



PALO ALTO NETWORKS EDU-210



Lab 5A: Content-ID

Document Version: 2021-08-24

Contents

| | |
|---|----|
| Introduction | 3 |
| Objectives..... | 3 |
| Lab Topology | 4 |
| Theoretical Lab Topology..... | 4 |
| Lab Settings | 5 |
| 5 Content-ID..... | 6 |
| 5.0 Load Lab Configuration | 6 |
| 5.1 Create Security Policy Rule with an Antivirus Profile..... | 9 |
| 5.2 Test Security Policy Rule..... | 12 |
| 5.3 Review Logs..... | 13 |
| 5.4 Create Security Policy Rule with an Anti-Spyware Profile | 16 |
| 5.5 Create a DMZ-Access Security Policy | 22 |
| 5.6 Configure DNS-Sinkhole External Dynamic List..... | 25 |
| 5.7 Create an Anti-Spyware Profile with DNS Sinkhole | 28 |
| 5.8 Test the Security Policy Rule | 31 |
| 5.9 Review the Logs..... | 33 |

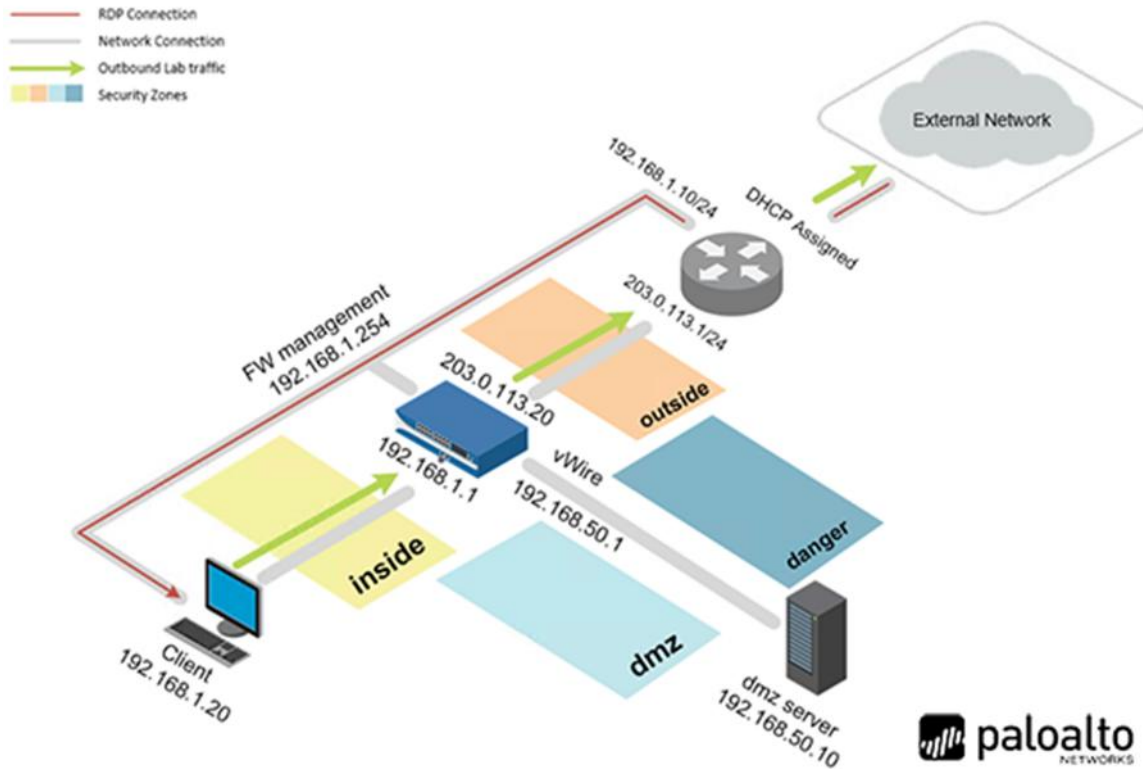
Introduction

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.

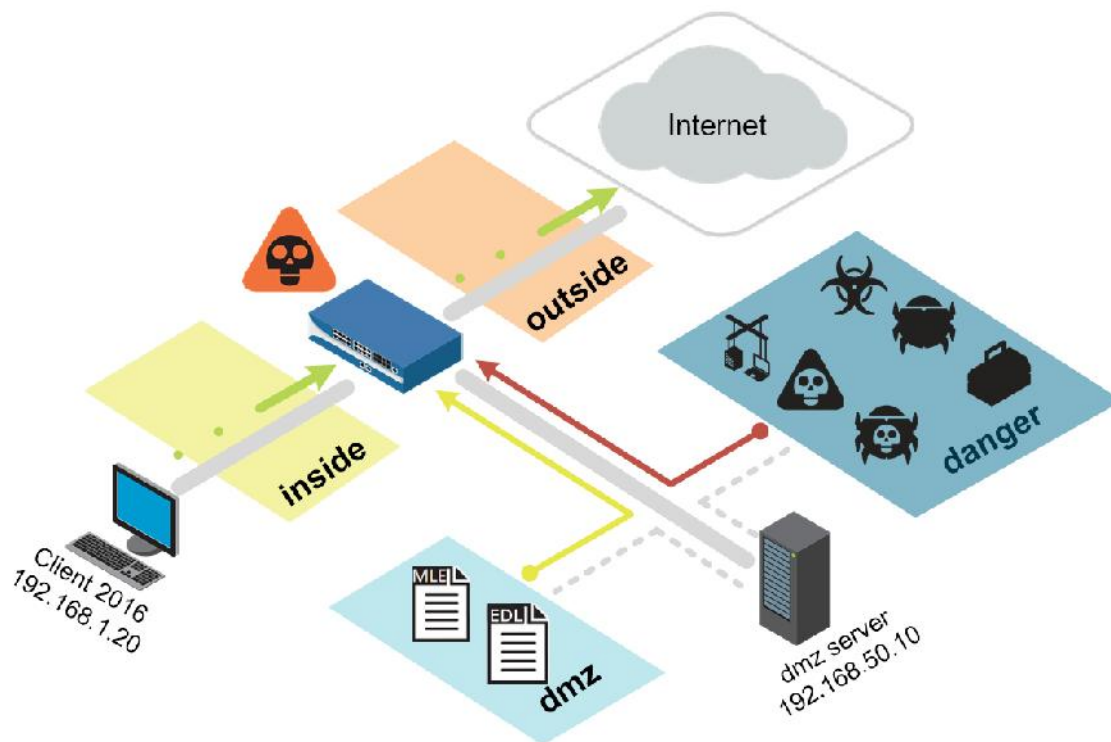
Objectives

-) 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 | Train1ng\$ |
| Firewall | 192.168.1.254 | admin | Train1ng\$ |

5 Content-ID

5.0 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. Log in as **lab-user** using the password **Train1ng\$**.



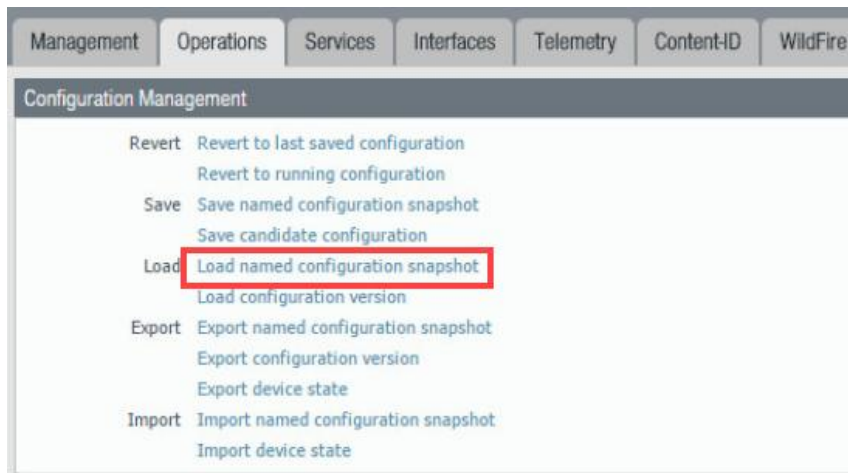
3. Launch the **Chromium Web Browser** and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

| Parameter | Value |
|-----------|------------|
| Name | admin |
| Password | Train1ng\$ |

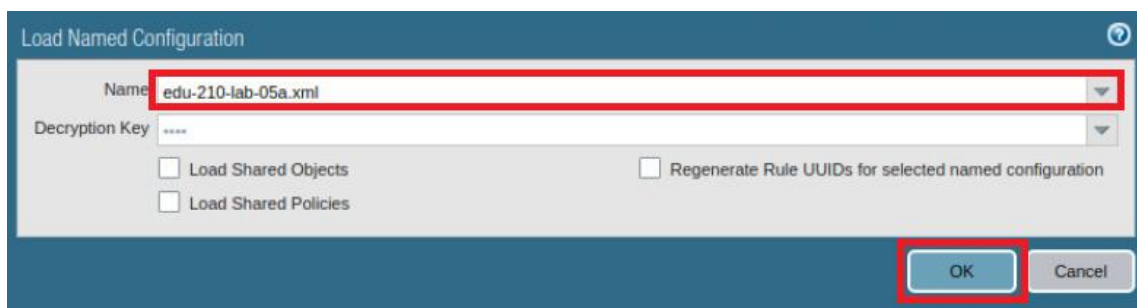
6. In the web interface, navigate to **Device > Setup > Operations**.



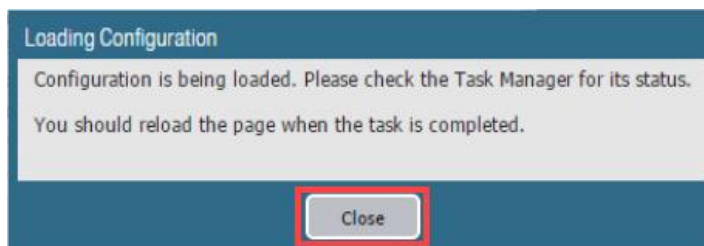
7. Click **Load named configuration snapshot**:



8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-05a.xml**. Click **OK**.



