瞭解AnyConnect SSL VPN連線流

目錄

簡介

本文檔重點介紹SSLVPN連線期間AnyConnect和安全網關之間發生的事件流。

背景資訊

AnyConnect

AnyConnect是為SSL和IKEv2協定設計的Cisco VPN客戶端。它適用於大多數案頭和移動平台。AnyConnect主要透過Firepower威脅防禦(FTD)、自適應安全裝置(ASA)或稱為安全網關的Cisco IOS®/Cisco IOS® XE路由器建立安全連線。

安全閘道

在思科術語中，SSL VPN伺服器稱為安全網關，而IPSec (IKEv2)伺服器稱為遠端訪問VPN網關。思科在以下平台上支援SSL VPN隧道終端：

- 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連線流

本文檔將SSL VPN連線建立期間AnyConnect和安全網關之間發生的事件分為六個階段：

1. SSL握手

2. POST -組選擇

3. POST -使用使用者名稱/口令的使用者驗證（可選）

4. VPN下載程式（可選）

5. CSTP連線

6. DTLS連線（可選）

1. SSL握手

SSL握手由AnyConnect客戶端在透過「Client Hello」消息完成TCP三次握手之後發起。事件流程和關鍵要點如前所述。

客戶端Hello

SSL會話從客戶端傳送「Client Hello」消息開始。在此訊息中：

a) SSL會話ID設定為0，表示啟動新會話。

b)負載包括客戶端支援的密碼套件和客戶端生成的隨機隨機數。

伺服器Hello

伺服器以「Server Hello」消息作出響應，其中包括：

a)從客戶端提供的清單中選擇的密碼套件。

b)伺服器生成了SSL會話ID，伺服器隨機生成了一個隨機事件。

伺服器憑證

在「Server Hello」之後，伺服器傳輸其SSL證書，該證書用作其身份。需要注意的要點包括：

a)如果此證書未通過嚴格驗證檢查，預設情況下AnyConnect會阻止伺服器。

b)使用者可以選擇停用此區塊，但後續連線會顯示警告，直到報告的錯誤解決為止。

使用者端憑證要求

伺服器還可以請求客戶端證書，從而傳送安全網關上載入的所有CA證書的使用者名稱DN清單。此請求有兩個用途：

a)如果有多個ID證書可用，它將幫助客戶端（使用者）選擇正確的身份證書。

b) 確保返回證書受安全網關信任，儘管仍必須進行進一步的證書驗證。

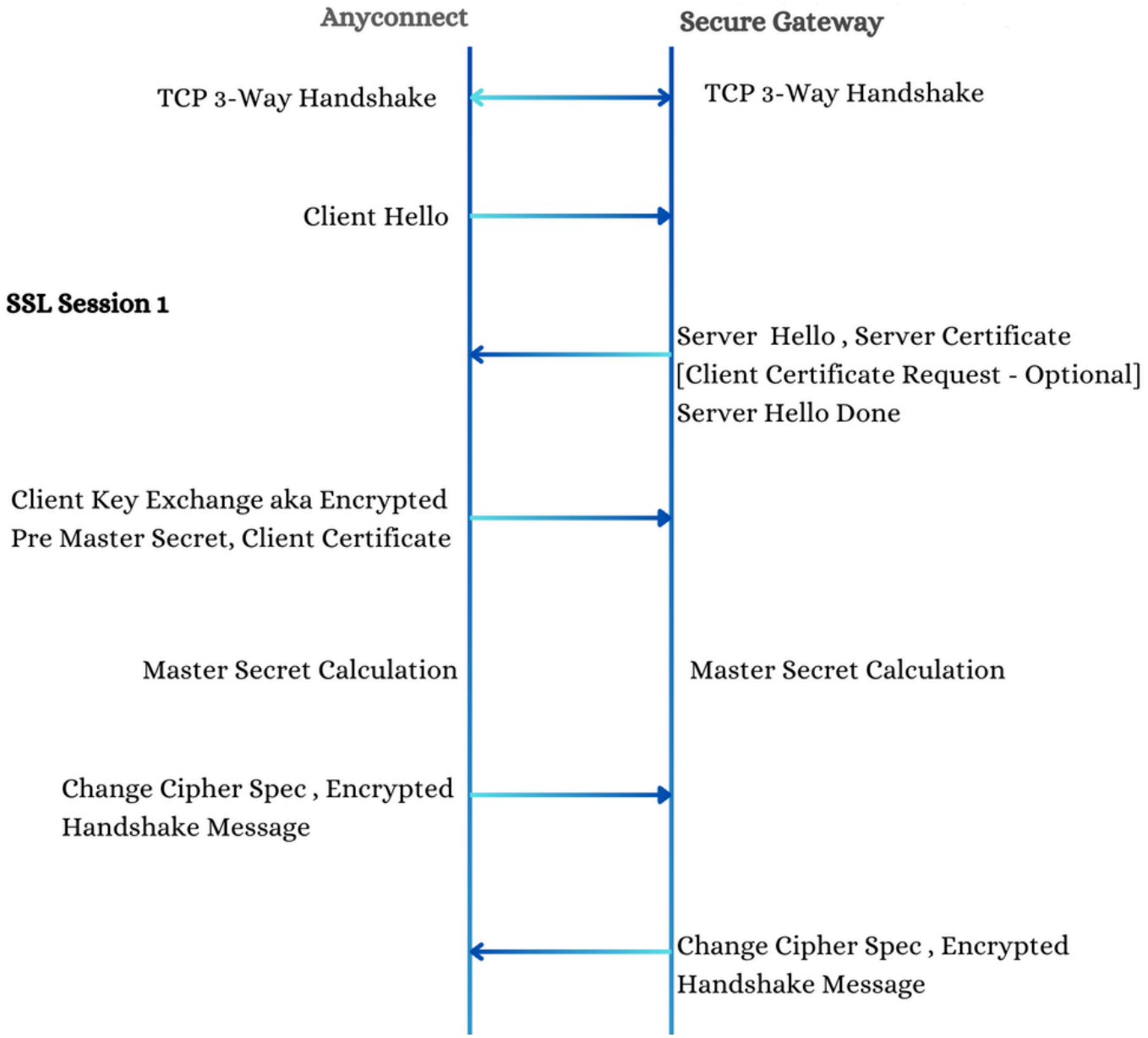
使用者端金鑰交換

然後使用者端傳送「使用者端金鑰交換」訊息，其中包括預先主控的金鑰。此金鑰使用以下內容加密：

a)伺服器憑證的伺服器公開金鑰，如果選擇的密碼套件是基於RSA的（例如，TLS_RSA_WITH_AES_128_CBC_SHA）。

b)如果選擇的密碼套件基於DHE（例如，TLS_DHE_DSS_WITH_AES_256_CBC_SHA），則為伺服器Hello消息中提供的伺服器DH公鑰。

根據預主金鑰、客戶端生成的隨機隨機金鑰和伺服器生成的隨機金鑰，客戶端和安全網關都會獨立生成主金鑰。然後，該主金鑰用於導出會話金鑰，確保客戶端和伺服器之間的安全通訊。



