Palo Alto Networks Cybersecurity Academy – Setting up Web Filtering

Colin J. Faletto, CCNA

paloalto® NETWORKS

Purpose

This lab serves to expand on the previous Palo Alto lab by teaching CCNP students how to set up the PA220 for a small-scale SOHO network, which is the primary use case for the device. This lab covers skills such as setting up DHCP services and trust boundaries on a router, which are essential for basic network functions and security.

Background

Palo Alto Networks is a networking and cybersecurity company from Santa Clara, California. They are a member of the S&P 500. They focus mainly on the business market, creating scalable security solutions for many of the largest companies worldwide.

The Palo Alto PA220 is a firewall sold by Palo Alto Networks. Contrary to Palo Alto's main market, the PA220 is intended for small office/home office solutions. The PA220 can also be used in a small school environment, as is the case in this lab. Marketed as a NGFW, or Next-Generation Firewall, the PA220 uses machine learning to identify attacks instead of relying on a simple signature check like traditional firewalls. This technology allows the PA220 to identify undocumented threats and brand-new exploits without intervention from Palo Alto networks themselves. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The latest version of PAN-OS is PAN-OS 11.2 Quasar, which was released in May 2024. In this lab, our firewall is running PAN-OS 8, which has reached end of life and is no longer supported.

PAN-OS's GUI has a variety of settings and tools to control advanced functionality of the router. The GUI's default page is a dashboard that displays vital information, such as console messages and link states of ports.

The PA220 is primarily intended for SOHO, or Small Office/Home office networks, which normally have ten or fewer employees and are perfect for small businesses. However, the PA220 also works in small-scale school environments, such as elementary school computer labs. This is the use case uponon which this lab is built.

The PA220 offers a variety of methods to filter and manage inbound and outbound traffic. One such method is URL filtering. A Uniform Resource Locator, or URL, is the primary identifier for hosts on the internet and can be used with a variety of protocols. In this case, the PA220 uses URLs to identify the destination of HTTP and HTTPS traffic.

Another filtering method offered by the PA220 is DNS-based filtering. Domain Name System, or DNS, is a method of mapping user-readable hostnames to computer-readable IP addresses. DNS uses port 53 and is unique in that it can use both TCP and UDP for data transmission. DNS works by having a central server keep a database of

IP-hostname mappings and provide them to clients upon requests. The PA220 can filter through DNS by intercepting these requests and choosing to respond with either a fake sinkhole address or no address at all.

Yet another filtering method offered by the PA220 is application-level filtering. At layer 4 of the OSI model, communication is primarily managed by the Transmission Control Protocol and the User Datagram Protocol, both of which communicate different types of traffic by assigning port numbers to different application layer protocols. Common port number examples are 80 for HTTP, 22 for SSH, and 443 for HTTPS. The PA220 can easily filter this traffic by checking for specified port numbers. Application-level filtering isn't as useful as DNS or URL filtering, as many protocols (DNS, HTTP(S), and DHCP) must be enabled for a network to function properly and most modern programs use HTTP(S) for any network functionality.

Another example of an application with its own port number is IRC. Internet Relay Chat, more commonly known as IRC, is an instant messaging protocol created in 1988 and popularized in the mid to late 1990s. It was created in Finland at the Universituy of Oulu and spread through various universities before eventually becoming popular with the general public. Nowadays, the protocol isn't commonly used for messaging, being replaced with web-based chat apps like Discord, Slack, and Microsoft Teams. However, IRC maintains a small cult following and has several active servers that keep it alive.

Lab Summary

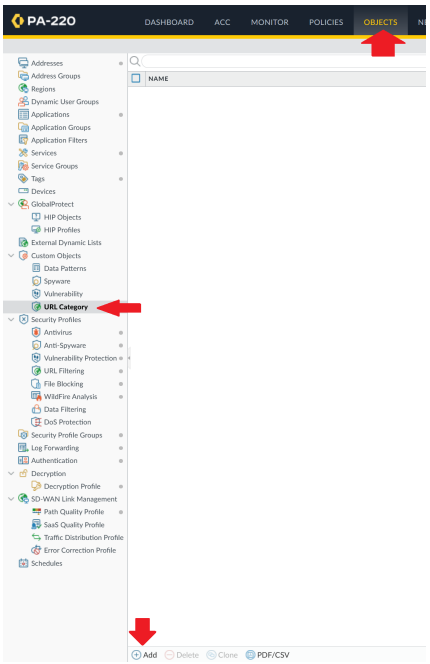
In this lab, we set up three different types of web filtering: URL filtering, DNS-based filtering, and application-level filtering. For URL filtering, we blocked all pre-defined categories that weren't appropriate for a school environment and created a custom URL category (adobe.com) that was blocked by default but could be overridden with a password. For DNS-based filtering, we set all requests for harmful/malicious categories to return a sinkhole IP address and alert the firewall. For application-level filtering, we blocked all IRC traffic.

Lab Commands

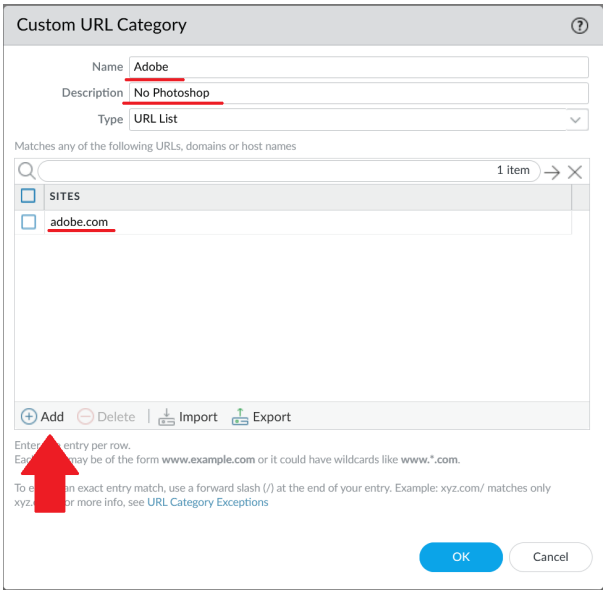
NOTE: These instructions build off of a firewall that already has basic configurations for a SOHO environment. Please refer to these instructions first (https://github.com/faletto/pa220-soho) if you are setting up a firewall from scratch.

