Project 4: FortiGate Security Profiles

ONL3_ISS8_S2

Group 1:

Mohannad Mohie 21043873

Muhammed Saeed 21045047

Yousef Mohamed 21007865

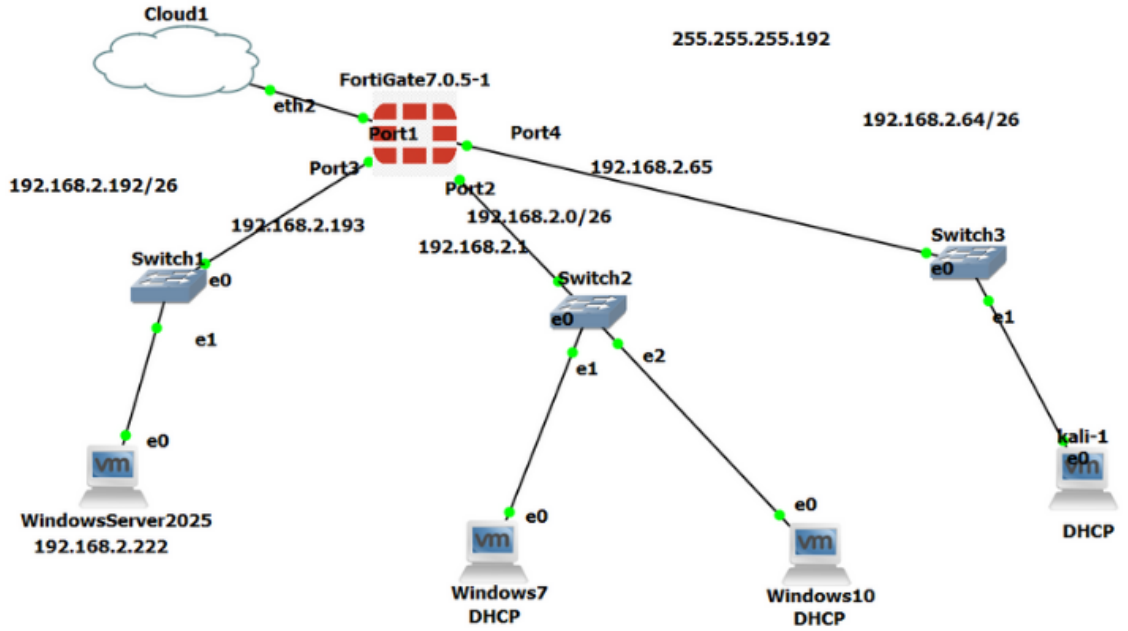
Akram Khaled 21037388

Mazen Mohamed 21052008

Table Of Contents

FORTINET

1 Topology

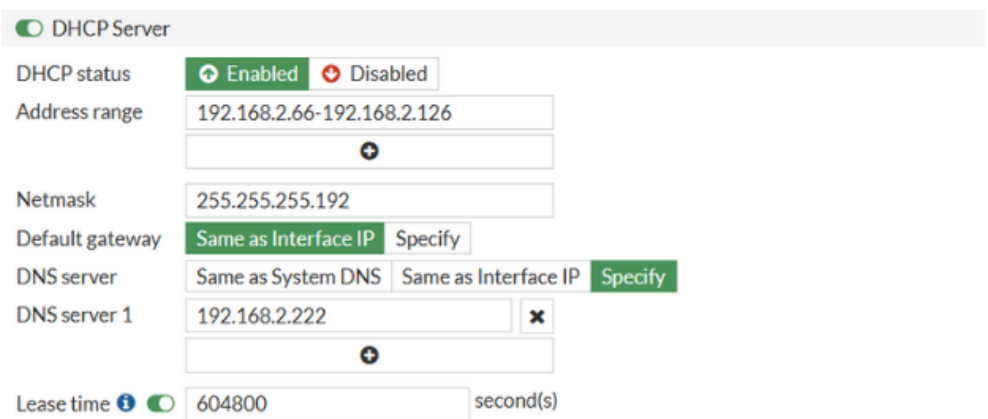


Name	Subnet	Description
LAN-1	192.168.2.0/26	It's a LAN that has two devices; Windows 7 and Windows 10.
LAN-2	192.168.2.64/26	It's a LAN that has one device; Kali-Linux.
DMZ-WEB	192.168.2.192/26	It's a DMZ that has Windows Server which will host a website and acts like the DNS for the whole topology

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.

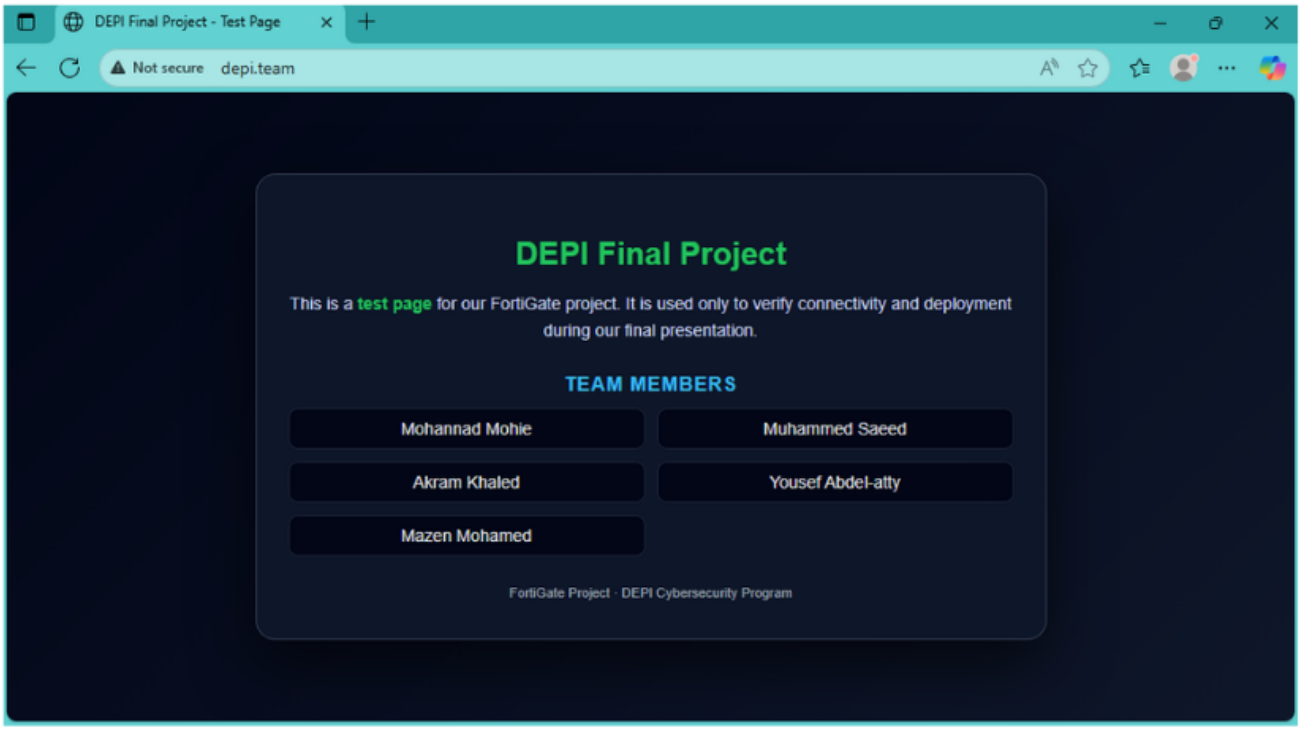
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
802.3ad Aggregate 1						
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254
Physical Interface 4						
DMZ-WEB (port3)	Physical Interface		192.168.2.193/255.255.255.192	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.

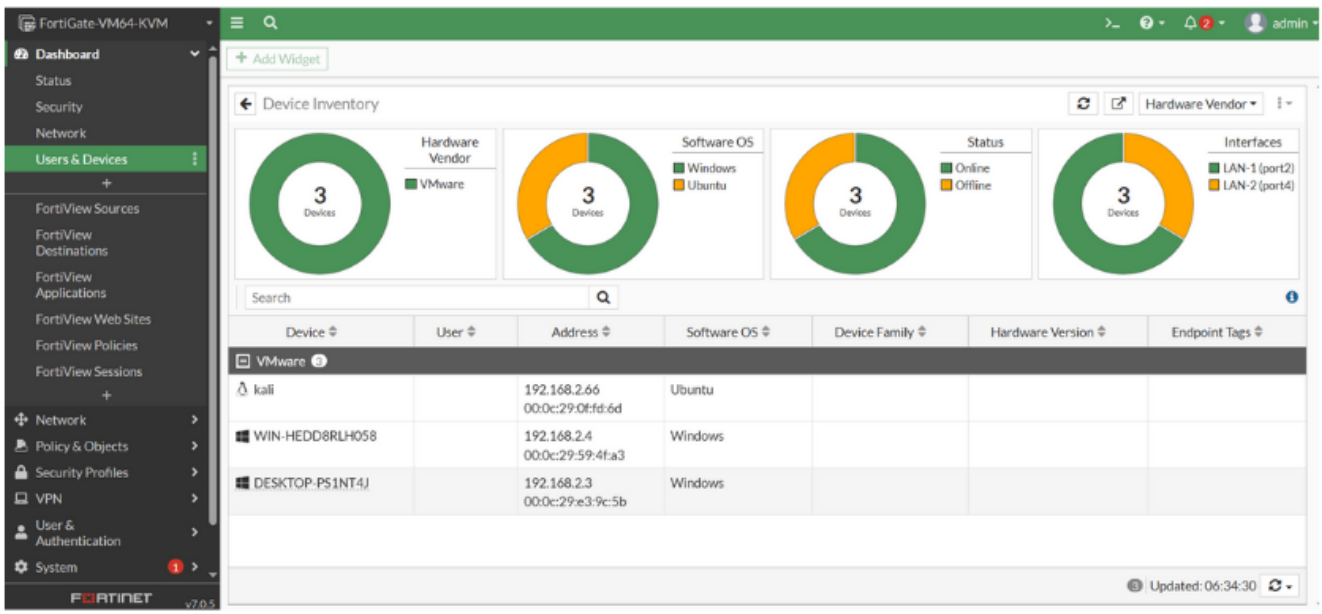


We specified the DNS server to be the Windows Server which has a forwarding route to the internet using Google's DNS server: 8.8.8.8

