

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

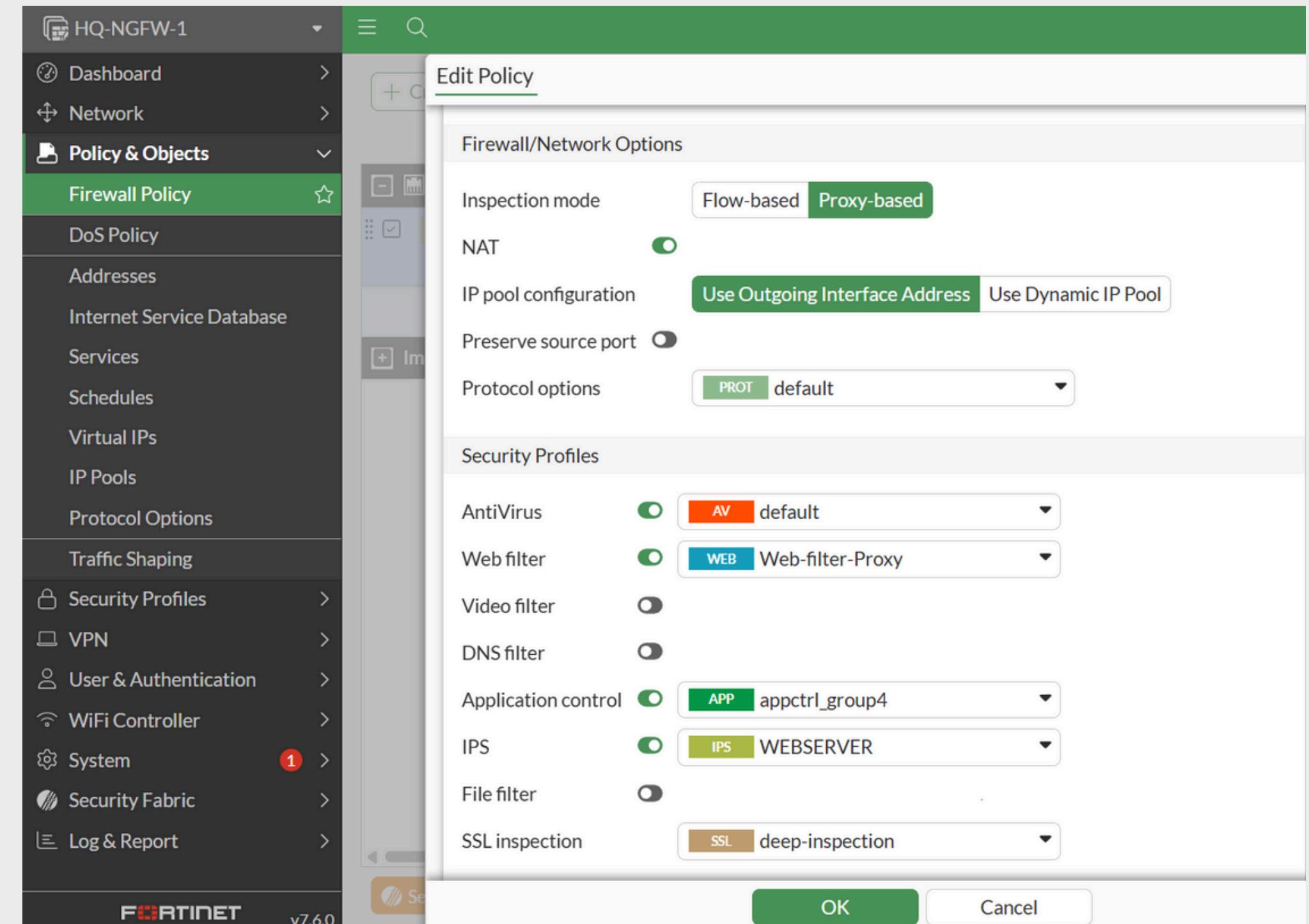
- App identification & control
- Risk-based policies

