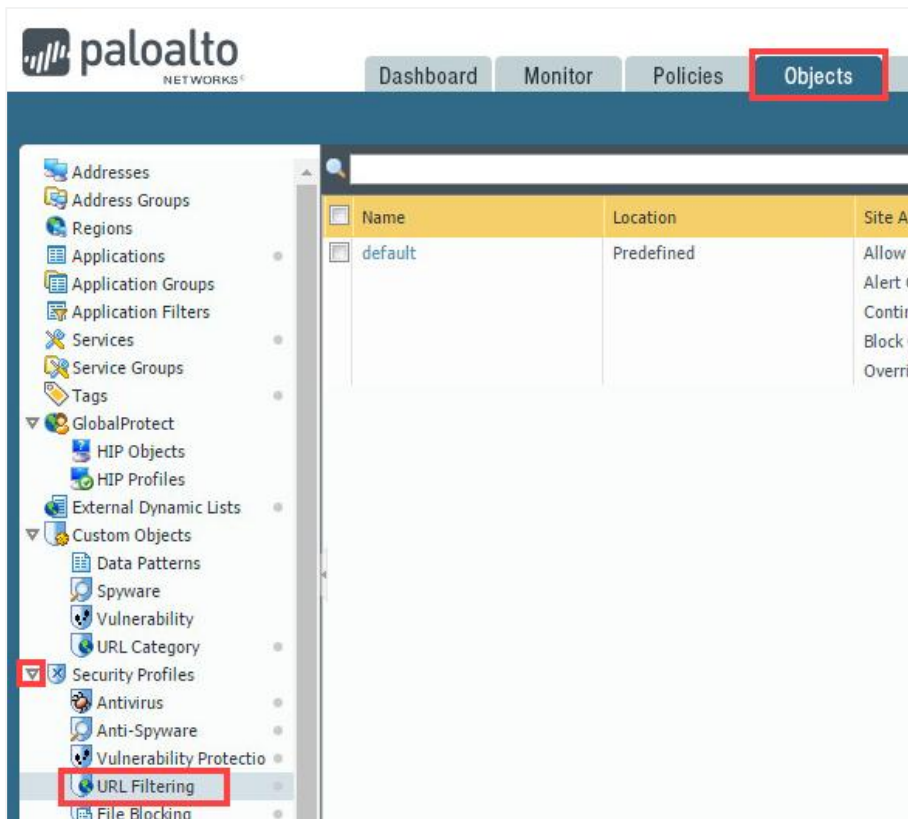
1. Change focus back to the firewall's web interface and navigate to **Monitor > Logs > URL Filtering**.
2. Notice that the *Category* column should display the name of the EDL you created, and the *Action* column shows that the URL is blocked.

	Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Destination	Application	Action
	09/19 20:52:44	url-block-list	url-block-list,computer-and-internet-info,low-risk	lifehacker.com/	inside	outside	192.168.1.20	151.101.194.166	web-browsing	block-url
	09/19 20:52:43	url-block-list	url-block-list	lifehacker.com/	inside	outside	192.168.1.20	151.101.194.166	web-browsing	block-url
	09/19 20:52:37	url-block-list	url-block-list,shopping,low-risk	newegg.com/	inside	outside	192.168.1.20	23.193.37.16	web-browsing	block-url
	09/19 20:52:32	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

