



CLOUD SECURITY FUNDAMENTALS V2

Lab 2: Preventing Threats from the Internet with File Blocking

Document Version: 2022-12-22

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark 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	3
Lab Topology	4
Lab Settings	5
1 Preventing Threats from the Internet with File Blocking	6
1.0 Load Lab Configuration	6
1.1 Create a File Blocking Security Profile	11
1.2 Apply the File Blocking Profile to a Security Policy	13
1.3 Test the File Blocking Profile	14

Introduction

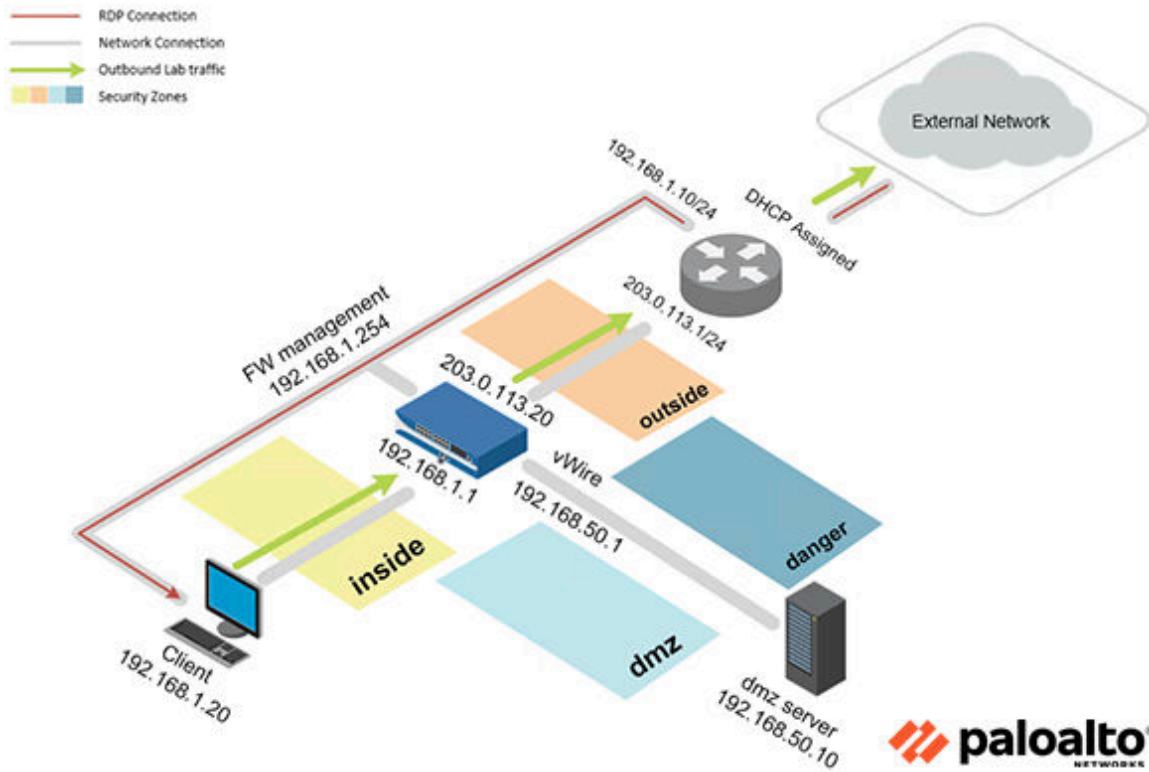
In this lab, you will create a File Blocking Profile to block PDF files. After you have created a File Blocking Profile, you will then test the profile by trying to download a PDF file.

Objective

In this lab, you will perform the following tasks:

- Create a File Blocking Security Profile
- Apply the File Blocking Profile to a Security Policy
- Test the File Blocking Profile

Lab Topology



Lab Settings

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

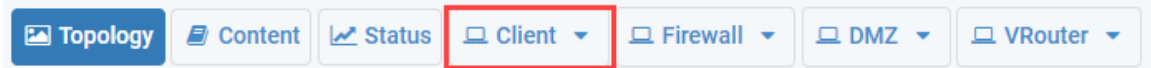
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Preventing Threats from the Internet with File Blocking

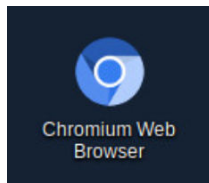
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

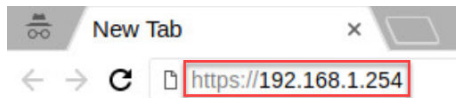
1. Click on the **Client** tab to access the Client PC.



