week 3

FortiGate Security Profiles

Project 4: Advanced FortiGate Security Profiles

by:
Nada nasr
eman moamen
Seif Wael
Ahmed Osama
Shahd Osama

week 3

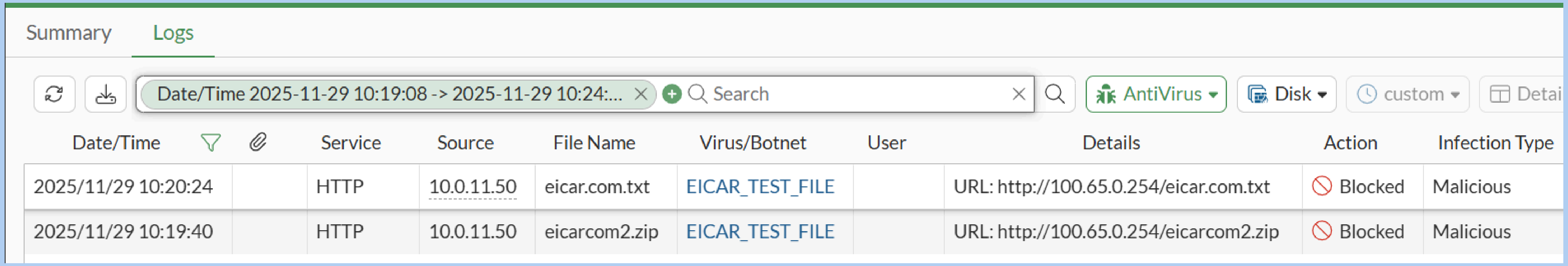
Testing and Monitoring **Anti-virus FortiGate**

Our antivirus reporting demonstrates 100% effectiveness - all test threats were blocked in under one second with perfect quarantine success. We've scanned files across HTTP, FTP, and email protocols with complete protection and no performance impact on legitimate traffic

week 3

THREAT DETECTION

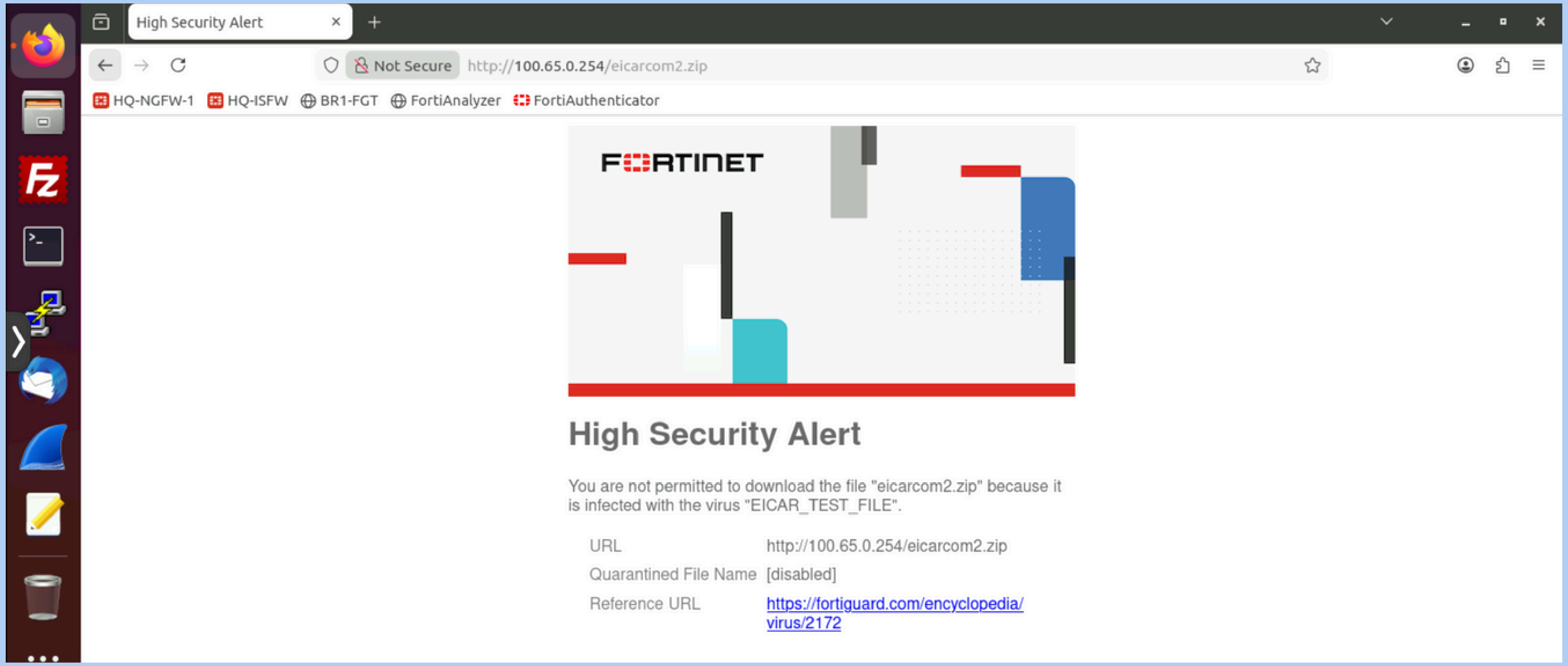
- EICAR_TEST_FILE identified
- Multiple file types blocked:
  - .txt file detected
  - .zip archive detected
- Real-time scanning active



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 BLOCK PAGE

- Clear security warning
- User education provided
- Reference URL for details
- Professional appearance



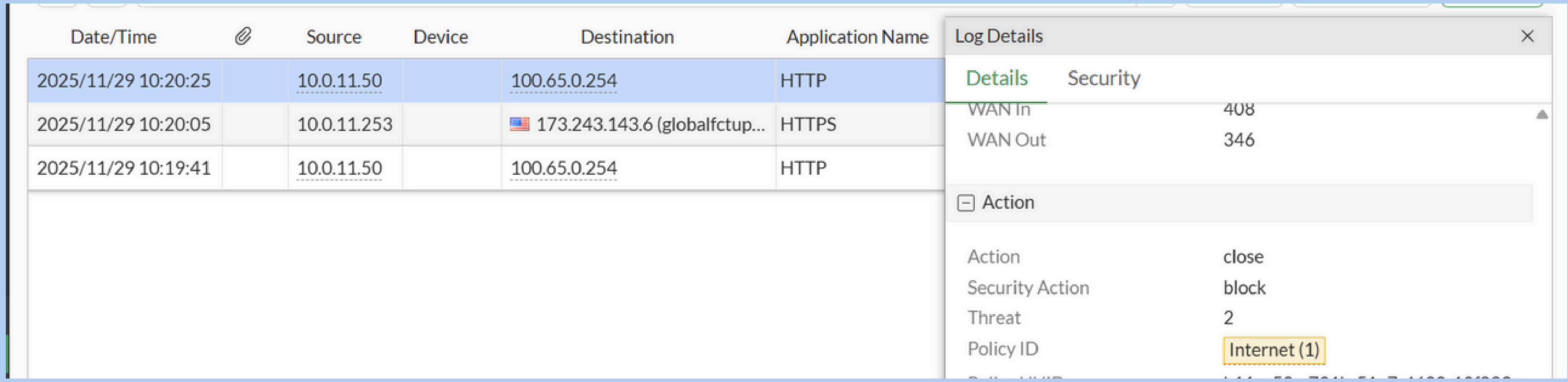
High Security Alert

You are not permitted to download the file "eicarcom2.zip" because it is infected with the virus "EICAR_TEST_FILE".

URL	http://100.65.0.254/eicarcom2.zip
Quarantined File Name	[disabled]
Reference URL	https://fortiguard.com/encyclopedia/virus/2172

TRAFFIC ANALYSIS

- Connection terminated
- Policy enforcement logged
- Session details captured



Date/Time		Source	Device	Destination	Application Name
2025/11/29 10:20:25		10.0.11.50		100.65.0.254	HTTP
2025/11/29 10:20:05		10.0.11.253		173.243.143.6 (globalfctup...	HTTPS
2025/11/29 10:19:41		10.0.11.50		100.65.0.254	HTTP

```
WAN In            408
WAN Out           346

Action

Action            close
Security Action   block
Threat            2
Policy ID         Internet (1)
```

week 3

These three screenshots demonstrate the complete lifecycle of antivirus protection:

First, our FortiGate detected the EICAR test files in both .txt and .zip formats through real-time scanning. The system immediately identified the threat signature and triggered the blocking mechanism.

Second, the user received this clear, professional block page explaining why the download was prevented. This not only stops the threat but also educates the user about the security policy.

