Week 3: Monitoring and Reporting

Introduction:

This document presents the monitoring and reporting procedures implemented on the FortiGate firewall as part of Week 3 of the project. Monitoring and reporting are essential components of an effective security strategy, as they provide continuous visibility into network activity, threat detections, and the overall performance of deployed security profiles. By leveraging FortiGate's built-in dashboards, logs, and reporting tools, administrators can assess the effectiveness of Antivirus, Web Filtering, and Application Control profiles configured in previous phases.

This guide outlines the configuration of key monitoring features, methods for analyzing security events, and the process of generating detailed reports. These insights help ensure proactive threat detection, support troubleshooting efforts, and contribute to ongoing optimization of the organization's security posture.

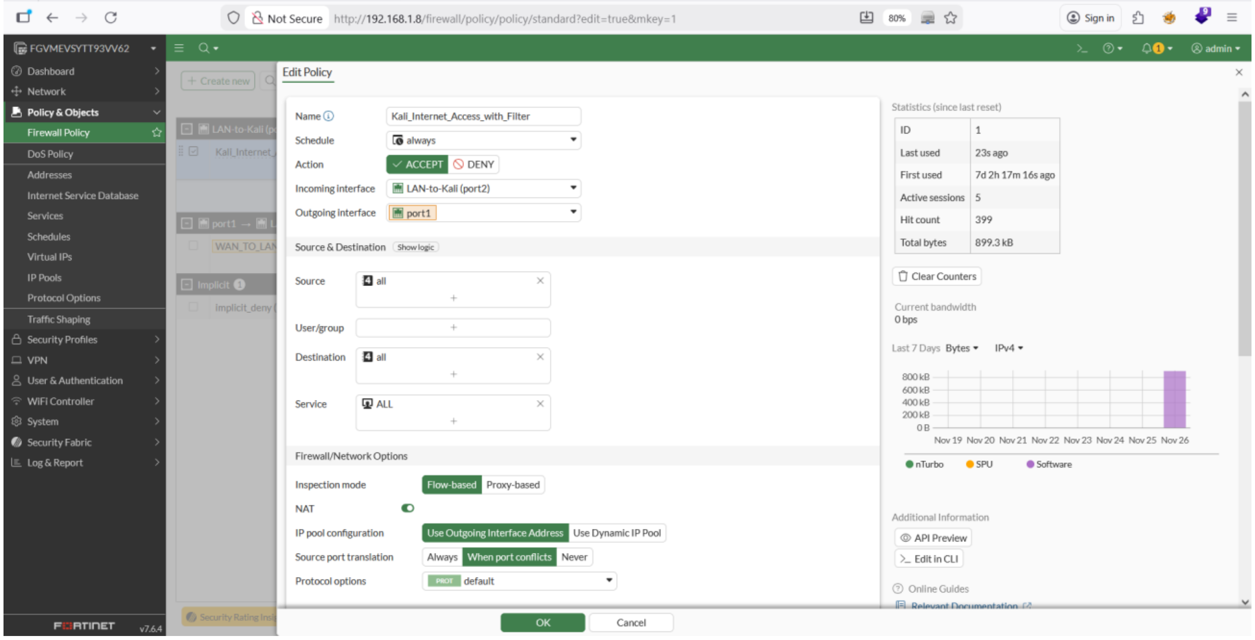
Objectives

- To enable and configure FortiGate monitoring tools for tracking security events.
- To analyze logs and dashboards to measure the effectiveness of deployed security profiles.
- To generate automated and on-demand reports for security visibility and documentation.
- To evaluate detected threats, blocked activities, and system performance.
- To provide clear configuration details and reporting examples for future reference.
- To support continuous improvement of the network's security controls.

Monitoring and Reporting

1-Web filter :

Firewall Policy:



Edit Policy

Name: Kali_Internet_Access_with_Filter
Schedule: always
Action: ACCEPT | DENY
Incoming interface: LAN-to-Kali (port2)
Outgoing interface: port1

Source & Destination (Show logic)

Source: all
User/group:
Destination: all
Service: ALL

Firewall/Network Options

Inspection mode: Flow-based | Proxy-based
NAT: on
IP pool configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Source port translation: Always | When port conflicts | Never
Protocol options: PROT default

Statistics (since last reset)

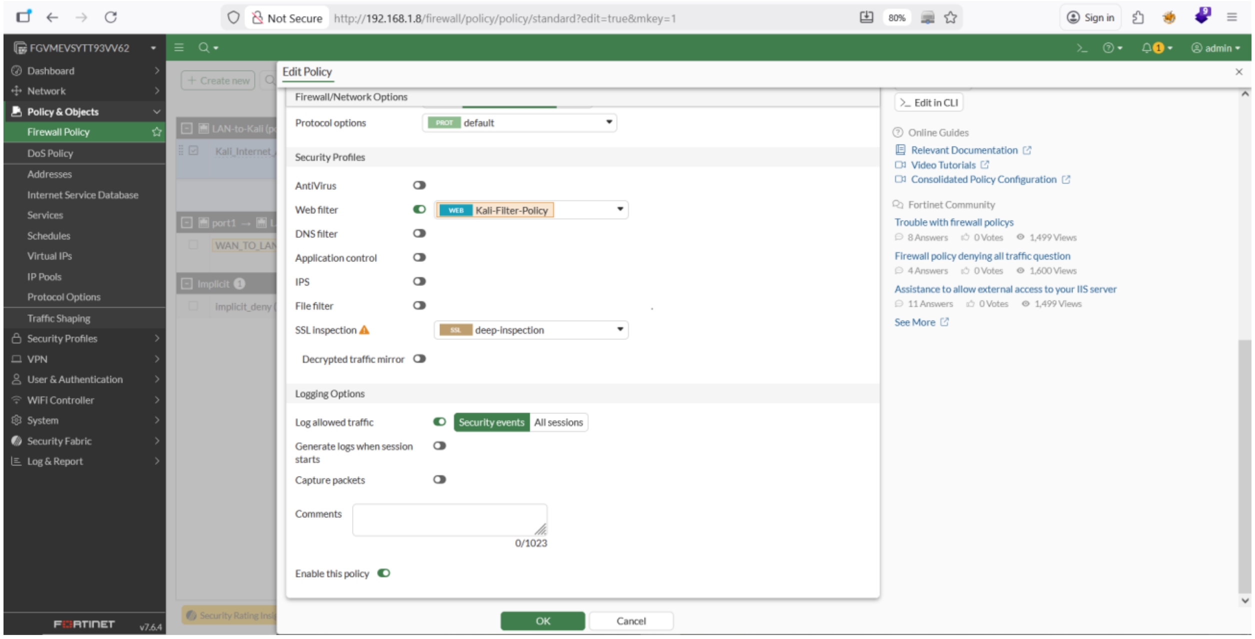
ID	1
Last used	23s ago
First used	7d 2h 17m 16s ago
Active sessions	5
Hit count	399
Total bytes	899.3 kB

Current bandwidth
0 bps

Last 7 Days Bytes IPv4

Additional Information

Firewall Policy Details: Policy Kali_Internet_Access_with_Filter governing LAN-to-WAN traffic.



