



PROJECT

ADVANCED FORTIGATE SECURITY PROFILES

PROJECT
DOCUMENTATION

وزارة الاتصالات
وتقنيات جيا المعلومات



› Start Slide



Our Great Team

Mohamed Abdelaal

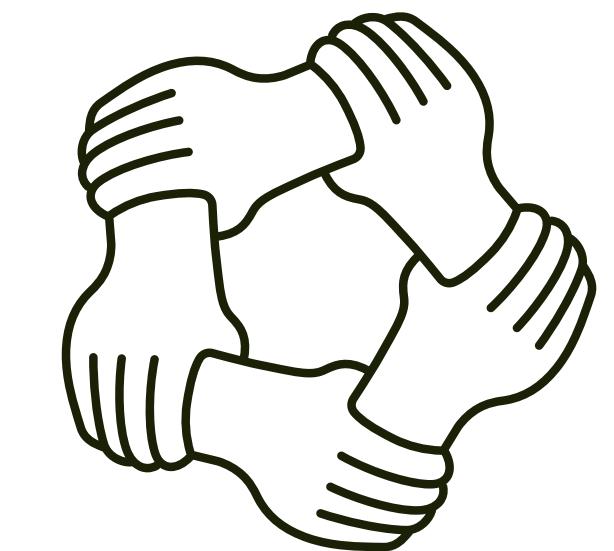
Eyad Mahmoud

Arwa Essam

Filopateer Atef

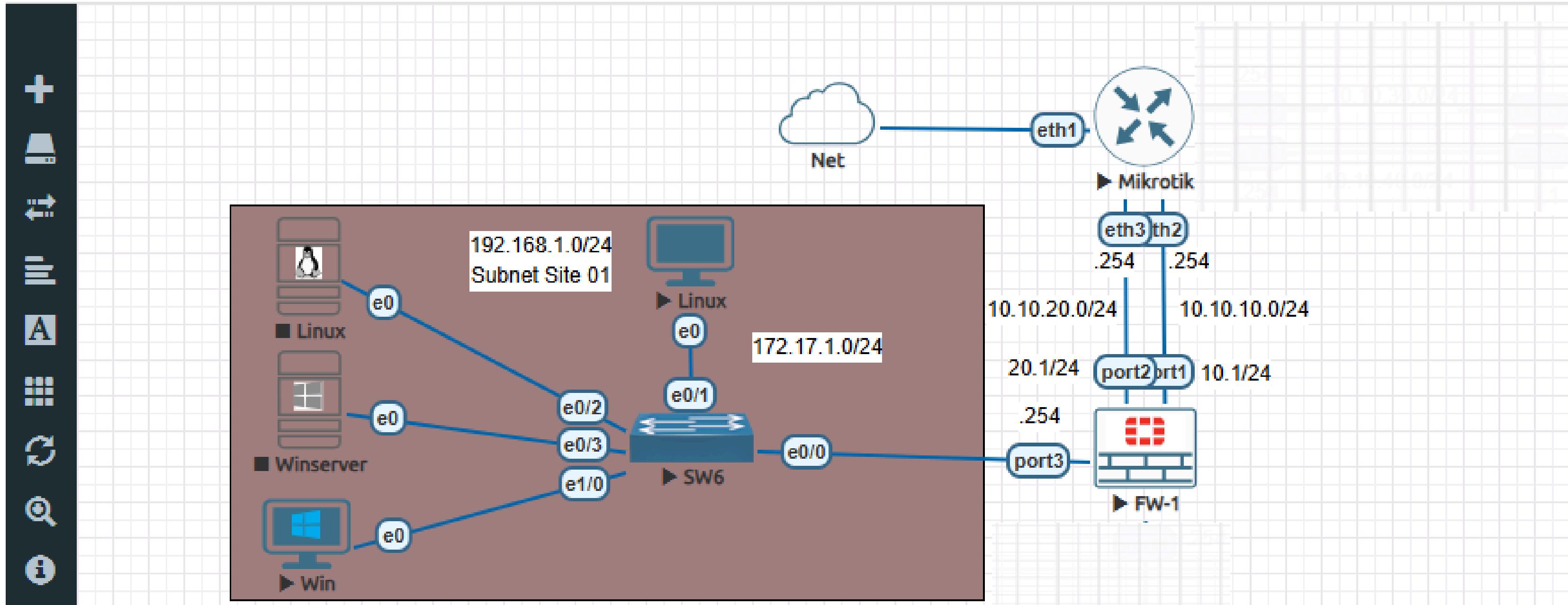
Youssef Yasser

وزارة الاتصالات
وتقنيات الاتصالات
وتقنيات الاتصالات





<https://depi.gov.eg>



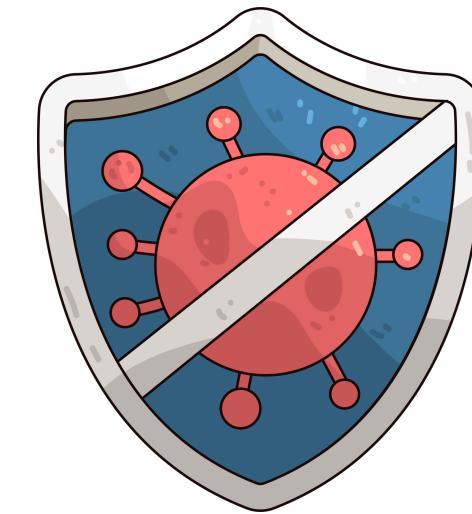


وزارة الاتصالات
وتقنيات جيا المعلومات



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.



Configuring Flow-Based Antivirus Scanning

<https://depi.gov.eg>

The screenshot shows the configuration interface for FW1. On the left, a sidebar lists various security profiles: Dashboard, Network, Policy & Objects, Security Profiles (selected), AntiVirus (selected), 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, and User & Authentication.

The main panel displays the 'Edit AntiVirus Profile' screen. It includes fields for Name (default), Comments (Scan files and block viruses. 29/255), and a switch for AntiVirus scan (set to Block). A red box highlights the 'Feature set' dropdown, which is set to 'Flow-based'. Below this is the 'Inspected Protocols' section, also highlighted with a red box, containing checkboxes for HTTP, SMTP, POP3, IMAP, FTP, and CIFS. A note below the protocols states 'CIFS? (Common Internet File System)'. The 'APT Protection Options' section is also highlighted with a red box, containing three checkboxes: 'Treat Windows executables in email attachments as viruses', 'Include mobile malware protection', and 'Quarantine'.

APT “Advanced Persistent Threat” = Advanced detection + sandbox + behavior analysis to stop smart, hidden, long-term attacks.



Apply Flow-Based Antivirus Scanning on Policy

1

Internet Service Database

VLAN_192-to-WAN

vlan_192

WAN-01 (port1)

