

Sirjan Singh

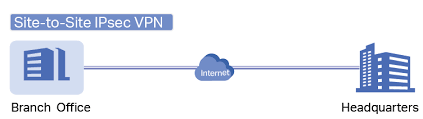
P5

Cybersecurity

LAB 9 –

SITE-to-SITE VPN over IPSec with Self-Signed Certificates

Palo Alto

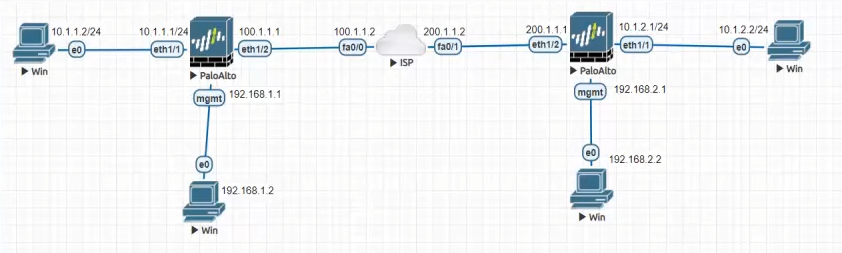


Background/Purpose: The purpose of this lab was to be able to use two of our palo alto firewalls and create a site-to-site VPN between them over IPsec. The topology was one host connected to one firewall, one host connected to the other, and a router in the middle of the two firewalls. A site-to-site VPN allows to create a virtual tunnel between the two firewalls which lets the two firewalls communicate with each other through a secure path. The best part is that this tunnel is simply created over the internet, which means that as long as both firewalls are connected to the internet, one can create a site-to-site VPN. Such a network design is especially helpful for enterprises that have several buildings, and a secure and stable path is needed for all the offices to be able to access resources situated in the corporate office. In this particular lab, we used sha256 encryption and pre-shared keys for confidentiality of data. That is, both firewalls need to have a pre-determined key shared between them for them to verify each other and the tunnel to work.

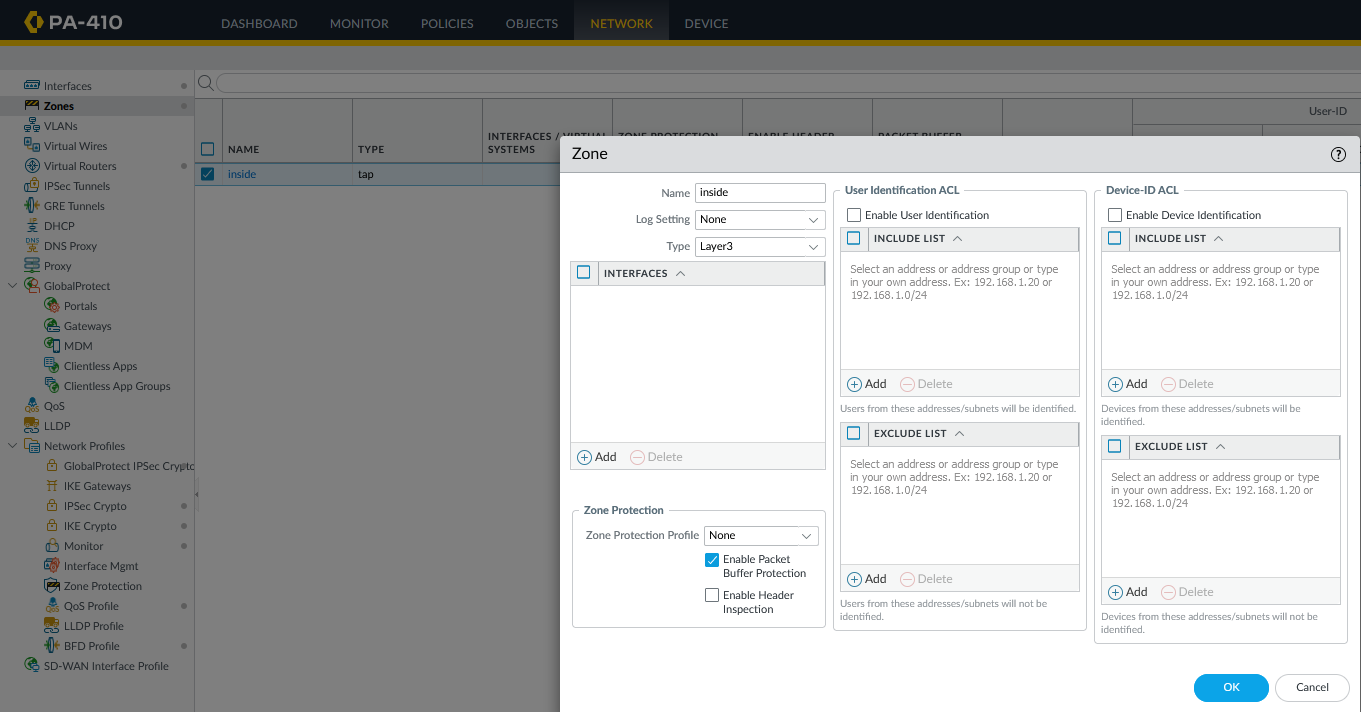
We first factory reset our firewalls so that we could use static Ips to configure all the interfaces in the topology. As opposed to what is shown in the topology, until all the configurations were done, we put both of our pcs in the management interfaces of the firewalls. This is because to put the configurations you need to be in the management interface. After all the configurations were done, we configured out pcs with the right Ips and connect them to the LAN of the firewalls. This process made troubleshooting a little hard, but with only 2 PCs, that is the only option we had.

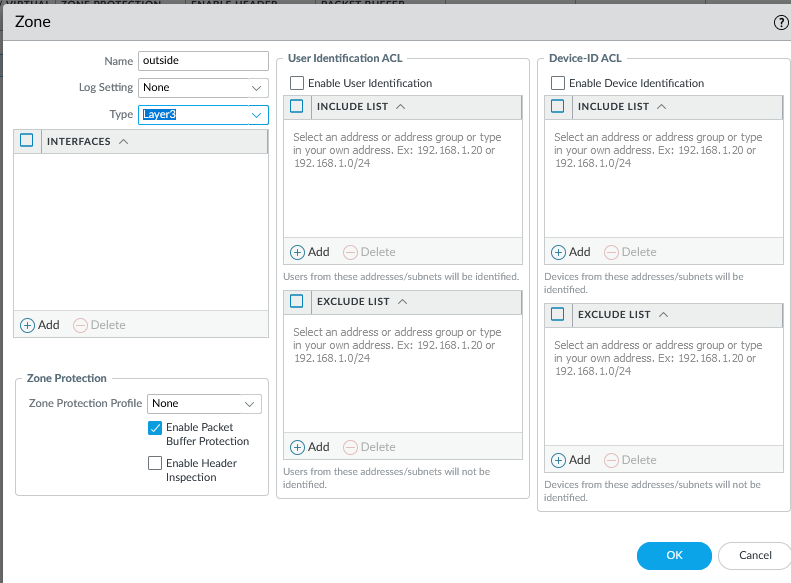
https://www.youtube.com/watch?v=jGh7ZPyqMHk

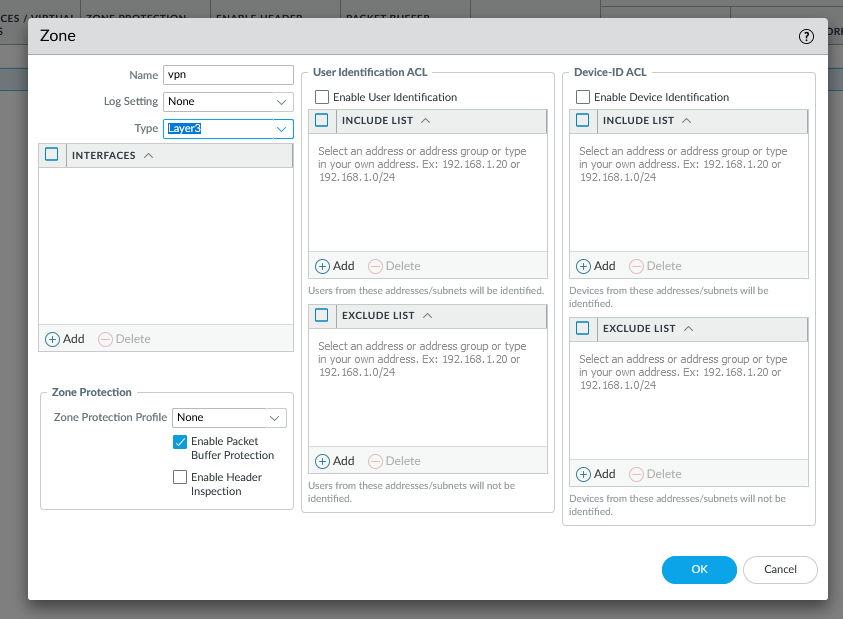
The first thing that needs to be made sure of is that you need two Palo Alto firewalls. We will alternate configuring the two.



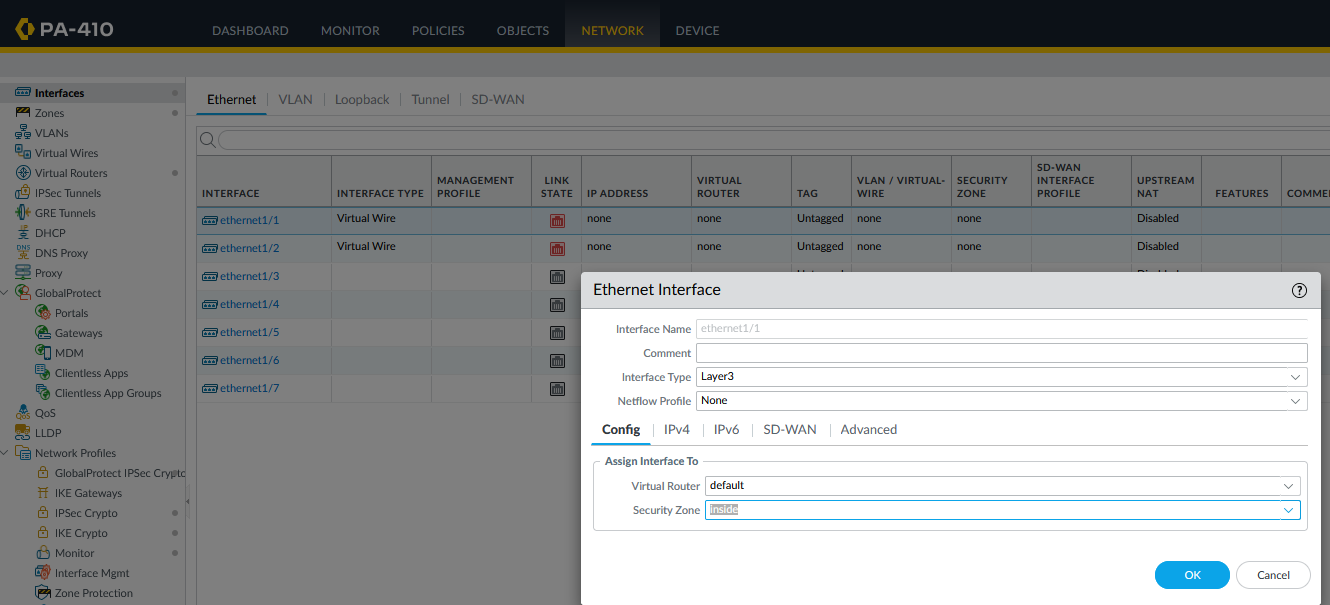
Lab Summary:

Step 1: Create inside outside, and vpn zone and set them to be layer 3

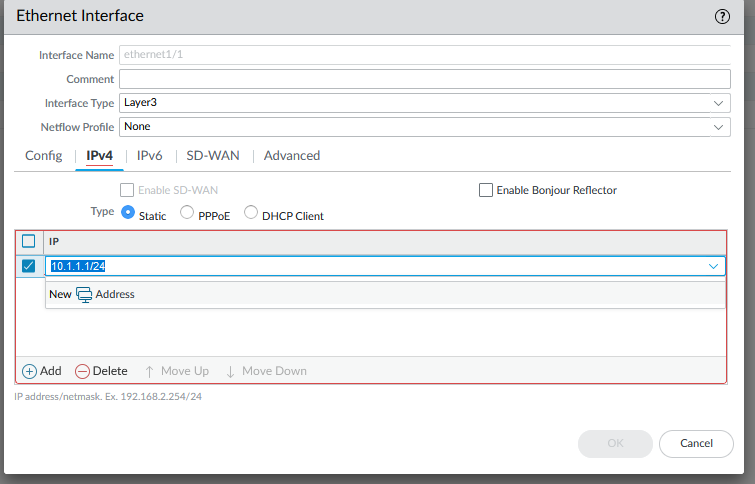


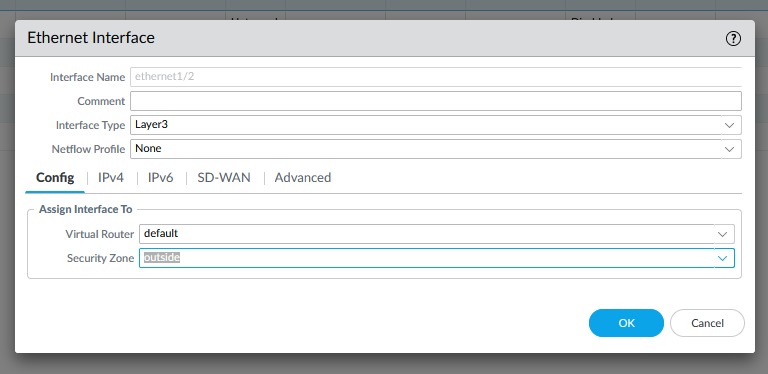


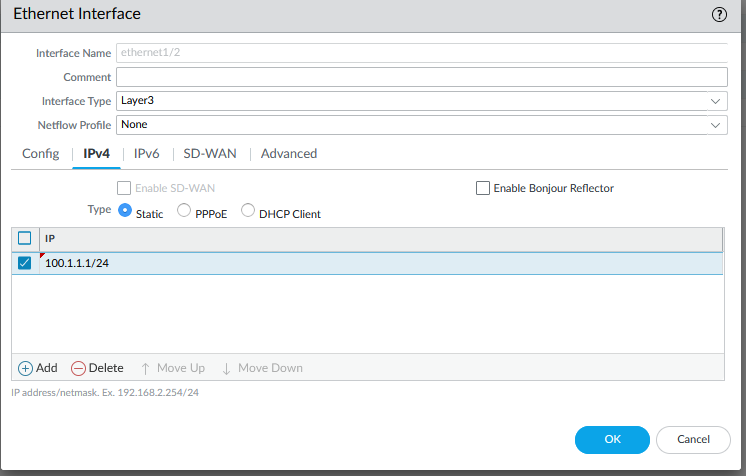
Step 2: Place eth 01 in inside zone



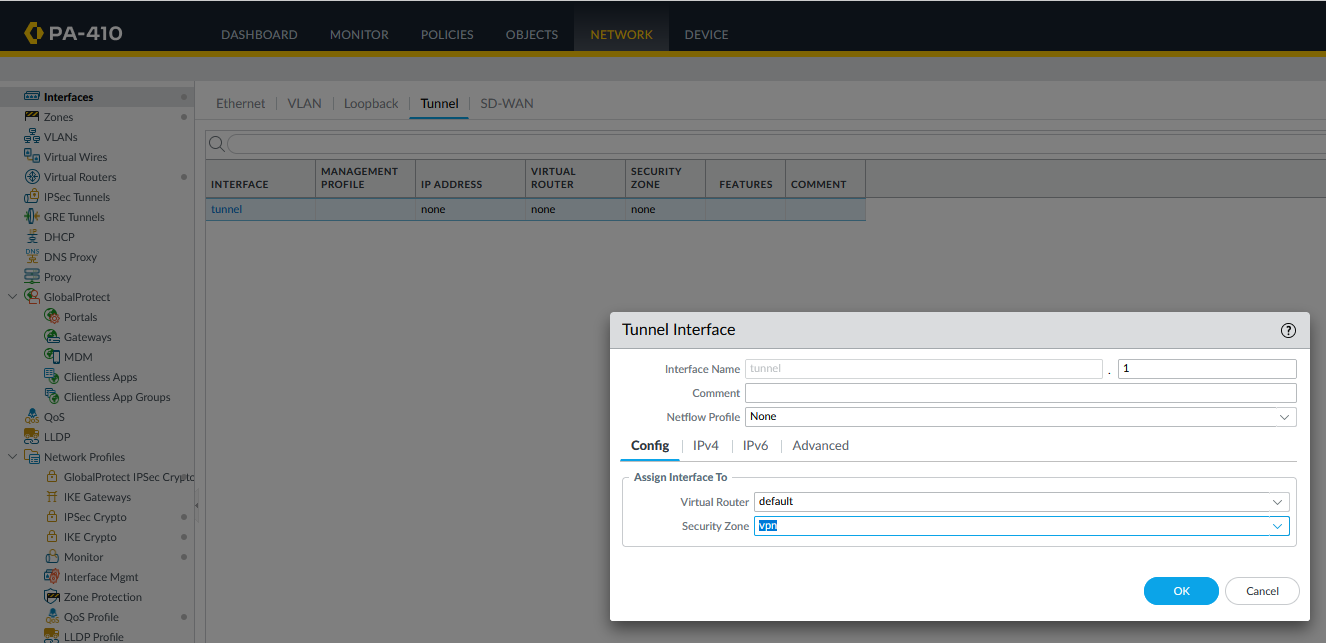
Step 3: Set the following ip in eth 01

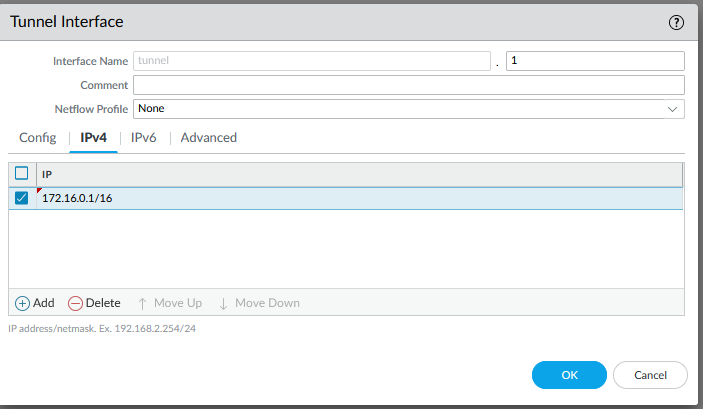


Step 4: place eth 02 in outside zone 

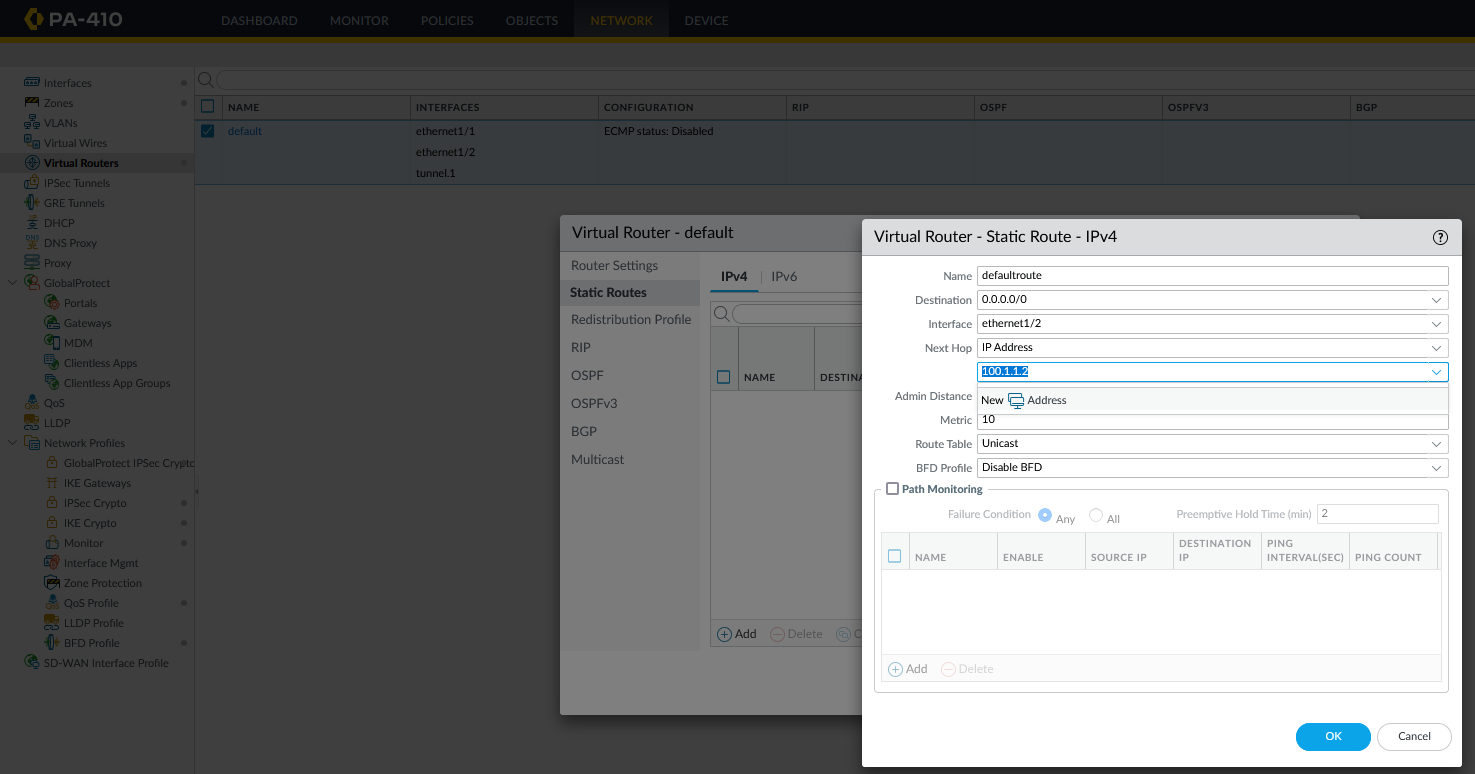
Step 5: give eth 02 the following ip address

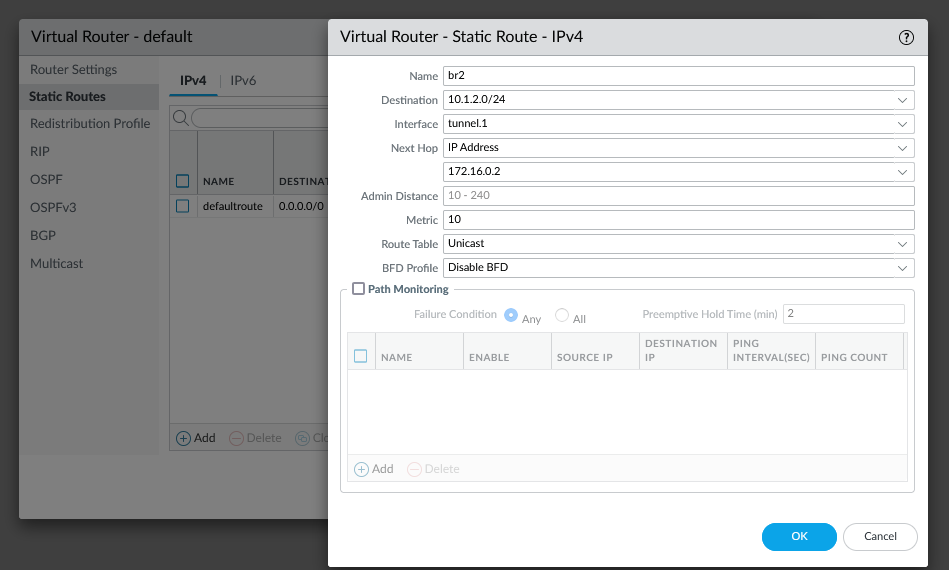
Step 6: Create a tunnel interface and place it in the vpn zone



