FORTIGATE SECURITY PROFILES

→

WHAT ARE SECURITY PROFILES?

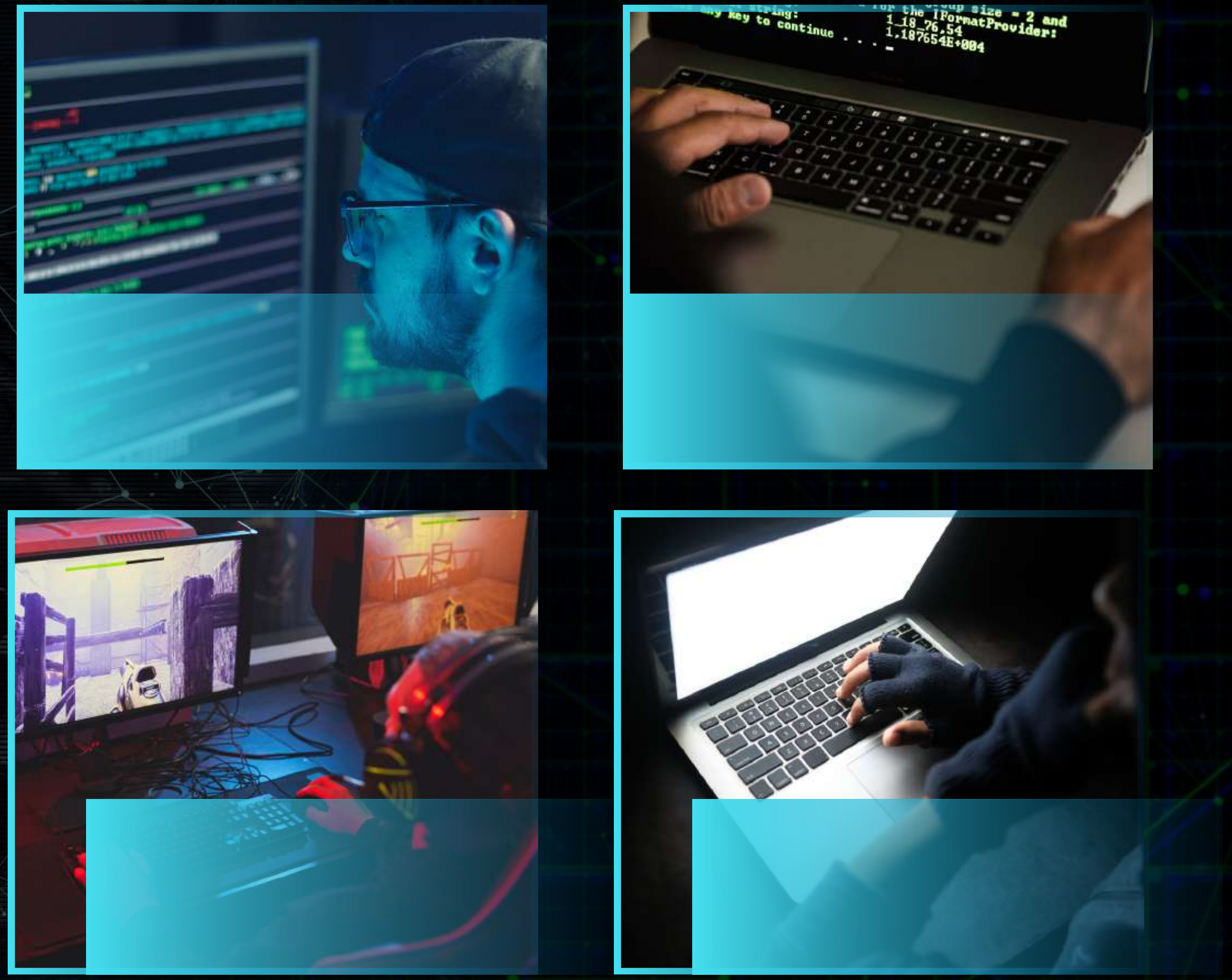
SECURITY PROFILES IN FORTIGATE ARE SECURITY FEATURES APPLIED TO FIREWALL POLICIES TO INSPECT AND PROTECT TRAFFIC.

- THEY PROVIDE PROTECTION AGAINST
- MALWARE AND VIRUSES
- MALICIOUS WEBSITES
- APPLICATION MISUSE
- INTRUSIONS AND EXPLOITS
- DNS-BASED ATTACKS
- EMAIL THREATS

TYPES OF SECURITY PROFILES

FORTIGATE SUPPORTS MULTIPLE PROTECTION MODULES INCLUDING:

- ANTIVIRUS
- WEB FILTERING
- APPLICATION CONTROL
- IPS (INTRUSION PREVENTION SYSTEM)
- DNS FILTERING
- EMAIL FILTERING
- SSL/SSH INSPECTION
- SANDBOX INTEGRATION



1.1-ANTIVIRUS

WHAT IS ANTIVIRUS PROTECTION?

The Antivirus profile scans network traffic to detect and block:

- Viruses
- Malware
- Trojans
- Worms
- Suspicious files
- Inspection methods:
- Flow-based inspection
- Proxy-based inspection

1.2-ANTIVIRUS

ANTIVIRUS FEATURES

Key features include:

- Real-time malware scanning
- Signature-based detection
- Heuristic analysis
- File quarantine
- Behavioral detection
- Cloud-assisted lookup (FortiGuard)

→

IMPORTANT ANTIVIRUS SETTINGS

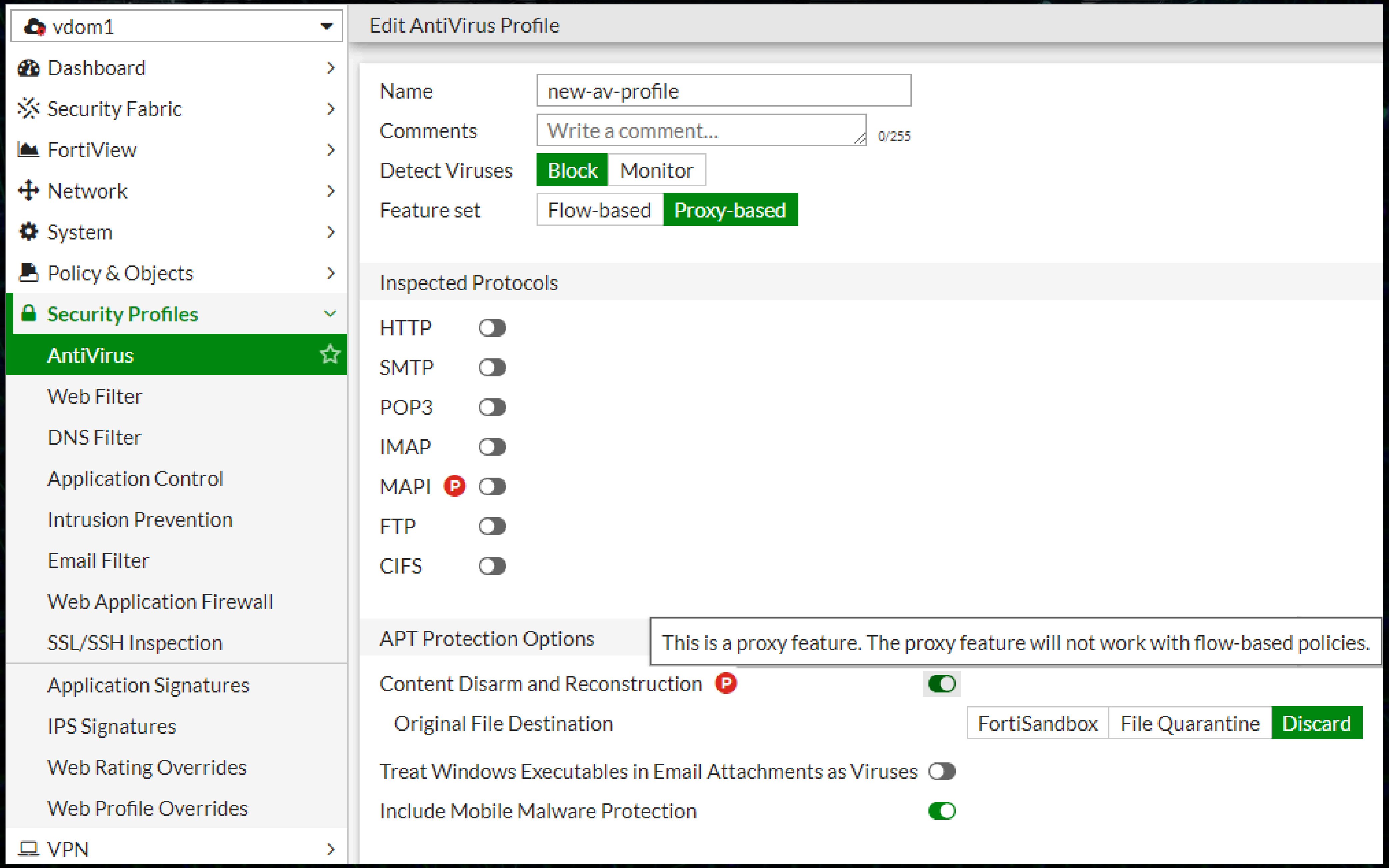
Common configuration options:

- Inspection Mode: Proxy or Flow-based
- File Type Filtering: Block specific file types
- Actions: Allow, Block, Quarantine
- Scan Thresholds: Maximum file size
- Logging: Log all malware events

→

1.4-ANTIVIRUS

ANTIVIRUS PROFILE IN THE GUI



Edit AntiVirus Profile

Name: new-av-profile

Comments: Write a comment... 0/255

Detect Viruses: [✓ Block] Monitor

Feature set: Flow-based [✓ Proxy-based]

Inspected Protocols

- HTTP ○
- SMTP ○
- POP3 ○
- IMAP ○
- MAPI P ○
- FTP ○
- CIFS ○

APT Protection Options

This is a proxy feature. The proxy feature will not work with flow-based policies.

