FORTINET CERTIFIED PROFESSIONAL Security Operations

FORTINET CERTIFIED PROFESSIONAL Network Security

FORTINET CERTIFIED PROFESSIONAL Public Cloud Security

FORTINET
Training Institute

FortiGate Administrator

Intrusion Prevention and Application Control

FortiOS 7.4

Last Modified: 18 April 2025

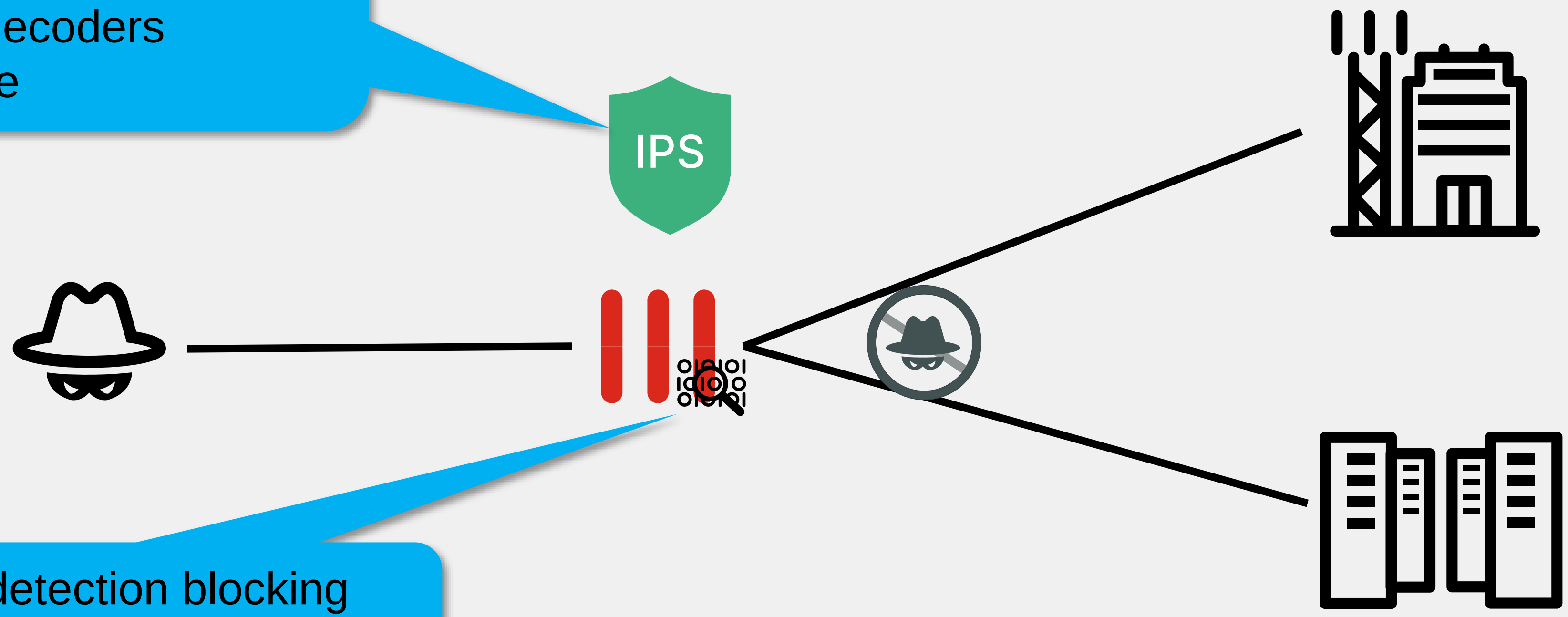
Objectives

- Configure an intrusion prevention system (IPS) sensor
- Troubleshoot IPS high-CPU usage
- Configure application control in profile mode
- Monitor application control events
- Troubleshoot traffic matching with application control profile issues

IPS

IPS components include:

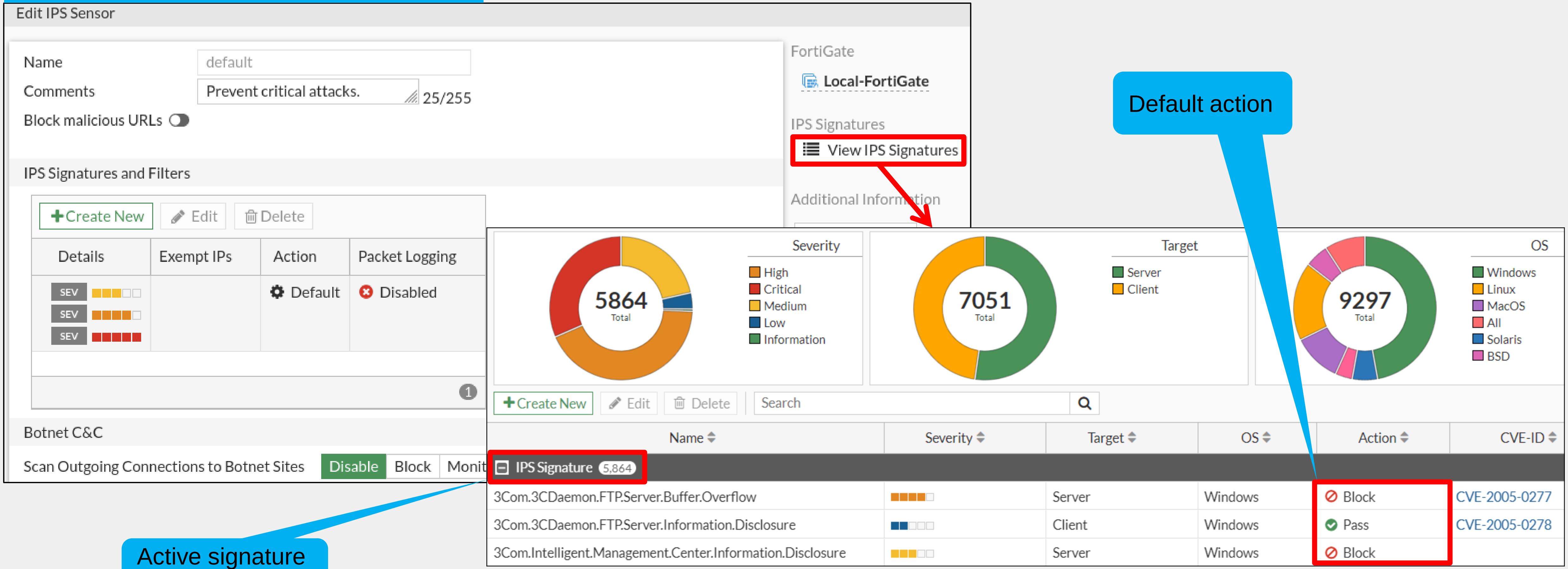
- IPS signature databases
- Protocol decoders
- IPS engine



Flow-based detection blocking anomalies and exploits

List of IPS Signatures

Security Profiles > Intrusion Prevention



Edit IPS Sensor

Name	default
Comments	Prevent critical attacks. 25/255
Block malicious URLs	○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
SEV ■■■□□ SEV ■■■■□ SEV ■■■■■		Default	Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites: Disable | Block | Monit

IPS Signature 5,864

Name	Severity	Target	OS	Action	CVE-ID
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	

Default action

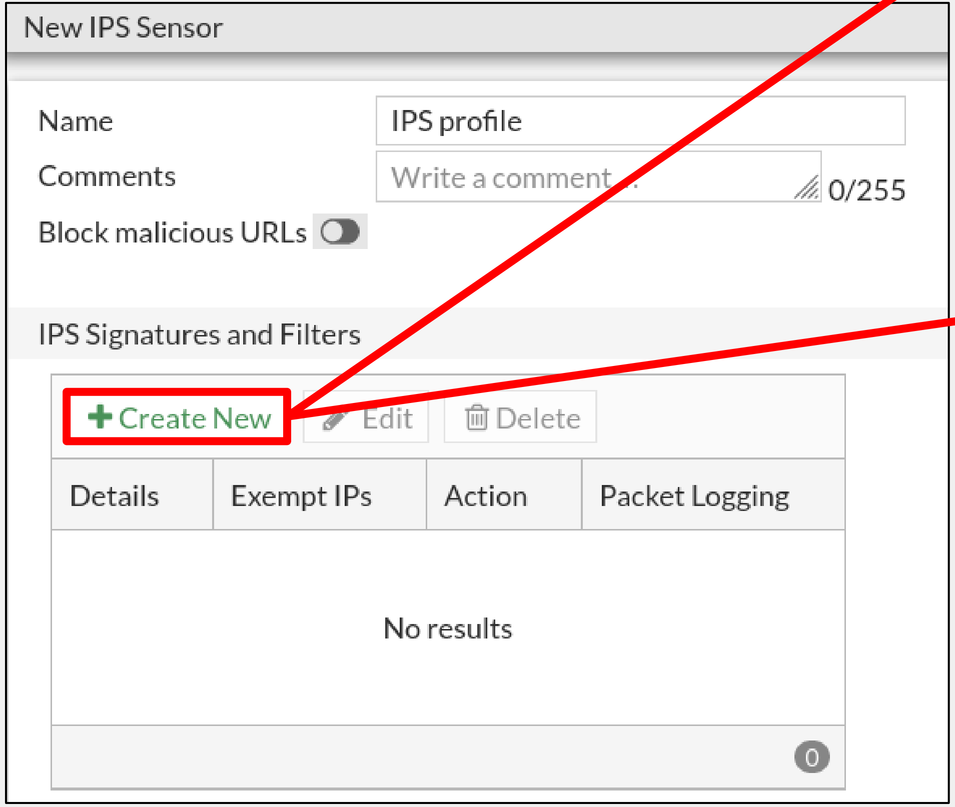
Active signature database

FORTINET Training Institute

Configuring IPS Sensors

- Add individual signatures
- Add groups of signatures using filters

Security Profiles > Intrusion Prevention



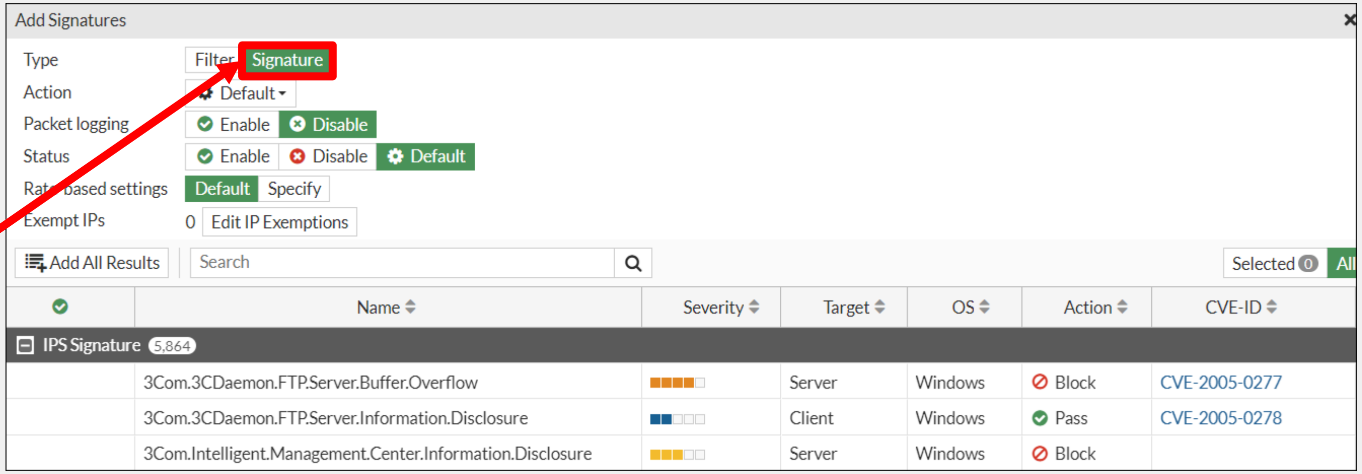
New IPS Sensor

Name	IPS profile
Comments	Write a comment... 0/255
Block malicious URLs	○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging

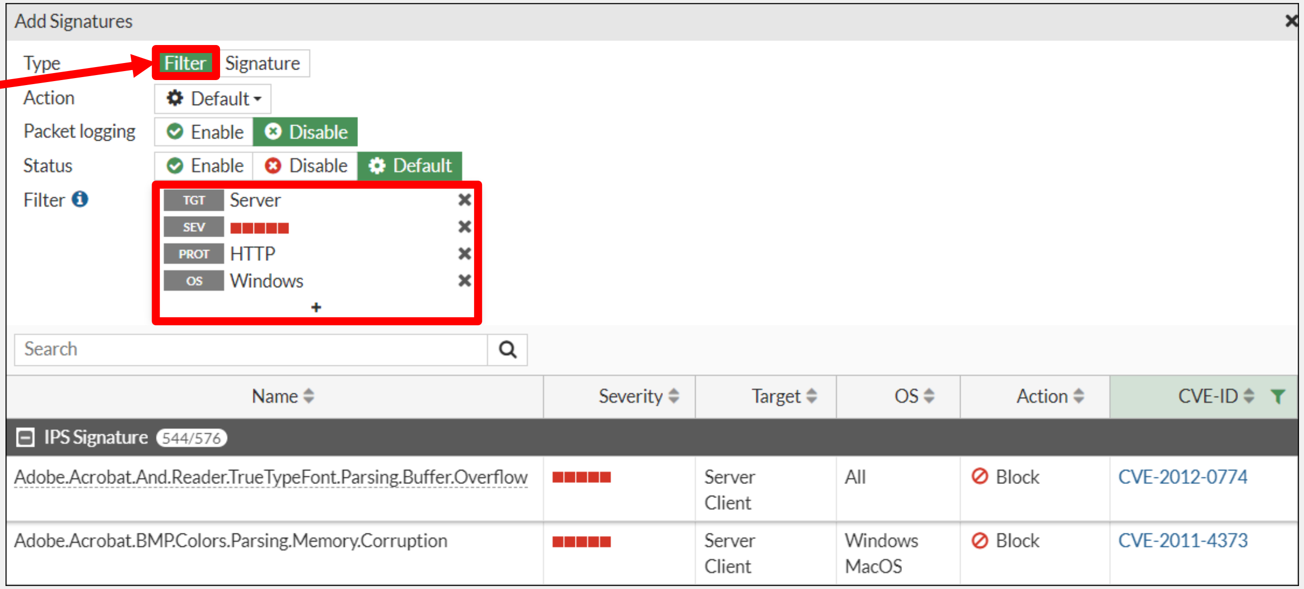
No results



Add Signatures

Type	Filter [✓ Signature]
Action	Default
Packet logging	Enable [✓ Disable]
Status	Enable Disable [✓ Default]
Rate based settings	[✓ Default] Specify
Exempt IPs	0 Edit IP Exemptions