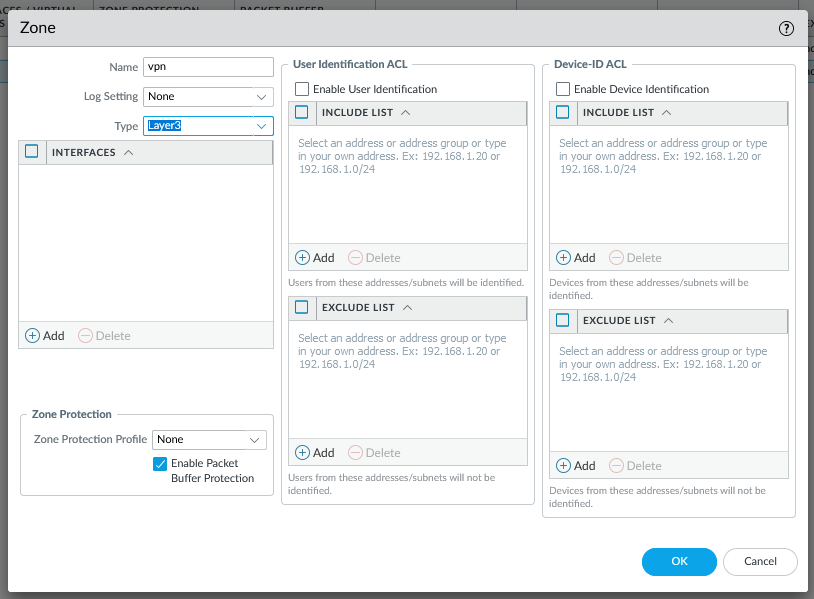
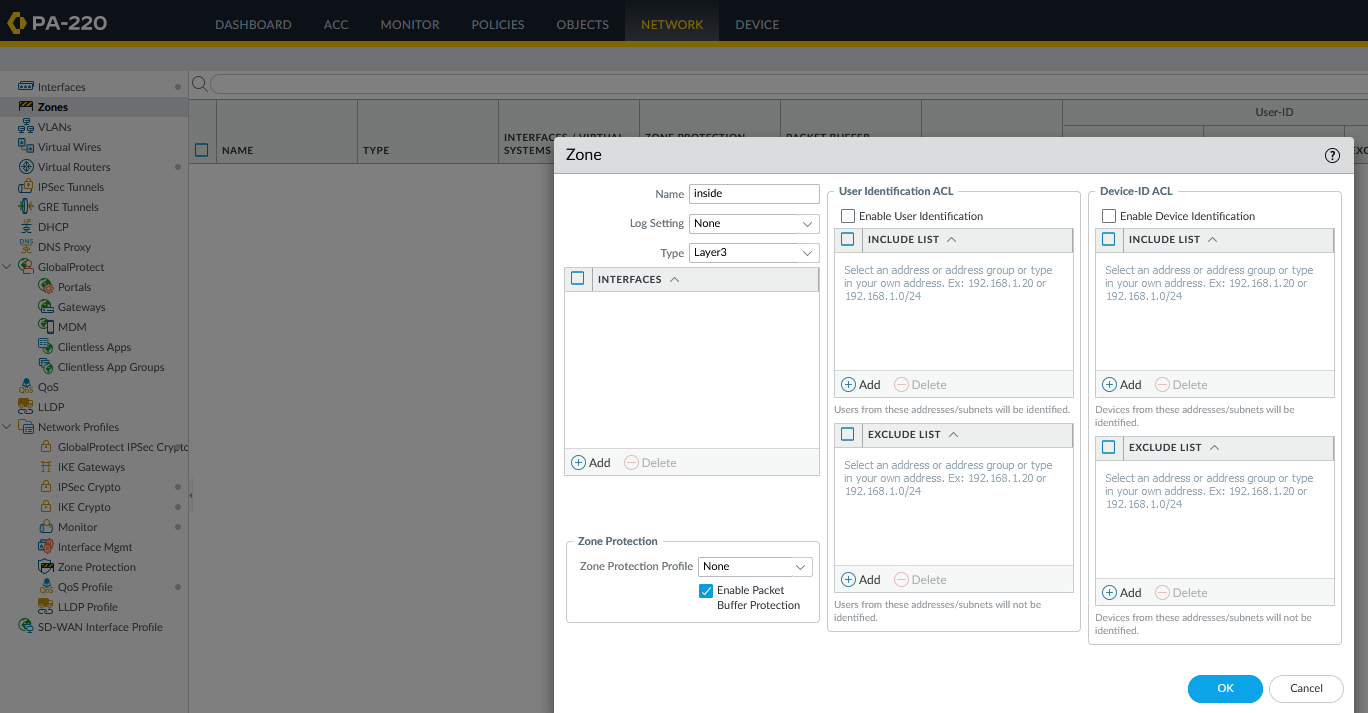
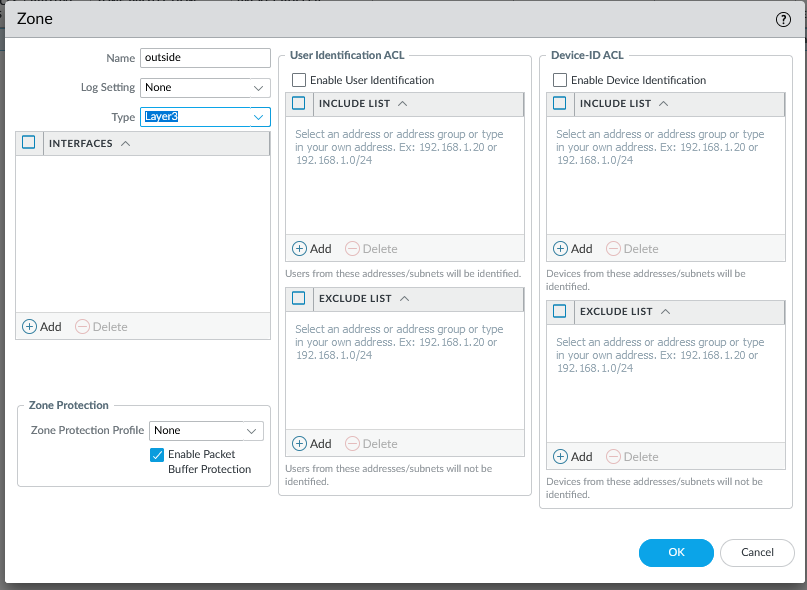
Step 7: Give the tunnel interface the following ip address