3. Leave the firewall web interface open to continue with the next task.

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

1. In the web interface, navigate to **Objects > Security Profiles > URL Filtering**.



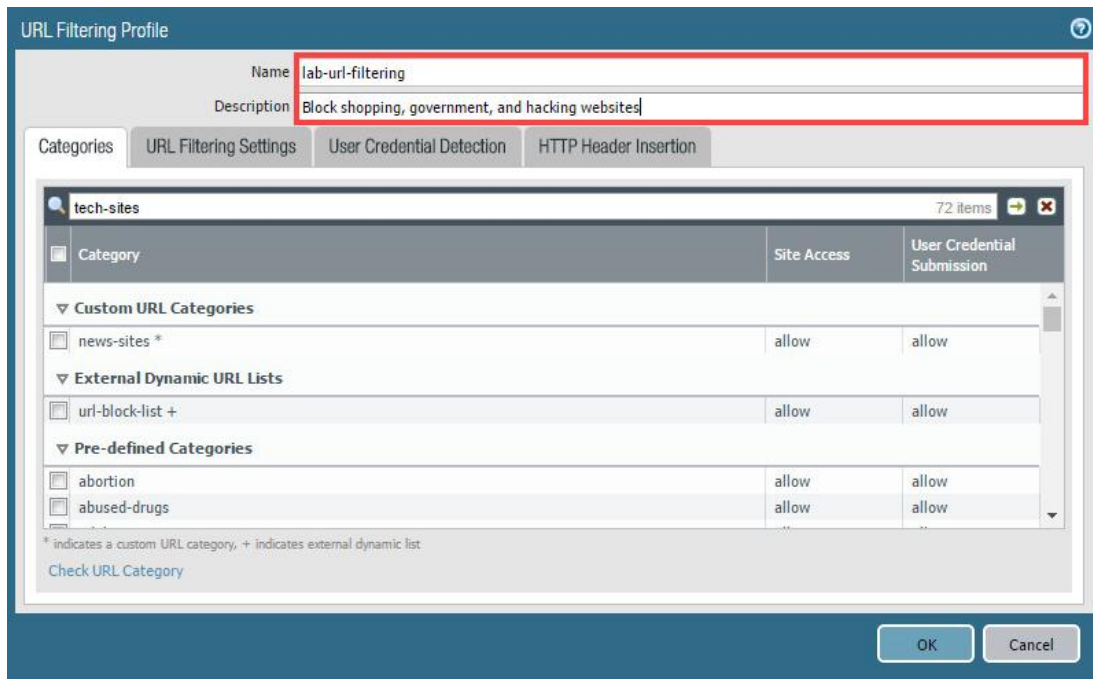
2. Click **Add** to define a URL Filtering Profile.



3. In the *URL Filtering Profile* window, configure the following.

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





URL Filtering Profile

Name: lab-url-filtering

Description: Block shopping, government, and hacking websites

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion

tech-sites 72 items

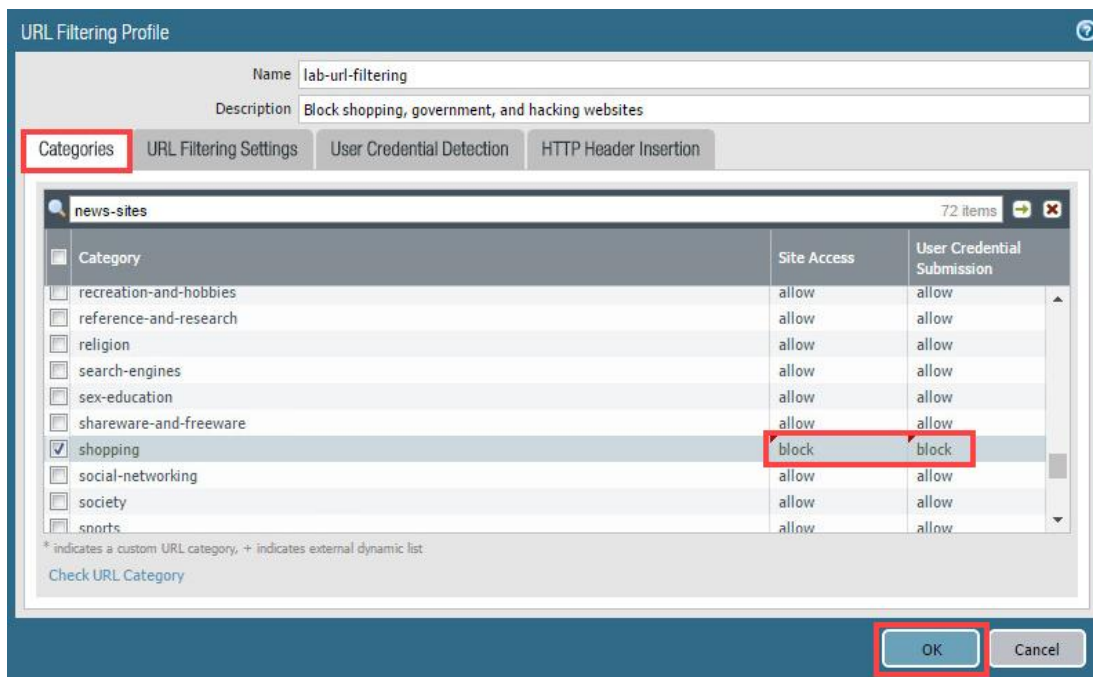
Category	Site Access	User Credential Submission
Custom URL Categories		
news-sites *	allow	allow
External Dynamic URL Lists		
url-block-list +	allow	allow
Pre-defined Categories		
abortion	allow	allow
abused-drugs	allow	allow

