PALO ALTO NETWORKS EDU-210

Lab 5A: Content-ID

Document Version: 2019-11-12

Contents

Introduction 3
Objectives.. 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
1 Content-ID.. 6
1.0 Load Lab Configuration 6
1.1 Create Security Policy Rule with an Antivirus Profile.................................... 8
1.2 Test Security Policy Rule.. 12
1.3 Review Logs 13
1.4 Create Security Policy Rule with an Anti-Spyware Profile 15
1.5 Create a DMZ-Access Security Policy 21
1.6 Configure DNS-Sinkhole External Dynamic List... 24
1.7 Create an Anti-Spyware Profile with DNS Sinkhole 26
1.8 Test the Security Policy Rule 28
1.9 Review the Logs... 30

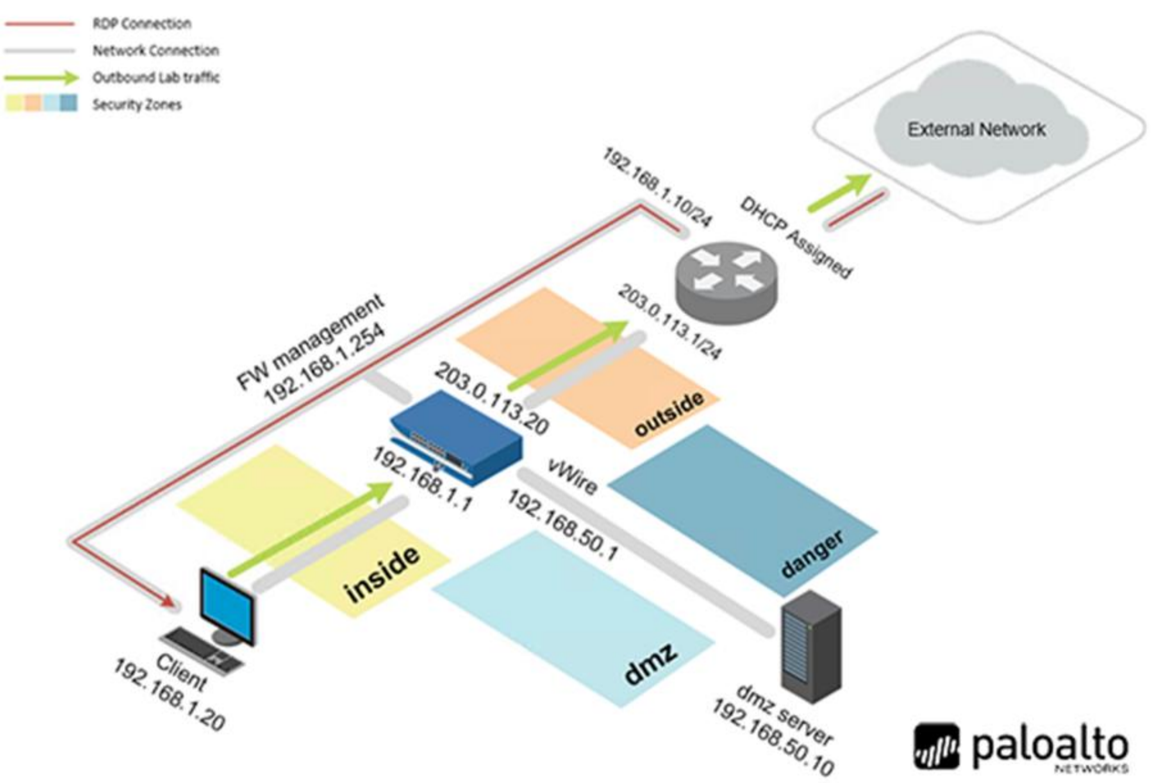
Introduction

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

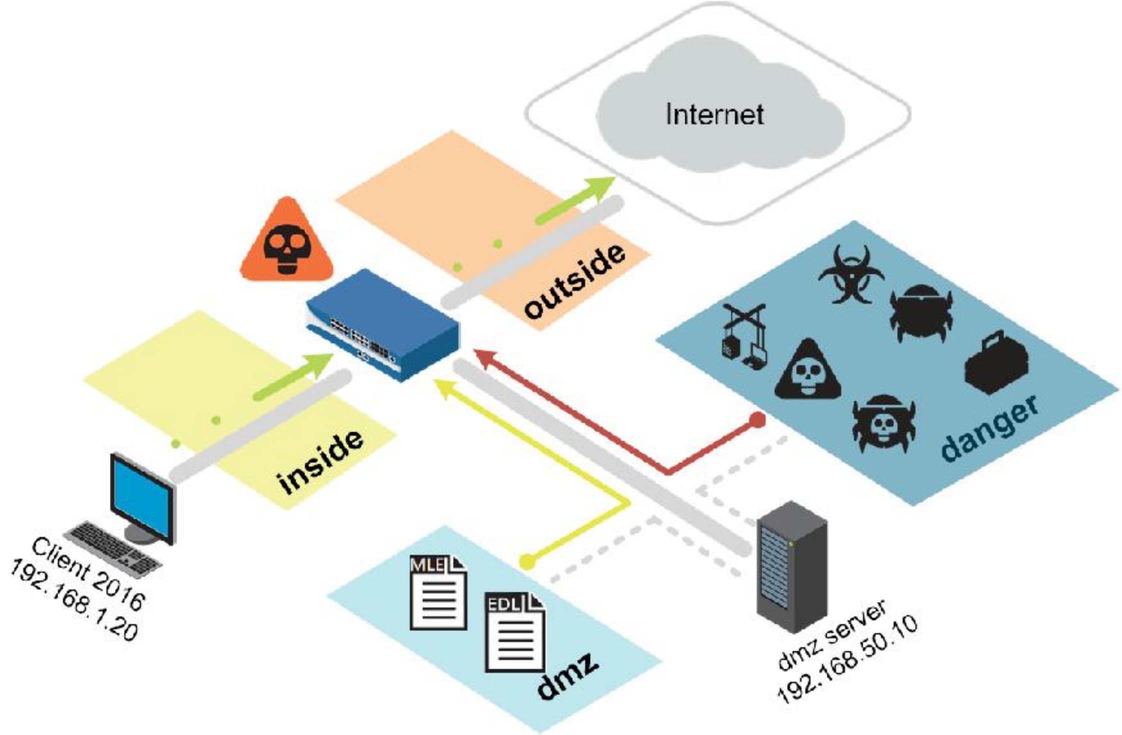
Objectives

- Configure and test an Antivirus Security Profile
- Configure and test an Anti-Spyware Security Profile
- Configure and test the DNS Sinkhole feature with an External Dynamic List

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`**	**`Pal0Alt0`**
Firewall	192.168.1.254	**`admin`**	**`admin`**

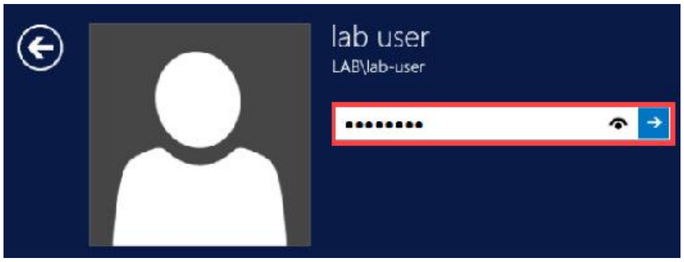
1 Content-ID

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.

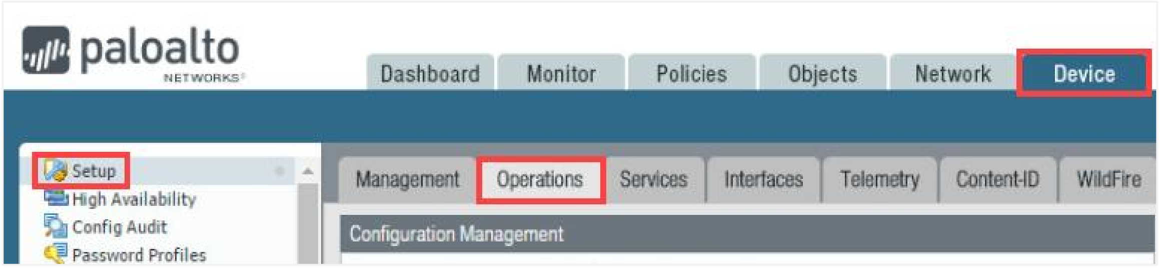
2. Click within the splash screen to bring up the login screen. Log in as **`lab-user`** using the password **`Pal0Alt0`**.



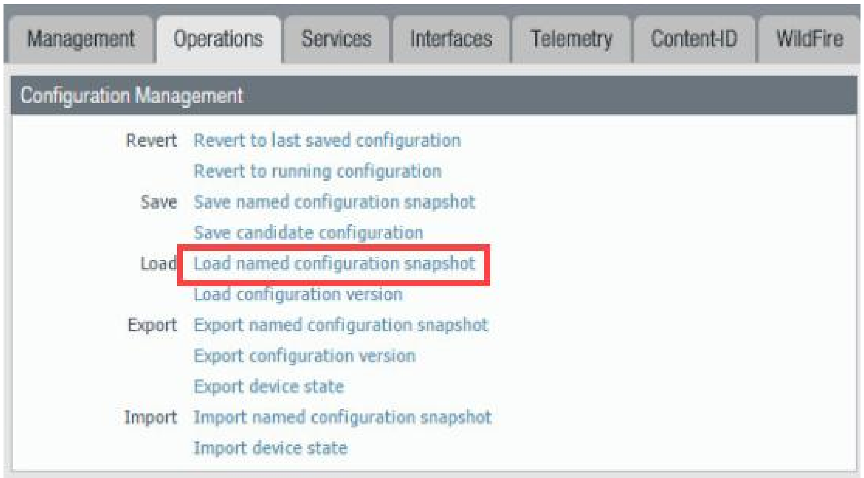
3. Launch the **Chrome** browser and connect to **`https://192.168.1.254.`**
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	**`admin`**
Password	**`admin`**

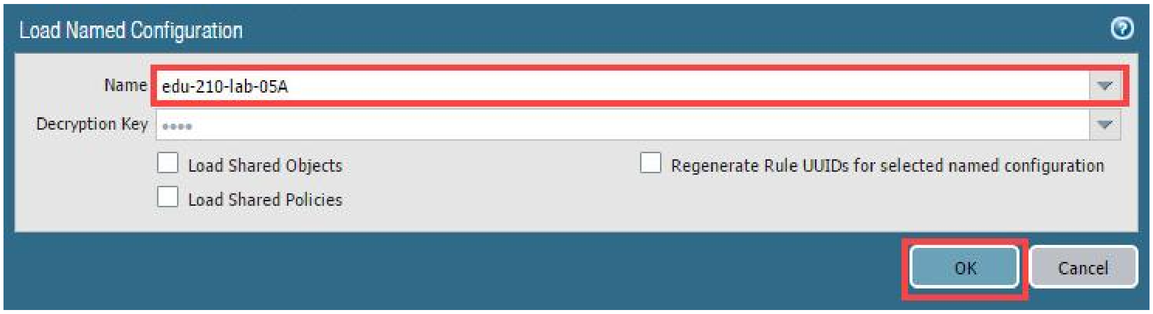
6. In the web interface, navigate to **Device > Setup > Operations**.



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


Management
Operations
Services
Interfaces
Telemetry
Content-ID
WildFire
Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-05A**. Click **OK**.


Load Named Configuration

Name: edu-210-lab-05A

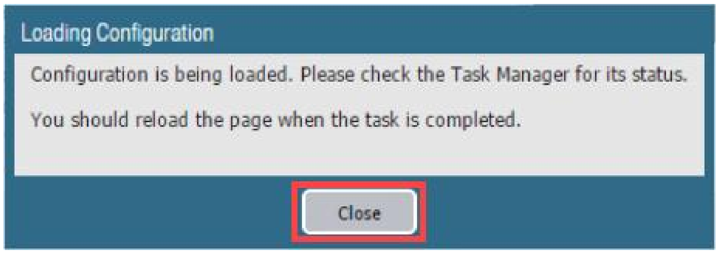
Decryption Key: ••••

□ Load Shared Objects

□ Regenerate Rule UUIDs for selected named configuration

□ Load Shared Policies

9. Click **Close**.

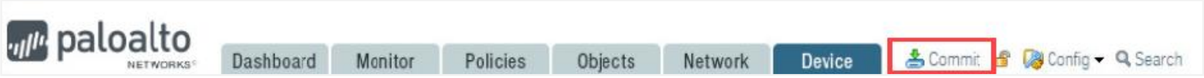

Loading Configuration

Configuration is being loaded. Please check the Task Manager for its status.

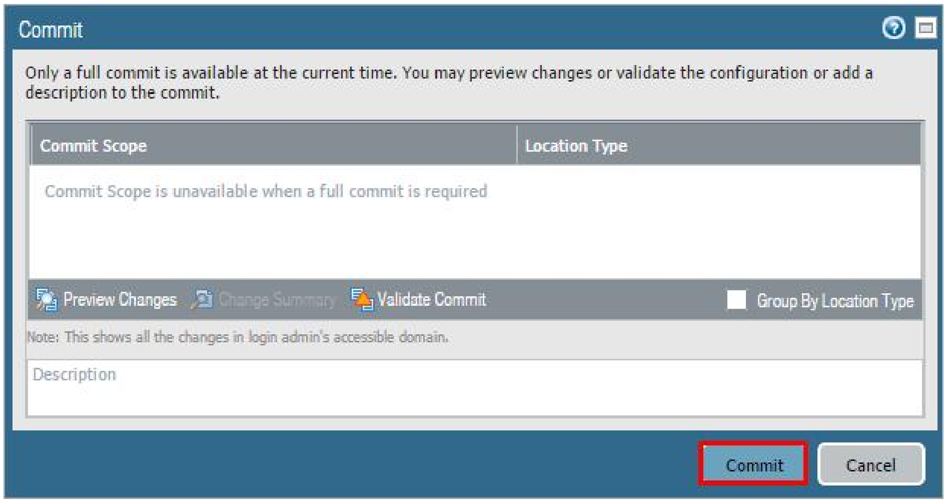
You should reload the page when the task is completed.

