Introduction:

In this scenario we are acting as school administrators in which we have to create a filtering list for our FortiGate 40F for a K-12 school district. This will restrict access to certain sites in predetermined categories for students within their scenario as well as monitor the use of unblocked websites. By downloading certificates on student's school computers, we are also about to have custom blocked messa

es appear when they attempt to go to a blocked website.

Background Information:

The FortiGate 40F is a "next-gen" firewall that enables small and midsized businesses (SMB) to get enterprise level security on a budget. Featuring many integrated security services such as: Firewall, VPN, Antivirus, Intrusion prevention, Web Filtering and Application Control, safeguarding your network from threats and provide control of network traffic. Web Filtering and Application Control are both part of Fortinet's Next Generation Firewall Service (NGFW) which uses AI/ML to prevent threats to a network and apply filter policies.

This lab used the Web Filtering, DNS Filtering and Application Control features on the firewall. Then using Firewall policy, we applied the desired filters to traffic passing through the firewall and in turn, blocking any categories of URLs, DNS, and applications from being used by users on the network.

Web Filtering (also known as URL filtering) restricts and controls access to websites based off preset categories offered to a network administrator. Administrators also have the ability to block specific websites that the presets might have overlooked. Administrators can also set categories to a monitor status which logs all URLs visited on the network. FortiOS Web Filtering uses 3 main components; Web Content Filtering, URL Filtering, and FortiGuard Web Filtering Service. These components of FortiOS's Web Filter collude to provide as much control as possible over what users on a network can view.

Domain Name System (DNS) Filtering works similar to Web Filtering however instead of using URL filtering it will filter websites via the domain name of the website. For example Web Filtering will filter the whole URL (www.youtube.com/watch?v=GNGH6E7-pFQ) while DNS filtering will filter out just "youtube.com" which will block all of YouTube while web filtering will only block certain videos. On a FortiGate firewall, DNS Filtering will take precedence over Web Filtering. DNS filtering also has features such as enforcing safe search for websites like Google or YouTube.

Application Control allows for administrators to see, block, allow, or restrict what applications users on their network are running. It allows administrators the ability to create control access to specific applications or entire categories. Using ISP protocol decoders, Application Control can analyze traffic passing through the network to determine whether it is application traffic even if the application uses a non-standard port or protocols.

Lab Summary:

This lab required us to make decisions regarding what categories of web filtering, DNS filtering, and applications control to block on the school network. In order to do as such, we first decided that it's best to set the preset filter to G-rated. This is done because this filter will be a one size fits all for K-12, which means kindergarteners will have the same restrictions as high school seniors. Having a more conservative filter will be better overall and protect younger students from potentially harmful and inappropriate content. We then added other categories to the g-rated preset that we believed was not appropriate for a school learning environment (shown below). Web Filter and DNS filter both have the same categories that are blocked with some extra things like safe search within DNS filtering. Application filtering was done the same, blocking thing we deemed inappropriate for a learning environment. Due to laws and regulations we also had to set all other categories that were not blocked to monitor in case any websites are inappropriate despite being in a unblocked category. Below you can see all the categories we decided was not appropriate and that are blocked.

Block list:

Web Filter:

Blocked; G-Rated preset +

- Games
- Social networking
- instant messaging
- Web Chat
- Newsgroups and messaging boards
- Personal Privacy
- Cryptocurrency
- AI
- Remote Access
- Entertainment

-
- Auction

All other categories set to monitor except for Child Education*

DNS filter:

Blocked; G-Rated preset +

- Auction (blocked)
- remote access
- AI
- Crypto
- Games
- social networking
- web chat
- instant messaging

All other categories set to monitor*

+ logging all DNS queries and respones

+ redirect botnet C&C request to block portal

+ enforce safe search for google and YouTube (strict)

Application Control:

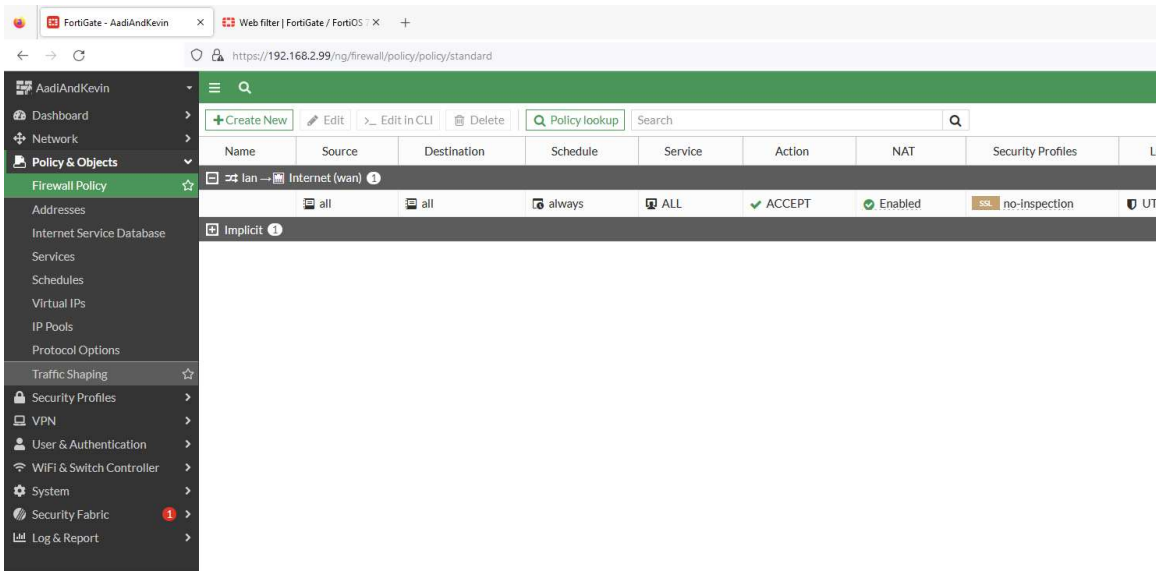
+ Block apps detected on non-default ports

Blocked:

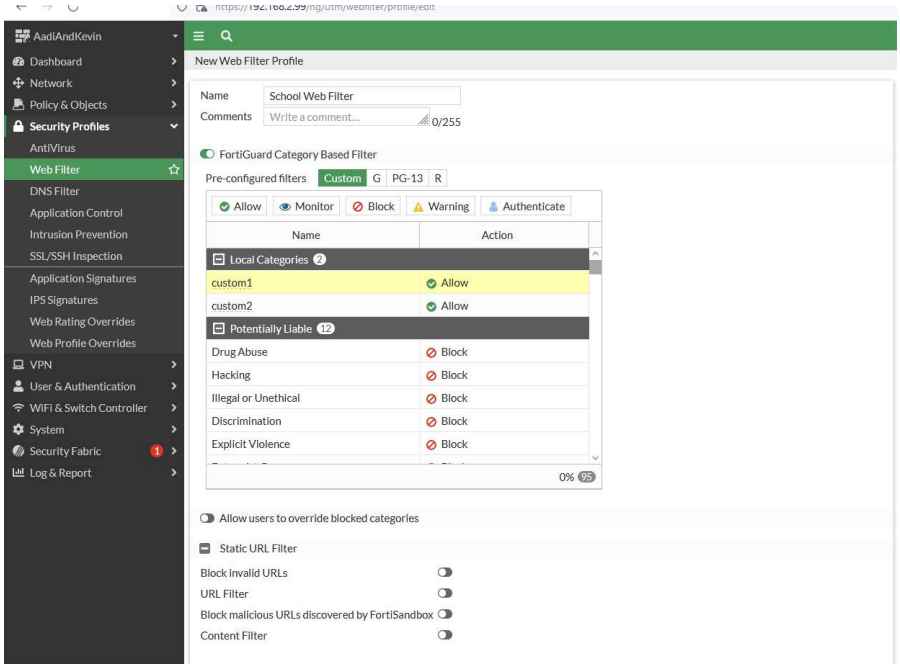
- proxy
- game
- remote access
- p2p
- social media

All other categories set to monitor*

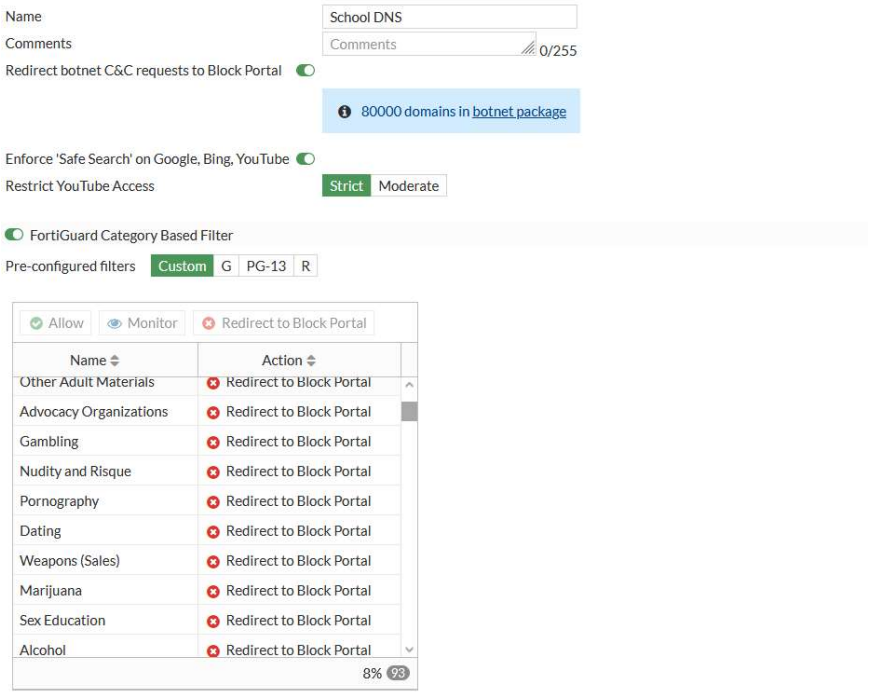
Step by Step:



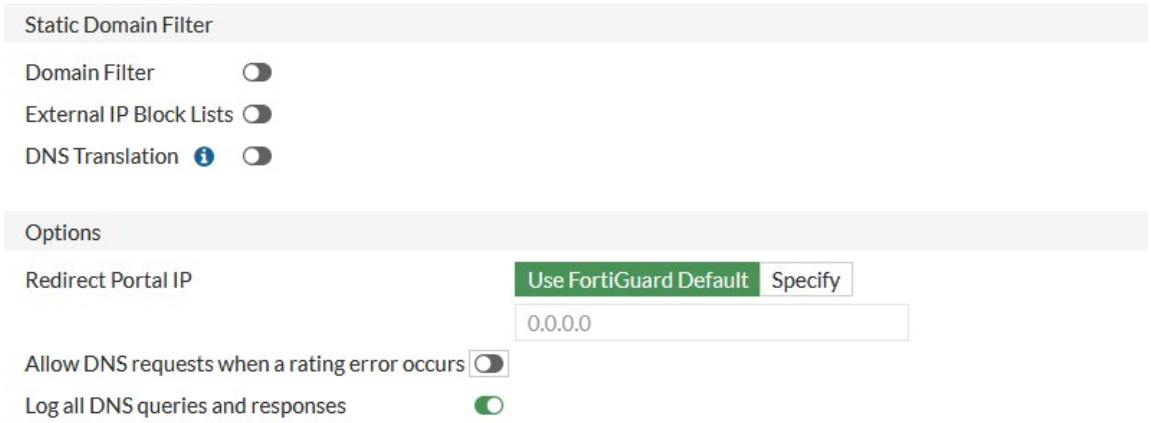
Going to Policy & Objects > Firewall Policy, we can see there are not set policies in place currently



