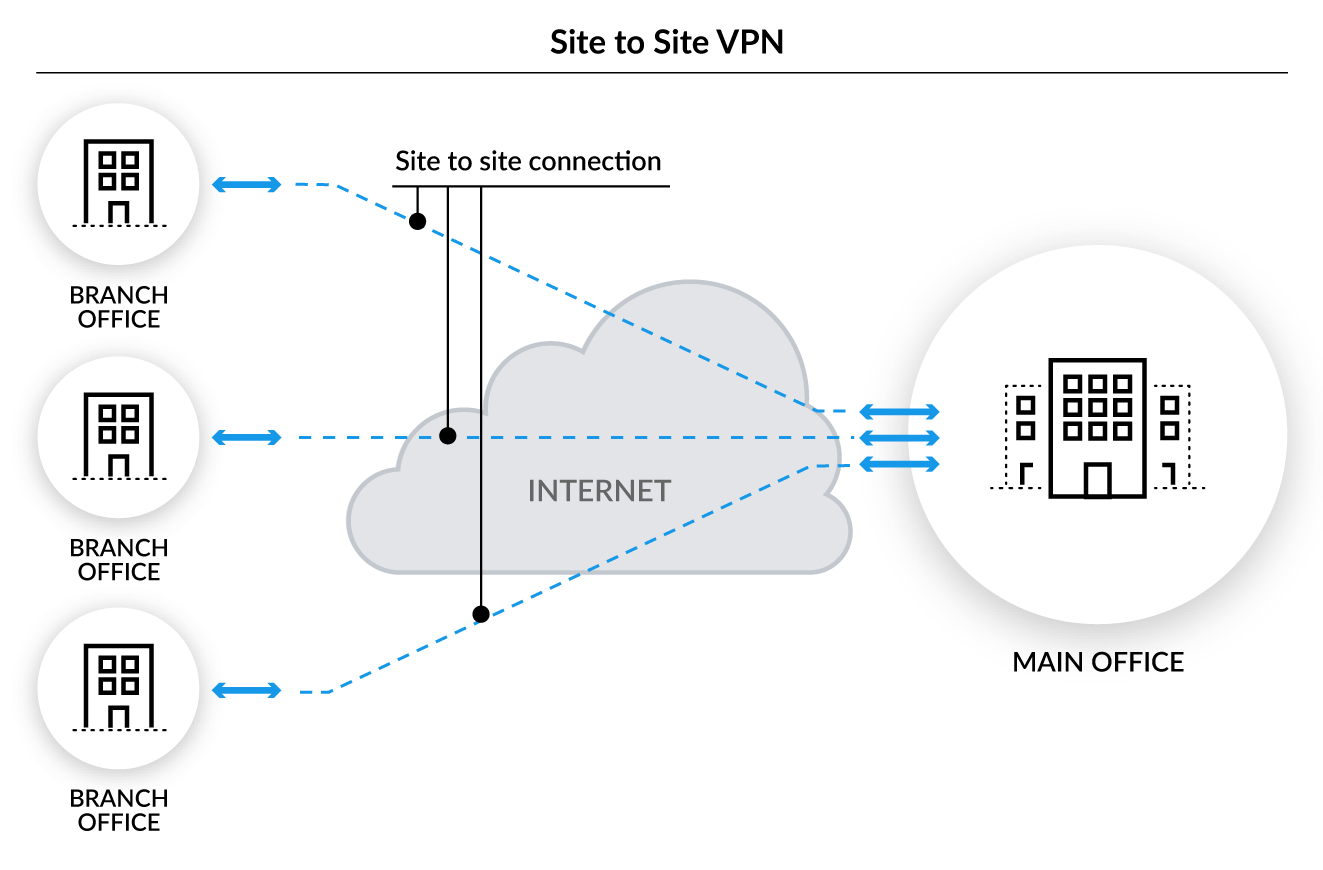
Site to Site VPN Palo Alto

Reed Holman | Cybersecurity | 3/8/2023



Purpose: The point of this lab was to fully configure two firewalls to connect using a Site-to-Site VPN with pre-shared keys.

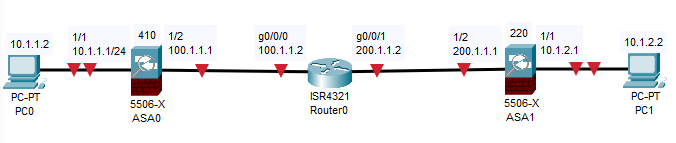
Background Information:

A VPN or a Virtual Private Network is a way to have a secure connection between different devices or networks. There were many different types of VPNs with different uses like Remote access, site-to-site, etc. VPNs are very useful for using a public network and wanting to access the internet securely.

Site-to-Site means that there is an encrypted connection between two networks. Site-to-Site is the protected and encrypted link usually between a branch office and the corporate network. Most companies have outgrown the need for site-to-site VPNs because they have started to move lots of their data to the cloud and they now have many employees using mobile devices. That means that it is no longer necessary to force all the data to go back to a data center and instead everyone can just access it in the cloud. Site-to-site can be hard to scale with that many moving variables, but it still has its uses. A remote access VPN is different because that connection is temporary and is most commonly used to gain secure access to a data center.

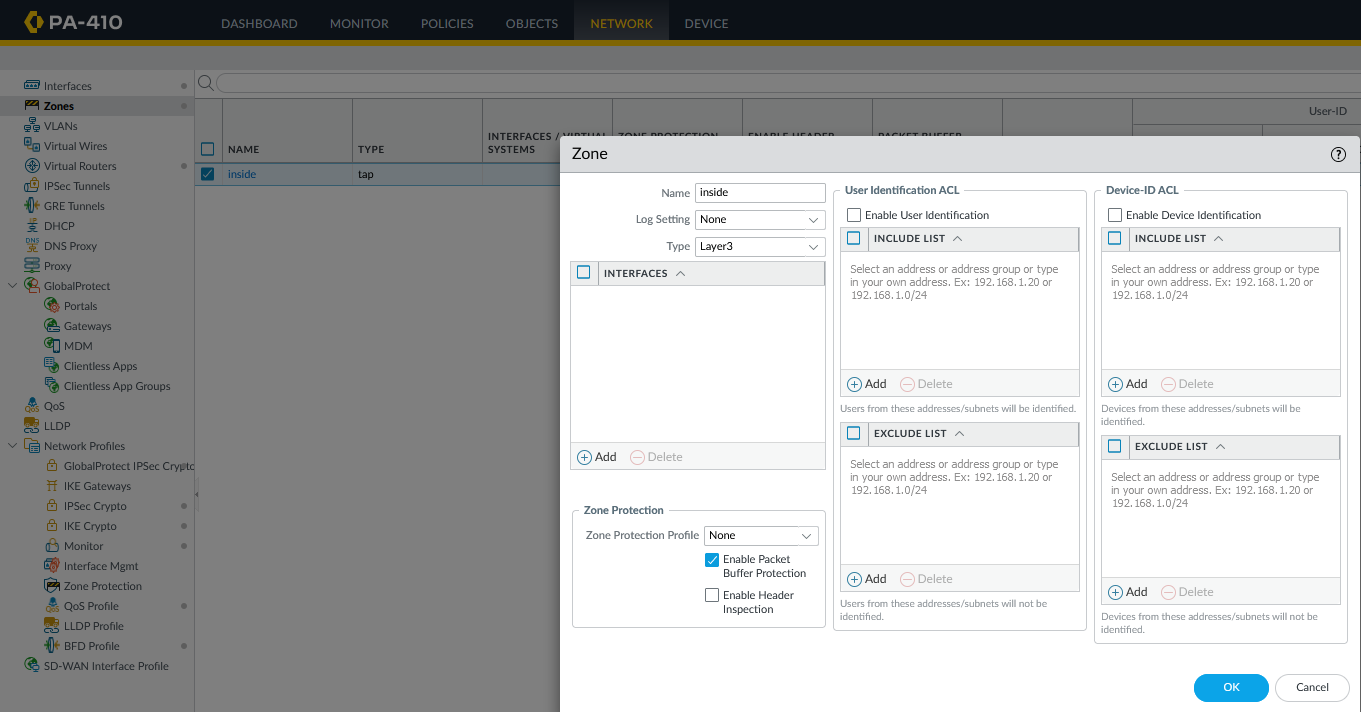
We used pre-shared keys to authenticate a connection between the networks. This means that each end of the tunnel is configured with the same key. So only networks using the same key were able to connect and communicate with each other.

Diagram:

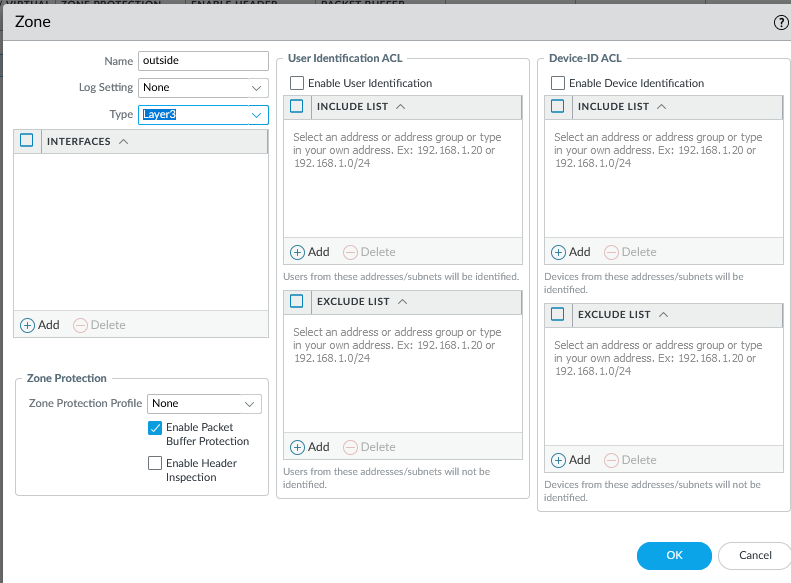


Steps:

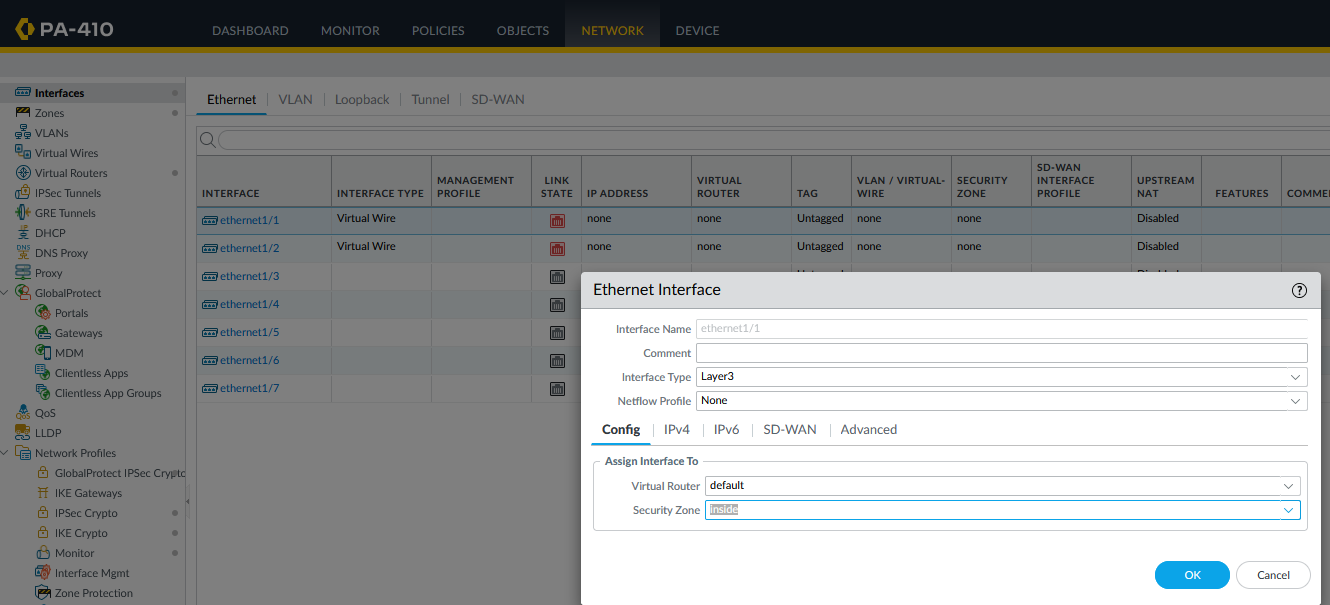
Create a new Layer3 Zone



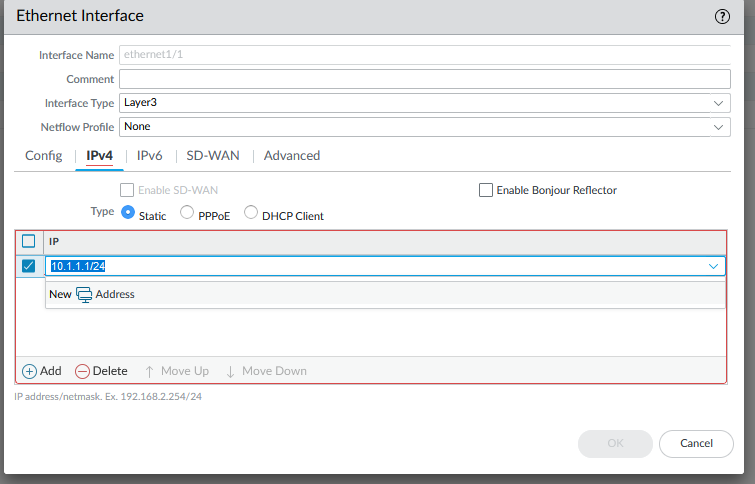
Name in outside



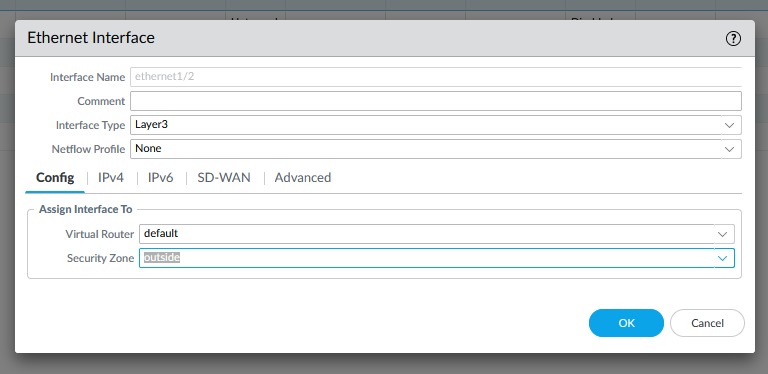
Configure the ethernet 1/1 interface



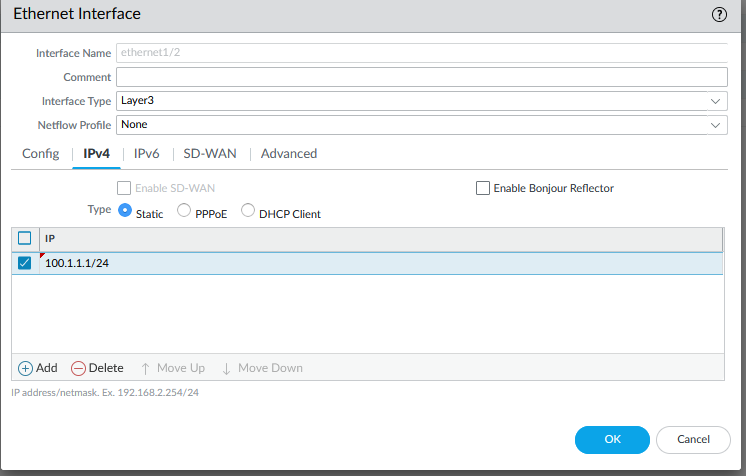
Make sure it is layer 3 and we also assigned an Ip address to the interface



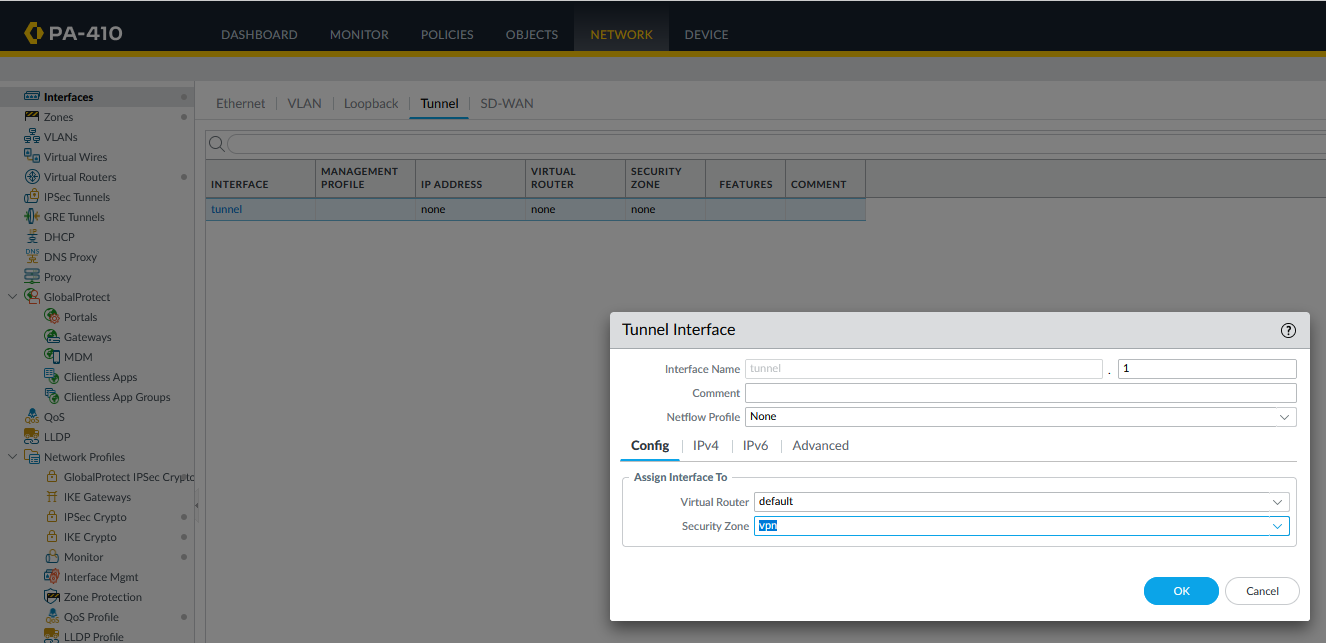
Next, configure the ethernet 1/2 interface



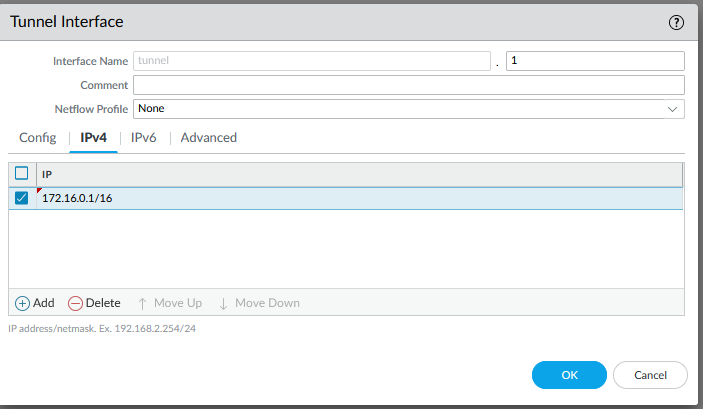
Give it an IP address for the inside subnet



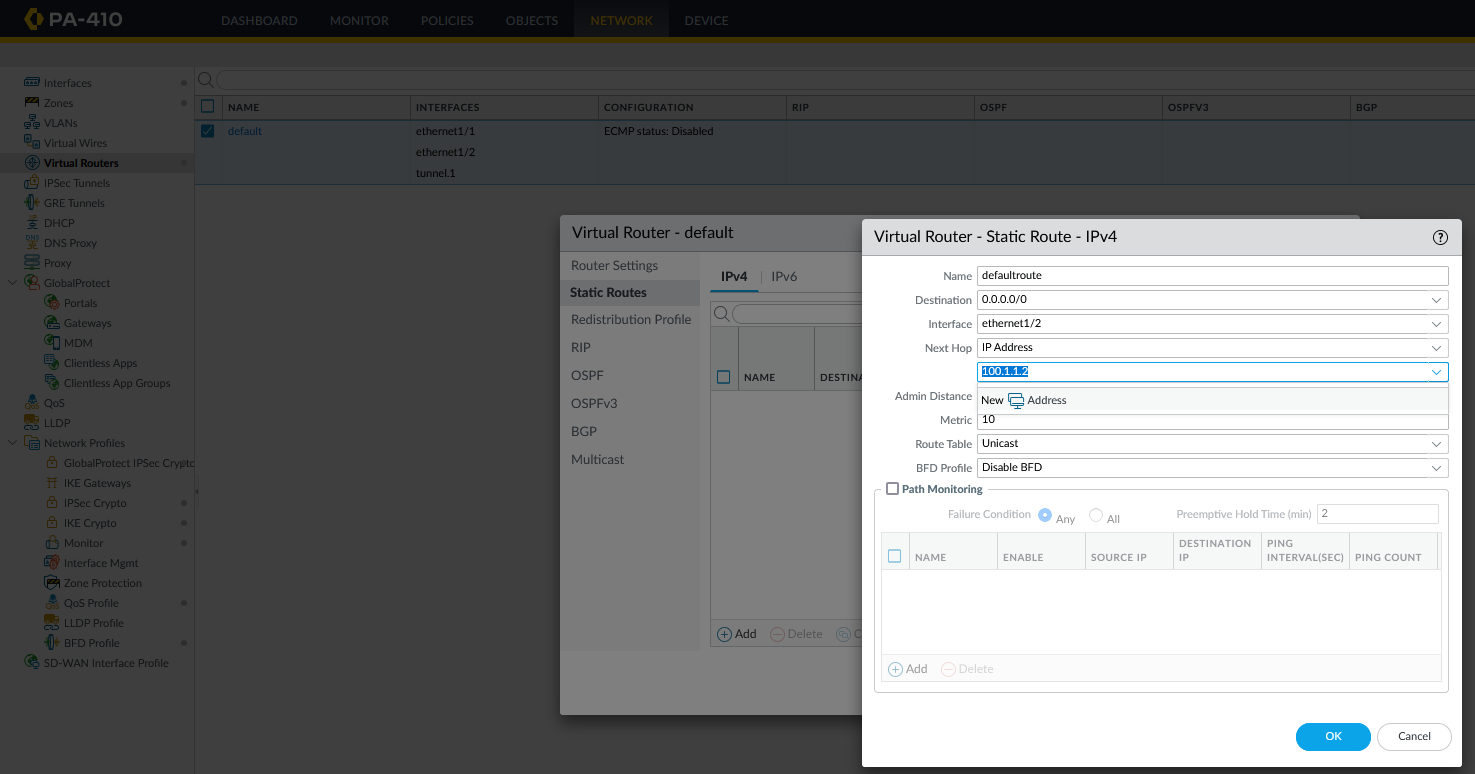
Create a tunnel interface and assigned it to the VPN security zone



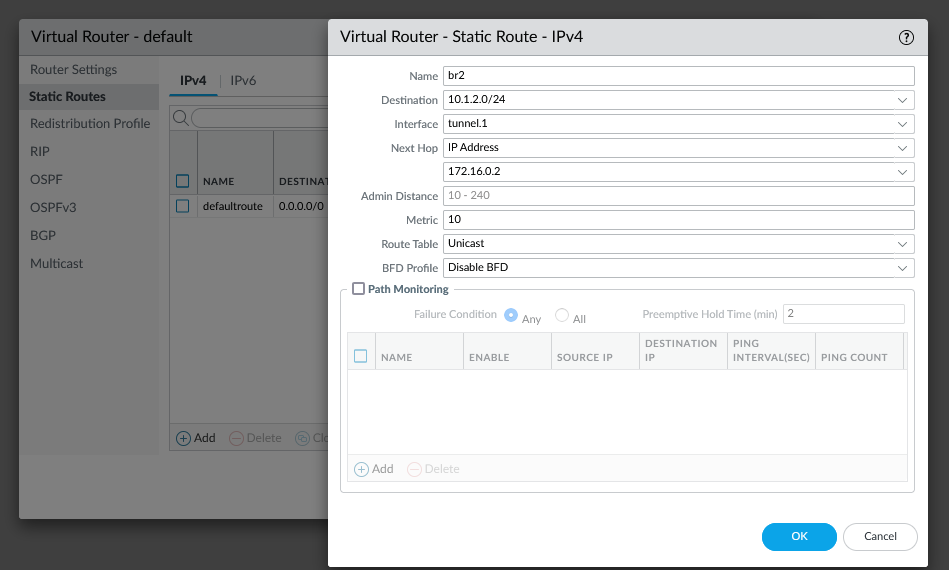
The tunnel itself also needs an IP address



