A black text on a white background

Description automatically generatedA logo with red and blue text

Description automatically generated

Fortinet IPsec Site-to-site VPN Lab

Joshua Widjaja

P5 Advanced Cisco Cybersecurity

Mr. Mason

**Purpose:**

The purpose of this lab was to give us hands on experience with configuring and testing a site-to-site Ipsec VPN using Fortinet’s Fortigate firewall. We gained experience on how to do this on the firewall’s GUI which had us understand how important it is that secure connections are made between remote users and an internal network when trying to get onto the internet. This lab specifically simulated where two separate networks must communicate over the internet securely.

**Background Information:**

|  |  |
| --- | --- |
| **What is a Firewall?** | * A firewall monitors and controls the incoming and outgoing network traffic. * Essentially, it’s a wall protecting an internal network from an external network. * As a network engineer you can choose which traffic comes in and the level of authorization needed to gain certain access. * Through the use of network segmentation (dividing the network) on the firewall, you can control what parts of each network can reach one another. * Based on the security policies configured on the firewall, your network can choose whether to allow or block certain incoming traffic. * Firewalls are key to network security, as it can block suspicious traffic and can intercept threats before reaching internal systems. |
| **Fortinet** | * Fortinet is a cybersecurity company that was founded in 2000 by Ken Xie and Michael Xie and is based in Sunnyvale, California. * Develops and sells security solutions such as firewalls, endpoint security, and intrusion detection systems. * This company is best known for its FortiGate firewalls which was its first product. FortiGate firewalls are heavily popularized due to their strong combination of security, performance, and cost-effectiveness whilst offering advanced threat protection, high throughput, and user friendly interface |
| **PA-220 Firewall** | * The firewall we used in this lab is a next generation firewall. * Designed for smaller networks but provides the same level of security features as the larger Palo Alto firewalls. * The physical descriptions include compact, no fan, 8 ethernet port openings. * Advanced threat prevention and easy to manage in smaller environments. |

|  |  |
| --- | --- |
| Types of Firewalls | Description |
| Hardware Firewall | * A physical device placed in between the network and the host (computer) * Found typically in server room |
| Software Firewall | * Acts as a service in virtual machines to secure network environments in the cloud. * Types of software firewalls include container firewalls, virtual firewalls, cloud firewalls, and managed service firewalls. |
| Next Generation firewall (NGFW) | * More advanced firewalls and better security solutions. * NGFW contains features to control application traffic and to locate threats in the cloud. * Closer examination of data to identify potential threats |
| Packet Filtering Firewall | * Operates at the network layer. * Controls the flow of data packets between different networks. * Packet is blocked if it doesn’t meet the established rules. |
| Proxy Firewalls | * Operates at the application letter. * Filters messages between external servers and the client. |

|  |  |
| --- | --- |
| **RDP (Remote Desktop)** | Remote Desktop allows a user to control a computer remotely from another computer across a network. It mimics a situation where you are using another person’s computer as your own right in front of you. You have enabled access to their files and applications. Remote Desktop is a great way for you to work on a certain desktop without physical access. |
| **IPsec site-to-site VPN** | IPSec site-to-site VPN creates a secure, encrypted tunnel between two separate networks. Ipsec, also known as internet protocol security, is a set of protocols that secures communication over IP networks. |
| **FortiClient VPN** | FortiClient VPN is a software created by the company Fortinet that allows for secure remote access towards a network. Users are able to securely protect their data transmission to a FortiGate firewall through encryption. For example, a user could connect to an internal network with resources from an outside company network and do it while protected with Fortinet capabilities. |
| **Wide Area Network (WAN)** | Networks that span across a large geographical area. It connects smaller networks and devices, often spanning cities, countries, etc. |
| **Dynamic Host Configuration Protocol (DHCP)** | A network protocol that automatically assigns IP addresses to devices on a network. This simplifies network assignments, reducing the risk of human errors that arise from manual configuration. |

**Lab Summary:**

We first powered on our Fortinet firewall and reset it. We logged onto the Graphical User Interface of our FortiGate firewall and assigned static IP addresses to both FortiGate firewalls. We hten configured Ipsec VPN settings on both ends. Next, we created static routes on the FortiGates to direct the network traffic through the VPN interface. We then implemented firewall policies to secure the tunnel. We then tested connectivity by pinging across the network from firewall to firewall. We then used a remote desktop application and after logging in with the required credentials, we were able to successfully access a device from another network using two firewalls.

**Lab Procedure:**

1. Go onto Ipsec Tunnels.

A screenshot of a computer

AI-generated content may be incorrect.

2. Click create new and then Ipsec Tunnel.

A white sign with black text

AI-generated content may be incorrect.

3. Under VPN Creation Wizard, make sure that there is no Nat between Sites and the remote device is Fortigate.

A screenshot of a computer

AI-generated content may be incorrect.

4. Go to Static Routes

A screenshot of a computer

AI-generated content may be incorrect.

5. Create new static route and set destination as subnet. IP address is 192.168.40.0/24. We selected the interface which we want to connect to and enabled it.

A white rectangular object with a black border

AI-generated content may be incorrect.

6. Now edit the Ipsec VPN policy in the firewall policy sidebar. Set the following configurations in the picture down below. Each picture is a different Firewall Policy that we set.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

7. Now go into Static Routes. The first picture is what your page should look like and the ones after that show the specific static routes we created.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

8. Click onto the IPsec tunnels sidebar and it should look like the first pictures. The pictures after show the IPsec VPN tunnels we created and their configurations.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

11. Now go onto remote desktop and enter in the address that you want to have direct access to.

A screenshot of a computer

AI-generated content may be incorrect.

12. Once you’ve hit connect, enter in your credentials to remotely connect to the outside user.

A screenshot of a computer

AI-generated content may be incorrect.

13. Click onto advanced and connect.

A screenshot of a computer

AI-generated content may be incorrect.

14. You now have remote access to another computer across a different network.A computer screen with a computer screen on it

AI-generated content may be incorrect.

**Problems:**

Our first issue was that we weren’t getting our pings across to work even though our firewall policies and VPN tunnel configurations seemed to be correct. We went to consult Mr. Mason and we found that there may be a possibility that someone else’s switch was doing a DHCP spoofing attack. When another rack fixed their wiring, we traced down our problem to possibly be on one of the switches on our rack. We found that there were no errors with that switch but decided to use a different one. We then found that our problem was that our ethernet cord wasn’t connected to the internet, thus eliminating the chance for connectivity with another network. Once this issue was fixed, we were able to get our pings working.

**Conclusion:**

In conclusion, we learned how to successfully configure and test a Fortinet IPsec site-to-site using two FortiGate firewalls. By being able to complete this network setup and establish secure communication using IPsec VPN tunnel, we were able to gain a deeper understanding on how we could apply this network architecture to real world connectivity.

**Lab Signoff:**

A white paper with a blue stamp

AI-generated content may be incorrect.