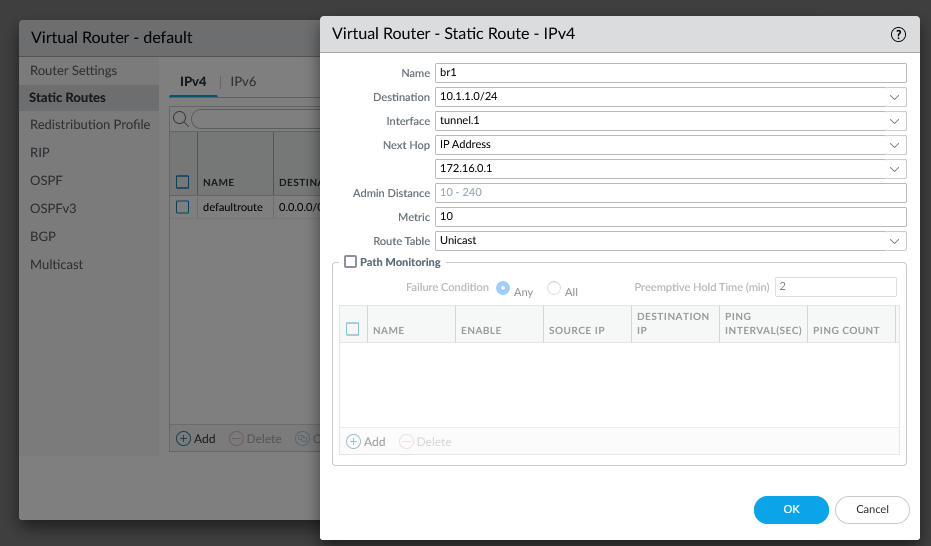
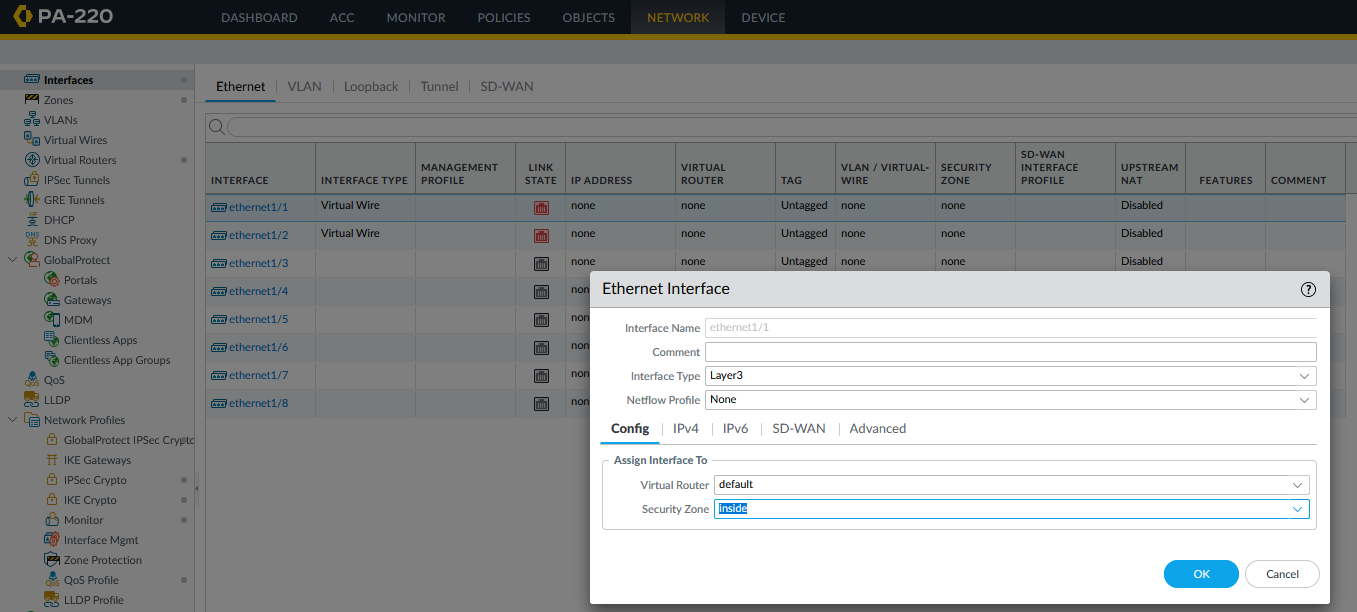
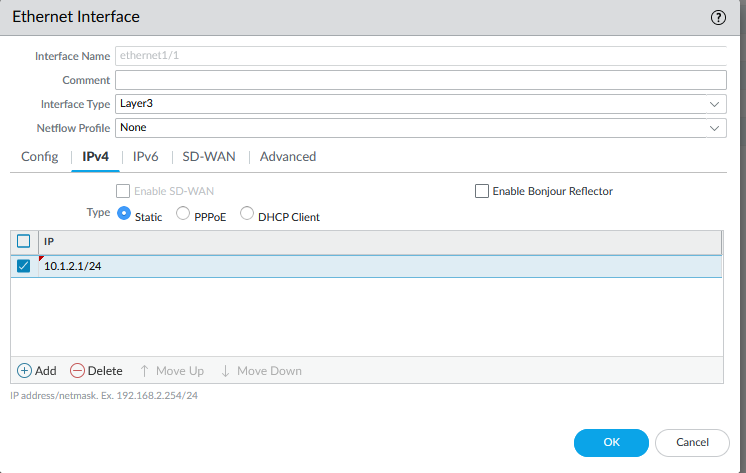
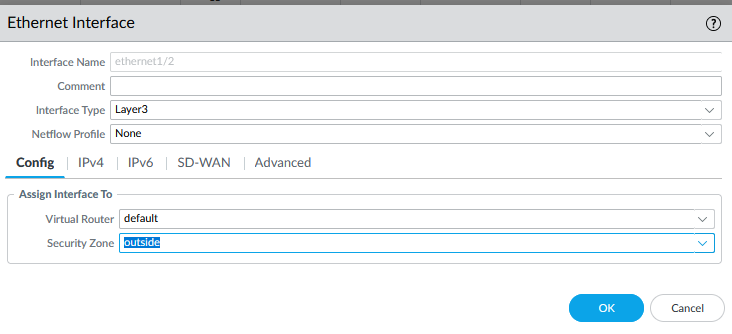
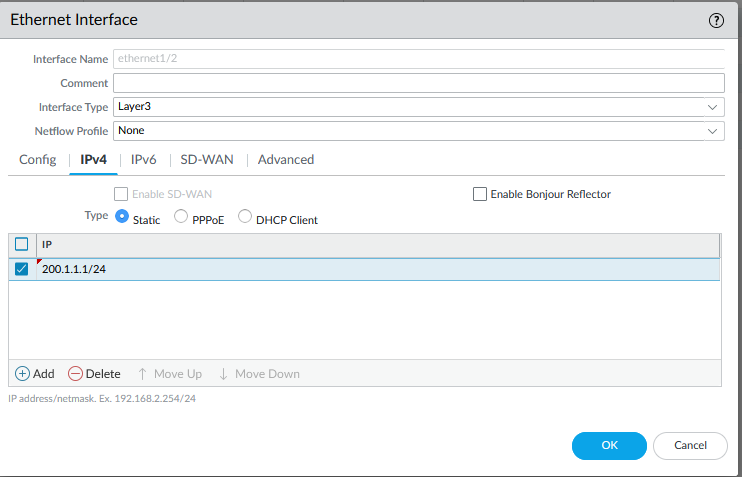
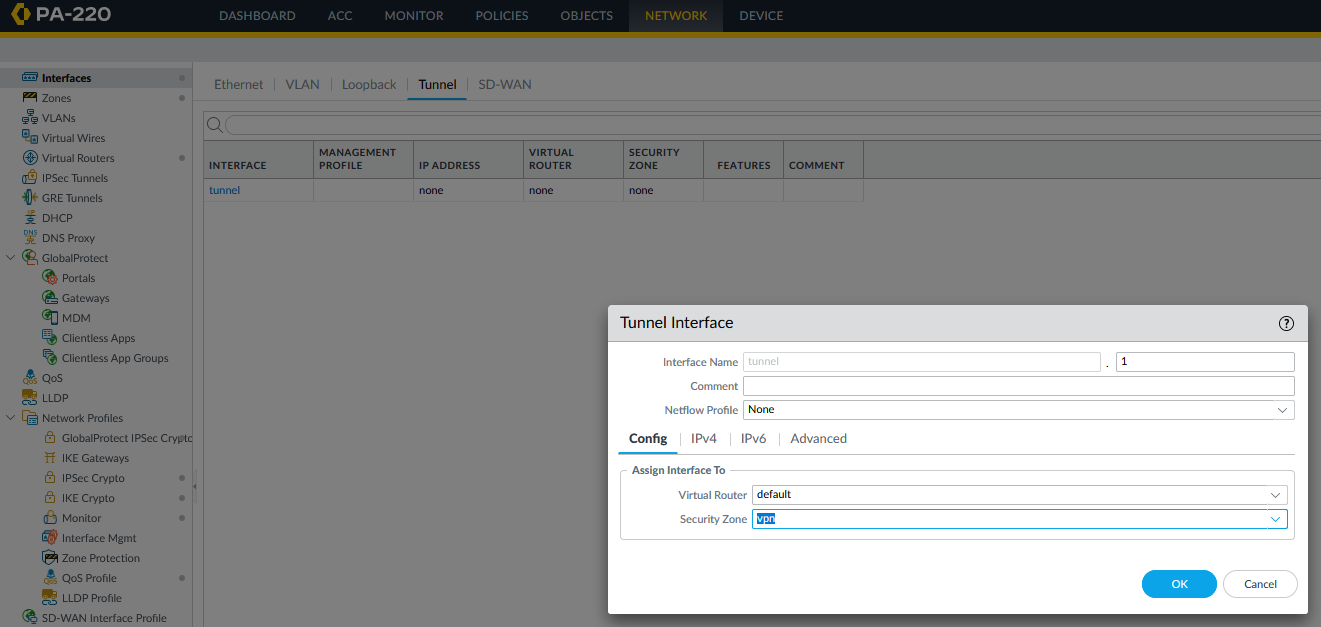
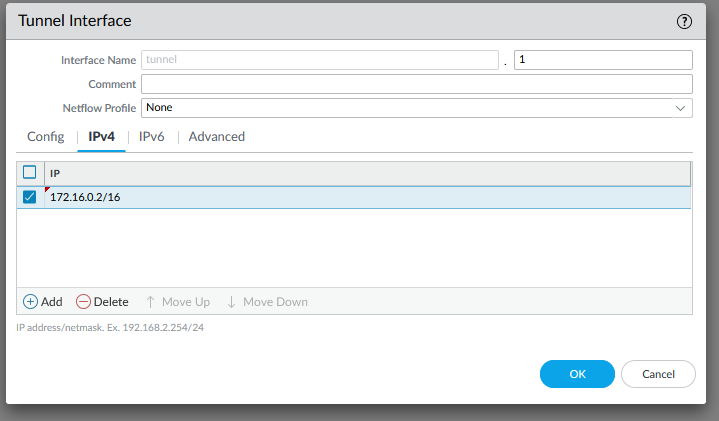
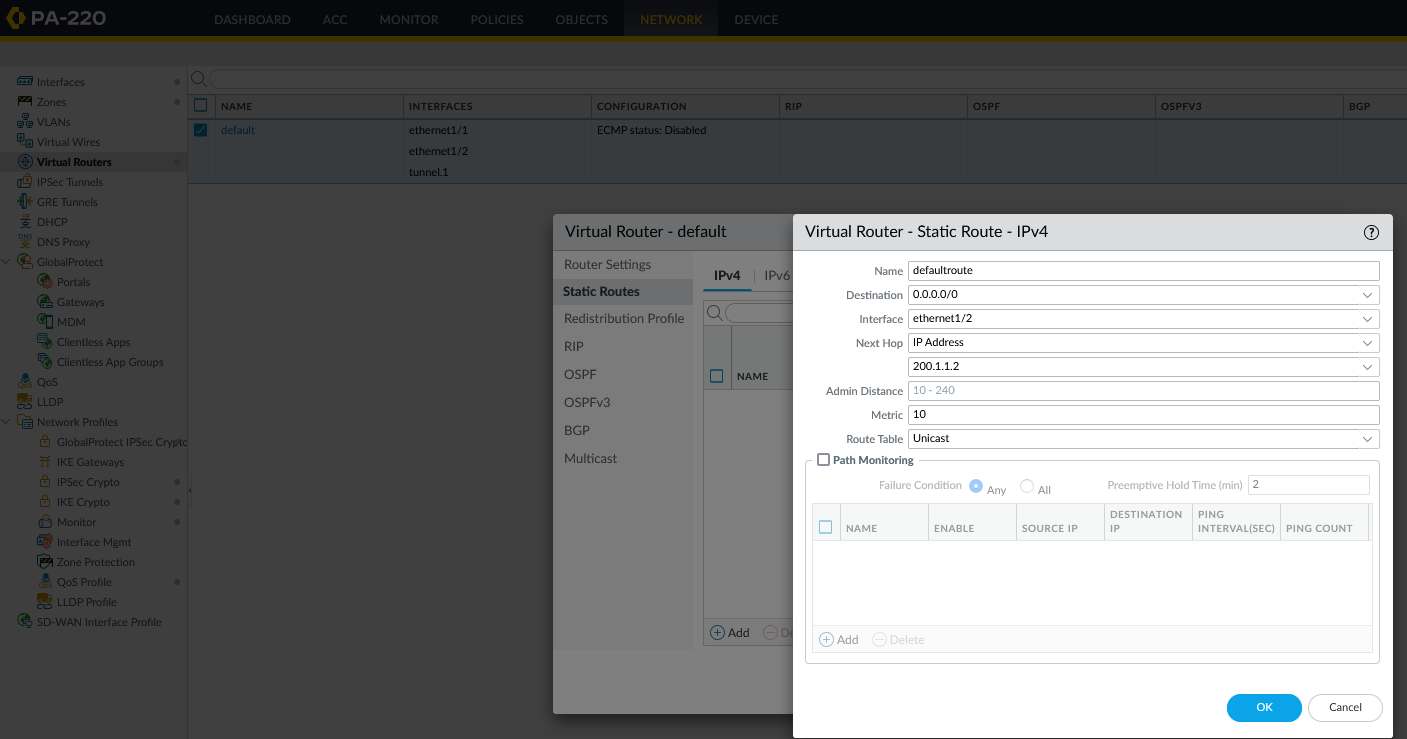
Step 8: Go to virtual routers -> static routes. Enter the following configurations for default.



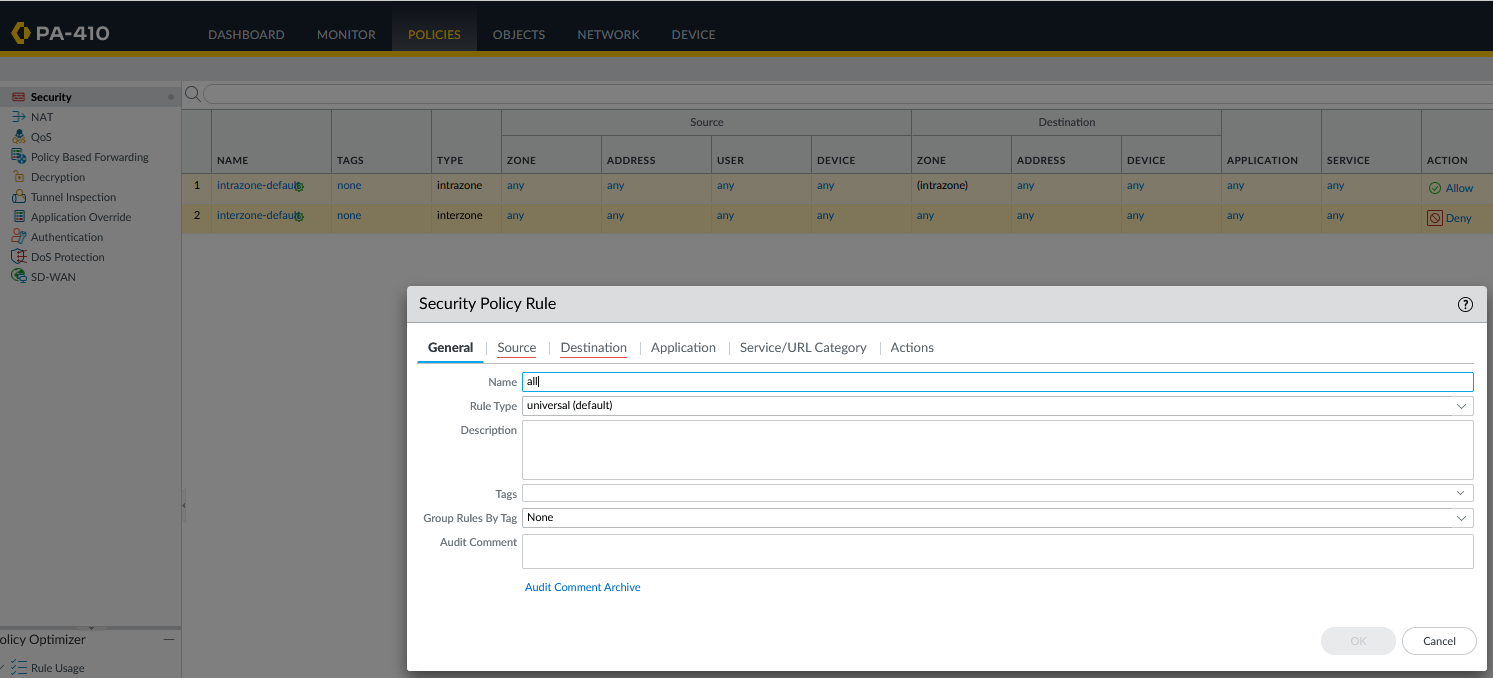
Step 9: Create another route, and enter the following configurations. 

