Brit Stevens 5/7/24

Fortinet SSL VPN Configuration

**Purpose:**

The purpose of this lab is to configure an SSL VPN tunnel on a FortiGate to enable remote connections to access the inside network. This lab emphasizes the use of encrypted tunnels and managed access by users with the use of SSL portals. We will learn how the tunnel functions differently from other VPN labs we have done such as IPsec with PaloAlto.

**Background Information on Lab Concepts:**

* **FortiGate SSL VPN**
  + **SSL-VPN:** 
    - This kind of **Virtual Private Network (VPN)** allows remote users to access resources that are contained inside a local network through an encrypted tunnel. A scenario of this would be like a remote worker in Australia access resources at the USA HQ through a tunnel. They can be configured in two different modes: web mode and tunnel mode. Web mode, like the one used in this lab, uses a SSL portal webpage with a certain IP and port to allow users access to the inside network. Tunnel mode is like a standard VPN where it directly connects the user to the inside network with VPN Clients such as FortiClient.
  + **SSL Portals:**
    - Like previously described, **Secure Sockets Layer (SSL) Portals** are used for the Web mode of the SSL VPN that allow users to access the inside network. You can make different SSL portals for different groups of users you define that limits the features of the portal. A Full Access portal like the one we used in this lab allows the user on the webpage fully unrestricted access to the networks, for example using RDP. They are completely configurable and enhance the security of your network and VPN tunnel to it.
  + **Server Certificates**
    - These are a method of securing a connection between the user’s device and the FortiGate that the tunnel is leading to. Certificates can either be self-assigned and imported into your security device like the FortiGate used or issued by a trusted Certificate Authority (CA) which are trusted and reputable. A CA could be thought of like a bank who you are seeking a loan from; you want that loan to be secure and having specifics details accurate. The Certificate works by verifying the identity of the client and FortiGate device, then encrypting the data to prevent the data from being tampered.
* **User Types** 
  + **Local:** Accounts that are created and managed directly on the FortiGate being stored in its database. Useful for small businesses or a small group of users who can access the firewall.
  + **Remote RADIUS: RADIUS** Accounts stored on an external RADIUS server and authenticated through the FortiGate’s connection to it. It’s often used for larger organization who need a more centralized authentication.
  + **Remote TACAS+: Terminal Access Controller Access-Control System Plus** accounts that are stored in a TACAS+ server. Similar to Remote RADIUS, this server is centralized with the AAA services: Authentication, Authorization, and Accounting. Its most commonly used when extensive control over users’ privileges is needed.
  + **Remote LDAP: Lightweight Directory Access Protocol** accounts authenticated through an external LDAP server. LDAP allows for centralized management of user credentials and can be integrated with directory services like Microsoft Active Directory. This is most useful for businesses that have an existing LDAP server and want to extend it for VPN authentication.
  + **FSSO: Fortinet Single Sign-On** accounts authenticated based on their desktop’s login credentials if configured to work with Active Directory. This will improve the client’s experience as their login credentials are automatically verified with their desktop login and is useful for businesses that do not have shared devices.
* **FortiNAC: Fortinet Network Access Control** uses a login and device compliance to verify credentials. It can be limited to only certain types of devices can connect to the network even if they login in credentials match. This is useful for a business wants strict control over what can access the network and gives out/communal workstations.

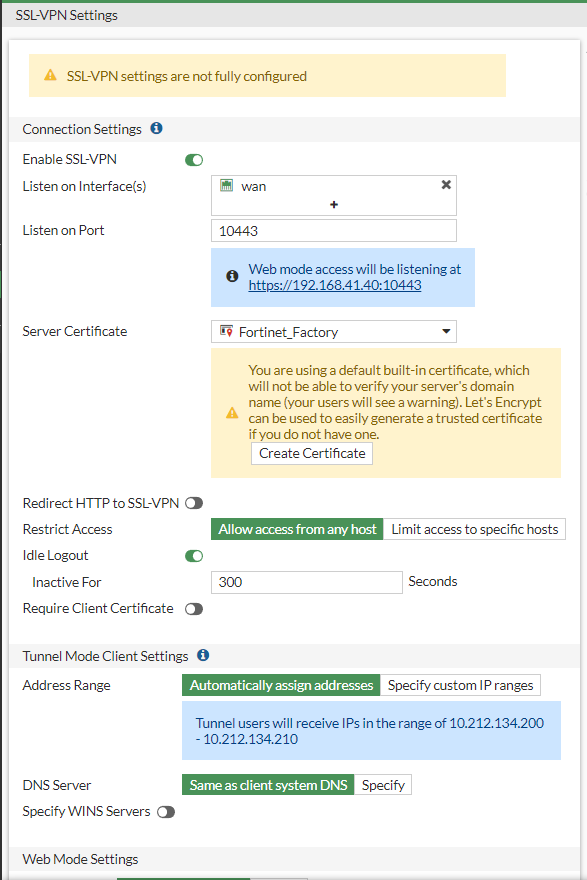
**Required Resources:**

* ***Switch (Cisco Catalyst 3560 series PoE-24).***
* ***Access to the Internet through a switch.***
* ***Desktop on the inside network.***
* ***Desktop on the outside network.***
* ***FortiGate 40F.***

