رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

PROJECT

ADVANCED FORTIGATE SECURITY PROFILES

PRESENTATION

https://depi.gov.eg

› Start Slide

رواد مصر الرقمية

Our Great Team

وزارة الاتصالات وتكنولوجيا المعلومات

Mohamed Abdelaal

Eyad Mahmoud

Arwa Essam

Filopateer Atef

Youssef Yasser

https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Understanding Security Profiles

Security Profiles in FortiGate are a group of features that help you inspect, control, and protect network traffic after it has been allowed by a firewall policy.

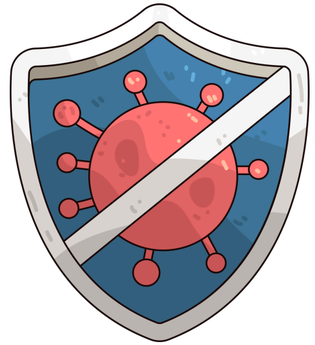
Think of Security Profiles as the tools FortiGate uses to check if the traffic is safe, clean, and not harmful.

When a firewall policy allows the traffic, Security Profiles then start analyzing that traffic to make sure it does not contain anything dangerous.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles



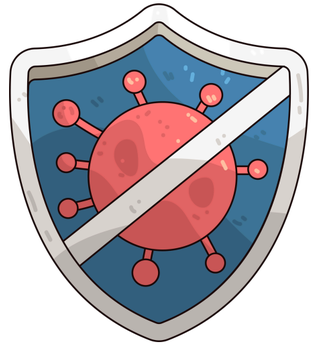
1. Antivirus

- Scans files and data passing through the firewall.
- Blocks viruses, malware, and suspicious downloads.
- Protects users from infected files.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :



Flow-based Inspection (Fast Mode)

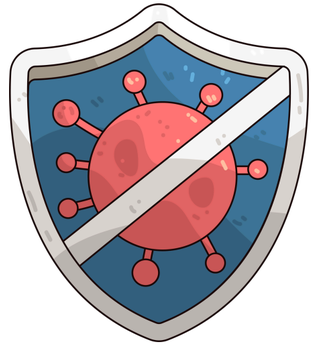
Fast – Lightweight – Low Resource Usage

- Scans traffic on the fly while it’s passing.
- Provides higher performance and better speed.
- Suitable for environments with many users or lower-spec devices.
- Detection rate is lower compared to Proxy mode.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :



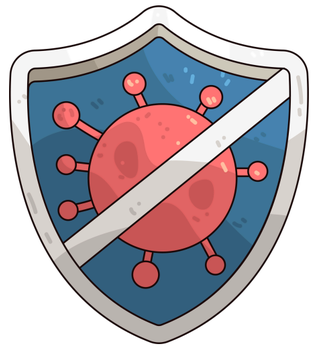
Flow-based Inspection (Fast Mode)

Use Cases when:

- Performance and speed are the priority.
- Your FortiGate hardware is limited.
- You want to reduce latency and save bandwidth.

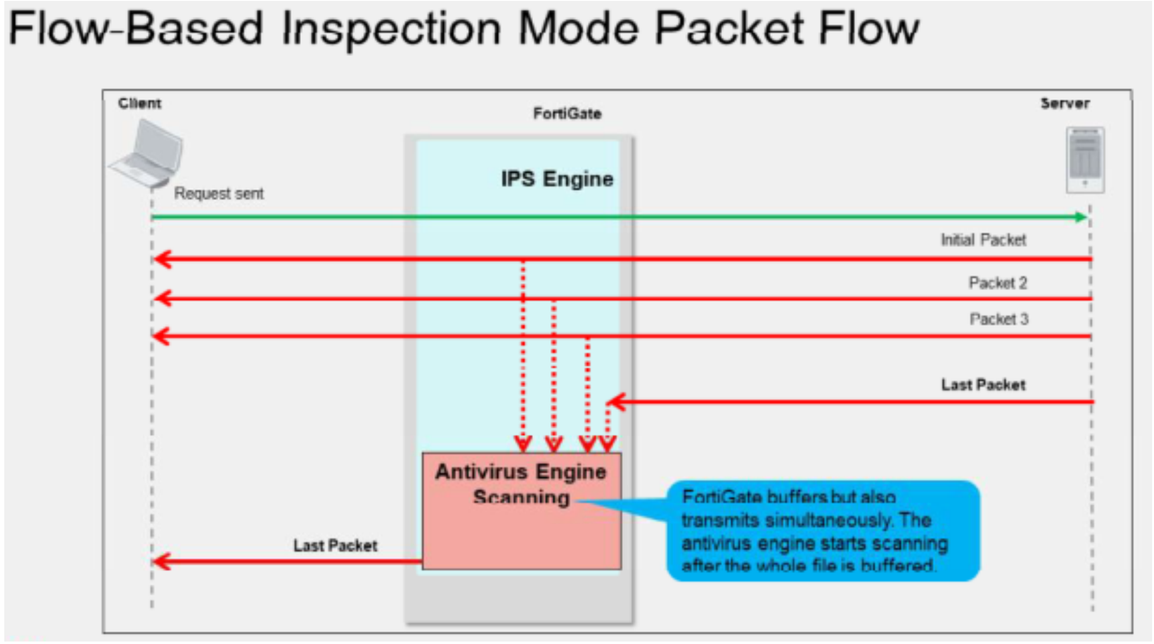
رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات



1.1 Antivirus Inspection Mode :

Flow-based Inspection (Fast Mode)



https://depi.gov.eg

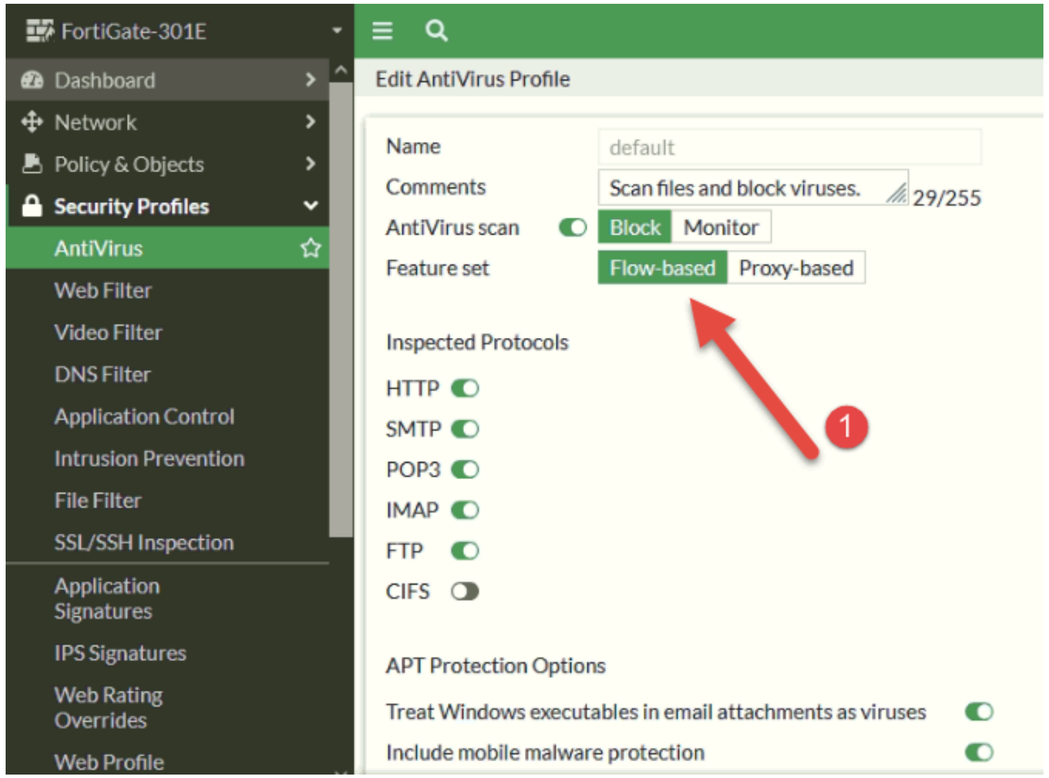
رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Flow-based Inspection (Fast Mode)

Configuration Profile



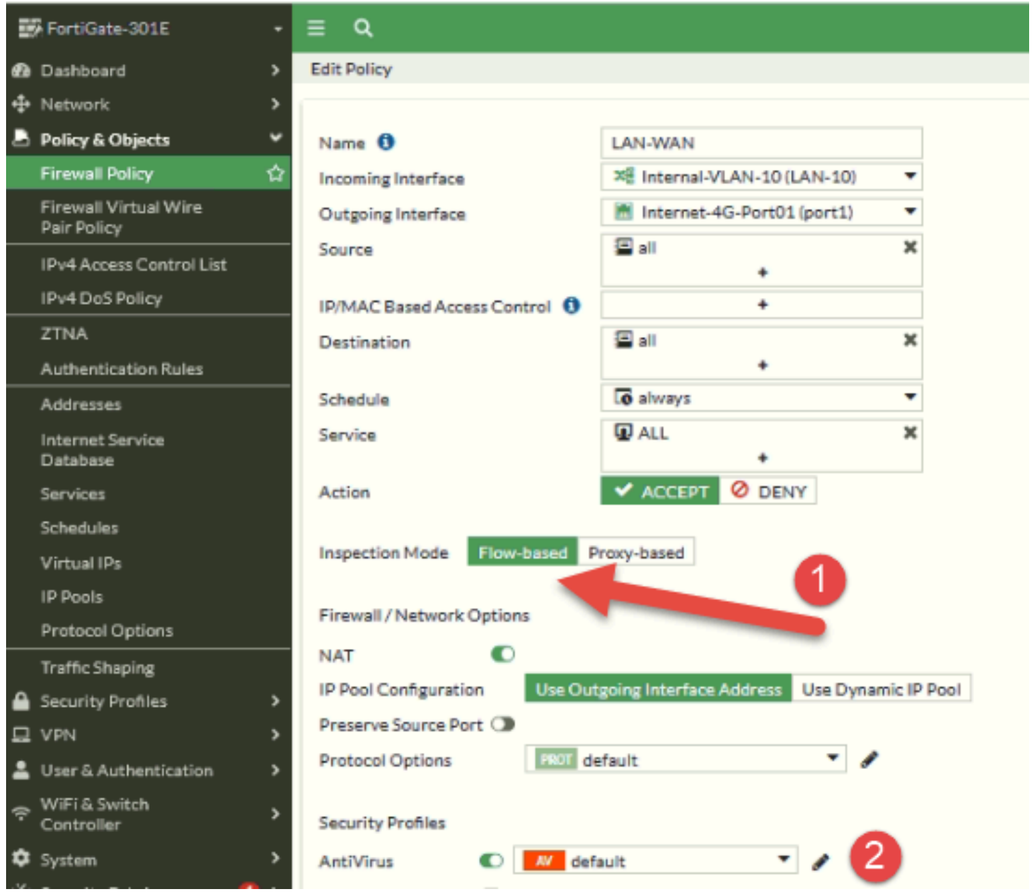
رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Flow-based Inspection (Fast Mode)