Edit Policy

Firewall/Network Options

Protocol options: PROT default

Security Profiles

AntiVirus: off
Web filter: on — WEB Kali-Filter-Policy
DNS filter: off
Application control: off
IPS: off
File filter: off
SSL inspection: SSL deep-inspection
Decrypted traffic mirror: off

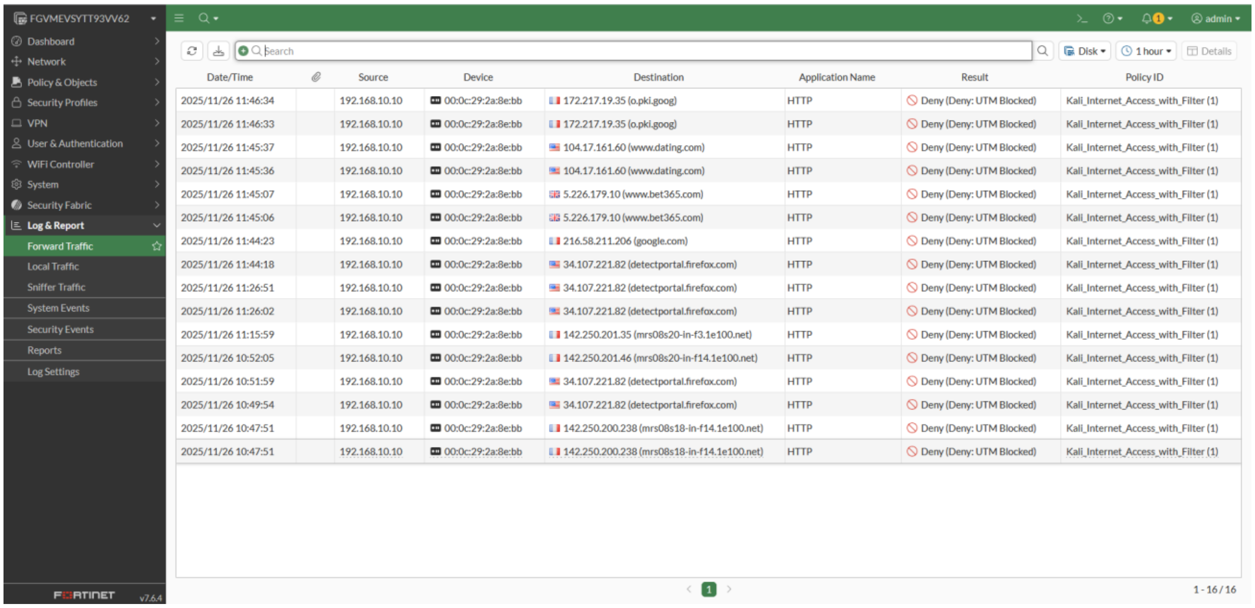
Logging Options

Log allowed traffic: on — Security events | All sessions
Generate logs when session starts: off
Capture packets: off
Comments: 0/1023
Enable this policy: on

Logging Configuration: Confirmation of Web Filter enforcement (Kali-Filter-Policy) and Logging Options set to 'Security events All' to ensure comprehensive traffic monitoring and security violation capture

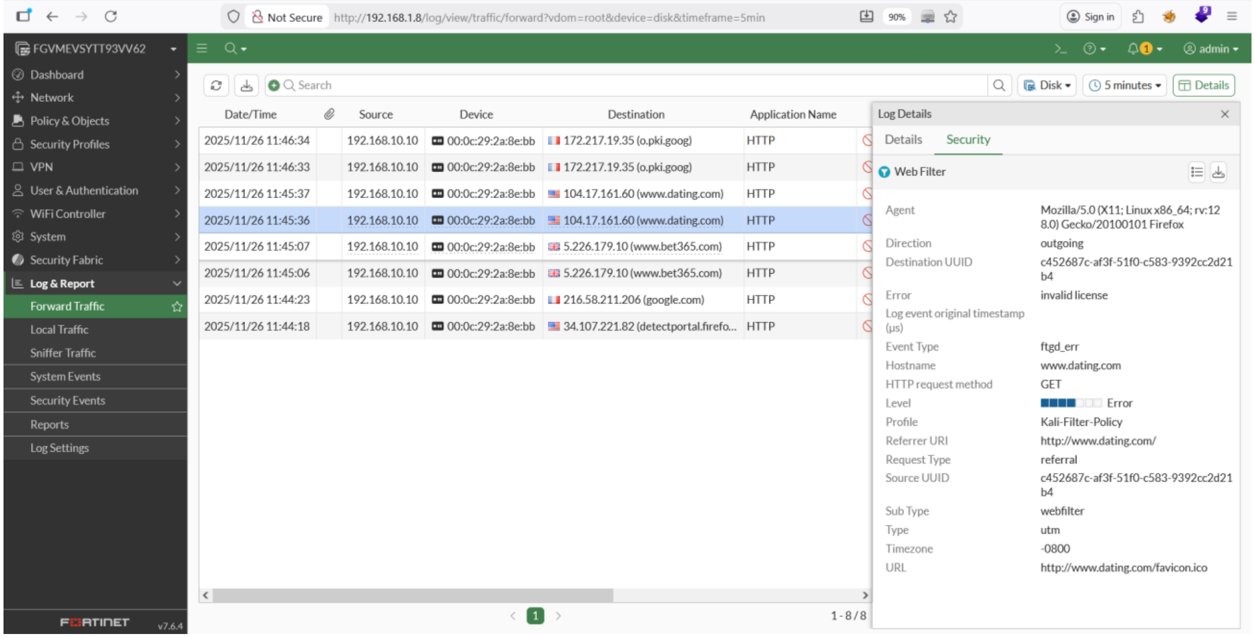
Log & Report:

1.1 Forward Traffic:



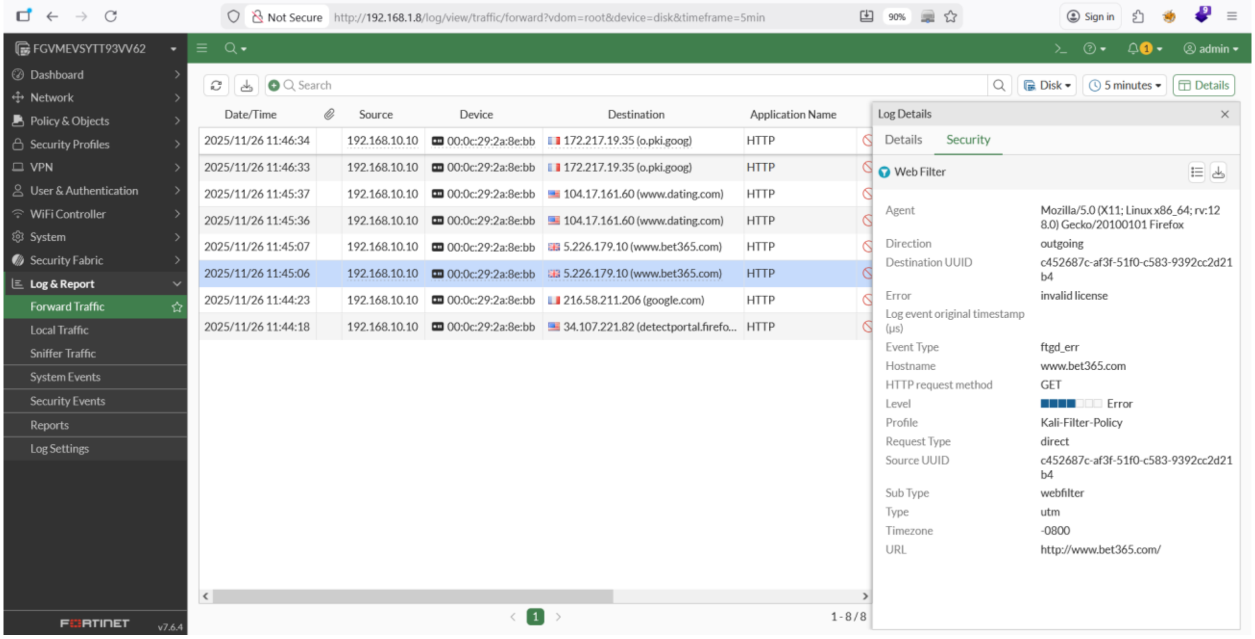
Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
2025/11/26 11:46:34		192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:46:33		192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:37		192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:36		192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:07		192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:06		192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:44:23		192.168.10.10	00:0c:29:2a:8e:bb	216.58.211.206 (google.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:44:18		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:26:51		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:26:02		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:15:59		192.168.10.10	00:0c:29:2a:8e:bb	142.250.201.35 (mrs08s20-in-f3.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:52:05		192.168.10.10	00:0c:29:2a:8e:bb	142.250.201.46 (mrs08s20-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:51:59		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:49:54		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:47:51		192.168.10.10	00:0c:29:2a:8e:bb	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:47:51		192.168.10.10	00:0c:29:2a:8e:bb	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)

Forward Traffic Logs: Logs filtered by the firewall policy, showing multiple HTTP sessions from the source IP (192.168.10.10) resulting in a Deny (Deny: UTM Blocked) action, confirming security profile enforcement.



