|  |
| --- |
|  |
|  |
| PALO ALTO CLINTLESS VPN  Made by: - Akshat Kansal |
| **Cybersecurity lab 10 – Mr. Mason & Mr. Hansen**  **Periods 0,1,2** |

**Purpose**

The objective of this laboratory exercise is to establish a remote access VPN without requiring any dedicated client software. By utilizing a clientless VPN approach, individuals accessing the network remotely will be able to establish a secure VPN connection and gain entry to internal resources simply by entering a specific address in the browser's search bar and providing valid credentials. This method allows for a streamlined and user-friendly remote access experience, eliminating the need for additional software installations on the remote device.

**Background**

A clientless VPN also known as a browser-based VPN enables users to access internal network resources through a web browser without the need for software installations or dedicated client applications. This approach proves valuable when individuals require quick and convenient remote access to resources from any device or location. It particularly benefits those who work on public or shared computers where administrative privileges for software installation may not be available.

However, it’s important to note that clientless VPNs have certain limitations compared to VPN clients. They primarily provide access to web-based applications and lack the performance and functionality of dedicated clients. Advanced security protocols like OpenVPN SSTP or two-factor authentication are not typically available in clientless VPNs. Furthermore, their reliance on web browsers introduces potential vulnerabilities due to the inherent complexity of browser software.

In terms of security clientless VPNs may not offer the same level of protection as traditional VPNs. The absence of advanced security features can leave the connection more susceptible to potential threats. Additionally clientless VPNs may not provide the same degree of control and visibility as traditional VPN clients making it more challenging to detect and mitigate potential security risks.

While clientless VPNs offer convenience and accessibility it’s crucial to consider the trade-offs in terms of security functionality and control when deciding on the appropriate VPN solution for a specific use case.

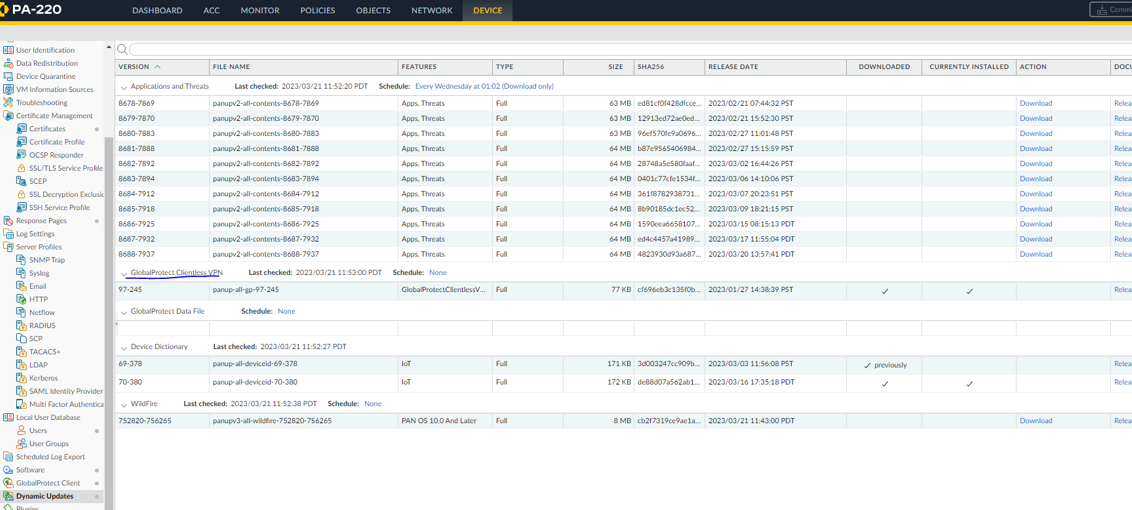
**Lab summary**

During this laboratory exercise we successfully established a clientless remote access VPN using a Palo Alto 220 device. To validate its functionality, we conducted tests by connecting to the VPN and successfully accessing an internal web server that is otherwise inaccessible from the public internet.

