瞭解AnyConnect SSL VPN連線流

目錄

簡介

背景資訊

- AnyConnect
- 安全閘道

AnyConnect SSL VPN連線流

- SSL握手
  - 客戶端Hello
  - 伺服器Hello
  - 伺服器證書
  - 客戶端證書請求
  - 客戶端金鑰交換
- POST — 組選擇
- POST — 使用者身份驗證
- AnyConnect下載程式
- CSTP連線
- DTLS握手
  - 用戶端
  - 伺服器
- DTLS埠被阻止

相關資訊

簡介

本文檔介紹SSLVPN連線建立期間AnyConnect和安全網關之間的事件流。

背景資訊

AnyConnect

AnyConnect是專為安全套接字層(SSL)和網際網路金鑰交換(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主要通過稱為安全網關的Firepower威脅防禦(FTD)、自適應安全裝置(ASA)或Cisco IOS®和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隧道終止：

- Cisco ASA（ASAv、5500和5500-X系列）

- Cisco FTD(FTDv、1000、2100、3100、4100、4200和9300系列)
- Cisco ISR 4000和ISR G2系列
- Cisco CSR 1000v
- Cisco Catalyst 8000v

AnyConnect SSL VPN連線流

在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/密碼的使用者身份驗證（可選）

4. VPN下載程式（可選）

5. CSTP CONNECT

6. DTLS連線（可選）

SSL握手

完成與客戶端Hello消息的傳輸控制協定(TCP)三次握手後，AnyConnect客戶端會啟動SSL握手。活動流程和關鍵要點如下所述：

客戶端Hello

SSL會話開始於客戶端傳送客戶端Hello消息。在以下訊息中：

- SSL會話ID設定為0，表示啟動新會話。
- 該負載包括客戶端支援的密碼套件和客戶端生成的隨機金鑰。

伺服器Hello

伺服器以伺服器Hello消息進行響應，該消息包括：

- 從客戶端提供的清單中選定的密碼套件。
- 伺服器生成了SSL會話ID和隨機事件。

伺服器證書

在伺服器Hello後，伺服器傳輸其SSL證書，該證書用作其身份。要點包括：

- 如果此證書未通過嚴格驗證檢查，則預設情況下AnyConnect會阻止伺服器。
- 使用者可以選擇禁用此塊，但後續連線將顯示警告，直到報告的錯誤得到解決。

客戶端證書請求

伺服器還可以請求客戶端證書，傳送在安全網關上載入的所有證書頒發機構(CA)證書的使用者名稱清單。此請求有兩個用途：

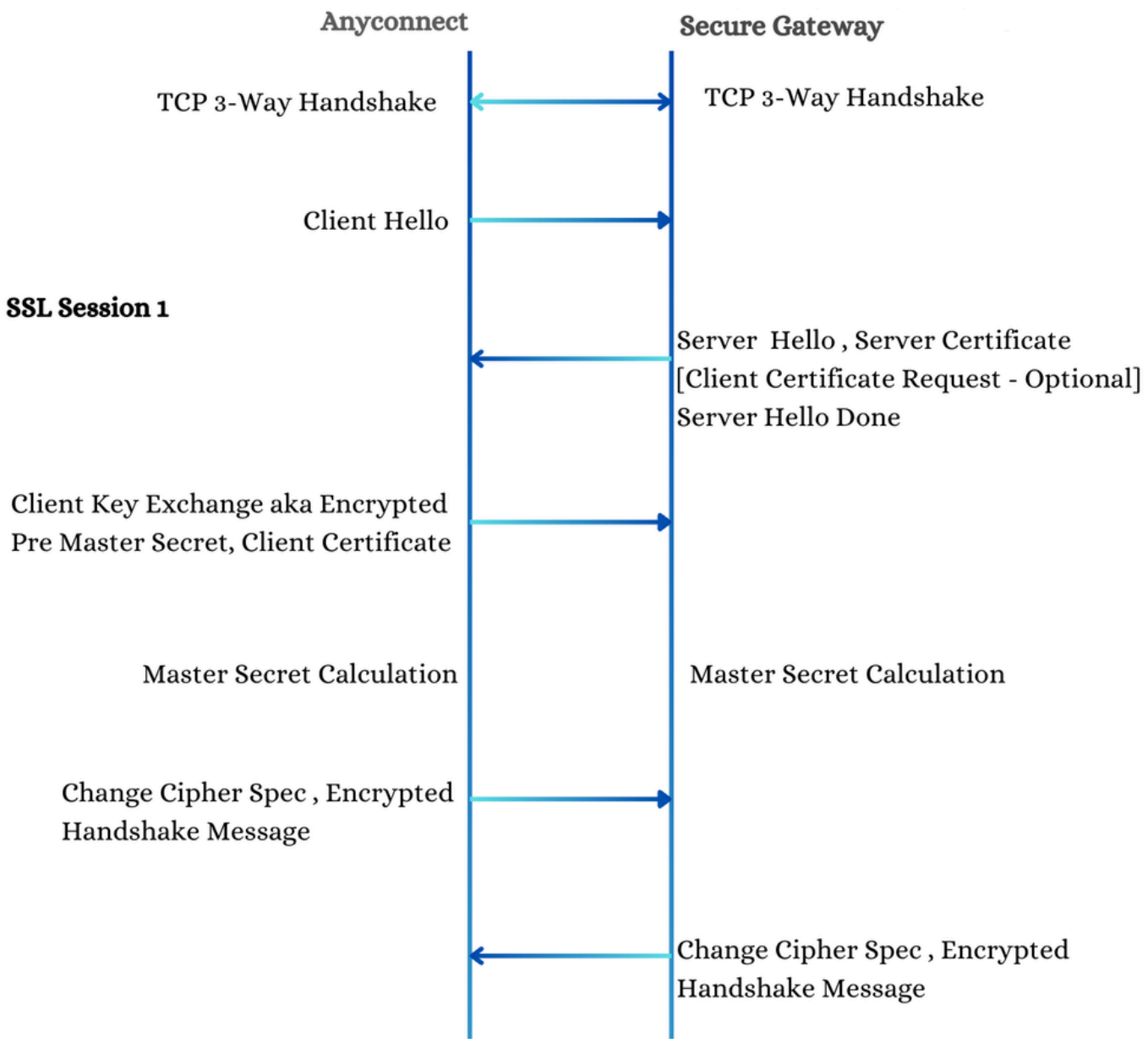
- 如果有多個ID證書可用，它將幫助客戶端（使用者）選擇正確的身份證書。
- 確保返回的證書受安全網關信任，儘管還必須進行進一步的證書驗證。

客戶端金鑰交換

然後，客戶端傳送客戶端金鑰交換消息，該消息包括預先主控金鑰。此金鑰已加密，使用：

- 來自伺服器證書的伺服器的公鑰（如果所選的密碼套件基於RSA）（例如，TLS_RSA_WITH_AES_128_CBC_SHA）
- 如果所選密碼套件基於DHE（例如，TLS_DHE_DSS_WITH_AES_256_CBC_SHA），則在「伺服器問候」消息中提供的伺服器的DH公鑰。