✓	Name	Severity	Target	OS	Action	CVE-ID
	IPS Signature 5,864					
	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	Default
Packet logging	Enable [✓ Disable]
Status	Enable Disable [✓ Default]
Filter	TGT Server SEV ■■■■■ PROT HTTP OS Windows +

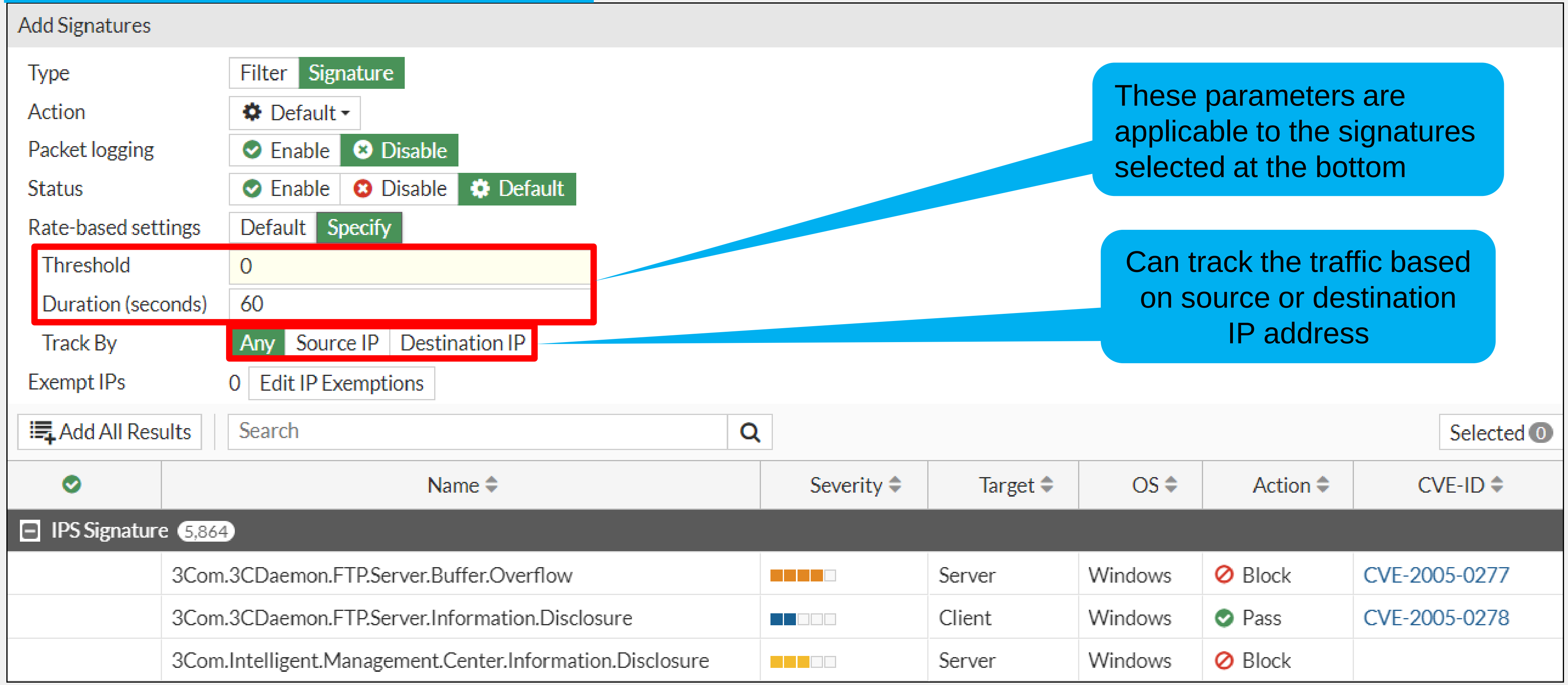
Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 544/576					
Adobe.Acrobat.And.Reader.TrueTypeFont.Parsing.Buffer.Overflow	■■■■■	Server Client	All	Block	CVE-2012-0774
Adobe.Acrobat.BMP.Colors.Parsing.Memory.Corruption	■■■■■	Server Client	Windows MacOS	Block	CVE-2011-4373

FORTINET
Training Institute

Configuring IPS Sensors—Rate-Based Signatures

- Add rate-based signatures to block traffic when the threshold is exceeded during a time period

Security Profiles > **Intrusion Prevention**



Add Signatures

Type	Filter [✓ Signature]
Action	Default ▾
Packet logging	Enable [✓ Disable]
Status	Enable Disable [✓ Default]
Rate-based settings	Default [✓ Specify]
Threshold	0
Duration (seconds)	60
Track By	[✓ Any] Source IP Destination IP
Exempt IPs	0 Edit IP Exemptions

Add All Results | Search | Selected 0

✓	Name	Severity	Target	OS	Action	CVE-ID
	IPS Signature 5,864					
	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	

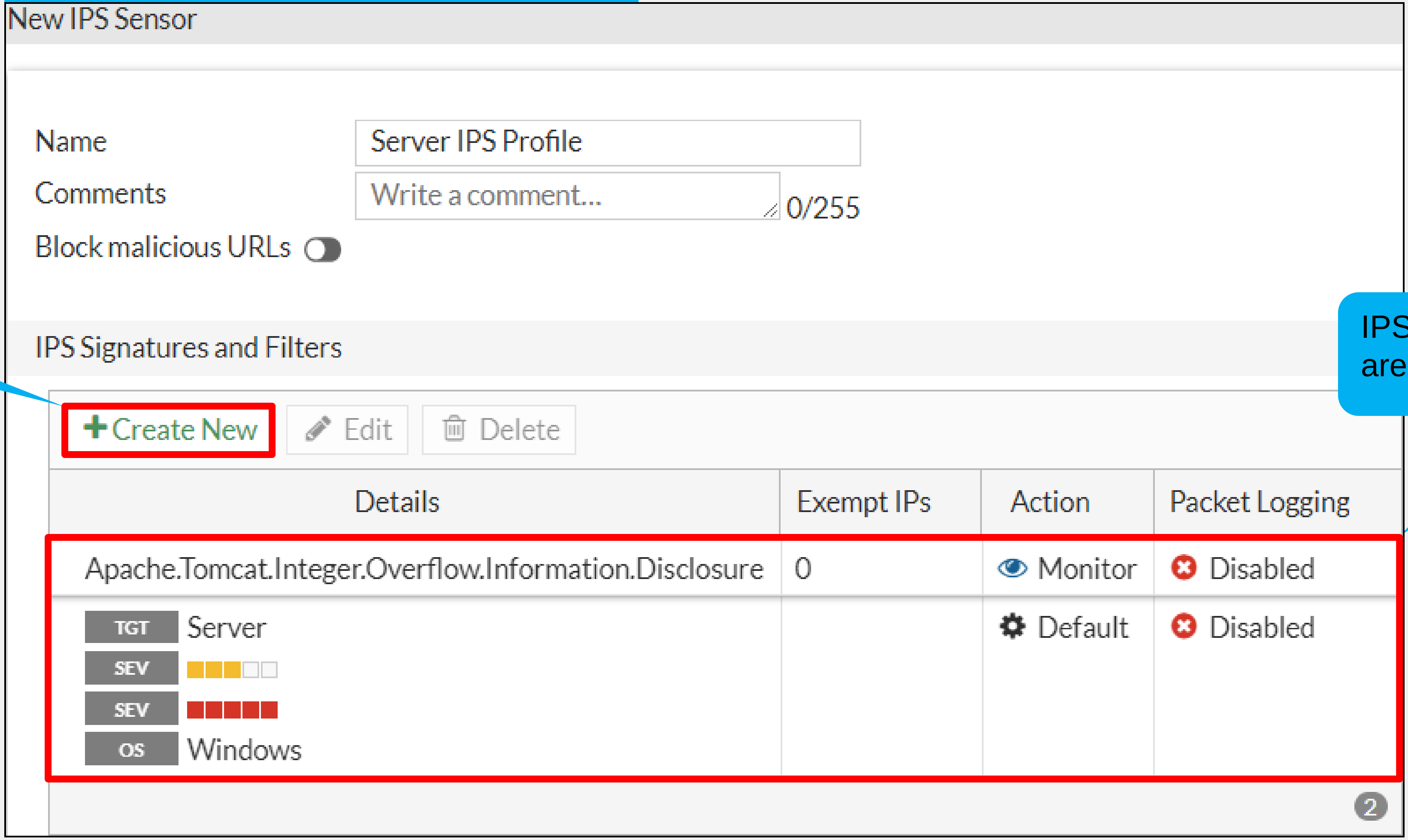
These parameters are applicable to the signatures selected at the bottom

Can track the traffic based on source or destination IP address

FORTINET
Training Institute

IPS Sensor Inspection Sequence

Security Profiles > Intrusion Prevention



New IPS Sensor

Name	Server IPS Profile
Comments	Write a comment... 0/255
Block malicious URLs	○

IPS Signatures and Filters

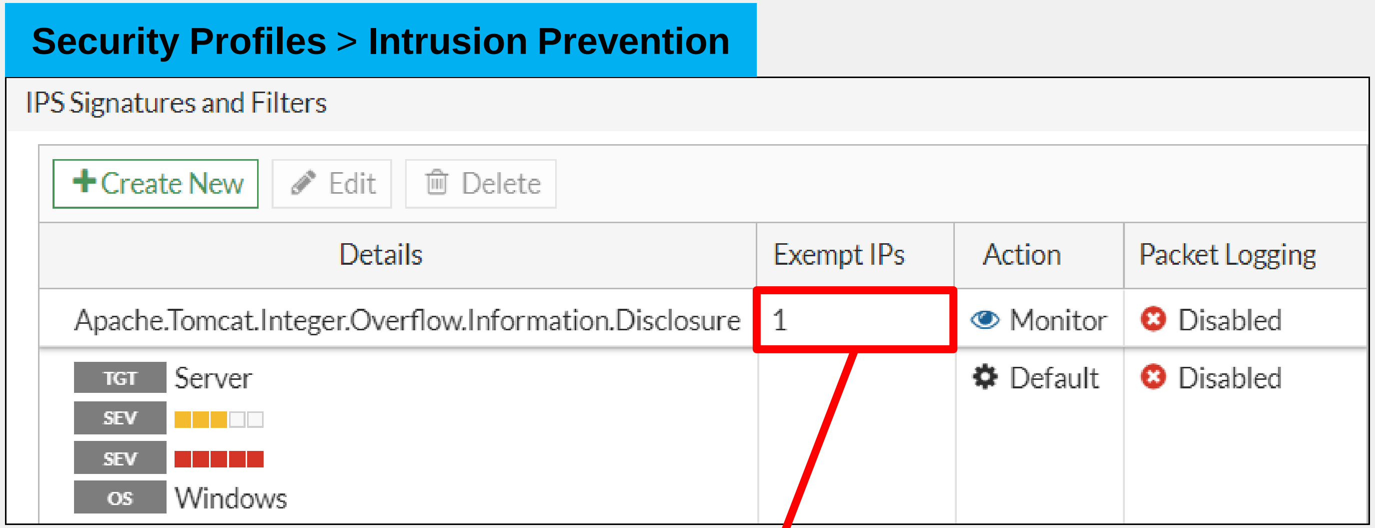
Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	0	Monitor	Disabled
TGT Server SEV 🟨🟨🟨□□ SEV 🟥🟥🟥🟥🟥 OS Windows		Default	Disabled

New entries are placed at the bottom of the list

IPS signatures and filters are processed in sequence

Configuring IP Exemptions

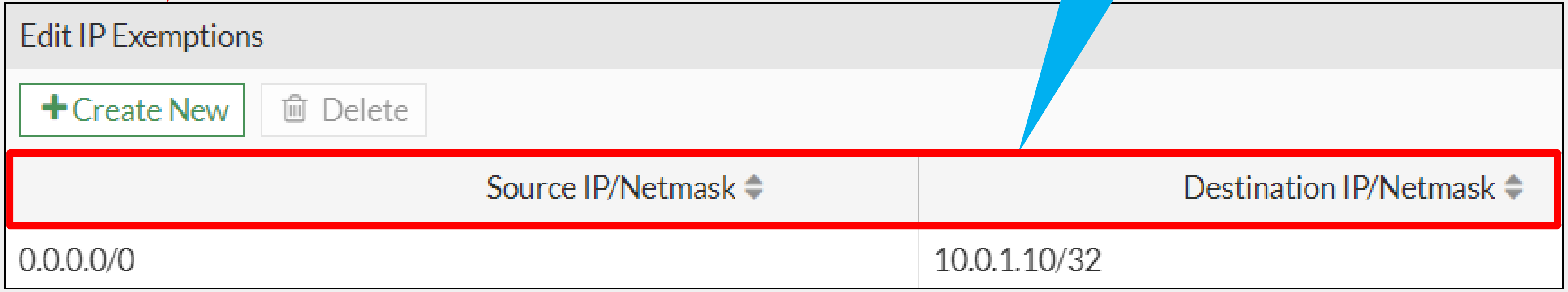
- Only configurable under individual IPS signatures



Security Profiles > **Intrusion Prevention**

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	1	Monitor	Disabled
TGT Server SEV 🟨🟨🟨□□ SEV 🟥🟥🟥🟥🟥 OS Windows		Default	Disabled

