



Palo Alto Networks Cybersecurity Academy – Setting up Web Filtering

Colin J. Faletto, CCNA

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 University 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

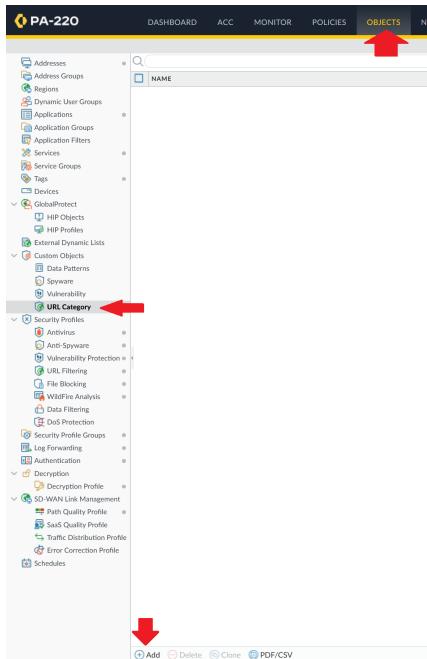
In this lab, we set up three different types of web filtering: URL filtering, DNS-based filtering, and application-level filtering. For URL filtering, we blocked all pre-defined categories that weren't appropriate for a school environment and created a custom URL category (adobe.com) that was blocked 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.

Custom URL Category

Name	<input type="text" value="Adobe"/>
Description	<input type="text" value="No Photoshop"/>
Type	<input type="text" value="URL List"/>

Matches any of the following URLs, domains or host names

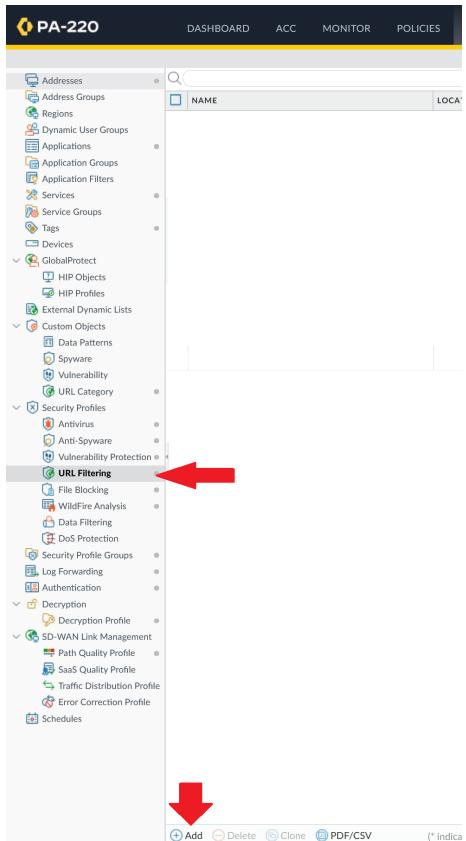
<input type="checkbox"/> SITES
<input type="checkbox"/> adobe.com

Add **Delete** **Import** **Export**

Enter one entry per row.
Each entry may be of the form www.example.com or it could have wildcards like www.*.com.
To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: xyz.com/ matches only xyz.com or more info, see URL Category Exceptions

OK **Cancel**

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.

