رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

PROJECT

ADVANCED FORTIGATE SECURITY PROFILES

PROJECT
DOCUMENTATION

https://depi.gov.eg

› Start Slide

رواد مصر الرقمية

Our Great Team

وزارة الاتصالات وتكنولوجيا المعلومات

Mohamed Abdelaal

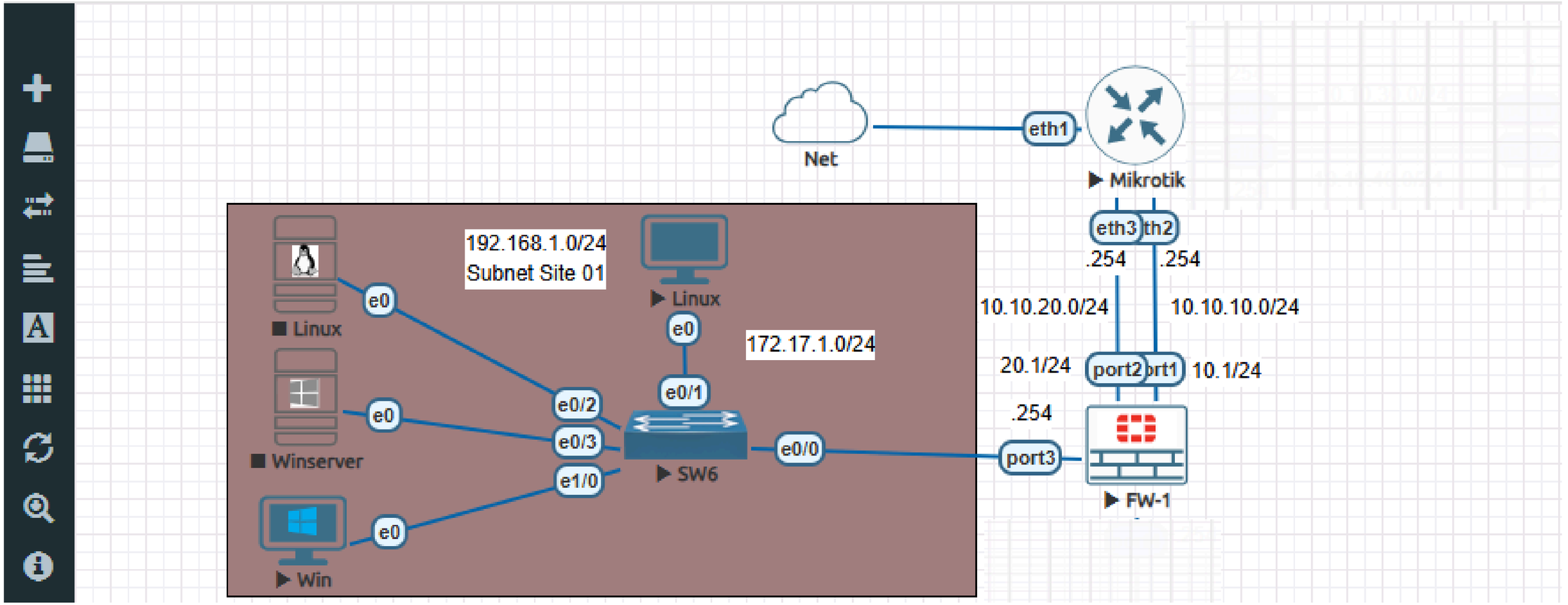
Eyad Mahmoud

Arwa Essam

Filopateer Atef

Youssef Yasser

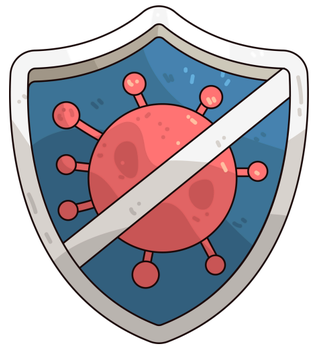
https://depi.gov.eg


Net
eth1
Mikrotik
eth3
th2
.254
.254
10.10.20.0/24
10.10.10.0/24
20.1/24
port2
rt1
10.1/24
.254
port3
FW-1
192.168.1.0/24
Subnet Site 01
Linux
e0
Linux
e0
172.17.1.0/24
e0/1
e0/2
e0
Winserver
e0/3
e0/0
SW6
e1/0
e0
Win

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles



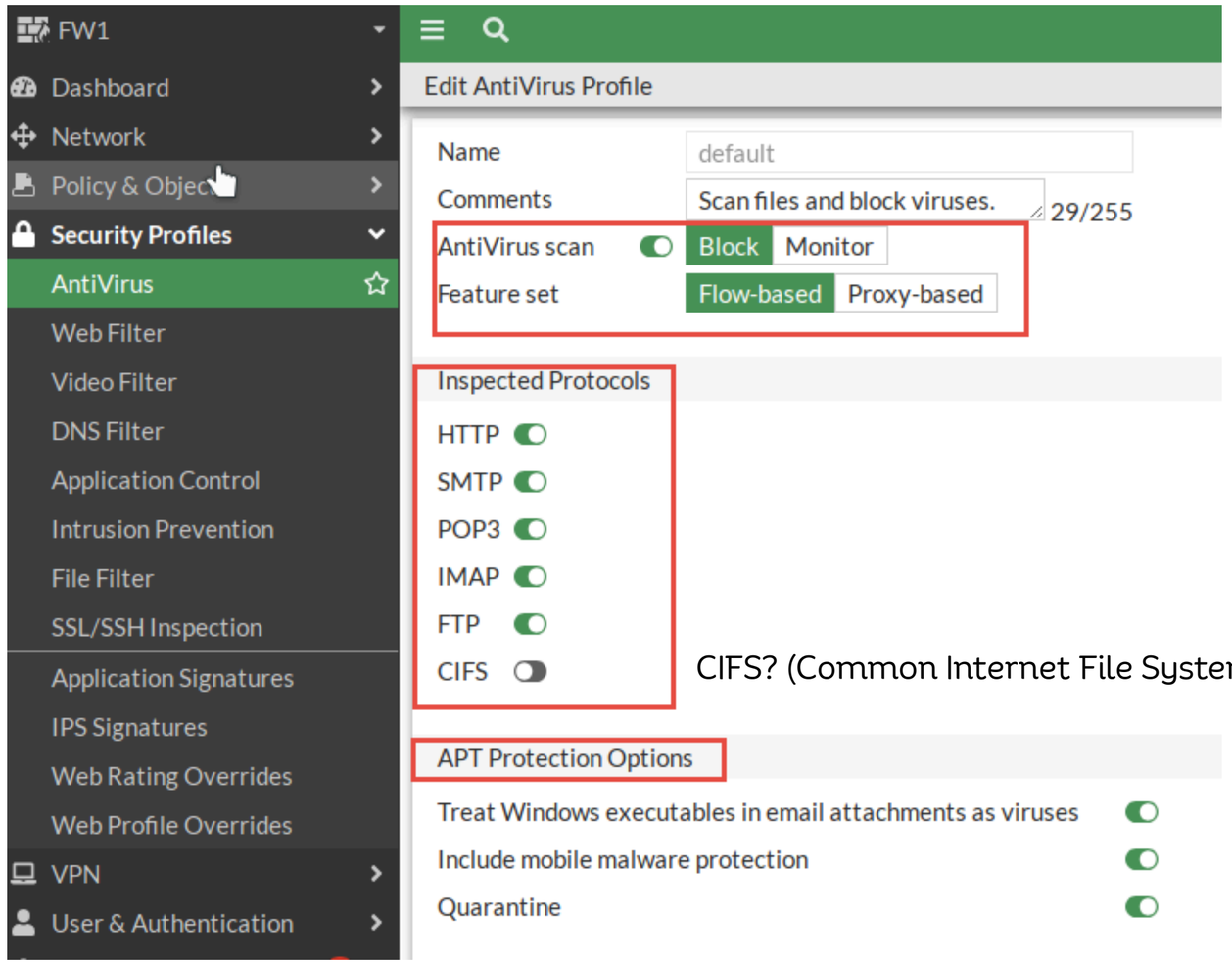
1. Antivirus

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

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Configuring Flow-Based Antivirus Scanning



CIFS? (Common Internet File System)

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

https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Apply Flow-Based Antivirus Scanning on Policy

1

Internet Service Database	VLAN_192-to-WAN	vlan_192	WAN-01 (port1)	all

2

- Network
- Policy & Objects
  - Firewall Policy
  - IPv4 DoS Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Virtual IPs
  - IP Pools
  - Protocol Options
  - Traffic Shaping
- Security Profiles
- VPN

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 | Proxy-based

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 15/1023

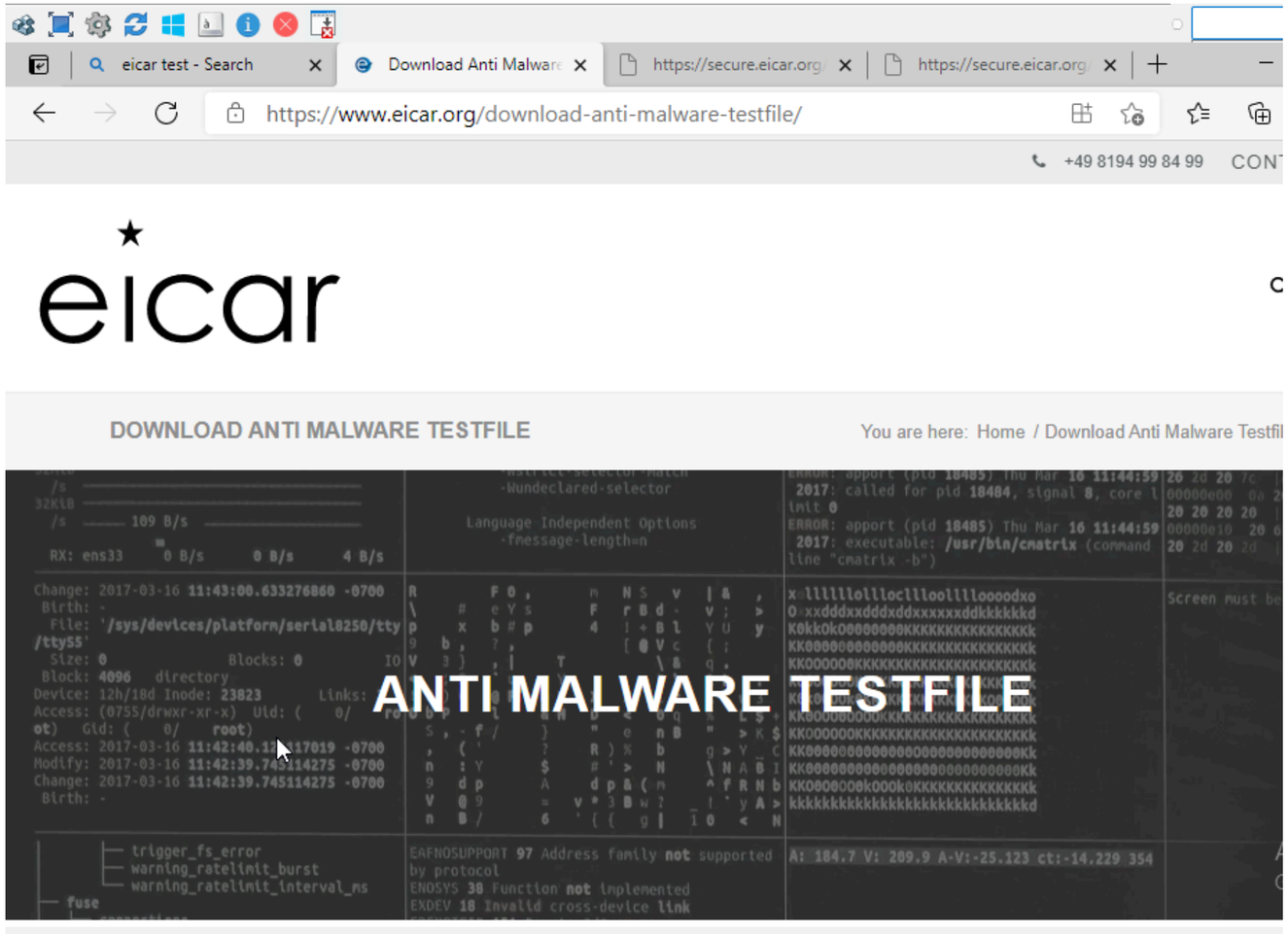
Enable this policy

https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــــالات
وتكنولوجيا المعلومات

