**palo alto Url filtering and override**

Derek Liu Cybersecurity Period 5

Lab #4

**URL Filtering and Override on a Palo Alto Firewall***Derek Liu*

Purpose

The purpose of this lab was to filter URLs in groups and also configure an option to override the filter for specific types of URLs if the user has a pre-shared password.

Background Information

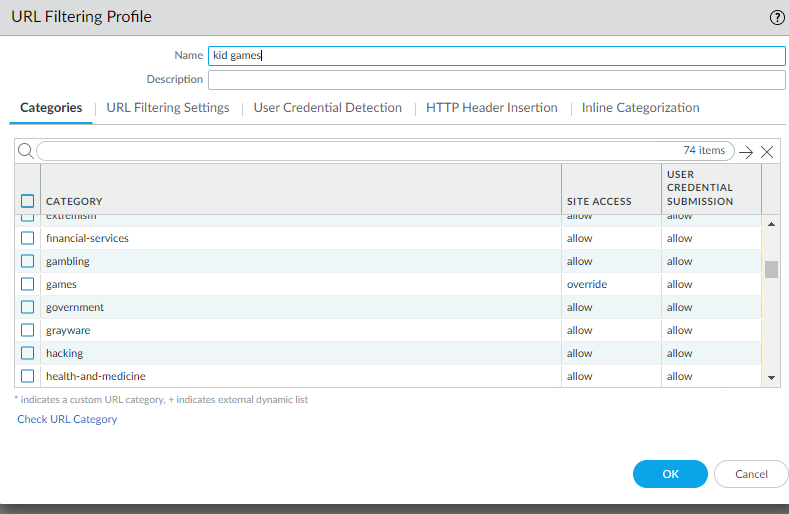
When configuring a firewall for a SOHO network or even a company, it is good practice to filter out harmful or potentially harmful websites on the internet. Using the Palo Alto firewall, there is an option to filter out groups of URLs ranging everything from “malware” to “home-and-garden”. In this lab we will be blocking all websites that belong in the category of “online games” to prevent off-task behavior during work. We will also configure an option to override the filtering of the website if a pre-shared password is provided.

The lab will be done without using certificates. A URL group will be selected to be blocked and then applied to an interface management profile and security policy rule. After typing in the pre-shared password, the override will be done in transparent mode which means that the user will be take directly to the site that was originally blocked.

Configurations

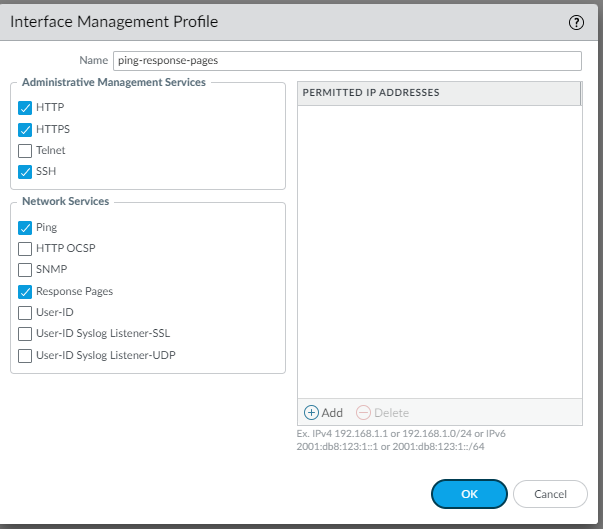
1. The first step would be to choose a website that you would want to filter on the firewall and then find what category it belongs to using the following website: <https://urlfiltering.paloaltonetworks.com/>
2. Go to Objects -> URL Filtering -> and click “add”

Configure the following:

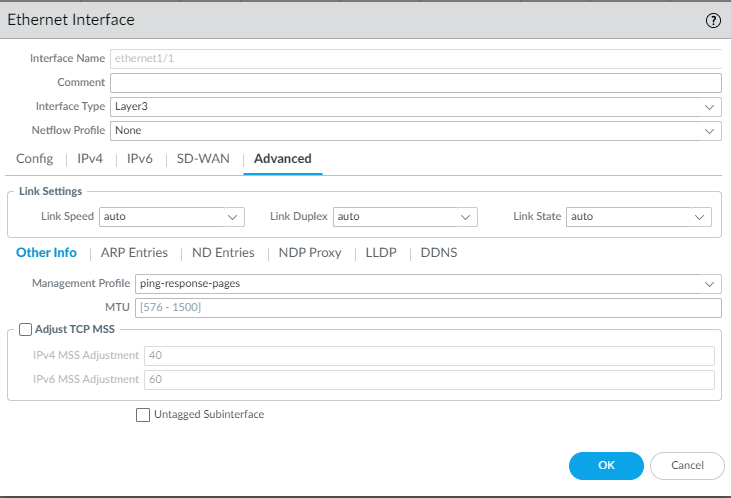


1. Go to Network -> interface management and click “add”

Configure the following:

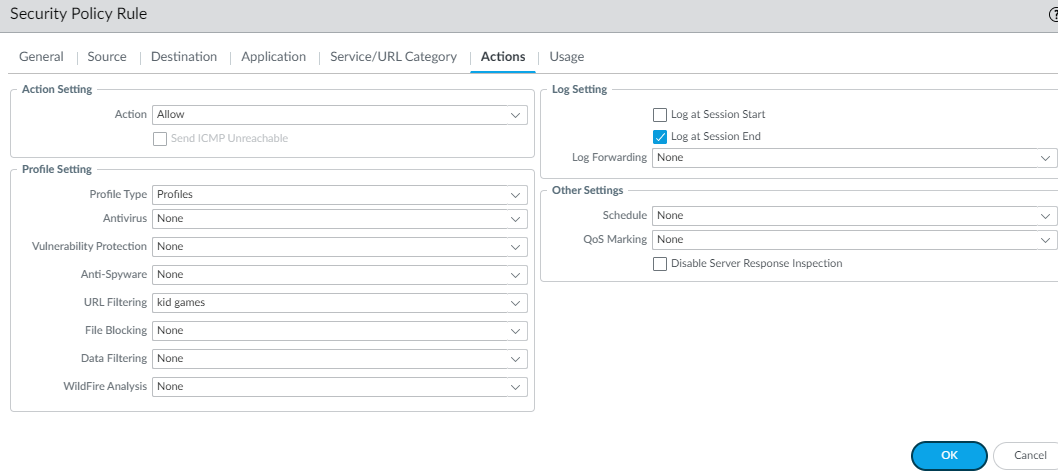


1. Go to Network -> Interfaces -> “ethernet 1/1” -> Advanced and configure the following

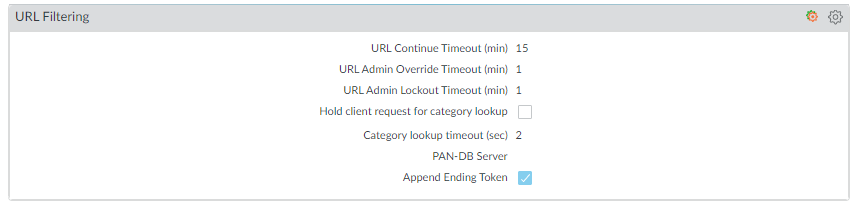


1. Go to Policies -> Security -> “Internet Outgoing” and go to “actions”

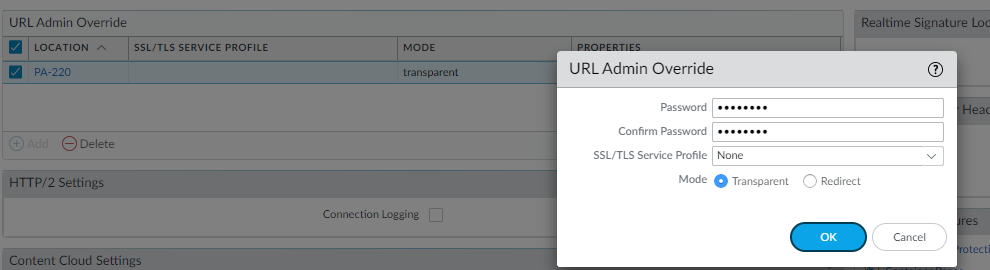
Configure the following:



1. Go to Device -> Setup -> Content-ID and change the URL filtering to what is desired. We configured the following to have the block screen appear every 1 minute:



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



1. Commit Changes.

Problems

Originally, we tried to configure the URL filtering to “override” and “block”. This didn’t let the override screen appear and when an online game website was opened it took us directly to a page that said, “site can’t be reached”. This was fixed by changing the configuration to “override” and “allow”. We also originally configured a certificate that allowed the filtering to work some of the time for http website but wouldn’t function for https websites. This was fixed by removing the filter and having the firewall filter without a certificate.

Conclusion

URL filtering and the URL override feature were implemented on a PA-220 firewall in this lab to block online games. This was necessary to both show the capabilities of the firewall and prevent users from potentially dangerous websites. However, if the user were to intentionally want to access a website given that it was filtered, they would be given the option to enter a pre-shared password to gain access to the website.