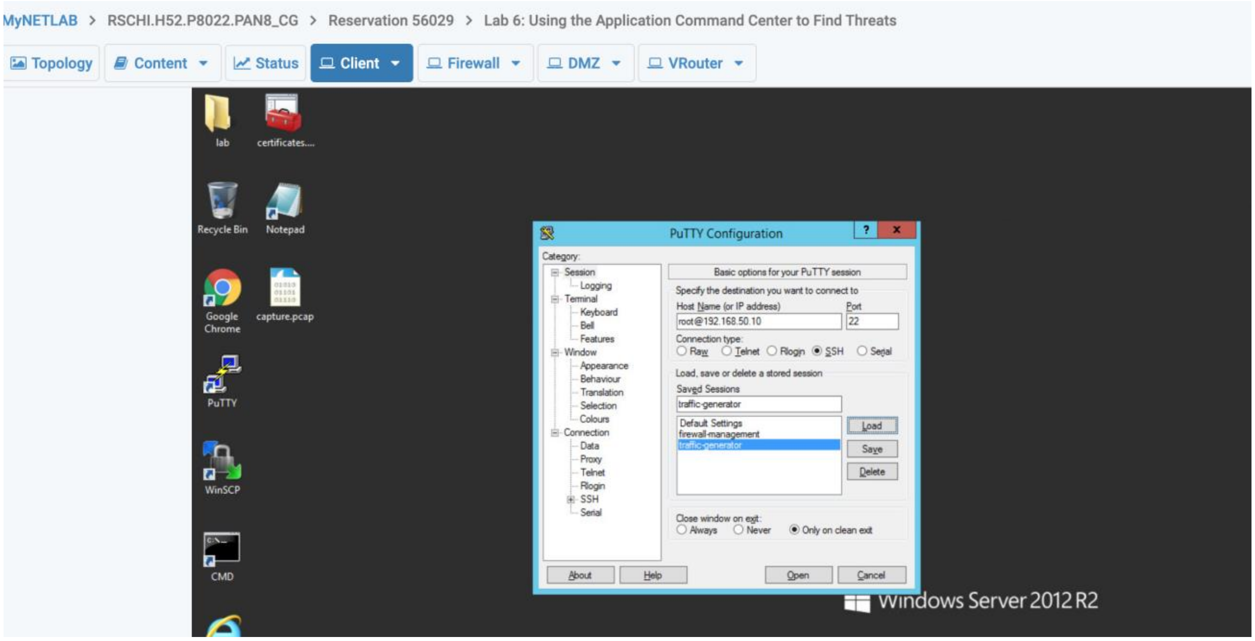
<u>Anjali Jain -Gateway II</u>

Lab 6: Using the Application Command Center to Find Threats

In this lab, I have performed the following tasks:

- Generate Malware Traffic to the Firewall
- Find Malware Threat in the Application Command Center

A) Loading of the malware script from putty



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): root@192.168.50.10   Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: traffic-generator

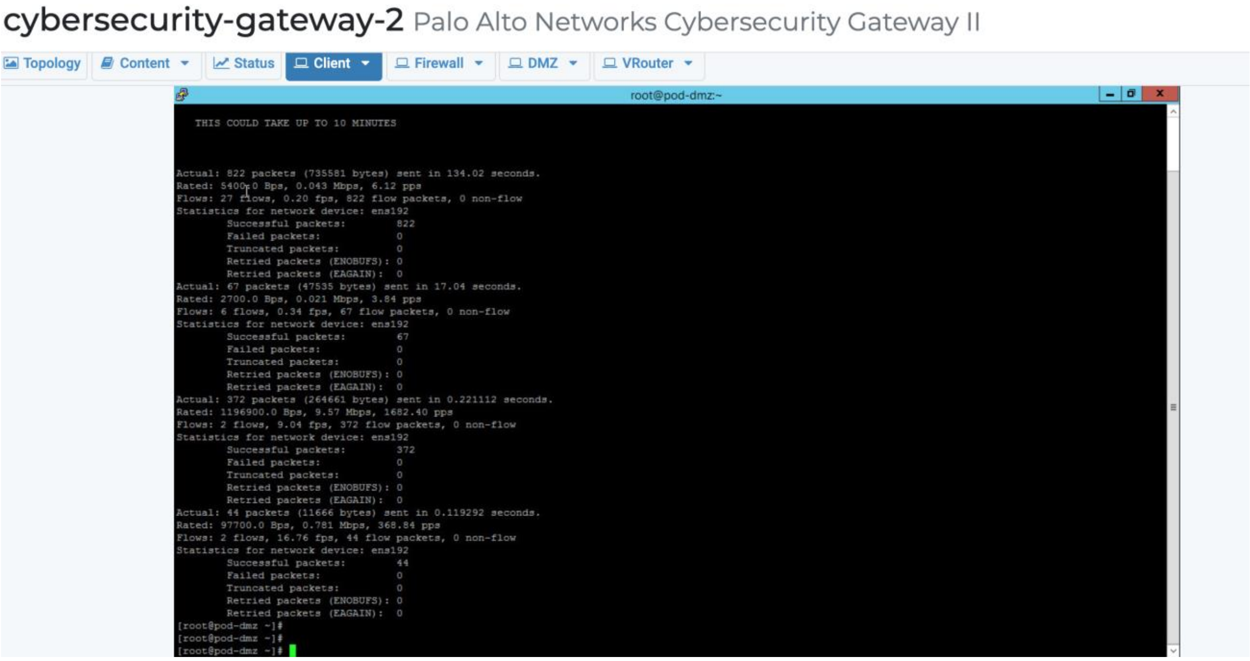
Default Settings
firewall-management
traffic-generator

Close window on exit: ○ Always ○ Never ● Only on clean exit

B) Threat in the Application Command Center

In this section, we will review Threat Activity and Blocked Activity in the Application

Threats generated after running the threat generator file.


cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II
Topology
Content
Status
Client
Firewall
DMZ
VRouter
root@pod-dmz:~

```
  THIS COULD TAKE UP TO 10 MINUTES


Actual: 822 packets (735581 bytes) sent in 134.02 seconds.
Rated: 5400.0 Bps, 0.043 Mbps, 6.12 pps
Flows: 27 flows, 0.20 fps, 822 flow packets, 0 non-flow
Statistics for network device: ens192
        Successful packets:        822
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 67 packets (47535 bytes) sent in 17.04 seconds.
Rated: 2700.0 Bps, 0.021 Mbps, 3.84 pps
Flows: 6 flows, 0.34 fps, 67 flow packets, 0 non-flow
Statistics for network device: ens192
        Successful packets:        67
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 372 packets (264661 bytes) sent in 0.221112 seconds.
Rated: 1196900.0 Bps, 9.57 Mbps, 1682.40 pps
Flows: 2 flows, 9.04 fps, 372 flow packets, 0 non-flow
Statistics for network device: ens192
        Successful packets:        372
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
Actual: 44 packets (11666 bytes) sent in 0.119292 seconds.
Rated: 97700.0 Bps, 0.781 Mbps, 368.84 pps
Flows: 2 flows, 16.76 fps, 44 flow packets, 0 non-flow
Statistics for network device: ens192
        Successful packets:        44
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
[root@pod-dmz ~]#
[root@pod-dmz ~]#
[root@pod-dmz ~]#
```

In this lab, I have generated malware traffic and used the Application Command Center to find the threat.

