WEEK 2

FORTIGATE SECURITY PROFILES

PROJECT 4: ADVANCED FORTIGATE SECURITY PROFILES

BY: NADA NASR
EMAN MOAMEN
SEIF WAEL
AHMED OSAMA
SHAHD OSAMA

Security Profiles Deployed:

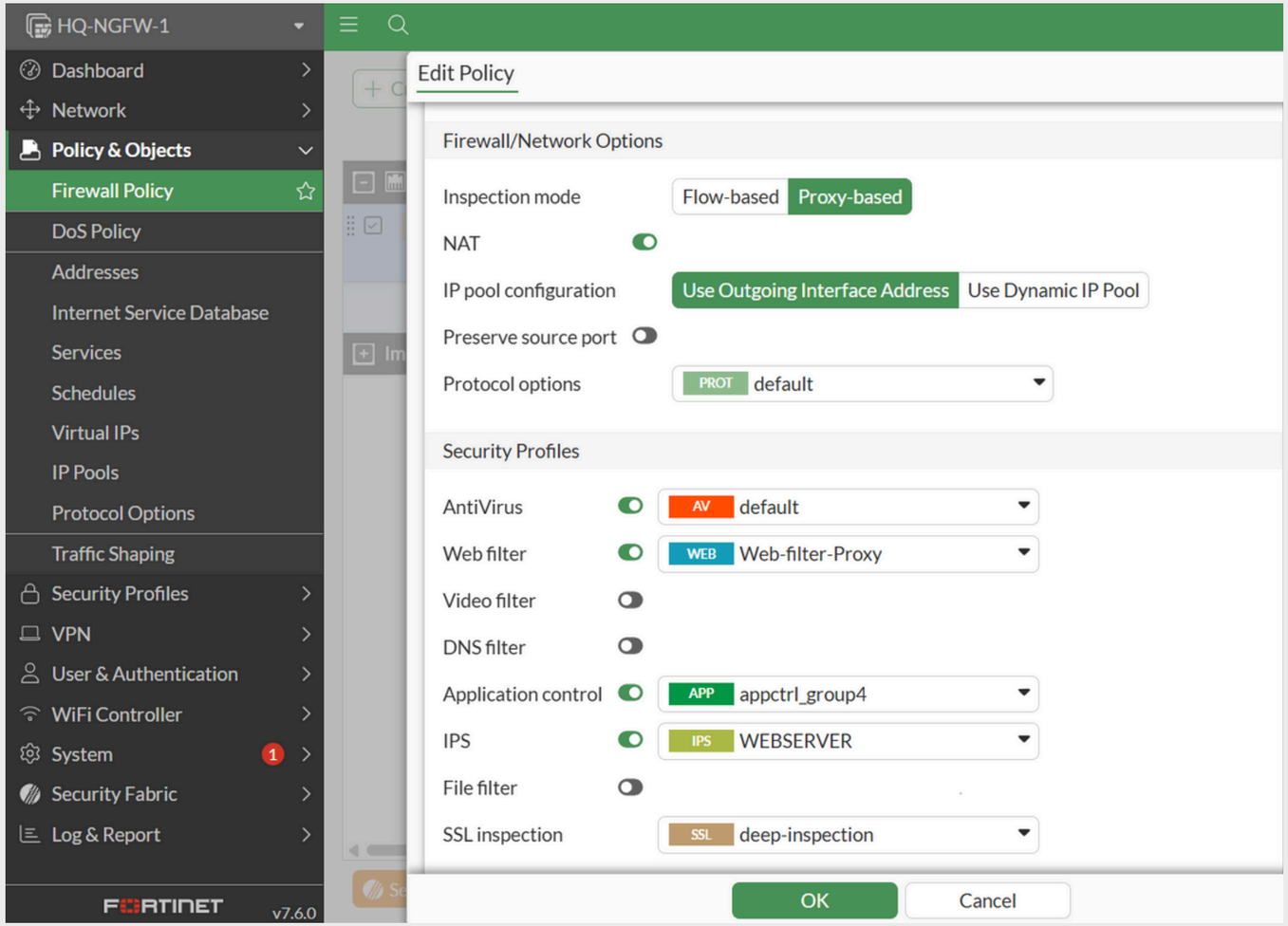
✓ AntiVirus
- Flow-based inspection
- Malware protection

✓ Web Filter
- URL & Category blocking
- Quota management

✓ Application Control
- App identification & control
- Risk-based policies

✓ IPS (Intrusion Prevention)
- Signature-based detection
- Network attack prevention

FIREWALL POLICY INTEGRATION:
• All profiles applied to Internet policy
• Flow-based inspection mode
• Active session monitoring



