The next generation of Cisco SSL VPN Solution

Written By Tuan Nguyen, Sunset Learning Cisco Specialized Instructor

History – A Secure Sockets Layer Virtual Private Network or SSL VPN protocol was originally developed by Netscape in 1994 to protect web transactions. Netscape continued to develop SSL until version 3.0, which was released as an Internet draft in 1996. In January 1999, the Internet Engineering Task Force (IETF) adopted the SSL protocol and called it Transport Layer Security, or TLS. TLS is also known as SSL version 3.1. Currently, almost all web browsers have implemented SSLv3 or TLSv1. Many other applications, including Cisco SSL VPN Clients, also use SSL/TLS for transmission protection.

Protocol – SSL/TLS provides endpoint authentication both for the client and the server; data encryption to ensure that it is only readable by the intended recipient; and data integrity and data authentication to ensure that the data has not been modified in transit. These services allow traffic to be protected as it traverses public network segments such as the Internet. SSL/TLS is designed to authenticate the server to the client; authenticate the client to the server (optional); select joint cryptography algorithms; generate shared secrets; and establish a protected path (an SSL/TLS tunnel) to provide protection to applications data or TCP and UDP connections.

SSL VPN does not require the installation of specialized client software on the end user's computer. In this way it is different from the traditional Internet Protocol Security (IPSec) VPN. An SSL VPN is designed to give remote users with access to Web applications, client/server applications and internal network connections.

There are three major types of SSL VPNs:

The first remote access SSL VPN architecture that is supported by the Cisco ASA security appliance is the Clientless remote access SSL VPN architecture. In this architecture, remote users use the web browser to establish an SSL/TLS session with the Cisco ASA security appliance. After bidirectional authentication, the user is presented with a web portal and the adaptive security appliance applies a set of authorization and accounting rules for the user session. The appliance may also deploy advanced security controls, such as a virtual desktop or a posture assessment to the VPN session. The Clientless SSL VPNs do not offer the complete network access that is provided by full-tunnel VPNs. To enable remote users to access enterprise applications, the security appliance acts as a proxy. It transforms web applications and some non-web applications so that they can be SSL-protected.

This type of SSL VPN can traverse most firewalls and NAT devices, because the SSL VPN encapsulation uses the HTTPS port (TCP port 443) and is indistinguishable from an HTTPS session to the transport network operator. It also allows access from endpoints that are not enterprise managed.

The second remote access VPN architecture that the Cisco ASA security appliance supports is the full-tunnel (client-based) remote access SSL VPN architecture. In this architecture, remote users use the Cisco AnyConnect VPN Client to establish an SSL/TLS tunnel with the appliance. After bidirectional authentication, the appliance applies a set of authorization and accounting rules to the user session and may deploy advanced security controls, such as a posture assessment using Cisco Secure Desktop to the VPN session.

After the appliance establishes an acceptable VPN environment with the remote user, the user can forward raw IP traffic into the SSL/VPN tunnel, because the Cisco AnyConnect Client creates a virtual network interface on the client to provide this functionality. The client can use any application to access any resource behind the Cisco ASA security appliance VPN gateway, subject to access rules that are applied to the VPN session.

This type of SSL VPN supports any IP application without application modification. It does not require any user training, except for how to initiate and terminate the VPN connection. It supports low-latency forwarding and enables the use of real-time applications, such as IP voice and real-time video. It is recommended that the use of DTLS encapsulation to support such applications. It can traverse most firewalls and Network Address Translation (NAT) devices, because the SSL VPN encapsulation uses the HTTPS port (TCP port 443) and is indistinguishable from an HTTPS session to the transport network operator. It is mostly used on managed devices that are typically more trustworthy compared to unmanaged devices because it is limited to users that have the Cisco AnyConnect VPN Client. The auto-update feature enables the security appliance to automatically push updates to the Cisco AnyConnect clients. It supports web launch to the full-tunnel client from the clientless portal.

The third remote access VPN architecture that the Cisco ASA security appliance supports is the full-tunnel (client-based) remote access IPsec VPN architecture. In this architecture, remote users use Cisco AnyConnect 3.0 or Cisco IPsec VPN Client to establish an IPsec tunnel with the appliance. Just like with the tunneling remote access SSL VPN, after bidirectional authentication, the appliance applies a set of authorization and accounting rules to the user session. After the Cisco ASA security appliance establishes an acceptable VPN policy for the remote user, the remote user can forward raw IP traffic into the IPsec tunnel. The client can use any application to access any resource behind the appliance VPN gateway, subject to access rules that are applied to the VPN session.

Its benefits are the same as the second remote access VPN.

The Cisco ASA security appliance also supports the full-tunnel Site-to-Site VPNs. In this type of VPN, remote networks use an IPsec VPN device, a VPN gateway, to establish an IPsec tunnel with the appliance. The Cisco ASA security appliance supports IPsec as the encapsulation method for Site-to-Site VPNs. It also interoperates with standard IKE (Internet Key Exchange) and IPsec VPN peers, such as Cisco IOS Software routers and third-party IPsec VPN devices.

Its benefits are the same as the second and third remote access VPN.

The Cisco ASA security appliance also supports IPv6 in LAN-to-LAN VPNs. Ensure that the topology in use supports IPv6. The following topologies are supported if both peers are Cisco ASA security appliances running Cisco ASA Software Version 8.4 and later:

- The appliances have IPv4 inside networks and the outside network is IPv6 (IPv4 addresses on the inside interfaces and IPv6 addresses on the outside interfaces).
- The appliances have IPv6 inside networks and the outside network is IPv4 (IPv6 addresses on the inside interfaces and IPv4 addresses on the outside interfaces).
- The appliances have IPv6 inside networks and the outside network is IPv6 (IPv6 addresses on the inside and outside interfaces).

The traditional Cisco IPsec VPN client does not support the use of IPv6. However, the Cisco AnyConnect 3.0 client does support IPv6. Therefore, the use of the Cisco AnyConnect 3.0 client is a must in order to support for remote access that uses IPv6.