

# SIDDHANT GAHTORI

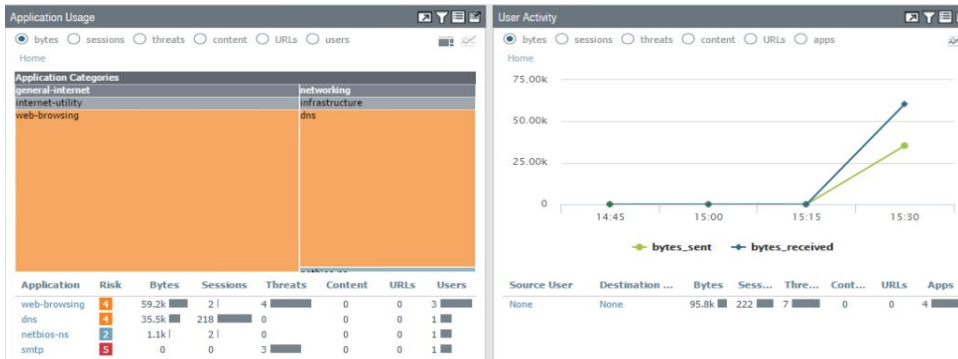
## GATEWAY PROJECT 2

### Module 1A (LAB 6): Using the Application Command Center

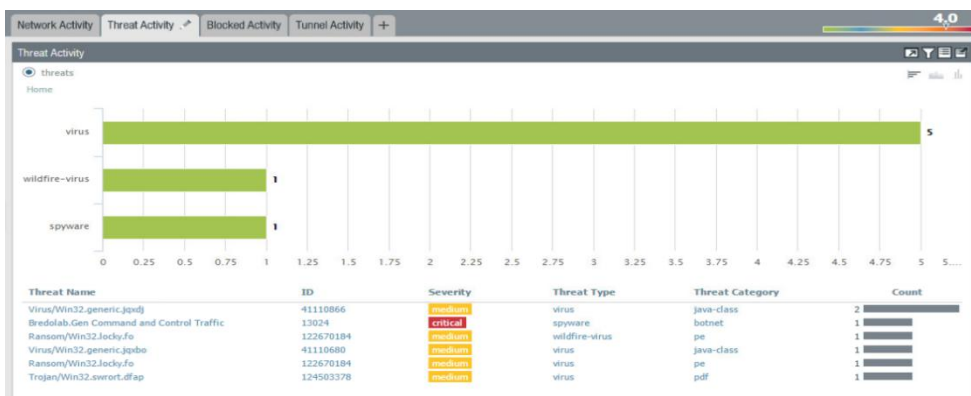
**Summary:** In this module, firstly we generated malware traffic towards firewall. Then to analyze the threat activity we clicked on Threat Activity tab on ACC Menu. After that we can see the network surge and unwanted activity on the firewall end.

```
root@pod-dmz:~  
Using username "root".  
root@192.168.50.10's password:  
Access denied  
root@192.168.50.10's password:  
Last failed login: Sun May 3 15:41:01 UTC 2020 from 192.168.1.20 on ssh:notty  
There was 1 failed login attempt since the last successful login.  
Last login: Wed Oct 3 18:27:09 2018 from 192.168.1.20  
[root@pod-dmz ~]# sh /tg/malware.sh  
  
THIS COULD TAKE UP TO 10 MINUTES
```

◆ Sending the malware traffic to firewall.



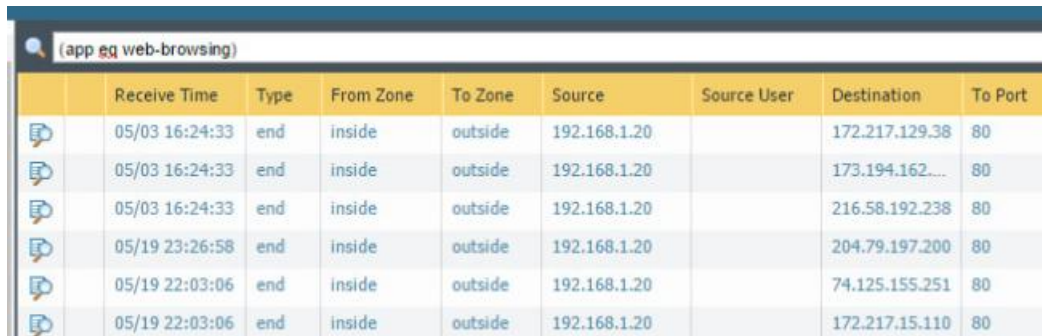
◆ Network Surge during the activity









◆ Threat Activity Monitor

## Module 1B (LAB 7): Analyzing Firewall Logs

**Summary:** In this module, firstly we generated malware traffic towards firewall. Then to analyze the logs we clicked on Monitor tab on Menu. After that we can see and analyze every kind of traffic.