FORTINET

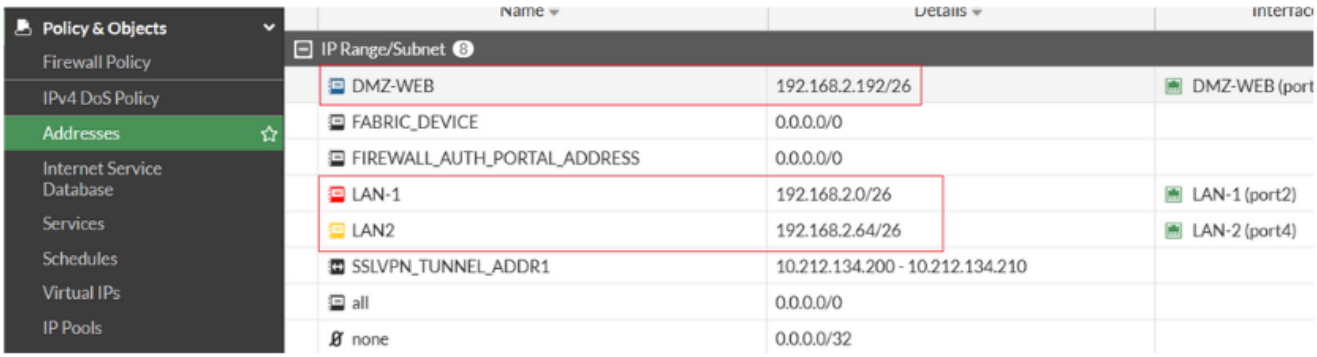


We made a test website page for our project and hosted it on the Windows Server and gave it a domain: depi.team which will later be accessed by all devices using the DNS server.



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



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	certificate-inspection	UTM
LAN-1 (port2) → DMZ-WEB (port3) 1								
LAN1-DMZ	LAN-1	DMZ-WEB	always	ALL	ACCEPT	Enabled	certificate-inspection	UTM
LAN-1 (port2) → port1 1								
LAN1-WAN	LAN-1	all	always	ALL	ACCEPT	Enabled	certificate-inspection	UTM
LAN-2 (port4) → DMZ-WEB (port3) 1								
LAN2-DMZ	LAN2	DMZ-WEB	always	ALL	ACCEPT	Enabled	certificate-inspection	UTM
LAN-2 (port4) → port1 1								
LAN2-WAN	LAN2	all	always	ALL	ACCEPT	Enabled	certificate-inspection	UTM
Implicit 1								

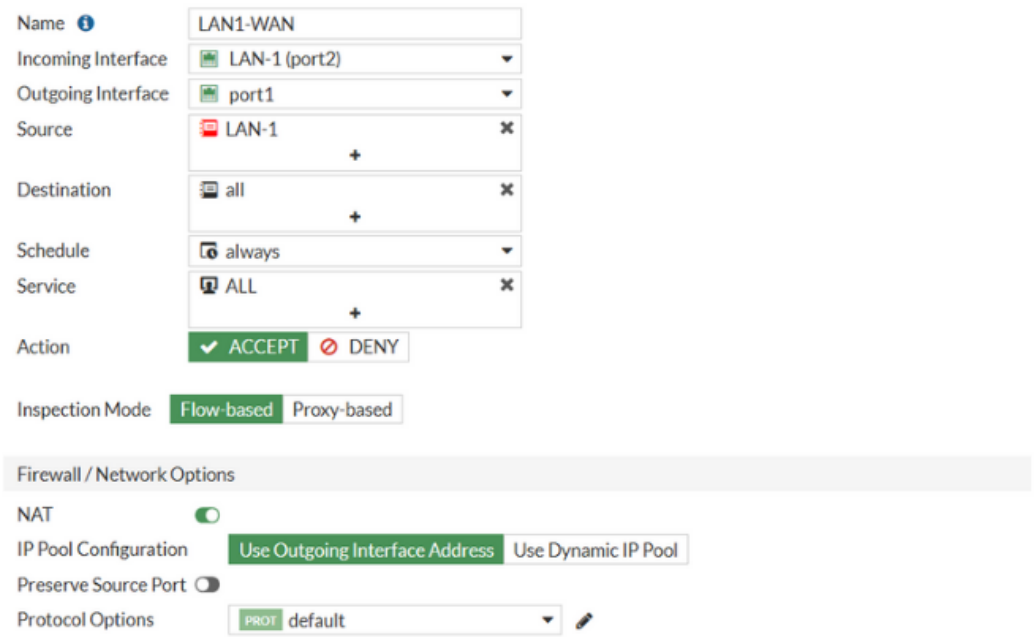
We have created 5 firewall policies:

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.

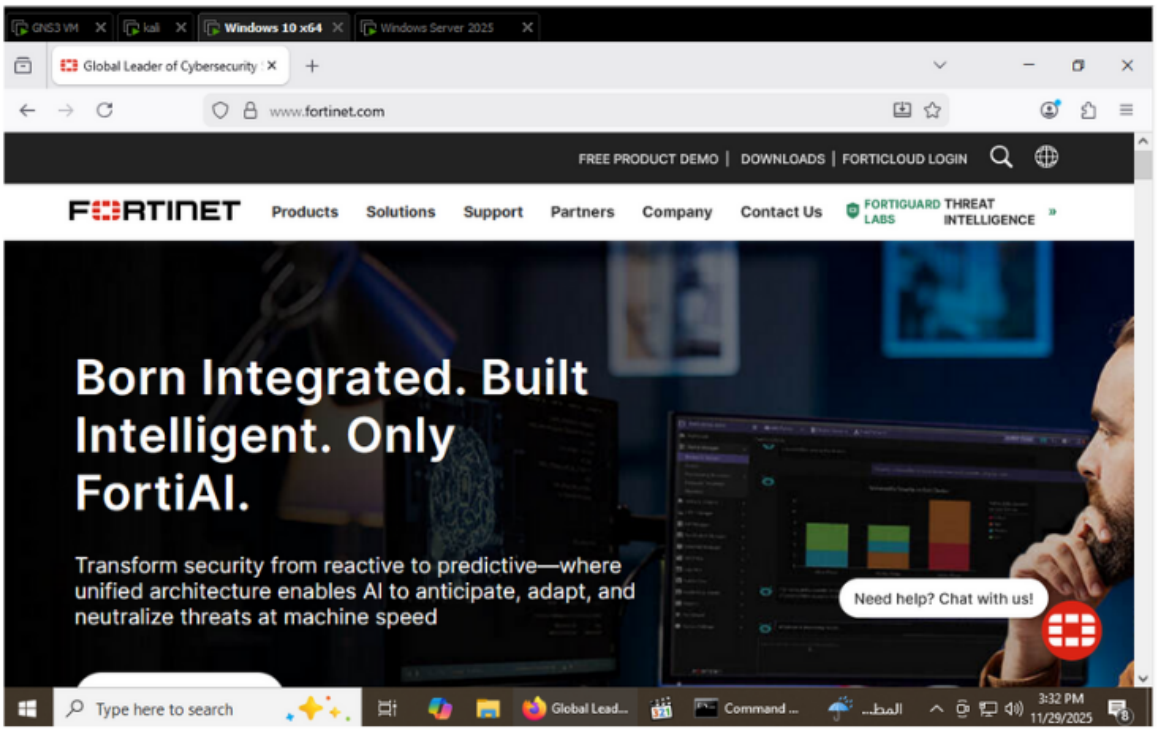
2) **LAN1-DMZ** → This one is made to let LAN-1 access the Windows Server for DNS and depi.team website.