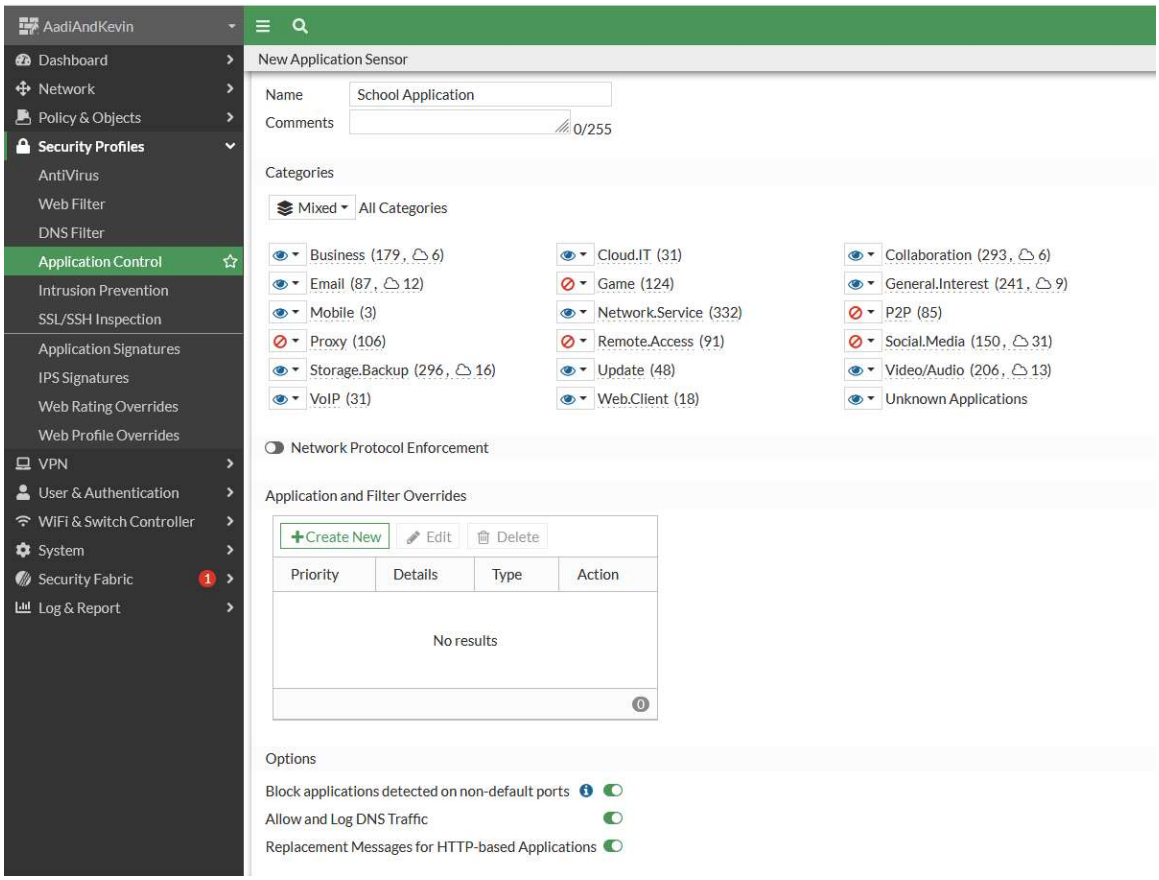
1: Under Security Profiles > Web Filter, we set a custom FortiGate Category Based Filter and filtered what we believe was inappropriate/distracting in a K-12 learning environment. All other websites were set to monitor.



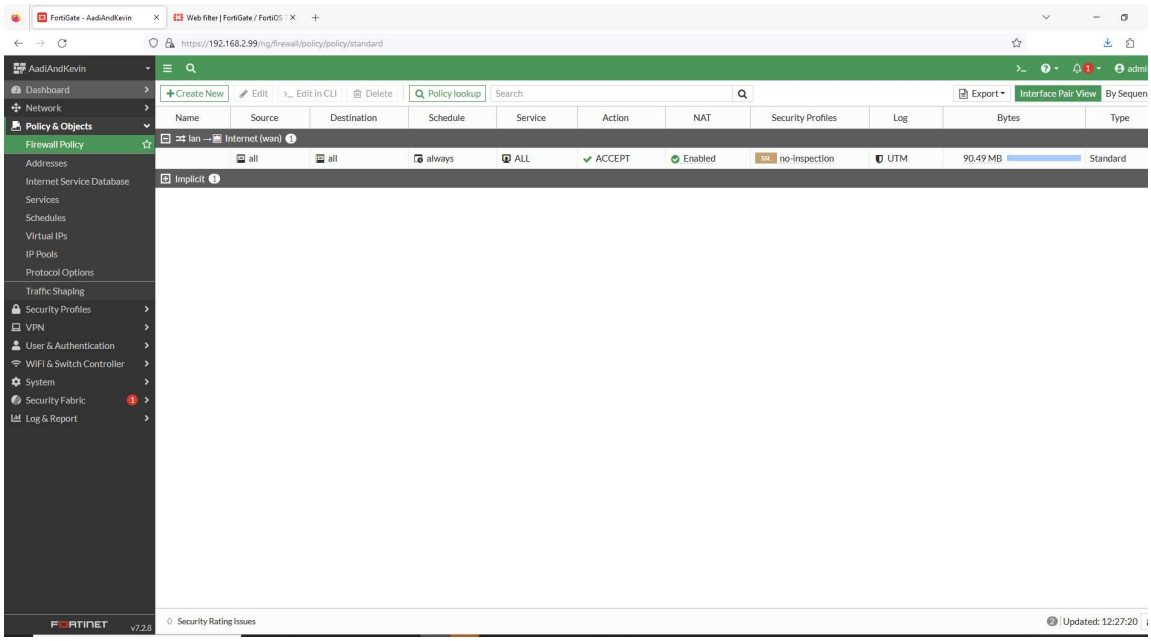
2: Going to Security Profiles > DNS Filter, do the same thing done before setting a custom Filter and blocking the same categories under Web Filter. Remember to set Enforce Safe to on