URL Filtering

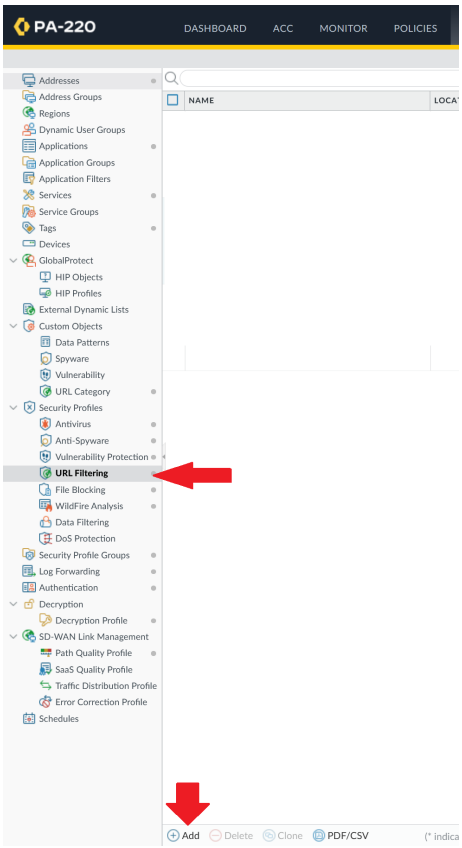
Go to Objects > Custom Objects > URL Category. Click "Add".



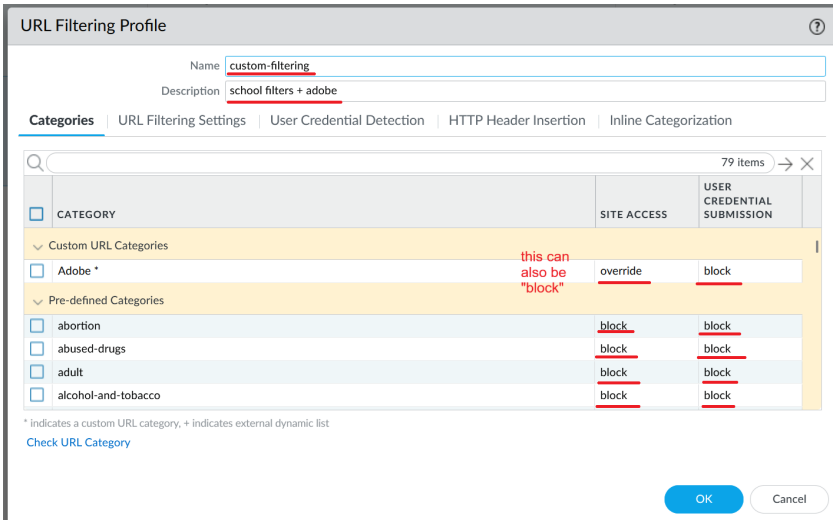
Type a name and description and enter the URL you would like to block. In this case, we blocked adobe.com as an example, despite the lack of malicious content.



Go to the “URL Filtering” section and click “Add”.

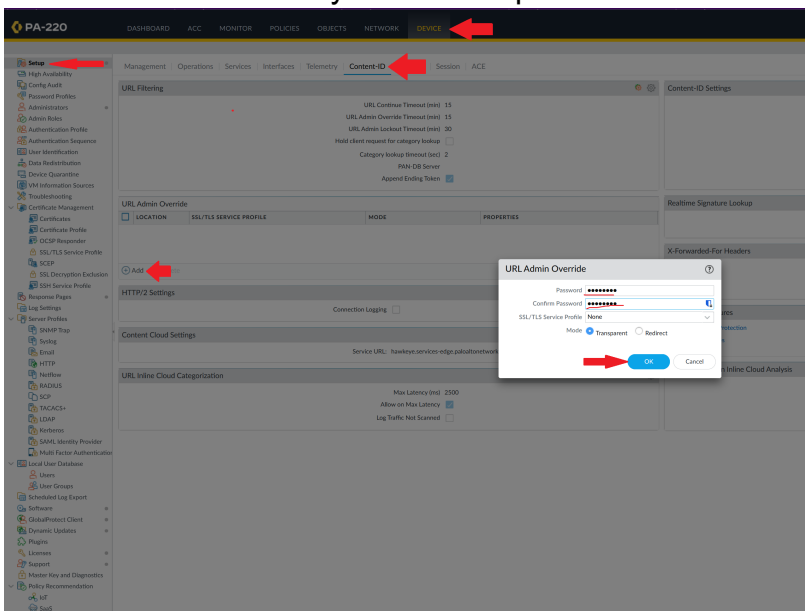


Name your profile and give it a description. Click the check next to your custom URL category, and make sure “Site Access” and “User Credential Submission” are set to “block”. Optionally, you can set the “Site Access” key to “override”, which will make the website require an administrator password to access. Properly configure the pre-defined categories to match what would be appropriate for a school setting.

