



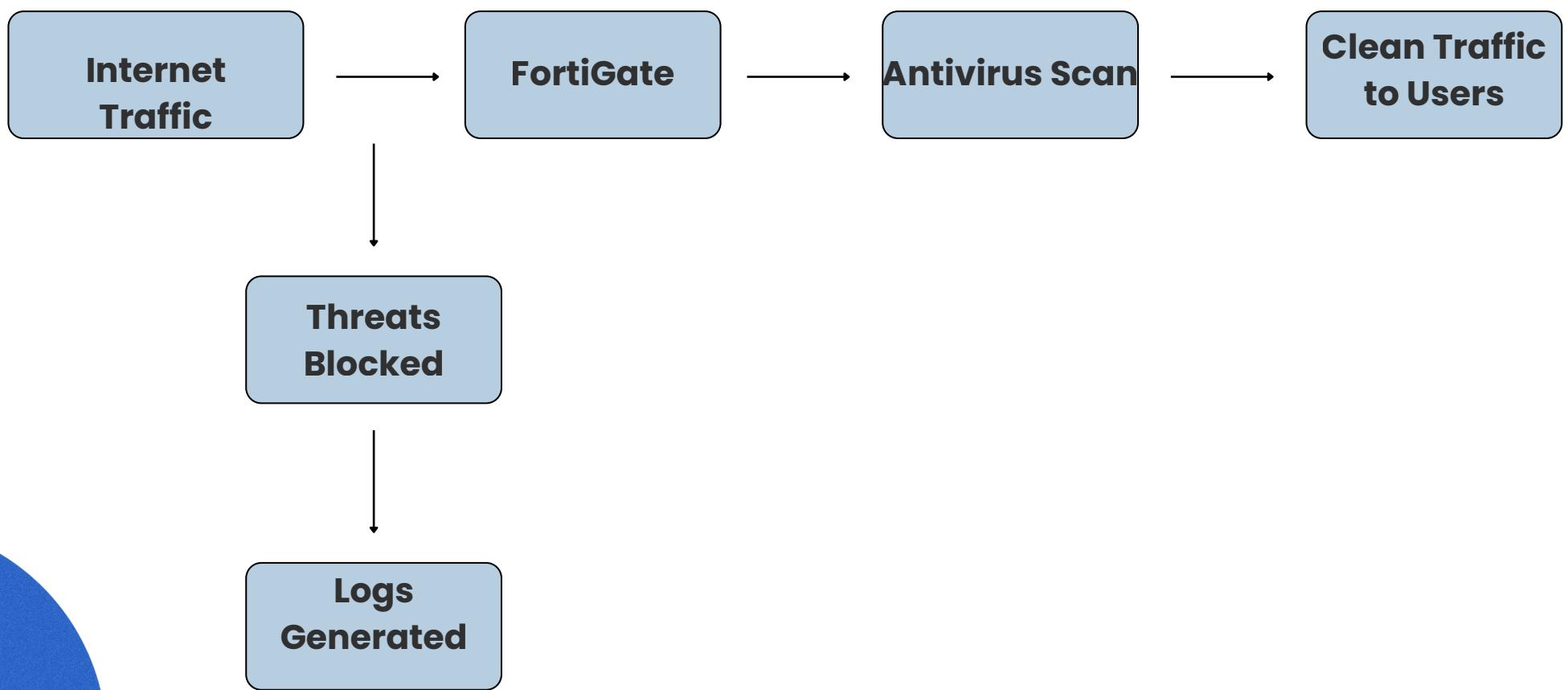
# FortiGate Security Profiles

Project 4: Advanced FortiGate Security  
Profiles

by:  
Nada nasr  
eman moamen  
Seif Wael  
Ahmed Osama  
shahd osama

# Week 1: Understanding Antivirus

We successfully implemented FortiGate's Antivirus protection using flow-based inspection across all major protocols. The profile was integrated into our main Internet firewall policy, providing real-time scanning for all outbound traffic with automatic blocking and quarantine capabilities.