On client Machine test using :

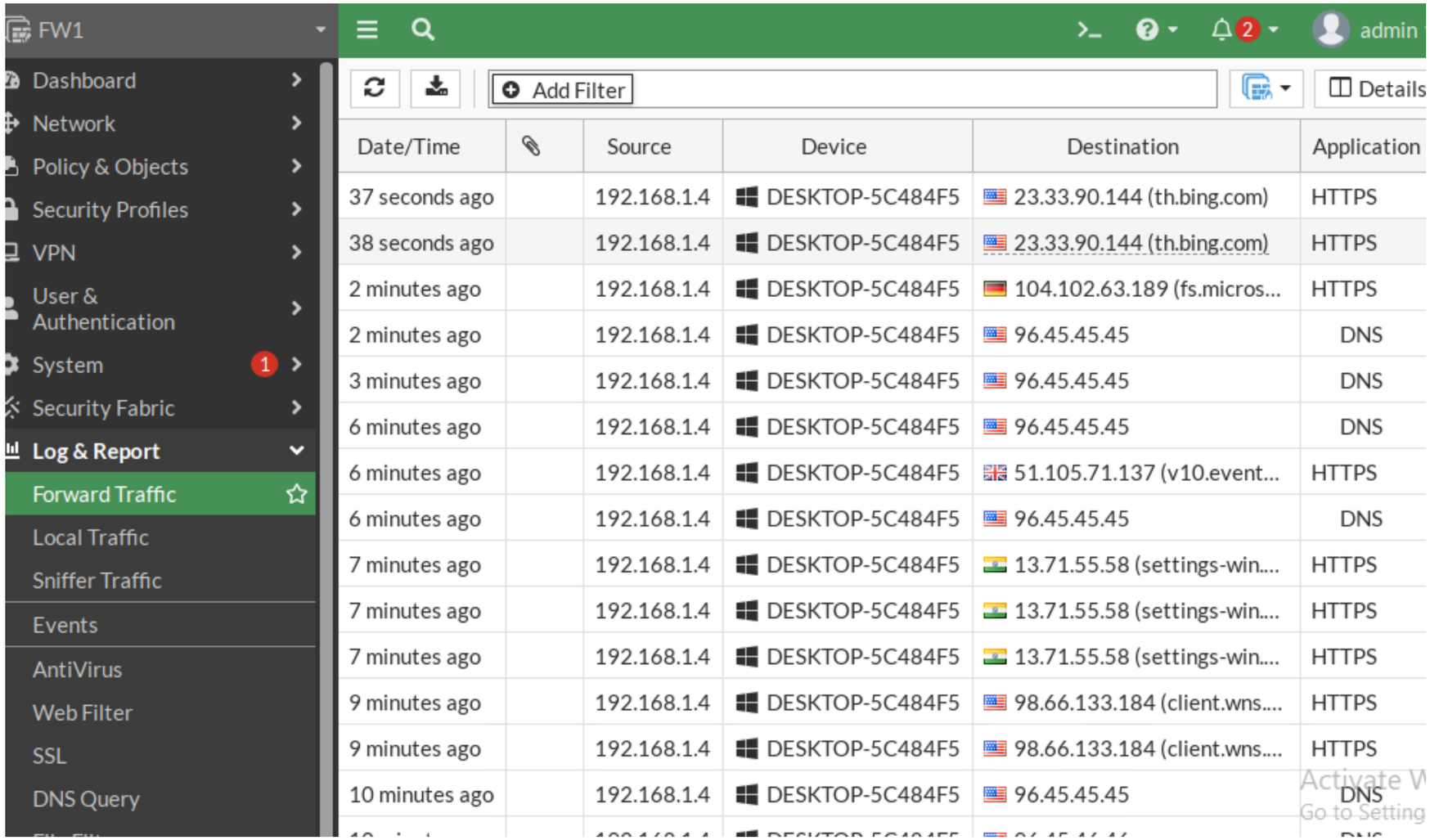


https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

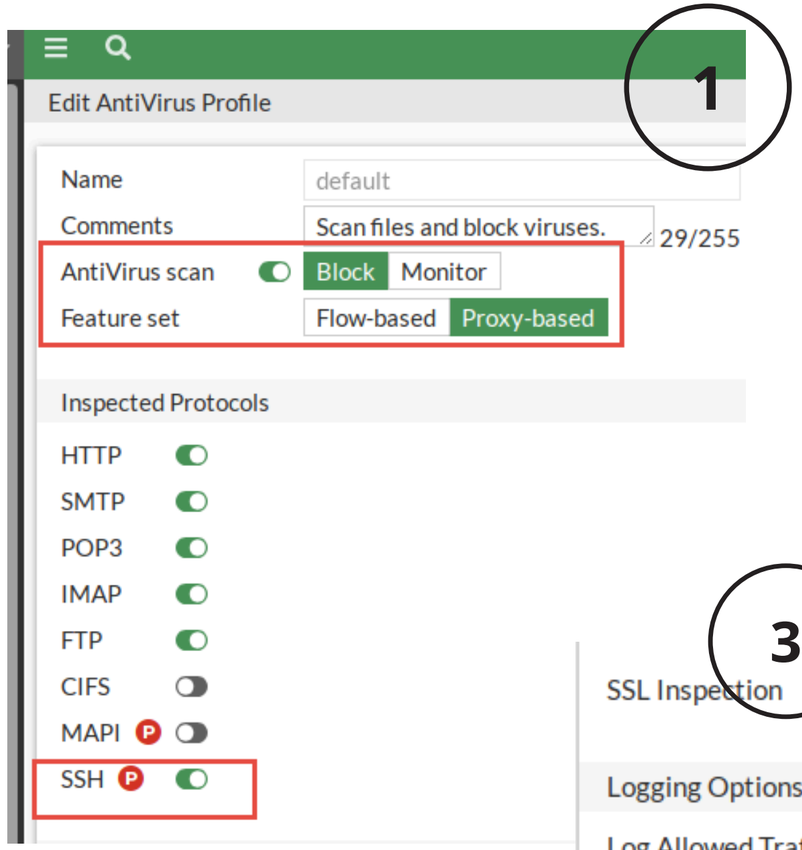
View Logs :

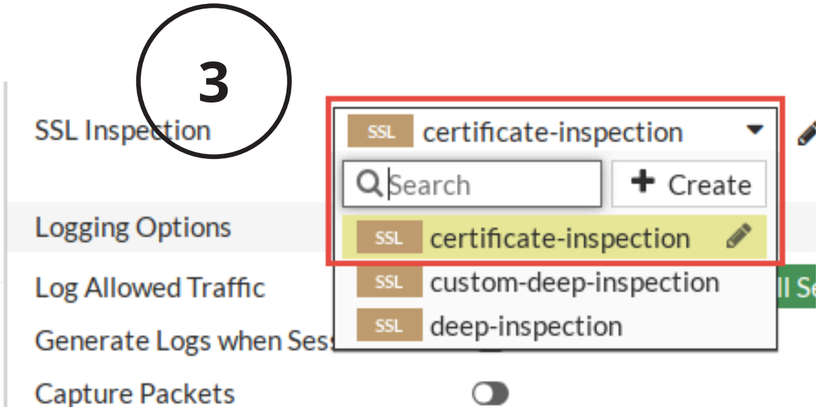


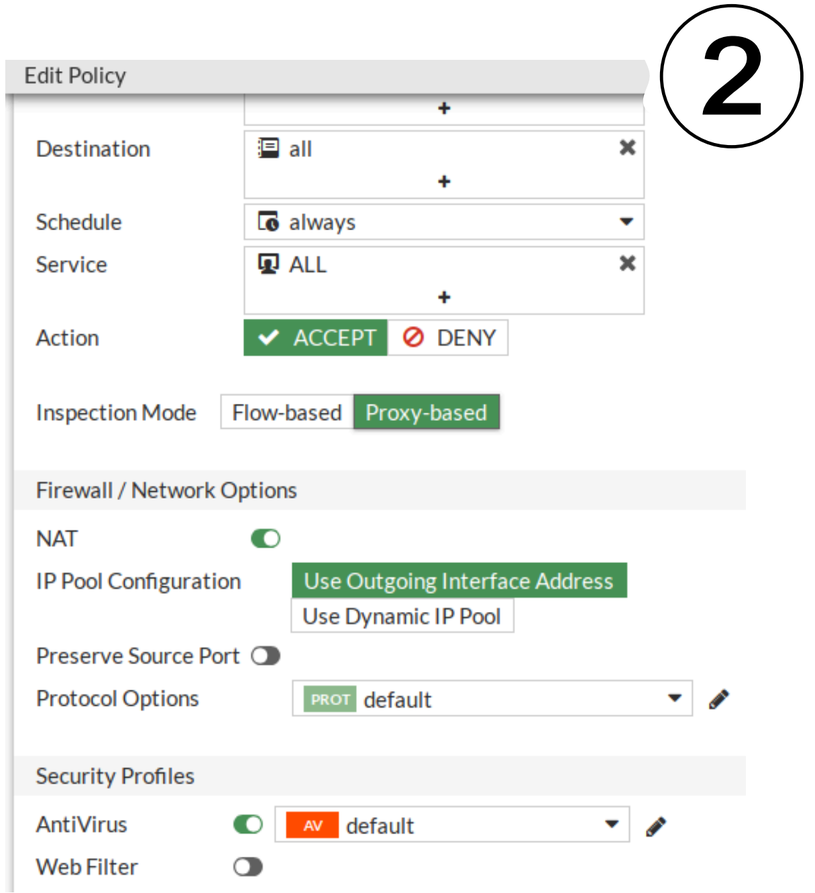
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Using Antivirus Scanning in Proxy-Based