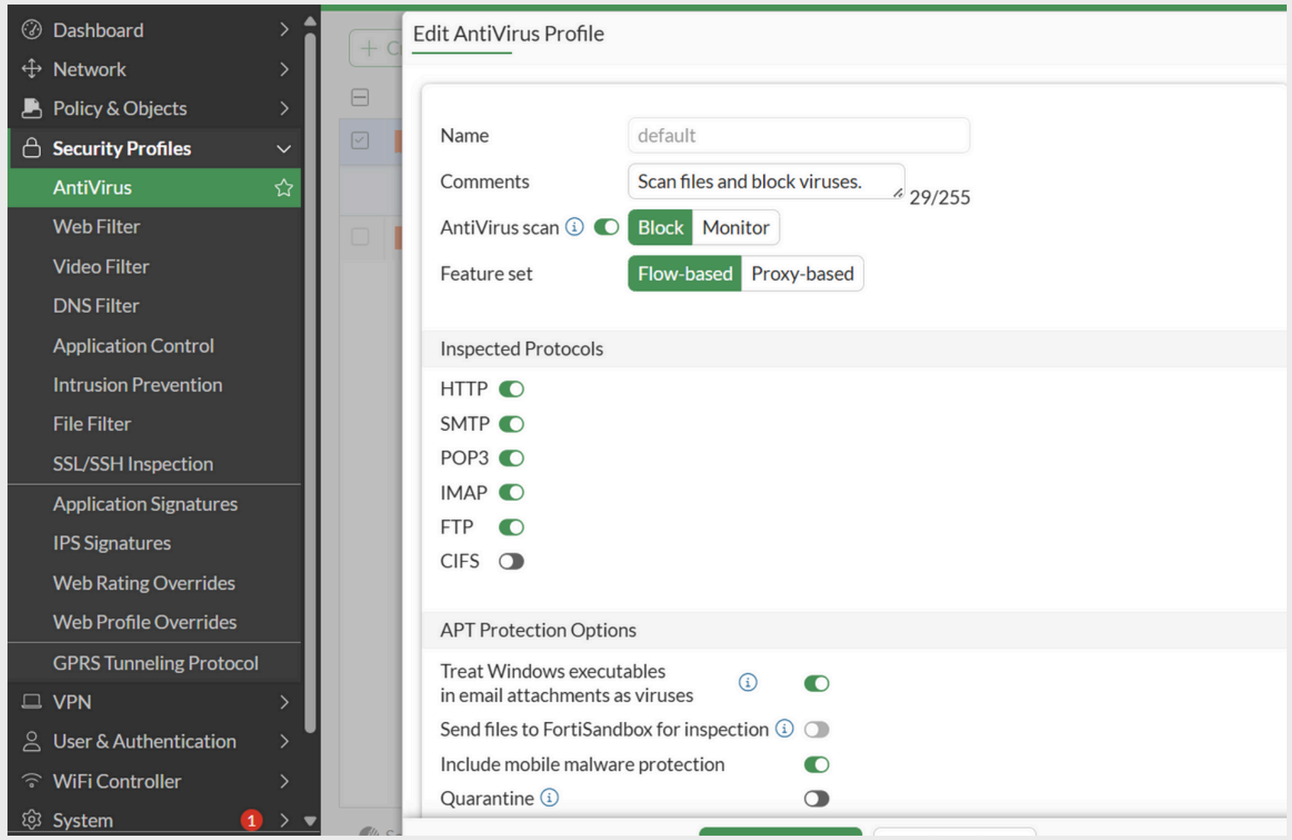
Anti-virus profile configuration

Profile Overview

Purpose: The Antivirus profile was configured to protect against malware threats through real-time scanning of network traffic.

Configuration summary

- **Profile Name:** default
- **Inspection Mode:** Flow-based
- **Inspected Protocols:** FTP, HTTP, SMTP, IMAP, POP3
- **Action:** Block
- **Applied to:** Internet firewall policy



Configuration steps

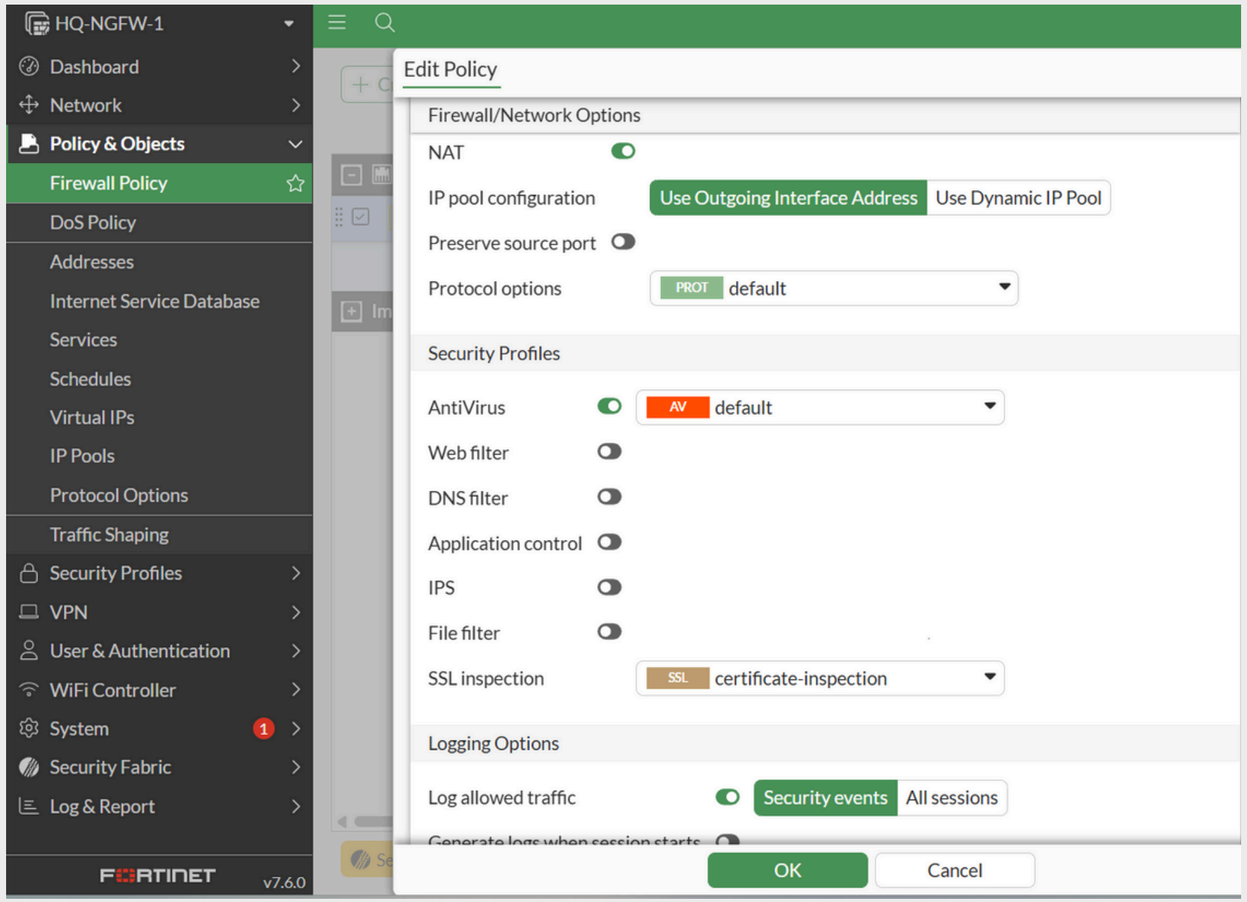
Step 1: Access Antivirus Profile

1. Navigate to Security Profiles > AntiVirus
2. Right-click the default profile
3. Select Edit
4. Feature Set: Flow-based (selected)
5. Inspected Protocols: Enabled FTP, HTTP, and other essential protocols

