Clientless VPN

By: Jordan Abu-Zahra

**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**

Palo Alto offers a feature call Clientless VPN that allows users to securely access corporate resources without the need to install any dedicated VPN client software. With Palo Alto Clientless VPN users can establish a secure connection to the corporate network using a standard web browser, providing a convenient and flexible remote access solution. Clientless VPN eliminates the requirement of installing a VPN client application on the user’s device which can simplify the deployment and management process. Instead, users can access the VPN portal through a web browser, providing a familiar interface for establishing the VPN connection. Some features that are provided by Palo Alto Clientless VPNs are secure web-based access, which SSL/TLS encryption to establish a secure connection between the user’s web browser and the Palo Alto network firewall. This ensures that data transmitted between the user and corporate network is protected from unauthorized access. It also offers Application access which is used once the user is connected it can access specific applications and resources that are configured for Clientless VPN access, this can include web applications, file shares, intranet sites and more. The Palo alto firewall acts as a proxy securely transmitting the user’s request to the backend serves. Granular Access control provides granular control over which resources users can access. Administrators can define access policies based on factors such as user identity, device type, and application requirements. This allows organizations to enforce fine-grained access controls and ensure that only authorized users can reach specific resources. Overall, Palo Alto Clientless VPN offers a secure and flexible solution for remote access without requiring the installation of dedicated VPN client software. It simplifies the user experience while providing organizations with granular access controls, strong encryption, and advanced security features to protect their networks and resources.

**Network Diagrams with IP**

A screenshot of a computer

Description automatically generated with medium confidence

(note: The web server was set up with a windows computer running an Apache web server with XAMPP).

Configurations

Step 1: Create a SOHO and remote access configuration. Refer to labs Remote Access VPN and SOHO Setup if needed.

Step 2: go to dynamic updates. Download and install the GlobalProtect Clientless VPN

A screenshot of a computer

Description automatically generated with medium confidence

Step 3: go to Network, Clientless Apps, and configure the following

Graphical user interface, text, application

Description automatically generated

Step 4: go to DNS proxy and configure the following

Graphical user interface, text, application

Description automatically generated

Step 5: Go to portals and configure the following (most of the tabs were configured in the previous lab)

Graphical user interface, text, application

Description automatically generated

Step 6: Go to authentication and double check the configuration Graphical user interface, application

Description automatically generated

Step 7: go to Clientless VPN and configure the following

Graphical user interface, text, application, table, email

Description automatically generated

Step 8: go to applications and configure the following

Graphical user interface, application

Description automatically generated

Step 9: go to Crypto Settings and configure the following

Graphical user interface, text

Description automatically generated

Step 10: go to Agent, Client Settings, and IP pools. We changed the IP pool so the devices will be on the same subnet.

Graphical user interface, application

Description automatically generated

Step 11: access the remote user and go to the IP address of the WAN interface

Graphical user interface, application

Description automatically generated

Step 12: Open the configured applicaiton

Graphical user interface, application

Description automatically generated

Step 13: our web server

Graphical user interface, text, application

Description automatically generated

**Problems**

The problem we had was that we forgot to install the clientless VPN on the firewall so the feature that Palo Alto provides did not activate. We solved this problem by using dynamic updates and downloading the clientless VPN feature

**Conclusion**

In this lab we learned how to set up a clientless VPN and how to get a secure connection with a working web browser