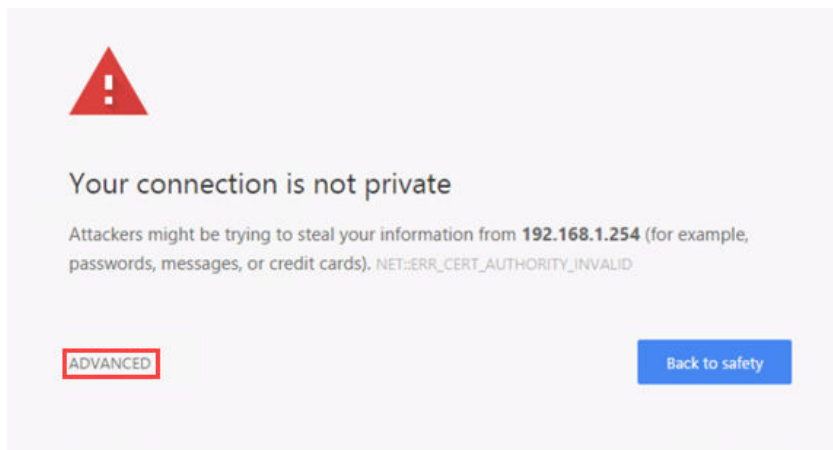
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



4. In the *Google Chrome* address field, type `https://192.168.1.254`, and press **Enter**.

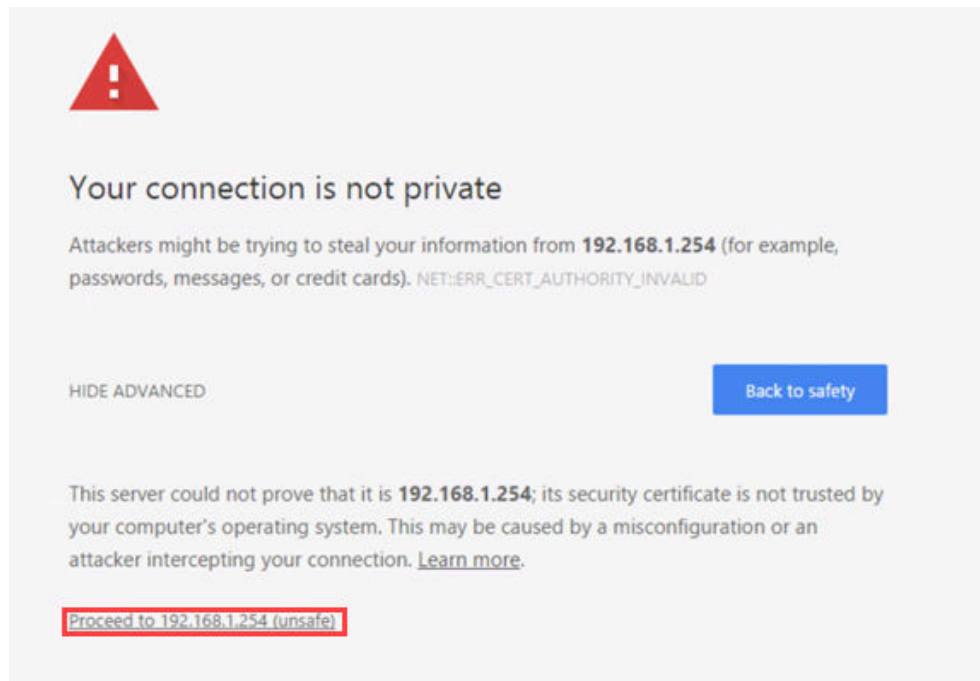


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

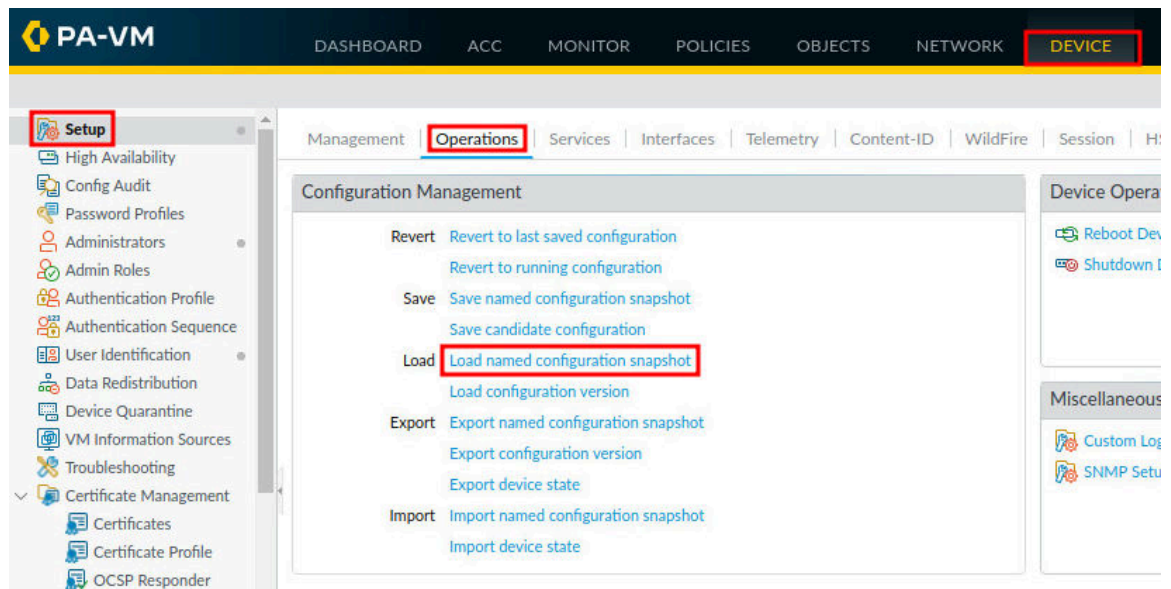
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