SSL會話1

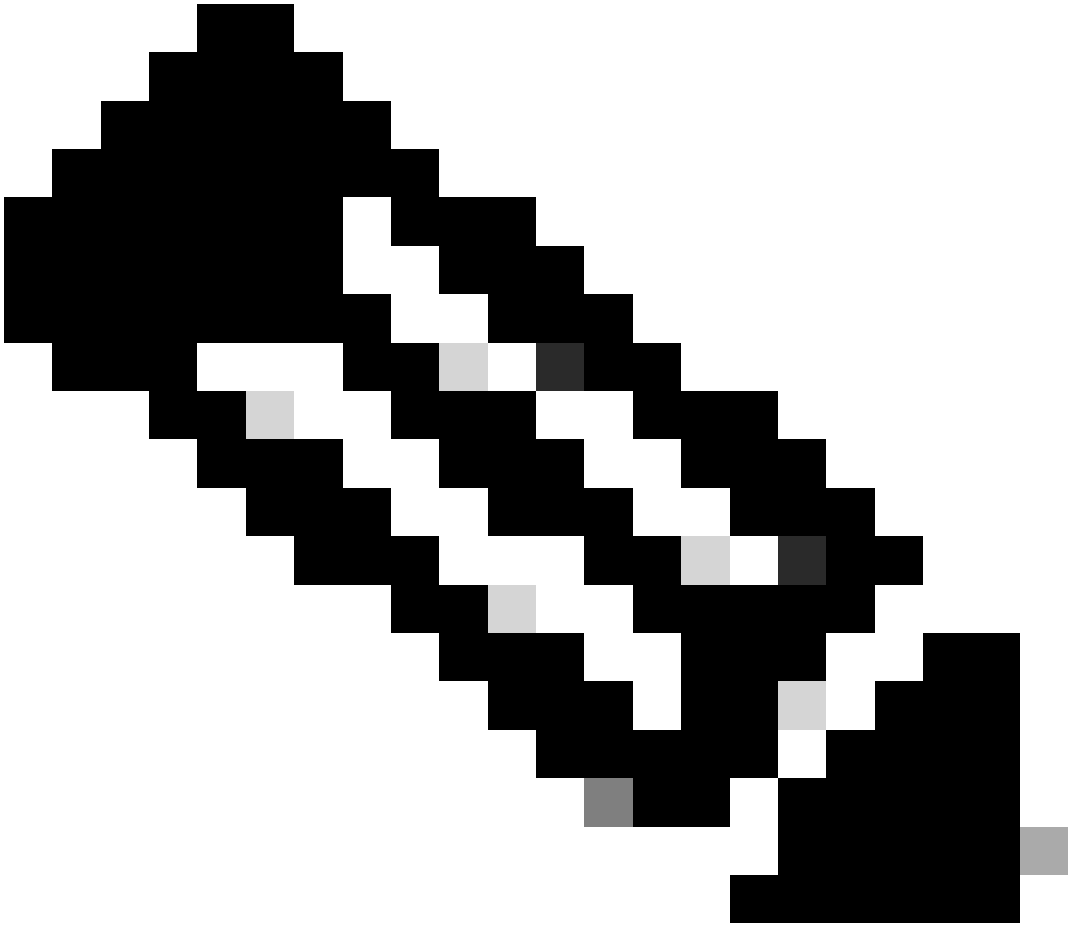
2. POST -組選擇

在此操作期間，除非使用者明確指定，否則客戶端不擁有關於連線配置檔案的資訊。連線嘗試定向到安全網關URL (asav.cisco.com)，如請求中的「group-access」元素所示。客戶端指示其支援「aggregate-authentication」版本2。此版本代表較舊版本有重大改進，特別是在高效的XML交易方面。安全網關和客戶端必須同意要使用的版本。在安全網關不支援版本2的情況下，會觸發另一個POST操作，導致客戶端回退到版本。