Create a new static route on the virtual route that will be the default route

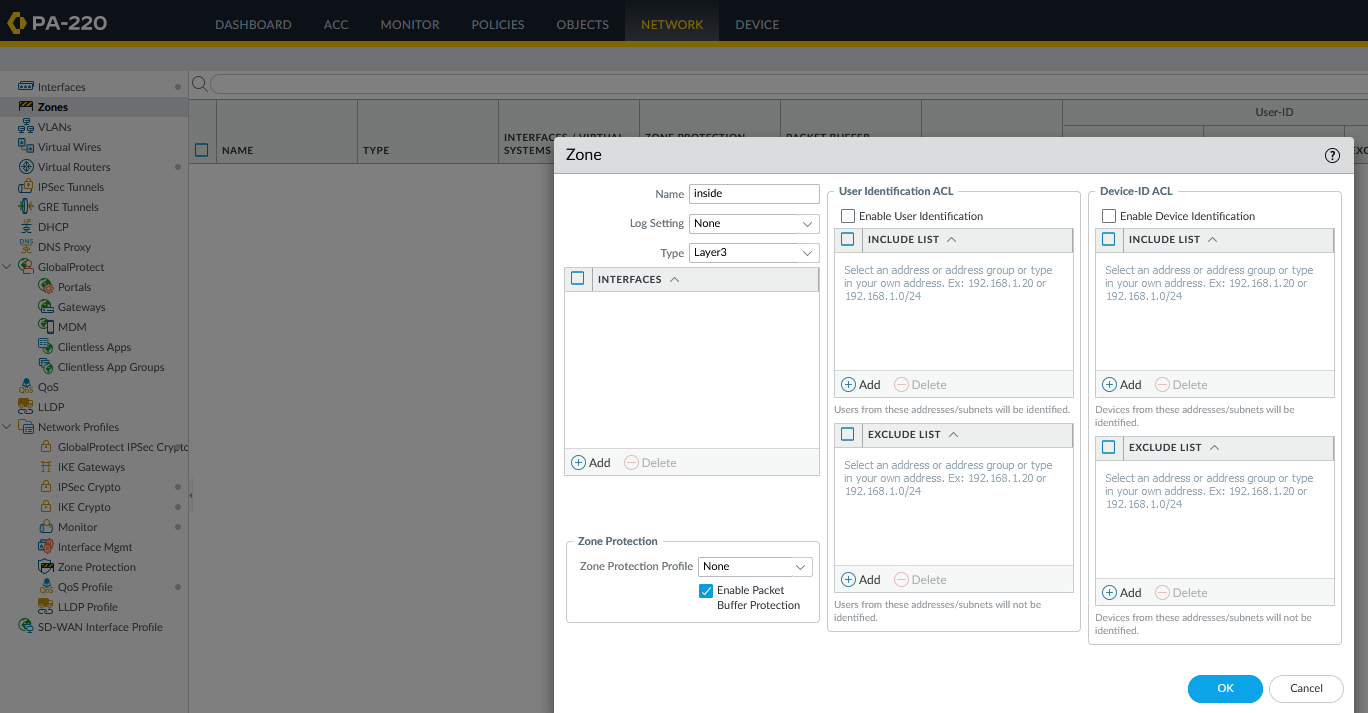


Create another static route that assigned to the tunnel interface

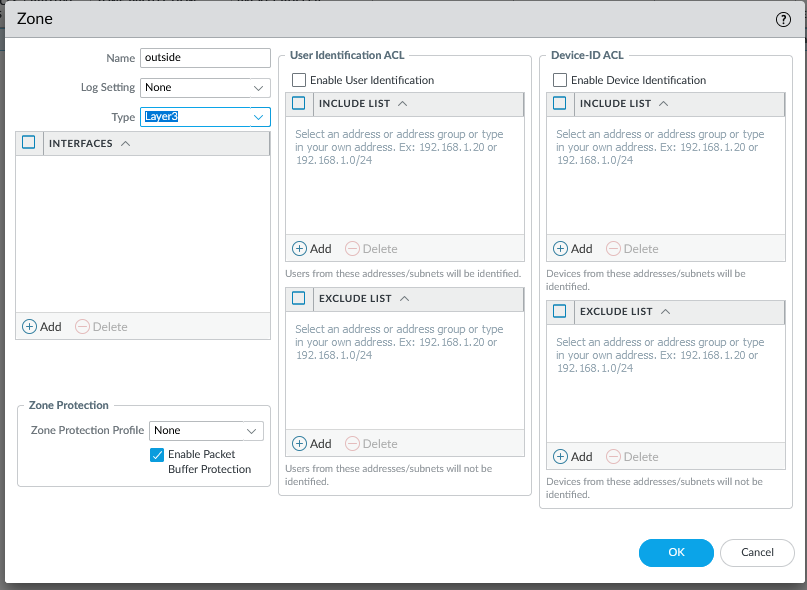


Switch to the PA-220 firewall

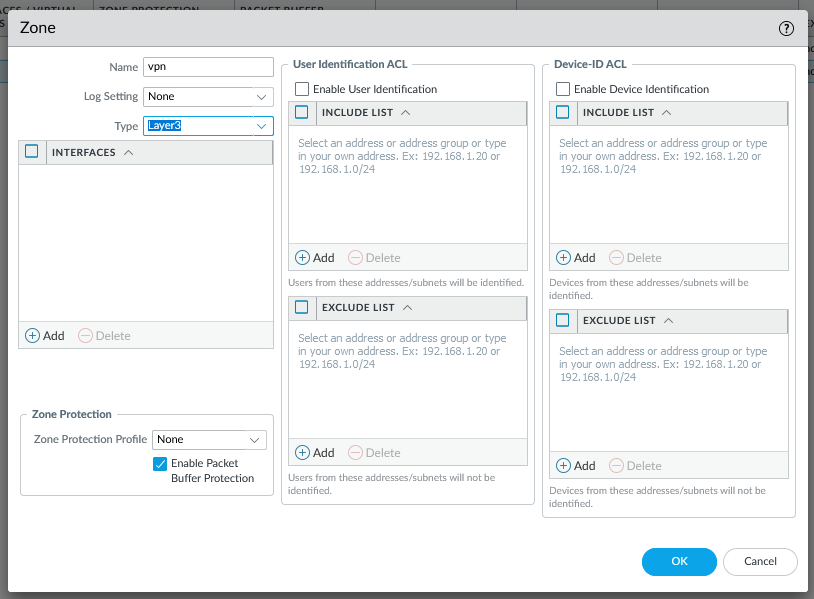
Create a new Layer 3 zone (inside)



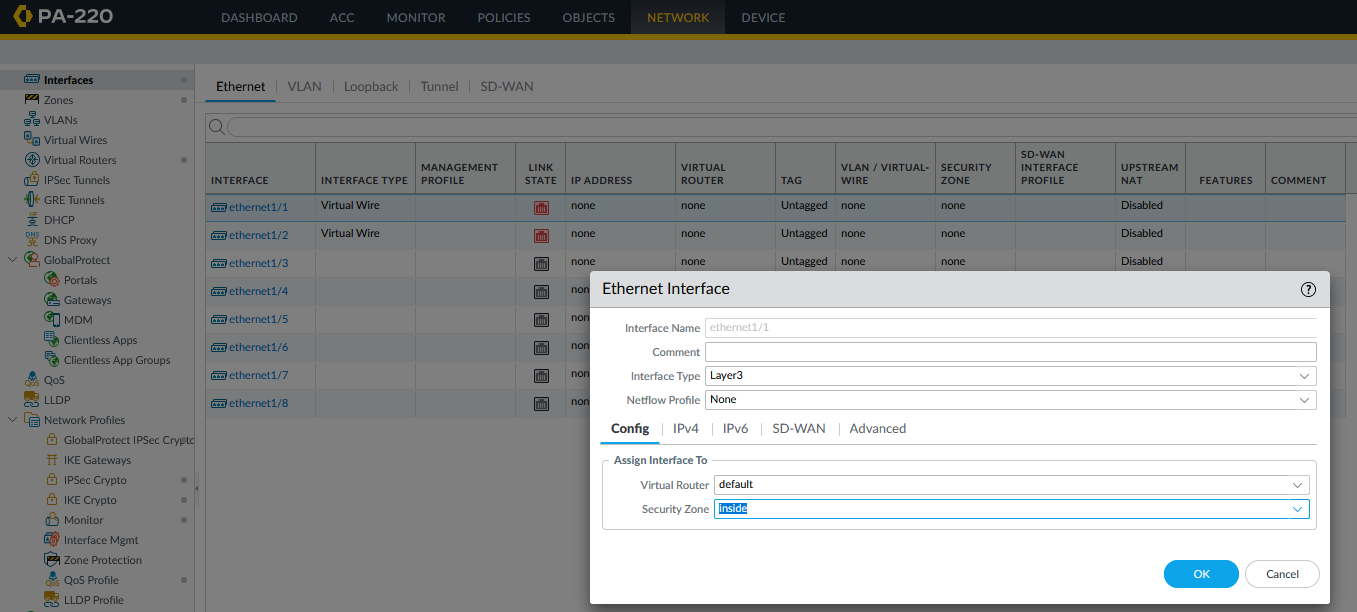
Create another new Layer3 zone (outside)



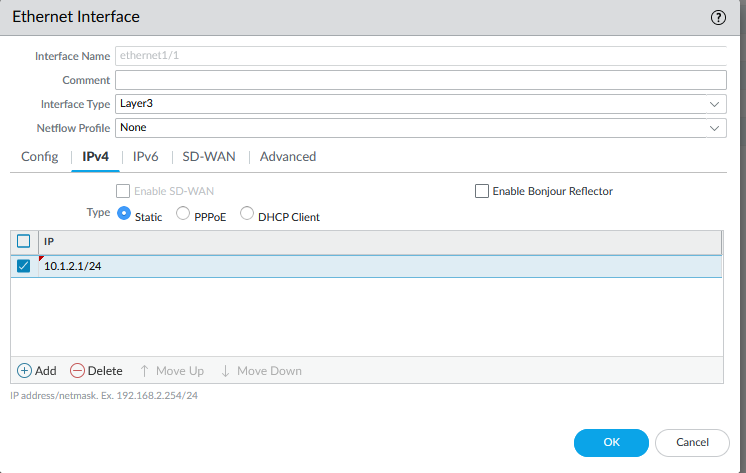
Also create the Layer3 VPN zone



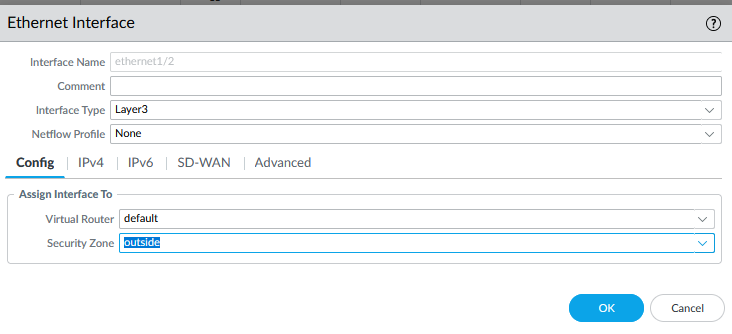
Configure the ethernet 1/1 interface to be in the inside zone



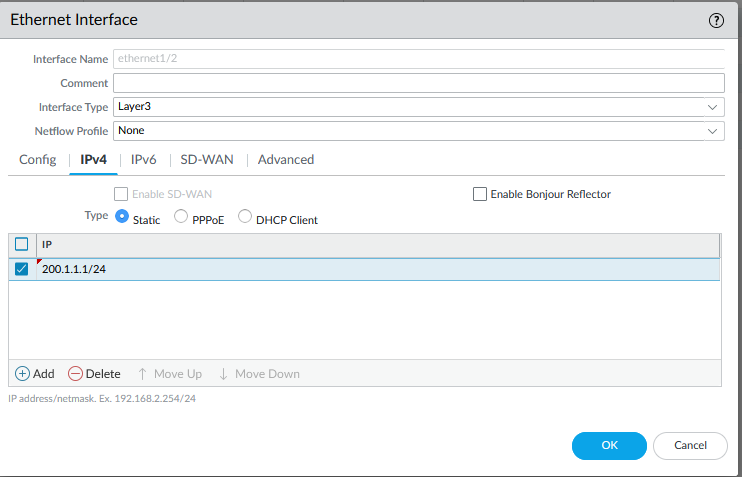
Also give it an IP address in the correct subnet group