\* indicates a custom URL category, + indicates external dynamic list

Check URL Category

OK Cancel

- Make sure that the **Categories** tab is selected and locate the **shopping** category by scrolling down the list. Set the *Site Access* to **block**. Notice that the *User Credential Submission* also will change to **block** once you click away. Click **OK**.



URL Filtering Profile

Name: lab-url-filtering

Description: Block shopping, government, and hacking websites

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion

news-sites 72 items

Category	Site Access	User Credential Submission
recreation-and-hobbies	allow	allow
reference-and-research	allow	allow
religion	allow	allow
search-engines	allow	allow
sex-education	allow	allow
shareware-and-freeware	allow	allow
shopping	block	block
social-networking	allow	allow
society	allow	allow
sports	allow	allow

\* indicates a custom URL category, + indicates external dynamic list

Check URL Category

OK Cancel

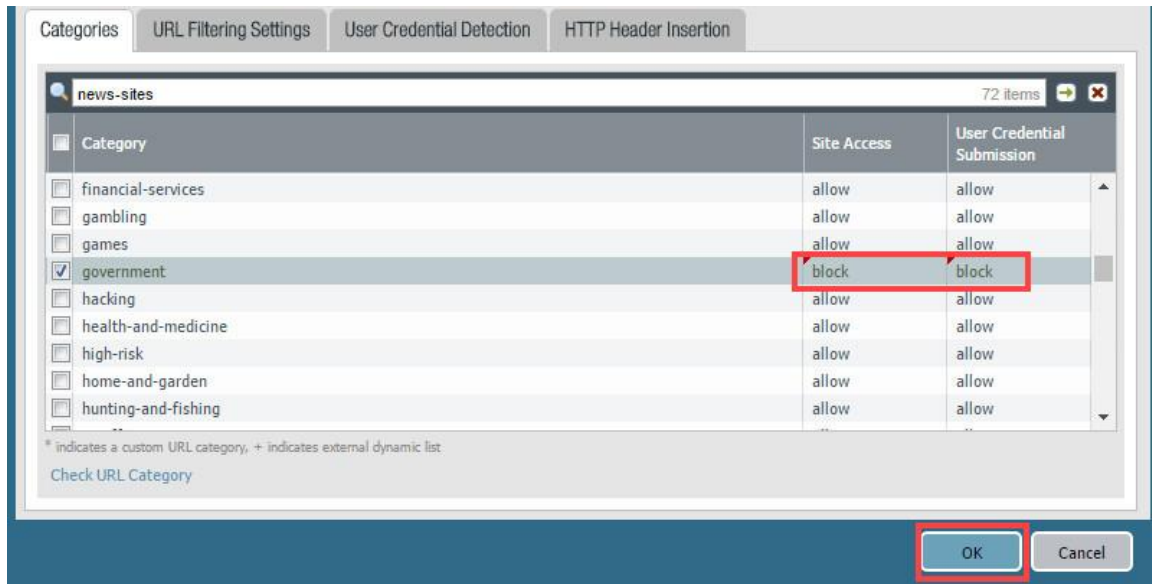
**Please Note**

Do not use the *Category* search field when configuring these settings, instead, manually find the categories in the list. Also, these settings need to be configured one at a time.

