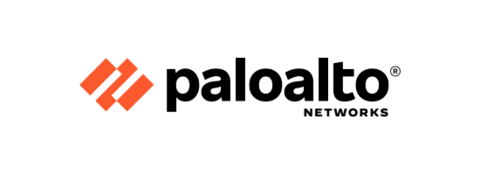


URL Filtering Lab Writeup

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose**

The purpose of this lab was to URL filter a selected website and to be able to override the filter with a password.

**Background**

Palo Alto has a list of categories built in with the firewall. You can filter using these categories such as the games categories and it’ll block all sites that Palo Alto has listed as game sites. This list is always updating.

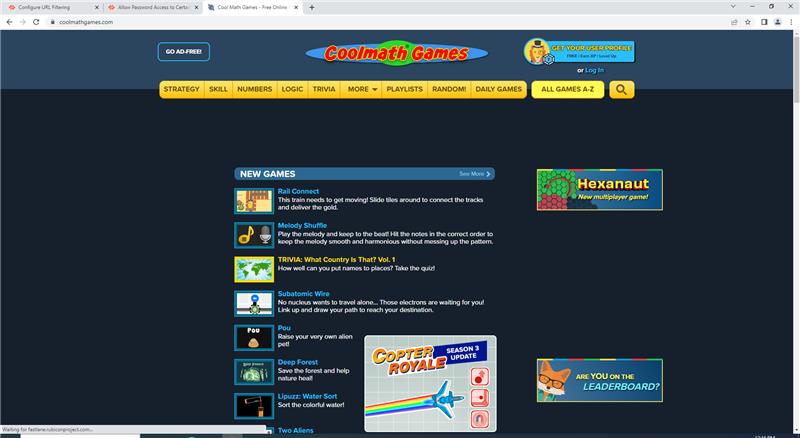
The purpose of filtering URLs is to filter traffic. There are many reasons you may want to filter traffic. One is to prevent people with mal intentions from getting access to your network. Another is to prevent people on your network from going to sites that you don’t want them in. These are used in schools to prevent students from getting distracted by games. Basically, you want to stop all unwanted traffic from going through to your network.

With filtering there is an override feature. The override feature is to bypass the filter that was put in place. Going to a site that is blocked if you have the override enabled it will take you to a page that asks for a password. This password is set on the firewall so if you want to access a blocked site you can use override to access it.

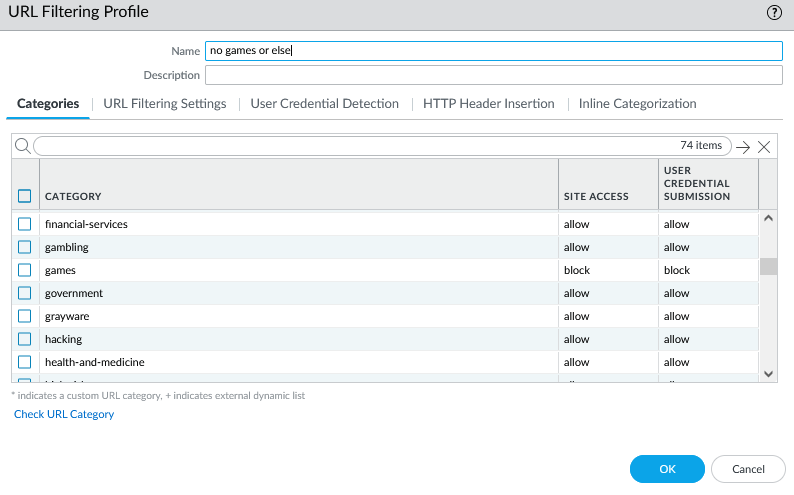
You can find a list of sites and categories on Palo Altos site to find out what is listed. Palo Alto has 72 listed categories ranging from games to adult. Both of which you probably don’t want students accessing at the very least on district networks. Some of these categories would probably be blocked by corporations as well. A caveat is that this is an additional safety measure but a more important one would be internet safety education for students and employees so that they would be able to identify what links they probably shouldn’t click on.

