Palo Alto Site to Site VPN with Certificates

Reed Holman | Cybersecurity | 3/30/2023



Purpose:

To configure a Site-to-Site VPN using Certificates

Background:

A VPN or a Virtual Private Network is a way to have a secure connection between different devices or networks. There were many different types of VPNs with different uses like Remote access, site-to-site, etc. VPNs are very useful for using a public network and wanting to access the internet securely.

Site-to-Site means that there is an encrypted connection between two networks. Site-to-Site is the protected and encrypted link usually between a branch office and the corporate network. Most companies have outgrown the need for site-to-site VPNs because they have started to move lots of their data to the cloud and they now have many employees using mobile devices. That means that it is no longer necessary to force all the data to go back to a data center and instead everyone can just access it in the cloud. Site-to-site can be hard to scale with that many moving variables, but it still has its uses. A remote access VPN is different because that connection is temporary and is most commonly used to gain secure access to a data center.

In this Lab instead of a pre-shared key we used self-signed certificates. Certificates are another way of authenticating and establishing a secure connection between networks.

Diagram:

Diagram

Description automatically generated

Configurations:

Create a Layer3 zone called inside

Graphical user interface, application

Description automatically generated

Create another zone called outside

Graphical user interface, text, application, email

Description automatically generated

Create the VPN zone

Graphical user interface, text, application, email

Description automatically generated

Configure the ethernet 1/1 interface

Graphical user interface, text, application, email

Description automatically generated

Configure with Ip address

Graphical user interface, text, application, email

Description automatically generated

Configure the 1/2 ethernet interface

Graphical user interface, text, application, email

Description automatically generated

Configure with Ip address

Graphical user interface, text, application, email

Description automatically generated

Create a tunnel

Graphical user interface, text, application, email

Description automatically generated

Set Ip address on tunnel

Graphical user interface, text, application, email

Description automatically generated

Create a default route

Graphical user interface, application

Description automatically generated

Create a static route goes to the other end of tunnel

Graphical user interface, text, application, email

Description automatically generated

REPEAT theses steps on the PA-210

Then create a security policy

Graphical user interface, text, application, email

Description automatically generated

Set the correct source zones

Graphical user interface, text, application

Description automatically generated

Set the correct destination zones

Graphical user interface, text, application

Description automatically generated

Repeat those steps on PA-220

Create an IKE crypto profile using correct encryption and authentication

Graphical user interface, application, email

Description automatically generated

Create an IPSec crypto profile using correct encryption and authenticationGraphical user interface, application

Description automatically generated

Generate a new root certificate

Graphical user interface, text, application, email

Description automatically generated

Export the certificate onto your PC

Graphical user interface, text, application

Description automatically generated

Import certificate to the other firewall

Graphical user interface, text, email

Description automatically generated

Generate new certificate on each firewallGraphical user interface, text, application, email

Description automatically generated

Graphical user interface

Description automatically generated

Create certificate profile on each firewall

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Create an IKE Gateway that uses the new certificate

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Create an IPsec tunnel

Graphical user interface, text, application, email

Description automatically generated

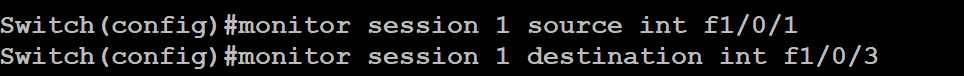
REPEAT Steps on PA-220

Go into router and configure the interfaces with IP address

Text

Description automatically generated

Use the monitor commands on the switch



Problems:

This lab was very similar to the past lab. However, our tunnel interface would not turn on, it was stuck in the in the off state. At first, we thought we messed up something in the configuration of tunnel. So, we spent some time double checking everything and we could not see anything wrong with our configuration on the firewalls. The issue however was that we did not do the test tunnel commands on the firewall and after we did those the tunnel was no longer off.