==

Lab 7. Analyzing Firewall Logs

In this lab, I have performed the following tasks:

• Generate Traffic to the Firewall

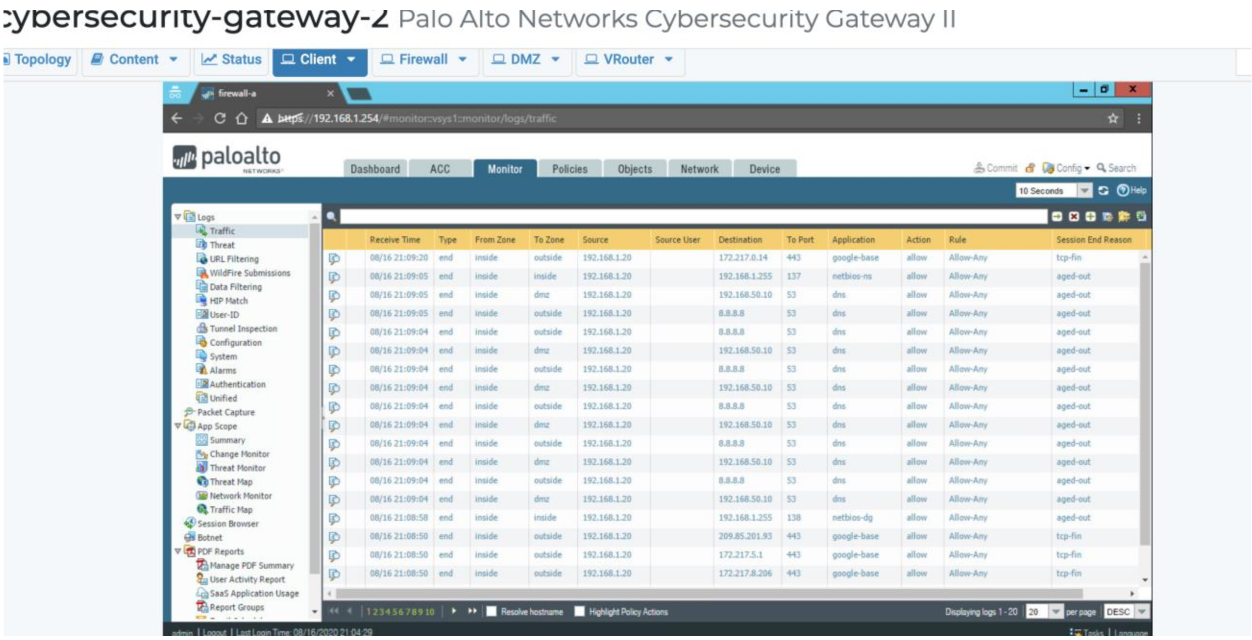
• Review Traffic in the Firewall Logs

Steps A)

The script has generated test malware traffic to the Firewall so that I can see malware traffic in the Firewall

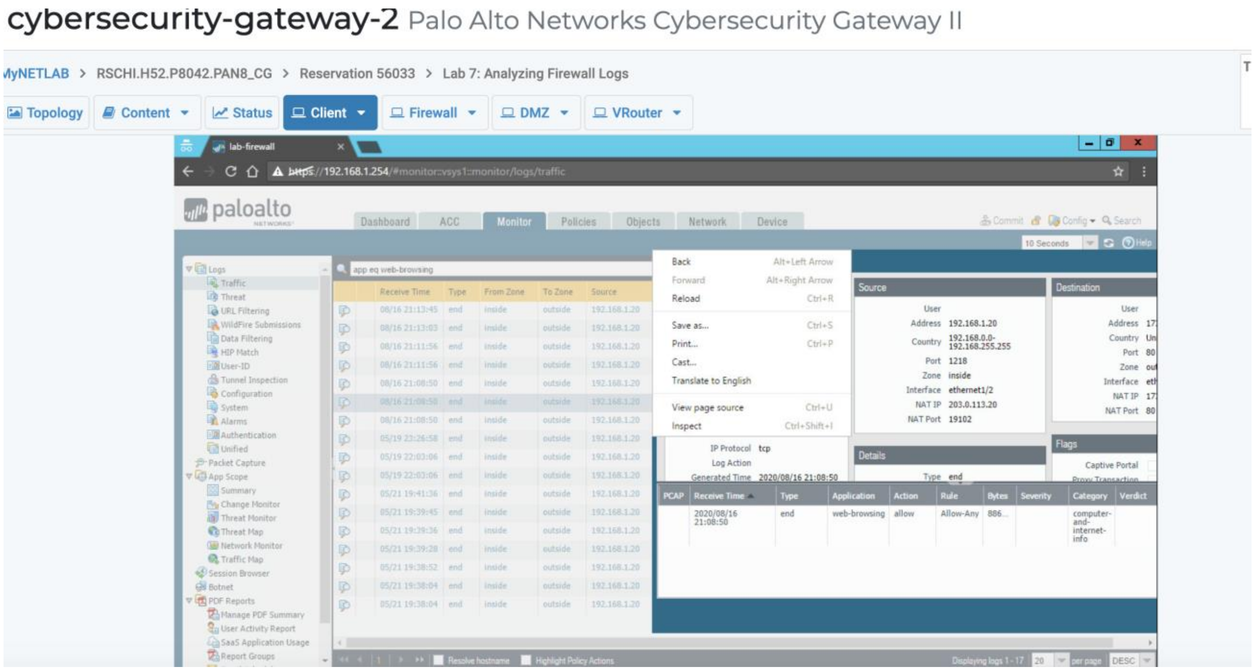
B)

Traffic monitor on the firewall in logs--> Traffic --> monitor



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason
08/16 21:09:20	end	inside	outside	192.168.1.20		172.217.0.14	443	google-base	allow	Allow-Any	tcp-fin
08/16 21:09:05	end	inside	inside	192.168.1.20		192.168.1.255	137	netbios-ns	allow	Allow-Any	aged-out
08/16 21:09:05	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:09:05	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	outside	192.168.1.20		8.8.8.8	53	dns	allow	Allow-Any	aged-out
08/16 21:09:04	end	inside	dmz	192.168.1.20		192.168.50.10	53	dns	allow	Allow-Any	aged-out
08/16 21:08:58	end	inside	inside	192.168.1.20		192.168.1.255	138	netbios-dg	allow	Allow-Any	aged-out
08/16 21:08:50	end	inside	outside	192.168.1.20		209.85.201.93	443	google-base	allow	Allow-Any	tcp-fin
08/16 21:08:50	end	inside	outside	192.168.1.20		172.217.5.1	443	google-base	allow	Allow-Any	tcp-fin
08/16 21:08:50	end	inside	outside	192.168.1.20		172.217.8.206	443	google-base	allow	Allow-Any	tcp-fin

C) Firewall logs filtered on web-browsing and detailed view of the logs also are captured



app eq web-browsing

Receive Time	Type	From Zone	To Zone	Source
08/16 21:13:45	end	inside	outside	192.168.1.20
08/16 21:13:03	end	inside	outside	192.168.1.20
08/16 21:11:56	end	inside	outside	192.168.1.20
08/16 21:11:56	end	inside	outside	192.168.1.20
08/16 21:08:50	end	inside	outside	192.168.1.20
08/16 21:08:50	end	inside	outside	192.168.1.20
08/16 21:08:50	end	inside	outside	192.168.1.20
05/19 22:26:58	end	inside	outside	192.168.1.20
05/19 22:03:06	end	inside	outside	192.168.1.20
05/19 22:03:06	end	inside	outside	192.168.1.20
05/21 19:41:36	end	inside	outside	192.168.1.20
05/21 19:39:45	end	inside	outside	192.168.1.20
05/21 19:39:36	end	inside	outside	192.168.1.20
05/21 19:39:28	end	inside	outside	192.168.1.20
05/21 19:38:52	end	inside	outside	192.168.1.20
05/21 19:38:04	end	inside	outside	192.168.1.20
05/21 19:38:04	end	inside	outside	192.168.1.20