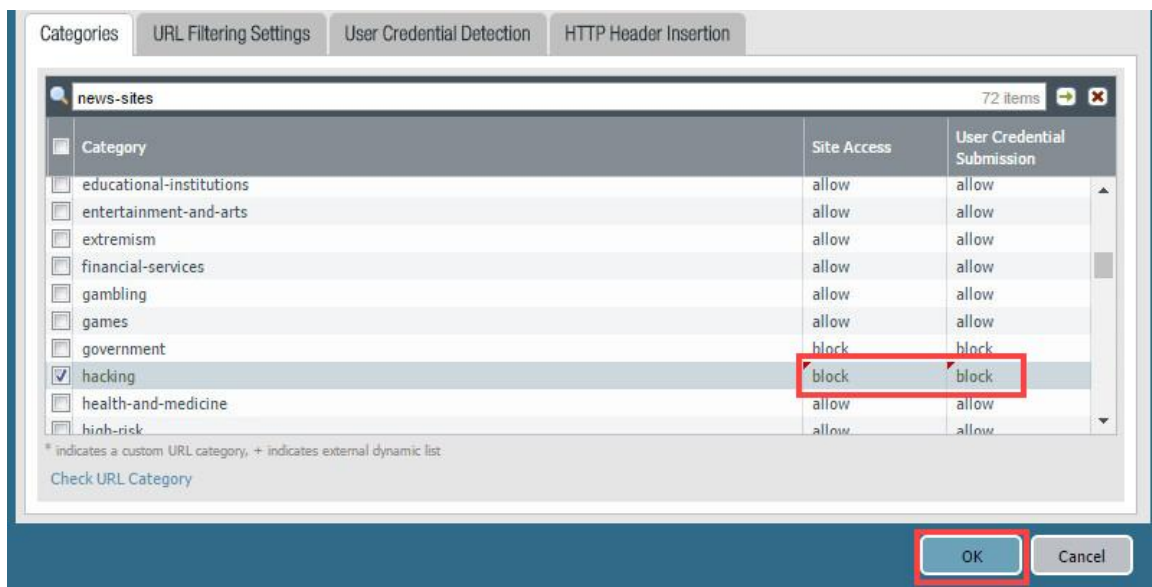


## Lab 6: URL Filtering

- Click on **lab-url-filtering** to configure the profile. Make sure that the **Categories** tab is selected and locate the **government** category by scrolling down the list. Set the **Site Access** to **block**. Notice that the *User Credential Submission* also will change to *block* once you click away. Click **OK**.

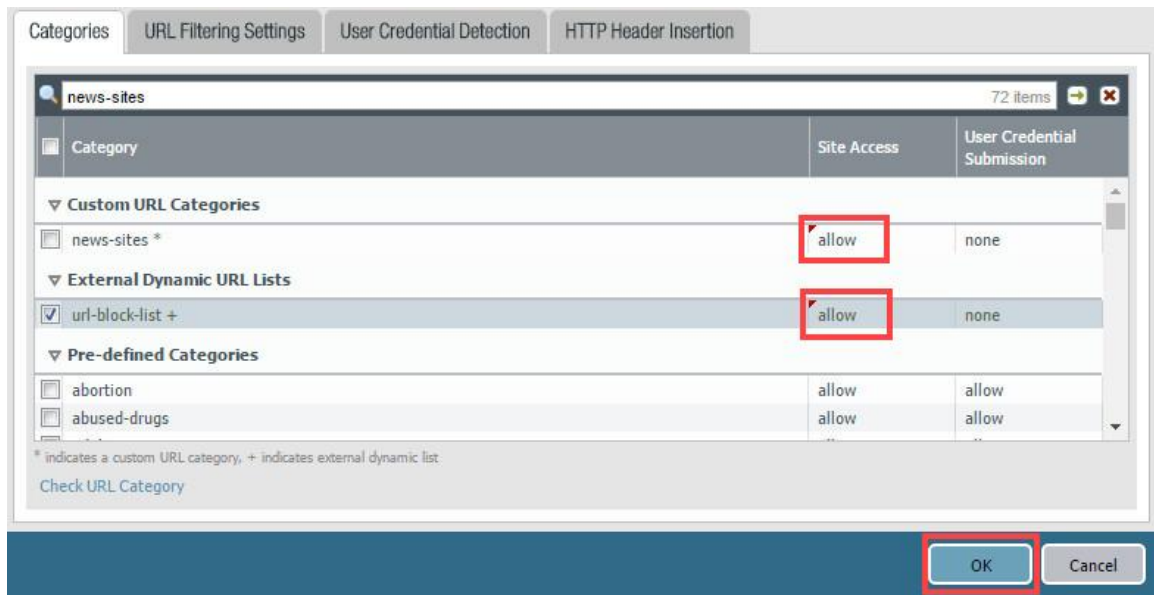


- Click on **lab-url-filtering** to configure the profile. Make sure that the **Categories** tab is selected and locate the **hacking** category by scrolling down the list. Set the **Site Access** to **block**. Notice that the *User Credential Submission* also will change to *block* once you click away. Click **OK**.