Content Disarm and Reconstruction P ●

Original File Destination: FortiSandbox File Quarantine [✓ Discard]

Treat Windows Executables in Email Attachments as Viruses ○

Include Mobile Malware Protection ●

WHAT IS WEB FILTERING?

Web Filtering controls user access to websites by:

- Categorizing URLs
- Blocking harmful or inappropriate content
- Applying browsing policies
- It protects users from phishing, malware sites, and unwanted content.

TYPES OF WEB FILTERING

FortiGate supports:

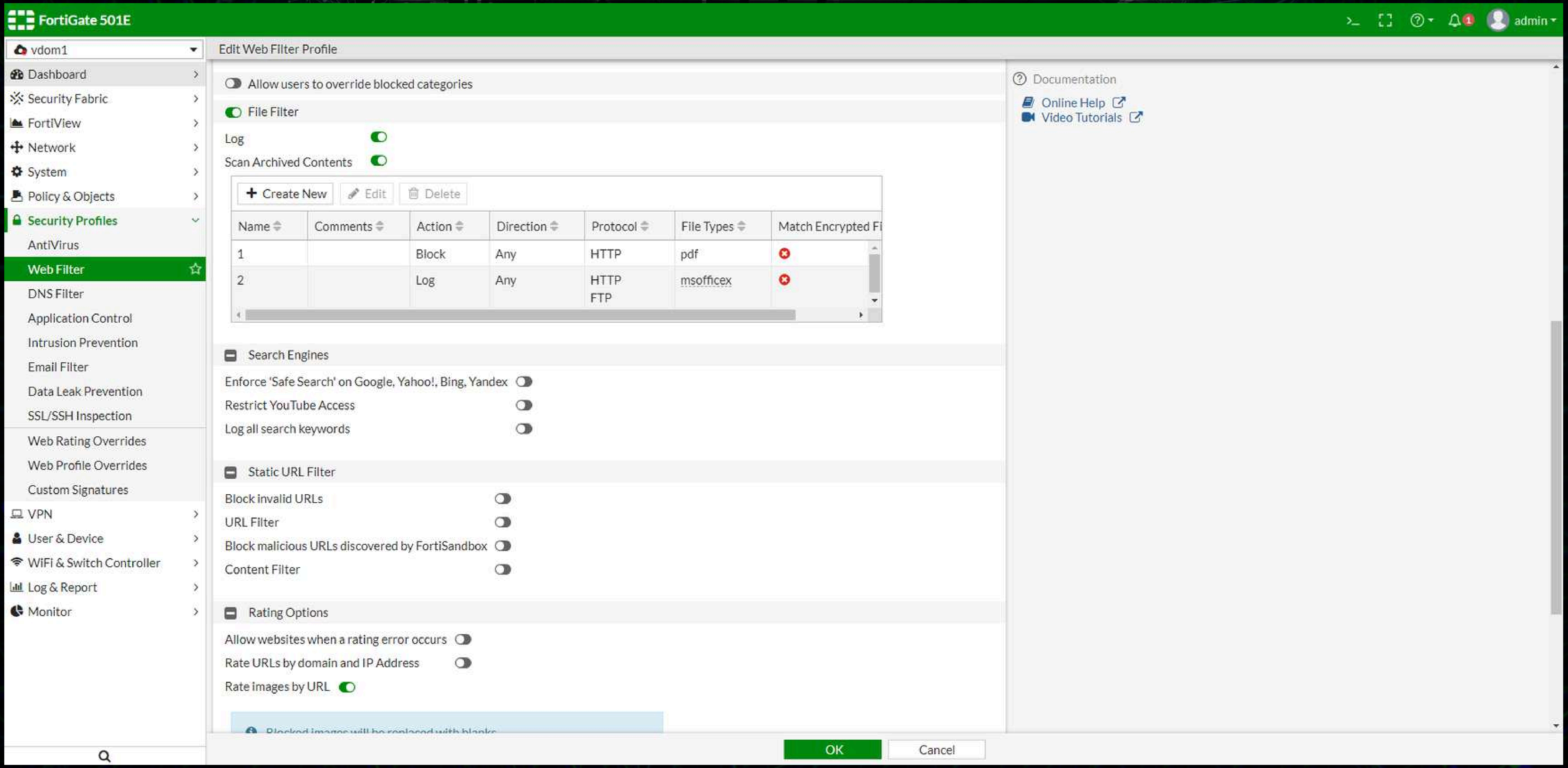
- Category-Based Filtering: Block whole categories (Gambling, Malware, etc.)
- URL Filtering: Allow/block specific URLs
- Content Filtering: Keywords or file downloads
- Safe Search Enforcement

IMPORTANT WEB FILTER SETTINGS

Key configurations:

- Allow / Block / Monitor rules
- SSL Deep Inspection requirement
- Web rating overrides
- Quota control (time / bandwidth limits)
- Logging blocked URLs

WEB FILTER GUI EXAMPLE



Edit Web Filter Profile

○ Allow users to override blocked categories

● File Filter

Log ●

Scan Archived Contents ●

Name	Comments	Action	Direction	Protocol	File Types	Match Encrypted Fi
1		Block	Any	HTTP	pdf	☒
2		Log	Any	HTTP FTP	msofficex	☒

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ○

Restrict YouTube Access ○

Log all search keywords ○

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 ○

Rate images by URL ●

Blocked images will be replaced with blanks

WHAT IS APPLICATION CONTROL?

Application Control identifies and controls applications in network traffic using DPI (Deep Packet Inspection).

It can detect:

- Social media
- Streaming apps
- VPN apps
- P2P applications
- Gaming apps

APPLICATION CONTROL FEATURES

Key features include:

- Block or allow specific applications
- Prioritize or limit bandwidth
- Prevent risky application use
- Control encrypted applications using SSL inspection
- Track user activity

