PAN9 CYBERSECURITY GATEWAY

Lab 8: Protecting Sensitive Data

Document Version: 2020-01-24

Contents

Introduction 3
Objective 3
Lab Topology 4
Lab Settings 5
8 Lab: Protecting Sensitive Data 6
8.0 Load Lab Configuration 6
8.1 Create a New Data Pattern 10
8.2 Create a Data Filtering Security Profile 12
8.3 Apply the Data Filtering Profile to the Security Policy 13
8.4 Create a Text File with Fake Social Security Numbers 15
8.5 Monitor Sensitive Data in the Palo Alto Networks Firewall 17

Introduction

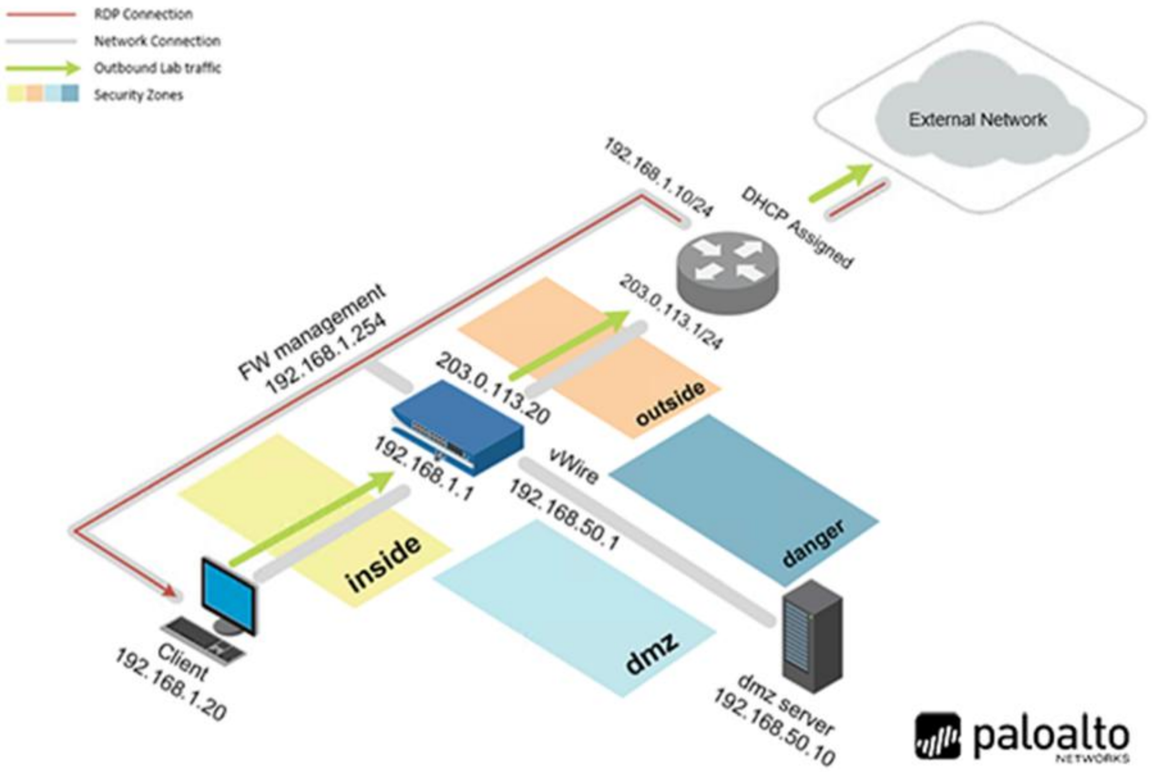
In this lab, you will set up a Data Filtering Profile to protect sensitive and confidential information, such as Social Security numbers.

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.

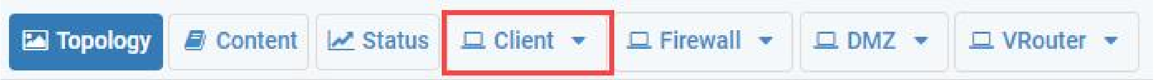
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

8 Lab: Protecting Sensitive Data

8.0 Load Lab Configuration

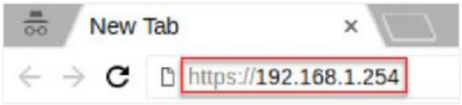
In this section, you will load the Firewall configuration file.

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

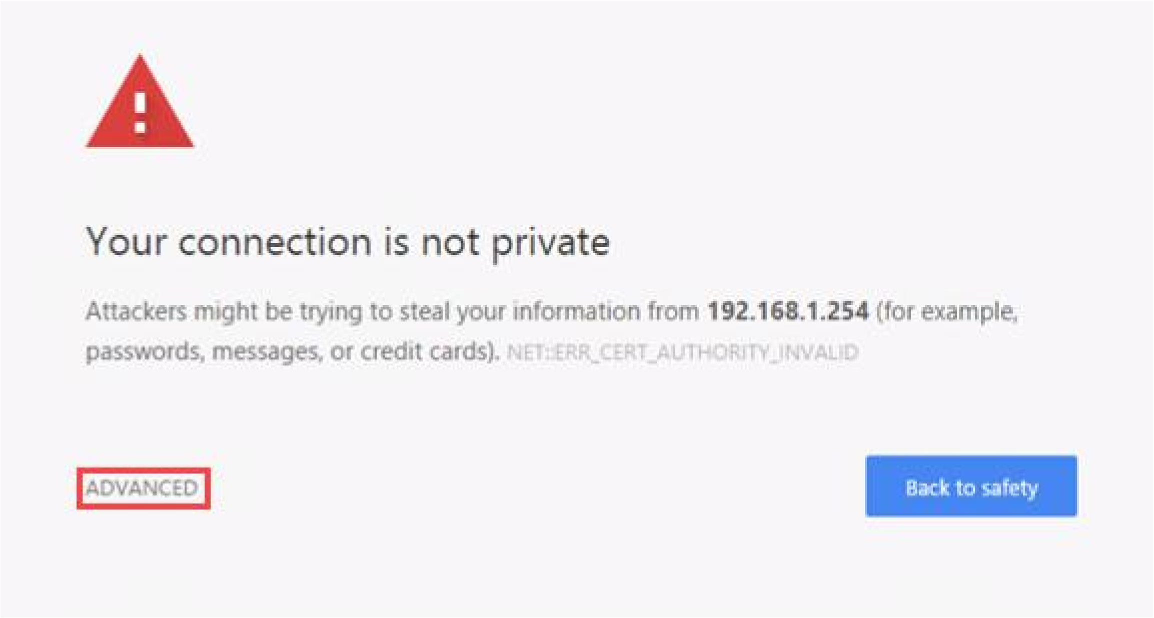


2. Log in to the Client PC as username `lab-user`, password `Train1ng$`.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.

4. In the *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.

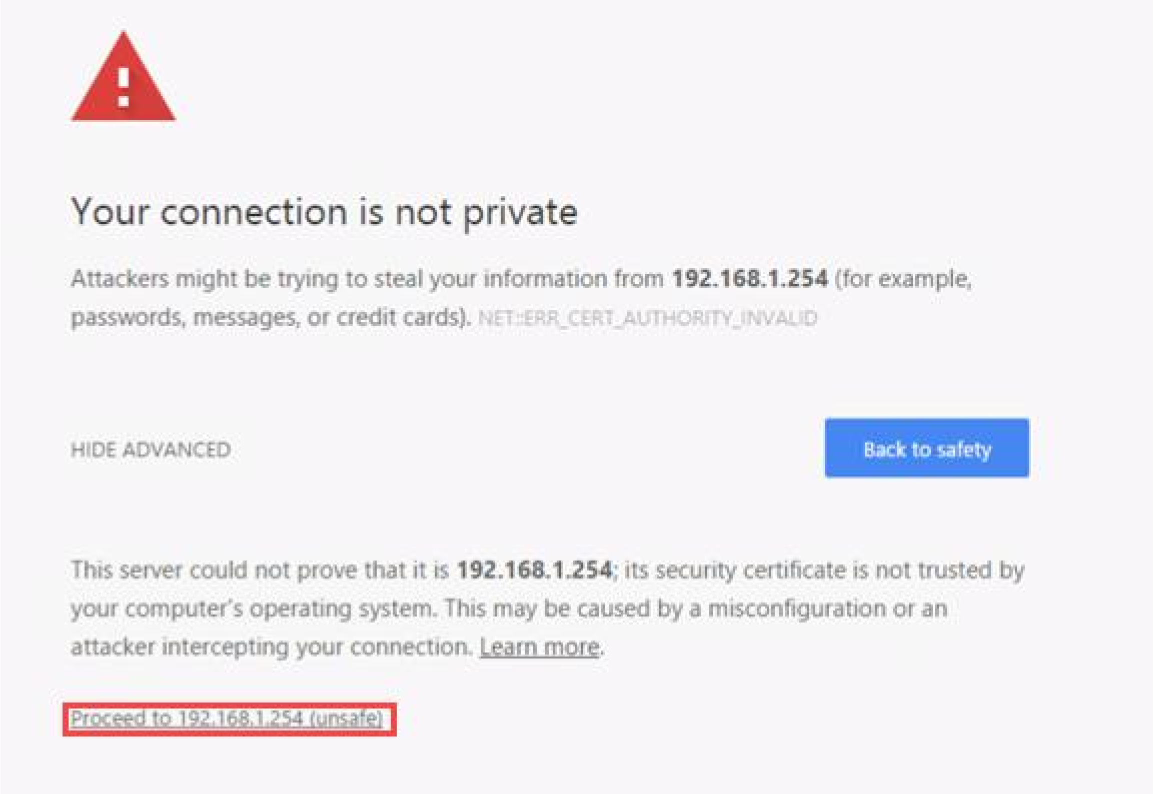


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.



