



PALO ALTO NETWORKS - EDU-210

Lab 5.2: Content ID Malware/Virus Protection

Document Version: 2017-09-29

Copyright © 2017 Network Development Group, Inc.
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. EMC² is a registered trademark of EMC Corporation.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
5.2 Lab: Interface Configuration	6
5.2.0 Load Lab Configuration.....	6
5.2.10 Create Security Policy Rule with a Vulnerability Protection Profile	7
5.2.11 Test Security Policy Rule	9
5.2.12 Review Logs	10
5.2.13 Update Vulnerability Profile	11
5.2.14 Group Security Profiles.....	13
5.2.15 Create a File Blocking Profile	17
5.2.16 Modify Security Profile Group	17
5.2.17 Test the File Blocking Profile	19
5.2.18 Multi-Level-Encoding.....	19
5.2.19 Modify Security Policy Rule	20
5.2.20 Test the File Blocking Profile with Multi-Level-Encoding	21
5.2.21 Modify Security Policy Rule	22
5.2.22 Test the File Blocking Profile with Multi-Level-Encoding	22
5.2.23 Create Danger Security Policy Rule	23
5.2.24 Generate Threats.....	25
5.2.25 Modify Security Profile Group	27
5.2.26 Generate Threats.....	28

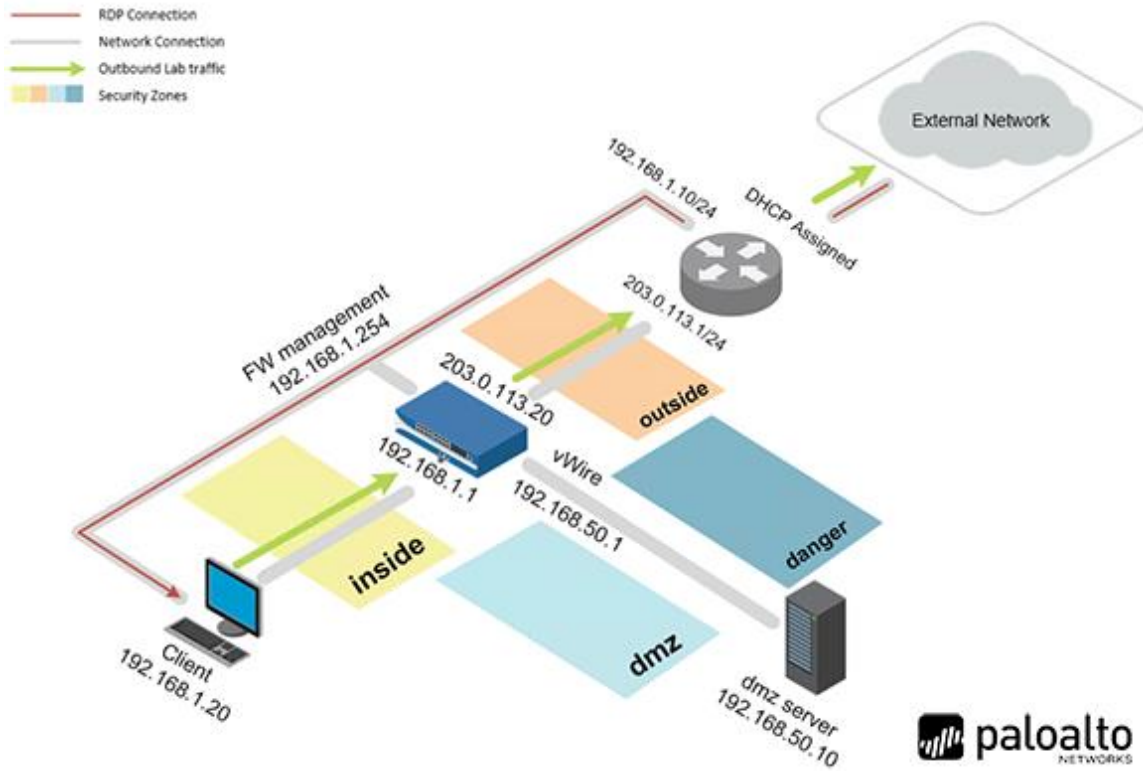
Introduction

We have enabled virus scanning and spyware blocking. Now we need to look at block users from downloading certain types of files and stopping exploits. We can do this with file blocking and vulnerability profiles.

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

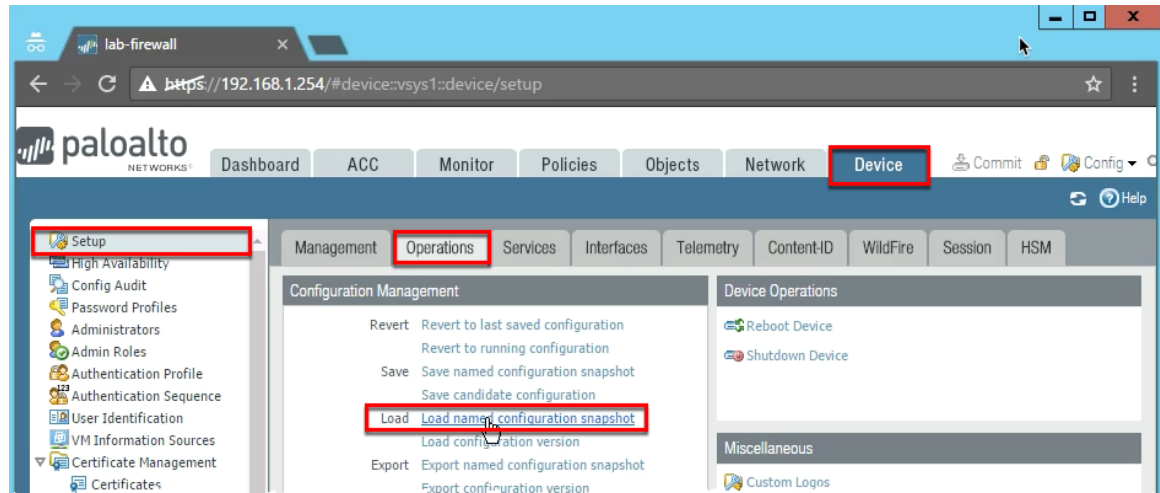
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