Configuration Policy



https://depi.gov.eg

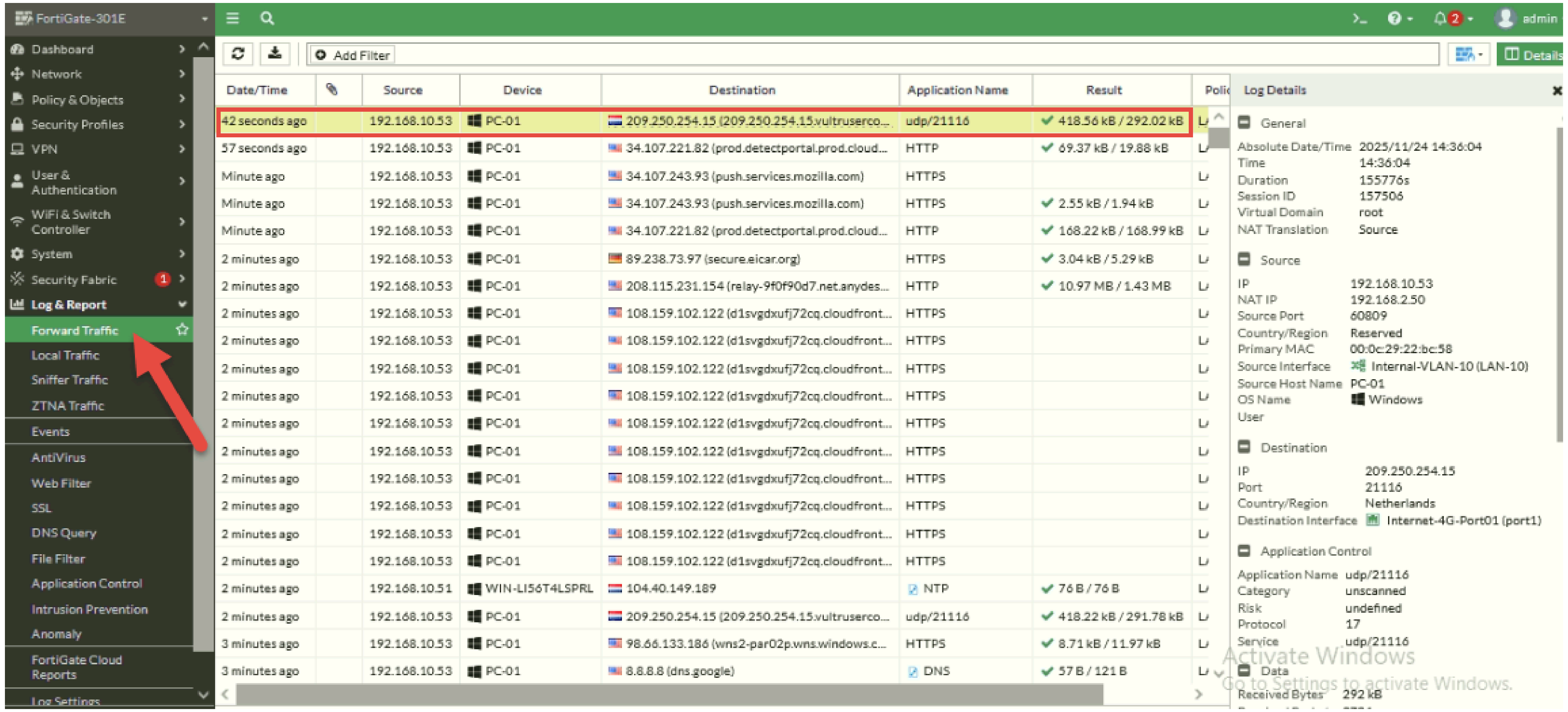
رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Flow-based Inspection (Fast Mode)

Logs & Monitoring

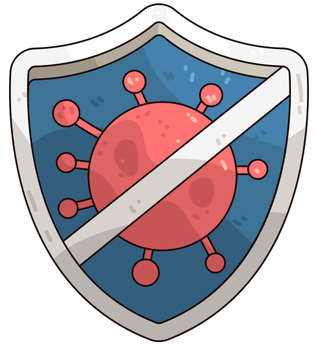


https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :



Proxy-based Inspection (Deep Mode)

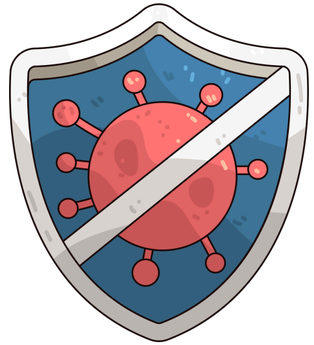
Deep – More Accurate – Full Inspection

- Acts as a proxy between the user and the internet.
- Temporarily stores part of the traffic and performs full content inspection.
- Higher accuracy and detection rate.
- Consumes more CPU and RAM than Flow-based.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :



Proxy-based Inspection (Deep Mode):

Use Cases when:

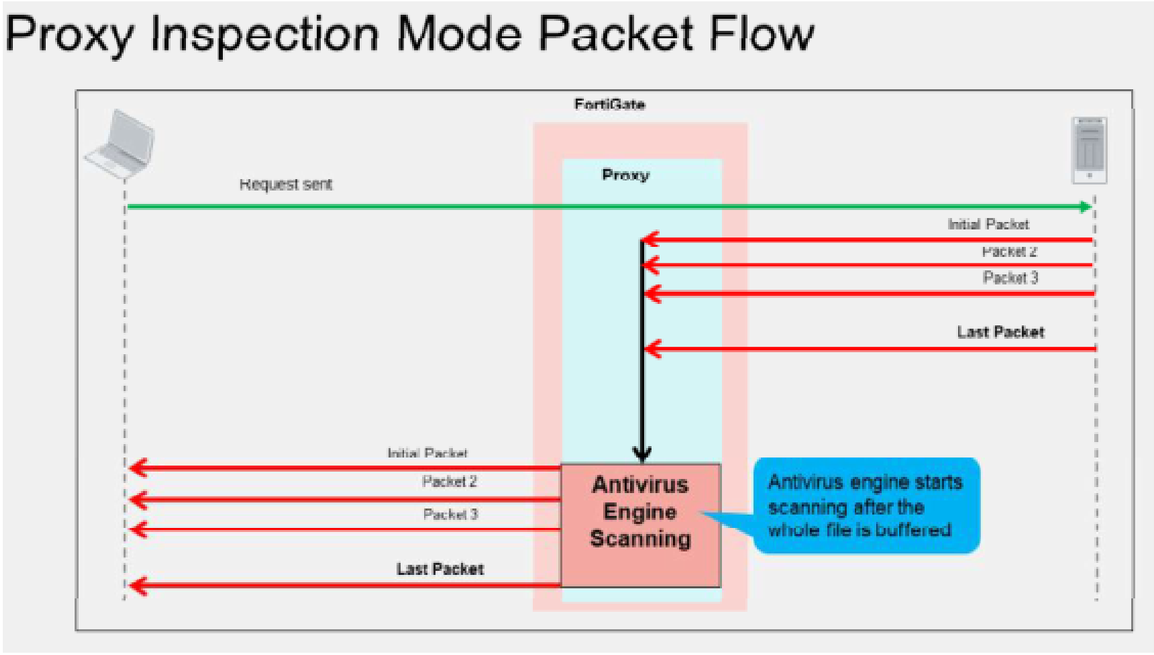
- High protection and accurate detection are required.
- You’re dealing with sensitive environments.
- The FortiGate device has strong hardware.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)



https://depi.gov.eg

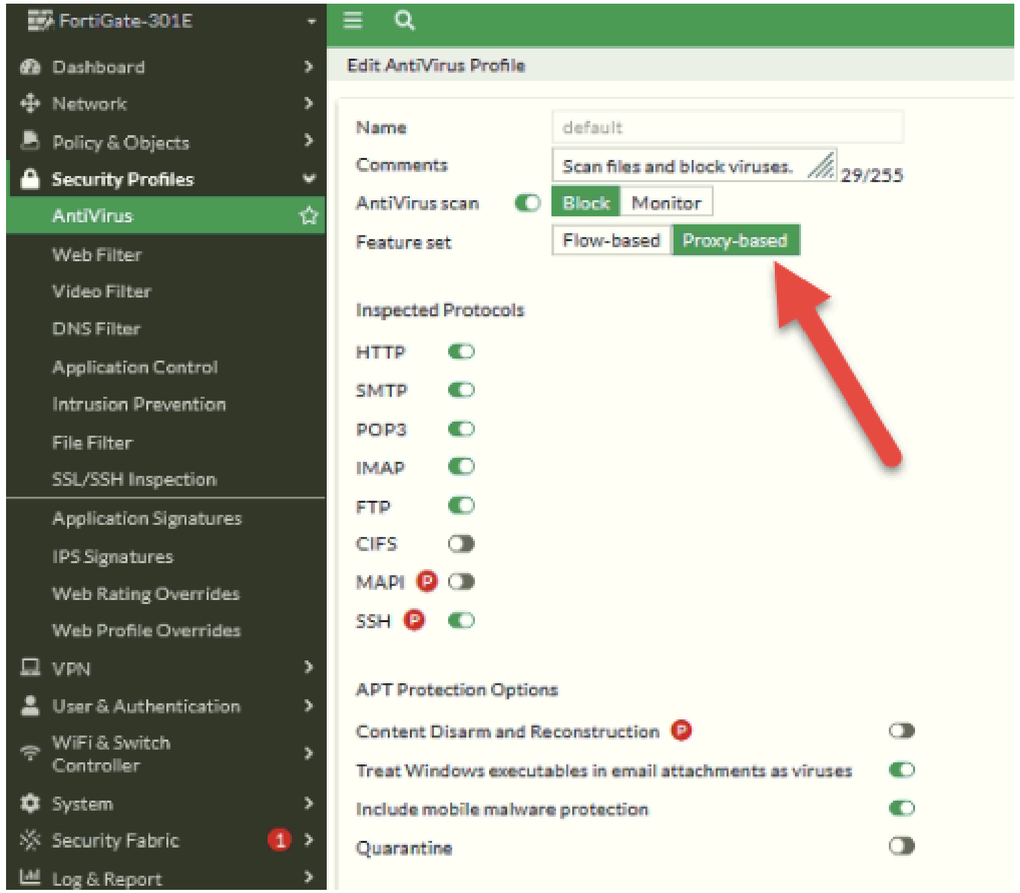
رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)