基於預主金鑰、客戶端生成的隨機nonce和伺服器生成的隨機nonce，客戶端和安全網關均獨立生成主金鑰。然後，該主金鑰用於派生會話金鑰，以確保客戶端與伺服器之間的安全通訊。



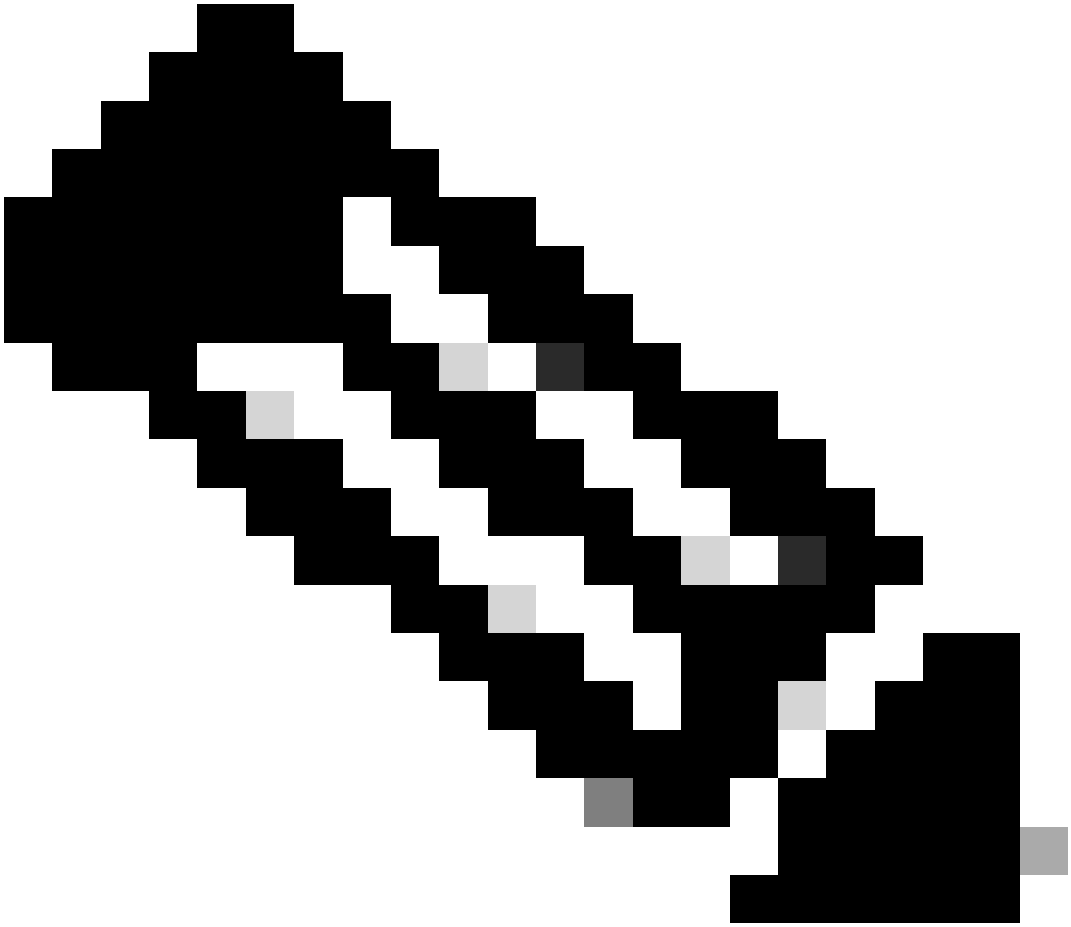
SSL作業階段1

POST — 組選擇

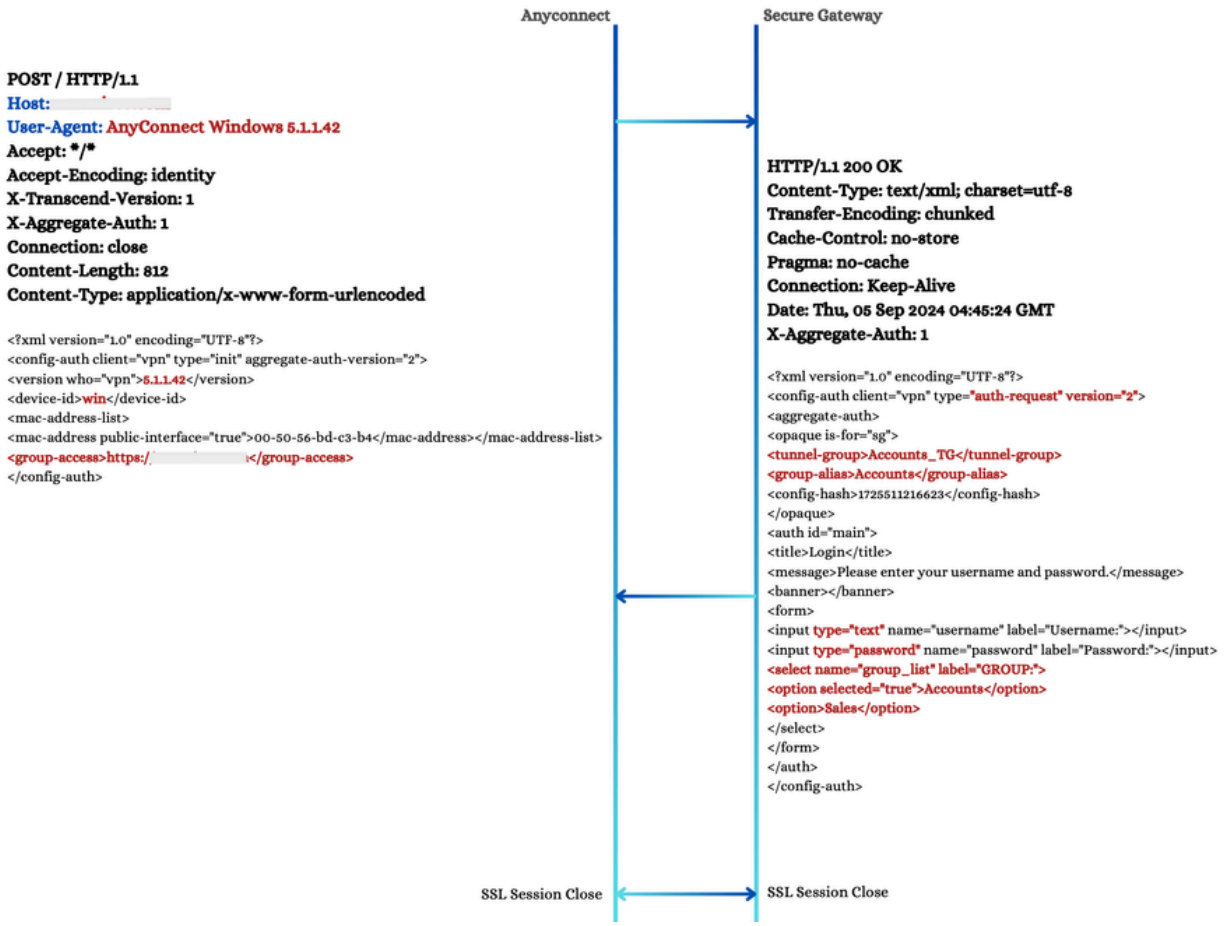
在此操作期間，除非使用者明確指定，否則客戶端不擁有關於連線配置檔案的資訊。如請求中的group-access元素所示，連線嘗試定向到安全網關URL(asa.example.com)。客戶端表示它支援聚合身份驗證第2版，這比早期版本有顯著改進，特別是在高效的XML事務方面。安全網關和客戶端必須同意要使用的版本。在安全網關不支援版本2的情況下，會觸發額外的POST操作，導致客戶端回退到較早版本。

