



PAN-OS 7.0 FIREWALL ESSENTIALS LAB SERIES

Lab 7: File Blocking and WildFire

Document Version: 2016-04-19

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	4
Pod Topology	5
Lab Settings	6
1 Configure the Initial Settings	7
2 Create a File Blocking Profile	10
3 Create a WildFire Analysis Profile	12
4 Assign the File Blocking and WildFire Profiles to the Profile Group	14
5 Test the File Blocking Profile	17
6 Test the WildFire Analysis Profile	18

Introduction



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

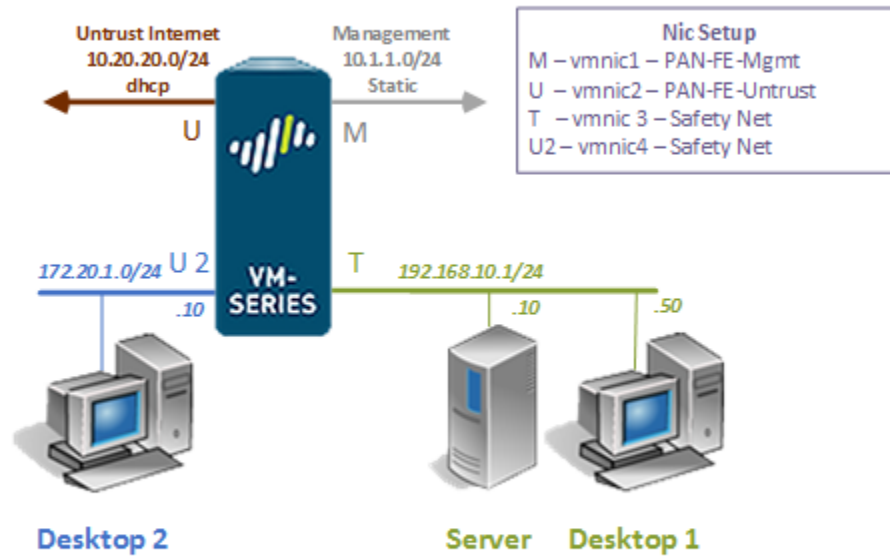
- Configure downloaded pdf files to be automatically blocked.
- Test file blocking by trying to download a pdf file.
- Configure WildFire and confirm that executable files are sent to WildFire for analysis.

Objective

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

1. Configure security profiles for file blocking and WildFire analysis
2. Add these security profiles to the security profile groups associated with the security 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 Configure the Initial Settings

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



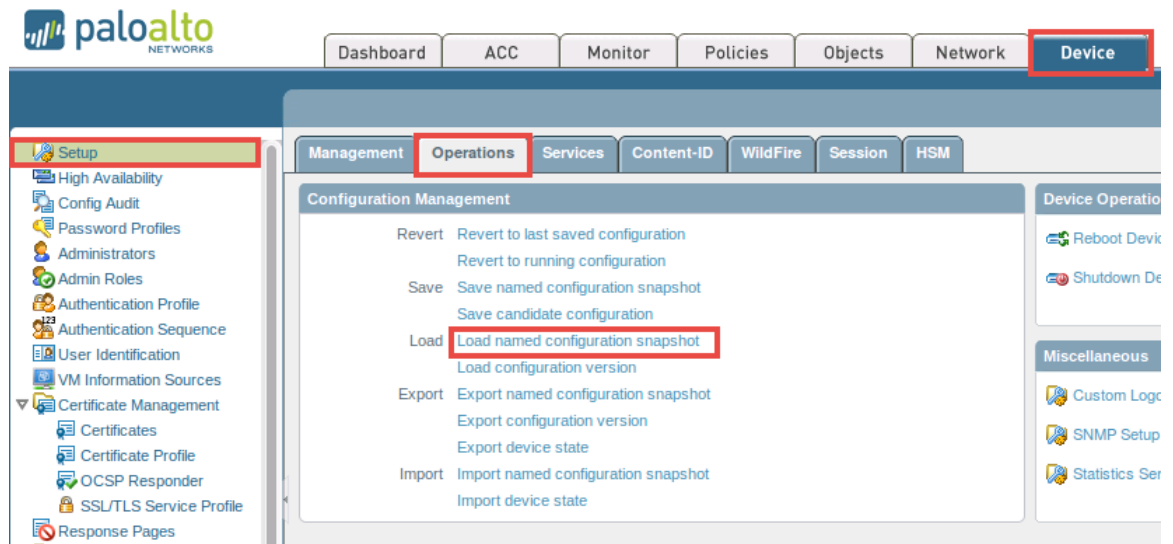
4. In the address field, type **https://192.168.10.1** and press **Enter**.

