



Palo Alto Networks Cybersecurity Academy – Setting up a PA220 Firewall for a SOHO Environment

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

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

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. 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. The PA220 also prevents threats by filtering URLs and securing against DNS-based attacks. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The PA220 doesn't have a fan, and instead uses hexagon-shaped vents to passively filter air. The firewall's compact form factor allows it to easily fit alongside existing network devices.

Palo Alto firewalls run on an operating system called PAN-OS. PAN-OS can be controlled through two methods: a Graphical User Interface (GUI) and a Command-Line Interface (CLI). The GUI is accessible through an HTTP connection and displays in any modern web browser. The HTTP connection is available through the firewall's MGT port and by default, is accessible at <http://192.168.1.1>. The firewall has a default username and password of *admin*.

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.

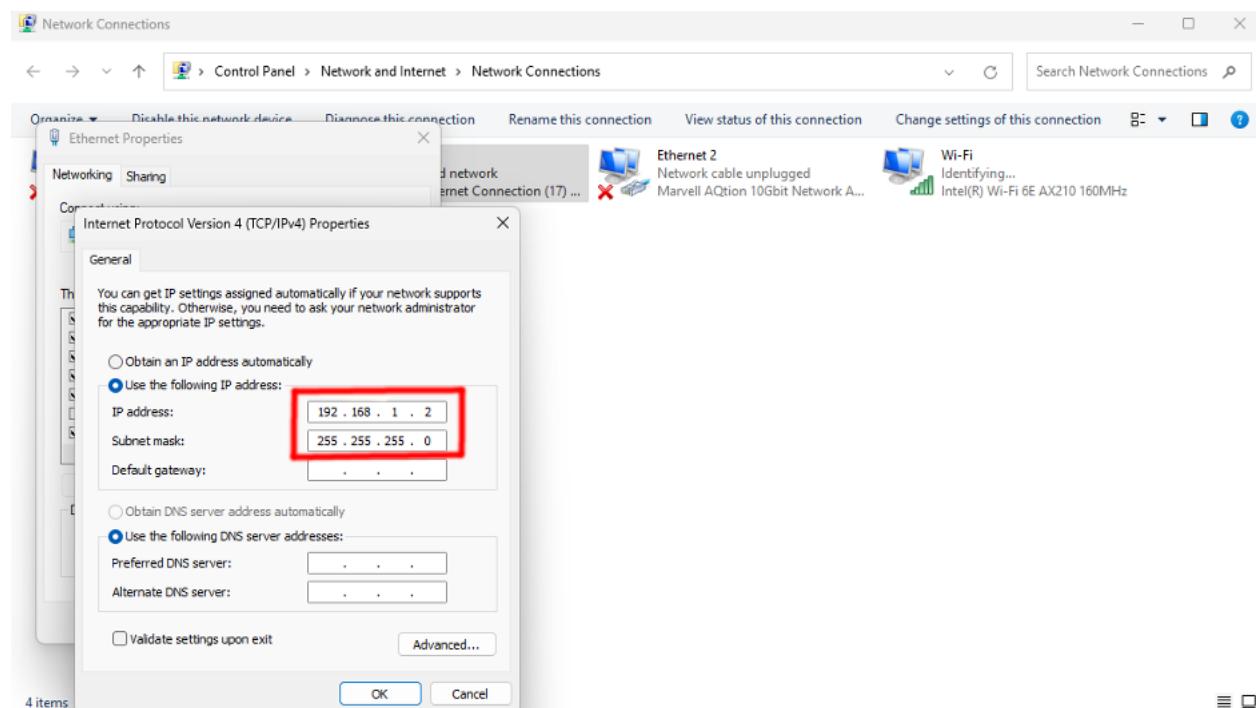
PAN-OS's GUI has a variety of settings and tools to control advanced functionality of the router. The GUI's default page is a dashboard that displays vital information, such as console messages and link states of ports.

Lab Summary

In this lab, we configured our firewall to connect to a DHCP-enabled ISP router and configured this traffic to be untrusted by default. We then configured the remainder of the router ports to be connected by a single VLAN, have trusted traffic, and be DHCP clients served by the firewall.

