



PAN9 CYBERSECURITY GATEWAY

Lab 9: Preventing Threats from the Internet with File Blocking

Document Version: 2020-01-24

Copyright © 2020 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	3
Lab Topology	4
Lab Settings	5
9 Lab: Preventing Threats from the Internet with File Blocking	6
9.0 Load Lab Configuration	6
9.1 Create a File Blocking Security Profile	10
9.2 Apply the File Blocking Profile to a Security Policy	11
9.3 Test the File Blocking Profile	14

Introduction

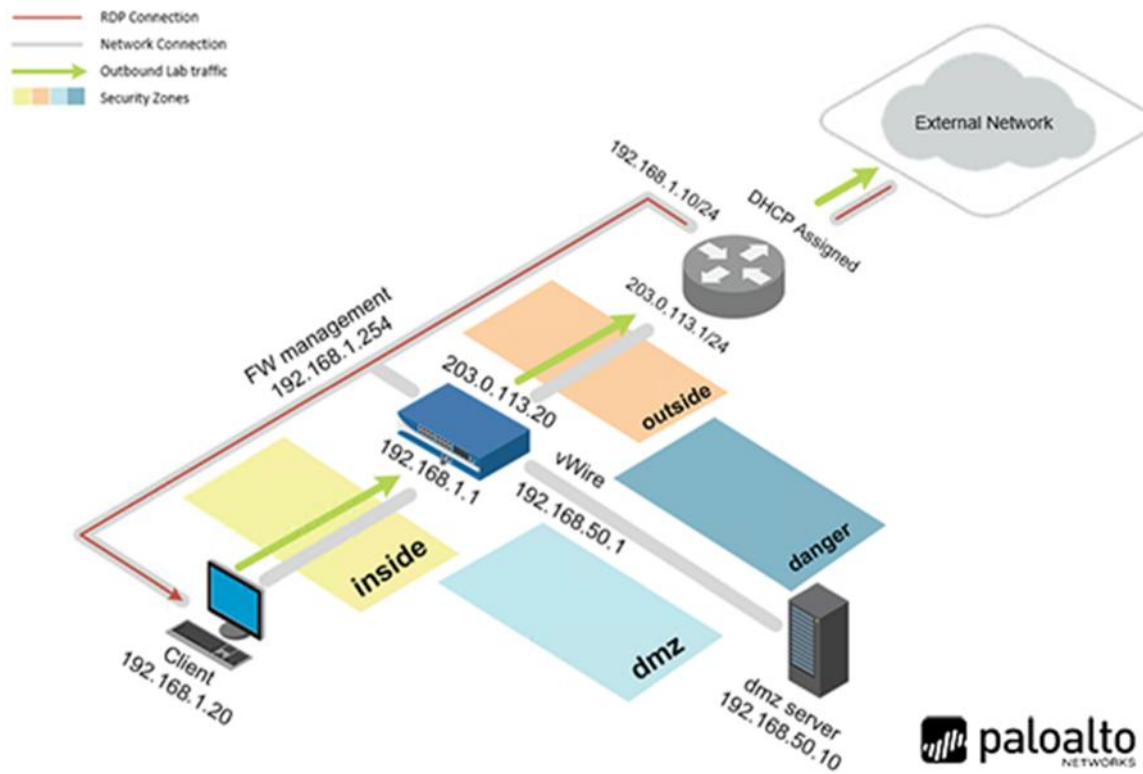
In this lab, you will create a File Blocking Profile to block PDF files. After you have created a File Blocking Profile, you will then test the profile by trying to download a PDF file.

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.

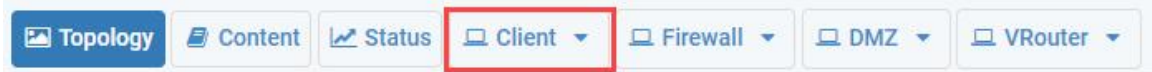
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

