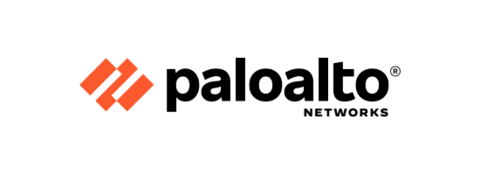


Palo Alto Site to Site VPN with Pre-Shared Keys

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose:**

The purpose of this lab was to configure site to site VPN with pre-shared keys on two Palo Alto firewalls.

**Background:**

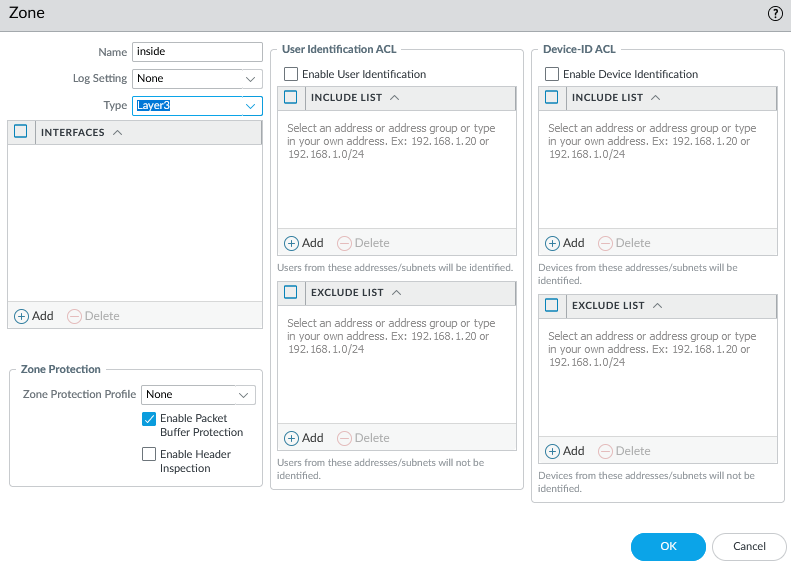
Virtual Private Network or VPNs are an encrypted connection over the internet. It allows for sensitive information to be kept more secure. VPN’s hide your online activity and are often used to guard against people with mal intentions, such as hackers, data sniffers, etc. VPNs can hide information like location and is the closest thing a person can have to true anonymity online.

The VPN was first put into use in 1996 by a Microsoft employee, and in 1999 the developed protocol was published. VPNs are used mostly in business, but with the development of companies like Nord VPN amongst many others, there began to be a growing market of consumers looking for VPN services. They are often used to do things like watch a different places Netflix or just to hid IP addresses in public games. This is very different from what VPNs used to be. In the early 2000s they were used by Businesses to access private business networks. When there was a rising issue in ISPs using consumer data among other privacy scares, VPNs started booming for public average citizen use.

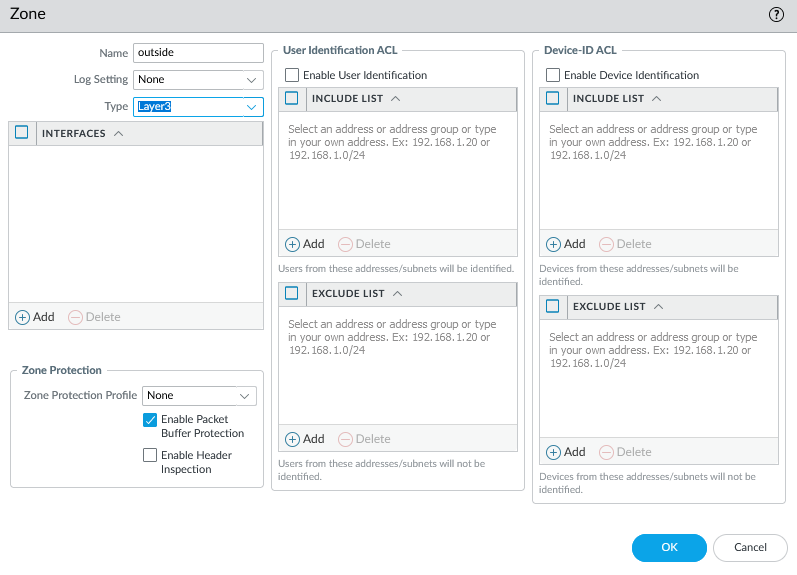
For our lab we set up site to site VPN, which is a connection between multiple networks, using two Palo Altos. We connected two Palo Alto’s and configured them with pre-shared keys at the sha-512 level. In order to prove the lab, we had to copy the traffic onto another port and monitor the packets that were going through. We like a lot of other groups had a lot of trouble getting our tunnels to work, and finding session monitoring to work.