→

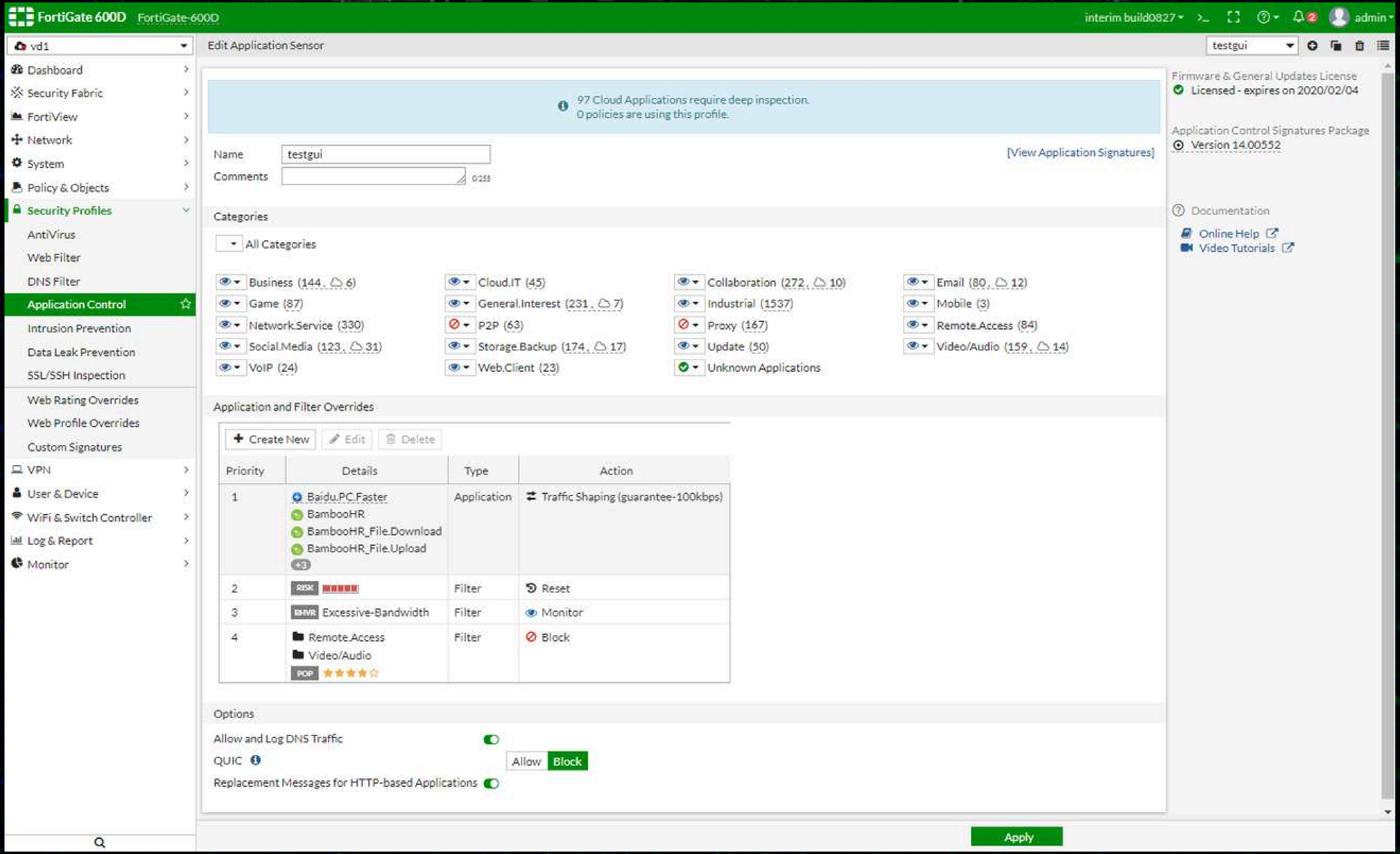
IMPORTANT APPLICATION CONTROL SETTINGS

Important options:

- Application categories (Cloud, Social Media, Gaming, etc.)
- Actions: Allow / Block / Monitor
- Traffic shaping rules
- Logging application sessions
- Protocol anomaly detection

3.4-APPLICATION CONTROL

APPLICATION CONTROL GUI



Edit Application Sensor

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

Name: testgui

Comments: 0/255

[View Application Signatures]

Firmware & General Updates License
✓ Licensed - expires on 2020/02/04

Application Control Signatures Package
Version 14.00552

Documentation
Online Help
Video Tutorials

Categories

All Categories

Business (144, 6)	Cloud.IT (45)	Collaboration (272, 10)	Email (80, 12)
Game (87)	General.Interest (231, 7)	Industrial (1537)	Mobile (3)
Network.Service (330)	⊘ P2P (63)	⊘ Proxy (167)	Remote.Access (84)
Social.Media (123, 31)	Storage.Backup (174, 17)	Update (50)	Video/Audio (159, 14)
VoIP (24)	Web.Client (23)	✓ Unknown Applications	

Application and Filter Overrides

Priority	Details	Type	Action
1	Baidu.PC.Faster BambooHR BambooHR_File.Download BambooHR_File.Upload +3	Application	Traffic Shaping (guarantee-100kbps)
2	RISK 🟥🟥🟥🟥🟥	Filter	Reset
3	BHVR Excessive-Bandwidth	Filter	Monitor
4	Remote.Access Video/Audio POP ★★★★☆	Filter	⊘ Block

Options

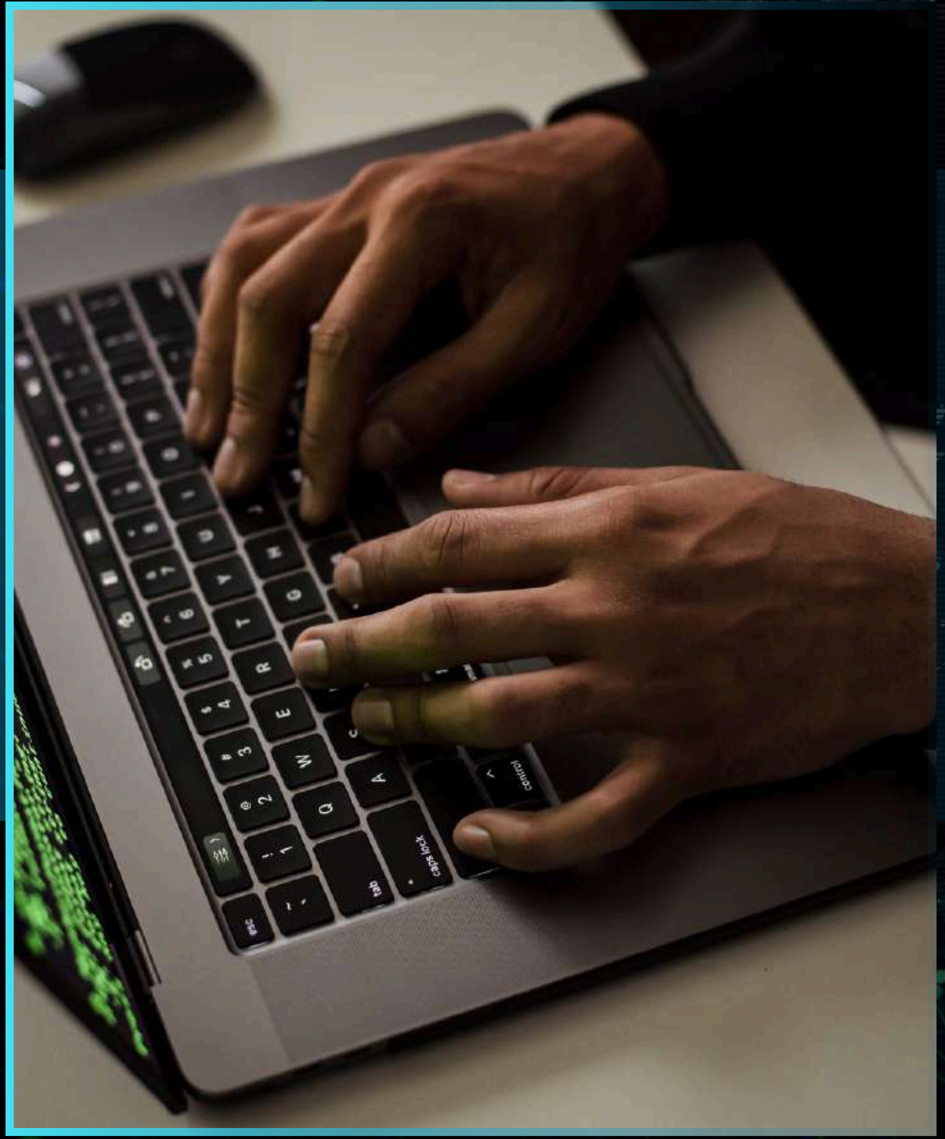
Allow and Log DNS Traffic: ●

QUIC: Allow [✓ Block]

Replacement Messages for HTTP-based Applications: ●

4.1-IPS

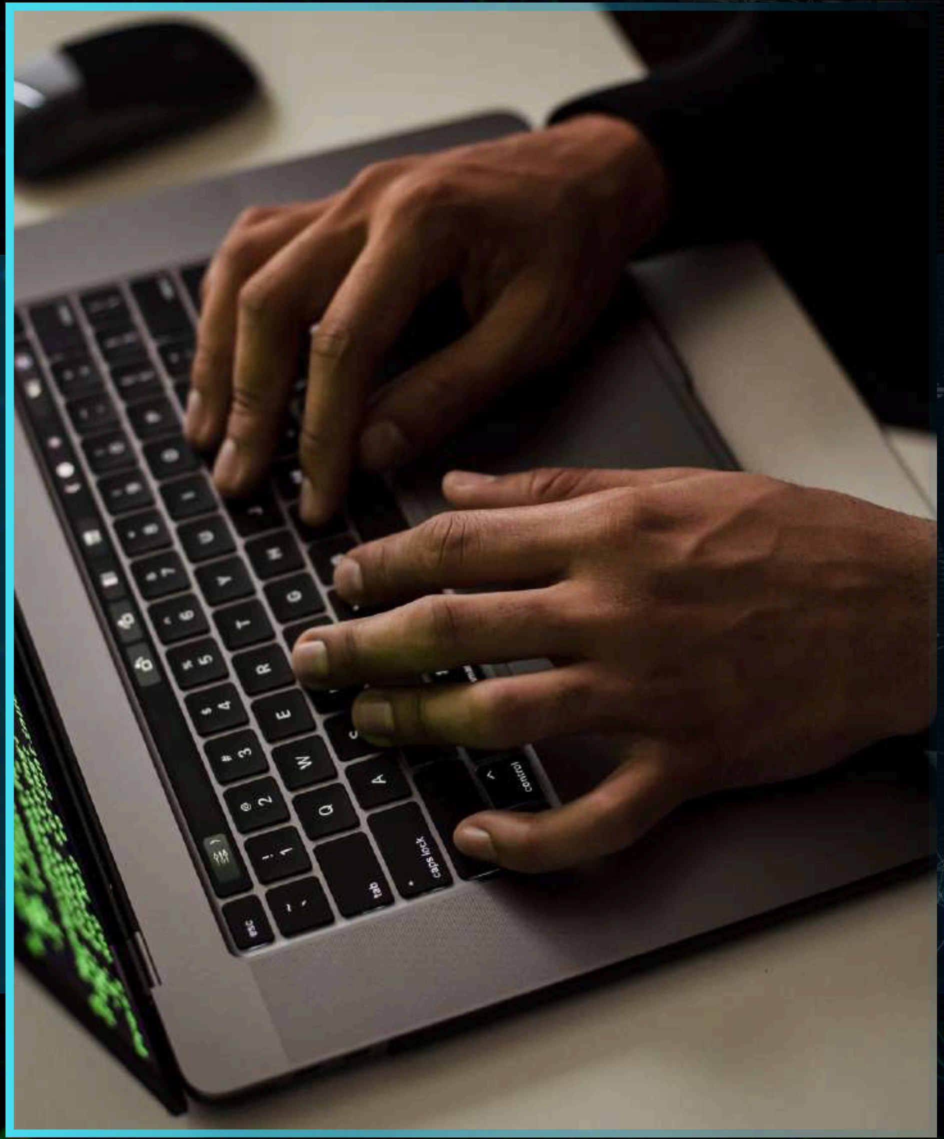
INTRUSION PREVENTION SYSTEM (IPS)



