Brit Stevens 3/8/24

Fortinet School District Filtering

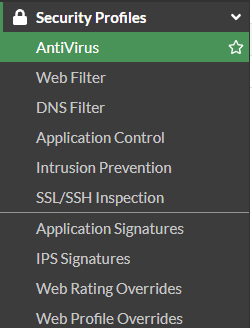
**Purpose:**

The purpose of this lab was to introduce us to how a firewall is used in a real-world scenario like in this case a school district. This lab showed us how a school may implement its network security with the use of security profiles and data inspection through a FortiGate firewall. It also is meant to show us how these profiles work and to make us learn what kind of data should be blocked and why.

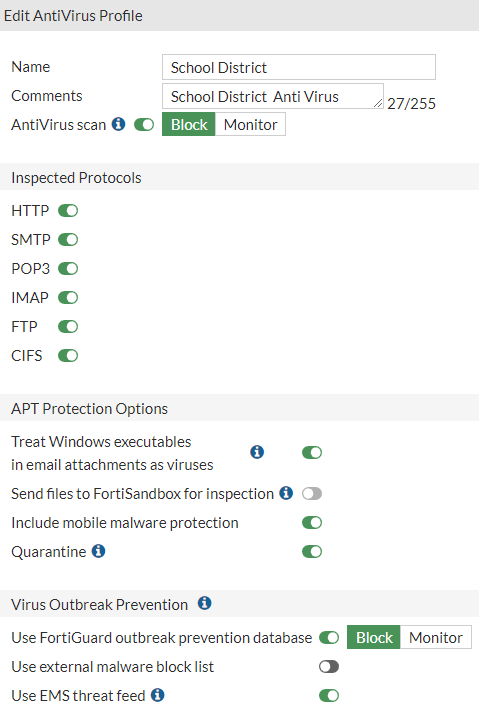
**Background Information on lab concepts:**

* **What Does A School District Need To Block?:** A school district would need to block a wide range of things from inappropriate or violent content to games and VPNs to bypass the school district blocks. We also need to protect the students from any malware or phishing scams to ensure data integrity for our school’s internal network. We go into detail on how and why we blocked certain things later in this lab.
* **Fortinet Security Profiles:** These security profiles are what admins at a school district would make use of to ensure the previously mentioned security risks/explicit content is blocked. They are a feature on the Fortigate-40F that we can define to inspect certain traffic that passes through the firewall. Some examples of security profiles are Anti-Virus, Web Filtering, DNS Filtering, Intrusion Prevention, and application control.
  + **Anti-Virus:** This Security Profile protects against malware, ransomware, and zero-day threats by delivering automated updates.
  + **Web Filtering:** This Security Profile involves blocking or controlling user access to web resources through the use of Web Content Filter, URL Filter, and web filtering.
  + **DNS Filtering:** This Security Profile controls user access to web resources by filtering DNS requests based on the FortiGuard domain rating or blocking known botnet domains.
    - **FortiGuard Domain Rating:** A system used by Fortinet that categorizes websites and domains based on their content and security risk for users.
  + **Intrusion Preventions:** This Security Profile monitors network activity for any activity that seems suspicious or any activity that triggers a policy.
  + **Application control:** This Security Profile blocks or allows specific applications on a network. You could use this to block VPNs with the use of blocking IKE or Proxy.
    - **Proxy and IKE:** Based on our past site-to-site VPN lab we know that IKE is required for a VPN connection same with Proxy. IKE works as a protocol between two endpoints of the VPN connection while Proxy works as an intermediary between a client and a VPN server. If both of these are blocked, VPNs cannot get into or out of our network.
* **Networking protocols:** These are a set of standards used universally on the Internet that dictate how data is transmitted, received, formatted, etc. Each protocol has a different use case and does something different to the data. Below are some common ones applicable to our lab.
  + **HTTP:** HyperText Transfer Protocol (HTTP) is what end devices use to access web pages and the protocol itself is what transmits the webpage to the browser. There is also HTTPS which is the same protocol but encrypted.
  + **SMTP:** Simple Mail Transfer Protocol (SMTP) is simply what is used to send emails across the internet.
  + **POP3:** Post Office Protocol Version 3 (POP3) is used by email clients to receive email from the internet or servers.
  + **IMAP:** Internet Message Access Protocol (IMAP) allows email clients to access and manipulate email messages on a server. This is essentially the same as POP3 but with more capabilities and a newer protocol.
  + **FTP:** File Transfer Protocol (FTP) is used to transfer files between a client and server on a network. This would be like sending a file to or from a server at your company.
  + **CIFS:** Common Internet File System (CIFS) is a protocol that allows programs to request files and services over the network. It is similar to FTP but has more capabilities like printer sharing.
* **Forti Sandbox:** This FortiGate service is a threat detection system that performs dynamic analysis to identify previously unknown malware by isolating suspicious files and running them in a safe environment to see if they have malicious behavior.

