

Advanced FortiGate Security Profiles

Infrastructure and Security – Fortinet Cybersecurity Engineer

Team Introduction

- Morkos Bekhit – Security Profiles Research
- Youssef Tarek – Configuration & Testing
- Youssef Rafeek – Monitoring & Logging
- Abdullah Ragab– Final Report & Presentation

Project Objective

- To understand and implement FortiGate Security Profiles
- Protect networks against advanced threats
- Monitor effectiveness and improve security posture

Project Timeline












- Week 1: Security Profile Research
- Week 2: Configuration
- Week 3: Monitoring and Reporting
- Week 4: Final Documentation and Presentation

What Are Security Profiles?

- FortiGate UTM Profiles applied to firewall policies
- Analyze and filter network traffic

Types of Security Profiles

- Antivirus
- Web Filtering
- Application Control
- IPS
- DNS Filtering

Security Profiles				
AntiVirus	<input checked="" type="checkbox"/>	AV	default	
Web Filter	<input checked="" type="checkbox"/>	WEB	default	
Video Filter	<input checked="" type="checkbox"/>	VF	video_filter	
DNS Filter	<input checked="" type="checkbox"/>	DNS	default	
Application Control	<input checked="" type="checkbox"/>	APP	default	
IPS	<input checked="" type="checkbox"/>	IPS	default	
File Filter	<input checked="" type="checkbox"/>	FILE	default	
Email Filter	<input checked="" type="checkbox"/>	EMAIL	default	
DLP Profile	<input checked="" type="checkbox"/>	DLP	default	
SSL Inspection 		SSL	deep-inspection	
Decrypted Traffic Mirror <input type="checkbox"/>				

Antivirus Profile

- Used Flow and Proxy-based inspection Modes
- Detects and removes malware in real-time

Antivirus and Inspection Modes

- Antivirus scanning engine uses antivirus signature databases to identify malicious codes

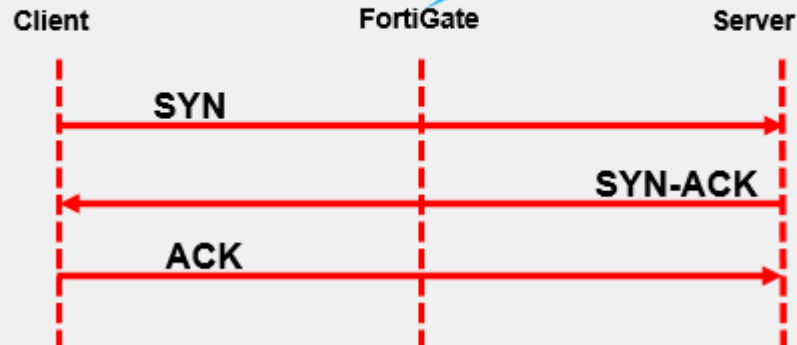


- Available inspection modes

- Flow-based inspection**

- Default inspection mode

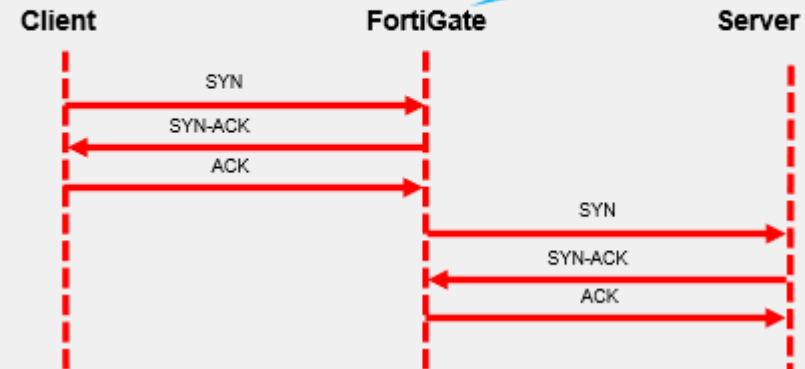
File is scanned on a flow basis



- Proxy-based inspection**

- Provides additional options

Two TCP connections



Flow-Based Inspection Mode

- Default mode

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ☒ **Block** ☐ Monitor

Inspected Protocols

HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>

Action applied to the infected files

Select protocols to be scanned

Policy & Objects > Firewall Policy

Create New Policy

Name:

Incoming Interface:

Outgoing Interface:

Source: +

Destination: +

Schedule: always

Service: +

Action: ☒ ACCEPT ☐ DENY

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: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

File Filter: ☐

SSL Inspection: ☐ SSL no-inspection

Select the antivirus profile

Proxy Inspection Mode Enabled

- Configure the antivirus profile
 - **Feature set is Proxy-based**
- Provides additional antivirus support
 - MAPI and SSH protocols inspection
 - Content disarm and reconstruction (CDR)
 - FortiNDR inspection

Feature visibility
activated through CLI

Available only in
proxy inspection mode

Security Profiles > AntiVirus

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	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input type="checkbox"/>
MAPI	<input checked="" type="checkbox"/>
SSH	<input checked="" type="checkbox"/>

APT Protection Options

Content Disarm and Reconstruction	<input checked="" type="checkbox"/>
Treat Windows executables in email attachments as viruses	<input checked="" type="checkbox"/>
Send files to FortiSandbox for inspection	<input type="checkbox"/>
Send files to FortiNDR for inspection	<input checked="" type="checkbox"/>
Include mobile malware protection	<input checked="" type="checkbox"/>
Quarantine	<input type="checkbox"/>

Firewall Policy With Proxy Inspection Mode

Policy & Objects > Firewall Policy

Create New Policy

Name

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

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 default

Security Profiles

AntiVirus ☒ ☒ default

Web Filter ☐ + Create

☒ Video Filter ☒ default ☒ with-default

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection ☐ SSL no-inspection

Set Inspection Mode to Proxy-based

Available only in proxy-based inspection mode


Proxy-based and flow-based antivirus profiles available

Detects and removes malware in real-time (Antivirus Logs)

Log & Report > Security Events

Summary Logs

3 Events

 **Antivirus**

Top Virus/Botnet	Action	Count
EICAR_TEST_FILE	Blocked	3

3 events

Summary Logs

Antivirus Disk 1 hour Details

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
2023/09/13 00:49:19	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:49:19	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:49:19	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	Blocked
2023/09/13 00:43:57	HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	Blocked
2023/09/13 00:43:12	HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	Blocked

Log entry when a virus is detected

Details on the virus with FortiGuard reference

Log Details

Protocol 6
Service HTTP

Data

File Name eicar.com

Action

Action Blocked
Threat 2
Policy ID 1 (Full Access)
Policy UUID b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type Firewall

Security

Level Warning
Threat Level Critical
Threat Score 50

Cellular

Service HTTP

Antivirus

Profile default
Virus/Botnet EICAR_TEST_FILE
Virus ID 2,172
Reference http://www.fortinet.com/ve?vm=EICAR_TEST_FILE
Detection Type cached
Direction Incoming
Quarantine Skip Quarantine-disabled
Submitted to FortiSandbox false
Message File is infected.

Web Filtering Profile

- Block or allow URLs by category
- Enforces company browsing policies

Configure Web Filter Profiles—Flow Based

- Apply web filter profile to a flow-based firewall policy

Select **Flow-based**

Enable **FortiGuard Category Based Filter** and configure each category

Enable and configure **Static URL Filter** if needed

Enable and configure **Rating Options** if needed

Security Profiles > Web Filter

New Web Filter Profile

Name WebFilter
Comments Write a comment... 0/255
Feature set **Flow-based** Proxy-based

☒ FortiGuard Category Based Filter

☒ Static URL Filter

Block invalid URLs ☐
URL Filter ☐
Block malicious URLs discovered by FortiSandbox ☐
Content Filter ☐