9 Lab: Preventing Threats from the Internet with File Blocking

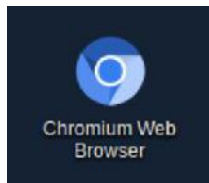
9.0 Load Lab Configuration

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

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



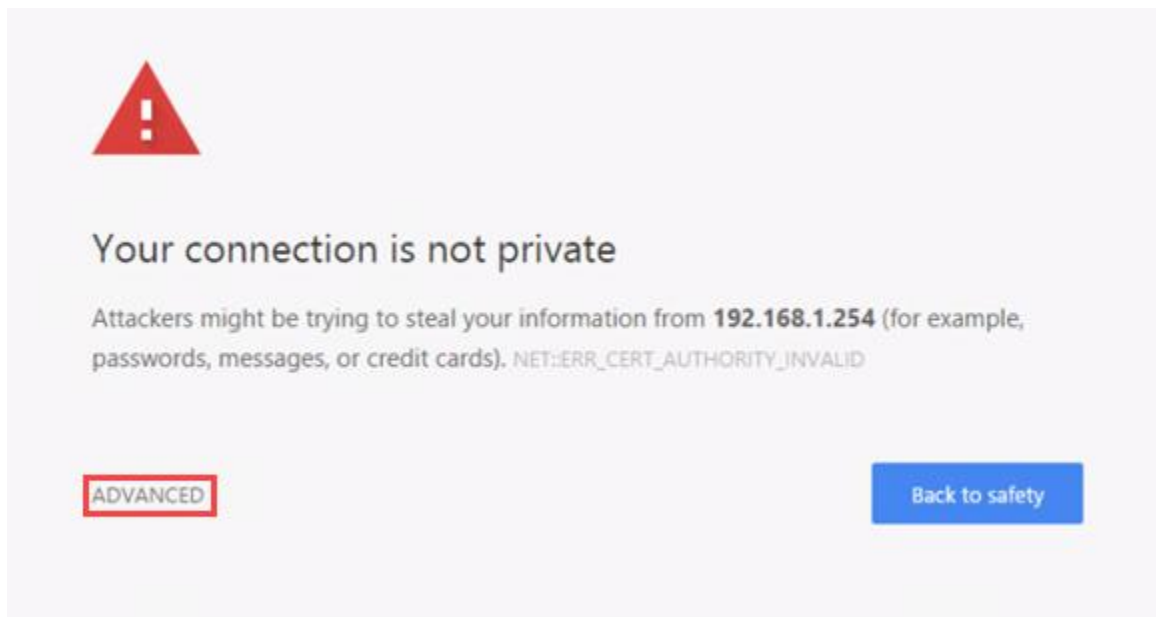
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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



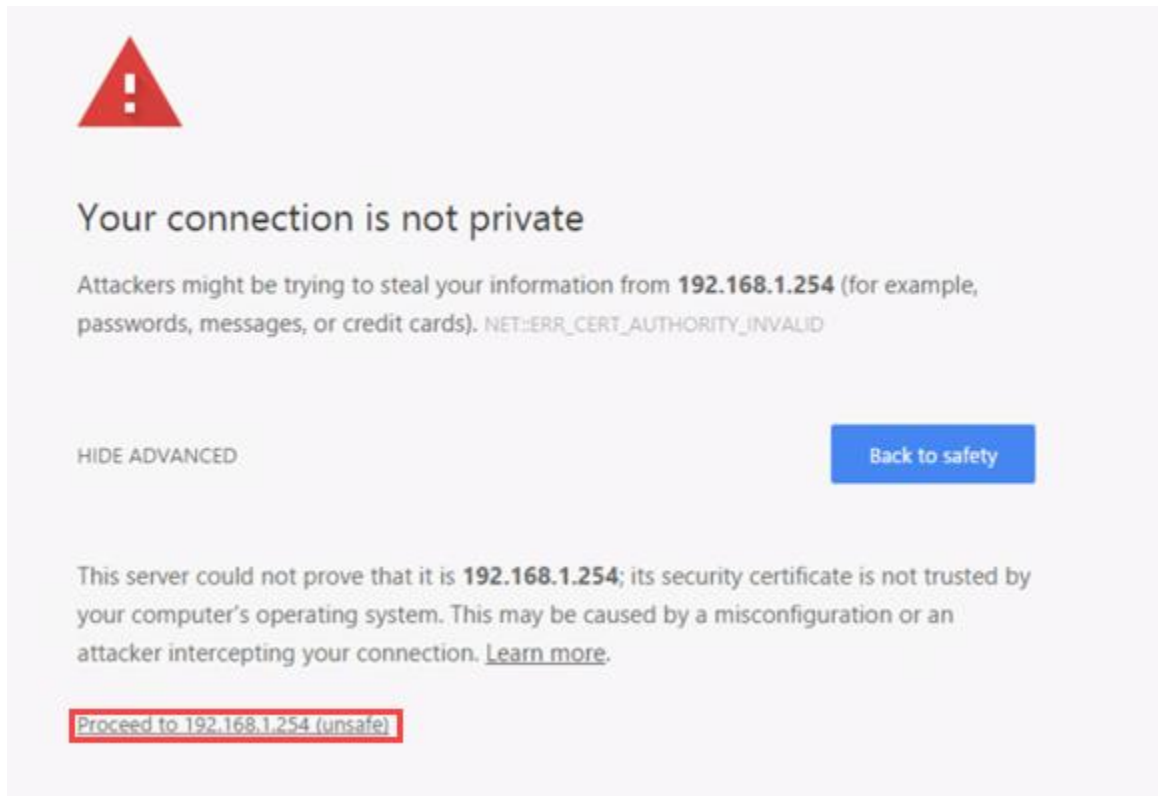
5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.