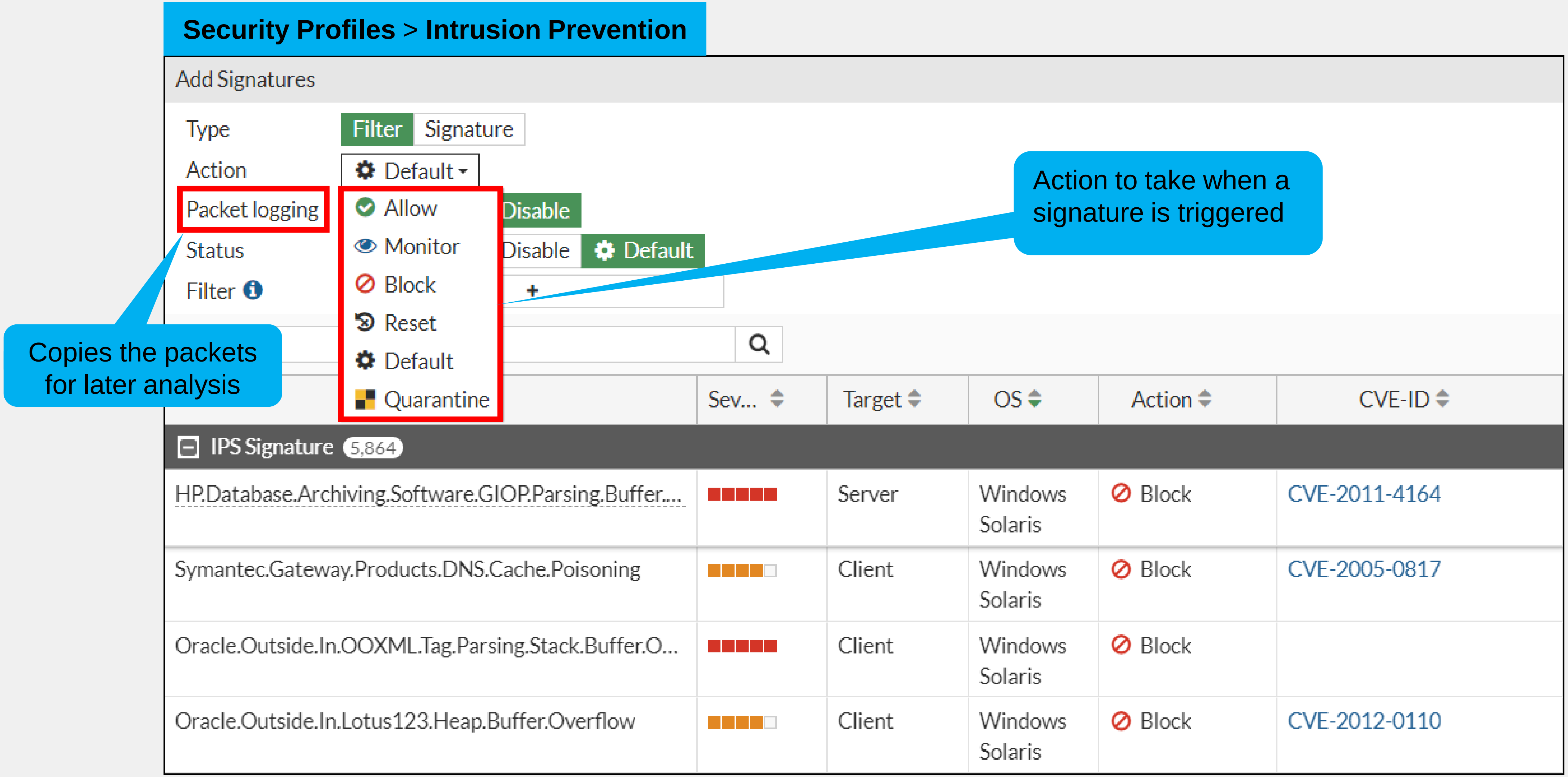


Edit IP Exemptions

Source IP/Netmask	Destination IP/Netmask
0.0.0.0/0	10.0.1.10/32

Exempt specific source or destination IP addresses

IPS Actions



Security Profiles > Intrusion Prevention

Add Signatures

Type: Filter | Signature

Action: Default

- Allow
- Monitor
- Block
- Reset
- Default
- Quarantine

Packet logging: Disable

Status: Disable | Default

Filter: +

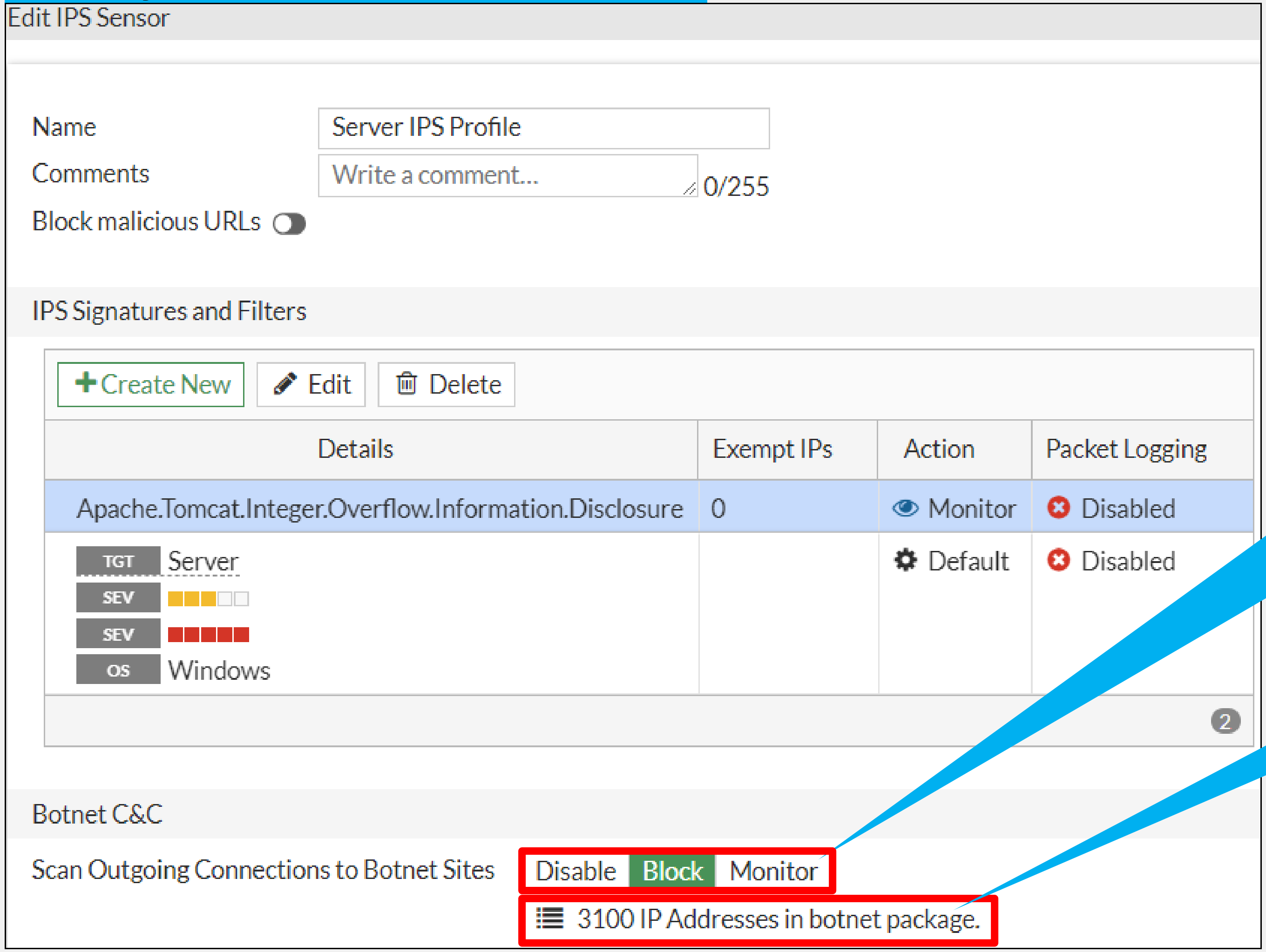
	Sev...	Target	OS	Action	CVE-ID
IPS Signature 5,864					
HP.Database.Archiving.Software.GIOP.Parsing.Buffer....	■■■■■	Server	Windows Solaris	Block	CVE-2011-4164
Symantec.Gateway.Products.DNS.Cache.Poisoning	■■■■□	Client	Windows Solaris	Block	CVE-2005-0817
Oracle.Outside.In.OOXML.Tag.Parsing.Stack.Buffer.O...	■■■■■	Client	Windows Solaris	Block	
Oracle.Outside.In.Lotus123.Heap.Buffer.Overflow	■■■■□	Client	Windows Solaris	Block	CVE-2012-0110

Action to take when a signature is triggered

Copies the packets for later analysis

Enabling Botnet Protection

Security Profiles > Intrusion Prevention



Edit IPS Sensor

Name	Server IPS Profile
Comments	Write a comment... 0/255
Block malicious URLs	○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Apache.Tomcat.Integer.Overflow.Information.Disclosure	0	Monitor	Disabled
TGT Server SEV 🟨🟨🟨⬜⬜ SEV 🟥🟥🟥🟥🟥 OS Windows		Default	Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites: Disable [✓ Block] Monitor

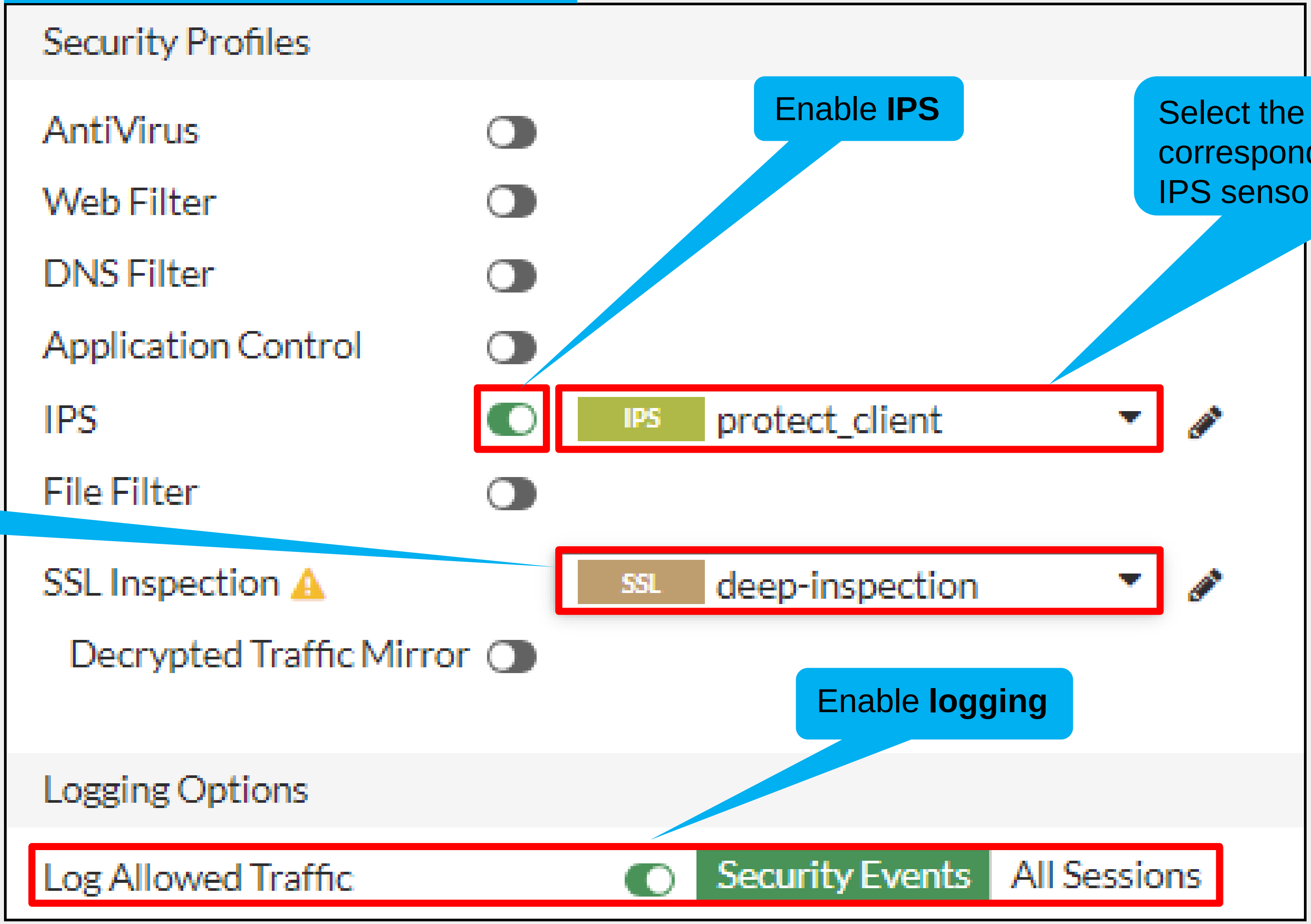
3100 IP Addresses in botnet package.