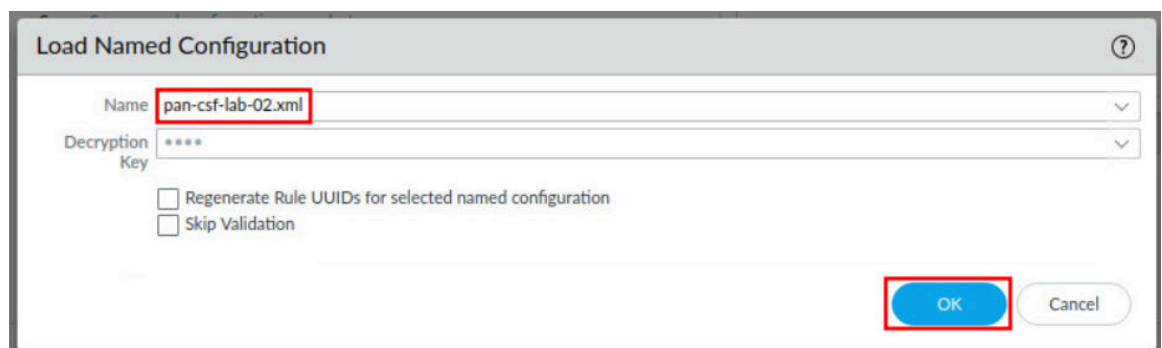
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



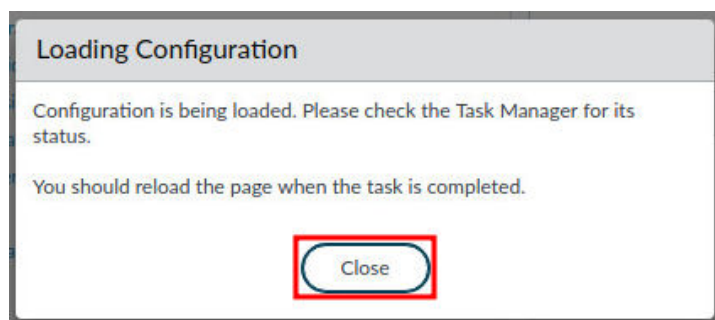
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



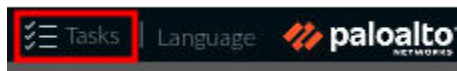
9. In the *Load Named Configuration* window, select **pan-csf-lab-02.xml** from the *Name* dropdown box and click **OK**.



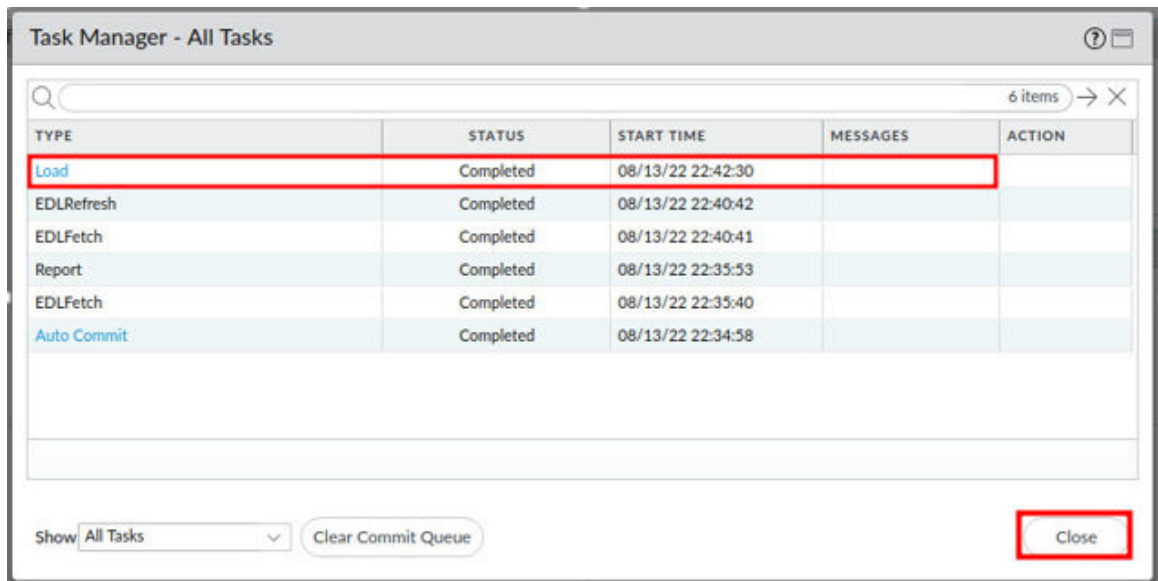
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