Configuration Profile



https://depi.gov.eg

رواد مصر الرقمية

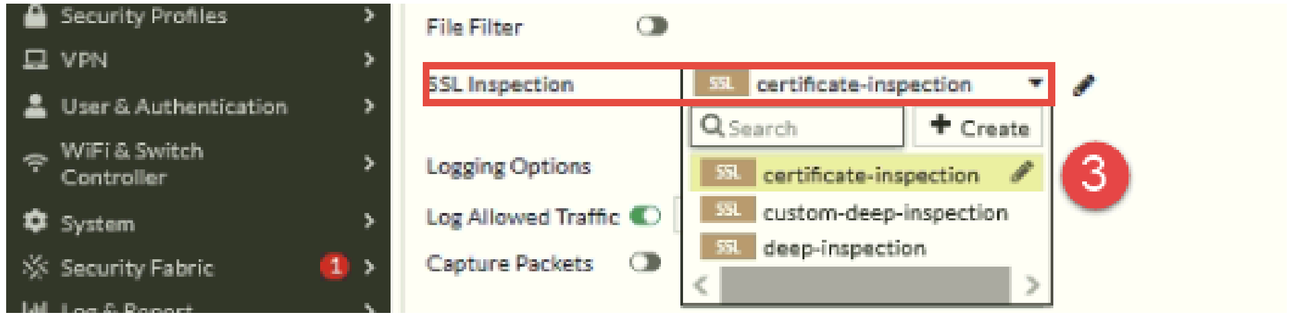
وزارة الاتصالات
وتكنولوجيا المعلومات

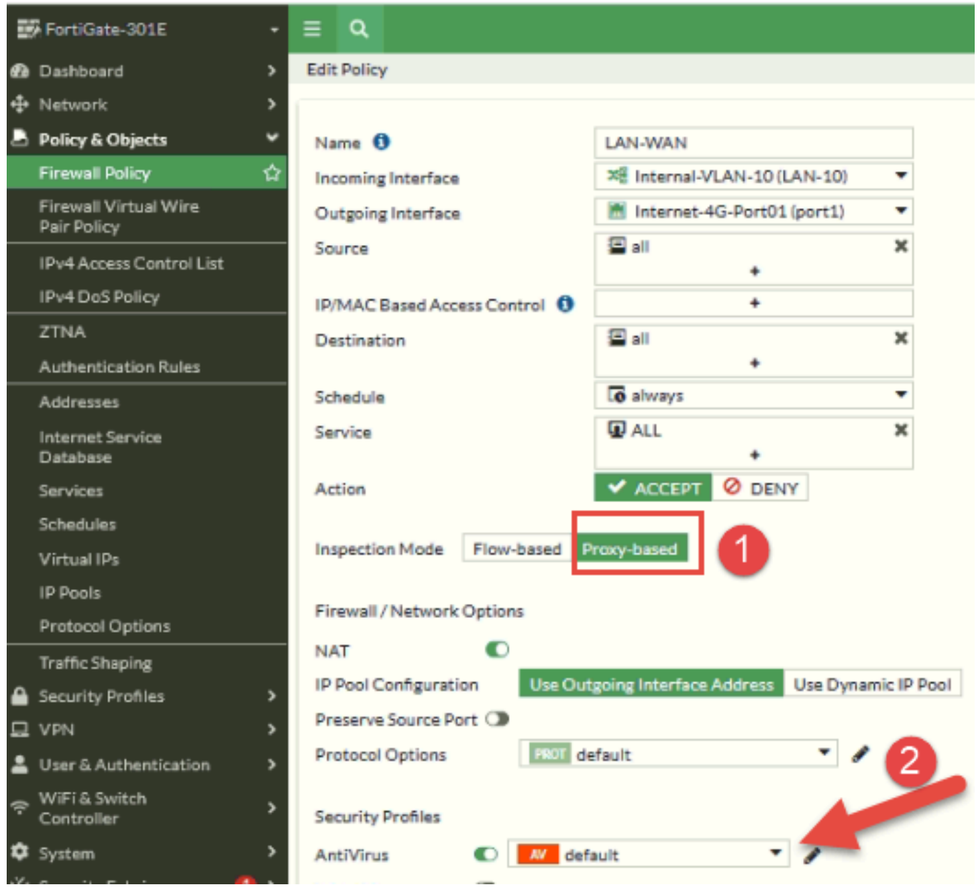
1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)

Configuration Policy

https://depi.gov.eg





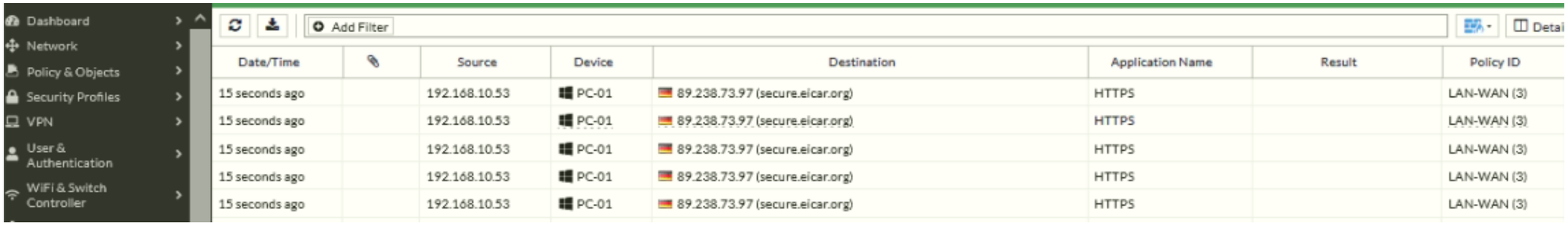
رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)

Logs & Monitoring



1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)

- _You Must Enable SSL Inspection When Using Antivirus Proxy Mode on FortiGate.
- Most internet traffic today is encrypted with HTTPS .
- Proxy Mode works like this:

"Open the file → Scan it → Deliver it safely" , This is impossible if the traffic is encrypted ,That’s why you must first decrypt the traffic.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

1.1 Antivirus Inspection Mode :

Proxy-based Inspection (Deep Mode)

https://depi.gov.eg

What happens if you use Proxy Mode without SSL Inspection?

❌ No scanning of files downloaded from Google Drive

❌ No scanning of Gmail attachments

❌ Malware inside HTTPS will pass without detection

❌ Web Filtering becomes limited

❌ Your protection will be very weak even if Proxy Mode is enabled.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles

2. Web Filtering

- Controls which websites users can access.
- Can block harmful, inappropriate, or time-wasting websites.
- Helps enforce company internet policies.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.1 Web Filter Inspection Mode :

Flow-based Inspection (Fast Mode)

✓ Fast
✓ Low CPU usage
✓ Basic URL filtering

How it works:

- Checks the website request quickly while traffic is passing through.
- Does not deeply inspect the full web content.

Best for:

- High-performance needs
- Low-spec FortiGate devices
- Simple URL filtering

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.1 Web Filter Inspection Mode :

Proxy-Based Mode

✓ Deep inspection

✓ More accurate filtering

✓ Can block specific pages, keywords, and content

How it works:

- FortiGate acts as a proxy (middle-man).
- It fully inspects the web page before allowing access.

Best for:

- Strong security requirements
- Content filtering and deep analysis
- Environments needing detailed web control

2.2 FortiGuard Category Filters:

Category Filters are groups of websites that share the same type of content.
Each website on the internet falls under one or more categories.

For example:

- Social Media , News , Gambling , Adult Content , Shopping ,Malware / Phishing , Cloud Storage , Job Search , Streaming Media & Education .

FortiGate uses FortiGuard’s global database to identify these categories.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.3 FortiGate Web Filter – Actions Explained

https://depi.gov.eg

Allow

✓ The user can open the website normally.
✓ No restrictions, no warnings.

Use when:

- The website category is safe.
- You want to give full access.

.

Monitor

✓ The user can access the website.
✓ FortiGate logs this activity (for reporting).
✓ No blocking.

Use when:

- You want to watch user activity without blocking.
- For analysis, reporting, or testing

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.3 FortiGate Web Filter – Actions Explained

https://depi.gov.eg

Block

❌The website is completely blocked.

❌The user sees a FortiGate "Blocked" page.

Use when:

- The website category is dangerous (Malware, Phishing).
- Not allowed (Adult, Gambling).
- Not needed at work (Social Media, Streaming).

Warning

⚠ The user sees a warning page first.

⚠ They must click "Proceed" to continue.

✔ Access is allowed only after user confirmation.

Use when:

- You want to warn users about risky categories without blocking.
- Example: Social media or shopping — not harmful, but distracting.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.3 FortiGate Web Filter – Actions Explained

Authenticate

🔐 The user must enter login credentials first.

✔️ If authentication passes → access allowed

❌ If user fails → access denied

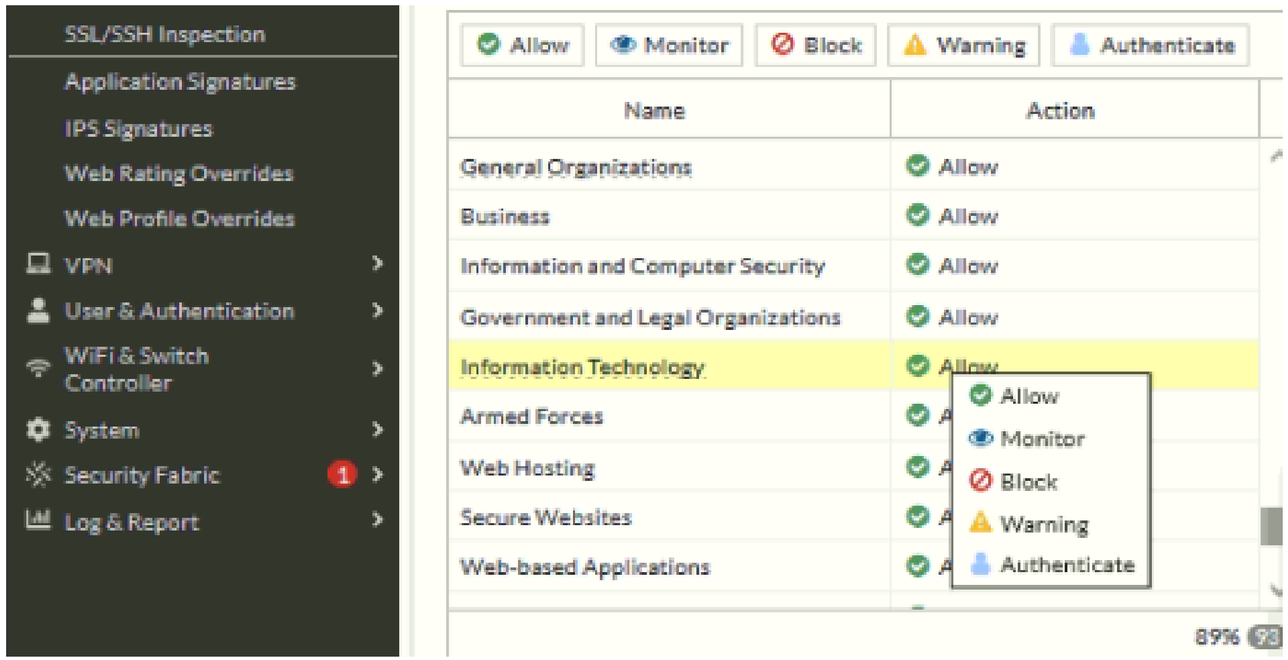
Use when:

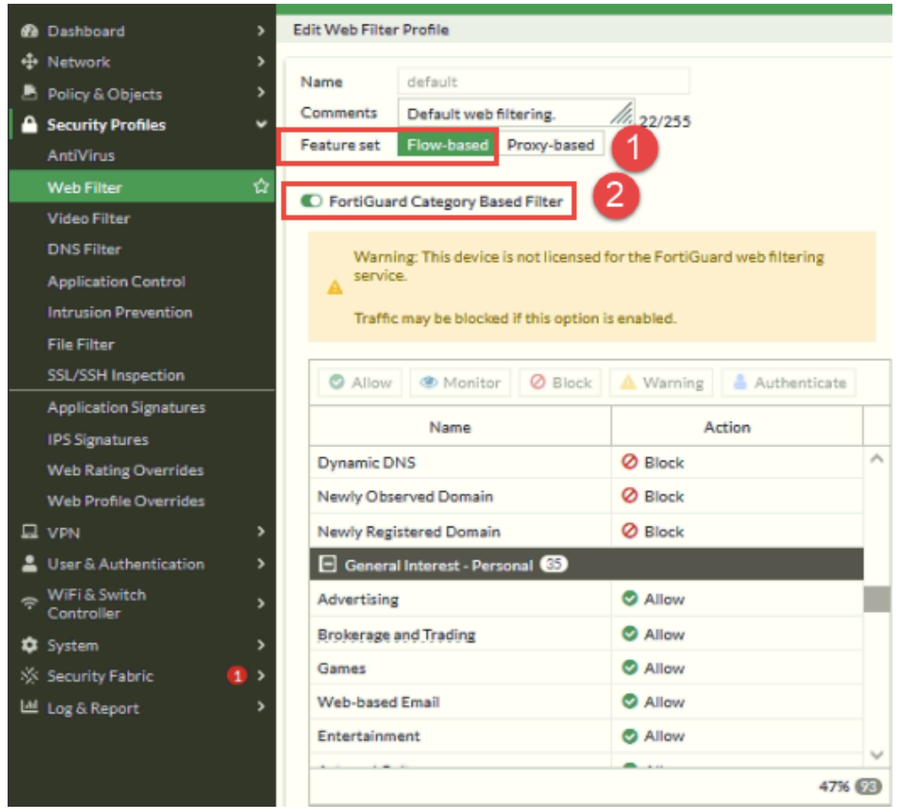
- You want only specific users to access a certain category.
- Example:
  - Managers can access Social Media
  - Normal employees cannot
- Or giving access to admins only.