## ✓ 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.

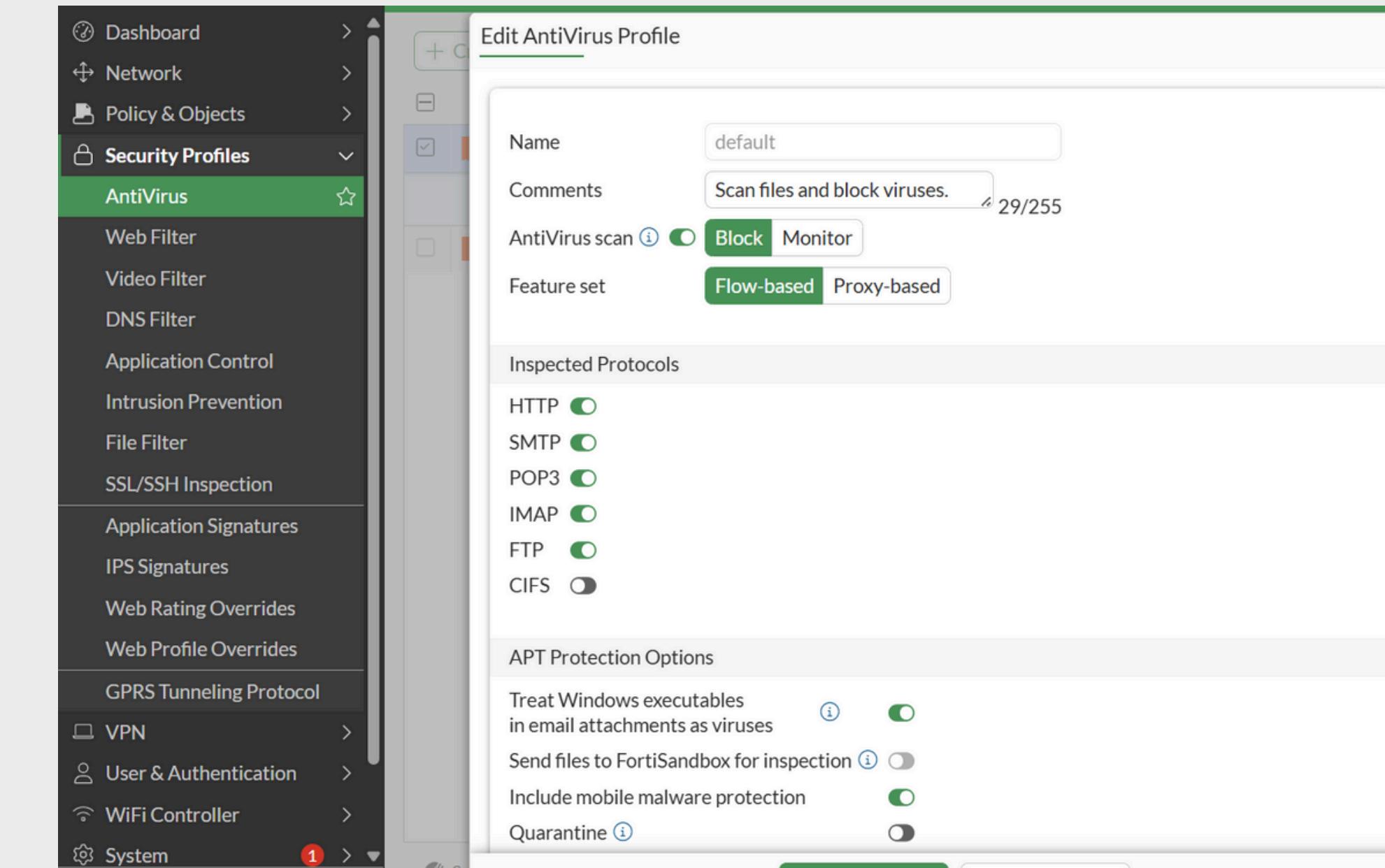
## Configuration summary

- 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

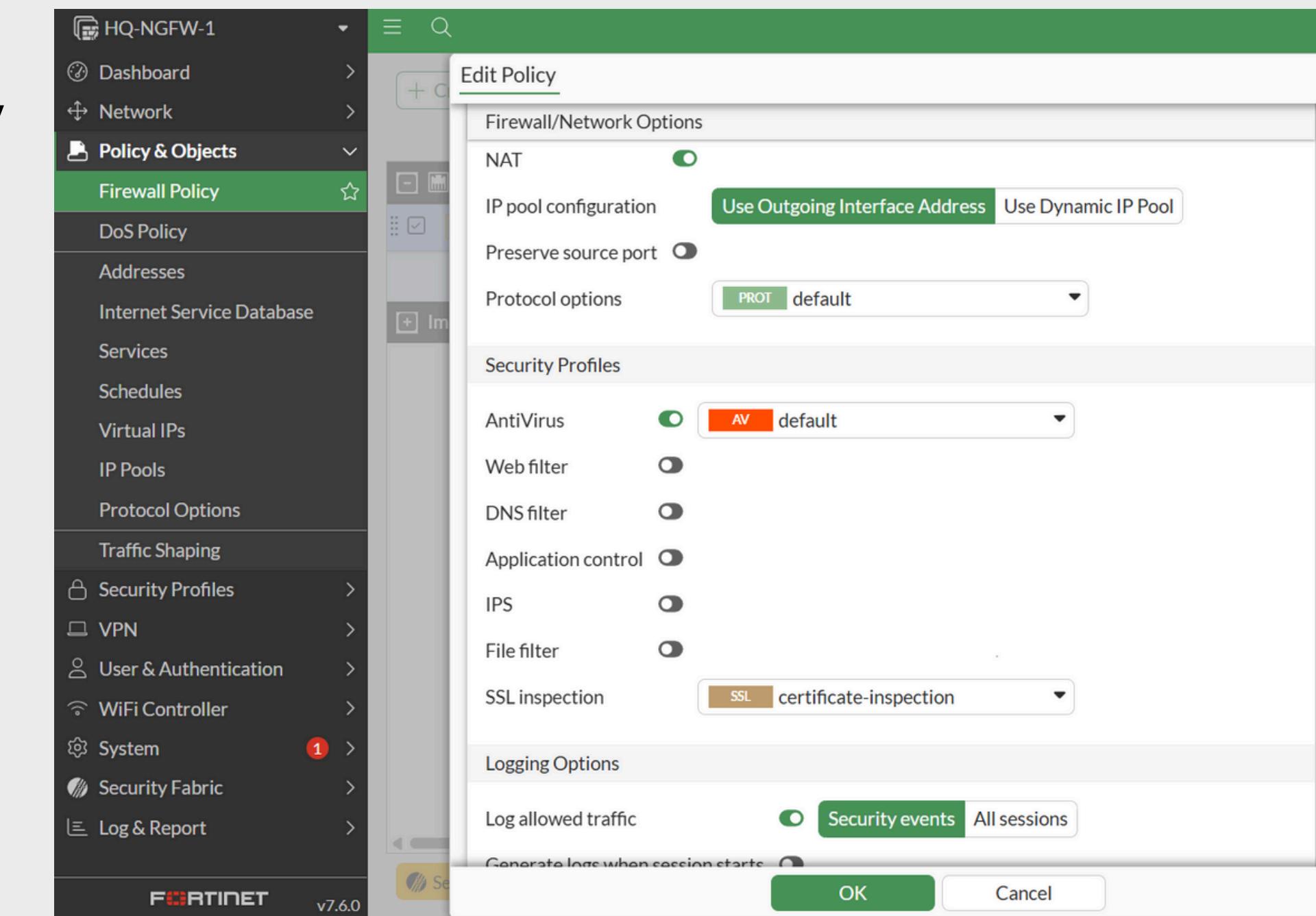
1. Navigate to Security Profiles > AntiVirus
2. Right-click the default profile
3. Select Edit
4. Feature Set: Flow-based (selected)
5. Inspected Protocols: Enabled FTP, HTTP, and other essential protocols



# 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

The screenshot shows a log entry for three separate connections from source 10.0.11.50 to destination 100.65.0.254. Each connection was denied due to an antivirus violation. The right panel displays detailed information about the third connection, including the FortiSandbox checksum (275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f), which is listed as 'infected' and 'Malicious' with a warning level.

