Understanding the AnyConnect SSL VPN Connection Flow

Contents

Introduction

This document focuses on the flow of events that take place between AnyConnect and the secure gateway during an SSLVPN connection.

Background Information

AnyConnect

AnyConnect is the Cisco VPN client designed for SSL and IKEv2 protocols. It is available for most of the desktop and mobile platforms. AnyConnect primarily establishes secure connections with Firepower Threat Defense (FTD), Adaptive Security Appliances (ASA), or Cisco IOS®/Cisco IOS® XE routers referred to as Secure Gateways.

Secure Gateway

In Cisco terminology, an SSL VPN server is referred to as a Secure Gateway, while an IPSec (IKEv2) server is known as a Remote Access VPN Gateway. Cisco supports SSL VPN tunnel termination on these platforms:

- Cisco ASA 5500 and 5500-X Series
- Cisco FTD (2100, 4100, and 9300 Series)
- Cisco ISR 4000 and ISR G2 Series
- Cisco CSR 1000 Series
- Cisco Catalyst 8000 Series

AnyConnect SSL VPN Connection Flow

This document breaks down the events that take place between AnyConnect and the Secure Gateway during an SSL VPN connection establishment into six phases:

1. SSL Handshake

2. POST - Group Selection

3. POST - User Authentication with Username/Password (Optional)

4. VPN Downloader (Optional)

5. CSTP CONNECT

6. DTLS Connection (Optional)

1. SSL Handshake

The SSL handshake is initiated by the AnyConnect client after the completion of the TCP 3-way handshake with a 'Client Hello' message. The flow of events and the key takeaways are as mentioned.

Client Hello

The SSL session begins with the client sending a 'Client Hello' message. In this message:

a) The SSL Session ID is set to 0, indicating the initiation of a new session.

b) The payload includes the client-supported cipher suites and a client-generated random nonce.

Server Hello

The server responds with a "Server Hello" message, which includes:

a) The selected cipher suite from the list provided by the client.

b) The server generated the SSL Session ID, and a server generated a random nonce.

Server Certificate

After the 'Server Hello', the server transmits its SSL certificate, which serves as its identity. Key points to note include:

a) If this certificate fails a strict validation check, AnyConnect, by default, blocks the server.

b) The user has the option to disable this block, but subsequent connections display a warning until the reported errors are resolved.

Client Certificate Request

The server can also request a client certificate, sending a list of Subject Name DNs of all the CA certificates loaded on the Secure Gateway. This request serves two purposes:

a) It helps the client (user) choose the correct identity certificate if multiple ID certificates are available.

b) Ensures that the returned certificate is trusted by the Secure Gateway, although further certificate validation must still occur.

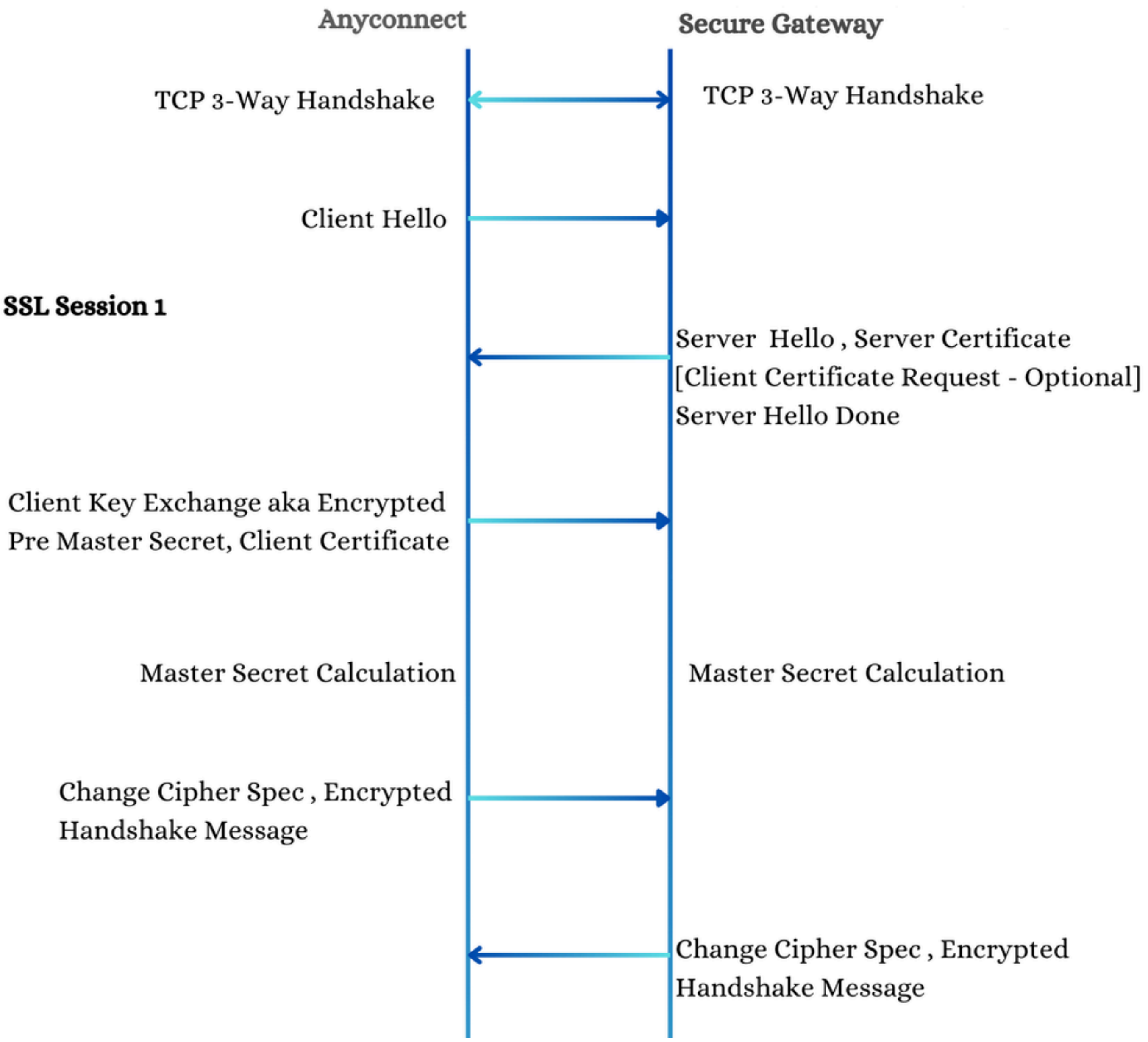
Client Key Exchange

The client then sends a 'Client Key Exchange' message, which includes a pre-master secret key. This key is encrypted using:

a) The public key of the server from the server certificate, if the chosen cipher suite is RSA-based (for example, TLS_RSA_WITH_AES_128_CBC_SHA).

b) The DH public key of the server provided in the Server Hello message, if the chosen cipher suite is DHE-based (for example, TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Based on the pre-master secret, the client-generated random nonce, and the server-generated random nonce, both the client and the Secure Gateway independently generate a master secret. This master secret is then used to derive session keys, ensuring secure communication between the client and the server.


