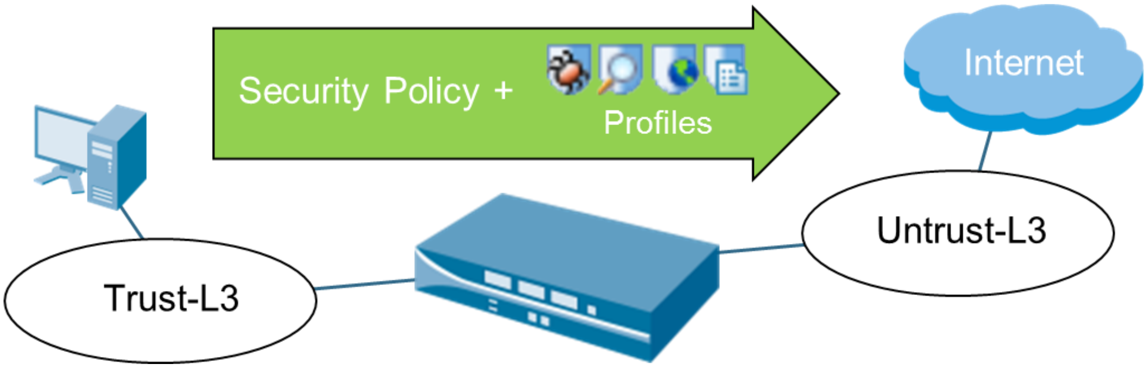
PAN-OS 7.0 FIREWALL ESSENTIALS
LAB SERIES

Lab 6: Anti-Virus & Anti-Spyware Profiles

Document Version: 2016-04-19

Contents

Introduction



Now that traffic is passing through the firewall, you decide to further protect the environment with security profiles. The specific security requirements for general Internet traffic are:

- Log, but do not block, all viruses detected and maintain packet captures of these events for analysis.
- Log spyware of severity levels medium, critical and high. Ignore all other spyware.
- After all of these profiles are configured, assign them to a security profile group, and assign the profile group to the security policy rule.
- Then, send test traffic to verify that the protection behaves as expected. Test the antivirus profile by downloading a file over http from eicar.org. After the initial testing is complete, you will be asked to change the antivirus protection to block viruses. Make the changes and verify the difference in behavior.

Lab Notes

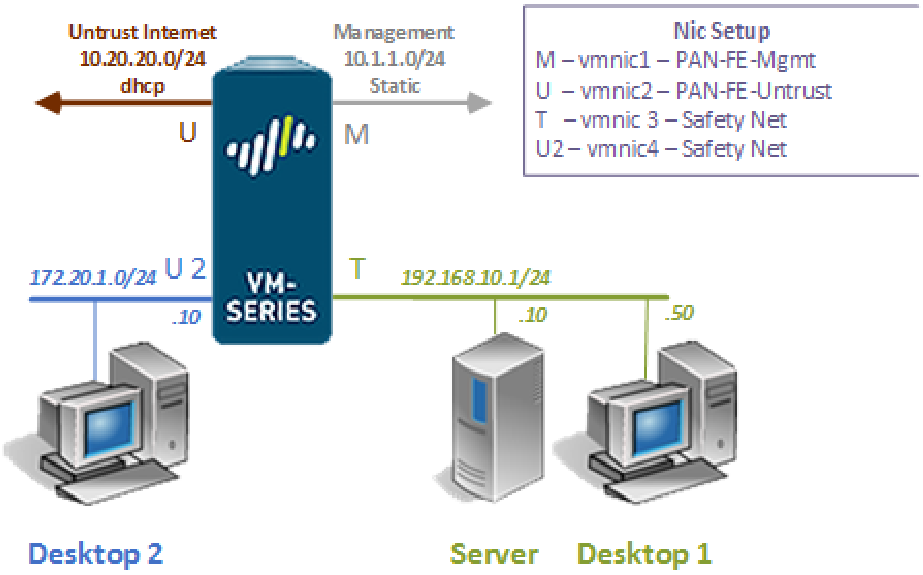
Test the antivirus profile using http and not https because decryption has not been configured on the firewall yet. Https connections will prevent the firewall from seeing the packet contents so the viruses contained will not be detected by the profile.

Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Configure security profiles
2. Create a security profile group
3. Associate the security profile group to security policy rule

Pod 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)
Ubuntu Desktop 1	192.168.10.50	sysadmin	Train1ng$
Ubuntu Server	192.168.10.10	sysadmin	Train1ng$
Ubuntu Desktop 2	172.30.1.10	sysadmin	Train1ng$
Palo Alto Firewall	192.168.10.1 172.30.1.1	admin	paloalto

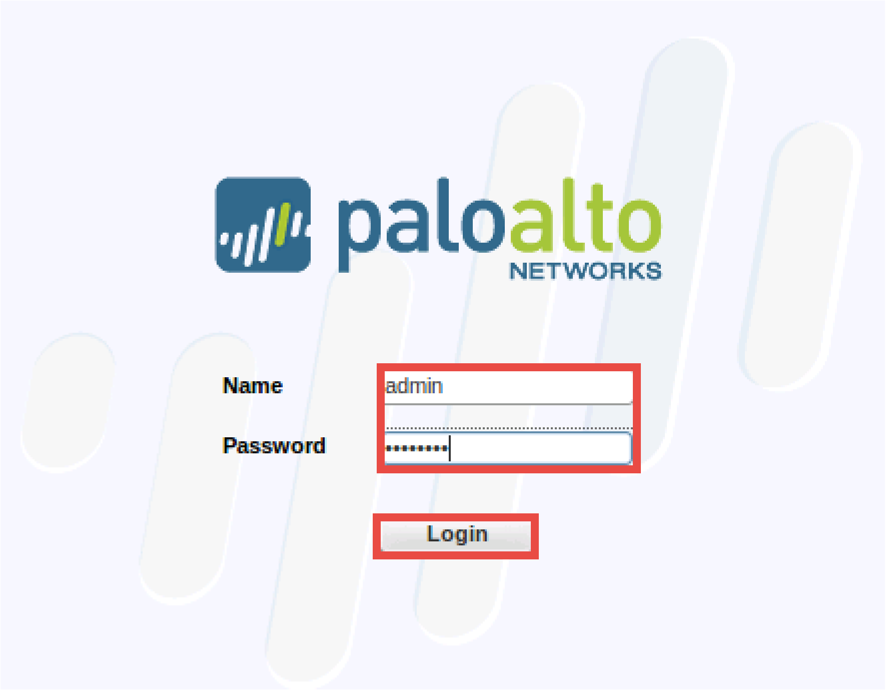
1 Initial Setup

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using `sysadmin` as the *username* and `Train1ng$` as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.

4. In the address field, type `https://192.168.10.1` and press **Enter**.

> If you experience the "*Unable to connect*" message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

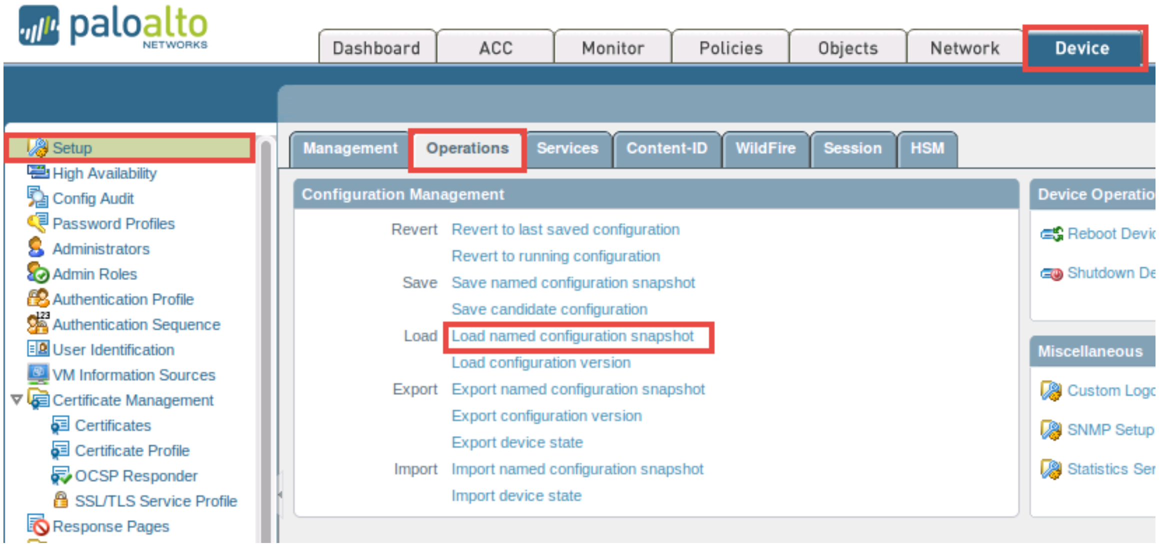
5. Login with the *username* `admin` and *password* `paloalto` on the firewall web interface.



