

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

01 TOPOLOGY

02 IP & DHCP

03 POLICIES

04 WEB FILTER

05 APP CONTROL

TABLE OF CONTENT

06 ANTI-VIRUS

07 MONITORING

08 CONCLUSION

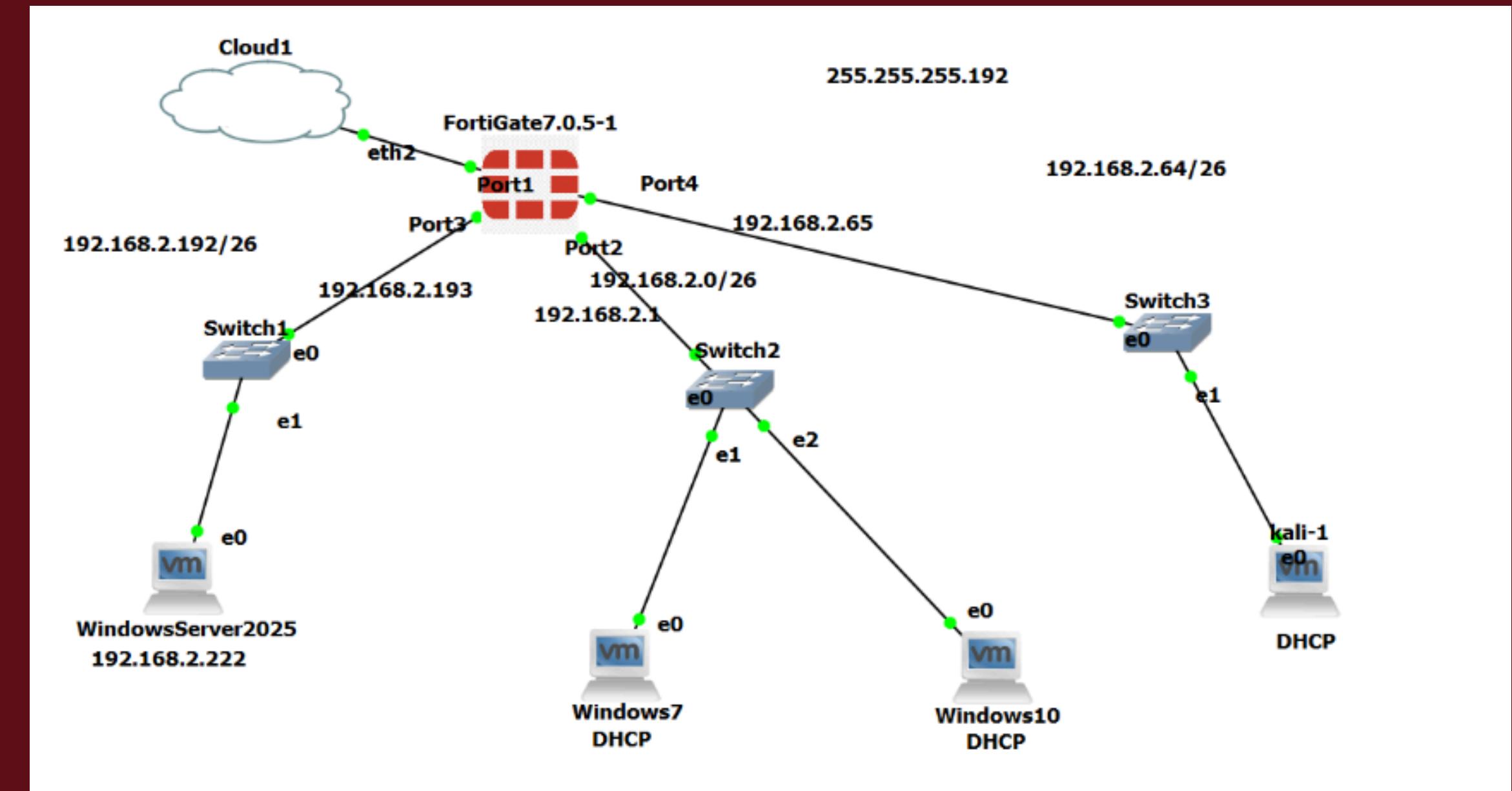
TOPOLOGY

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	802.3ad Aggregate	fortilink	Dedicated to FortiSwitch
Physical Interface 4	Physical Interface	DMZ-WEB (port3)	192.168.2.193/255.255.255.192
Physical Interface	Physical Interface	LAN-1 (port2)	192.168.2.1/255.255.255.192
Physical Interface	Physical Interface	LAN-2 (port4)	192.168.2.65/255.255.255.192
Physical Interface	Physical Interface	port1	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.

IP Range/Subnet ⑧		
	DMZ-WEB	192.168.2.192/26
	FABRIC_DEVICE	0.0.0.0/0
	FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
	LAN-1	192.168.2.0/26
	LAN2	192.168.2.64/26
	SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
	all	0.0.0.0/0
	none	0.0.0.0/32