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

2.3 FortiGate Web Filter



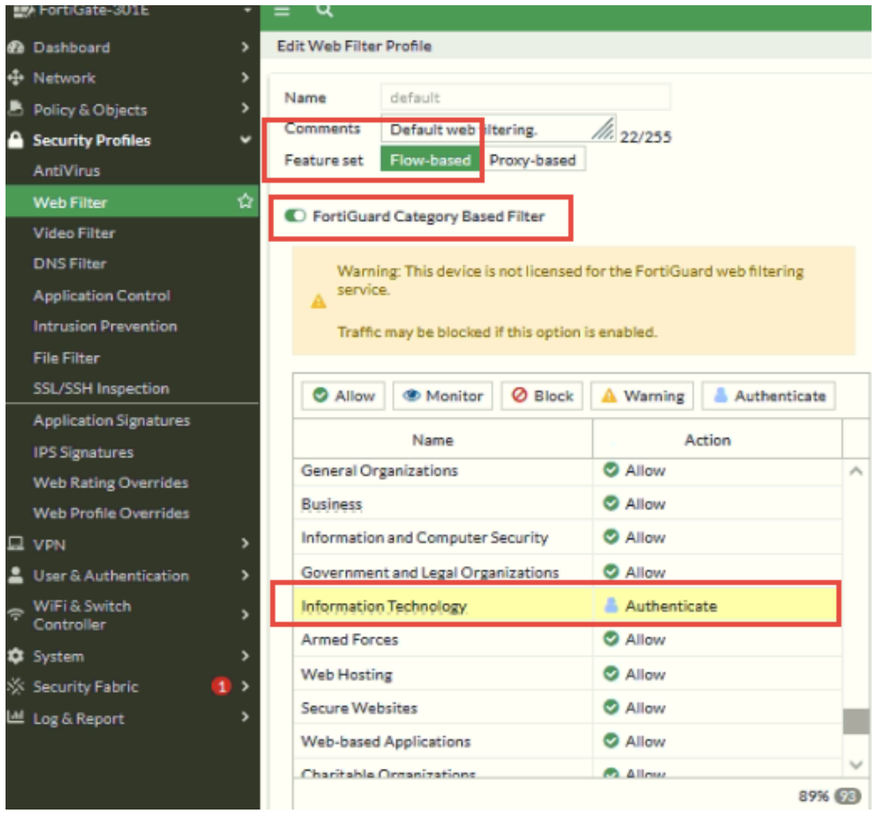


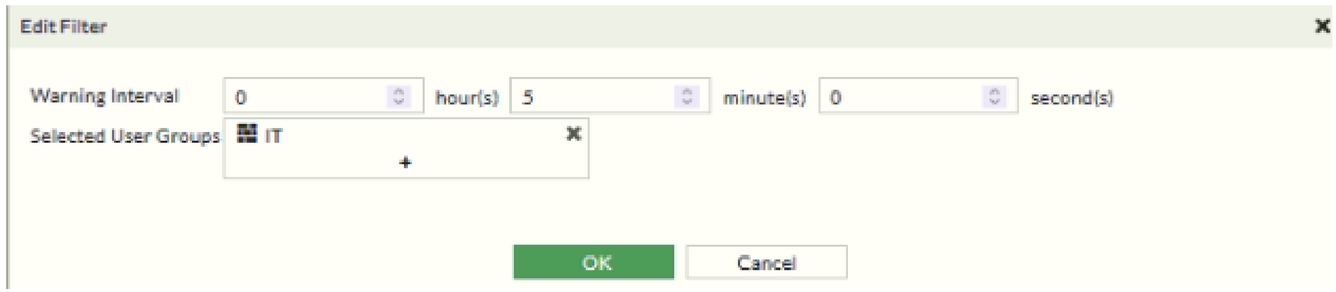
https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

2.3 FortiGate Web Filter - Authentication Required



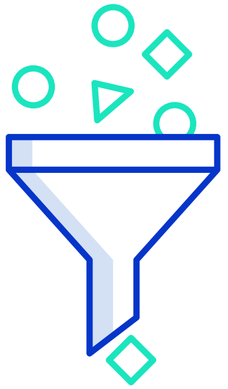


https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.4 Web Rating Override:



Web Rating Override allows you to manually change the category of a website inside your FortiGate.

Use Case :

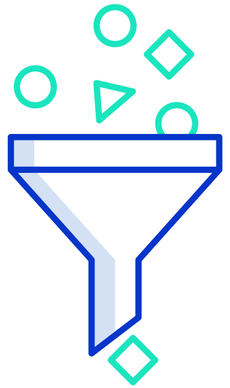
1- When FortiGuard categorizes a website incorrectly
ex : A business site is categorized as "Shopping" —
You can override it to "Business

2- When you want special rules for specific websites
ex : Allow YouTube for managers only, even if the category is blocked

3-When a new website is not categorized yet.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات



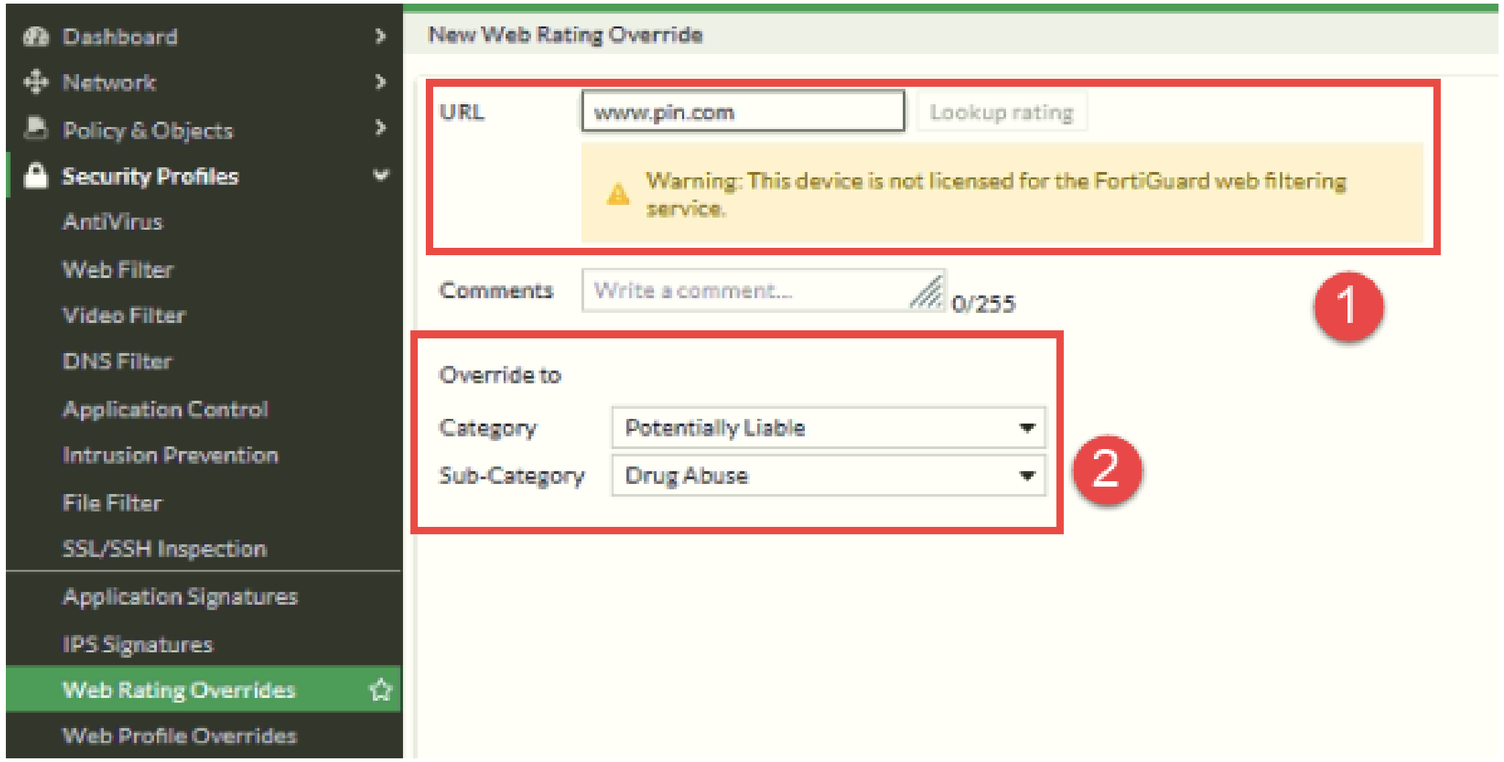
2.4 Web Rating Override:

- You can override URL, domain, or IP .
- Overrides take priority over FortiGuard categories .
- very useful for custom business needs
- Helps fix wrong or uncategorized websites

رواد مصر الرقمية

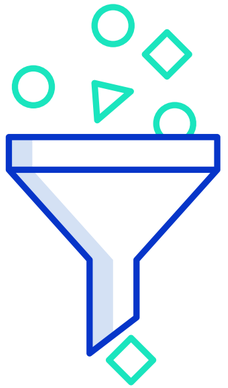
وزارة الاتصـــــالات
وتكنولوجيا المعلومات

2.4 Web Rating Override:



رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات



2.5 URL Filter :

URL Filter allows you to Allow, Block, or Monitor specific websites or domains — regardless of their FortiGuard category.