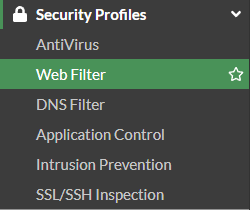
**Lab Summary:**

****

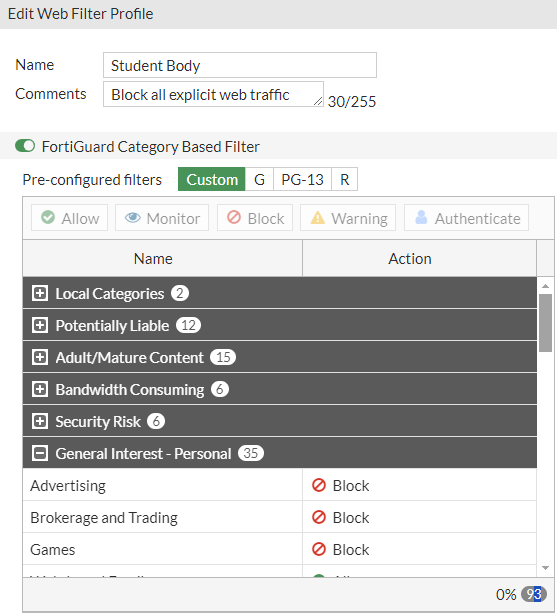
First, we need to go to **Antivirus** to create a new antivirus policy.



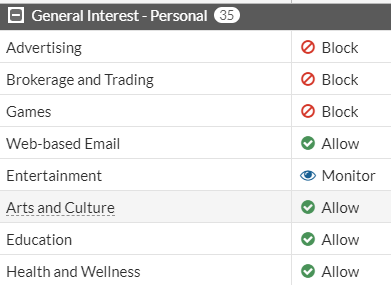
Click Create New and name it something recognizable. Select all protocols to look for viruses and ensure that no malware or viruses are let into the network. Leave the other settings as default as all of the settings selected are useful for network integrity.



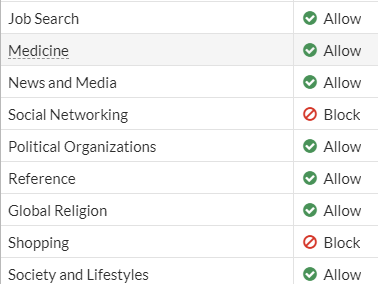
Next, select Web Filter to create a new security profile.



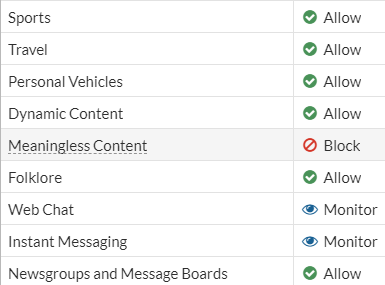
Here we must determine what web pages we must block to protect our district. Name the profile something recognizable for the future and look down to the Pre-configured filters. We left Potentially Liable, Adult content, Bandwidth Consuming, and security risk filters as blocked because all of these seem unnecessary in a school environment and could breach the network.

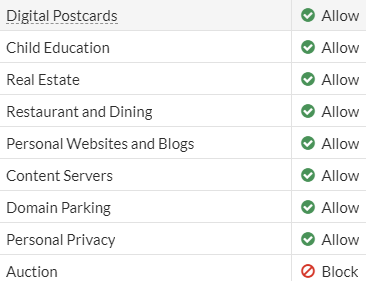


For General Interest we had to go in and block individual categories like Advertising, Brokerage and Trading, and games. These things shouldn’t be in a learning environment as they would just distract students. We set entertainment to monitor because then we could monitor and see if any entertainment sources are being actively used and are causing distractions. If it is not being abused during class time, then we see it okay to leave it unblocked.

