SITE TO SITE VPN WITH Certificates

By: Jordan Abu-Zahra

**Purpose:**

In this lab we used 2 different Palo Alto firewalls including the PA220 and the PA410 for our site-to-site VPN set up and set it up on the web interface. We learned how to set up site to site and how certificates work.

**Background:**

Site-to-Site VPN (Virtual Private Network) is a type of VPN connection that allows two or more sites or networks to securely connect with each other over the internet. In the traffic between the two sites are encrypted and travels over a public network such as the internet to create a secure private connection. Some important aspects to Site-to-Site VPNs are Authentication and Encryption: Site-to-Site can use authentication and encryption to protect the data that is transmitted between the two network. This is usually done using a combination of secure tunneling protocols, such as IPsec, IKE, and encryption algorithms such as AES. Network topology, since two networks are connection through a CPN gateway or router at each site. The VPN gateways or routes must be configured to establish and maintain the VPN connection, and to route traffic between the two networks. Internet connection, since Site-to-Site VPNs use the internet to transmit data between the wo networks, the quality of the internet connection is an important factor to consider. Factors such as bandwidth, latency and reliability can all impact the performance and reliability of the VPN connection. Security all VPNS should be configured with strong security policies and protocols to ensure that the connection remains secure. This includes implementing firewall rules, access control lists, and other security measures to prevent unauthorized access and protect against threats such as malware or hacking attempts. But for this lab specifically we used Certificates. Certificates are digital documents that is issued by a trusted authority, know as a certificate authority and it contains information about the identity of the certificate holder, such as their name, address and public key but for VPNS certificate are used to verify the identity of the VPN client and server during the initial phase of the VPN connection establishment. And the client and the server exchanger their certificates and use them to establish a secure and encrypted communication channel between them.

Network Diagrams with IP

Diagram

Description automatically generated

Configurations

Step 1: Reset firewalls. Set up a topology like what is shown in Network Diagrams with IP. We used Palo Alto firewalls in this lab rather than Cisco ASAs. We also included a layer 2 device between the Palo Alto 410 and the Router.

Step 2: Connect to the management interface of the 410 and manually set IP address of the end device to 192.168.1.2 255.255.255.0 and access <https://192.168.1.1>

Step 3: log in with user: admin and password: admin. Create a more secure password and disable ZTP.

Step 4: Configure the following

Graphical user interface, application

Description automatically generated

Step 5: Create another zone

Graphical user interface, text, application, email

Description automatically generated

Step 6: Create another zone

Graphical user interface, text, application, email

Description automatically generated

Step 7: Delete the virtual wires. Go to Policies and delete any preconfigured ZTP rules

Step 8: Configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 9: Configure the following in the IPv4 tab

Graphical user interface, text, application, email

Description automatically generated

Step 10: configure the other interface

Graphical user interface, text, application, email

Description automatically generated

Step 11: Configure the following in the IPv4 tab

Graphical user interface, text, application, email

Description automatically generated

Step 12: create a new tunnel

Graphical user interface, text, application, email

Description automatically generated

Step 13: set an IPv4 address on the tunnel (not required for site-to-site).

Graphical user interface, text, application, email

Description automatically generated

Step 14: create a default route

Graphical user interface, application

Description automatically generated

Step 15: create a route to the network on the other side of the tunnel

Graphical user interface, text, application, email

Description automatically generated

Step 16: Commit changes. While it is committing changes, console into the PA210

Step 17: create a new zone

Graphical user interface, application

Description automatically generated

Step 18: create another new zone

Graphical user interface, text, application

Description automatically generated

Step 19: create another new zone

Graphical user interface, text, application

Description automatically generated

Step 20: configure the interface

Graphical user interface, text, application, email

Description automatically generated

Step 21: give the interface an IP address

Graphical user interface, text, application, email

Description automatically generated

Step 22: configure the other interface

Graphical user interface, text, application, email

Description automatically generated

Step 23: give the interface an IP address

Graphical user interface, text, application, email

Description automatically generated

Step 24: create a new tunnel

Graphical user interface, text, email

Description automatically generated

Step 25: give the tunnel an IP address (once again, note required for site-to-site)

Graphical user interface, text, application, email

Description automatically generated

Step 26: create a default route

Graphical user interface, application

Description automatically generated

Step 27: create a route to the network on the other side of the VPN Graphical user interface, text, application, email

Description automatically generated

Step 28: commit changes. While committing, console back into 410. Ensure that the previous configurations successfully committed.