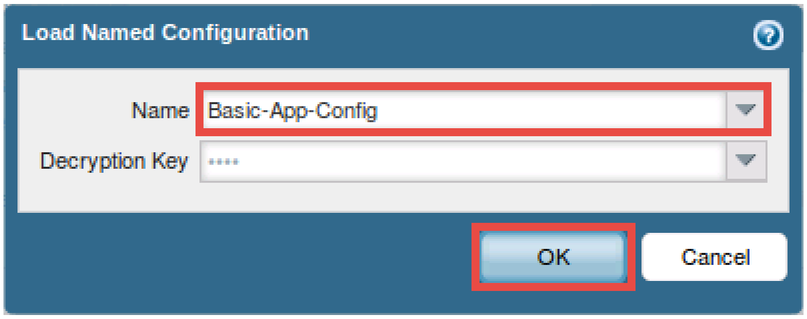
Name admin

Password ••••••••

6. Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.

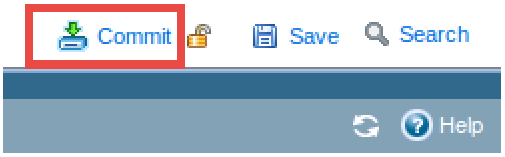


7. In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.

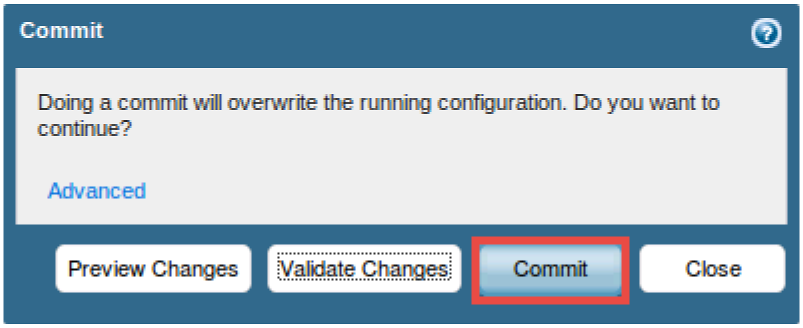


Name: Basic-App-Config
Decryption Key: ••••

8. When prompted with the config loaded message, click on the **Close** button to continue.
9. Click on the **Commit** link located at the top-right of the *WebUI*.



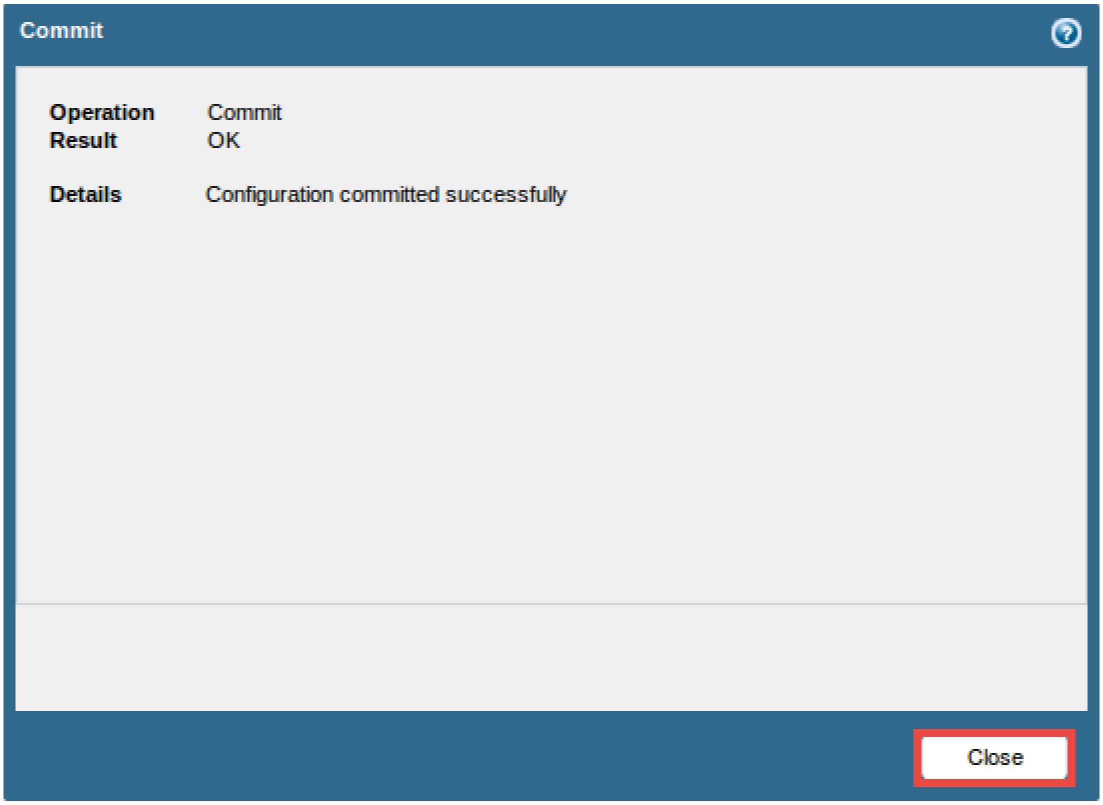
10. In the *Commit* window, click **Commit** to proceed with committing the changes.



Commit

Doing a commit will overwrite the running configuration. Do you want to continue?

