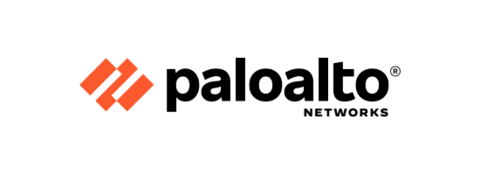


Palo Alto Site to Site VPN with Certificates

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose:**

The purpose of this lab was to configure site to site VPN with self-signed certificates on two Palo Alto firewalls.

**Background:**

Virtual Private Networks (VPNs), an encrypted connection on the internet, secures our sensitive information. They allow our online activity and information to be hidden, and often are used to prevent people with bad intentions, such as data sniffers, hackers, cyber criminals etc from getting in. The information that VPNs use to hide includes location, and helps users try to approach true online anonymity.

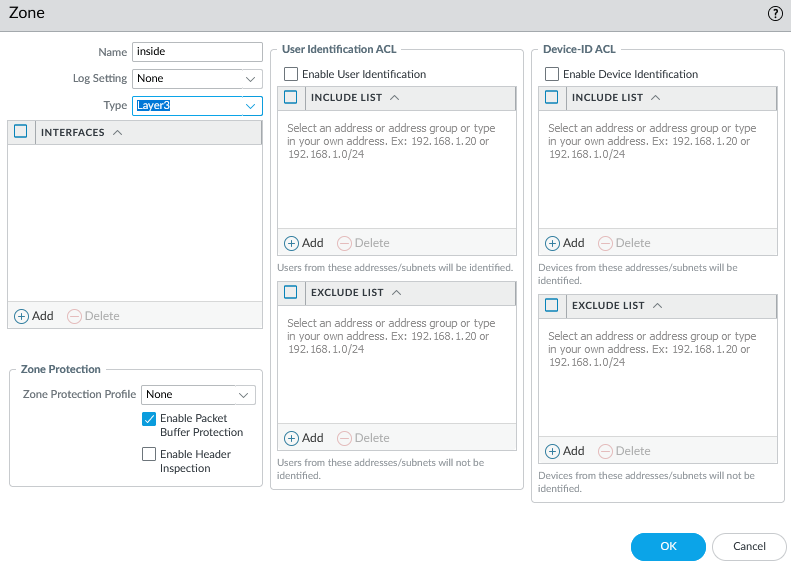
Using SSL certificates create a trust environment by authenticating communicating parties. Both security and authentication are crucial for successful institutions online. Certificates allow for encryption of data over the networks, and protect against people or anything with mal intentions, including hackers and cybercriminals. Usually, to be considered trustworthy by enterprises and users, certificates have to be signed and validated by a trusted Certificate Authority. Otherwise, it is possible that rogue certificates are impersonating trustworthy companies.

Certificates are used to secure connections between devices, applications, and machines. Self-signed SSL certificates are a quick, efficient, and cheap way to add SSL encryption to applications. By default, self-signed certificates will never be trusted by websites and many other things on the internet.

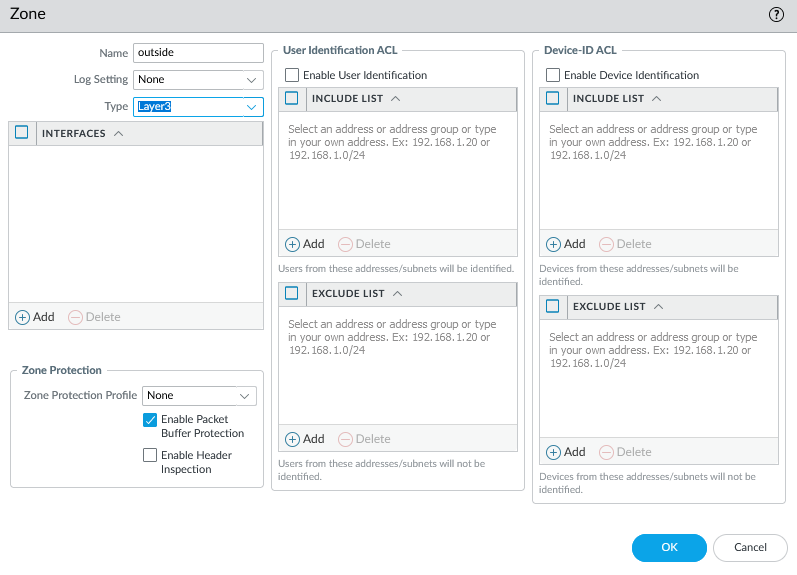
For our lab we set up site to site VPN, which is a connection between multiple networks, using two Palo Altos. We, similar to a lot of other groups had a lot of trouble getting our tunnels to work and troubleshooted for long periods of time.

**Lab Procedure:**

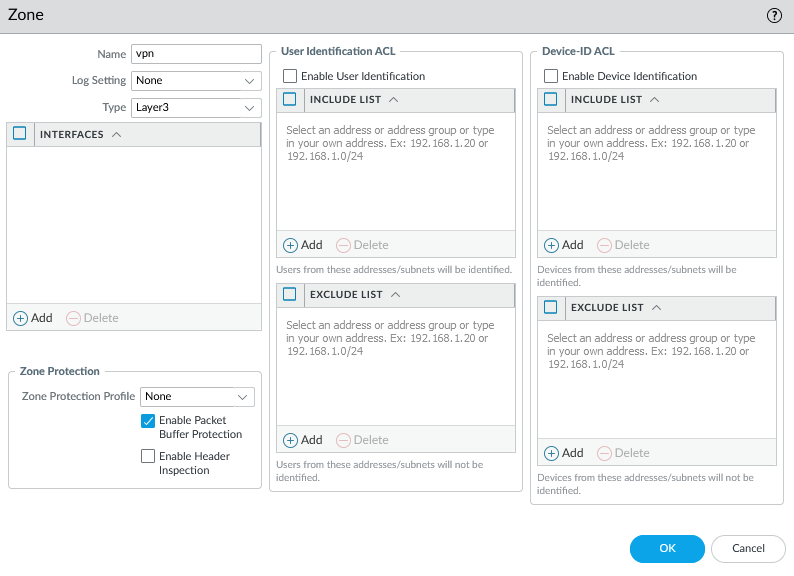
1. Go to Zones and click add.
2. Name the zone “inside” and change type to “Layer 3”