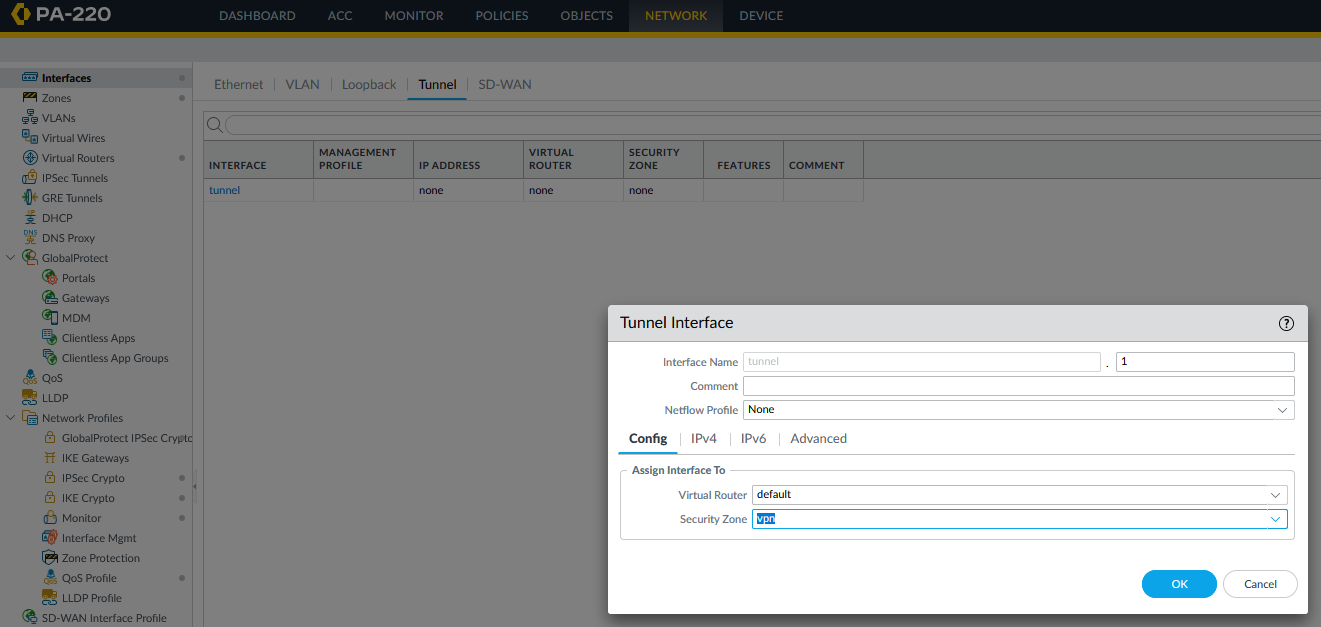
Configure the ethernet 1/2 interface to be part of the outside zone



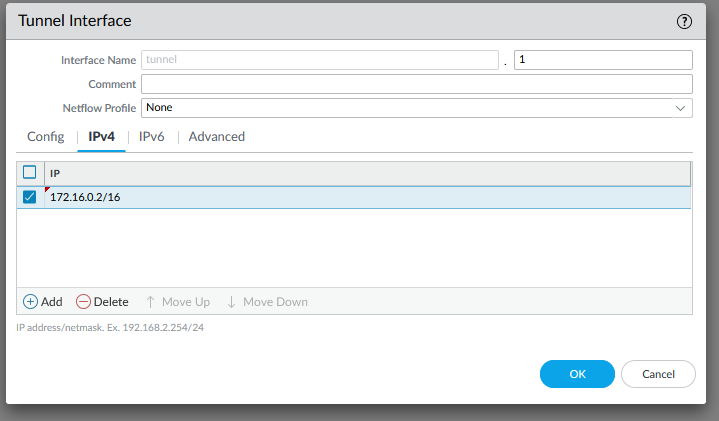
Also give it an IP address



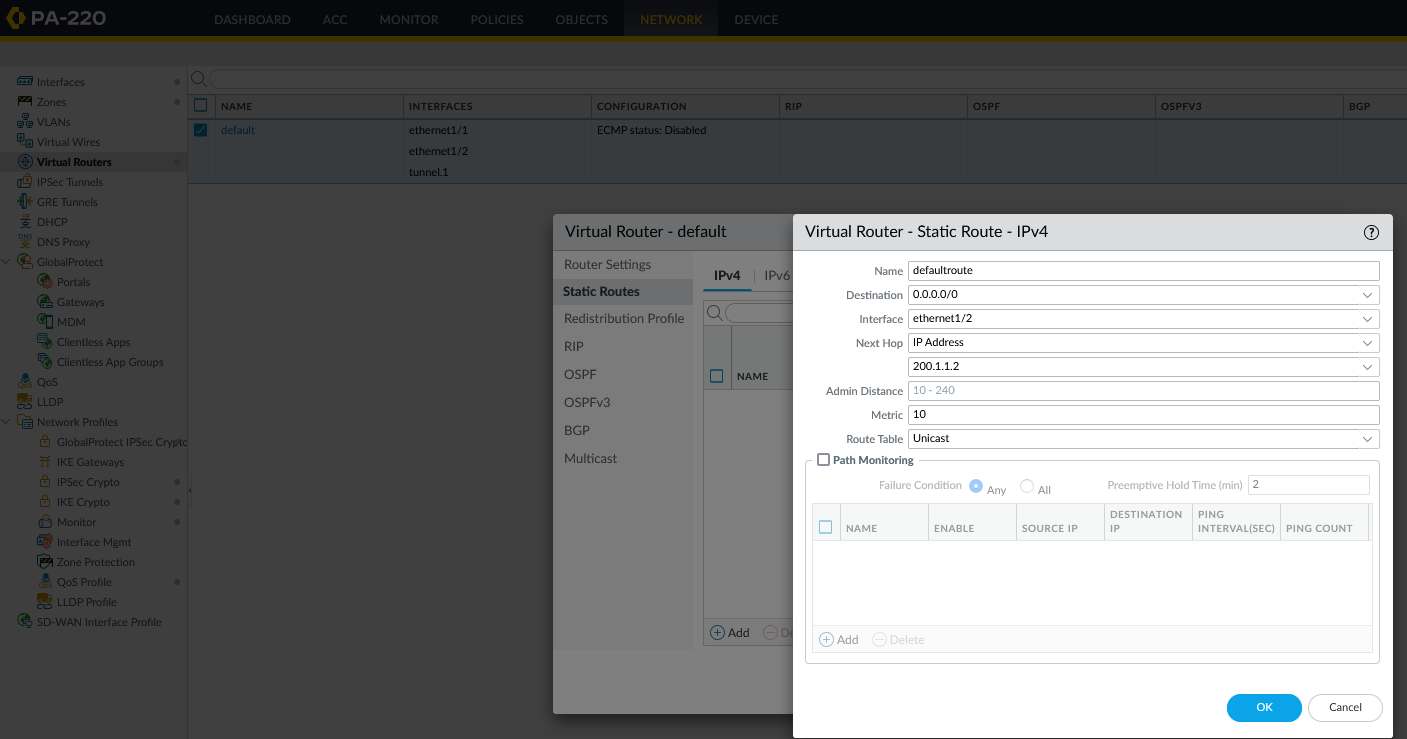
Next, create the tunnel interface and place it in the VPN zone



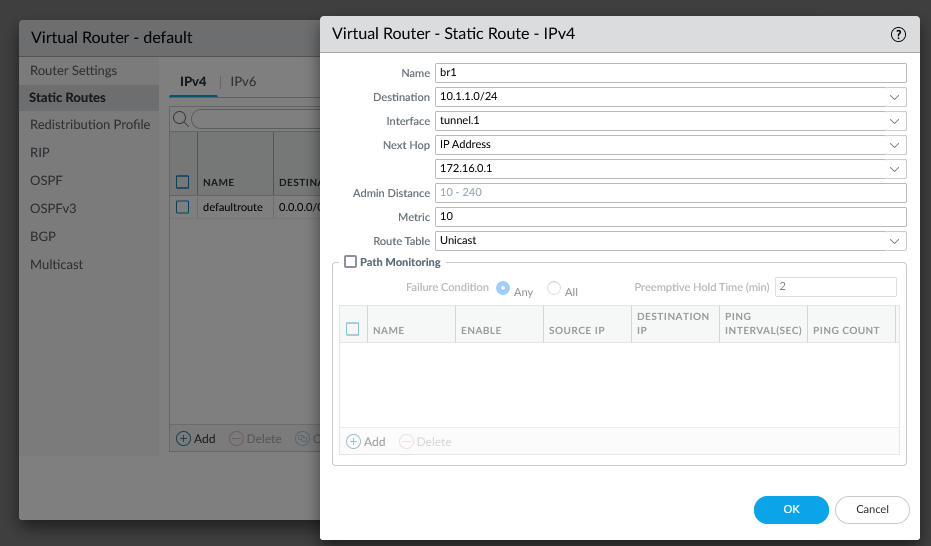
Give the tunnel interface an IP in the same subnet as the tunnel of the other firewall



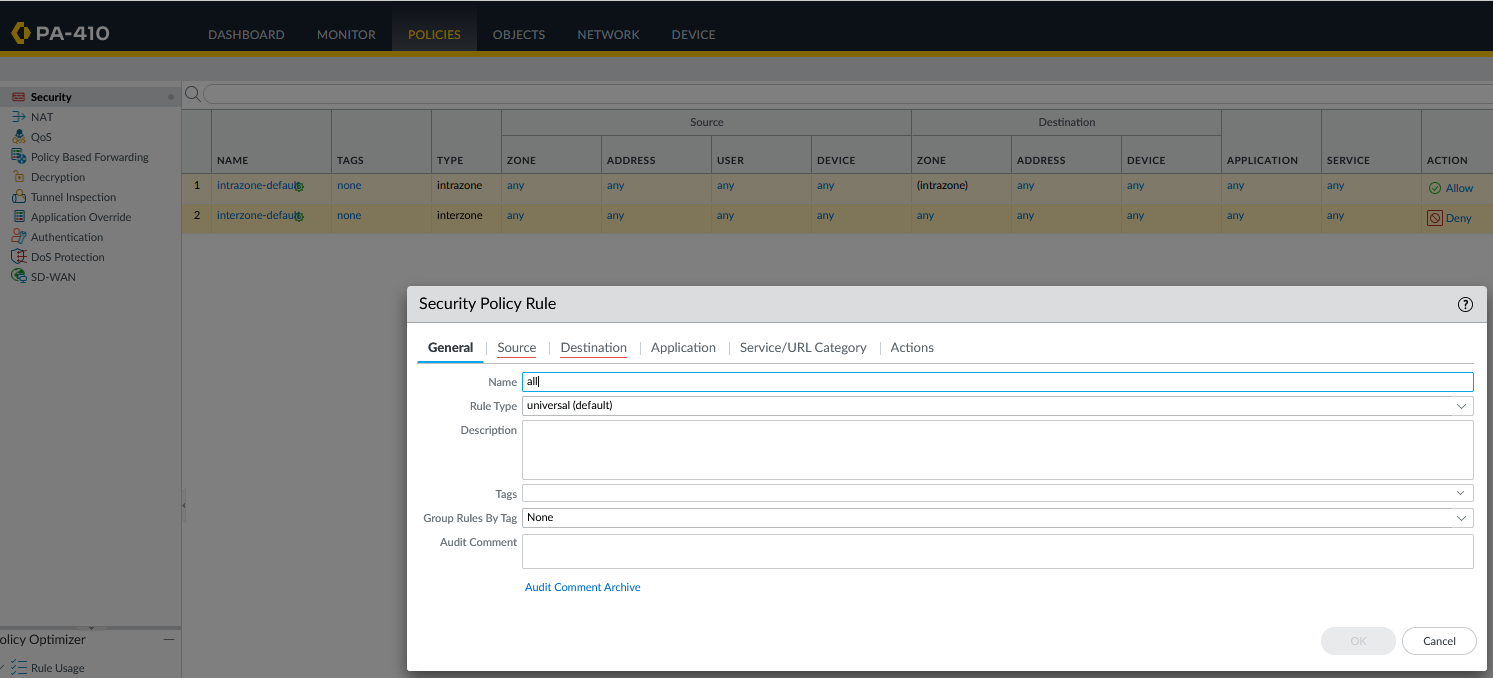
Create a default static route for the ethernet 1/2 interface

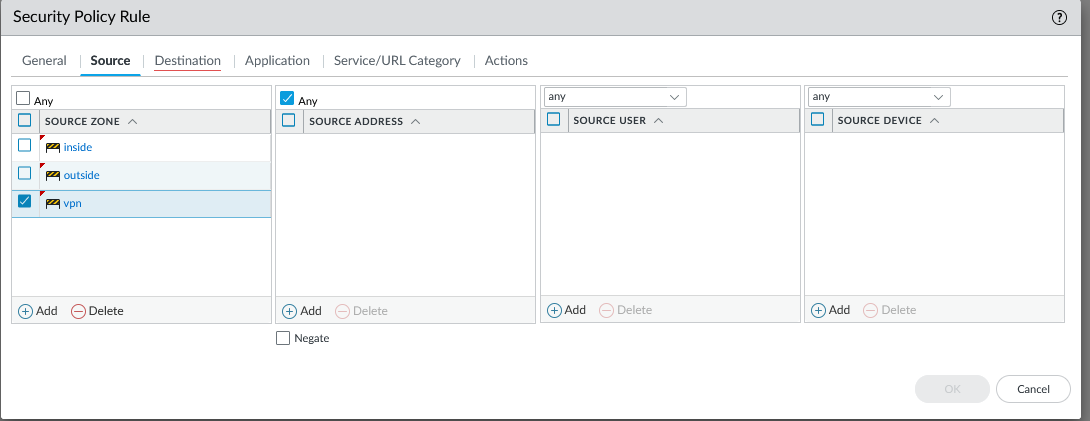


Create a new static route for the tunnel interface.