☒ Rating Options

Allow websites when a rating error occurs ☐
Rate URLs by domain and IP Address ☐

Configure Web Filter Profiles—Proxy Based

- Apply a web filter profile to a flow-based firewall policy

Select **Proxy-based**

Feature available only in proxy-based

Security Profiles > Web Filter

New Web Filter Profile

Name: WebFilter

Comments: Write a comment... 0/255

Feature set: Flow-based **Proxy-based**

☐ FortiGuard Category Based Filter

☐ Allow users to override blocked categories

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☒ **P**

Restrict YouTube Access ☒ **P**

Log all search keywords ☒ **P**

Static URL Filter

Rating Options

Proxy Options

Restrict Google account usage to specific domains ☒ **P**

HTTP POST Action **Allow** **Block**

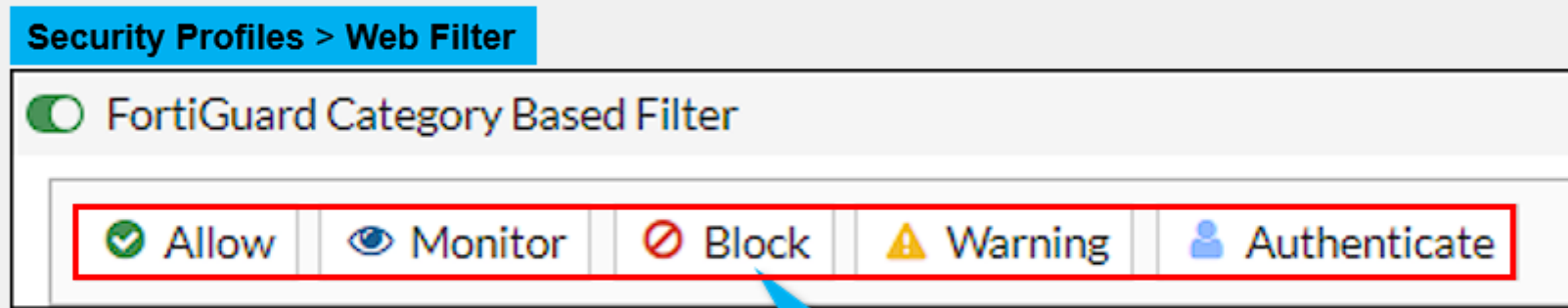
Remove Java Applets ☒ **P**

Remove ActiveX ☒ **P**

Remove Cookies ☐

FortiGuard Category Filter

- Websites split into multiple categories
- Live connection to FortiGuard with active contract required
- Can use FortiManager instead of FortiGuard



Available actions per category

IPS and DNS Filtering

- **IPS: Intrusion Prevention System (IPS)** analyzes network traffic for malicious patterns, blocking exploits and attacks that target vulnerabilities in systems and applications.
- **DNS Filtering:** This security measure prevents users from accessing malicious or inappropriate websites by filtering domain name system (DNS) requests.

Configuring IPS Sensors

- Add individual signatures
- Add groups of signatures using filters

Security Profiles > Intrusion Prevention

New IPS Sensor

Name:

Comments: 0/255

Block malicious URLs: ☐

IPS Signatures and Filters

+ Create New

Details	Exempt IPs	Action	Packet Logging
No results			

Add Signatures

Type: **Signature**

Action:

Packet logging: ☒ Enable ☐ Disable

Status: ☒ Enable ☐ Disable

Rate-based settings:

Exempt IPs:

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature: 5,054					
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■■	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Disclosure	■■■■■	Client	Windows	Pass	CVE-2005-0278
3Com.Intelligent.Management.Center.Information.Disclosure	■■■■■	Server	Windows	Block	

Add Signatures

Type: **Filter** **Signature**

Action:

Packet logging: ☒ Enable ☐ Disable

Status: ☒ Enable ☐ Disable

Filter:

TGT	Server	x
SEV	■■■■■	x
PROT	HTTP	x
OS	Windows	x

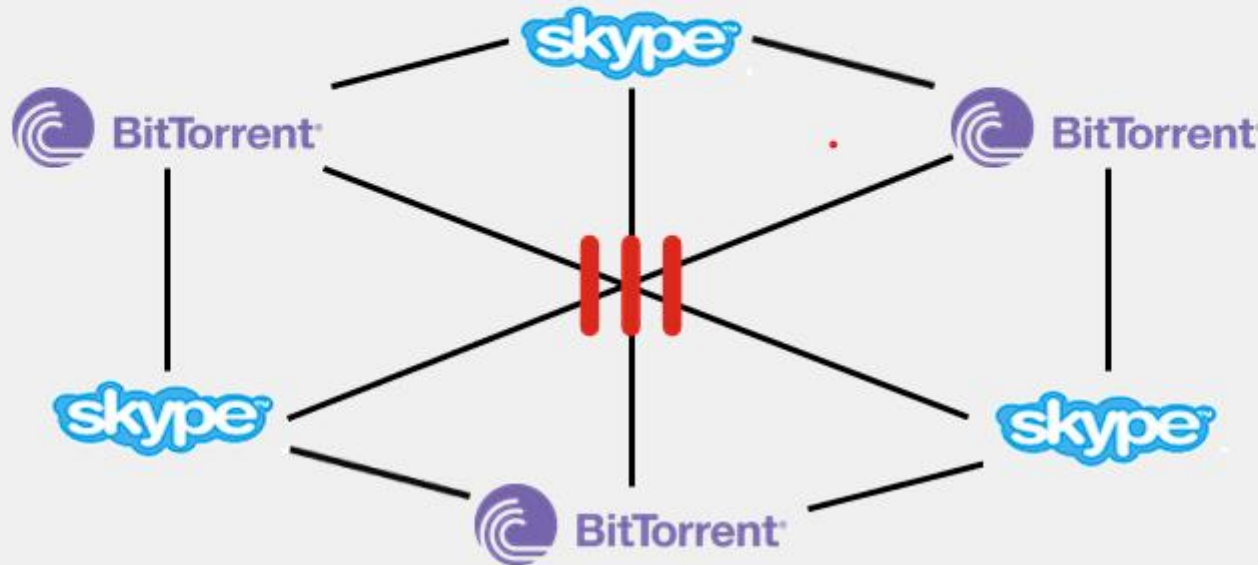
Name	Severity	Target	OS	Action	CVE-ID
IPS Signature: 644/576					
Adobe.Acrobat.And.Reader.TrueTypeFont.Parsing.Buffer.Overflow	■■■■■	Server Client	All	Block	CVE-2012-0774
Adobe.Acrobat.BMPCOLORS.Parsing.Memory.Corruption	■■■■■	Server Client	Windows MacOS	Block	CVE-2011-4373

Application Control

- Identify apps based on signatures and behavior
- Block unwanted applications like proxy/VPNs

Application Control

- Uses the IPS engine in flow-based scan
- Detects and acts on network application traffic
- Appropriate for detecting peer-to-peer (P2P) applications



Configuring an Application Control in Profile Mode

Security Profiles > Application Control

Edit Application Sensor

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

Name: default
Comments: Monitor all applications. 25/255

Categories

☒ Mixed All Categories

<input checked="" type="checkbox"/> Business (157, ☁ 6)	<input checked="" type="checkbox"/> Cloud/IT (68, ☁ 1)	<input checked="" type="checkbox"/> Collaboration (271, ☁ 16)
<input checked="" type="checkbox"/> Email (77, ☁ 12)	<input checked="" type="checkbox"/> Game (86)	<input checked="" type="checkbox"/> General Interest 238, ☁ 12
<input checked="" type="checkbox"/> Mobile (3)	<input checked="" type="checkbox"/> Network Service (333)	<input checked="" type="checkbox"/> Operational Technology
<input checked="" type="checkbox"/> P2P (56)	<input checked="" type="checkbox"/> Proxy (184)	<input checked="" type="checkbox"/> Remote Access (99)
<input checked="" type="checkbox"/> Social Media (118, ☁ 30)	<input checked="" type="checkbox"/> Storage/Backup (160, ☁ 19)	<input checked="" type="checkbox"/> Update (49)
<input checked="" type="checkbox"/> Video/Audio (155, ☁ 17)	<input checked="" type="checkbox"/> VoIP (24)	<input checked="" type="checkbox"/> Web Client (25)
<input checked="" type="checkbox"/> Unknown Applications		

