URL Filtering

By: Jordan Abu-Zahra

**Purpose:**

the purpose of this lab was to learn how to filter URL’s so that we can block things that would harm the network and we learned how to override the block by putting a password on it

**Background:**

in the previous lab we configured our Pa220 for a SOHO setting and now we need to block certain URLs to keep people from doing things on our network that we don’t want like for example we are blocking games so that people in our SOHO environment are doing what they are supposed to be doing.

In this lab we added an internet filter which is a software that restricts/controls the content a user on your network can access, and this is used especially when you need to restrict material delivered over the internet via web, email, or other apps you communicate over. Pretty much every network technician uses URL filtering when they are making a network especially people who need to keep important information safe like in the government or people high up at big enterprise companies.

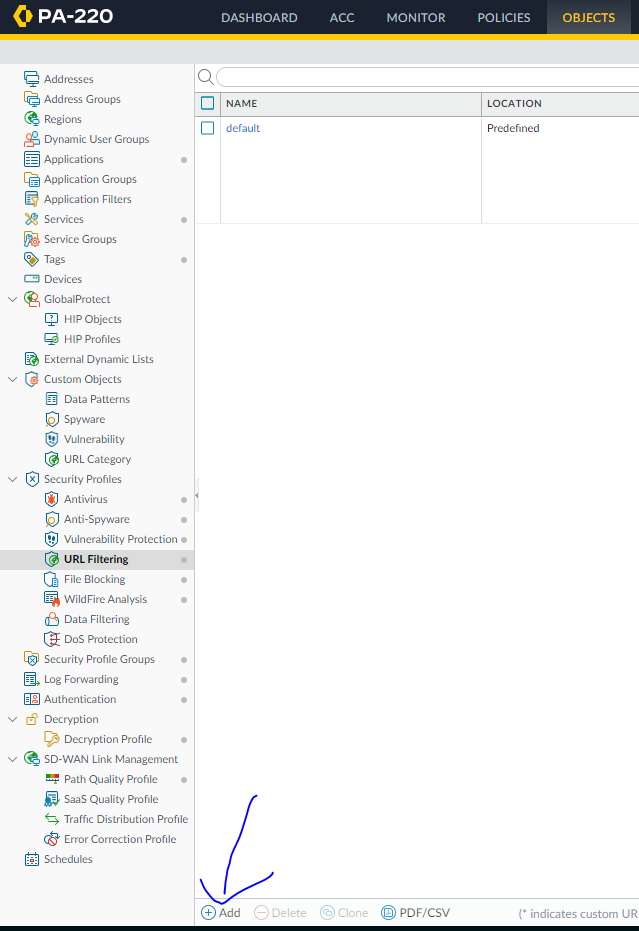
Advanced URL filtering classifies websites based on site content features, and safety, URLs can have up to four URL categories including risk categories which are high, medium, and low and that means that the site will expose you to threats and how likely you will get those threats from visiting that site. And with advanced URL filtering it will allow you to have real time analyses of the websites you visit which basically makes it so that the gap that normal firewalls have when the scan the website the advanced version eliminates that gap and will allow way better safety from some of the best hackers, and they are continuously updated to detect various malicious URLs and phishing web pages.

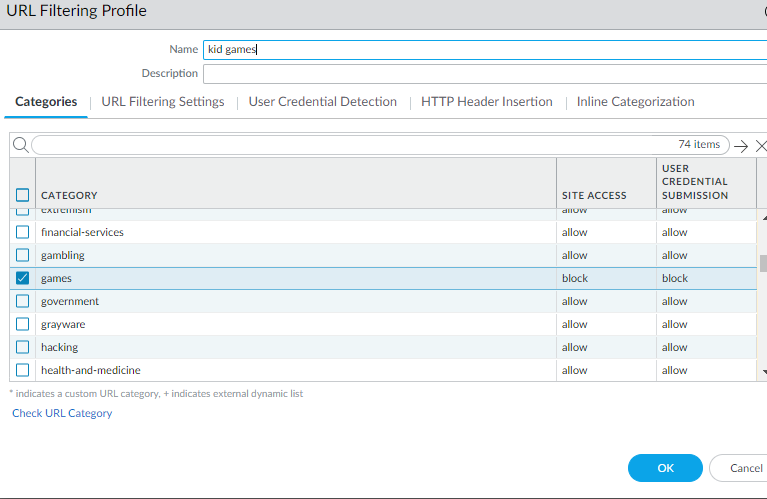
Firewalls the are made to analyze URLs in real time using machine learning provides an additional layer of protection against phishing websites and JavaScript exploits. And when a fire checks for a URL its also looks for critical updates such as URLs that previously qualified as benign but are now malicious which is a super useful feature advanced firewalls offer. And if you don’t trust/ are skeptical about the site that the software categorized a site incorrectly you can submit a category change request in your browser through a test A site or directly from the firewall logs