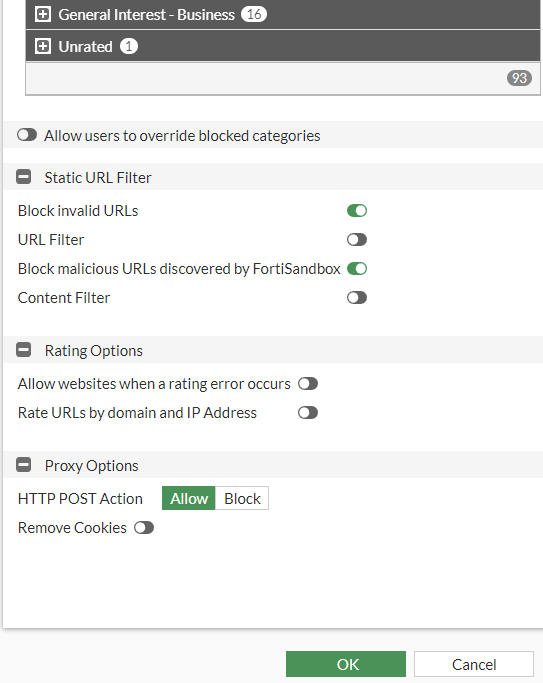


We blocked Social Networking and shopping for the same reason, they are just distractions and not needed during class time.





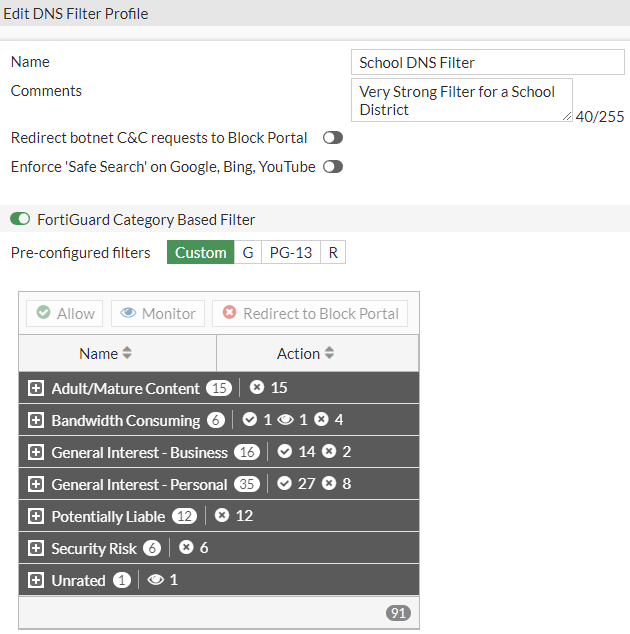
We blocked meaningless content and auctions because they seemed unnecessary in the school environment. We chose to monitor web chats and instant messaging because students could use a messaging app like Microsoft Teams to communicate with other students during the school day. If we block that it could cause issues so we can monitor for overuse instead.



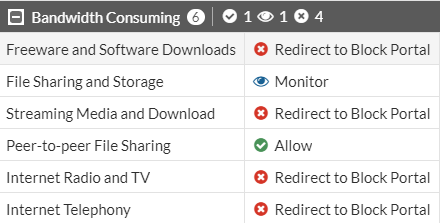
Finally, we left business general interests unblocked because they could need to be researched in classes like economics or personal finance. Select to block invalid URLs as if it is invalid it could be a risky website. Select OK to move forward.

****

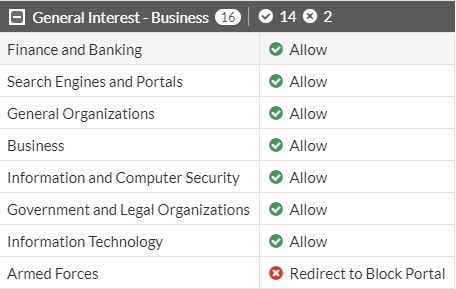
Next, we are going to configure DNS filters.

