

**PALO ALTO SITE TO SITE VPN SELF-SIGNED**

****Brendon Ahn | Cybersecurity | 2022-2023

**Purpose:**

Configure site-to-site VPN with self-signed certificates on two Palo-Altos

**Background:**

A site-to-site VPN (Virtual Private Network) has many advantages. They encrypt traffic that passes through it so private information can be protected. The protected information includes but is not limited to personal information like location. It prevents unwanted people with possible malintent from accessing information on your network.

The first commercial VPN was called Private Network access or PNA which was launched by Microsoft in 1995. They didn’t start to be widely implemented until 2000s. VPNs used to be used mostly by businesses but as they grew and privacy became more of a concern, everyday consumers started using VPNs and they have become a very popular industry. Some very common ones are like Nord VPN and in our own class its Proton. VPNs nowadays are used to watch a different countries Netflix or to play video games when they are blocked on the Cisco Network.

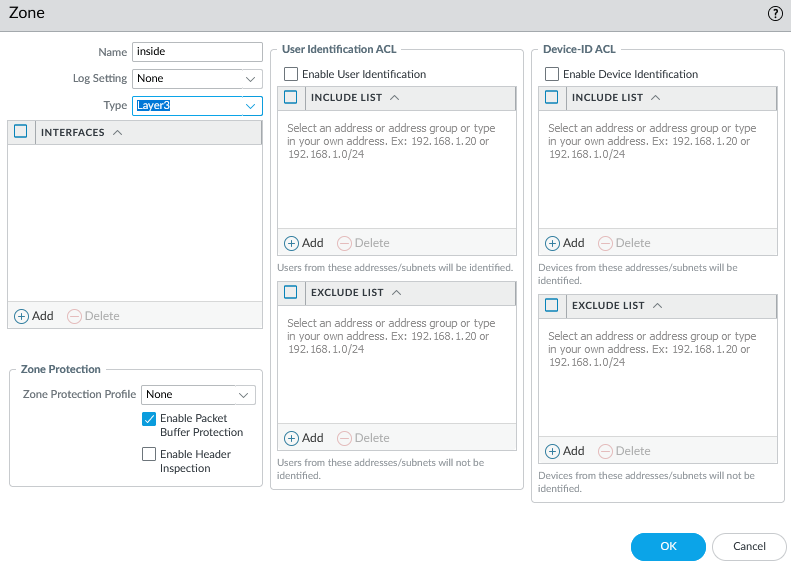
VPNs have many benefits. They are more cost effective then leased lines or MPLS because they use internet connections that are already present in a network. The job of managing a VPN typically falls to a network manager. The way we configure this site-to-site VPN is with self-signed certification and tunnels. The lab consisted of a PA-220 and a PA-410, both configurations being shown below. We were configuring using a pre-existing VPN connection that was configured for pre-shared key VPN. Benefits of self-signed certificates is that they don’t require the purchase of third-party certificates. You have more control over the process and are pretty quick to configure. A drawback is that they may not necessarily be as secure as using a third party. They may be more susceptible to attacks like man-in-the-middle attacks since the certificates are not trusted by defaults.

**Lab Summary:**

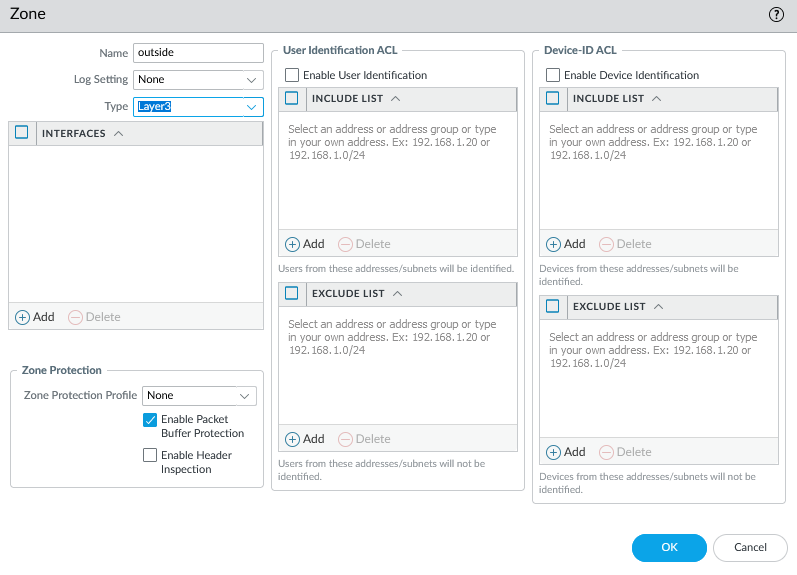
We had to learn how to configure self-signed certificates and IKE-gateways onto our already configured Palo Altos for site-to-site VPN. We did so using YouTube videos and the lab went relatively quick.

**Lab Procedure:**

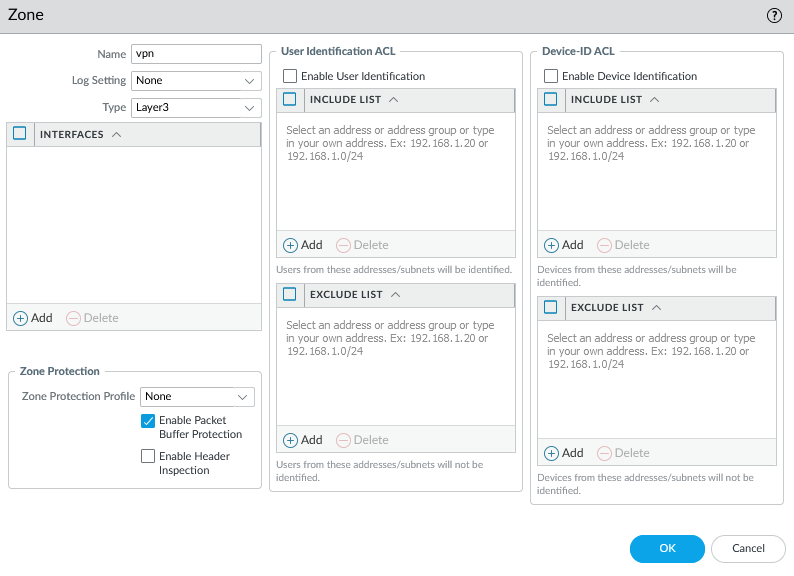
1. Go to Zones and click add.
2. Name the zone “inside” and change type to “Layer 3”



