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

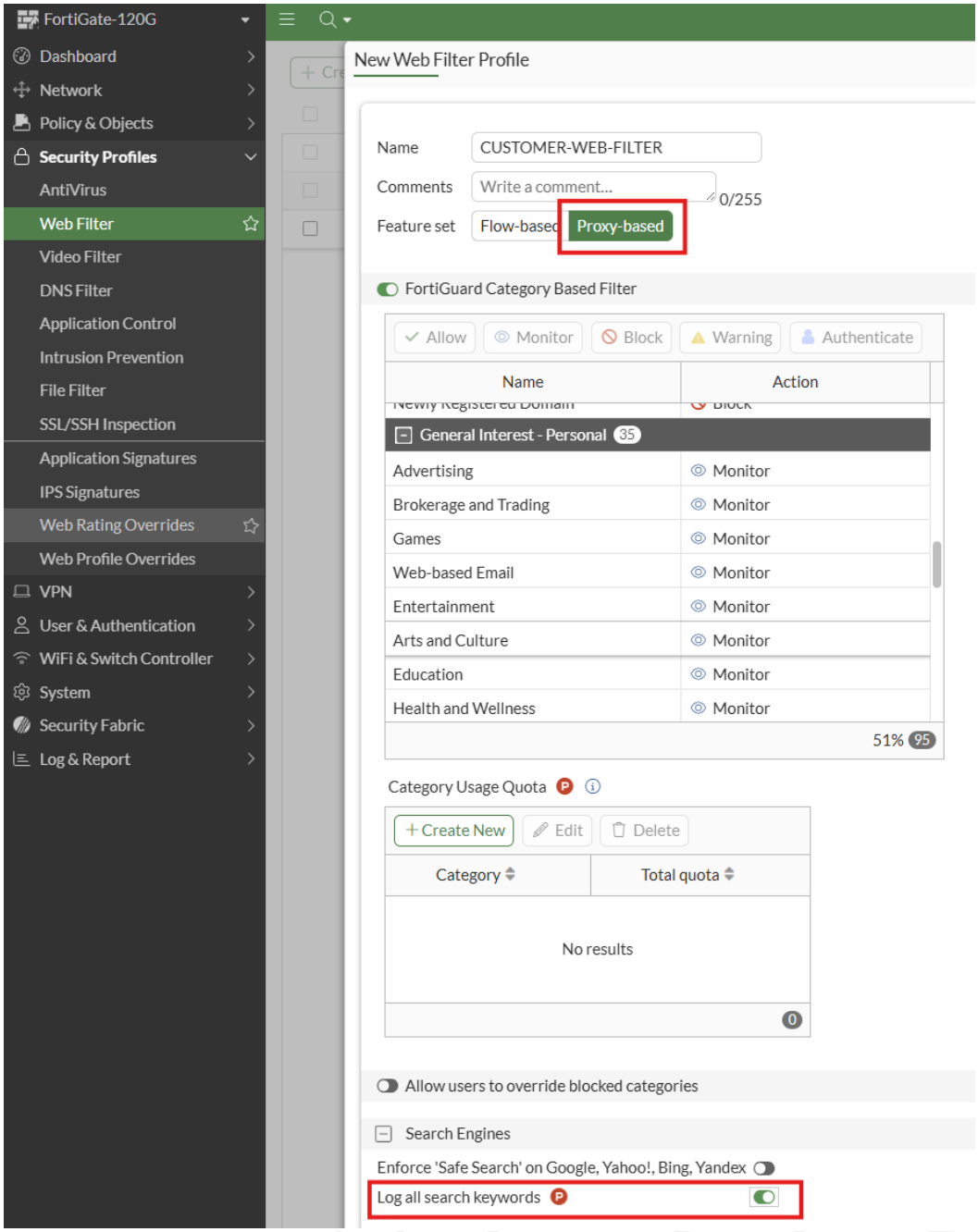
Web Filter Setup – Keyword Detection

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

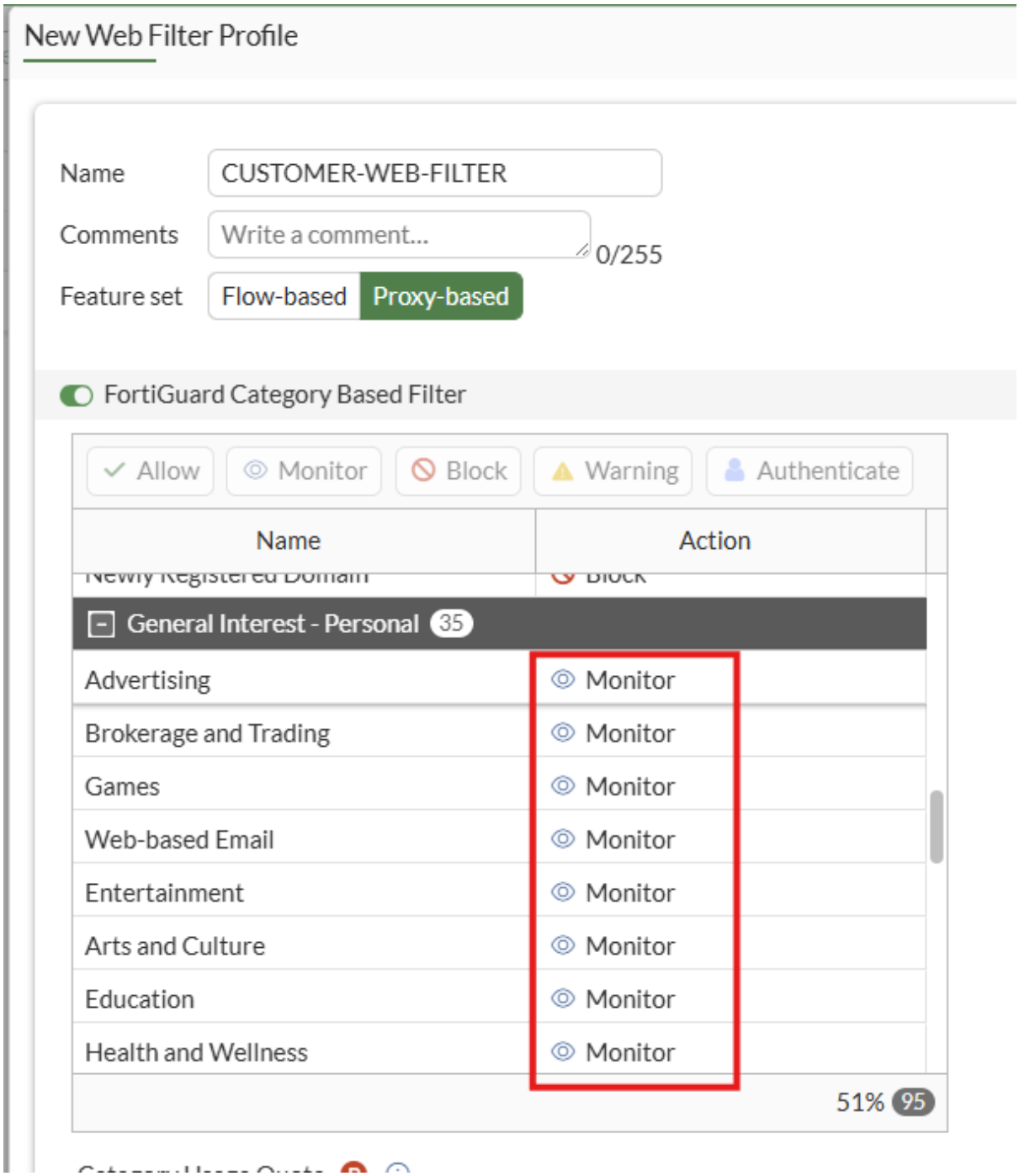
- Feature set – Proxy-based
- Log all search keywords - enable



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.