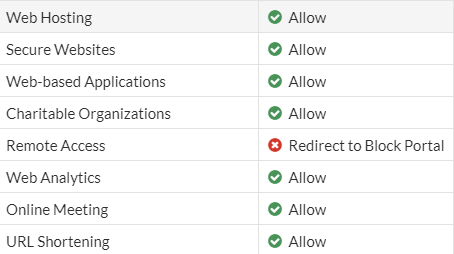


Name your profile something recognizable to use in the future. We Fully blocked adult, security, and potentially liable risk with this filter as those categories of DNS aren’t necessary in a school environment.

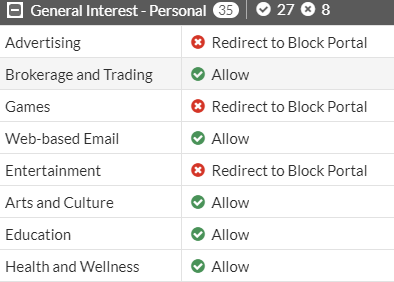


We blocked all streaming, software, internet calls, and radio. These things do not need to be accessed by students. All software on the student devices will be downloaded by an admin and put onto the devices before becoming the students’ devices. We are going to monitor fire sharing and storage to allow OneDrive and such but to ensure it is not abused. Allow p2p file sharing on the school’s network so students can share files.

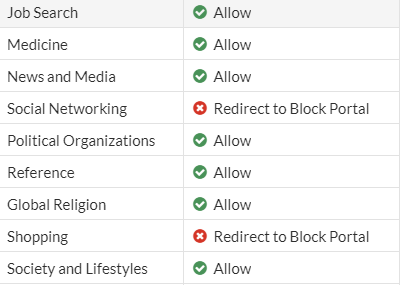




There is no need for remote desktop or looking up armed forces in school. If students need to research either of these the teacher could put in a request to whitelist certain websites.

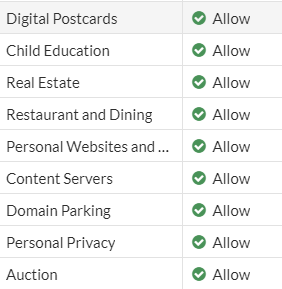


We will block games, entertainment, and advertising. We’re blocking games and advertising because of the same reason as before as they will be annoyances or distractions to students. We chose to block entertainment here because white lists the DNS addresses of the entertainment sites we will choose to monitor like YouTube for instance.

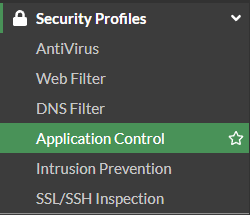


We are blocking social networking and shopping because those can both be done outside of the school and will only distract students. The other categories are unblocked because they may need to be frequently researched in classes.

