



RepLog Implementation Guide

Keyword Firewall Requirements

With RepLog 2.0 additional search strings can be detected using App Control the instructions enclosed cover all the setup required to enable RepLog, if you are an existing RepLog customer you will only have to complete the App Control section, but you may wish to review all the steps to ensure your configuration matches.

Switchshop recommend using FortiOS version 7.6 for RepLog, other versions are supported.

The following profiles must be configured and then applied to all user traffic policies.

- Web filter - In proxy mode with keyword logging enabled
- App Control **NEW** – Overrides added and monitored for keyword detection
- Antivirus – Compromised endpoint detection
- Intrusion Prevention – Optional, additional compromised endpoint detection
- SSL Inspection - With deep packet inspection enabled

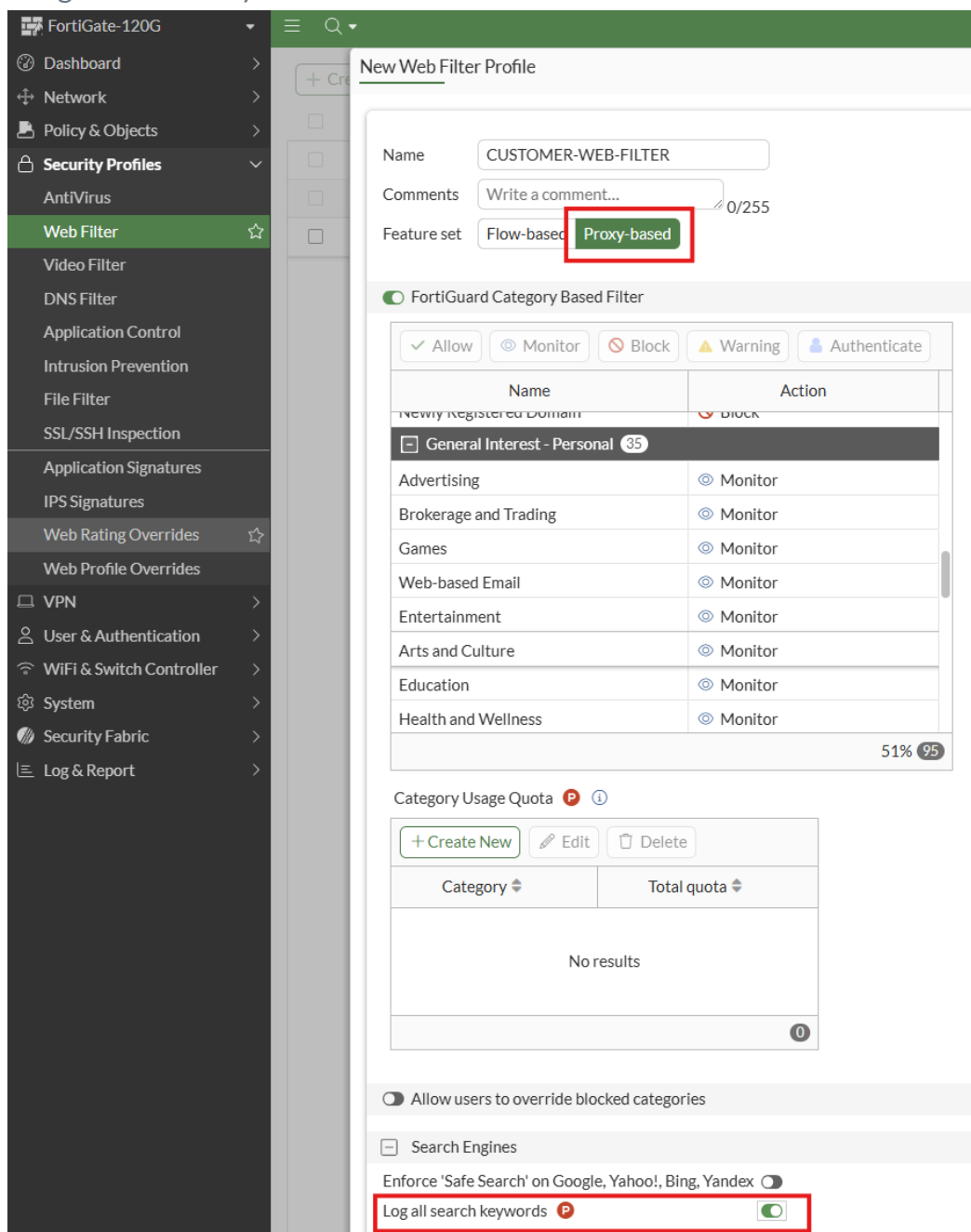
Web Filter Setup – Keyword Detection

On sub 2Gb RAM models proxy mode will be unavailable after upgrading to v7.4.4 and v7.6.0 and therefore keyword logging will be unavailable on these hardware models. Contact Switchshop if you have these models for further discussion.