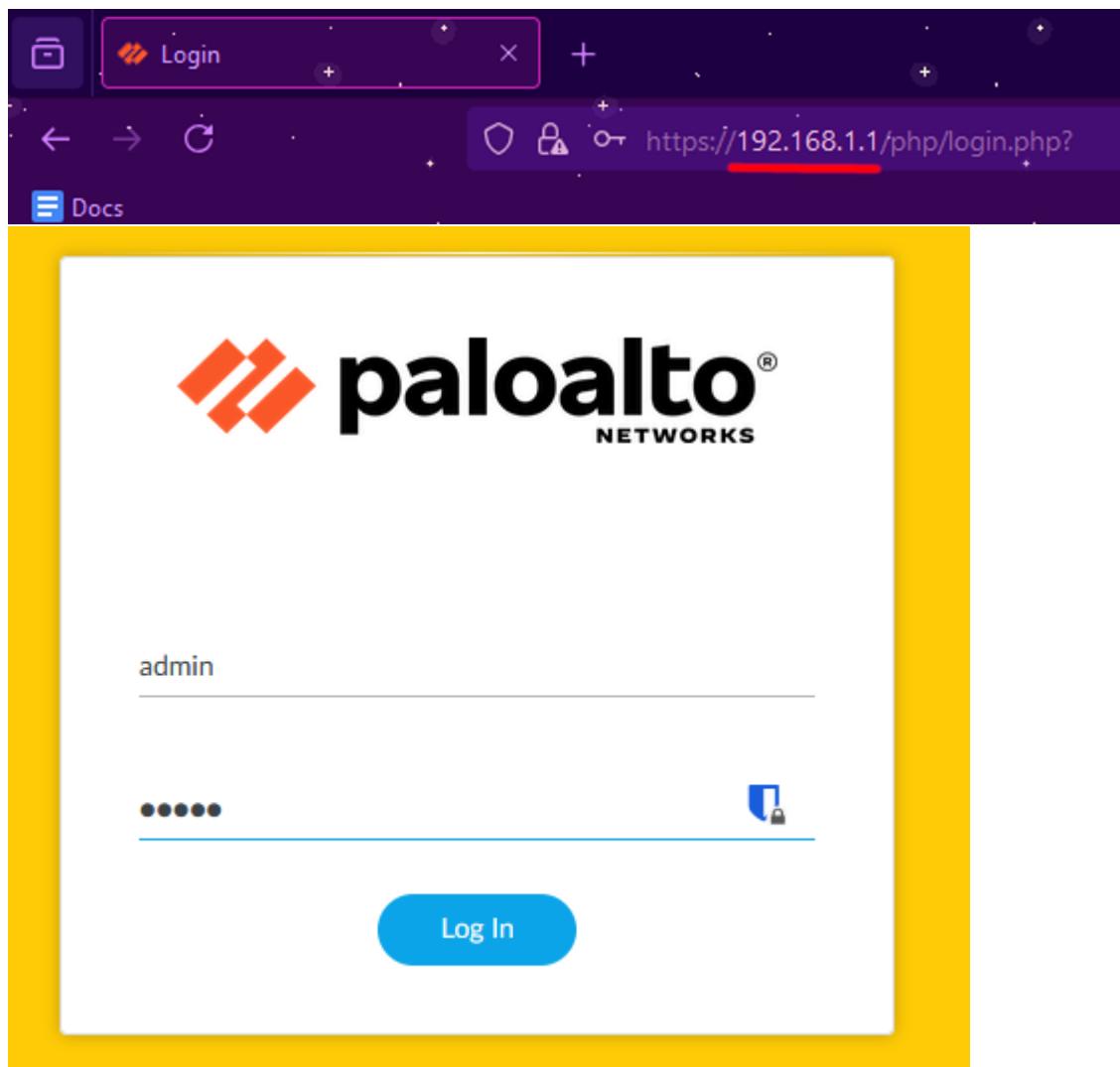
Lab Commands

Make sure the PA220 is connected to power and that the STAT, TEMP, and PWR lights are green. Connect an ethernet cable from the MGT port to a PC. Set the PC's IP address to 192.168.1.2 with a subnet mask of 255.255.255.0.



In a web browser, connect to 192.168.1.1. (Note: only some browsers are officially supported. Firefox works universally, Chrome works on Windows and Mac OS)

You should see a login page. Log into the default account, which has the username and password *admin*.



After a login, you will be prompted to reset the administrator's password. Choose a secure password to keep your firewall secure.

Connect the ethernet1/1 port of the firewall to the router provided by your ISP.

In the PA220's dashboard, go to the *Interfaces* section of the *Network* tab.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Virtual Wire		Up	none	none	Untagged	default-vwire	untrust		Disabled		
ethernet1/2	Virtual Wire		Up	none	none	Untagged	default-vwire	trust		Disabled		
ethernet1/3	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		
ethernet1/4	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		
ethernet1/5	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		
ethernet1/6	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		
ethernet1/7	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		
ethernet1/8	Virtual Wire		Up	none	none	Untagged	none	none		Disabled		

Under *ethernet1/1*, change the interface type to *Layer3*, the virtual router to default, and under *Security Zone*, click *New Zone*.

Ethernet Interface

Interface Name: ethernet1/1

Comment:

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

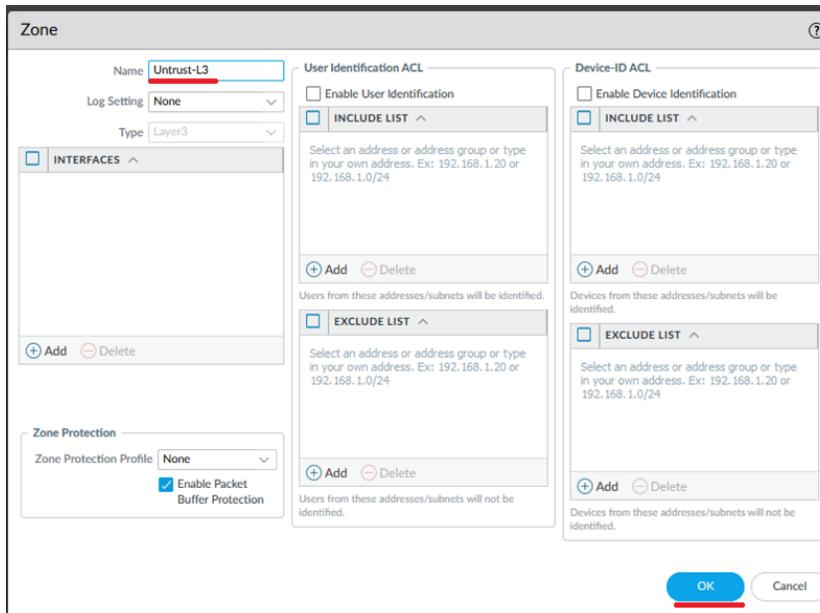
Virtual Router: default

Security Zone: None

New Zone

OK Cancel

Name this zone Untrust-L3. This zone will be used for untrusted IP traffic on the connection to the ISP.