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.

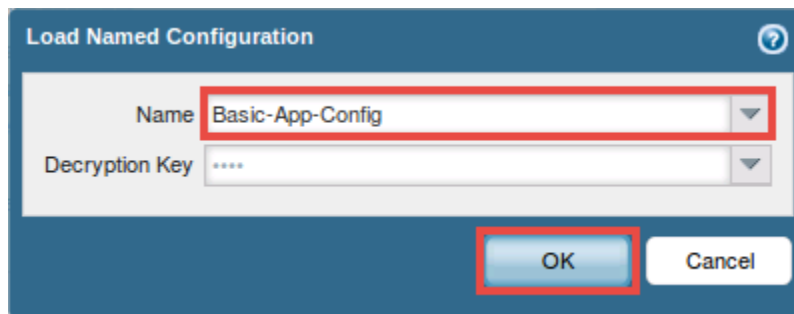
5. Login with the *username* **admin** and *password* **paloalto** on the firewall web interface.



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



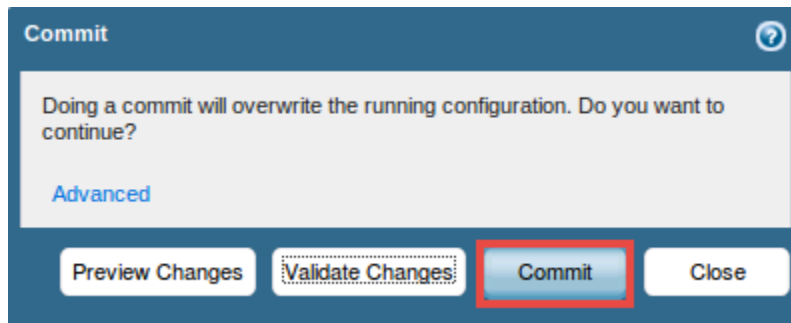
7. In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.



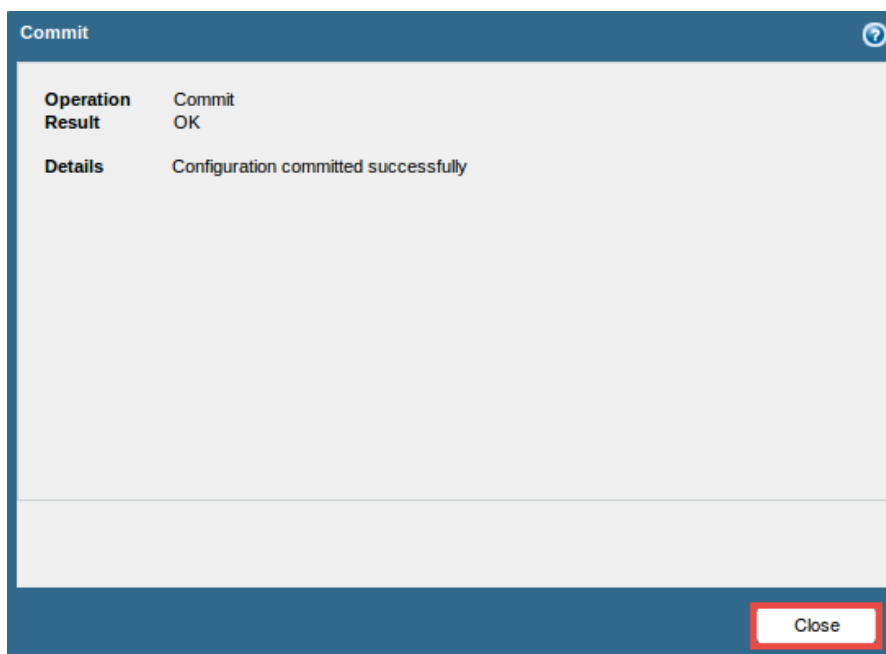
8. When prompted with the config loaded message, click on the **Close** button to continue.
9. Click on the **Commit** link located at the top-right of the *WebUI*.