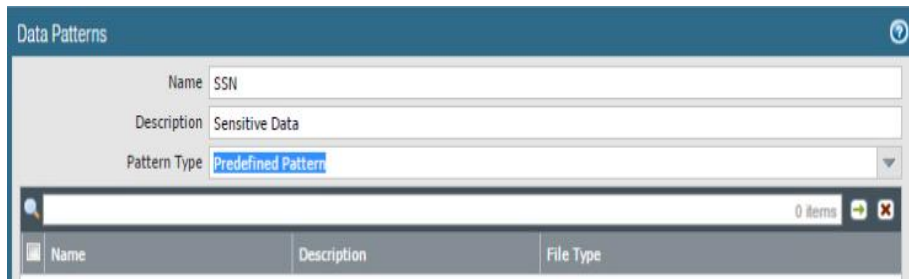


	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port
	05/03 16:24:33	end	inside	outside	192.168.1.20		172.217.129.38	80
	05/03 16:24:33	end	inside	outside	192.168.1.20		173.194.162....	80
	05/03 16:24:33	end	inside	outside	192.168.1.20		216.58.192.238	80
	05/19 23:26:58	end	inside	outside	192.168.1.20		204.79.197.200	80
	05/19 22:03:06	end	inside	outside	192.168.1.20		74.125.155.251	80
	05/19 22:03:06	end	inside	outside	192.168.1.20		172.217.15.110	80

- ◆ Analyzing traffic for web based activities

## Module 2A (LAB 8): Protecting Sensitive Data

**Summary:** In this module first we made a policy to restrict access of certain type of traffic for a predefined pattern. After that we tested and verified that policy. We monitored sensitive data like social security numbers in palo alto networks firewall.

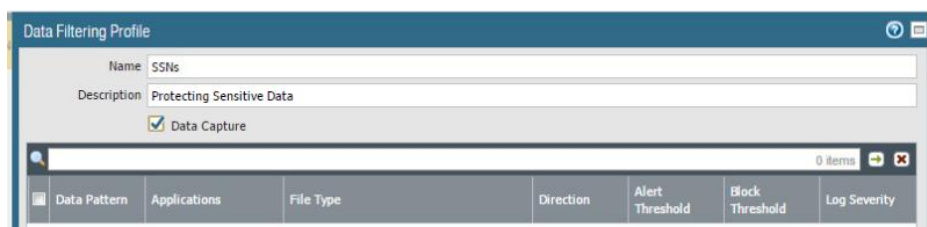


The 'Data Patterns' configuration window shows the following details:

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

Below the configuration fields is a table with columns: Name, Description, File Type. The table is currently empty, showing 0 items.