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.



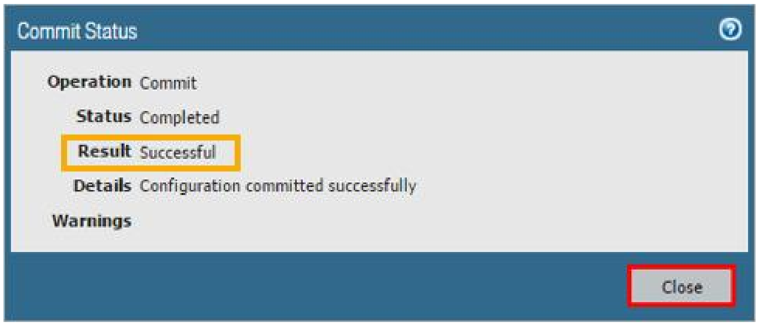
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

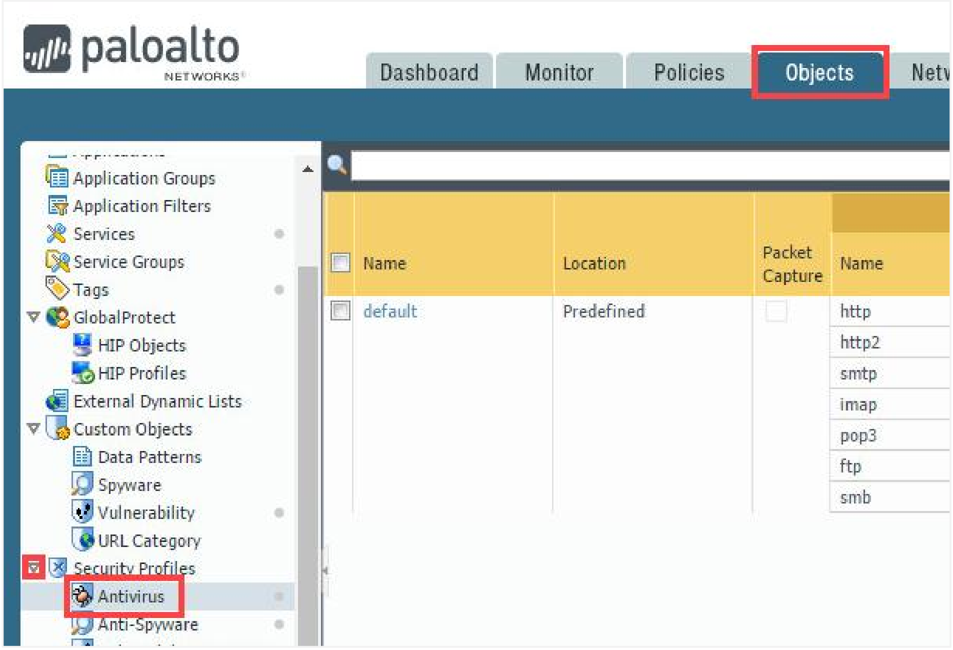
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

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

1.1 Create Security Policy Rule with an Antivirus Profile

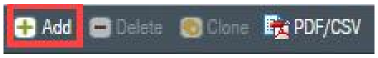
Use an *Antivirus Profile* object to configure options to have the firewall scan for viruses on traffic matching a Security Policy Rule. Set the applications that should be inspected for viruses and the action to take when a virus is detected.

1. In the web interface, select **Objects > Security Profiles > Antivirus.**



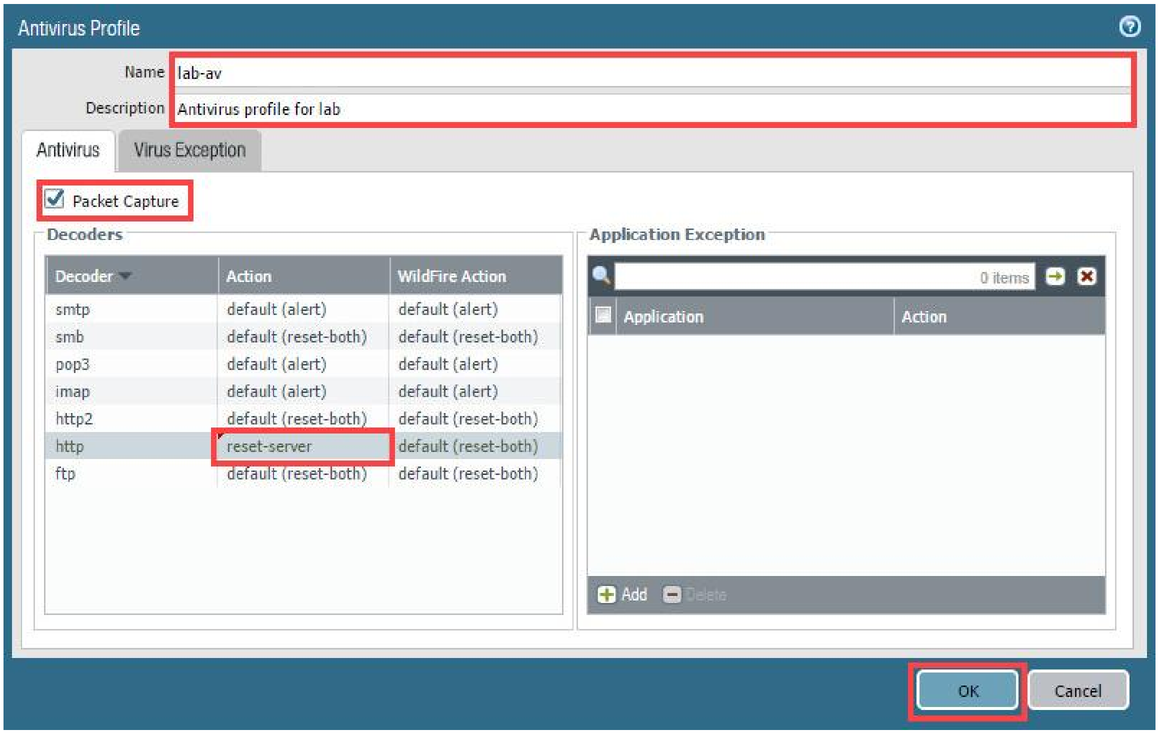
☐ Name	Location	Packet Capture	Name
☐ default	Predefined	☐	http
			http2
			smtp
			imap
			pop3
			ftp
			smb

2. Click **Add** to create an Antivirus Profile.



3. In the *Antivirus Profile* window, configure the following and then click **OK**.

Parameter	Value
Name	`lab-av`
Description	Type **`Antivirus profile for lab`**
Packet Capture	Select **Packet Capture** checkbox
Decoder	Set the **Action** column for **http** to **reset-server**



Antivirus Profile

Name: lab-av

Description: Antivirus profile for lab

☑ Packet Capture

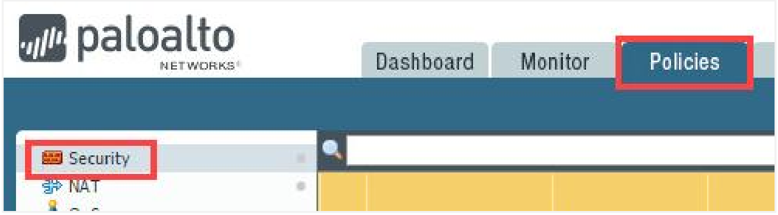
Decoders

Decoder	Action	WildFire Action
smtp	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)
pop3	default (alert)	default (alert)
imap	default (alert)	default (alert)
http2	default (reset-both)	default (reset-both)
http	reset-server	default (reset-both)
ftp	default (reset-both)	default (reset-both)

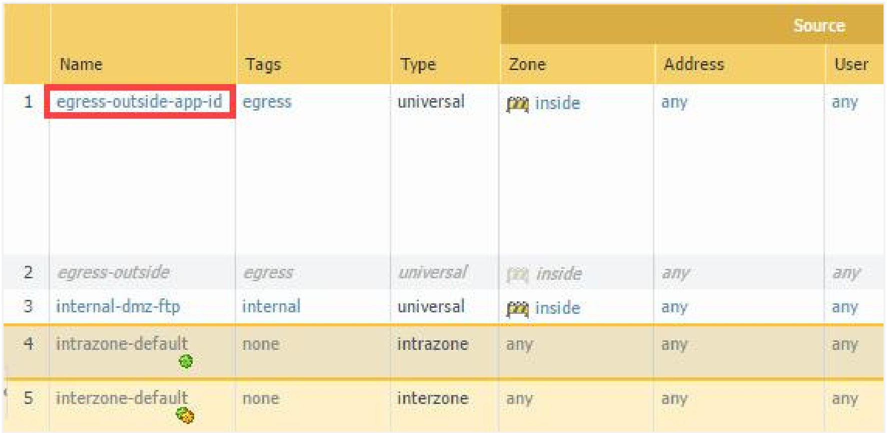
Application Exception

☐ Application	Action

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



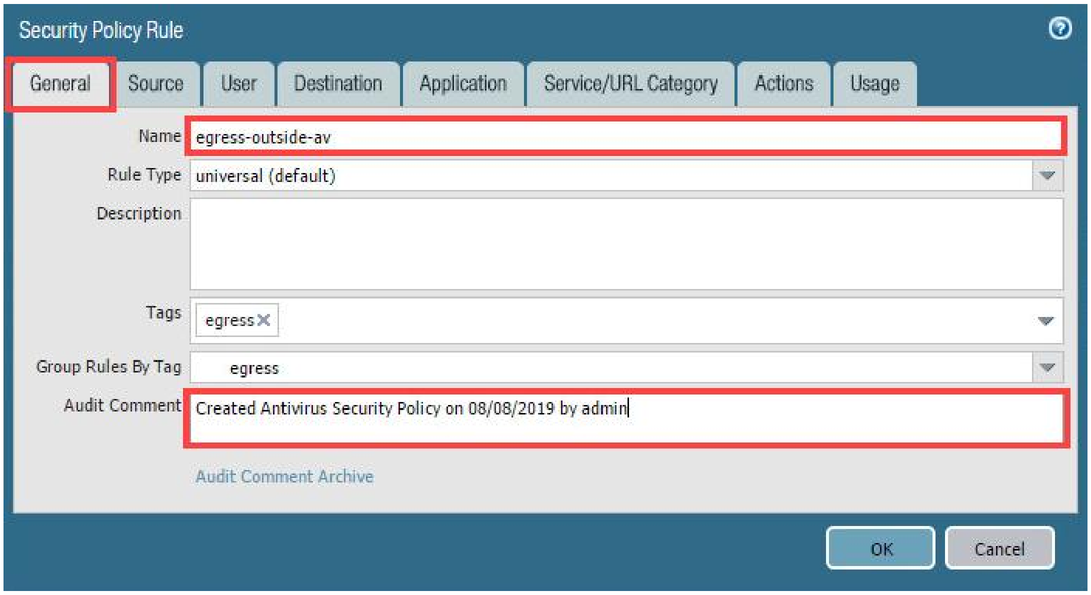
5. Select the **egress-outside-app-id** security policy rule.



				Source		
	Name	Tags	Type	Zone	Address	User
1	egress-outside-app-id	egress	universal	inside	any	any
2	egress-outside	egress	universal	inside	any	any
3	internal-dmz-ftp	internal	universal	inside	any	any
4	intrazone-default	none	intrazone	any	any	any
5	interzone-default	none	interzone	any	any	any

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

Parameter	Value
Name	Rename policy to **`egress-outside-av`**
Audit Comment	Type **`Created Antivirus Security Policy on <date> by admin`**



Name: egress-outside-av

Rule Type: universal (default)

Description:

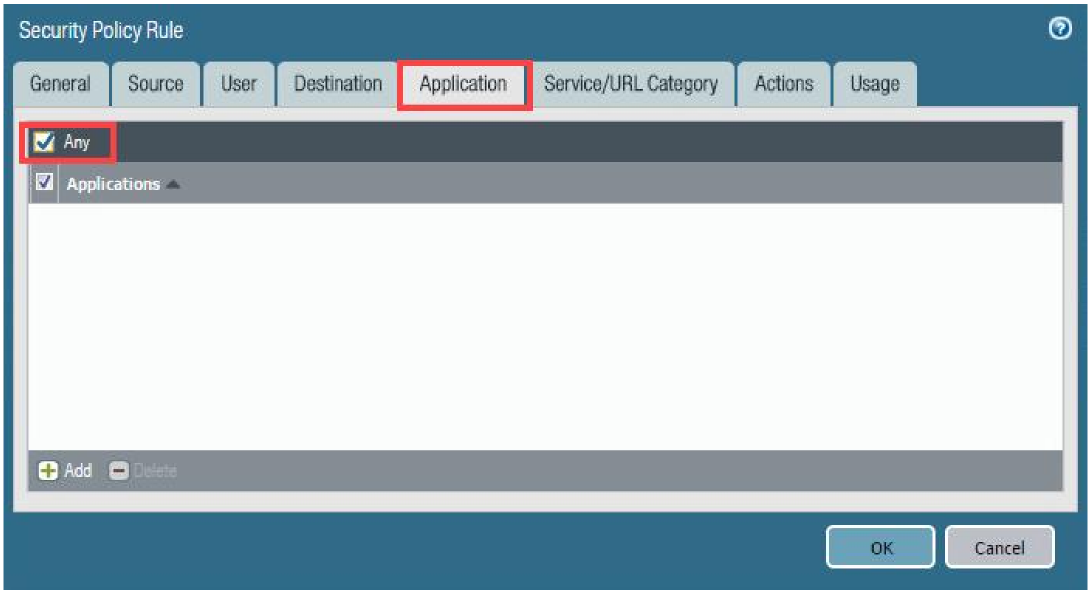
Tags: egress

Group Rules By Tag: egress

Audit Comment: Created Antivirus Security Policy on 08/08/2019 by admin

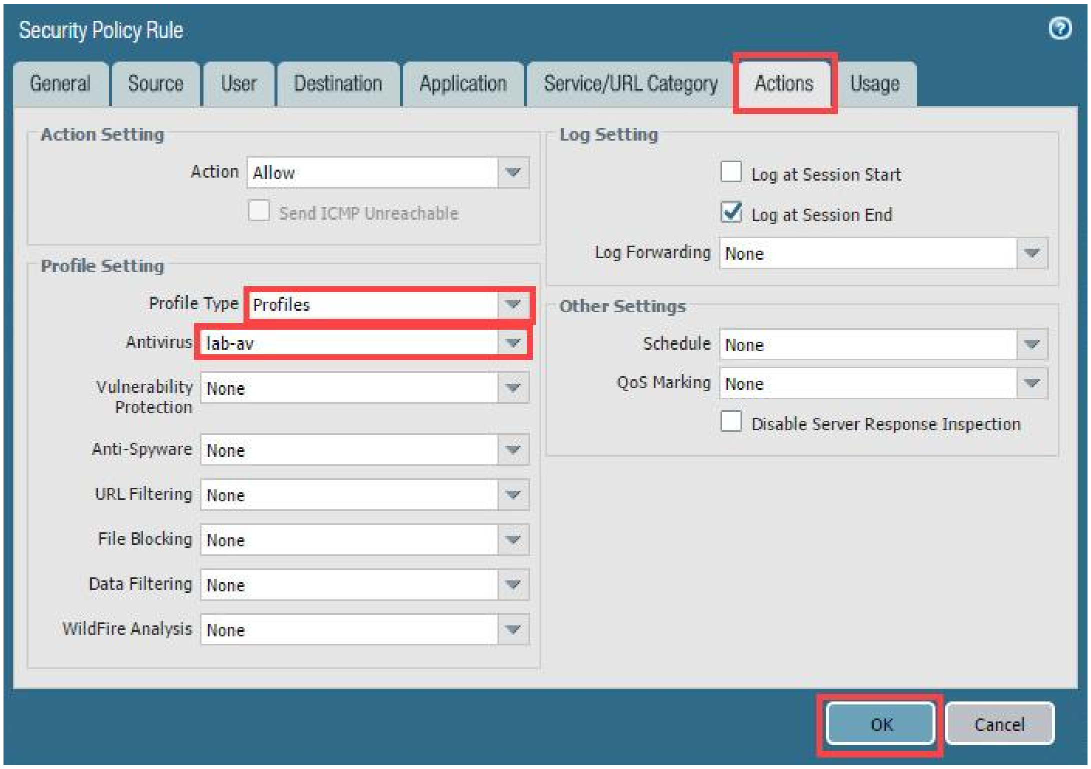
7. In the *Security Policy Rule* window, click the **Application** tab and configure the following:

Parameter	Value
Applications	Select the **Applications** checkbox and click **Delete**
Applications	Verify that the **Any** checkbox is selected



8. In the *Security Policy Rule* window, click the **Actions** tab and configure the following. Once finished, click **OK**.

Parameter	Value
Profile Type	Select **Profiles** from the drown-down list
Antivirus	Select **lab-av** from the drop-down list



Action: Allow

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Type: Profiles

Antivirus: lab-av

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Schedule: None

QoS Marking: None

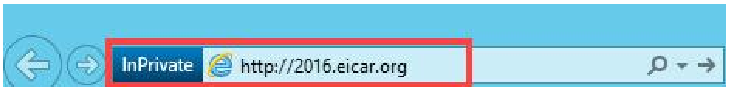
□ Disable Server Response Inspection

9. **Commit** all changes.

1.2 Test Security Policy Rule

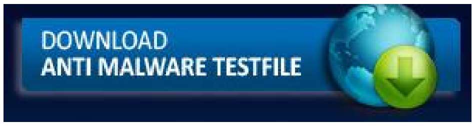
In this task, you will test your Antivirus Security Profile.

1. Open **Internet Explorer** in **private/incognito** mode and browse to `http://2016.eicar.org`.

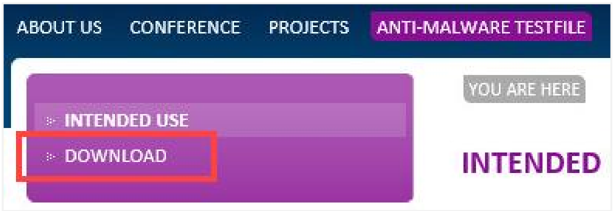


http://2016.eicar.org

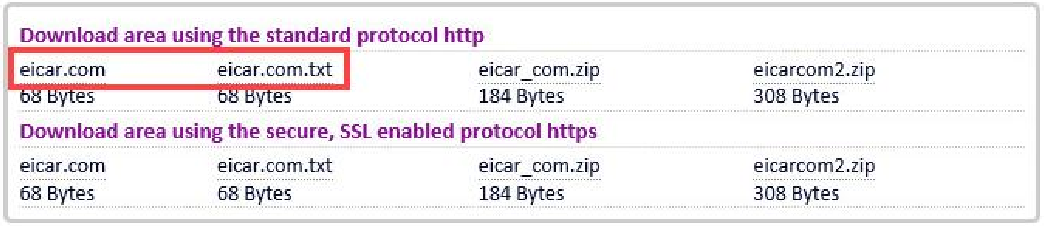
2. Click the **DOWNLOAD ANTIMALWARE TESTFILE** image in the top-right corner:



3. Click the **Download** link on the left of the web page:



4. Within the *Download area using the standard protocol http* 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.



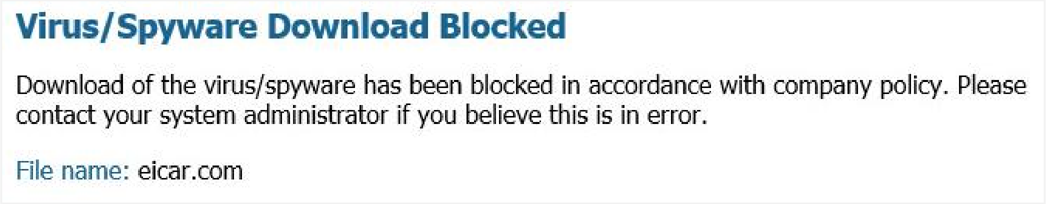
Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

5. Notice that a message appears, showing the file download was blocked. **Close** the browser window.



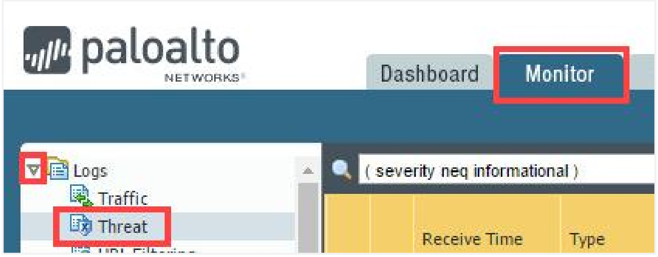
Virus/Spyware Download Blocked

Download of the virus/spyware has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

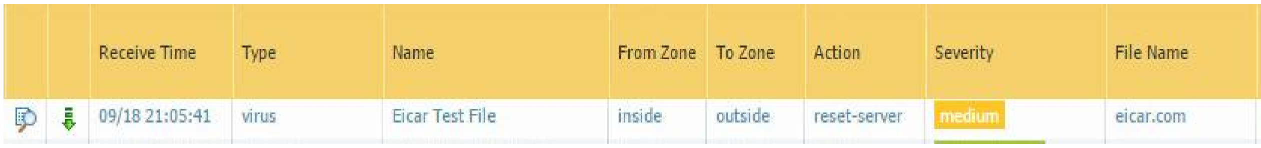
File name: eicar.com

1.3 Review Logs

1. In the web interface, select **Monitor > Logs > Threat**.

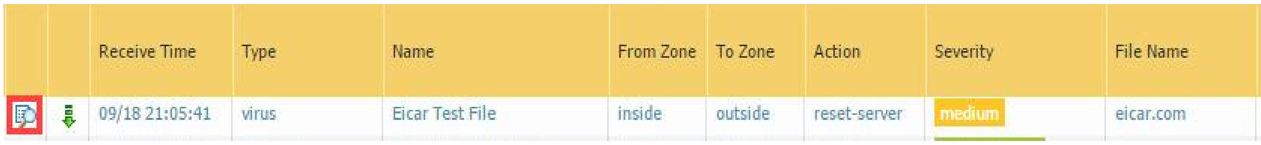


2. Make sure that the filter is cleared and find the log message that detected the **Eicar Test File**. Notice that the action for the file is *reset-server*.



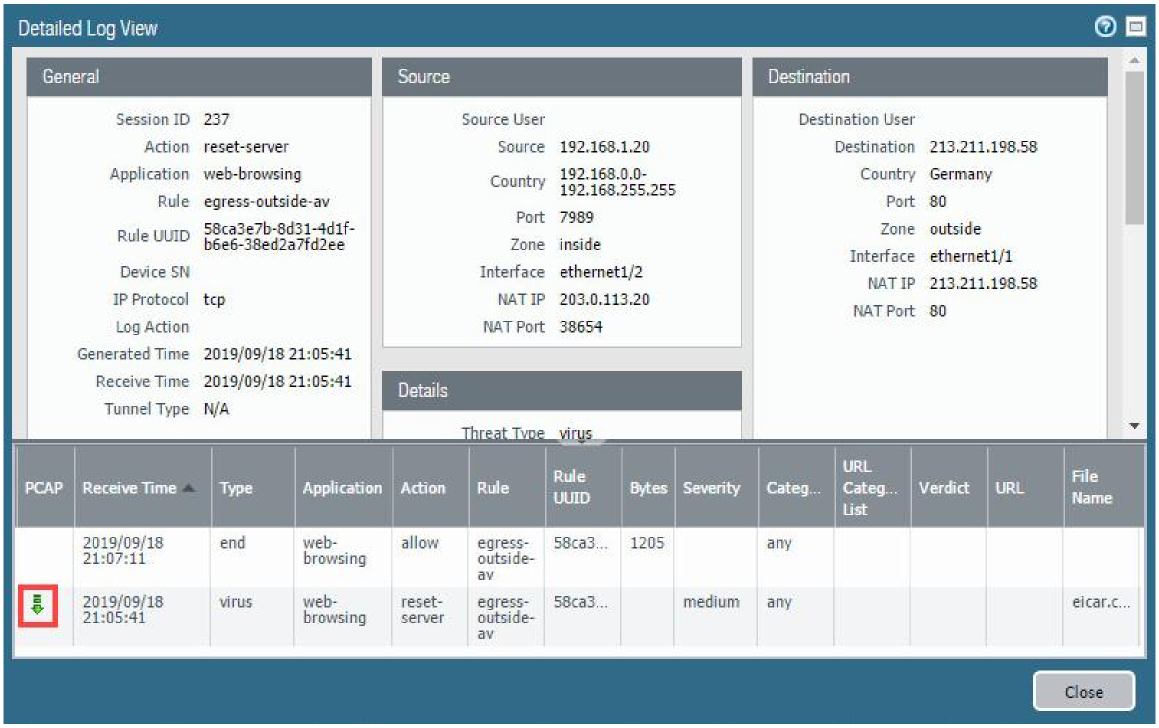
		Receive Time	Type	Name	From Zone	To Zone	Action	Severity	File Name
		09/18 21:05:41	virus	Eicar Test File	inside	outside	reset-server	medium	eicar.com

3. Notice the download icon on the left side of the entry for the *Eicar Test File*. It indicates that there is a packet capture (*pcap*). To display the packet capture through the *Detailed Log View*, first, click the **Detailed Log View icon** to open the *Detailed Log View* of the threat entry.



		Receive Time	Type	Name	From Zone	To Zone	Action	Severity	File Name
		09/18 21:05:41	virus	Eicar Test File	inside	outside	reset-server	medium	eicar.com

4. From the *Detailed Log View* window, click the **download icon** underneath the *PCAP* column to open the packet capture.



Detailed Log View

General

Session ID	237
Action	reset-server
Application	web-browsing
Rule	egress-outside-av
Rule UUID	58ca3e7b-8d31-4d1f-b6e6-38ed2a7fd2ee
Device SN	
IP Protocol	tcp
Log Action	
Generated Time	2019/09/18 21:05:41
Receive Time	2019/09/18 21:05:41
Tunnel Type	N/A

Source

Source User	
Source	192.168.1.20
Country	192.168.0.0-192.168.255.255
Port	7989
Zone	inside
Interface	ethernet1/2
NAT IP	203.0.113.20
NAT Port	38654

Details

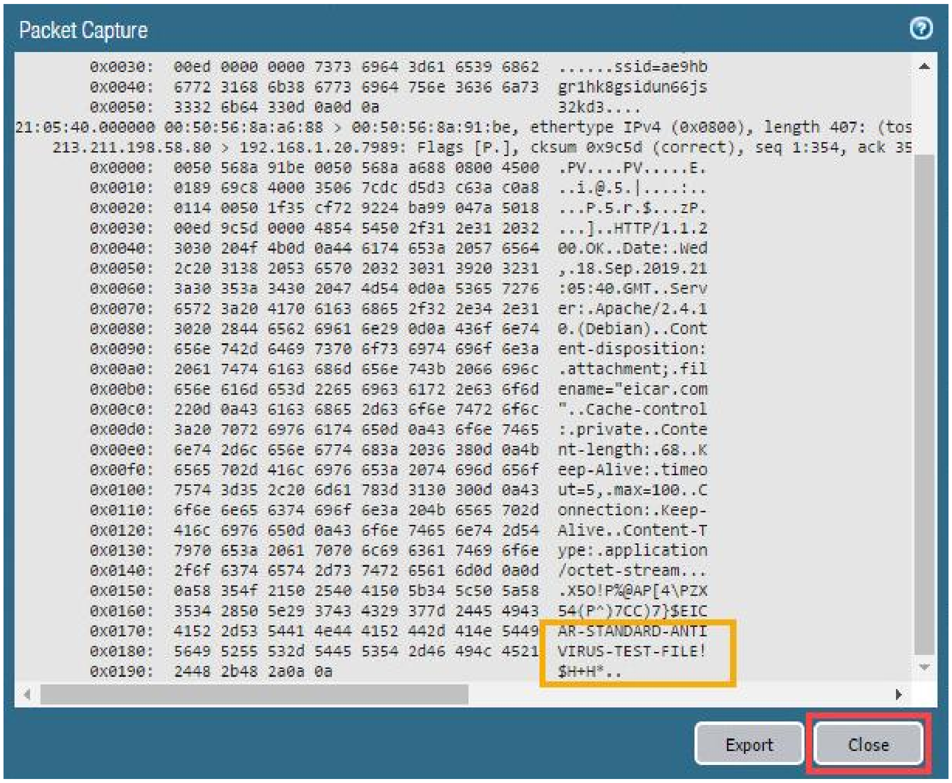
Threat Type	virus

Destination

Destination User	
Destination	213.211.198.58
Country	Germany
Port	80
Zone	outside
Interface	ethernet1/1
NAT IP	213.211.198.58
NAT Port	80

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/09/18 21:07:11	end	web-browsing	allow	egress-outside-av	58ca3...	1205		any				
	2019/09/18 21:05:41	virus	web-browsing	reset-server	egress-outside-av	58ca3...		medium	any				eicar.c...