**Lab Procedure:**

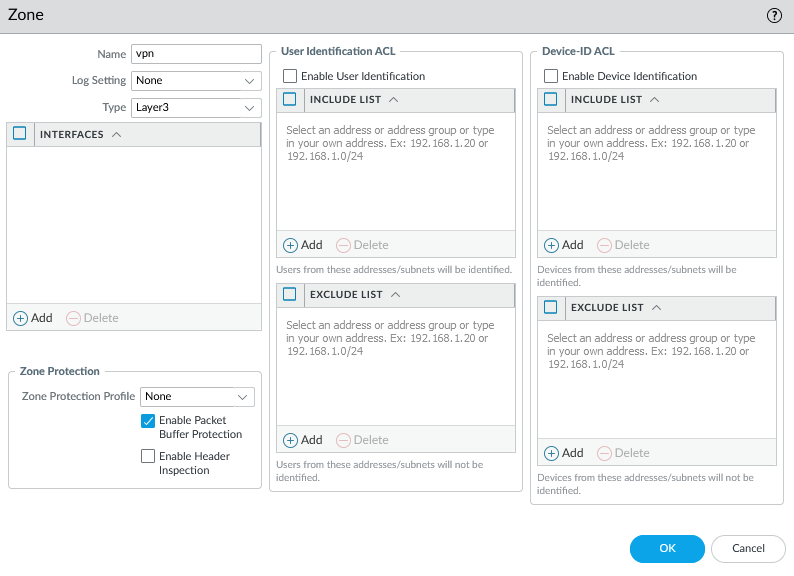
1. Go to Zones and click add.
2. Name the zone “inside” and change type to “Layer 3”



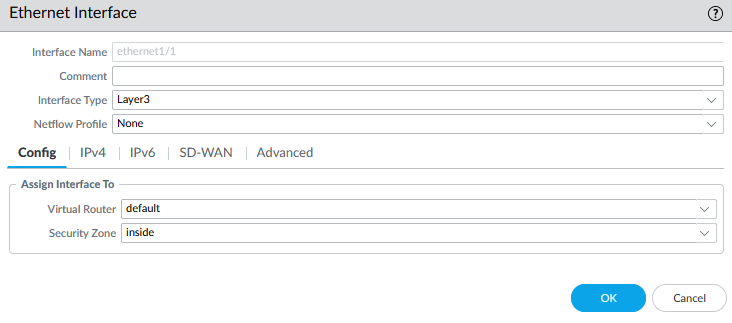
1. Add another zone, name the zone “outside” and change type to “Layer 3”



