Informazioni sul flusso della connessione VPN SSL AnyConnect

Sommario

Introduzione

Questo documento si concentra sul flusso di eventi che si verificano tra AnyConnect e il gateway sicuro durante una connessione VPN.

Premesse

AnyConnect

AnyConnect è il client VPN Cisco progettato per i protocolli SSL e IKEv2. È disponibile per la maggior parte delle piattaforme desktop e portatili. AnyConnect stabilisce principalmente connessioni protette con i router Firepower Threat Defense (FTD), Adaptive Security Appliance (ASA) o Cisco IOS®/Cisco IOS® XE noti come gateway sicuri.

Secure Gateway

Nella terminologia Cisco, un server VPN SSL viene definito gateway protetto, mentre un server

IPSec (IKEv2) viene definito gateway VPN di accesso remoto. Cisco supporta la terminazione del tunnel VPN SSL sulle seguenti piattaforme:

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

Flusso di connessione AnyConnect SSL VPN

In questo documento gli eventi che si verificano tra AnyConnect e Secure Gateway durante la connessione VPN SSL vengono suddivisi in sei fasi:

1. Handshake SSL

2. POST - Selezione gruppo

3. POST - Autenticazione utente con nome utente/password (facoltativo)

4. VPN Downloader (opzionale)

5. CSTP CONNECT

6. Connessione DTLS (opzionale)

1. Handshake SSL

L'handshake SSL viene avviato dal client AnyConnect dopo il completamento dell'handshake TCP a 3 vie con un messaggio 'Client Hello'. Il flusso degli eventi e le principali soluzioni sono come già detto.

Hello del client

La sessione SSL inizia con l'invio da parte del client di un messaggio 'Client Hello'. In questo messaggio:

a) L'ID sessione SSL è impostato su 0, per indicare l'avvio di una nuova sessione.

b) Il payload include le suite di cifratura supportate dal client e un nonce casuale generato dal client.

Server Hello

Il server risponde con un messaggio "Server Hello", che include:

a) La suite di cifratura selezionata dall'elenco fornito dal cliente.

b) Il server ha generato l'ID sessione SSL e un server ha generato un nonce casuale.

Certificato server

Dopo il messaggio "Server Hello", il server trasmette il proprio certificato SSL, che funge da identità. I punti chiave da tenere in considerazione includono:

a) Se questo certificato non supera un rigoroso controllo di convalida, AnyConnect per impostazione predefinita blocca il server.

b) L'utente ha la possibilità di disattivare questo blocco, ma le connessioni successive visualizzano un avviso fino a quando gli errori segnalati non vengono risolti.

Richiesta certificato client

Il server può inoltre richiedere un certificato client, inviando un elenco di DN del nome soggetto di tutti i certificati CA caricati nel gateway protetto. La richiesta ha due finalità:

a) Aiuta il client (utente) a scegliere il certificato di identità corretto se sono disponibili più certificati ID.

b) Assicura che il certificato restituito sia considerato attendibile dal gateway protetto, anche se è necessario eseguire ulteriori convalide del certificato.

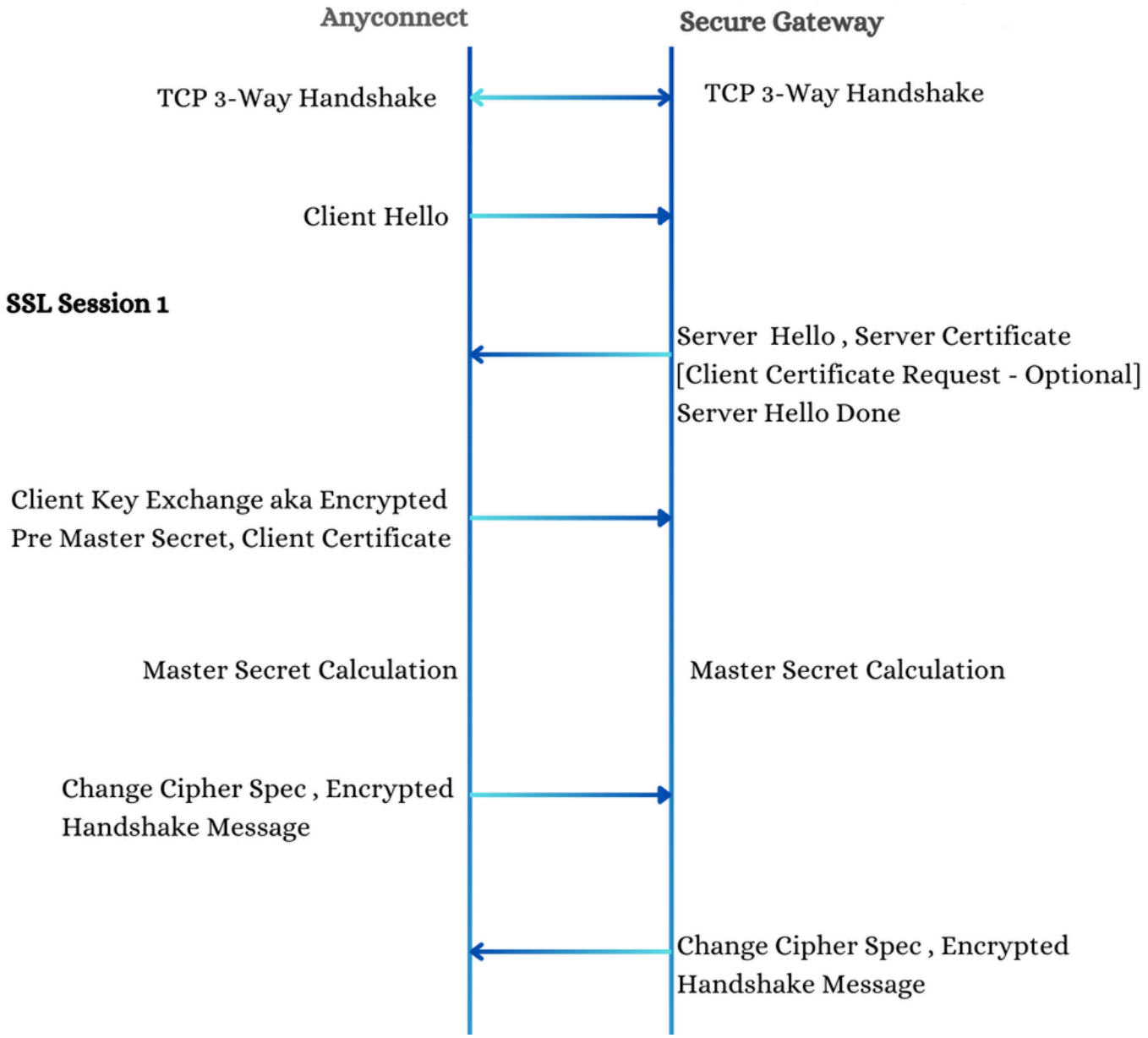
Scambio chiavi client

Il client invia quindi un messaggio 'Scambio chiave client', che include una chiave segreta pre-master. Questa chiave è crittografata con:

a) La chiave pubblica del server dal certificato del server, se la suite di cifratura scelta è basata su RSA (ad esempio, TLS_RSA_WITH_AES_128_CBC_SHA).

b) La chiave pubblica DH del server fornita nel messaggio Server Hello, se la suite di cifratura scelta è basata su DHE (ad esempio, TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

In base al segreto pre-master, al nonce casuale generato dal client e al nonce casuale generato dal server, sia il client che il gateway protetto generano in modo indipendente un master secret. Questo master secret viene quindi utilizzato per derivare le chiavi di sessione, garantendo una comunicazione sicura tra il client e il server.



