ASSIGNMENT

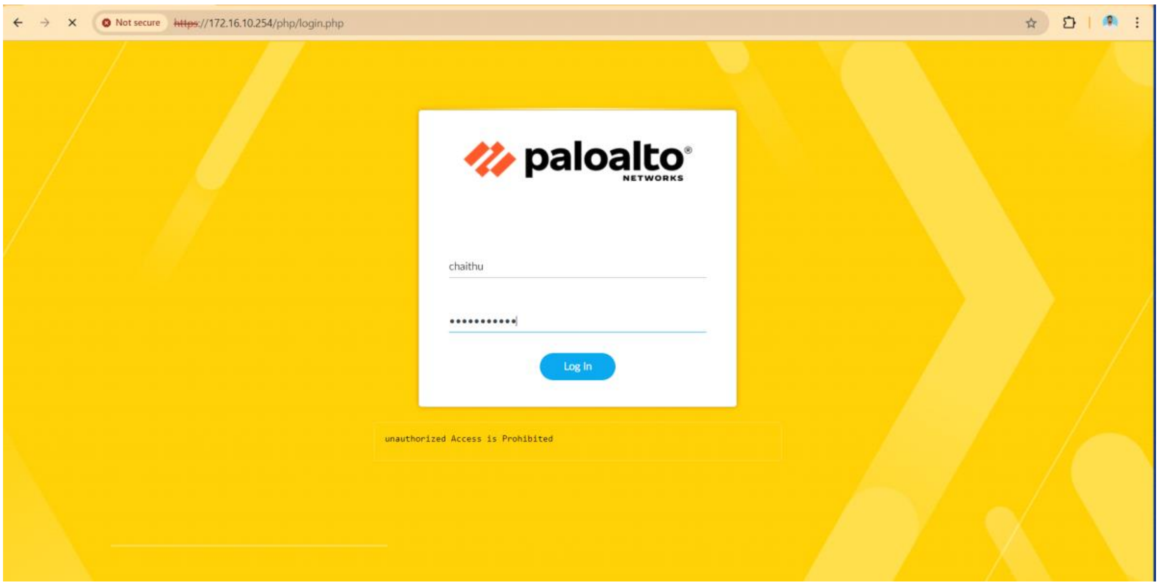
COURSE	PAN Firewall	**ASSIGNMENT NO**	7
MODULE	Security profile and Packet capture	**ASSIGNMENT DATE**	03-Oct-2024
STUDENT NAME	Konganti Chaithanya Kumar	**SUBMIT DATE**	03-Oct-2024

1. Steps to Configure Security Profiles: File Blocking and DoS Protection on Palo Alto Firewall

A. File Blocking Security Profile Configuration

Step 1: Login to the PAN Firewall

- Open a web browser and navigate to the firewall's IP address.
- Log in with your admin credentials.



Not secure ~~https~~://172.16.10.254/php/login.php

chaithu

•••••••••••

unauthorized Access is Prohibited

Step 2: Navigate to File Blocking Profile

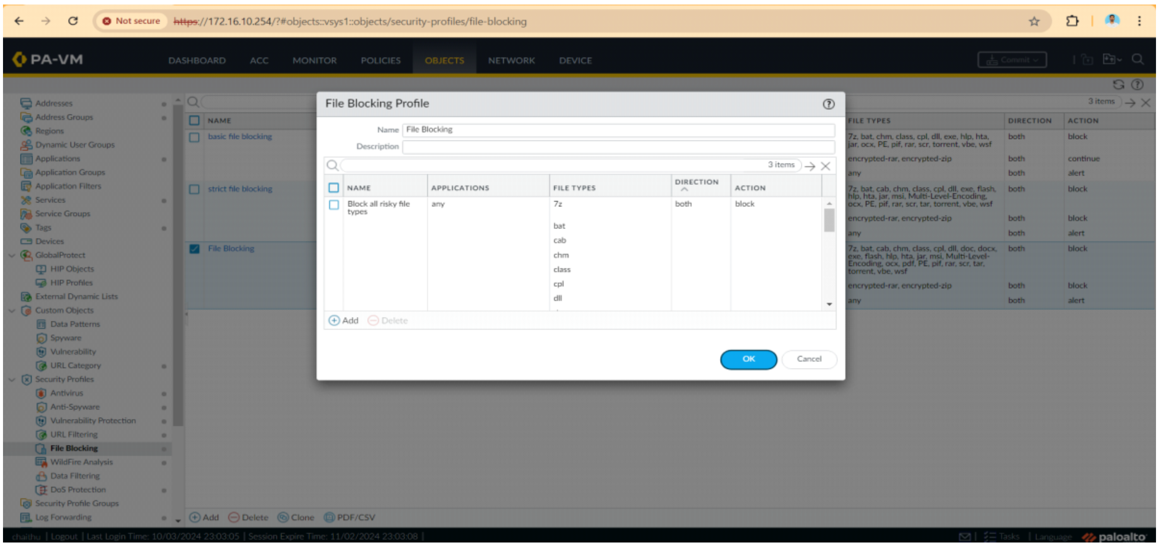
- On the web interface, go to **Objects > Security Profiles > File Blocking**.

Step 3: Create a New File Blocking Profile

- Click **Add** to create a new File Blocking profile.
- Name the profile (e.g., "File-Block-Policy").

Step 4: Add Blocking Rules

- Under **File Blocking Rules**, click **Add**.
- Select the **Application** (e.g., web-browsing, ftp, etc.).
- Select the **File Type** (e.g., PE files, PDF, MS Office, etc.) you want to block.
- Choose the **Action** (e.g., Block or Alert).
- Click **OK** to save.