☐ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
No results			

Applies an action to all categories at once

Applies an action to one category

Matches traffic to unidentified applications

Creates specific actions for a single application or group of applications

The number to the right of the cloud symbol indicates the number of cloud applications in the category

Applying an Application Control Profile in Profile Mode

- You must apply the **Application Control** profile on a firewall policy to scan the passing traffic

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input checked="" type="checkbox"/> APP default
IPS	<input type="checkbox"/>
File Filter	<input type="checkbox"/>
SSL Inspection ⚠	SSL deep-inspection
Decrypted Traffic Mirror <input type="checkbox"/>	

Logging Options

Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events All Sessions
---------------------	---

Enable **Application Control** and select the profile

Use **deep-inspection** profile to scan encrypted traffic

Enable logging

List of Application Signatures

Security Profiles > Application Control

New Application Sensor

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

Name
Comments 0/255

Categories

Mixed All Categories

- Business (157, 6)
- Collaboration (271, 16)
- Game (86)
- Mobile (3)
- Operational Technology
- Proxy (184)
- Social Media (118, 30)
- Update (49)
- VoIP (24)
- Unknown Applications
- Cloud/IT (68, 1)
- Email (77, 12)
- General Interest (238, 12)
- Network Service (333)
- P2P (56)
- Remote Access (99)
- Storage/Backup (160, 19)
- Video/Audio (155, 17)
- Web Client (25)

Firmware & General Updates License
✓ Licensed (Expiration Date: 2026/01/19)