Sessione 1 SSL

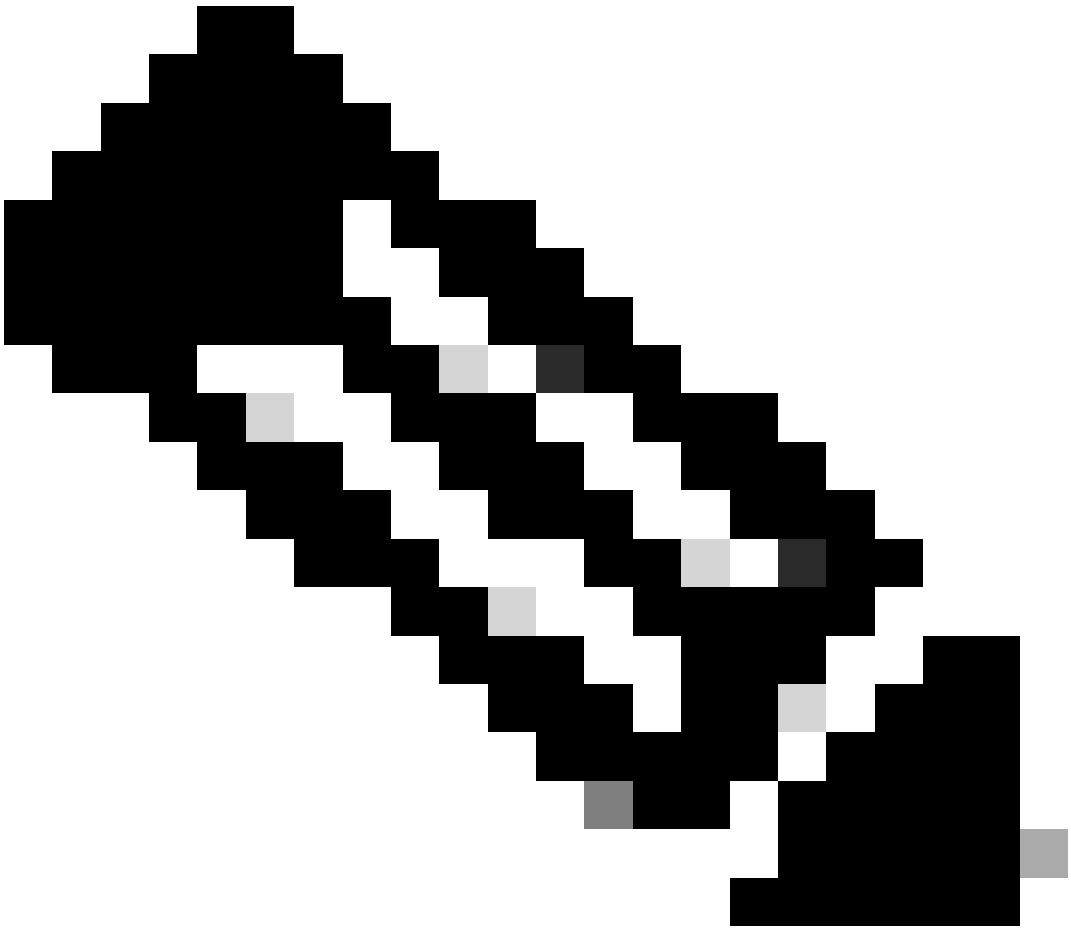
2. POST - Selezione gruppo

Durante questa operazione, il client non possiede informazioni sul profilo di connessione a meno che non sia esplicitamente specificato dall'utente. Il tentativo di connessione è diretto all'URL del gateway sicuro (asav.cisco.com), come indicato dall'elemento 'group-access' nella richiesta. Il client indica il supporto per la versione 2 di 'aggregate-authentication'. Questa versione rappresenta un miglioramento significativo rispetto alla versione precedente, in particolare in termini di transazioni XML efficienti. Sia il gateway sicuro che il client devono concordare la versione da utilizzare. Negli scenari in cui il gateway sicuro non supporta la versione 2, viene attivata un'operazione POST aggiuntiva che determina il ripristino della versione del client.

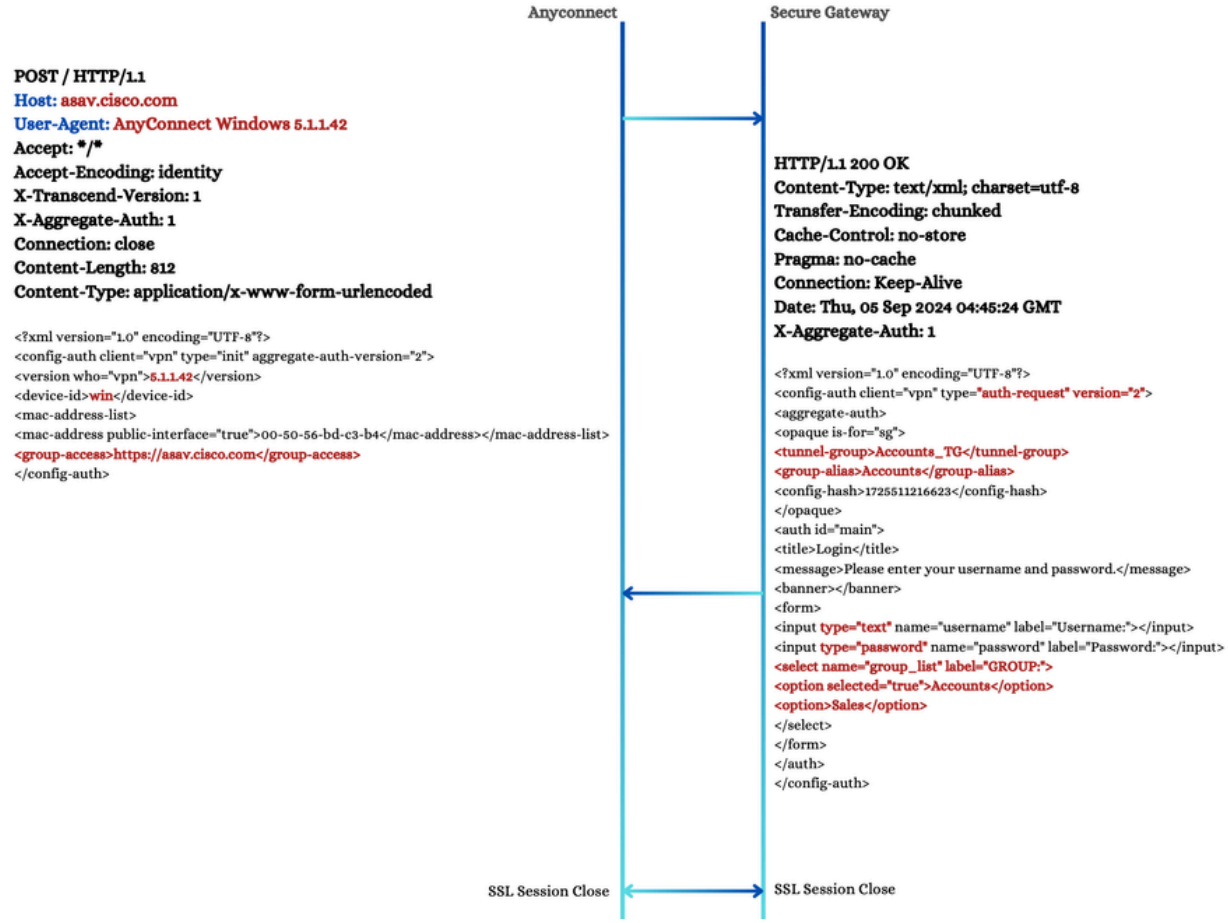
Nella risposta HTTP, il gateway sicuro indica quanto segue:

1. La versione dell'autenticazione aggregata supportata dal gateway sicuro.

2. Elenco dei gruppi di tunnel e Modulo nome utente/password.

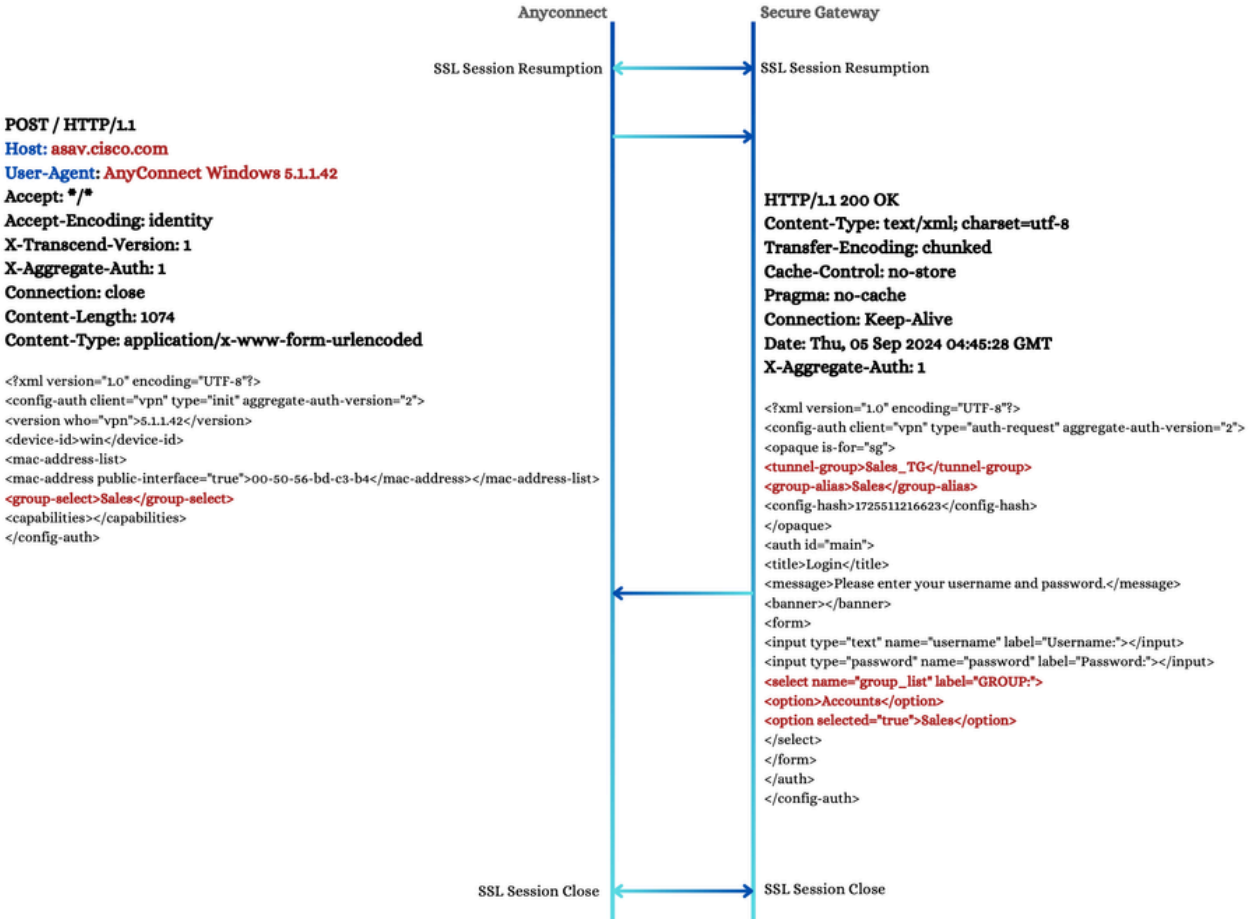


Nota: il form include un elemento 'select', che elenca gli alias di gruppo di tutti i profili di connessione configurati sul gateway sicuro. Per impostazione predefinita, uno di questi alias di gruppo viene evidenziato con l'attributo booleano selezionato = "true". Gli elementi tunnel-group e group-alias corrispondono al profilo di connessione scelto.



POST - Selezione gruppo 1

Se l'utente sceglie un profilo di connessione diverso da questo elenco, viene eseguita un'altra operazione POST. In questo caso, il client invia una richiesta POST con l'elemento 'group-select' aggiornato per riflettere il profilo di connessione scelto, come mostrato di seguito.



