



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

### **Lab 5.1: Content ID Malware/Virus Protection**

**Document Version: 2017-09-29**

Copyright © 2017 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.

VMware is a registered trademark of VMware, Inc. Cisco, IOS, Cisco IOS, Networking Academy, CCNA, and CCNP are registered trademarks of Cisco Systems, Inc. EMC<sup>2</sup> is a registered trademark of EMC Corporation.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
5.1 Lab: Interface Configuration .....	6
5.1.0 Load Lab Configuration.....	6
5.1.1 Create Security Policy Rule with an Antivirus Profile .....	7
5.1.2 Test Security Policy Rule .....	9
5.1.3 Review Logs .....	10
5.1.4 Create Security Policy Rule with an Anti-Spyware Profile.....	11
5.1.5 Create DMZ Security Policy .....	15
5.1.6 Configure DNS-Sinkhole External Dynamic List.....	18
5.1.7 Anti-Spyware Profile with DNS Sinkhole .....	19
5.1.8 Test Security Policy Rule .....	20
5.1.9 Review the Logs .....	21

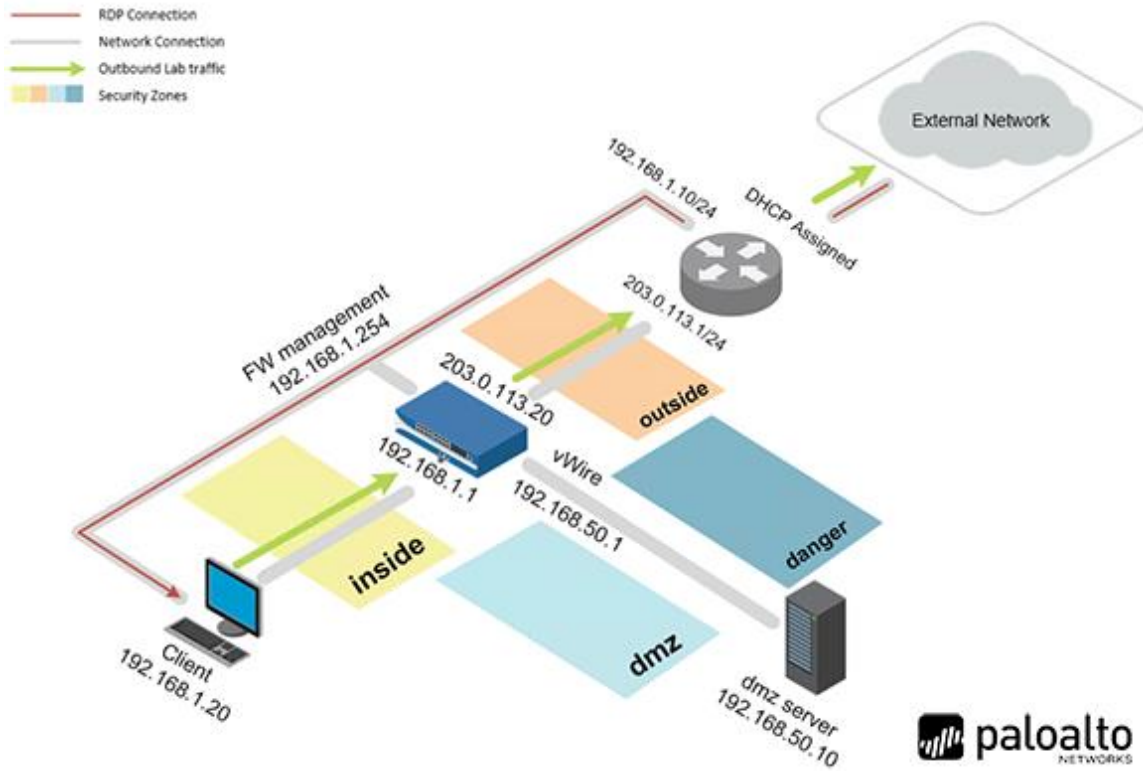
## Introduction

The Palo Alto Networks next-generation firewall has been deployed. The company has setup policies to allow certain types of applications. Now we need begin scanning the traffic as it passes through the firewall for threats. We need to look for exploits, viruses, spyware and other malicious threats.

## Objectives

- Configure and test a Vulnerability Security Profile.
- Configure and test a File Blocking Security Profile.
- Use the Virtual Wire mode and configure the danger zone.
- Generate threats and observe the actions taken.

## Lab Topology



## Lab Settings

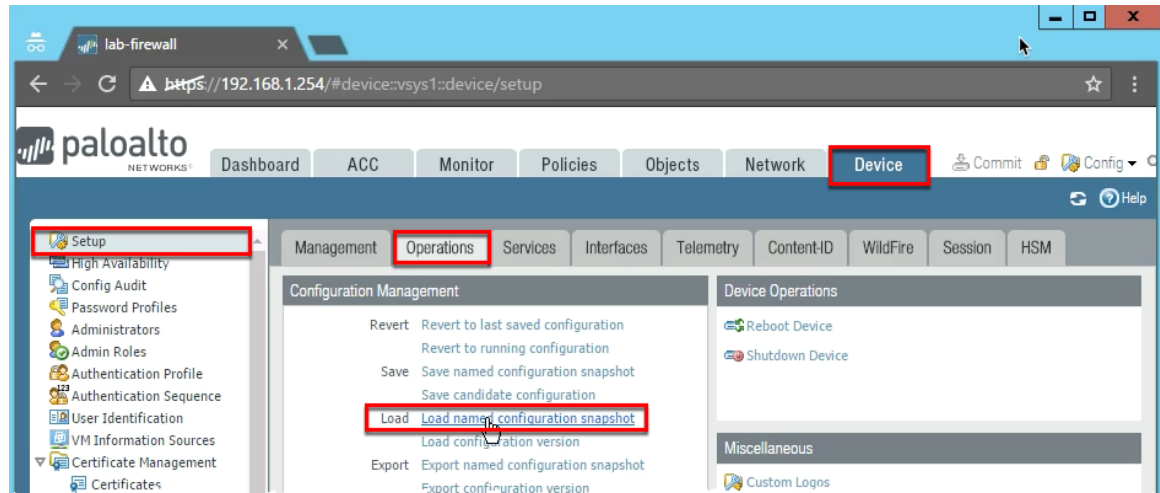
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