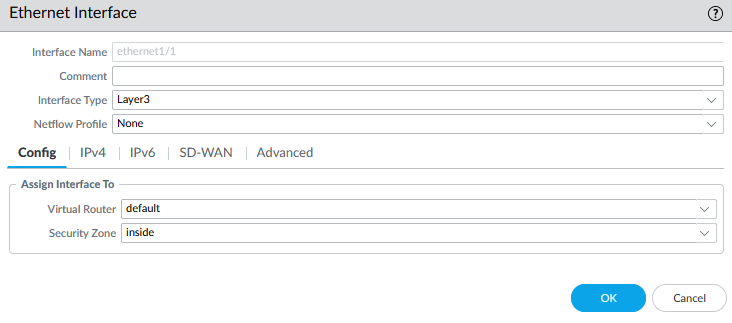
1. Add another zone, name the zone “outside” and change type to “Layer 3”



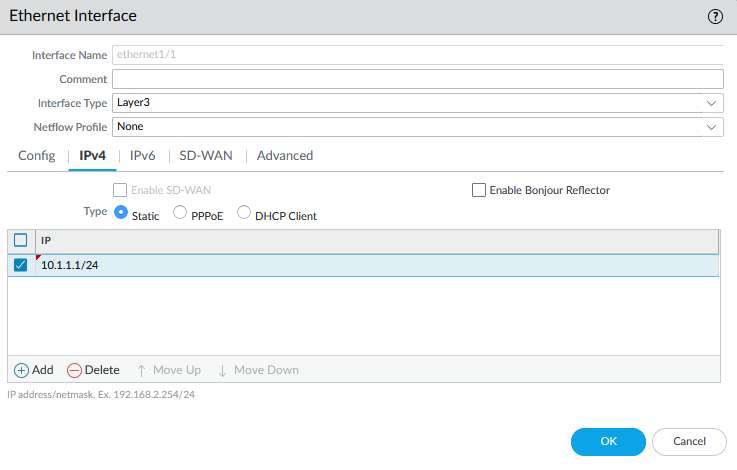
1. Add another zone, name the zone “vpn” and change type to “Layer 3”



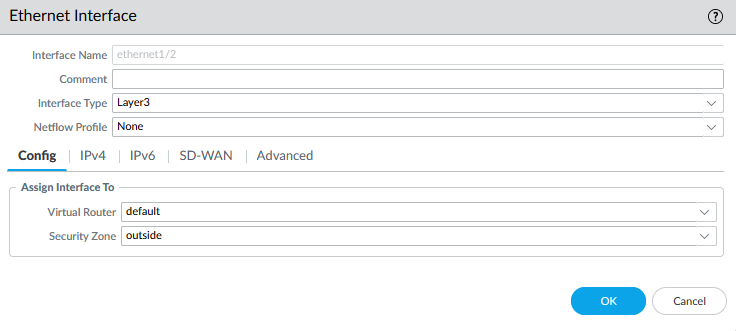
1. Configure the ethernet interface “ethernet1/1” as shown:



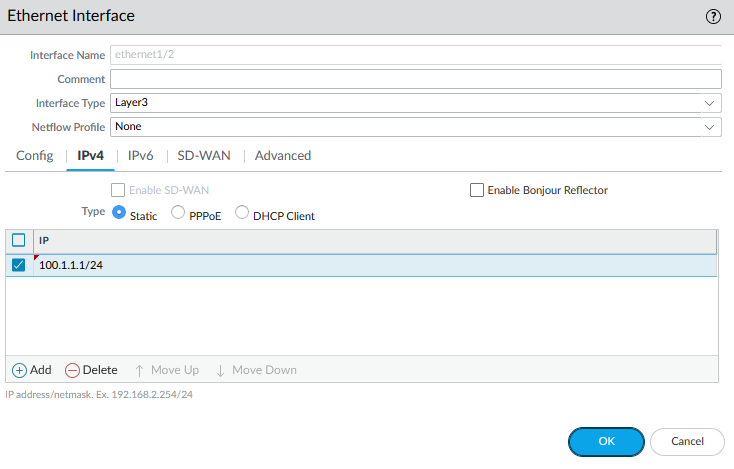
1. Configure the ethernet interface “ethernet1/1” as shown:



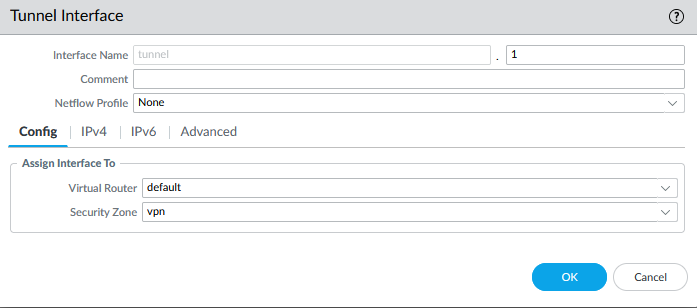
1. Configure the ethernet interface “ethernet1/2” as shown:



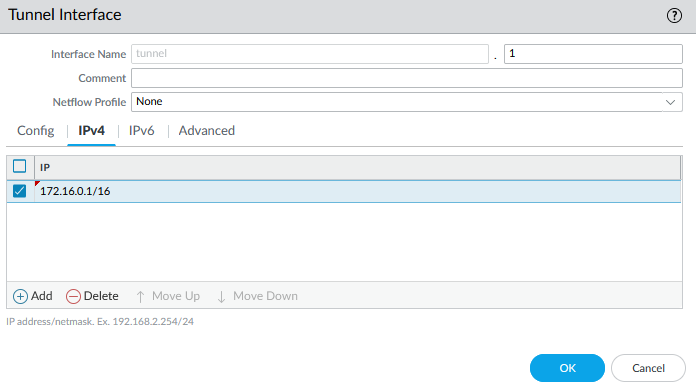
1. Configure the ethernet interface “ethernet1/2” as shown:

****

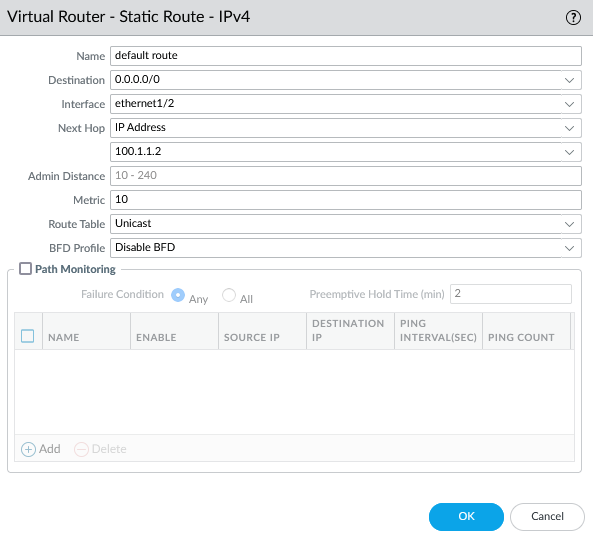
1. Configure the tunnel interface “tunnel” as shown:



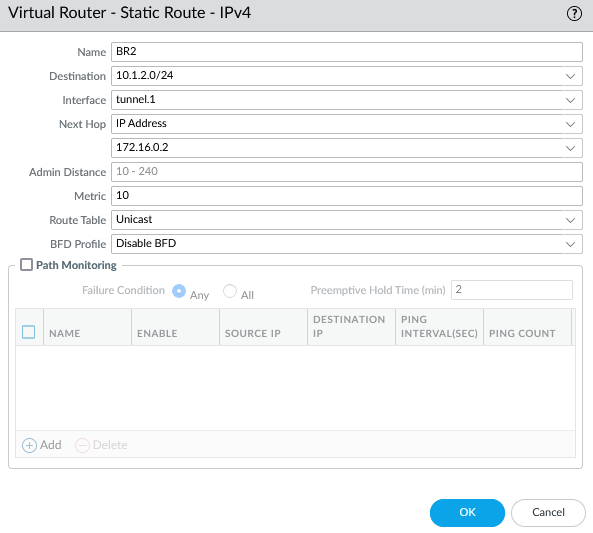
1. Configure the tunnel interface “tunnel” as shown:



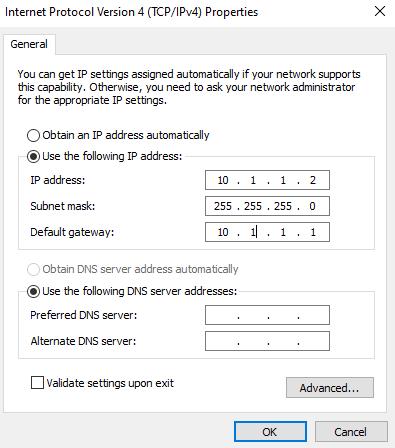
1. Add a default static route and configure as shown:



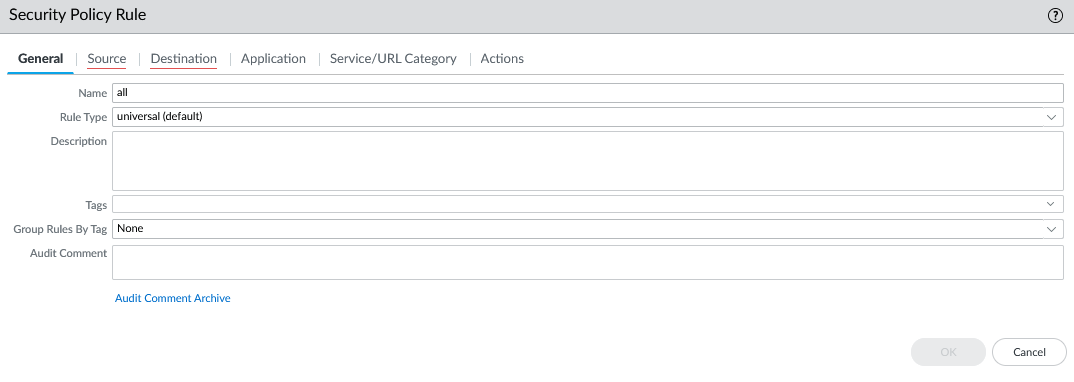
1. Add a static route and configure as shown:

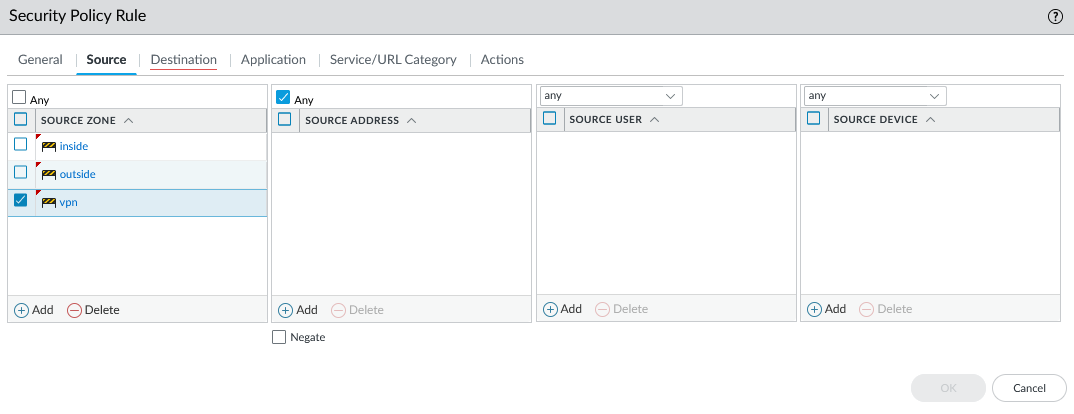


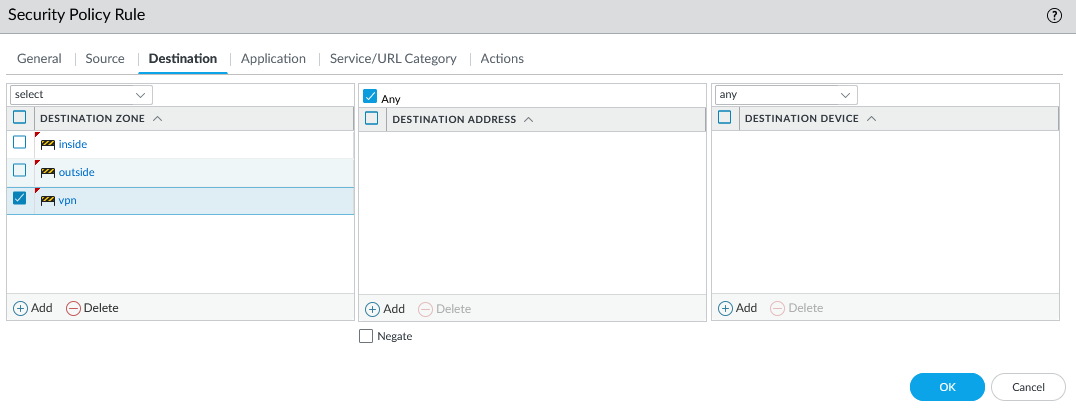
1. Change the computer adapter settings as shown:



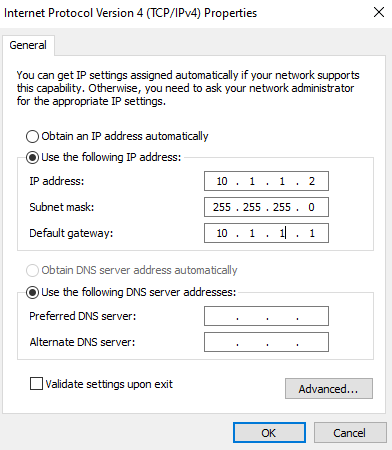
1. Repeat all above steps on the other router, but with appropriate addresses.
2. Set up policy rule as shown:



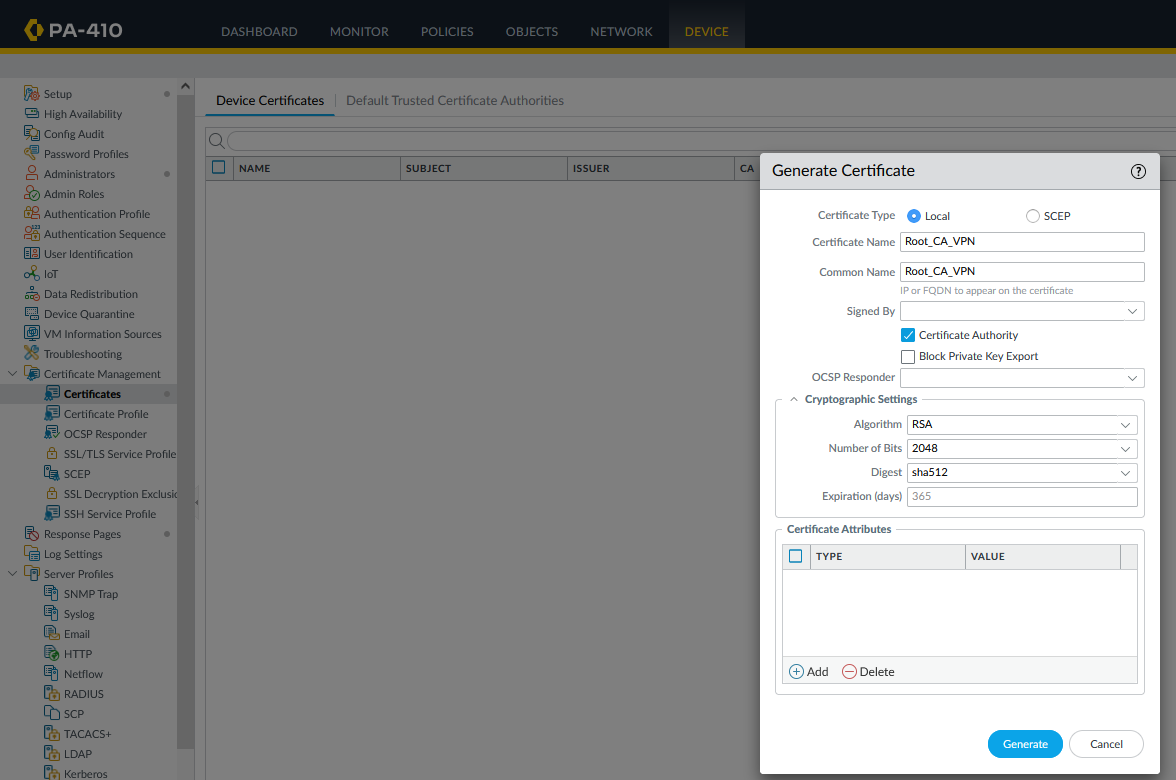


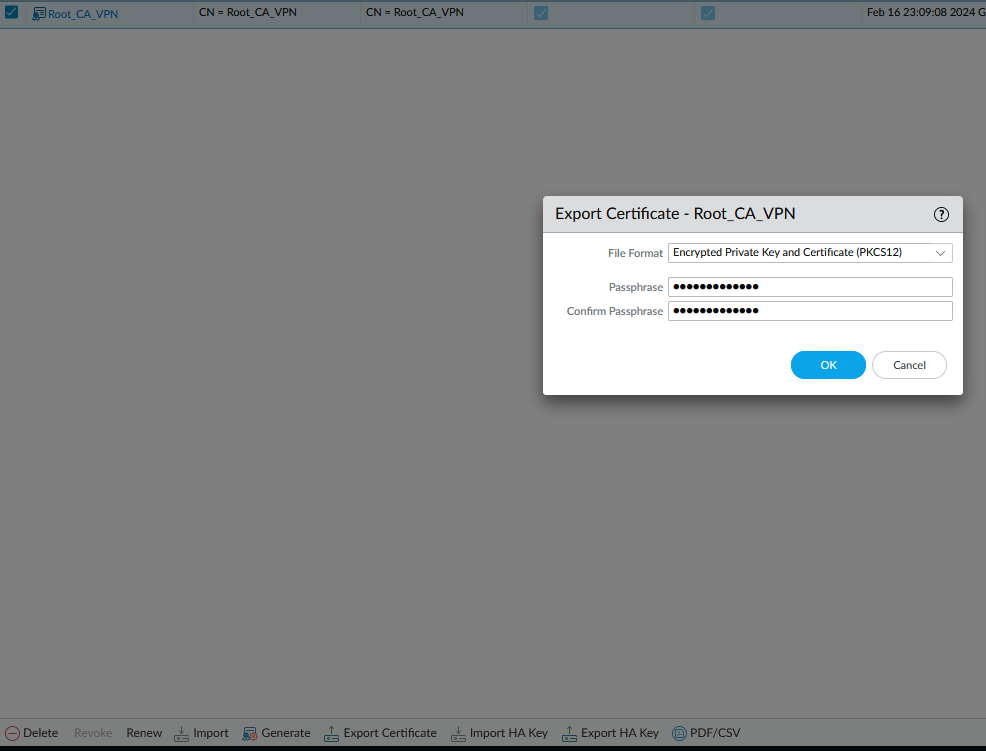


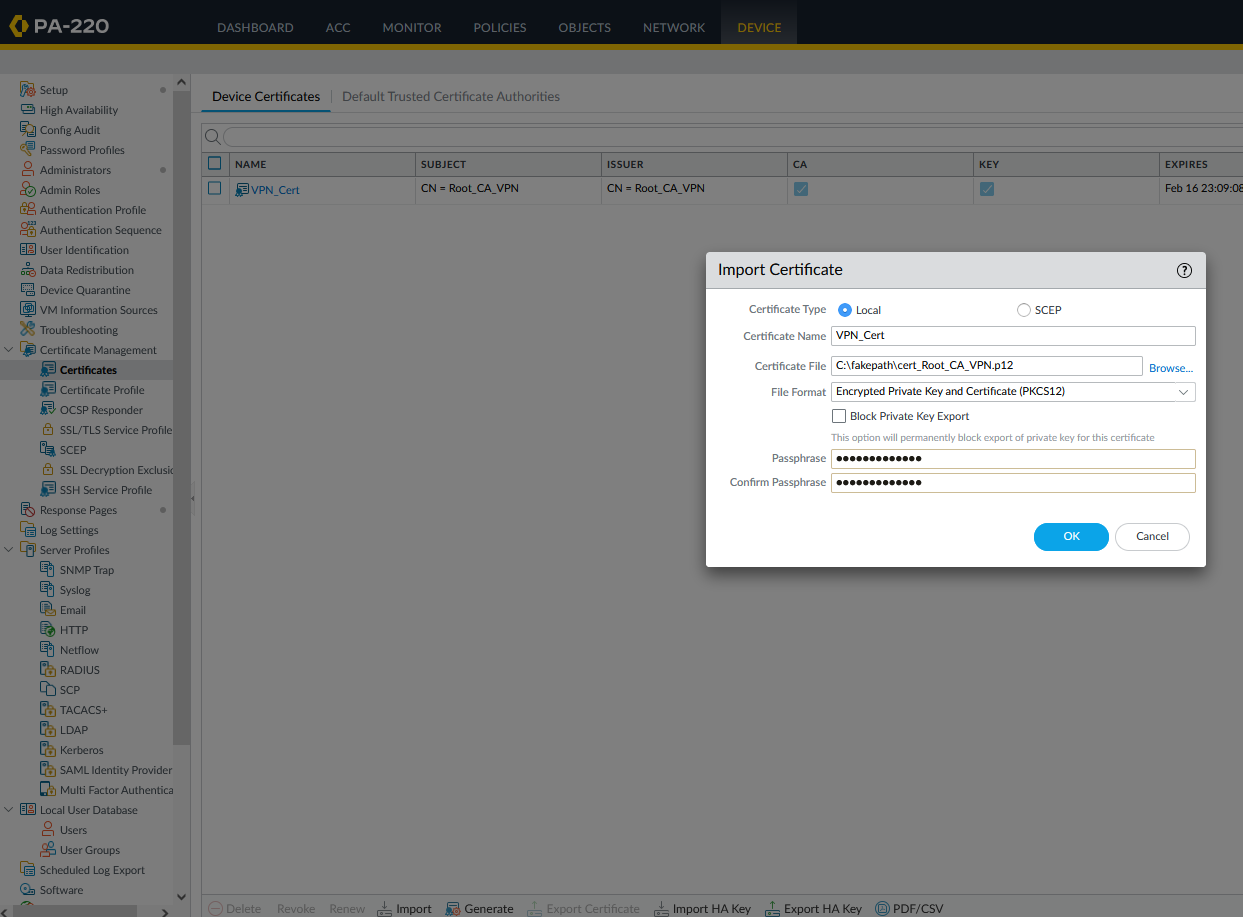
1. Commit changes
2. Repeat above steps for both firewalls.
3. Configure IPv4 properties as shown:

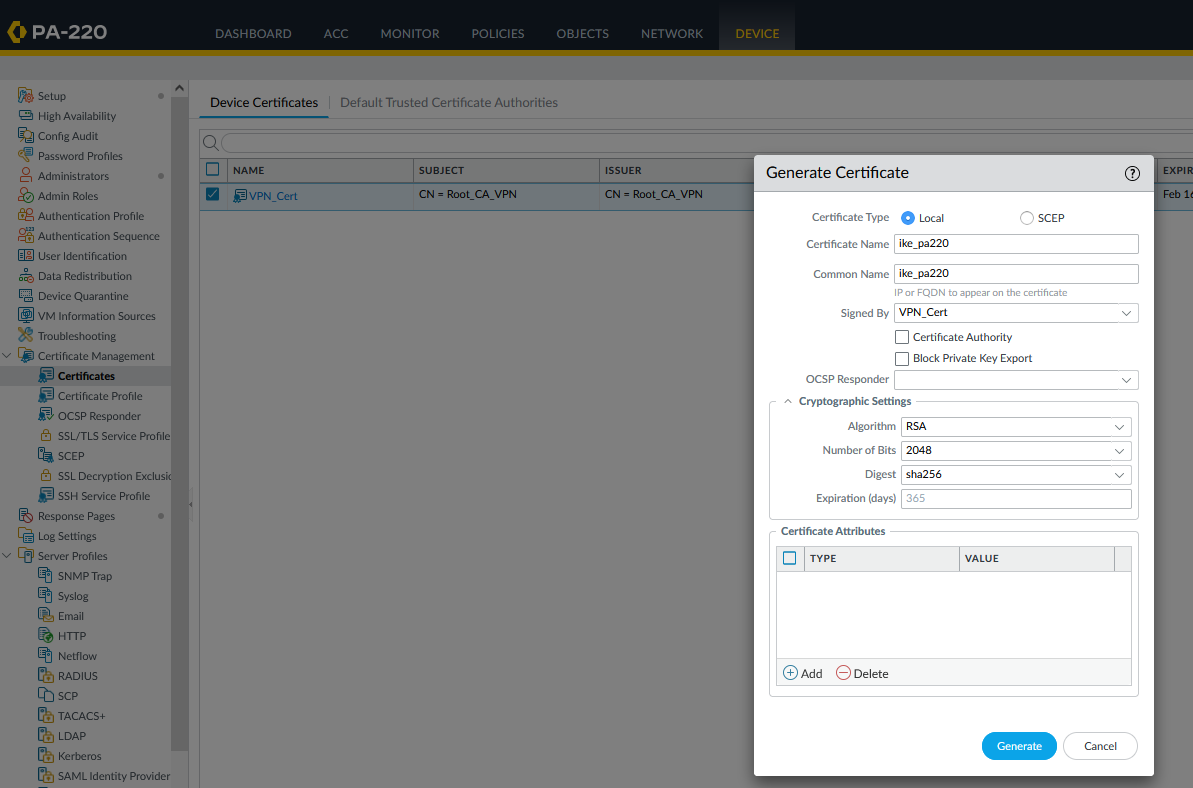


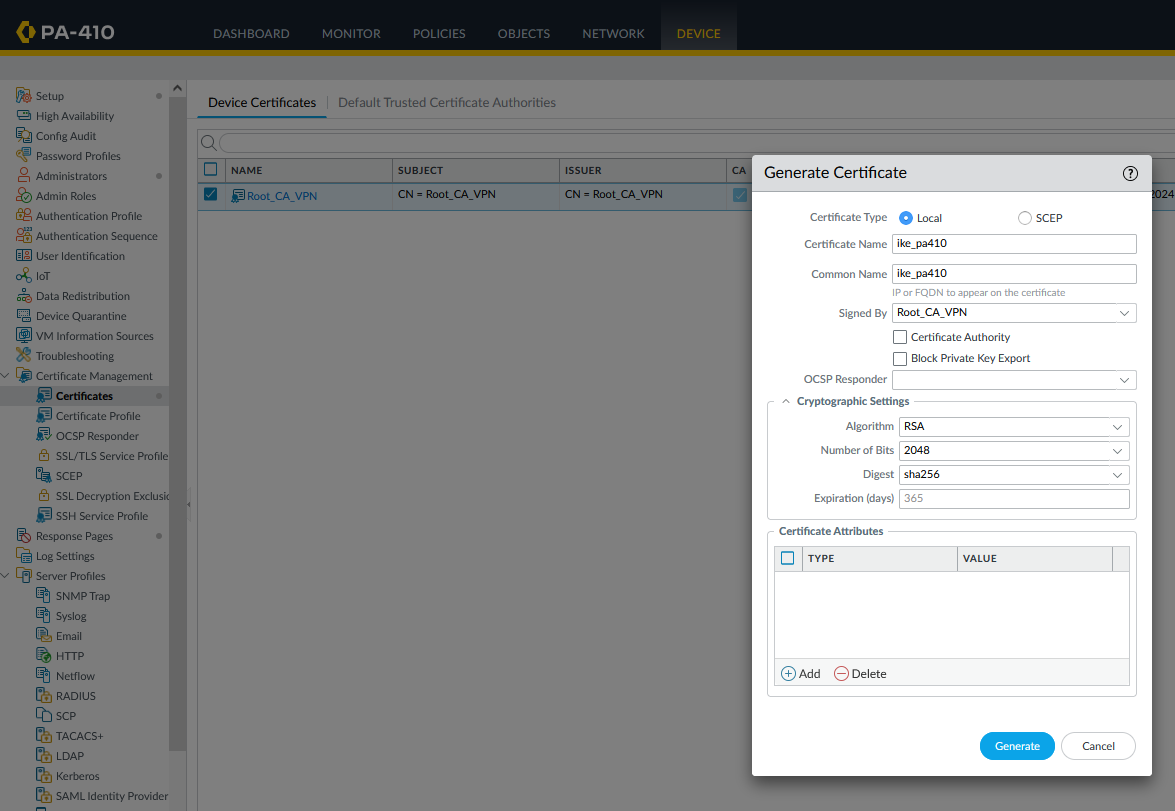
1. Generate certificates as shown on both firewalls