Source

User	
Address	192.168.1.20
Country	192.168.0.0- 192.168.255.255
Port	1218
Zone	inside
Interface	ethernet1/2
NAT IP	203.0.113.20
NAT Port	19102

Destination

User	
Address	17
Country	Un
Port	80
Zone	out
Interface	eth
NAT IP	17
NAT Port	80

IP Protocol	tcp
Log Action	
Generated Time	2020/08/16 21:08:50

Details

Type end

Flags

Captive Portal ☐
Proxy Transaction ☐

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict
	2020/08/16 21:08:50	end	web-browsing	allow	Allow-Any	886...		computer-and-internet-info	

Lab 8: Protecting Sensitive Data

========================

In this lab,

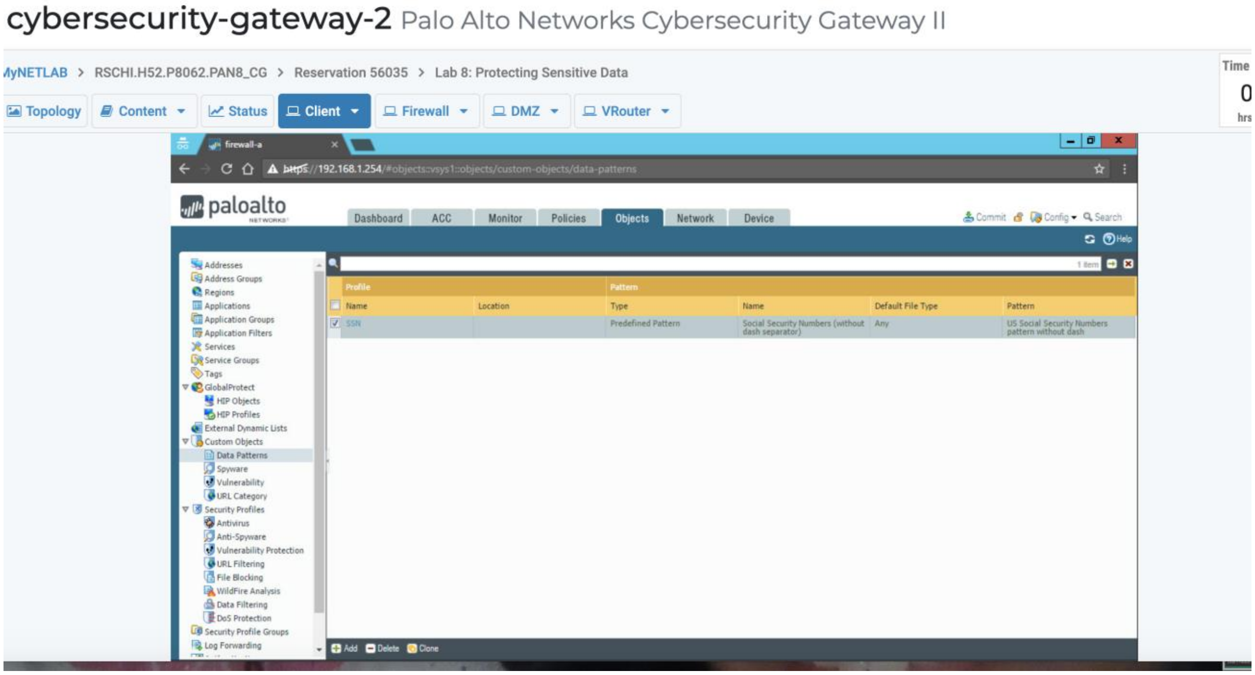
I have set up a Data Filtering Profile to protect sensitive and confidential information, such as Social Security numbers.

Objective In this lab, I have 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

In this section, I have created 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, i have used the predefined patterns.

SSn used as sensitive information



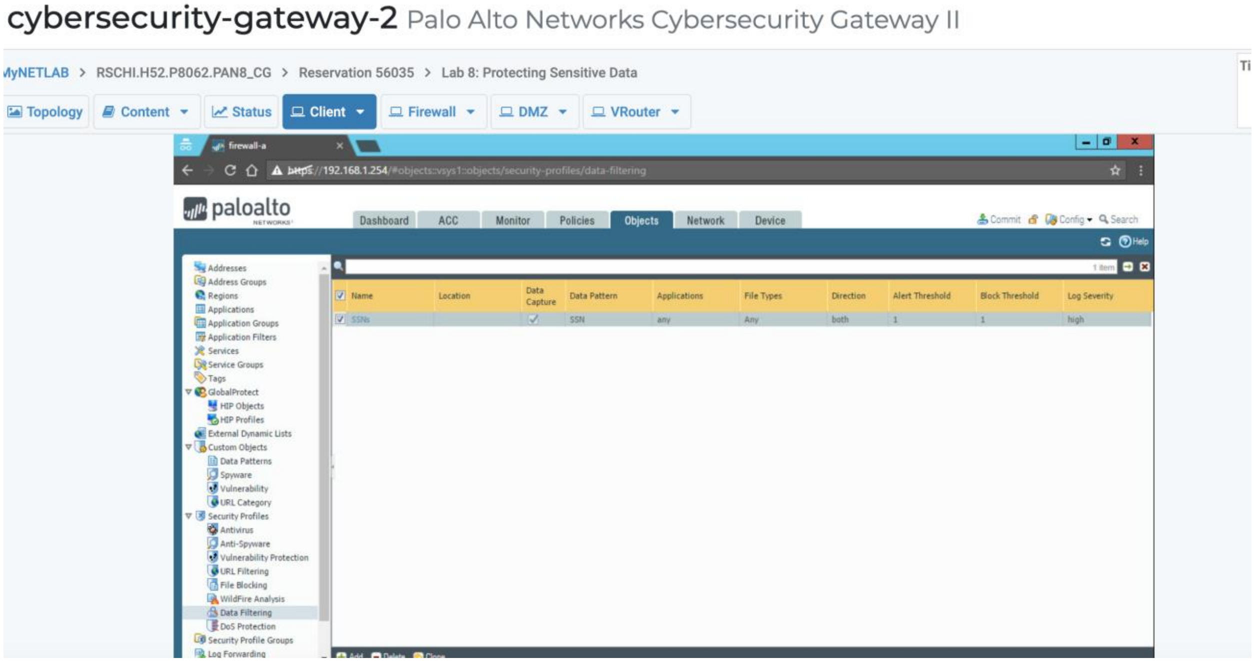
cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

MyNETLAB > RSCHI.H52.P8062.PAN8_CG > Reservation 56035 > Lab 8: Protecting Sensitive Data

https://192.168.1.254/#objects::vsys1::objects/custom-objects/data-patterns

Profile		Pattern			
Name	Location	Type	Name	Default File Type	Pattern
☑ SSN		Predefined Pattern	Social Security Numbers (without dash separator)	Any	US Social Security Numbers pattern without dash