11. Once the operation successfully completes, click **Close** to continue.



Commit

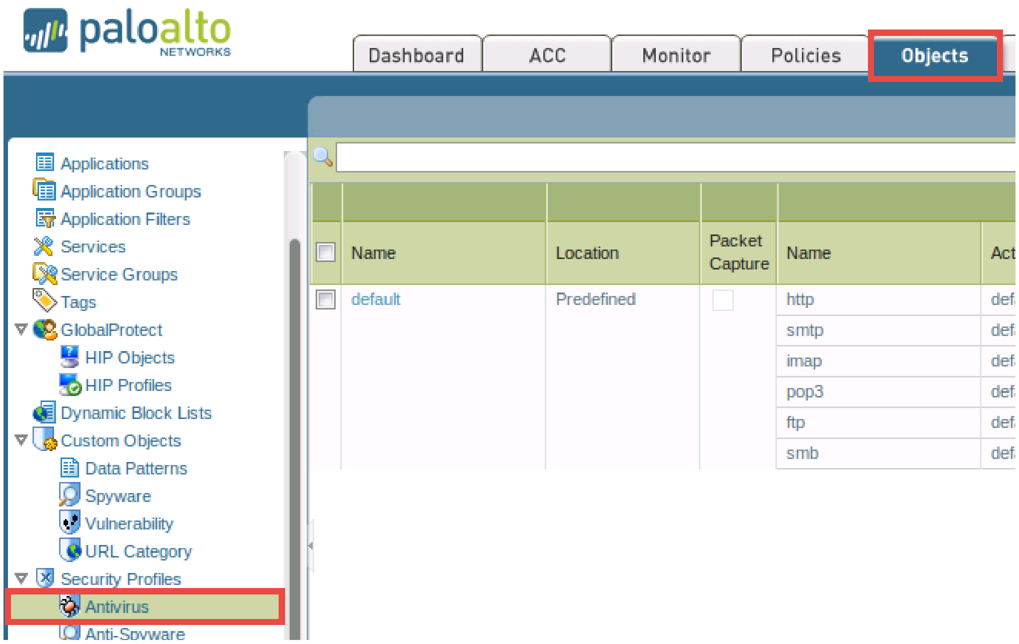
Operation Commit
Result OK

Details Configuration committed successfully

12. Leave the *WebUI* opened to continue with the next task.

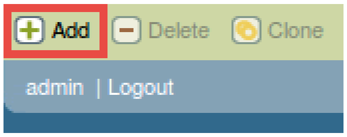
2 Configure an Antivirus Profile

1. Using the *WebUI*, navigate to **Objects > Security Profiles > Anti-Virus**.

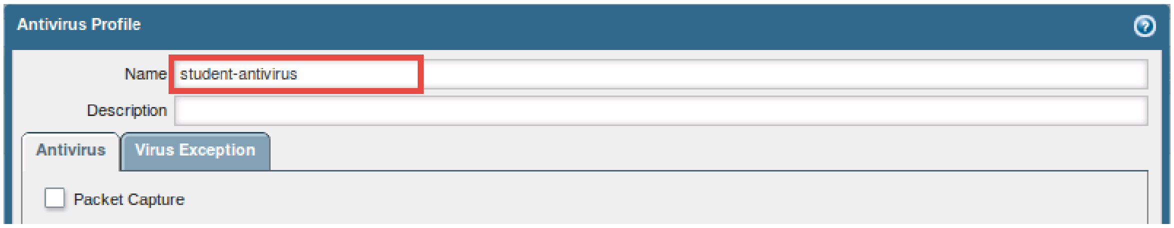


☐ Name	Location	Packet Capture	Name	Act
☐ default	Predefined	☐	http	def
			smtp	def
			imap	def
			pop3	def
			ftp	def
			smb	def

2. Click on **Add**, located near the bottom of the window, to create a new antivirus profile.



3. In the *Antivirus Profile* window, enter **`student-antivirus`** into the *Name* text field.



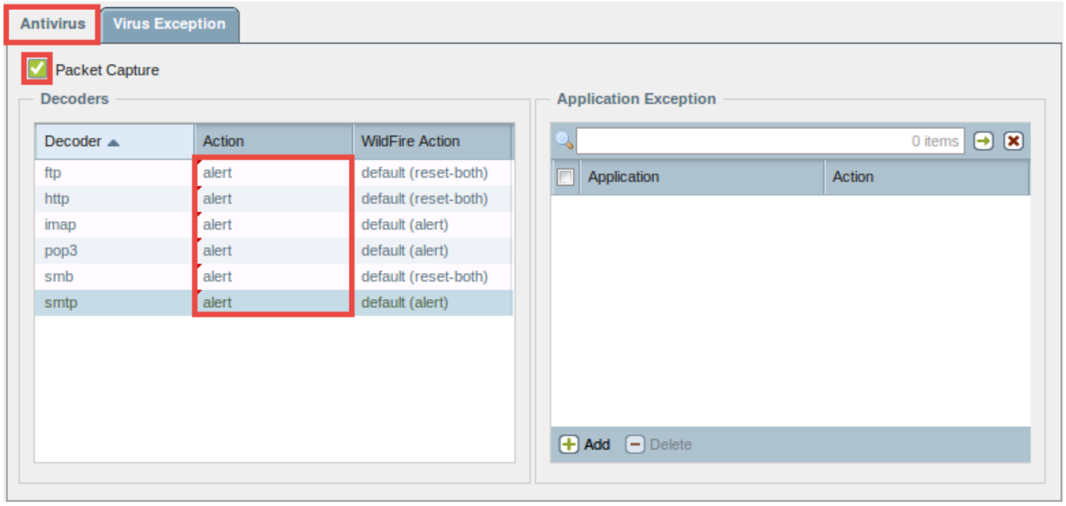
Name student-antivirus

Description

☐ Packet Capture

4. In the *Antivirus Profile* window, select the **Antivirus** tab and use the information from the table below to fill out the form fields.

Field	Data/Selection
Packet Capture	Check the **Packet Capture** box
Decoders	Set the **Action** column to **alert** for all decoders



☑ Packet Capture

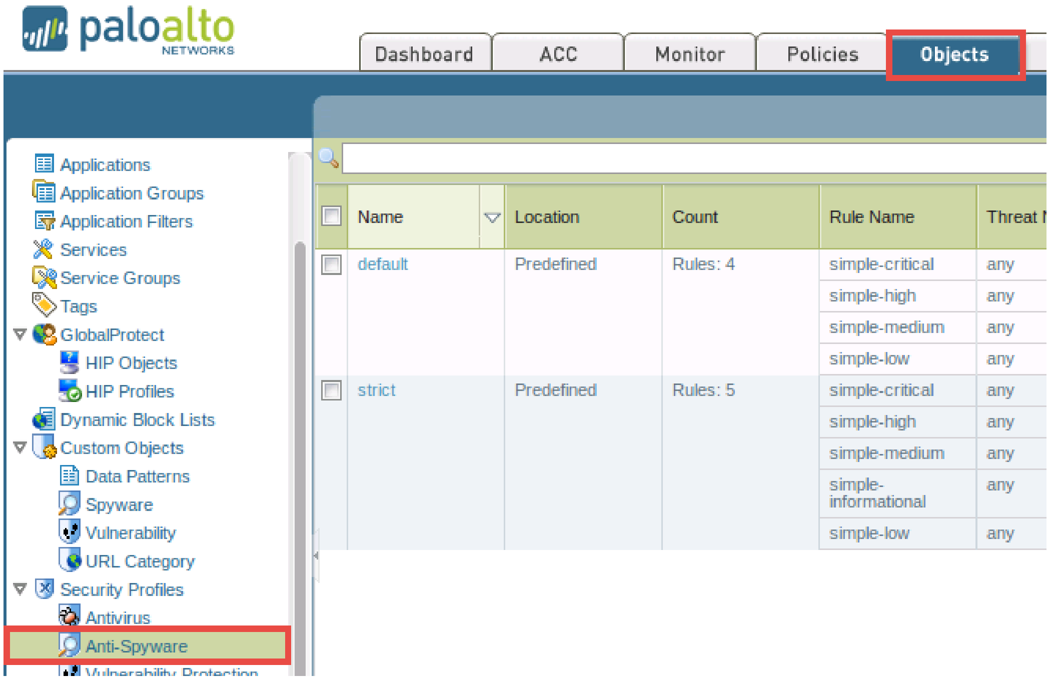
Decoders

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

5. Click **OK** to save changes.
6. Leave the *WebUI* opened to continue with the next task.

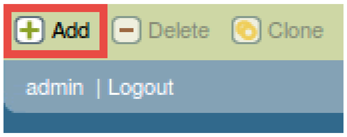
3 Configure an Anti-Spyware Profile

1. Using the *WebUI*, navigate to **Objects > Security Profiles > Anti-Spyware**.

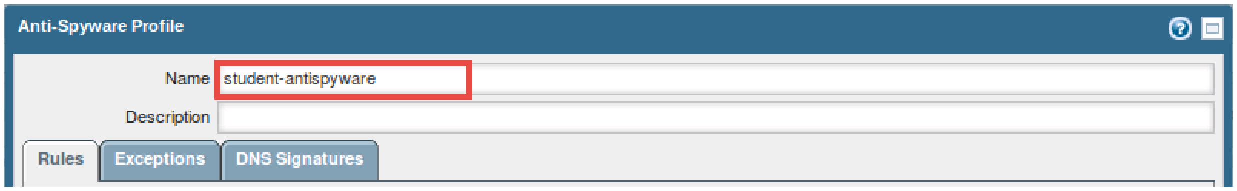


□	Name	Location	Count	Rule Name	Threat N
□	default	Predefined	Rules: 4	simple-critical	any
				simple-high	any
				simple-medium	any
				simple-low	any
□	strict	Predefined	Rules: 5	simple-critical	any
				simple-high	any
				simple-medium	any
				simple-informational	any
				simple-low	any