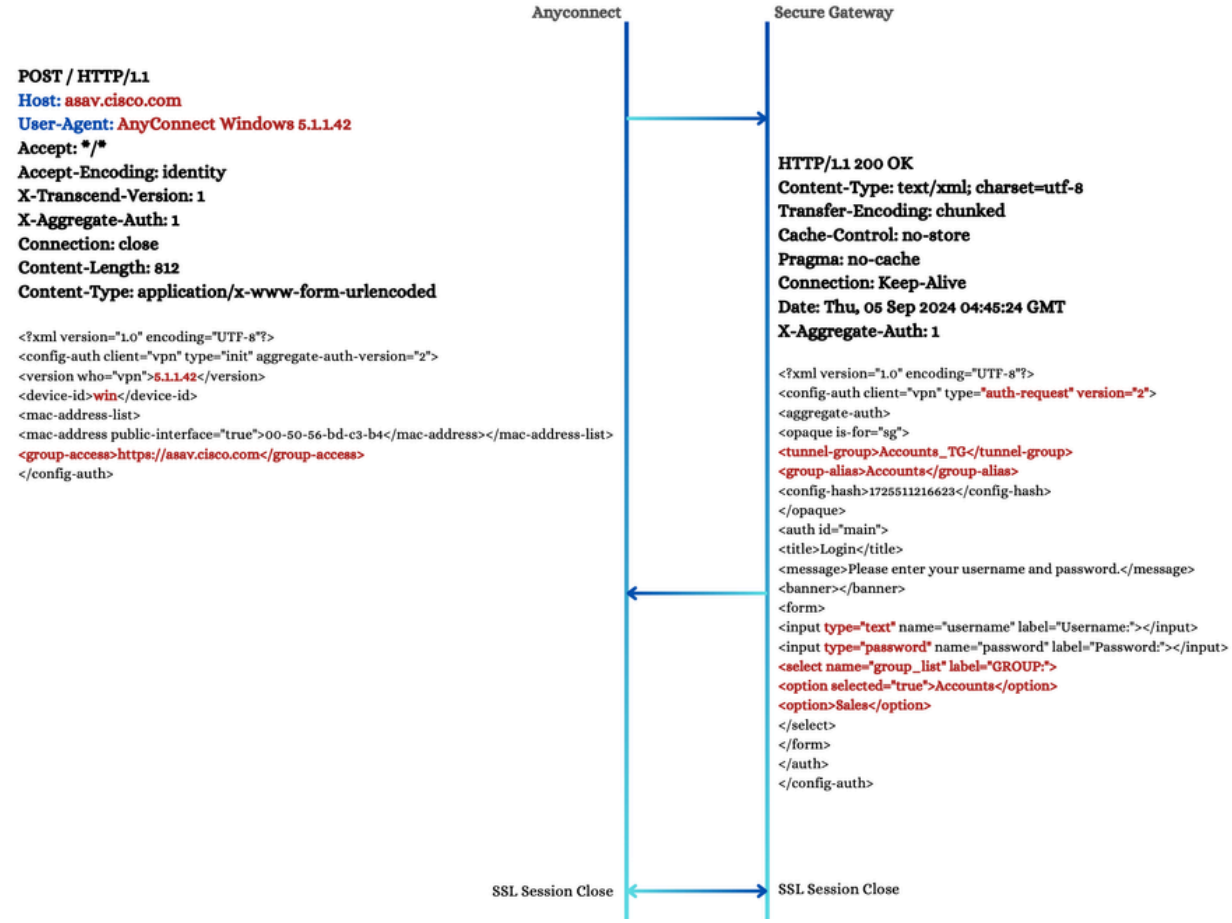
在HTTP回應中，安全閘道會指出以下專案：

1. 安全網關支援的聚合身份驗證版本。

2. 隧道組清單和使用者名稱/密碼表單。

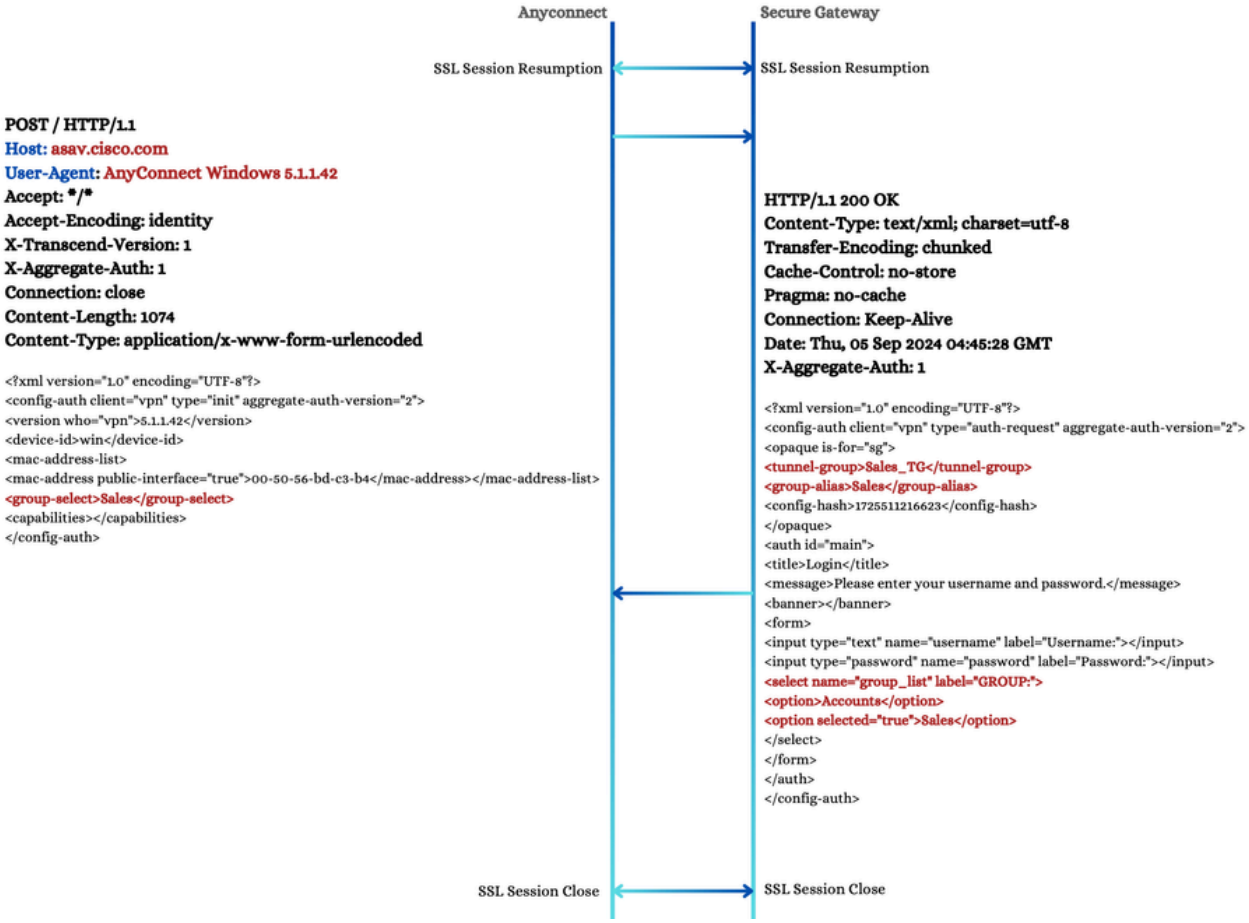


注意：此表單包括「select」元素，該元素列出了安全網關上配置的所有連線配置檔案的組別名。依預設，這些群組別名之一會以selected =「true」布林屬性反白顯示。tunnel-group和group-alias元素與此選擇的連線配置檔案相對應。



POST -組選擇1

如果使用者從此清單中選擇不同的連線設定檔，則會進行另一個POST作業。在這種情況下，客戶端會傳送一個POST請求，其中「group-select」元素已更新，以反映所選的連線配置檔案，如下所示。