Date/Time		Source	Device	Destination	Application Name
2025/11/26 11:46:34		192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP
2025/11/26 11:46:33		192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP
2025/11/26 11:45:37		192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP
2025/11/26 11:45:36		192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP
2025/11/26 11:45:07		192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP
2025/11/26 11:45:06		192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP
2025/11/26 11:44:23		192.168.10.10	00:0c:29:2a:8e:bb	216.58.211.206 (google.com)	HTTP
2025/11/26 11:44:18		192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefo...	HTTP

Agent	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox
Direction	outgoing
Destination UUID	c452687c-af3f-51f0-c583-9392cc2d21b4
Error	invalid license
Log event original timestamp (µs)	
Event Type	ftgd_err
Hostname	www.dating.com
HTTP request method	GET
Level	Error
Profile	Kali-Filter-Policy
Referrer URI	http://www.dating.com/
Request Type	referral
Source UUID	c452687c-af3f-51f0-c583-9392cc2d21b4
Sub Type	webfilter
Type	utm
Timezone	-0800
URL	http://www.dating.com/favicon.ico



Date/Time	Source	Device	Destination	Application Name
2025/11/26 11:46:34	192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP
2025/11/26 11:46:33	192.168.10.10	00:0c:29:2a:8e:bb	172.217.19.35 (o.pki.goog)	HTTP
2025/11/26 11:45:37	192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP
2025/11/26 11:45:36	192.168.10.10	00:0c:29:2a:8e:bb	104.17.161.60 (www.dating.com)	HTTP
2025/11/26 11:45:07	192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP
2025/11/26 11:45:06	192.168.10.10	00:0c:29:2a:8e:bb	5.226.179.10 (www.bet365.com)	HTTP
2025/11/26 11:44:23	192.168.10.10	00:0c:29:2a:8e:bb	216.58.211.206 (google.com)	HTTP
2025/11/26 11:44:18	192.168.10.10	00:0c:29:2a:8e:bb	34.107.221.82 (detectportal.firefo...	HTTP

Log Details

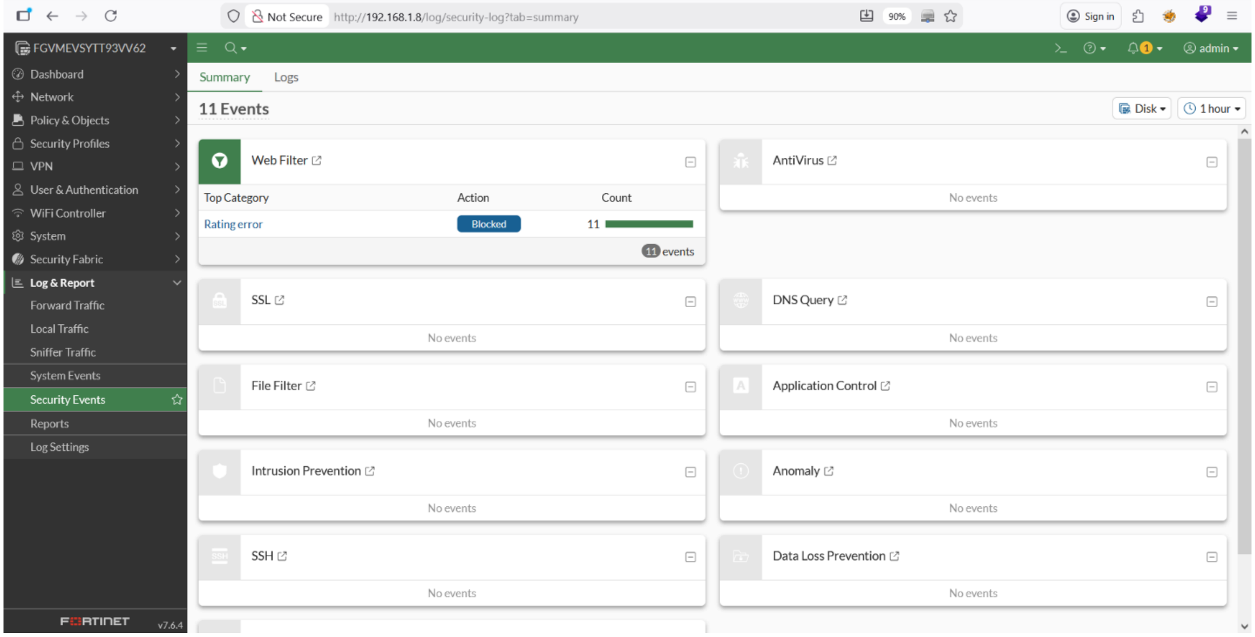
Details | Security

Web Filter

Agent	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox
Direction	outgoing
Destination UUID	c452687c-af3f-51f0-c583-9392cc2d21b4
Error	invalid license
Log event original timestamp (µs)	
Event Type	ftgd_err
Hostname	www.bet365.com
HTTP request method	GET
Level	■■■■□□□ Error
Profile	Kali-Filter-Policy
Request Type	direct
Source UUID	c452687c-af3f-51f0-c583-9392cc2d21b4
Sub Type	webfilter
Type	utm
Timezone	-0800
URL	http://www.bet365.com/

Log Detail View: Detailed view of a blocked session (e.g., dating.com), confirming the action was taken by the 'Kali-Filter-Policy' security profile, consistent with the productivity policy.

1.2 Security Events:



11 Events

Web Filter

Top Category	Action	Count
Rating error	Blocked	11

11 events

AntiVirus — No events

SSL — No events

DNS Query — No events

File Filter — No events

Application Control — No events

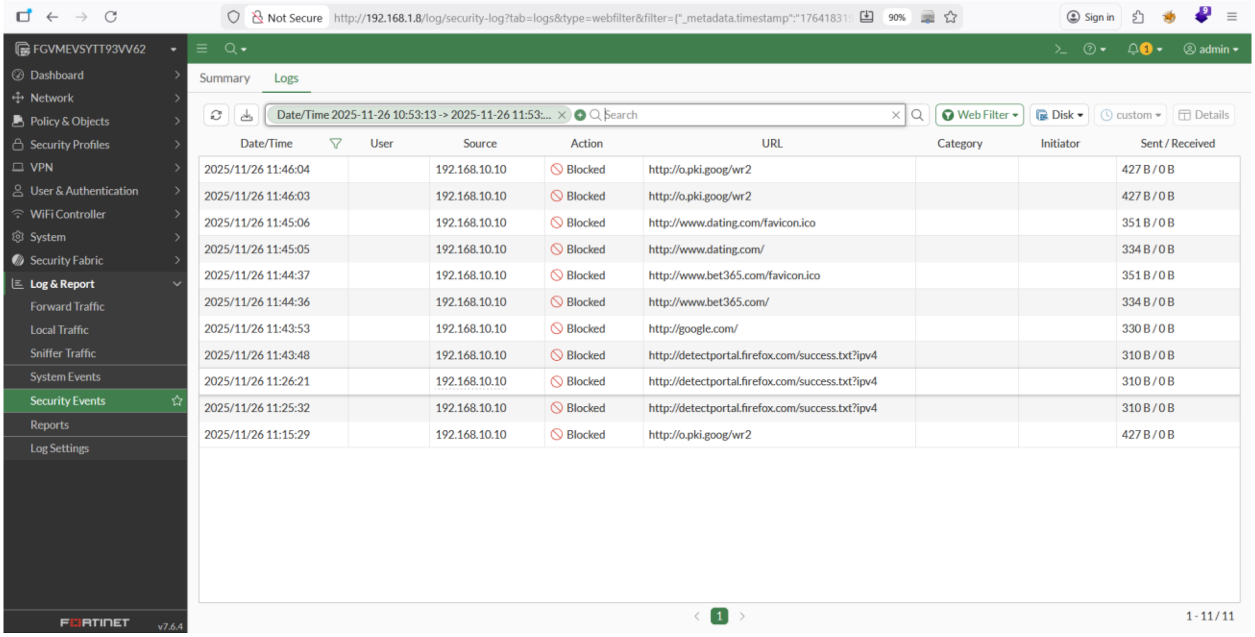
Intrusion Prevention — No events

Anomaly — No events

SSH — No events

Data Loss Prevention — No events

Security Events Summary: Web Filter events dashboard highlighting 11 Blocked actions recorded under the 'Rating error' (or other blocked category), demonstrating active violation enforcement.