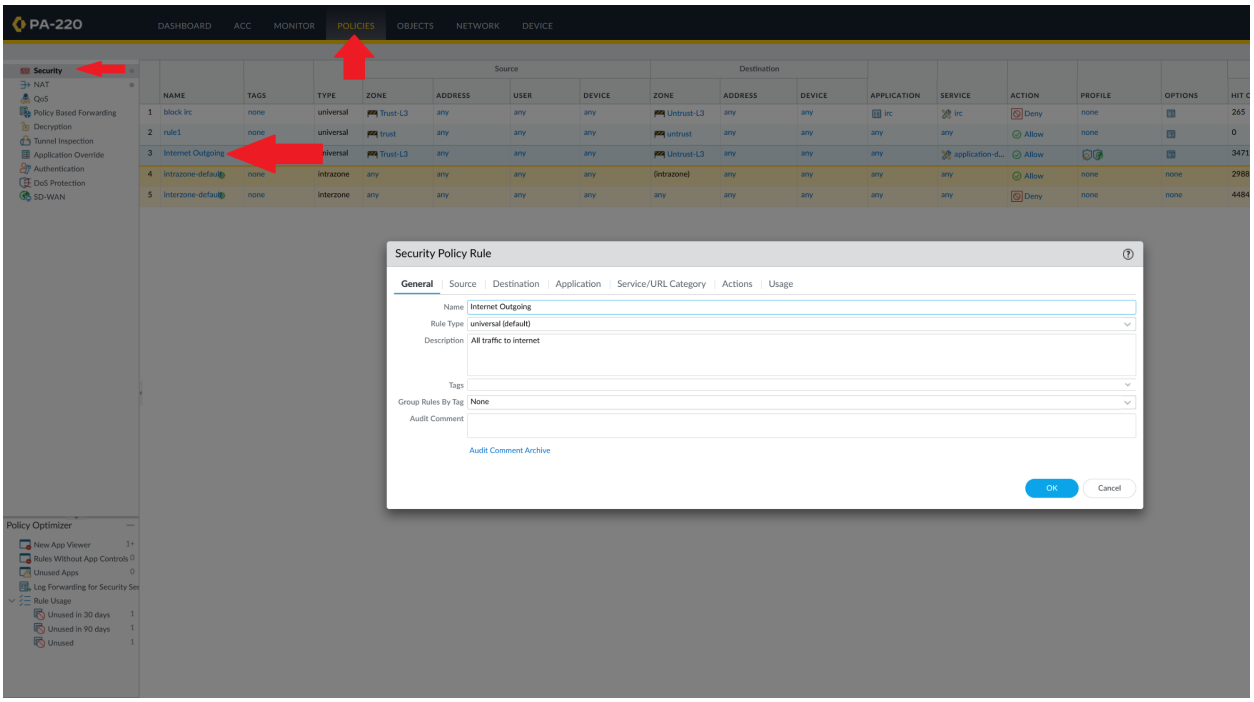


Optional: Configuring override

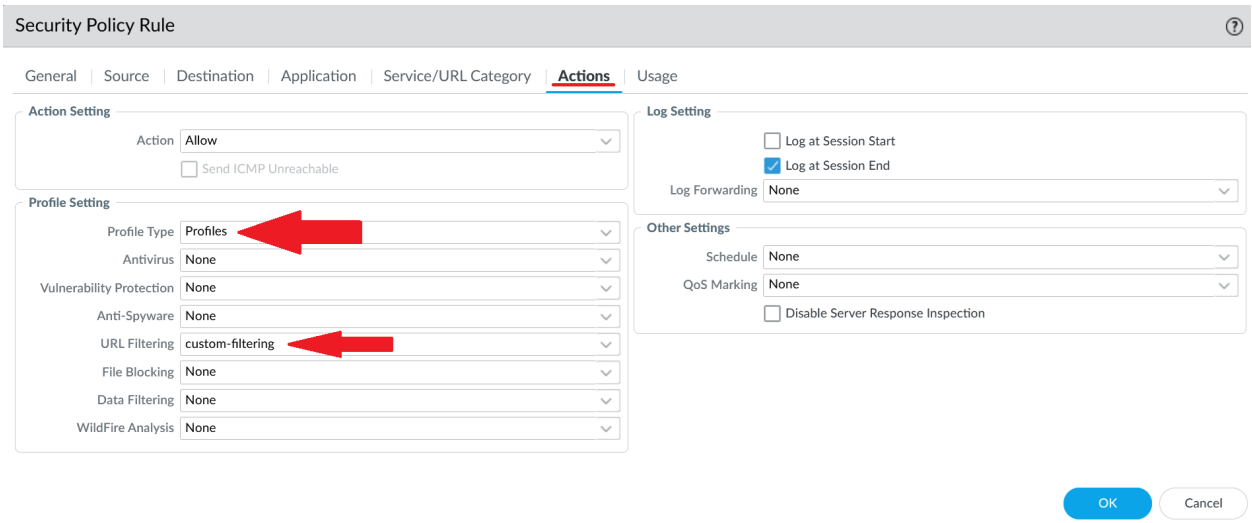
paloalto NETWORKS

- Go to “Device” > “Setup” > “Content ID” and click “Add” under the “URL Admin Override” section. Add your desired password and click “OK”.
- 

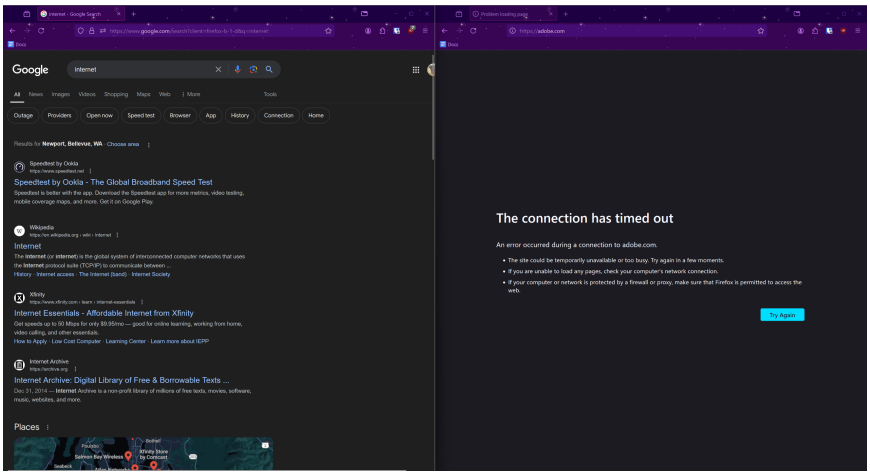
Go to “Policies” > “Security” and select the security policy that controls outgoing internet traffic.