在HTTP響應中，安全網關指示以下內容：

- 安全網關支援的聚合身份驗證版本。
- 隧道組清單和使用者名稱/密碼表單。

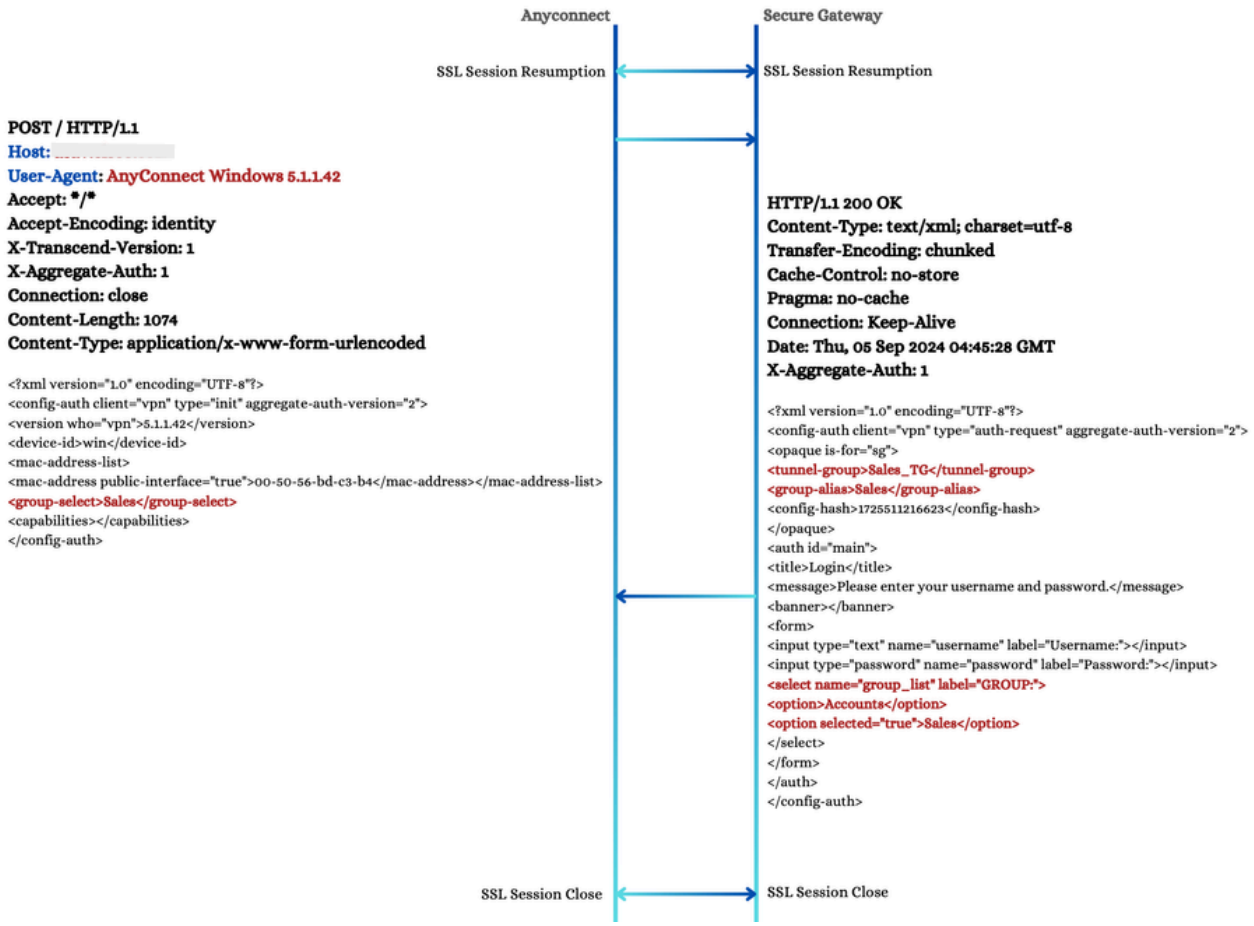


附註：表單包括一個選擇元素，該元素列出了在安全網關上配置的所有連線配置檔案的組別名。預設情況下，其中一個組別名會突出顯示selected = "true"布林屬性。tunnel-group和group-alias元素與此選擇的連線配置檔案相對應。



POST — 組選擇1

如果使用者從此清單中選擇不同的連線配置檔案，將進行另一個POST操作。在這種情況下，客戶端傳送一個POST請求，其中更新了組選擇元素，以反映所選的連線配置檔案，如下圖所示。

