

Palo Alto URL Filtering and Overriding

Evan Choi | Cisco Cybersecurity | 1/31/2023**Purpose**

The purpose of this lab is to create URL Filtering Policies to deny access to specified website categories. After, Admin Override will be configured to allowed users who enter the correct password access.

**Background Information on lab concepts**

URL filtering is an important tool to use on firewalls. It allows network administrators access to monitor and control the sites users can access by either restricting certain URLs or by restricting whole website categories. Once Advanced URL Filtering is enabled, URL requests are compared with Palo Alto’s PAN-DB URL database, which classifies websites based on the content in their site, features, and safety. URLs also have different risk categories which are High, Medium, and Low.

There are many ways that you can use URL Filtering. You can control web access based on URL category by creating a URL Filtering profile, which defines an action for a certain URL category. A profile will be attached to a policy rule, which a firewall will enforced based on. You can also use URL Filtering to do Multi-Category URL Filtering. URLs can have four categories, which allow network administrators to control how users interact with online content. This could be seen in an organization, where employers see specific URL categories as risky, but don’t want to block them because they could provide important resources or services to their employees. Using Multi-category URL Filtering, they can allow users to access these websites while also protecting their network by decrypting all network traffic and making content read-only. Administrators can also create custom URL categories by selecting Category Match and defining two or more PAN-DB categories. URL Filtering can also be used to block or allow corporate credential submissions based on URL category, where administrators can prevent credential phishing by controlling submissions based on URL category. This can be used to block users from submitting to malicious sites, warn them from submitting to unknown sites, and allow them to submit to corporate sites. Safe Search settings can also be enforced using URL Filtering. This allows administrators to filter images and videos that may not be safe for work. There are also other uses of URL Filtering, such as allowing certain users access to sites with a password, blocking high-risk file downloads, and enforcing security, decryption, authentications, and QoS policies.

**Lab Summary**

In this lab, we used a Palo Alto PA220 firewall and 3 ethernet cables to connect the firewall to internet and jumper the management port to LAN. Afterwards, we accessed the webGUI to configure URL Filtering.

We first created a Profile and selected the different categories we wanted to modify. Categories are allowed by default, so we changed certain categories to be restricted by using either the block or override option. We then saved the profile and edited the internet outgoing rule to use that profile for URL filtering. After testing, we were able to see that any sites in that category were blocked. We then changed the Site Access to override and added a password. After committing changes, we tested going to a shopping website under the category we blocked, and upon going to the website, it was blocked but allowed for us to enter a password to access it.

**Network Diagram**

A picture containing diagram

Description automatically generated

**Procedure**

1. Under the **Objects,** go to **Security Profiles** and **URL profiles**. The default security profile should be selected

Table

Description automatically generated

1. Next, create a profile that blocks your targeted categories. We named this category **First URL filter** and blocked the **shopping** category.

Table

Description automatically generated

1. In the **URL filtering** menu in the **actions** tab, apply the created profile to the **security policy rule.**

Graphical user interface, table

Description automatically generated

1. In the top right, press the **Commit changes** button. A successful commit will look like this.

Graphical user interface, text, application

Description automatically generated

1. Now, check to see if shopping websites are blocked. Go to your browser and enter a shopping website in the search bar. We searched for Amazon. You should notice that you cannot access the website, while other websites such as Britannica, an education website, is still allowed.

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. Now, change the site access and user credential submission to **Override.** Go to **Setup** and click **Content-ID** and go to **URL Admin Override.** Create an Override password and select **Transparent** mode.

Graphical user interface, text, application

Description automatically generated

1. Go back to your web browser and enter a shopping website into the search bar. We looked at Craigslist this time. You will notice that it is blocked but you have the option of clicking **advanced action.** Click the **Advanced** option and click **Accept the Risk and Continue.**

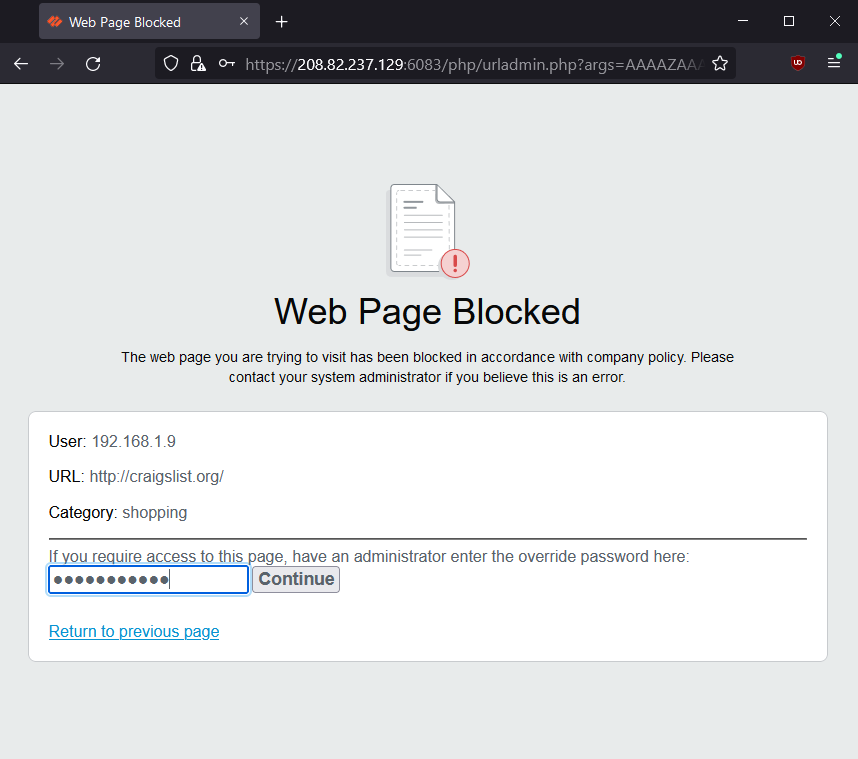
Graphical user interface, text, website

Description automatically generated

Graphical user interface, text, website

Description automatically generated

1. You will be asked to enter the admin override password. Enter the password you set.



1. Press **Continue.** If the right password is entered, you will gain access to the website.

A screenshot of a computer

Description automatically generated

**Problems**

We had some problems in this lab, but most were small. These included our URL profile not affecting the internet going out of the internet. We were able to fix this by assigning our URL profile to rule1, which was the default interface created by the firewall.

The bigger problem we had was that we thought that Admin Override functions for HTTPS protocol websites. We tried creating Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates, creating self-assigned certificate hosts, reducing the Admin Override timeout time, and redirected addresses, but we weren’t able to override a website block. We figured that as long as we tried to access HTTP sites, we were able to override it.

**Conclusion**

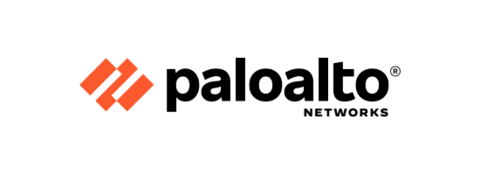
URL filtering allows network administrators access to monitor and control the sites users can access. In order to create a URL Filter, you must access the Palo Alto GUI and go to the URL Filtering Tab under Security Profiles. Although having problems with Overriding, we were able to troubleshoot and figure out why it wasn’t working. Through this lab, not only learned what URL Filtering is and how it works, but I also learned how to configure it and troubleshoot any problems I had along the way.

The stamp below recognizes that

Evan Choi

has completed

**Lab 4 – URL Filtering and Overriding**

 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

Period 5

Letter

Description automatically generated