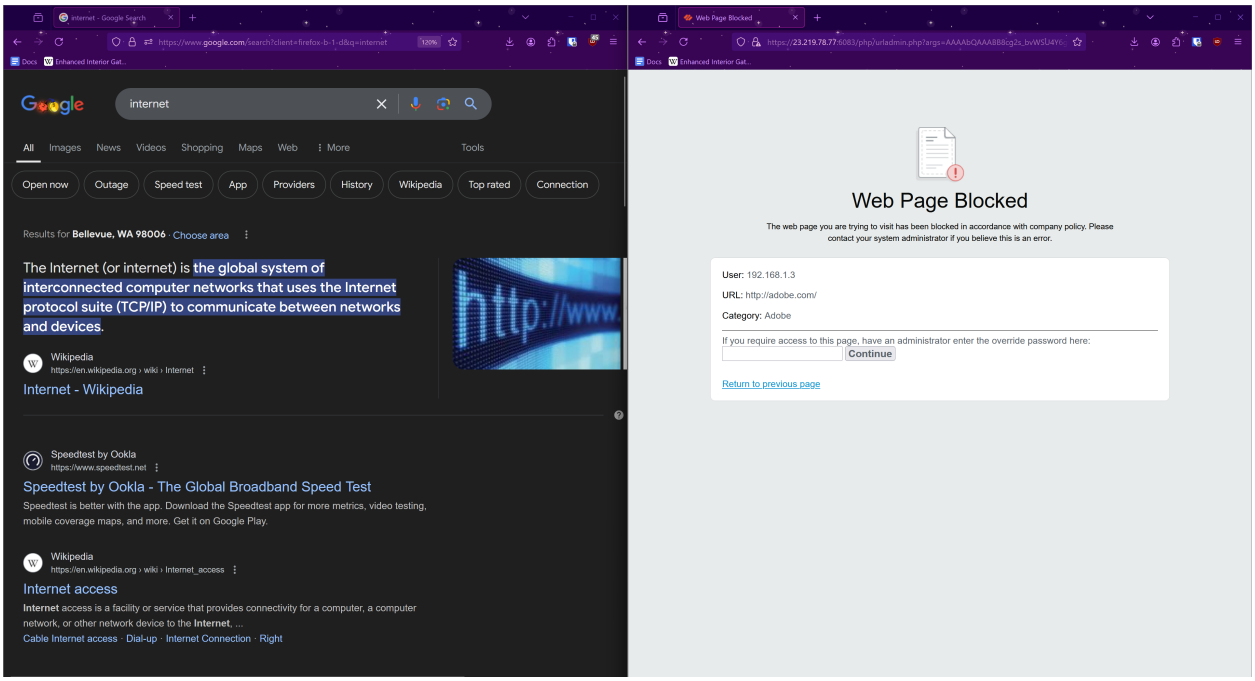
Click the “Actions” tab, set “Profile Type” to “Profiles”, and set the URL Filtering profile to the profile you set up.



URL-Based filtering should now work. As shown in the screenshot below, general internet traffic is allowed through, but HTTP connections to adobe.com are blocked.



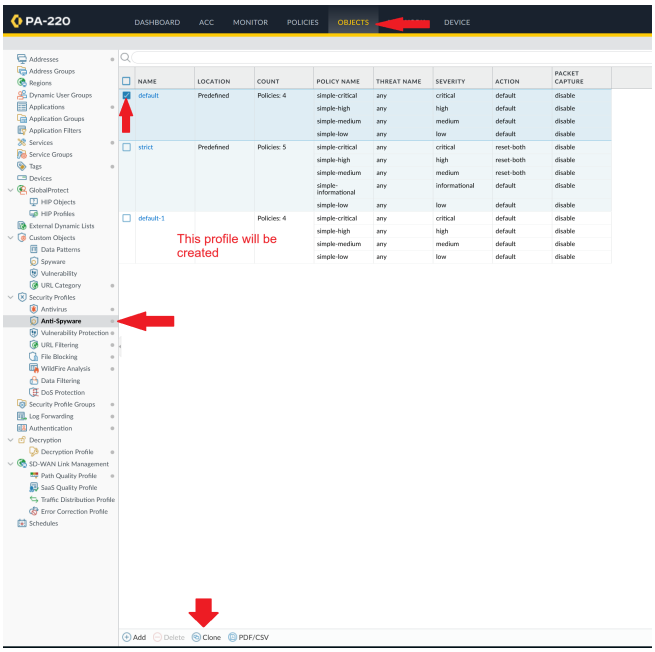
As shown in the image below, if the URL category is configured as “Override” instead of “Block”, requests to adobe.com will show a “Web Page Blocked” page that can be bypassed using a password.



DNS-Based Filtering

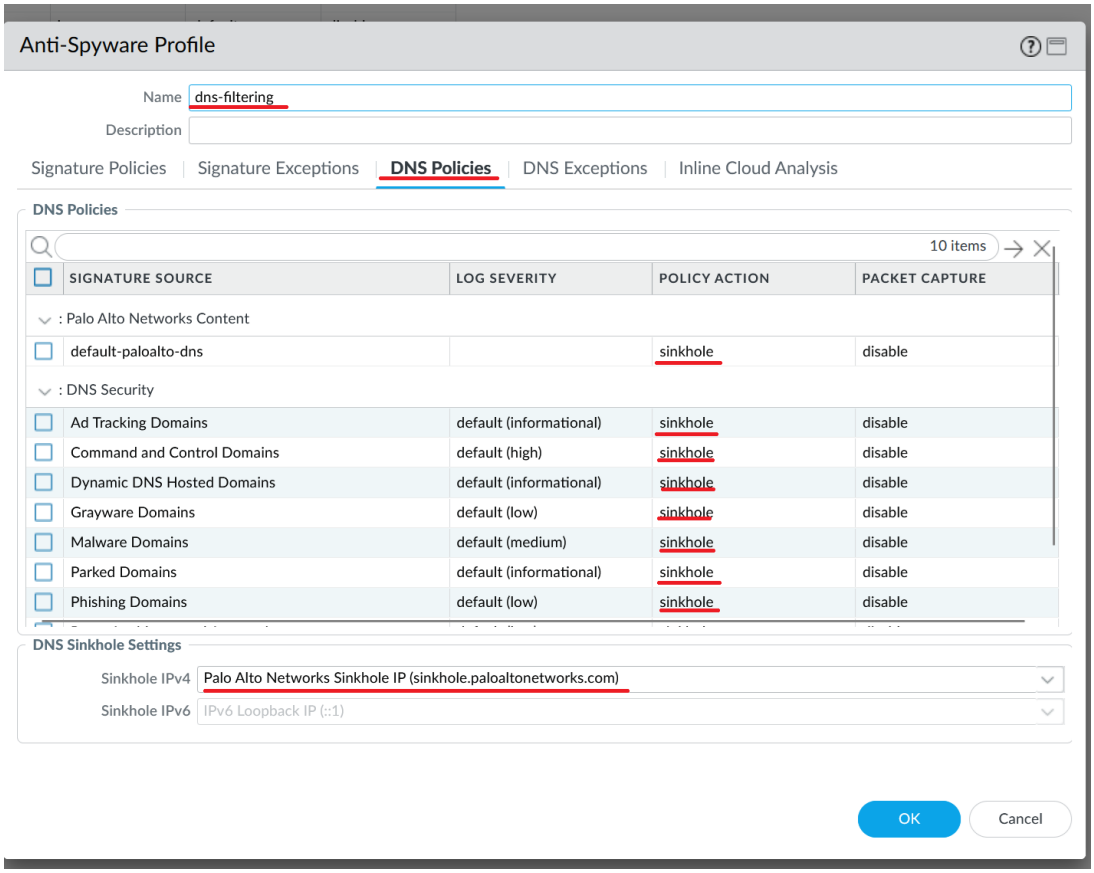
Go to Device > Licenses and make sure there's a valid "DNS Security" license.

