URL Filtering

*Palo Alto*

Adv Cisco Cybersecurity – Lab 4

Jason Liu

Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

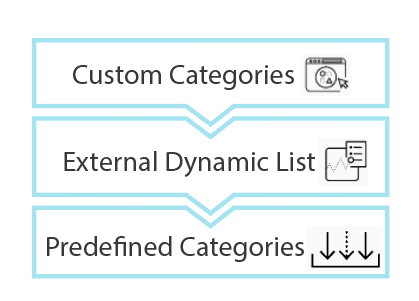
*Lab 4: PA 220 – URL Filtering*

**Purpose**

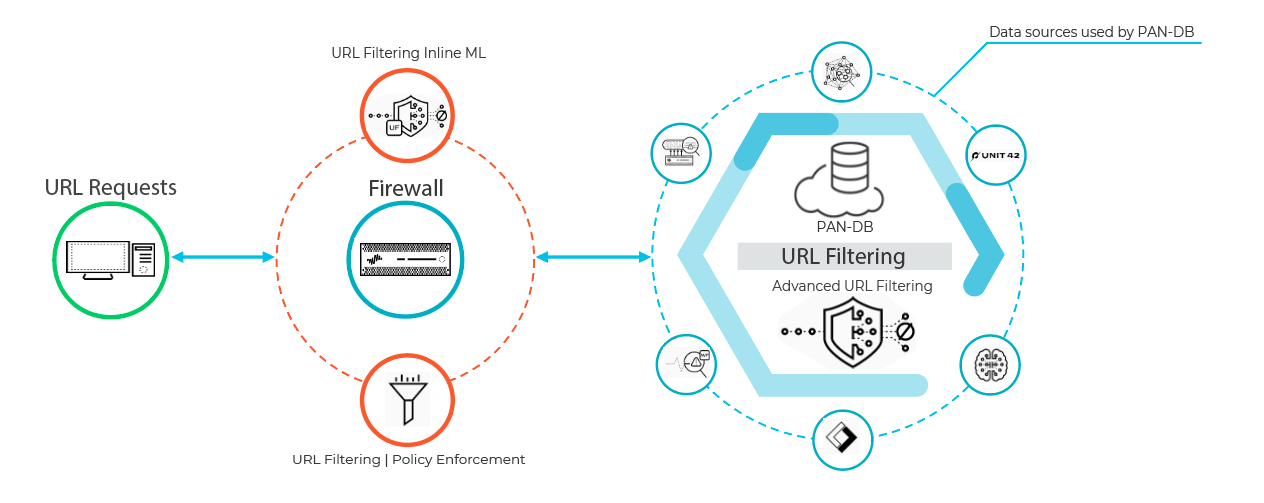
The objective of this lab is to update and create URL Filtering Policies to deny access to a specified site category. Afterwards, Admin Override must be configured to allow access to those denied categories if a created password has been correctly entered.

**Background Information**

URL filtering is a fundamental and powerful tool on firewalls. It allows the ability to monitor and restrict sites users can access, either through specified URLs or through whole categories. Categories are defined by Palo Alto’s PAN-DB, their Advanced URL Filtering URL database, which sorts sites to predefined categories based off of site content, features, and safety. A user can also create their own categories called Custom Categories, or access categories from external Dynamic Lists (a text file from external servers that import IP addresses, URLs, and domains). URLs also have risk categories, defined as High, Medium, and Low. URL categories can be tested using this palo alto site: <https://urlfiltering.paloaltonetworks.com/query/>.



Palo Alto’s order of priority for comparing a website’s URL category to entries in Custom Categories, then External Dynamic Lists, and lasty the default predefined categories.

 Advertised to defend against threats and provide live analysis within its array of applications such as Unit 42, Wildfire, passive DNS, Palo Alto Networks telemetry data, and Cyber Threat Alliance data, it should be noted Advanced URL Filtering is a paid feature. According to its online documents at <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/url-filtering/pan-db-categorization>, the process can be visualized by a firewall and database 2-segment process:

URL request passes through Palo Alto’s defensive services.