Step 10: Now you will do the same thing for the other palo alto that you are working with.

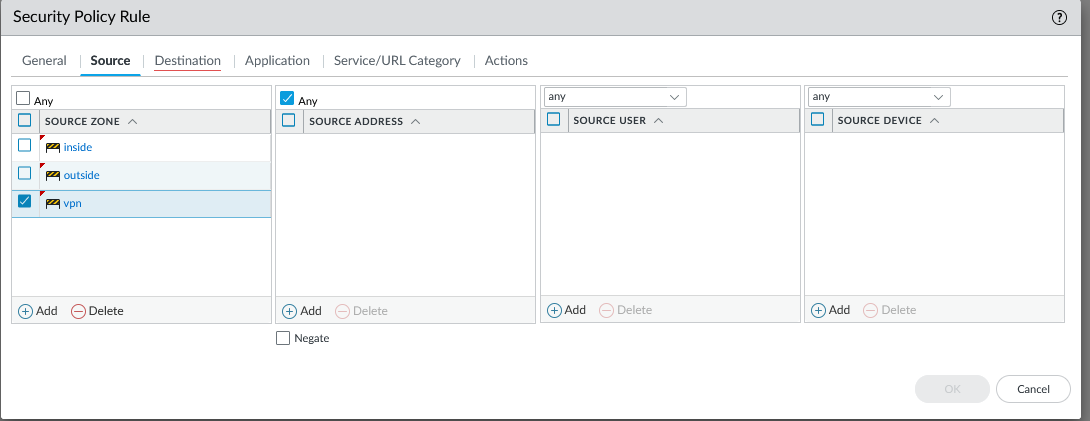


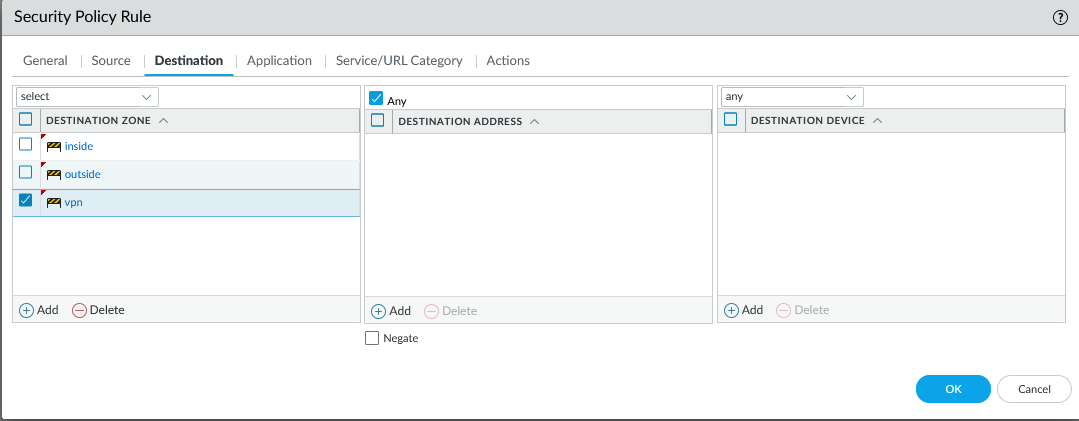


Step 11: Switch back to the first firewall. Create a security policy rule.

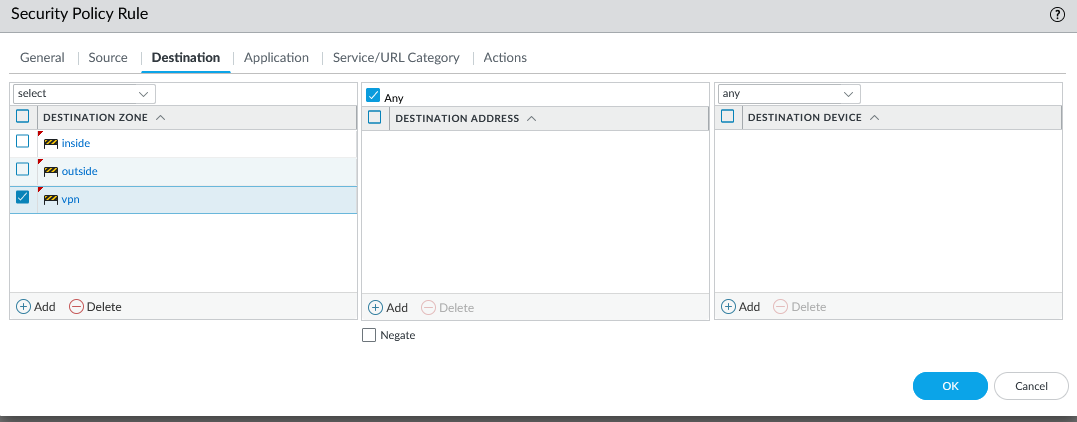
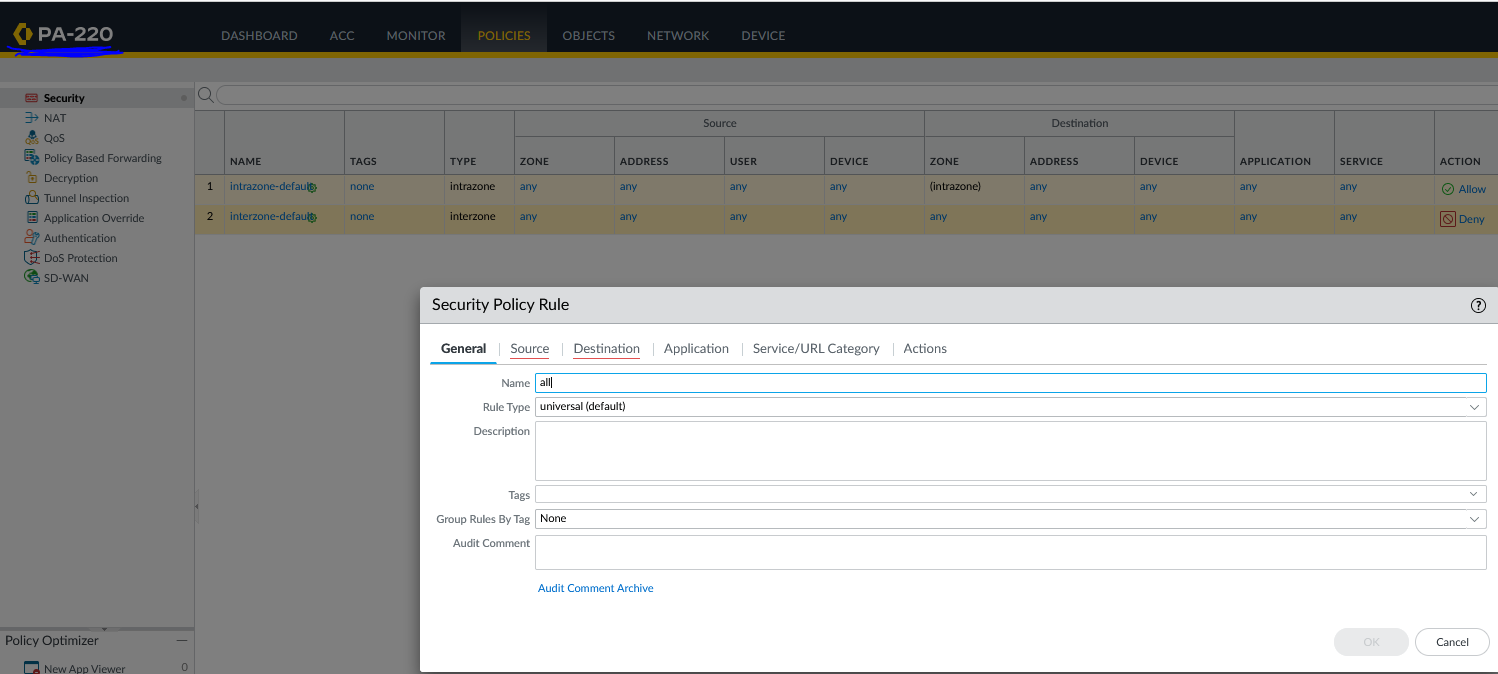
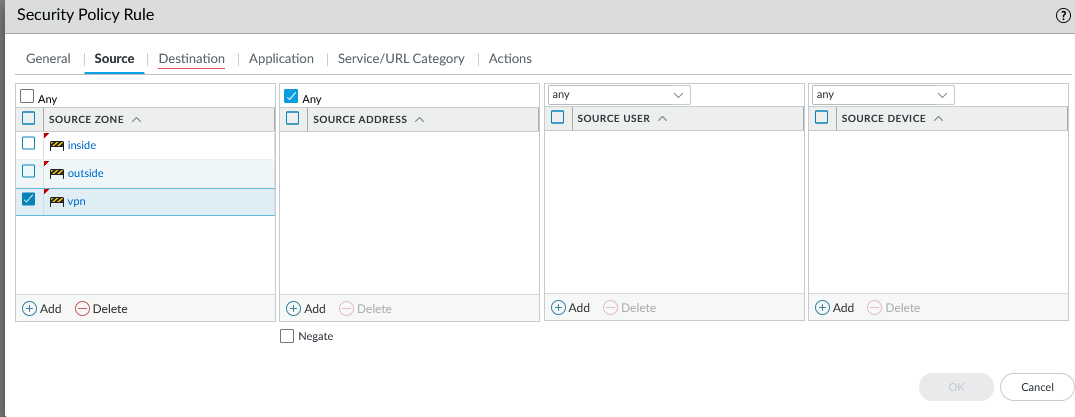


Step 12: The source should be all zones (inside, outside, vpn)

