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:

1-Web Filter

Objective

- **Goal:** To implement and enforce internet usage policies using FortiGate Web Filtering.
- **Security Purpose:** To protect the internal network from web-based threats, including malicious URLs and phishing sites.
- **Productivity Purpose:** To restrict user access to non-work-related content, specifically blocking Social Media and entertainment categories to minimize distractions.
- **Tool Used:** FortiGate Web Filter Security Profile & Firewall Policies.

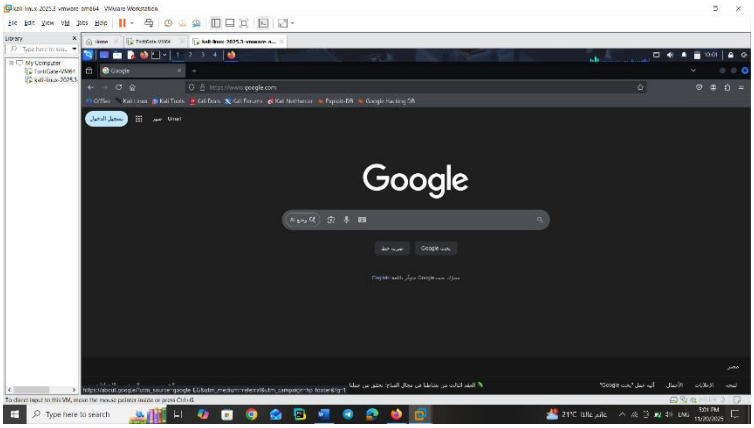
Lab Environment & Network Topology : To simulate a real-world internal network, Kali Linux was deployed as an end-user workstation within VMware Workstation.

- **Connectivity:** The Network Adapter of the Kali VM was mapped to the same custom virtual network (e.g., VMnet 1or LAN Segment) as the FortiGate LAN Interface (Port 2).
- **Routing:** The Kali machine was configured to use the FortiGate's LAN IP address as its Default Gateway, ensuring all internet traffic is inspected by firewall policies.

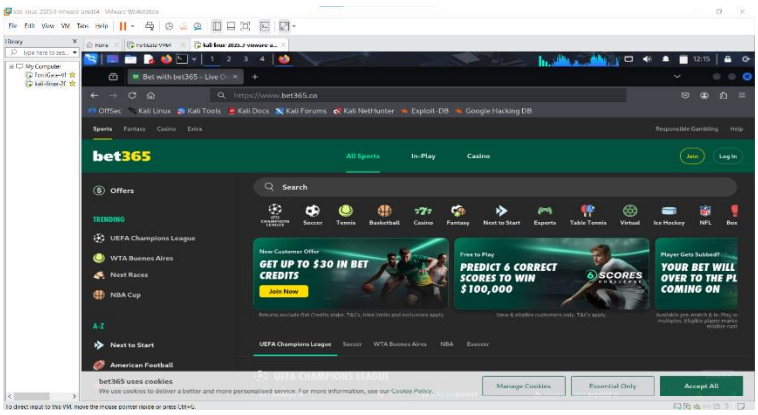
Part 2: Testing & Verification (Before vs. After)

Scenario 1: Before Applying Web Filter Before linking the Web Filter profile to the firewall policy, the user had unrestricted access to the internet.

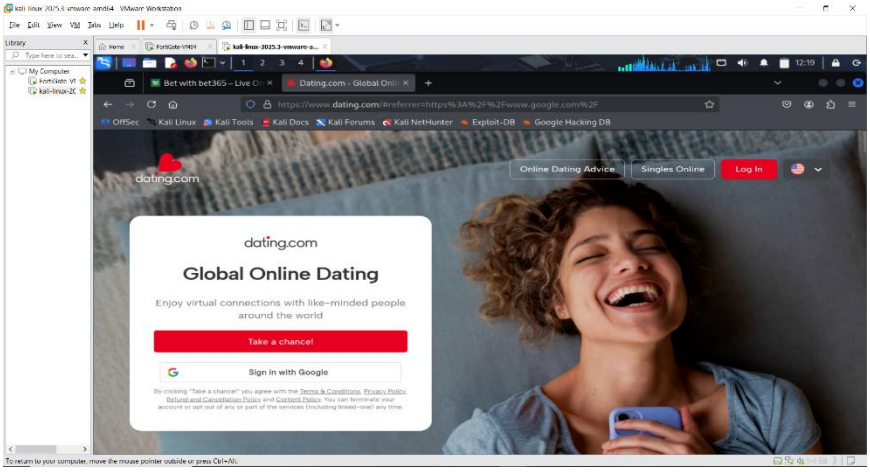
- **Observation:** The user could successfully access Social Media platforms (e.g., Facebook, Twitter).
- **Evidence:**



Successful access to Google from the Kali Linux workstation before applying any FortiGate Web Filter restrictions



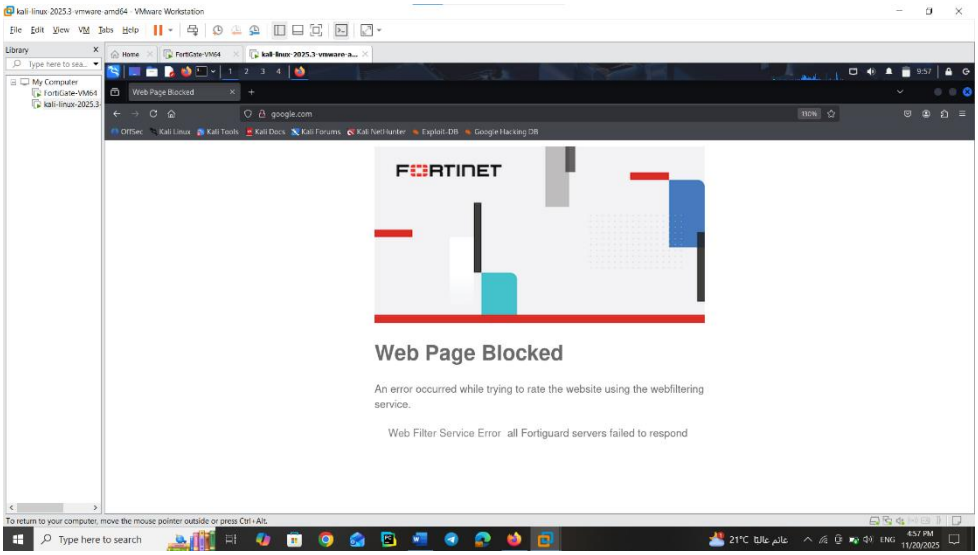
Successful access to a Gambling website (bet365.com), confirming no productivity restrictions were in place prior to filter activation



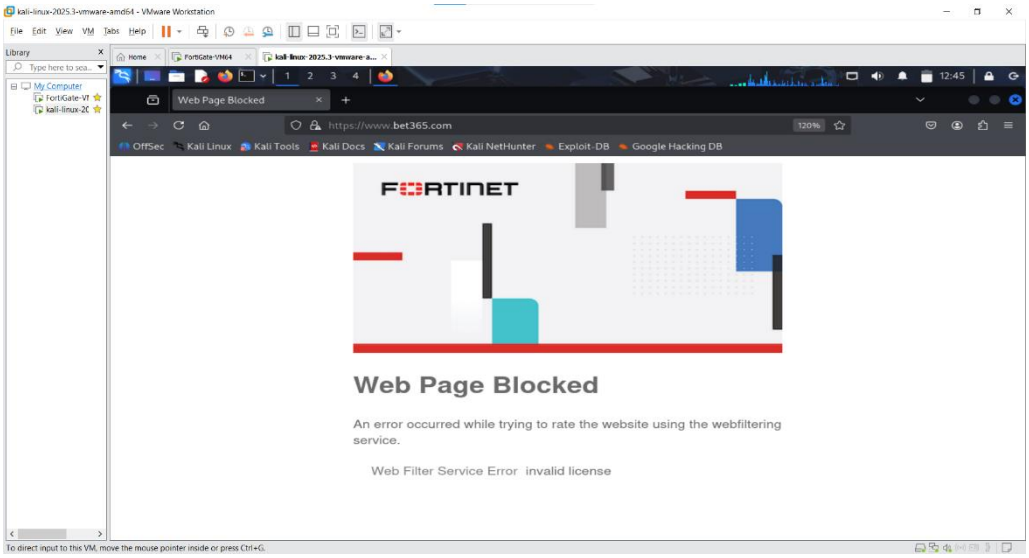
Successful access to a Dating website (dating.com), indicating that traffic was not yet inspected by the FortiGate

Scenario 2: After Applying Web Filter Once the Web Filter profile was applied to the LAN-to-WAN policy, the restrictions took immediate effect.