On the firewall, policies and filtering are enforced.

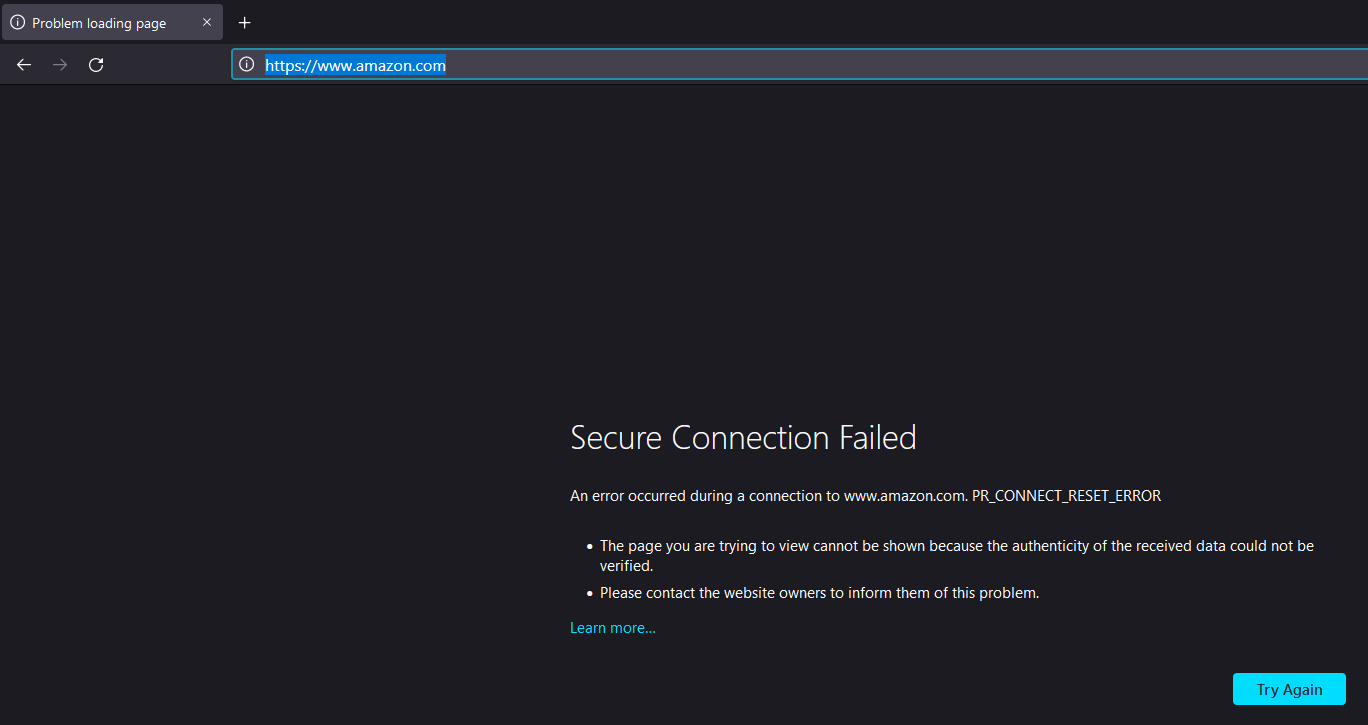
In the PAN database, information services sort and monitor content.

Without paid, advanced URL filtering features, simple site categories can still be blocked by applying a URL filtering profile onto a Security Policy rule. Admin Override can also still be applied for sites under URL categories with the Site Access option “Override” selected.

As a reminder, Security Policy rules are the building block of cybersecurity. Those configured rules, under certain conditions, determines whether to block or allow the session. Applying URL filtering configuration to the rule on an interface, such as one that outgoes to the internet, adds a layer of depth and decision for the Security Policy.