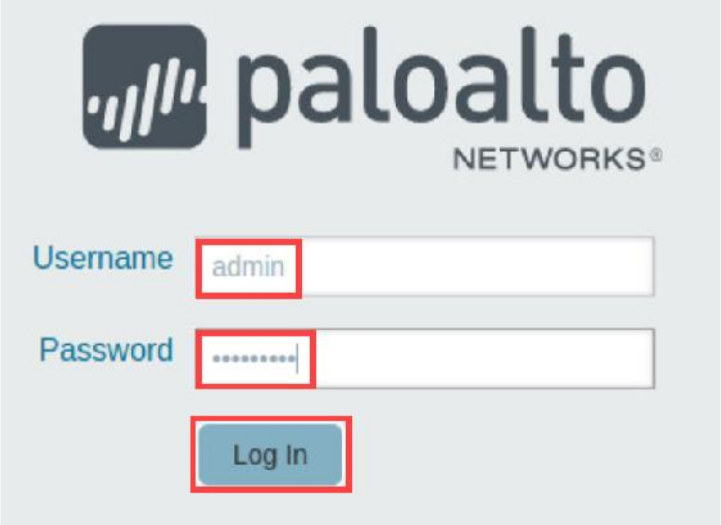
Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to 192.168.1.254 (unsafe)

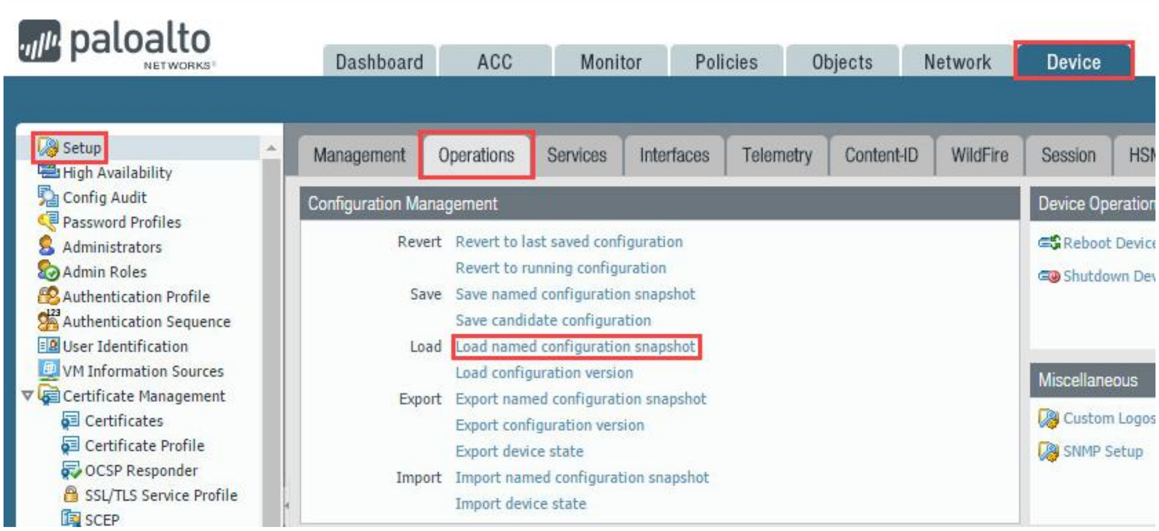
7. Log in to the Firewall web interface as username `admin`, password `Train1ng$`.



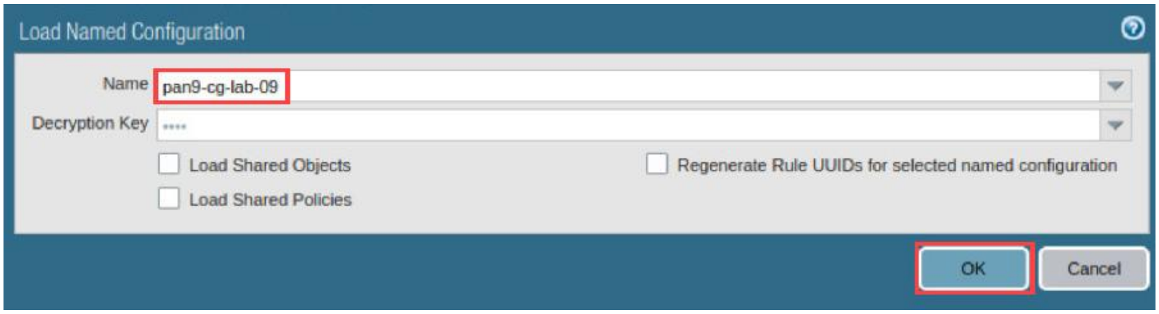
Username admin

Password ••••••••••

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-08** from the *Name* drop-down box and click **OK**.


Load Named Configuration

Name: pan9-cg-lab-09

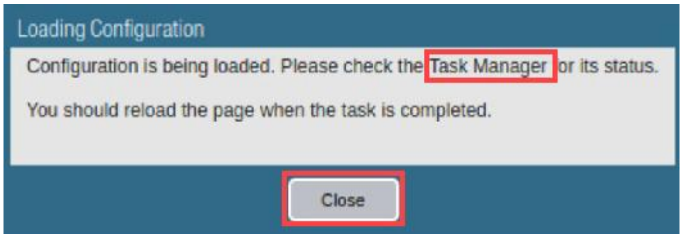
Decryption Key: ••••

□ Load Shared Objects

□ Regenerate Rule UUIDs for selected named configuration

□ Load Shared Policies

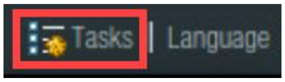
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

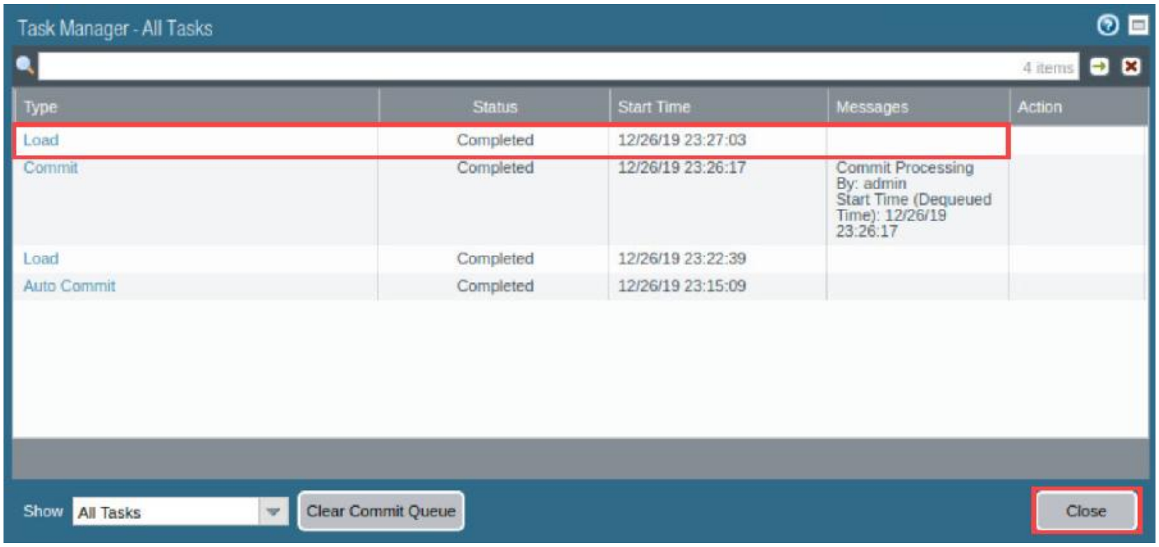
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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