9. Click **Close**.

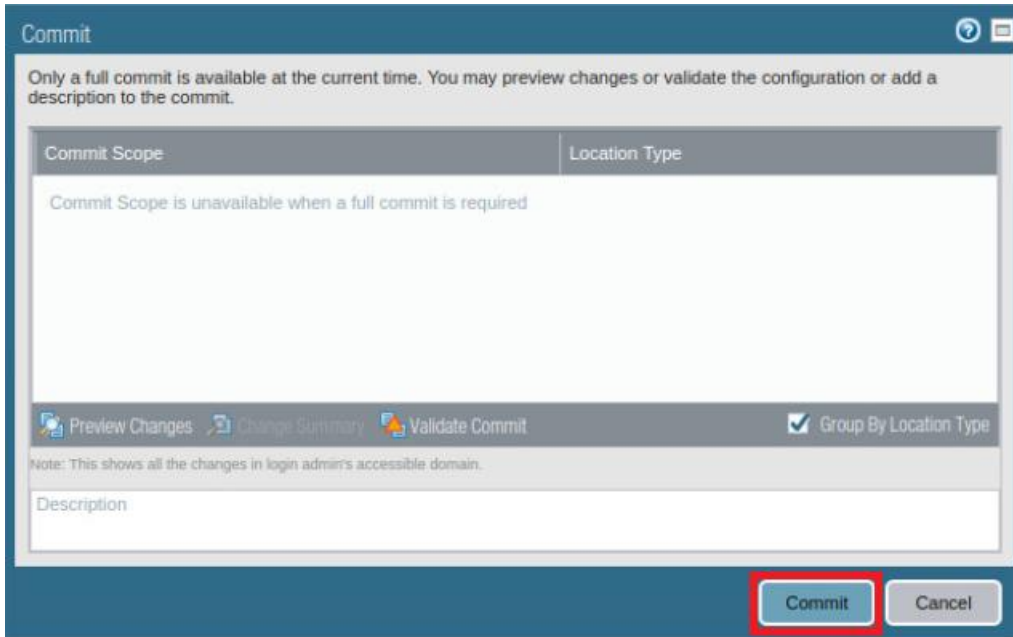


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

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

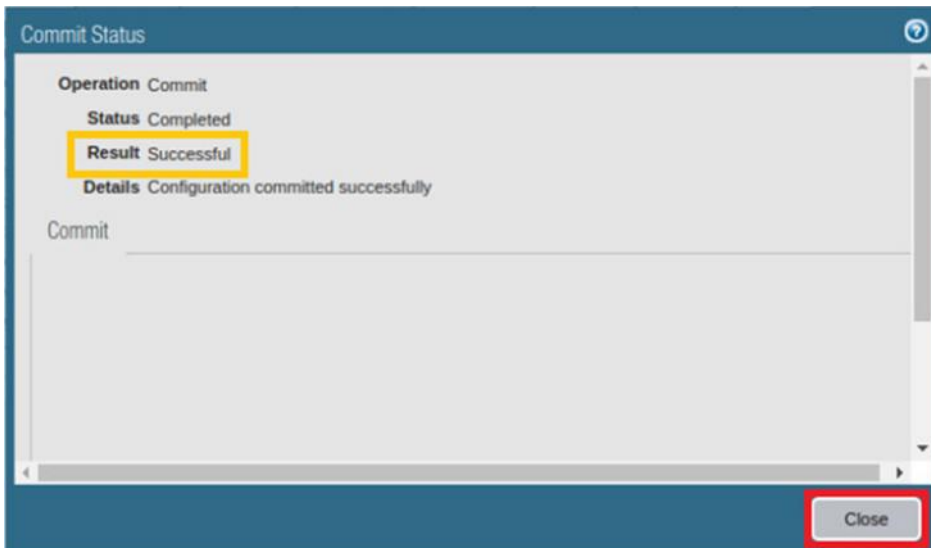


11. Click **Commit** and wait until the commit process is complete.



The 'Commit' dialog box has a title bar with a question mark icon. The main text reads: '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.' Below this is a table with two columns: 'Commit Scope' and 'Location Type'. The 'Commit Scope' column contains the text 'Commit Scope is unavailable when a full commit is required'. Below the table are three buttons: 'Preview Changes', 'Change Summary', and 'Validate Commit'. To the right of these buttons is a checked checkbox labeled 'Group By Location Type'. Below the buttons is a text area labeled 'Description' with the note: 'Note: This shows all the changes in login admin's accessible domain.' At the bottom right are two buttons: 'Commit' (highlighted with a red box) and 'Cancel'.

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



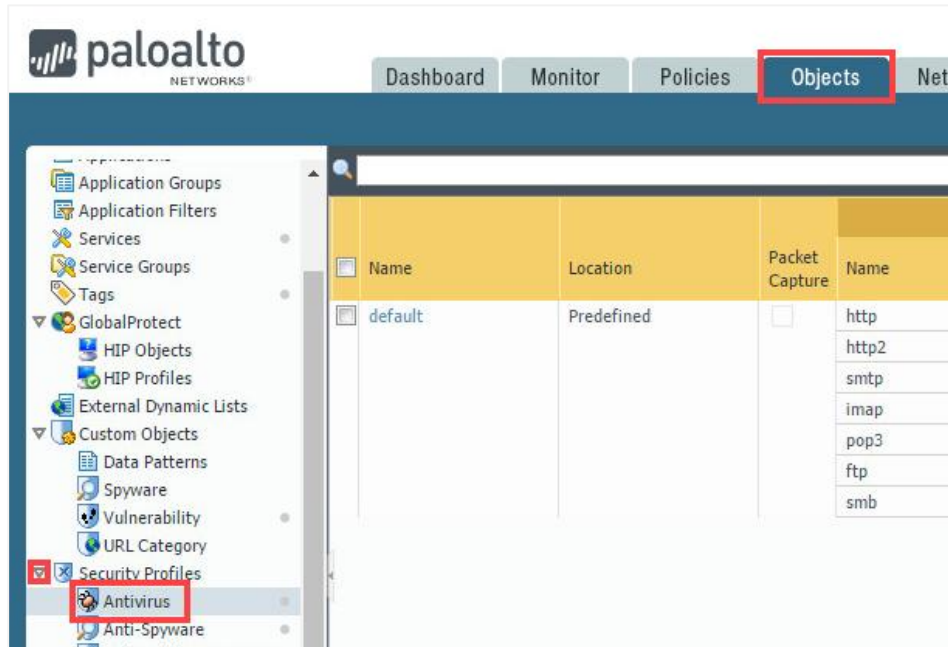
The 'Commit Status' dialog box has a title bar with a question mark icon. It displays the following information: 'Operation Commit', 'Status Completed', 'Result Successful' (highlighted with a yellow box), and 'Details Configuration committed successfully'. Below this is a text area labeled 'Commit'. At the bottom right is a button labeled 'Close' (highlighted with a red box).

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

5.1 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**.



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

Antivirus Virus Exception

☒ 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

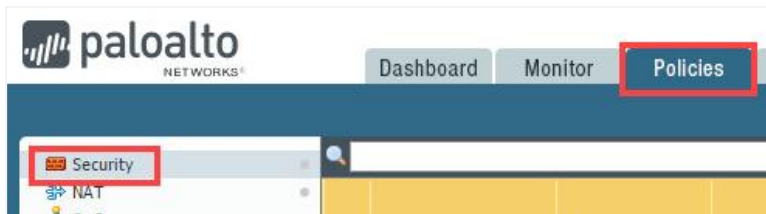
0 items

Application Action

Add Delete

OK Cancel

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

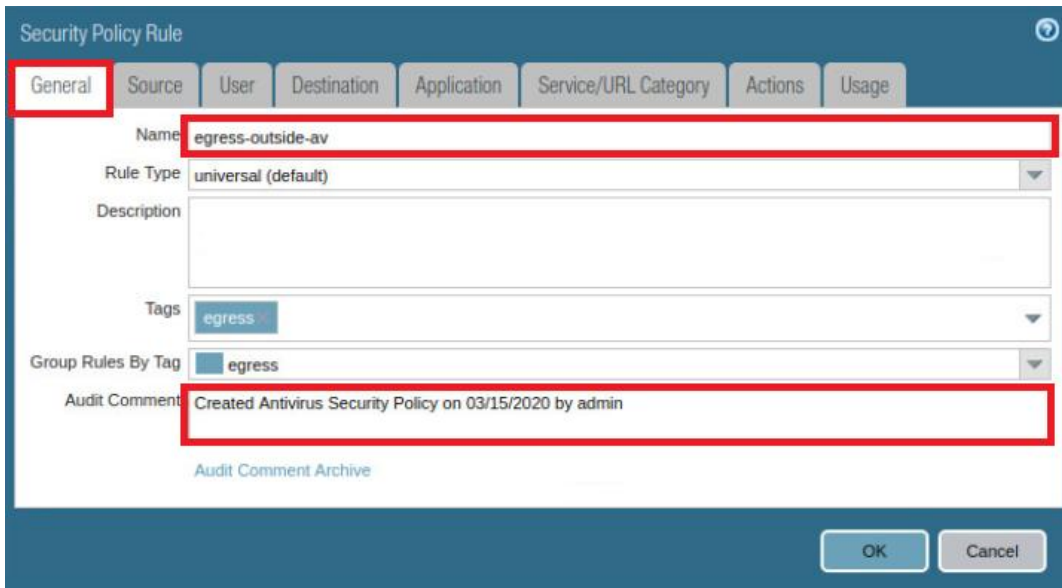


- Click the **egress-outside-app-id** Security Policy Rule to configure the policy.

| | Name | Tags | Type | Source | | |
|---|-----------------------|----------|-----------|--------|---------|------|
| | | | | 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 |

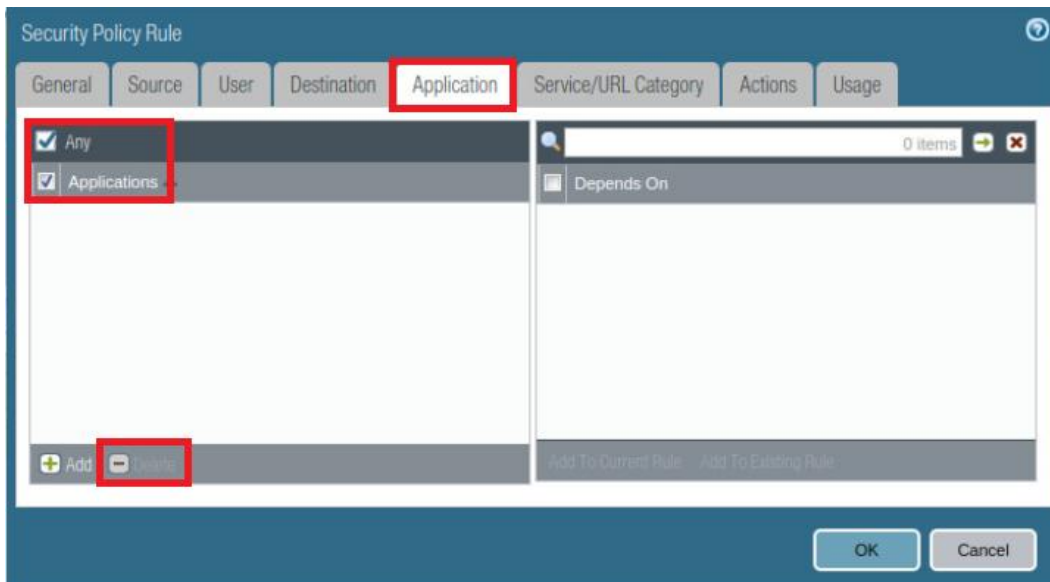
6. In the *Security Policy Rule* window under the *General* tab, configure the following.

