SOHO Configuraton Lab

By Jordan Abu-Zahra

**Purpose:**

In this lab we learned how to set up a small office home office configuration on a Palo Alto Firewall Pa 220 from scratch just after resetting it with now background information on how to configure it and we had to get internet with an IP from DHCP.

**Background Information:**

In this lab we set up a SOHO configuration of the Pa 220 firewall after we factory reset it previously in our first lab and we did this by setting up a DHCP server to give us an IP and a Virtual router with Virtual wires to get us out to the internet. Soho means Small Office/Home Office and basically is what most people use at home so they can access the internet through their firewall, and you normally do this after you reset or are setting up a new firewall.

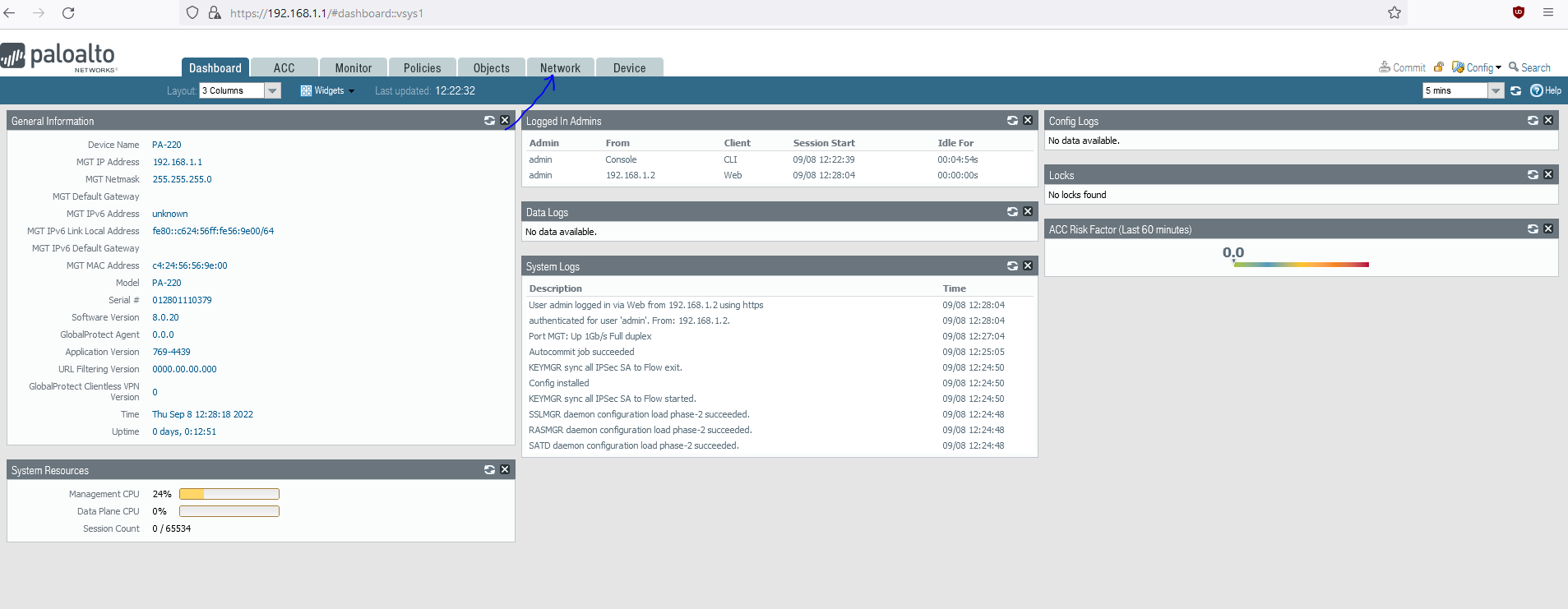
Some of the aspects we used in configuring our palo alto firewall was Nat (Network Address Translation) and why we used NAT was because it hides the IP address of any device on you network giving them all one single Ip address, it requires every incoming packet of information to have been asked for by a device so nothing going into your network that you did not want. Another aspect of the firewall is VLAN’s which allow you to direct traffic like for example if you want to put your workers on one VLAN all the worker traffic would go to VLAN 189 and another VLAN for guest is like VLAN 173, its just a way to separate traffic so you can be secure in where you packet to go and who you want it to go to.

Security zones are also used while configuring the Pa 220 and they are used for controlling outbound and inbound traffic going through the network and if you don’t have this on your firewall it will basically be as protective as a piece of paper since these security layers protect your most critical data but before you configure them you have to decide what type of zone you want, there are 3 types of zones and one of them is a uncontrolled zone which is a public domain, such as the internet and since the internet cannot be controlled by an internal organization this zone is deemed as un-trusted since it can be considered as a major security risk due to the limited controls that can be put into place in this zone, the controlled zone and unlike the uncontrolled zone the controlled zone is a sub-network of an organization’s network, it can be physical or logical. it allows access to an un-trusted zone such as the internet but can’t reach back to the internal network, and its run through an intranet which is a internal network of an organization that is secured behind one or more firewalls with a medium level of restriction with certain controls in place to monitor network traffic. The last zone is called the restricted zone which is highly controlled and must not have any type of un-trusted zones. This zone can have critical level data and systems operating on it. This zone will have the highest level of security features and strict firewall rules in place to control all incoming and outgoing traffic