# Week 2: Configuration

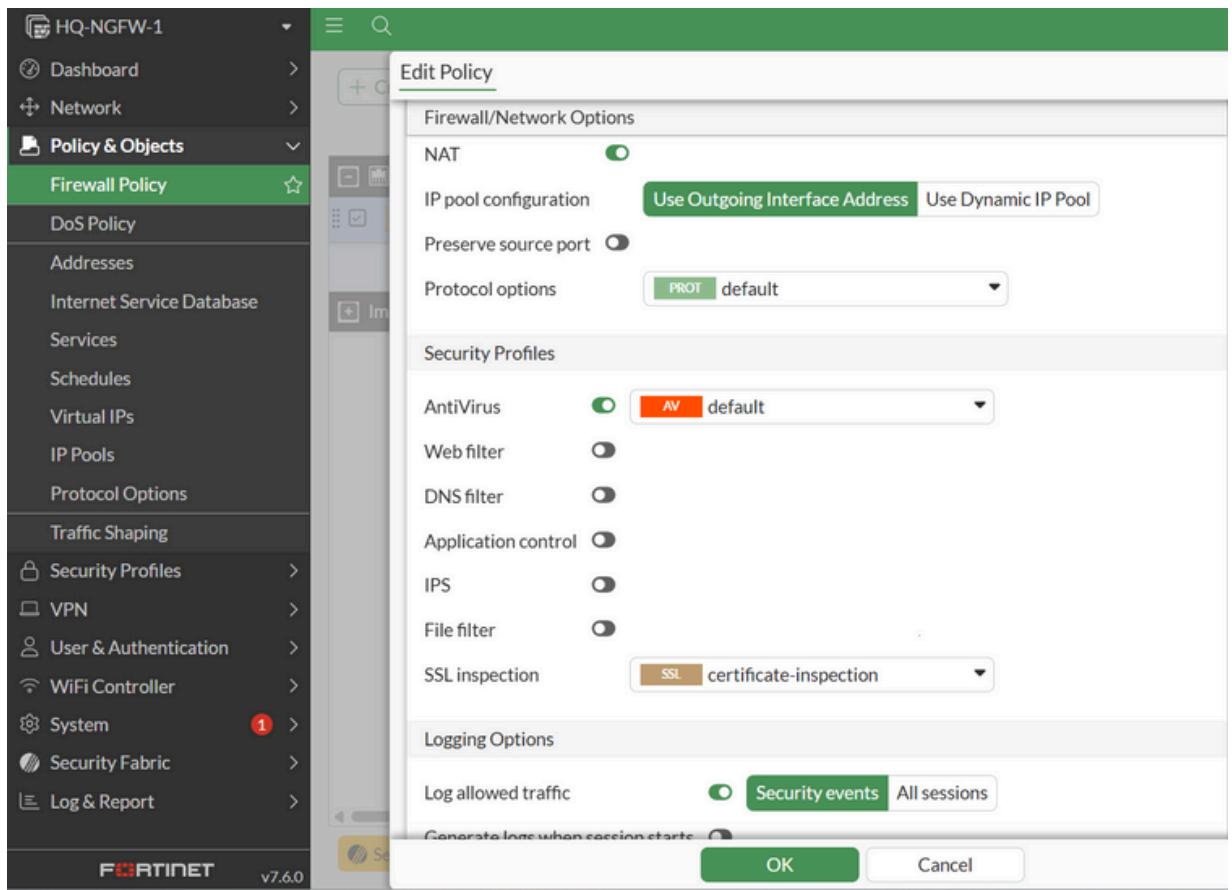
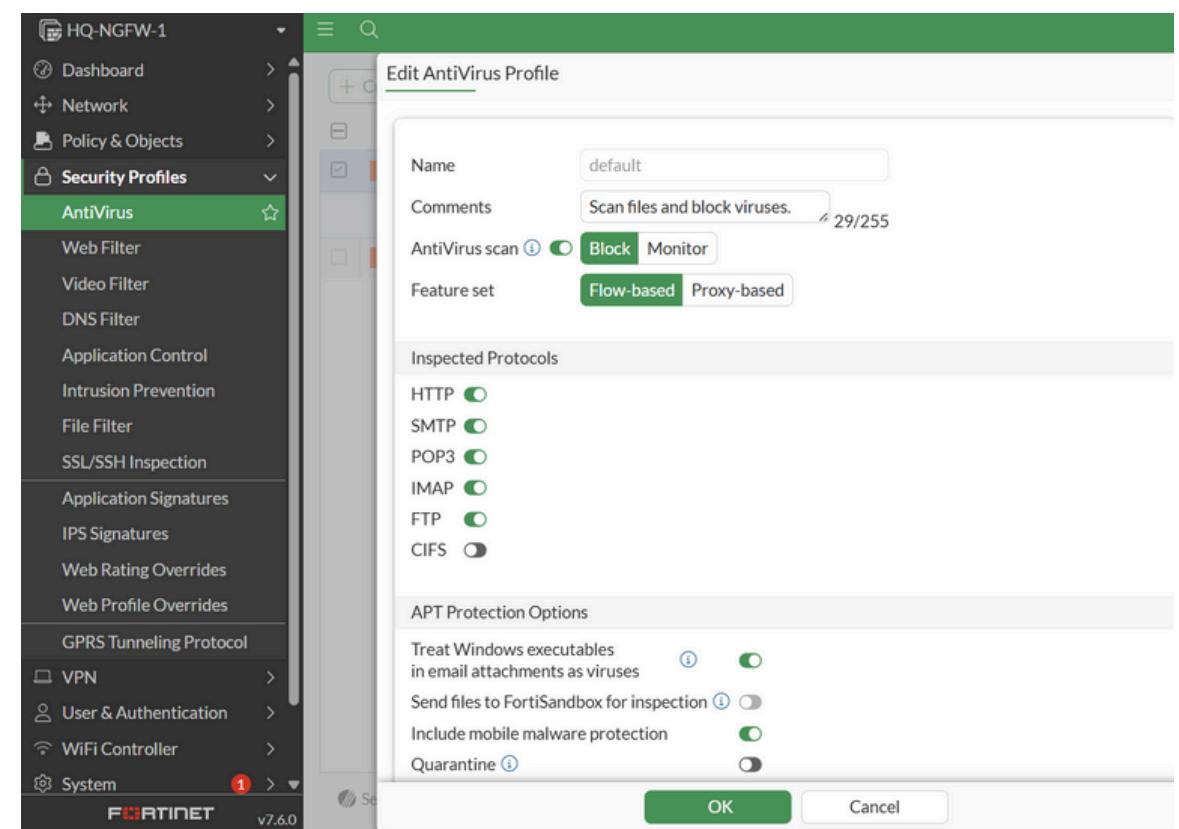
Steps Taken:

Feature verification

profile creation

actions / Protocols

firewall policy

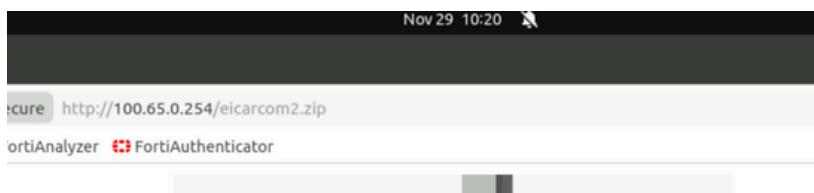


# Week 3: Monitoring

## Threat DETECTION

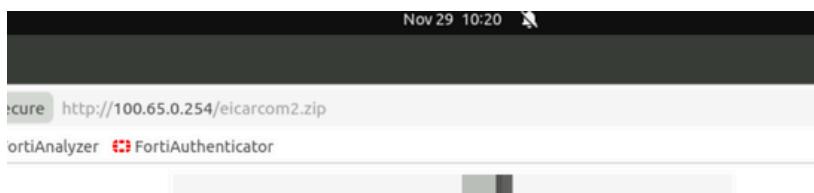
- EICAR test files identified
- Multiple formats detected:
  - .txt files
  - .zip archives
- Instant threat recognition

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action	Infection Type
2025/11/29 10:20:24	HTTP	10.0.11.50	eicar.com.txt	EICAR_TEST_FILE		URL: http://100.65.0.254/eicar.com.txt	Blocked	Malicious
2025/11/29 10:19:40	HTTP	10.0.11.50	eicarcom2.zip	EICAR_TEST_FILE		URL: http://100.65.0.254/eicarcom2.zip	Blocked	Malicious



## User Protection

- Clear user block pages
- Educational messaging
- Connection termination
- Zero infections



## COMPLETE LOGGING

- All events documented
- Policy enforcement recorded
- Session details captured
- Compliance ready

Date/Time	Source	Device	Destination	Application Name	Result
2025/11/29 10:10:51	10.0.11.50	100.65.0.254	tcp/40278		Deny (Deny)
2025/11/29 10:10:51	10.0.11.50	100.65.0.254	tcp/62096		Deny (Deny)
2025/11/29 10:10:51	10.0.11.50	100.65.0.254	tcp/37204		Deny (Deny)