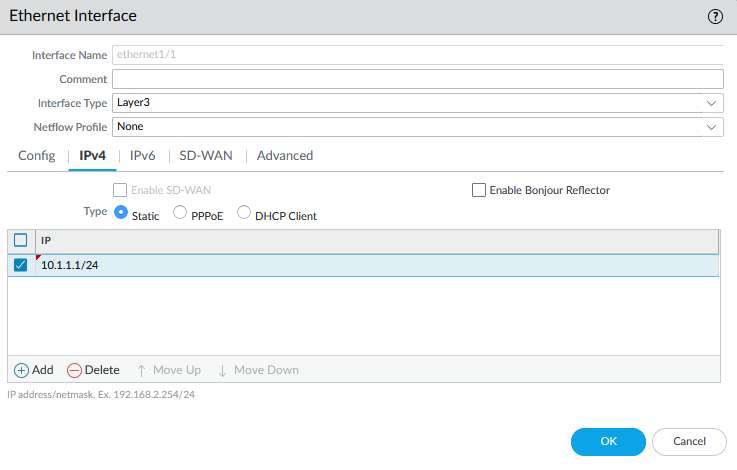
1. Add another zone, name the zone “vpn” and change type to “Layer 3”



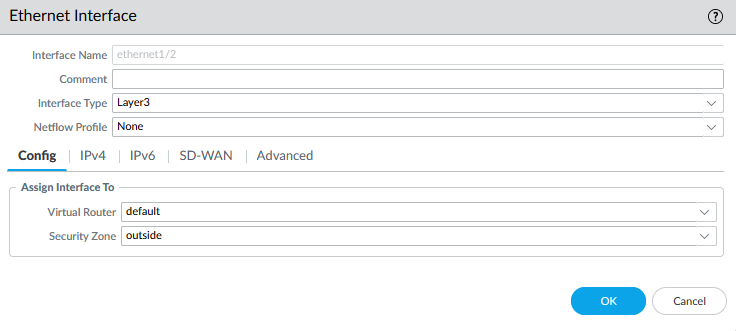
1. Configure the ethernet interface “ethernet1/1” as shown:



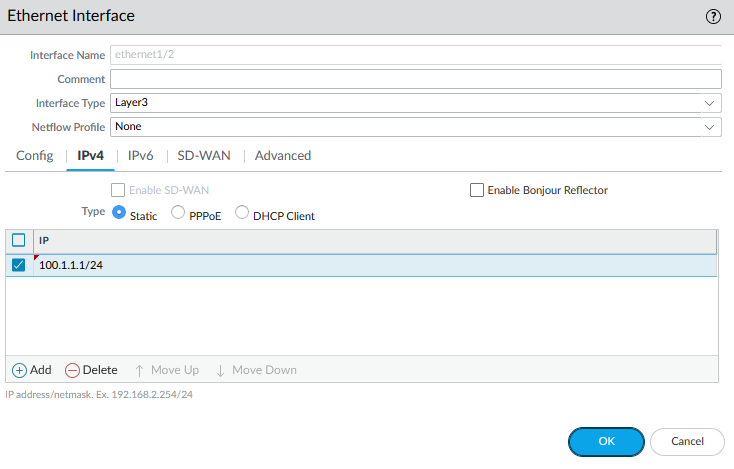
1. Configure the ethernet interface “ethernet1/1” as shown:



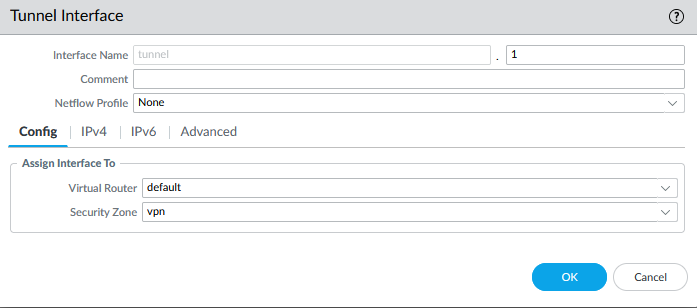
1. Configure the ethernet interface “ethernet1/2” as shown:



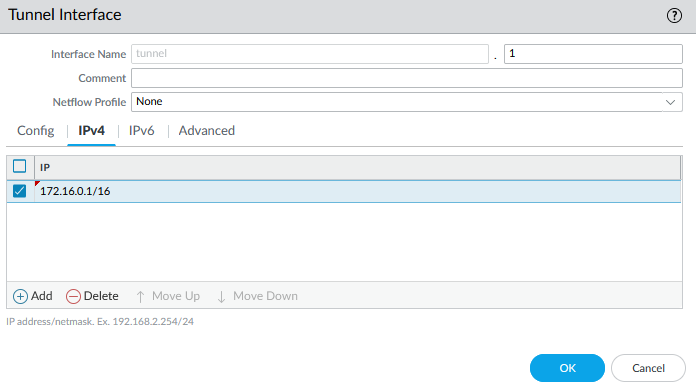
1. Configure the ethernet interface “ethernet1/2” as shown:

****

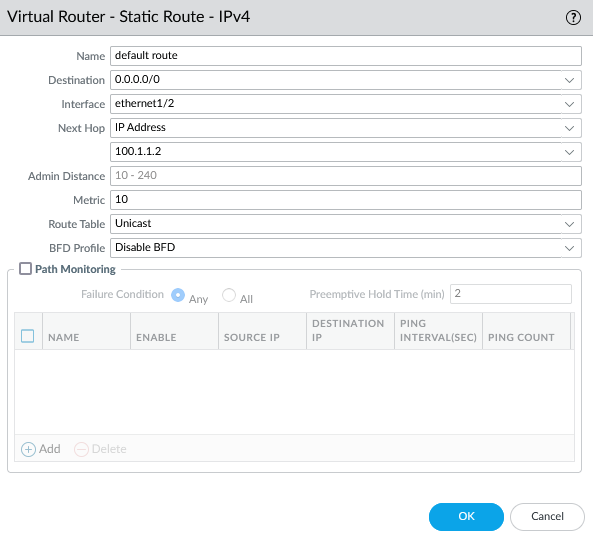
1. Configure the tunnel interface “tunnel” as shown:



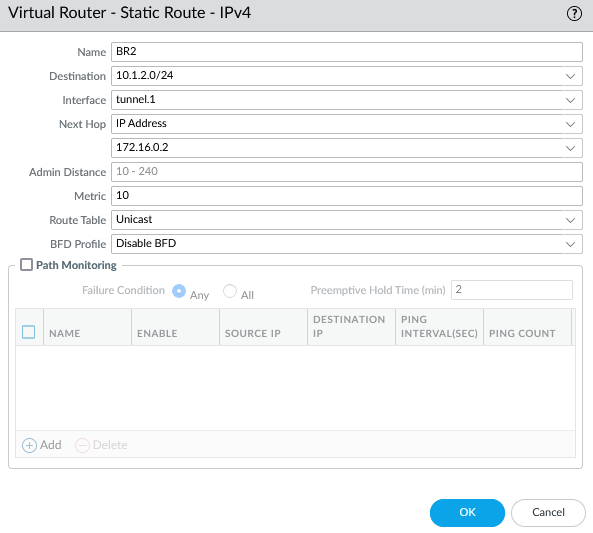
1. Configure the tunnel interface “tunnel” as shown:



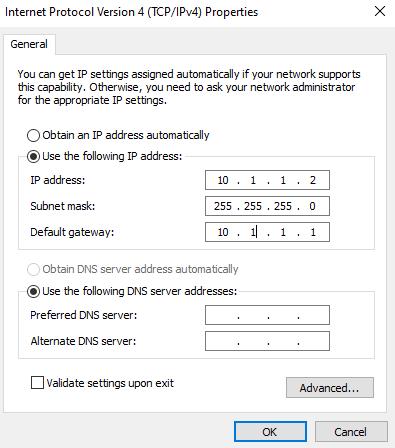
1. Add a default static route and configure as shown:



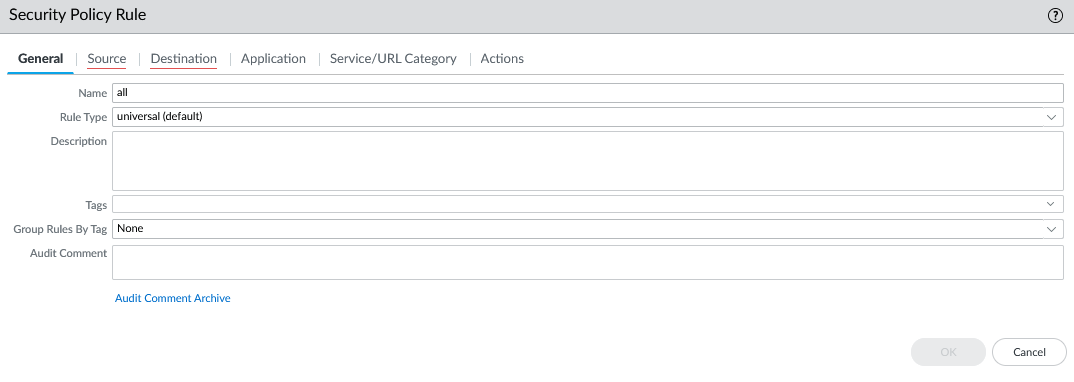
1. Add a static route and configure as shown:

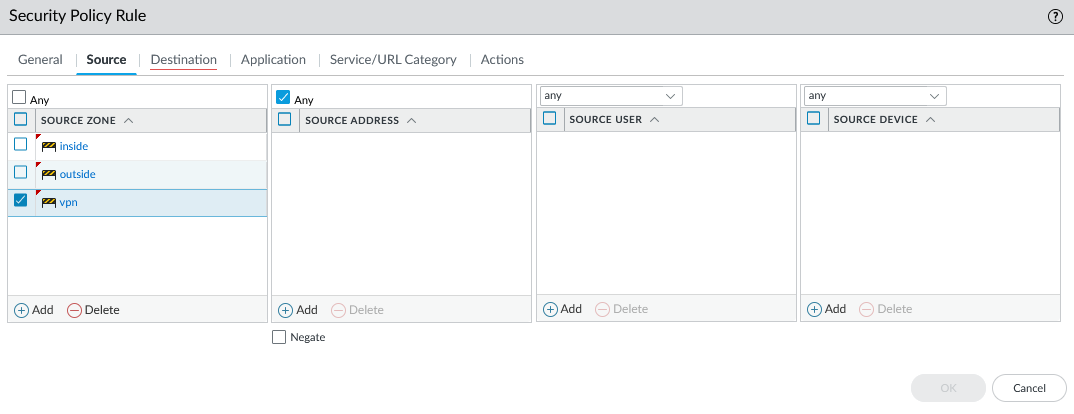


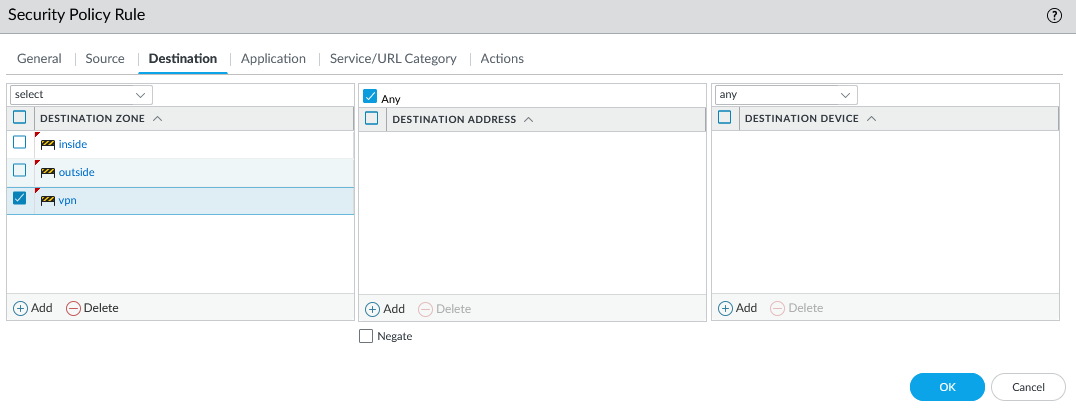
1. Change the computer adapter settings as shown:



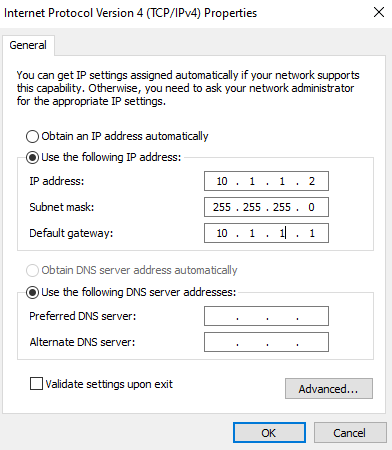
1. Repeat all above steps on the other router, but with appropriate addresses.
2. Set up policy rule as shown:



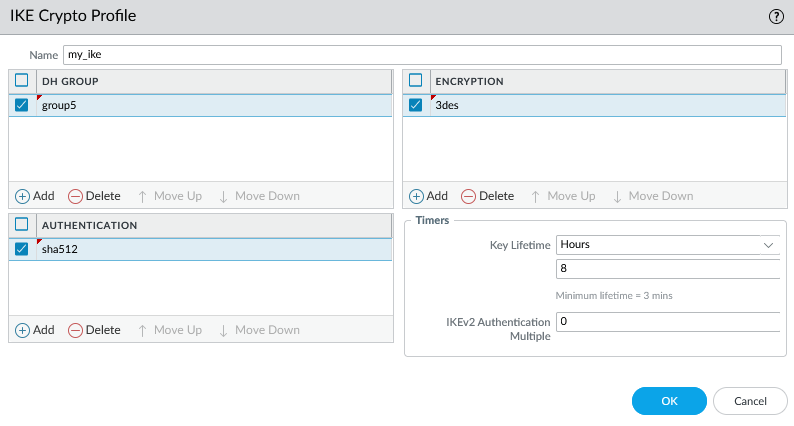




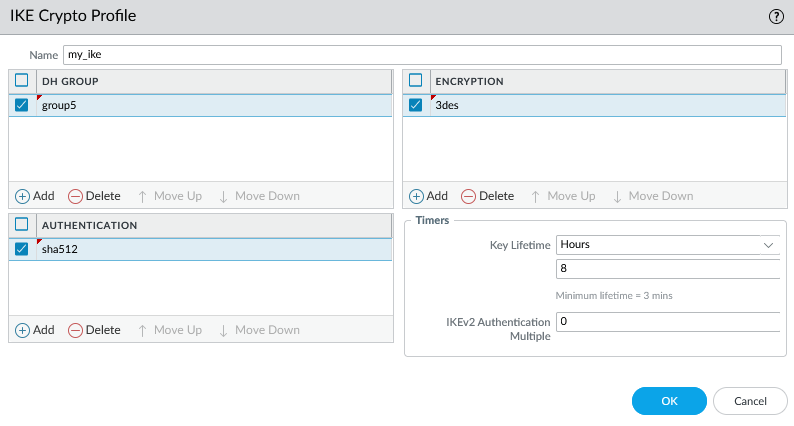
1. Commit changes
2. Repeat above steps for both firewalls.
3. Configure IPv4 properties as shown:



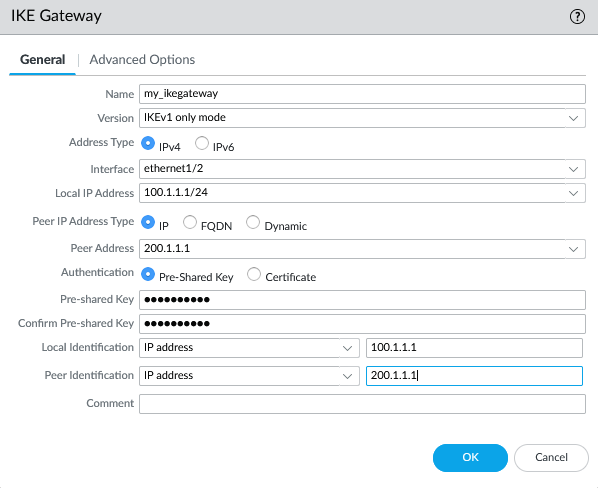
1. Add a new IKE crypto profile and configure as shown:

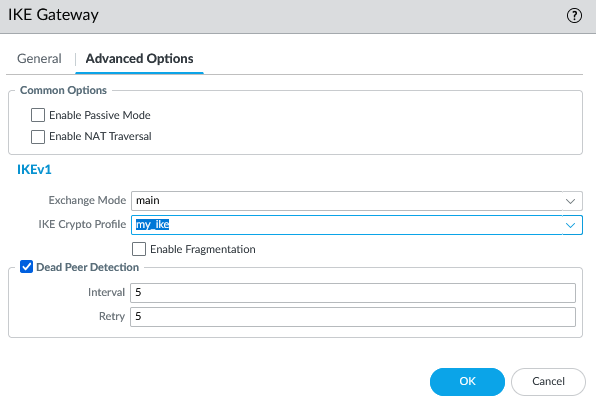


1. Add a new IPSec crypto profile and configure as shown:

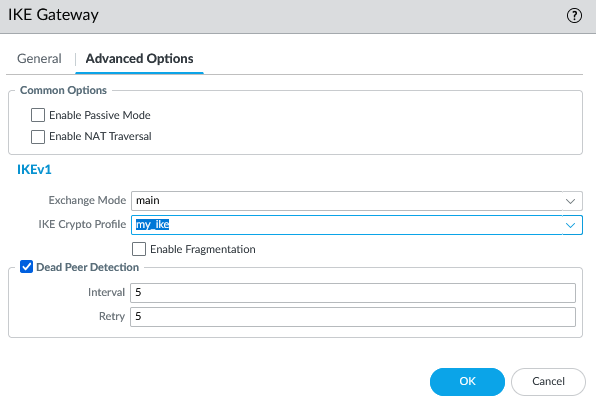


1. Add a new IKE Gateway and configure as shown:

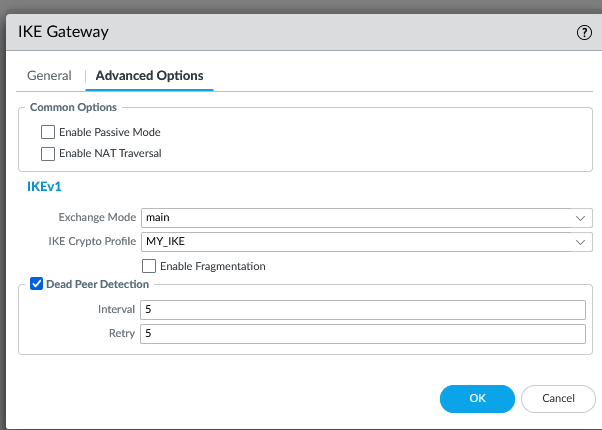




1. Add a new IPSec tunnel and configure as shown:



1. Configure this on the IKE gateway



1. Repeat all above steps on other firewall.
2. Assign IPs to interfaces on router
3. Delete virtual wires

**Problems:**

Our main issue with this lab was having to watch a configuration guide in Hindi. The language barrier made it extremely difficult to understand, and the video was very blurry. Additionally, the video was missing many steps, causing us to have to figure them out on our own, which also took a significant amount of time. In the beginning, our firewalls had trouble factory resetting easily, so we spent very large chunks of multiple periods attempting to perform a factory reset. Also, many times when we got to class, our rack was turned off when we arrived, so we wasted a lot of class time waiting for our racks to turn on. Loading time took a significant amount of time in our completion of this lab. Our tunnels were also not working, and we took a long time figuring that out on our own. Lastly, we had to figure out how to do session monitoring on our own.

**Conclusion:**

In this lab, we configured a site to site VPN with pre-shared keys on two Palo Alto firewalls.