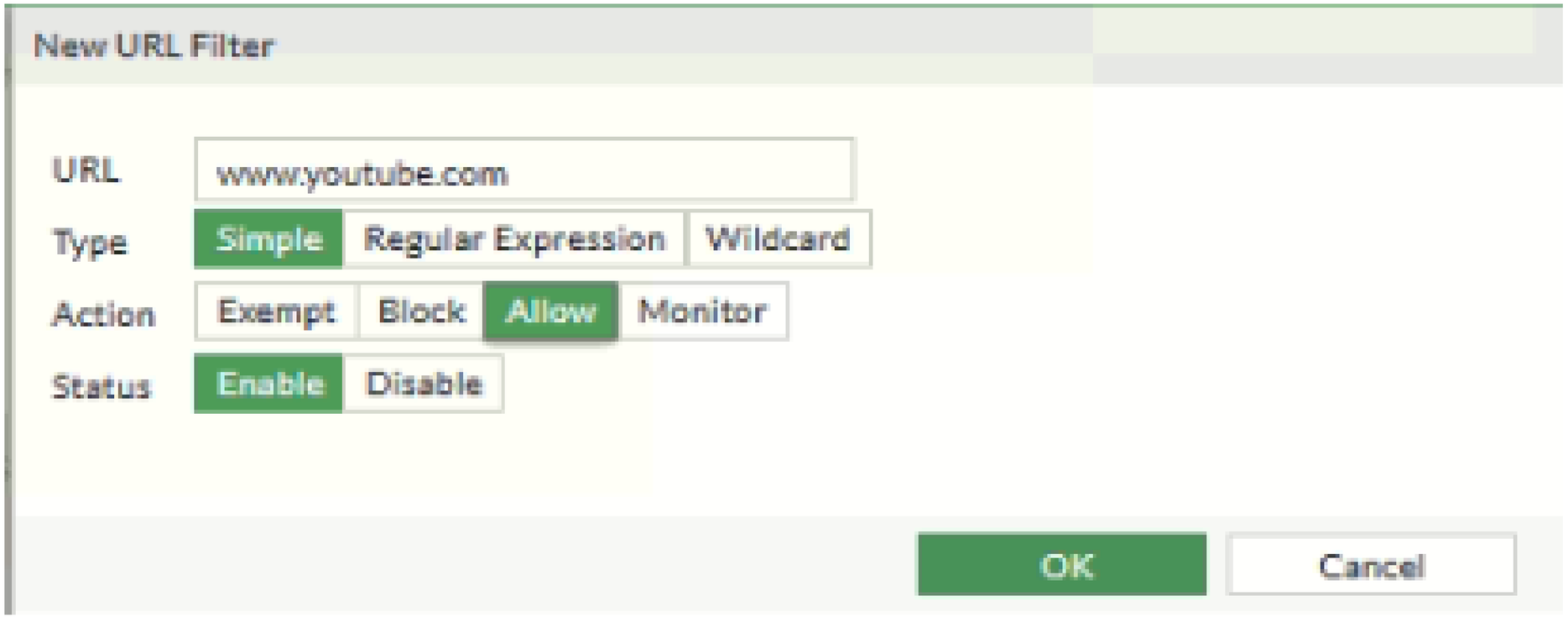
Actions You Can Apply

- Allow → Let users access
- Block → Deny access
- Monitor → Allow but log
- Exempt → Skip inspection (bypass)
-

Simple Example

- Block: youtube.com
- Allow: portal.company.com
- Wildcard: *.ads.com → block all ad networks

2.5 URL Filter :

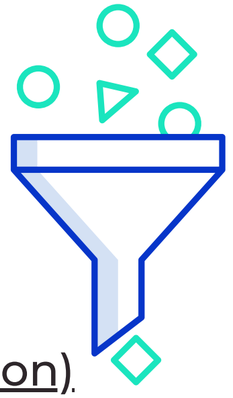


URL Filter has higher priority than FortiGuard categories — but lower than Web Rating Override.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

2.6 FortiGate Web Filter – SSL Certificate Inspection



https://depi.gov.eg

Certificate Inspection (Basic / Simplified)

- Only inspects the website's SSL Certificate.
- Checks:
  - Is the website trusted?
  - Is the certificate valid?
- Very limited: does not see the content or files inside HTTPS.

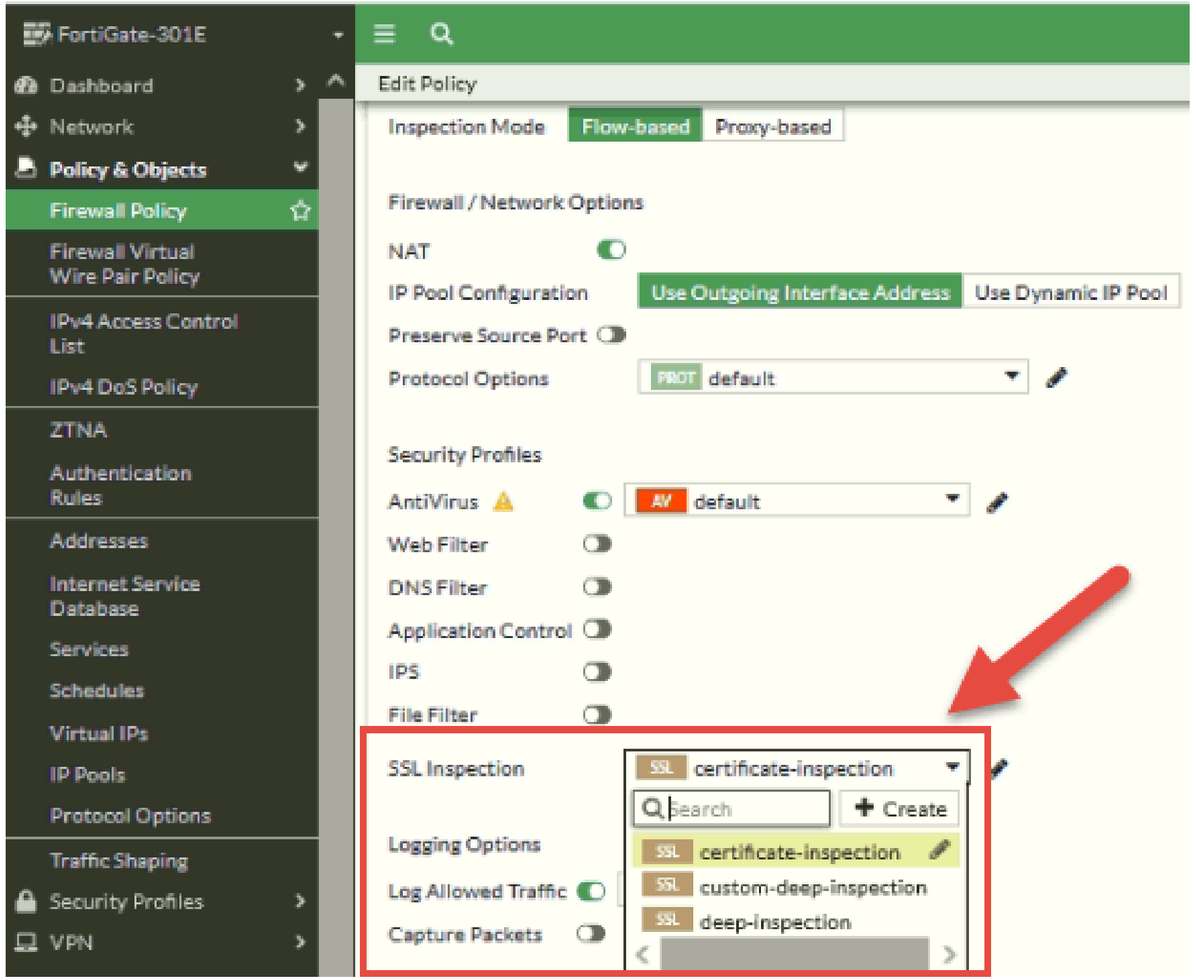
Deep Inspection (Full SSL Inspection)

- Decrypts the traffic completely.
- Allows:
  - Web Filtering (Categories)
  - Antivirus Scanning
  - Application Control
- Provides full protection for HTTPS websites.

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

2.6 FortiGate Web Filter – SSL Certificate Inspection



https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles

3-Application Control

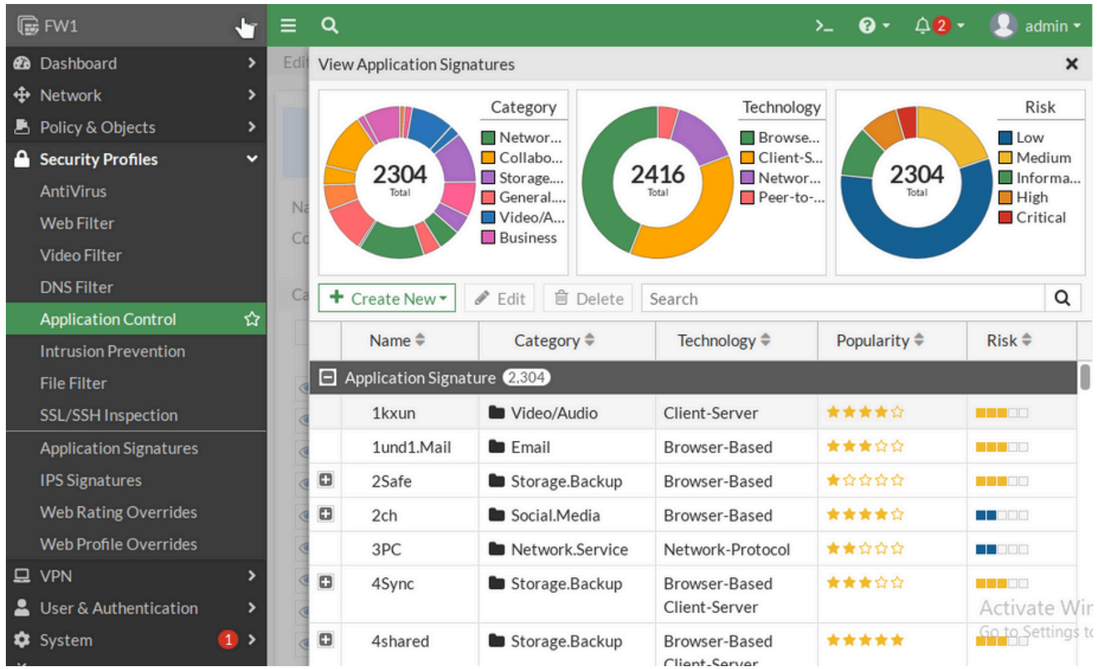
- Identifies and controls applications running on the network.
- You can block or allow specific apps like: Facebook , Torrent & WhatsApp
- Helps reduce risk and bandwidth misuse.
- Application Contorl use the IPS engine to scan traffic against application pattern .