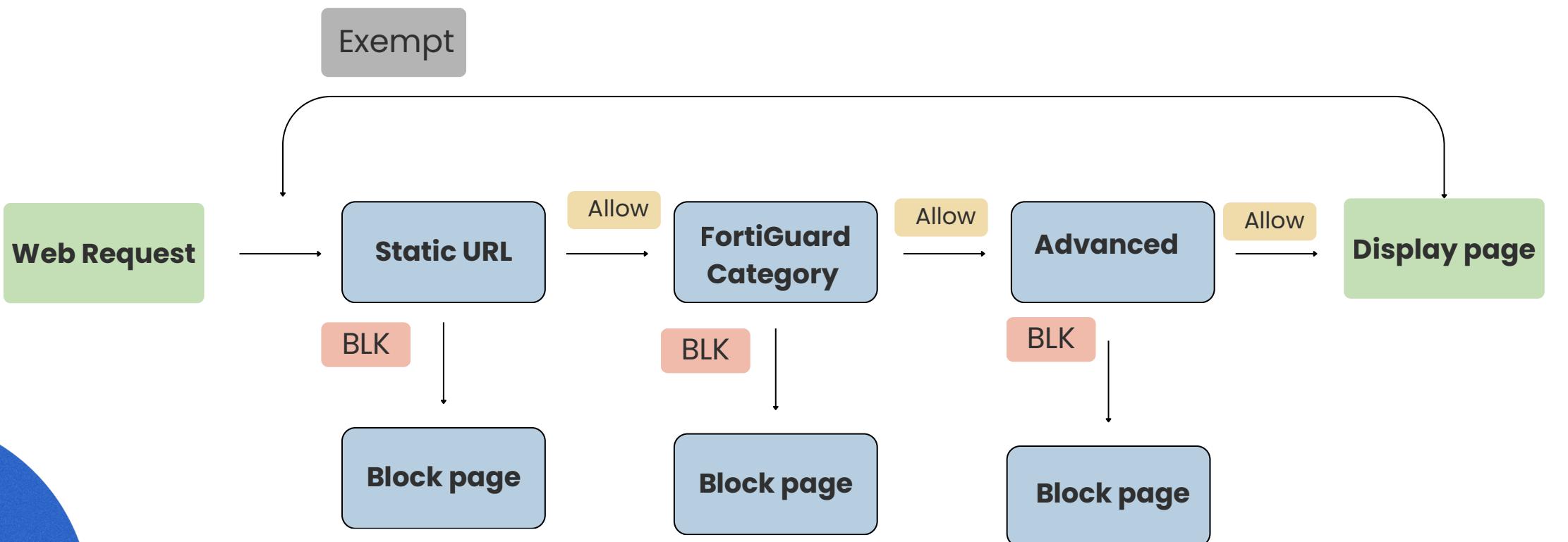
**Log Details**

AntiVirus

FortiSandbox Checksum: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f  
 Submitted to FortiSandbox: false  
 Direction: incoming  
 Destination UUID: 7bc87d34-7916-51e7-3d5b-71812aa1b98e  
 Detection Type: av-engine  
 Log event original timestamp: 1,764,439,845,427,552,300  
 Event Type: infected  
 File Name: eicar.com  
 Infection Type: Malicious  
 Level: Warning  
 Profile: default  
 Quarantine Skip: Quarantine-disabled  
 Reference: https://fortiguard.com/encyclopedia/virus/2172  
 Source UUID: 703e6ff6-791a-51e7-daa0-9859ce6c1d02  
 Sub Type: virus

# Week 1: Understanding Webfilter

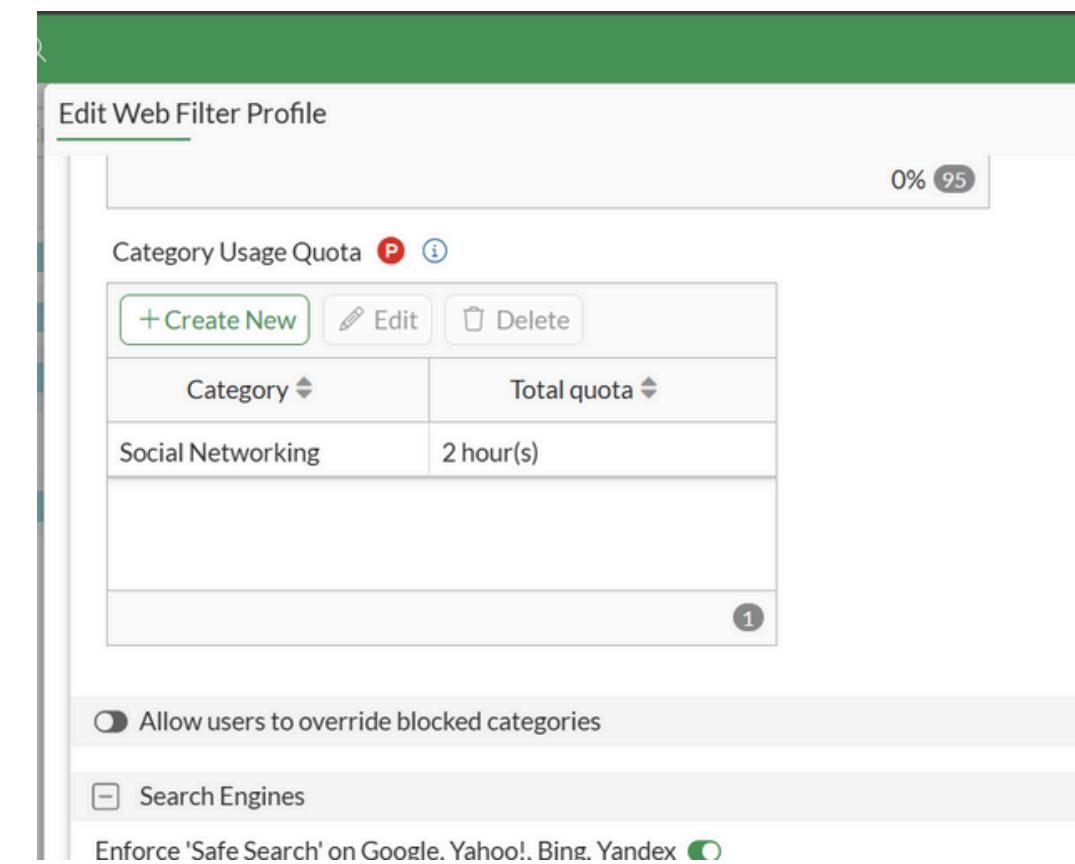
We implemented a multi-layered web filtering solution using FortiGuard categories, static URL rules, and quota management. The system provides granular control over internet access while maintaining user productivity through features like rating overrides and error handling



# Week 2: Configuration

Steps Taken:

- Feature verification
- profile creation
- categories/actions
- firewall policy



1

Edit Web Filter Profile

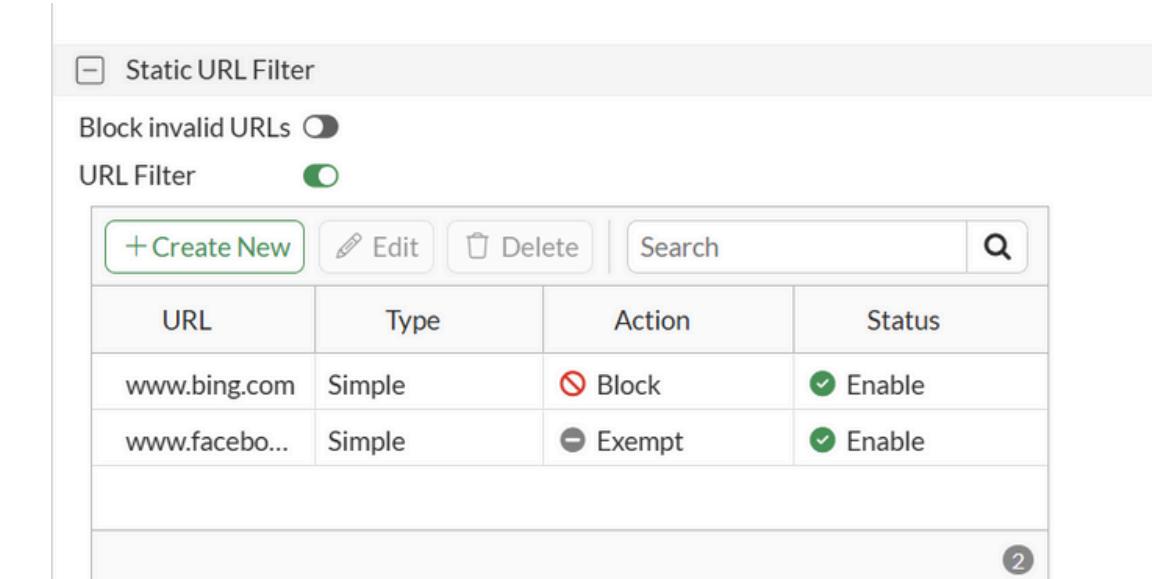
Category Usage Quota P i

+ Create New	Edit	Delete
Category	Total quota	
Social Networking	2 hour(s)	

