رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Final Project-DEPI

FortiGate Security Configuration&Monitoring

Mohammed Gabriel

Ebraam Ibrahim Sobhey

Ganna Eslam Eldeep

Kenzy Yasser Helmy

Salma Yasser abdulmoneim

Sandra Hany Tadros

Ziad Ayman Rehan

Supervised by: Eng.Mina Moheb

Content

Introduction:

In this project, a complete FortiGate next-generation firewall deployment was designed, configured, and monitored to provide multi-layer network security. The work was divided across several key security features: Application Control, Antivirus, Web Filtering, Firewall Policies, Logging, Threat Weight, and FortiView monitoring.

During Week 2, the focus was on building and applying the main security profiles, including the AppControl_profile, Antivirus profG, and Ziad-WebFilter, as well as configuring global logging and firewall policies for LAN-to-WAN and WAN-to-LAN traffic. In Week 3, real and simulated traffic was generated to verify that these configurations were working correctly by analyzing Forward Traffic logs, Web Filter logs, Application Control logs, and Antivirus security events. Finally, in Week 4, all configurations and monitoring results were documented, analyzed, and evaluated to demonstrate how FortiGate can effectively control applications, filter web traffic, detect malware, and provide full visibility into network activity in a real-world environment

1.2 Configuration Steps

Step 1 – Login

Login to FortiGate GUI using:

https://<fortigate-ip>

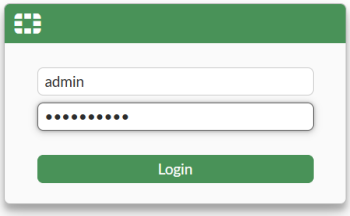


Figure1 :Fortigate login

Step 2 – Create Application Control Profile

Navigate to:

Security Profiles → Application Control → Create New

Name the profile:

AppControl_profile

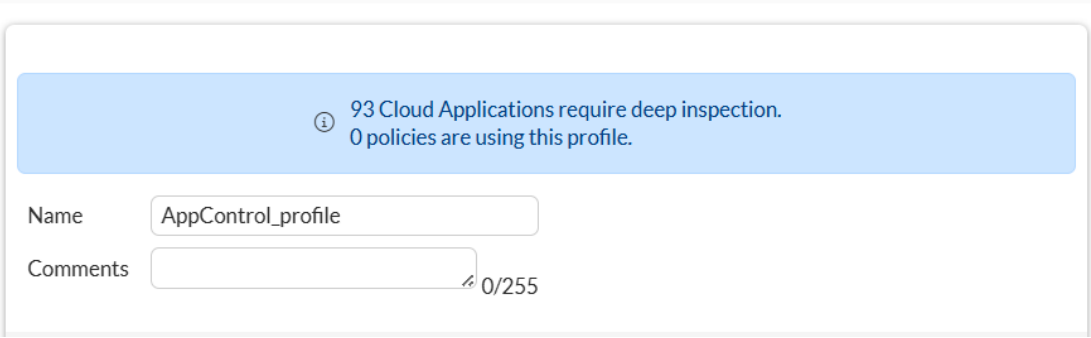


Figure2 :AppControl_profile

1.3 Category Actions

Configure the following categories:

Category – Action

• Social Media → Monitor
• Video / Audio → Monitor
• Collaboration → Monitor
• Mobile Apps → Monitor
• Games → Block
• P2P → Block
• Proxy → Block
• Unknown Apps → Allow / Monitor
• High-Risk Applications → Block
• Remote Access Tools → Block
• Email & Messaging Apps → Monitor
• Software Updates → Allow

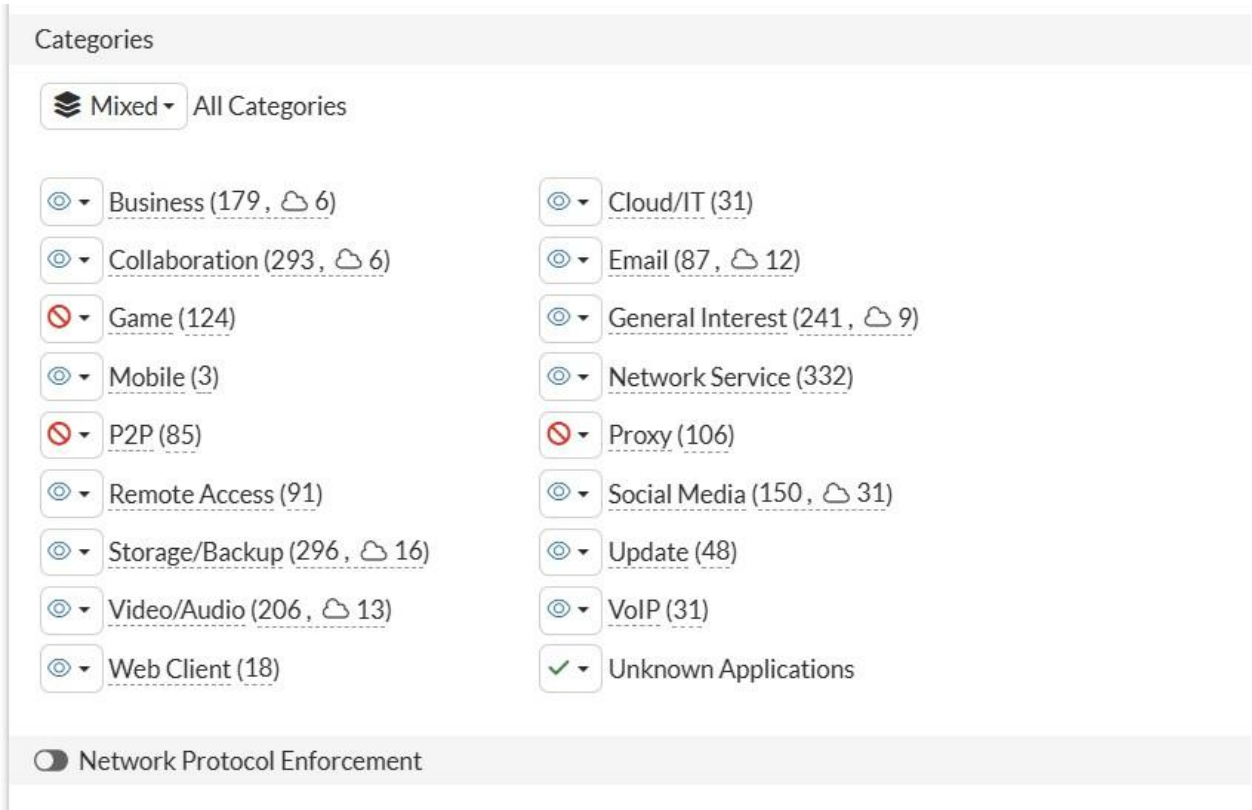


Figure 3:Category Actions

1.4 Application Overrides

Go to:
Application & Filter Overrides → Create New
Add the following applications:

Application – Action – Logging

- Facebook → Block → Enabled
- Facebook.App → Block → Enabled
- Instagram → Block → Enabled
- YouTube → Block → Enabled
- Telegram → Block → Enabled
- Reddit → Block → Enabled
- Steam → Block → Enabled
- EpicGames → Block → Enabled
- Google Drive → Monitor → Enabled

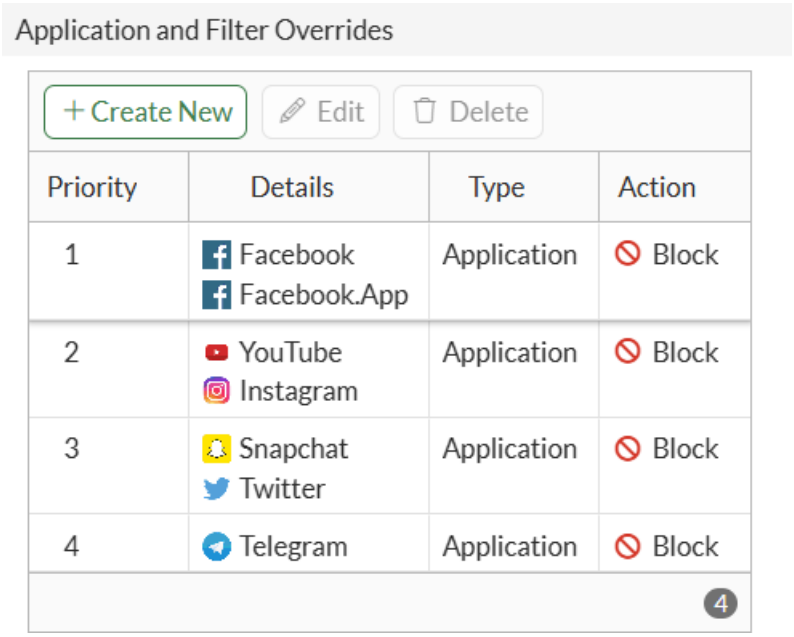


Figure4 :Application Overrides

1.5 Options Configuration

In **Options**, enable the following:

- Allow and Log DNS Traffic = ON
- Replacement messages for HTTP-based applications = ON
- Block applications on non-default ports = OFF

1.6 Save Configuration

Click **OK** to save the profile.

1.7 Screenshots to Include

• Application Control profile overview
• Categories actions page
• Logging options page
• Application Overrides list

1.8 Expected Behavior

When this Application Control profile is attached to a firewall policy:

- Social media & streaming applications will be monitored
- Games, P2P, and Proxy applications will be blocked
- Facebook, Instagram, and YouTube will always be blocked due to overrides
- All allowed and blocked application events will be logged for analysis

1.9 Conclusion

The **AppControl_profile** was fully configured and documented.
Logging is enabled, categories and overrides are applied correctly, and the profile is ready to be attached to the firewall policy

2. Logging & Threat Weight – Week 2

2.1 Introduction

This task covers configuring logging and threat-weight features to ensure accurate monitoring, scoring, and visibility of all security events on the FortiGate firewall .

