A black text on a white background

Description automatically generatedA logo with red and blue text

Description automatically generated

Fortinet SSL VPN Remote Access 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 an SSL VPN (Secure Sockets Layer Virtual Private Network) remote access on our Fortinet 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.

**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. |
| **SSL (Secure Sockets Layer)** | Secure Sockets Layer, also known as SSL, is a security protocol that protects internet communications from the web browser and a website. It prevents unauthorized web access, protecting sensitive information such as a user’s credentials. |
| **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 configured our FortiGate firewall with the necessary SSL VPN settings. We then created a local user account on the FortiGate and assigned it to a user group we made with VPN access. Next, we set up firewall policies to allow SSL VPN traffic to go through and that the interfaces were turned on to allow these connections. 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.

**Lab Procedure:**

1. Go onto SSL-VPN Settings.

A screenshot of a computer

AI-generated content may be incorrect.

2. Under connection settings set the interface to wan and the port 4443. Server certificate will be Fortinet\_Factory and Allow access from any host. Automatically assign addresses and for DNS Server use the same as client system DNS.

A screenshot of a computer

AI-generated content may be incorrect.

3. Under Web Mode Settings, set Cisco, guest, and admin to have tunnel access and all other users/groups to have web access.

A screenshot of a computer

AI-generated content may be incorrect.

4. Go to Firewall Policy

A screenshot of a phone

AI-generated content may be incorrect.

5. This is what it should look like. Click edit SSL VPN > LAN AccessA screenshot of a computer

AI-generated content may be incorrect.

6. When editing that policy, set the incoming interface as SSL-VPN tunnel interface as the root one. Make the outgoing interface the LAN. Set the source as all, admin, guest, and cisco. Set the Destination to LAN. Turn off NAT under Firewall options and toggle log allowed traffic to on and all sessions and enable the policy.

A screenshot of a computer

AI-generated content may be incorrect.

7. Click on the 3 lines and click edit the selected connection.A screenshot of a computer

AI-generated content may be incorrect.

8. Set Remote Gateway address as 192.168.40.213 and port as 4443. Hit save.

A screenshot of a computer

AI-generated content may be incorrect.

9. Enter in your necessary credentials.

A screenshot of a computer

AI-generated content may be incorrect.

10. When successful, you should see that your VPN is connected.

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 security

AI-generated content may be incorrect.

A close-up of a number

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 biggest issue came down to layer 1 mistakes. We mistakenly didn’t connect the FortiGate firewall’s WAN interface to the switch that provided internet access. Due to this, the deviec couldn’t create an external network connection, resulting in our VPN to be unable to connect across the network. Our next issue was that we had WIFI turned on. Since the computer remained connected to a separate Wi-Fi network, it caused routing conflicts because our device was prioritizing the Wi-Fi traffic over the ethernet interface that was connnected to our Firewall. After disabling Wi-Fi, we were able to reach the VPN portal and the connection was a success.

**Conclusion:**

In conclusion, we learned how to successfully configure and test a Fortinet SSL VPN using remote access and a FortiGate Firewall. We gained hands on experience with VPN configuration, access control, and being able to see the benefits of secure remote connectivity specifically with Fortinet’s resources.

**Lab Signoff:**

A close up of a paper

AI-generated content may be incorrect.