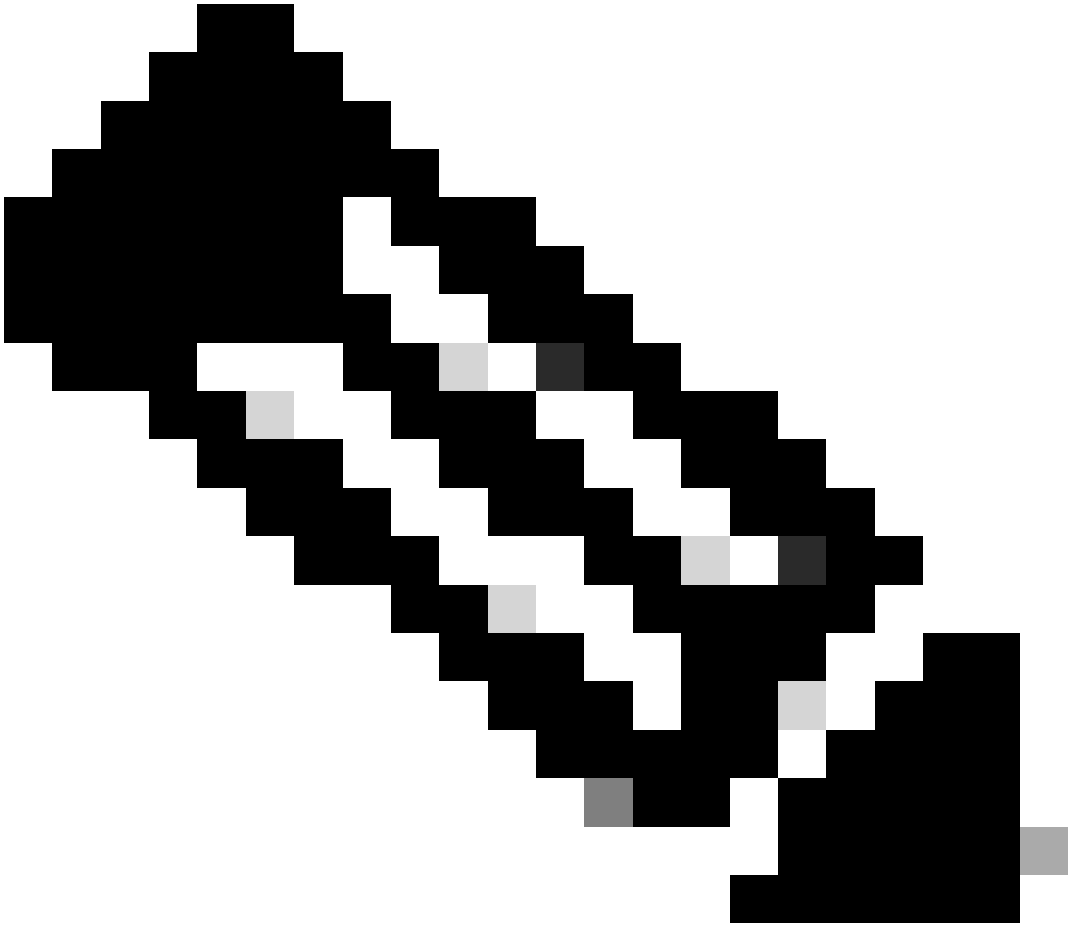
POST - Selezione gruppo 2

3. Autenticazione POST - utente

In questa operazione, che segue la selezione POST-gruppo, AnyConnect invia queste informazioni al gateway sicuro:

1. Informazioni sul profilo di connessione scelto: includono il nome del gruppo di tunnel e l'alias del gruppo come indicato dal gateway protetto nell'operazione precedente.

2. Username and Password: le credenziali di autenticazione dell'utente.



Nota: poiché questo flusso è specifico dell'autenticazione AAA, può differire da altri metodi di autenticazione.

In risposta all'operazione POST, Secure Gateway invia un file XML contenente le seguenti informazioni:

1. ID sessione: diverso dall'ID sessione SSL.

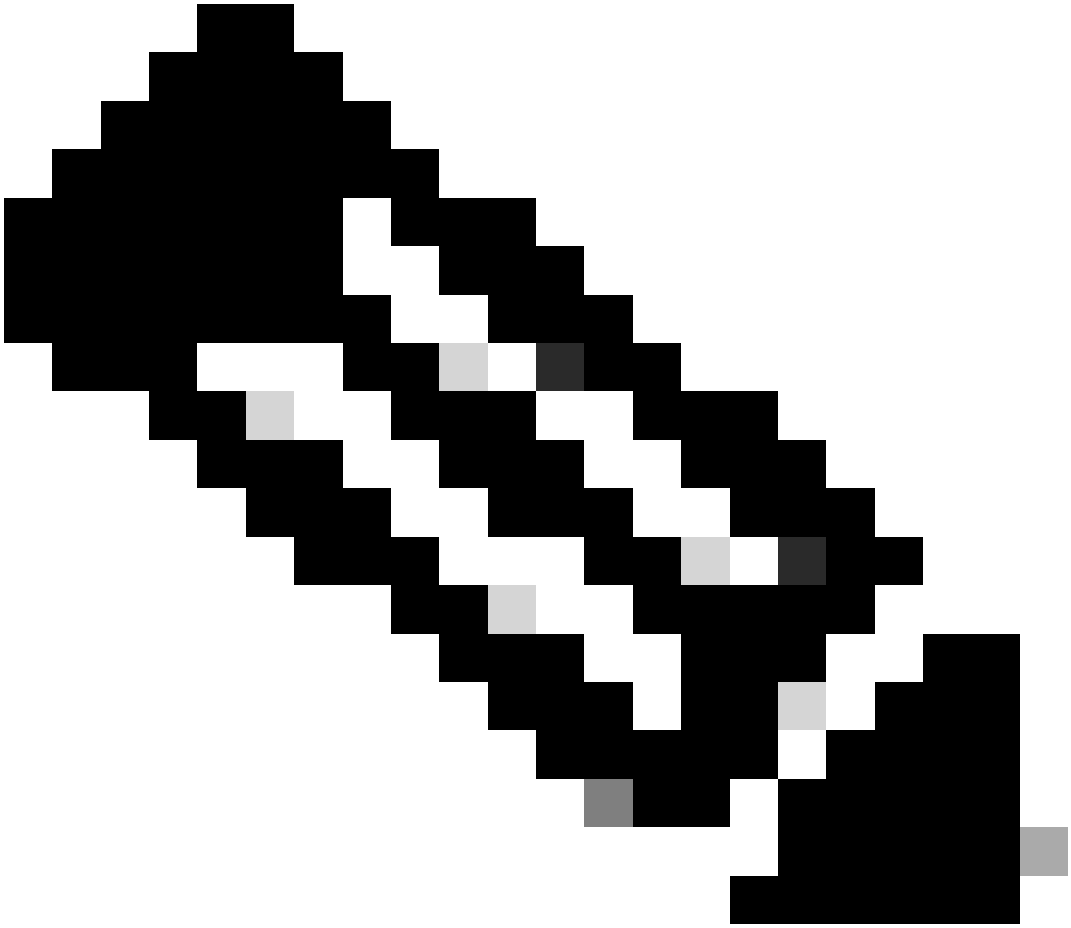
2. Token di sessione: questo token viene in seguito utilizzato dal client come cookie WebVPN.