## Lab 6: URL Filtering

- Click on **lab-url-filtering** to configure the profile. Locate **url-block-list** and **news-sites**. Notice that your custom URL categories are also listed. Set their *Site Access* to **allow**. Click **OK**.



Category	Site Access	User Credential Submission
<b>Custom URL Categories</b>		
news-sites *	allow	none
<b>External Dynamic URL Lists</b>		
url-block-list +	allow	none
<b>Pre-defined Categories</b>		
abortion	allow	allow
abused-drugs	allow	allow

\* indicates a custom URL category, + indicates external dynamic list

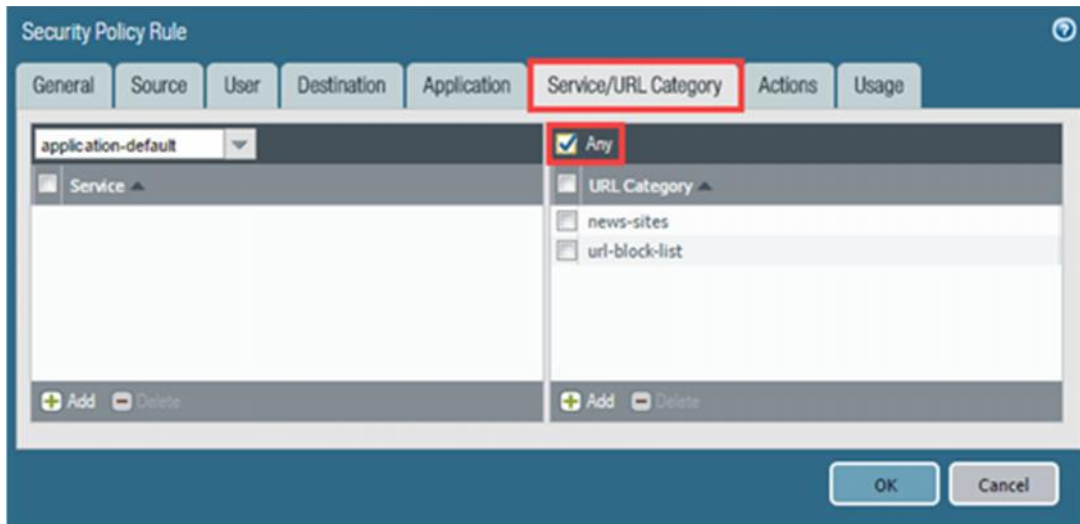
Check URL Category

OK Cancel

- In the web interface, navigate to **Policies > Security**.
- Click on **egress-outside-url** to configure the policy.

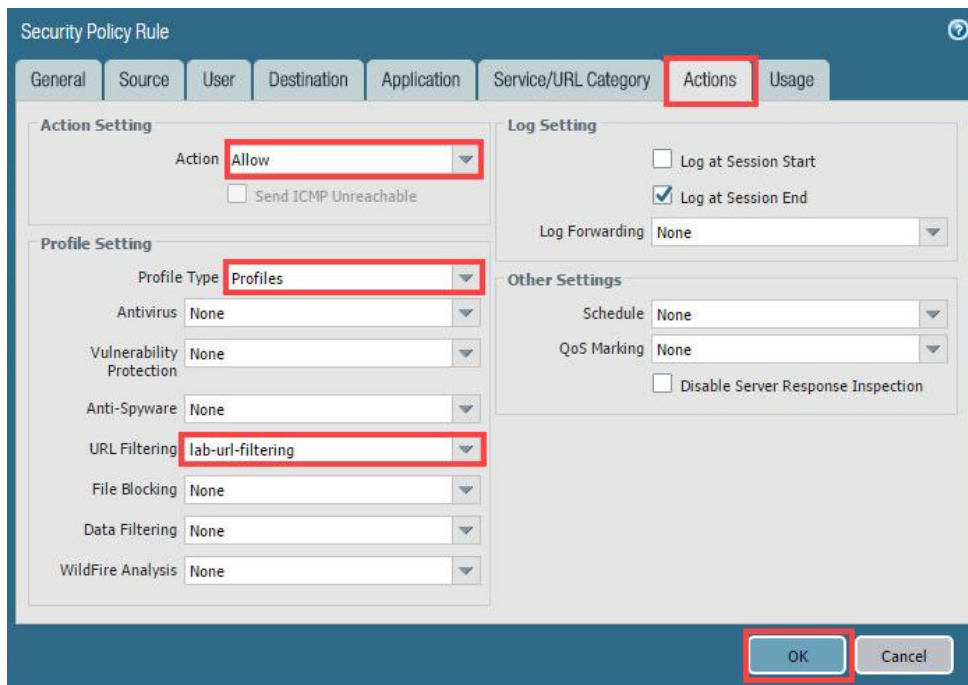
	Name	Tags	Type	Zone	Add
1	internal-inside-dmz	internal	universal	inside	any
2	egress-outside-url	egress	universal	inside	any
3	egress-outside	egress	universal	inside	any
4	danger-simulated-traffic	none	universal	danger	any
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any