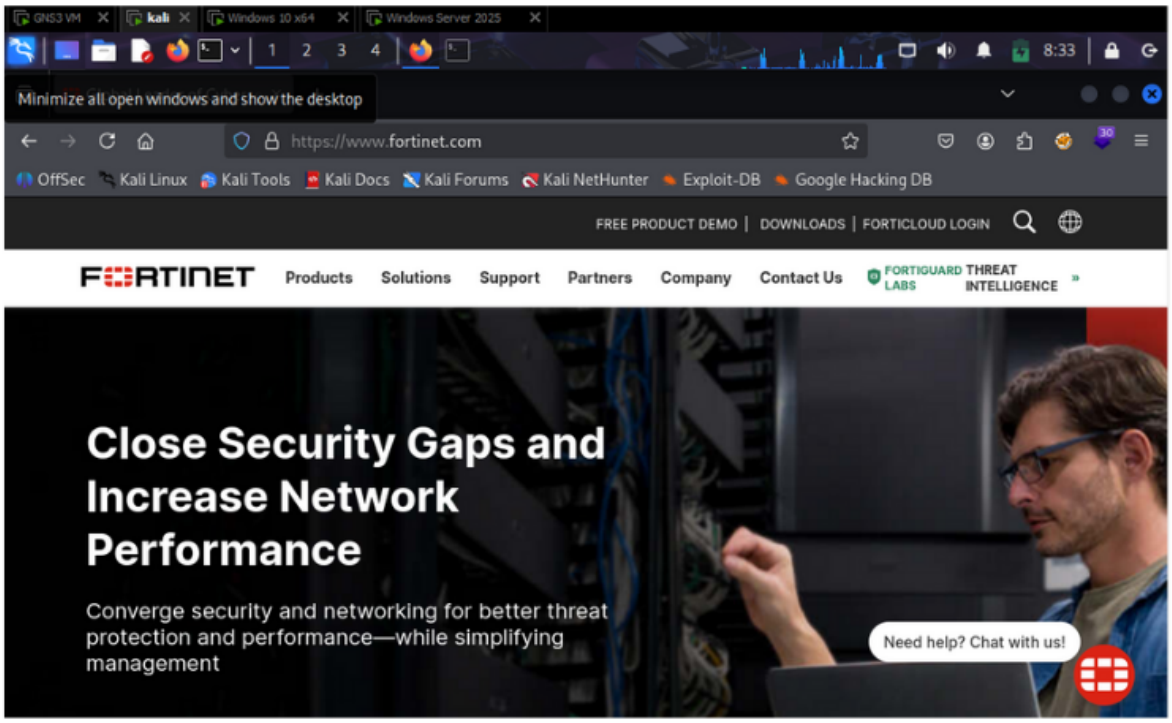
FORTINET

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.

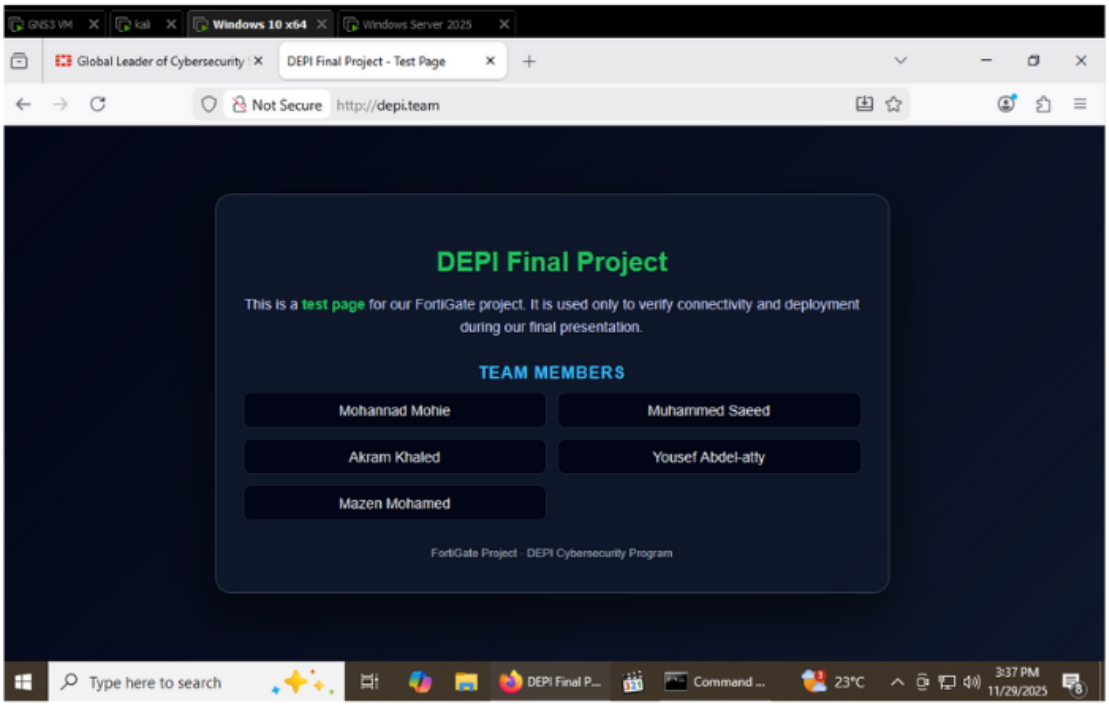


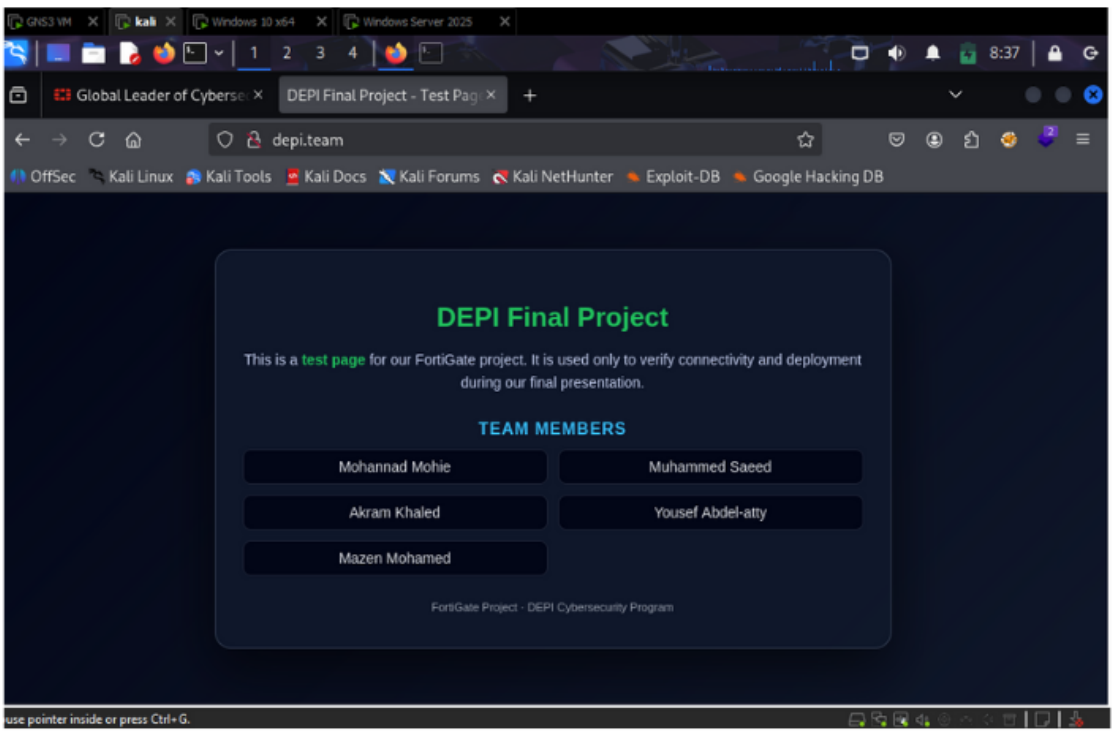
Here's an example of LAN1-WAN policy configuration.





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.