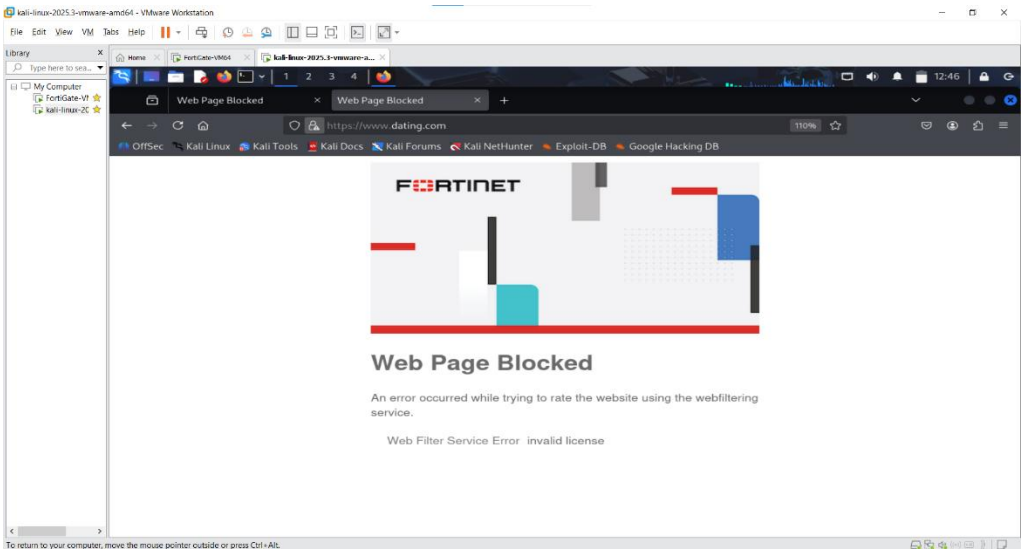
- **Observation:** Access to prohibited categories was blocked, and the user was redirected to the Fortinet replacement message.



The "Web Page Blocked" message displayed on the user's browser, confirming the Web Filter's successful enforcement on user traffic



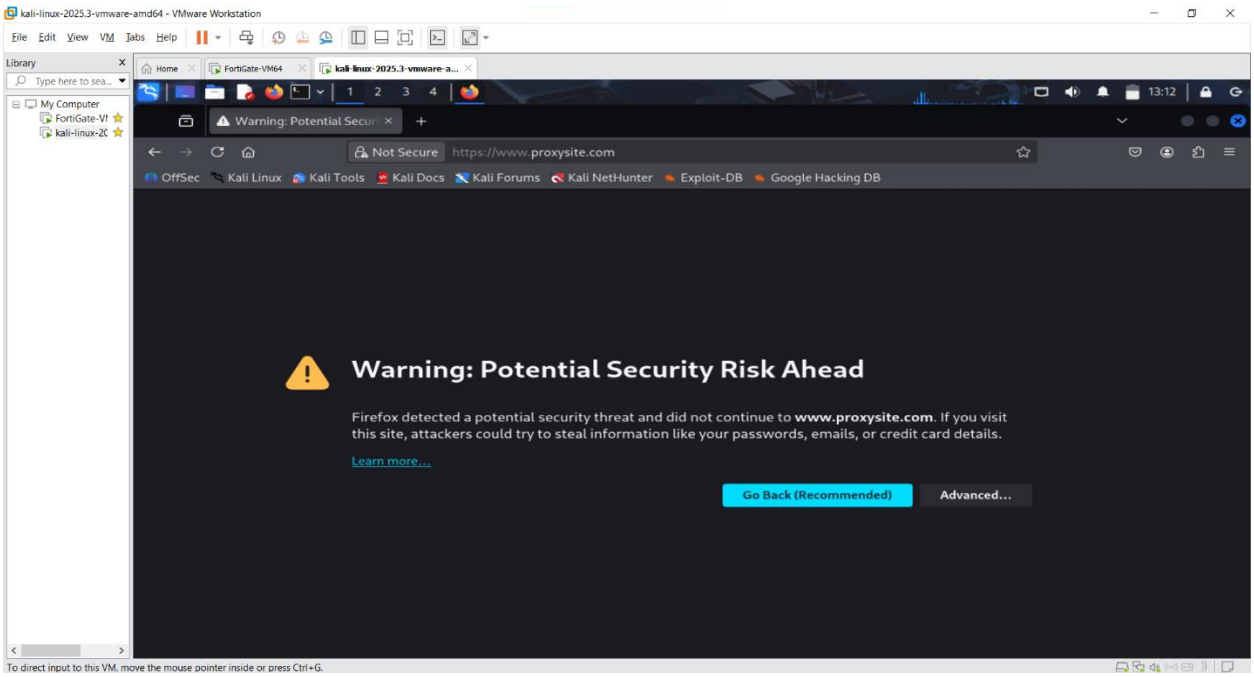
Block page confirming the restriction of the Gambling website (bet365.com) due to the applied Web Filter policy



Block page confirming the restriction of the Dating website (dating.com) as per the new productivity policy.

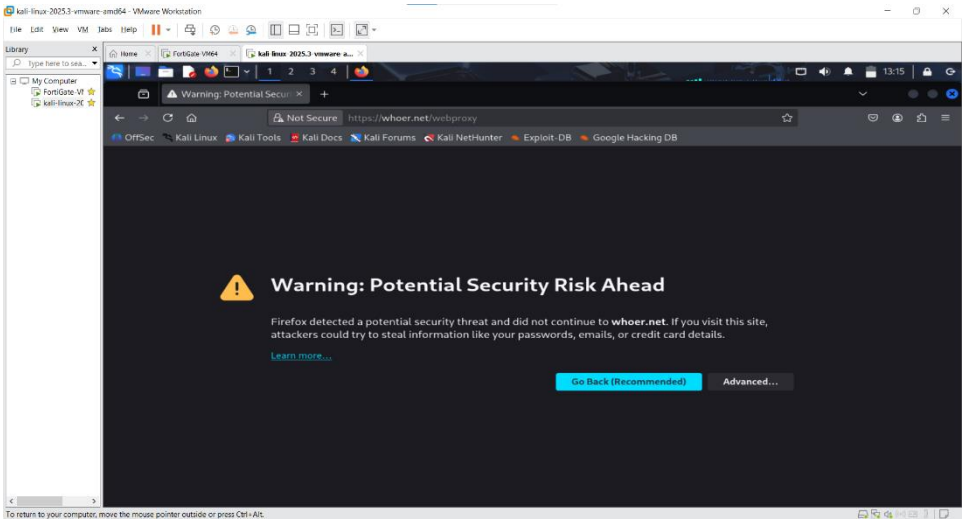
Proxy Avoidance Test:

https://www.proxysite.com



A browser security warning displayed upon attempting to access a proxy avoidance site (proxysite.com), as the "Proxy Avoidance" category was set to Warning in the Web Filter profile

https://whoer.net/webproxy



A similar security warning confirming the policy's effectiveness against another web proxy site (whoer.net/webproxy).

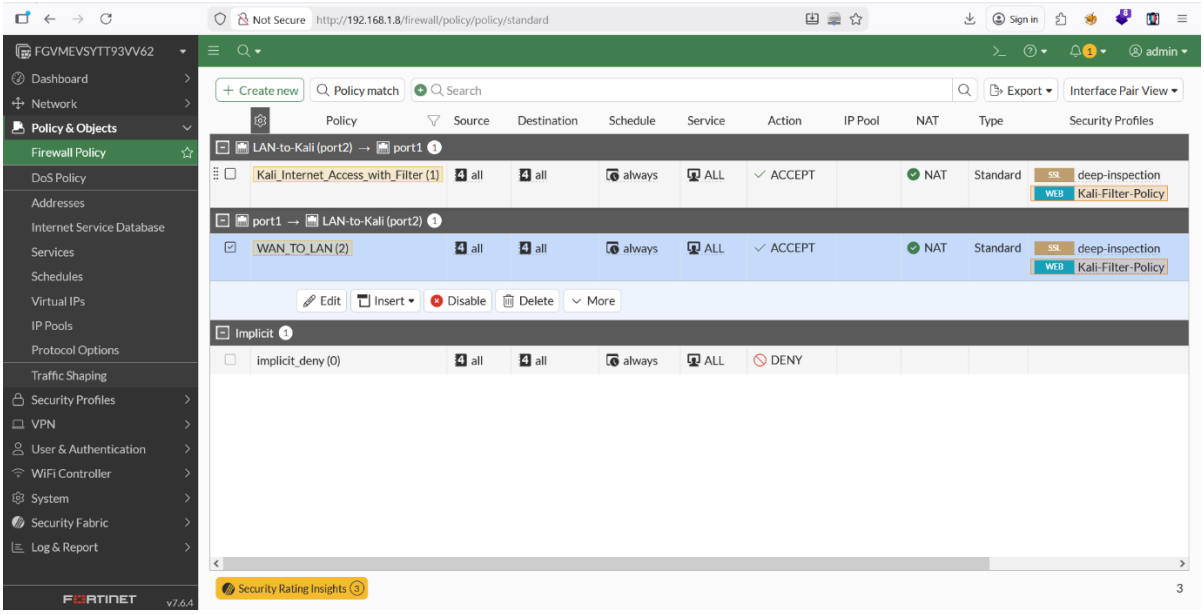
Part 3: Security Profile Enforcement via Firewall Policy