2. Click on **Add**, located near the bottom of the window, to create a new anti-spyware profile.



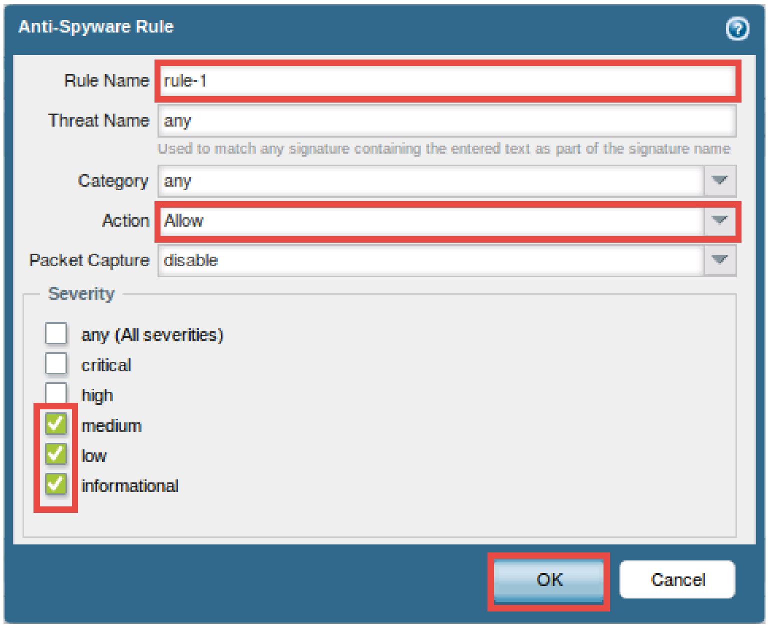
3. In the *Anti-Spyware Profile* window, enter **`student-antispyware`** into the *Name* text field.



Name: student-antispyware

Description:

4. In the *Anti-Spyware Profile* window, select the **Rules** tab and click **Add** to create a rule using the parameters below.
   a. *Rule Name*: **`rule-1`**
   b. *Action*: Select **Allow**
   c. *Severity*: Check the boxes for **informational**, **low**, and **medium**



Anti-Spyware Rule

Rule Name: rule-1

Threat Name: any

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

Category: any

Action: Allow

Packet Capture: disable

Severity

□ any (All severities)

□ critical

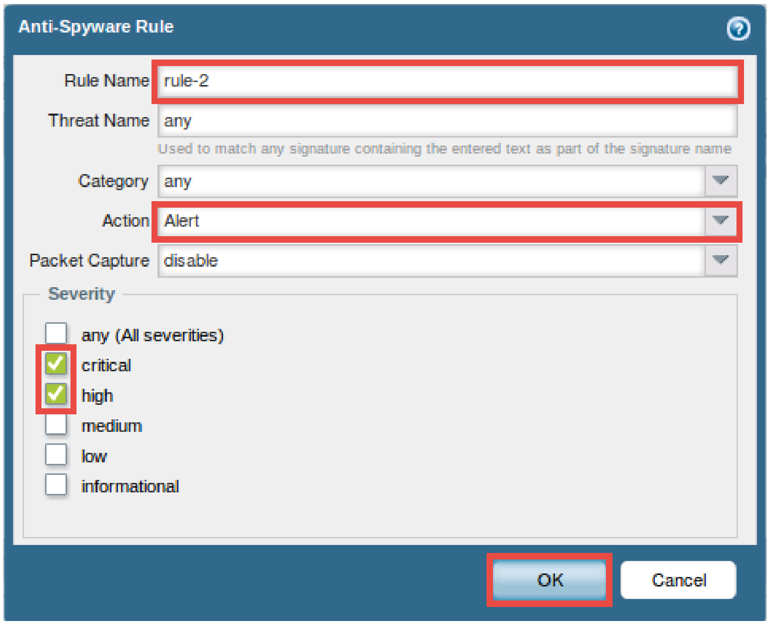
□ high

☑ medium

☑ low

☑ informational

5. Click **OK** to save the rule.
6. In the *Anti-Spyware Profile* window, click **Add** to create another rule using the parameters below.
   a. *Rule Name*: **`rule-2`**
   b. *Action*: Select **Alert**
   c. *Severity*: Check the boxes for **high** and **critical**



Anti-Spyware Rule

Rule Name: rule-2

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

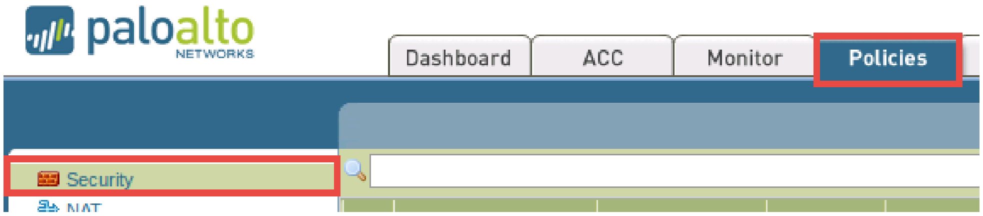
□ low

□ informational

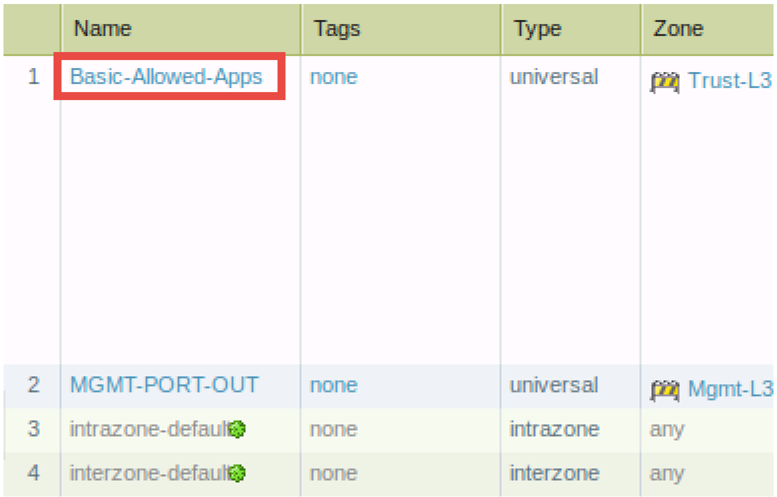
7. Click **OK** to save the rule.
8. Verify that both *rule-1* and *rule-2* appear and click **OK** to save changes in the Anti-Spyware Profile window.
9. Leave the *WebUI* opened to continue with the next task.