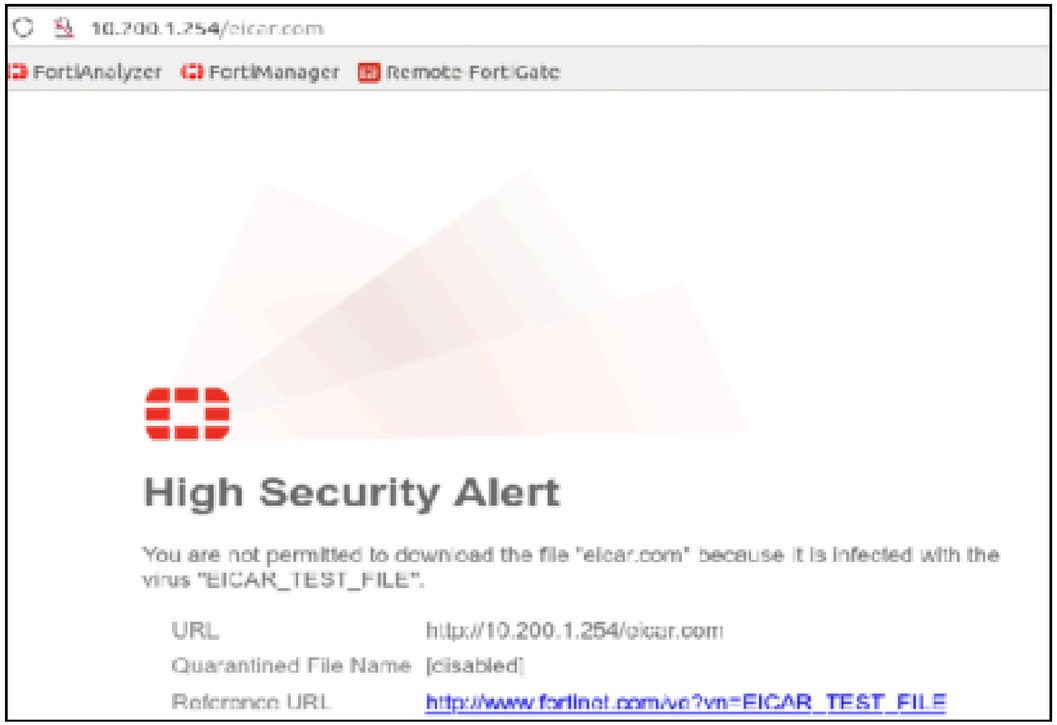


https://depi.gov.eg

Testing Policy

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:



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

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles

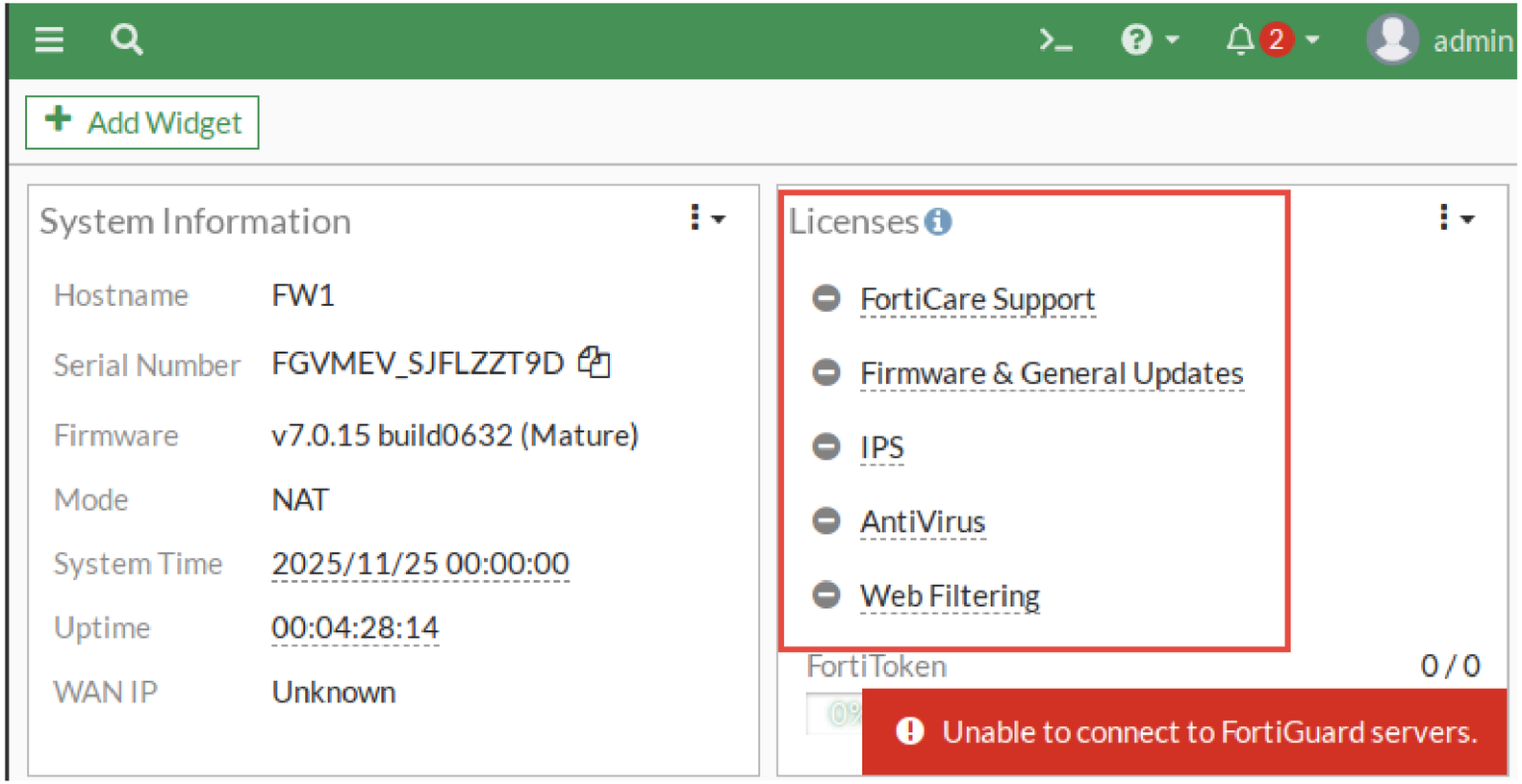
2. Web Filtering

- 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

Configuring FortiGuard Web Filtering

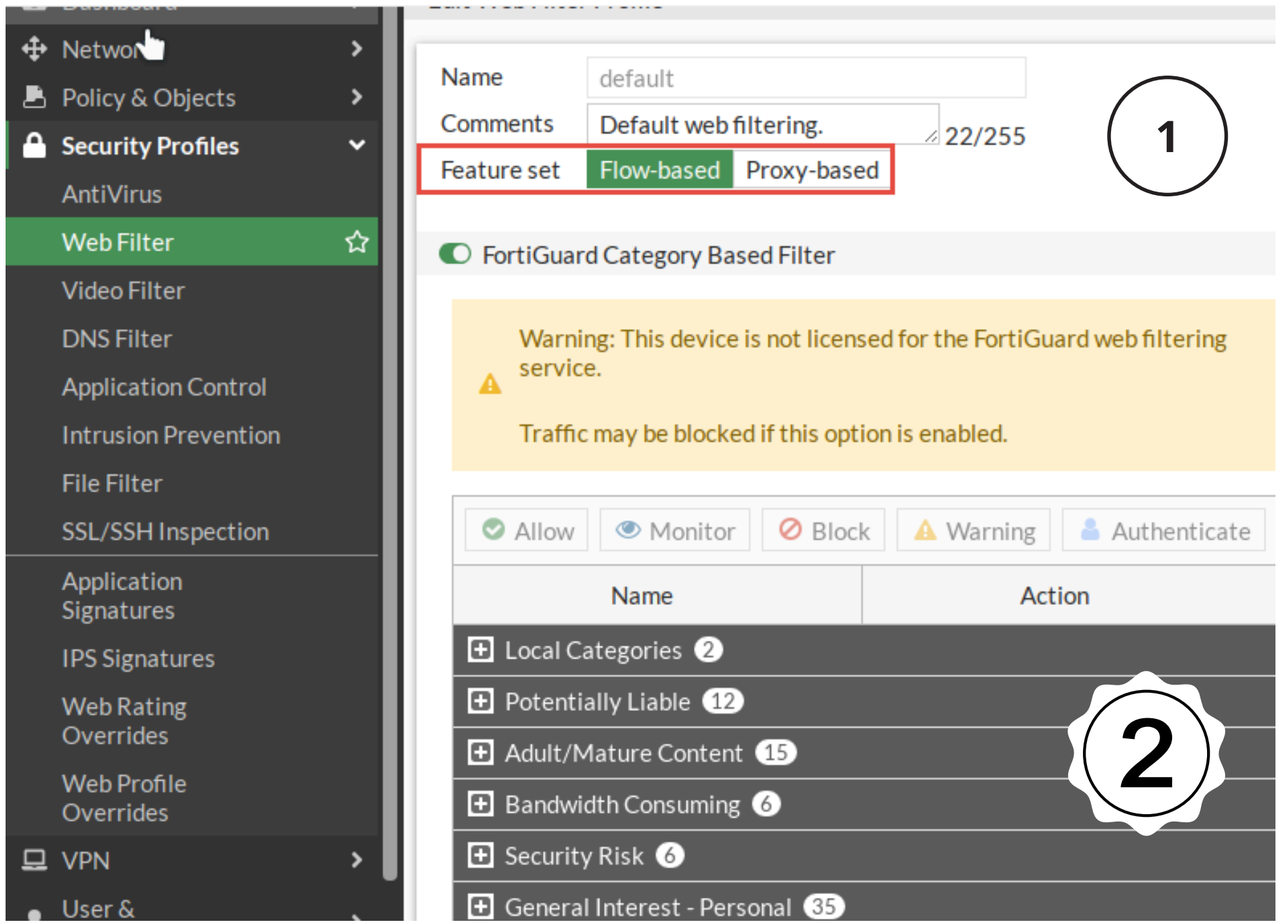


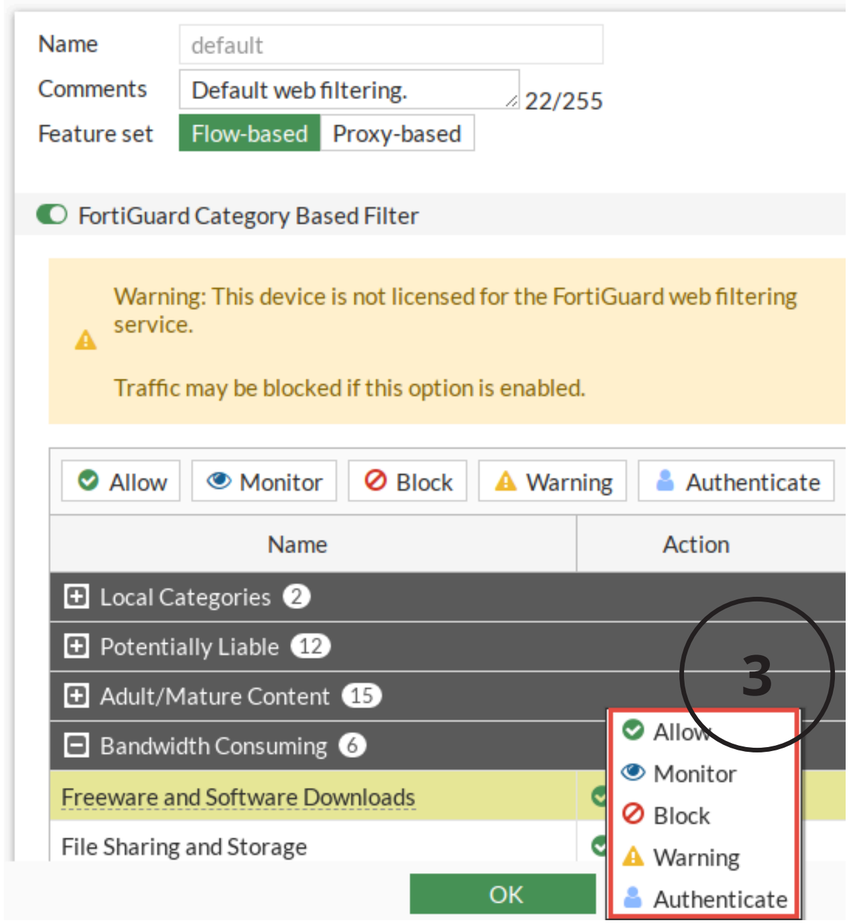
To configure FortiGate for web filtering based on FortiGuard categories, you must make sure that FortiGate has a valid FortiGuard security subscription license. The license provides the web filtering capabilities necessary to protect against inappropriate websites.