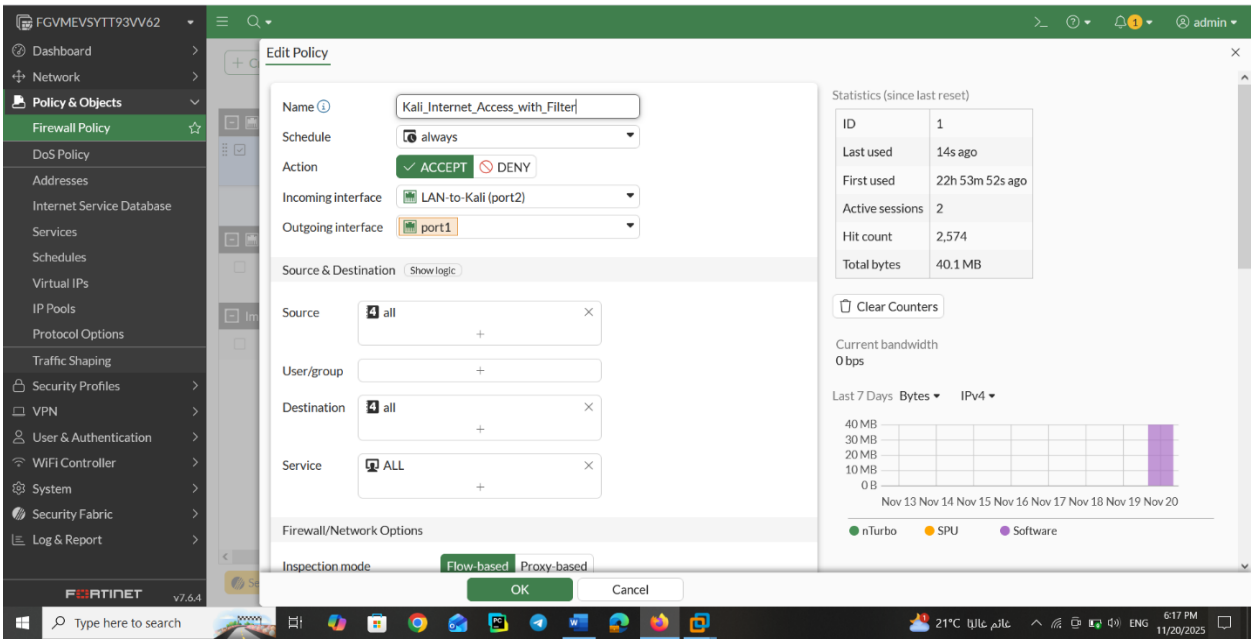
To ensure the Web Filter and other security profiles are enforced on user traffic, the profiles were linked to the primary LAN-to-WAN Firewall Policy**.**

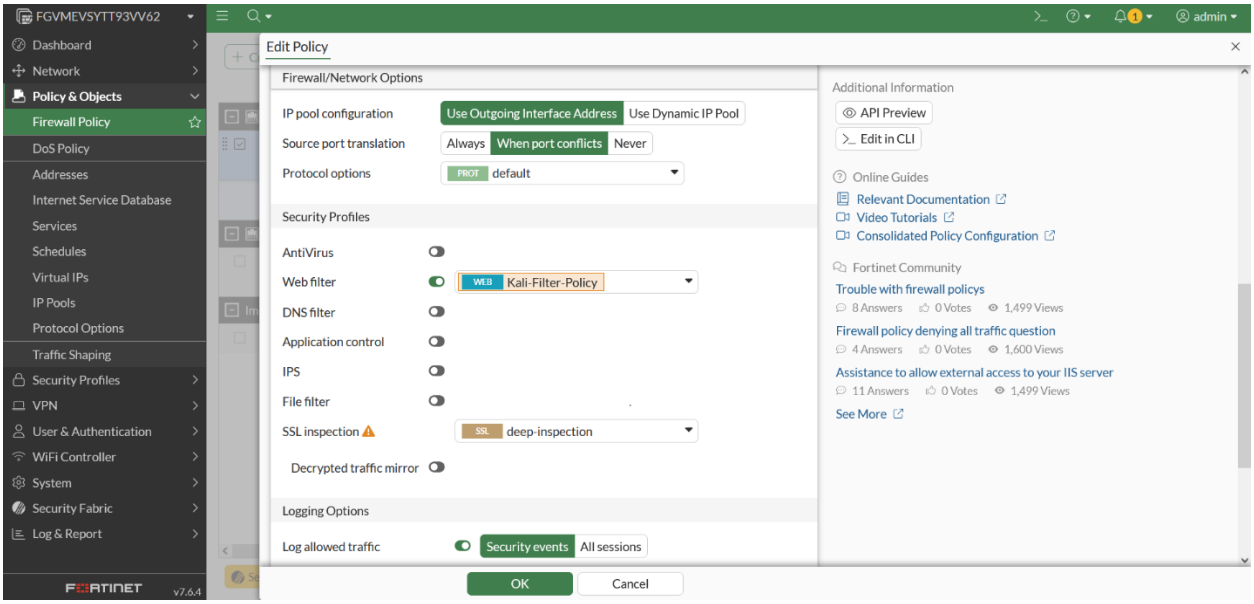
This policy dictates that all outbound traffic originating from the internal network must pass through the defined security checks before accessing the internet.

Firewall Policy:

The Firewall Policy list, highlighting the main outbound policy (Kali_Internet_Access_with_Filter) used to govern traffic from the internal network (Port 2).

