Sarkar, Mohul (Student)

Palo Alto Site to Site VPN with Shared Secret keysLab

Mohul Sarkar

**Purpose:**

The purpose of a Site-to-Site VPN with Shared Secret keys in Palo Alto Networks is to establish a secure and encrypted communication channel between two or more sites over the Internet or any other untrusted network. This type of VPN is often used to connect remote offices, data centers, or cloud environments. The Shared Secret key is a pre-shared key that is used by both ends of the VPN tunnel to authenticate and establish a secure connection. It is a secret key that is known only to the participating devices and is used to encrypt and decrypt data transmitted over the VPN. This provides a secure and encrypted connection by using the IPsec protocol, which is an industry-standard protocol for secure communication over the Internet.

**Background Information on Lab Concepts:**

From previous labs, I know now how to use web interfaces to apply changes to firewalls proficiently. This lab introduces the idea of using 2 Palo Alto routers to secure the connection on both sides of the device. Many of the other labs utilized the same interface, so I have an easy time navigating through all of the settings.

**Lab Summary:**

A Palo Alto Site-to-Site VPN involves configuring a VPN tunnel between two Palo Alto Networks firewalls using a pre-shared key for authentication. The lab aims to provide a hands-on experience in configuring and verifying the Site-to-Site VPN tunnel. The lab typically involves configuring the network interfaces on the Palo Alto firewalls, including setting up IP addresses and subnets, creating the necessary security policies to allow traffic to flow between the two networks, configuring the IKE Gateway and IPSec tunnel on both firewalls, including configuring the pre-shared key and other settings such as encryption algorithms, hash algorithms, and lifetime settings and verifying the configuration by checking the IPSec and IKE status and verifying that traffic is flowing correctly between the two networks. The lab is designed to provide practical experience in configuring a Site-to-Site VPN on Palo Alto Networks firewalls. It also aims to develop skills in troubleshooting and verifying VPN connectivity and security settings.

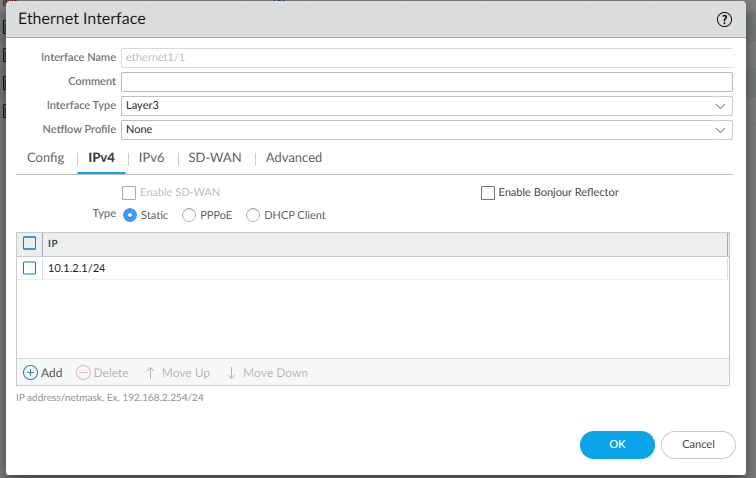
**Lab Commands:**

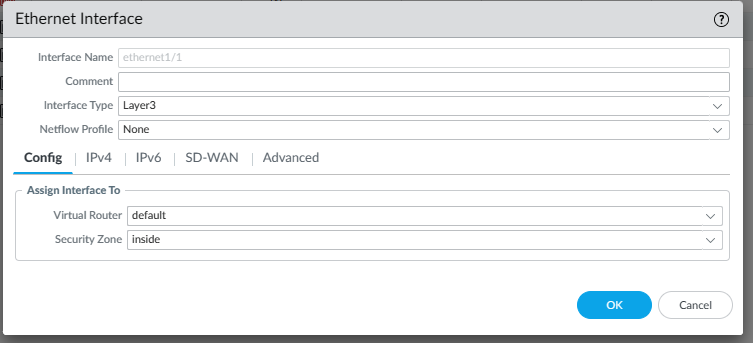
Step 1: Configure the Network Interfaces

The first step is to configure the network interfaces on both Palo Alto firewalls. This includes assigning IP addresses and configuring the subnets. To do this, follow these steps:

Log in to the Palo Alto firewall web interface.

Go to Network > Interfaces and click Add to create a new interface.

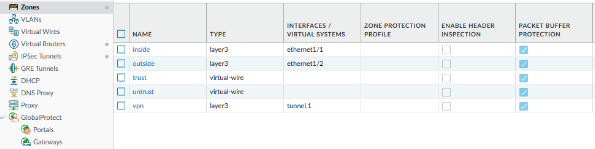




Assign an IP address to the interface and configure the subnet mask.

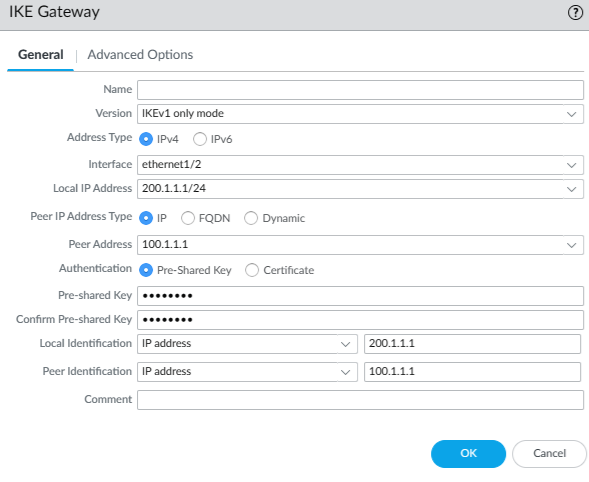
Configure the interface to use the correct zone (e.g., trust or untrust).