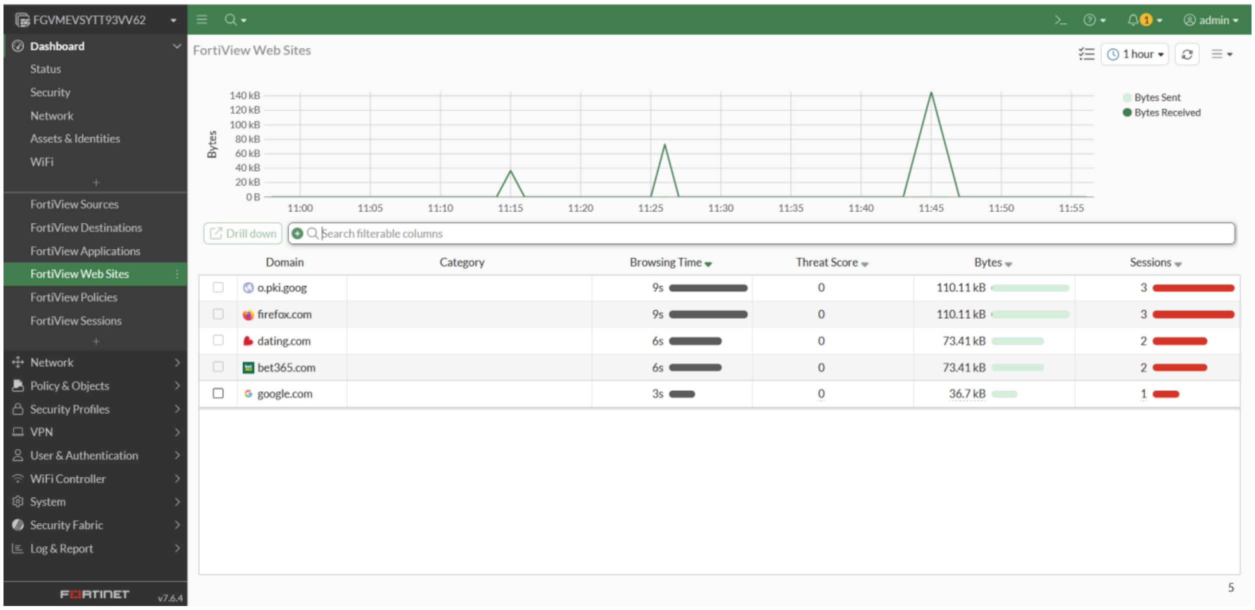


Date/Time	User	Source	Action	URL	Category	Initiator	Sent / Received
2025/11/26 11:46:04		192.168.10.10	Blocked	http://o.pki.goog/wr2			427 B / 0 B
2025/11/26 11:46:03		192.168.10.10	Blocked	http://o.pki.goog/wr2			427 B / 0 B
2025/11/26 11:45:06		192.168.10.10	Blocked	http://www.dating.com/favicon.ico			351 B / 0 B
2025/11/26 11:45:05		192.168.10.10	Blocked	http://www.dating.com/			334 B / 0 B
2025/11/26 11:44:37		192.168.10.10	Blocked	http://www.bet365.com/favicon.ico			351 B / 0 B
2025/11/26 11:44:36		192.168.10.10	Blocked	http://www.bet365.com/			334 B / 0 B
2025/11/26 11:43:53		192.168.10.10	Blocked	http://google.com/			330 B / 0 B
2025/11/26 11:43:48		192.168.10.10	Blocked	http://detectportal.firefox.com/success.txt?ipv4			310 B / 0 B
2025/11/26 11:26:21		192.168.10.10	Blocked	http://detectportal.firefox.com/success.txt?ipv4			310 B / 0 B
2025/11/26 11:25:32		192.168.10.10	Blocked	http://detectportal.firefox.com/success.txt?ipv4			310 B / 0 B
2025/11/26 11:15:29		192.168.10.10	Blocked	http://o.pki.goog/wr2			427 B / 0 B

Web Filter Blocked Logs: Detailed log view showing multiple distinct URLs (dating.com, bet365.com) from the source 192.168.10.10 resulting in a 'Blocked' action.

2- Dashboard

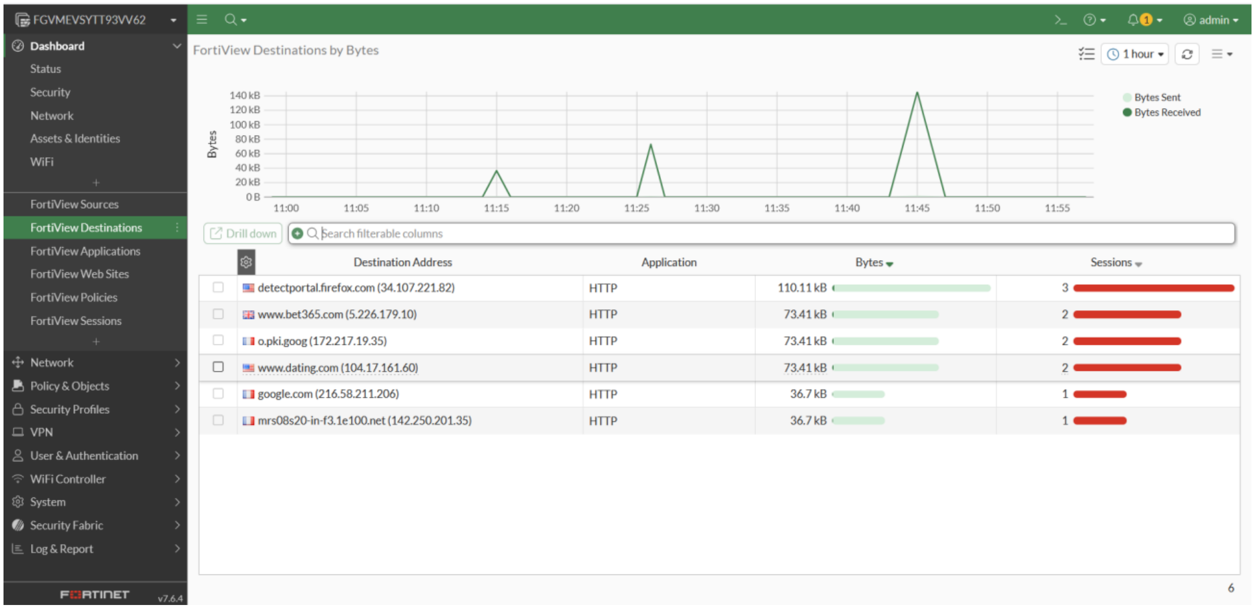
2.1 FortiView Web Sites



Domain	Category	Browsing Time	Threat Score	Bytes	Sessions
o.pki.goog		9s	0	110.11 kB	3
firefox.com		9s	0	110.11 kB	3
dating.com		6s	0	73.41 kB	2
bet365.com		6s	0	73.41 kB	2
google.com		3s	0	36.7 kB	1

FortiView Web Sites: Dashboard view showing the attempted access to prohibited domains such as 'dating.com' and 'bet365.com' with corresponding session count, which were subsequently blocked by the applied Web Filter policy.