Anti-virus profile configuration

Firewall Policy Integration

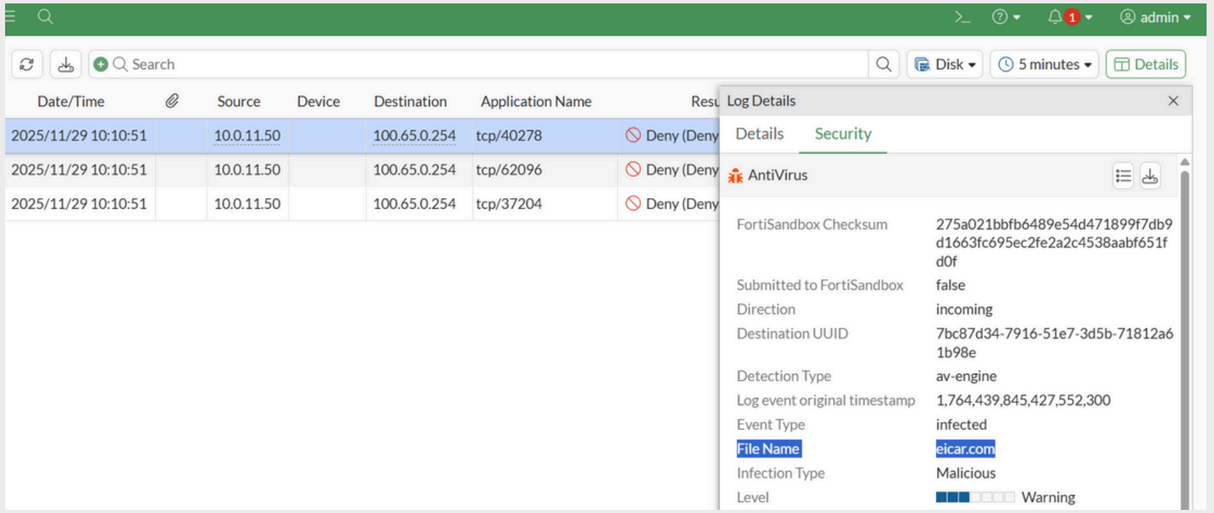
1. Navigate to Policy & Objects > Firewall Policy
2. Edit the Internet policy
3. Set Inspection Mode to Flow-based
4. Enable AntiVirus and select default profile



Anti-virus profile configuration

Testing Methodology

1. Tool Used: FileZilla FTP Client
2. Test File: eicar.com (harmless antivirus test file)
3. Protocol: FTP
4. Expected Result: Connection termination and file block

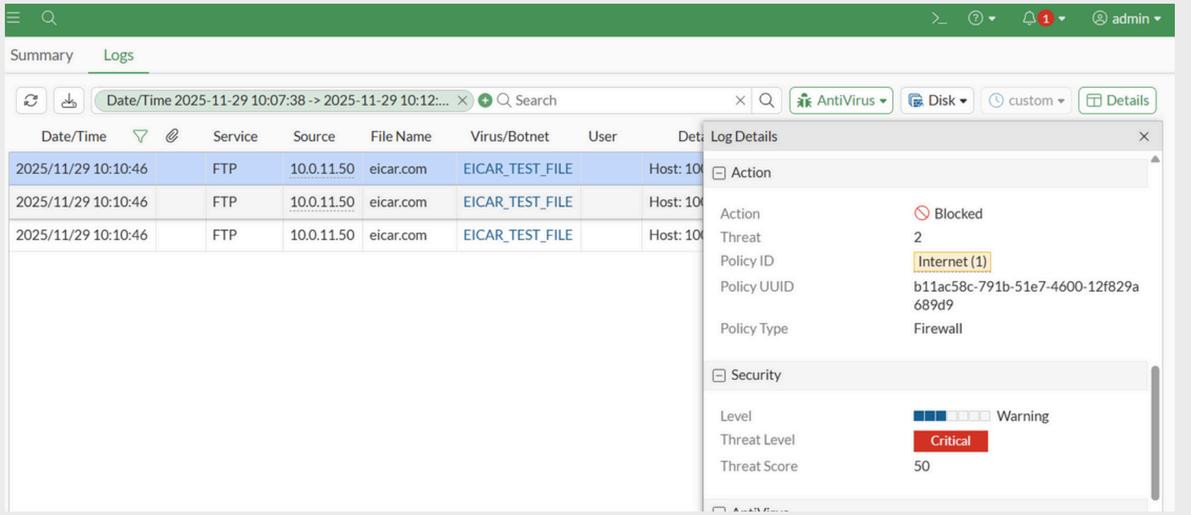


Log Analysis - Forward Traffic:

1. Location: Log & Report > Forward Traffic
2. Event: Antivirus violation detected
3. Action: Reset (connection terminated)
4. File: eicar.com

Log Analysis - Security Events:

1. Location: Log & Report > Security Events > AntiVirus
2. Threat: EICAR_TEST_FILE
3. Action: Blocked
4. Protocol: FTP



Web filter profile configuration

Profile Overview

- Name: Web-filter-Proxy
- Purpose: control web access and malicious sites

Configuration details

1. **FortiGuard Categories:**
   - Malicious websites : Block
     Figure 1.1
   - Job offer: Allow
   - Search engine: Allow
   - Social networking: Block
   - Streaming: Monitor
   - internet telephony: Warning
     Figure 1.2

Figure 1.1

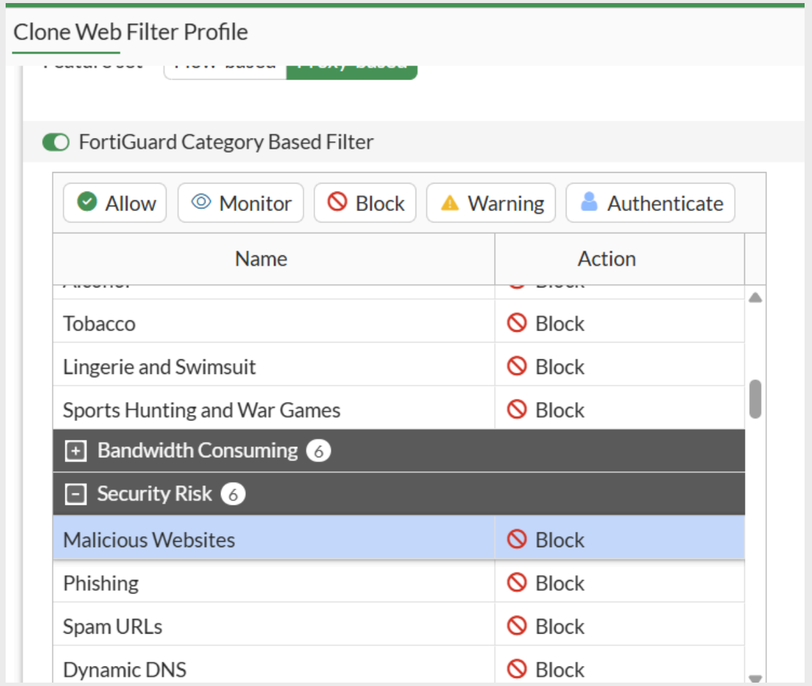
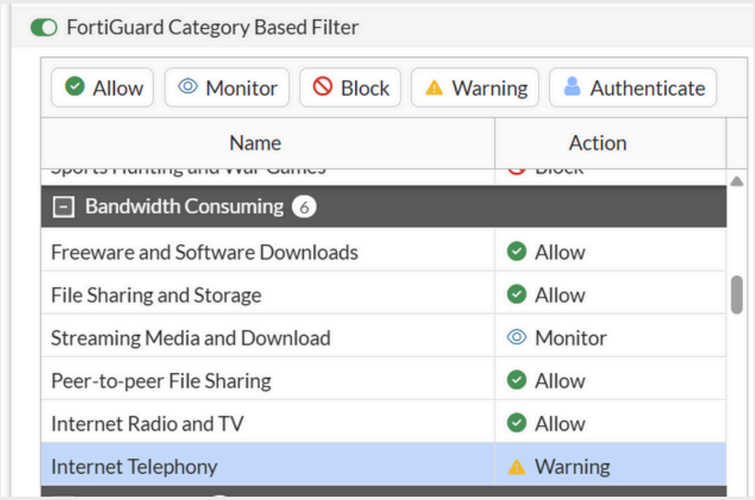
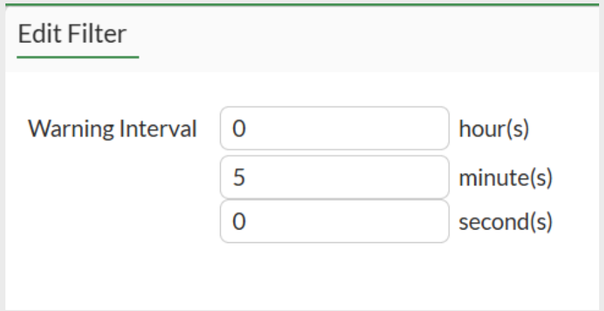