POLICIES

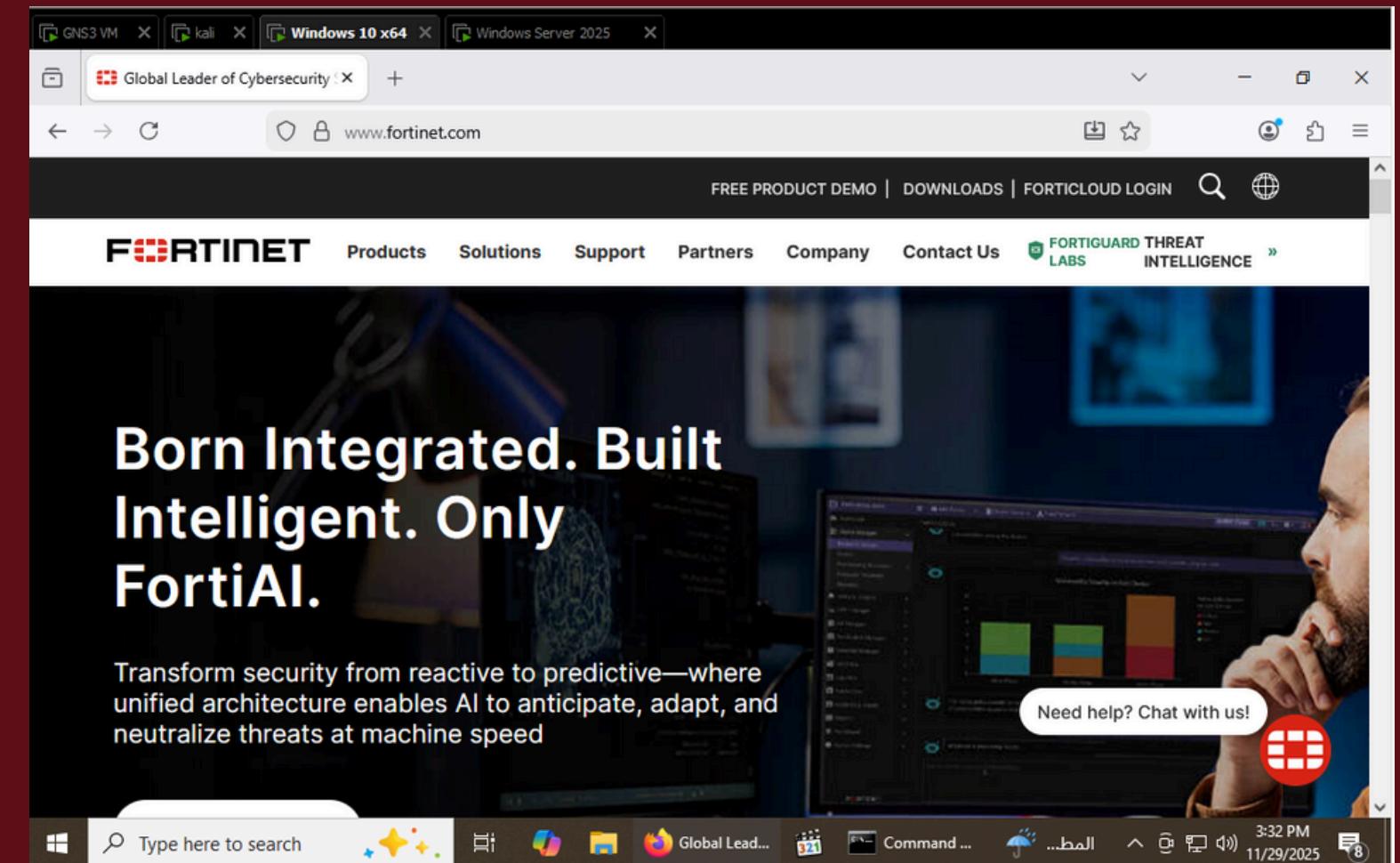
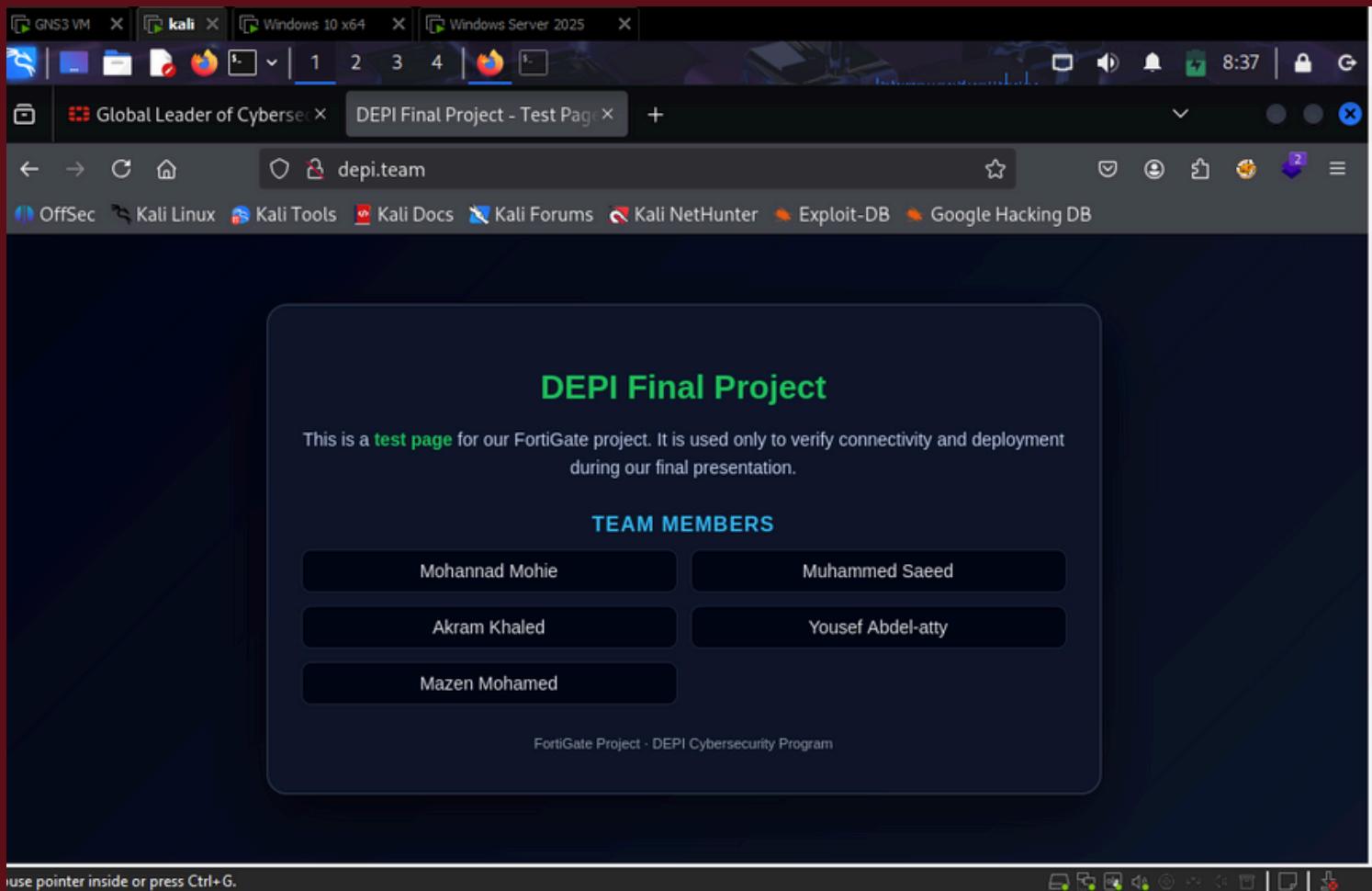
Five firewall policies
were created:

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	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								

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

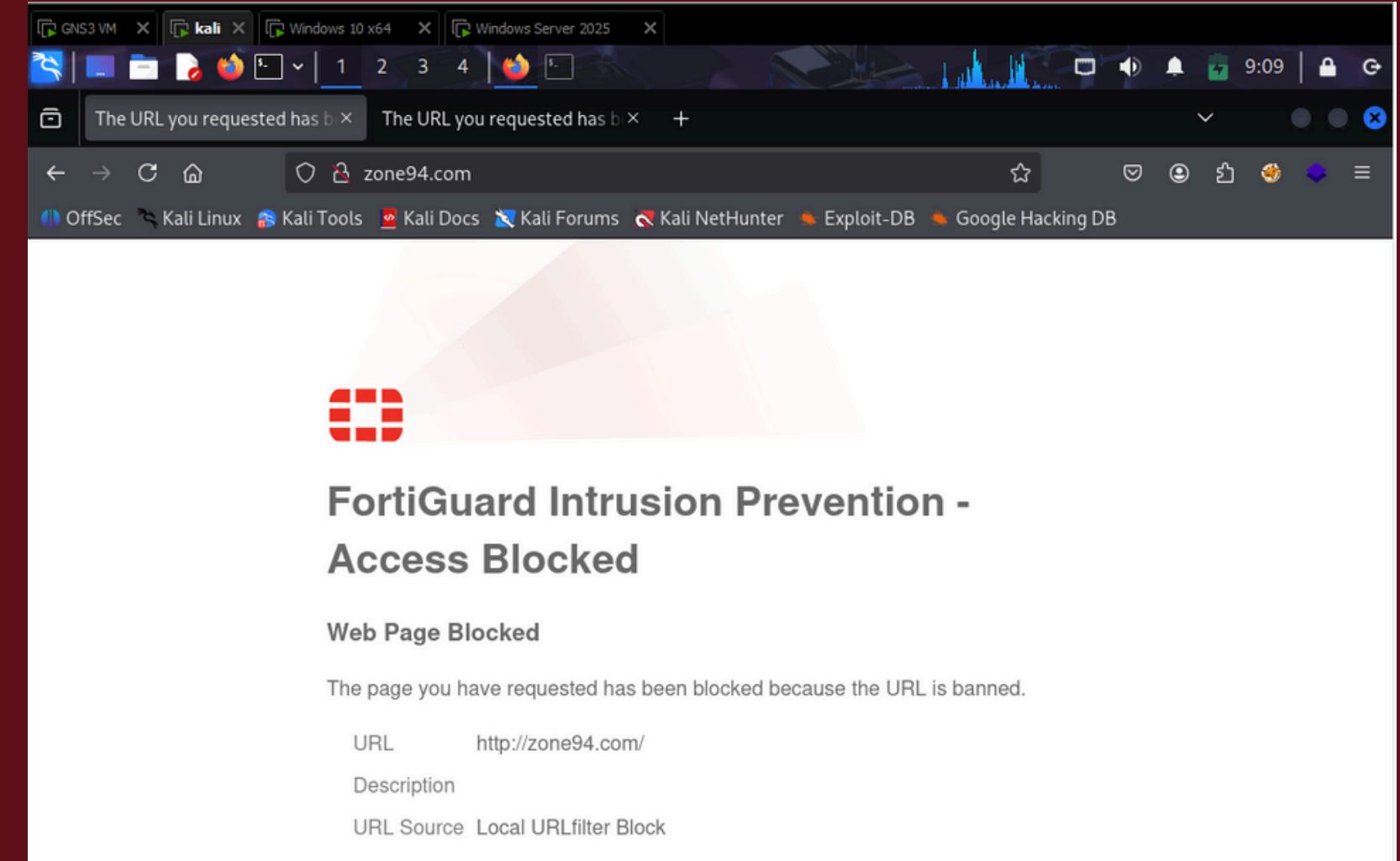
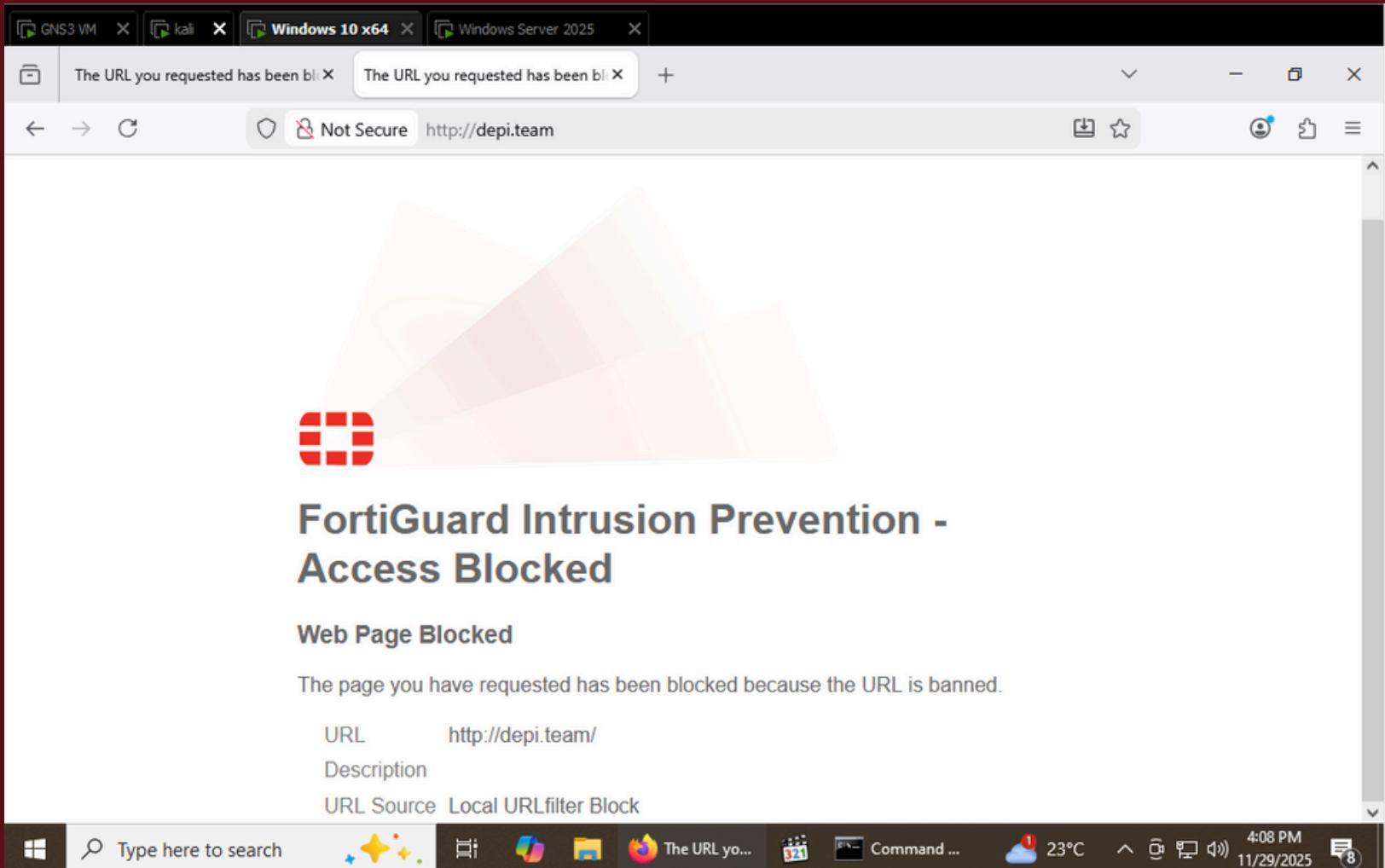
WEB FILTER

