Cyber Security SOHO Lab

Purpose:

The purpose of this lab is to show our understanding of how to set up SOHO and to see if we can set it up successfully. It is also a way for us to learn and explore Palo Alto’s GUI and see the different ways to use it. We are also capturing every step of the process troubleshooting when there are problems that come up.

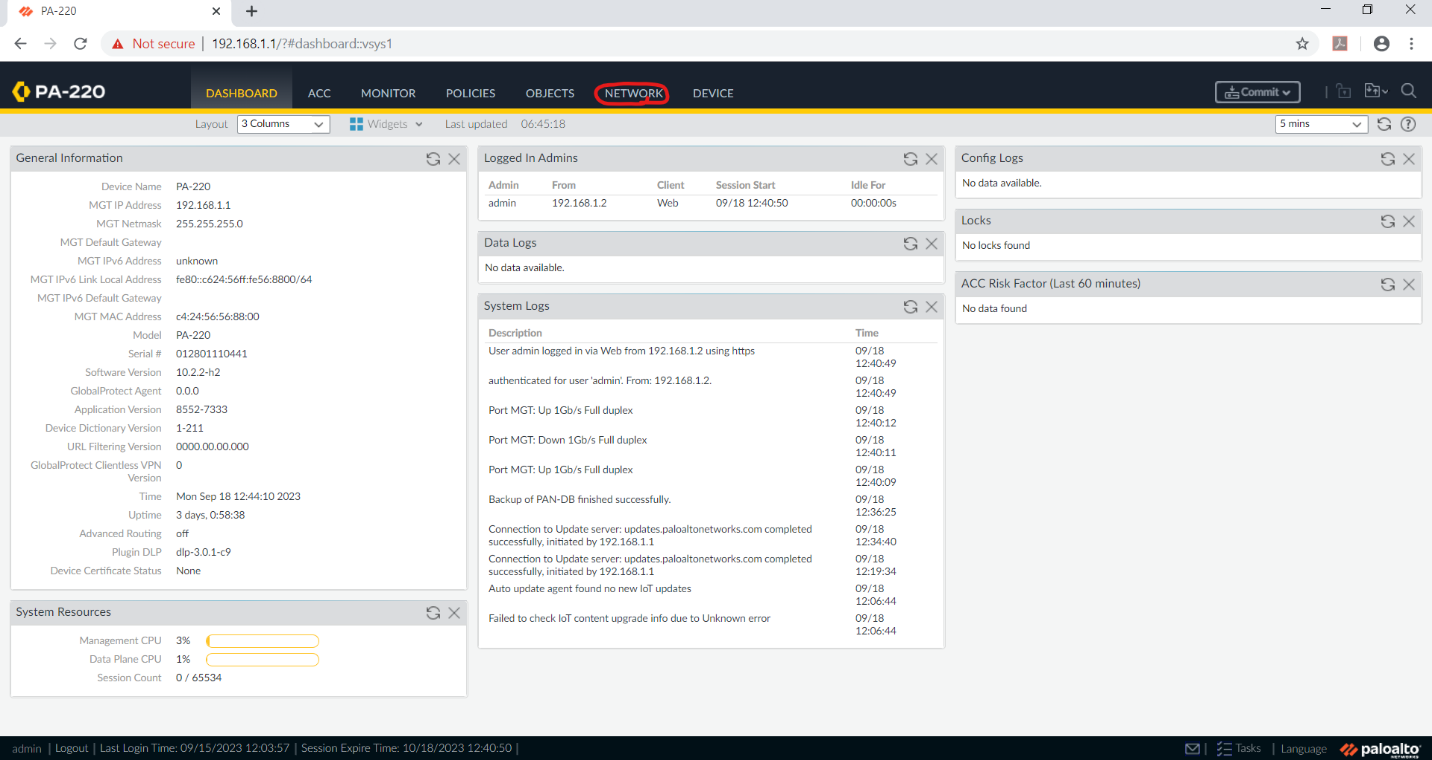
Background:

SOHO, stands for single office/home office, it is a network configuration designed for home networks or smaller companies. A SOHO firewall should be for a network with 25 computers or less. The main purpose of a SOHO firewall is to protect a smaller network in a home office or a small office for work. Having a SOHO firewall for your house or company is crucial because it protects your network from cybersecurity attacks like viruses and malware. It is easier to set up than an actual firewall system still providing the same features and the same protection.

