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 CONTENT

01 TOPOLOGY

02 IP & DHCP

03 POLICIES

04 WEB FILTER

05 APP CONTROL

06 ANTI-VIRUS

07 MONITORING

08 CONCLUSION

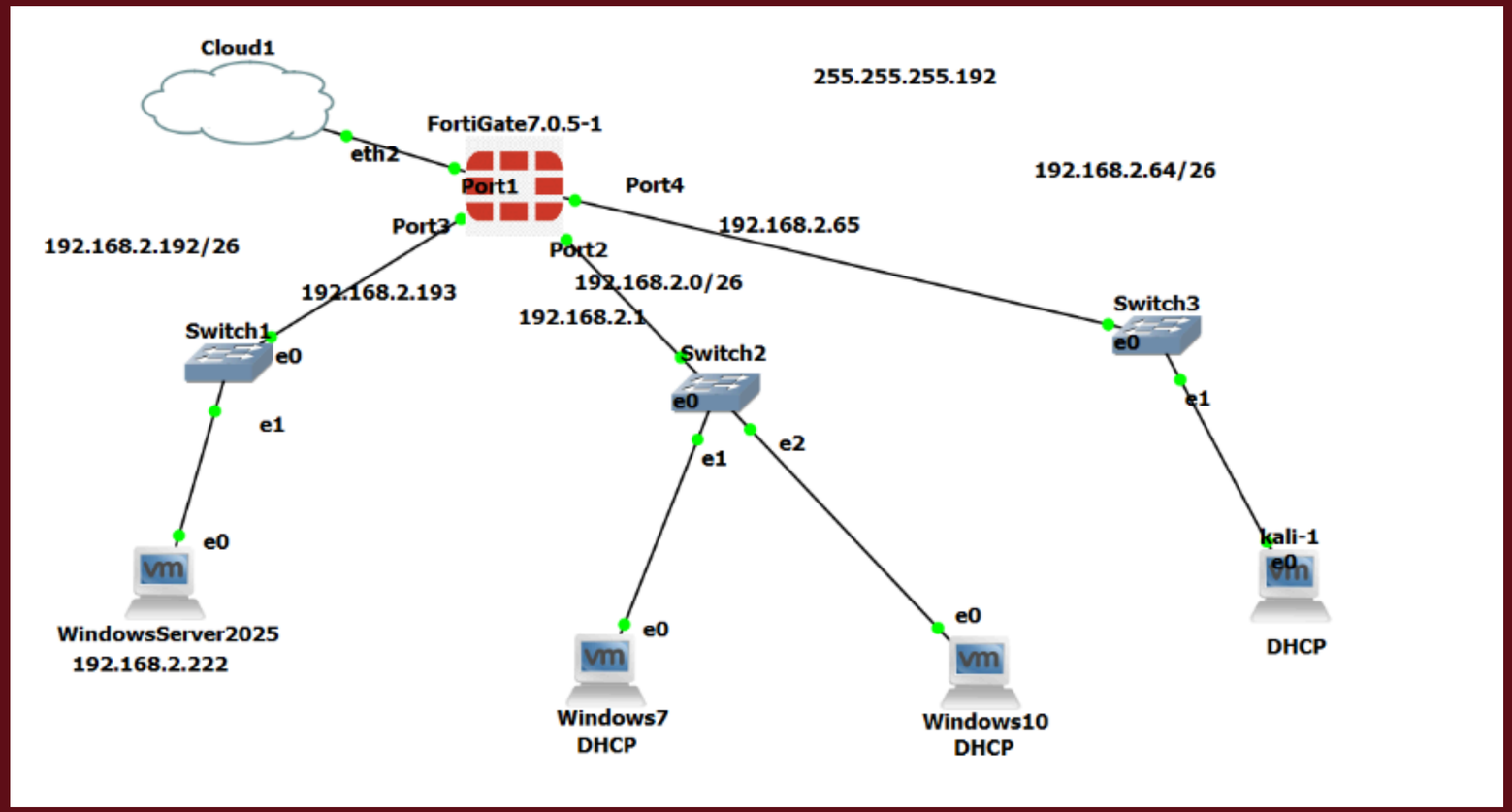
TOPOLOGY

FortiGate firewall connected to:

- Two LAN networks
- One DMZ network
- The Internet

End devices:

- Windows 7
- Windows 10
- Kali Linux
- Windows Server



IP & DHCP

- LAN-1: 192.168.2.0/26
- LAN-2: 192.168.2.64/26
- DMZ-WEB: 192.168.2.192/26
- FortiGate assigns IP addresses using DHCP
- Windows Server is used as DNS and Web Server

PORTS

- Port 1: WAN (Internet)
- Port 2: LAN-1
- Port 3: DMZ-WEB
- Port 4: LAN-2

Each port uses the first available IP address in its subnet.

