



# PROJECT

## ADVANCED FORTIGATE SECURITY PROFILES

P R E S E N T A T I O N

وزارة الاتصالات  
وتقنيات جيا المعلومات



› Start Slide



# Our Great Team

---

Mohamed Abdelaal

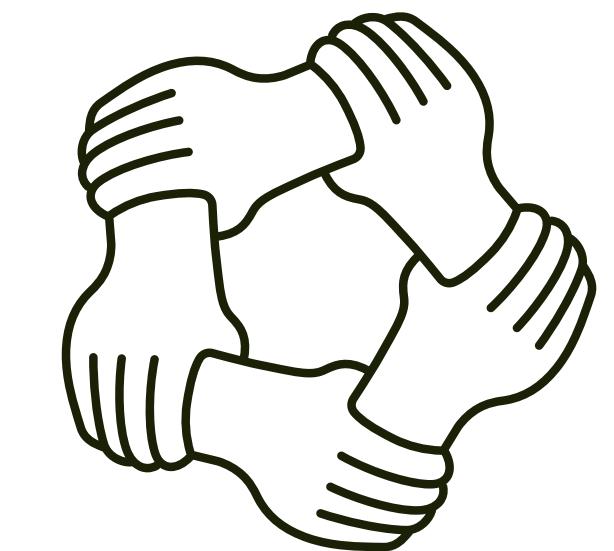
Eyad Mahmoud

Arwa Essam

Filopateer Atef

Youssef Yasser

وزارة الاتصالات  
وتقنيات جيا 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.



## 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.



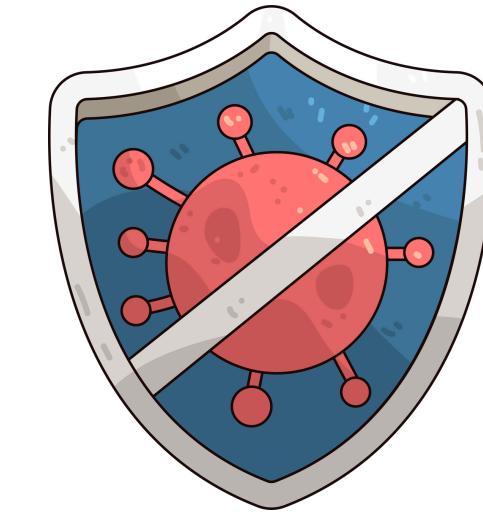
وزارة الاتصالات  
وتقنيات جيا المعلومات



## 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.



وزارة الاتصالات  
وتقنيات جيا 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.