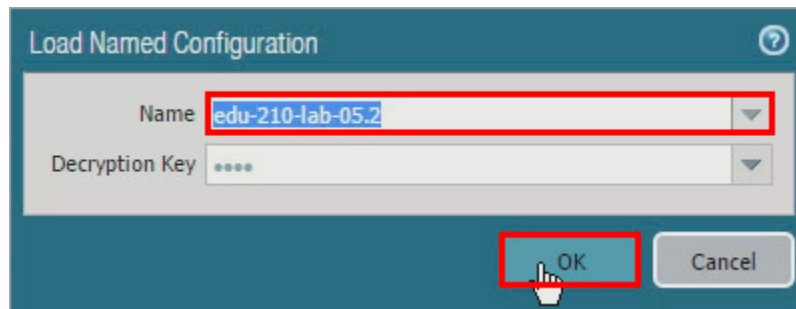
5.2 Lab: Interface Configuration

5.2.0 Load Lab Configuration

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



3. Select **edu-210-lab-05.2** and click **OK**.

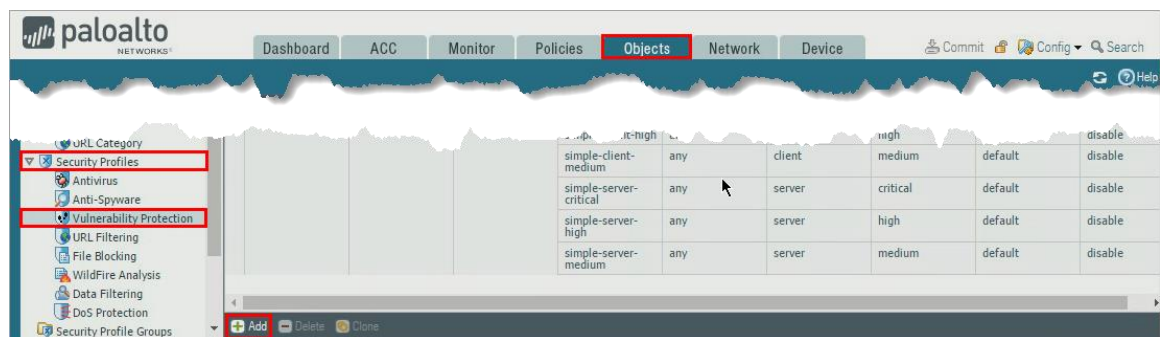


4. Click **Close**.
5. **Commit** all changes.

5.2.10 Create Security Policy Rule with a Vulnerability Protection Profile

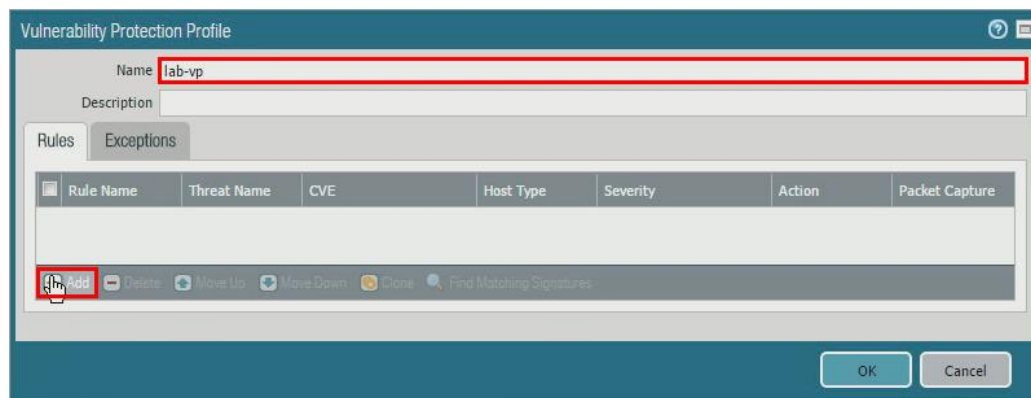
A Security policy rule can include specification of a Vulnerability Protection Profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

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



2. On the Vulnerability Protection Profile window configure the following, then under the Rules tab click **Add**.

Parameter	Value
Name	lab-vp



3. Configure the following then click **OK** twice.

Parameter	Value
Name	lab-vp-rule
Packet Capture	single-packet
Severity	any

Vulnerability Protection Rule

Rule Name: **lab-vp-rule**

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

Action: Default

Host Type: any

Packet Capture: **single-packet**

Category: any

Severity:

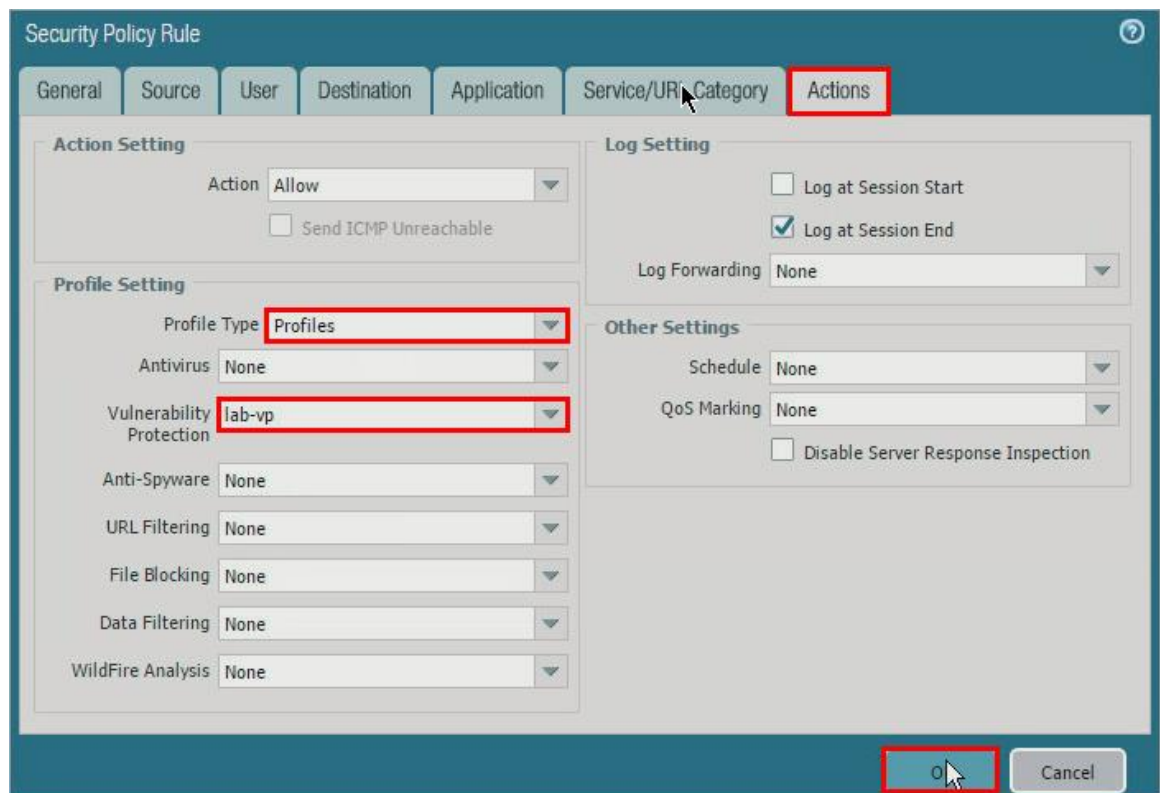
- ☒ any (All severities)
- ☐ critical
- ☐ high
- ☐ medium
- ☐ low
- ☐ informational

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK Cancel

4. Select **Policies > Security**.
5. Click to open the **internal-inside-dmz** Security policy rule.
6. Click the **Actions** tab and configure the following then click **OK**.

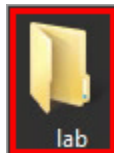
Parameter	Value
Profile Type	Profiles
Profile Setting	
Vulnerability Protection	lab-vp



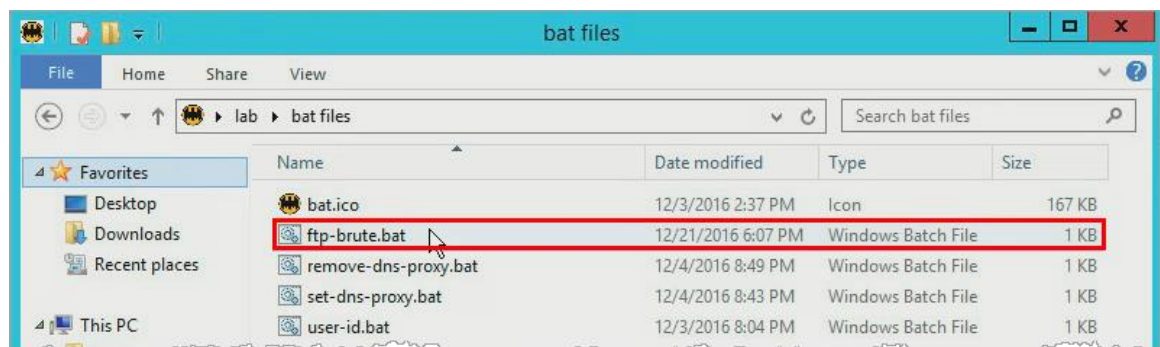
7. **Commit** all changes.

5.2.11 Test Security Policy Rule

1. On the Windows desktop, double-click the **lab** folder and then the bat files folder.



2. Double-click **ftp-brute.bat** and wait until you see the *Press any key to continue...* response before continuing.



```
C:\Users\lab-user\Desktop\lab\bat files>nmap --script ftp-brute 192.168.50.10 -p 21

Starting Nmap 7.31 ( https://nmap.org ) at 2017-09-08 23:11 Coordinated Universal Time
Nmap scan report for 192.168.50.10
Host is up (0.0010s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-brute:
|_ Accounts: No valid accounts found
|_ Statistics: Performed 1255 guesses in 604 seconds, average tps: 2.1

Nmap done: 1 IP address (1 host up) scanned in 605.29 seconds
C:\Users\lab-user\Desktop\lab\bat files>pause
Press any key to continue . . .
```

Note: This action launches an FTP brute force attack at the DMZ FTP server. The script is expected to take about 10 minutes to complete.

5.2.12 Review Logs

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

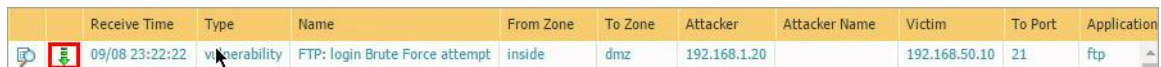


The screenshot shows the Palo Alto Networks Monitor interface. The 'Monitor' tab is selected. In the left sidebar, 'Logs' is expanded, and 'Threat' is selected. The main area displays a table of threat logs. The first three rows are highlighted with a red box, showing 'FTP: login Brute Force attempt' with a severity of 'high'.