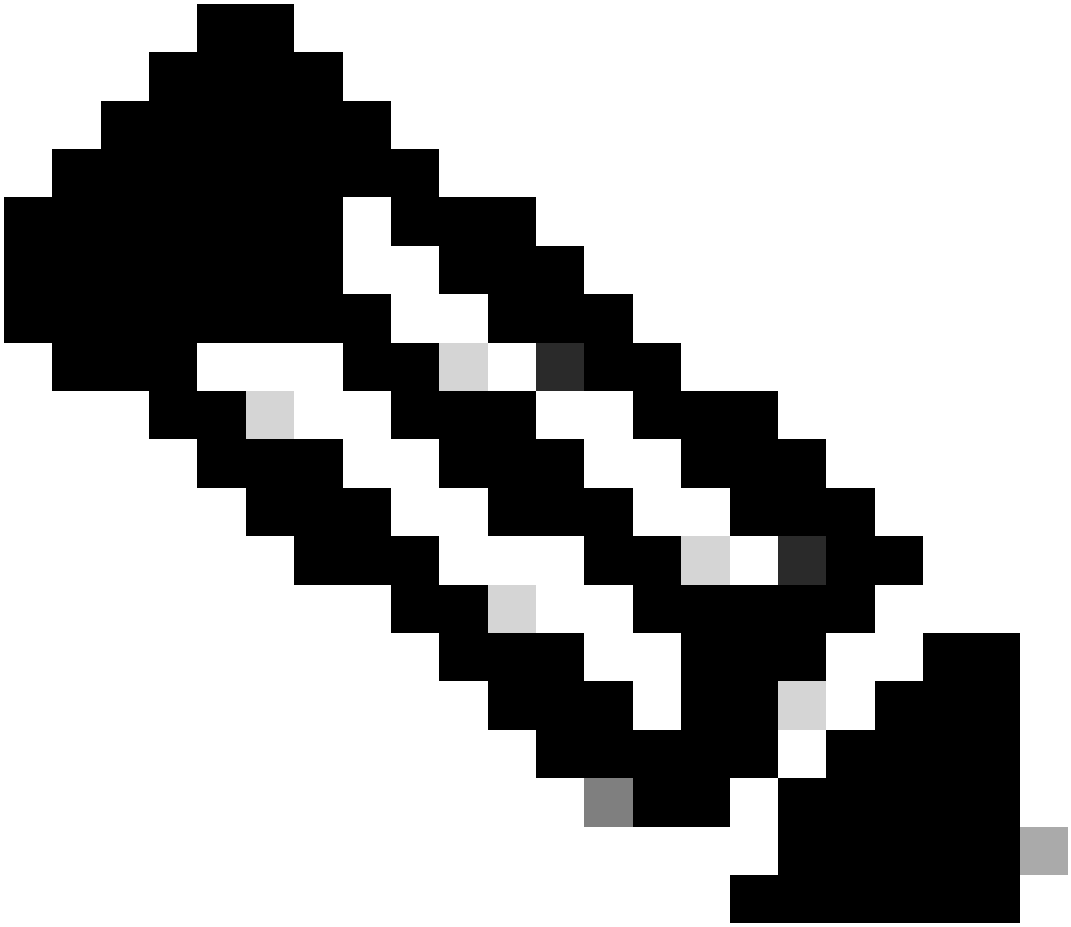


POST — 組選擇2

POST — 使用者身份驗證

在此操作中，AnyConnect將此資訊傳送到安全網關：

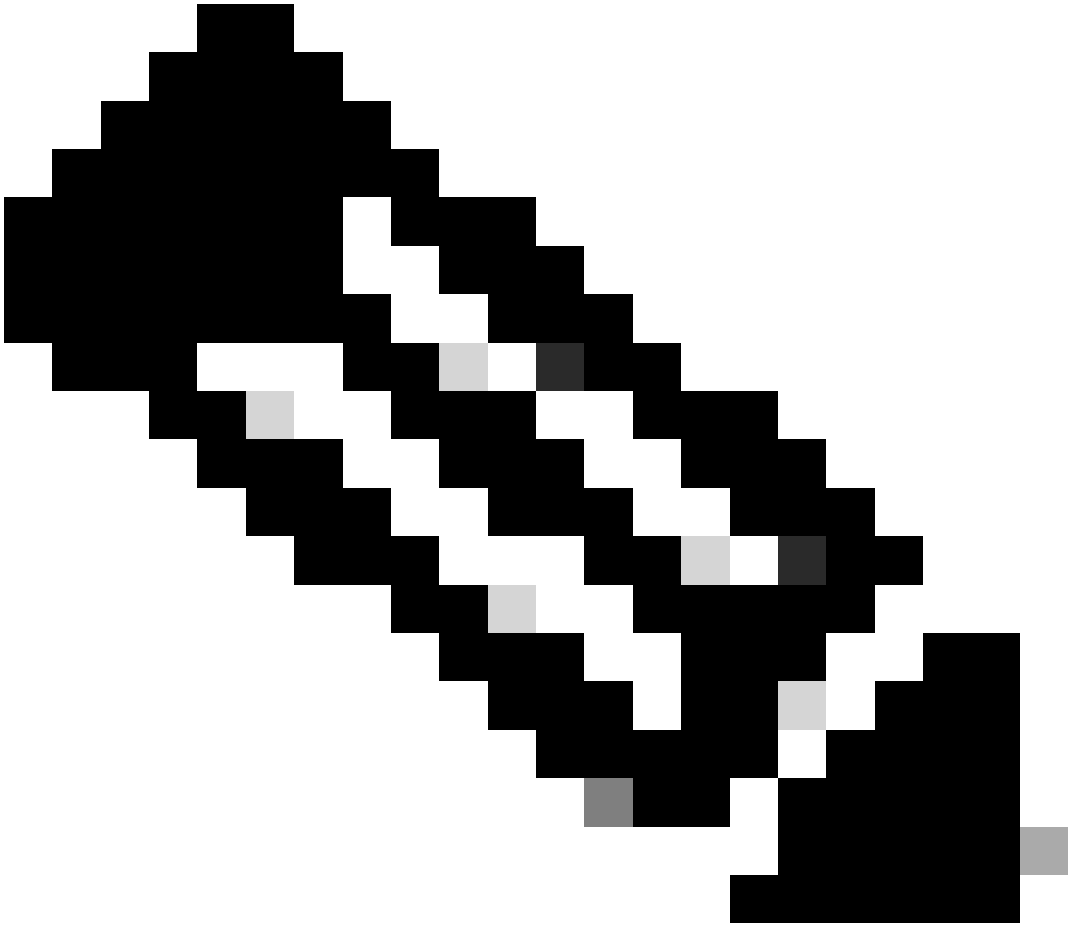
- 所選連線配置檔案信息：這包括隧道組名稱和組別名（如前面操作中的安全網關所示）。
- 使用者名稱和密碼：使用者的身份驗證憑據。