File Blocking Profile

Name: File Blocking

Description:

3 items

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
Block all risky file types	any	7z bat cab chm class cpl dll	both	block

⊕ Add ⊖ Delete

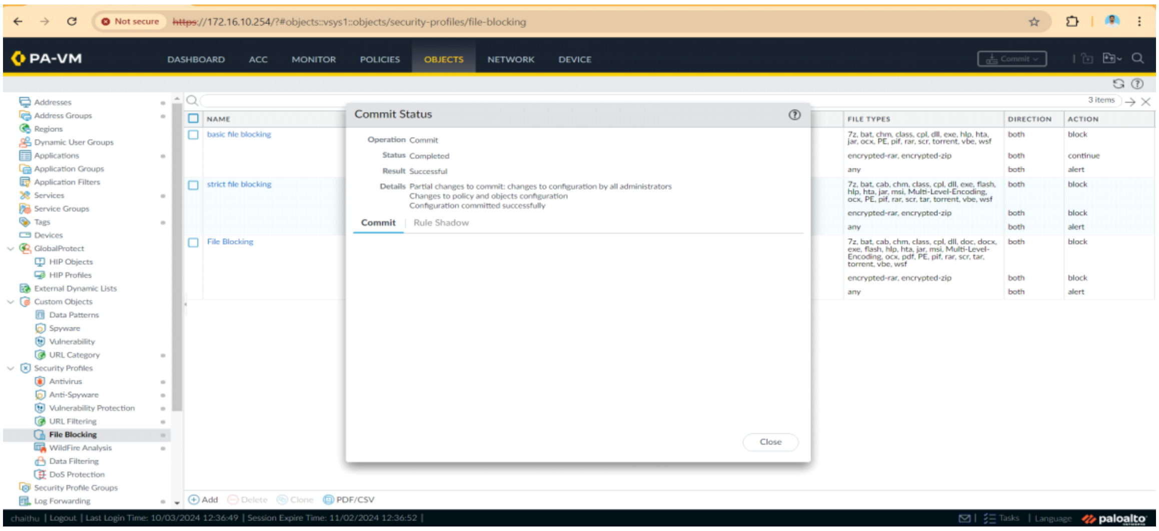
OK Cancel

NAME	FILE TYPES	DIRECTION	ACTION
basic file blocking	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	continue
	any	both	alert
strict file blocking	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	block
	any	both	alert
File Blocking	7z, bat, cab, chm, class, cpl, dll, doc, docx, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, pdf, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	block
	any	both	alert

chaithu | Logout | Last Login Time: 10/03/2024 23:03:05 | Session Expire Time: 11/02/2024 23:03:08 |

Step 5: Attach File Blocking Profile to Security Policy

- Go to **Policies > Security**.
- Choose an existing Security Policy or create a new one.
- Under the **Actions** tab, apply the newly created File Blocking profile by selecting it from the dropdown.



Commit Status

Operation: Commit

Status: Completed

Result: Successful

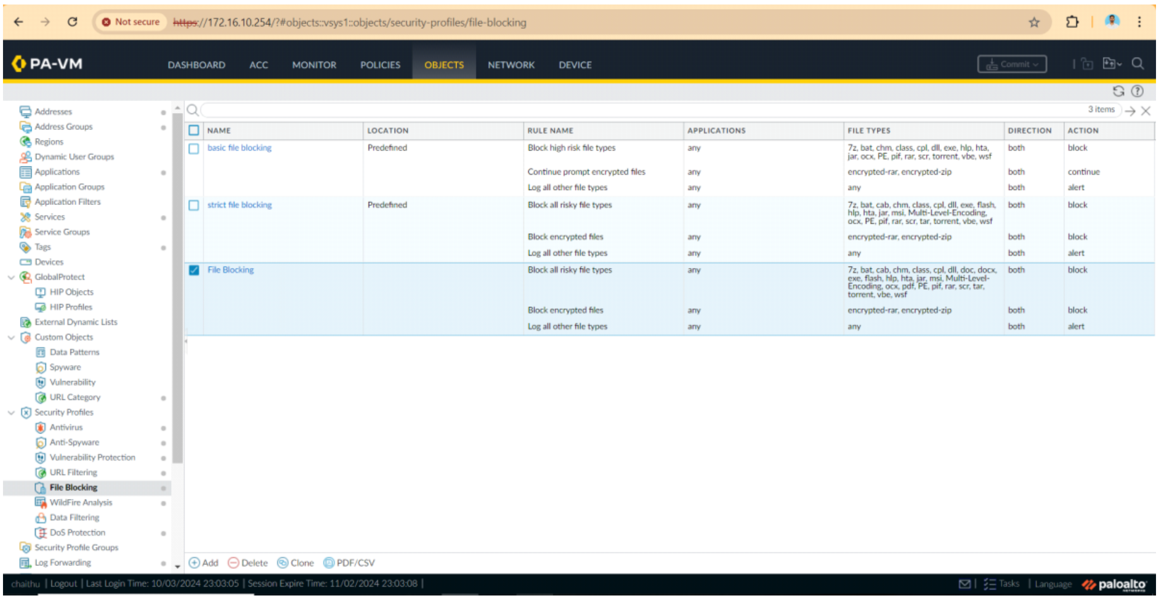
Details: Partial changes to commit: changes to configuration by all administrators
Changes to policy and objects configuration
Configuration committed successfully

Commit | Rule Shadow

Close

NAME	FILE TYPES	DIRECTION	ACTION
basic file blocking	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	continue
	any	both	alert
strict file blocking	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	block
	any	both	alert
File Blocking	7z, bat, cab, chm, class, cpl, dll, doc, docx, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, pdf, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
	encrypted-rar, encrypted-zip	both	block
	any	both	alert

chaithu | Logout | Last Login Time: 10/03/2024 12:36:49 | Session Expire Time: 11/02/2024 12:36:52 |



	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, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
			Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
			Log all other file types	any	any	both	alert
☑	File Blocking		Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, doc, docx, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, pdf, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
			Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
			Log all other file types	any	any	both	alert

