



CLOUD SECURITY FUNDAMENTALS V2

Lab 1: Protecting Sensitive Data

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 Protecting Sensitive Data	6
1.0 Load Lab Configuration	6
1.1 Create a New Data Pattern	11
1.2 Create a Data Filtering Security Profile	13
1.3 Apply the Data Filtering Profile to the Security Policy	15
1.4 Create a Text File with Fake Social Security Numbers	17
1.5 Monitor Sensitive Data in the Palo Alto Networks Firewall	19

Introduction

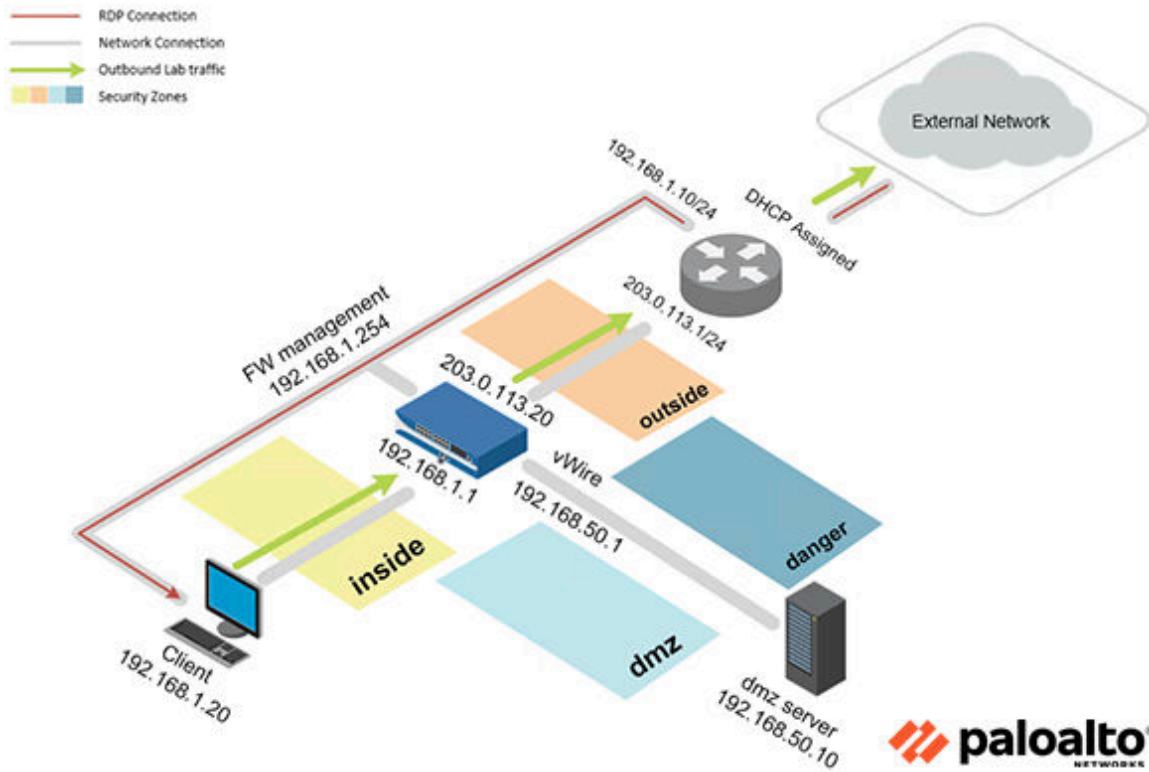
In this lab, you will set up a Data Filtering Profile to protect sensitive and confidential information, such as Social Security numbers.

Objective

In this lab, you will perform the following tasks:

- Create a New Data Pattern
- Create a Data Filtering Security Profile
- Apply the Data Filtering Profile to the Security Policy
- Create a Text File with Fake Social Security Numbers
- Monitor Sensitive Data in the Palo Alto Networks Firewall

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.

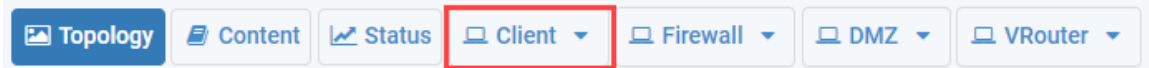
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Protecting Sensitive Data

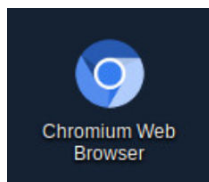
1.0 Load Lab Configuration

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

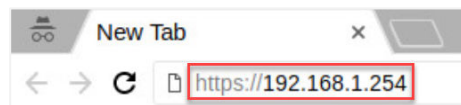
1. Click on the **Client** tab to access the Client PC.



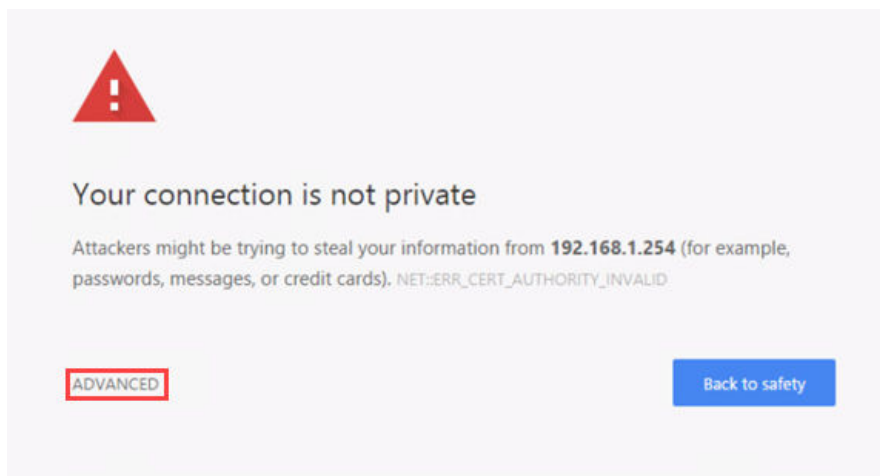
2. Log in to the Client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