Anyconnect
Secure Gateway
TCP 3-Way Handshake
TCP 3-Way Handshake
Client Hello
SSL Session 1
Server Hello , Server Certificate
[Client Certificate Request - Optional]
Server Hello Done
Client Key Exchange aka Encrypted
Pre Master Secret, Client Certificate
Master Secret Calculation
Master Secret Calculation
Change Cipher Spec , Encrypted
Handshake Message
Change Cipher Spec , Encrypted
Handshake Message

SSL Session 1

2. POST - Group Selection

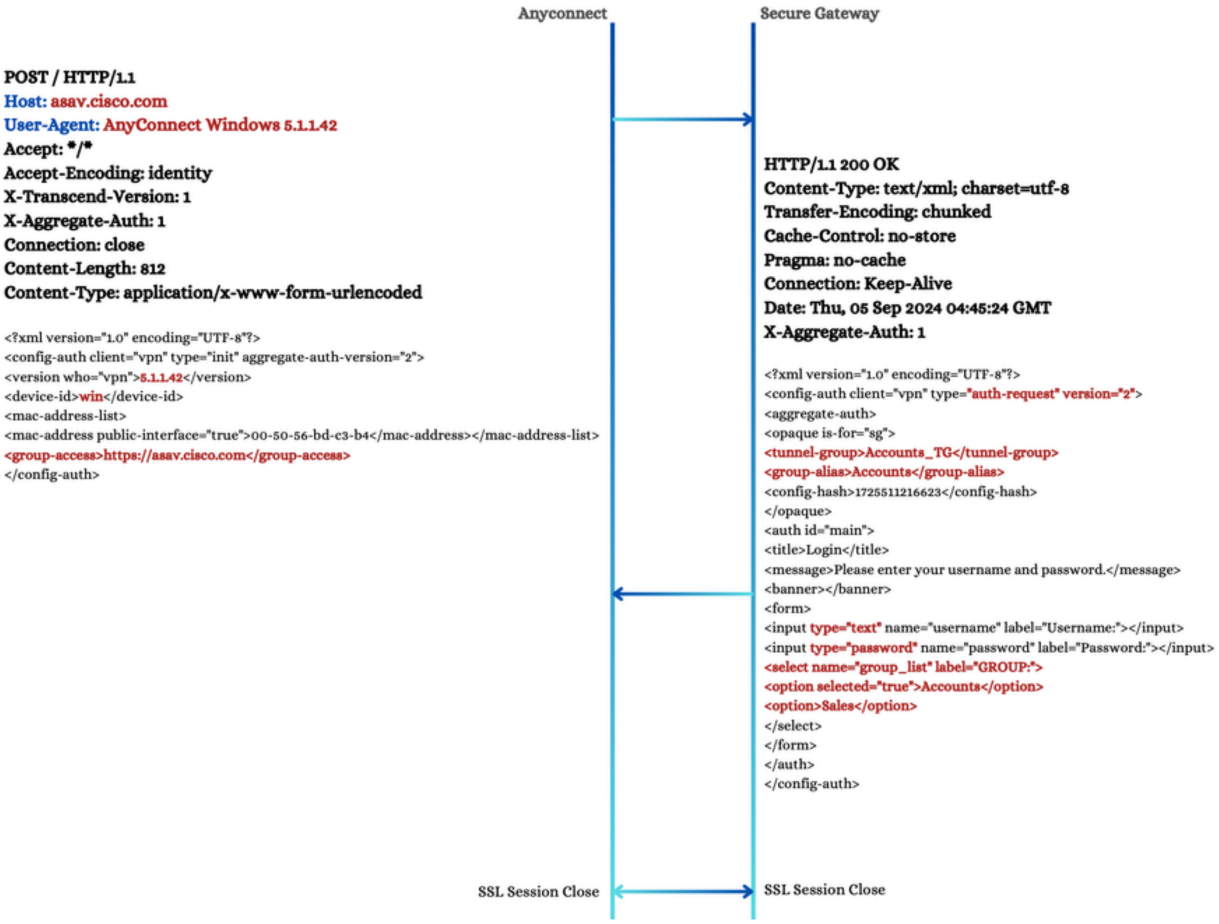
During this operation, the client does not possess information about the connection profile unless explicitly specified by the user. The connection attempt is directed towards the Secure Gateway URL (**asav.cisco.com**), as indicated by the 'group-access' element in the request. The client indicates its support for '**aggregate-authentication**' version 2. This version represents a significant improvement over the earlier version, particularly in terms of efficient XML transactions. Both the secure gateway and the client must agree on the version to be used. In scenarios where the secure gateway does not support version 2, an additional POST operation is triggered, causing the client to fall back to the version.

In the HTTP response, the secure gateway indicates these:

1. The version of aggregate authentication that the secure gateway supports.

2. Tunnel group list and the Username/Password Form.

Note: The Form includes a 'select' element, which lists the group aliases of all connection profiles configured on the secure gateway. By default, one of these group aliases is highlighted with the selected = "true" boolean attribute. The tunnel-group and group-alias elements correspond to this chosen connection profile.