B. DoS Protection Security Profile Configuration

Step 1: Navigate to DoS Protection Profiles

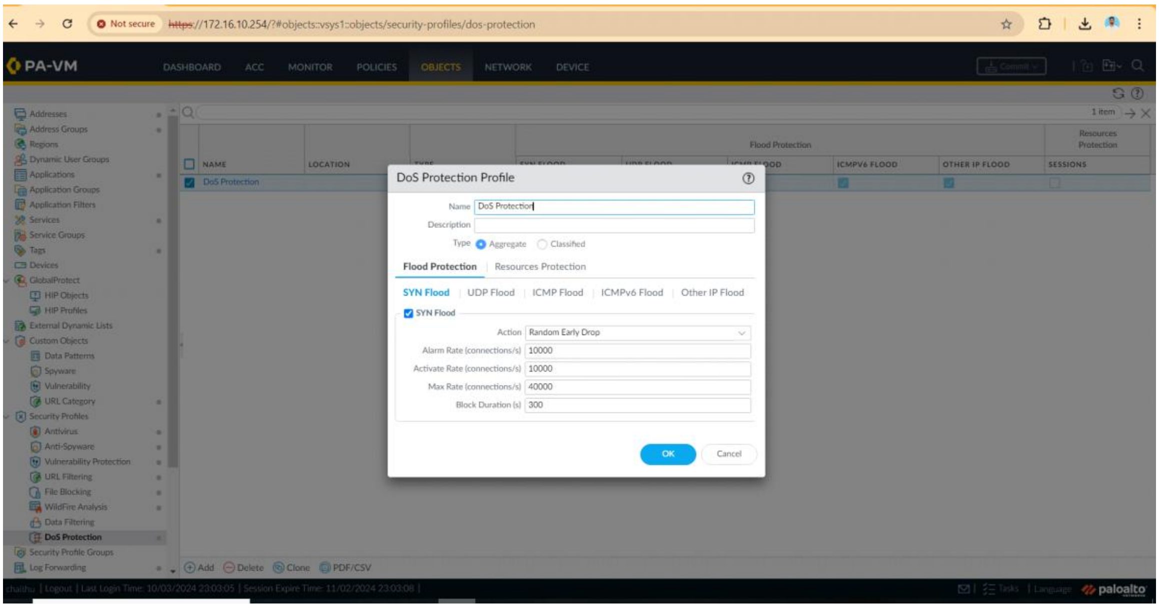
- Go to **Objects > Security Profiles > DoS Protection**.

Step 2: Create a New DoS Protection Profile

- Click **Add** to create a new DoS protection profile.
- Name the profile (e.g., "DoS-Protection").

Step 3: Configure Flood Protection

- Under the **Flood Protection** section, enable protection against **SYN Flood**, **ICMP Flood**, or **UDP Flood**.
- Set the **Threshold** values based on the traffic load. For example, configure a SYN Flood with a rate of 1000 packets per second.
- Enable **Aggregate** or **Classified** protection based on your requirement.



DoS Protection Profile

Name: DoS Protection

Description:

Type: ● Aggregate ○ Classified

Flood Protection | Resources Protection

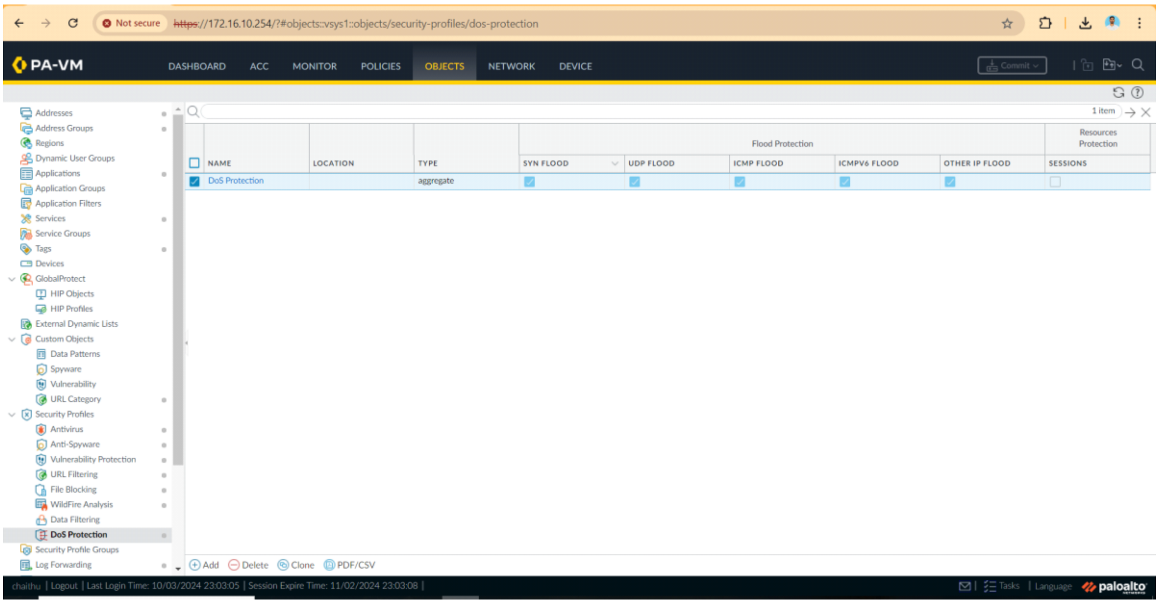
SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

☑ SYN Flood

Action	Random Early Drop
Alarm Rate (connections/s)	10000
Activate Rate (connections/s)	10000
Max Rate (connections/s)	40000
Block Duration (s)	300

Step 4: Apply DoS Protection to a Security Policy

- Go to **Policies > DoS Protection**.
- Create a new DoS policy and apply the created DoS profile to protect specific zones or IP ranges.



https://172.16.10.254/?#objects::vsys1::objects/security-profiles/dos-protection

			Flood Protection					Resources Protection
NAME	LOCATION	TYPE	SYN FLOOD	UDP FLOOD	ICMP FLOOD	ICMPV6 FLOOD	OTHER IP FLOOD	SESSIONS
DoS Protection		aggregate	☑	☑	☑	☑	☑	□

