



Project 4: FortiGate Security Profiles

ONL3_ISS8_S2

Group 1:

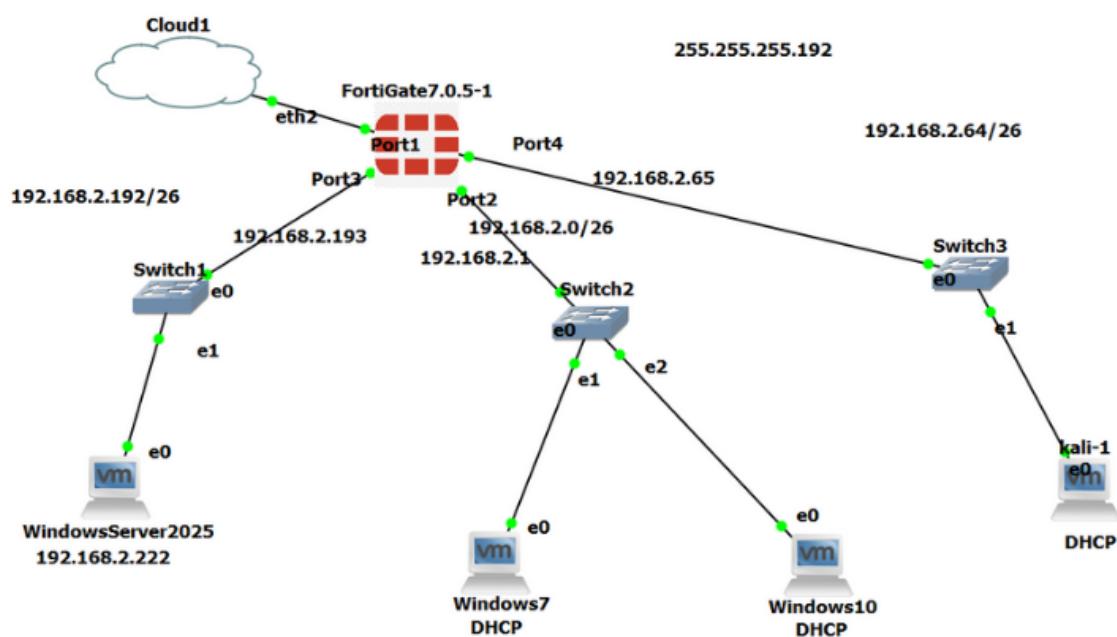
Mohannad Mohie 21043873
Muhammed Saeed 21045047
Yousef Mohamed 21007865
Akram Khaled 21037388
Mazen Mohamed 21052008

Table Of Contents

- | **01 Topology**
- | **02 FortiGate Policies**
- | **03 Web Filtering**
- | **04 Application Control**
- | **05 Anti-Virus**
- | **06 Conclusion**

1

Topology



Name	Subnet	Description
LAN-1	192.168.2.0/26	It's a LAN that has two devices; Windows 7 and Windows 10.
LAN-2	192.168.2.64/26	It's a LAN that has one device; Kali-Linux.
DMZ-WEB	192.168.2.192/26	It's a DMZ that has Windows Server which will host a website and acts like the DNS for the whole topology

LAN-1 is connected to the FortiGate using port 2, LAN-2 is connected using port 4, DMZ-WEB is connected using port 3, and lastly, our FortiGate is connecting to the internet using port 1.

	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch		PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface 4							
DMZ-WEB (port3)	Physical Interface			192.168.2.193/255.255.255.192	PING HTTPS SSH HTTP		
LAN-1 (port2)	Physical Interface			192.168.2.1/255.255.255.192	PING HTTPS HTTP	3	192.168.2.2-192.168.2.62
LAN-2 (port4)	Physical Interface			192.168.2.65/255.255.255.192	PING HTTPS SSH HTTP	1	192.168.2.66-192.168.2.126
port1	Physical Interface			192.168.1.5/255.255.255.0	PING HTTPS SSH HTTP FMG-Access		

Here we gave the first IP address in the subnet to each port. We made port2 and port4 work as DHCP to their LAN.

DHCP Server

DHCP status Enabled Disabled

Address range

Netmask

Default gateway Same as Interface IP Specify

DNS server Specify

DNS server 1

Lease time second(s)

We specified the DNS server to be the Windows Server which has a forwarding route to the internet using Google's DNS server: 8.8.8.8

This is a **test page** for our FortiGate project. It is used only to verify connectivity and deployment during our final presentation.

TEAM MEMBERS

Mohannad Mohie	Muhammed Saeed
Akram Khaled	Yousef Abdel-atty
Mazen Mohamed	

FortiGate Project - DEPI Cybersecurity Program

We made a test website page for our project and hosted it on the Windows Server and gave it a domain: `depi.team` which will later be accessed by all devices using the DNS server.

Device Inventory

Hardware Vendor	Software OS	Status	Interfaces
VMware	Windows Ubuntu	3 Devices	LAN-1 (port2) LAN-2 (port4)

Device	User	Address	Software OS	Device Family	Hardware Version	Endpoint Tags
kali		192.168.2.66 00:ec:29:0f:fd:6d	Ubuntu			
WIN-HEDD8RLH058		192.168.2.4 00:ec:29:59:4f:a3	Windows			
DESKTOP-P51NT4J		192.168.2.3 00:ec:29:e3:9c:5b	Windows			

We can see here, our three virtual machines took with their IP addresses that they took through the FortiGate's ports DHCP.

2

FortiGate Policies

Policy & Objects		Name	Details	Interface
Firewall Policy				
IPv4 DoS Policy				
Addresses	★	IP Range/Subnet 8		
Internet Service		DMZ-WEB	192.168.2.192/26	DMZ-WEB (port)
Database		FABRIC_DEVICE	0.0.0.0/0	
Services		FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0	
Schedules		LAN-1	192.168.2.0/26	LAN-1 (port2)
Virtual IPs		LAN2	192.168.2.64/26	LAN-2 (port4)
IP Pools		SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	
		all	0.0.0.0/0	
		none	0.0.0.0/32	

We created 3 addresses, one for each LAN and DMZ and assigned them to their interfaces, to use them later in policies.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
DMZ-WEB (port3) → port1 ①								
DMZ-WAN	DMZ-WEB	all	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection	UTM
LAN-1 (port2) → DMZ-WEB (port3) ①								
LAN1-DMZ	LAN-1	DMZ-WEB	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection	UTM
LAN-1 (port2) → port1 ①								
LAN1-WAN	LAN-1	all	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection	UTM
LAN-2 (port4) → DMZ-WEB (port3) ①								
LAN2-DMZ	LAN2	DMZ-WEB	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection	UTM
LAN-2 (port4) → port1 ①								
LAN2-WAN	LAN2	all	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection	UTM
+ Implicit ①								

We have created 5 firewall policies:

- 1) **DMZ-WAN** → This one is made to let our DMZ (Windows Server) access the internet to let it forward the DNS requests to 8.8.8.8 when needed.
- 2) **LAN1-DMZ** → This one is made to let LAN-1 access the Windows Server for DNS and depi.team website.