Go to Objects > Security Policies > Anti-Spyware. Click the read-only default profile and click "Clone".

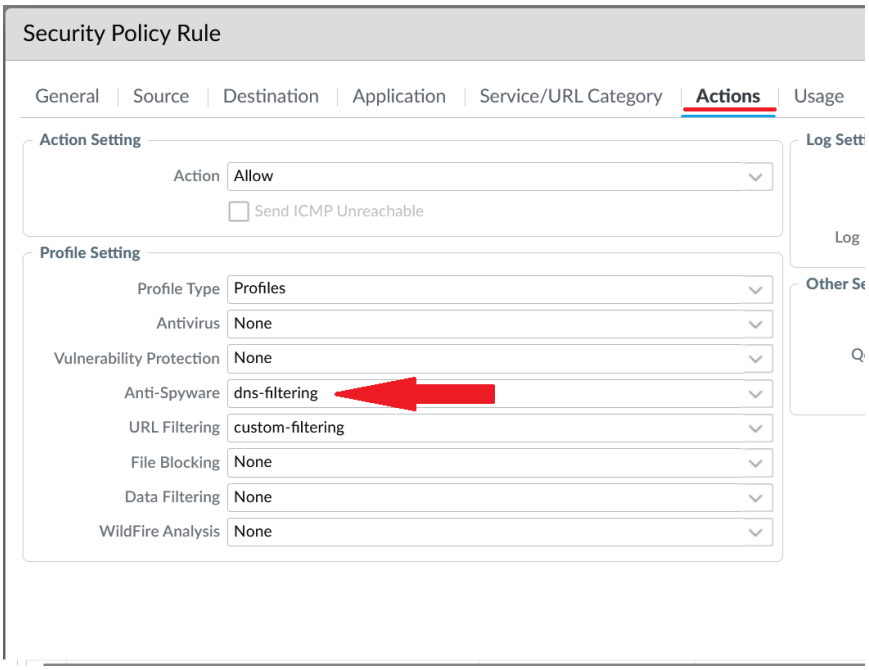


Click on the new "default-1" profile. Optionally, rename the profile to make it easier to identify. Go to the "DNS policies" tab. Under "signature source", set all items in the "Policy Action" tab to "sinkhole". Set the items in the "log severity" column to your

desired severity level for requests to different DNS types (in this example, log severity levels are at their default values). Make sure the sinkhole IP is set to “Palo Alto Networks Sinkhole IP”.

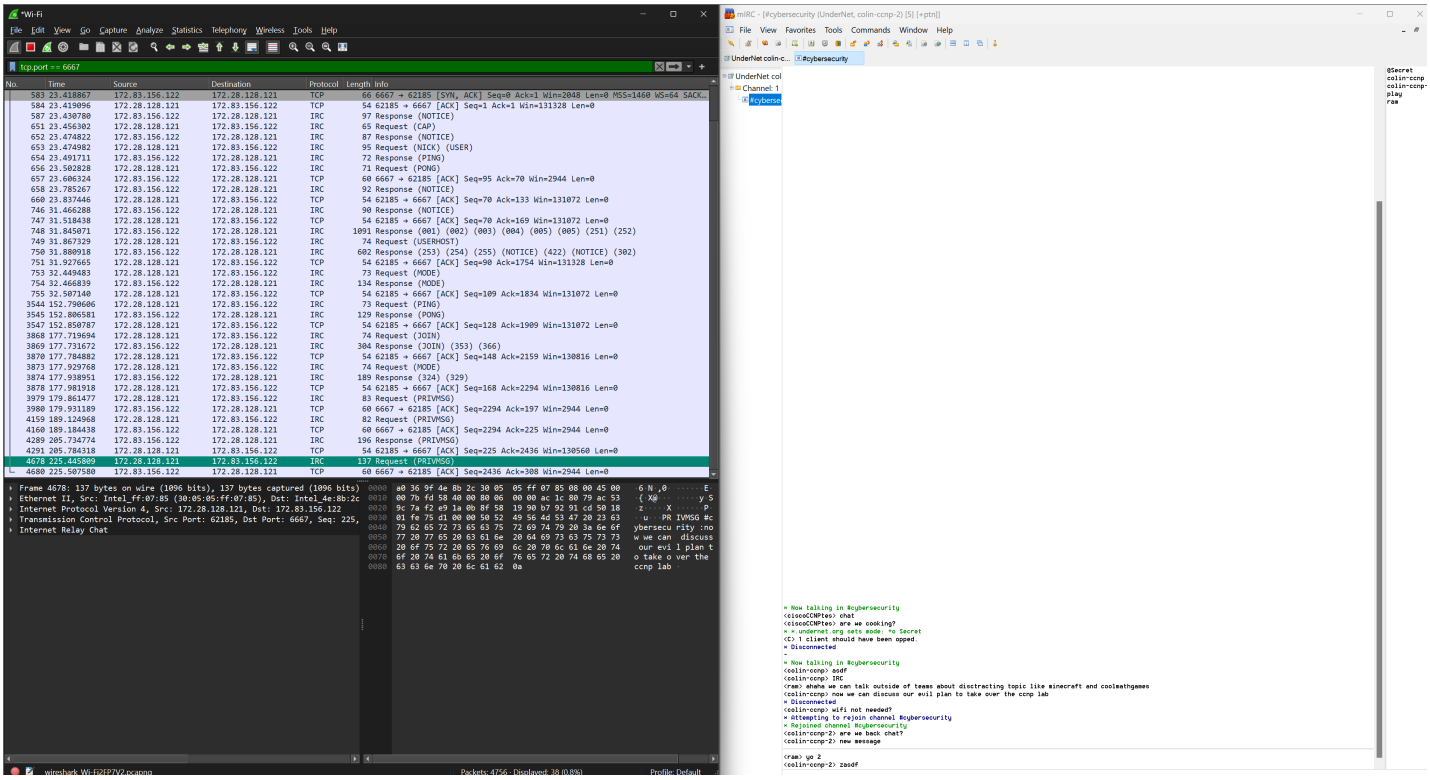


Go to Policies > Security and click on your outgoing internet rule. Go to “Actions” and under “Profile Settings”, set the “Anti-Spyware” setting to the rule you created.

