

# FORTIGATE

## ADVANCED FORTIGATE SECURITY PROFILES





## TEAM MEMBERS

- Sagda Ashraf
- Marolla fouad
- Shahd Ali
- Jihan Elkhouly
- Nour Elsheikh



# AGENDA

**Week 1: Understanding Security**

**Profiles**

**Week 2: Configuration &  
Implementation**

**Week 3: Monitoring & Reporting**

**Week 4: Final Summary &  
Recommendations**



# PROJECT OBJECTIVE

**Understand, deploy, monitor, and evaluate FortiGate security profiles including:**

**Antivirus  
Web Filtering  
Application Control**

# FORTIGATE SECURITY PROFILES

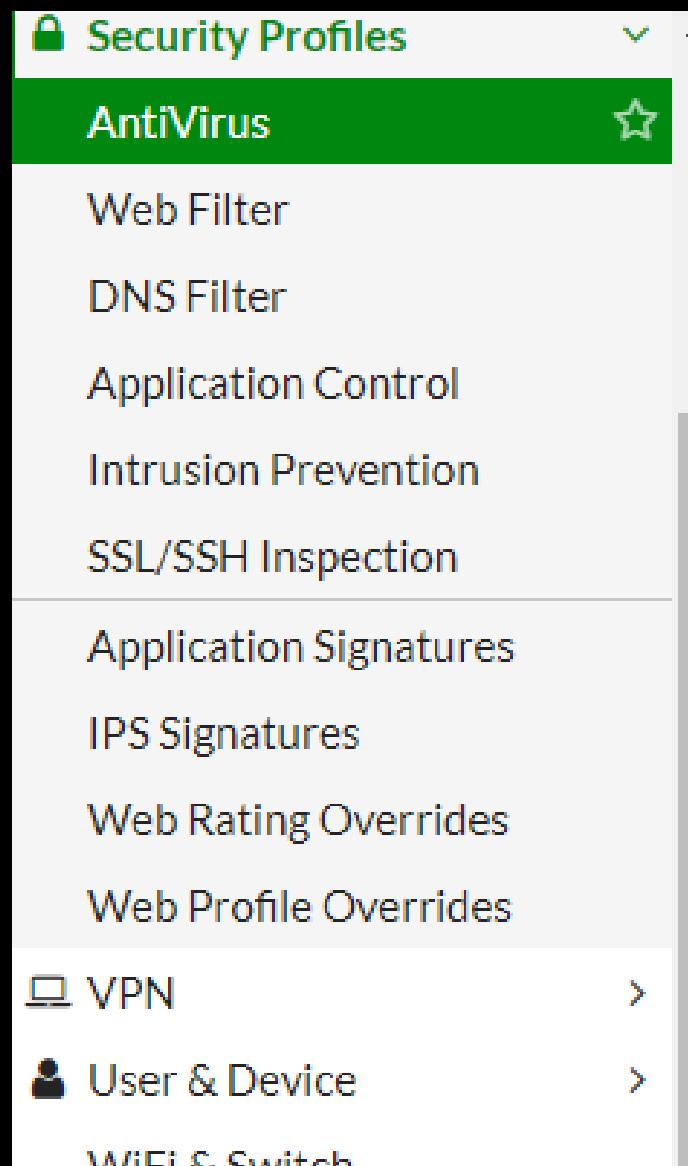


## FORTIGATE SECURITY PROFILES OVERVIEW

Security Profiles provide layered protection against:

- Malware
- Malicious websites
- Risky applications
- Intrusions & exploits

# TYPES OF SECURITY PROFILES



## TYPES OF SECURITY PROFILES

FortiGate supports:

- Antivirus
- Web Filter
- Application Control
- IPS
- DNS Filter
- Email Filter
- SSL/SSH Inspection
- Sandbox Integration

# ANTIVIRUS PROFILE BASICS

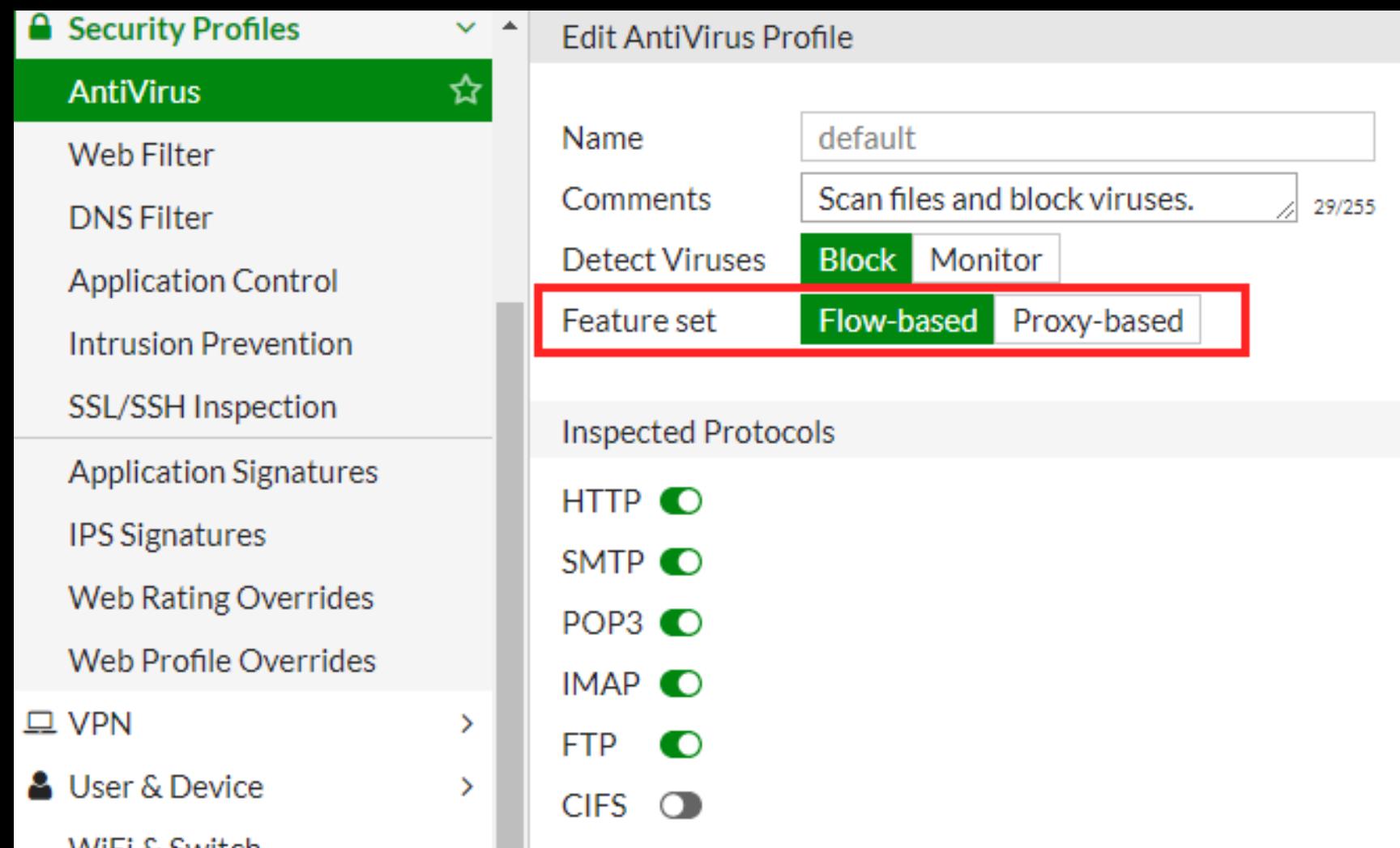


## — ANTIVIRUS PROFILE BASICS

The Antivirus engine detects and blocks:

- Malware
- Viruses
- Trojans
- Suspicious files

# ANTIVIRUS INSPECTION MODES



## ANTIVIRUS INSPECTION MODES

1. Flow-based: high speed
2. Proxy-based: deep content scanning

# KEY ANTIVIRUS FEATURES



## KEY ANTIVIRUS FEATURES

- Signature-based detection
- Heuristic scanning
- File quarantine
- Cloud-assisted threat lookup

## What is Web Filtering?



# WEB FILTERING OVERVIEW

## WEB FILTERING OVERVIEW

Web Filter controls access to websites based on:

- Categories
- URLs
- Keywords
- Content rules



# WEB FILTERING USE CASES

## —WEB FILTERING USE CASES—

Block harmful websites  
Enforce productivity rules  
Prevent phishing  
Control browsing behavior



# WEB FILTER CATEGORY EXAMPLES

## WEB FILTER CATEGORY EXAMPLES

- Gambling
- Social Media
- Adult
- Streaming
- Malware Sites
- Proxy Avoidance



# APPLICATION CONTROL BASICS

## APPLICATION CONTROL BASICS

Deep Packet Inspection (DPI) identifies and controls:

- Applications
- App behaviors
- Encrypted app traffic (with SSL inspection)

# APPLICATION CONTROL EXAMPLES



## APPLICATION CONTROL EXAMPLES

- VPN applications
- Streaming apps
- Gaming
- P2P
- Social media applications

# LAB ENVIRONMENT

## — LAB ENVIRONMENT —

Tools used:

- FortiGate Firewall
- VMware Workstation
- Kali Linux (client test machine)

# NETWORK TOPOLOGY

## — NETWORK TOPOLOGY —

Kali LAN → FortiGate LAN  
Port → NAT → Internet  
All traffic inspected by  
firewall policies.

# WEEK 2 OVERVIEW

## WEEK 2 OVERVIEW

Configuration of:

Antivirus Profile  
Web Filter Profile  
Application Control Profile  
Applied to:

LAN → WAN policy  
With SSL Deep Inspection

for more info check :

### Week 2: Configuring Security Profiles

#### Introduction:

This document presents the configuration and implementation of Security Profiles on the FortiGate firewall as part of Week 2 of the project. Security Profiles play a critical role in protecting network traffic from a wide range of threats, including malware, unauthorized applications, web-based attacks, and intrusion attempts. By applying these profiles to firewall policies, the FortiGate device performs deep inspection of traffic, ensuring that users, servers, and applications remain secure.