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



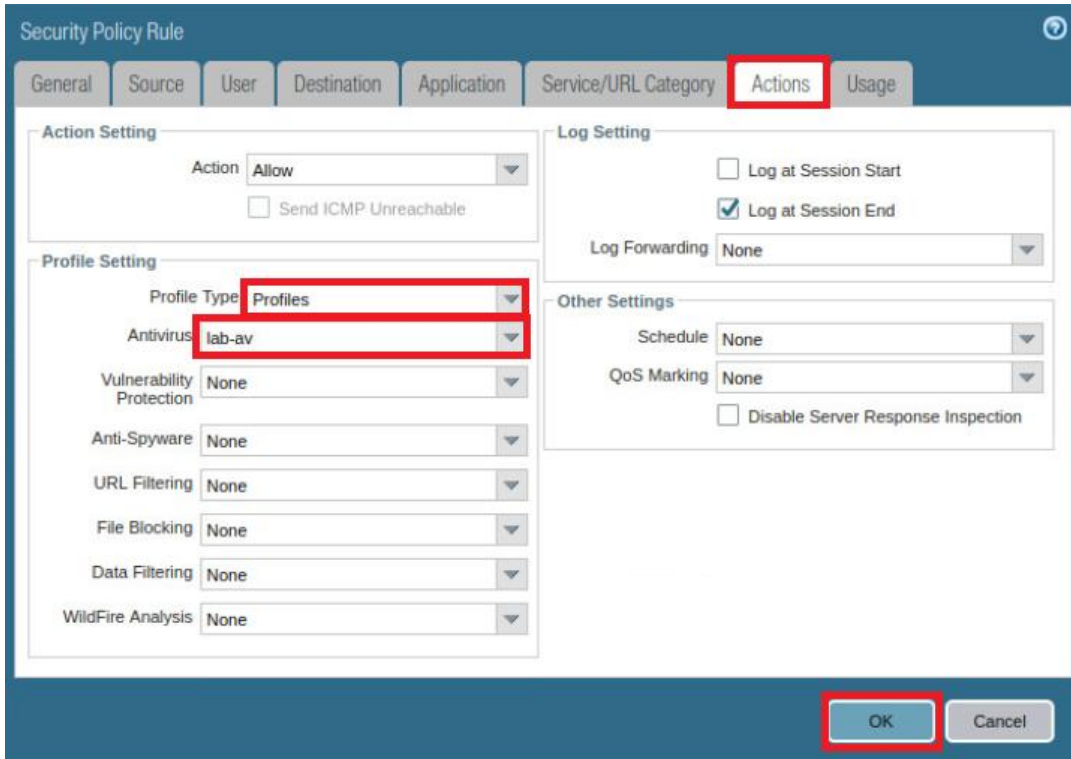
7. In the *Security Policy Rule* window, click the **Application** tab and configure the following:

| 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 dropdown list |
| Antivirus | Select lab-av from the dropdown list |

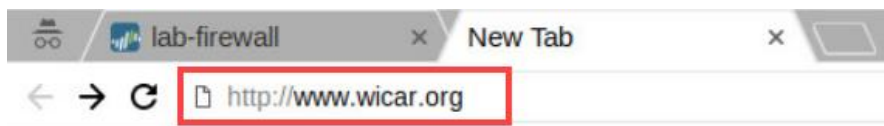


9. **Commit** all changes.

5.2 Test Security Policy Rule

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

1. Open a new tab in **Chromium Web Browser** and browse to <http://www.wicar.org>.



- Click the **Test Malware!** menu option located at the top.



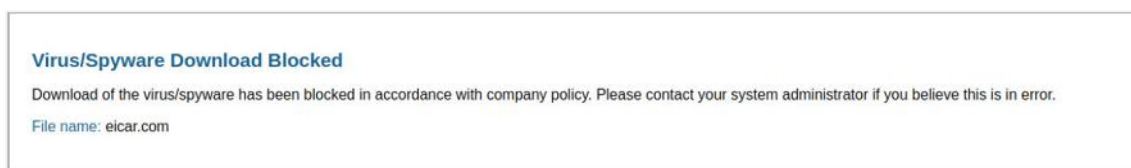
- On the option to select a test payload, click on the **EICAR TEST-VIRUS** button.

Select a test payload...

Each test will open up a new browser window at <http://malware.wicar.org/>. You may wish to try each test systematically. Ideally, all tests should be blocked by your anti-malware defences. If a blank window loads, then it likely was not detected/prevented.



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





5.3 Review Logs



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



- 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 | Source address | Source User | Action |
|---|---|----------------|-------|-----------------|-----------|---------|----------------|-------------|--------------|
|  |  | 02/22 19:10:30 | virus | Eicar Test File | inside | outside | 192.168.1.20 | | reset-server |

- 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 |
|---|---|----------------|-------|-----------------|-----------|---------|
|  |  | 02/22 19:10:30 | virus | Eicar Test File | inside | outside |

- 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 251

Action reset-server

Application web-browsing

Rule egress-outside-av

Rule UUID 7a4f9659-4910-4940-a1d2-db26909ad290

Device SN

IP Protocol tcp

Log Action

Generated Time 2021/02/22 19:10:30

Receive Time 2021/02/22 19:10:30

Tunnel Type N/A

Source

Source User

Source 192.168.1.20

Country 192.168.0.0-192.168.255.255

Port 55954

Zone inside

Interface ethernet1/2

NAT IP 203.0.113.20

NAT Port 23442

Destination

Destination User

Destination 208.94.116.21

Country United States

Port 80

Zone outside


Interface ethernet1/1

NAT IP 208.94.116.21

NAT Port 80

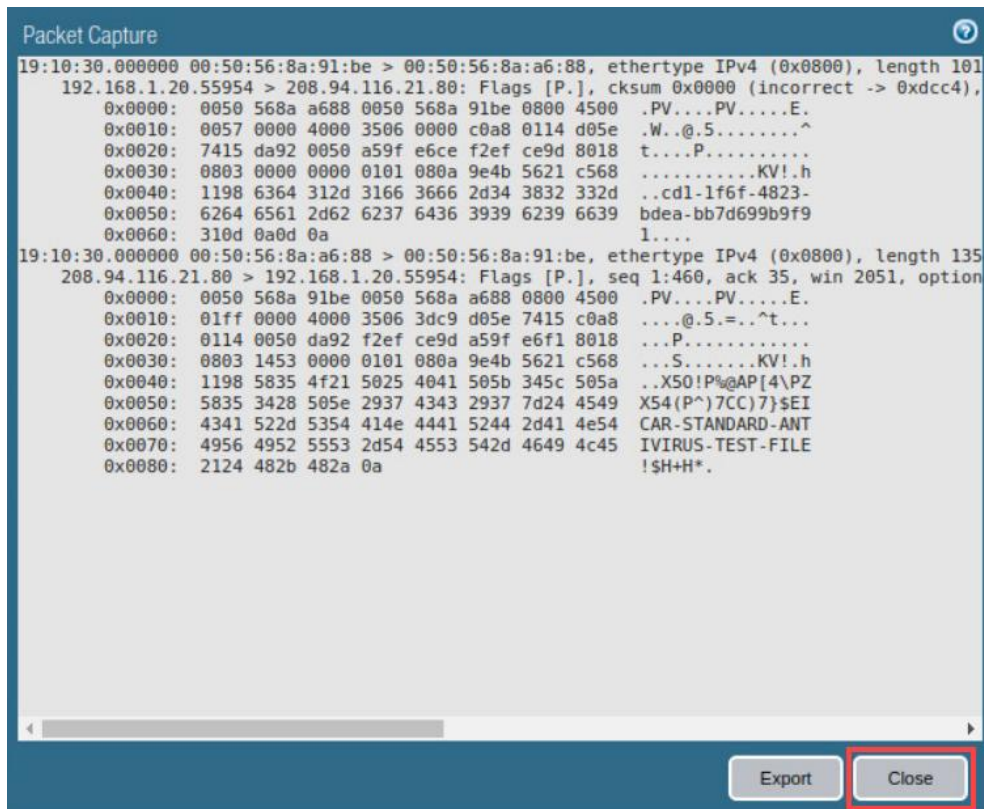
Details

Threat Type virus

| PCAP | Receive Time | Type | Application | Action | Rule | Rule UUID | Byt... | Severity | Categ... | URL Categ... | Verdict | URL | File Name |
|---|---------------------|-------|--------------|--------------|-------------------|-----------|--------|----------|----------|--------------|---------|-----|------------|
|  | 2021/02/22 19:10:30 | virus | web-browsing | reset-server | egress-outside-av | 7a4f9... | | medium | any | | | | eicar.c... |
| | 2021/02/22 19:12:00 | end | web-browsing | allow | egress-outside-av | 7a4f9... | 1855 | | any | | | | |

