FN IPSec VPN

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

The objective of this lab is to set up an IPSec VPN connection to enable secure communication across an insecure network, such as the internet. By encrypting transmitted data, IPSec tunnels ensure confidentiality against unauthorized access. Additionally, IPSec helps mitigate potential network threats like interception and data manipulation.

**Background Info**

Fortinet is a company specializing in cybersecurity solutions, providing a range of products and services aimed at safeguarding networks, data, and applications against cyber threats. In our current lab setup, we are utilizing Fortinet’s 40F firewall, a crucial network security device that monitors and manages incoming and outgoing network traffic based on predefined security rules. The firewall ensures that only authorized traffic passes through, enhancing network security.

Graphical User Interface (GUI) is another integral component, offering users an intuitive interface to interact with software and devices through graphical icons, buttons, and menus, simplifying complex configurations compared to traditional text-based interfaces. Through the Web GUI, the main concept applied in this lab is IPSec. Internet Protocol Security (IPSec) is a suite of protocols utilized to secure IP communications by encrypting and authenticating each IP packet, thereby ensuring data confidentiality and integrity during transmission.

Virtual Private Networks (VPNs) establish secure, encrypted connections over potentially insecure networks like the internet, safeguarding data privacy as it travels between devices. Private networks are restricted to specific groups of devices, shielding sensitive resources from unauthorized access. Firewall policies play a crucial role by defining sets of rules that dictate which network traffic is permitted or denied based on factors such as IP addresses, protocols, and applications, thereby bolstering network defenses. Remote access capabilities enable users to connect to and utilize separate devices remotely, enabling efficient management and access to resources as if physically present. Remote Desktop Protocol (RDP) facilitates remote control and interaction with end devices over network connections, offering seamless management capabilities irrespective of physical proximity.

Another concept applied in this lab is the NAT process. Network Address Translation (NAT) is a networking technique that modifies IP address information as it traverses routing devices, optimizing address allocation and enhancing network efficiency by reducing the number of publicly accessible IP addresses used within an organization's infrastructure.

**Lab Summary**

1. Setup the topology
2. Create the VPN User and User Group
3. Configure the IPSec Wizard Settings
4. Configure firewall Policies
5. Connect using FortiClient

**Lab Commands**

All of the configurations were done in the Web GUI – no new commands were used.

**Network Diagram/Topology**

A diagram of a network

Description automatically generated

**Configurations** – screenshots of the process

|  |  |
| --- | --- |
| 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. This new user should now show up in the Usser Defination homepage |
| 1. User Authentication > User Groups > New |  |
|  | 1. To create a new user group, configure is with the following settings on the left. 2. Click OK. |
|  | 1. The newly created user group should shsow up in the User Groups homepage |
| 1. VPN > IPSec Wizard |  |
|  | 1. The following settings on the left should be configured. 2. Click Next. |
|  | 1. Configure the following settings on the left. 2. Click Next. |
|  | 1. Configure the following settings on the left. 2. Click Nect |
|  | 1. Configure the following settings on the left. |
| 1. Next > Create |  |
|  | 1. Double check to make sure that the VPN is setup with the same message as the left in the green banner. |
| 1. Policy & Objects > Firewall Policy |  |
| 1. In the firewall policy from VPN to LAN, disable NAT. |  |
| 1. Copy and paste the firewall policy above the currently configured one. |  |
| 1. Right click new firewall policy > Edit |  |
|  | 1. After double checking that the new policy is directed towards the WAN, configure the new policy settings shown on the left. 2. Click OK |
|  | 1. The WAN firewall policy should show up in the Firewall Policy homepage. |
| 1. Download FortiClient onto the device (PC). |  |
|  | 1. Open FortiClient > Configure VPN |
|  | 1. IPSec VPN > configure the following settings for the VPN. 2. Click Save. |
|  | 1. Enter the same credentials as the VPN User that was set up earlier. |
| 1. Click Connect > Connection should be successful. |  |

**Problems**

* One of the problems we had during this lab was that our very first try to connect out IPSec VPN in the FortiClient application did not work, and the connection was shown as “down.”
* **A black rectangular object with white text

  Description automatically generated**
* To fix this, instead of using the username/password for out VPN user, we used the username and password that we used for our firewall. After these settings were chnaged, we were able to connect.

**Conclusion**

We began by creating a user and a corresponding user group for later login purposes. Subsequently, we used the FortiGate GUI's IPSec Wizard to configure our VPN settings. Following this, we established a firewall policy directing traffic from our interface to the WAN. Proceeding with the setup, we installed FortiClient on our PC, entered the VPN configuration details, and attempted to connect. Initially, the connection failed because we mistakenly used the credentials of our firewall instead of those assigned to the VPN user we had set up earlier. Once we corrected this error by using the correct VPN user credentials, the connection successfully established.