**Palo alto Site to Site VPN (shared key)**

Derek Liu Cybersecurity Period 5

**Implementing Site-to-Site VPN**

*Derek Liu*

Purpose

The purpose of this lab is to create a site-to-site VPN with a pre-shared key and verify the existence of the VPN using a packet sniffer and capture VPN packets being sent across the network.

Background Information

A site-to-site VPN is a type of connection that encrypts traffic to create secure communications between two different networks. Site-to-site VPNs are useful when connecting networks from different locations over the internet while preventing unauthorized access or interception of data traffic through encryption.

An important protocol suite that provides security for IP communications over untrusted networks is IPsec or internet protocol security. IPsec is used to encrypt, decrypt, and authenticate IP packets in a VPN. Two services in IPsec are the authentication header (AH) and the encapsulation security payload (ESP). The authentication header provides authentication for the packet while the encapsulation security payload encrypts the data so if the packet is intercepted, it cannot be read. In this lab, we will intercept ESP packets but will not attempt to decrypt them.

In terms of encryption and hashing in this lab, we used AES256 and SHA512. AES256 is a symmetric encryption algorithm that used a 256-bit encryption key. This encryption method is widely used and considered one of the strongest encryption methods available today (2023). We used SHA512 as the cryptographic hash function that produces an output of 512 bits. It is a more secure version of SHA256 and is also widely used in security protocols.

Site-to-site VPNs work by establishing an IPsec tunnel between two separate networks usually using the internet as a medium of transporting data traffic. Traffic is encrypted in the first gateway and decrypted at the second. The gateways in this lab were the Palo Alto firewalls. The gateways authenticate by using a pre-shared key.

However, it is also important to keep in mind that regardless of strength all encryptions are still vulnerable to attacks given that the attacker has enough time and resources to crack the encryption. Additionally, advancements in technology and research in cryptography can render current encryption methods obsolete or vulnerable in the future.

VPNs can be used for more than just securing data traffic. Some notable examples include masking you public IP address and your location, access restricted content or services that are blocked in certain countries, reducing the cost of communication without the cost of dedicated infrastructure, and allowing for workers to securely access corporate network resources while being at home or travelling.

Lab Summary

This lab was completed using static routes on the interfaces. The lab was relatively straightforward with minimal problems. Connection across the network was verified with pings and the IPSec tunnel was verified as function by capturing ESP packets that were being transmitted between the two firewalls.

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: Create an IKE gateway and set your pre-shared keyGraphical user interface, application

Description automatically generated

Step 40: configure the following

Graphical user interface, text, application

Description automatically generated

Step 41: Create the IPsec tunnel

Graphical user interface, text, application, email

Description automatically generated

Step 42: commit changes and console into 220 and ensure the previous commit was successful

Step 43: 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 44: Create an IPSec crypto profile. Ensure that adequate encryption and authentication methods are used.

Graphical user interface, application, email

Description automatically generated

Step 45: Create an IKE gateway. Set pre-shared key.

Graphical user interface, application

Description automatically generated

Step 46: Configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 47: Create the IPSec tunnel

Graphical user interface, text, application

Description automatically generated

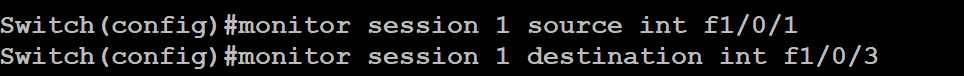
Step 48: Console into the router and configure the following (set IP address on interfaces and activate them).

Text

Description automatically generated

Step 49: 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 50: 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

While time consuming, there were relatively few problems with this lab. The main challenge was figuring out what topology should be used and what IP address should be used as the next hop. The tunnel initially refused to activate but after some time, it activated by itself. Capturing ESP packets required more than just connecting the device to the switch but also “monitor session” command.

Conclusion

The site-to-site VPN is a widely used and especially useful when used to protect data traffic from attackers. In this lab, we set up a site-to-site VPN on a private network with very few problems. Most of our time was spent reimaging our PFSense firewall into a windows OS so we could capture ESP packets being transmitted across the network. In the future, we plan on exploring site-to-site VPNs with certificate verifications and remote access VPNs.