The purpose of this guide is to outline the steps taken to configure essential Security Profiles—such as Antivirus, Web Filtering, Application Control, and demonstrate how they are applied to relevant firewall policies. This documentation also highlights key considerations, best practices, and verification methods to ensure the security policies function effectively.

The configurations covered in this document aim to enhance network protection, improve visibility, and support the overall security posture of the environment.

#### Objectives:

- To configure Antivirus, Web Filtering, and Application Control profiles on the FortiGate device.
- To apply the configured profiles to appropriate firewall policies for effective traffic inspection.
- To ensure protection against malware, harmful websites, and unauthorized applications.
- To document each configuration in a clear and repeatable format.

#### Configuring Security Profiles:

# WEB FILTERING CONFIGURATION

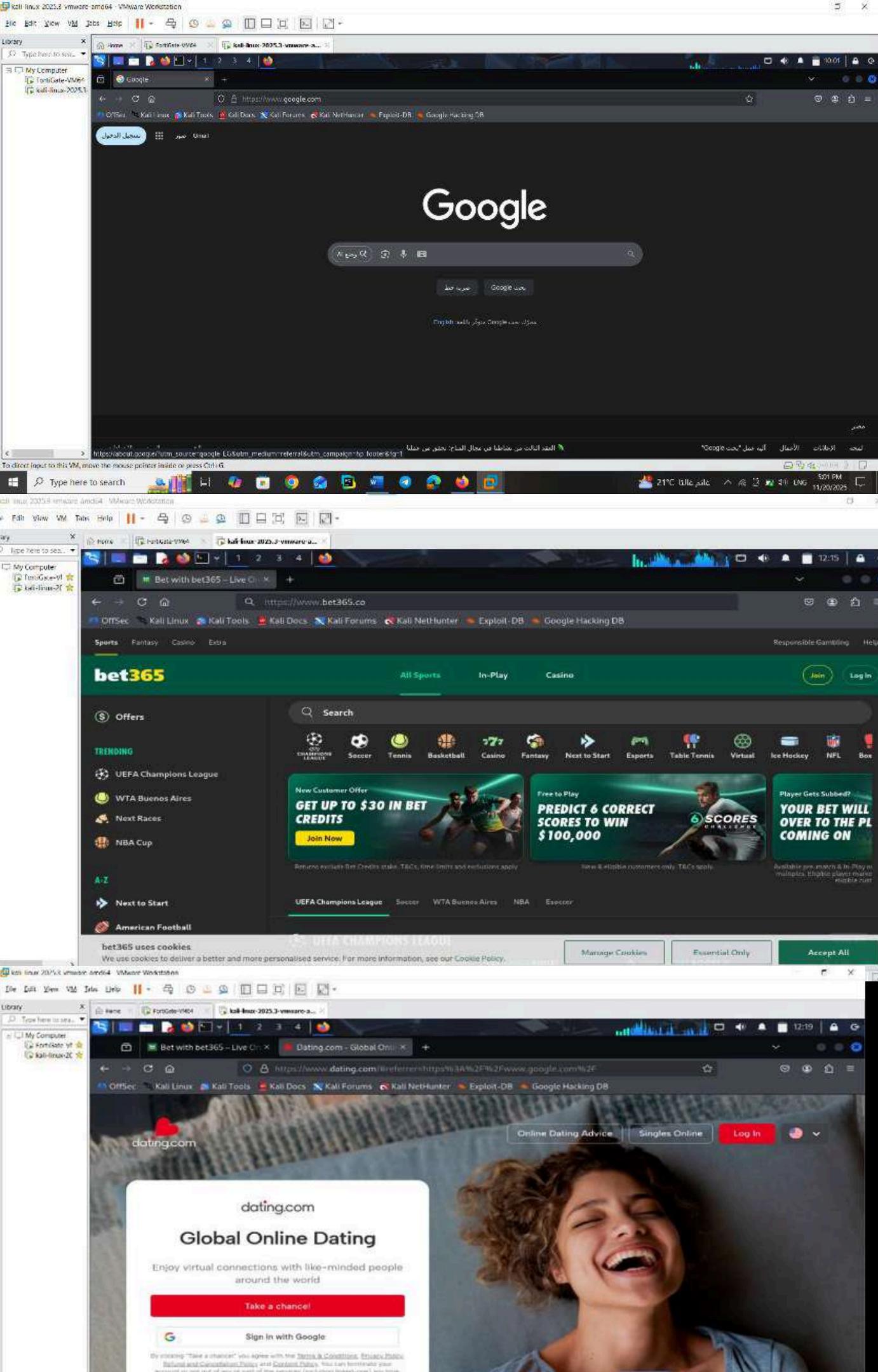
## WEB FILTERING CONFIGURATION

Configured rules to block:

Gambling  
Dating  
Social media  
High-risk sites

The screenshot shows the 'Edit Web Filter Profile' dialog for 'Kali-Filter-Policy'. It includes fields for Name (Kali-Filter-Policy), Comments (Write a comment...), Feature set (Flow-based), and a warning about being unlicensed for FortiGuard web filtering. The main table lists categories: Local Categories (custom1, custom2), Potentially Liable (Drug Abuse, Hacking), and a section for Monitoring. Buttons OK and Cancel are at the bottom.

The screenshot shows the 'Edit Web Filter Profile' dialog for 'Kali-Filter-Policy'. It includes fields for Name (Kali-Filter-Policy), Comments (Write a comment...), Feature set (Flow-based), and a warning about being unlicensed for FortiGuard web filtering. The main table lists categories with 'Block' actions: Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Nudity and Risque, Pornography, Dating, and Weapons (Sales). Buttons OK and Cancel are at the bottom.

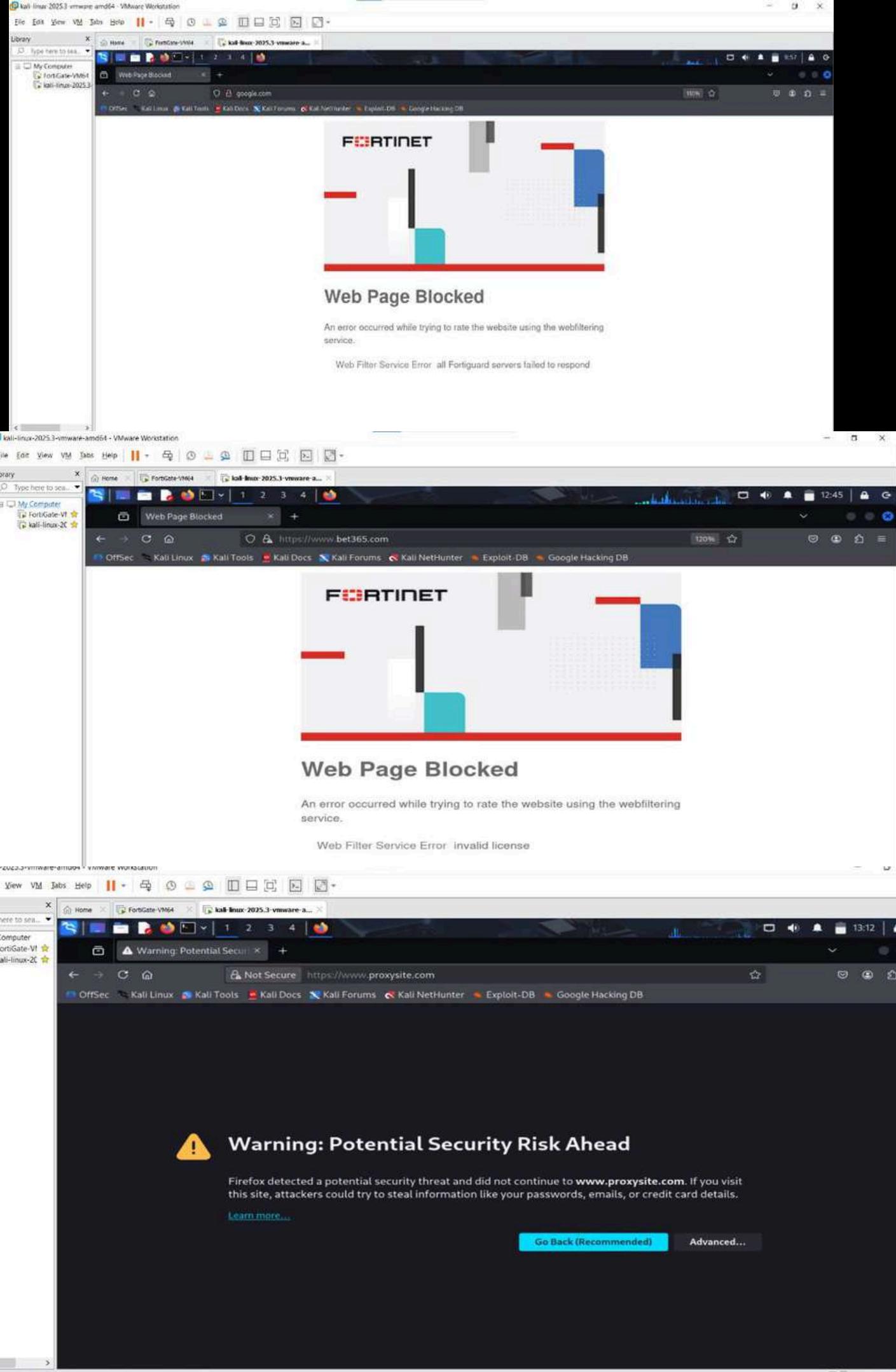


# WEB FILTER BEFORE TESTING

## WEB FILTER BEFORE TESTING

Before applying the profile:

All websites accessible  
No restrictions in place



# WEB FILTER AFTER TESTING

## WEB FILTER AFTER TESTING

After profile enforcement:

Block pages displayed  
Restricted websites denied  
Proxy avoidance sites warned

# WEB FILTER FIREWALL POLICY

## WEB FILTER FIREWALL POLICY

Policy:  
Kali\_Internet\_Access\_with\_Filter  
Includes:  
Web Filter profile (Kali-Filter-Policy)  
Deep SSL Inspection  
Security Events Logging: ON

The screenshot shows the FortiManager interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. It displays a list of firewall policies. Two policies are visible: 'LAN-to-Kali (port2) --> port1' and 'port1 --> LAN-to-Kali (port2)'. Both policies are associated with the 'Kali-Filter-Policy' Web filter profile. The policy details include source and destination as 'all', action as 'ACCEPT', and deep inspection enabled.