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:

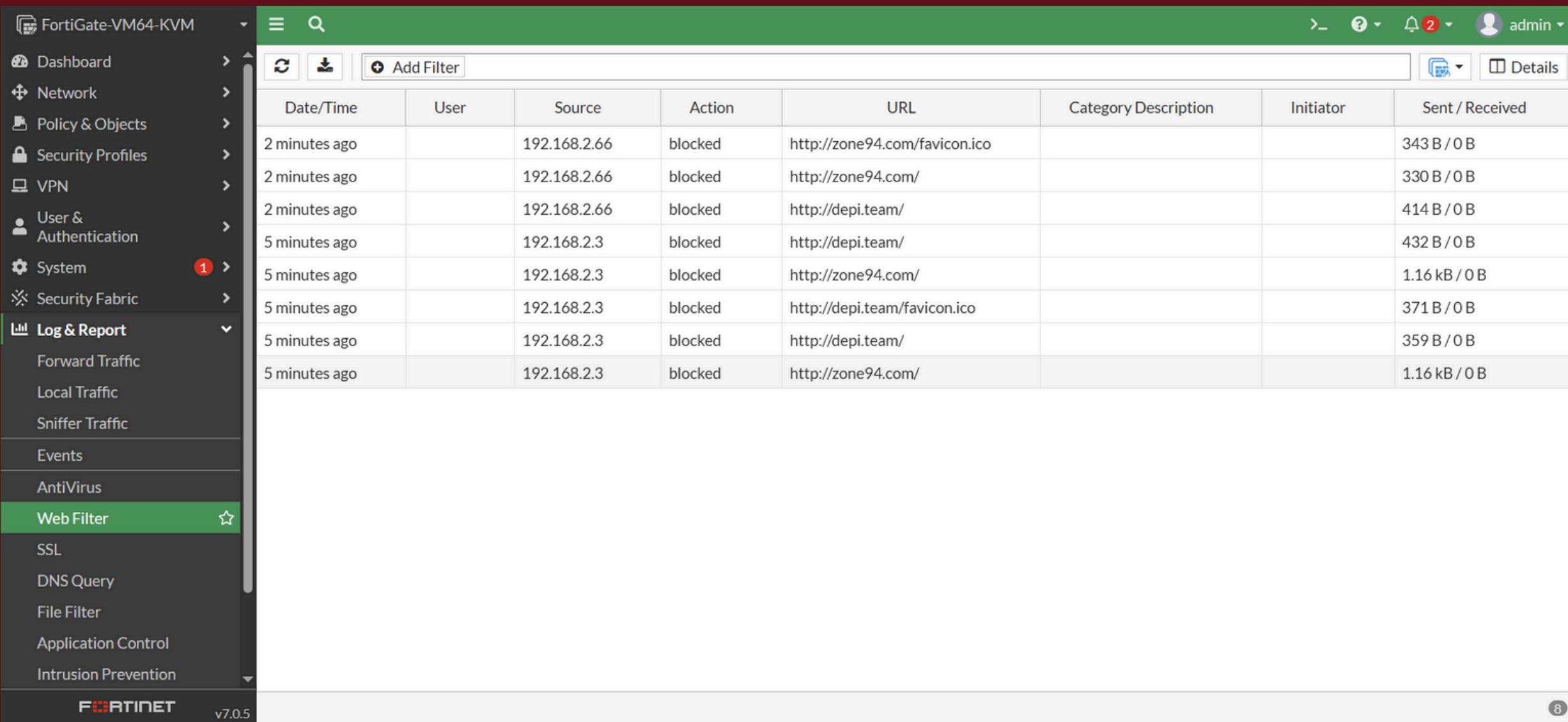
- Block-DEPI: Blocks depi.team
- Block-Web: Blocks zone94.com
- Filtering method: URL Filtering