Thresholds added for SSN profile



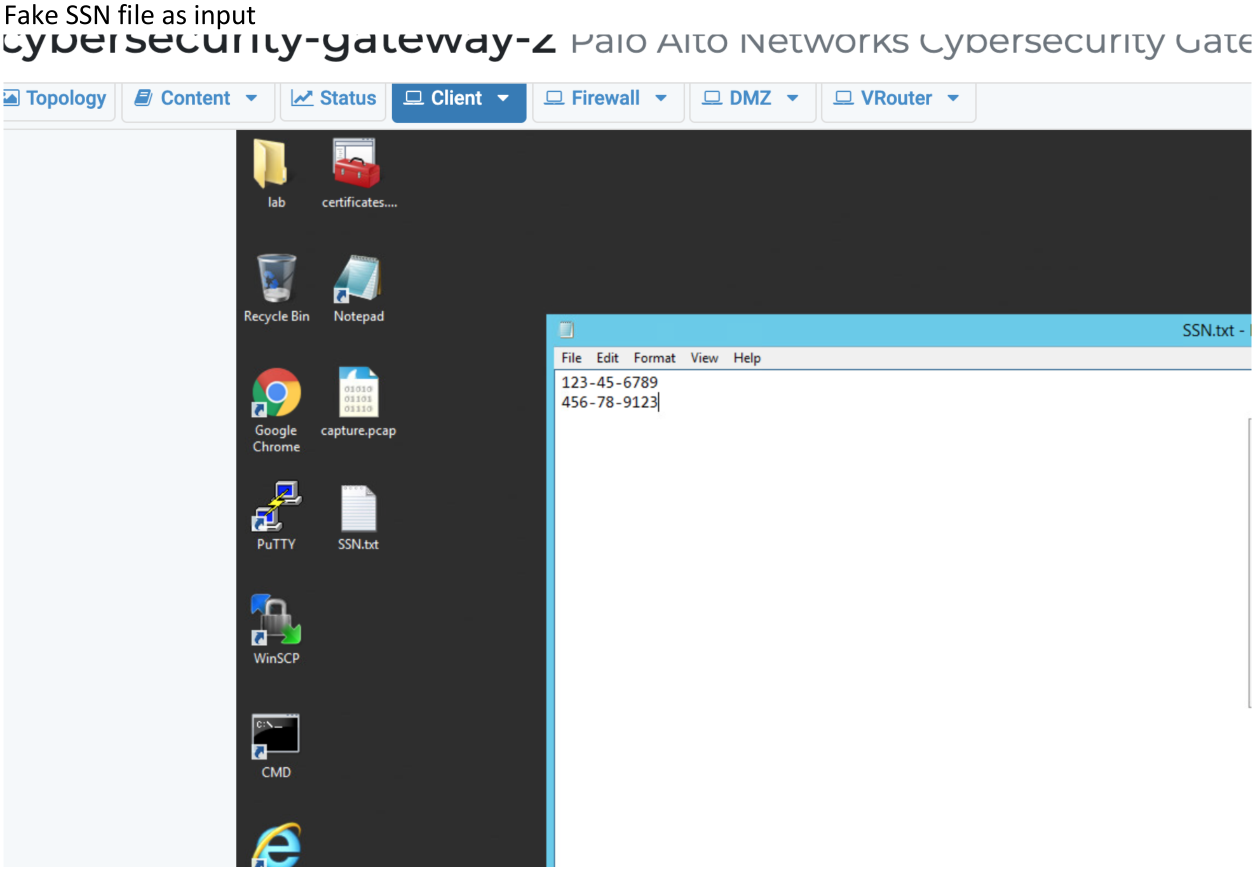
cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

MyNETLAB > RSCHI.H52.P8062.PAN8_CG > Reservation 56035 > Lab 8: Protecting Sensitive Data

https://192.168.1.254/#objects::vsys1::objects/security-profiles/data-filtering

☑ Name	Location	Data Capture	Data Pattern	Applications	File Types	Direction	Alert Threshold	Block Threshold	Log Severity
☑ SSNs		✓	SSN	any	Any	both	1	1	high

Fake SSN file as input



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

Lab 10: Log Forwarding to Linux (Setup syslog to DMZ Server)

==

Introduction

In this lab, I have configured Syslog Monitoring in the Palo Alto Networks Firewall.

I will confirm the logs are being forwarded and view the files on the DMZ server.

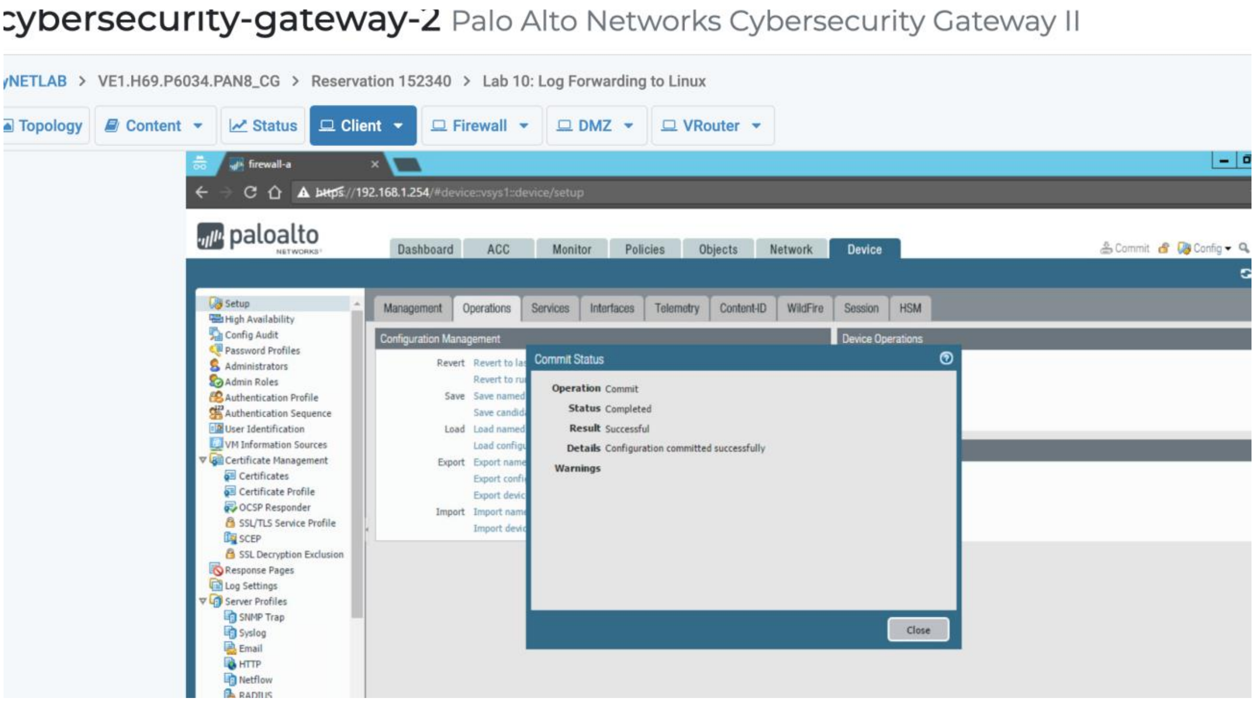
Objective

In this lab, following tasks will be performed:

• Configure Syslog Monitoring via Palo Alto Firewall

- Verify Syslog Forwarding

A) commiting the lab changes



cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

NETLAB > VE1.H69.P6034.PAN8_CG > Reservation 152340 > Lab 10: Log Forwarding to Linux

https://192.168.1.254/#device::vsys1::device/setup

Commit Status

Operation Commit

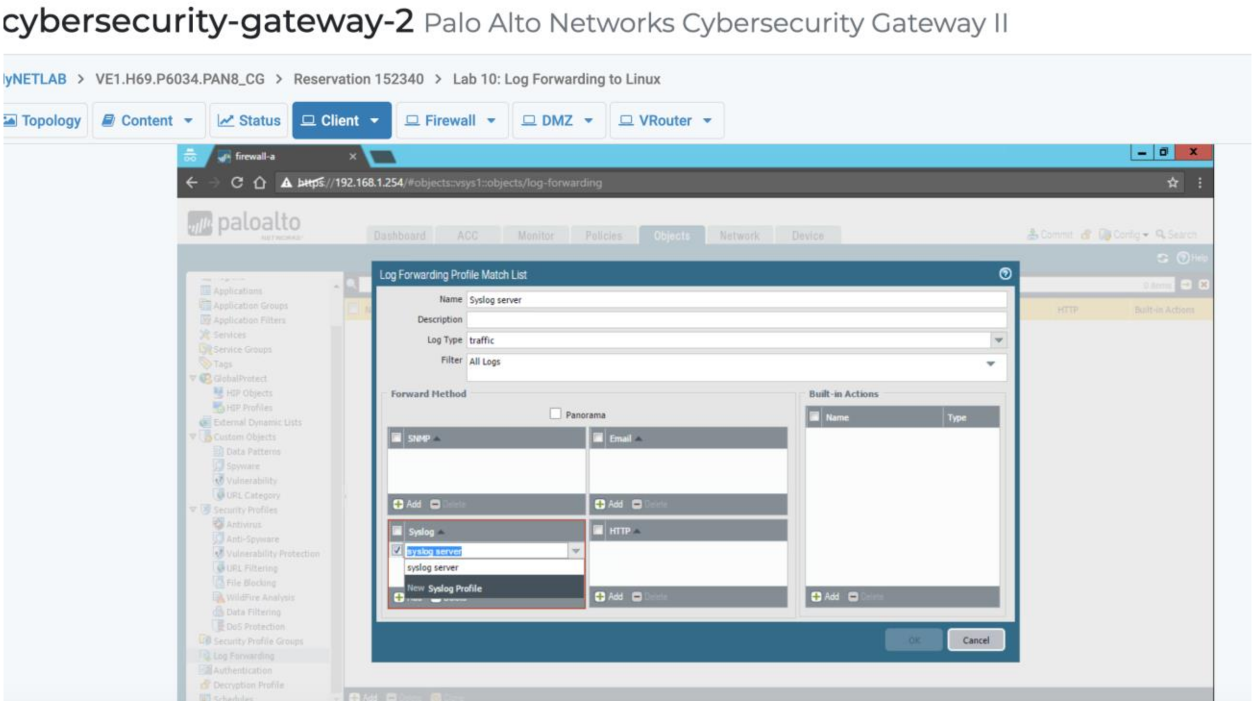
Status Completed

Result Successful

Details Configuration committed successfully

Warnings

B) setting up the log forwarding profile match list and set up of syslog server



cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

NETLAB > VE1.H69.P6034.PAN8_CG > Reservation 152340 > Lab 10: Log Forwarding to Linux

https://192.168.1.254/#objects::vsys1::objects/log-forwarding

Log Forwarding Profile Match List

Name: Syslog server

Description:

Log Type: traffic

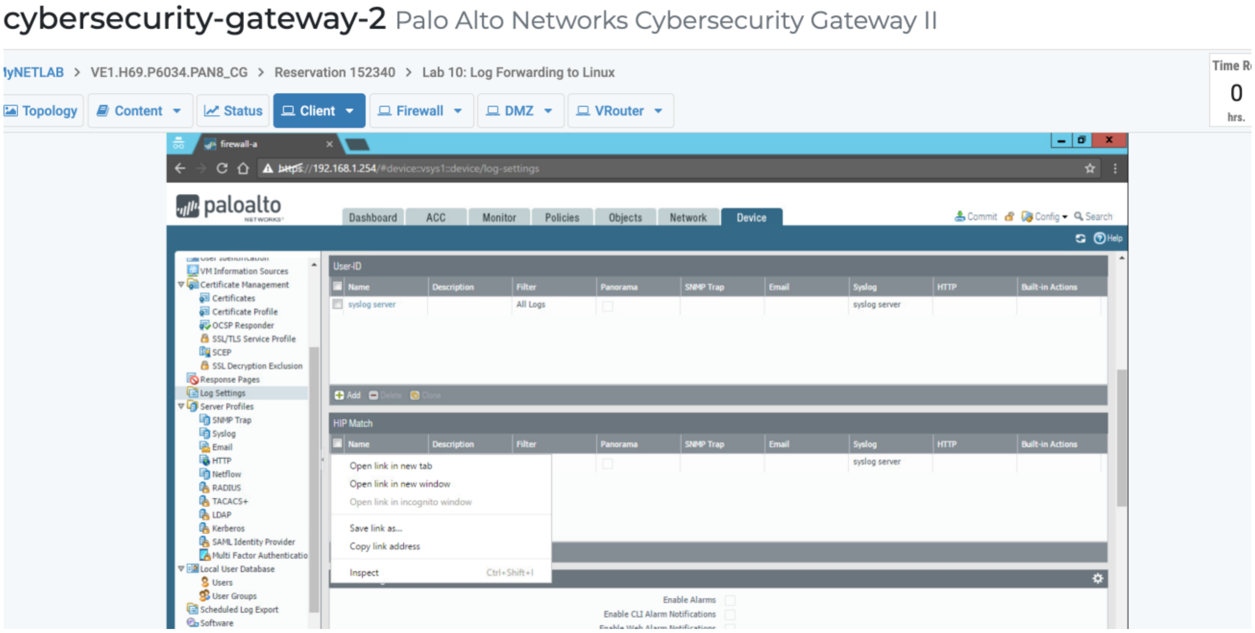
Filter: All Logs

Forward Method

□ Panorama

Syslog: ☑ syslog server

C) Setting up user-ID , HIPA match


cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

User-ID

Name	Description	Filter	Panorama	SNMP Trap	Email	Syslog	HTTP	Built-in Actions
syslog server		All Logs	□			syslog server		

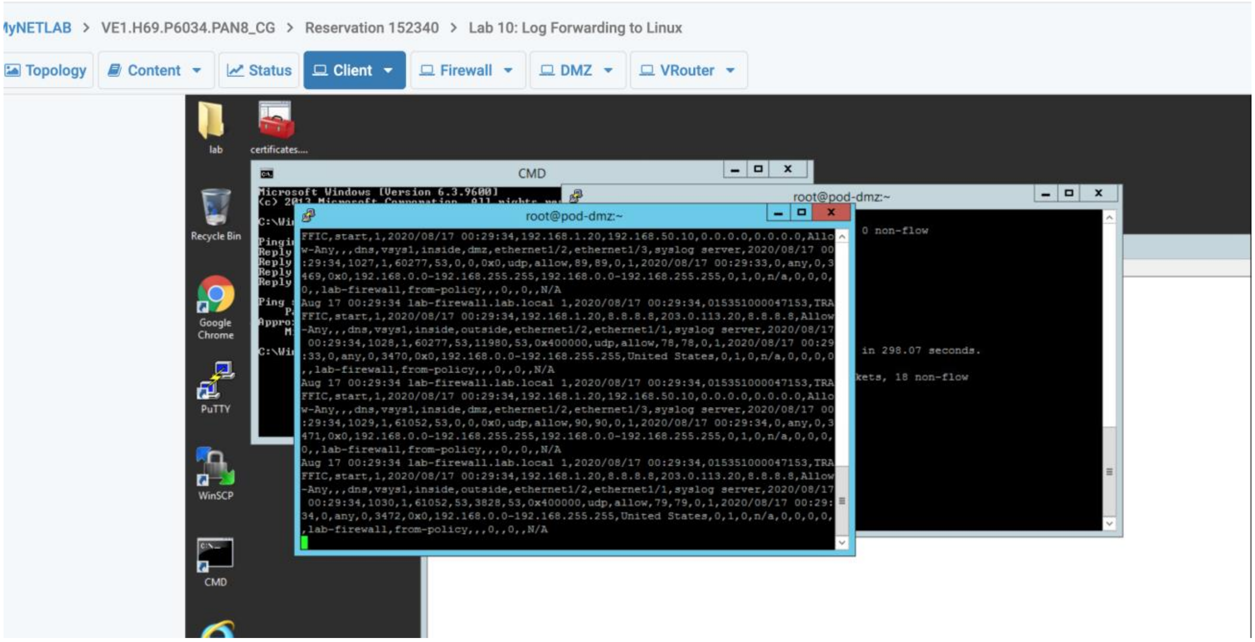
HIP Match

Name	Description	Filter	Panorama	SNMP Trap	Email	Syslog	HTTP	Built-in Actions
			□			syslog server		

