了解AnyConnect SSL VPN连接流

目录

简介

本文档重点介绍SSLVPN连接期间AnyConnect和安全网关之间发生的事件流。

背景信息

AnyConnect

AnyConnect是专为SSL和IKEv2协议设计的思科VPN客户端。它适用于大多数桌面和移动平台。AnyConnect主要通过Firepower威胁防御(FTD)、自适应安全设备(ASA)或Cisco IOS®/Cisco IOS® XE路由器（称为安全网关）建立安全连接。

安全网关

在思科术语中，SSL VPN服务器称为安全网关，而IPSec (IKEv2)服务器称为远程访问VPN网关。思科在以下平台上支持SSL VPN隧道终端：

- Cisco ASA 5500和5500-X系列
- Cisco FTD（2100、4100和9300系列）

- Cisco ISR 4000和ISR G2系列
- 思科CSR 1000系列
- Cisco Catalyst 8000 系列

AnyConnect SSL VPN连接流

本文档将SSL VPN连接建立期间AnyConnect和安全网关之间发生的事件分为六个阶段：

1. SSL握手

2. POST -组选择

3. POST -使用用户名/口令的用户身份验证（可选）

4. VPN下载程序（可选）

5. CSTP连接

6. DTLS连接（可选）

1. SSL握手

SSL握手由AnyConnect客户端在使用“Client Hello”消息完成TCP三次握手后发起。文中还介绍了事件的流程和关键要点。

客户端问候消息

SSL会话开始于客户端发送“Client Hello”消息。在此消息中：

a) SSL会话ID设置为0，表示发起新会话。

b)负载包括客户端支持的密码套件和客户端生成的随机随机随机随机随机随机数。

服务器问候消息

服务器以“Server Hello”消息做出响应，包括：

a)从客户端提供的列表中选择的密码套件。

b)服务器生成SSL会话ID，服务器生成随机随机随机随机随机随机数。

服务器证书

在“Server Hello”之后，服务器传输其SSL证书，该证书用作其身份。需要注意的要点包括：

a)如果此证书未通过严格验证检查，默认情况下，AnyConnect会阻止服务器。

b)用户可以选择禁用此阻止，但后续连接会显示警告，直到报告的错误得到解决。

客户端证书请求

服务器还可以请求客户端证书，发送安全网关上加载的所有CA证书的使用者名称DN的列表。此请求有两个作用：

a)如果有多个ID证书可用，它将帮助客户端（用户）选择正确的身份证书。

b)确保返回的证书受安全网关信任，不过仍必须进行进一步的证书验证。

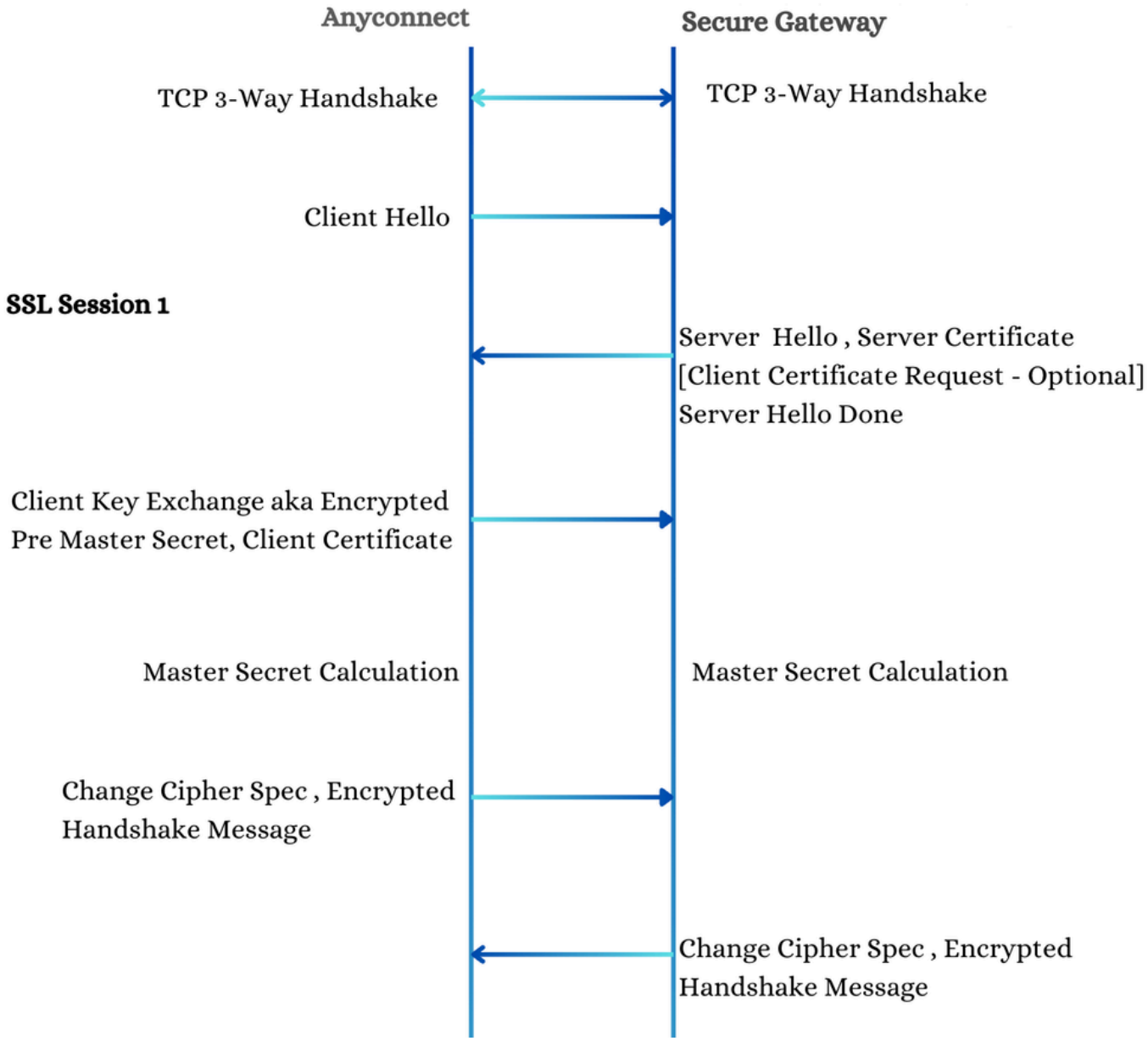
客户端密钥交换

然后，客户端发送“客户端密钥交换”消息，其中包含预主密钥。此密钥使用以下内容加密：

a)来自服务器证书的服务器的公钥（如果所选的密码套件基于RSA）（例如
，TLS_RSA_WITH_AES_128_CBC_SHA）。

b)服务器问候消息中提供的服务器DH公钥（如果所选的密码套件基于DHE）（例如
，TLS_DHE_DSS_WITH_AES_256_CBC_SHA）。

根据预主密钥、客户端生成的随机nonce和服务器生成的随机nonce，客户端和安全网关都会独立生成主密钥。然后，此主密钥用于派生会话密钥，从而确保客户端和服务器之间的安全通信。