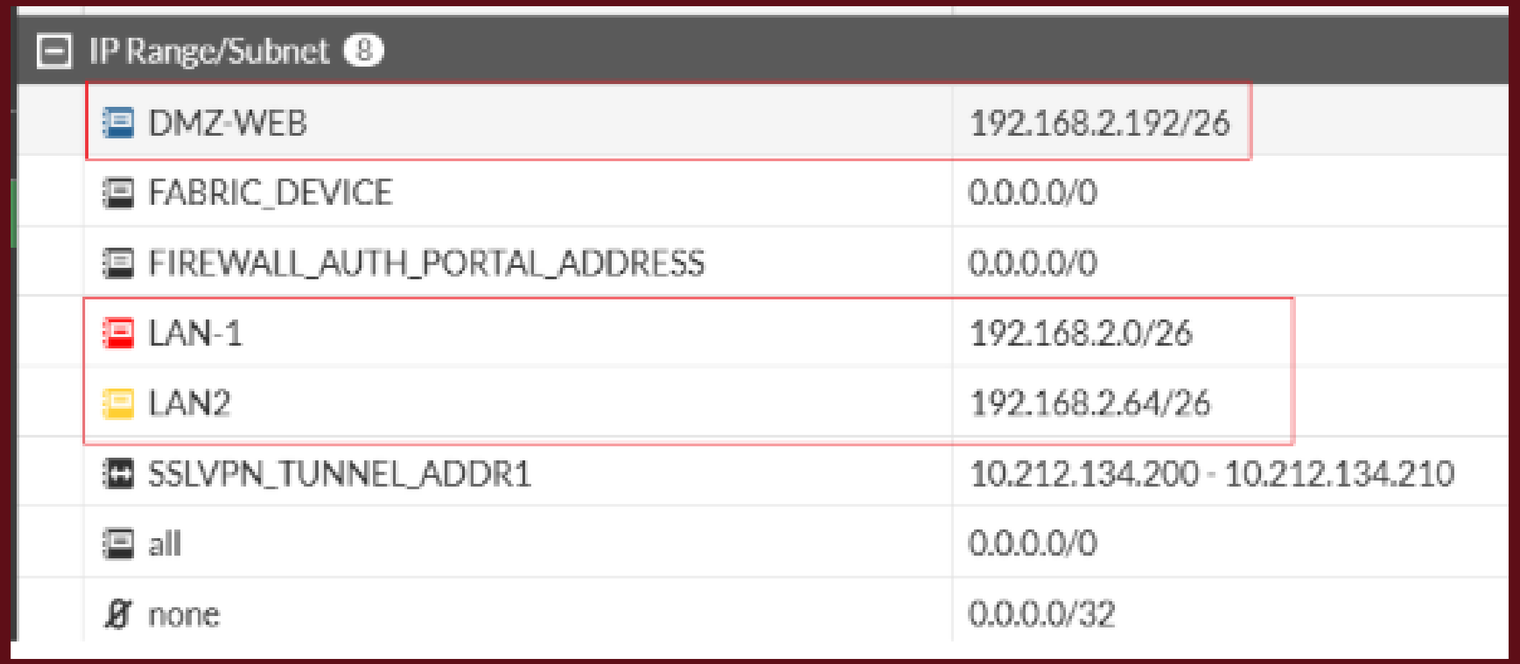
Name	Type	Members	IP/Netmask
802.3ad Aggregate 1			
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch
Physical Interface 4			
DMZ-WEB (port3)	Physical Interface		192.168.2.193/255.255.255.192
LAN-1 (port2)	Physical Interface		192.168.2.1/255.255.255.192
LAN-2 (port4)	Physical Interface		192.168.2.65/255.255.255.192
port1	Physical Interface		192.168.1.5/255.255.255.0

ADDRESSES

Firewall address objects were created for:

- LAN-1
- LAN-2
- DMZ-WEB

These objects simplify policy creation and traffic control.



POLICIES

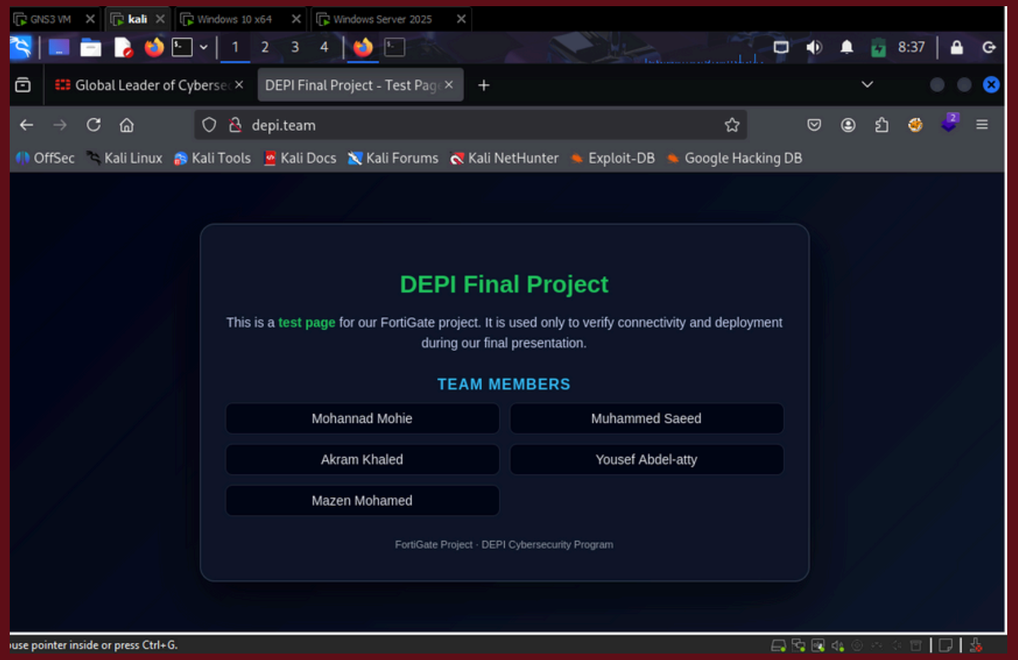
Five firewall policies were created:

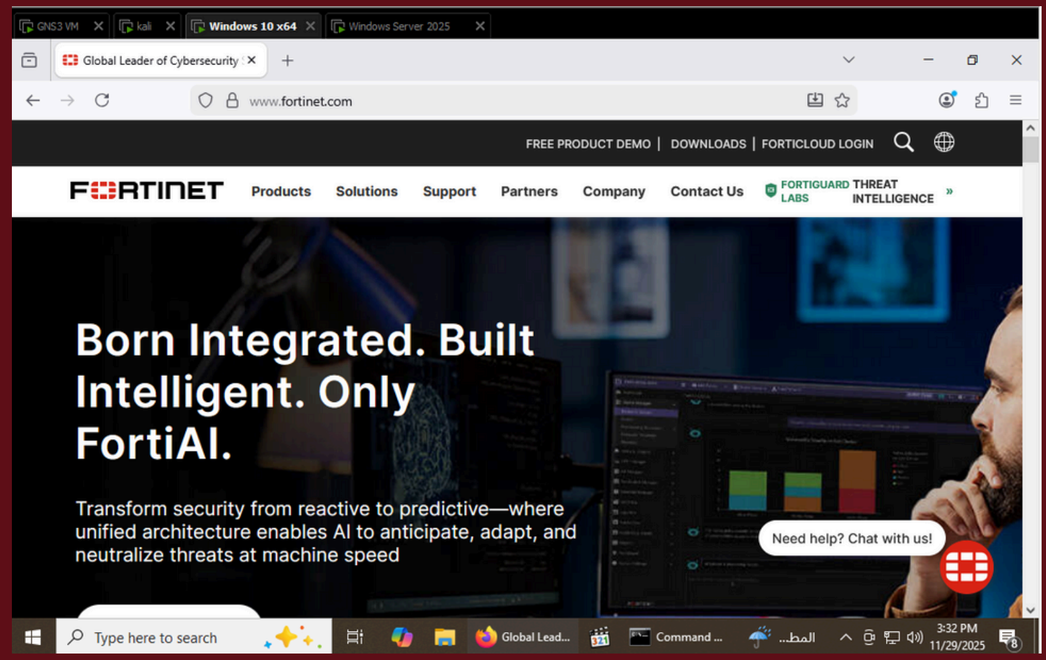
1. DMZ → WAN
2. LAN-1 → DMZ
3. LAN-1 → WAN
4. LAN-2 → DMZ
5. LAN-2 → WAN

No policy was created between LAN-1 and LAN-2 to maintain isolation.

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								

CONNECTIVITY





- All LAN devices can access the Internet
- All LAN devices can access the DMZ website
- DNS resolution is working correctly
- Firewall policies are functioning as expected

WEB FILTER

Block access to:

- depi.team (local DMZ website)
- zone94.com (external website)

Apply filtering on:

- LAN-1 → DMZ
- LAN-2 → DMZ
- LAN-1 → WAN
- LAN-2 → WAN

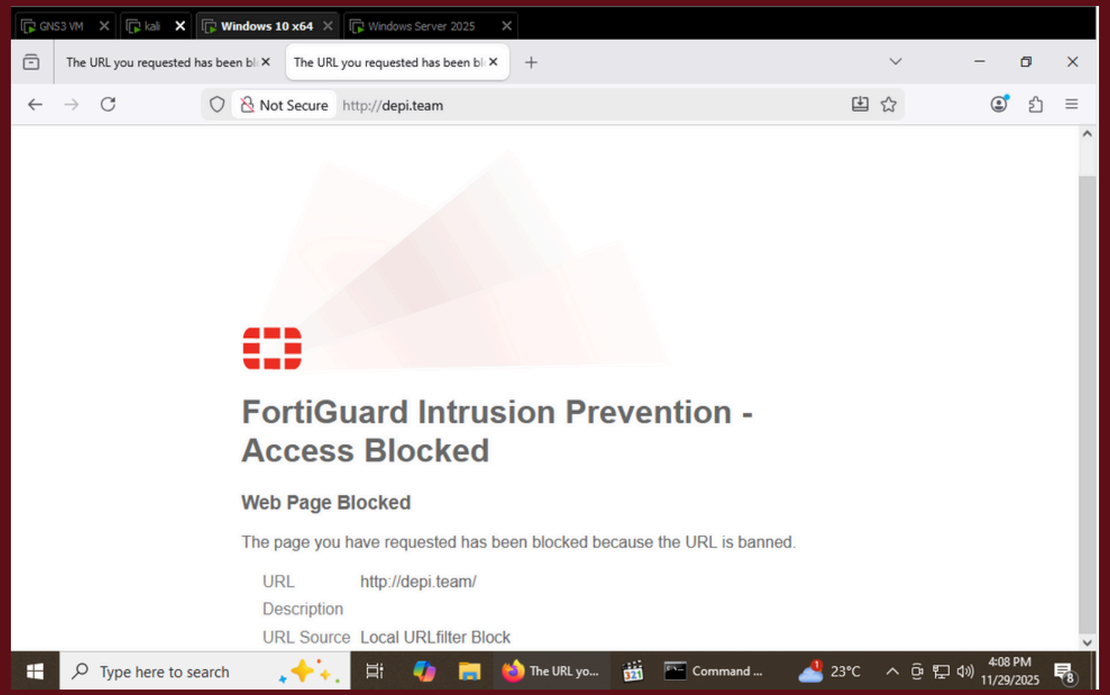
WEB FILTER

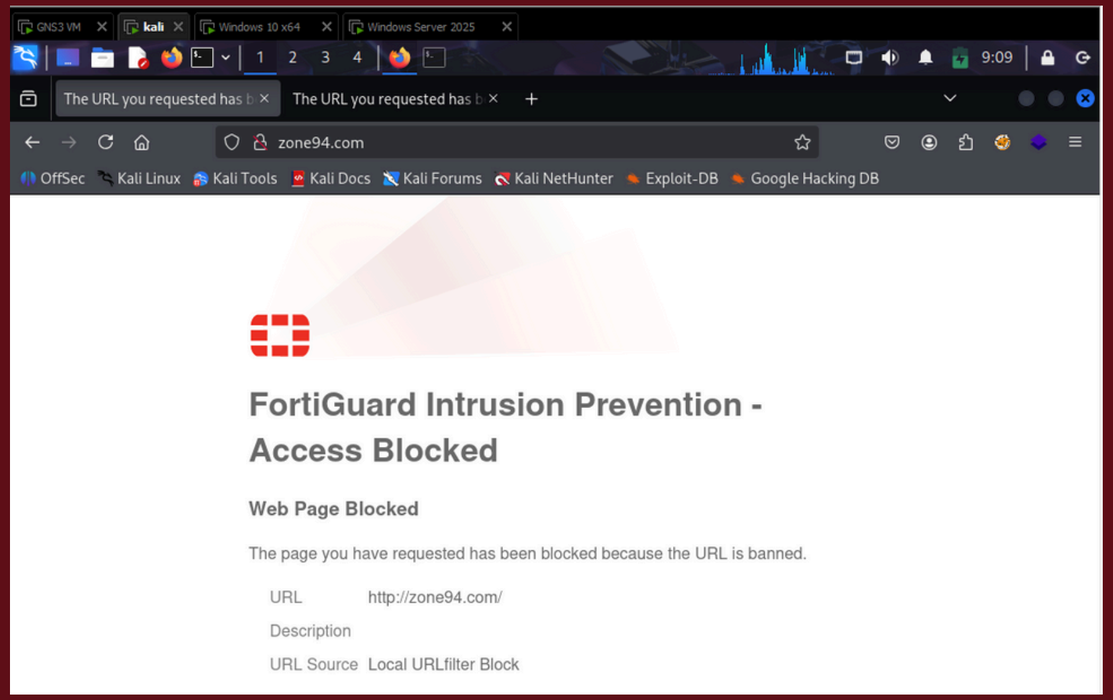
Name	Comments	Ref.
WEB Block-DEPI	To block the access to depi.team	2
WEB Block-Web	To block the access to zone94 website.	2