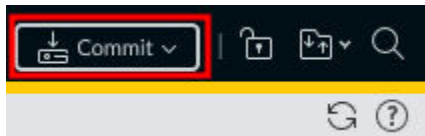
11. Click the **Tasks** icon located at the bottom-right of the web interface.



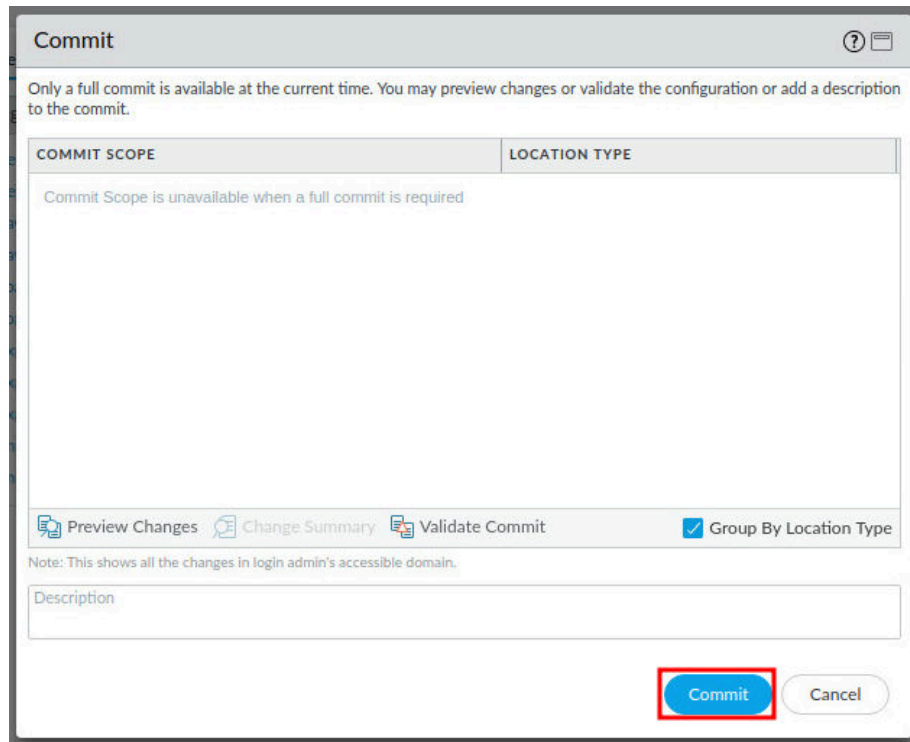
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



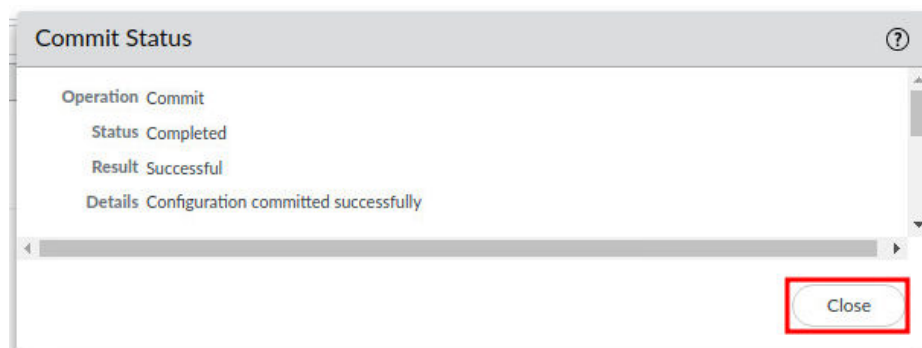
13. Click the **Commit** link located at the top-right of the web interface.