3. Authentication Status: indicato da un elemento auth con id = 'success'.

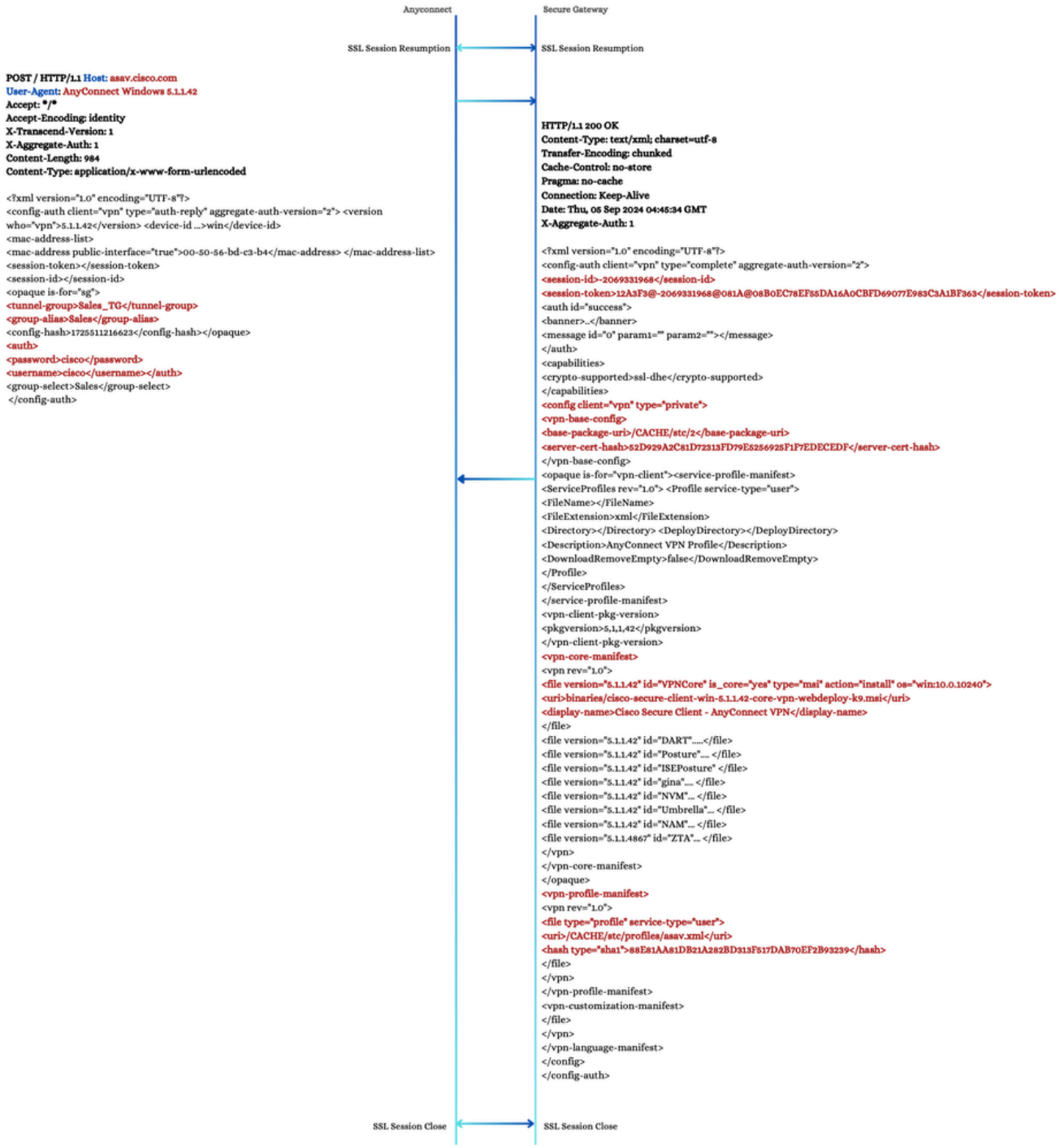
4. Hash certificato server: questo hash viene memorizzato nella cache nel file preferences.xml.

5. vpn-core-manifest Element: questo elemento indica il percorso e la versione del pacchetto principale AnyConnect, insieme ad altri componenti come Dart, Posture, ISE Posture e così via. Viene utilizzato dal download VPN nella sezione successiva.

6. vpn-profile-manifest Element: questo elemento indica il percorso (il nome del profilo) e l'hash SHA-1 del profilo.



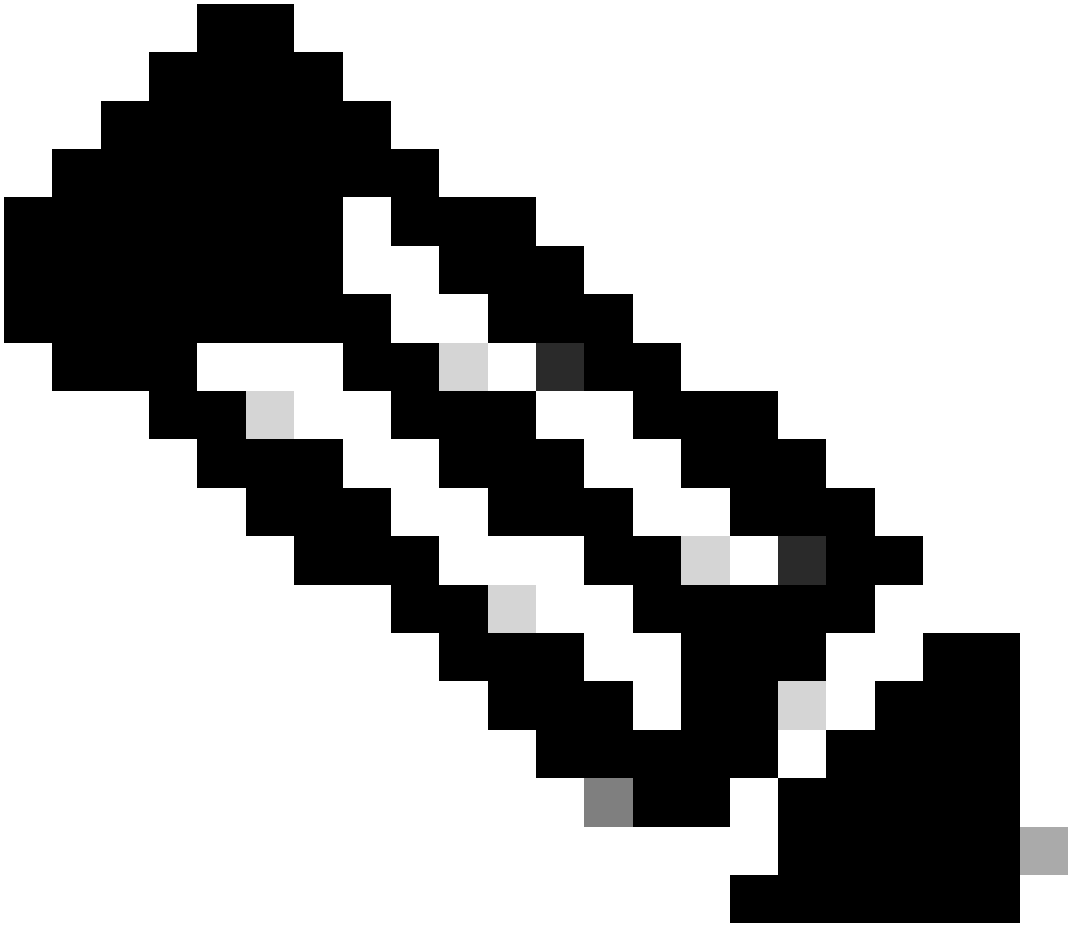
Nota: se il client non dispone del profilo, VPN Downloader lo scarica nella sezione successiva. Se il client dispone già del profilo, l'hash SHA-1 del profilo client viene confrontato con quello del server. In caso di mancata corrispondenza, il downloader VPN sovrascrive il profilo client con quello sul gateway sicuro. In questo modo il profilo sul gateway sicuro viene applicato sul client dopo l'autenticazione.