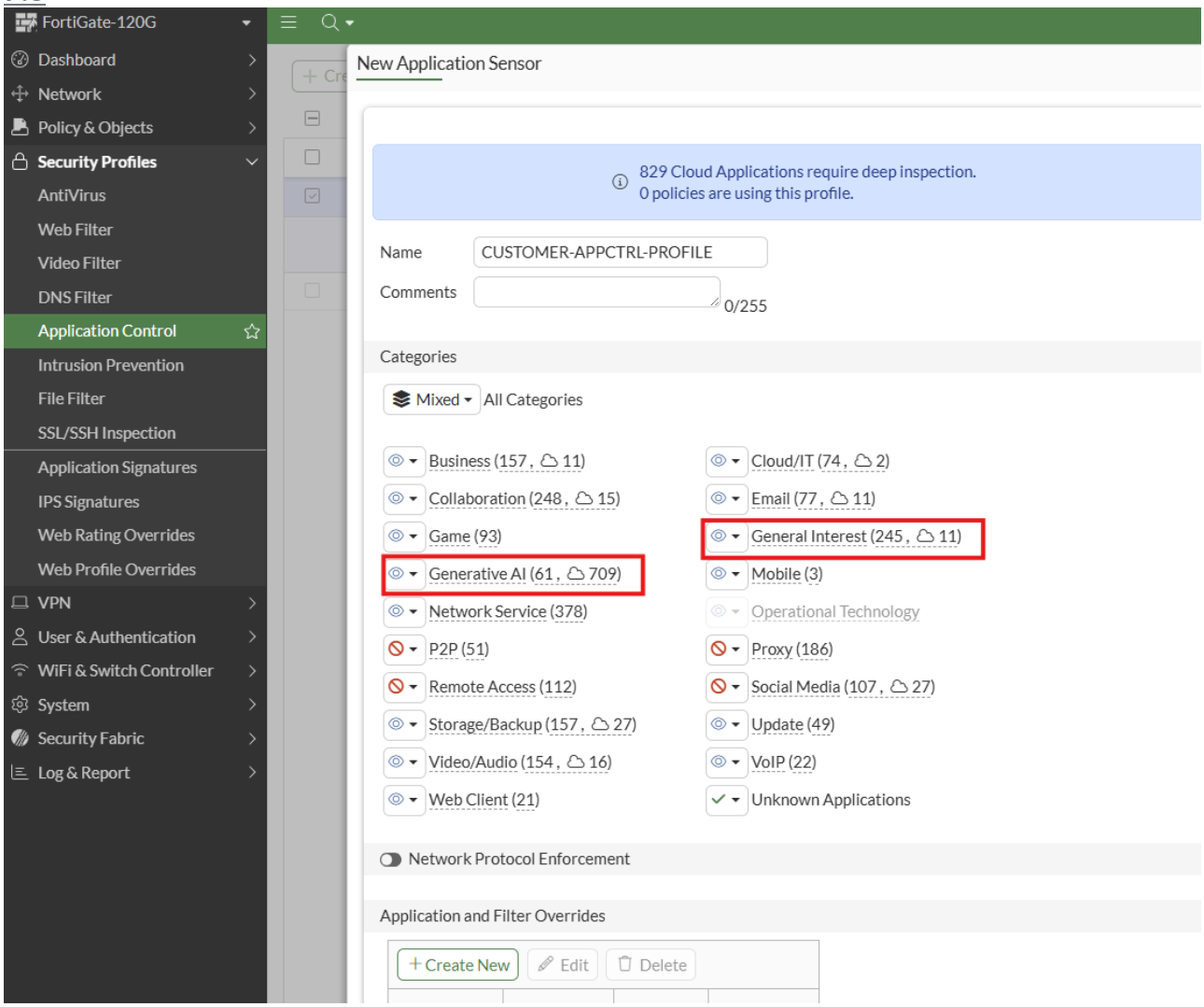
Application Control – Keyword Detection NEW

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

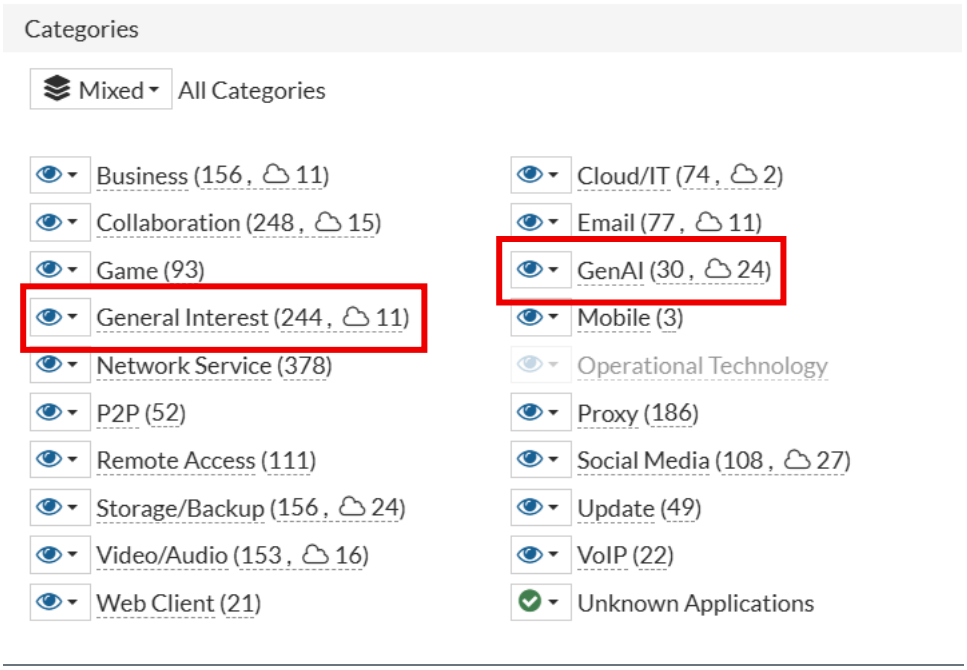
7.6



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.