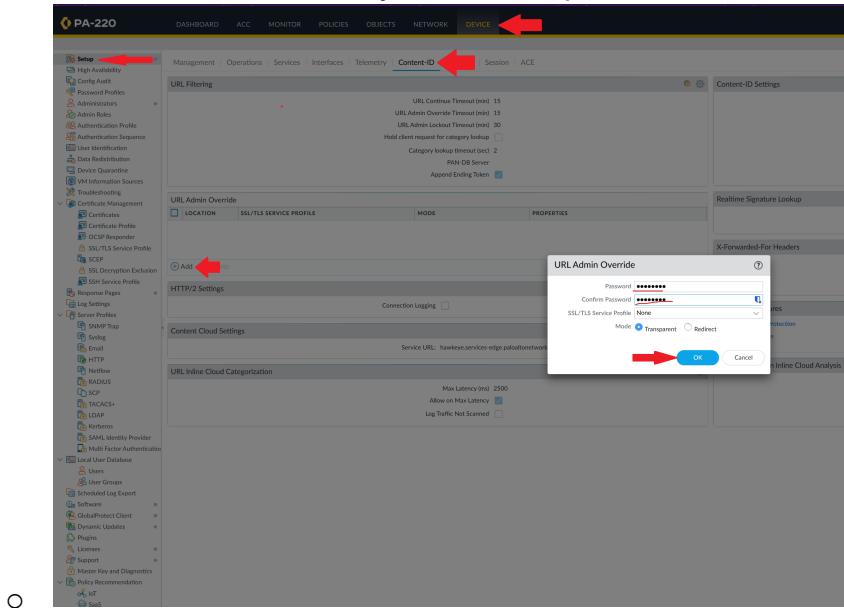
URL Filtering Profile

Categories		URL Filtering Settings	User Credential Detection	HTTP Header Insertion	Inline Categorization
<input checked="" type="checkbox"/> Adobe *		this can also be "block"	override	block	
<input type="checkbox"/> abortion			block	block	
<input type="checkbox"/> abused-drugs			block	block	
<input type="checkbox"/> adult			block	block	
<input type="checkbox"/> alcohol-and-tobacco			block	block	

* indicates a custom URL category, + indicates external dynamic list
Check URL Category

Optional: Configuring override

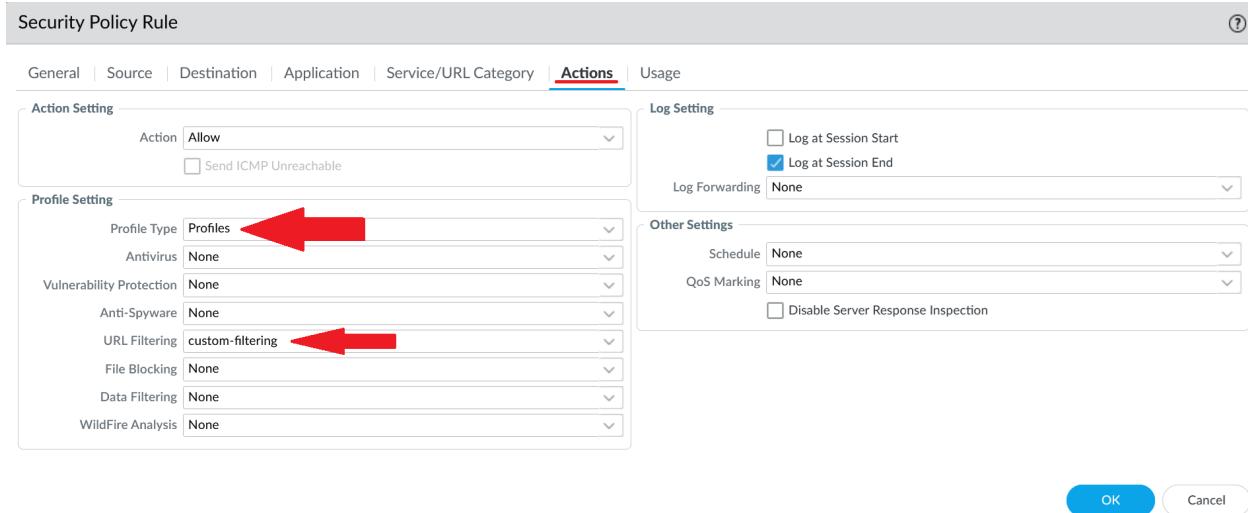
- Go to “Device” > “Setup” > “Content ID” and click “Add” under the “URL Admin Override” section. Add your desired password and click “OK”.