all

2

Name: VLAN_192-to-WAN

Incoming Interface: vlan_192

Outgoing Interface: WAN-01 (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT ✘ DENY

Inspection Mode: Flow-based (highlighted)

3

Security Profiles

AntiVirus: AV default

Web Filter:

DNS Filter:

Application Control:

IPS:

File Filter:

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic: Security Events All Sessions

Generate Logs when Session Starts:

Capture Packets:

Comments: VLAN_192-to-WAN

Enable this policy:



On client Machine test using :

<https://depi.gov.eg>

The screenshot shows a Microsoft Edge browser window with multiple tabs. The active tab displays the URL <https://www.eicar.org/download-anti-malware-testfile/>. The page content includes:

- A large "eICAR" logo with a star above it.
- A "DOWNLOAD ANTI MALWARE TESTFILE" button.
- A "Language Independent Options" section with the command "-fmessage-length=n".
- Terminal-like output showing system logs and error messages, including:
 - "ERROR: apport (pid 18485) Thu Mar 16 11:44:59 2017: called for pid 18484, signal 8, core linit 0"
 - "ERROR: apport (pid 18485) Thu Mar 16 11:44:59 2017: executable: /usr/bin/cmatrix (command line "cmatrix -b")"
 - File system statistics: "RX: ens33 109 B/s", "IO: 0 B/s", "Blocks: 0", "Size: 0", "Block: 4096 directory", "Device: 12h/18d Inode: 23823", "Links: 0", "Access: (0755/drwxr-xr-x)", "UId: (0/ root)", "GId: (0/ root)", "Modify: 2017-03-16 11:42:39.745114275 -0700", "Change: 2017-03-16 11:43:00.633276860 -0700", "Birth: -".
 - Kernel errors: "trigger_fs_error", "warning_ratelimit_burst", "warning_ratelimit_interval_ms", "fuse", "EAFNOSUPPORT 97 Address family not supported by protocol", "ENOSYS 38 Function not implemented", "EXDEV 18 Invalid cross-device link".
- A message: "Screen must be 80x25 or higher to display this file."