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

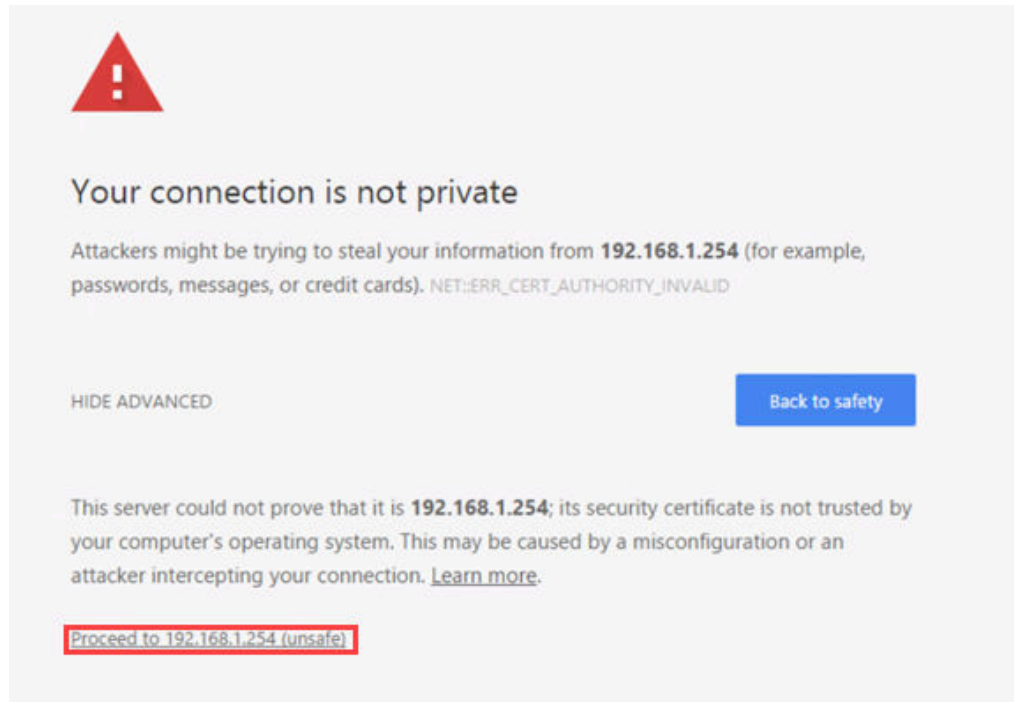


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

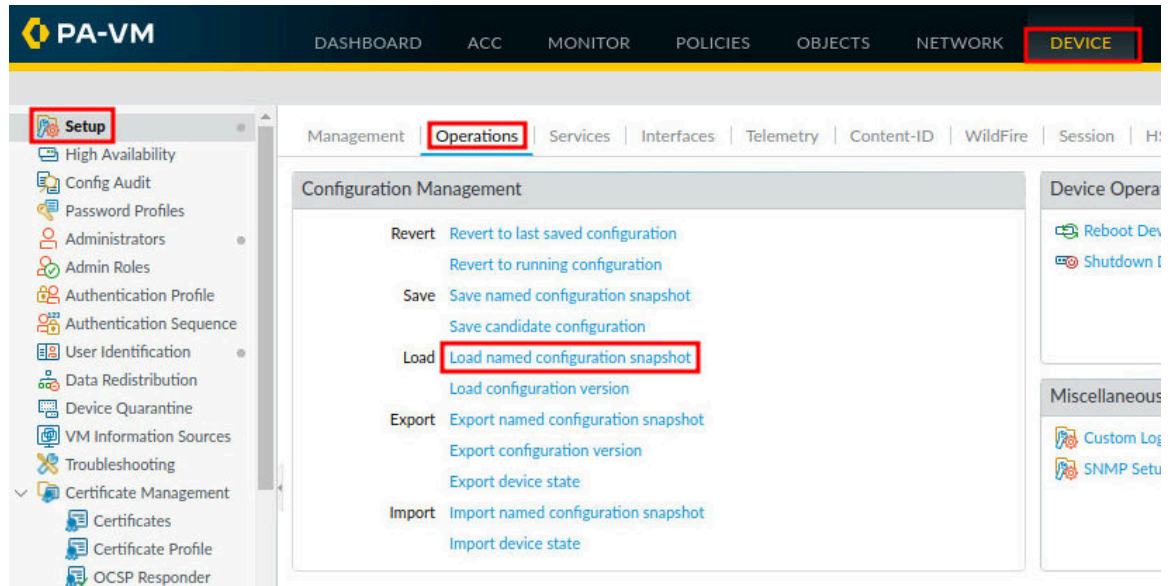
- Click on **Proceed to 192.168.1.254 (unsafe)**.



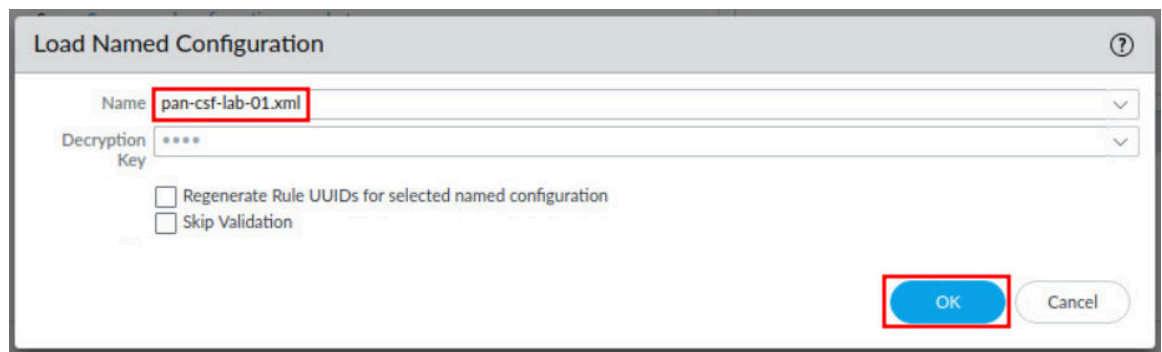
- Log in to the Firewall web interface as username admin, password Pa10Alt0!.



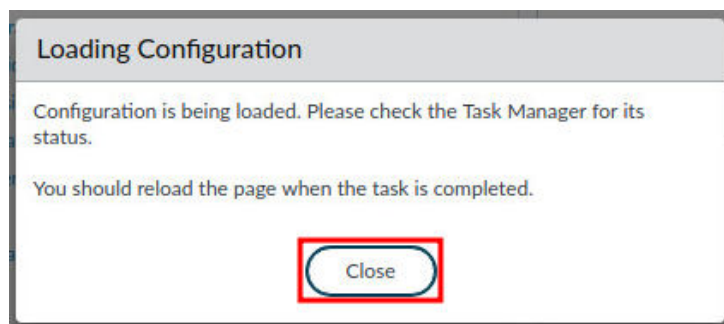
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-csf-lab-01.xml** from the *Name* dropdown box and click **OK**.



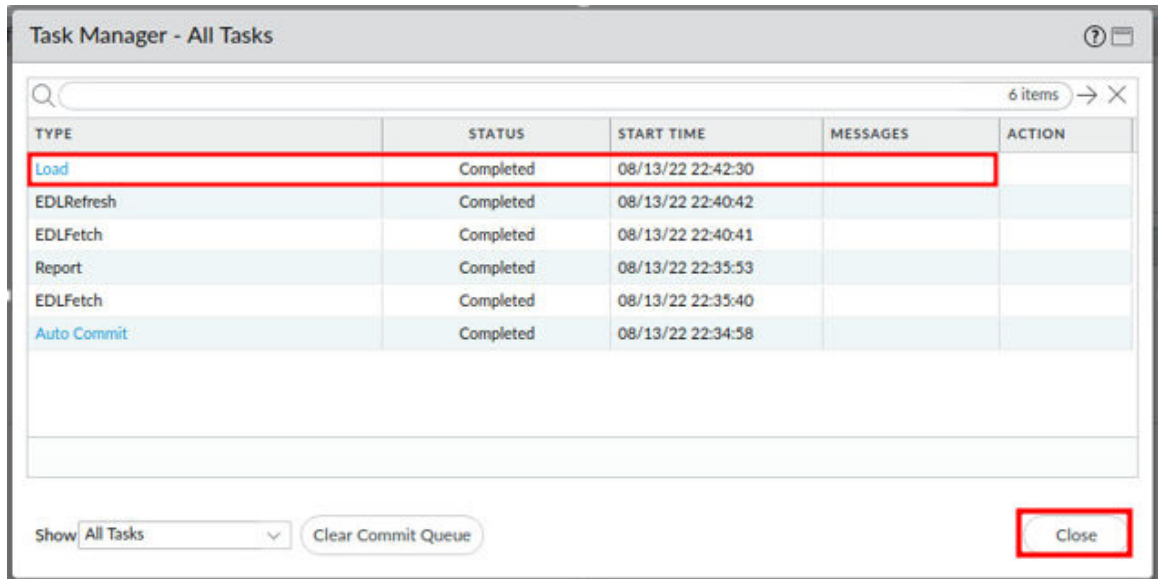
10. In the Loading Configuration window, a message will show *Configuration is being loaded*. Please check the Task Manager for its status. You should reload the page when the task is completed. Click **Close** to continue.



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



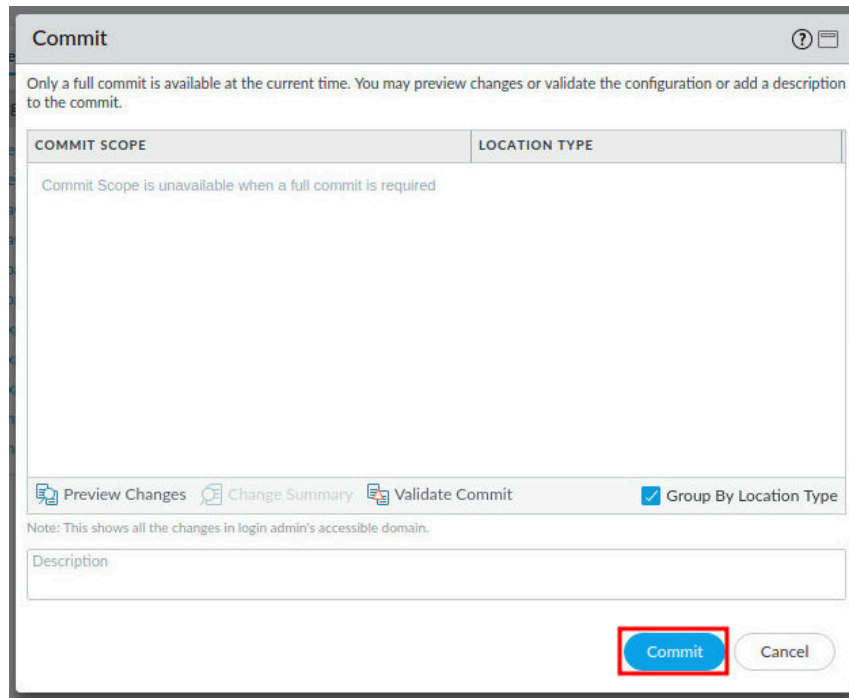
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**