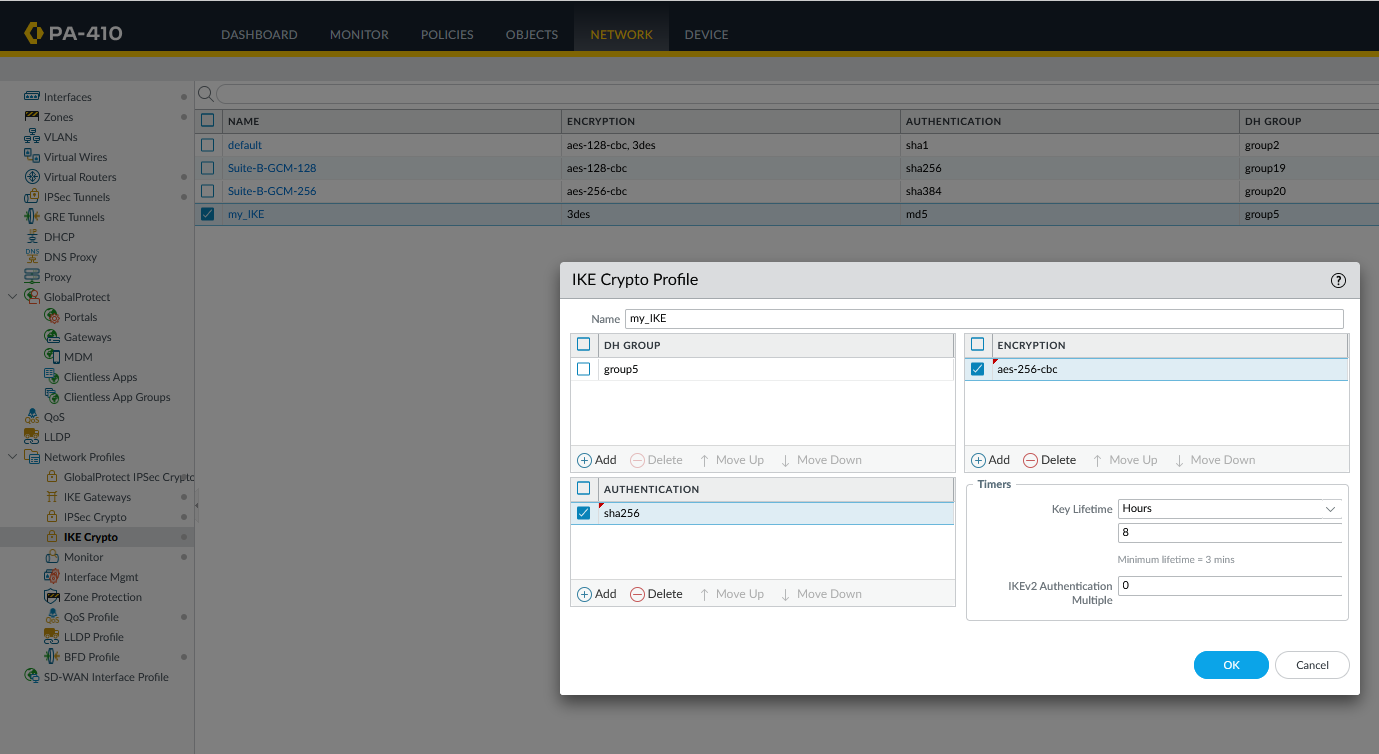


Step 13: Should apply to destination for all zones too. 

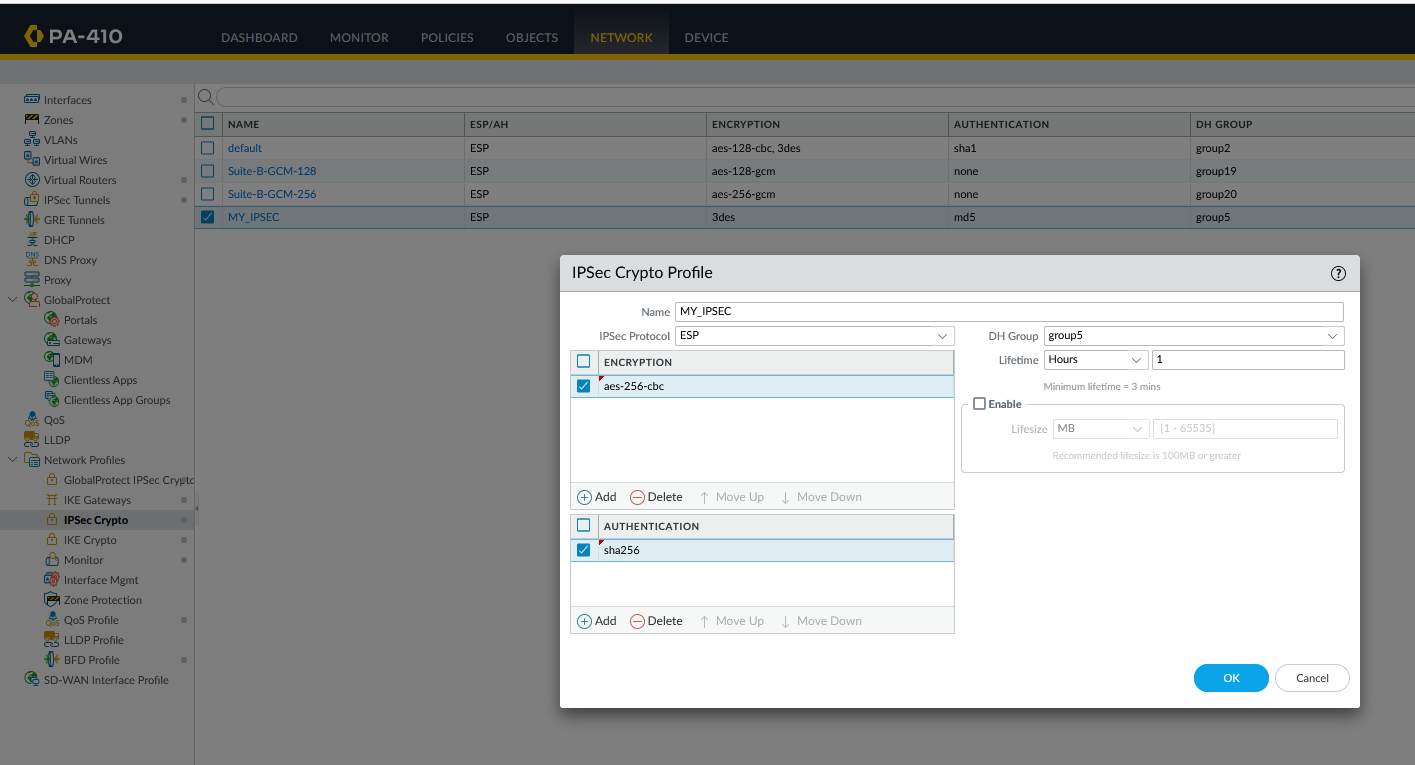
Step 14: Do the Same for the other firewall



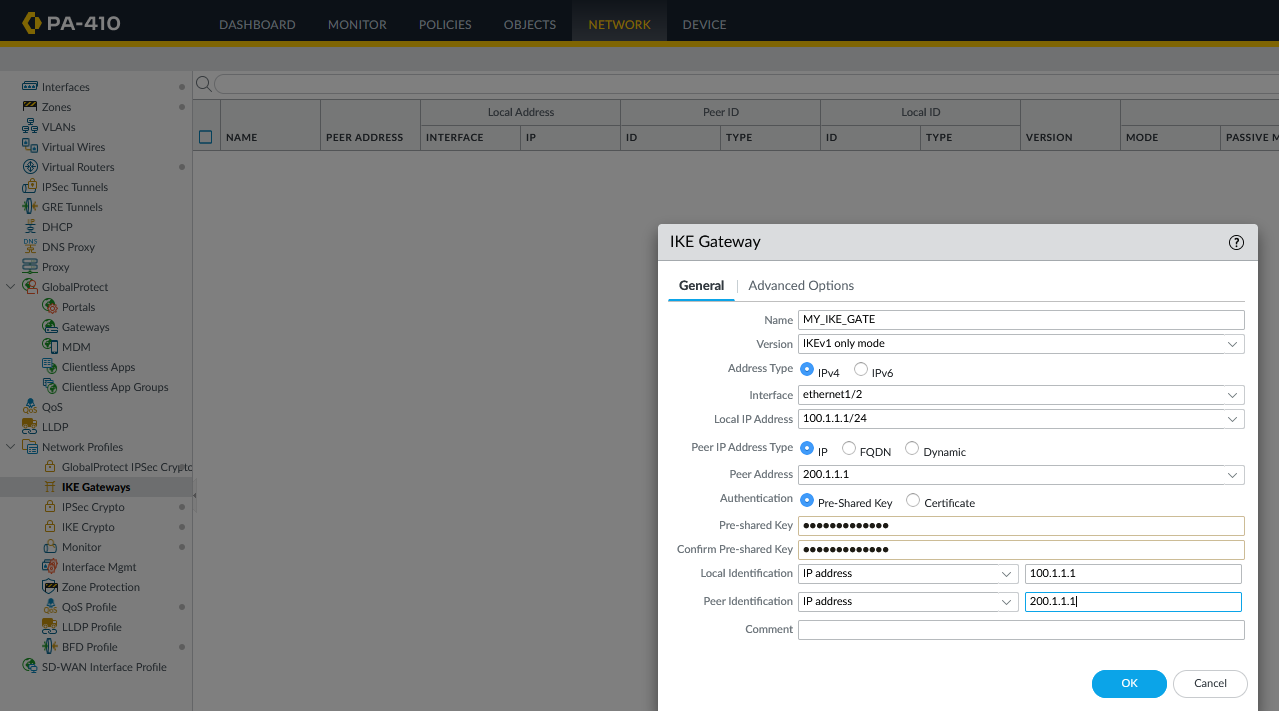
Step 15: Go to Ike gateways and enter the following configurations.

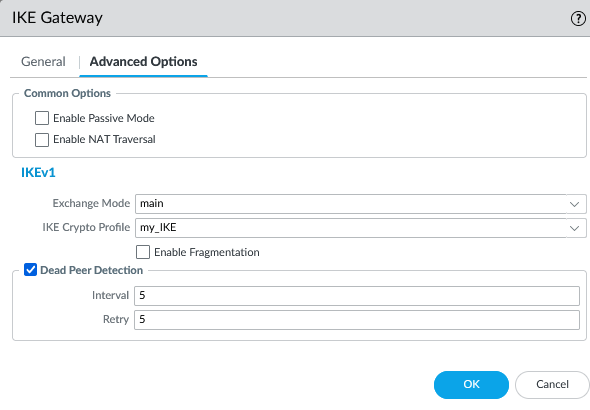


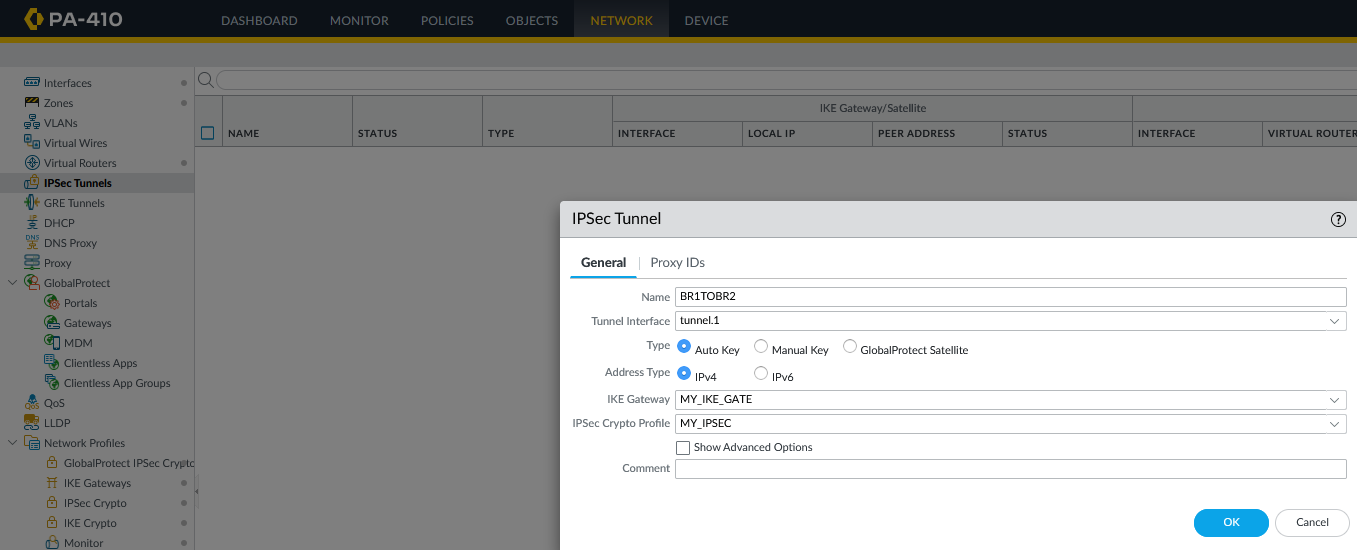
Step 16: now go to IPSec crypto profile and enter the follow configurations.