From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high		
inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high		
inside	dmz	192.168.1.20		192.168.50.10	21	ftp	alert	high		

Notice that you now have logs reflecting the FTP brute force attempt. However, the firewall is only set to alert.

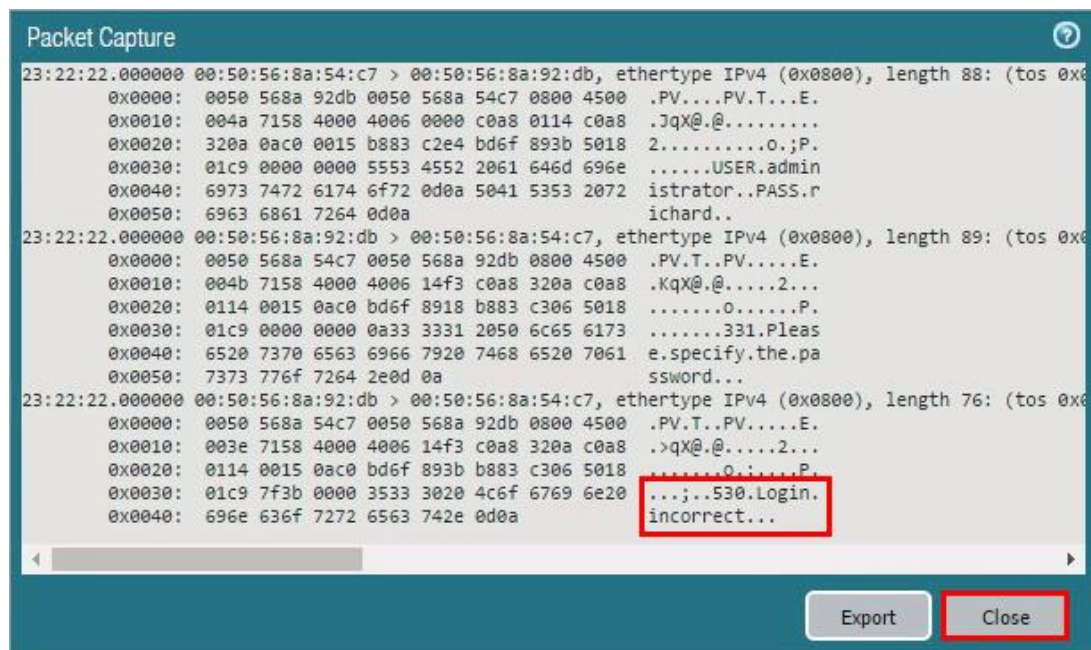
2. Click the **Download Packet Capture** icon to the left of any log entry to open the packet capture.



The screenshot shows a close-up of the log entry from the previous table. A red box highlights the 'Download Packet Capture' icon (a green download arrow) located to the left of the first log entry.

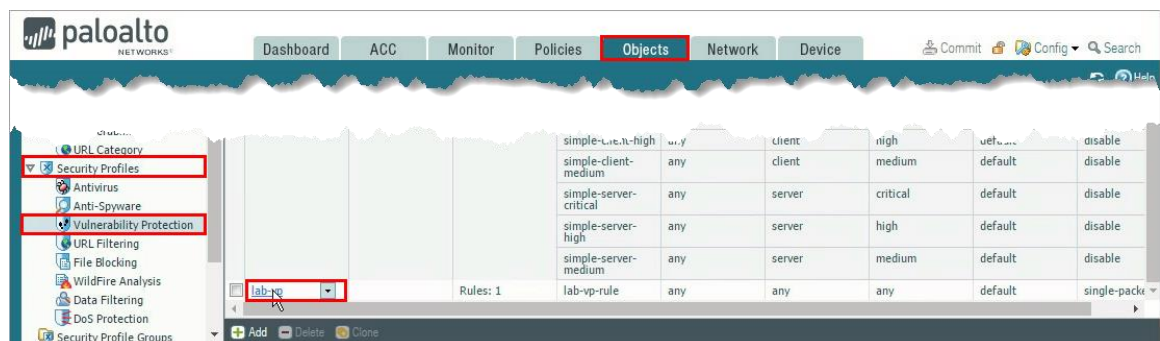
Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application
09/08 23:22:22	vulnerability	FTP: login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp

Notice the username and password that was attempted along with the 530 response from the FTP server.



5.2.13 Update Vulnerability Profile

1. Select **Objects > Security Profiles > Vulnerability Protection** then click **lab-vp** to open the profile.



2. Click to open the **lab-vp-rule** rule and configure the following:

Parameter	Value
Action	Reset Both
Severity	high

Vulnerability Protection Rule

Rule Name:

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

Action: Packet Capture:

Host Type: Category:

☒ Any
☐ CVE

☒ Any
☐ Vendor ID

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

Severity:

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

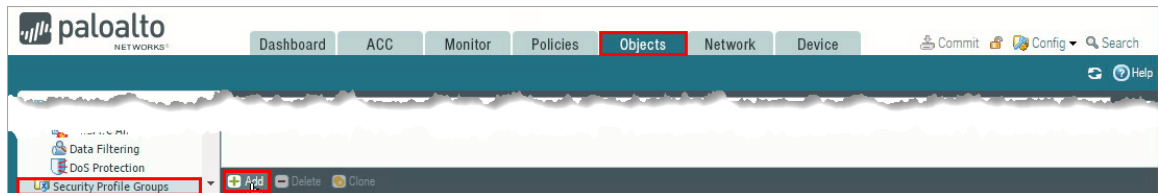
- Click **OK** twice.
- Commit** all changes.
- Rerun **ftp-brute.bat** and review the logs to confirm that the new FTP brute force attempts are reset.

	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	reset-both	high		
Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	reset-both	high		

5.2.14 Group Security Profiles

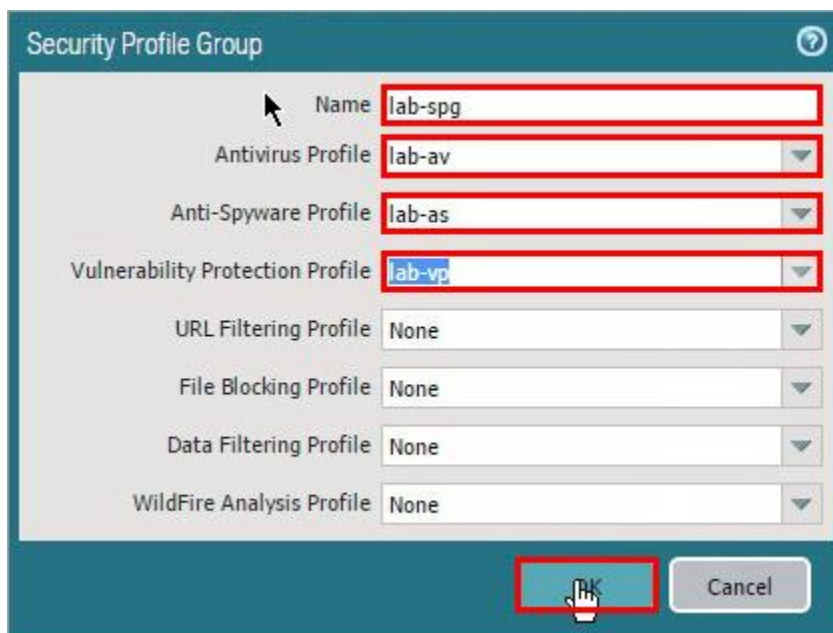
The firewall supports the ability to create Security Profile Groups, which specify sets of Security Profiles that can be treated as a unit and then added to Security policy rules.

1. Select **Objects > Security Profile Groups** then click **Add** to open the Security Profile Group configuration window.