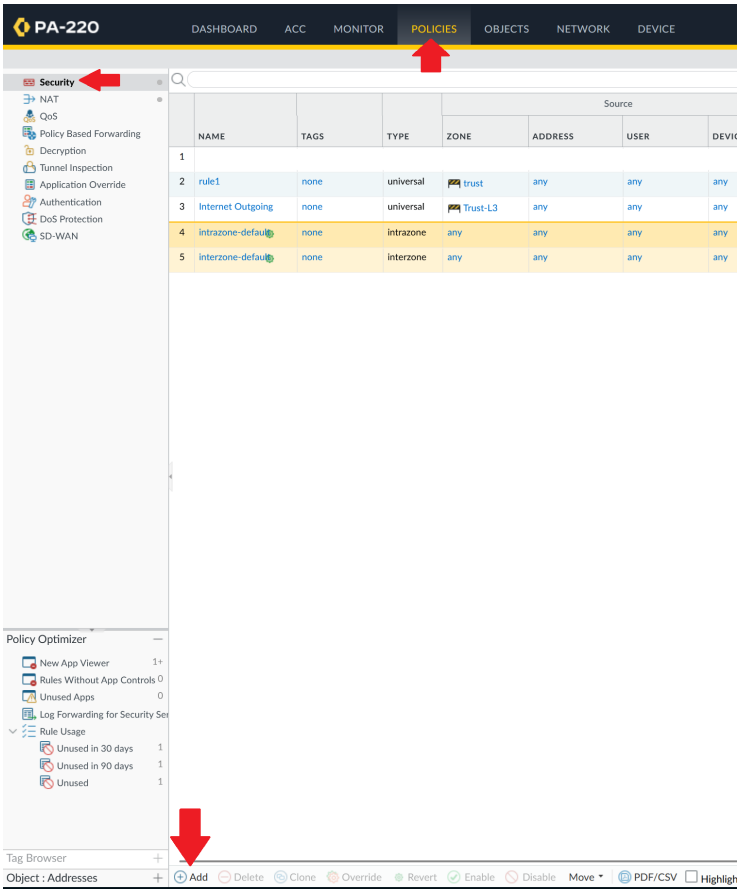


Application-level filtering (Blocking IRC Internet Relay Chat)

(Note: As shown in the image below, IRC chat was unblocked on this network before any configuration. This was tested by downloading the mIRC client and connecting to the server irc.undernet.org on TCP port 6667.)

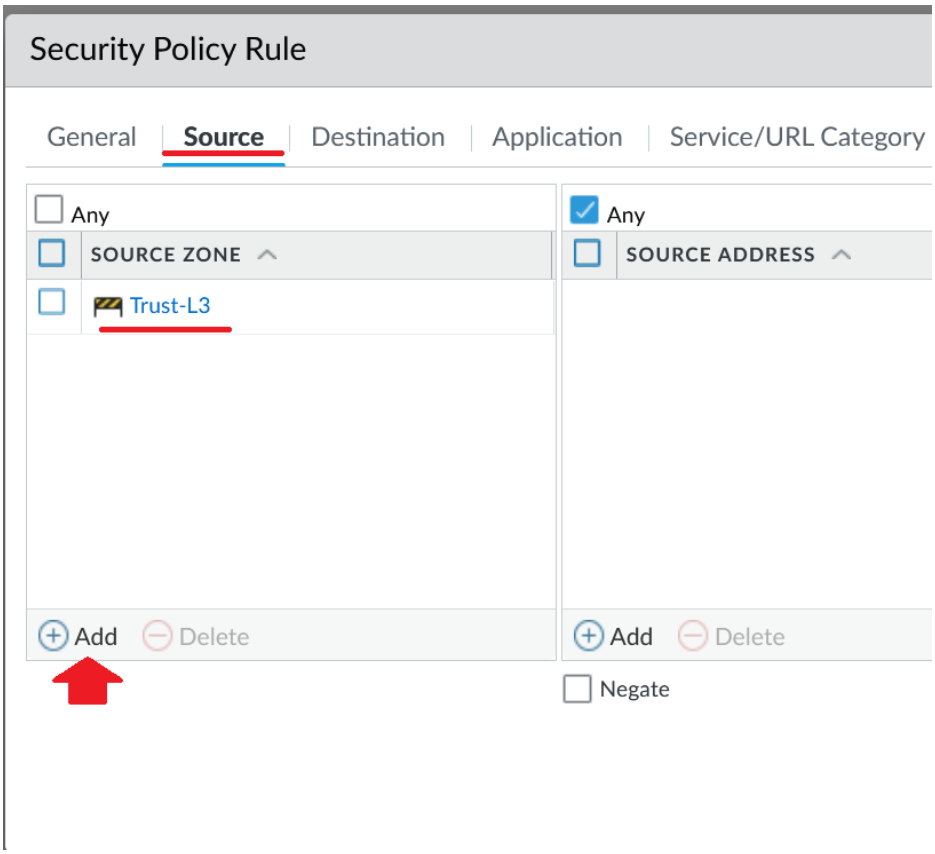


Go to Policies > Security and click “Add”.