Set action to **Block** or **Monitor**

Botnet database from FortiGuard (included with a valid IPS license)

Applying IPS Inspection

Policy & Objects > Firewall Policy



Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ● IPS protect_client

File Filter ○

SSL Inspection SSL deep-inspection

Decrypted Traffic Mirror ○

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Enable **IPS**

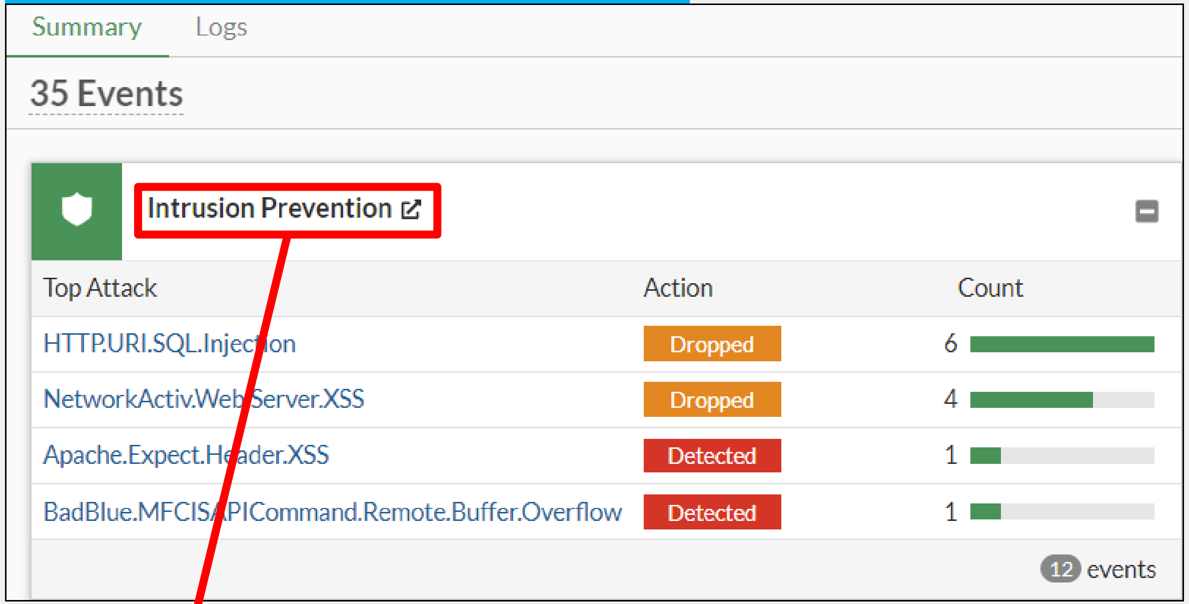
Select the IPS security profile corresponding to the configured IPS sensors

Set **deep-inspection** for encrypted protocols

Enable **logging**

IPS Logging

Log & Report > Security Events



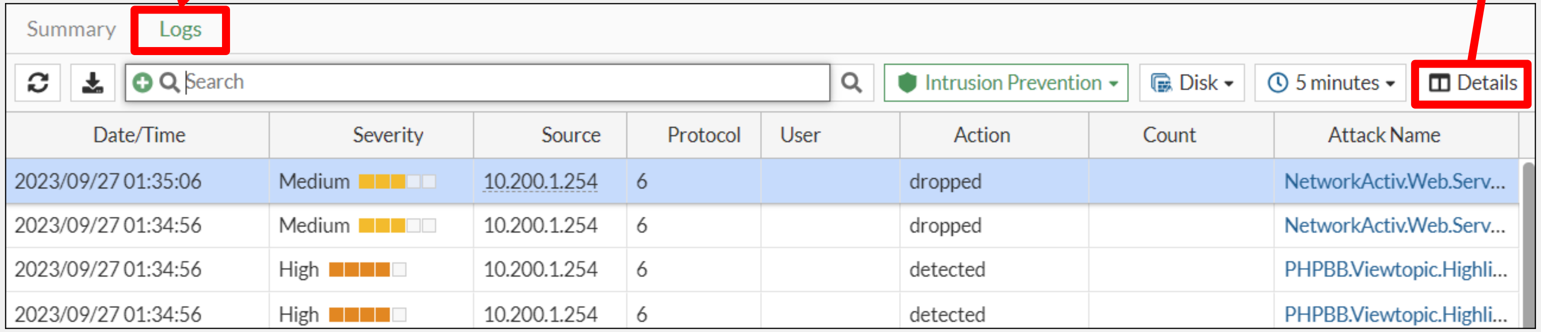
Summary | Logs

35 Events

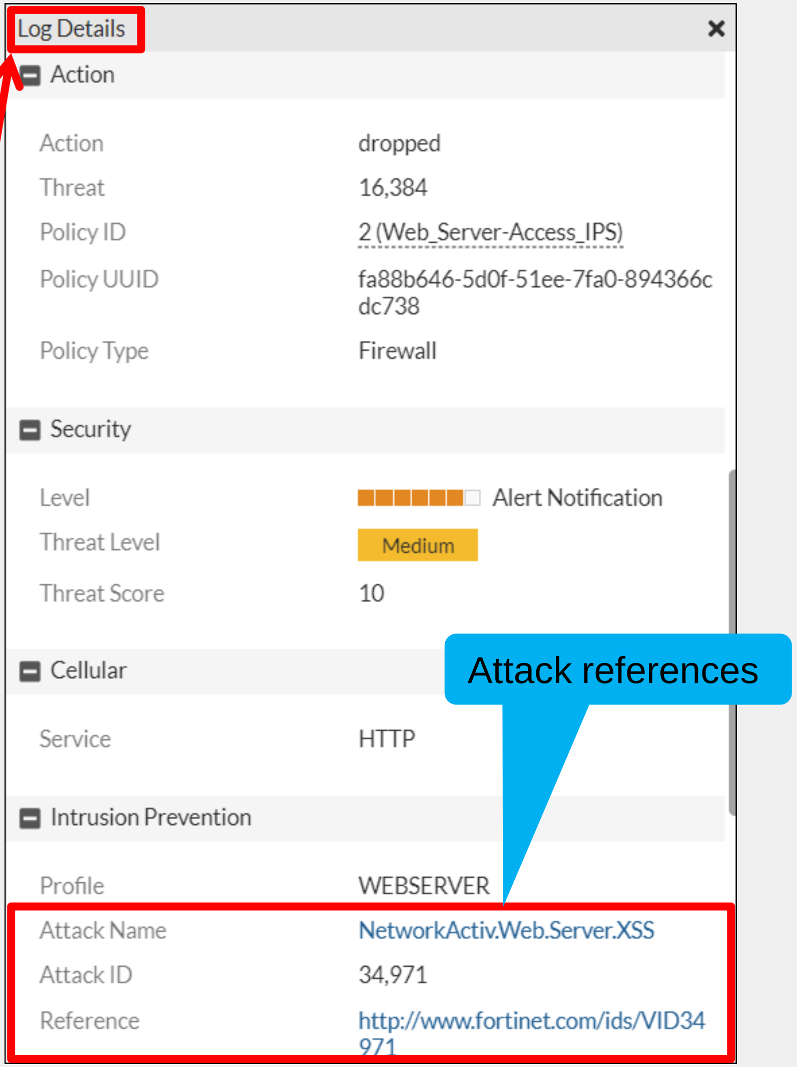
Intrusion Prevention

Top Attack	Action	Count
HTTP.URI.SQL.Injection	Dropped	6
NetworkActiv.Web.Server.XSS	Dropped	4
Apache.Expect.Header.XSS	Detected	1
BadBlue.MFCISAPICommand.Remote.Buffer.Overflow	Detected	1

12 events



Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
2023/09/27 01:35:06	Medium	10.200.1.254	6		dropped		NetworkActiv.Web.Serv...
2023/09/27 01:34:56	Medium	10.200.1.254	6		dropped		NetworkActiv.Web.Serv...
2023/09/27 01:34:56	High	10.200.1.254	6		detected		PHPBB.Viewtopic.Highli...
2023/09/27 01:34:56	High	10.200.1.254	6		detected		PHPBB.Viewtopic.Highli...



Log Details

Action

Action	dropped
Threat	16,384
Policy ID	2 (Web_Server-Access_IPS)
Policy UUID	fa88b646-5d0f-51ee-7fa0-894366cdc738
Policy Type	Firewall

Security

Level	Alert Notification
Threat Level	Medium
Threat Score	10

Cellular

Service	HTTP

Intrusion Prevention

Profile	WEBSERVER
Attack Name	NetworkActiv.Web.Server.XSS
Attack ID	34,971
Reference	http://www.fortinet.com/ids/VID34971

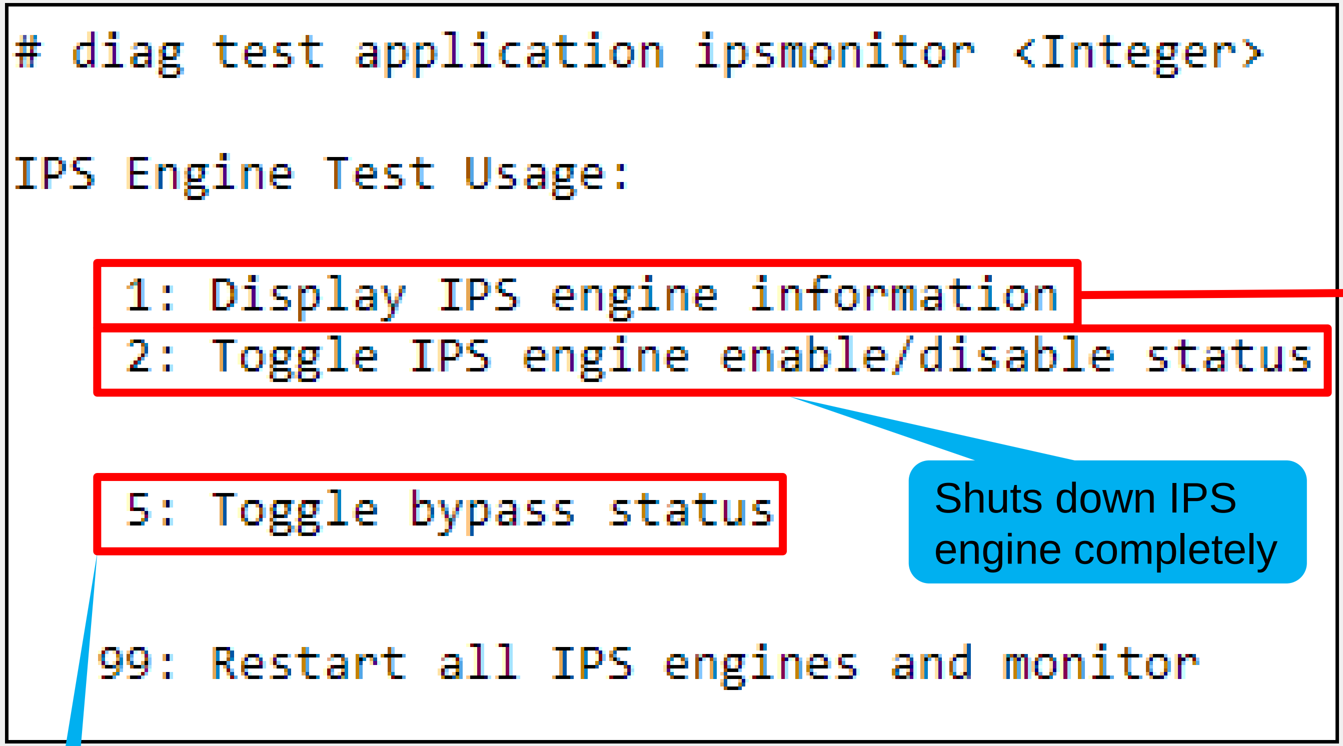
Attack references

Training Institute

© Fortinet Inc. All Rights Reserved.

Troubleshoot IPS High-CPU Usage

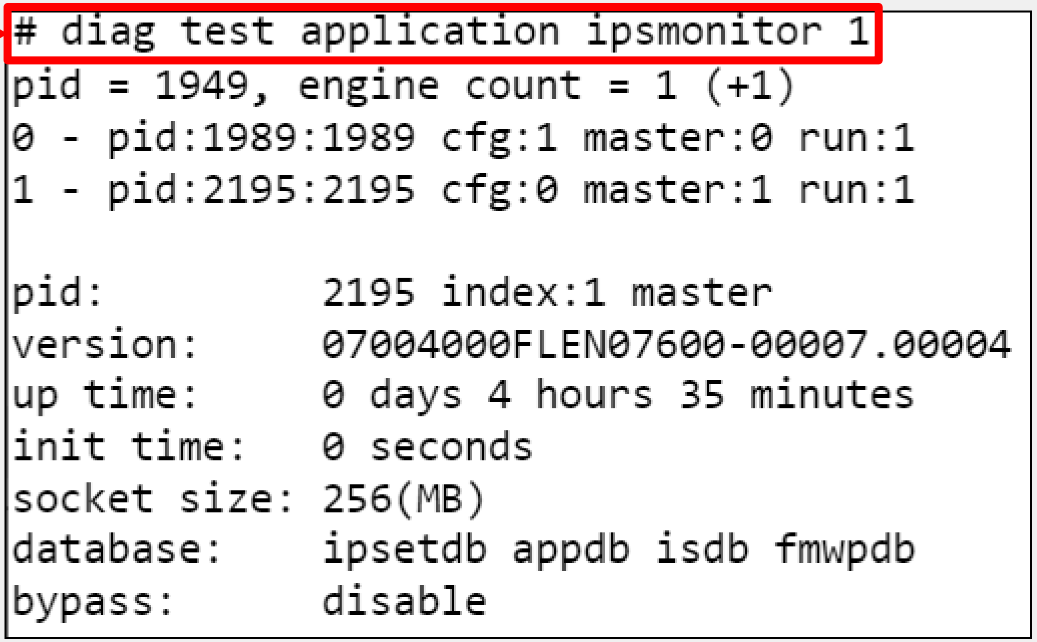
- CLI command to troubleshoot continuous high-CPU use by IPS engines



```
# diag test application ipsmonitor <Integer>

IPS Engine Test Usage:

    1: Display IPS engine information
    2: Toggle IPS engine enable/disable status

    5: Toggle bypass status

   99: Restart all IPS engines and monitor
```