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



15. When the commit operation successfully completes, click **Close** to continue.

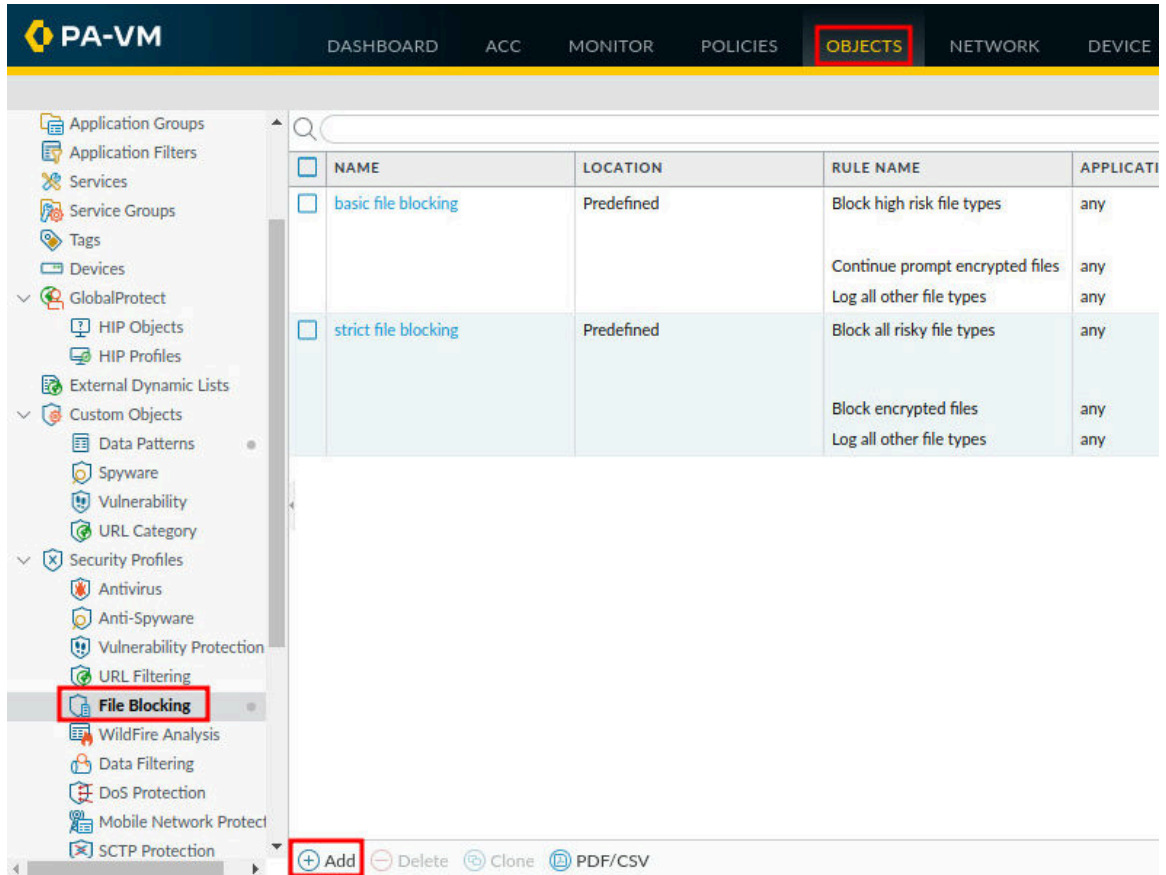


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

1.1 Create a File Blocking Security Profile

In this section, you will create a File Blocking Security Profile to block PDF files.