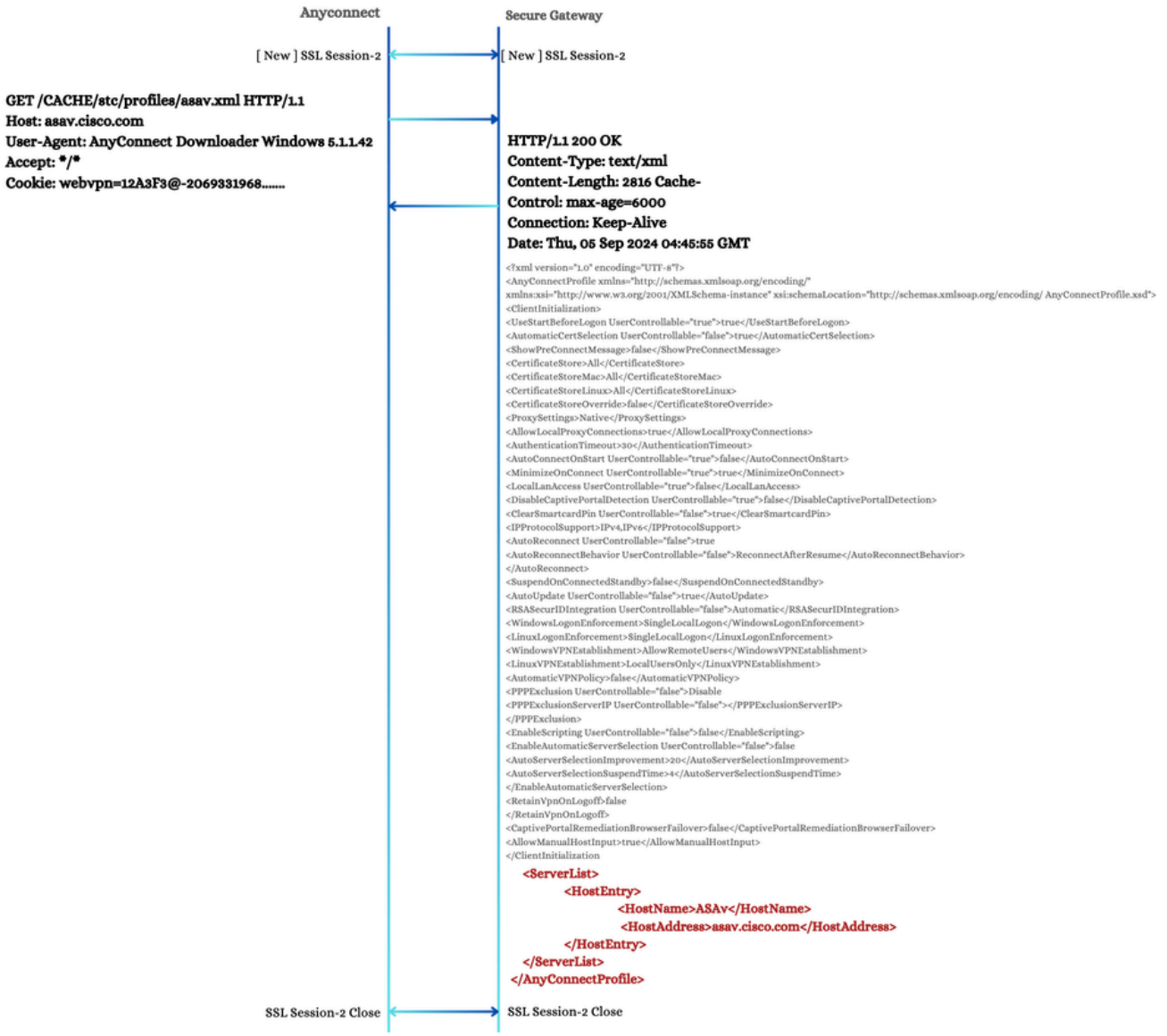
POST - Autenticazione utente

4. AnyConnect Downloader

AnyConnect Downloader avvia sempre una nuova sessione SSL, quindi gli utenti possono ricevere un secondo avviso di certificato nel caso in cui il certificato del gateway sicuro non sia attendibile. Durante questa fase, esegue operazioni GET separate per ogni elemento da scaricare.



Nota: se il profilo client viene caricato su Secure Gateway, è obbligatorio per il download; in caso contrario, l'intero tentativo di connessione viene terminato.

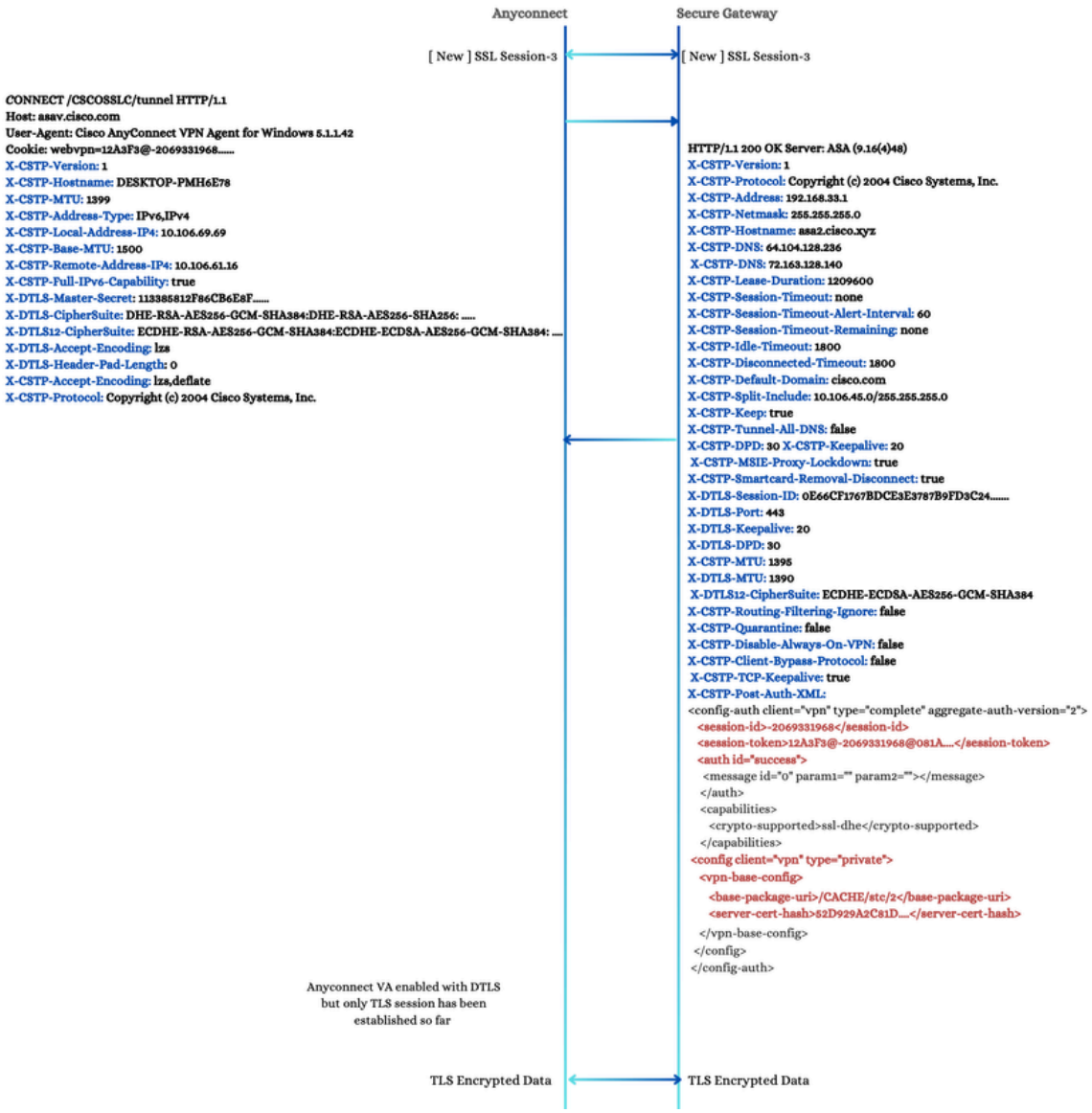


VPN Downloader

5. CONNESSIONE CSTP

AnyConnect esegue un'operazione CONNECT come fase finale della creazione di un canale sicuro. Durante l'operazione CONNECT, il client AnyConnect invia vari attributi X-CSTP e X-DTLS per il gateway sicuro da elaborare. Secure Gateway risponde con attributi X-CSTP e X-DTLS aggiuntivi che il client applica al tentativo di connessione corrente. Questo scambio include X-CSTP-Post-Auth-XML, accompagnato da un file XML, che è in gran parte simile a quello visto nella fase di post - autenticazione dell'utente.