### ◆ Defining Data Patterns

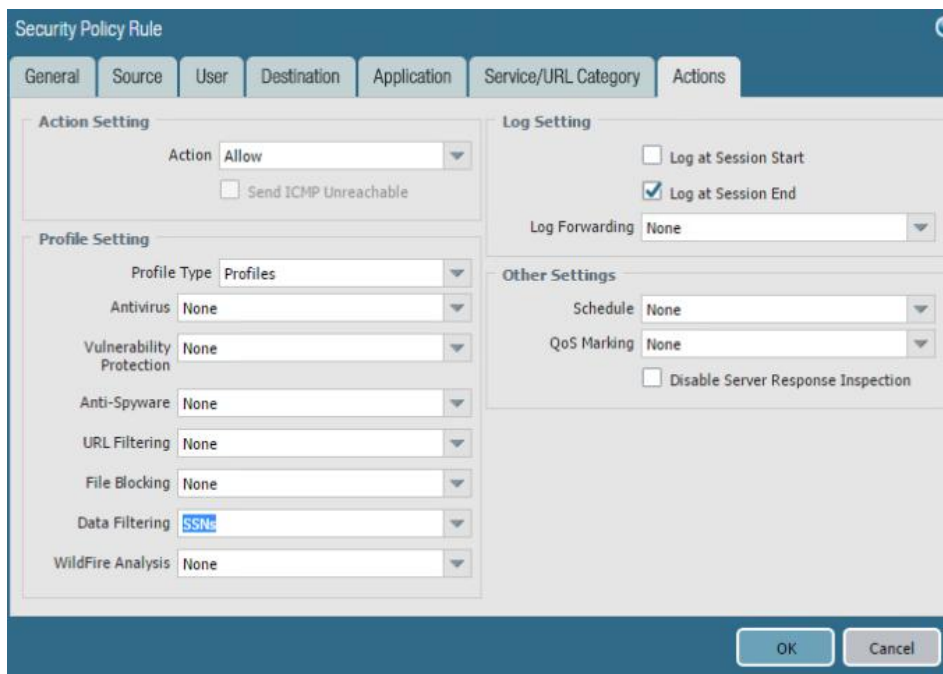


The 'Data Filtering Profile' configuration window shows the following details:

- Name: SSNs
- Description: Protecting Sensitive Data
- ☒ Data Capture

Below the configuration fields is a table with columns: Data Pattern, Applications, File Type, Direction, Alert Threshold, Block Threshold, Log Severity. The table is currently empty, showing 0 items.

### ◆ Defining Data Filtering Profile for Social Security Numbers

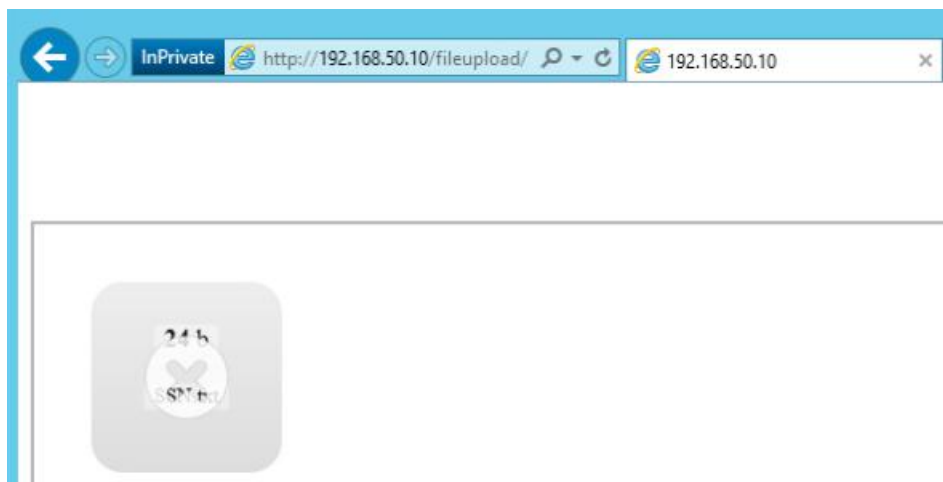


The 'Security Policy Rule' configuration window shows the following details:

- General tab is selected.
- Action Setting: Action is set to 'Allow'. ☐ Send ICMP Unreachable.
- Profile Setting: Profile Type is 'Profiles'. Antivirus, Vulnerability Protection, Anti-Spyware, URL Filtering, File Blocking, Data Filtering (set to 'SSNs'), and WildFire Analysis are all set to 'None'.
- Log Setting: ☐ Log at Session Start, ☒ Log at Session End. Log Forwarding is set to 'None'.
- Other Settings: Schedule is 'None', QoS Marking is 'None', and ☐ Disable Server Response Inspection.