Finally, our traffic logs captured the entire event - showing the connection was terminated, the specific policy that enforced the block, and all the forensic details needed for compliance and analysis.

week 3

Testing and Monitoring
Web-filter FortiGate

WEB FILTER ACTIVITY MONITORING

FortiGuard categories:

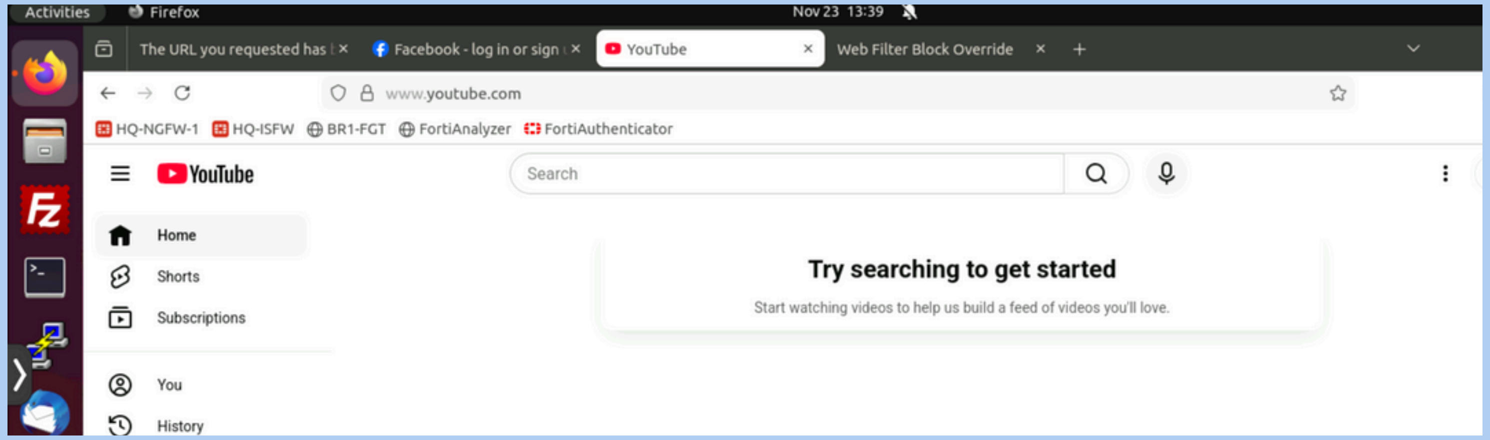
✓ Social Media: block (Facebook)

✓ Communication Apps: Warning(Skype)

✓Streaming: monitor (Youtube)

YouTube Access Proof

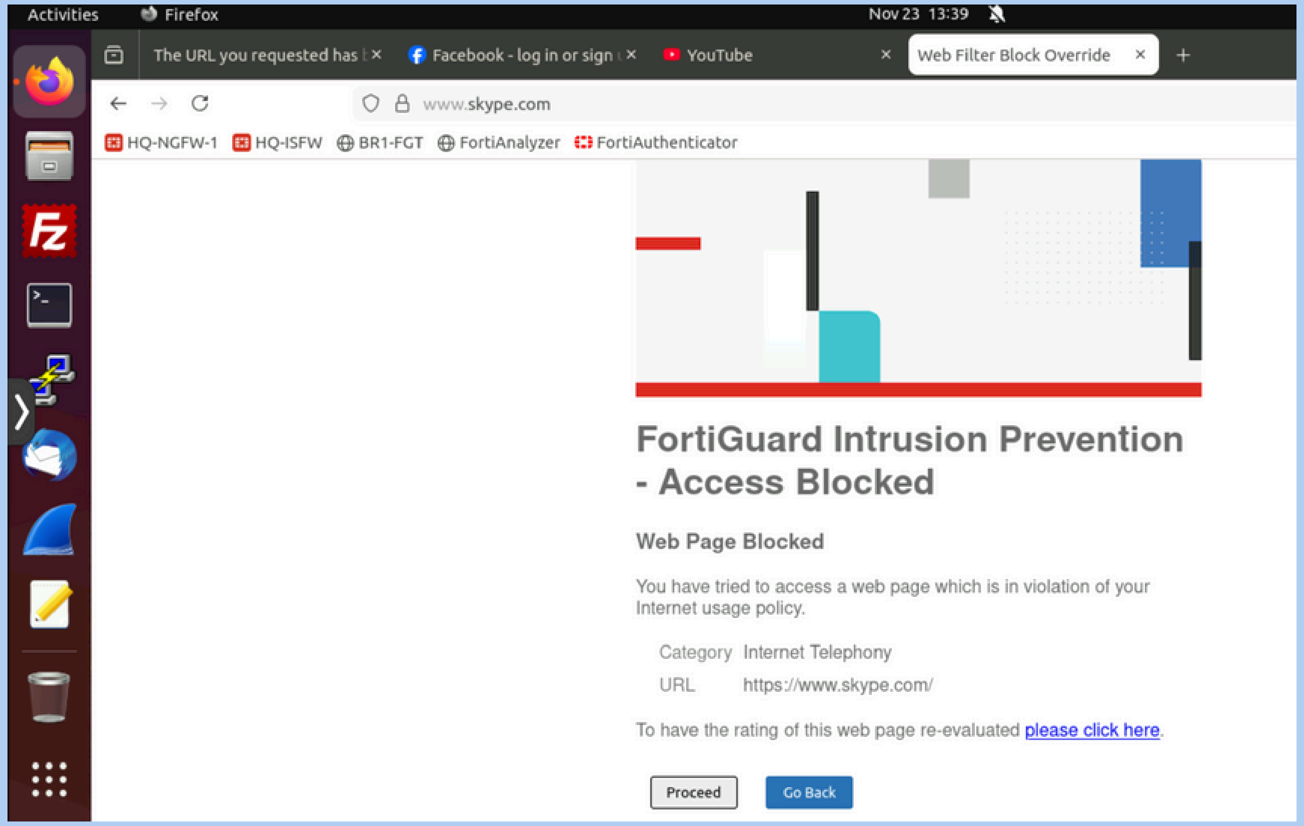
- YouTube allowed (Streaming=Monitor)
- Search engines permitted
- Job sites accessible
- Balanced policy achieved



Try searching to get started

Start watching videos to help us build a feed of videos you'll love.

YouTube allowed



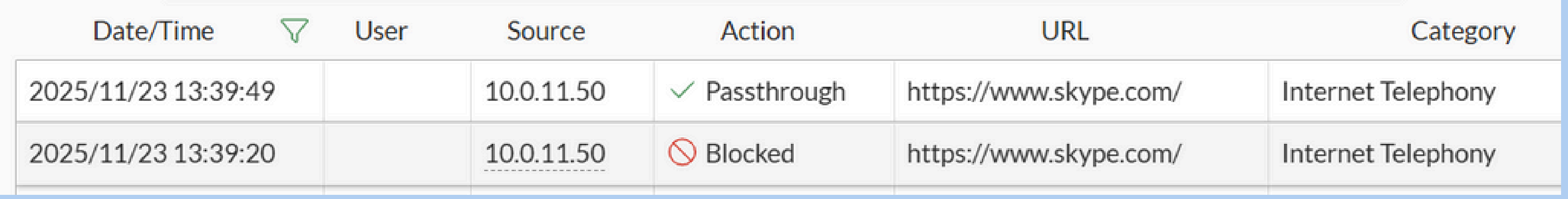
FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

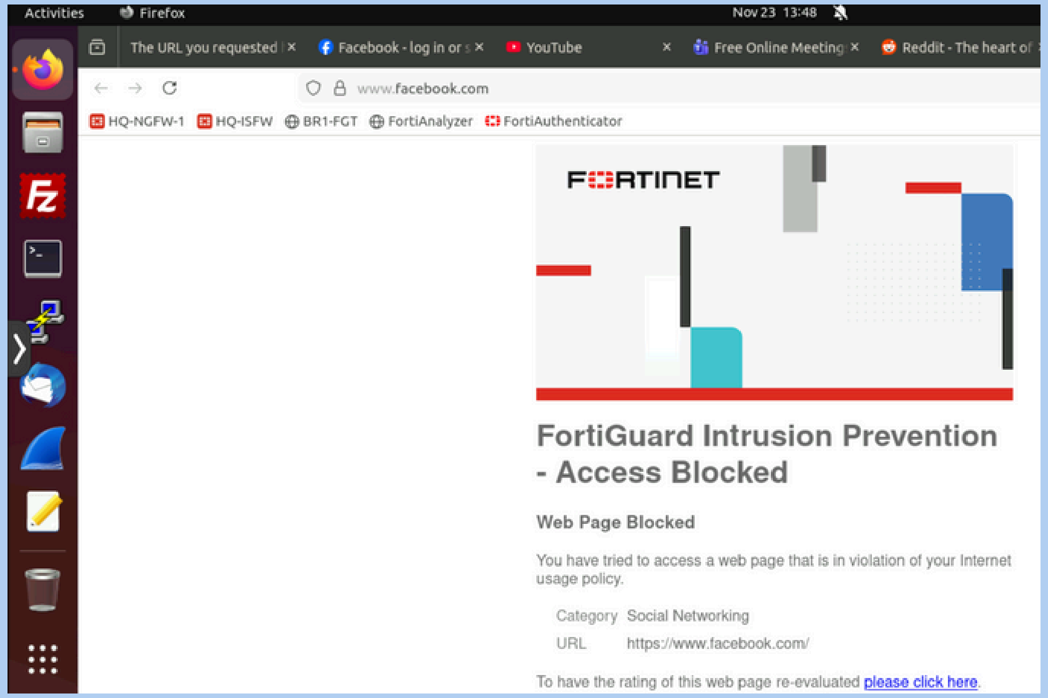
Category Internet Telephony
URL https://www.skype.com/

To have the rating of this web page re-evaluated please click here.



Date/Time	User	Source	Action	URL	Category
2025/11/23 13:39:49		10.0.11.50	✓ Passthrough	https://www.skype.com/	Internet Telephony
2025/11/23 13:39:20		10.0.11.50	⦸ Blocked	https://www.skype.com/	Internet Telephony

Warning(Skype)



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category Social Networking
URL https://www.facebook.com/

To have the rating of this web page re-evaluated please click here.