2. Packet Capture of Dropped Rule

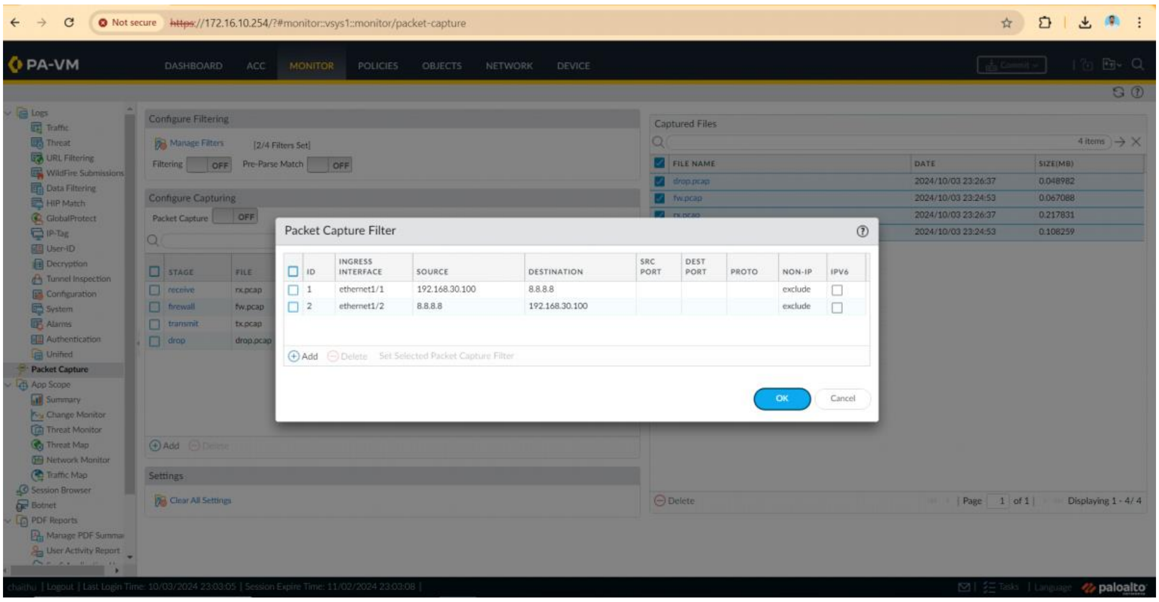
Step-by-Step Packet Capture of Dropped Traffic

Step 1: Navigate to Packet Capture Settings

- Go to **Monitor > Packet Capture** on the web interface.

Step 2: Create a Packet Capture Filter

- Click **Add** to create a new packet capture filter.
- Under **Match**, specify the conditions for the packet you want to capture (e.g., source IP, destination IP, application, or port).
- For a dropped packet rule, you can match the IP address or port of the traffic being dropped.



https://172.16.10.254/?#monitor::vsys1::monitor/packet-capture

Configure Filtering: Manage Filters [2/4 Filters Set] Filtering OFF Pre-Parse Match OFF

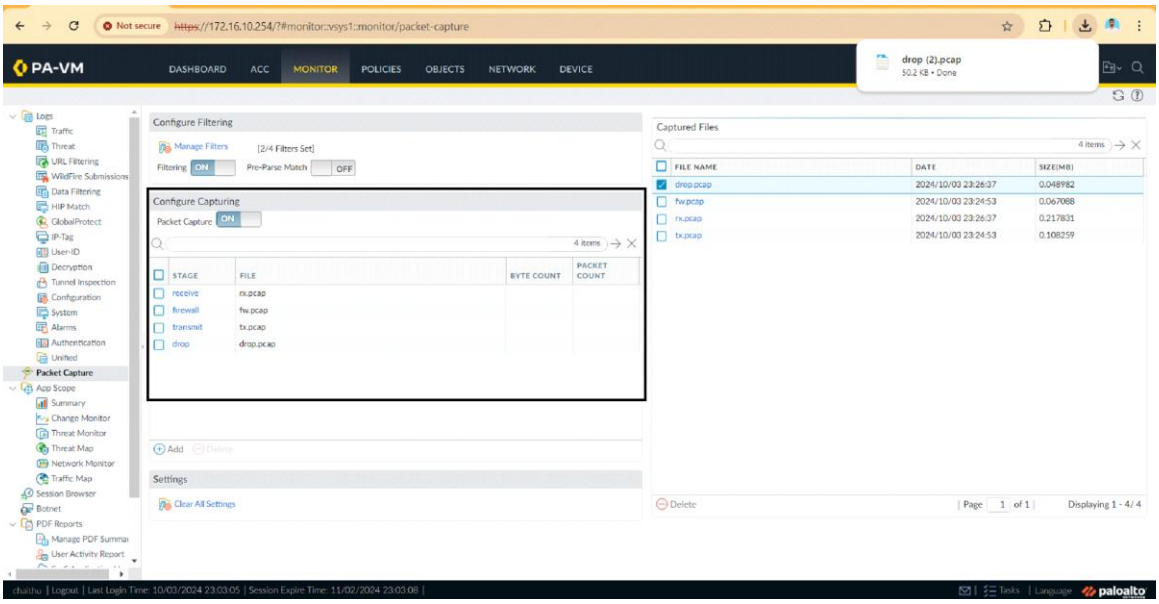
Configure Capturing: Packet Capture OFF

Packet Capture Filter

☐	ID	INGRESS INTERFACE	SOURCE	DESTINATION	SRC PORT	DEST PORT	PROTO	NON-IP	IPV6
☐	1	ethernet1/1	192.168.30.100	8.8.8.8				exclude	☐
☐	2	ethernet1/2	8.8.8.8	192.168.30.100				exclude	☐

Step 3: Define Stages to Capture

- Choose the capture stages: **Firewall stage**, **Receive**, **Transmit**, and **Drop**. For dropped traffic, select **Drop**.



https://172.16.10.254/?#monitor::vsys1::monitor/packet-capture

drop (2).pcap 50.2 KB • Done

Configure Filtering: Manage Filters [2/4 Filters Set] Filtering ON Pre-Parse Match OFF

Configure Capturing: Packet Capture ON

☐	STAGE	FILE	BYTE COUNT	PACKET COUNT
☐	receive	rx.pcap		
☐	firewall	fw.pcap		
☐	transmit	tx.pcap		
☐	drop	drop.pcap		