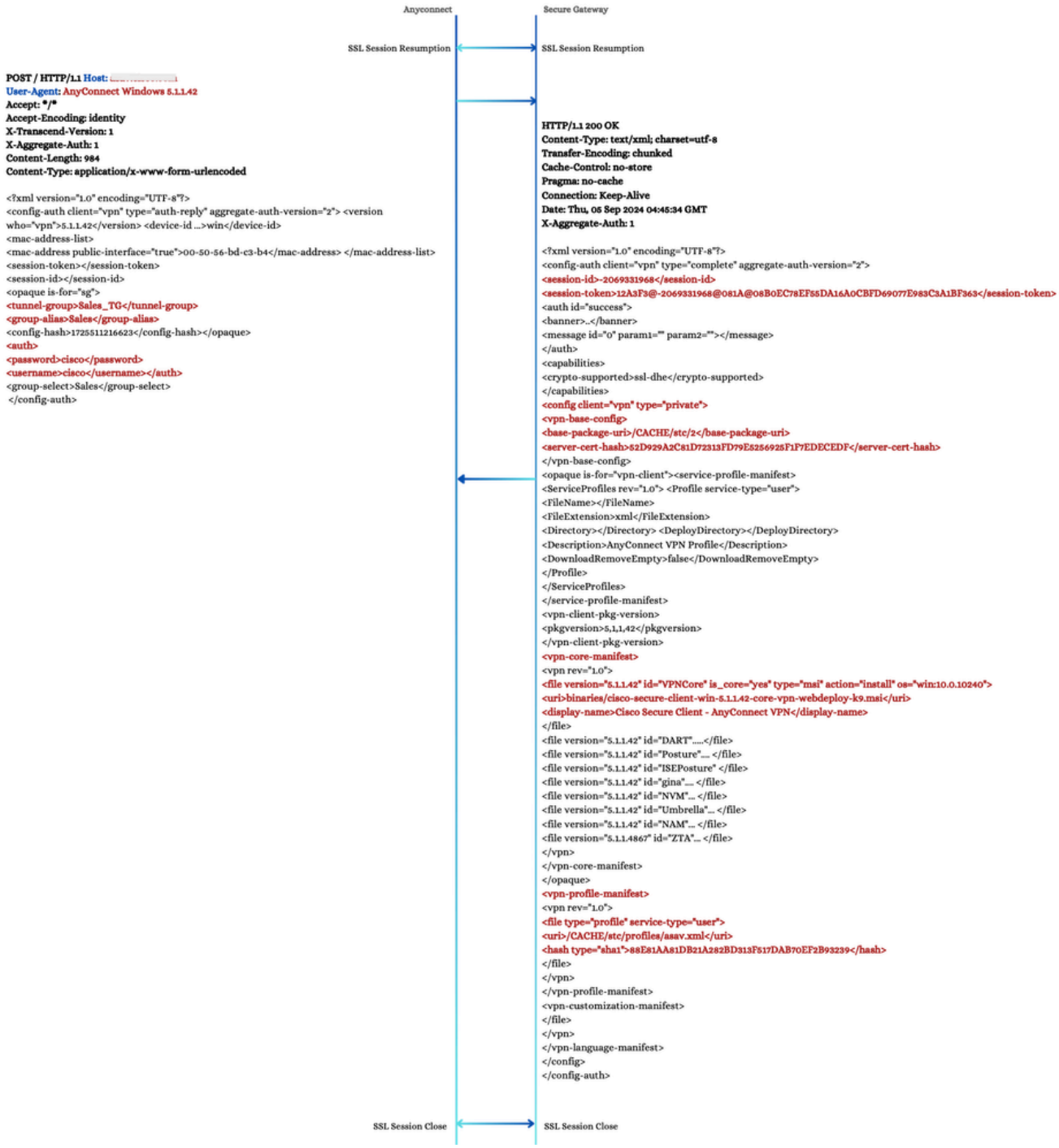
附註：由於此流量專用於AAA身份驗證，因此它可能不同於其他身份驗證方法。

為響應POST操作，安全網關會傳送包含以下資訊的XML檔案：

- 會話ID:這與SSL會話ID不同。
- 會話令牌:客戶端稍後會將此令牌用作WebVPN cookie。
- 身份驗證狀態：由id = success的auth元素表示。
- 伺服器證書雜湊:此雜湊值在preferences.xml檔案中快取。
- vpn-core-manifest元素:此元素指示AnyConnect核心包的路徑和版本，以及其他元件，如Dart、安全狀態、ISE安全狀態等。VPN下載程式將在下一節中使用它。
- 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。



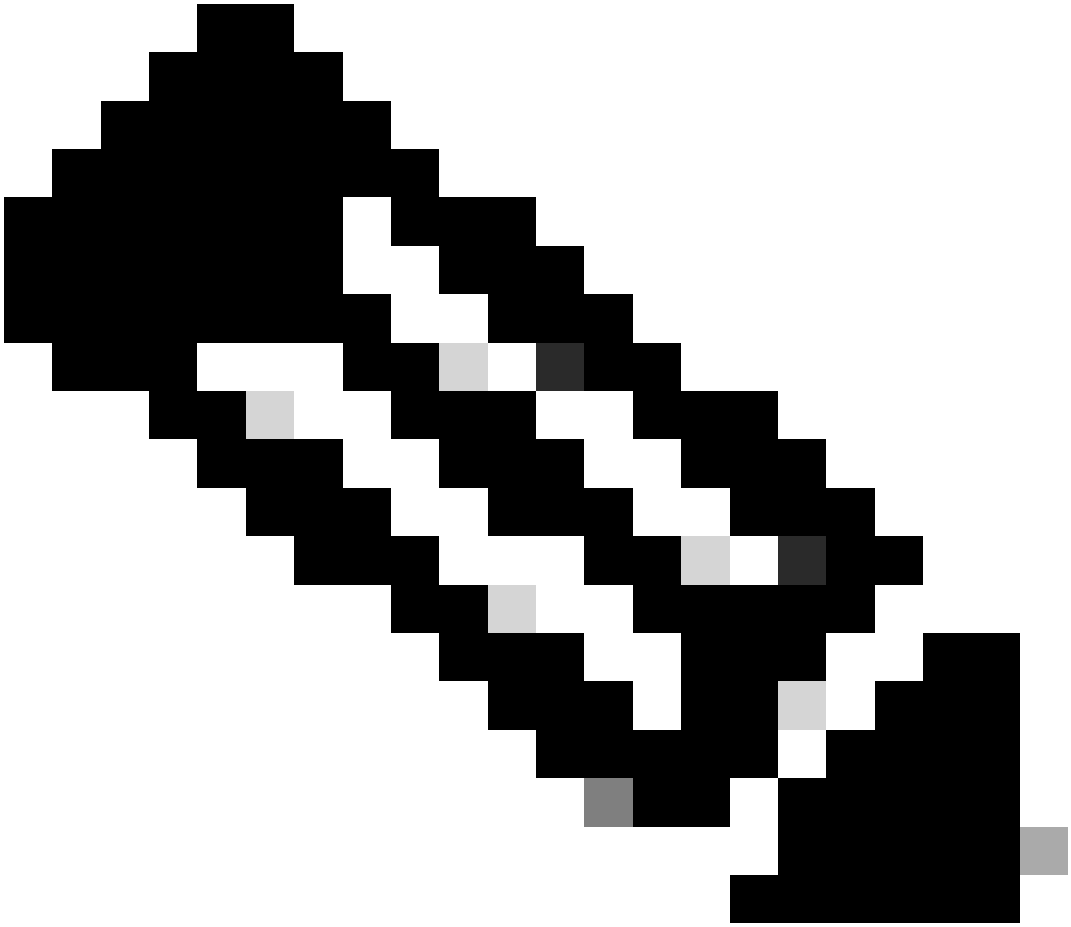
附註：如果客戶端沒有配置檔案，下一部分中的VPN下載程式將下載該配置檔案。如果使用者端已有設定檔，則會比較使用者端設定檔的SHA-1雜湊與伺服器的雜湊值。如果不匹配，VPN下載程式會使用安全網關上的配置檔案覆蓋客戶端配置檔案。這可確保身份驗證後，安全網關上的配置檔案在客戶端上實施。