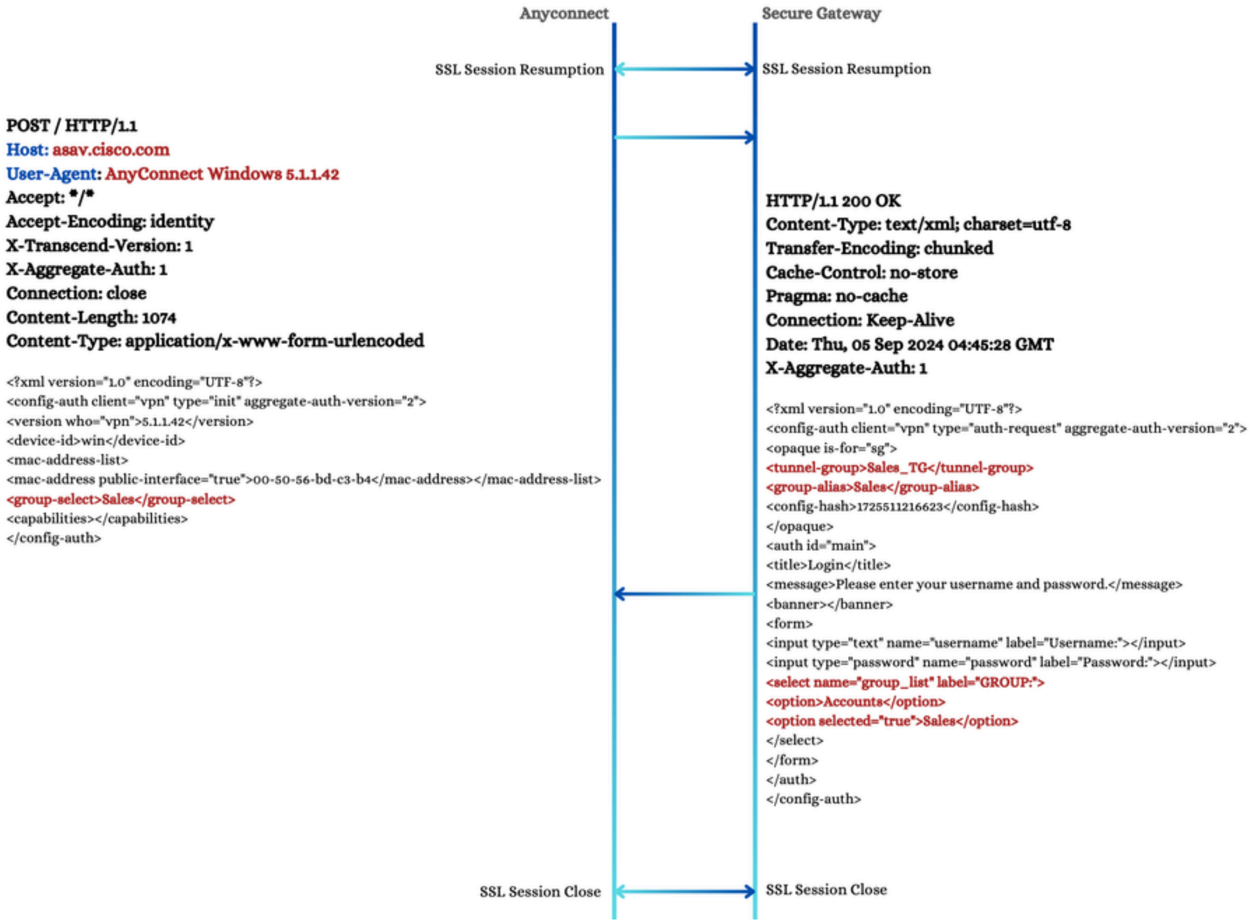


```
POST / HTTP/1.1
Host: asav.cisco.com
User-Agent: AnyConnect Windows 5.1.1.42
Accept: */*
Accept-Encoding: identity
X-Transcend-Version: 1
X-Aggregate-Auth: 1
Connection: close
Content-Length: 812
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="init" aggregate-auth-version="2">
<version who="vpn">5.1.1.42</version>
<device-id>win</device-id>
<mac-address-list>
<mac-address public-interface="true">00-50-56-bd-c3-b4</mac-address></mac-address-list>
<group-access>https://asav.cisco.com</group-access>
</config-auth>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Thu, 05 Sep 2024 04:45:24 GMT
X-Aggregate-Auth: 1

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request" version="2">
<aggregate-auth>
<opaque is-for="sg">
<tunnel-group>Accounts_TG</tunnel-group>
<group-alias>Accounts</group-alias>
<config-hash>1725511216623</config-hash>
</opaque>
<auth id="main">
<title>Login</title>
<message>Please enter your username and password.</message>
<banner></banner>
<form>
<input type="text" name="username" label="Username:"></input>
<input type="password" name="password" label="Password:"></input>
<select name="group_list" label="GROUP:">
<option selected="true">Accounts</option>
<option>Sales</option>
</select>
</form>
</auth>
</config-auth>
```

POST - Group Selection 1

If the user chooses a different connection profile from this list, another POST operation takes place. In this case, the client sends a POST request with the 'group-select' element updated in order to reflect the chosen connection profile, as shown here.



```
POST / HTTP/1.1
Host: asav.cisco.com
User-Agent: AnyConnect Windows 5.1.1.42
Accept: */*
Accept-Encoding: identity
X-Transcend-Version: 1
X-Aggregate-Auth: 1
Connection: close
Content-Length: 1074
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="init" aggregate-auth-version="2">
<version who="vpn">5.1.1.42</version>
<device-id>win</device-id>
<mac-address-list>
<mac-address public-interface="true">00-50-56-bd-c3-b4</mac-address></mac-address-list>
<group-select>Sales</group-select>
<capabilities></capabilities>
</config-auth>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Thu, 05 Sep 2024 04:45:28 GMT
X-Aggregate-Auth: 1

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request" aggregate-auth-version="2">
<opaque is-for="sg">
<tunnel-group>Sales_TG</tunnel-group>
<group-alias>Sales</group-alias>
<config-hash>1725511216623</config-hash>
</opaque>
<auth id="main">
<title>Login</title>
<message>Please enter your username and password.</message>
<banner></banner>
<form>
<input type="text" name="username" label="Username:"></input>
<input type="password" name="password" label="Password:"></input>
<select name="group_list" label="GROUP:">
<option>Accounts</option>
<option selected="true">Sales</option>
</select>
</form>
</auth>
</config-auth>
```

POST - Group Selection 2

3. POST - User Authentication

In this operation, which follows the POST-Group Selection, AnyConnect sends this information to the Secure Gateway:

1. Chosen Connection Profile Information: This includes the tunnel-group name and the group alias as indicated by the Secure Gateway in the earlier operation.