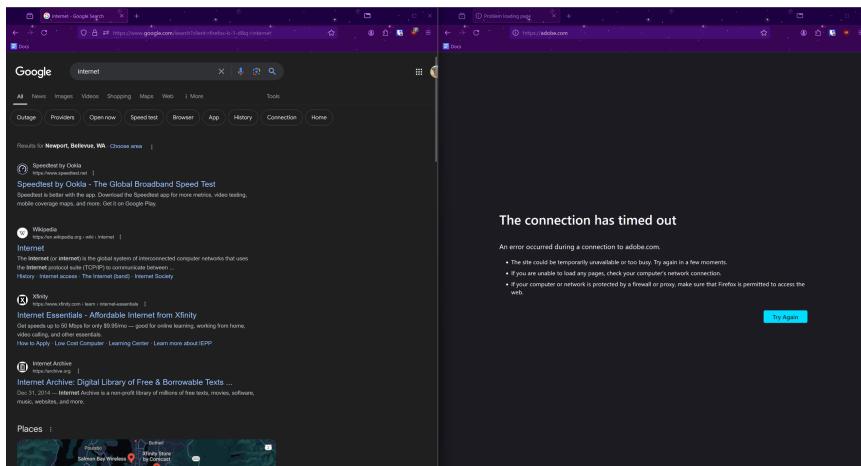
Go to “Policies” > “Security” and select the security policy that controls outgoing internet traffic.

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT C
1 block_ic	none	universal	Trust-L3	any	any	any	Untrust-L3	any	any	irc	irc	Deny	none		265
2 rule1	none	universal	trust	any	any	any	untrust	any	any	any	any	Allow	none		0
3 Internet Outgoing	none	universal	Trust-L3	any	any	any	Untrust-L3	any	any	any	any	Allow	application-d...		3471
4 Intrazone-default	none	intrazone	any	any	any	any	(Intrazone)	any	any	any	any	Allow	none		2985
5 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none		4484

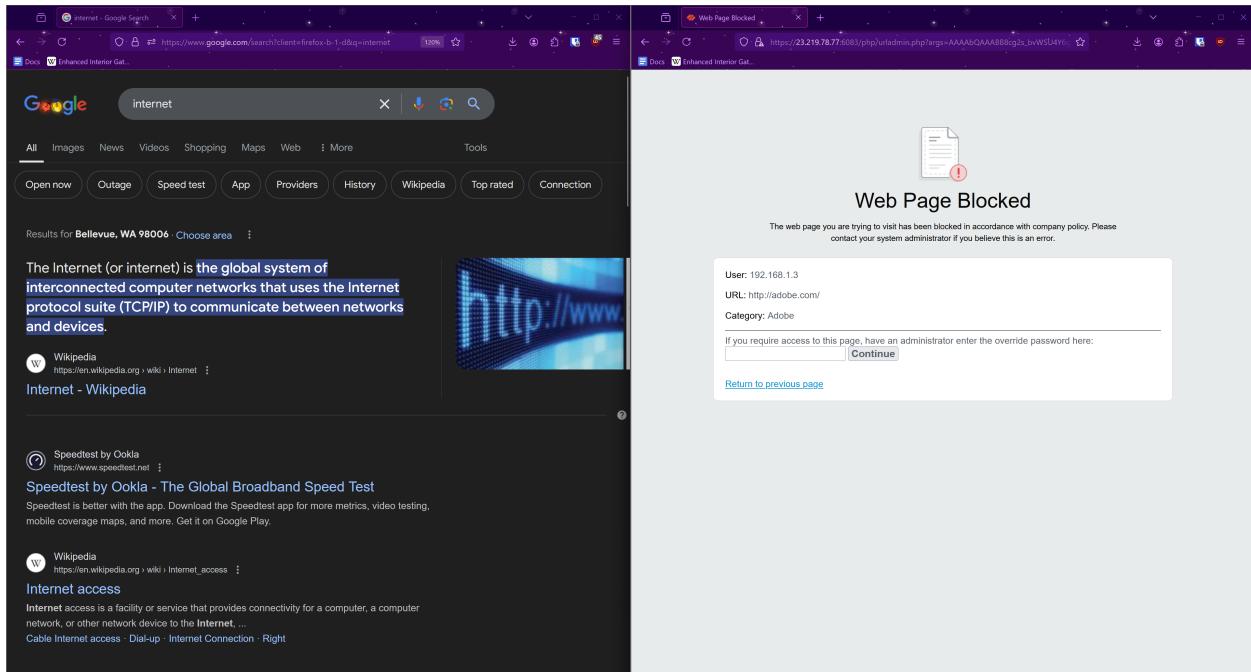
Click the “Actions” tab, set “Profile Type” to “Profiles”, and set the URL Filtering profile to the profile you set up.