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

3.1 List Of Application Signatures

https://depi.gov.eg

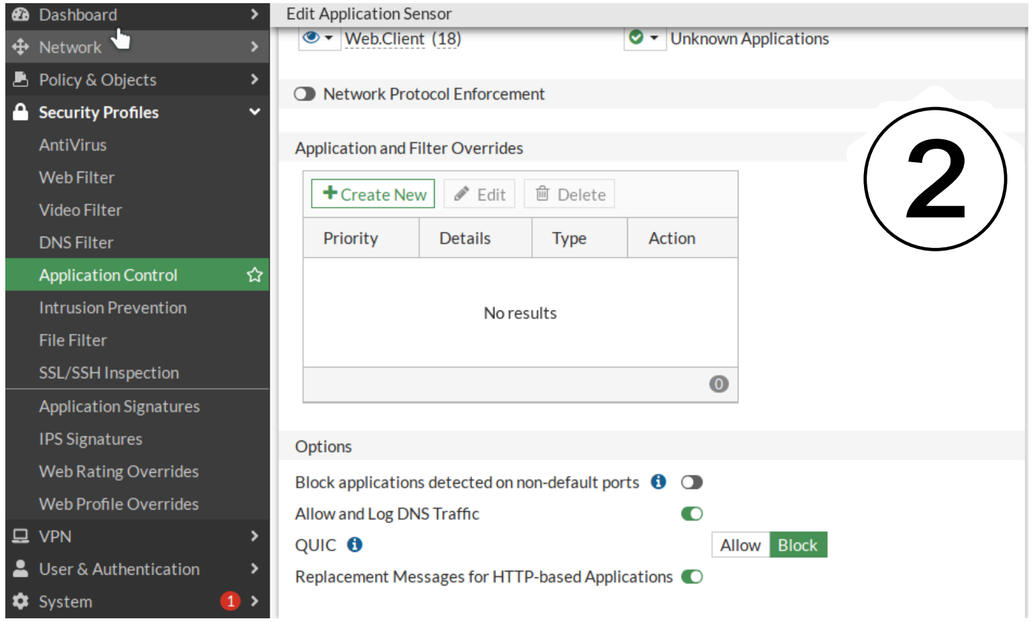


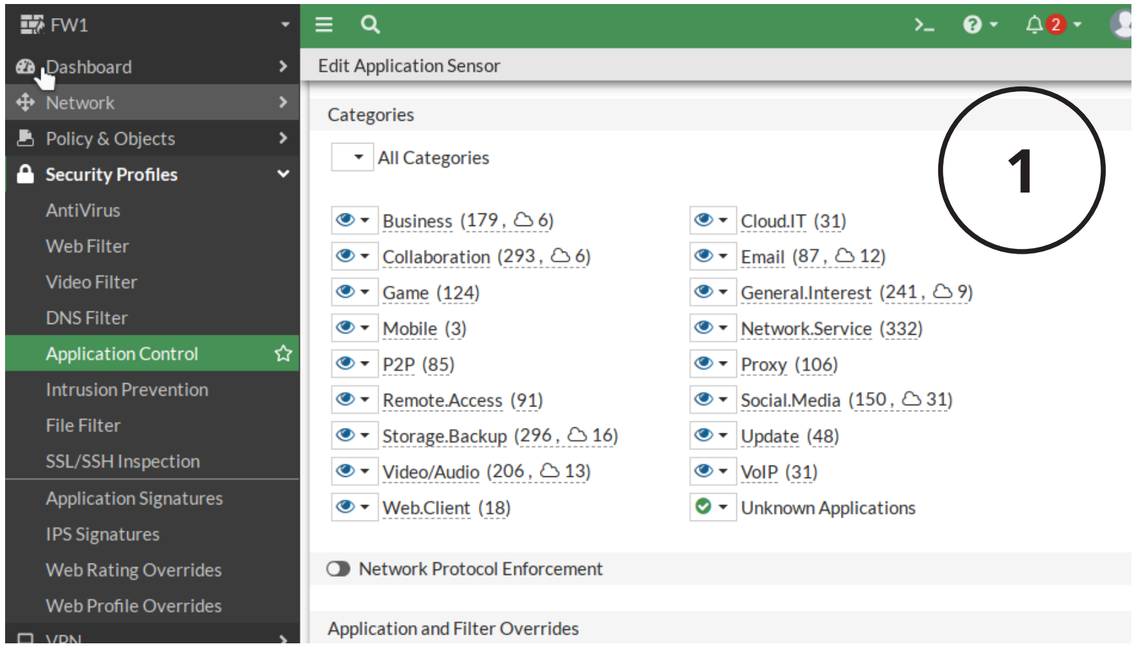
رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

3.2 Application Control Inspection

https://depi.gov.eg

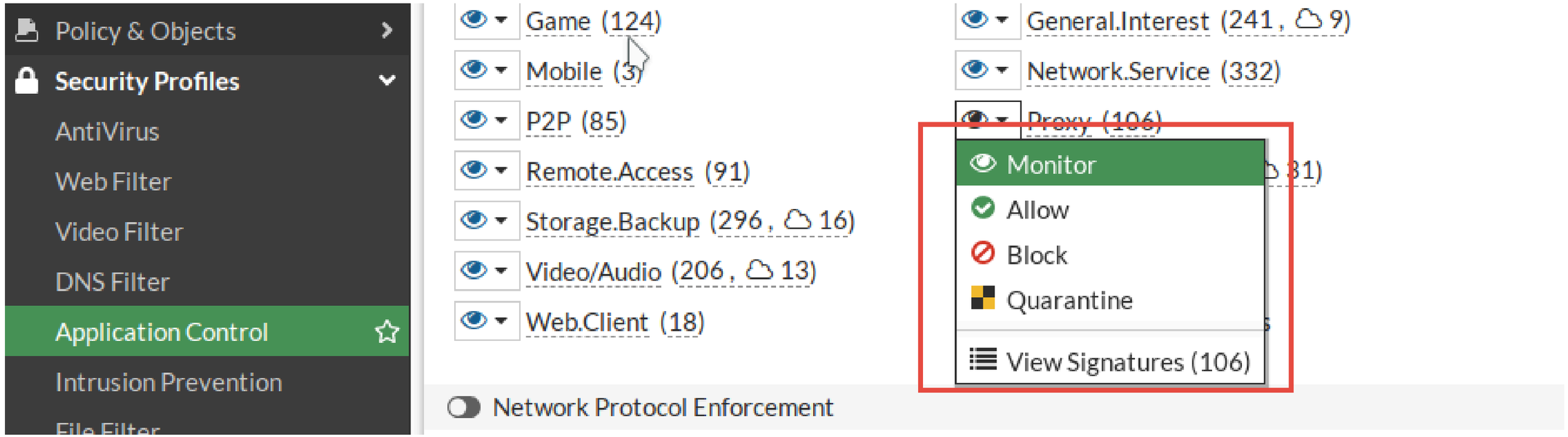




رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

3.3 Application Control Filter Actions



رواد مصر الرقمية

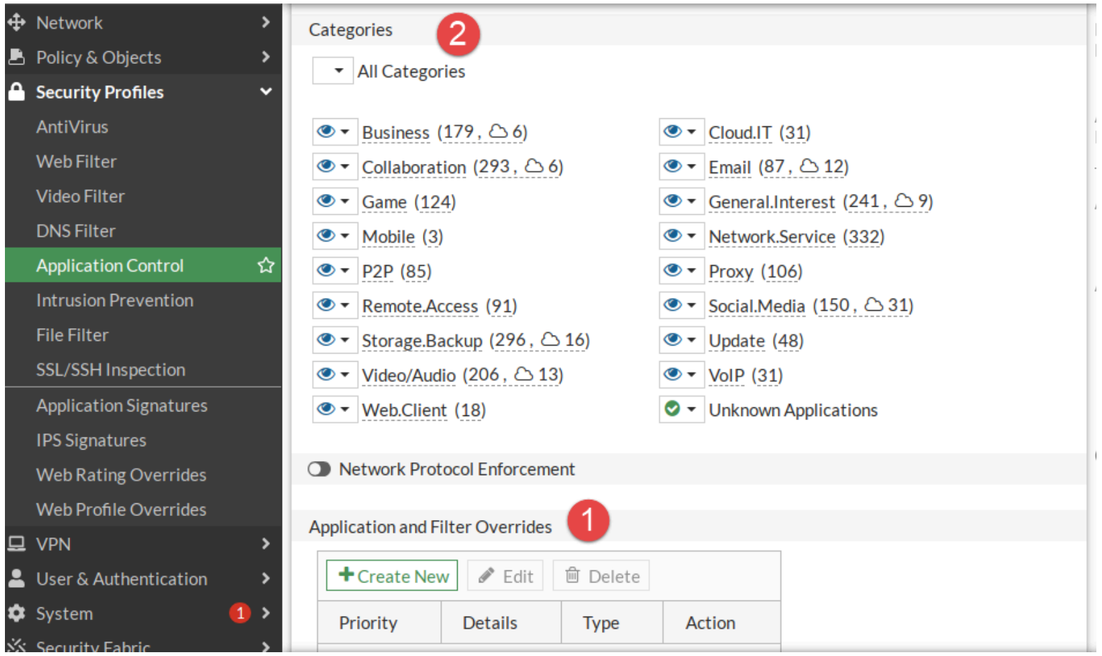
وزارة الاتصالات وتكنولوجيا المعلومات

3.4 Application Control Scanning Order

1- Application .

2- Filter .

3- Fortiguard Category .



https://depi.gov.eg

رواد مصر الرقمية

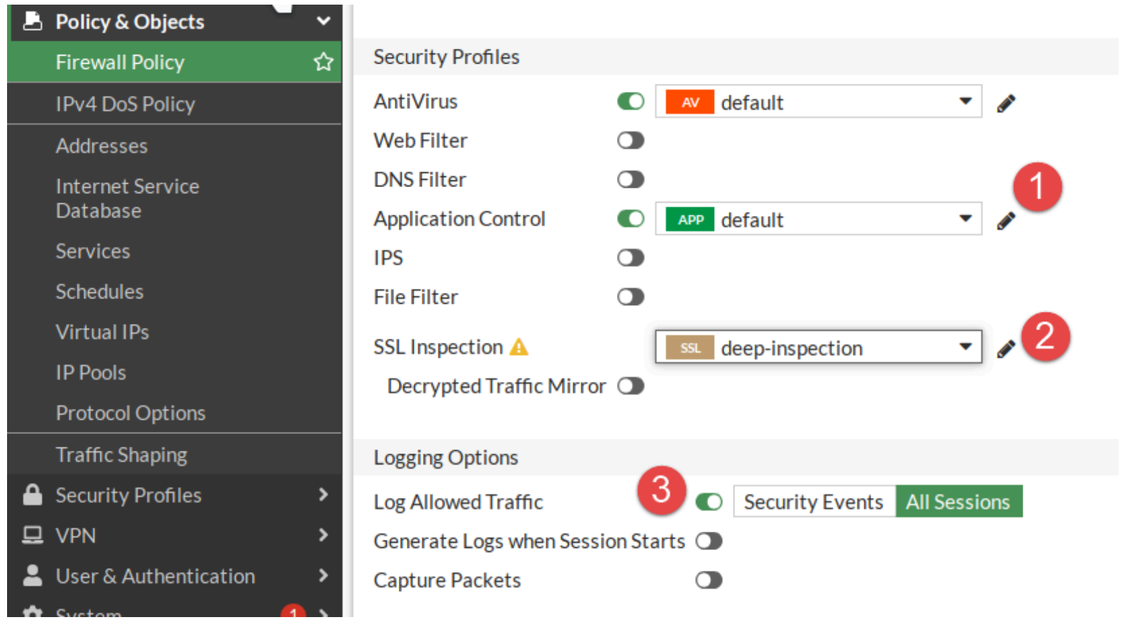
وزارة الاتصالات وتكنولوجيا المعلومات

3.5 Application Control in Policy

1- Select Application Contorl Profile.

2- SSL using deep inspection .

3- Log Allowed traffics ..



3.6 Application Control Bandwidth limit by Traffic Shaper

What is a Traffic Shaper?

- Imagine your network is a highway, and the data passing through it are cars.
- A Traffic Shaper is like a traffic officer:
  - It decides who can go how fast
  - Slows down some traffic if needed
  - Prevents congestion when the highway is busy .

In short: It’s a tool on the firewall that controls the speed of internet traffic for different users or applications.

3.6 Application Control Bandwidth limit by Traffic Shaper

Role of Traffic Shaper in Bandwidth Limit

- Bandwidth = the width of the road / maximum available internet speed.
- Bandwidth Limit = the maximum speed allowed for each service or user.

Practical Example:

- You have 50 Mbps internet for the company.
- Employee A / VoIP service → needs 5 Mbps guaranteed so calls don’t drop.
- Other employees / big downloads → can use the rest as needed.

3.6 Application Control Bandwidth limit by Traffic Shaper

Here, the Traffic Shaper does

- Distributes the speed among users or apps according to policies .
- Prevents one application (like a big file download) from using all the bandwidth .
- Ensures network stability and quality for critical services .

