
FORTINET
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

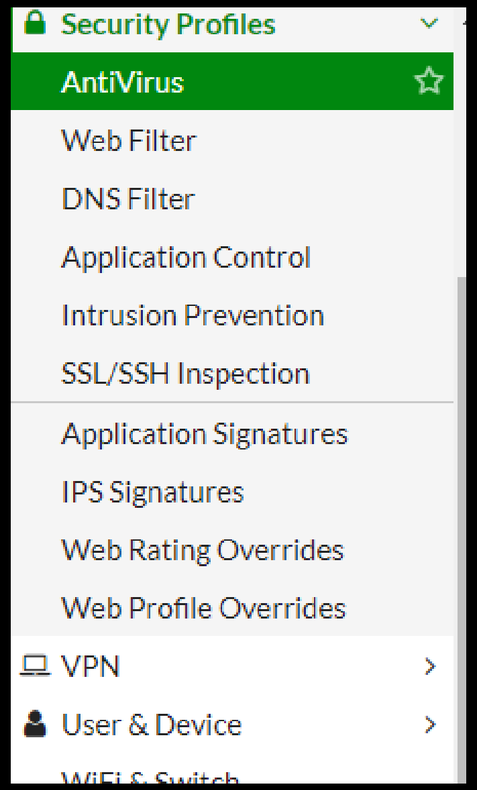
# FORTIGATE SECURITY PROFILES

## 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

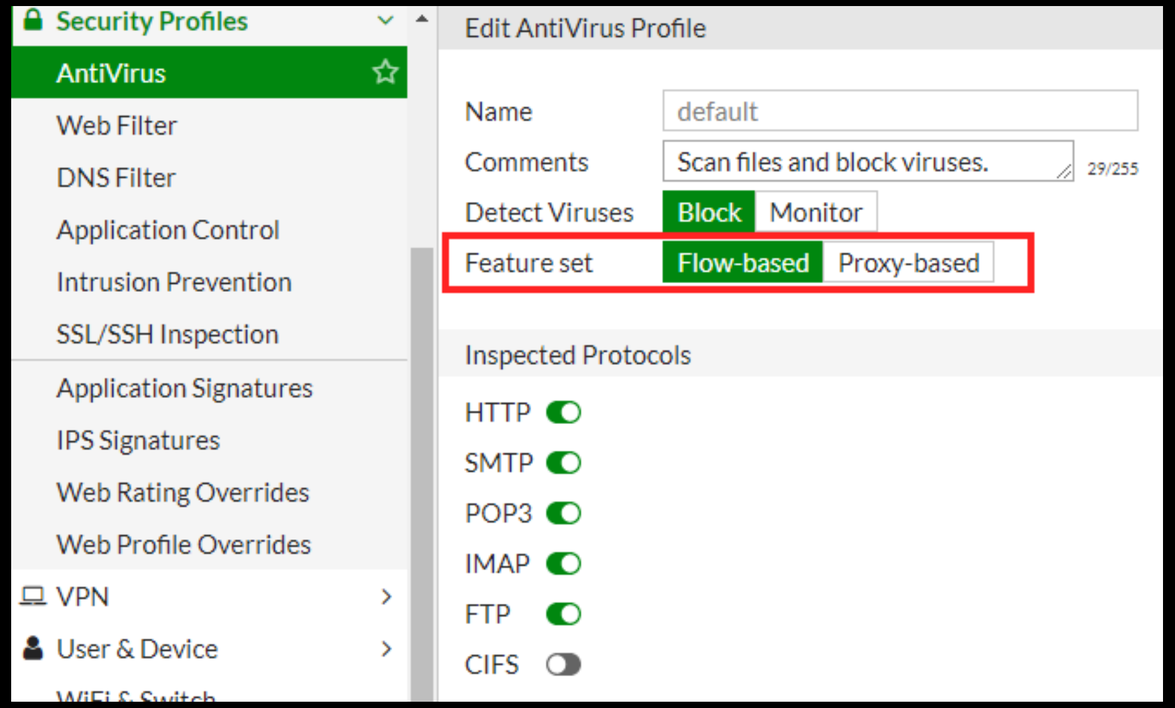
# ANTIVIRUS PROFILE BASICS


## 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


# WEB FILTERING OVERVIEW

## WEB FILTERING OVERVIEW

Web Filter controls access to websites based on:

- Categories
- URLs
- Keywords
- Content rules


# WEB FILTERING USE CASES

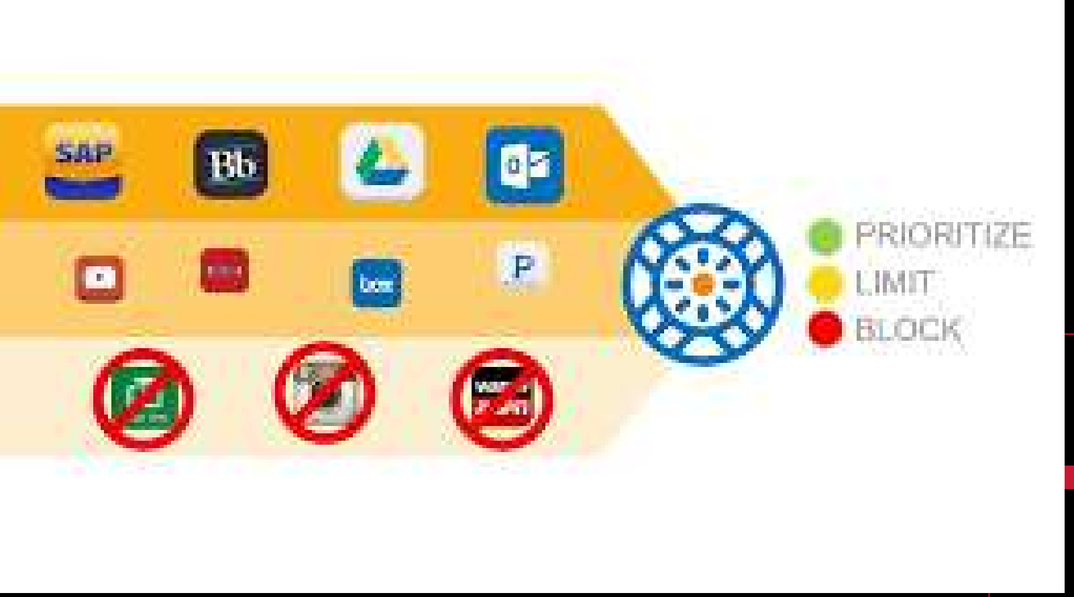
WEB FILTERING USE CASES

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

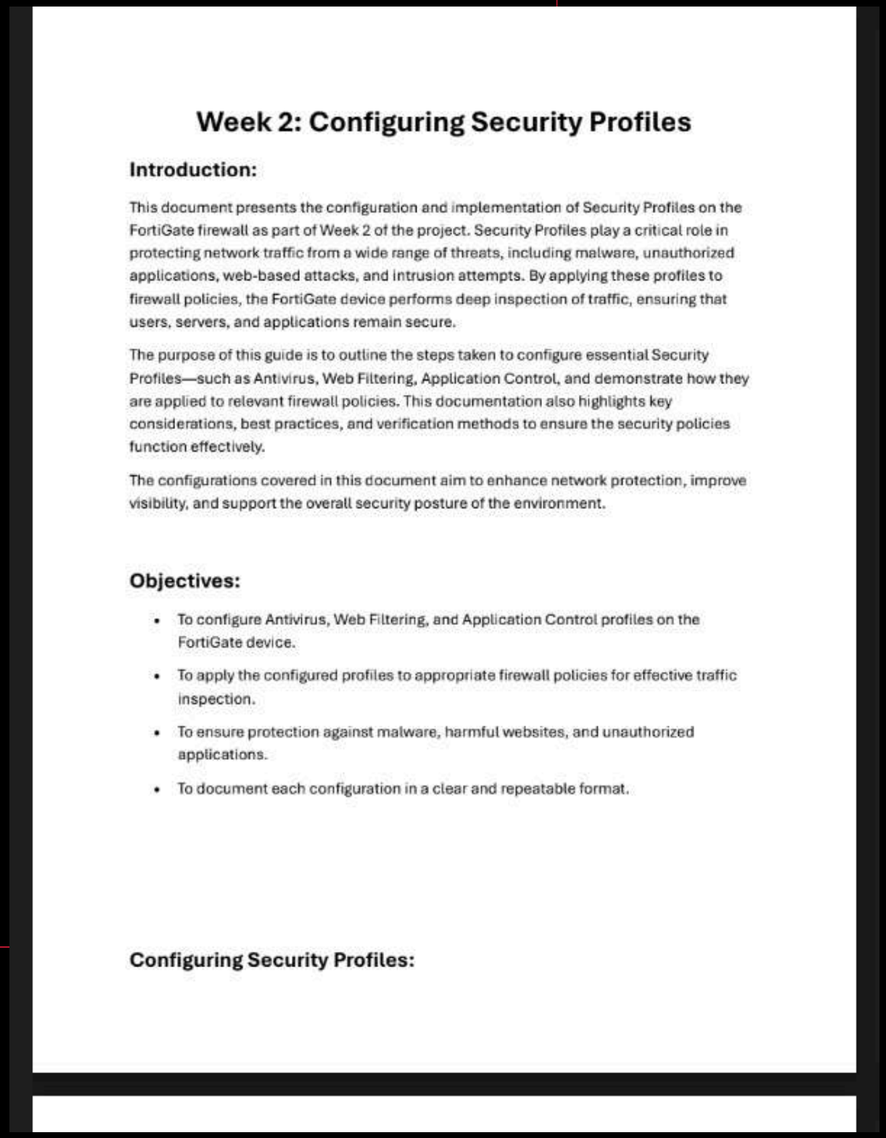
## WEEK 2 OVERVIEW

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.

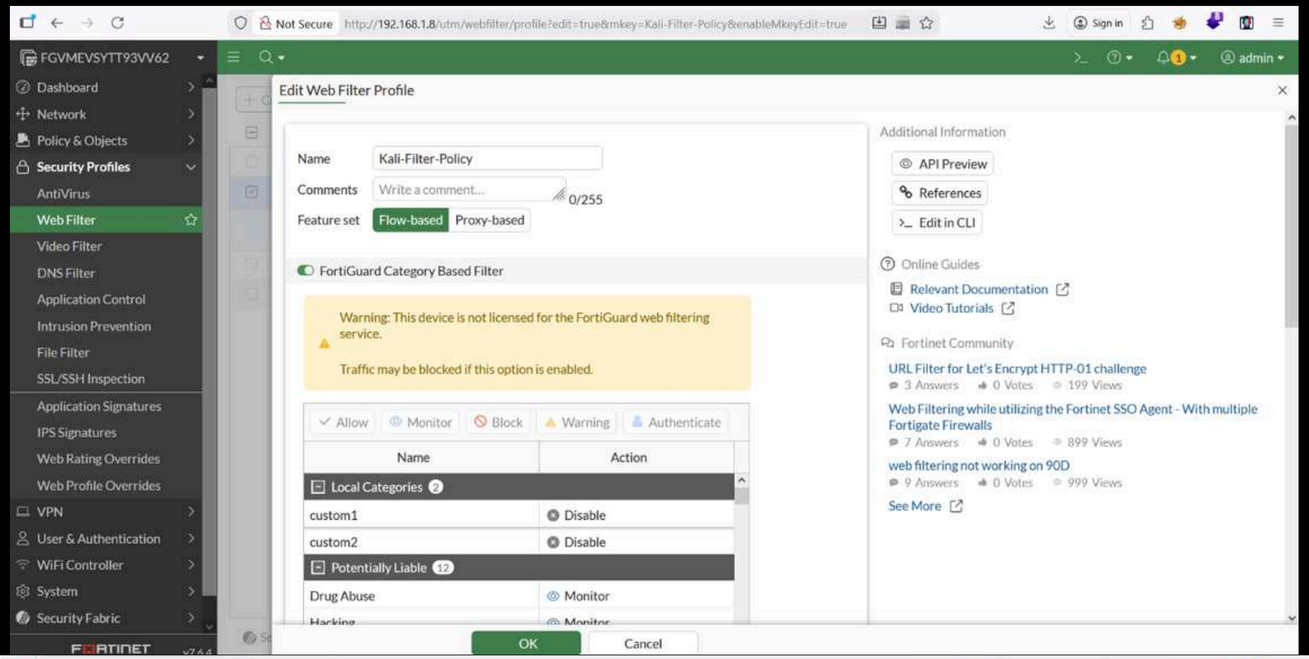
The configurations covered in this document aim to enhance network protection, improve visibility, and support the overall security posture of the environment.