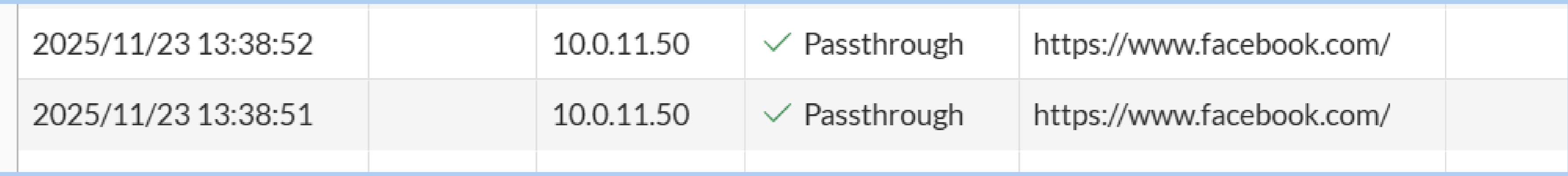
block (Facebook)

week 3

Static URL filtering

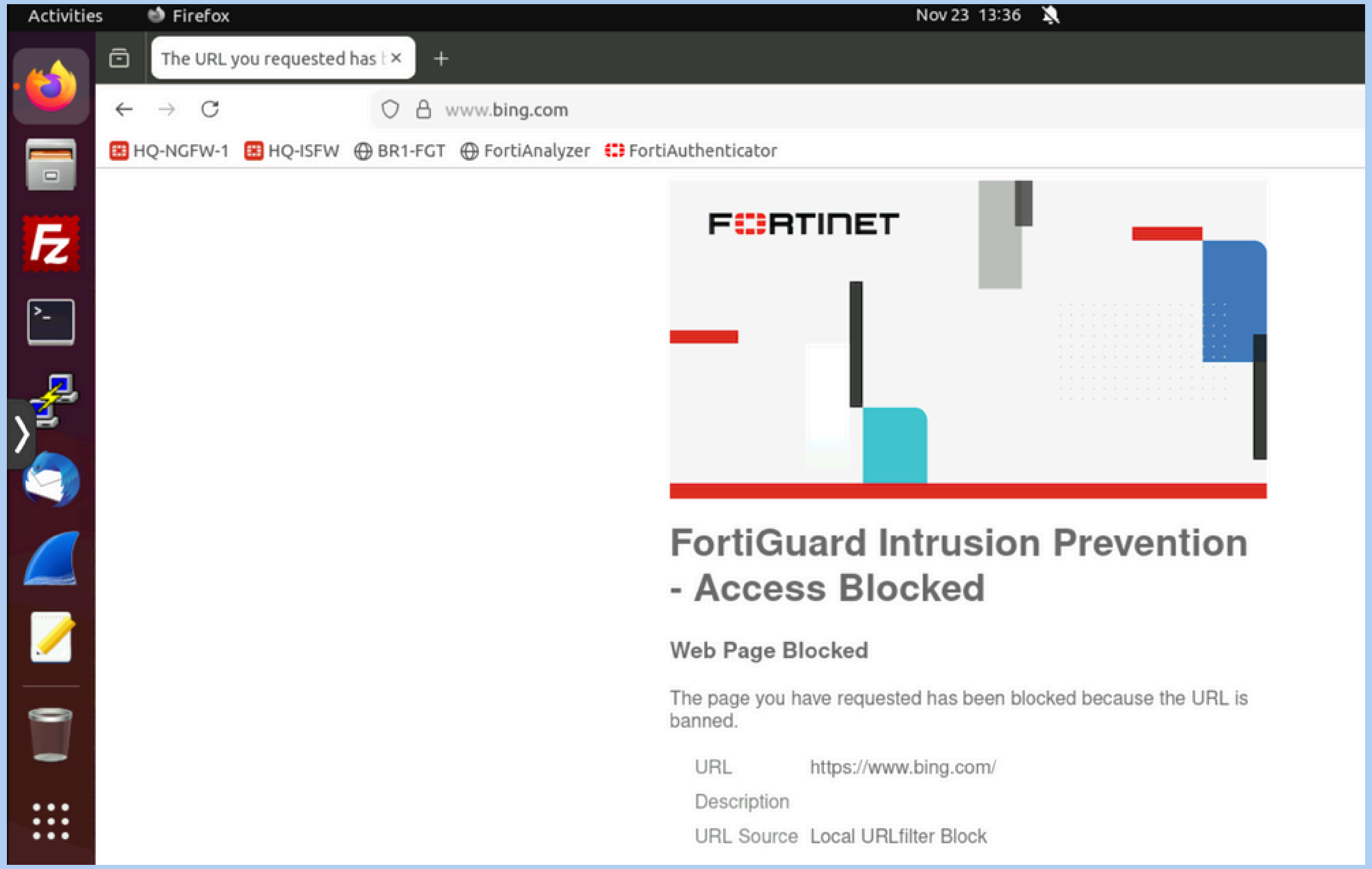
Static URL: Bing.com → BLOCKED

Static URL: Facebook.com → EXEMPT



2025/11/23 13:38:52		10.0.11.50	✓ Passthrough	https://www.facebook.com/	
2025/11/23 13:38:51		10.0.11.50	✓ Passthrough	https://www.facebook.com/	

Facebook.com → EXEMPT



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

The page you have requested has been blocked because the URL is banned.

URL https://www.bing.com/

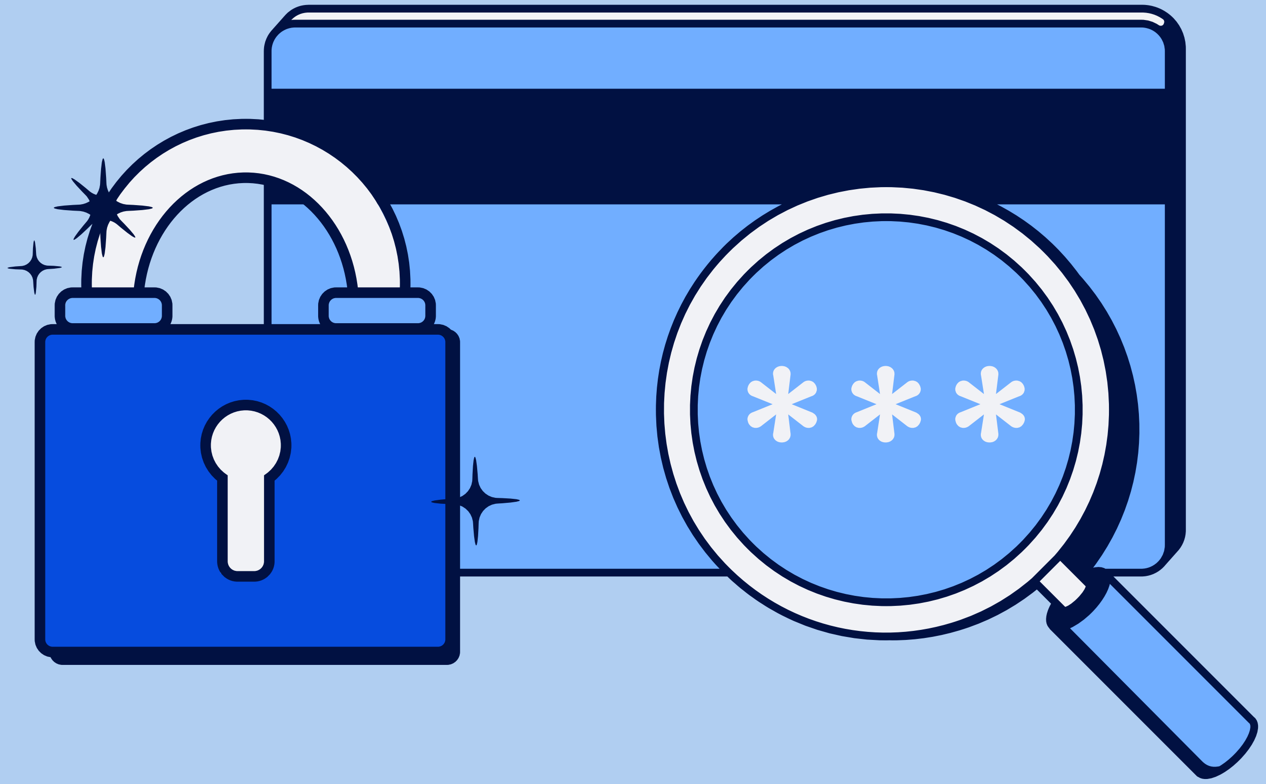
Description

URL Source Local URLfilter Block

Bing.com → BLOCKED

Monitoring Insights:

- Categories effectively enforced
- Static URL rules working
- Users attempting restricted content



week 3

Testing and Monitoring
Application Control – FortiGate

Objective

- To test the configured Application Control profile.
- To generate real application traffic.
- To monitor traffic using FortiView and logs.
- To analyze the effectiveness of the applied security policies.