Click on the IPv4 section. Set the type to *DHCP Client* and ensure that *Automatically create default route pointing to default gateway provided by server* is enabled.

Config | **IPv4** | IPv6 | SD-WAN | Advanced

<input type="checkbox"/> Enable SD-WAN	<input type="checkbox"/> Enable Bonjour Reflector
Type <input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP Client	
<input checked="" type="checkbox"/> Enable	
<input checked="" type="checkbox"/> Automatically create default route pointing to default gateway provided by server	
<input type="checkbox"/> Send Hostname	system-hostname
Default Route Metric	10
Show DHCP Client Runtime Info	
OK Cancel	

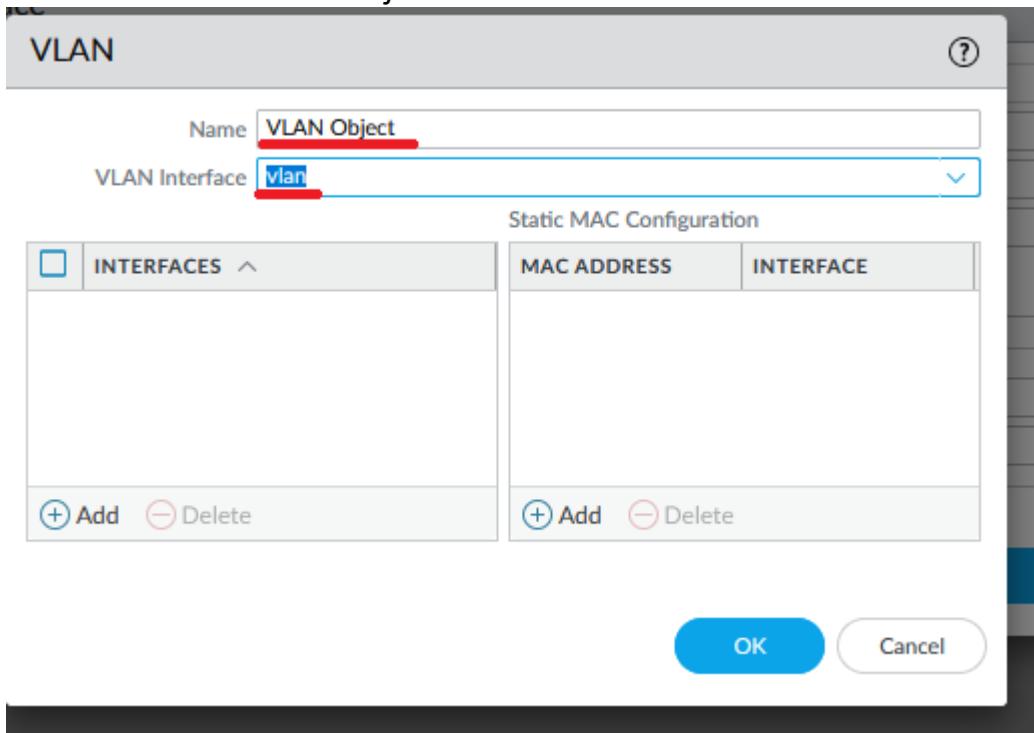
Next, go to the *Virtual Wires* section, select *default-vwire*, and click *Delete*.

The screenshot shows the PA-220 interface configuration interface. The left sidebar contains a tree view of configuration categories: Interfaces, Zones, VLANs, and Virtual Wires. The 'Virtual Wires' category is selected and expanded, showing sub-options like Virtual Routers, IPsec Tunnels, GRE Tunnels, DNS Proxy, GlobalProtect, Portals, Gateways, iNQM, Clientless Apps, Clientless App Groups, QoS, UDP, Network Profiles, and GlobalProtect IPsec Crypto. The main panel displays a table titled 'INTERFACES' with one item: 'default_wire'. The table columns are NAME, INTERFACES, INTERFACE2, TAG ALLOWED, MULTICAST FIREWALLING, and LINK STATE PASS THROUGH. A red arrow points to the 'Delete' button at the bottom of the table.

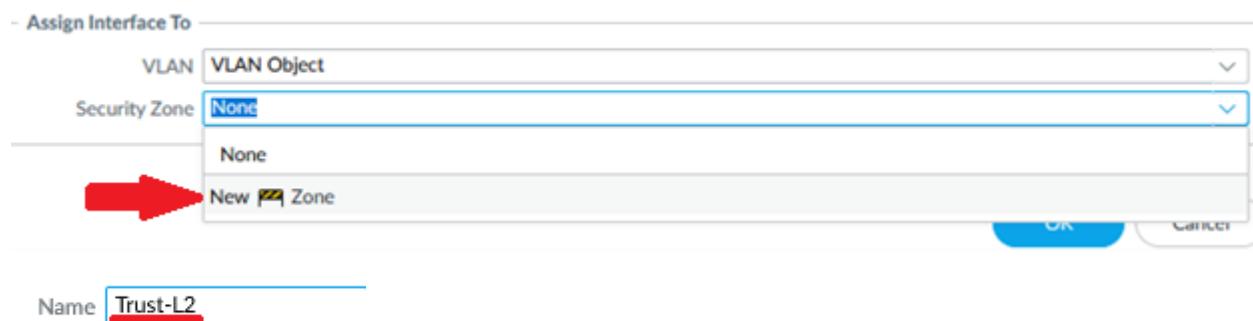
Return to the interfaces tab. Under `ethernet1/2`, set the interface type to Layer2, and under VLAN, click New VLAN.