2.2 Global Log Settings

Navigate to:
Log & Report → Log Settings → Global Settings
Event Logging
• Event Logging: **Enabled (All)**
Ensures all system and network events are logged.
Local Traffic Logging

- Local-in Logging: **Enabled**
- Local-out Logging: **Enabled**

This allows monitoring of:

- Local management traffic
- Outbound system traffic

Syslog Logging
• Syslog Logging: **Disabled**

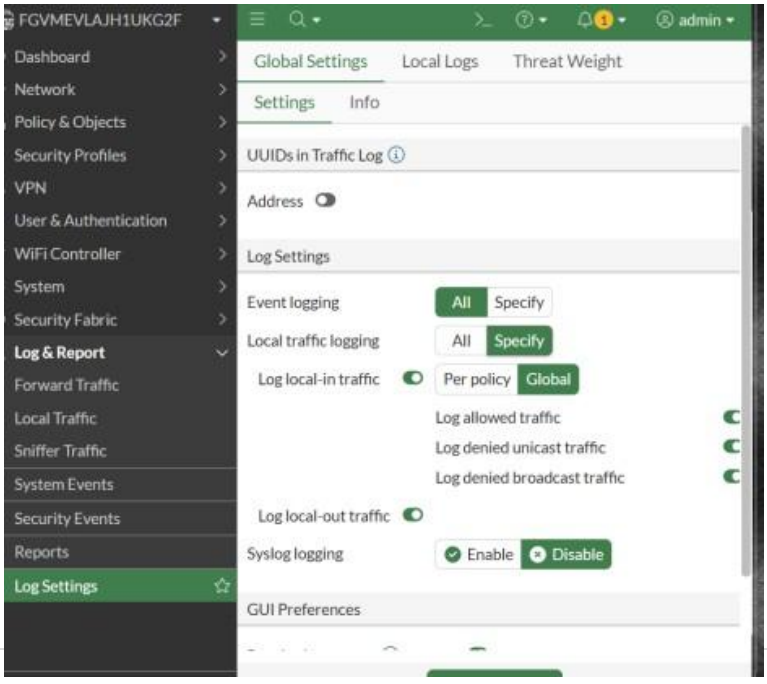


Figure5 :SyslogLogging

2.3 Threat Weight Configuration

Navigate to:

Security → Threat Weight

Enable Threat Weight Logging

• Log Threat Weight: **Enabled**

Application Protection Categories

Category – Weight:

• P2P → Low

• Proxy → Medium

Intrusion Prevention – Severity Weight

Severity Level – Assigned Weight:

• Informational → Off

• Low → Low

• Medium → Medium

• High → High

• Critical → Critical

• Botnet Communications → Critical

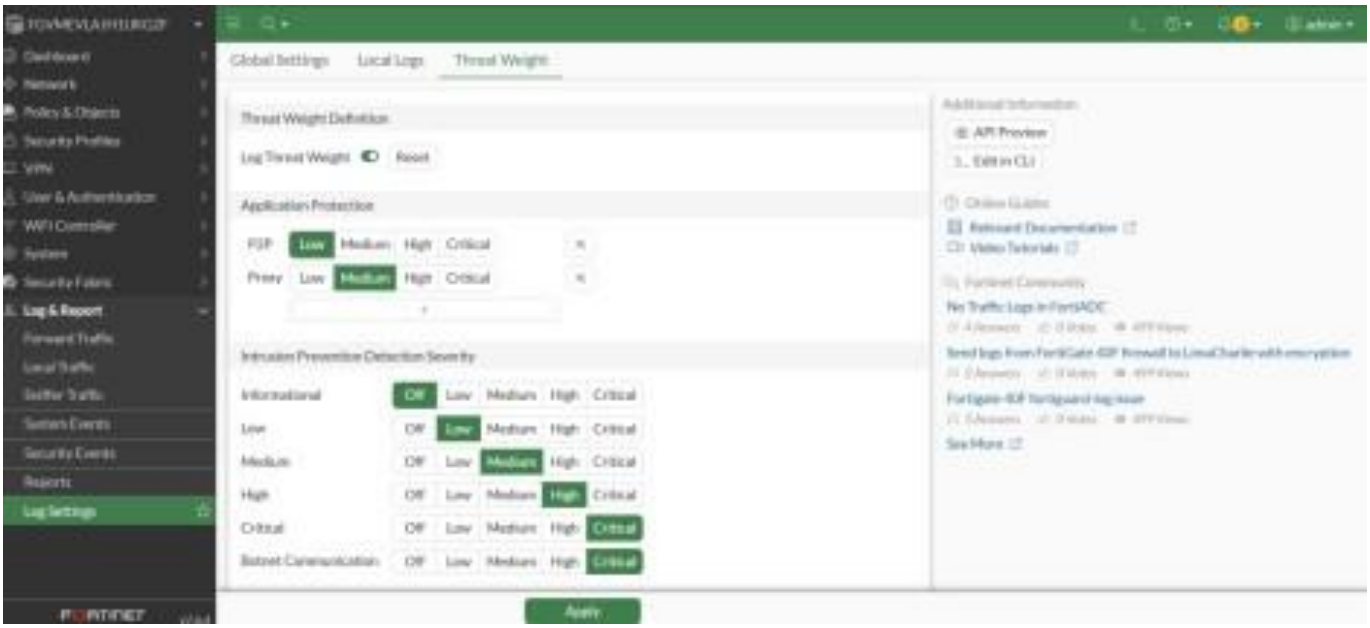


Figure 6:Severity Weights

2.4 Local Logs Verification

Navigate to:

Log & Report → Local Logs

Verify that:

• Traffic logs appear normally

• Event logs are generated correctly

• Threat-weight scores appear when threats occur

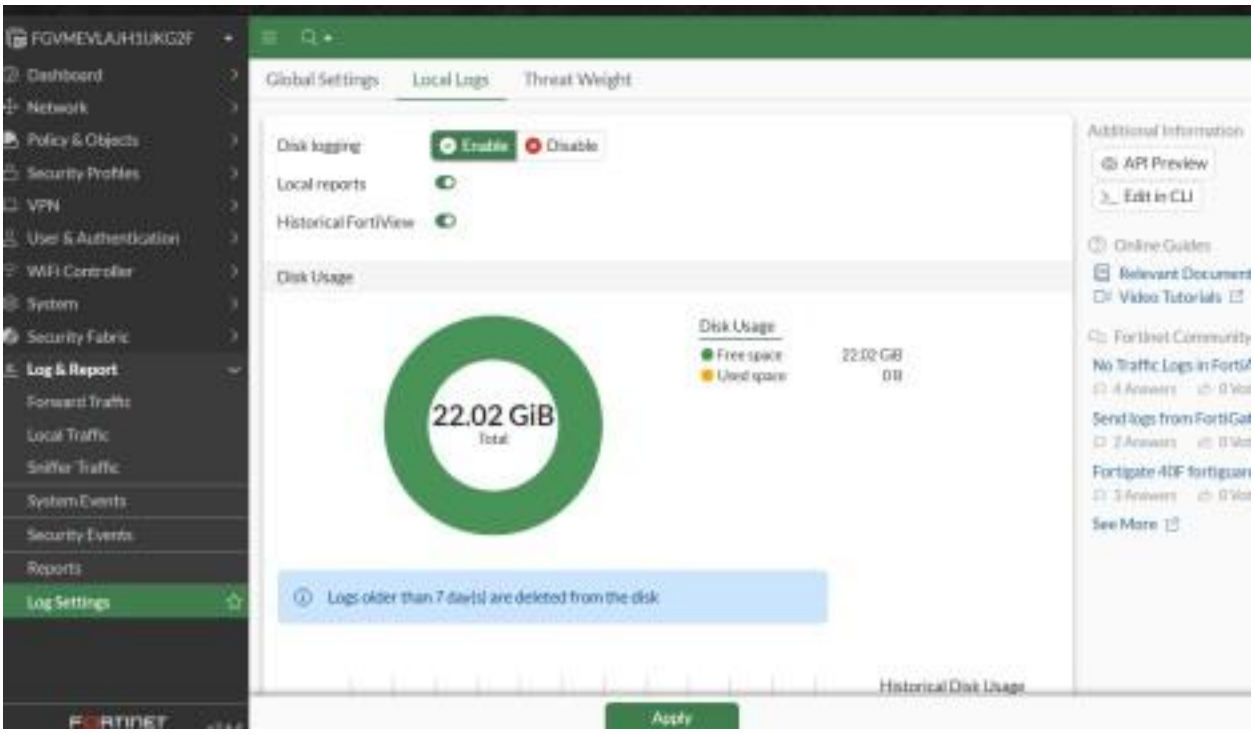


Figure 7:Local Logs Verification

2.5 Conclusion – Logging & Threat Weight

Successfully configured:

- All global logging options
- Local-in / Local-out traffic logging
- Threat weight scoring
- Severity mappings
- Application category weights

This ensures accurate visibility and proper prioritization of threats.

3. Monitoring & Reporting – Application Control (Week 3)

3.1 Introduction

During Week 3, the focus was on monitoring the behavior of the Application Control profile during real traffic inspection.

Real traffic was generated from an Ubuntu machine connected on **port2 (LAN)**, and multiple dashboards were reviewed to verify application detection, blocking, and logging.

3.2 FortiView & Log Sections Overview

Top Applications

FortiView showed detected applications such as:

- YouTube
- Facebook
- Google services
- DNS/HTTP
- SSL

Applications were categorized under:

- Social Media
- Streaming
- Web Services
- Network Services

All Sessions View

Displayed detailed real-time session information:

- Source & destination IPs
- Application signatures
- Protocols & ports
- Bytes sent/received
- Packet count
- Session duration

FortiView Sessions

now

End sessions | Search filterable columns

Source	Device	Destination Address	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	49605	53	418 B	2	2m 49s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	50405	53	184 B	2	50s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	44285	53	368 B	2	1m 2s
192.168.2.50	ebraam-VMware-Virtual-Platform	142.251.37.174	YouTube	tcp	52294	443	224 B	4	9s
192.168.2.50	ebraam-VMware-Virtual-Platform	34.107.243.93	HTTPS.BROWSER	tcp	49888	443	4.63 kB	23	13m 11s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	49138	53	364 B	2	2m 40s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	50544	53	196 B	2	50s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	36100	53	273 B	2	50s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	36106	53	364 B	2	32s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	39384	53	290 B	2	2m 49s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	48308	53	368 B	2	2m 49s
192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	udp	48300	53	184 B	2	2m 51s
192.168.2.50	ebraam-VMware-Virtual-Platform	172.217.171.206	YouTube	tcp	38054	443	224 B	4	1m 2s

Figure 8:FortiView – All Sessions

Application Control Logs

The logs showed:

- Allowed or blocked actions
- Category (Video/Audio, Social Media, etc.)
- Policy ID used
- Action taken
- Risk level

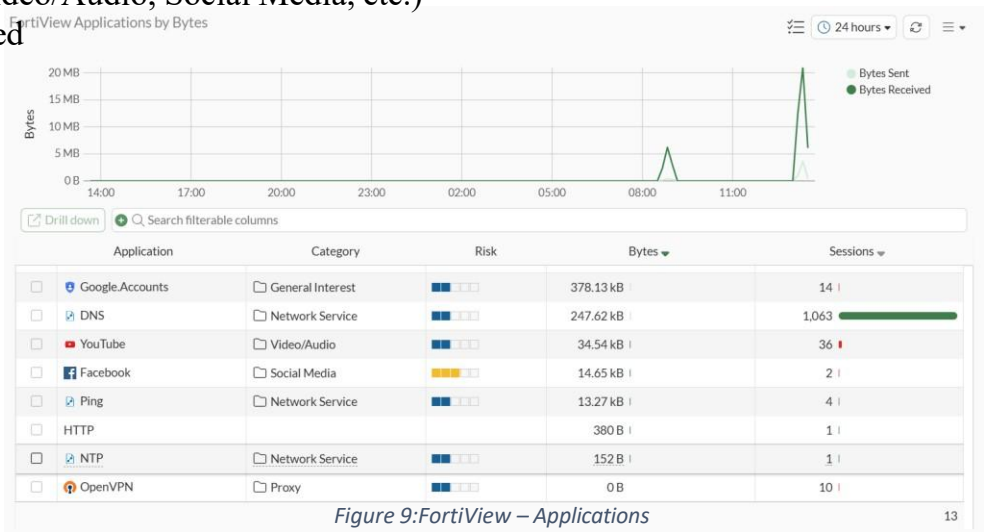


Figure 9:FortiView – Applications

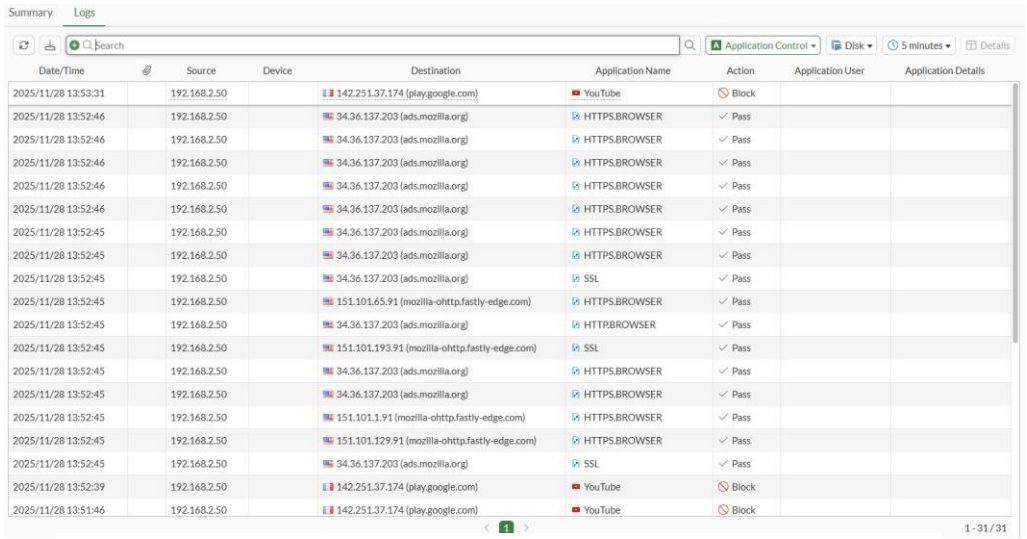


Figure10 :Application Control Logs

3.3 Policy Statistics & Internal Counters

Policy Hit Counters

• The LAN2 → WAN1 outbound policy showed increasing hit counts.