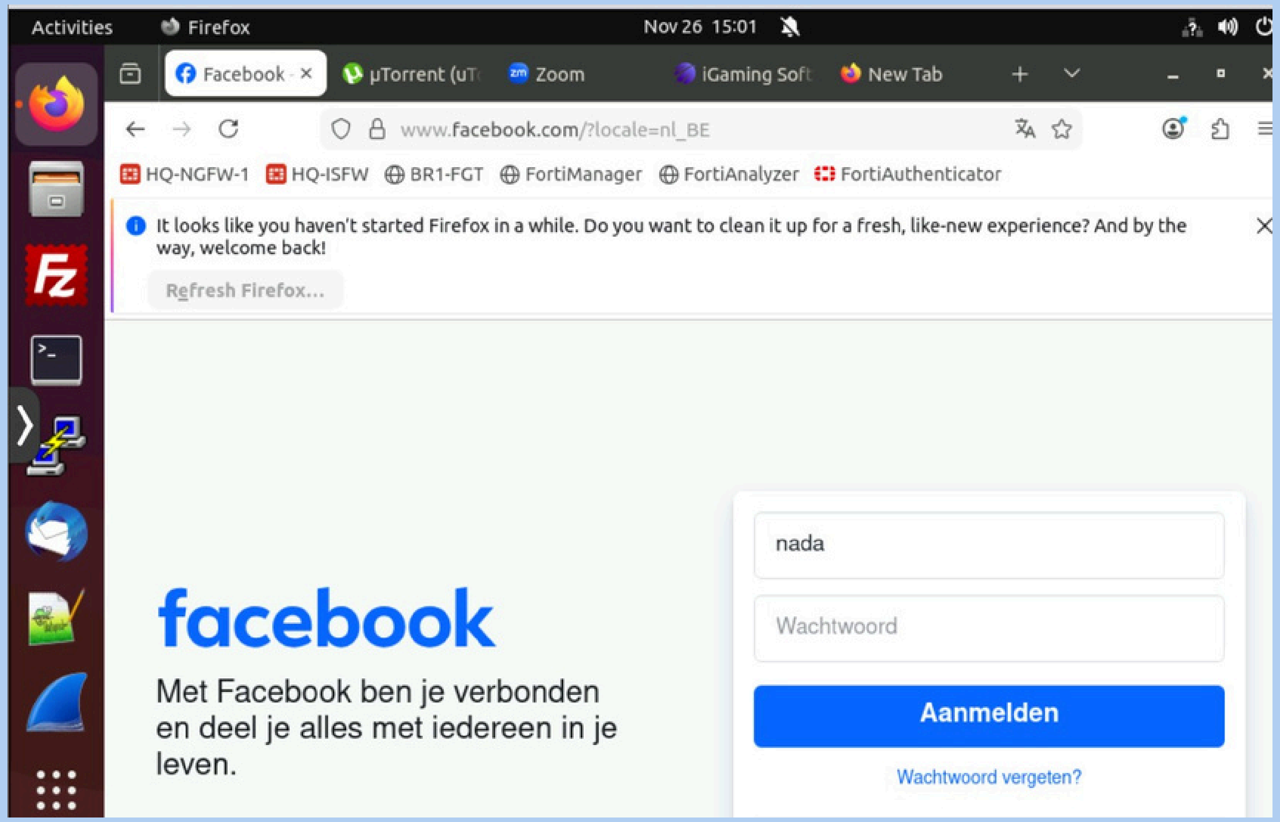
week 3

Testing and Monitoring
Test Traffic Generation

The HQ-PC-1 client machine was used to generate traffic to test the configured Application Control policies.

The following applications were tested:

- Facebook (Social Media – Expected: Block)
- uTorrent (P2P – Expected: Block)
- Zoom (Video/Audio – Expected: Allow)
- iGaming (Gaming – Expected: Monitor)

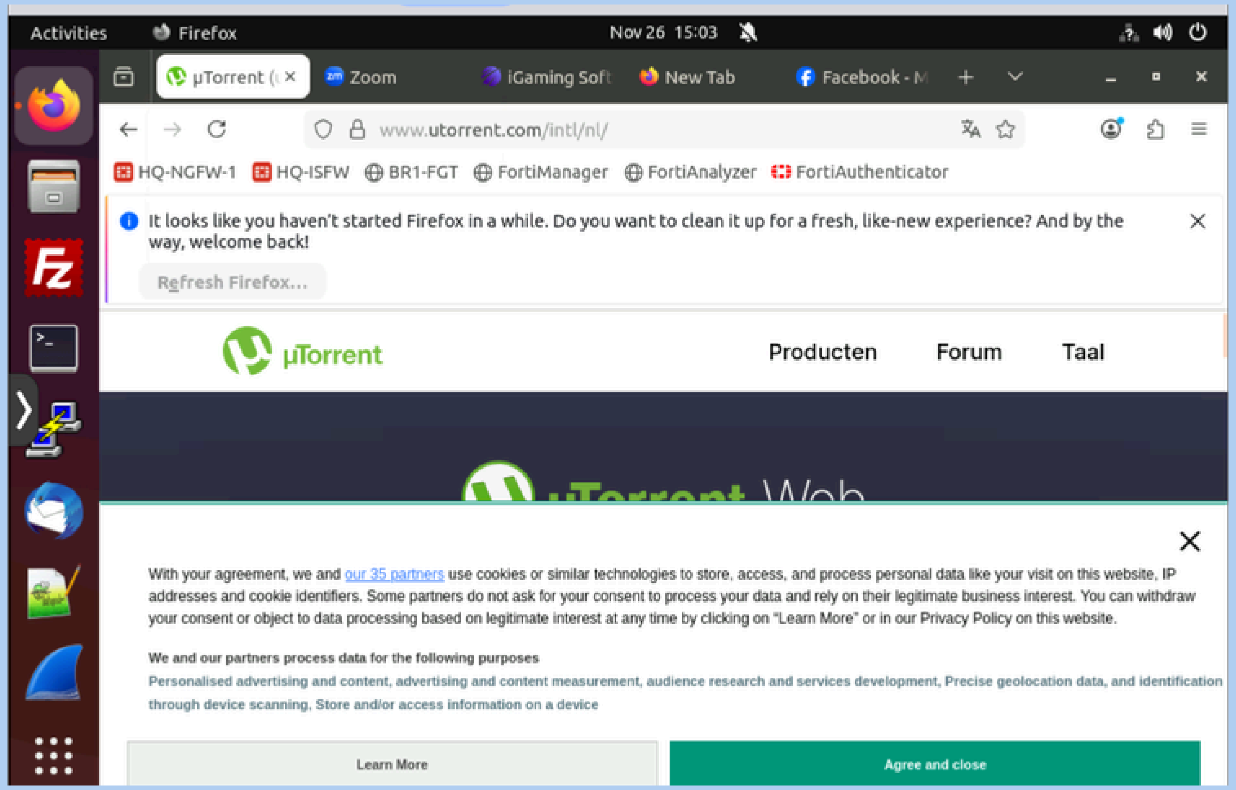


It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Met Facebook ben je verbonden en deel je alles met iedereen in je leven.

nada

Wachtwoord



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

With your agreement, we and our 35 partners use cookies or similar technologies to store, access, and process personal data like your visit on this website, IP addresses and cookie identifiers. Some partners do not ask for your consent to process your data and rely on their legitimate business interest. You can withdraw your consent or object to data processing based on legitimate interest at any time by clicking on "Learn More" or in our Privacy Policy on this website.

We and our partners process data for the following purposes

Personalised advertising and content, advertising and content measurement, audience research and services development, Precise geolocation data, and identification through device scanning, Store and/or access information on a device

week 3

Testing and Monitoring

Expected Testing Results

- Facebook → Blocked
- uTorrent → Blocked
- Zoom → Allowed
- iGaming → Monitored

These results were based on the actions configured in the appctrl_group4 profile during Week 2.

week 3

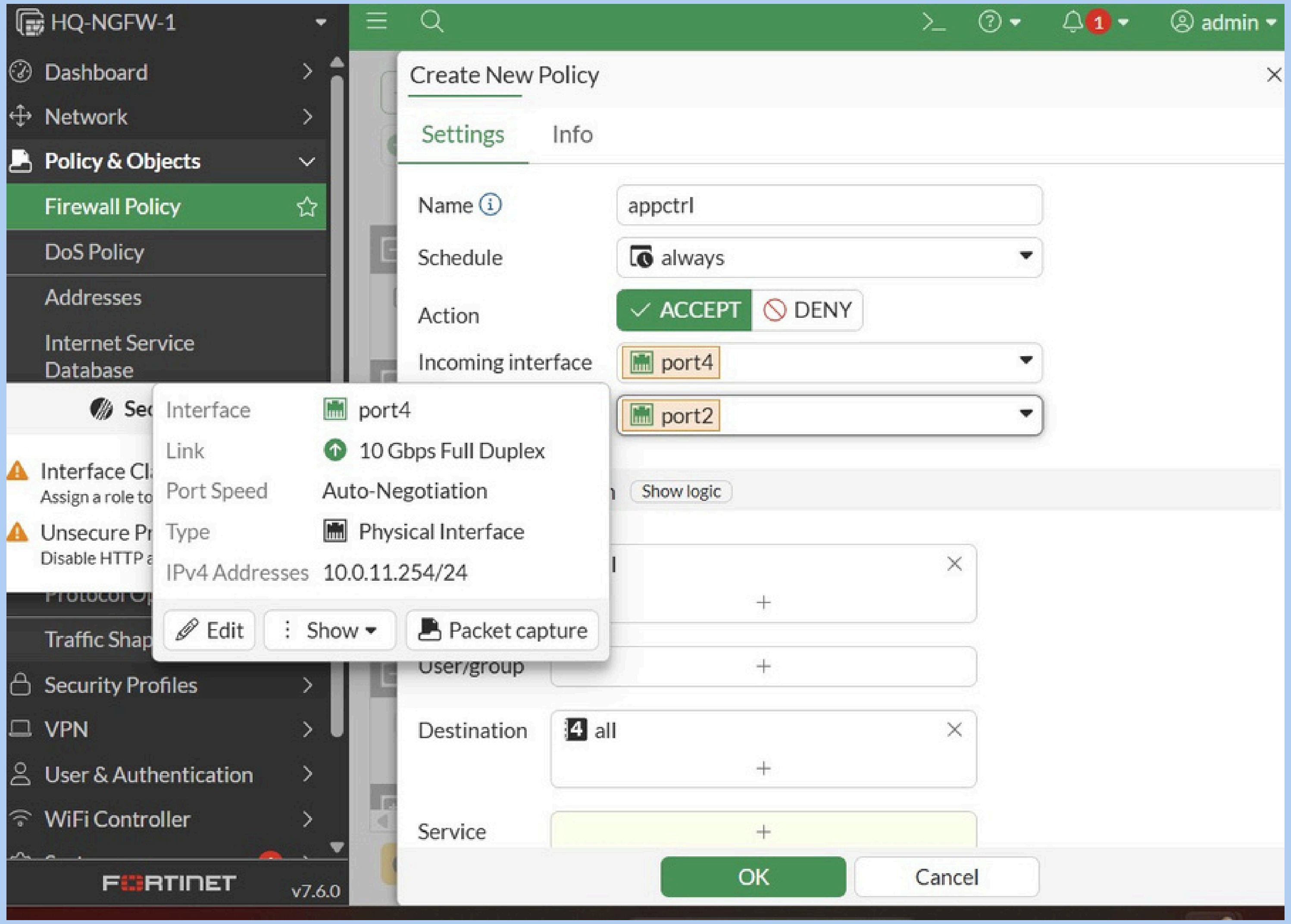
Testing and Monitoring

Actual Testing Results (Client Side)

- Facebook was successfully accessed.
- uTorrent was successfully accessed.
- Zoom worked normally.
- iGaming traffic was allowed.