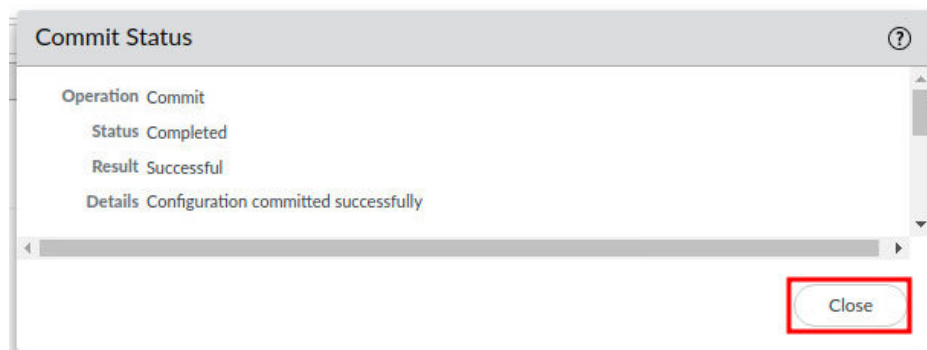
13. Click the **Commit** link located at the top-right of the web interface.



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



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

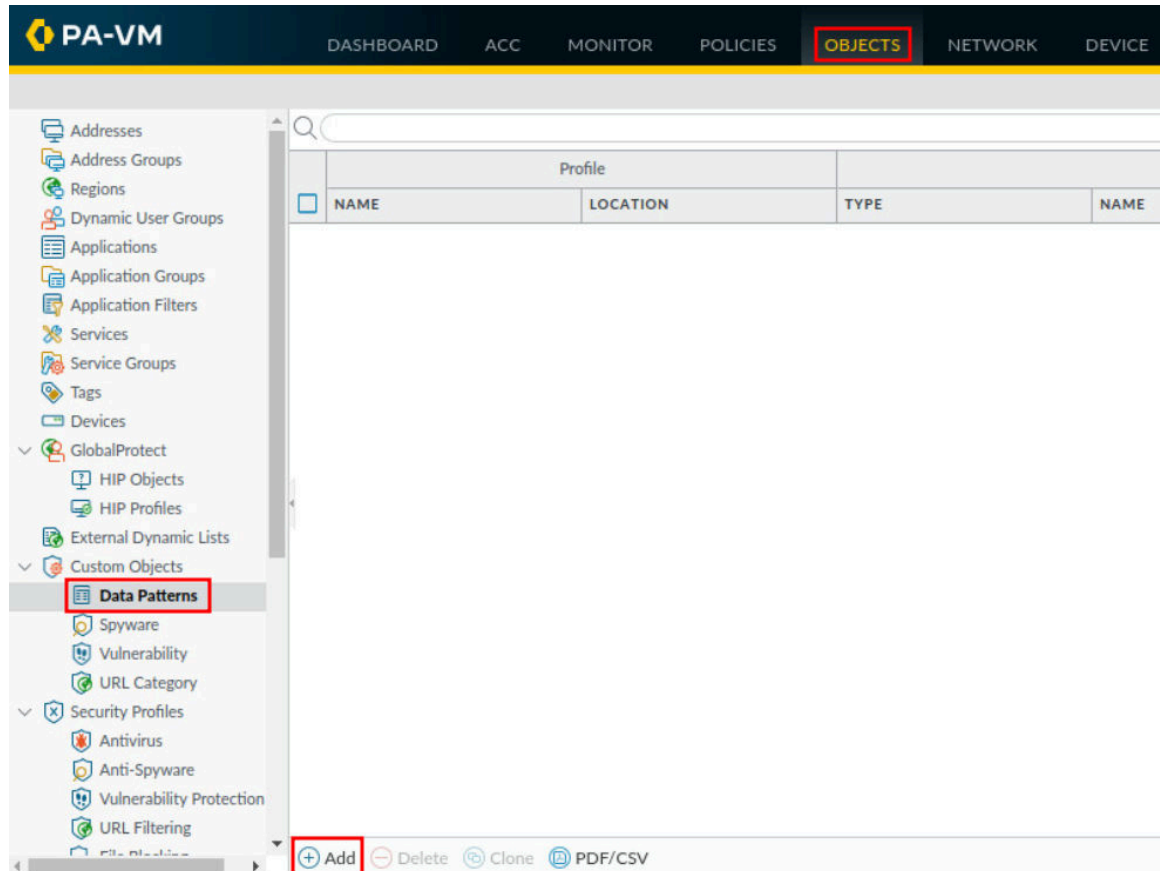


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

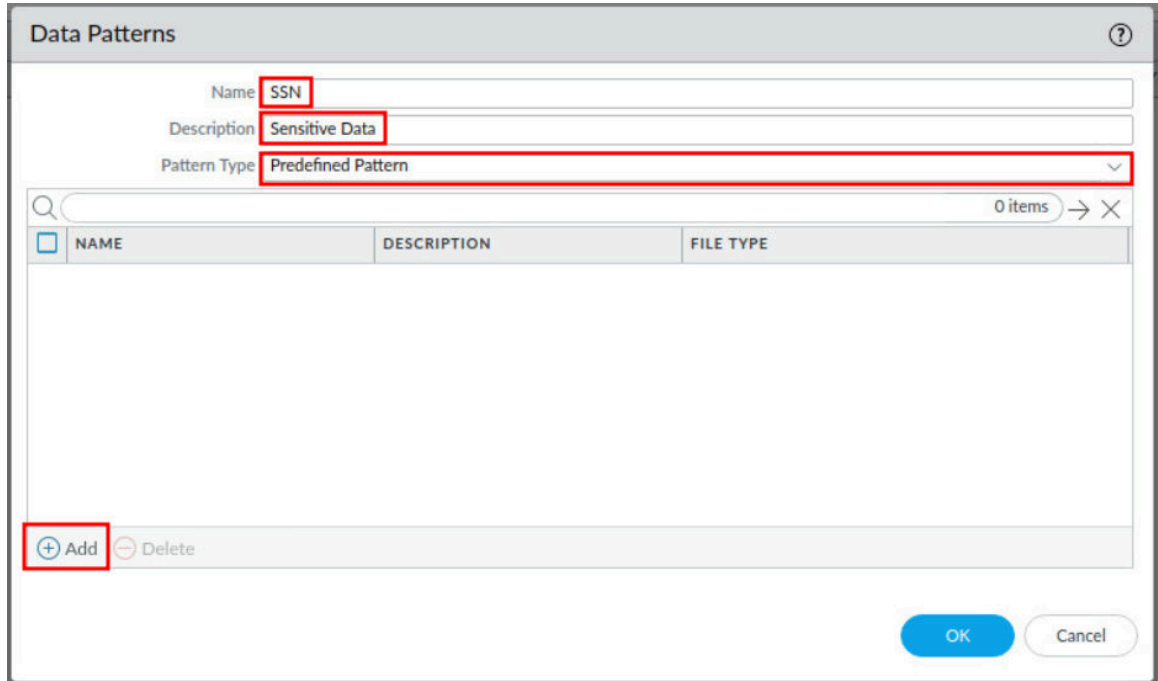
1.1 Create a New Data Pattern

In this section, you will create a new data pattern. Data pattern objects detect the information that needs to be filtered. Three types of data patterns are utilized for scanning sensitive information. Predefined patterns are preset patterns used to detect Social Security and credit card numbers. Regular expressions are used to create custom data patterns. File properties are used to scan files for specific file properties and values. For this lab, you will use predefined patterns.