1. Navigate to **Objects > Security Profiles > File Blocking > Add**.

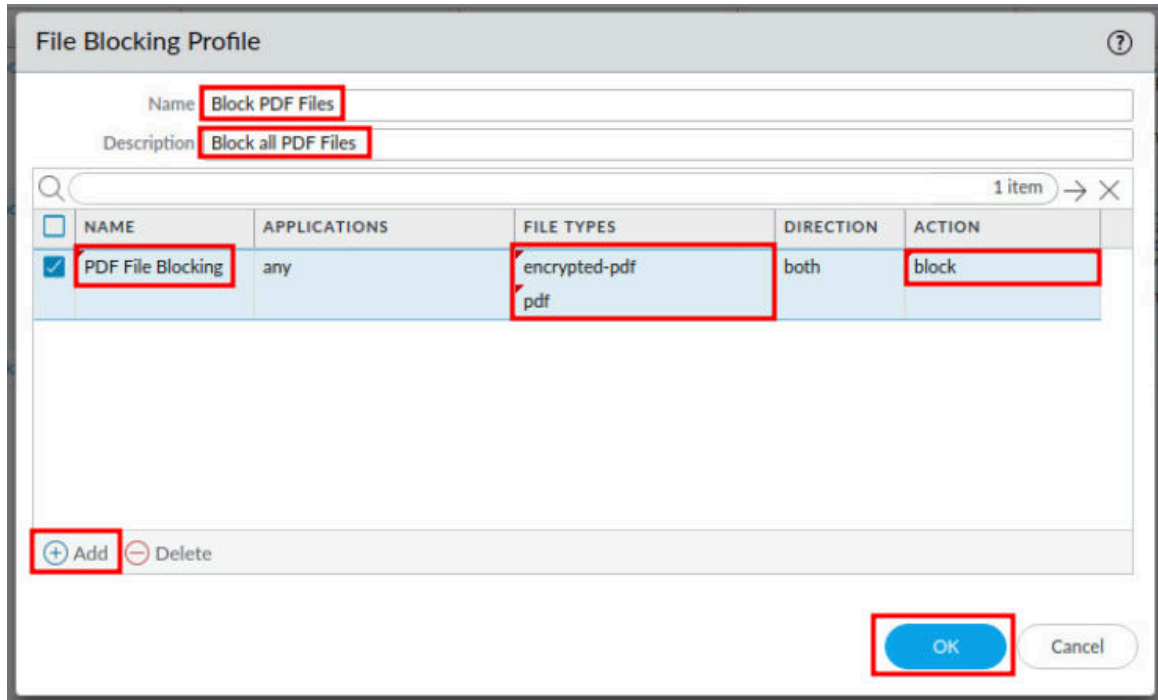


The screenshot shows the PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, **OBJECTS** (highlighted), NETWORK, and DEVICE. The left sidebar lists various configuration categories, with **File Blocking** highlighted under the Security Profiles section. The main content area displays a table of predefined file blocking rules.

NAME	LOCATION	RULE NAME	APPLICATION
<input type="checkbox"/> basic file blocking	Predefined	Block high risk file types	any
		Continue prompt encrypted files	any
		Log all other file types	any
<input type="checkbox"/> strict file blocking	Predefined	Block all risky file types	any
		Block encrypted files	any
		Log all other file types	any

At the bottom of the main content area, there is a toolbar with the following buttons: **+ Add** (highlighted), **- Delete**, **Clone**, and **PDF/CSV**.

2. In the *File Blocking Profile* window, type **Block PDF Files** in the *Name* field. Then, in the *Description* field, type **Block all PDF Files**. Next, click on **Add** in the lower-left. In the *Name* column, type **PDF File Blocking**. Next, in the *File Types* column, click **Add** and select **pdf**. Then, click **add** again and select **encrypted-pdf**. Finally, in the *Action* column, select **block** and click **OK**.



File Blocking Profile

Name: **Block PDF Files**

Description: **Block all PDF Files**

1 item

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input checked="" type="checkbox"/>	PDF File Blocking	any	encrypted-pdf pdf	both	block

+ Add - Delete

OK Cancel

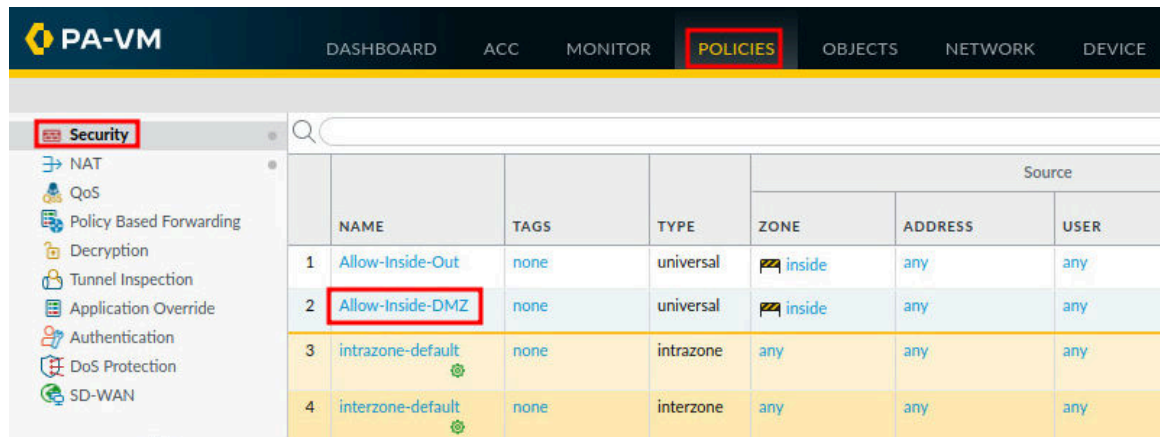
Please Note

For this step, you will add both the encrypted-pdf and pdf to the File Types. In the next task you will only block a standard pdf file. As a Palo Alto Networks Firewall administrator, it is important to block all PDF file types in the File Block Profile if you wish for any and all pdf files to block during download.