→ Confirms that traffic is correctly passing through the policy with the AppControl profile attached.

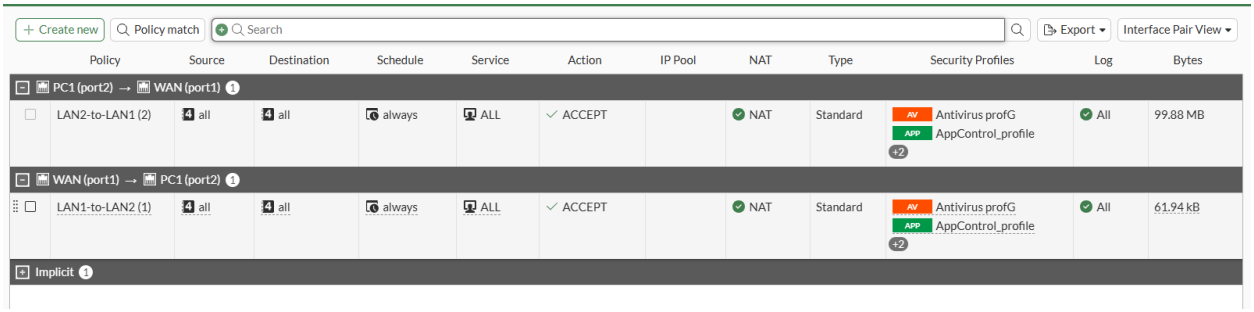


Figure 11:Firewall Policy Statistics

Byte Counters

• Logs showed MB-level data transfer.

→ Proves active traffic inspection.

Internal Resource Counters

System Resources dashboard showed:

- CPU usage: ~9%
- Memory usage: ~68%
- Active sessions: ~23
- Interface throughput changing based on traffic load

This confirms proper firewall processing and inspection.

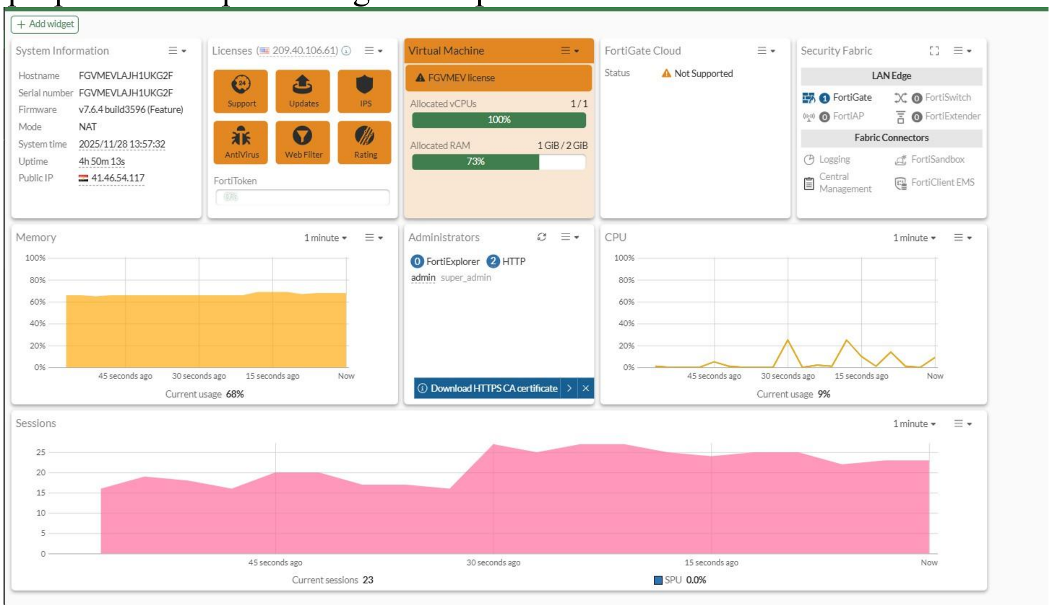


Figure 12:System Resource Counters

3.4 Conclusion

Week 3 monitoring confirms that:

- Application Control properly detects applications
- Blocked apps (Facebook, YouTube ,.e.g) are logged
- Allowed applications are monitored
- Policy, session details, and application categories appear correctly

The system behaves exactly as expected under real traffic.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2025/11/28 13:55:45	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (96 B / 189 B)	LAN2-to-LAN1 (2)
2025/11/28 13:55:45	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (72 B / 141 B)	LAN2-to-LAN1 (2)
2025/11/28 13:55:45	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (84 B / 184 B)	LAN2-to-LAN1 (2)
2025/11/28 13:55:45	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (84 B / 232 B)	LAN2-to-LAN1 (2)
2025/11/28 13:55:20	192.168.2.50	ebraam-VMware-Virtual-Platform	185.125.190.97 (connectivity-check.ubuntu.com)	HTTP.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:55:03	192.168.2.50	ebraam-VMware-Virtual-Platform	142.251.37.174 (play.google.com)	YouTube	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:54:58	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (86 B / 422 B)	LAN2-to-LAN1 (2)
2025/11/28 13:54:12	192.168.2.50	ebraam-VMware-Virtual-Platform	142.251.37.174 (play.google.com)	YouTube	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:30	192.168.2.50	ebraam-VMware-Virtual-Platform	8.8.8.8	DNS	Accept (86 B / 278 B)	LAN2-to-LAN1 (2)
2025/11/28 13:53:19	192.168.2.50	ebraam-VMware-Virtual-Platform	142.251.37.174 (play.google.com)	YouTube	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:16	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:16	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:16	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:16	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	SSL	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	151.101.65.91 (mozilla-ohttp.fastly-edge.com)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	151.101.193.91 (mozilla-ohttp.fastly-edge.com)	SSL	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)
2025/11/28 13:53:15	192.168.2.50	ebraam-VMware-Virtual-Platform	34.36.137.203 (ads.mozilla.org)	HTTPS.BROWSER	Deny (Deny: UTM Blocked)	LAN2-to-LAN1 (2)

1 - 39 / 39

Figure13 :Forward Traffic Logs

4. FortiGate Antivirus – Monitoring Report (Week 3)

4.1 Introduction

This report covers the verification of **Antivirus profG**, ensuring it detects malware, blocks malicious files, and logs events correctly in **Forward Traffic** and **Security Events**.

4.2 Generating Traffic for Antivirus Scanning

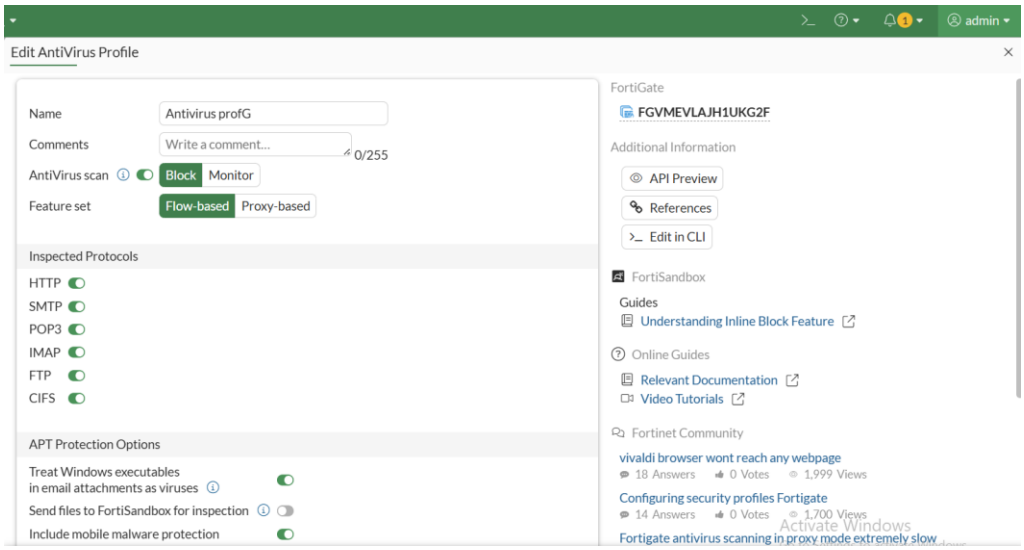
Malware Test Using FTP

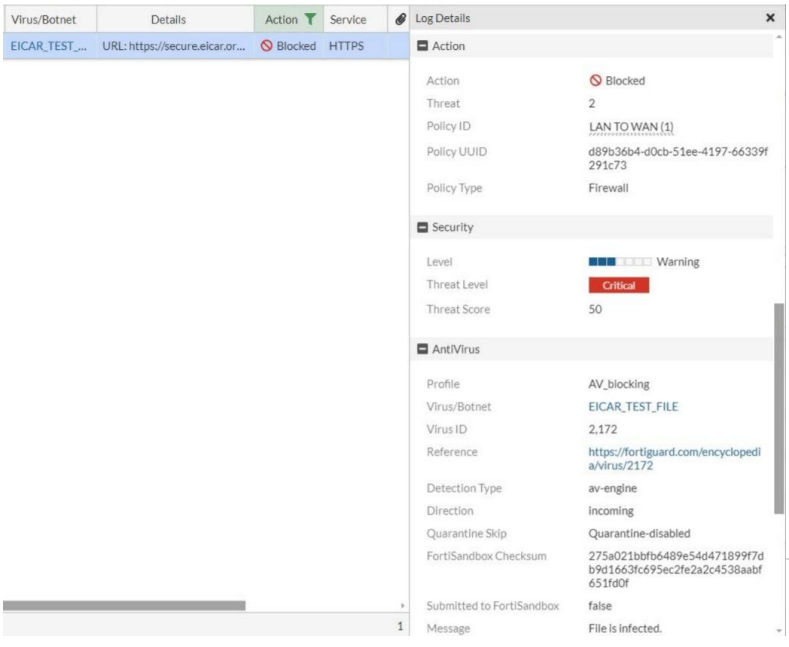
Using FileZilla from HQ-PC-1:

- Connected to the Linux FTP server
- Attempted to download **eicar.com** (malware test file)
- The download failed and the connection was reset

Expected behavior in flow-based mode:

- Malicious sessions are terminated immediately
- A replacement message is displayed
-
- The antivirus engine blocks the transfer before the file reaches the user