Date/Time	Source	Device	Destination	Application Name	Result
2025/11/29 10:10:51	10.0.11.50		100.65.0.254	tcp/40278	Deny (Deny)
2025/11/29 10:10:51	10.0.11.50		100.65.0.254	tcp/62096	Deny (Deny)
2025/11/29 10:10:51	10.0.11.50		100.65.0.254	tcp/37204	Deny (Deny)

## Log Analysis - Security Events:

1. Location: Log & Report > Security Events > AntiVirus
2. Threat: EICAR\_TEST\_FILE
3. Action: Blocked
4. Protocol: FTP

The screenshot shows three security events for the threat 'EICAR\_TEST\_FILE' from source 10.0.11.50 to destination 100.65.0.254 via the FTP protocol. All three events were blocked. The right panel shows the threat is identified as 'Internet (1)' with a policy ID of b11ac58c-791b-51e7-4600-12f829a689d9 and a firewall policy type.

Date/Time	Service	Source	File Name	Virus/Botnet	User	Host
2025/11/29 10:10:46	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254
2025/11/29 10:10:46	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254
2025/11/29 10:10:46	FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254

# 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**
- Job offer: **Allow**
- Search engine: **Allow**
- Social networking: **Block**
- Streaming: **Monitor**
- internet telephony: **Warning**

Figure 1.1

Name	Action
Sports Hunting and War Games	Block
Bandwidth Consuming	Block
Security Risk	Block
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block

Figure 1.1

### 2. Static URL Filter:

- Bing.com : **Block**
- Facebook.com : **Exempt**

Figure 1.3

URL	Type	Action	Status
www.bing.com	Simple	Block	Enable
www.facebook.com	Simple	Exempt	Enable

Figure 1.3

Figure 1.3

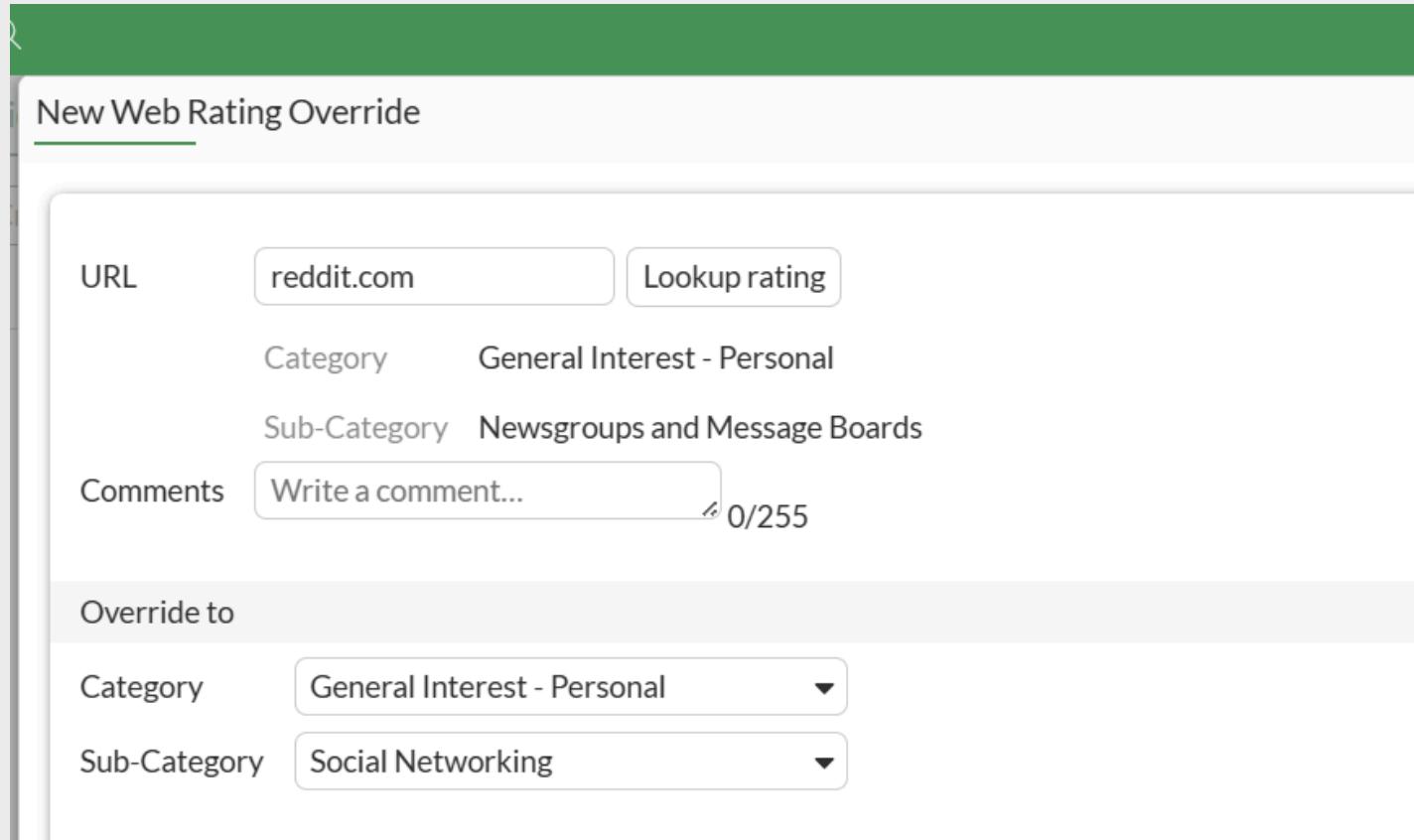
Name	Action
Sports Hunting and War Games	Block
Bandwidth Consuming	Allow
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Monitor
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Warning