Application Control Signatures Package
Version 25.00619

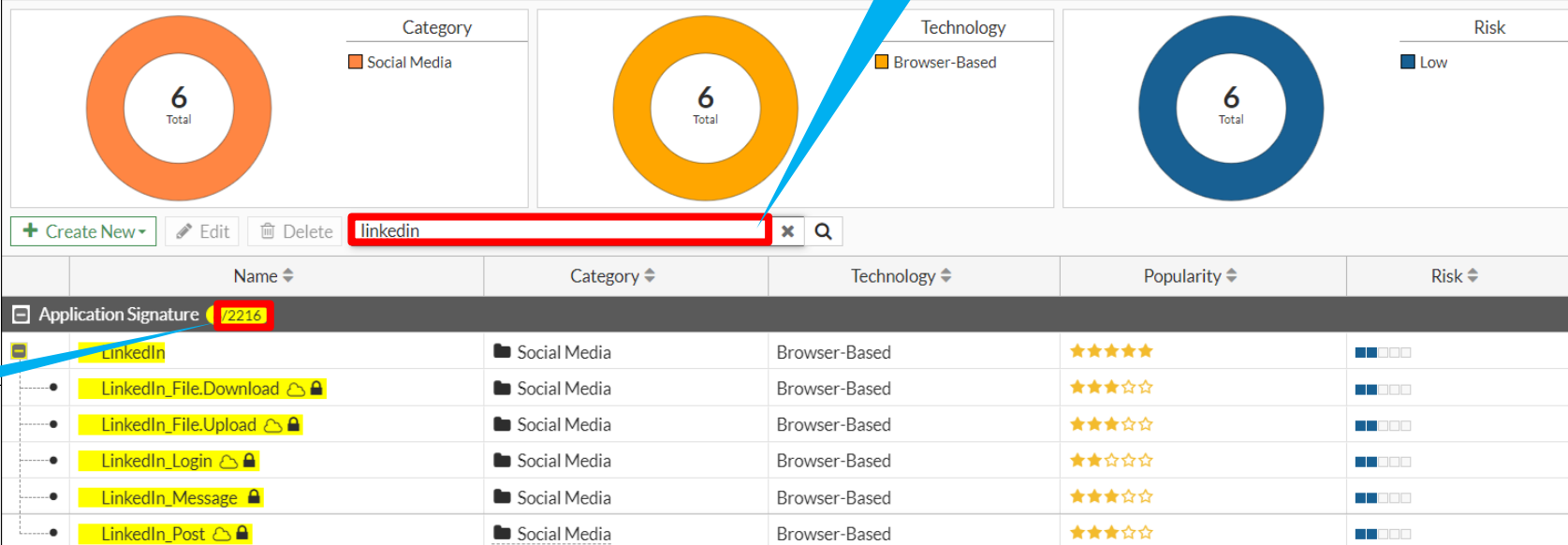
Application Signatures

View Application Signatures

Additional Information

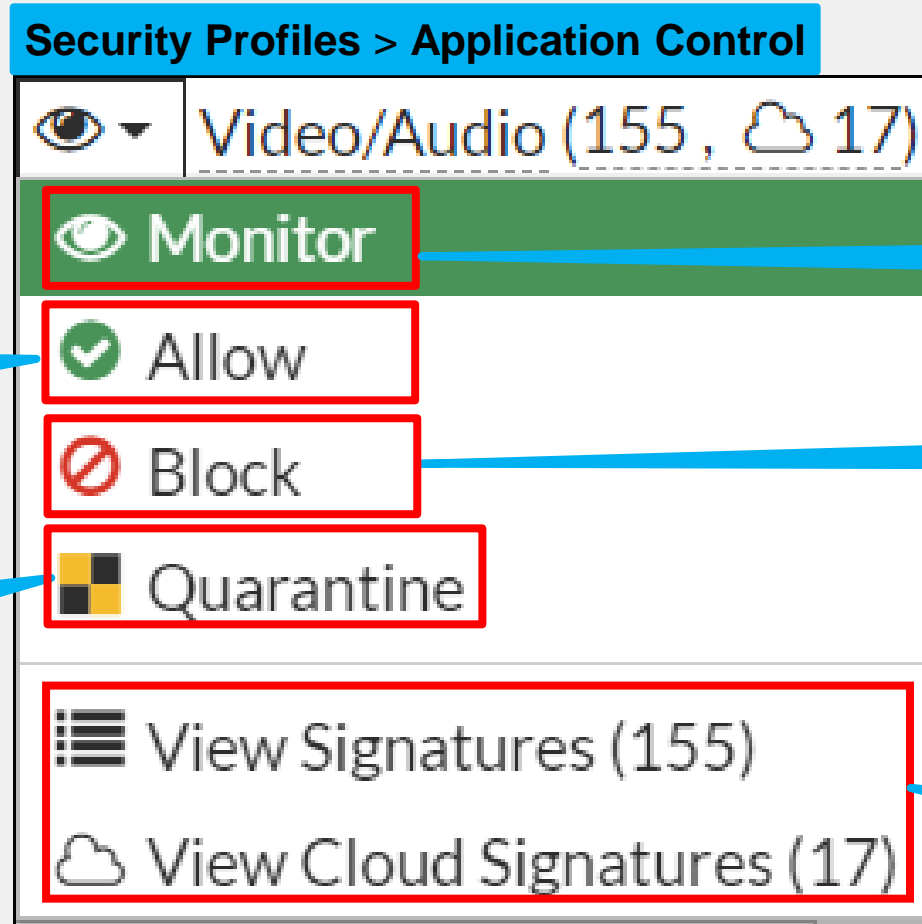
Filter option

View Application Signatures



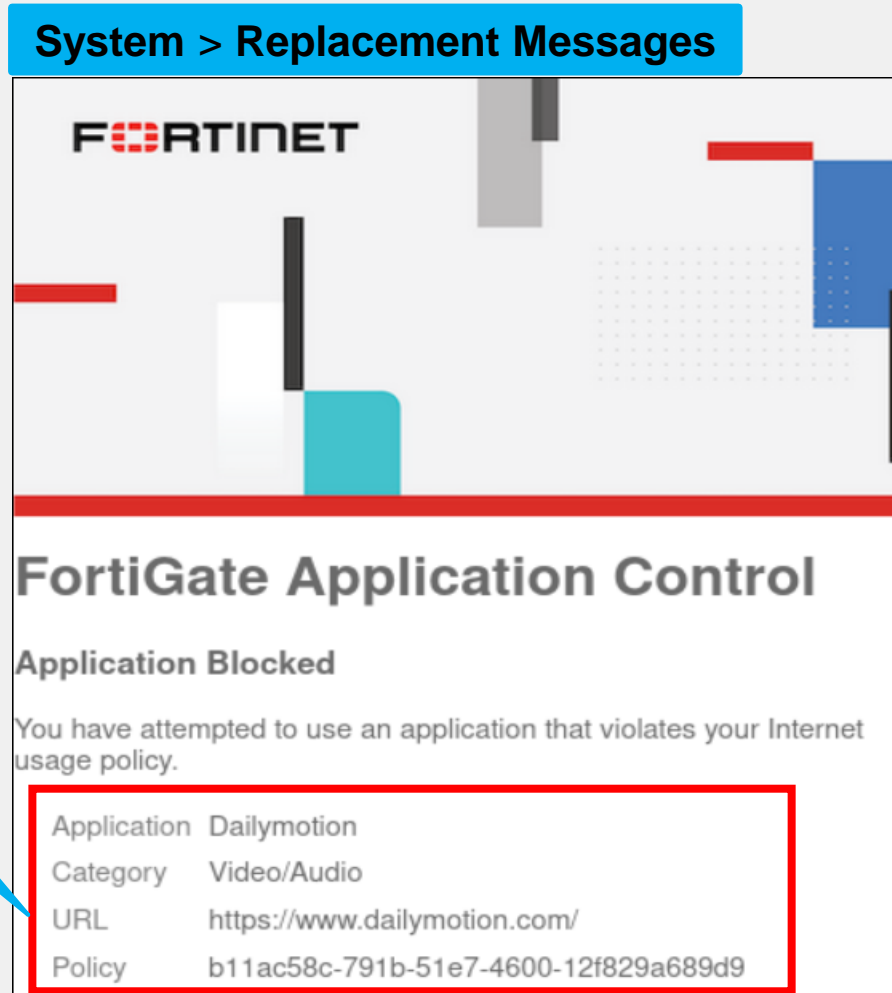
Active signature database

Filters Actions



HTTP Block Page

- Application control HTTP block pages in profile mode



Information related to the HTTP page being blocked

Configuration Overview

- Configured profiles via GUI and CLI
- Applied to outbound internet policy
- CLI Example:

config firewall policy

set av-profile "AV-Custom"

set webfilter-profile "WF-Strict"

Configured profiles via CLI

```
config firewall policy
edit 10
    set name "Secure-Access"
    set srcintf "lan"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set av-profile "AV-Custom"
    set webfilter-profile "WF-Strict"
    set application-list "App-Control-1"
next
end