2. Username and Password: The authentication credentials of the user.

Note: Since this flow is specific to AAA authentication, it can differ from other authentication methods.

In response to the POST operation, the Secure Gateway sends an **XML** file containing this information:

1. Session ID: This is not the same as the SSL session ID.

2. Session Token: This token is later used by the client as the WebVPN cookie.

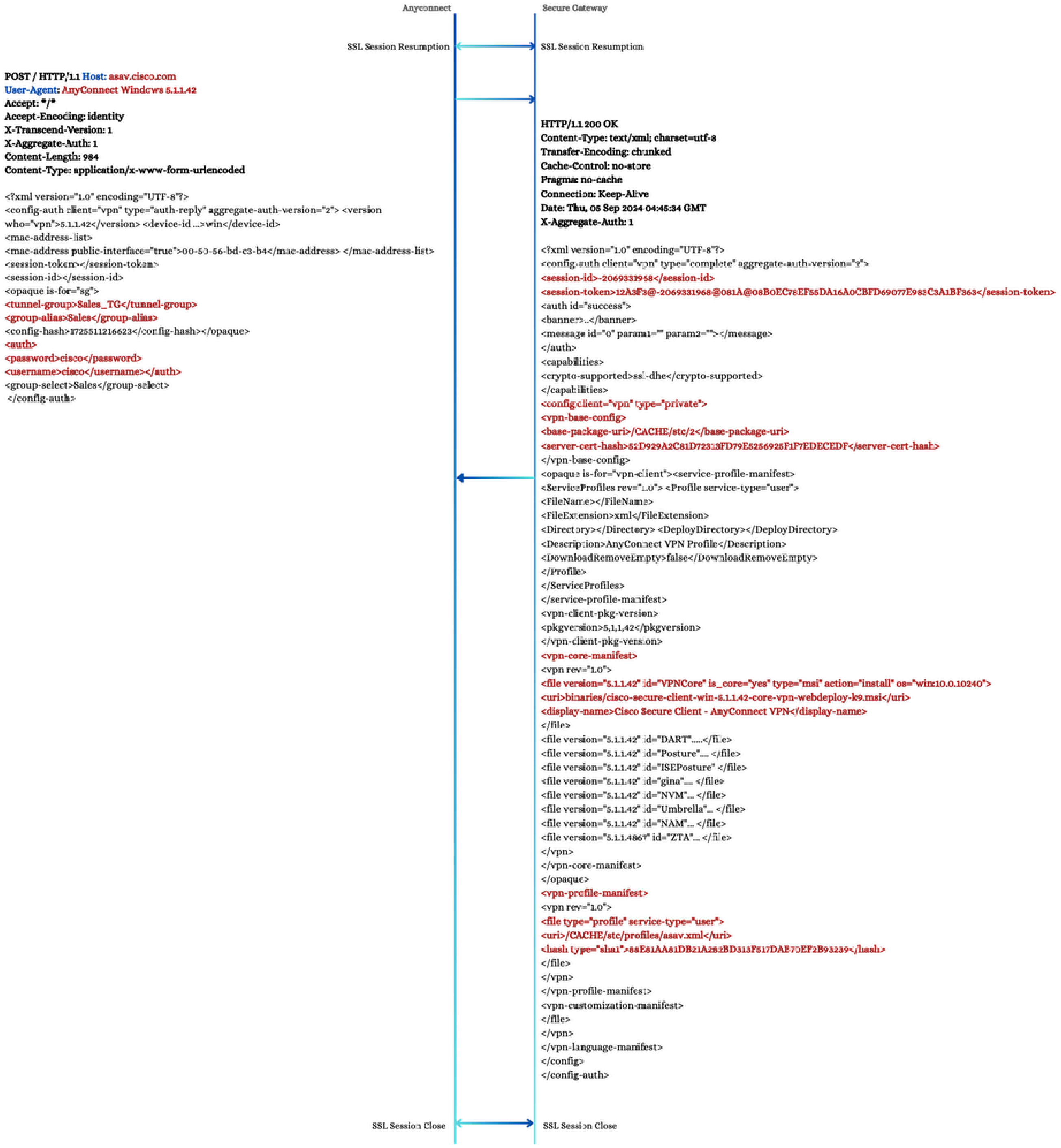
3. Authentication Status: Indicated by an auth element with id = 'success'.

4. Server Certificate Hash: This hash is cached in the **preferences.xml** file.

5. vpn-core-manifest Element: This element indicates the path and version of the AnyConnect core package, along with other components like Dart, Posture, ISE Posture, and so on. It is used by the VPN Downloader in the next section.

6. vpn-profile-manifest Element: This element indicates the path (the name of the profile) and the SHA-1 hash of the profile.

Note: If the client does not have the profile, the VPN Downloader in the next section downloads it. If the client already has the profile, the SHA-1 hash of the client profile is compared with that of the server. In case of a mismatch, the VPN Downloader overwrites the client profile with the one on the Secure Gateway. This ensures that the profile on the Secure Gateway is enforced on the client post-authentication.



```
POST / HTTP/1.1 Host: asav.cisco.com
User-Agent: AnyConnect Windows 5.1.1.42
Accept: */*
Accept-Encoding: identity
X-Transcend-Version: 1
X-Aggregate-Auth: 1
Content-Length: 984
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-reply" aggregate-auth-version="2"> <version
who="vpn">5.1.1.42</version> <device-id ...>win</device-id>
<mac-address-list>
<mac-address public-interface="true">00-50-56-bd-c3-b4</mac-address> </mac-address-list>
<session-token></session-token>
<session-id></session-id>
<opaque is-for="sg">
<tunnel-group>Sales_TG</tunnel-group>
<group-alias>Sales</group-alias>
<config-hash>1725511216623</config-hash></opaque>
<auth>
<password>cisco</password>
<username>cisco</username></auth>
<group-select>Sales</group-select>
 </config-auth>
```