View Logs :

<https://depi.gov.eg>

FW1

Dashboard Network Policy & Objects Security Profiles VPN User & Authentication System Security Fabric Log & Report Forward Traffic Local Traffic Sniffer Traffic Events AntiVirus Web Filter SSL DNS Query

1

Date/Time Source Device Destination Application

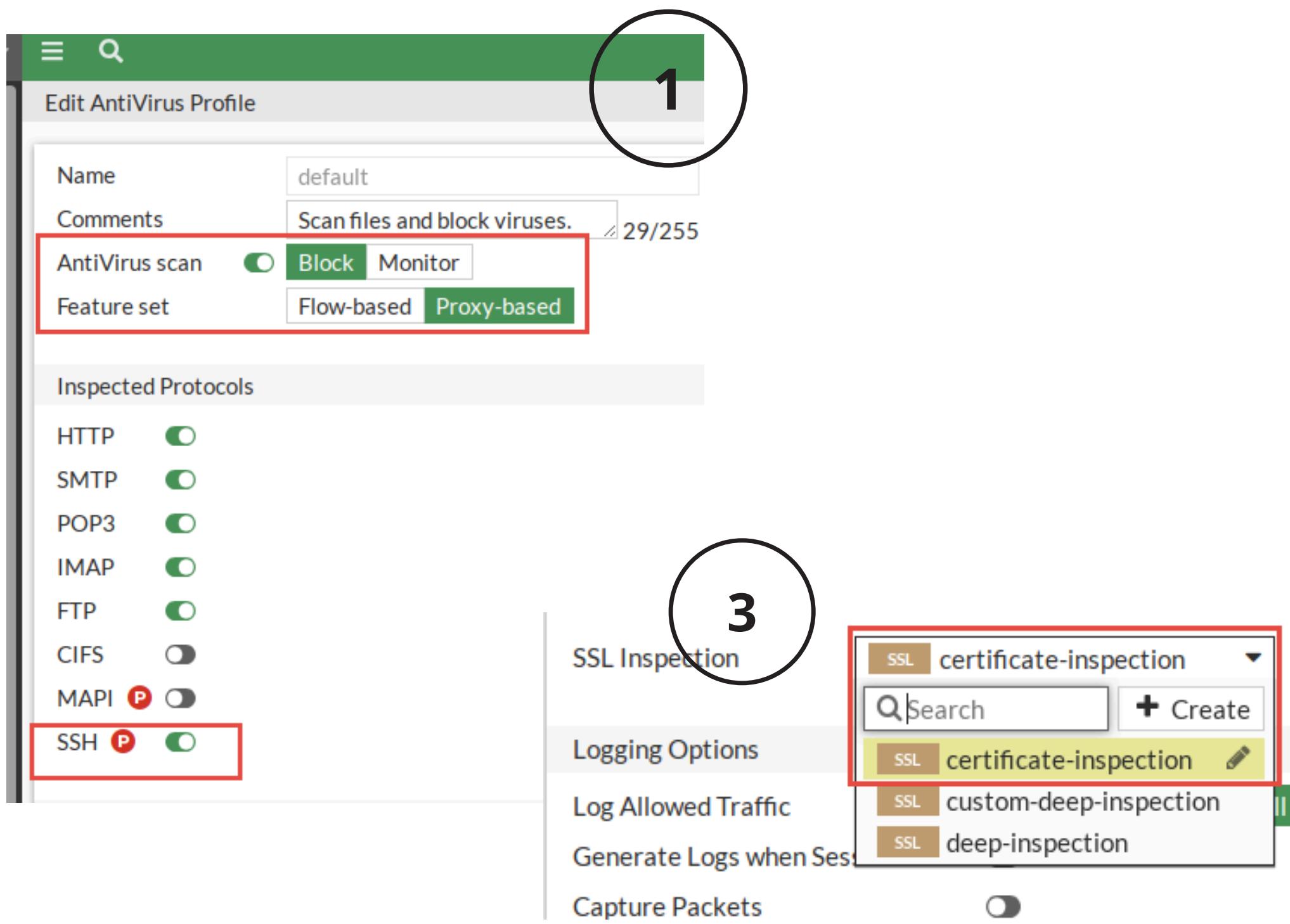
Date/Time	Source	Device	Destination	Application
37 seconds ago	192.168.1.4	DESKTOP-5C484F5	23.33.90.144 (th.bing.com)	HTTPS
38 seconds ago	192.168.1.4	DESKTOP-5C484F5	23.33.90.144 (th.bing.com)	HTTPS
2 minutes ago	192.168.1.4	DESKTOP-5C484F5	104.102.63.189 (fs.micros...	HTTPS
2 minutes ago	192.168.1.4	DESKTOP-5C484F5	96.45.45.45	DNS
3 minutes ago	192.168.1.4	DESKTOP-5C484F5	96.45.45.45	DNS
6 minutes ago	192.168.1.4	DESKTOP-5C484F5	96.45.45.45	DNS
6 minutes ago	192.168.1.4	DESKTOP-5C484F5	51.105.71.137 (v10.event...	HTTPS
6 minutes ago	192.168.1.4	DESKTOP-5C484F5	96.45.45.45	DNS
7 minutes ago	192.168.1.4	DESKTOP-5C484F5	13.71.55.58 (settings-win...	HTTPS
7 minutes ago	192.168.1.4	DESKTOP-5C484F5	13.71.55.58 (settings-win...	HTTPS
7 minutes ago	192.168.1.4	DESKTOP-5C484F5	13.71.55.58 (settings-win...	HTTPS
9 minutes ago	192.168.1.4	DESKTOP-5C484F5	98.66.133.184 (client.wns...	HTTPS
9 minutes ago	192.168.1.4	DESKTOP-5C484F5	98.66.133.184 (client.wns....	HTTPS
10 minutes ago	192.168.1.4	DESKTOP-5C484F5	96.45.45.45	DNS