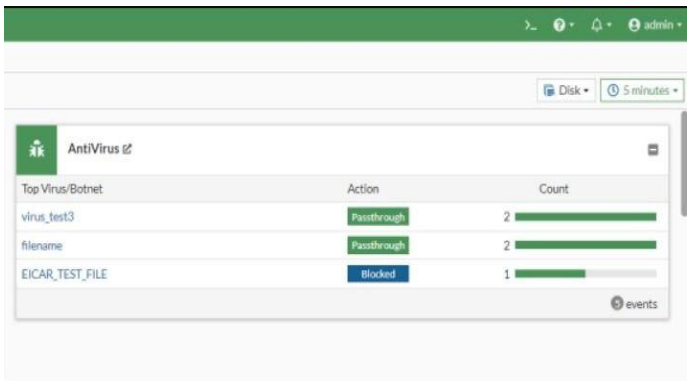


Figure 14:Monitoring Logs on FortiGate

4.3 Monitoring Logs on FortiGate

Forward Traffic Logs

Path:

Log & Report → Forward Traffic

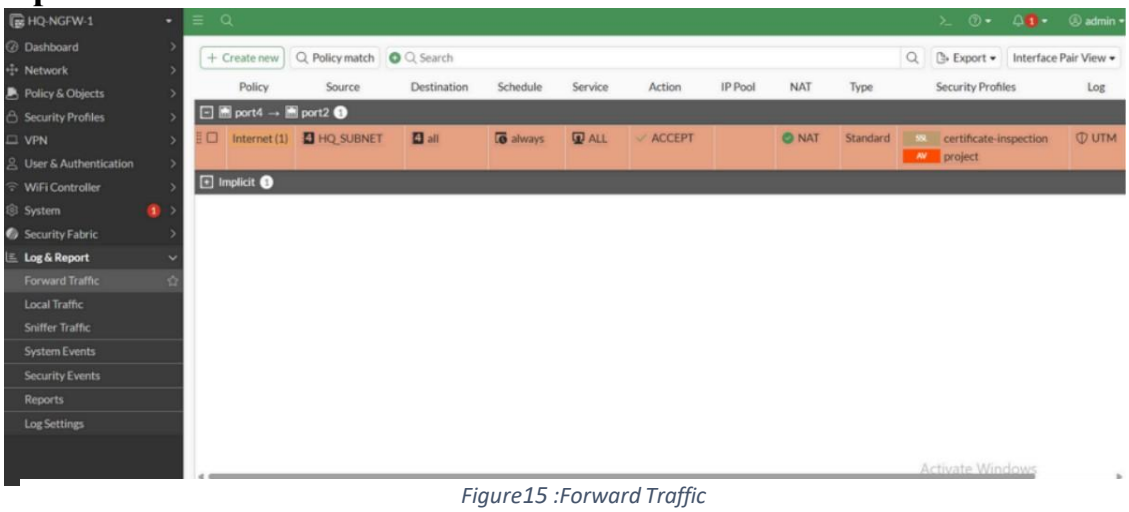


Figure15 :Forward Traffic

Logs showed:

- Source device: HQ-PC-1
- Destination: Linux FTP server
- Protocol: FTP
- Action: Blocked / Reset
- Security profile: Antivirus profG
- Detected threat: EICAR Test File
- Policy: Internet policy

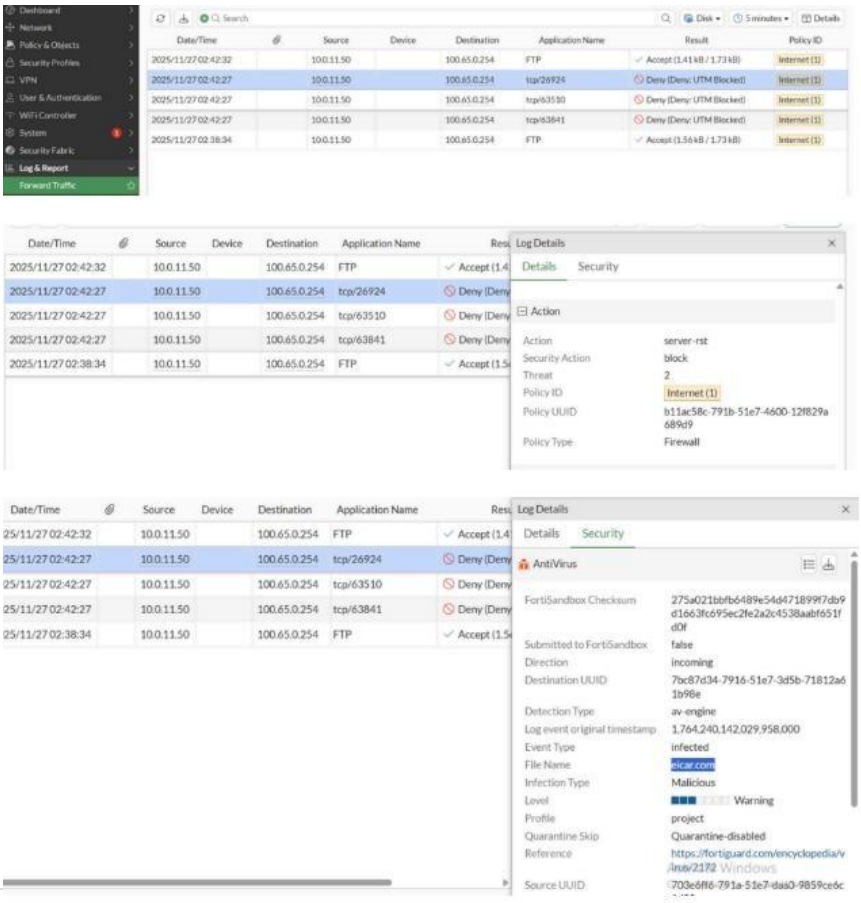


Figure16 :Log Details

Antivirus Security Logs

Path:

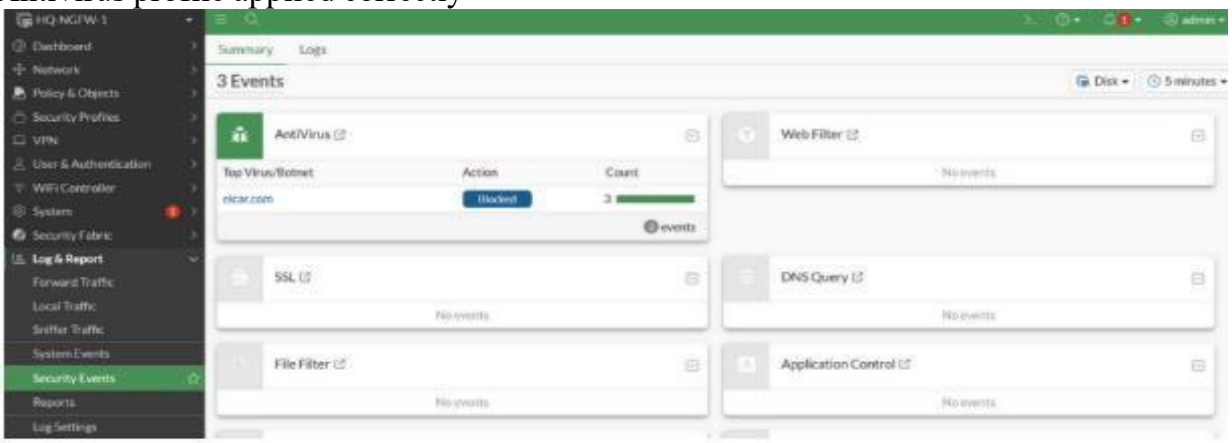
Log & Report → Security Events → Antivirus

Included details:

- Virus name: EICAR_TEST_FILE
- File name: eicar.com
- Action: Block
- Mode: Flow-Based
- Protocol: FTP
- Additional classification info

Logs confirm:

- Correct threat detection
- Session terminated immediately
- Antivirus profile applied correctly



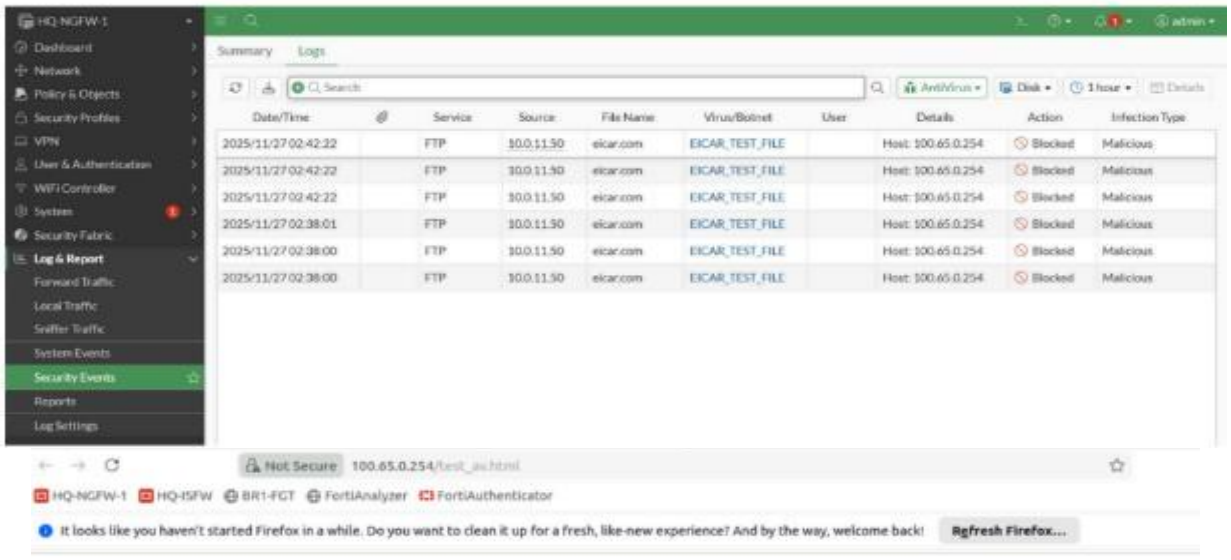


Figure17 :Antivirus Security Logs

4.4 Log Interpretation

Confirmed indicators:

- Malware detection is accurate
- Correct profile enforcement
- Expected reset behavior in flow-based scanning
- FTP protocol was scanned successfully