Buttons: OK, Cancel

### ◆ Creating firewall rules



#### ◆ Testing the Policy

**Detailed Log View**

Log Action		Details		Flags	
Category	any	Content Type	data	Captive Portal	<input type="checkbox"/>
Generated Time	2020/05/03 17:28:03	Content	SSN	Proxy Transaction	<input type="checkbox"/>
Receive Time	2020/05/03 17:28:03	ID	60000 (View in Threat Vault)	Decrypted	<input type="checkbox"/>
Tunnel Type	N/A	Severity	high	Packet Capture	<input type="checkbox"/>
		Repeat Count	1	Client to Server	<input checked="" type="checkbox"/>
		File Name	SSN.txt	Server to Client	<input type="checkbox"/>
		URL		Tunnel Inspected	<input type="checkbox"/>

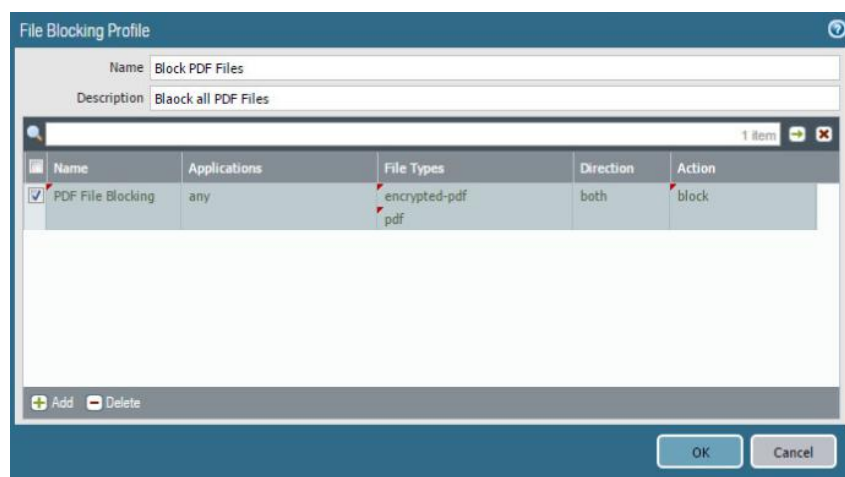
  

PCAP	Receive Time	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
	2020/05/03 17:28:03	data	web-browsing	reset-server	Allow-Inside-DMZ		high	any			SSN.txt

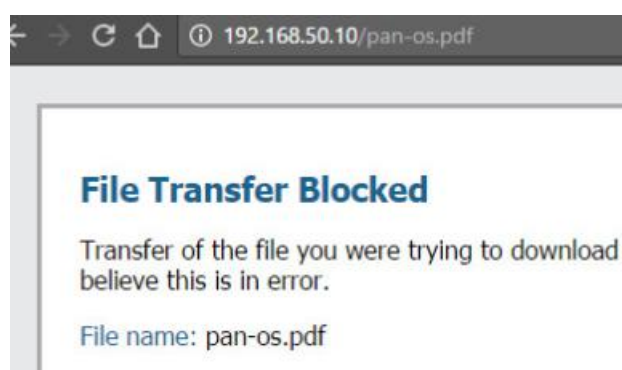
#### ◆ Verifying the Policy

## Module 2B (LAB 9): File Blocking

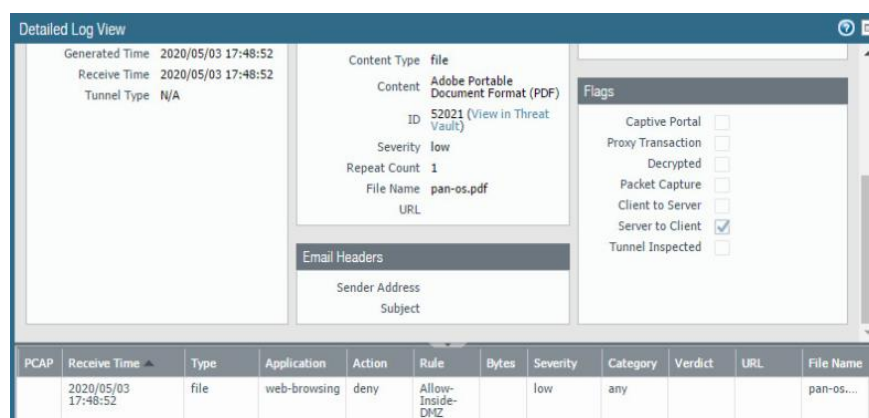
**Summary:** Objectives of this module consist of creating, applying and testing File Blocking Security Profile. To achieve that, first we clicked File Blocking option from Object Tab. After that we made a policy to block all kind of PDF Files and added to the firewall rules. Then we tested the rule and analyzed the logs.