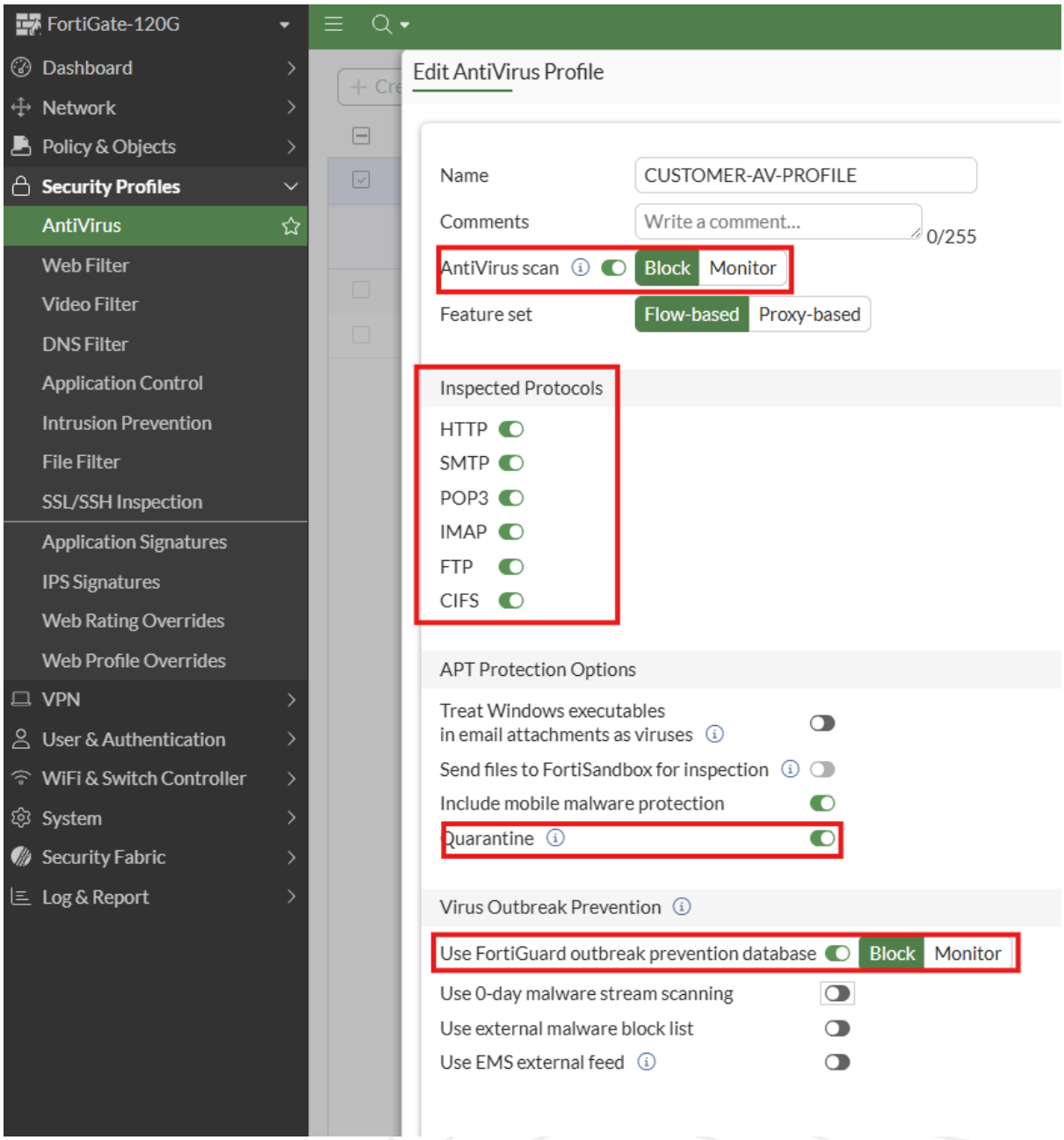


Antivirus Setup - Compromised Endpoint Detection

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

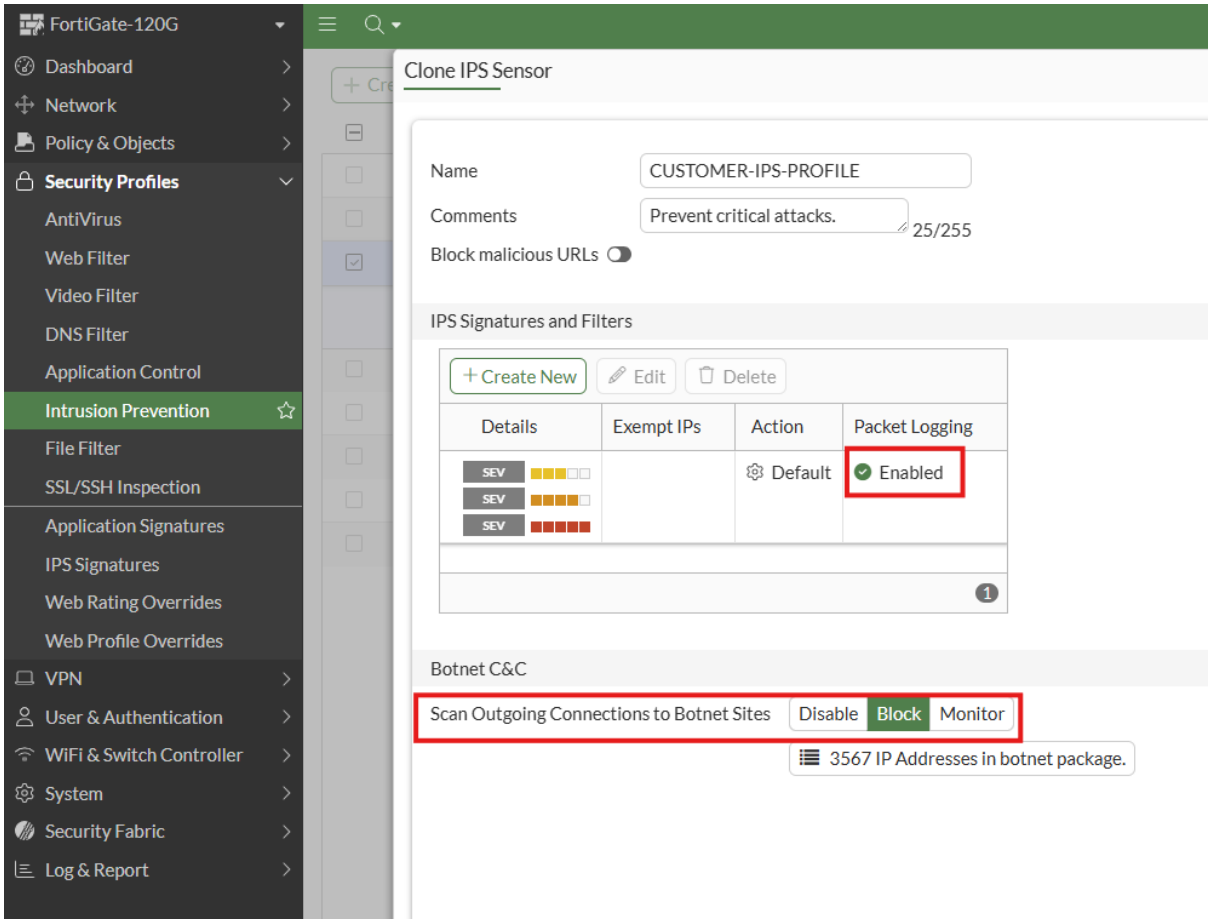
- Feature set – Proxy-based
- AntiVirus Scan – Block
- Inspected protocols – all
- Content Disarm and Reconstruction – Enable
- Quarantine – Enable
- Use FortiGuard outbreak prevention database - Enable



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**.