Allow users to override blocked categories

Search Engines

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



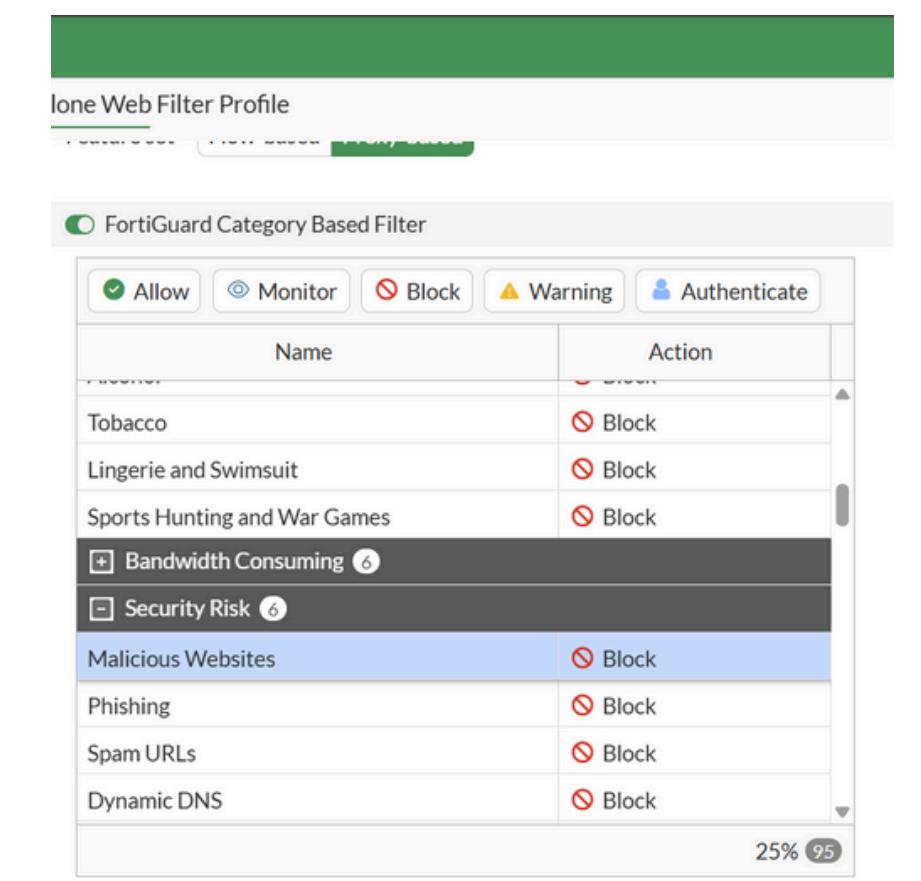
2

Static URL Filter

Block invalid URLs

URL Filter

+ Create New	Edit	Delete	Search
URL	Type	Action	Status
www.bing.com	Simple	Block	Enable
www.facebo...	Simple	Exempt	Enable



Lone Web Filter Profile

FortiGuard Category Based Filter

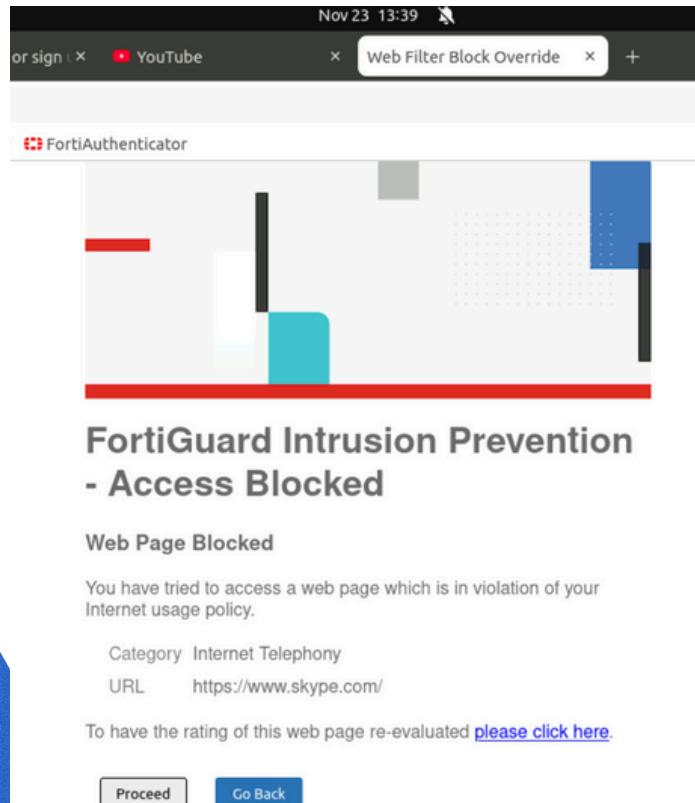
Allow	Monitor	Block	Warning	Authenticate
Name	Action			
Tobacco	Block			
Lingerie and Swimsuit	Block			
Sports Hunting and War Games	Block			
Bandwidth Consuming	Block			
Security Risk	Block			
Malicious Websites	Block			
Phishing	Block			
Spam URLs	Block			
Dynamic DNS	Block			



# Week 3: Monitoring

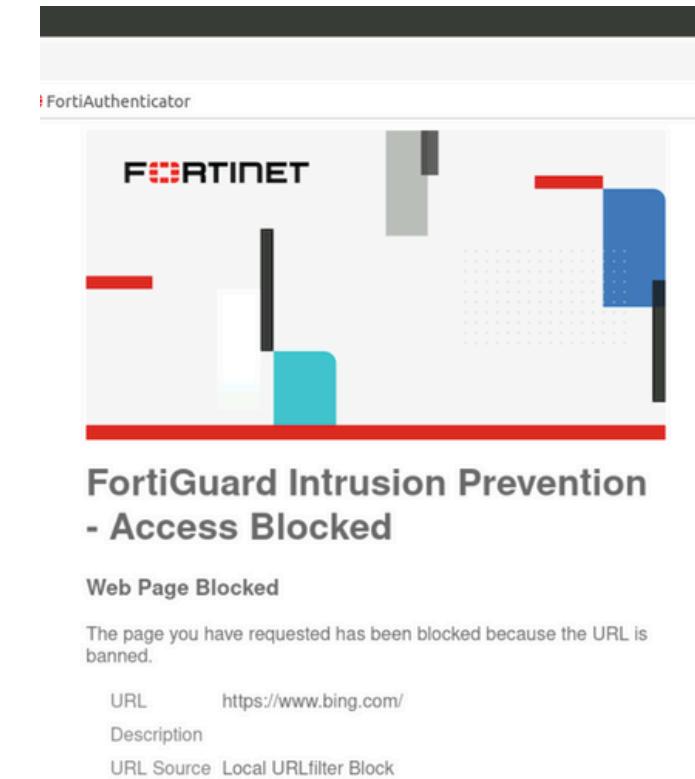
## CATEGORY ENFORCEMENT

- Social Networking: Blocked
- Internet Telephony: Warned
- Malicious Websites: Blocked
- Clear policy messaging



