

Palo Alto Site to Site VPN with Certificates

Evan Choi | Cisco Cybersecurity | 4/26/2023

**Purpose**

The purpose of this lab is to setup a two Palo Alto firewalls with certificates that authenticate the VPN connection between two or more networks. You must then be able to monitor a session on a Cisco switch using Wireshark, where you will be able to see the packets travelling through the tunnel. This lab is a addition to the Palo Alto Site to Site VPN with Shared Keys lab, where the process for configuring for the whole lab is the same expect this lab includes certificates.

**Background Information on lab concepts**

As this lab is exactly the same as the prior lab, expect the few steps on certificates, the background information needed is mostly the same. Since the background for both labs is so similar, I will be talking only about certificates and how they differ from shared keys. For information on the other parts of this lab, refer to the previous lab (Lab 8 - Palo Alto Site to Site VPN for Shared Keys).

In a site-to-site VPN, certificates provide are an authentication method that provides networks with a secure and encrypted channel of communication.

Each network that is in the VPN will have a digital certificate created for it, which usually use a public key infrastructure (PKI), including a public and private key. Once created, these certificates will be exchanged between the different networks in the VPN, which usually happens in the setup part of the VPN connection.

After exchanging certificates, each network will use its private key to sign all the outgoing data packets, and the receiving networks can use the public key in the certificate to verify that signature to make sure the data wasn’t intercepted or manipulated when travelling through the tunnel.

Shared keys and certificates are different methods of authentication that are used in site-to-site VPNs. Certificates use a public key infrastructure or PKI to establish authenticate the VPN connection. With certificates, each network has its own unique certificate that include a public and private key. The private key is used to sign outgoing data packets and the public key is used to verify that signature to make sure it wasn’t manipulated in travel. Shared keys, however, use a pre-shared key (PSK) that both sides of the VPN know, and this is used to encrypt and authenticate traffic going through the VPN.

Certificates are more complex to manage than shared keys since you need a PKI and you need to issue and manage certificates. Once the infrastructure is put in place however, managing certificates becomes easier than managing shared keys since each networks unique certificate can be replaced or removed when a network administrator needs to.

Although certificates are more complex to manage initially, they are more secure than shared keys since they have a complex mathematical algorithm that creates unique keys that are really had to guess through brute-force. Shared keys use one shared secret, making it way more probable to be vulnerable to brute-force attacks.

<https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-tls.html>

<https://www.ibm.com/support/pages/ipsec-pre-shared-keys-vs-certificates#:~:text=IPsec%20has%20two%20ways%20of,less%20secure%20than%20a%20certificate.&text=Pros%3A,process%20of%20obtaining%20a%20certificate>

<https://www.cloudflare.com/learning/ssl/tls-certificate-vs-shared-key/>

<https://www.thesslstore.com/blog/certificates-vs-pre-shared-keys-for-vpn-authentication/>

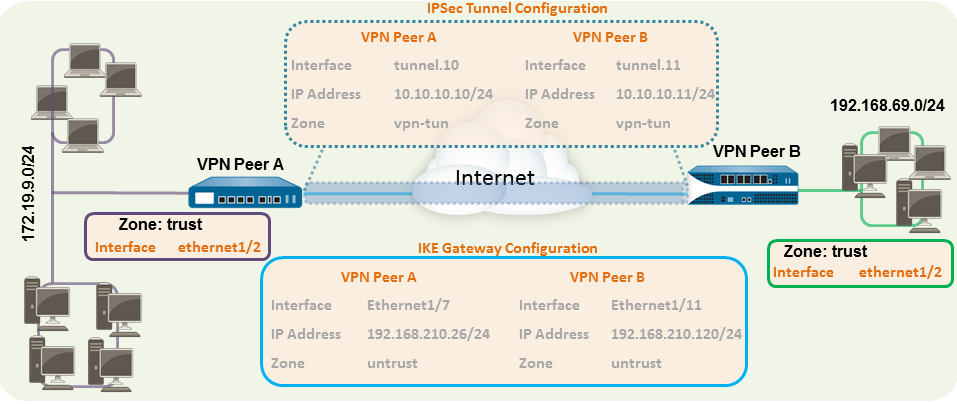
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/vpns/site-to-site-vpns/site-to-site-vpn-configuration-parameters/certificate-and-pre-shared-key-authentication.html>

**Lab Summary**

In this I set up two Palo Alto PA-410 firewalls to have a VPN connection using certificates. I used ethernet cable to connect to the management port of each firewall, where I used PuTTY and the management GUI to configure all the different things needed for the shared connection.