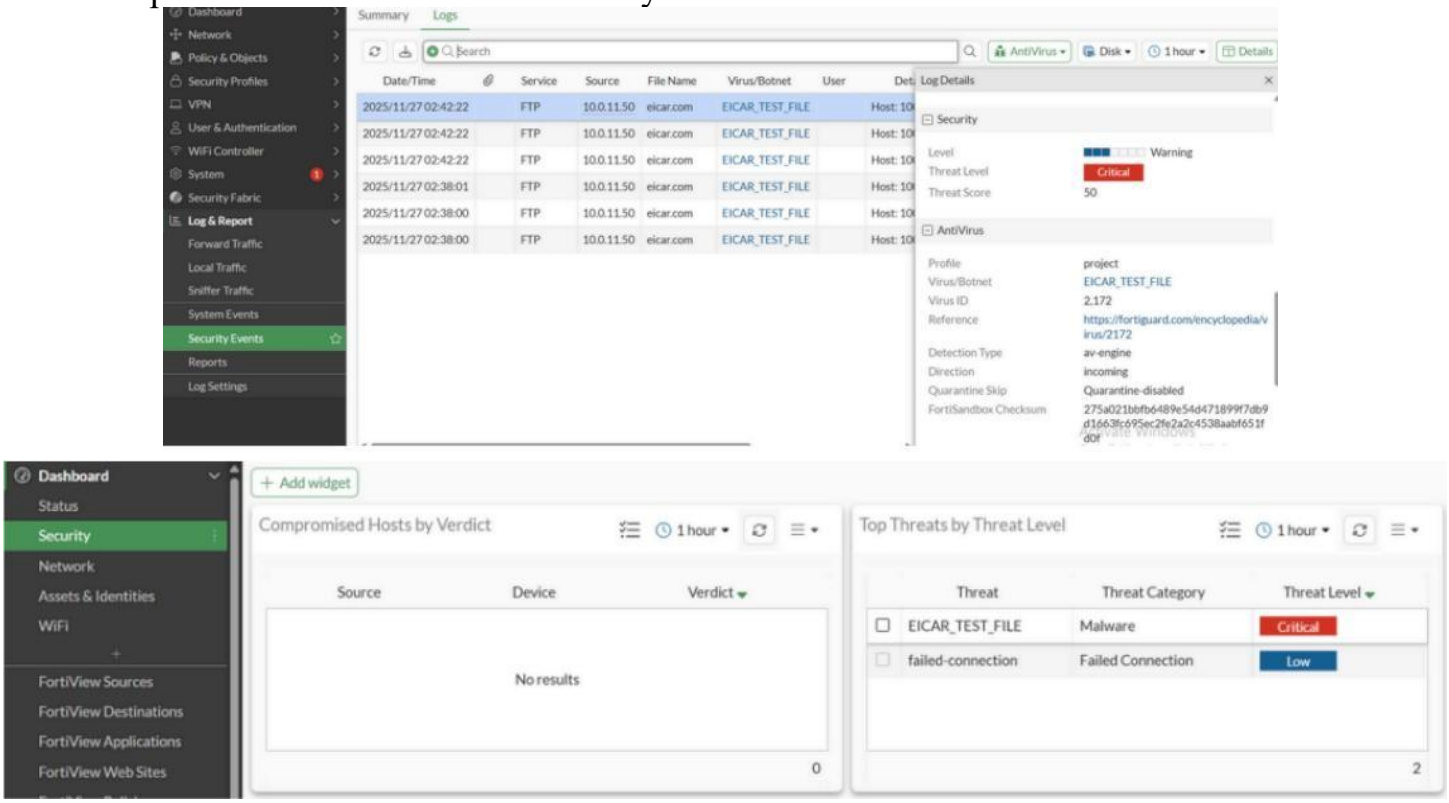


Figure 18:Log Interpretation

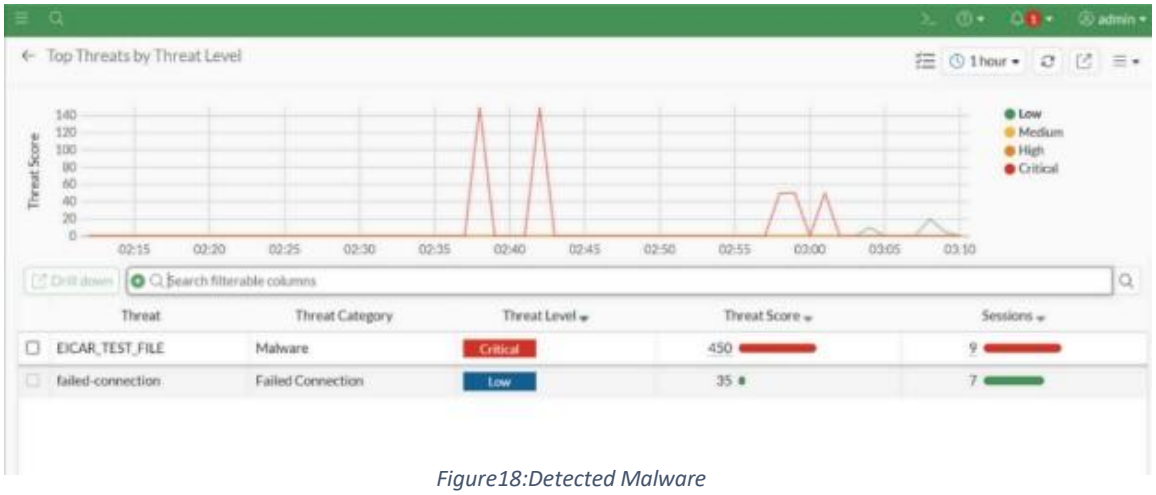


Figure18:Detected Malware

4.5 Conclusion

Antivirus monitoring validated:

- Malware detection works
- EICAR file was blocked successfully
- Logs clearly show threat actions
- Antivirus profG is fully operational

5. Week 2 Logging & Threat Weight (Re-used in Week 3 for Verification)

5.1 Introduction

Logging and Threat Weight settings ensure complete visibility of:

- System events
- Network traffic
- Security threats
- Severity-based prioritization

5.2 Global Log Settings

From:

Log & Report → Log Settings → Global Settings

Configured:

- Event Logging: Enabled (All)
- Local-in Logging: Enabled
- Local-out Logging: Enabled
- Syslog Logging: Disabled (not required)

5.3 Threat Weight Configuration

From:

Security → Threat Weight

Settings:

• Log Threat Weight: Enabled

Application Protection Weights:

- P2P = Low
- Proxy = Medium

Severity Mapping:

- Informational → Off
- Low → Low
- Medium → Medium
- High → High
- Critical → Critical
- Botnet → Critical

5.4 Local Logs Verification

From:

Log & Report → Local Logs

Verified:

- Traffic logs appearing normally
- Event logs generated
- Threat-weight scores appearing when threats are detected

5.5 Conclusion

Logging and threat-weighting work properly and enhance monitoring accuracy.

6. FortiView – Monitoring & Analysis (Week 3)

6.1 Introduction

FortiView is FortiGate's main real-time monitoring dashboard.
It provides visibility for:

- Applications
- Users
- Threats
- Sessions
- Sources & Destinations

6.2 FortiView Main Views

Applications View

Shows:

- Most used applications
- Bandwidth consumption
- Risk level

Examples: Facebook, YouTube, DNS, SSL

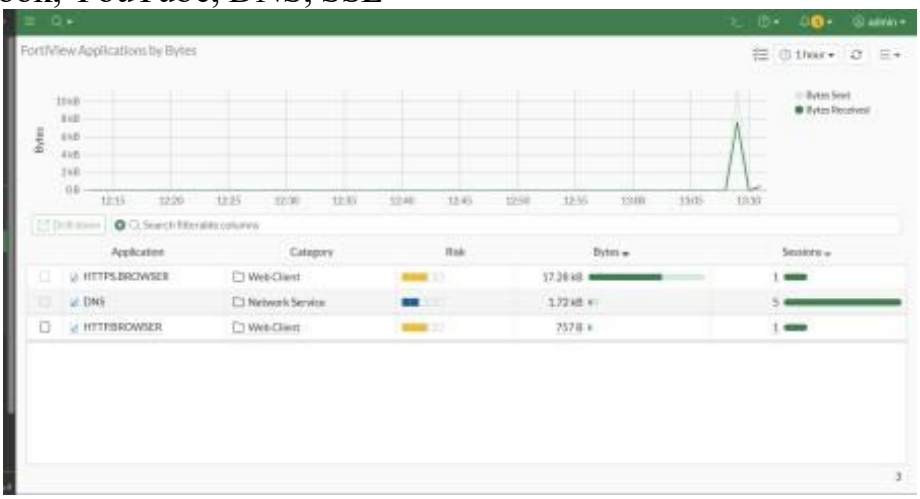


Figure 19:Applications View

Sources View

Shows internal hosts generating traffic.

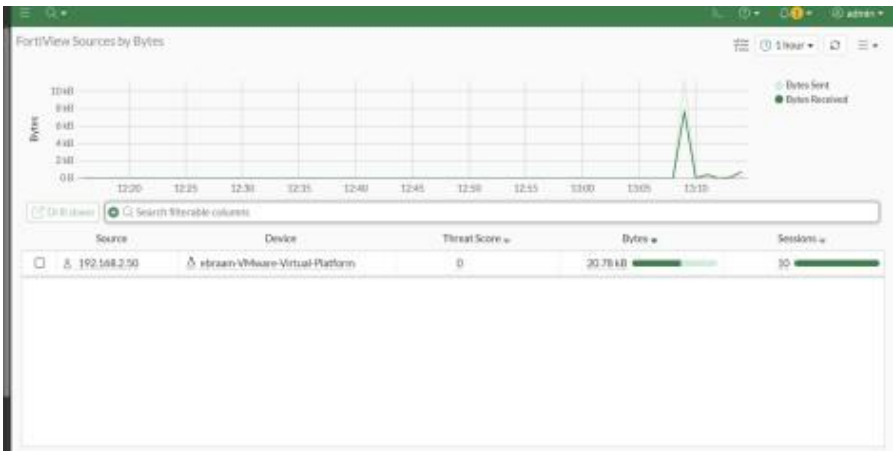


Figure 20:Sources View

Destinations View

Shows external hosts contacted.

Figure 21:Destinations View

Sessions View

Shows active sessions with:

- Protocol
- Ports
- NAT information
- Duration

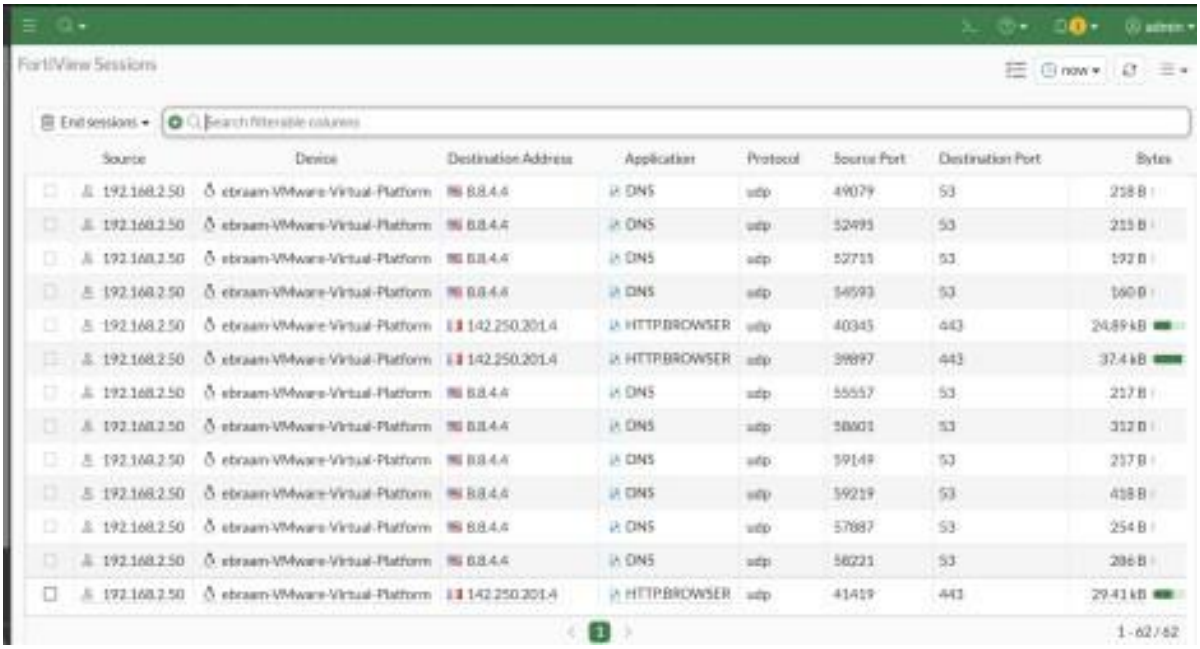


Figure 22:Sessions View

Threats View

Shows IPS alerts, malware signatures, and botnet detection.