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”.

NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	enable
default-1	Predefined	Policies: 4	simple-critical	any	critical	default	enable

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”.

The screenshot shows the 'Anti-Spyware Profile' configuration window. The 'Name' field is set to 'dns-filtering'. The 'DNS Policies' tab is active, displaying a table of policies:

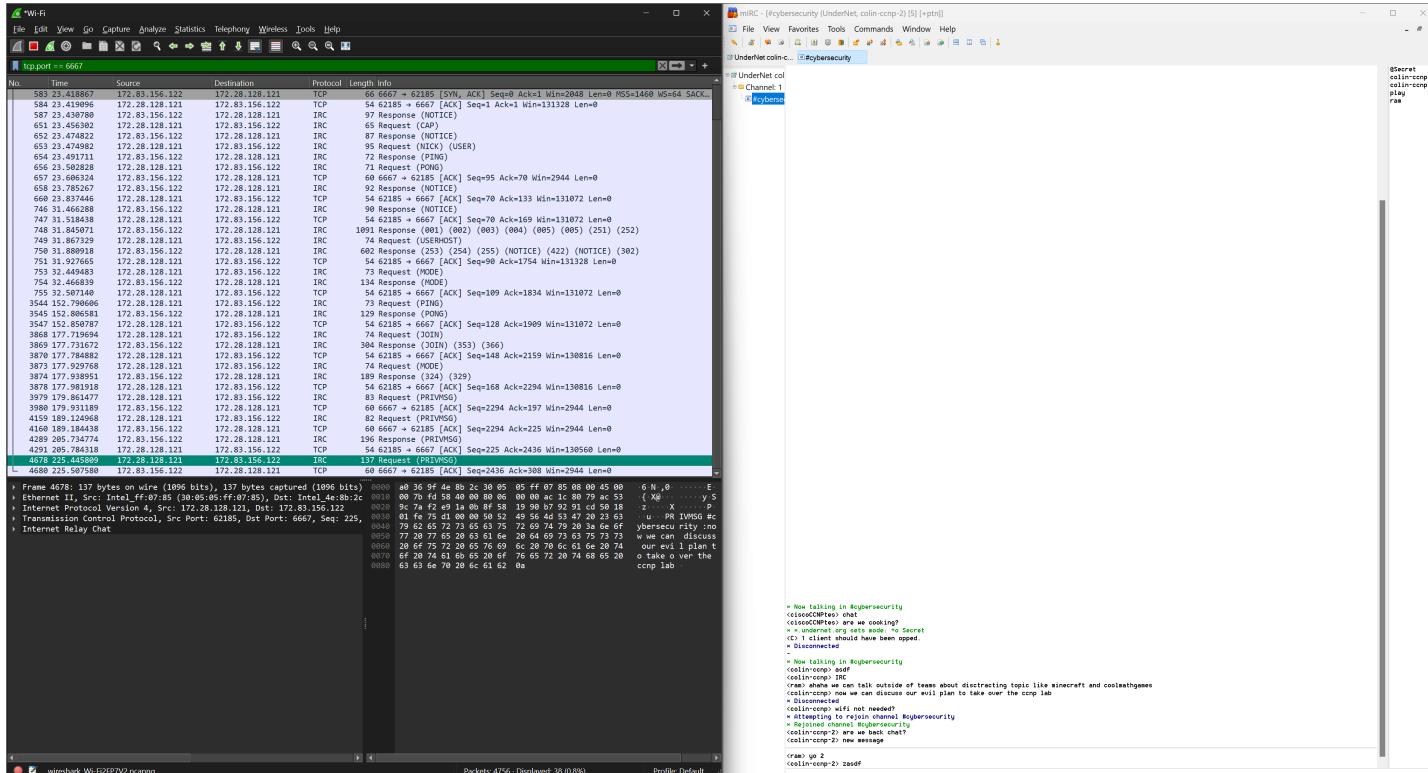
SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		<u>sinkhole</u>	disable
: DNS Security			
Ad Tracking Domains	default (informational)	<u>sinkhole</u>	disable
Command and Control Domains	default (high)	<u>sinkhole</u>	disable
Dynamic DNS Hosted Domains	default (informational)	<u>sinkhole</u>	disable
Grayware Domains	default (low)	<u>sinkhole</u>	disable
Malware Domains	default (medium)	<u>sinkhole</u>	disable
Parked Domains	default (informational)	<u>sinkhole</u>	disable
Phishing Domains	default (low)	<u>sinkhole</u>	disable