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



```
        0x0030:  00ed 0000 0000 7373 6964 3d61 6539 6862  ......ssid=ae9hb
        0x0040:  6772 3168 6b38 6773 6964 756e 3636 6a73  gr1hk8gsidun66js
        0x0050:  3332 6b64 330d 0a0d 0a                   32kd3....
21:05:40.000000 00:50:56:8a:a6:88 > 00:50:56:8a:91:be, ethertype IPv4 (0x0800), length 407: (tos
    213.211.198.58.80 > 192.168.1.20.7989: Flags [P.], cksum 0x9c5d (correct), seq 1:354, ack 35
        0x0000:  0050 568a 91be 0050 568a a688 0800 4500  .PV....PV.....E.
        0x0010:  0189 69c8 4000 3506 7cdc d5d3 c63a c0a8  ..i.@.5.|....:..
        0x0020:  0114 0050 1f35 cf72 9224 ba99 047a 5018  ...P.5.r.$...zP.
        0x0030:  00ed 9c5d 0000 4854 5450 2f31 2e31 2032  ...]..HTTP/1.1.2
        0x0040:  3030 204f 4b0d 0a44 6174 653a 2057 6564  00.OK..Date:.Wed
        0x0050:  2c20 3138 2053 6570 2032 3031 3920 3231  ,.18.Sep.2019.21
        0x0060:  3a30 353a 3430 2047 4d54 0d0a 5365 7276  :05:40.GMT..Serv
        0x0070:  6572 3a20 4170 6163 6865 2f32 2e34 2e31  er:.Apache/2.4.1
        0x0080:  3020 2844 6562 6961 6e29 0d0a 436f 6e74  0.(Debian)..Cont
        0x0090:  656e 742d 6469 7370 6f73 6974 696f 6e3a  ent-disposition:
        0x00a0:  2061 7474 6163 686d 656e 743b 2066 696c  .attachment;.fil
        0x00b0:  656e 616d 653d 2265 6963 6172 2e63 6f6d  ename="eicar.com
        0x00c0:  220d 0a43 6163 6865 2d63 6f6e 7472 6f6c  "..Cache-control
        0x00d0:  3a20 7072 6976 6174 650d 0a43 6f6e 7465  :.private..Conte
        0x00e0:  6e74 2d6c 656e 6774 683a 2036 380d 0a4b  nt-length:.68..K
        0x00f0:  6565 702d 416c 6976 653a 2074 696d 656f  eep-Alive:.timeo
        0x0100:  7574 3d35 2c20 6d61 783d 3130 300d 0a43  ut=5,.max=100..C
        0x0110:  6f6e 6e65 6374 696f 6e3a 204b 6565 702d  onnection:.Keep-
        0x0120:  416c 6976 650d 0a43 6f6e 7465 6e74 2d54  Alive..Content-T
        0x0130:  7970 653a 2061 7070 6c69 6361 7469 6f6e  ype:.application
        0x0140:  2f6f 6374 6574 2d73 7472 6561 6d0d 0a0d  /octet-stream...
        0x0150:  0a58 354f 2150 2540 4150 5b34 5c50 5a58  .X5O!P%@AP[4\PZX
        0x0160:  3534 2850 5e29 3743 4329 377d 2445 4943  54(P^)7CC)7}$EIC
        0x0170:  4152 2d53 5441 4e44 4152 442d 414e 5449  AR-STANDARD-ANTI
        0x0180:  5649 5255 532d 5445 5354 2d46 494c 4521  VIRUS-TEST-FILE!
        0x0190:  2448 2b48 2a0a 0a                        $H+H*..
```

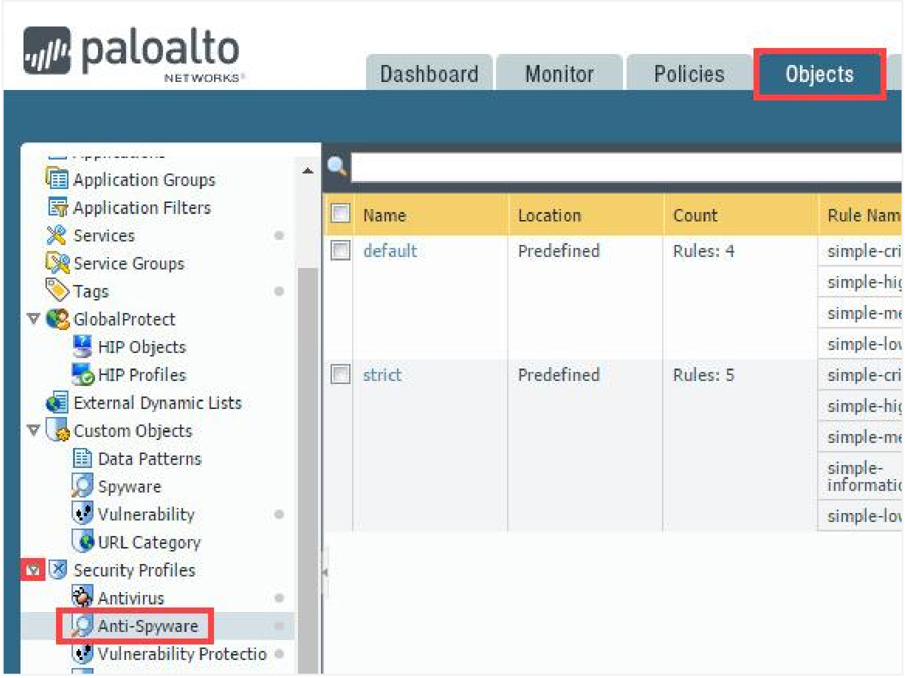
Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

6. Back on the *Detailed Log View* window, click **Close**.
7. Leave the firewall web interface open to continue with the next task.

1.4 Create Security Policy Rule with an Anti-Spyware Profile

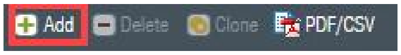
Anti-Spyware profiles block spyware on compromised hosts from trying to phone home or beacon out to external command-and-control (C2) servers, thus allowing you to detect malicious traffic, leaving the network from infected clients.

1. In the web interface, select **Objects > Security Profiles > Anti-Spyware**.



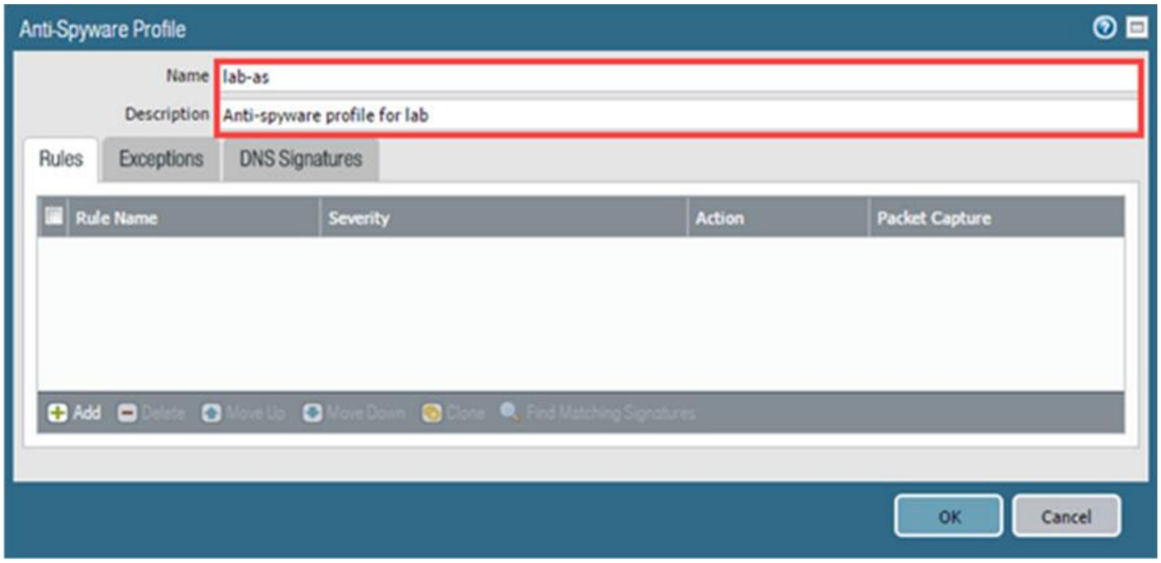
Name	Location	Count	Rule Nam
default	Predefined	Rules: 4	simple-cri simple-hi simple-me simple-lov
strict	Predefined	Rules: 5	simple-cri simple-hi simple-me simple-informati simple-lov

2. Click **Add** to create an Anti-Spyware Profile.



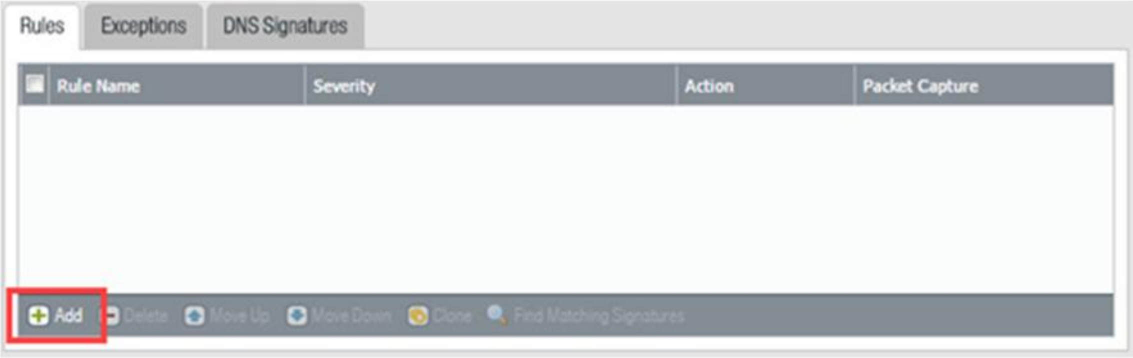
3. In the *Anti-Spyware Profile* window, configure the following.

Parameter	Value
Name	`lab-as`
Description	`Anti-spyware profile for lab`



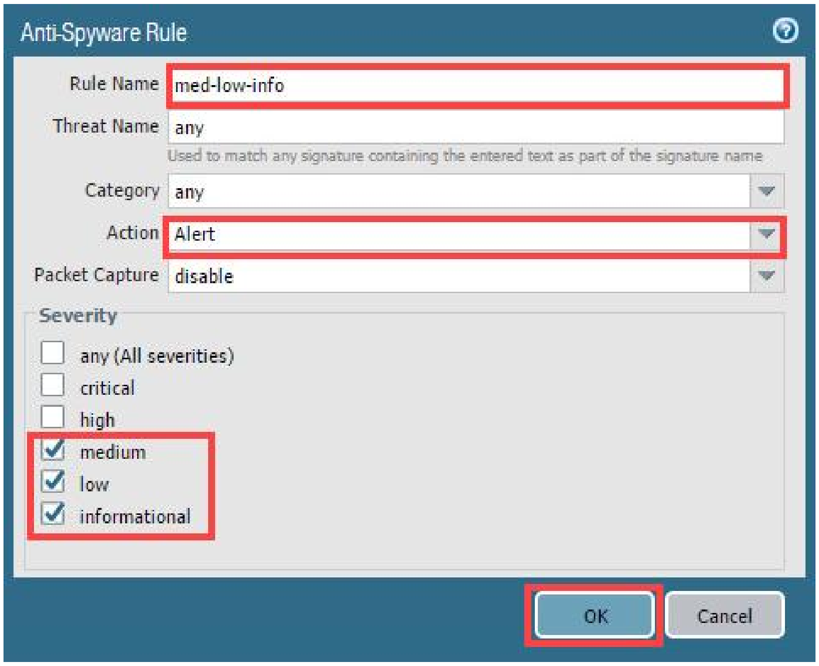
Name: lab-as
Description: Anti-spyware profile for lab

4. In the *Anti-Spyware Rule* window, click the **Add** button while on the *Rules* tab.



5. In the *Anti-Spyware Rule* window, configure the following and then click **OK**.

Parameter	Value
Rule Name	`med-low-info`
Action	**Alert**
Severity	**medium** **low** **informational**


Anti-Spyware Rule

Rule Name: med-low-info

Threat Name: any

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

Category: any

Action: Alert

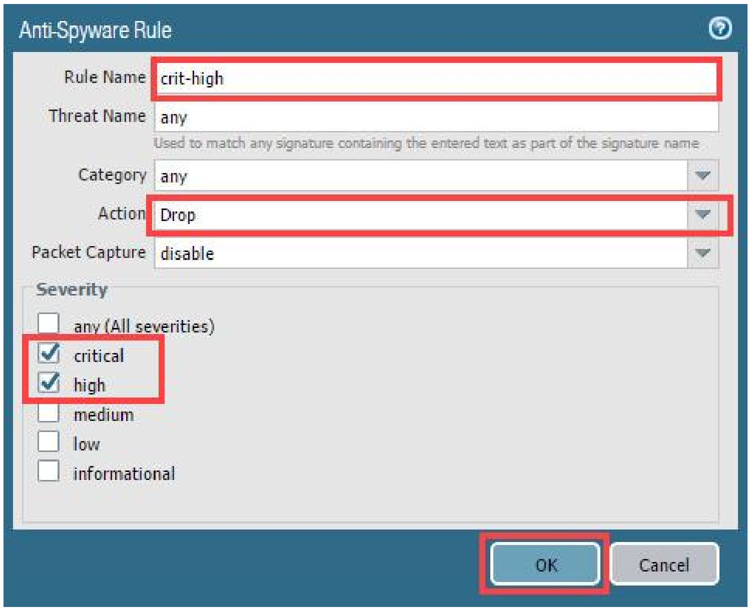
Packet Capture: disable

Severity

☐ any (All severities)
☐ critical
☐ high
☑ medium
☑ low
☑ informational

6. Back on the *Anti-Spyware Profile* window, click **Add** once more to create a new *Anti-Spyware Rule***,** then fill in the following data and click **OK**.

