Lab 4 – Url filtering and override

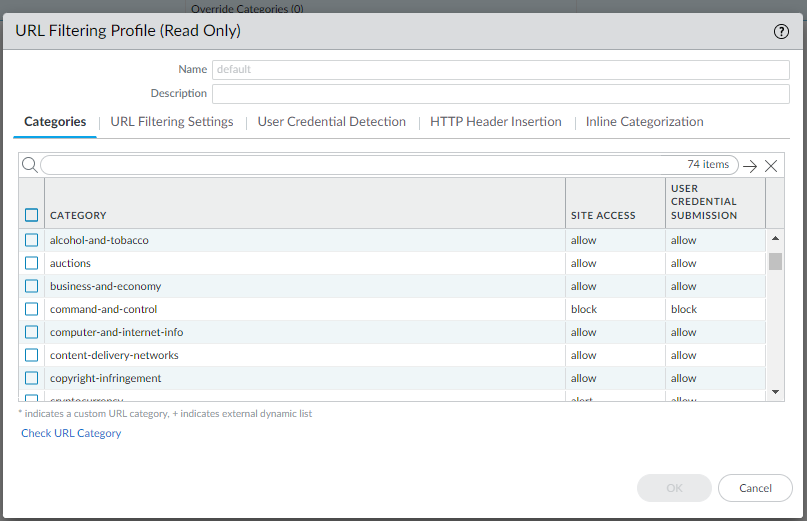
Background: This is the first ever time we used a function of the firewall to do something practical. The goal was to find documentation online that could help us do that. The purpose of this lab was to filter certain categories of websites and block them. Then. make it possible to enter a password to override the block. We were finished setting up the SOHO configurations of the firewall at this point and were on the latest version, meaning that we were now completely ready to start using the features of the firewall, such as url filtering and overriding.

The way overriding works is that you have to place the firewall between your pc and your gateway. Then, any time the user tries to go to a website that the firewall does not want you to go to, it blocks it and prevents your request for that website get through to you gateway. Note that the heavy lifting here is being done by the firewall, the router does not care which website you go to and cannot block it, it is the firewall.

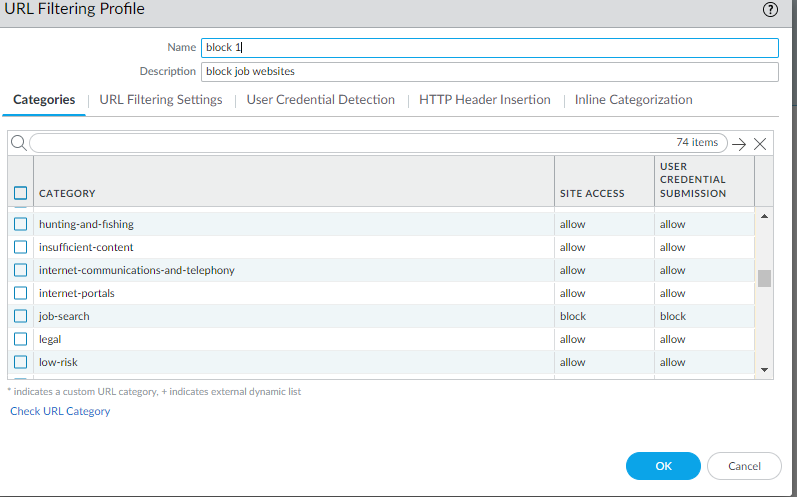
An example of this could be a school. You would not want students using laptops in a school to be able to go to gaming websites or pornographic websites. The easiest solution to this would be installing a firewall before the gateway so that the web simply does not any user to go to the gateway. However, for some rare exceptions, the network administrator of the school might want to go to a blocked site on a student’s computer, in which case it would be appropriate to allow for manual overriding so that the administrator can enter a secured password which can enable him to do what he wants to do.

Lab Summary:

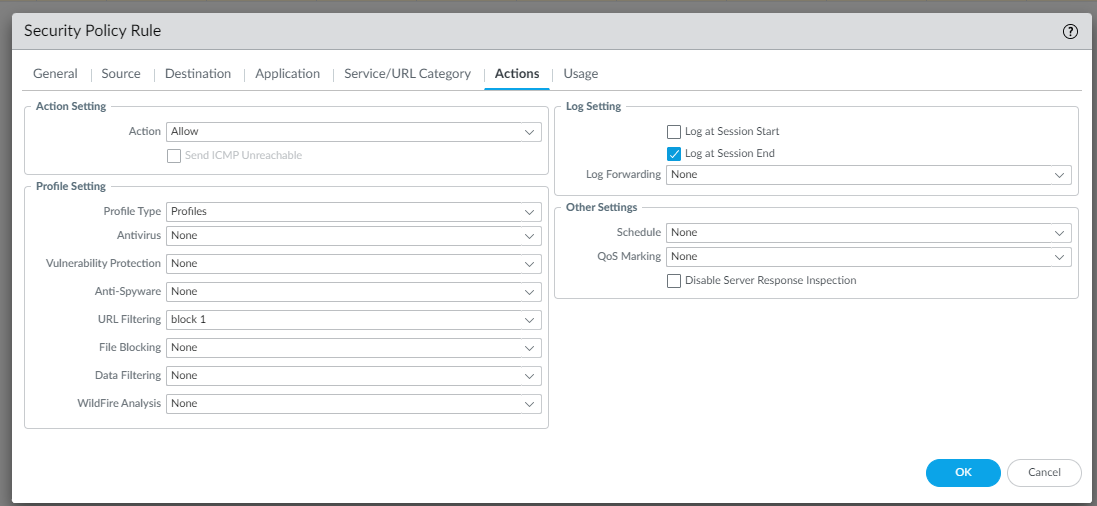
Step 1: go to network > url filtering and click the default to see the categories of websites that are already blocked.