3) **LAN1-WAN** → This one is made to let LAN-1 access the internet.

4) **LAN2-DMZ** → This one is made to let LAN-2 access the Windows Server for DNS and depi.team website.

5) **LAN2-WAN** → This one is made to let LAN-2 access the internet.

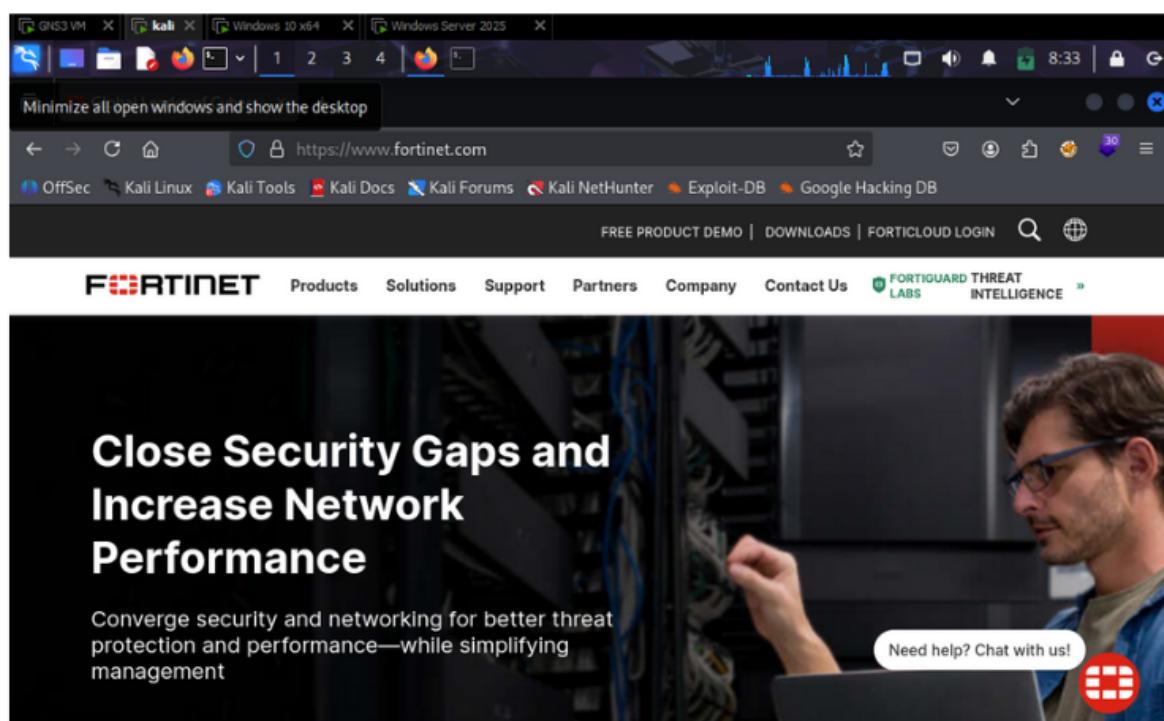
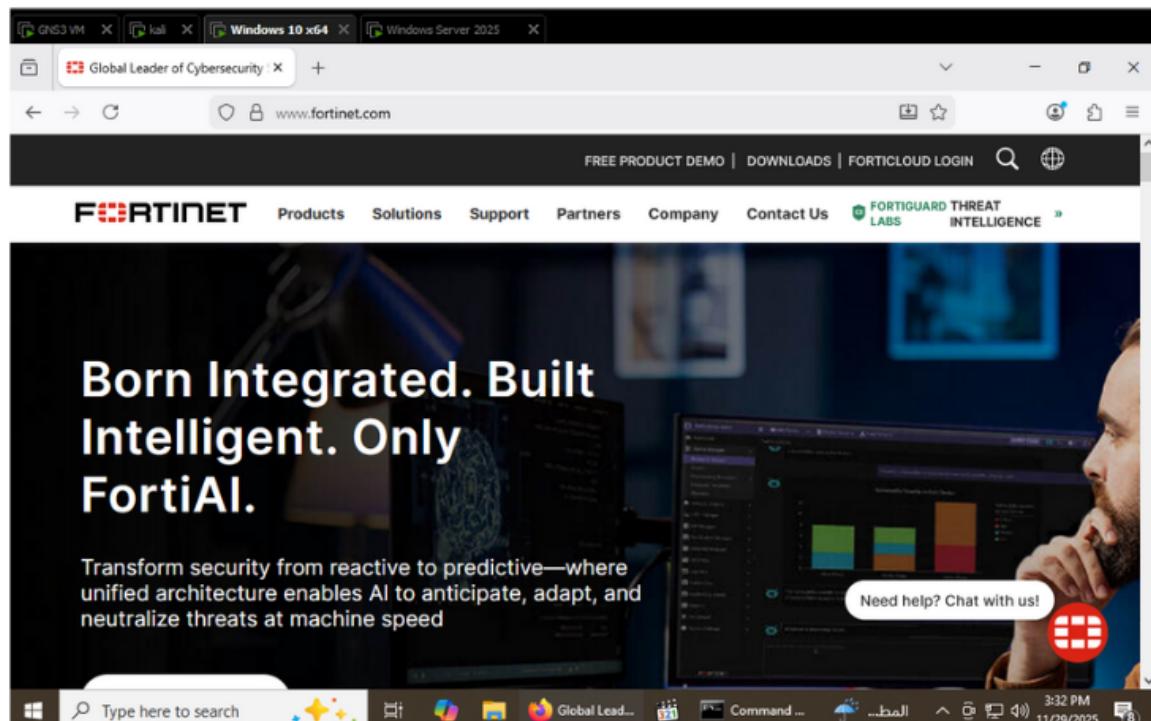
Notice that we didn't make a policy for LAN-1 and LAN-2 to access each other, so they won't access each other because they lay under the implicit deny policy.