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.

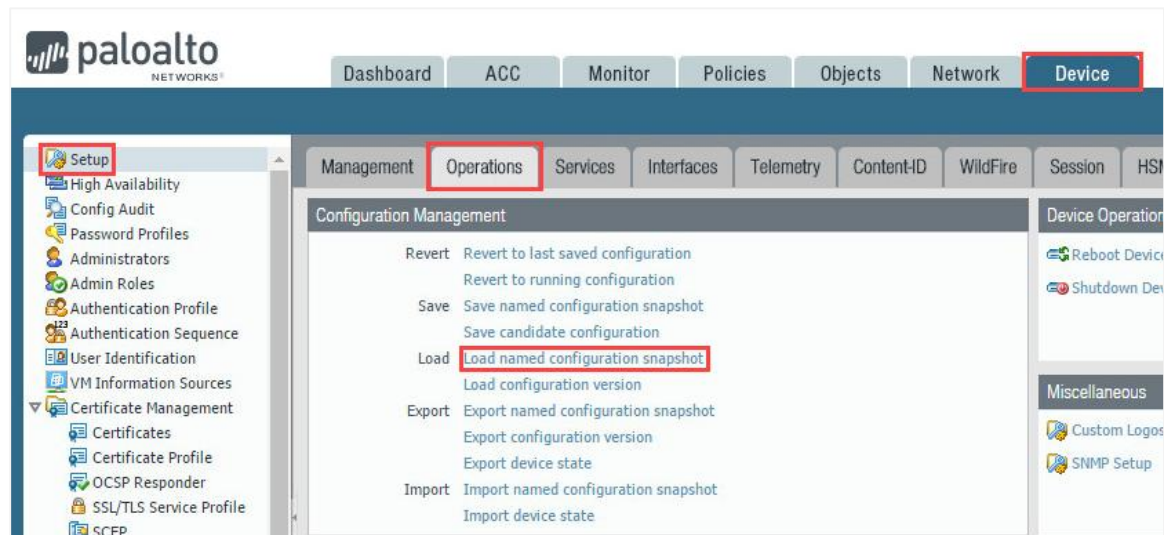
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



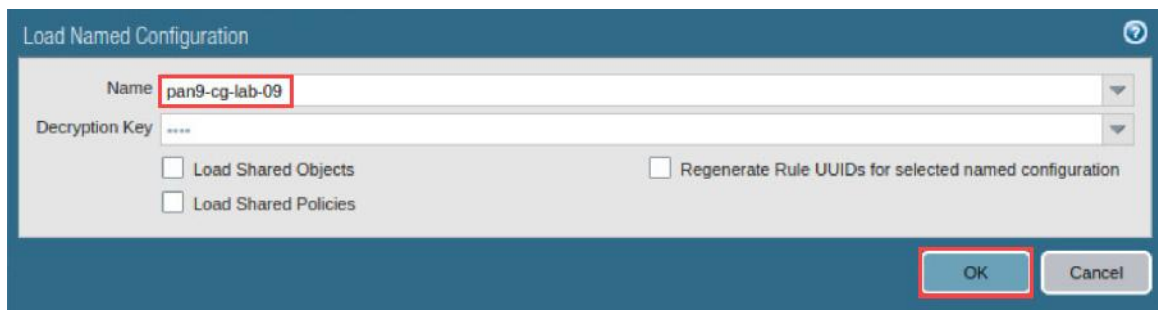
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