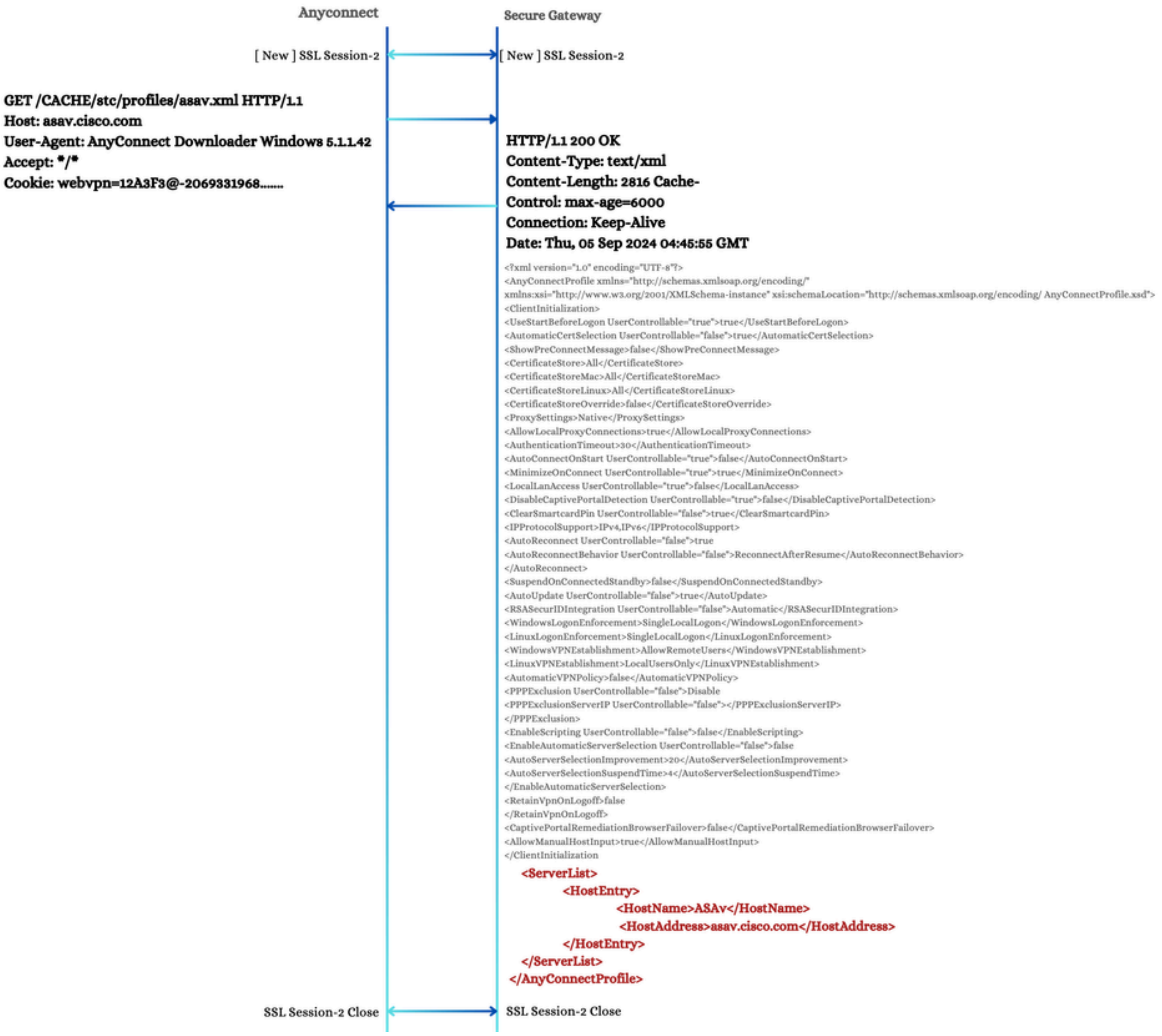
```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Transfer-Encoding: chunked
Cache-Control: no-store
Pragma: no-cache
Connection: Keep-Alive
Date: Thu, 05 Sep 2024 04:45:34 GMT
X-Aggregate-Auth: 1

<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="complete" aggregate-auth-version="2">
<session-id>-2069331968</session-id>
<session-token>12A3F3@-2069331968@081A@08B0EC78EF55DA16A0CBFD69077E983C3A1BF363</session-token>
<auth id="success">
<banner>..</banner>
<message id="0" param1="" param2=""></message>
</auth>
<capabilities>
<crypto-supported>ssl-dhe</crypto-supported>
</capabilities>
<config client="vpn" type="private">
<vpn-base-config>
<base-package-uri>/CACHE/stc/2</base-package-uri>
<server-cert-hash>52D929A2C81D72313FD79E5256925F1F7EDECEDF</server-cert-hash>
</vpn-base-config>
<opaque is-for="vpn-client"><service-profile-manifest>
<ServiceProfiles rev="1.0"> <Profile service-type="user">
<FileName></FileName>
<FileExtension>xml</FileExtension>
<Directory></Directory> <DeployDirectory></DeployDirectory>
<Description>AnyConnect VPN Profile</Description>
<DownloadRemoveEmpty>false</DownloadRemoveEmpty>
</Profile>
</ServiceProfiles>
</service-profile-manifest>
<vpn-client-pkg-version>
<pkgversion>5,1,1,42</pkgversion>
</vpn-client-pkg-version>
<vpn-core-manifest>
<vpn rev="1.0">
<file version="5.1.1.42" id="VPNCore" is_core="yes" type="msi" action="install" os="win:10.0.10240">
<uri>binaries/cisco-secure-client-win-5.1.1.42-core-vpn-webdeploy-k9.msi</uri>
<display-name>Cisco Secure Client - AnyConnect VPN</display-name>
</file>
<file version="5.1.1.42" id="DART".....</file>
<file version="5.1.1.42" id="Posture".... </file>
<file version="5.1.1.42" id="ISEPosture" </file>
<file version="5.1.1.42" id="gina".... </file>
<file version="5.1.1.42" id="NVM"... </file>
<file version="5.1.1.42" id="Umbrella"... </file>
<file version="5.1.1.42" id="NAM"... </file>
<file version="5.1.1.4867" id="ZTA"... </file>
</vpn>
</vpn-core-manifest>
</opaque>
<vpn-profile-manifest>
<vpn rev="1.0">
<file type="profile" service-type="user">
<uri>/CACHE/stc/profiles/asav.xml</uri>
<hash type="sha1">88E81AA81DB21A282BD313F517DAB70EF2B93239</hash>
</file>
</vpn>
</vpn-profile-manifest>
<vpn-customization-manifest>
</file>
</vpn>
</vpn-language-manifest>
</config>
</config-auth>
```

POST - User Authentication

4. AnyConnect Downloader

The AnyConnect Downloader always initiates a new SSL session, which is why users can encounter a second certificate warning if the certificate of the Secure Gateway is untrusted. During this phase, it performs separate GET operations for each item that needs to be downloaded.