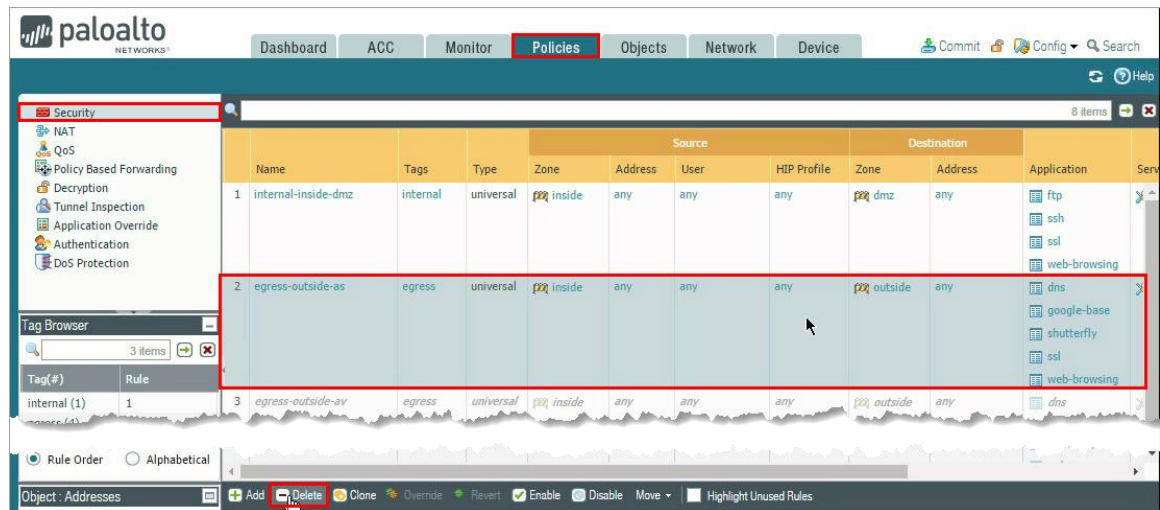
2. Configure the following then click **OK**.

Parameter	Value
Name	lab-spg
Antivirus Profile	lab-av
Anti-Spyware Profile	lab-as
Vulnerability Protection Profile	lab-vp

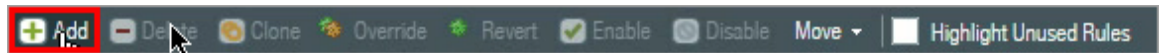


3. Select **Policies > Security**.
4. Click the **Delete** button after selecting each of the following rules.

Parameter	Value
Security Policy Rules	egress-outside-as egress-outside-av

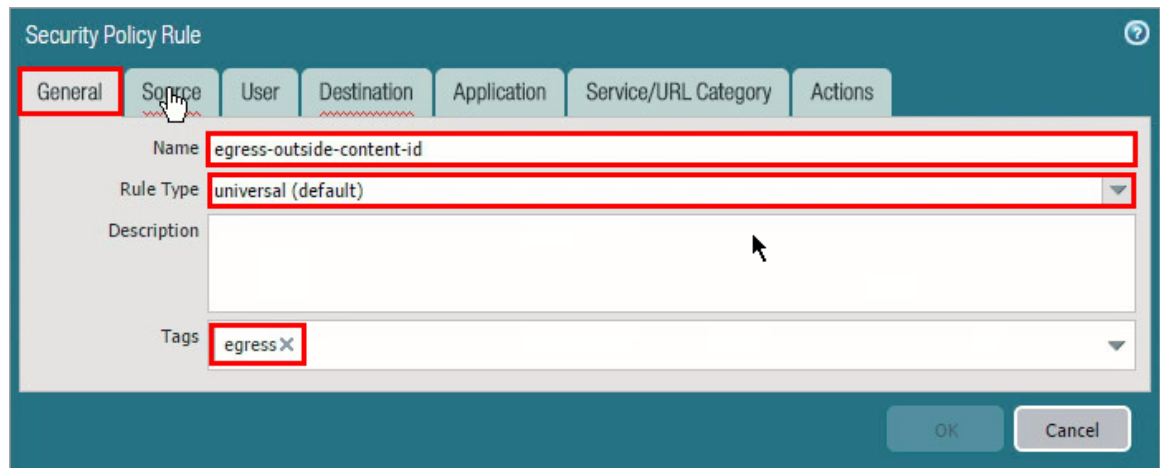


5. Click **Add** to define a Security policy rule.



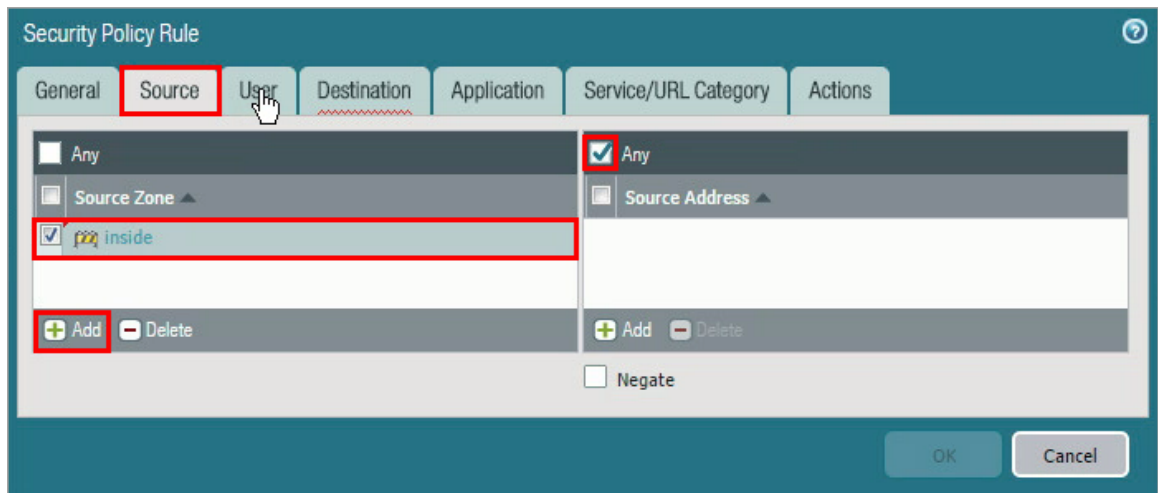
6. Under the **General** tab configure the following.

Parameter	Value
Name	egress-outside-content-id
Rule Type	universal (default)
Tags	egress



7. Click the **Source** tab and configure the following.

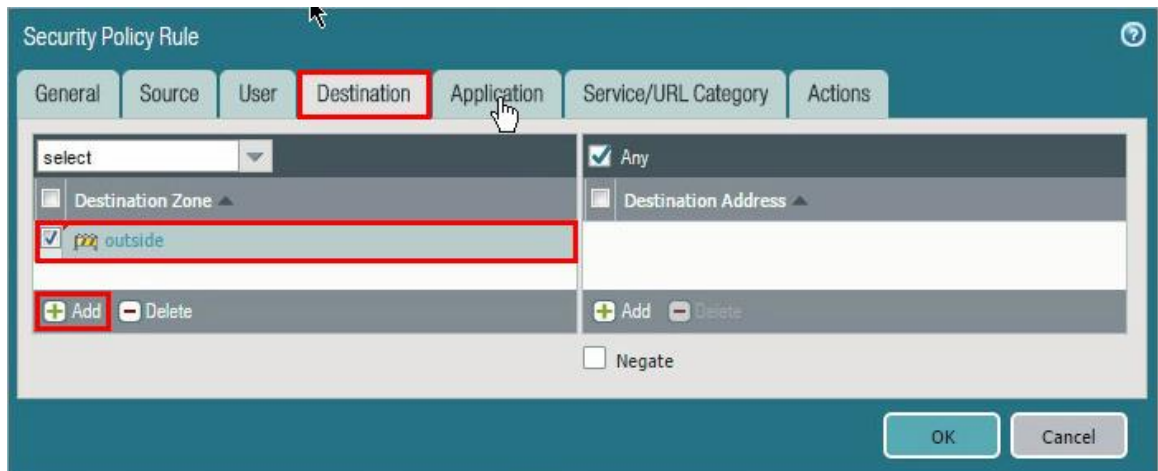
Parameter	Value
Source Zone	inside
Source Address	Any



The screenshot shows the 'Security Policy Rule' configuration window with the 'Source' tab selected. The 'Source Zone' list contains 'Any' and 'inside', with 'inside' selected. The 'Source Address' list contains 'Any', which is also selected. The 'Add' button is highlighted with a red box. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

8. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	outside
Destination Address	Any



The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The 'Destination Zone' list contains 'select', 'outside', and 'inside', with 'outside' selected. The 'Destination Address' list contains 'Any', which is also selected. The 'Add' button is highlighted with a red box. The 'Negate' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

9. Click the **Application** tab and verify that **Any** is checked.
 10. Click the **Service/URL Category** tab and verify that **application-default** is selected.
 11. Click the **Actions** tab to configure the following then click **OK**.