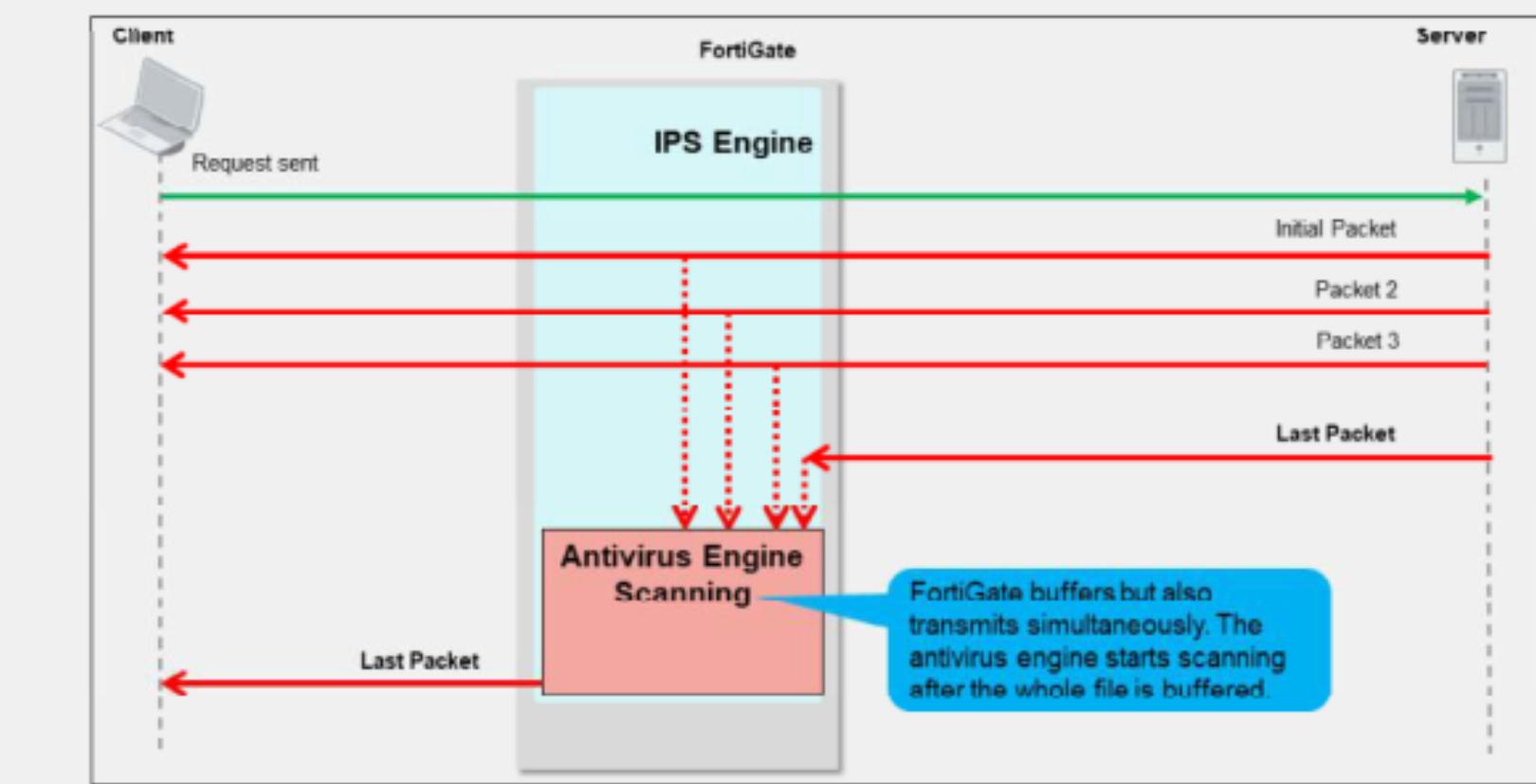


وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Flow-based Inspection (Fast Mode).

Flow-Based Inspection Mode Packet Flow





وزارة الاتصالات  
وتكنولوجيا المعلومات



## 1.1 Antivirus Inspection Mode : Flow-based Inspection (Fast Mode).

<https://depi.gov.eg>

### Configuration Profile

The screenshot shows the FortiGate 301E configuration interface. On the left is a navigation sidebar with options like Dashboard, Network, Policy & Objects, Security Profiles, AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention, File Filter, SSL/SSH Inspection, Application Signatures, IPS Signatures, Web Rating Overrides, and Web Profile. The 'Security Profiles' option is expanded, and 'AntiVirus' is selected. To the right is the 'Edit AntiVirus Profile' screen. It has fields for Name (default), Comments (Scan files and block viruses. 29/255), and Feature set (with 'Flow-based' selected, indicated by a red arrow and the number 1). Other tabs in the Feature set section include 'Proxy-based'. Under 'Inspected Protocols', options for HTTP, SMTP, POP3, IMAP, FTP, and CIFS are listed with their status. At the bottom are sections for APT Protection Options, including 'Treat Windows executables in email attachments as viruses' and 'Include mobile malware protection'.



## 1.1 Antivirus Inspection Mode : Flow-based Inspection (Fast Mode)

<https://depi.gov.eg>

FortiGate-301E

Edit Policy

Name: LAN-WAN

Incoming Interface: Internal-VLAN-10 (LAN-10)

Outgoing Interface: Internet-4G-Port01 (port1)

Source: all

IP/MAC Based Access Control: all

Destination: all

Schedule: always

Service: ALL

Action:  ACCEPT  DENY

Inspection Mode: **Flow-based**  Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration:  Use Outgoing Interface Address  Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROT default

Security Profiles: AV default

AntiVirus: AV default



## **بيانات الاتصال وتقنيات جيأ المعلومات**



# **1.1 Antivirus Inspection Mode :**

## **Flow-based Inspection (Fast Mode).**

# Logs & Monitoring



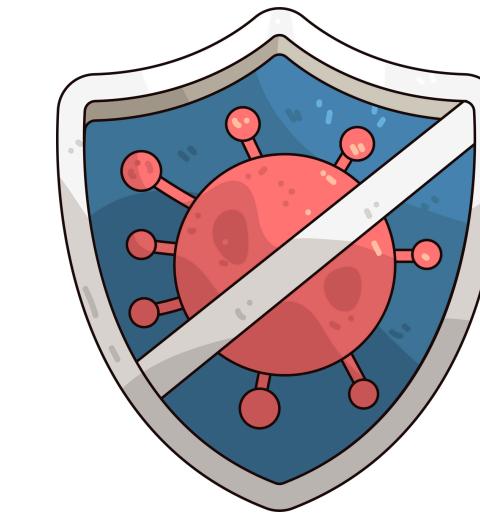
وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode :

### Proxy-based Inspection (Deep Mode)

Deep – More Accurate – Full Inspection

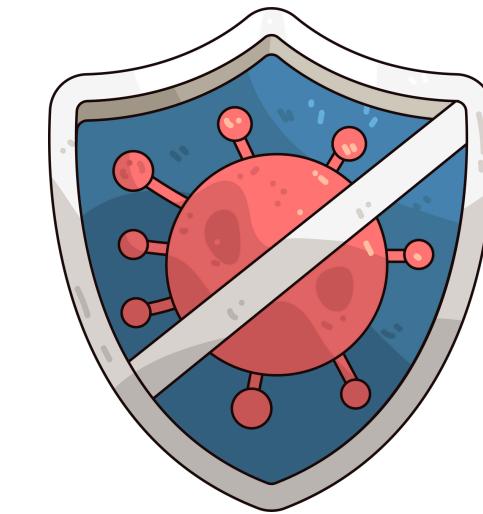


- Acts as a proxy between the user and the internet.
- Temporarily stores part of the traffic and performs full content inspection.
- Higher accuracy and detection rate.
- Consumes more CPU and RAM than Flow-based.