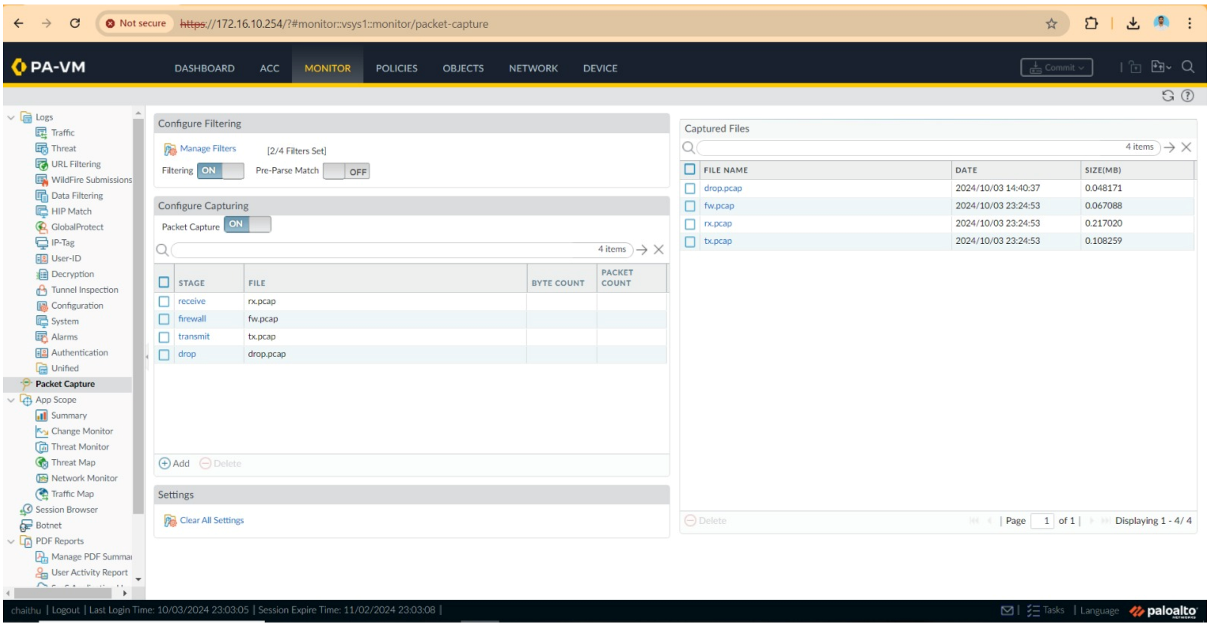
Captured Files

☐	FILE NAME	DATE	SIZE(MB)
☑	drop.pcap	2024/10/03 23:26:37	0.048982
☐	fw.pcap	2024/10/03 23:24:53	0.067088
☐	rx.pcap	2024/10/03 23:26:37	0.217831
☐	tx.pcap	2024/10/03 23:24:53	0.108259

Step 4: Enable Packet Capture

- Enable the packet capture by selecting the **Enable** checkbox.

- Click **OK** to save the configuration.



https://172.16.10.254/?#monitor::vsys1::monitor/packet-capture

Configure Filtering

Manage Filters [2/4 Filters Set]

Filtering ON Pre-Parse Match OFF

Configure Capturing

Packet Capture ON

4 items

□	STAGE	FILE	BYTE COUNT	PACKET COUNT
□	receive	rx.pcap		
□	firewall	fw.pcap		
□	transmit	tx.pcap		
□	drop	drop.pcap		

Captured Files

4 items

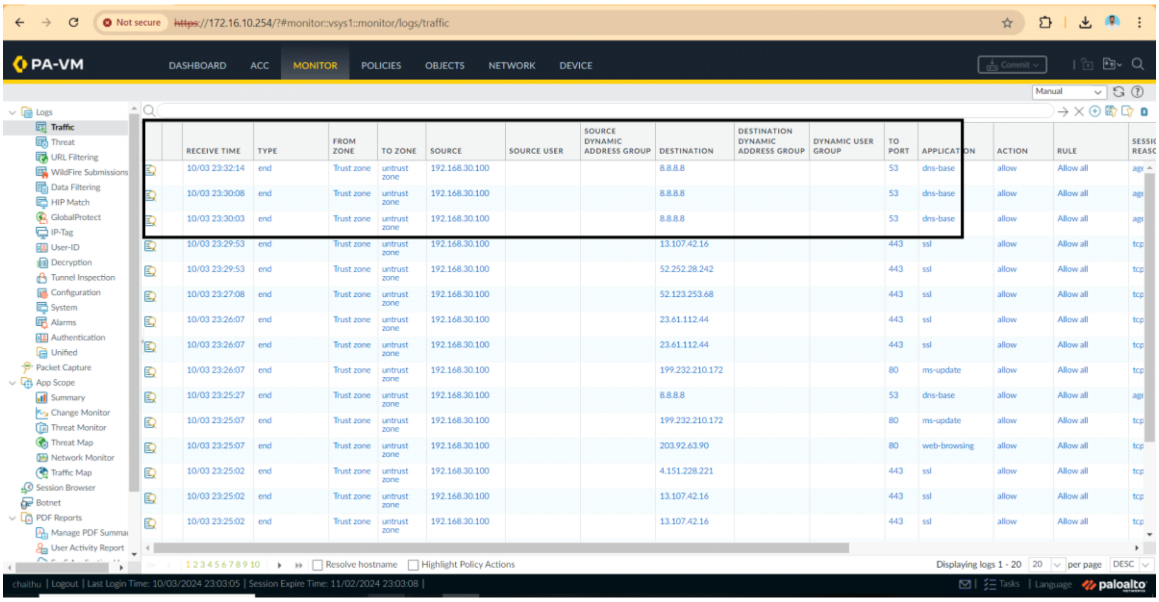
□	FILE NAME	DATE	SIZE(MB)
□	drop.pcap	2024/10/03 14:40:37	0.048171
□	fw.pcap	2024/10/03 23:24:53	0.067088
□	rx.pcap	2024/10/03 23:24:53	0.217020
□	tx.pcap	2024/10/03 23:24:53	0.108259

Page 1 of 1 Displaying 1 - 4 / 4

chaithu | Logout | Last Login Time: 10/03/2024 23:03:05 | Session Expire Time: 11/02/2024 23:03:08 |

