Présentation du flux de connexion VPN SSL AnyConnect

Table des matières

Introduction

Ce document se concentre sur le flux des événements qui se produisent entre AnyConnect et la passerelle sécurisée pendant une connexion SSLVPN.

Informations générales

AnyConnect

AnyConnect est le client VPN Cisco conçu pour les protocoles SSL et IKEv2. Il est disponible pour la plupart des plates-formes de bureau et mobiles. AnyConnect établit principalement des connexions sécurisées avec les routeurs Firepower Threat Defense (FTD), Adaptive Security Appliances (ASA) ou Cisco IOS®/Cisco IOS® XE, appelés passerelles sécurisées.

Passerelle sécurisée

Dans la terminologie Cisco, un serveur VPN SSL est appelé passerelle sécurisée, tandis qu'un

serveur IPSec (IKEv2) est appelé passerelle VPN d'accès à distance. Cisco prend en charge la terminaison de tunnel VPN SSL sur ces plates-formes :

- Gammes Cisco ASA 5500 et 5500-X
- Cisco FTD (gammes 2100, 4100 et 9300)
- Cisco ISR 4000 et ISR G2
- Cisco CSR 1000
- Cisco Catalyst série 8000

Flux de connexion VPN SSL AnyConnect

Ce document présente les événements qui se produisent entre AnyConnect et Secure Gateway lors de l'établissement d'une connexion VPN SSL en six phases :

1. Connexion SSL

2. POST - Sélection des groupes

3. POST - Authentification utilisateur avec nom d'utilisateur/mot de passe (facultatif)

4. Téléchargeur VPN (facultatif)

5. CONNEXION CSTP

6. Connexion DTLS (facultatif)

1. Connexion SSL

La connexion SSL est initiée par le client AnyConnect après la fin de la connexion TCP en trois étapes avec un message « Client Hello ». Le déroulement des événements et les principales leçons à retenir sont tels que mentionnés.

Allô du client

La session SSL commence par l'envoi par le client d'un message « Client Hello ». Dans ce message :

a) L'ID de session SSL est défini sur 0, ce qui indique le lancement d'une nouvelle session.

b) La charge utile inclut les suites de chiffrement prises en charge par le client et une nonce aléatoire générée par le client.

Allô du serveur

Le serveur répond par un message « Server Hello », qui inclut :

a) La suite de chiffrement sélectionnée dans la liste fournie par le client.

b) Le serveur a généré l'ID de session SSL et un serveur a généré une fois aléatoire.

certificat du serveur

Après le « Server Hello », le serveur transmet son certificat SSL, qui sert d'identité. Points importants à noter :

a) Si ce certificat échoue à un contrôle de validation strict, AnyConnect bloque le serveur par défaut.

b) L'utilisateur a la possibilité de désactiver ce bloc, mais les connexions suivantes affichent un avertissement jusqu'à ce que les erreurs signalées soient résolues.

Demande de certificat client

Le serveur peut également demander un certificat client, en envoyant une liste de DN de noms d'objet de tous les certificats d'autorité de certification chargés sur la passerelle sécurisée. Cette demande a deux objectifs :

a) Il aide le client (utilisateur) à choisir le certificat d'identité correct si plusieurs certificats d'identité sont disponibles.

b) Garantit que le certificat renvoyé est approuvé par la passerelle sécurisée, même si une validation plus poussée du certificat doit encore avoir lieu.