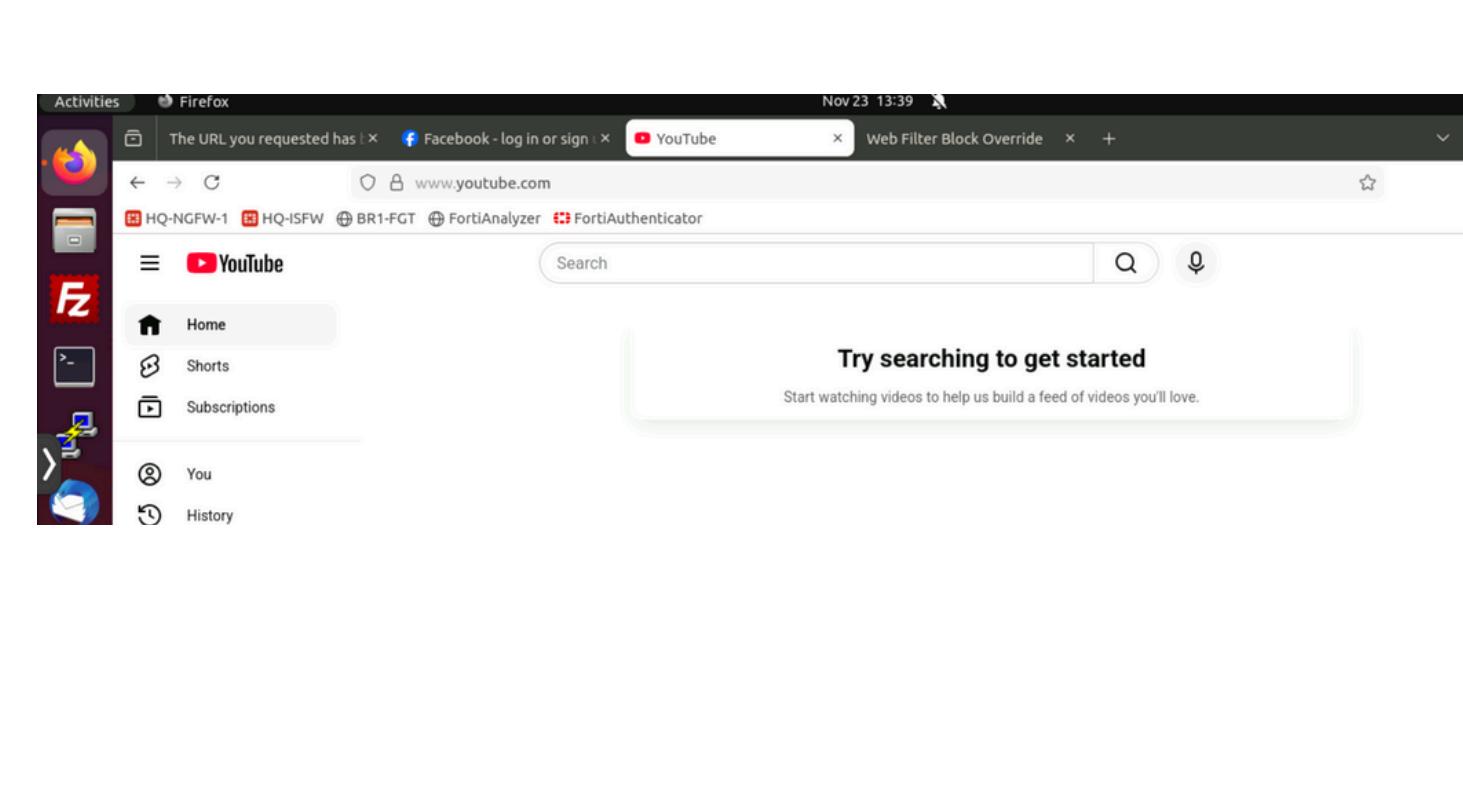
## Static URL Control

- Bing.com: Double-blocked
  - Malicious category
  - Static URL filter
- Facebook.com: Exempted



## Balanced Access

- YouTube: Accessible
- Search Engines: Allowed
  - Job Sites: Permitted
- Legitimate work enabled



# Week 1: Understanding Application Control

- Definition
- Purpose
- How it works
- Use Cases



The screenshot shows the FortiGate Management UI for Application Control profiles. The left sidebar menu is visible with various security profiles like AntiVirus, Web Filter, Video Filter, DNS Filter, Application Control, and more. The main panel displays a table of application control profiles:

Name	Comments	Ref.
appctrl_group4		0
block-high-risk		0
default	Monitor all applications.	0
wifi-default	Default configuration for offloading Wi...	1

The screenshot shows the FortiGate Management UI for Application Sensor categories. The left sidebar menu is visible. The main panel displays a hierarchical list of application categories:

- Mixed (All Categories)
  - Business (154, △ 6)
  - Cloud/IT (72, △ 12)
  - Collaboration (266, △ 13)
  - Email (76, △ 11)
  - Game (83)
  - General Interest (253, △ 15)
  - Mobile (3)
  - Network Service (338)
  - P2P (55)
  - Remote Access (96)
  - Storage/Backup (150, △ 20)
  - Video/Audio (147, △ 17)
  - Web Client (24)
- Operational Technology
- Proxy (189)
- Social Media (113, △ 29)
- Update (48)
- VoIP (23)
- Unknown Applications

# Week 2 : Configuration

Steps Taken:

✓ Feature verification

✓ profile creation

✓ categories/actions

✓ firewall policy

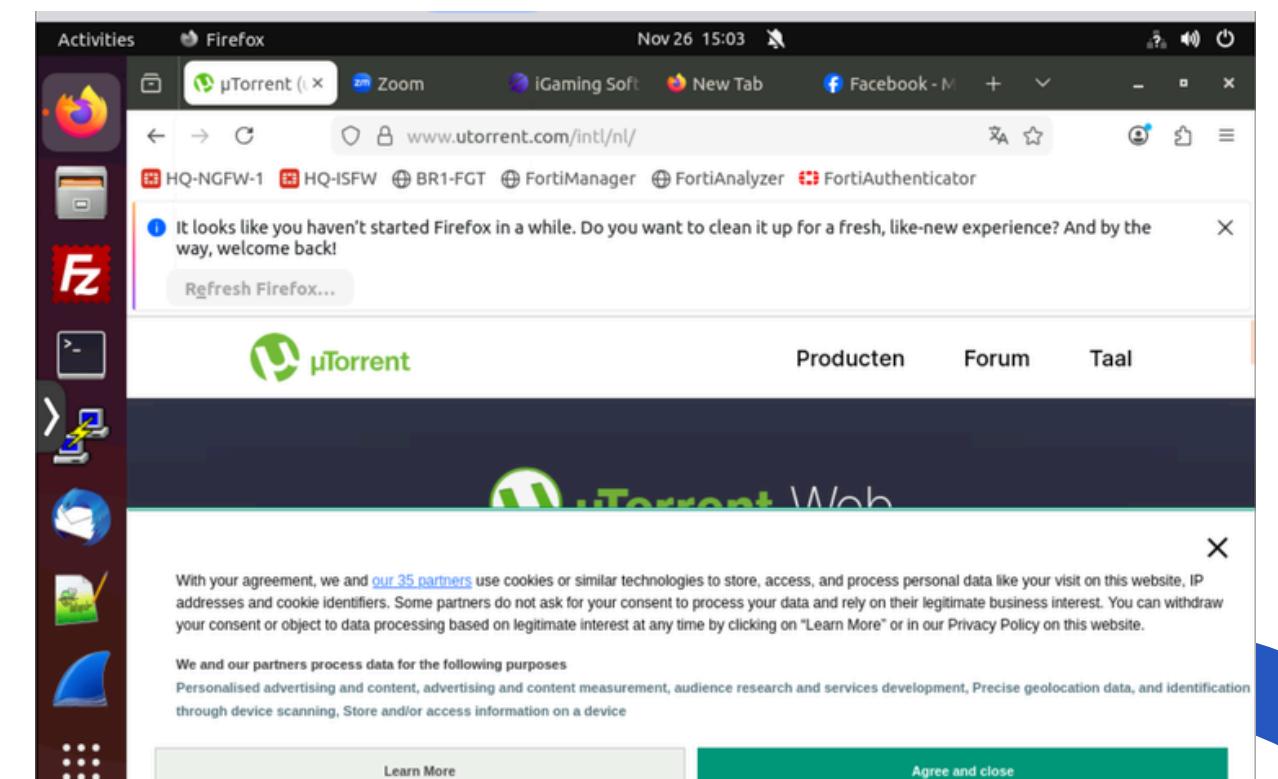
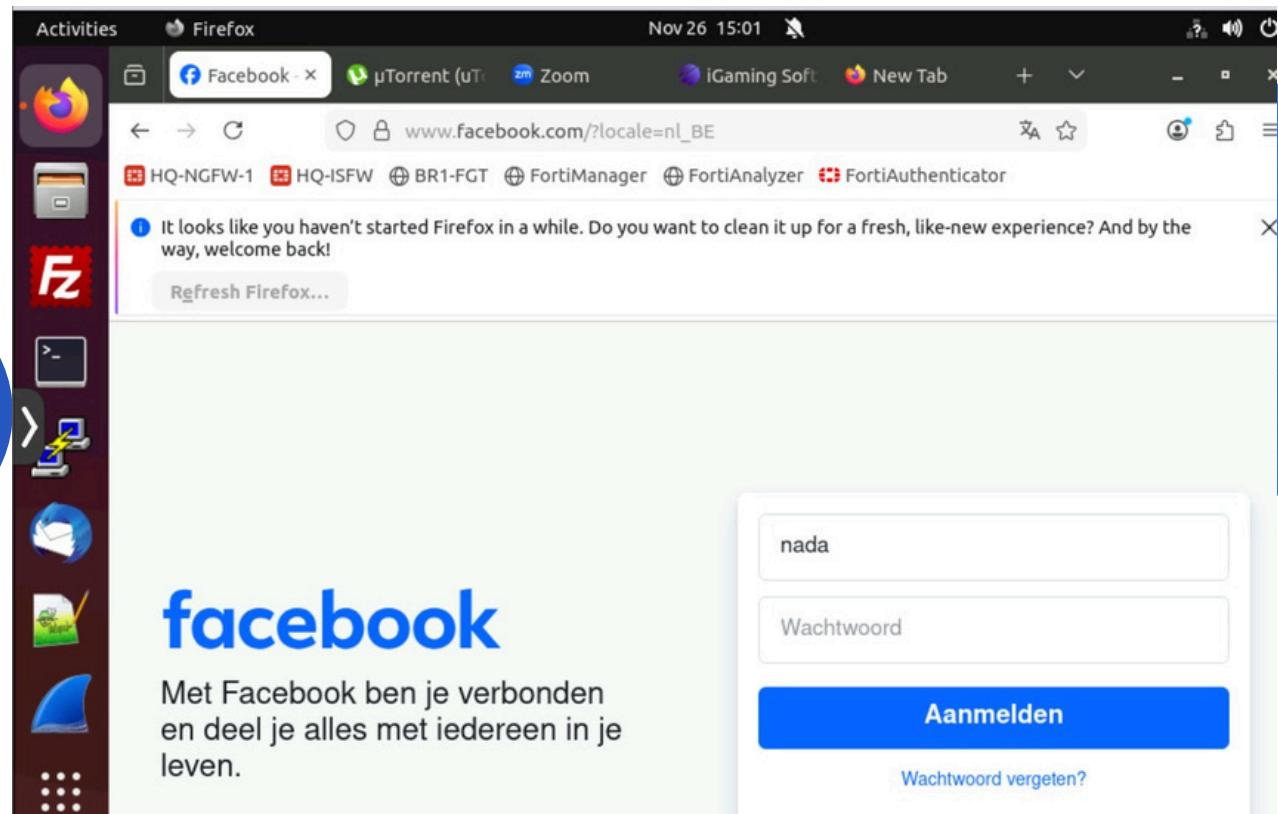
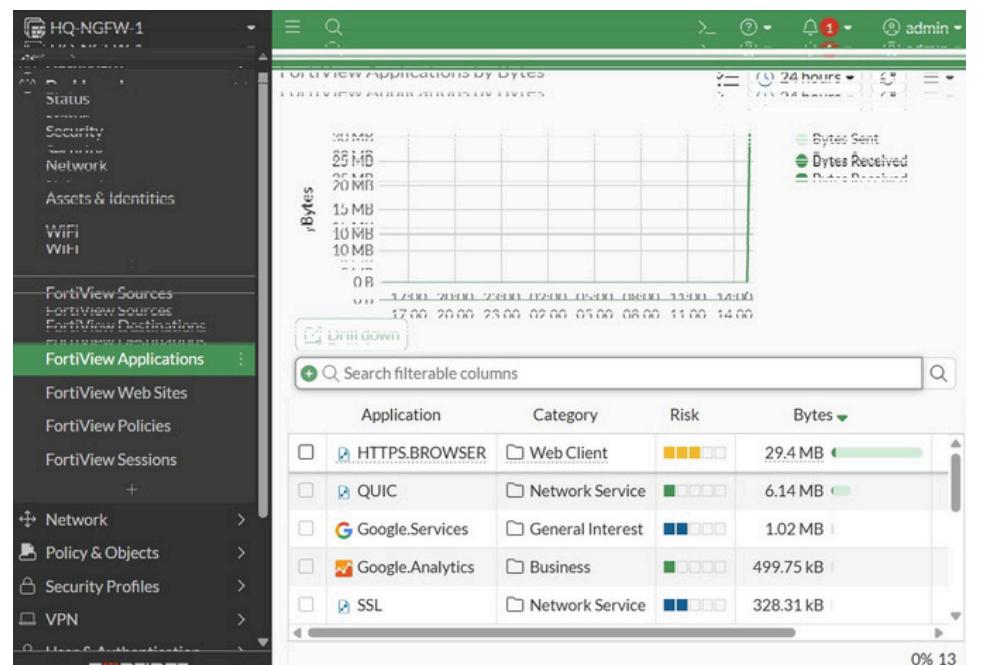
The screenshot shows the FortiGate Management UI for editing a Firewall Policy. The left sidebar menu is visible. The main panel shows the configuration settings for the policy:

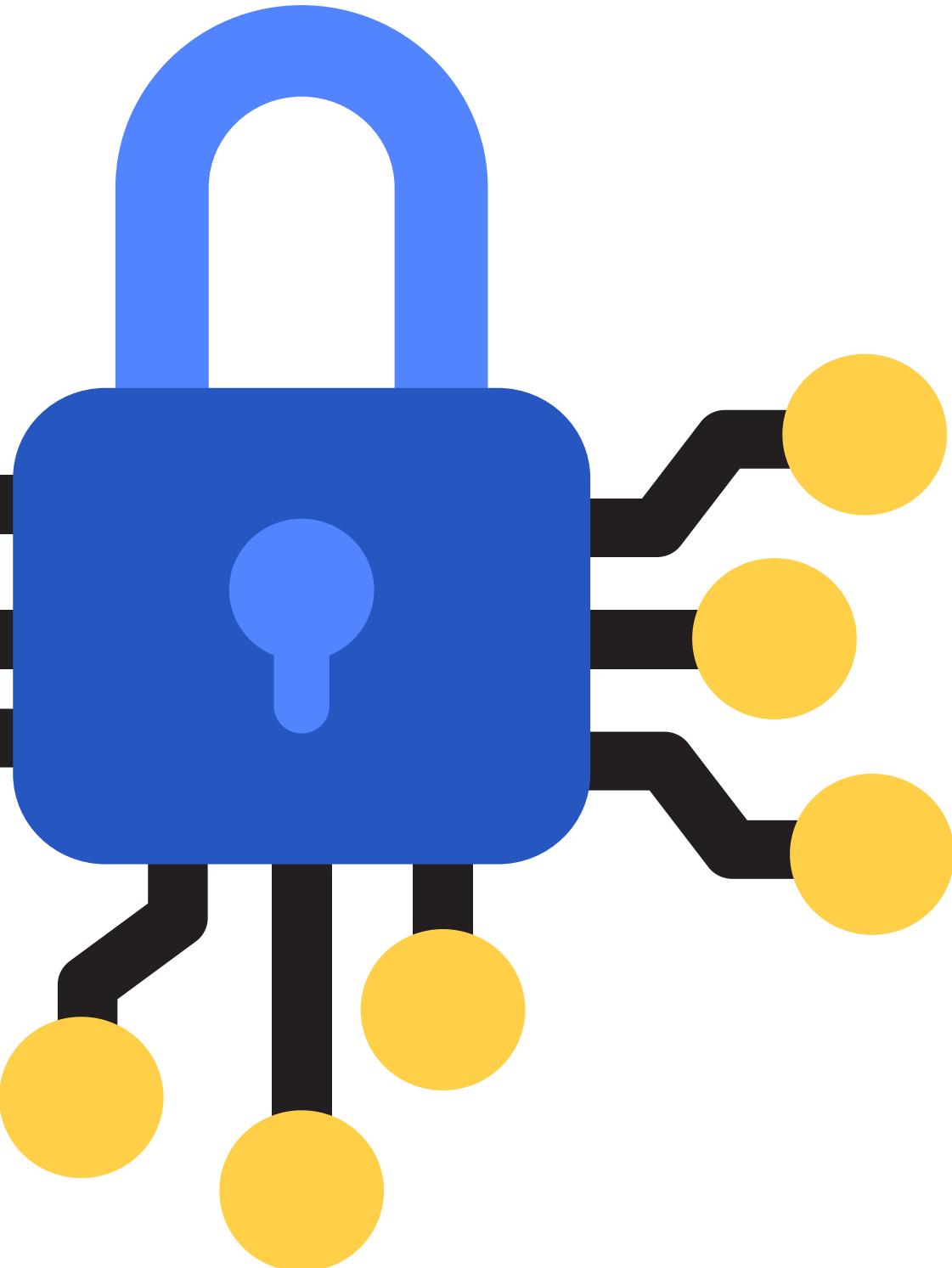
- Security Profiles: Web filter (selected)
- DNS filter: Off
- Application control: Off
- IPS: Off
- File filter: Off
- SSL inspection: no-inspection
- Logging Options:
  - Log allowed traffic: On
  - Generate logs when session starts: On
  - Capture packets: On
- Comments: (empty)
- Enable this policy: On

Buttons at the bottom: OK and Cancel.

# Week 3 : Testing & Monitoring

- Test Traffic
- Results
- Analysis





# Application Control Summary & Transition

## Key Takeaways from Application Control

- Application Control was successfully configured and applied on FortiGate.
- Traffic logging and monitoring were enabled using FortiView.
- Policy enforcement depends heavily on Firewall Policy Priority.
- Full visibility of application traffic was achieved.

# Week 1: Understanding IPS

- Definition
- Purpose
- How it works
- Use Cases



The screenshot shows two main windows from the FortiManager interface:

- Create New Policy:** This window allows configuring various security options. Under "SSL Inspection Options", the "Log allowed traffic" dropdown is expanded, showing "ssl certificate-inspection" selected.
- New IPS Sensor:** This window configures an IPS sensor named "WEB SERVER". Under "IPS Signatures and Filters", a table lists signatures for different protocols (TGT, SEV, APP) and severities (Low, Medium, High).

# Week 2 : Configuration

## Steps Taken:

- ✓ Feature verification
- ✓ profile creation
- ✓ categories/actions
- ✓ firewall policy

This screenshot shows the "IPS Sensors" configuration page. A profile named "WEB SERVER" is selected, highlighted in blue. The right pane displays detailed information about this profile, including its description and protection settings.