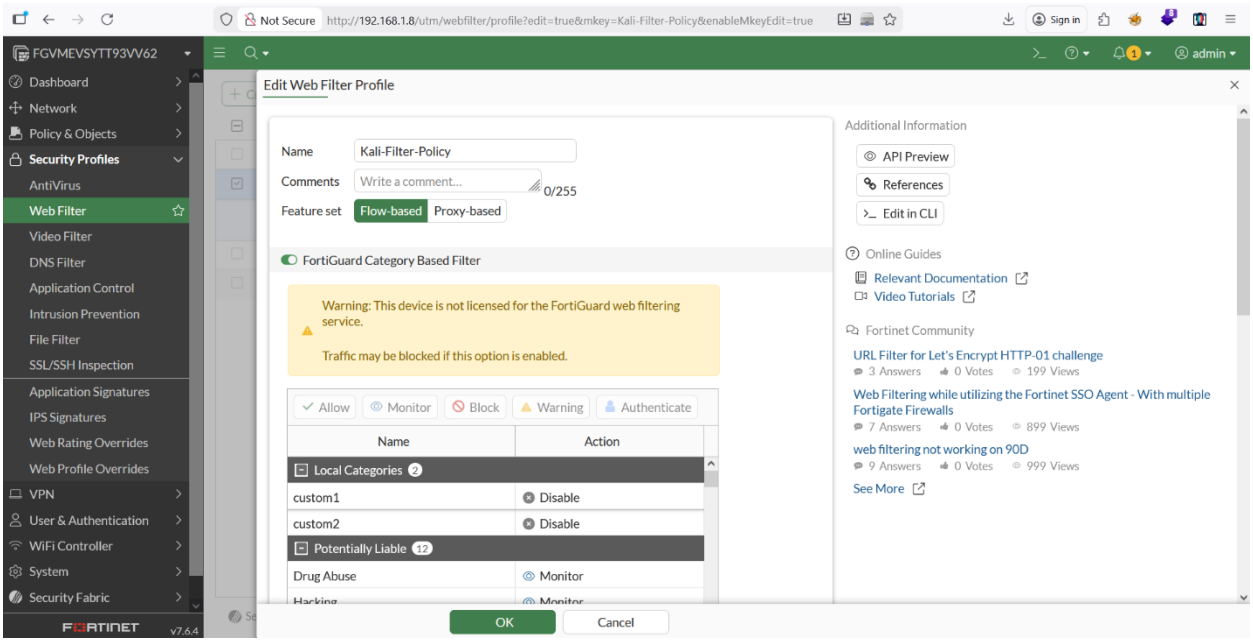


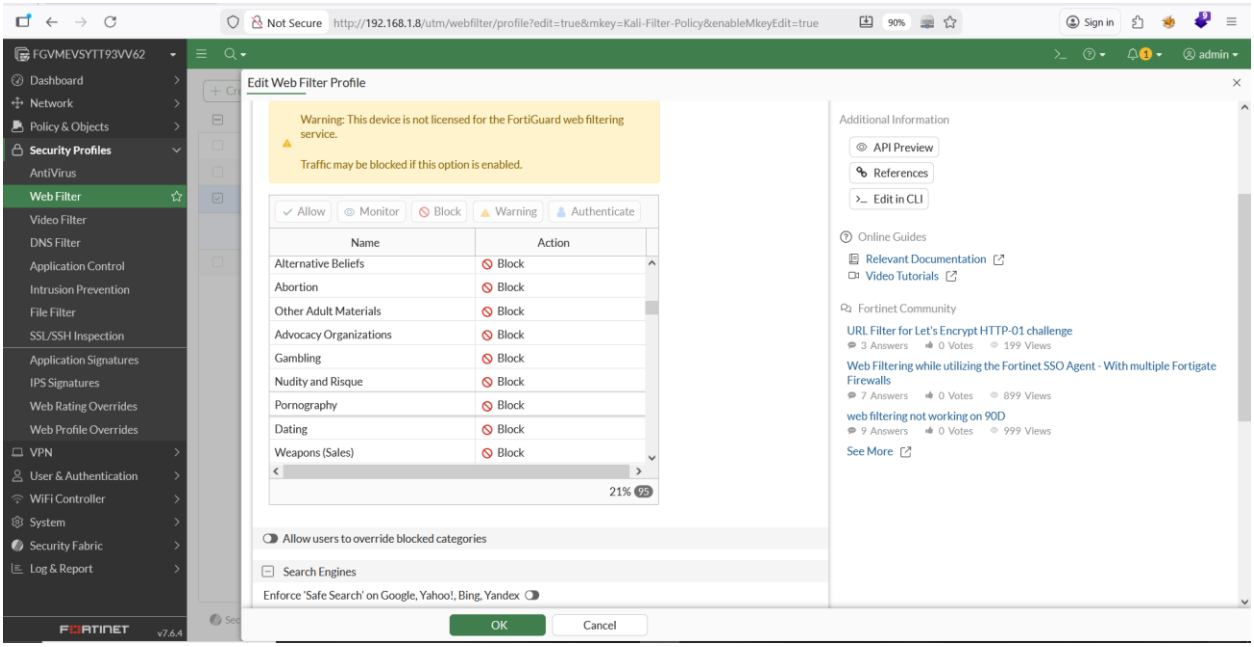




Policy Security Profiles Enforcement Details of the policy confirming the successful linkage and enforcement of the Web Filter profile (Kali-Filter-Policy) and Deep SSL Inspection on all outbound traffic.

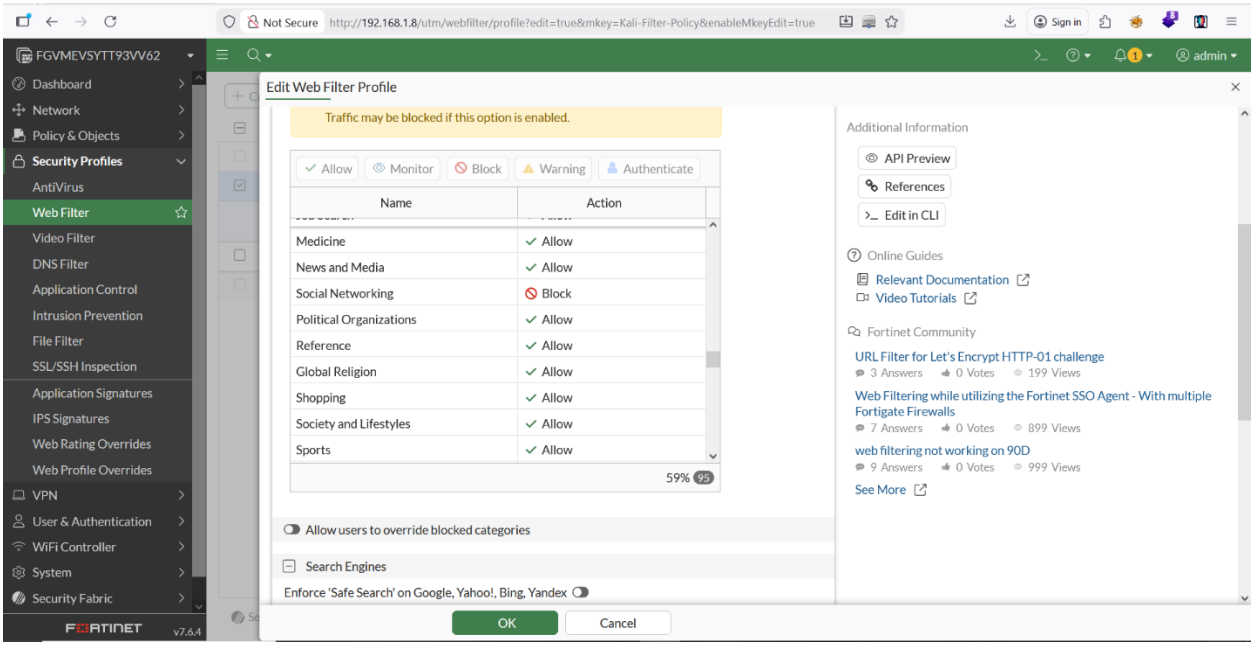
Web Filter Profile Configuration (Kali-Filter-Policy):



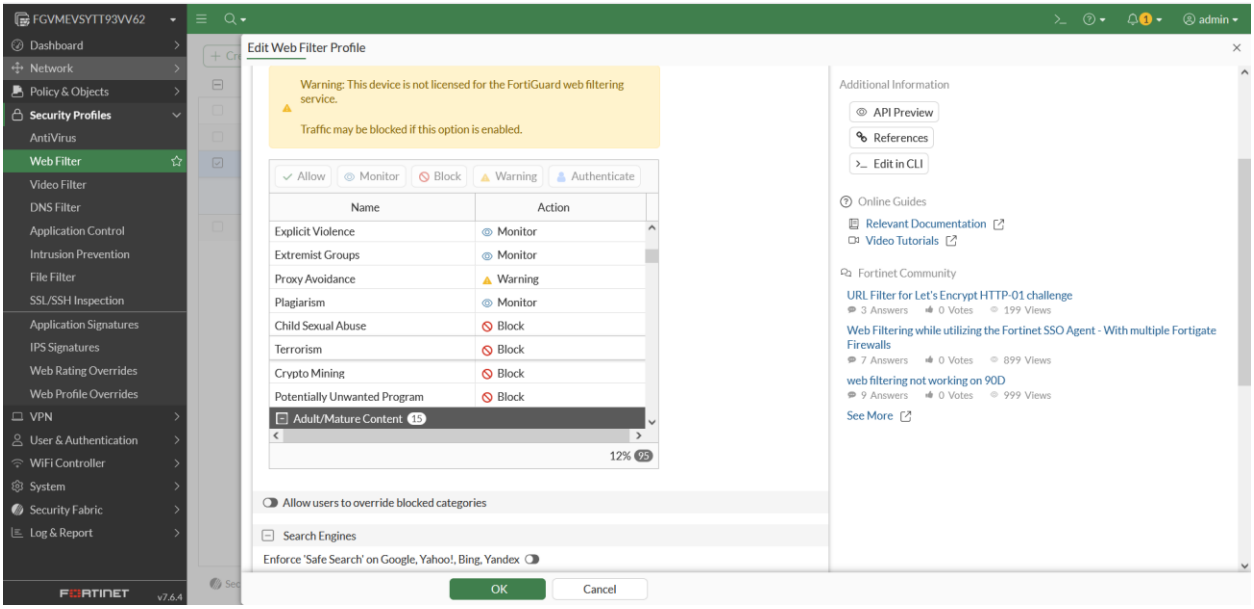


Snippet of the Web Filter profile configuration, showing multiple potentially liable categories (e.g., Gambling, Dating,

Pornography) explicitly set to Block to enforce productivity and acceptable usage policies.



Configuration utilizing FortiGuard Category-Based Filtering, with the Social Networking category explicitly set to Block to enforce the distraction mitigation productivity policy



"Proxy Avoidance" category was set to Warning in the Web Filter profile.

2-Apllication Control:

Objective

- **Goal:** To implement and enforce internet usage policies using FortiGate Application Control.
- **Security Purpose:** To identify, monitor, and regulate (allow, block, or restrict) specific applications and application behaviors traversing the network, regardless of the port or protocol used.
- **Productivity Purpose:** To restrict user access to a non-work-related content application, specifically blocking abc.go.com (ABC.Com).
- **Tool Used:** FortiGate Application Control Security Profile & Firewall Policies.