Two web filter profiles were created:

- Block-DEPI: Blocks depi.team
- Block-Web: Blocks zone94.com
- Filtering method: URL Filtering

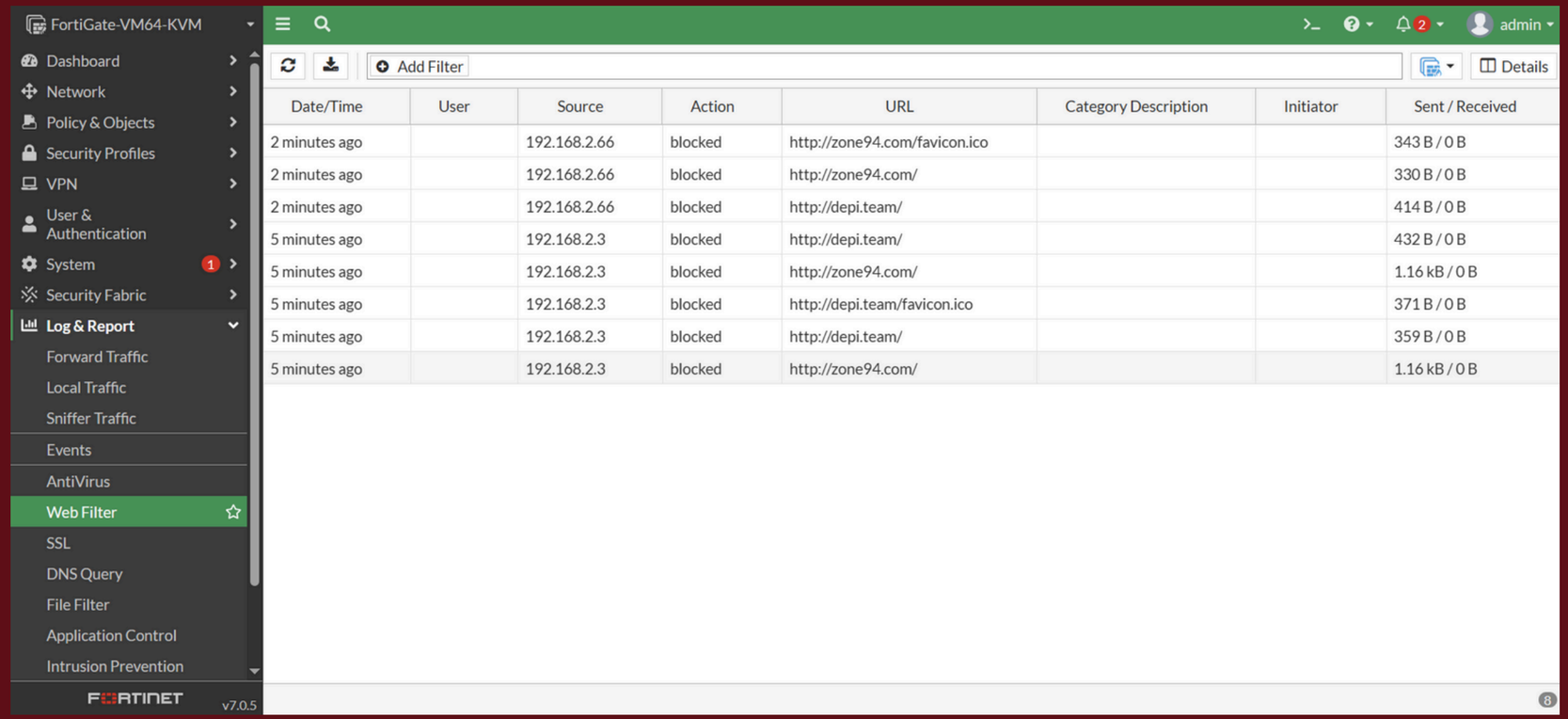
WEB FILTER





- depi.team blocked on Windows 10 and Kali Linux
- zone94.com blocked successfully
- FortiGuard block page displayed when access is denied

WEB FILTER



- All blocked websites appear in Log & Report
- Source IP addresses are recorded
- Time, category, and action are visible