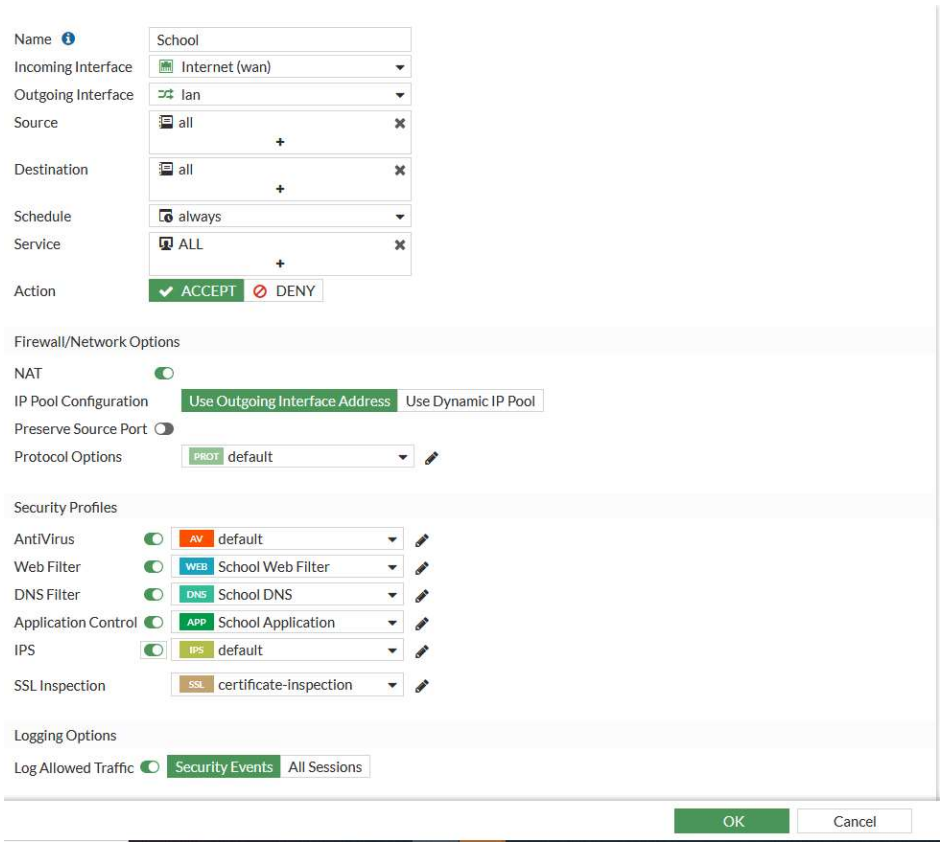
3: At the bottom of the page we also set Log all DNS queries responses.



4: Security Profiles > Application Control block. We blocked as shown above as well as selected the Options and turning on the 3 options of: Block applications detected on non-default ports, Allow and Log DNS Traffic and Replace Messages for HTTP-based Applications

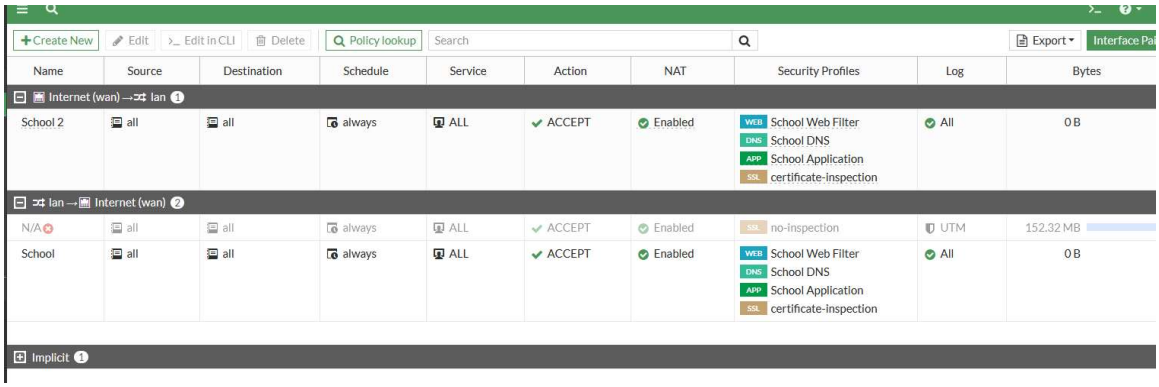


5: Now going to Policy & Objects > Firewall policy > +Create New

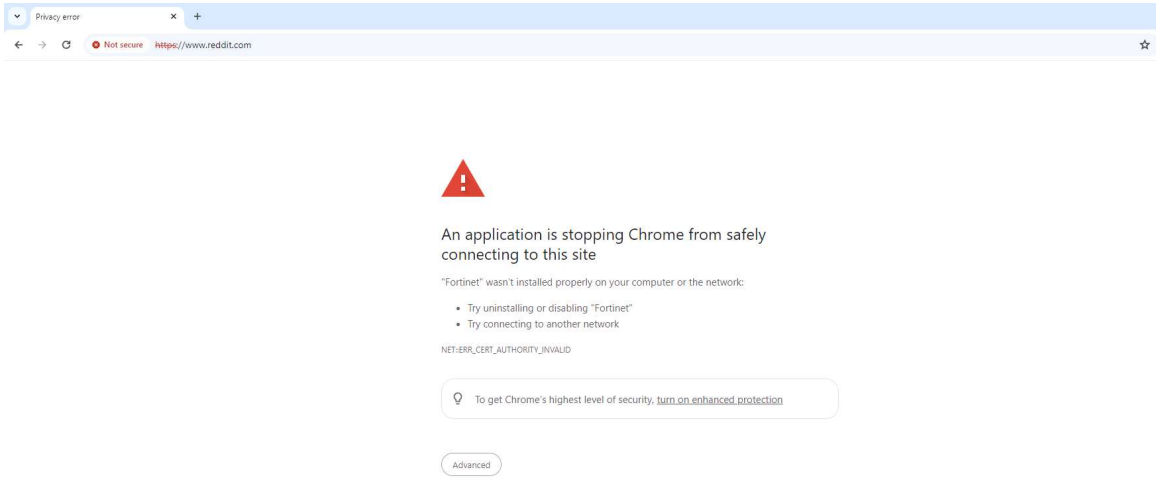


6: We named our policy “School” and set the Income interface to Internet (wan) and outgoing to lan. Enabled our Web/DNS Filters and Application Control as well as Antivirus and IPS