Parameter	Value
Rule Name	**`crit-high`**
Action	**Drop**
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

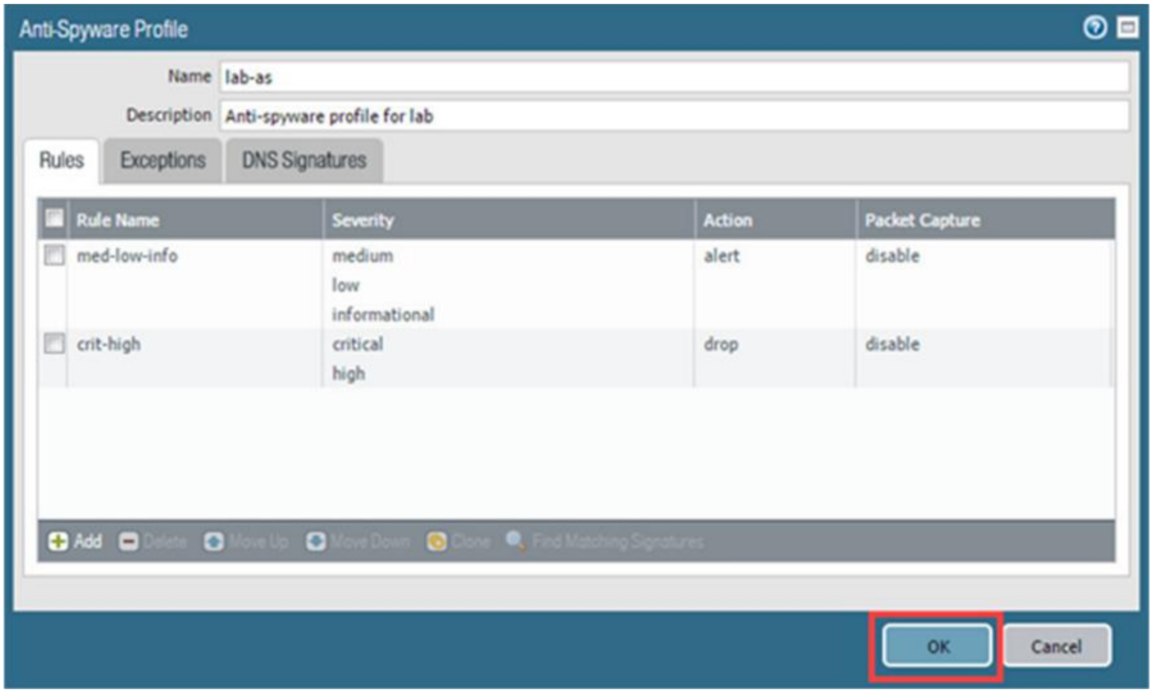
Action: Drop

Packet Capture: disable

Severity

- □ any (All severities)
- ☑ critical
- ☑ high
- □ medium
- □ low
- □ informational

7. Back on the *Anti-Spyware Profile* window, click **OK**.



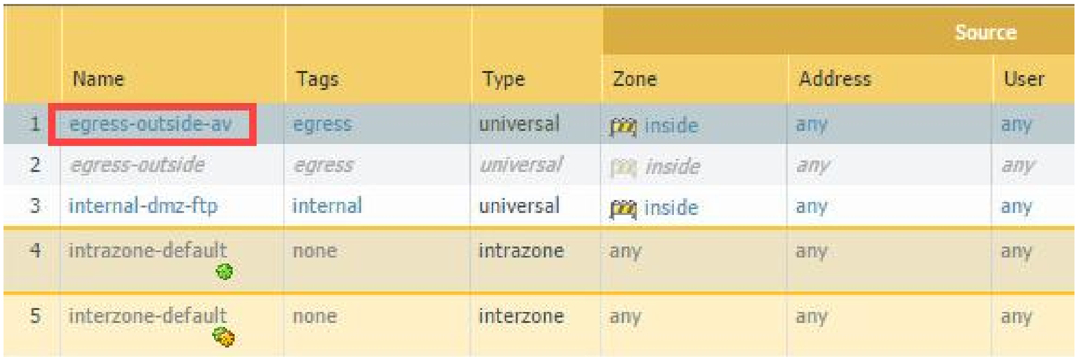
Anti-Spyware Profile

Name: lab-as

Description: Anti-spyware profile for lab

Rule Name	Severity	Action	Packet Capture
med-low-info	medium low informational	alert	disable
crit-high	critical high	drop	disable

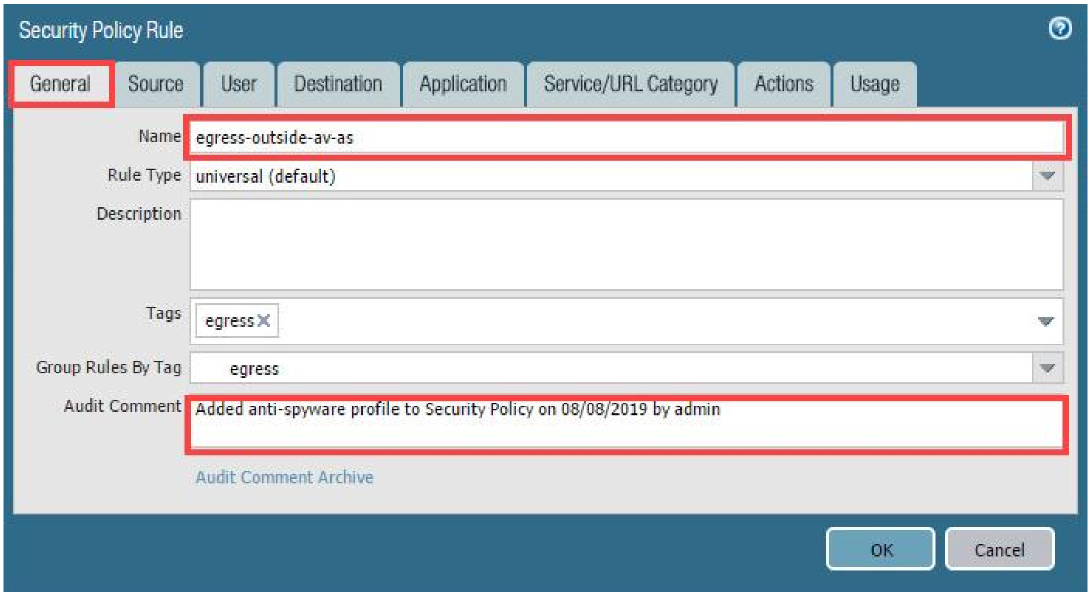
8. In the web interface, select **Policies > Security**.
9. Select the **egress-outside-av** Security policy rule.



				Source		
	Name	Tags	Type	Zone	Address	User
1	egress-outside-av	egress	universal	inside	any	any
2	*egress-outside*	*egress*	*universal*	*inside*	*any*	*any*
3	internal-dmz-ftp	internal	universal	inside	any	any
4	intrazone-default	none	intrazone	any	any	any
5	interzone-default	none	interzone	any	any	any

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

Parameter	Value
Name	Rename policy to `egress-outside-av-as`
Audit Comment	Type **`Added anti-spyware profile to Security Policy on <date> by admin`**



Name: egress-outside-av-as

Rule Type: universal (default)

Description:

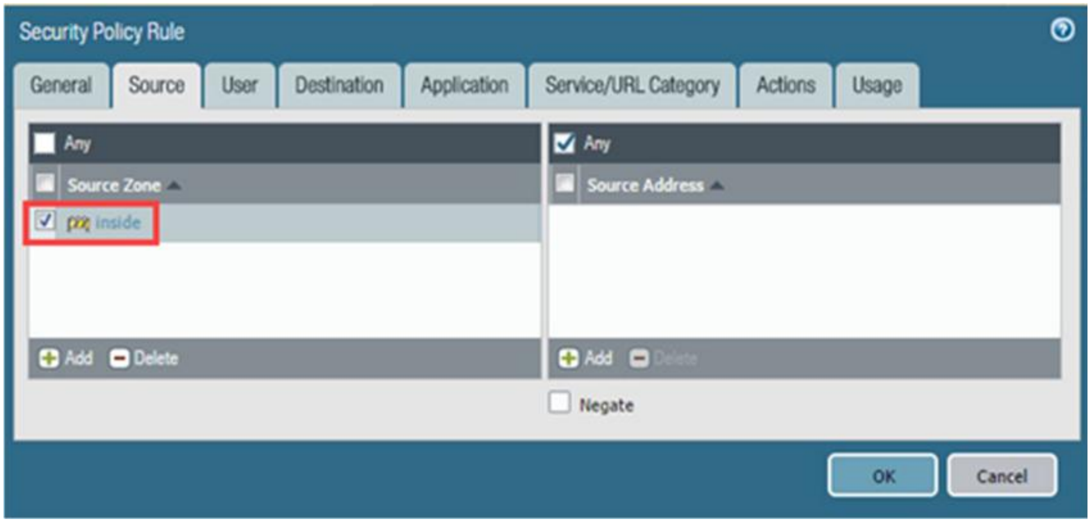
Tags: egress

Group Rules By Tag: egress

Audit Comment: Added anti-spyware profile to Security Policy on 08/08/2019 by admin

11. Click the **Source** tab and verify the following.

Parameter	Value
Source Zone	Verify that **inside** checkbox is selected



□ Any

Source Zone

☑ inside

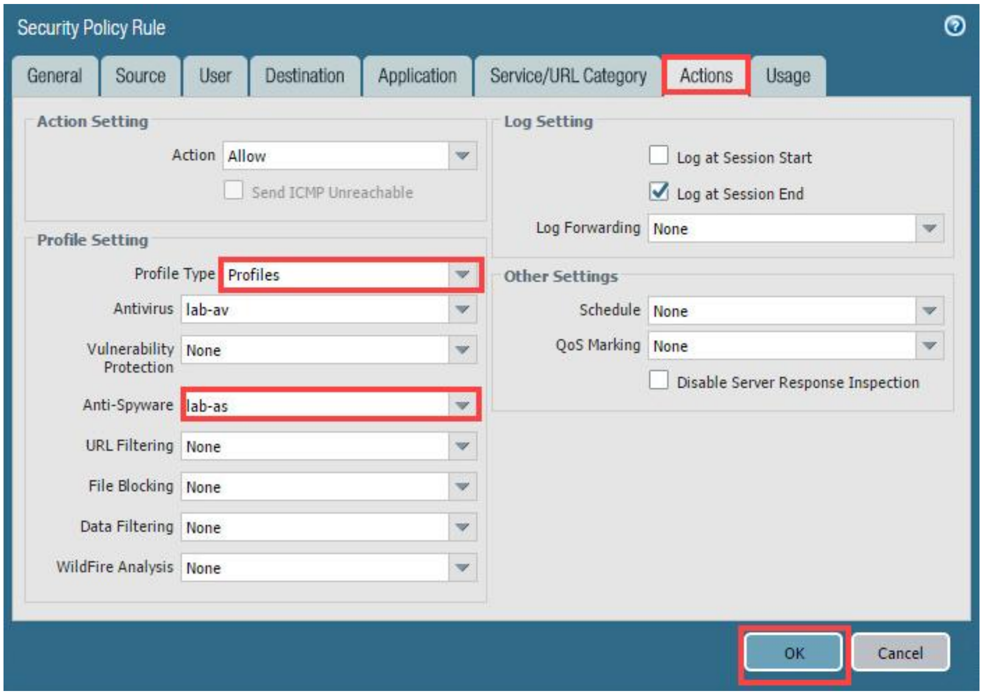
☑ Any

Source Address

□ Negate

12. In the *Security Policy Rule* window, click the **Actions** tab, configure the following and then click **OK**.

Parameter	Value
Profile Type	Verify that **Profiles** is selected
Anti-Spyware	Select **lab-as**



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: lab-av

Vulnerability Protection: None

Anti-Spyware: lab-as

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

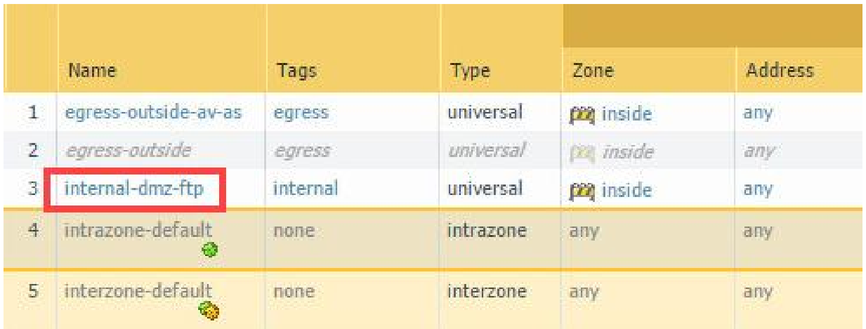
□ Disable Server Response Inspection

13. Click **OK** to close the *Security Policy Rule* configuration window.
14. Leave the firewall web interface open to continue with the next task.