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



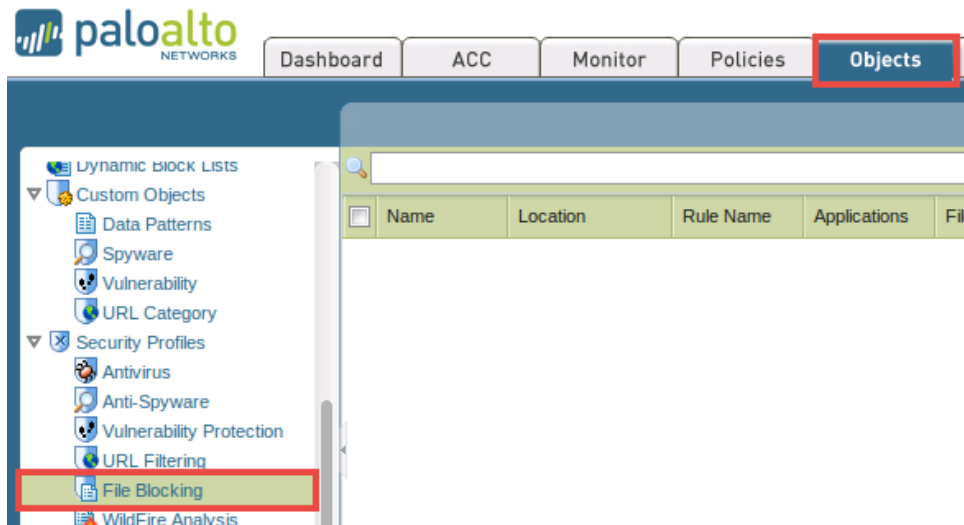
11. Once the operation successfully completes, click **Close** to continue.



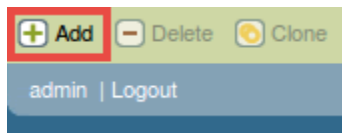
12. Leave the *WebUI* opened to continue with the next task.

2 Create a File Blocking Profile

1. Using the *WebUI*, navigate to **Objects > Security Profiles > File Blocking**.



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



3. In the *File Blocking Profile* window, use the information from the table below to fill out the form fields.

Field	Data/Selection
Name	Enter student-file-blocking
Rules list	<p>Click Add and create a rule with these parameters:</p> <ul style="list-style-type: none"> • Rule Name: Enter BlockPDF • Applications: any • File Types: pdf • Direction: both • Action: block

File Blocking Profile

Name:

Description:

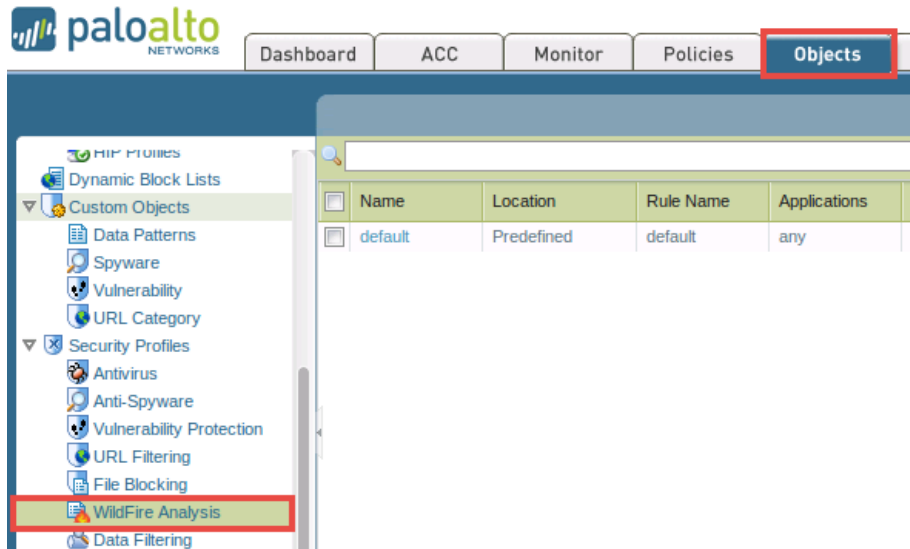
1 item

<input type="checkbox"/>	Name	Applications	File Types	Direction	Action
<input checked="" type="checkbox"/>	BlockPDF	any	pdf	both	block