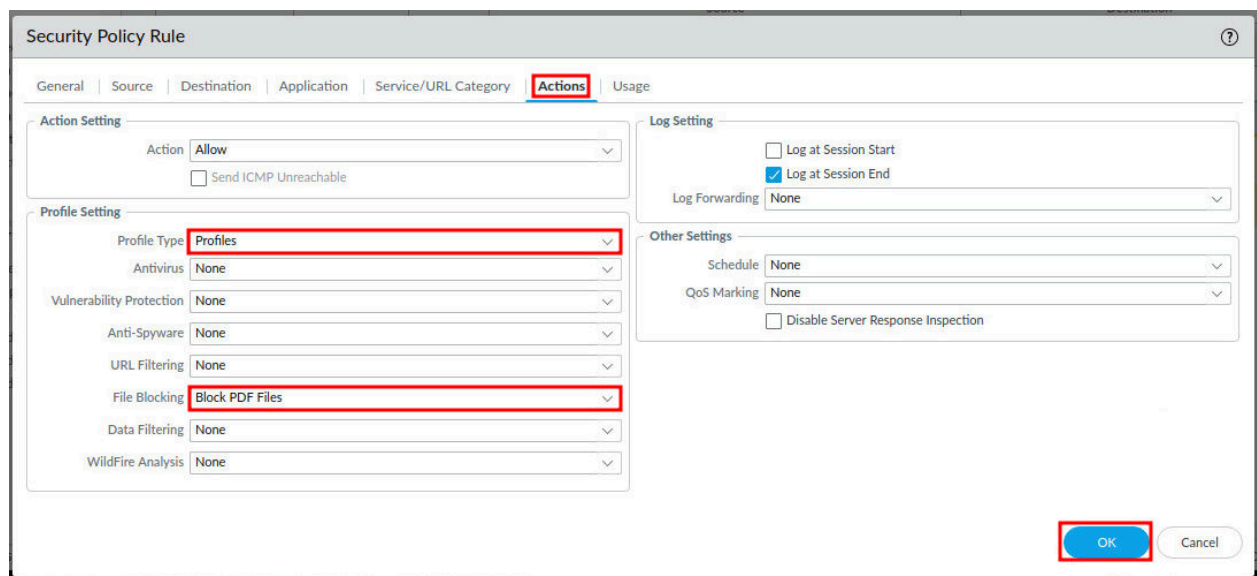
1.2 Apply the File Blocking Profile to a Security Policy

In this section, you will apply the File Blocking Security Profile you created in the previous section to a Security Policy.

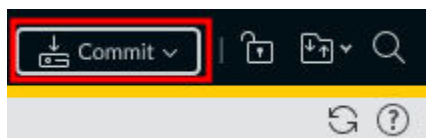
1. Navigate to **Policies > Security** and click on **Allow-Inside-DMZ**.



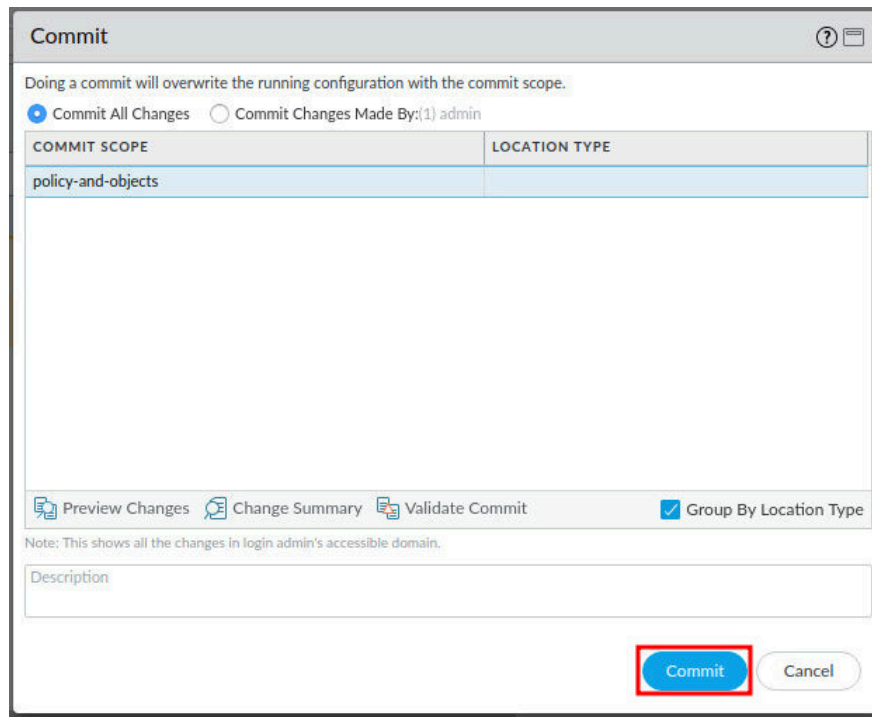
2. In the *Security Policy Rule* window, click on the **Actions** tab. Next, verify **Allow** is selected for the *Action* dropdown. Then, select **Profiles** for the *Profile Type* dropdown. Finally, select **Block PDF Files** in the *File Blocking* dropdown and click **OK**.