Create a new web filter profile or customise your existing profiles. The profile should then be applied to all user policies going to the internet.

Enable the following

- Feature set – Proxy-based
- Log all search keywords - enable



FortiGate-120G

Dashboard > Network > Policy & Objects > Security Profiles > Web Filter > Video Filter > DNS Filter > Application Control > Intrusion Prevention > File Filter > SSL/SSH Inspection > Application Signatures > IPS Signatures > Web Rating Overrides > Web Profile Overrides > VPN > User & Authentication > WiFi & Switch Controller > System > Security Fabric > Log & Report >

New Web Filter Profile

Name: CUSTOMER-WEB-FILTER

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

☒ FortiGuard Category Based Filter

Name	Action
Newly registered Domain	Block
General Interest - Personal 35	
Advertising	Monitor
Brokerage and Trading	Monitor
Games	Monitor
Web-based Email	Monitor
Entertainment	Monitor
Arts and Culture	Monitor
Education	Monitor
Health and Wellness	Monitor

51% 95

Category Usage Quota

Category	Total quota
No results	

0

☐ Allow users to override blocked categories

☐ Search Engines

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

Log all search keywords ☒

Web Filter Cont.

- Set all categories actions appropriately, for allowed categories set the action to **monitor** for blocked categories set to **block**

Make sure categories are not set to allow, as traffic will not be logged, and no alerting will occur.

New Web Filter Profile

Name

CUSTOMER-WEB-FILTER

Comments

Write a comment... 0/255

Feature set

Flow-based Proxy-based

☒ FortiGuard Category Based Filter

✓ Allow

👁 Monitor

🚫 Block

⚠ Warning

👤 Authenticate

Name	Action
Newly registered Domain	🚫 Block
[-] General Interest - Personal 35	
Advertising	👁 Monitor
Brokerage and Trading	👁 Monitor
Games	👁 Monitor
Web-based Email	👁 Monitor
Entertainment	👁 Monitor
Arts and Culture	👁 Monitor
Education	👁 Monitor
Health and Wellness	👁 Monitor

51% 95

Application Control – Keyword Detection **NEW**

Create a new application control profile or customise your existing profiles. The profile should then be applied to all user policies going to the internet.

Enable the following

- Enable monitor for at least General Interest and Generative AI application categories.
- Create application overrides on version 7.2/7.4

7.6

FortiGate-120G

Dashboard > Network > Policy & Objects > Security Profiles > AntiVirus > Web Filter > Video Filter > DNS Filter > **Application Control** > Intrusion Prevention > File Filter > SSL/SSH Inspection > Application Signatures > IPS Signatures > Web Rating Overrides > Web Profile Overrides > VPN > User & Authentication > WiFi & Switch Controller > System > Security Fabric > Log & Report >

New Application Sensor

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

Name: CUSTOMER-APPCTRL-PROFILE

Comments: 0/255

Categories

Mixed All Categories

☒ Business (157, ☁ 11)	☒ Cloud/IT (74, ☁ 2)
☒ Collaboration (248, ☁ 15)	☒ Email (77, ☁ 11)
☒ Game (93)	☒ General Interest (245, ☁ 11)
☒ Generative AI (61, ☁ 709)	☒ Mobile (3)
☒ Network Service (378)	☒ Operational Technology
☒ P2P (51)	☒ Proxy (186)
☒ Remote Access (112)	☒ Social Media (107, ☁ 27)
☒ Storage/Backup (157, ☁ 27)	☒ Update (49)
☒ Video/Audio (154, ☁ 16)	☒ VoIP (22)
☒ Web Client (21)	☒ Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

+ Create New Edit Delete

Application Control Cont.

7.4

If GenAI is not visible please upgrade to 7.4.11 and add an application control profile to a firewall policy, this will force the database to update within 15 minutes, alternatively run `execute update-now` from the firewall CLI.