SSL会话1

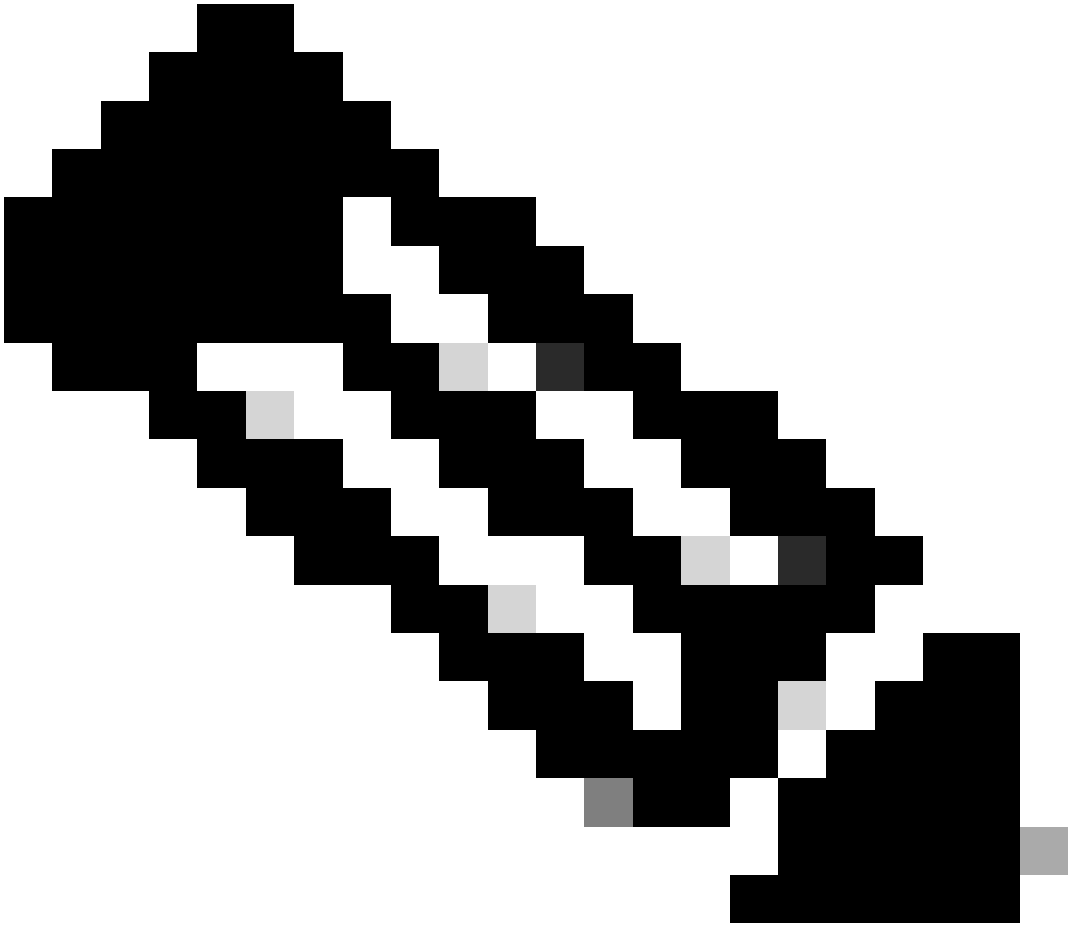
2. POST -组选择

在此操作期间，除非用户明确指定，否则客户端不拥有有关连接配置文件的信息。连接尝试被定向到安全网关URL (asav.cisco.com)，如请求中的“group-access”元素所示。客户端指示它支持“aggregate-authentication”版本2。与早期版本相比，此版本具有重大改进，尤其是在高效的XML事务方面。安全网关和客户端必须同意要使用的版本。在安全网关不支持版本2的情况下，会触发其他POST操作，导致客户端回退到版本。