**Lab Procedure**

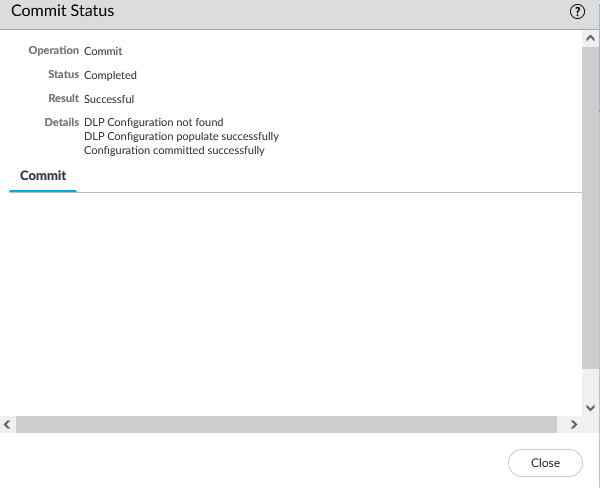
1. Select the website you would like to URL filter



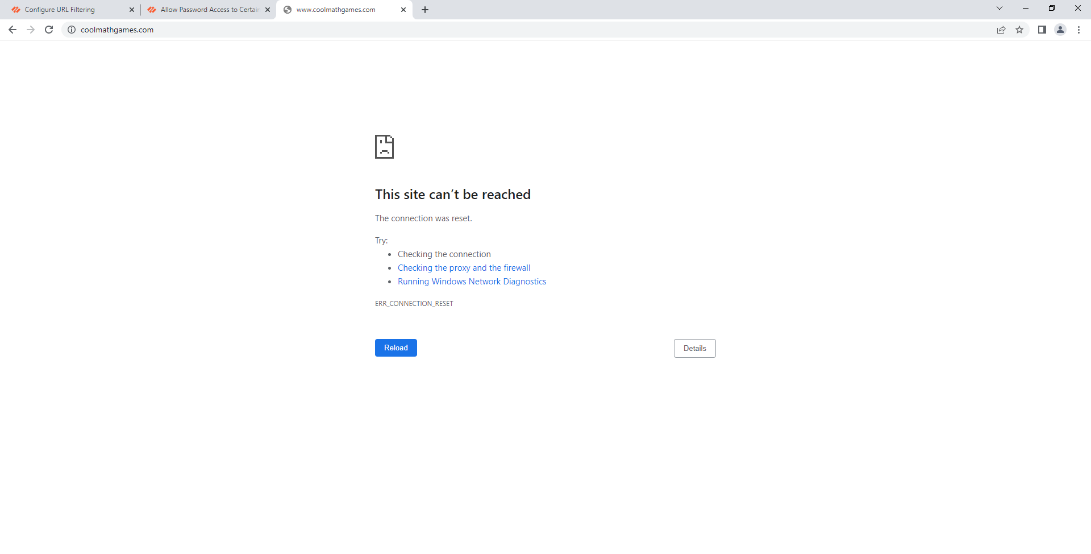
1. Find what category your selected website belongs to using the following website: <https://urlfiltering.paloaltonetworks.com/>
2. Go to Objects -> URL Filtering -> and click “add”, and configure the following:



1. Commit changes

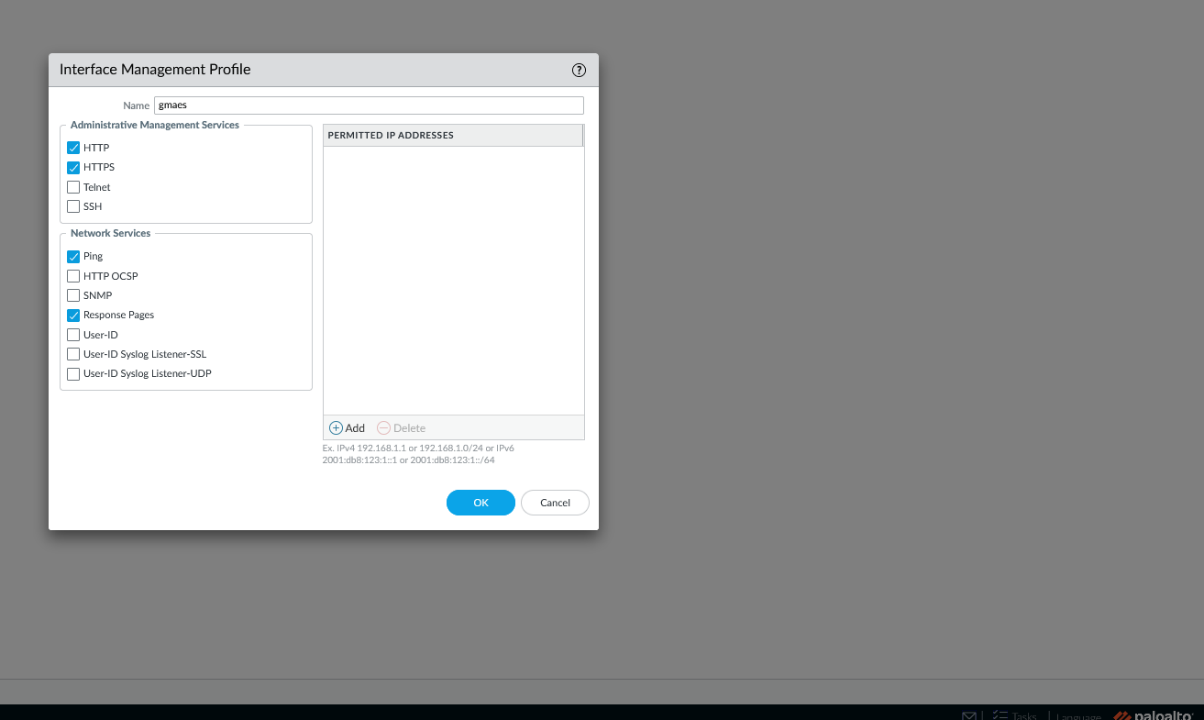


1. Your website should now be blocked:

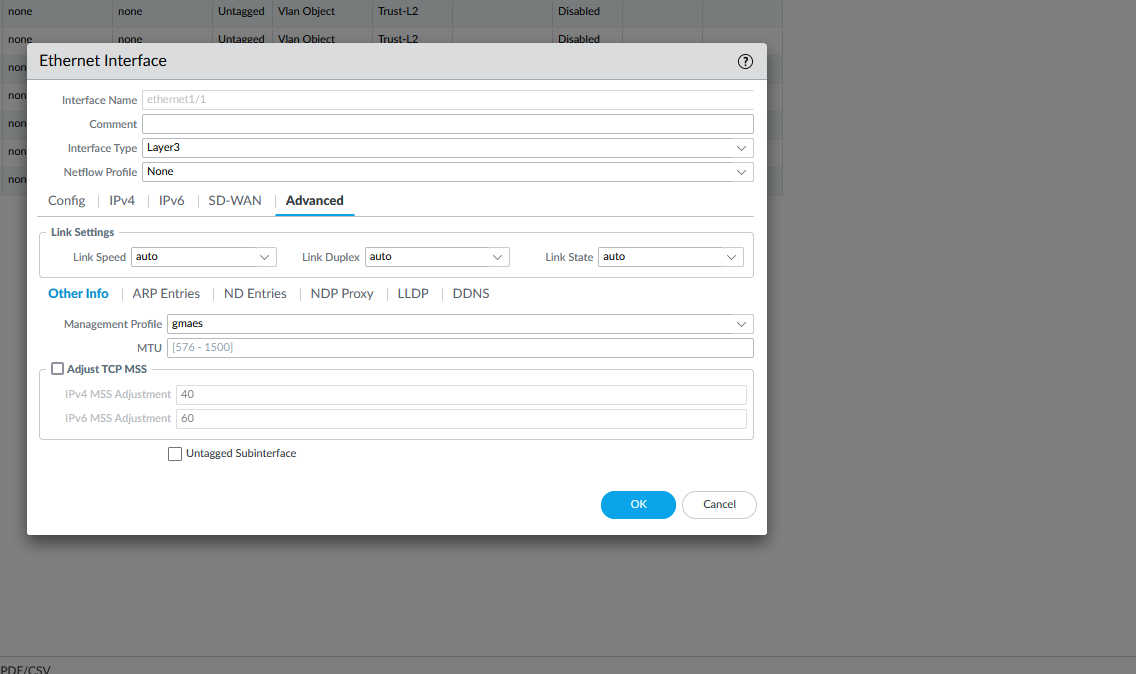


1. To complete the override, go to Network -> interface management and click “add”

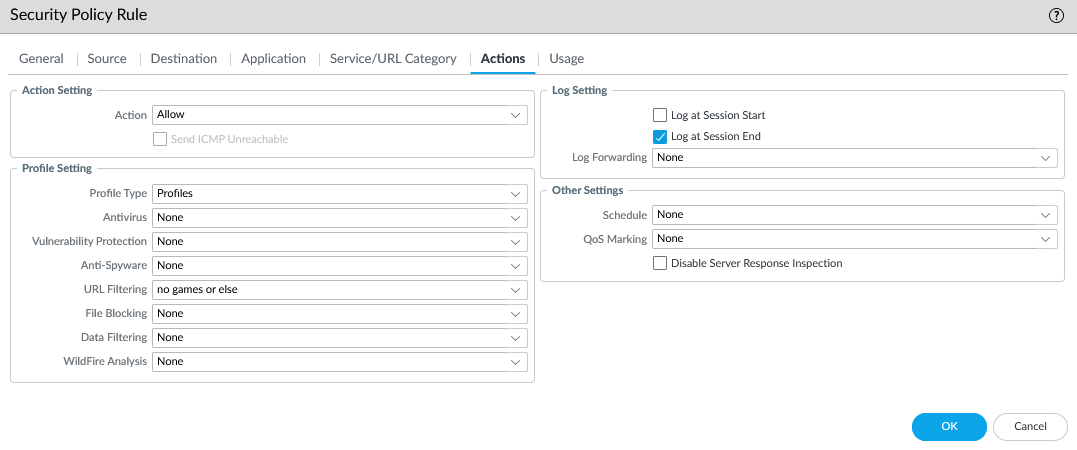
Configure the following:



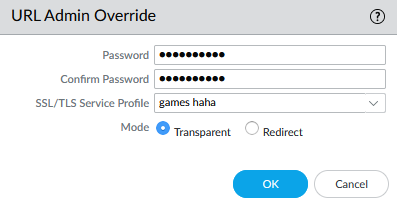
1. Go to Network -> Interfaces -> “ethernet 1/1” -> Advanced and configure the following



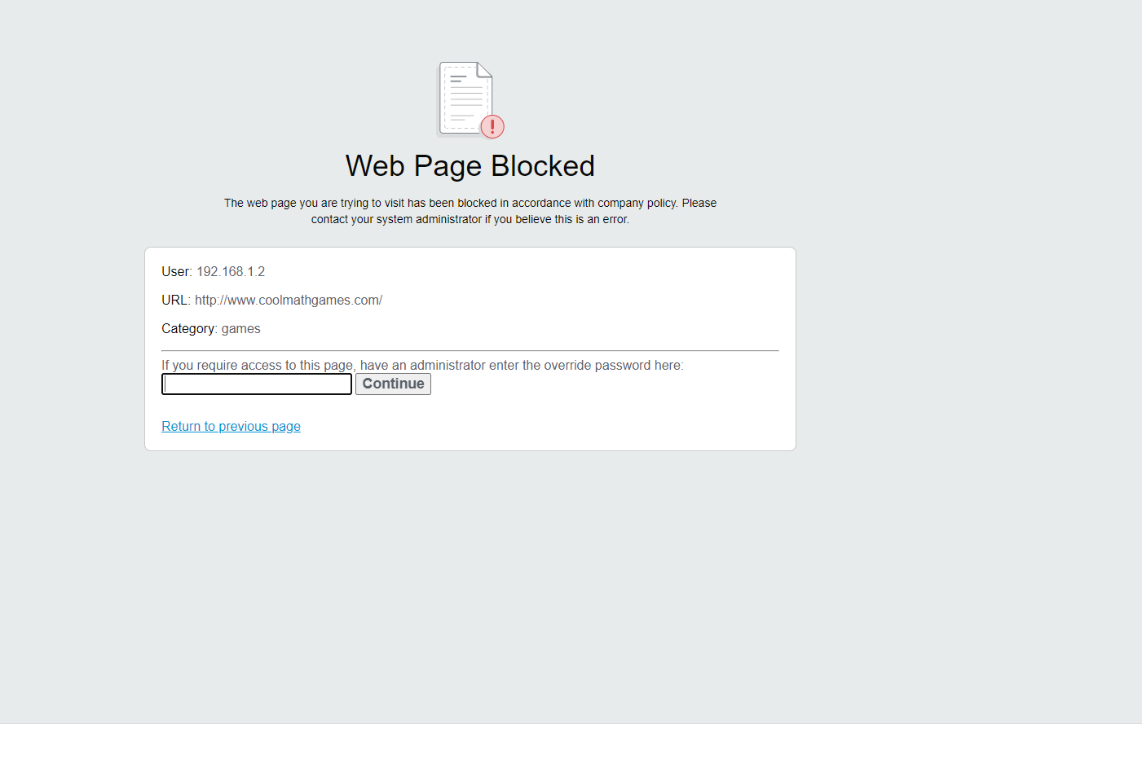
1. Go to Policies -> Security -> “Internet Outgoing” and go to “actions”, and configure the following:



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**

One of the main problems was that we created our certificate incorrectly, causing us to restart the entire lab. We configured one of the settings for “self-signing” wrong, and our certificate was not able to function. Frustrated, we restarted the entire lab in hopes to find our mistake. This was not only tedious and time-consuming, but also set us back a couple days. Secondly, we were unable to get the URL filter to work for https:// websites, but the URL filter was successful for http:// websites. Both these issues took significant time to fix and was a setback in our completion of this lab.

**Conclusion**

In this lab, we configured the Palo-Alto PA-220 firewall to have a URL filter to block cool math games.