

**PALO ALTO URL FILTERING + OVERRIDE**

****Brendon Ahn | Cybersecurity | 2022-2023

**Purpose**

To set up URL Filtering on the PA-220 as well as an override for the filter.

**Background**

Palo Alto URL filtering is very important for corporations to have. The PA-220’s have packet inspection and filtering and so it has the ability to filter out undesired URLs. This is very useful as you may not want employees accessing certain sites. This can prevent viruses and ip leaks from dangerous URLs as well. This is equally if not more important in schools. You can block games, dating sites, etc. using the PA-220s.

How the URL filtering works is pretty simple. Palo Alto has a constantly updating list of categories of sites. They deem what is a game for example and everything that falls under the game category can be easily blocked. You can also block additional sites on top of this. The configuration of URL filtering doesn’t take a lot of time; however, you must be connected to the firewall for this to work. The firewall that connected to the internet will monitor traffic coming to and from the pc before it goes either out or in and that is where the PA-220 will filter URLs.

There is another process that comes with URL Filtering and that is the Override feature. Using an administrative key, you are able to bypass the block on certain sites. This can be very useful if there a site, say a teacher wants to be able to go to like a video site, that they don’t want students to be able to access.

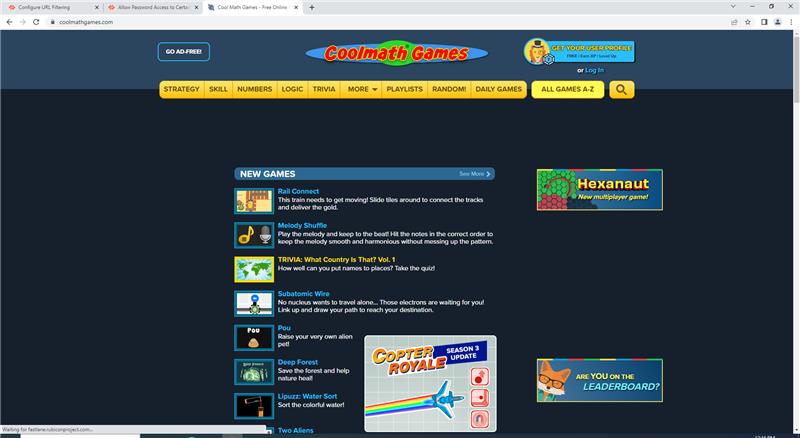
The way we set our URL Filtering up is using the pre-existing categories that Palo Alto has on their system. For the override, the setup was more complicated. There are multiple paths you could take and the recommended one on the Palo Alto site is to use a self-signed certificate which doesn’t work. The override itself had some issues as it didn’t work on https sites and only really worked on Firefox. This issue has not been solved.

**Lab Summary**

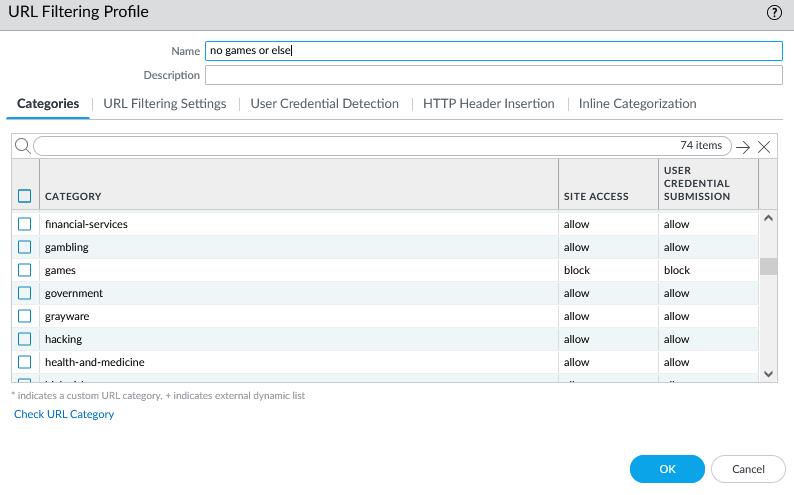
We successfully filtered out games using the PA-220 Firewall and made it so that we could override the filter in specific situations, unfortunately not for all.