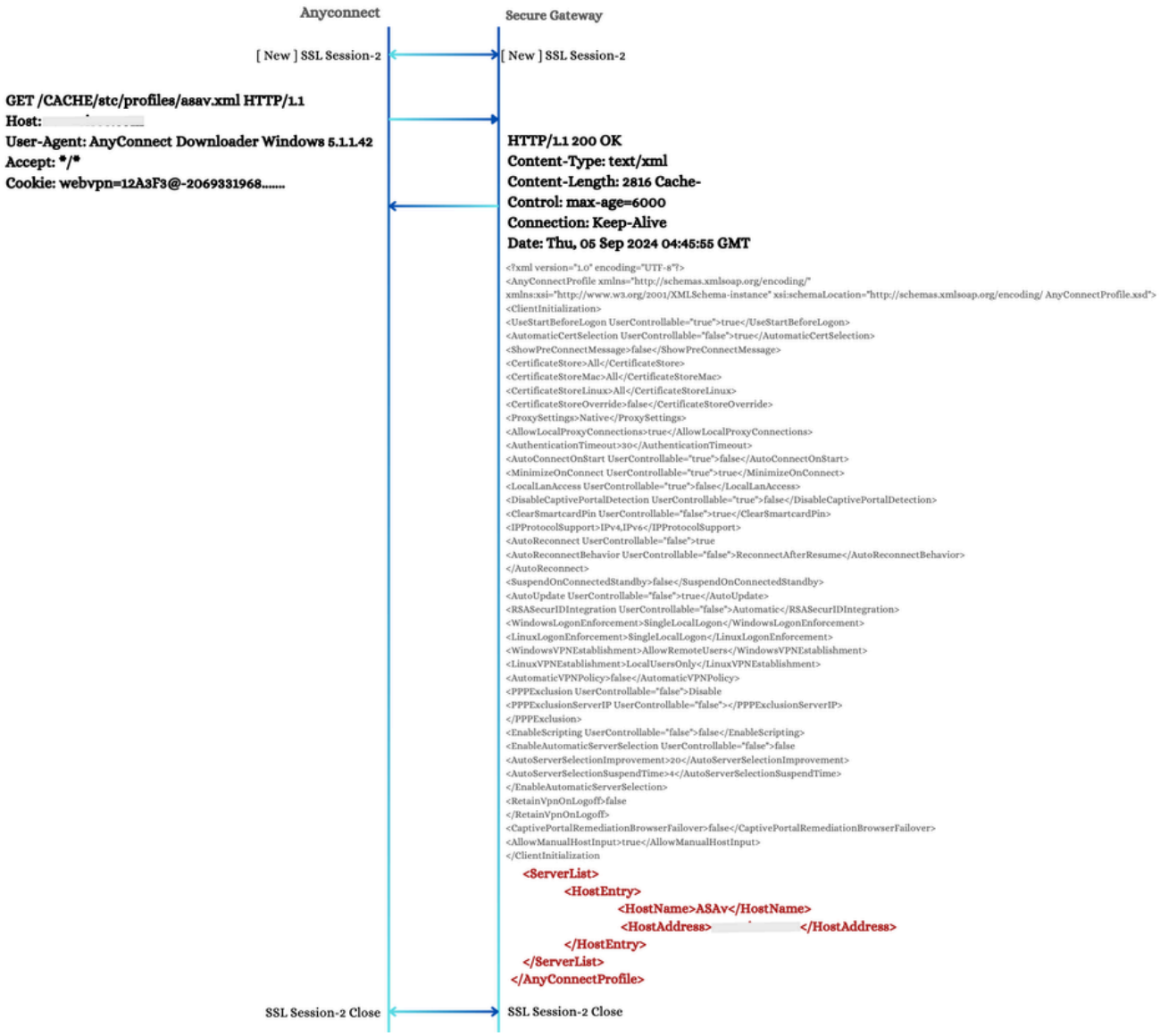
POST — 使用者身份驗證

AnyConnect下載程式

AnyConnect下載程式始終啟動新的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個證書警告。在此階段中，它會針對必須下載的每個專案執行單獨的GET操作。