Figure 1.3





2. **Static URL Filter:**
   - Bing.com : Block
   - Facebook.com : Exempt

Figure 1.3

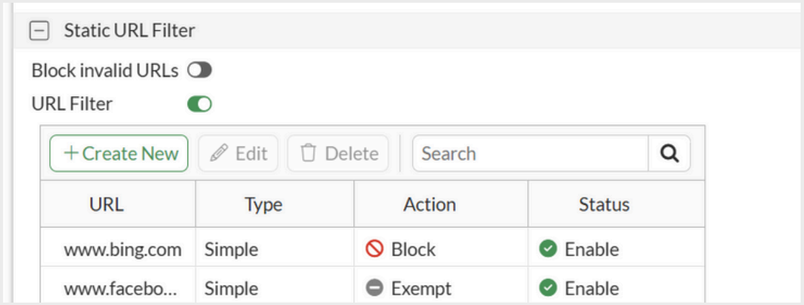
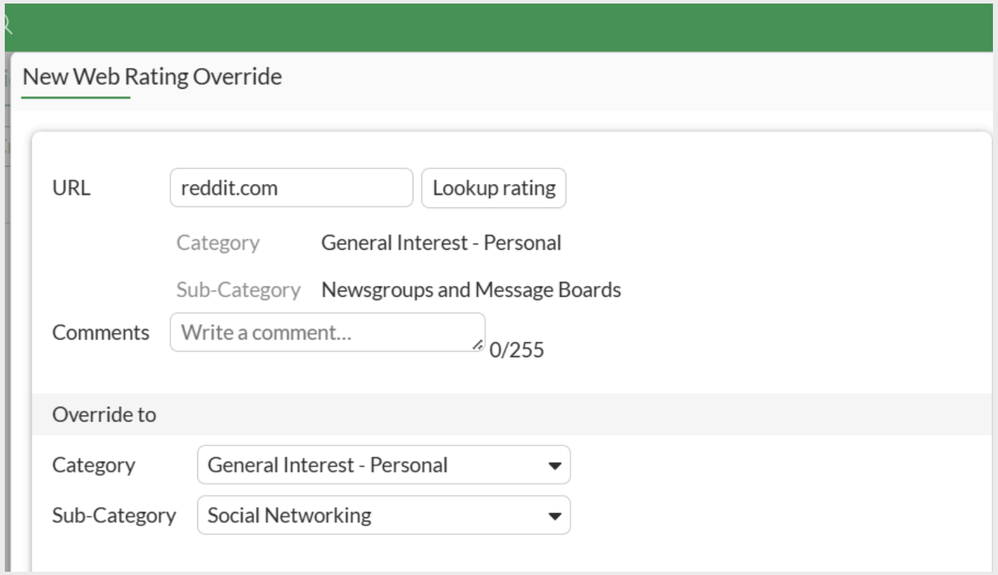


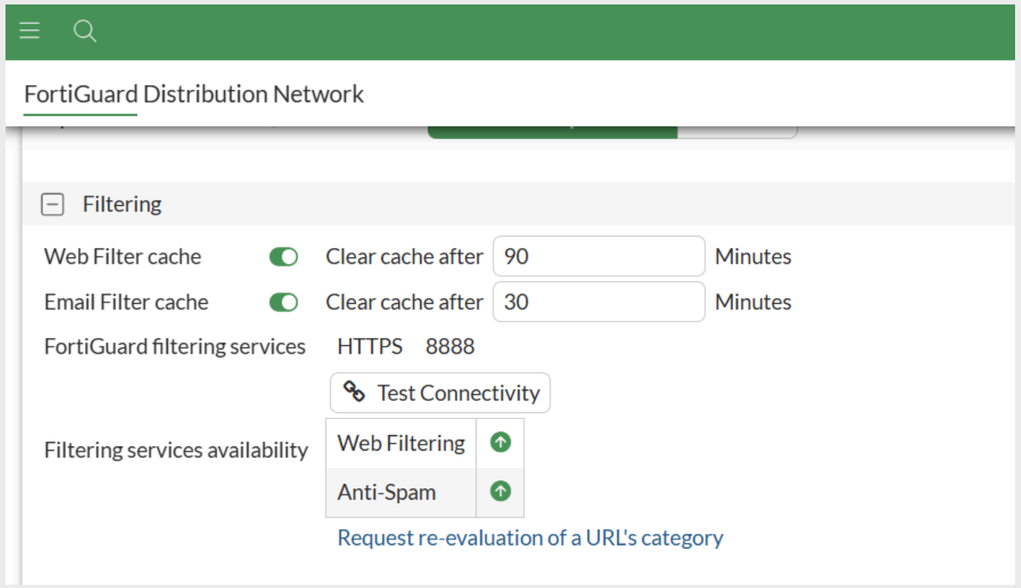
Figure 1.3

Special Features:

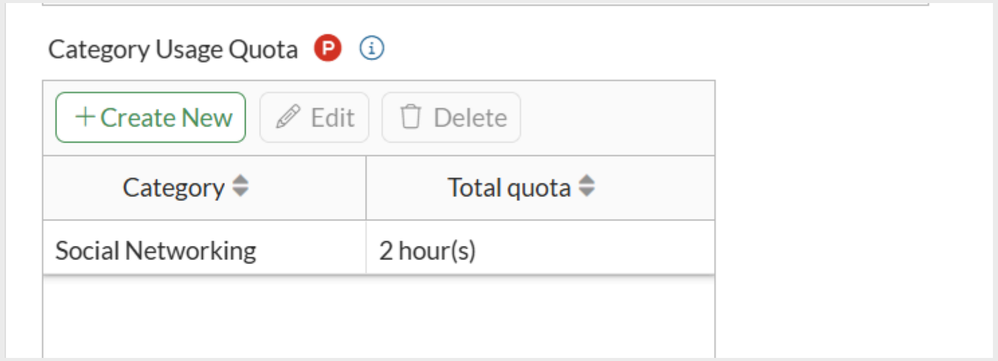
- **Web Rating Override: reddit.com**
  from “general interest-personal” to “Social networking”



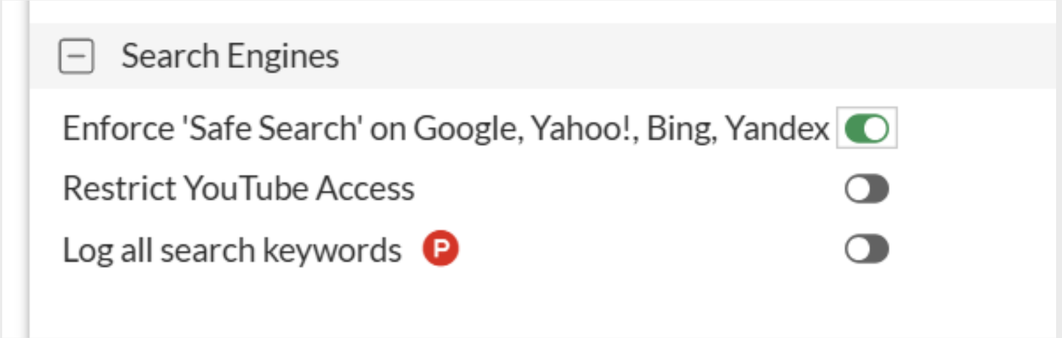
- **Web filter cash:**
  for 90 minutes



- **Quota:**
  on social networking for 2 hours



- **Safe search**



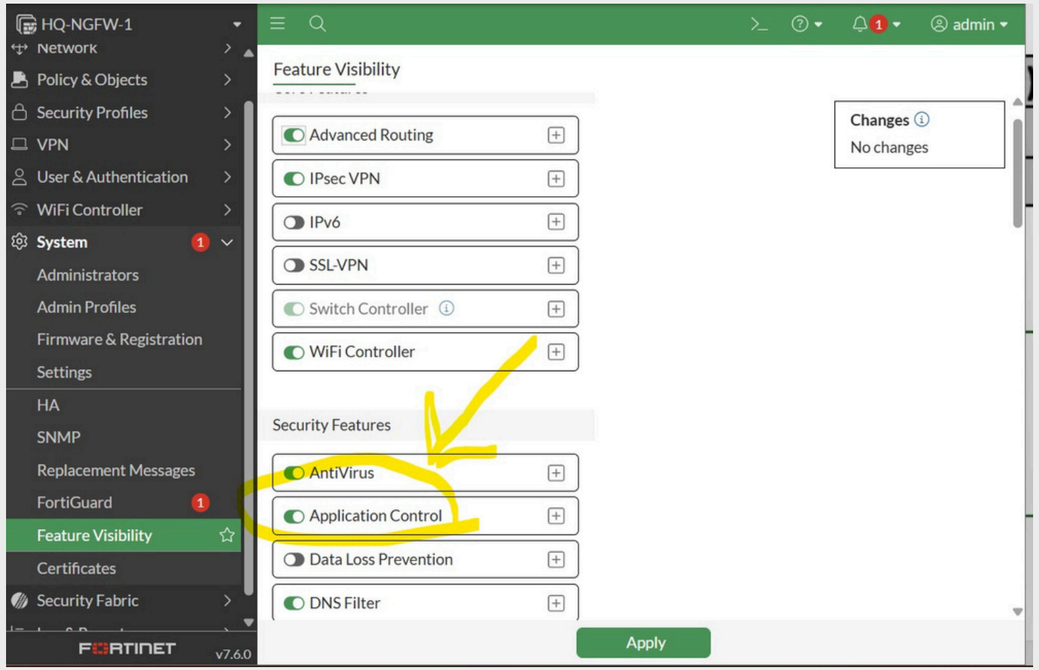
Configuring Application Control – FortiGate (Week 2)

Objective:

- To configure the Application Control security profile on FortiGate.
- To control network traffic based on application categories.
- To prepare the system for monitoring and reporting in Week 3.

Step 1: Feature Visibility Verification
Title: Verification of Feature Visibility
Content:

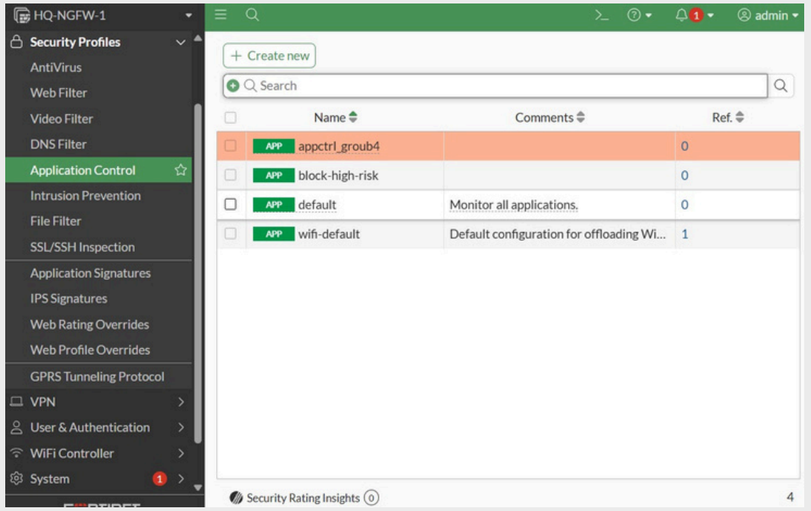
- Path: System → Feature Visibility
- The Application Control feature was verified and enabled.
- This step is required before creating any security profile.