2.2 FortiView Destinations

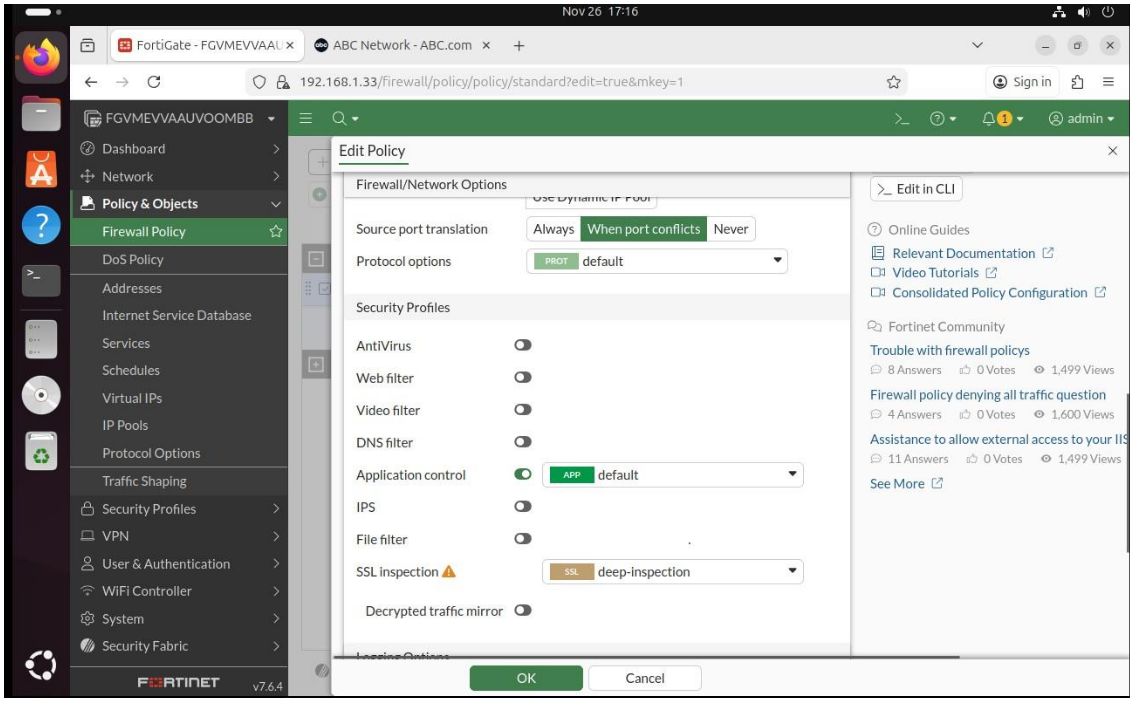


Destination Address	Application	Bytes	Sessions
detectportal.firefox.com (34.107.221.82)	HTTP	110.11 kB	3
www.bet365.com (5.226.179.10)	HTTP	73.41 kB	2
o.pki.goog (172.217.19.35)	HTTP	73.41 kB	2
www.dating.com (104.17.161.60)	HTTP	73.41 kB	2
google.com (216.58.211.206)	HTTP	36.7 kB	1
mrs08s20-in-f3.1e100.net (142.250.201.35)	HTTP	36.7 kB	1

FortiView Destinations: Analysis of network destinations, confirming connections attempted towards the IP addresses associated with restricted websites like '**bet365.com**' and '**www.dating.com**'

2-Application Control

Firewall Policy:



Firewall/Network Options

Source port translation: Always | **When port conflicts** | Never

Protocol options: PROT default

Security Profiles

AntiVirus: off

Web filter: off

Video filter: off

DNS filter: off

Application control: on — APP default

IPS: off

File filter: off

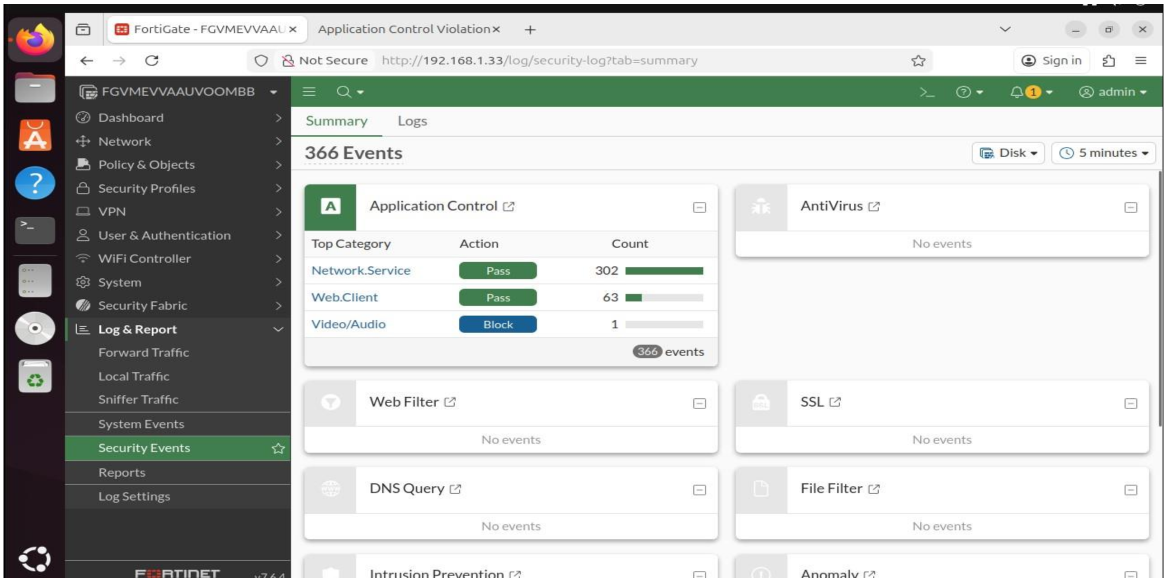
SSL inspection: SSL deep-inspection

Decrypted traffic mirror: off

Application control enforcement (default profile) and Logging Options set to 'Security events All' to ensure comprehensive traffic monitoring and security violation capture related to application usage.

Log & Report:

1-Security Events:



366 Events

Application Control

Top Category	Action	Count
Network.Service	Pass	302
Web.Client	Pass	63
Video/Audio	Block	1

366 events

AntiVirus: No events

Web Filter: No events

SSL: No events

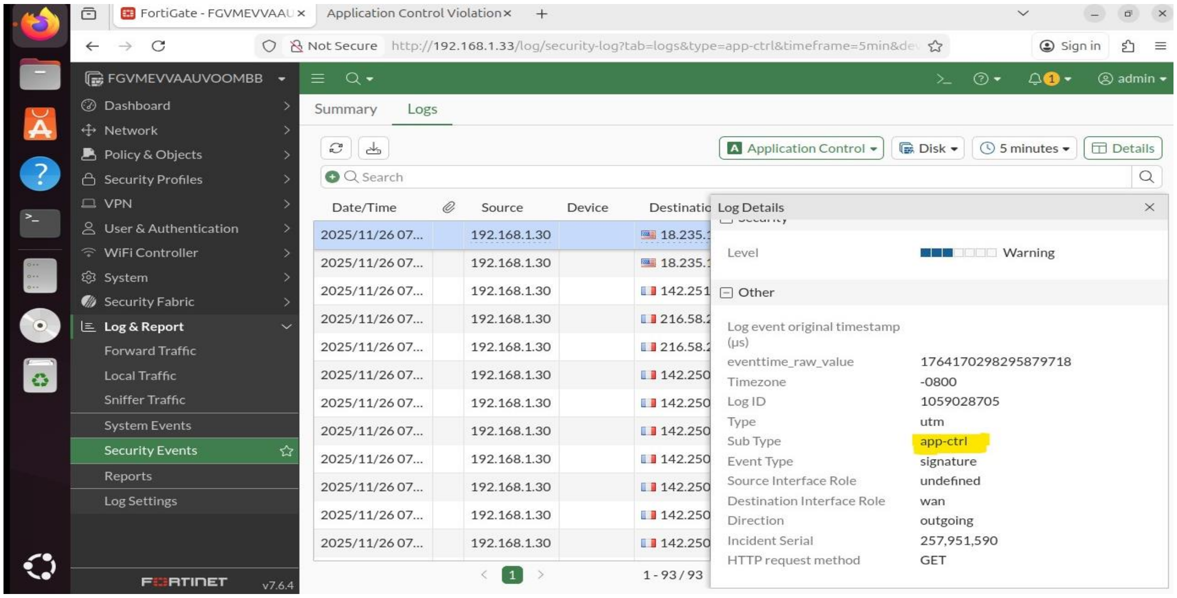
DNS Query: No events

File Filter: No events

Intrusion Prevention

Anomaly

Security Events Summary: Web Filter events dashboard highlighting 11 Blocked actions recorded under the 'Rating error' (or other blocked category), demonstrating active violation enforcement.