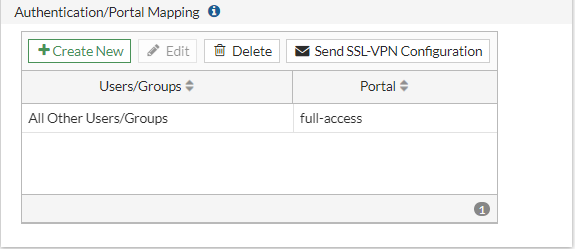
**Lab Summary:**



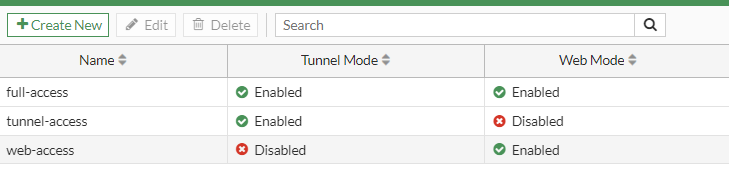
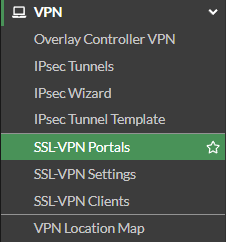
To begin SSL-VPN setup navigate to **SSL-VPN Settings.**



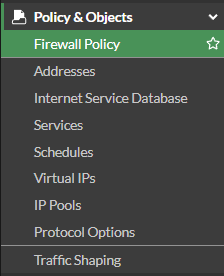
First toggle enable to turn on the SSL-VPN and set to listen on the interface facing the outside network. Set the port to 10443, the standard for SSL-VPN tunnels, and that will give you an IP you can enter in a website to access the SSL portal.



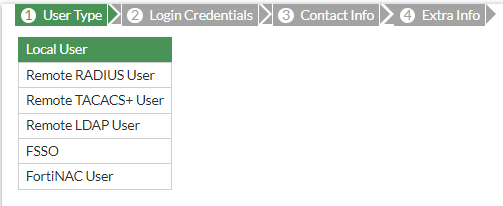
When scrolling down you can adjust which users go to certain portals either through user logins or a user group. For this lab we send all users to the same portal.



To understand and configure the portals, navigate to **SSL-VPN Portals** and view the following. These portals can be adjusted to fit your needs or company requirements.



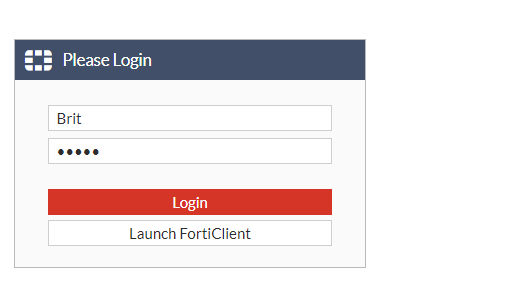
Like with many other features on the FortiGate, you must configure the SSL VPN then allow it’s traffic through the firewall by navigating to **Firewall Policy** and creating a new policy. Set the incoming interface to SSL-VPN tunnel interface and the outgoing to lan. Set the source to all IP addresses and restrict it with the local user access, a user group that we are created. Ensure Nat is on.



go through the process of creating a user through the user wizard.



after creating the user, make a user group and and the users you want to be able to access SSL portal with.



Now enter the IP of your SSL portal an attempt to log in. Here we are using an invalid login to show that only the permitted users can access the portal.

A login screen with red and blue text

Description automatically generated

A screenshot of a computer

Description automatically generated

Using the correct login you can now access that SSL portal. Once in, click quick connection to access all features of the SSL portal including RDP which we will be using.

A screenshot of a computer

Description automatically generated

We use the ping function to ensure we get access to the inside network’s user.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

On the desktop you are trying to remote desktop into create a user by typing in lusrmgr.msc to access the local user groups and right-click to create a new user. Once you create the user navigate to groups and add the user into your admin category to give it permissions. This is the login you will use with RDP.

A screenshot of a computer

Description automatically generated

Back in the SSL portal, select RDP to begin configuring. Enter the host IP address, leave the port as default, and choose your screen height and width to fit your monitor then launch.

A computer screen with a black box

Description automatically generated

A black page like this should appear if the connection is successful. Now log in with the user you created on the host PC.

A screenshot of a computer

Description automatically generated

you can confirm the connection is successful when you can access the inside networks PC.

**Problems:**

* Did not apply the SSL profile to the SSL settings.
  + Could not access the SSL portal.
    - Applied profile and checked the firewall policies.
      * Could now access the SSL portal.
* Couldn’t remote desktop through the SSL portal.
  + Had firewalls on both the host PCs which complicated the connection.
    - Disabled firewalls and could RD.

**Conclusion:**

Overall this lab was very easy as we had done a similar lab before with a PaloAlto device so we knew the concepts and functions of a VPN. Configuring the VPN for a Client instead of point-to-point felt like it could be more useful for a remote company while p2p feels like it would be useful office to office. They’re both just different ways to secure your company’s traffic, each having its use cases. My biggest takeaway from this lab is how flexible some cybersecurity protocols can be allowing for configurations that fit your needs in any use case. FortiGate especially emphasizes this with their client VPN option even including Cisco proprietary options allowing for integration into your pre-existing network with Cisco firewalls or software.