7: We set another policy with the same settings but swap the Incoming Interface to lan and Outgoing to Internet (lan)

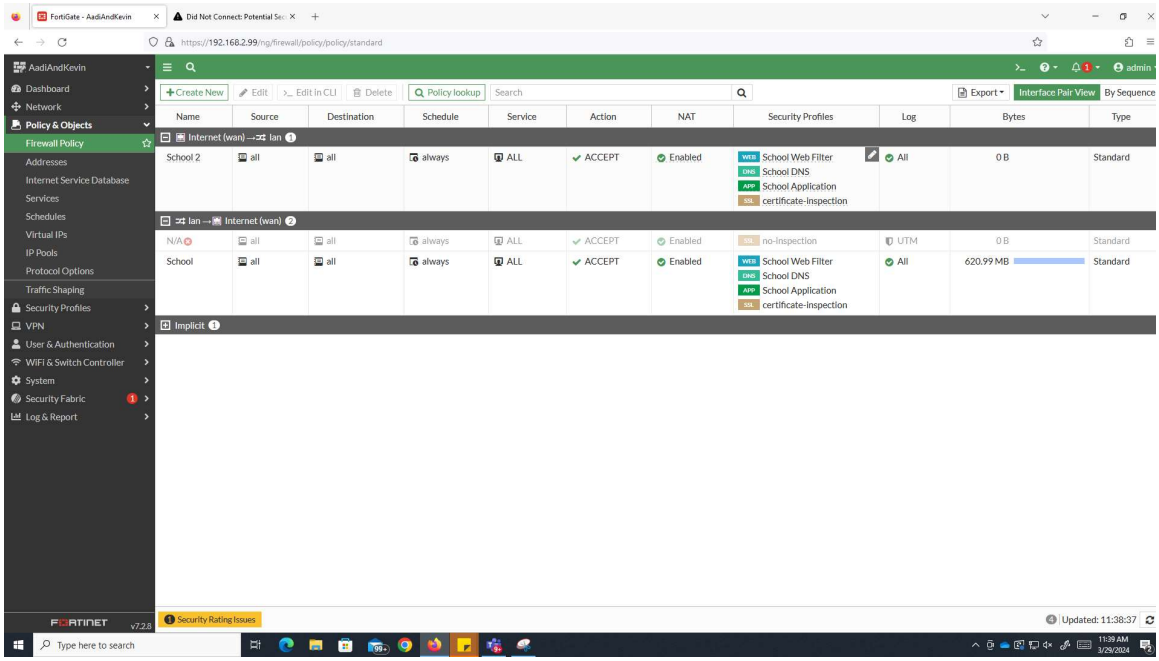


8: We now have our policies up and working

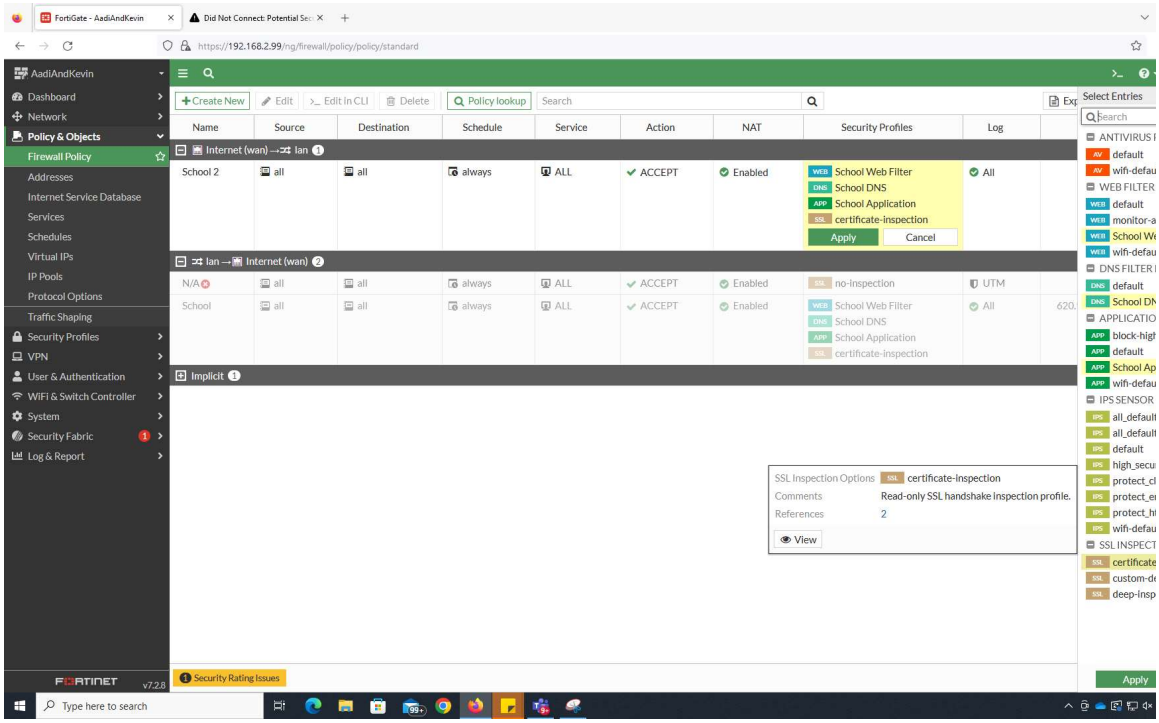


9: Going to a site like reddit.com which is blocked under the category of Newsgroups and Message Boards.