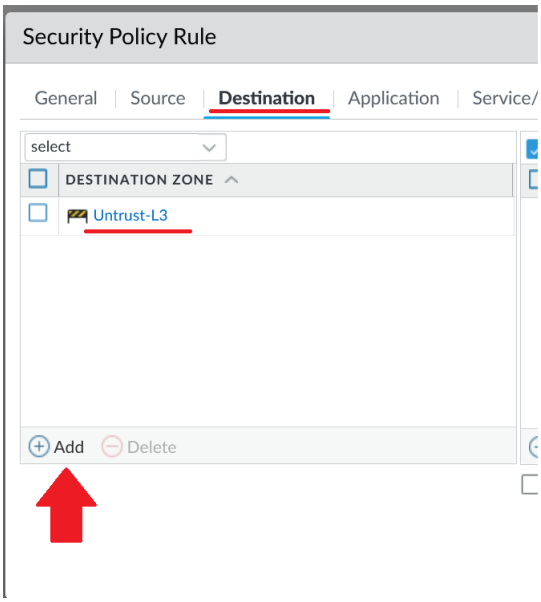


Give the policy an appropriate name for its purpose, as shown below:

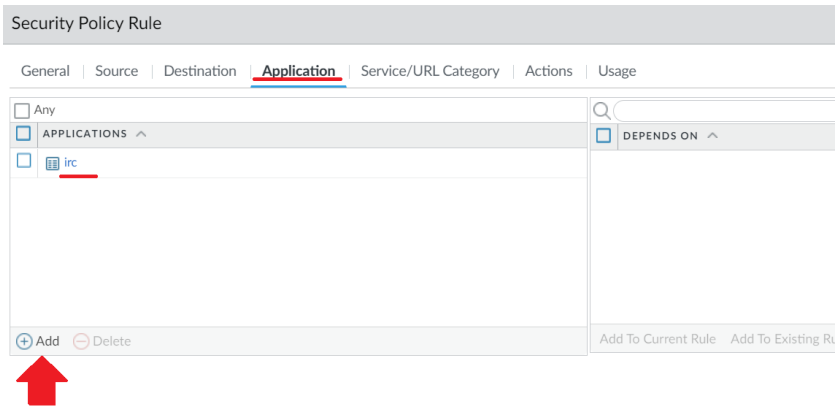
Under “Source”, click “Add” and set the source zone to “Trust-L3’.



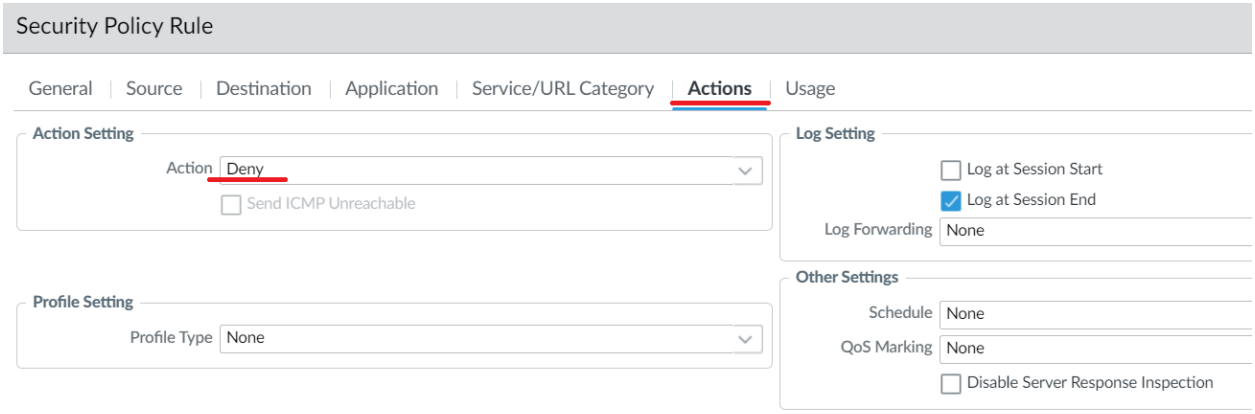
Under “Destination”, click “Add” and set the destination zone to “Untrust-L3”.



Under “Appliction”, click “Add” and set the application to “irc”.

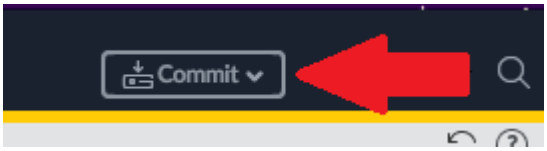


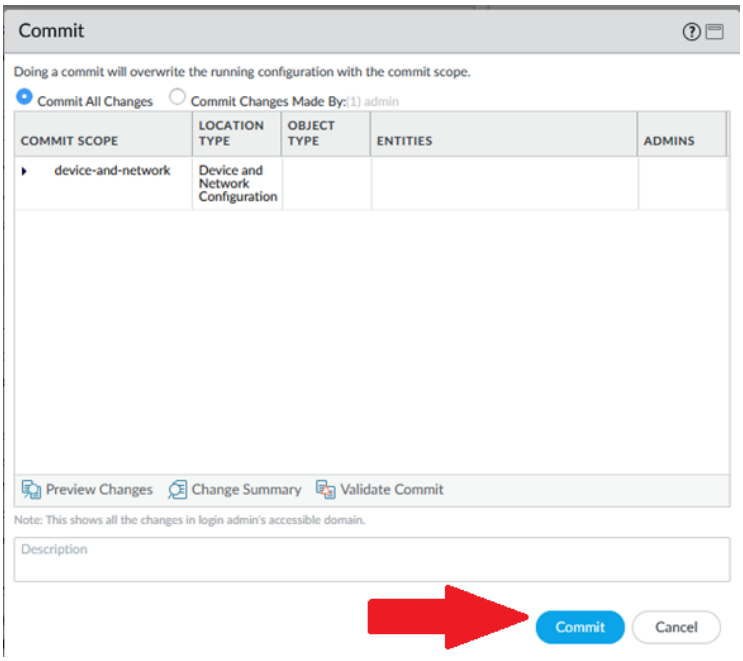
Under “Actions”, set the action to “Deny”.



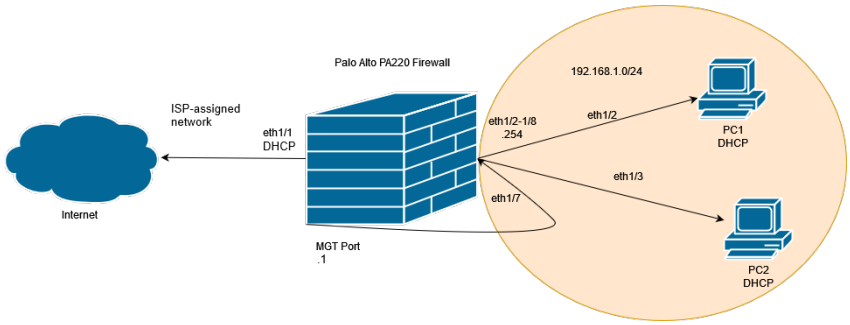
Finalizing Setup

Finally, click the *Commit* button in the top-right corner. In the resulting window, click *Commit* again.