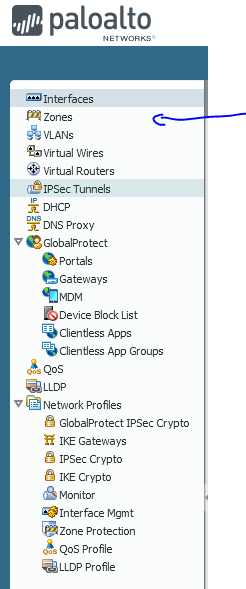
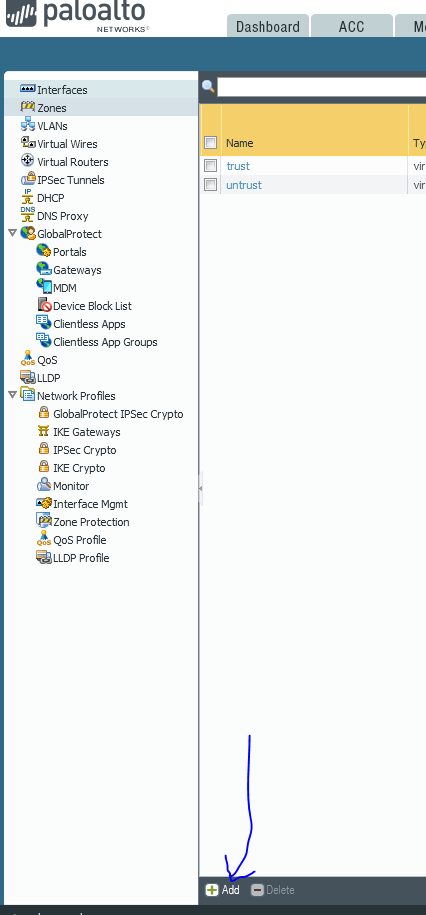
**Steps**

****

#1 go to the ip address of your firewall in your web browser and log in using your username and password (Default admin for both username and password)



#2 go the network tab

  
 #3 go to the zones tab on the left of the screen

#4 click the add button on the bottom left of the screen and configure 3 zones

create 3 zones:

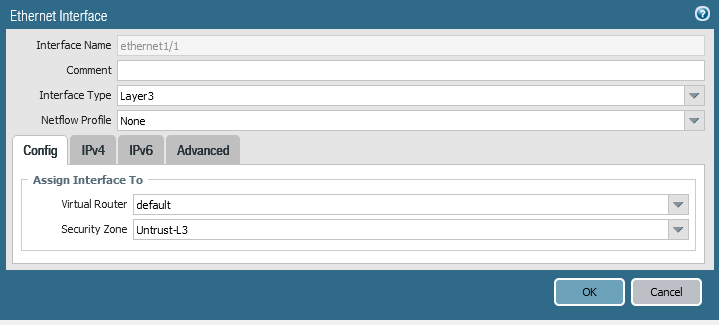
-untrust-L3, type layer 3

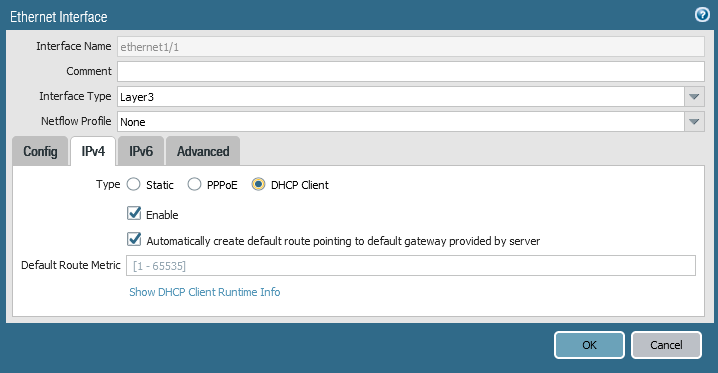
-trust-L3, type layer 3

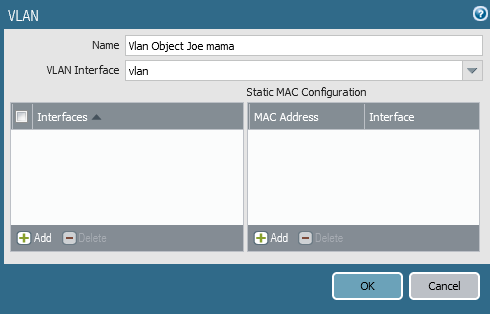
-trust-L2, type layer 2

(See images below)