### ◆ Creation of File Blocking Rule for PDF Files



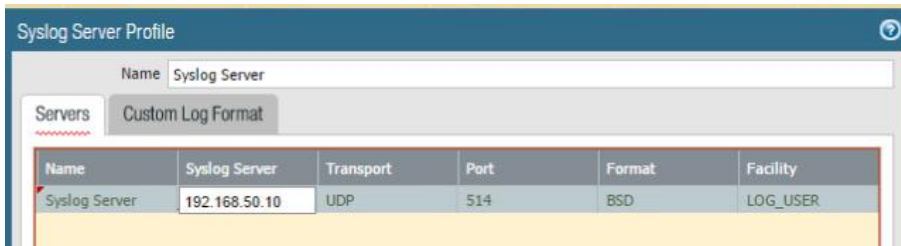
### ◆ Testing of the Rule



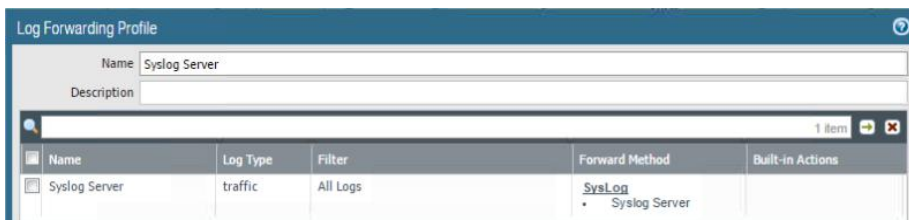
### ◆ Log Analysis of Unwanted Action

## Module 3A (LAB 10): Log Forwarding

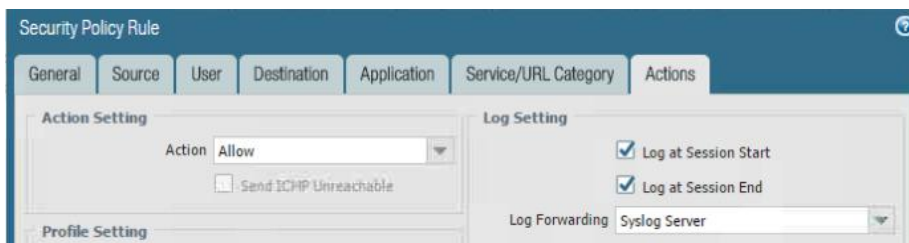
**Summary:** In this module, the objective is to configure Syslog on palo alto firewall and verify Syslog forwarding. For that, A First we clicked Device > Syslog tab. Then we add a Syslog server at IP of 192.168.50.10. Then we clicked Objects > Log Forwarding option. Then in Log Settings, we added Syslog Server. Then we changed security policy to modify log forwarding option. Then we verified the implementation.



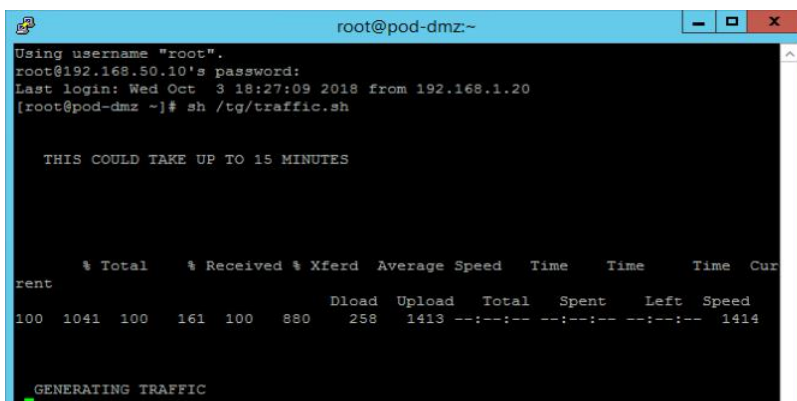
### ◆ Syslog Server Profile Configurations