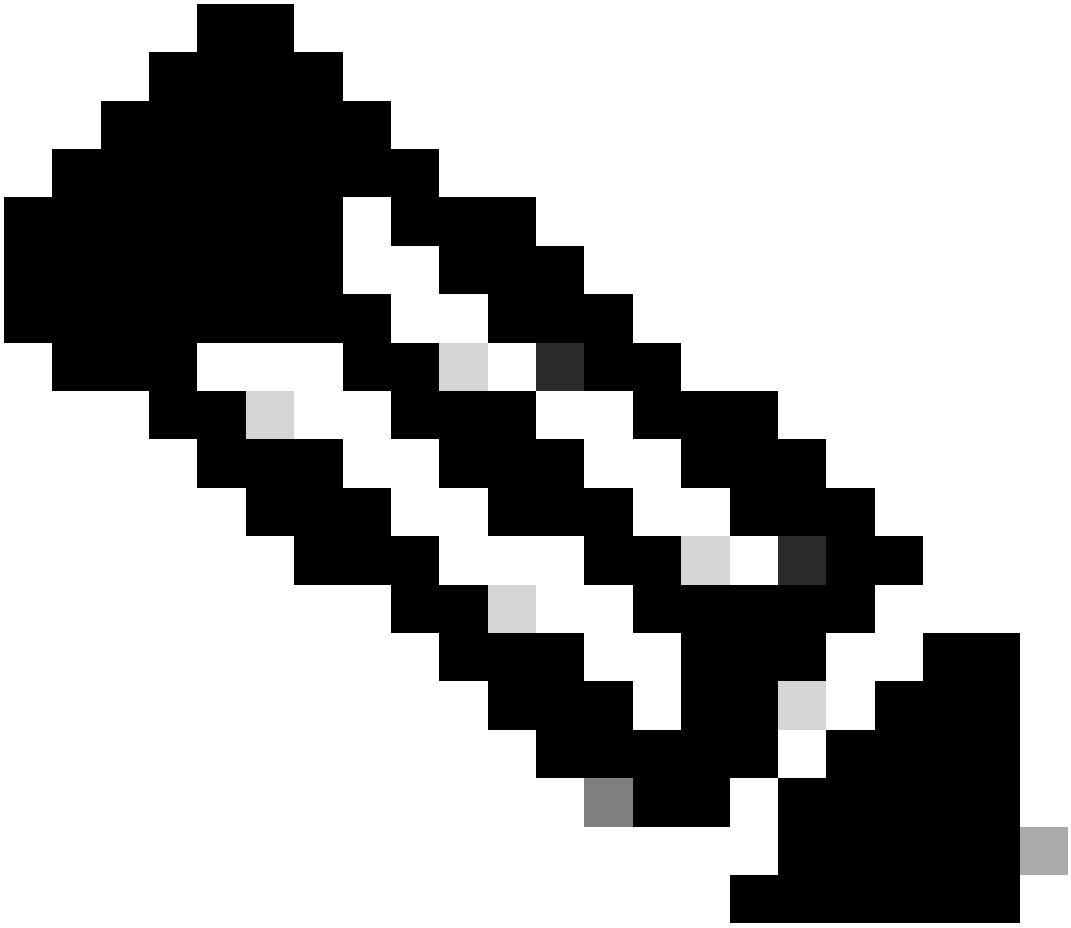
POST -組選擇2

3. POST -使用者身份驗證

在此操作中（在POST-Group選擇之後），AnyConnect將以下資訊傳送到安全網關：

1. 選擇的連線配置檔案資訊：其中包括隧道組名稱和組別名（如前面操作中的「安全網關」所示）。

2.使用者名稱和密碼：使用者的認證證明資料。



注意：由於此流特定於AAA身份驗證，因此它與其他身份驗證方法可能不同。

為響應POST操作，安全網關傳送一個包含此資訊的XML檔案：

1.階段作業ID：與SSL階段作業ID不同。

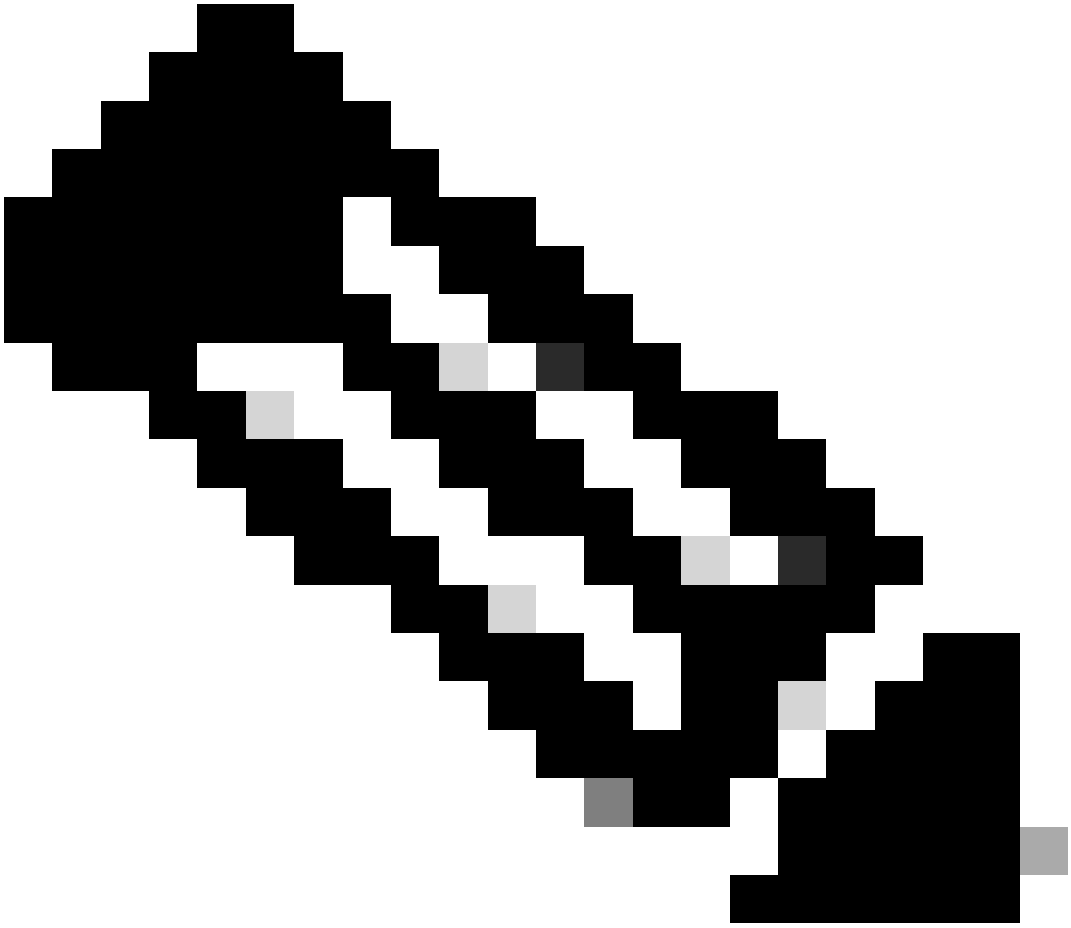
2. 會話令牌：客戶端稍後會將此令牌用作WebVPN Cookie。

3. Authentication Status：由auth元素表示，id = 'success'。