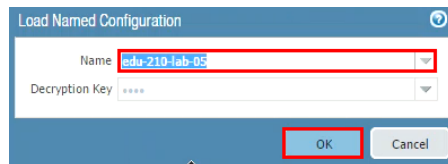
## 5.1 Lab: Interface Configuration

### 5.1.0 Load Lab Configuration

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



3. Select **edu-210-lab-05** and click **OK**.



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

### 5.1.1 Create Security Policy Rule with an Antivirus Profile

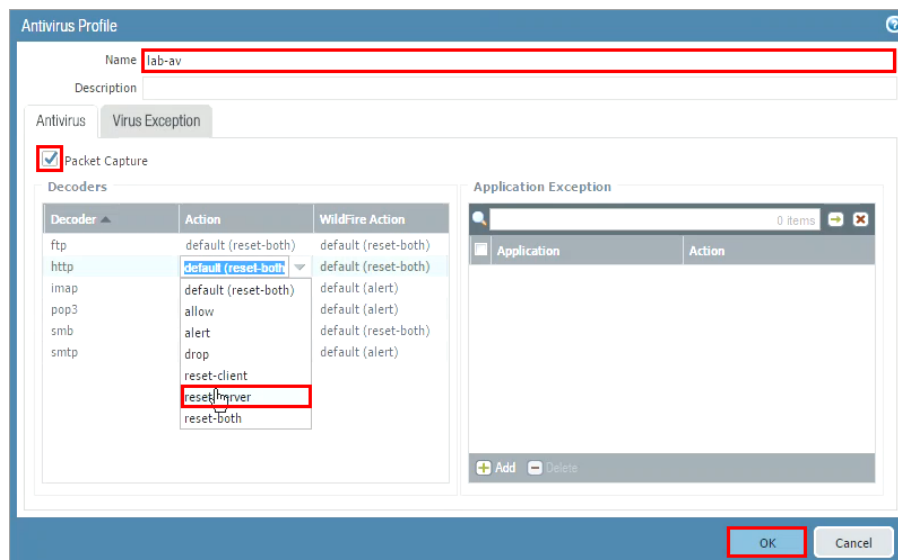
Use an Antivirus Profile object to configure options to have the firewall scan for viruses on traffic matching a Security policy rule.

1. Select **Objects > Security Profiles > Antivirus** then click **Add** to create a Antivirus Profile.

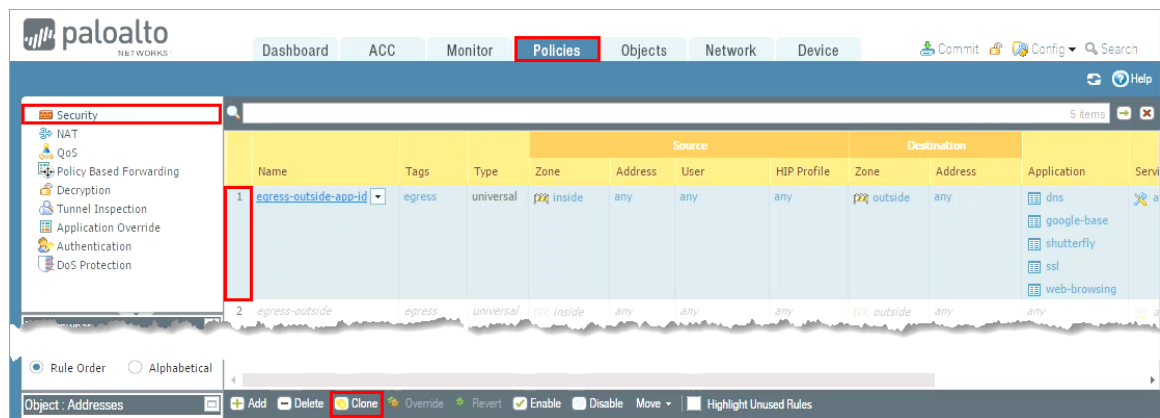


2. In the **Antivirus Profile** window configure the following the click **OK**.

Parameter	Value
Name	lab-av
Packet Capture	Checked
<b>Decoders</b>	
http	reset-server



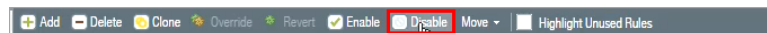
3. Select **Policies > Security**, select the **egress-outside-app-id** security policy rule without opening it then click **Clone**.



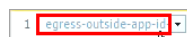
4. Select **Move top** from the Rule order drop-down list then click **OK**.



5. With the original egress-outside-app-id still selected, click **Disable**.

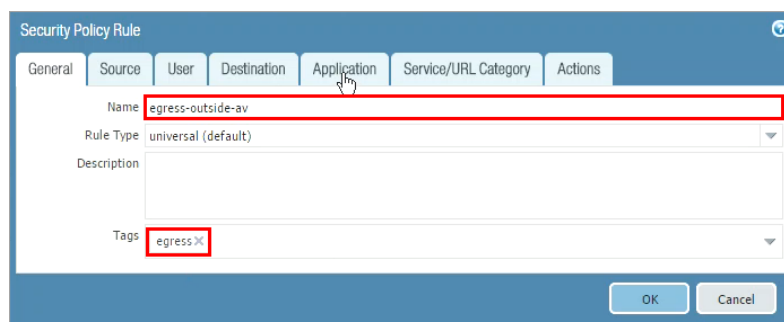


6. Click to open the cloned Security policy rule named **egress-outside-app-id-1**.



7. In the **Security Policy Rule** window under the **General** tag configure the following.

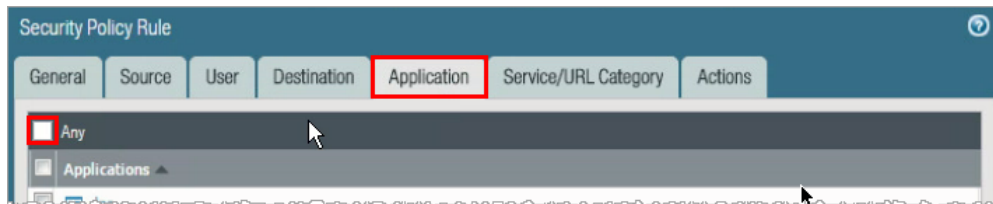
Parameter	Value
Name	egress-outside-av
Tags	egress





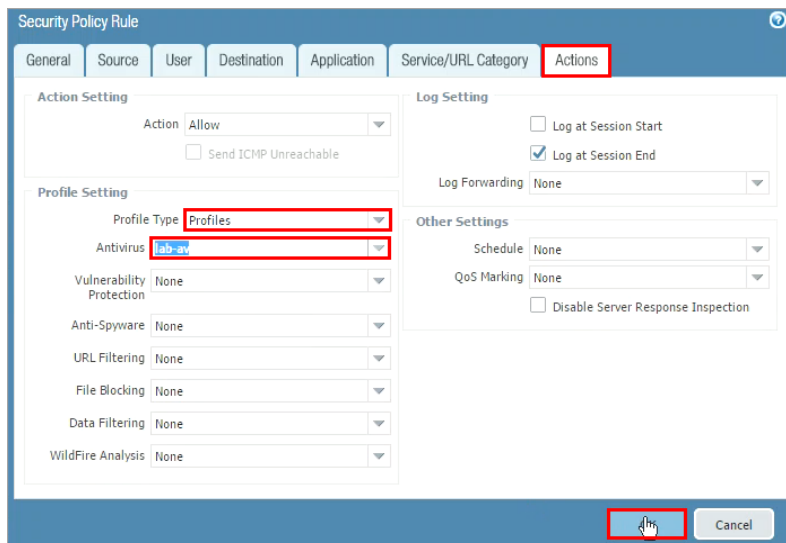
8. Click the **Application** tab and configure the following:

Parameter	Value
Any	Checked



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

Parameter	Value
Profile Type	Profiles
<b>Profile Setting</b>	
Antivirus	lab-av



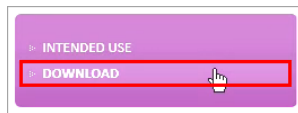
10. Click **OK** to close the Security Policy Rule configuration window.  
 11. **Commit** all changes.