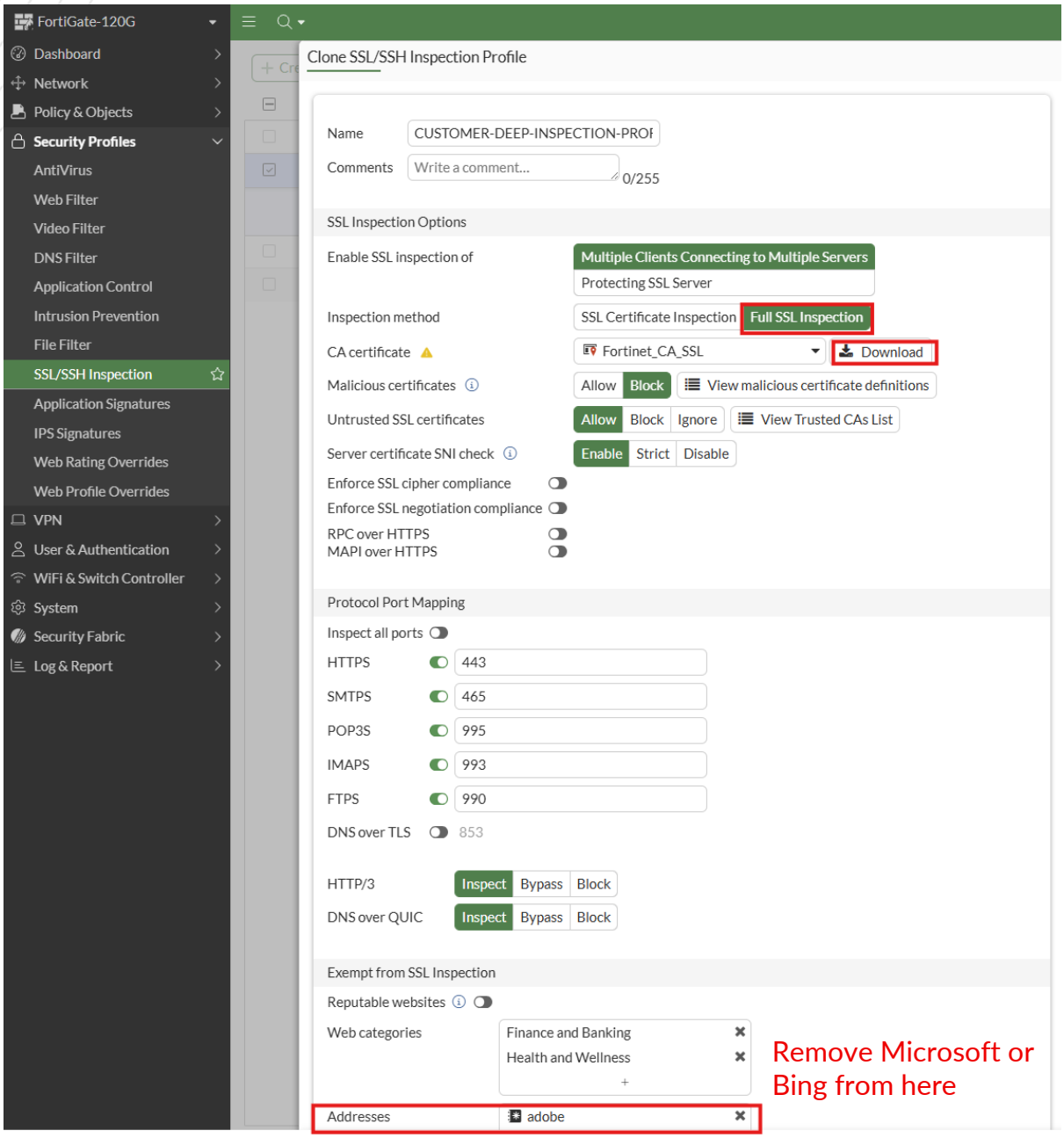
Generic Deep SSL Inspection - Needed for Everything to Work

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.

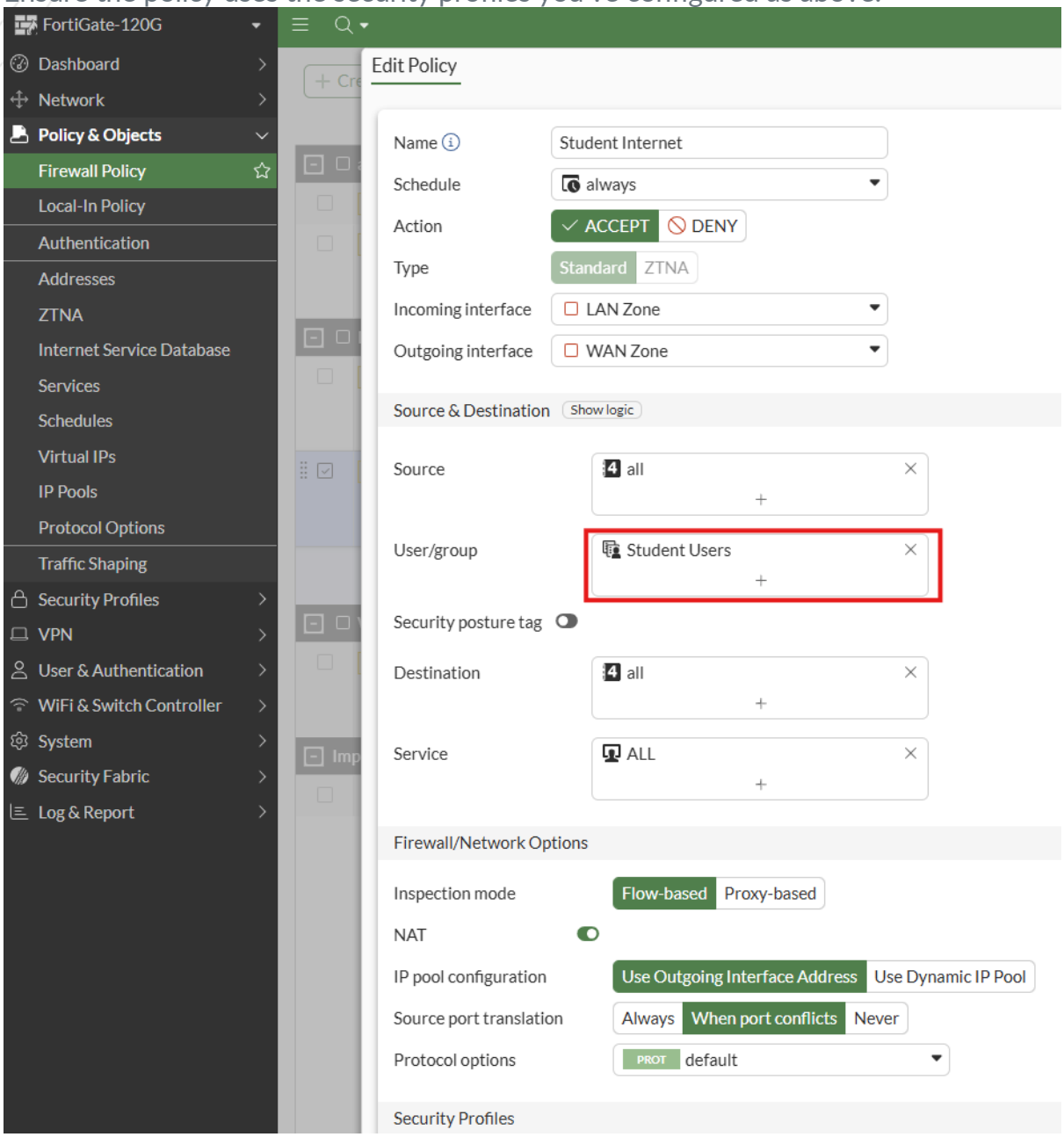
You should deploy this CA certificate into the trusted root store on your managed devices through group policy, Intune, GSuite, or other management platform. If you have a bring your own device network, in order to get your CA certificate on students / employees' phones, we recommend our certificate 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.