The screenshot shows the 'Edit Policy' dialog for the 'Kali\_Internet\_Access\_with\_Filter' policy. The basic configuration includes a schedule of 'always', an action of 'ACCEPT', and traffic flowing from 'LAN-to-Kali (port2)' to 'port1'. The 'Source & Destination' tab is selected, showing 'all' for both source and destination. The 'Firewall/Network Options' tab is also visible.

The screenshot shows the 'Edit Policy' dialog for the 'Kali\_Internet\_Access\_with\_Filter' policy, focusing on advanced options. It includes 'Firewall/Network Options' such as 'IP pool configuration' (using 'Outgoing Interface Address'), 'Source port translation' (set to 'Always'), and 'Protocol options' (set to 'PROT default'). Under 'Security Profiles', the 'Web filter' is set to 'Kali-Filter-Policy'. Other sections like 'SSL inspection' (set to 'deep-inspection') and 'Logging Options' (with 'Security events' checked) are also shown.

# APPLICATION CONTROL CONFIGURATION

The screenshot shows the FortiGate Application Control configuration interface. It displays a list of applications under the "Application Control" tab. One application, "ABC.com", is selected and shown in detail. The application is categorized under "Video/Audio" and has a "Category" of "Browser-Based". There are also tabs for "Technology", "Popularity", and "Risk". The interface includes a search bar and a toolbar with various icons.

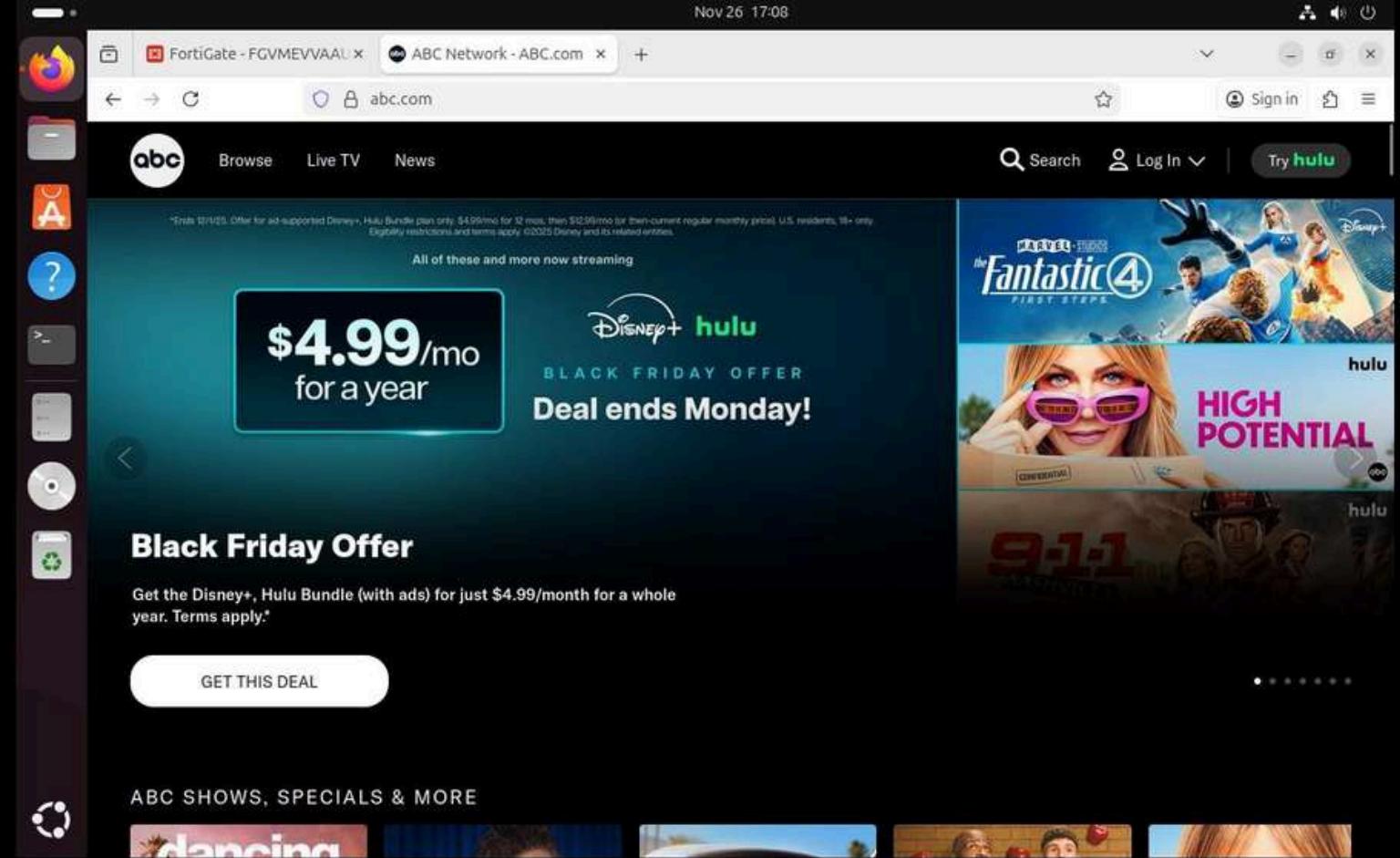
The screenshot shows the FortiGate Firewall Policy configuration interface. Under the "Firewall Policy" tab, the "Edit Policy" dialog is open. In the "Firewall/Network Options" section, the "Application control" dropdown is set to "APP default". Other options like "Source port translation" and "Protocol options" are also visible. The interface includes a sidebar with various policy and network-related settings.

The screenshot shows the FortiGate Application Control configuration interface, similar to the one above but with a different view. It displays a list of applications under the "Application Control" tab. One application, "ABC.com", is selected and shown in detail. The application is categorized under "Video/Audio" and has a "Category" of "Browser-Based". There are also tabs for "Technology", "Popularity", and "Risk". The interface includes a search bar and a toolbar with various icons.

## APPLICATION CONTROL CONFIGURATION

Configured to block:

ABC.com  
Classified under  
“Video/Audio” category

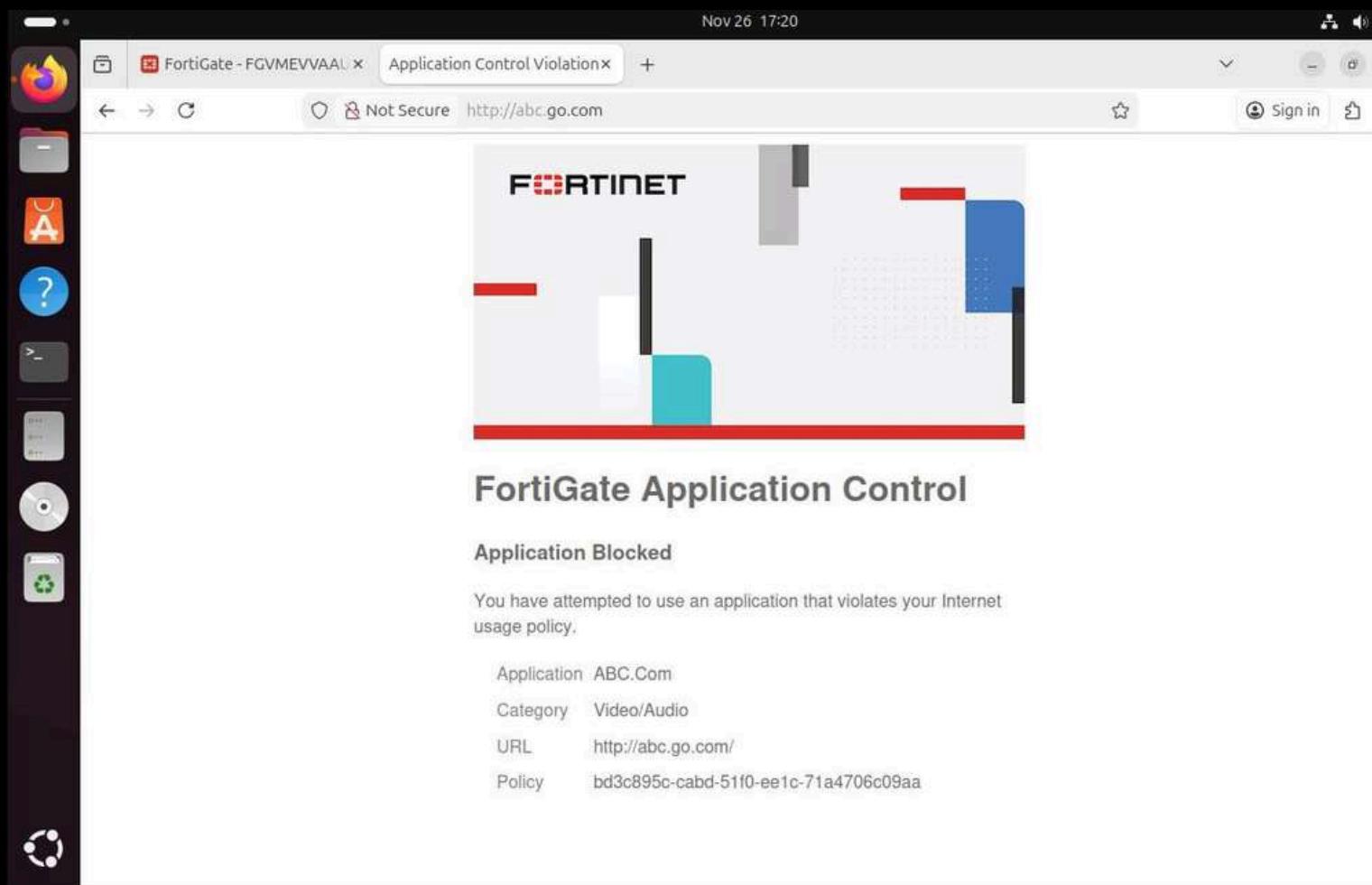


# APPLICATION CONTROL BEFORE TESTING

## APPLICATION CONTROL BEFORE TESTING

Before configuration:

ABC.com loaded  
normally  
No restrictions applied



# APPLICATION CONTROL AFTER TESTING

## APPLICATION CONTROL AFTER TESTING

After profile enforcement:

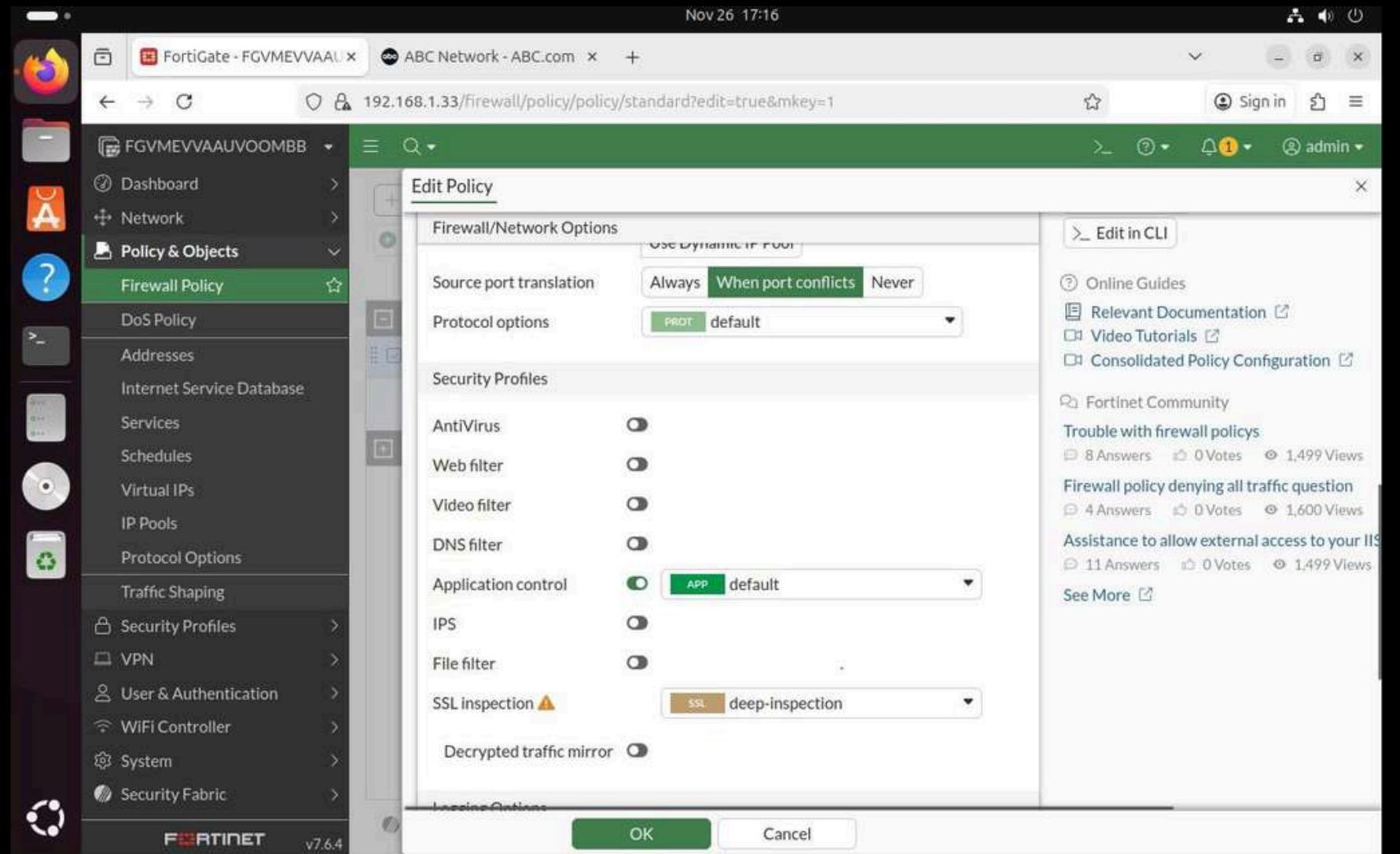
Connection blocked  
App Control logs displayed  
SSL Inspection detected  
encrypted session

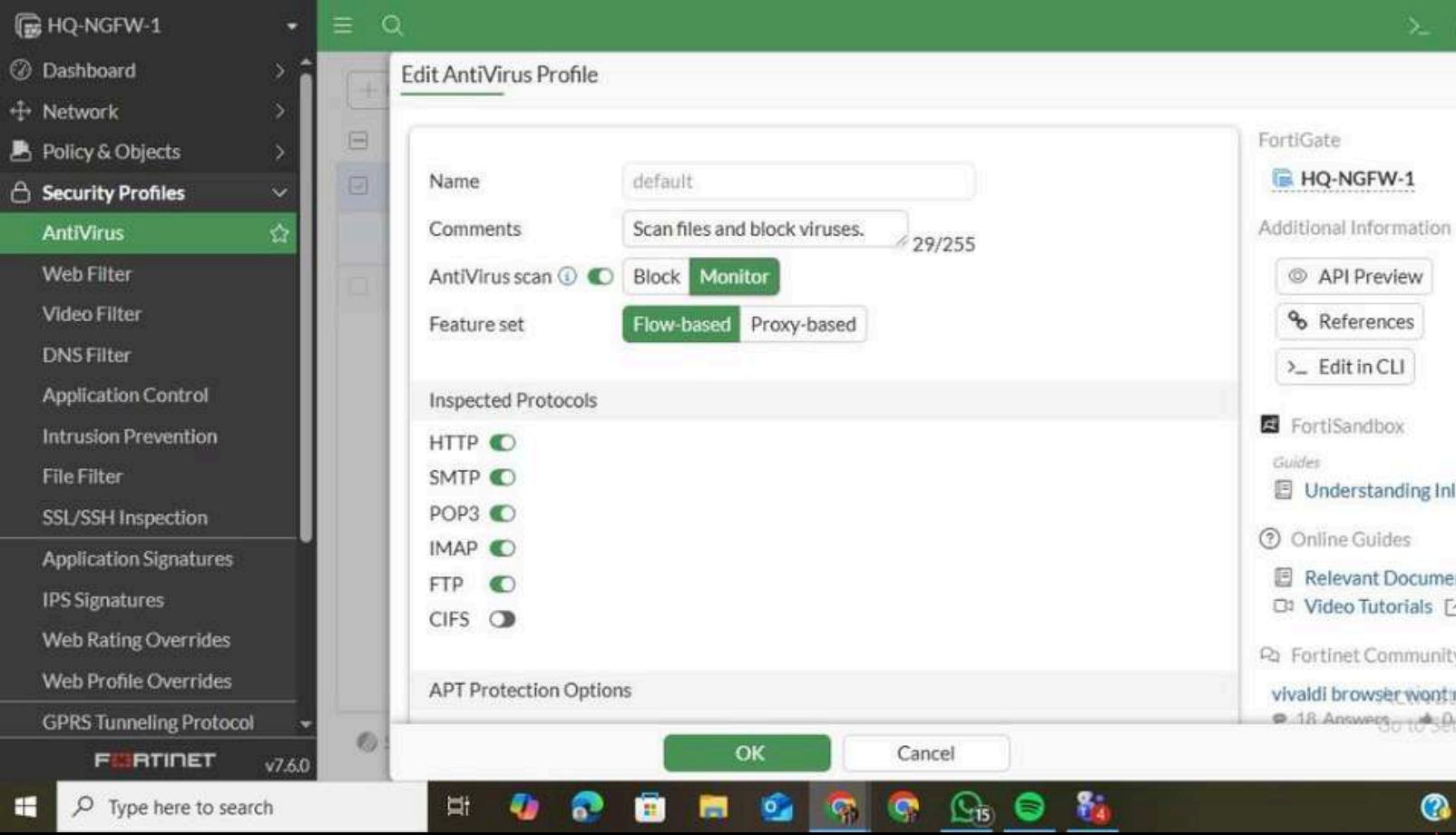
# APPLICATION CONTROL FIREWALL POLICY

## APPLICATION CONTROL FIREWALL POLICY

Policy applied to: LAN → WAN  
Includes:

- Application Control Profile
- Web Filter
- SSL Deep Inspection enabled





# ANTIVIRUS CONFIGURATION ENABLED:

## ANTIVIRUS CONFIGURATION ENABLED:

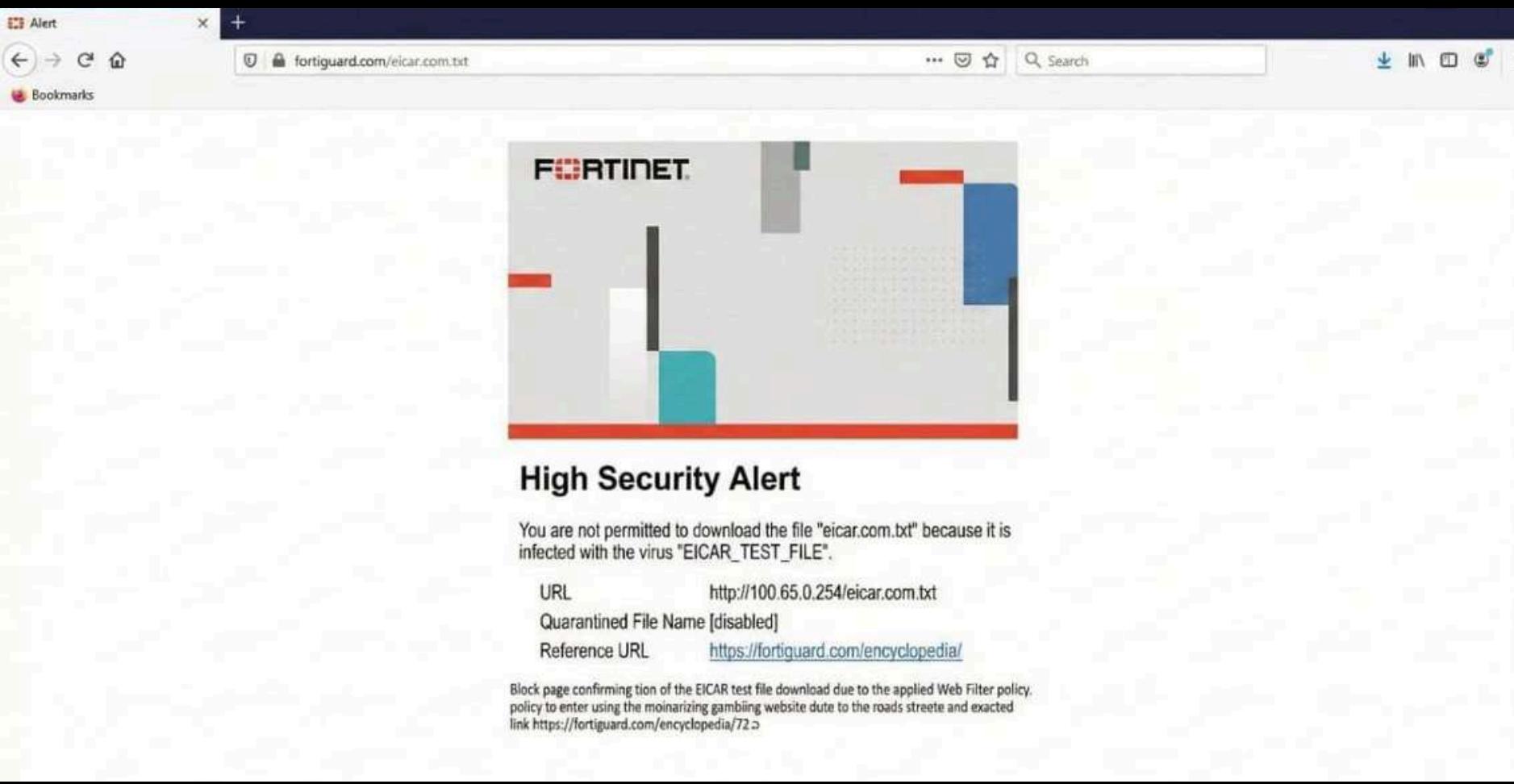
- Protect against malware, Trojans, viruses
- Secure HTTP/HTTPS file downloads
- Prevent system infections



# ANTIVIRUS BEFORE TESTING

## — ANTIVIRUS BEFORE — TESTING

Before applying Antivirus profile:  
EICAR test virus successfully  
downloaded  
No malware inspection active

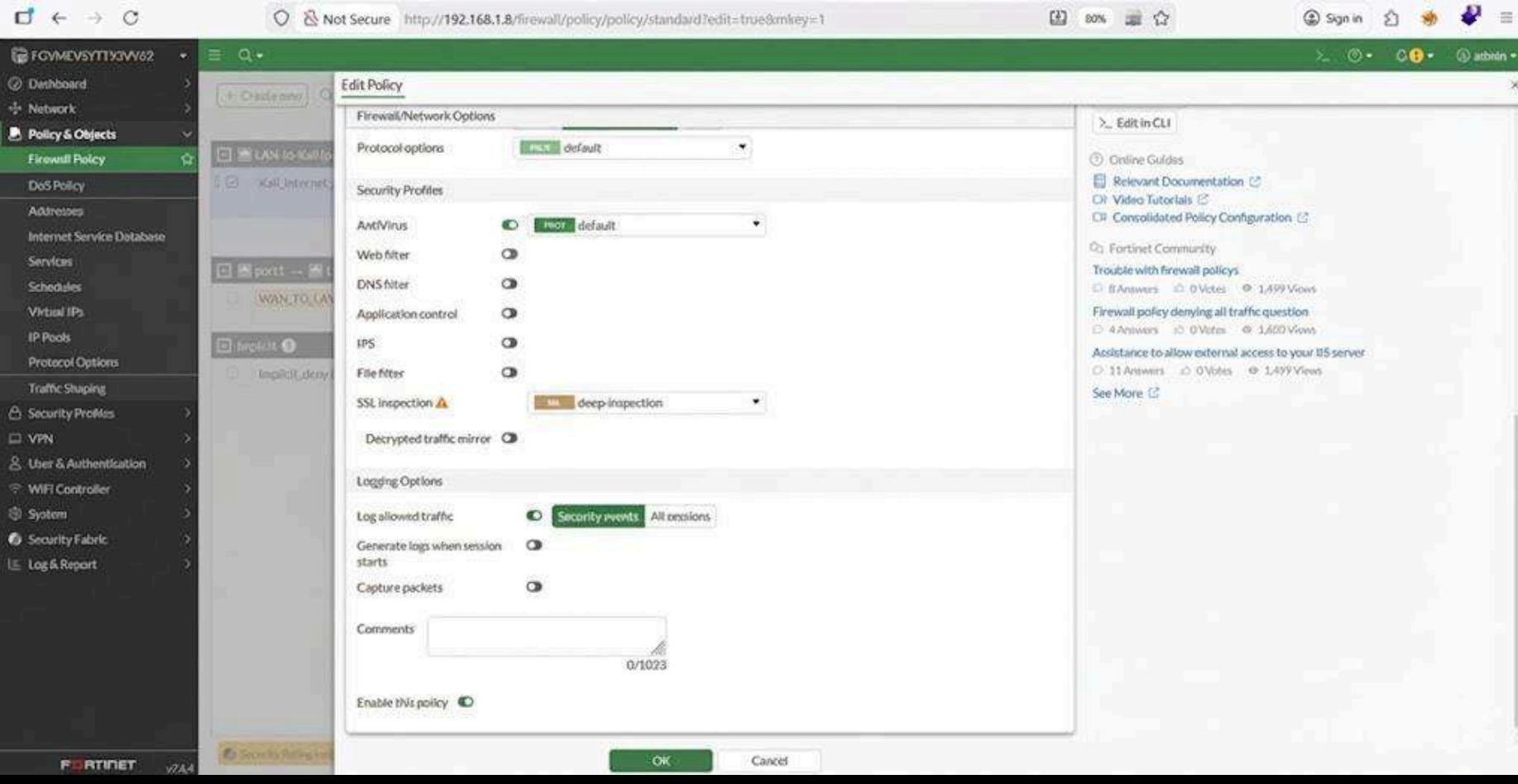


# ANTIVIRUS AFTER TESTING

## ANTIVIRUS AFTER TESTING

After applying Antivirus:

Download blocked  
FortiGate displayed:  
“Virus/Malware Detected”  
EICAR test file intercepted



# ANTIVIRUS FIREWALL POLICY

## — ANTIVIRUS FIREWALL — POLICY

Policy:  
`Kali_Internet_Access_with_AV`

Enabled:

- Antivirus (Flow-based)
- SSL Deep Inspection
- Security Logging: ALL

# WEEK 3 OVERVIEW

## WEEK 3 OVERVIEW

Monitoring and reporting using:

Forward Traffic Logs  
Security Events Logs  
FortiView Dashboards

for more info check :

### Week 3: Monitoring and Reporting

#### Introduction:

This document presents the monitoring and reporting procedures implemented on the FortiGate firewall as part of Week 3 of the project. Monitoring and reporting are essential components of an effective security strategy, as they provide continuous visibility into network activity, threat detections, and the overall performance of deployed security profiles. By leveraging FortiGate's built-in dashboards, logs, and reporting tools, administrators can assess the effectiveness of Antivirus, Web Filtering, and Application Control profiles configured in previous phases.

This guide outlines the configuration of key monitoring features, methods for analyzing security events, and the process of generating detailed reports. These insights help ensure proactive threat detection, support troubleshooting efforts, and contribute to ongoing optimization of the organization's security posture.

#### Objectives

- To enable and configure FortiGate monitoring tools for tracking security events.
- To analyze logs and dashboards to measure the effectiveness of deployed security profiles.
- To generate automated and on-demand reports for security visibility and documentation.
- To evaluate detected threats, blocked activities, and system performance.
- To provide clear configuration details and reporting examples for future reference.
- To support continuous improvement of the network's security controls.

#### Monitoring and Reporting

##### 1-Web filter :

##### Firewall Policy:

# LOG SETTINGS ENABLED

## — LOG SETTINGS ENABLED —

Monitoring includes:

- UTM events
- Allowed sessions
- Denied sessions
- Application events

# WEB FILTER FIREWALL POLICY AT MONITORING

The screenshot displays the Fortinet FortiManager web interface with two overlapping windows for editing firewall policies.

**Left Window (Foreground): Edit Policy - Kali\_Internet\_Access\_with\_Filter**

- Name:** Kali\_Internet\_Access\_with\_Filter
- Schedule:** always
- Action:** ACCEPT (selected)
- Incoming Interface:** LAN-to-Kali (port2)
- Outgoing Interface:** port1
- Source & Destination:** Show logic
- Source:** all
- User/group:** (empty)
- Destination:** all
- Service:** ALL
- Firewall/Network Options:**
  - Inspection mode:** Flow-based (selected)
  - NAT:** Enabled
  - IP pool configuration:** Use Outgoing Interface Address (selected)
  - Source port translation:** Always (selected)
  - Protocol options:** **proto default**
- Statistics (since last reset):**

ID	1
Last used	23s ago
First used	7d 2h 17m 16s ago
Active sessions	5
Hit count	399
Total bytes	899.3 kB
- Current bandwidth:** 0 bps
- Last 7 Days:** Bytes (IPv4)  
A line chart showing traffic volume over the last seven days. The Y-axis ranges from 0 B to 800 kB. The X-axis shows dates from Nov 19 to Nov 26. The chart shows a sharp peak on Nov 26.
- Additional Information:**
  - API Preview
  - Edit in CLI
  - Online Guides
  - Relevant Documentation

**Right Window (Background): Edit Policy - LAN-to-Kali (port2) (Implicit deny)**

- Protocol options:** **proto default**
- Security Profiles:**
  - AntiVirus: Off
  - Web filter: On (selected) - **Kali-Filter-Policy**
  - DNS filter: Off
  - Application control: Off
  - IPS: Off
  - File filter: Off
  - SSL inspection: **deep-inspection**
  - Decrypted traffic mirror: Off
- Logging Options:**
  - Log allowed traffic: On (selected) - **Security events All sessions**
  - Generate logs when session starts: Off
  - Capture packets: Off
- Comments:** 0/1023
- Enable this policy:** On