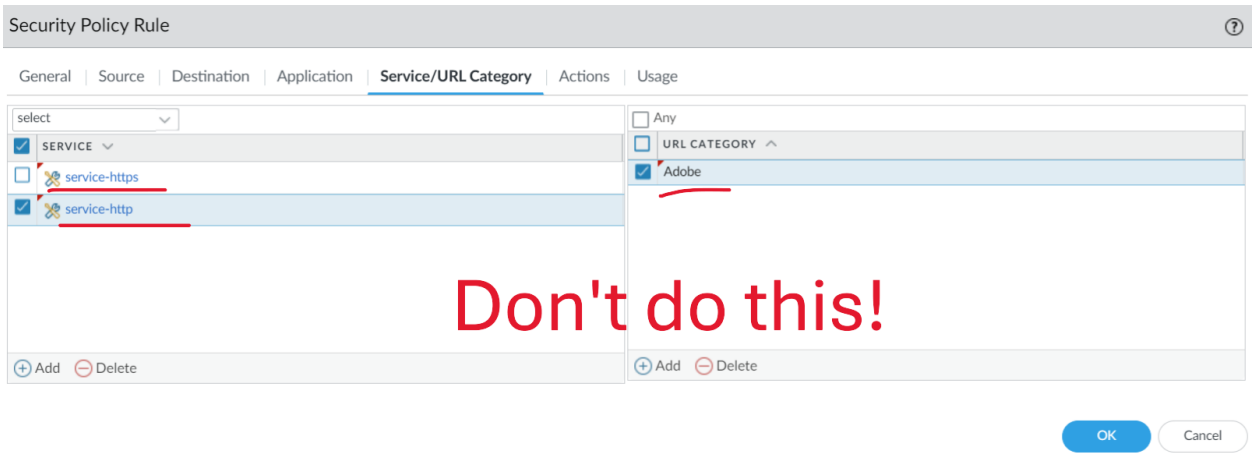


Network Diagram

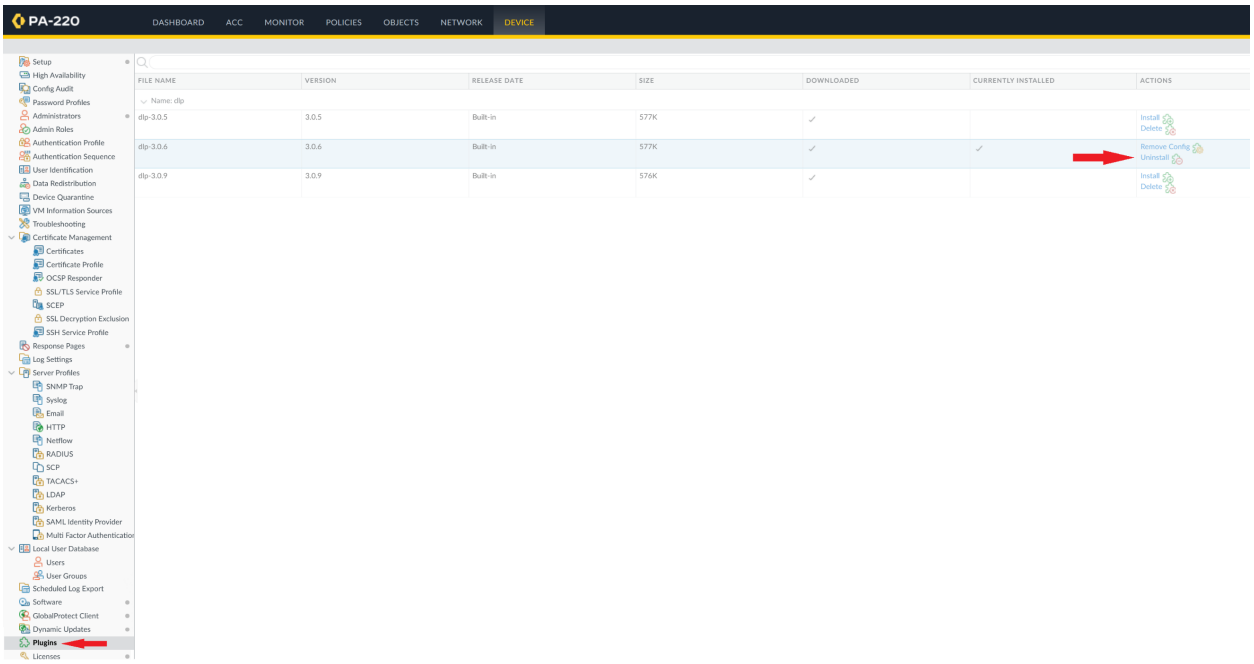


Problems

Originally, we configured our URL filtering security policy under “Service / URL Category” and configured “Adobe” (capital A) as the only URL category. When URL filtering is configured in this manner, it blocks all HTTP and HTTPS traffic outside of the security policy. Since our category did nothing but block adobe.com, we blocked every possible URL, which was not the intended effect. We fixed this by configuring filtering under the “Profile Section” section of the “Actions” tab and using the “adobe” (lowercase a) profile we configured.



When configuring a URL filtering override password, the “Setup” page under the “Device” tab was blank. After doing some research, I found that this wasn’t a unique issue, and that it could be remedied by uninstalling the “dlp” plugin, which had an issue that interfered with the override password configuration.



Conclusion

To wrap up, the Palo Alto PA220 is a very capable device for small school environments. Through the PA220’s web interface, setting up URL filtering, DNS-based filtering, and application-level filtering are all relatively straightforward. I am sure that the skills required to set up this triple-layer filtering will serve me well in the future if I am ever expected to set up a firewall for a monitored environment, such as a small office or school. With the advent of remote work/school becoming normalized in the professional/educational worlds, this small office/school architecture will only become

paloalto® NETWORKS

more common, making the ability to set up filtering even more valuable in these environments.