Activate V Go to Setting DNS



Using Antivirus Scanning in Proxy-Based

<https://depi.gov.eg>



1

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: Block Monitor

Feature set: Flow-based Proxy-based

Inspected Protocols

- HTTP:
- SMTP:
- POP3:
- IMAP:
- FTP:
- CIFS:
- MAPI:
- SSH:

2

SSL Inspection

Logging Options

Log Allowed Traffic

Generate Logs when Session

Capture Packets

3

Edit Policy

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

AntiVirus: AV default

Web Filter:



Testing Policy

<https://depi.gov.eg>

وزارة الاتصالات
وتقنيات جيا المعلومات



Download area using the standard protocol HTTP or secure, SSL enabled protocol HTTPS

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
---------------------------	-------------------------------	-------------------------------	-------------------------------

FortiGate should block the download attempt, and insert a replacement message similar to the following example:

10.200.1.254/eicar.com

FortiAnalyzer FortiManager Remote FortiGate

High Security Alert

You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".

URL: http://10.200.1.254/eicar.com

Quarantined File Name: [disabled]

Reference URL: http://www.fortinot.com/vn?vn=EICAR_TEST_FILE

FortiGate shows the HTTP virus message when it blocks or quarantines infected files.

A
G



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.



Configuring FortiGuard Web Filtering

The screenshot shows the FortiGate management interface. On the left, there's a sidebar with a green header containing a search bar and a 'Add Widget' button. Below it, the 'System Information' section lists the following details:

Hostname	FW1
Serial Number	FGVMEV_SJFLZZT9D
Firmware	v7.0.15 build0632 (Mature)
Mode	NAT
System Time	2025/11/25 00:00:00
Uptime	00:04:28:14
WAN IP	Unknown

On the right, the 'Licenses' section is highlighted with a red box. It lists five categories, each with a circular icon and a link:

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

Below the licenses, there's a 'FortiToken' section showing '0 / 0' and a red warning message: 'Unable to connect to FortiGuard servers.'

To configure FortiGate for web filtering based on FortiGuard categories, you must make sure that FortiGate has a valid FortiGuard security subscription license. The license provides the web filtering capabilities necessary to protect against inappropriate websites.



Configuring FortiGuard Web Filtering

<https://depi.gov.eg>

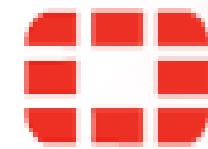
The screenshot shows the FortiGate management interface under the 'Web Filter' section. A security profile named 'default' is being edited. The 'Feature set' tab is selected, showing 'Flow-based' and 'Proxy-based' options. A warning message states: 'Warning: This device is not licensed for the FortiGuard web filtering service. Traffic may be blocked if this option is enabled.' Below this, there are five action buttons: Allow, Monitor, Block, Warning, and Authenticate. A table lists various content categories with their counts: Local Categories (2), Potentially Liable (12), Adult/Mature Content (15), Bandwidth Consuming (6), Security Risk (6), and General Interest - Personal (35). A large number '2' is overlaid on the bottom right of this section.

