

Palo Alto Site to Site VPN with Shared Keys

Evan Choi | Cisco Cybersecurity | 4/26/2023

**Purpose**

The purpose of this lab is to setup a two Palo Alto firewalls to so they can have a VPN connection using shared keys. 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.

**Background Information on lab concepts**

Palo Alto is a company that offers next-generation firewalls and security solutions. Site-to-site VPN is a feature of Palo Alto firewalls that enables a secure communication between two different sites using static routes. The VPN tunnel part allows data transmitted between the two networks to be transmitted securely.

Site-to-site VPN is important for a variety of reasons. Mainly because it allows for a secure communication between two or more networks over the internet, which is very important for organizations and businesses that want to exchange important and sensitive information from two different locations. There are many other reasons site-to-site VPN including the following: security, connectivity, scalability, and cost effectiveness. Site-to-site VPN provides a secure and encrypted connection between two networks, which protects data from being access by unauthorized people. It can also help organizations extend their security policies to remote locations and help keep the same security measures between all locations. This makes site-to-site a very secure option. Site-to-site VPN also allows employees working remotely to access company resources and applications from other locations with a high level of security, allowing organizations to operate way more efficiently and effectively. Site-to-site is also very cost effective since it allows businesses to use the public internet for connectivity instead of buying dedicated lines for their company. Site-to-site also allows organizations to add and remove locations from the VPN network, making it a very good option in terms of scalability.

To set up site-to-site on Palo Alto firewalls you need to configure a variety of things which include VPN tunnel interfaces, IPsec Crypto Profiles, IPsec Tunnel Interfaces, and a security policy.

A VPN tunnel interface is a virtual interface that establishes an encrypted and secure connection between two networks. There are many things that are needed to make it work. Each side of a VPN connection is configured with a VPN tunnel interface and will have a local interface and a remote interface. The tunnel interface also needs to be configured with encrypted algorithms and authentications protocols, so data transmitted is secure. You then need to establish a tunnel between them which is done by created a shared secret key that both networks use so it can encrypt and decrypt data that is transmitted through the tunnel. After the tunnel is established, data should be able to be transmitted through the two networks.

IPsec Crypto profiles, or an Internet Protocol Security profile, specifics how data is secured within a tunnel when Auto Key IKE is used to generate keys for IKE SAs. IPsec profiles can be configured within the GUI. They are created on the VPN device that initiates the VPN connection and it will define the security settings used to establish the VPN tunnel. Profiles can include many things like encryption algorithm, key exchange methods, integrity algorithms, etc. After being initiated, the VPN gateway on one side will send its IPsec profile to the other device. The device that receives this IPsec profile will use that profile to configure its security settings in the VPN tunnel. The device will check if the IPSec profiles on both sides of the tunnel are the same, and if they are a VPN tunnel will be established and traffic will be able to pass through them. However, if they are not the same, a VPN tunnel will not be established, and any VPN connection will fail.

IPsec tunnel interfaces or VTIs are a newer method to configure site-to-site IPSec VPNs. They provide a routable interface type for terminating IPsec tunnels and provide a simple way set a definition for protection between sites to form a network. They establish a secure tunnel between two networks over the Internet, and by using IPsec protocols, it can encrypt and authenticate the traffic that goes through the tunnel. They are first configured on both sides of the VPN connection, with both sides having a local and remote interface. It is configured with security settings like encryption algorithms and authentication protocols that make traffic going through the tunnel secure. After being configured, the two sides establish a secure tunnel between them by using a shared secret key that encrypts and decrypts traffic going through the tunnel. When a secure tunnel becomes established, data going through the IPsec VTI will be received by the remote interface on the receiving side where it will be decrypted.

Security policies are a defined set a rule that determine how an organization wants to protect its assets from unauthorized access. All traffic that passes through a firewall is matches with a session and each session is matched with a Security policy rule. When this occurs, the firewall applies the matching Security policy rule, and if the traffic doesn’t match any defined rules, the default rules will apply to it. A security policy defining the rules for traffic that is and isn’t allowed to pass through the firewall is first created. Each security policy will consist of certain criteria like source and destination IP addresses, application, user, and other different attributes. This criterion will be matched against every packet that passes through the firewall, and if it fits the criteria it will pass.

