**Palo Alto soho configuration**

Derek Liu Cybersecurity Period 5

Lab #2

**Palo Alto SOHO Config***Derek Liu*

Purpose

The purpose of this lab was to use the web interface to configure the Palo Alto firewall for a SOHO setting and connect it to the internet. This was done through configuring DHCP and using NAT.

Background Information

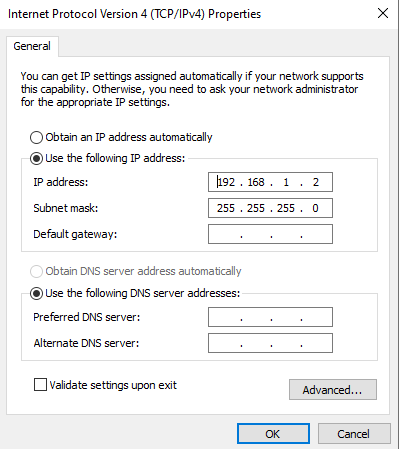
After factory resetting a Palo Alto firewall, it will not be initially configured to be completely functional for a SOHO setting. In this lab we will make the necessary changes in the web interface for it to function. In this lab we configured ethernet 1/1 to be the interface to be connected to the ISP while interfaces 1/2 to 1/4 were configured to be trusted interfaces. We did not set any static routes and used DHCP to obtain IP addresses. VLANs and NAT were also configured in this lab.

After successful configuration of the Palo Alto for a SOHO network, you can access service through the Palo Alto. For example, if your network comes under attack, you can contact Unit 42 through the Palo Alto website for them to contain and remediate the breach. Unit 42 is made up of the industry’s elite incident response advisors.

Palo Alto firewalls are at the forefront of leaders in network firewalls and positioned highest in execution and furthest in vision by Gartner. A firewall comes with features for a zero trust enterprise, cloud native security, security operations, threat intel & consulting, ML-powered network security, and cloud delivered security.

Configurations

1. Connect to the management interface and change pc ipv4 address to 192.168.1.2 in order to access the web interface



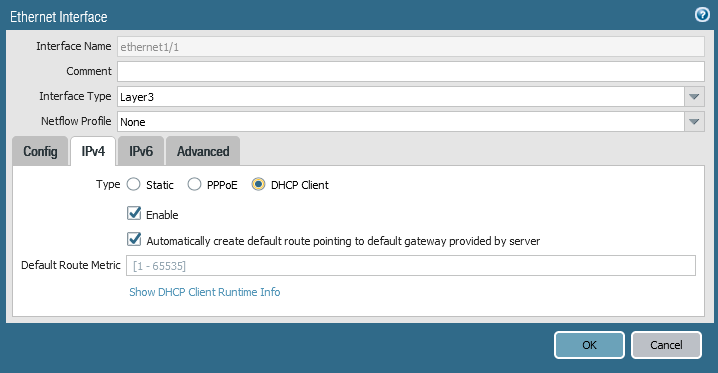
Go to <https://192.168.1.1> Default credentials should be username: admin, password: admin.

1. Go to network -> zones and then click “add” on the bottom left.

Create three different zones:

* Untrust, Type Layer 3.
* Trust-L3, Type Layer 3.
* Trust-L2, Type Layer 2

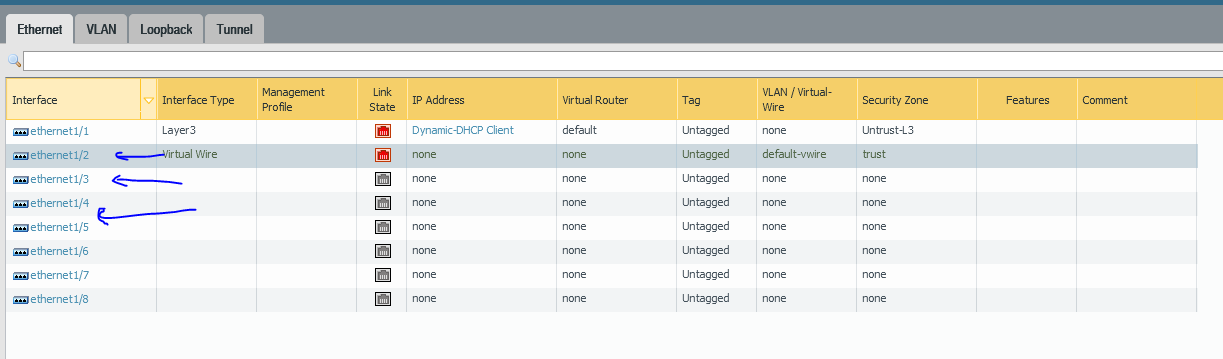
1. Connect ethernet 1/1 to the ISP.
2. Go to Network -> interfaces and select “ethernet 1/1”