Lab Summary:

In this lab, we are going to set up a soho topology with a router, a firewall in between and the internet. First, we will have to set all the security zones on the firewall and then the ethernet ports. Then we must add a new vlan and assign that to a port. We will have to set up a DHCP server with our firewall and set the policies allowing certain zones to let certain things through. The next step we have to set up NAT on a port and send that NATed packet to the right destination. The last step we have to set a management interface Ip and also set the DNS server for the management interface.

Step 1



Click on network

Step 2

A screenshot of a computer

Description automatically generated

Click on Zones

Step 3

A screenshot of a computer

Description automatically generated

Click on Add

Step 4

A screenshot of a computer

Description automatically generated

Name this Zone Untrust-L3

Set the type to Layer 3

Step 5

A screenshot of a computer

Description automatically generated

Add another zone

Set the name to Trust-L2

Set the type to layer 3

Step 6

A screenshot of a computer

Description automatically generatedAdd another zone

Name it trust-L2

Set the type as Layer 2

Step 7

A screenshot of a computer

Description automatically generatedGo to interfacw

Step 8

A screenshot of a computer

Description automatically generatedClick on interface1/1

Step 9

A screenshot of a computer

Description automatically generated

Set the interface type to Layer 3

Set the security zone to Untrust-L3

Set the virtual router to default

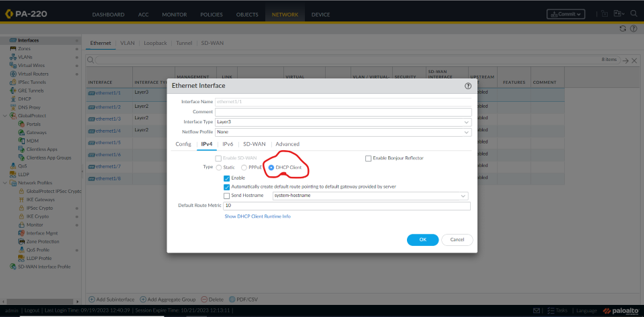
Step 10

A screenshot of a computer

Description automatically generated

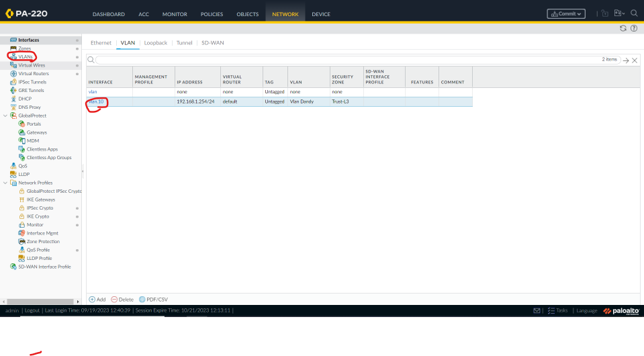
Click on the IPv4 tab

Step 11