<https://www.cbtnuggets.com/blog/technology/networking/how-ipsec-site-to-site-vpn-tunnels-work>

<https://docs.sophos.com/nsg/sophos-firewallmanager/v17.0.0/Help/en-us/webhelp/onlinehelp/index.html#page/onlinehelp/VPNPolicyManage.html>

<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>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns/set-up-site-to-site-vpn/define-cryptographic-profiles/define-ipsec-crypto-profiles>

<https://networklessons.com/cisco/ccie-routing-switching-written/ipsec-static-virtual-tunnel-interface#:~:text=IPSec%20VTIs%20(Virtual%20Tunnel%20Interface,define%20what%20traffic%20to%20encrypt>.

<https://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtIPSctm.html>

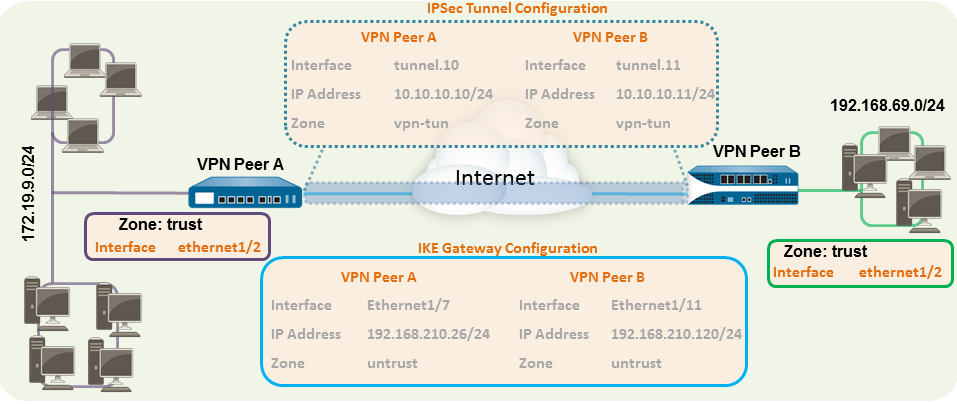
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-policy>

**Lab Summary**

In this I set up two Palo Alto PA-410 firewalls to have a VPN connection using shared keys. 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 a 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**

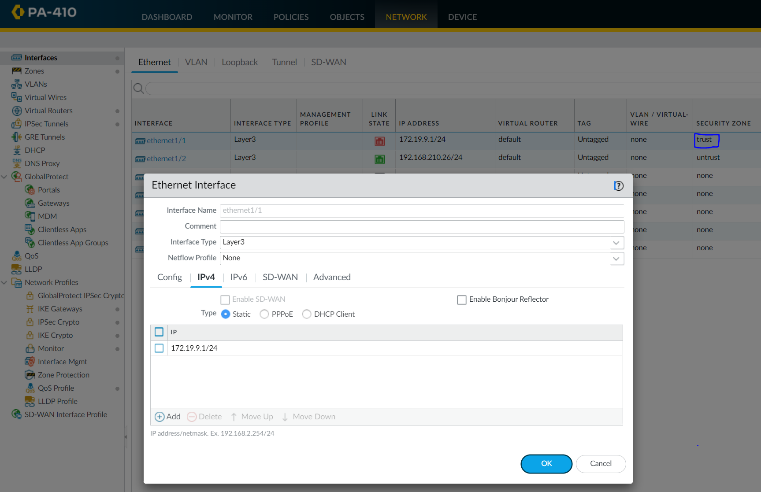
Security Zone: **untrust**

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:

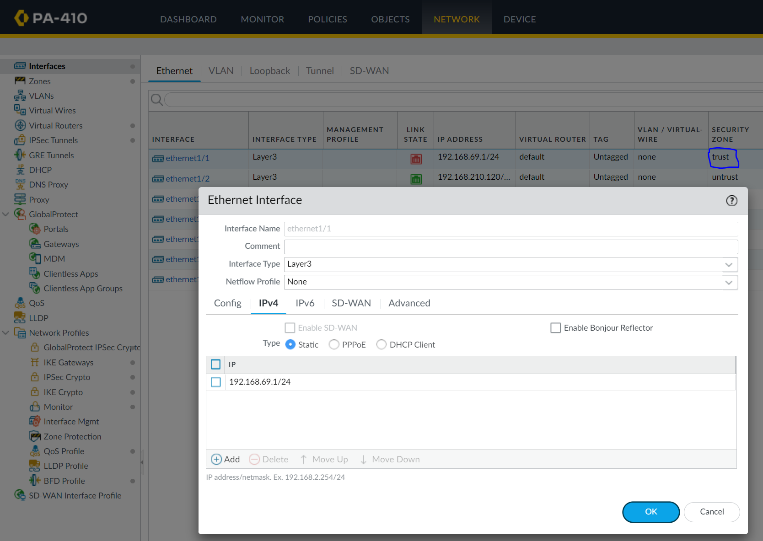
Ethernet: **1/1**

Security Zone: **trust**

Virtual Router: **default**

IPv4 tab:

IP: **172.19.9.1/24**

 Peer B:

Config tab:

Ethernet: **1/1**

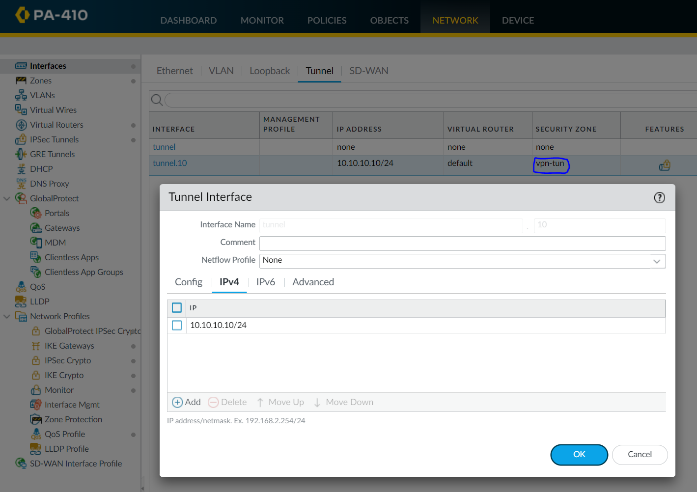
Security Zone: **trust**

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**

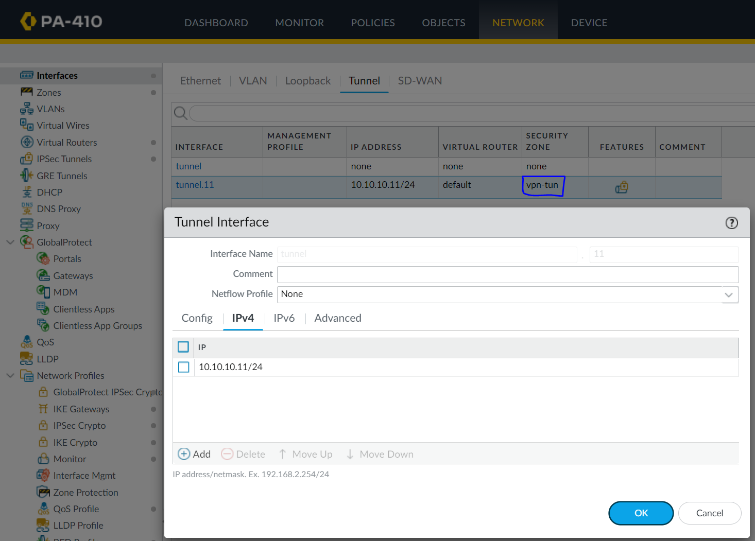
Virtual Router: **default**

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**

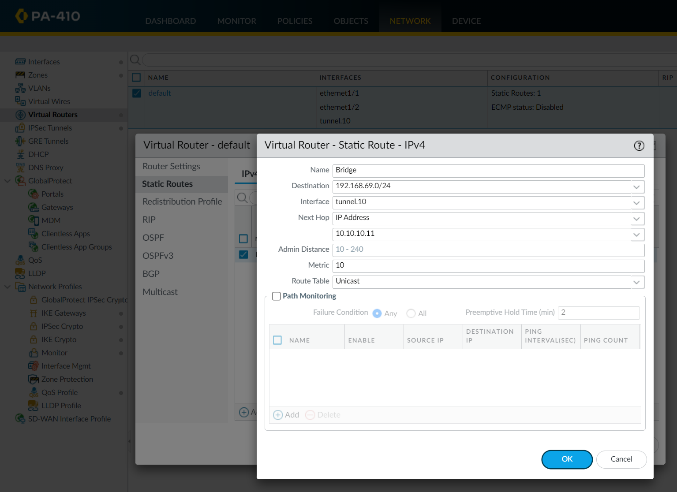
1. On both firewalls, your zones should be configured like the following:

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.**

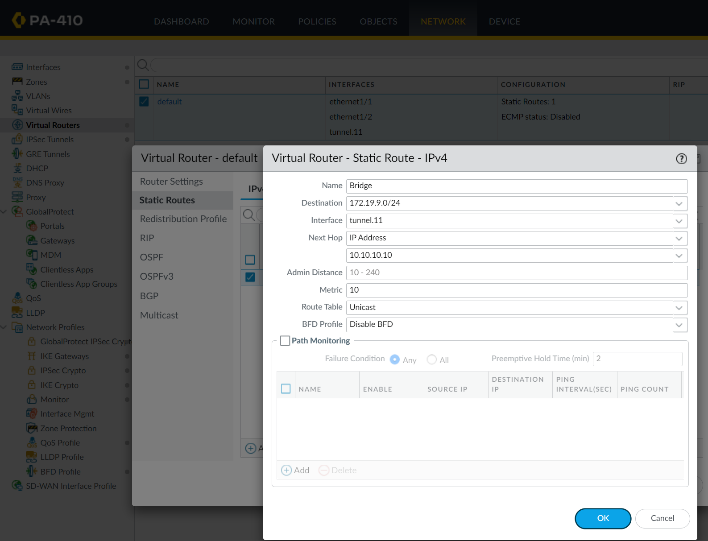
Peer A:

Name: **Bridge**

Destination: **192.168.69.0/24**

Interface: **tunnel.10**

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

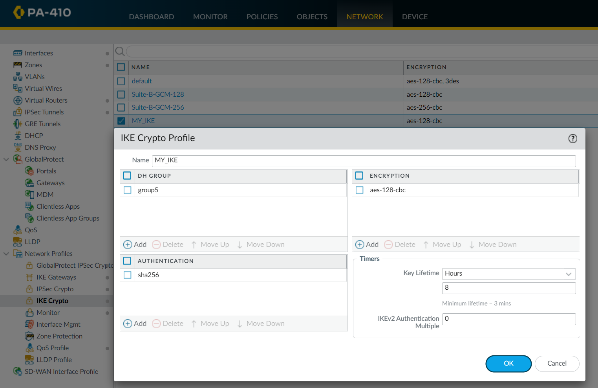
 Peer B:

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.**

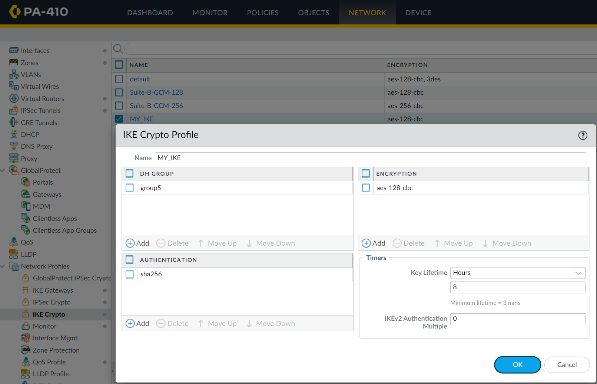
Peer A:

Name: **MY\_IKE**

Group: **group5**

Authentication: **sha256**

Encryption: **aes-128-cbc**

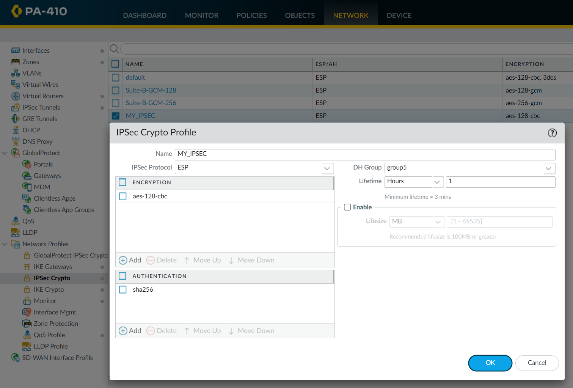
 Peer B:

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**

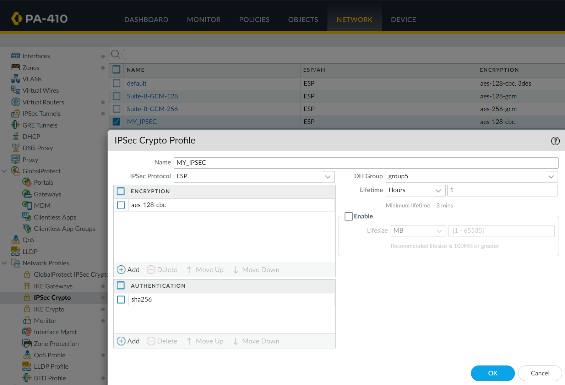
IPSec Protocol: **ESP**

DH Group: **group5**

Encryption: **aes-128-cbc**

Authentication: **sha256**

Peer B:

Name: **MY\_IPSEC**

IPSec Protocol: **ESP**

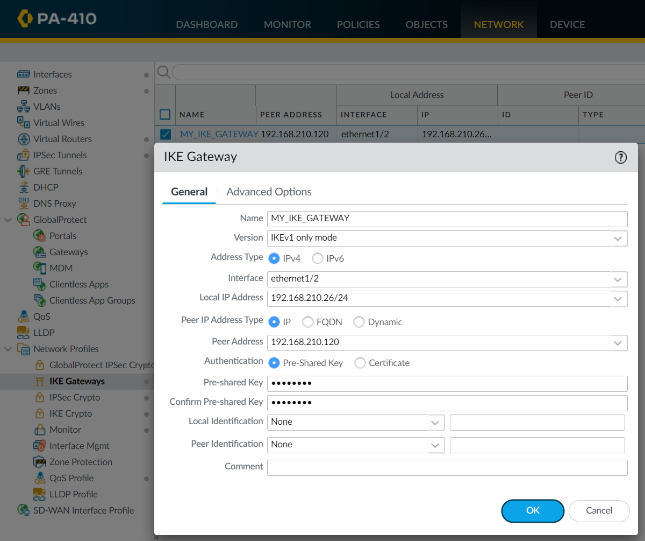
DH Group: **group5**

Encryption: **aes-128-cbc**

Authentication: **sha256**

1. Now setup the IKE Gateway. Go to **Network > Network Profiles > IKE Gateway.** Click **Add** on the bottom and configure the following in their respective tabs (General and Advanced Options):

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.

Peer A:

General

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**

Graphical user interface, text, application

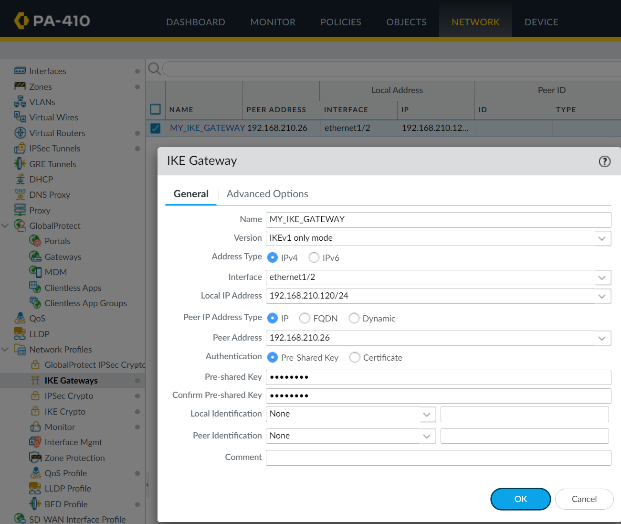
Description automatically generatedPre-shared Key: **JasoEvan**