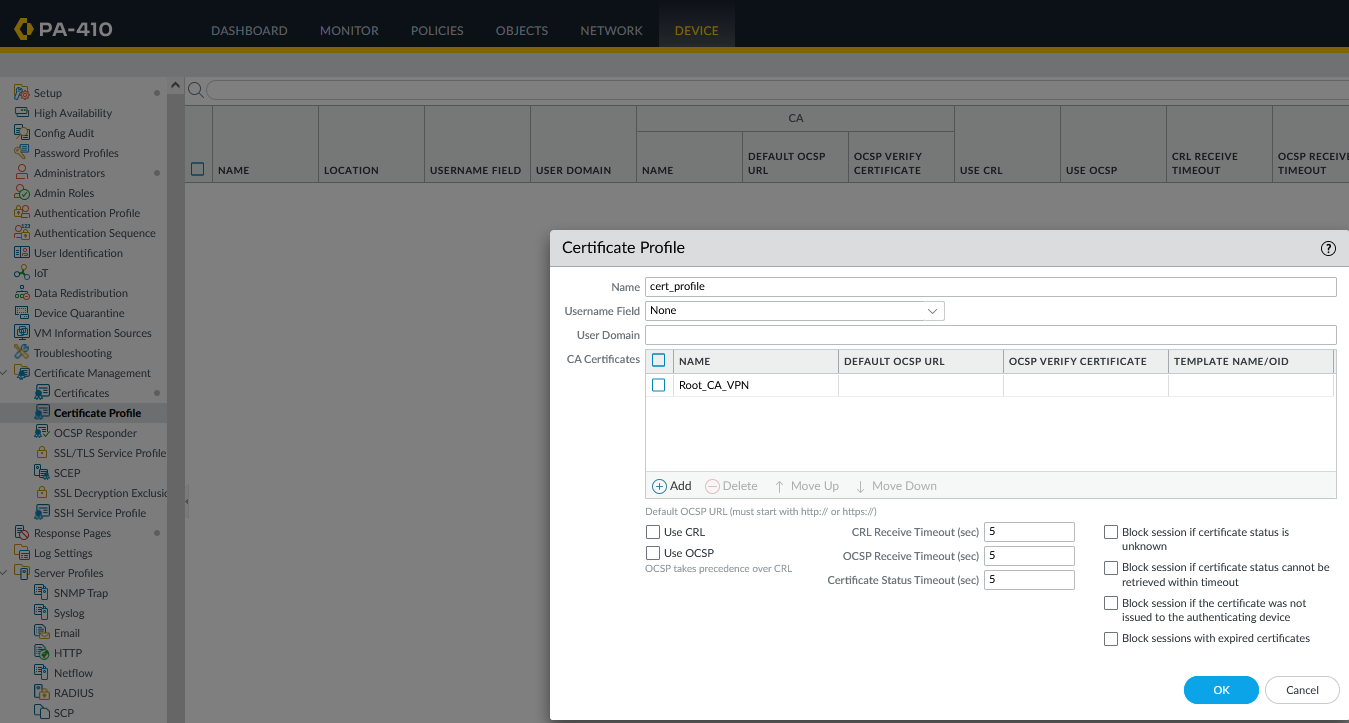


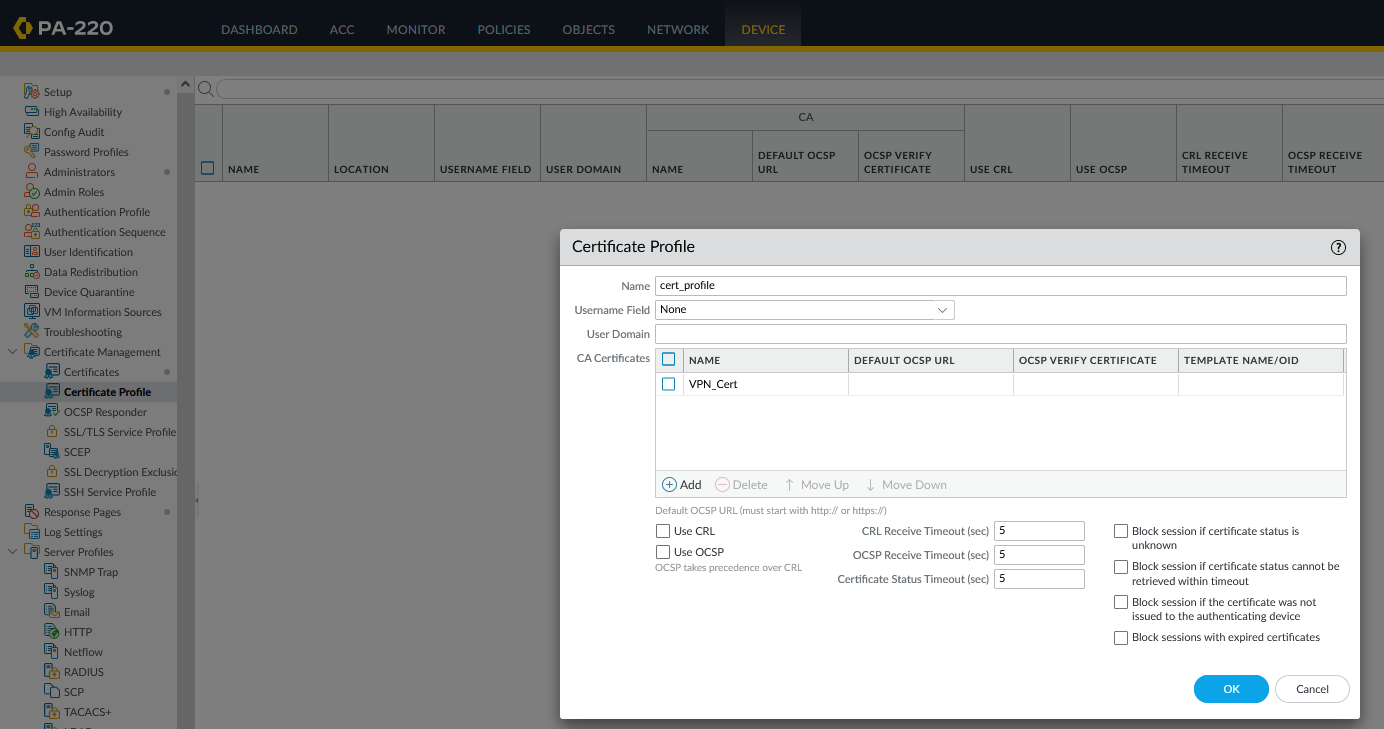




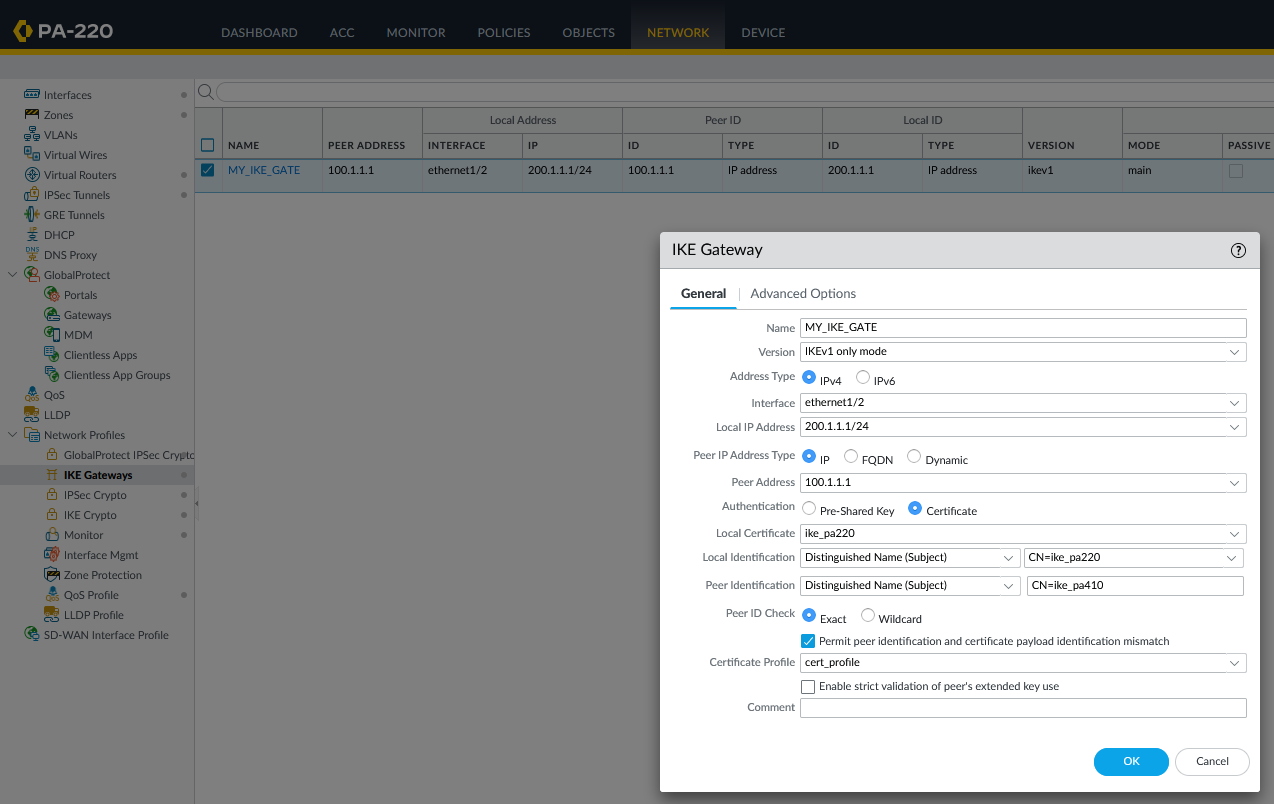


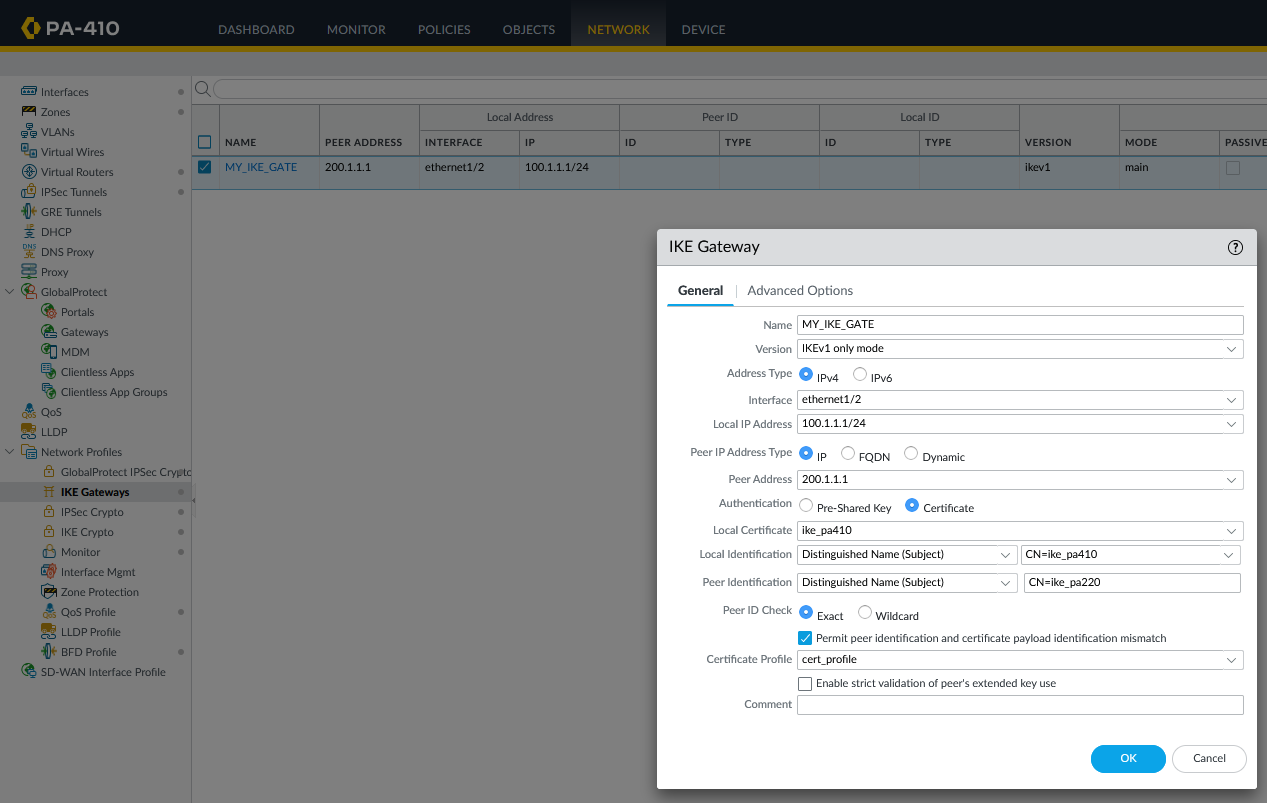
1. Configure certificate profiles





1. Configure IKE Gateways matching the IP address scheme





**Problems:**

We had almost no problems as we got help from classmates and the lab itself was relatively simple with a YouTube video with all the steps. Most of the lab was already configured from the previous lab and only took some minor changes to configure the certificate. There were extra delays because of personal reasons such as one of the partners not showing up due to medical reasons.

**Conclusion:**

Overall, the lab went pretty quick and was pretty simple. The configurations didn’t require much finding as people finished this lab prior to us and was just a few tweaks to the previous configuration. Nothing went wrong as we had some guidance, and we were able to ask question if we ever needed pretty easily. It didn’t take long for us to successfully manage to configure site-to-site VPN on two Palo Altos with self-signed certificates.