Step 5: Generate Traffic

- Generate the traffic that will be dropped by the firewall according to the applied security rule (e.g., by accessing a blocked URL or application).



https://172.16.10.254/?#monitor::vsys1::monitor/logs/traffic

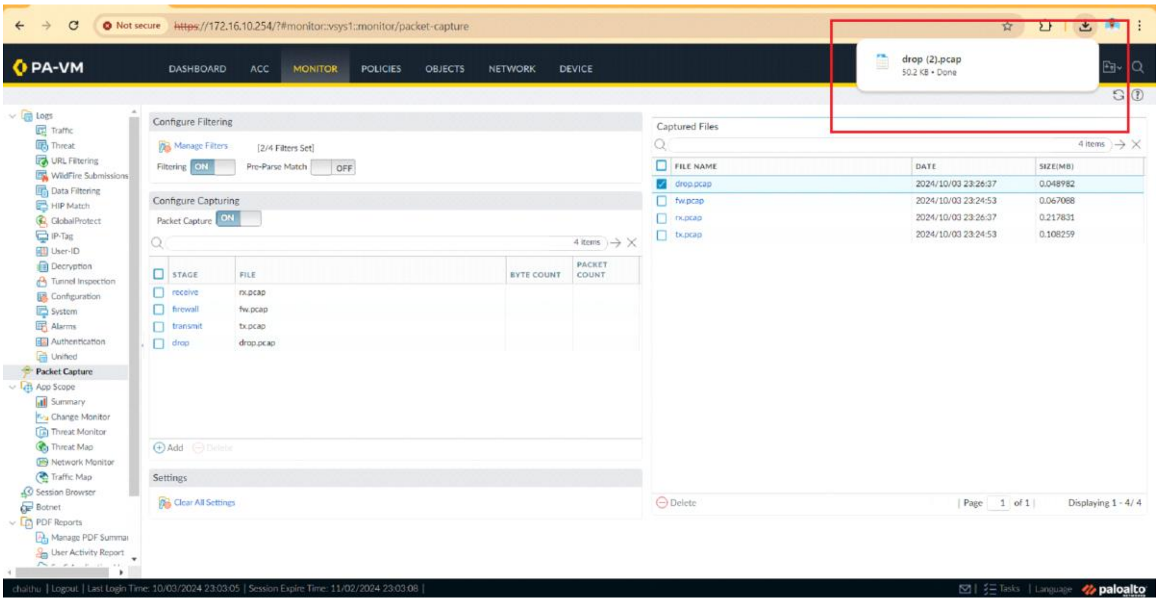
RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSI REASO
10/03 23:32:14	end	Trust zone	untrust zone	192.168.30.100			8.8.8.8			53	dns-base	allow	Allow all	age
10/03 23:30:08	end	Trust zone	untrust zone	192.168.30.100			8.8.8.8			53	dns-base	allow	Allow all	age
10/03 23:30:03	end	Trust zone	untrust zone	192.168.30.100			8.8.8.8			53	dns-base	allow	Allow all	age
10/03 23:29:53	end	Trust zone	untrust zone	192.168.30.100			13.107.42.16			443	ssl	allow	Allow all	tcp
10/03 23:29:53	end	Trust zone	untrust zone	192.168.30.100			52.252.28.242			443	ssl	allow	Allow all	tcp
10/03 23:27:08	end	Trust zone	untrust zone	192.168.30.100			52.123.253.68			443	ssl	allow	Allow all	tcp
10/03 23:26:07	end	Trust zone	untrust zone	192.168.30.100			23.61.112.44			443	ssl	allow	Allow all	tcp
10/03 23:26:07	end	Trust zone	untrust zone	192.168.30.100			23.61.112.44			443	ssl	allow	Allow all	tcp
10/03 23:26:07	end	Trust zone	untrust zone	192.168.30.100			199.232.210.172			80	ms-update	allow	Allow all	tcp
10/03 23:25:27	end	Trust zone	untrust zone	192.168.30.100			8.8.8.8			53	dns-base	allow	Allow all	age
10/03 23:25:07	end	Trust zone	untrust zone	192.168.30.100			199.232.210.172			80	ms-update	allow	Allow all	tcp
10/03 23:25:07	end	Trust zone	untrust zone	192.168.30.100			203.92.63.90			80	web-browsing	allow	Allow all	tcp
10/03 23:25:02	end	Trust zone	untrust zone	192.168.30.100			4.151.228.221			443	ssl	allow	Allow all	tcp
10/03 23:25:02	end	Trust zone	untrust zone	192.168.30.100			13.107.42.16			443	ssl	allow	Allow all	tcp
10/03 23:25:02	end	Trust zone	untrust zone	192.168.30.100			13.107.42.16			443	ssl	allow	Allow all	tcp

1 2 3 4 5 6 7 8 9 10 □ Resolve hostname □ Highlight Policy Actions Displaying logs 1 - 20 20 per page DESC

chaithu | Logout | Last Login Time: 10/03/2024 23:03:05 | Session Expire Time: 11/02/2024 23:03:08 |

Step 6: View and Download Packet Capture

- Once the traffic is generated and captured, go to **Monitor > Packet Capture**.
- Download the .pcap file for further analysis in tools like Wireshark.