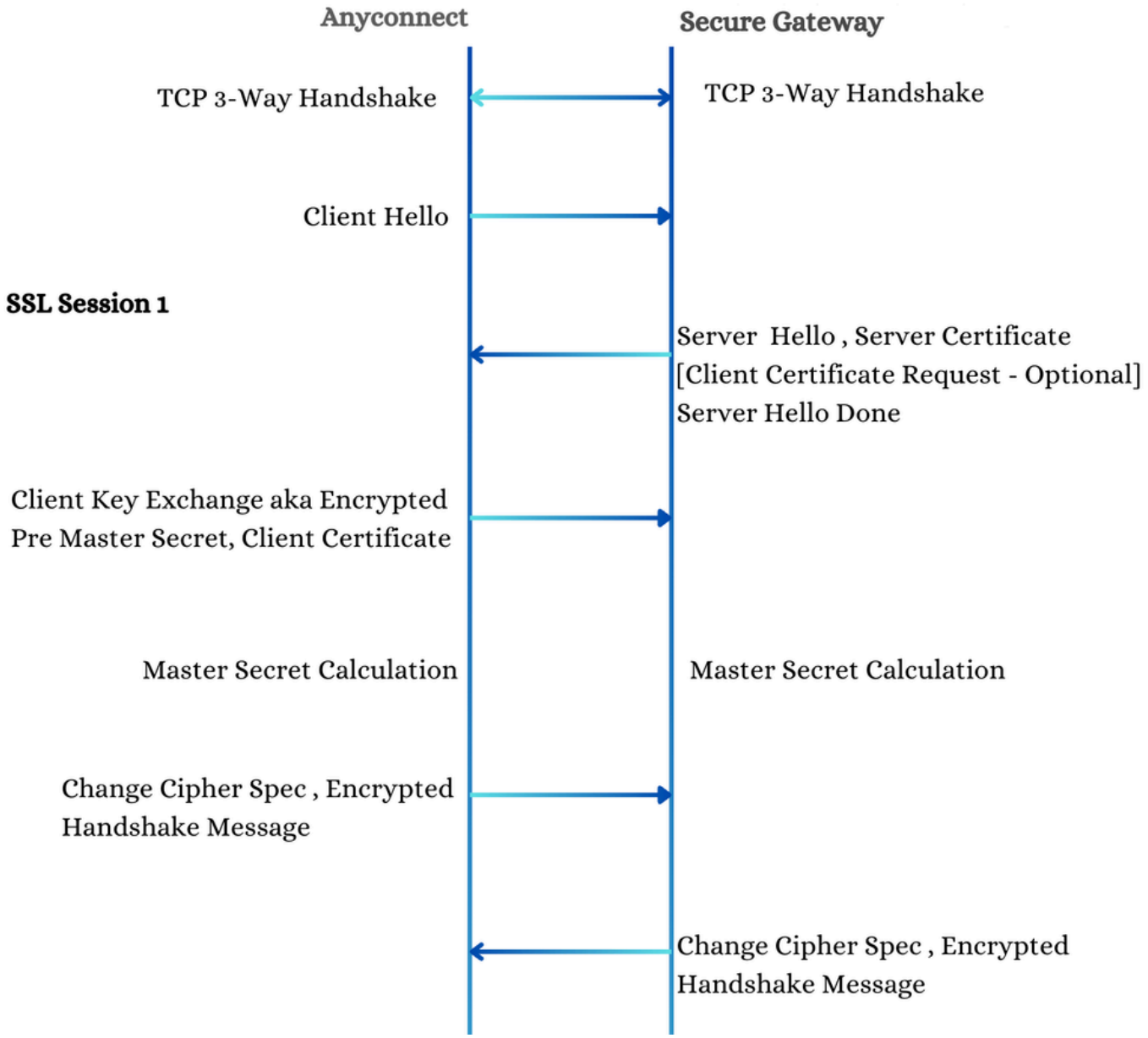
Échange de clés client

Le client envoie ensuite un message « Client Key Exchange », qui inclut une clé secrète pré-maître. Cette clé est chiffrée à l'aide de :

a) La clé publique du serveur du certificat du serveur, si la suite de chiffrement choisie est basée sur RSA (par exemple, TLS_RSA_WITH_AES_128_CBC_SHA).

b) La clé publique DH du serveur fournie dans le message Hello du serveur, si la suite de chiffrement choisie est basée sur DHE (par exemple, TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Sur la base du secret pré-maître, du nonce aléatoire généré par le client et du nonce aléatoire généré par le serveur, le client et la passerelle sécurisée génèrent indépendamment un secret maître. Ce secret principal est ensuite utilisé pour dériver les clés de session, assurant ainsi une communication sécurisée entre le client et le serveur.