附註：如果使用者端設定檔上傳到Secure Gateway，必須下載該使用者端設定檔；否則，整個連線嘗試將終止。

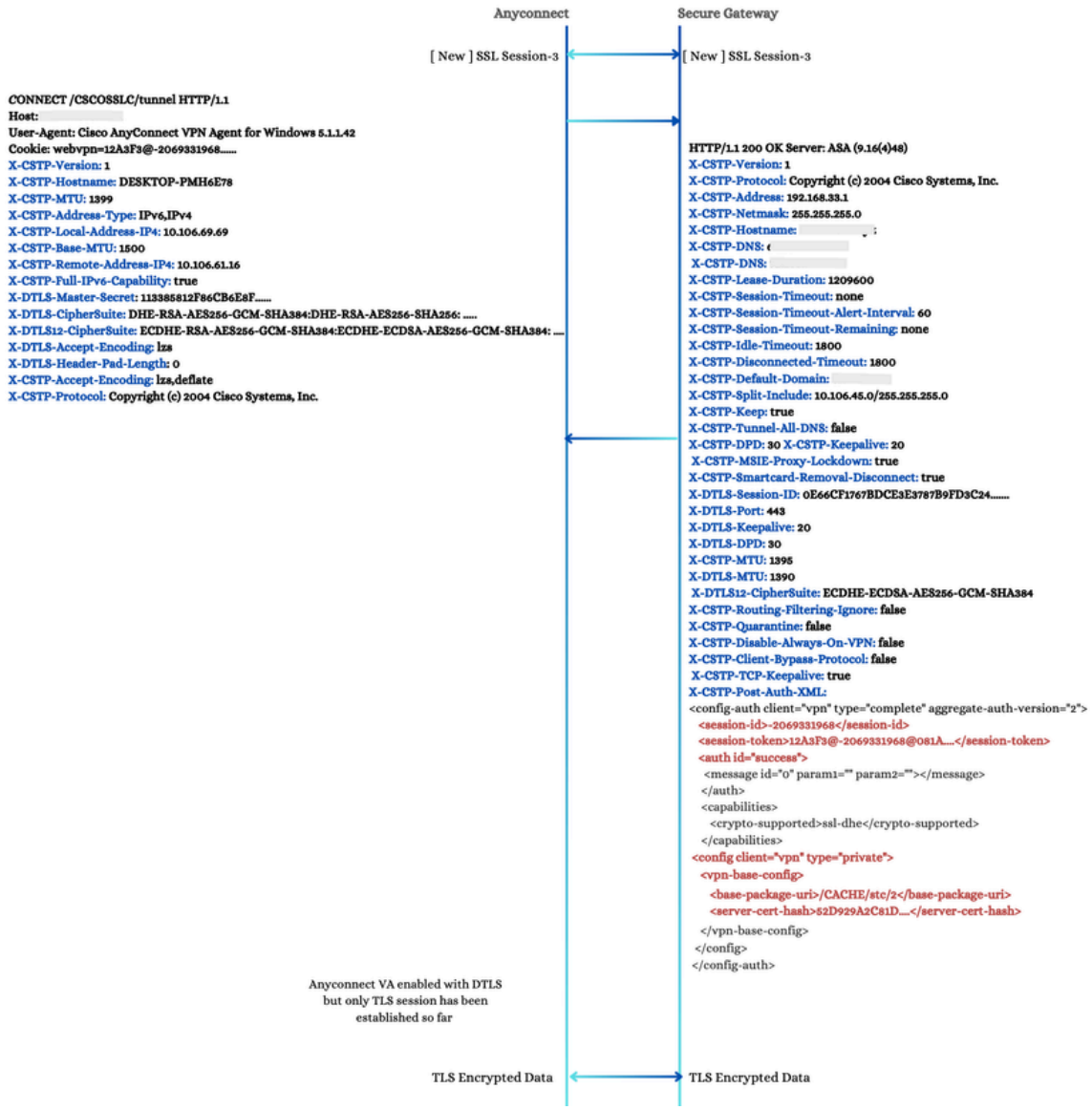


VPN下載器

CSTP連線

AnyConnect執行CONNECT操作是建立安全通道的最後一步。在CONNECT操作期間，AnyConnect客戶端將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屬性進行響應。此交換包括X-CSTP-Post-Auth-XML以及XML檔案，該檔案與使用者後身份驗證步驟中的檔案基本相似。

收到成功響應後，AnyConnect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

DTLS握手

由於CONNECT事件期間客戶端和伺服器之間交換的屬性，此握手相對較快。資料包傳輸層安全(DTLS)握手過程如下：

用戶端

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。

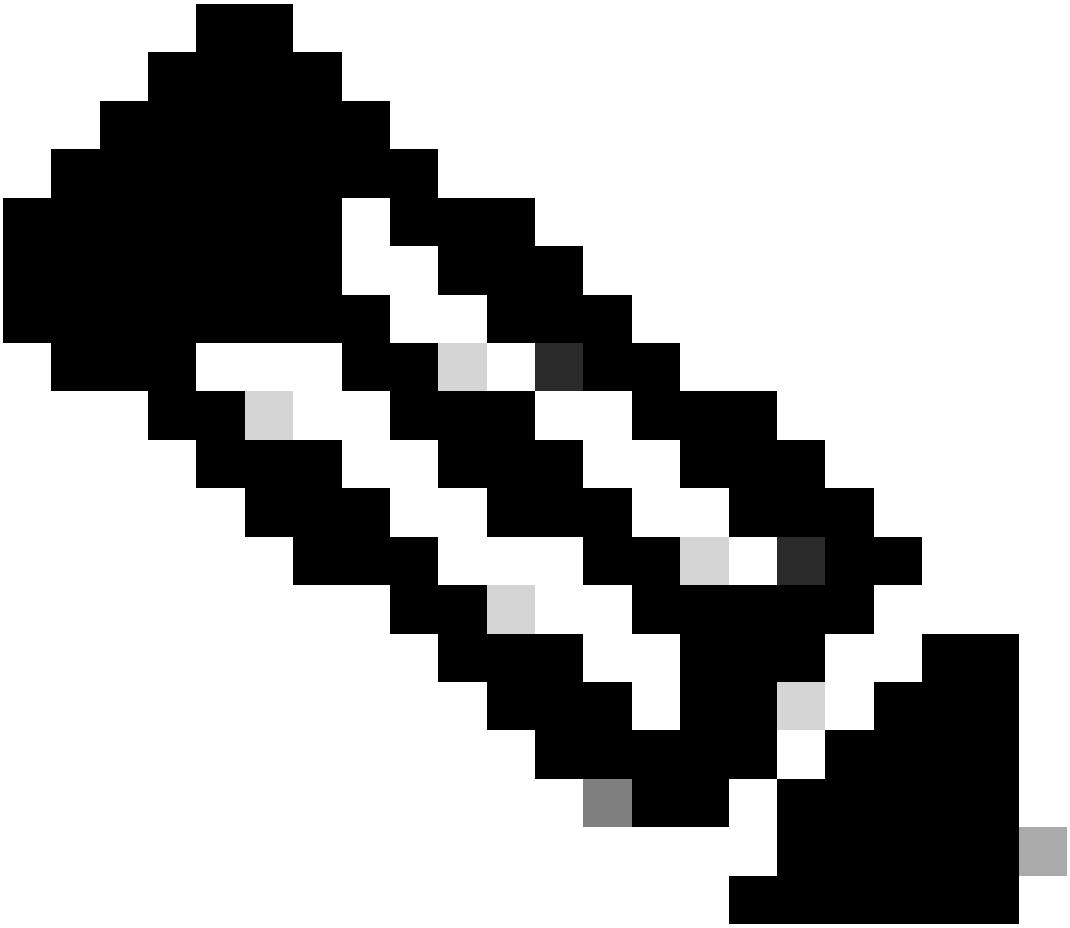
X-DTLS-CipherSuite:客戶端支援的DTLS密碼套件清單，指示客戶端的加密功能。