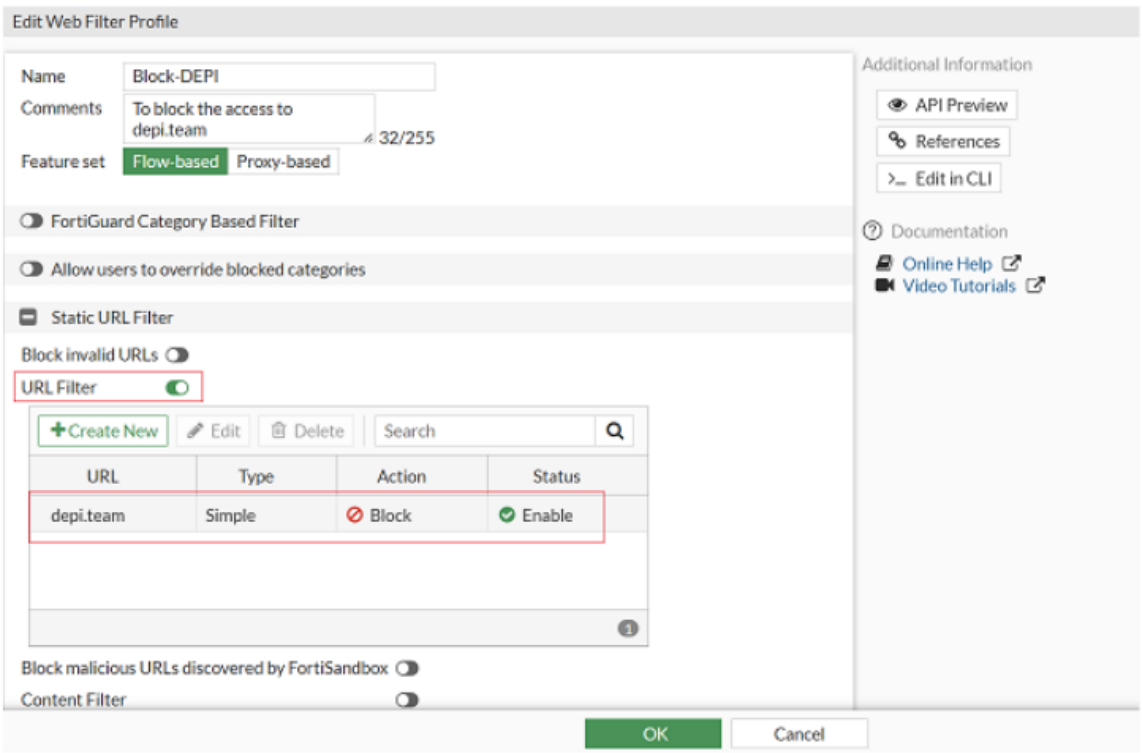




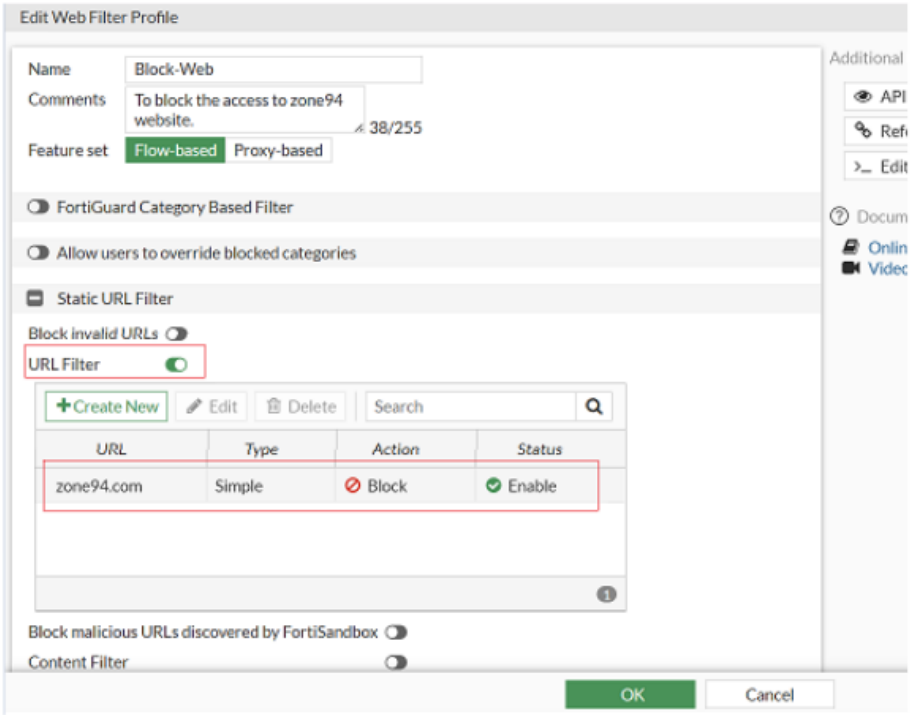
Also here to verify the connectivity between LAN 1 and LAN 2 to the DMZ, here they can access the depi.team website.
We can now say that our firewall policies are working fine.

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.



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.

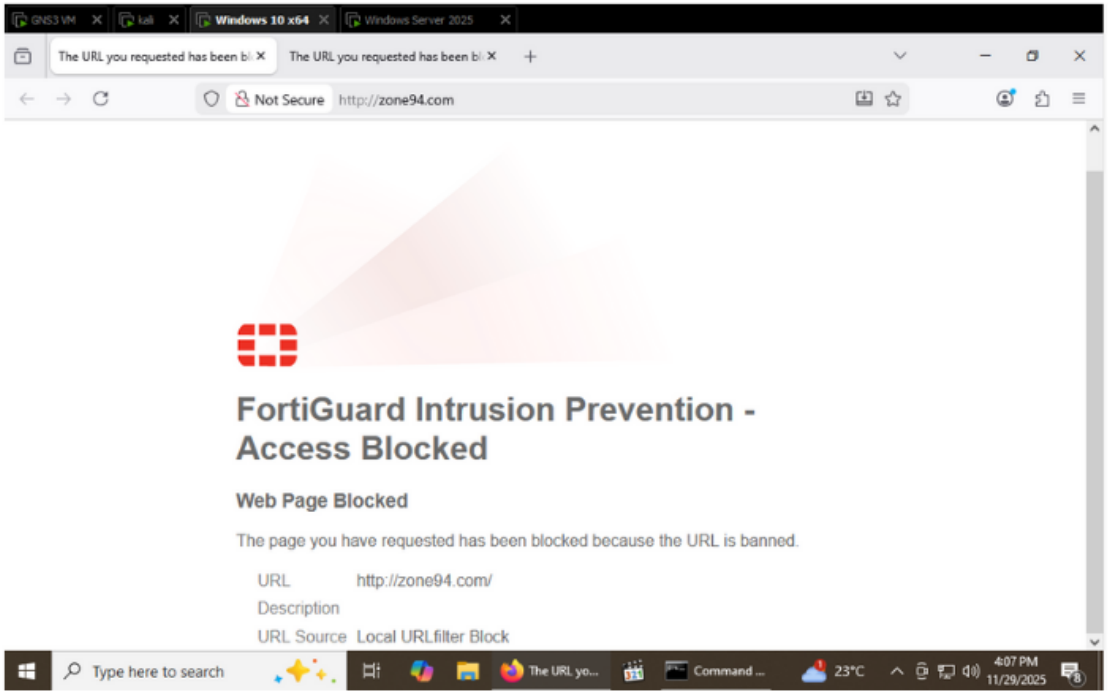


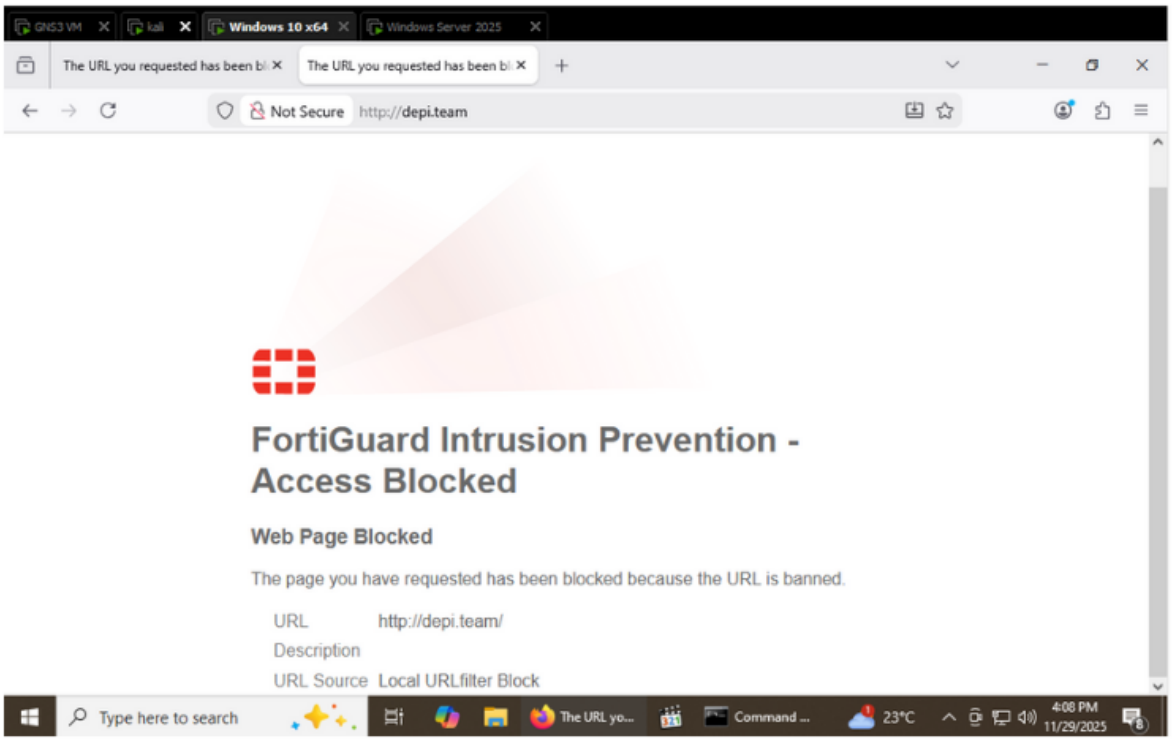
Then, we created the **Block-Web** web filter profile and used **URL Filter** to block the access to the website.
Then we applied the web profile to both **LAN1-WAN** and **LAN2-WAN** policies.