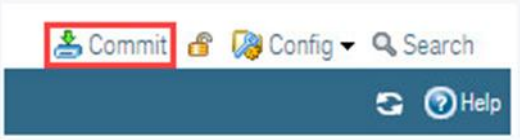


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**

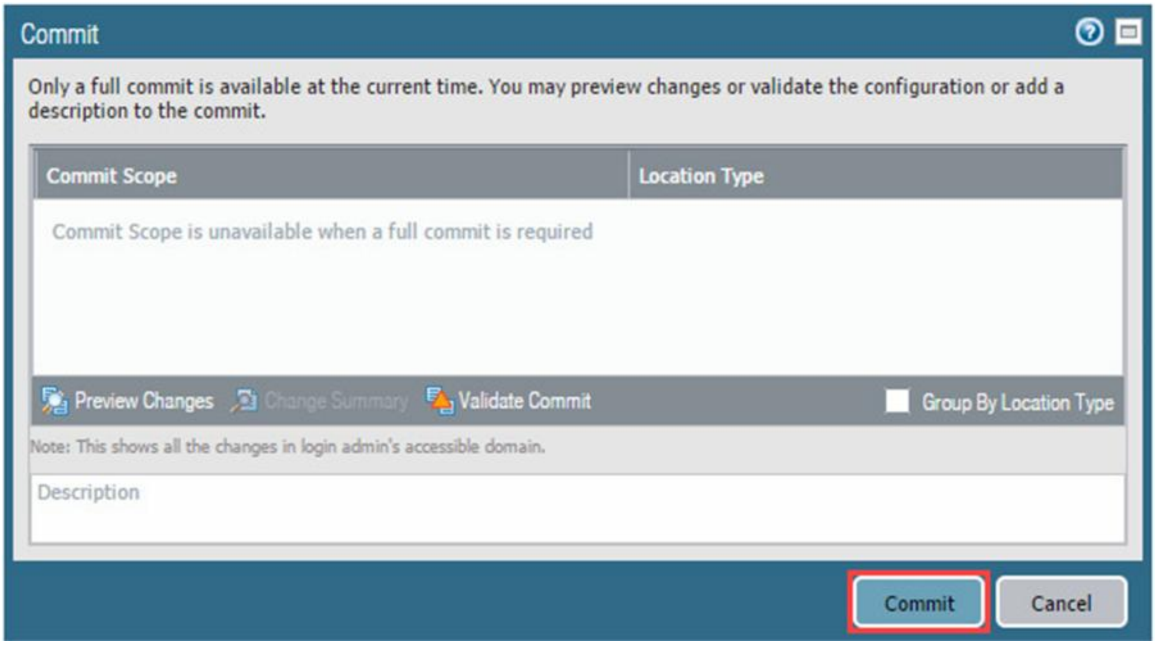


Type	Status	Start Time	Messages	Action
Load	Completed	12/26/19 23:27:03		
Commit	Completed	12/26/19 23:26:17	Commit Processing By: admin Start Time (Dequeued Time): 12/26/19 23:26:17	
Load	Completed	12/26/19 23:22:39		
Auto Commit	Completed	12/26/19 23:15:09		

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.

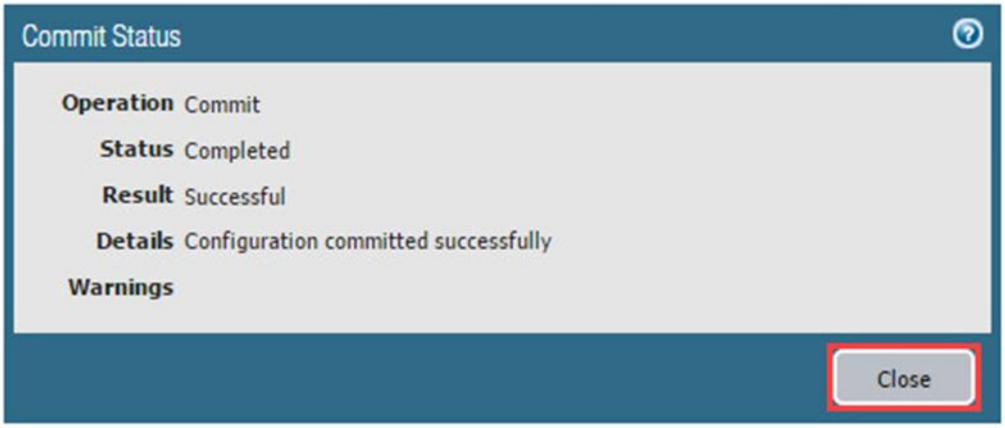


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope is unavailable when a full commit is required

Note: This shows all the changes in login admin's accessible domain.

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



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

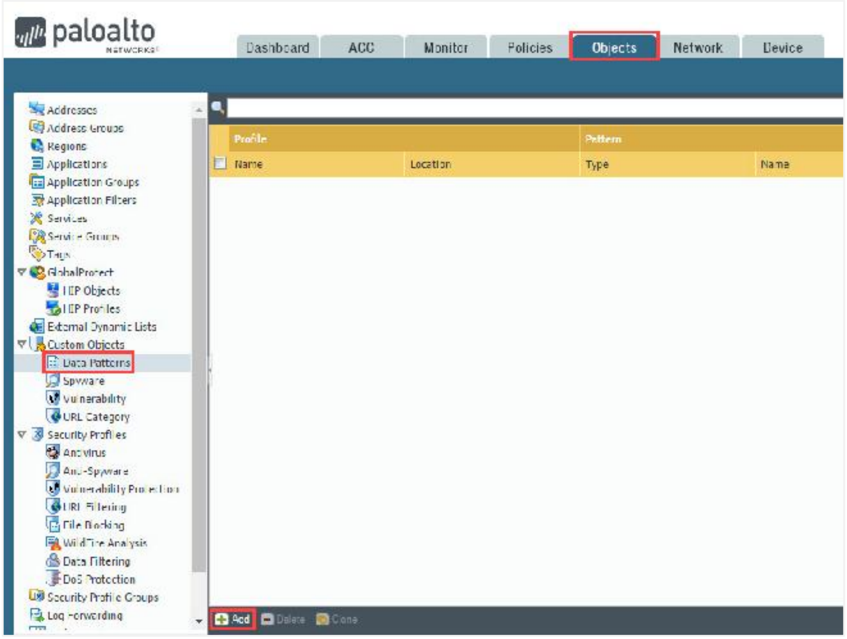
Warnings

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.

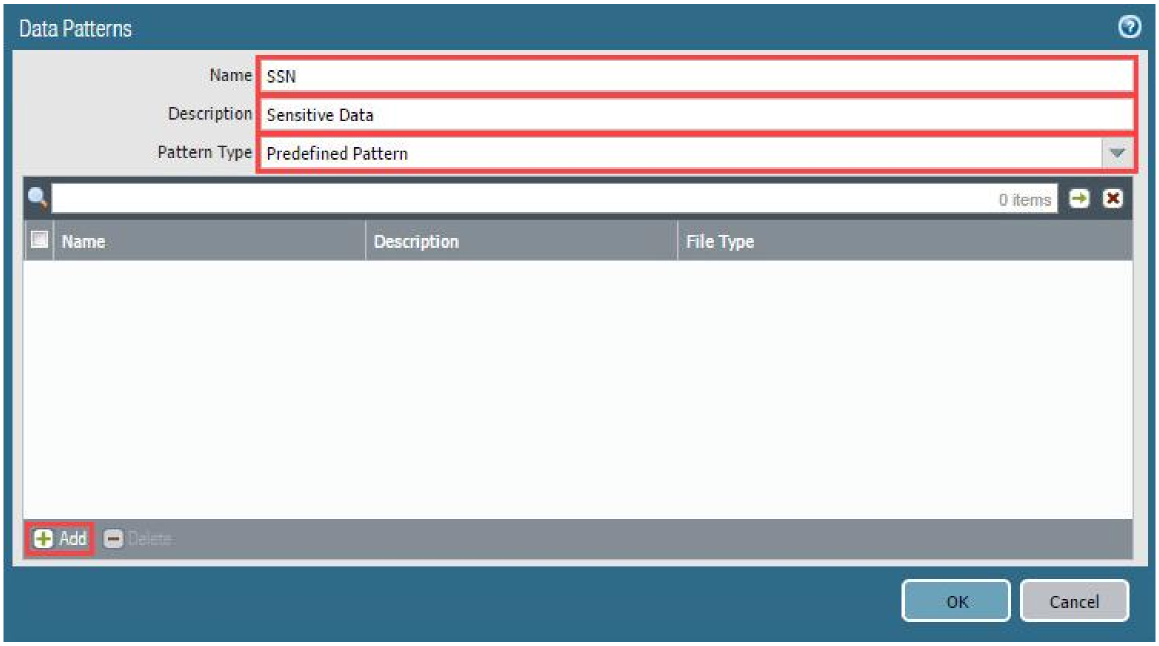
8.1 Create a New Data Pattern

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**.



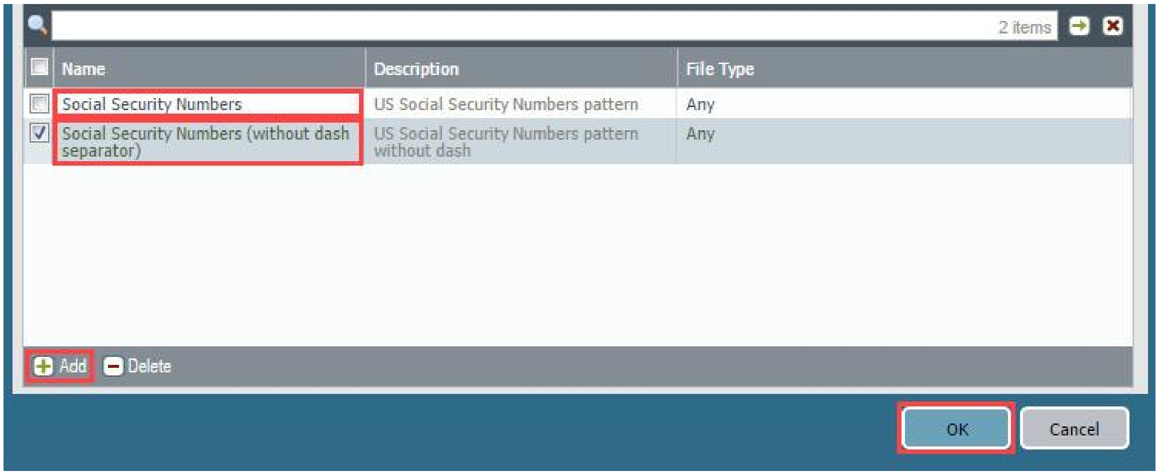
2. In the *Data Patterns* window, type `SSN` in the *Name* field. Then, type `Sensitive Data` in the *Description* field. Next, select **Predefined Pattern** for the *Pattern Type*. Finally, click **Add**.