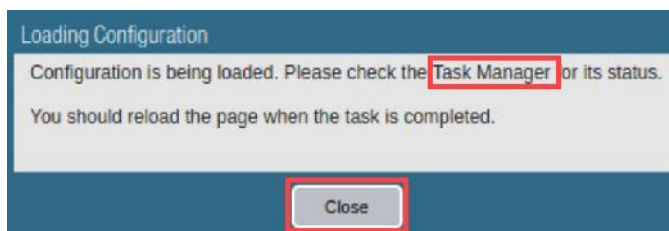
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



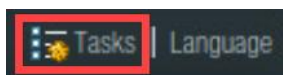
9. In the *Load Named Configuration* window, select **pan9-cg-lab-09** from the *Name* dropdown box and click **OK**.



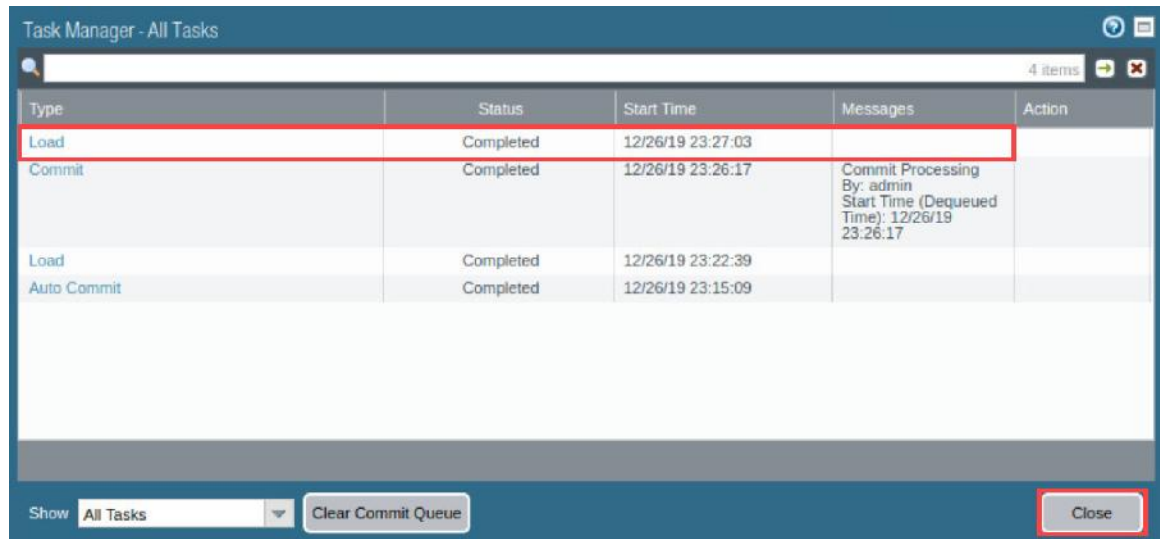
10. In the Loading Configuration window, a message will show *Configuration is being loaded*. Please check the *Task Manager* for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