```

Configured profiles via GUI

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus	<input checked="" type="checkbox"/>	AV	default	▼	✎
Web Filter	<input checked="" type="checkbox"/>	WEB	default	▼	✎
Video Filter	<input checked="" type="checkbox"/>	VF	video_filter	▼	✎
DNS Filter	<input checked="" type="checkbox"/>	DNS	default	▼	✎
Application Control	<input checked="" type="checkbox"/>	APP	default	▼	✎
IPS	<input checked="" type="checkbox"/>	IPS	default	▼	✎
File Filter	<input checked="" type="checkbox"/>	FILE	default	▼	✎
Email Filter	<input checked="" type="checkbox"/>	EMAIL	default	▼	✎
DLP Profile	<input checked="" type="checkbox"/>	DLP	default	▼	✎
SSL Inspection ⚠		SSL	deep-inspection	▼	✎
Decrypted Traffic Mirror	<input type="checkbox"/>				

Monitoring

- FortiView dashboards
- Monitoring Application Control Logging

Security Dashboard

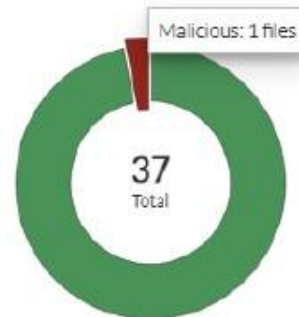
- Security widget and dashboard allow you to monitor your network