Enable Alarms □
Enable CLI Alarm Notifications □

D) Traffic generated and captured on the server

Aa flow of traffic information occurring. The information to verify within the output should be clearly describing the date, source of the syslog data and information about the traffic.



```
FFIC,start,1,2020/08/17 00:29:34,192.168.1.20,192.168.50.10,0.0.0.0,0.0.0.0,Allo
w-Any,,,dns,vsys1,inside,dmz,ethernet1/2,ethernet1/3,syslog server,2020/08/17 00
:29:34,1027,1,60277,53,0,0,0x0,udp,allow,89,89,0,1,2020/08/17 00:29:33,0,any,0,3
469,0x0,192.168.0.0-192.168.255.255,192.168.0.0-192.168.255.255,0,1,0,n/a,0,0,0,
0,,lab-firewall,from-policy,,,0,,0,,N/A
Aug 17 00:29:34 lab-firewall.lab.local 1,2020/08/17 00:29:34,015351000047153,TRA
FFIC,start,1,2020/08/17 00:29:34,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow
-Any,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,syslog server,2020/08/17
 00:29:34,1028,1,60277,53,11980,53,0x400000,udp,allow,78,78,0,1,2020/08/17 00:29
:33,0,any,0,3470,0x0,192.168.0.0-192.168.255.255,United States,0,1,0,n/a,0,0,0,0
,,lab-firewall,from-policy,,,0,,0,,N/A
Aug 17 00:29:34 lab-firewall.lab.local 1,2020/08/17 00:29:34,015351000047153,TRA
FFIC,start,1,2020/08/17 00:29:34,192.168.1.20,192.168.50.10,0.0.0.0,0.0.0.0,Allo
w-Any,,,dns,vsys1,inside,dmz,ethernet1/2,ethernet1/3,syslog server,2020/08/17 00
:29:34,1029,1,61052,53,0,0,0x0,udp,allow,90,90,0,1,2020/08/17 00:29:34,0,any,0,3
471,0x0,192.168.0.0-192.168.255.255,192.168.0.0-192.168.255.255,0,1,0,n/a,0,0,0,
0,,lab-firewall,from-policy,,,0,,0,,N/A
Aug 17 00:29:34 lab-firewall.lab.local 1,2020/08/17 00:29:34,015351000047153,TRA
FFIC,start,1,2020/08/17 00:29:34,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow
-Any,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,syslog server,2020/08/17
 00:29:34,1030,1,61052,53,3828,53,0x400000,udp,allow,79,79,0,1,2020/08/17 00:29:
34,0,any,0,3472,0x0,192.168.0.0-192.168.255.255,United States,0,1,0,n/a,0,0,0,0,
,lab-firewall,from-policy,,,0,,0,,N/A
```

Lab 11: Backing up Firewall Logs

============================

Introduction

In this lab, back up your Firewall logs using both FTP and SCP protocols.

Objective In this lab, perform the following tasks:

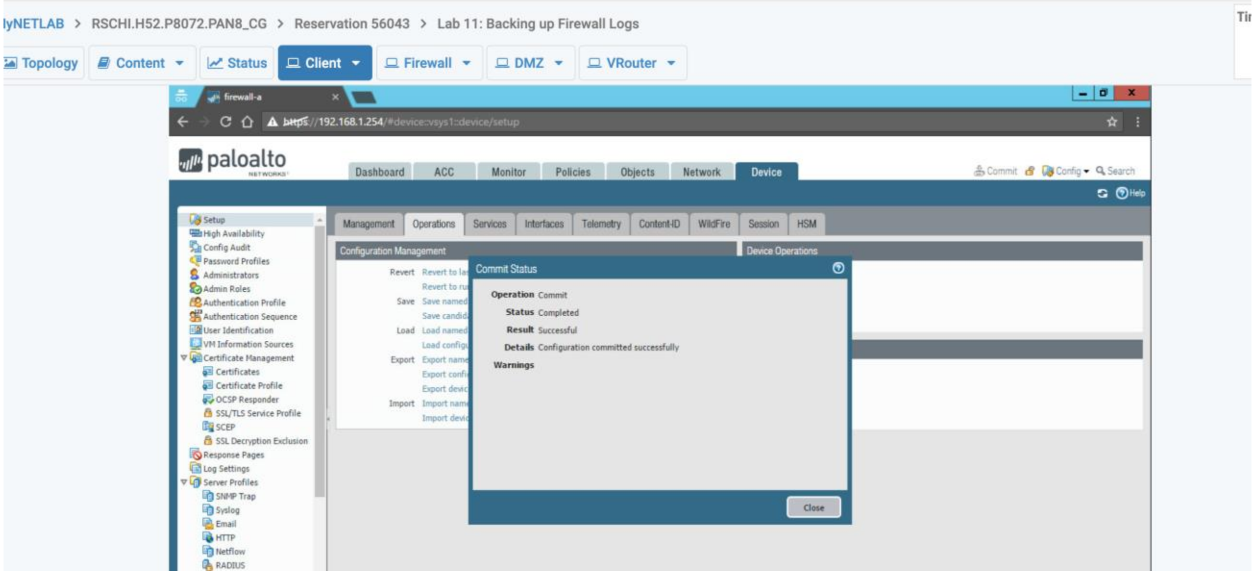
- Back up Firewall Logs

A) Committing the lab changes

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.

B) Back Up Firewall Logs

In this section, export Firewall logs to another location. Exporting firewall logs to an FTP Server is beneficial for keeping logs in the event that the logs are overwritten or an unforeseen event happens to the Firewall and the logs cannot be retrieved.