Session SSL 1

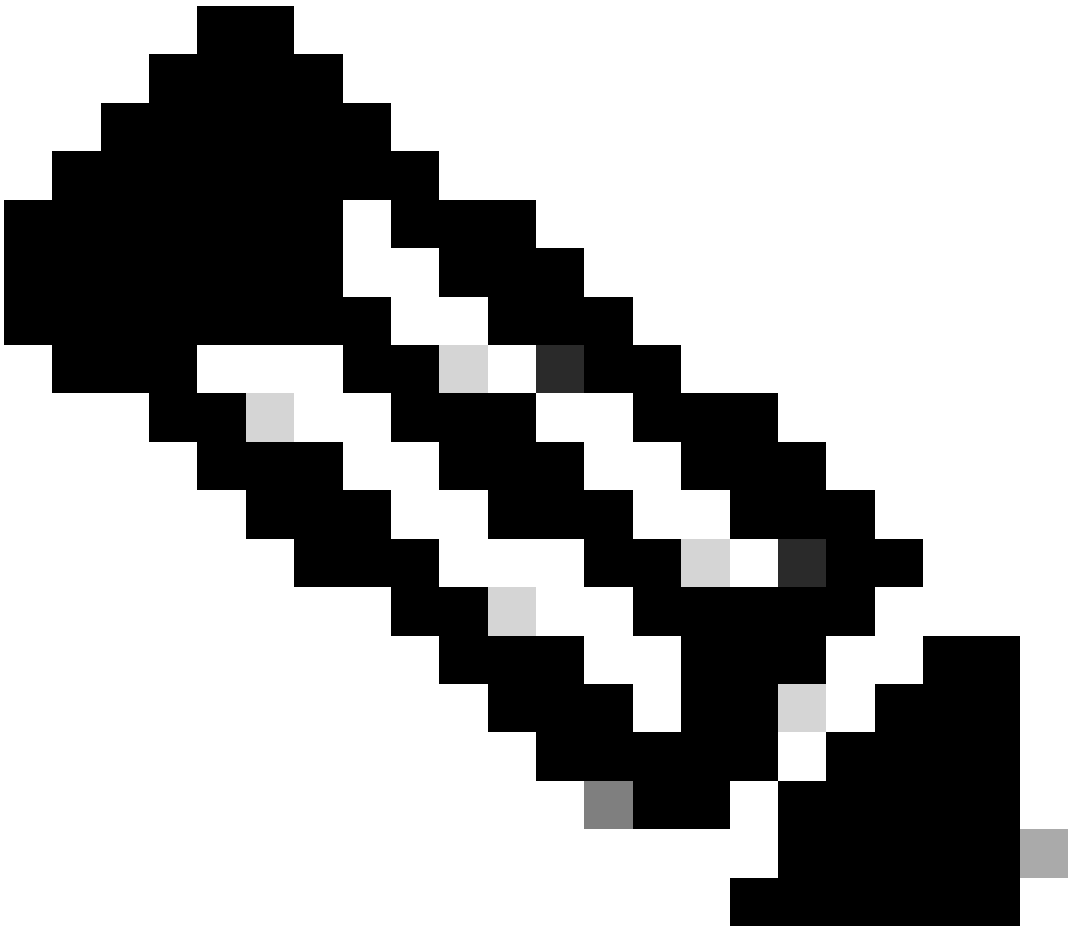
2. POST - Sélection de groupe

Au cours de cette opération, le client ne possède pas d'informations sur le profil de connexion, sauf indication explicite de l'utilisateur. La tentative de connexion est dirigée vers l'URL de la passerelle sécurisée (asav.cisco.com), comme indiqué par l'élément « group-access » dans la demande. Le client indique sa prise en charge de l'authentification d'agrégation version 2. Cette version représente une amélioration significative par rapport à la version précédente, notamment en termes d'efficacité des transactions XML. La passerelle sécurisée et le client doivent s'entendre sur la version à utiliser. Dans les cas où la passerelle sécurisée ne prend pas en charge la version 2, une opération POST supplémentaire est déclenchée, entraînant le retour du client à la version 2.