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Configuring FortiGuard Web Filtering



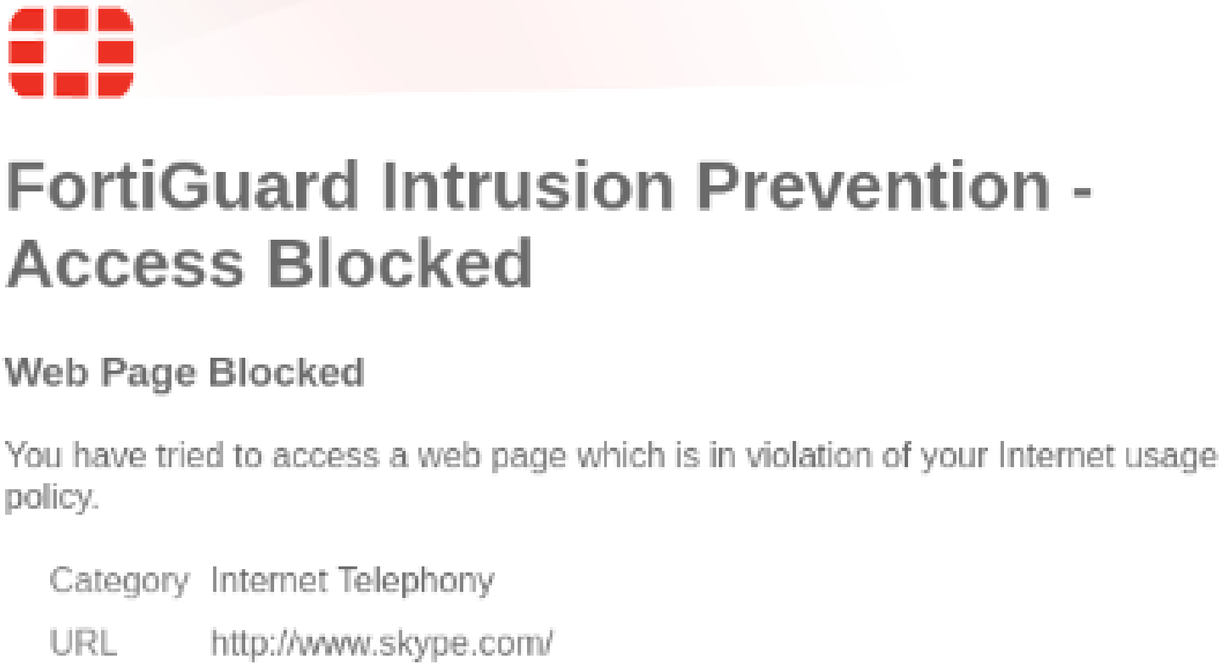


https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

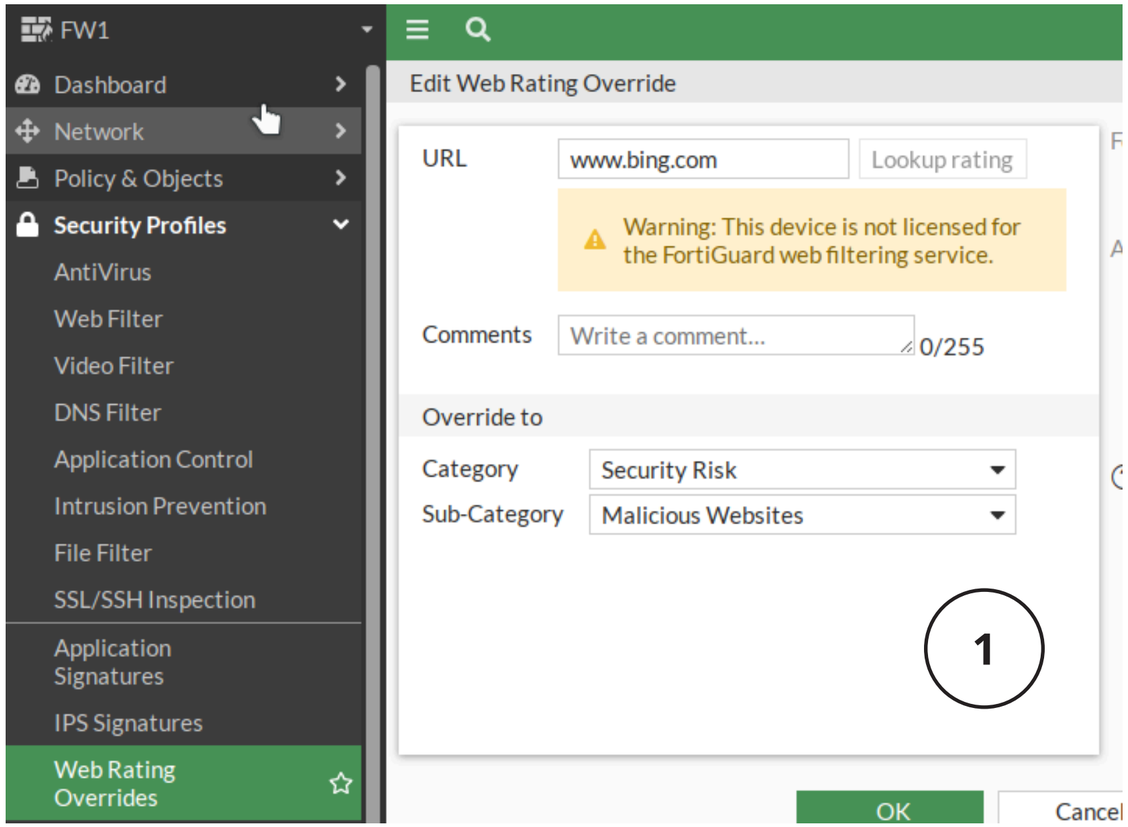
Configuring FortiGuard Web Filtering



رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Configuring FortiGuard Web Rating



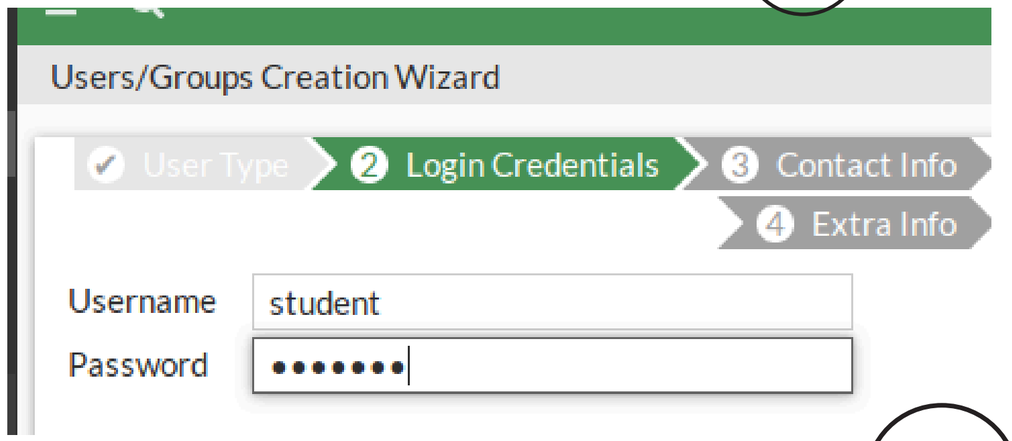
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

