Clientless SSL VPN

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.
- email proxies, including POP3S, IMAP4S, and SMTPS.
- Microsoft Outlook Web Access Exchange Server 2000, 2003, and 2007.
- 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

See the *Supported VPN Platforms, Cisco ASA Series* for the platforms and browsers supported by ASA Release 9.0.

Guidelines and Limitations

- 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.
- The ASA does not support DSA or RSA certificates for Clientless SSL VPN connections.
- 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.
- The *vpn-filter* command under group policy is for client-based access and is not supported. *Filter* under Clientless SSL VPN mode in group policy is for clientless-based access only.
- Neither NAT or PAT is applicable to the client.
- The ASA does not support the use of the QoS rate-limiting commands, such as **police** or **priority-queue**.
- The ASA does not support the use of connection limits, checking via the static or the Modular Policy Framework **set connection** command.
- 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 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.