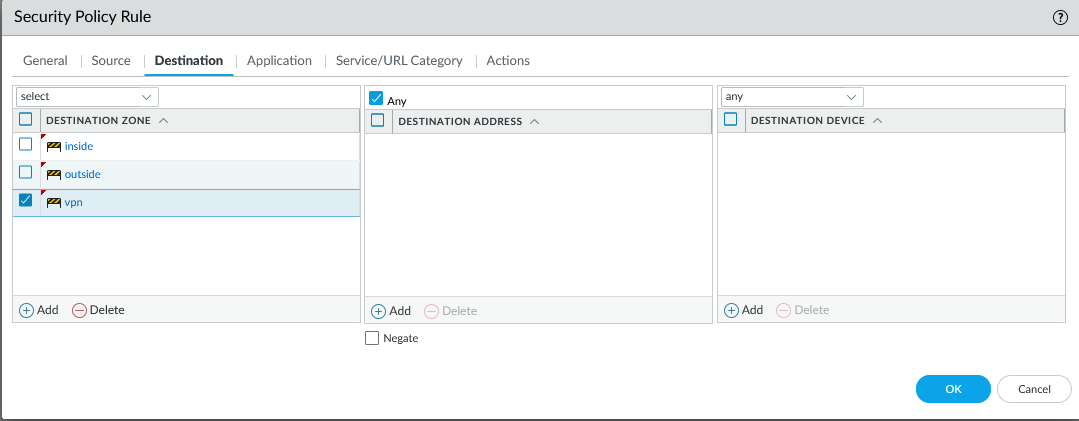


Now we need a Security Policy Rule

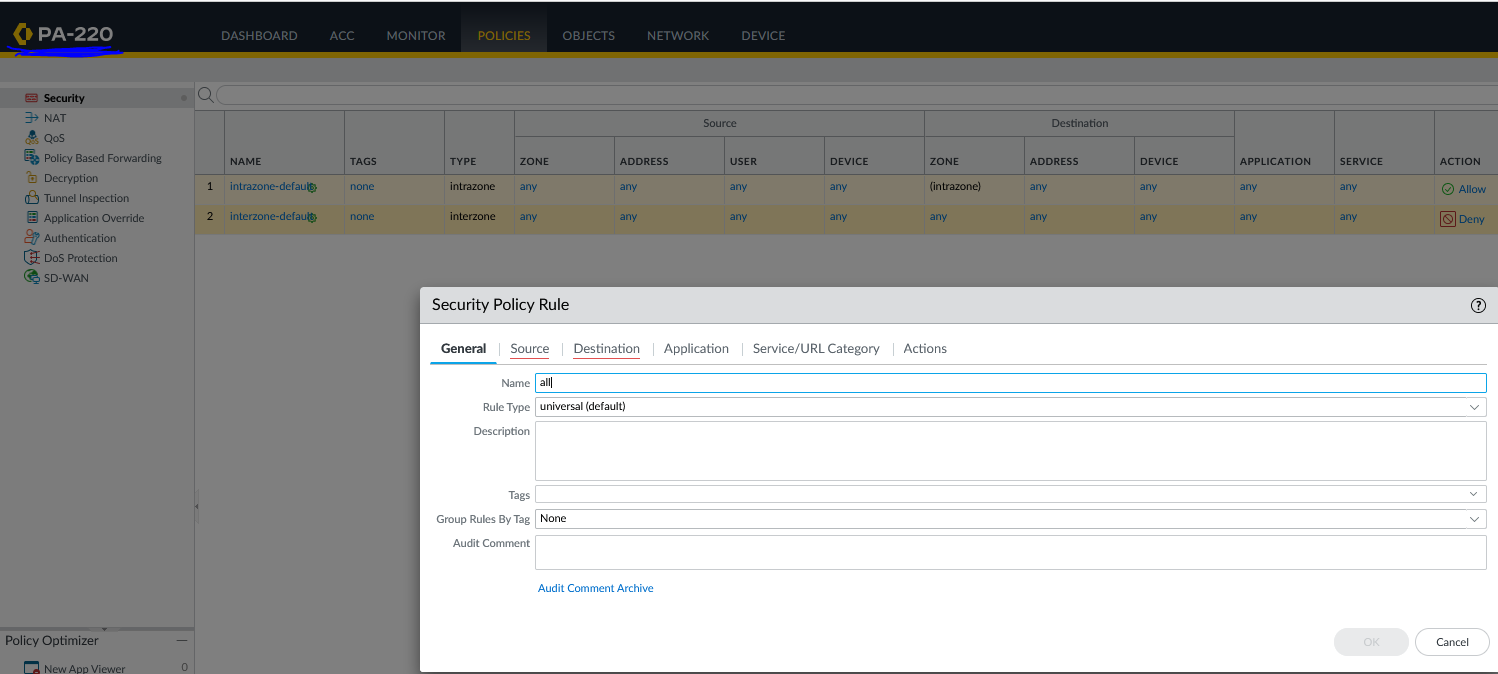


The source for this role will be from the VPN zone

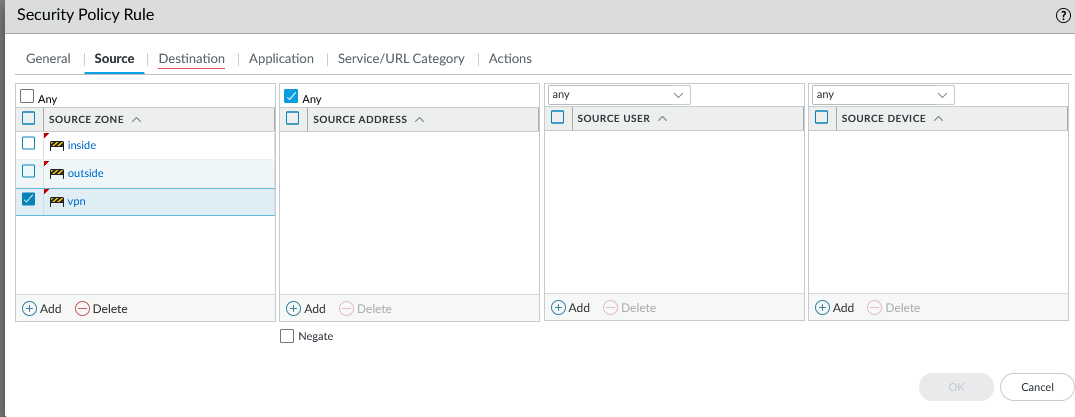
The Destination will also be the VPN zone