Important options:

- Application categories (Cloud, Social Media, Gaming, etc.)
- Actions: Allow / Block / Monitor
- Traffic shaping rules
- Logging application sessions
- Protocol anomaly detection

IPS FEATURES



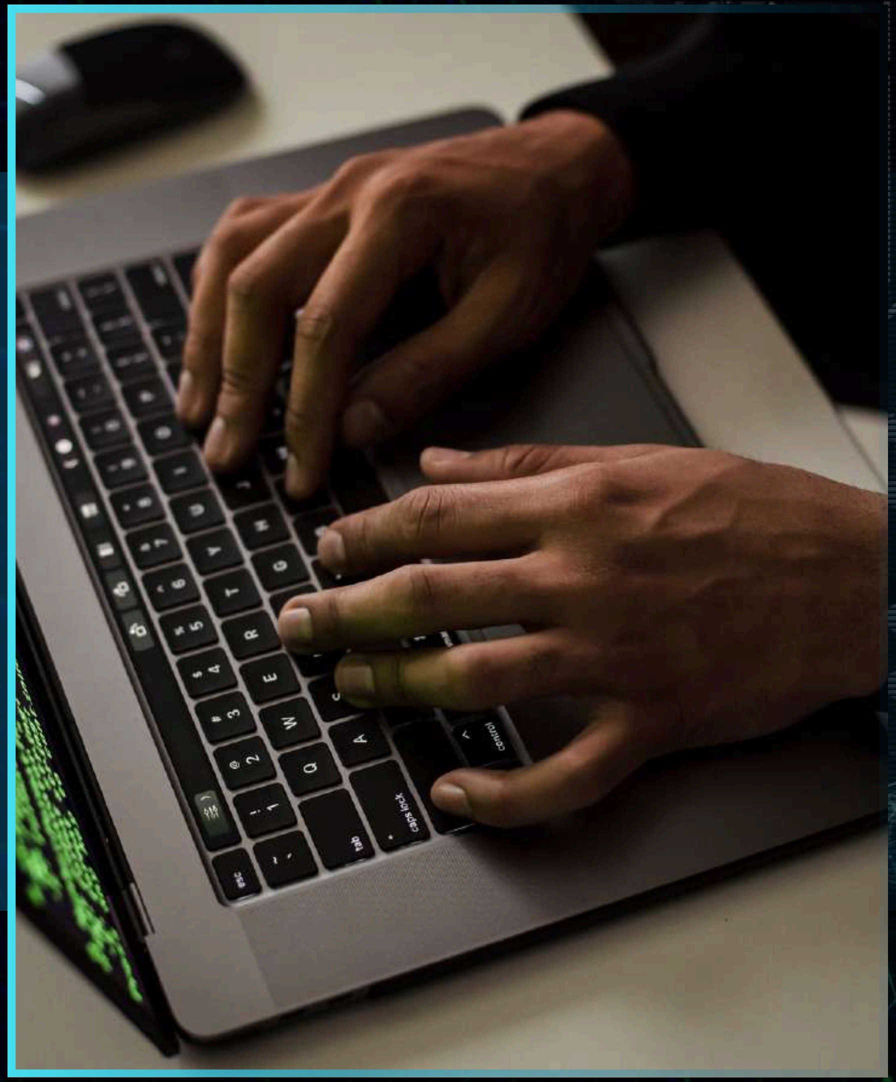
Key features:

- Signature-based detection
- Anomaly-based detection
- Virtual patching
- Rate-based attack blocking
- FortiGuard signature updates

→

4.3-IPS

IPS IMPORTANT SETTINGS

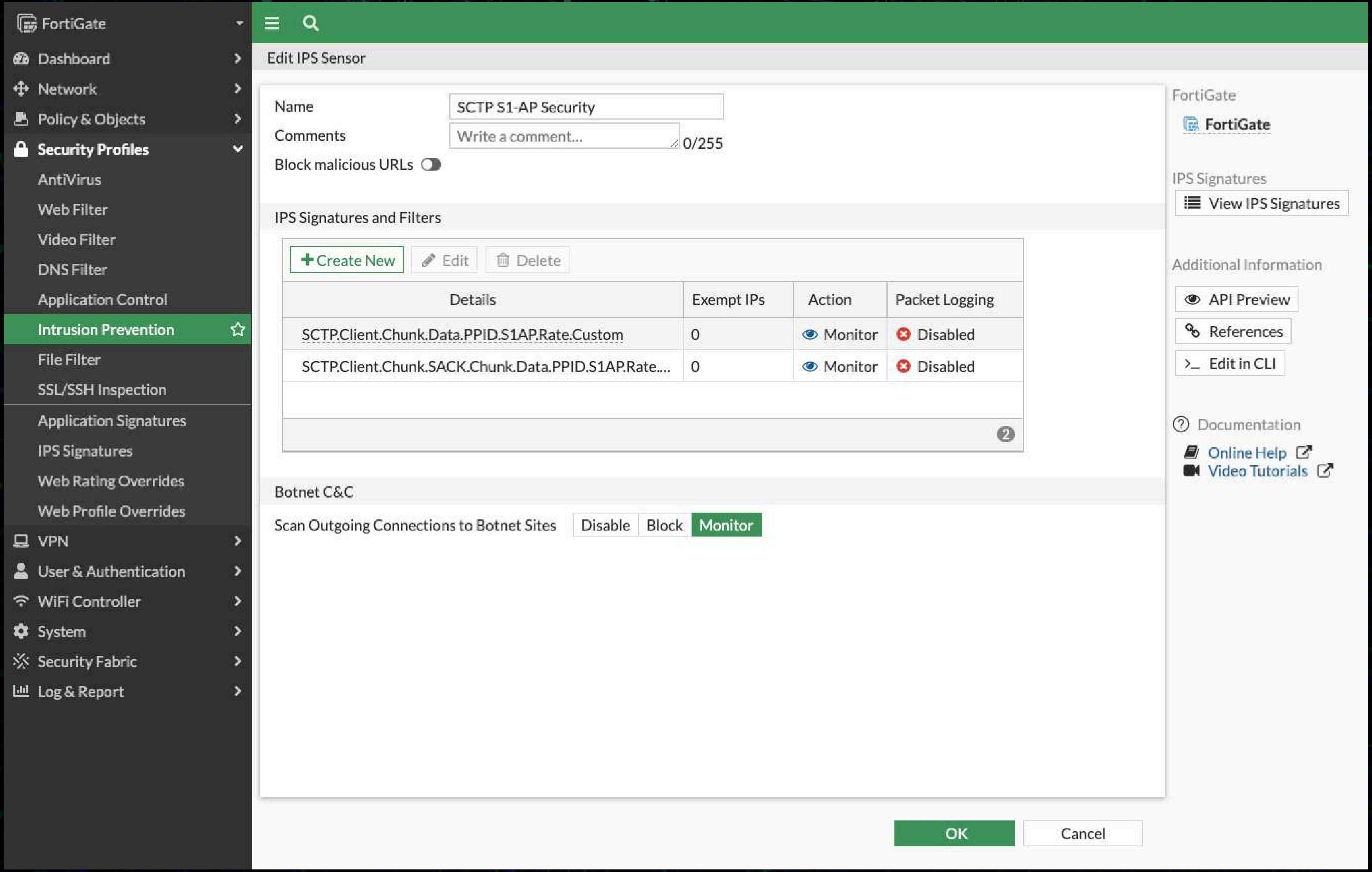


Key configuration items:

- Default, Strict, or Custom profile
- Packet logging
- Signature filters (OS, protocol, severity)
- Performance vs Security trade-off
- Blocking or monitoring actions