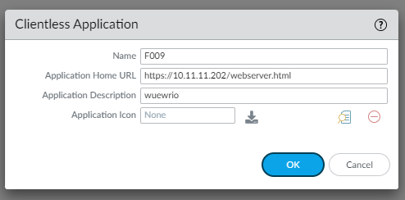
**Configurations**

Step 1: Begin by configuring the Small Office/Home Office (SOHO) and remote access settings. If necessary refer to the lab guides for Remote Access VPN and SOHO Setup for detailed instructions.

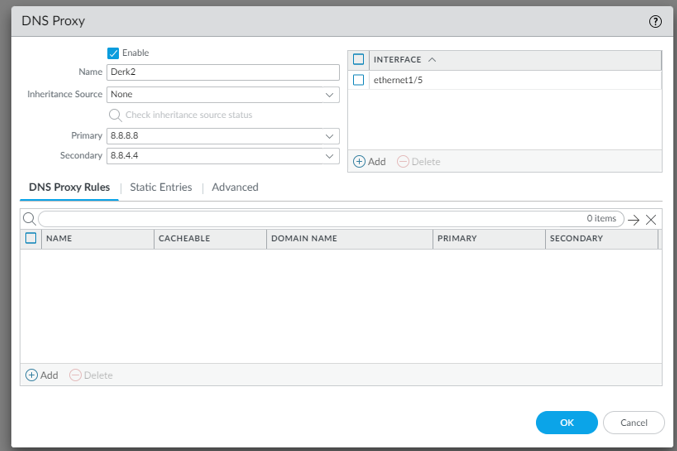
Step 2: Proceed to the dynamic updates section of the configuration. From there download and install the GlobalProtect Clientless VPN software ensuring that it is properly integrated into the system.



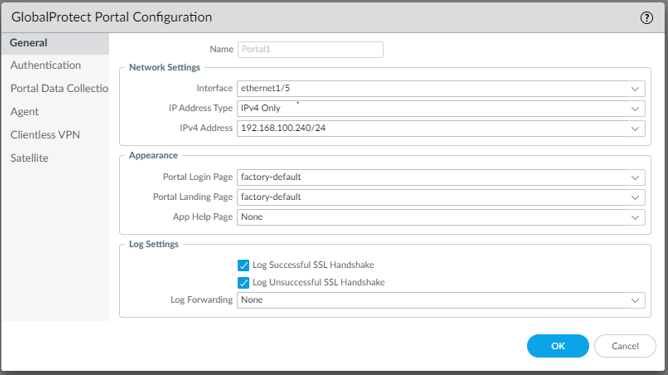
Step 3: Access the Network settings and navigate to the Clientless Apps configuration. Proceed to configure the required settings as specified.



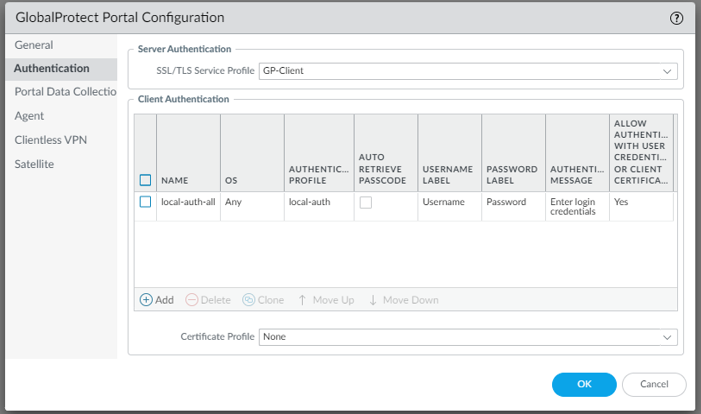
Step 4: Proceed to the DNS proxy settings and configure the necessary parameters as outlined.



