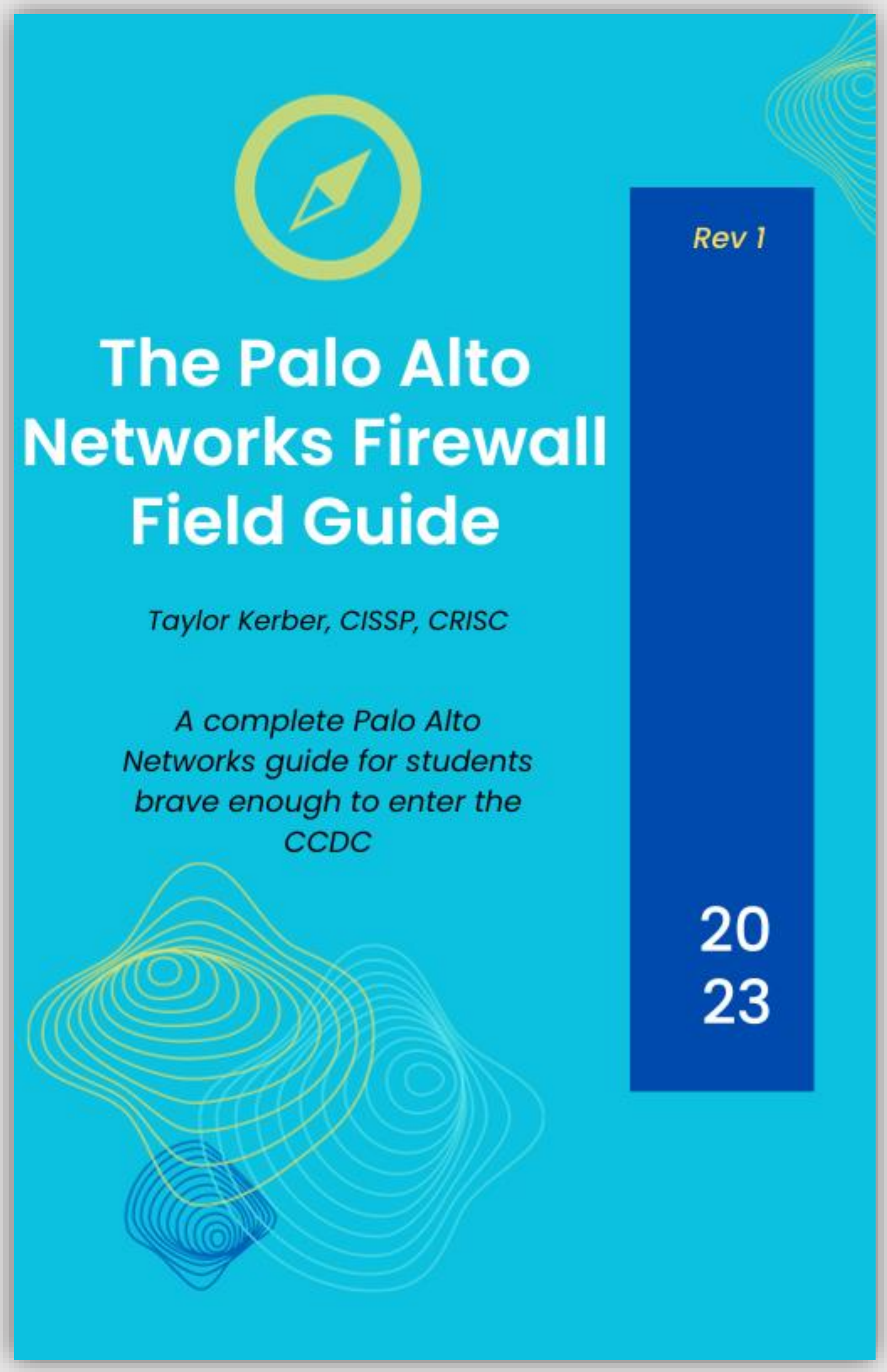


Rev 1

The Palo Alto Networks Firewall Field Guide

Taylor Kerber, CISSP, CRISC

A complete Palo Alto Networks guide for students brave enough to enter the CCDC

20
23

Content

License & Usage

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for commercial purposes.

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

About This Guide

My name is Taylor Kerber and I’ve written this guide to aid all students looking to be a part of the CCDC and needing to learn more about the Palo Alto Networks NGFW platform. The CCDC is a fantastic way to get some real hands-on experience with real technologies and scenarios and I highly recommend all students who have the opportunity - to take it and join.

This guide covers the fundamentals of what a firewall is and how it can take many forms. Then we pivot to basic Palo Alto Networks knowledge and end with the best ways to quickly harden a Palo Alto Networks NGFW for the CCDC, lock down policies with App-ID and Content-ID, and lastly a checklist that you can take and utilize as your own CCDC Palo Alto Networks checklist.

I hope you enjoy learning this content and if you have any questions, please feel free to reach out to me via the links on my personal blog site: https://www.caffeinetech.info/content.html

1. Introduction

This guide was written with the intention of helping students prepare for the Collegiate Cyber Defense Competition (CCDC). It can also be used freely by curious individuals from all backgrounds to learn about the Palo Alto Networks firewall platform. This guide will focus on the Palo Alto Networks firewall solutions with configuring and optimizing a PanOS deployment from a fresh out the box (FOB) / CCDC perspective. A lot of topics like HA, advanced routing, Panorama, User ID, VPN, HIP Profiles, may be referenced but not covered in-depth.

The Palo Alto Networks security suite has been around since their inception in 2005. Palo Alto Networks has since branched out to offer many different types of security services with an emphasis on Cloud native solutions.

The Palo Alto Networks firewall can be referred to as a Swiss army knife of security platforms. It has a lot of functions and capabilities that can be easily configured and deployed right out of the box. The following list below is a quick list of many of the capabilities this firewall can offer.

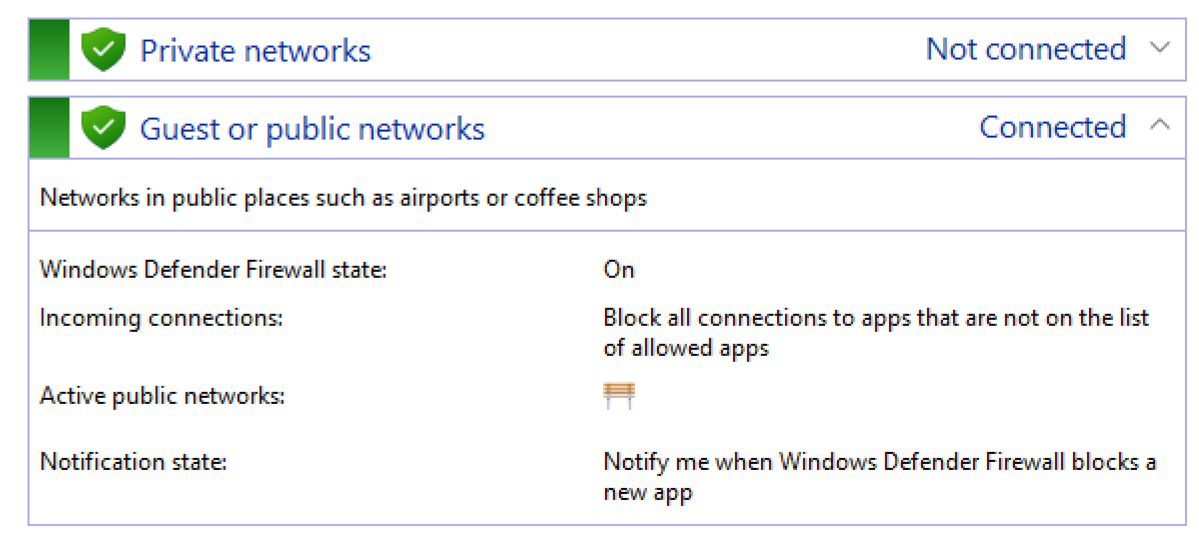
- NGFW Policy (App-ID & Content-ID)
- IPS/IDS (Threat Profiles)
- Website Filtering (URL Filtering)
- File Blocking (Data Filtering)
- Vulnerability Detection / Response
- VPN Services (Global Protect)
- Device Profiling (HIP Profiles)
- User Profiling (User ID)
- Zero Day Threat Protection (WildFire)
- DoS Protection & Zone Protection

2. What is a Firewall?

Before exploring some of the wonderful functions and features of the Palo Alto Network firewalls we need to have a basic understanding of a firewall and its main purpose.

A firewall can be either a physical appliance, a virtual appliance, software, or even a combination of these. In its simplest definition it is essentially a computer system that is designed to inspect content based on certain criteria and match that content to a policy to either allow or deny the content access. When we think of a firewall we often think of the internet and traffic but firewalls can also be application based and live on individual hosts as well. Here are a few examples below of different types of firewalls.

- All Microsoft computers come with a built-in application firewall that is referred to as the Windows Filtering Platform. See a screenshot from my Windows 11 PC in Figure 2.1.



Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

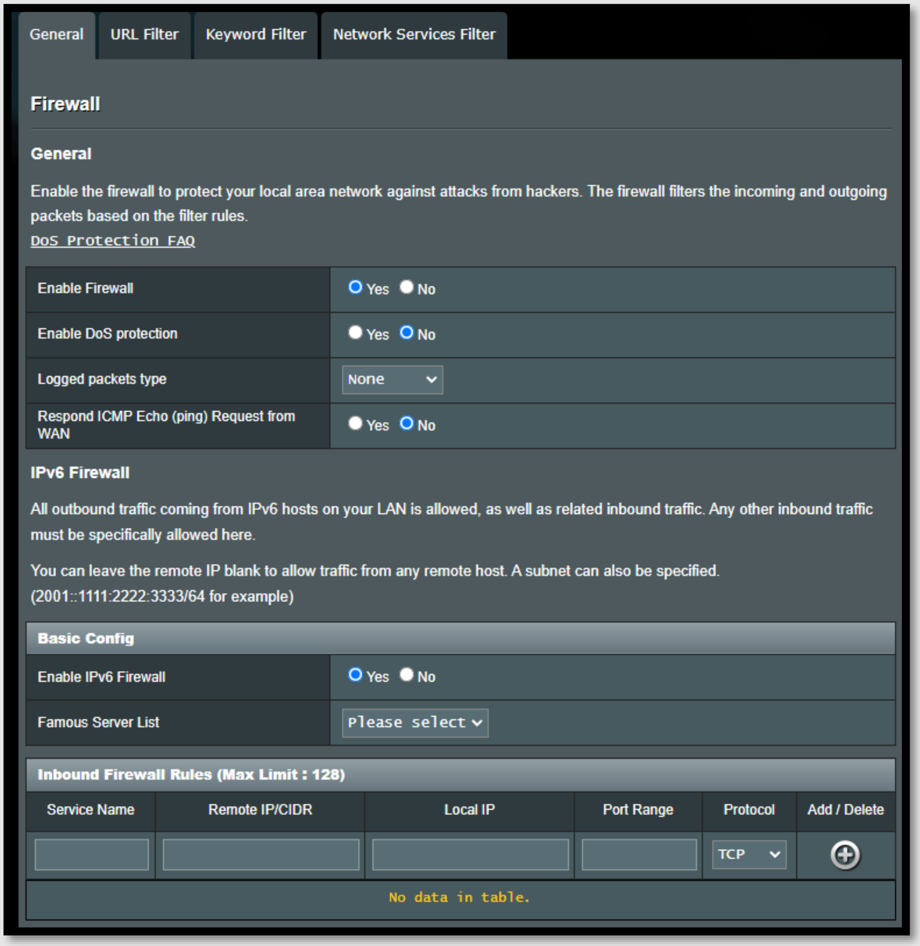
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks:

Notification state: Notify me when Windows Defender Firewall blocks a new app

Figure 2.1

- Your home routers have built-in packet filtering firewalls that usually block ALL incoming traffic by default and allow all outbound traffic. As you can see, I've taken a screenshot of the firewall settings in a home ASUS router I use for guest wireless. Figure 2.2



Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.