The screenshot shows the 'Ethernet Interface' configuration dialog box. The 'Config' tab is selected. The 'Interface Name' field is set to 'ethernet1/2'. The 'Interface Type' dropdown is set to 'Layer2'. The 'Netflow Profile' field is set to 'None'. In the 'Assign Interface To' section, the 'VLAN' dropdown is set to 'None'. A red arrow points to the 'New VLAN' link, which is highlighted in blue. The 'OK' and 'Cancel' buttons are at the bottom right.

Name this VLAN *VLAN Object* and set the VLAN Interface to *vlan*.



Under *Security Zone*, click *New Zone*. Name this zone *Trust-L2*.



Repeat this process for interfaces *ethernet1/3* through *ethernet1/8* using the VLAN and Security Zone created for *ethernet1/2*. These ports will be used for trusted traffic on the local network.

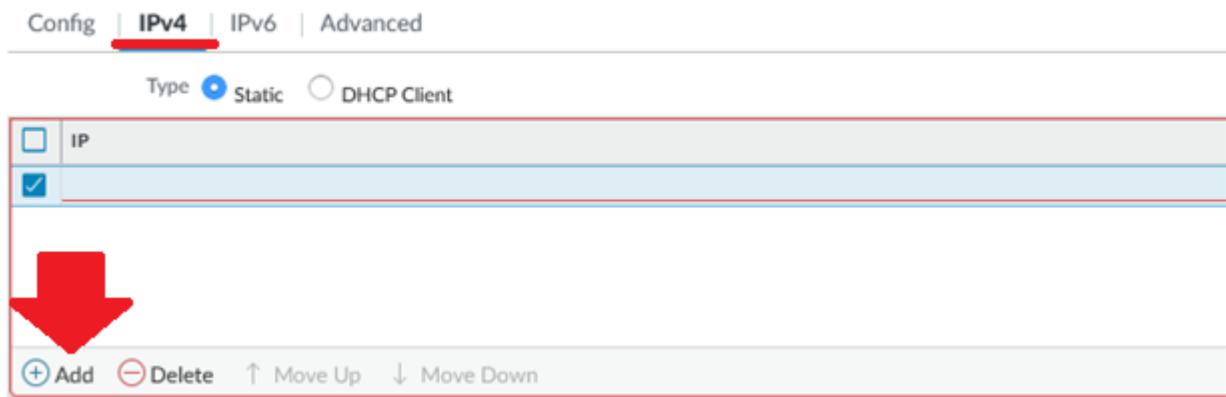
Go to the *VLAN* section of *Interfaces* and click on *vlan*.



Set the virtual router to *default* and create a new security zone called *Trust-L3*.

Name

This VLAN will be used as a gateway for all hosts connected to the firewall. Go to the *IPv4* tab and click *Add* under the *IP* section.



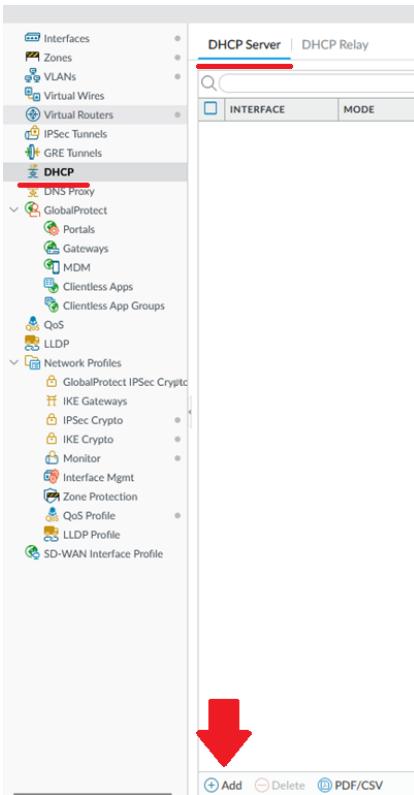
Create a new address and name it *Gateway*, assigning it an appropriate description. Choose a subnet for your local network and set the IP to an address within this subnet. In this lab, we used the last host address in the 192.168.1.0/24 network.

The screenshot shows the 'Address' creation dialog box. It has fields for 'Name' (set to 'Gateway'), 'Description' (set to 'Default gateway for eth1/2-eth1/8'), 'Type' (set to 'IP Netmask'), and an 'IP Netmask' input field containing '192.168.1.254/24'. There is also a 'Resolve' button next to the IP field. At the bottom right are 'OK' and 'Cancel' buttons.

Name	<input type="text" value="Gateway"/>
Description	<input type="text" value="Default gateway for eth1/2-eth1/8"/>
Type	IP Netmask
IP Netmask	<input type="text" value="192.168.1.254/24"/> Resolve
Tags	<input type="text"/>

OK Cancel

Next, set up the DHCP server. Go to the *DHCP* section and click *Add*.