Configuring Application Control – FortiGate (Week 2)

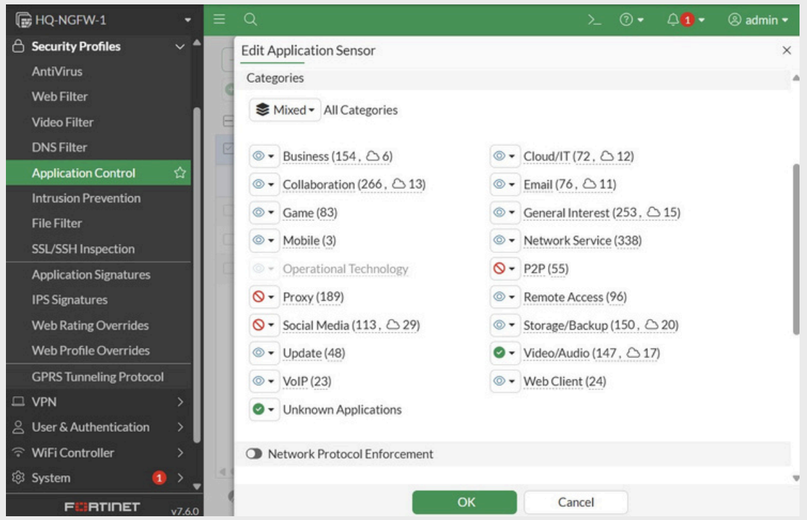
Step 2: Creating Application Control Profile
Title: Application Control Profile Creation
Content:

- Path: Security Profiles → Application Control
- A new profile was created.
- Profile Name: appctrl_group4
- Default inspection mode was used.



Step 3: Configuring Categories & Actions
Title: Application Categories Configuration
Content:

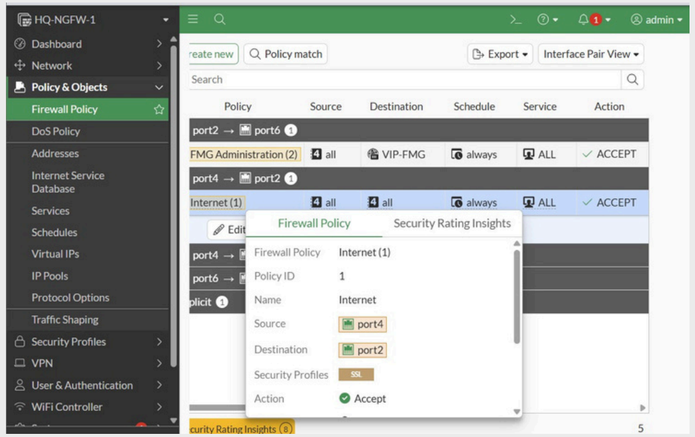
- Social Media → Block
- P2P → Block
- Gaming → Monitor
- Video/Audio → Allow

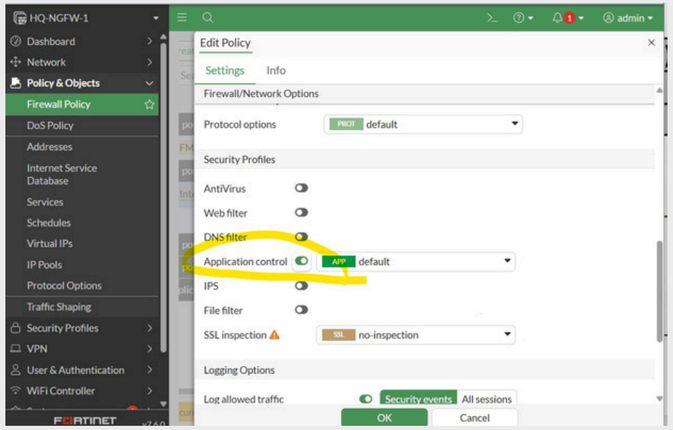


Configuring Application Control – FortiGate (Week 2)

Step 4: Applying Profile to Firewall Policy
Title: Firewall Policy Configuration
Content:

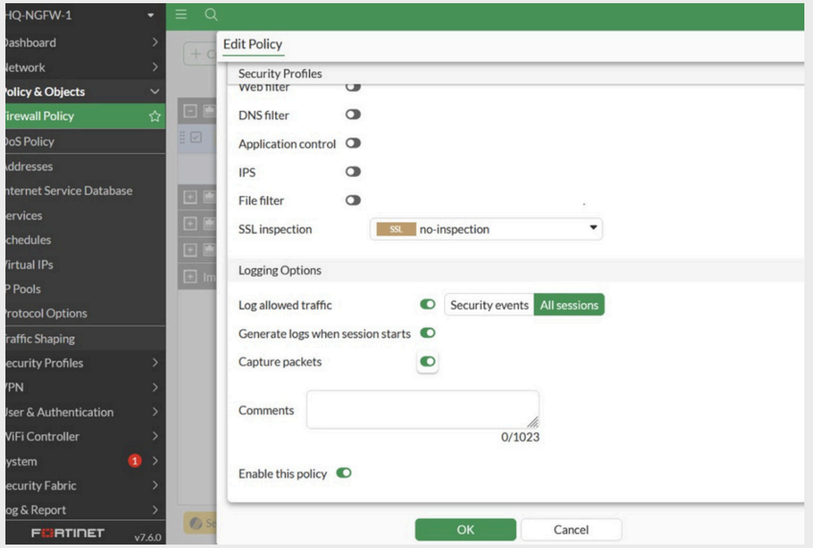
- Path: Policy & Objects → Firewall Policy
- Target Policy: Internet (1) (port4 → port2)
- Application Control was enabled.
- Profile appctrl_group4 was selected.





Enabling Logging (Important for Week 3)
Title: Logging Configuration
Content:

- Log Allowed Traffic was enabled.
- Logging Mode was set to All Sessions.
- This step ensures all application traffic is recorded.



Configuring Application Control – FortiGate (Week 2)

Configuration Summary

- Application Control feature enabled.
- New profile created and configured.
- Categories were blocked, allowed, or monitored.
- Profile successfully applied to the firewall policy.
- Logging enabled for monitoring.

Preparation for Week 3

- The system is now ready for traffic testing.
- Application logs will be generated.
- Monitoring and reporting will be performed in Week 3.

Conclusion:

- Application Control provides effective control over network applications.
- It enhances security by blocking unwanted traffic.
- Proper logging supports accurate monitoring and analysis.