There were many different things I needed to configure in this lab, such as layer 3 interfaces, tunnel interfaces, static routes on virtual routers, crypto profiles, IKE Gateways, IPsec tunnels, and security policies.

**Network Diagram**



**Procedure**

1. In this lab there are two firewalls. I will call them VPN Peer A and VPN Peer B. This document was used during this lab. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-routing>
2. Type in <https://192.168.1.1> into your web browser, and the management GUI should appear. You will be prompted to enter standard mode or ZTP mode. Go into PuTTY and type the following command to enter standard mode: **set system ztp disable**

Graphical user interface

Description automatically generated with medium confidence

1. Now you will configure the Outbound Ethernet Interface. Go to **Network > Interfaces > Ethernet,** and select **ethernet ½.** Set the Interface Type to **Layer 3.** Configure the following on each firewall and in their respective tabs.

Graphical user interface, text, application, email

Description automatically generatedPeer A:

Config tab:

Ethernet: **1/2**

Security Zone: **untrust**

Virtual Router: **default**

IPv4 tab:

IP: **192.168.210.26/24**

Graphical user interface, text, application, email

Description automatically generatedPeer B:

Config tab:

Ethernet: **1/2**

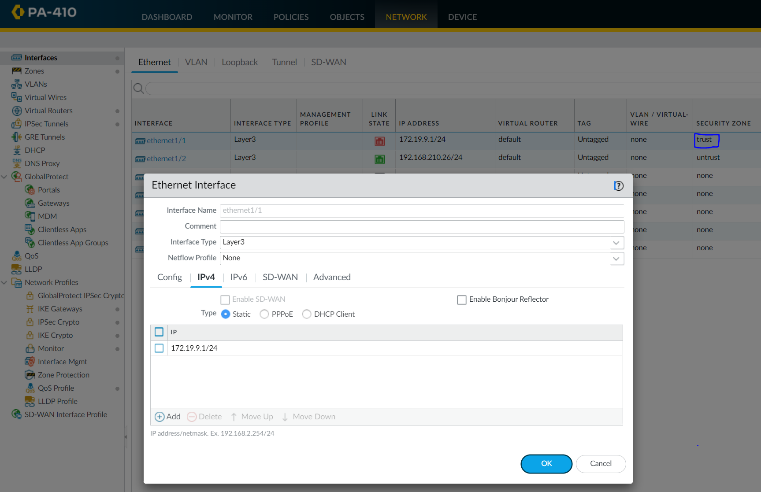
Security Zone: **untrust**

Virtual Router: **default**

IPv4 tab:

IP: **192.168.210.120/24**

1. Now you will configure the Inbound Ethernet Interface. Go to **Network > Interfaces > Ethernet,** and select **ethernet 1/1.** Set the Interface Type to **Layer 3.** Configure the following on each firewall and in their respective tabs.

Peer A:

Config tab:

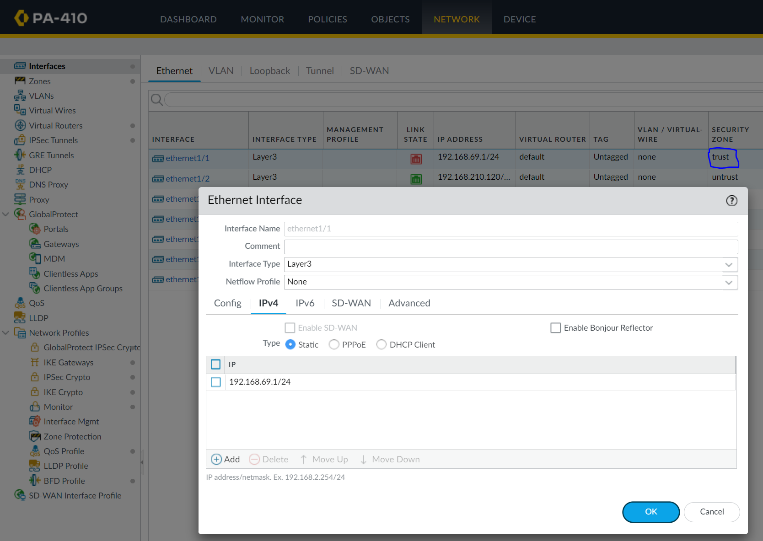
Ethernet: **1/1**

Security Zone: **trust**

Virtual Router: **default**

IPv4 tab:

IP: **172.19.9.1/24**

 Peer B:

Config tab:

Ethernet: **1/1**

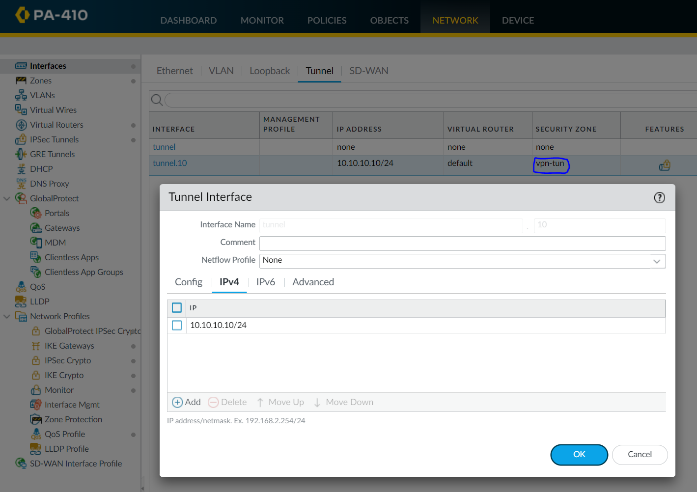
Security Zone: **trust**

Virtual Router: **default**

IPv4 tab:

IP: **192.168.69.1/24**

1. Now create the tunnel interface. Go to **Network > Interfaces > Tunnel,** and click the **Add** button. Configure the following on each firewall and in their respective tabs.

Peer A:

Config tab:

Interface: **tunnel.10**

Security Zone: **vpn\_tun**

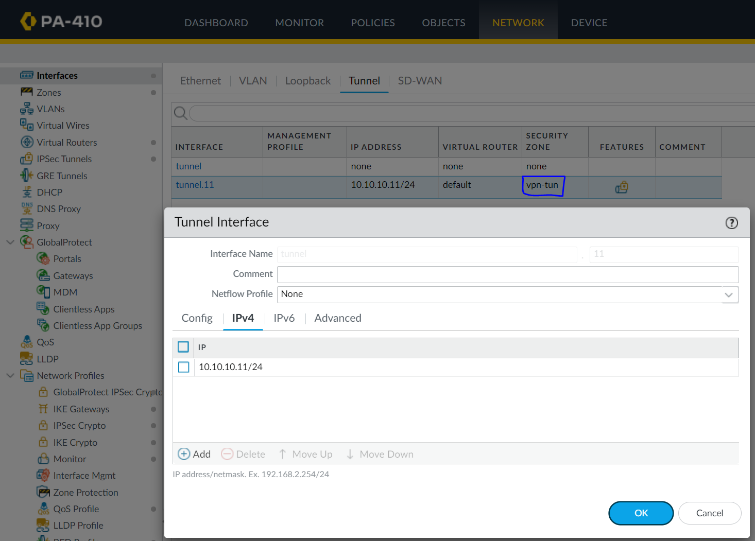
Virtual Router: **default**

IPv4 tab:

IP: **10.10.10.10/24**

Peer B:

Config tab:

Interface: **tunnel.11**

Security Zone: **vpn\_tun**

Virtual Router: **default**

IPv4 tab:

IP: **10.10.10.11/24**

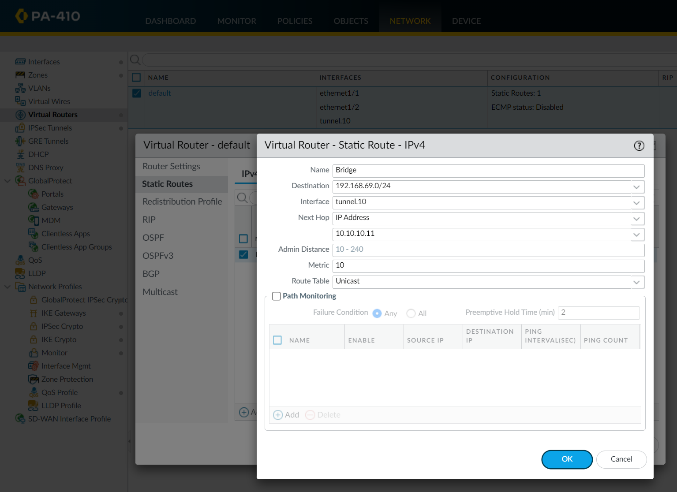
1. On both firewalls, your zones should be configured like the following:

Table

Description automatically generatedTable

Description automatically generated

1. Now you will configure a static route on the virtual router. Go to **Network > Virtual Router.** On the side click **Static Routes** and click **Add.**

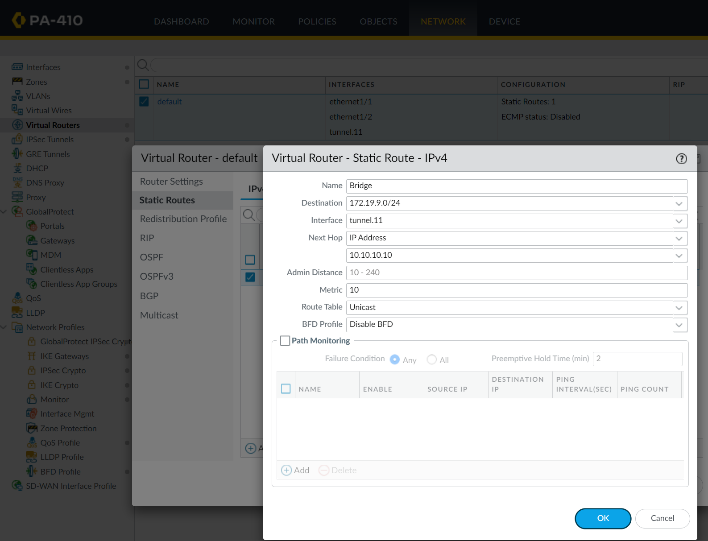
Peer A:

Name: **Bridge**

Destination: **192.168.69.0/24**

Interface: **tunnel.10**

Next Hop: **IP Address**; **10.10.10.11**

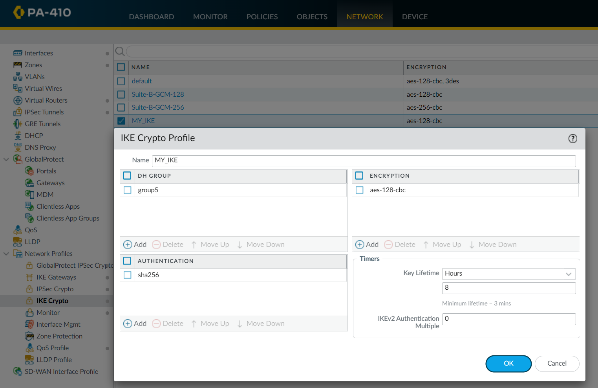
 Peer B:

Name: **Bridge**

Destination: **172.19.9.0/24**

Interface: **tunnel.11**

Next Hop: **IP Address**; **10.10.10.10**

1. Now, set up the IKE Crypto profile. Go to **Network > Network Profiles > IKE Crypto.**

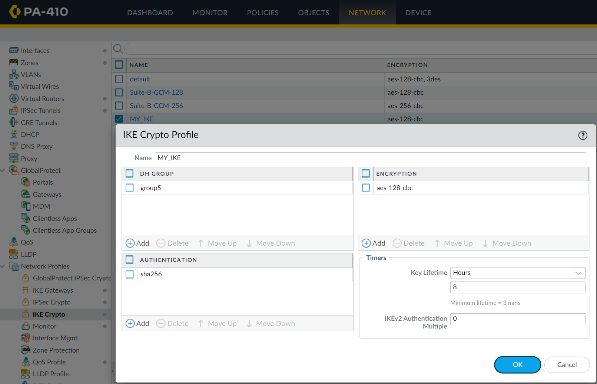
Peer A:

Name: **MY\_IKE**

Group: **group5**

Authentication: **sha256**

Encryption: **aes-128-cbc**

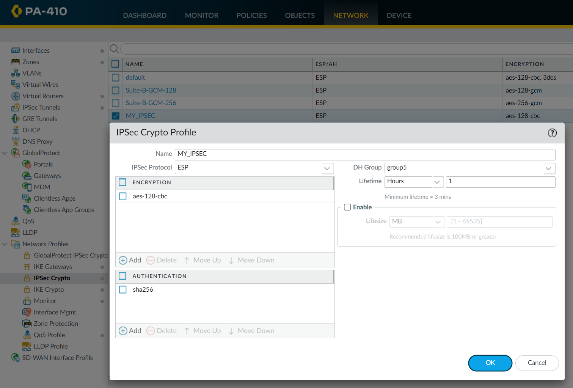
 Peer B:

Name: **MY\_IKE**

Group: **group5**

Authentication: **sha256**

Encryption: **aes-128-cbc**

1. Now, set up the IKE Crypto profile. Go to **Network > Network Profiles > IPSec Crypto.**

Peer A:

Name: **MY\_IPSEC**

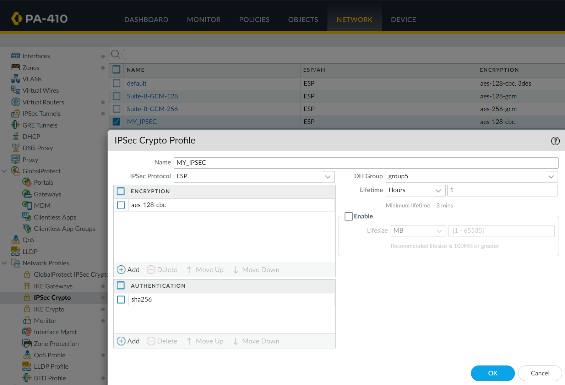
IPSec Protocol: **ESP**

DH Group: **group5**

Encryption: **aes-128-cbc**

Authentication: **sha256**

Peer B:

Name: **MY\_IPSEC**

IPSec Protocol: **ESP**

DH Group: **group5**

Encryption: **aes-128-cbc**

Authentication: **sha256**

1. Now, create security policies. Go to **Policies > Security.** Configure the following.

Peer A:

A screenshot of a computer

Description automatically generated

Peer B:

A screenshot of a computer

Description automatically generated

1. Go to **Device > Certificates** and click the **Generate** button at the bottom. Check the button next to **Certificate Authority** and configure the following:

Certificate Name: **Root\_CA\_VPN**

Common Name: **Root\_CA\_VPN**

Graphical user interface, application, table

Description automatically generated with medium confidence

1. Now, click the **Export Certificate** button at the bottom of the page, and do the following:

File Format: **Base64 Encoded Certificate (PEM)**

Check the box next to **Export private key**.

Passphrase (choose one you will remember and write it down): **JasoEvan**

Confirm Passphrase: **JasoEvan**

You should receive a file after pressing okay. Send that file to the computer connected to the other firewall.

Graphical user interface, text, application, email

Description automatically generated

1. Now go to your other firewall and import that Certificate into your peer firewall. Click the **Import** button at the bottom of the page and configure the following:

Certificate Name: **VPN\_Cert**

Certificate File: should be something ending in **cert\_VPN\_Root.pem**. It will be the file that was sent from the other computer.

File Format: **Base64 Encoded Certificate (PEM)**

Check the **Import private key** box.