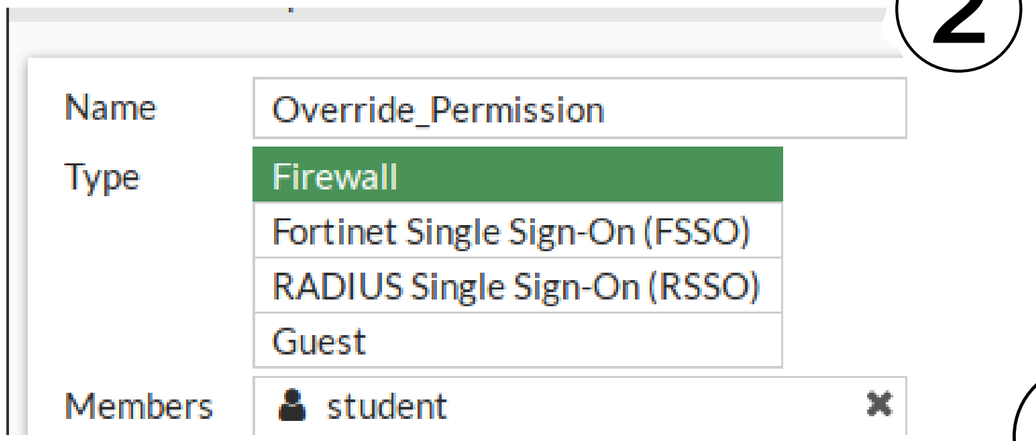
Setting Up Web Filtering Authentication

https://depi.gov.eg

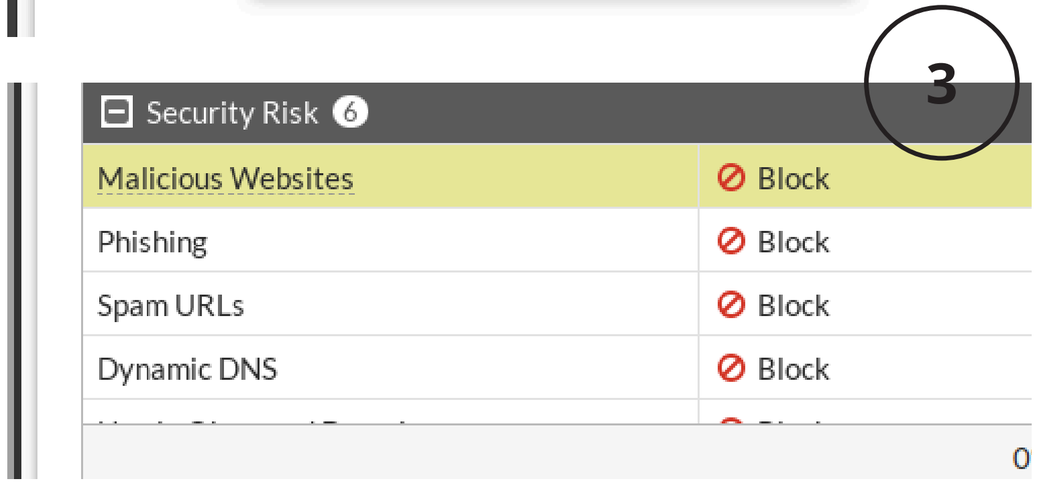
1



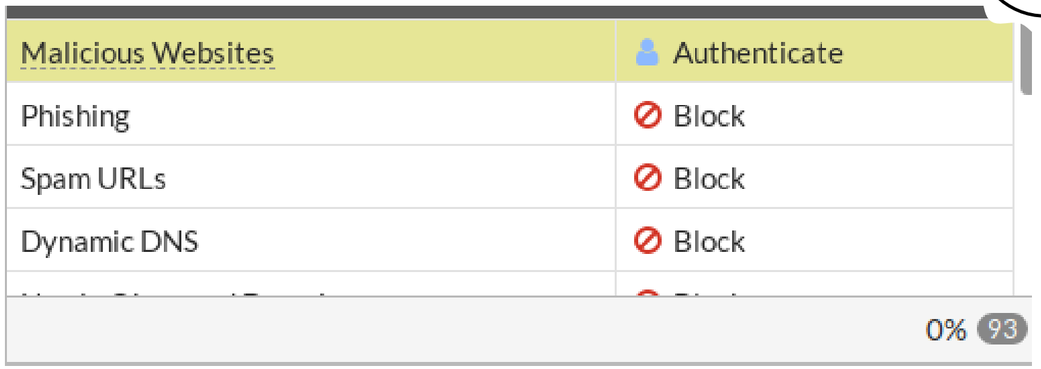
2



3



4

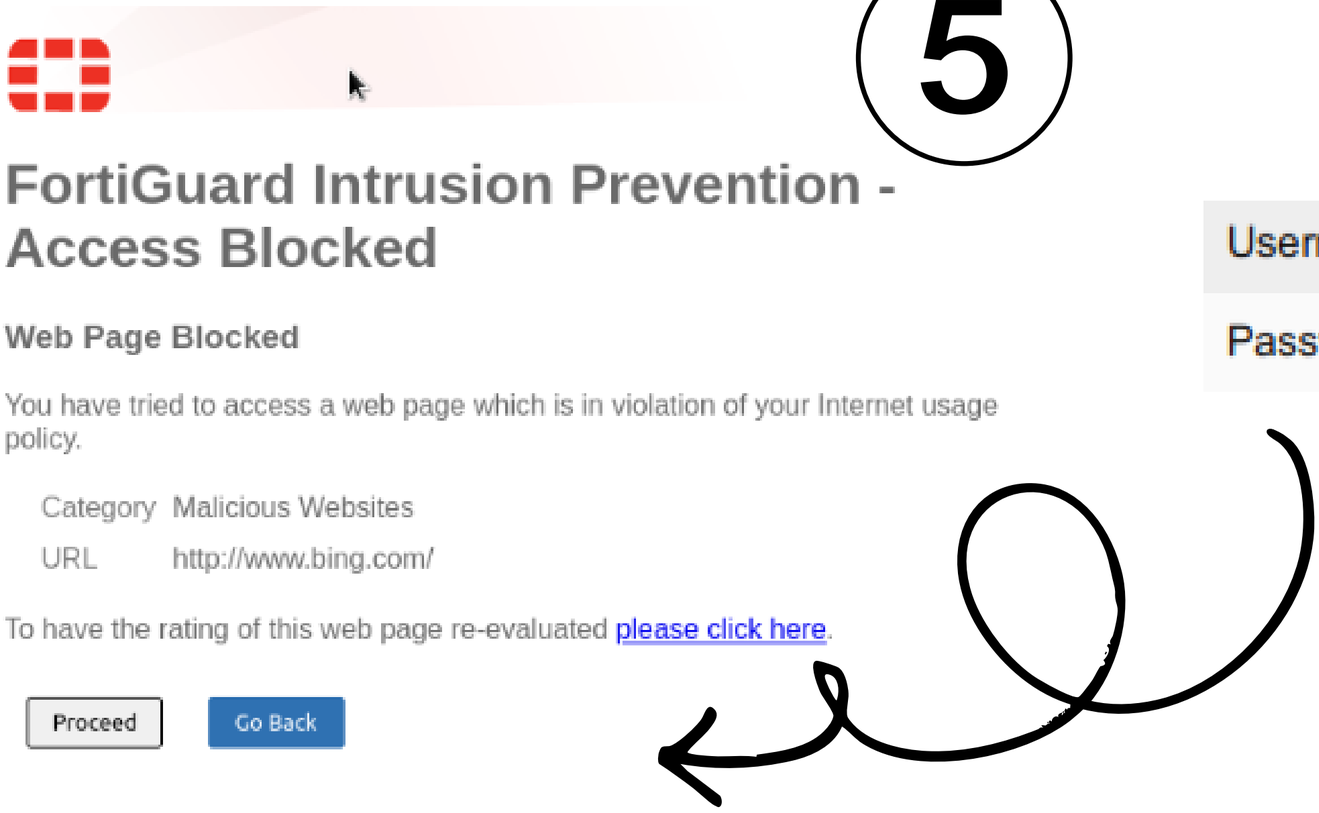


رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Setting Up Web Filtering Authentication

5

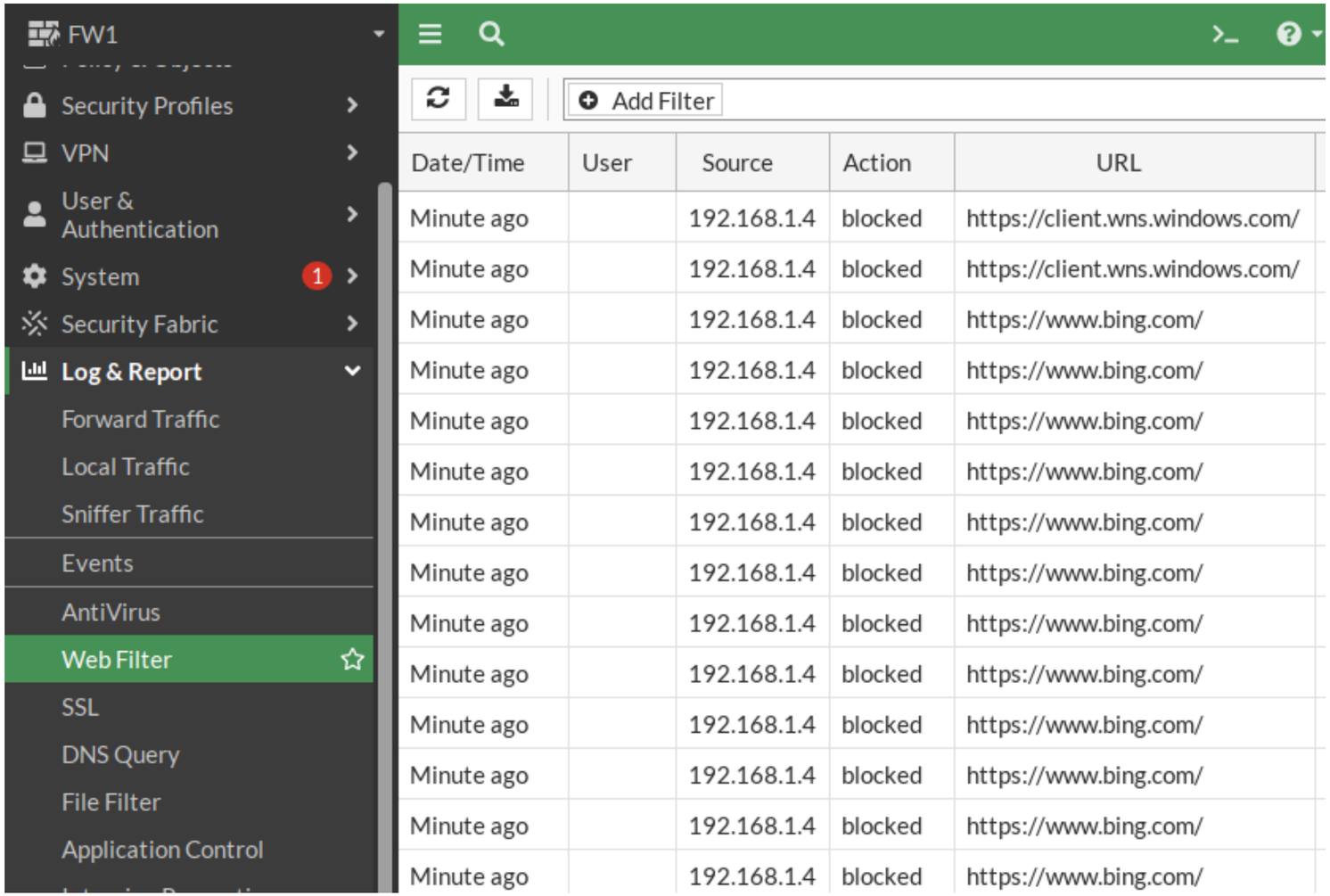


Username	student
Password	fortinet

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Login & Monitoring



https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Key Types of Security Profiles

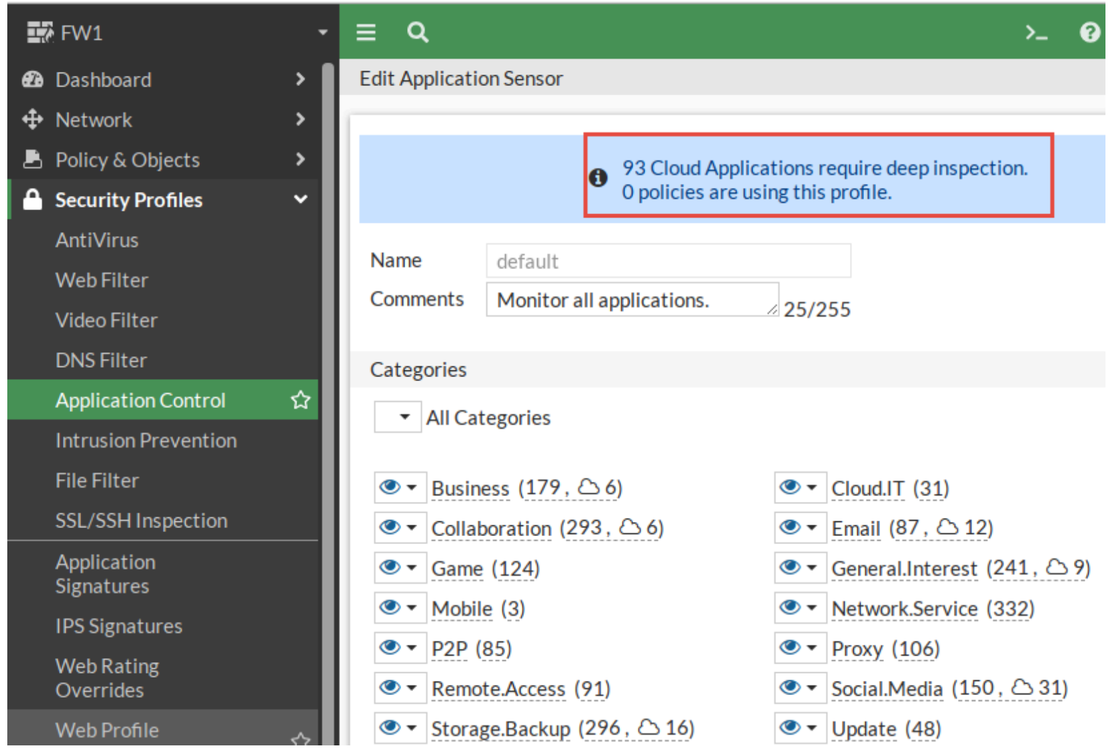
3-Application Control

- 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 .