1.5 Create a DMZ-Access Security Policy

In the next task, you will configure the firewall to download an *External Dynamic List* (EDL) of URLs from the DMZ server. You will then apply the EDL to the Anti-Spyware DNS Sinkhole configuration. Before the EDL and DNS Sinkhole configurations can work, you must create a security policy that allows the management interface to connect to the DMZ server. The management interface establishes connections from the *inside* zone. The DMZ server responds to connection requests from the *dmz* zone.

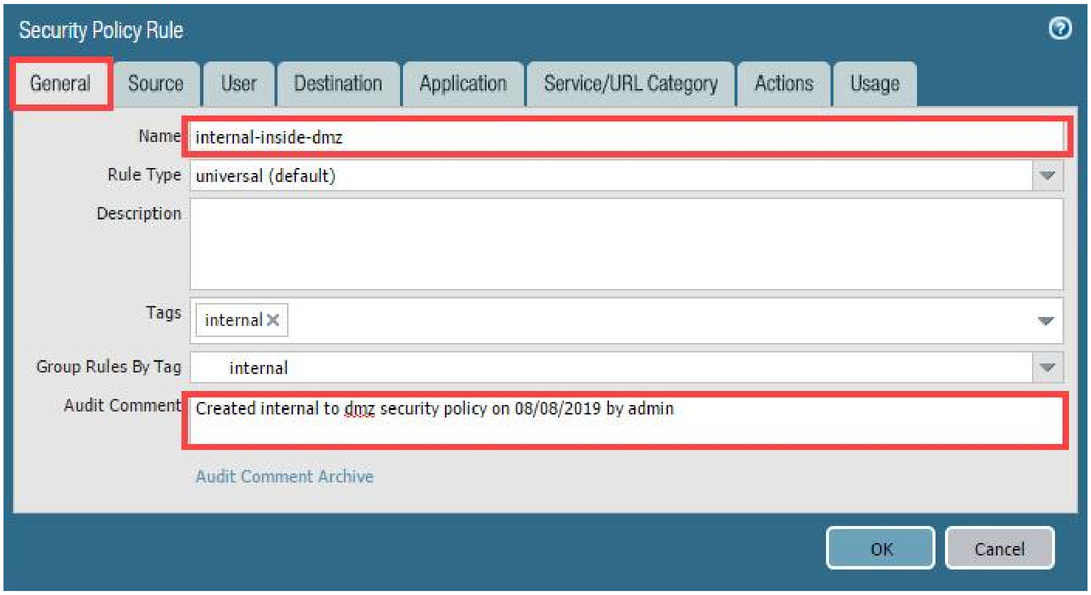
1. In the web interface, click on the **internal-dmz-ftp** Security policy rule.



	Name	Tags	Type	Zone	Address
1	egress-outside-av-as	egress	universal	inside	any
2	egress-outside	egress	universal	inside	any
3	internal-dmz-ftp	internal	universal	inside	any
4	intrazone-default	none	intrazone	any	any
5	interzone-default	none	interzone	any	any

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

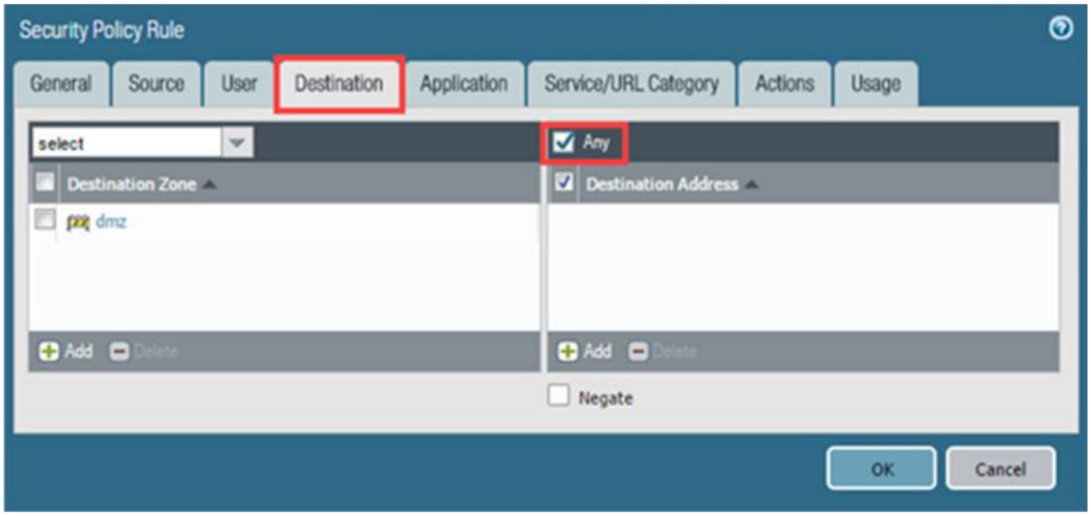
Parameter	**Value**
Name	Rename the policy to **`internal-inside-dmz`**
Audit Comment	Type **`Created internal to dmz security policy on <date> by admin`**



Name: internal-inside-dmz
Rule Type: universal (default)
Description:
Tags: internal ✕
Group Rules By Tag: internal
Audit Comment: Created internal to dmz security policy on 08/08/2019 by admin

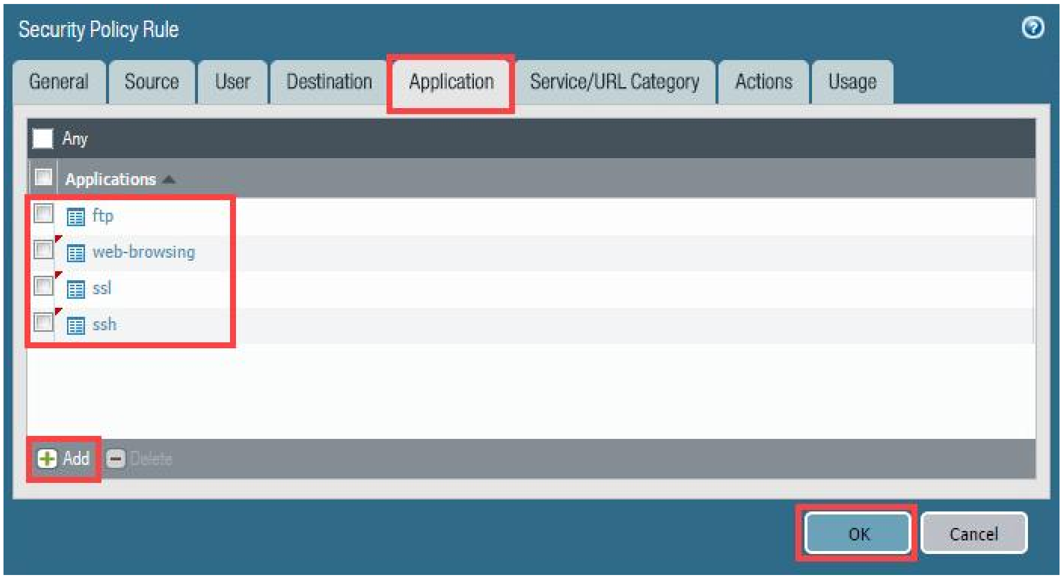
3. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

Parameter	Value
Destination Address	Select the **Destination Address** checkbox and click **Delete**
Destination Address	Verify that the **Any** checkbox is selected

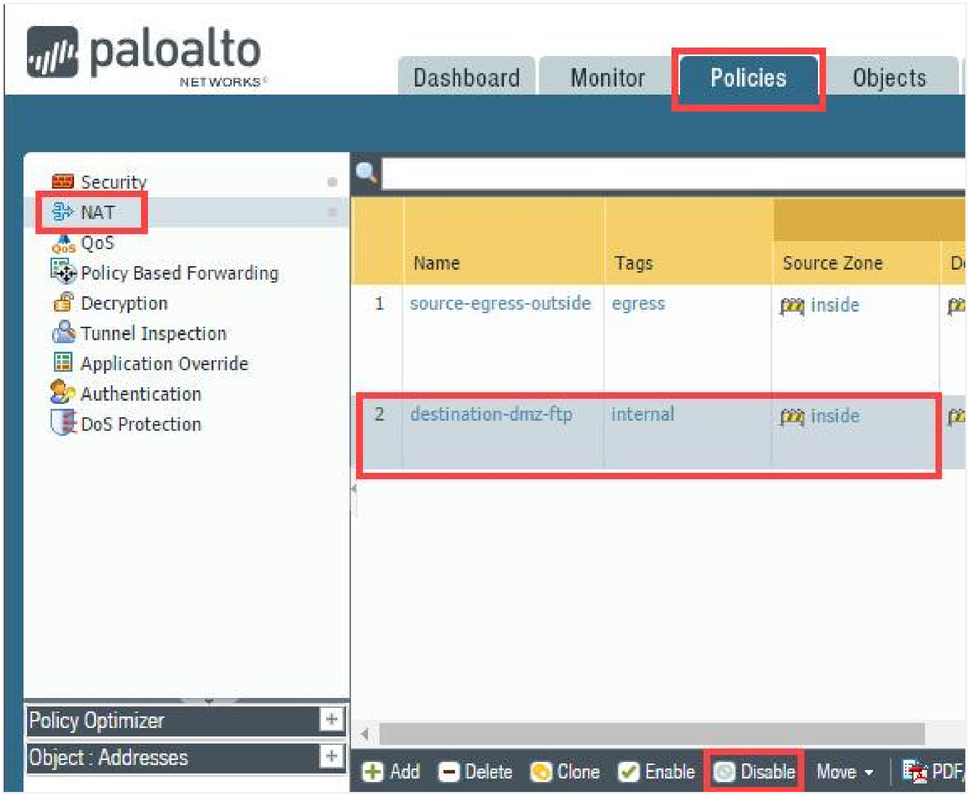


4. In the *Security Policy Rule* window, click the **Application** tab to configure the following and then click **OK**.

Parameter	Value
Applications	Click **Add** and select the following from the drop-down list: **ftp** **web-browsing** **ssl** **ssh**

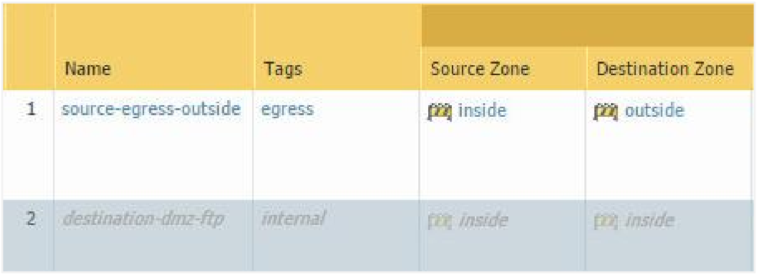


5. In the web interface, navigate to **Policies > NAT**, select the **destination-dmz-ftp** NAT policy rule without opening it, and click **Disable**.



	Name	Tags	Source Zone	D
1	source-egress-outside	egress	inside	
2	destination-dmz-ftp	internal	inside	

6. Verify that the rule is now disabled, with the entry being grayed out.



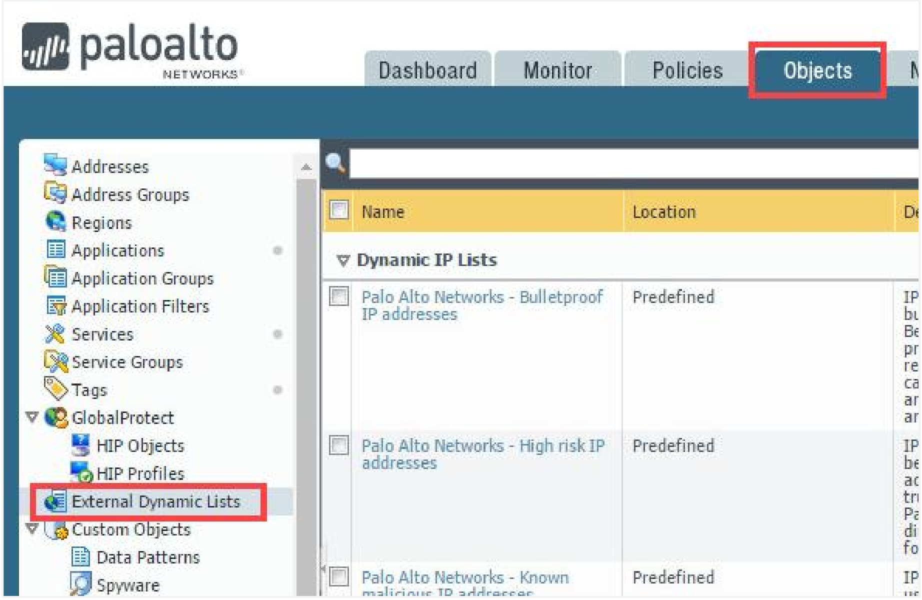
	Name	Tags	Source Zone	Destination Zone
1	source-egress-outside	egress	inside	outside
2	*destination-dmz-ftp*	*internal*	*inside*	*inside*

7. **Commit** all changes.
8. Leave the firewall web interface open to continue with the next task.