4 Assign Profiles to a Policy

1. Using the *WebUI*, navigate to **Policies > Security**.



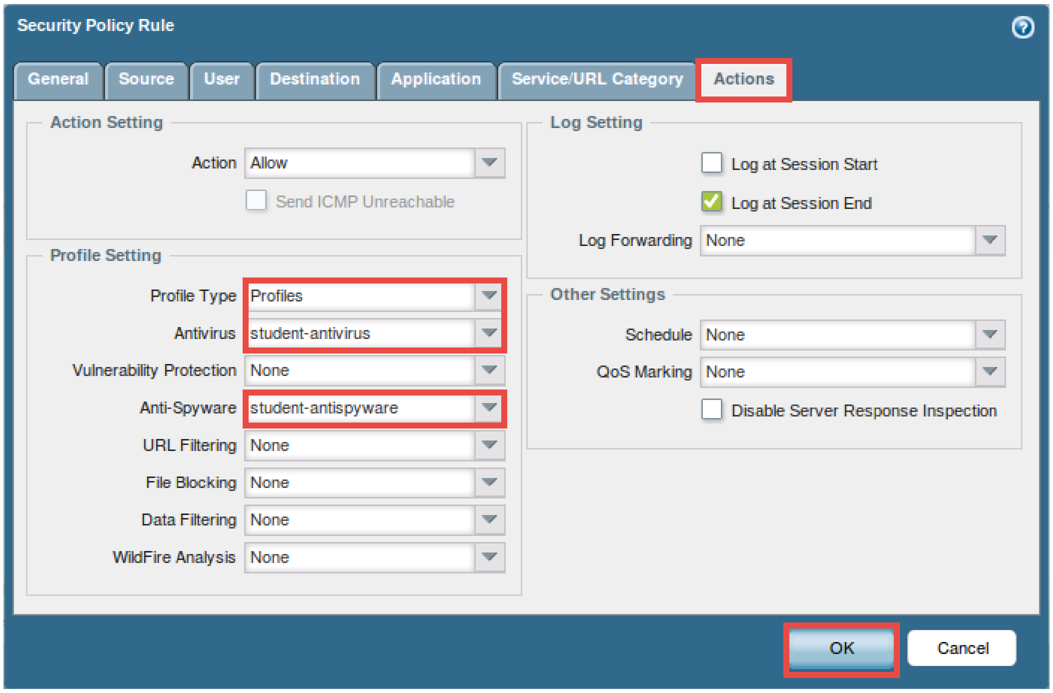
2. Click on **Basic-Allowed-Apps** from the list of policy names.



	Name	Tags	Type	Zone
1	Basic-Allowed-Apps	none	universal	Trust-L3
2	MGMT-PORT-OUT	none	universal	Mgmt-L3
3	intrazone-default	none	intrazone	any
4	interzone-default	none	interzone	any

3. In the *Security Policy Rule* window, click on the **Actions** tab and edit the policy rule to include the newly created profiles by following along with the table below.

Field	Data/Selection
Profile Type	Select **Profiles**
Antivirus	Select **student-antivirus**
Anti-Spyware	Select **student-antispyware**



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: student-antivirus

Vulnerability Protection: None

Anti-Spyware: student-antispyware

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

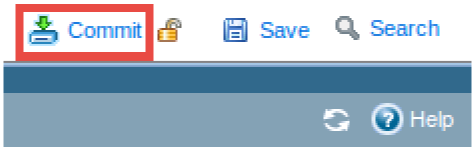
Other Settings

Schedule: None

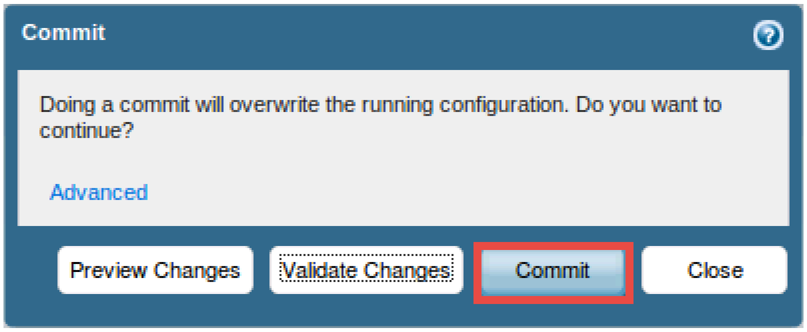
QoS Marking: None

□ Disable Server Response Inspection

4. Click **OK** to save changes.
5. Click on the **Commit** link, located near the top-right of the *WebUI*.



6. In the *Commit* window, click the **Commit** button.

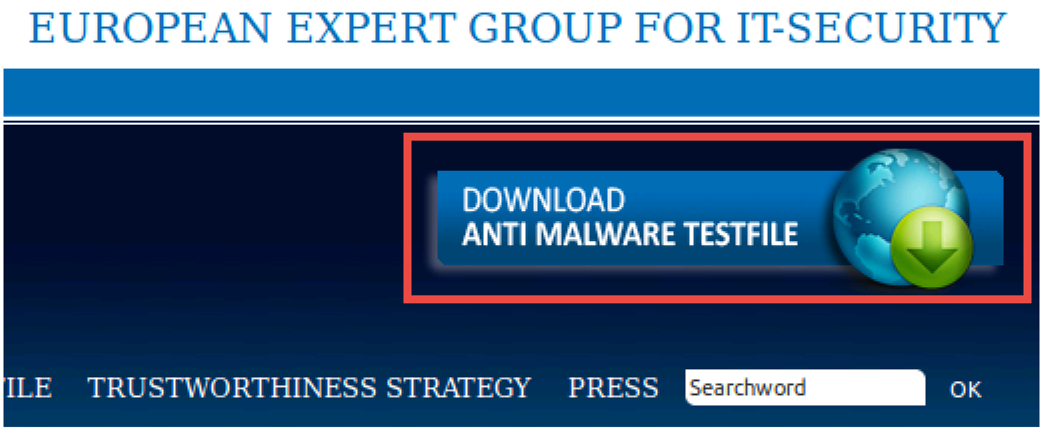


Doing a commit will overwrite the running configuration. Do you want to continue?

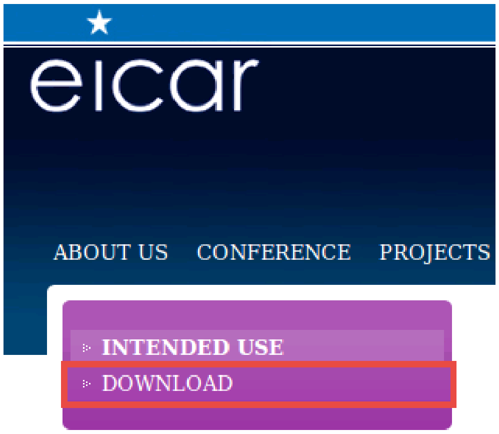
7. Once the commit process successfully completes, click the **Close** button to continue.
8. Leave the *Firefox* application opened to continue with the next task.

5 Test the Antivirus Profile

1. Using the *Firefox* application, open a **new tab**.
2. Type `www.eicar.org` into the address field and press **Enter**.
3. On the *eicar* homepage, click on the **Download Anti Malware Testfile** icon located near the top.

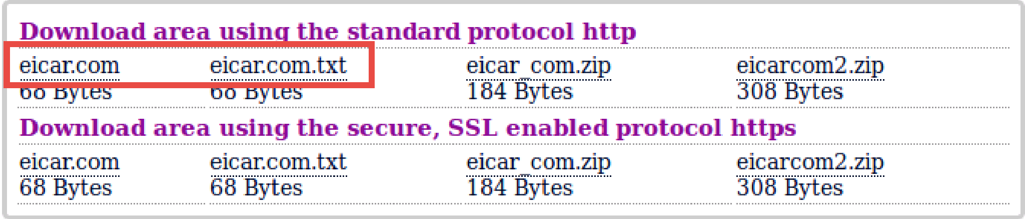


4. Within the *Download* area, click on the **Download** link located on the left pane.



5. Once the page redirects, scroll towards the bottom of the page and click either the **eicar.com** or the **eicar.com.txt** file to download the file using the standard protocol *HTTP*.

> Do not use the SSL-encrypted downloads. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.