connect to ISP modem with 1/1 after you are done

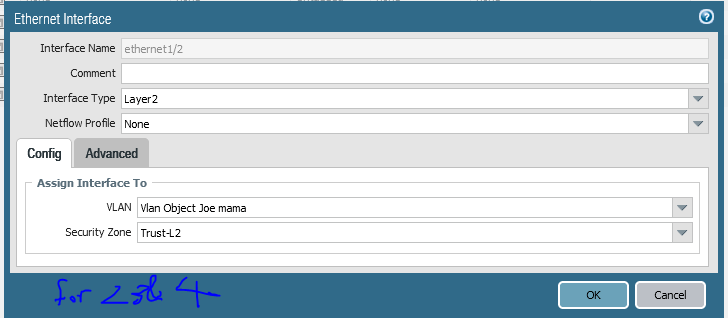


****

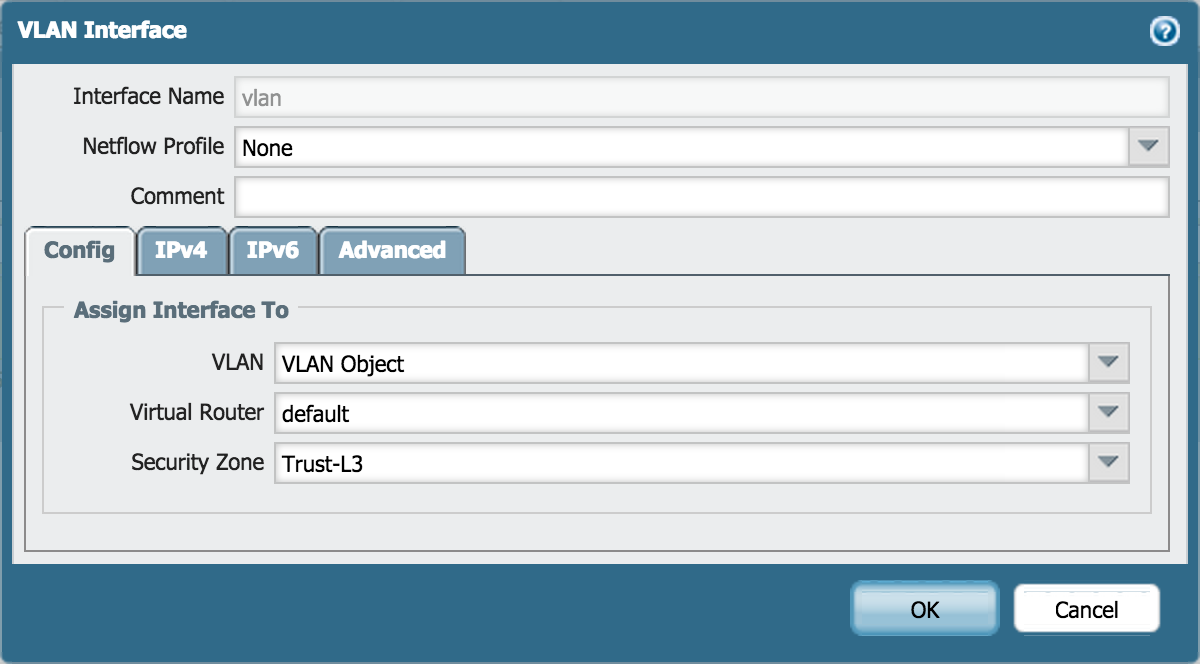


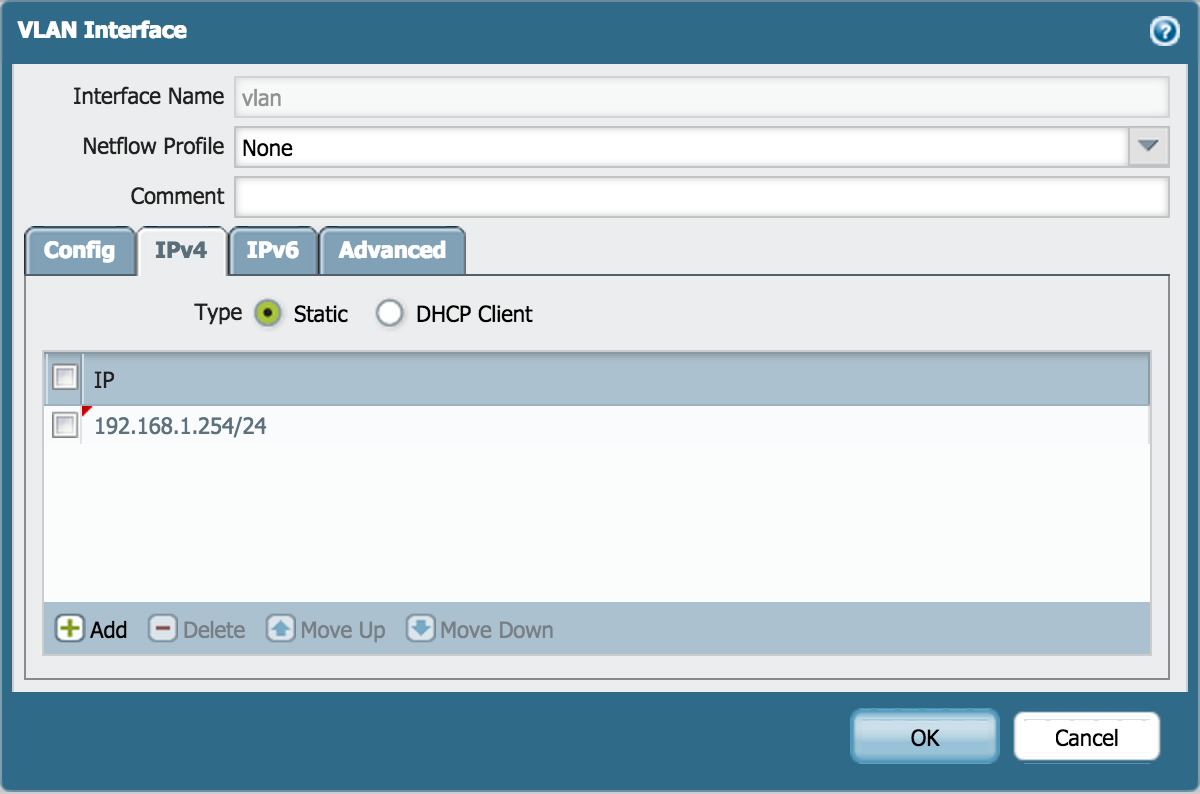
**#5** Go to Network > VLANs and click Add.