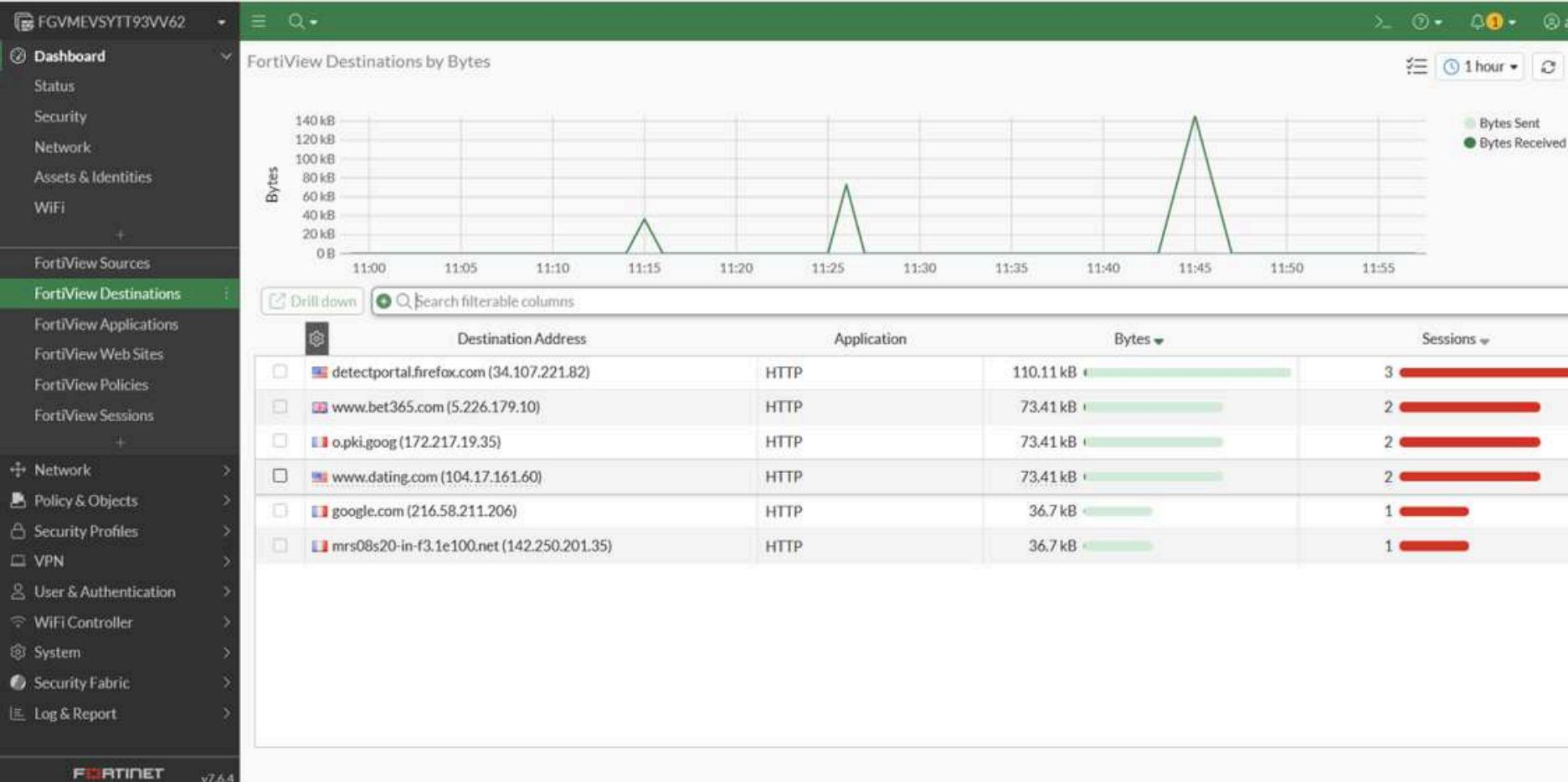
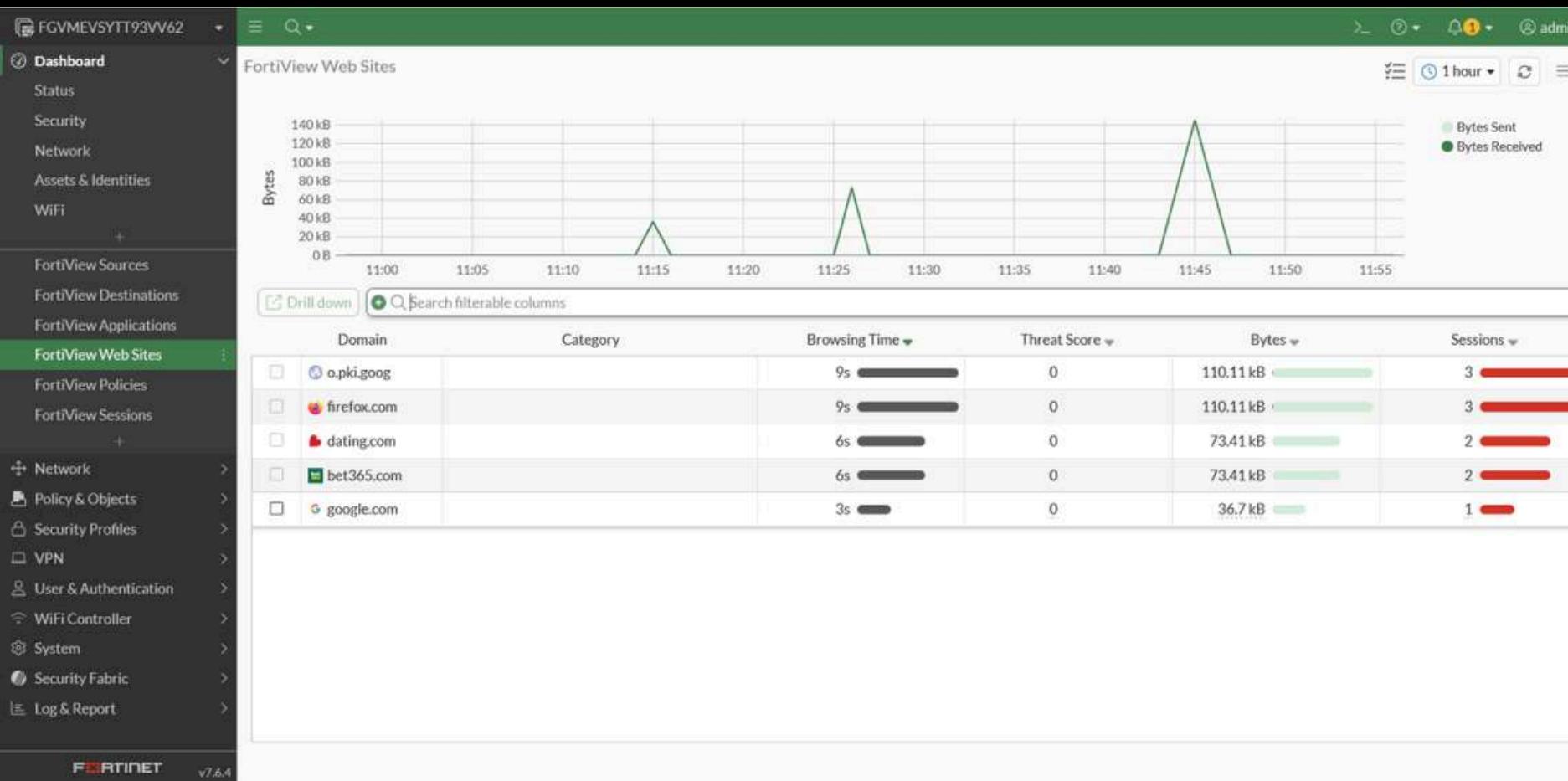
# MONITORING WEB FILTER LOGS OBSERVATION:

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2025/11/26 11:46:34	192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:46:33	192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:45:37	192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:45:36	192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:45:07	192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:45:01	192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:44:23	192.168.10.10	00:0c:29:2a:8e:bb	216.58.211.206 (google.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:44:18	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:26:51	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:26:02	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 11:15:59	192.168.10.10	00:0c:29:2a:8e:bb	142.250.201.35 (mrs08s20-in-f3.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 10:52:05	192.168.10.10	00:0c:29:2a:8e:bb	142.250.201.46 (mrs08s20-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 10:51:59	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 10:49:54	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 10:47:51	192.168.10.10	00:0c:29:2a:8e:bb	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}
2025/11/26 10:47:51	192.168.10.10	00:0c:29:2a:8e:bb	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter {1}