Drill down for further details

Dashboard

Advanced Threat Protection Statistics



FortiGate Scanned Files 37

Clean	36
Malicious	1
Suspicious	0
FortiGuard Outbreak Pre...	0
External Malware Block L...	0
EMS Threat Feed	0

Security widget

Monitoring Application Control Logging

Log & Report > Security Events

Summary Logs

51 Events

A Application Control [🔗](#)

Top Category	Action	Count
Web.Client	Pass	40
Network.Service	Block	5
Video/Audio	Block	3

Summary **Logs**

A Application Control Disk 5 minutes **Details**

Search

Date/Time	Source	Destination	Application Name	Action
2023/09/29 07:38:41	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	WebSocket	Block
2023/09/29 07:38:41	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	HTTPS.BROWSER	Pass
2023/09/29 07:38:32	10.0.1.10	185.125.190.58 (prod-ntp-5.ntp1.ps...)	NTP	Pass
2023/09/29 07:38:01	10.0.1.10	34.117.65.55 (autopush.prod.mozaw...)	WebSocket	Block

Application Control information

Log Details

Application Control

Sensor	default
Application Name	Dailymotion
Application ID	16072
Category	Video/Audio
Application Risk	Low
Protocol	6
Service	HTTP
Message	Video/Audio: Dailymotion

Action

Action	Block
Policy ID	1 (Application_Control)
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall

Key Findings from Monitoring

- Blocked high-risk websites
- Prevented proxy tools usage
- Logged malware attempts

Certificate Management

- Applying an SSL Inspection Profile to a Firewall Policy
- Enabled SSL inspection in profiles
- Certificate upload/settings

Applying an SSL Inspection Profile to a Firewall Policy

- For SSL inspection
 - Define SSL inspection profile
 - Allow the traffic with a firewall policy
 - Apply security profiles
 - Apply SSL inspection
- Combine SSL inspection with security profiles
- With the **no-inspection** SSL profile there is no SSL or SSH traffic inspection
 - No web filtering
 - No application control

Policy & Objects > Firewall Policy

Security Profiles

AntiVirus



AV default



Web Filter



WEB default



DNS Filter



Application Control



IPS



File Filter



SSL Inspection ⚠

SSL custom-deep-inspection



Decrypted Traffic Mirror



Search

+ Create

SSL certificate-inspection

SSL custom-deep-inspection

SSL deep-inspection

SSL no-inspection

Enable to mirror decrypted SSL traffic

Select SSL inspection profiles

Enabled SSL inspection in profiles

- Ready-to-use profiles for inspection of outbound encrypted sessions
 - SSL certificate inspection
 - SSL full inspection
- Customizable profile
 - Outbound deep inspection with options
- User-defined profile
 - Inbound traffic
 - Outbound traffic

Security Profiles > SSL/SSH Inspection

Name	Comments
SSL custom-deep-inspection	Customizable deep inspection profile.
SSL deep-inspection	Read-only deep inspection profile.
SSL no-inspection	Read-only profile that does no inspection.
SSL certificate-inspection	Read-only SSL handshake inspection profile.

Predefined profile for
SSL full inspection

Predefined profile for
certificate inspection

Challenges & Solutions

- Challenge: Limited lab access → Solution: Scheduled shared sessions
- Challenge: Config errors → Solution: Peer reviews and documentation

Risk Management

- Assigned backups for technical roles
- Used official Fortinet guides
- Weekly sync meetings

Communication Tools

- Microsoft Teams
- Google Docs for collaborative edits
- Group chat for quick decisions

Recommendations

- Enable deep inspection where applicable
- Use FortiAnalyzer for long-term analytics
- Update profiles frequently

Key Takeaways

- Profiles significantly improve security
- Configuration and testing are vital
- Monitoring ensures policy enforcement

Thank You

- Questions & Answers
- Contact Info