Name: SSN
Description: Sensitive Data
Pattern Type: Predefined Pattern

□	Name	Description	File Type

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**.

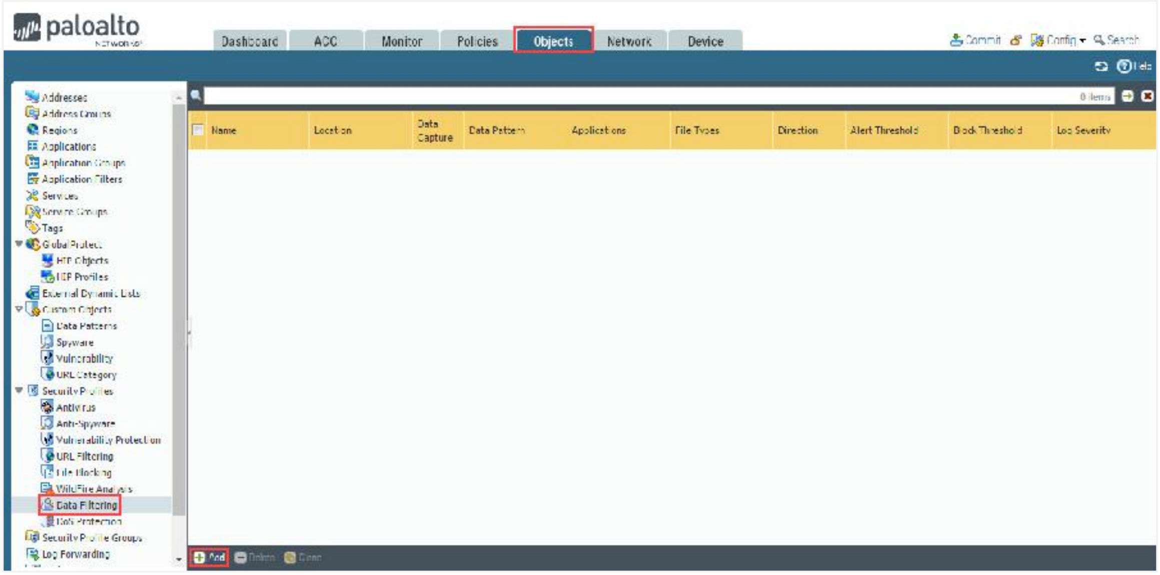


□	Name	Description	File Type
□	Social Security Numbers	US Social Security Numbers pattern	Any
☑	Social Security Numbers (without dash separator)	US Social Security Numbers pattern without dash	Any

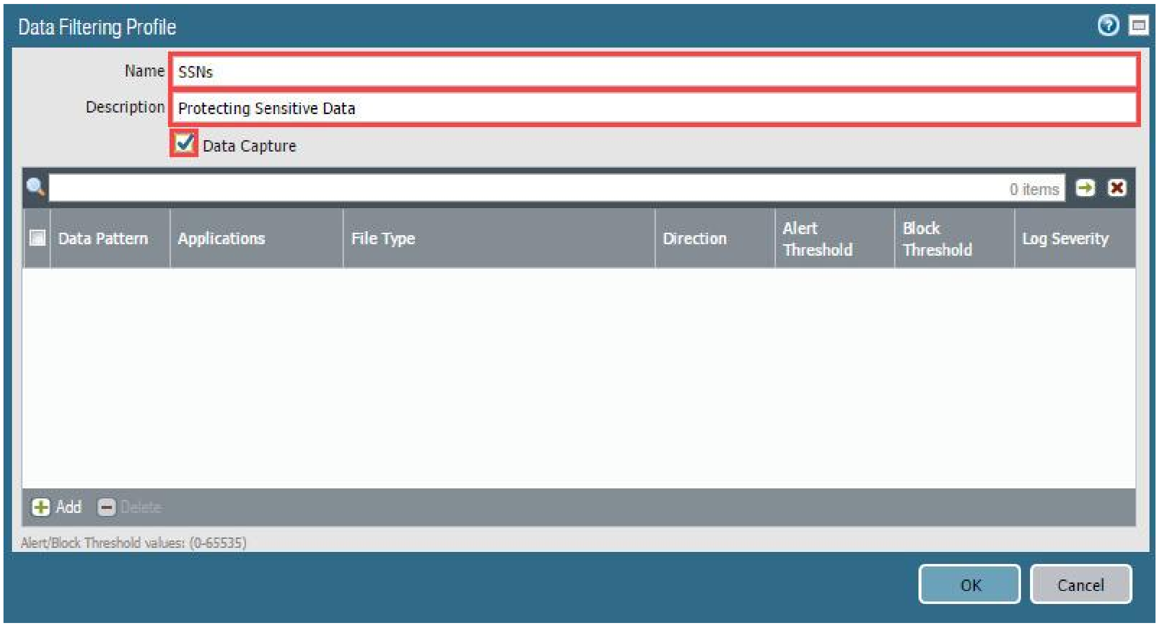
8.2 Create a Data Filtering Security Profile

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**.

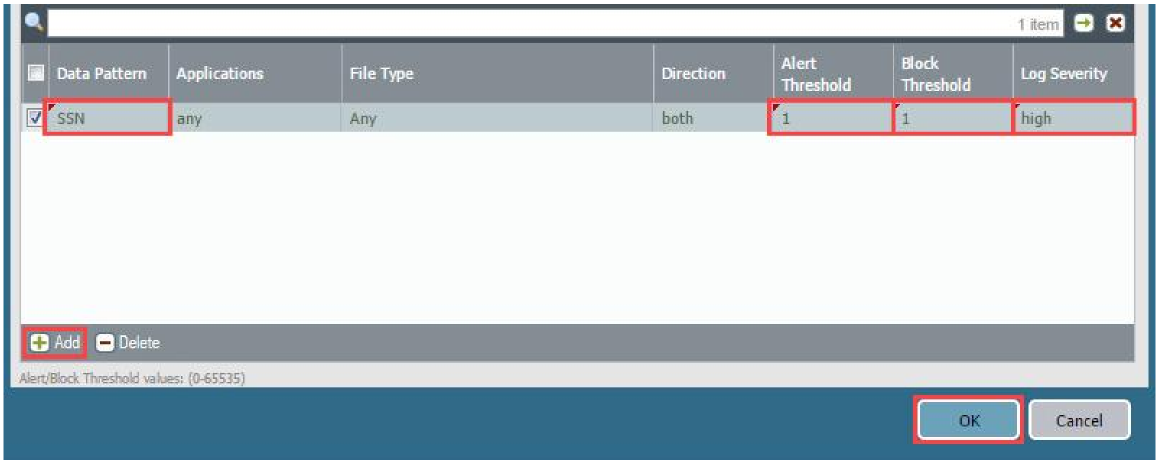

Data Filtering Profile

Name: SSNs

Description: Protecting Sensitive Data

☑ Data Capture

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**.