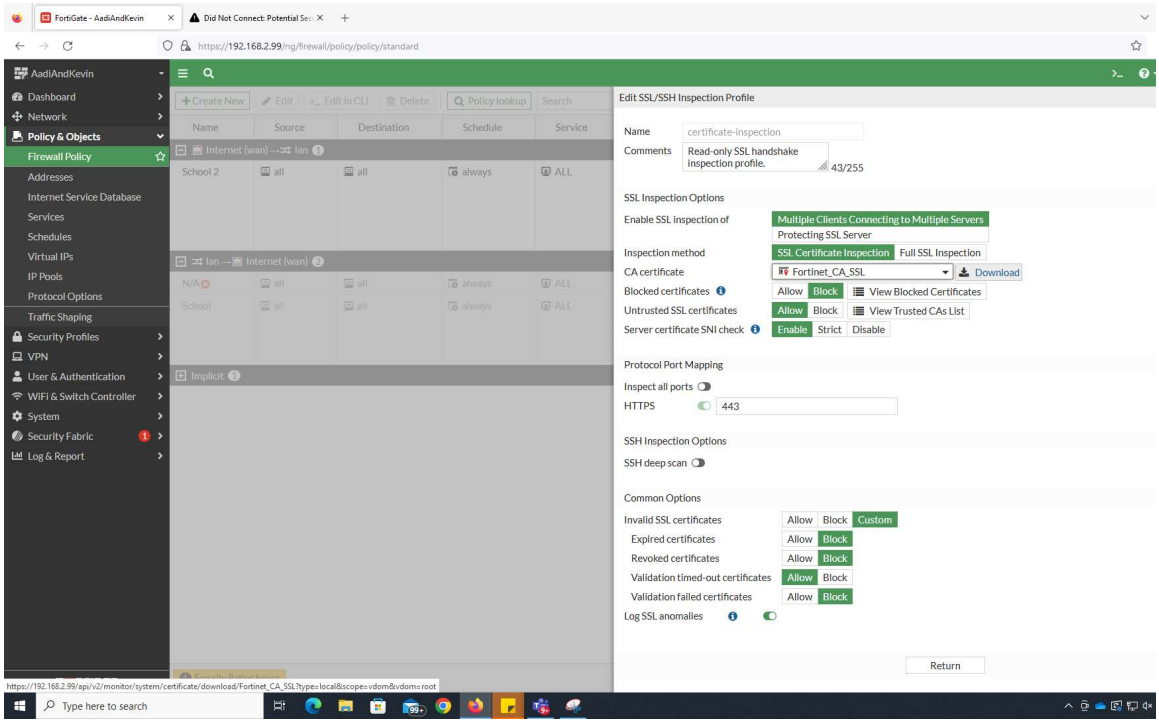
Now we downloaded the SSL certificate of the FortiGate 40F



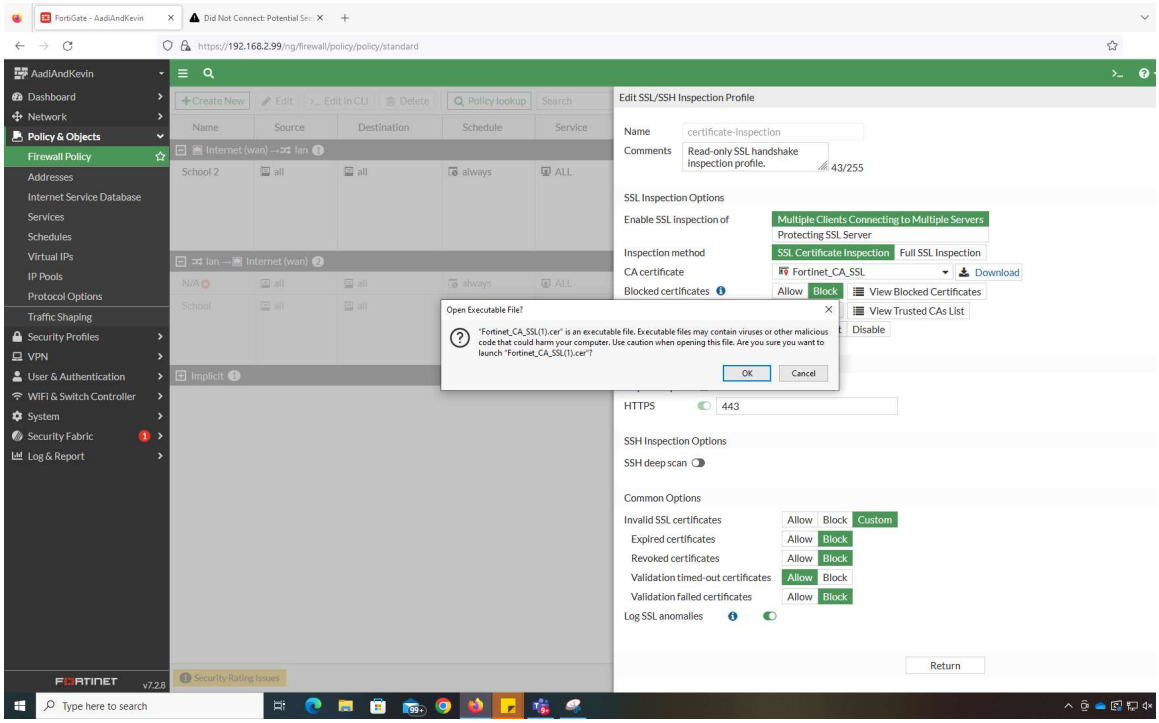
10: Under Firewall Policy, we hovered of on one of the policy Security Profiles and clicked the small edit button.



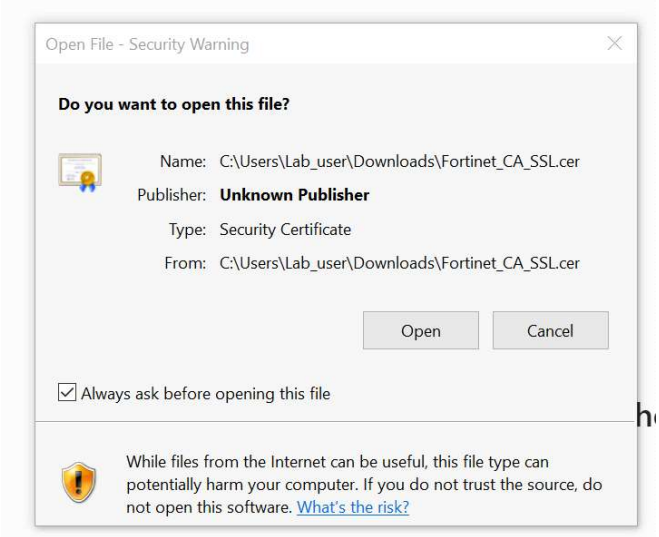
11: Near the bottom, click on certificate-inspection and edit