Passphrase (will be the same as before): **JasoEvan**

Confirm Passphrase: **JasoEvan**

A screenshot of a computer

Description automatically generated

1. Now, you will create a Certificate Profile on both firewalls and add the CA certificate. Configure the following:

Graphical user interface, text

Description automatically generatedRoot side:

Name: **cert\_profile**

CA Certificates: **Root\_CA\_VPN**

Importing side:

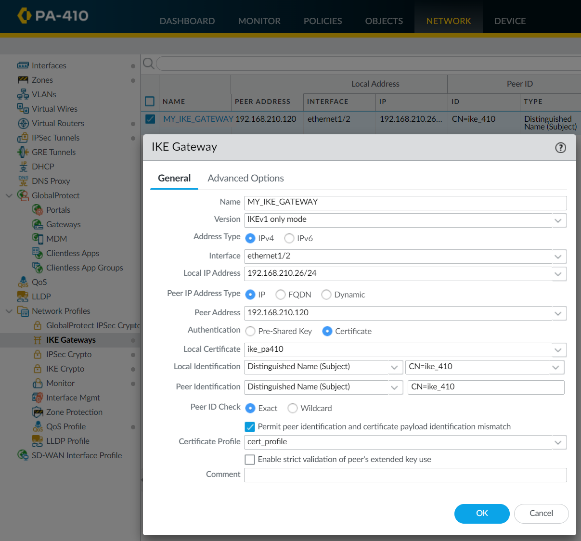
Graphical user interface, application

Description automatically generatedName: **cert\_profile**

CA Certificates: **VPN\_Cert**

1. Now setup the IKE Gateway. Go to **Network > Network Profiles > IKE Gateway.** Click **Add** on the bottom and configure the following:

Note: Set the pre-shared key to anything you can remember. It may limit you to 8 characters so choose a pre-shared key of 8 letters or less.

Importing Side:

Name: **MY\_IKE\_GATEWAY**

Version: **IKEv1 only mode**

Interface: **ethernet1/2**

Local IP Address: **192.168.210.26/24**

Peer Address: **192.168.210.120**

Authentication: **Certificate**

Local Certificate: **ike\_pa410**

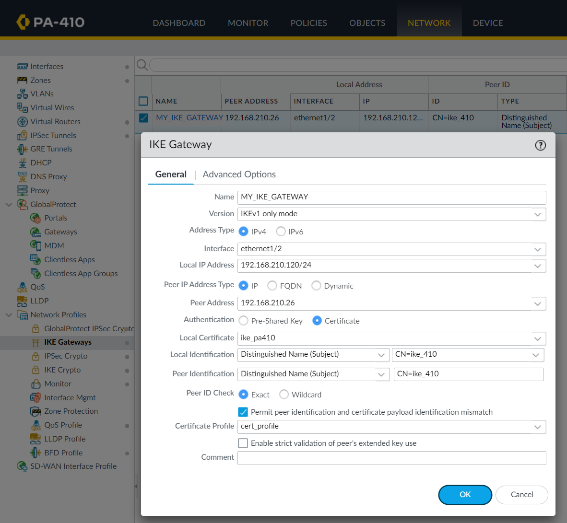
Local Identification: **Distinguished Name (Subject); CN=ike\_410**

Peer Identification: **Distinguished Name (Subject); CN=ike\_410**

Peer ID Check: **Exact**

Check the box next to **Permit peer identification and certificate payload identification mismatch.**

Certificate Profile: **cert\_profile**

 Peer B:

General

Name: **MY\_IKE\_GATEWAY**

Version: **IKEv1 only mode**

Interface: **ethernet1/2**

Local IP Address: **192.168.210.120/24**

Peer Address: **192.168.210.26**

Authentication: **Certificate**

Local Certificate: **ike\_pa410**

Local Identification: **Distinguished Name (Subject); CN=ike\_410**

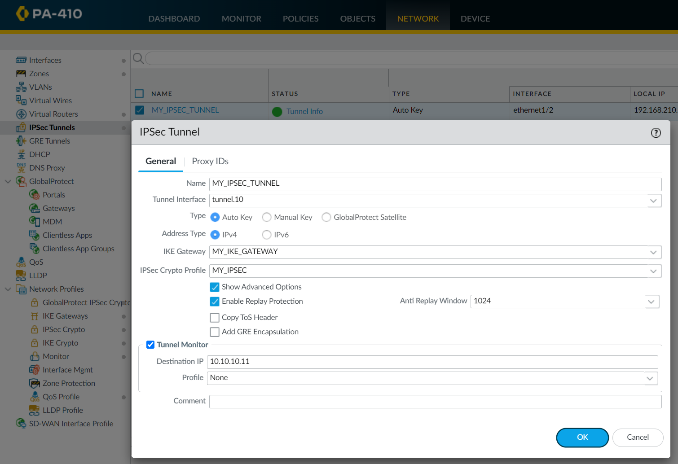
Peer Identification: **Distinguished Name (Subject); CN=ike\_410**

Peer ID Check: **Exact**

Check the box next to **Permit peer identification and certificate payload identification mismatch.**

Certificate Profile: **cert\_profile**

1. Now, setup the IPSec Tunnel. Go to **Network > IPSec Tunnels.** Click the **Add** button and configure the following on their respective firewalls.

Peer A:

Name: **MY\_IPSEC\_TUNNEL**

Tunnel Interface: **tunnel.10**

IKE Gateway: **MY\_IKE\_GATEWAY**

IPSec Crypto Profile: **MY\_IPSEC**

Destination IP: **10.10.10.11**

Peer B:

Name: **MY\_IPSEC\_TUNNEL**

Tunnel Interface: **tunnel.11**

IKE Gateway: **MY\_IKE\_GATEWAY**

Graphical user interface, text, application, email

Description automatically generatedIPSec Crypto Profile: **MY\_IPSEC**

Destination IP: **10.10.10.10**

1. Now, commit your changes on both firewalls.



1. After a successful commit, there should be a green light on the management GUI for both firewalls, indicating that the tunnel is up and working.

Peer A:

Graphical user interface, application, website

Description automatically generated

Peer B:

Graphical user interface, application, website

Description automatically generated

1. To test, you can ping the other firewall from your computer. Change the IP address to one that’s in the subnet and ping the IP address of another device on the other firewall.

Importing side:

Graphical user interface, text

Description automatically generated

1. Using another device with wireshark, you can trace the packets going through the tunnel. This can be done by plugging the device into a switch connected to the firewall and using two commands before pinging a device from one of your original computers. The commands are the ones that follow:

monitor session 1 source int f1/0/4

monitor session 1 destination int f1/0/2

You should be able to see packets traveling through the tunnel with the ESP protocol as we configured in step 9.

Table

Description automatically generatedA computer screen capture

Description automatically generated with medium confidence

Text

Description automatically generated

**Problems**

This lab only required a few steps, so there were not many problems we ran into. The problems we had configuring the parts up to certificates are listed in the Lab 8 – Palo Alto Site to Site VPN with Shared Keys.

The only problem we ran into this lab was when pinging to monitor traffic flowing through the tunnel. Before pinging, you enter the following commands, allowing you to monitor packets:

monitor session 1 source int f1/0/4

monitor session 1 destination int f1/0/2

When we entered the commands, instead of typing destination for the second command we typed source which cause the session monitoring to not work. After looking at our pings to see if something was wrong, we realized the second command said source instead of destination, and once we changed that we were able to monitor the different sessions.

**Conclusion**

Site-to-site VPN with certificates is a more secure way to provide networks with a secure and encrypted channel of communication. Throughout this lab, I was able to successfully configure Site-to-site VPN after configuring VPN tunnel interfaces, IPsec Crypto Profiles, IPsec Tunnel Interfaces, a security policy, certificates. Although I had some problems throughout this lab, I was able to troubleshoot them and eventually I was able to successfully ping through a tunnel and monitor traffic between it.

The stamp below recognizes that

Evan Choi

 has completed

**Lab 8 – Site to Site VPN with Certificates**



 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

         Period 5