4.4-IPS

IPS GUI EXAMPLE



Edit IPS Sensor

Name: SCTP S1-AP Security

Comments: Write a comment... 0/255

Block malicious URLs ○

IPS Signatures and Filters

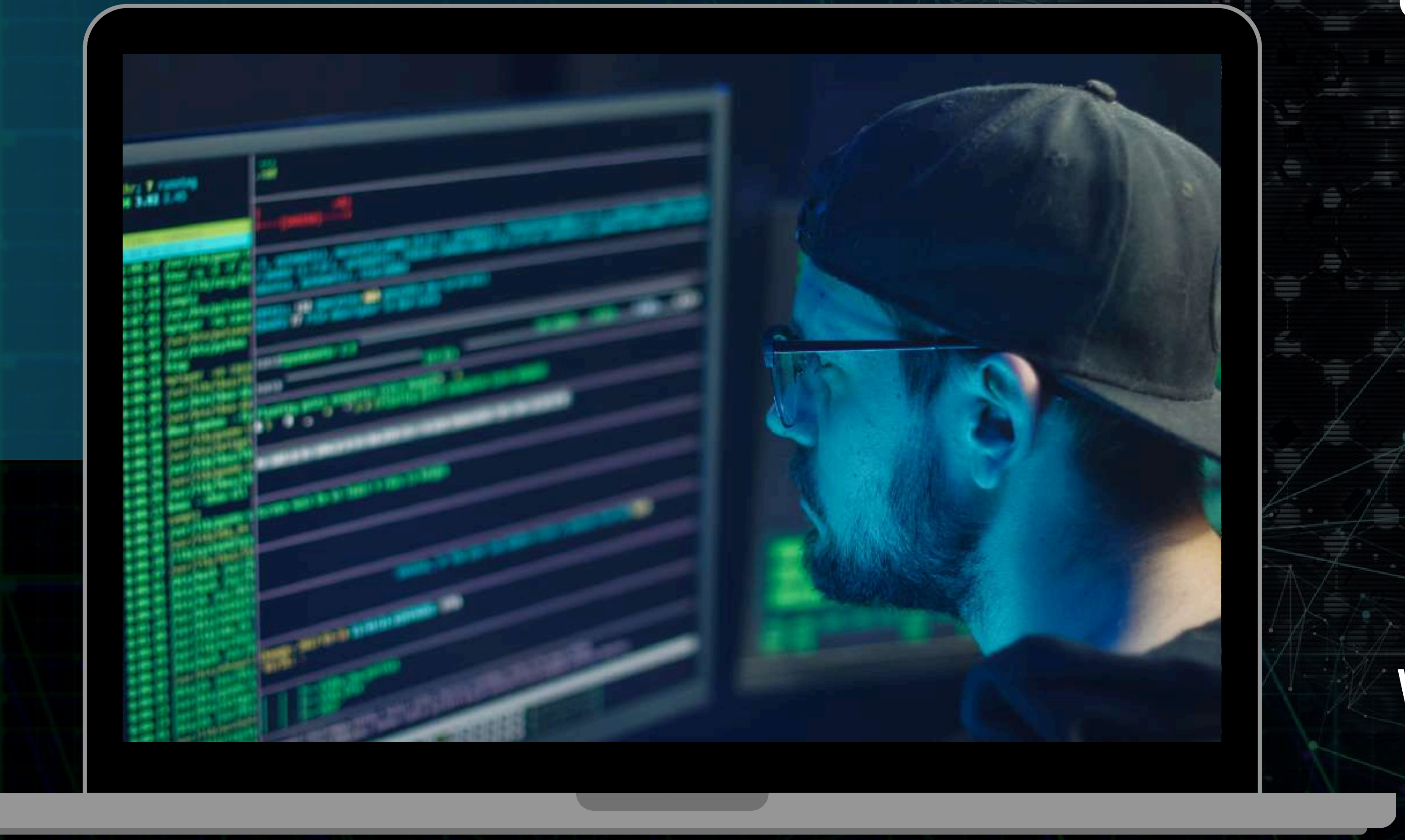
Details	Exempt IPs	Action	Packet Logging
SCTP.Client.Chunk.Data.PPID.S1AP.Rate.Custom	0	Monitor	Disabled
SCTP.Client.Chunk.SACK.Chunk.Data.PPID.S1AP.Rate....	0	Monitor	Disabled

Botnet C&C

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

5.1-DNS FILTERING

WHAT IS DNS FILTERING?

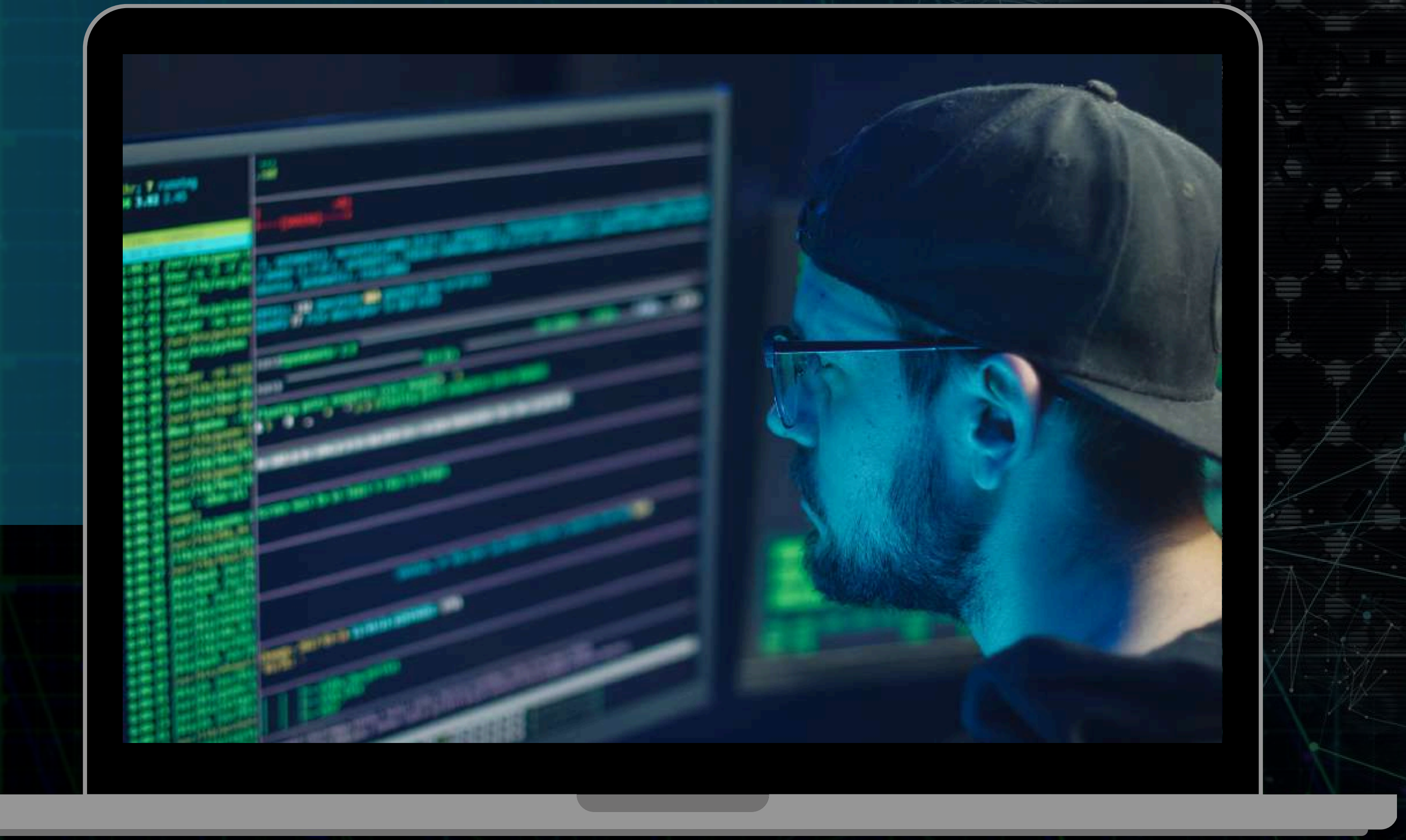


DNS Filtering protects users by controlling and blocking domains before connection is established.
It prevents:

- Malware command-and-control (C2)
- Phishing domains
- Botnet communications
- Adult / social media / high-risk categories
- DNS tunneling attacks

Works at DNS level → fast, lightweight, and effective.