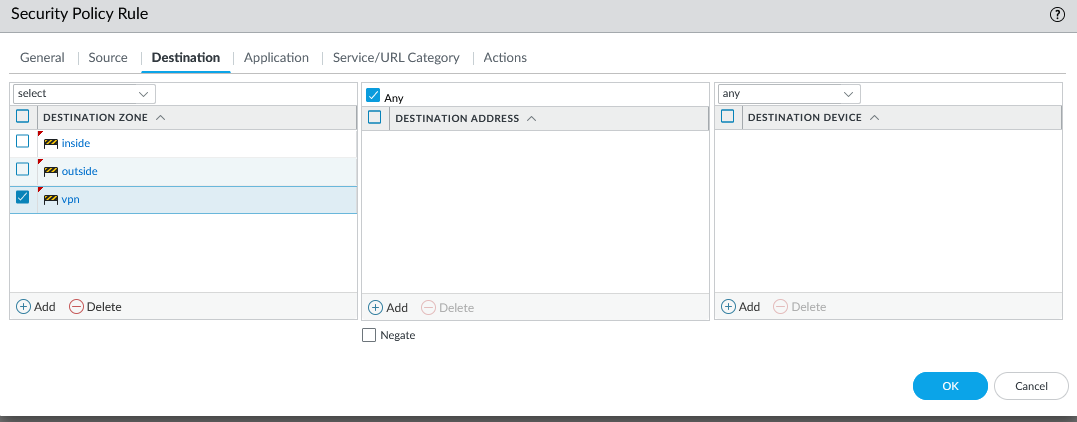
Switch to the PA-220 policy role



The source is set to VPN

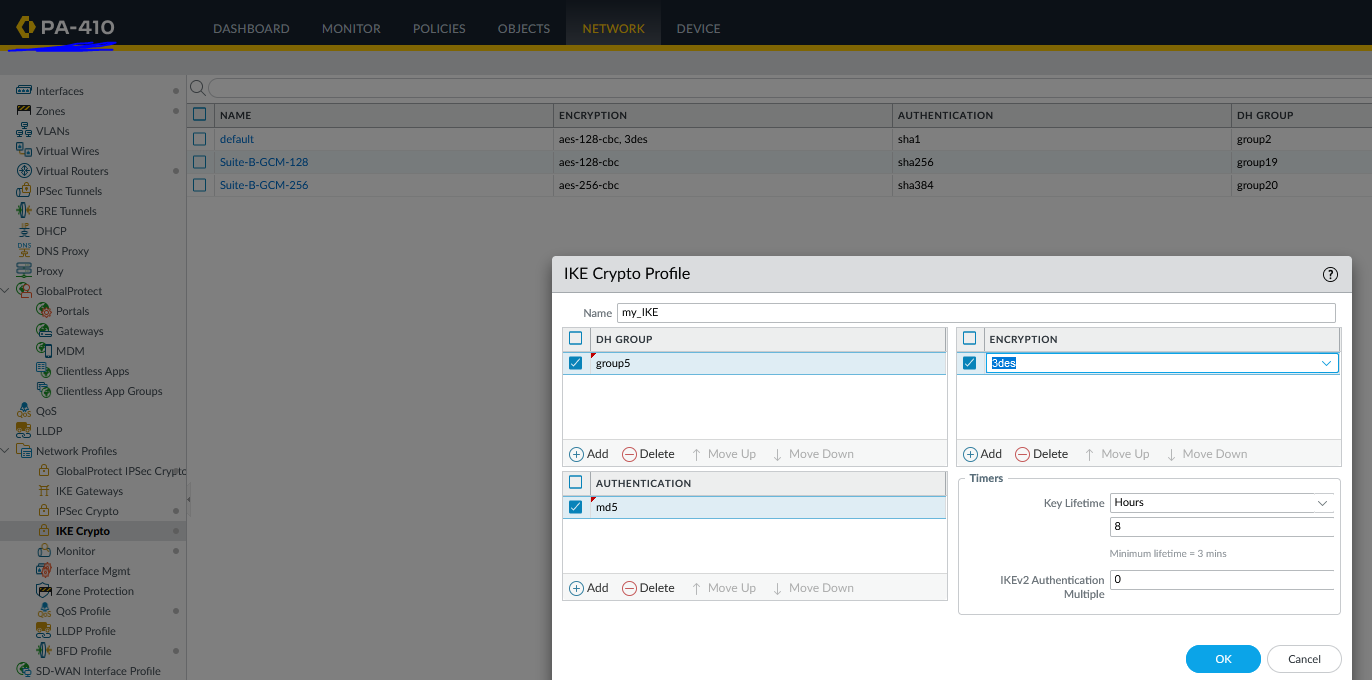


Destination also set to VPN

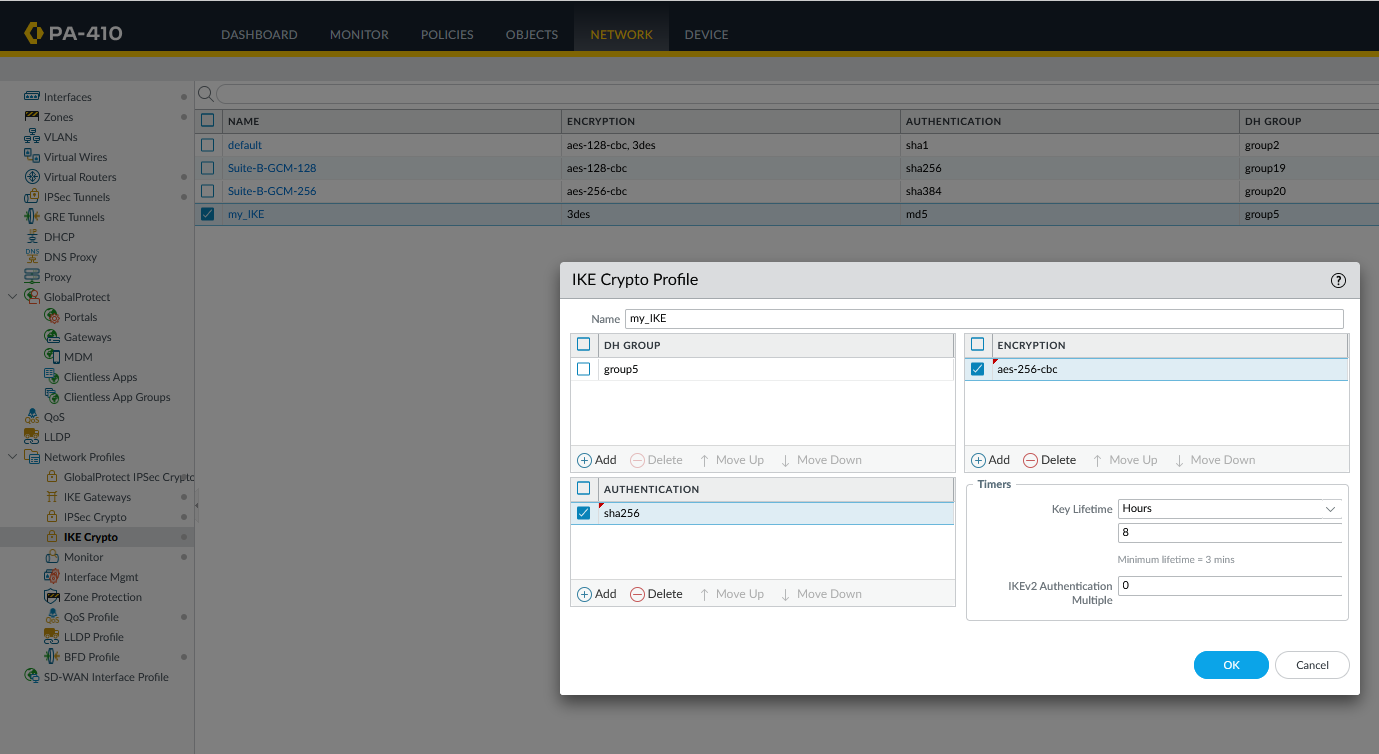


Go back to the PA-410 and create a new IKE Crypto Profile

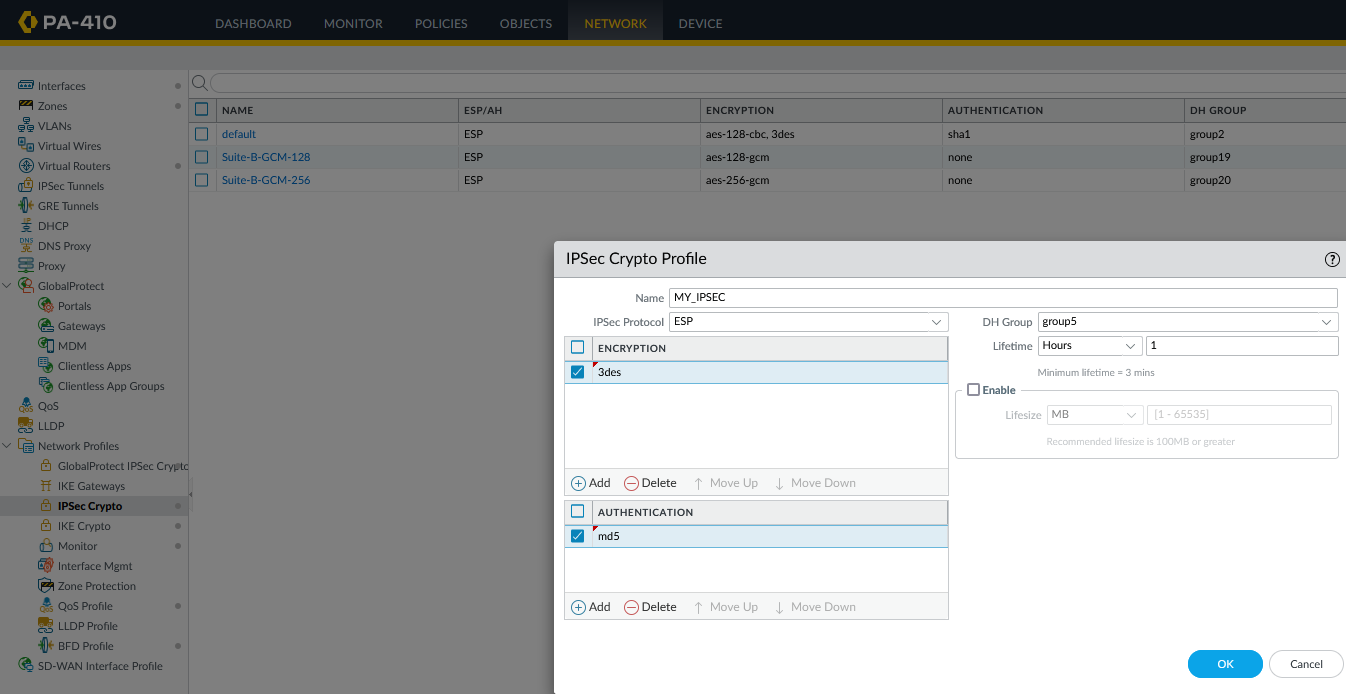
DH is group5



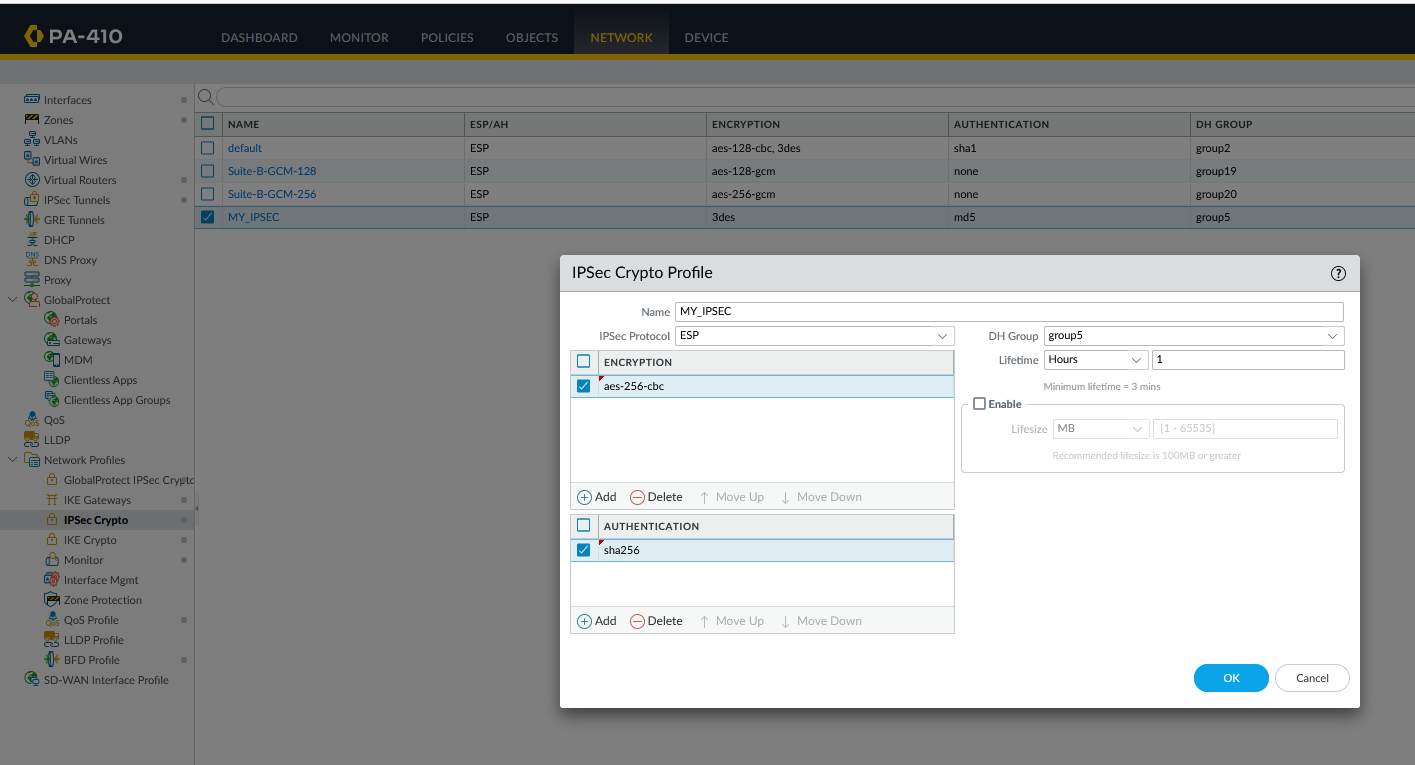
We changed the encryption to aes-256-cbc and the authentication to sha256



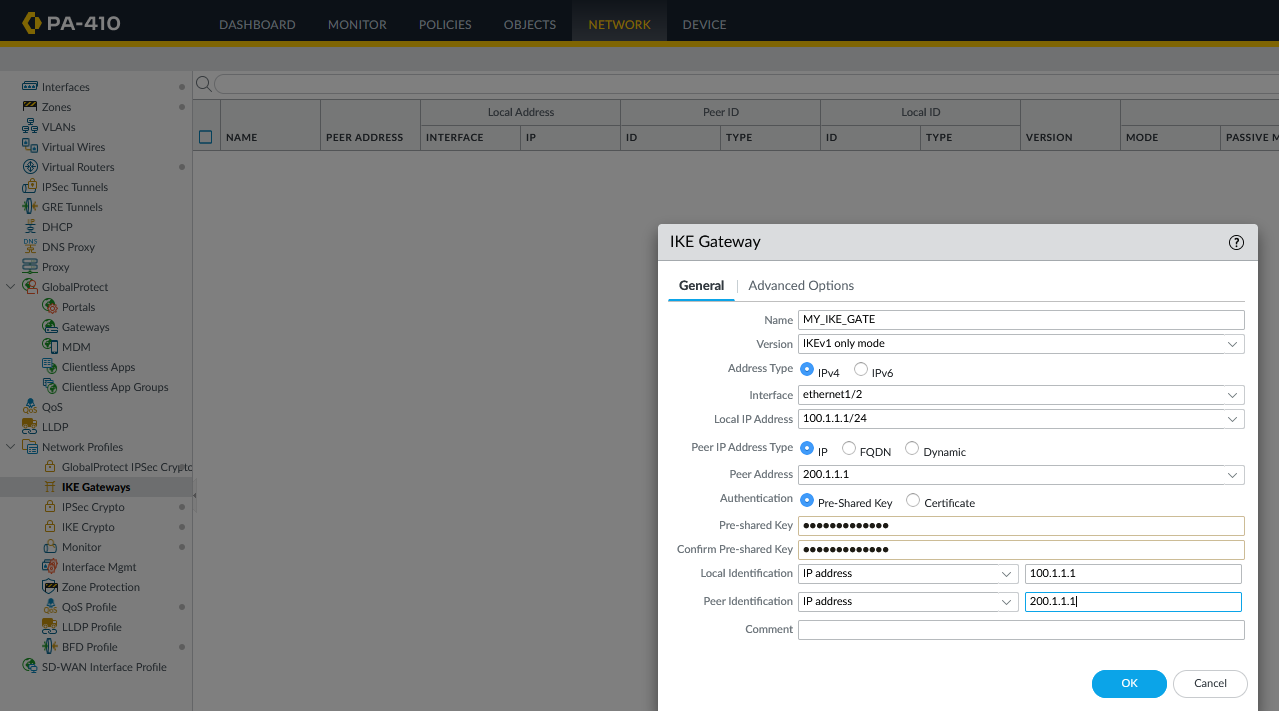
Create an IPsec Crypto Profile and set DH Group to Group5



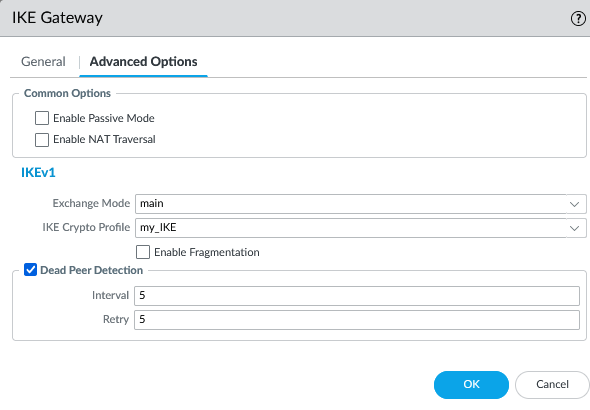
We changed the encryption to aes-256-cbc and the authentication to sha256