Set the interface to *vlan* and the mode to *enabled*. Click *Add* under *IP Pools* and add all the assignable addresses in the subnet. In this case, the IP range was 192.168.1.2-192.168.1.253.

DHCP Server

RESERVED ADDRESS	MAC ADDRESS	DESCRIPTION
192.168.1.20	xx:xx:xx:xx:xx:xx	(Optional MAC Address)

Interface: *vlan* Mode: *enabled*

Lease Options

Ping IP when allocating new IP

Lease: Unlimited Timeout

IP POOLS ^
192.168.1.2-192.168.1.253

Add **Delete** **OK** **Cancel**

A red arrow points down to the 'Add' button at the bottom left of the IP Pools table.

Go to the *Options* tab. Set the gateway/mask to the IP/mask assigned to the vlan interface (In this case, 192.168.1.254 and 255.255.255.0). Set the primary and secondary DNS to valid DNS servers (In this case, we used Cloudflare's DNS servers, 1.1.1.1 and 1.0.0.1).

Inheritance Source	None
Gateway	192.168.1.254
Subnet Mask	255.255.255.0
Primary DNS	1.1.1.1
Secondary DNS	1.0.0.1
Primary WINS	None
Secondary WINS	None
Primary NIS	None
Secondary NIS	None
Primary NTP	None
Secondary NTP	None
POP3 Server	None
SMTP Server	None
DNS Suffix	None

Go to Objects > Security Profile Groups and click the Add button. Set the name to Internet, the anti-spyware profile to *strict*, and the vulnerability protection profile to *strict*.

NAME	LOCATION	ANTIVIRUS PROFILE	ANTI-SPYWARE PROFILE	VULNERABILITY PROTECTION PROFILE	URL FILTERING PROFILE	FILE BLOCKING PROFILE	DATA FILTERING PROFILE	WILDFIRE ANALYSIS PROFILE
internet		default	strict	strict	default			

Security Profile Group

Name:	internet
Antivirus Profile:	default
Anti-Spyware Profile:	strict
Vulnerability Protection Profile:	strict
URL Filtering Profile:	default
File Blocking Profile:	None
Data Filtering Profile:	None
Wildfire Analysis Profile:	None

OK **Cancel**

Go to Policies > Security and click the Add button. Name this policy *Internet Outgoing* and set the description to *All traffic to the internet*. This policy will be implemented on ethernet1/1, the connection to the ISP.

The screenshot shows the Palo Alto Networks PA-220 interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES (selected), OBJECTS, NETWORK, DEVICE, and a Commit button. On the left, a sidebar lists Security features like NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. Below the sidebar is a 'Policy Optimizer' section with links for New App Views, Rules Without Apps, Unused Apps, Log Forwarding, and Rule Usage. The main panel displays a table of security policy rules:

NAME	TAGS	TYPE	Source			
			ZONE	ADDRESS	USER	DEVICE
rule1	none	universal	trust	any	any	any
intrazone-default	none	intrazone	any	any	any	any
interzone-default	none	interzone	any	any	any	any

A modal window titled 'Security Policy Rule' is open, showing the 'General' tab. The 'Name' field is set to 'Internet Outgoing', 'Rule Type' is 'universal (default)', and 'Description' is 'All traffic to internet'. The 'Source' tab is also visible at the top of the modal.

Go to the *Source* tab and set the source zone to *Trust-L3*.

The screenshot shows the 'Source' tab configuration. The 'SOURCE ZONE' dropdown is set to 'Trust-L3'. At the bottom of the list, there is an 'Add' button highlighted by a red arrow.

Go to the *Destination* tab and set the destination zone to *Untrust-L3*.

The screenshot shows the 'Destination' tab configuration. The 'DESTINATION ZONE' dropdown is set to 'Untrust-L3'. At the bottom of the list, there is an 'Add' button highlighted by a red arrow.

Go to the *Actions* tab and set the *Action Setting* to *Allow*.

The screenshot shows a navigation bar with tabs: General, Source, Destination, Application, Service/URL Category, and Actions. The Actions tab is selected and highlighted with a red underline. Below the tabs, there is a section titled "Action Setting". It contains a dropdown menu labeled "Action" with the option "Allow" selected. There is also a checkbox labeled "Send ICMP Unreachable".

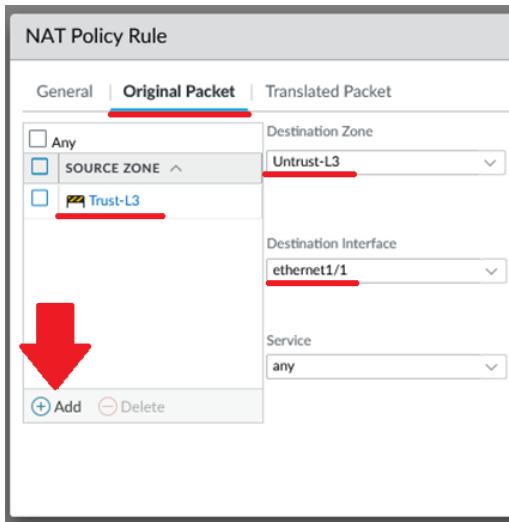
Next, go to the *NAT* section of the *Policies* tab and click the *Add* button.

The screenshot shows the Policies tab with the NAT section selected. The table has columns: NAME, TAGS, SOURCE ZONE, DESTINATION ZONE, DESTINATION INTERFACE, and SOURCE ADDRESS. At the bottom left of the table area, there is an "Add" button with a red arrow pointing to it.