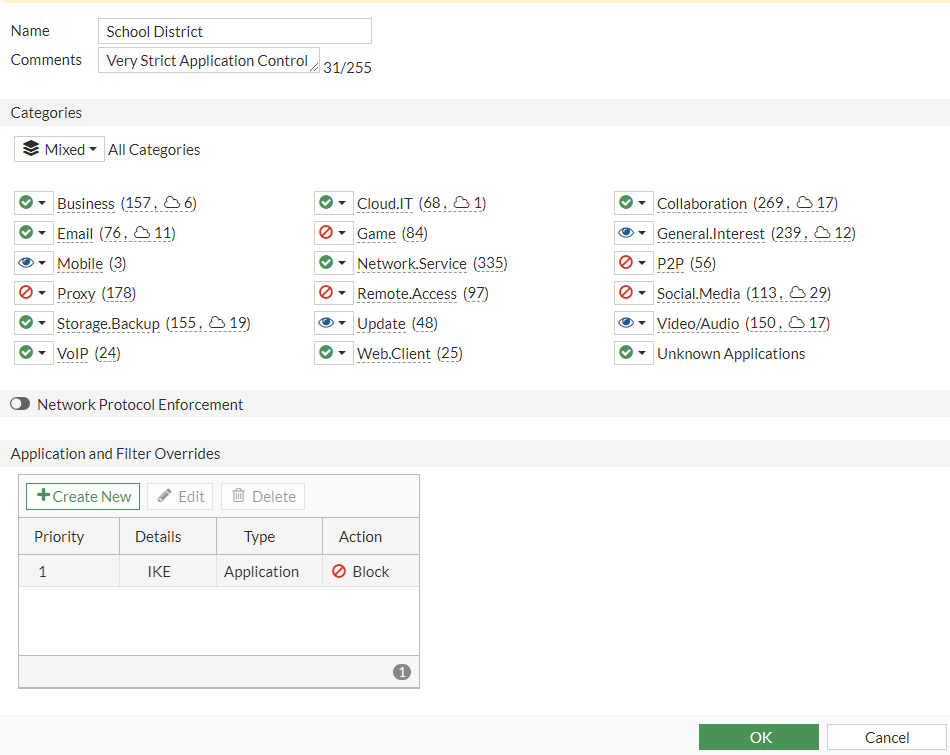




We blocked sports, webchats, and instant messaging because they will pose distractions and are not necessary at school. For webchats and instant messaging, we will whitelist the sites we want to allow students to communicate with but will monitor for overuse and distractions just like with entertainment.

****

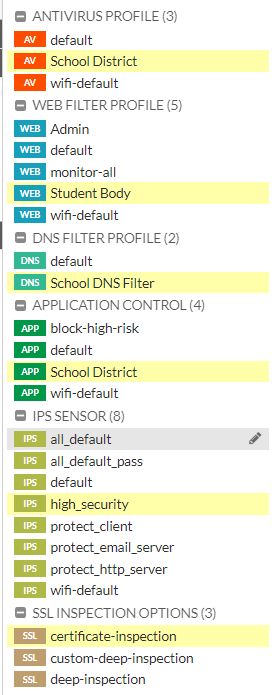
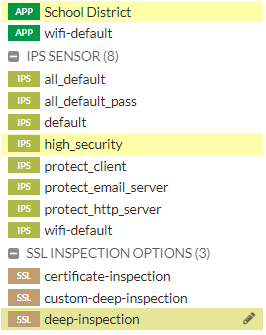
Next, go to Application Control to configure that Security Profile.