1. Navigate to **Objects > Custom Objects > Data Patterns > Add**.

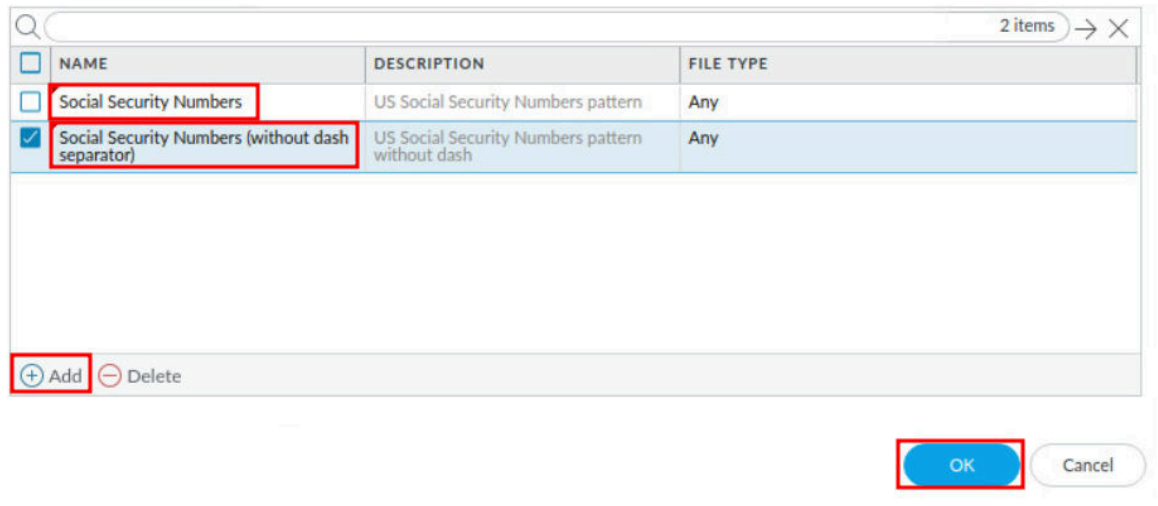


2. In the *Data Patterns* window, type SSN in the *Name* field. Then, type Sensitive Data in the *Description* field. Next, select **Predefined Pattern** for the *Pattern Type*. Finally, click **Add**.



The screenshot shows the 'Data Patterns' window. The 'Name' field contains 'SSN', the 'Description' field contains 'Sensitive Data', and the 'Pattern Type' dropdown is set to 'Predefined Pattern'. Below these fields is a table with columns 'NAME', 'DESCRIPTION', and 'FILE TYPE'. The table is currently empty. At the bottom left, there is a '+ Add' button and a '- Delete' button. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. In the *Data Patterns* window, select **Social Security Numbers**. Next, click **Add** again and select **Social Security Numbers (without dash separator)**. Finally, click **OK**.



The screenshot shows the 'Data Patterns' window after adding two items. The table now contains two rows:

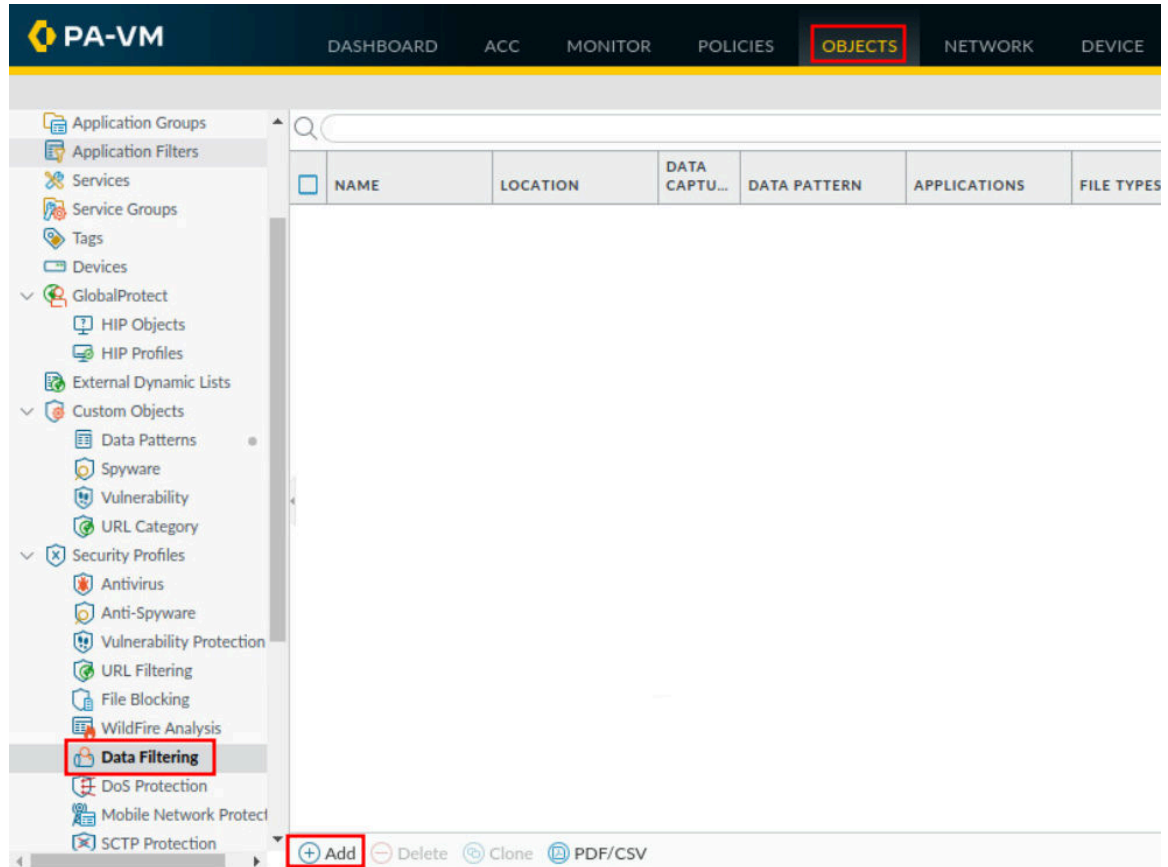
	NAME	DESCRIPTION	FILE TYPE
<input type="checkbox"/>	Social Security Numbers	US Social Security Numbers pattern	Any
<input checked="" type="checkbox"/>	Social Security Numbers (without dash separator)	US Social Security Numbers pattern without dash	Any

At the bottom left, there is a '+ Add' button and a '- Delete' button. At the bottom right, there are 'OK' and 'Cancel' buttons.

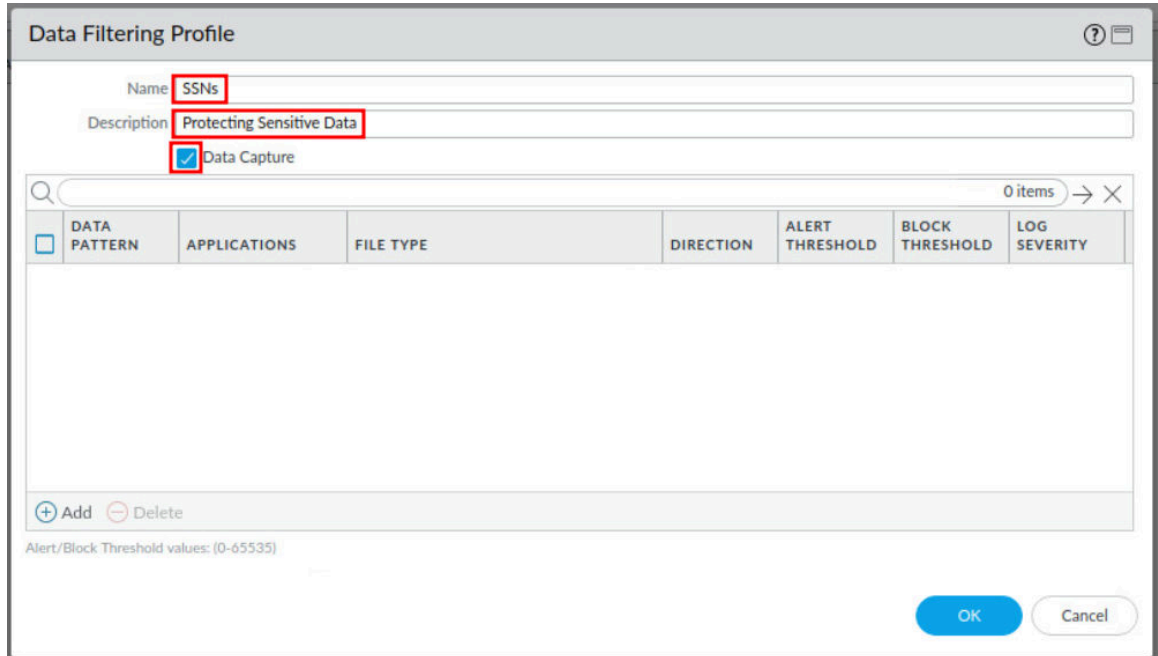
1.2 Create a Data Filtering Security Profile

In this section, you will create a Data Filtering Security Profile. Data Filtering Security Profiles prevent sensitive information such as credit card and Social Security numbers from leaving a secured network.