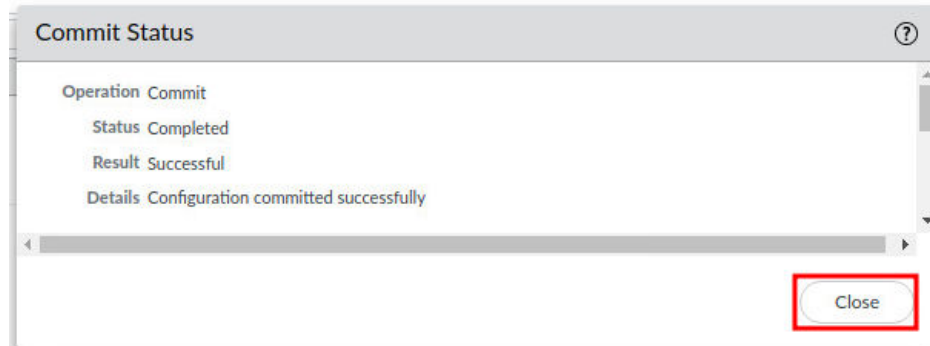
3. Click the **Commit** link located at the top-right of the web interface.



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



5. When the commit operation successfully completes, click **Close** to continue.



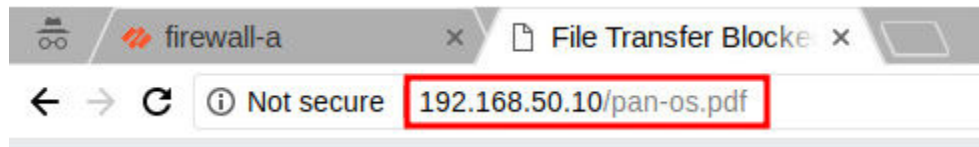
1.3 Test the File Blocking Profile

In this section, you will test the security policy you just applied.

1. Click on the **New tab** button in the *Chromium* web browser.



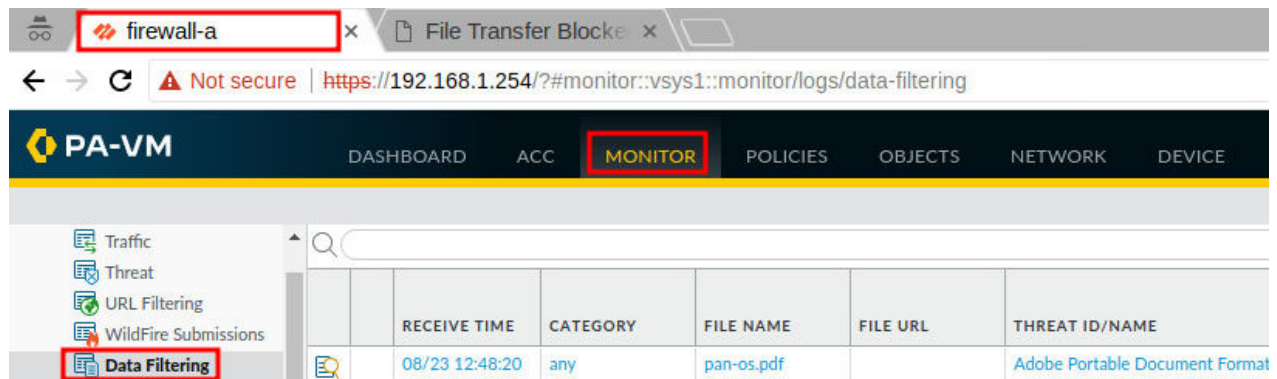
2. In the *address bar*, type `http://192.168.50.10/pan-os.pdf` and press **Enter**.



3. Notice the File Transfer was blocked via the File Blocking Profile that was created in a previous section.



4. Click on the **firewall-a** tab in the upper-left and navigate to **Monitor > Logs > Data Filtering**.



5. Notice that **pan-os.pdf** has been logged. View the *Source address*, *Destination address*, *Application* type, and the *Action*. You will notice that the *Action* is to “deny”; therefore, the file has been denied the opportunity to open.

CATEGORY	FILE NAME	FILE URL	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	TO PORT	APPLICATI...	ACTION
any	pan-os.pdf		Adobe Portable Document Format (PDF)	inside	dmz	192.168.1.20	192.168.50.10	80	web-browsing	deny

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