## 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.

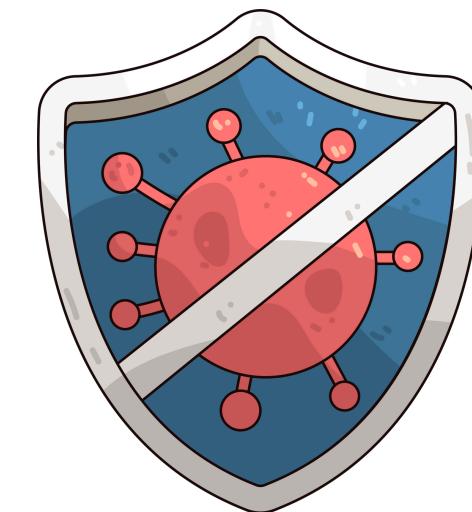
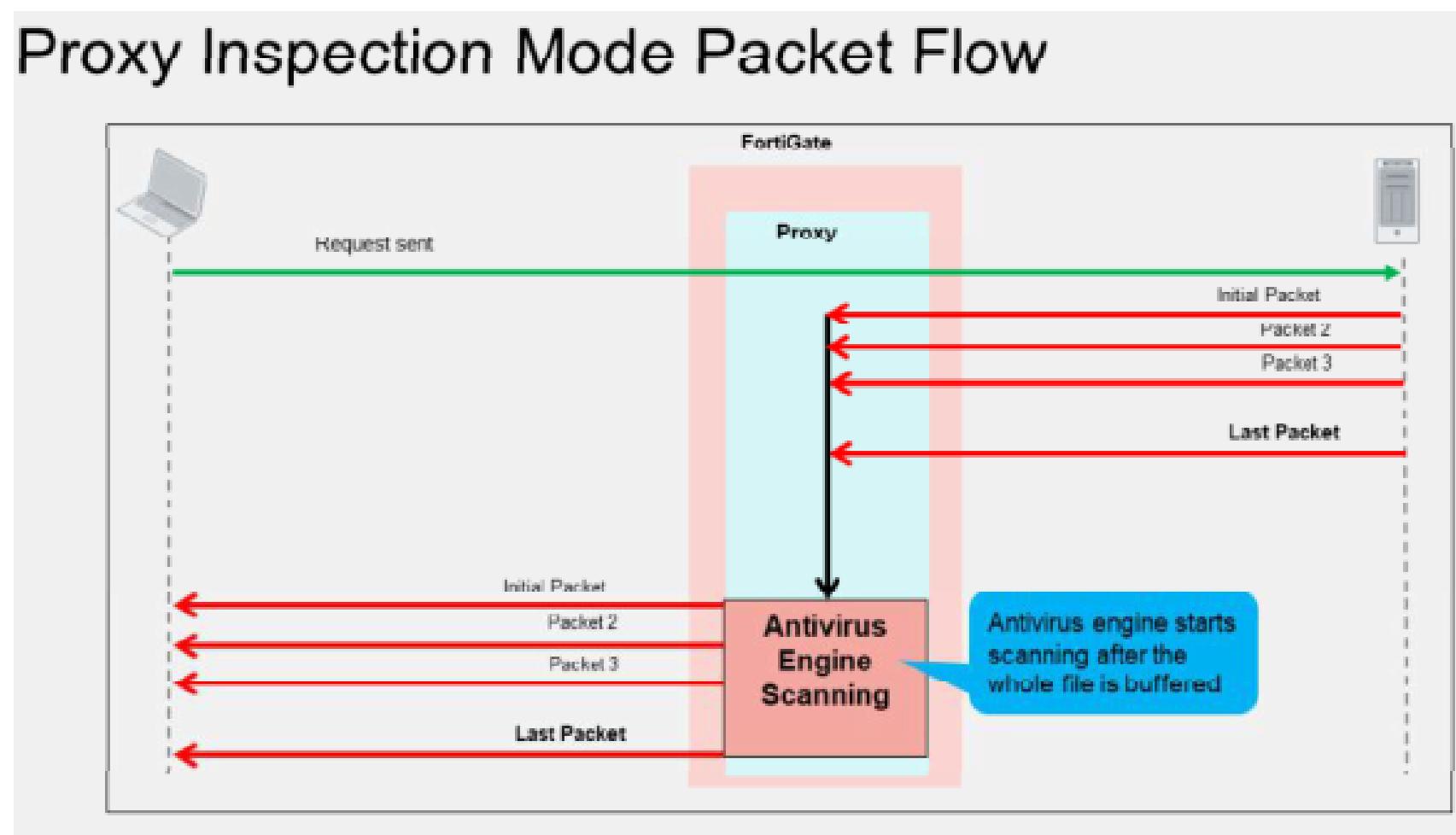


وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Proxy-based Inspection (Deep Mode)

<https://depi.gov.eg>





وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Proxy-based Inspection (Deep Mode)