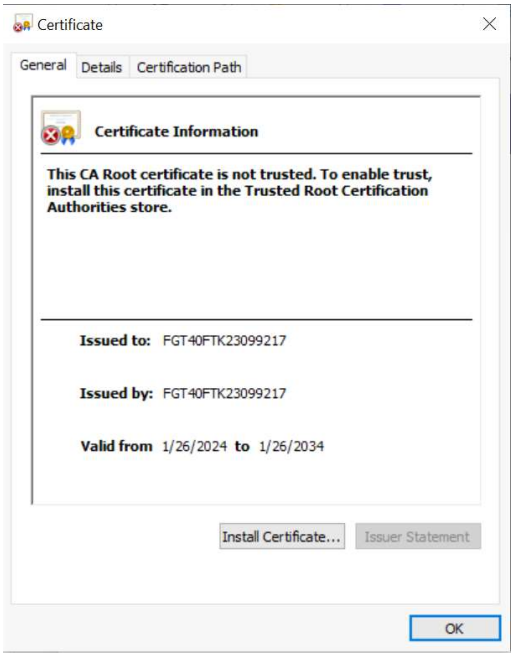
12: From here we were able to download the CA certificate.



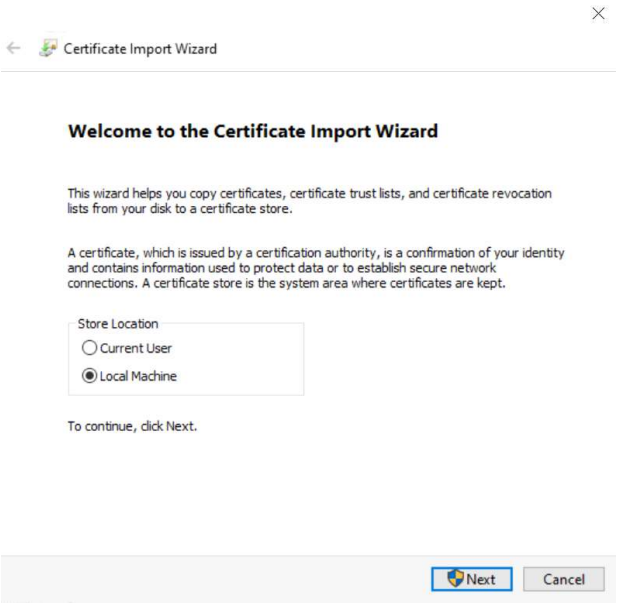
13: Download and click ok



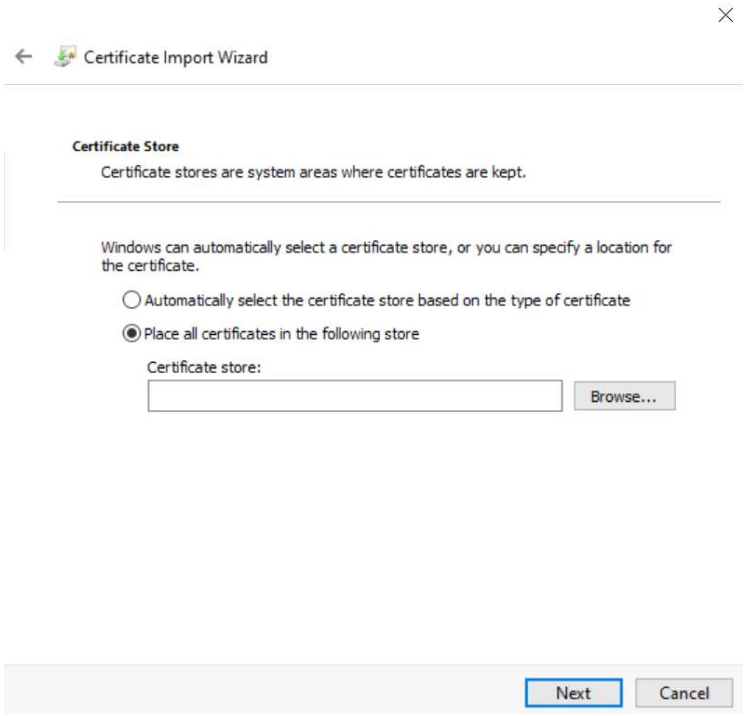
14: Open the executable file.



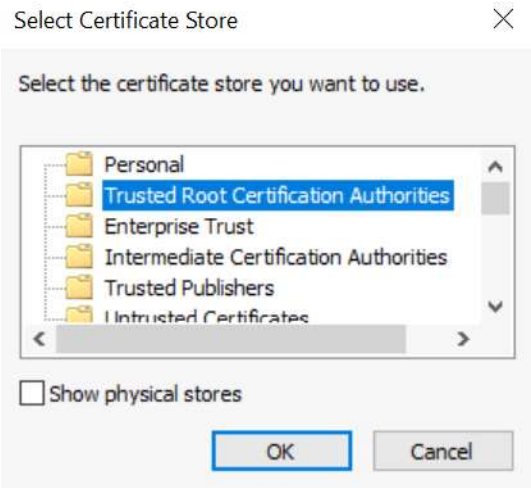
15: It will open this window, to install click Install Certificate…



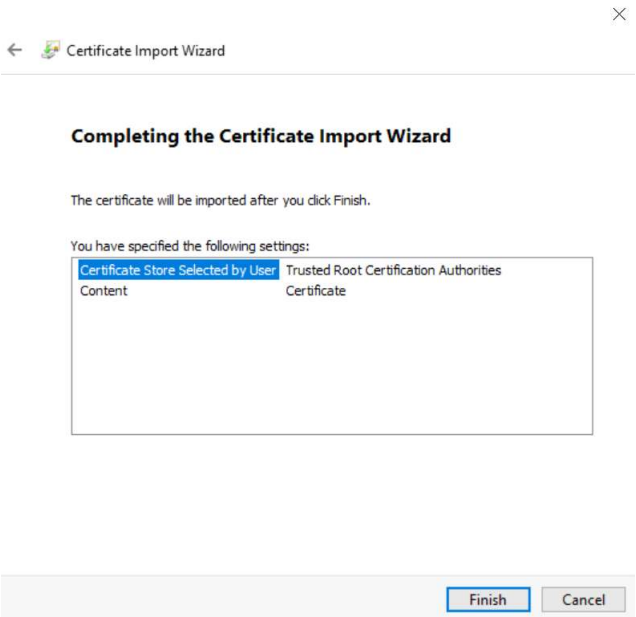
16: Install the Certificate onto the Local Machine and click Next