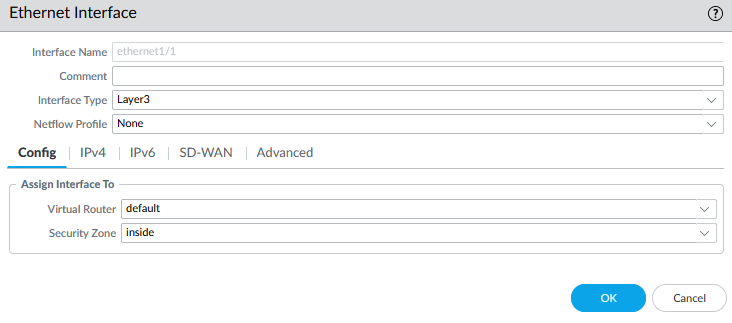
1. Add another zone, name the zone “outside” and change type to “Layer 3”



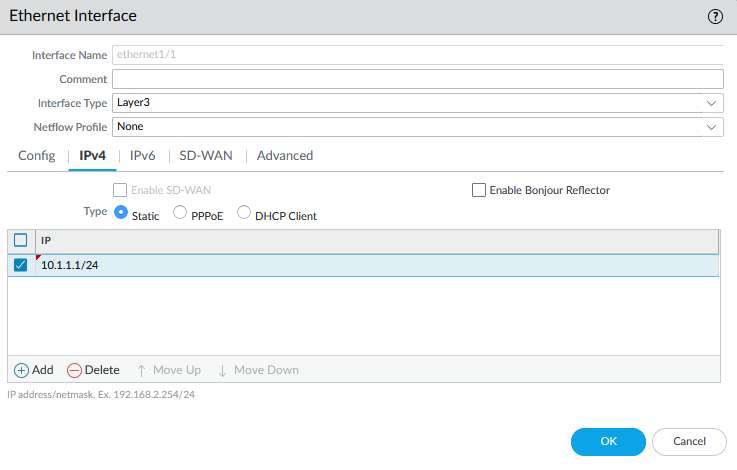
1. Add another zone, name the zone “vpn” and change type to “Layer 3”



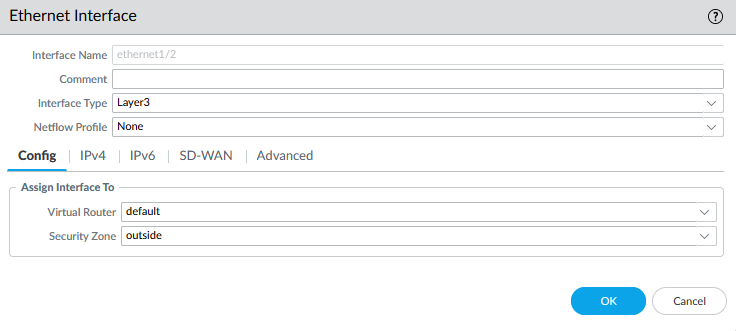
1. Configure the ethernet interface “ethernet1/1” as shown:



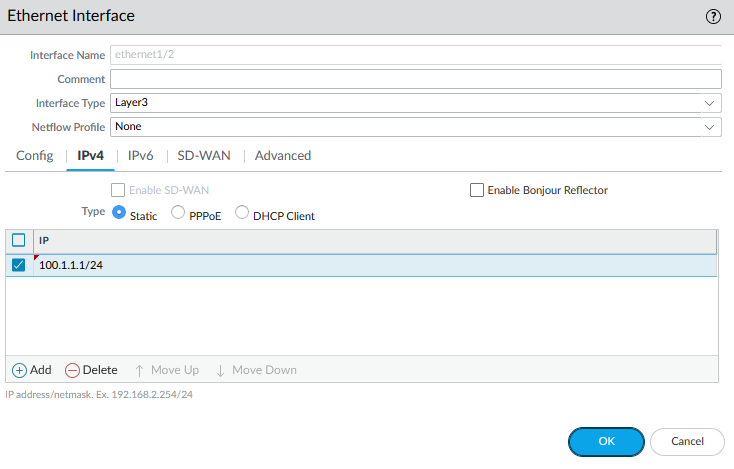
1. Configure the ethernet interface “ethernet1/1” as shown:



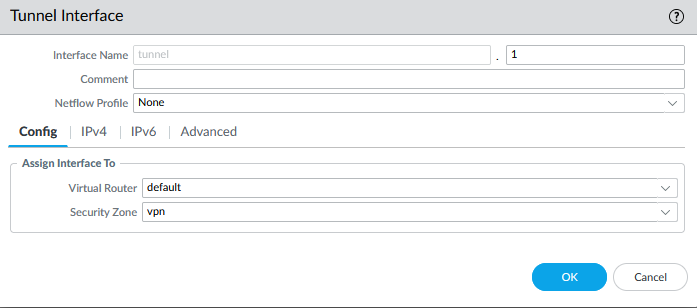
1. Configure the ethernet interface “ethernet1/2” as shown:



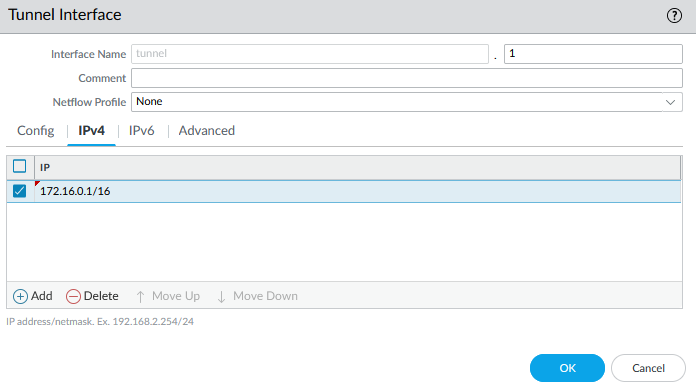
1. Configure the ethernet interface “ethernet1/2” as shown:

****

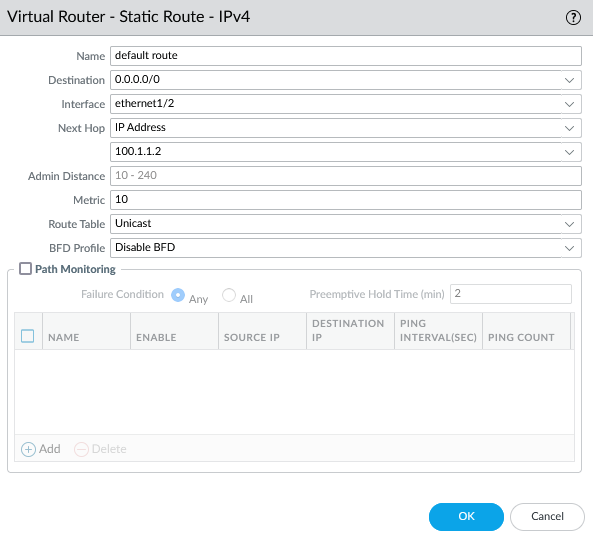
1. Configure the tunnel interface “tunnel” as shown:



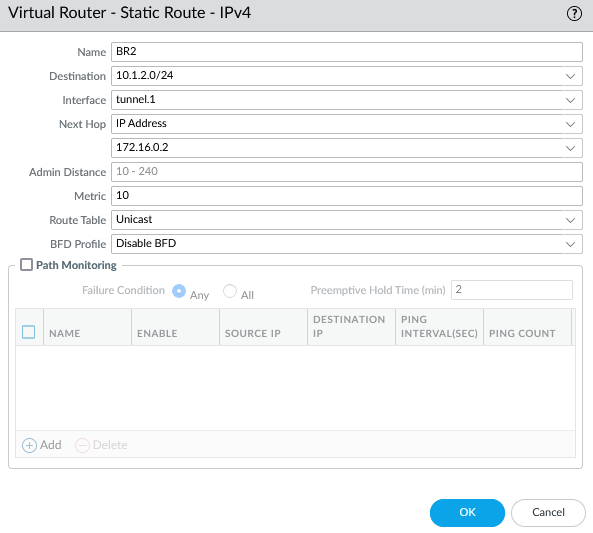
1. Configure the tunnel interface “tunnel” as shown:



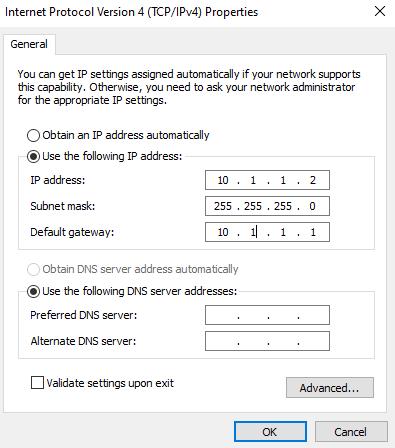
1. Add a default static route and configure as shown:



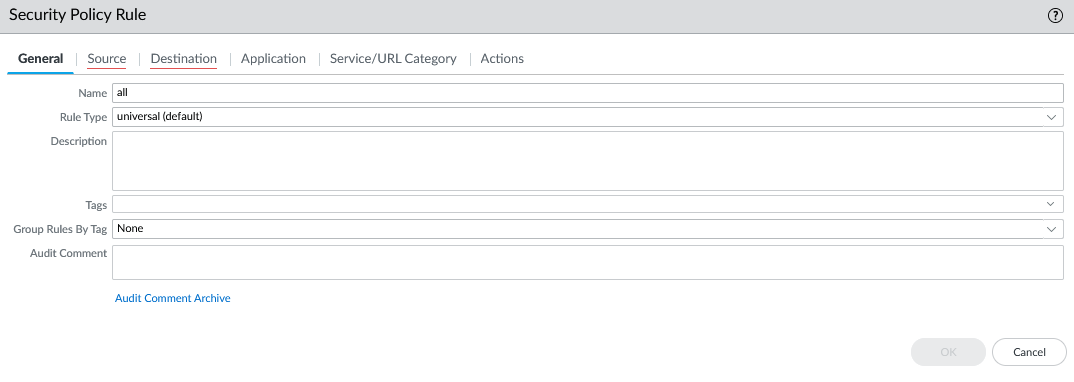
1. Add a static route and configure as shown:

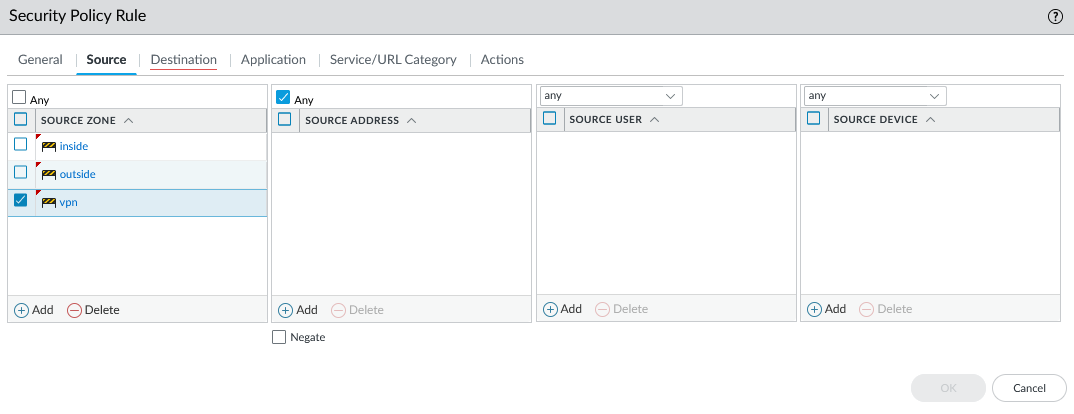


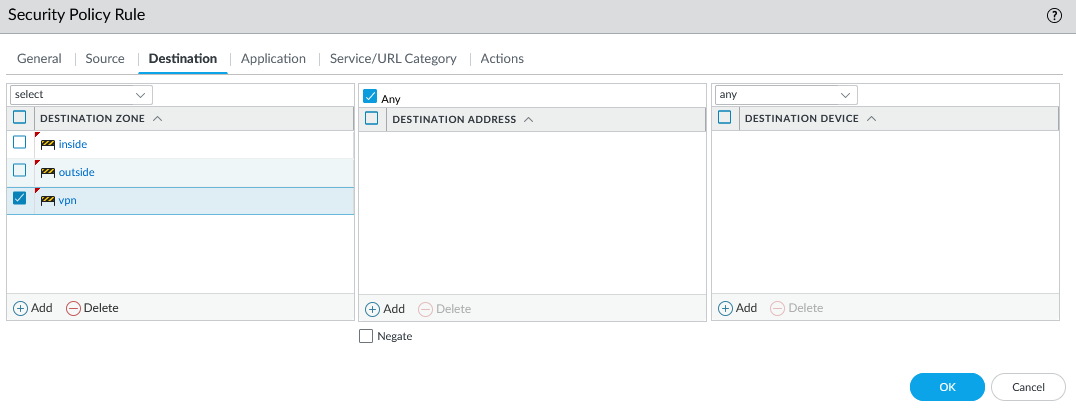
1. Change the computer adapter settings as shown:



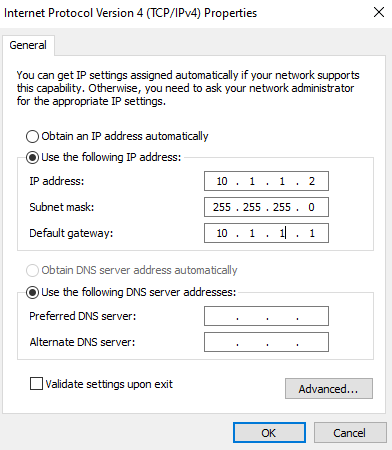
1. Repeat all above steps on the other router, but with appropriate addresses.
2. Set up policy rule as shown:



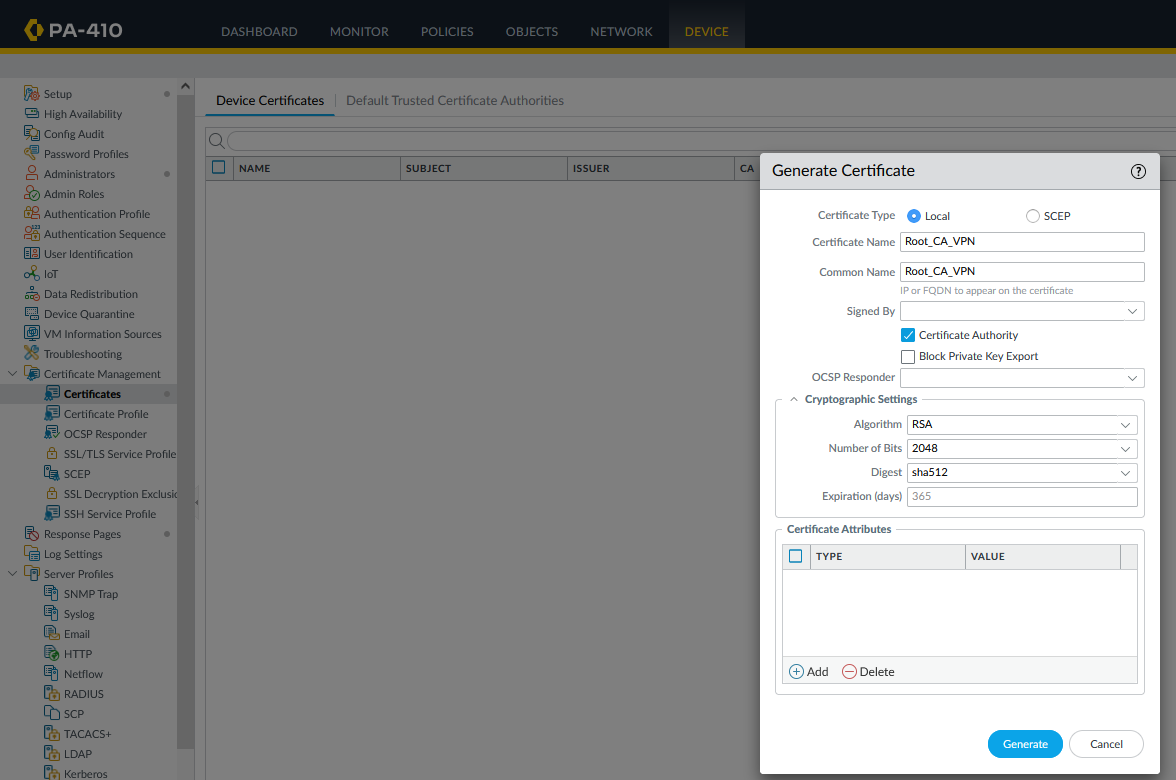


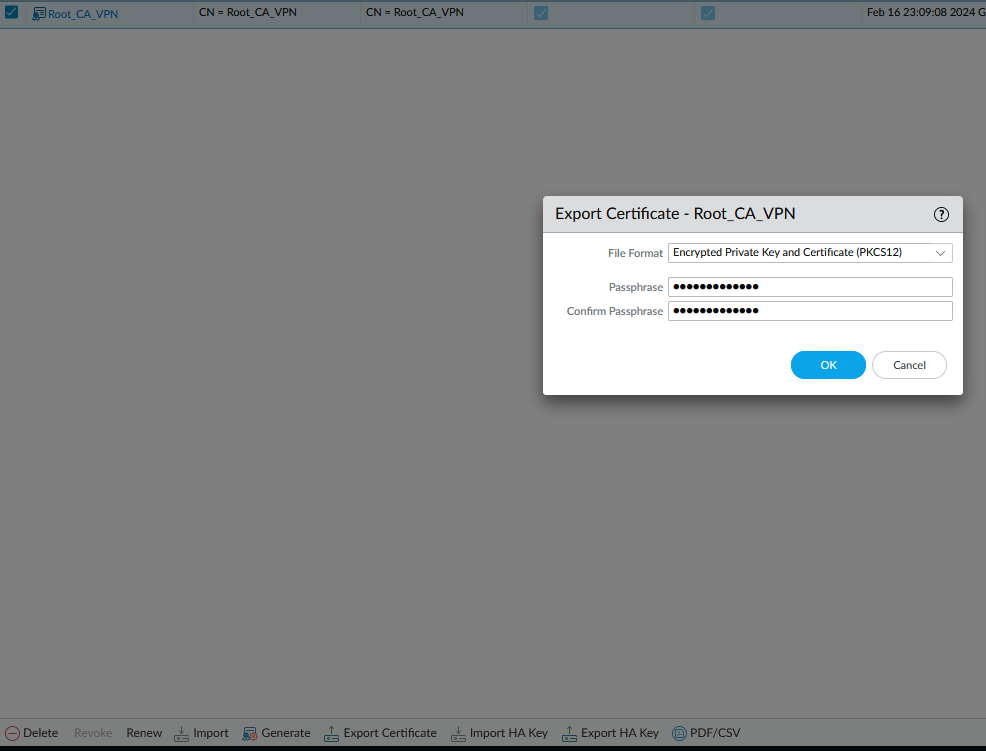


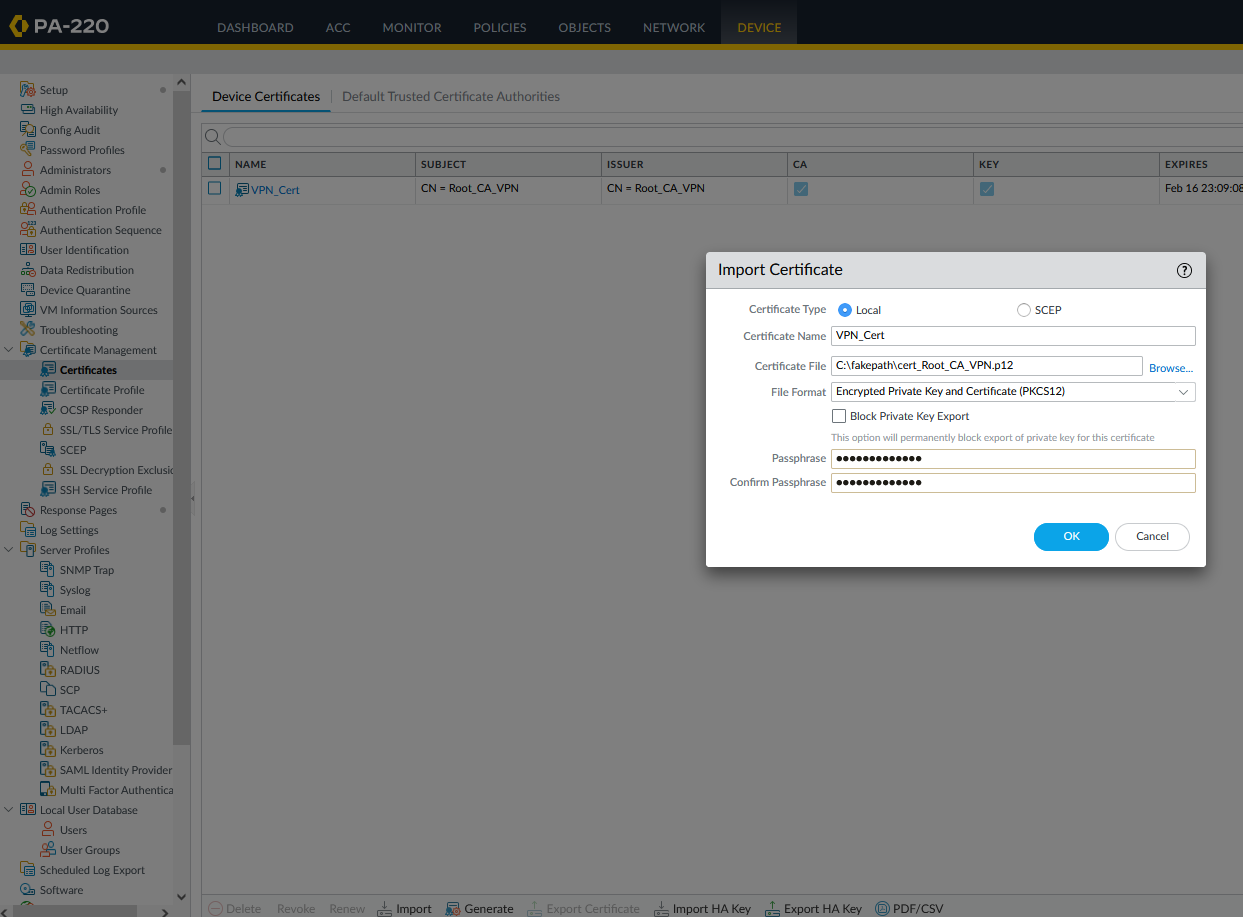
1. Commit changes
2. Repeat above steps for both firewalls.
3. Configure IPv4 properties as shown:

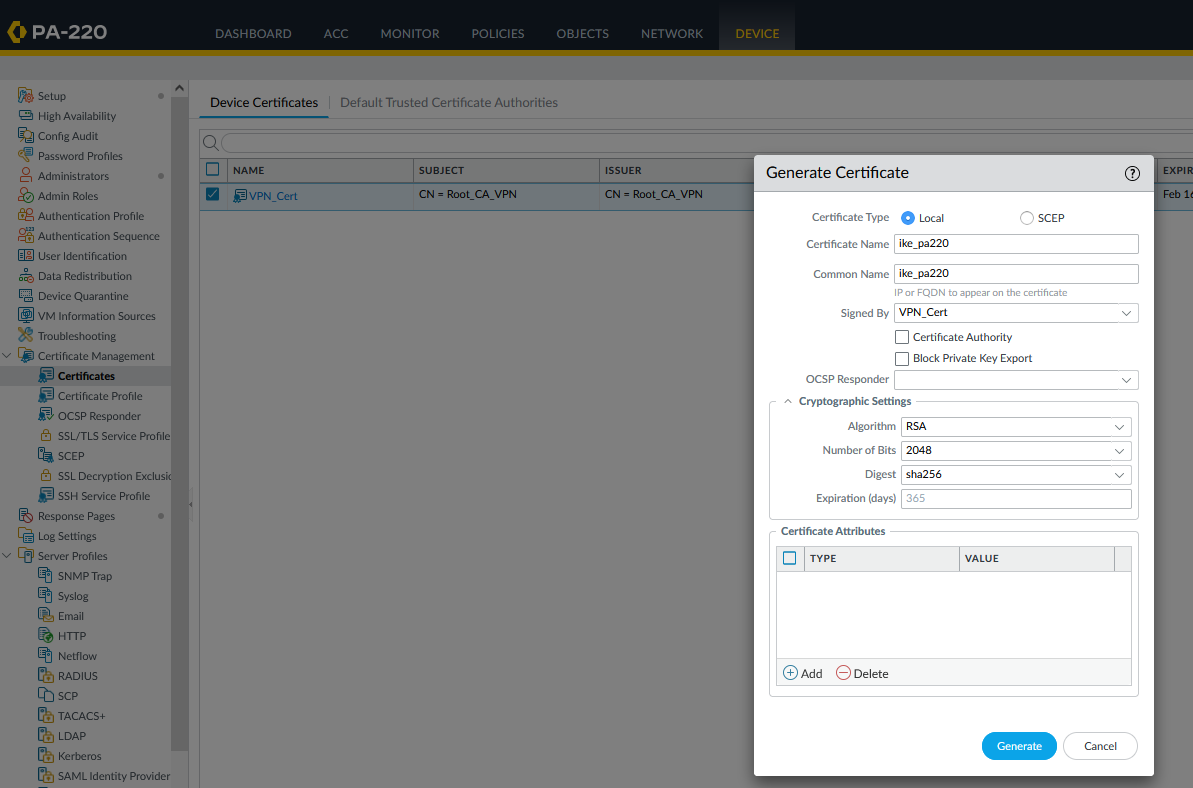


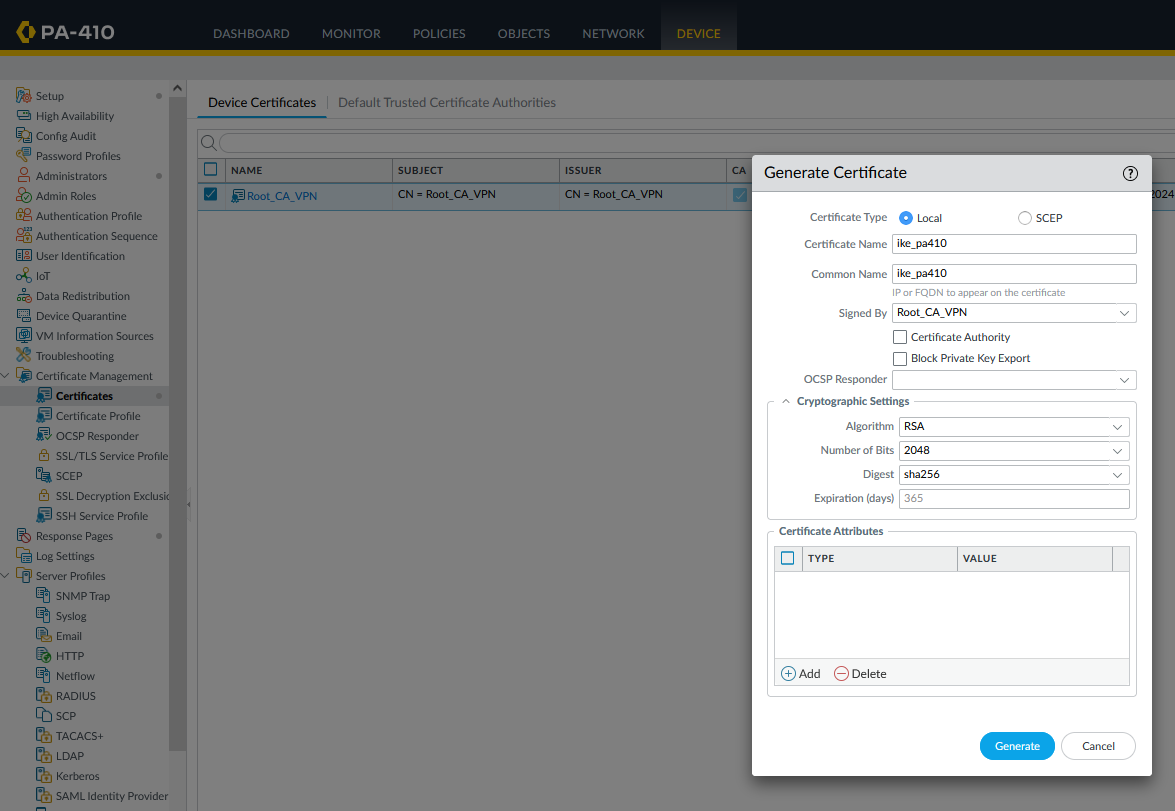
1. Generate certificates as shown on both firewalls