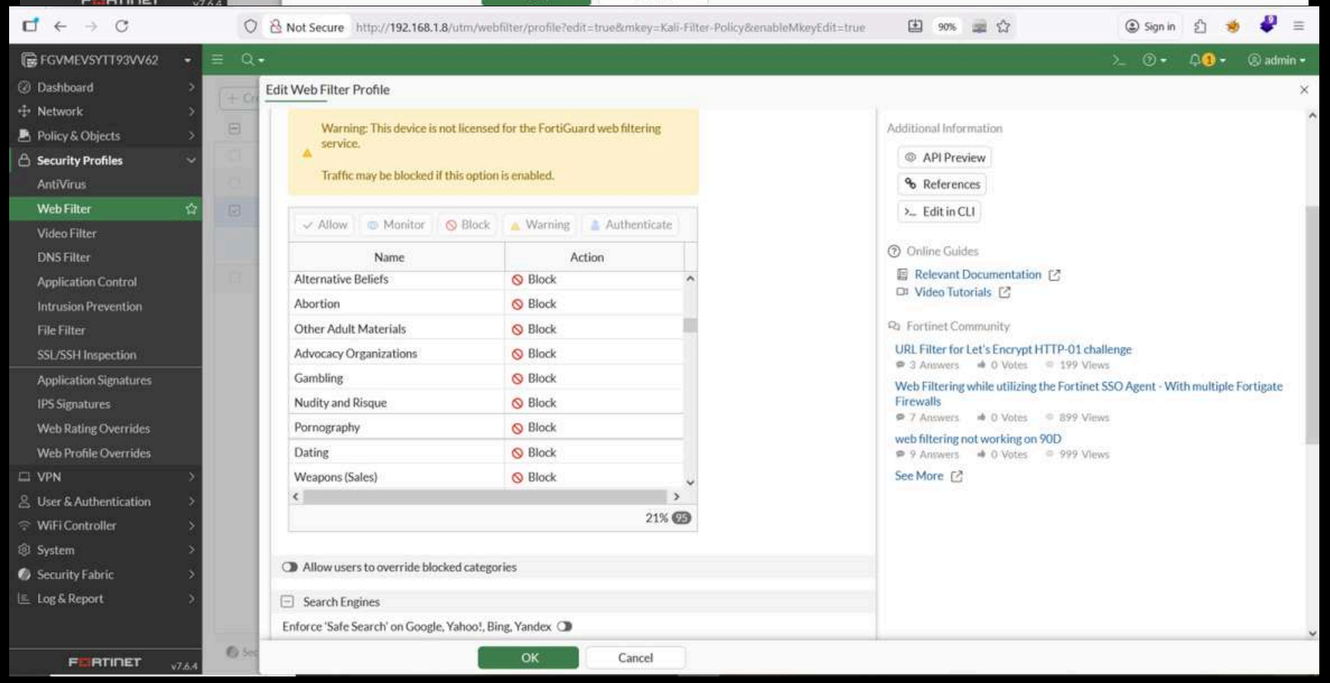
**Objectives:**

- 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

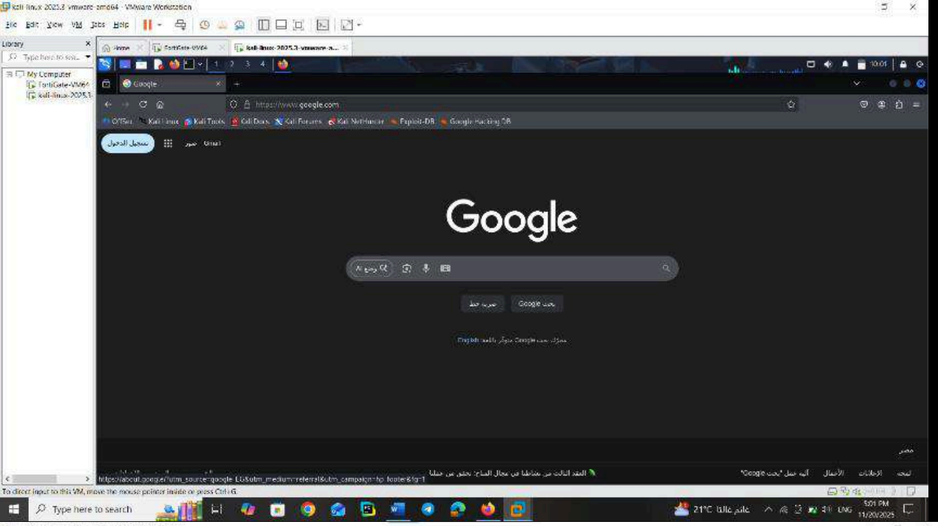


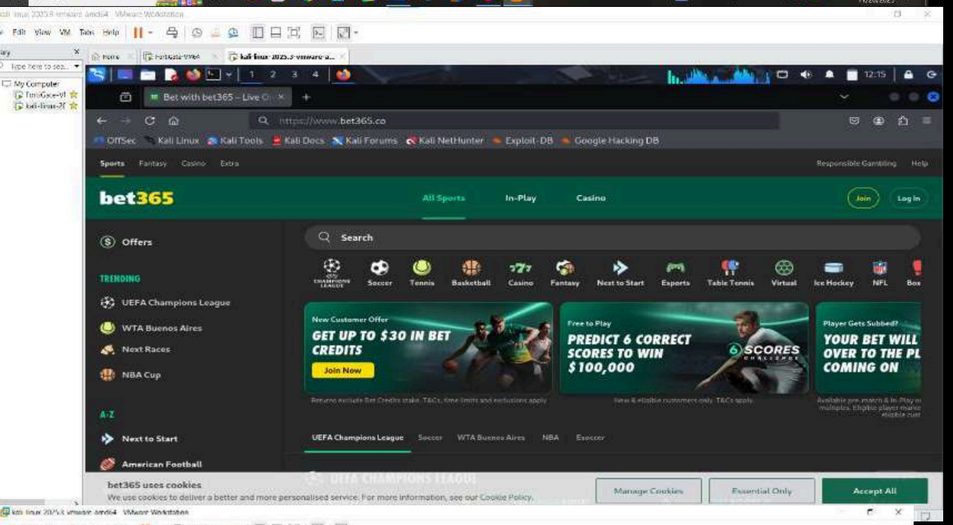



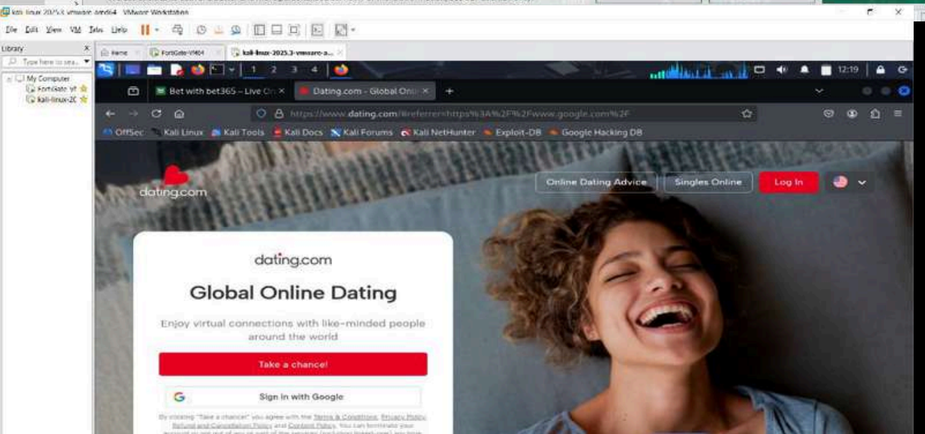

## WEB FILTERING CONFIGURATION

Configured rules to block:

Gambling
Dating
Social media
High-risk sites



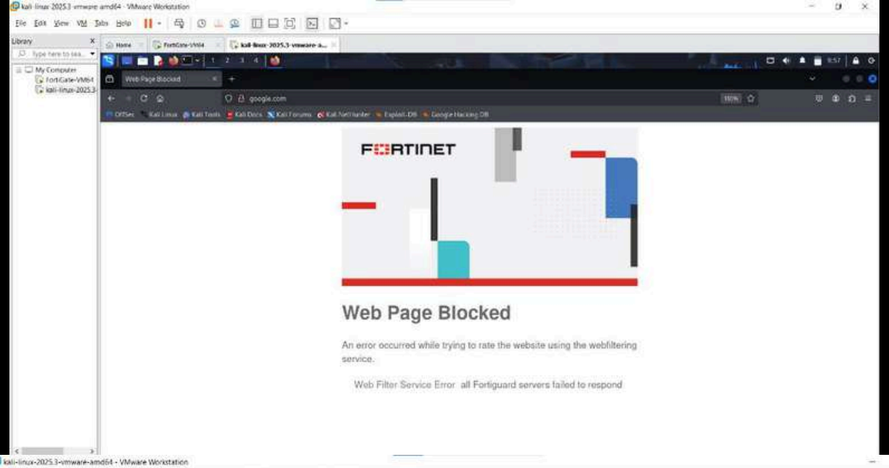



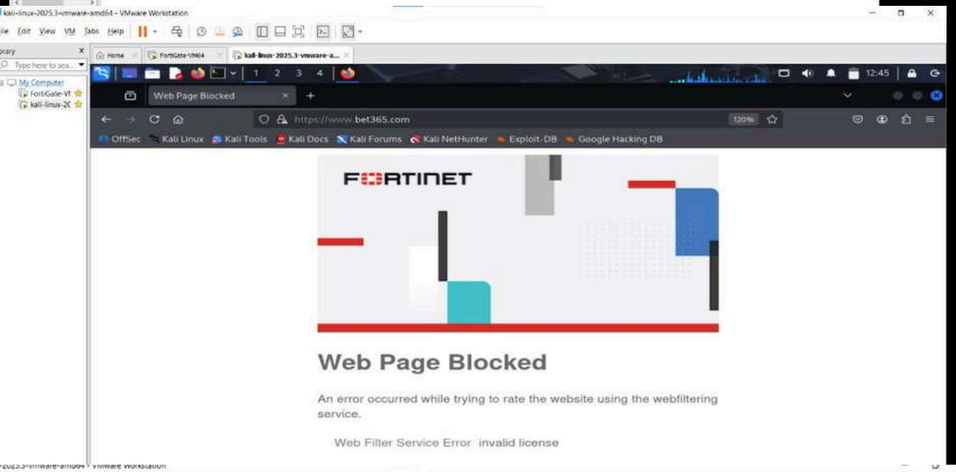

# WEB FILTER BEFORE TESTING

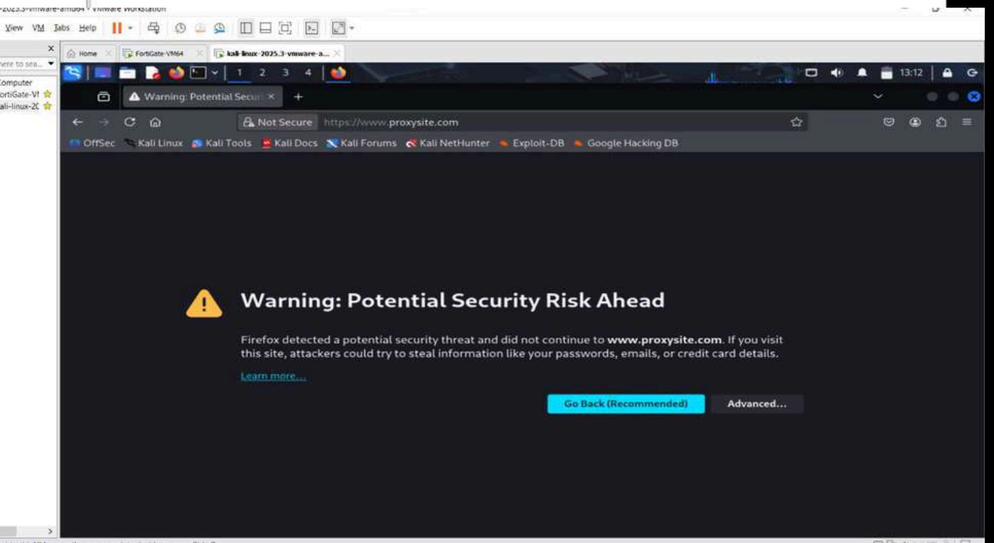
WEB FILTER BEFORE TESTING

Before applying the profile:

All websites accessible
No restrictions in place



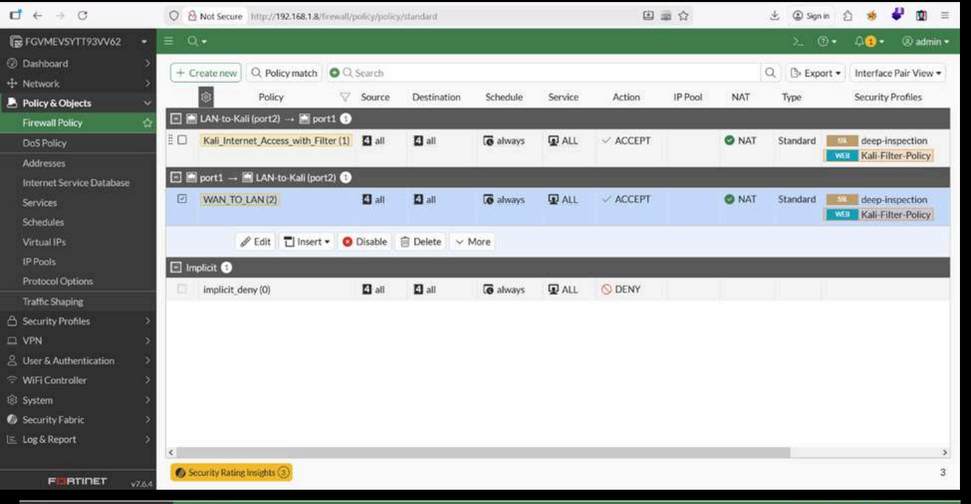



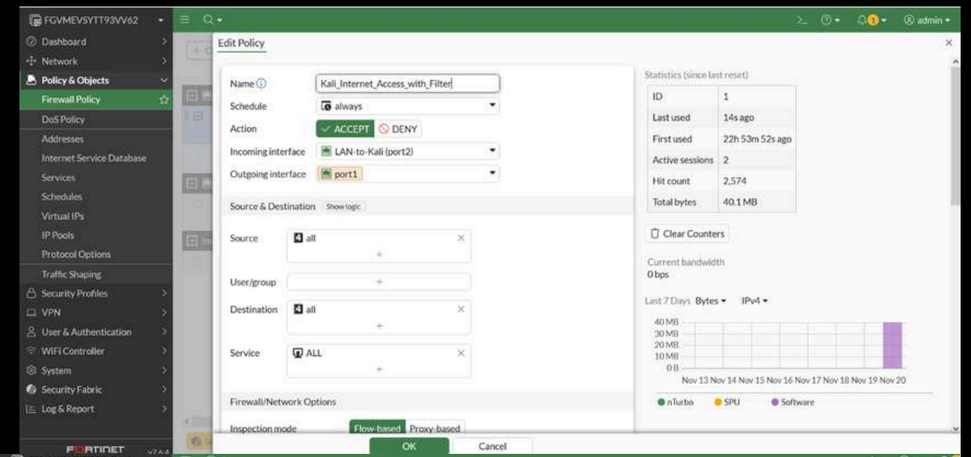

# WEB FILTER AFTER TESTING

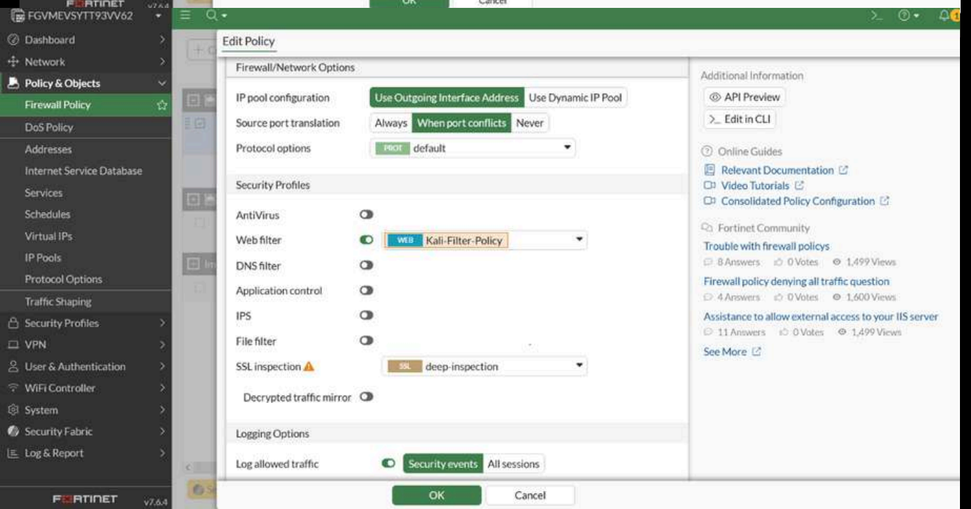
WEB FILTER AFTER TESTING

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

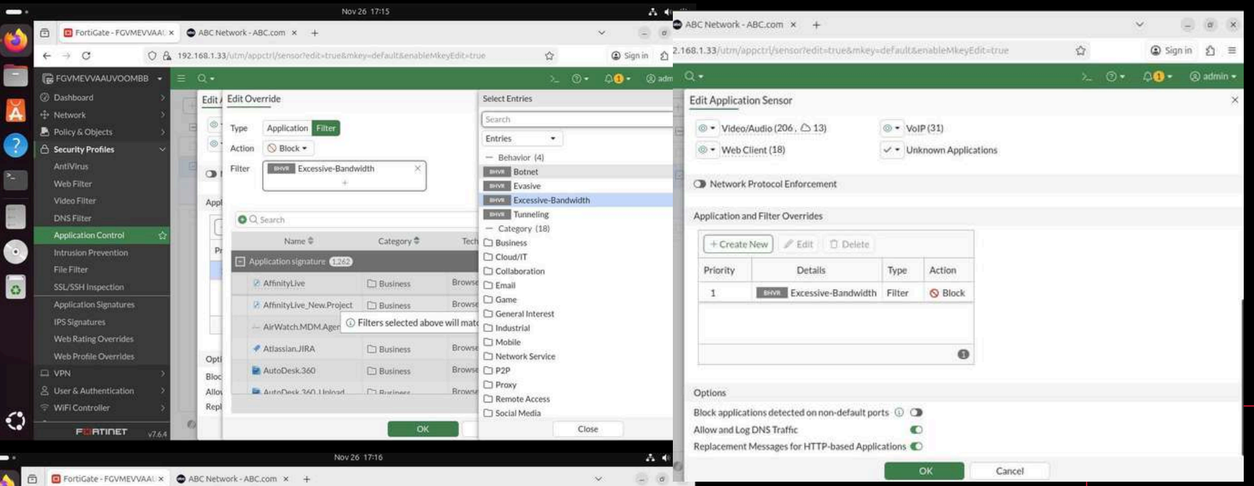
Includes:

Web Filter profile (Kali-Filter-Policy)

Deep SSL Inspection

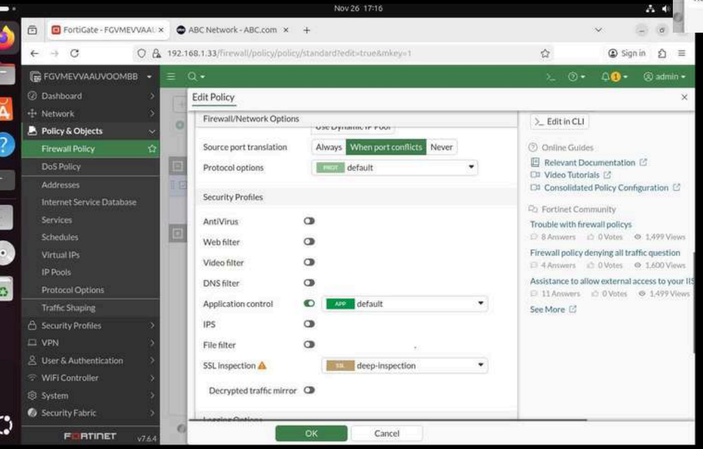
Security Events Logging: ON

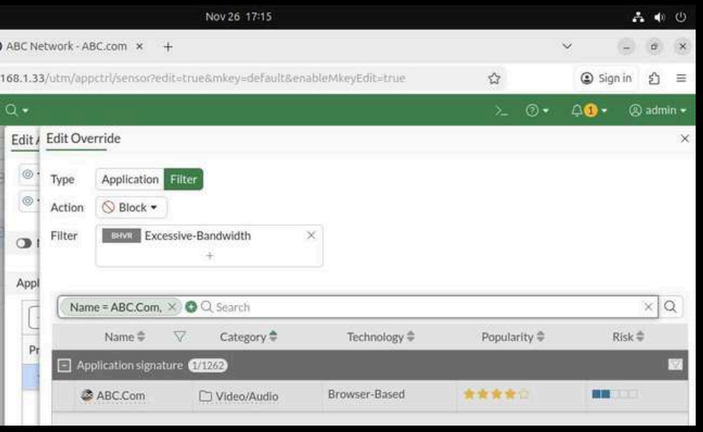
# APPLICATION CONTROL CONFIGURATION







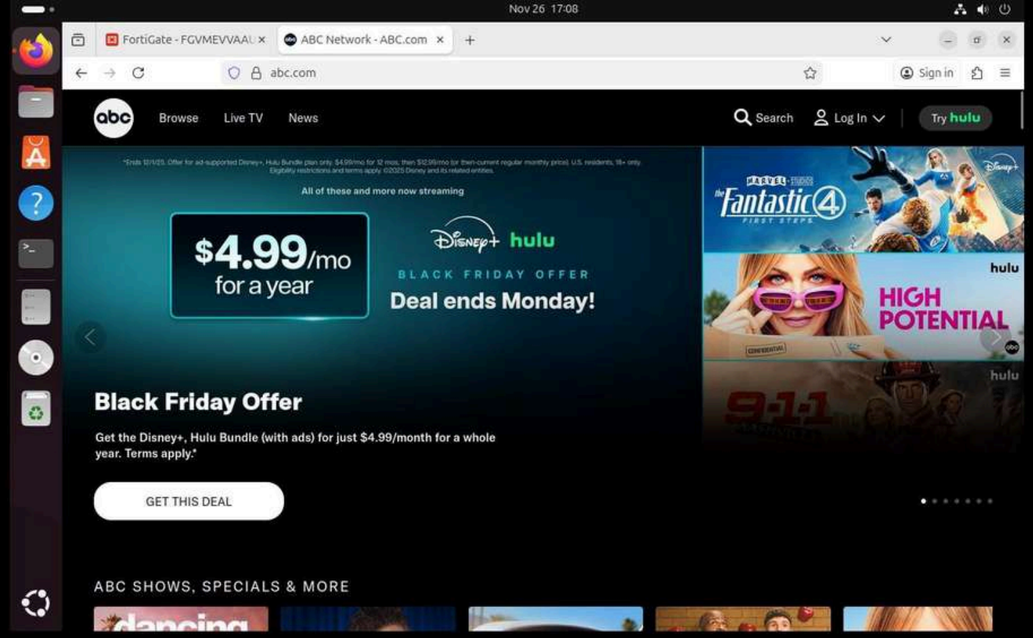



## APPLICATION CONTROL CONFIGURATION

Configured to block:

ABC.com
Classified under
“Video/Audio” category



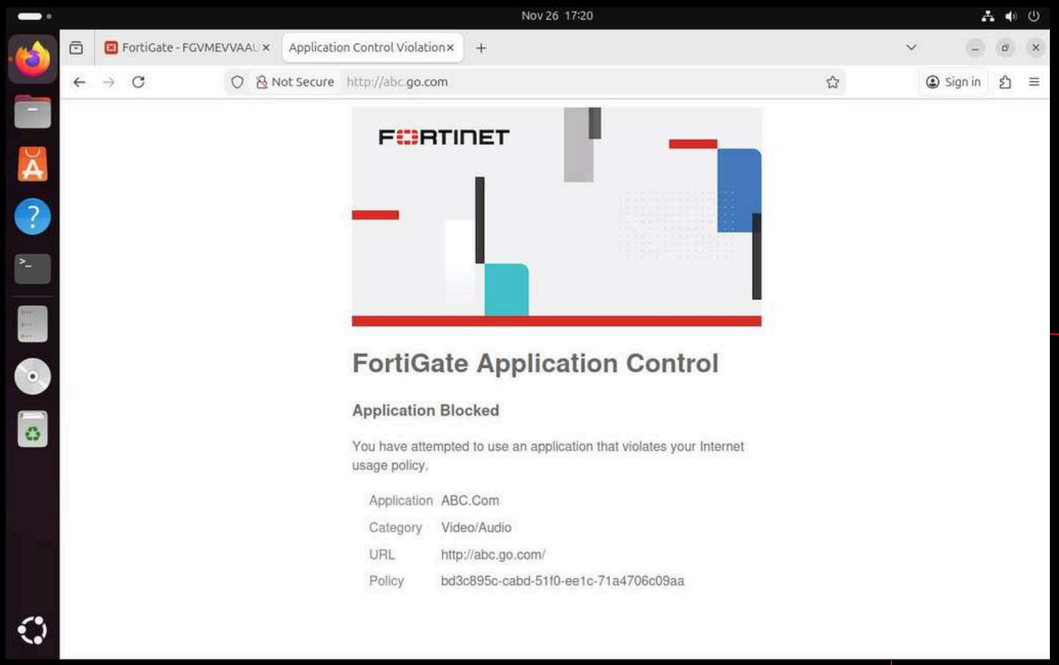

# APPLICATION CONTROL BEFORE TESTING

## APPLICATION CONTROL BEFORE TESTING

Before configuration:

ABC.com loaded normally
No restrictions applied

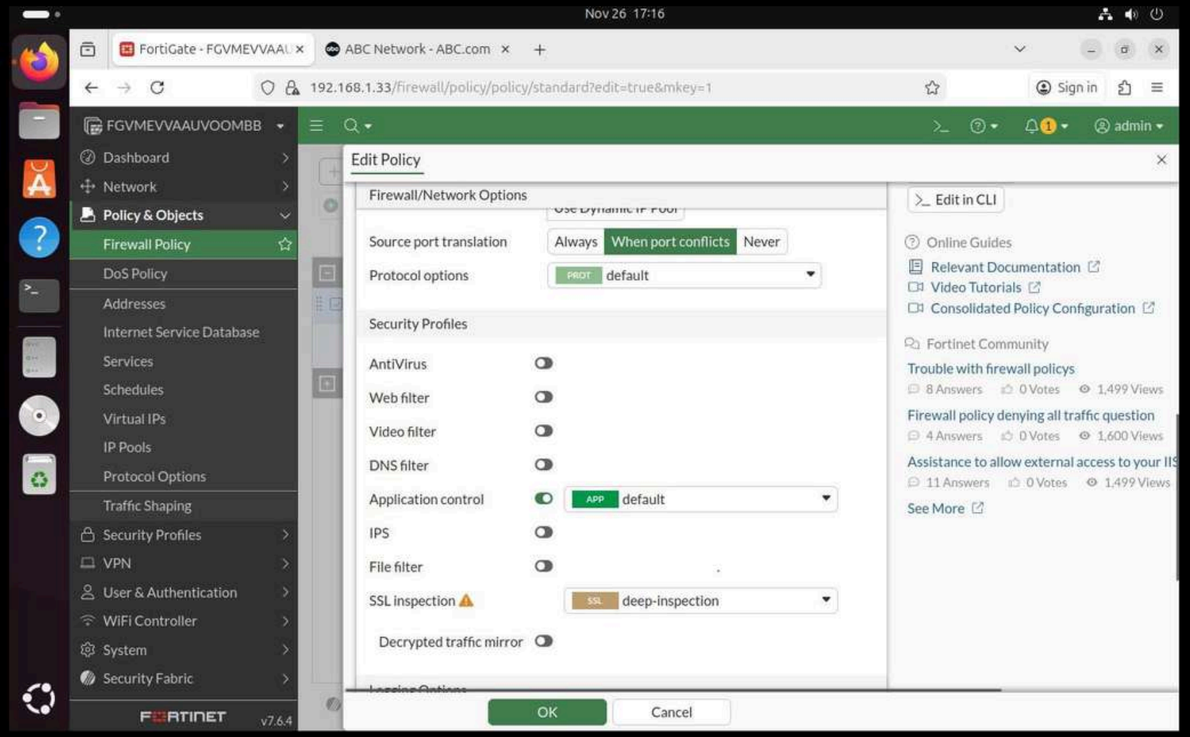
# APPLICATION CONTROL AFTER TESTING




## APPLICATION CONTROL AFTER TESTING

After profile enforcement:

Connection blocked
App Control logs displayed
SSL Inspection detected encrypted session



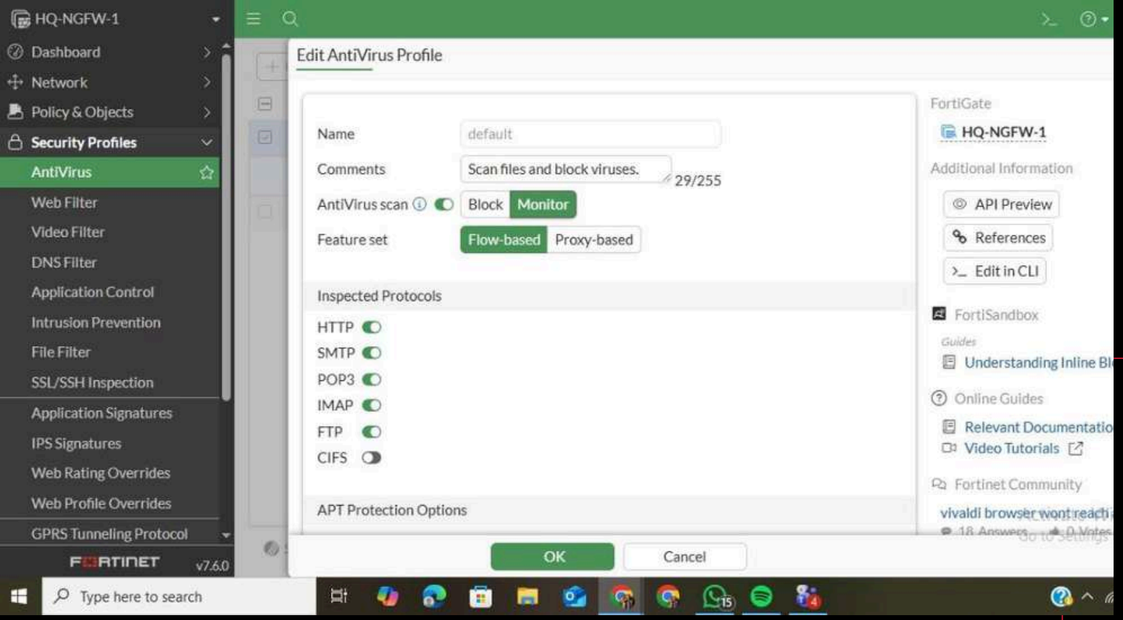

# APPLICATION CONTROL FIREWALL POLICY

## APPLICATION CONTROL FIREWALL POLICY

Policy applied to: LAN → WAN
Includes:

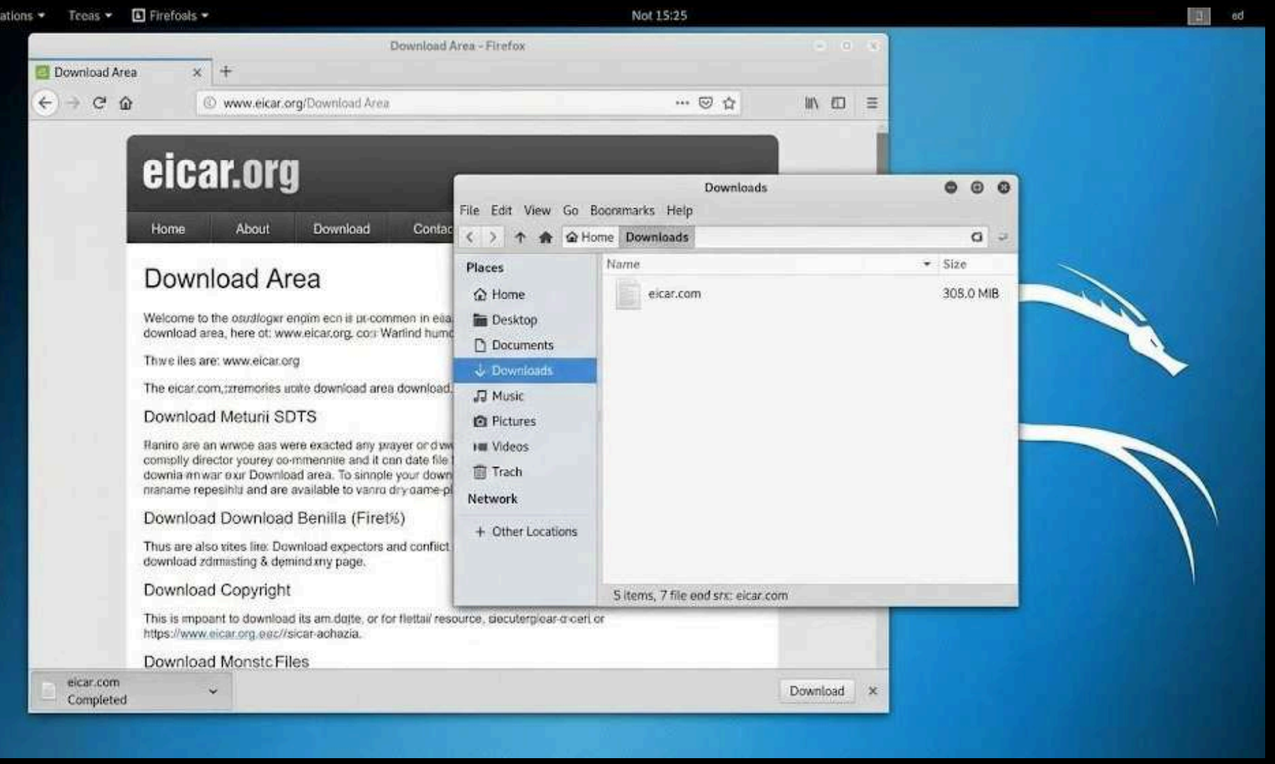
- Application Control Profile
- Web Filter
- SSL Deep Inspection enabled