Confirm Pre-shared Key: **JasoEvan**

Advanced Options

Exchange Mode: **auto**

IKE Crypto Profile: **MY\_IKE**

 Peer B:

General

Name: **MY\_IKE\_GATEWAY**

Version: **IKEv1 only mode**

Interface: **ethernet1/2**

Local IP Address: **192.168.210.120/24**

Graphical user interface, text, application

Description automatically generatedPeer Address: **192.168.210.26**

Pre-shared Key: **JasoEvan**

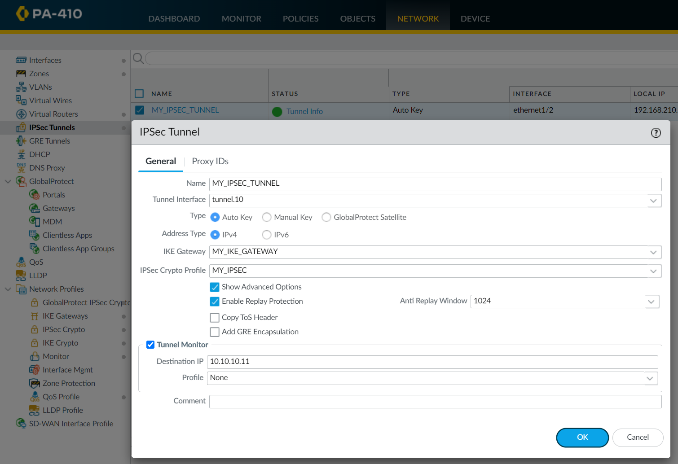
Confirm Pre-shared Key: **JasoEvan**

Advanced Options

Exchange Mode: **auto**

IKE Crypto Profile: **MY\_IKE**

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, 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. 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.

Peer A:

Graphical user interface, text

Description automatically generated

Peer B:

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 pinging a device from one of your original computers. You should be able to see packets traveling through the tunnel with the ESP protocol as we configured in step 9.

Text

Description automatically generatedTable

Description automatically generated

**Problems**

As there are many different parts of Site-to-site VPN, we ran into many problems. Some problems were configuration problems, and some were physical hardware problems. Some of them took a lot of effort to troubleshoot, even starting with a new IP scheme.

One of the first problems we ran into was that our configuration was invalid as the default wire was missing on one or more interfaces. To solve this, you must simply delete the virtual wire.

When configuring, we ran into a problem with authentication and encryption. Initially we configured md5 for our authentication and DES for our encryption. We figured out that we must have an authentication of at least sha256, and an encryption of at least aes.

We also ran into an issue entering our pre-shared keys. Our initial password for it was over 8 characters, and after committing and our changes not committing, we figured out that the pre-shared key password had a max of 8 characters, so we set the password to 8 characters instead of 9.

For the lab, we were using a Palo Alto PA410 and a Palo Alto PA220. However, after doing our configurations on them, it didn’t work, so we tried using two PA410’s instead. After making this change in addition to IP scheme changes, we were able to get site-to-site working.

To do this lab, we did research and found a source on how to do the lab. We used an IP scheme similar to their, but it didn’t work, so we decided to change our whole IP scheme, and after doing that, our lab worked.

Another part of this lab was session monitoring. We did not have another laptop to do session monitoring on, so we had to borrow a laptop from another group. Since that laptop had pfSense installed on it, we had to wipe the whole computer and install a fresh copy of windows on it using a windows media creation tool.

When we were trying to ping the firewalls for session monitoring, the pings didn’t work, and after looking it up online, we figured out that we had to turn Wi-Fi off to make it work.

**Conclusion**

Site-to-site VPN is an important Palo Alto feature that allows for a secure communication between two or more networks over the internet. Throughout this lab, I was able to successfully configure Site-to-site VPN after configuring VPN tunnel interfaces, IPsec Crypto Profiles, IPsec Tunnel Interfaces, and a security policy. Although I had many 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 Shared Keys**



 Adv Cisco Cybersecurity – Mr. Mason & Mr. Hansen

         Period 5