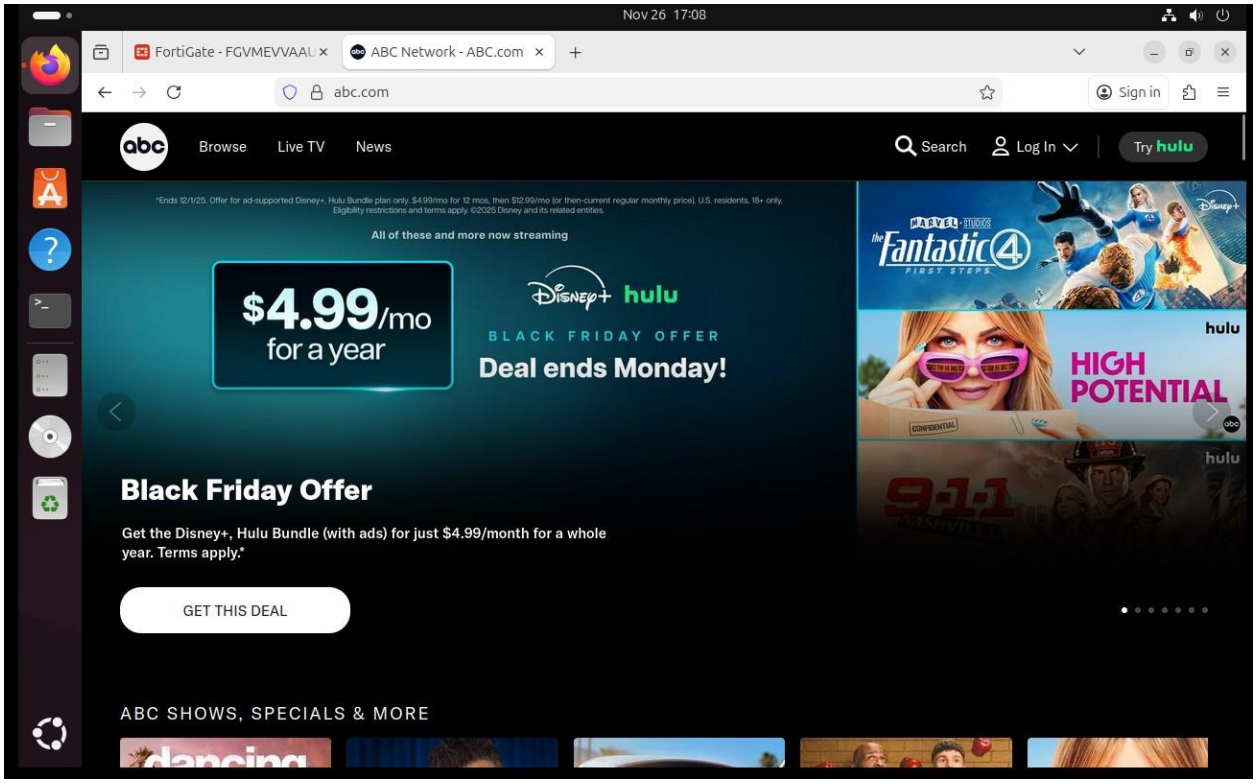
Lab Environment & Network Topology To simulate a real-world internal network, **Kali Linux** was deployed as an end-user workstation within **VMware Workstation**.

- **Connectivity:** The Network Adapter of the Kali VM was mapped to the same custom virtual network (e.g., VMnet2 or LAN Segment) as the **FortiGate LAN Interface (Port 2)**.
- **Routing:** The Kali machine was configured to use the FortiGate's LAN IP address as its **Default Gateway**, ensuring all internet traffic is inspected by the firewall policies.

Part 2: Testing & Verification (Before vs. After)

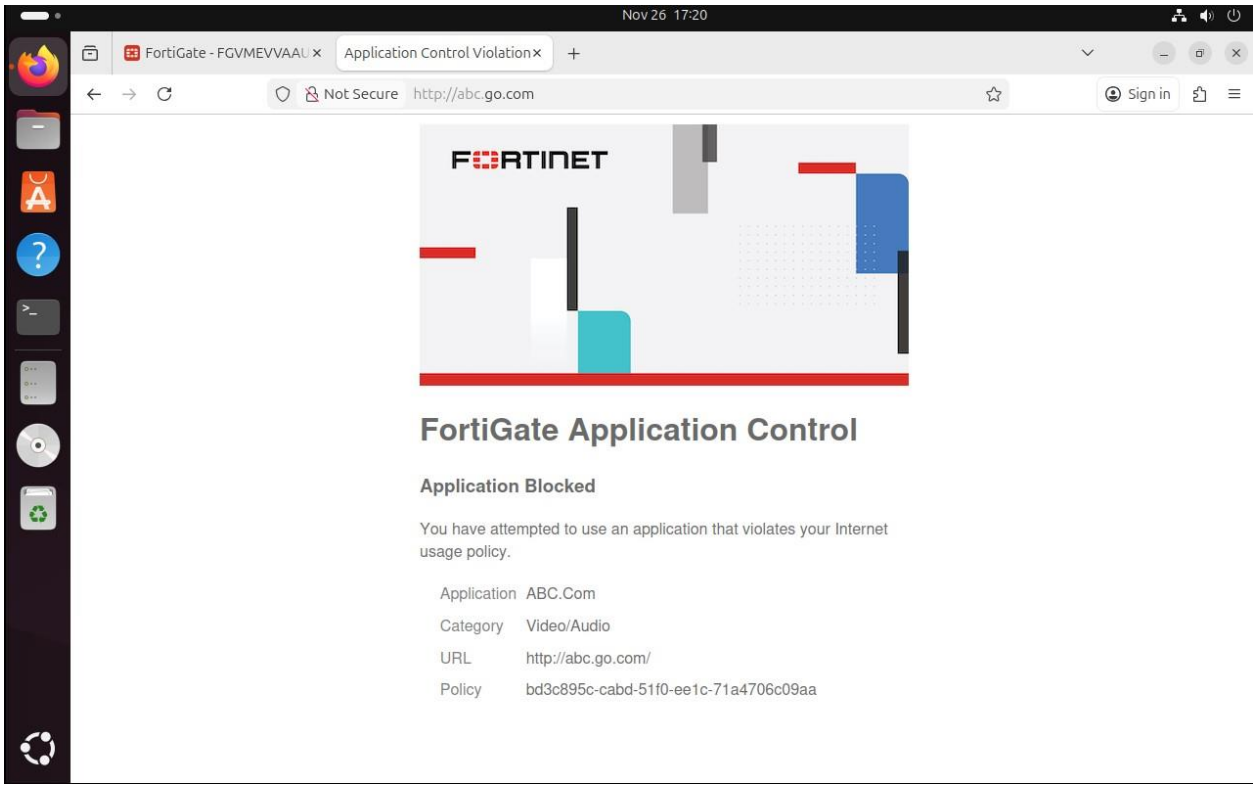
Scenario 1: Before Application Control Before linking the Application Control profile to the firewall policy, the user had unrestricted access to the internet.

- **Observation:** The user could successfully access platforms (e.g., ABC)
- **Evidence:**



Scenario 2: After Applying Application Control Once the Application Control profile was applied to the **LAN-to-WAN** policy, the restrictions took immediate effect.

- **Observation:** Access to prohibited categories was blocked, and the user was redirected to the Fortinet replacement message.



Access denied message displayed on the user's browser after applying the Application Control.

Web Filter Policy Enforcement and SSL Interception

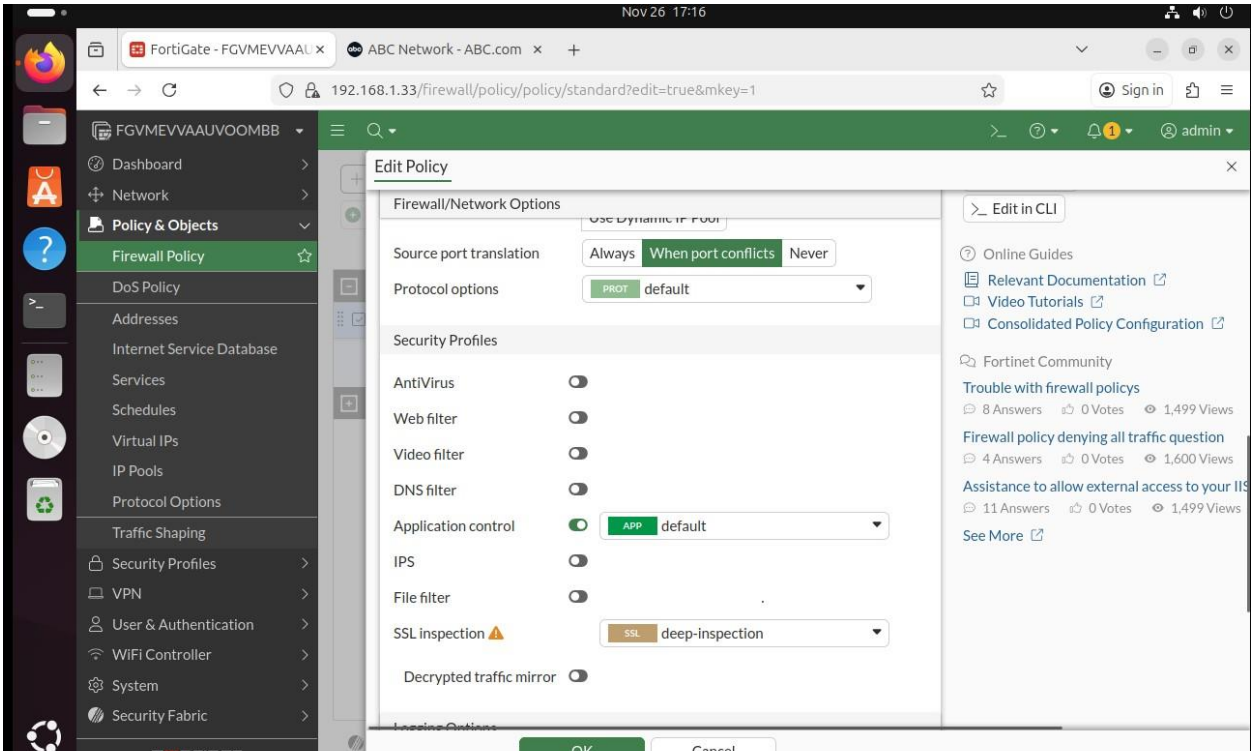
Description: Attempted access to the restricted application (ABC.Com) confirms that the Application Control policy is successfully enforced. The FortiGate firewall, utilizing SSL Deep Inspection, is able to decrypt the traffic and identify the application signature for blocking. The client browser rejects the connection or displays a security warning/error due to the FortiGate's CA certificate not being trusted by the client, which is necessary for Deep Inspection to function seamlessly with HTTPS applications. This outcome validates the effectiveness of the application blocking mechanism.