**Edit Filter**

Warning Interval: 0 hour(s), 5 minute(s), 0 second(s)

## Special Features:

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



New Web Rating Override

URL: reddit.com [Lookup rating](#)

Category: General Interest - Personal

Sub-Category: Newsgroups and Message Boards

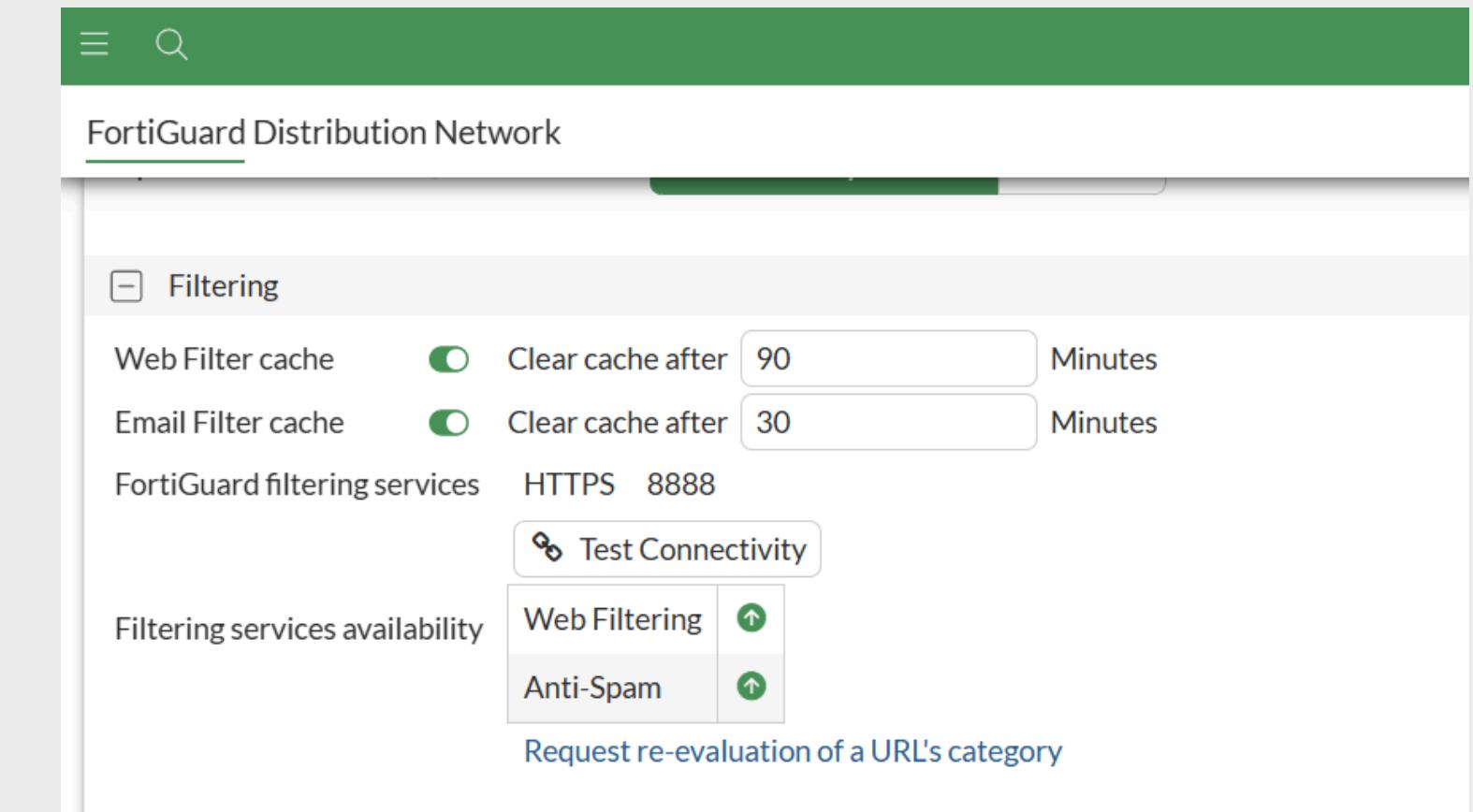
Comments: Write a comment... 0/255

Override to:

Category: General Interest - Personal

Sub-Category: Social Networking

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



FortiGuard Distribution Network

Filtering

Web Filter cache:  Clear cache after 90 Minutes

Email Filter cache:  Clear cache after 30 Minutes

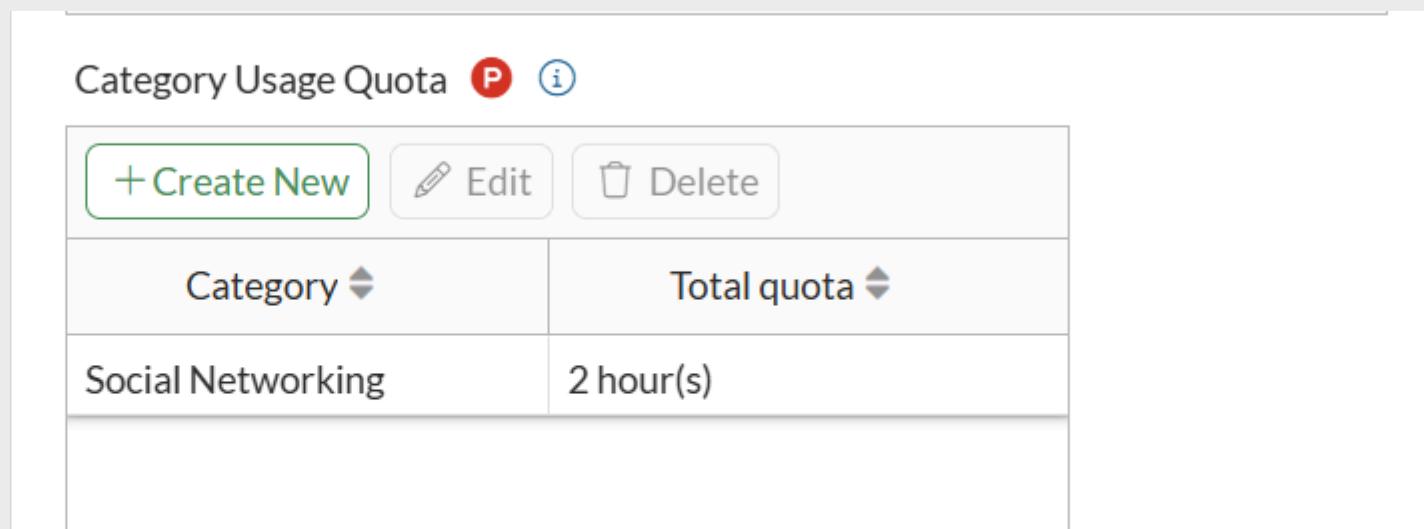
FortiGuard filtering services: HTTPS 8888 [Test Connectivity](#)

Filtering services availability:

Web Filtering	
Anti-Spam	

[Request re-evaluation of a URL's category](#)

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

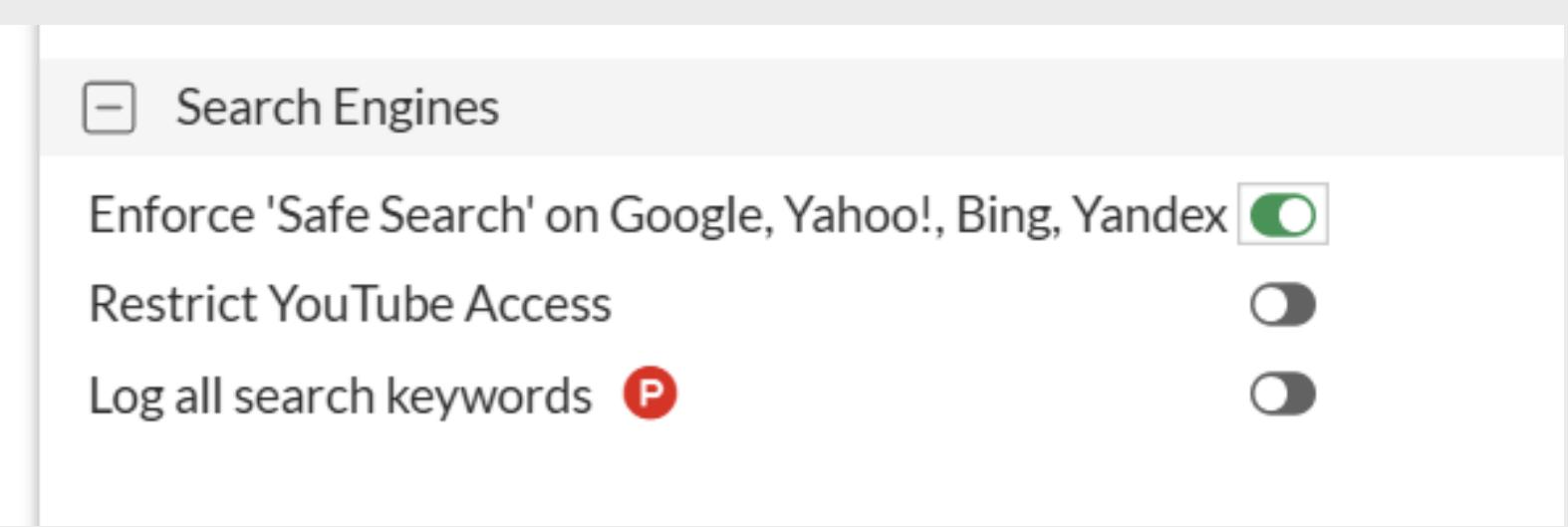


Category Usage Quota  

+ Create New  

Category	Total quota
Social Networking	2 hour(s)

- **Safe search**



Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex

Restrict YouTube Access

Log all search keywords 

## Configuring Application Control – FortiGate (Week 2)

Objective:

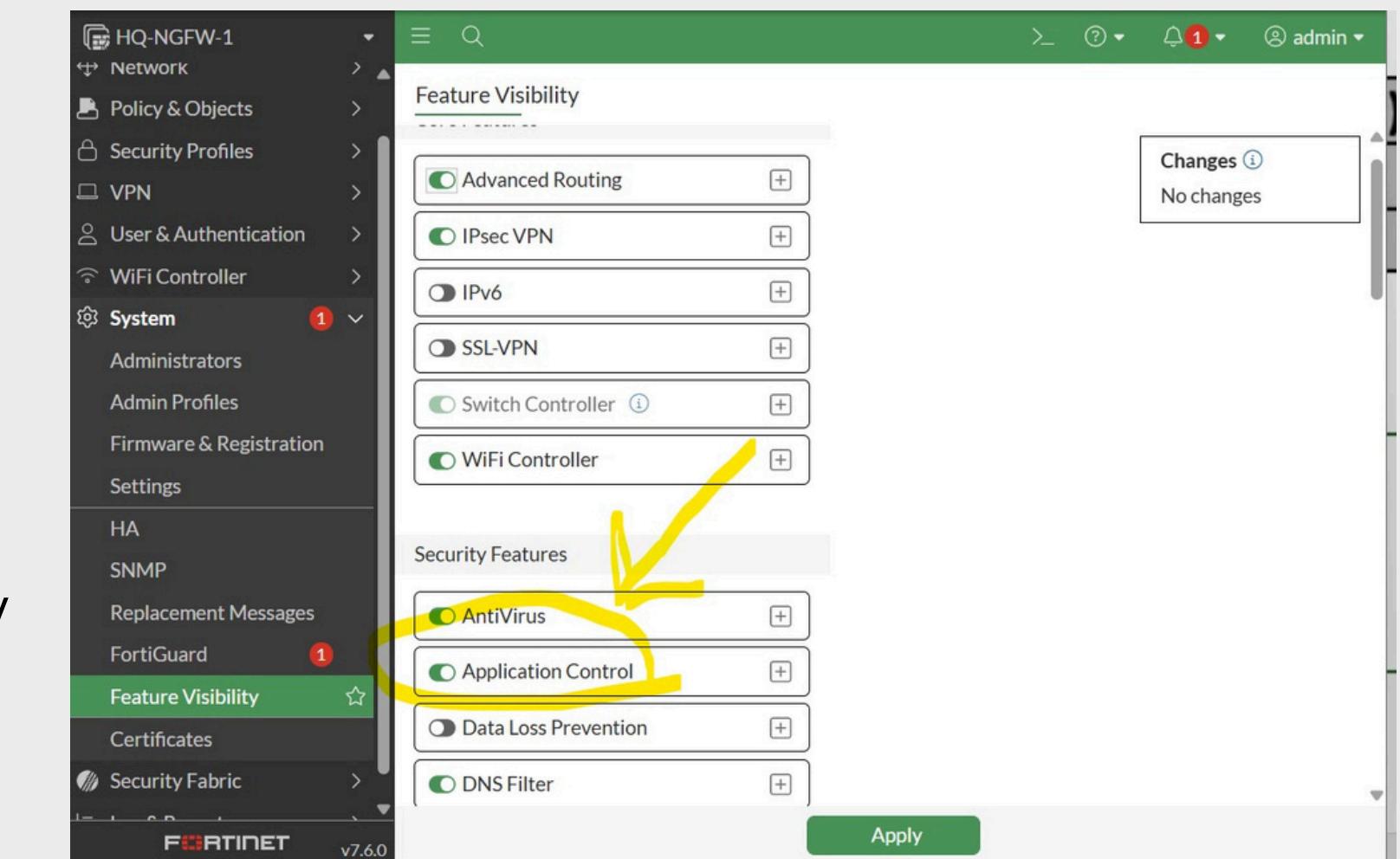
- To configure the Application Control security profile on FortiGate.
- To control network traffic based on application categories.
- To prepare the system for monitoring and reporting in Week 3.

### 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.

The screenshot shows the FortiGate Management UI with the title bar "HQ-NGFW-1" and user "admin". The left sidebar menu is open, showing various security profiles like AntiVirus, Web Filter, Video Filter, DNS Filter, and Application Control (which is selected). The main pane displays a table of application control profiles:

Name	Comments	Ref.
appctrl_group4		0
block-high-risk		0
default	Monitor all applications.	0
wifi-default	Default configuration for offloading Wi...	1

Step 3: Configuring Categories & Actions

Title: Application Categories Configuration

Content:

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

The screenshot shows the "Edit Application Sensor" dialog box. The left sidebar menu is identical to the previous screenshot. The main pane shows the "Categories" section with a tree view of application categories and their counts:

- Mixed - All Categories
  - Business (154, ▲ 6)
  - Collaboration (266, ▲ 13)
  - Game (83)
    - Mobile (3)
  - Operational Technology
  - Proxy (189)
    - Social Media (113, ▲ 29)
  - Update (48)
  - VoIP (23)
  - Unknown Applications
- Cloud/IT (72, ▲ 12)
- Email (76, ▲ 11)
- General Interest (253, ▲ 15)
- Network Service (338)
  - P2P (55)
- Remote Access (96)
  - Storage/Backup (150, ▲ 20)
- Video/Audio (147, ▲ 17)
  - Web Client (24)

## 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.

The first screenshot shows the 'Firewall Policy' list with two entries: 'port2 → port6' and 'port4 → port2'. The second screenshot shows the 'Edit Policy' dialog for the 'Internet (1)' policy, where 'Application control' is selected under 'Protocol Options'. The third screenshot shows the 'Edit Policy' dialog with 'SSL inspection' set to 'no-inspection' and 'Log allowed traffic' checked.

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.

The screenshot shows the 'Edit Policy' dialog with 'Log allowed traffic' checked under 'Logging Options'.

