|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto URL Filtering Lab** | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

Purpose

The purpose of the lab was to learn how to set up URL filtering on the Palo Alto (A220) fire wall.

Background information

Palo Alto Firewalls are highly used in Enterprise networks. Compared to other firewall brands, Palo Alto firewalls don’t use up a ton of network bandwidth. And Palo Alto firewalls can even allow a user to monitor, inspect, and protect traffic at a high rate. Palo Alto Firewalls can monitor and control the applications that are allowed to work on a user’s network. And unlike other firewalls, Palo Alto Firewalls don’t identify applications by standard ports. Instead, they identify applications by monitoring all network traffic. And has cloud-based threat protection, for defending your network against almost any attack. By setting SOHO configuration you can Install Licenses Configure Dynamic Updates Configure Interfaces, VLANs, appropriate switch tagging Setup DHCP Server(s) Configure Zones Configure Network Address Objects Create Security Policies Create NAT Policies Ingress and Egress. URL filtering on Palo Alto firewalls allows access to websites, deny access, or have it be overridden by a password. Which websites can be blocked, overridden, allowed, show a warning, or have an alert logged on the firewall.

Lab Summary

### To begin the configurations, you need to first connect a UTP cable from your computer to the Palo Alto Networks firewall. Next configure a IP and netmask for the computer and Firewall. To access the management console, go to a web browser with the firewall’s IP address and type in your password and username. After logging into Pan OS, First, go to Objects, Security Profiles and URL Filtering then, create a URL Filtering profile. Next in the Categories set and define site access for each URL category. Select block to deny access to websites and select override to only allow access if users provide a configured password. For each URL category to which you allow Site Access, select how you want to treat User Credential Submissions. Define URL category exception lists to specify websites that should always be blocked or allowed, regardless of URL category. After completing configurations. save the URL profile and commit changes.

Configurations

Setup URL Filtering:

Table

Description automatically generated

Graphical user interface, text, application, chat or text message

Description automatically generated

Before blocking sites:

Graphical user interface, application

Description automatically generated

After blocking sites:

Graphical user interface, text, application, email

Description automatically generated

Blocked page after being overridden:

Graphical user interface, website

Description automatically generated

Problems

We have not encountered any major problems while configuring the URL filtering lab. But we did encounter some small mistakes during the lab. one problem was after we have set up the URL filtering profile, some websites would not connect after overriding. But we found out that the connections depend on the site we tested it on. So, we were able to fix it by overriding the blocked website category. We fixed the problem by deleting the virtual wire interfaces.

Conclusion

The objective of the lab was to be able to set up or create a URL filtering on the Palo Alto (A220) fire wall. During this prosses of figuring out URL filtering it allowed us to practice familiarizing ourselves with Palo Alto Firewall management console and test out the different functions of URL filtering. During the lab we encountered some small mistakes that we learned from, but in the end, we were able setup URL filtering on the Palo Alto Fire Wall.