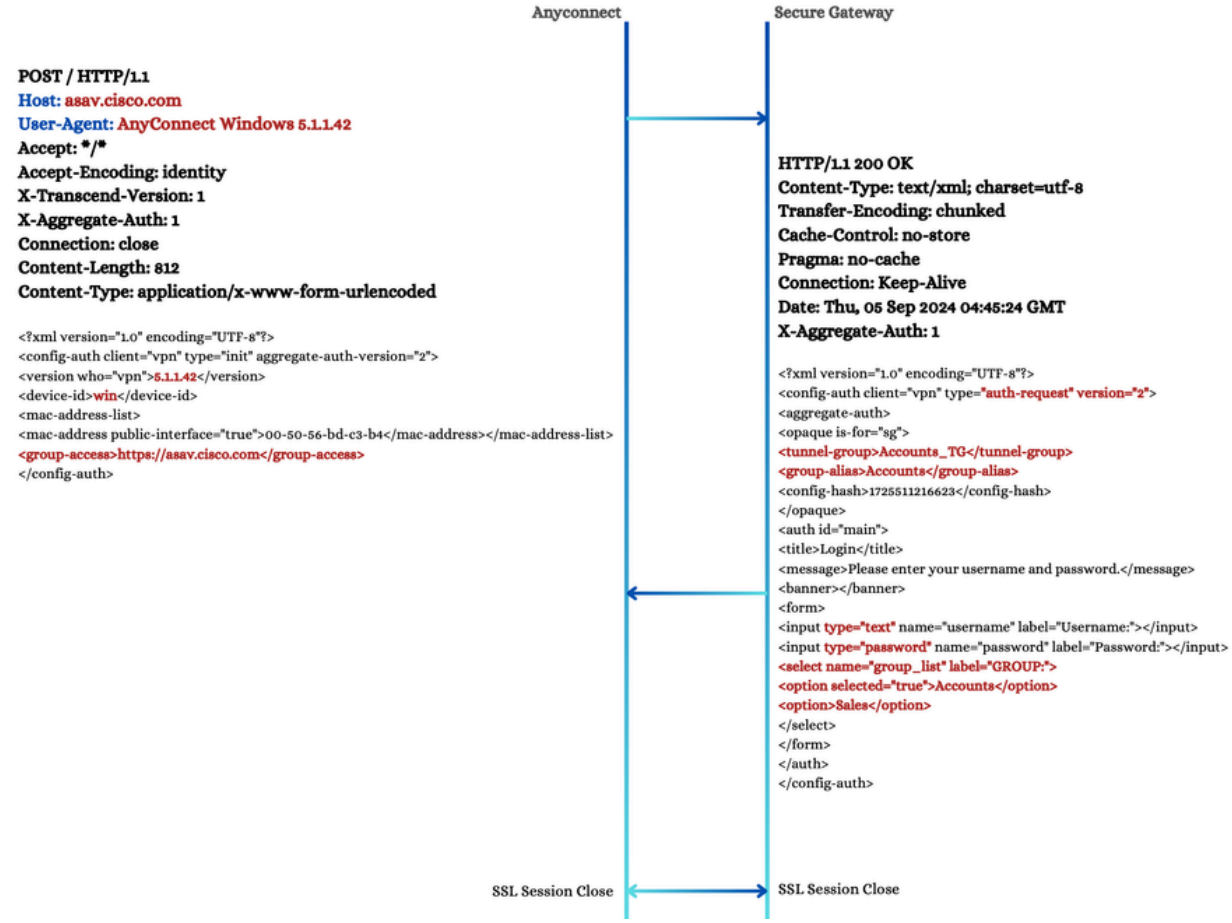
在HTTP响应中，安全网关指示以下内容：

1. 安全网关支持的聚合身份验证版本。

2. 隧道组列表和用户名/密码表单。

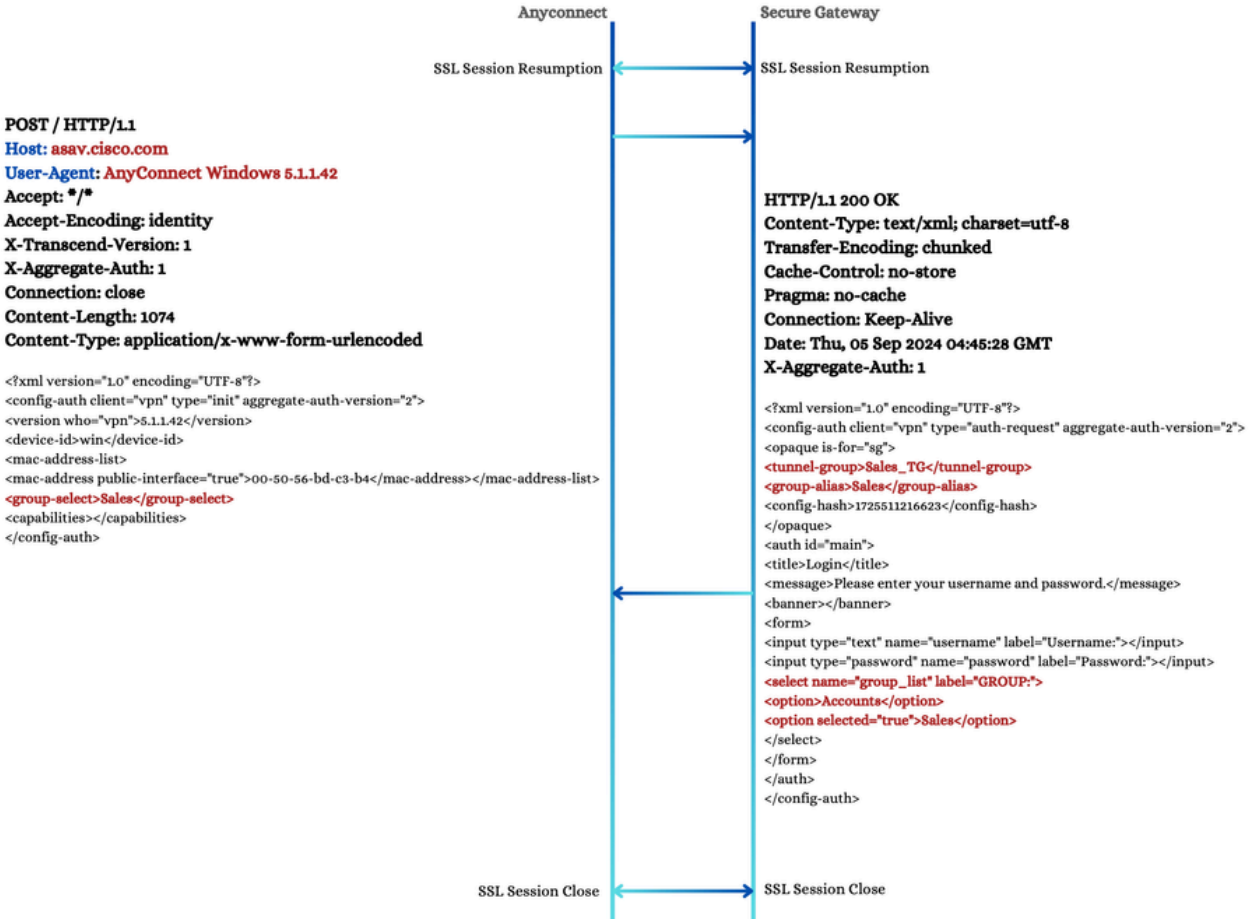


注意：该表单包括一个“select”元素，该元素列出了安全网关上配置的所有连接配置文件的组别名。默认情况下，这些组别名之一会突出显示，并带有selected = "true"布尔属性。tunnel-group和group-alias元素与此选择的连接配置文件相对应。



POST -组选择1

如果用户从此列表中选择其他连接配置文件，将进行另一个POST操作。在这种情况下，客户端会发送一个POST请求，其中更新了“group-select”元素，以反映选定的连接配置文件，如下所示。