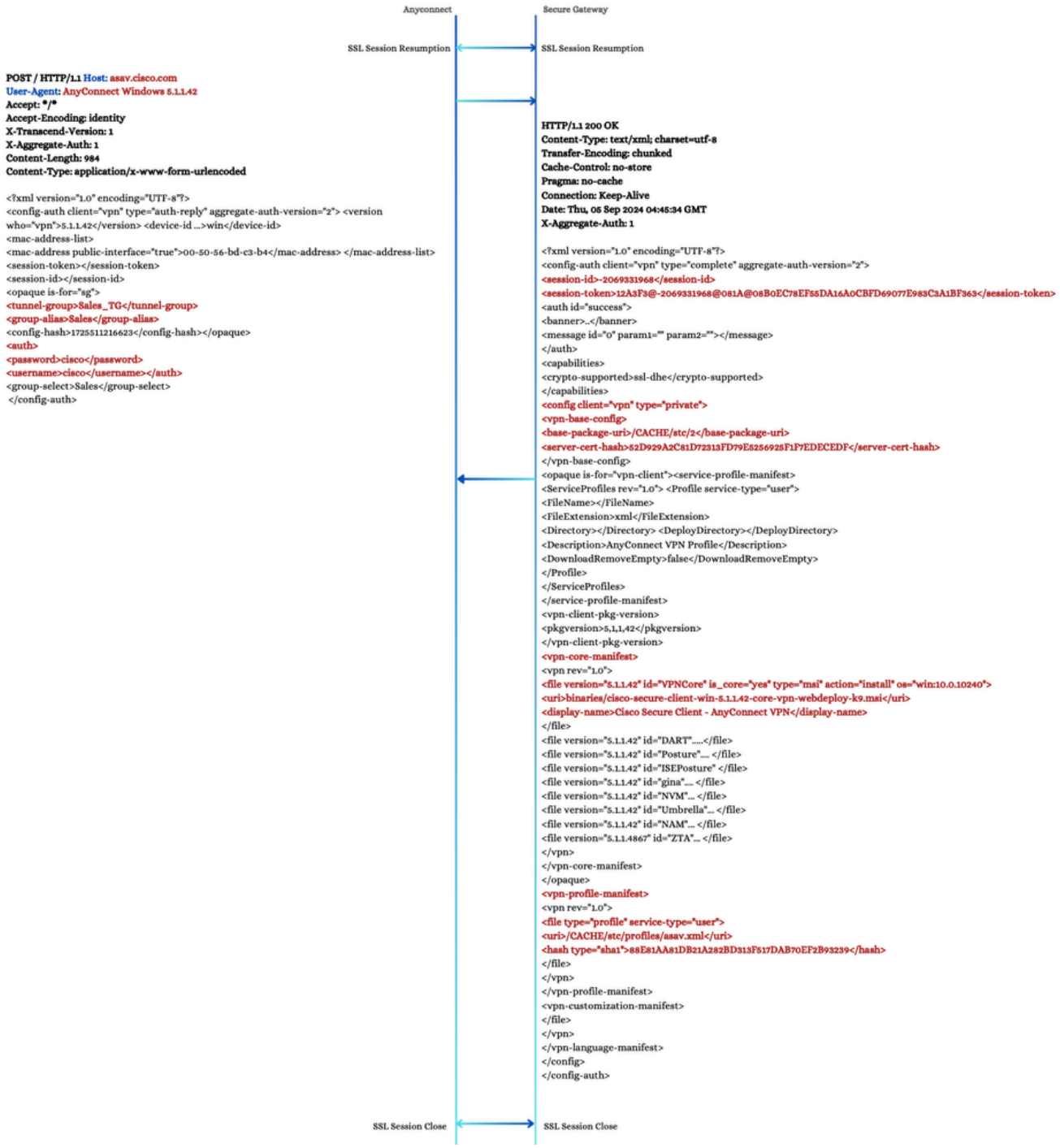
4.伺服器憑證雜湊：此雜湊會快取至preferences.xml檔案。

5. vpn-core-manifest元素：此元素指示AnyConnect核心軟體套件的路徑和版本，以及其他元件（如Dart、終端安全評估、ISE終端安全評估等）。VPN下載程式將在下一節中使用它。

6. vpn-profile-manifest元素：此元素指示配置檔案的路徑（配置檔案的名稱）和SHA-1雜湊。



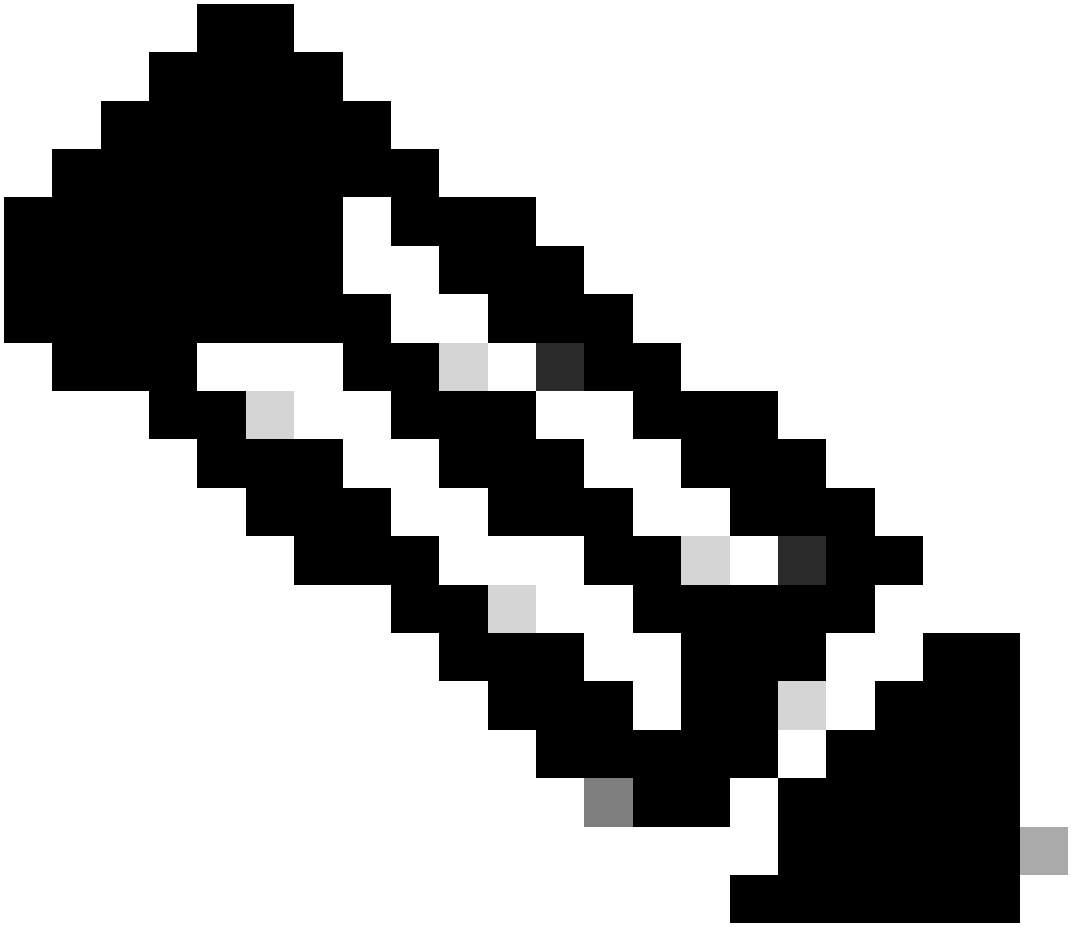
注意：如果客戶端沒有配置檔案，下一部分中的VPN下載程式會下載該檔案。如果使用者端已有設定檔，則會比較使用者端設定檔與伺服器的SHA-1雜湊。如果不匹配，VPN下載程式會使用安全網關上的客戶端配置檔案覆蓋客戶端配置檔案。這可確保安全網關上的配置檔案在客戶端身份驗證後執行。