伺服器

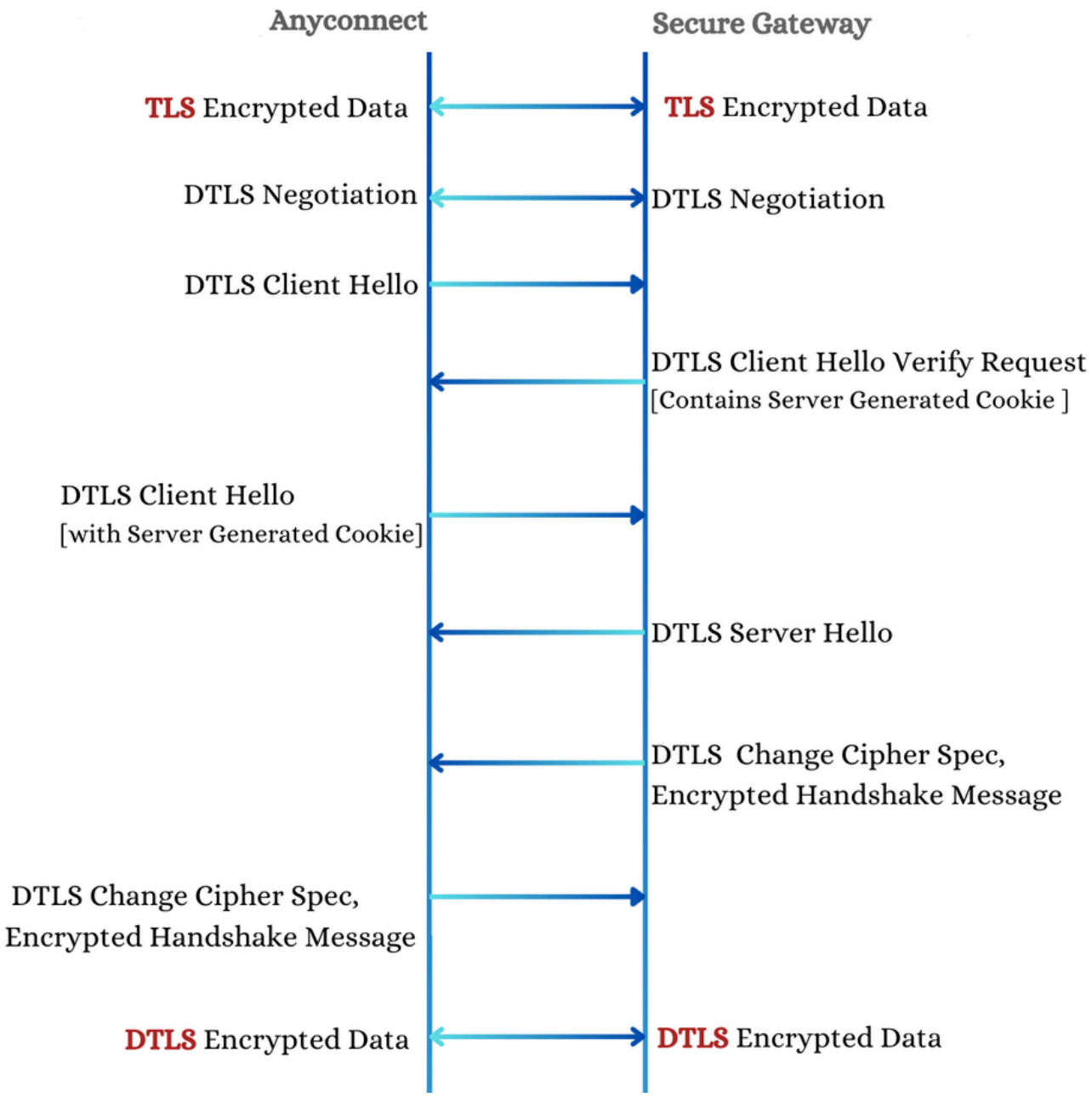
X-DTLS-Session-ID:由伺服器分配給客戶端使用的DTLS會話ID，從而確保會話的連續性。

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

。



附註：當DTLS握手正在進行時，TLS資料通道將繼續運行。這可確保資料傳輸在握手過程中保持一致和安全。到DTLS資料加密通道的無縫轉換僅在DTLS握手完成之後發生。

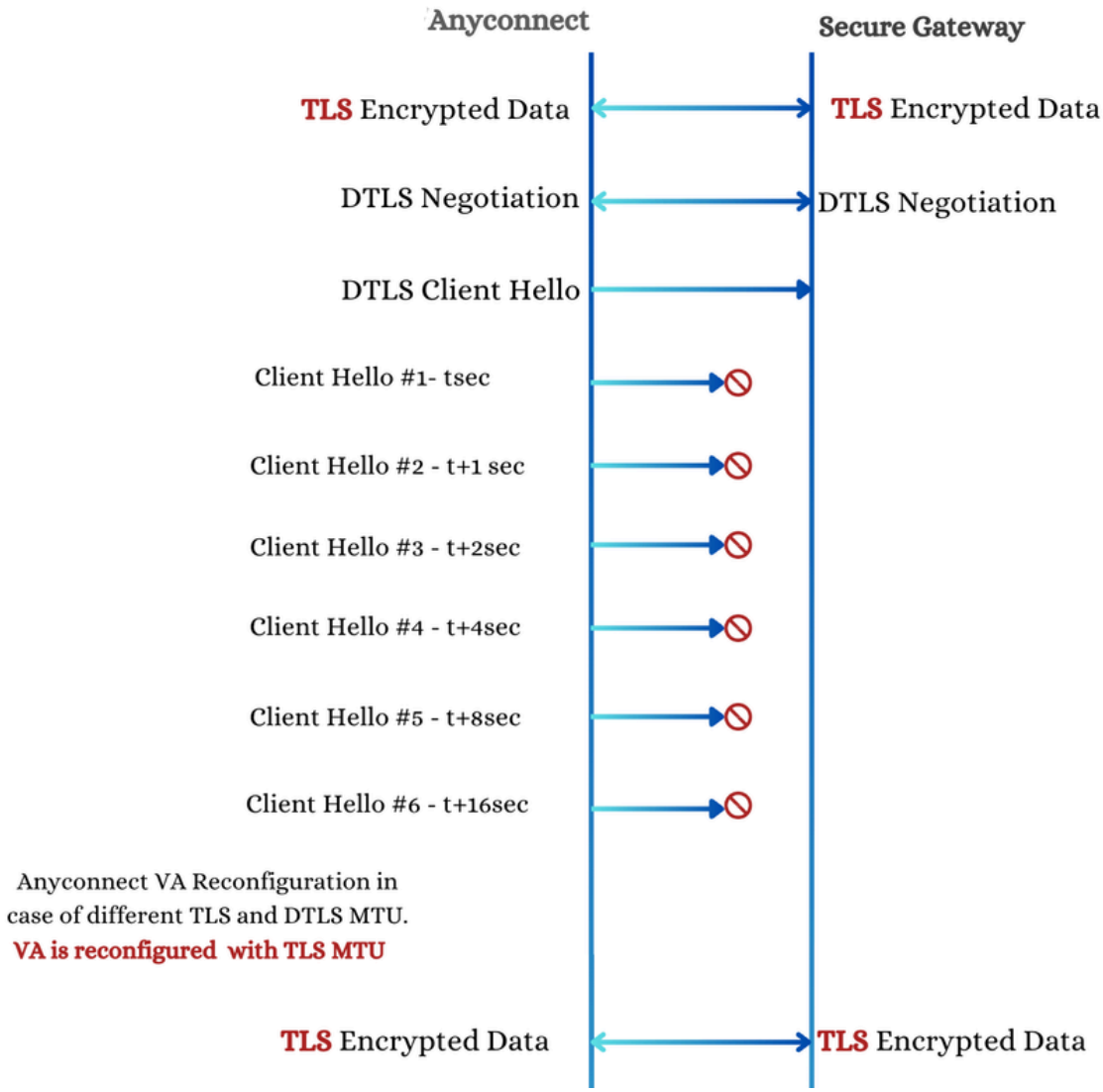


DTLS握手

DTLS埠被阻止

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執行指數回退，最多重試5次，從1秒延遲開始，最多增加16秒。

如果這些嘗試失敗，AnyConnect會將實際TLS MTU（由Secure Gateway在CONNECT操作期間返回的X-CSTP-MTU值指定）應用到AnyConnect虛擬介面卡。由於此MTU與先前應用的MTU(X-DTLS-MTU)不同，因此必須重新配置虛擬介面卡。在終端使用者看來，此重新配置是重新連線嘗試，但在過程中不會發生新的協商。虛擬介面卡重新配置後，TLS資料通道將繼續運行。



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）。