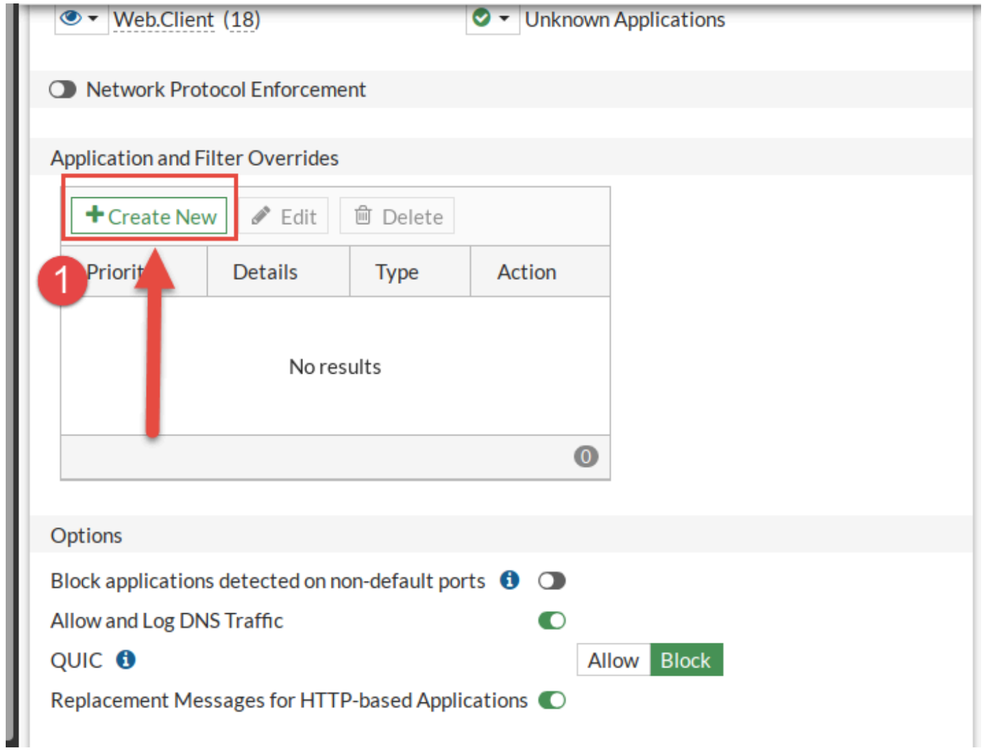
رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Controlling Application Traffic



1



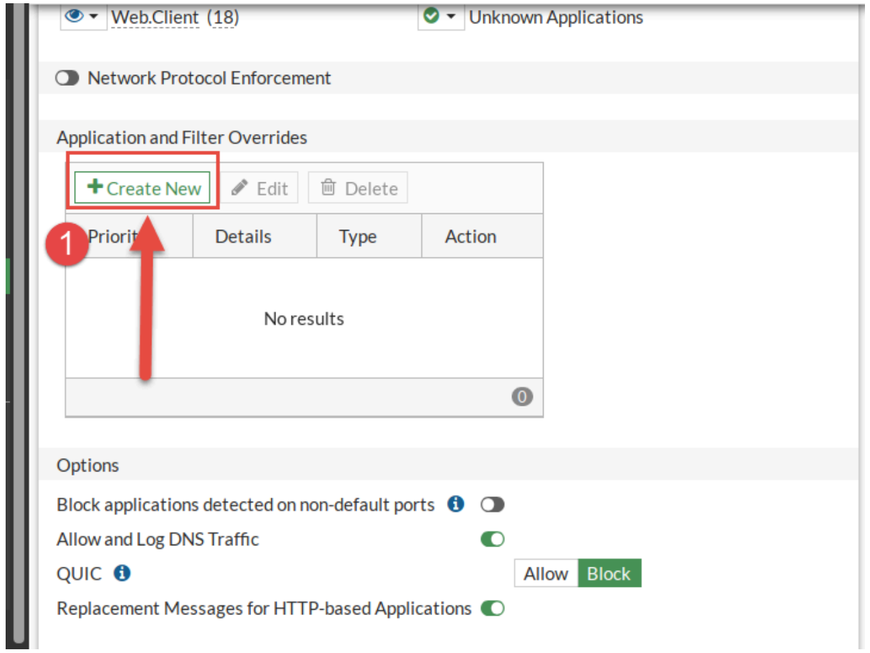
2

https://depi.gov.eg

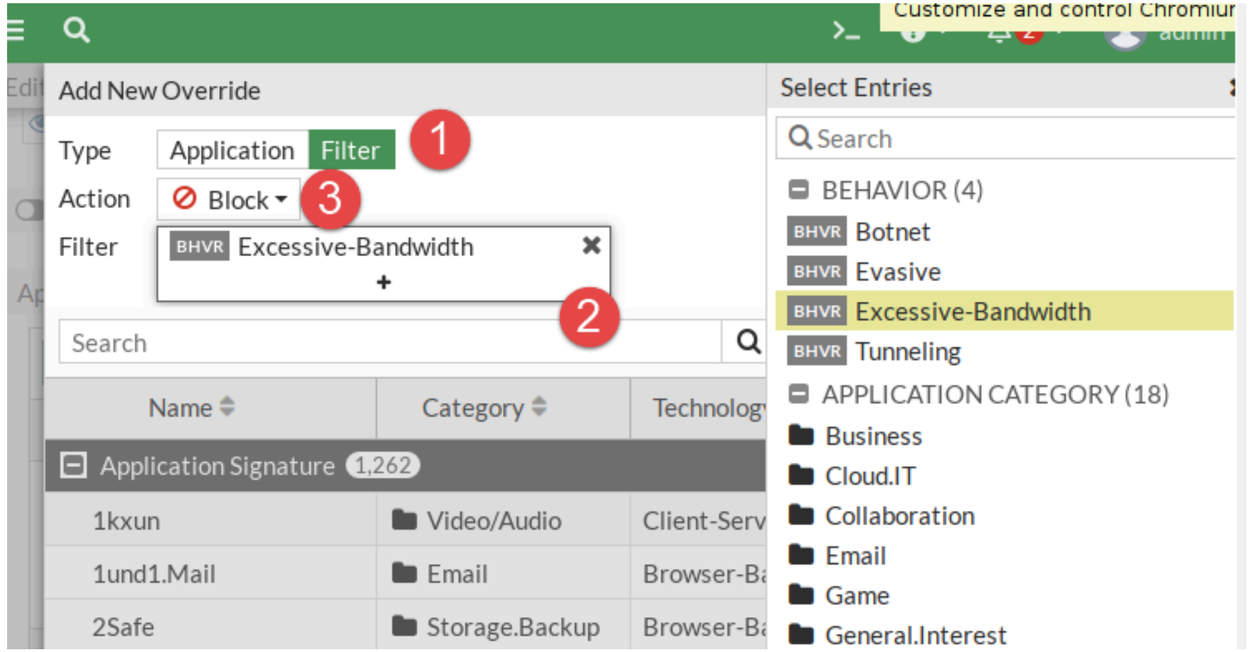
رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Controlling Application Traffic



3



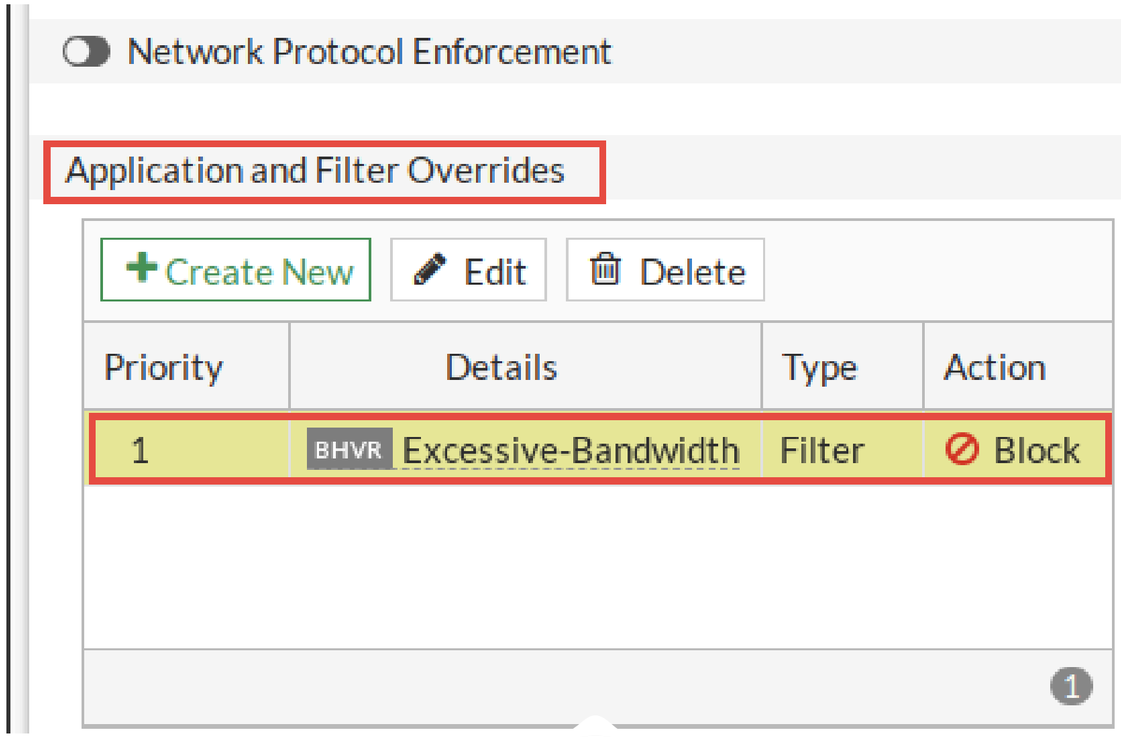
4

https://depi.gov.eg

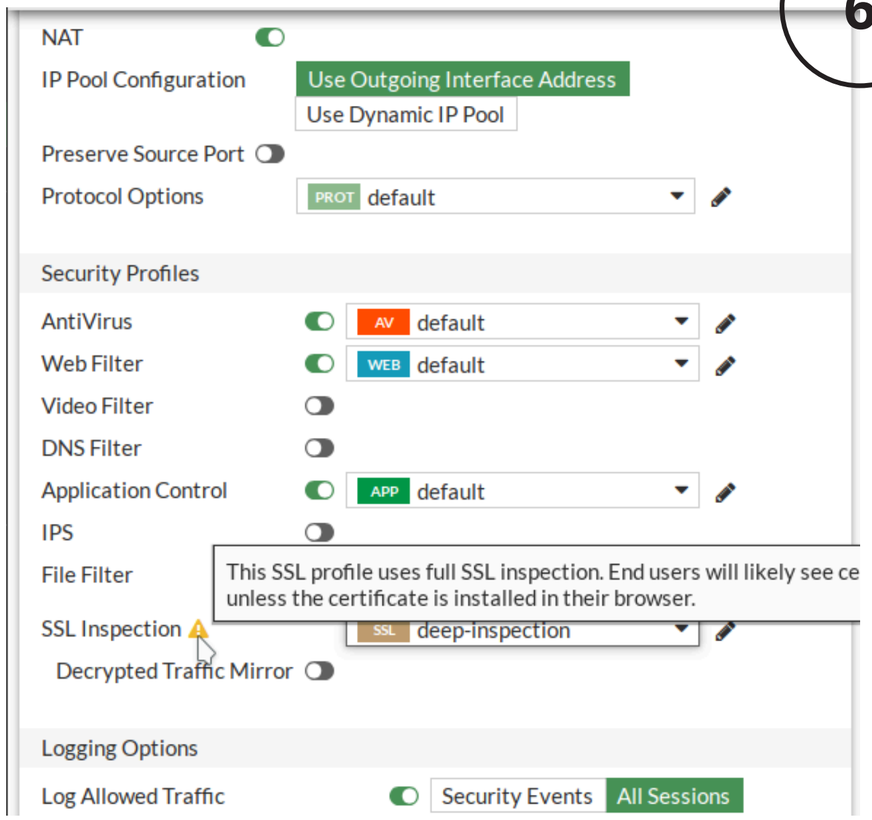
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Controlling Application Traffic