DNS FILTER FEATURES



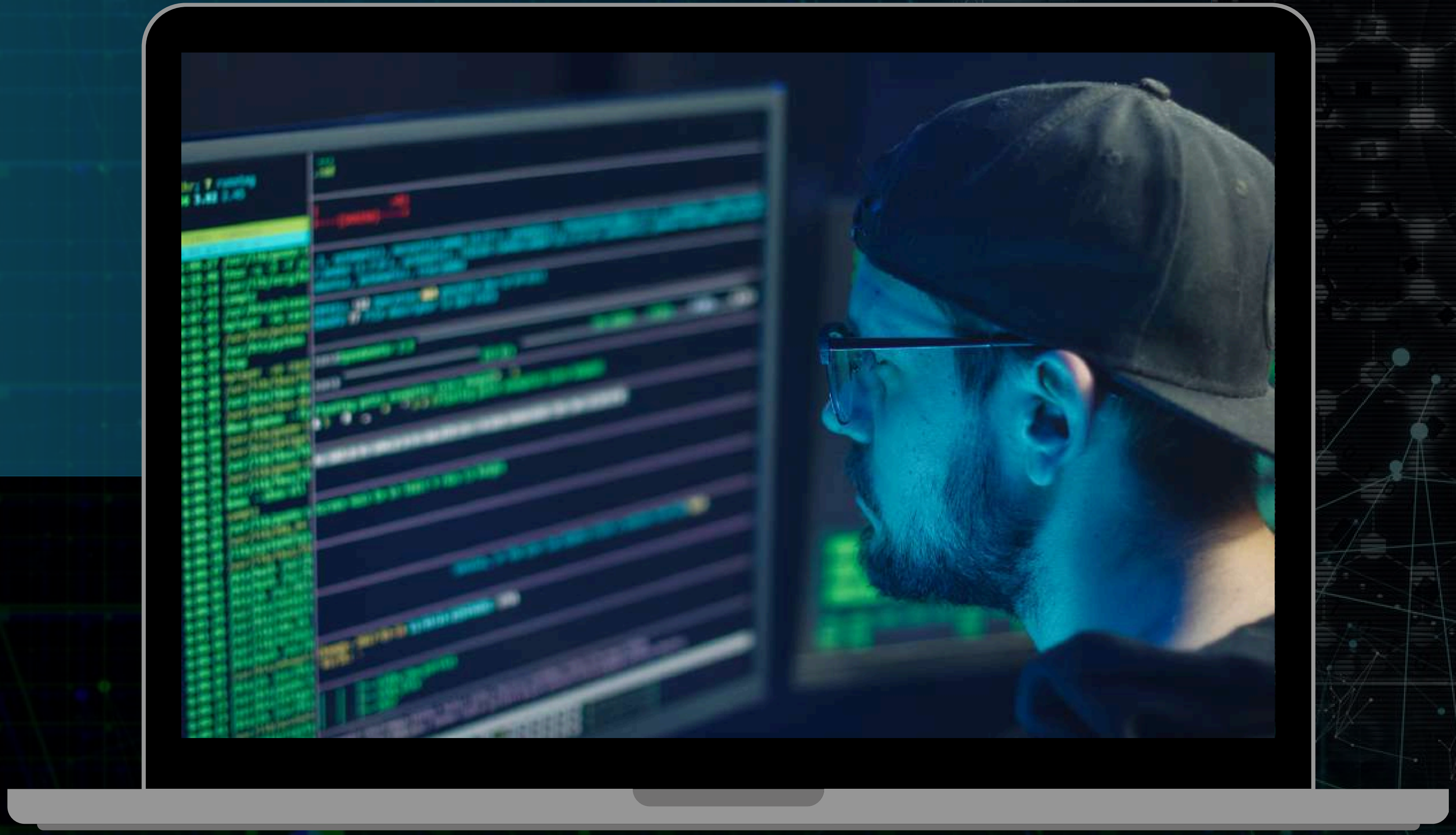
DMain capabilities include:

- Domain Categorization via FortiGuard
- Blocking Malicious and High-Risk Domains
- Real-Time Reputation Scoring
- Newly Registered Domain (NRD) Blocking
- DNS Tunneling Detection
- SafeSearch Enforcement
-

Additional benefits:

- Very low performance impact
- Works without decrypting traffic

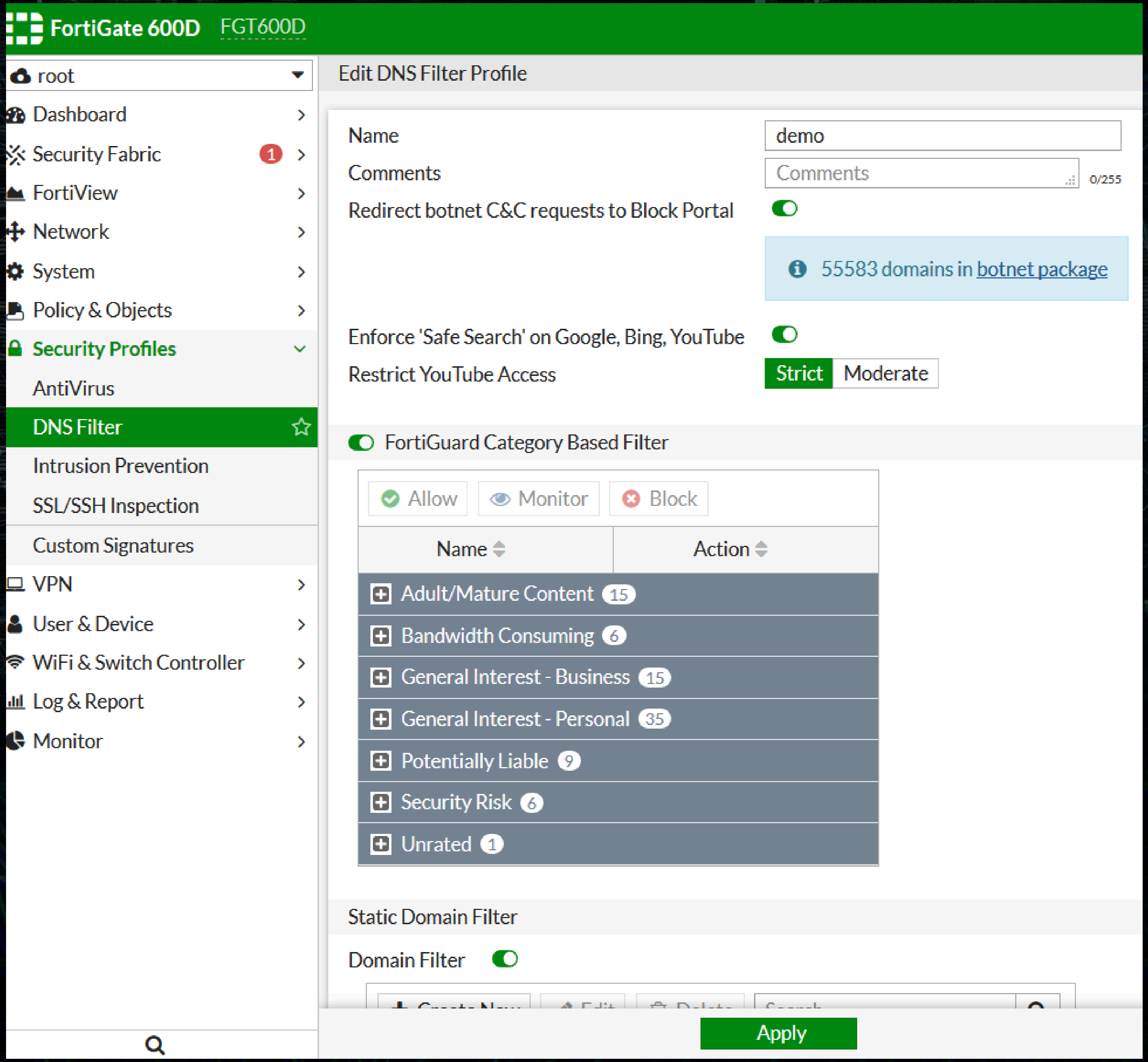
DNS FILTER IMPORTANT SETTINGS



Key configuration options:

- Category Filtering: Social media, malware, adult content, etc.
- Domain Overrides: Allow or block specific domains
- Reputation Threshold: High, Medium, Low
- DNS Logging: Log all DNS queries or blocked requests
- Response Actions: Block / Redirect / Monitor
- DoH Control: Prevent bypass using DNS-over-HTTPS

DNS FILTER GUI EXAMPLE



Edit DNS Filter Profile

Name: demo

Comments: Comments 0/255

Redirect botnet C&C requests to Block Portal ●

55583 domains in botnet package

Enforce 'Safe Search' on Google, Bing, YouTube ●

Restrict YouTube Access [✓ Strict] Moderate

● FortiGuard Category Based Filter

Name	Action
⊞ Adult/Mature Content 15	
⊞ Bandwidth Consuming 6	
⊞ General Interest - Business 15	
⊞ General Interest - Personal 35	
⊞ Potentially Liable 9	
⊞ Security Risk 6	
⊞ Unrated 1	

Static Domain Filter

Domain Filter ●

6.1-EMAIL FILTERING

WHAT IS EMAIL FILTERING?

Email Filtering protects against message-based threats by scanning SMTP traffic and analyzing email metadata.