### 5.1.2 Test Security Policy Rule

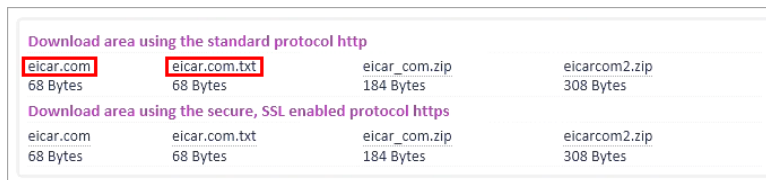
1. On your desktop, open a new browser in private/incognito mode and browse to <http://www.eicar.org>.
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:



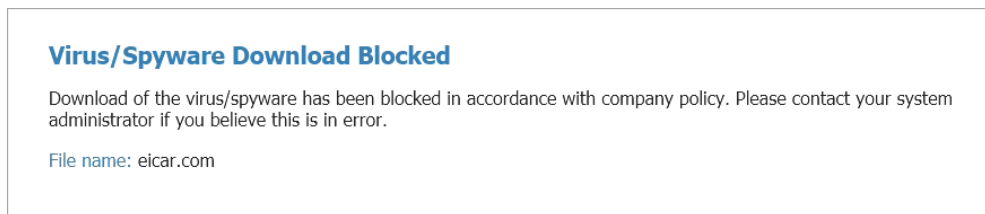
- Click the **Download** link on the left of the web page:



- Within the Download area at the bottom of the page, click either the **eicar.com** or the **eicar.com.txt** file to download the file using standard HTTP and not SSL-enabled HTTPS. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.



- If prompted, **Save** the file. Do not open or run the file.



- Close the browser window.

### 5.1.3 Review Logs

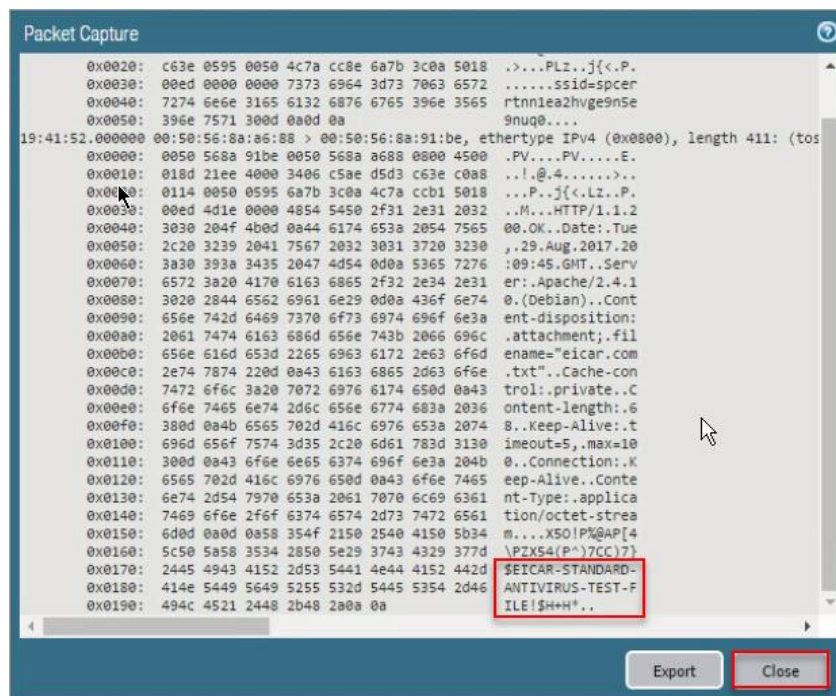
- In the WebUI select **Monitor > Logs > Threat**.
- Find the log message that detected the **Eicar Test File**. Notice that the action for the file is **reset-server**.

To Port	Application	Action	Severity	File Name
56835	web-browsing	reset-server	medium	eicar.com.txt

- Click the **Packet Capture Download** icon on the left side of the entry for the **Eicar Test File** to display the packet capture (pcap):

	Receive Time	Type	Name	From Zone	To Zone	Attacker
	08/29 19:41:52	virus	Eicar Test File	outside	inside	213.211.198.62

Here is an example of what a pcap might look like:

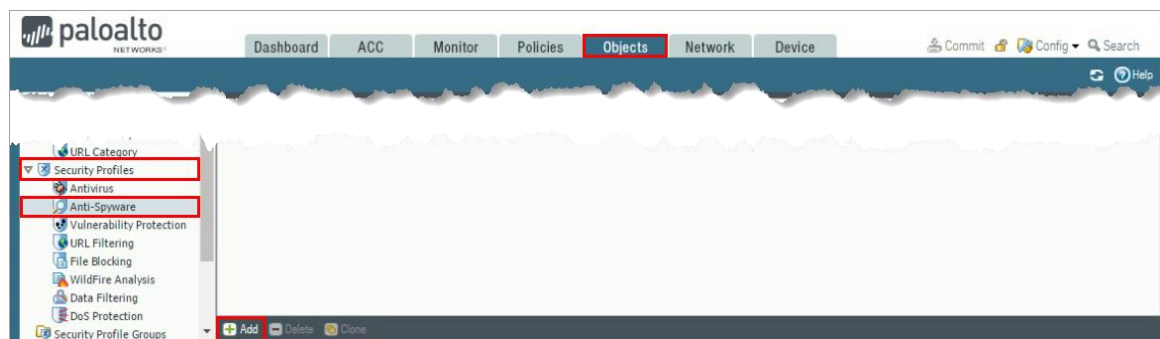


Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

4. After viewing the pcap, click **Close**.

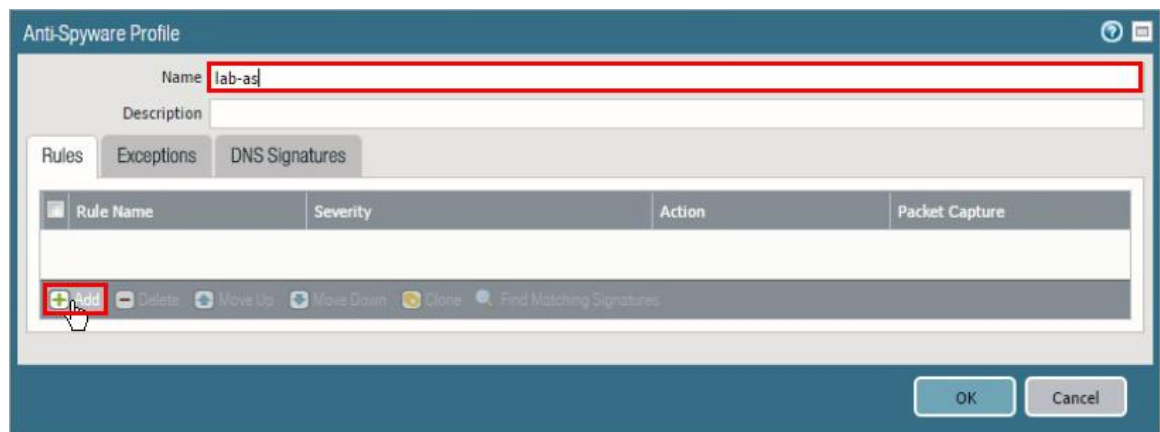
#### 5.1.4 Create Security Policy Rule with an Anti-Spyware Profile

1. Select **Objects > Security Profiles > Anti-Spyware** then click **Add** to create an Anti-Spyware Profile.



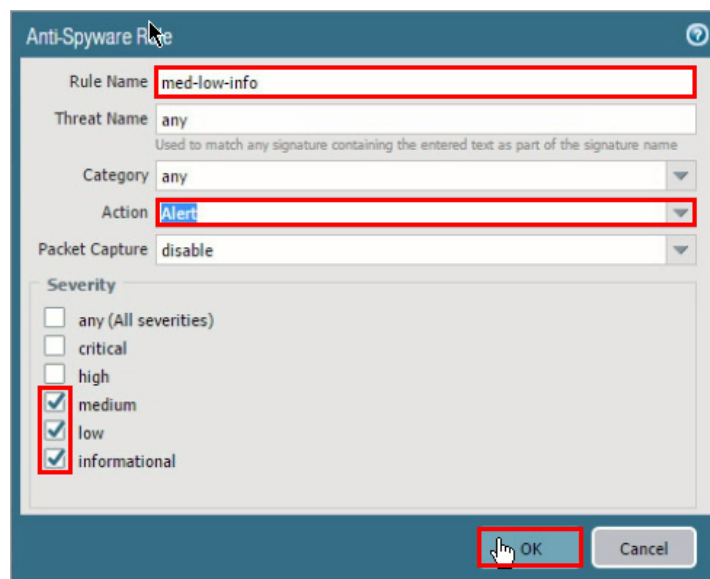
2. In the **Anti-Spyware Profile** window configure the following then click Add under the **Rules** tab.

Parameter	Value
Name	lab-as



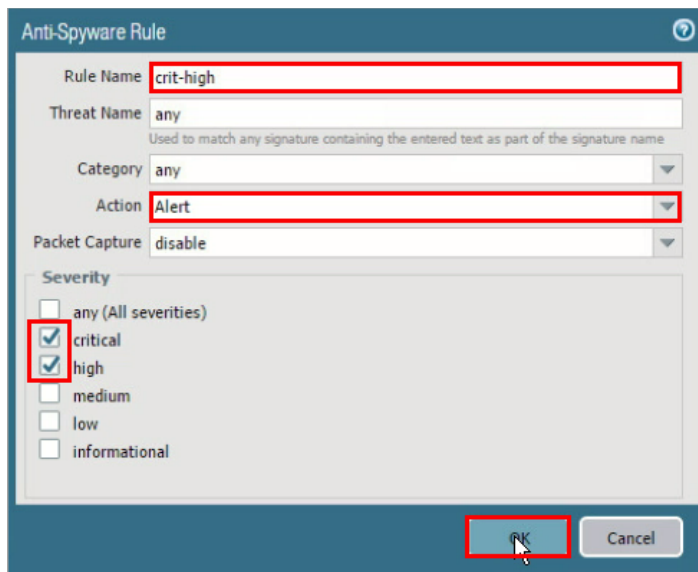
3. In the **Anti-Spyware Rule** window configure the following then click **OK**.

Parameter	Value
Rule Name	med-low-info
Action	<b>Alert</b>
Severity	medium low informational



4. Click **Add** to create a new **Anti-Spyware Rule** then fill in the following data and click **OK**.

Parameter	Value
Rule Name	crit-high
Action	<b>Alert</b>
Severity	critical high



**Anti-Spyware Rule**

Rule Name: **crit-high**

Threat Name: any  
Used to match any signature containing the entered text as part of the signature name

Category: any

Action: **Alert**

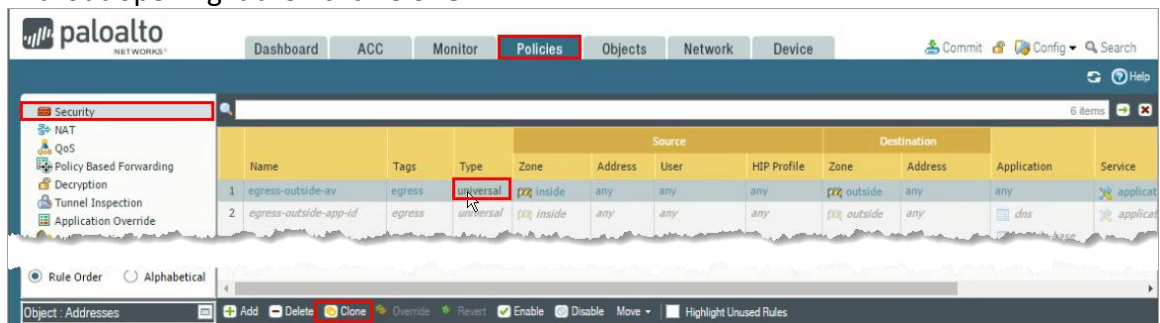
Packet Capture: disable

Severity:

- ☐ any (All severities)
- ☒ critical
- ☒ high
- ☐ medium
- ☐ low
- ☐ informational

OK Cancel

5. Click **OK** to close the **Anti-Spyware Profile** window.
6. Under **Policies > Security** select the **egress-outside-av** Security policy rule without opening it then click **Clone**.