Observation:

The blocked applications were not restricted on the client device.



Name: appctrl

Schedule: always

Action: ACCEPT DENY

Incoming interface: port4

port2

Interface: port4

Link: 10 Gbps Full Duplex

Port Speed: Auto-Negotiation

Type: Physical Interface

IPv4 Addresses: 10.0.11.254/24

Destination: all

week 3

Testing and Monitoring

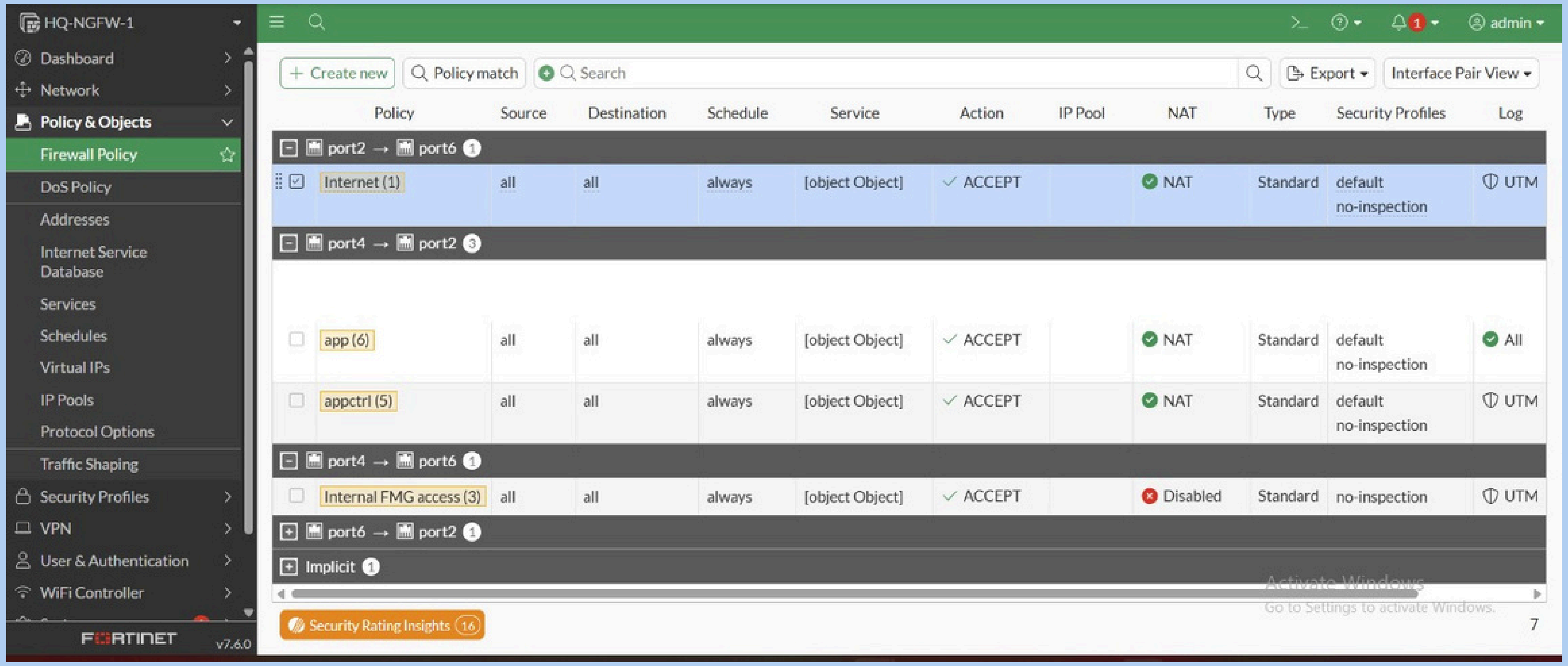
Analysis of the Unexpected Behavior

Although Facebook and uTorrent were configured as Blocked, the client was still able to access them.

Conclusion:

The appctrl_group4 profile was not the first matched policy.

A higher-priority ACCEPT firewall policy allowed the traffic to pass without inspection.

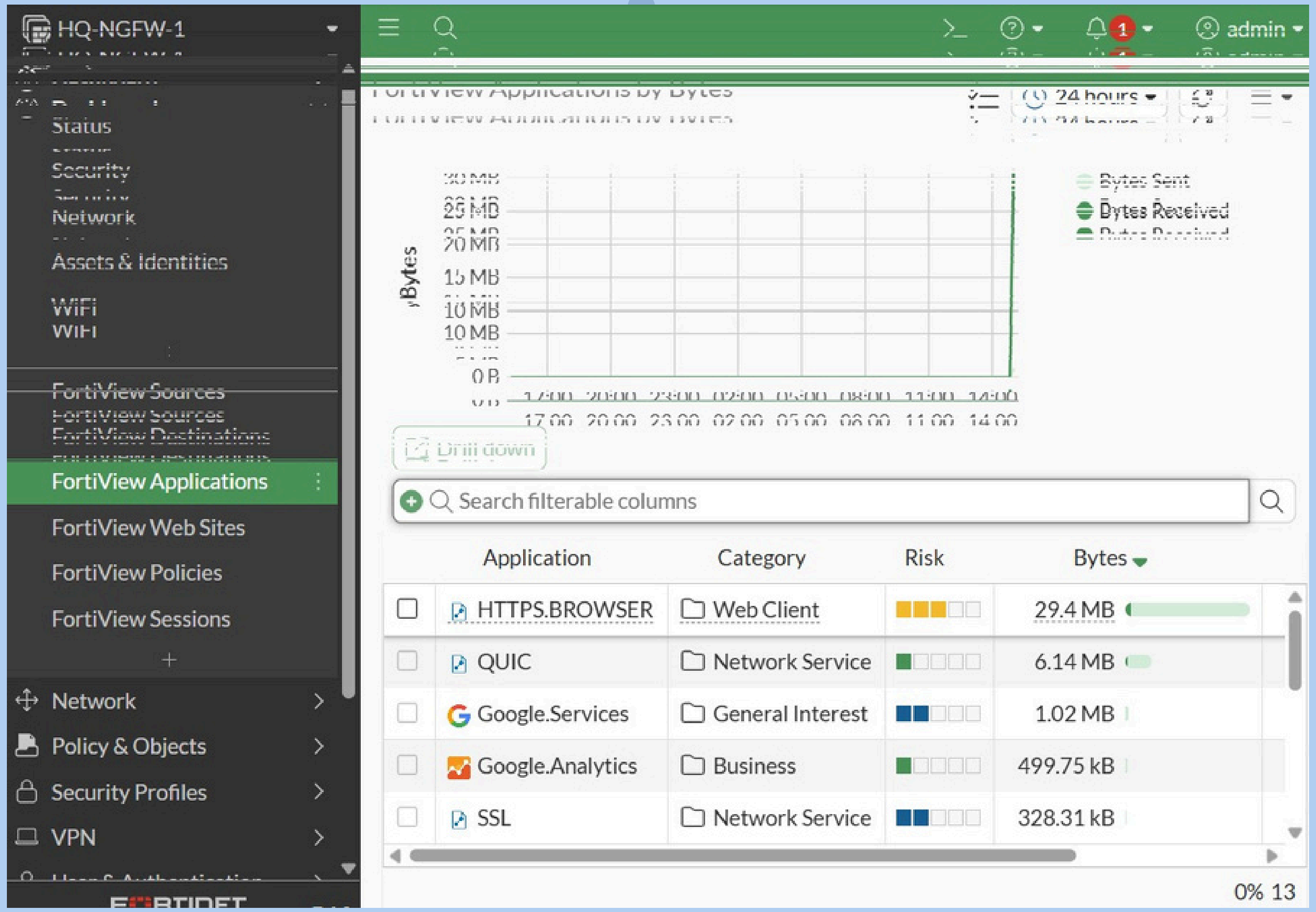


Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log
port2 → port6 1										
☑ Internet (1)	all	all	always	[object Object]	✓ ACCEPT		✓ NAT	Standard	default no-inspection	UTM
port4 → port2 3										
□ app (6)	all	all	always	[object Object]	✓ ACCEPT		✓ NAT	Standard	default no-inspection	✓ All
□ appctrl (5)	all	all	always	[object Object]	✓ ACCEPT		✓ NAT	Standard	default no-inspection	UTM
port4 → port6 1										
□ Internal FMG access (3)	all	all	always	[object Object]	✓ ACCEPT		✗ Disabled	Standard	no-inspection	UTM
port6 → port2 1										
Implicit 1										