### ◆ Creating Log Forwarding Profile



### ◆ Security Policy Rule Configurations



### ◆ Traffic Generation

```

root@pod-dmz:~
FFIC,start,1,2020/05/04 02:19:38,192.168.1.20,192.168.50.10,0.0.0.0,0.0.0.0,Allow-Any,,,dns,vsys1,inside,dmz,ethernet1/2,ethernet1/3,Syslog Server,2020/05/04 02:19:38,757,1,49913,53,0,0,0x0,udp,allow,90,90,0,1,2020/05/04 02:19:38,0,any,0,2871,0x0,192.168.0.0-192.168.255.255,192.168.0.0-192.168.255.255,0,1,0,n/a,0,0,0,0,,lab-firewall,from-policy,,,0,,0,,N/A
May  4 02:19:38 lab-firewall.lab.local 1,2020/05/04 02:19:38,015351000028085,TRAFFIC,start,1,2020/05/04 02:19:38,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow-Any,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,Syslog Server,2020/05/04 02:19:38,758,1,49913,53,10538,53,0x400000,udp,allow,79,79,0,1,2020/05/04 02:19:38,0,any,0,2872,0x0,192.168.0.0-192.168.255.255,United States,0,1,0,n/a,0,0,0,0,,lab-firewall,from-policy,,,0,,0,,N/A
May  4 02:19:38 lab-firewall.lab.local 1,2020/05/04 02:19:38,015351000028085,TRAFFIC,end,1,2020/05/04 02:19:38,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow-Any,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,Syslog Server,2020/05/04 02:19:38,734,1,65304,53,7250,53,0x400064,udp,allow,184,78,106,2,2020/05/04 02:19:08,0,any,0,2873,0x0,192.168.0.0-192.168.255.255,United States,0,1,1,aged-out,0,0,0,0,,lab-firewall,from-policy,,,0,,0,,N/A

```

#### ◆ Captured Logs & Analysis

## Module 3B (LAB 11): Backup Firewall Logs

**Summary:** In this lab, the objective is to backup firewall logs. At First we go to Schedule Log Export option. We configure settings as per our convenience . After committing the changes, we can go to Monitor > Logs > System to see the backed up logs.

Scheduled Log Export

Name: Backup Traffic Log

Description:

☒ Enable

Log Type: traffic

Scheduled Export Start Time (Daily): 04:28

Protocol: ☐ SCP ☒ FTP

Hostname: 192.168.50.10

Port: 21

Path: /

Username: lab user

Password: .....

Confirm Password: .....

☒ Enable FTP Passive Mode

Test SCP server connection

OK Cancel

### ◆ Log Schedule Setting

05/04 04:28:02	general	informational	general	Failed exporting traffic log via ftp (last-calendar-day)
05/04 04:27:54	general	informational	general	User admin accessed Monitor tab

### ◆ Backed up Logs



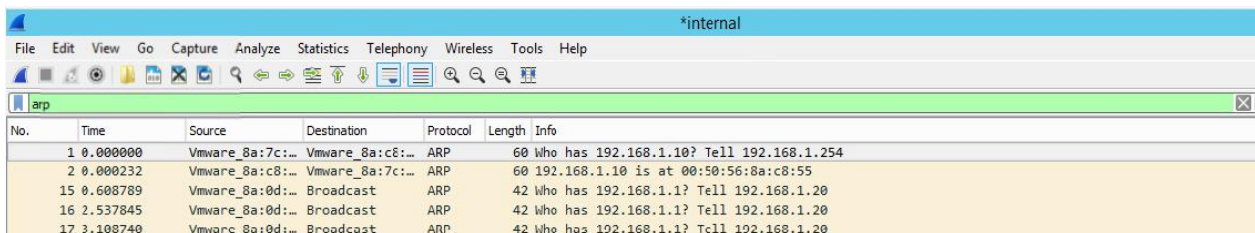
## Project Introduction:

In this project, you will utilize Wireshark to initiate a packet capture. Wireshark captures packets and allows network administrators to examine the data within the packet.