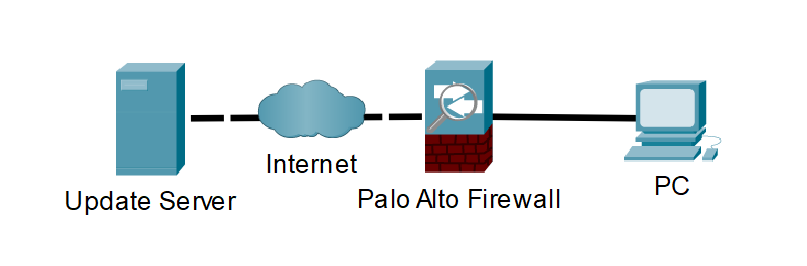
**Lab Summary**

In the same SOHO configuration setup as done in *Lab 2: SOHO Configuration*, the LAN’s PC should have direct access to the internet through wired connection via the firewall. Assuming updates and licenses are complete and the Management interface is reachable, start by accessing the webGUI.

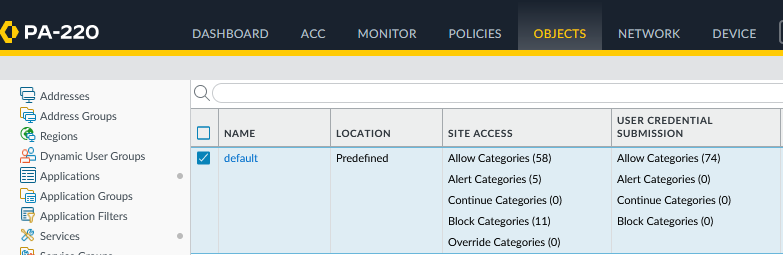
 Under the Objects > Security and URL Profiles, create a Profile and select the categories that you wish to modify. By default, all categories are allowed, so change access rules to target categories to be restricted, either under the “block” or the “override” option. We first did the “block” option to test if the rule is effective, but later moved to “override” for Admin Override configuration. Sticking with the “block” option first, save the Profile and navigate to the Security Policy Rules. Under the internet outgoing rule in use, edit it to use the URL profile for “URL filtering” under the Actions tab. This applies our configurations to the Security Policy. Commit changes. You can now notice that shopping sites are now blocked.

A shopping website, like Amazon, has been blocked by the firewall.

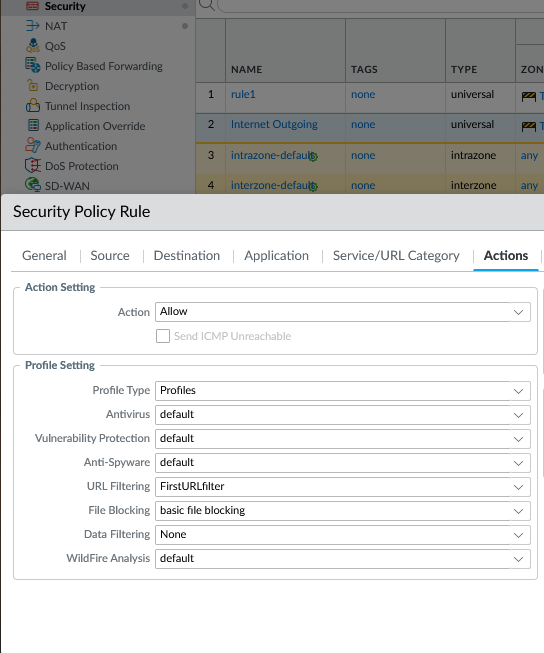
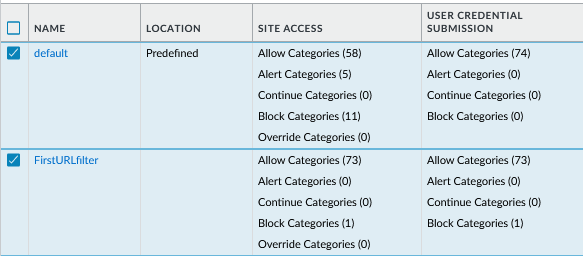
Returning to the URL profile configuration, change Site Access to “override” for both drop-down menus, including the user credentials. Under Setup > Content-ID, Add an Admin Override configuration, adding a password. Select transparent, as there is no need to redirect blocked sites to another address. Commit changes. Under Shopping websites, it now gives an advanced options to continue by entering a password. If override is activated, all sites are clear of restrictions for a set amount of time (default of 15 minutes). The scope of these sites is explained under the *Problems* sections. Example can be seen in *Configurations* below.