Parameter	Value
Action Setting	Allow
Log Setting	Log at Session End
Profile Setting	
Profile Type	Group
Group Profile	lab-spg

Security Policy Rule

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

Action Setting

Action **Allow**

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding **None**

Profile Setting

Profile Type **Group**

Group Profile **lab-spc**

Other Settings

Schedule **None**

QoS Marking **None**

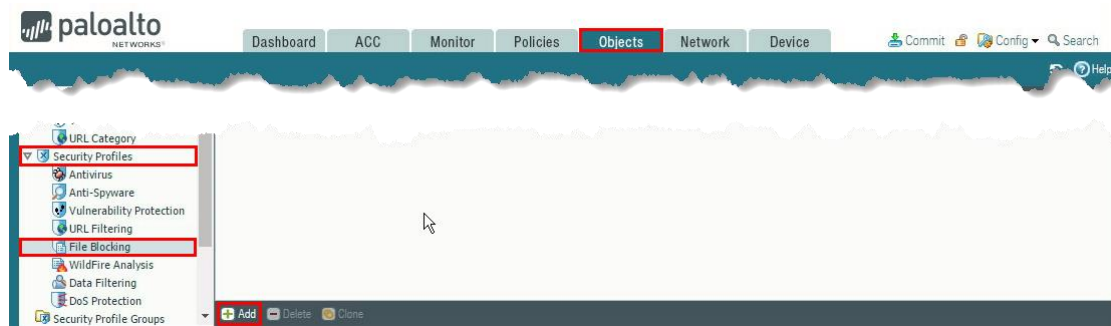
☐ Disable Server Response Inspection

OK Cancel

5.2.15 Create a File Blocking Profile

A Security policy rule can include specification of a File Blocking Profile that blocks selected file types from being uploaded or downloaded, or generates an alert when the specified file types are detected.

1. In the WebUI select **Objects > Security Profiles > File Blocking** then click **Add** to open the File Blocking Profile configuration window.

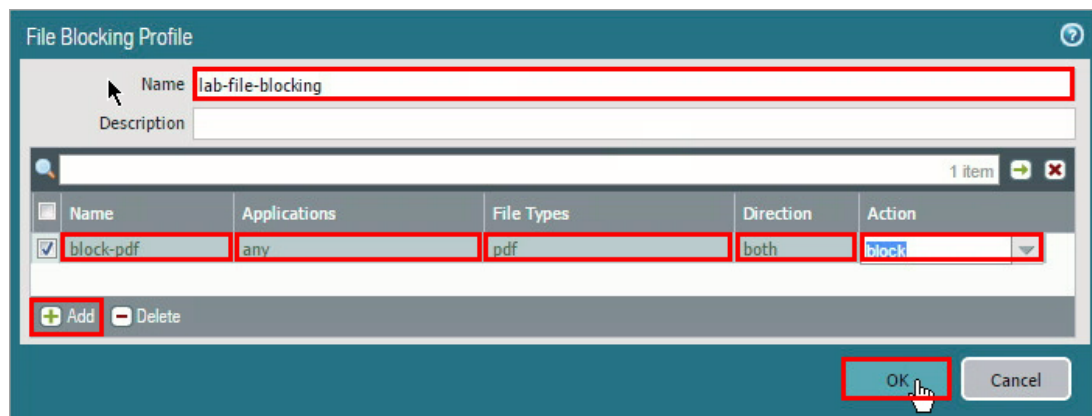


2. In the **File Blocking Profile** window configure the following:

Parameter	Value
Name	lab-file-blocking

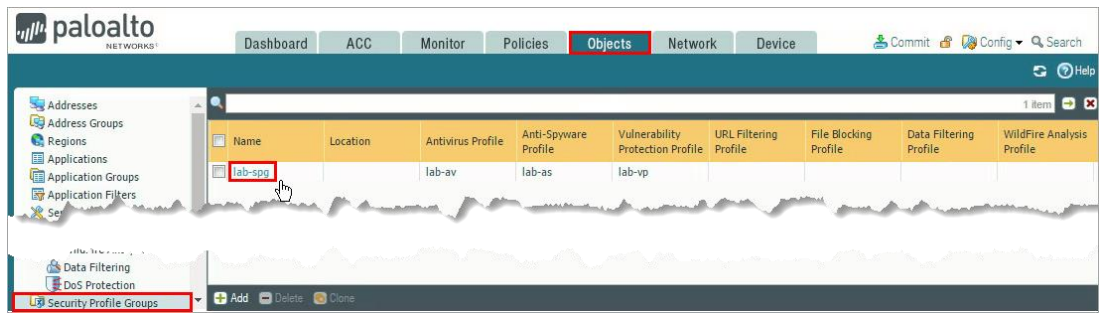
3. Click **Add** and configure the following then click **OK**.

Parameter	Value
Name	block-pdf
Applications	any
File Types	pdf
Direction	both
Action	block

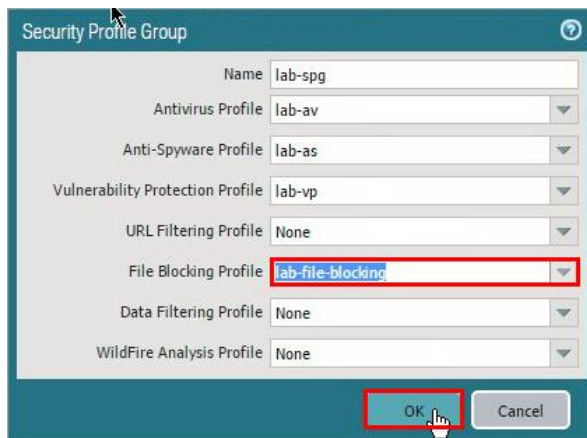


5.2.16 Modify Security Profile Group

1. Select **Objects > Security Profile Groups** then click lab-spg.



2. In the **File Blocking Profile** box select **lab-file-blocking** then click **OK**.



3. **Commit** all changes.

5.2.17 Test the File Blocking Profile

1. Open a new browser window in private/incognito mode and browse to <http://www.panedufiles.com/>.
2. Click the **Panorama_AdminGuide.pdf** link. The download fails.



Note: If you get “failed to download pdf” and not the block page, then refresh the browser window.

3. Select **Monitor > Logs > Data Filtering** then find the log entry for the PDF file that has been blocked.

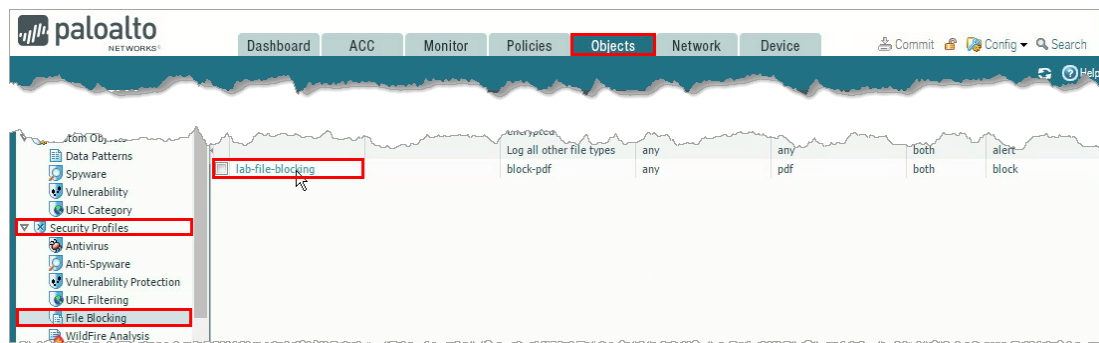


Note: The Action column is located on the far right. The column can be moved via drag-and-drop using the mouse cursor.

5.2.18 Multi-Level-Encoding

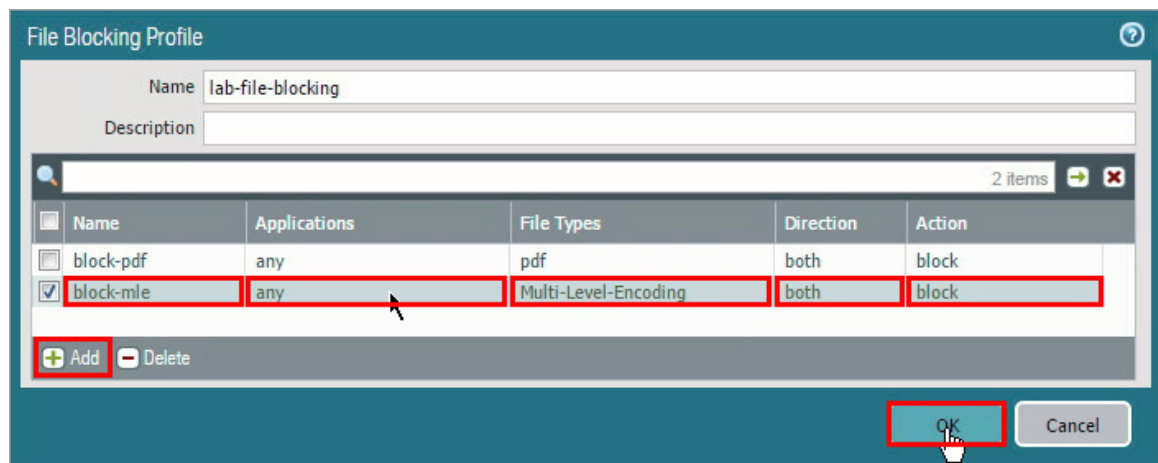
Multi-Level-Encoding can be used to block content that is not inspected by the firewall because of the file being encoded five or more times.