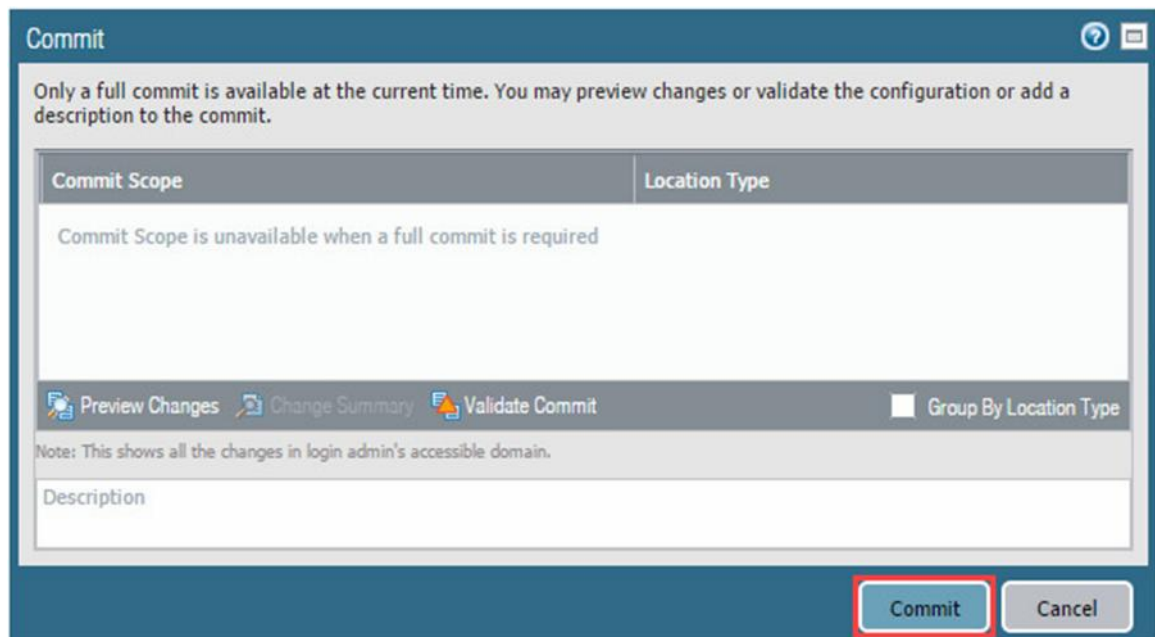
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



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.