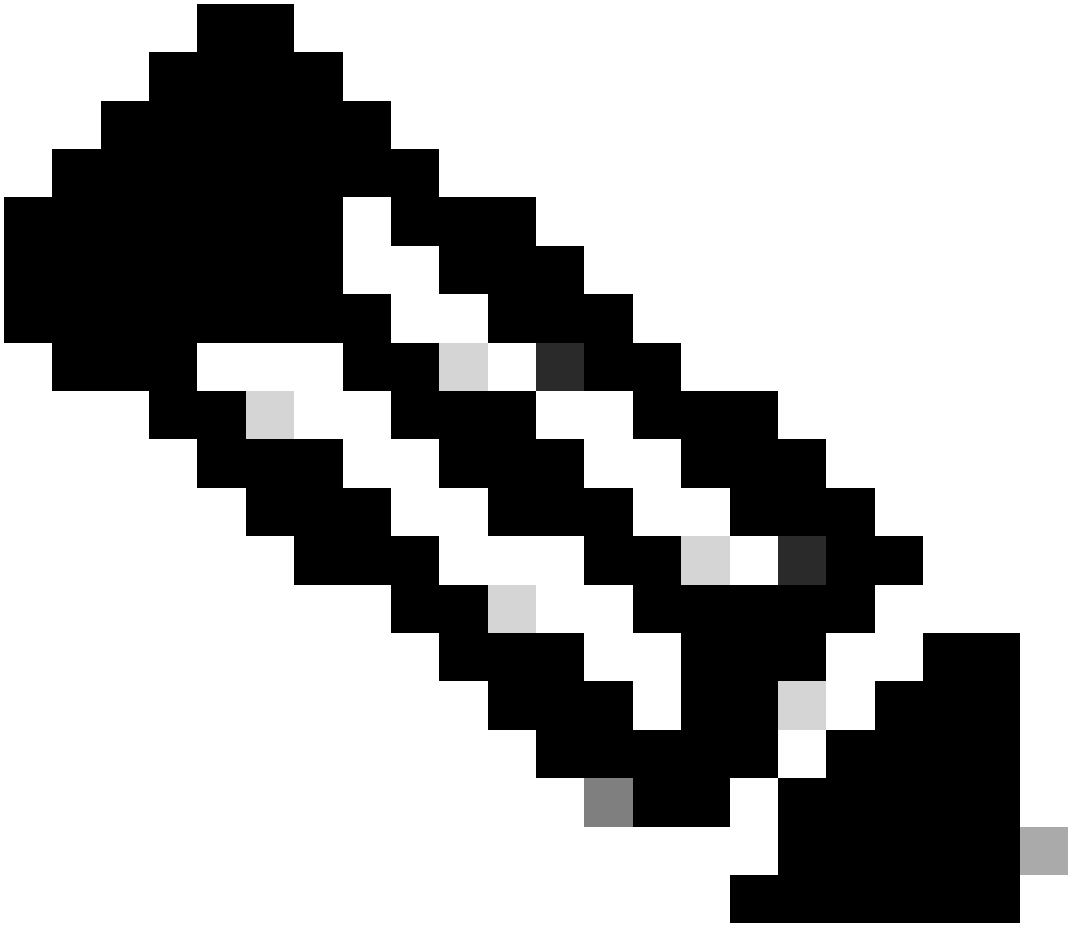
POST -组选择2

3. POST -用户身份验证

在POST组选择之后的此操作中，AnyConnect将以下信息发送到安全网关：

1. Selected Connection Profile Information：这包括隧道组名称和组别名（如早期操作中的安全网关所示）。

2. 用户名和口令：用户的身份验证凭证。



注意：由于此流特定于AAA身份验证，因此它可能与其他身份验证方法不同。

为响应POST操作，安全网关会发送一个包含以下信息的XML文件：

1. 会话ID：这与SSL会话ID不同。

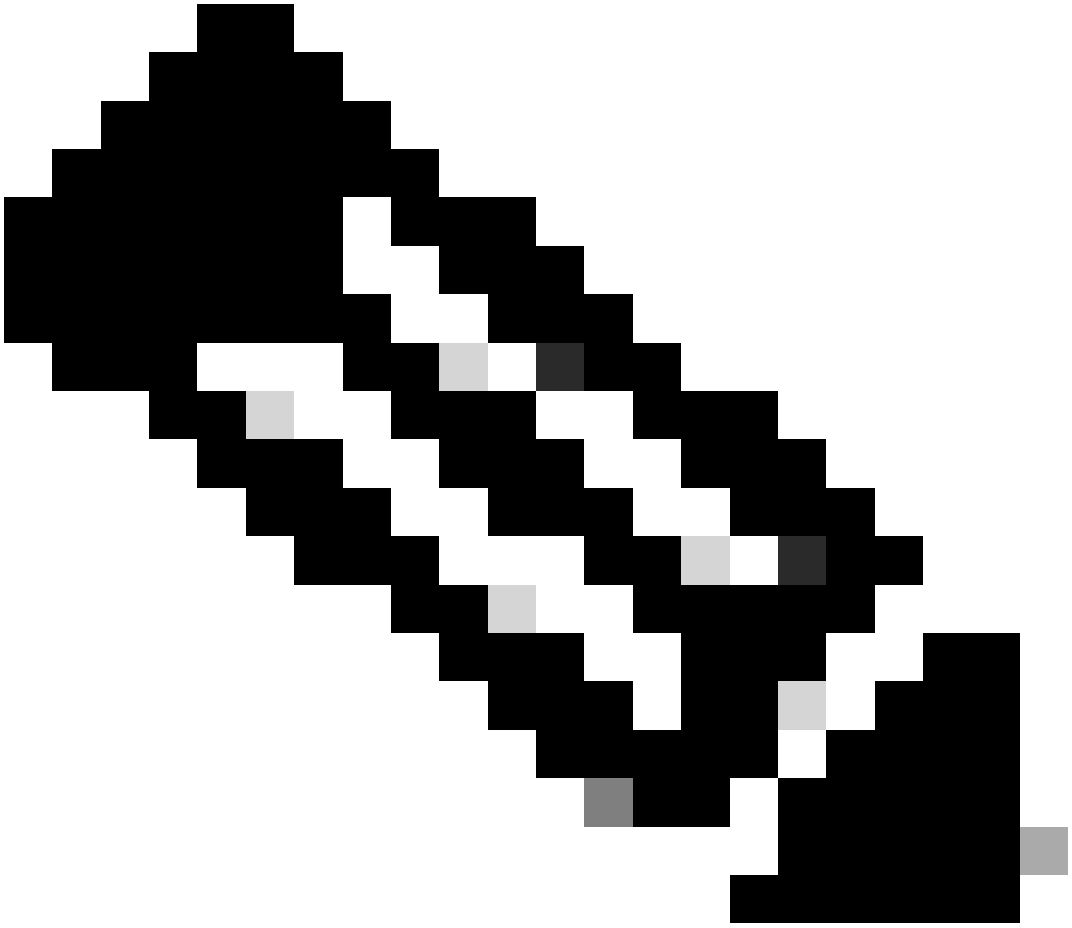
2. 会话令牌：客户端稍后会将此令牌用作WebVPN Cookie。

3. 身份验证状态：由auth元素表示，id = '成功'。