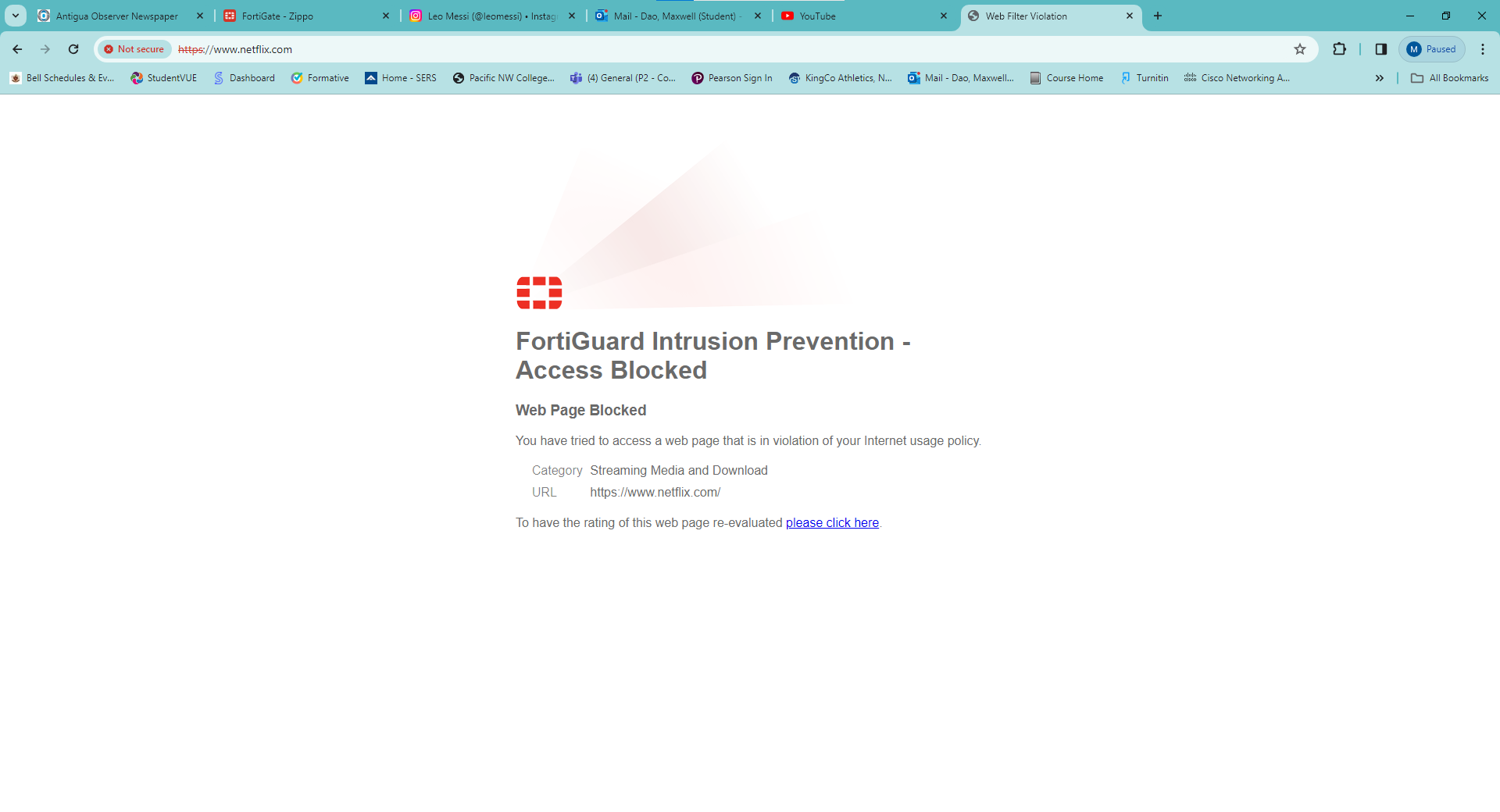
We wanted there to be no games in the network, so we blocked any game applications. We monitored general-use websites, mobile, update, and video/audio applications because these kinds of applications are not inherently bad and we monitor to see if too many students are creating traffic to certain sites to determine if they need to be blocked as distractions. We monitored updates to ensure students were upgrading or downgrading any software that distinctly changes it and bypasses our policies but didn’t wish to fully block it since, for example, Google Chrome updates provide greater web security. We blocked Proxy, P2P, social media, and IKE as these are all things that could be distractions like social media or used to bypass our security profiles. Proxy and IKE are used in VPNs to establish links so if we block those then no VPN connections can be formed on the network. Remote Desktop is blocked for a similar reason as there is no need for a student to access a device that is not their own on the network. P2P is blocked here as we only want certain P2P applications to be available to students and we would white list those on the Application filter.



Go back to Firewall Policy and edit the Policies to use your newly created Security Profiles and high-security IPS and SSL profiles.

**** ****

choose your profiles and include high security to block all high threats using Intrusion prevention service and deep inspection for the SSL inspection option. This verifies that encrypted traffic using SSL (an encryption protocol) is fully inspected before being allowed into the network by decrypting and re-encrypting the data. This will detect any malicious data and activity in the packet.

****

We can see here that our file wall is successfully blocking a media streaming website because we did not white-list the URL.

**Problems:**

* DHCP pool out of range of firewall interface, could not access the firewall.
  + Set static IP to access and reconfigured pool.
  + Additionally forgot to turn off static IP and could not access the firewall occasionally.
* Fewer guides than PaloAlto firewalls.
  + Researched using owner manuals and figuring out the steps ourselves.
* Unsure how to block VPN.
  + Tried only allowing addresses within our DHCP pool to go in and out of our firewall but that did not work to block a VPN.
  + Determined that VPNs need IKE protocols needed to establish VPN.
  + Proxy works too and is less direct.
* Websites were not blocked.
  + Had to apply the security profiles to the firewall policy.

**Conclusion:** Overall this lab was more complicated than we first thought. At first, it seemed relatively easy with the preconfigured filter lists that could applied in every security profile but later realized that for our scenario we need the custom lists. The categories in the security profiles made it easier to determine what data should be allowed and what shouldn’t but we still ran into some issues. We thought we were done with the lab many times but forgot to block some traffic like VPNs. It took a few days of trial and error to get VPNs finally blocked with the use of Proxy blocking. The biggest takeaway from this lab is understanding what each security profile does and how they’re different from each other in the ways they block traffic.