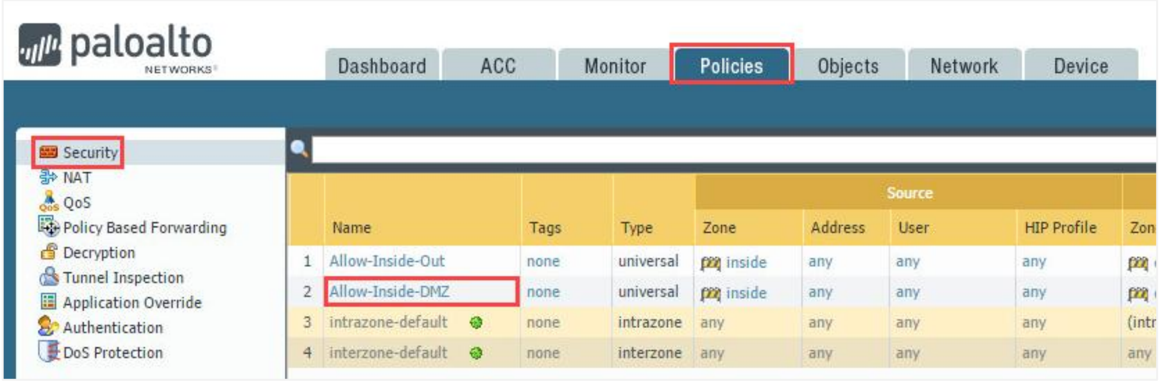
□	Data Pattern	Applications	File Type	Direction	Alert Threshold	Block Threshold	Log Severity
☑	SSN	any	Any	both	1	1	high

Alert/Block Threshold values: (0-65535)

8.3 Apply the Data Filtering Profile to the Security Policy

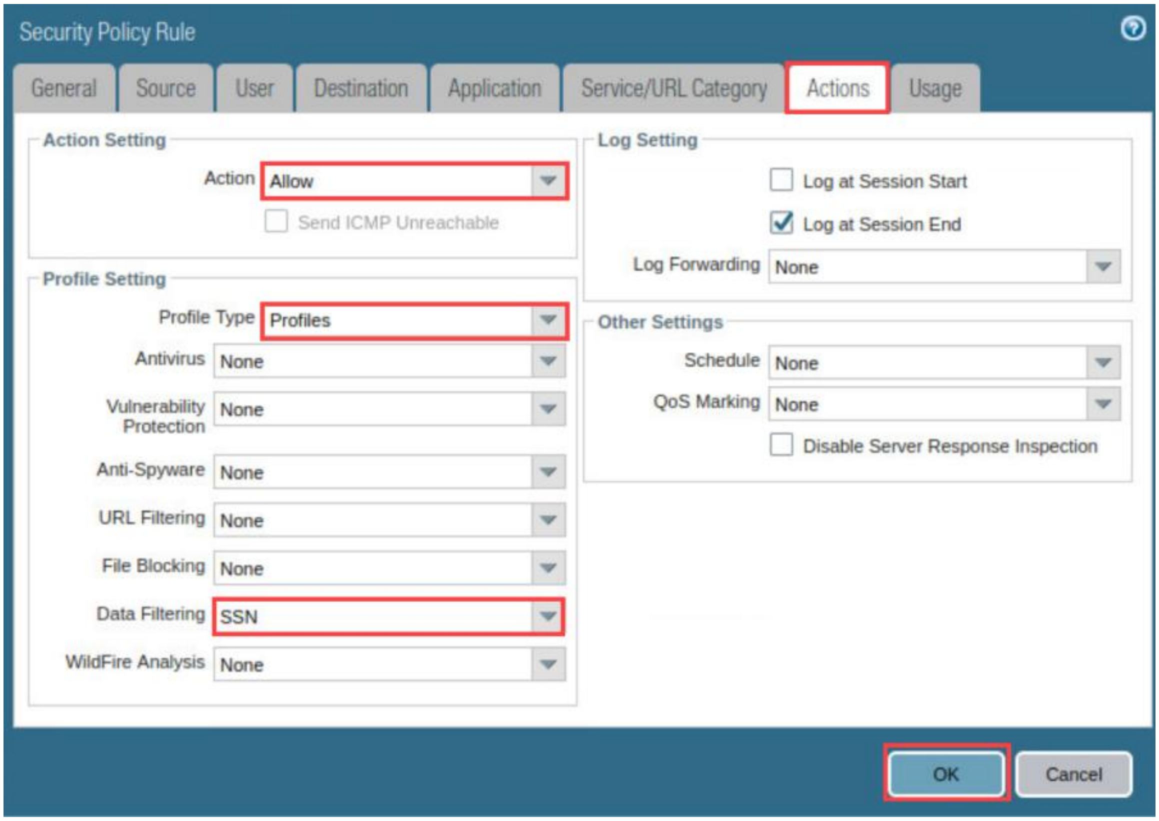
In this section, you will apply the Data Filtering Security Profile you created to the **Allow-Inside-DMZ** Security Policy.

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



				Source				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zon
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	(intr
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 **SSNs** in the *Data Filtering* dropdown and click **OK**.



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: SSN

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

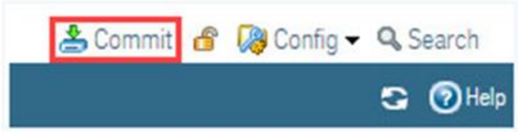
Other Settings

Schedule: None

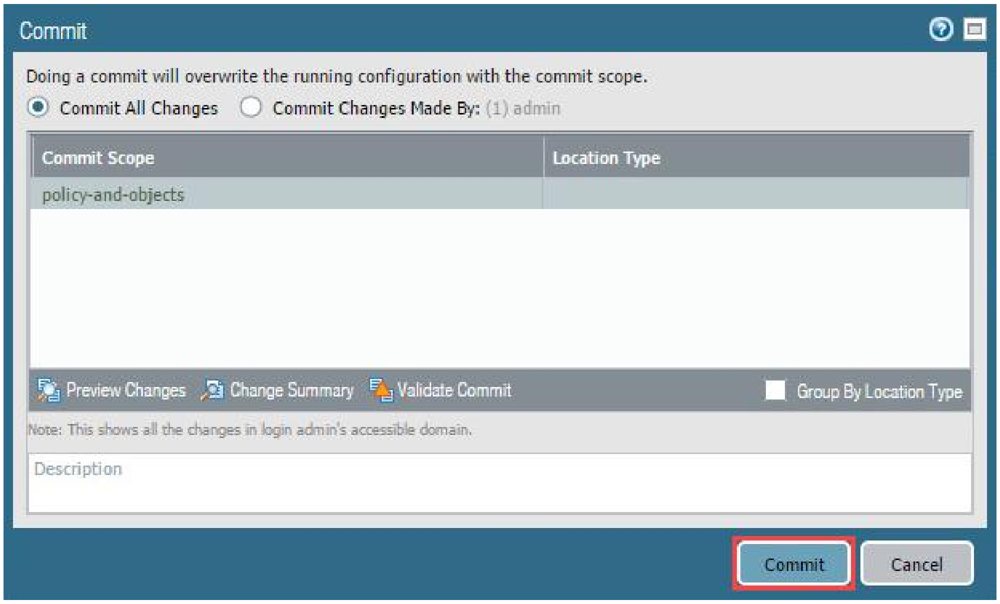
QoS Marking: None

□ Disable Server Response Inspection

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.



Commit

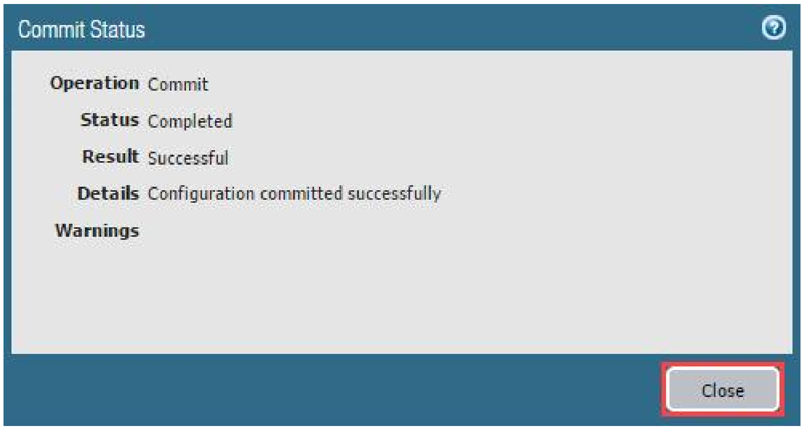
Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By: (1) admin

Commit Scope	Location Type
policy-and-objects	

Note: This shows all the changes in login admin's accessible domain.

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



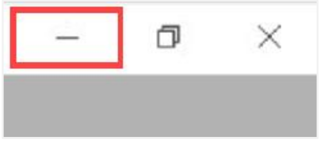
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

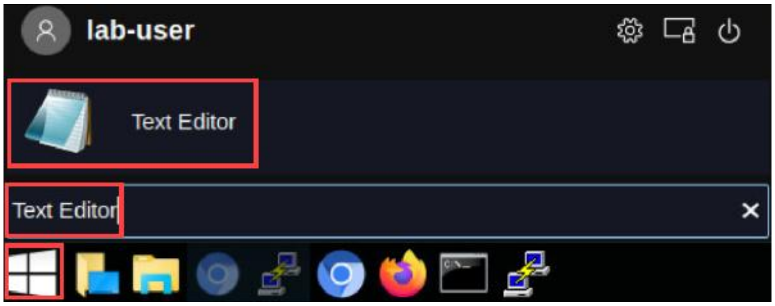
8.4 Create a Text File with Fake Social Security Numbers

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.

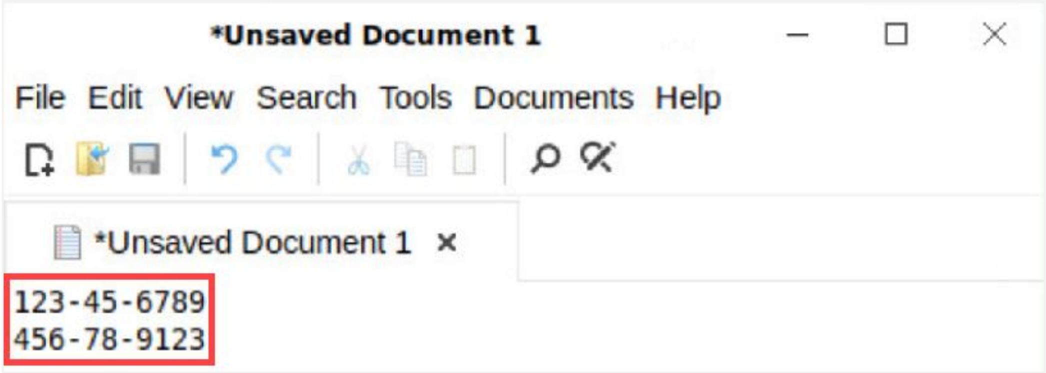
1. Minimize *Chromium* in the upper-right.