Part 3:

Application of Security Profiles via Firewall Policy

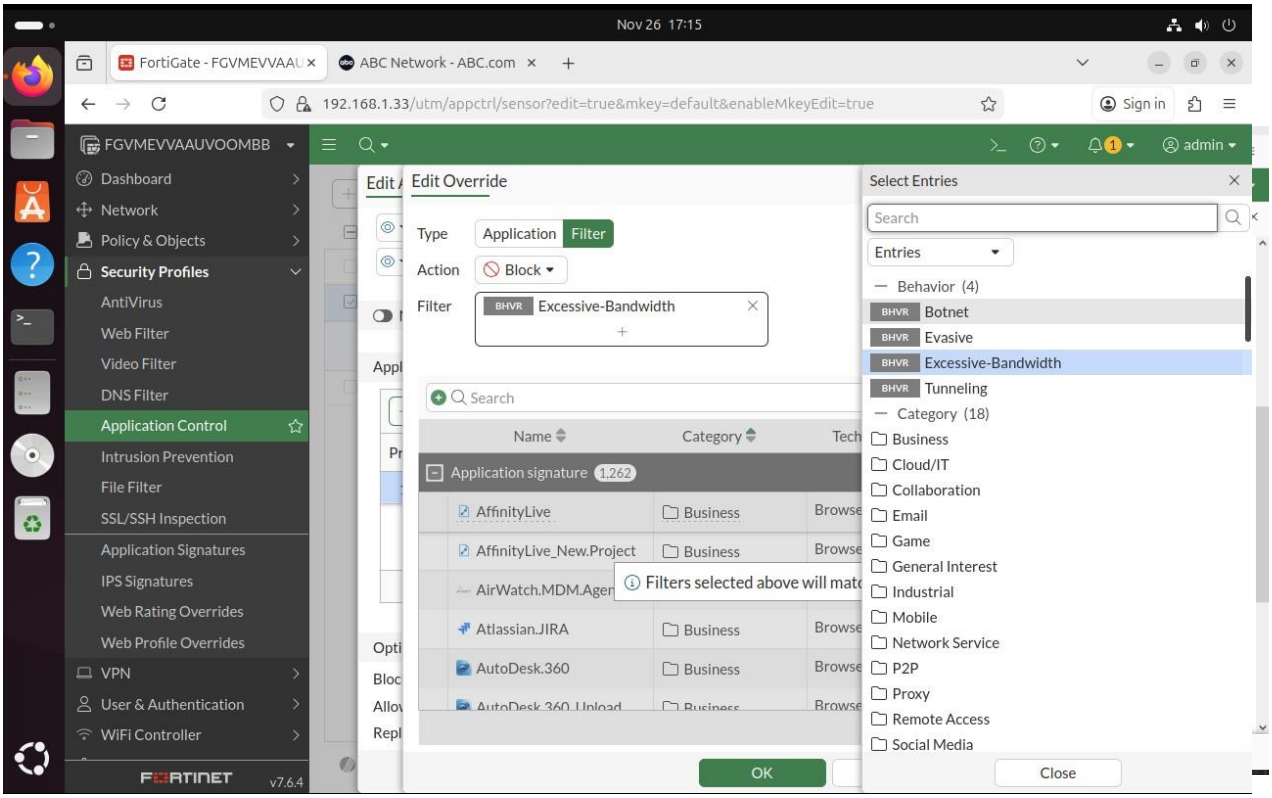
To ensure the Application Control profile and other security profiles are enforced on user traffic , the profiles were linked to the primary LAN-to-WAN Firewall Policy. This policy dictates that all outbound traffic originating from the internal network must pass through the defined security checks, including Application Control, before accessing the internet.

Firewall Policy:

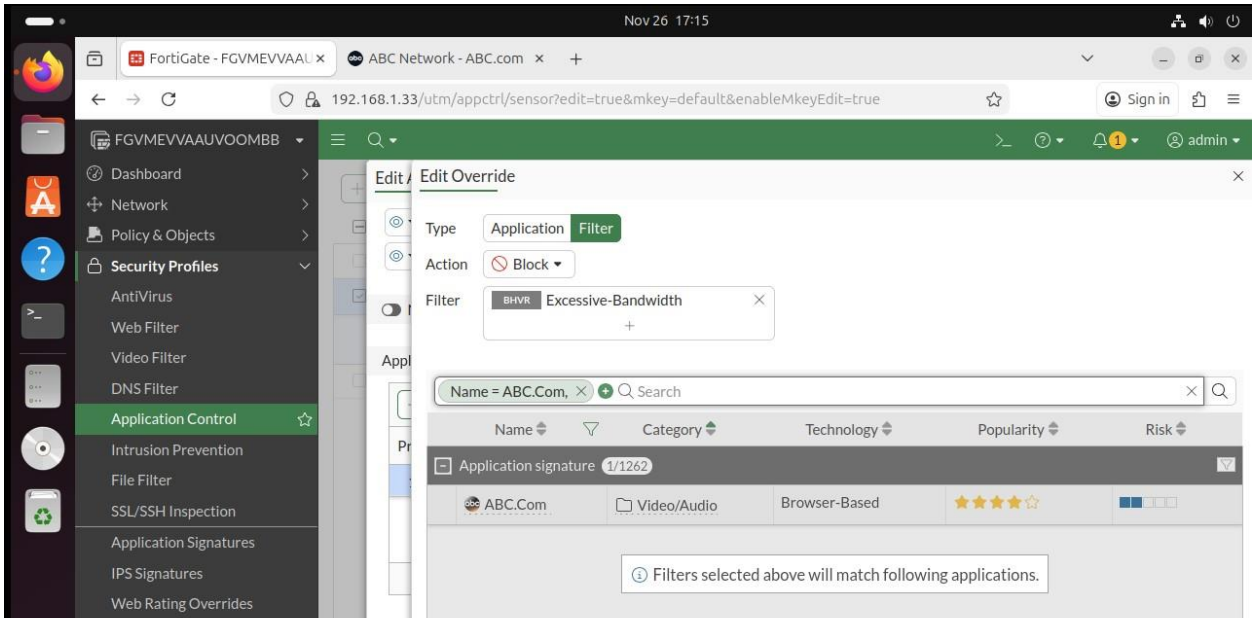


Policy Security Profiles Enforcement Details of the policy confirming the successful linkage and enforcement of the **Web Filter** profile (Kali-Filter-Policy) and **Deep SSL Inspection** on all outbound traffic.