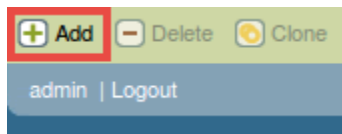
4. Click **OK** to save changes.
5. Leave the *WebUI* opened to continue with the next task.

3 Create a WildFire Analysis Profile

1. Using the *WebUI*, navigate to **Objects > Security Profiles > WildFire Analysis**.



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



3. In the *WildFire Analysis Profile* window, use the information from the table below to fill out the form fields.

Field	Data/Selection
Name	Enter student-wildfire
Rules list	<p>Click Add and create a rule with these parameters:</p> <ul style="list-style-type: none"> • Rule Name: Enter AnalyzeEXE • Applications: any • File Types: pe • Direction: both • Analysis: public-cloud

WildFire Analysis Profile

Name: student-wildfire

Description:

1 item

	Name	Applications	File Types	Direction	Analysis
<input checked="" type="checkbox"/>	AnalyzeEXE	any	pe	both	public-cloud

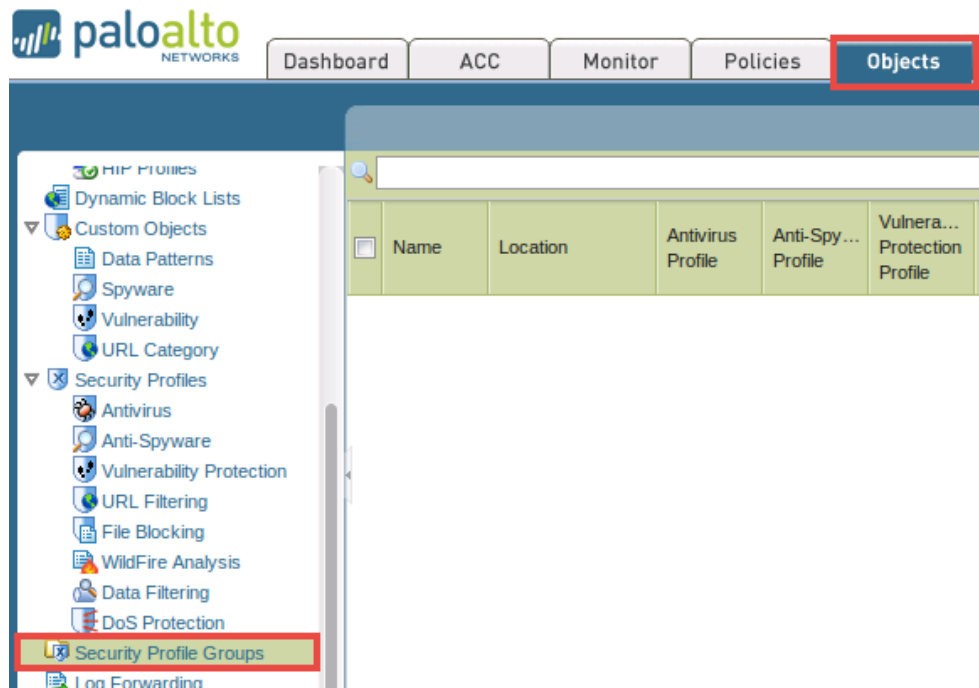
+ Add - Delete

OK Cancel

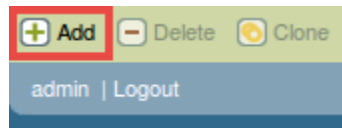
4. Click **OK** to save the rule.
5. Leave the *WebUI* opened to continue with the next task.

