Sarkar, Mohul (Student)

Palo Alto Remote Access VPNs using SSL Lab

Mohul Sarkar

**Purpose:**

The purpose of Palo Alto Remote Access VPNs using SSL is to provide secure and encrypted access to an organization's internal network for remote users. SSL VPNs establish a secure connection between the user's device and the organization's network over the public internet, allowing users to access network resources as if they were directly connected to the internal network.

**Background Information on Lab Concepts:**

A clientless VPN, also known as an SSL VPN or browser-based VPN, is a type of VPN that allows users to securely access private networks and resources without requiring the installation of a dedicated VPN client software on their devices. Instead, users can establish a VPN connection directly through a web browser. Clientless VPNs provide a web-based interface or portal that users can access using a standard web browser. This interface acts as a gateway to the private network and allows users to authenticate and access network resources. VPNs operate through a web browser; they are generally platform independent. Users can access the VPN from various devices and operating systems, including Windows, macOS, Linux, and mobile platforms like iOS and Android, without needing specific VPN client software. Clientless VPNs are particularly useful for remote workers, contractors, or partners who need secure access to specific resources on a private network without the need for complex VPN client installations.

SSL is a cryptographic protocol that provides secure communication over the internet. It was developed by Netscape in the 1990s and has been succeeded by Transport Layer Security (TLS) as its successor protocol. However, the term SSL is still commonly used to refer to both SSL and TLS.

SSL is widely used in various applications and protocols, including remote access VPNs, web browsing (HTTPS), email services (SMTPS, IMAPS), and more. It operates at the transport layer of the TCP/IP protocol stack and ensures secure and encrypted communication between a client and a server. Some terms to note about SSL is the Handshake Protocol which is responsible for establishing a secure connection between the client and server. It performs several key functions, including negotiating the version of SSL/TLS, authenticating the server (and optionally the client), and agreeing on the encryption algorithms and cryptographic parameters to be used. Another key component to VPNs using SSL are certificates. Certificates are digital documents that serve as identification and trust mechanisms in SSL/TLS. They are issued by trusted certificate authorities and contain information such as the website's domain name, public key, and the CA's digital signature. Certificates allow the client to verify the authenticity of the server and establish a secure connection.

**Lab Summary:**

In a Palo Alto Remote Access VPNs using SSL lab, you would set up the infrastructure and configure the SSL VPN settings on the Palo Alto firewall. Customize the SSL VPN portal, test and troubleshoot the SSL VPN, ensuring successful connections and proper SSL encryption. The lab aims to familiarize you with configuring and managing Palo Alto's SSL VPN solution, providing secure remote access to network resources.

**Lab Commands:**

Step 1) Navigate to previous labs containing SOHO and remote access configuration and apply settings to firewall.

Step 2) Navigate to Dynamic Updates and Download GlobalProtect Clientless VPN

A screenshot of a computer

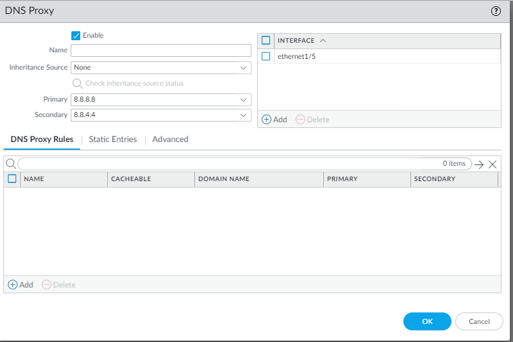
Description automatically generated with low confidence

Step 3) Navigate to Network > Clientless Apps > Set Application Home URL

A screenshot of a computer

Description automatically generated with medium confidence

Step 4) Go to Network > DNS Proxy > create new Proxy > set Primary to 8.8.8.8 > set Secondary to 8.8.4.4 > Enable.



Step 5) Navigate to Network > GlobalProtect > Portals > create new portal and assign interface.

A screenshot of a computer

Description automatically generated

Step 6) Within the same settings box, Select Authentication and verify configuration.

A screenshot of a computer

Description automatically generated with medium confidence

Step 7) Within the same settings box, Navigate to Clientless VPN and set a VPN address and the DNS Proxy

A screenshot of a computer

Description automatically generated with medium confidence

Step 8) Within Clientless VPN > Applications > create a new application to user mapping

A screenshot of a computer

Description automatically generated

Step 9) From Clientless VPN > Crypto Settings > Select following boxes

A screenshot of a computer

Description automatically generated

Step 10) Select GlobalProtect > Gateways > Enter GlobalProtect Gateway Configuration > Agent > Client Settings > IP Pools and change the IP Pool so the device is on the same subnet

A screenshot of a computer

Description automatically generated with medium confidence

Step 11) Open a new web browser and enter https:// and the ip address of the WAN Interface

A screenshot of a login screen

Description automatically generated with medium confidence

Step 12) Open the application you have created from the previous configuration.

A close up of a logo

Description automatically generated with low confidence

Step 13) View web server by using configured application.

A screenshot of a computer

Description automatically generated with medium confidence

Lab Complete.

**Problems:**

As I configured this lab I encountered some simple resolvable problems. One possible issue was incorrect SSL/TLS settings, leading to connection failures or insecure connections. To resolve this, I verified and adjusted the SSL/TLS settings to align with the desired security protocols and cipher suites. Another problem I faced is authentication failure, where users are unable to authenticate and access the SSL VPN portal. I reviewed the authentication settings, ensured the correct methods are configured, and troubleshooted any authentication server connectivity issues. Access control issues also arose, preventing users from accessing network resources or clientless apps. To address this, I reviewed the access control policies, adjusted them as needed to grant appropriate access permissions based on user roles, zones, or applications. By addressing these problems, I ensured smooth and secure operation of the Palo Alto Remote Access VPNs using SSL in my lab.

**Conclusion:**

Through this lab, I have learned how to configure Palo Alto Remote Access VPNs using SSL, including clientless apps and DNS proxy. I have gained knowledge in setting up the infrastructure, configuring SSL/TLS settings, creating an SSL VPN portal, implementing access control policies, and troubleshooting common issues. I now understand the importance of proper authentication, access control, DNS resolution, and endpoint security in ensuring secure remote access. This lab has equipped me with valuable skills to deploy and maintain a robust SSL VPN solution using Palo Alto Networks firewalls, enhancing the remote connectivity and security of my network.