6.3 How FortiView Works

FortiView depends entirely on logging.
Required:

- Event Logging = All
- Local Traffic Logging = All
- Local-in / Local-out = Enabled
- Disk / Memory logging = Enabled

6.4 Expected Behavior Under Real Traffic

FortiView normally shows:

- Constant DNS traffic
- HTTPS / SSL traffic
- Application Control categorizations
- Session NAT transitions
- IPS threats if enabled

6.5 Conclusion

FortiView provides deep visibility and is the most important monitoring tool in FortiGate for understanding network behavior.

7. Web Filtering – Monitoring & Logging (Week 3)

7.1 Introduction

This part covers monitoring of the **Ziad-WebFilter** profile using real generated traffic.

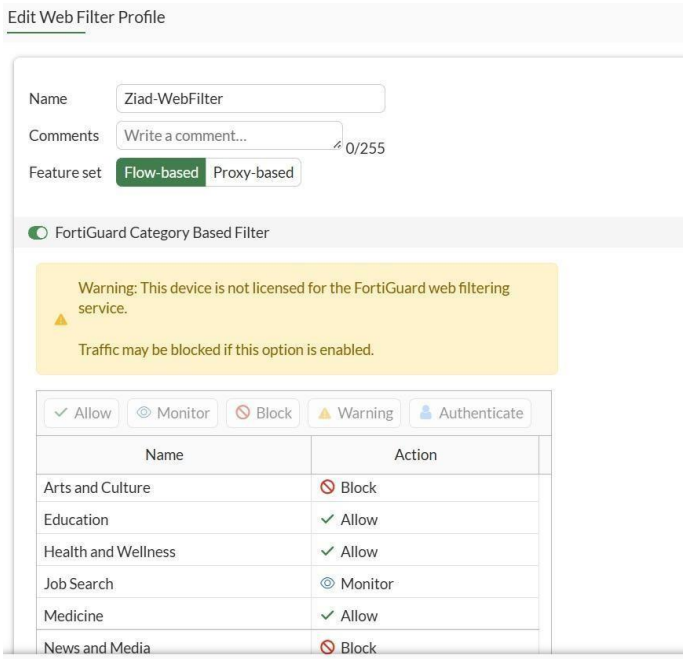


Figure23 :Web Filtering Profile

7.2 Generating Traffic

Traffic was generated from a Kali machine:

- Pinging external sites
- Accessing HTTP & HTTPS
- Testing allowed and blocked categories
- Using curl / wget
- Testing URL filtering (facebook.com, tiktok.com, etc.)

7.3 Web Filter Logs

From:

- Log & Report → Web Filter
- FortiView → Web Filter

Logs included:

- Allowed and blocked URLs
- Category (Social Media, Malware, Adult, etc.)
- URL rating by FortiGuard
- Applied Web Filter profile
- Source device information

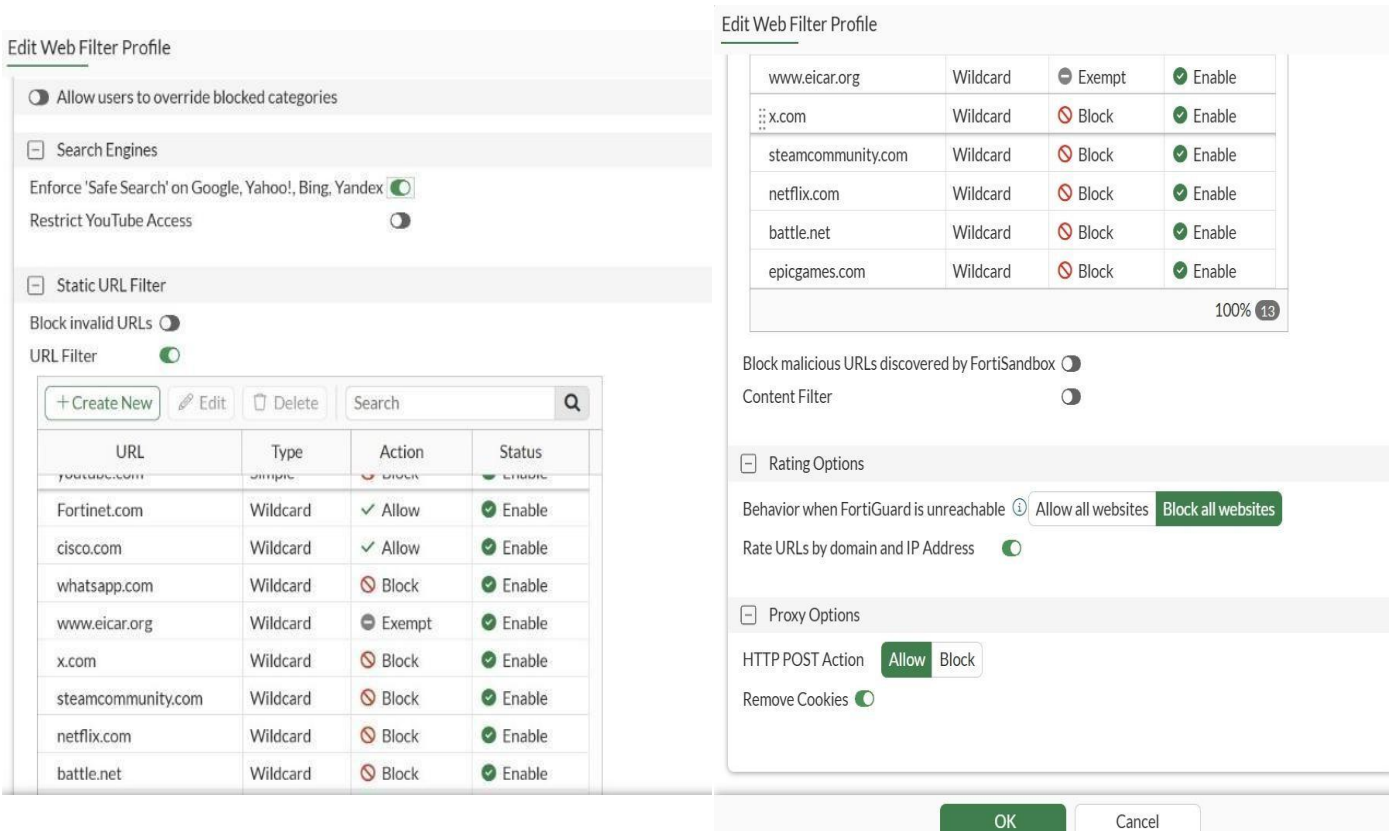


Figure24 : Web Filtering Configuration

7.4 Forward Traffic Logs

Showed:

- Source IP (Ubuntu)
- Destination IP
- Action taken (Allow / Block)
- Policy used
- Service type (HTTP, HTTPS, DNS, etc.)
- Country, bytes, and session details

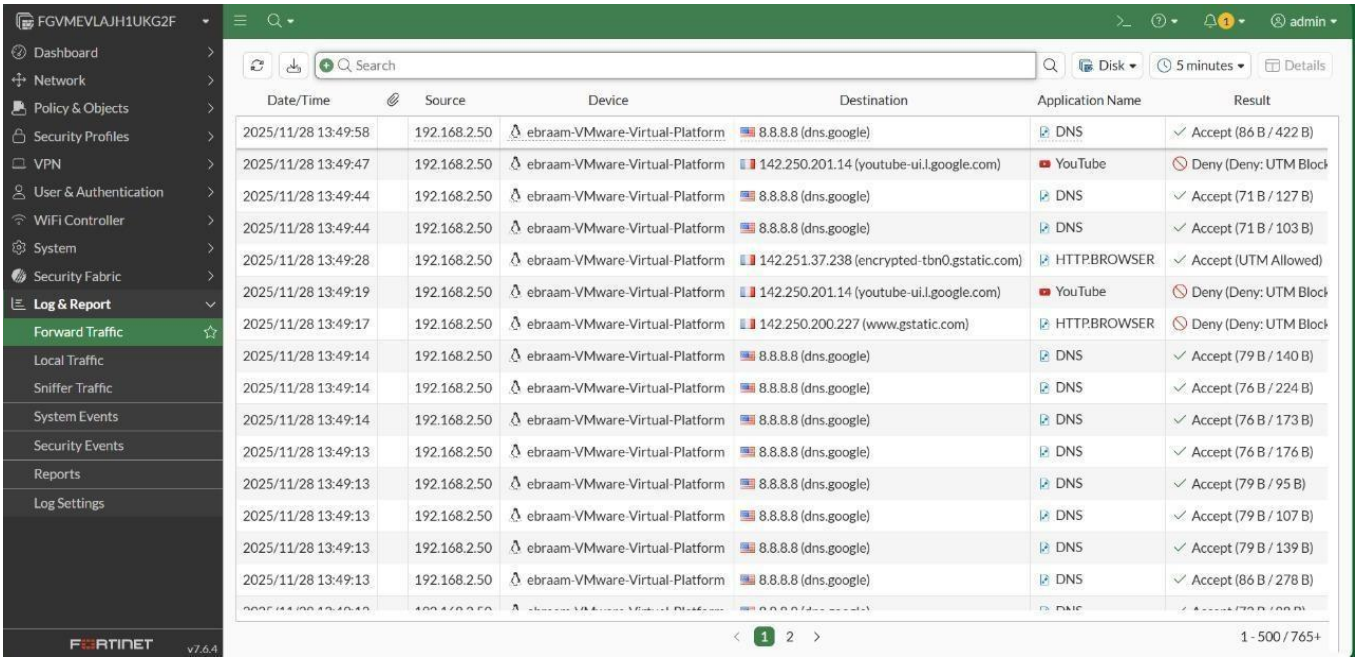


Figure25 :Forward Traffic Logs

7.5 Log Interpretation

Logs confirmed:

- Category-based blocks worked correctly
- URL filters were applied correctly
- SSL inspection applied when needed
- Traffic categorized accurately

7.6 Summary

Week 3 Web Filtering verified:

- Proper profile application
- Category and URL enforcement
- Accurate logging
- Full monitoring visibility

8. WEEK 4 – Final Report

8.1 Application Control – Final Report Section

8.1.1 Overview

The Application Control security profile on FortiGate is used to identify, classify, and control applications at the application layer, even when they use non-standard ports or encryption.
It improves:

- Network visibility
- Productivity (blocking non-work apps)
- Bandwidth usage
- Security

For this project, the Application Control profile was configured to block social media and streaming applications while allowing normal browsing traffic.

8.1.2 Configuration Summary

Profile Name: AppControl_prof

Enabled Application Categories:

- Social Media
- Video / Streaming
- Games
- Cloud Services
- Web Applications
- Unknown Applications
- General Internet Applications

Manually Blocked Applications (Overrides):

- Facebook
- Facebook.App
- Instagram
- YouTube

These apps were chosen as examples of high-bandwidth and productivity-impacting applications.