The screenshot shows the 'FortiGuard Category Based Filter' configuration dialog. It includes fields for 'Name' (default) and 'Comments' (Default web filtering.). The 'Feature set' tab is selected, showing 'Flow-based' and 'Proxy-based' options. A warning message states: 'Warning: This device is not licensed for the FortiGuard web filtering service. Traffic may be blocked if this option is enabled.' Below this, there are five action buttons: Allow, Monitor, Block, Warning, and Authenticate. A table lists categories with their counts: Local Categories (2), Potentially Liable (12), Adult/Mature Content (15), Bandwidth Consuming (6), Freeware and Software Downloads, and File Sharing and Storage. A large number '3' is overlaid on the bottom right of this section, and a red box highlights the 'Allow' button in the action row.



Configuring FortiGuard Web Filtering

<https://depi.gov.eg>



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category: Internet Telephony

URL: <http://www.skype.com/>



Configuring FortiGuard Web Rating

<https://depi.gov.eg>

The screenshot shows the FortiGate management interface. On the left, the navigation menu includes options like FW1, Dashboard, Network (with a cursor pointing to it), Policy & Objects, Security Profiles, AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, Intrusion Prevention, File Filter, SSL/SSH Inspection, Application Signatures, IPS Signatures, and Web Rating Overrides. The 'Web Rating Overrides' option is highlighted with a green bar at the bottom. The main panel is titled 'Edit Web Rating Override' and shows a URL input field containing 'www.bing.com' with a 'Lookup rating' button next to it. A yellow warning box states: 'Warning: This device is not licensed for the FortiGuard web filtering service.' Below this, there's a 'Comments' section with a text input field and a character count of 0/255. The 'Override to' section allows setting the category and sub-category. The 'Category' dropdown is set to 'Security Risk' and the 'Sub-Category' dropdown is set to 'Malicious Websites'. At the bottom are 'OK' and 'Cancel' buttons. A large number '1' is overlaid on the bottom left of the main panel.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category Malicious Websites

URL http://www.bing.com/

To have the rating of this web page re-evaluated [please click here](#).

2



Setting Up Web Filtering Authentication

<https://depi.gov.eg>

1

Users/Groups Creation Wizard

User Type → 2 Login Credentials → 3 Contact Info → 4 Extra Info

Username: student

Password: student

Security Risk: 6

Malicious Websites	Action
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block

0

2

Name: Override_Permission

Type: Firewall

Members: student

3

Malicious Websites

Authenticate

Phishing

Block

Spam URLs

Block

Dynamic DNS

Block

0% 93

4



Setting Up Web Filtering Authentication



FortiGuard Intrusion Prevention -
Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category Malicious Websites

URL http://www.bing.com/

To have the rating of this web page re-evaluated [please click here](#).

Proceed

Go Back

5

Username	student
Password	fortinet



Login & Monitoring

<http://depi.gov.eg>



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 .



Controlling Application Traffic

<https://depi.gov.eg>

FW1

Edit Application Sensor

93 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: default

Comments: Monitor all applications. 25/255

Categories:

- All Categories
- Business (179)
- Cloud.IT (31)
- Collaboration (293)
- Email (87)
- Game (124)
- General.Interest (241)
- Mobile (3)
- Network.Service (332)
- P2P (85)
- Proxy (106)
- Remote.Access (91)
- Social.Media (150)
- Storage.Backup (296)
- Update (48)

1

Web.Client (18) Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New	Priority	Details	Type	Action
No results				

Options

- Block applications detected on non-default ports
- Allow and Log DNS Traffic
- QUIC
- Replacement Messages for HTTP-based Applications

2



Controlling Application Traffic

<https://depi.gov.eg>

The screenshot shows a list of application overrides under "Web.Client (18)". A red arrow points to the "Create New" button, which is highlighted with a red box and labeled "1". The "Type" dropdown is set to "Application" (highlighted with a red box and labeled "1"). The "Action" dropdown is set to "Block" (highlighted with a red box and labeled "3"). The "Filter" section shows a selected filter: "BHVR Excessive-Bandwidth" (highlighted with a red box and labeled "2").

The screenshot shows the "Add New Override" dialog. The "Type" dropdown is set to "Application" (highlighted with a red box and labeled "1"). The "Action" dropdown is set to "Block" (highlighted with a red box and labeled "3"). The "Filter" section shows a selected filter: "BHVR Excessive-Bandwidth" (highlighted with a red box and labeled "2"). The sidebar on the right lists various application categories and behaviors, with "Excessive-Bandwidth" highlighted in yellow.