# Week 3 : Testing & Monitoring

- Simulated Attack
- Results
- Analysis

**Log Details**

**Action**

Action	dropped
Threat	8,192
Policy ID	Web_Server_Access_IPS (5)
Policy UUID	5f7d68ba-ccc3-51f0-5c57-c45d7234
Policy Type	Firewall

**Security**

Level	High
Threat Level	High
Threat Score	30

**Intrusion Prevention**

Profile	WEB SERVER
Attack Name	HTTP.URI.SQL.Injection
Attack ID	15,621
Reference	<a href="https://fortiguard.fortinet.com/encyclopedia/ips/15621">https://fortiguard.fortinet.com/encyclopedia/ips/15621</a>
Incident Serial	171,966,470
Direction	outgoing
Severity	High
Message	HTTP.URI.SQL.Injection

**Log Details**

**Action**

Action	detected
Threat	16,384
Policy ID	Web_Server_Access_IPS (5)
Policy UUID	5f7d68ba-ccc3-51f0-5c57-c45d7234
Policy Type	Firewall

**Security**

Level	Medium
Threat Level	Medium
Threat Score	10

**Intrusion Prevention**

Profile	WEBSERVER
Attack Name	Apache.Expect.Header.XSS
Attack ID	15,229
Reference	<a href="https://fortiguard.fortinet.com/encyclopedia/ips/15229">https://fortiguard.fortinet.com/encyclopedia/ips/15229</a>
Incident Serial	171,966,465
Direction	outgoing
Severity	Medium
Message	Apache.Expect.Header.XSS

```
100.65.0.254 - PuTTY
applicable law.

You have new mail.
Last login: Mon Nov 18 09:00:33 2024 from 100.65.0.101
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

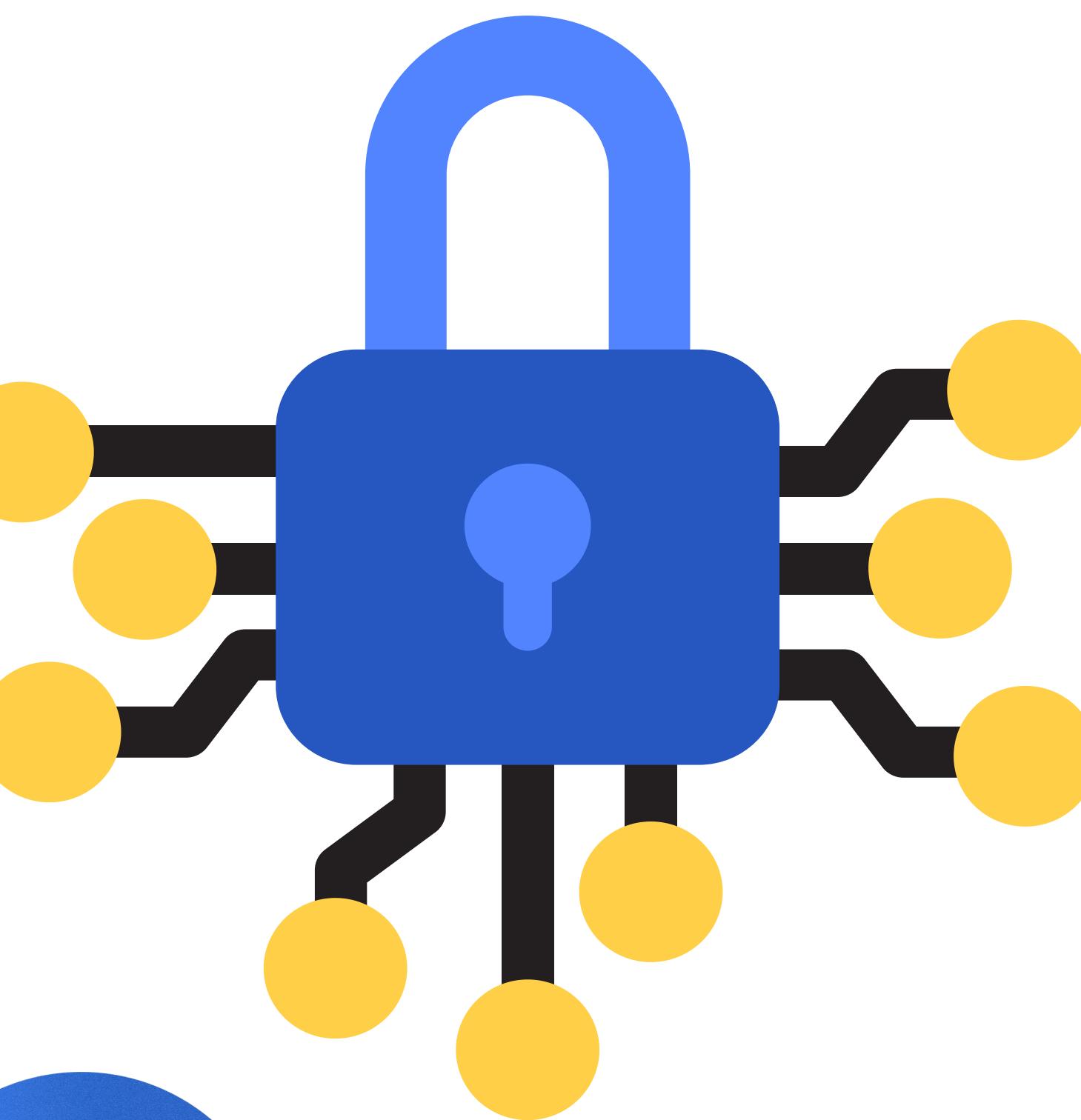
admin@ubuntu-2204-desktop:~$ ni
nice      nikto.pl      nisdomainname
admin@ubuntu-2204-desktop:~$ nikto.pl -host 100.65.0.200
- Nikto v2.1.5
-----
+ Target IP:          100.65.0.200
+ Target Hostname:    100.65.0.200
+ Target Port:        80
+ Start Time:         2025-11-28 17:37:29 (GMT-8)
-----
+ Server: Apache/2.4.52 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2aa6 0x59c3
1496ec4d4
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

**Logs**

**Summary**   **Logs**

Date/Time 2025-11-28 17:33:17 -> 2025-11-28 17:38:...   Search   Intrusion Prevention   Disk   custom   Details

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
2025/11/28 17:38:12	High	100.65.0.254	6		dropped		HTTP.URI.SQL.Injection
2025/11/28 17:38:02	High	100.65.0.254	6		dropped		HTTP.URI.SQL.Injection
2025/11/28 17:37:52	High	100.65.0.254	6		dropped		HTTP.URI.SQL.Injection
2025/11/28 17:37:42	High	100.65.0.254	6		dropped		HTTP.URI.SQL.Injection
2025/11/28 17:37:32	High	100.65.0.254	6		dropped		HTTP.URI.SQL.Injection
2025/11/28 17:37:30	Medium	100.65.0.254	6		detected		Apache.Expect.Header.XSS



# IPS Summary & Transition

## Key Takeaways from IPS

- IPS was successfully configured and applied on FortiGate.
- Threat detection and prevention were verified through FortiView.
- IPS actions (Block, Reset, Monitor) were tested.
- Clear visibility of attacks and signatures was achieved.

# Conclusion

Throughout our project, we've demonstrated that FortiGate Security Profiles are much more than just individual features - they form a cohesive security framework that provides comprehensive protection.

Security Profiles are not just features – they're the foundation of modern network security, providing the intelligent, adaptive protection essential in today's threat landscape.