<https://depi.gov.eg>

### Configuration Profile

The screenshot shows the configuration interface for a FortiGate 301E device. On the left is a navigation sidebar with various security profiles like Dashboard, Network, Policy & Objects, Security Profiles, and AntiVirus. The AntiVirus profile is currently selected. The main right panel is titled 'Edit AntiVirus Profile' and shows a configuration form. At the top, there's a 'Name' field set to 'default' and a 'Comments' field containing 'Scan files and block viruses.' with a file count of '29/255'. Below these are two tabs: 'Block' (selected) and 'Monitor'. Under 'Feature set', there are two options: 'Flow-based' (disabled) and 'Proxy-based' (selected). A large red arrow points from the bottom right towards the 'Proxy-based' tab. The 'Inspected Protocols' section lists several protocols with their status: HTTP (on), SMTP (on), POP3 (on), IMAP (on), FTP (on), CIFS (off), MAPI (P off), and SSH (P on). The 'APT Protection Options' section includes three items: 'Content Disarm and Reconstruction' (P off), 'Treat Windows executables in email attachments as viruses' (on), and 'Include mobile malware protection' (on). The bottom section, 'Quarantine', has a single item with an off switch.



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Proxy-based Inspection (Deep Mode)

<https://depi.gov.eg>

### Configuration Policy

SSL Inspection

SSL certificate-inspection

Logging Options

Log Allowed Traffic

Capture Packets

FortiGate-301E

Edit Policy

Name: LAN-WAN

Incoming Interface: Internal-VLAN-10 (LAN-10)

Outgoing Interface: Internet-4G-Port01 (port1)

Source: all

Destination: all

Schedule: always

Action: ACCEPT

Inspection Mode: **Proxy-based** (highlighted with a red box, marked 1)

Firewall / Network Options

NAT: On

IP Pool Configuration: Use Outgoing Interface Address

Preserve Source Port: Off

Protocol Options: PROT default

Security Profiles: default

AntiVirus: default



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Proxy-based Inspection (Deep Mode)

<https://depi.gov.eg>

### Logs & Monitoring

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
15 seconds ago	192.168.10.53	PC-01	89.238.73.97 (secure.elcar.org)	HTTPS		LAN-WAN (3)
15 seconds ago	192.168.10.53	PC-01	89.238.73.97 (secure.elcar.org)	HTTPS		LAN-WAN (3)
15 seconds ago	192.168.10.53	PC-01	89.238.73.97 (secure.elcar.org)	HTTPS		LAN-WAN (3)
15 seconds ago	192.168.10.53	PC-01	89.238.73.97 (secure.elcar.org)	HTTPS		LAN-WAN (3)
15 seconds ago	192.168.10.53	PC-01	89.238.73.97 (secure.elcar.org)	HTTPS		LAN-WAN (3)



## 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.



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 1.1 Antivirus Inspection Mode : Proxy-based Inspection (Deep Mode)

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.



## 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.



## 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





وزارة الاتصالات  
وتكنولوجيا المعلومات



## 2.1 Web Filter Inspection Mode :

### Proxy-Based Mode

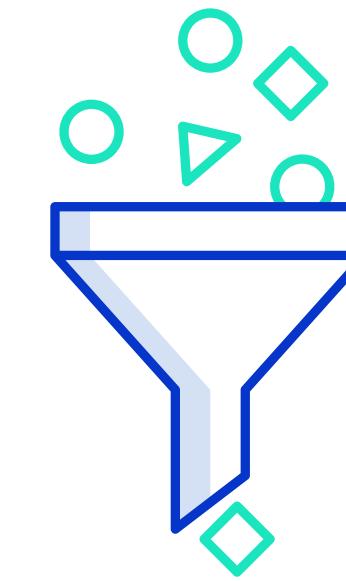
- ✓ Deep inspection
- ✓ More accurate filtering
- ✓ Can block specific pages, keywords, and content

### 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.



## 2.3 FortiGate Web Filter – Actions Explained

### 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





## 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.





## 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.



## 2.3 FortiGate Web Filter

<https://depi.gov.eg>

The screenshot shows the FortiGate management interface. The left sidebar includes options like SSL/SSH Inspection, Application Signatures, IPS Signatures, Web Rating Overrides, Web Profile Overrides, VPN, User & Authentication, WiFi & Switch Controller, System, Security Fabric (with a red notification badge), and Log & Report. A red circle with the number 1 is placed near the Security Fabric icon.

This screenshot displays the 'Edit Web Filter Profile' screen. It features a table with columns for Name and Action. Several rows are listed: General Organizations (Allow), Business (Allow), Information and Computer Security (Allow), Government and Legal Organizations (Allow), Information Technology (Allow), Armed Forces (Allow), Web Hosting (Allow), Secure Websites (Allow), and Web-based Applications (Allow). A context menu is open over the 'Information Technology' row, showing options: Allow, Monitor, Block, Warning, and Authenticate. The 'Allow' option is selected. The status bar at the bottom indicates 89% 93.