The screenshot shows the configuration for a firewall policy named "LAN1-WAN". The policy details are as follows:

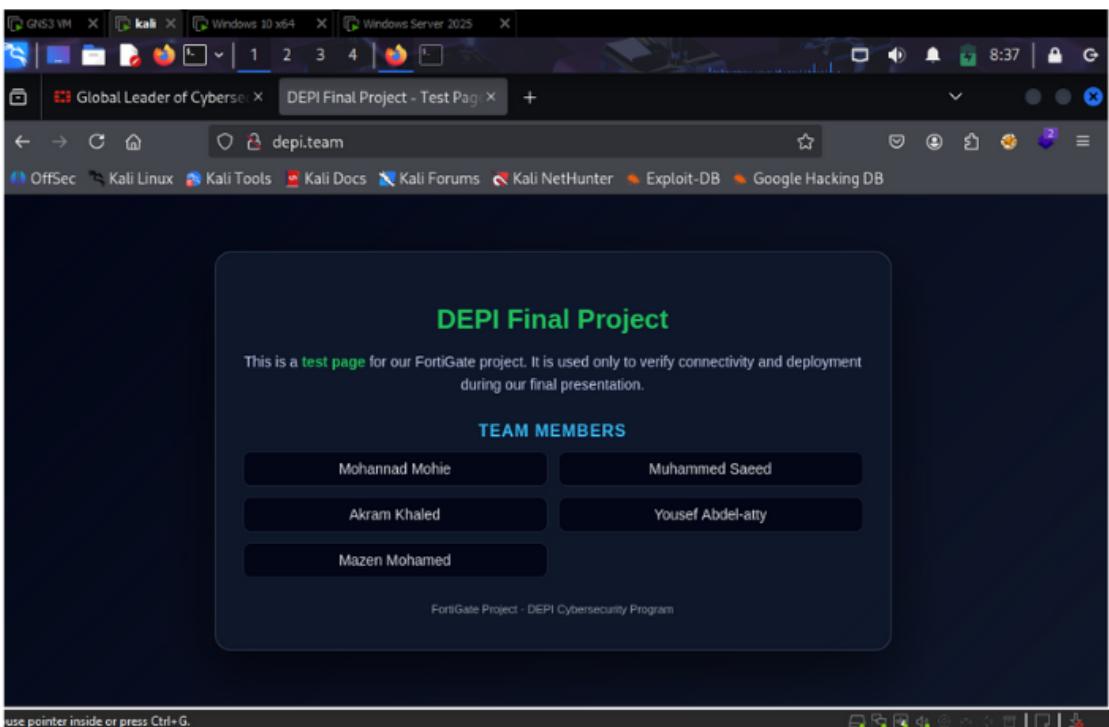
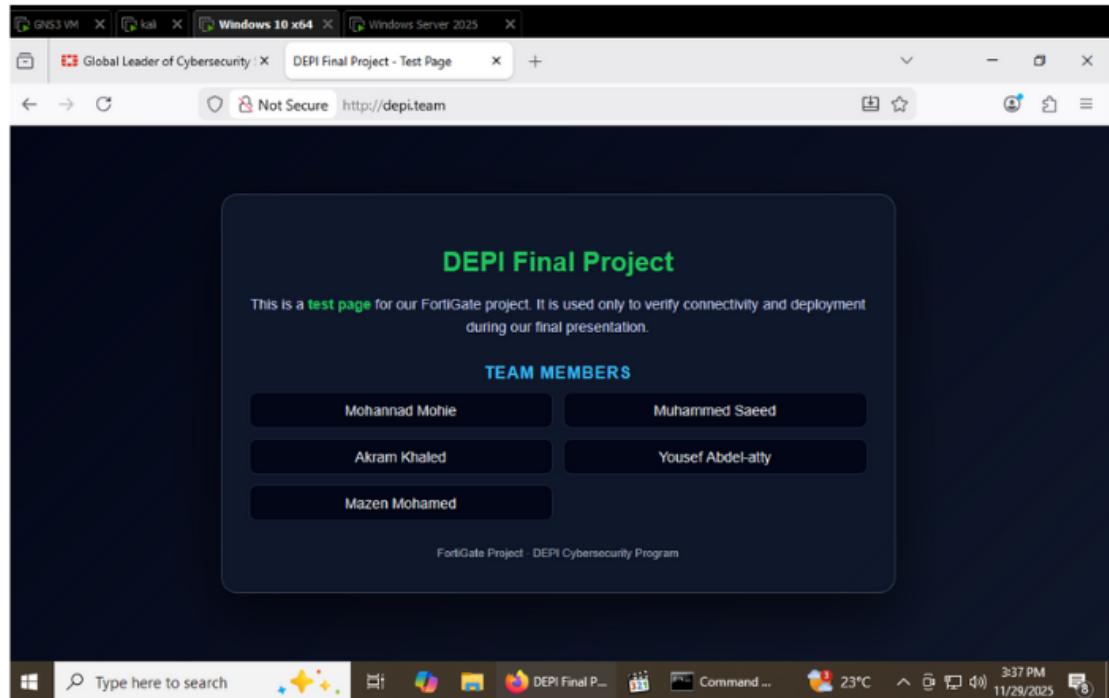
- Name:** LAN1-WAN
- Incoming Interface:** LAN-1 (port2)
- Outgoing Interface:** port1
- Source:** LAN-1
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)

Below the main configuration, there are tabs for "Inspection Mode" (Flow-based is selected) and "Firewall / Network Options". Under "Firewall / Network Options", the NAT setting is enabled, and the IP Pool Configuration section shows "Use Outgoing Interface Address" selected. There are also options for "Preserve Source Port" and "Protocol Options" (PROT default).

Here's an example of LAN1-WAN policy configuration.



To verify internet and DNS connectivity, here we can see that both Windows 10 (LAN-1) and Kali-Linux (LAN-2) can access the internet.



Also here to verify the connectivity between LAN 1 and LAN 2 to the DMZ, here they can access the depi.team website. We can now say that our firewall policies are working fine.