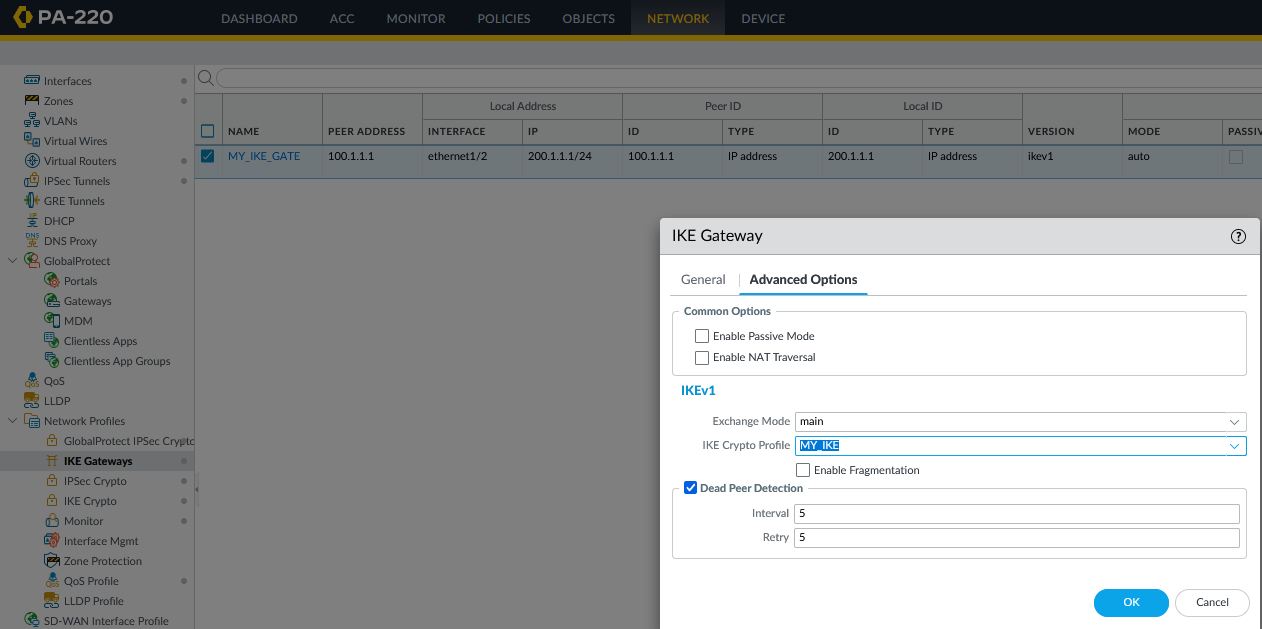
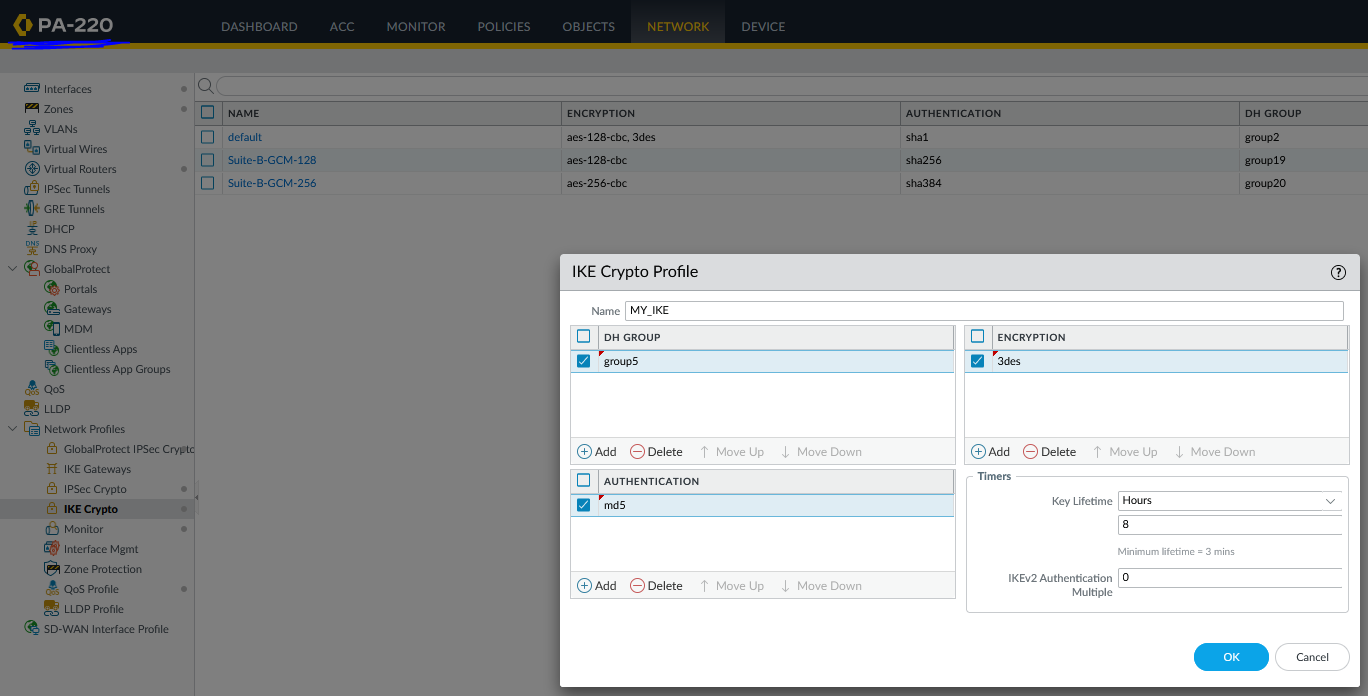
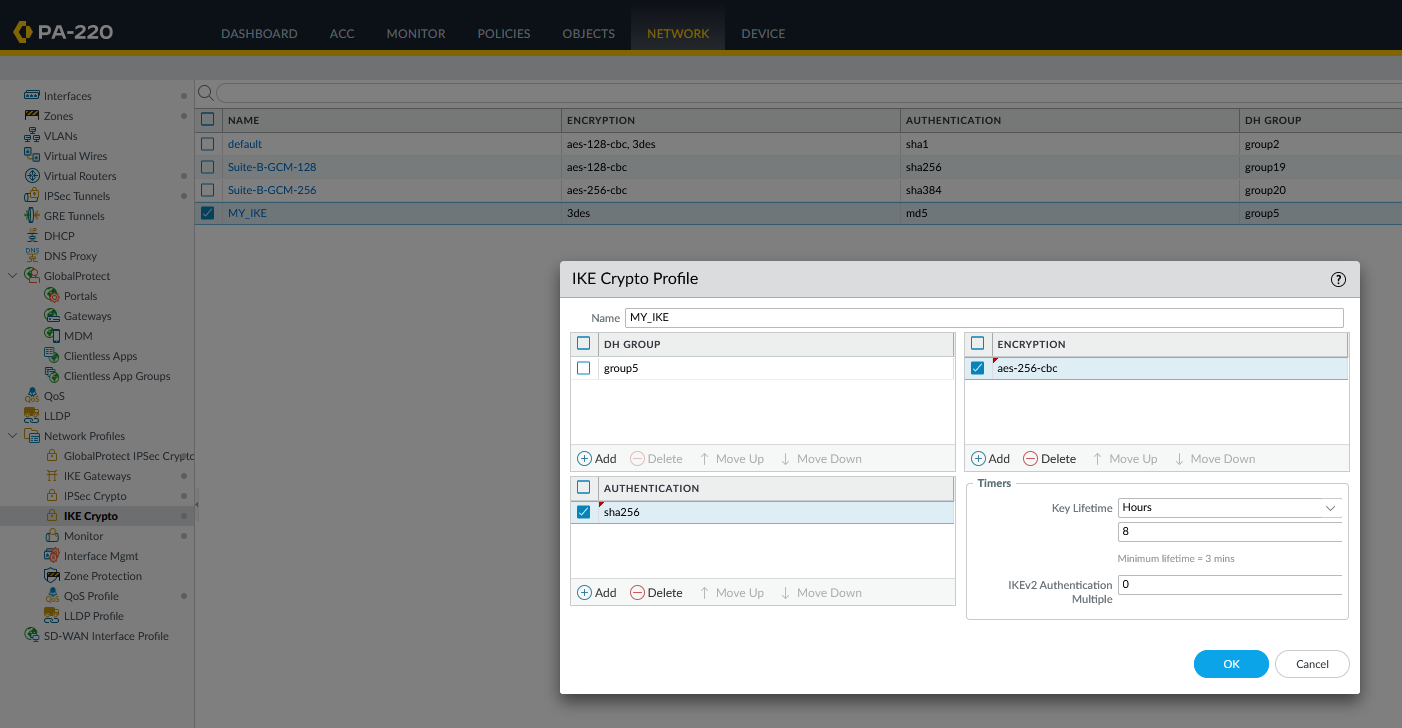
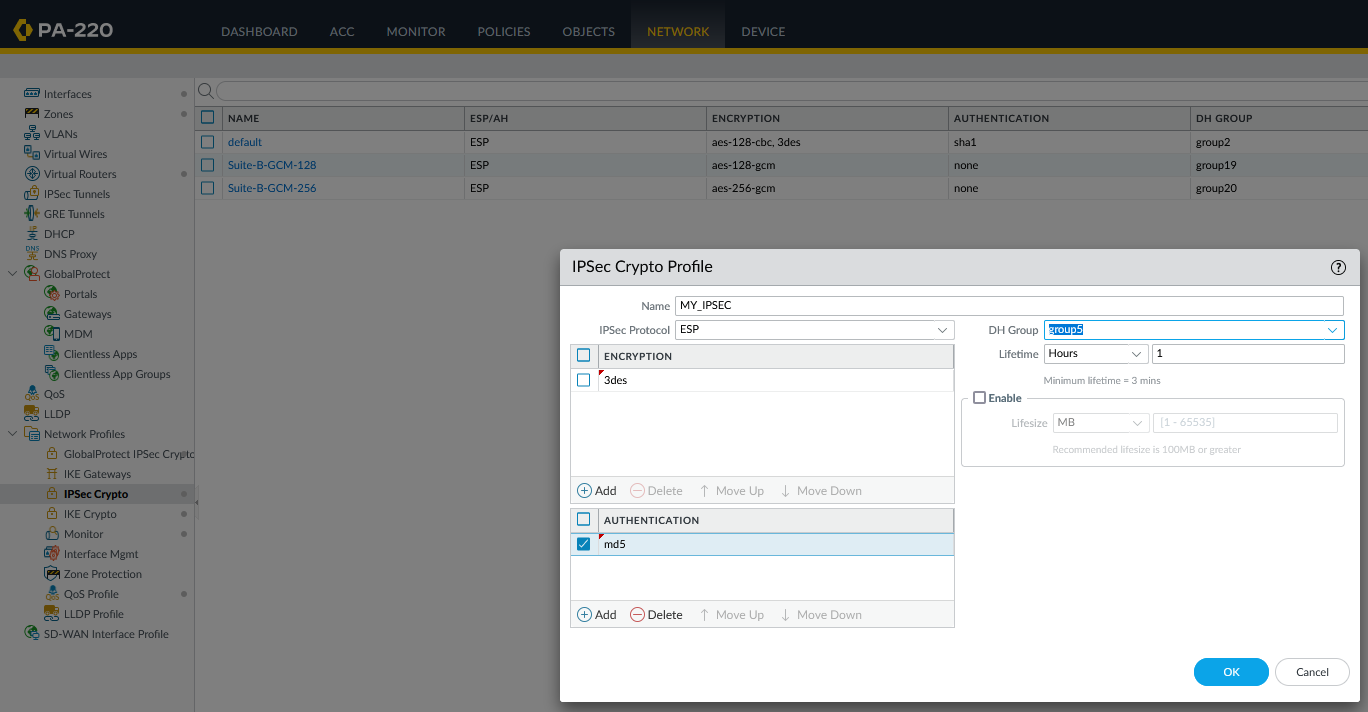
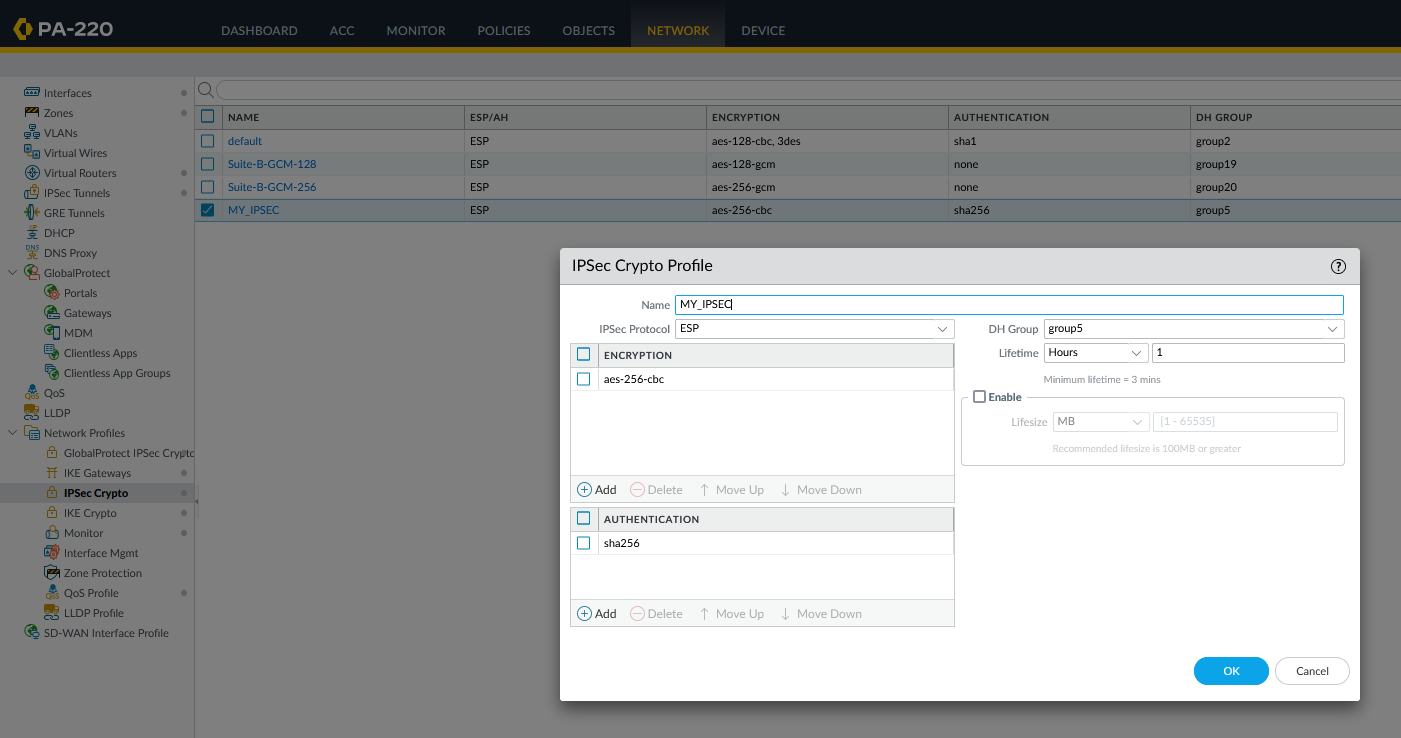
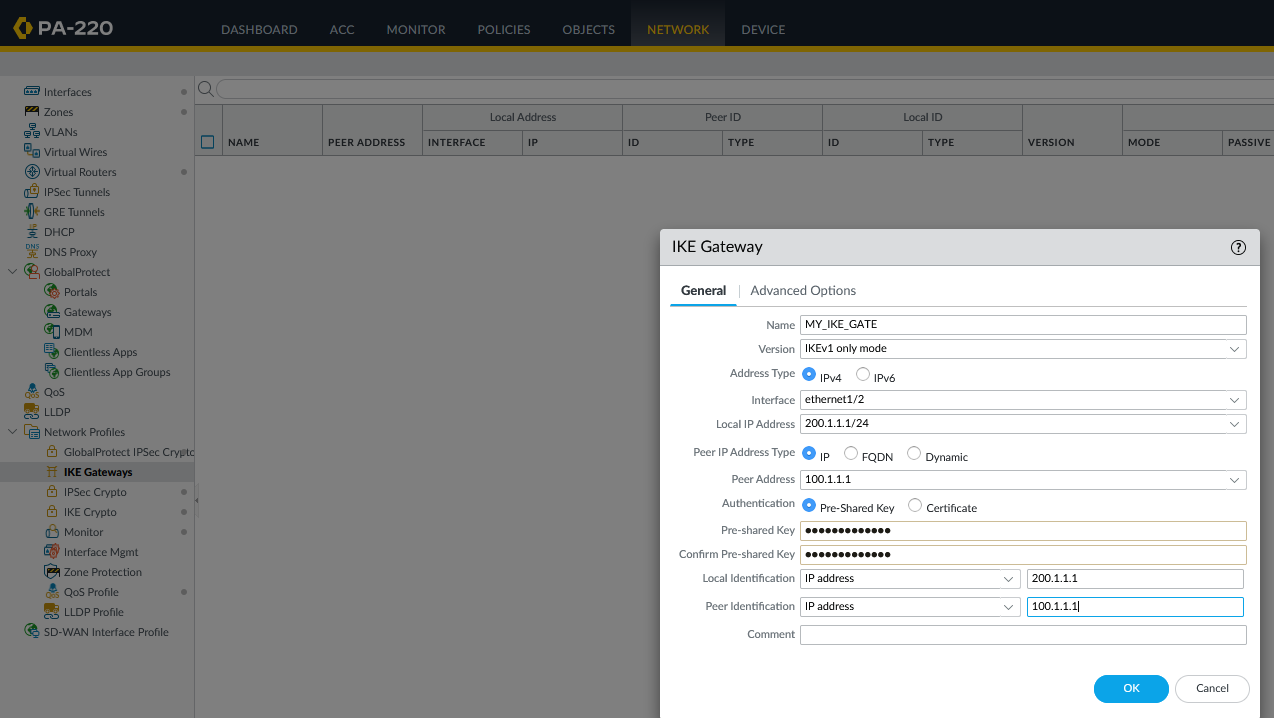
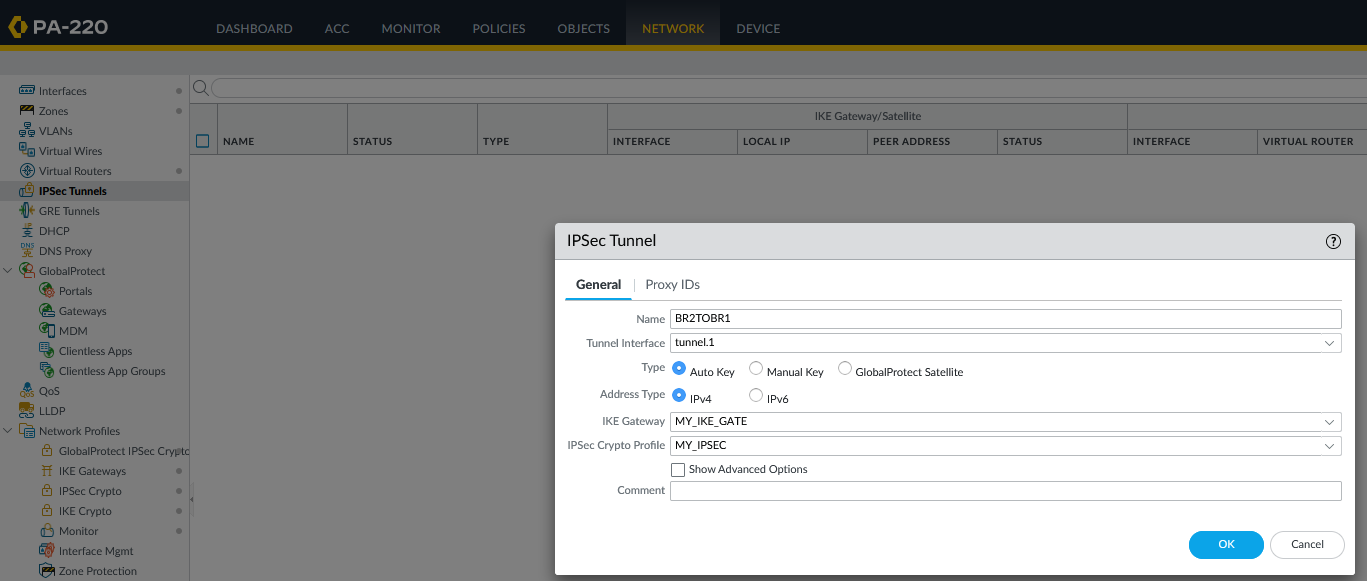
Step 17: Now go to IKE gateways and enter the following configurations