This screenshot shows the 'Edit Web Filter Profile' screen with the 'Flow-based' tab selected (marked with a red circle 1). It includes a warning message about not having a license for FortiGuard web filtering. Below the warning, there is another table with rows for Dynamic DNS (Block), Newly Observed Domain (Block), Newly Registered Domain (Block), and a large section for 'General Interest - Personal' (35 items) which includes Advertising, Brokerage and Trading, Games, Web-based Email, and Entertainment, all set to Allow. The status bar at the bottom indicates 47% 93.



## 2.3 FortiGate Web Filter - Authentication Required

<https://depi.gov.eg>

Name	Action
General Organizations	Allow
Business	Allow
Information and Computer Security	Allow
Government and Legal Organizations	Allow
Information Technology	Authenticate
Armed Forces	Allow
Web Hosting	Allow
Secure Websites	Allow
Web-based Applications	Allow
Charitable Organizations	Allow

Edit Filter

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

Selected User Groups: IT

OK Cancel



## 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.



## 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





## 2.4 Web Rating Override:

<https://depi.gov.eg>

New Web Rating Override

URL  Lookup rating

Warning: This device is not licensed for the FortiGuard web filtering service.

Comments Write a comment... 0/255

Override to

Category

Sub-Category



وزارة الاتصالات  
وتقنيات جيا 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 :

New URL Filter

URL	www.youtube.com
Type	Simple
Action	Allow
Status	Enable

OK Cancel

<https://depi.gov.eg>

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



## 2.6 FortiGate Web Filter – SSL Certificate Inspection

### 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.





## 2.6 FortiGate Web Filter – SSL Certificate Inspection

<https://depi.gov.eg>

The screenshot shows the FortiGate management interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. The 'Flow-based' inspection mode is selected. In the 'SSL Inspection' section, a red box highlights the 'certificate-inspection' profile, which is also selected in a dropdown menu. A red arrow points to this highlighted area. The 'Logging Options' section shows 'Log Allowed Traffic' is enabled.

SSL Inspection Profile	Status
SSL certificate-inspection	Selected
SSL certificate-inspection	Enabled
SSL custom-deep-inspection	Disabled
SSL deep-inspection	Disabled



## 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 Control use the IPS engine to scan traffic against application pattern .

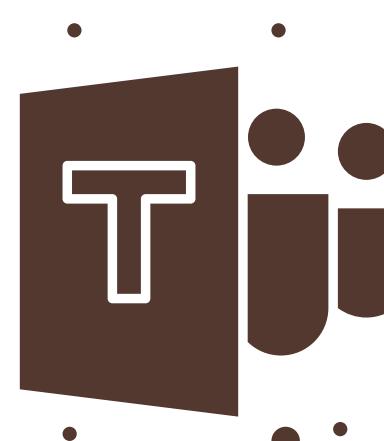
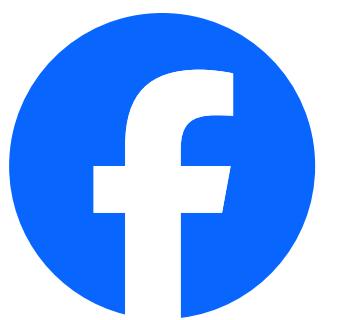


وزارة الاتصالات  
وتقنيات جيا المعلومات



### 3.1 List Of Application Signatures

<https://depi.gov.eg>



The screenshot shows a software interface for managing network security profiles. The left sidebar lists various security features: Dashboard, Network, Policy & Objects, Security Profiles (selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control (selected), Intrusion Prevention, File Filter, SSL/SSH Inspection, Application Signatures (selected), IPS Signatures, Web Rating Overrides, Web Profile Overrides, VPN, User & Authentication, and System.

The main area displays "View Application Signatures" with three donut charts:

- Category: Total 2304. Breakdown: Network (green), Collaboration (orange), Storage (purple), General (red), Video/Audio (blue), and Business (pink).
- Technology: Total 2416. Breakdown: Browser (green), Client-Server (orange), Information (purple), and Peer-to-Peer (red).
- Risk: Total 2304. Breakdown: Low (blue), Medium (yellow), Information (green), High (orange), and Critical (red).

A table titled "Application Signature 2,304" lists the following data:

Name	Category	Technology	Popularity	Risk
1kxun	Video/Audio	Client-Server	★★★★★	■■□□
1und1.Mail	Email	Browser-Based	★★★★★	■■□□
2Safe	Storage.Backup	Browser-Based	★★★★★	■■□□
2ch	Social.Media	Browser-Based	★★★★★	■■□□
3PC	Network.Service	Network-Protocol	★★★★★	■■□□
4Sync	Storage.Backup	Browser-Based	★★★★★	■■□□
4shared	Storage.Backup	Client-Server	★★★★★	■■□□



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 3.2 Application Control Inspection

<https://depi.gov.eg>

2

Edit Application Sensor

Web.Client (18) Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Create New	Edit	Delete	
Priority	Details	Type	Action
No results			

Options

Block applications detected on non-default ports  Allow  Block

Allow and Log DNS Traffic

QUIC

Replacement Messages for HTTP-based Applications

Dashboard Network Policy & Objects Security Profiles Application Control Intrusion Prevention File Filter SSL/SSH Inspection Application Signatures IPS Signatures Web Rating Overrides Web Profile Overrides VPN User & Authentication System