Categories

 Mixed ▾ All Categories

 Business (156, ☁ 11)

 Collaboration (248, ☁ 15)

 Game (93)

 General Interest (244, ☁ 11)

 Network Service (378)

 P2P (52)

 Remote Access (111)

 Storage/Backup (156, ☁ 24)

 Video/Audio (153, ☁ 16)

 Web Client (21)

 Cloud/IT (74, ☁ 2)

 Email (77, ☁ 11)

 GenAI (30, ☁ 24)

 Mobile (3)

 Operational Technology

 Proxy (186)

 Social Media (108, ☁ 27)

 Update (49)

 VoIP (22)

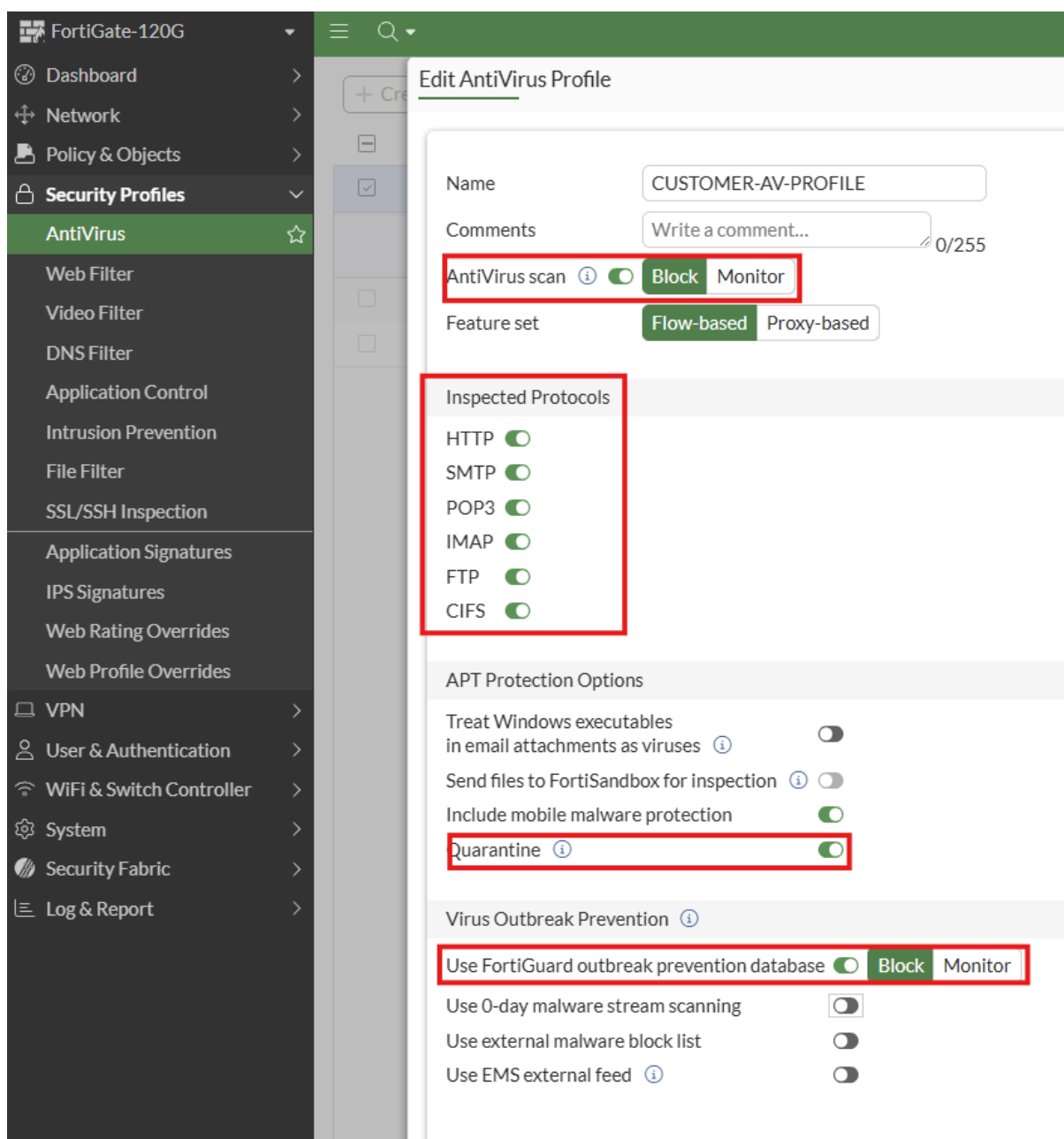
 Unknown Applications

Antivirus Setup - Compromised Endpoint Detection

Create a new antivirus profile or customise your existing profiles. The profile should then be applied to all user policies going to the internet.

Enable the following

- Feature set – Proxy-based
- AntiVirus Scan – Block
- Inspected protocols – all
- Content Disarm and Reconstruction – Enable
- Quarantine – Enable
- Use FortiGuard outbreak prevention database - Enable



Intrusion Prevention

Nothing is mandatory here check that the action for elements you want to protect against are set to block. **Monitor** / **Warning** / **Block** will result in a log which you will be alerted on.

Below is an example of an all purpose IPS profile that can be used, it's based off the built-in profile called "default" with packet logging enabled and Scan Outgoing Connections to Botnet sites set to **Block**.