It blocks:

- Spam
- Phishing messages
- Malicious attachments
- Fake or spoofed sender addresses

Focuses on email traffic security & authenticity

→

EMAIL FILTER FEATURES

EKey feature set:

- Header Inspection (sender/receiver validation)
- Attachment Scanning
- MIME Type Filtering
- Anti-Spam Scoring
- Keyword Filtering
- Spoof Detection
- URL Scanning inside emails

Advanced functions:

- Quarantine suspicious messages
- Allow/Block lists for senders

6.3-EMAIL FILTERING

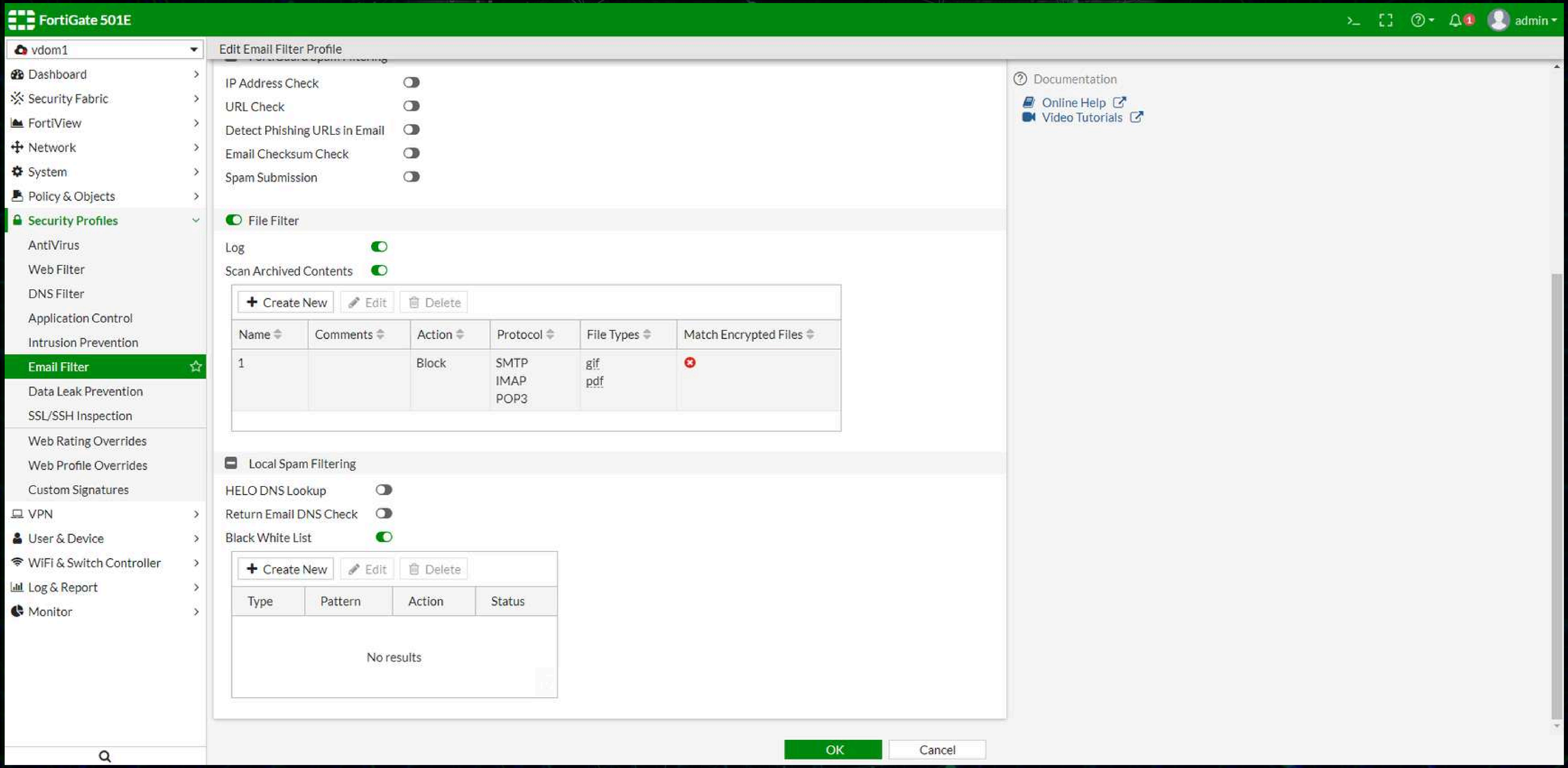
IMPORTANT EMAIL FILTER SETTINGS

Configuration includes:

- Spam Action: Tag / Block / Quarantine
- Attachment Filtering: Block executable or risky extensions
- Keyword Matching: Subject and body filters
- Black/White Lists: Emails or domains
- Heuristic and Reputation Scoring: Identify suspicious patterns
- Mail Header Anomaly Check

6.4-EMAIL FILTERING

EMAIL FILTER GUI EXAMPLE



Edit Email Filter Profile

FortiGuard Spam Filtering

- IP Address Check ○
- URL Check ○
- Detect Phishing URLs in Email ○
- Email Checksum Check ○
- Spam Submission ○

● File Filter

- Log ●
- Scan Archived Contents ●

+ Create New | Edit | Delete

Name	Comments	Action	Protocol	File Types	Match Encrypted Files
1		Block	SMTP IMAP POP3	gif pdf	✗

Local Spam Filtering

- HELO DNS Lookup ○
- Return Email DNS Check ○
- Black White List ●

+ Create New | Edit | Delete

Type	Pattern	Action	Status
	No results		

OK | Cancel

WHAT IS SSL/SSH INSPECTION?

SSL/SSH Inspection is used to decrypt encrypted traffic so FortiGate can inspect it with:

- Antivirus
- Web Filter
- Application Control
- IPS
- DLP
- Sandbox

Encrypted traffic includes HTTPS, SSH, SMTPS, IMAPS, and more.

DEEP VS CERTIFICATE INSPECTION

1. Full (Deep) Inspection
   - Decrypts and inspects full traffic content
   - Highest security level
   - Requires installing FortiGate CA on clients

2. Certificate Inspection
   - Only inspects certificate information
   - Does NOT decrypt the content
   - Lower security but higher privacy

WHY SSL INSPECTION IS ESSENTIAL

Most modern attacks use encryption to avoid detection.
SSL Inspection enables detection of:

- Malware inside HTTPS downloads
- Encrypted phishing sites
- Hidden C2 traffic
- Encrypted application traffic
- TLS-based exploit delivery
-

Without SSL Inspection → more than 70% of threats pass unnoticed.

SSL/SSH INSPECTION FEATURES

Key features:

- TLS 1.3 support
- Deep inspection of HTTPS
- SSH command inspection
- Certificate validation
- SNI-based detection
- Exemption list for privacy sites
- Full logging of decrypted sessions