**Lab Procedure**

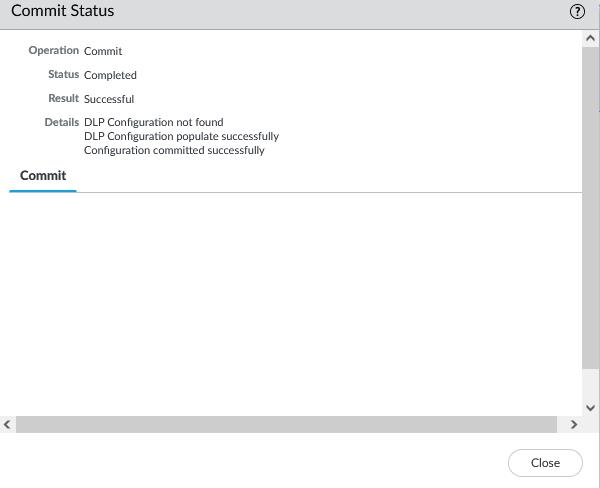
1. Select the website you would like to URL filter



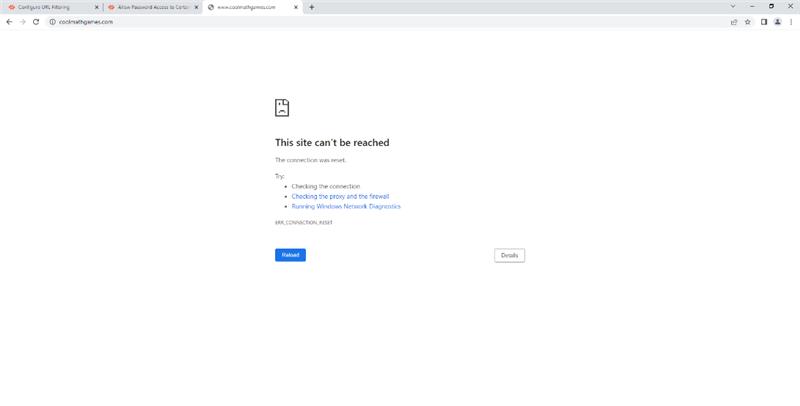
1. Find what category your selected website belongs to using the following website: <https://urlfiltering.paloaltonetworks.com/>
2. Go to Objects -> URL Filtering -> and click “add”, and configure the following:



1. Commit changes

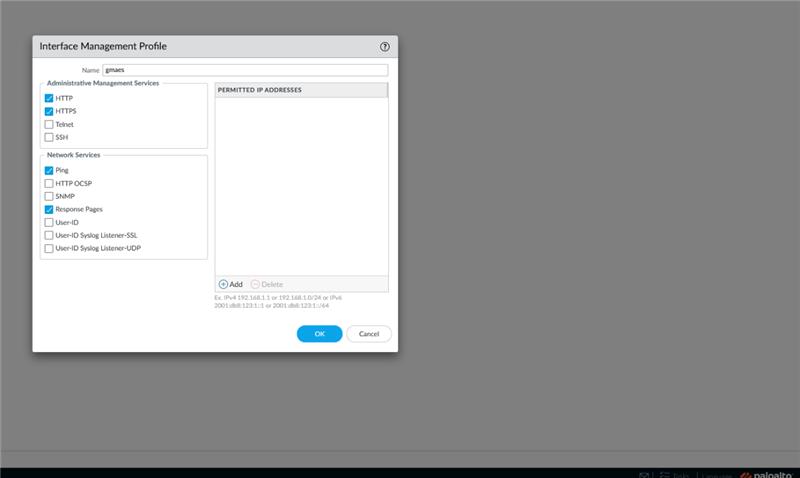


1. Your website should now be blocked:

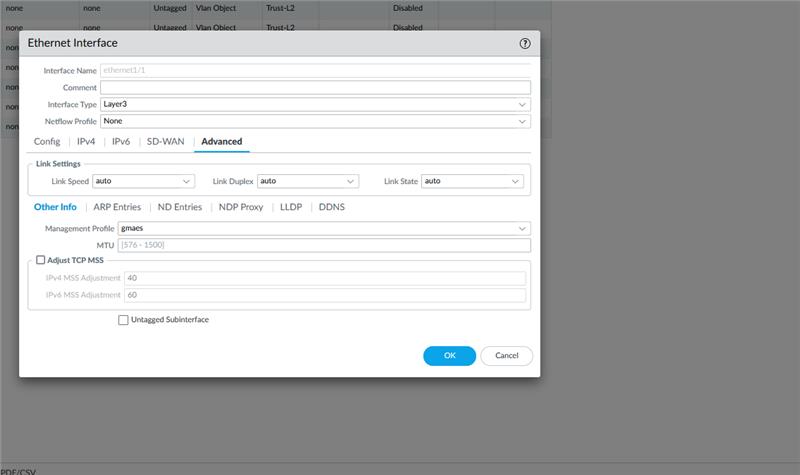


1. To complete the override, go to Network -> interface management and click “add”

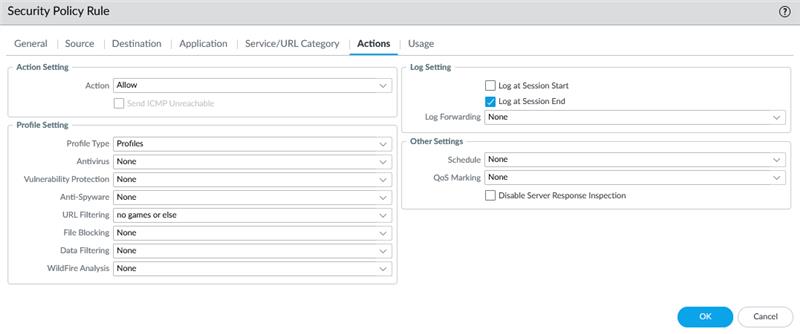
Configure the following:



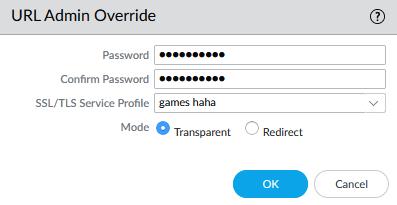
1. Go to Network -> Interfaces -> “ethernet 1/1” -> Advanced and configure the following



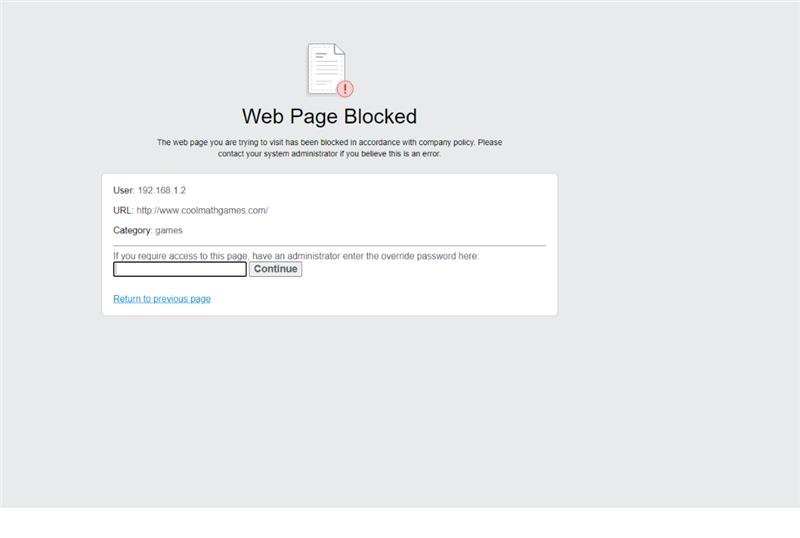
1. Go to Policies -> Security -> “Internet Outgoing” and go to “actions”, and configure the following:



1. Go to Device -> Setup -> Content-ID and under URL Admin Override click “add”. Configure a password and configure the following:



1. Commit changes. Afterwards, this screen should appear on your selected website.



**Problems**

The URL Filtering step on the PA-220 went smoothly other than forgetting to commit the changes one time. The override process on the other hand had more problems. We changed the filtering process to an override process to try to get override to work however this was the wrong move. We were to set it to allow for the actual ability to override. Setting up the Override had a problem as we tried self-signed certificates. This was solved by using no certificate however even then the process didn’t work with every site and didn’t work on chrome.

**Conclusion**

We configured URL Filtering onto our Palo Alto Firewalls and made minor success in setting up override for the firewall. The override being a minor success as it doesn’t work everywhere and isn’t the most consistent.