4 Assign the File Blocking and WildFire Profiles to the Profile Group

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

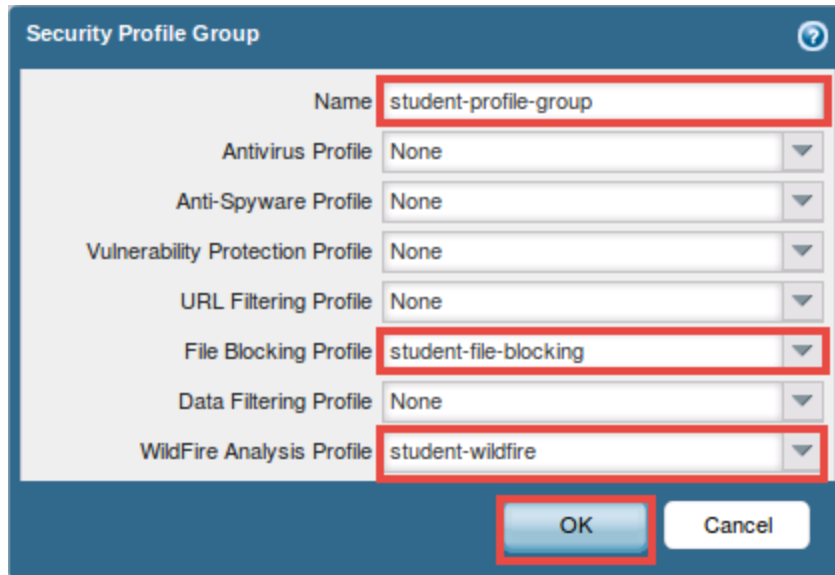


2. Click on **Add**, located near the bottom of the window, to define a security profile group.



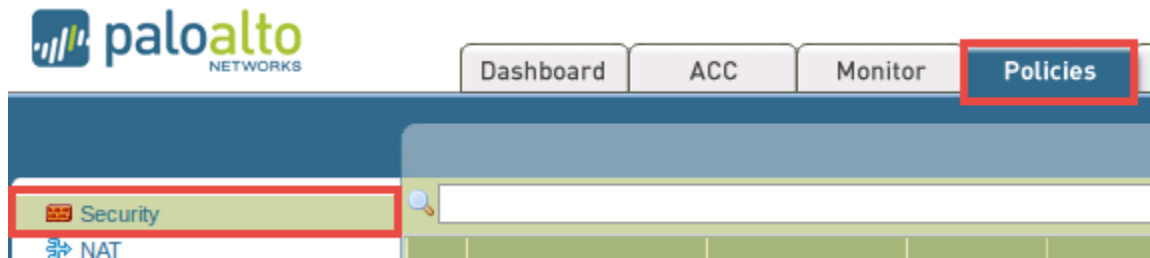
3. In the *Security Profile Group* window, use the information from the table below to fill out the form fields.

Field	Data/Selection
Name	Enter student-profile-group
File Blocking Profile	Select student-file-blocking
WildFire Analysis Profile	Select student-wildfire



The image shows a 'Security Profile Group' configuration window. The 'Name' field is set to 'student-profile-group'. The 'Antivirus Profile', 'Anti-Spyware Profile', 'Vulnerability Protection Profile', 'URL Filtering Profile', 'Data Filtering Profile', and 'WildFire Analysis Profile' are all set to 'None'. The 'File Blocking Profile' is set to 'student-file-blocking'. The 'OK' button is highlighted with a red box.