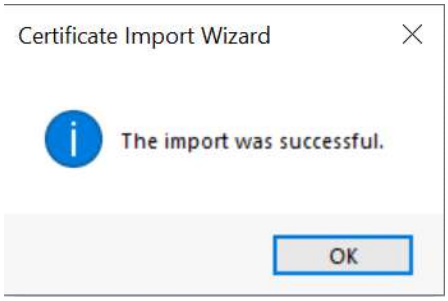
17: Place all certificates in the following store > Browse…



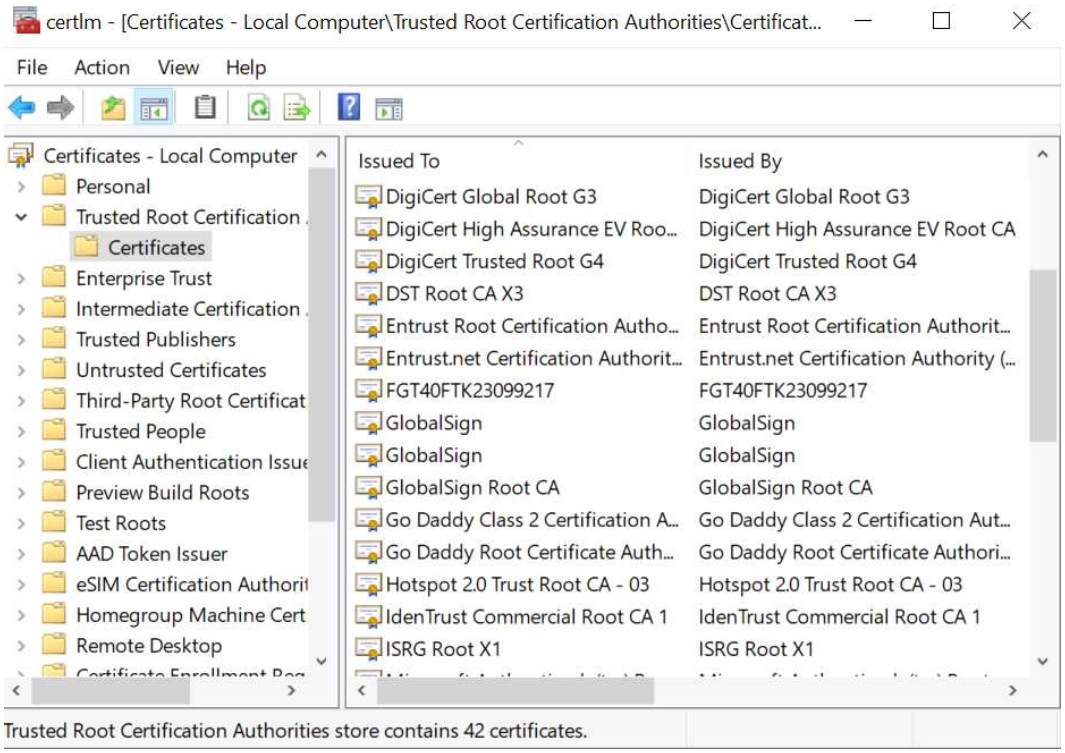
18: Select Trusted Root Certification Authorities. Click OK



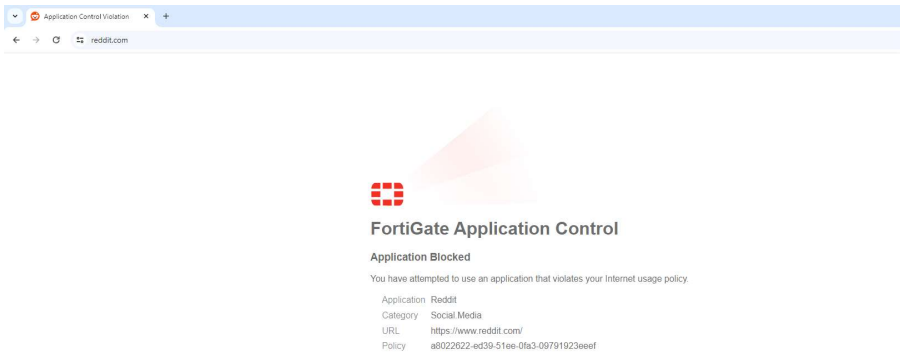
19: Finish the Import



20: It was successful.



21: Search for Certificates manager in the windows search menu and go to Trusted Root Certification > Certificates. Here you should find **FGT40FTK23099217.**



Now when we restarted Chrome, going to reddit.com will now show the FortiGate certificate.

Issues:

We ran into one issue in this lab near the end. It turns out you have to have an outgoing and incoming filtering policy in order for the firewall to work. This will ensure that no data is getting through the firewall either way ensuring the blocking of the websites categories selected. If only one of outgoing or incoming filtering is applied, users on the network will still be able to go to blocked websites like we were able to do with reddit. Shown in step 8, School and School 2 are the outgoing and incoming filters that will filter any and all traffic to and from those websites blocked under the preset filter categories.

Conclusion:

This lab mainly consisted of making administrator level decisions on what websites and applications to block and which ones to allow in a K-12 school setting. In terms of actual configurations, it was all just pressing buttons in the FortiGate GUI on a preset category filter feature built into FortiOS. In the end, we based our firewall filtering decisions on what we've seen being blocked on our own school district, Bellevue School District, as a real life example of what schools block and allow on their networks used in an actual learning environment

for students K-12.