week 3

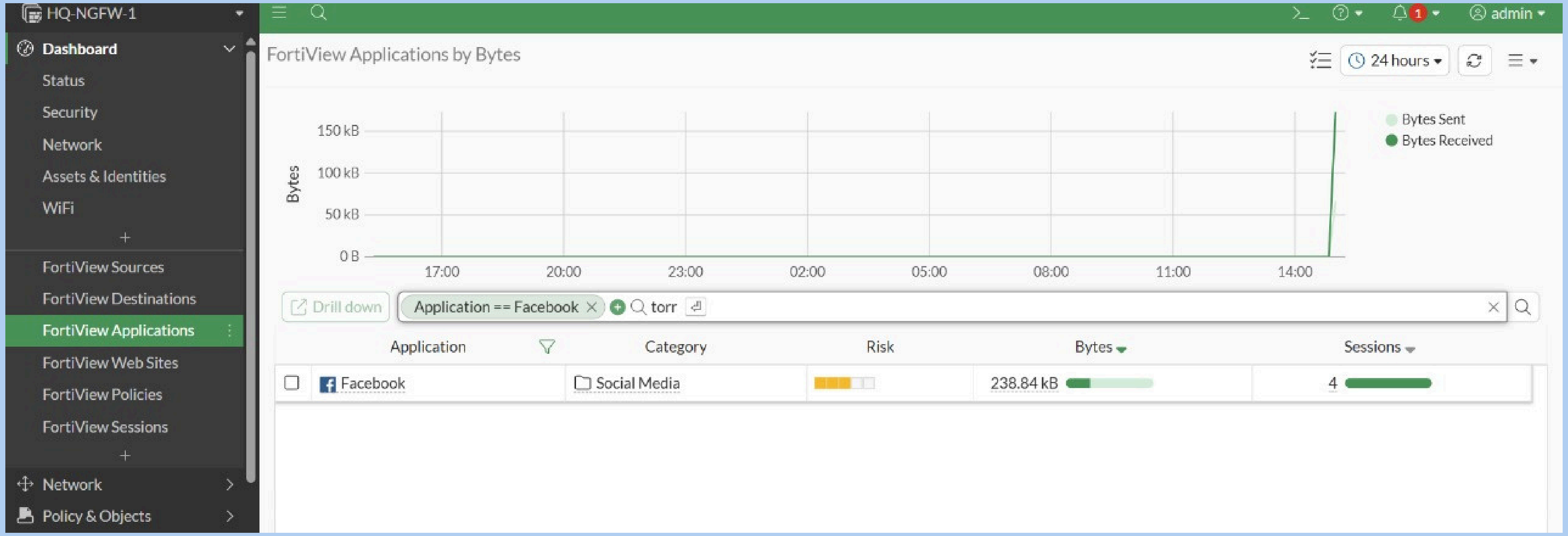
Testing and Monitoring

FortiView Applications Monitoring



Application	Category	Risk	Bytes
HTTPS.BROWSER	Web Client		29.4 MB
QUIC	Network Service		6.14 MB
Google.Services	General Interest		1.02 MB
Google.Analytics	Business		499.75 kB
SSL	Network Service		328.31 kB

0% 13



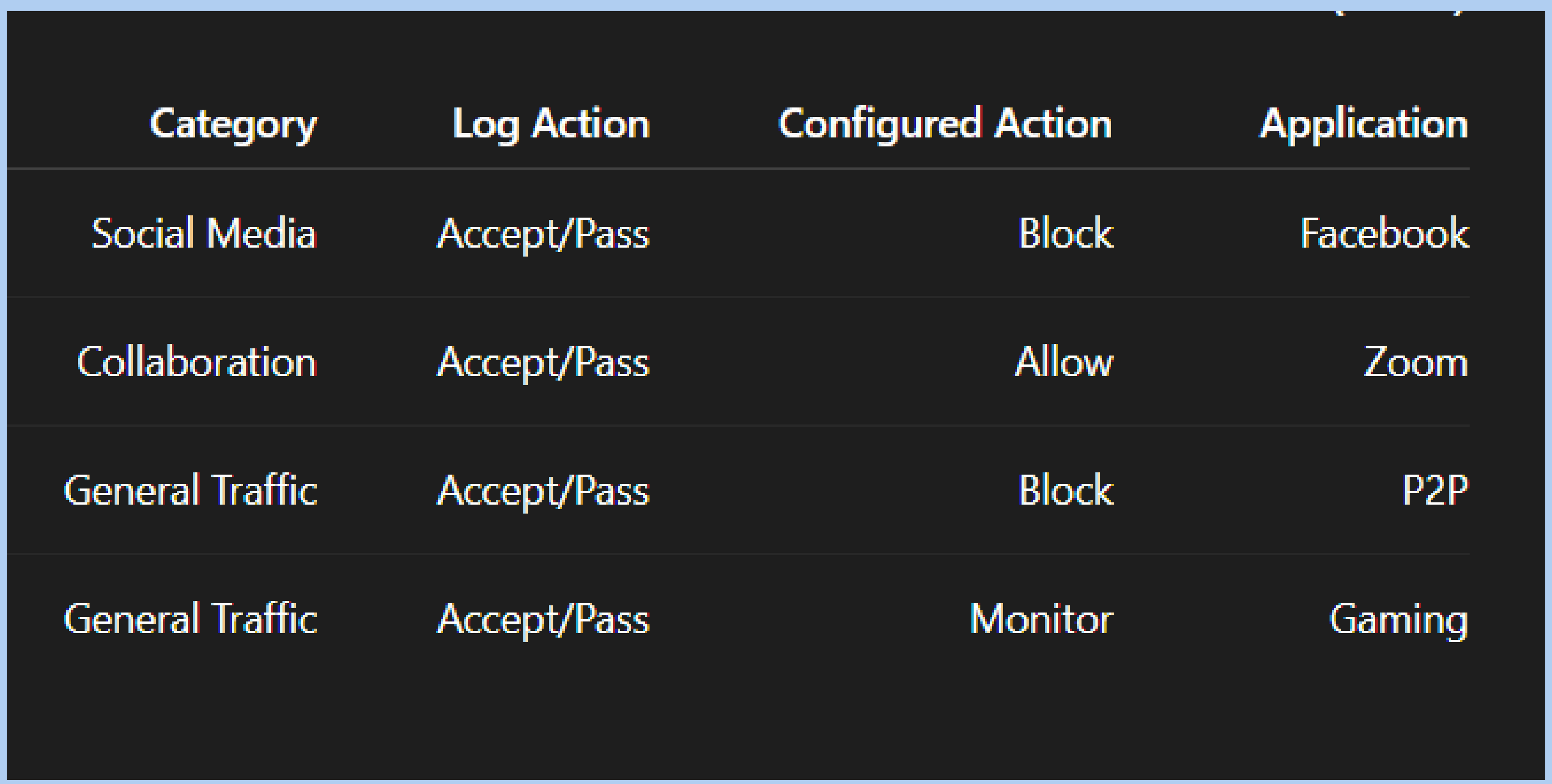
Application == Facebook torr

Application	Category	Risk	Bytes	Sessions
Facebook	Social Media		238.84 kB	4

Despite the failure of the block action, all application traffic was successfully recorded in FortiView due to proper logging configuration.

week 3

Testing and Monitoring **Application Control Logs**



Category	Log Action	Configured Action	Application
Social Media	Accept/Pass	Block	Facebook
Collaboration	Accept/Pass	Allow	Zoom
General Traffic	Accept/Pass	Block	P2P
General Traffic	Accept/Pass	Monitor	Gaming

Logging Results

- Log allowed traffic was set to All Sessions.
- All traffic was successfully captured.
- Full visibility of application traffic was achieved.
- Logs were successfully extracted for documentation.

week 3

Conclusion

- Logging configuration was successfully implemented.
- Application traffic visibility was achieved.
- Application Control actions were bypassed due to firewall policy order.
- This confirms the critical importance of firewall policy priority on FortiGate devices.

week 3

Testing and Monitoring
IPS – FortiGate

Objective

- To test the configured IPS profile.
- To generate real or simulated attack traffic.
- To monitor IPS events and logs.
- To analyze the effectiveness of IPS signatures and security actions.
- To ensure threats are properly detected and blocked according to policy.

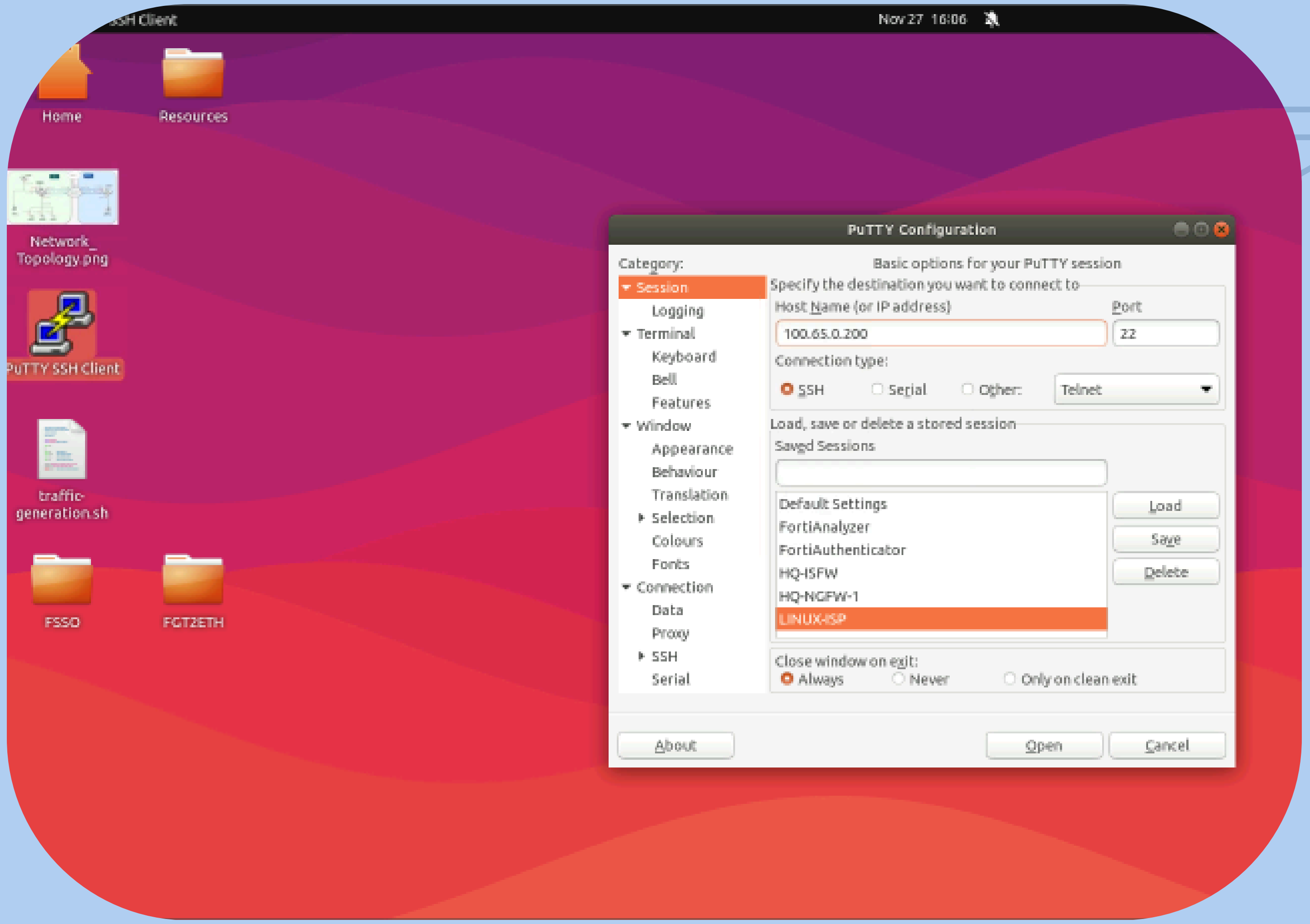
week 3

Testing and Monitoring
Attack Traffic

The HQ-PC-1 client machine was used to generate attack to test the configured IPS policies.