Dopo aver ricevuto una risposta positiva, AnyConnect avvia il canale dati TLS. Contemporaneamente, l'interfaccia della scheda virtuale AnyConnect viene attivata con un valore MTU uguale a X-DTLS-MTU, a condizione che il successivo handshake DTLS abbia esito positivo.



CSTP Connect

6. Handshake DTLS

L'handshake DTLS procede come descritto di seguito. Questa configurazione è relativamente rapida a causa degli attributi scambiati tra il client e il server durante l'evento CONNECT.

Client

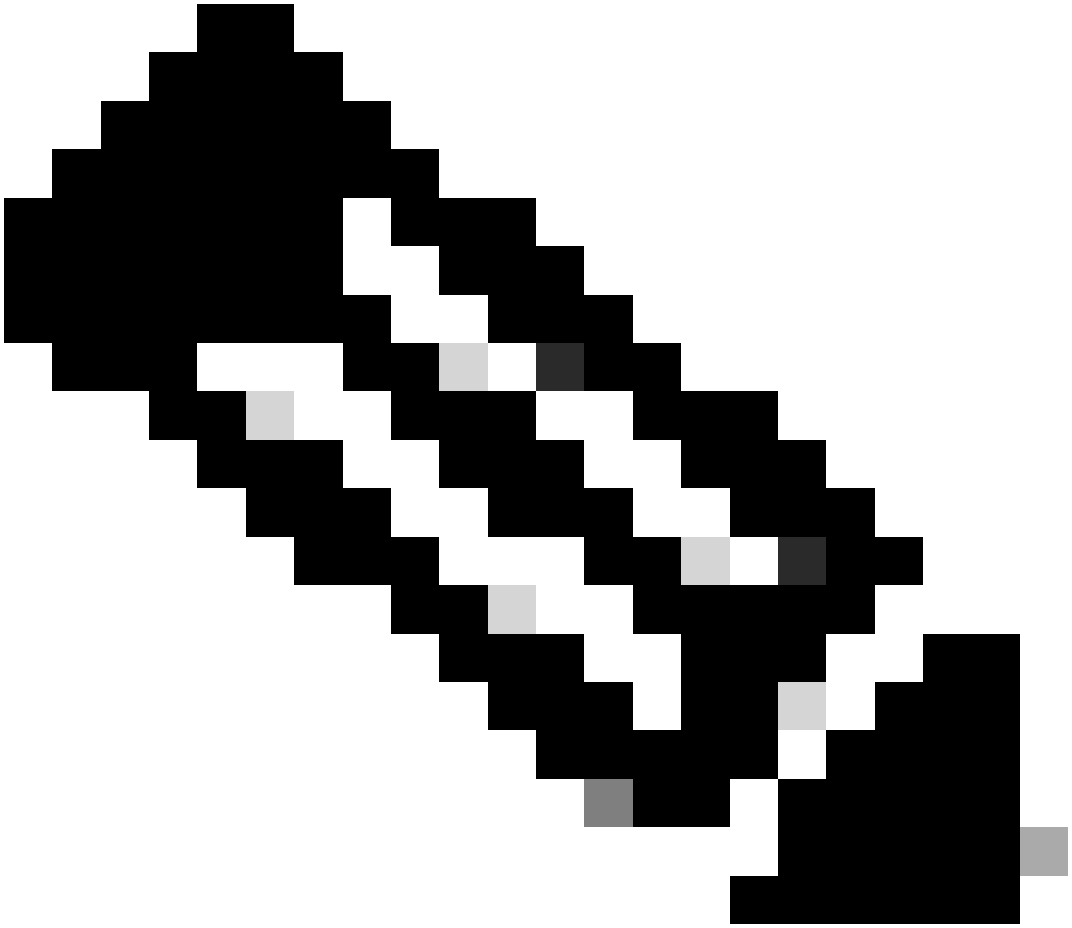
X-DTLS-Master-Secret: il Master Secret DTLS viene generato dal client e condiviso con il server. Questa chiave è fondamentale per stabilire una sessione DTLS sicura.

X-DTLS-CipherSuite: elenco di suite di cifratura DTLS supportate dal client, che indica le funzionalità di crittografia del client.