Shuts down IPS engine completely

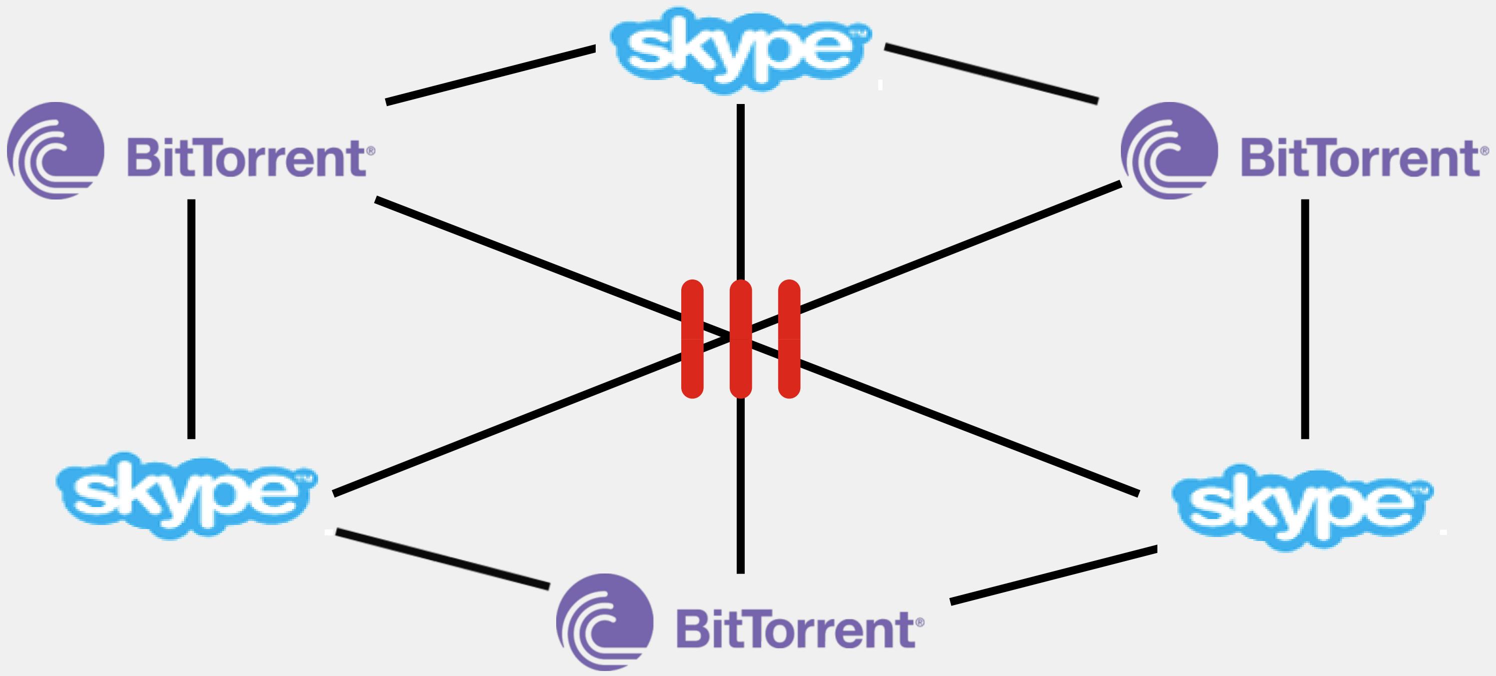
IPS engine remains active, but does not inspect traffic



```
# diag test application ipsmonitor 1
pid = 1949, engine count = 1 (+1)
0 - pid:1989:1989 cfg:1 master:0 run:1
1 - pid:2195:2195 cfg:0 master:1 run:1

pid:         2195 index:1 master
version:     07004000FLEN07600-00007.00004
up time:     0 days 4 hours 35 minutes
init time:   0 seconds
socket size: 256(MB)
database:    ipsetdb appdb isdb fmwpdb
bypass:      disable
```

Application Control

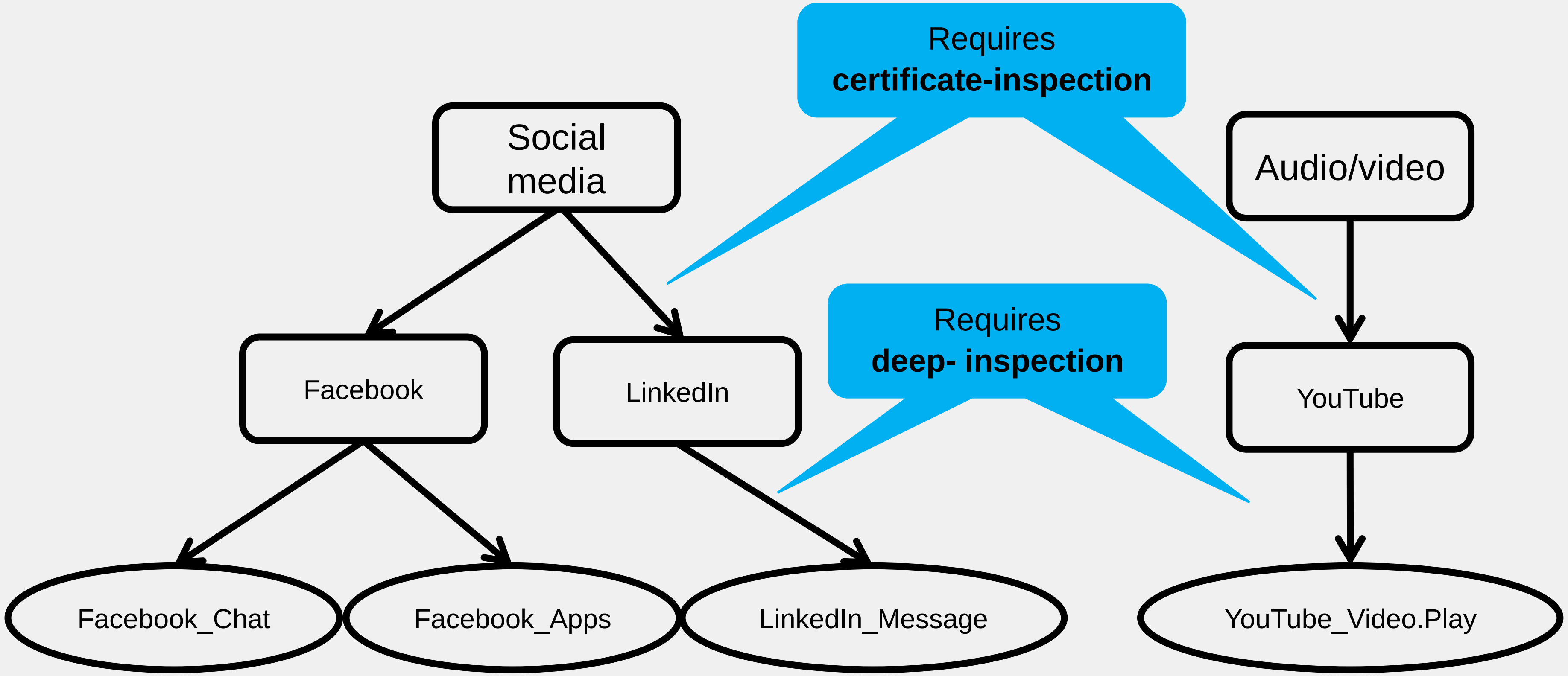
- Uses the IPS engine in flow-based scan
- Detects and acts on network application traffic
- Appropriate for detecting peer-to-peer (P2P) applications



FORTINET
Training Institute

Application Control—Hierarchical Structure

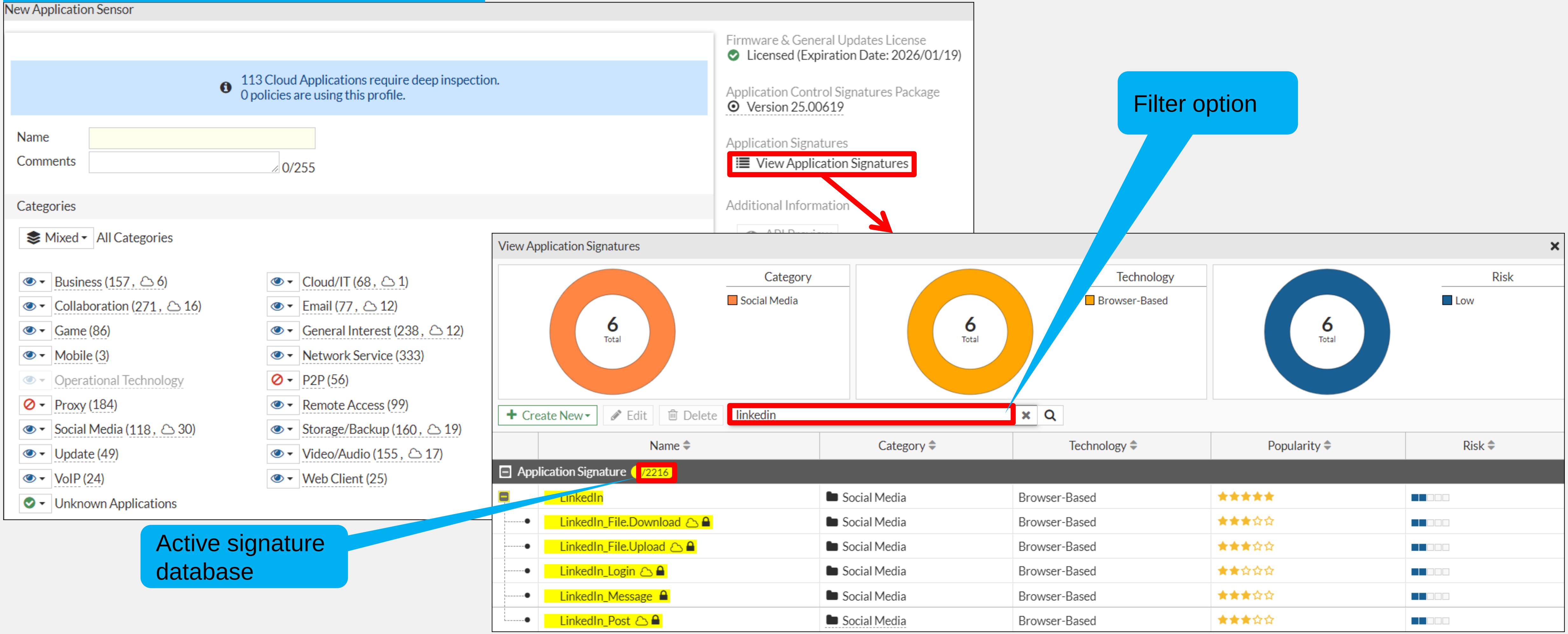
- Application control signatures are organized in a hierarchical structure
  - The parent signature takes precedence over the child signature



FORTINET Training Institute

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

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

Application Control Signatures Package
Version 25.00619

Application Signatures
View Application Signatures

Additional Information

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)

View Application Signatures

+ Create New ▾ | Edit | Delete | linkedin

Name	Category	Technology	Popularity	Risk
Application Signature 6/2216				
LinkedIn	Social Media	Browser-Based	★★★★★	■■□□□
LinkedIn_File.Download	Social Media	Browser-Based	★★★☆☆	■■□□□
LinkedIn_File.Upload	Social Media	Browser-Based	★★★☆☆	■■□□□
LinkedIn_Login	Social Media	Browser-Based	★★☆☆☆	■■□□□
LinkedIn_Message	Social Media	Browser-Based	★★★☆☆	■■□□□
LinkedIn_Post	Social Media	Browser-Based	★★★☆☆	■■□□□