Close

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



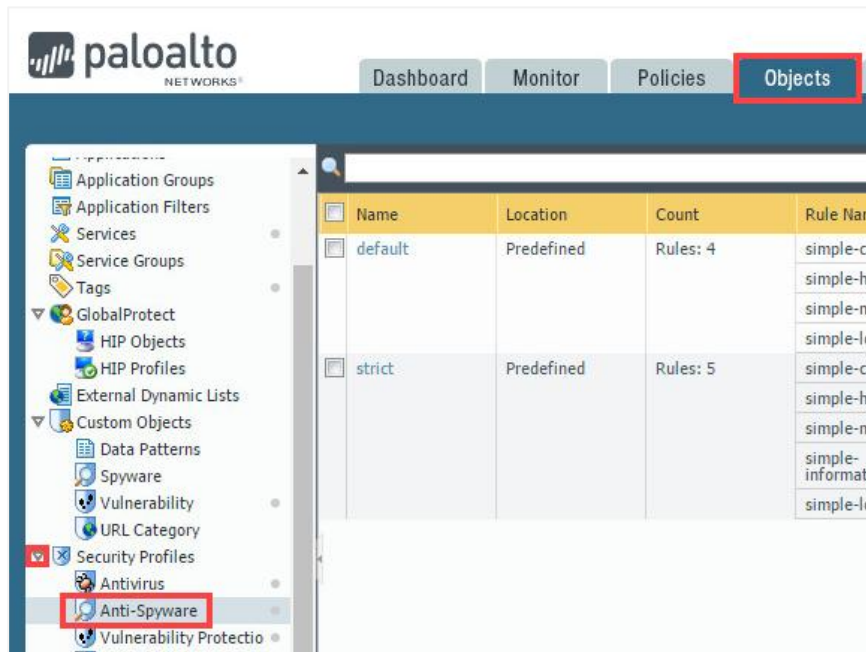
Captured packets can be exported in pcap format and examined with an offline analyzer for further investigation.

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

5.4 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**.

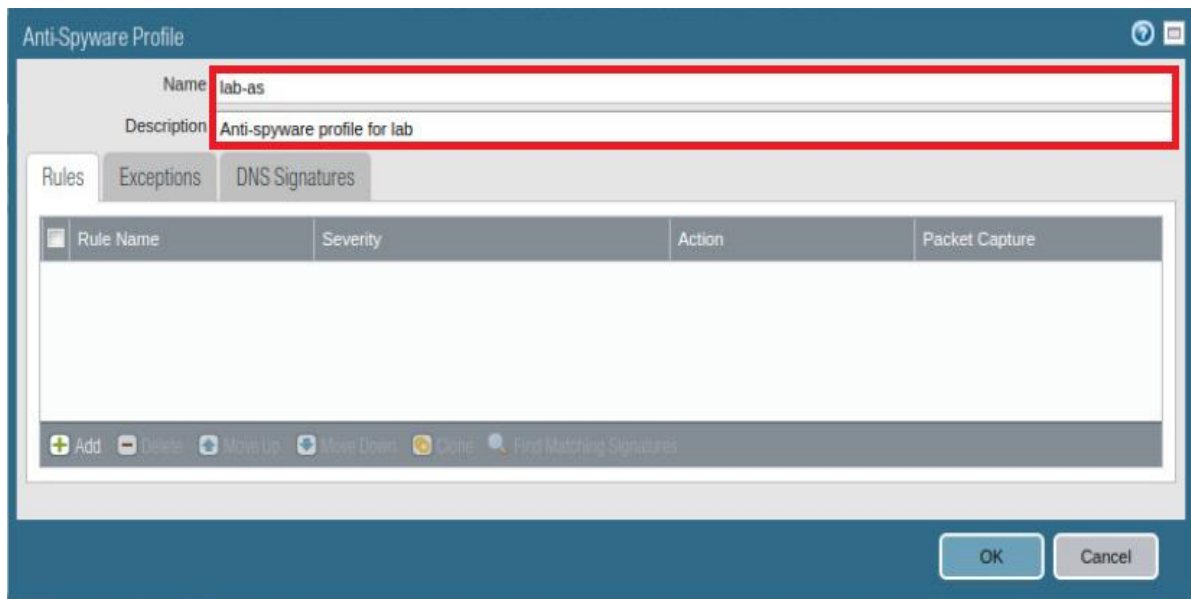


2. Click **Add** to create an Anti-Spyware Profile.



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

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



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

OK Cancel

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**

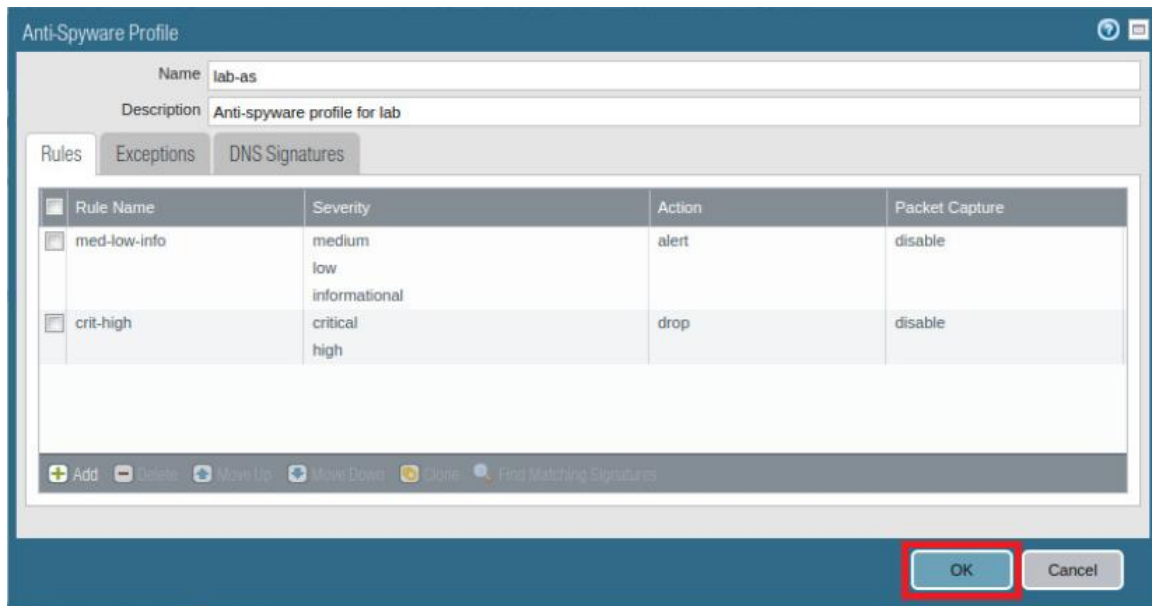
Packet Capture: disable

Severity:

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

OK Cancel

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

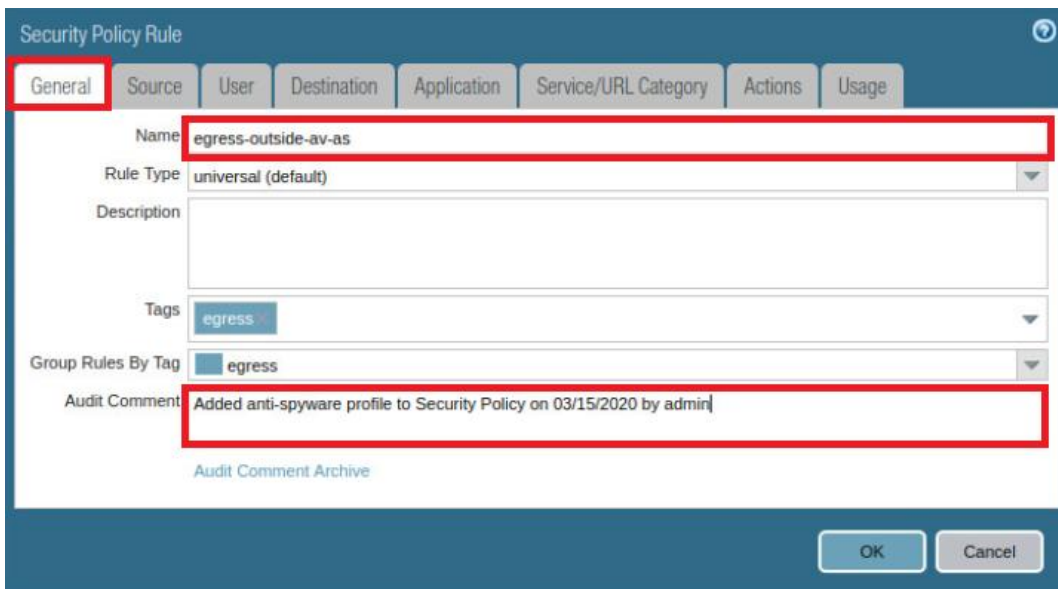


8. In the web interface, select **Policies > Security**.
9. Click on the **egress-outside-av** Security Policy Rule to config the policy.

| | Name | Tags | Type | Source | | |
|---|--------------------------|----------|-----------|--------|---------|------|
| | | | | 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.

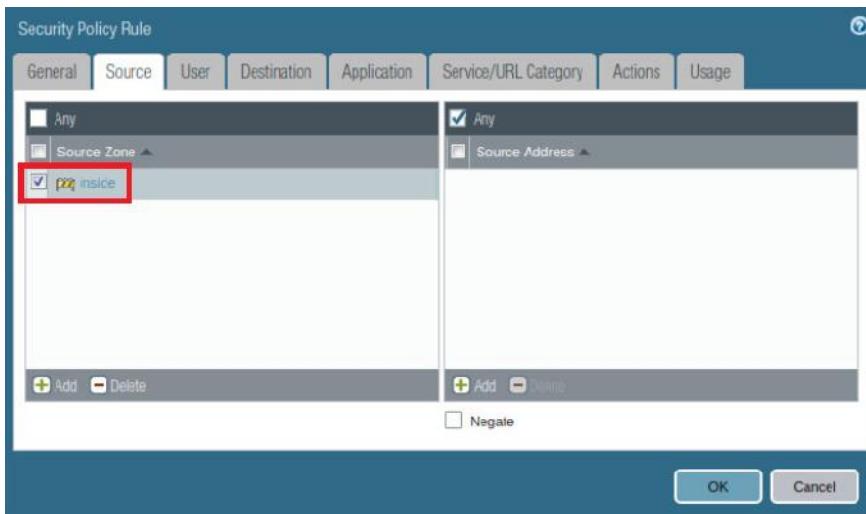
| Parameter | Value |
|---------------|---|
| Name | Rename policy to egress-outside-av-as |
| Audit Comment | Type Added anti-spyware profile to Security Policy on <date> by admin |



The screenshot shows the 'Security Policy Rule' configuration window with the 'General' tab selected. The 'Name' field is 'egress-outside-av-as'. The 'Rule Type' is 'universal (default)'. The 'Description' field is empty. The 'Tags' field contains 'egress'. The 'Group Rules By Tag' field also contains 'egress'. The 'Audit Comment' field contains 'Added anti-spyware profile to Security Policy on 03/15/2020 by admin'. There is a link for 'Audit Comment Archive' below the comment field. 'OK' and 'Cancel' buttons are at the bottom right.