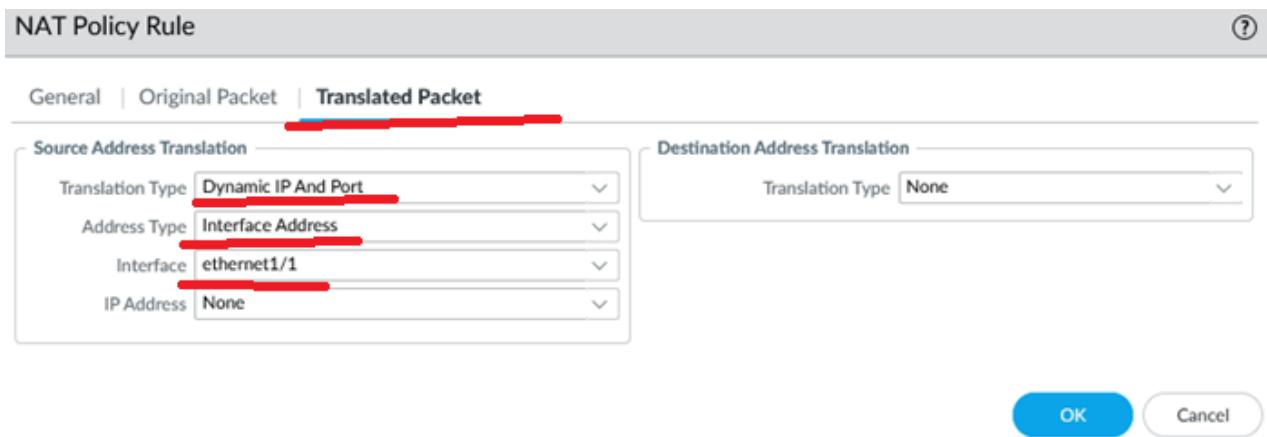
Name it *Internet Outgoing*.

The screenshot shows the "NAT Policy Rule" dialog box with the "General" tab selected. The "Name" field is filled with "Internet Outgoing". Other fields include "Description", "Tags", "Group Rules By Tag" (set to "None"), "NAT Type" (set to "ipv4"), and "Audit Comment". At the bottom right, there are "OK" and "Cancel" buttons.

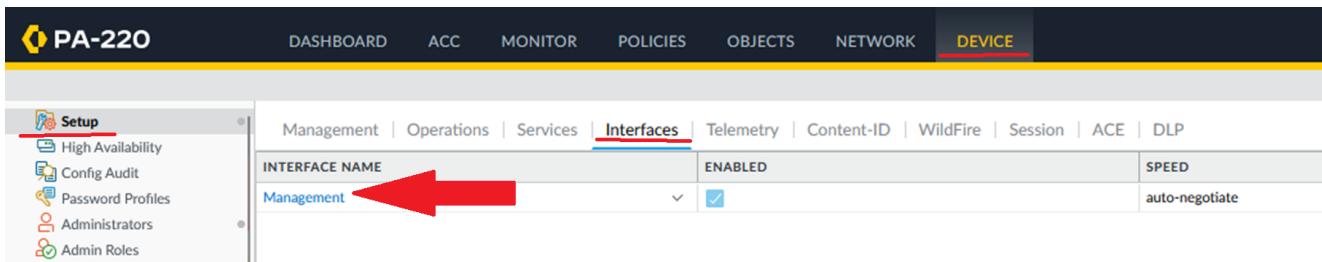
Under *Original Packet*, set the source zone to *Trust-L3*, the destination zone to *Untrust-L3*, and the destination interface to *ethernet1/1*.



Under Translated Packet, the translation type to *Dynamic IP and Port*, the address type to *Interface Address*, and the interface to *ethernet1/1*.



Next, go to Device > Setup > Interfaces and click *Management*.



Set the IP address/netmask to your desired settings (in this case, we used 192.168.1.1 and 255.255.255.0). Set the default gateway to the IP of the VLAN interface (in this case, 192.168.1.254).

Management Interface Settings

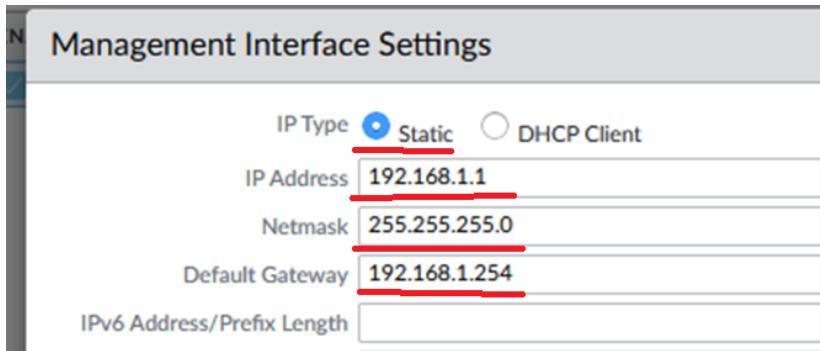
IP Type Static DHCP Client

IP Address **192.168.1.1**

Netmask **255.255.255.0**

Default Gateway **192.168.1.254**

IPv6 Address/Prefix Length



Next, switch to the Services tab, and click the gear next to Services.