## MONITORING WEB FILTER LOGS

Multiple blocked attempts  
Categories: gambling, dating, social media

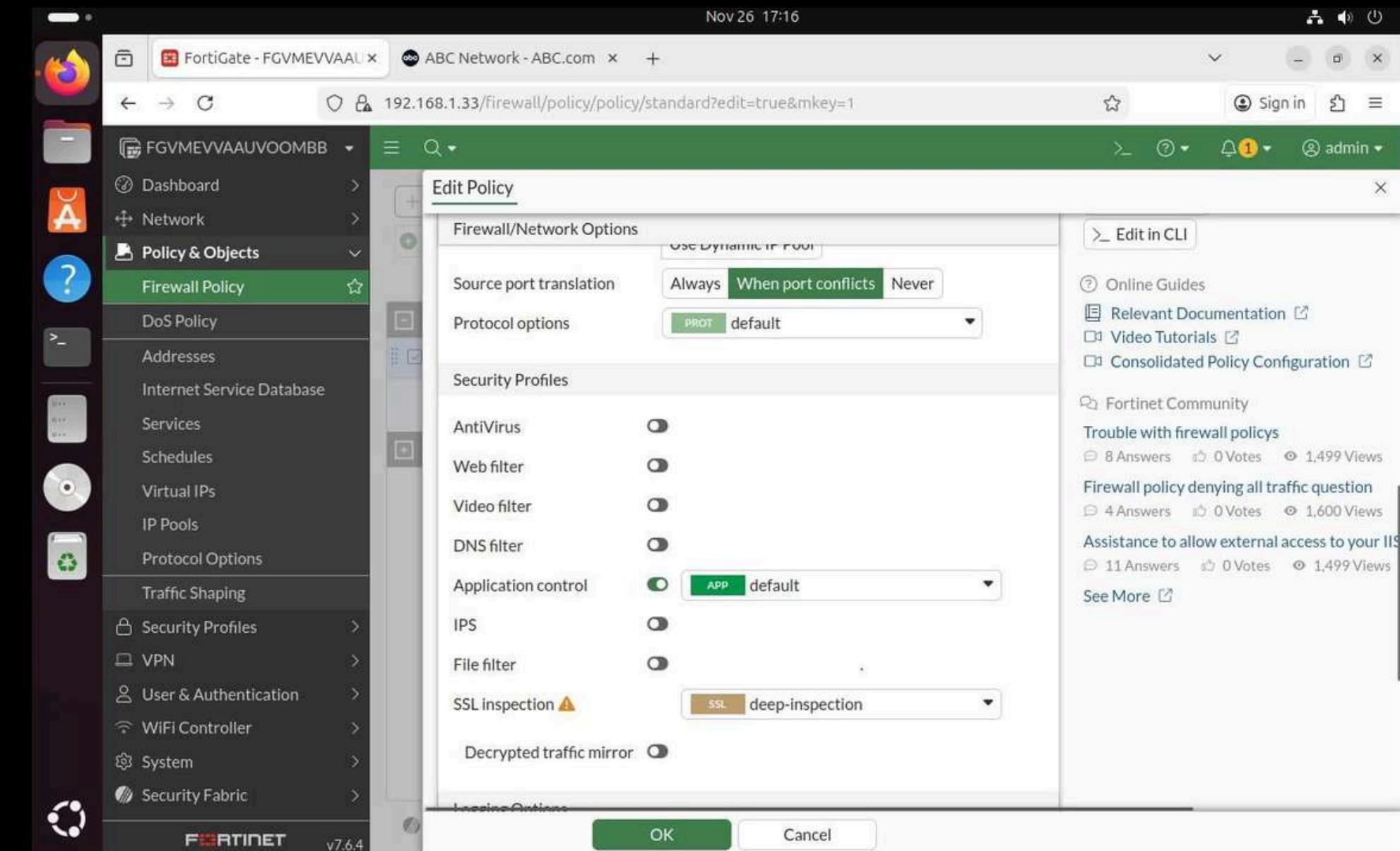
# FORTIVIEW WEB FILTER DASHBOARD DISPLAYS:



## FORTIVIEW WEB FILTER DASHBOARD

Blocked domains  
Attempt counts  
Trend charts

# APPLICATION CONTROL FIREWALL POLICY FOR MINTORING



# APPLICATION CONTROL SECURITY EVENTS

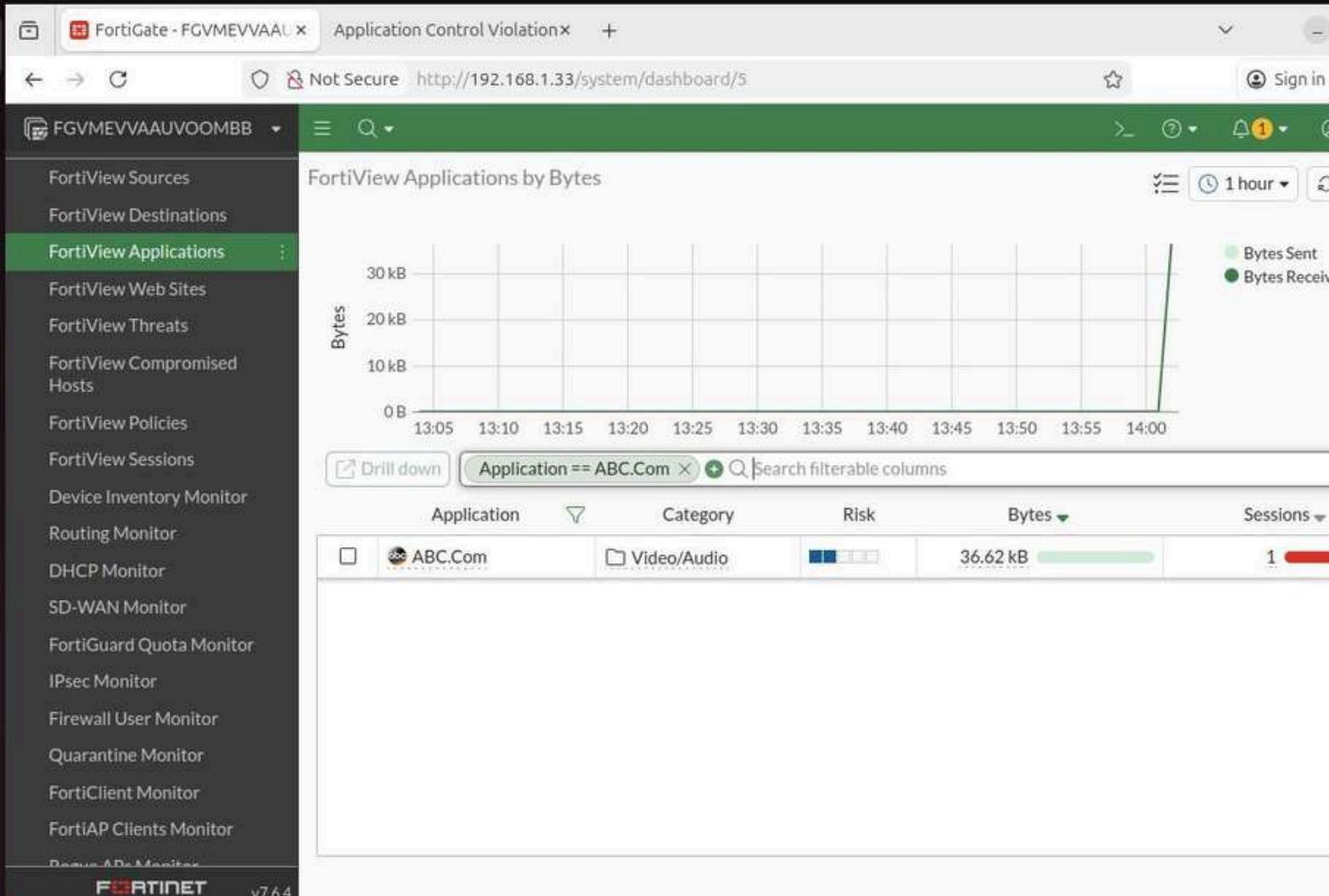
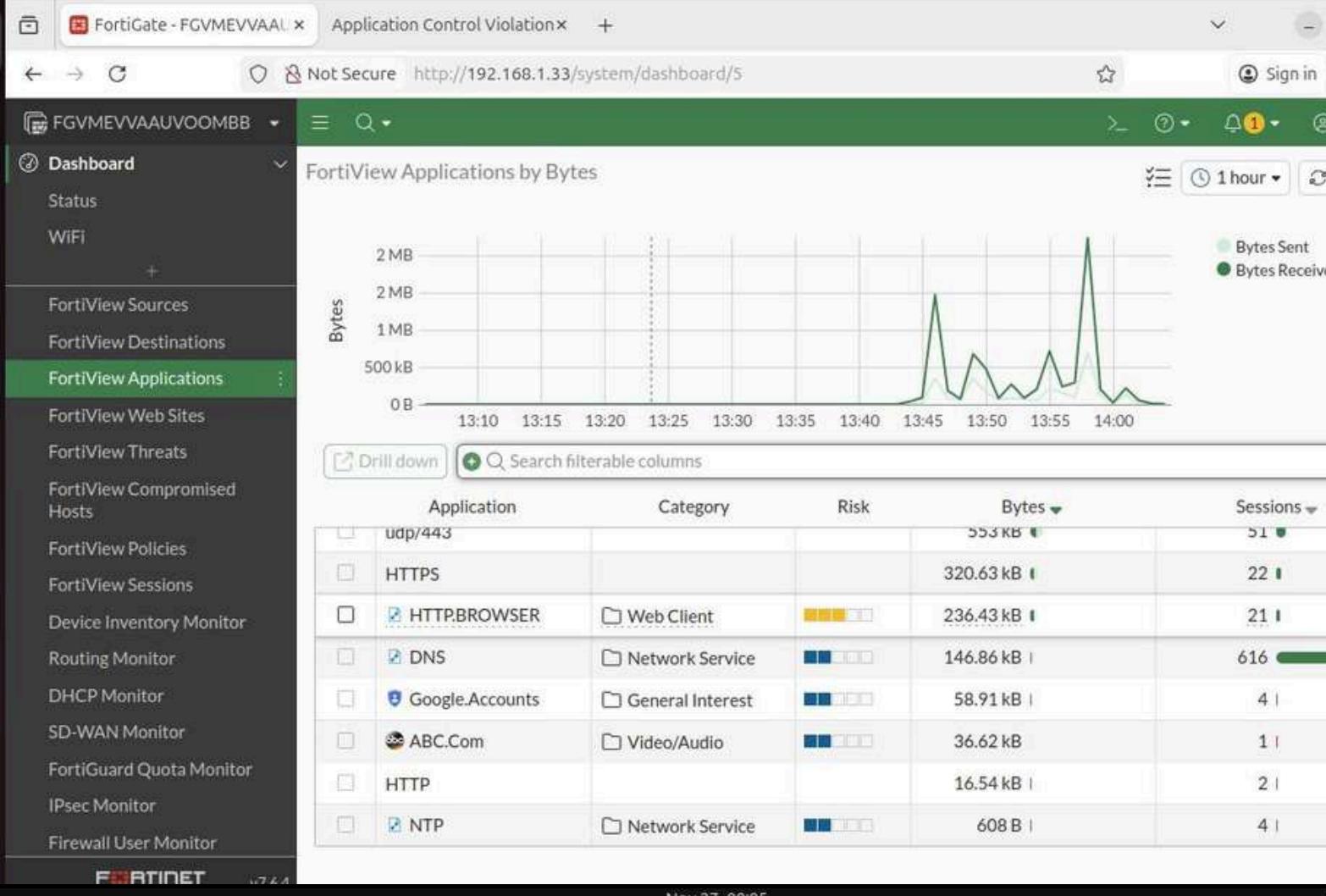
## APPLICATION CONTROL REVEALED:

### APPLICATION CONTROL SECURITY EVENTS

ABC.com session blocked  
Detected category:

Video/Audio  
SSL inspection detected  
traffic

The screenshot displays two windows from the FortiGate management interface. The top window is titled 'Application Control Violation' and shows a summary of 366 events. It includes a table for 'Application Control' with rows for Network.Service (Pass, 302), Web.Client (Pass, 63), and Video/Audio (Block, 1). The bottom window is titled 'Logs' and shows a detailed log entry for an application control violation. The log details include a timestamp (2025/11/26 07...), source (192.168.1.30), destination (18.235.2.142.251), level (Warning), and type (app-ctrl). The log ID is 1059028705, and the event was triggered by a GET request.