The screenshot shows the FortiGate-120G web interface for configuring an IPS Sensor. The left sidebar lists various security features, with 'Intrusion Prevention' selected. The main panel is titled 'Clone IPS Sensor' and shows the configuration for a sensor named 'CUSTOMER-IPS-PROFILE'. The 'Name' field is 'CUSTOMER-IPS-PROFILE', the 'Comments' field is 'Prevent critical attacks.', and the 'Block malicious URLs' toggle is turned on. Below this is the 'IPS Signatures and Filters' section, which contains a table with columns for 'Details', 'Exempt IPs', 'Action', and 'Packet Logging'. The table has three rows, each representing a signature. The first row shows a signature with a severity of 'SEV' and a status of 'Enabled'. The 'Packet Logging' column for this row is set to 'Enabled'. The 'Botnet C&C' section at the bottom shows the 'Scan Outgoing Connections to Botnet Sites' toggle set to 'Block'. A status bar at the bottom indicates '3567 IP Addresses in botnet package.'

Details	Exempt IPs	Action	Packet Logging
SEV		Default	Enabled
SEV			
SEV			

Generic Deep SSL Inspection - Needed for Everything to Work

SSL deep inspection enables the inspection of encrypted HTTPS packets sent from clients to the internet, to do this a trusted CA certificate issued by the FortiGate needs to be installed onto all devices to enable them to be decrypted

Beware that enabling this without installing the CA certificate in the screenshot on all devices subject to SSL inspection will cause endpoint devices to present certificate warnings to your users and in some cases break application functionality. It is recommended that you log SSL anomalies to be able to diagnose SSL inspection errors.

You should deploy this CA certificate into the trusted root store on your managed devices through group policy, Intune, GSuite, or other management platform. If you have a bring your own device network, in order to get your CA certificate on students / employees' phones, we recommend our certificate onboarding service MySSP-Onboard which provides steps for a range of devices by detecting what browser and system they're using. You can view an example of it here:
<https://certificate.switchshop.co.uk>

Deep SSL Inspection Cont.

FortiGate-120G

Dashboard > Network > Policy & Objects > Security Profiles > AntiVirus > Web Filter > Video Filter > DNS Filter > Application Control > Intrusion Prevention > File Filter > **SSL/SSH Inspection** > Application Signatures > IPS Signatures > Web Rating Overrides > Web Profile Overrides > VPN > User & Authentication > WiFi & Switch Controller > System > Security Fabric > Log & Report >

Clone SSL/SSH Inspection Profile

Name: CUSTOMER-DEEP-INSPECTION-PROF

Comments: Write a comment... 0/255

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](#)

Malicious certificates: Allow Block View malicious certificate definitions

Untrusted SSL certificates: Allow Block Ignore View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

Enforce SSL cipher compliance: ☐

Enforce SSL negotiation compliance: ☐

RPC over HTTPS: ☐

MAPI over HTTPS: ☐

Protocol Port Mapping

Inspect all ports: ☐

HTTPS: ☒ 443

SMTPS: ☒ 465

POP3S: ☒ 995

IMAPS: ☒ 993

FTPS: ☒ 990

DNS over TLS: ☐ 853

HTTP/3: Inspect Bypass Block

DNS over QUIC: Inspect Bypass Block

Exempt from SSL Inspection

Reputable websites: ☐

Web categories: Finance and Banking Health and Wellness +

Addresses: adobe

Remove Microsoft or Bing from here

Example Policy Which Implements the Security Profiles

Ensure the policy uses the security profiles you've configured as above.

FortiGate-120G

Policy & Objects

- Dashboard
- Network
- Policy & Objects**
- Firewall Policy
- Local-In Policy
- Authentication
- Addresses
- ZTNA
- Internet Service Database
- Services
- Schedules
- Virtual IPs
- IP Pools
- Protocol Options
- Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- System
- Security Fabric
- Log & Report

Edit Policy

Name: Student Internet

Schedule: always

Action: ☒ ACCEPT ☐ DENY

Type: Standard ZTNA

Incoming interface: LAN Zone

Outgoing interface: WAN Zone

Source & Destination Show logic

Source: all

User/group: **Student Users**

Security posture tag: ☐

Destination: all

Service: ALL

Firewall/Network Options

Inspection mode: Flow-based Proxy-based

NAT: ☒

IP pool configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Source port translation: Always When port conflicts Never

Protocol options: PROT default

Security Profiles

Continued on next page.