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

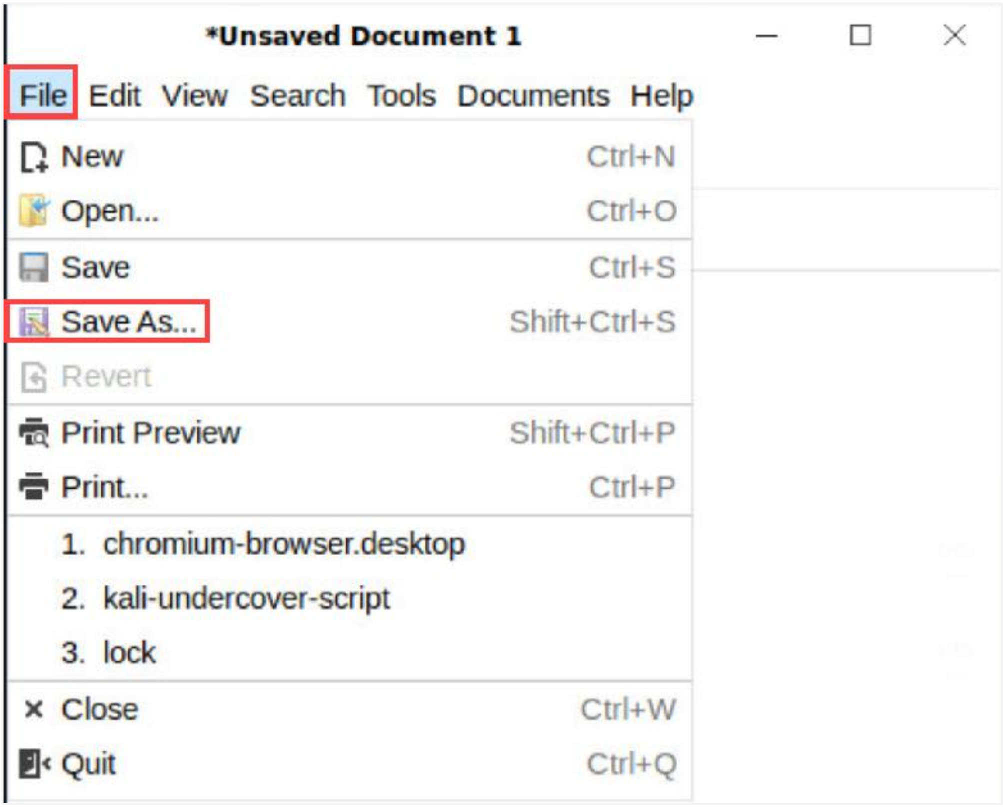


3. In the *Unsaved Document 1 – Text Editor* window, type `123-45-6789` and `456-78-9123`. These will be the fake Social Security numbers.

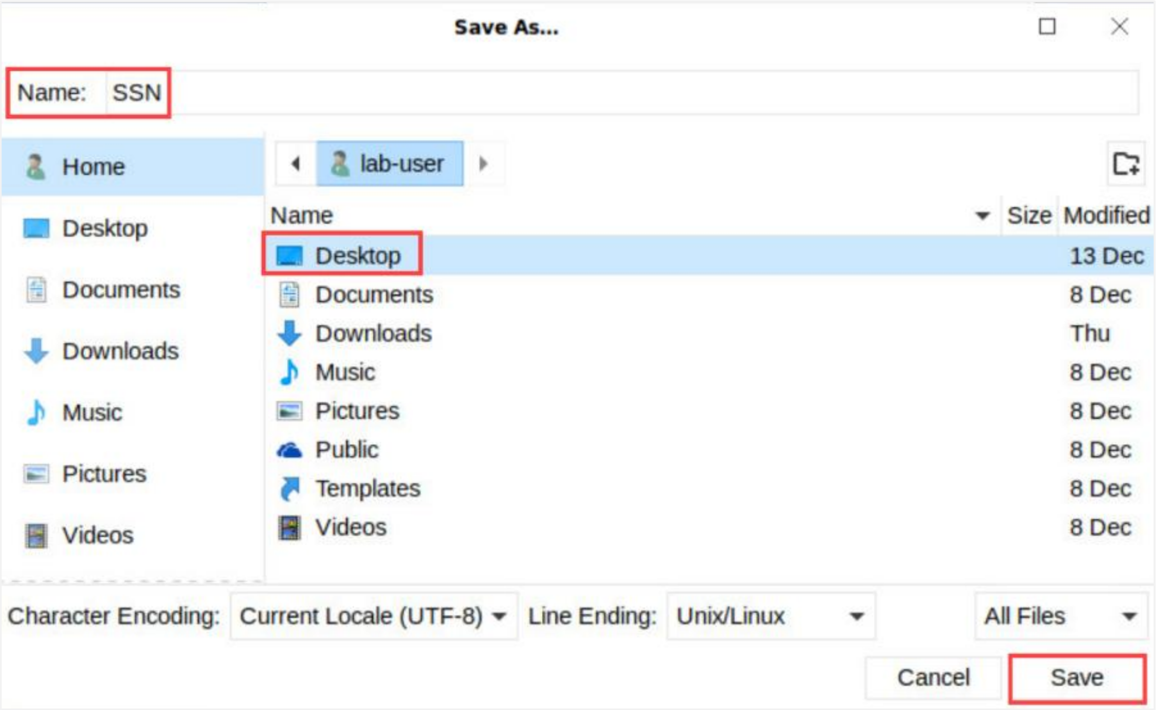


```
123-45-6789
456-78-9123
```

4. Click **File** > **Save As…**.



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



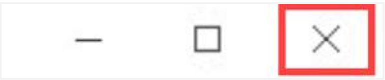
Save As...

Name: SSN

Name	Size	Modified
Desktop		13 Dec
Documents		8 Dec
Downloads		Thu
Music		8 Dec
Pictures		8 Dec
Public		8 Dec
Templates		8 Dec
Videos		8 Dec

Character Encoding: Current Locale (UTF-8)
Line Ending: Unix/Linux
All Files

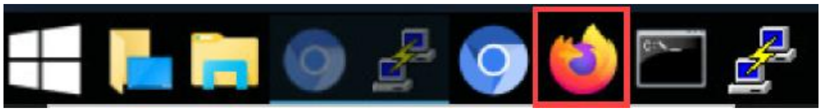
6. Click the **X** in the upper-right to close Text Editor.



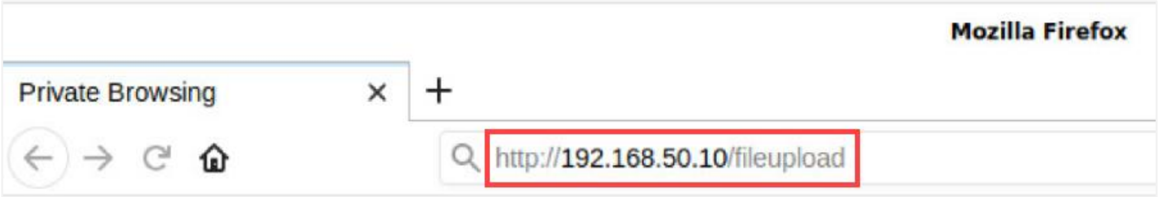
8.5 Monitor Sensitive Data in the Palo Alto Networks Firewall

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*.

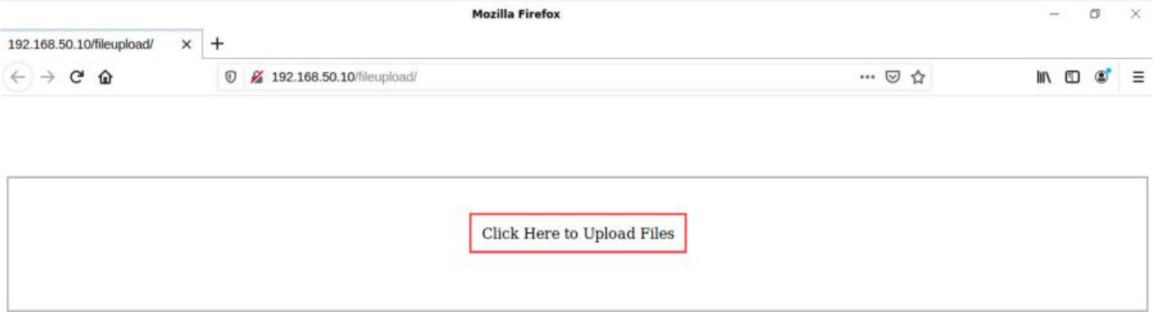
1. Navigate and click on the **Firefox** browser in the Taskbar.