Firewall has is in Layer 3 mode to interact with internet connections to and from the PC client.

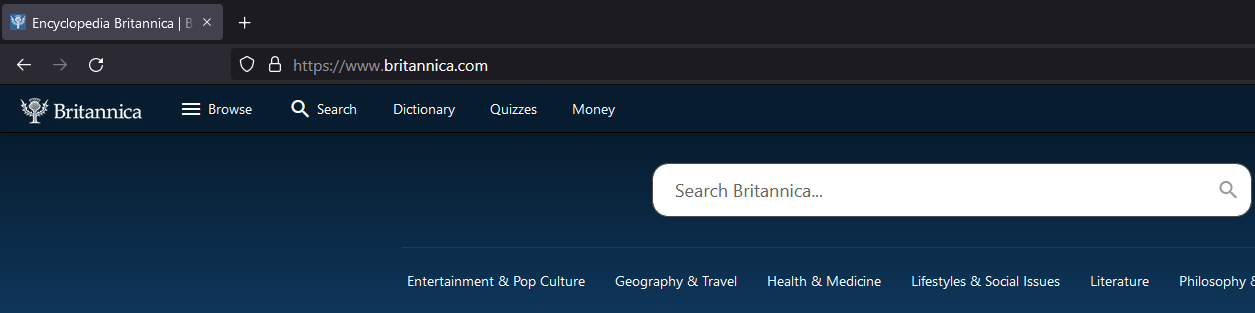
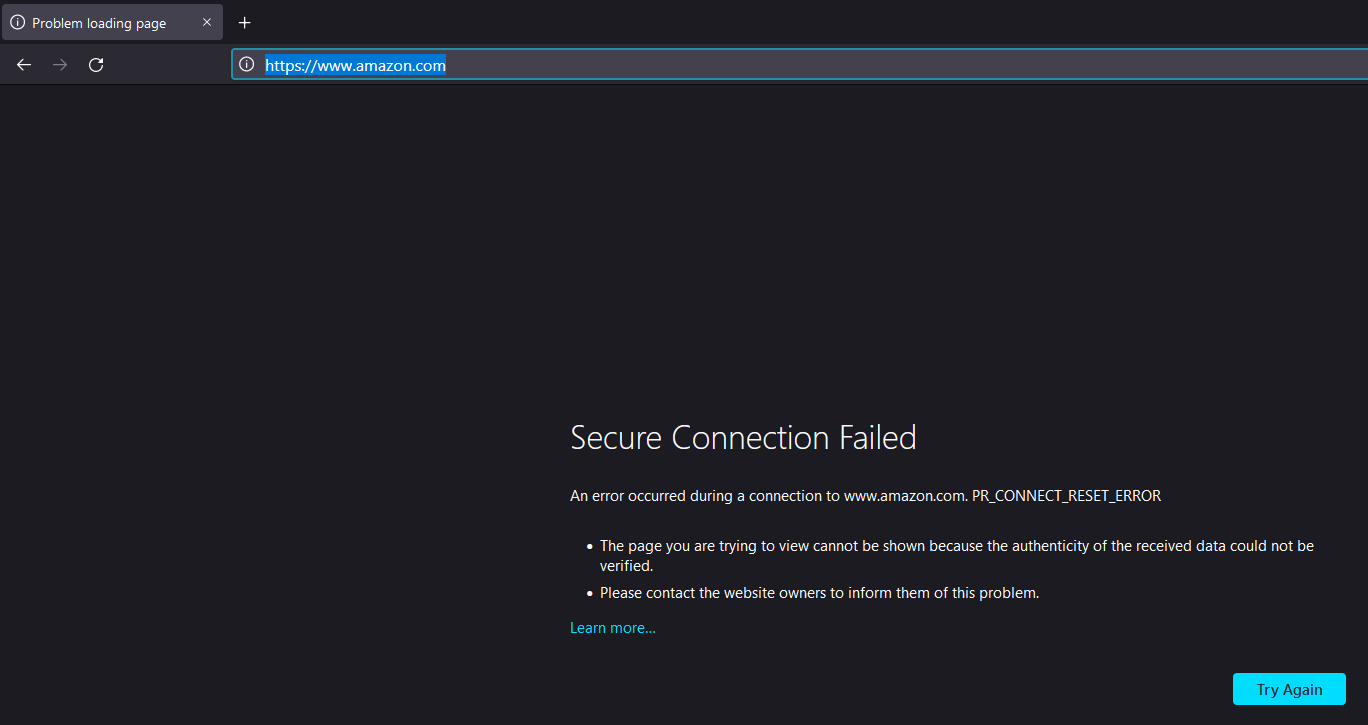
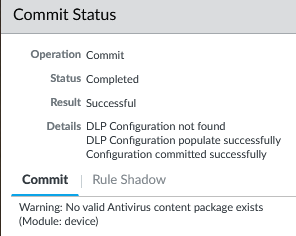
 **Configuration**