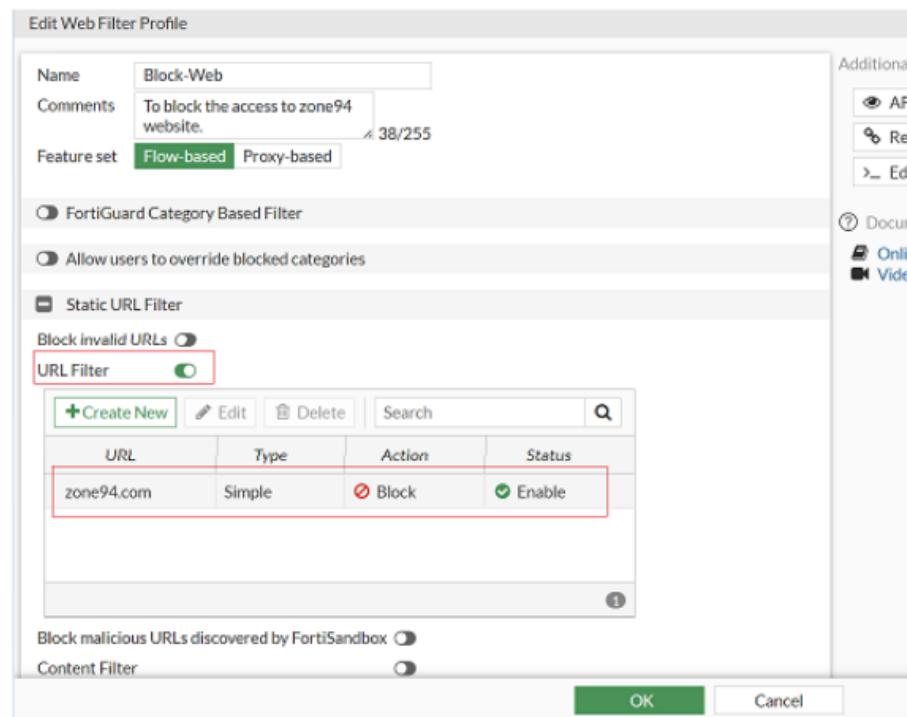
3

Web Filtering

Our goal in the web filtering is to block the access to depi.team website from LAN 1 and LAN 2 through the DMZ, and to also block the access to zone94.com website through the internet.

URL	Type	Action	Status
depi.team	Simple	Block	Enable

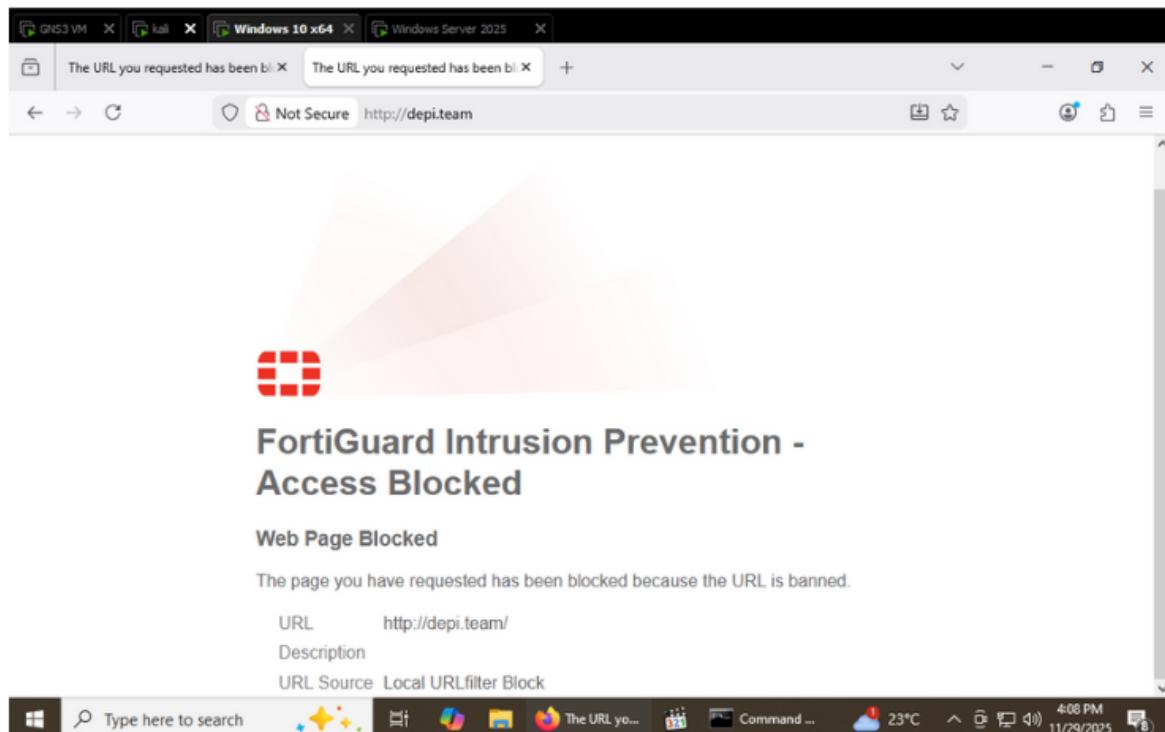
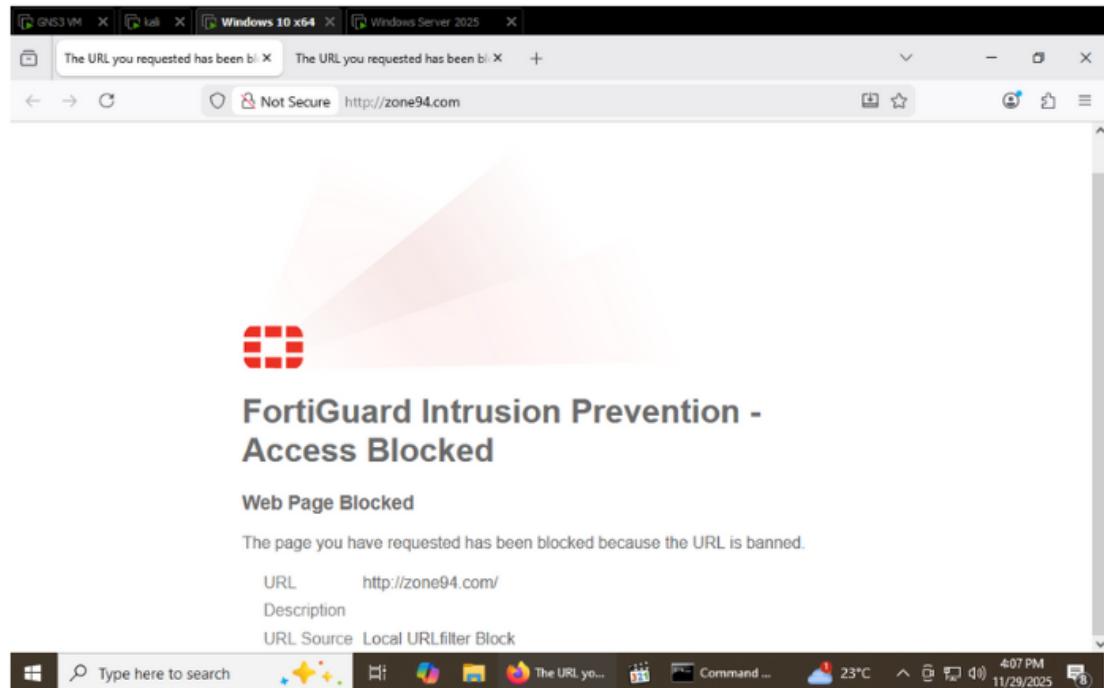
First, we created the **Block-DEPI** web filter profile and used **URL Filter** to block the access to the website. Then we applied the web profile to both **LAN1-DMZ** and **LAN2-DMZ** policies.