  
Change interface type to layer 2, set virtual router to default, and set as DHCP client

1. Go to Virtual Wire and delete everything on the page
2. Go to Network -> VLANs and click “add”

Set the name as “Vlan Object” and VLAN interface as “vlan”.

1. Go to Network -> interfaces and configure the following interfaces:

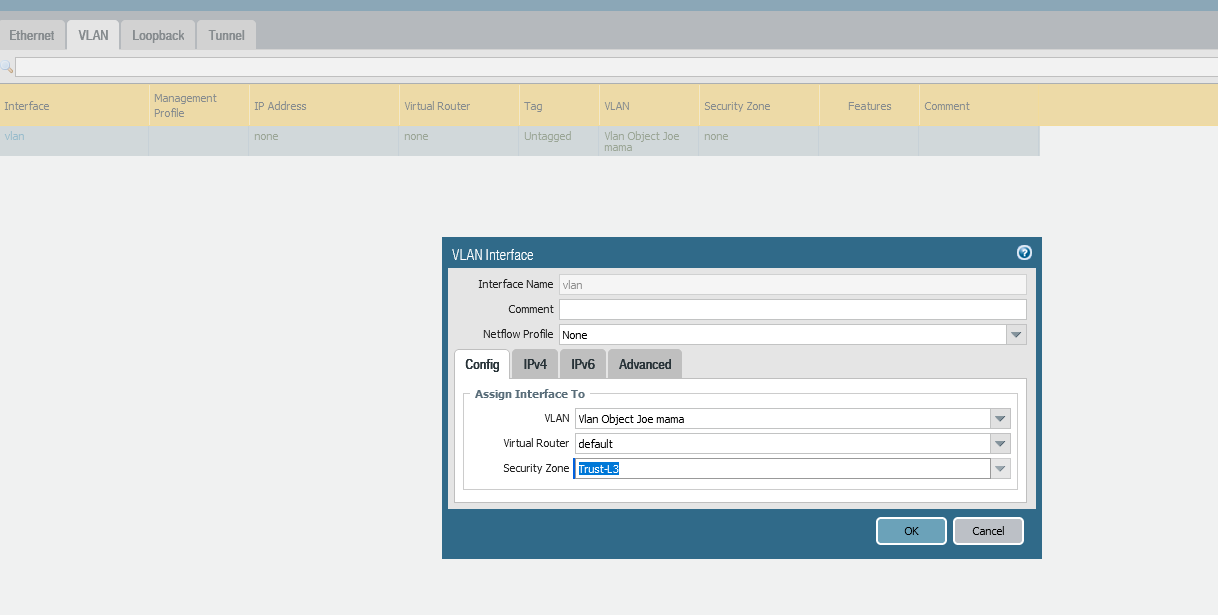


For all of them (1/2, 1/3, 1/4) Select the following:

* Interface type: Layer2
* VLAN: Vlan Object
* Security Zone: Trust-L2

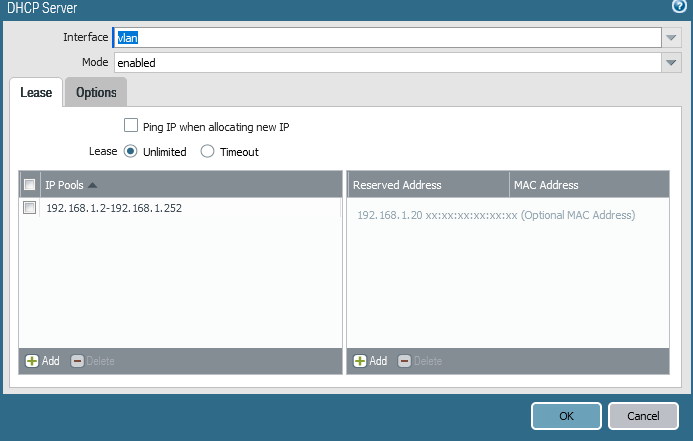
1. Go to Network -> interfaces -> VLAN and edit the following:

* VLAN: Vlan Object
* Virtual Router: Default
* Security Zone: Trust-L3

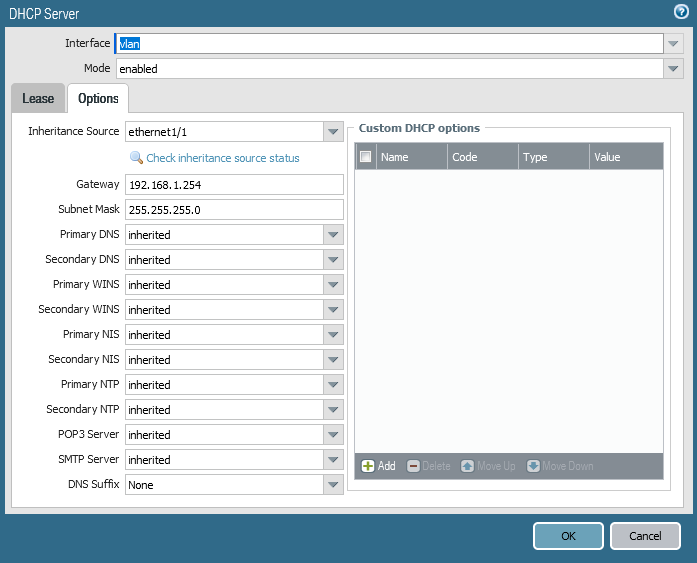


1. Go to the IPV4 tab and select DHCP Client (or set a static IP address if step 10 doesn’t work)
2. Go to Network -> DHCP -> DHCP Server and click “add”

And put in the following configuration:

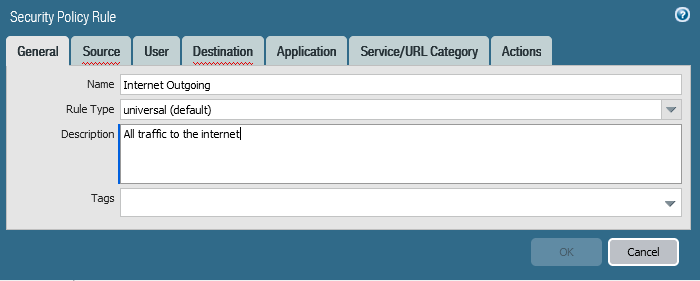


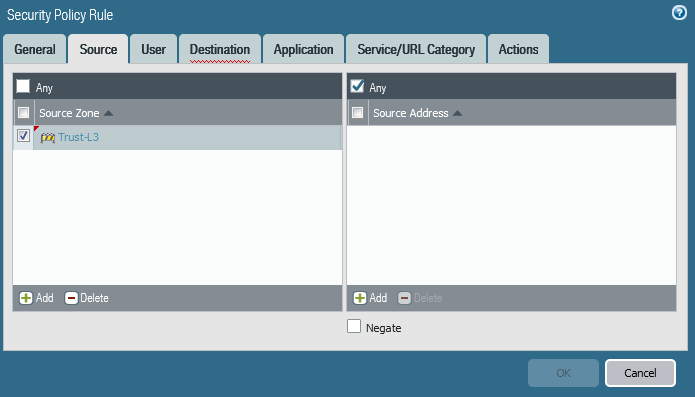
Go to options and configure the following:

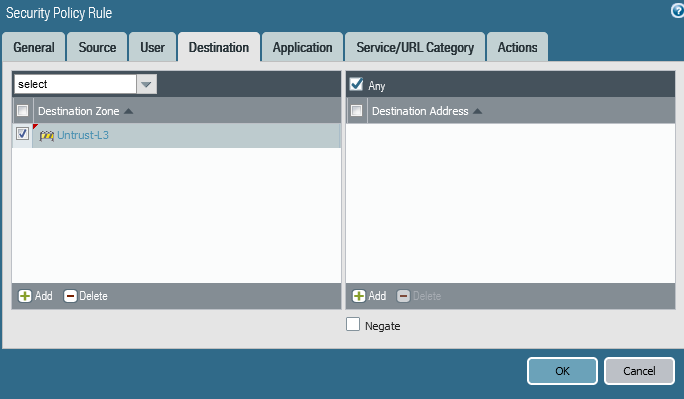


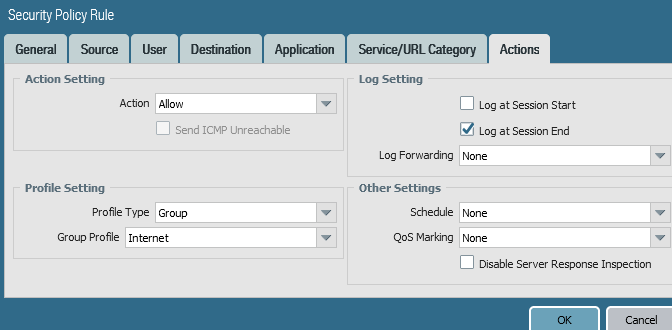
1. Objects -> Security Profile Groups and click “add”
2. Name: “Internet”; Antivirus profile: “default”; Anti-spyware profile: “strict”; Vulnerability protection profile: “strict”; URL filtering profile: “default”.
3. Policies -> security and click “add”

Configure the following:



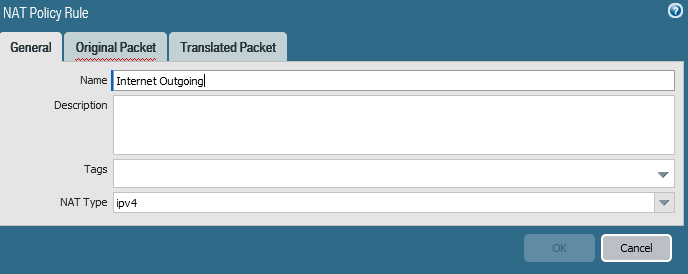


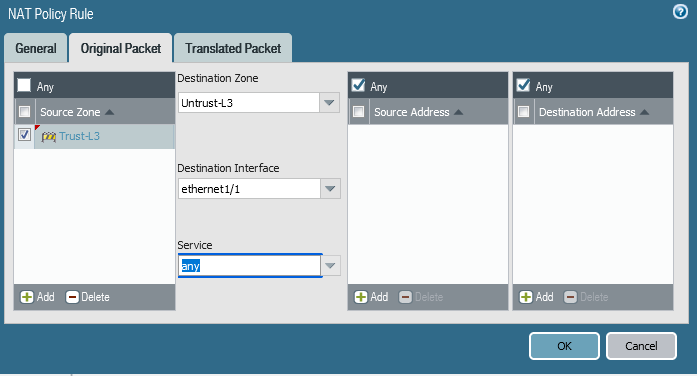


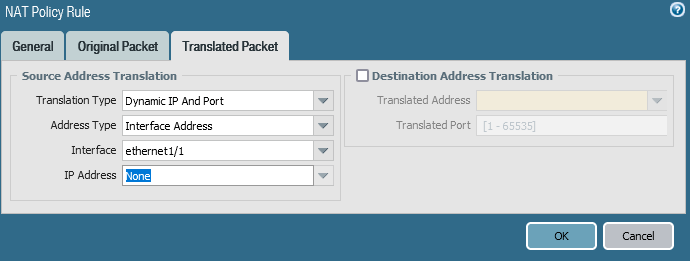


1. Go to Policies -> NAT, and click “add”

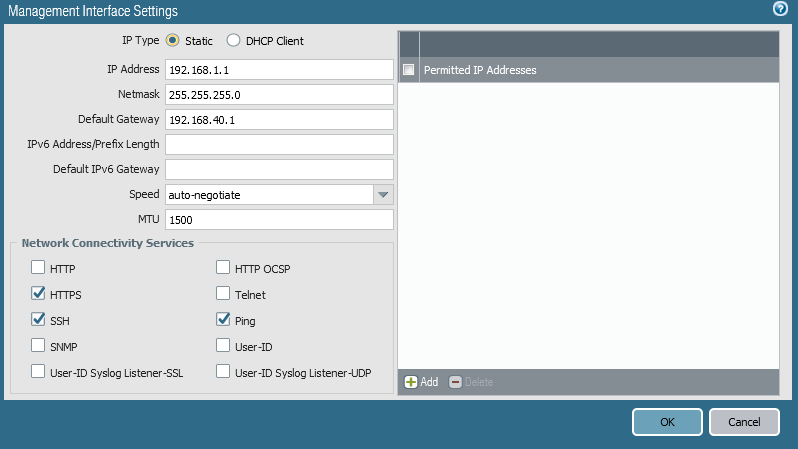
Configure the following:





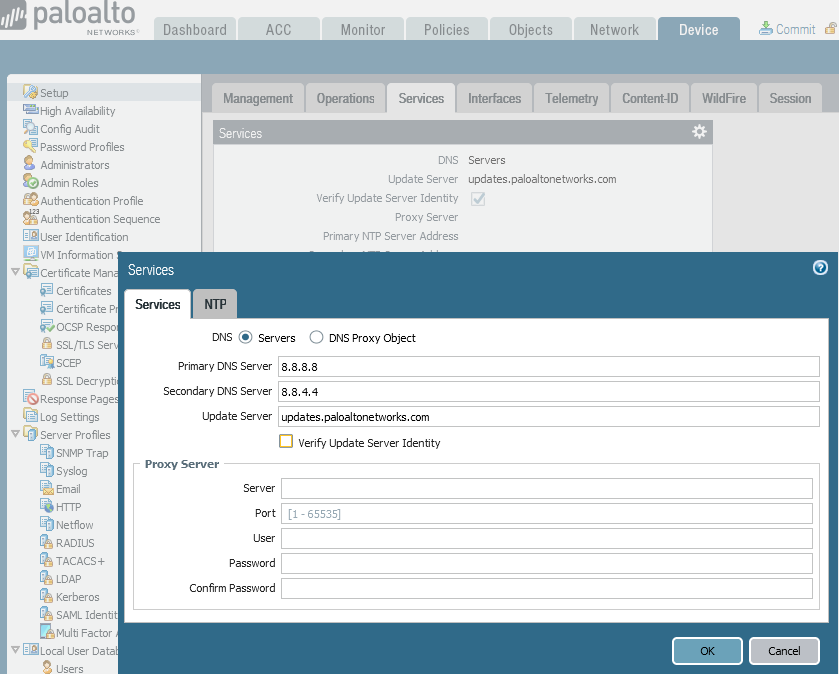


1. Go to Device -> Setup -> Interfaces



1. Go to Device -> Setup -> Services

Configure the following:



1. Click the commit button at the top right of the web interface to save configurations.
2. Change ipv4 configuration of PC to DHCP

Problems

The lab had a lot of steps that weren’t very specific so the first time we tried to configure the firewall it didn’t go smoothly. We originally configured static routes which didn’t work very well so we switched to DHCP and there was a lot of confusion following which steps were meant for static routes and which ones were meant for DHCP. Another problem that we had was that we were getting warnings while committing with the virtual wire. We fixed it by deleting the virtual wire. Another problem that we had was finding a suitable DHCP pool. We originally chose a DHCP pool in the range of 192.168.40.1 to 192.168.40.252 but that ended up cutting off the connection to the web interface. The fix was using the DHCP pool of 192.168.1.1-192.168.1.252. Another problem that we ran into was that we often forgot to change the ipv4 address of the pc to DHCP which caused the connection to time out while we were trying to connect to the web interface.

Conclusion

In this lab we successfully configured a Palo Alto 220 firewall for a SOHO network. This was done through configurate of the Palo Alto through the web interface after we connected an ethernet cable to the management port. While no software updates were done, the firewall can now successfully connect to the internet and also create a DHCP pool and NAT for the trusted interfaces.