Name	Comments	Ref.
WEB Block-DEPI	To block the access to depi.team	2
WEB Block-Web	To block the access to zone94 website.	2

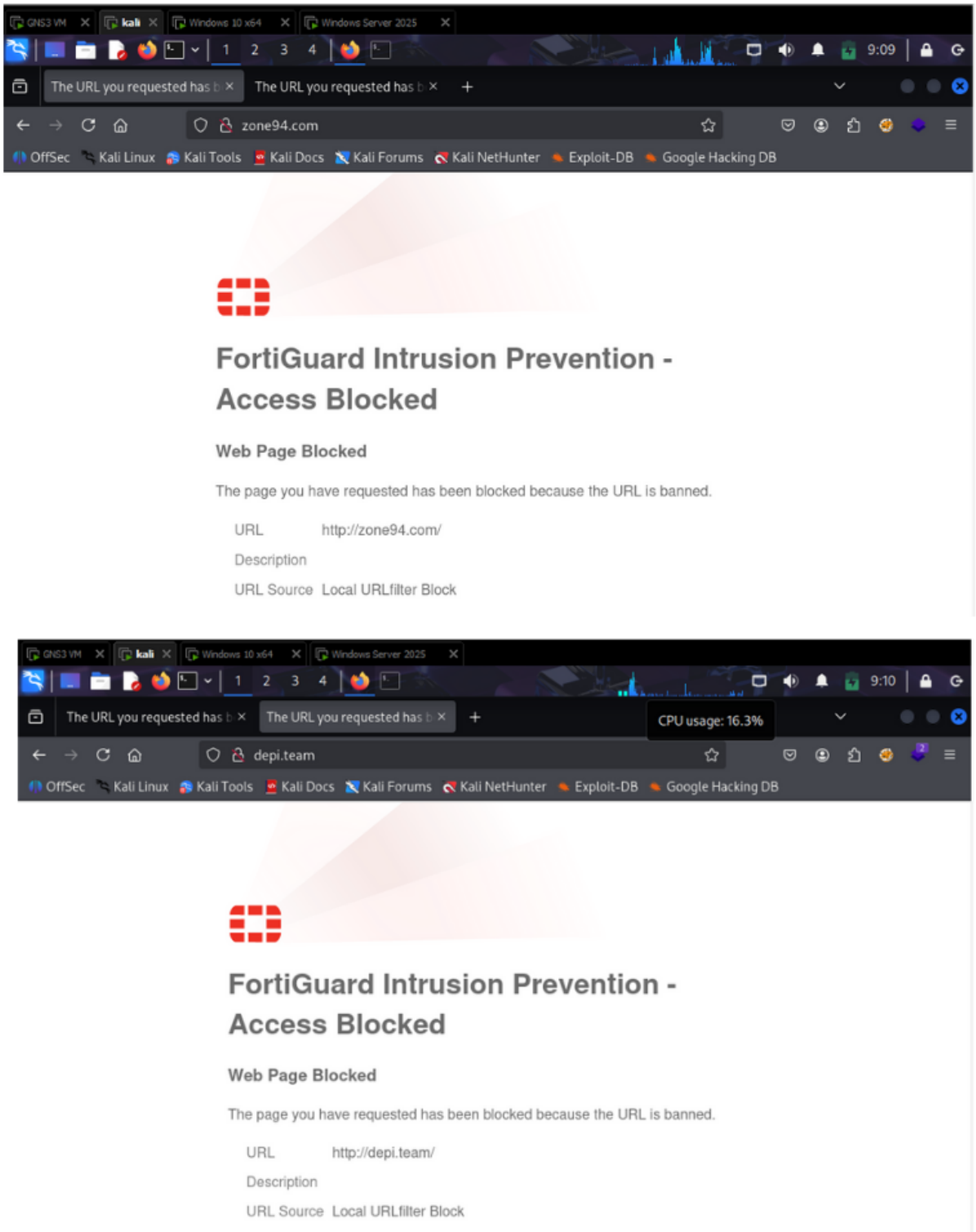
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
DMZ-WEB (port3) → port1 1								
DMZ-WAN	DMZ-WEB	all	always	ALL	ACCEPT	Enabled	SSL certificate-inspection	UTM
LAN-1 (port2) → DMZ-WEB (port3) 1								
LAN1-DMZ	LAN-1	DMZ-WEB	always	ALL	ACCEPT	Enabled	WEB Block-DEPI SSL certificate-inspection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

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

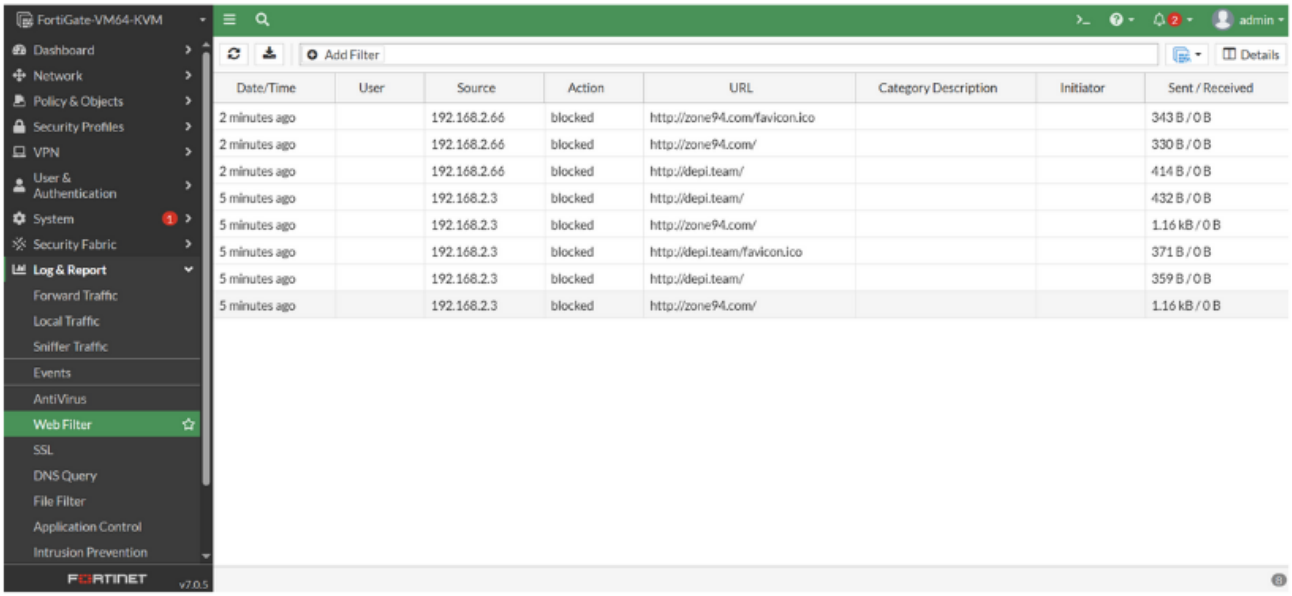




Here we can see that both web filter profiles works correctly on Windows 10 (LAN 1) and blocked the access to the websites.



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

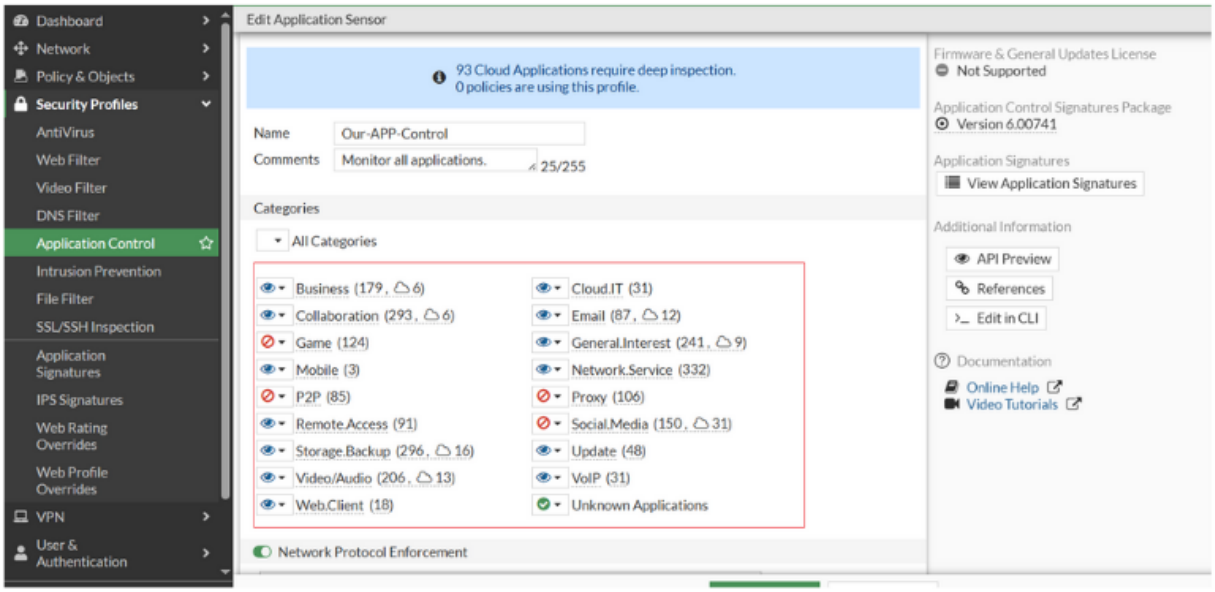


If we went to Log & Report then Web Filter, we can see that they got blocked and logged here so we can monitor it easily.