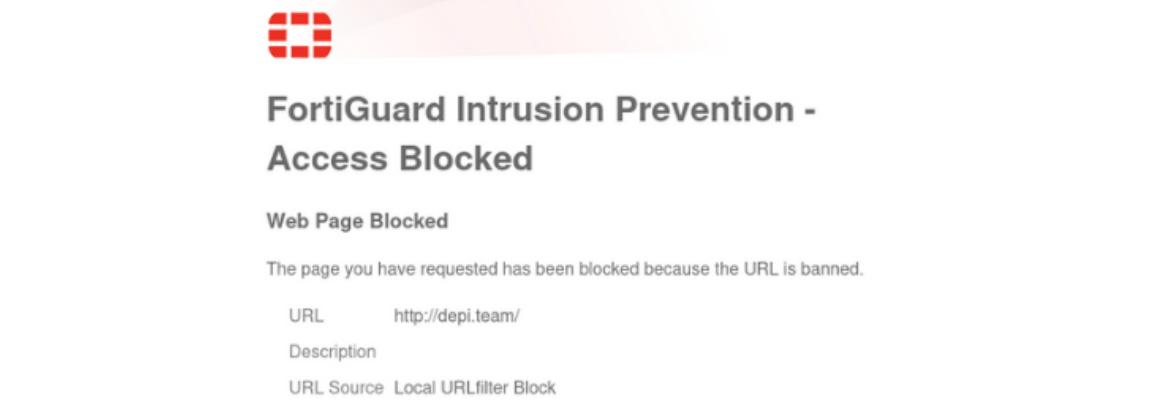
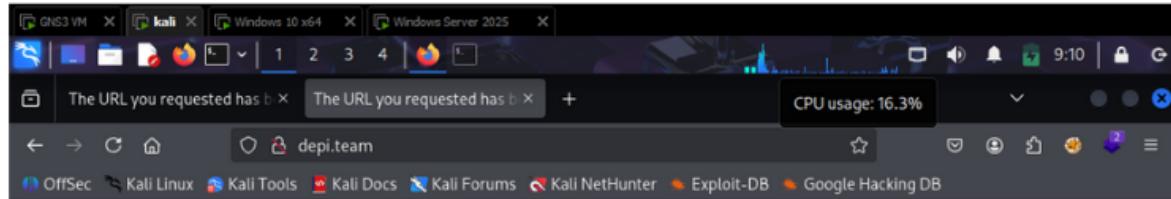
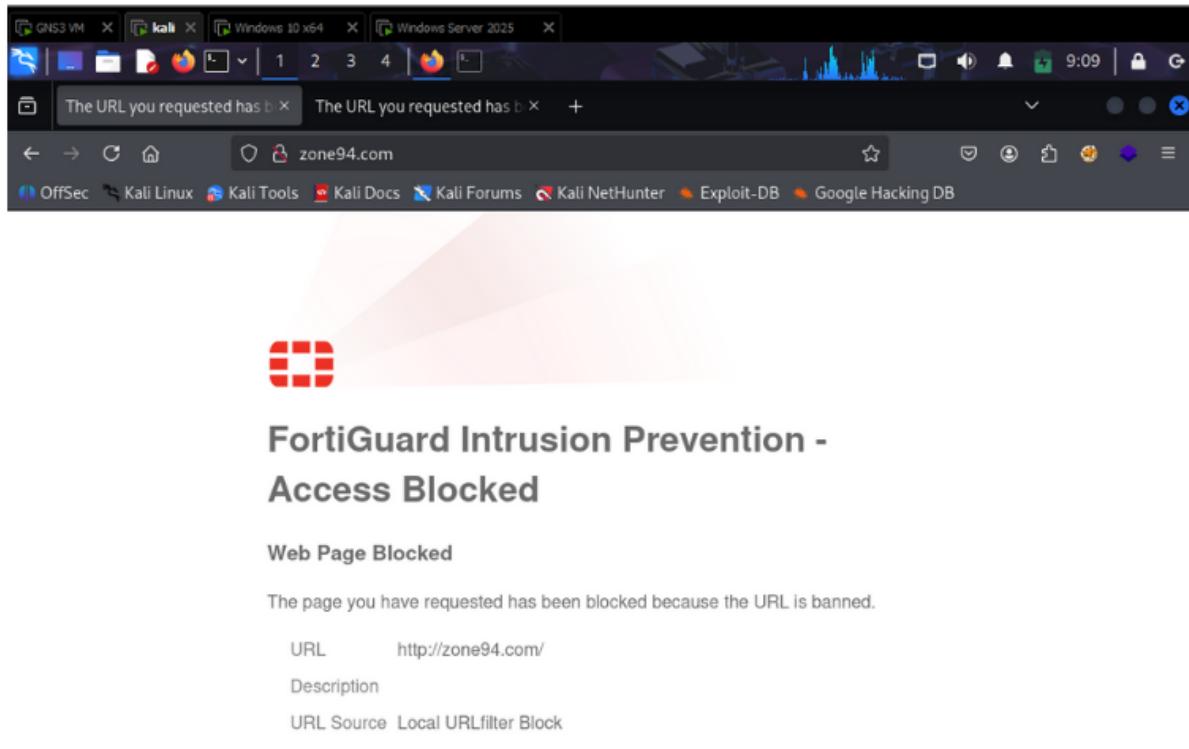
Then, we created the **Block-Web** web filter profile and used **URL Filter** to block the access to the website.
Then we applied the web profile to both **LAN1-WAN** and **LAN2-WAN** policies.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
DMZ-WEB (port3) → port1	DMZ-WAN	DMZ-WEB	all	always	ALL	ACCEPT	Enabled	certificate-inspection UTM
LAN-1 (port2) → DMZ-WEB (port3)	LAN-1	DMZ-WEB	all	always	ALL	ACCEPT	Enabled	Block-DEPI certificate-inspection UTM
LAN-1 (port2) → port1	LAN-1	all	always	ALL	ACCEPT	Enabled	Block-Web certificate-inspection UTM	
LAN-2 (port4) → DMZ-WEB (port3)	LAN2	DMZ-WEB	all	always	ALL	ACCEPT	Enabled	Block-DEPI certificate-inspection UTM
LAN-2 (port4) → port1	LAN2	all	always	ALL	ACCEPT	Enabled	Block-Web certificate-inspection UTM	
Implicit								

And here are the firewall policies after applying the web filter.



