FN Remote Access SSL VPN

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

The purpose of this lab is to familiarize ourselves with the process of configuring SSL VPNs to ensure data confidentiality when accessing a private network. SSL VPNs set up secure and encrypted connections for remote users using the SSL protocol. This enables remote access to internal network resources securely, safeguarding sensitive information from potential cyber threats during transmission.

**Background Info**

Fortinet is a leading cybersecurity company that specializes in creating products and services designed to safeguard networks, data, and applications from a variety of cyber threats. In our lab, we utilize Fortinet's 40F firewall to enhance our network security. A firewall serves as a network security device that oversees and regulates incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to block malicious traffic.

A GUI, or Graphical User Interface, is a user interface that enables users to interact with software and devices through graphical elements like icons, buttons, and menus. This is in contrast to text-based interfaces that require users to input text commands, making GUIs generally more user-friendly and intuitive. Secure Sockets Layer (SSL) is a standard security protocol that establishes an encrypted link between a server and a client. This technology ensures that data transmitted between the two entities remains private and integral, protecting it from eavesdropping and tampering. A VPN, or Virtual Private Network, creates a secure, encrypted connection over a less secure network, typically the internet. VPNs are used to protect the privacy and integrity of data as it travels from one device to another, making it appear as if the devices are directly connected to a private network. A private network is restricted to a specific group of devices and users, ensuring that access to the network and its resources is limited to authorized users only. This type of network is not accessible to the general public, providing enhanced security and control over the data shared within it.

A firewall policy consists of a set of rules configured on a firewall to manage and control network traffic. These rules determine which traffic is allowed or blocked based on criteria such as IP addresses, protocols, and applications, ensuring that only legitimate traffic can pass through. A tunnel interface is used to encapsulate and route traffic securely between different networks. This interface allows secure communication between remote devices by creating a virtual tunnel through which data can be transmitted safely. Split tunnelling is a feature used with VPNs that allows users to route some of their traffic through the VPN while other traffic accesses the internet directly. This means that only specific data is encrypted and routed through the VPN, while other data can be transmitted normally, optimizing both security and performance. FortiClient is a software application developed by Fortinet to be used alongside FortiGate firewalls. In our lab setup, FortiClient plays a crucial role by providing endpoint security and secure remote access, enhancing the overall protection offered by the FortiGate firewall.

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that allows users to remotely access and control another computer over a network connection. This protocol enables users to interact with the remote device as if they were physically present, facilitating tasks such as troubleshooting, administrative maintenance, and remote work. These concepts are integral to understanding and implementing robust cybersecurity measures in a networked environment. By utilizing Fortinet's tools and technologies, such as the 40F firewall and FortiClient, along with implementing secure practices like SSL, VPNs, and firewall policies, we can significantly enhance the security and functionality of our network infrastructure.

**Lab Summary**

1. Connect FortiGate firewall.
2. Create SSL User and User Group
3. Configure the SSL VPN
4. Create a Firewall Policy
5. Test out the Remote Access

**Lab Commands**

Because everything was done in the Web GUI, no new commands were used.

**Network Diagram/Topology**

A diagram of a fire alarm system

Description automatically generated

**Configurations**

|  |  |
| --- | --- |
| 1. Connect the FortiGate firewall to a switch with internet access. |  |
| 1. Connect your PC to the firewall in Port 1 with an ethernet cable. |  |
| 1. Log into the Fortinet GUI using the “admin” and “Cisco123” password set in previous labs. |  |
| 1. User & Authentication > User Definition |  |
| 1. Click “New” to create a new client for the VPN |  |
|  | 1. Configure the user with the same settings shown on the left, and click OK. |
| 1. User & Authentication > User Groups > New  * To create a user group for our VPN user |  |
|  | 1. Configure the same settings on the left, and click OK |
| 1. VPN > SSL-VPN Portals > New  * Create a new portal with full-access |  |
|  | 1. Use the settings on the left to configure the portal. Click OK. |
| 1. VPN > SSL-VPN Settings |  |
|  | 1. Configure the same settings as shown on the left |
|  | 1. Authentication/Potal Mapping > Create New  * Add user and user group for the SSL VPN  1. Click OK |
|  | 1. The following VPN commands should be as shown on the left. 2. Click OK |
| 1. Policy & Objects > Firewall Policy > NEW |  |
|  | 1. Configure the policy with the following settings, then click OK. |
|  | 1. The firewall policy homepage should look like the left. |
| 1. VPN > SSL-VPN Setting |  |
|  | 1. Find public IP address website and open it in a separte tab on a separate host |
|  | 1. Log in with the username and password that you created earlier. |
|  | 1. This is the homepage that should come up. |
| 1. Select Quick Connection |  |
|  | 1. Ping the host we are trying to remote into to make sure it is reachable. |
|  | 1. The following message should pop up to indicate that the ping was successful. |
| 1. Configure the username, passwords, IPs, etc. under RDP. |  |
|  | 1. Click “Launch” and the following screen should pop up. Type the username and password of the host that you are trying to reote into. 2. Click :Log in: |
|  | 1. This screen is the final roduct of what the remote desktop should look like. |

**Problems**

Here are the problems we experienced:

* We couldn’t configure out SSL VPN setting because there was no default portal for us to put it in. We gave “All Other Users/Groups” entry a portal under the Authentication/Poral Mapping section to grant full-access to all users and groups.
* **A screenshot of a computer

  Description automatically generated**
* We weren’t able to access the remote desktop even though we click launch – it was shown as “unreachable.” To solve this, we turned off our Windows Defender Firewall and the problem was solved.
* A screenshot of a computer

  Description automatically generated
* **A screenshot of a computer

  Description automatically generated**

**Conclusion**

We configured a remote access SSL VPN using the FortiGate GUI, allowing us to remote desktop into a device on a private network. We set up SSL users and user groups, adjusted the VPN settings, and established a firewall policy. By utilizing the public IP address website, we logged in as a VPN user and accessed the desired host via remote desktop. One problem we encountered was that the Windows Defender Firewall setting was not disabled, which blocked pings to the private network.