PaloAlto-220 Site-to-Site VPN Lab

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

The purpose of this lab is to learn the way that PA-220s interact with each other. The goal is to operate two different networks that are both protected by Pa-220, through a site-to-site VPN connection. While using the public IPs, both routers should have full connectivity through the secure site-to-site VPN connection under a secure IPsec protocol suite.

**Background Info**

The big main concept of this lab is the concept of VPNs. A VPN, a virtual private network, is what establishes a digital connection for a computer and a remote server owned by a VPN provider. It creates a point-to-point tunnel that encrypts personal data, masks IP addresses, and sidestep website blocks and firewalls up on the internet. In short, a VPN is:

Virtual: no physical cables are used in the process

Private: no one else can see personal data or browsing activity

Networked: multiple hardware work together to maintain the overall connection

VPN, in general, provides a safe, free and secure connection. It makes sure that the users are protected by encryption and masking, which leads to the browsing history and location untraceable. With there being multiple types (such as remote access VPN, site-to-site VPN, and VPN applications). Some scenarios where VPN could be used include:

|  |  |
| --- | --- |
| Scenario | Description of the VPN work in the scenario |
| Secure the Data | * Sensitive data (emails, payment info, location tagging) * Easy to track through public network * VPN scrambles data into code and renders it unreadable (without an encryption key) * Hides browsing activity |
| Working from Home | * Workers can access company resources from home (as long as they have internet connection) * Greater sense of flexibility * Ensures company data is protected/secure |
| Access/stream regional content remotely | * VPN disguises the location of local server * Could access sites that restrict their media based on physical location |
| Bypass censorship | * Same as above – location spoofing could give access to bypass government restrictions, censorship, or surveillance |
| Prevent tracking | * Internet service provides log and track browsing history through IP addresses * VPN masks IP address to prevent ISP tracking and to keep personal data private |

There are a wide variety of VPNs in this world right now, compatible for computers and mobile, for free and not, and for professional and personal use. The most common types are as shown below:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Connection method | Use Case |
| Remote access VPN / client-to-site VPN | Home | Connection via SSL/TSL – to a private network or third-party server | * Remote workers that need access to company resources from home. * Users that wish to browse public Internet with an encrypted connection. |
| Site-to-site VPN | Private | Connection via LAN/WAN – to another network | * Large organizations that need to link internal networks across multiple sites with different physical locations. * Maintaining secure connection |
| VPN applications | Mobile | Connection via VPN app on mobile/smartphone device | * Mobile users that wish to take advantage of benefits of VPN on the go. * While experiencing unstable connection on the internet. |

There are a wide variety of protocols among VPN providers, each with their own routing methods – each with their own use cases. Below is the information:

|  |  |
| --- | --- |
| OpenVPN | * Most widely used protocols * Security, stability, flexibility * 256-bit encryption technology * Provides tunneling through SSL/TSL |
| SSTP | * Secure Socket Tunneling Protocol * Features 256-bit encryption and SSL.TSL certifications for authentication * Built into Windows OS |
| IKEv2/IPsec | * Internet Protocol Security, IKEv2/IPsec maintains your connection under unstable Internet conditions * Best protocol for mobile VPNS |
| L2TP/IPsec | * Layer 2 Tunneling Protocol is frequently paired with IPsc for additional security * Natively built into Windows OS * Generally easy to set up |
| PPTP | * Point-To-Point Tunneling Protocol * Original predecessor to L2TP * Has since been rendered obsolete |
| WireGuard | * Newer, up-and-coming protocol * Continues to gain traction in VPN space * Touts a leaner codebase, more modern encryption technology, and greater mobile compatibility. |

**Lab Summary**

1. Configure in Management to change subnet details
   1. Use different subnets to endure traffic is leaving the assigned subnet
2. Create a new security zone
   1. Identified by tunnel
   2. Used to create policy rules
3. Create static route to the other site on the 2 firewalls
4. Configure security that go along with IPsec and IKE Crypto section
5. Exchange of information
6. Create security policy rules to allow tagged traffic

**Lab Commands**

No new commands were used in this lab because all of the configurations were done through the PA-220 GUI.

**Network Diagram/Topology**A diagram of a network connection

Description automatically generated

|  |  |  |
| --- | --- | --- |
| Public Network | LAN 1 | LAN 2 |
| R1 -> S1: 172.28.128.1 | S1 -> FW1: 172.28.128.81 | S1 -> FW2: 172.28.128.125 |
|  | Management Interface: 10.0.0.1 | Management Interface: 192.168.1.1 |
|  | Virtual Router Default Gateway: 10.0.0.254 | Virtual Router Default Gateway: 192.168.1.254 |
|  | PC1 DHCP: | PC2 DHCP: |