Logging Settings Enabled:

- Log all application events
- Log session start and end
- Log blocked and allowed application attempts
- Show replacement messages for blocked applications
- Enable DNS / unknown application resolution

Screenshots to include:

- Application Control profile page
- Blocked overrides list
- Profile logging and category actions

8.1.3 Monitoring Results (Week 3)

Traffic was generated from an Ubuntu VM (port2 – LAN) by visiting:

- google.com
- youtube.com
- facebook.com
- instagram.com
- speedtest.net
- ubuntu.com

FortiView – Applications

FortiGate detected multiple applications, including:

- Google services
- YouTube
- Facebook
- Instagram
- Ubuntu repository traffic
- DNS

Application Control Logs showed:

- Blocked attempts for Facebook, Instagram, and YouTube
- Allowed traffic for general web applications
- Proper classification of protocols and signatures

Forward Traffic Logs confirmed:

- Source: Ubuntu VM
- Correct destinations
- NAT usage
- Policy used: LAN → WAN
- Allowed and blocked events

Policy Hit Counters:

The LAN → WAN policy showed increasing:

- Byte counters
- Session counters
- Hit counts

This proves that all traffic passed through FortiGate with Application Control applied.

8.1.4 Expected Real-World Behavior

In a real organization, this configuration would:

- Improve Productivity

– Blocking social media and streaming apps during working hours.

- Save Bandwidth

– YouTube and streaming services consume heavy bandwidth.

- Increase Security

– Detects:

o Risky applications
o Tunneling apps
o Unknown signatures
o Unusual outbound traffic

• Provide Visibility
– Security teams can see:
o Which users tried to access blocked apps
o When they tried
o Which protocol or signature was used

8.1.5 Recommendations

Improvements for real environments:
• Enable SSL Deep Inspection
• Combine Web Filter + Application Control
• Create separate profiles for each department (IT, HR, Marketing, etc.)
• Turn on automatic signature updates
• Monitor regularly using FortiView

8.2 FortiGate Antivirus – Full Report (Week 4 Documentation)

8.2.1 Introduction

This section documents the configuration, monitoring, and analysis of FortiGate Antivirus protection using flow-based inspection mode.
Goals:
• Scan traffic for malware
• Block infected files
• Monitor antivirus activity in Forward Traffic and Security logs
Includes:
• Week 2 – Antivirus configuration
• Week 3 – Monitoring and verification (documented in Week 4)

8.2.2 Week 2 – Configuration Tasks

Creating a Flow-Based Antivirus Profile
• Profile Name: **Antivirus profG**
• Feature Set: Flow-based
• Enabled inspection protocols:
– FTP
– HTTP
– HTTPS
– SMB
– CIFS
This ensures common web and file-transfer protocols are scanned.
Applying Antivirus Profile to Firewall Policy
• Navigate to: Policy & Objects → Firewall Policy
• Edit policy: Internet
• Confirm:
– Inspection Mode: Flow-based
– Antivirus: Enabled
– Selected profile: Antivirus profG
Result: All outgoing LAN traffic is scanned by the antivirus profile

8.2.3 Week 3 – Monitoring and Logging

Because the lab had limited external traffic, manual traffic was generated:

Generating Traffic for Antivirus Scanning

• Used FileZilla to connect to FTP server on HQ-PC-1
• Attempted to download eicar.com
• Browsed multiple HTTP/HTTPS sites
• Sent requests via FTP, SMB, and browsers

This triggered antivirus logging.

Viewing Forward Traffic Logs

Path: Log & Report → Forward Traffic

Logs showed:

- Source IP address
- Destination IP / URL
- Protocol used
- Antivirus action (Blocked / Monitored)
- Profile: Antivirus profG
- Policy ID
- Malware: EICAR Test File

→ Confirms malware detection and blocking.

Viewing Security (Antivirus) Logs

Path: Log & Report → Security Events → Antivirus

Details included:

- Virus name: EICAR_TEST_FILE
- Action: Block / Quarantine
- Detection method: Flow-based
- Protocol: FTP / HTTP
- File name: eicar.com
- Client device: HQ-PC-1

→ Confirms correct antivirus behavior.

Log Interpretation

Logs showed:

- Successful detection of EICAR
- Malicious content blocked before reaching the endpoint
- Flow-based resets on detection
- Proper application of Antivirus profG
- Scanning on FTP, HTTP, SMB, etc.

Expected Behavior of Antivirus Logs

Antivirus logs should show:

• Detected malware events
• Protocol used
• File name and hash (if available)
• Action taken
• Device IP
• Policy ID

Observed logs matched expectations.

8.2.4 Final Summary

The Antivirus project covered:

Week 2:

• Creation of flow-based Antivirus profile
• Enabling scanning for FTP, HTTP, HTTPS, SMB, CIFS
• Applying the profile to the Internet firewall policy

Week 3:

• Generating test traffic (FileZilla + web browsing)
• Viewing Forward Traffic logs
• Viewing Antivirus Security logs
• Confirming detection of EICAR
• Verifying correct policy and profile assignment

Result:

The FortiGate Antivirus engine is active, properly configured, and effectively detecting malicious content.

9. Firewall Policies & Real-Time Logs – Final Overview

9.1 Firewall Policy Configuration – LAN2-to-LAN1

Policy Overview

• Name: LAN2-to-LAN1
• Direction: Internal (PC1 port2) → External (WAN port1)
• Action: ACCEPT
• Schedule: Always

Traffic Specs:

• Source: All internal devices
• Destination: All external networks
• Service: ALL protocols and ports

Security Configuration:

• Inspection Mode: Flow-based
• NAT: Enabled with source port translation

Security Profiles Applied:

1. Antivirus: Antivirus profG
2. Web Filter: Ziad-WebFilter
3. Application Control: AppControl_profile
4. SSL Inspection: certificate-inspection

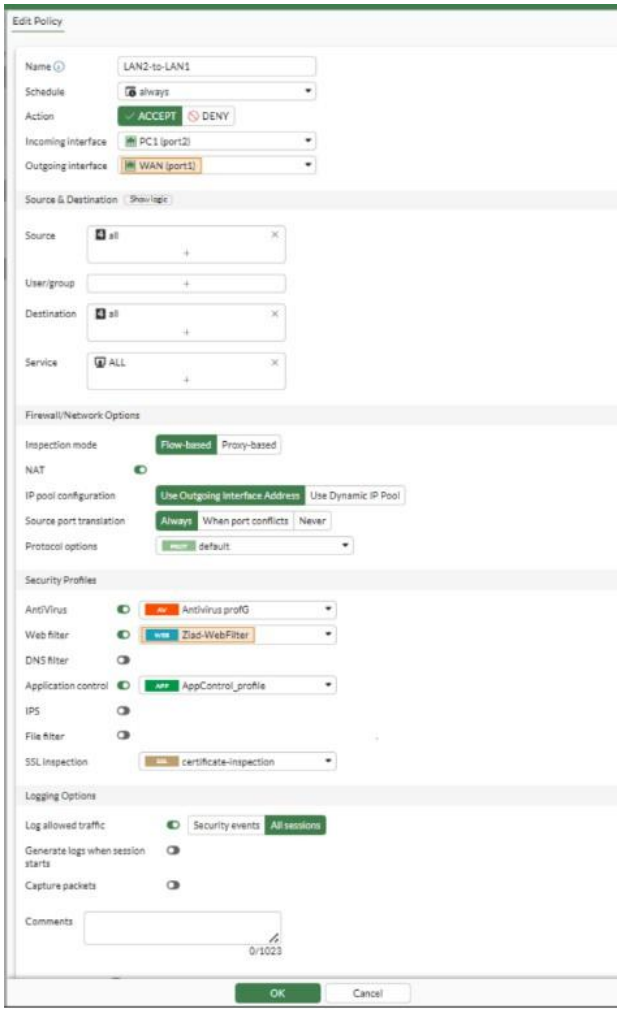


Figure26 :Firewall Policy – LAN2-to-LAN1

Logging & Monitoring:
• All sessions logging enabled
• Comprehensive security events logging
Purpose:
Allow controlled internet access from internal devices with multiple security layers and full visibility.

9.2 Firewall Policy Configuration – LAN1-to-LAN2

Policy Overview
• Name: LAN1-to-LAN2
• Direction: External (WAN port1) → Internal (PC1 port2)
• Action: ACCEPT
• Schedule: Always
Traffic Specs:
- • Source: All external networks
- • Destination: All internal devices
- • Service: ALL

Security configuration and profiles are the same as LAN2 → LAN1.
Purpose:
Allow legitimate external traffic to reach internal resources under strict controls.

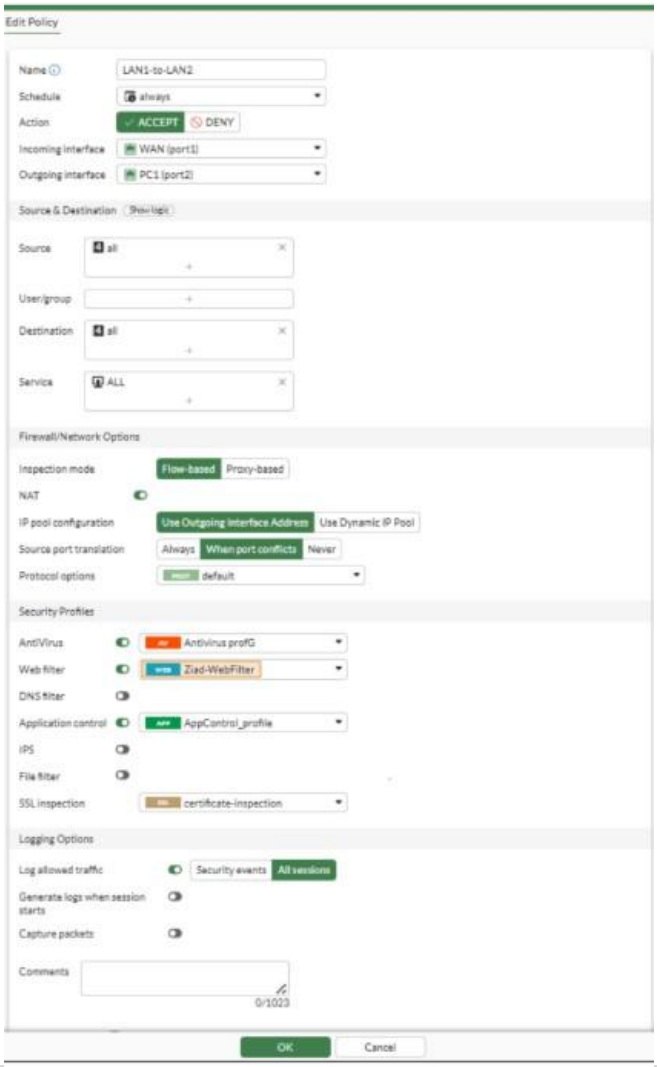


Figure27 :Firewall Policy _ LAN1-to-LAN2

Firewall Policies Overview:

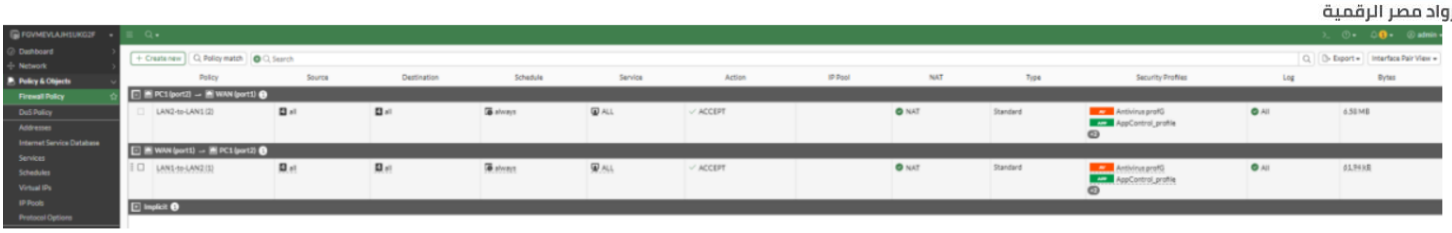


Figure28 :Policies Overview

9.3 Real-Time Traffic – Forward Traffic Logs

Live Traffic Analysis

• Source: 192.168.2.50 (Ubuntu VM)
• Destinations: Google, YouTube, Bing, CloudFlare, DNS servers
• Applications: Ping, DNS, HTTP Browser
Policy used: **LAN2-to-LAN1 (2)**