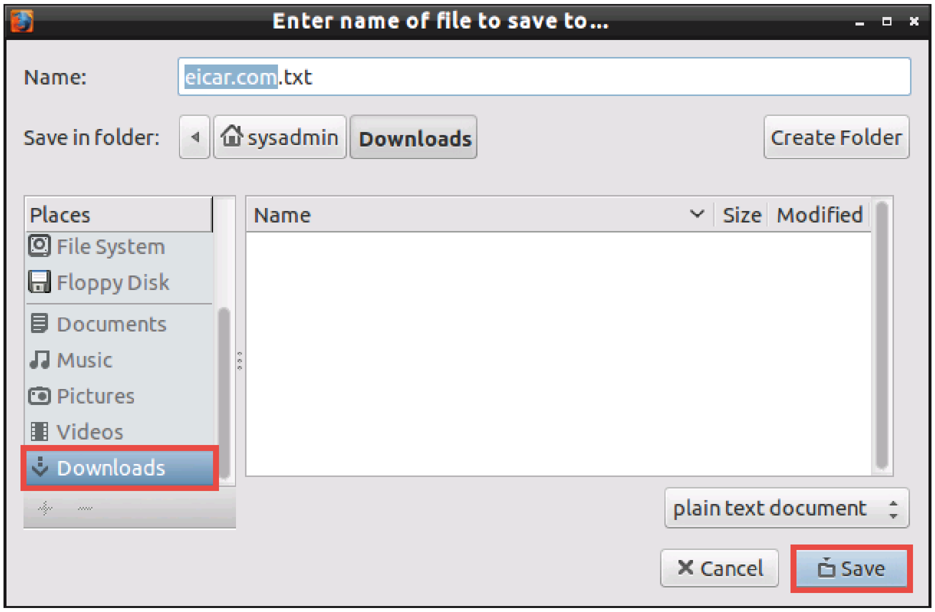
Download area using the standard protocol http

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

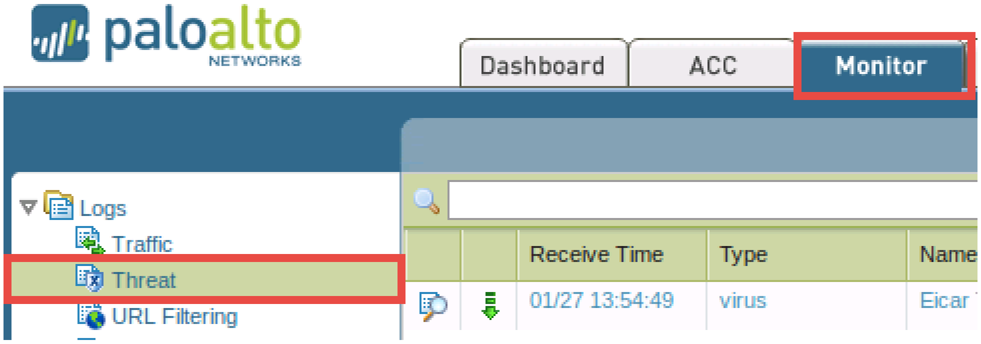
Download area using the secure, SSL enabled protocol https

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

6. If prompted, click on the **Save File** button.
7. When prompted where to save, choose the **Downloads** directory and click **Save**.

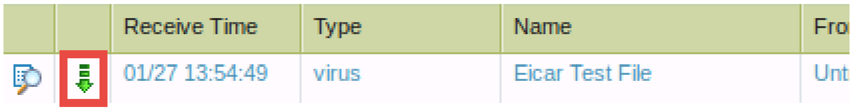


8. Close the **second tab**.
9. Navigate back to the **first tab** with the *WebUI*.
10. Using the *WebUI*, navigate to **Monitor > Logs > Threat** to view the threat log.



		Receive Time	Type	Name
		01/27 13:54:49	virus	Eicar

11. Click the **green down arrow** for the *Eicar Test File* detection to view the packet capture (*PCAP*).

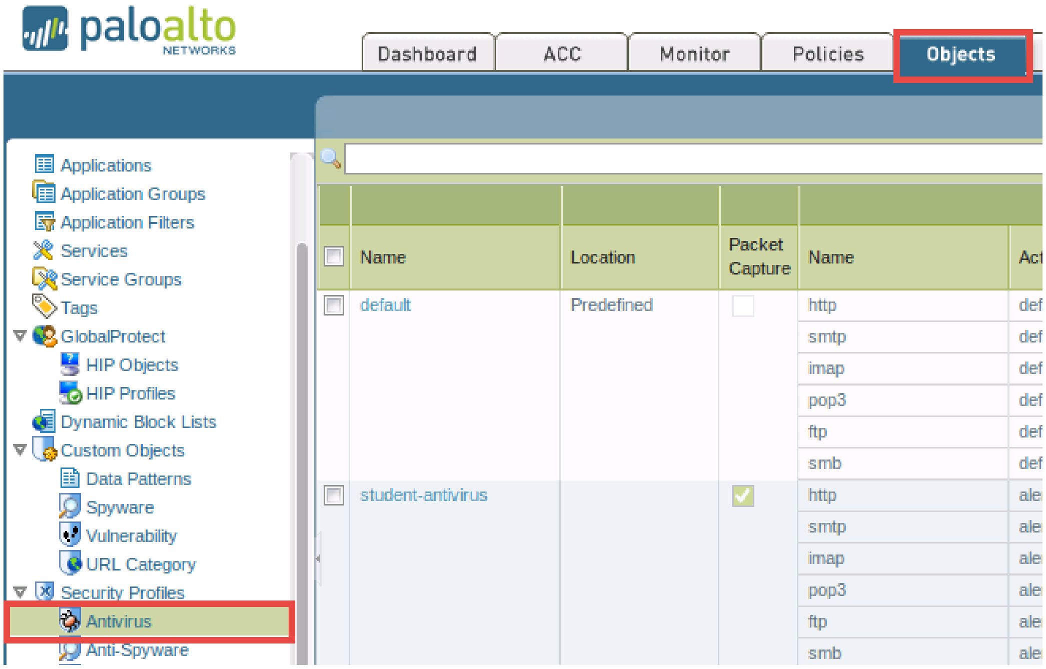


		Receive Time	Type	Name	Fro
		01/27 13:54:49	virus	Eicar Test File	Unt

12. Review the *PCAP* file.

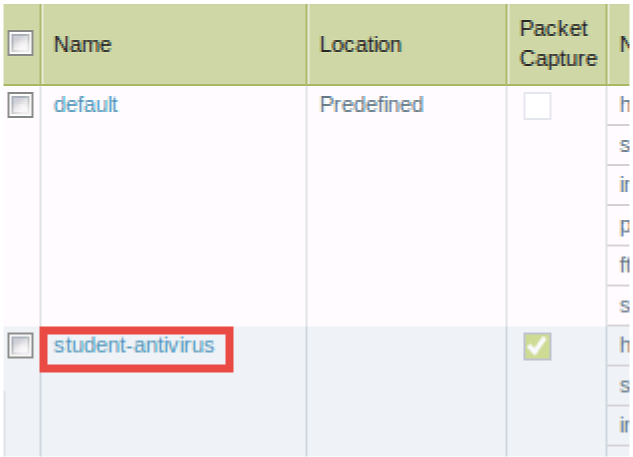
> Captured packets can be exported in PCAP format and be examined with a protocol analyzer offline for further investigation.

13. After viewing the PCAP file, click **Close**.
14. Using the WebUI, navigate to **Objects > Security Profiles > Antivirus**.