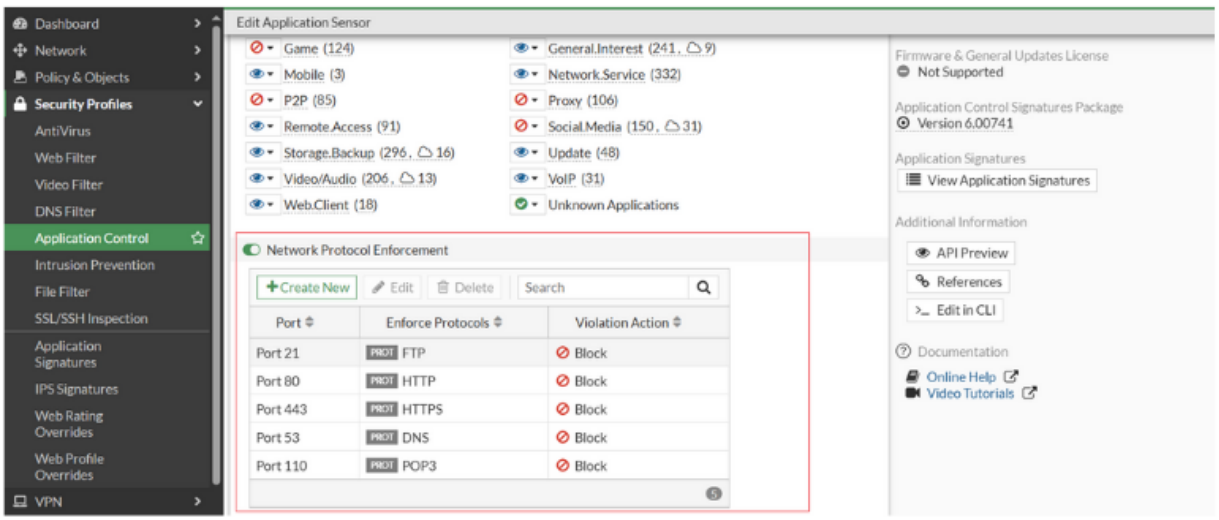
FORTINET

4 Application Control

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

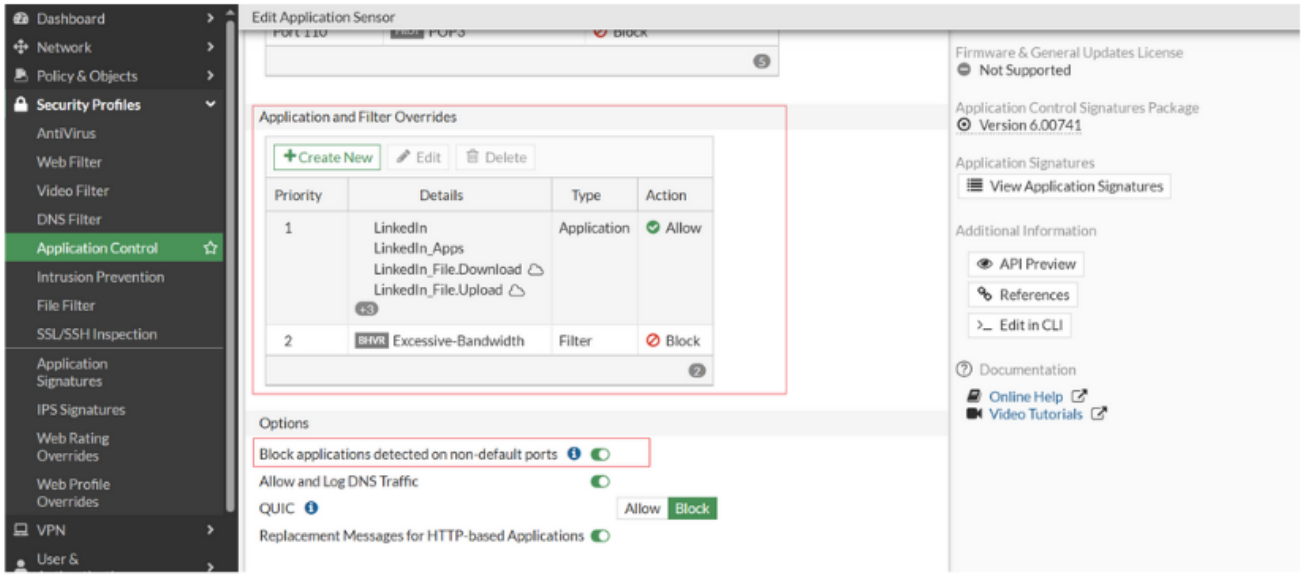


We created the application sensor: **Our-APP-Control** and in categories we blocked: Games, P2P, Proxy, Social Media, and monitored the rest.

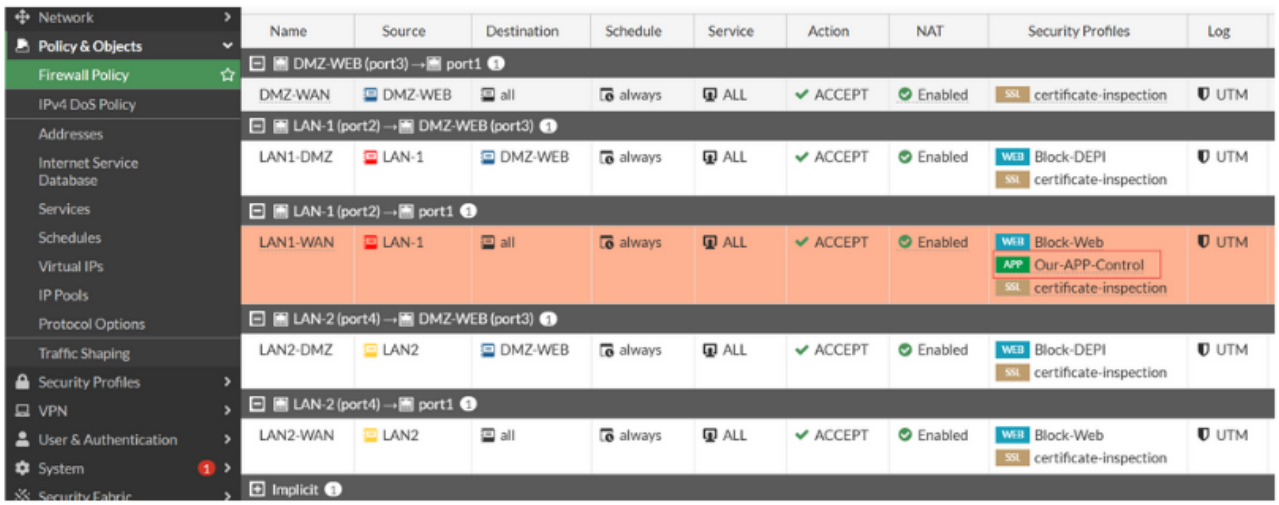


FORTINET

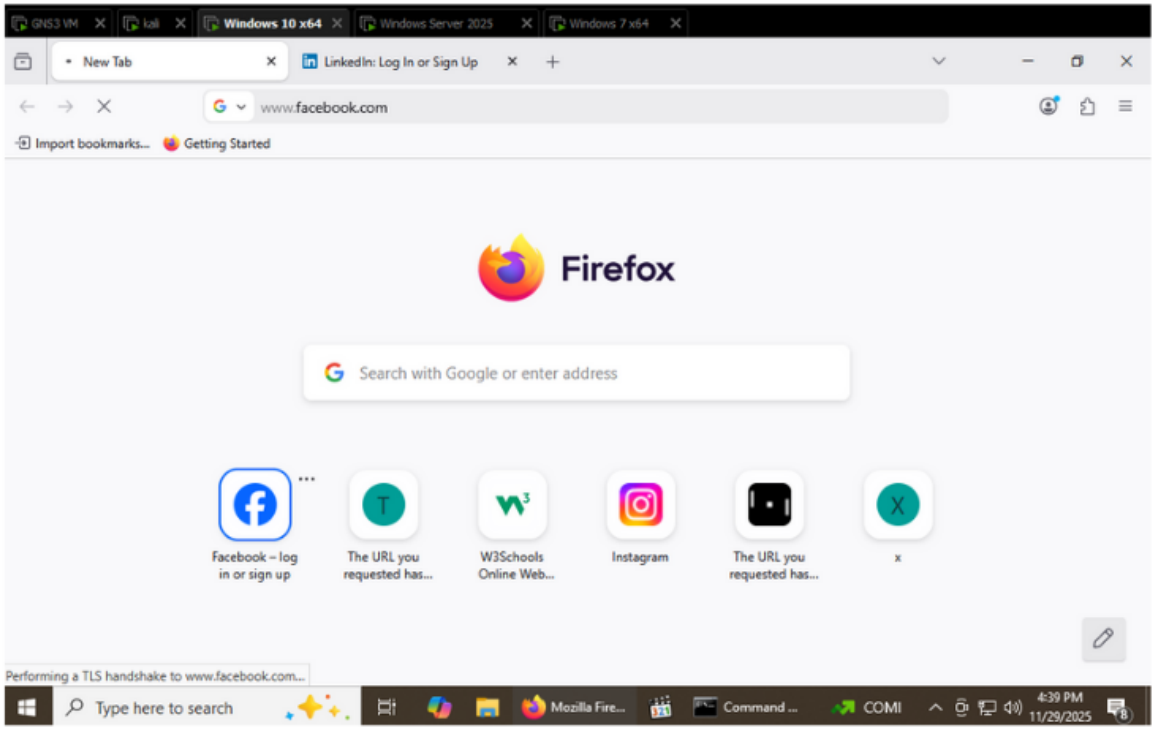
Also we enabled the Network Protocol Enforcement and sat some protocol ports, to make sure any violation or trying to access the protocol using another port will be blocked.