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

| Parameter | Value |
|-------------|--|
| Source Zone | Verify that inside checkbox is selected |



The screenshot shows the 'Security Policy Rule' configuration window with the 'Source' tab selected. The 'Source Zone' section has a list with 'Any' and 'Source Zone'. The 'inside' checkbox is selected and highlighted with a red box. The 'Source Address' section has a list with 'Any'. There are 'Add' and 'Delete' buttons at the bottom of each list. A 'Negate' checkbox is at the bottom center. 'OK' and 'Cancel' buttons are at the bottom right.

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 |

Security Policy Rule

General Source User Destination Application Service/URL Category **Actions** Usage

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

OK Cancel

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

5.5 Create a DMZ-Access Security Policy

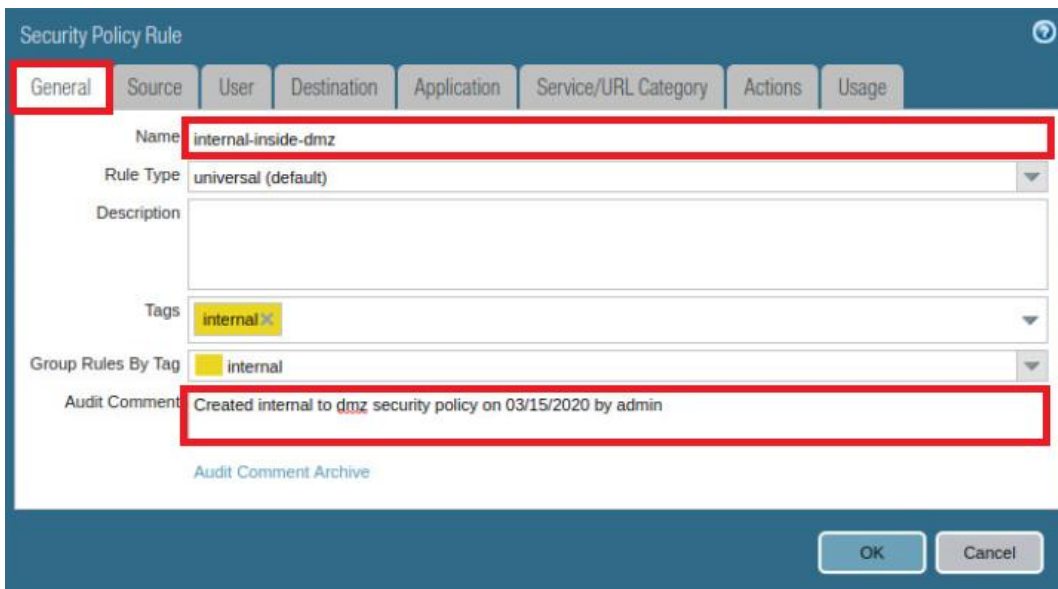
In the next task, you will configure the firewall to download an *External Dynamic List* (EDL) of URLs from the DMZ server. You will then apply the EDL to the Anti-Spyware DNS Sinkhole configuration. Before the EDL and DNS Sinkhole configurations can work, you must create a security policy that allows 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 to configure the policy.

| | Name | Tags | Type | Source | | |
|---|----------------------|----------|-----------|--------|---------|------|
| | | | | Zone | Address | User |
| 1 | egress-outside-av-sa | 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 |

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 |



Security Policy Rule

General Source User Destination Application Service/URL Category Actions Usage

Name: internal-inside-dmz

Rule Type: universal (default)

Description:

Tags: internal

Group Rules By Tag: internal

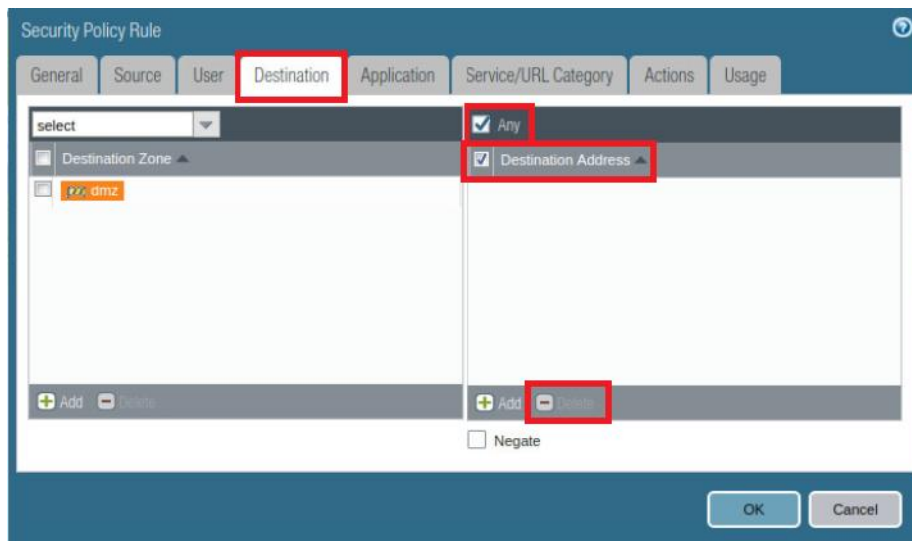
Audit Comment: Created internal to dmz security policy on 03/15/2020 by admin

Audit Comment Archive

OK Cancel

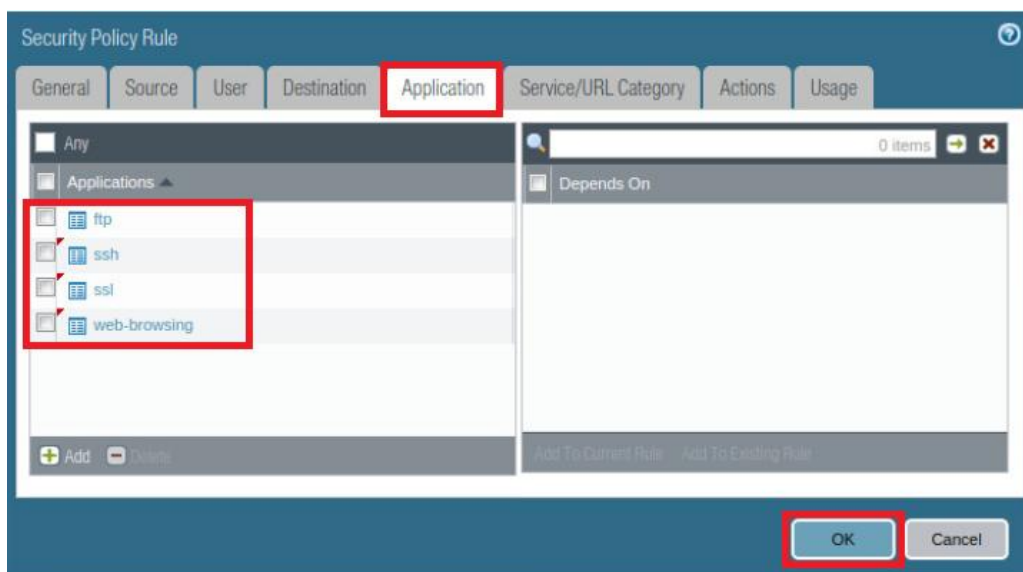
3. In the *Security Policy Rule* window, click the **Destination** tab and configure the following.