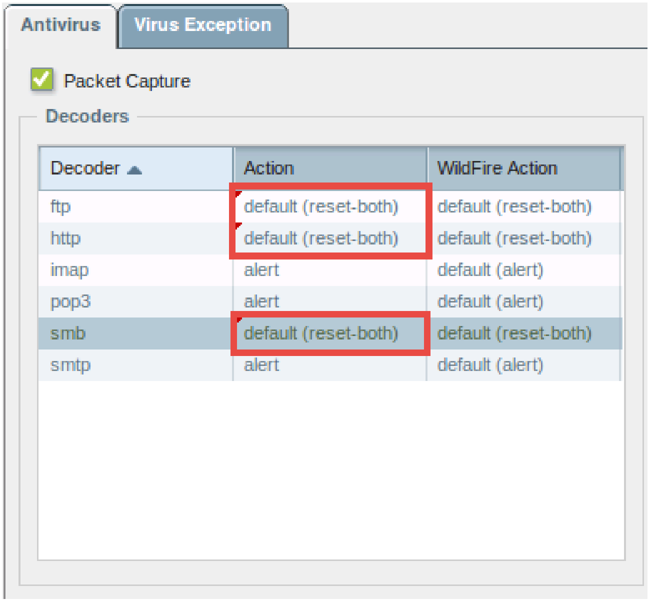
☐	Name	Location	Packet Capture	Name	Act
☐	default	Predefined	☐	http	def
				smtp	def
				imap	def
				pop3	def
				ftp	def
				smb	def
☐	student-antivirus		✓	http	ale
				smtp	ale
				imap	ale
				pop3	ale
				ftp	ale
				smb	ale

15. Click on the **student-antivirus** profile underneath the *Name* column.



☐	Name	Location	Packet Capture	N
☐	default	Predefined	☐	h
				s
				ir
				p
				ft
				s
☐	student-antivirus		✓	h
				s
				ir

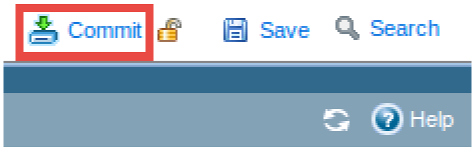
16. Click on the **Antivirus** tab and change the **Action** column for **ftp**, **http**, and **smb** decoders to **default (reset-both)**.



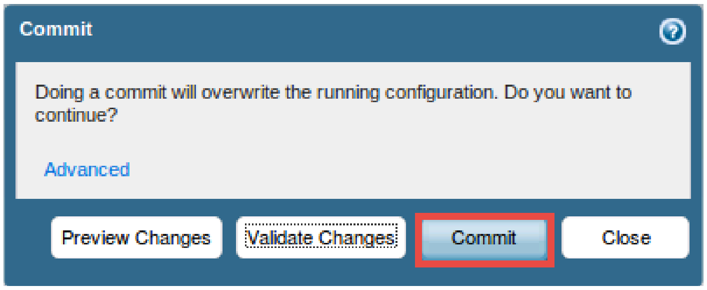
☑ Packet Capture

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

17. Click **OK**.
18. Click on the **Commit** link, located near the top-right of the *WebUI*.



19. In the *Commit* window, click the **Commit** button.

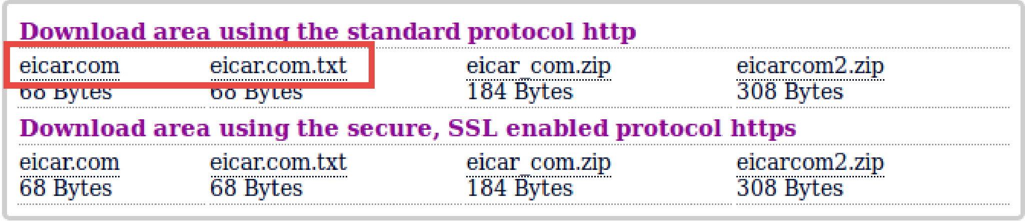


Doing a commit will overwrite the running configuration. Do you want to continue?

20. Once the commit process successfully completes, click the **Close** button to continue.
21. Open a **new tab** in the *Firefox* web browser.
22. Type `www.eicar.org/85-0-Download.`html into the address bar and press **Enter**.

23. Scroll towards the bottom of the page and attempt to download either the **eicar.com** or the **eicar.com.txt** file to download the file using the standard protocol *HTTP*.

Do not use the SSL-encrypted downloads. The firewall will not be able to detect the viruses in an HTTPS connection until decryption is configured.



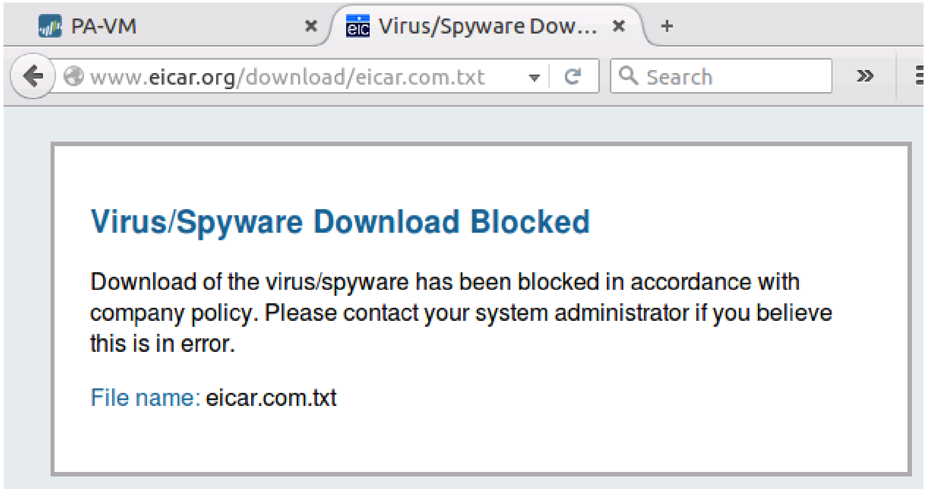
Download area using the standard protocol http

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

24. Notice the response page given. The antivirus profile is now set to block.



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.txt

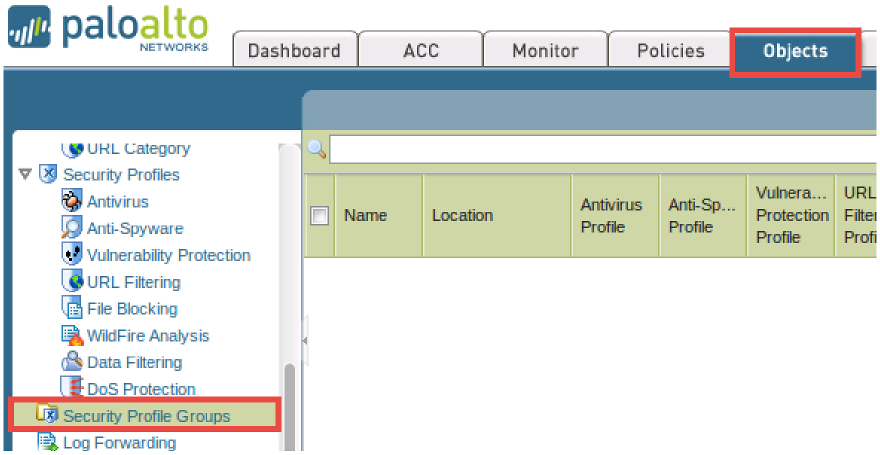
25. Close the **second tab**.
26. Navigate back to the **first tab** with the *WebUI*.
27. Using the *WebUI*, navigate to **Monitor > Logs > Threat** to view the threat log. Note the new log entry stating that the *Eicar* virus was detected and denied.

After 15 minutes, the threats that were just generated will appear on the *ACC* tab under *Threat Activity* and the *Blocked Activity* tabs.

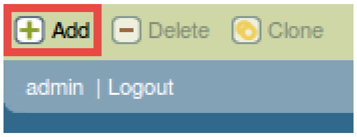
28. Leave the *WebUI* opened to continue with the next task.