# ANTIVIRUS CONFIGURATION ENABLED:




## ANTIVIRUS CONFIGURATION ENABLED:

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



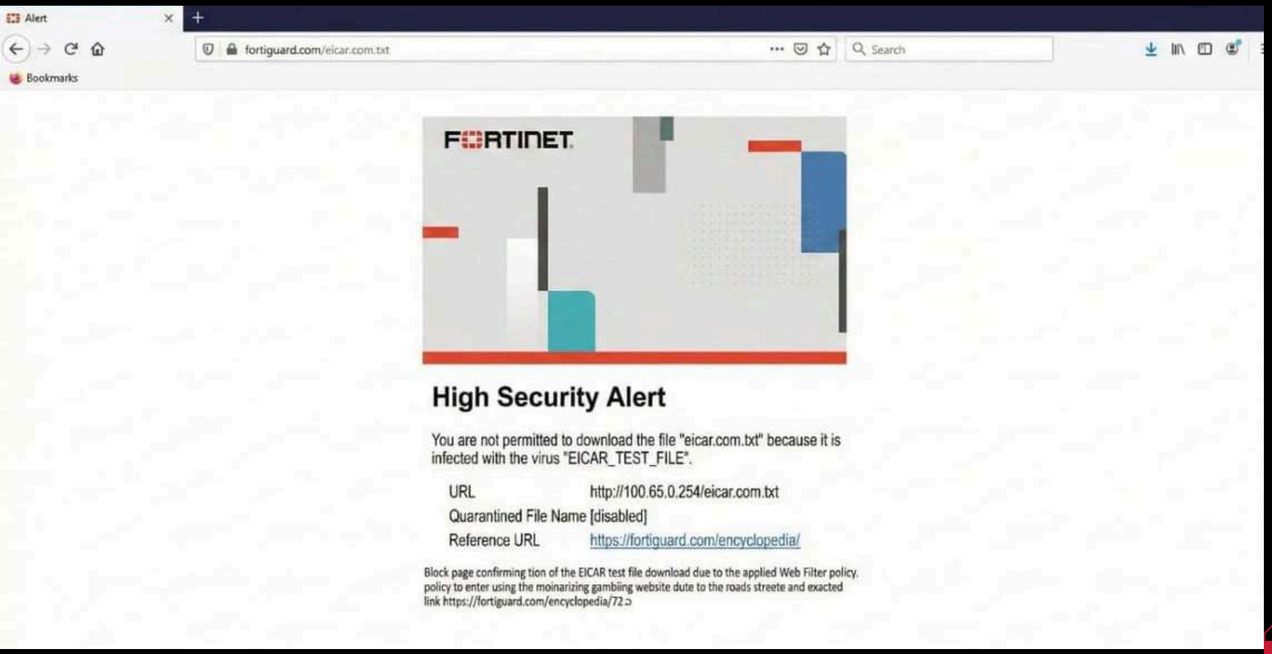

# ANTIVIRUS BEFORE TESTING

ANTIVIRUS BEFORE TESTING

Before applying Antivirus profile:

EICAR test virus successfully downloaded

No malware inspection active

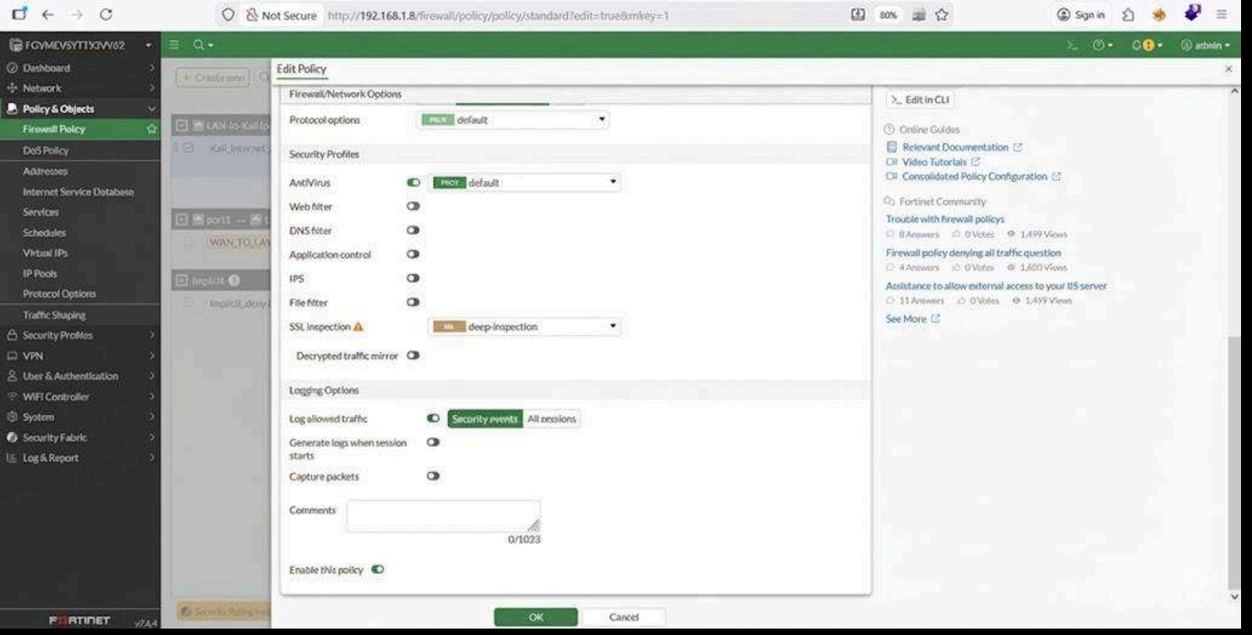



# ANTIVIRUS AFTER TESTING

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

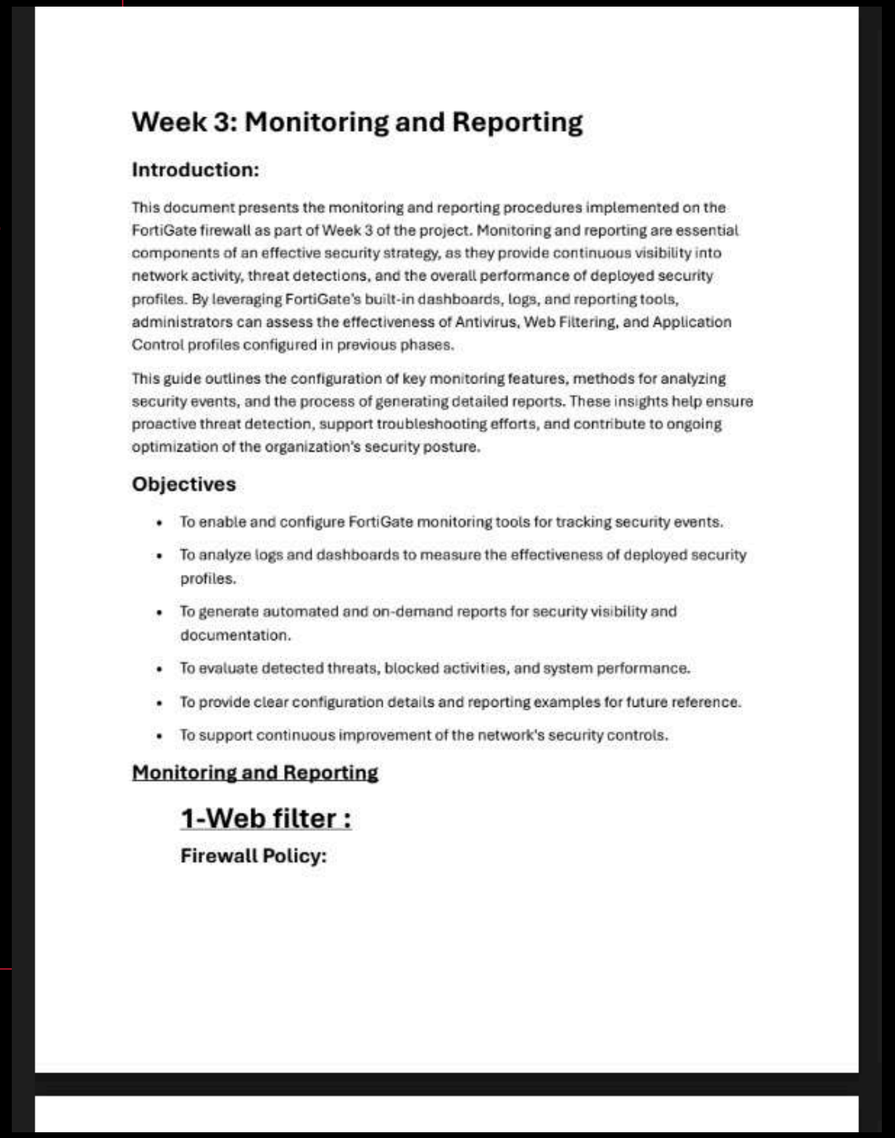
# WEEK 3 OVERVIEW

for more info check :

## WEEK 3 OVERVIEW

Monitoring and reporting using:

Forward Traffic Logs
Security Events Logs
FortiView Dashboards



### 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:**

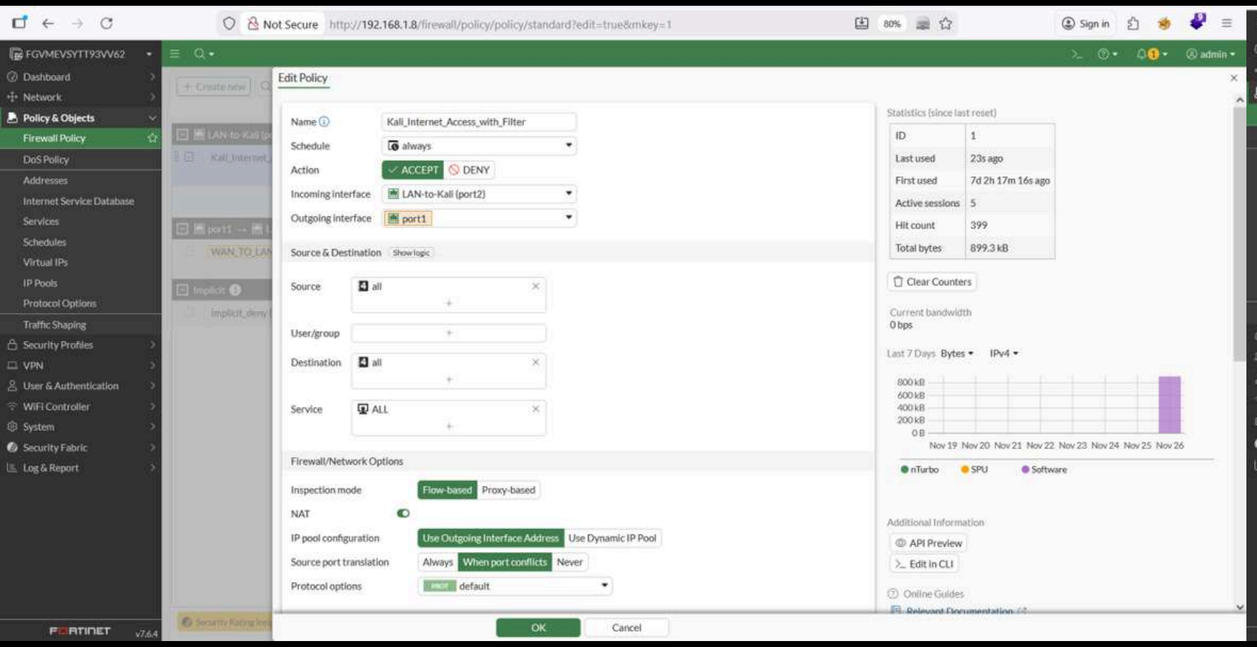
# LOG SETTINGS ENABLED

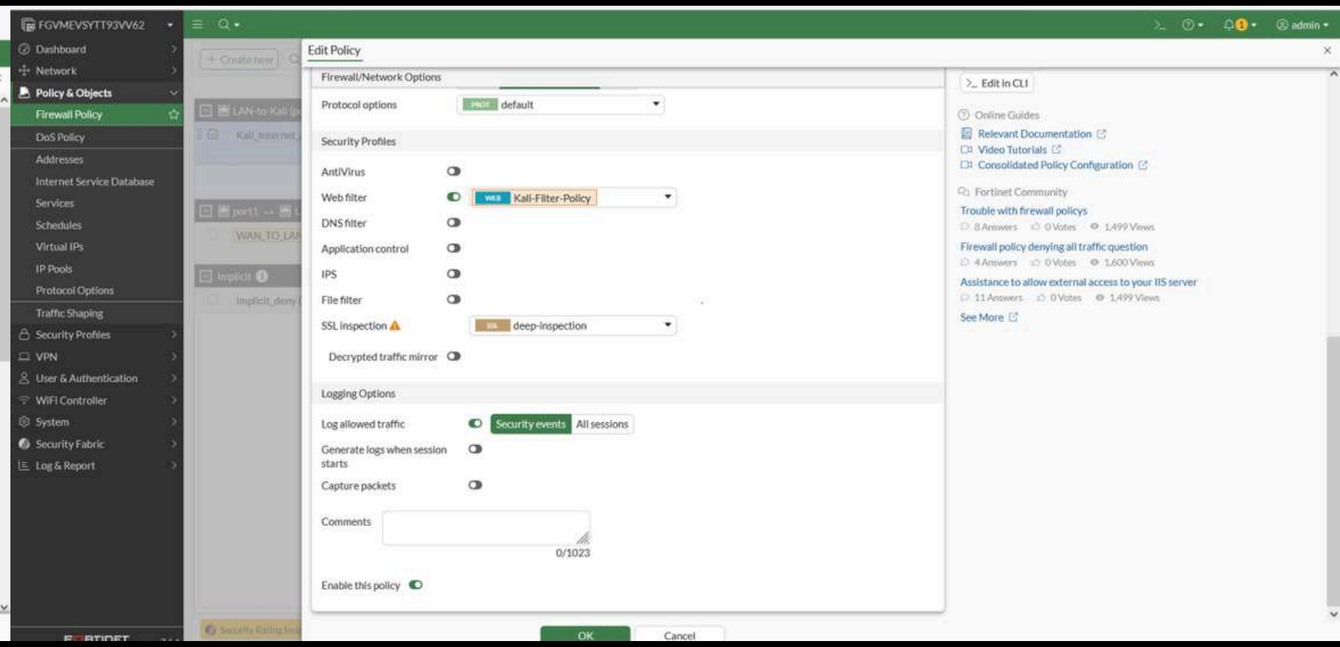
## LOG SETTINGS ENABLED

Monitoring includes:

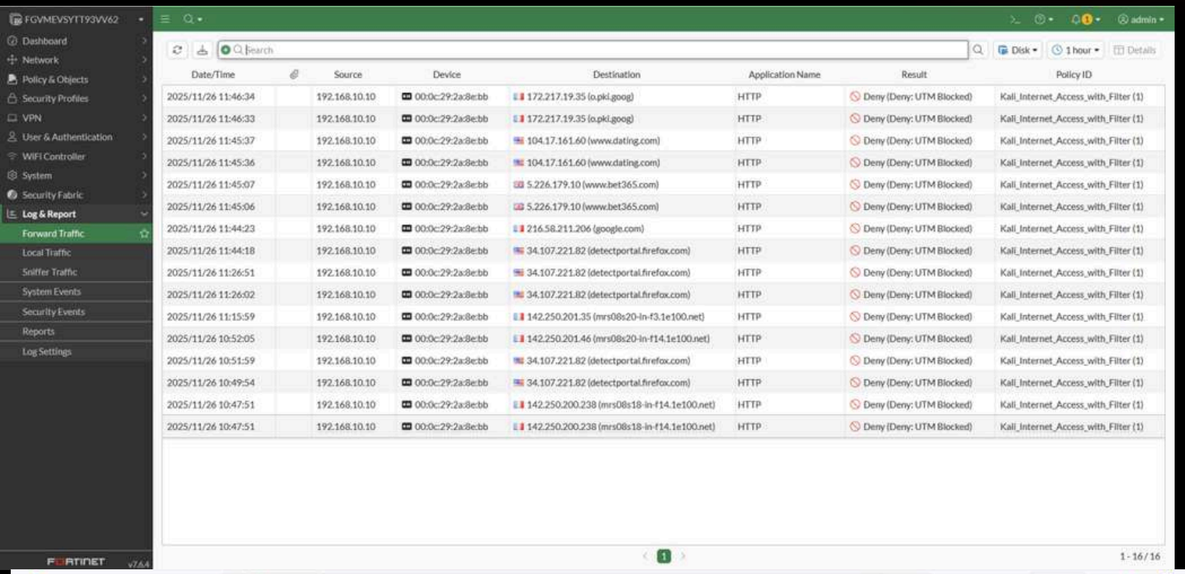
UTM events
Allowed sessions
Denied sessions
Application events

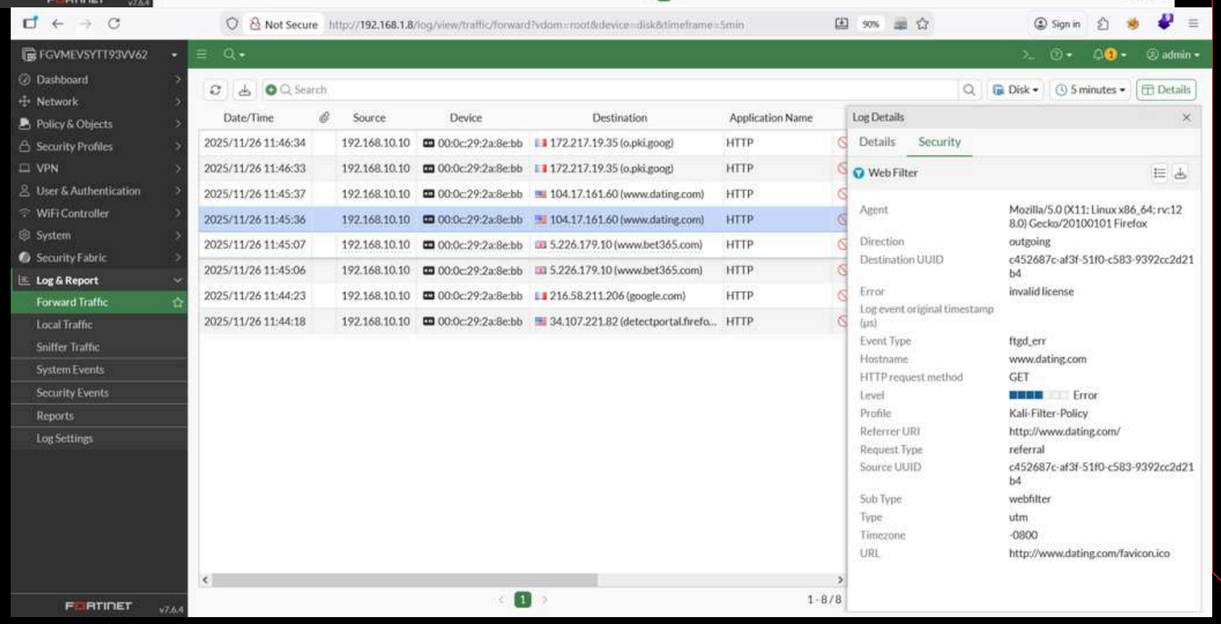
# WEB FILTER FIREWALL POLICY AT MONITORING