**paloalto** NETWORKS

Dashboard ACC Monitor **Policies** Objects Network Device

Commit Config Search

Security 6 items

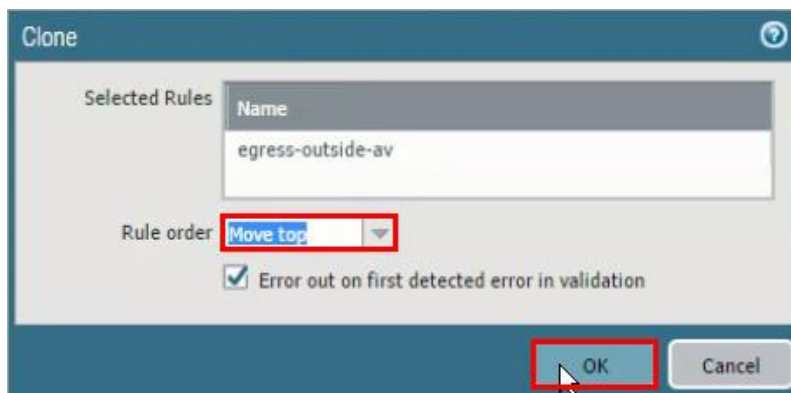
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
1	egress-outside-av	egress	universal	outside	any	any	any	outside	any	any	application
2	egress-outside-app-id	egress	universal	inside	any	any	any	outside	any	dns	application

Rule Order Alphabetical

Object: Addresses

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

7. Select **Move top** from the Rule order drop-down list then click **OK**.



**Clone**

Selected Rules

Name: egress-outside-av

Rule order: **Move top**

☒ Error out on first detected error in validation

OK Cancel

8. With the original egress-outside-av still selected, click **Disable**.



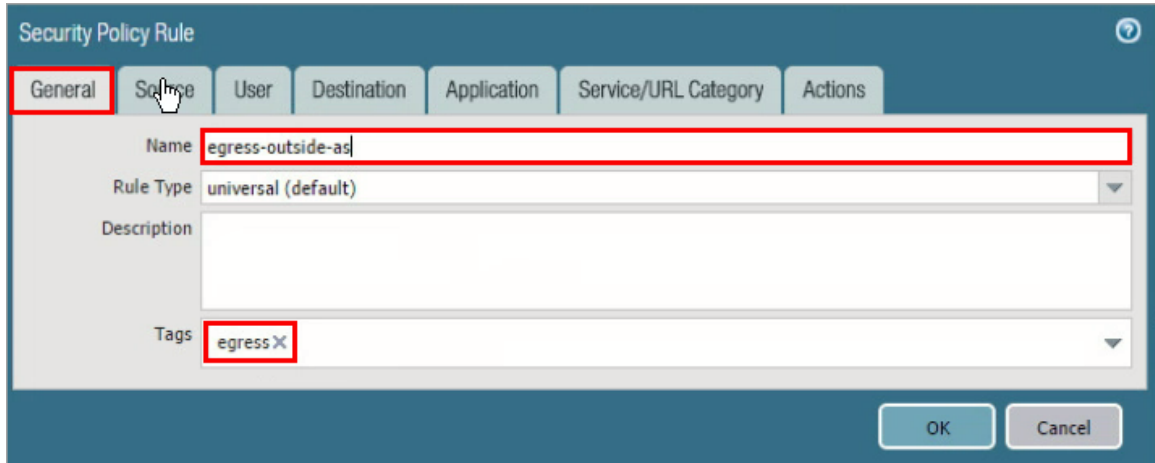
Add Delete Clone Override Revert Enable **Disable** Move Highlight Unused Rules

9. Click to open the cloned Security policy rule named **egress-outside-av-1**.

	Name	Tags	Type
1	egress-outside-av-1	egress	universal

10. In the **Security Policy Rule** window under the **General** tab and configure the following.

Parameter	Value
Name	egress-outside-as
Tags	egress



Security Policy Rule

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

Name: egress-outside-as

Rule Type: universal (default)

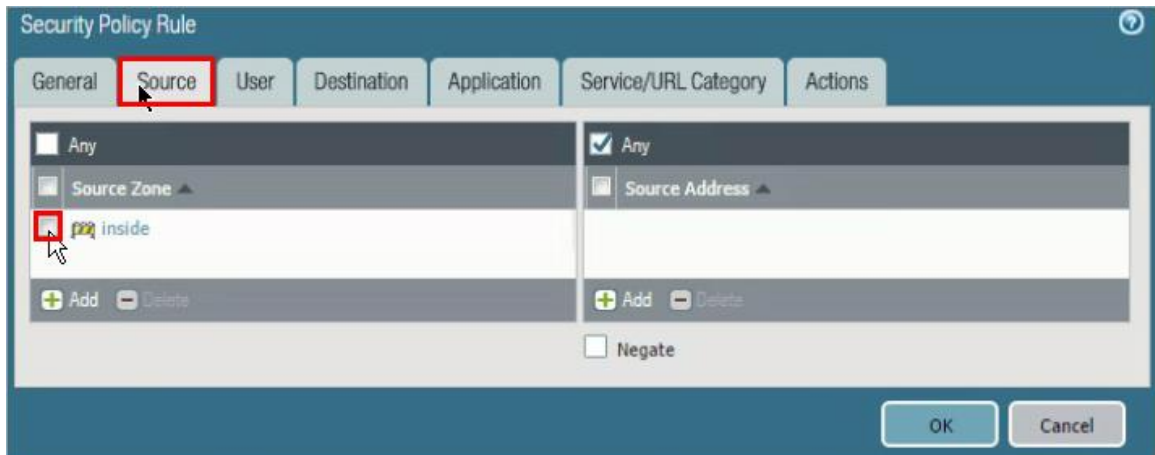
Description:

Tags: egress

OK Cancel

11. Under the **Source** tab is configure the following.

Parameter	Value
Source Zone	inside



Security Policy Rule

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

Any

Source Zone: inside

Source Address: Any

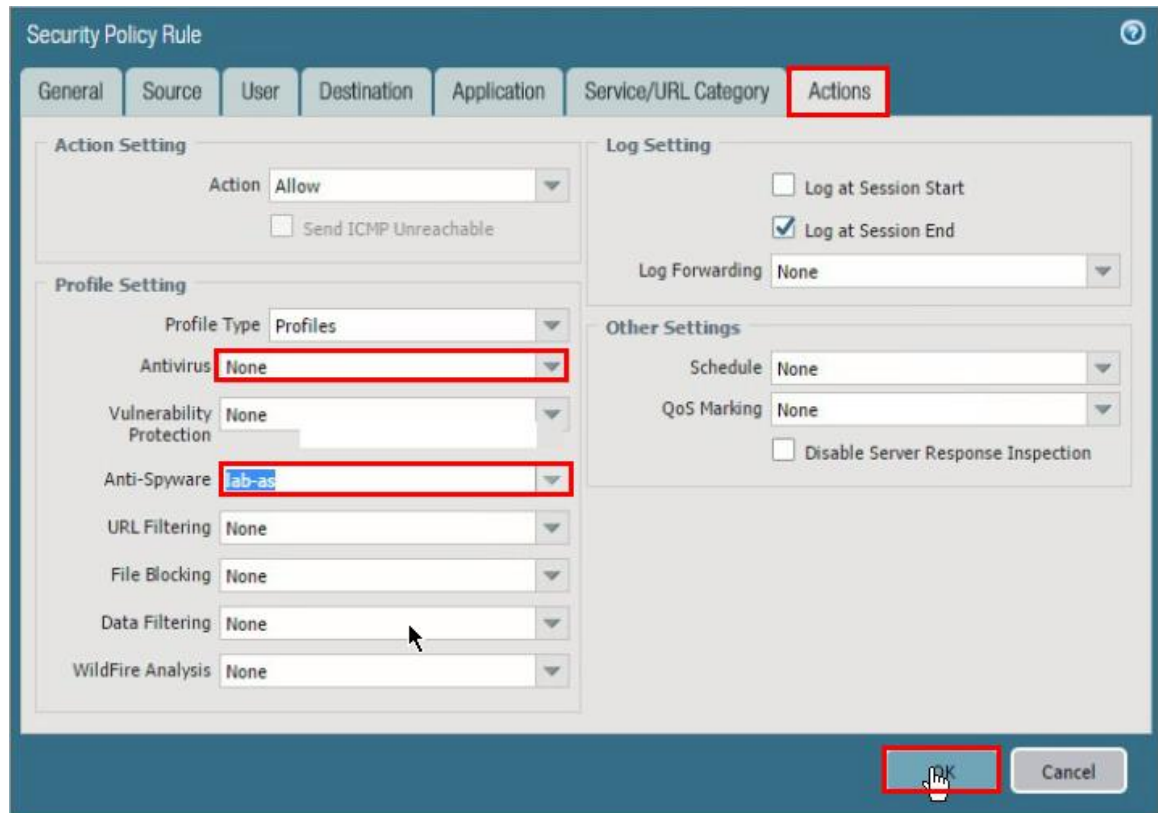
Add Delete

Negate

OK Cancel

12. Under the **Actions** tab configure the following then click **OK**.

Parameter	Value
Antivirus	None
Anti-Spyware	lab-as



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

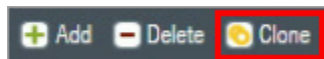
### 5.1.5 Create DMZ Security Policy

Because the management interface uses the inside interface as the gateway, you need to allow this traffic via a Security policy rule.