Note: If the client profile is uploaded on Secure Gateway, it is mandatory for download; otherwise, the entire connection attempt is terminated.



```
GET /CACHE/stc/profiles/asav.xml HTTP/1.1
Host: asav.cisco.com
User-Agent: AnyConnect Downloader Windows 5.1.1.42
Accept: */*
Cookie: webvpn=12A3F3@-2069331968.......
```

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: 2816 Cache-
Control: max-age=6000
Connection: Keep-Alive
Date: Thu, 05 Sep 2024 04:45:55 GMT
```

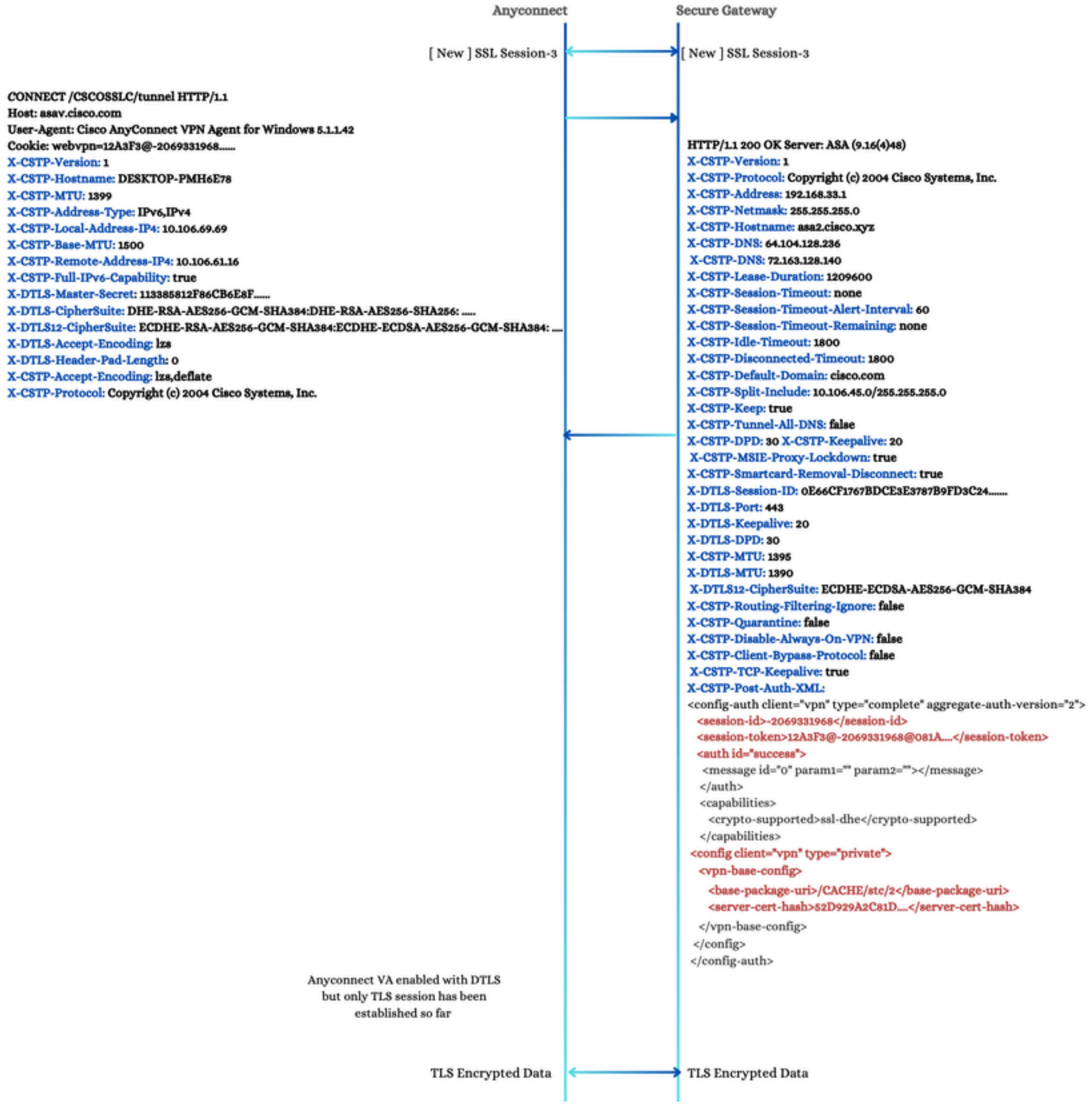
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreLinux>All</CertificateStoreLinux>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization
   <ServerList>
         <HostEntry>
                 <HostName>ASAv</HostName>
                 <HostAddress>asav.cisco.com</HostAddress>
         </HostEntry>
   </ServerList>
 </AnyConnectProfile>
```

VPN Downloader

5. CSTP CONNECT

AnyConnect performs a CONNECT operation as the final step in establishing a secure channel. During the CONNECT operation, the AnyConnect client sends various X-CSTP and X-DTLS attributes for the Secure Gateway in order to process. The Secure Gateway responds with additional X-CSTP and X-DTLS attributes that the client applies to the current connection attempt. This exchange includes the X-CSTP-Post-Auth-XML, accompanied by an **XML** file, which is largely similar to the one seen in the POST - User Authentication step.