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



The screenshot shows the FortiGate management interface with the 'Log & Report' section selected. Under 'Web Filter', a table displays a list of blocked web traffic entries. The columns are Date/Time, User, Source, Action, URL, Category Description, Initiator, and Sent / Received.

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

- 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:

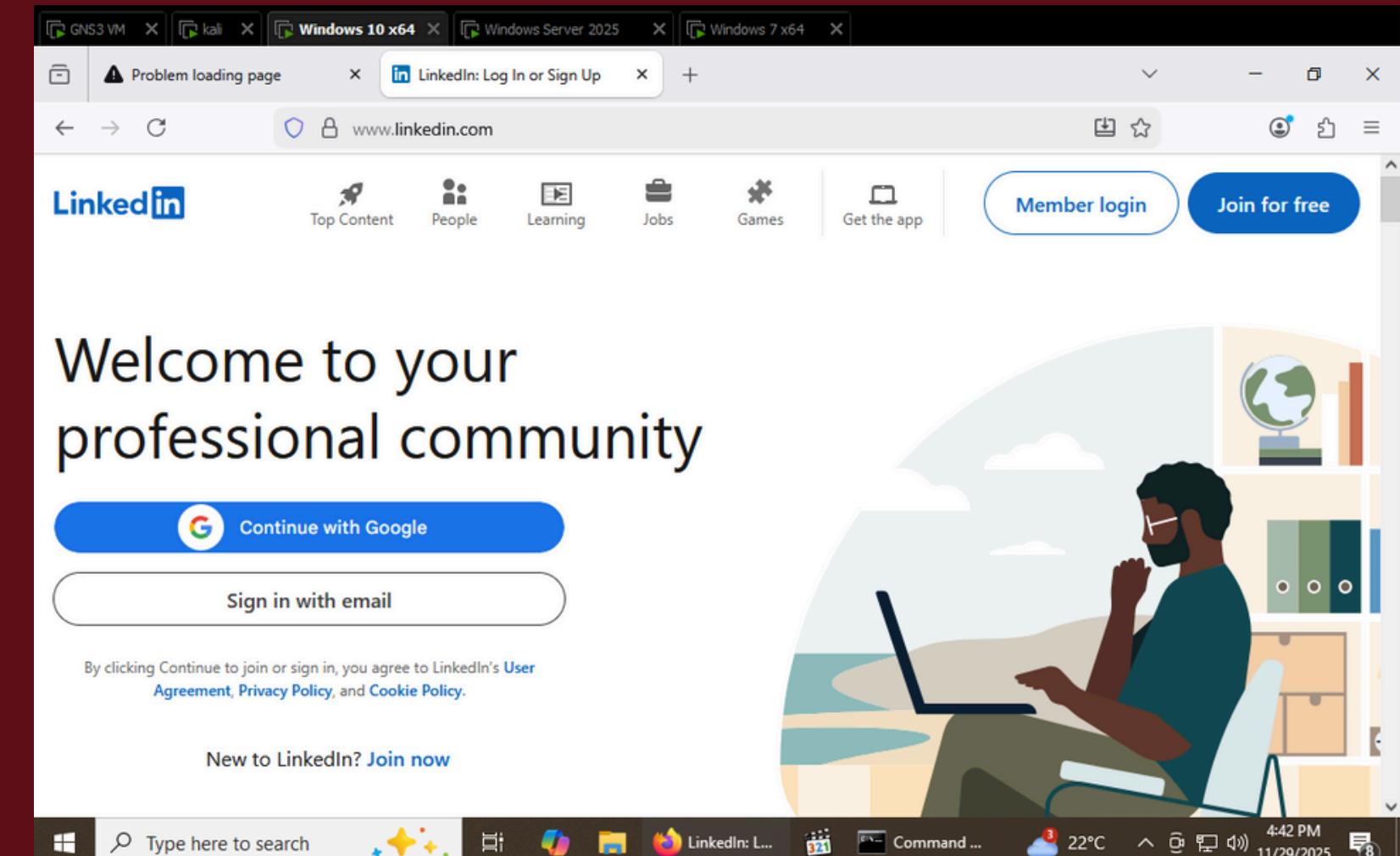
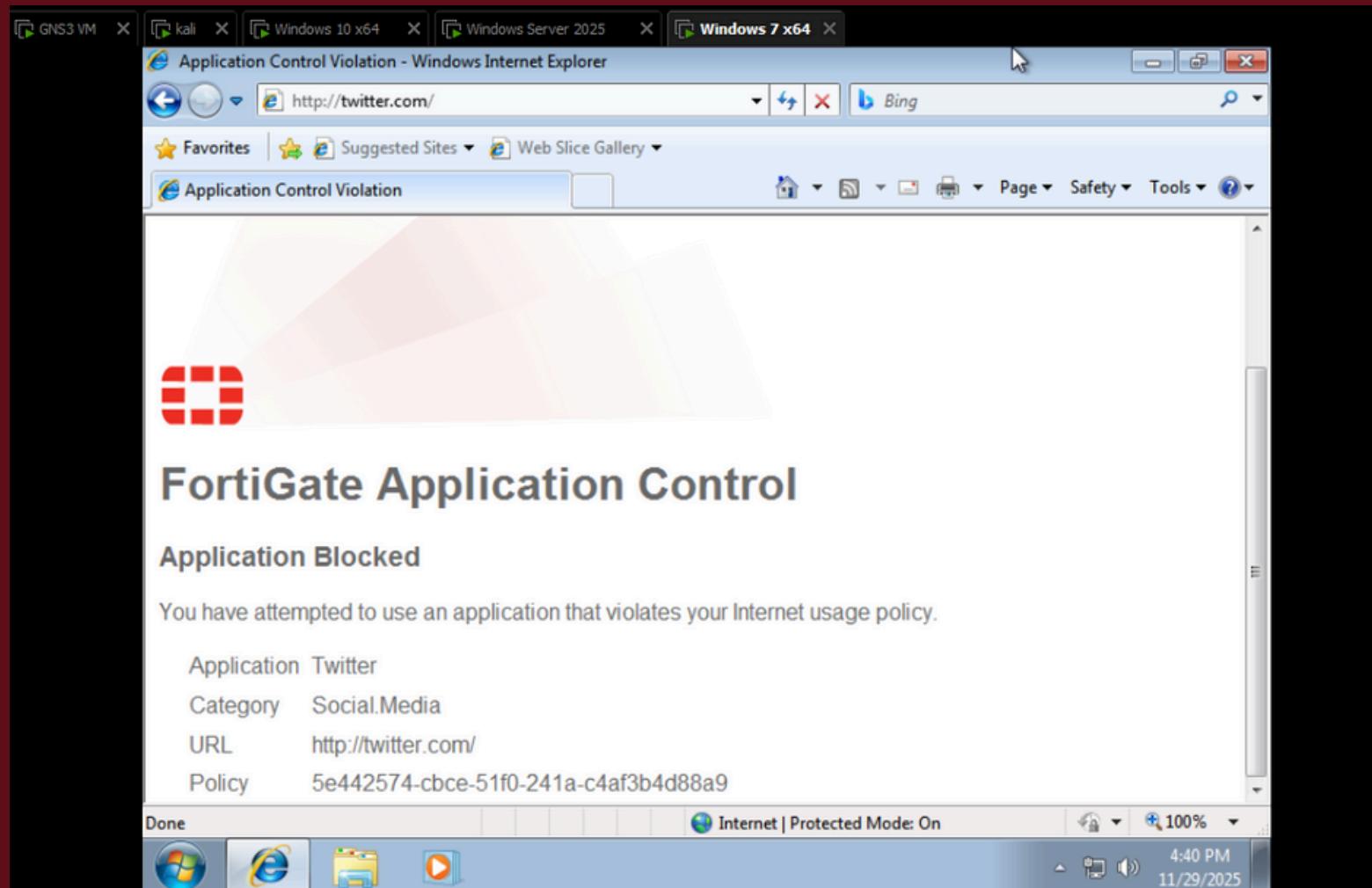
- Social Media
- Games
- Proxy
- P2P