1. Select the **internal-dmz-ftp** Security policy rule without opening it.

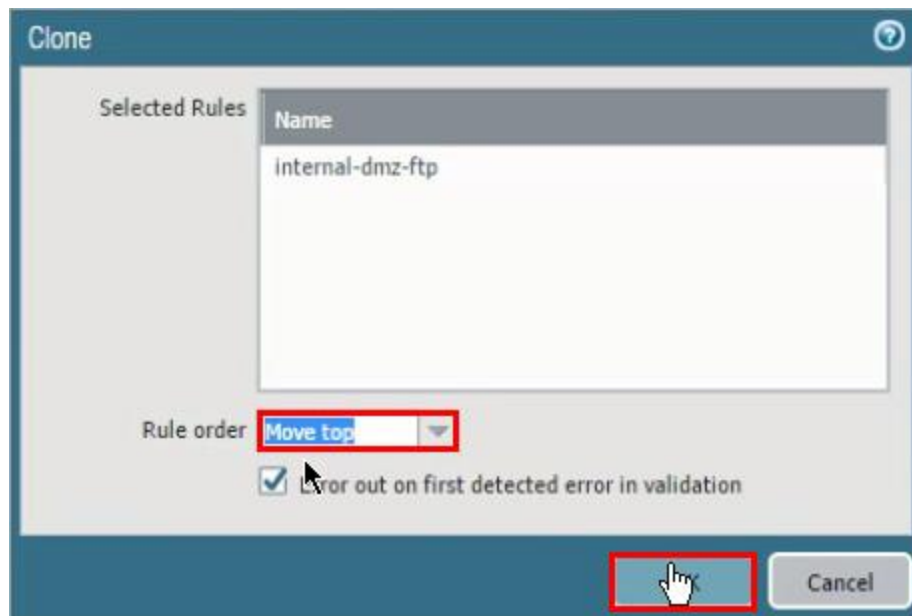


2. Click **Clone**. The Clone configuration window opens.

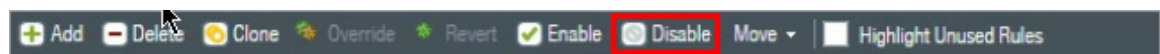


3. Select **Move top** from the Rule order drop-down list then click **OK** to close the Clone configuration window.





4. With the original internal-dmz-ftp still selected, click **Disable**.

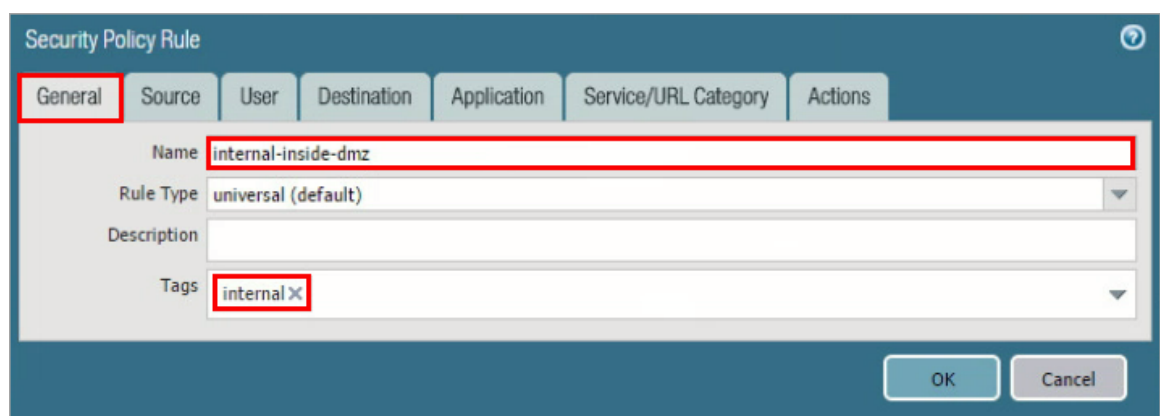


5. Click to open the cloned Security policy rule named **internal-dmz-ftp-1**.



6. Under the **General** tab configure the following:

Parameter	Value
Name	internal-inside-dmz
Tags	internal

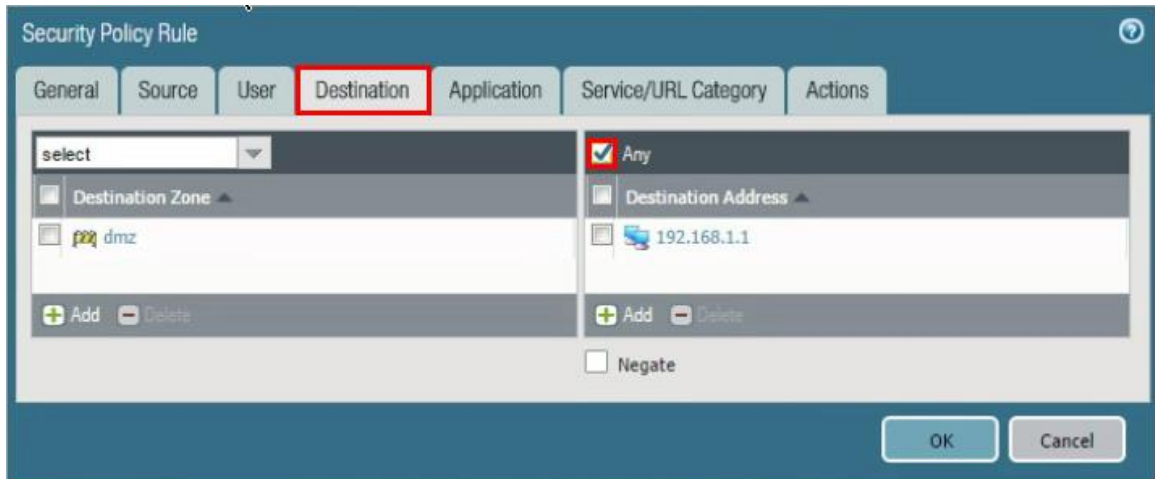


7. Under the **Destination** tab and configure the following:

Parameter	Value
Destination Address	



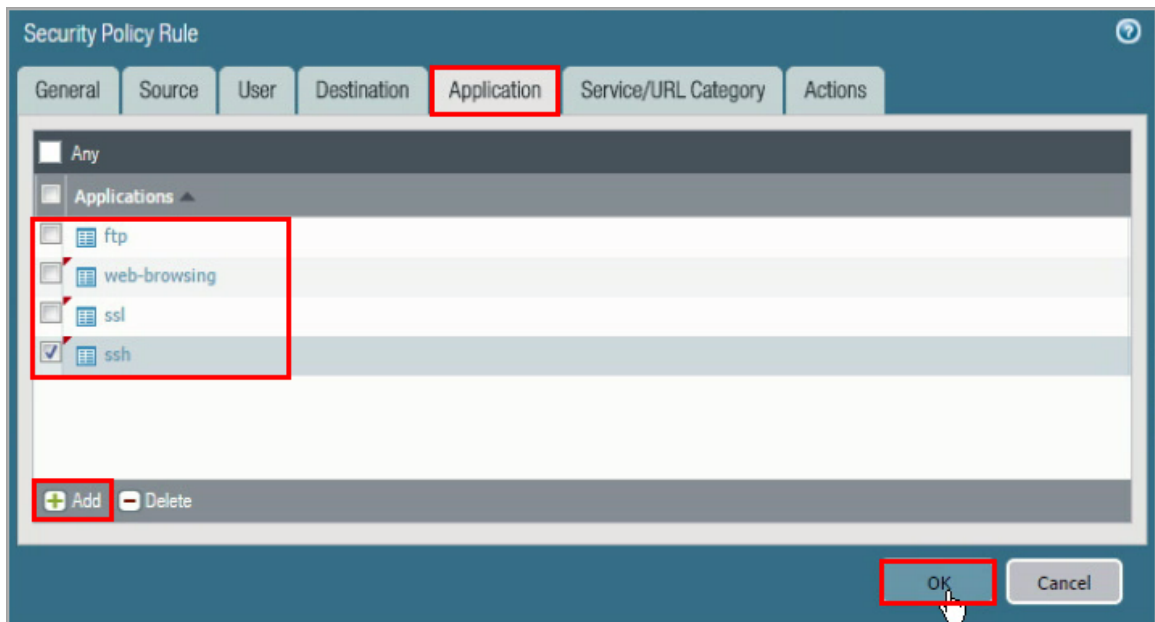
Any	Checked
-----	---------



The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'Destination Zone' list contains 'dmz'. The 'Destination Address' list contains '192.168.1.1'. The 'Any' checkbox is checked. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

8. Click the **Application** tab to configure the following than click **OK**.

Parameter	Value
Applications	web-browsing ssl ssh ftp

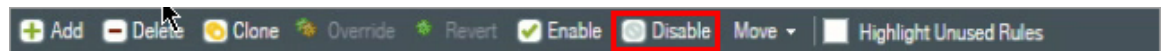


The screenshot shows the 'Security Policy Rule' configuration window with the 'Application' tab selected. The 'Applications' list contains 'ftp', 'web-browsing', 'ssl', and 'ssh'. The 'ssh' application is selected with a checkmark. The 'Add' button is highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom right, with the 'OK' button also highlighted with a red box.

9. Under **Policies > NAT** select the **destination-dmz-ftp** NAT policy rule without opening it.



10. Click **Disable**.



11. **Commit** all changes.

### 5.1.6 Configure DNS-Sinkhole External Dynamic List

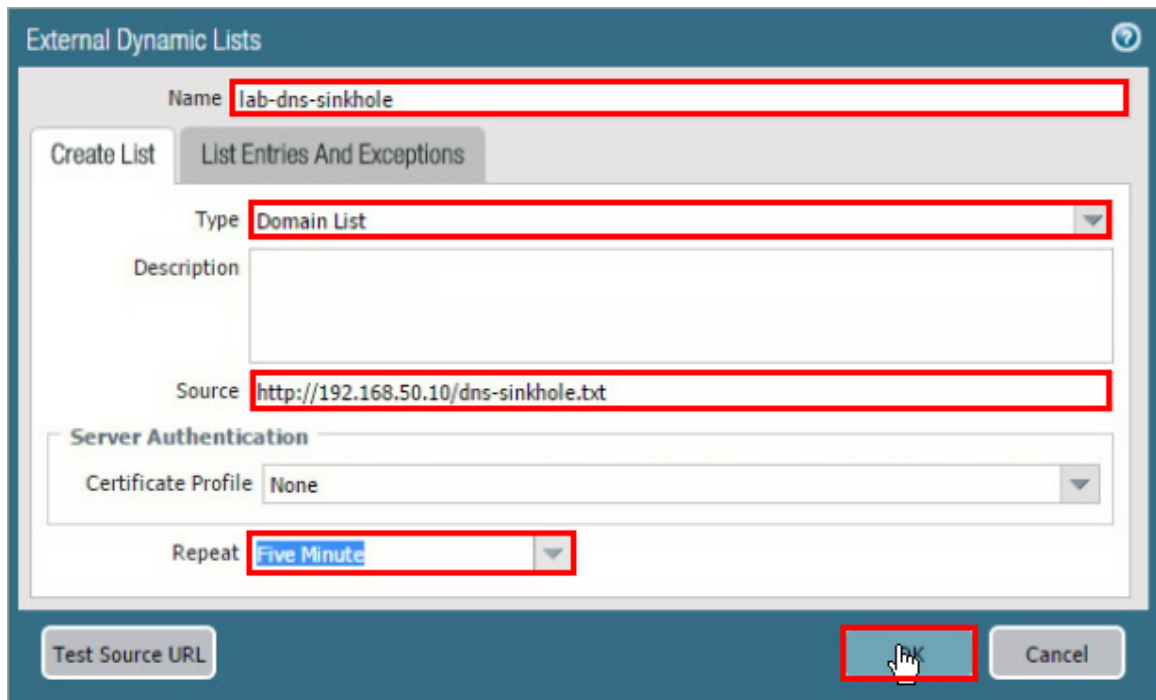
An External Dynamic List is an object that references an external list of IP addresses, URLs, or domain names that can be used in policy rules. You must create this list as a text file and save it to a web server that the firewall can access. By default, the firewall uses its management port to retrieve the list items.