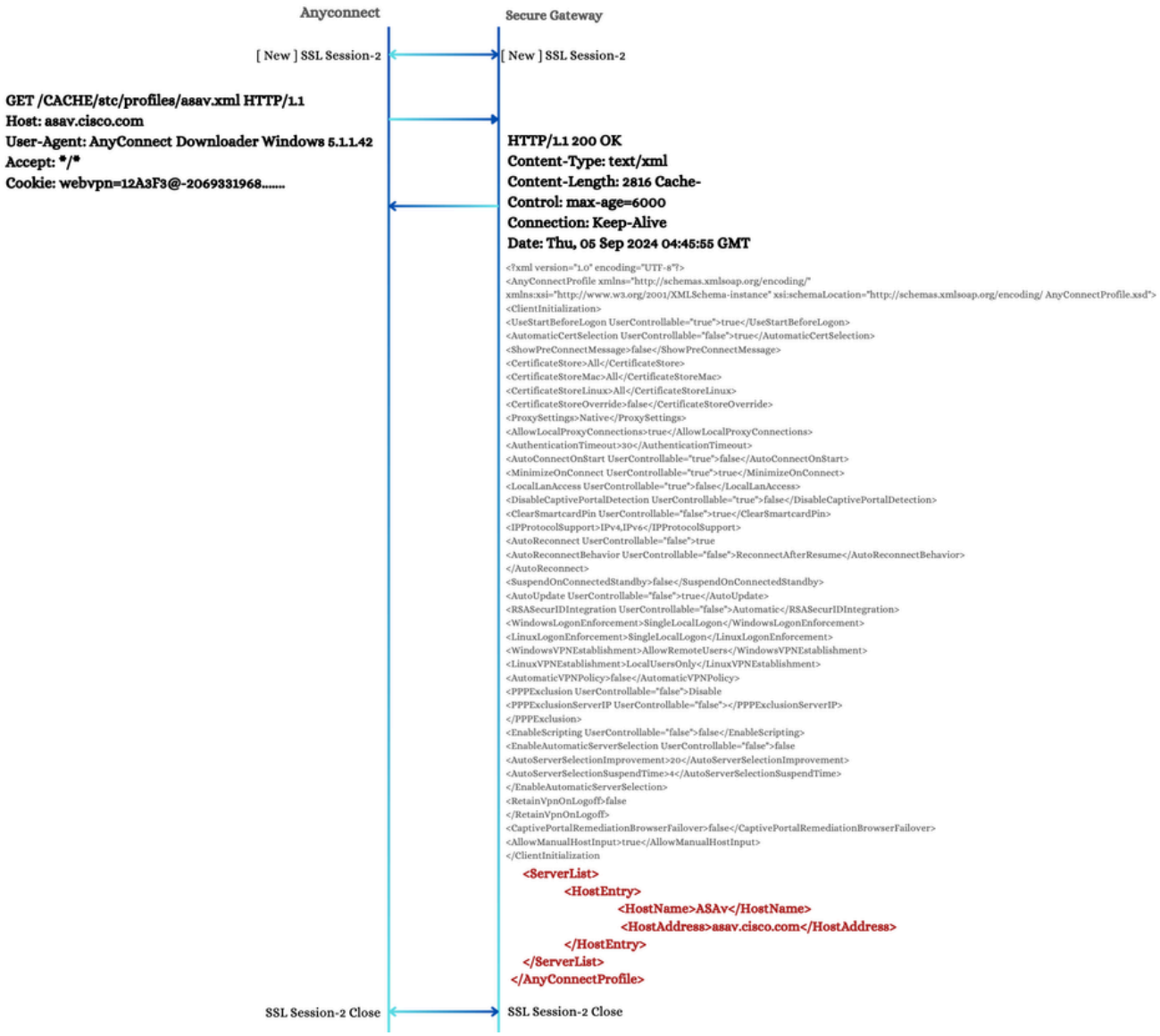
POST -使用者驗證

4. AnyConnect下載程式

AnyConnect下載程式始終會啟動新的SSL會話，因此，如果安全網關的證書不受信任，使用者可能會遇到第二次證書警告。在此階段，它會針對需要下載的每個專案執行單獨的GET操作。



注意：如果客戶端配置檔案上傳到安全網關中，則必須下載；否則，將終止整個連線嘗試。

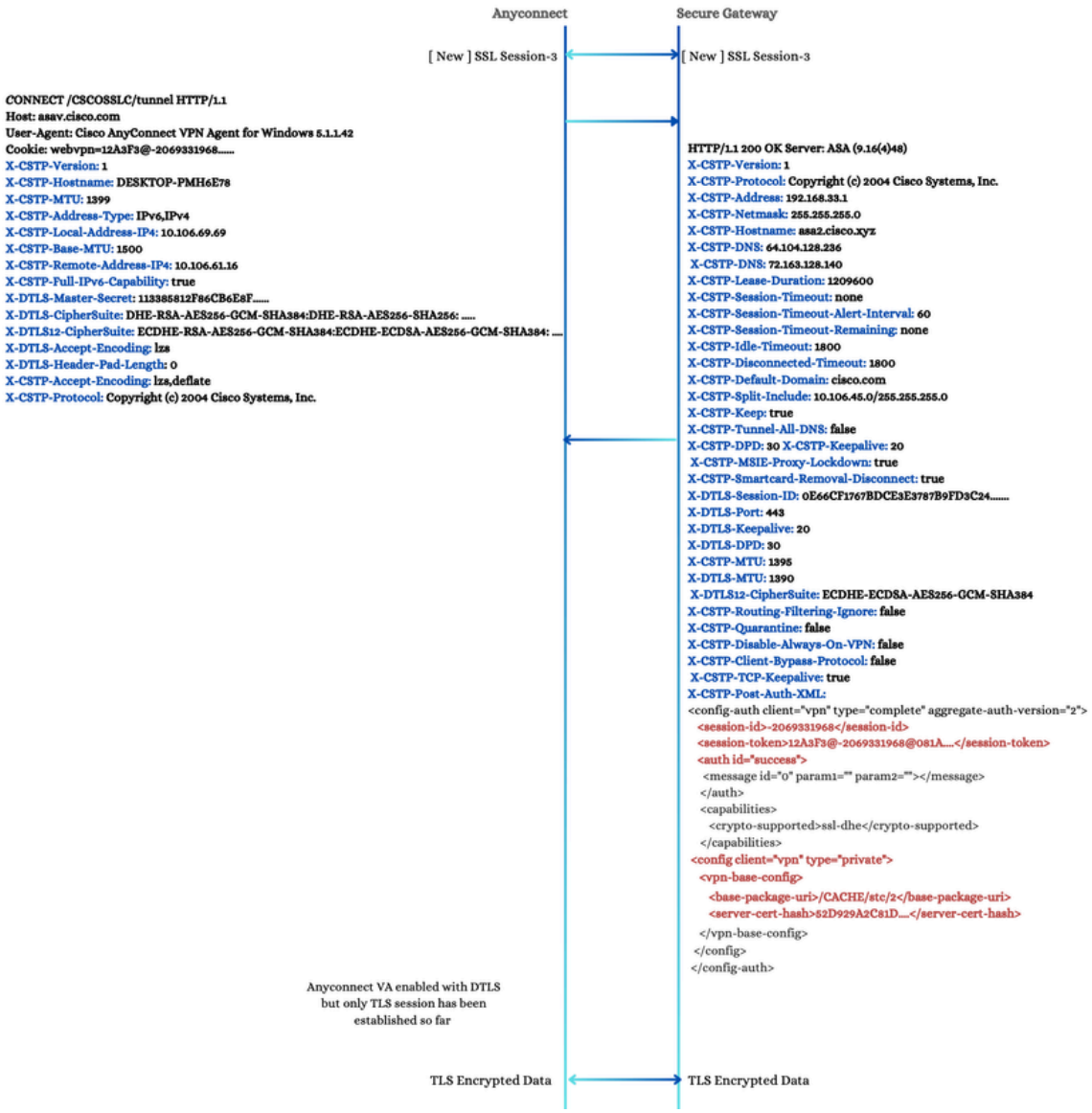


VPN下載器

5. CSTP連線

AnyConnect執行CONNECT操作是建立安全通道的最後步驟。在CONNECT操作期間，AnyConnect客戶端會傳送安全網關的各種X-CSTP和X-DTLS屬性以進行處理。安全網關以客戶端應用於當前連線嘗試的其他X-CSTP和X-DTLS屬性做出響應。此交換包括X-CSTP-Post-Auth-XML，隨附一個XML檔案，該檔案與「POST -使用者身份驗證」步驟中的檔案大體相似。