Use PuTTY to Access the Attacker Machine

- Open PuTTY SSH Client
- Enter the target IP : 100.65.0.200
- Use port 22
- Load the saved session: LINUX-ISP or your configured attacker VM
- Click Open and log in
- Run the following commands from the attacker VM :<Nikto.pl -host 100.65.0.200>



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 100.65.0.200

Port: 22

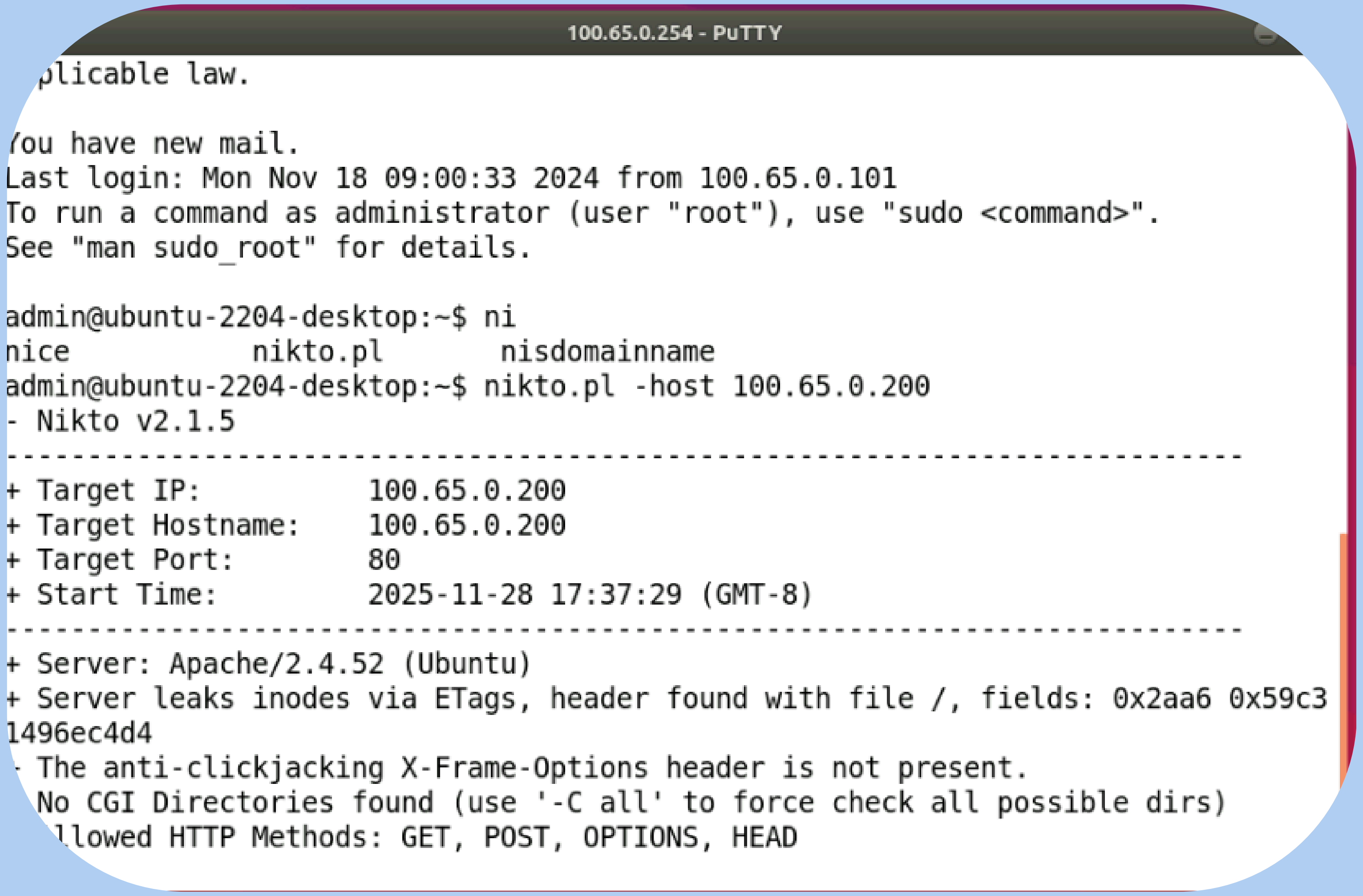
Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings
FortiAnalyzer
FortiAuthenticator
HQ-ISFW
HQ-NGFW-1
LINUX-ISP