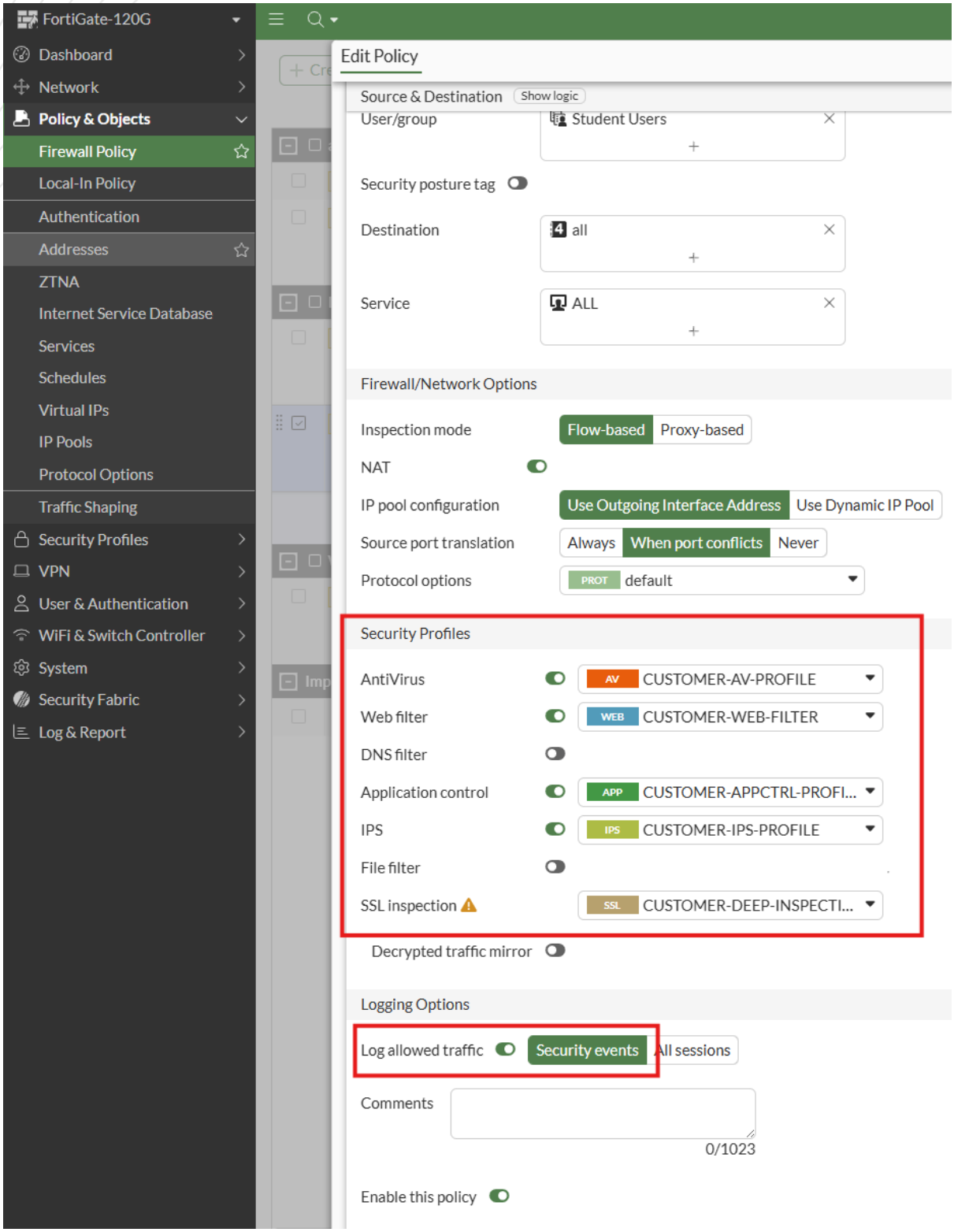


Example Policy Which Implements the Security Profiles

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



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.