DoS Protection FAQ

Enable Firewall	● Yes ○ No
Enable DoS protection	○ Yes ● No
Logged packets type	None
Respond ICMP Echo (ping) Request from WAN	○ Yes ● No

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (2001::1111:2222:3333/64 for example)

Basic Config

Enable IPv6 Firewall	● Yes ○ No
Famous Server List	Please select

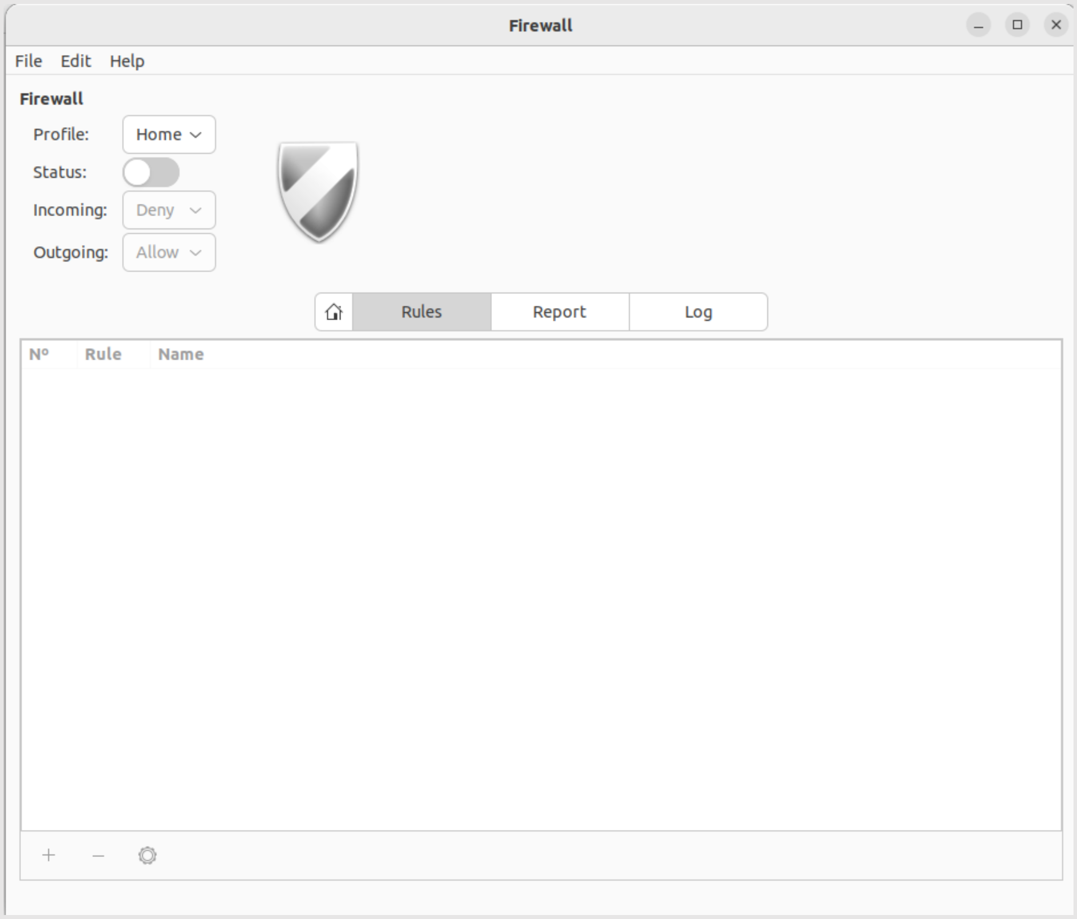
Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
				TCP	⊕

No data in table.

Figure 2.2

- Most all Linux operating systems have a built-in host-based firewall that can be used via the CLI or with optional GUI applications like you will see in this guide. For RHEL it is nftables or firewalld and for BSD it is usually UFW/iptables. UFW is stateful and in Figure 2.3 you can see the GUFW GUI (Firewall Configuration) for Ubuntu UFW.



Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

Figure 2.3

Section Summary

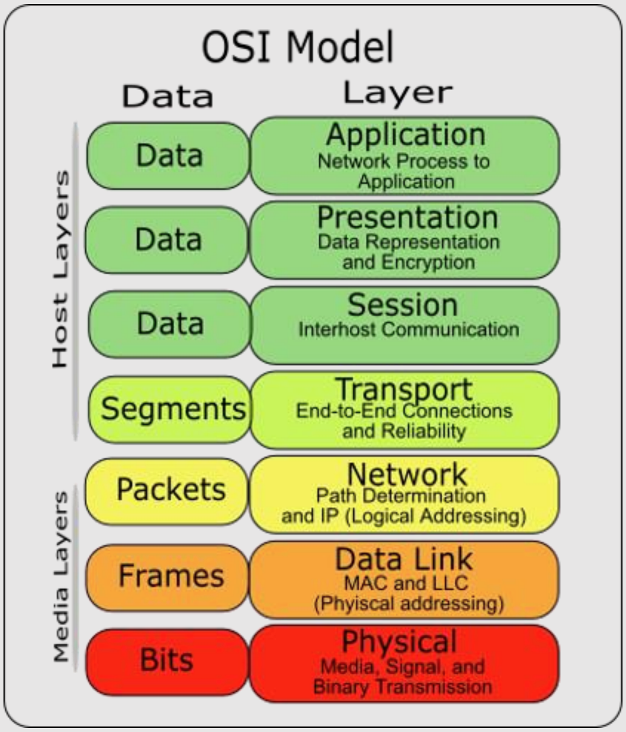
Almost everything you do on a network connected device goes through a firewall or packet filtering device. These examples we’ve talked about are simple and mostly operate at the OSI Model Layer 4 or TCP/IP Internet Layer. This means they will filter traffic based on source and destination IP, port, and protocol only.

3. OSI Model & DPI

Of course, no Network Security guide would be complete without a quick refresher of the TCP / IP & OSI Models. However, what needs to be understood here is not necessarily the model itself but where these firewalls operate. Earlier generations of firewalls operated at the OSI Layer 4. This meant a policy would allow certain traffic with a source, destination, protocol, and port. The firewall had no understanding of anything beyond that. If the traffic that passed through it matched the source, destination, protocol, and port, it would be permitted access.

A NGFW differs in that it can operate and identify traffic all the way up to Layer 7 (Application) of the OSI model. This means that instead of looking at just the header information of a packet, it also inspects the actual payload. This is the key difference between a NGFW and a traditional packet inspection firewall.

So why is this so important? Imagine if a bad actor wants to send malicious traffic to your network and try to infiltrate it. With a traditional firewall if their traffic fits your policy, it gets in. If this traffic is sent over the correct port to the right destination, it doesn't matter what else is inside the packet. With a Next-Generation Firewall, this all changes. The firewall now has what's called Deep Packet Inspection. The firewall can act as an IPS or IDS and can analyze the payload of the traffic and look for patterns that it finds malicious. Based on what it finds it could then potentially alert or even take a specific action based on how you configure your policy.



OSI Model

	Data	Layer
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation and Encryption
	Data	Session Interhost Communication
	Segments	Transport End-to-End Connections and Reliability
Media Layers	Packets	Network Path Determination and IP (Logical Addressing)
	Frames	Data Link MAC and LLC (Phyiscal addressing)
	Bits	Physical Media, Signal, and Binary Transmission

Figure 3.1

This Photo by Unknown author is licensed under CC BY

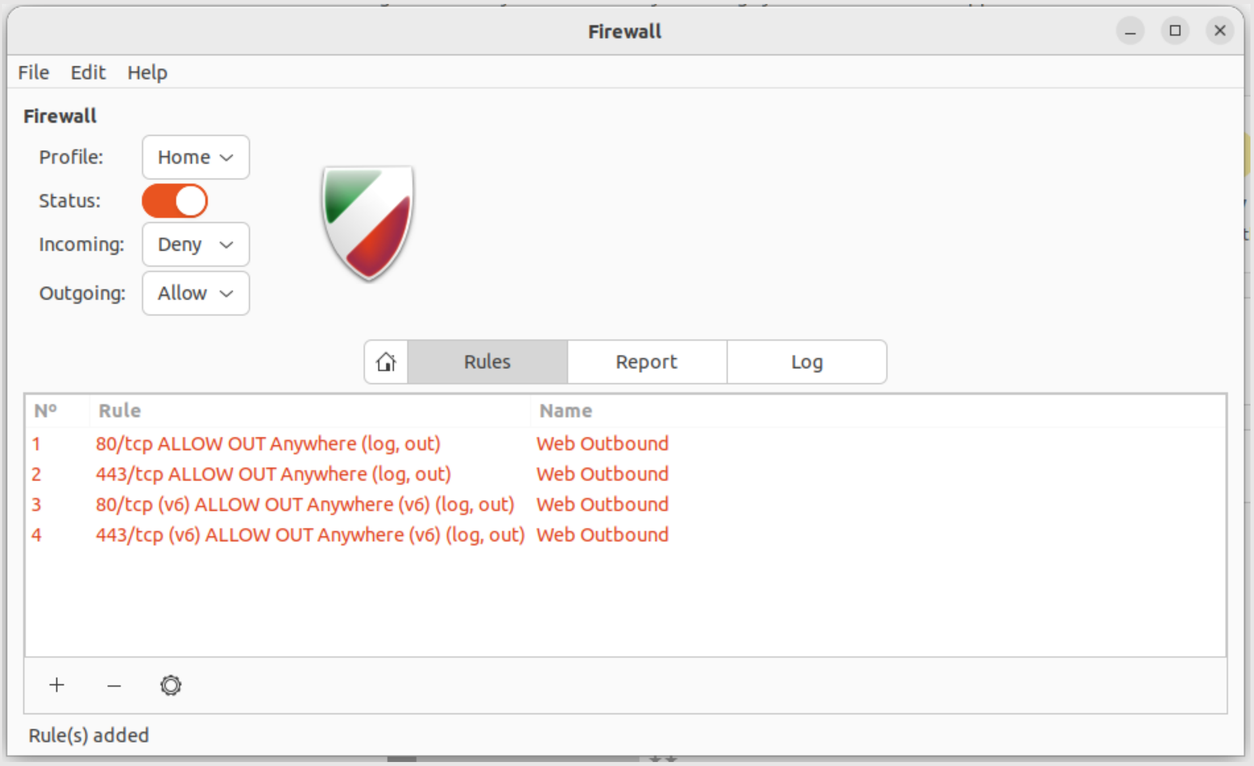
4. Stateful vs non-Stateful

Some of the first generations of firewalls were simply packet filtering firewalls. These typically operated at OSI Layer 4 and were not stateful. What's important about this is that if a firewall isn't stateful, you had to account for this in your policy as the firewall does not keep track of active sessions of what is going in and what is going out.