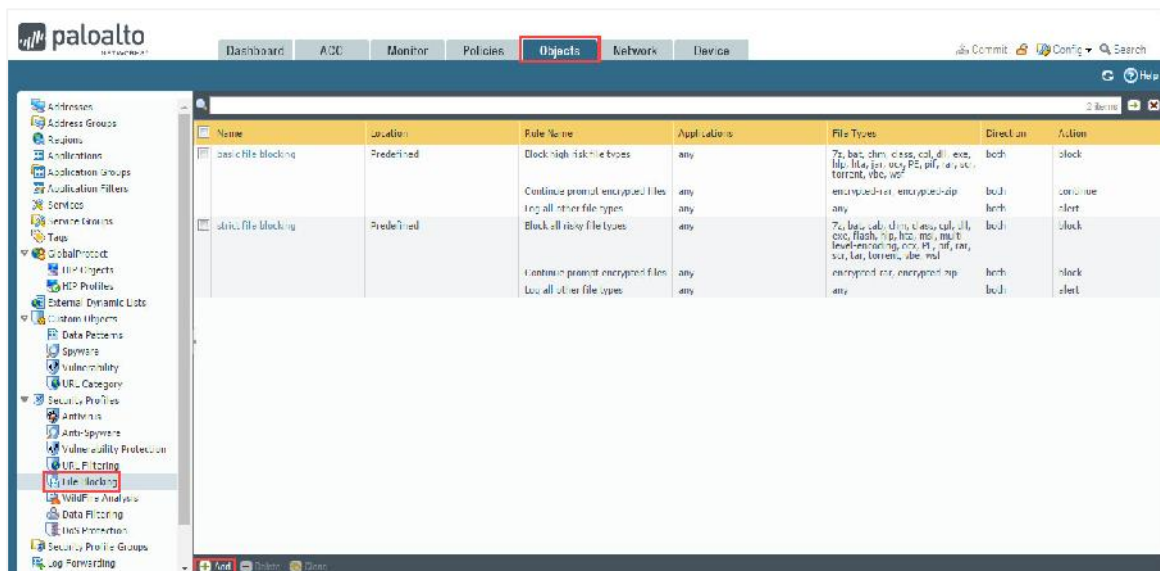


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

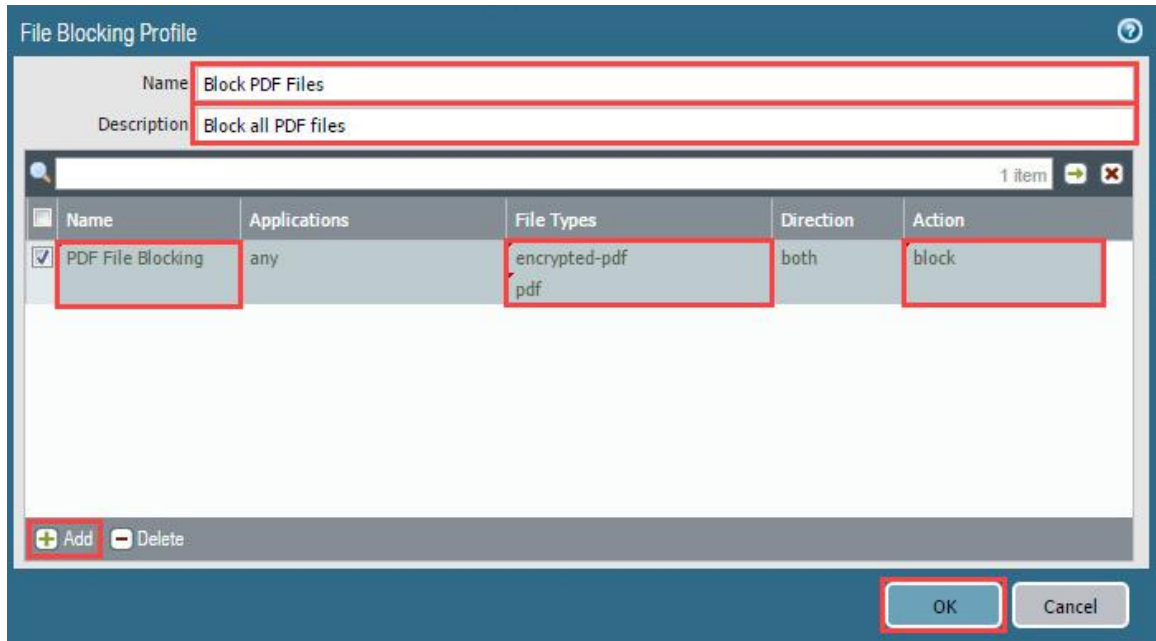
9.1 Create a File Blocking Security Profile

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

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



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**.



The screenshot shows the 'File Blocking Profile' configuration window. The 'Name' field is 'Block PDF Files' and the 'Description' is 'Block all PDF files'. Below is a table with one item:

Name	Applications	File Types	Direction	Action
PDF File Blocking	any	encrypted-pdf pdf	both	block

At the bottom, there are 'Add' and 'Delete' buttons, and 'OK' and 'Cancel' buttons.

9.2 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.

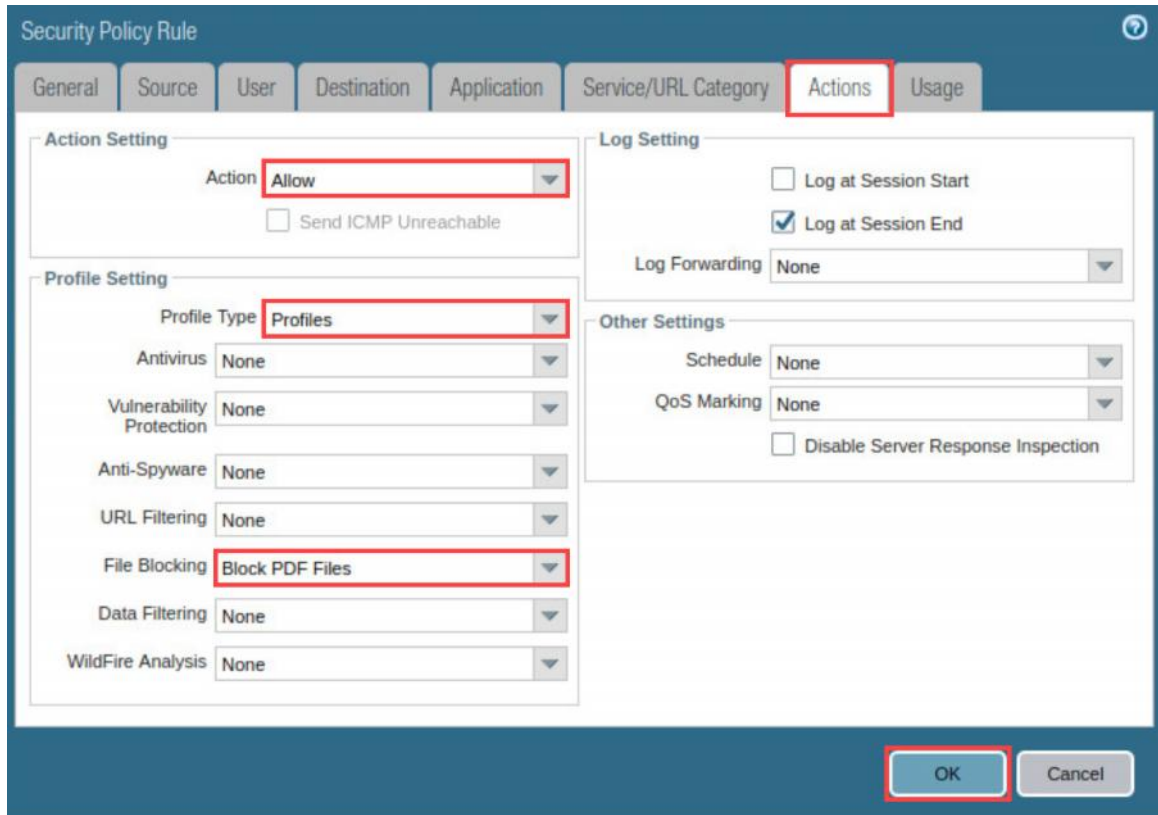
1. Navigate to **Policies > Security** and click on **Allow-Inside-DMZ**.