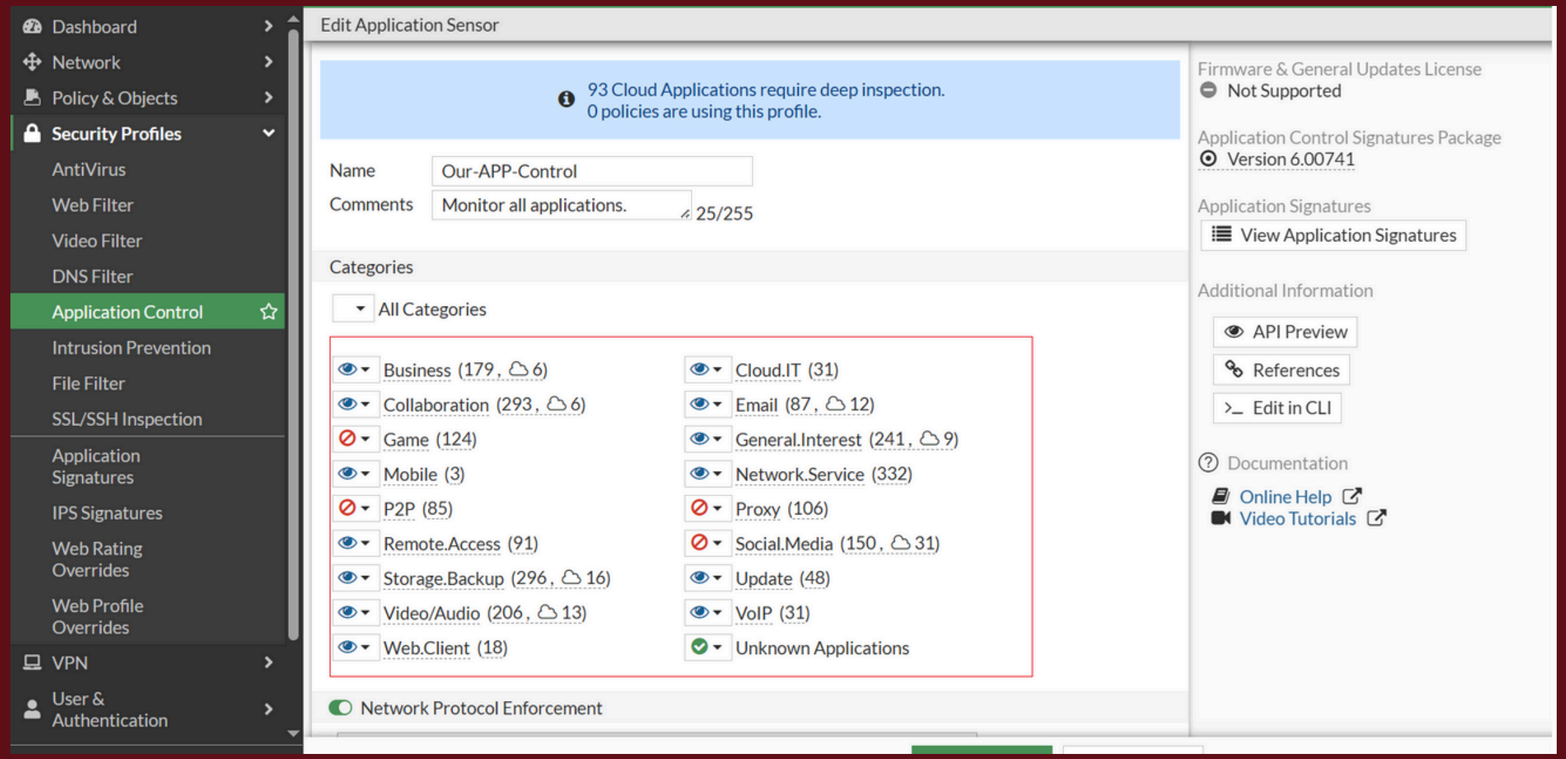
APP CONTROL

Applied only to LAN-1

The following categories were blocked:

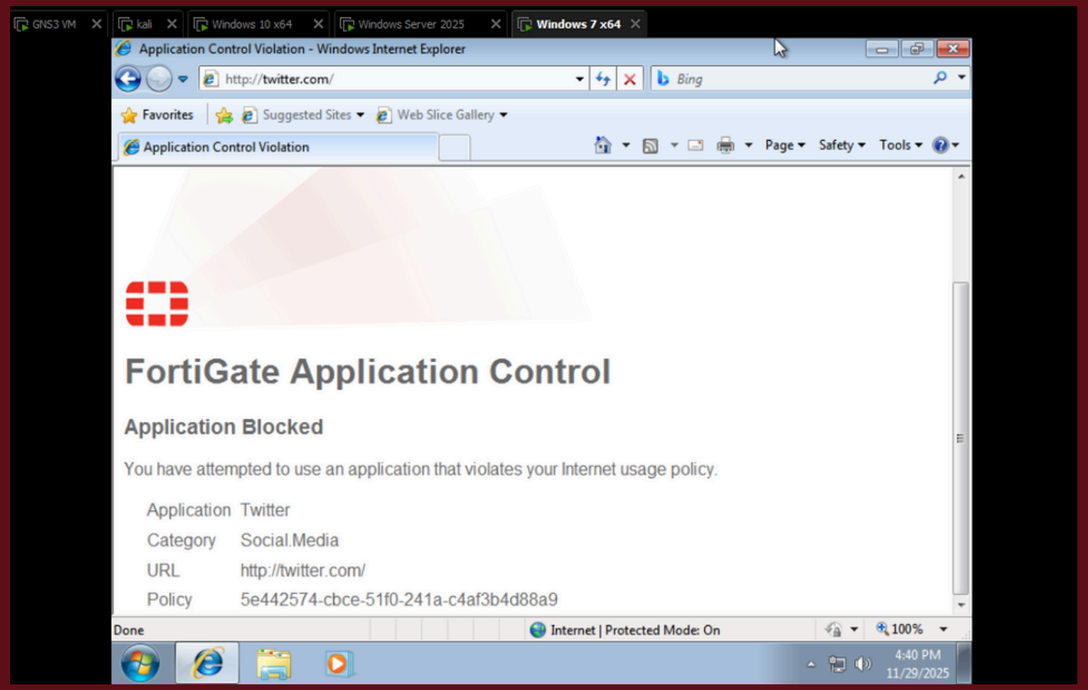
- Social Media
- Games
- Proxy
- P2P

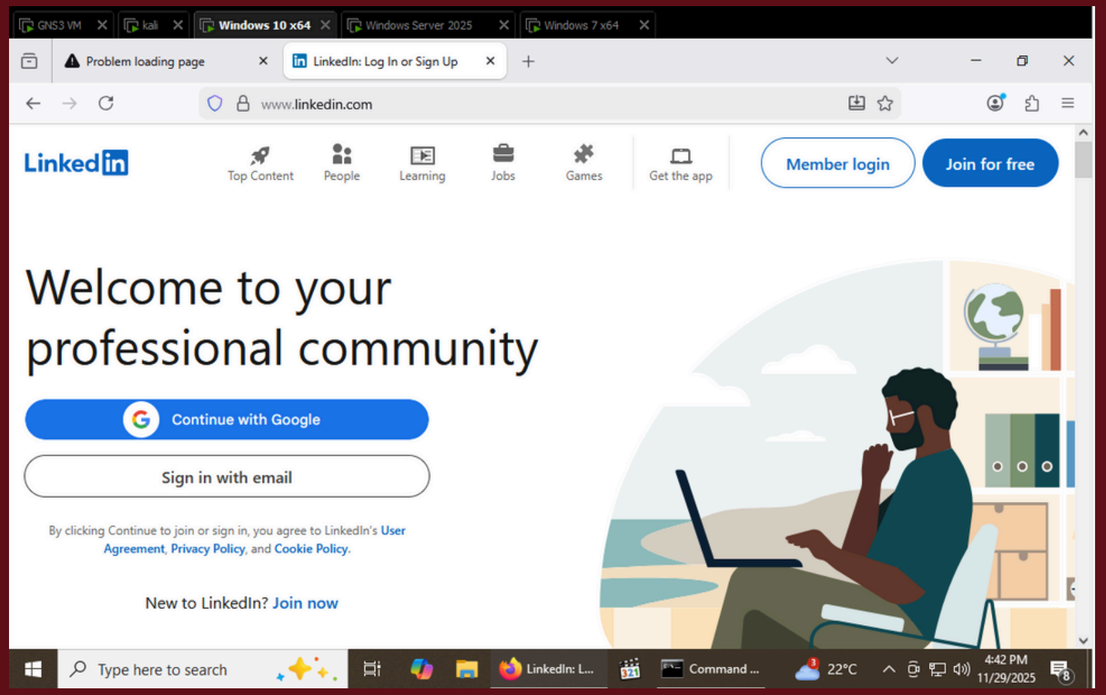
APP CONTROL



- Custom sensor created: Our-APP-Control
- LinkedIn allowed using Application Override
- Excessive bandwidth usage blocked
- Applications on non-default ports blocked

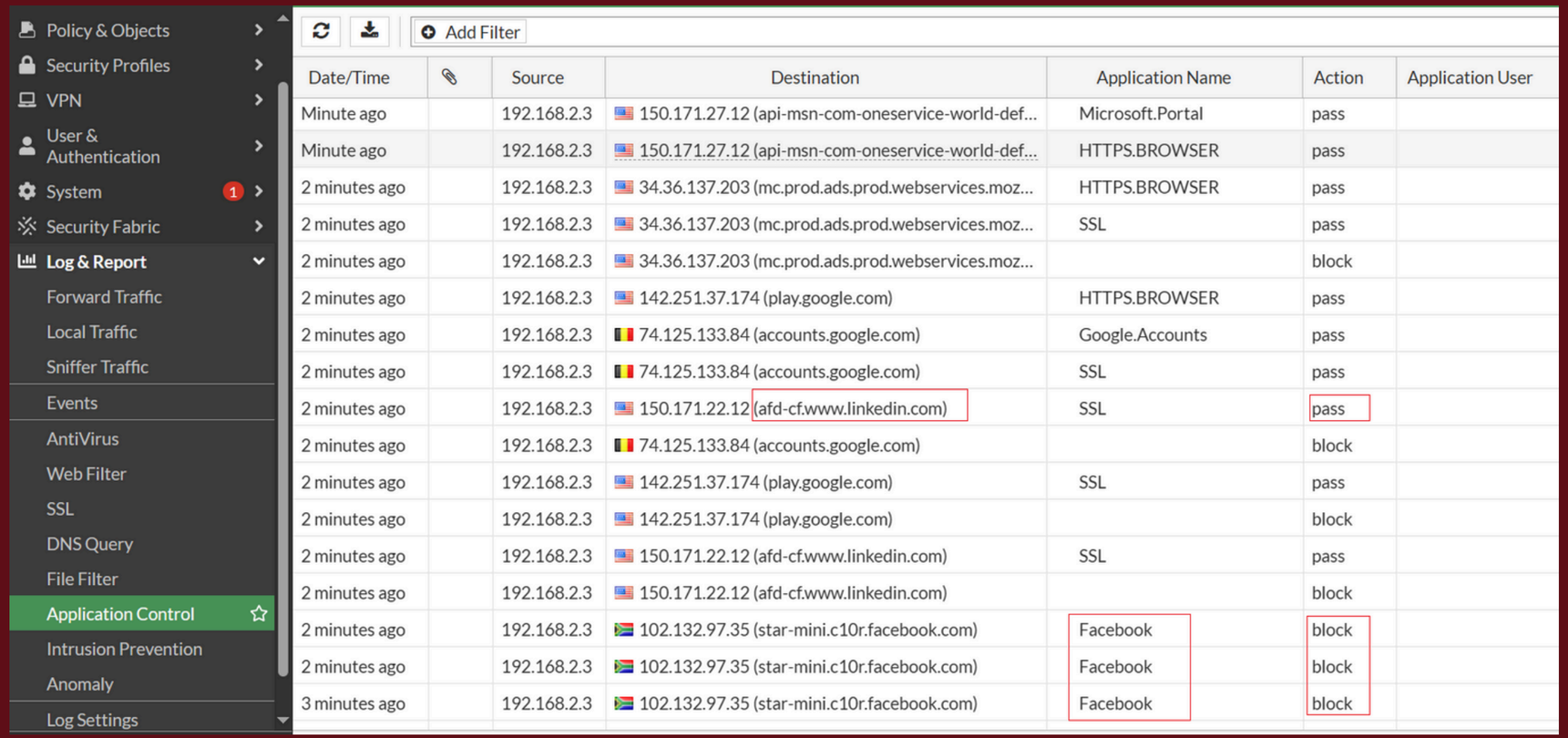
APP CONTROL





- Facebook blocked
- Twitter blocked
- LinkedIn allowed
- Block message displayed by FortiGate