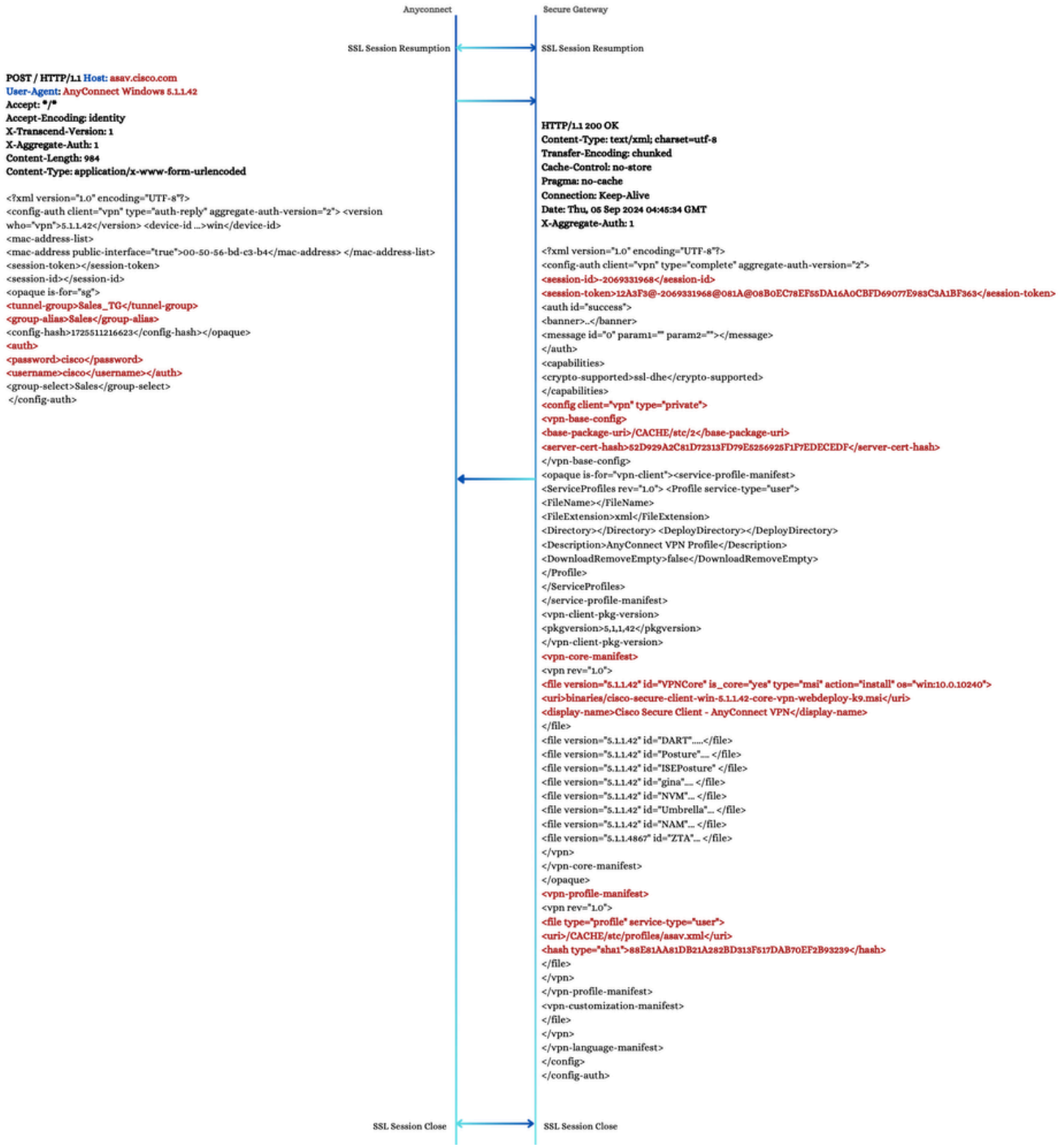
4. Server Certificate Hash：此哈希缓存在preferences.xml文件中。

5. vpn-core-manifest元素：此元素指示AnyConnect核心软件包的路径和版本，以及其他组件（如DART、安全评估、ISE安全评估等）。VPN下载程序将在下一节中使用它。

6. vpn-profile-manifest元素：此元素指示配置文件的路径（配置文件的名称）和SHA-1哈希。



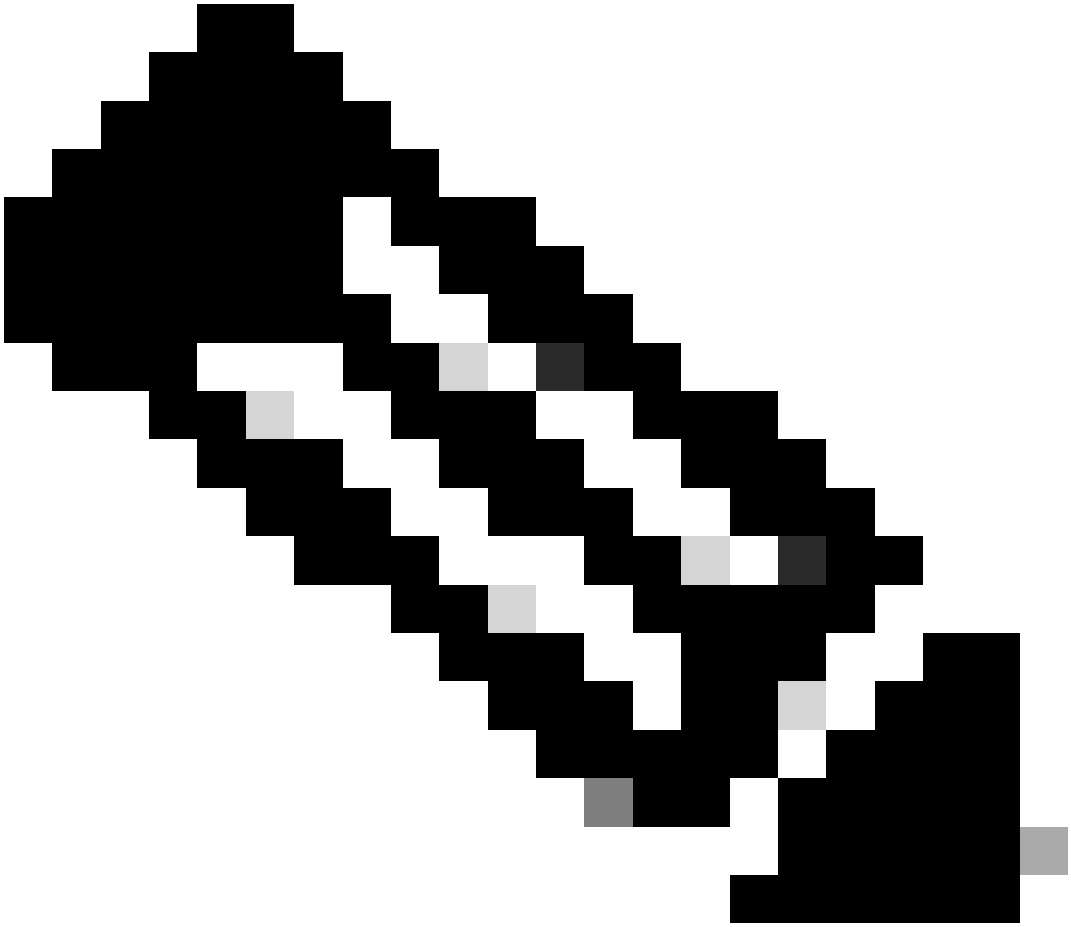
注意：如果客户端没有配置文件，下一部分中的VPN下载程序会下载配置文件。如果客户端已具有配置文件，则比较客户端配置文件的SHA-1散列与服务器的散列。如果不匹配，VPN下载程序会使用安全网关上的配置文件覆盖客户端配置文件。这确保在身份验证后对客户端实施安全网关上的配置文件。