Date/Time	Source	Device	Destinatio
2025/11/26 07...	192.168.1.30		18.235.1
2025/11/26 07...	192.168.1.30		18.235.1
2025/11/26 07...	192.168.1.30		142.251
2025/11/26 07...	192.168.1.30		216.58.2
2025/11/26 07...	192.168.1.30		216.58.2
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250
2025/11/26 07...	192.168.1.30		142.250

1 - 93 / 93

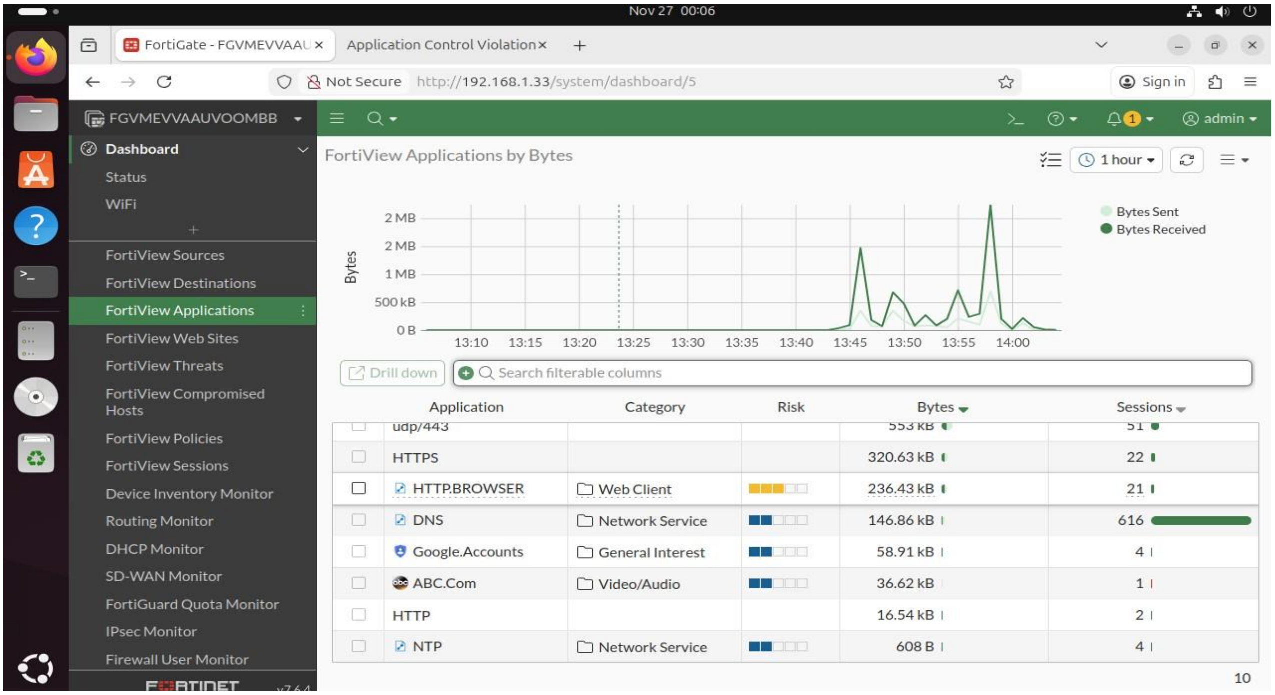
Log Details

Level	Warning
Other	
Log event original timestamp (µs)	
eventtime_raw_value	1764170298295879718
Timezone	-0800
Log ID	1059028705
Type	utm
Sub Type	app-ctrl
Event Type	signature
Source Interface Role	undefined
Destination Interface Role	wan
Direction	outgoing
Incident Serial	257,951,590
HTTP request method	GET

Application Control Blocked Logs: The detailed log view shows multiple entries. The system attempted to identify an application named ABC.com, which falls under the Video/Audio category. This activity resulted in a 'Block' action, enforced by the Lan-to-Wan (1) firewall policy, with the log type identified as app-ctrl at a Warning level.

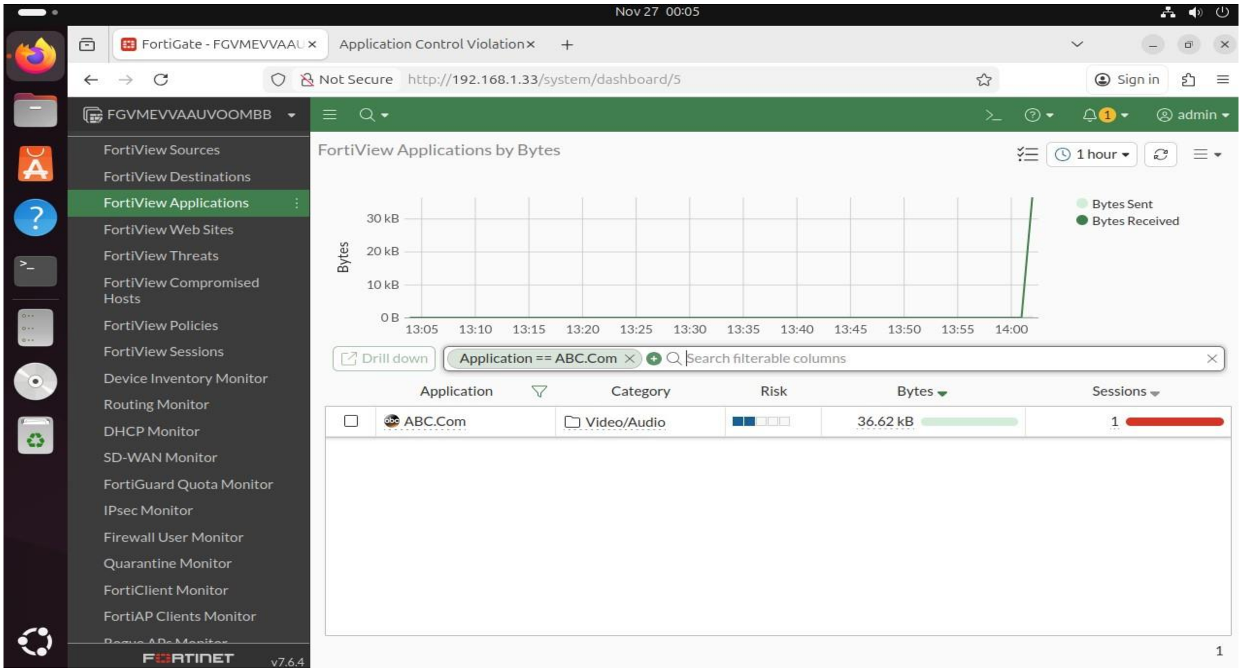
2-Dashboard

- **FortiView Applications**



	Application	Category	Risk	Bytes	Sessions
□	udp/443			553 kB	51
□	HTTPS			320.63 kB	22
□	HTTP.BROWSER	Web Client	■■■□□	236.43 kB	21
□	DNS	Network Service	■■□□□	146.86 kB	616
□	Google.Accounts	General Interest	■■□□□	58.91 kB	4
□	ABC.Com	Video/Audio	■■□□□	36.62 kB	1
□	HTTP			16.54 kB	2
□	NTP	Network Service	■■□□□	608 B	4