The screenshot shows the Palo Alto Networks web interface. The 'Policies' tab is selected, and the 'Security' sub-tab is active. A table lists the security policies:

	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone
1	Allow-Inside-Out	none	universal	inside	any	any	any	
2	Allow-Inside-DMZ	none	universal	inside	any	any	any	
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
4	interzone-default	none	interzone	any	any	any	any	any

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**.

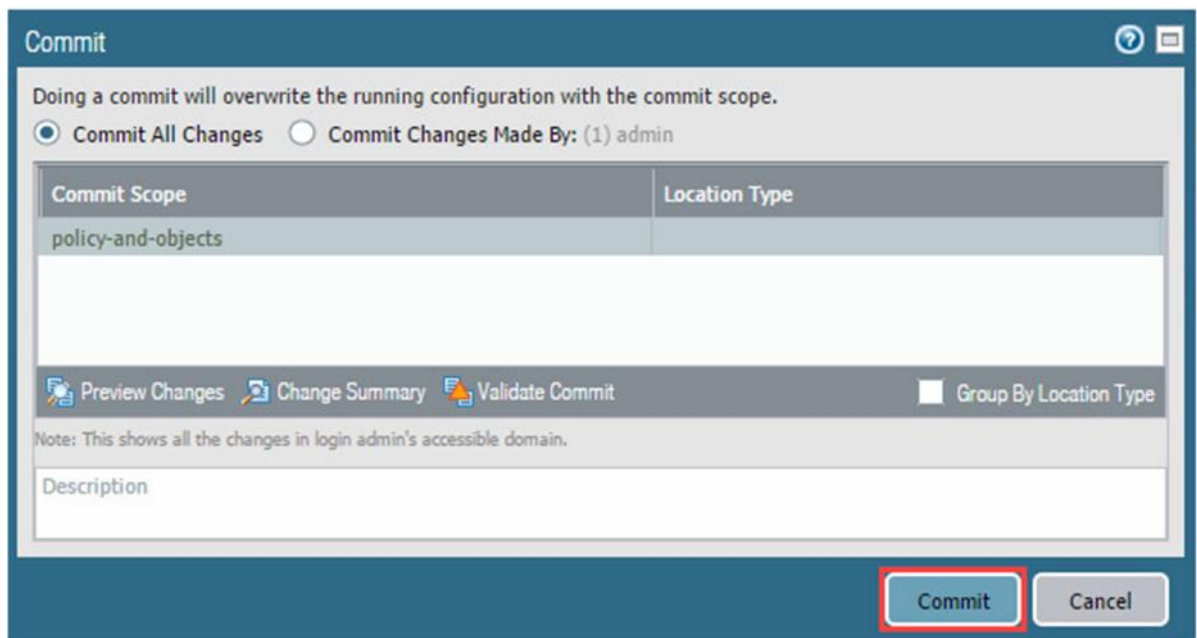


The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow' and 'Send ICMP Unreachable' unchecked. The 'Profile Setting' section has 'Profile Type' set to 'Profiles', and 'File Blocking' set to 'Block PDF Files'. The 'Log Setting' section has 'Log at Session End' checked and 'Log Forwarding' set to 'None'. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None', and 'Disable Server Response Inspection' unchecked. The 'OK' button is highlighted with a red box.