1

FW1

Edit Application Sensor

Categories

All Categories

- Business (179, 6)
- Cloud.IT (31)
- Collaboration (293, 6)
- Email (87, 12)
- Game (124)
- General.Interest (241, 9)
- Mobile (3)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- Video/Audio (206, 13)
- VoIP (31)
- Web.Client (18)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Dashboard Network Policy & Objects Security Profiles Application Control Intrusion Prevention File Filter SSL/SSH Inspection Application Signatures IPS Signatures Web Rating Overrides Web Profile Overrides VPN



وزارة الاتصالات  
وتقنيات جيا المعلومات



### 3.3 Application Control Filter Actions

<https://depi.gov.eg>

The screenshot shows the left sidebar of a web-based management interface. The 'Application Control' option is highlighted with a green background and a star icon. Other visible options include 'Policy & Objects', 'Security Profiles', 'AntiVirus', 'Web Filter', 'Video Filter', 'DNS Filter', 'Intrusion Prevention', and 'File Filter'. A small orange arrow points from the 'Application Control' section towards the main content area.

The screenshot shows a list of application categories under the 'Game' filter. Each item has an eye icon and a dropdown arrow. The items are: Game (124), Mobile (3), P2P (85), Remote.Access (91), Storage.Backup (296, 16), Video/Audio (206, 13), and Web.Client (18). A cursor arrow is pointing at the 'Mobile' item.

The screenshot shows the 'Proxy' filter action details. A red box highlights the 'Monitor' action, which is selected. Below it are other options: 'Allow' (green checkmark), 'Block' (red circle), 'Quarantine' (yellow square), and 'View Signatures (106)'.



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 3.4 Application Control Scanning Order

1- Application .

2- Filter .

3- Fortiguard Category .

The screenshot shows a software interface for managing network security policies. On the left, a sidebar menu lists various security profiles and their sub-options. The 'Application Control' option is highlighted with a green background. To the right, there are two main sections: 'Categories' and 'Application and Filter Overrides'.  
  
**Categories:**  
- Business (179, 6)  
- Collaboration (293, 6)  
- Game (124)  
- Mobile (3)  
- P2P (85)  
- Remote.Access (91)  
- Storage.Backup (296, 16)  
- Video/Audio (206, 13)  
- Web.Client (18)  
- Cloud.IT (31)  
- Email (87, 12)  
- General.Interest (241, 9)  
- Network.Service (332)  
- Proxy (106)  
- Social.Media (150, 31)  
- Update (48)  
- VoIP (31)  
- Unknown Applications (checkbox checked)  
  
**Application and Filter Overrides:**  
- Create New  
- Edit  
- Delete  
- Priority  
- Details  
- Type  
- Action



## 3.5 Application Control in Policy

- 1- Select Application Control Profile.
- 2- SSL using deep inspection .
- 3- Log Allowed traffics ..

The screenshot shows a 'Policy & Objects' menu on the left with 'Firewall Policy' selected. On the right, under 'Security Profiles', three configurations are highlighted with red circles numbered 1, 2, and 3:

- AntiVirus: Enabled (green switch), set to 'AV default' (orange dropdown).
- Application Control: Enabled (green switch), set to 'APP default' (green dropdown).
- SSL Inspection: Enabled (green switch), set to 'SSL deep-inspection' (orange dropdown).

Under 'Logging Options', 'Log Allowed Traffic' is enabled (green switch) and set to 'Security Events All Sessions' (green dropdown).



## 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.



وزارة الاتصالات  
وتقنيات جيا المعلومات



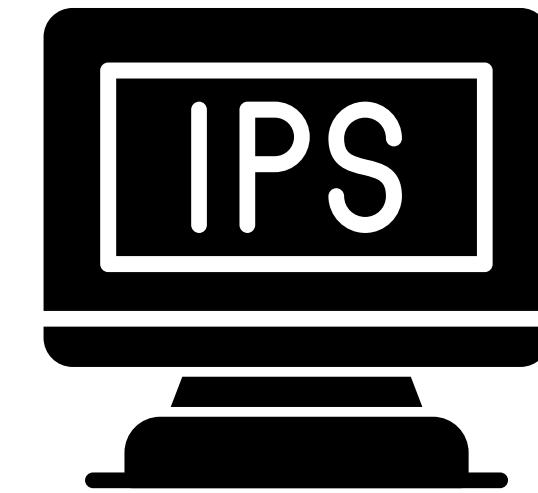
### 3.6 Application Control Bandwidth limit by Traffic Shaper



وزارة الاتصالات  
وتقنيات جيا المعلومات



## Key Types of Security Profiles



### 4- IPS (Intrusion Prevention System).

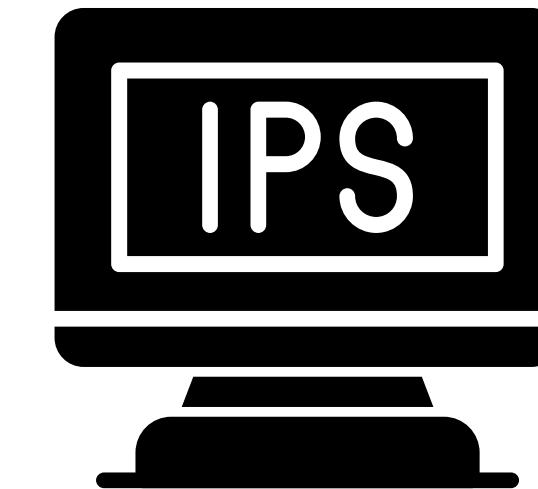
- Detects and blocks attacks targeting: Servers , Applications & Network devices
- Protects from exploitation of vulnerabilities.
- IPS = a system that detects and prevents intrusions.
- Its main purpose is to protect the network from attacks before they reach devices and servers.