10. In the *Security Policy Rule* window, click the **Service/URL Category** tab and then select **Any** above the **URL Category** list.



11. Click the **Actions** tab and configure the following. Once finished, click **OK**.

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



12. Select the **egress-outside** rule without opening it and click **Disable**.

	Name	Tags	Type	Zone
1	internal-inside-dmz	internal	universal	inside
2	egress-outside-url	egress	universal	inside
3	egress-outside	egress	universal	inside
4	danger-simulated-traffic	none	universal	danger
5	intrazone-default	none	intrazone	any
6	interzone-default	none	interzone	any

 Add
  Delete
  Clone
  Override
  Revert
  Enable
  Disable
  Move

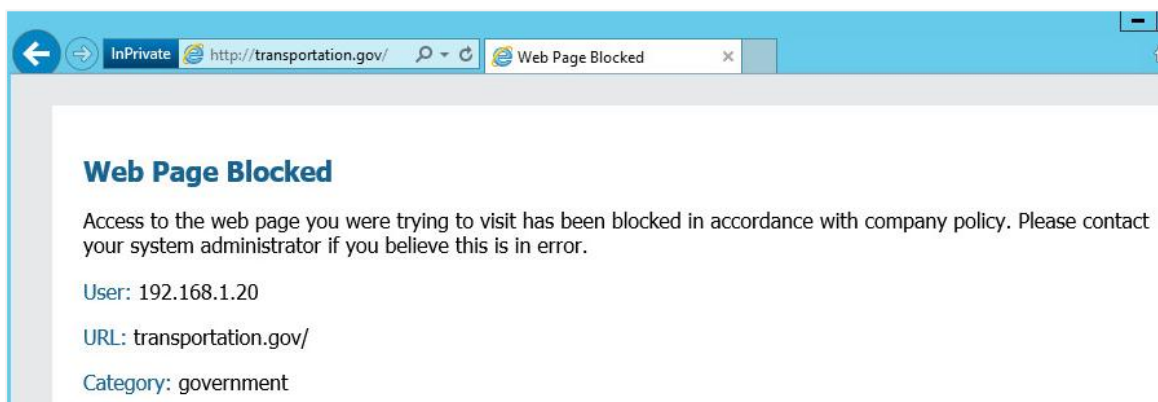


You can disable the *egress-outside* rule because the *URL Filtering Profile* is being used and the *egress-outside-url* Security policy rule now allows traffic.

13. **Commit** all changes.

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

1. Open the **Internet Explorer** browser in **private/incognito mode** and verify that **http://transportation.gov** (government), **http://2600.org** (hacking) are blocked.







2. Close the **IE** browser.

## 1.9 Review Logs

1. Change focus to the firewall's web interface and navigate to **Monitor > Logs > URL Filtering**.
2. Review the actions taken on the following entries:

	Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Destination	Application	Action
	09/19 21:15:12	hacking	hacking,low-risk	2600.org/	inside	outside	192.168.1.20	166.84.5.162	web-browsing	block-url
	09/19 21:14:39	government	government,low-risk	transportation.g...	inside	outside	192.168.1.20	204.63.195.12	web-browsing	block-url

3. The lab is now complete; you may end the reservation.