Under Objects, navigate to Security Profiles and URL profiles. A default security profile should already be configured.

****

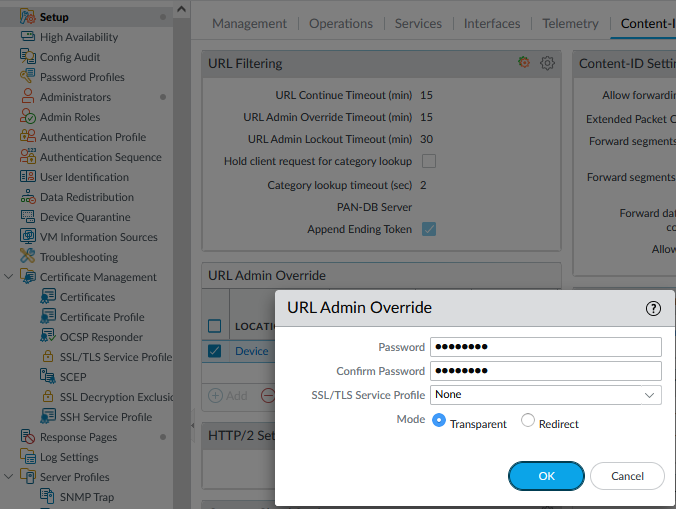
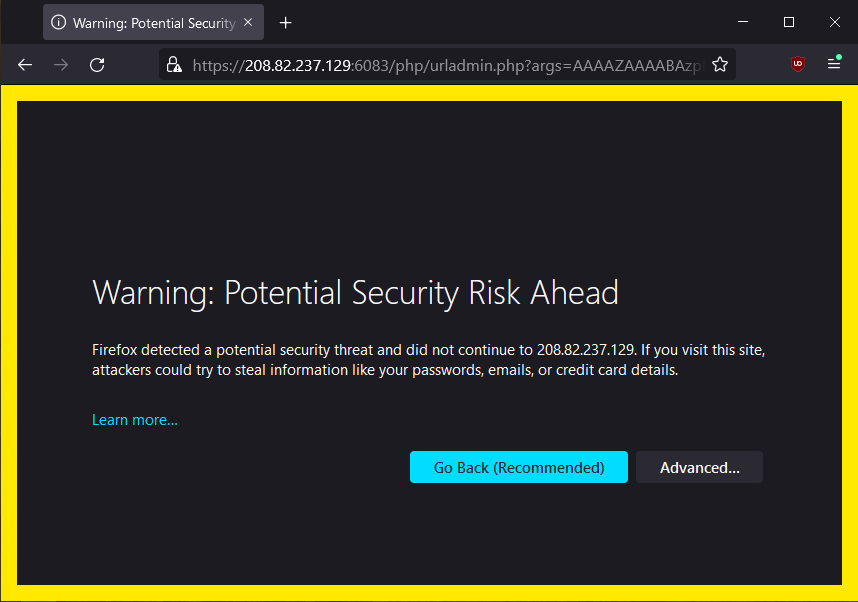
Apply the profile to the security policy rule at the “URL filtering” menu of the actions tab.