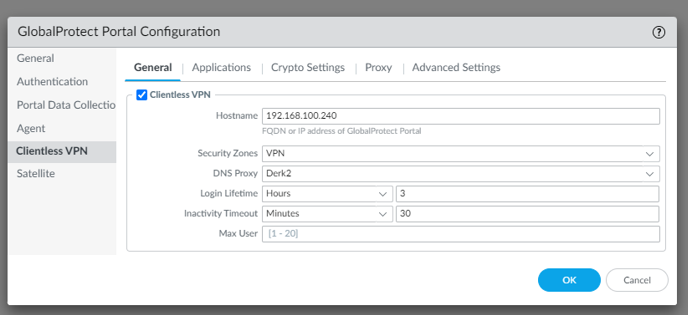
Step 5: Navigate to the Portals section and configure the specified settings according to the requirements.



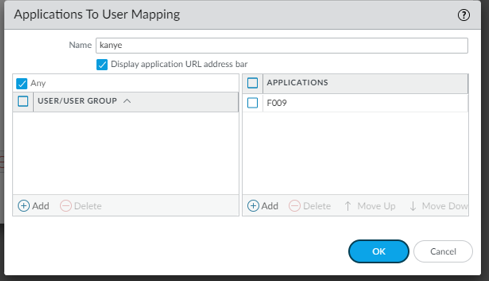
Step 6: Access the authentication settings and ensure that the configuration aligns with the desired setup. Verify all the relevant parameters.



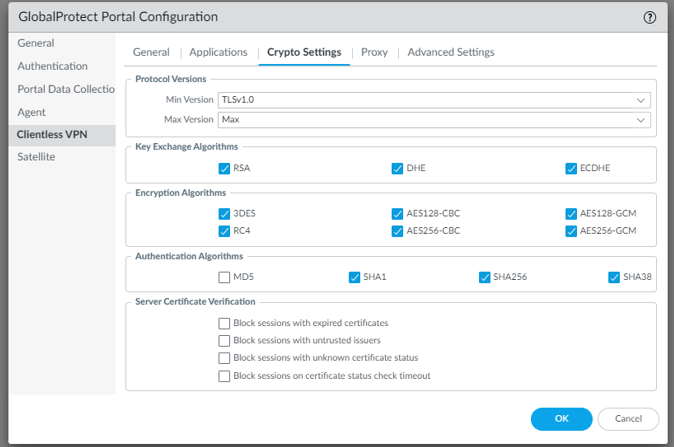
Step 7: Proceed to the Clientless VPN settings and configure the specified options as instructed.



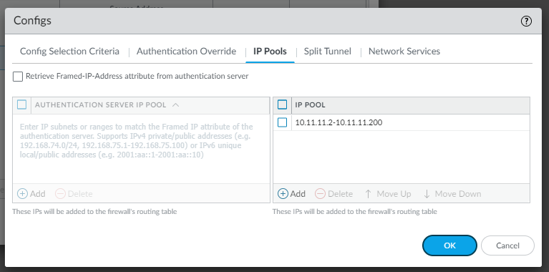
Step 8: Access the applications configuration and make the necessary adjustments as outlined.