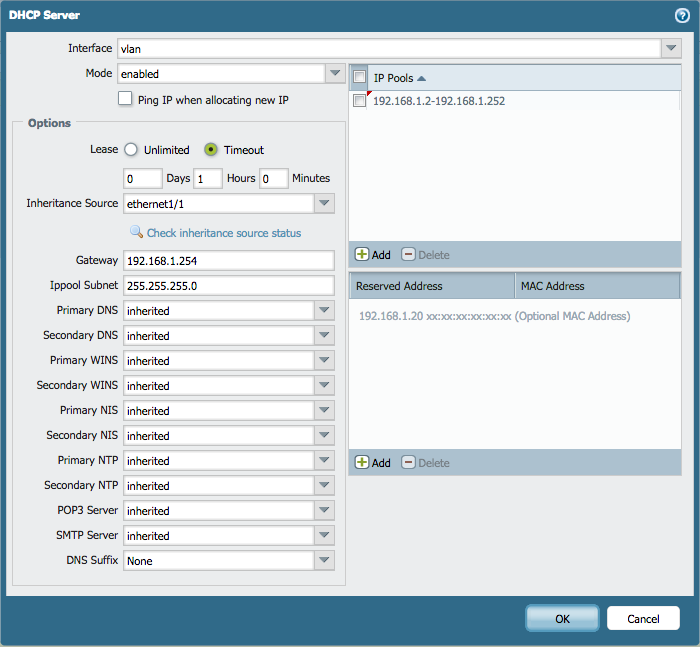
Enter a name and select 'v' for VLAN Interface

#6 Go to Network > Interfaces > Ethernet.

Edit the following settings for the ethernet1/2, ethernet1/3 and ethernet1/4

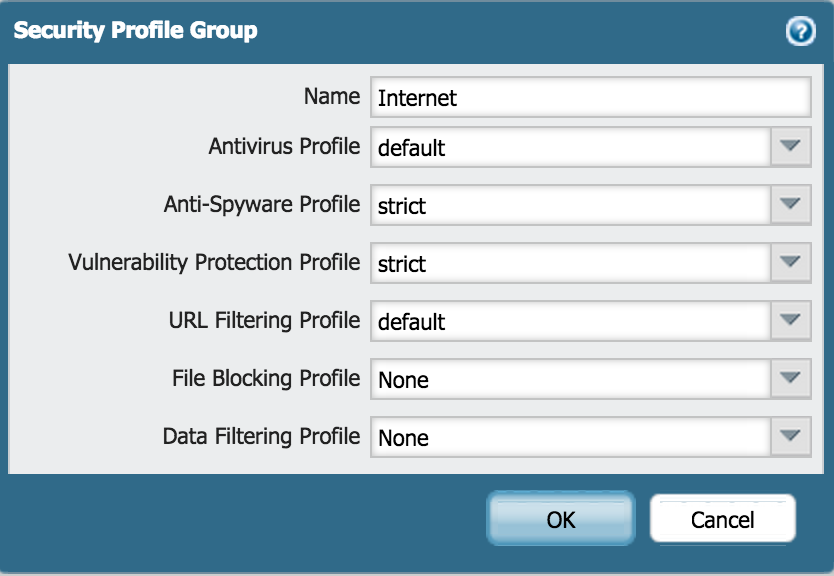


7# Network > Interfaces > VLAN and edit the following setting above

**8#** Go to Network > DHCP > DHCP Server.

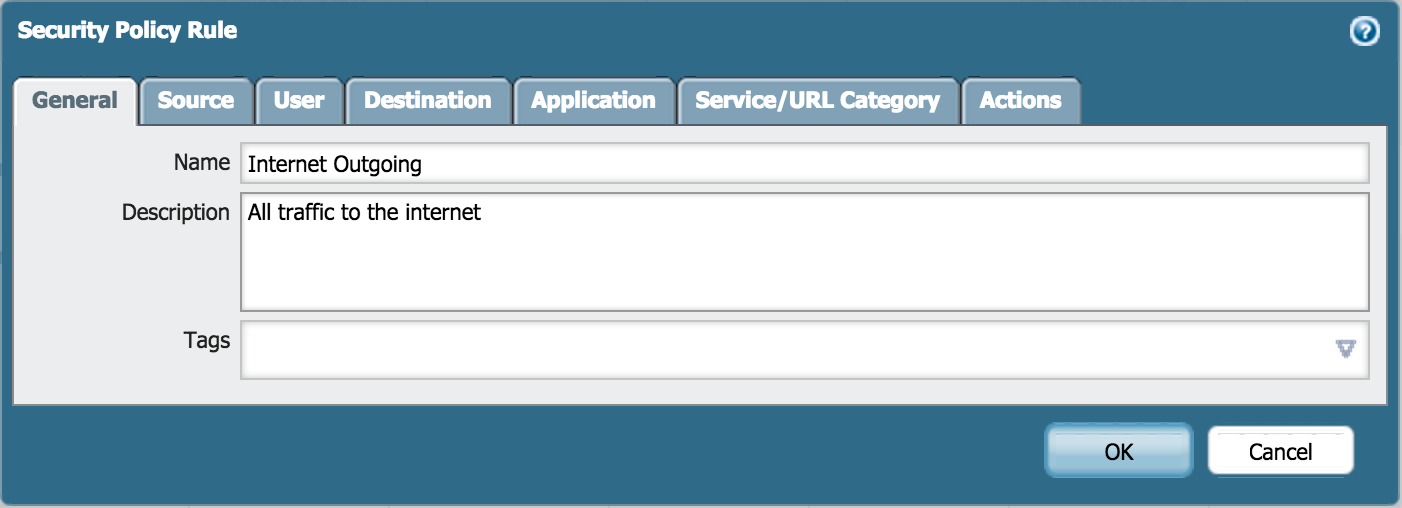
Click Add.