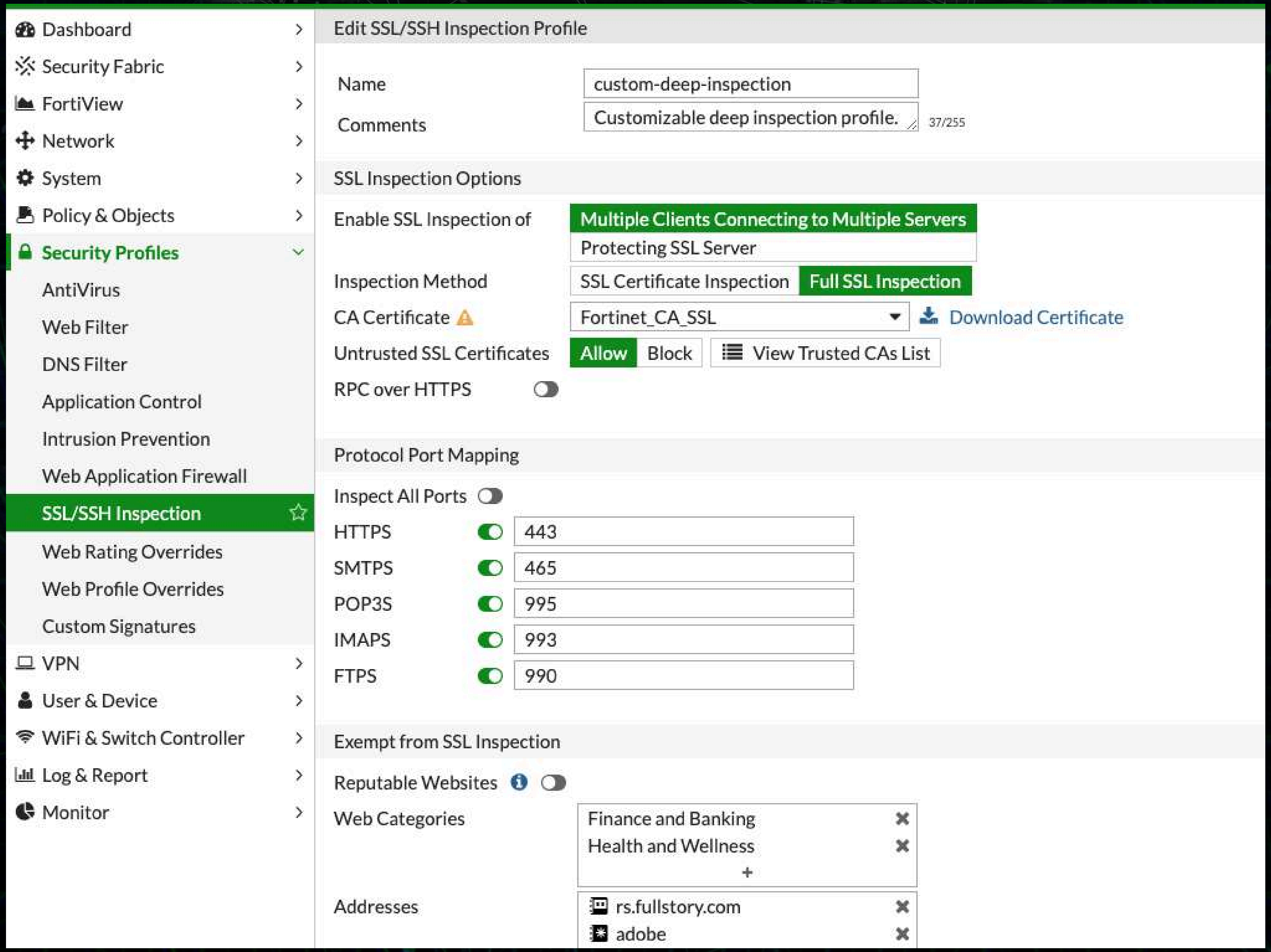
IMPORTANT SSL/SSH SETTINGS

Configurable options:

- Full vs Certificate inspection mode
- Allowed/blocked SSL versions
- CA certificate installation
- Inspection profiles per firewall policy
- Exempt categories:
  - Banking
  - Healthcare
  - Government services
- Session logging & warnings

→

SSL/SSH GUI EXAMPLE



Edit SSL/SSH Inspection Profile

Name: custom-deep-inspection

Comments: Customizable deep inspection profile. 37/255

SSL Inspection Options

Enable SSL Inspection of: [✓ Multiple Clients Connecting to Multiple Servers] Protecting SSL Server

Inspection Method: SSL Certificate Inspection [✓ Full SSL Inspection]

CA Certificate ⚠: Fortinet_CA_SSL ▾ Download Certificate

Untrusted SSL Certificates: [✓ Allow] Block View Trusted CAs List

RPC over HTTPS: ○

Protocol Port Mapping

Inspect All Ports: ○

HTTPS	●	443
SMTPS	●	465
POP3S	●	995
IMAPS	●	993
FTPS	●	990

Exempt from SSL Inspection

Reputable Websites ℹ ○

Web Categories: Finance and Banking ✖
Health and Wellness ✖
+

Addresses: rs.fullstory.com ✖
adobe ✖

WHAT IS FORTISANDBOX?

FortiSandbox analyzes suspicious files in an isolated virtual environment to detect:

- Zero-day attacks
- Ransomware
- Polymorphic malware
- Unknown file behaviors
- Script-based attacks

It observes file behavior instead of relying only on signatures.

→

8.1- FORTISANDBOX

HOW SANDBOX WORKS

Workflow:

1. File is scanned by FortiGate
2. If suspicious → submitted to Sandbox
3. Sandbox runs the file in a virtual machine
4. Behavior is monitored (API calls, registry edits, file actions...)
5. Verdict: Clean / Suspicious / Malicious
6. FortiGate blocks or quarantines accordingly

SANDBOX FEATURES

Core capabilities:

- Multi-VM analysis (Windows/Linux)
- Static + dynamic analysis
- Script and macro emulation
- Ransomware detonation chamber
- Real-time threat intelligence
- Automatic signature sharing back to FortiGat

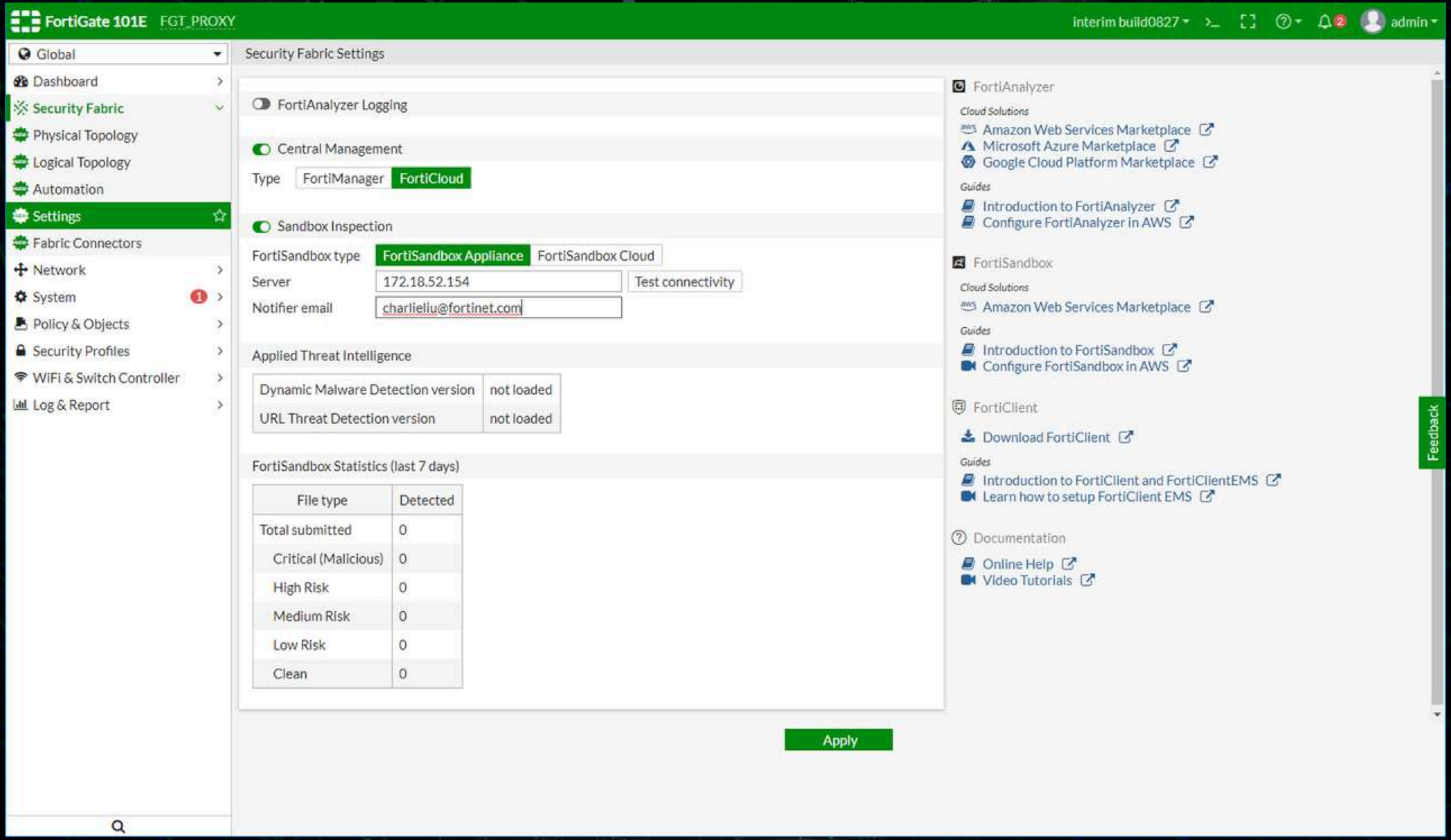
SANDBOX SETTINGS IN FORTIGATE

Important options:

- File submission types (EXE, DOC, PDF, JS, etc.)
- Size limits
- Cloud vs On-prem Sandbox
- Quarantine on malicious verdict
- Logging & alerting
- Integration with AV, Web Filter, and Email Filter

8.5- FORTISANDBOX

SANDBOX GUI EXAMPLE



Security Fabric Settings

○ FortiAnalyzer Logging

● Central Management

Type: FortiManager [✓ FortiCloud]

● Sandbox Inspection

FortiSandbox type: [✓ FortiSandbox Appliance] FortiSandbox Cloud

Server: 172.18.52.154 Test connectivity

Notifier email: charlieliu@fortinet.com

Applied Threat Intelligence

Dynamic Malware Detection version	not loaded
URL Threat Detection version	not loaded

FortiSandbox Statistics (last 7 days)

File type	Detected
Total submitted	0
Critical (Malicious)	0
High Risk	0
Medium Risk	0
Low Risk	0
Clean	0

CONCLUSION

FortiGate Security Profiles work together to deliver layered, intelligent protection across the entire network.

From DNS and Email filtering to IPS, Application Control, SSL inspection, and Sandbox analysis, each profile blocks a specific class of threats and enhances visibility.

By combining these profiles within firewall policies, organizations achieve stronger security, better control over traffic and applications, and a safer, more reliable network environment.

THANK YOU

←