4. Click **OK** to save changes.
5. Navigate to **Policies > Security**.

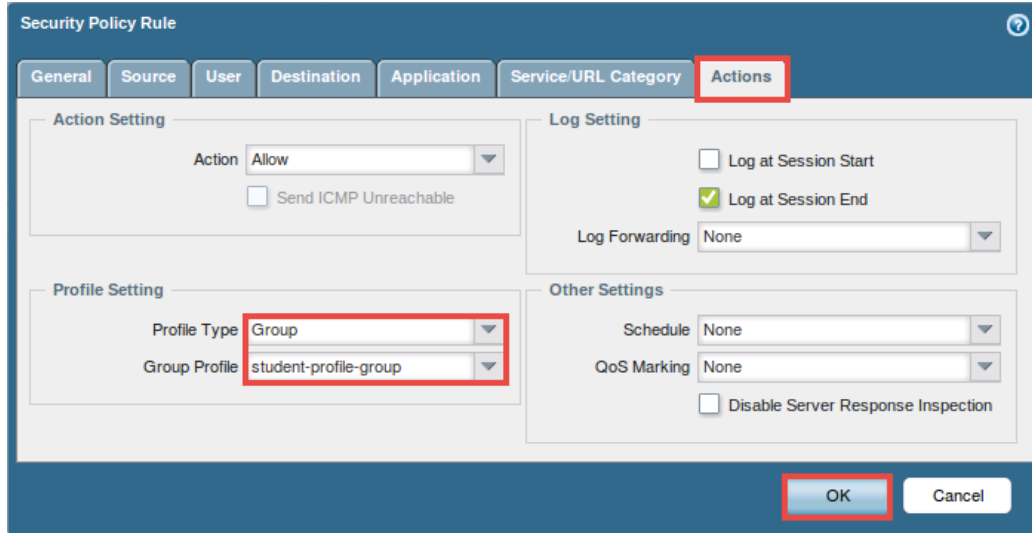


6. Click on the **Basic-Allowed-Apps** link in the list of policy names.

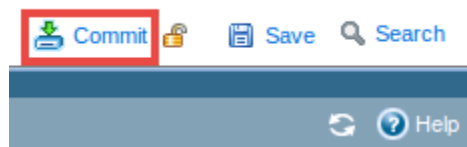
	Name	Tags	Type	Zone
1	Basic-Allowed-Apps	none	universal	Trust-L3
2	MGMT-PORT-OUT	none	universal	Mgmt-L3
3	intrazone-default	none	intrazone	any
4	interzone-default	none	interzone	any

7. In the *Security Policy Rule* window, edit the policy by clicking on the **Actions** tab.
8. Select **Group** from the *Profile Type* drop-down menu.

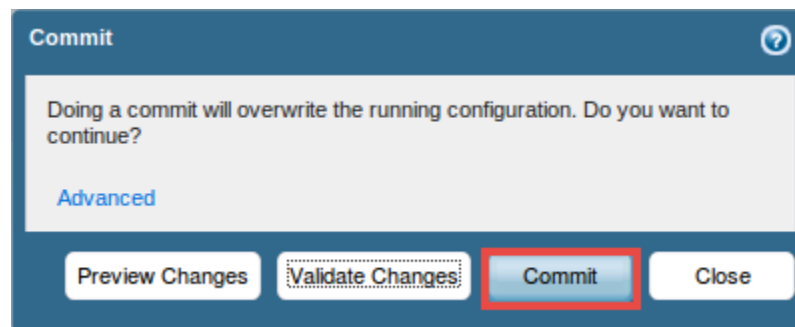
9. Then, select **student-profile-group** from the *Group Profile* drop-down menu.



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



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



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

5 Test the File Blocking Profile

1. Using the *Firefox* application, open a **new tab**.
2. Type `http://www.panedufiles.com` into the address field and press **Enter**.
3. Click on the **Panorama_AdminGuide70.pdf** file link located near the top of the webpage.

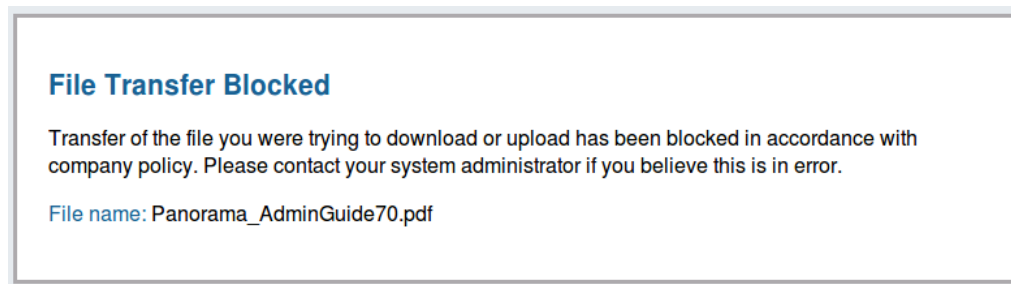


201 PAN Firewall Essentials I (7.0) Files

File-Blocking and WildFire Lab

[Panorama_AdminGuide70.pdf](#)

4. Notice the file transfer was blocked.



5. Close the **second tab**.
6. Navigate back to the **first tab** with the *WebUI*.
7. Using the *WebUI*, navigate to **Monitor > Logs > Data Filtering** to view the log entries.
8. Identify the log entry for the *PDF* file that has been blocked.