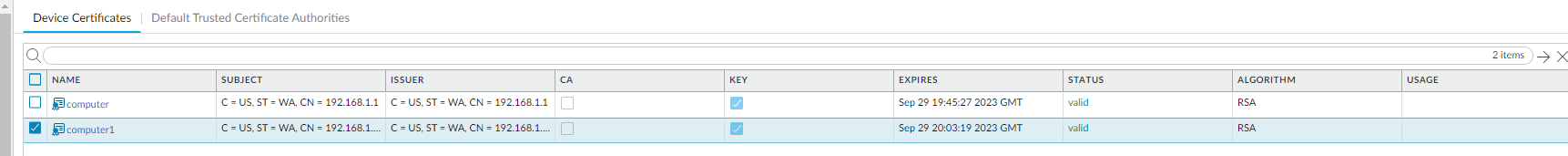
Step 2: Click add. Name the profile anything and pick a category to block. Under site access, select override for that category and under user credential submission select allow.

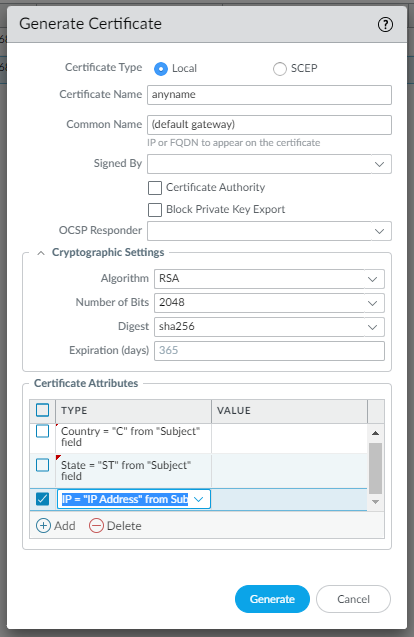


Step 3: go to policies > security > and go to internet outgoing. Go to actions and under url filtering, select the profile you just created. Click ok.



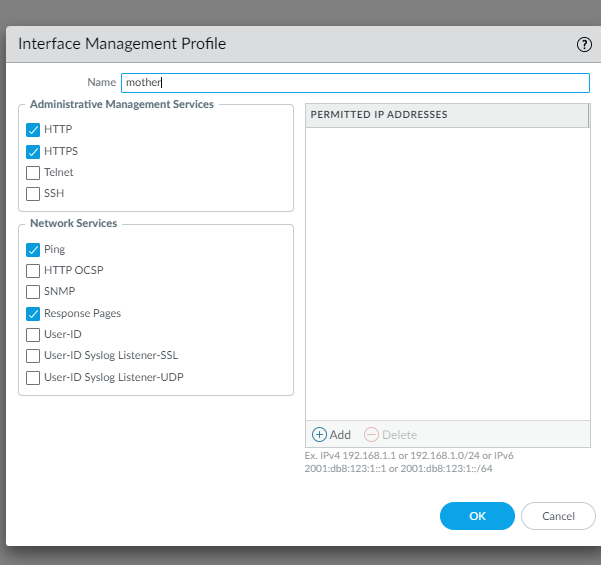
Step 4: go to device > certificates. Click generate.





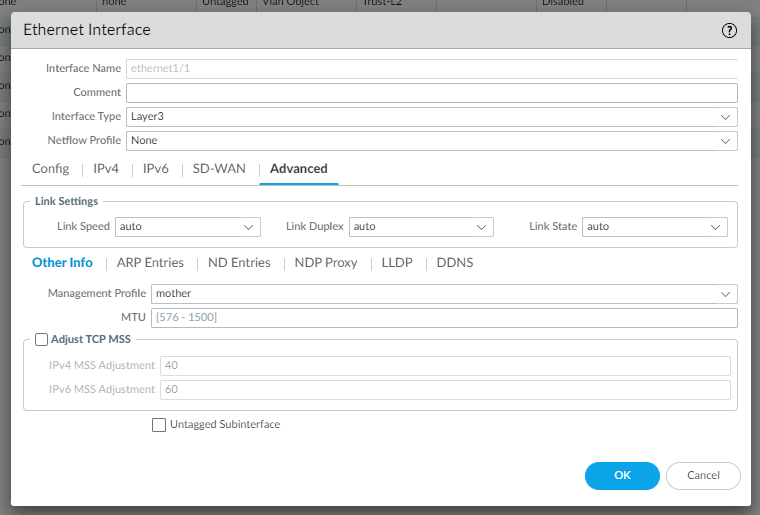
Use these to make your certificate

Step 5: go to network > interface management. Click add.



Use the following to setup management profile

Step 6: go to network > interfaces and ethernet. On your layer 3 interface, go to advanced. Apply the management interface that you just created to management profile



Problems: For a very long time, we tried going to device > response pages and tried configuring override on URL filtering Continue and Override Page. This was a massive waste of time because there is no way to configure anything on this page, you can only use what is preconfigured.

A problem that we had to solve through trial and error was that we were what combination of block and continue we had to put on the url filtering profile page. After a couple of times of committing changes and testing whether url filtering override would work, we figured out that site access should be block and user credentials should be on continue to make it so that you get a warning on a blocked website before you try to manually override it.

Finally, the biggest problem, and kind of an unresolved one was that despite selecting https on out interface management profile, our url filtering did not work for https sites; it only worked for http sites. We tried several things, such as importing licenses and generating out own self singed ones and applying them to our pcs. However, none of this worked and applying those licenses caused even http blocking to stop working. We eventually had to remove those licenses and delete them completely to get to where we were before.

Conclusion: This lab gave us a basic idea about one of the most powerful and useful functions of firewall. Even if this was a very basic configuration, it kind of helped u