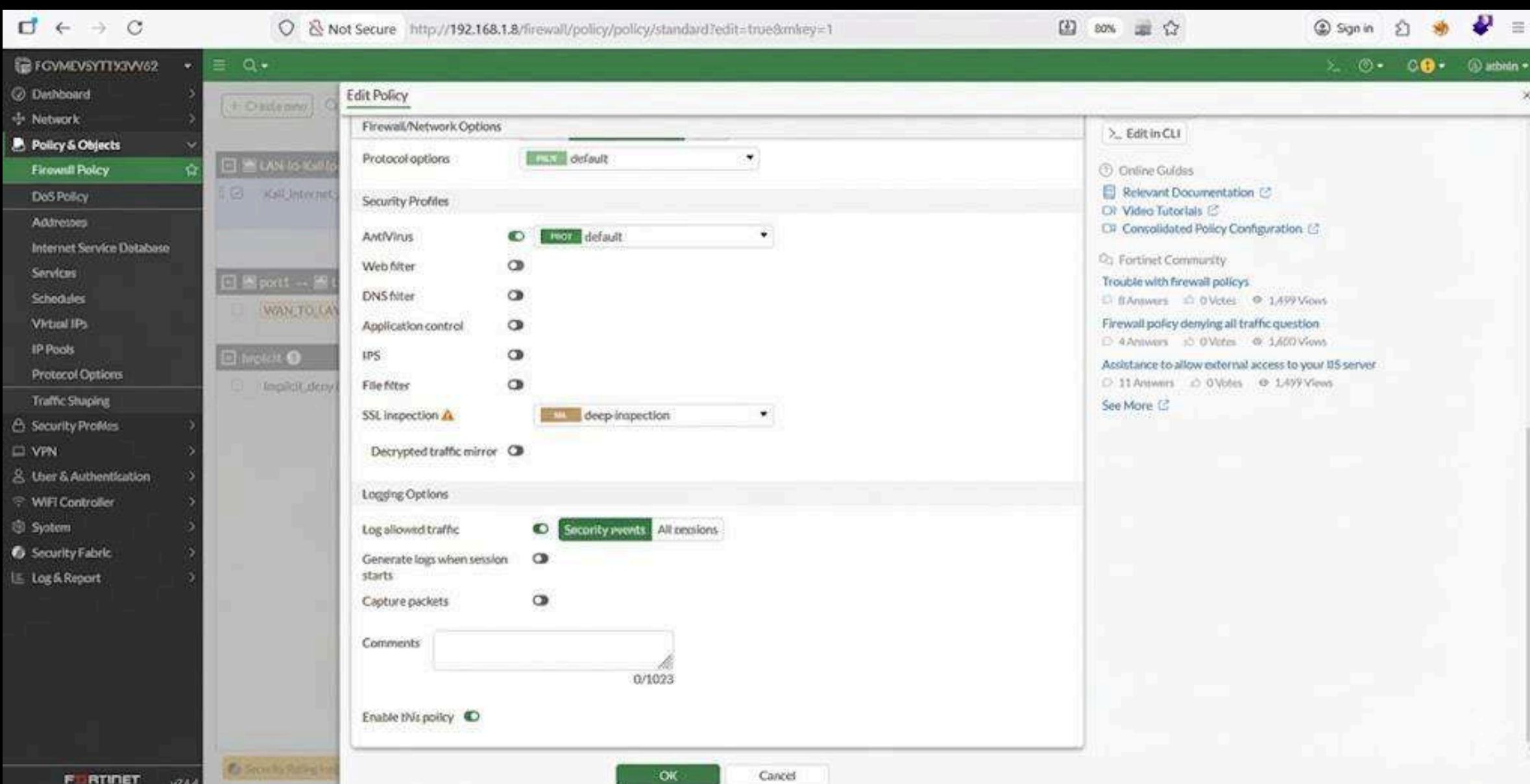


# FORTIVIEW APPLICATION DASHBOARD SHOWS:

## FORTIVIEW APPLICATION DASHBOARD SHOWS:

Top consumed apps  
Blocked applications  
Bandwidth usage

# ANTIVIRUS FIREWALL POLICY FOR MONITORING:



Forward Traffic							
Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	
2025/11/26 11:46:34	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 172.217.19.25 (apk.apk)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:48:00	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 172.217.19.25 (apk.apk)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:45:37	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 104.17.16.1:40 (remotely.ip.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:45:36	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 104.17.14.1:80 (www.dating.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:45:07	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 5.22.6.179.10 (www.be365.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:45:06	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 5.22.6.179.10 (www.be365.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:44:39	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 172.217.11.204 (george.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:44:18	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 34.537.221.82 (detectportal.firefox.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:28:55	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 34.537.221.82 (detectportal.firefox.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:26:02	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 34.537.221.82 (detectportal.firefox.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 11:15:39	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 143.250.255.35 (mimicbot-in-43.16.100.net)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 10:52:05	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 142.250.205.45 (mimicbot-in-74.54.100.net)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 10:51:59	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 34.537.221.82 (detectportal.firefox.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 10:49:54	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 34.537.221.82 (detectportal.firefox.com)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 10:47:55	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 142.250.200.238 (mimicbot-in-74.54.100.net)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	
2025/11/26 10:47:51	192.168.10.10	■ 00:0c:29:2a:8e:36	■ 142.250.200.238 (mimicbot-in-74.54.100.net)	HTTP	🚫 Deny (Deny; UTM Blocked)	Kali_Internet_Access_with_Filter (1)	

Date/Time	Source	Device	Destination	Application Name	Result	Log Details
11/26 10:26:51	10.0.11.50		100.65.0.254	HTTP	🚫 Deny (Deny; UTM Blocked)	
11/26 10:24:41	10.0.11.50		100.65.0.254	HTTP	🚫 Deny (Deny; UTM Blocked)	
11/26 10:23:42	100.65.0.101		■ 34.117.188.166 (spocs.getpocket.com)	HTTPS	✓ Accept (1.06 kB / 3.38 kB)	
11/26 10:23:42	100.65.0.101		■ 34.110.138.217 (merino.services.mozilla.com)	HTTPS	✓ Accept (1.06 kB / 3.42 kB)	
11/26 09:31:26	10.0.11.50		100.65.0.254	FTP	✓ Accept (1.82 kB / 1.73 kB)	
11/26 09:31:08	10.0.11.50		100.65.0.254	tcp/45809	🚫 Deny (Deny; UTM Blocked)	
11/26 09:31:08	10.0.11.50		100.65.0.254	tcp/6467	🚫 Deny (Deny; UTM Blocked)	
11/26 09:31:03	10.0.11.50		100.65.0.254	tcp/50796	🚫 Deny (Deny; UTM Blocked)	

Date/Time	Service	Service	File Name	Virus/Botnet	User	Details	Action	Infection Type	Log Details
2025/11/26 09:31:03	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	🚫 Blocked	Malicious	
2025/11/26 09:31:03	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	🚫 Blocked	Malicious	
2025/11/26 09:31:03	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	🚫 Blocked	Malicious	

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action	Infection
2024/11/26 10:26:50		HTTP	10.0.11.50	eicar.com.txt	EICAR_TEST_FILE		URL: http://100.65.0.254/eicar.com.txt	🚫 Blocked
2024/11/26 10:24:40		HTTP	10.0.11.50	eicar.com.txt	EICAR_TEST_FILE		URL: http://100.65.0.254/eicar.com.txt	🚫 Blocked

# ANTIVIRUS MONITORING LOGS LOG ENTRIES DISPLAY:

# ANTIVIRUS MONITORING LOGS LOG ENTRIES DISPLAY:

Malware attempts  
File types scanned  
Actions taken  
(blocked/quarantined)



## ANTIVIRUS FORTIVIEW THREAT DASHBOARD

## ANTIVIRUS FORTIVIEW THREAT DASHBOARD

- Shows attempted EICAR download
- Classified as malware
- Action: Blocked

## PROJECT ACHIEVEMENTS

Deployed 3 major profiles  
Enforced UTM security  
Validated via logs  
Demonstrated real-world  
blocking

# SECURITY IMPROVEMENTS FORTIGATE NOW PROVIDES:

## SECURITY IMPROVEMENTS FORTIGATE NOW PROVIDES:

- Malware protection
- Web content control
- Application control
- Full traffic visibility

# RECOMMENDATIONS

## RECOMMENDATIONS

- Enable FortiAnalyzer for detailed reports
- Add Sandbox integration
- Deploy DNS filtering
- Expand application policies

# WHY THESE IMPROVEMENTS?

## WHY THESE IMPROVEMENTS?

- FortiAnalyzer: Provides deeper insights and more detailed security reports.
- Sandbox: Protects against zero-day and advanced malware.
- DNS Filtering: Blocks malicious domains early and reduces risk.
- Expanded App Policies: Improves control, prevents bypass apps, and manages bandwidth.

## CONCLUSION:

FINAL CONCLUSION  
THE IMPLEMENTED SECURITY  
PROFILES IMPROVED:

- Network protection
- Traffic visibility
- User control
- Threat detection



# THANK YOU!