Select DHCP Client

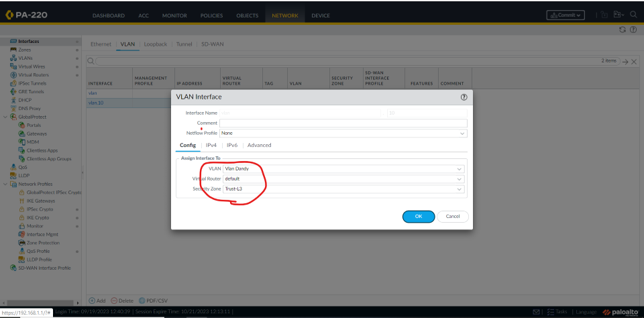
Step 12



Click on Vlans

Click on add

Step 13

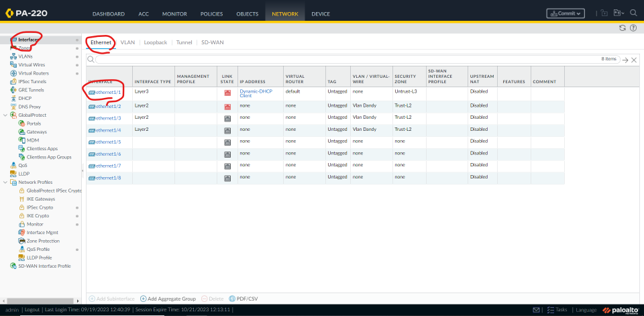


Set name

Set virtual router to default

Set Security zone to Trust-L2

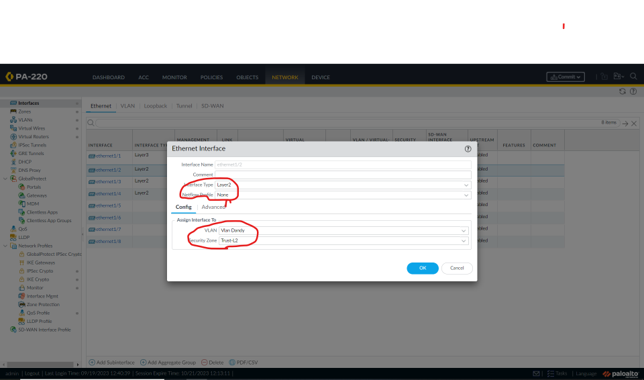
Step 14



Click on interfaces then ethernet

Click on ethernet 1 / 2

Step 15



Set the following

Interface Type: Layer2

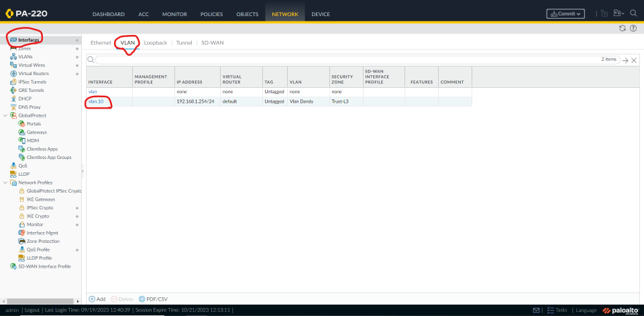
Netflow Profile: None

VLAN: VLAN Object

Security Zone: Trust-L2

Repeat for ethernet 1 / 3 and 1 / 4

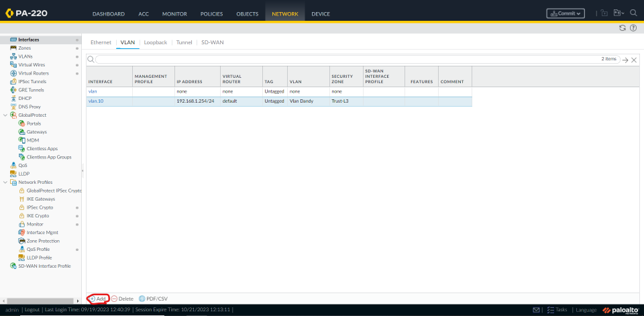
Step 16



Click on interfaces

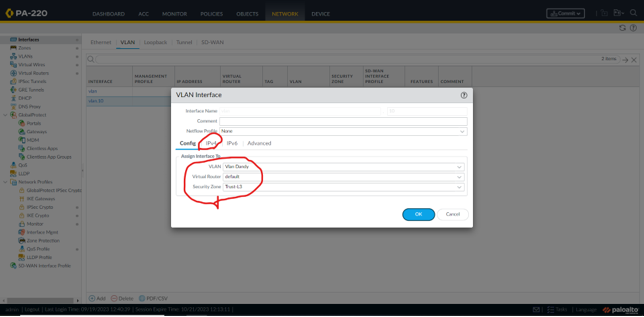
Click on VLAN

Step 17



Click on Add

Step 18

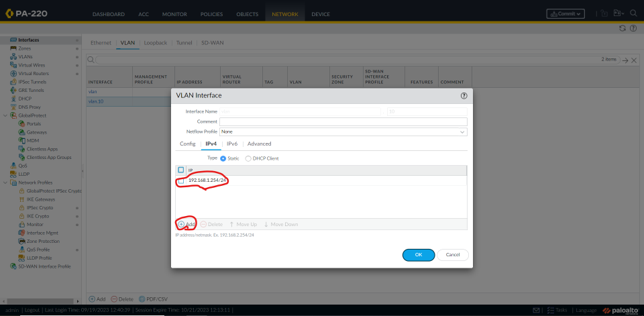


Set the vlan

Set the Virtual router do default

Set the security zone to Trust-L3

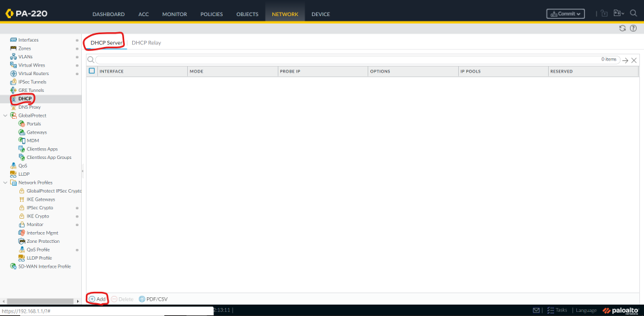
Step 19



Click on the IPv4 tab

Add an ip address

Step 20



Add a new DHCP server

Step 21

A computer screen with a red marker on it

Description automatically generated



Set the interface to vlan.10, the timeout to 1 hour, and add an IP pool from 192.168.1.2-1.252

Step 22

A computer screen with a red marker on it

Description automatically generated



Set the inheritance source, gateway, and subnet mask. Set everything but DNS suffix to inherited.

Step 23

A screenshot of a computer

Description automatically generated

Go to objects.

Step 24A screenshot of a computer

Description automatically generated

Go to Security Profiles

Step 25

A screenshot of a computer

Description automatically generated

Add a profile group called “Internet”, and set the options as listed above.

Step 26A screenshot of a computer

Description automatically generated

Go to policies, then security, then add a new security policy rule.