In the 'DNS Sinkhole Settings' section, the 'Sinkhole IPv4' field is set to 'Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)' and the 'Sinkhole IPv6' field is set to 'IPv6 Loopback IP (::1)'. At the bottom right are 'OK' and 'Cancel' buttons.

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”.

The screenshot shows the PA-220 configuration interface. At the top, there's a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a yellow background), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar lists various policy categories with small icons: NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below the sidebar is a section titled 'Policy Optimizer' with items like 'New App Viewer', 'Rules Without App Controls', 'Unused Apps', 'Log Forwarding for Security Set', 'Rule Usage' (with sub-items 'Unused in 30 days', 'Unused in 90 days', and 'Unused'), and 'Tag Browser'. At the bottom of the main content area is a table titled 'Source' with columns: NAME, TAGS, TYPE, ZONE, ADDRESS, USER, and DEVICE. Five rows are listed: rule1 (universal, trust, any, any, any, any), Internet Outgoing (universal, Trust-L3, any, any, any, any), intrazone-default (intrazone, any, any, any, any, any), and interzone-default (interzone, any, any, any, any, any). At the very bottom of the page, there's a toolbar with buttons for Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, and Highlight.

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

Name

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

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^
<input type="checkbox"/> Trust-L3	

Add **Delete** **Add** **Delete** Negate



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

Security Policy Rule

General | Source | **Destination** | Application | Service/

select	
<input type="checkbox"/> DESTINATION ZONE ^	
<input type="checkbox"/> Untrust-L3	

Add **Delete**



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

Security Policy Rule

General | Source | Destination | **Application** | Service/URL Category | Actions | Usage

Any
 APPLICATIONS ▾
 irc

DEPENDS ON ▾

+ Add **Delete** Add To Current Rule Add To Existing Rule



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

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action **Deny**
 Send ICMP Unreachable

Log Setting

Log at Session Start
 Log at Session End
Log Forwarding None

Profile Setting

Profile Type None

Other Settings

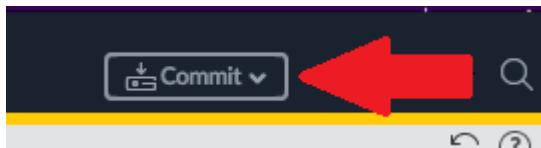
Schedule None
QoS Marking None
 Disable Server Response Inspection