Configuring IPS – FortiGate (Week 2)

Objective:

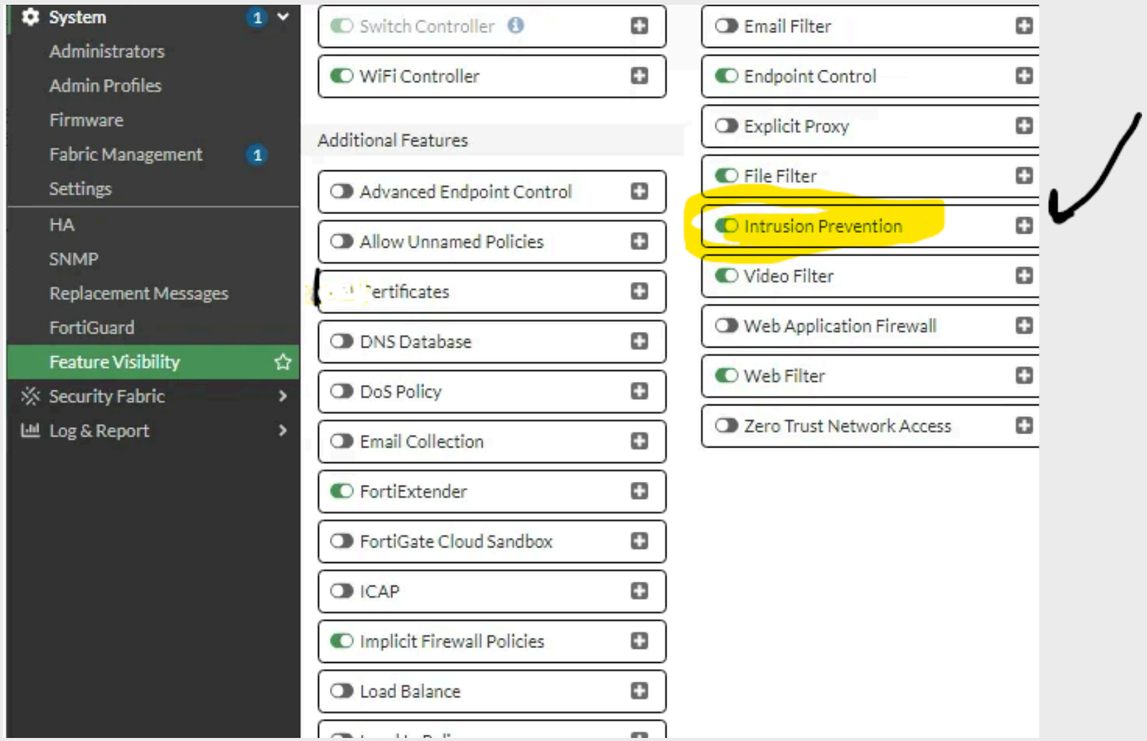
- To configure the Intrusion Prevention System (IPS) security profile on FortiGate.
- To protect servers and clients from known vulnerabilities and attack signatures.
- To prepare the system for monitoring and reporting in Week 3.

Step 1: Verifying IPS Availability

Title: IPS Feature Availability Check

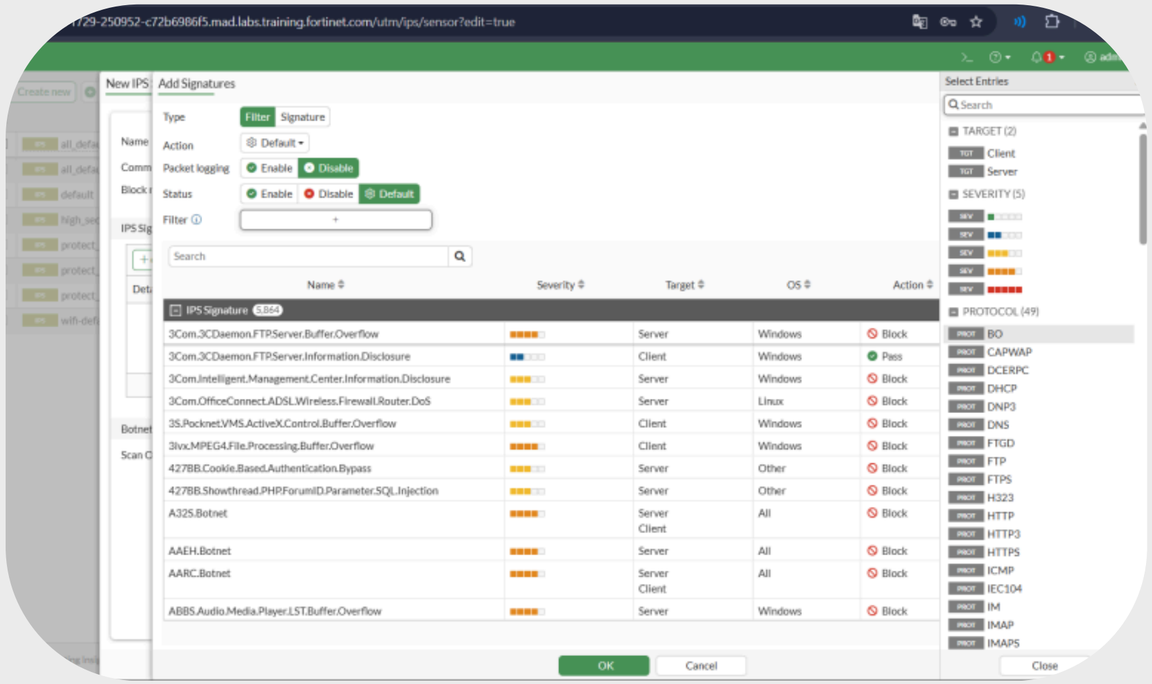
Content:

- Path: System → Feature Visibility
- Confirmed that the Intrusion Prevention System (IPS) feature is enabled.
- Ensuring IPS visibility is required before creating or applying IPS sensors.



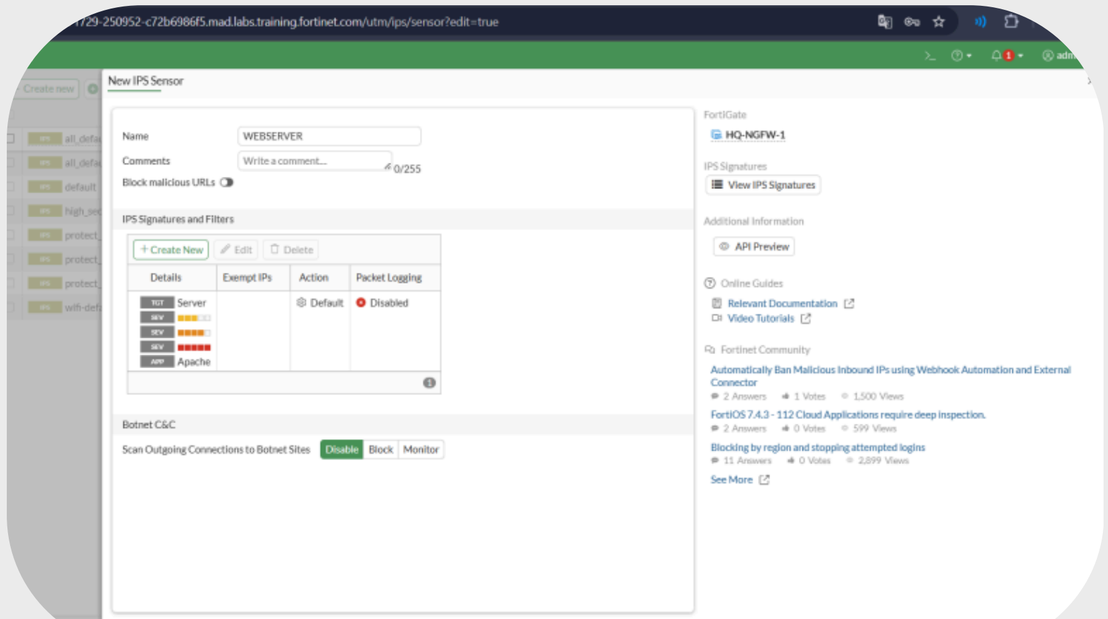
Configuring IPS – FortiGate (Week 2)