## 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:

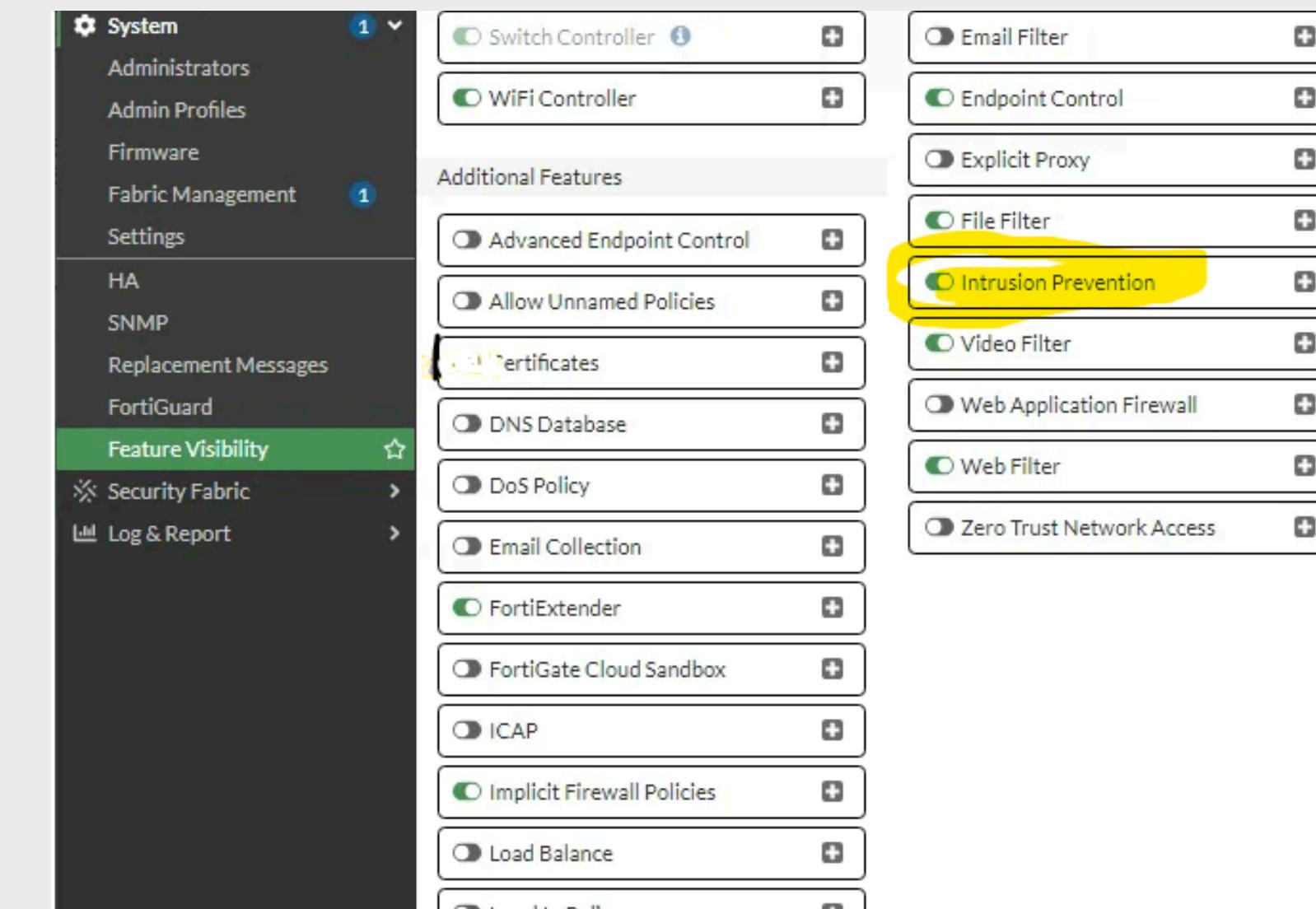
- To configure the Intrusion Prevention System (IPS) security profile on FortiGate.
- To protect servers and clients from known vulnerabilities and attack signatures.
- To prepare the system for monitoring and reporting in Week 3.

### 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 "WEB SERVER" was created.

Block malicious URLs was kept at default.

This step initializes the IPS policy to be customized in the next steps.

Name	Severity	Target	OS	Action
3Com.3CDaemon.FTP.Server.Buffer.Overflow	High	Server	Windows	Block
3Com.3CDaemon.FTP.Server.Information.Disclosure	Medium	Client	Windows	Pass
3Com.Intelligent.Management.Center.Information.Disclosure	Medium	Server	Windows	Block
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	Medium	Server	Linux	Block
3S.Rocknet.VMS.ActiveX.Control.Buffer.Overflow	Medium	Client	Windows	Block
3Ivx.MPEG4.File.Processing.Buffer.Overflow	Medium	Client	Windows	Block
427BB.Cookie.Based.Authentication.Bypass	Medium	Server	Other	Block
427BB.Showthread.PHPForumID.Parameter.SQL.Injection	Medium	Server	Other	Block
A32S.Botnet	Medium	Server	All	Block
AAEH.Botnet	Medium	Server	All	Block
AARC.Botnet	Medium	Server	Client	Block
ABBS.Audio.Media.Player.LST.Buffer.Overflow	Medium	Server	Windows	Block

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.