Example

- ✓ Without a stateful firewall if you wanted to allow traffic to communicate out of your LAN on port 443 and 80 (Web) - You must also account for the return traffic coming back in and appropriately create a policy for that traffic. This was time consuming and resource intensive.

- ✓ With this same example and a stateful firewall, you would only need to create the policy allowing your traffic out of your LAN. The firewall would keep track of what is leaving the network and where it’s going with a session table. The firewall would see the return traffic and match that to an existing session therefore allowing the outbound traffic to come back in without the need of an inbound policy with policies like what is in Figure 4.1.



Firewall

Profile: Home

Status: on

Incoming: Deny

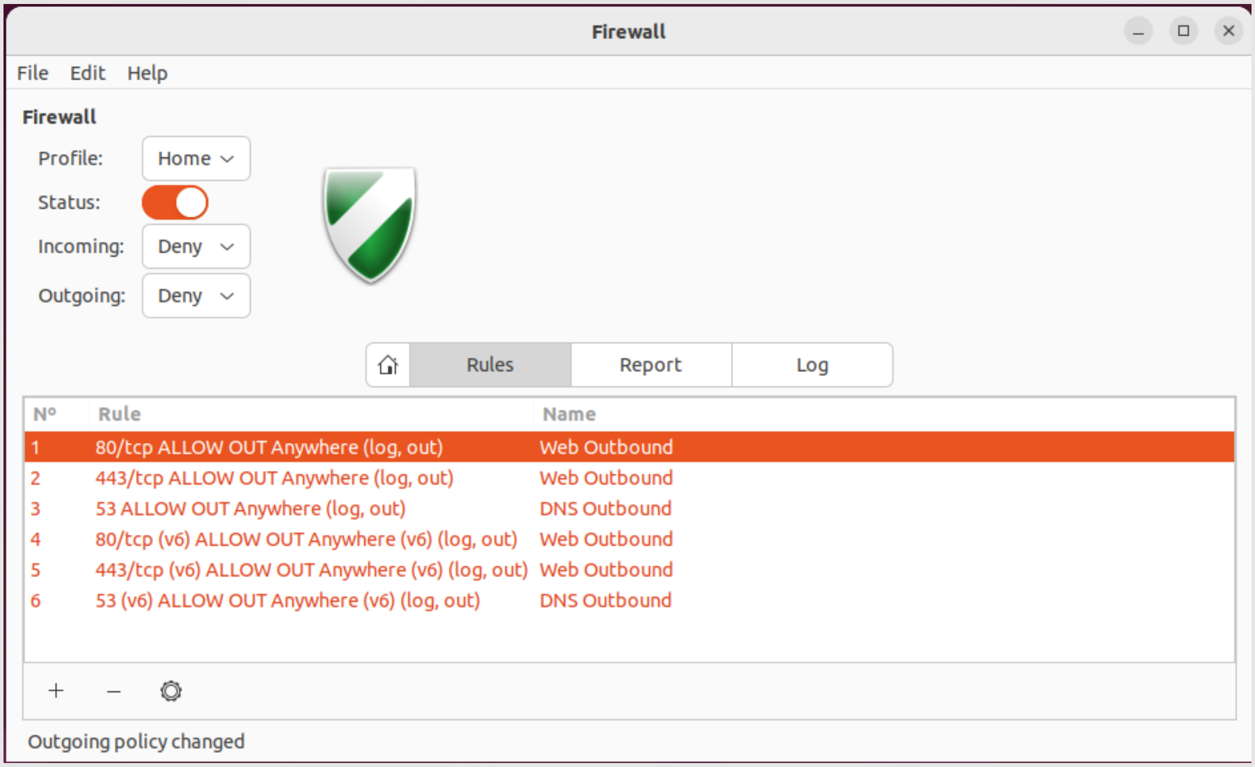
Outgoing: Allow

Nº	Rule	Name
1	80/tcp ALLOW OUT Anywhere (log, out)	Web Outbound
2	443/tcp ALLOW OUT Anywhere (log, out)	Web Outbound
3	80/tcp (v6) ALLOW OUT Anywhere (v6) (log, out)	Web Outbound
4	443/tcp (v6) ALLOW OUT Anywhere (v6) (log, out)	Web Outbound

Rule(s) added

Figure 4.1

- ✓ Realistically we would also need to allow DNS outbound as well so let’s look at Figure 4.2.



Profile: Home

Status: ●

Incoming: Deny

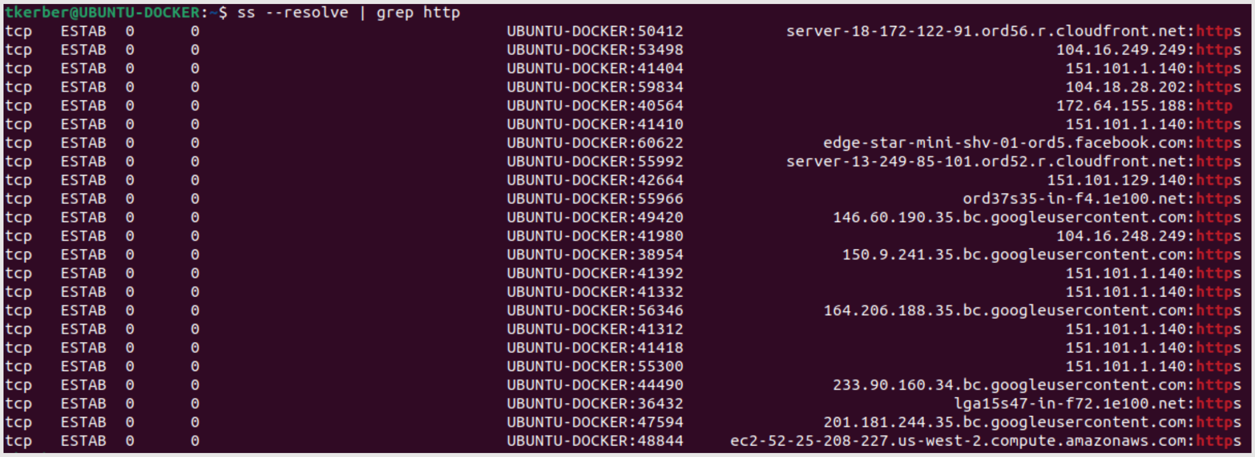
Outgoing: Deny

Nº	Rule	Name
1	80/tcp ALLOW OUT Anywhere (log, out)	Web Outbound
2	443/tcp ALLOW OUT Anywhere (log, out)	Web Outbound
3	53 ALLOW OUT Anywhere (log, out)	DNS Outbound
4	80/tcp (v6) ALLOW OUT Anywhere (v6) (log, out)	Web Outbound
5	443/tcp (v6) ALLOW OUT Anywhere (v6) (log, out)	Web Outbound
6	53 (v6) ALLOW OUT Anywhere (v6) (log, out)	DNS Outbound

Outgoing policy changed

Figure 4.2

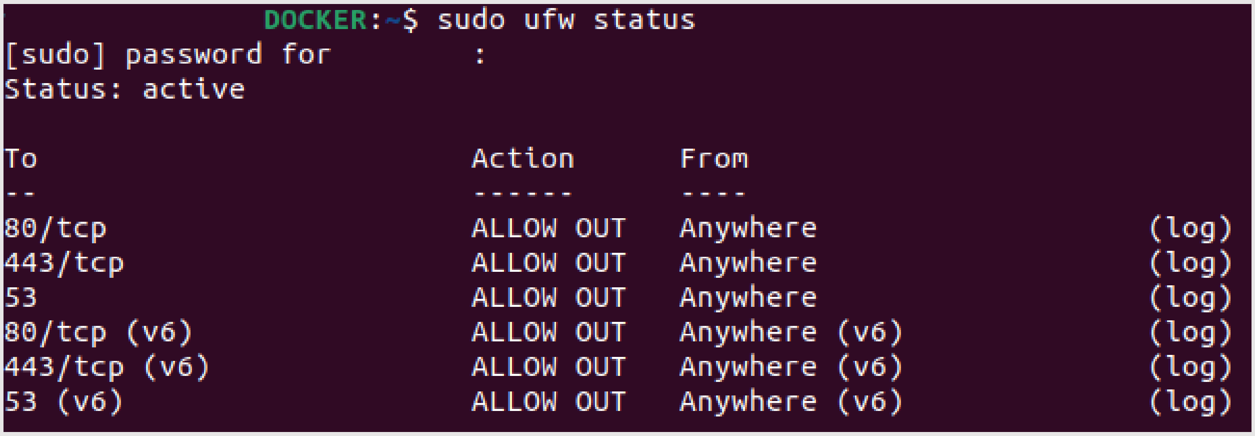
✓ The policy above is now enabled, and I have opened a browser session in my Ubuntu VM and navigated to Facebook. I can confirm these connections in the terminal with the following command and output seen in Figure 4.3.



```
tkerber@UBUNTU-DOCKER:~$ ss --resolve | grep http
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:50412           server-18-172-122-91.ord56.r.cloudfront.net:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:53498                                        104.16.249.249:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41404                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:59834                                         104.18.28.202:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:40564                                        172.64.155.188:http
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41410                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:60622               edge-star-mini-shv-01-ord5.facebook.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:55992           server-13-249-85-101.ord52.r.cloudfront.net:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:42664                                       151.101.129.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:55966                              ord37s35-in-f4.1e100.net:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:49420                146.60.190.35.bc.googleusercontent.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41980                                        104.16.248.249:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:38954                 150.9.241.35.bc.googleusercontent.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41392                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41332                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:56346               164.206.188.35.bc.googleusercontent.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41312                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:41418                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:55300                                         151.101.1.140:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:44490                233.90.160.34.bc.googleusercontent.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:36432                       lga15s47-in-f72.1e100.net:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:47594               201.181.244.35.bc.googleusercontent.com:https
tcp   ESTAB  0       0                                     UBUNTU-DOCKER:48844     ec2-52-25-208-227.us-west-2.compute.amazonaws.com:https
```

Figure 4.3

- ✓ Lastly to see the UFW CLI non-GUI manager I can run the command and see the output in Figure 4.4.



```
               DOCKER:~$ sudo ufw status
[sudo] password for         :
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW OUT   Anywhere                   (log)
443/tcp                    ALLOW OUT   Anywhere                   (log)
53                         ALLOW OUT   Anywhere                   (log)
80/tcp (v6)                ALLOW OUT   Anywhere (v6)              (log)
443/tcp (v6)               ALLOW OUT   Anywhere (v6)              (log)
53 (v6)                    ALLOW OUT   Anywhere (v6)              (log)
```

Figure 4.4

Section Summary

We have learned the importance of state fullness and this concept will become more important later as we cover policies and how they are written.