	Receive Time	File Name	Name	From Zone	To Zone
	03/24 10:37:31	Panorama_Adm...	Adobe Portable Document Format (PDF)	Untrust-L3	Trust-L3

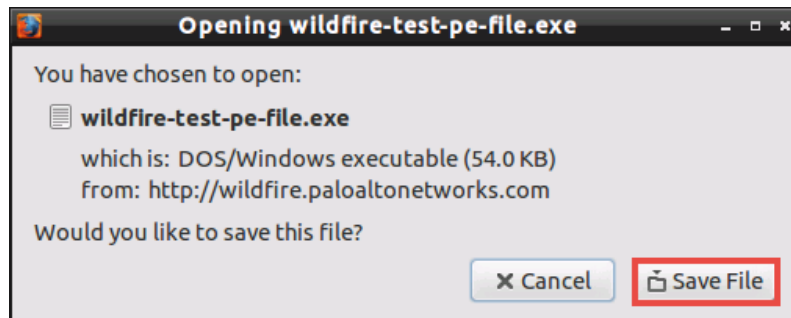
9. Leave the *Firefox* web browser opened to continue with the next task.

6 Test the WildFire Analysis Profile

1. Using the *Firefox* application, open a **new tab**.
2. Type `http://wildfire.paloaltonetworks.com/publicapi/test/pe` into the address field and press **Enter**.

This site generates an attack file with a unique signature, which simulates a zero-day attack.

3. When prompted, click the **Save File** button.



4. Save the file in the **Downloads** directory and click **Save**.
5. Close the second **tab**.
6. To verify the file was uploaded to the *Public WildFire Cloud*, open a terminal window by clicking on the **LXTerminal** icon located on the bottom tool pane.



7. In the terminal window, type the command below followed by pressing the Enter key.

```
ssh admin@192.168.10.1
```

8. When prompted for a password, enter `pa1oalto`. Press **Enter**.

9. Once logged in via SSH, enter the debug command below to view the output showing “log: 0, filename: wildfire-test-pe-file-exe processed...”. This verifies the file was uploaded to the *WildFire Public Cloud*.

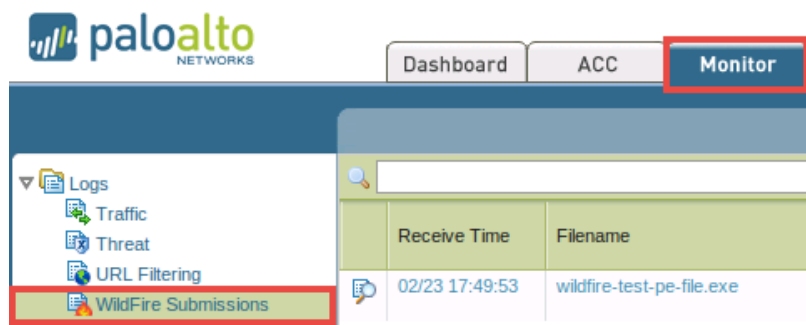
```
debug wildfire upload-log show
```

```
Upload Log disk log rotation size: 2.000 MB.
Public Cloud upload logs:

log: 0, filename: wildfire-test-pe-file.exe
processed 60 seconds ago, action: upload success
vsys_id: 1, session_id: 1102, transaction_id: 1
file_len: 55296, flag: 0x801c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.10.50/56369 to 52.20.176.145/80
SHA256: 7dfd57fc5c882d71e02e31c968a3c39d16b3f890f3a3c16cd99882f528b307f9
Private Cloud upload logs:

admin@PA-VM>
```