Edit the DHCP Server settings, as shown above



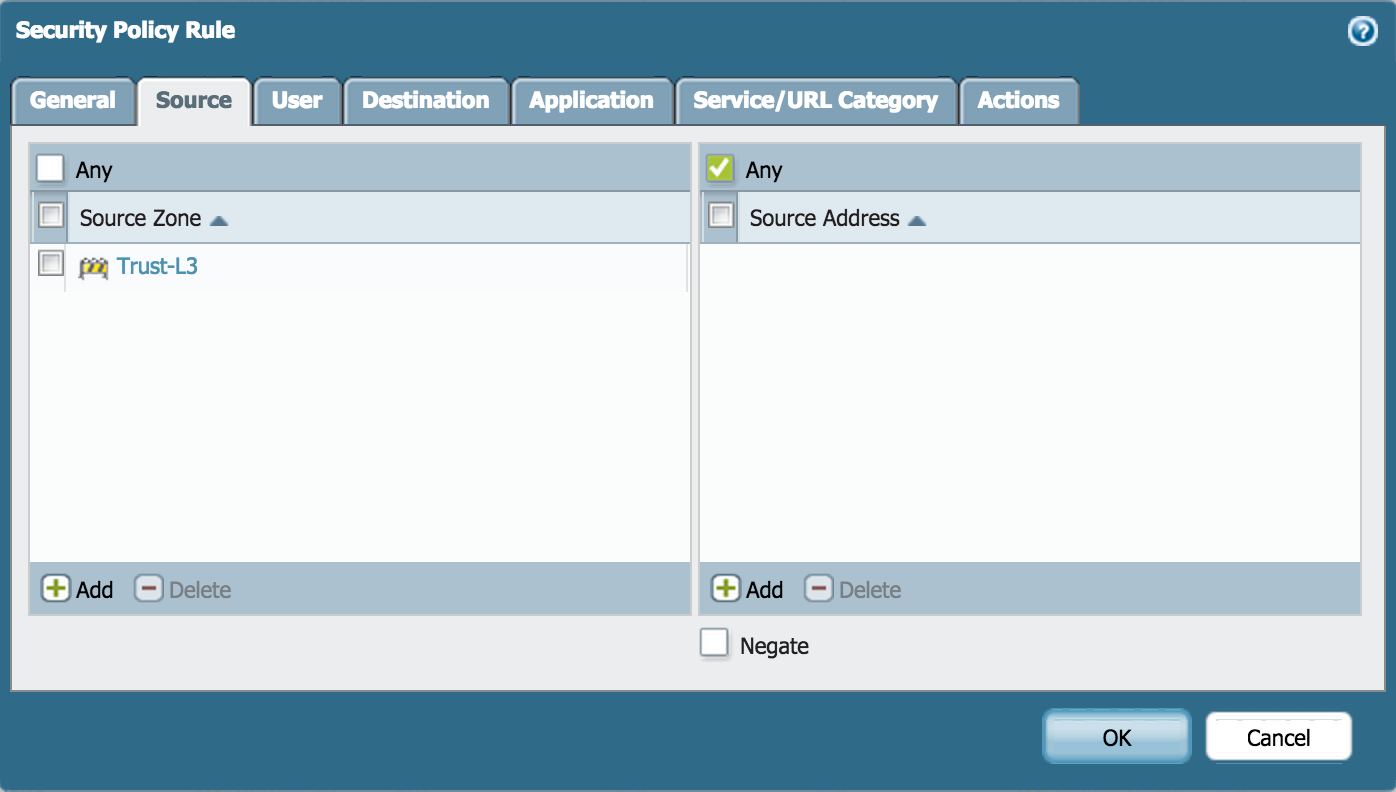
9# Go to Objects > Security Profile Groups and click Add.

Edit the following Security Profile Group settings as desired:

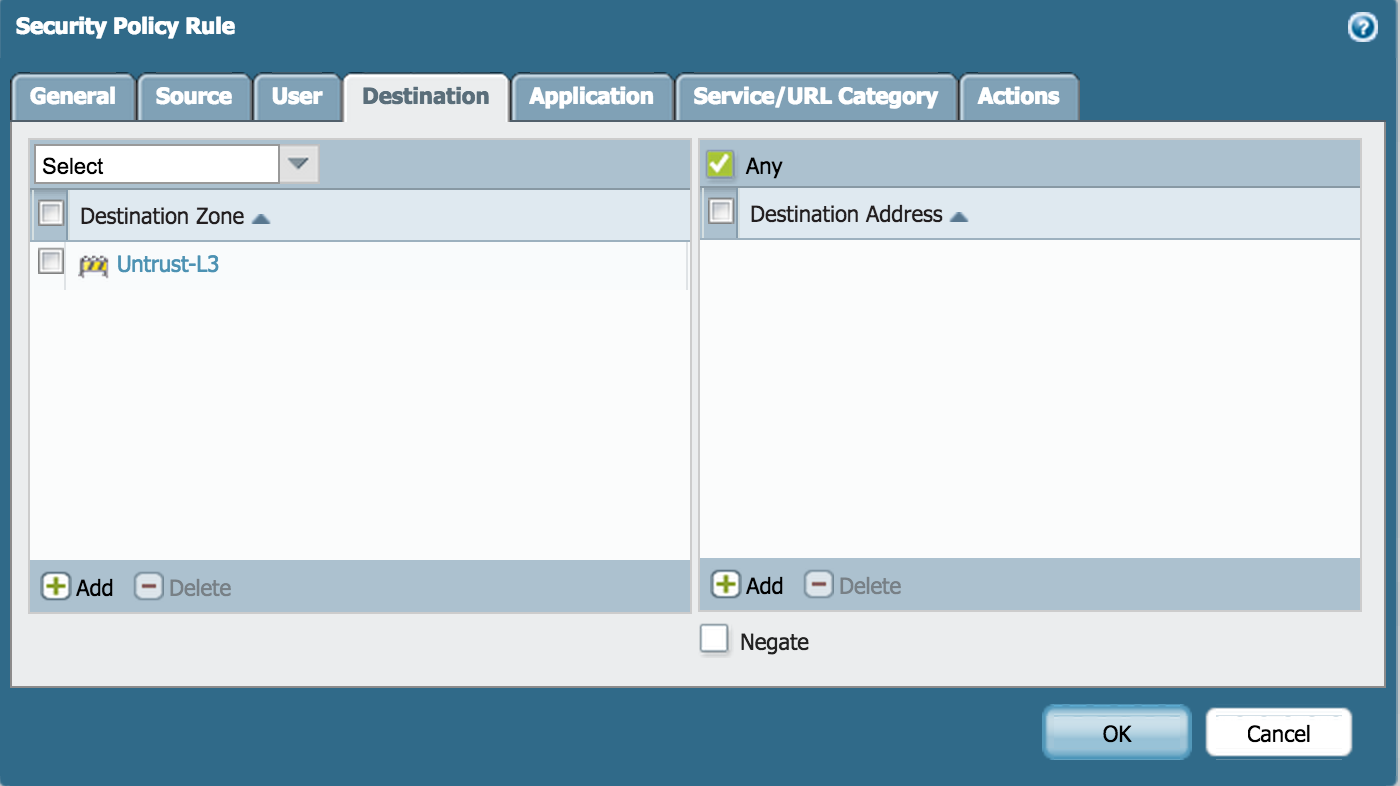


10# Go to Policies > Security and click Add.

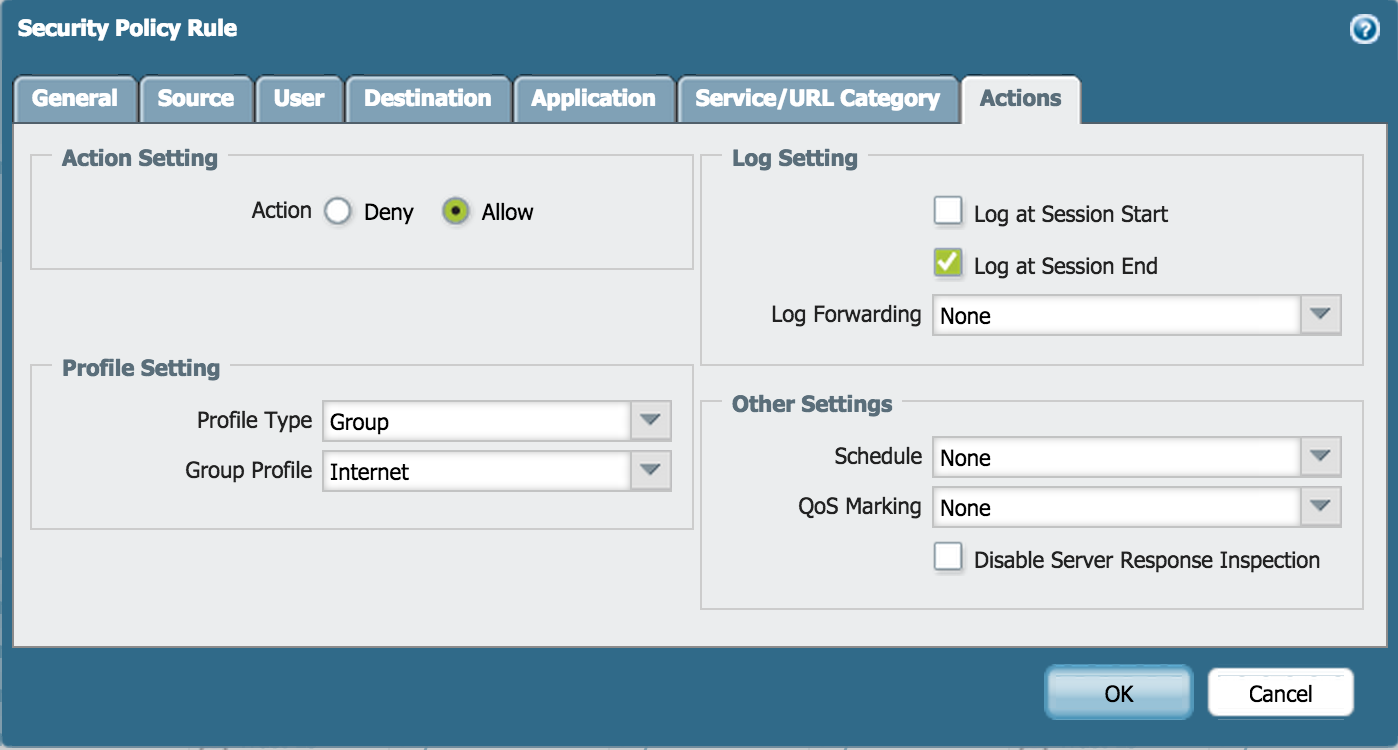
Enter a Name and Description:



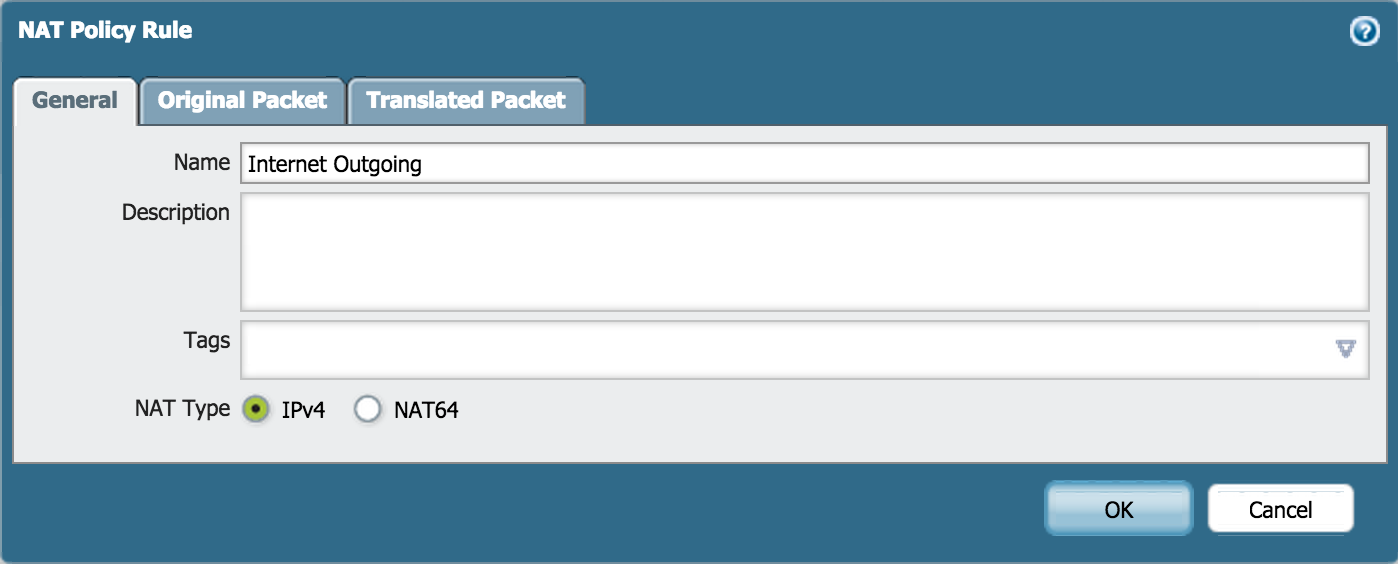
**11# set up the source zone**



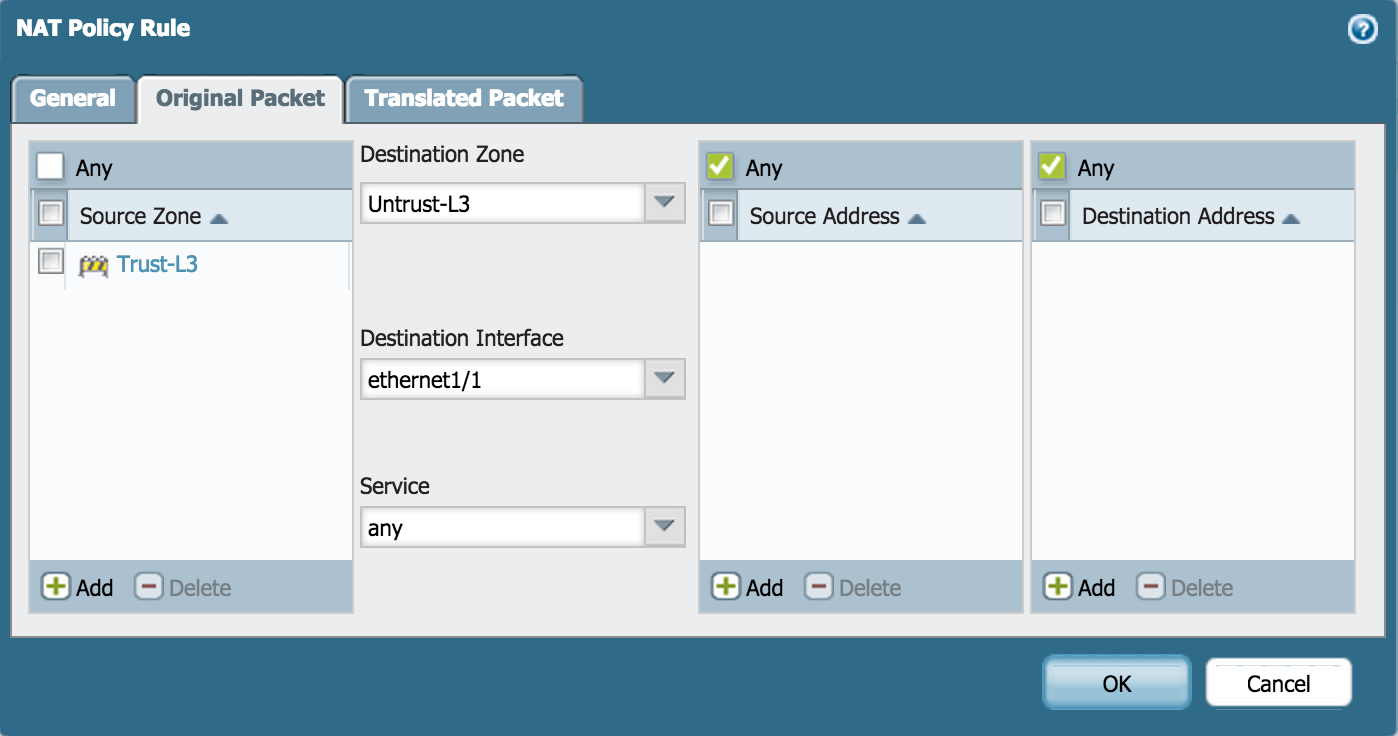
**12# set up the destination zone**



**13# set up the actions tab as the following above**

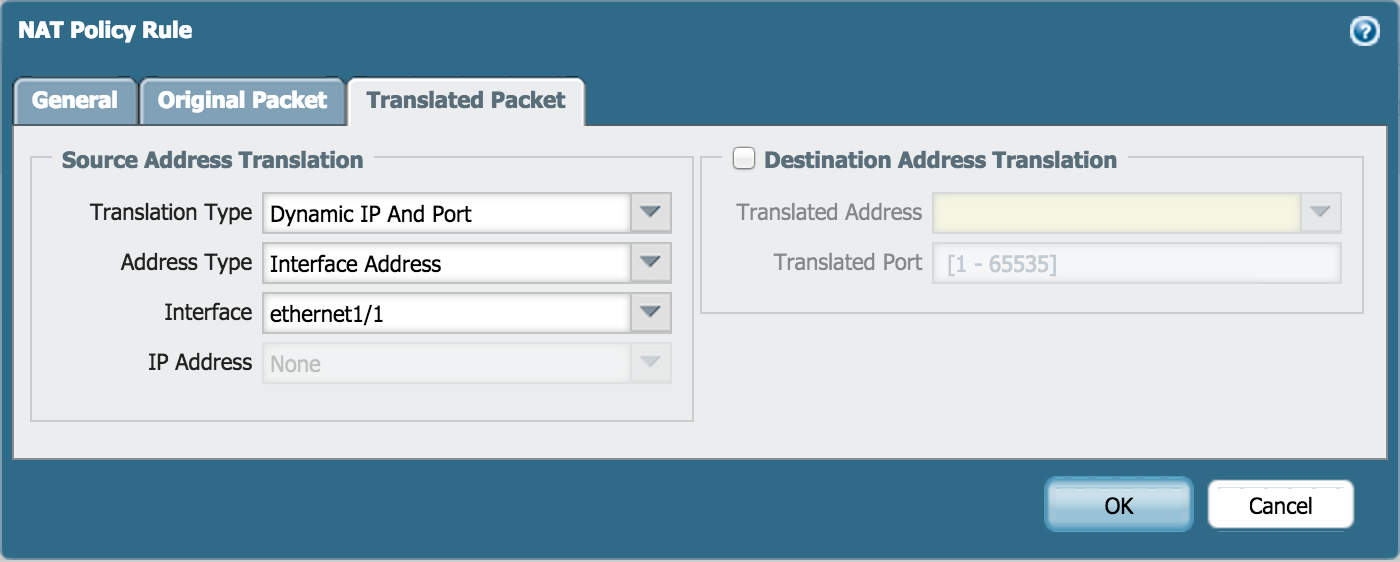


14# On Original Packet, specify the Source Zone, Destination Zone, and Destination Interface



15# On Translated Packet, set:

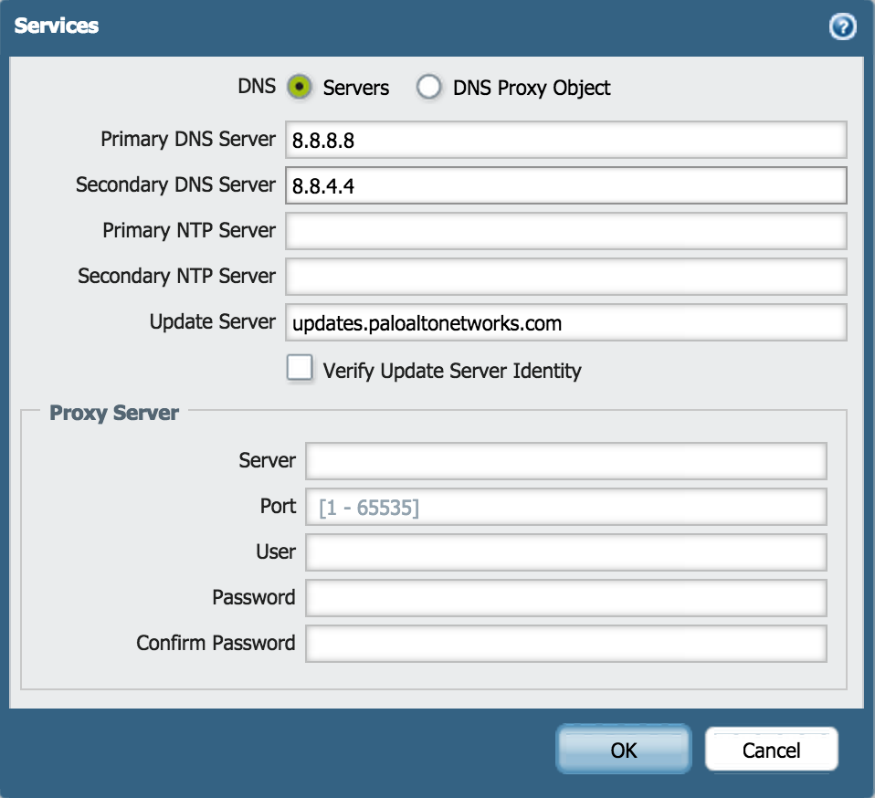
* Translation Type: Dynamic IP And Port
* Address Type: Interface Address
* Interface: ethernet1/1



16# Go to Device > Setup > Management and specify the following Management Interface Settings:

17# Go to Device > Setup > Management and specify the following Management Interface Settings:

* IP Address
* Netmask
* Default Gateway



18# Go to Device > Setup > Services.

Enter the DNS server IPs. For example: Google DNS IP's 8.8.8.8 and 8.8.4.4.

Then commit

**Problems**

Our DHCP pool was not working so we had to change it to do a 192.168.40.1 to 192.168.40.252 and we had to change it to 192.168.1.1 to 192.168.1.252 since I wouldn’t go to the internet with the .40 network, another problem we had was that our zones were not paired together so our traffic was not going to the right place. We also had one of our pc’s is not able to connect to the internet and we still don’t know the reasons it was a equipment issue and nothing we could fix with out knowledge but we got the one working.

**Conclusion**

Now I know how to set up a PA220 fire wall from factory reset to a whole working SOHO configuration with no errors on commit and letting us go to the internet through the ISP with only connecting to the firewalls ethernet connection with no problems