5



6

https://depi.gov.eg

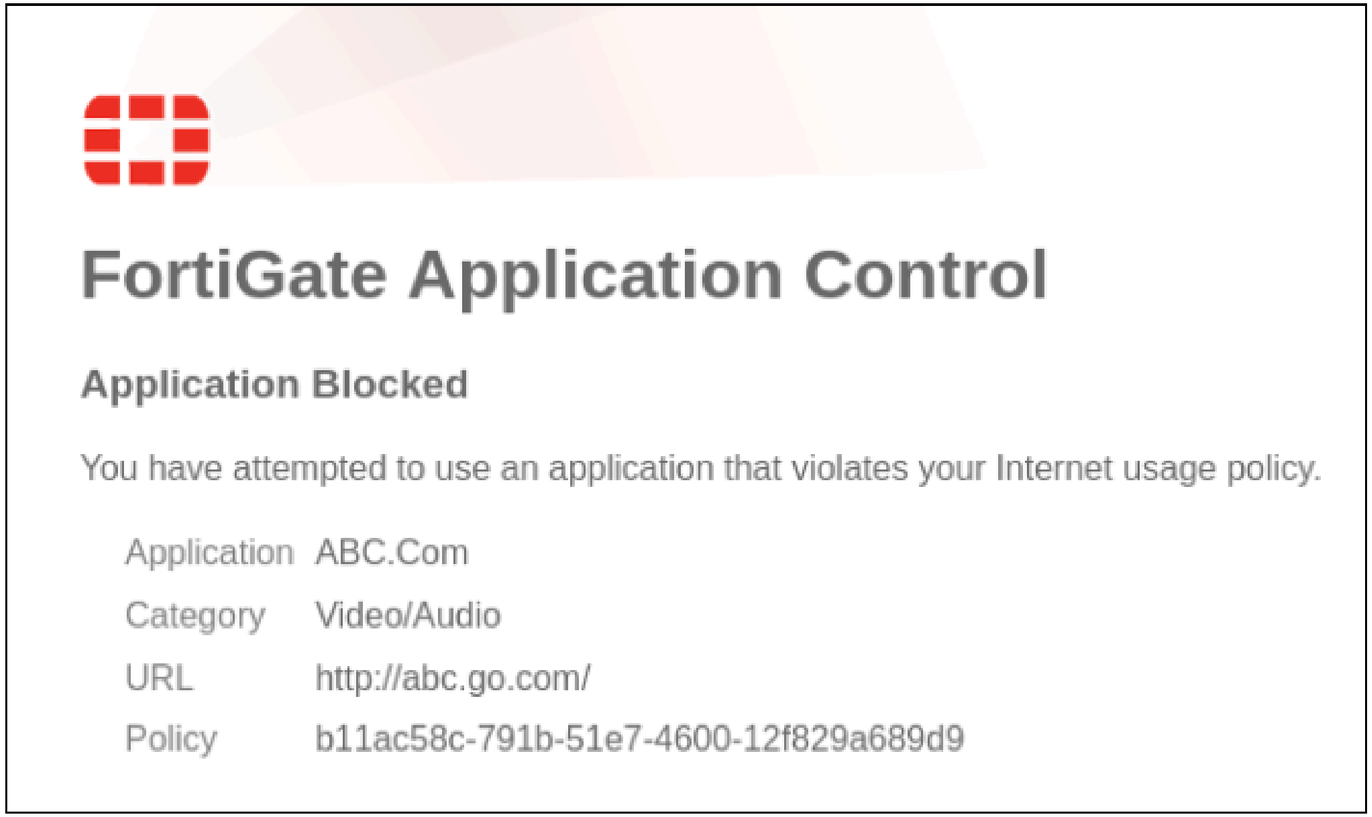
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

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.

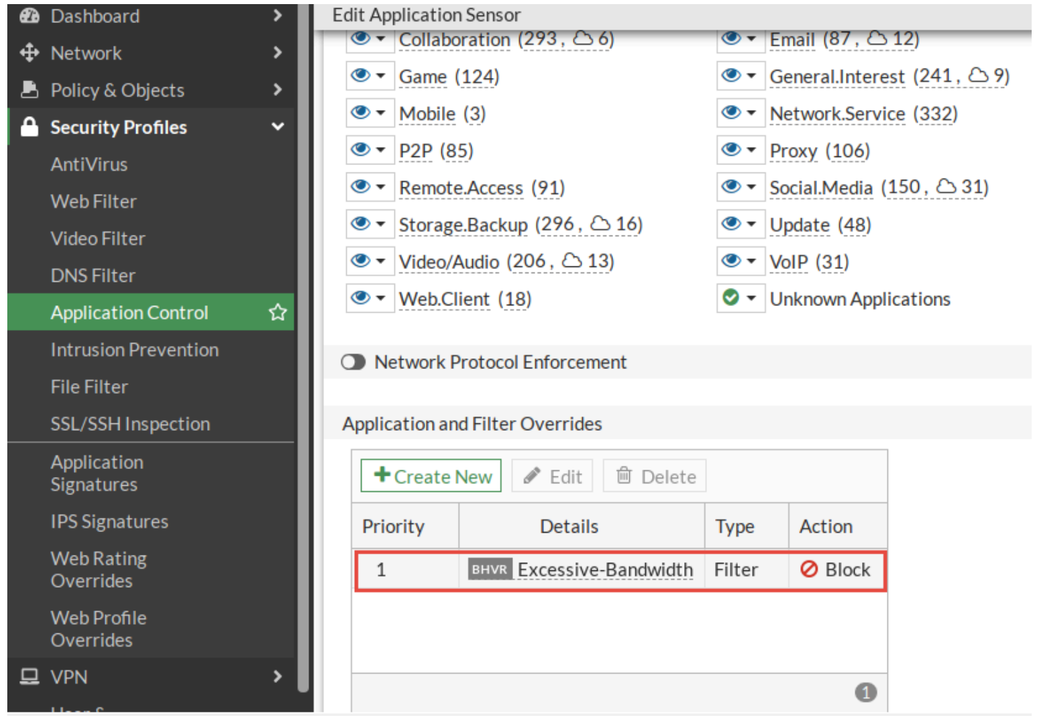


رواد مصر الرقمية

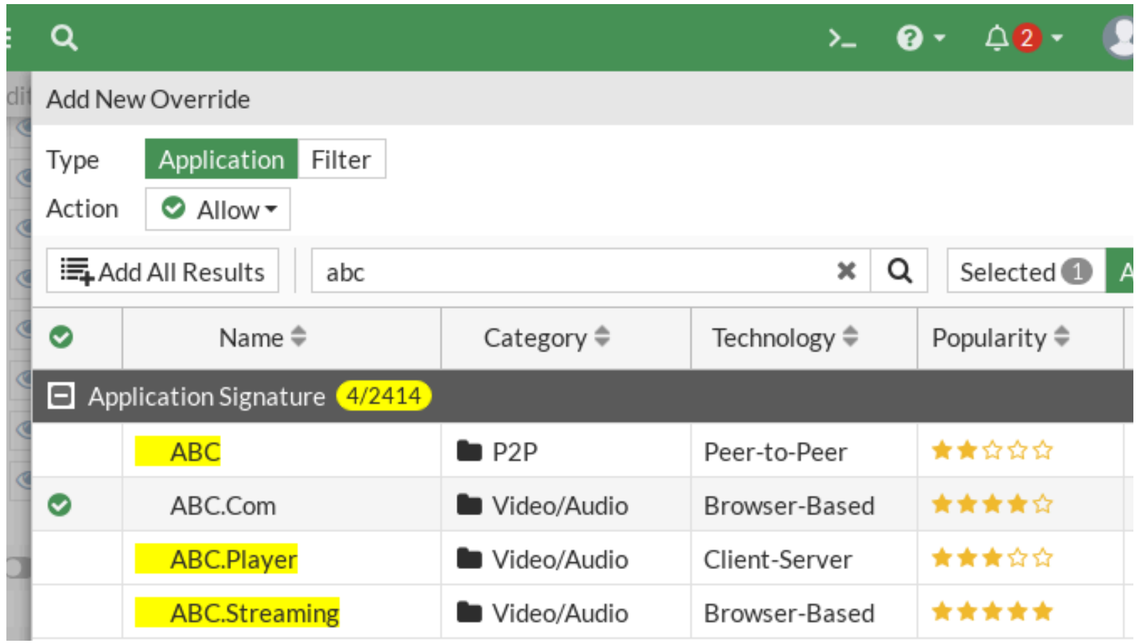
وزارة الاتصالات
وتكنولوجيا المعلومات

Configure Application Overrides

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



1



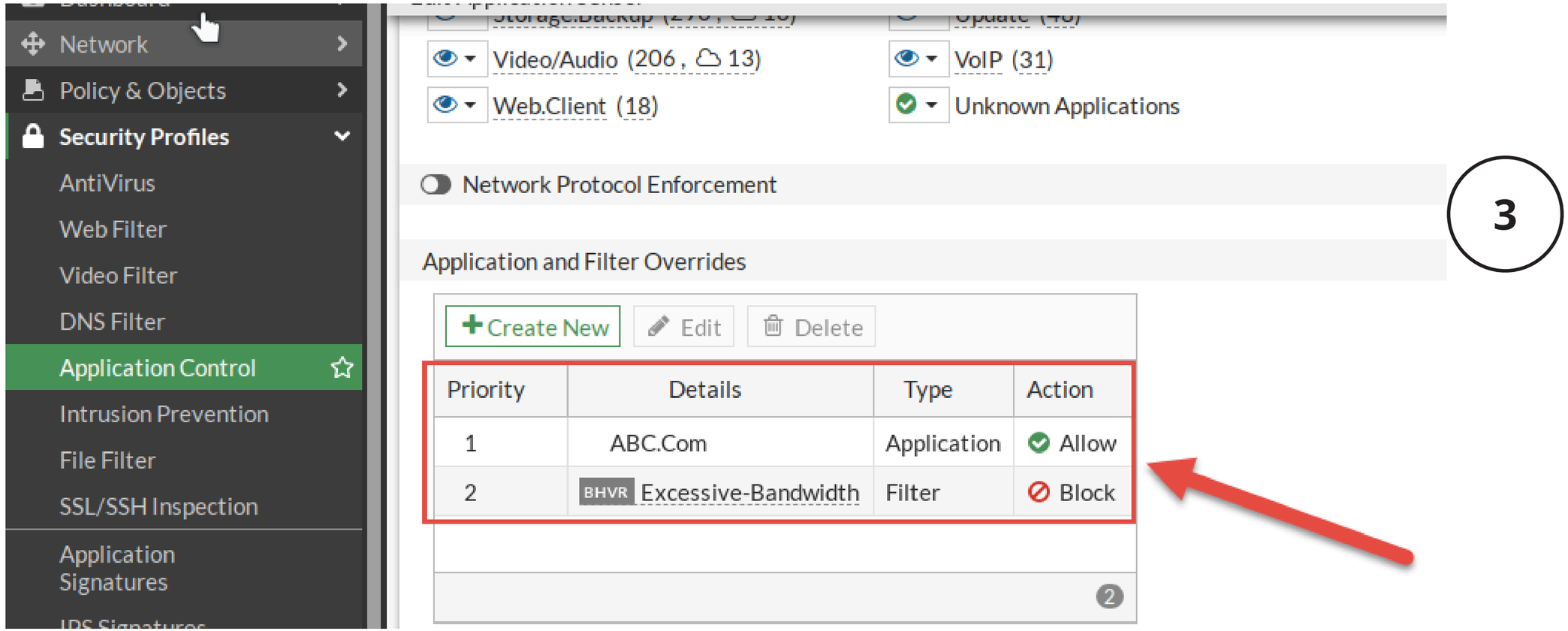
2

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Configure Application Overrides