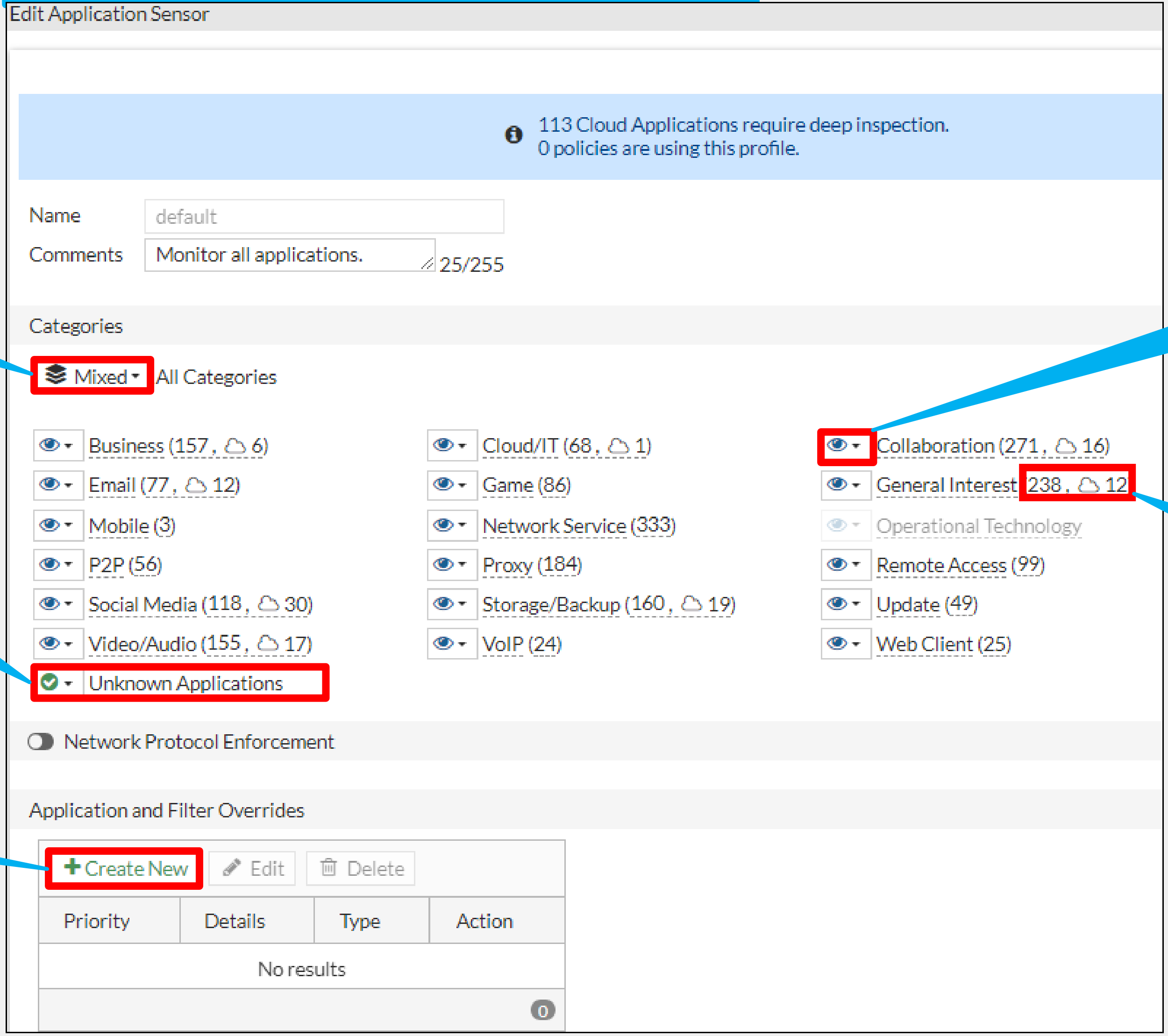
Filter option

Active signature database

FORTINET
Training Institute

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

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

○ Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
No results			

0

Applies an action to all categories at once

Matches traffic to unidentified applications

Creates specific actions for a single application or group of applications

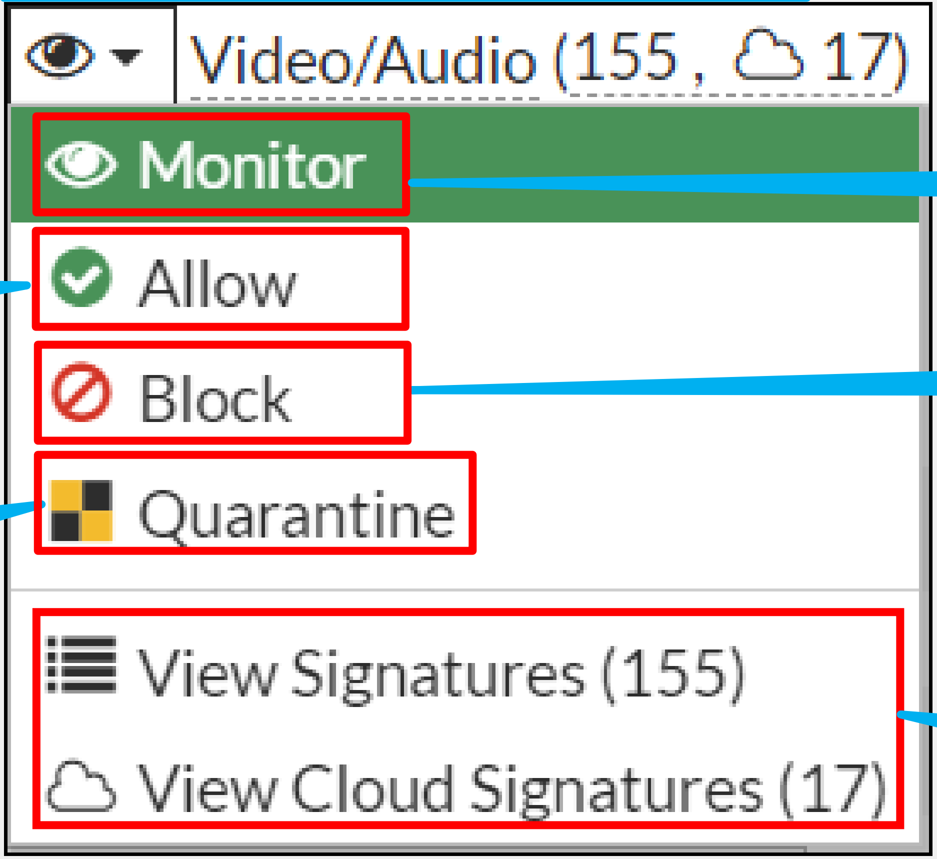
Applies an action to one category

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

FURTINET
Training Institute

Filters Actions

Security Profiles > Application Control



Allows and also logs

Continues to next scan or feature and does not log

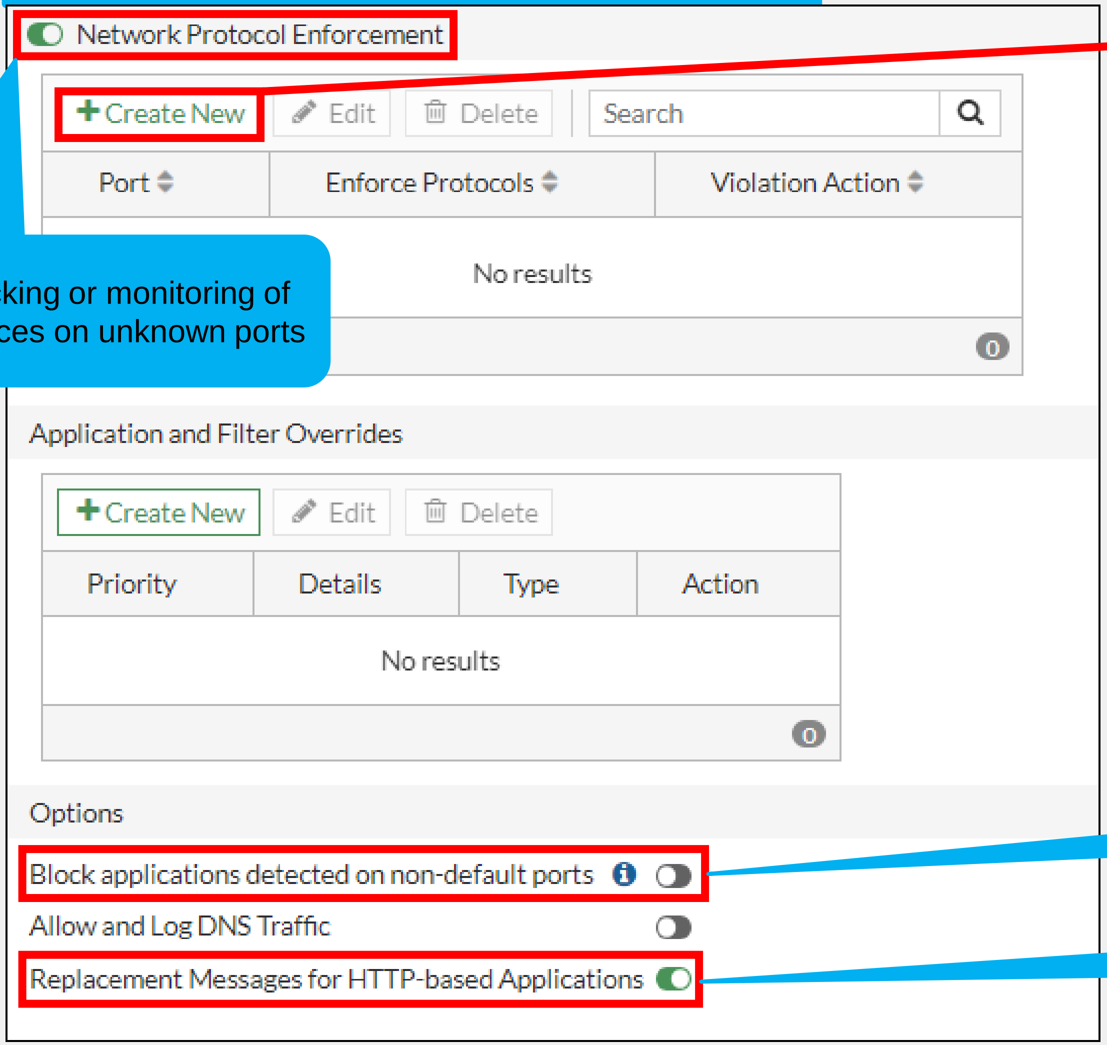
Drops packets and logs

Block and log traffic from attacker IP address until the expiration time

View the list of signatures of native or cloud applications for a specific category

Configuring Additional Options

Security Profiles > Application Control



Network Protocol Enforcement

+ Create New | Edit | Delete | Search

Port	Enforce Protocols	Violation Action
No results		

0

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
No results			

0

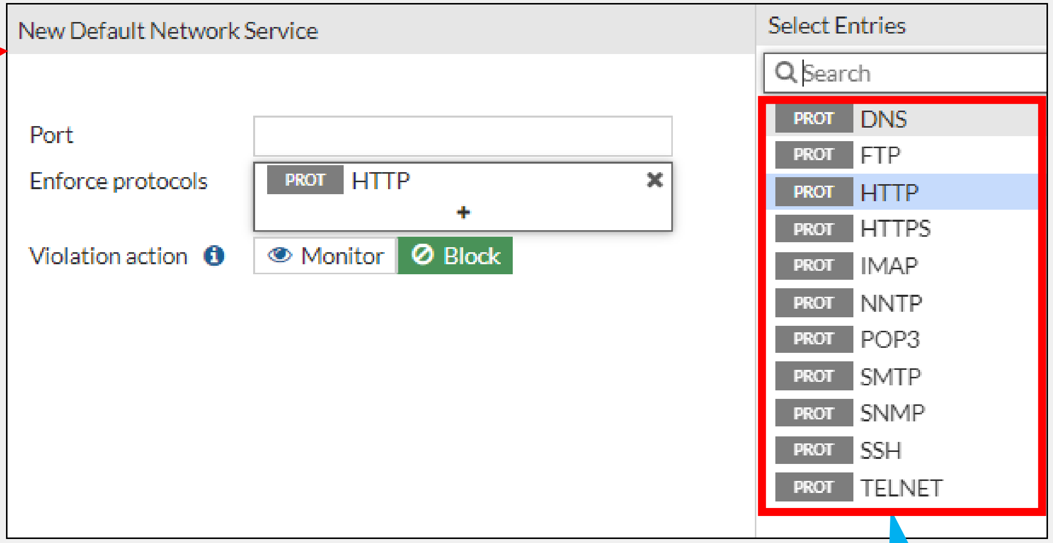
Options

Block applications detected on non-default ports ○

Allow and Log DNS Traffic ○

Replacement Messages for HTTP-based Applications ●

Allows blocking or monitoring of known services on unknown ports



New Default Network Service

Port:

Enforce protocols: PROT HTTP

Violation action: Monitor [✓ Block]

Select Entries

Search

PROT	DNS
PROT	FTP
PROT	HTTP
PROT	HTTPS
PROT	IMAP
PROT	NNTP
PROT	POP3
PROT	SMTP
PROT	SNMP
PROT	SSH
PROT	TELNET

List of known services

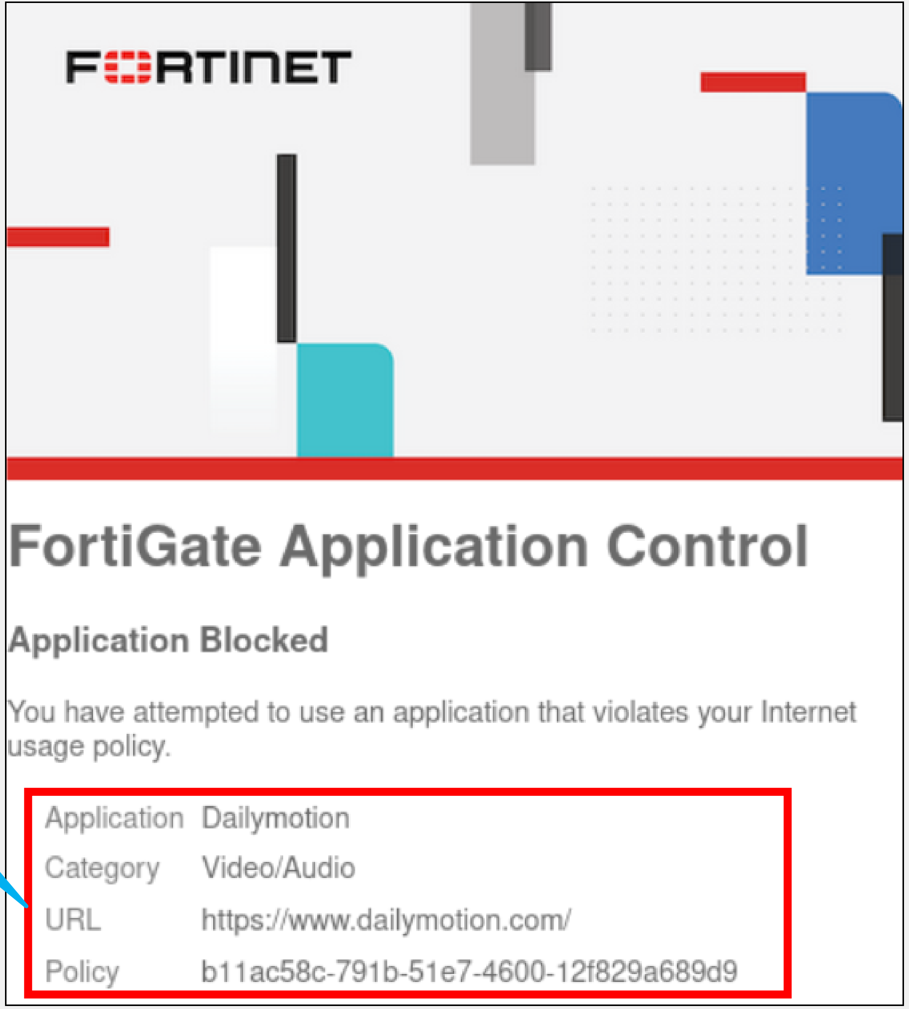
Enforces applications to run on its default port