APP CONTROL

The screenshot shows the 'Edit Application Sensor' page in the FortiManager interface. The left sidebar is a navigation menu with sections like Dashboard, Network, Policy & Objects, Security Profiles, and Application Control (which is selected). The main content area is titled 'Edit Application Sensor' and displays a message: '93 Cloud Applications require deep inspection. 0 policies are using this profile.' Below this, there are fields for 'Name' (set to 'Our-APP-Control') and 'Comments' (set to 'Monitor all applications. 25/255'). A 'Categories' section lists various application categories with counts: 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), VoIP (31), and Unknown Applications (checkbox checked). A red box highlights the 'Unknown Applications' category. At the bottom of the main panel, there is a 'Network Protocol Enforcement' toggle switch which is turned on. To the right of the main panel, there are several status and link buttons: 'Firmware & General Updates License' (Not Supported), 'Application Control Signatures Package' (Version 6.00741), 'Application Signatures' (View Application Signatures), 'Additional Information' (API Preview, References, Edit in CLI), and 'Documentation' (Online Help, Video Tutorials).

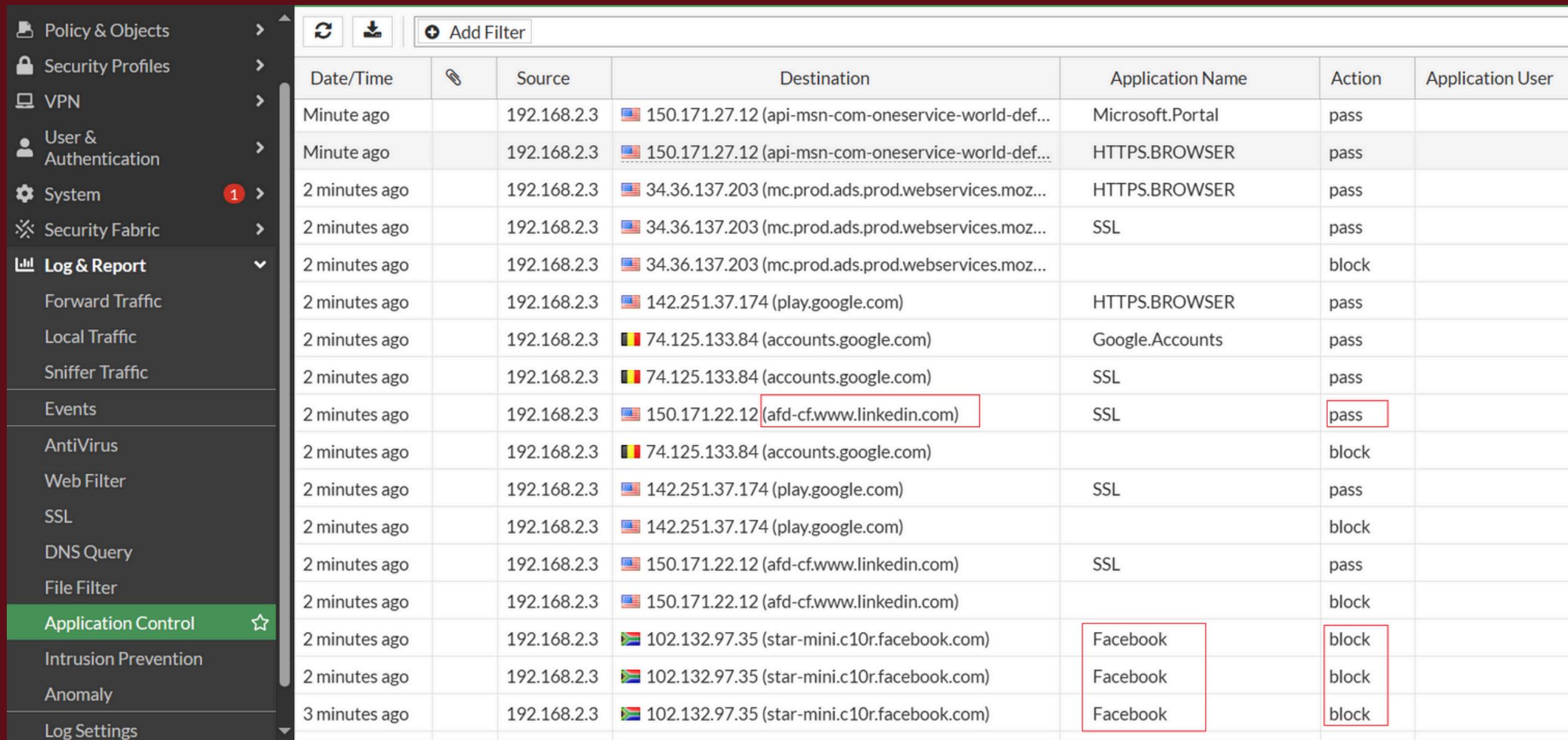
- Custom sensor created: Our-APP-Control
- LinkedIn allowed using Application Override
- Excessive bandwidth usage blocked
- Applications on non-default ports blocked

APP CONTROL



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

APP CONTROL



The screenshot shows a log table titled "Log & Report" under the "Application Control" section. The table has columns for Date/Time, Source, Destination, Application Name, Action, and Application User. The "Action" column includes "pass" and "block". Three rows of traffic from source 192.168.2.3 to destination 102.132.97.35 (Facebook) are highlighted with red boxes around the destination and action columns.

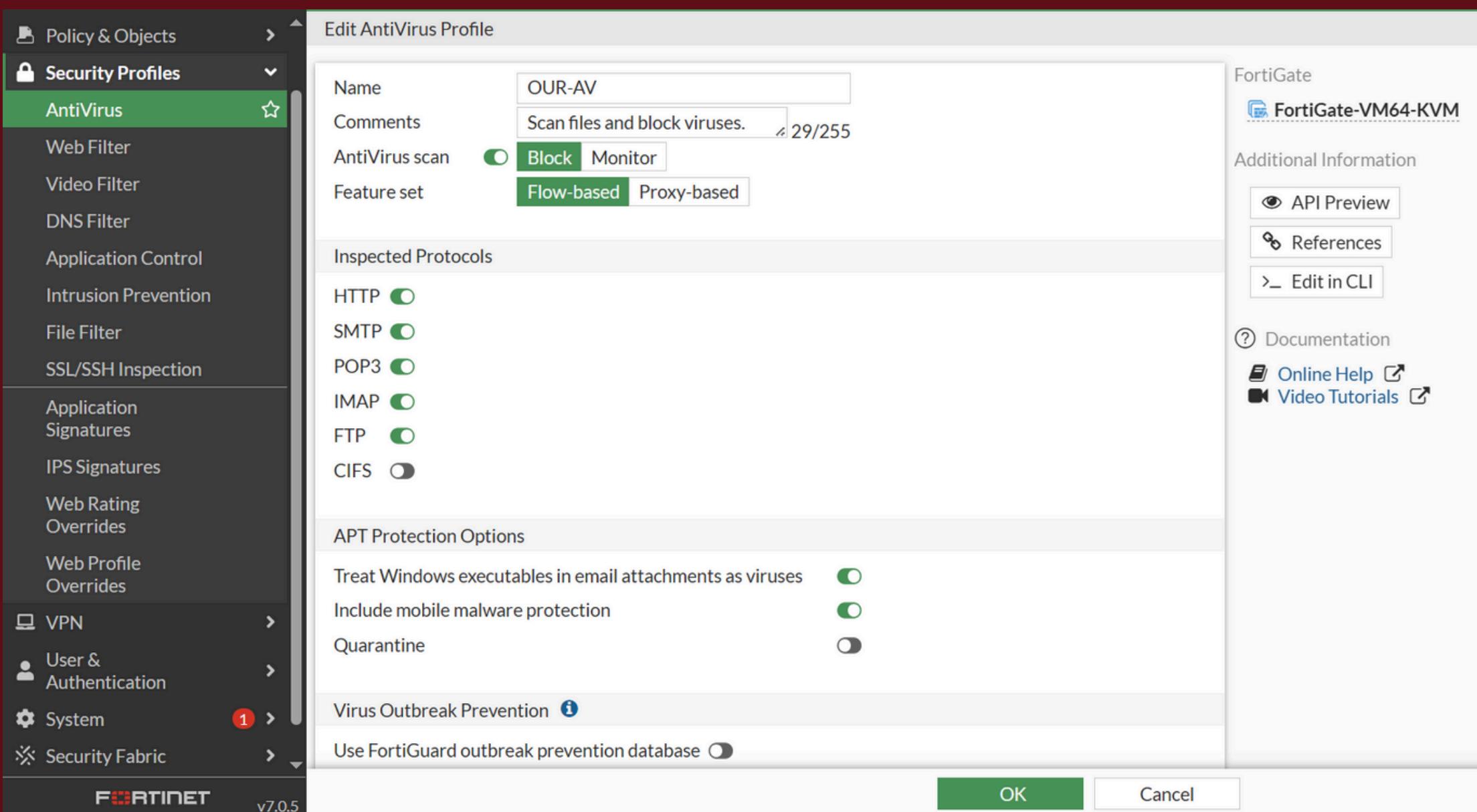
Date/Time	Source	Destination	Application Name	Action	Application User
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...)	Microsoft.Portal	pass	
Minute ago	192.168.2.3	150.171.27.12 (api-msn-com-oneservice-world-def...)	HTTPS.BROWSER	pass	
2 minutes ago	192.168.2.3	34.36.137.203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