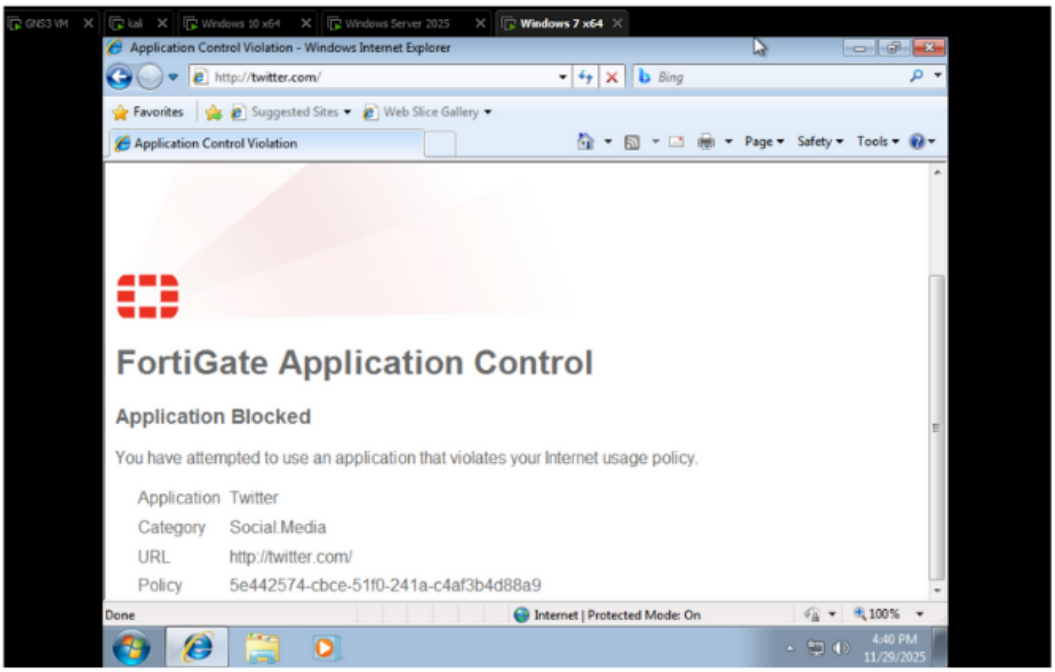
We used Application and Filters Overrides to allow the access to LinkedIn instead of being blocked using the social media category.
We blocked any traffic that uses excessive bandwidth.
We enabled Block applications detected on non-default ports.



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

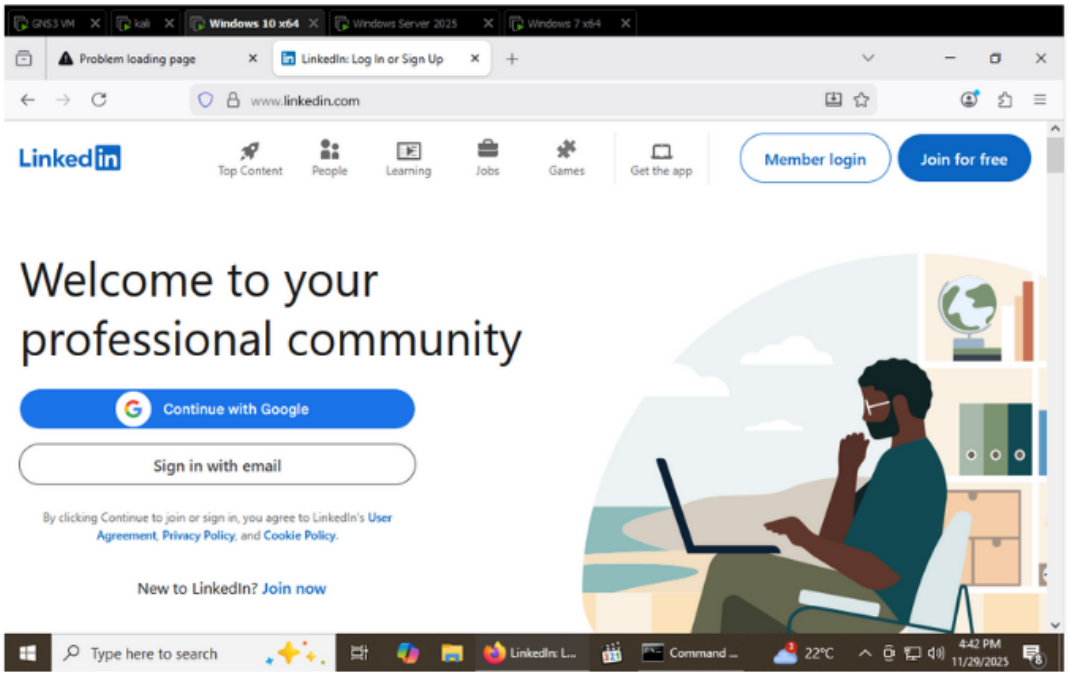


From the Windows 10 device, if we tried to access Facebook, it will just keep loading like this with no reachability.

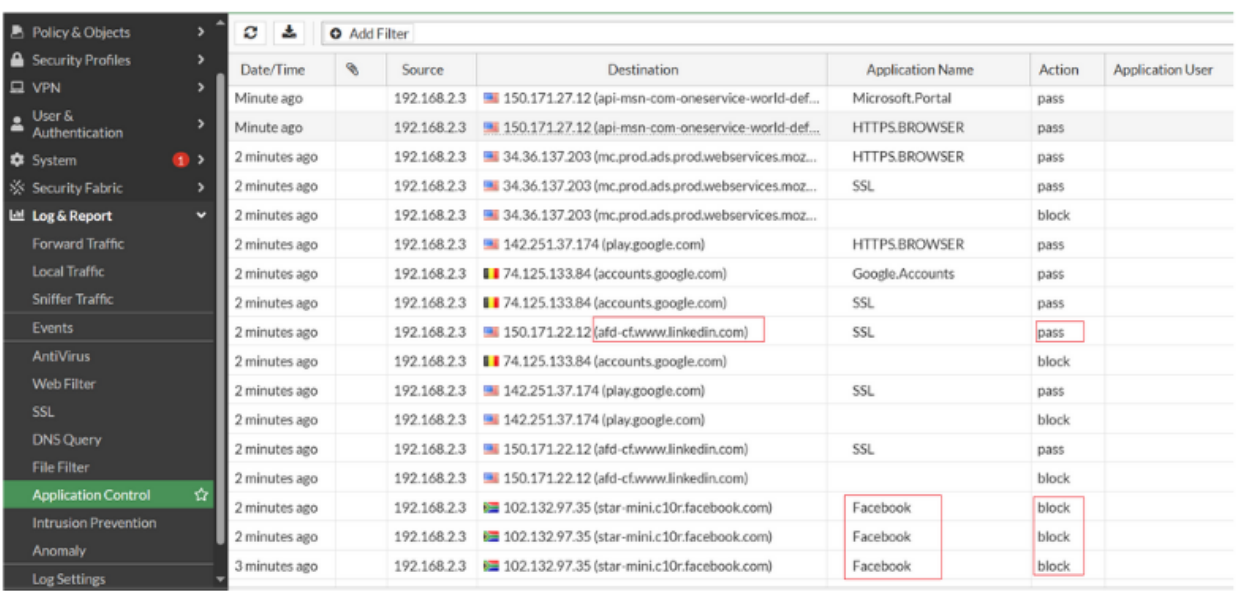


Also here from the Windows 7, if we tried to access Twitter, it will be blocked showing this message from application control.