Here we can see that both web filter profiles work correctly on Windows 10 (LAN 1) and blocked the access to the websites.



Also here we can see that both web profiles are working correctly on the Kali Linux (LAN 2) and blocked the access.

The screenshot shows the FortiGate management interface. The left sidebar is a navigation tree with sections like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, Log & Report, Forward Traffic, Local Traffic, Sniffer Traffic, Events, AntiVirus, and Web Filter. The 'Web Filter' section is currently selected and highlighted in green. The main pane displays a table of logs. The columns are Date/Time, User, Source, Action, URL, Category Description, Initiator, and Sent / Received. There are 10 entries in the log, all from the source IP 192.168.2.3, all labeled 'blocked', and all pointing to URLs like 'http://zone94.com/favicon.ico' or 'http://depi.team/'. The last entry is 5 minutes ago.

Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
2 minutes ago		192.168.2.66	blocked	http://zone94.com/favicon.ico			343 B / 0 B
2 minutes ago		192.168.2.66	blocked	http://zone94.com/			330 B / 0 B
2 minutes ago		192.168.2.66	blocked	http://depi.team/			414 B / 0 B
5 minutes ago		192.168.2.3	blocked	http://depi.team/			432 B / 0 B
5 minutes ago		192.168.2.3	blocked	http://zone94.com/			1.16 kB / 0 B
5 minutes ago		192.168.2.3	blocked	http://depi.team/favicon.ico			371 B / 0 B
5 minutes ago		192.168.2.3	blocked	http://depi.team/			359 B / 0 B
5 minutes ago		192.168.2.3	blocked	http://zone94.com/			1.16 kB / 0 B

If we went to Log & Report then Web Filter, we can see that they got blocked and logged here so we can monitor it easily.

4

Application Control

Our goal in application control is to apply to LAN 1 only.

The screenshot shows the 'Edit Application Sensor' page. The 'Categories' section is highlighted with a red box. The categories listed are: Business (179), Collaboration (293), Game (124), Mobile (3), P2P (85), Remote Access (91), Storage Backup (296), Video/Audio (206), Web.Client (18), Cloud.IT (31), Email (87), General.Interest (241), Network.Service (332), Proxy (106), Social.Media (150), Update (48), and VoIP (31). The 'Unknown Applications' category is selected. The left sidebar shows the navigation menu with 'Application Control' selected.

We created the application sensor: **Our-APP-Control** and in categories we blocked: Games, P2P, Proxy, Social Media, and monitored the rest.

The screenshot shows the 'Edit Application Sensor' page. The 'Network Protocol Enforcement' section is highlighted with a red box. It lists the following rules:

Port	Enforce Protocols	Violation Action
Port 21	PROT FTP	Block
Port 80	PROT HTTP	Block
Port 443	PROT HTTPS	Block
Port 53	PROT DNS	Block
Port 110	PROT POP3	Block

The left sidebar shows the navigation menu with 'Application Control' selected.

Also we enabled the Network Protocol Enforcement and sat some protocol ports, to make sure any violation or trying to access the protocol using another port will be blocked.

The screenshot shows the 'Edit Application Sensor' configuration page. In the 'Application and Filter Overrides' section, there are two entries:

- Priority 1:** LinkedIn (LinkedIn_Apps, LinkedIn_File.Download, LinkedIn_File.Upload) - Type: Application, Action: Allow
- Priority 2:** BHVR_Excessive-Bandwidth - Type: Filter, Action: Block

Below this, under 'Options', the 'Block applications detected on non-default ports' toggle is turned on. Other options like 'Allow and Log DNS Traffic' and 'QUIC' are also visible.

We used Application and Filters Overrides to allow the access to LinkedIn instead of being blocked using the social media category.

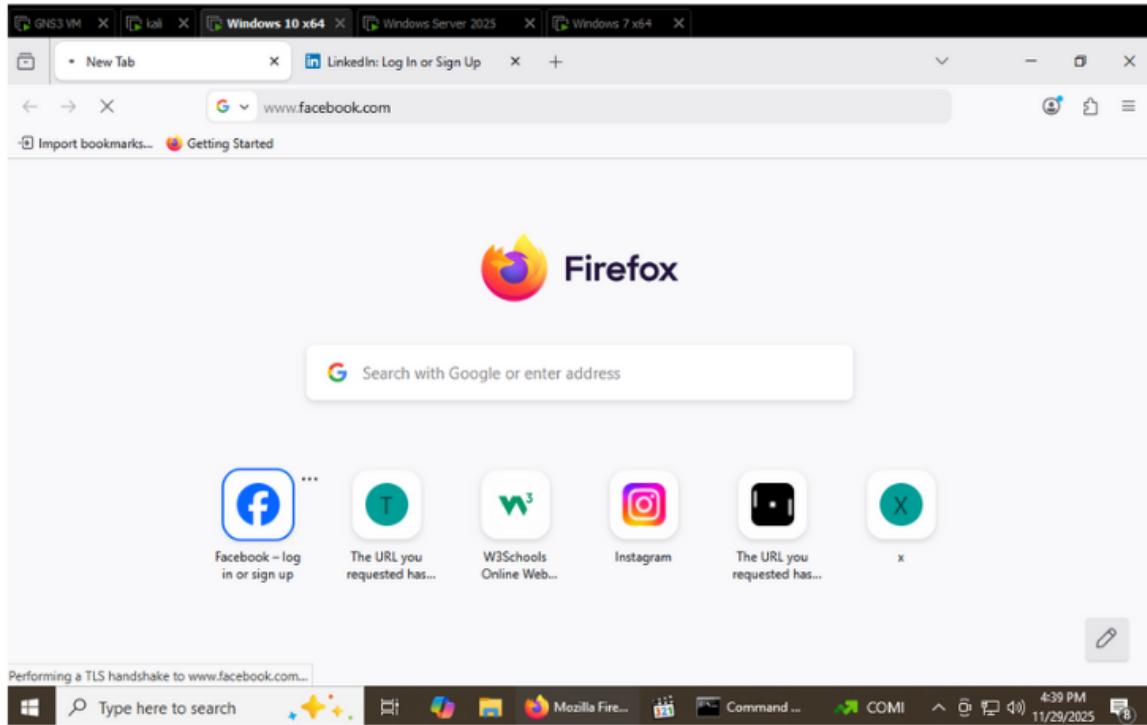
We blocked any traffic that uses excessive bandwidth.