**Steps**

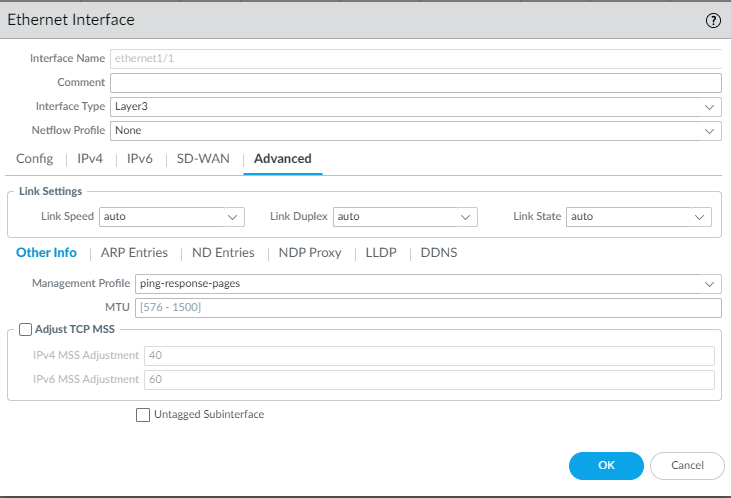
#1 go to https://urlfiltering.paloaltonetworks.com/ and look at the website to see the category of it so you can block that category of websites.

#2 go to the objects tab on the top then find URL Filtering on the left of your screen then click add



#3 Name your profile then select the category of the website you want to block 

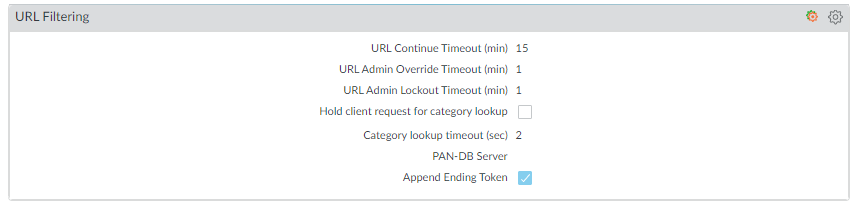
#4 Go to network 🡪 interface 🡪 ethernet 1/1 🡪 advanced and configure the following

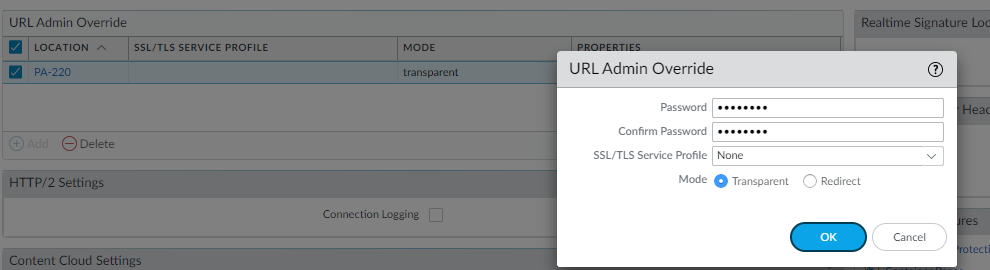


#5 Go to policies 🡪 security 🡪 actions and configure the following

Go to device 🡪 Setup 🡪 content-ID and change the URL filtering to what you want

(for example we have the block screen appear every 1 minute)



#6 Go to device 🡪 Setup 🡪 content-ID and find URL Admin override click add then configure the following to your liking 

#7 Commit

**Problem:**

we set the URL filtering to override and block but we had to change it to override and allow so that we can see the override screen instead of taking us to the “This page can’t be reached”. We also had and issue that is would only work sometimes but we had to filter without a certificate and that made it work 100% of the time

**Conclusion:**

URL filtering and overriding is important so that a office/enterprise company can be safe so they do not have to worry about people doing things on their network that they don’t want to happen