Applies only to HTTP/HTTPS applications

HTTP Block Page

- Application control HTTP block pages in profile mode

System > Replacement Messages



FortiGate Application Control

Application Blocked

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

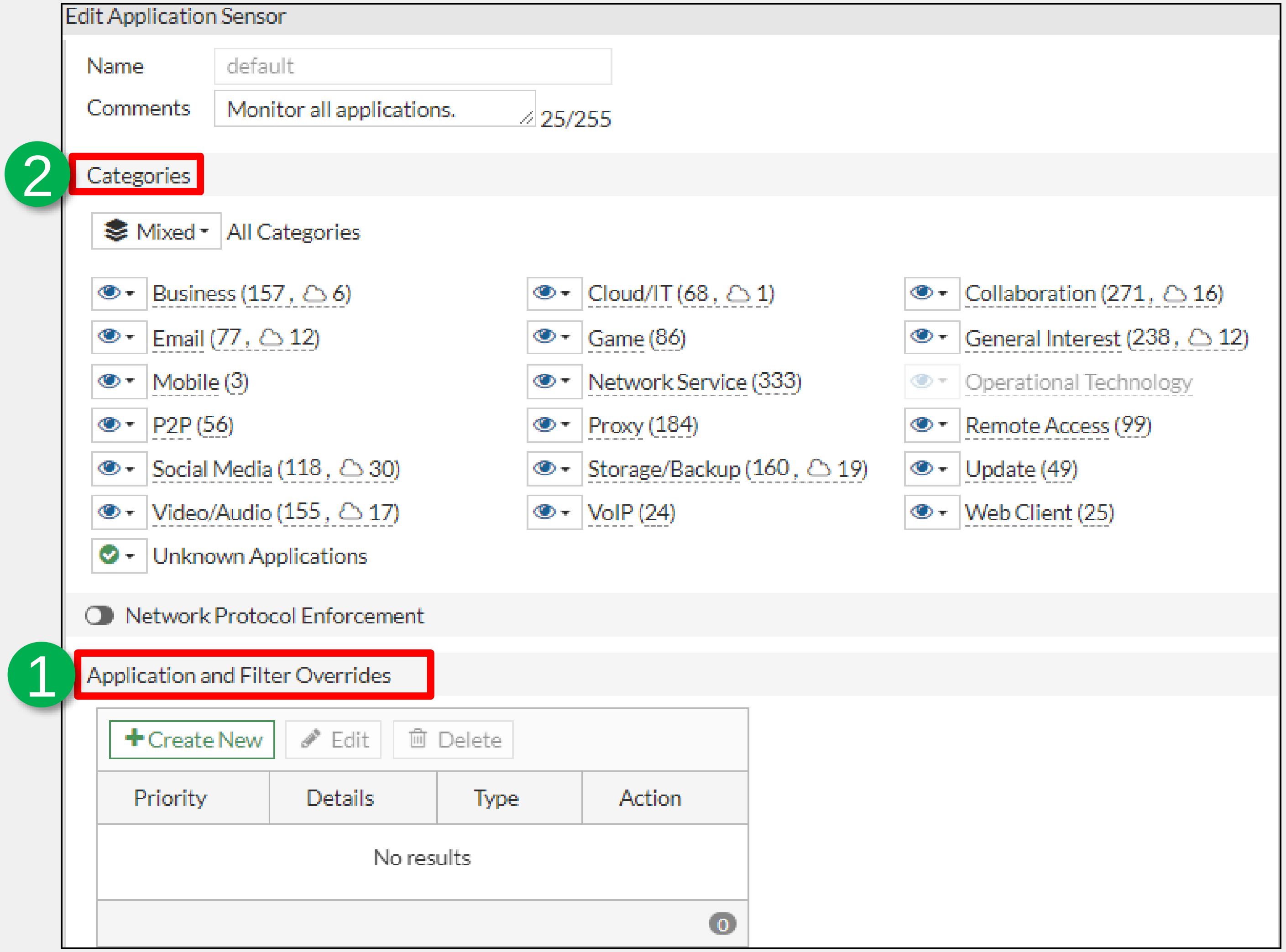
Application	Dailymotion
Category	Video/Audio
URL	https://www.dailymotion.com/
Policy	b11ac58c-791b-51e7-4600-12f829a689d9

Information related to the HTTP page being blocked

Scanning Order

- The IPS engine identifies the application
- The application control profile scans for matches in this order:
  1. Application and filter overrides
  2. Categories

Security Profiles > Application Control



Edit Application Sensor

Name: default

Comments: Monitor all applications. 25/255

2 Categories

Mixed ▾ All Categories

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

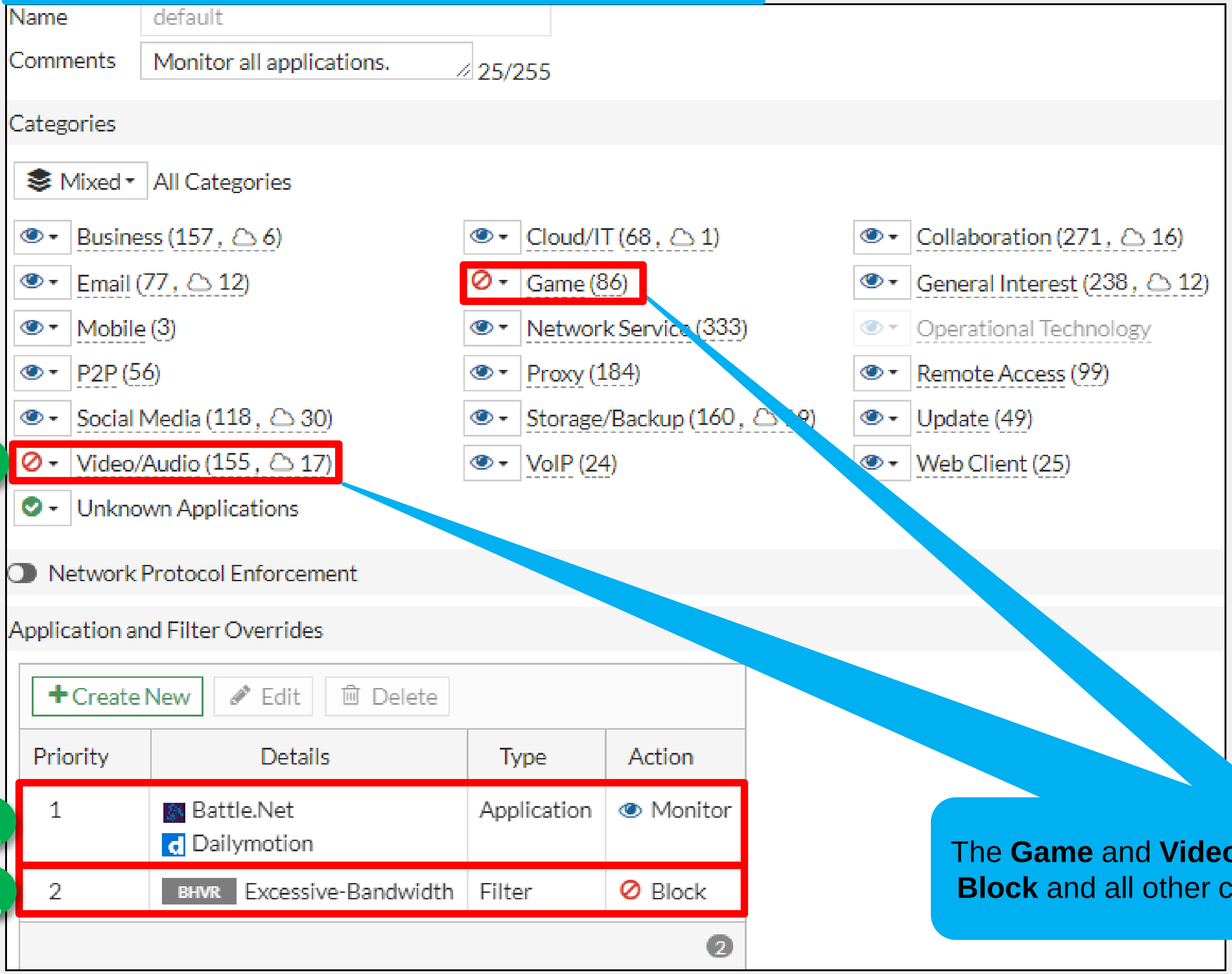
Network Protocol Enforcement

1 Application and Filter Overrides

Priority	Details	Type	Action
No results			

Order of Scan and Blocking Behavior (Scenario 1)

Security Profiles > Application Control



Name: default

Comments: Monitor all applications. 25/255

Categories

Mixed ▾ All Categories

Business (157, ☁ 6)	Cloud/IT (68, ☁ 1)	Collaboration (271, ☁ 16)
Email (77, ☁ 12)	⊘ Game (86)	General Interest (238, ☁ 12)
Mobile (3)	Network Service (333)	Operational Technology
P2P (56)	Proxy (184)	Remote Access (99)
Social Media (118, ☁ 30)	Storage/Backup (160, ☁ [illegible]9)	Update (49)
⊘ Video/Audio (155, ☁ 17)	VoIP (24)	Web Client (25)
✓ Unknown Applications		

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Battle.Net Dailymotion	Application	Monitor
2	BHVR Excessive-Bandwidth	Filter	⊘ Block

Application Overrides set for Battle.Net and Dailymotion applications

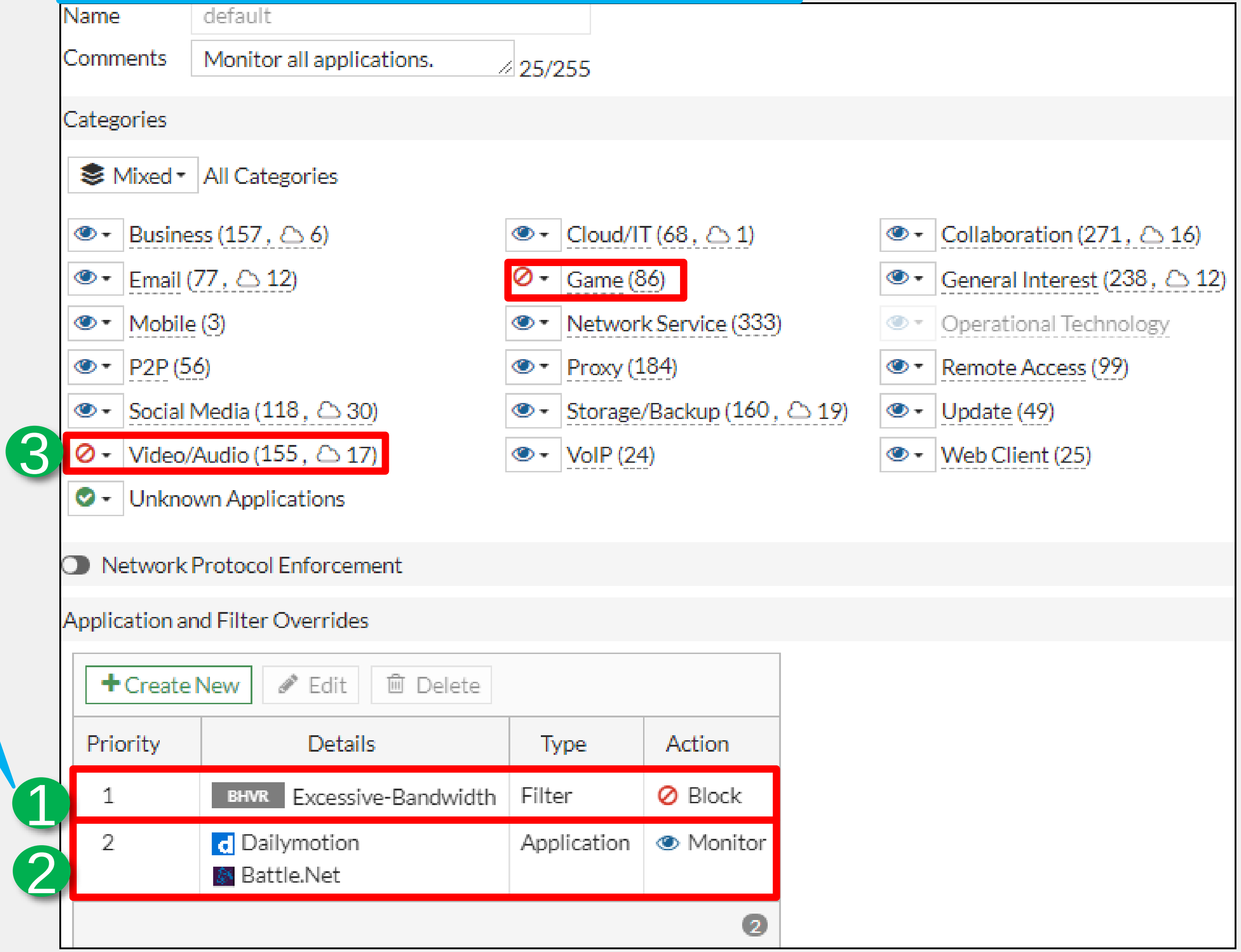
Filter Overrides set for applications that consume excessive bandwidth

The **Game** and **Video/Audio** categories are set to **Block** and all other categories are set to **Monitor**

Order of Scan and Blocking Behavior (Scenario 2)

The filter override entry is moved above the application override entry

Security Profiles > Application Control



Name: default

Comments: Monitor all applications. 25/255

Categories

Mixed ▾ All Categories

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

○ Network Protocol Enforcement

Application and Filter Overrides

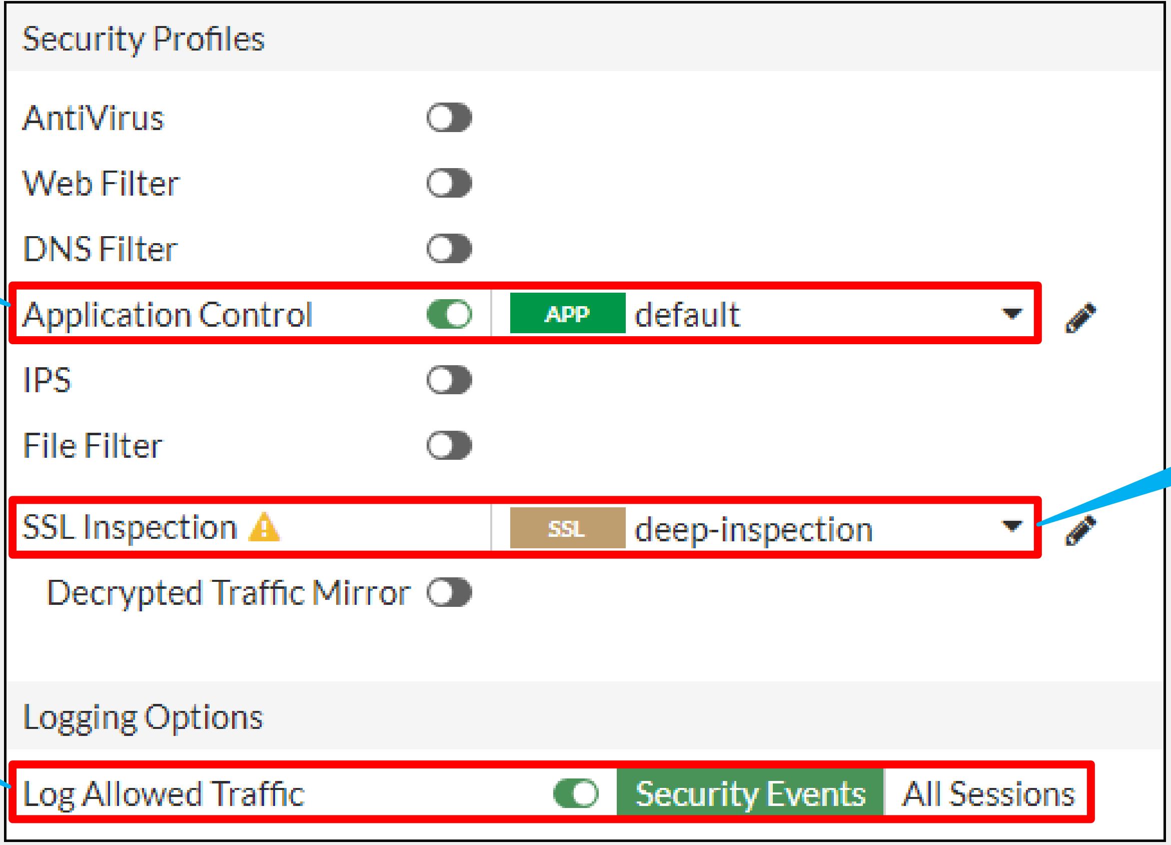
+ Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	Dailymotion Battle.Net	Application	👁 Monitor