1. Navigate **Objects > Security Profiles > Data Filtering > Add**.

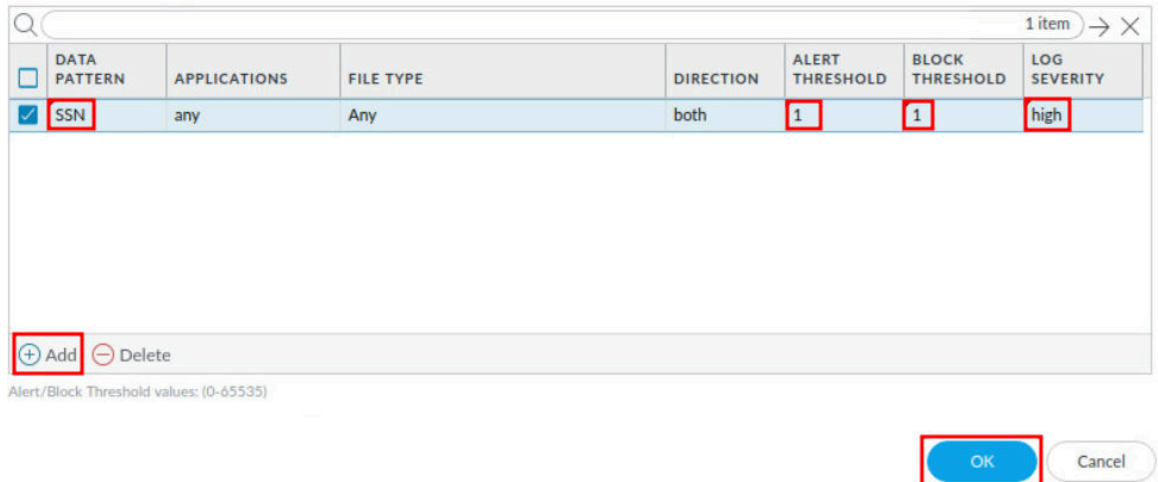


2. In the *Data Filtering Profile* window, type SSNs in the *Name* field. Then, type **Protecting Sensitive Data** in the *Description* field. Finally, click the checkbox for **Data Capture**.



The **Data Filtering Profile** window is shown. The **Name** field contains "SSNs", the **Description** field contains "Protecting Sensitive Data", and the **Data Capture** checkbox is checked. Below the fields is a table with columns: DATA PATTERN, APPLICATIONS, FILE TYPE, DIRECTION, ALERT THRESHOLD, BLOCK THRESHOLD, and LOG SEVERITY. The table is currently empty, showing "0 items". At the bottom, there are "Add" and "Delete" buttons, and a note: "Alert/Block Threshold values: (0-65535)". The "OK" and "Cancel" buttons are at the bottom right.

3. In the *Data Filtering Profile* window, click **Add**. Select **SSN** in the *Data Pattern* field. Then, in the *Alert* and *Block Threshold* fields, type 1 for the values. Next, select **high** from the *Log Severity* dropdown. Finally, click **OK**.



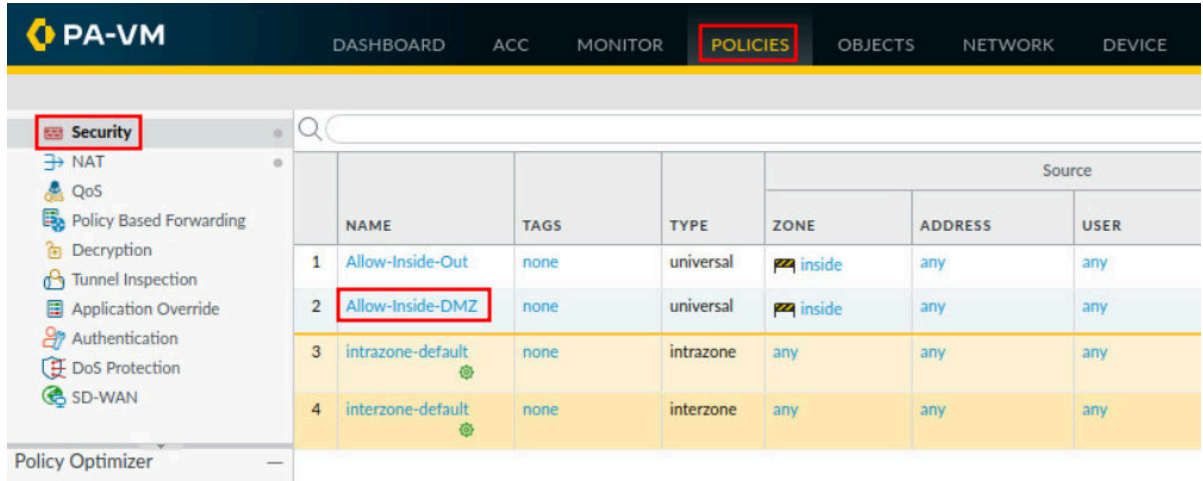
The **Data Filtering Profile** window is shown with one item added to the table. The **Add** button is highlighted. The table has one row with the following values: **SSN** (Data Pattern), any (Applications), Any (File Type), both (Direction), 1 (Alert Threshold), 1 (Block Threshold), and high (Log Severity). The "OK" button is highlighted. The "Alert/Block Threshold values: (0-65535)" note is at the bottom.

DATA PATTERN	APPLICATIONS	FILE TYPE	DIRECTION	ALERT THRESHOLD	BLOCK THRESHOLD	LOG SEVERITY
SSN	any	Any	both	1	1	high

1.3 Apply the Data Filtering Profile to the Security Policy

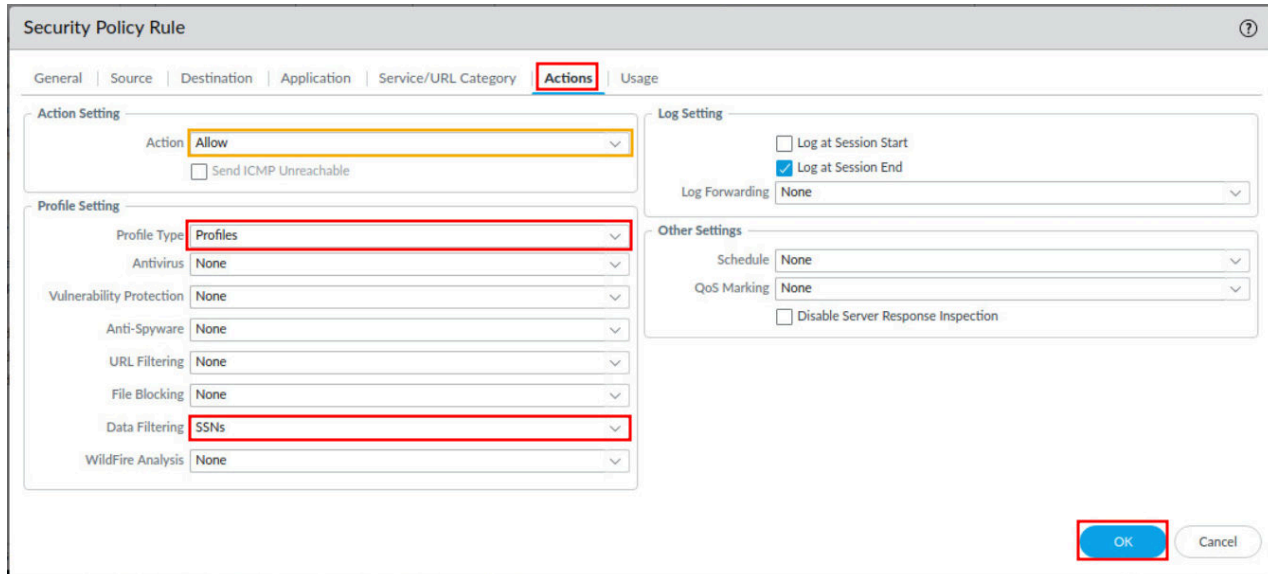
In this section, you will apply the Data Filtering Security Profile you created to the **Allow-Inside-DMZ** Security Policy.