After receiving a successful response, AnyConnect initiates the TLS data channel. Simultaneously the AnyConnect Virtual adapter interface is activated with an MTU value equal to X-DTLS-MTU, assuming that the subsequent DTLS handshake is successful.



```
CONNECT /CSCOSSLC/tunnel HTTP/1.1
Host: asav.cisco.com
User-Agent: Cisco AnyConnect VPN Agent for Windows 5.1.1.42
Cookie: webvpn=12A3F3@-2069331968......
X-CSTP-Version: 1
X-CSTP-Hostname: DESKTOP-PMH6E78
X-CSTP-MTU: 1399
X-CSTP-Address-Type: IPv6,IPv4
X-CSTP-Local-Address-IP4: 10.106.69.69
X-CSTP-Base-MTU: 1500
X-CSTP-Remote-Address-IP4: 10.106.61.16
X-CSTP-Full-IPv6-Capability: true
X-DTLS-Master-Secret: 113385812F86CB6E8F......
X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256: .....
X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384: ....
X-DTLS-Accept-Encoding: lzs
X-DTLS-Header-Pad-Length: 0
X-CSTP-Accept-Encoding: lzs,deflate
X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.
```

```
HTTP/1.1 200 OK Server: ASA (9.16(4)48)
X-CSTP-Version: 1
X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.
X-CSTP-Address: 192.168.33.1
X-CSTP-Netmask: 255.255.255.0
X-CSTP-Hostname: asa2.cisco.xyz
X-CSTP-DNS: 64.104.128.236
 X-CSTP-DNS: 72.163.128.140
X-CSTP-Lease-Duration: 1209600
X-CSTP-Session-Timeout: none
X-CSTP-Session-Timeout-Alert-Interval: 60
X-CSTP-Session-Timeout-Remaining: none
X-CSTP-Idle-Timeout: 1800
X-CSTP-Disconnected-Timeout: 1800
X-CSTP-Default-Domain: cisco.com
X-CSTP-Split-Include: 10.106.45.0/255.255.255.0
X-CSTP-Keep: true
X-CSTP-Tunnel-All-DNS: false
X-CSTP-DPD: 30 X-CSTP-Keepalive: 20
 X-CSTP-MSIE-Proxy-Lockdown: true
X-CSTP-Smartcard-Removal-Disconnect: true
X-DTLS-Session-ID: 0E66CF1767BDCE3E3787B9FD3C24.......
X-DTLS-Port: 443
X-DTLS-Keepalive: 20
X-DTLS-DPD: 30
X-CSTP-MTU: 1395
X-DTLS-MTU: 1390
 X-DTLS12-CipherSuite: ECDHE-ECDSA-AES256-GCM-SHA384
X-CSTP-Routing-Filtering-Ignore: false
X-CSTP-Quarantine: false
X-CSTP-Disable-Always-On-VPN: false
X-CSTP-Client-Bypass-Protocol: false
 X-CSTP-TCP-Keepalive: true
X-CSTP-Post-Auth-XML:
<config-auth client="vpn" type="complete" aggregate-auth-version="2">
  <session-id>-2069331968</session-id>
  <session-token>12A3F3@-2069331968@081A....</session-token>
  <auth id="success">
   <message id="0" param1="" param2=""></message>
  </auth>
  <capabilities>
    <crypto-supported>ssl-dhe</crypto-supported>
  </capabilities>
 <config client="vpn" type="private">
  <vpn-base-config>
    <base-package-uri>/CACHE/stc/2</base-package-uri>
    <server-cert-hash>52D929A2C81D....</server-cert-hash>
  </vpn-base-config>
 </config>
 </config-auth>
```

CSTP Connect

6. DTLS Handshake

The DTLS handshake proceeds as outlined here. This setup is relatively quick due to the attributes exchanged between the client and server during the CONNECT event.

Client

X-DTLS-Master-Secret: The DTLS Master Secret is generated by the client and shared with the server. This key is crucial for establishing a secure DTLS session.

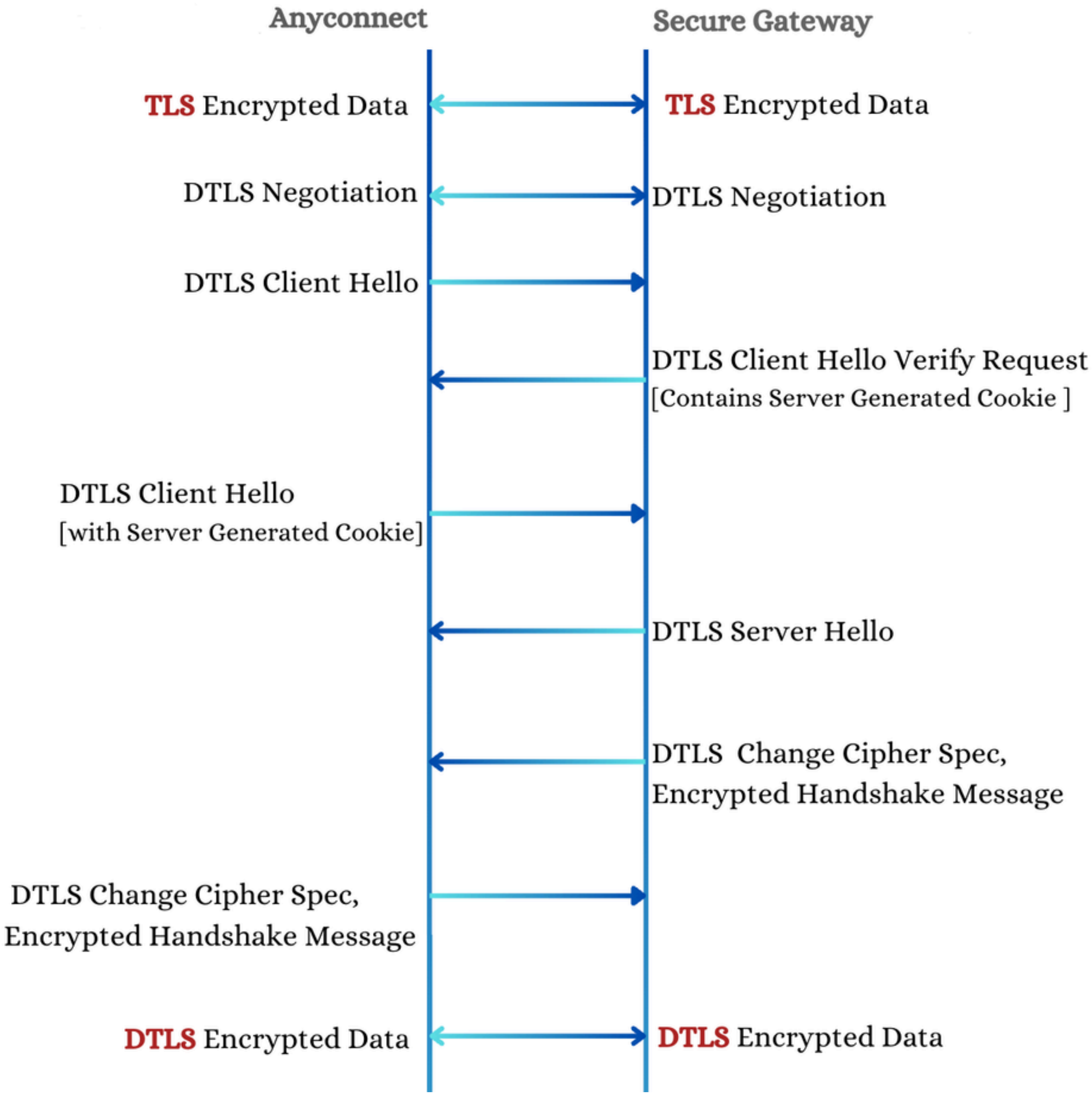
X-DTLS-CipherSuite: The list of DTLS cipher suites supported by the client, indicating the encryption capabilities of the client.