10



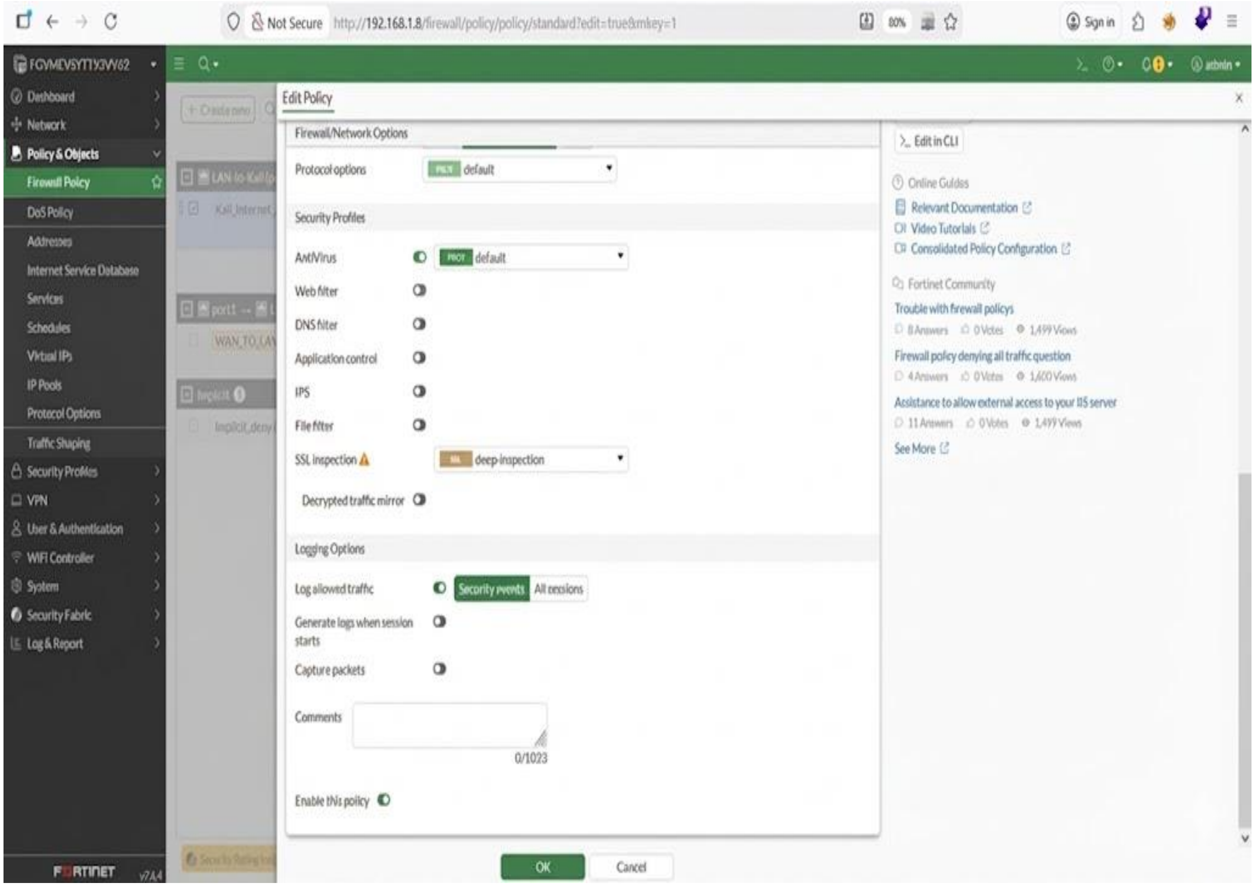
	Application	Category	Risk	Bytes	Sessions
□	ABC.Com	Video/Audio	■■□□□	36.62 kB	1

1

FortiView Application: The dashboard view shows the applications consuming bandwidth during the specified timeframe. The display captures an attempt to access the ABC.com application (categorized under Video/Audio) consuming 36.62 KB over 1 Session, aligning with the attempts that were subsequently blocked by the applied Application Control policy as seen in the logs.

3-Anti-Virus:

Firewall Policy Details: Policy Kali_Internet_Access_with_AV governing LAN-to-WAN traffic. This policy has the AntiVirus security profile enabled to scan and block malicious files during HTTP/HTTPS sessions.



Edit Policy

Firewall/Network Options

Protocol options: PROT default

Security Profiles

- AntiVirus: ● PROT default
- Web filter: ○
- DNS filter: ○
- Application control: ○
- IPS: ○
- File filter: ○
- SSL inspection: SSL deep-inspection
- Decrypted traffic mirror: ○

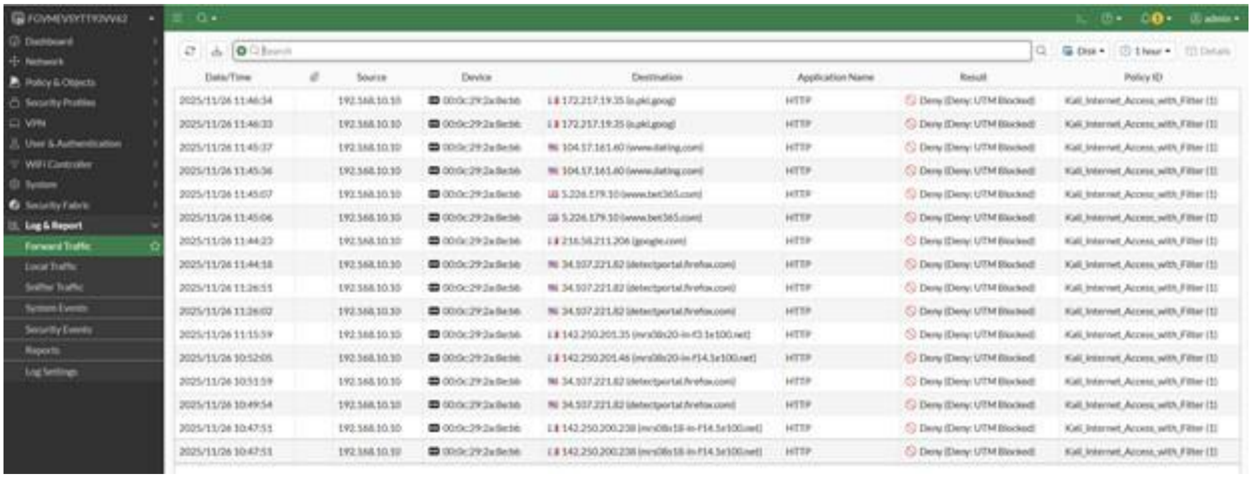
Logging Options

- Log allowed traffic: ● [✓ Security events] All sessions
- Generate logs when session starts: ○
- Capture packets: ○

Comments: 0/1023

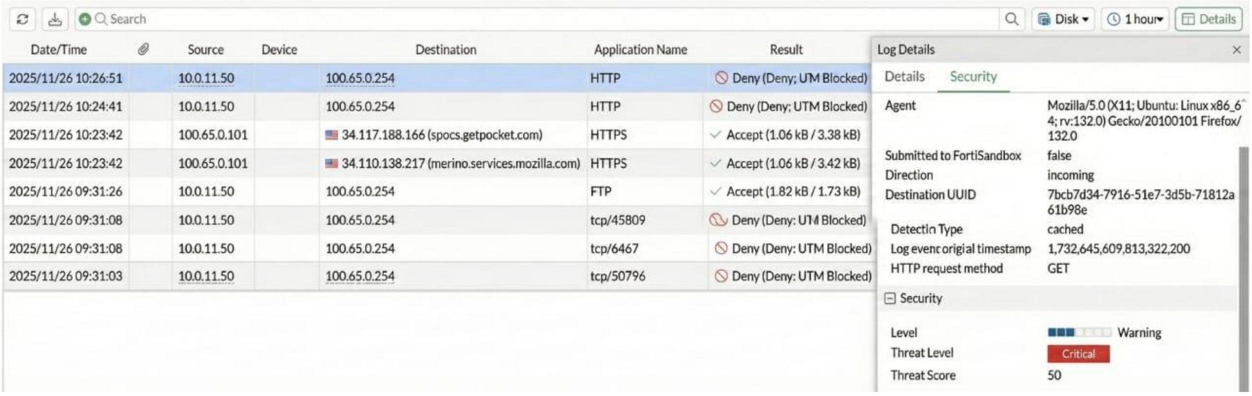
Enable this policy ●

Logging Configuration: Confirmation of AntiVirus profile enforcement and Logging Options set to 'Security events' or 'All sessions' to ensure comprehensive traffic monitoring and capture of any virus detection events.



Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2025/11/26 11:46:34	192.168.10.10	00:0c:29:2a:8e:b6	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:46:33	192.168.10.10	00:0c:29:2a:8e:b6	172.217.19.35 (o.pki.goog)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:37	192.168.10.10	00:0c:29:2a:8e:b6	104.17.161.40 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:36	192.168.10.10	00:0c:29:2a:8e:b6	104.17.161.40 (www.dating.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:07	192.168.10.10	00:0c:29:2a:8e:b6	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:45:06	192.168.10.10	00:0c:29:2a:8e:b6	5.226.179.10 (www.bet365.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:44:23	192.168.10.10	00:0c:29:2a:8e:b6	216.58.211.206 (google.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:44:18	192.168.10.10	00:0c:29:2a:8e:b6	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:26:51	192.168.10.10	00:0c:29:2a:8e:b6	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:26:02	192.168.10.10	00:0c:29:2a:8e:b6	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 11:15:59	192.168.10.10	00:0c:29:2a:8e:b6	142.250.201.35 (mrs08s20-in-f3.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:52:05	192.168.10.10	00:0c:29:2a:8e:b6	142.250.201.46 (mrs08s20-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:51:59	192.168.10.10	00:0c:29:2a:8e:b6	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:49:54	192.168.10.10	00:0c:29:2a:8e:b6	34.107.221.82 (detectportal.firefox.com)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:47:51	192.168.10.10	00:0c:29:2a:8e:b6	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)
2025/11/26 10:47:51	192.168.10.10	00:0c:29:2a:8e:b6	142.250.200.238 (mrs08s18-in-f14.1e100.net)	HTTP	Deny (Deny: UTM Blocked)	Kali_Internet_Access_with_Filter (1)

Forward Traffic Logs: Logs filtered by the firewall policy, showing HTTP sessions from the source IP (e.g., 192.168.10.10) resulting in a **Deny (Deny: UTM Blocked)** action, confirming that the Antivirus profile successfully detected and blocked the test file EICAR).