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



	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	Allow-Inside-Out	none	universal	inside	any	any
2	Allow-Inside-DMZ	none	universal	inside	any	any
3	intrazone-default	none	intrazone	any	any	any
4	interzone-default	none	interzone	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 **SSNs** in the *Data Filtering* dropdown and click **OK**.



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type: **Profiles**

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: **SSNs**

WildFire Analysis: None

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

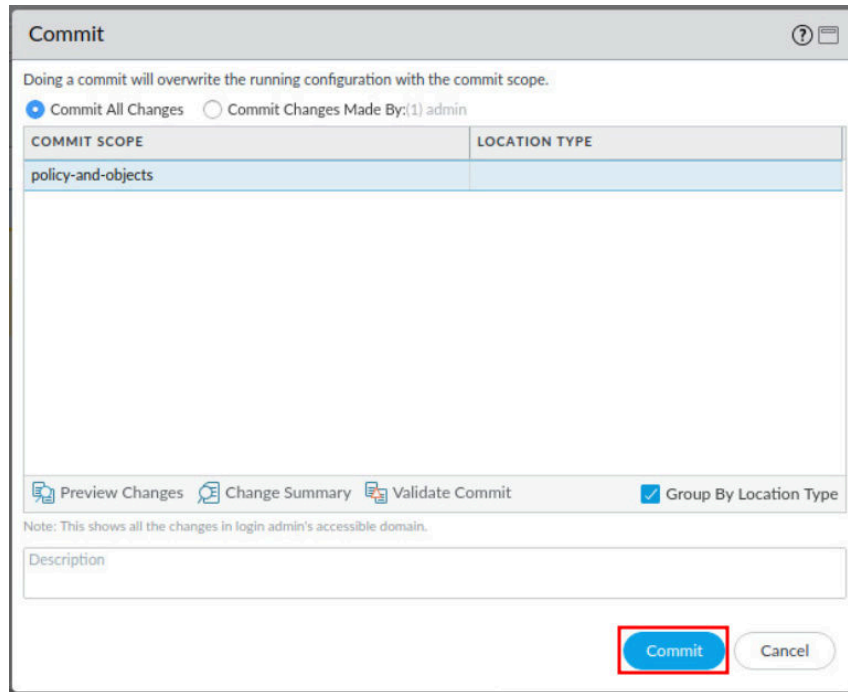
☐ Disable Server Response Inspection

OK Cancel

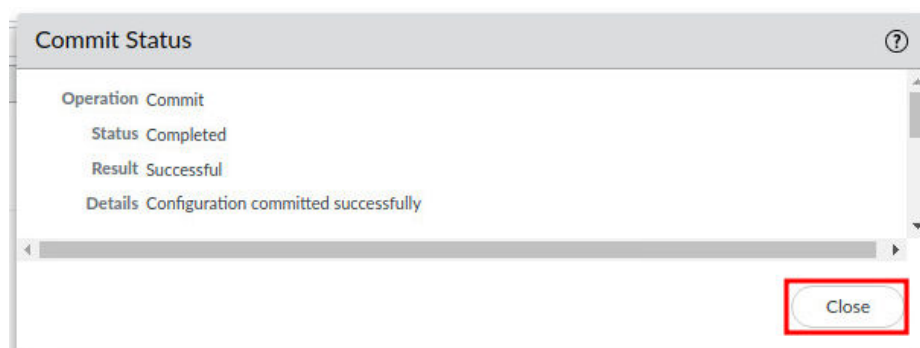
3. Click the **Commit** link located at the top-right of the web interface.



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



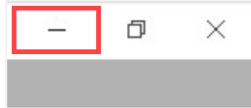
5. When the commit operation successfully completes, click **Close** to continue.



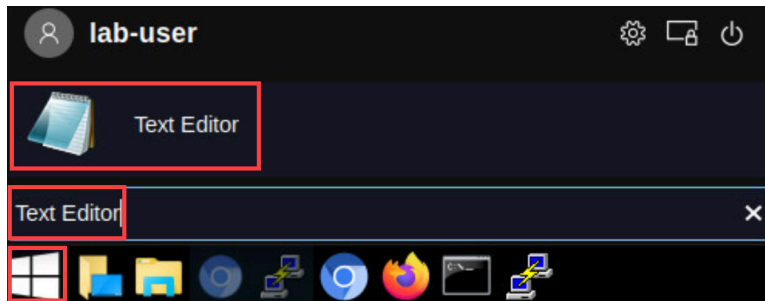
1.4 Create a Text File with Fake Social Security Numbers

In this section, you will create a text file in Notepad with fake Social Security numbers to test the policy you just applied to the Firewall.

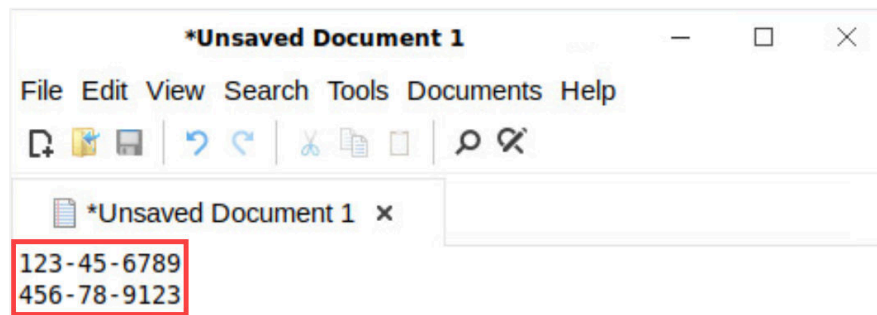
1. Minimize *Chromium* in the upper-right.



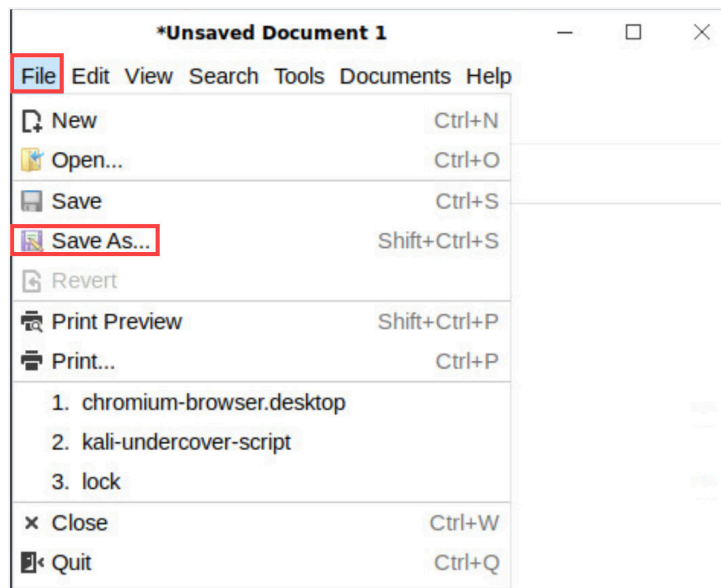
2. Click on the **Start** icon, type **Text Editor**, and click **Enter**.