5. PanOS

Now that we have the basics of firewalls under our belt, we will jump into the wonderful world of Palo Alto Networks. PanOS is the proprietary operating system that runs on all Palo Alto Networks firewalls. What is unique about PanOS is that the exact same software is running on all firewall platforms from the small office PA-220 all the way up to the blade chassis PA-7080s. PanOS also carries the exact same look and feel for both the Panorama and firewalls. This makes it incredibly easy to navigate and find what you are looking for.

Versioning

PanOS versioning is somewhat straight forward to follow but can get confusing with more recent versions of code. Generally, there is a major release once a year and it increments by 1 digit or is a X.1.X release.

So PanOS 9.0.X and 9.1.X are two different major versions but there is no 9.2 - it ends at .1 and then goes to the next major number, 10.0. However, starting with 10, there is now a 10.2 major version. I have pasted a quick list below of valid versions. Highlighted in red are depreciated and no longer supported as of writing this guide. Highlighted in green are currently supported versions. For up-to-date information you can visit the following site: endoflife.date.

- ✓ 7.1
- ✓ 8.0
- ✓ 8.1
- ✓ 9.0
- ✓ 9.1
- ✓ 10.0
- ✓ 10.1
- ✓ 10.2

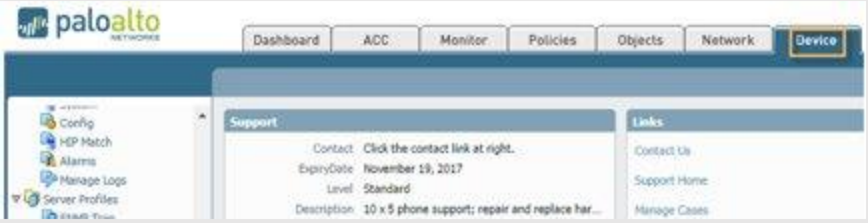
For minor versions see the following example: .9 of 9.0.9 is a minor version and if you see an 'h' like 9.0.9-h1 – This is a minor version with a hotfix.

- *A hotfix is an out-of-cycle version that may fix a specific bug for a specific platform only for example bug found only in the PA-5200 series firewall may be addressed with a hotfix.*

- [Official Palo Alto Networks EOL Announcements]

PanOS UI

As mentioned earlier the PanOS UI has the same look and feel for all models and even between Panorama and firewalls. Below are screenshots of older and current versions of the PanOS web UI. The first is 6.X-7.X, the next is 8.X-9.X, and the last is 10.X. It's not important to see the older versions but I just wanted to show that even as the UI gets refreshed with different colors, logos, etc. It generally has the same look and feel.



Contact Click the contact link at right.
ExpiryDate November 19, 2017
Level Standard
Description 10 x 5 phone support; repair and replace har...

Figure 5.1

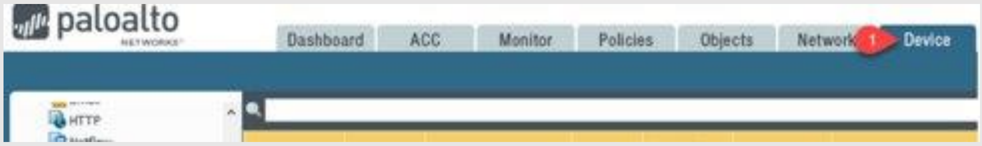


Figure 5.2

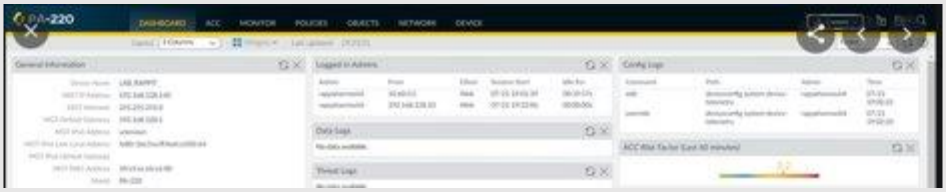
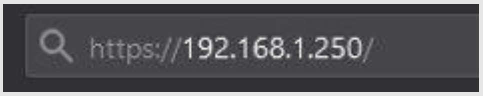


Figure 5.3

PanOS can be manipulated / interfaced with in three ways, the main way we saw in the previous slide is the web GUI. All firewalls and Panoramas come with a web user interface which can be accessed by typing the firewalls FQDN or IP into a browser like our example below:



https://192.168.1.250/

Figure 5.4

PanOS CLI

Next, PanOS has a very robust CLI and much like the Cisco IOS (which many of you have probably learned from your other classes) there are a lot of commands and different modes.

Operational Mode: The first mode you will be in when you connect to a firewall via CLI. It is used to view information and traffic. You can also reboot, load a config, or shut down the device in this mode.

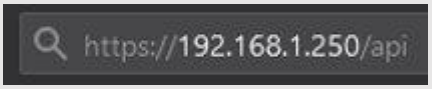
Configure Mode: Use the configuration mode to view and modify the configuration of the device (for example routing, interfaces, etc.)

There are many commands in the PanOS that are very similar to IOS. This guide will not dive into the CLI but if you want to learn more you can check out information in the links below:

- 10.1 Change CLI Modes
- 10.1 CLI Quick Start

PanOS XML and REST API

The API allows you to manage your firewalls and Panorama through a third-party application or custom scripts. This is very powerful for automation and orchestration and the API has essentially many of the same features and functionality as the GUI and CLI. You can access a web browser for the API that helps you create valid API calls by typing the firewall IP in the browser like you normally would but then adding /api behind it like seen in Figure 5.5.



https://192.168.1.250/api

Figure 5.5

The API is a very advanced topic and requires more in-depth knowledge. Using the API is outside of the scope of this guide but just understand what it is at a basic level and how it can be utilized / consumed.

- ❖ 10.1 PanOS Panorama API

Section Summary

In this section we have learned about PanOS, it's different versions and the three different ways to interact with it: GUI, CLI, and XML/REST API.

6. Configurations & Commits

Before learning how to configure policies and settings on our firewalls we need to understand the commit process and the difference between the candidate config and running config. On all Palo Alto Networks firewalls there are two types of configuration files, and both are in XML format. The running config is the config that contains all settings currently active on the firewall. Any changes made in the UI, CLI, or XML API are made on the candidate config. The candidate config is a copy of the running config with staged changes. If a commit operation is performed then the candidate config replaced the running config. You can also save, export, import, and load older configurations or even pieces of configuration files.

Example

In this example we will quickly walk through the logic of adding a new address object and committing it. See Figure 6.1.

✓ The running configuration is what is currently running on and operating the firewall and what is referred to as the data plane.

✓ The candidate configuration is a copy of the running configuration plus the changes you are actively making that are not yet running. You create a new address object in the web UI.

✓ You then perform a commit operation which overwrites the running configuration with the candidate configuration thus activating all changes and adding your address object to the running config.

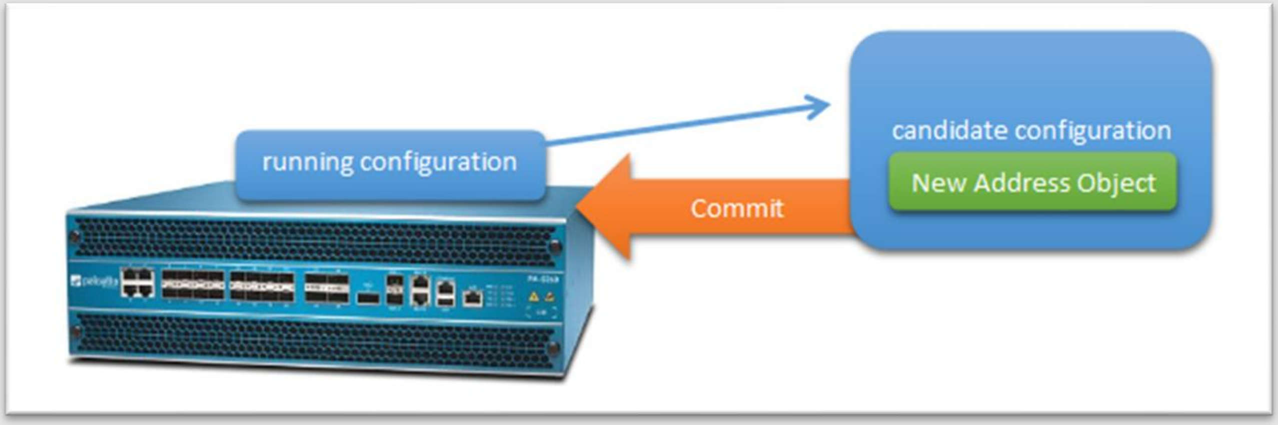


Figure 6.1

- ❖ KB Article: Backing Up and Restoring Configurations
- ❖ KB Article: What is the difference between running configuration and candidate configuration?

7. Mgmt Interface & Admin Accounts

One of the very first configuration changes you will want to make on a Palo Alto Networks firewall is changing the Administrator Account and configuring the Management interface or also referred to as the mgmt interface. Along with the management interface you will want to ensure all network interface profiles only allow ping. You can think of this part as your phase 1 approach of locking the doors and battening down the hatches.

Administrator Types

There are two types of Administrator accounts in the Palo Alto Networks firewalls.

Dynamic – These are default or built-in roles that provide access to the firewall. These will be automatically updated when new features are released.

- **Superuser** – Full access to the entire firewall with no restrictions think of this as like a God mode.
- **Superuser (read-only)** – You can view everything on the firewall, all settings, users, etc.
- **Device administrator** – Full access to all firewall settings except you cannot create new accounts and virtual systems.
- **Device administrator (read-only)** – Read-only access to all firewall settings except password profiles and other admin accounts.
- **Virtual system administrator** – Can only access a selected virtual system and its settings. Think of a virtual system as a completely separate virtual firewall (like a VM) that lives off of a physical firewall. You will not be able to manage interfaces, VLANs, virtual wires, virtual routers, IPSec tunnels, GRE tunnels, DHCP, DNS Proxy, QoS, LLDP, or network profiles with this account.

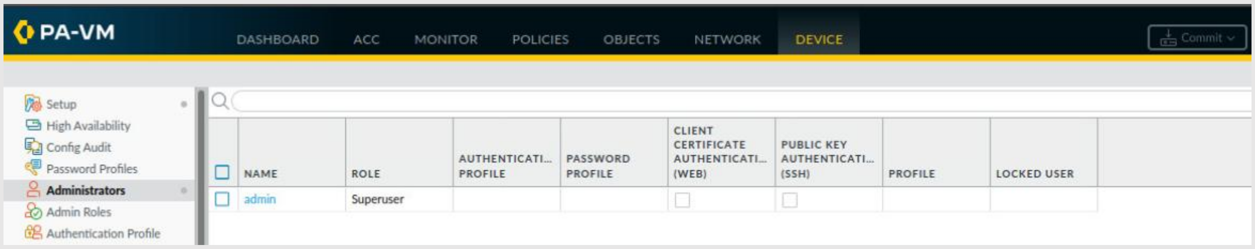
- **Virtual system administrator (read-only)** - This is read-only access to a selected virtual system and its settings much like the previous role.

Role Based – Role based accounts are custom built roles that can be applied to a user. The idea behind this is extreme granularity. Think of scenarios where you would want certain users to only be able to see very specific information or perform specific tasks where dynamic roles are too broad.