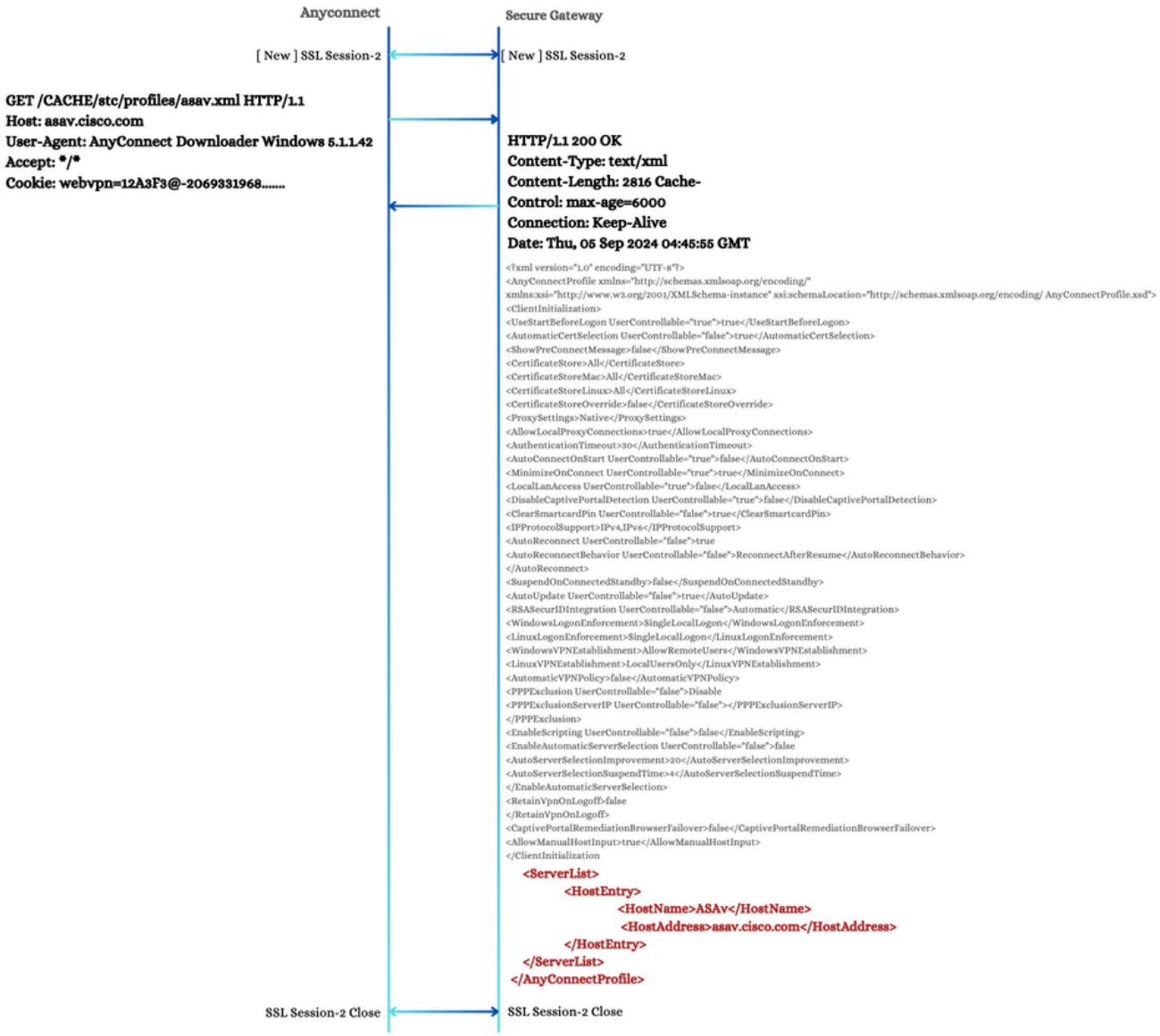
POST -用户身份验证

4. AnyConnect下载程序

AnyConnect下载程序始终会启动新的SSL会话，因此，如果安全网关的证书不受信任，用户可能会遇到第二次证书警告。在此阶段，它会针对每个需要下载的项目执行单独的GET操作。



注意：如果客户端配置文件上传到安全网关中，则必须下载；否则，整个连接尝试会终止。

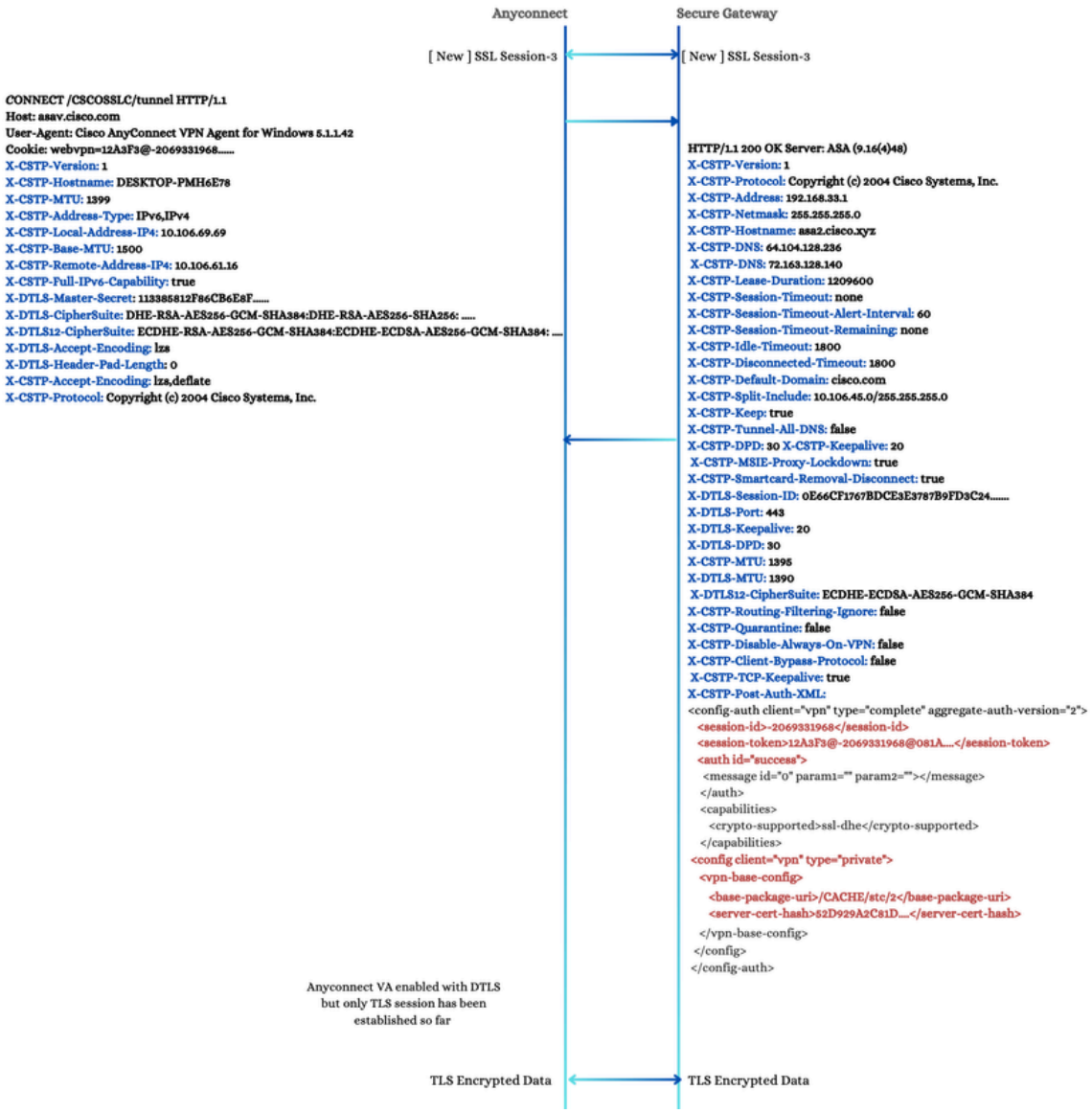


VPN下载程序

5. CSTP连接

AnyConnect执行CONNECT操作，作为建立安全通道的最后一步。在CONNECT操作期间，AnyConnect客户端发送安全网关的各种X-CSTP和X-DTLS属性以进行处理。安全网关使用客户端应用于当前连接尝试的其他X-CSTP和X-DTLS属性进行响应。此交换包括X-CSTP-Post-Auth-XML，随附一个XML文件，该文件大致类似于POST -用户身份验证步骤中的文件。