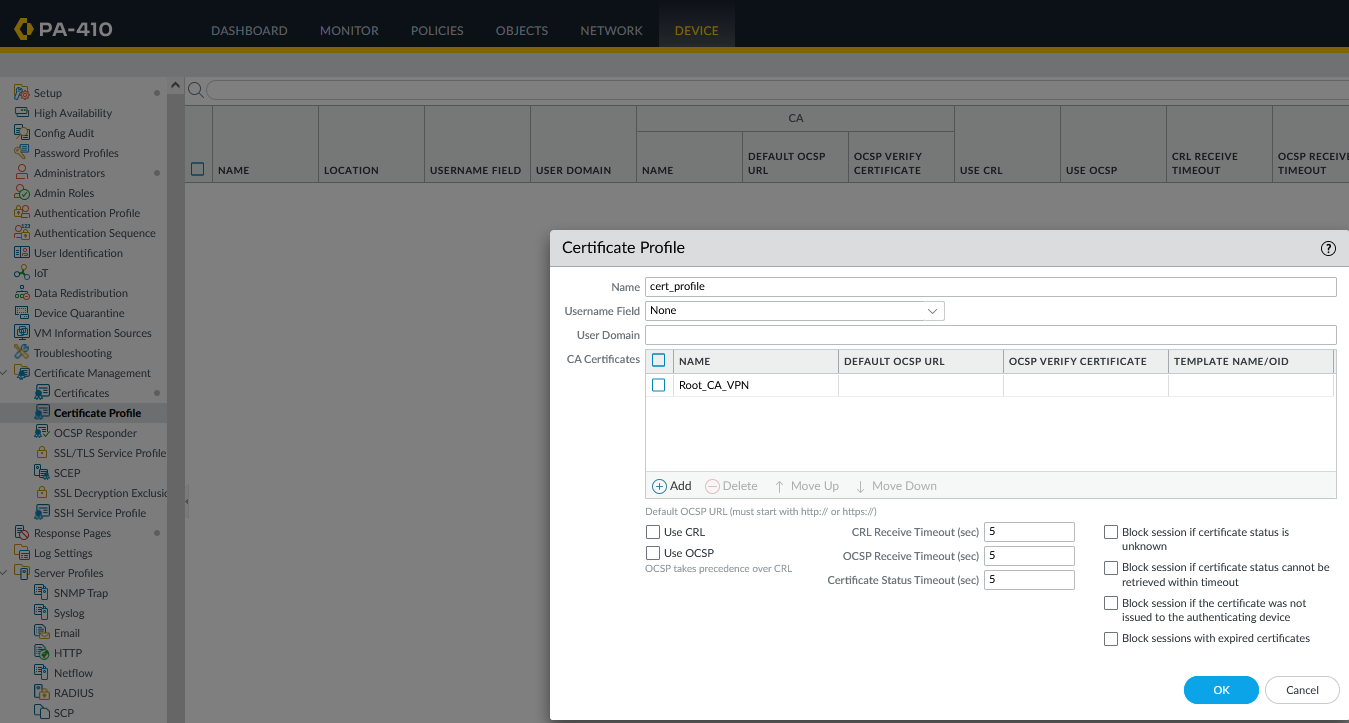


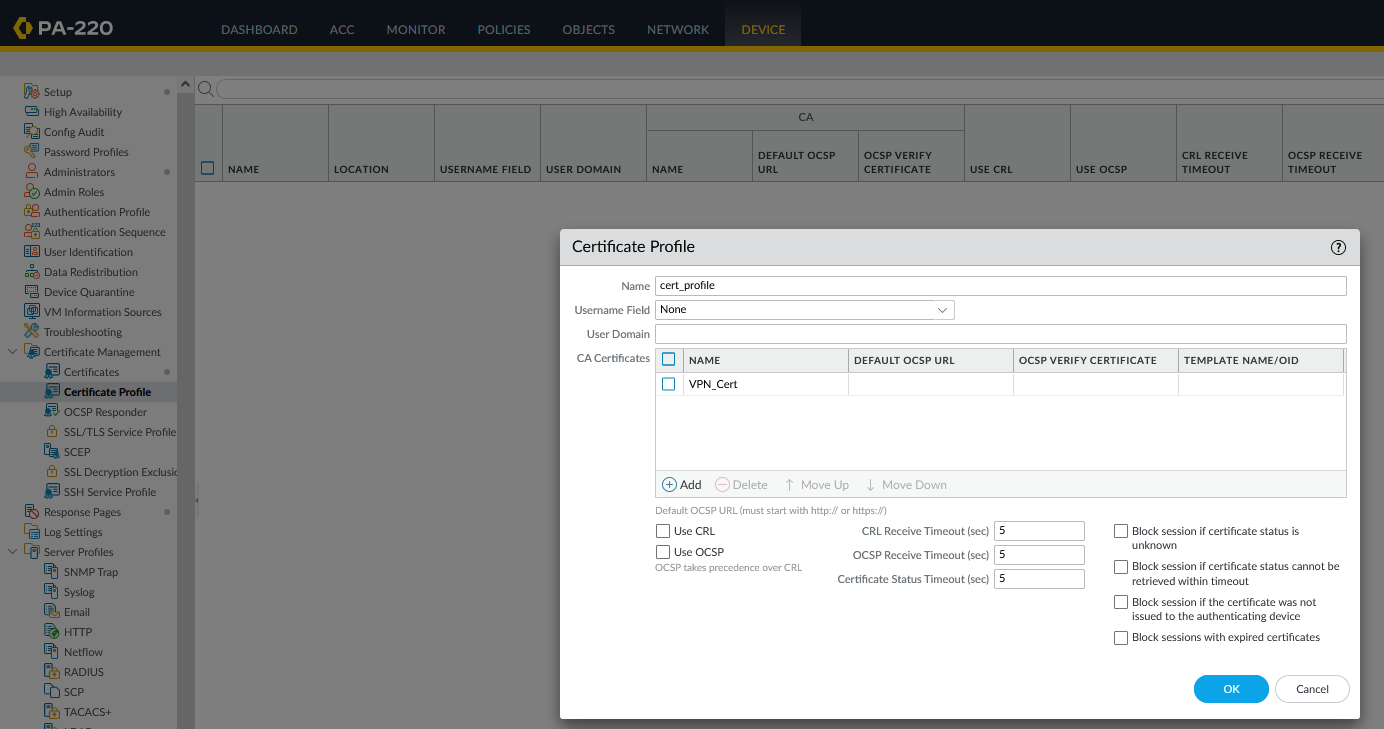




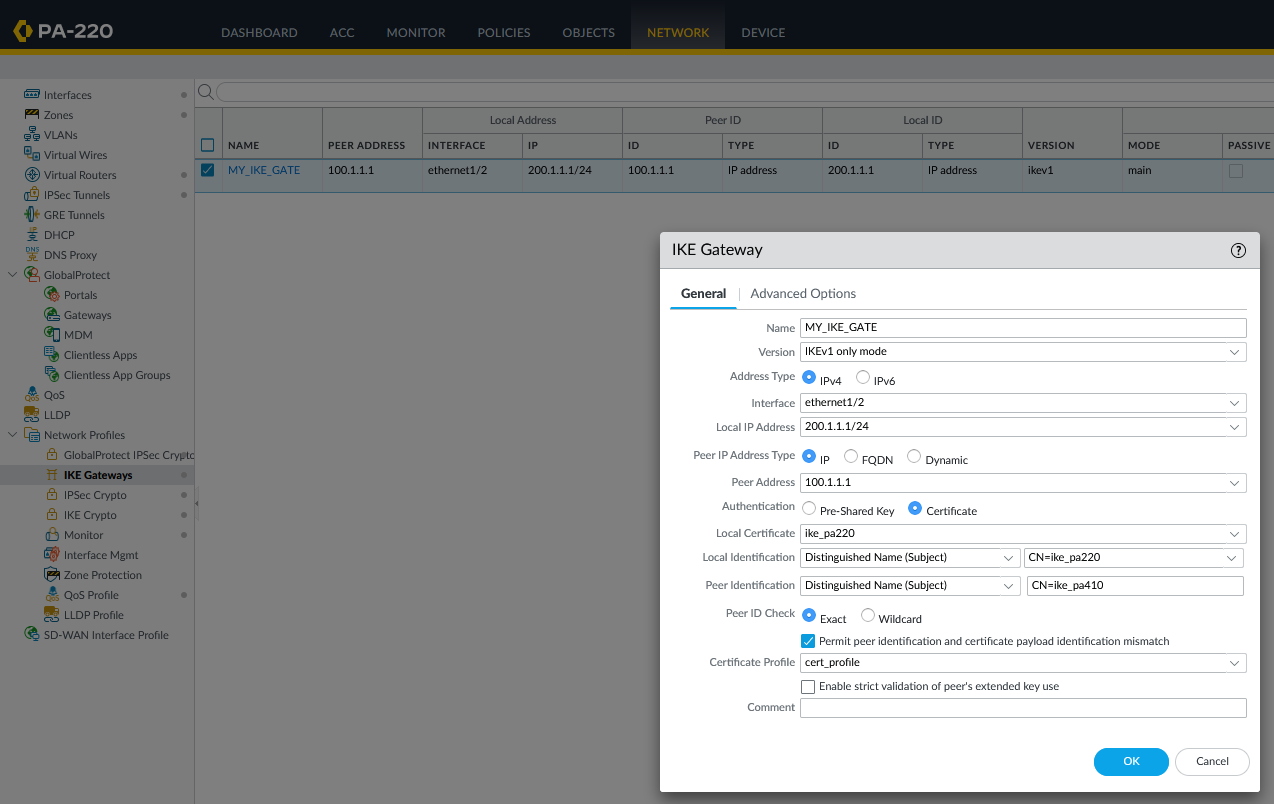


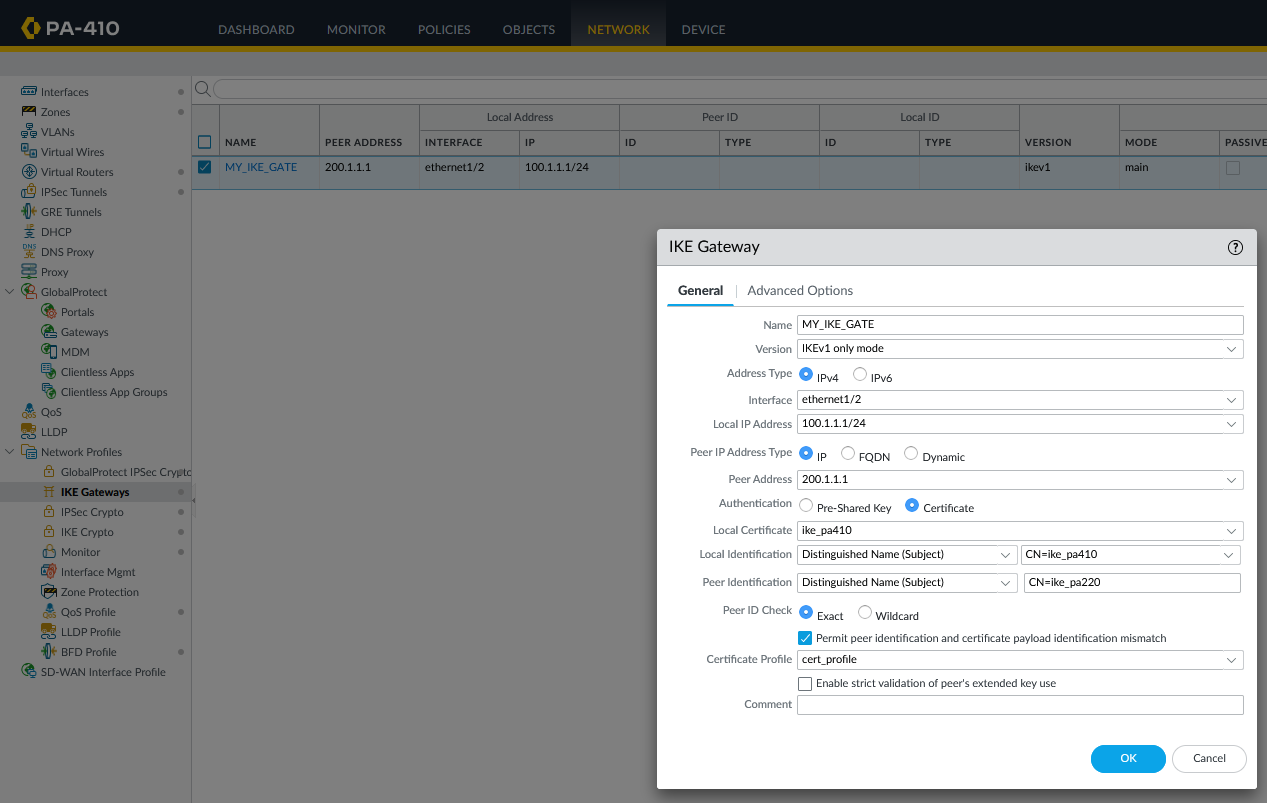
1. Configure certificate profiles





1. Configure IKE Gateways matching the IP address scheme





**Problems**

We had little no problems this lab. We were able to ask around to classmates for help when we had questions about how to complete the lab and procedures. However, the completion of the lab and writeup were delayed significantly because of health reasons of one of our group members. One member was diagnosed with a concussion, which meant that they missed multiple days of school.

**Conclusion**

In this lab, we configured a site-to-site VPN with certificates on a Palo Alto firewall.