Adding and Removing Administrator Example

Now that we know about the different types of accounts see my walk-through below of me creating a new account, committing the changes, logging in with my new account, then finally removing the built-in admin, and committing again.

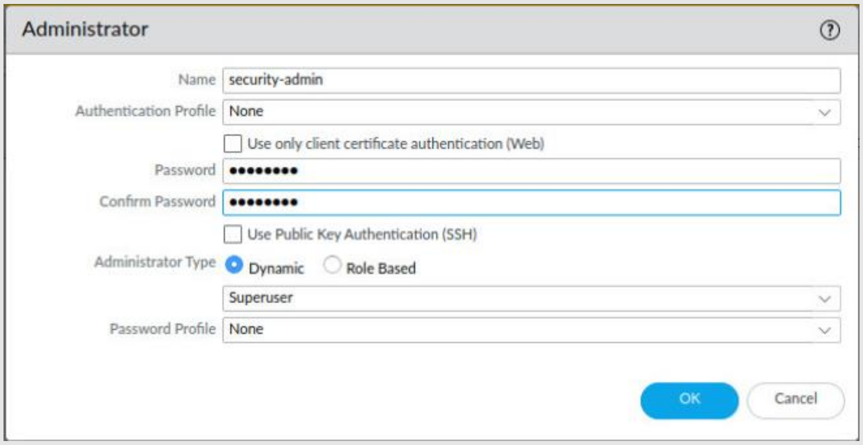
✓ First, I will click add and create my new account.



☐	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE	LOCKED USER
☐	admin	Superuser			☐	☐		

Figure 7.1

✓ Here I fill in the details and choose my dynamic Superuser role.

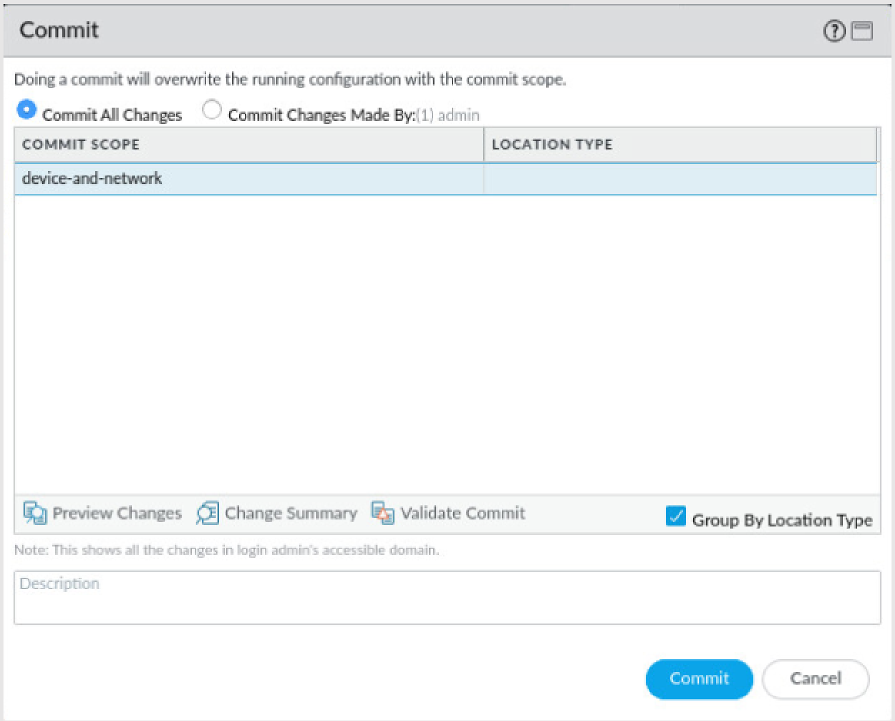


Name: security-admin
Authentication Profile: None
☐ Use only client certificate authentication (Web)
Password: ●●●●●●●●
Confirm Password: ●●●●●●●●
☐ Use Public Key Authentication (SSH)
Administrator Type: ● Dynamic ○ Role Based
Superuser
Password Profile: None

Figure 7.2

- ✓ I commit the changes and when finished click Logout on the lower left-hand corner.

✓



Commit

Doing a commit will overwrite the running configuration with the commit scope.

● Commit All Changes ○ Commit Changes Made By:(1) admin

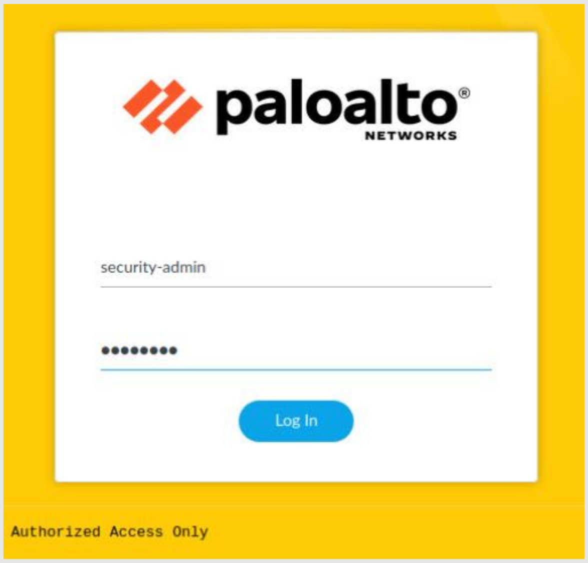
COMMIT SCOPE	LOCATION TYPE
device-and-network	

☑ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Figure 7.3

- ✓ I log in with my new account.



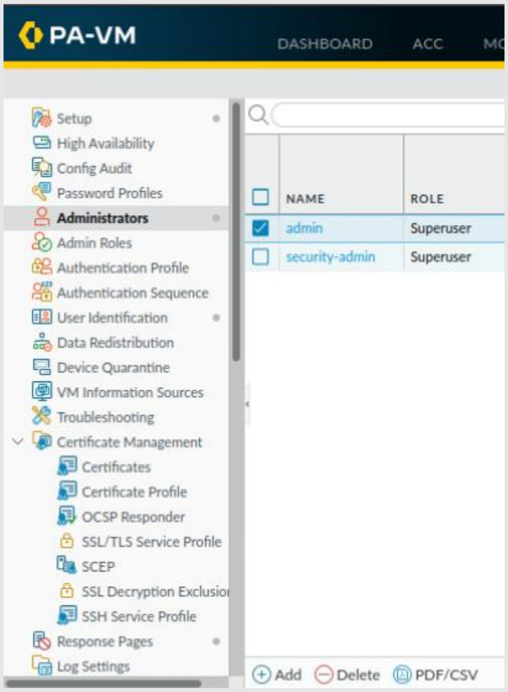
security-admin

●●●●●●●●

Authorized Access Only

Figure 7.4

- ✓ go back and delete the old admin account and then commit the changes one last time.



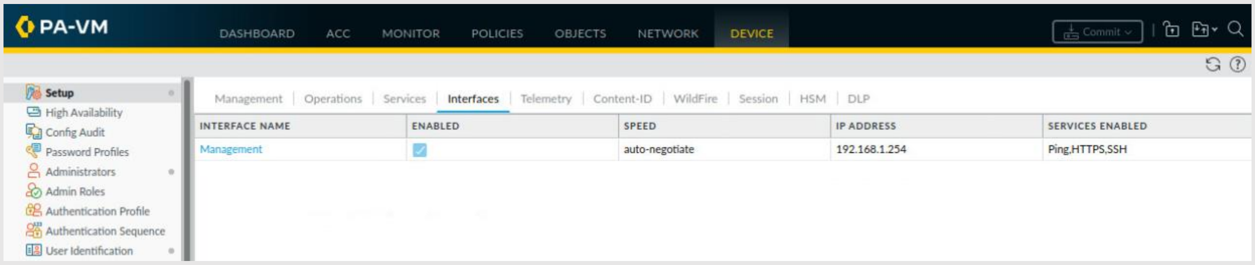
□	NAME	ROLE
☑	admin	Superuser
□	security-admin	Superuser

Figure 7.5

Hardening The Mgmt Interface

We now have our new administrator account created and the default has been removed. We can focus on hardening the management interface with the following demonstration.

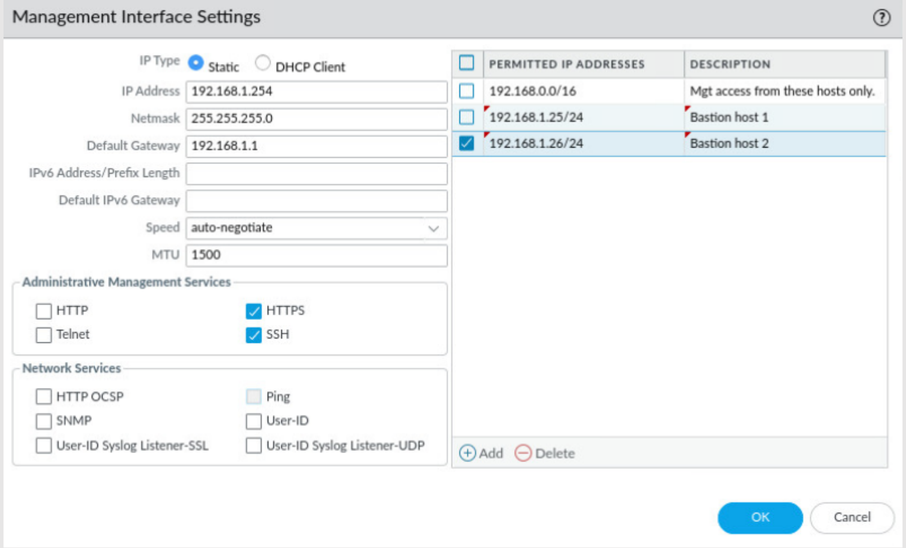
- ✓ We will go back to the Device tab and go to Setup, then choose Interfaces, and click Management.



INTERFACE NAME	ENABLED	SPEED	IP ADDRESS	SERVICES ENABLED
Management	☑	auto-negotiate	192.168.1.254	Ping,HTTPS,SSH

Figure 7.6

- ✓ If possible, lock down the management interface to be accessed only by a secure bastion host or secure access network. This is often a network that is dedicated to securely accessing and managing infrastructure and resources. You will also want to lock down mgmt access to only HTTPS and SSH (if needed). Ping can be enabled if it is absolutely needed.