FORTINET



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



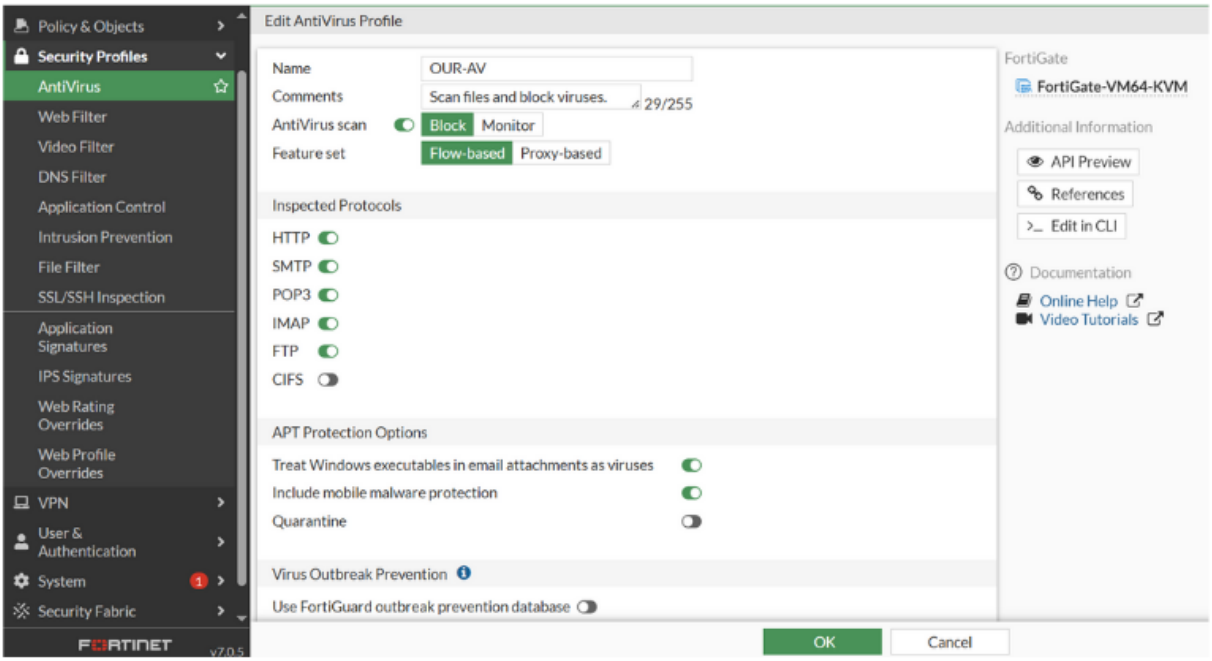
Date/Time	Source	Destination	Application Name	Action	Application User
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	Microsoft.Portal	pass	
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	HTTPS.BROWSER	pass	
2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...	HTTPS.BROWSER	pass	
2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...	SSL	pass	
2 minutes ago	192.168.2.3	34.36.137.203 (mc.prod.ads.prod.webservices.moz...		block	
2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)	HTTPS.BROWSER	pass	
2 minutes ago	192.168.2.3	74.125.133.84 (accounts.google.com)	Google.Accounts	pass	
2 minutes ago	192.168.2.3	74.125.133.84 (accounts.google.com)	SSL	pass	
2 minutes ago	192.168.2.3	150.171.22.12 (afd-cf.www.linkedin.com)	SSL	pass	
2 minutes ago	192.168.2.3	74.125.133.84 (accounts.google.com)		block	
2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)	SSL	pass	
2 minutes ago	192.168.2.3	142.251.37.174 (play.google.com)		block	
2 minutes ago	192.168.2.3	150.171.22.12 (afd-cf.www.linkedin.com)	SSL	pass	
2 minutes ago	192.168.2.3	150.171.22.12 (afd-cf.www.linkedin.com)		block	
2 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10r.facebook.com)	Facebook	block	
2 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10r.facebook.com)	Facebook	block	
3 minutes ago	192.168.2.3	102.132.97.35 (star-mini.c10r.facebook.com)	Facebook	block	

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.

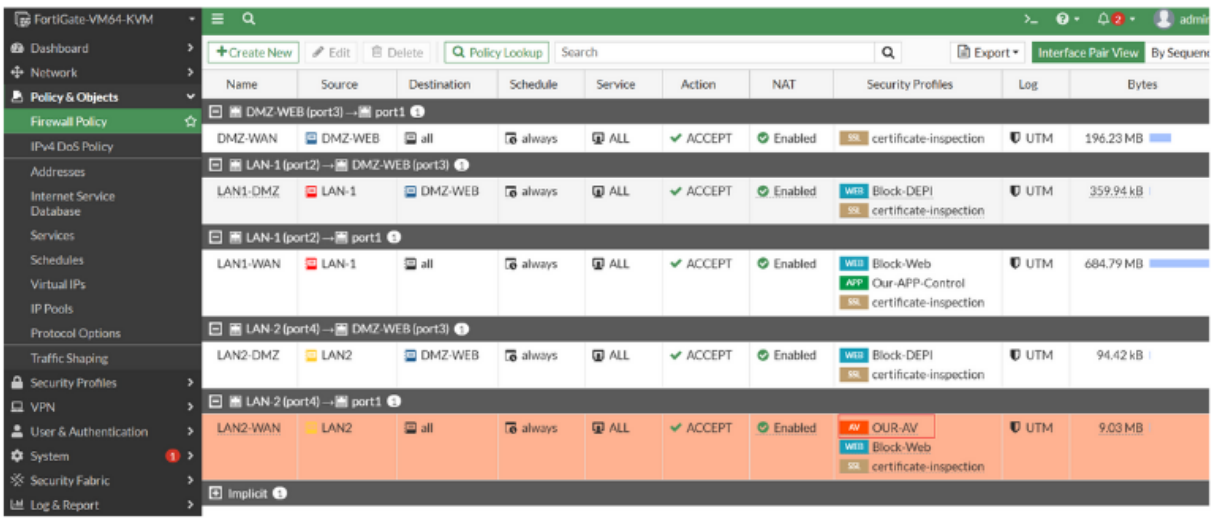
FORTINET

5 Anti-Virus

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

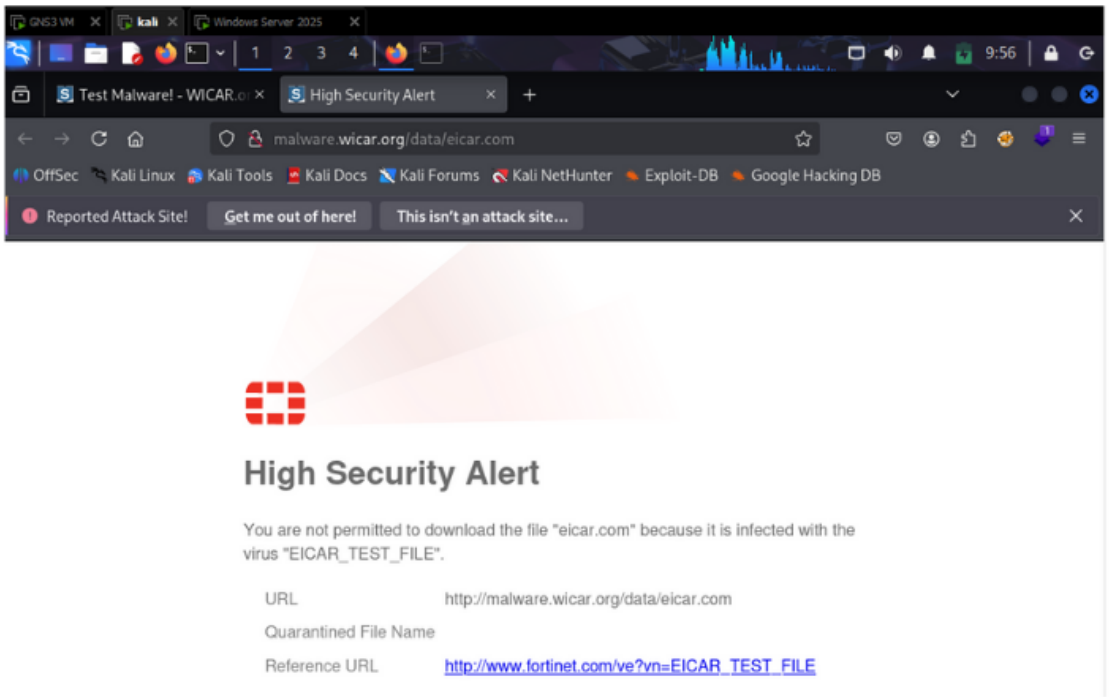


We created the AntiVirus profile: **OUR-AV** with the default settings to scan and block malicious files.

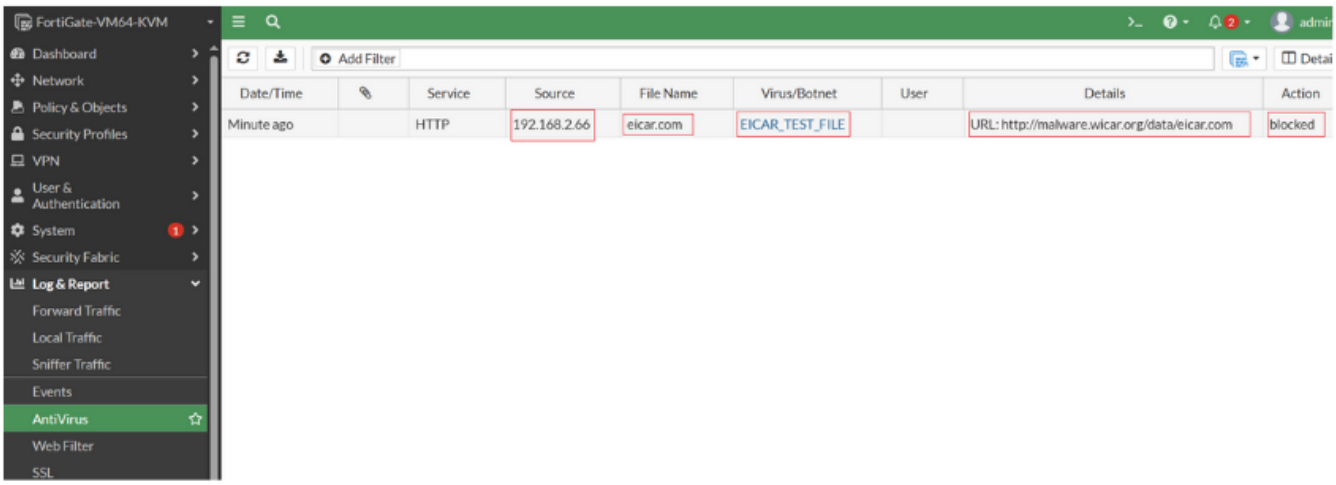


FORTINET

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



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.



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.