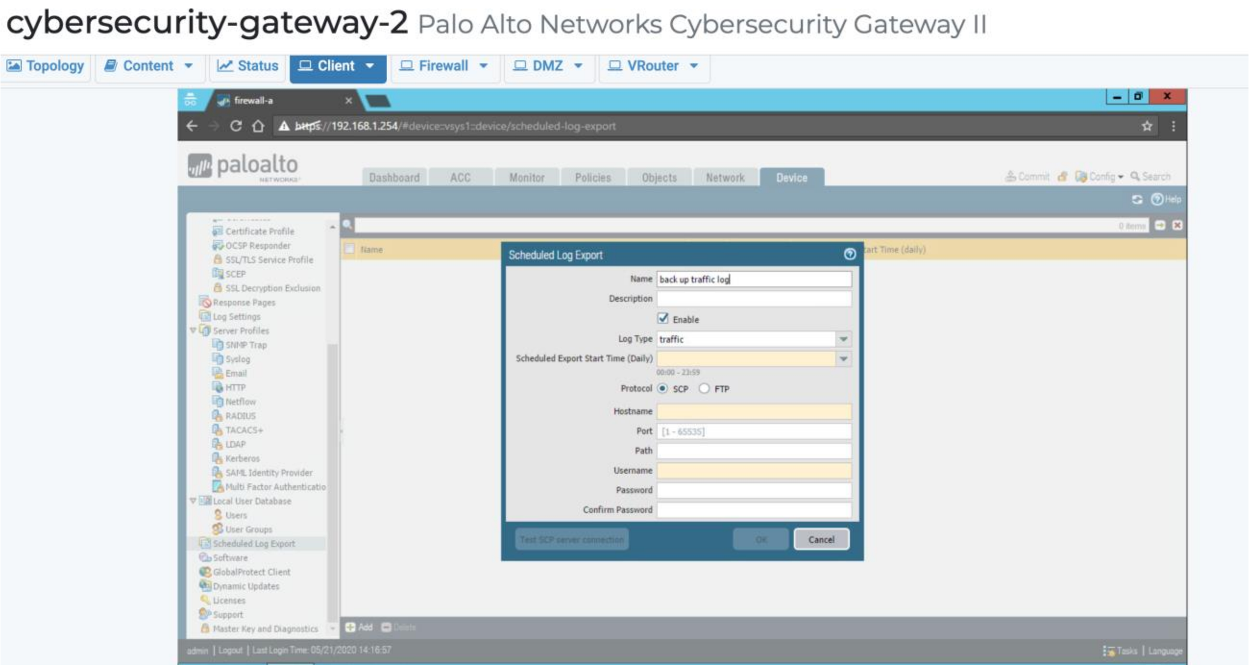


https://192.168.1.254/#device::vsys1::device/setup

Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully
Warnings

C) schedule log export



cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

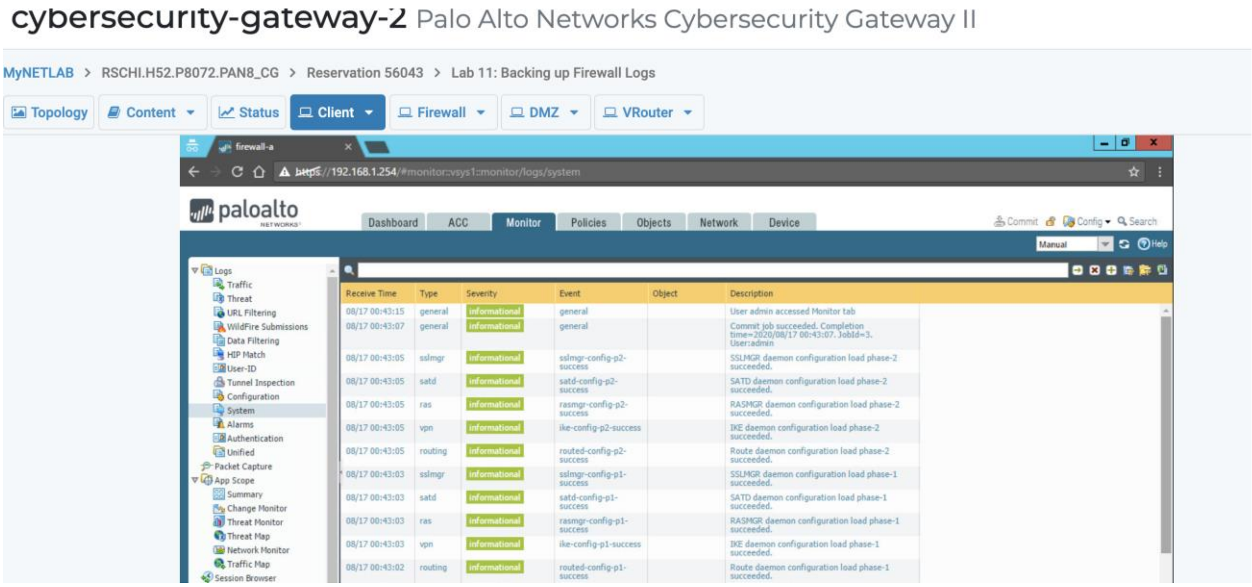
https://192.168.1.254/#device::vsys1::device/scheduled-log-export

Scheduled Log Export

Name: back up traffic log
Description:
☑ Enable
Log Type: traffic
Scheduled Export Start Time (Daily):
00:00 - 23:59
Protocol: ● SCP ○ FTP
Hostname:
Port: [1 - 65535]
Path:
Username:
Password:
Confirm Password:

admin | Logout | Last Login Time: 05/21/2020 14:16:57

D) Monitor log systems



Receive Time	Type	Severity	Event	Object	Description
08/17 00:43:15	general	informational	general		User admin accessed Monitor tab
08/17 00:43:07	general	informational	general		Commit job succeeded. Completion time=2020/08/17 00:43:07. JobId=3. User:admin
08/17 00:43:05	sslmgr	informational	sslmgr-config-p2-success		SSLMGR daemon configuration load phase-2 succeeded.
08/17 00:43:05	satd	informational	satd-config-p2-success		SATD daemon configuration load phase-2 succeeded.
08/17 00:43:05	ras	informational	rasmgr-config-p2-success		RASMGR daemon configuration load phase-2 succeeded.
08/17 00:43:05	vpn	informational	ike-config-p2-success		IKE daemon configuration load phase-2 succeeded.
08/17 00:43:05	routing	informational	routed-config-p2-success		Route daemon configuration load phase-2 succeeded.
08/17 00:43:03	sslmgr	informational	sslmgr-config-p1-success		SSLMGR daemon configuration load phase-1 succeeded.
08/17 00:43:03	satd	informational	satd-config-p1-success		SATD daemon configuration load phase-1 succeeded.
08/17 00:43:03	ras	informational	rasmgr-config-p1-success		RASMGR daemon configuration load phase-1 succeeded.
08/17 00:43:03	vpn	informational	ike-config-p1-success		IKE daemon configuration load phase-1 succeeded.
08/17 00:43:02	routing	informational	routed-config-p1-success		Route daemon configuration load phase-1 succeeded.

Lab 9: Preventing Threats from the Internet with File Blocking

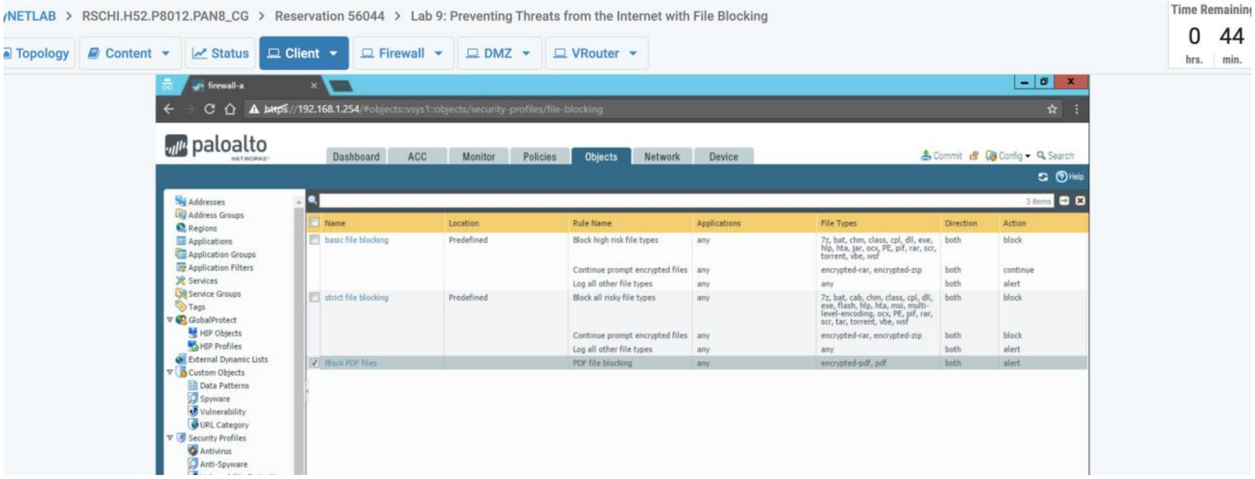
===

Introduction In this lab, create a File Blocking Profile to block PDF files.