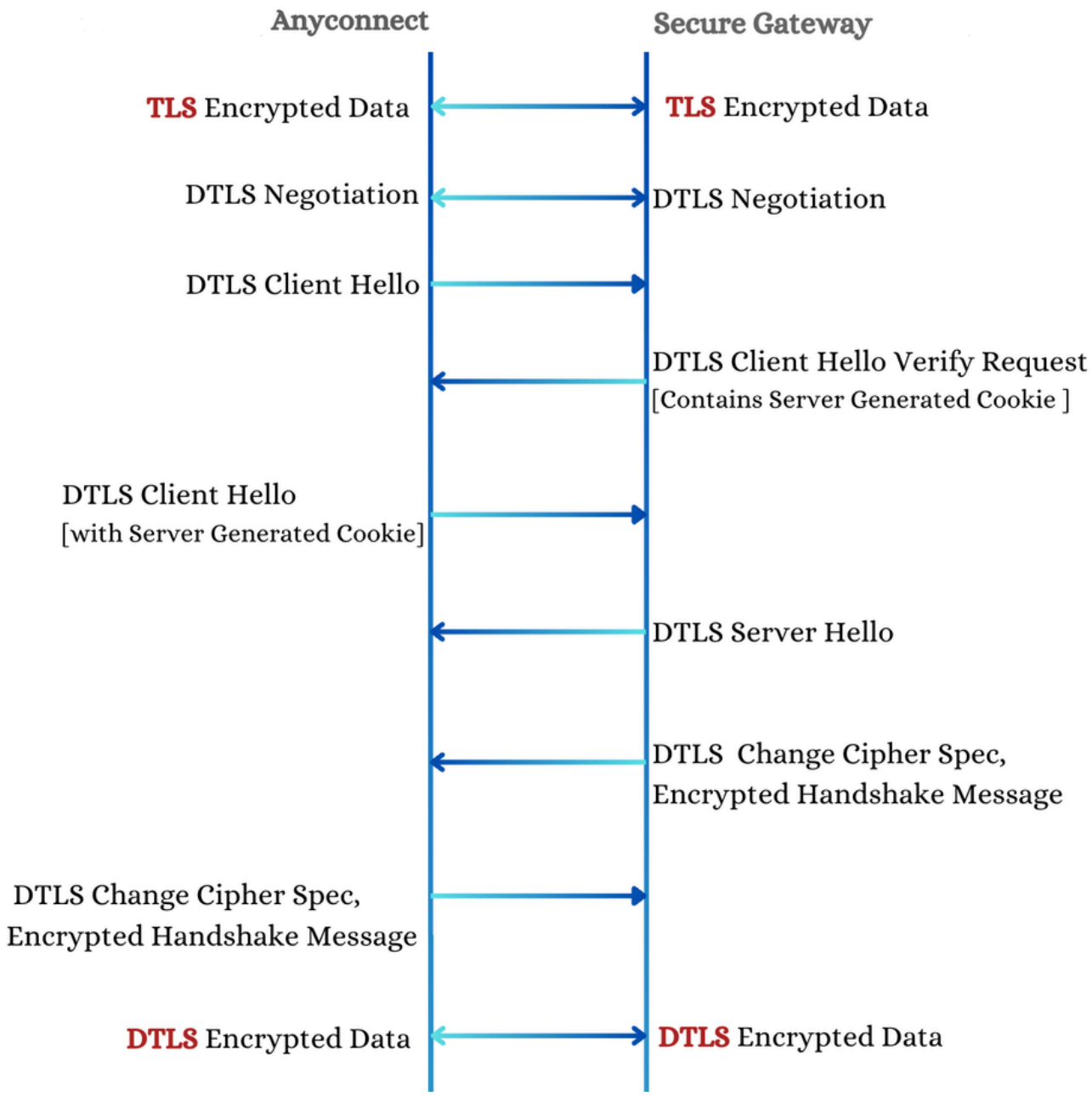
Server

X-DTLS-Session-ID: l'ID sessione DTLS assegnato dal server per l'utilizzo da parte del client, che garantisce la continuità della sessione.

X-DTLS-CipherSuite: la suite di cifratura selezionata dal server dall'elenco fornito dal client, in modo che entrambe le parti utilizzino un metodo di crittografia compatibile.



Nota: mentre l'handshake DTLS è in corso, il canale dati TLS continua a funzionare. Ciò garantisce che la trasmissione dei dati rimanga coerente e sicura durante il processo di handshake. La transizione al canale di crittografia dei dati DTLS avviene senza interruzioni solo dopo il completamento dell'handshake DTLS.

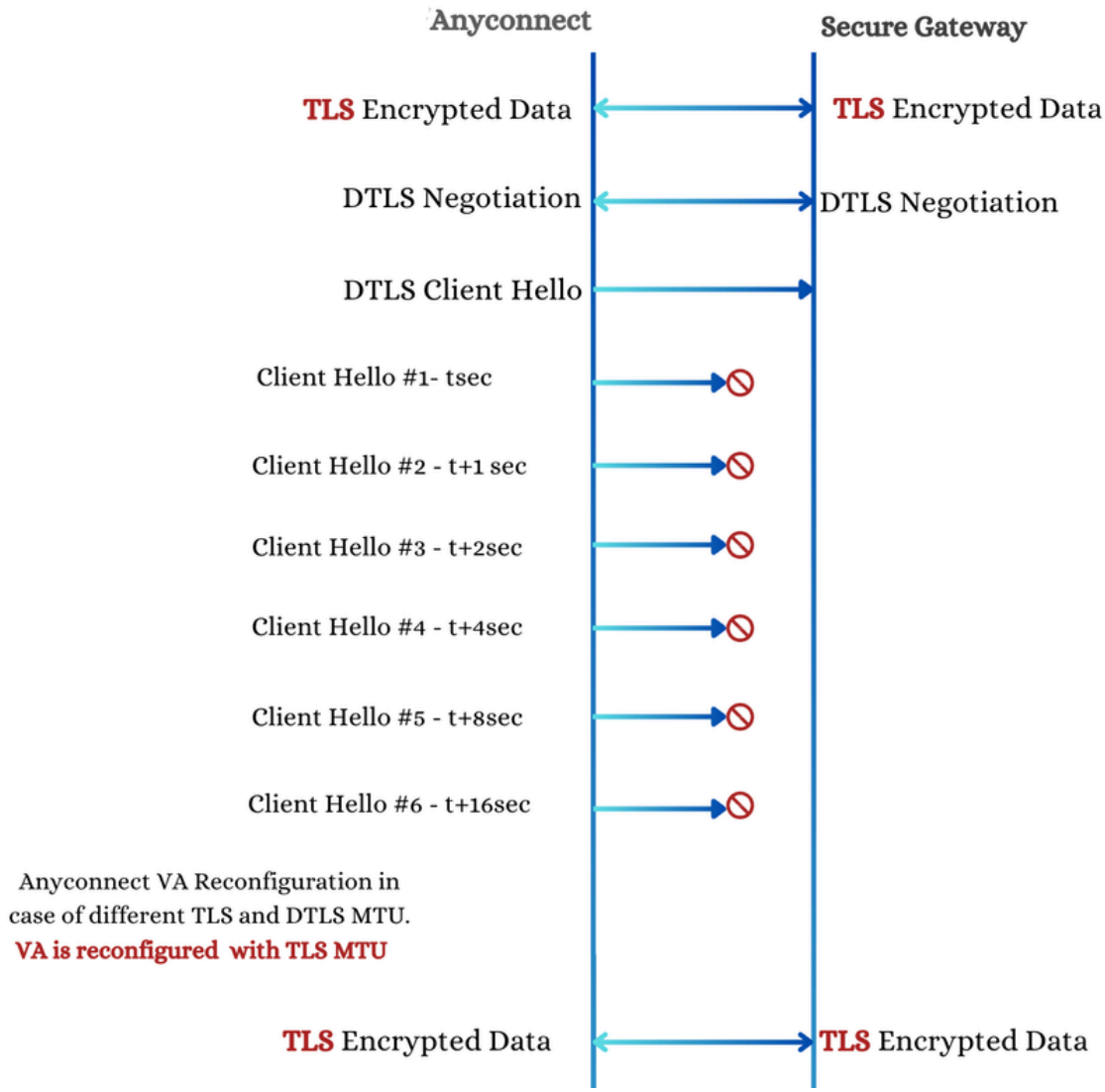


Handshake DTLS

6.1. Porta DTLS bloccata

Nel caso in cui la porta DTLS sia bloccata o il gateway sicuro non risponda ai pacchetti Hello del client DTLS, AnyConnect esegue un backoff esponenziale con un massimo di cinque tentativi, iniziando con un ritardo di 1 secondo e aumentando fino a 16 secondi.

Se il tentativo non riesce, AnyConnect applica l'MTU TLS effettiva, come specificato dal valore X-CSTP-MTU restituito dal gateway sicuro nella fase 5., alla scheda virtuale AnyConnect. Poiché questa MTU è diversa dalla MTU applicata in precedenza (X-DTLS-MTU), è necessaria una riconfigurazione della scheda virtuale. Questa riconfigurazione viene visualizzata all'utente finale come un tentativo di riconnessione, anche se durante questo processo non si verificano nuove negoziazioni. Dopo la riconfigurazione della scheda virtuale, il canale dati TLS continua a funzionare.



Blocco porta DTLS

Informazioni correlate

- Guida di riferimento alla documentazione delle tecnologie VPN Cisco
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).