FortiGate-120G

- Dashboard
- Network
- Policy & Objects
 - Firewall Policy
 - Local-In Policy
 - Authentication
 - Addresses
 - ZTNA
 - Internet Service Database
 - Services
 - Schedules
 - Virtual IPs
 - IP Pools
 - Protocol Options
 - Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- WiFi & Switch Controller
- System
- Security Fabric
- Log & Report

Edit Policy

Source & Destination Show logic

User/group: Student Users

Security posture tag: ☐

Destination: all

Service: ALL

Firewall/Network Options

Inspection mode: Flow-based Proxy-based

NAT: ☒

IP pool configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Source port translation: Always When port conflicts Never

Protocol options: PROT default

Security Profiles

AntiVirus: ☒ AV CUSTOMER-AV-PROFILE

Web filter: ☒ WEB CUSTOMER-WEB-FILTER

DNS filter: ☐

Application control: ☒ APP CUSTOMER-APPCTRL-PROFI...

IPS: ☒ IPS CUSTOMER-IPS-PROFILE

File filter: ☐

SSL inspection: ☒ SSL CUSTOMER-DEEP-INSPECTI...

Decrypted traffic mirror: ☐

Logging Options

Log allowed traffic: ☒ Security events All sessions

Comments: 0/1023

Enable this policy: ☒

Block QUIC

QUIC is a protocol that enables HTTPS over UDP in an effort to improve web browsing performance, as a by product it can bypass web filtering solutions on older version of FortiOS.

Blocking QUIC on older versions will cause apps to fall back to HTTPS on port TCP 443 instead of UDP 443 which allows the FortiGate to inspect the traffic. Newer versions have the ability to inspect QUIC traffic.

7.4 & 7.6

You can allow QUIC and inspect it in firmware 7.4 however this isn't recommended if you are not already on 7.4 or 7.6 firmware.

<https://docs.fortinet.com/document/fortigate/7.4.0/new-features/777101/enhancement-to-quic-and-http3-inspection-7-4-1>

7.2

In firmware 7.2 the toggle in application control to disabled QUIC was removed the configuration required now looks like the below.

<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/984075/remove-option-to-block-quic-by-default-in-application-control-7-2-4>

Application Control Configuration

Categories

Category	Count
Business	157
Email	76
Mobile	3
Proxy	189
Storage.Backup	150
VoIP	23
Cloud.IT	72
Game	83
Network.Service	338
Remote.Access	96
Update	48
Web.Client	24
Collaboration	266
General.Interest	253
P2P	55
Social.Media	113
Video/Audio	147
Unknown Applications	

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	QUIC	Application	Block

Options

- Block applications detected on non-default ports: ☐
- Allow and Log DNS Traffic: ☒
- Replacement Messages for HTTP-based Applications: ☒

7.0 or below

Use the toggle at the bottom of an application control profile or create a firewall rule above all policies (or at the level that will otherwise best serve you if QUIC is required for a reason specific to your site) that blocks QUIC.

The screenshot displays the Fortinet FortiGate web interface. On the left is a dark sidebar menu with the following items: CUSTOMER-DEMO-40F, Dashboard, Network, Policy & Objects (selected), Firewall Policy (highlighted with a star), Local In Policy, IPv4 DoS Policy, Proxy Policy, Authentication Rules, Addresses, ZTNA, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, System, Security Fabric, and Log & Report. The main content area is titled 'Edit Policy' and shows the configuration for a policy named 'Block-QUIC'. The configuration includes: Name: Block-QUIC; Type: Standard (selected) and ZTNA; Incoming Interface: Local VLANS; Outgoing Interface: virtual-wan-link; Source: all; IP/MAC Based Access Control: (empty); Destination: all; Schedule: always; Service: QUIC{UDP443}; Action: ACCEPT (checked) and DENY (unchecked). Below the configuration fields, there is a 'Log Violation Traffic' toggle (unchecked), a 'Comments' field with the text 'Write a comment...' and a character count of 0/1023, and an 'Enable this policy' toggle (checked).

Name	Block-QUIC
Type	Standard ZTNA
Incoming Interface	Local VLANS
Outgoing Interface	virtual-wan-link
Source	all
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	QUIC{UDP443}
Action	ACCEPT DENY