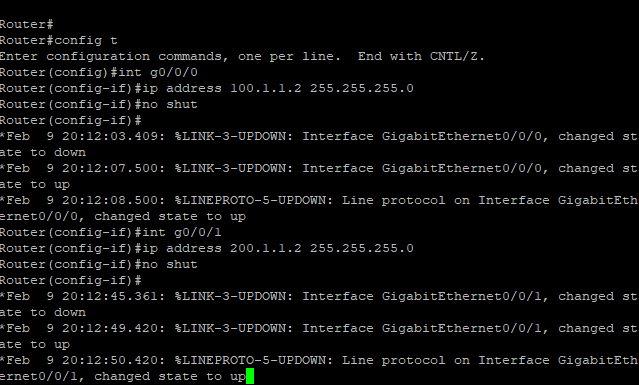
Step 18: Go to advanced options and enter the following.

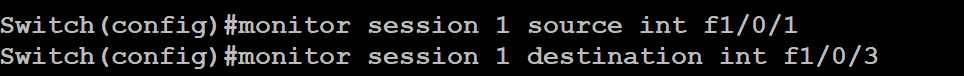
Step 19: Go to IPSec and enter these configurations

Step 20: Now, do these same steps for the other firewall



Step 21: Now, you will need a router. Place a router in the middle of the two firewalls according to the topology show above the first step. Plug it in. Enter the following configurations on it.





Problems:

The first problem that we faced was that despite completing all the step, out tunnels were showing that they were off. We realized that after completing the configurations, you actually need to press enable (hidden in the bottom of the page) on the tunnel on both firewalls as well as on the IKE gateway page. However, that alone won’t do the trick because after that we needed to commit your changes. But that still didn’t turn on the tunnels. After a lot of research, we found out that there are commands that you can use to troubleshoot and activate the tunnels. First, to activate the IPSec tunnels, we consoled into the firewall and then entered the command: . To turn on the IKE gateway, we entered the command: . After a while, after waiting, the tunnels were finally on. However, we still weren’t able to ping across. To fix this, we confirmed out configurations a number of times and saw that out pre-shared key actually weren’t matching on both. This was surprising until we realized that the reason for this was that the pre-shared key have to be exactly 8 characters long on both, otherwise palo alto adds random characters or removed random characters from the password, causing the pre-shared keys to not match and the IPSec tunnel to not work. After making out password 8 characters long and committing changes, we were able to ping across.

Conclusion:

In this lab, we learned several different troubleshooting techniques. First we leaned the importance of knowing console commands on the firewall that help expedite the process of activating tunnels. We also learned that you can set a filter on the firewall web interface that allows you to see the traffic coming through each zone. This helped us because we were able to figure out whether the reason we weren’t able to ping was an internal (LAN) issue or an external issues (side of the network that faces the router). It also showed us how the tunnel interface traffic which led us to figure out that the pings were actually being and sent and received on both sides of the tunnel, but they were simply getting dropped for some reason. We understood that this must be a security policy issue rather than an issue with the tunnels themselves.