Configure Filtering

Manage Filters [2/4 Filters Set]

Filtering ON   Pre-Parse Match OFF

Configure Capturing

Packet Capture ON

4 items

□	STAGE	FILE	BYTE COUNT	PACKET COUNT
□	receive	rx.pcap		
□	firewall	fw.pcap		
□	transmit	tx.pcap		
□	drop	drop.pcap		

Settings

Captured Files

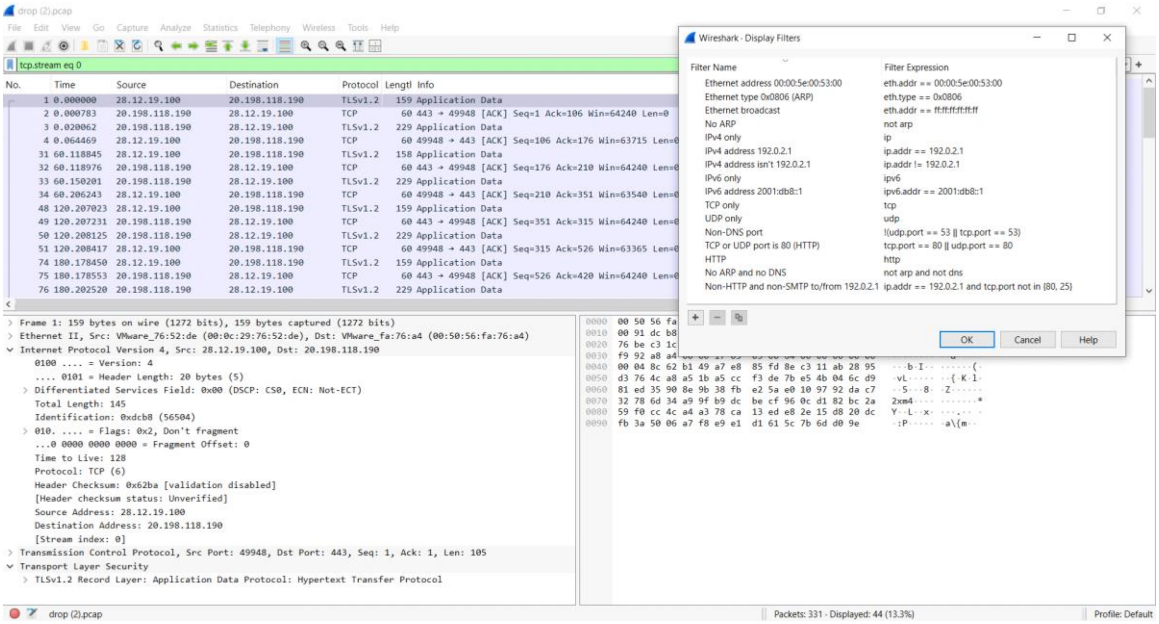
4 items

□	FILE NAME	DATE	SIZE(MB)
☑	drop.pcap	2024/10/03 23:26:37	0.048982
□	fw.pcap	2024/10/03 23:24:53	0.067088
□	rx.pcap	2024/10/03 23:26:37	0.217831
□	tx.pcap	2024/10/03 23:24:53	0.108259

chaithu | Logout | Last Login Time: 10/03/2024 23:03:05 | Session Expire Time: 11/02/2024 23:03:08 |

Step 7: Analyze the .pcap File

- Open the downloaded .pcap file in Wireshark.
- Look for packets that match the dropped rule criteria, such as TCP resets or dropped connections.



tcp.stream eq 0

```
No.   Time        Source          Destination     Protocol Lengtl Info
    1 0.000000    28.12.19.100    20.198.118.190  TLSv1.2  159 Application Data
    2 0.000783    20.198.118.190  28.12.19.100    TCP       60 443 → 49948 [ACK] Seq=1 Ack=106 Win=64240 Len=0
    3 0.020062    20.198.118.190  28.12.19.100    TLSv1.2  229 Application Data
    4 0.064469    28.12.19.100    20.198.118.190  TCP       60 49948 → 443 [ACK] Seq=106 Ack=176 Win=63715 Len=0
   31 60.118845   28.12.19.100    20.198.118.190  TLSv1.2  158 Application Data
   32 60.118976   20.198.118.190  28.12.19.100    TCP       60 443 → 49948 [ACK] Seq=176 Ack=210 Win=64240 Len=0
   33 60.150201   20.198.118.190  28.12.19.100    TLSv1.2  229 Application Data
   34 60.206243   28.12.19.100    20.198.118.190  TCP       60 49948 → 443 [ACK] Seq=210 Ack=351 Win=63540 Len=0
   48 120.207023  28.12.19.100    20.198.118.190  TLSv1.2  159 Application Data
   49 120.207231  20.198.118.190  28.12.19.100    TCP       60 443 → 49948 [ACK] Seq=351 Ack=315 Win=64240 Len=0
   50 120.208125  20.198.118.190  28.12.19.100    TLSv1.2  229 Application Data
   51 120.208417  28.12.19.100    20.198.118.190  TCP       60 49948 → 443 [ACK] Seq=315 Ack=526 Win=63365 Len=0
   74 180.178450  28.12.19.100    20.198.118.190  TLSv1.2  159 Application Data
   75 180.178553  20.198.118.190  28.12.19.100    TCP       60 443 → 49948 [ACK] Seq=526 Ack=420 Win=64240 Len=0
   76 180.202520  20.198.118.190  28.12.19.100    TLSv1.2  229 Application Data
```