Create a profile that blocks targeted categories. Only the “shopping” category has been blocked for to see the specified desired results. This profile has been named “First URL filter.”

****

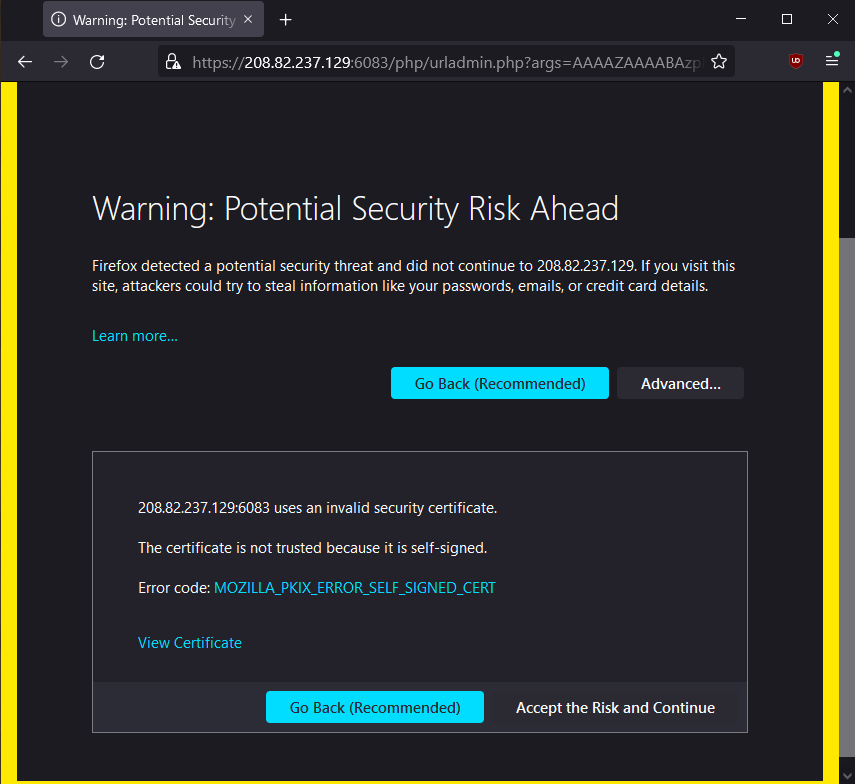
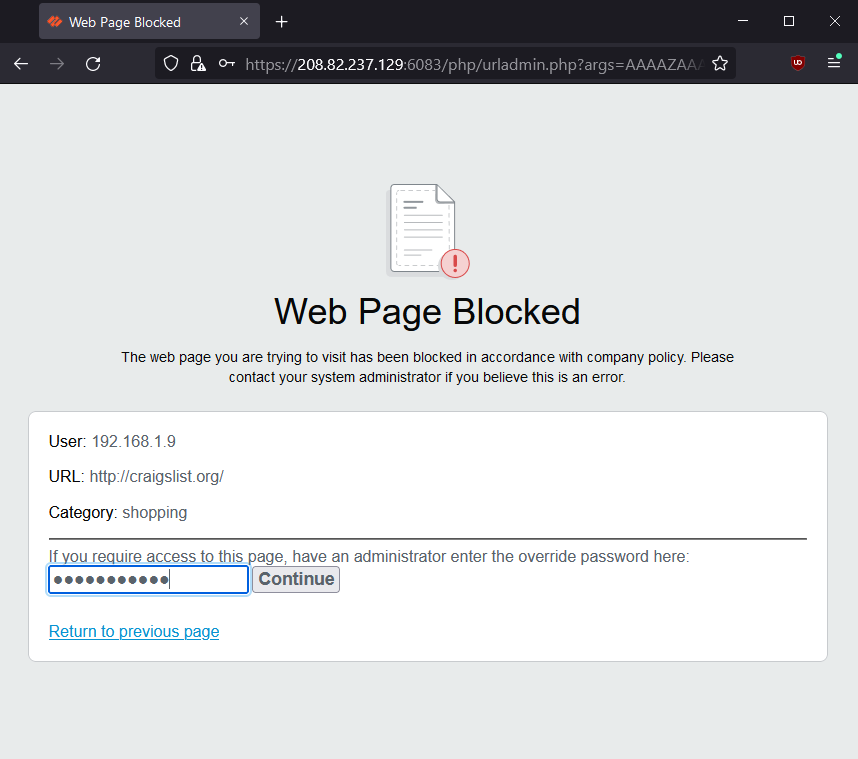
Other site categories, like “educational” are still allowed access.