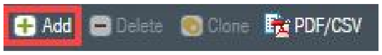
1.6 Configure DNS-Sinkhole External Dynamic List

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

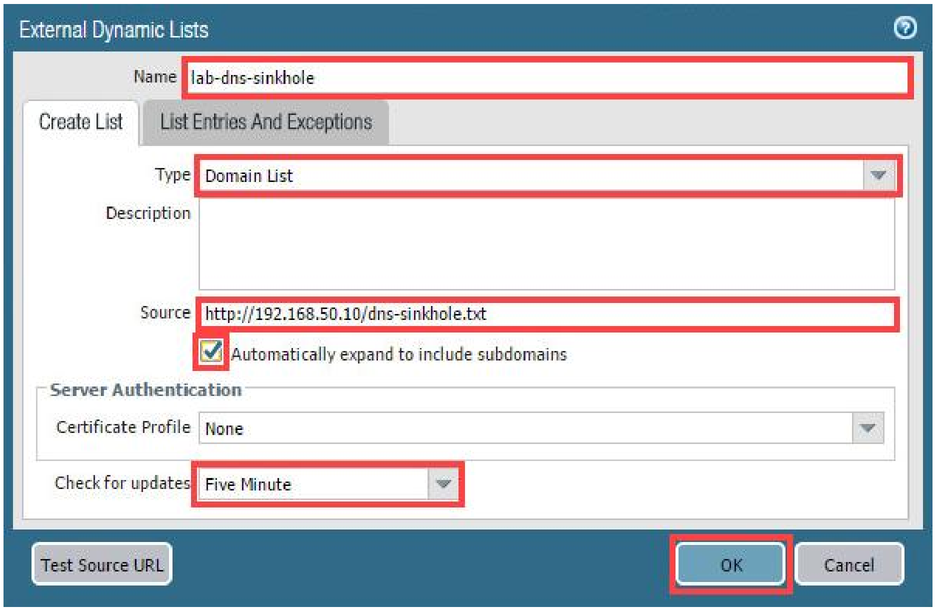


2. Click **Add** to configure a new External Dynamic List.



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

Parameter	Value
Name	`lab-dns-sinkhole`
Type	**Domain List**
Source	Type `http://192.168.50.10/dns-sinkhole.txt` (This is hosted on the DMZ server.)
Automatically expand to include subdomains	Select the checkbox
Check for updates	**Five Minute**


External Dynamic Lists

Name: lab-dns-sinkhole

Type: Domain List

Description:

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

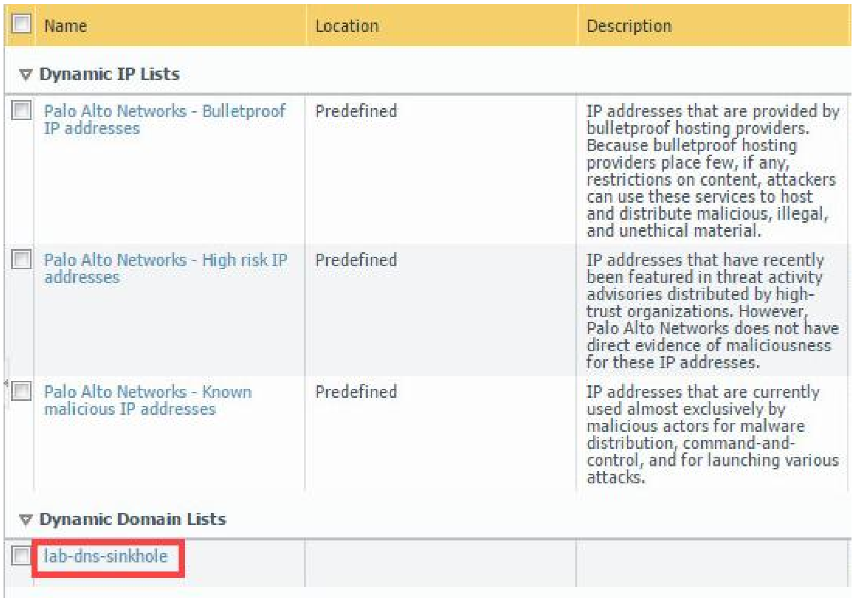
☑ Automatically expand to include subdomains

Server Authentication

Certificate Profile: None

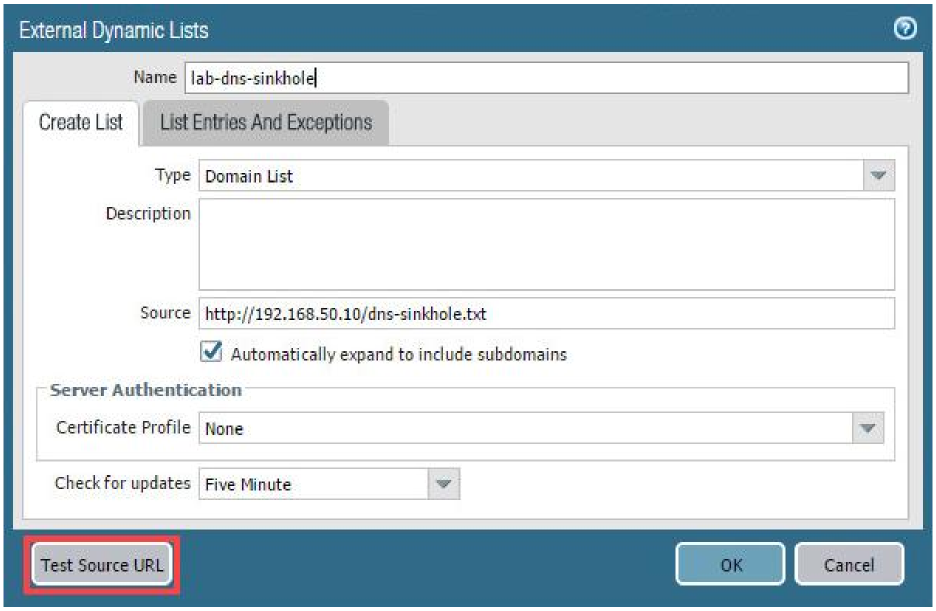
Check for updates: Five Minute

4. **Commit** all changes.
5. Click on **lab-dns-sinkhole** to open the configuration you just created.



□ Name	Location	Description
Dynamic IP Lists		
□ Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.
□ Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.
□ Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.
Dynamic Domain Lists		
□ lab-dns-sinkhole		

6. In the *External Dynamic List* window, click the **Test Source URL** button.



External Dynamic Lists

Name: lab-dns-sinkhole

Type: Domain List

Description:

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

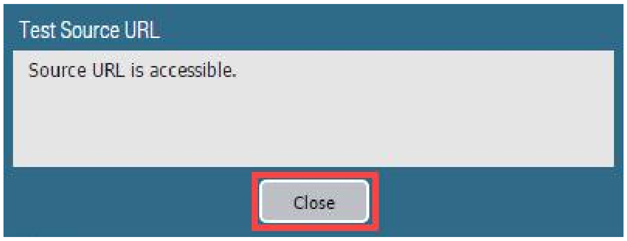
☑ Automatically expand to include subdomains

Server Authentication

Certificate Profile: None

Check for updates: Five Minute

7. Confirm that the firewall reports that the source URL is accessible and click **Close**. If the firewall reports a “URL access error”, check the source address, correct any errors, and rerun the test.



Test Source URL

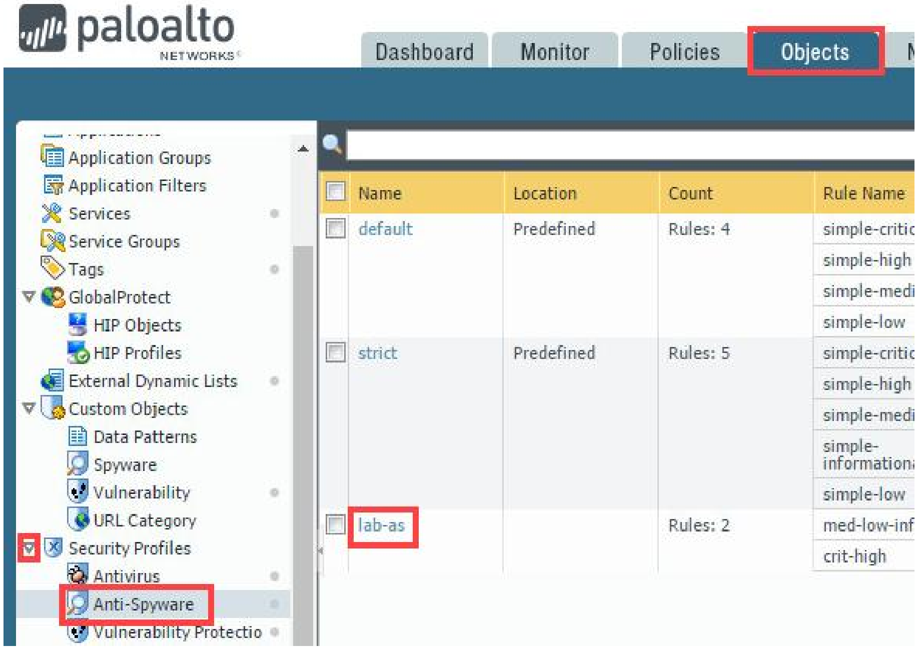
Source URL is accessible.

8. Back on the *External Dynamic Lists* window, click **Cancel** to close it.
9. Leave the firewall web interface open to continue with the next task

1.7 Create an Anti-Spyware Profile with DNS Sinkhole

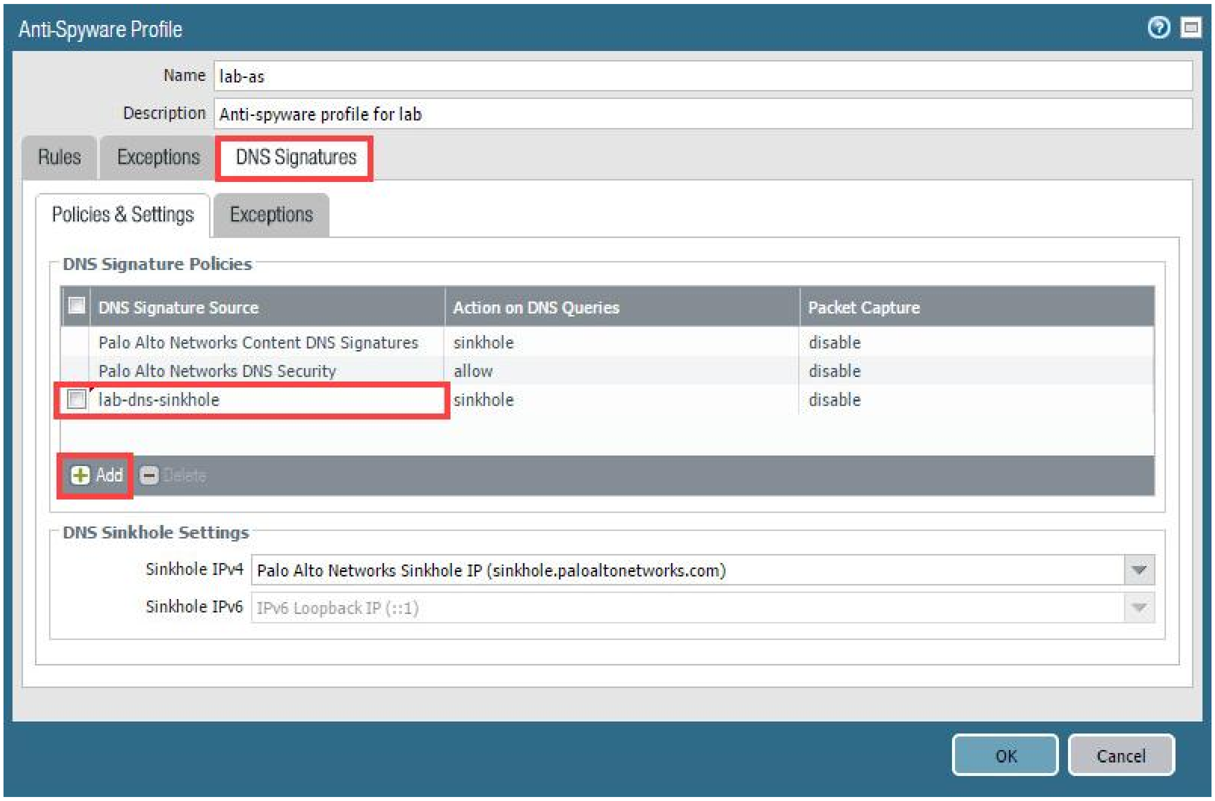
The DNS sinkhole action provides administrators with a method of identifying infected hosts on the network using DNS traffic, even when the firewall cannot see the originator of the DNS query because the DNS server is not on the internal network.

1. In the web interface, navigate to **Objects > Security Profiles > Anti-Spyware** and then click the Anti-Spyware Profile named **lab-as**.



Name	Location	Count	Rule Name
default	Predefined	Rules: 4	simple-critic simple-high simple-medi simple-low
strict	Predefined	Rules: 5	simple-critic simple-high simple-medi simple-informationa simple-low
lab-as		Rules: 2	med-low-inf crit-high

2. In the *Anti-Spyware Profile* window, click the **DNS Signatures** tab. Locate the DNS Signature Policies box, click **Add**, and select **lab-dns-sinkhole**.



Name: lab-as

Description: Anti-spyware profile for lab

DNS Signature Policies

DNS Signature Source	Action on DNS Queries	Packet Capture
Palo Alto Networks Content DNS Signatures	sinkhole	disable
Palo Alto Networks DNS Security	allow	disable
□ lab-dns-sinkhole	sinkhole	disable

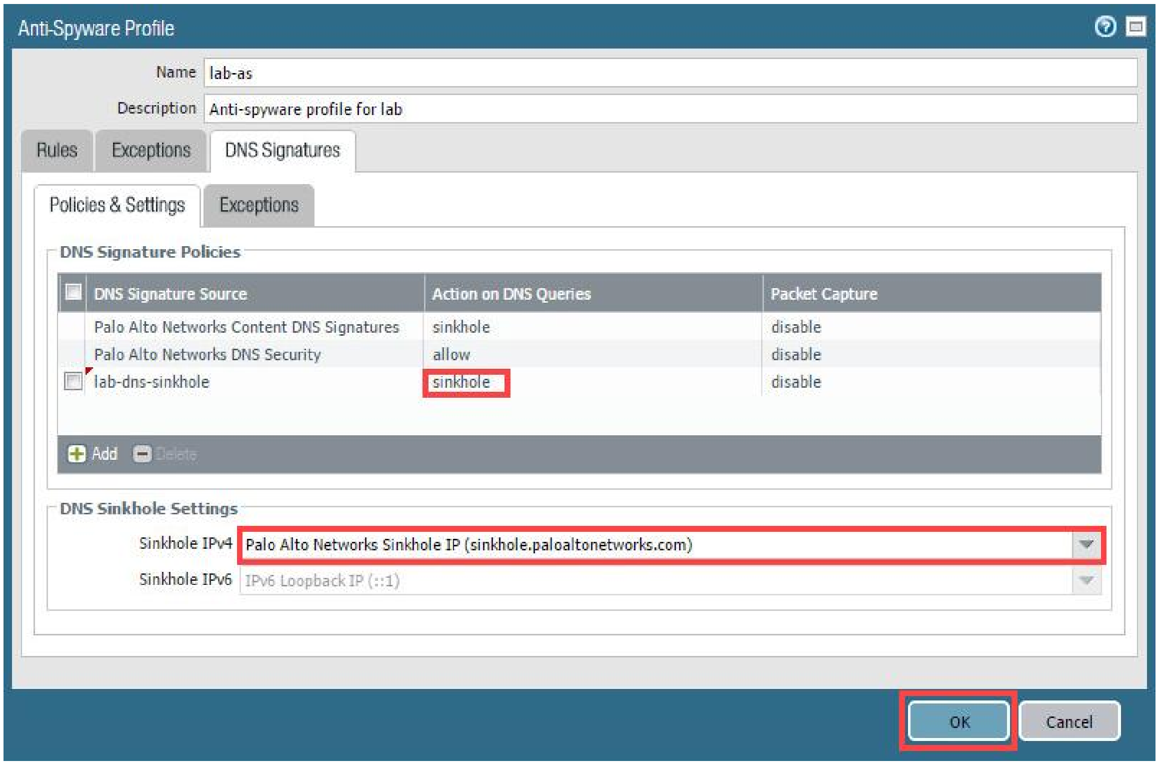
DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

3. Verify that the *Action on DNS Queries* column for *lab-dns-sinkhole* is set to **sinkhole**.

4. Verify that the *Sinkhole IPv4* is set to **Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)** in the *DNS Sinkhole Settings* box. Click **OK** to close the *Anti-Spyware Profile* configuration window.