10. Change focus back to the *Firefox* web browser and navigate to **Monitor > Logs > WildFire Submissions**.



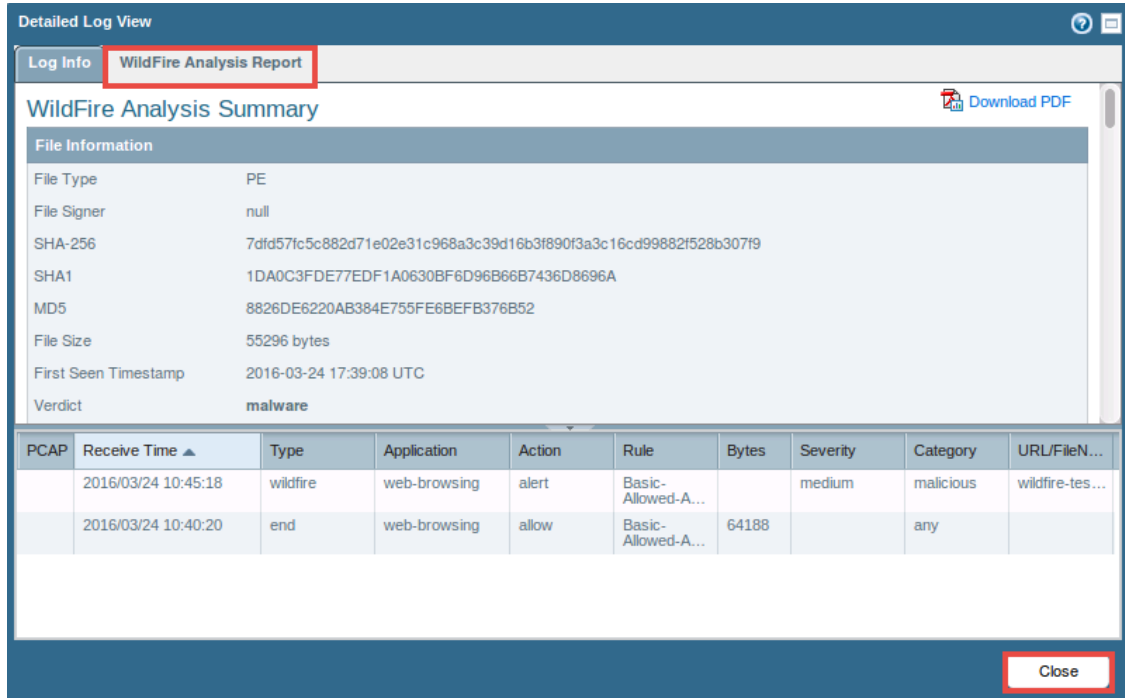
11. Locate the entry for *wildfire-test-pe-file.exe* that has been submitted to WildFire and notice the file has been identified as *malicious* underneath its respective *Verdict* column.

If the *wildfire-test-pe-file.exe* does not automatically appear in the list, wait a couple of minutes for it to populate. The manual refresh button may be used if necessary.

12. Click on the **magnifying glass** icon next to the *wildfire-test-pe-file.exe* entry to see a detailed log view.

	Receive Time	Filename
	03/24 10:45:18	wildfire-test-pe-file.exe

13. In the *Detailed Log View* window, make sure to view the **Log Info** tab and review the information within the *General*, *Details*, and *Destination* panels.
14. In the *Detailed Log View* window, click on the **Wildfire Analysis Report** tab and review the information provided. Click on the **Close** button when finished.



Detailed Log View

Log Info **WildFire Analysis Report**

WildFire Analysis Summary [Download PDF](#)

File Information

File Type	PE
File Signer	null
SHA-256	7dfd57fc5c882d71e02e31c968a3c39d16b3f890f3a3c16cd99882f528b307f9
SHA1	1DA0C3FDE77EDF1A0630BF6D96B66B7436D8696A
MD5	8826DE6220AB384E755FE6BEFB376B52
File Size	55296 bytes
First Seen Timestamp	2016-03-24 17:39:08 UTC
Verdict	malware

PCAP	Receive Time ▲	Type	Application	Action	Rule	Bytes	Severity	Category	URL/FileN...
	2016/03/24 10:45:18	wildfire	web-browsing	alert	Basic-Allowed-A...		medium	malicious	wildfire-tes...
	2016/03/24 10:40:20	end	web-browsing	allow	Basic-Allowed-A...	64188		any	

Close

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