**Configurations** – screenshots of the process

|  |  |
| --- | --- |
|  | 1. Configuring Internet Access – this is from the previous lab, where SOHO configuration was done on the firewall + there is active internet connection. 2. Creating tunnel Interface – a virtual router and security zone should be assigned to the tunnel interface. If necessary, create a new security zone. |
| 1. Network -> Interface -> Tunnel -> Add |  |
|  | 1. Creating the tunnel zone – a new Zone made specifically for the tunnel should be added to a newly creates tunnel interface. 2. Zone type layer MUST by Layer 3, NOT tunnel. |
| 1. Network -> Zones |  |
|  | 1. Configuring defaults router with VPN route – describe the network destination that the tunnel is meant to reach and set the interface’s configuration to match the tunnel interface and indicate the Next. 2. Define the hop address as the virtual router’s default gate way, which is situated on the other side of the tunnel. |
| 1. Network -> Virtual Routers -> Default -> Static Routes -> IPv4 -> Add |  |
|  | 1. Configuring Security Policies - Set up appropriate security rules to direct traffic between zones. For trusted Layer 3 communications, Trust-L3 is used, whereas Tunnel is used for VPN traffic. 2. Even though everything else seems to be working, traffic will not route without these Security Policies. The defined zone for trusted Layer 3 traffic is called Trust-L3. 3. The tunnel is the area where VPN traffic is allowed. It should be noted that two new security policies need to be developed for VPN tunnel traffic. Without them, nothing will function. |
| 1. Policies -> Security |  |
|  | 1. Configuring IKE Crypto Profile - Selected SHA384 for its data integrity and authentication capabilities, AES 256 for its robust encryption, and DH (Diffie Hellman) Group 20 for its powerful cryptography. |
| 1. Network -> Ike Crypto -> Suite-B-GCM-256 |  |
|  | 1. Configuring the IKE Gateway - Employ IKEv2 to improve security. 2. Assign the Internet interface's interface (such as eth1/1) to the IKE Gateway. If the interface has a DHCP given IP address, leave the Local IP Address field empty. |
| 1. Network -> IKE Gateways -> Gateway |  |
|  | 1. Select the correct IKE Crypto Profile on the Advanced Options section |
| 1. Network -> IKE Gateways -> Gateway -> Advanced |  |
|  | 1. Configuring IPsec Crypto Profile - In this arrangement, we made use of DH (Diffie Hellman) Group 20, ESP (Encapsulating Security Payload), and AES (Advanced Encryption Standard) 256 for improved safety. |
| 1. Network -> IPsec Crypto -> Suite-B-GCM-256 |  |
|  | 1. Configuring the IPsec VPN tunnel - Assign the IPsec Crypto Profile, the IKE Gateway you specified, and the Tunnel interface to your tunnel interface. |
| 1. Network -> IPsec Tunnels -> Tunnel |  |
|  | 1. Commit |
|  | 1. Verifying connectivity through pings of across the network devices 2. Configuring the Remote Desktop Software - Here, we made advantage of RustDesk. You must allow direct IP access while using the remote desktop software in order to confirm that you are using the site-to-site VPN tunnel. |
| 1. Settings -> Security |  |
|  | 1. Controlling the remote desktop - The IP address of the device you wish to remote desktop into must be entered. 2. The remote desktop session will be created by RustDesk. |
|  | 1. Unencrypted Wireshark Captures from PC1 to PC2 – the data captured from the computer, currently unencrypted, is shown on the left. It is encrypted because it hasn’t reached the other firewall yet. |
|  | 1. Verifying IPsec Tunnel Encryption - We must intercept the traffic while it is in transit in order to confirm the encryption of network communications because the data will not be encrypted when it reaches the other side of the IPsec Tunnel and will therefore be readable by the recipient. 2. Copying and rerouting the switch traffic – we will use the switch that both firewalls are plugged into for traffic interception. For packet analysis, we need to set up the switch to copy traffic from the firewall to the PC. 3. Commands used: **monitor session 1 source interface [firewall-interface] & monitor session 1 destination interface [pc-interface]** 4. Plugging the PC into the Switch - When it's finished, the switch ought to be simultaneously switching traffic out of the two ports—the one that has the other firewall and the one you've chosen. |
|  | 1. Final encryption verification – data section is displaying the Encapsulating Security Payload |

**Problems**

There were a bunch of problems when completing this lab. The list below shows the countless misses we had to fix:

There were multiple hardware issues when completing this lab. First off, even though we marked it clear, a lot of the other users of the rack kept on unplugging and re-plugging in our cables. This was truly inconvenient because of how these PA-220s are designed—we must have the exact same port number as the configuration, or else the firewall won’t work. To solve this problem, made sure to document every port and cable used, just so we can set it up every time, in the correct way.

Along with that, there was a power outage during our lab period. This resulted in IPv6 getting disabled, since the network had to mitigate for the outage. We simply put it back up, but this made me aware that weather and inconveniences like this is something I have to keep in mind and is something that causes cyber engineers a huge problem.

We also had problems within our web GUI. The most often one we experienced were wrong IP addresses. Through the configuration of VPNs, there are multiple times where you must enter in the same IP address to more than one place. We often got confused on which IP address to put in and got some errors because of that. We just figured this out, at this time, because we made the same error a lot that we remembered the IP addresses, but now that I think back, I believe it was most sufficient for us to have an IP address scheme physically.

The tunnel turning on was also a problem when configuring this VPN network. We did not notice that both of the tunnels had to be up for the mark to turn from red to green. We simply fixed by turning both tunnel configurations on and committing it.

**Conclusion**

In conclusion, this lab has taught us a lot about the VPN connections between two different networks. We utilized our skills to navigate through the web GUI, and side note, also learned how to prove that our VPN connection is working. Along with that, we also learned about the complications of the PA-220 firewalls. We had numerous times when we configured something, committed it, went back the next day just to find that it was not saved and gone. Although PA-220s are perfectly functional, my partner and I found this extremely inconvenient and frustrating and did not find anything to work around this in the end (I believe we weren’t doing anything wrong, and it was just PA-220s being PA-220s). So, through this experience, we were able to nurture problem-solving skills and also the skill of being introduced to a new hardware and being able to utilize it perfectly fine.

A close-up of a letter

Description automatically generated