We enabled Block applications detected on non-default ports.

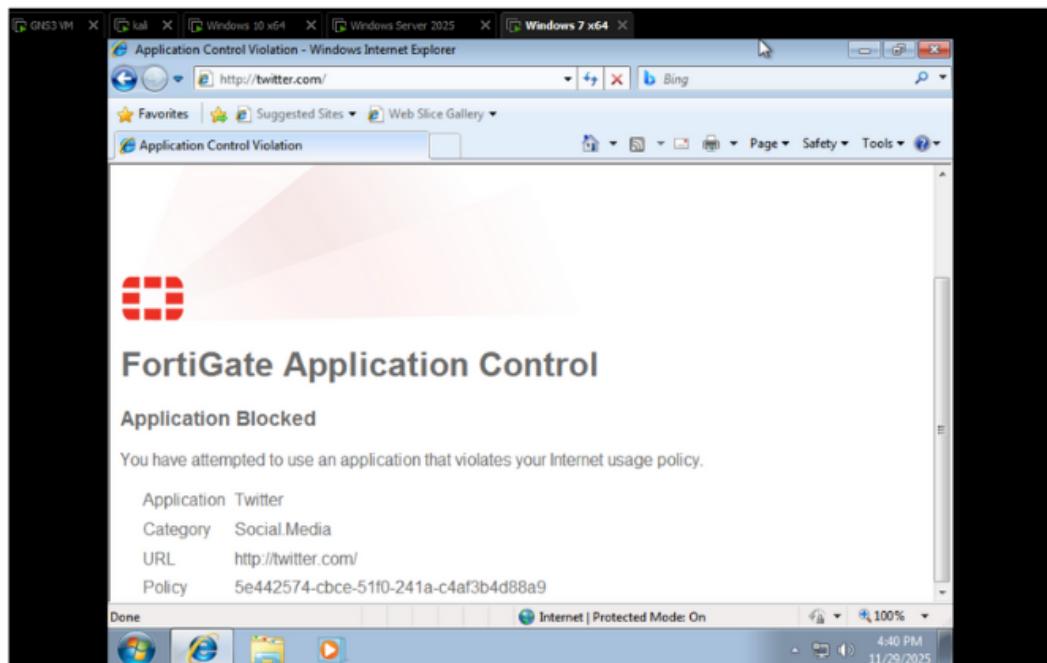
The screenshot shows the 'Firewall Policy' table with several entries:

- Row 1:** DMZ-WAN to DMZ-WEB (port3) - Action: ACCEPT, Enabled, SSL certificate-inspection, UTM
- Row 2:** LAN1-DMZ to DMZ-WEB (port3) - Action: ACCEPT, Enabled, WEB Block-DEPI, SSL certificate-inspection, UTM
- Row 3:** LAN1-WAN to DMZ-WEB (port3) - Action: ACCEPT, Enabled, WEB Block-Web, APP Our-APP-Control, SSL certificate-inspection, UTM
- Row 4:** LAN2-DMZ to DMZ-WEB (port3) - Action: ACCEPT, Enabled, WEB Block-DEPI, SSL certificate-inspection, UTM
- Row 5:** LAN2-WAN to DMZ-WEB (port3) - Action: ACCEPT, Enabled, WEB Block-Web, SSL certificate-inspection, UTM
- Row 6:** Implicit - (Default rule)

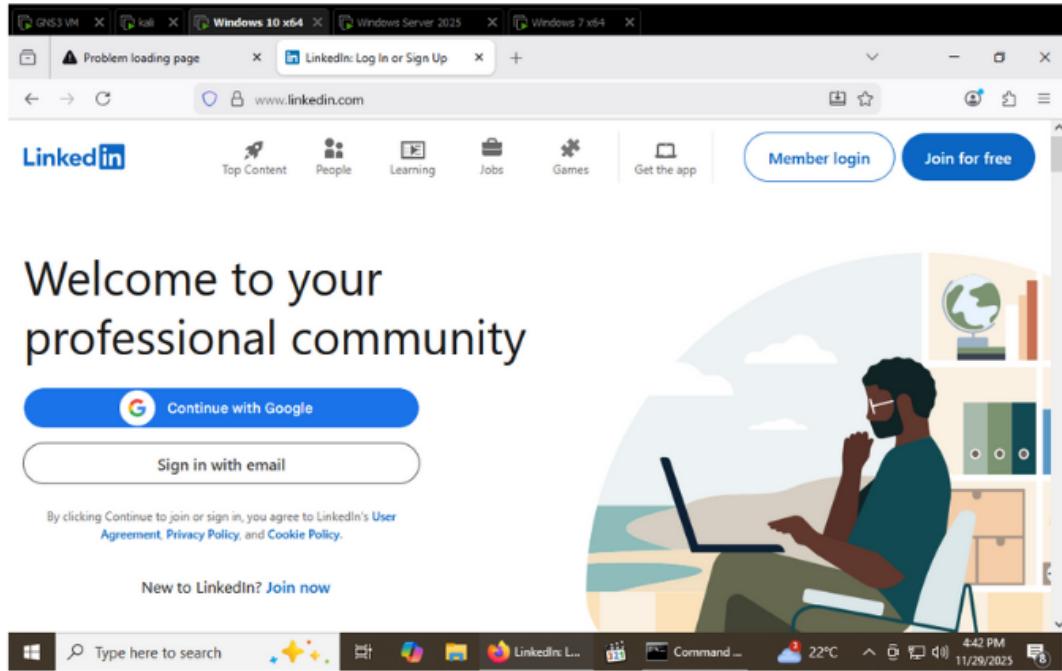
We applied the application control to the **LAN1-WAN** policy to apply it correctly on LAN 1 on its access to the internet.



From the Windows 10 device, if we tried to access Facebook, it will just keep loading like this with no reachability.



Also here from the Windows 7, if we tried to access Twitter, it will be blocked showing this message from application control.



But if we tried to access LinkedIn, it will work fine because we overrode the social media category by passing LinkedIn.