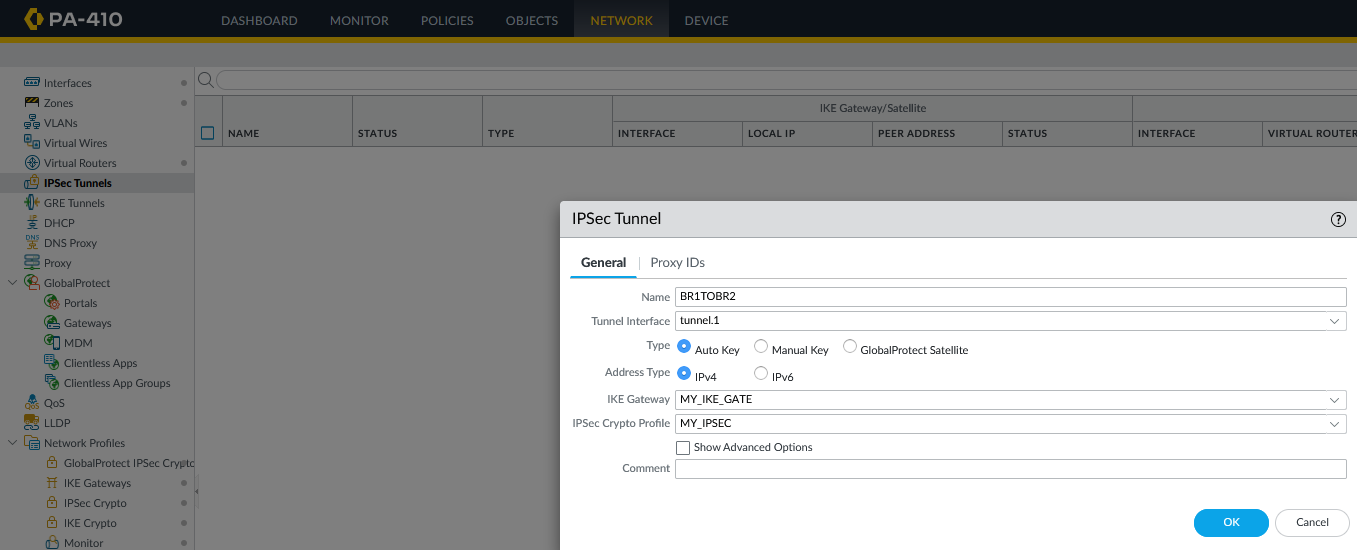
Finally we created an IKE Gateway in the 1/2 interface



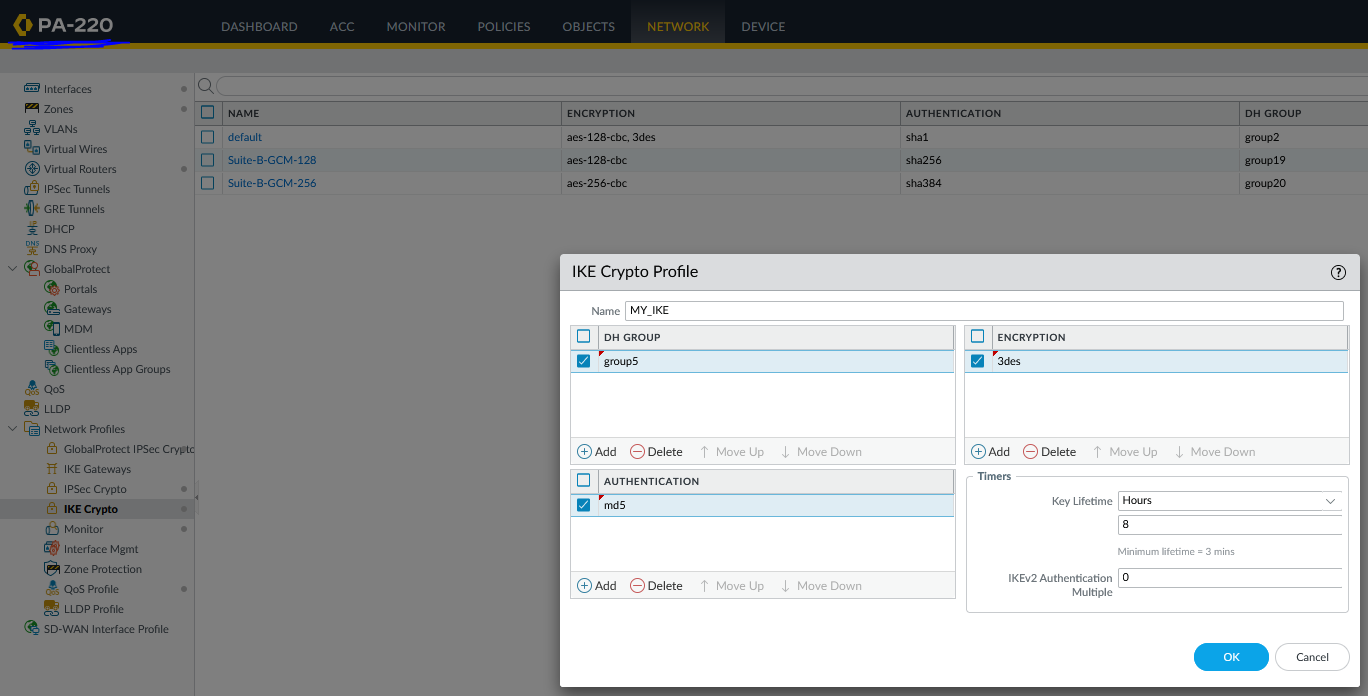
We set the IKE profile to the one we just created

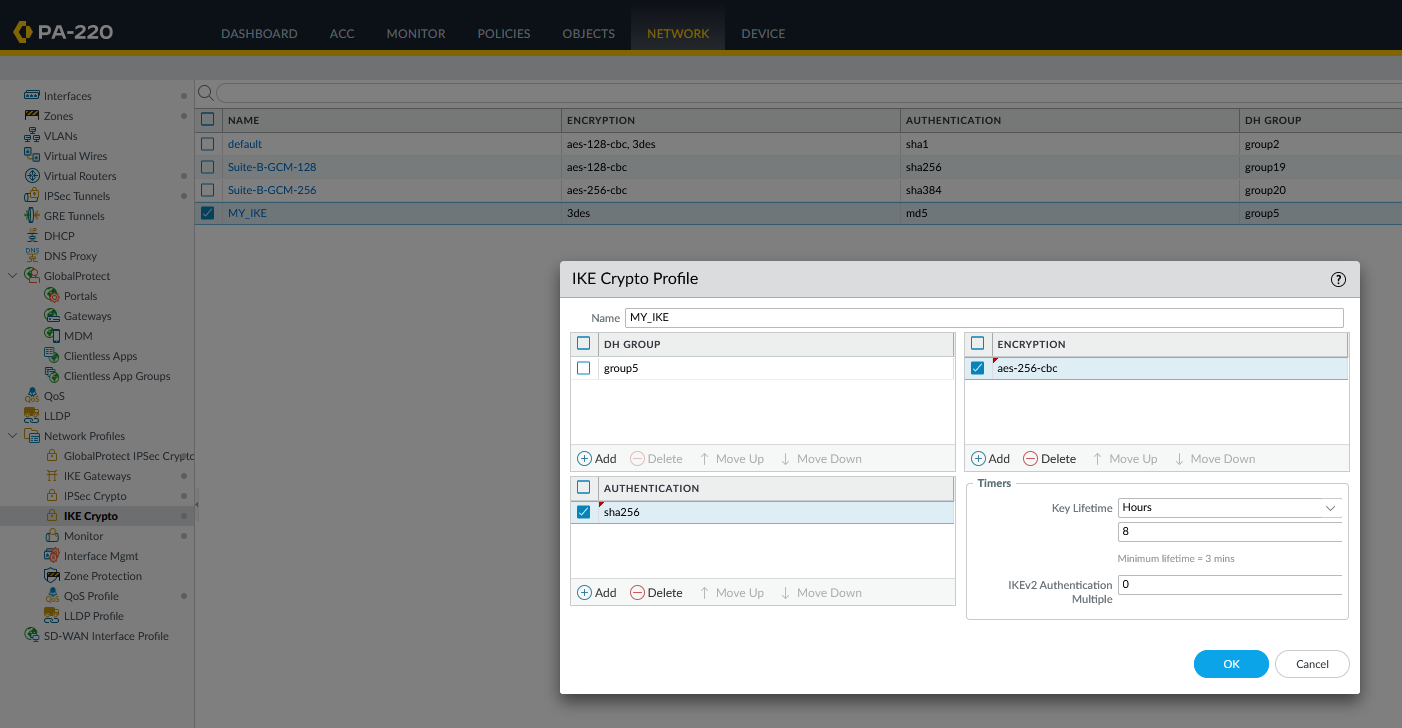


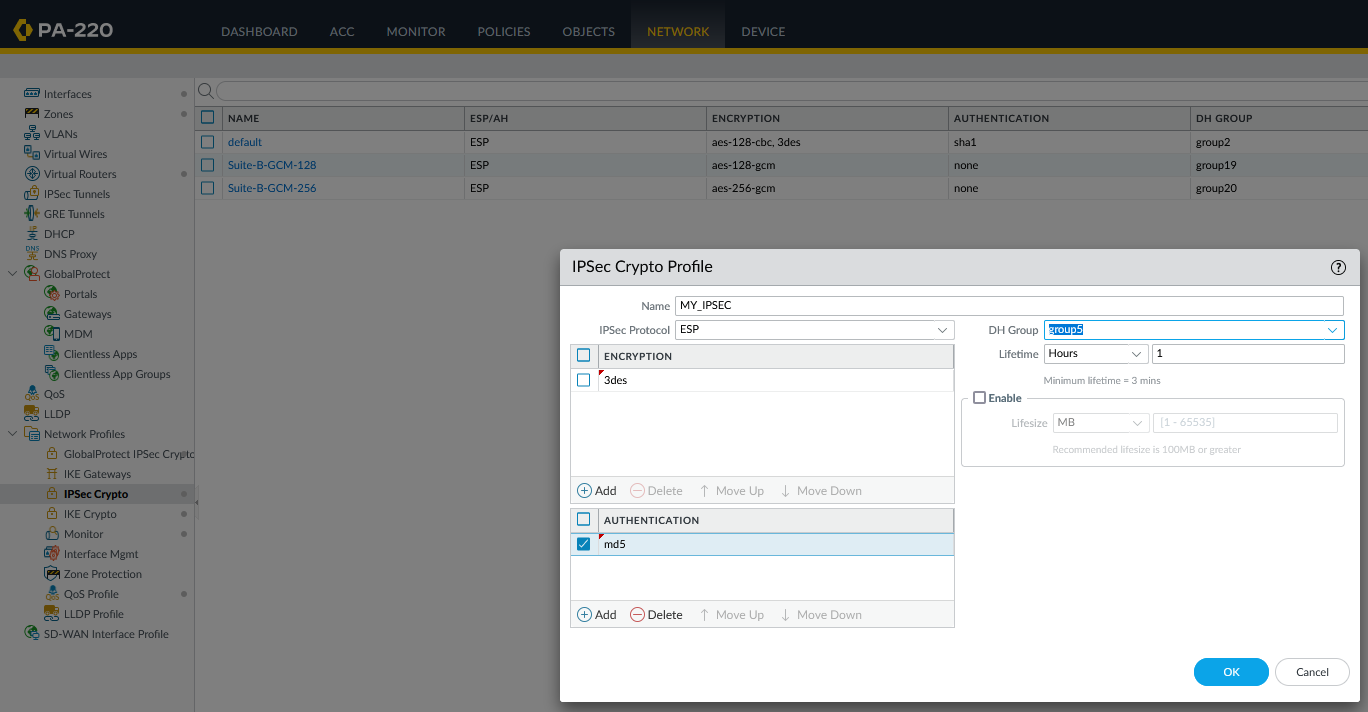
Me made a IPsec tunnel in out IKE Gateway using the IPSec profile we just made