Management Interface Settings

IP Type ● Static ○ DHCP Client

IP Address 192.168.1.254

Netmask 255.255.255.0

Default Gateway 192.168.1.1

IPv6 Address/Prefix Length

Default IPv6 Gateway

Speed auto-negotiate

MTU 1500

Administrative Management Services

□ HTTP ☑ HTTPS

□ Telnet ☑ SSH

Network Services

□ HTTP OCSP □ Ping

□ SNMP □ User-ID

□ User-ID Syslog Listener-SSL □ User-ID Syslog Listener-UDP

□	PERMITTED IP ADDRESSES	DESCRIPTION
□	192.168.0.0/16	Mgt access from these hosts only.
□	192.168.1.25/24	Bastion host 1
☑	192.168.1.26/24	Bastion host 2

Figure 7.7

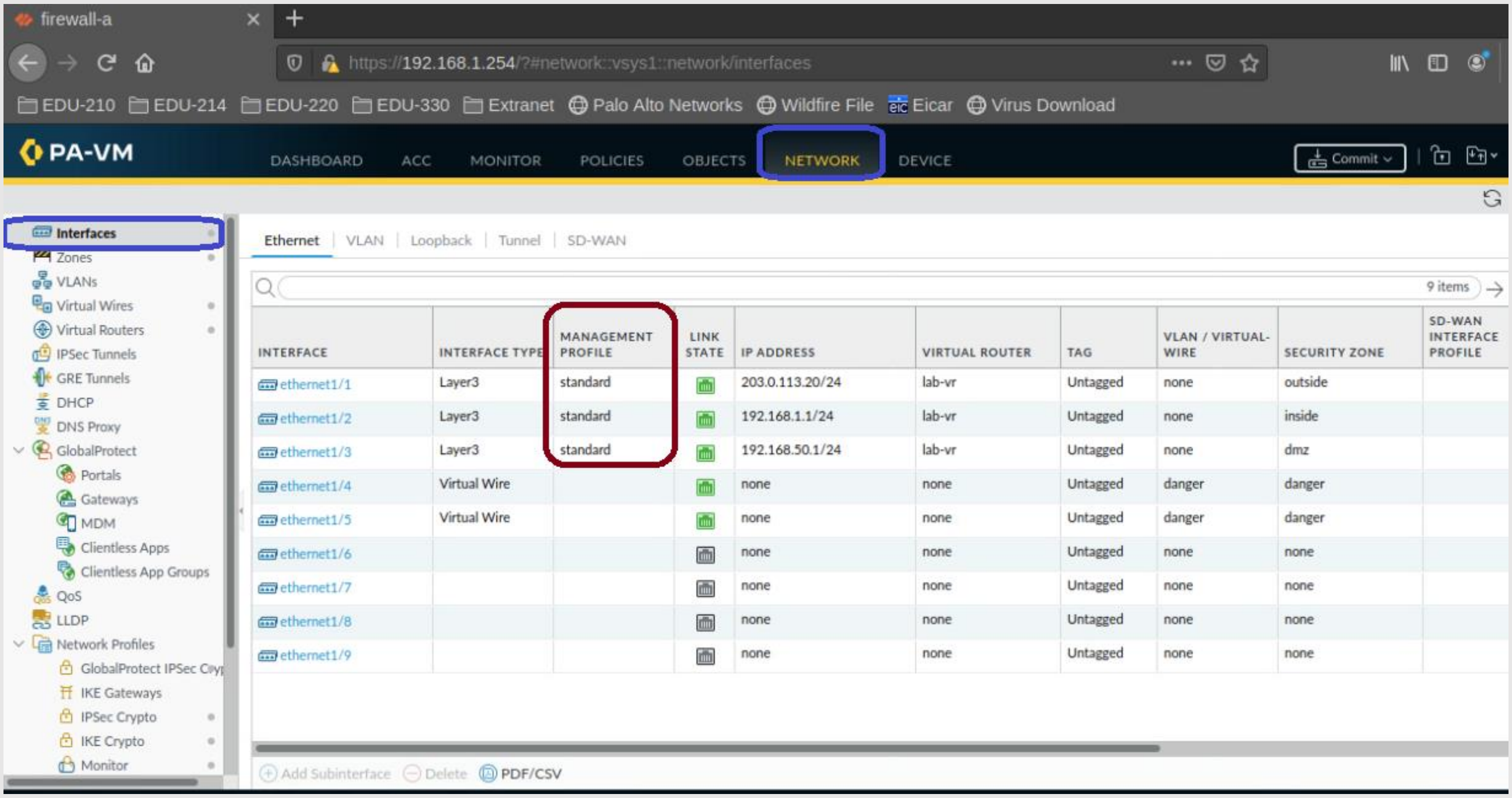
- ✓ Commit your changes and you successfully have setup your mgmt interface and configured a new administrator that is not default.

8. Interface Mgmt Profiles

The management interface has been locked down and our next goal should be checking actual network interfaces for profiles. Like most network devices, you can utilize the actual network interfaces for administration purposes. In the Palo Alto Networks firewalls you can accomplish this by creating a Management Profile and applying it to the appropriate interface. In the CCDC competition you will most likely want to allow all interfaces to ping, but any other services can be considered a risk and disabled.

Removing Unnecessary Services on Management Profiles

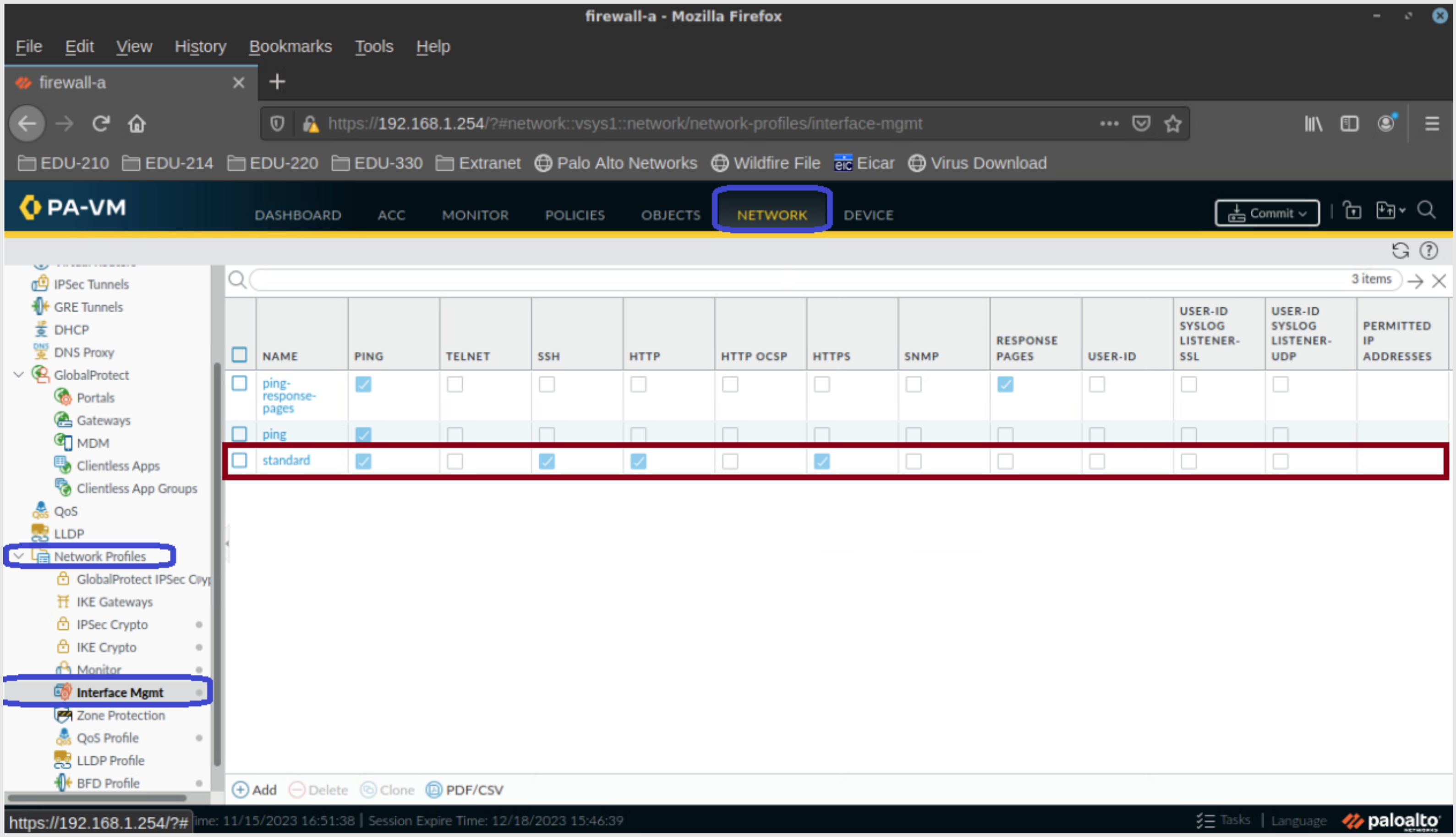
- ✓ Go to Network tab and click on Interfaces.
- ✓ Look at the Management Profile tab for your interfaces.
- ✓ Note in my example we have a Management Profile called standard.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE
ethernet1/1	Layer3	standard	🟩	203.0.113.20/24	lab-vr	Untagged	none	outside	
ethernet1/2	Layer3	standard	🟩	192.168.1.1/24	lab-vr	Untagged	none	inside	
ethernet1/3	Layer3	standard	🟩	192.168.50.1/24	lab-vr	Untagged	none	dmz	
ethernet1/4	Virtual Wire		🟩	none	none	Untagged	danger	danger	
ethernet1/5	Virtual Wire		🟩	none	none	Untagged	danger	danger	
ethernet1/6			▨	none	none	Untagged	none	none	
ethernet1/7			▨	none	none	Untagged	none	none	
ethernet1/8			▨	none	none	Untagged	none	none	
ethernet1/9			▨	none	none	Untagged	none	none	

Figure 8.1

- ✓ Let’s look at what the profile named standard provides by going to Network tab, Network Profiles, Interface Mgmt.