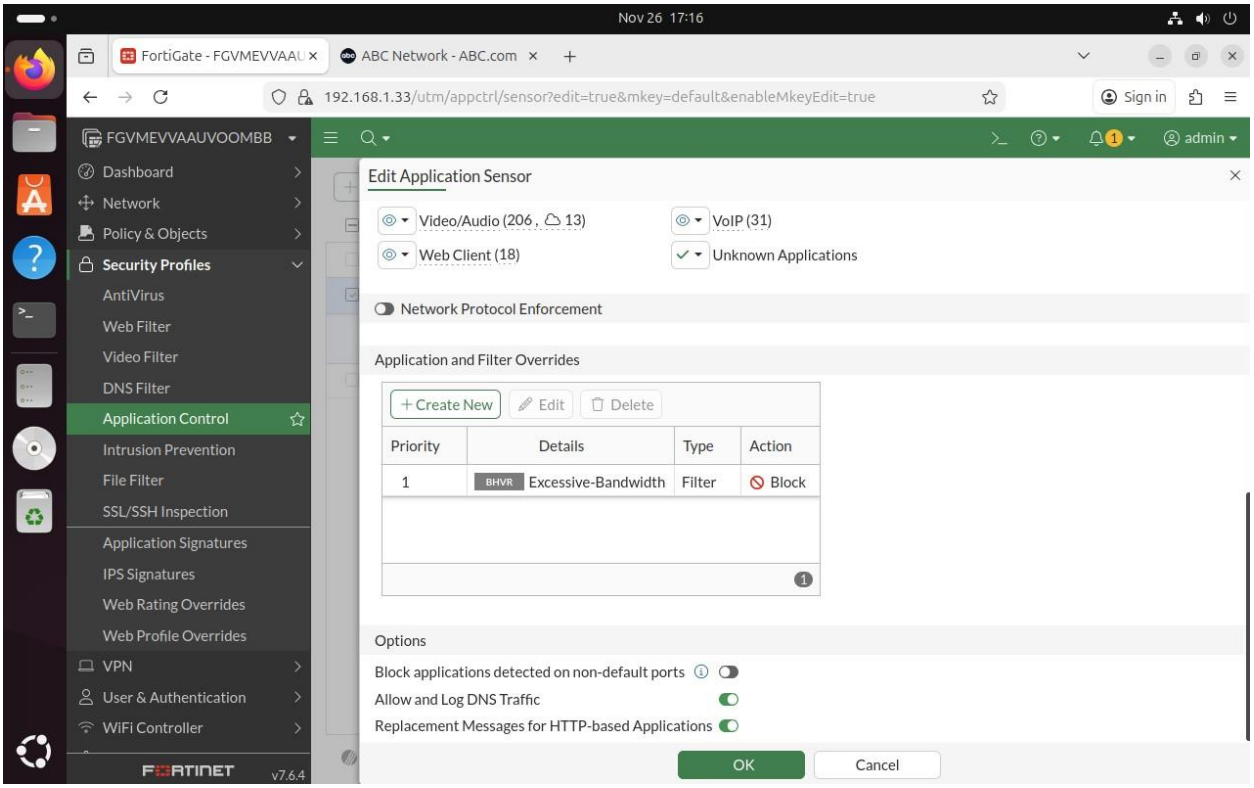
Application Control Profile:



Application Control settings on a FortiGate device. The action is set to 'Block' and the behavior filter 'Excessive-Bandwidth' is applied. This configuration is used to mitigate high bandwidth consumption caused by certain applications or activities on the network.".



Application Control policy, where the application 'ABC.Com' has been explicitly selected to be blocked. Classified under the 'Video/Audio' category, this action is taken to enforce productivity policies and mitigate high bandwidth consumption often caused by video and audio streaming content.



Final summary view of the Application Sensor configuration. It clearly shows the defined Application and Filter Override with Priority 1 set to 'Block' the Excessive-

Bandwidth behavior filter. This confirms the policy's primary function is to aggressively control and mitigate high bandwidth consumption across the network

3-Anti Virus:

Part 1: Objectives & Environment

Task Objective

- **Goal:** To implement and enforce malware protection using **FortiGate Antivirus Security Profile**.
- **Security Purpose:** To protect the internal network from malicious files, viruses, Trojans, and ransomware transmitted via HTTP, SMTP, POP3, IMAP, and FTP protocols.
- **Productivity Purpose:** To ensure business continuity by preventing system infections that could lead to data loss or downtime.
- **Tool Used:** FortiGate Antivirus Profile & Firewall Policies.

Lab Environment & Network Topology

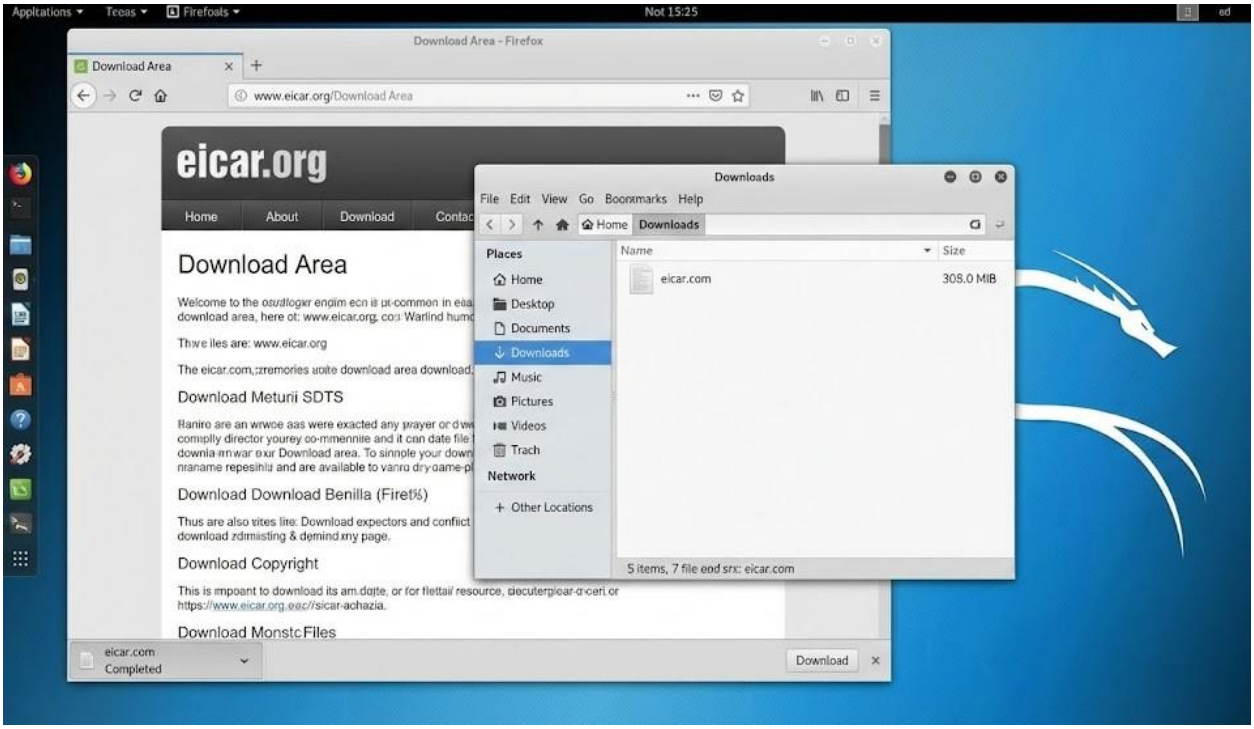
- **Simulation:** Similar to the Web Filter lab, **Kali Linux** is used as the end-user workstation.
- **Connectivity:** The workstation is routed through the FortiGate LAN Interface (Port 2).
- **Routing:** All traffic passes through the FortiGate firewall for inspection.

Part 2: Testing & Verification (Before vs. After)

Test Vector used: EICAR Standard Anti-Virus Test File (A harmless file used industry-wide to test antivirus response).

Scenario 1: Before Applying Antivirus Profile Before linking the Antivirus profile to the firewall policy, the user attempts to download a malicious test file.

- **Observation:** The user could successfully download the eicar.com test file from www.eicar.org.
- **Evidence:**

- 

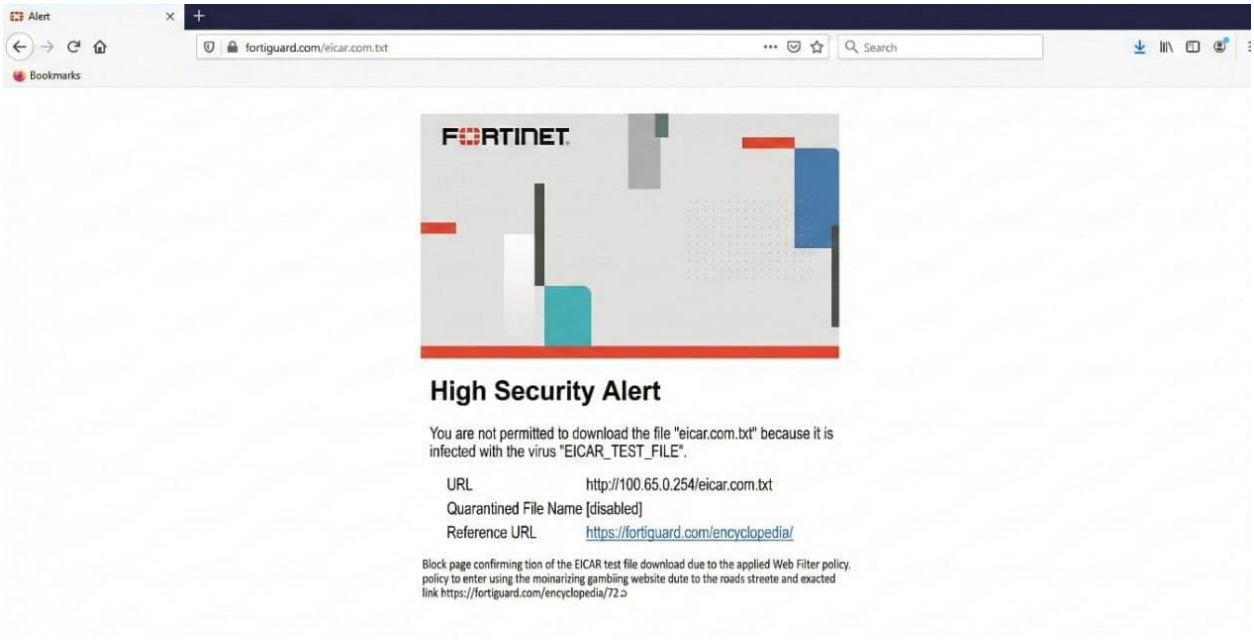
  -

Description: Successful download of the test virus file, indicating no malware inspection

Scenario 2: After Applying Antivirus Profile Once the Antivirus profile (default) was applied to the **LAN-to-WAN** policy, the restrictions took immediate effect.