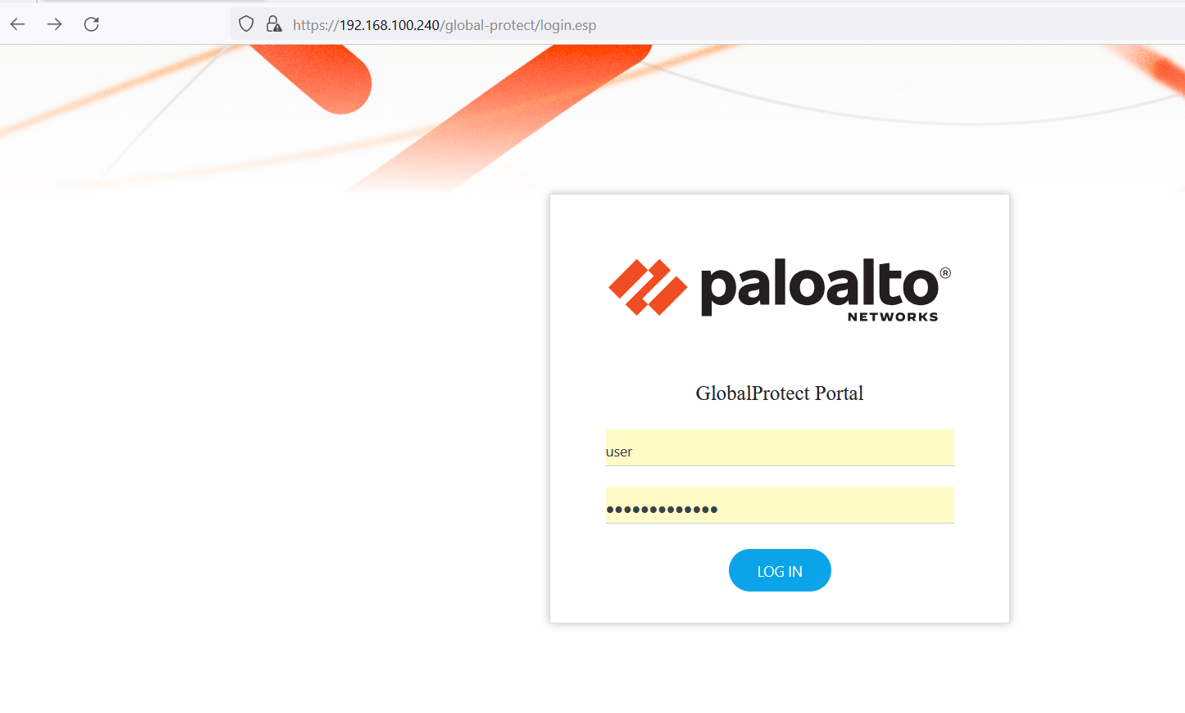
Step 9: Proceed to the Crypto Settings section and configure the specified parameters according to the provided instructions.



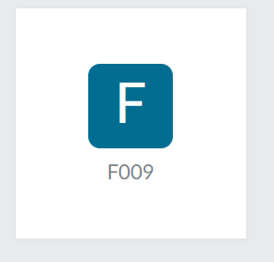
Step 10: Go to the Agent settings and access the Client Settings and IP Pools section. Modify the IP pool settings to ensure that the devices are assigned IP addresses within the same subnet.



Step 11: Once the remote user has established the connection they should access the WAN interface's IP address as instructed.



Step 12: Open the application that has been previously configured for access.



Step 13: Access the web server that is specifically designated for this purpose.

**Problems**

Initially we encountered an issue where the clientless VPN feature was not operational on the Palo Alto firewall. This problem arose due to the oversight of not installing the necessary clientless VPN component. As a result attempts to activate the feature were unsuccessful.

To resolve this issue we took the following steps. Firstly we accessed the dynamic updates section within the firewall's configuration. Within this section we proceeded to download and install the specific clientless VPN feature that was missing. By successfully completing this installation process we were able to overcome the initial problem and activate the clientless VPN functionality on the Palo Alto firewall.

**Conclusion**

During this lab session our focus was on setting up a clientless VPN which enables users to establish a secure connection to a network using only a web browser without the requirement of installing any additional software or client applications. The objective was to streamline the process and simplify it as much as possible using the Palo Alto firewall.

Overall the configuration of the clientless VPN on the Palo Alto firewall was relatively smooth and straightforward with minimal complications encountered. The Palo Alto firewall provided user-friendly features and a clear interface facilitating the setup process.

By implementing the clientless VPN we successfully eliminated the need for users to install dedicated VPN clients on their devices. Instead they can effortlessly establish a secure connection to the network using a web browser providing a convenient and accessible method for remote access.

The lab exercise allowed us to appreciate the benefits of a clientless VPN such as the ease of deployment and the flexibility it offers to users particularly when accessing resources from public or shared computers. By leveraging the capabilities of the Palo Alto firewall we were able to achieve a streamlined and efficient setup for the clientless VPN ensuring a seamless experience for remote users.