收到成功响应后，AnyConnect启动TLS数据信道。同时，激活AnyConnect虚拟适配器接口，其MTU值等于X-DTLS-MTU（假设后续DTLS握手成功）。



CSTP连接

6. DTLS握手

DTLS握手过程按照此处所述进行。由于在CONNECT事件期间客户端和服务器之间交换的属性，此设置相对较快。

客户端

X-DTLS-Master-Secret：DTLS主密钥由客户端生成并与服务器共享。此密钥对于建立安全DTLS会话至关重要。

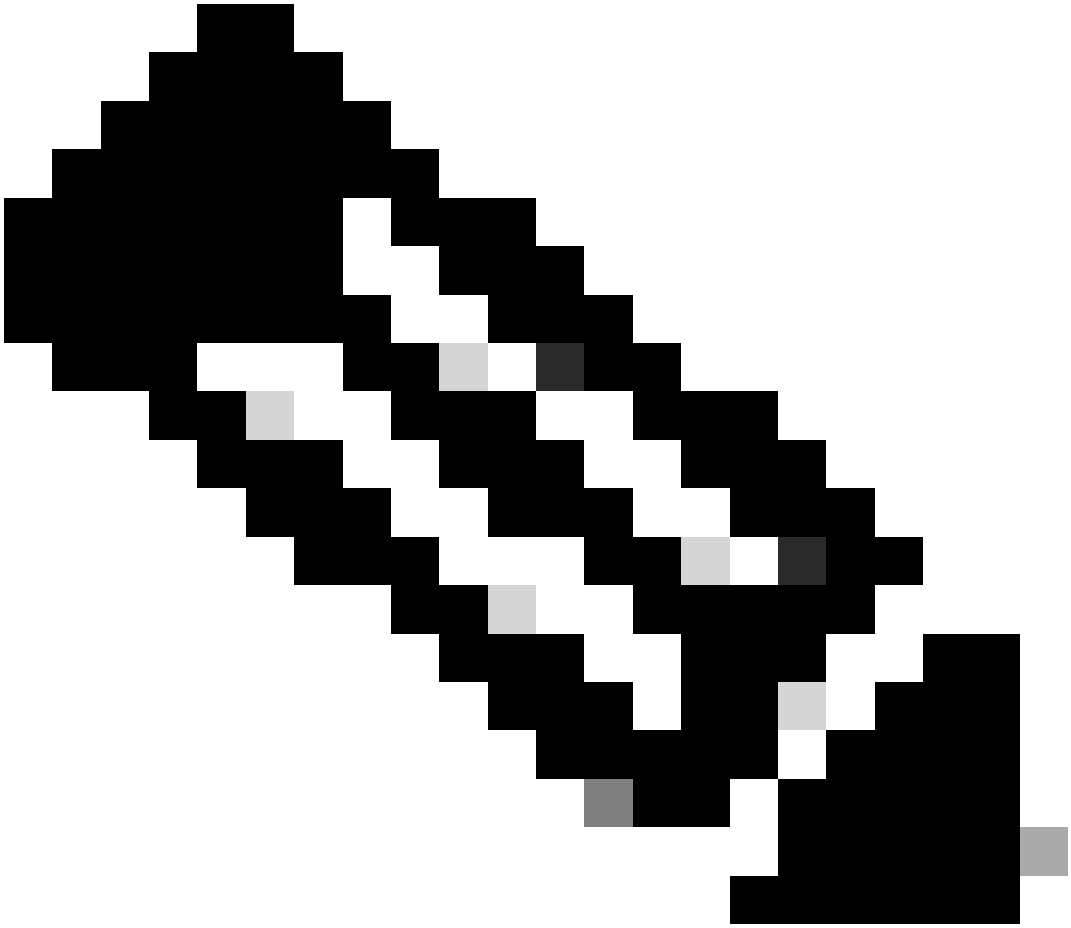
X-DTLS-CipherSuite：客户端支持的DTLS密码套件列表，指示客户端的加密功能。

服务器

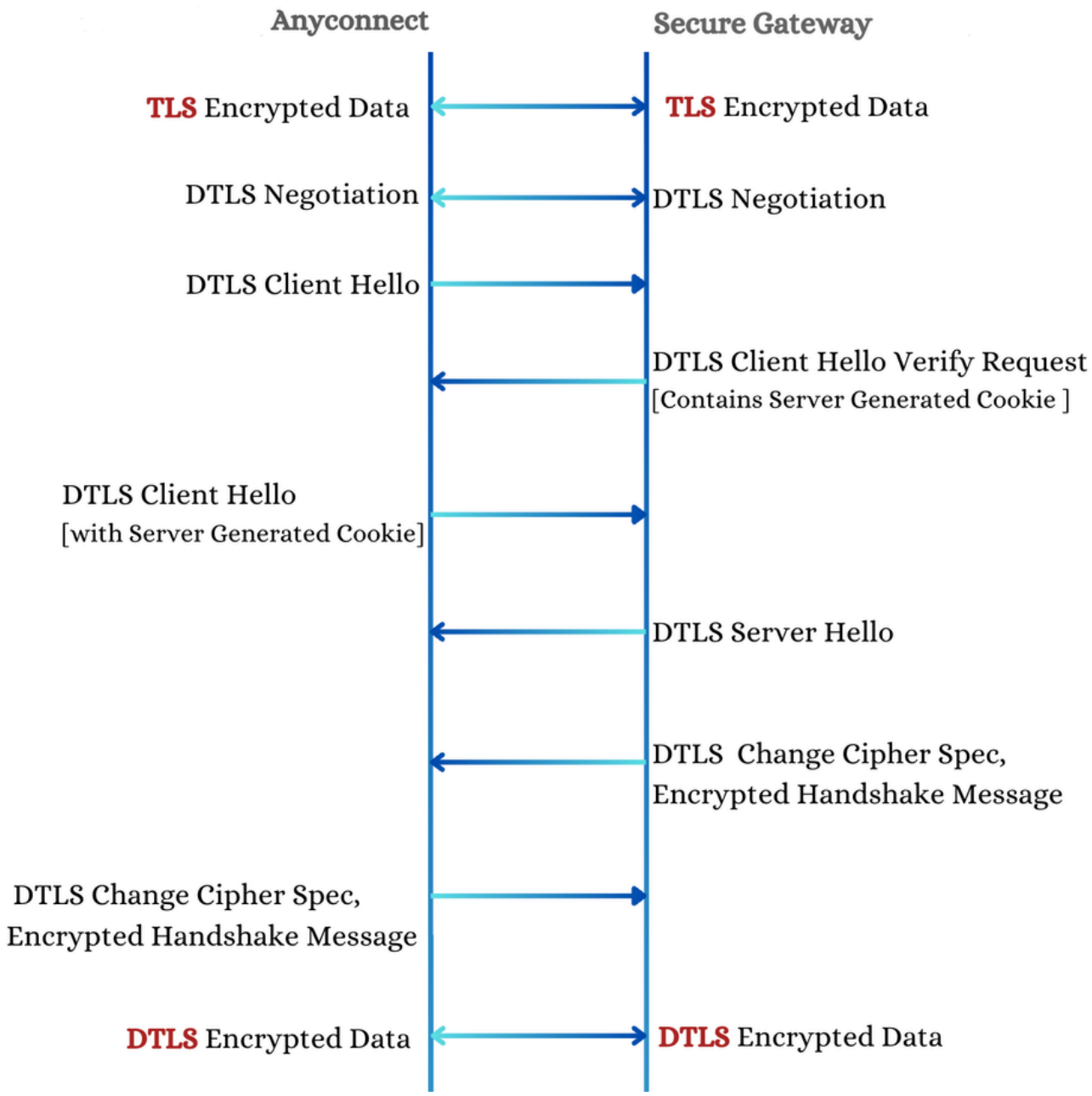
X-DTLS-Session-ID：由服务器分配给客户端使用的DTLS会话ID，确保会话连续性。