Step 29: create a security policy rule

Graphical user interface, text, application, email

Description automatically generated

Step 30: set source zones

Graphical user interface, text, application

Description automatically generated

Step 31: set destination zones

Graphical user interface, text, application

Description automatically generated

Step 32: Commit changes and console back into the 220 and ensure that changes have successfully committed.

Step 33: create new security policy rule

Graphical user interface, text, application, email

Description automatically generated

Step 34: set source zones

Graphical user interface, text, application, email

Description automatically generated

Step 35: set destination zones

Graphical user interface, text, application

Description automatically generated

Step 36: commit changes and console back into the 410. Ensure that the commit was completed successfully.

Step 37: Create an IKE crypto profile. Make sure an adequate encryption and authentication are used. Graphical user interface, application, email

Description automatically generated

Step 38: Create and IPSec crypto profile. Make sure an adequate encryption and authentication are used.

Graphical user interface, application

Description automatically generated

Step 39: Generate a root certificate

Graphical user interface, text, application, email

Description automatically generated

Step 40: Export certificate

Graphical user interface, text, application

Description automatically generated

Step 41: Import root certificate

Graphical user interface, text, email

Description automatically generated

Step 42: generate certificate

Graphical user interface, text, application, email

Description automatically generated

Step 43: generate certificate on other firewall

Graphical user interface

Description automatically generated

Step 44: create certificate profile

Graphical user interface, text, application

Description automatically generated

Step 45: create certificate profile on the other firewall

Graphical user interface, text, application

Description automatically generated

Step 47: Create an IKE gateway using the certificate that was generated

Graphical user interface, application

Description automatically generated

Step 48: configure the following

Graphical user interface, text, application

Description automatically generated

Step 49: Create the IPsec tunnel

Graphical user interface, text, application, email

Description automatically generated

Step 50: commit changes and console into 220 and ensure the previous commit was successful

Step 51: Create an IKE crypto profile. Ensure that adequate authentication and encryption methods are used.

Graphical user interface, text, application, email, website

Description automatically generated

Step 52: Create an IPSec crypto profile. Ensure that adequate encryption and authentication methods are used.

Graphical user interface, application, email

Description automatically generated

Step 53: Create an IKE gateway. Use previously created certificate as authenticate method.

Graphical user interface, application

Description automatically generated

Step 54: Configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 55: Create the IPSec tunnel

Graphical user interface, text, application

Description automatically generated

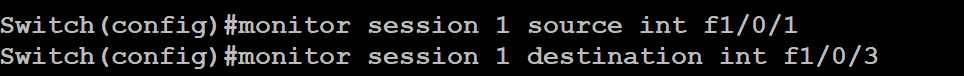
Step 56: Console into the router and configure the following (set IP address on interfaces and activate them).

Text

Description automatically generated

Step 57: Console into the switch. Connect f1/0/1 to the firewall and f1/0/2 to the router. Connect f1/0/3 to a pack sniffer (PC running Wireshark).

Step 58: Configure the following



Access the management interface of either firewall and ensure that IPSec tunnel status is green. Sometimes some tunnel takes a moment to activate. If it remains inactive, try using the “enable” button on the bottom left. If that doesn’t work, console the firewall and issue these commands and ensure that these are the outputs:

admin@PA-410> test vpn ike-sa

Start time: Feb.09 13:08:23

Initiate 1 IKE SA.

admin@PA-410> test vpn ipsec-sa

Start time: Feb.09 13:08:30

Initiate 1 IPSec SA.

These should appear the monitor after the two previous commands are issued:

Calendar

Description automatically generated with low confidence

To ensure functionality of the site-to-site VPN, disable the windows defender firewall on both end devices or create a rule to allow for pings. Ping from one end device to another. These should be the outputs:

C:\Users\user>ping 10.1.2.2

Pinging 10.1.2.2 with 32 bytes of data:

Reply from 10.1.2.2: bytes=32 time=2ms TTL=126

Reply from 10.1.2.2: bytes=32 time=2ms TTL=126

Reply from 10.1.2.2: bytes=32 time=2ms TTL=126

Reply from 10.1.2.2: bytes=32 time=2ms TTL=126

Ping statistics for 10.1.2.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\user>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=2ms TTL=126

Reply from 10.1.1.2: bytes=32 time=2ms TTL=126

Reply from 10.1.1.2: bytes=32 time=2ms TTL=126

Reply from 10.1.1.2: bytes=32 time=2ms TTL=126

Ping statistics for 10.1.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 2ms, Average = 2ms

The packet sniffer capturing traffic on the layer 2 device should also capture traffic. If using Wireshark and filter for ESP traffic.

Table

Description automatically generated

Problems:

No problems

Conclusion:

In this lab I learned how to set up a Site to Site VPN with a self-assigned certificate