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

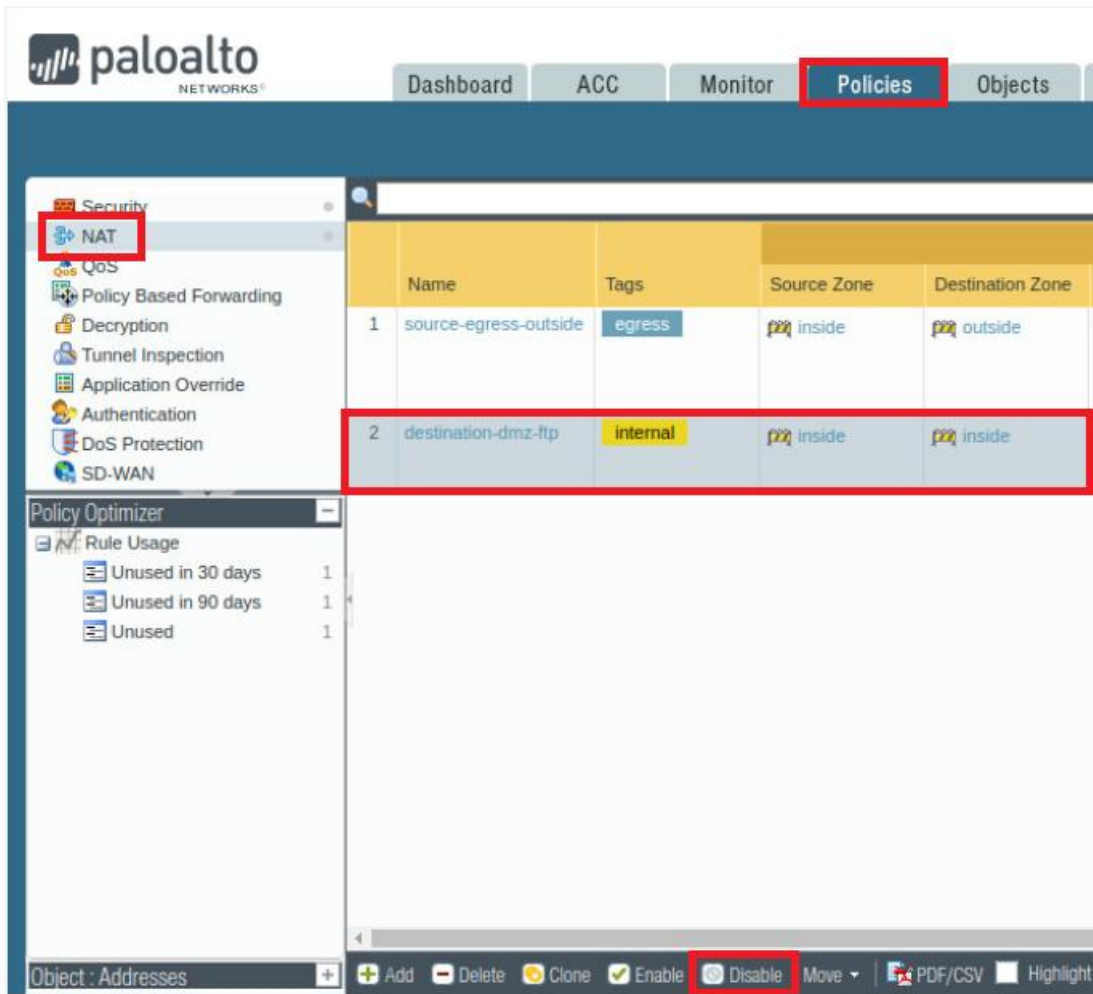


4. In the *Security Policy Rule* window, click the **Application** tab to configure the following and then click **OK**.

| Parameter | Value |
|--------------|--|
| Applications | Click Add and select the following from the dropdown list: ftp web-browsing ssl ssh |



- 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 | Destination Zone |
|---|-----------------------|----------|-------------|------------------|
| 1 | source-egress-outside | egress | inside | outside |
| 2 | destination-dmz-ftp | internal | inside | inside |

Object : Addresses

+ Add - Delete 🔄 Clone ✅ Enable ❌ Disable ⬇ Move 📄 PDF/CSV 🖨 Highlight

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

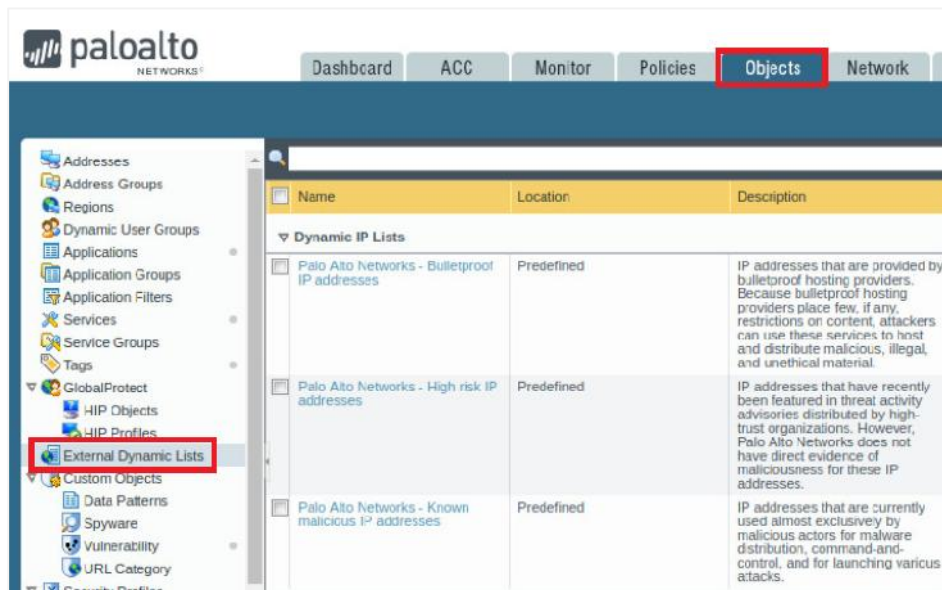
| | Name | Tags | Source Zone | Destination Zone |
|---|-----------------------|----------|-------------|------------------|
| 1 | source-egress-outside | egress | inside | outside |
| 2 | destination-dmz-ftp | internal | inside | inside |

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

5.6 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**.

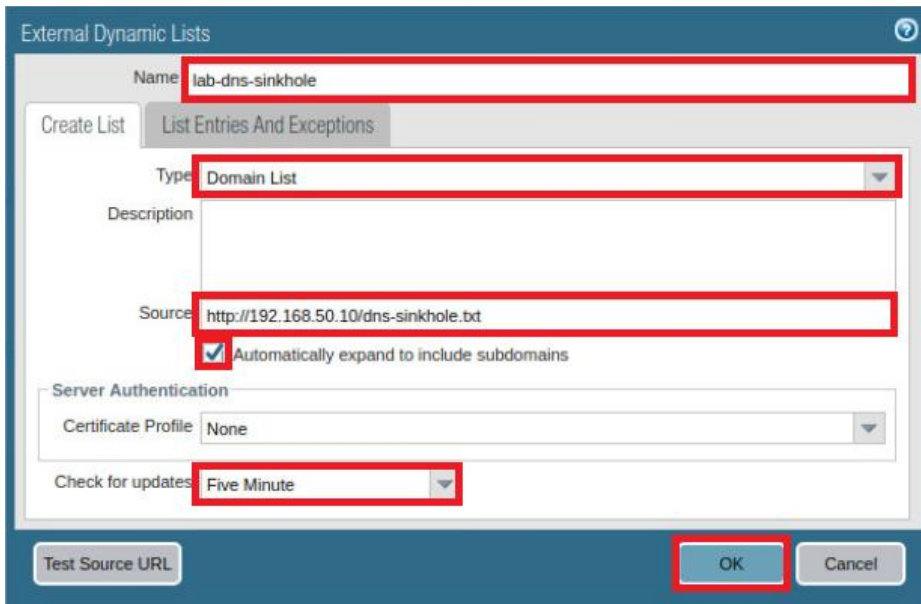


2. Click **Add** to configure a new External Dynamic List.



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

Create List | List Entries And Exceptions

Type: Domain List

Description:

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

☒ Automatically expand to include subdomains

Server Authentication

Certificate Profile: None

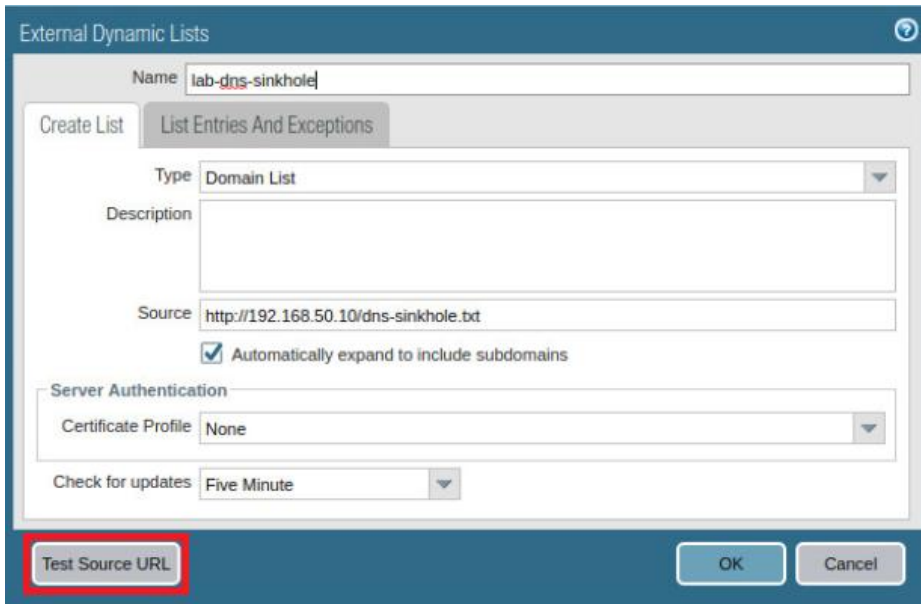
Check for updates: Five Minute

Test Source URL | OK | Cancel

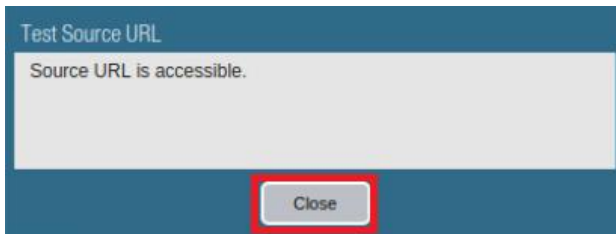
4. **Commit** all changes.
5. Click on **lab-dns-sinkhole** to open the configuration you just created.

| Name | Location | Description |
|--|------------|--|
| Dynamic IP Lists | | |
| <input type="checkbox"/> 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. |
| <input type="checkbox"/> 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. |
| <input type="checkbox"/> 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 | | |
| <input type="checkbox"/> lab-dns-sinkhole | | |

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



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.