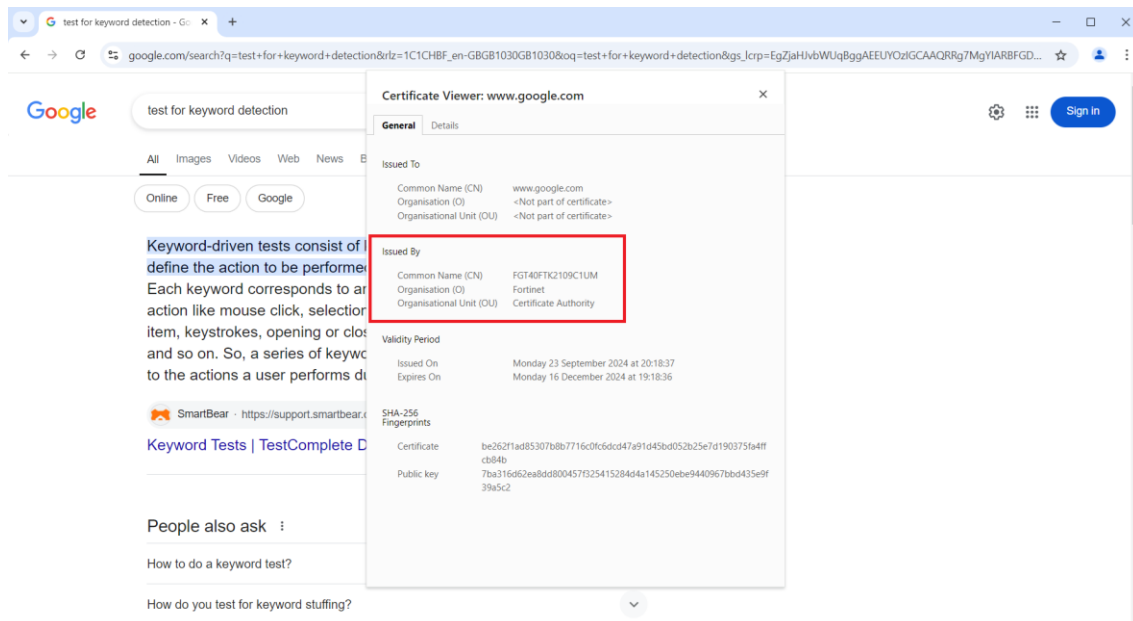
☐ Log Violation Traffic

Comments Write a comment... 0/1023

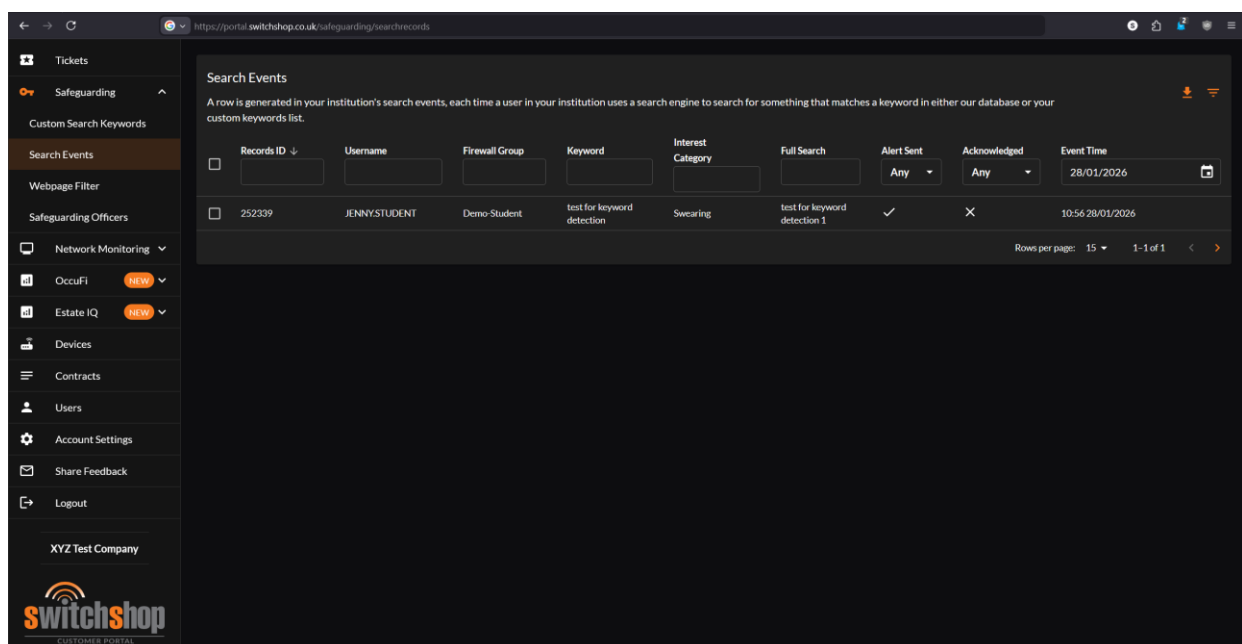
Enable this policy ☒

Verification

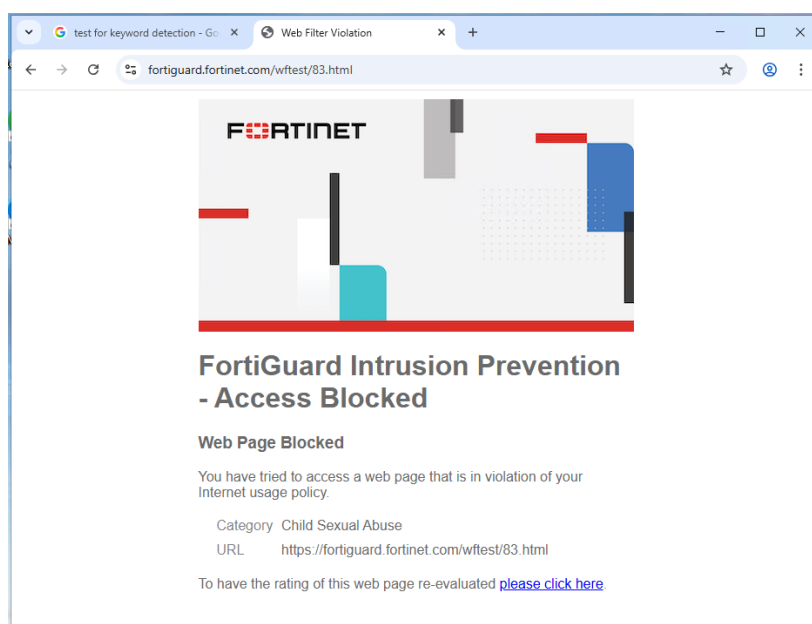
Ensure that you have setup the relevant settings across the security profiles logging to work correctly. You can further verify this by reviewing the certificate on a website such as google to confirm it is being deep packet inspected. Expect to see the certificate selected in the SSL Inspection profile.



Alerts for keywords can be tested by searching for the phrase “test for keyword detection” via Google, Bing, Yandex, Yahoo, or Baidu. Expect to receive an email alert and an entry in the [Switchshop Customer Portal](#) on the search records page if your service setup has been completed.



Alerts for website visit or visit attempts can be tested by going to: <https://www.fortiguard.com/webfilter/categories> and then clicking on one of the test links. We recommend testing the “Child Sexual Abuse” category which can be found in the “Potentially Liable” section lower down on the page.



Summary									
Logs									
Web Filter Memory Details									
Date/Time	User	Group	Source	Action	URL	Category	Initiator	Sent / Received	
2024/01/28 18:18:24	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	https://google-ohp-relay-safeforbusiness-fastly-edge.com/	Information Technology	3.026 kB / 526 B		