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

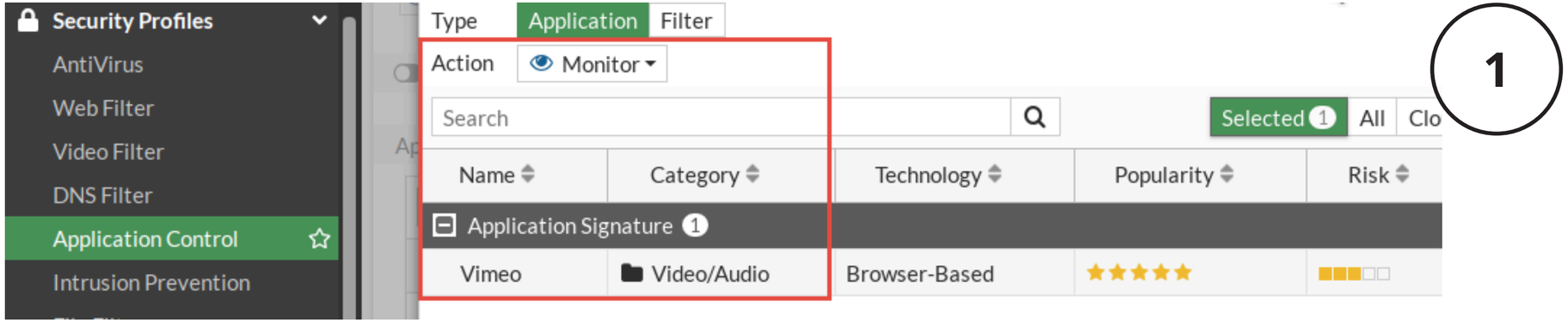


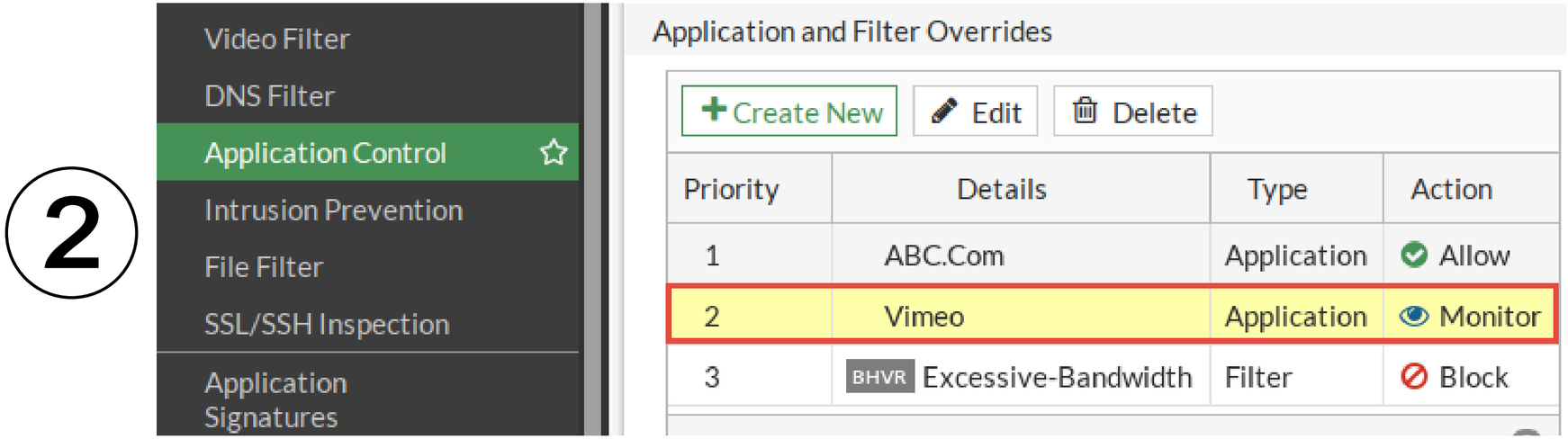
رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Controlling Application Bandwidth Usage

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





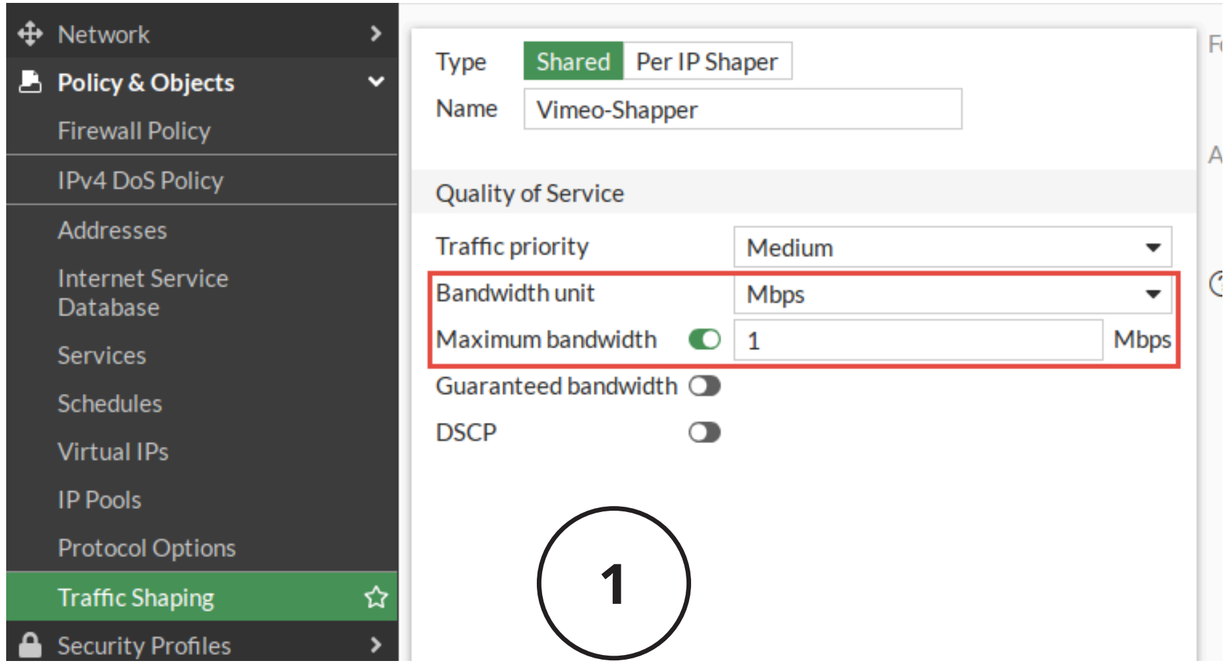
رواد مصر الرقمية

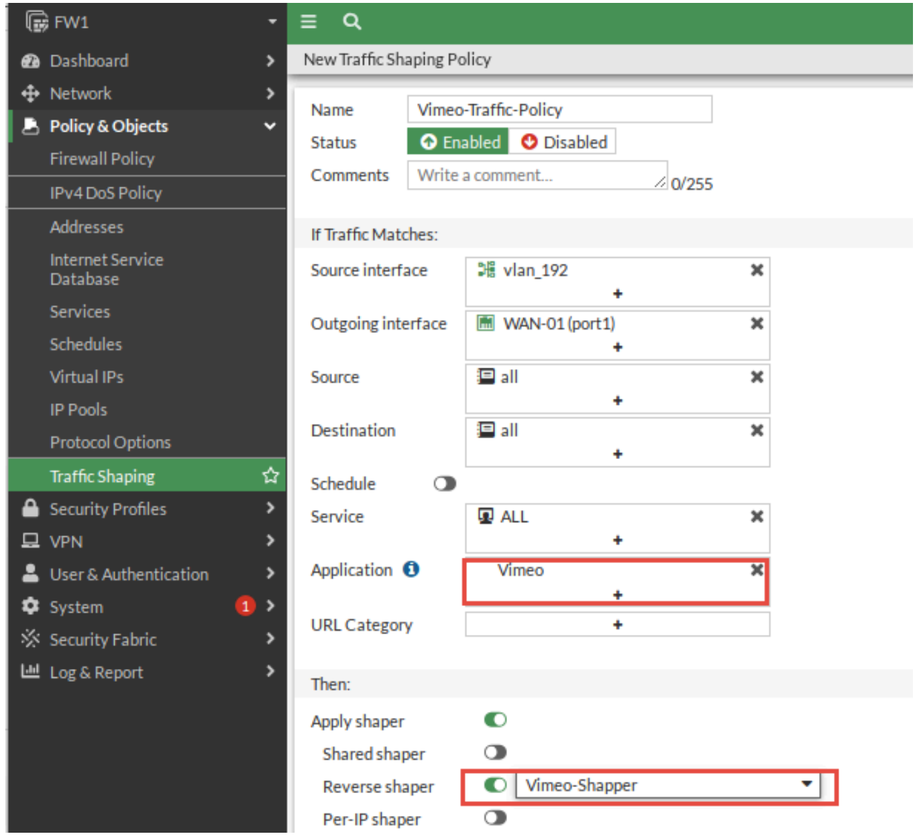
وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Controlling Application Bandwidth Usage

To Configure Bandwidth Usage need to Trafic Shaper

2





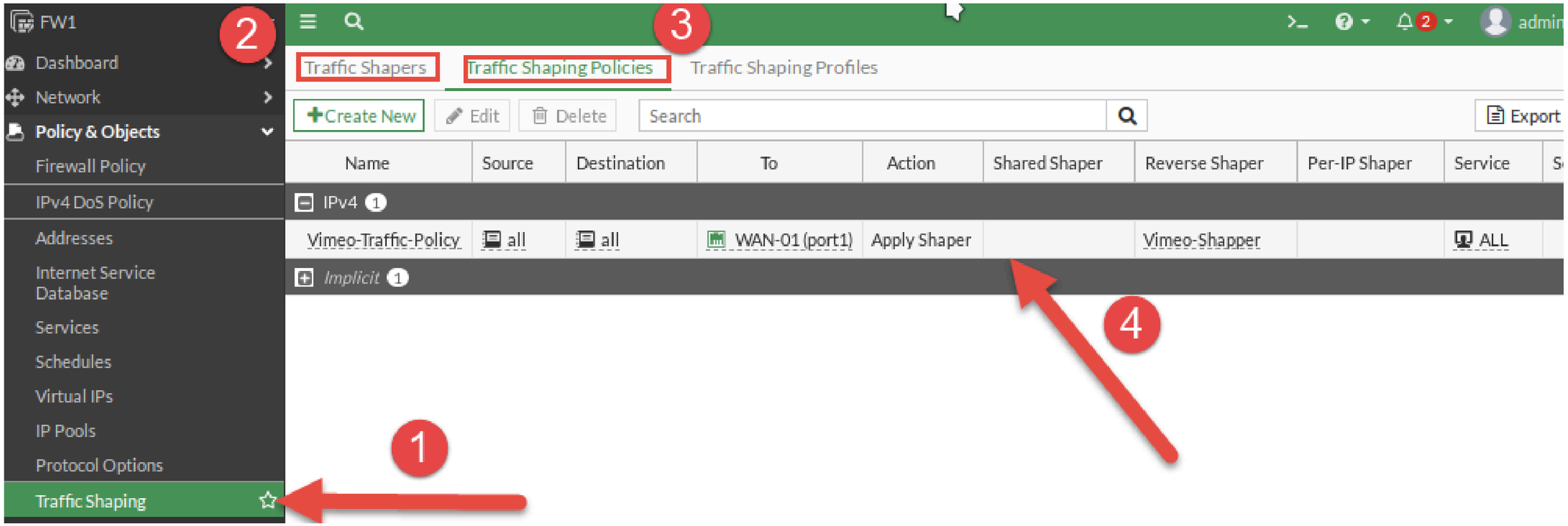
https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Controlling Application Bandwidth Usage

To Configure Bandwidth Usage need to Trafic Shaper



https://depi.gov.eg

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

THANK YOU

https://depi.gov.eg

› End Slide