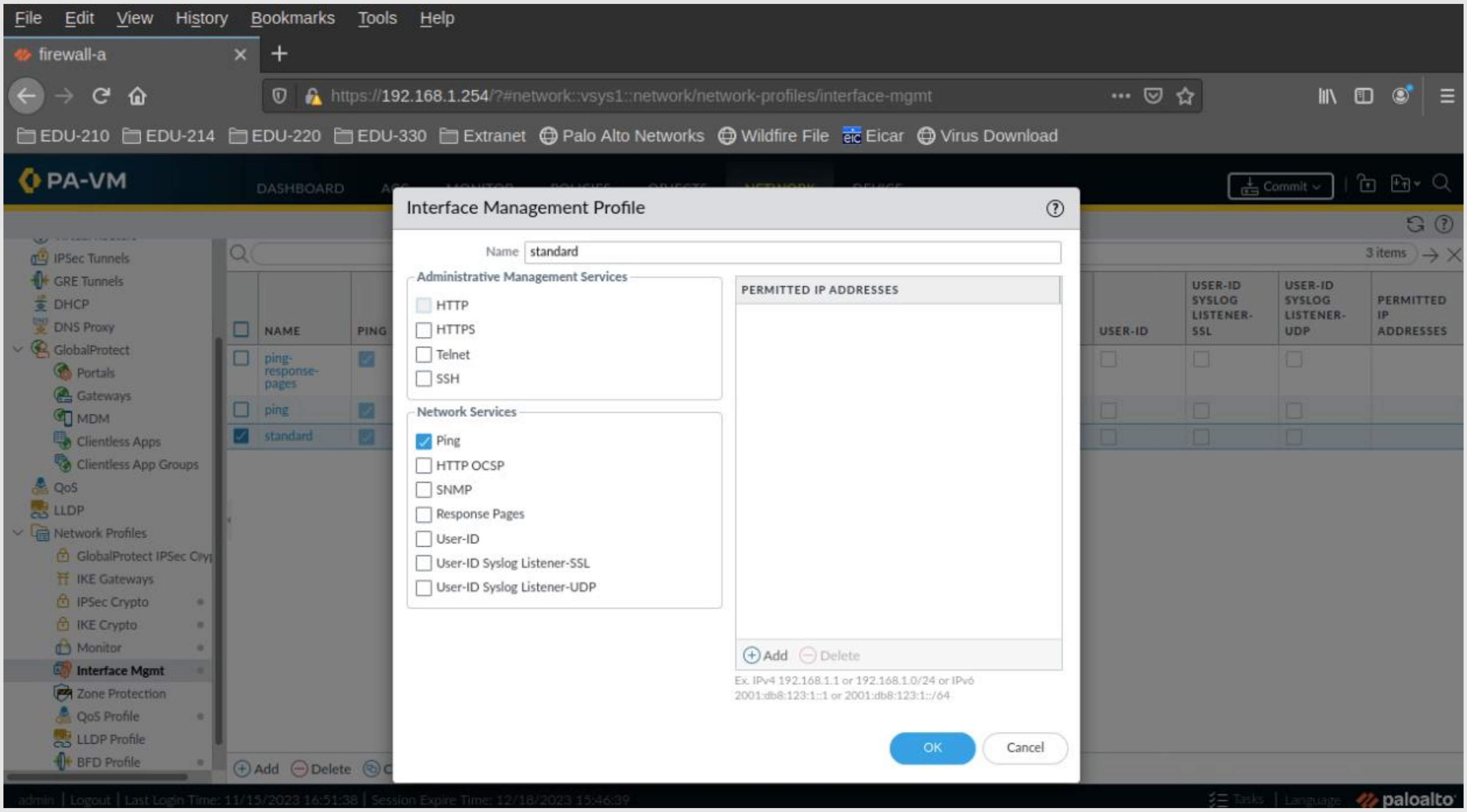

firewall-a - Mozilla Firefox
File Edit View History Bookmarks Tools Help
firewall-a
https://192.168.1.254/?#network::vsys1::network/network-profiles/interface-mgmt
EDU-210 EDU-214 EDU-220 EDU-330 Extranet Palo Alto Networks Wildfire File Eicar Virus Download
PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
Commit
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Cryp
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
BFD Profile
3 items
Add Delete Clone PDF/CSV
https://192.168.1.254/?# ime: 11/15/2023 16:51:38 | Session Expire Time: 12/18/2023 15:46:39
Tasks | Language
paloalto

☐	NAME	PING	TELNET	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	RESPONSE PAGES	USER-ID	USER-ID SYSLOG LISTENER-SSL	USER-ID SYSLOG LISTENER-UDP	PERMITTED IP ADDRESSES
☐	ping-response-pages	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	
☐	ping	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
☐	standard	☑	☐	☑	☑	☐	☑	☐	☐	☐	☐	☐	

Figure 8.2

- ✓ Observe that this profile allows a lot of services we really don’t need enabled on all our network interfaces, particularly HTTP.

- ✓ Remove this access by opening the standard profile and unchecking all services except ping. Once completed you can commit these changes and verify by testing.



Interface Management Profile

Name: standard

Administrative Management Services

- □ HTTP
- □ HTTPS
- □ Telnet
- □ SSH

Network Services

- ☑ Ping
- □ HTTP OCSP
- □ SNMP
- □ Response Pages
- □ User-ID
- □ User-ID Syslog Listener-SSL
- □ User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES

Add Delete

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

OK Cancel

Figure 8.3

✓ Congratulations you’ve now hardened the network interfaces. If you want to learn more about device hardening, see the following KB article.

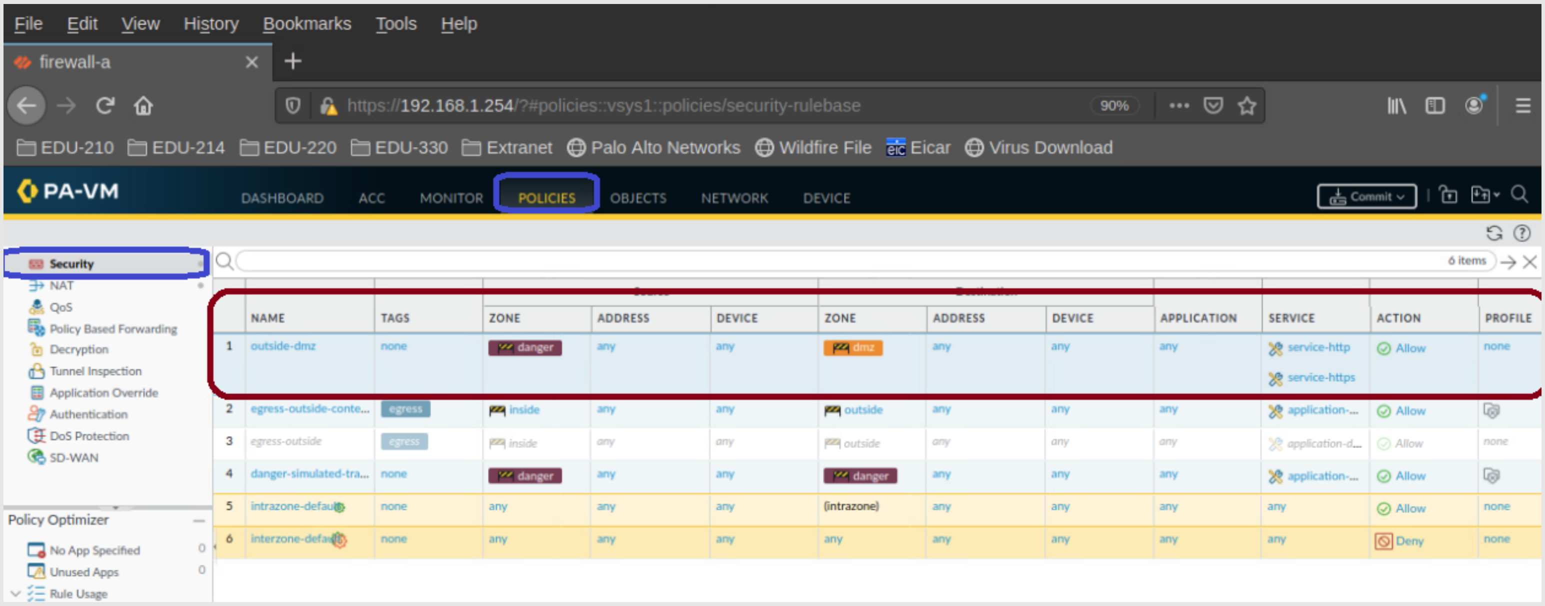
❖ KB Article: Configuration Hardening Guide

9. App-ID & Content-ID

App-ID and Content-ID are two very important elements of utilizing the Palo Alto Networks NGFW. They are arguably the two features that make the PAN a NGFW. In the CCDC competition leveraging these is going to be a critical component to securing the network. There will most likely be policies created already but they may be overly permissive and not be utilizing App-ID or Content-ID. In this walk-through I will demonstrate how to utilize App-ID and Content-ID. This section will not cover how to create policies from scratch. Additional resources will be linked for that.

Enabling App-ID

- ✓ Let’s look at the policies at the Policies tab, then navigate to Security.

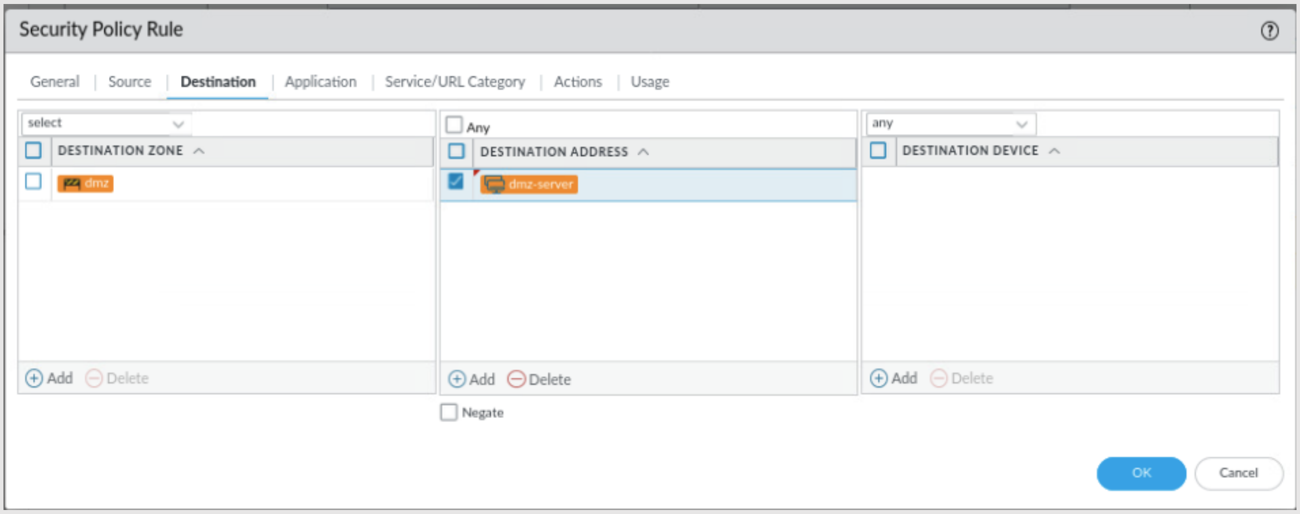


	NAME	TAGS	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	outside-dmz	none	danger	any	any	dmz	any	any	any	service-http service-https	Allow	none
2	egress-outside-conte...	egress	inside	any	any	outside	any	any	any	application-...	Allow	
3	egress-outside	egress	inside	any	any	outside	any	any	any	application-d...	Allow	none
4	danger-simulated-tra...	none	danger	any	any	danger	any	any	any	application-...	Allow	
5	intrazone-default	none	any	any	any	(intrazone)	any	any	any	any	Allow	none
6	interzone-default	none	any	any	any	any	any	any	any	any	Deny	none

Figure 9.1

- ✓ Notice that this rule I’ve highlighted is wide open. Anything from danger (internet) can talk to anything in the DMZ over port 80 and 443. We could lock this down a lot better while still allowing all necessary communication.

- ✓ Open the policy and go to the Destination tab. In my scenario I only have one web server in the DMZ so I create a new address object for it and move to the Application tab.