Security Actions:

• Accept (UTM allowed) for legitimate traffic
• Real-time inspection of DNS and web traffic

Key Insights:

• Firewall policies actively filtering and monitoring traffic
• UTM security profiles working correctly
• Stable and secure connectivity
• Full network visibility via logs

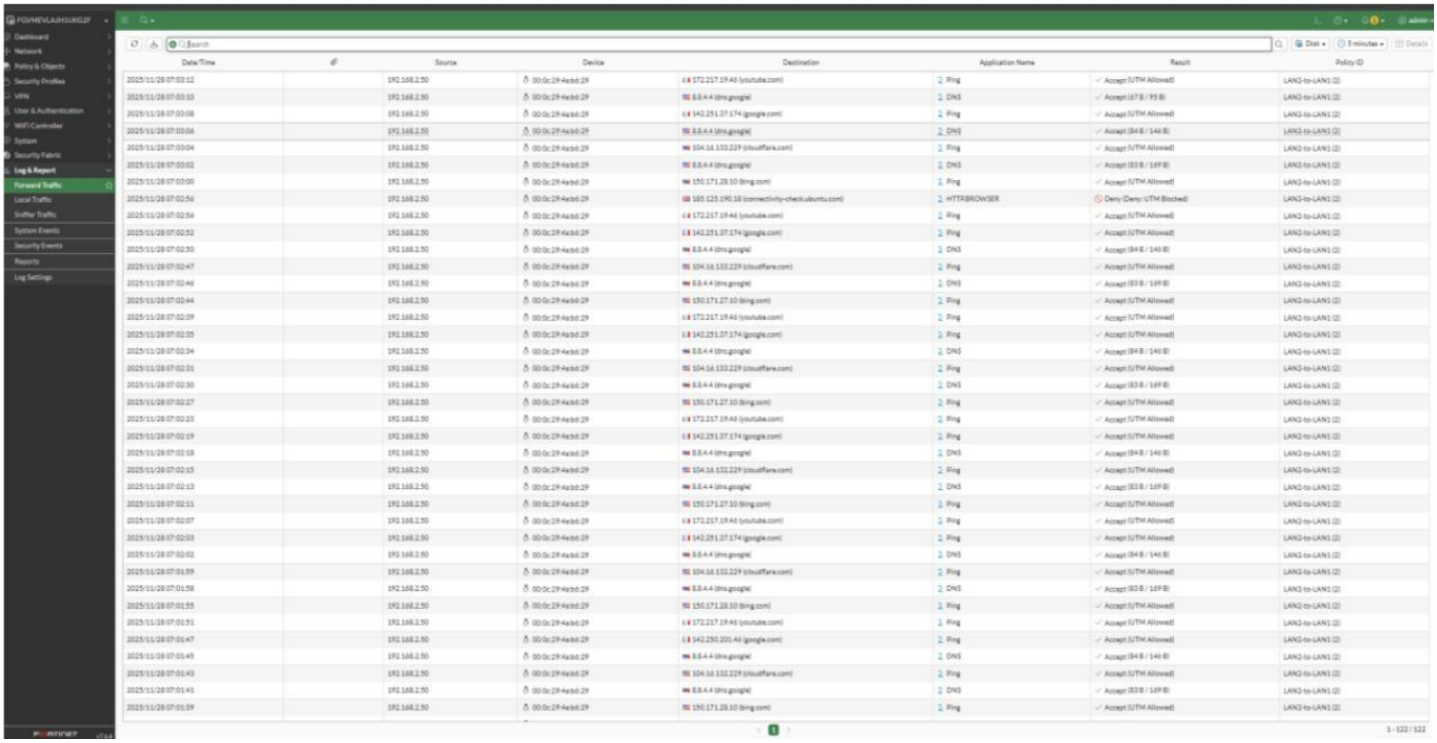


Figure 29:Real Time Monitoring

9.4 Security Events Summary – Comprehensive Protection

Summary:

• Application Control – 73 events
– 72 Network-Service (allowed)
– 1 WebClient (allowed)
• Web Filter – 1 event (rating error blocked)
• Antivirus – no events (clean traffic)
• IPS – no intrusion attempts
• SSL Inspection – no issues

Security Effectiveness:

• Proactive blocking of risky content
• Full visibility into network applications
• No malware or intrusion detected
• Multiple layers working together

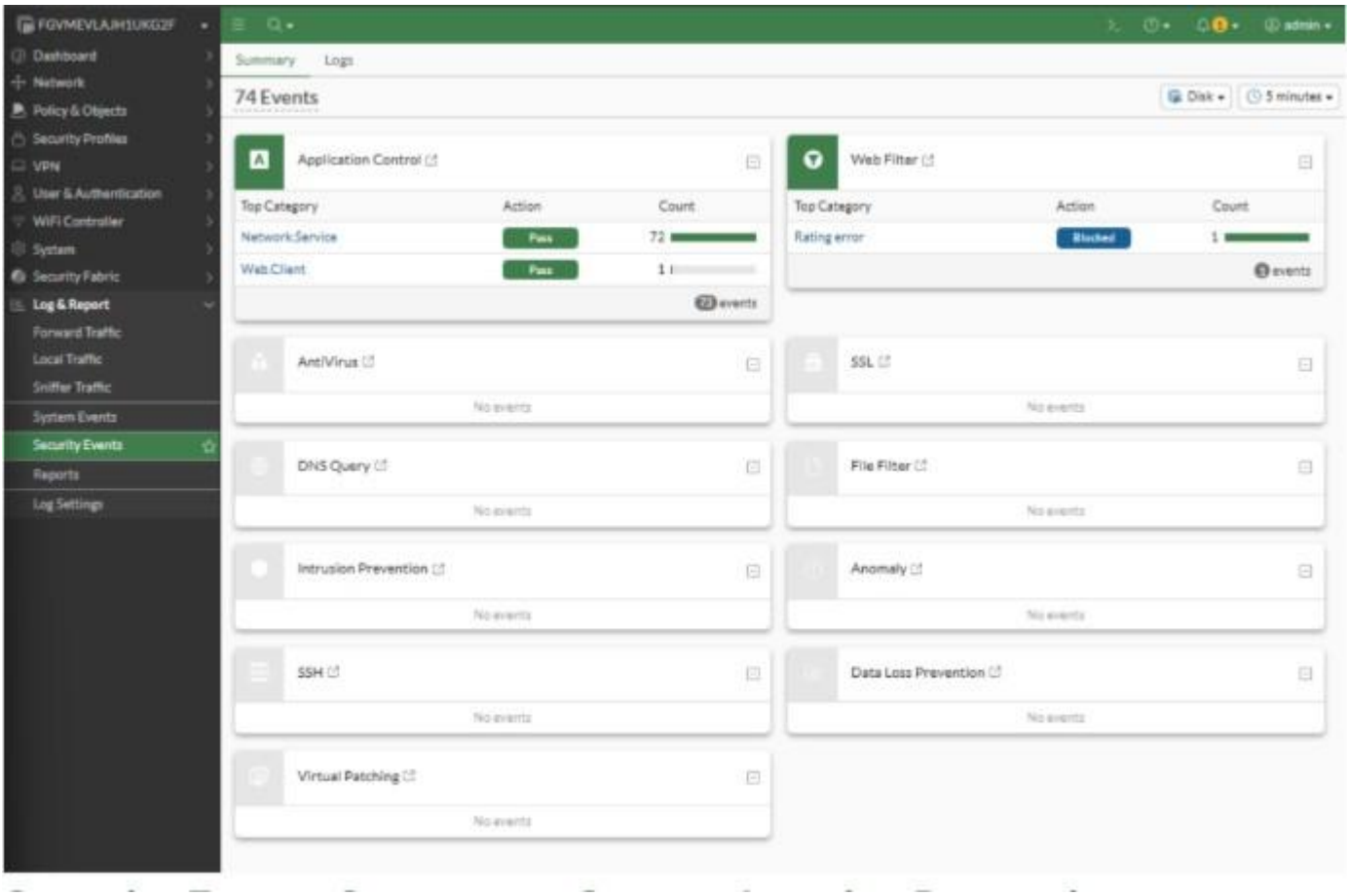


Figure 30:Security Events Summary - Comprehensive Protection

Conclusion:

The security infrastructure successfully identifies, categorizes, and controls traffic while preventing potential threats.

10. Web Filtering – Final Report (Summary of Project)

10.1 Introduction

This report documents Web Filtering configuration, monitoring, and results using FortiGate.
Objectives:
• Block harmful categories
• Filter specific URLs
• Enable advanced protections (sandbox, HTTP POST control, etc.)

10.2 Week 2 – Configuration Summary

Profile: Ziad-WebFilter

Category-Based Filtering:

Category – Action:
• Social Media → Block
• Adult/Mature → Block
• Games → Block
• Education → Allow
• Business → Allow

URL Filter Rules:

URL – Action:
• facebook.com → Block
• tiktok.com → Block
• eicar.org → Exempt
• Fortinet → Allow

Advanced Options Enabled:
• Rate URLs by Domain and IP Address
• Block HTTP POST
• Block malicious URLs from FortiSandbox
• Remove Cookies
• Block when FortiGuard is unreachable

10.3 Week 3 – Monitoring & Logging

Web Filter logs checked via:
• Log & Report → Web Filter
• FortiView → Web Filter

Due to lab limitations, traffic was generated from Kali:
• Pings
• HTTP/HTTPS requests
• Category and URL tests

Forward Traffic logs used to view:
• Source IP (Ubuntu)
• Destination IP
• Allow / Block action
• Policy ID
• Service (HTTP/HTTPS/DNS)

Logs showed:
• Allowed normal browsing
• Blocked forbidden categories and URLs
• Correct FortiGuard categorization and ratings

10.4 Expected Behavior of Web Filter Logs

Web Filter logs typically include:

- Allowed and blocked URLs
- Website category
- User IP
- Action (Allow / Block)
- Policy ID
- FortiGuard URL rating

This proves accurate detection and enforcement.

10.5 Final Summary

The Web Filtering project successfully achieved:

- Full Web Filter profile configuration
- Blocking unwanted categories
- Allowing safe categories
- Custom URL controls
- Advanced protections (FortiSandbox, HTTP POST blocking, etc.)
- Comprehensive logging and documentation

This setup improves security, prevents access to harmful websites, and controls user web activity with high accuracy.

Conclusion

In conclusion, the project successfully demonstrated how FortiGate can be used to implement a robust and layered security architecture for an enterprise network. Application Control was able to block non-productive and high-risk applications such as Facebook, Instagram, and YouTube while still allowing normal web browsing, which improves productivity and optimizes bandwidth usage. The Web Filter profile enforced safe browsing by blocking harmful categories and malicious URLs, while the Antivirus profG profile detected and blocked the EICAR test file across multiple protocols using flow-based inspection.

The configured firewall policies, together with comprehensive logging, Threat Weight, and FortiView dashboards, provided full visibility into sessions, applications, threats, and user behavior. Monitoring results confirmed that traffic was passing through the correct policies, security profiles were applied as expected, and all relevant security events were recorded for analysis. Overall, the system is correctly configured, stable, and ready to be used as a foundation for real-world network protection, with recommended future enhancements including SSL deep inspection, per-department policies, and continuous monitoring via fortiview.