APP CONTROL



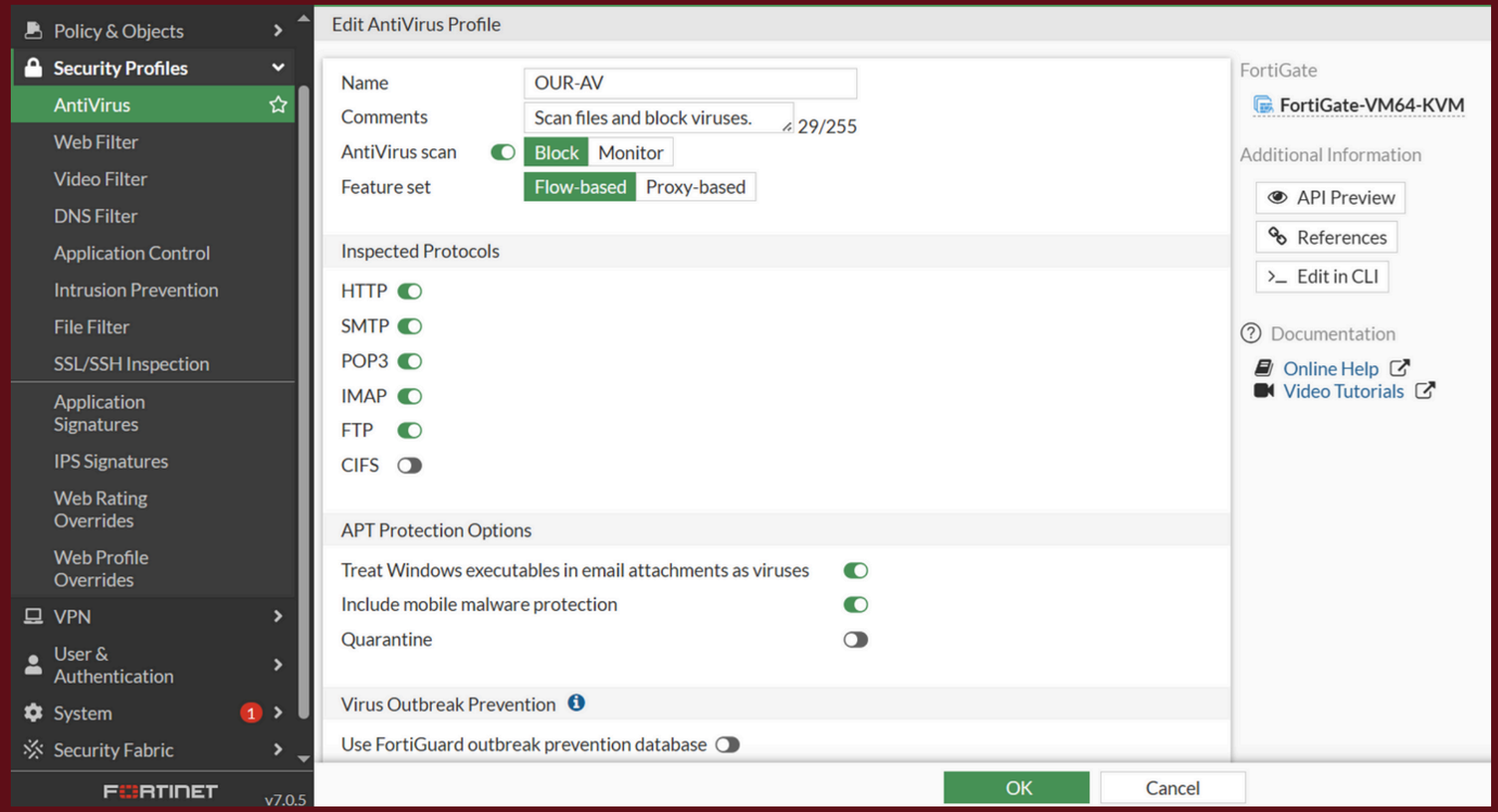
Date/Time	Source	Destination	Application Name	Action	Application User
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	Microsoft.Portal	pass	
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...	HTTPS.BROWSER	pass	
2 minutes ago	192.168.2.3	34.36.137.203 (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	

- All application actions are logged
- Blocked and allowed traffic is recorded
- Category, source, and destination are visible