3

4



Controlling Application Traffic

<https://depi.gov.eg>

Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	🚫 Block

1

5

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options PROT default

Security Profiles

AntiVirus AV default

Web Filter WEB default

Video Filter

DNS Filter

Application Control APP default

IPS

File Filter

SSL Inspection deep-inspection

This SSL profile uses full SSL inspection. End users will likely see certificate errors unless the certificate is installed in their browser.

Decrypted Traffic Mirror

Logging Options

Log Allowed Traffic

Security Events All Sessions

6



Controlling Application Traffic - Testing

Open a new browser tab, and then go to the following URL: <http://abc.go.com>.

FortiGate should display a block message—it can take up to two minutes for the block page to appear because of the change in configuration.

The screenshot shows a red grid icon followed by the text "FortiGate Application Control". Below it, a large "Application Blocked" message is displayed, along with details about the blocked application: "Application ABC.Com", "Category Video/Audio", "URL http://abc.go.com/", and "Policy b11ac58c-791b-51e7-4600-12f829a689d9".

FortiGate Application Control

Application Blocked

You have attempted to use an application that violates your Internet usage policy.

Application ABC.Com

Category Video/Audio

URL http://abc.go.com/

Policy b11ac58c-791b-51e7-4600-12f829a689d9



Configure Application Overrides

Application Overrides for the ABC.Com application signature, and set the action to Allow

<https://depi.gov.eg>

The screenshot shows the 'Edit Application Sensor' interface. Under 'Collaboration', there are 293 items. Under 'Web.Client', there are 18 items. In the 'Application and Filter Overrides' table, there is one row with Priority 1, Details 'BHVR Excessive-Bandwidth', Type 'Filter', and Action 'Block'. This row is highlighted with a red border.

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block

1

The screenshot shows the 'Add New Override' interface with 'Type' set to 'Application' and 'Action' set to 'Allow'. A search bar shows 'abc'. The 'Application Signature' table lists four entries: ABC (P2P, Peer-to-Peer), ABC.Com (Video/Audio, Browser-Based), ABC.Player (Video/Audio, Client-Server), and ABC.Streaming (Video/Audio, Browser-Based). All entries have a green checkmark next to them.

Name	Category	Technology	Popularity
ABC	P2P	Peer-to-Peer	★★★★★
ABC.Com	Video/Audio	Browser-Based	★★★★★
ABC.Player	Video/Audio	Client-Server	★★★★★
ABC.Streaming	Video/Audio	Browser-Based	★★★★★

