A close-up of a sign

Description automatically generated

**Purpose**

This lab covers the basics of URL filtering, used to prevent access to specific sites and protect users from digital threats and malware. The skills learned in this lab are commonly implemented in real-world school or office environments as an important safety measure.

**Background Information**

To begin this lab, we first set up a SOHO network, which is a skill we learned in a previous lab. SOHO networks are often at risk of cyberattacks, and in such small network environments, users may not have the same cybersecurity expertise compared to larger organizations. The SOHO network was ideal for our small lab setting, and emulated larger, typical networks used in school/office spaces. These kinds of networks are largely supported by security features such as URL filtering, the method of preventing certain types of content from reaching end users.

URL filtering is essentially restricting access to specific websites and content categories on the Internet, through their URL. URL filtering aids the prevention of phishing attacks, unplanned downloads, and bandwidth waste. Content categories such as social media, entertainment, shopping, etc. are reviewed by administrators, and based on the scenario or company policy, they can choose to filter access to specific domain names, keywords, categories of websites, or block a site for a set time or location. The concept of URL filtering originates from early efforts to boost employee productivity and bandwidth control and is currently used as a common safety measure to prevent leaking of sensitive information, system infections, and phishing attempts.

Through URL filtering, administrators can block or allow websites based on content categories in order to improve both security and efficiency of the network. For example, when a company’s administrators use URL filtering, they can block any websites that would possibly steal any classified information for higher data security, or block access to distracting categories such as social media or adult content for the company’s internet usage policy.

Of the PA-220 firewall we used specifically, URL filtering is one of its key features along with its enterprise-level security. The Palo Alto GUI makes the filtering process more efficient, as administrators can create URL filtering profiles to define how network traffic will be handled using Palo Alto’s predefined URL categories. Based on specific scenarios and needs, each category can be assigned an action such as allow, block, continue, or override, which we used to complete this lab. Palo Alto also supports a URL filtering database which automatically blocks harmful websites and inappropriate content in real-time, minimizing security hazards. With real-time responses and ability to quickly block new threats, our PA-220 firewall ensures company protection from cyberattacks.

Overall, understanding how to use URL filtering within a SOHO network helps us better understand how its configuration can be applied to larger enterprise networks, which require further precision with configuration and monitoring. Learning to design URL filtering policies through the PA-220’s firewall features, we can gain a representative view of how this technology contributes to Internet safety.

**Lab Summary**

1. Access the Palo Alto GUI to create an initial SOHO setup by setting up DHCP and NAT on the firewall to set automatic IP addresses.
2. To block certain websites from end users, create a new URL Filtering Profile that blocks content categories, based on your scenario needs.
3. Change the *internet outgoing* security policy rule to URL filter based off of your newly created profile in Step 2.
4. Commit your configuration and test if it works by clicking a link of a category you have just blocked. If successful, you should not be able to access the site.
5. To override URLs, instead of fully blocking them, create another URL Filtering Profile that overrides certain categories.
6. Set your URL override password for later use, as well as URL Continue Timeout and URL Admin Override Timeout.
7. Commit your changes and test a link in the category you have overridden. With your password in Step 6, you should be able to enter the website safely.

**Lab Configurations**

**Part 1: Blocking URLs**

Go to Objects -> URL Filtering

**A screenshot of a computer

Description automatically generated**

At the bottom left corner, click ‘Add’ to create a new URL Filtering Profile to block categories for an elementary school. We named this profile *ElementaryBlocked.*

A screenshot of a computer

Description automatically generated

We will block categories that we believe are inappropriate/unnecessary in an elementary school environment, such as: *abortion, abused-drugs, adult, alcohol-and-tobacco, malware, nudity, social media, weapons.*

A screenshot of a computer

Description automatically generated

Then, click ‘OK.’ The URL Filtering page should now display that there are **8** categories blocked in the *ElementaryBlocked* profile:

A screenshot of a computer

Description automatically generated

Go to Policies -> Security -> internet outgoing

A screenshot of a computer

Description automatically generated

Go to the Actions tab choose *ElementaryBlocked* under the URL Filtering dropdown:

A screenshot of a computer

Description automatically generated

Click ‘OK,’ then press Commit in the top right corner. Make sure your configuration commits successfully in order for your URL filtering to function properly.

A screenshot of a computer

Description automatically generated

To test your configuration, navigate to Palo Alto’s website to find a testing link. Click on the link from the category you have blocked and would like to test. We chose *malware.*

A screenshot of a computer

Description automatically generated

\

If your configuration is successful, the website should be blocked and display like this:

*A screenshot of a computer

Description automatically generated*

**Part 2: Overriding URLs**

Go back to the GUI and go to Objects -> URL Filtering

A screenshot of a computer

Description automatically generated

Click ‘Add’ to create a new URL Filtering Profile named *Override.* For easier testing purposes, we chose to override the *shopping* category since we presumed that other categories such as *sex-education* or *social-networking* could have automatically been blocked by administration.

*A screenshot of a computer

Description automatically generated*

Click ‘OK.’ Go to Devices -> Setup -> Content-ID and change both your URL Continue Timeout and URL Admin Override Timeout to 15 minutes.

**A screenshot of a computer

Description automatically generated**

\

Go to URL Admin Override and set password to *admin:*

A screenshot of a computer

AI-generated content may be incorrect.

Click Commit. Make sure your configuration commits successfully before testing.

A screenshot of a computer

AI-generated content may be incorrect.

When we go to amazon.com, a well-known website within the *shopping* category that we have overridden, we see that the website is blocked. But, we can still enter using the *admin* password that we set up earlier in the GUI.

A screenshot of a computer screen

Description automatically generated

\

With the correct credentials, now we have full access to the website!

A screenshot of a website

AI-generated content may be incorrect.

**Problems**

Initially, we had set a static IP address for our host, but this blocked our connection to the default gateway which interfered with our ability to block certain websites. To fix this issue, we configured a DHCP server and changed our host IP address to be generated by DHCP instead, which allowed a proper connection to the default gateway.

In Part 2 of the lab, when changing some content categories to be overridden instead of blocked, we attempted to override content categories that were likely already blocked by school admin, and therefore were unable to enter the websites at all. We also began by configuring all settings to ‘override,’ which was not effective when committed. Later, keeping *user credential submission* as 'block' and only changing *site access* to 'override' allowed us to successfully override websites.

After successfully overriding a site and entering, the site remained completely unblocked during every attempt after the first time we accessed it. To fix this issue, we set a URL Continue Timeout and a URL Admin Override Timeout, both to 15 minutes, to ensure that the site would require admin credentials to be accessed again after a period of time.

**Conclusion**

URL filtering is an important step to preventing network threats and ensuring a safe, productive environment for all. The skills in this lab cater to all demographics and is a common, practical approach to setting up networks for any kind of organization. URL filtering is a flexible method of security as well, allowing administrators to easily customize filtering behavior based on needs and company requirements.

**Signoff**

A close-up of a document

Description automatically generated