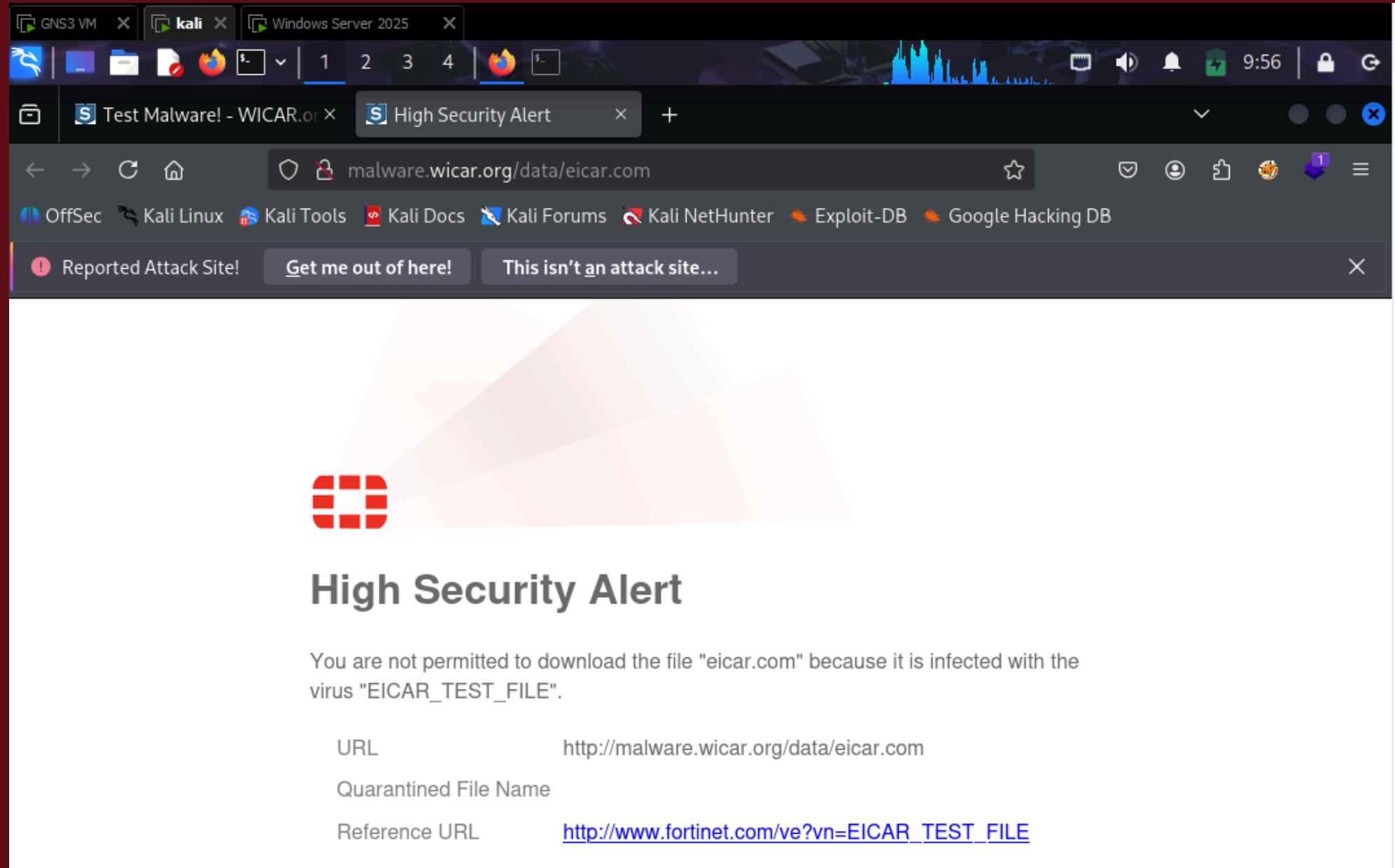
- Applied only to LAN-2
- Protect devices from malicious files
- Real-time malware detection

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

The screenshot shows the FortiGate management interface. The left sidebar navigation bar is visible, with the 'AntiVirus' option highlighted in green. The main content area displays a log entry in a table format. The table has columns: Date/Time, Service, Source, File Name, Virus/Botnet, User, Details, and Action. The entry details are: Date/Time: Minute ago, Service: HTTP, Source: 192.168.2.66, File Name: eicar.com, Virus/Botnet: EICAR_TEST_FILE, User: (empty), Details: URL: http://malware.wicar.org/data/eicar.com, Action: blocked. The 'Source' and 'File Name' fields are highlighted with red boxes.

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

- 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

FORTIGATE SECURITY PROFILES

THANK YOU!