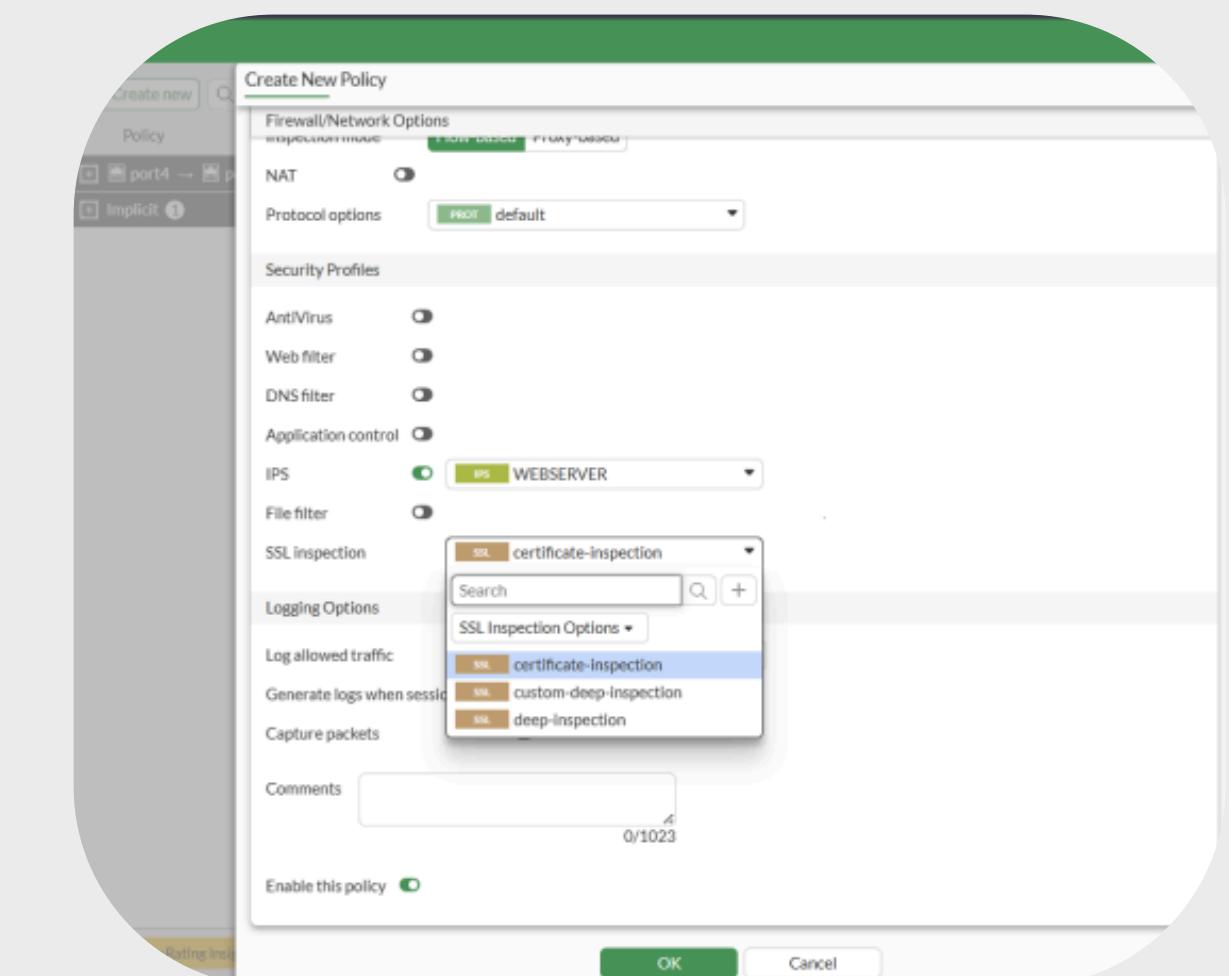
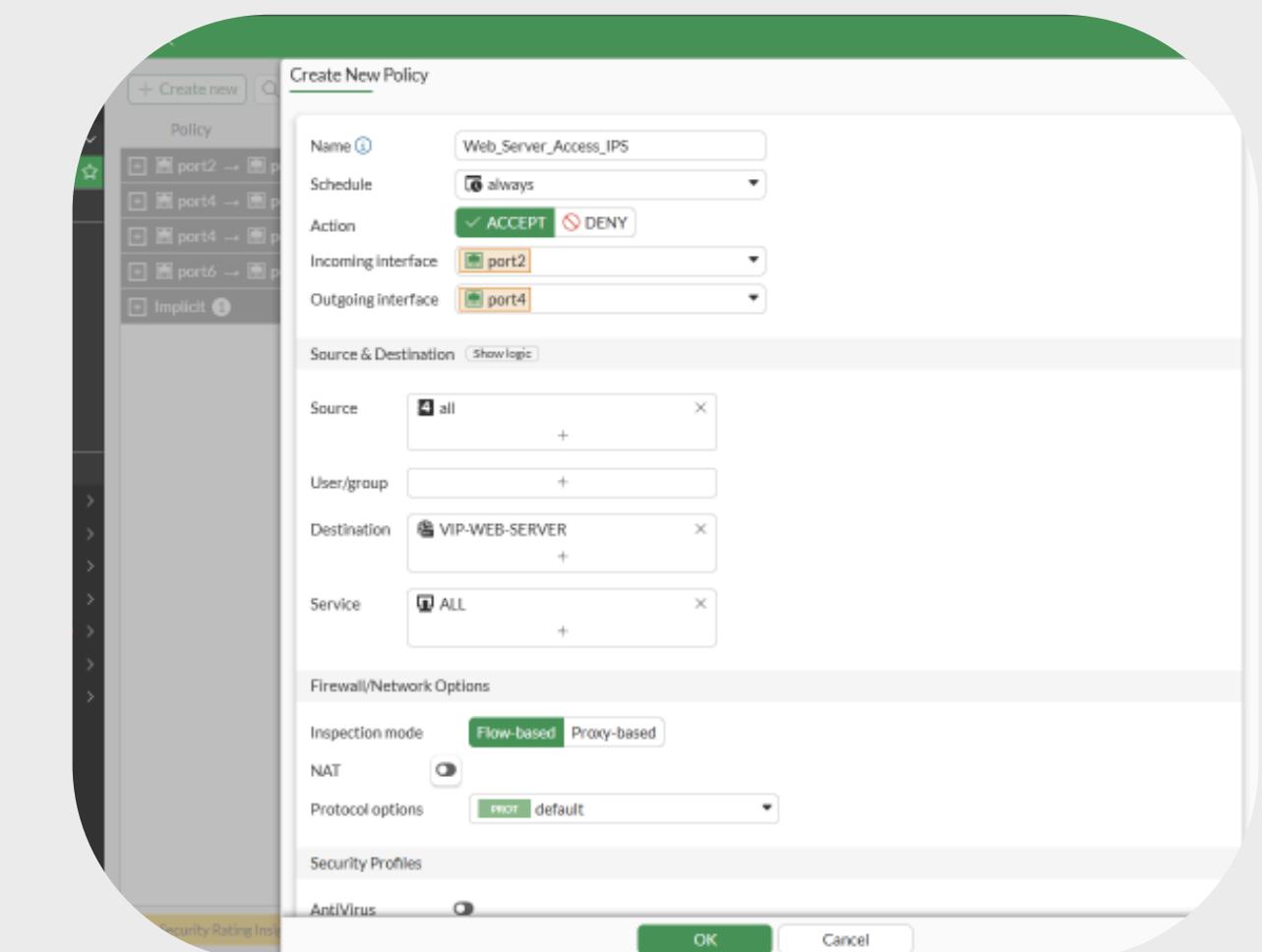
# Configuring IPS – FortiGate (Week 2)

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 WEB SERVER".
- The Intrusion Prevention System (IPS) feature was enabled.
- The "WEB SERVER" IPS profile was applied to the policy to inspect traffic for threats.
- SSL Inspection was enabled to allow visibility into encrypted traffic.

### 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.



### 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.