After creating a File Blocking Profile, then test the profile by trying to download a PDF file.

Objective In this lab, perform the following tasks: • Create a File Blocking Security Profile • Apply the File Blocking Profile to a Security Policy • Test the File Blocking Profile

a. Creating a file blocking profile



NETLAB > RSCHI.H52.P8012.PAN8_CG > Reservation 56044 > Lab 9: Preventing Threats from the Internet with File Blocking

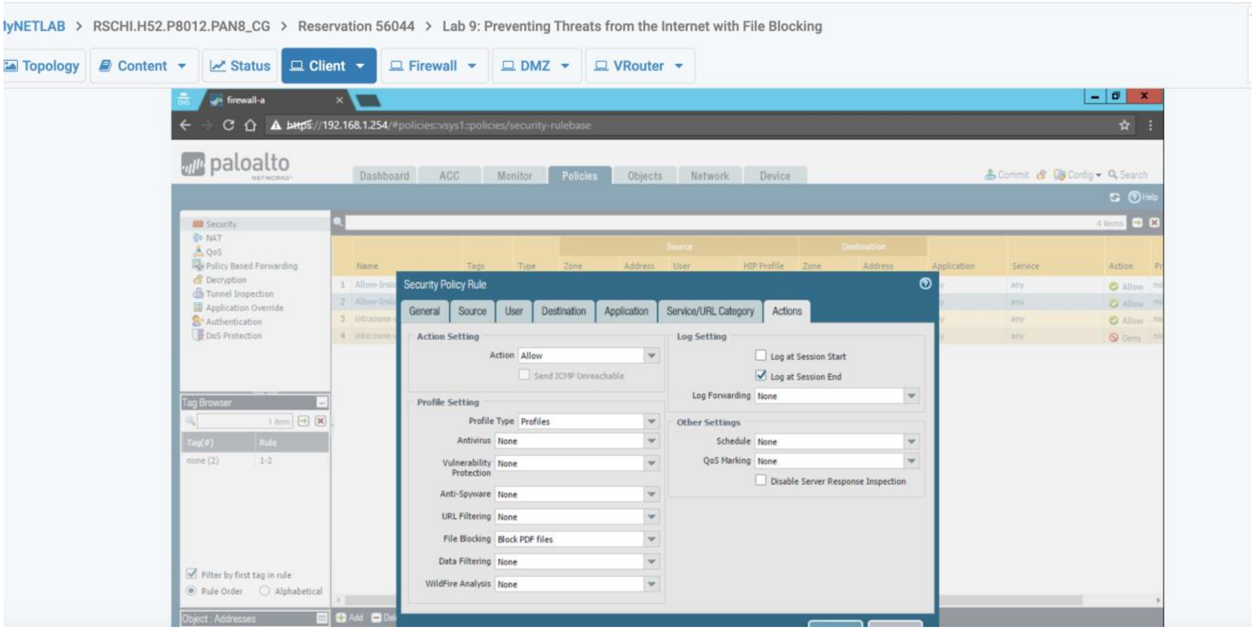
Time Remaining 0 hrs. 44 min.

https://192.168.1.254/#objects::vsys1::objects/security-profiles/file-blocking

Name	Location	Rule Name	Applications	File Types	Direction	Action
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, multi-level-encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert
☑ Block PDF files		PDF file blocking	any	encrypted-pdf, pdf	both	alert

B) applying the security policy rule

cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II



NETLAB > RSCHI.H52.P8012.PAN8_CG > Reservation 56044 > Lab 9: Preventing Threats from the Internet with File Blocking

https://192.168.1.254/#policies::vsys1::policies/security-rulebase

Security Policy Rule — Actions

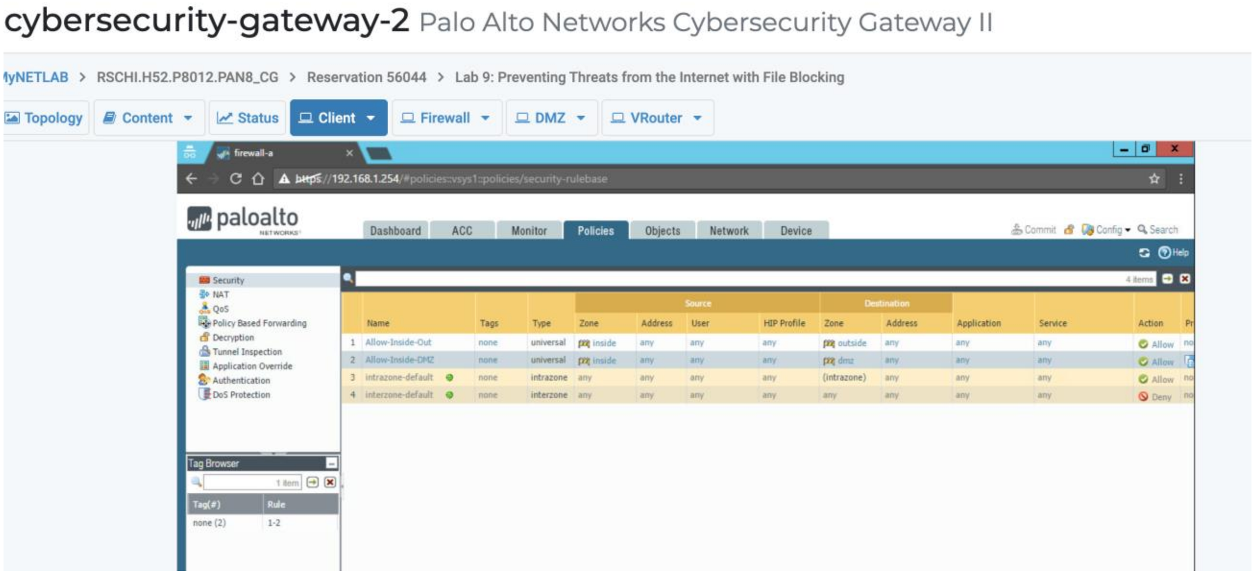
Action Setting
- Action: Allow
- □ Send ICMP Unreachable

Profile Setting
- Profile Type: Profiles
- Antivirus: None
- Vulnerability Protection: None
- Anti-Spyware: None
- URL Filtering: None
- File Blocking: Block PDF files
- Data Filtering: None
- 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

C) allow-inside-DMZ policy has blocked the PDF files



cybersecurity-gateway-2 Palo Alto Networks Cybersecurity Gateway II

				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Pr
1	Allow-Inside-Out	none	universal	inside	any	any	any	outside	any	any	any	Allow	no
2	Allow-Inside-DMZ	none	universal	inside	any	any	any	dmz	any	any	any	Allow	
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	no
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	no

Tag(#)	Rule
none (2)	1-2

In this lab we have applied security policy to block pdf files.

==

Student Input : project 2.

1. What function does ARP perform:

ARP helps to find the mac-address with known IP address for a device on local network. ARP is address resolution protocol.

It helps to discover the mac address for a known IP address(typically an IPv4 address)

2. What is the purpose of DNS?

DNS is domain name service and is used to resolve the domain name to an IP address. It translated domain names into IP addresses that a client can understand.

3. Explain how TCP works?

TCP provides a reliable communication at layer 4 between two nodes. It establishes connection between two machines using a three way handshake and utilizes features as acknowledgement, fragmentation of data to provide a reliable communication while taking cares of buffer at receiver using sliding windows mechanism. Tear down of connection is performed after the transmission.

4. What is the purpose of HTTP?

HTTP is hyper text transfer protocol and is an application protocol.

It was developed for the communication between web browsers and web servers.

It is used for transmitting hyper media documents such as HTML.