Close window on exit: ● Always ○ Never ○ Only on clean exit



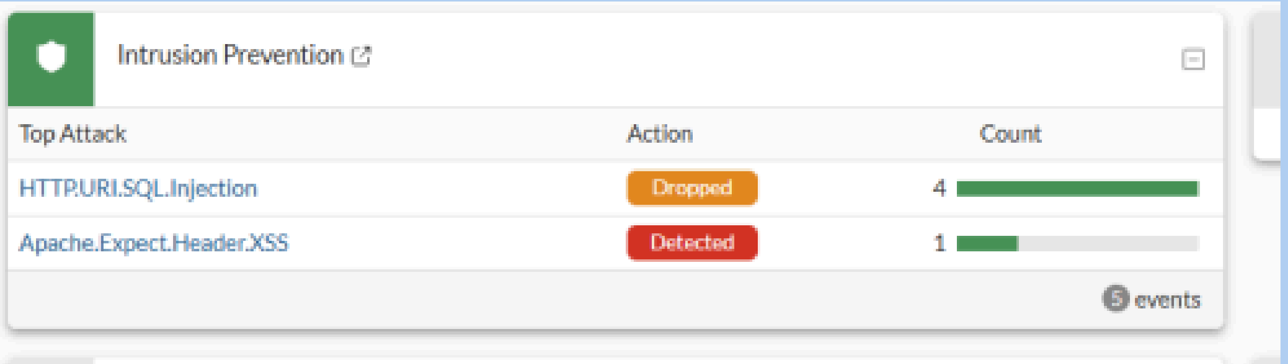
```
plicable law.

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)
 llowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

week 3

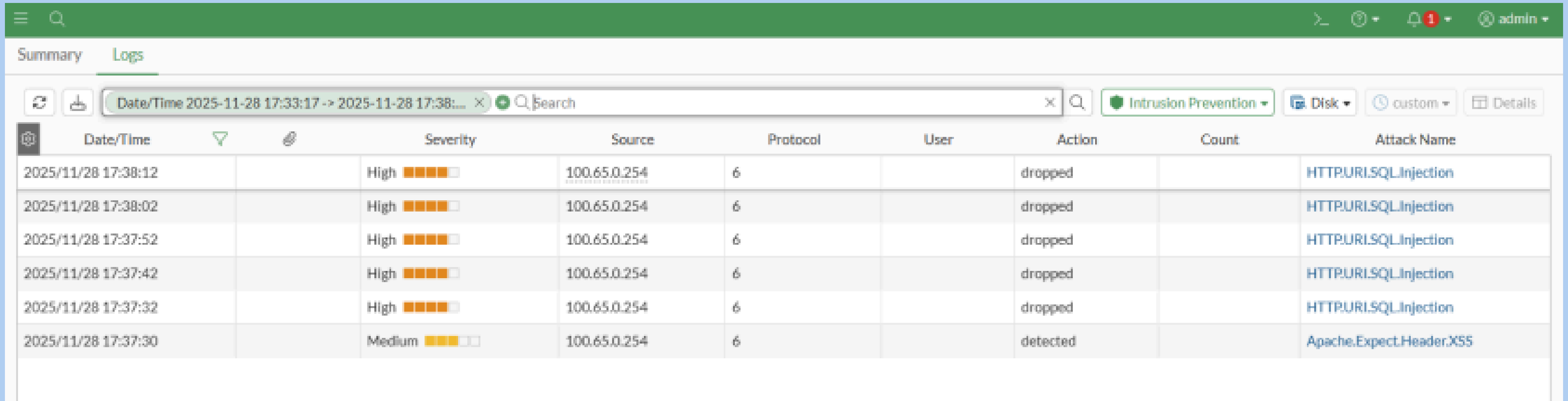
Testing and Monitoring
Monitoring the IPS



Intrusion Prevention

Top Attack	Action	Count
HTTP.URI.SQL.Injection	Dropped	4
Apache.Expect.Header.XSS	Detected	1

5 events



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

Navigate to IPS Logs

1. On the left menu, click Log & Report
2. Select Intrusion Prevention
3. Click a log entry, and then click Details.
4. In the Attack Name field, click the link.

Testing and Monitoring

Review the Logged Events

week 3

Severity

Indicates how dangerous the attack is (High, Medium, Low).

- **Protocol**

Displays the protocol used for the attack
 (e.g., 6 = TCP).

- **Action**

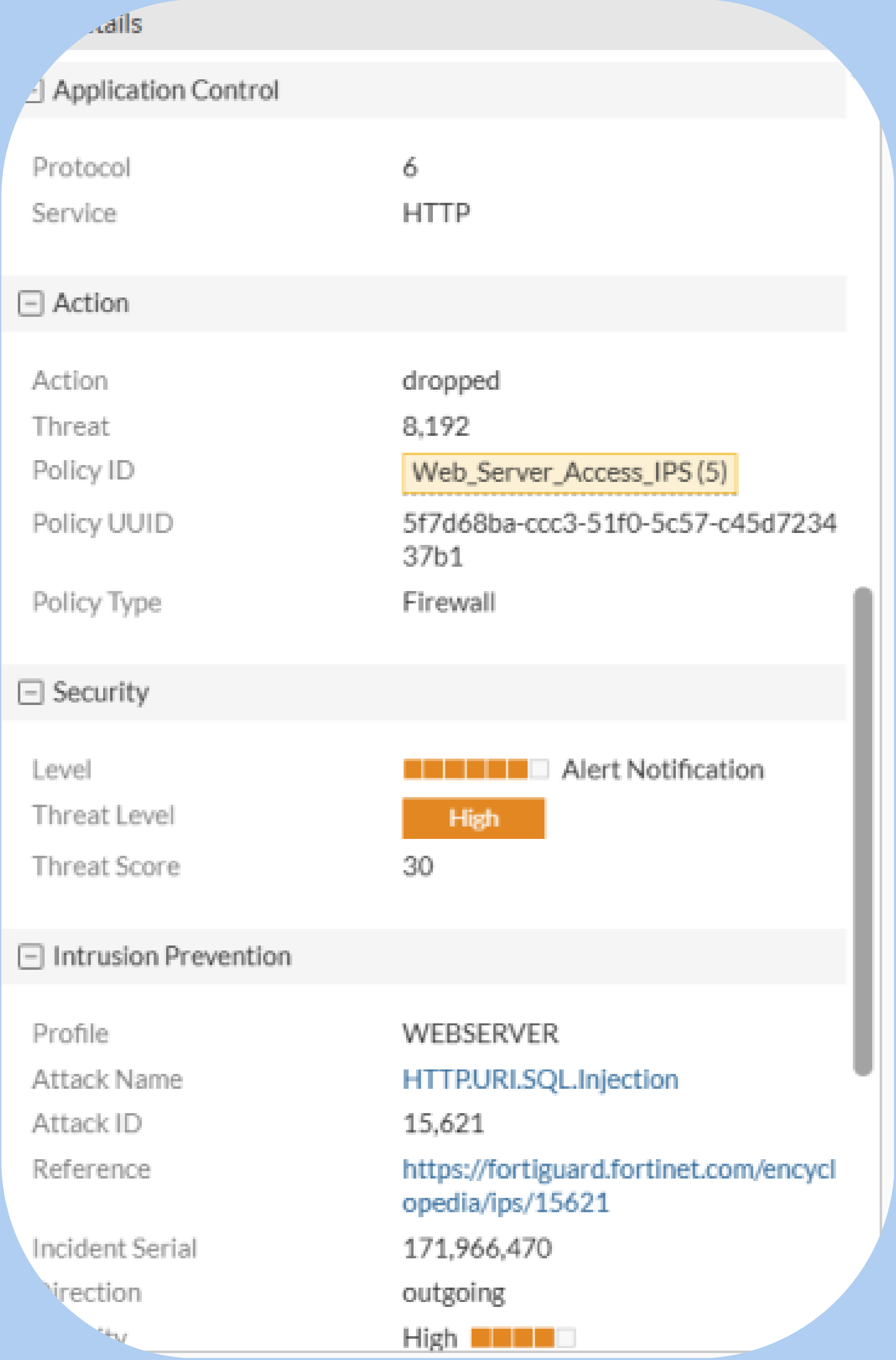
Shows what FortiGate did:

- dropped → attack blocked
- detected → attack detected but allowed

- **Attack Name**

Identifies the signature triggered, such as:

- HTTP.URI.SQL_Injection
- Apache.Expect.Header.XSS



ails

⊟ Application Control

Protocol	6
Service	HTTP

⊟ Action

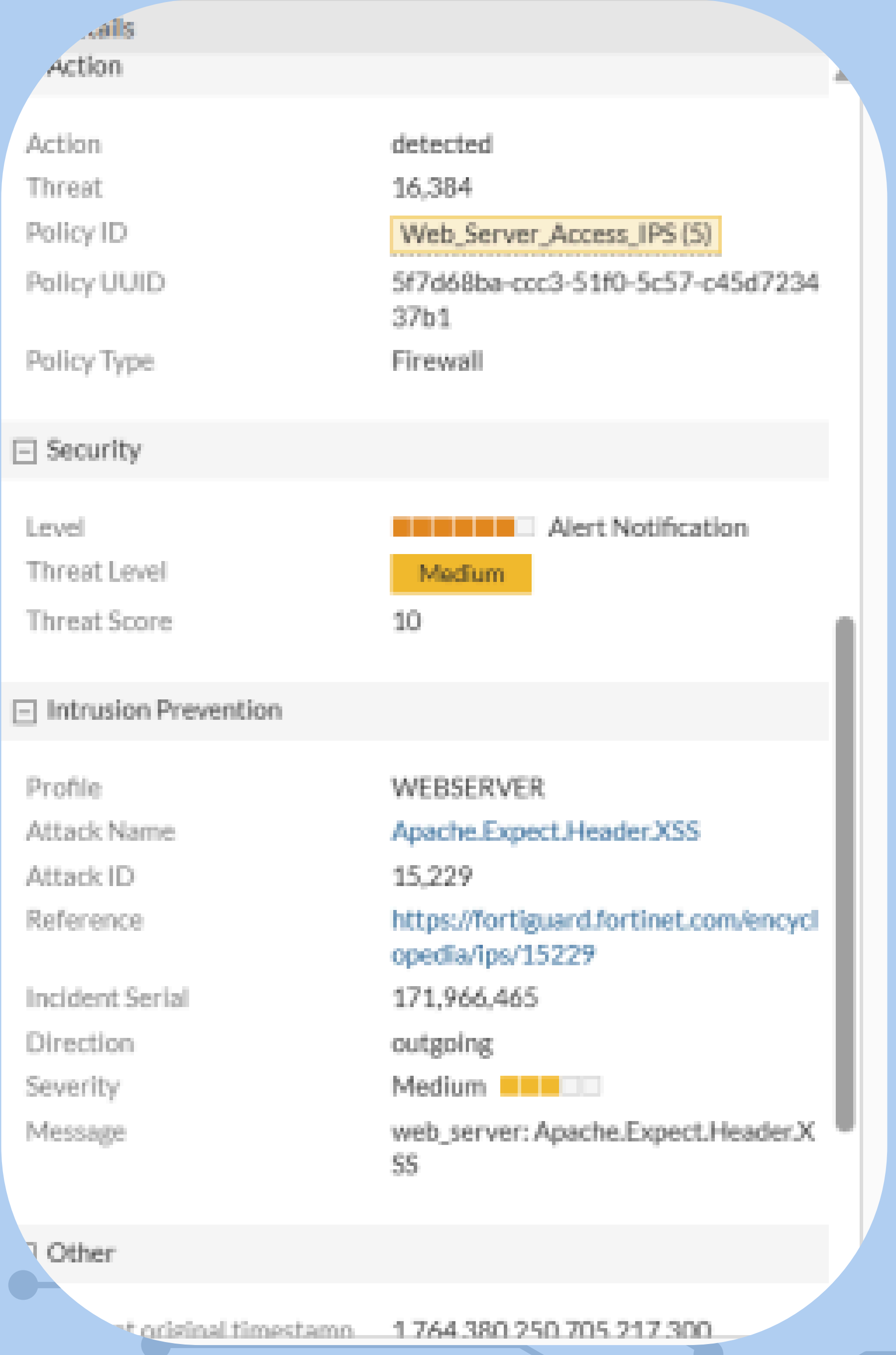
Action	dropped
Threat	8,192
Policy ID	Web_Server_Access_IPS (5)
Policy UUID	5f7d68ba-ccc3-51f0-5c57-c45d7234 37b1
Policy Type	Firewall

⊟ Security

Level	■■■■■■□ Alert Notification
Threat Level	High
Threat Score	30

⊟ Intrusion Prevention

Profile	WEBSERVER
Attack Name	HTTP.URI.SQL.Injection
Attack ID	15,621
Reference	https://fortiguard.fortinet.com/encyclopedia/ips/15621
Incident Serial	171,966,470
irection	outgoing
ity	High ■■■■□



ails

Action

Action	detected
Threat	16,384
Policy ID	Web_Server_Access_IPS (5)
Policy UUID	5f7d68ba-ccc3-51f0-5c57-c45d7234 37b1
Policy Type	Firewall

⊟ Security

Level	■■■■■■□ Alert Notification
Threat Level	Medium
Threat Score	10

⊟ Intrusion Prevention

Profile	WEBSERVER
Attack Name	Apache.Expect.Header.XSS
Attack ID	15,229
Reference	https://fortiguard.fortinet.com/encyclopedia/ips/15229
Incident Serial	171,966,465
Direction	outgoing
Severity	Medium ■■■□□
Message	web_server: Apache.Expect.Header.XSS

Other

t original timestamp	1,764,380,250,705,217,300

week 3

Conclusion

- IPS profile configuration was successfully implemented.
- Malicious traffic simulation generated multiple detectable threats.
- FortiGate accurately identified and blocked attacks such as SQL injection and XSS attempts.
- IPS logs provided clear visibility into attack sources, severity levels, and actions taken.
- This confirms the effectiveness of FortiGate's Intrusion Prevention System in proactively protecting the network and enforcing security policies.