After committing changes, shopping sites like Amazon are blocked.

****

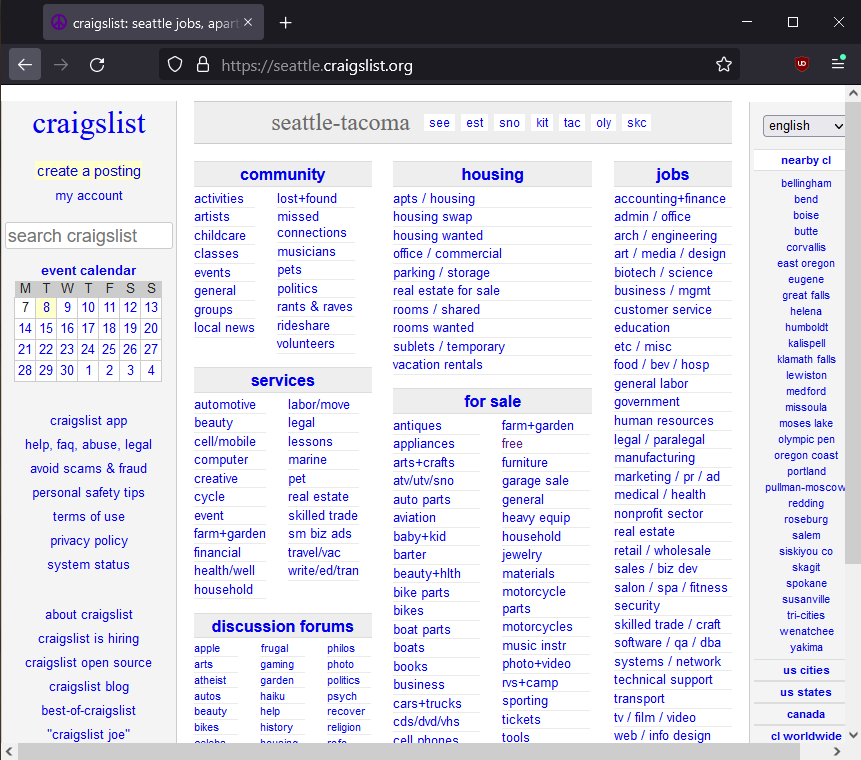
Shopping sites are blocked but allow an “advanced action.” Craigslist was attempted to be accessed here.

After changing the site access and user credential submission to “Override,” move to URL Admin Override under Setup > Content-ID and configure an Override password. Select Transparent mode. We should not redirect to any other address.