1. In the WebUI select **Objects > Security Profiles > File Blocking**.
2. Click to open the **lab-file-blocking** File Blocking Profile.



3. In the File Blocking Profile window click **Add** to configure the following then click **OK**.

Parameter	Value
Name	block-mle
Applications	any
File Types	Multi-Level-Encoding
Direction	both
Action	block



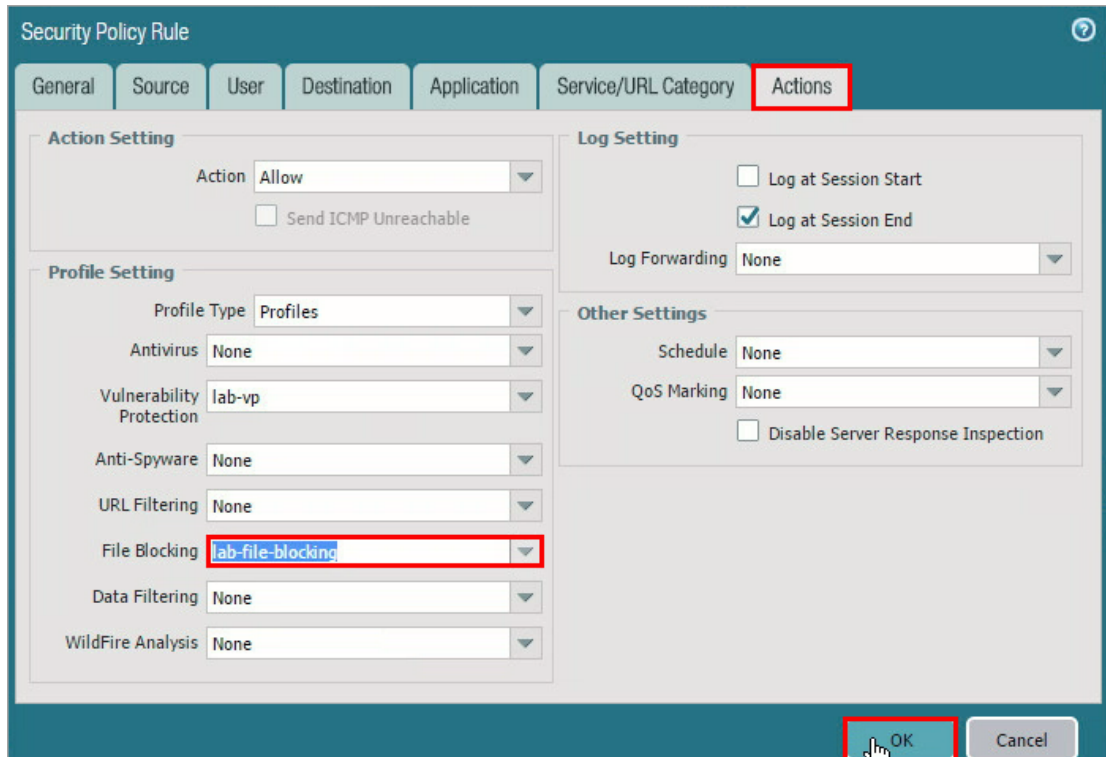
5.2.19 Modify Security Policy Rule

1. In the WebUI select **Policies > Security** click on **internal-inside-dmz** to open the Security policy rule.



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

Parameter	Value
File Blocking	lab-file-blocking



Security Policy Rule

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

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: lab-vp

Anti-Spyware: None

URL Filtering: None

File Blocking: **lab-file-blocking**

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

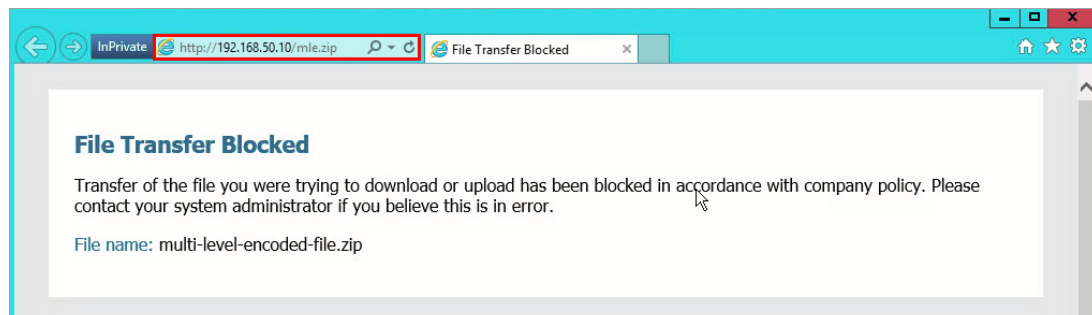
☐ Disable Server Response Inspection

OK Cancel

- Commit** all changes.

5.2.20 Test the File Blocking Profile with Multi-Level-Encoding

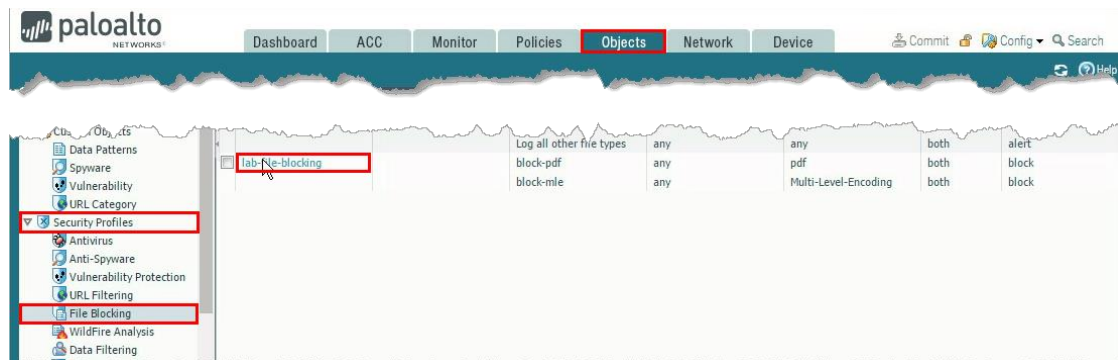
- Open a new browser in private/incognito mode and browse to <http://192.168.50.10/mle.zip>. The URL links to a file that is compressed five times.



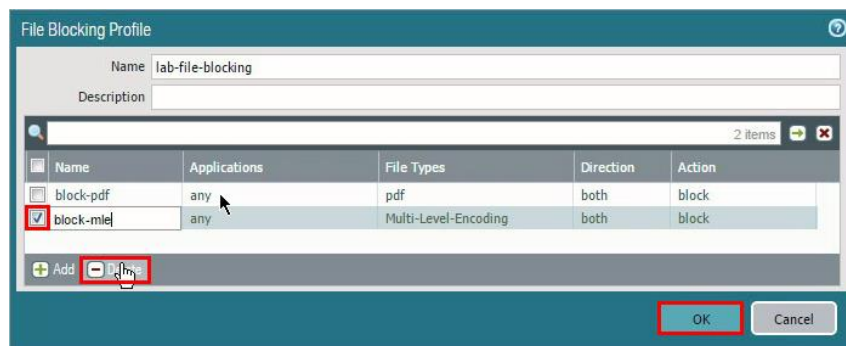
- The file is blocked in accordance with the new file blocking rule.

5.2.21 Modify Security Policy Rule

1. In the WebUI select **Objects > Security Profiles > File Blocking** then click on **lab-file-blocking** to open the File Blocking Profile.