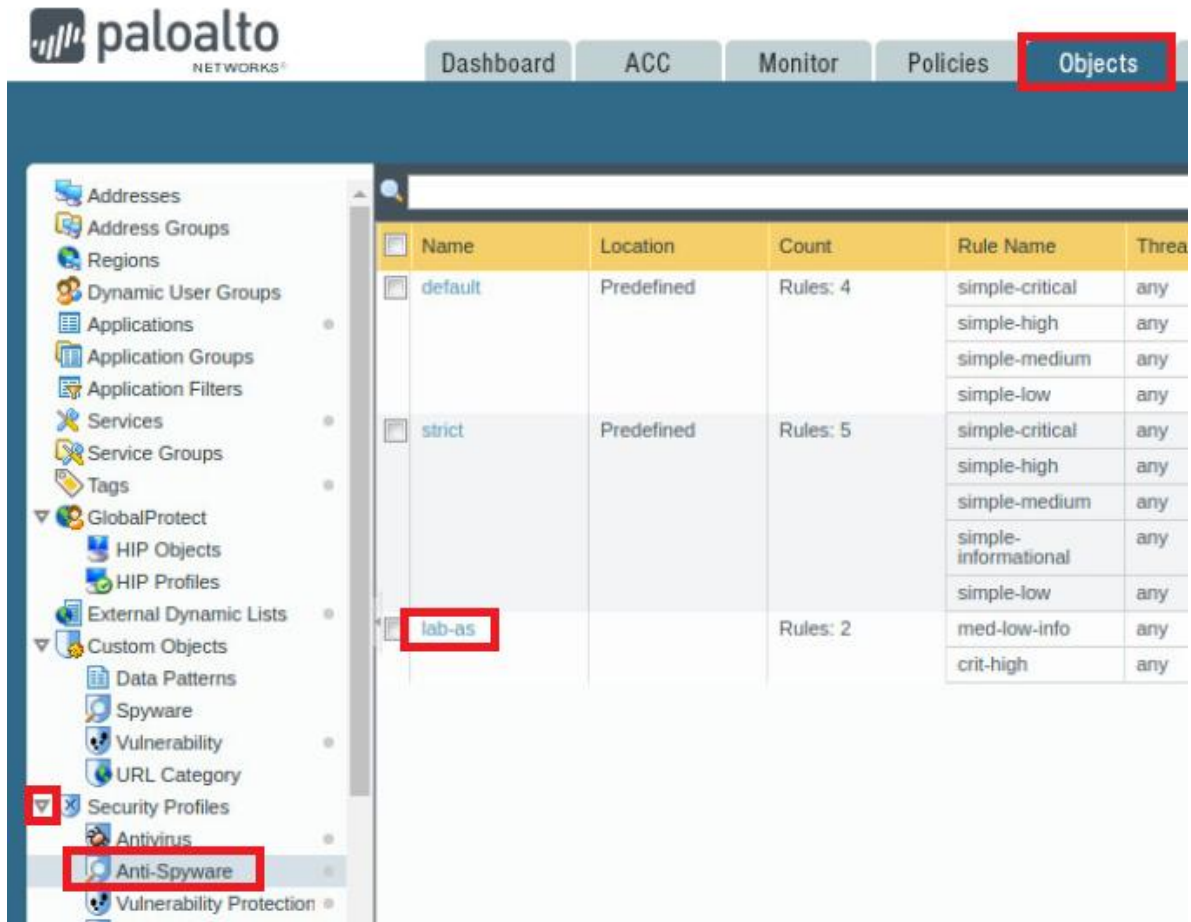


8. Back on the *External Dynamic Lists* window, click **Cancel** to close it.
9. Leave the firewall web interface open to continue with the next task

5.7 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.

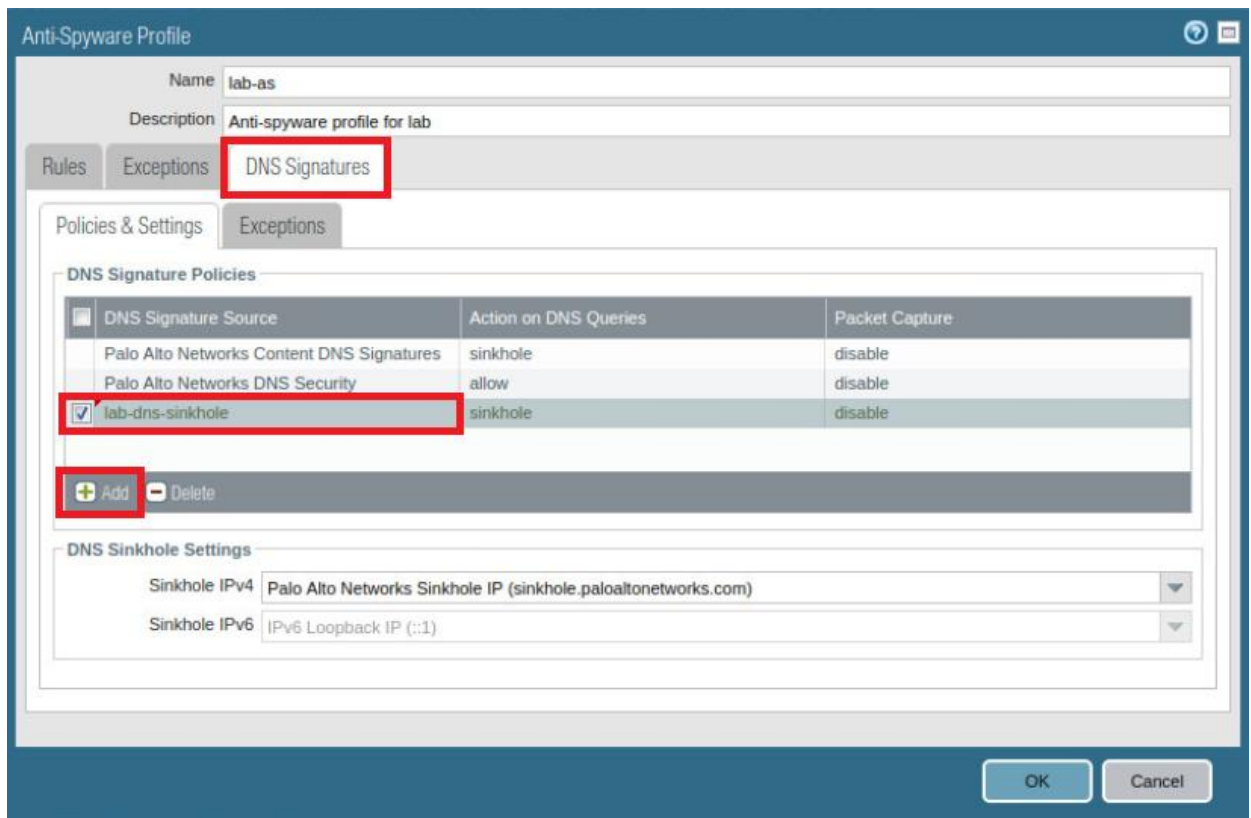
1. In the web interface, navigate to **Objects > Security Profiles > Anti-Spyware** and then click the Anti-Spyware Profile named **lab-as**.



The screenshot shows the Palo Alto Networks web interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', and 'Objects' (highlighted with a red box). The left sidebar contains a tree view of configuration objects, with 'Security Profiles' and 'Anti-Spyware' highlighted. The main content area displays a table of Anti-Spyware profiles:

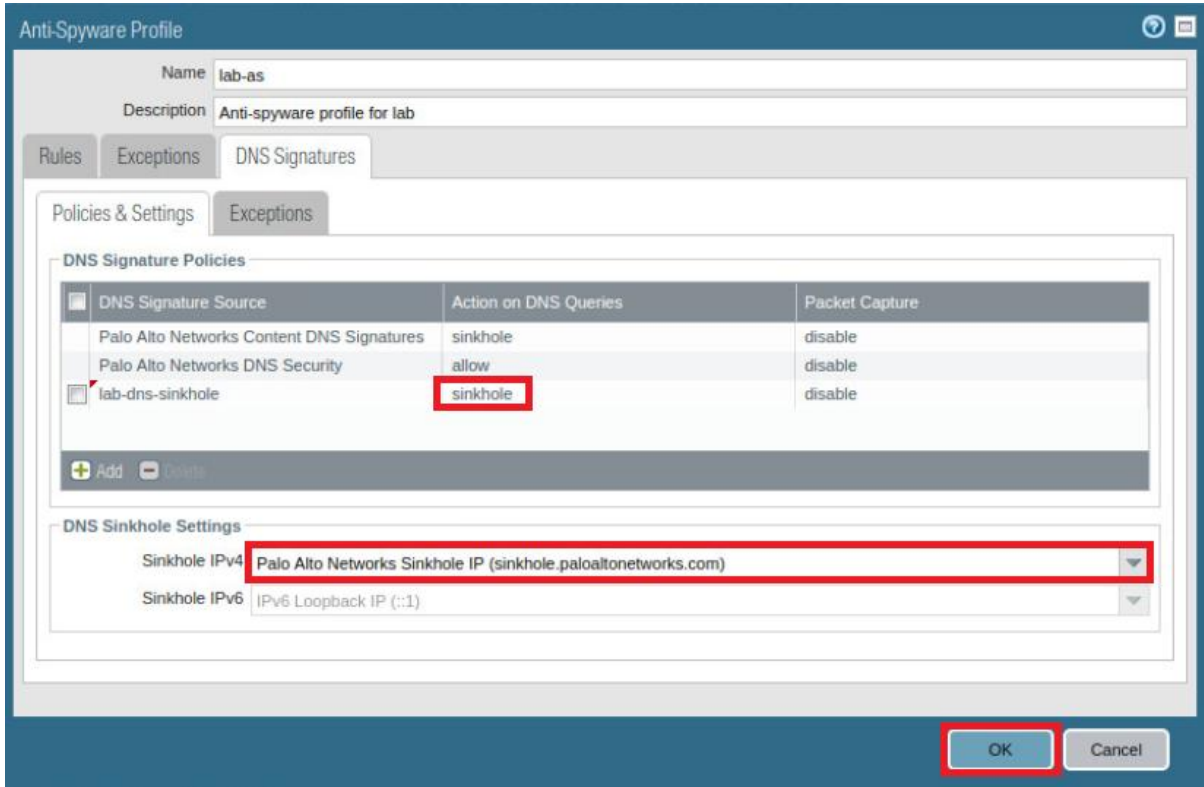
| Name | Location | Count | Rule Name | Threat |
|---------|------------|----------|----------------------|--------|
| default | Predefined | Rules: 4 | simple-critical | any |
| | | | simple-high | any |
| | | | simple-medium | any |
| | | | simple-low | any |
| strict | Predefined | Rules: 5 | simple-critical | any |
| | | | simple-high | any |
| | | | simple-medium | any |
| | | | simple-informational | any |
| | | | simple-low | any |
| lab-as | | Rules: 2 | med-low-info | any |
| | | | crit-high | any |

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**.



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

- 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.



Anti-Spyware Profile

Name: lab-as

Description: Anti-spyware profile for lab

Rules Exceptions DNS Signatures

Policies & Settings Exceptions

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 |

+ Add - Delete

DNS Sinkhole Settings

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

Sinkhole IPv6: IPv6 Loopback IP (::1)

OK Cancel

- Commit** all changes.

5.8 Test the Security Policy Rule

1. Launch the *Terminal* window by clicking on the **Xfce Terminal** icon in the toolbar.



2. Type the **nslookup** command and press the **Enter** key.
3. Type the command **server 8.8.8.8** and press the **Enter** key.