Date/Time		Source	Device	Destination	Application Name	Result
2025/11/26 10:26:51		10.0.11.50		100.65.0.254	HTTP	Deny (Deny; UM Blocked)
2025/11/26 10:24:41		10.0.11.50		100.65.0.254	HTTP	Deny (Deny; UTM Blocked)
2025/11/26 10:23:42		100.65.0.101		34.117.188.166 (spocs.getpocket.com)	HTTPS	✓ Accept (1.06 kB / 3.38 kB)
2025/11/26 10:23:42		100.65.0.101		34.110.138.217 (merino.services.mozilla.com)	HTTPS	✓ Accept (1.06 kB / 3.42 kB)
2025/11/26 09:31:26		10.0.11.50		100.65.0.254	FTP	✓ Accept (1.82 kB / 1.73 kB)
2025/11/26 09:31:08		10.0.11.50		100.65.0.254	tcp/45809	Deny (Deny: UTM Blocked)
2025/11/26 09:31:08		10.0.11.50		100.65.0.254	tcp/6467	Deny (Deny: UTM Blocked)
2025/11/26 09:31:03		10.0.11.50		100.65.0.254	tcp/50796	Deny (Deny: UTM Blocked)

Log Details

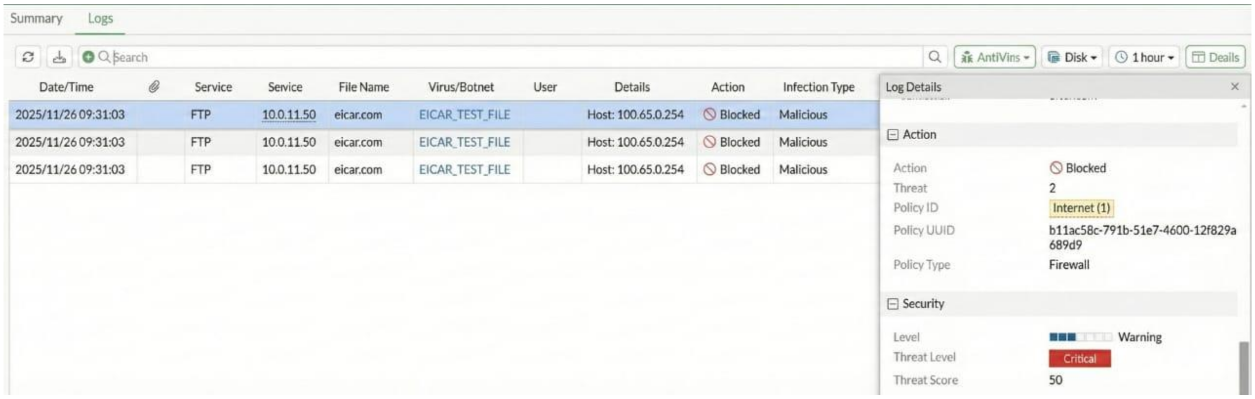
Details Security

Agent	Mozilla/5.0 (X11; Ubuntu: Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
Submitted to FortiSandbox	false
Direction	incoming
Destination UUID	7bcb7d34-7916-51e7-3d5b-71812a61b98e
Detectin Type	cached
Log evenc origial timestamp	1,732,645,609,813,322,200
HTTP request method	GET

⊟ Security

Level	■■■□□□□ Warning
Threat Level	Critical
Threat Score	50

Log Detail View: Detailed view of a blocked session, confirming the action was taken by the **AntiVirus** security profile due to a detected threat (Virus: EICAR_TEST_FILE), consistent with the security policy.



Date/Time		Service	Service	File Name	Virus/Botnet	User	Details	Action	Infection Type
2025/11/26 09:31:03		FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	Blocked	Malicious
2025/11/26 09:31:03		FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	Blocked	Malicious
2025/11/26 09:31:03		FTP	10.0.11.50	eicar.com	EICAR_TEST_FILE		Host: 100.65.0.254	Blocked	Malicious

Log Details

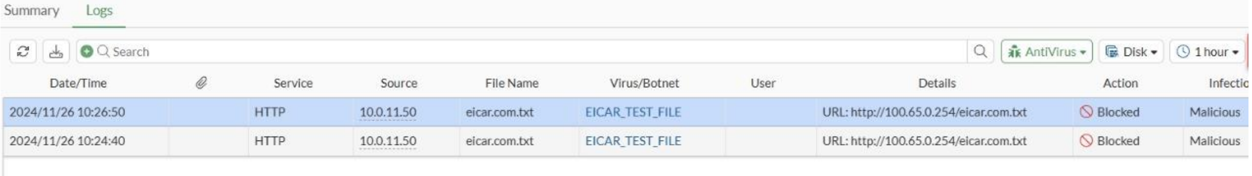
⊟ Action

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

⊟ Security

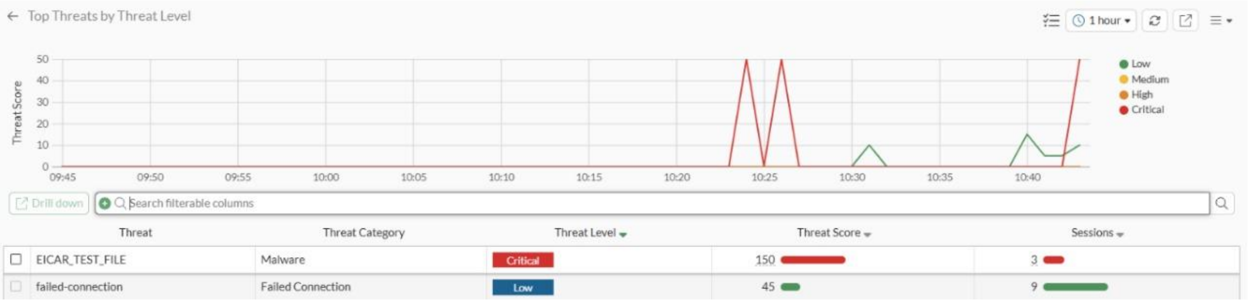
Level	■■■□□□□ Warning
Threat Level	Critical
Threat Score	50

Security Events Summary: Antivirus events dashboard highlighting **Blocked** actions recorded under the 'Virus' category, demonstrating active protection against malware downloads.



Date/Time		Service	Source	File Name	Virus/Botnet	User	Details	Action	Infectio
2024/11/26 10:26:50		HTTP	10.0.11.50	eicar.com.txt	EICAR_TEST_FILE		URL: http://100.65.0.254/eicar.com.txt	Blocked	Malicious
2024/11/26 10:24:40		HTTP	10.0.11.50	eicar.com.txt	EICAR_TEST_FILE		URL: http://100.65.0.254/eicar.com.txt	Blocked	Malicious

FortiView Threats: Dashboard view showing the attempted access to malicious files (identified as EICAR Test File) from the source device, which were subsequently blocked by the applied Antivirus policy.



	Threat	Threat Category	Threat Level	Threat Score	Sessions
□	EICAR_TEST_FILE	Malware	Critical	150	3
□	failed-connection	Failed Connection	Low	45	9

Conclusion:

Monitoring and reporting are critical for maintaining a secure, well-managed network environment. Through the configuration and use of FortiGate's monitoring tools, administrators gain real-time visibility into threats, user activity, and the behavior of security profiles. The reports generated during this phase provide valuable insights into the effectiveness of Antivirus, Web Filtering, and Application Control, enabling informed decisions and timely responses to emerging risks.

By completing the monitoring and reporting tasks outlined in this document, the organization strengthens its ability to detect threats early, respond efficiently, and maintain a proactive security posture. These capabilities form a key part of ongoing security management and support the long-term reliability of the network.