Clientless SSL VPN Overview

Introduction to Clientless SSL VPN

Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first authenticates with a Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources.

Note Security contexts (also called firewall multimode) and Active/Active stateful failover are not supported when Clientless SSL VPN is enabled.

Clientless SSL VPN creates a secure, remote-access VPN tunnel to an ASA using a web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP. They include:

- Internal websites.
- Web-enabled applications.
- NT/Active Directory file shares.
- Microsoft Outlook Web Access Exchange Server 2000, 2003, 2007, and 2013.
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later.
- Application Access (smart tunnel or port forwarding access to other TCP-based applications).

Clientless SSL VPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide the secure connection between remote users and specific, supported internal resources that you configure as an internal server. The ASA recognizes connections that must be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of Clientless SSL VPN sessions on a group basis. Users have no direct access to resources on the internal network.

Prerequisites for Clientless SSL VPN

See the Supported VPN Platforms, Cisco ASA 5500 Series for the platforms and browsers supported by Clientless SSL VPN on the ASA.

Guidelines and Limitations for Clientless SSL VPN

- ActiveX pages require that you enable ActiveX Relay or enter **activex-relay** on the associated group policy. If you do so or assign a smart tunnel list to the policy, and the browser proxy exception list on the endpoint specifies a proxy, the user must add a “shutdown.webvpn.relay.” entry to that list.
- The ASA does not support clientless access to Windows Shares (CIFS) Web Folders from Windows 7, Vista, Internet Explorer 8 to 10, Mac OS X, or Linux.
- Certificate authentication, including the DoD Common Access Card and SmartCard, works with the Safari keychain only.
- Even if you install a trusted certificate for clientless connections, clients might see an untrusted certificate warning.
- The ASA does not support DSA certificates for Clientless SSL VPN connections. RSA certificates are supported.
- Some domain-based security products have requirements beyond those requests that originate from the ASA.
- Configuration control inspection and other inspection features under the Modular Policy Framework are not supported.
- Neither NAT or PAT is applicable to the client.
- Because AnyConnect works on lower network layers without a dependency to web content, we recommend that you configure AnyConnect on ASA to access web applications that seem unsupported with clientless WebVPN.
- Some components of Clientless SSL VPN require the Java Runtime Environment (JRE). With Mac OS X v10.7 and later, Java is not installed by default. For details of how to install Java on Mac OS X, see http://java.com/en/download/faq/java_mac.xml.
- When a clientless VPN session is initiated, RADIUS accounting start messaging is generated. The start message will not contain a Framed-IP-Address because addresses are not assigned to clientless VPN sessions. If a Layer3 VPN connection is subsequently initiated from the clientless portal page, an address is assigned and is reported to the RADIUS server in an interim-update accounting message. You can expect similar RADIUS behavior when a Layer3 VPN tunnel is established using the weblaunch feature. In this case, the accounting start message is sent without a framed IP address after a user is authenticated but before the Layer3 tunnel is established. This start message is followed by an interim update message once the Layer3 tunnel is established.

- HTML pages must abide by RFC 2616. Any empty line after a header is interpreted as the start of the body. Thus, if you insert empty lines between headers, some headers might appear in the body, and users might need to refresh their windows to correct page problems.
- The clientless WebVPN Java rewriter, which is used for Java code processing, does not support Oracle Forms.
- Clientless WebVPN rewriter is not able to detect JavaScript object bracket notation assignments, as they are dynamically set in runtime.
- Clientless WebVPN does not support spaces between chunk-size and CRLF in the server's responses, as ASA does not expect spaces in chunk-size and is not able to put chunks together.
- Content Security Policy (CSP) is not supported.
- Angular custom event listeners and location changes may not work properly using Clientless WebVPN rewriter.
- Clientless WebVPN does not have support for Cross-Origin Resource Sharing (CORS) filters on the server-side.
- Clientless WebVPN rewriter currently does not support HTML5 and Javascript Blob API.
- According to the WebVPN architecture, Fetch API is not supported.
- Clientless WebVPN doesn't share MDM attributes with a RADIUS server when authenticating.
- When you have several group policies configured for the clientless portal, they are displayed in a drop-down on the logon page. When the first group policy in the list requires a certificate, then the user must have a matching certificate. If some of your group policies do not use certificates, you must configure the list to display a non-certificate policy first. Alternatively, you may want to create a dummy group policy with the name “0-Select-a-group.”

  

  Tip You can control which policy is displayed first by naming your group polices alphabetically, or prefix them with numbers. For example, 1-AAA, 2-Certificate.

- Links to pages on another server must be routable from the ASA, or the user might see the following error. Ensure that your links are usable, and are not blocked by access control rules, SSL configuration, or other firewall features, and that there is a route to the server.

```
Connection failed, Server "<DNS name>" unavailable.
```

Licensing for Clientless SSL VPN

Use of the AnyConnect Secure Mobility Client requires that you purchase either an AnyConnect Plus and Apex license. The license(s) required depends on the AnyConnect VPN Client and Secure Mobility features that you plan to use, and the number of sessions that you want to support. These user-based licences include access to support and software updates to align with general BYOD trends.

AnyConnect 4.4 licenses are used with ASA (and also ISR, CSR, and ASR), as well as other non-VPN headends such as Identity Services Engine (ISE), Cloud Web Security (CWS), and Web Security Appliance

(WSA). A consistent model is used regardless of the headend, so there is no impact when headend migrations occur.

For a full description of the licensing model for AnyConnect, refer to http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.