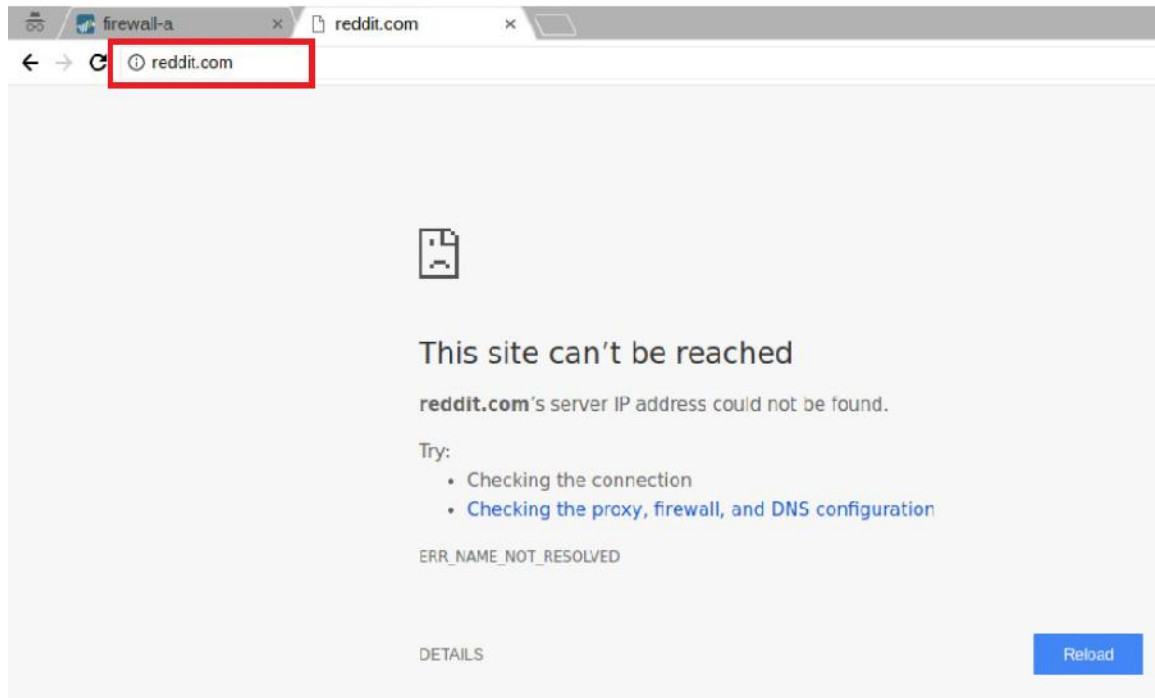
```
C:\home\lab-user> nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> 
```

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

```
> reddit.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
reddit.com   canonical name = sinkhole.paloaltonetworks.com.
> 
```

5. Notice that the reply for *reddit.com* shows *canonical name = sinkhole.paloaltonetworks.com*. The request has been sinkholed. Type **exit** and press **Enter** to exit *nslookup*.
6. Type **exit** and press **Enter** again to exit the Terminal window.
7. Open a new tab in **Chromium Web Browser** and browse to **http://reddit.com**. Wait for the connection to time out.

**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.

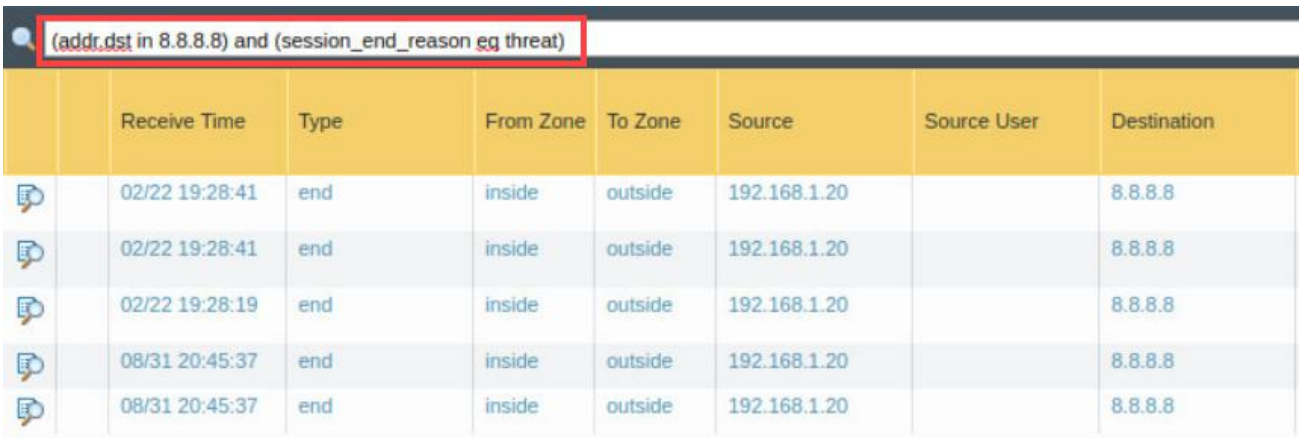
8. Close the reddit browser tab.






5.9 Review the Logs


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



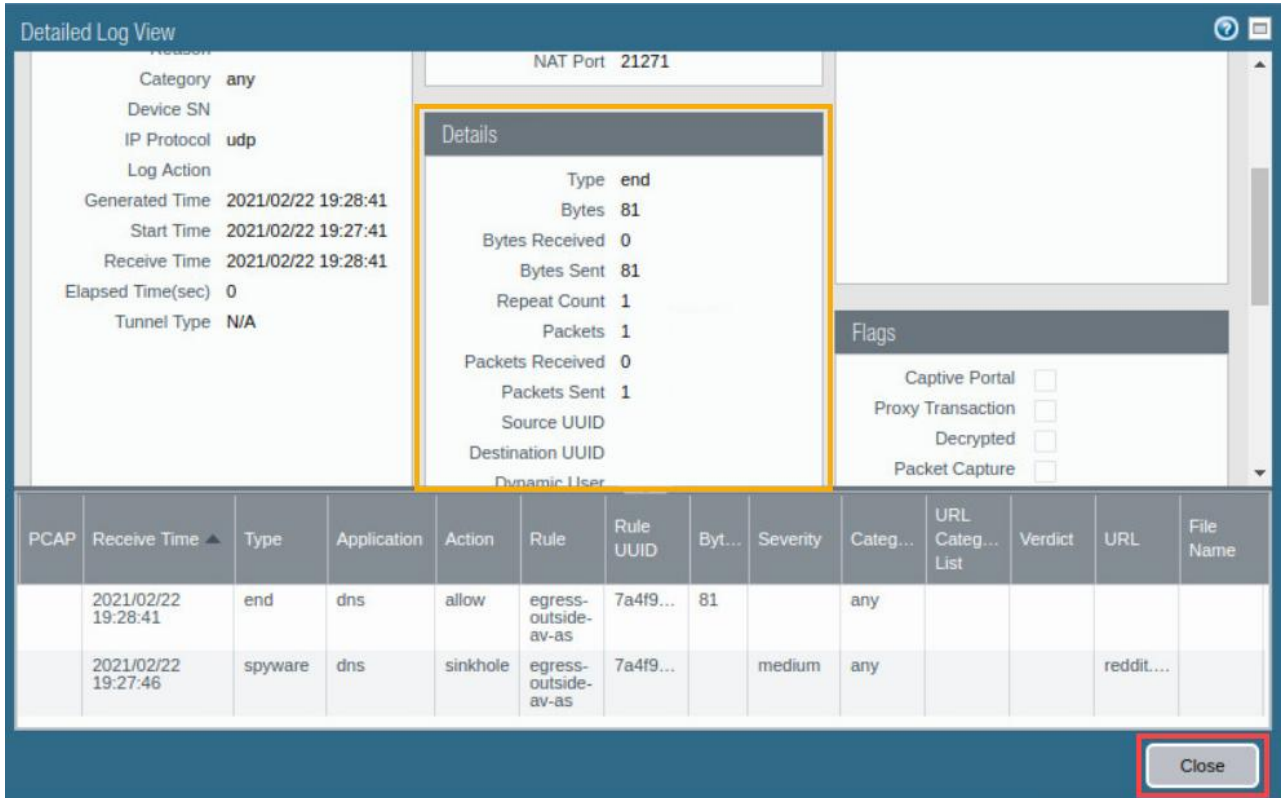
2. To find the DNS request in the Traffic log, use the following filter statement `(addr.dst in 8.8.8.8) and (session_end_reason eq threat)` and then press **Enter**.



| | Receive Time | Type | From Zone | To Zone | Source | Source User | Destination |
|---|----------------|------|-----------|---------|--------------|-------------|-------------|
|  | 02/22 19:28:41 | end | inside | outside | 192.168.1.20 | | 8.8.8.8 |
|  | 02/22 19:28:41 | end | inside | outside | 192.168.1.20 | | 8.8.8.8 |
|  | 02/22 19:28:19 | end | inside | outside | 192.168.1.20 | | 8.8.8.8 |
|  | 08/31 20:45:37 | end | inside | outside | 192.168.1.20 | | 8.8.8.8 |
|  | 08/31 20:45:37 | end | inside | outside | 192.168.1.20 | | 8.8.8.8 |

3. Click the **magnifying glass** icon  next to one of the entries to see the *Detailed Log View*.

- 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

Reason:

Category: any
Device SN:
IP Protocol: udp
Log Action:
Generated Time: 2021/02/22 19:28:41
Start Time: 2021/02/22 19:27:41
Receive Time: 2021/02/22 19:28:41
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:
Dynamic User:

Flags

Captive Portal ☐
Proxy Transaction ☐
Decrypted ☐
Packet Capture ☐

| PCAP | Receive Time ▲ | Type | Application | Action | Rule | Rule UUID | Byt... | Severity | Categ... | URL Categ... List | Verdict | URL | File Name |
|------|---------------------|---------|-------------|----------|----------------------|-----------|--------|----------|----------|-------------------|---------|-----------|-----------|
| | 2021/02/22 19:28:41 | end | dns | allow | egress-outside-av-as | 7a4f9... | 81 | | any | | | | |
| | 2021/02/22 19:27:46 | spyware | dns | sinkhole | egress-outside-av-as | 7a4f9... | | medium | any | | | reddit... | |

Close

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