Server

X-DTLS-Session-ID: The DTLS Session ID assigned by the server for the client to use, ensuring session continuity.

X-DTLS-CipherSuite: The cipher suite selected by the server from the list provided by the client, ensuring both parties use a compatible encryption method.

Note: While the DTLS handshake is in progress, the TLS data channel continues to operate. This ensures that data transmission remains consistent and secure during the handshake process. A seamless transition to the DTLS data encryption channel occurs only after the DTLS handshake is complete.

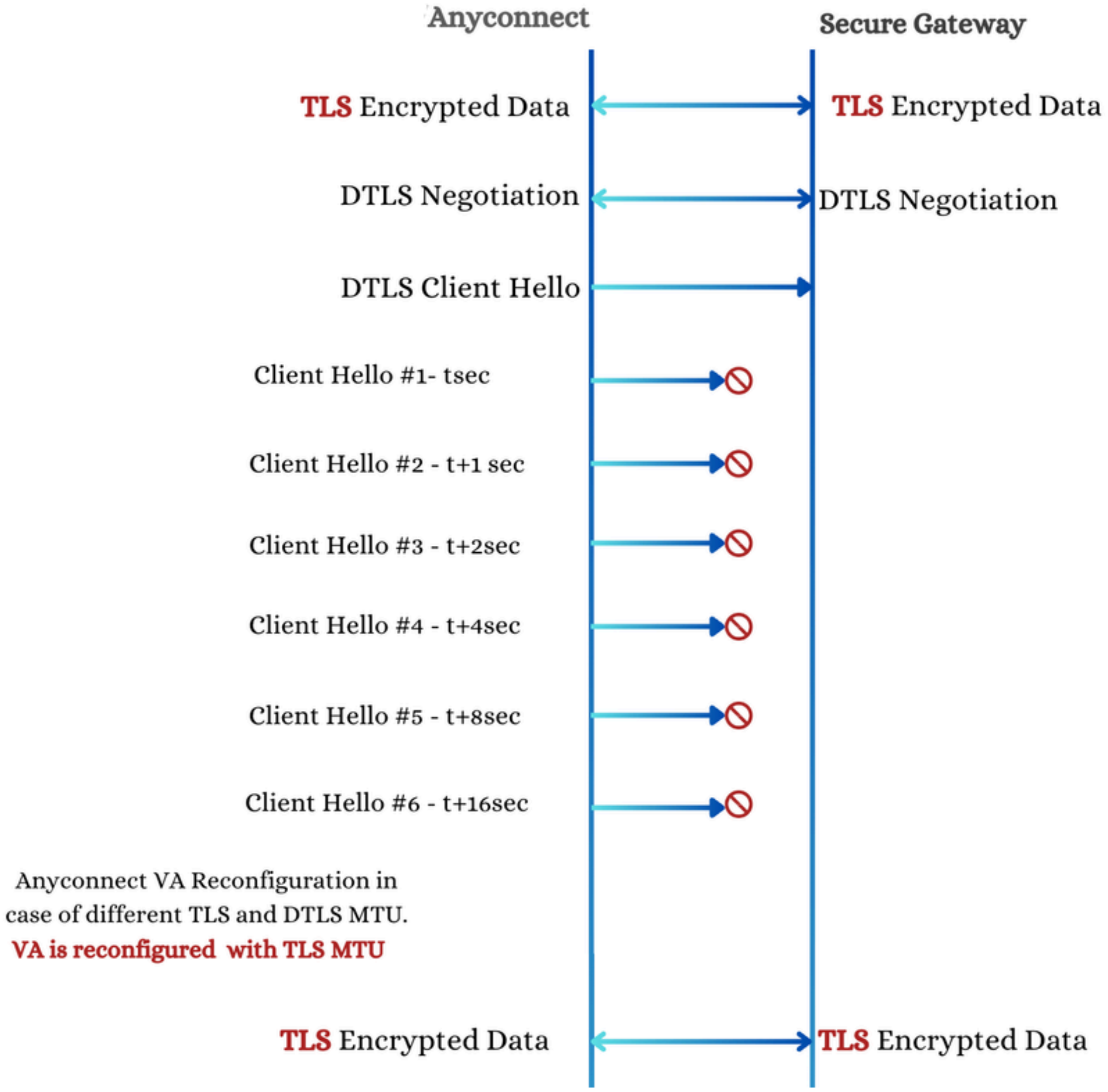


DTLS Handshake

6.1. DTLS Port Blocked

In the event that the DTLS port is blocked or the Secure Gateway fails to respond to DTLS Client Hello packets, AnyConnect performs an exponential backoff with up to five retries, beginning with a 1-second delay and increasing up to 16 seconds.

If these attempts are unsuccessful, AnyConnect then applies the actual TLS MTU, as specified by the X-CSTP-MTU value returned by the Secure Gateway in Phase 5., to the AnyConnect virtual adapter. Since this MTU differs from the earlier applied MTU (X-DTLS-MTU), a reconfiguration of the virtual adapter is necessary. This reconfiguration appears to the end-user as a reconnect attempt, though no new negotiations occur during this process. Once the virtual adapter is reconfigured, the TLS data channel continues to operate.



DTLS Port Block

Related Information

- Cisco VPN Technologies Documentation Reference
- Cisco Technical Support & Downloads