在收到成功的響應後，AnyConnect將啟動TLS資料通道。同時，AnyConnect虛擬介面卡介面的MTU值等於X-DTLS-MTU（假設後續DTLS握手成功）。



CSTP連線

6. DTLS握手

DTLS握手將依照此處所述進行。由於在CONNECT事件期間客戶端和伺服器之間交換的屬性，此設定相對較快。

使用者端

X-DTLS-Master-Secret：DTLS主金鑰由客戶端生成並與伺服器共用。此金鑰對於建立安全DTLS會話至關重要。

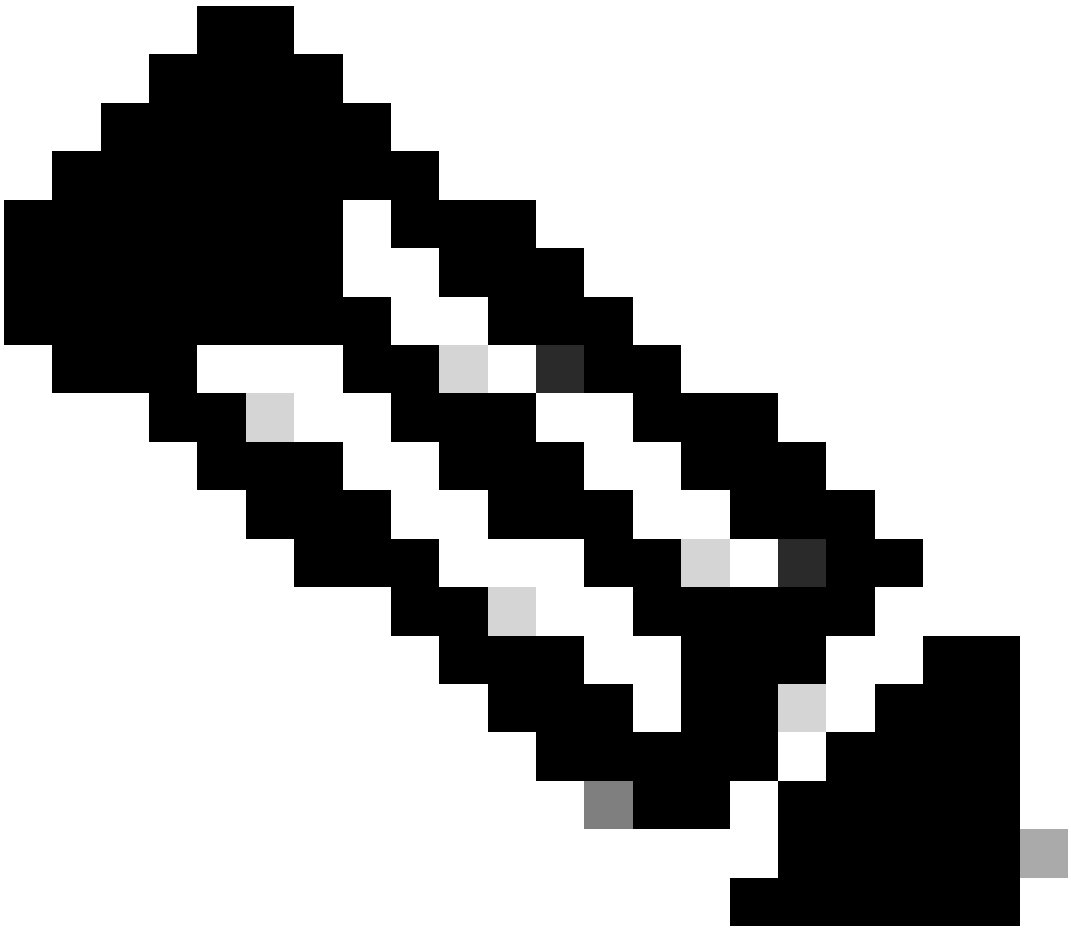
X-DTLS-CipherSuite：客戶端支援的DTLS密碼套件清單，指示客戶端的加密功能。

伺服器

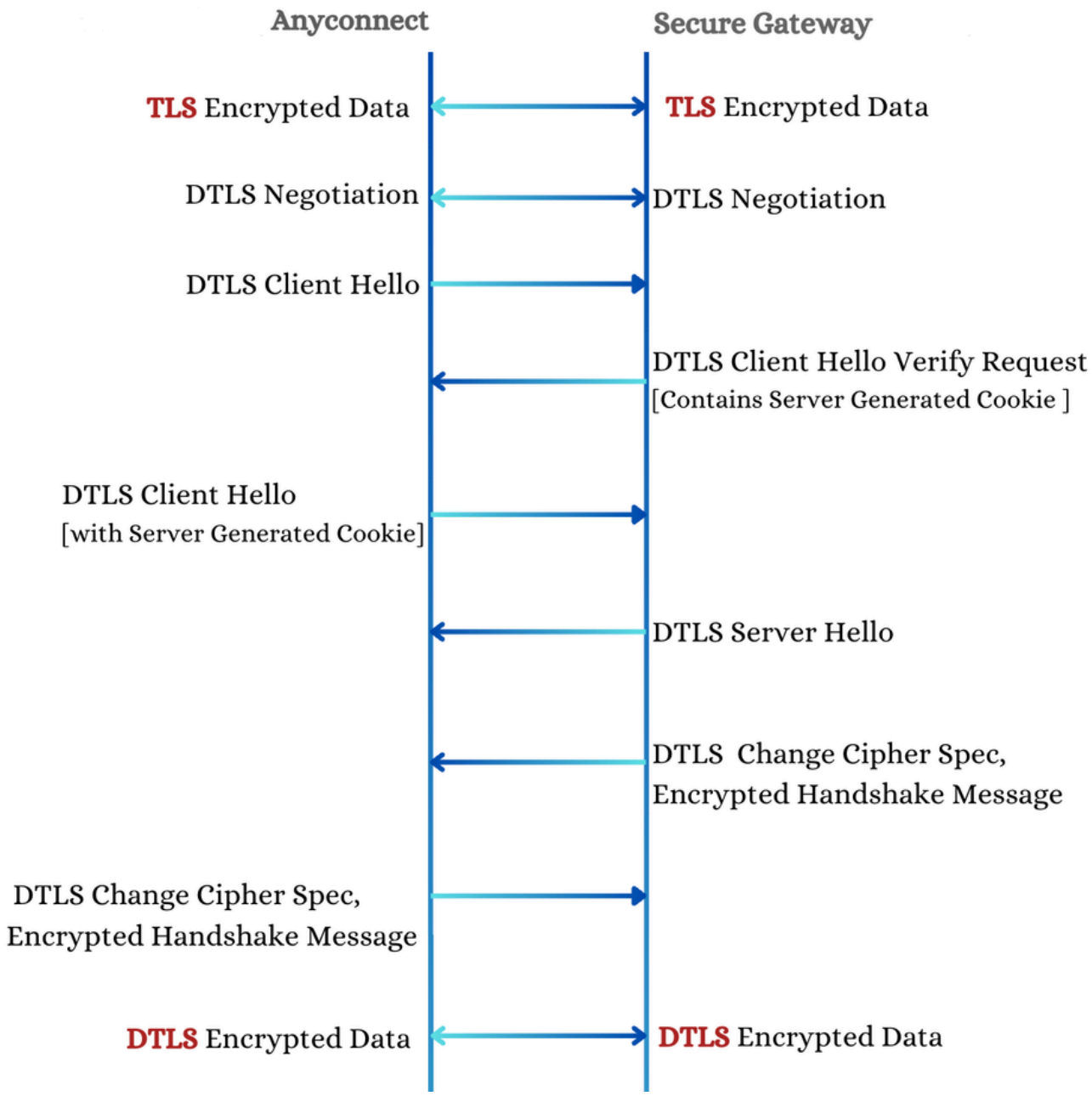
X-DTLS-Session-ID：伺服器分配給客戶端使用的DTLS會話ID，用於確保會話的連續性。