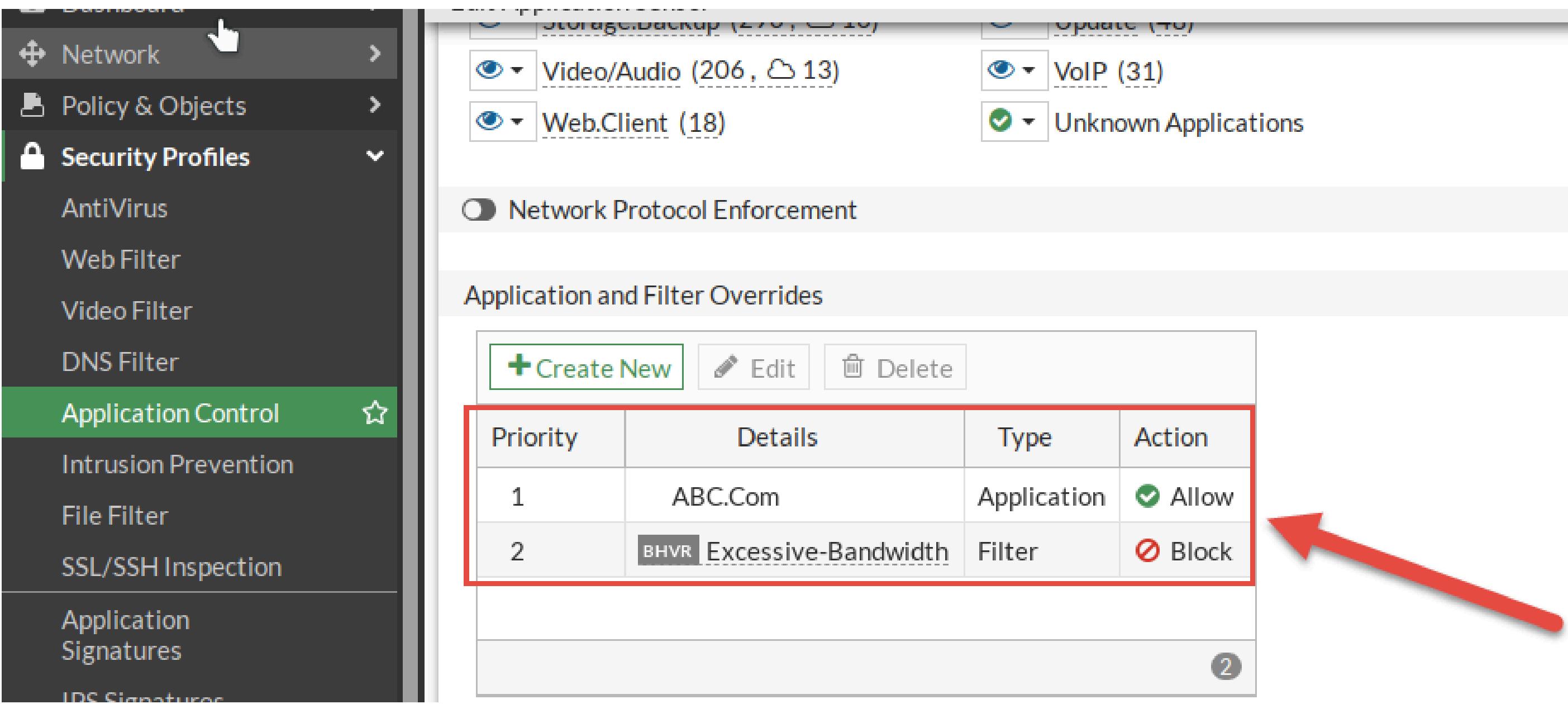
2



Configure Application Overrides

Application Overrides for the ABC.Com application signature, and set the action to Allow

<https://depi.gov.eg>



The screenshot shows a network configuration interface with a sidebar menu and a main application overrides table.

Left Sidebar:

- Network
- Policy & Objects
- Security Profiles
- AntiVirus
- Web Filter
- Video Filter
- DNS Filter
- Application Control** (selected)
- Intrusion Prevention
- File Filter
- SSL/SSH Inspection
- Application Signatures
- IDS Signatures

Main Area:

- Storage Backup (200, 100)
- Update (70)
- Video/Audio (206, 13)
- VoIP (31)
- Web.Client (18)
- Unknown Applications

Network Protocol Enforcement: Off

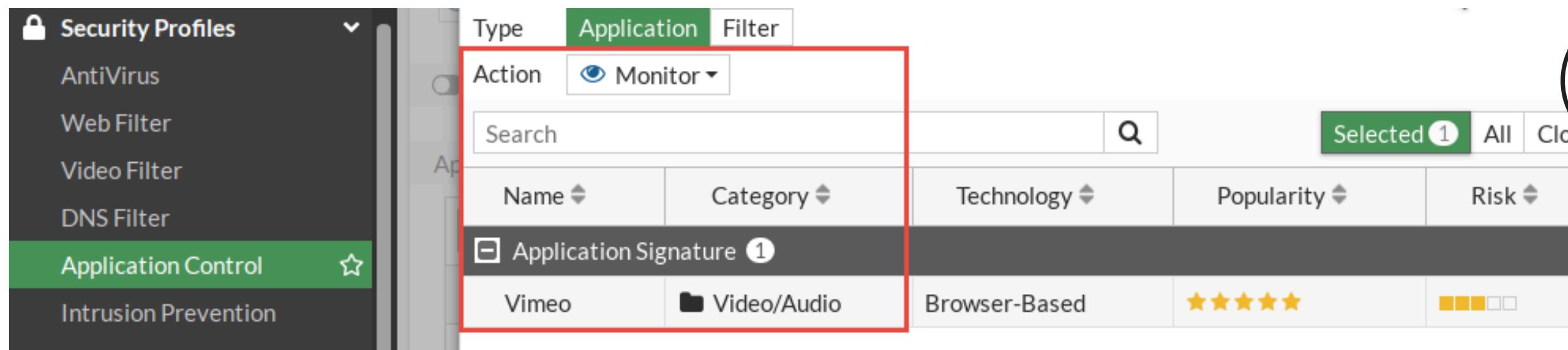
Application and Filter Overrides:

Priority	Details	Type	Action
1	ABC.Com	Application	Allow
2	BHVR Excessive-Bandwidth	Filter	Block



Controlling Application Bandwidth Usage

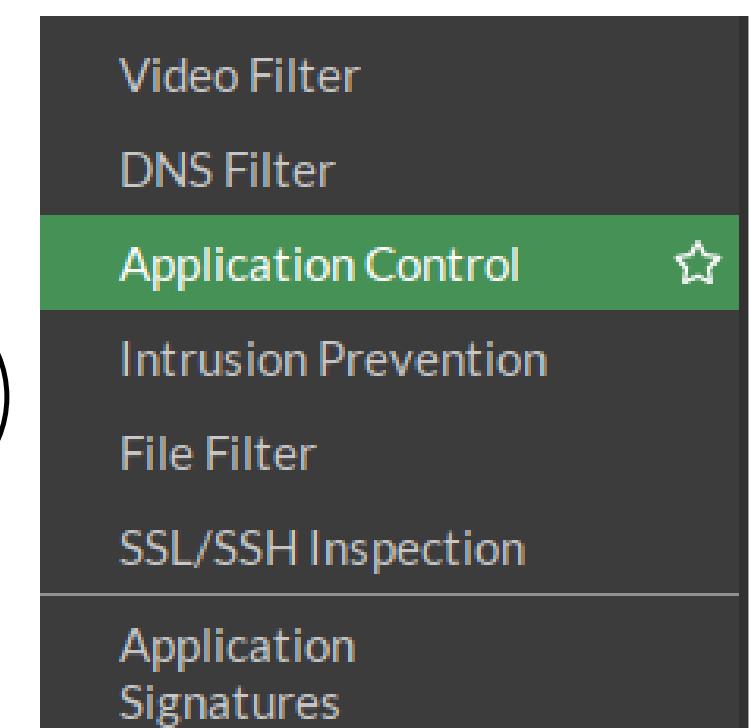
Ex: Vimeo is Audio / Video Application will be use in testing



Name	Category	Technology	Popularity	Risk
Vimeo	Video/Audio	Browser-Based	★★★★★	□□□□□

<https://depi.gov.eg>

2



Application and Filter Overrides

Priority	Details	Type	Action
1	ABC.Com	Application	Allow
2	Vimeo	Application	Monitor
3	BHVR Excessive-Bandwidth	Filter	Block



Controlling Application Bandwidth Usage

To Configure Bandwidth Usage need to Trafic Shaper

2

1

Type: Shared Per IP Shaper

Name: Vimeo-Shapper

Quality of Service

Traffic priority: Medium

Bandwidth unit: Mbps

Maximum bandwidth: 1 Mbps

Guaranteed bandwidth: Off

DSCP: Off

New Traffic Shaping Policy

Name: Vimeo-Traffic-Policy

Status: Enabled

Comments: Write a comment... 0/255

If Traffic Matches:

- Source interface: vlan_192
- Outgoing interface: WAN-01 (port1)
- Source: all
- Destination: all
- Schedule: Off
- Service: ALL
- Application: Vimeo
- URL Category: Off

Then:

- Apply shaper: On
- Shared shaper: Off
- Reverse shaper: Off
- Per-IP shaper: Off

Vimeo-Shapper



Controlling Application Bandwidth Usage

To Configure Bandwidth Usage need to Trafic Shaper

The screenshot shows the Fortinet Firewall interface. The left sidebar has a red arrow pointing to the 'Traffic Shaping' option under 'Policy & Objects'. The main content area has a red box around the 'Traffic Shaping Policies' tab. A red circle with '2' is on the sidebar, and another red circle with '3' is above the tab. A red arrow points from the bottom-left towards the 'Create New' button. A large red arrow points from the bottom-left towards the 'Implicit' policy entry. A red circle with '4' is on the right side of the 'Implicit' entry.

FW1

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

2

3

Traffic Shapers

Traffic Shaping Policies

Traffic Shaping Profiles

+Create New

Edit

Delete

Search

Export

Name

Source

Destination

To

Action

Shared Shaper

Reverse Shaper

Per-IP Shaper

Service

IPv4 1

Vimeo-Traffic-Policy

all

all

WAN-01(port1)

Apply Shaper

Vimeo-Shapper

All

Implicit 1



وزارة الاتصالات
وتقنيات جيا المعلومات



THANK YOU

› End Slide