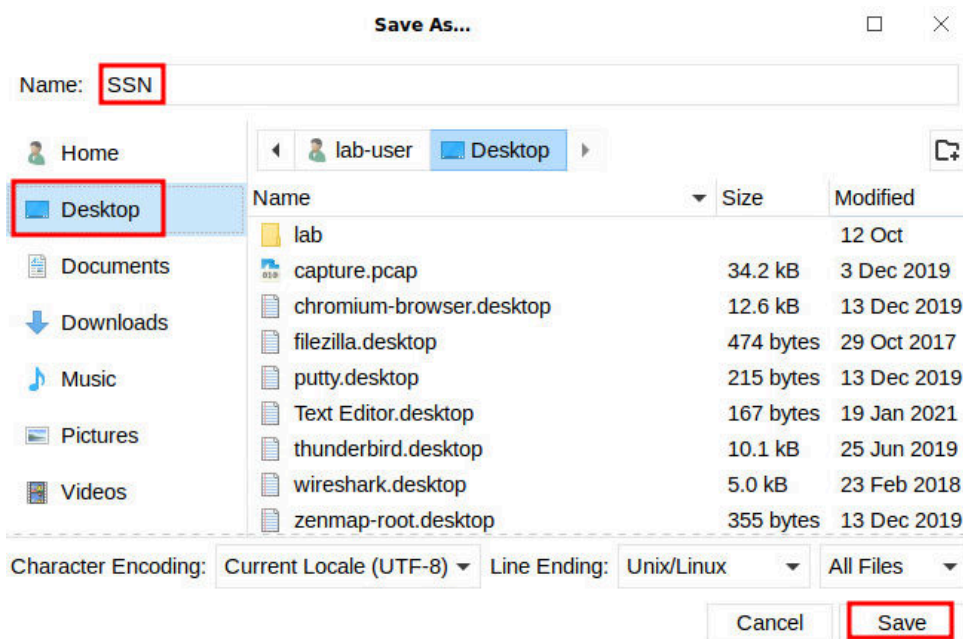
3. In the *Unsaved Document 1* window, type 123-45-6789 and 456-78-9123. These will be the fake Social Security numbers.



- Click **File > Save As....**



- In the *Save As* window, type SSN in the *Name* field. Then, click Desktop on the left. Finally, click **Save**.



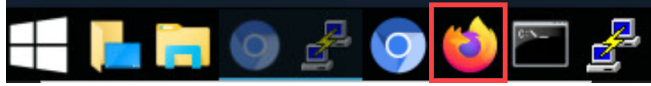
- Click the **X** in the upper-right to close the Text Editor.



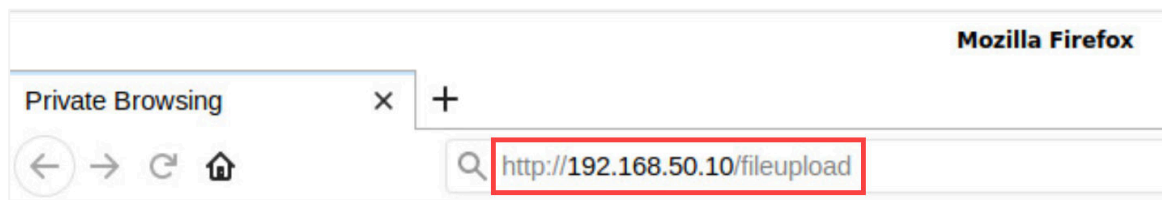
1.5 Monitor Sensitive Data in the Palo Alto Networks Firewall

In this section, you will monitor the Social Security number text file created in the previous section. You will notice that the text file you created has been blocked by the Data Security Profile, *SSN*.

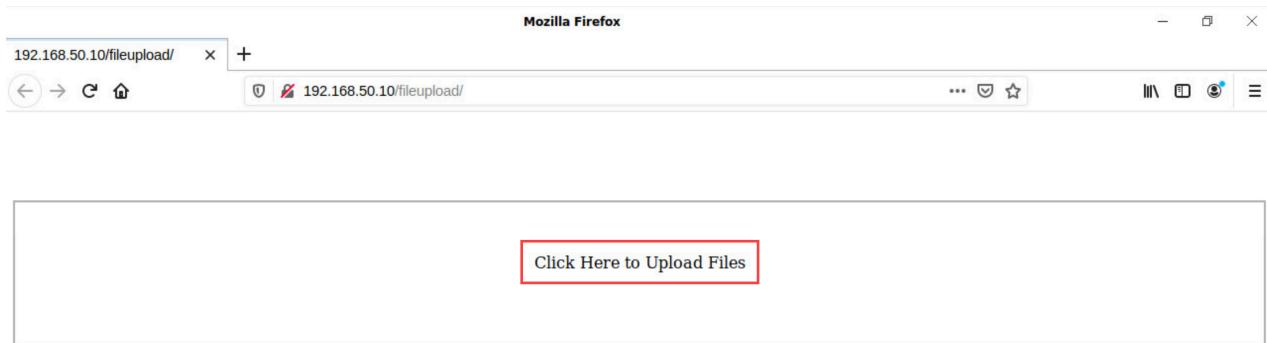
1. Navigate and click on the **Firefox** browser in the Taskbar.



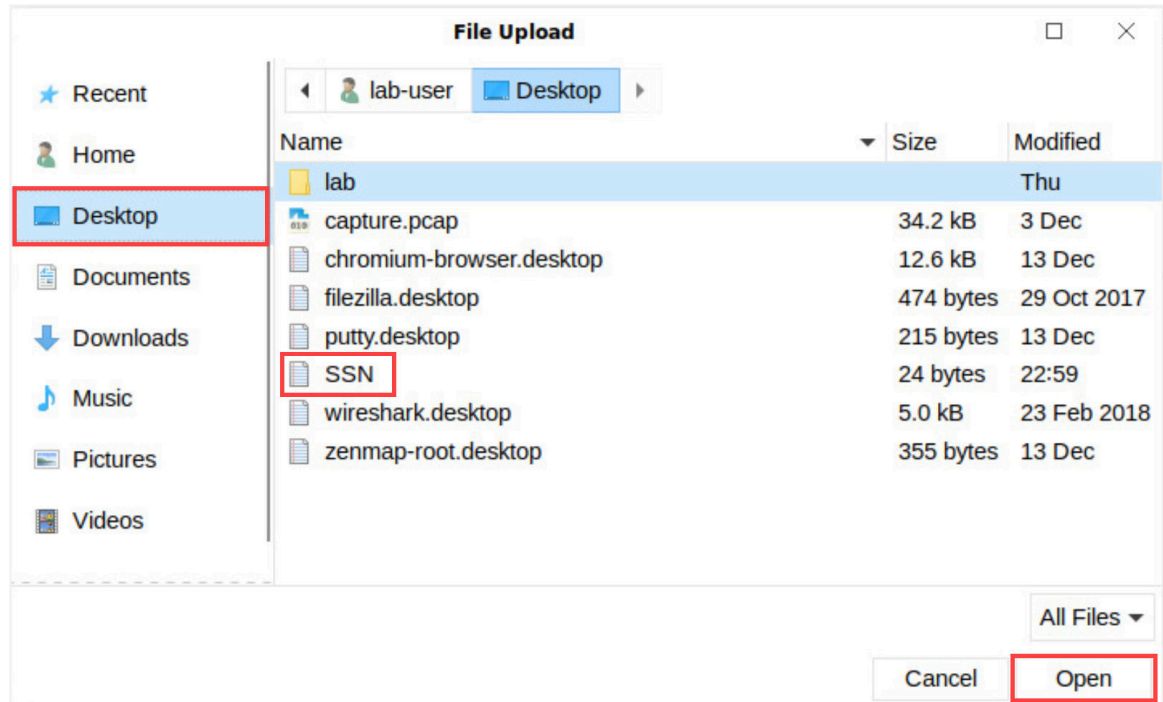
2. In the *Firefox* address field, type `http://192.168.50.10/fileupload` and press **Enter**.



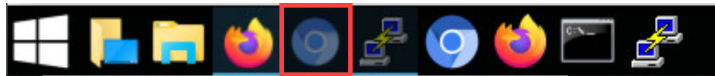
3. Click on **Click Here to Upload Files**.