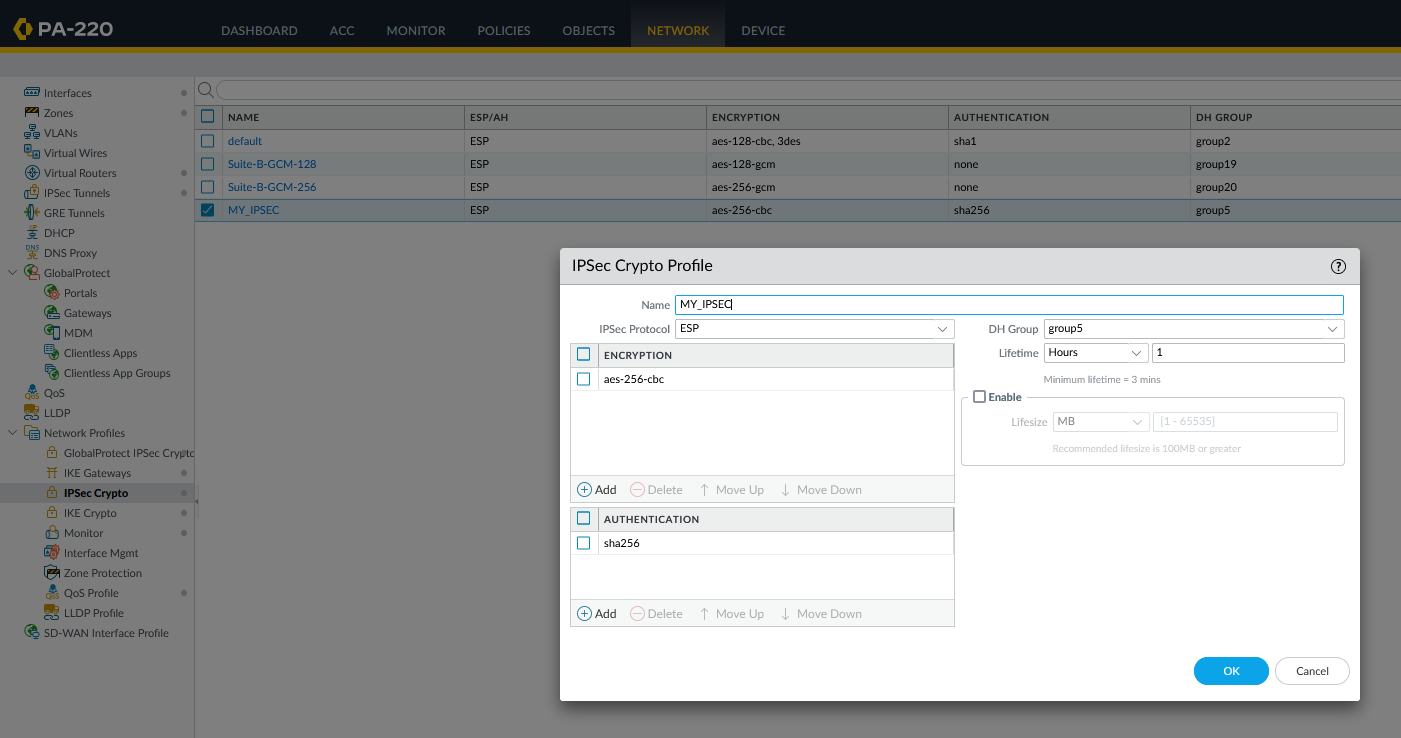


Switch to the PA-220 and create the profile with the same settings

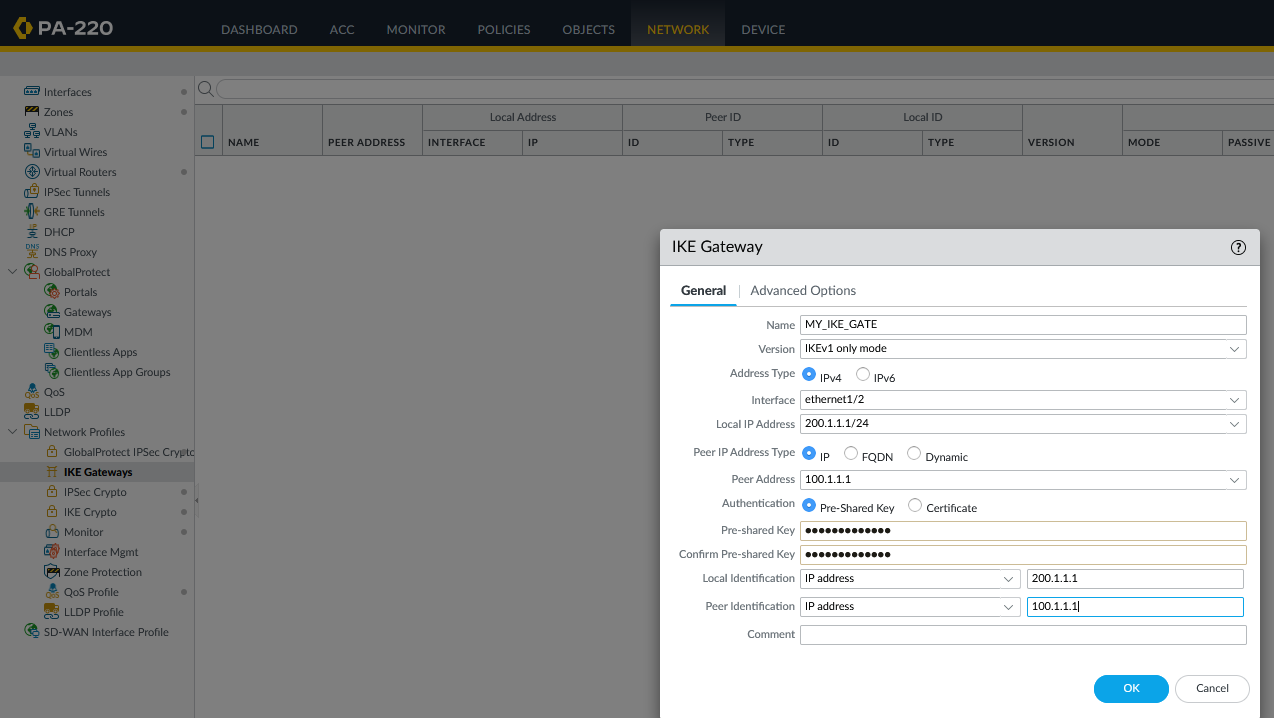




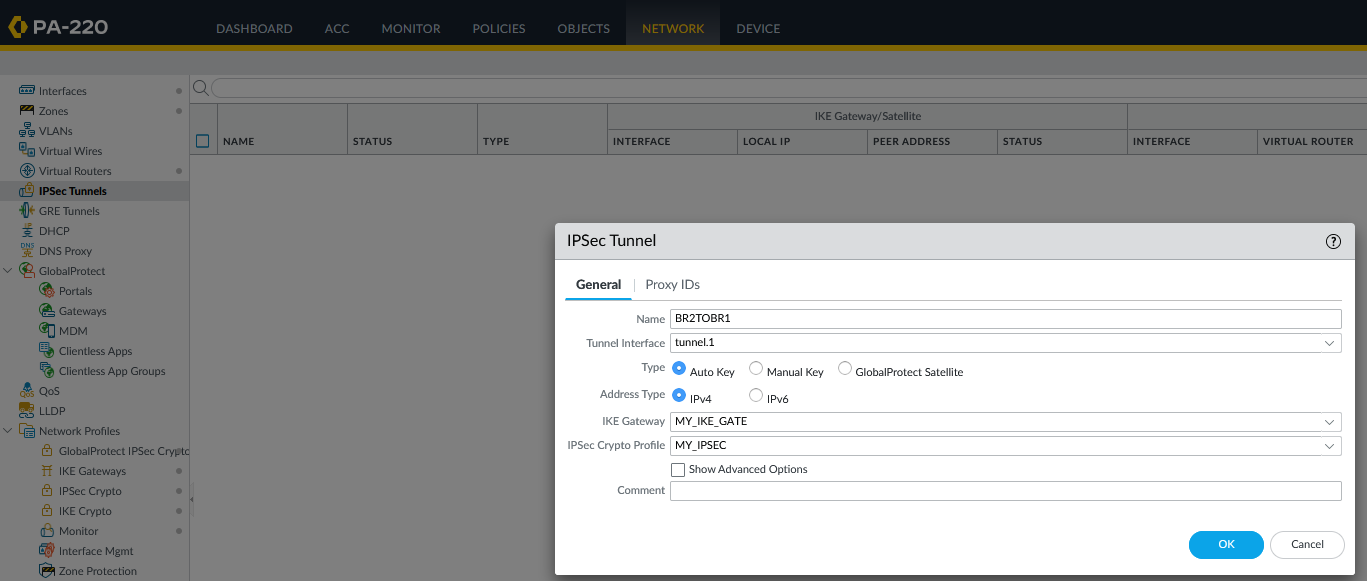




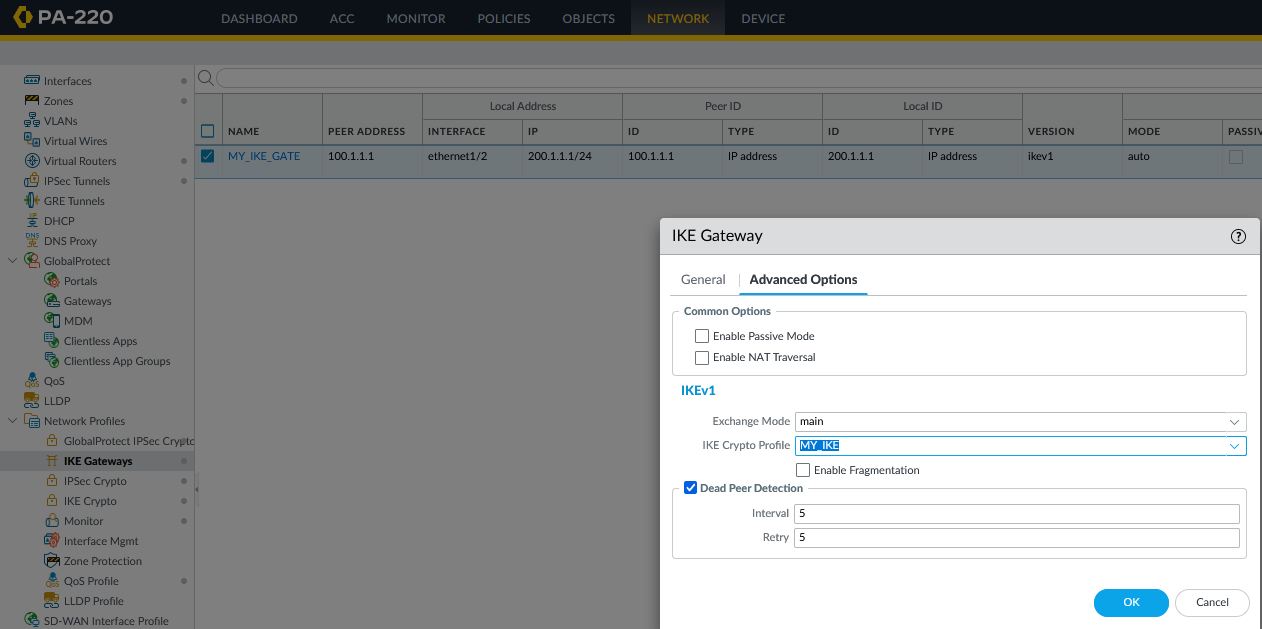
Create the same IKE Gateway on the PA-220



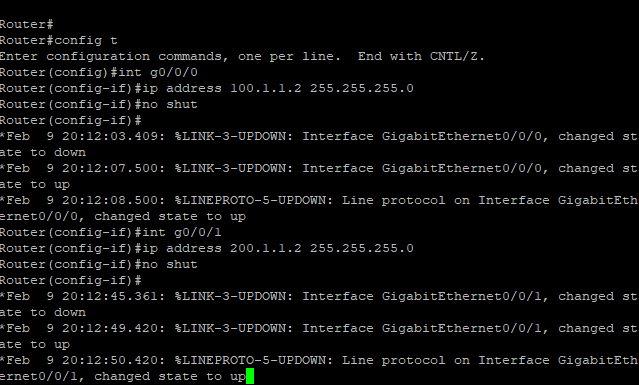
Make the Ipse Tunnel on the PA-220



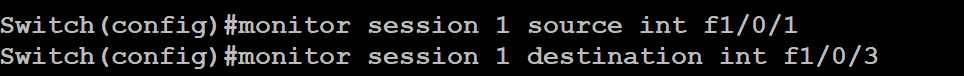
Add the profile to the IKE gateway



On the Router configure the interfaces g0/0/0 and g0/0/1 with IP addresses



On the switch use monitor commands to see traffic going through the tunnel



Problems: One of our major issues was that we did not make the passphrases match on both of our firewalls. That meant that even with correct configurations on everything else the tunnel would not work. After that easy fix that lab worked great.