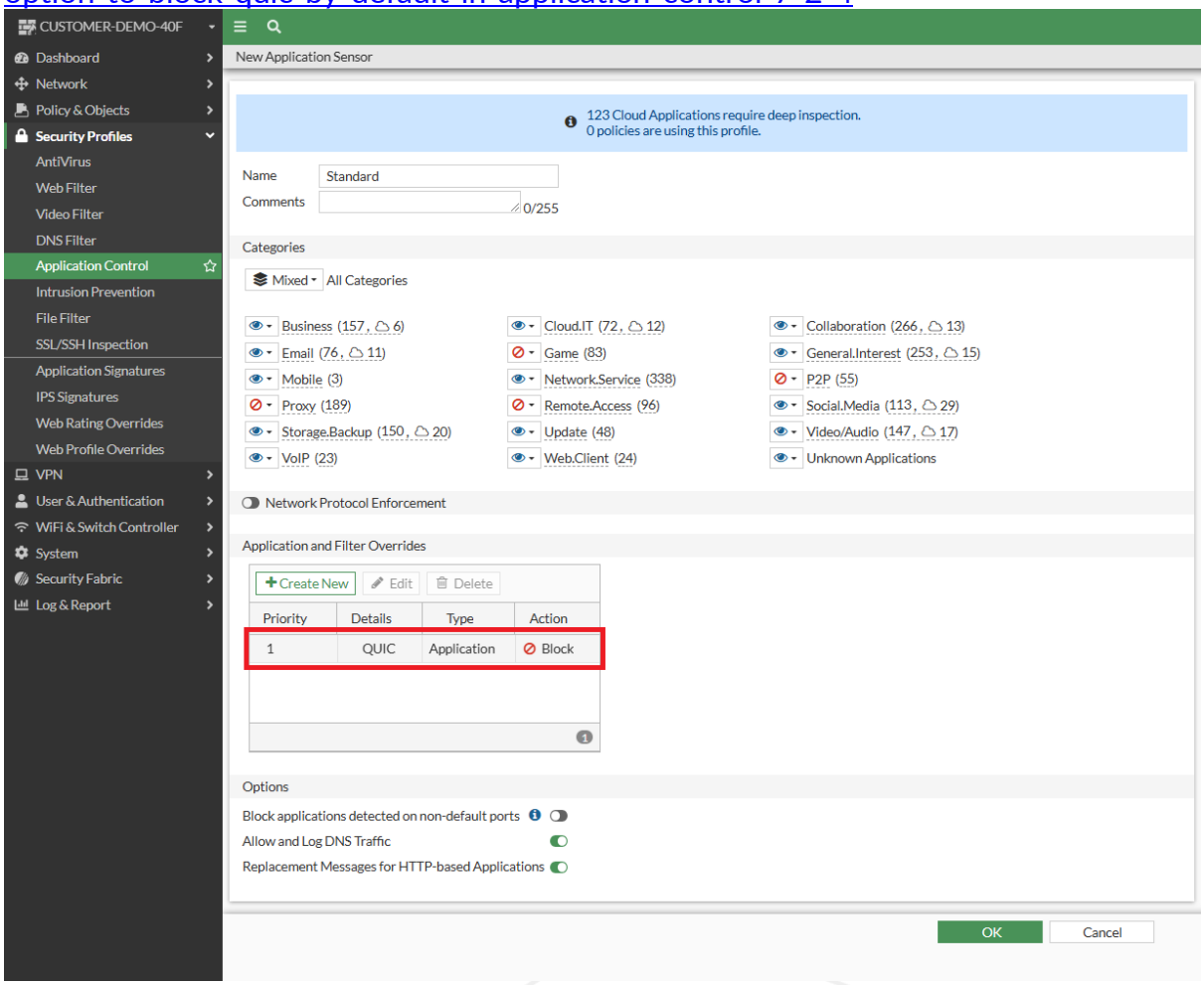
Blocking QUIC on older versions will cause apps to fall back to HTTPS on port TCP 443 instead of UDP 443 which allows the FortiGate to inspect the traffic. Newer versions have the ability to inspect QUIC traffic.