X-DTLS-CipherSuite：伺服器從客戶端提供的清單中選擇的密碼套件，用於確保雙方使用相容的加

密方法。



注意：當DTLS握手正在進行時，TLS資料通道將繼續運行。這可確保在握手過程中資料傳輸保持一致和安全。只有在DTLS握手完成後，才會無縫轉換到DTLS資料加密通道。

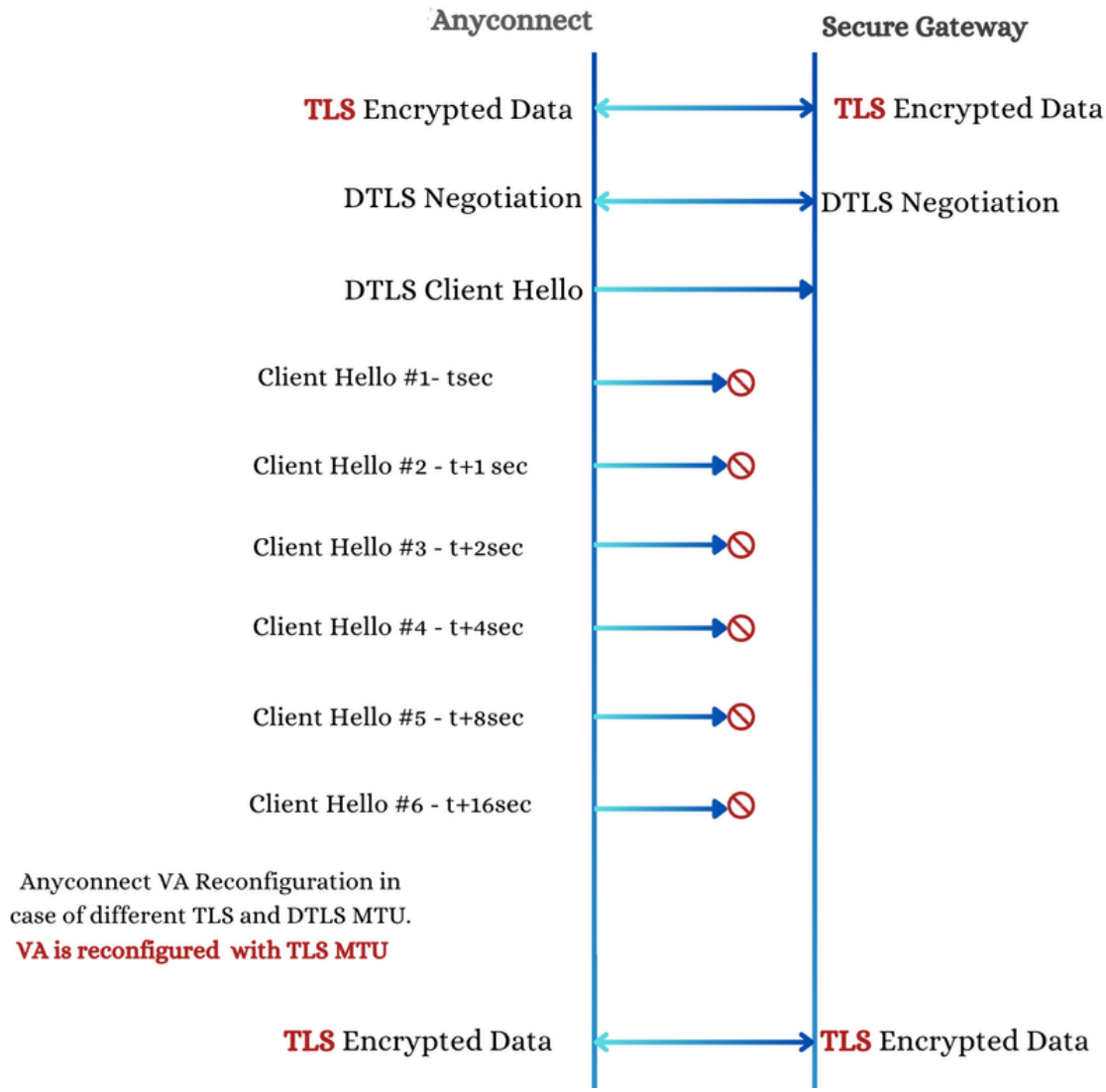


DTLS握手

6.1. DTLS埠被阻塞

如果DTLS埠被阻止或安全網關無法響應DTLS客戶端Hello資料包，則AnyConnect會執行指數型回退，最多重試5次，從1秒延遲開始，最多增加16秒。

如果這些嘗試不成功，AnyConnect會將安全網關在第5階段返回的X-CSTP-MTU值所指定的實際TLS MTU應用於AnyConnect虛擬介面卡。因為此MTU與先前套用的MTU (X-DTLS-MTU)不同，所以必須重新設定虛擬介面卡。此重新配置對終端使用者而言是重新連線嘗試，但在此過程中不會發生新的協商。虛擬介面卡重新設定後，TLS資料通道會繼續運作。



DTLS埠塊

相關資訊

- Cisco VPN技術文檔參考
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。