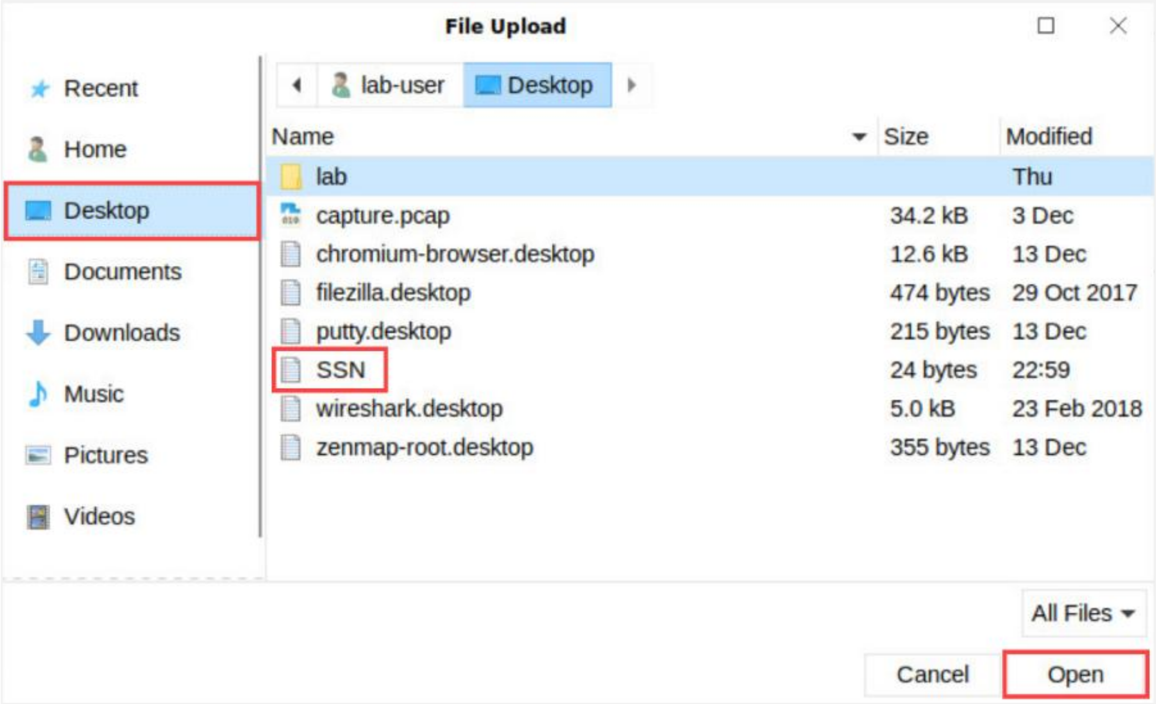
2. In the *Firefox* address field, type `http://192.168.50.10/fileupload` and press **Enter**.



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

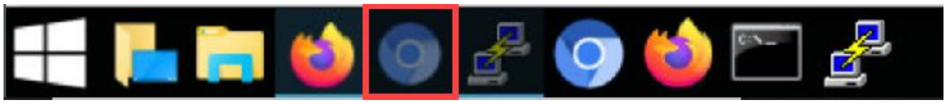

Mozilla Firefox
192.168.50.10/fileupload/
192.168.50.10/fileupload/
Click Here to Upload Files

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

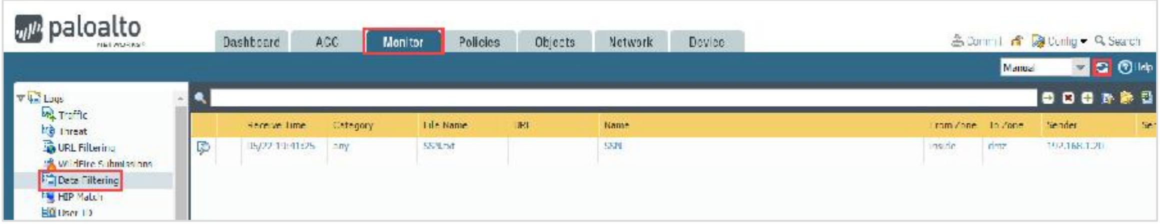


Name	Size	Modified
lab		Thu
capture.pcap	34.2 kB	3 Dec
chromium-browser.desktop	12.6 kB	13 Dec
filezilla.desktop	474 bytes	29 Oct 2017
putty.desktop	215 bytes	13 Dec
SSN	24 bytes	22:59
wireshark.desktop	5.0 kB	23 Feb 2018
zenmap-root.desktop	355 bytes	13 Dec

5. Maximize *Chromium* from the Taskbar.

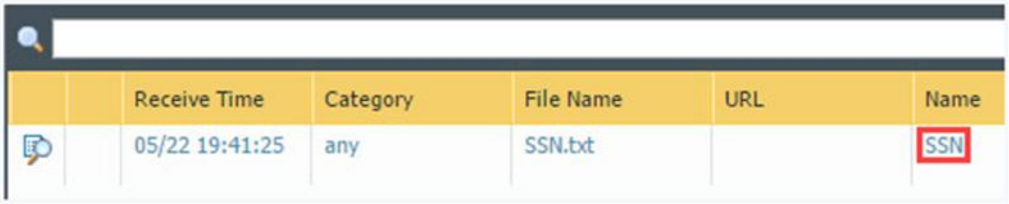


6. Navigate to **Monitor** > **Logs** > **Data Filtering**. You may need to click the **Refresh** button in the upper-right to refresh the logs. You may need to wait a few minutes for the logs to update.



	Receive Time	Category	File Name	URL	Name	From Zone	To Zone	Sender
	05/22 19:41:25	any	SSN.txt		SSN	inside	dmz	192.168.1.20

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

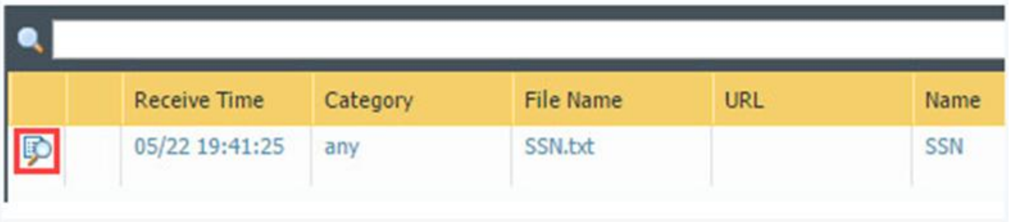


		Receive Time	Category	File Name	URL	Name
		05/22 19:41:25	any	SSN.txt		SSN

STOP

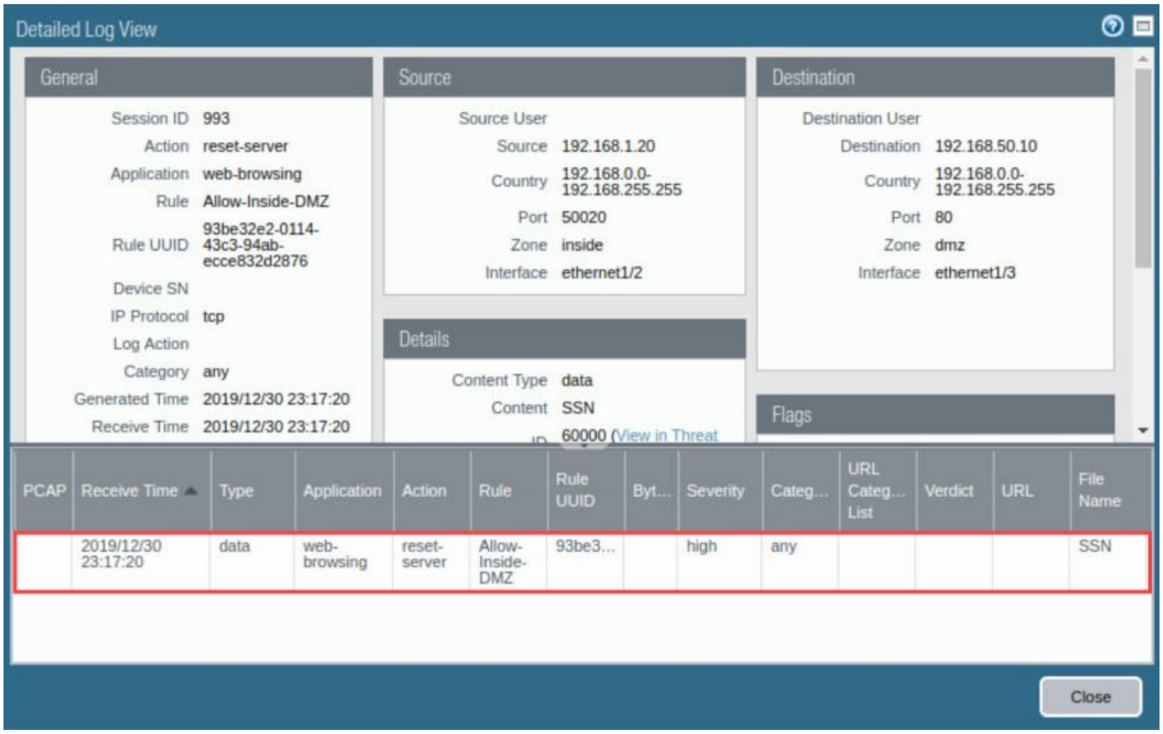
Pause here for 5 minutes to let the logs populate before continuing.