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.



وزارة الاتصالات  
وتقنيات جيا 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.

<https://depi.gov.eg>

- Web Filter
- Video Filter
- DNS Filter
- Application Control
- Intrusion Prevention ★
- File Filter
- SSL/SSH Inspection
- Application Signatures

IPS Signatures and Filters			
<a href="#">Create New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	
Details	Exempt IPs	Action	Packet Logging
SEV		<span style="color: #007bff;">Default</span>	<span style="color: #dc3545;">Disabled</span>
SEV			
SEV			



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 4.3 IPS Actions :

<https://depi.gov.eg>

### Allow

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

### Use case:

Testing or low-risk signatures.

The screenshot shows a software interface for managing network security profiles. On the left, a sidebar lists various security features: Dashboard, Network, Policy & Objects, Security Profiles (selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (highlighted in green), and File Filter. To the right, a main panel titled 'Add Signatures' displays a table of signatures. A context menu is open over the 'Signature' tab, showing options: Type, Action, Packet logging, Status, Rate-based settings, Exempt IPs, Add All Results, and a list of actions: Allow (green checkmark), Monitor (blue eye), Block (red circle), Reset (black gear), Default (green gear), and Quarantine (black square). The 'Signature' tab is highlighted in green.



## 4.3 IPS Actions :

<https://depi.gov.eg>

### Monitor

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

### Use case:

Monitoring new signatures before blocking .

The screenshot shows a software interface for managing network security profiles. On the left, there's a sidebar with options like Dashboard, Network, Policy & Objects, Security Profiles (which is currently selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (highlighted in green), and File Filter. To the right, there's a main panel titled 'Add Signatures' with tabs for 'Filter' and 'Signature'. A context menu is open over a specific signature entry, listing actions: Default, Allow, Monitor, Block, Reset, Default, and Quarantine. The 'Monitor' option is highlighted with a green background. The signature entry itself shows 'Name: IPS Signature 5,864', 'Severity: 5', and 'Target: 1'. There are also buttons for 'Add All Results' and 'Disable'.



## 4.3 IPS Actions :

<https://depi.gov.eg>

### Block

- Blocks the traffic completely if it matches the IPS signature

### Use case:

Critical & High severity attacks .

The screenshot shows a software interface for managing network security profiles. On the left, there's a sidebar with options like Dashboard, Network, Policy & Objects, Security Profiles (which is currently selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (highlighted in green), and File Filter. The main panel has a title 'Add Signatures' and a 'Signature' tab selected. A context menu is open over the 'Signature' tab, listing options: Default (selected), Allow, Monitor, Block (highlighted in red), Reset, Default, and Quarantine.



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 4.3 IPS Actions :

### Reset

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

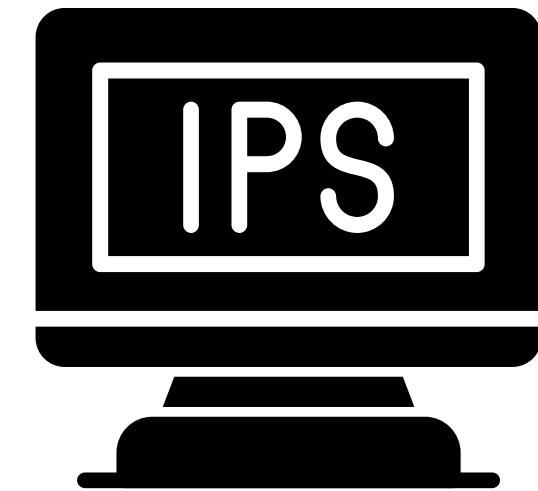
### Use case:

- Stopping attacks that depend on long-lived sessions .

The screenshot shows a software interface for managing network security profiles. On the left, a sidebar lists various security features: Dashboard, Network, Policy & Objects, Security Profiles (selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (highlighted in green), and File Filter. The main panel is titled 'Add Signatures' and contains tabs for 'Filter' and 'Signature'. A context menu is open over the 'Signature' tab, listing options: Default, Allow, Monitor, Block, Reset, Default, and Quarantine. The 'Signature' tab is currently selected. At the bottom of the main panel, there is a table header with columns for Name, Severity, and Target.



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 .

