**CIsco Asa clientless vpn**

Derek Liu Cybersecurity Period 5

**Setting Up a Clientless VPN***Derek Liu*

Purpose

The purpose of this lab is to set up a clientless remote access VPN. With a clientless VPN, the remote should be able to set up a VPN tunnel to a network and access internal resources by typing an address into the search bar and entering credentials.

Background Information

A clientless VPN or browser-based VPN allows for users to access internal resources in a network through a web browser without the need to install software or client-based applications.

Clientless VPNs are useful when resources need to be accessed from a remote location easily and quickly and from any device. This can be helpful for those working on a public or shared computer that do not have administrative privileges to install software on their devices.

However, clientless VPNs are limited in terms of performances and functionality compared to VPN clients as they are only able to access web-based applications. They don’t offer advanced security protocols or features such as split tunneling.

Clientless VPNs also are not as secure compared to a traditional VPN since they do not offer advanced security features such as Open VPN, SSTP, or two factor authentication. Another shortcoming is its reliance on web browsers which have a lot of possible vulnerabilities due to their complexity.

Clientless VPNs are also not able to provide the same amount of control and visibility as a traditional VPN client which means that potential threats are harder to detect.

Lab Summary

In this lab, we set up a clientless remote access VPN with a Cisco ASA. It is a very straightforward and streamlined process with an SSL VPN Wizards that the Cisco ASA offers. Functionality was tested by connecting to the VPN and accessing an internal web server that is not reachable from the internet.

Network Diagrams with IP

Diagram

Description automatically generated

(note: in this lab, the 192.168.41.117 address was obtained with DHCP. The 192.168.1.5 address was obtained with the factory default DHCP configuration. The web server was set up with a windows computer running an Apache web server with XAMPP).

Configurations

Step 1: Set up the Cisco ASA with factory default configurations (refer to factory reset lab writeup if needed). Set up the topology as shown in the network diagram.

Step 2: In the Cisco ASDM, go to Wizards, VPN Wizards, Clientless VPN Wizard.

Graphical user interface, application

Description automatically generated

Step 3: click next

Graphical user interface, text, application, email

Description automatically generated

Step 4: type in the connection profile name as anyconnect\_profile. Note the URL needed to access the VPN service.

Graphical user interface, text, application, email

Description automatically generated

Step 5: choose Authenticate using local user database

Graphical user interface, text, email

Description automatically generated

Step 6: Choose Create New Policy and name it test\_anyconnect\_policy

Graphical user interface, text, application, email

Description automatically generated

Step 7: click manage, add, and add.

Graphical user interface, text, application

Description automatically generated

Step 8: select the following

Graphical user interface, application

Description automatically generated

Step 9: configure the following.

Graphical user interface, text, application, email

Description automatically generated

Step 10: click finish

Graphical user interface, text, email

Description automatically generated

Step 11: go to configurations, remote access VPNs, connection profiles, anyconnect\_profile

Graphical user interface, text, application

Description automatically generated

Step 12: click advanced, yes, and apply.

Graphical user interface, text, application

Description automatically generated

Step 13: access the remote user and type into a web browser (Firefox recommended) the URL noted in step 4

Graphical user interface, text, application

Description automatically generated

Step 14: enter credentials

Graphical user interface, text

Description automatically generated

Step 15: from this screen, you can access internal resources. For example, we have an internal web server on <https://195.168.1.5/webserver.html> that can be accessed from here.Graphical user interface, application

Description automatically generated

Problems

We were unsure of what IP address to put for the bookmark. Apparently, any IP address works. Someone unplugged our ASA while we were trying to get a sign off. Other than that, there were no problems.

Conclusion

In this lab, we configured a clientless VPN which is a VPN that establishes a connection with a web browser without the need to install any software or client. The process is very streamlined and simple on the Cisco ASA and was completed with relatively few problems.