- **Observation:** Access to the malicious file was blocked, and the download was terminated by the FortiGate.

- **Evidence:**



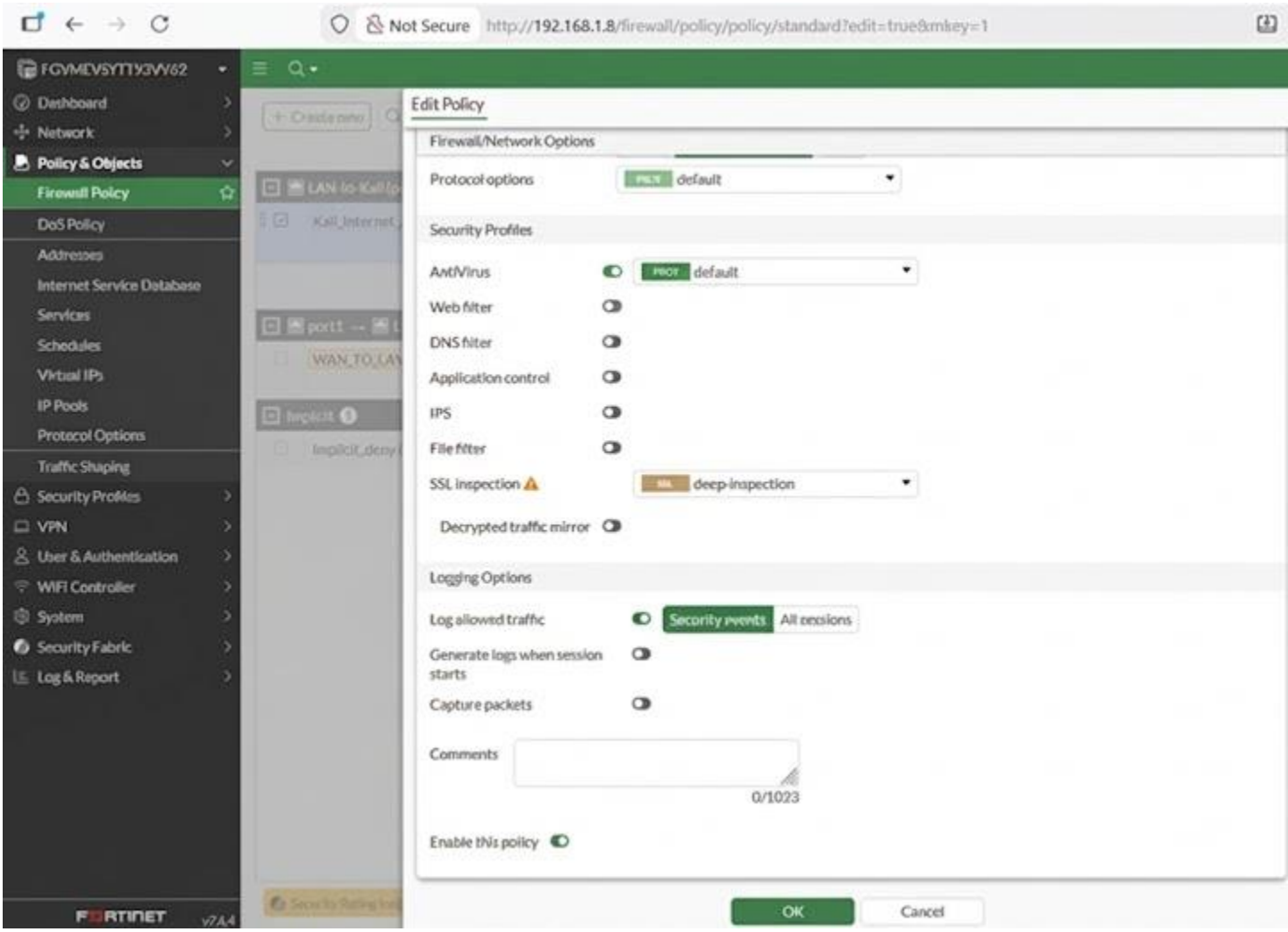
-
    - *Description:* The "Virus/Malware Detected" message displayed on the user's browser, confirming the Antivirus profile successfully intercepted the threat.

      Part 3: Security Profile Enforcement via Firewall Policy

      Policy Configuration To ensure the Antivirus engine inspects traffic, the profile was linked to the primary **LAN-to-WAN Firewall Policy**.

- **Firewall Policy:**
    - The policy Kali_Internet_Access_with_Filter (or your specific policy name) was edited.
    - **Action:** ACCEPT.
    - **Inspection Mode:** Flow-based (standard for high performance) or Proxy-based.

Enforcement Evidence

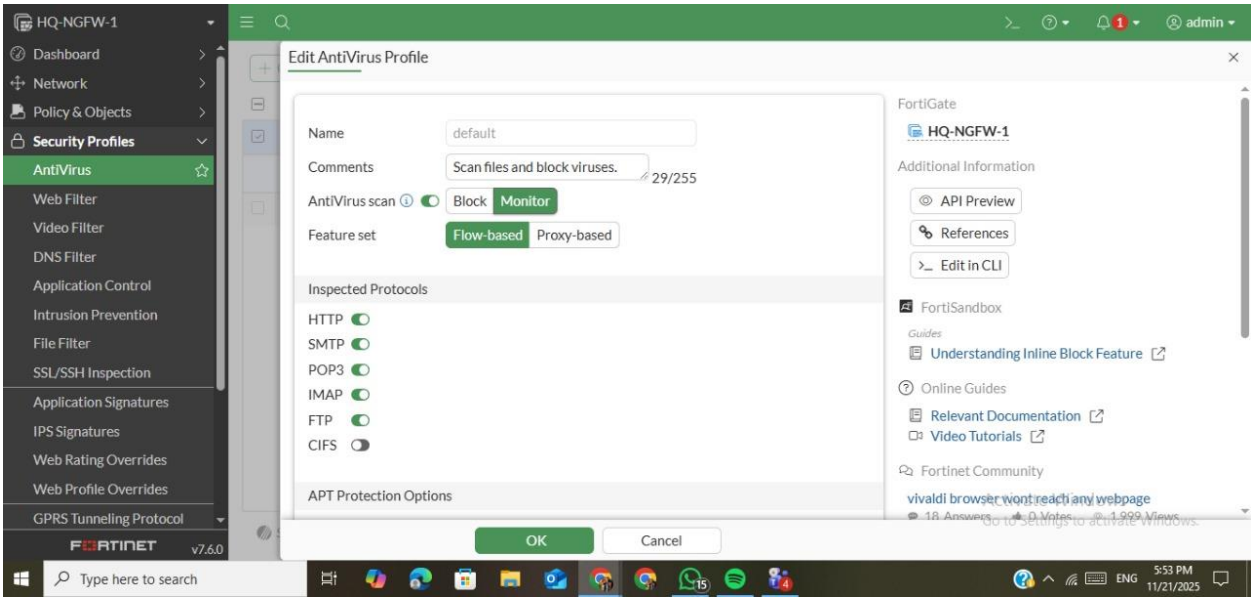


Antivirus: Toggled **ON** (Profile: default).

- **SSL Inspection:** deep-inspection (Recommended to detect viruses inside encrypted HTTPS traffic).

Antivirus Profile Configuration (Default):

- **Inspected Protocols:** HTTP, SMTP, POP3, IMAP, FTP.
- **Virus Outbreak Prevention:** Enabled.
- **Content Disarm and Reconstruction (CDR):** Optional (can be enabled to strip malicious macros from documents).

- 

Conclusion:

The configuration and implementation of the Antivirus, Web Filtering, and Application Control profiles on the FortiGate firewall significantly enhance the security posture of the network. By enabling these essential security layers, the system gains robust protection against malware infections, unsafe web access, and unauthorized or high-risk applications. Applying these profiles to the appropriate firewall policies ensures that all incoming and outgoing traffic is inspected thoroughly, reducing exposure to modern cyber threats.