Repeat the steps for the other firewall.



Step 3: Configure IKE Gateway

The next step is to configure the IKE Gateway on both firewalls. The IKE Gateway defines the parameters for establishing the IKE phase 1 negotiation. To configure the IKE Gateway, follow these steps:

Go to Network > IKE Gateways and click Add to create a new IKE Gateway. 

Configure the IKE Gateway with the appropriate settings, including the peer IP address, pre-shared key and authentication method.

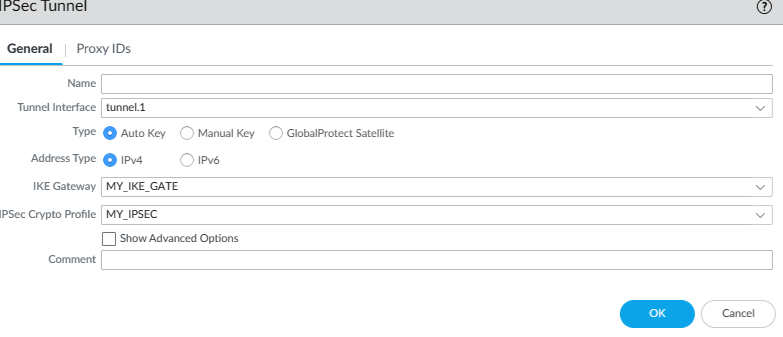
Click OK to save the configuration.

Repeat the steps for the other firewall.

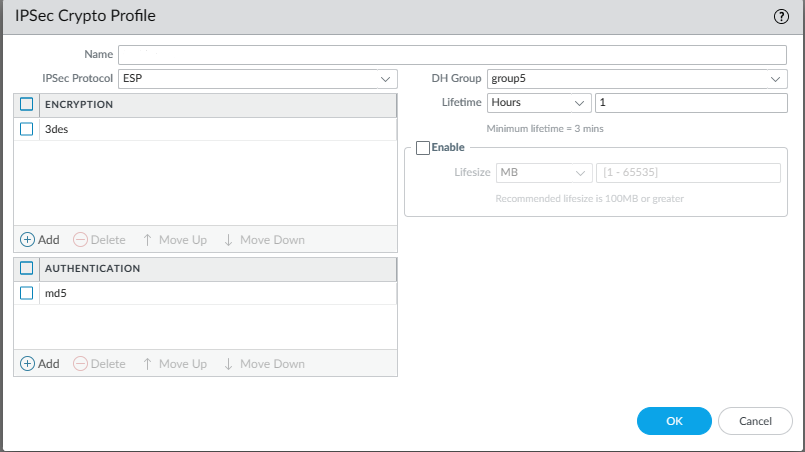
Step 4: Configure IPSec Tunnel

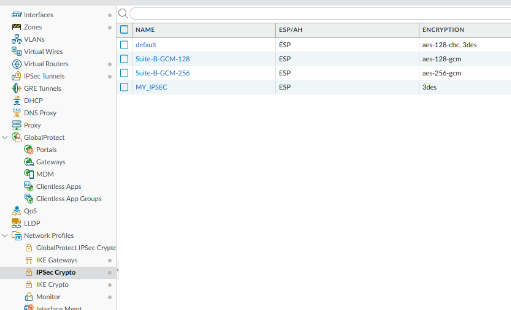
After configuring the IKE Gateway, the next step is to configure the IPSec tunnel on both firewalls. The IPSec tunnel defines the parameters for establishing the IPSec phase 2 negotiation. To configure the IPSec tunnel, follow these steps:

Go to Network > IPSec Tunnels and click Add to create a new IPSec tunnel.



Configure the IPSec tunnel with the appropriate settings, including the tunnel name and the IKE Gateway





Click OK to save the configuration.

Repeat the steps for the other firewall.

Step 5: Configure Pre-Shared Key

The final step is to configure the pre-shared key that will be used for authentication. To do this, follow these steps:

Go to Device > Local User Database and click Add to create a new user.

Enter a username and password for the user.

Click OK to save the configuration.

Go to Network > IKE Gateways and edit the IKE Gateway.

Enter the username and password for the user in the Pre-Shared Key field.

Click OK to save the configuration.

Repeat the steps for the other firewall.

Once you have completed these steps, you should be able to establish a Site-to-Site VPN with Shared Secret keys between the two Palo Alto Networks firewalls. You can verify the VPN status by checking the IPSec and IKE status, and by testing traffic flow between the two networks.

**Problems:**

While configuring a Palo Alto Site to Site VPN with shared secret keys, I encounter a problem with incorrect shared secret key. One of the most common issues while configuring a Site to Site VPN is entering an incorrect shared secret key. This can cause the VPN tunnel to fail to function, and I have to double-check the key and ensure that it is the same on both sides of the tunnel. Another issue I had was an IP address mismatch. During my configuration there was a mismatch between the local and remote endpoints. I may have to ensure that both endpoints have the correct IP addresses configured and that they can communicate with each other.

**Conclusion:**

My conclusion from configuring Palo Alto Site to Site VPN with Shared Secret keys is that configuring a VPN can be a complex task that requires attention to detail. The configuration of a VPN involves several different components, including shared secret keys, IP addresses, firewall rules and firmware versions. Each of these components must be configured correctly for the VPN to function properly. Configuring a VPN also requires a good understanding of networking concepts and protocols, such as IPsec, IKE, and NAT traversal. As a networking student, it is important to have a solid foundation in these concepts to be able to configure a VPN correctly. In addition, troubleshooting skills are essential when configuring a VPN, as there are many potential issues that can arise during the configuration process. It is important to be able to identify and troubleshoot these issues quickly to minimize downtime of the network and ensure that the VPN is functioning correctly.