ANTI-VIRUS

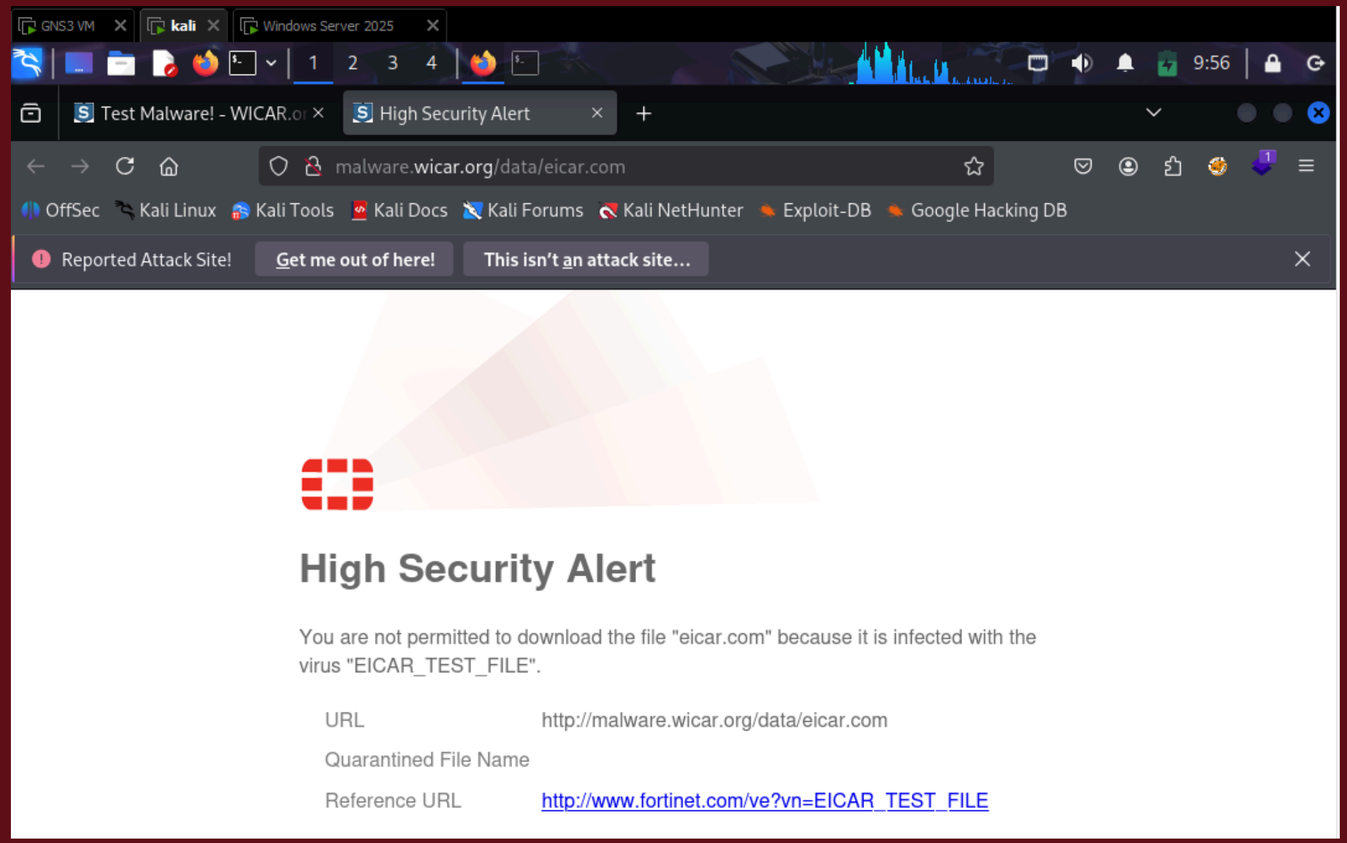
- Applied only to LAN-2
- Protect devices from malicious files
- Real-time malware detection

ANTI-VIRUS



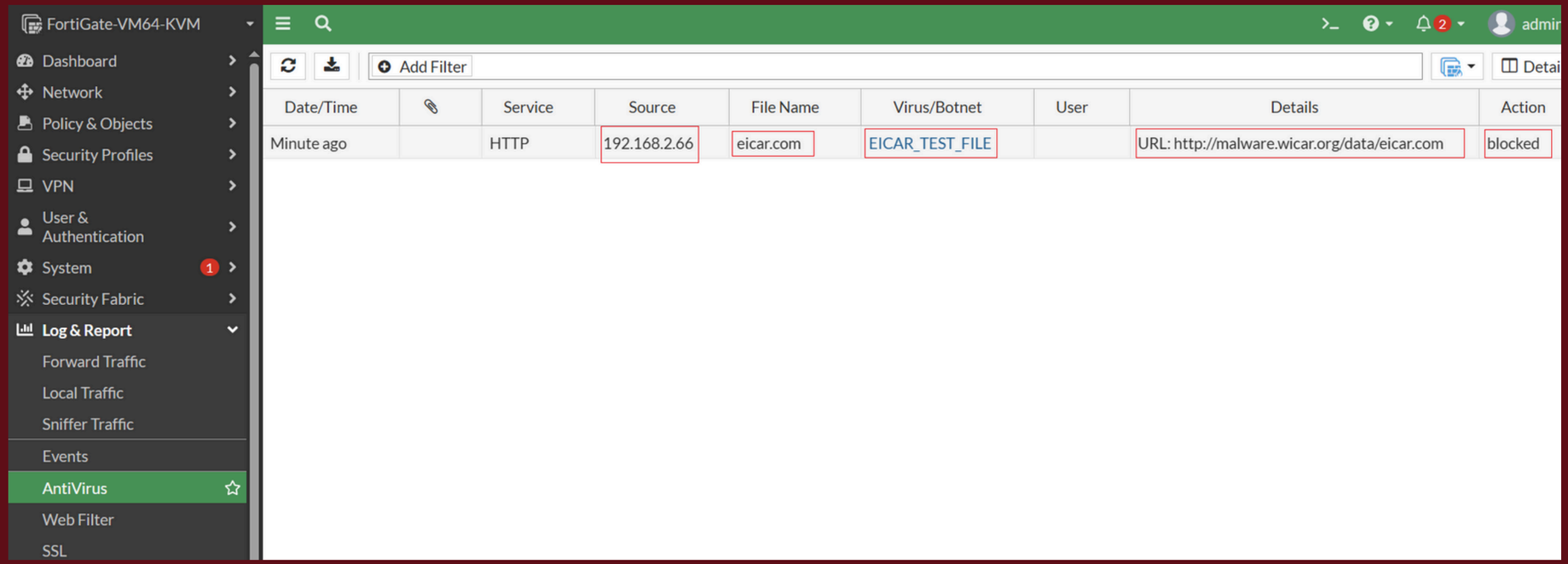
- Anti-Virus Profile Name: OUR-AV
- Default scan settings enabled
- Download inspection activated

ANTI-VIRUS



- EICAR test virus was downloaded
- FortiGate blocked the malicious file
- High security alert message was displayed

ANTI-VIRUS



- Malware detection is logged
- Source device IP is recorded
- Action taken: Blocked

MONITORING

- Security monitoring is done using:
- Web Filtering Logs
- Application Control Logs
- Anti-Virus Logs
- Real-time FortiGate reporting

CONCLUSION

- Network successfully segmented
- Users’ internet access is controlled
- Malicious websites and applications are blocked
- Malware is detected and prevented
- All actions are monitored using logs

THANK YOU!