Name: lab-as

Description: Anti-spyware profile for lab

DNS Signature Policies

DNS Signature Source	Action on DNS Queries	Packet Capture
Palo Alto Networks Content DNS Signatures	sinkhole	disable
Palo Alto Networks DNS Security	allow	disable
lab-dns-sinkhole	sinkhole	disable

DNS Sinkhole Settings

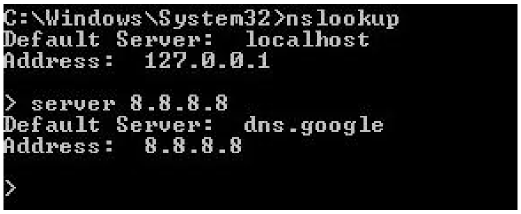
Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

5. **Commit** all changes.

1.8 Test the Security Policy Rule

1. 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.

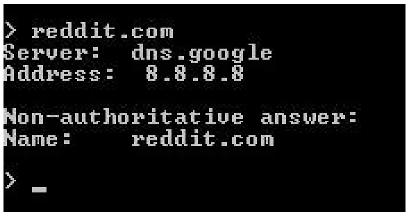


```
C:\Windows\System32>nslookup
Default Server:  localhost
Address:  127.0.0.1

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

>
```

4. At the *nslookup* command prompt, type **`reddit.com`**. and press the **Enter** key.

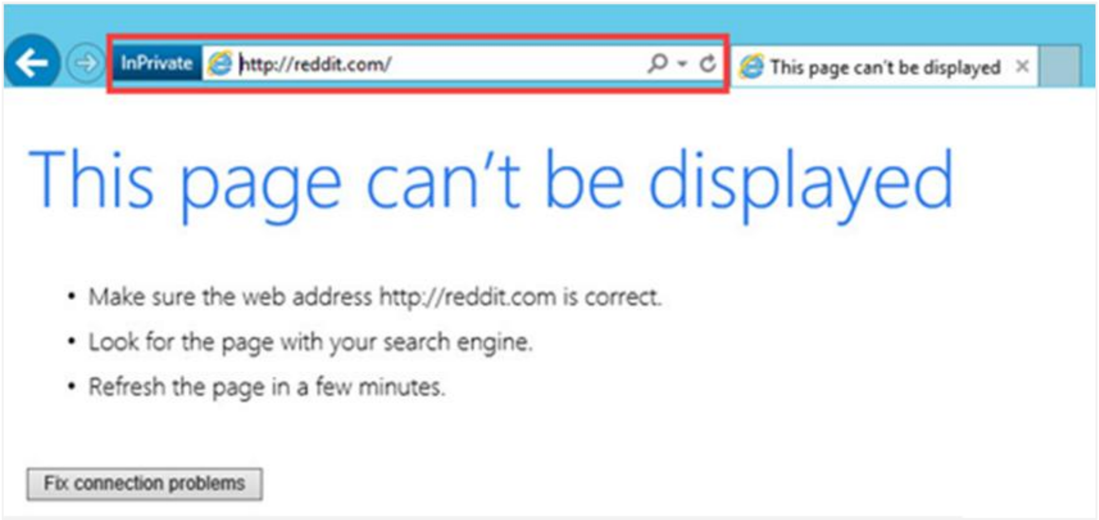


```
> reddit.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    reddit.com

> _
```

5. Notice that the reply for *reddit.com* does not display an IP address. The request has been sinkholed. Type **`exit`** and press **Enter** to exit *nslookup*.
6. Type **`exit`** and press **Enter** again to exit the CLI.
7. Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to **`http://reddit.com`**. Wait for the connection to time out.



This page can't be displayed

- Make sure the web address http://reddit.com is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

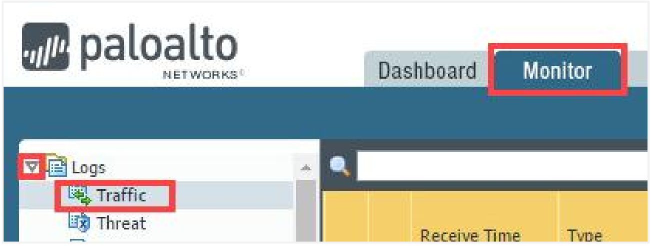
Please Note

Make sure that you do not include "www." in the URL, because "www.reddit.com" is not in the EDL; "reddit.com" is currently the only entry in the list.

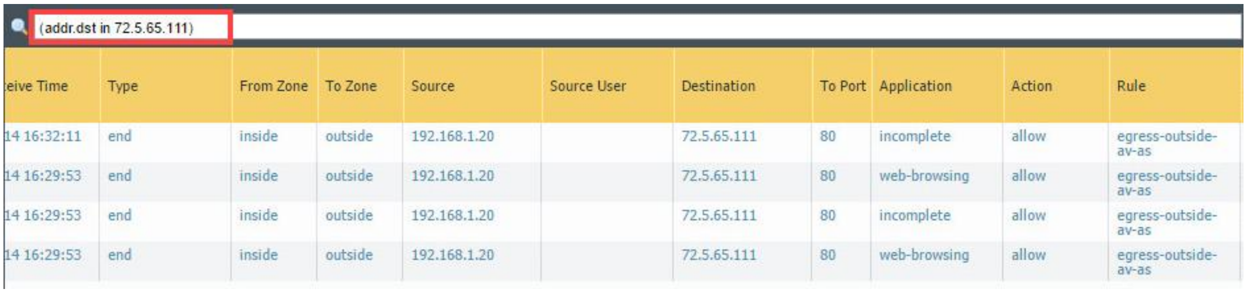
8. Close the browser window.

1.9 Review the Logs

1. Change focus to the firewall's web interface and navigate to **Monitor > Logs > Traffic**.



2. Type the following filter statement **`(addr.dst in 72.5.65.111)`** and press **Enter**.

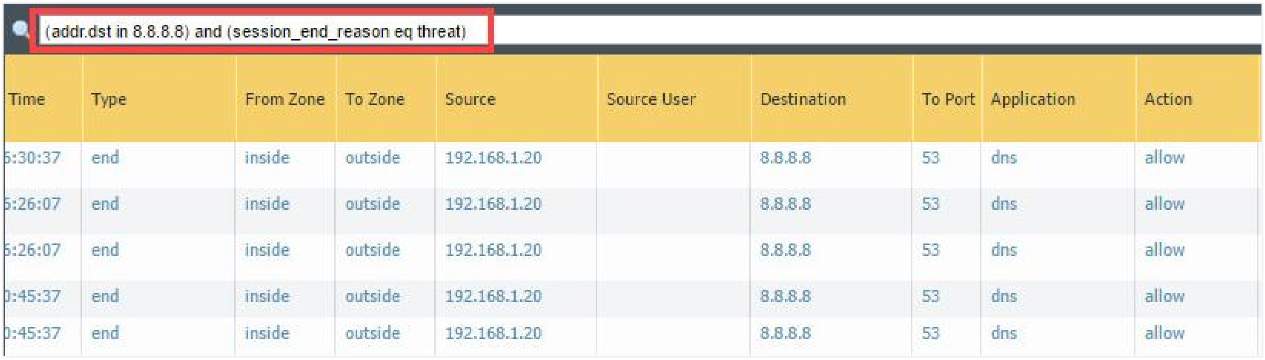


(addr.dst in 72.5.65.111)

eive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
14 16:32:11	end	inside	outside	192.168.1.20		72.5.65.111	80	incomplete	allow	egress-outside-av-as
14 16:29:53	end	inside	outside	192.168.1.20		72.5.65.111	80	web-browsing	allow	egress-outside-av-as
14 16:29:53	end	inside	outside	192.168.1.20		72.5.65.111	80	incomplete	allow	egress-outside-av-as
14 16:29:53	end	inside	outside	192.168.1.20		72.5.65.111	80	web-browsing	allow	egress-outside-av-as

Notice that the *Application* type is *incomplete*. This result occurs because the sinkhole address does not reply to the connection attempt made by the browser to reach *reddit.com*. The browser attempts to connect to the sinkhole address because the firewall is blocking the original DNS request. The firewall then returns a firewall-generated DNS reply that tells the browser that *reddit.com* is located at the sinkhole address.

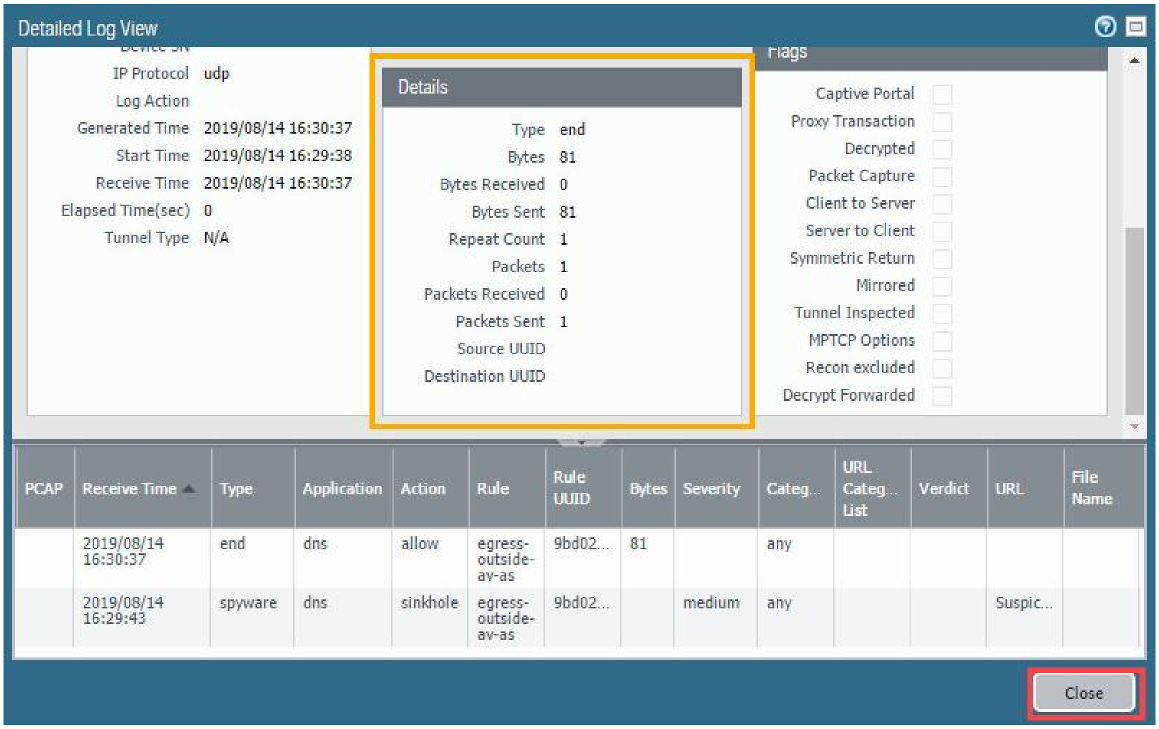
3. To find the original DNS request in the Traffic log, use the following filter statement **`(addr.dst in 8.8.8.8) and (session_end_reason eq threat)`** and then press **Enter**.



(addr.dst in 8.8.8.8) and (session_end_reason eq threat)

Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
5:30:37	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow
5:26:07	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow
5:26:07	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow
0:45:37	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow
0:45:37	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow

4. Click the **magnifying glass** icon 🔍 next to one of the entries to see the *Detailed Log View*.
5. In the *Detailed Log View* window, you should notice the additional information that matches what you previously viewed in the Threat log. Next, scroll down and review the information in the Details section in the middle column of the main display area. Notice that the traffic log records only one packet. This packet is the original DNS query send from the client. The DNS response packet with the sinkhole address is sent directly from the firewall itself. Click **Close** to close the *Detailed Log View* window.



Detailed Log View

IP Protocol	udp
Log Action	
Generated Time	2019/08/14 16:30:37
Start Time	2019/08/14 16:29:38
Receive Time	2019/08/14 16:30:37
Elapsed Time(sec)	0
Tunnel Type	N/A

Details

Type	end
Bytes	81
Bytes Received	0
Bytes Sent	81
Repeat Count	1
Packets	1
Packets Received	0
Packets Sent	1
Source UUID	
Destination UUID	

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Client to Server	□
Server to Client	□
Symmetric Return	□
Mirrored	□
Tunnel Inspected	□
MPTCP Options	□
Recon excluded	□
Decrypt Forwarded	□

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/08/14 16:30:37	end	dns	allow	egress-outside-av-as	9bd02...	81		any				
	2019/08/14 16:29:43	spyware	dns	sinkhole	egress-outside-av-as	9bd02...		medium	any			Suspic...	

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