Management | Operations | **Services** | Interfaces | Telemetry | Content-ID | Wi-Fi

Services 

Update Server **updates.paloaltonetworks.com**

Verify Update Server Identity

DNS Servers

Primary DNS Server **1.1.1.1**

Secondary DNS Server **1.0.0.1**

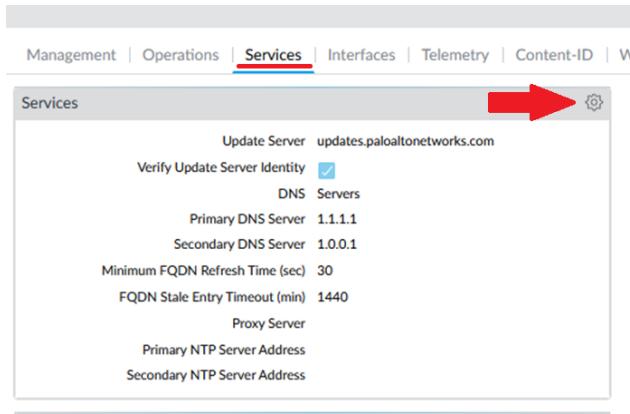
Minimum FQDN Refresh Time (sec) **30**

FQDN Stale Entry Timeout (min) **1440**

Proxy Server

Primary NTP Server Address

Secondary NTP Server Address



Set the update server to *updates.paloaltonetworks.com* and set the DNS servers to your desired DNS service (in this lab, we used Cloudflare's DNS, 1.1.1.1 and 1.0.0.1).

Services | NTP

Update Server **updates.paloaltonetworks.com**

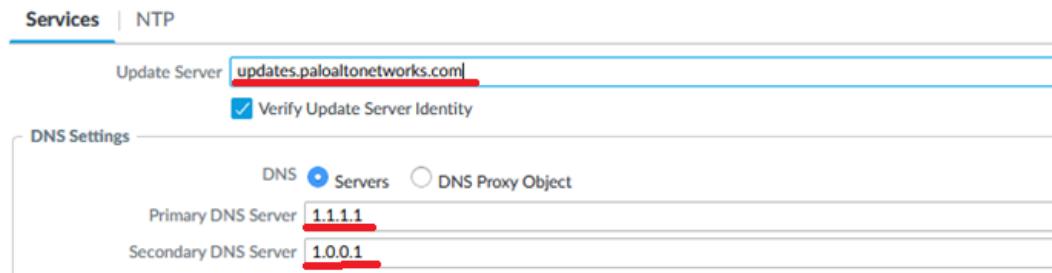
Verify Update Server Identity

DNS Settings

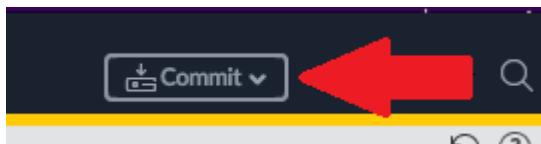
DNS Servers DNS Proxy Object

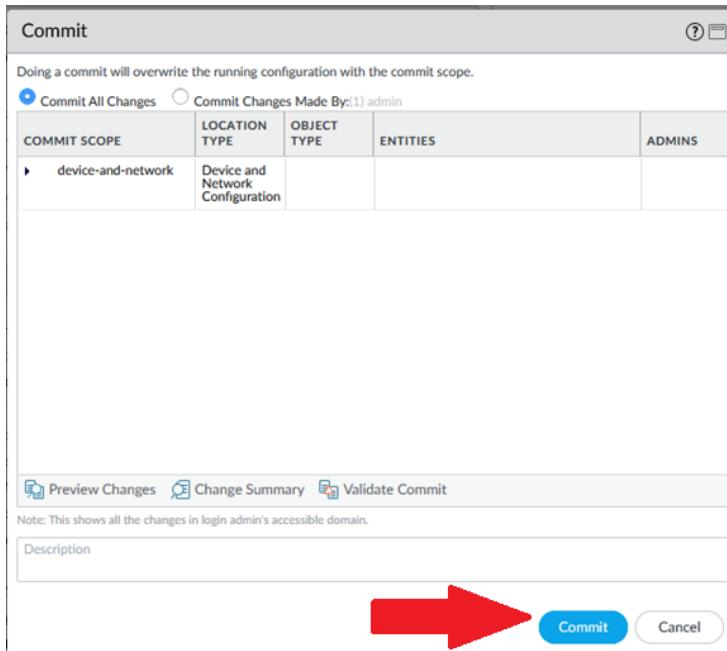
Primary DNS Server **1.1.1.1**

Secondary DNS Server **1.0.0.1**



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





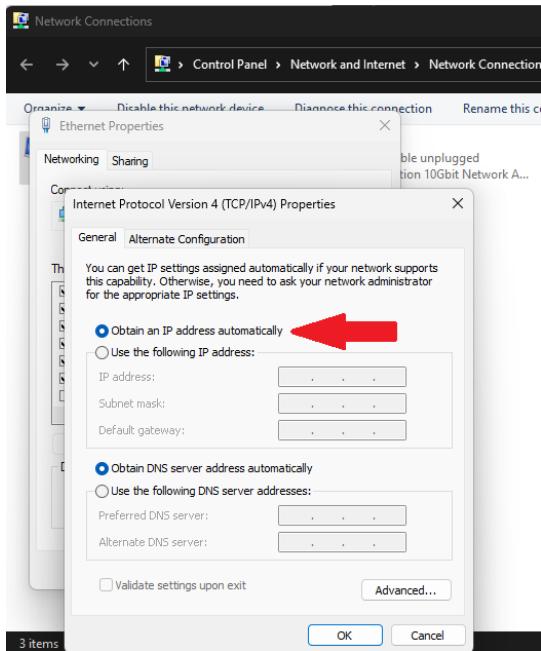
Go to the Dashboard tab.