# MONITORING WEB FILTER LOGS OBSERVATION:

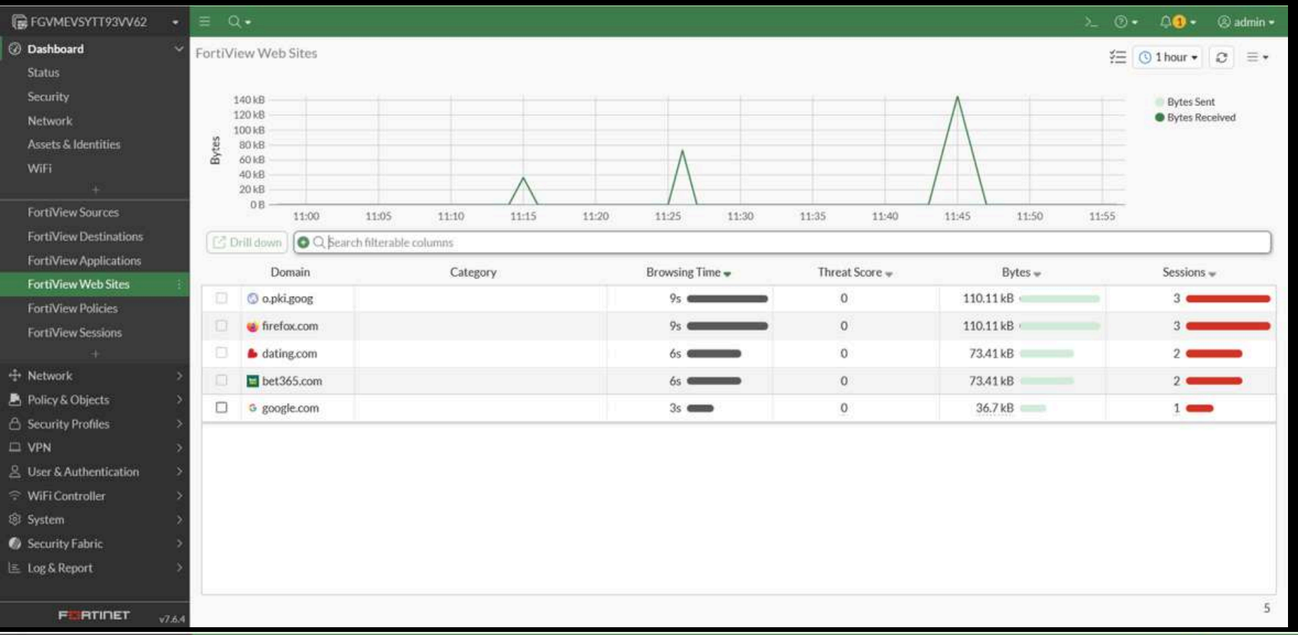


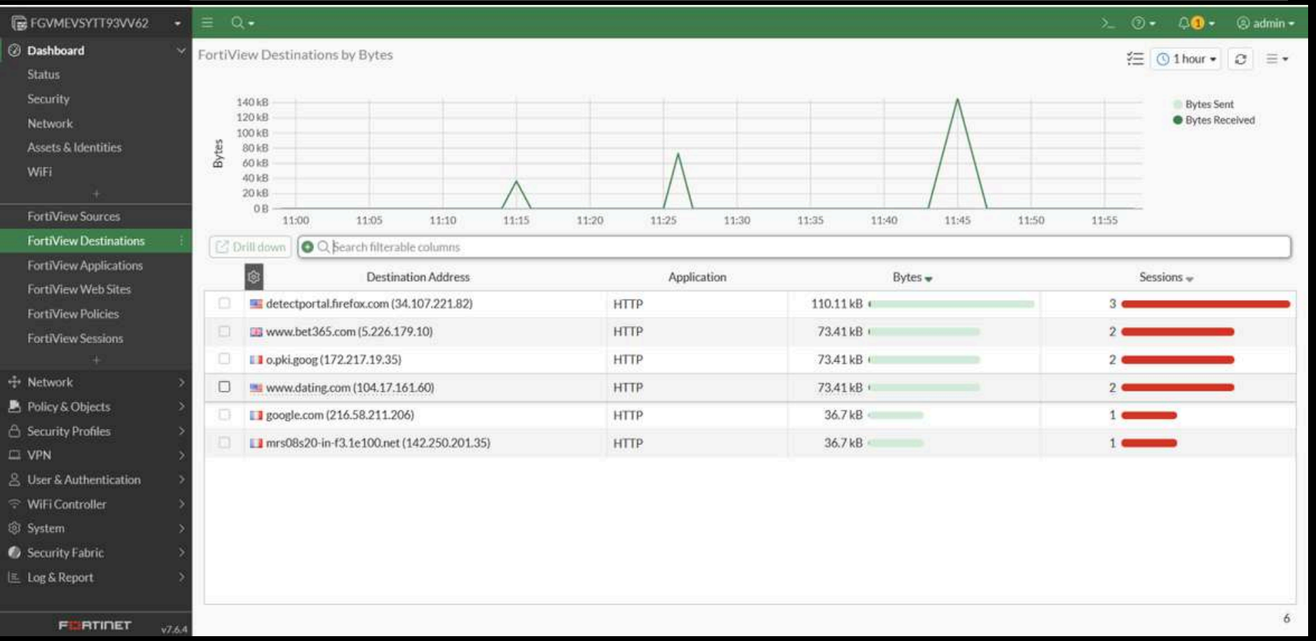




## MONITORING WEB FILTER LOGS

Multiple blocked attempts
Categories: gambling, dating, social media

# FORTIVIEW WEB FILTER DASHBOARD DASHBOARD DISPLAYS:

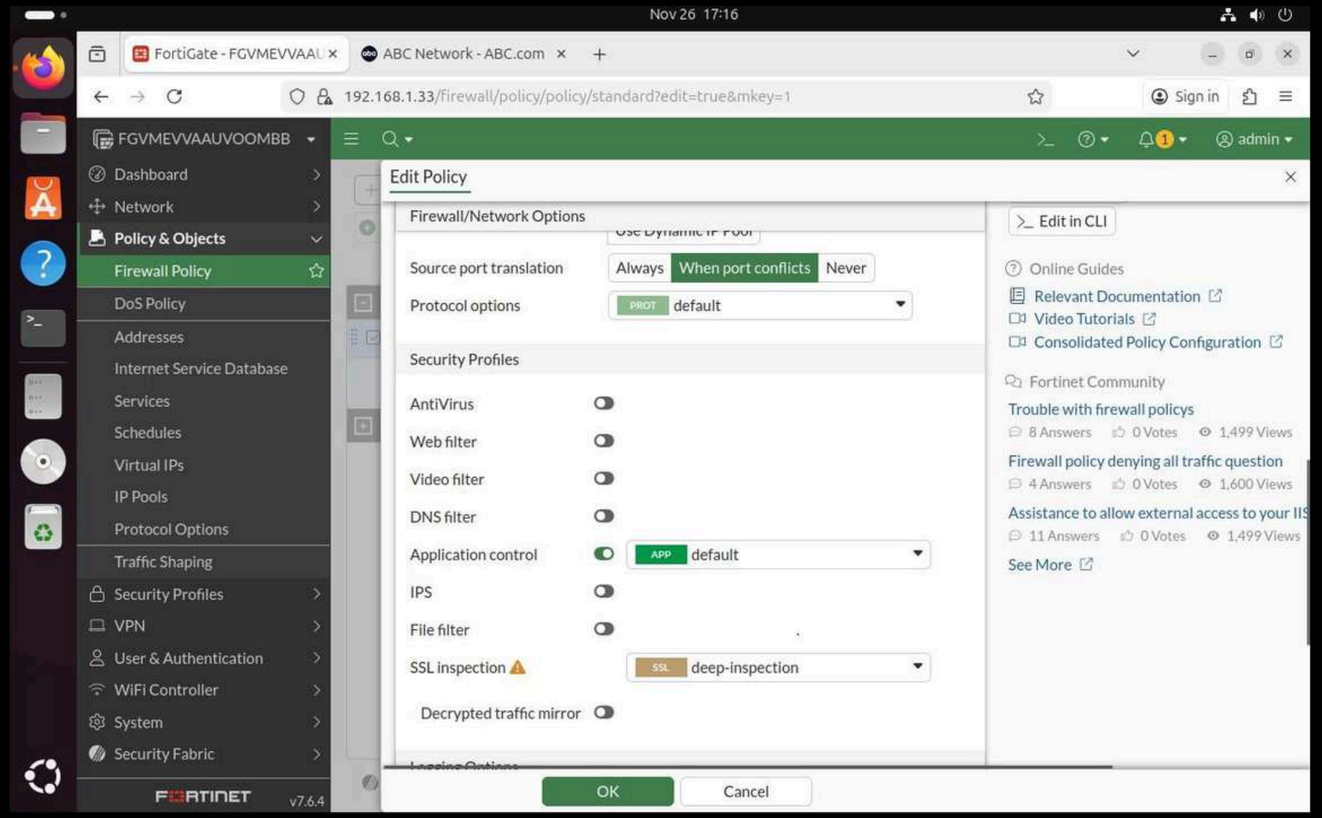


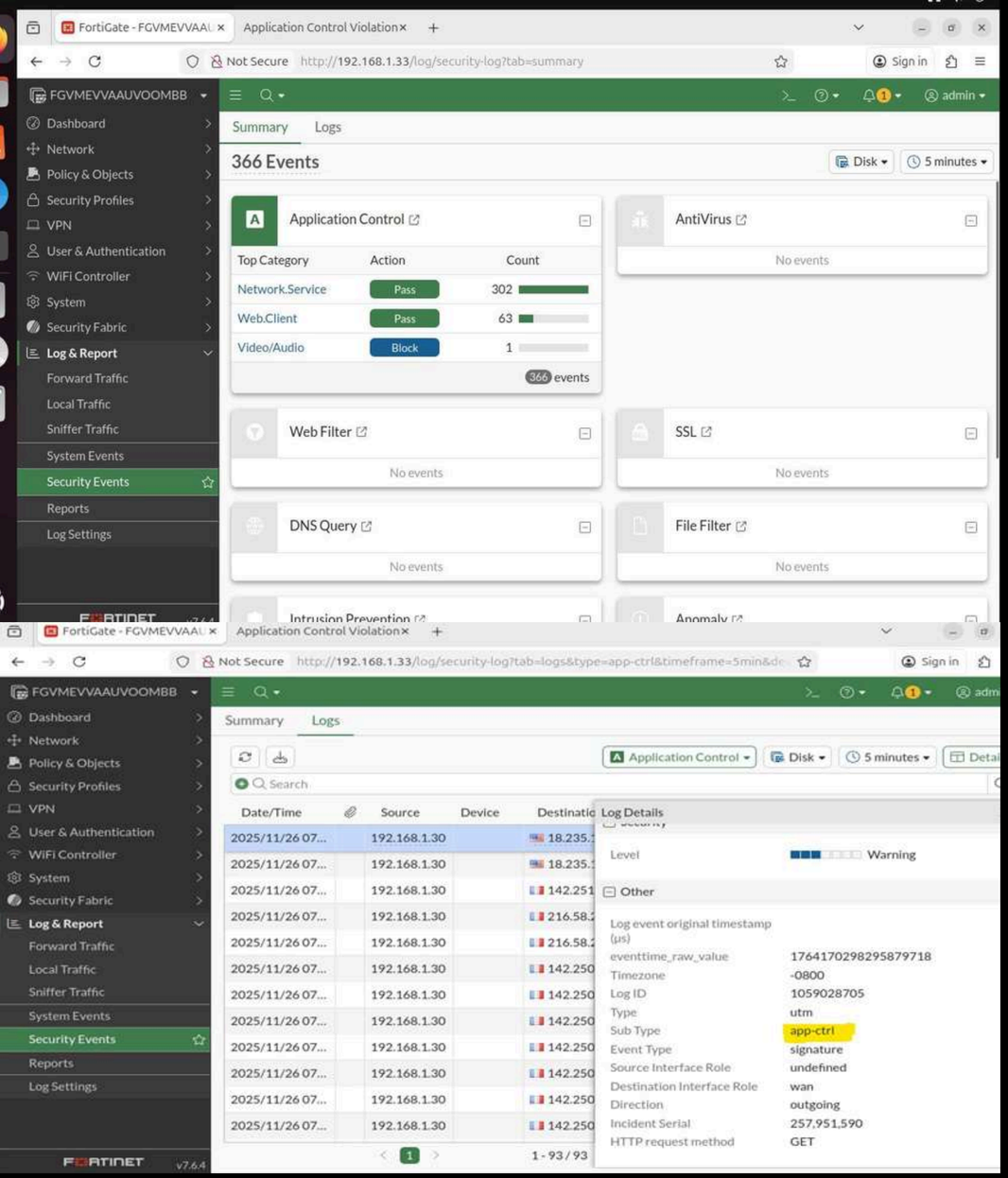

## FORTIVIEW WEB FILTER DASHBOARD

Blocked domains
Attempt counts
Trend charts

# APPLICATION CONROL FIREWALL POLICY FOR MINTORING



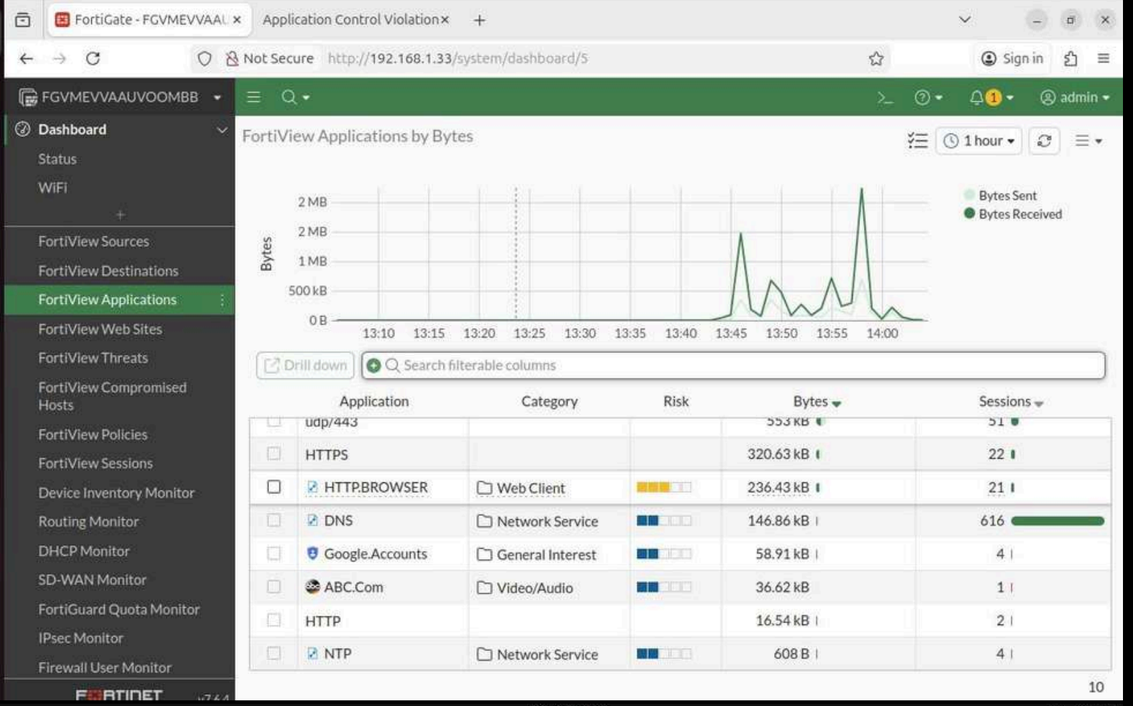
# APPLICATION CONTROL SECURITY EVENTS APPLICATION CONTROL REVEALED:

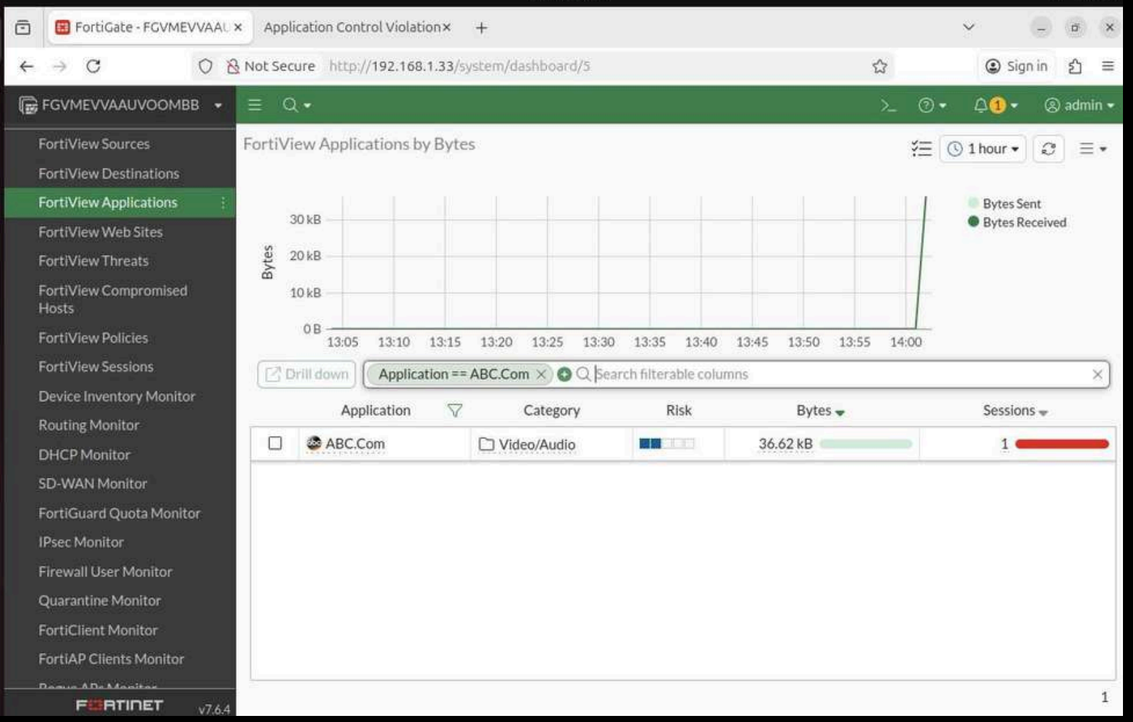



## APPLICATION CONTROL SECURITY EVENTS

ABC.com session blocked
Detected category:

Video/Audio
SSL inspection detected traffic



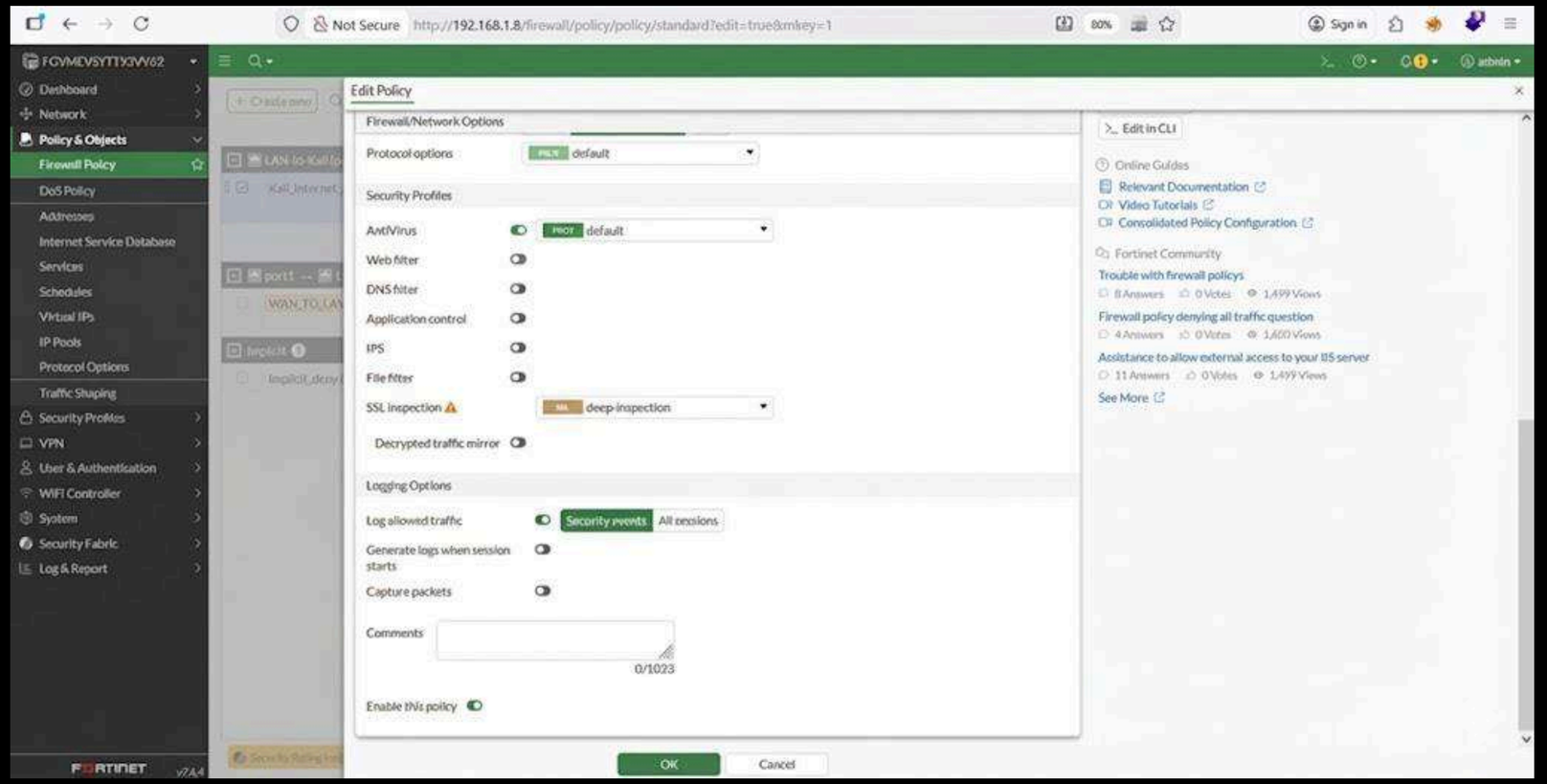




# FORTIVIEW APPLICATION DASHBOARD SHOWS:

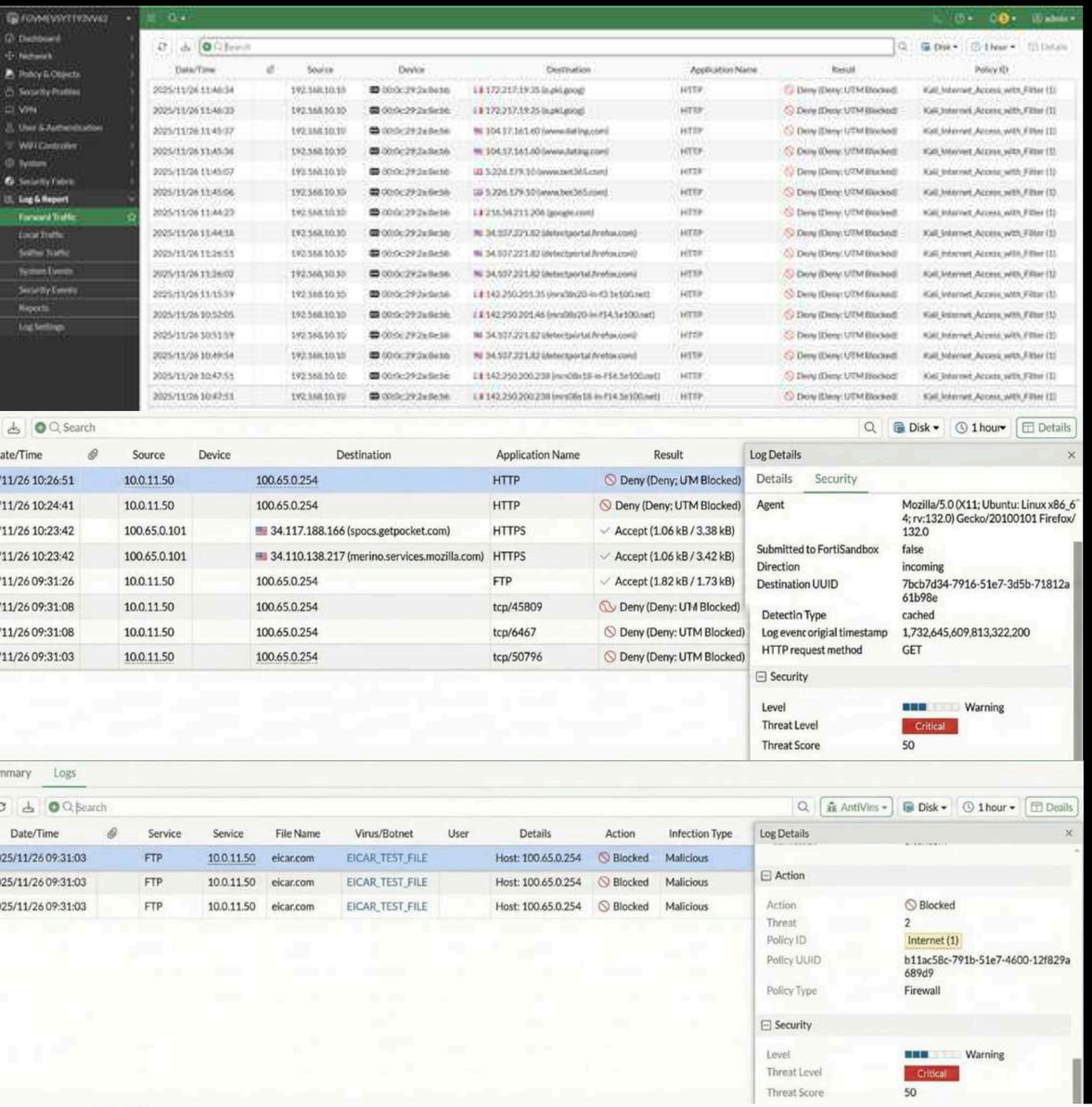
FORTIVIEW APPLICATION DASHBOARD SHOWS:

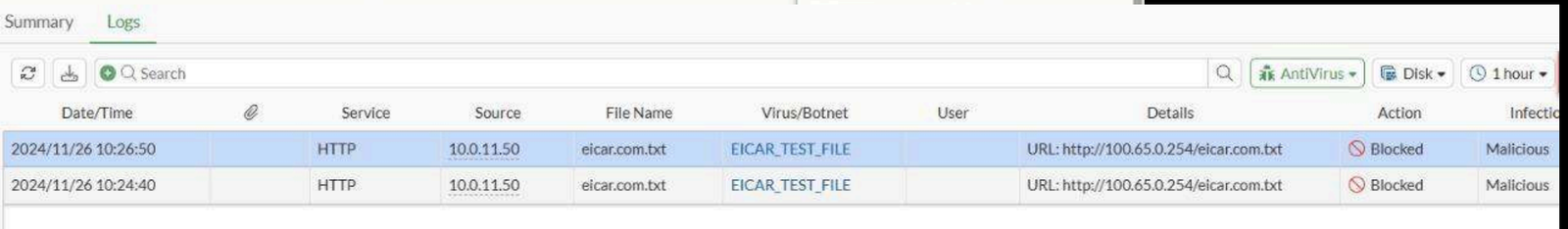
Top consumed apps
Blocked applications
Bandwidth usage

# ANTIVIRUS FIREWALL POLICY FOR MINTORING:



# 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!