Objective In this project, you will perform the following tasks:

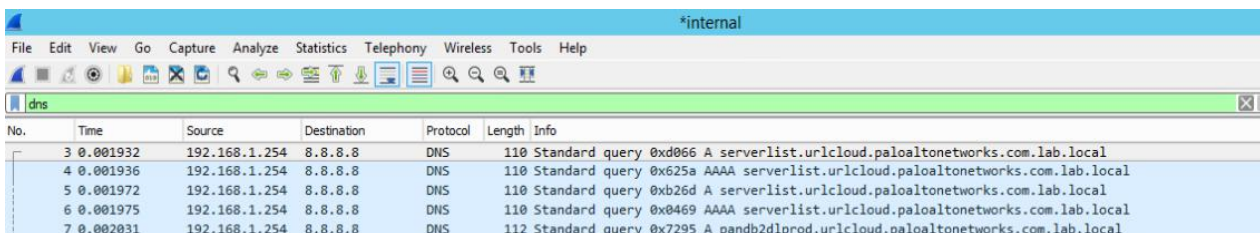
- ◆ Create and analyze a Packet Capture using Wireshark

### Screenshot:



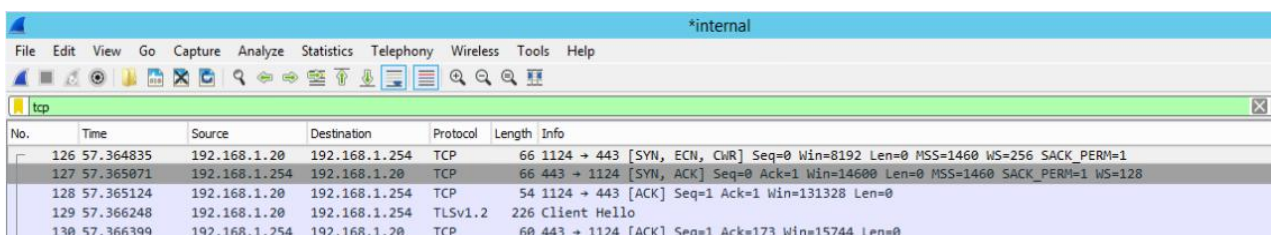
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_8a:7c:...	Vmware_8a:c8:...	ARP	60	Who has 192.168.1.10? Tell 192.168.1.254
2	0.000232	Vmware_8a:c8:...	Vmware_8a:7c:...	ARP	60	192.168.1.10 is at 00:50:56:8a:c8:55
15	0.608789	Vmware_8a:0d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
16	2.537845	Vmware_8a:0d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20
17	3.108740	Vmware_8a:0d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.20

### ◆ ARP Packet Capture



No.	Time	Source	Destination	Protocol	Length	Info
3	0.001932	192.168.1.254	8.8.8.8	DNS	110	Standard query 0xd066 A serverlist.urlcloud.paloaltonetworks.com.lab.local
4	0.001936	192.168.1.254	8.8.8.8	DNS	110	Standard query 0x625a AAAA serverlist.urlcloud.paloaltonetworks.com.lab.local
5	0.001972	192.168.1.254	8.8.8.8	DNS	110	Standard query 0xb26d A serverlist.urlcloud.paloaltonetworks.com.lab.local
6	0.001975	192.168.1.254	8.8.8.8	DNS	110	Standard query 0x0469 AAAA serverlist.urlcloud.paloaltonetworks.com.lab.local
7	0.002031	192.168.1.254	8.8.8.8	DNS	112	Standard query 0x7295 A pandb2dlprod.urlcloud.paloaltonetworks.com.lab.local

### ◆ DNS Captures



No.	Time	Source	Destination	Protocol	Length	Info
126	57.364835	192.168.1.20	192.168.1.254	TCP	66	1124 → 443 [SYN, ECN, Chr] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
127	57.365071	192.168.1.254	192.168.1.20	TCP	66	443 → 1124 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
128	57.365124	192.168.1.20	192.168.1.254	TCP	54	1124 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
129	57.366248	192.168.1.20	192.168.1.254	TLSv1.2	226	Client Hello
130	57.366399	192.168.1.254	192.168.1.20	TCP	60	443 → 1124 [ACK] Seq=1 Ack=173 Win=15744 Len=0

### ◆ TCP Captures

```
> Frame 1596: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
> Ethernet II, Src: Azurewav_93:2c:81 (80:a5:89:93:2c:81), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 55536, Dst Port: 1900
▼ Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/1]
```

## ◆ HTTP Captures

### Explanations:

1. Function of ARP : Conversion between IP and MAC Addresses
2. Purpose of DNS : Converting IP Addresses to Domain Names on Port 53
3. Working of TCP : 3 way handshake (SYN, SYN-ACK, ACK) Packets
4. Purpose of HTTP : Web Based Communications on Port 80