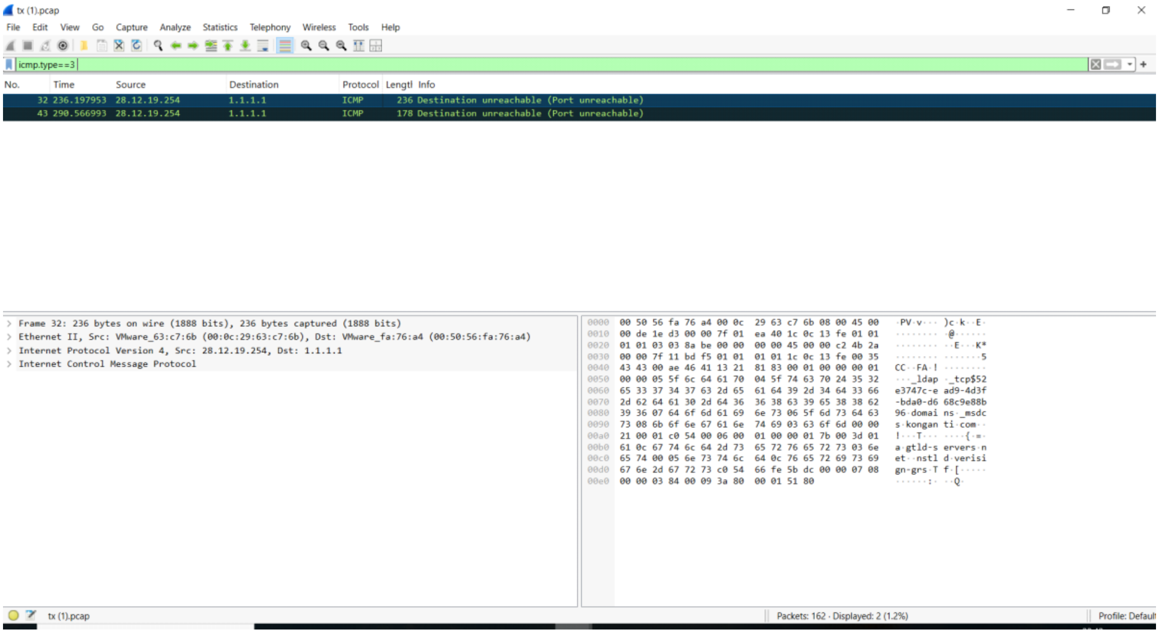
```
> Frame 1: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> Ethernet II, Src: VMware_76:52:de (00:0c:29:76:52:de), Dst: VMware_fa:76:a4 (00:50:56:fa:76:a4)
v Internet Protocol Version 4, Src: 28.12.19.100, Dst: 20.198.118.190
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 145
    Identification: 0xdcb8 (56504)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x62ba [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 28.12.19.100
    Destination Address: 20.198.118.190
    [Stream index: 0]
> Transmission Control Protocol, Src Port: 49948, Dst Port: 443, Seq: 1, Ack: 1, Len: 105
v Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
```

```
0000  00 50 56 fa
0010  00 91 dc b8
0020  76 be c3 1c
0030  f9 92 a8 a4
0040  00 04 8c 62 b1 49 a7 e8  85 fd 8e c3 11 ab 28 95   ···b·I·· ······(·
0050  d3 76 4c a8 a5 1b a5 cc  f3 de 7b e5 4b 04 6c d9   ·vL····· ··{·K·l·
0060  81 ed 35 90 8e 9b 38 fb  e2 5a e0 10 97 92 da c7   ··5···8· ·Z······
0070  32 78 6d 34 a9 9f b9 dc  be cf 96 0c d1 82 bc 2a   2xm4···· ·······*
0080  59 f0 cc 4c a4 a3 78 ca  13 ed e8 2e 15 d8 20 dc   Y··L··x· ···.·· ·
0090  fb 3a 50 06 a7 f8 e9 e1  d1 61 5c 7b 6d d0 9e      ·:P····· ·a\{m··
```

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}

drop (2).pcap | Packets: 331 · Displayed: 44 (13.3%) | Profile: Default

ICMP unreachable messages: icmp.type==3



icmp.type==3

```
No.   Time        Source          Destination   Protocol  Lengtl  Info
   32 236.197953  28.12.19.254    1.1.1.1       ICMP         236  Destination unreachable (Port unreachable)
   43 290.566993  28.12.19.254    1.1.1.1       ICMP         178  Destination unreachable (Port unreachable)
```

```
> Frame 32: 236 bytes on wire (1888 bits), 236 bytes captured (1888 bits)
> Ethernet II, Src: VMware_63:c7:6b (00:0c:29:63:c7:6b), Dst: VMware_fa:76:a4 (00:50:56:fa:76:a4)
> Internet Protocol Version 4, Src: 28.12.19.254, Dst: 1.1.1.1
> Internet Control Message Protocol
```

```
0000  00 50 56 fa 76 a4 00 0c  29 63 c7 6b 08 00 45 00   ·PV·v··· )c·k··E·
0010  00 de 1e d3 00 00 7f 01  ea 40 1c 0c 13 fe 01 01   ········ ·@······
0020  01 01 03 03 8a be 00 00  00 00 45 00 00 c2 4b 2a   ········ ··E···K*
0030  00 00 7f 11 bd f5 01 01  01 01 1c 0c 13 fe 00 35   ········ ·······5
0040  43 43 00 ae 46 41 13 21  81 83 00 01 00 00 00 01   CC··FA·! ········
0050  00 00 05 5f 6c 64 61 70  04 5f 74 63 70 24 35 32   ···_ldap ·_tcp$52
0060  65 33 37 34 37 63 2d 65  61 64 39 2d 34 64 33 66   e3747c-e ad9-4d3f
0070  2d 62 64 61 30 2d 64 36  36 38 63 39 65 38 38 62   -bda0-d6 68c9e88b
0080  39 36 07 64 6f 6d 61 69  6e 73 06 5f 6d 73 64 63   96·domai ns·_msdc
0090  73 08 6b 6f 6e 67 61 6e  74 69 03 63 6f 6d 00 00   s·kongan ti·com··
00a0  21 00 01 c0 54 00 06 00  01 00 00 01 7b 00 3d 01   !···T··· ····{·=·
00b0  61 0c 67 74 6c 64 2d 73  65 72 76 65 72 73 03 6e   a·gtld-s ervers·n
00c0  65 74 00 05 6e 73 74 6c  64 0c 76 65 72 69 73 69   et··nstl d·verisi
00d0  67 6e 2d 67 72 73 c0 54  66 fe 5b dc 00 00 07 08   gn-grs·T f·[·····
00e0  00 00 03 84 00 09 3a 80  00 01 51 80               ······:· ··Q·
```

After applying the filters, observe packets that match the drop criteria, such as:

- **TCP resets** (indicating the firewall reset the connection).
- **ICMP unreachable** messages (indicating a service is unreachable due to a firewall block).
- Look for additional clues like **zero-window** packets (indicating a buffer overflow or service refusal).

Analyze the packet details, focusing on the **Source IP**, **Destination IP**, **Port**, and other relevant protocol information to verify which rule caused the drop.

Over All Conclusion:

- we configured Palo Alto firewall security profiles for File Blocking and DoS Protection, ensuring that specific file types are blocked and network flood attacks are mitigated. The packet capture showed dropped traffic based on security policies, confirmed through Wireshark analysis with TCP resets, indicating effective traffic blocking. This demonstrates the firewall's capability to enforce network security policies and protect against unauthorized or malicious traffic

Thank You