Security Policy Rule

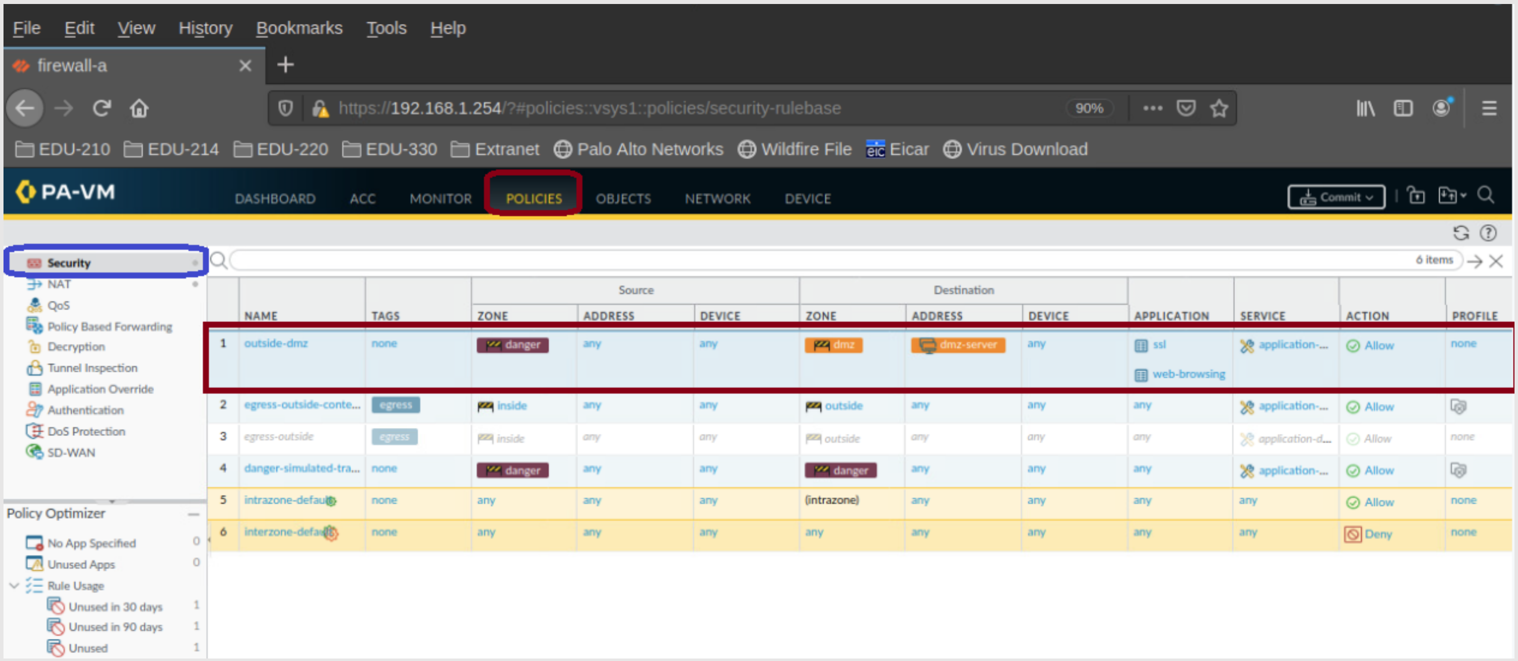
General | Source | Destination | Application | Service/URL Category | Actions | Usage

select	Any	any
□ DESTINATION ZONE	□ DESTINATION ADDRESS	□ DESTINATION DEVICE
□ dmz	☑ dmz-server	

⊕ Add ⊖ Delete
□ Negate
OK
Cancel

Figure 9.2

- ✓ In the application tab add web-browsing and SSL. Next go to the Service tab and remove the service-http and service-https and select application-default in the dropdown box. By doing this we're allowing the PAN to utilize the App-ID engine to determine what ports these apps use.
- ✓ Go look at these Apps in the Applepedia or under Objects and Applications, you can see it's TCP 80 and TCP 443.



File Edit View History Bookmarks Tools Help
firewall-a
https://192.168.1.254/?#policies::vsys1::policies/security-rulebase
90%
EDU-210 EDU-214 EDU-220 EDU-330 Extranet Palo Alto Networks Wildfire File Eicar Virus Download
PA-VM
DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE
Commit
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
6 items

			Source			Destination						
	NAME	TAGS	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE
1	outside-dmz	none	danger	any	any	dmz	dmz-server	any	ssl web-browsing	application-...	Allow	none
2	egress-outside-conte...	egress	inside	any	any	outside	any	any	any	application-...	Allow	
3	egress-outside	egress	inside	any	any	outside	any	any	any	application-d...	Allow	none
4	danger-simulated-tra...	none	danger	any	any	danger	any	any	any	application-...	Allow	
5	intrazone-default	none	any	any	any	(intrazone)	any	any	any	any	Allow	none
6	interzone-default	none	any	any	any	any	any	any	any	any	Deny	none

Policy Optimizer

No App Specified	0
Unused Apps	0
Rule Usage	
Unused in 30 days	1
Unused in 90 days	1
Unused	1

Figure 9.3

- ✓ When finished with all these changes, commit them and start testing. Look for policy hit count and if necessary, go to the Monitor tab and look at Traffic logs.

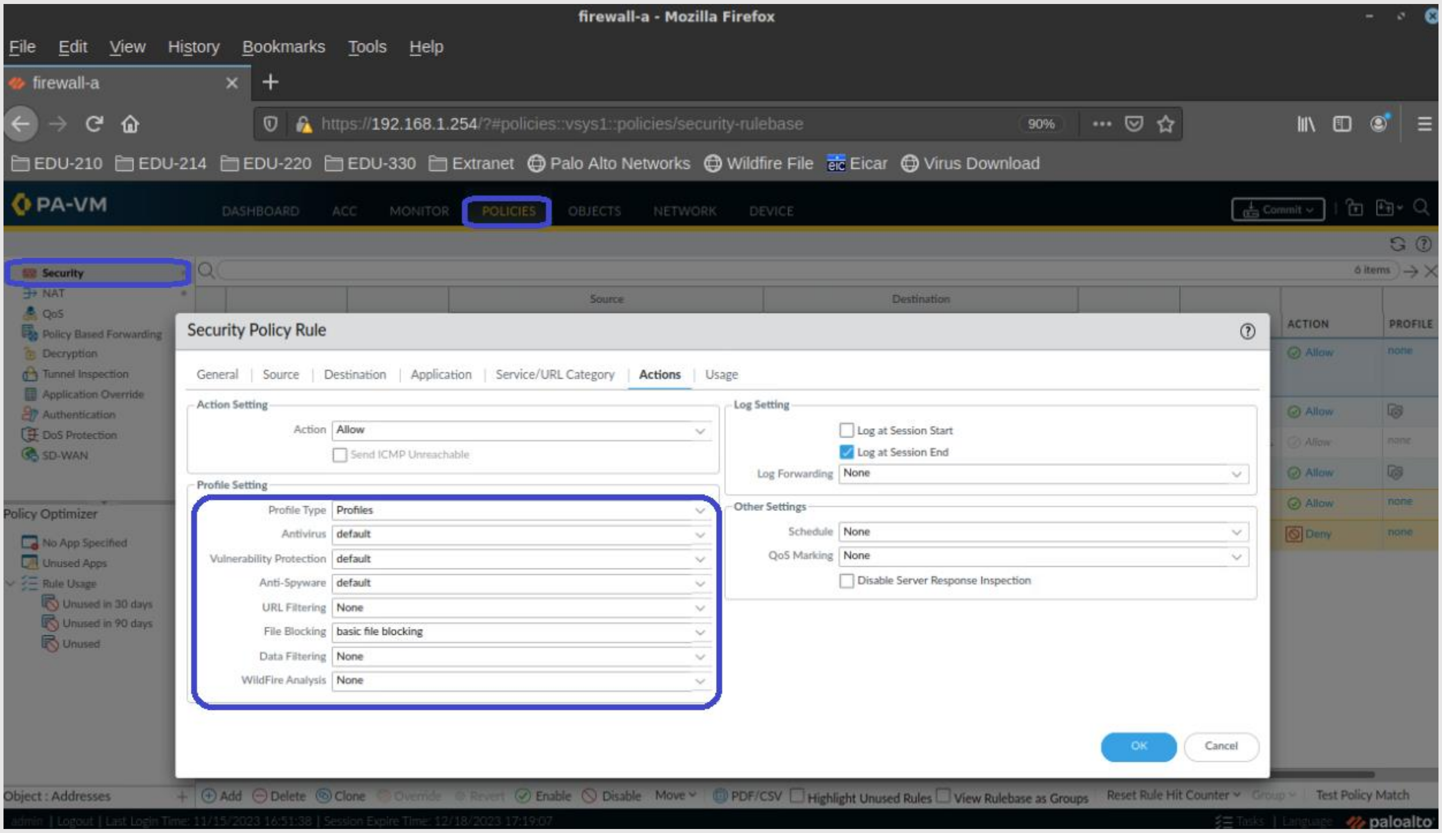
- ✓ Looking at our policy we now see that our destination has been changed to a single server and instead of using ports we are utilizing App-ID and letting App-ID determine what ports are necessary for these applications.

Enabling Content-ID

Enabling Content-ID is quite simple if we use the default built-in profiles provided by Palo Alto Networks. In the real world we would want to ensure our security profiles align with our organizational policies and risk appetite. For the sake of the CCDC I am simply going to enable default profiles.

- ✓ Under Policies in the Security section, you will open the previous policy we worked on in the App-ID section.

- ✓ Go to the Actions tab and under Profile Settings select Profiles and see my example utilizing default and built-in profiles.



Security Policy Rule

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: default

URL Filtering: None

File Blocking: basic file blocking

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Figure 9.4

- ✓ Once completed go ahead and commit your changes.

10. CCDC Practice Checklist

In this final section I have created a sample CCDC checklist. I recommend using a lab environment like NDG to simulate this checklist.

- ✓ Change all administrator passwords and disallow SSH Public Key Authentication unless specified.
- ✓ Disallow all services on the MGMT interface except HTTPS, Ping, and SSH (only if it is needed).
- ✓ Create a Permitted IP list on the MGMT interface and lock it down to a few select bastion hosts.
- ✓ Ensure all network interfaces do not allow any service other than ping. These services would be allowed via a management profile you will have to investigate.
- ✓ Investigate security policies and look for opportunities to utilize App-ID where possible. Take note of how permissive policies are. Do they allow entire subnets? Entire zones?
- ✓ Double-check zone usage on security policies and make sure they are not overly permissive.
- ✓ If necessary, you may need to clone existing security policies and create your own underneath. When completed you can disable old policies and test. Practice cloning policies and enable/disable feature.
- ✓ It might be easier to create objects for your servers in your different zones. With objects you can quickly add or remove these devices to policies as needed. Practice object creation with IP addresses and subnets.

- ✓ Check NAT policies and ensure they are configured to allow only what is necessary for your servers and workstations to function.
- ✓ Leverage Content-ID built-in profiles in your security policies
- ✓ Commit your changes and start testing!
- ✓ Can you get to your servers and utilize necessary services?
- ✓ Go to the Monitor tab and look at Traffic logs and Threat logs. What do you see?
- ✓ HAVE FUN!

Reference Documents

Document / Link	Description	Type
KB Article: Configuration Hardening Guide	A quick KB article for general device hardening	KB Article
KB Article: Backing Up and Restoring Configurations	A KB article describing how to back up and restore firewall config files.	KB Article
KB Article: What is the difference between running configuration and candidate configuration?	A KB article describing the difference between running and candidate config.	KB Article
Applepedia	A Palo Alto Networks hosted site to show all current applications that can be used in policies.	Applepedia
TechDocs: App-ID Overview	A Palo Alto Networks Tech Docs article describing App-ID from a high-level.	Tech Docs
TechDocs: Configure NAT	A Palo Alto Networks Tech Docs article describing NAT policies and how to configure them.	Tech Docs

Revisioning

Version	Description	Date	Author / Editor
1.0	Initial document creation.	11/18/2023	Kerber, Taylor