6 Configure a Security Profile Group

1. Using the *WebUI*, navigate to **Objects > Security Profile Groups**.

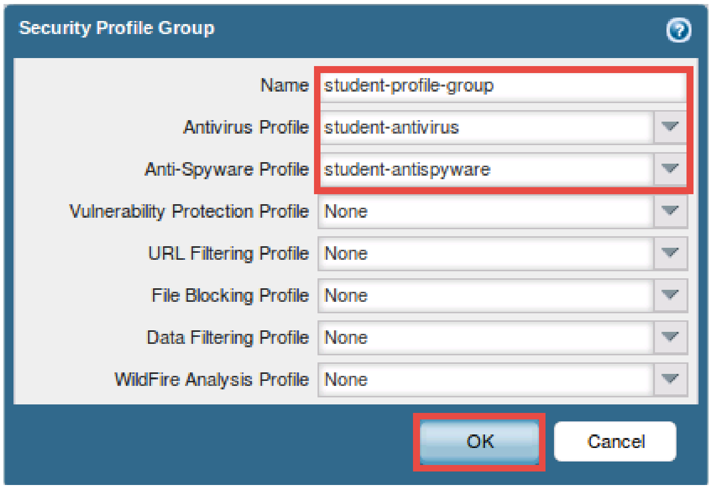


2. Click **Add**, located near the bottom of the *WebUI*, to define a security profile group.



3. In the Security Profile Group window, use the information from the table below to fill the appropriate form fields.

Field	Data/Selection
Name	Enter **student-profile-group**
Antivirus Profile	Select **student-antivirus**
Anti-Spyware Profile	Select **student-antispyware**



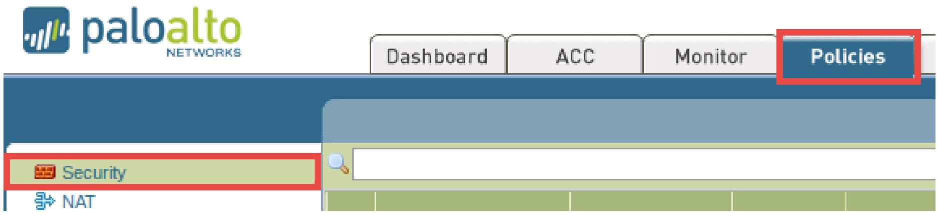
Security Profile Group

Name	student-profile-group
Antivirus Profile	student-antivirus
Anti-Spyware Profile	student-antispyware
Vulnerability Protection Profile	None
URL Filtering Profile	None
File Blocking Profile	None
Data Filtering Profile	None
WildFire Analysis Profile	None

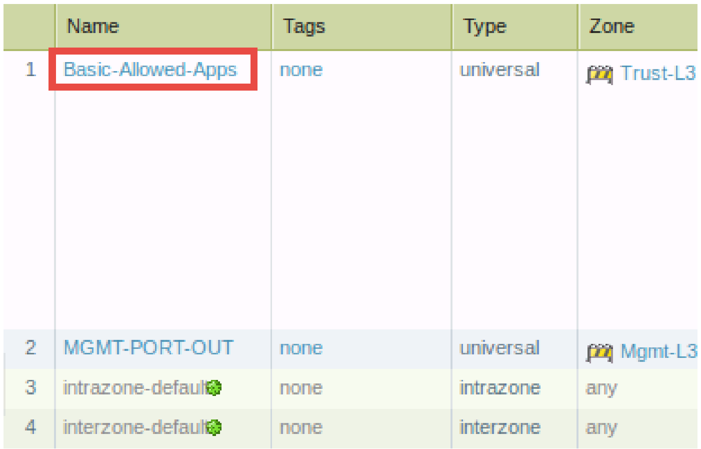
4. Click **OK** to save changes.
5. Leave the *WebUI* opened to continue with the next task.

7 Assign the Security Profile Group to a Policy

1. Using the *WebUI*, navigate to **Policies > Security**.



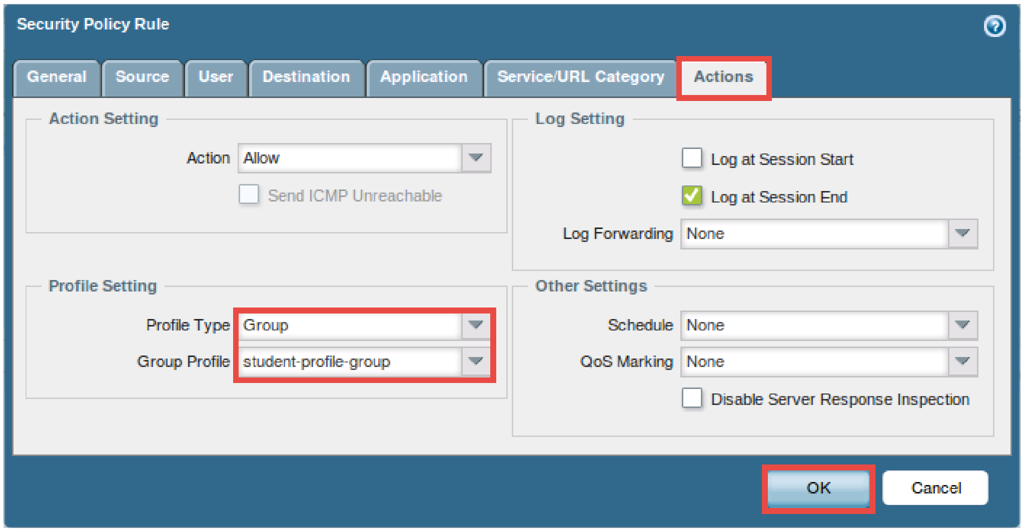
2. Click on the **Basic-Allowed-Apps** links in the list of policy names.



	Name	Tags	Type	Zone
1	Basic-Allowed-Apps	none	universal	Trust-L3
2	MGMT-PORT-OUT	none	universal	Mgmt-L3
3	intrazone-default	none	intrazone	any
4	interzone-default	none	interzone	any

3. In the *Security Policy Rule* window, click on the **Actions** tab and edit the policy to replace the profiles with the profile group by using the table below as guidance.

Field	Data/Selection
Profile Type	Select **Group**
Group Profile	Select **student-profile-group**



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: student-profile-group

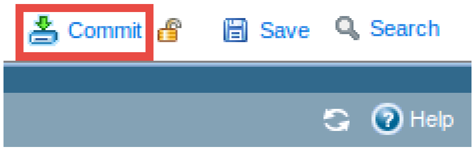
Other Settings

Schedule: None

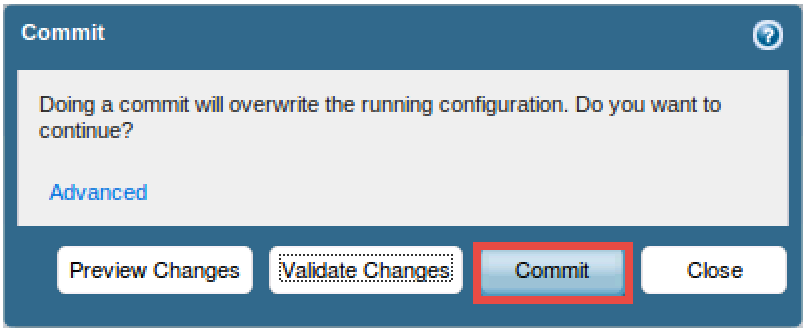
QoS Marking: None

□ Disable Server Response Inspection

4. Click **OK** to save changes.
5. Click on the **Commit** link, located near the top-right of the *WebUI*.



6. In the *Commit* window, click the **Commit** button.


Commit

Doing a commit will overwrite the running configuration. Do you want to continue?

7. Once the commit process successfully completes, click the **Close** button to continue.
8. To test the security profile group, complete **steps 21-25** once more from *Section 5*.

> Notice that the same output is given as before. This confirms that applying a security profile group works the same as applying individual security profiles.

9. Close the **Desktop 1** PC viewer.