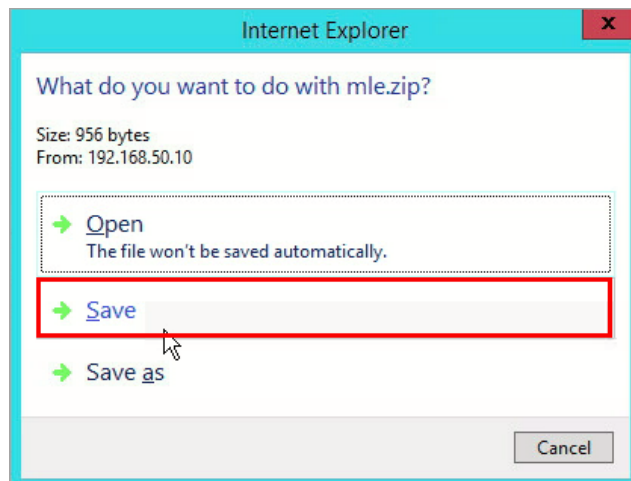
2. Select the **block-mle** rule then click **Delete**.



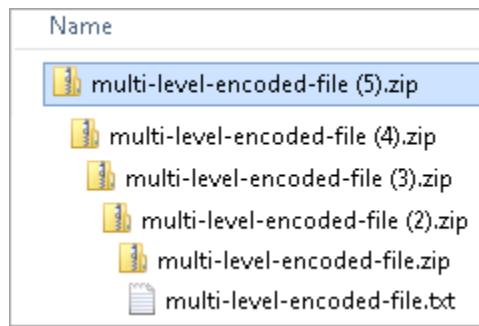
3. Click **OK** to close the File Blocking Profile configuration window.
4. **Commit** all changes.

5.2.22 Test the File Blocking Profile with Multi-Level-Encoding

1. Open a new browser in private/incognito mode and browse to <http://192.168.50.10/mle.zip>. The URL links to a file that is compressed five times. The file is no longer blocked. Save the file.



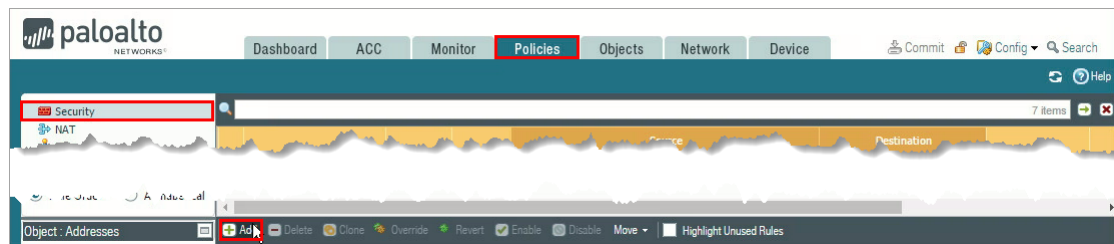
2. Open the file to exam the contents.



5.2.23 Create Danger Security Policy Rule

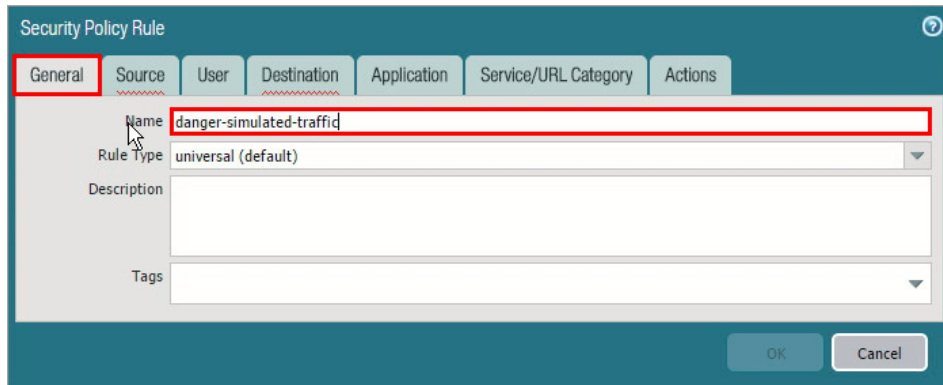
Create a Security policy rule that references the danger Security zone for threat and traffic generation.

1. Select **Policies > Security** then click **Add**.



2. Under the **General** tab configure the following.

Parameter	Value
Name	danger-simulated-traffic



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: danger-simulated-traffic

Rule Type: universal (default)

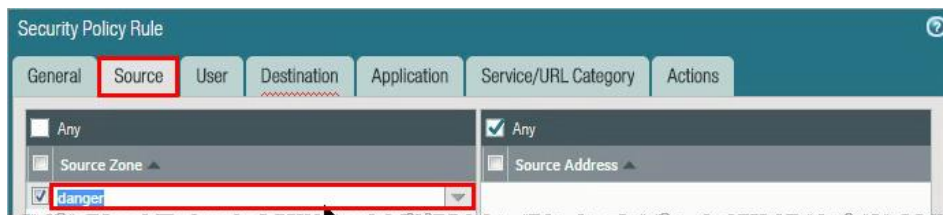
Description:

Tags:

OK Cancel

3. Under the **Source** tab and configure the following.

Parameter	Value
Source Zone	danger



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone

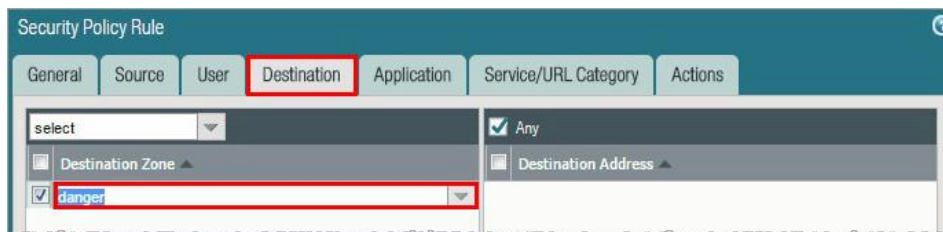
danger

Any

Source Address

4. Under the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	danger



Security Policy Rule

General Source User Destination Application Service/URL Category Actions

select

Destination Zone

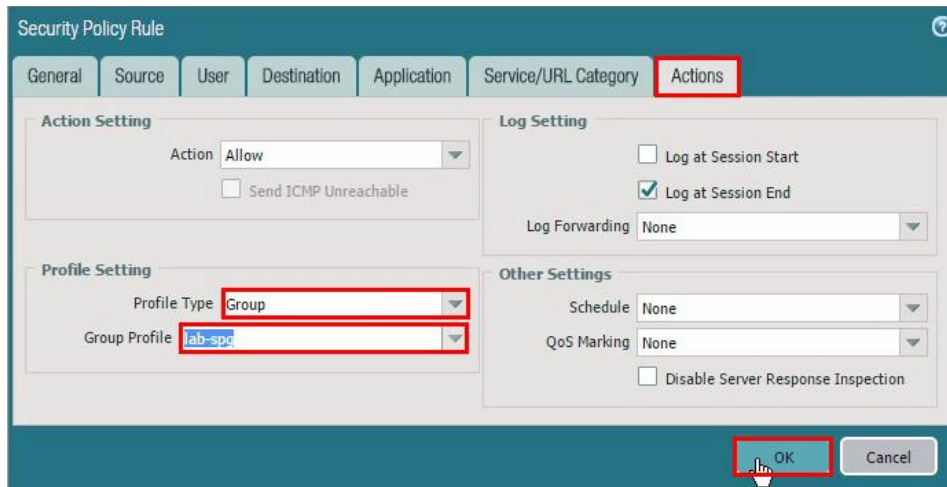
danger

Any

Destination Address

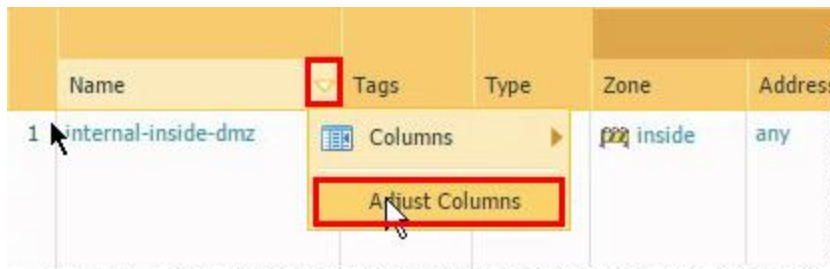
5. Under the **Actions** tab and configure the following then click **OK**.

Parameter	Value
Profile Type	group
Group Profile	lab-spg



The image shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action' is set to 'Allow'. Under 'Profile Setting', 'Profile Type' is 'Group' and 'Group Profile' is 'lab-spc'. Under 'Log Setting', 'Log at Session End' is checked. Under 'Other Settings', 'Schedule' and 'QoS Marking' are both set to 'None'. The 'OK' button is highlighted with a red box and a mouse cursor.