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

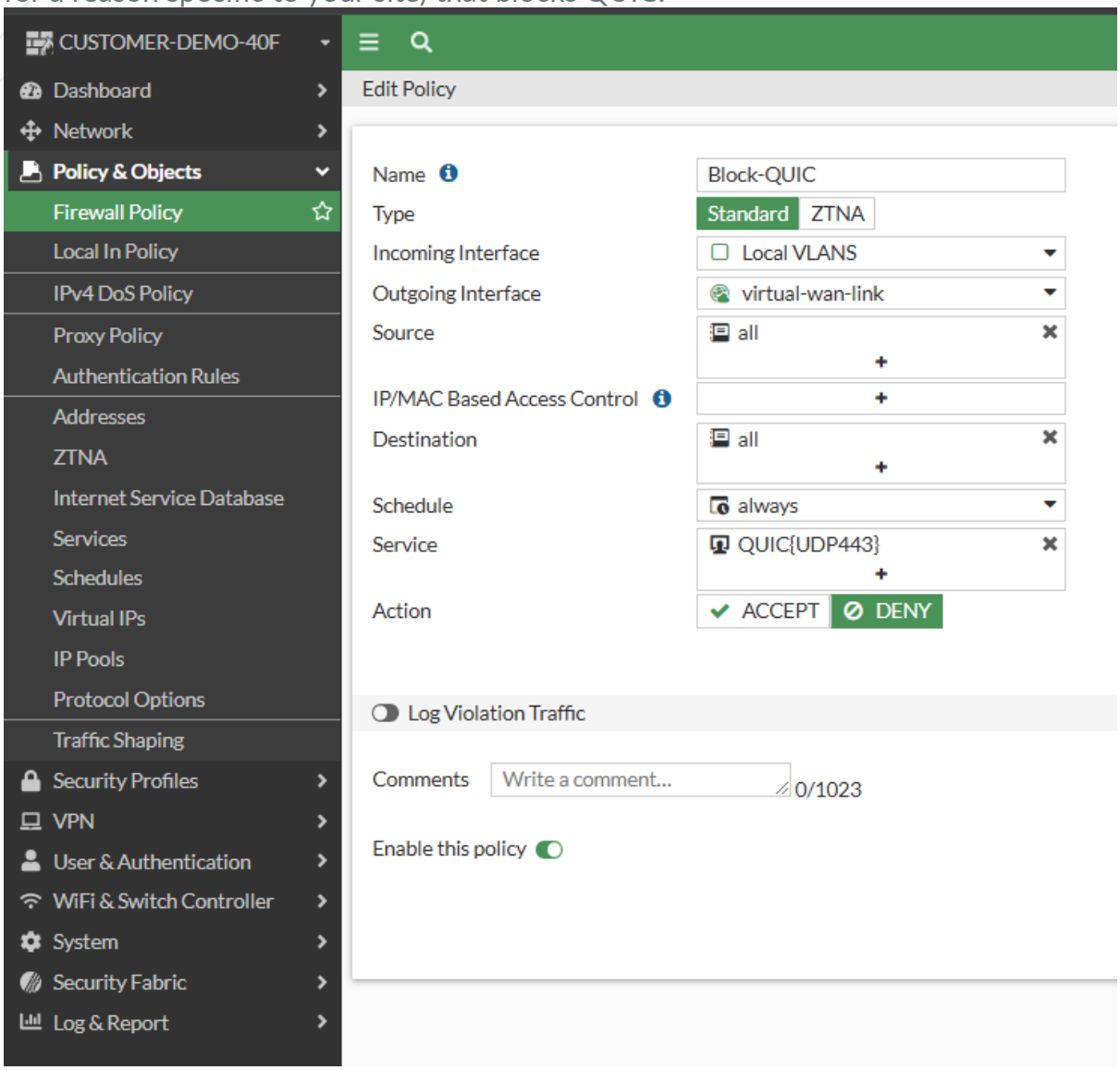
7.2

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



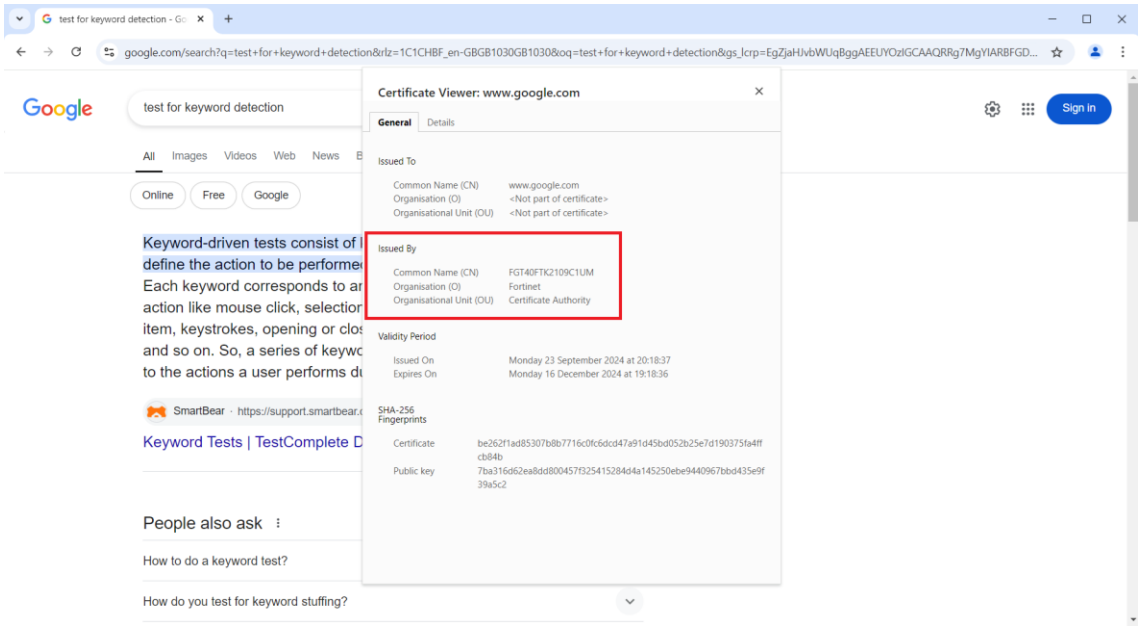
7.0 or below

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.

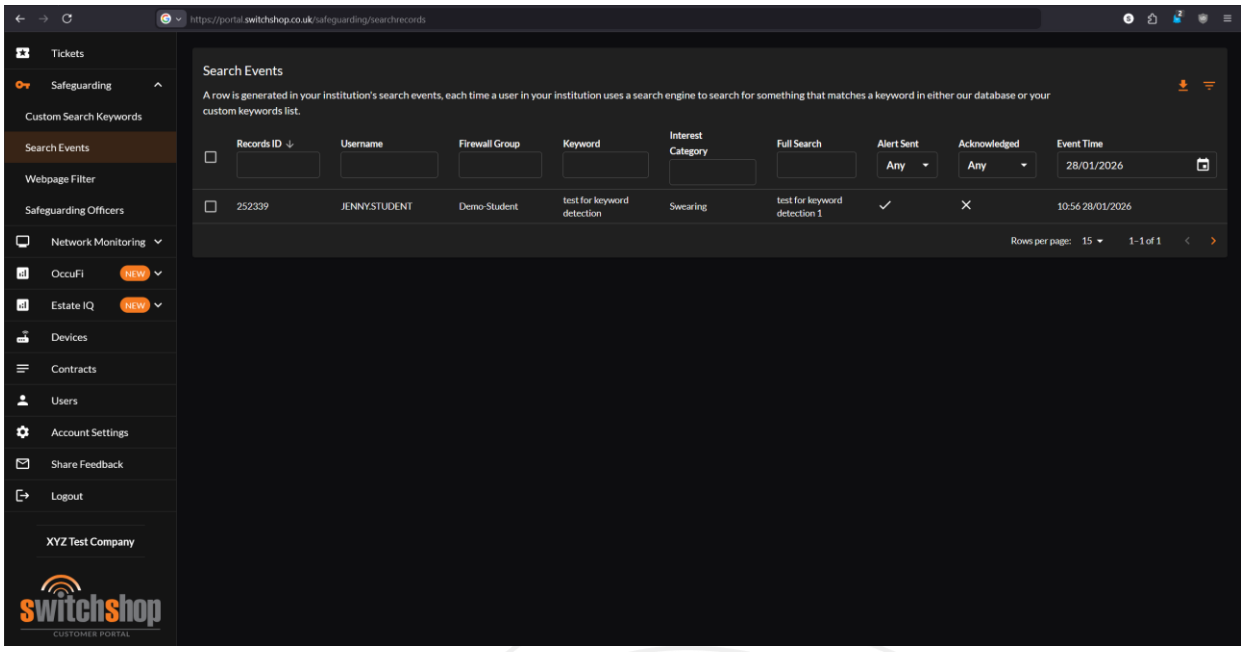


Verification

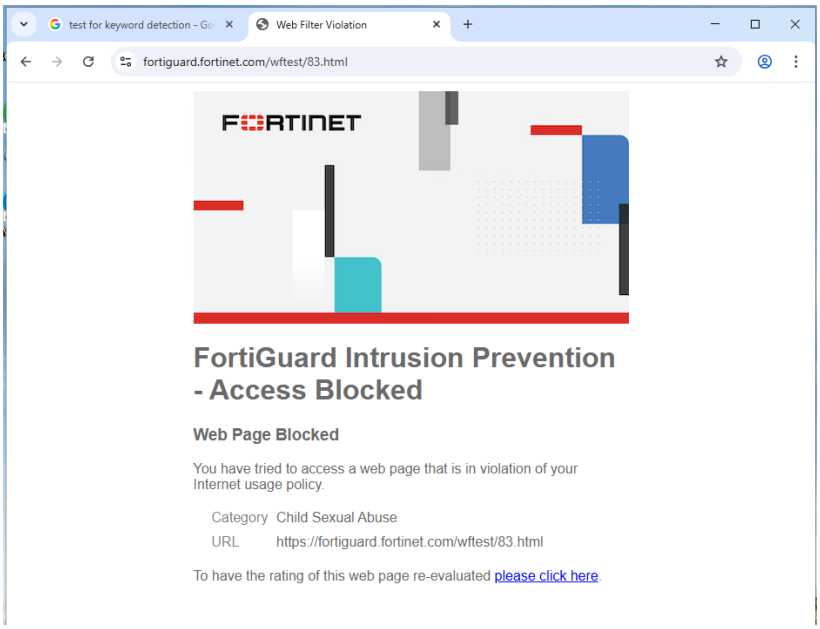
Ensure that you have setup the relevant settings across the security profiles logging to work correctly. You can further verify this by reviewing the certificate on a website such as google to confirm it is being deep packet inspected. Expect to see the certificate selected in the SSL Inspection profile.