1. Select **Objects > External Dynamic Lists** click **Add** to configure a new External Dynamic List.



2. In the External Dynamic Lists window, configure the following then click **OK**.

Parameter	Value
Name	lab-dns-sinkhole
Type	<b>Domain List</b>
Source	<a href="http://192.168.50.10/dns-sinkhole.txt">http://192.168.50.10/dns-sinkhole.txt</a> (This is hosted on the DMZ server.)
Repeat	<b>Five Minute</b>



External Dynamic Lists

Name: **lab-dns-sinkhole**

Create List | List Entries And Exceptions

Type: **Domain List**

Description:

Source: **http://192.168.50.10/dns-sinkhole.txt**

Server Authentication

Certificate Profile: **None**

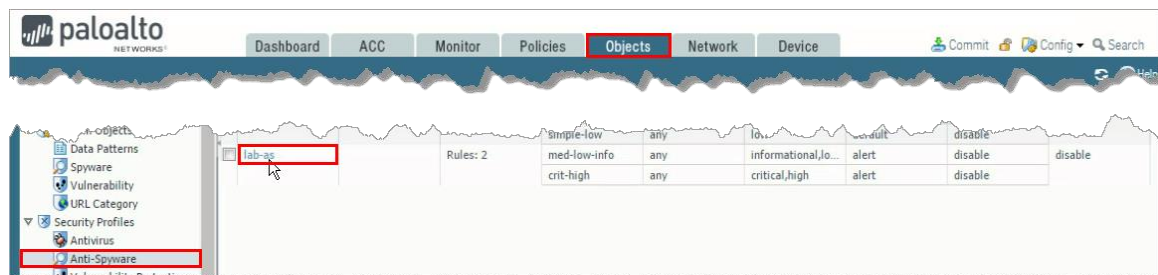
Repeat: **Five Minute**

Test Source URL | **OK** | Cancel

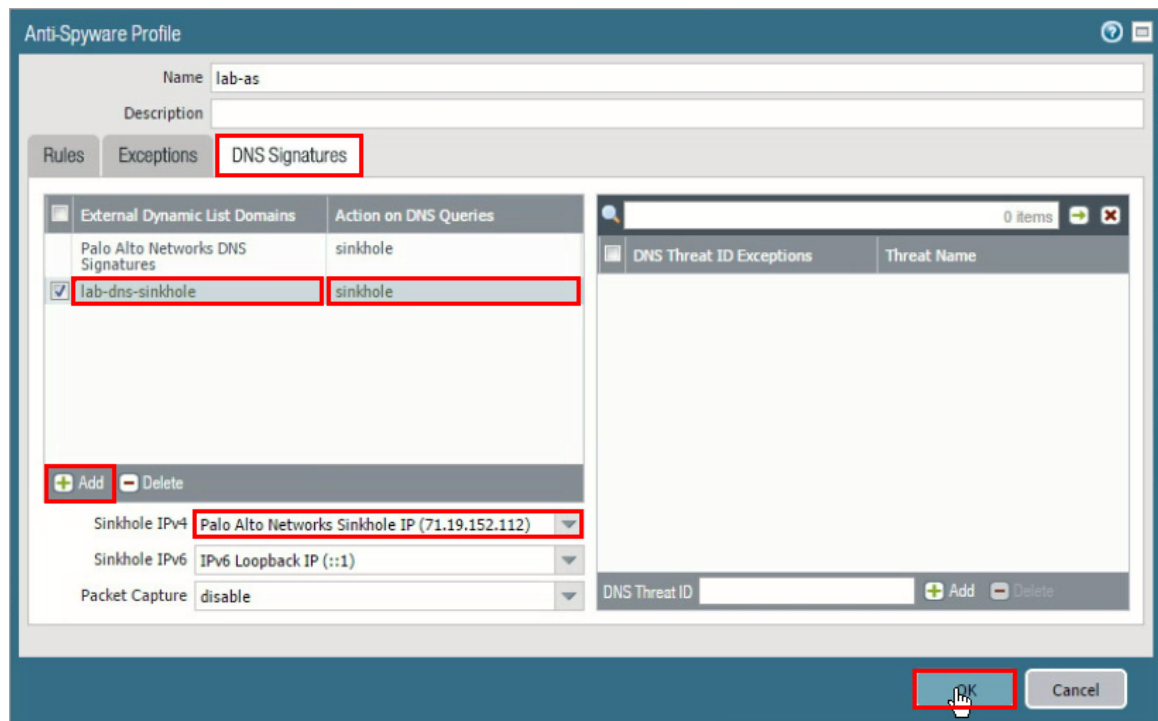
### 5.1.7 Anti-Spyware Profile with DNS Sinkhole

The DNS sinkhole action provides administrators with a method of identifying infected hosts on the network using DNS traffic, even when the firewall is north of a local DNS server (i.e., the firewall cannot see the originator of the DNS query).

1. Select **Objects > Security Profiles > Anti-Spyware** then click the Anti-Spyware Profile named **lab-as**.



2. Click the **DNS Signatures** tab then click **Add** and select **lab-dns-sinkhole**.



3. Set the **Action on DNS Queries** to **sinkhole**:
4. Verify that the **Sinkhole IPv4** is set to 71.19.152.112.
5. Click **OK** to close the Anti-Spyware Profile configuration window.
6. **Commit** all changes.

### 5.1.8 Test Security Policy Rule

1. From the Windows desktop, open a command-prompt window.
2. Type the `nslookup` command and press the **Enter** key.
3. Type the command `server 8.8.8.8` and press the **Enter** key:
4. At the `nslookup` command prompt, type `reddit.com` and press the **Enter** key:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup
Default Server: localhost
Address: 127.0.0.1

> server 8.8.8.8
Default server: google-public-dns-a.google.com
Address: 8.8.8.8

> reddit.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: reddit.com
Addresses: ::1
          71.19.152.112

>
```


Notice that the reply for reddit.com is 71.19.152.112. The request has been sinkholed.

### 5.1.9 Review the Logs

1. Select **Monitor > Logs > Threat**.

You may need to clear the log filter to view the entries that you are interested in.

2. Identify the **Suspicious Domain** log entry. Notice that the action is **sinkhole**. Note that you will not see an entry for this activity in the Traffic log because the Windows system did not try to initiate a connection to 71.19.152.112:

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim
	08/29 19:52:46	spyware	Suspicious Domain	inside	outside	192.168.1.20		8.8.8.8

**Stop.** This is the end of the 5.1 Content ID Malware/Virus Protection lab.