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



		Receive Time	Category	File Name	URL	Name
		05/22 19:41:25	any	SSN.txt		SSN

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



General

Session ID 993
Action reset-server
Application web-browsing
Rule Allow-Inside-DMZ
Rule UUID 93be32e2-0114-43c3-94ab-ecce832d2876
Device SN
IP Protocol tcp
Log Action
Category any
Generated Time 2019/12/30 23:17:20
Receive Time 2019/12/30 23:17:20

Source

Source User
Source 192.168.1.20
Country 192.168.0.0-192.168.255.255
Port 50020
Zone inside
Interface ethernet1/2

Details

Content Type data
Content SSN
ID 60000 (View in Threat

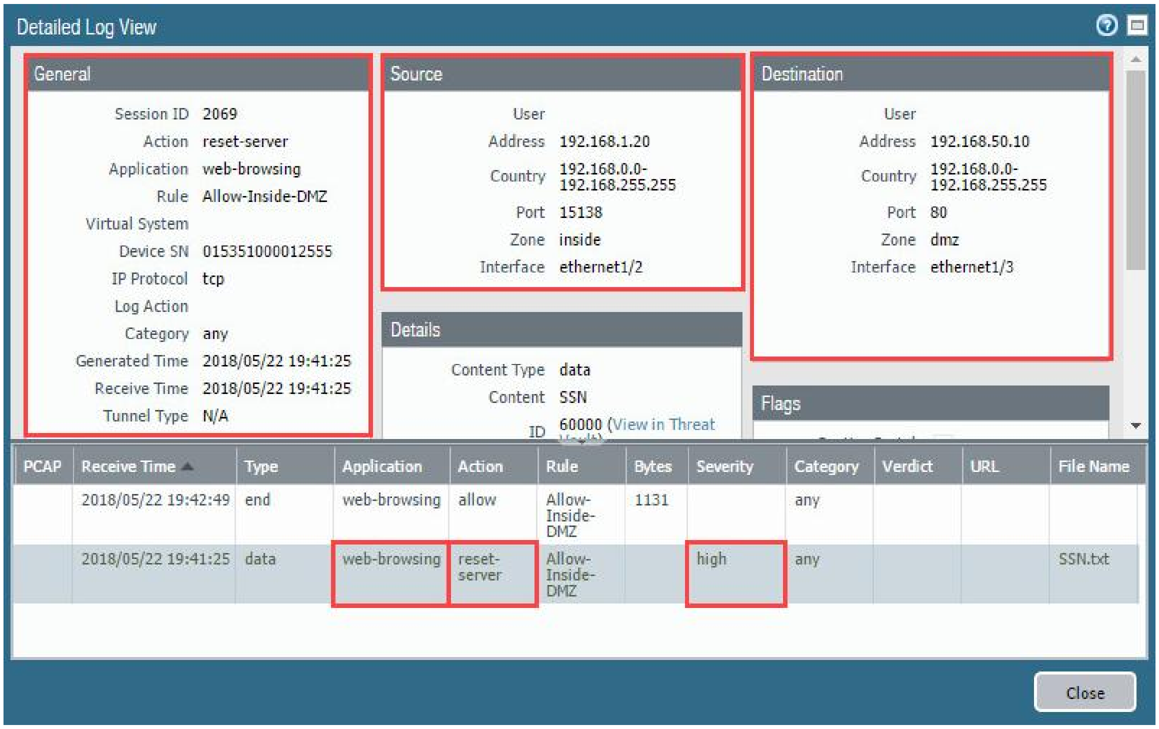
Destination

Destination User
Destination 192.168.50.10
Country 192.168.0.0-192.168.255.255
Port 80
Zone dmz
Interface ethernet1/3

Flags

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/12/30 23:17:20	data	web-browsing	reset-server	Allow-Inside-DMZ	93be3...		high	any				SSN

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 *Designation* section will identify where the file was designated.



General

Session ID 2069
Action reset-server
Application web-browsing
Rule Allow-Inside-DMZ
Virtual System
Device SN 015351000012555
IP Protocol tcp
Log Action
Category any
Generated Time 2018/05/22 19:41:25
Receive Time 2018/05/22 19:41:25
Tunnel Type N/A

Source

User
Address 192.168.1.20
Country 192.168.0.0-192.168.255.255
Port 15138
Zone inside
Interface ethernet1/2

Details

Content Type data
Content SSN
ID 60000 (View in Threat

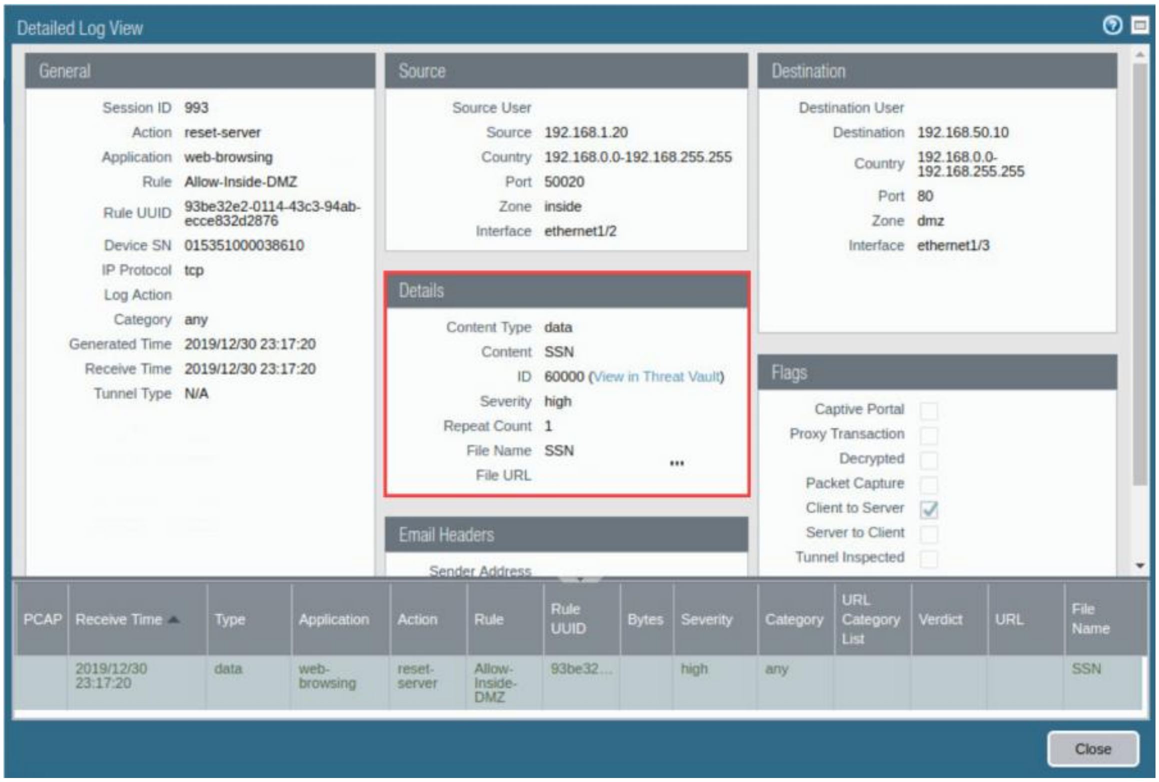
Destination

User
Address 192.168.50.10
Country 192.168.0.0-192.168.255.255
Port 80
Zone dmz
Interface ethernet1/3

Flags

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
	2018/05/22 19:42:49	end	web-browsing	allow	Allow-Inside-DMZ	1131		any			
	2018/05/22 19:41:25	data	web-browsing	reset-server	Allow-Inside-DMZ		high	any			SSN.txt

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



General

Session ID	993
Action	reset-server
Application	web-browsing
Rule	Allow-Inside-DMZ
Rule UUID	93be32e2-0114-43c3-94ab-ecce832d2876
Device SN	015351000038610
IP Protocol	tcp
Log Action	
Category	any
Generated Time	2019/12/30 23:17:20
Receive Time	2019/12/30 23:17:20
Tunnel Type	N/A

Source

Source User	
Source	192.168.1.20
Country	192.168.0.0-192.168.255.255
Port	50020
Zone	inside
Interface	ethernet1/2

Destination

Destination User	
Destination	192.168.50.10
Country	192.168.0.0-192.168.255.255
Port	80
Zone	dmz
Interface	ethernet1/3

Details

Content Type	data
Content	SSN
ID	60000 (View in Threat Vault)
Severity	high
Repeat Count	1
File Name	SSN
File URL	

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Client to Server	☑
Server to Client	□
Tunnel Inspected	□

Email Headers

Sender Address

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Bytes	Severity	Category	URL Category List	Verdict	URL	File Name
	2019/12/30 23:17:20	data	web-browsing	reset-server	Allow-Inside-DMZ	93be32…		high	any				SSN

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