Step 2: Creating a New IPS Sensor
Title: Create New IPS Sensor
Content:
Path: Security Profiles → Intrusion Prevention → Create New
A new IPS sensor named "WEBSERVER" was created.
Block malicious URLs was kept at default.
This step initializes the IPS policy to be customized in the next steps.



Step 3: Adding IPS Signatures and Filters
Title: Adding IPS Filters
Content:

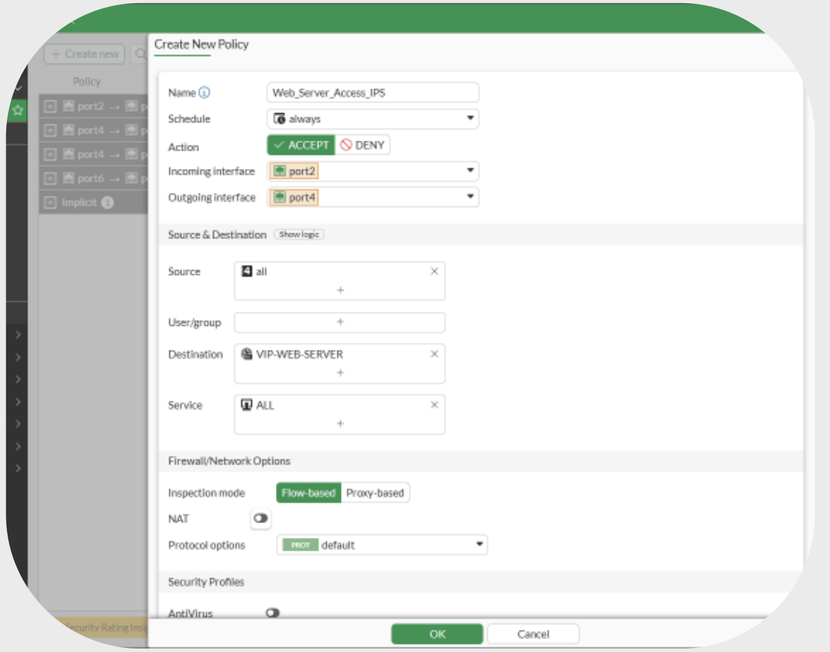
- Inside the newly created IPS sensor, click “Create New”.
- Added filters for:
  - Target: Server
  - Severity: High, Critical, Medium.
  - Protocol: HTTP, HTTPS, FTP, etc.
- The Action for threats was configured as Default.
- Packet Logging for selected signatures was Disabled.

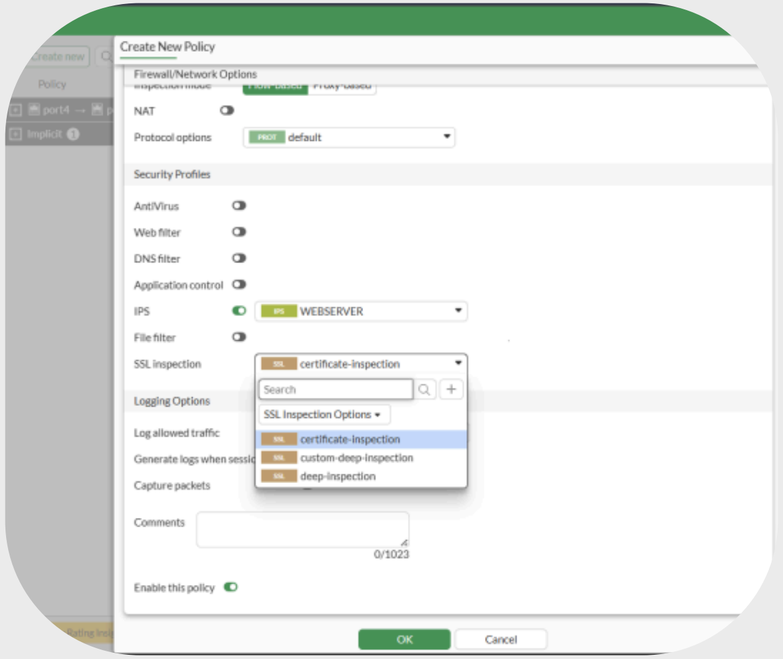


Configuring IPS – FortiGate (Week 2)

Step 4: Configuring Firewall Policy for Web Server Access
Title: Firewall Policy Configuration
Content:

- A new policy was created with the name WEB_SERVER_ACCESS_IPS.
- The Incoming Interface was set to port2 and the Outgoing Interface to port4.
- The Source was configured to all, and the Destination was set to VIP WEBSERVER.
- The Service was set to ALL, and the Action was set to ACCEPT.
- Under Security Profiles, IPS was enabled with the WEBSERVER profile.
- SSL Inspection was set to certificate-inspection.





Configuring Virtual IP (VIP) for Web Server
Title: Virtual IP (VIP) Configuration
Content:

- Path: Policy & Objects -> Virtual IPs
- Name: VIP WEBSERVER
- Interface:port2
- External IP address: 100.65.0.200
- Map to IPv4 address: 10.0.11.50

Configuring IPS– FortiGate (Week 2)

Configuration Summary

- Firewall policy "WEB_SERVER_ACCESS_IPS" was created and enabled.
- The policy was configured to protect the "VIP WEBSERVER".
- The Intrusion Prevention System (IPS) feature was enabled.
- The "WEBSERVER" IPS profile was applied to the policy to inspect traffic for threats.
- SSL Inspection was enabled to allow visibility into encrypted traffic.

Preparation for Week 3

- The system is now ready for traffic testing.
- Ready to simulate an attack to test IPS effectiveness.
- IPS logs will be generated upon detection.
- Monitoring and reporting will be performed in Week 3.

Conclusion:

- The IPS provides an effective security layer against network-based threats.
- It enhances security by actively blocking known exploits and malicious activity.
- Proper logging supports accurate monitoring and analysis of potential attacks.