6. Hover over the Name column header and select Adjust Columns from the drop-down list.



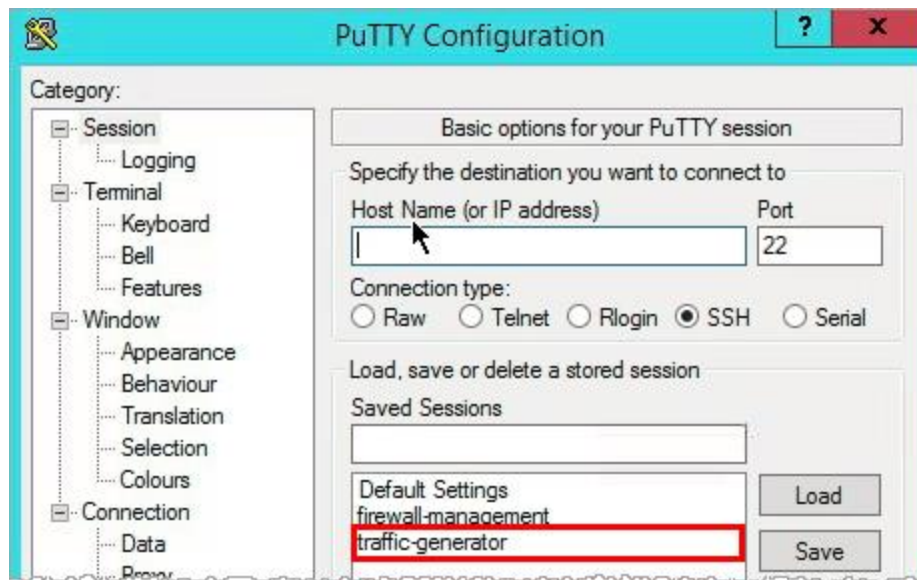
Notice that the width of all the columns were adjusted to fit the text in the columns.

7. **Commit** all changes.

5.2.24 Generate Threats

1. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.





2. Enter the following information when prompted:

Parameter	Value
Password	Pa10Alt0

```
Using username "root".
root@192.168.50.10's password: 
```

3. In the PuTTY window, type the command `sh /tg/malware.sh`

```
Using username "root".
root@192.168.50.10's password:
Last login: Tue Feb 21 22:43:00 2017
[root@pod-dmz ~]# sh/tg/malware.sh
-bash: sh/tg/malware.sh: No such file or directory
[root@pod-dmz ~]# sh /tg/malware.sh

THIS COULD TAKE UP TO 10 MINUTES
```

Note: The script can take up to 10 minutes to complete. Wait until the script complete prior to continuing.

4. Select **Monitor > Logs > Threat** then type the following filter (`severity neq informational`) and execute.



5. Notice the threats currently listed from the generated traffic.
6. Select **Monitor > Logs > Data Filtering**.



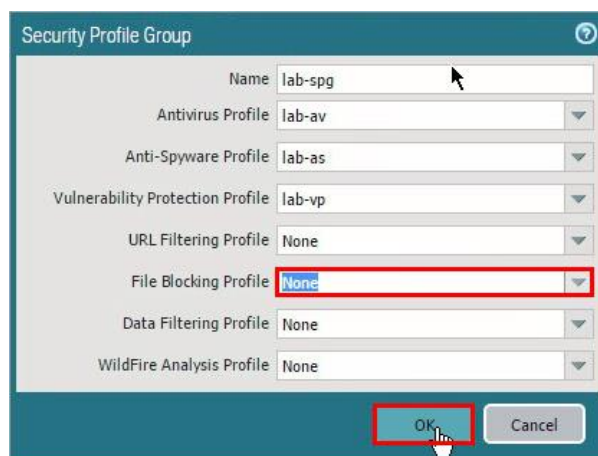
7. Notice the blocked files.

5.2.25 Modify Security Profile Group

1. Select **Objects > Security Profile Groups** then click on **lab-spg** to open the Security Profile Group.



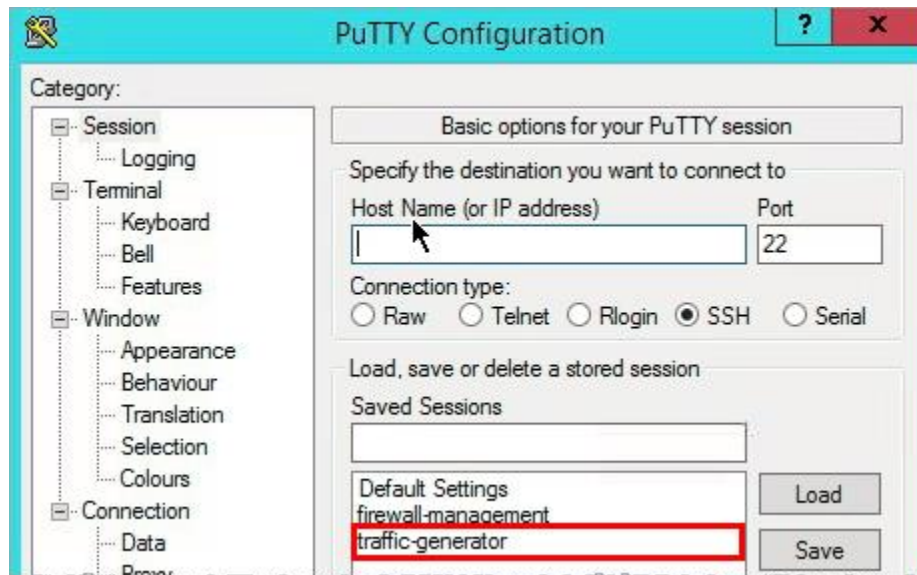
2. Set the File Blocking Profile field to **None** then click **OK**.



3. **Commit** all changes.

5.2.26 Generate Threats

1. On the Windows desktop, open **PuTTY** and double-click **traffic-generator**.



2. Enter the following information when prompted.

Parameter	Value
Password	Pa10A1t0

```
Using username "root".
root@192.168.50.10's password: 
```

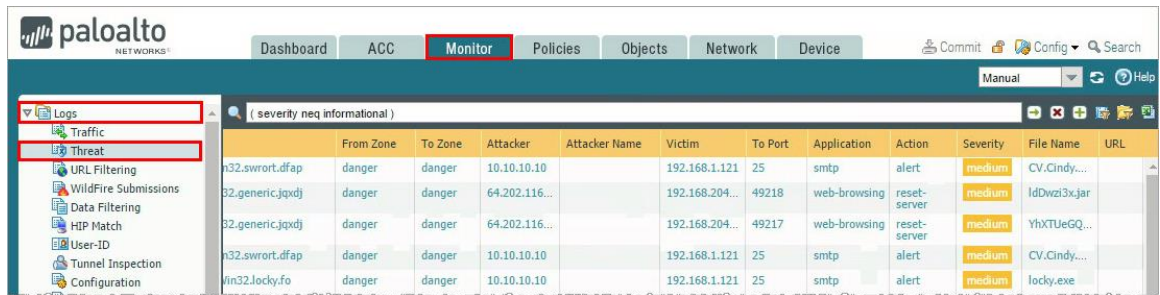
3. In the **PuTTY** window, type the command `sh /tg/malware.sh`

```
Using username "root".
root@192.168.50.10's password:
Last login: Tue Feb 21 22:43:00 2017
[root@pod-dmz ~]# sh/tg/malware.sh
-bash: sh/tg/malware.sh: No such file or directory
[root@pod-dmz ~]# sh /tg/malware.sh

THIS COULD TAKE UP TO 10 MINUTES
```

Note: The script can take up to 10 minutes to complete. Wait until the script complete prior to continuing.

4. Select **Monitor > Logs > Threat** then input the following filter (`severity neq informational`) and execute.



	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Name	URL
n32.swrort.dfap	danger	danger	10.10.10.10		192.168.1.121	25	smtp	alert	medium	CV.Cindy....	
32_generic.jqxdj	danger	danger	64.202.116...		192.168.204...	49218	web-browsing	reset-server	medium	ldDwzi3x.jar	
32_generic.jqxdj	danger	danger	64.202.116...		192.168.204...	49217	web-browsing	reset-server	medium	YhXTUeGQ...	
n32.swrort.dfap	danger	danger	10.10.10.10		192.168.1.121	25	smtp	alert	medium	CV.Cindy....	
lin32.locky.fo	danger	danger	10.10.10.10		192.168.1.121	25	smtp	alert	medium	locky.exe	

5. Notice the blocked files.

Stop. This is the end of the 5.2 Content ID Malware/Virus Protection lab.