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.



9.3 Test the File Blocking Profile

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

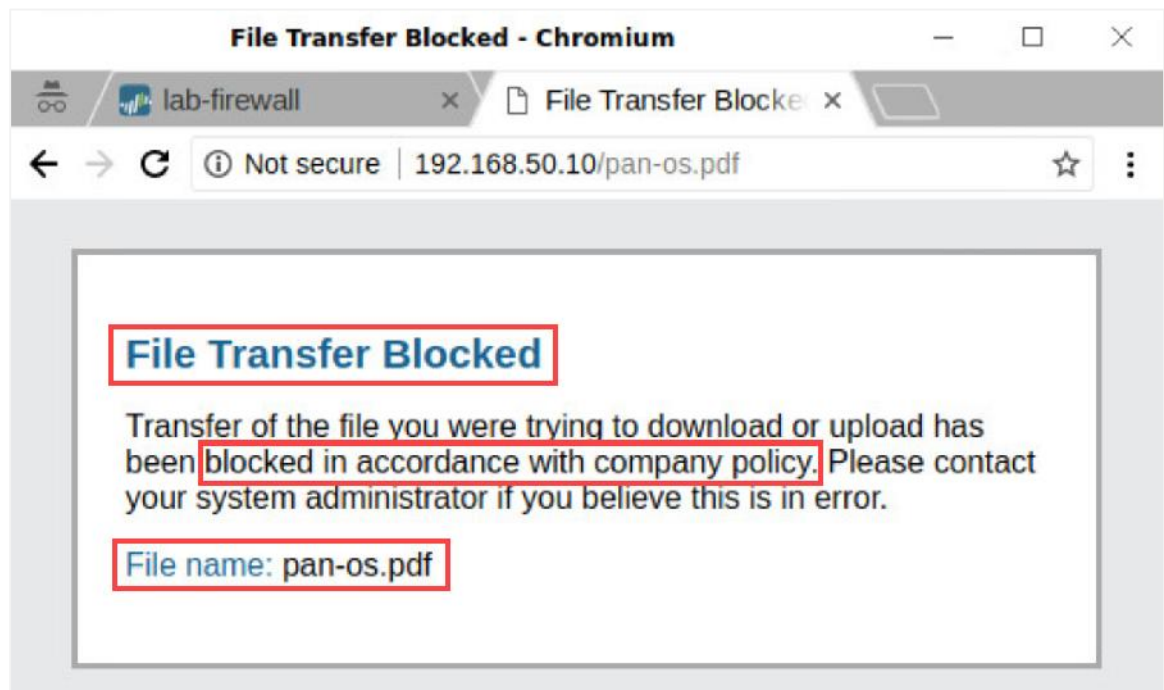
1. Click on the **New tab** button in the *Chromium* web browser.



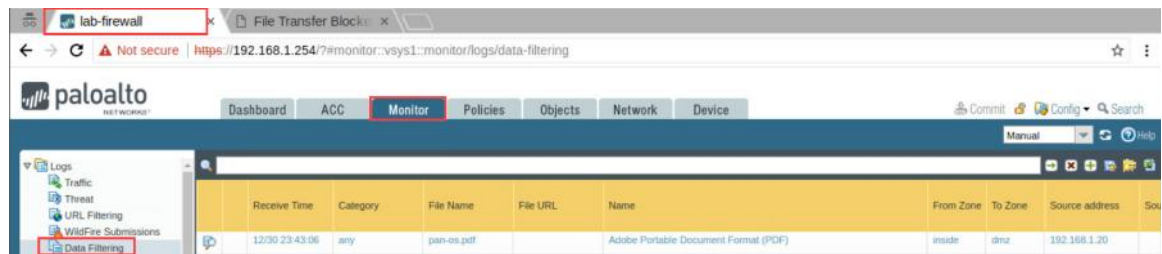
2. In the *address bar*, type `http://192.168.50.10/pan-os.pdf` and press **Enter**.



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



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



- Notice that **pan-os.pdf** is 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.

File Name	Name	Source address	Destination address	Application	Action
pan-os.pdf	Adobe Portable Document Format (PDF)	192.168.1.20	192.168.50.10	web-browsing	deny

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