Step 27

A screenshot of a computer

Description automatically generated

Name it Internet Outgoing, and set the rule type to universal.

Step 28

A screenshot of a computer

Description automatically generated

Go to source, add a new source zone, and set it to Trust-L3.

Step 29

A screenshot of a computer

Description automatically generated

Click on destination

Add a destination zone

Set the zone to Untrust-L3

Step 30

A screenshot of a computer

Description automatically generated

Press actions

Set profile type to group

Set group profile to internet

Step 31

A screenshot of a computer

Description automatically generated

Go to policies

Go to NAT

Press Add

Step 32

A screenshot of a computer

Description automatically generated

Set the name to internet outgoing

Set the NAT type to ipv4

Step 33

A screenshot of a computer

Description automatically generated

Go to original packet

Add zone as trust-L3

Set destination zone to Untrust-L3

Set destination interface to ethernet1/1

Step 34

A screenshot of a computer

Description automatically generated

Go to translated packet

Set translation type

Set address type

Set interface

Step 35

A screenshot of a computer

Description automatically generated

Press setup

press device

press management

Step 36

A screenshot of a computer

Description automatically generated

Set the ip address.

Set the netmask.

Set the default gateway.

Step 37

A screenshot of a computer

Description automatically generated

Set the primary DNS server to 8.8.8.8

Set the secondary DNS server to 8.8.4.4

Step 38

A screenshot of a computer

Description automatically generated

Press commit and commit all changes

A paper with a logo

Description automatically generated