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 ○

Web Filter ○

DNS Filter ○

Application Control ● APP default

IPS ○

File Filter ○

SSL Inspection ⚠ SSL deep-inspection

Decrypted Traffic Mirror ○

Logging Options

Log Allowed Traffic ● Security Events All Sessions

Enable **Application Control** and select the profile

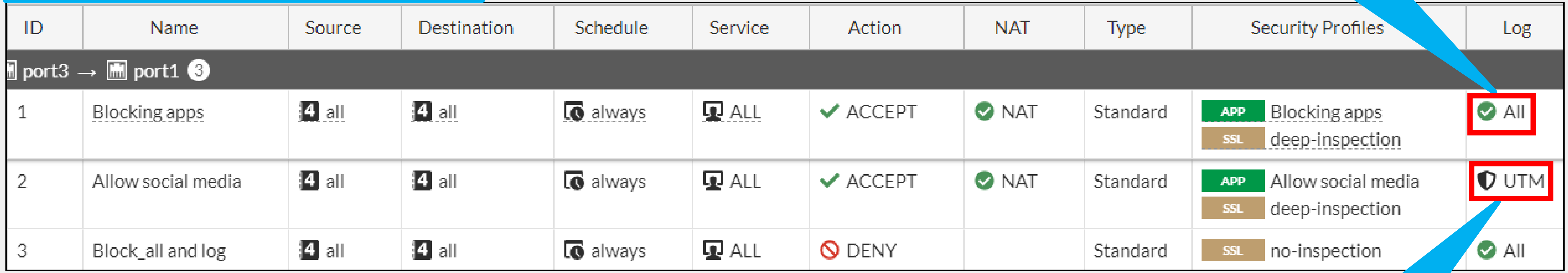
Use **deep-inspection** profile to scan encrypted traffic

Enable logging

Logging Application Control Events

- Example of NGFW profile-based mode firewall policies

Policy & Objects > Firewall Policy



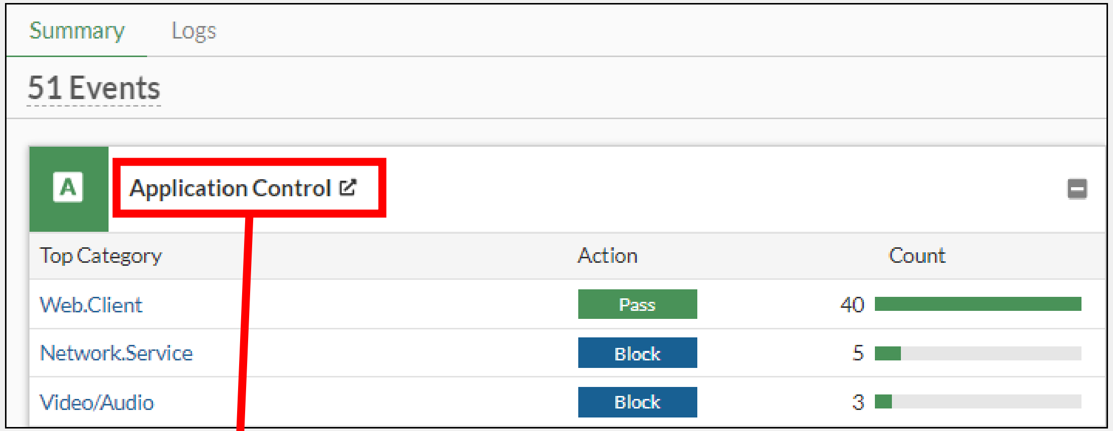
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles	Log
port3 → port1 3										
1	Blocking apps	all	all	always	ALL	✓ ACCEPT	✓ NAT	Standard	APP Blocking apps SSL deep-inspection	✓ All
2	Allow social media	all	all	always	ALL	✓ ACCEPT	✓ NAT	Standard	APP Allow social media SSL deep-inspection	UTM
3	Block_all and log	all	all	always	ALL	⊘ DENY		Standard	SSL no-inspection	✓ All

Logging set to **All Sessions**

Logging set to **Security Events**

Monitoring Application Control Logging

Log & Report > Security Events

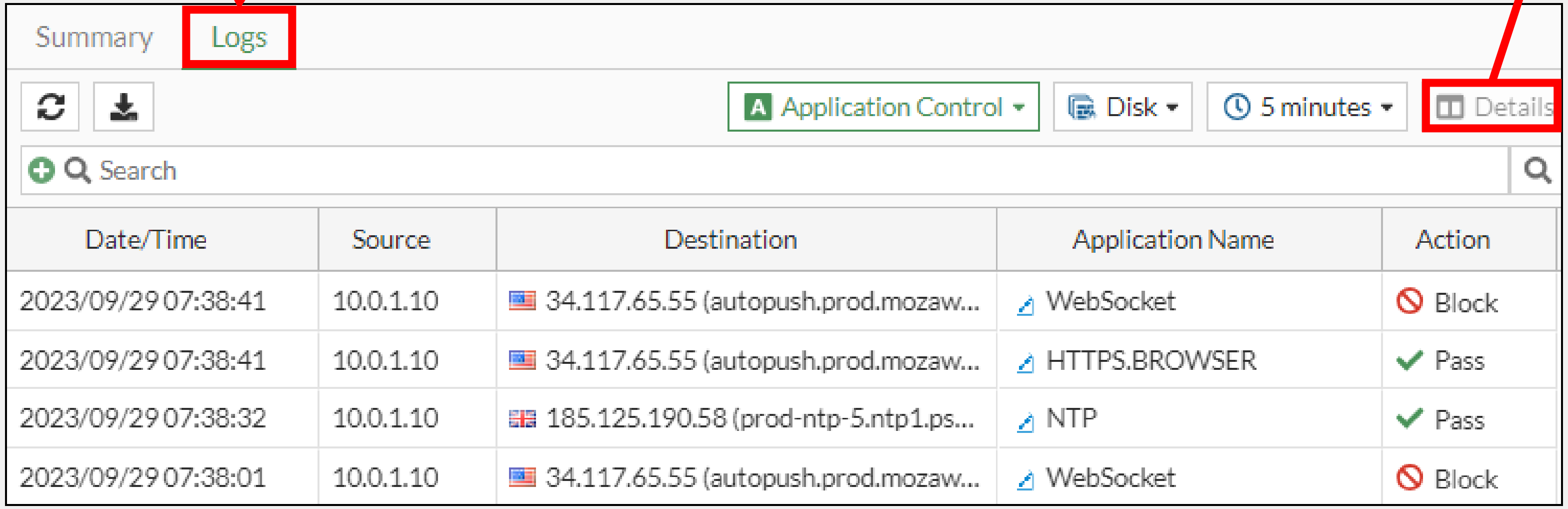


Summary Logs

51 Events

Application Control

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



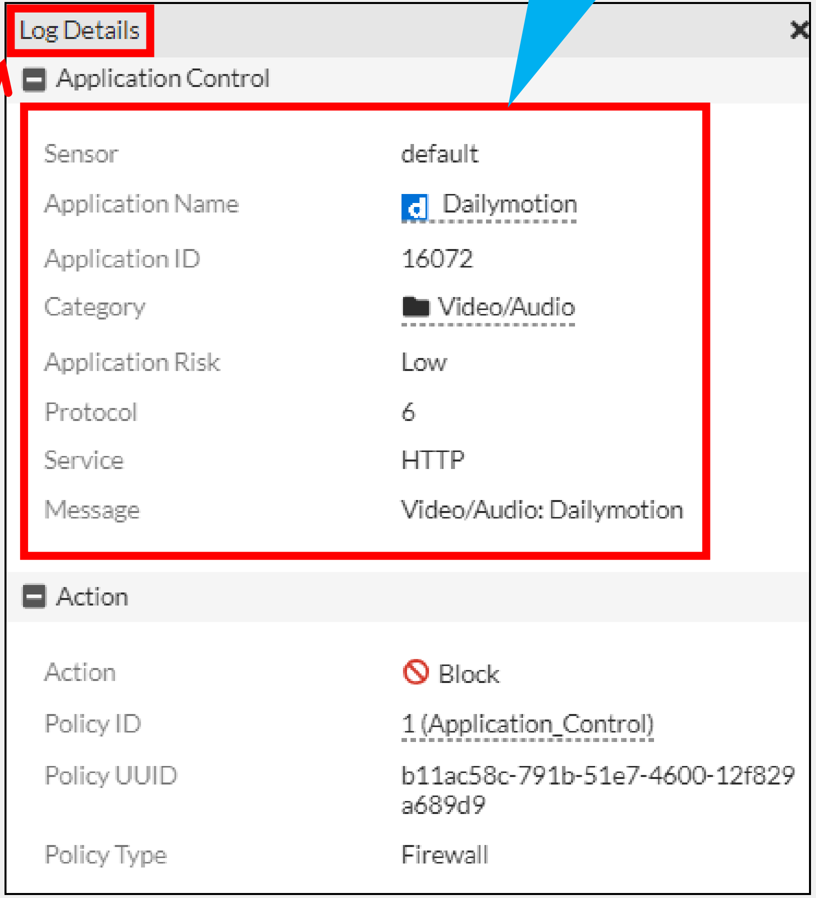
Summary Logs

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

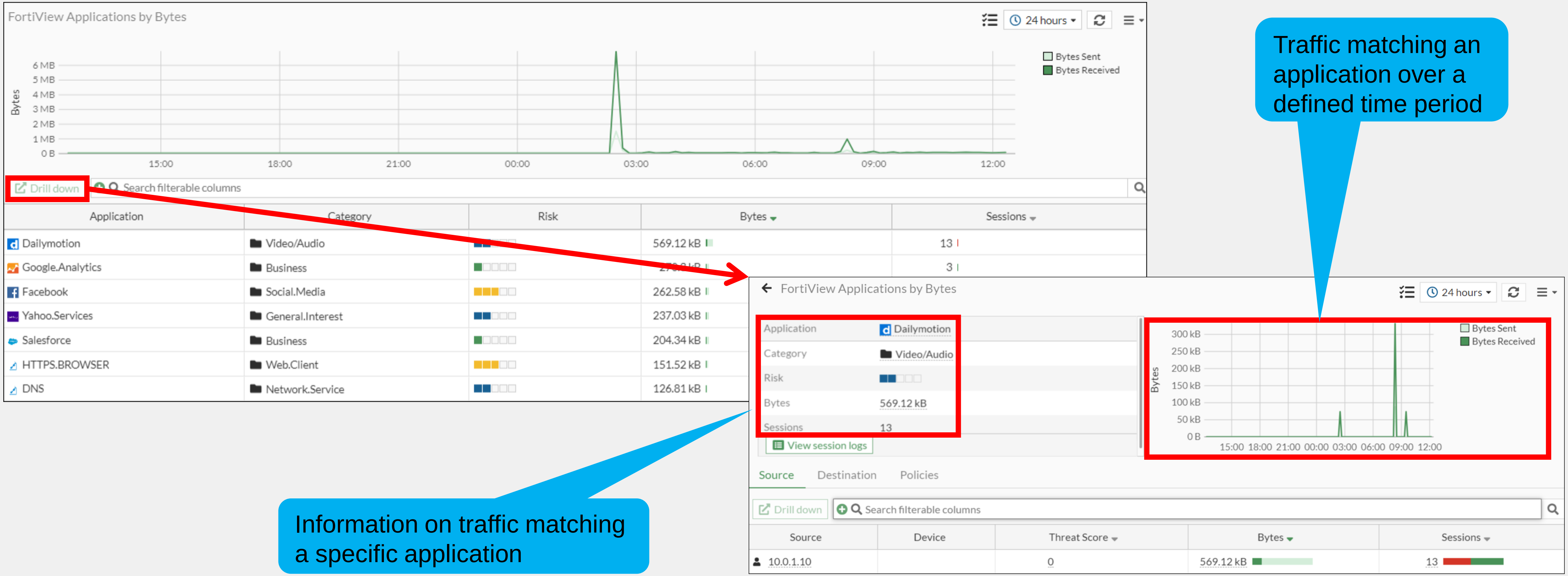
Action	Block
Policy ID	1 (Application_Control)
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall

FORTINET Training Institute

Troubleshoot Traffic Matching Application Control Profile

- Apply application control only to the traffic that requires it, and enable logging
- Review the logs and apply according configuration modifications

Dashboard > FortiView Applications



Application	Category	Risk	Bytes	Sessions
Dailymotion	Video/Audio	■■□□□	569.12 kB	13
Google.Analytics	Business	■□□□□	[illegible]	3
Facebook	Social.Media	■■■□□	262.58 kB	
Yahoo.Services	General.Interest	■■□□□	237.03 kB	
Salesforce	Business	■□□□□	204.34 kB	
HTTPS.BROWSER	Web.Client	■■■□□	151.52 kB	
DNS	Network.Service	■■□□□	126.81 kB	

Application	Dailymotion
Category	Video/Audio
Risk	■■□□□
Bytes	569.12 kB
Sessions	13

Source	Device	Threat Score	Bytes	Sessions
10.0.1.10		0	569.12 kB	13

Traffic matching an application over a defined time period

Information on traffic matching a specific application

Knowledge Check

1. Which IPS action allows traffic and logs the activity?

   A. Allow

   ✓ B. Monitor

2. Which statement about application control is true?

   ✓ A. Application control uses the IPS engine to scan traffic for application patterns.

   B. Application control is unable to scan P2P architecture traffic.

3. Which statement about the HTTP block page for application control is true?

   ✓ A. It can be used only for web applications.

   B. It works for all types of applications.

Review

- ✓ Configure an intrusion prevention system (IPS) sensor
- ✓ Troubleshoot IPS high-CPU usage
- ✓ Configure application control in profile mode
- ✓ Monitor application control events
- ✓ Troubleshoot traffic matching with application control profile issues