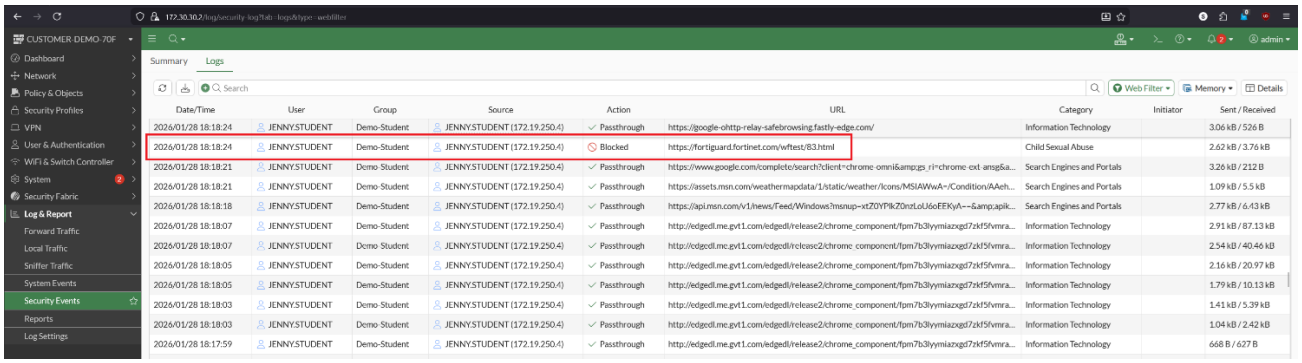


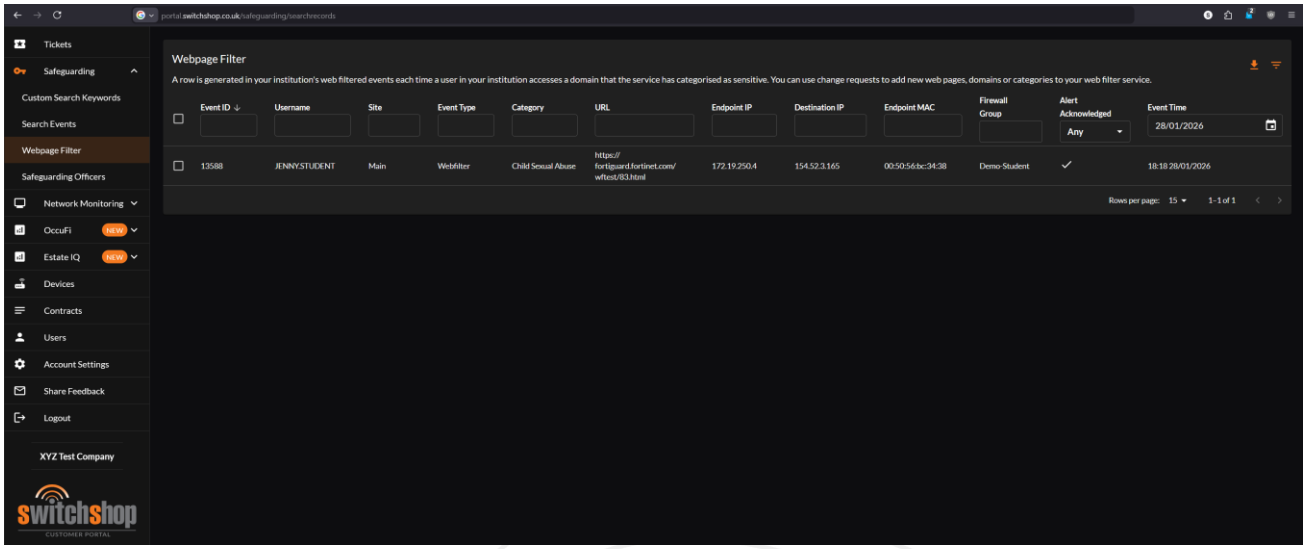
Alerts for keywords can be tested by searching for the phrase “test for keyword detection“ via Google, Bing, Yandex, Yahoo, or Baidu. Expect to receive an email alert and an entry in the [Switchshop Customer Portal] on the search records page if your service setup has been completed.



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.

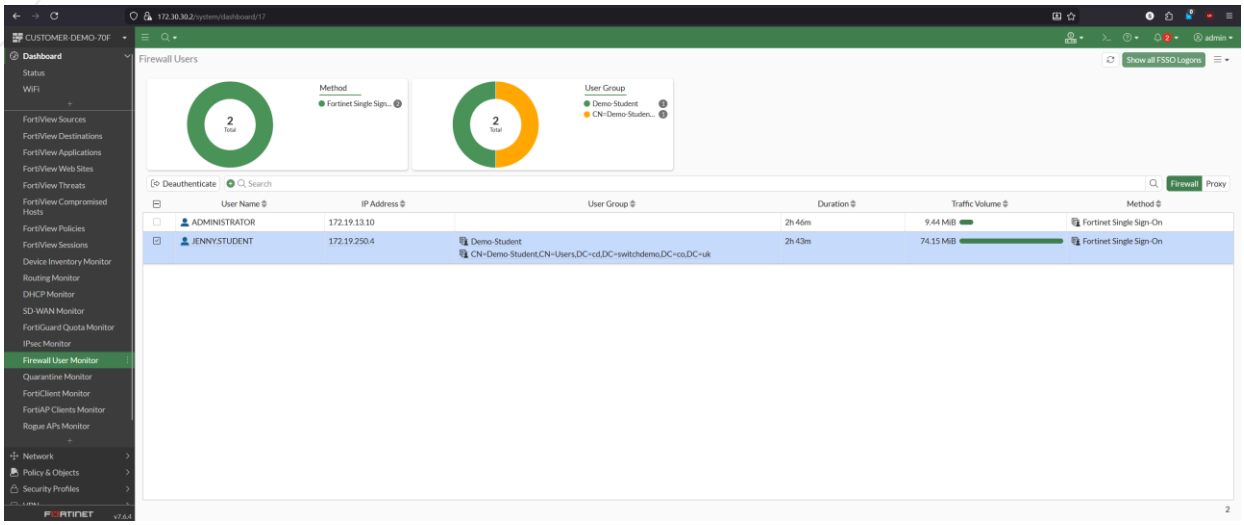






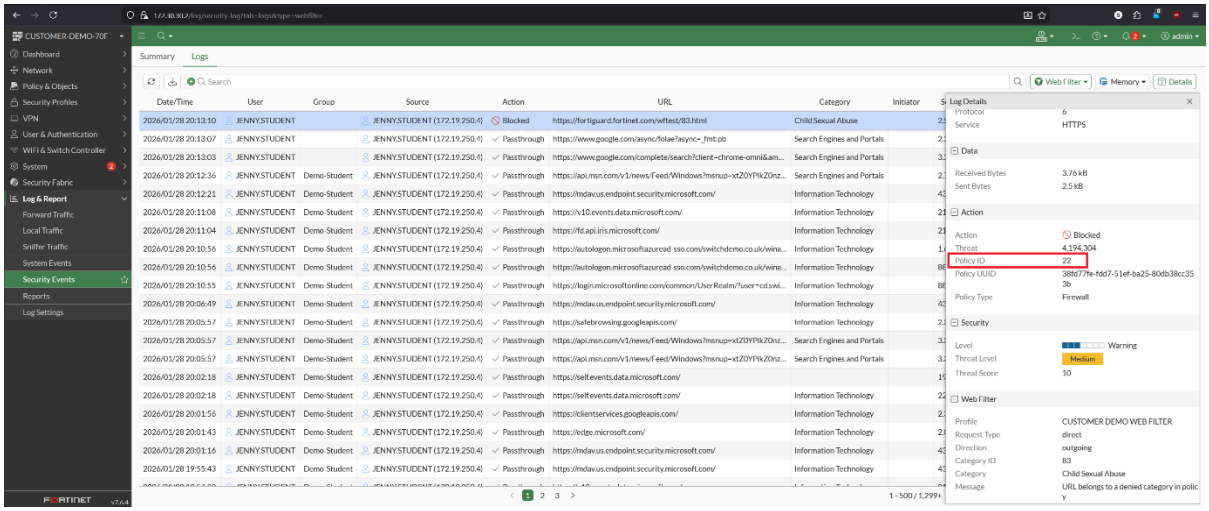
Missing All User information?

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.