Guaranteed vs Max Bandwidth:

- Guaranteed → the speed reserved for important traffic (VoIP, critical apps)
- Max → the maximum speed any user or service can take.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

3.6 Application Control Bandwidth limit by Traffic Shaper

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

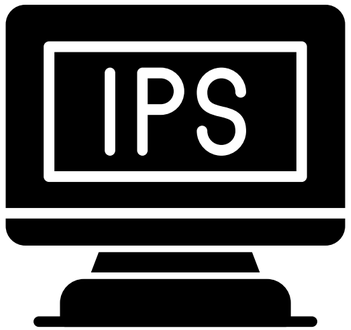
Key Types of Security Profiles

4- IPS (Intrusion Prevention System)

- Detects and blocks attacks targeting: Servers , Applications & Network devices
- Protects from exploitation of vulnerabilities.
- IPS = a system that detects and prevents intrusions.
- Its main purpose is to protect the network from attacks before they reach devices and servers.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات



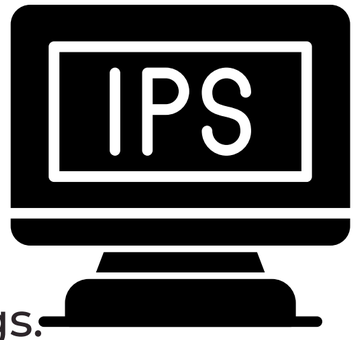
4.1 IPS Work

How IPS Works

1. Traffic Monitoring
   - FortiGate monitors all traffic entering or leaving the network.
2. Pattern Matching / Signatures
   - Compares the traffic against a database of known attack signatures.
   - Example: SQL Injection, Cross-Site Scripting, Port Scans, Malware Traffic.
3. Action
   - If the traffic is suspicious → FortiGate blocks, drops, or logs it.
   - Different actions can be applied for each type of threat.

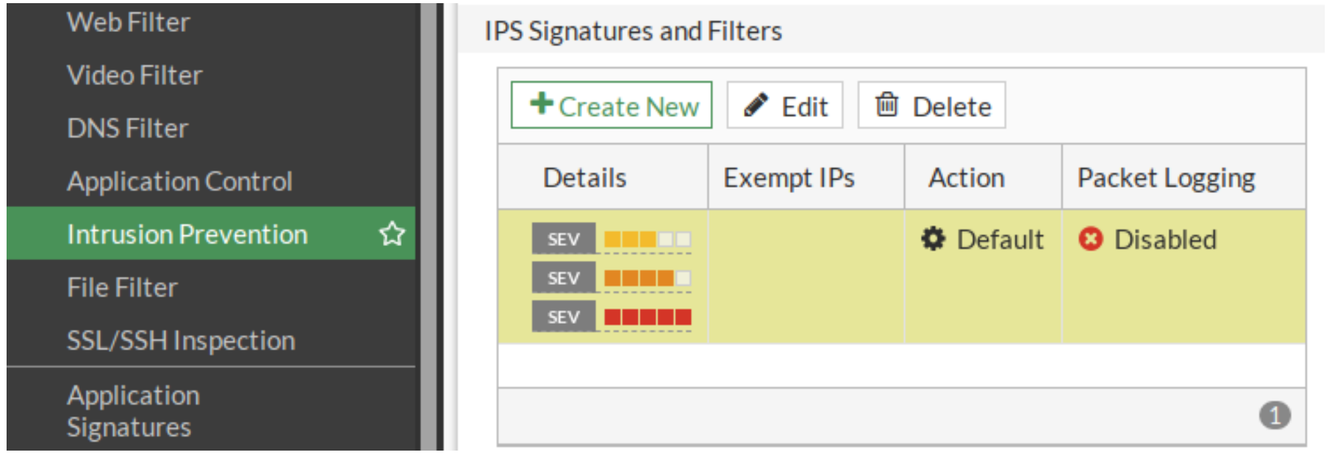
رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات



4.2 IPS Sensors

An IPS Sensor is a security profile that contains all IPS rules and settings.
It includes filters, signatures, and actions used to detect and block network attacks.



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

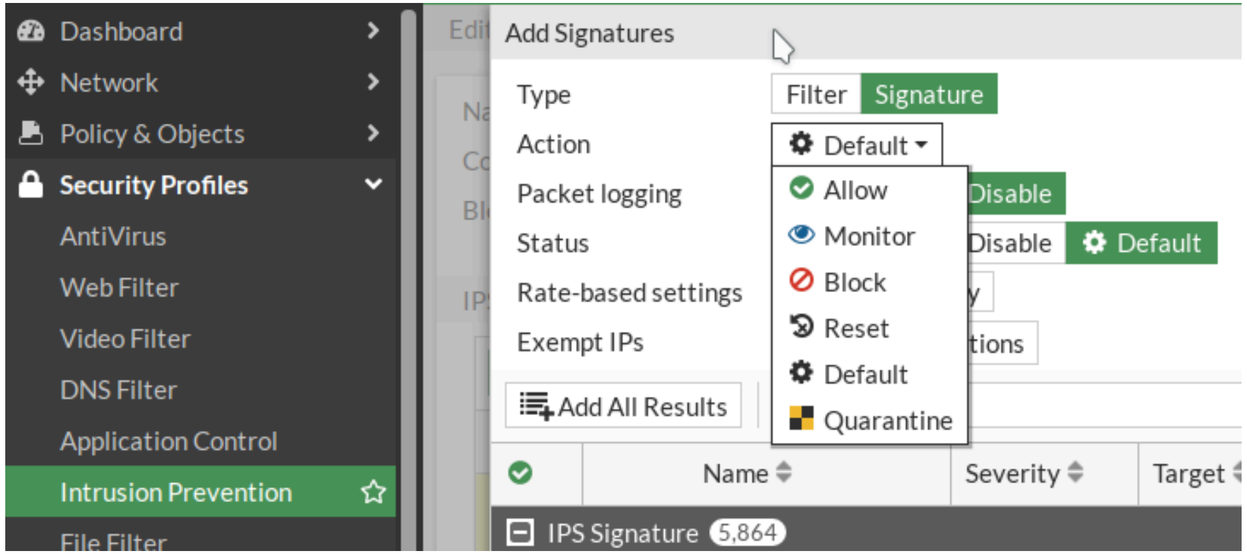
4.3 IPS Actions :

Allow

- Allows the traffic even if it matches an IPS signature.

Use case:

Testing or low-risk signatures.



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

https://depi.gov.eg

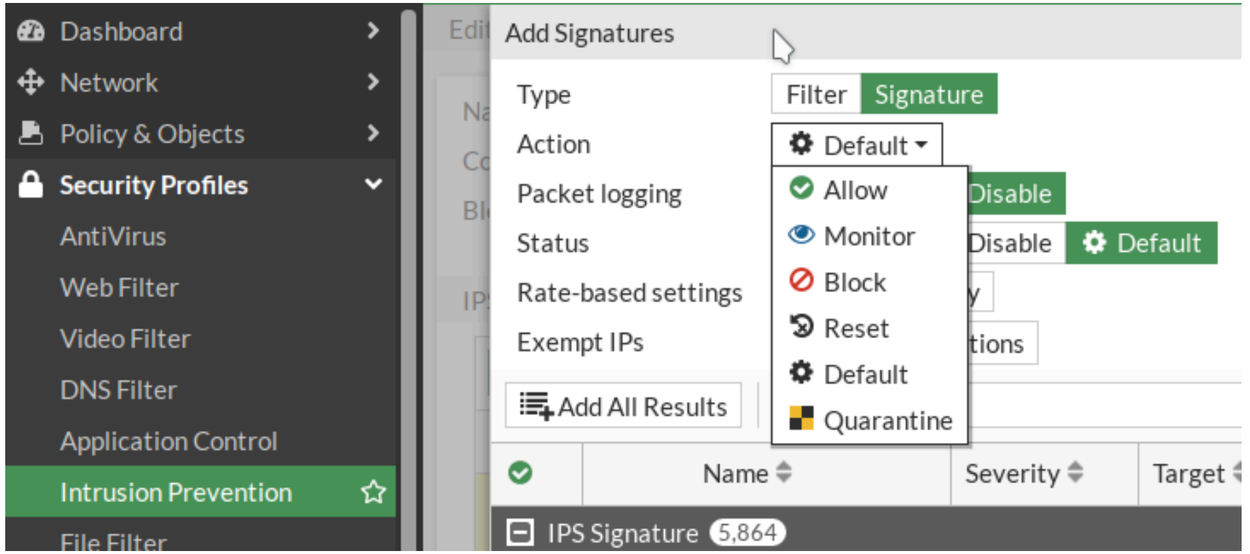
4.3 IPS Actions :

Monitor

- Allows traffic but logs the event when a threat is detected.

Use case:

Monitoring new signatures before blocking .

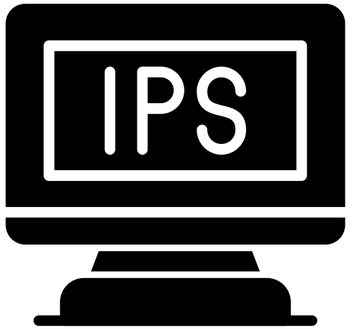


رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

https://depi.gov.eg

4.3 IPS Actions :

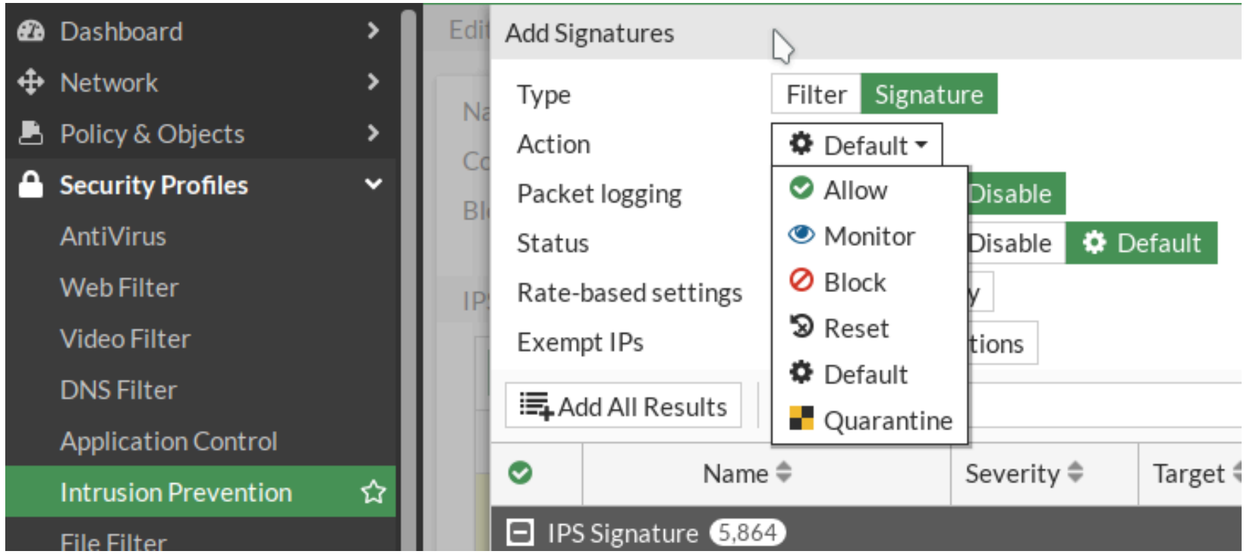


Block

- Blocks the traffic completely if it matches the IPS signature

Use case:

Critical & High severity attacks .