****

It will ask for admin override password. Enter it here.

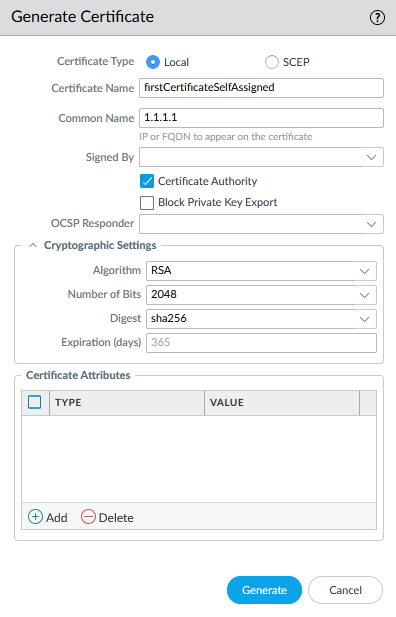
The URL Override is causing this message. Accept risk and continue.

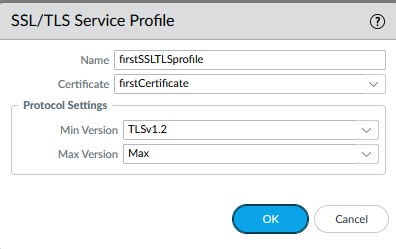
****

A shopping site, like Craigslist, has been entered via Admin Override.

**Problems**

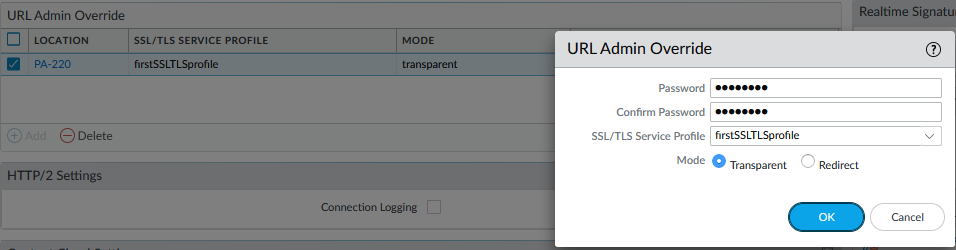
The problems that we came across had many variables, inconsistencies, and lack of success that blurred the solution. Minor problems could be quickly identified and adjusted, like how the URL profile applied to the internet outgoing interface we made did not affect the internet going of the internet. The simple solution was that the default interface created by the firewall was named “rule1,” is the outgoing interface that functioned properly. Applying the URL profile onto the proper outgoing interface allowed us to see the results of the filtering, and having sites blocked.

 The greatest issue was the assumption that Admin Override functions for the secure HTTPS protocol websites. From trying Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates, creating self-assigned certificate hosts, redirecting addresses, and even reducing the Admin Override timeout to minimize waiting time – nothing worked. Our lab director and teacher Jeffrey Mason also did not recognize the unique attribute of HTTPS to reject Admin Override. The firewall continued to only block the site. Few resources on forums and sites give insight to this issue. For time efficiency, as long as HTTP (non-secure) sites could allow Admin Override for the site category, the lab was considered effective and complete. For documentation purposes, the following is the process in SSL/TLS certificate creation: [docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service-profile](https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssltls-service-profile)



Create a self-assigned certificate, which acts as a certificate authority.

Afterwards, create the SSL/TLS service profile.



Lastly, associate the profile with the Admin Override configuration. A SSL/TLS profile has been assigned.

**Conclusion**

URL filtering changed my perspective on firewall usage. It gave control and direct manipulation of websites on an internet browser, which has never been interacted with in any of the prior labs. Giving a sense of Palo Alto’s industry use and ability, URL filtering was a great opportunity and feature to explore. I wish further research can be done on under-recognized aspects like SLL/TLS profiles and self-assigned certificates, to give explanation and detail to why HTTPS sites can be blocked yet do not allow Override.