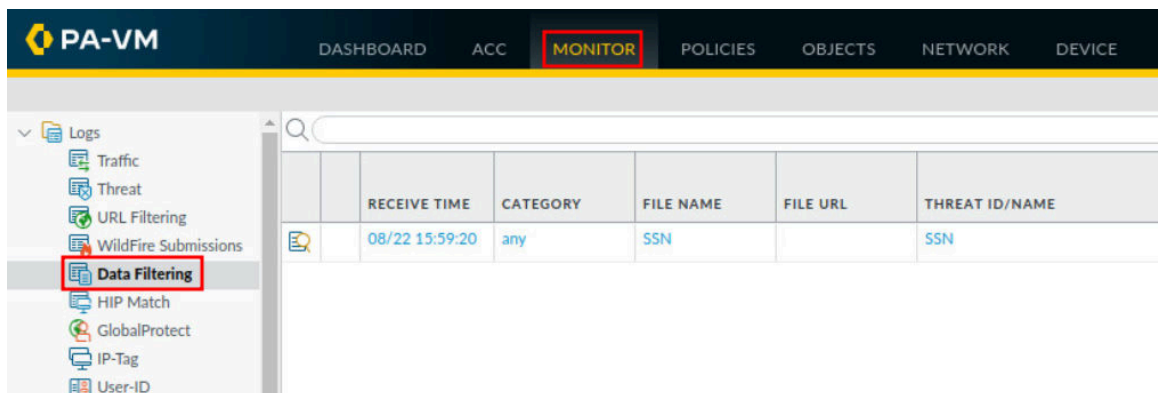
- In the *File Upload* window, click on **Desktop** on the left. Then, select the **SSN** text file. Finally, click **Open**.



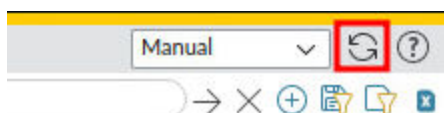
- Maximize *Chromium* from the Taskbar.




- Navigate to **Monitor > Logs > Data Filtering**.



You may need to click the **Refresh** button in the upper-right to refresh the logs and see the log entry appear.





7. Notice that the *SSN* was blocked by the *SSN Data Filtering Profile*.

		RECEIVE TIME	CATEGORY	FILE NAME	FILE URL	THREAT ID/NAME
		08/22 15:59:20	any	SSN		SSN



You may need to pause here for 5 minutes to let the logs populate before continuing.

8. Click on the **Detailed Log View** button.

		RECEIVE TIME	CATEGORY	FILE NAME	FILE URL	THREAT ID/NAME
		08/22 15:59:20	any	SSN ...		SSN

9. On the *Detailed Log View* window, click the **log** file that was just created.

Detailed Log View

General

Session ID 508

Action reset-server

Application web-browsing

Rule Allow-Inside-DMZ

Rule UUID 2ef2cd00-21ed-4c5e-9c72-603469c42ae8

Device SN 015351000081504

IP Protocol tcp

Log Action

Category any

Source

Source User

Source 192.168.1.20

Source DAG

Country 192.168.0.0-192.168.255.255

Port 60122

Zone inside

Interface ethernet1/2

X-Forwarded-For IP 0.0.0.0

Destination

Destination User

Destination 192.168.50.10

Destination DAG

Country 192.168.0.0-192.168.255.255

Port 80

Zone dmz

Interface ethernet1/3

Flags

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/08/22 15:59:29	end	web-browsing	allow	Allow-Inside-DMZ	2ef2cd...	1435		any				
	2022/08/22 15:59:20	data	web-browsing	reset-server	Allow-Inside-DMZ	2ef2cd...		high	any				SSN

Close

10. Notice the Application **web-browsing** was **reset**, and the Severity was **high** as applied by the Data Security Policy. The *General* section will show the Application, Protocol, and the Category it was assigned. The *Source* section is used to identify where the source originated, and the *Destination* section will identify where the file was designated.

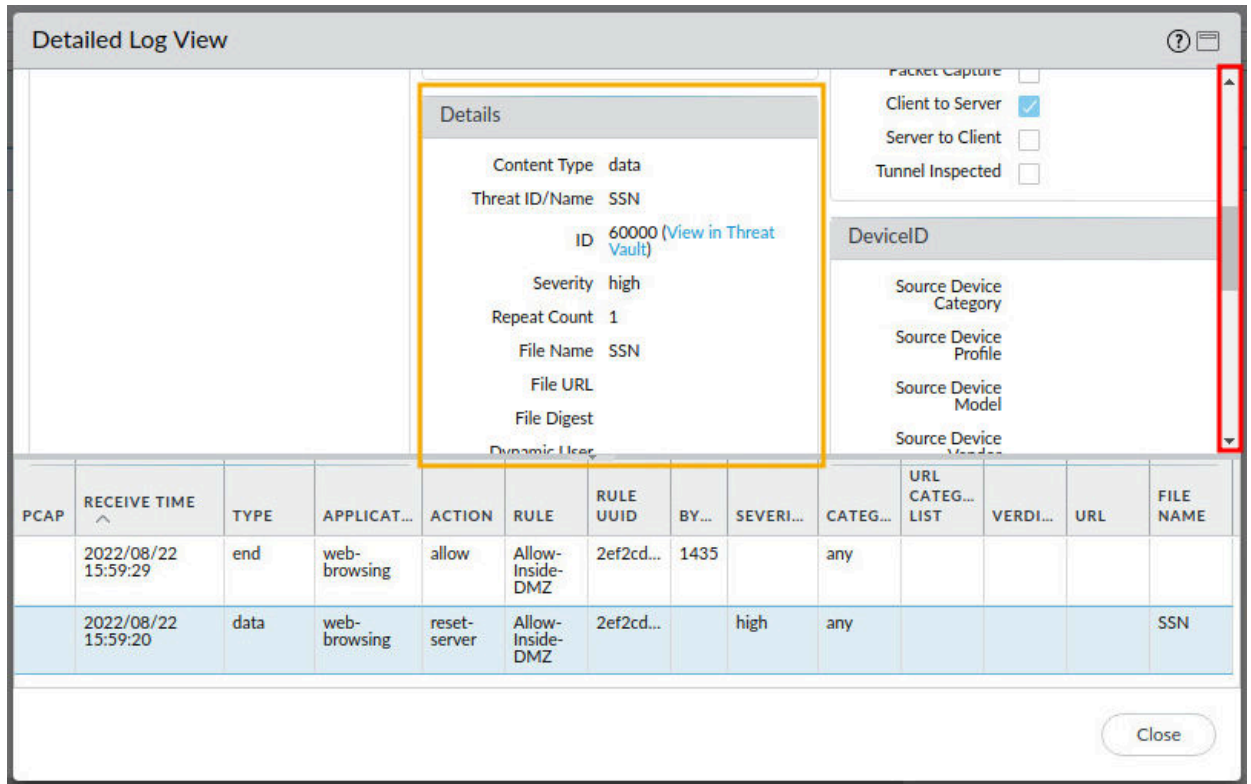
Detailed Log View

General			Source			Destination		
Session ID	508		Source User			Destination User		
Action	reset-server		Source	192.168.1.20		Destination	192.168.50.10	
Application	web-browsing		Source DAG			Destination DAG		
Rule	Allow-Inside-DMZ		Country	192.168.0.0-192.168.255.255		Country	192.168.0.0-192.168.255.255	
Rule UUID	2ef2cd00-21ed-4c5e-9c72-603469c42ae8		Port	60122		Port	80	
Device SN	015351000081504		Zone	inside		Zone	dmz	
IP Protocol	tcp		Interface	ethernet1/2		Interface	ethernet1/3	
Log Action			X-Forwarded-For IP	0.0.0.0				
Category	any					Flags		

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/08/22 15:59:29	end	web-browsing	allow	Allow-Inside-DMZ	2ef2cd...	1435		any				
	2022/08/22 15:59:20	data	web-browsing	reset-server	Allow-Inside-DMZ	2ef2cd...		high	any				SSN

Close

11. Use the scroll bar on the right to review the *Details* section.



The interface shows a 'Detailed Log View' window. A table at the bottom displays log entries. The second entry is highlighted in blue. To the right of the table, a 'Details' pane is open, showing information for the selected entry. A yellow box highlights the 'Details' section, and a red box highlights the scroll bar on the right side of the window.

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2022/08/22 15:59:29	end	web-browsing	allow	Allow-Inside-DMZ	2ef2cd...	1435		any				
	2022/08/22 15:59:20	data	web-browsing	reset-server	Allow-Inside-DMZ	2ef2cd...		high	any				SSN

Details

- Content Type: data
- Threat ID/Name: SSN
- ID: 60000 (View in Threat Vault)
- Severity: high
- Repeat Count: 1
- File Name: SSN
- File URL
- File Digest
- Dynamic User

DeviceID

- Source Device Category
- Source Device Profile
- Source Device Model
- Source Device Vendor

Close

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