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

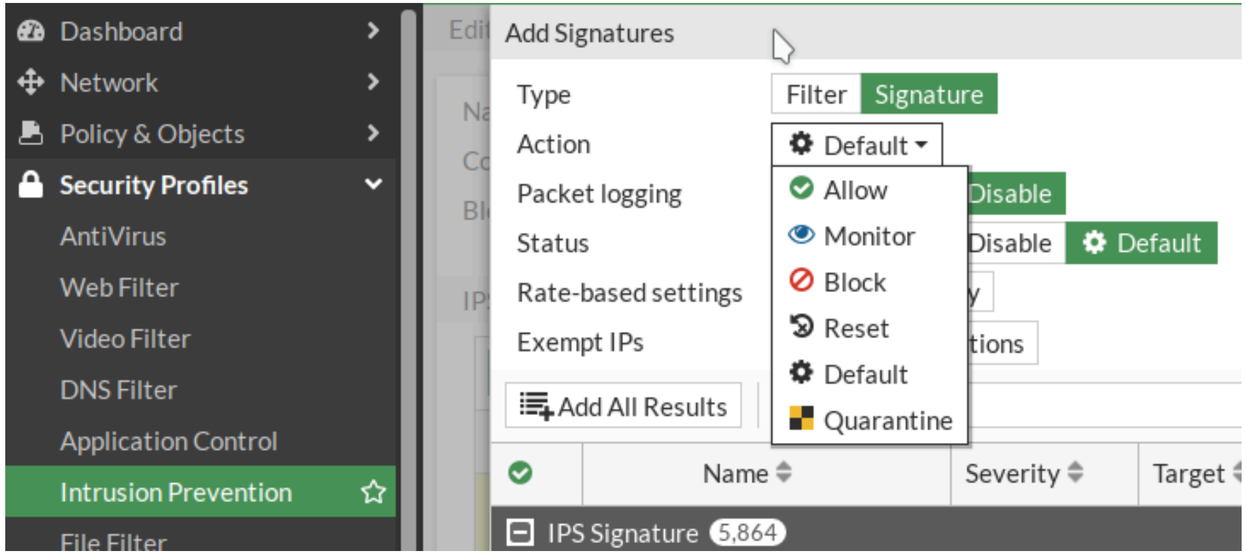
4.3 IPS Actions :

Reset

- Drops the connection and sends a TCP Reset to both sides.

Use case:

- Stopping attacks that depend on long-lived sessions .



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

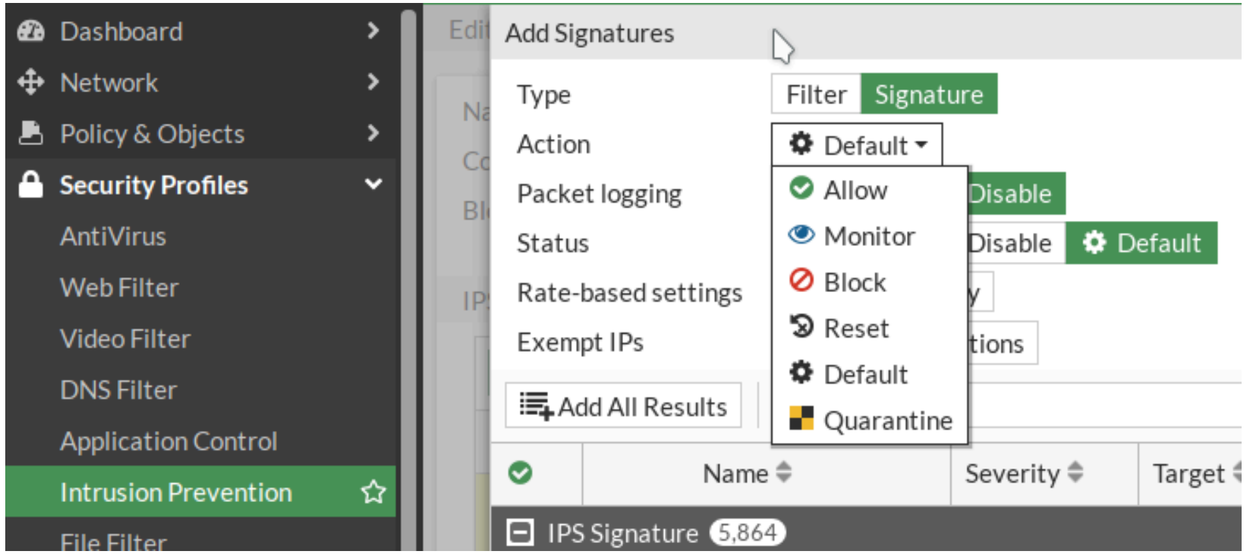
4.3 IPS Actions :

Default

- Drops the connection and sends a TCP Reset to both sides.

Use case:

- Stopping attacks that depend on long-lived sessions .



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

https://depi.gov.eg

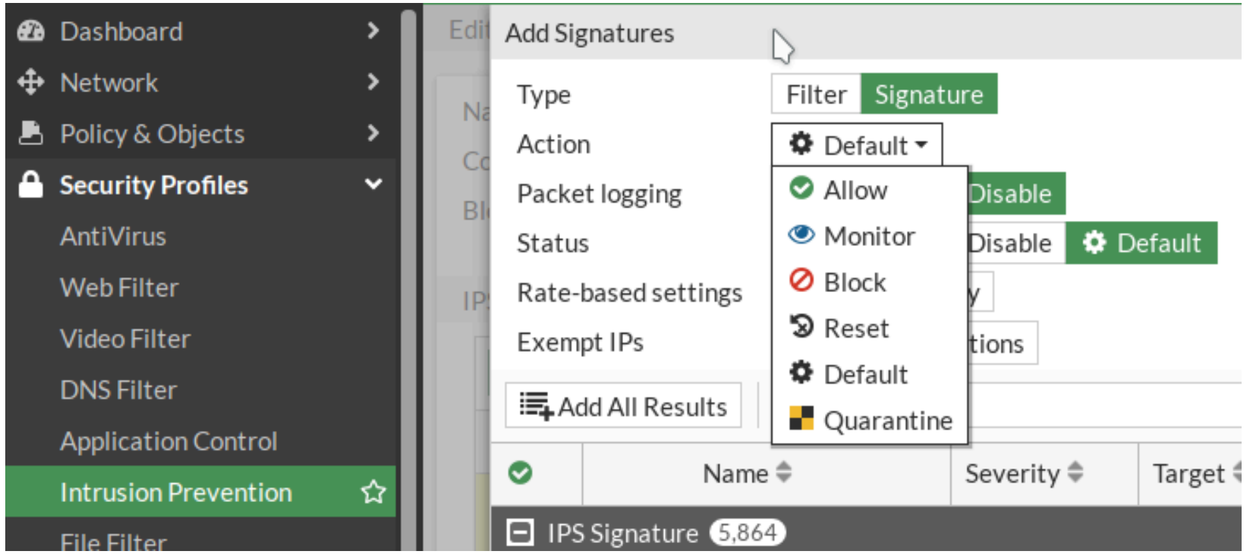
4.3 IPS Actions :

Quarantine

- Blocks the source IP for a period of time (temporary ban).

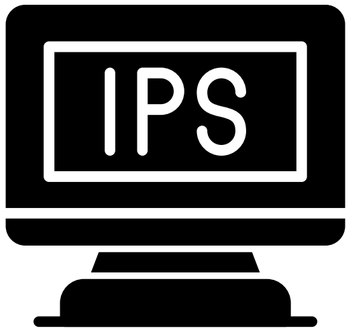
Use case:

- Repeated attacks, brute force attempts, or infected hosts inside the LAN .



رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

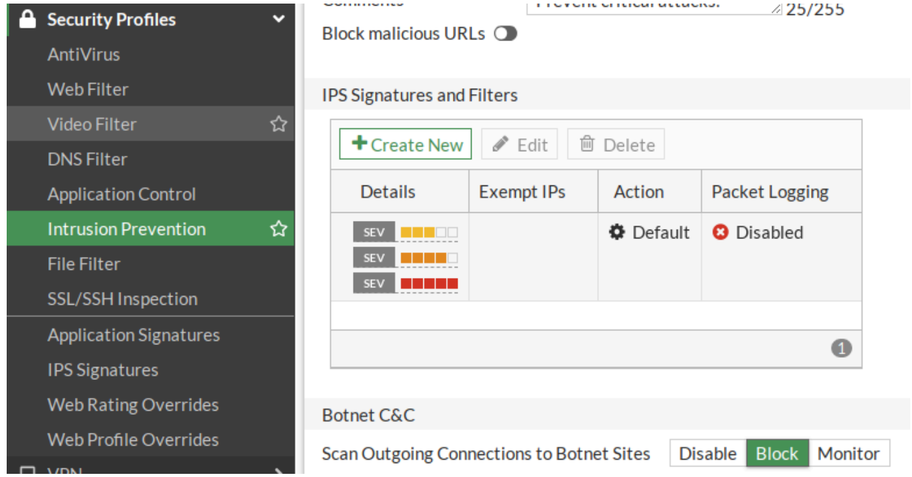


4.4 A Botnet C&C

https://depi.gov.eg

A Botnet C&C (Command and Control) is a server used by hackers to control infected devices.

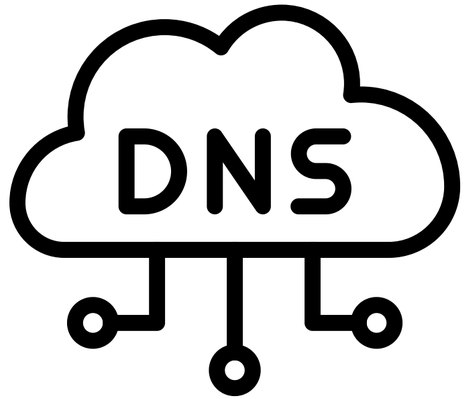
- A Botnet = a group of compromised devices (PCs, servers, IoT).
- C&C Server = the place where the hacker sends commands.



رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles



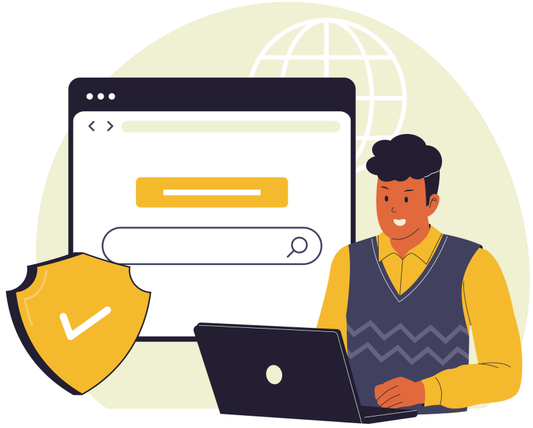
5- DNS Filter

- Blocks malicious domains before the connection happens.
- Protects against phishing, botnets, and C&C attacks.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles



6-SSL Inspection

- Allows FortiGate to inspect encrypted traffic (HTTPS).
- Helps detect threats inside encrypted connections.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Why Security Profiles Are Important ?

- They provide deep inspection.
- Protect against modern threats.
- Ensure compliance with security policies.
- Reduce risk of viruses, attacks, and data leakage.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

How Security Profiles Work Together ?

- Traffic hits the firewall.
- Firewall policy either allows or denies the traffic.
- If allowed, assigned Security Profiles start checking:
- Is the website safe?
- Is the file clean?
- Is the application allowed?
- Is the domain malicious?
- If something suspicious appears → FortiGate blocks it.

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

THANK YOU

https://depi.gov.eg

› End Slide