Look under the *System Logs* section. DHCP to the Internet if you see that an IP has been assigned to the ethernet1/1 interface

Description	Time
User admin logged in via Web from 192.168.1.3 using https	09/19 10:06:29
authenticated for user 'admin'. From: 192.168.1.3.	09/19 10:06:29
Port ethernet1/1: Down 100Mb/s-full duplex	09/19 10:01:49
Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.1	09/19 10:00:35
Reconnect to MLAV cloud, enable all machine Learning engines	09/19 10:00:34
DHCP client assigned IP: 192.168.40.20 on interface: ethernet1/1 for lease time of: 7 days 0h:00m:00s from server: 192.168.40.1 Subnet mask:255.255.254.0 Gateway:192.168.40.1 DNS1:9.9.9.9 DNS2:1.1.1.1	09/19 10:00:32
Port ethernet1/1: MAC Up	09/19 10:00:22
Port ethernet1/1: Up 100Mb/s-full duplex	09/19 10:00:22
Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.1	09/19 09:46:13
Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.1.1	09/19 09:30:39

Connect PC1 and PC2 to the ethernet1/2 and ethernet1/3 ports of the firewall. Connect the MGT port of the firewall to any unused port from ethernet1/4-1/8 (in our lab, we used port ethernet1/7). Set both PCs to obtain an IP address automatically.



On either PC, open the command prompt and type *ipconfig*.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Colin>ipconfig
```

If you see an address in your DHCP address pool, DHCP is working correctly.

```
Ethernet adapter Ethernet:

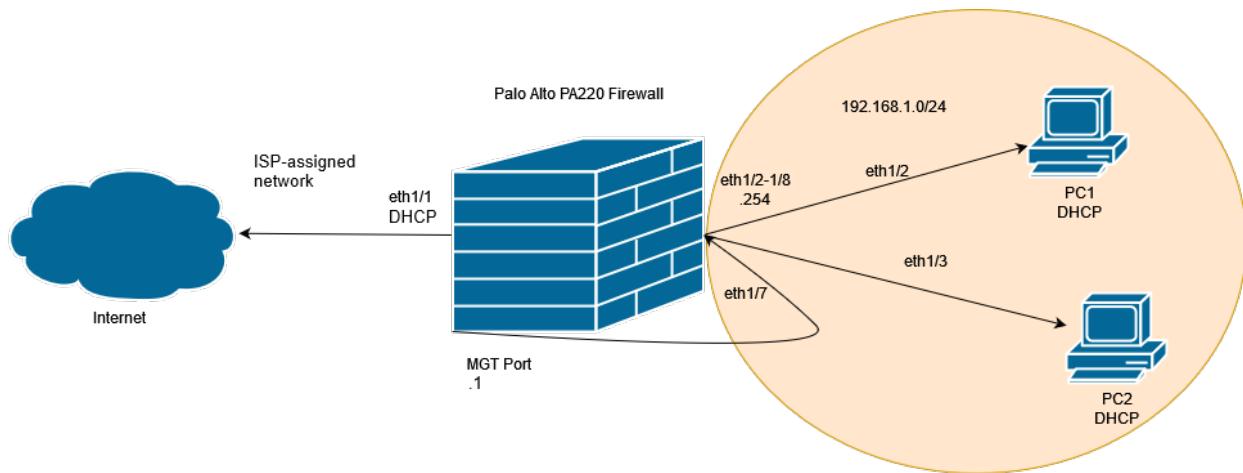
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d12c:67e4:d5e7:b56b%17
IPv4 Address. . . . . : 192.168.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
```

Next, from the command prompt, ping a website on the internet (such as www.google.com). If you get a reply, internet connectivity is working correctly.

```
C:\Users\Colin>ping www.google.com

Pinging www.google.com [142.250.69.196] with 32 bytes of data:
Reply from 142.250.69.196: bytes=32 time=14ms TTL=112
Reply from 142.250.69.196: bytes=32 time=13ms TTL=112
Reply from 142.250.69.196: bytes=32 time=17ms TTL=112
Reply from 142.250.69.196: bytes=32 time=12ms TTL=112
```

Network Diagram



Problems

Virtual Wire

By default, ethernet1/1 and ethernet1/2 are connected by a virtual wire, which causes the ports to act as a direct connection to each other and lose their ability to route and switch traffic. Originally, we ran into an error with our commit, as while the interfaces had been changed to Layer 3 and Layer 2 respectively, the firewall still had an unbound virtual wire.

This error was fixed by going to the *Virtual Wires* section of the *Network* tab, selecting *default-vwire*, and clicking *Delete*, as shown in the Lab Commands section above.

Conclusion

The PA220's web interface was confusing to navigate at first, but after configuring the firewall for a SOHO network, I believe I have gained a strong understanding of how to navigate PAN-OS's interface. All in all, a SOHO network configuration using a PA220 firewall had a relatively simple setup process and would work great for an individual or small business.

Signoff



Setting up a PA220 Firewall for a SOHO Environment

Colin Faletto

P5 Cybersecurity

Mr. Mason