X-DTLS-CipherSuite：服务器从客户端提供的列表中选择的密码套件，确保双方使用兼容的加密方

法。



注意：当DTLS握手正在进行时，TLS数据通道将继续运行。这样可以确保在握手过程中数据传输保持一致和安全。只有在DTLS握手完成之后，才会无缝过渡到DTLS数据加密通道。

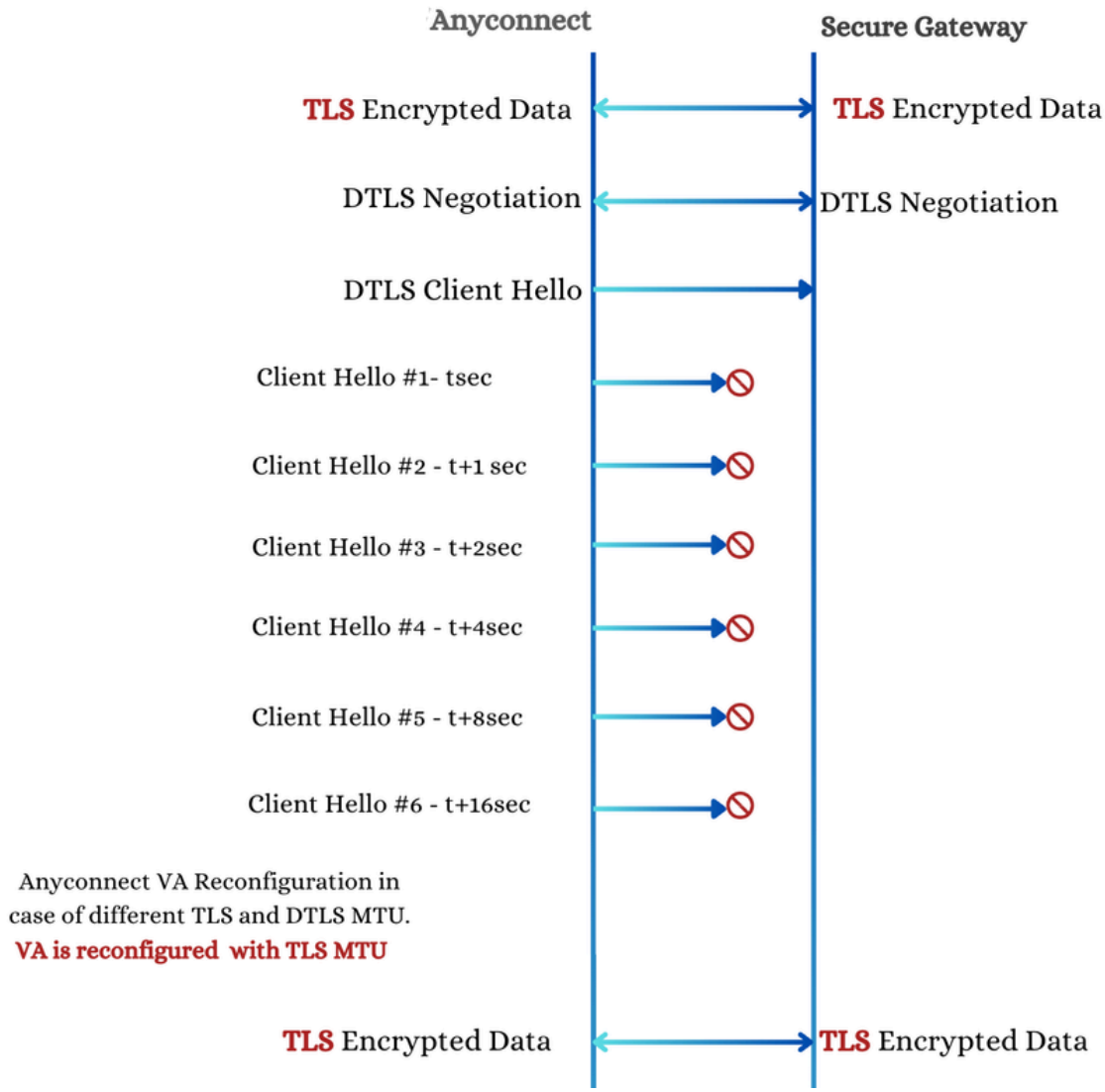


DTLS握手

6.1.已阻止DTLS端口

如果DTLS端口被阻止或安全网关无法响应DTLS客户端Hello数据包，则AnyConnect执行一次指数型回退，最多重试五次，从1秒延迟开始，增加最多16秒。

如果这些尝试不成功，则AnyConnect会将安全网关在第5阶段返回的X-CSTP-MTU值所指定的实际TLS MTU应用到AnyConnect虚拟适配器。由于此MTU与之前应用的MTU (X-DTLS-MTU)不同，因此必须重新配置虚拟适配器。此重新配置对最终用户显示为重新连接尝试，但在此过程中不会发生新的协商。虚拟适配器重新配置后，TLS数据通道将继续运行。



DTLS端口块(DTLS Port Block)

相关信息

- [Cisco VPN技术文档参考]
- [思科技术支持和下载]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。