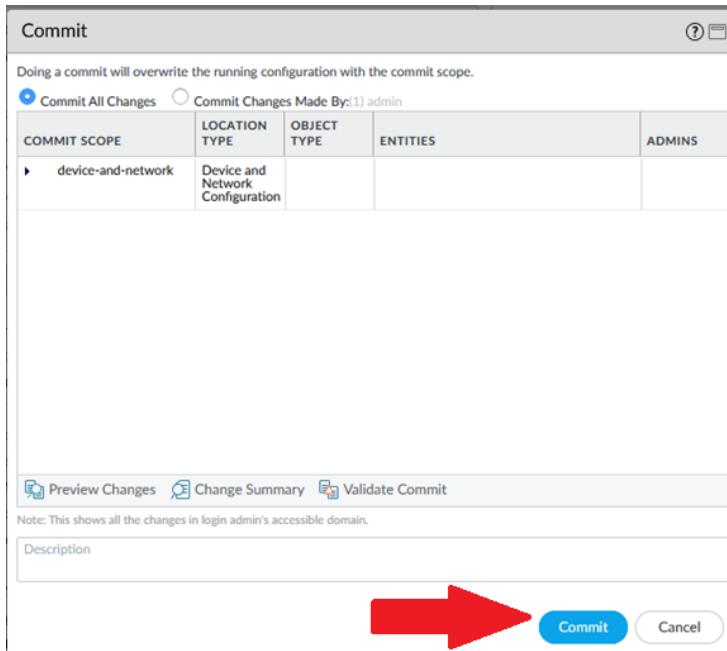
2

2

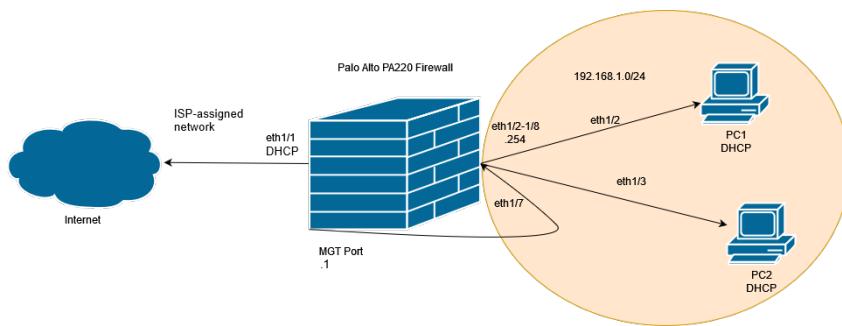
Finalizing Setup

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



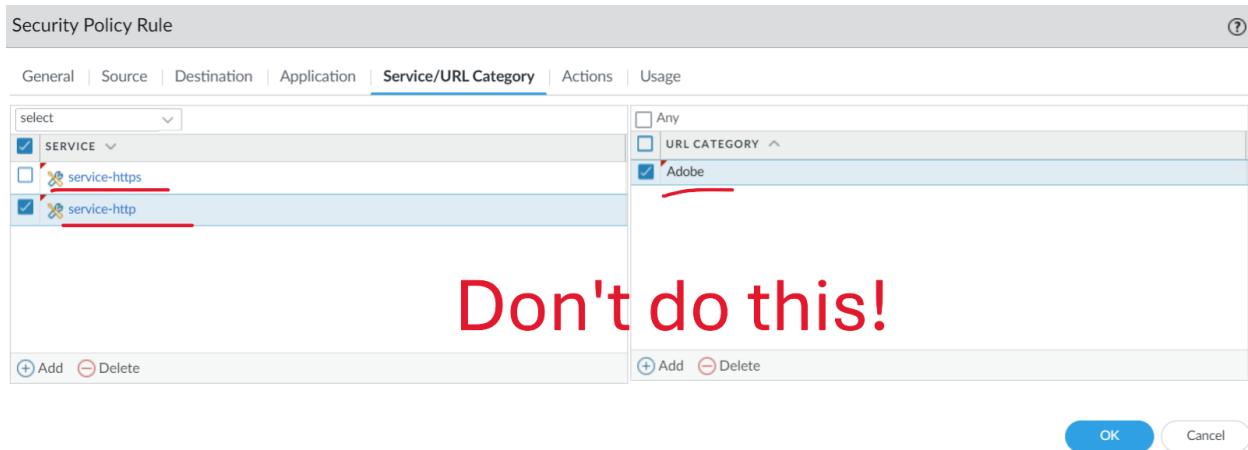


Network Diagram



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.

FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS
dlp.dlp	3.0.5	Built-in	577K	✓		Install Delete
dlp.dlp	3.0.6	Built-in	577K	✓	✓	Remove Config Uninstall Install Delete
dlp.dlp	3.0.9	Built-in	576K	✓		Uninstall Install Delete

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

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