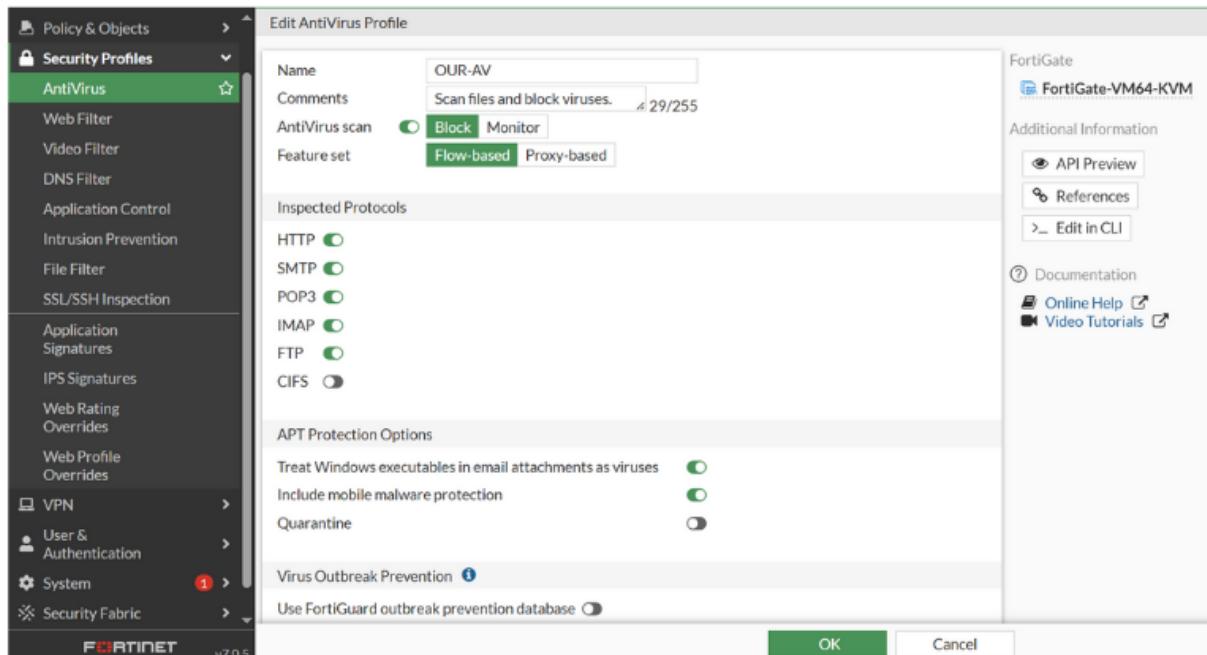
Policy & Objects		Date/Time	Source	Destination	Application Name	Action	Application User
Policy & Objects	>	Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	Microsoft.Portal	pass	
Security Profiles	>	Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	HTTPS.BROWSER	pass	
VPN	>	2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...	HTTPS.BROWSER	pass	
User & Authentication	>	2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...	SSL	pass	
System	1 >	2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...		block	
Security Fabric	>	2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)	HTTPS.BROWSER	pass	
Log & Report	>	2 minutes ago	192.168.2.3	74.125.133.84 (accounts.google.com)	Google.Accounts	pass	
Forward Traffic		2 minutes ago	192.168.2.3	74.125.133.84 (accounts.google.com)	SSL	pass	
Local Traffic		2 minutes ago	192.168.2.3	150.171.22.12 (afdfcfwww.linkedin.com)	SSL	pass	
Sniffer Traffic		2 minutes ago	192.168.2.3	150.171.22.12 (afdfcfwww.linkedin.com)		block	
Events		2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)	SSL	pass	
AntiVirus		2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)		block	
Web Filter		2 minutes ago	192.168.2.3	150.171.22.12 (afdfcfwww.linkedin.com)	SSL	pass	
SSL		2 minutes ago	192.168.2.3	150.171.22.12 (afdfcfwww.linkedin.com)		block	
DNS Query		2 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10.facebook.com)	Facebook	block	
File Filter		2 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10.facebook.com)	Facebook	block	
Application Control	★	3 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10.facebook.com)	Facebook	block	
Intrusion Prevention							
Anomaly							
Log Settings							

If we went to Log & Report then Application Control, we can see here that Facebook was blocked while LinkedIn was passed. We can monitor and view the actions here easily.

5

Anti-Virus

Our goal in Anti-Virus is to apply it to LAN 2 only for testing.



We created the AntiVirus profile: **OUR-AV** with the default settings to scan and block malicious files.

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
DMZ-WAN	DMZ-WEB	all	always	ALL	ACCEPT	Enabled	certificate-inspection	196.23 MB
LAN1-DMZ	LAN-1	DMZ-WEB	always	ALL	ACCEPT	Enabled	WEB Block-DEPI certificate-inspection	359.94 kB
LAN1-WAN	LAN-1	all	always	ALL	ACCEPT	Enabled	WEB Block-Web APP Our-APP-Control certificate-inspection	684.79 MB
LAN2-DMZ	LAN2	DMZ-WEB	always	ALL	ACCEPT	Enabled	WEB Block-DEPI certificate-inspection	94.42 kB
LAN2-WAN	LAN2	all	always	ALL	ACCEPT	Enabled	AV OUR-AV WEB Block-Web certificate-inspection	9.03 MB
Implicit								

We applied the Antivirus profile to the **LAN2-WAN** policy to prevent any malicious file coming from the internet to LAN 2.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab displays a 'High Security Alert' from malware.wicar.org. The alert message reads: 'You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".' Below the message, it lists the URL as http://malware.wicar.org/data/eicar.com and a Reference URL as http://www.fortinet.com/ve?vn=EICAR_TEST_FILE.

For testing, we went to WICAR website on Kali Linux (LAN 2) and tried to download the test malicious file, and it was blocked by FortiGate's AntiVirus that we applied.

The screenshot shows the FortiGate management interface under the 'Log & Report' section, specifically the 'AntiVirus' tab. A log entry is visible in the table:

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
Minute ago	HTTP	192.168.2.66	eicar.com	EICAR_TEST_FILE		URL: http://malware.wicar.org/data/eicar.com	blocked

If we went to Log & Report then AntiVirus, we can see that it got blocked and logged here so we can monitor it easily.

6

Conclusion

In the end, we can say that we applied FortiGate's security profiles: **Web Filter, Application Control, and AntiVirus** effectively on our topology.

As we applied:

- 1) **Web Filter** to LAN 1 and LAN 2 through the internet and through our DMZ (Windows Server) and it showed correct actions by blocking the websites through testing and reporting logs.
- 2) **Application Control** to LAN 1 through the internet and it showed correct actions by blocking and passing the applications we want through testing and reporting logs.
- 3) **AntiVirus** to LAN 2 through the internet and it showed correct action by blocking a test malicious file download attempt and it was confirmed through testing and reporting logs.