The screenshot shows a software interface for managing network security profiles. On the left, there's a sidebar with options like Dashboard, Network, Policy & Objects, Security Profiles (which is currently selected), AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (highlighted in green), and File Filter. The main panel has a title 'Add Signatures' and a 'Type' dropdown set to 'Default'. Below it are buttons for 'Filter' and 'Signature'. A context menu is open over the 'Default' button in the 'Action' dropdown, listing options: Allow, Monitor, Block, Reset, Default (which is selected and highlighted in green), and Quarantine. There are also 'Disable' and 'Default' buttons next to the menu. At the bottom, there's a table header with columns for Name, Severity, and Target.



## 4.3 IPS Actions :

<https://depi.gov.eg>

### 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 .

The screenshot shows a software interface for managing network security profiles. On the left, there's a sidebar with options like Dashboard, Network, Policy & Objects, Security Profiles, AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention (which is highlighted in green), and File Filter. The main area has a title 'Add Signatures' with tabs for 'Filter' and 'Signature'. A context menu is open over the 'Action' dropdown, which includes options: Default, Allow, Monitor, Block, Reset, Default, and Quarantine. The 'Quarantine' option is highlighted with a yellow background. Below the menu, there's a table header for 'IPS Signature' with columns for Name, Severity, and Target.



وزارة الاتصالات  
وتقنيات جيا المعلومات



## 4.4 A Botnet C&C

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.

Security Profiles

- AntiVirus
- Web Filter
- Video Filter
- DNS Filter
- Application Control
- Intrusion Prevention
- File Filter
- SSL/SSH Inspection
- Application Signatures
- IPS Signatures
- Web Rating Overrides
- Web Profile Overrides
- VPN

IPS Signatures and Filters

Create New	Edit	Delete	
Details	Exempt IPs	Action	Packet Logging
SEV Low	SEV Medium	SEV High	Default
Disabled			Disabled

Botnet C&C

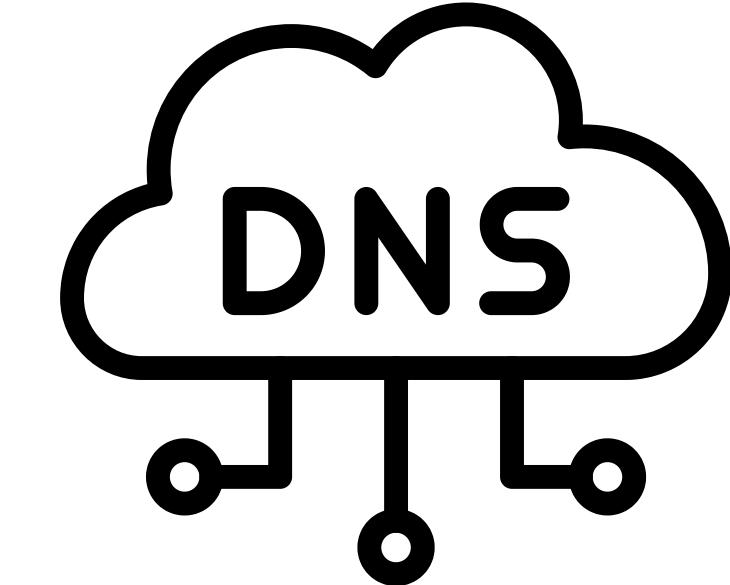
Scan Outgoing Connections to Botnet Sites

Disable Block Monitor



## Key Types of Security Profiles

### 5- DNS Filter



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

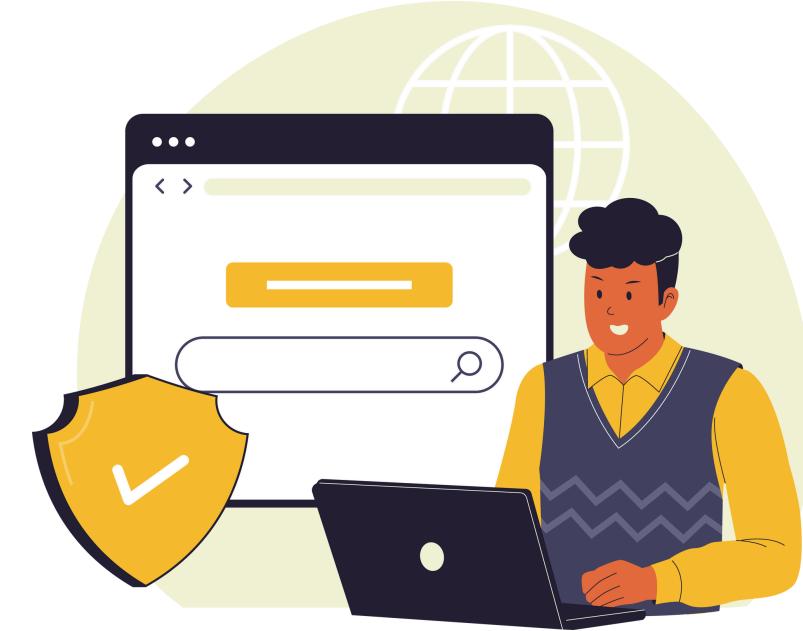


وزارة الاتصالات  
وتقنيات جيا المعلومات



## Key Types of Security Profiles

### 6-SSL Inspection



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



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.



وزارة الاتصالات  
وتقنيات جياب 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.



وزارة الاتصالات  
وتقنيات جيا المعلومات



# THANK YOU

› End Slide