2024/01/28 18:18:24	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	⛔ Blocked	https://fortiguard.fortinet.com/wfext/83.html	Child Sexual Abuse	2.62 kB / 3.76 kB		
2024/01/28 18:18:21	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	https://www.google.com/completesearch/client/chrome-omni&campus=r1nchrome-ex-ang&sa...	Search Engines and Portals	3.256 kB / 129 B		
2024/01/28 18:18:21	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	https://assets.msn.com/weathertapdata/15static/weather/icons/MSA4Ww-a-ConditionAAeh...	Search Engines and Portals	1.09 kB / 5.5 kB		
2024/01/28 18:18:18	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	https://api.msn.com/v1/news/Trend/WindowsThrup...z0Y9P8Z0n0zJ6EFkYj...&appk...	Search Engines and Portals	2.776 kB / 6.43 kB		
2024/01/28 18:18:07	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	2.916 kB / 87.13 kB		
2024/01/28 18:18:03	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	2.941 kB / 40.46 kB		
2024/01/28 18:18:05	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	2.166 kB / 20.97 kB		
2024/01/28 18:18:05	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	1.79 kB / 10.13 kB		
2024/01/28 18:18:03	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	1.41 kB / 5.39 kB		
2024/01/28 18:18:03	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	10.4 kB / 2.42 kB		
2024/01/28 18:17:59	JENNYSTUDENT	Demo-Student	JENNYSTUDENT (172.19.250.4)	✓ Passthrough	http://edgedp.mt.gv1.com/edged1/release2/chrome_component/fpm7h3ymyzagzf7m5fvmr...	Information Technology	668 B / 627 B		

Tickets

Safeguarding

Custom Search Keywords

Search Events

Webpage Filter

Safeguarding Officers

Network Monitoring

OccuFi

Estate IQ

Devices

Contracts

Users

Account Settings

Share Feedback

Logout

XYZ Test Company



portal.switchshop.co.uk/safeguarding/touchrecords

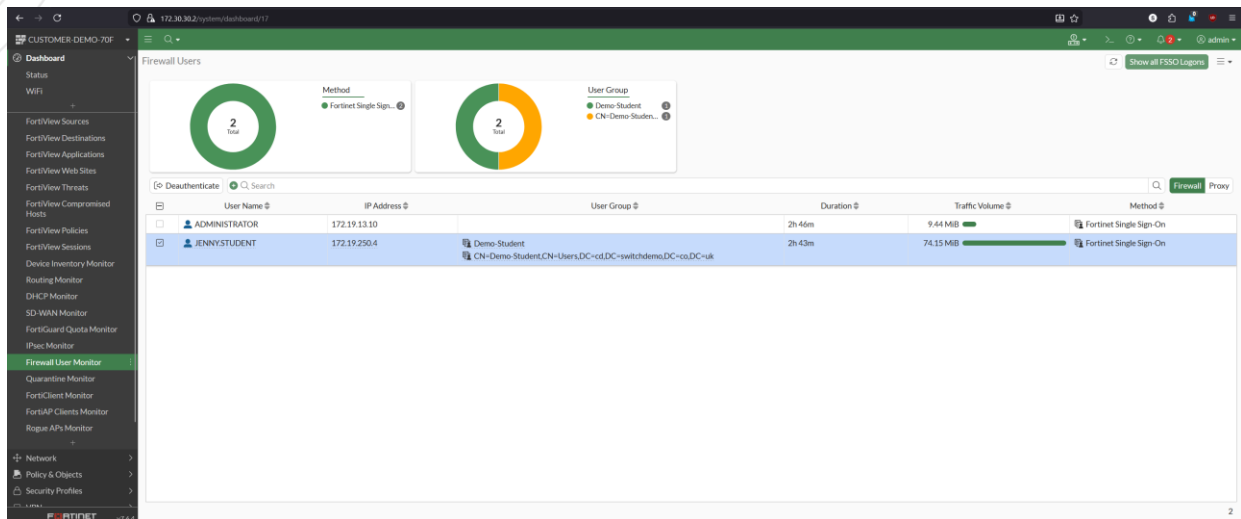
Webpage Filter

A row is generated in your institution's web filtered events each time a user in your institution accesses a domain that the service has categorised as sensitive. You can use change requests to add new web pages, domains or categories to your web filter service.

Event ID ↓	Username	Site	Event Type	Category	URL	Endpoint IP	Destination IP	Endpoint MAC	Firewall Group	Alert Acknowledged	Event Time	
☐										Any	28/01/2026	
☐	13588	JENNY-STUDENT	Main	Webfilter	Child Sexual Abuse	https://forfiguard4.fortinet.com/wftest/83.html	172.19.250.4	154.52.3.165	00:50:56:b3:34:38	Demo Student	☒	18:18:28/01/2026

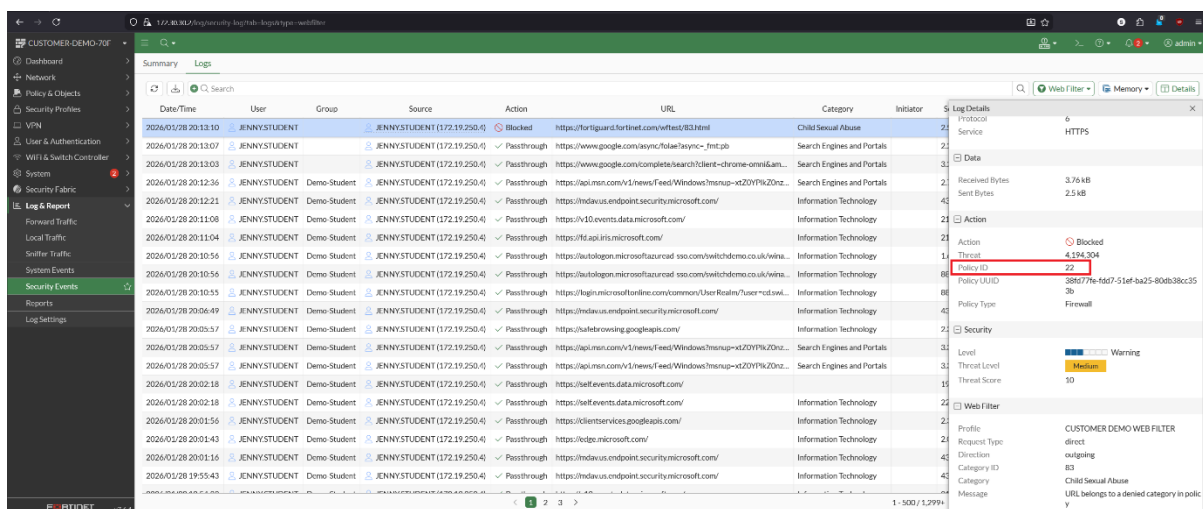
Rows per page: 151-1 of 1

Check the user table. If your user isn't in there with group information then you will need work on sign on integrations.



Missing Group Information?

Check that you've included the user group in the matched firewall policy.



Missing MAC Information?

The FortiGate will only report MAC addresses into logs if the devices are on directly connected networks.