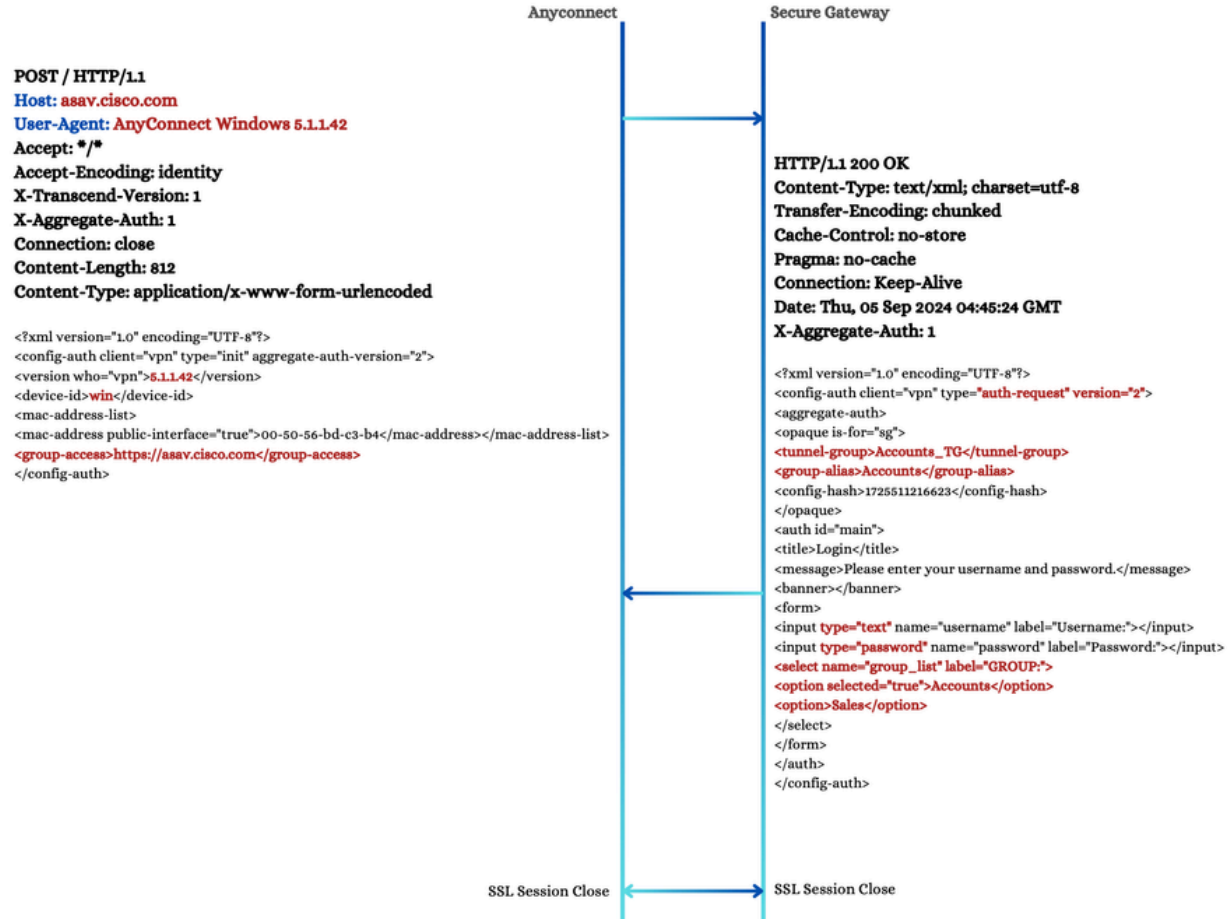
Dans la réponse HTTP, la passerelle sécurisée indique les éléments suivants :

1. Version de l'authentification agrégée prise en charge par la passerelle sécurisée.

2. Liste des groupes de tunnels et formulaire Nom d'utilisateur/Mot de passe.

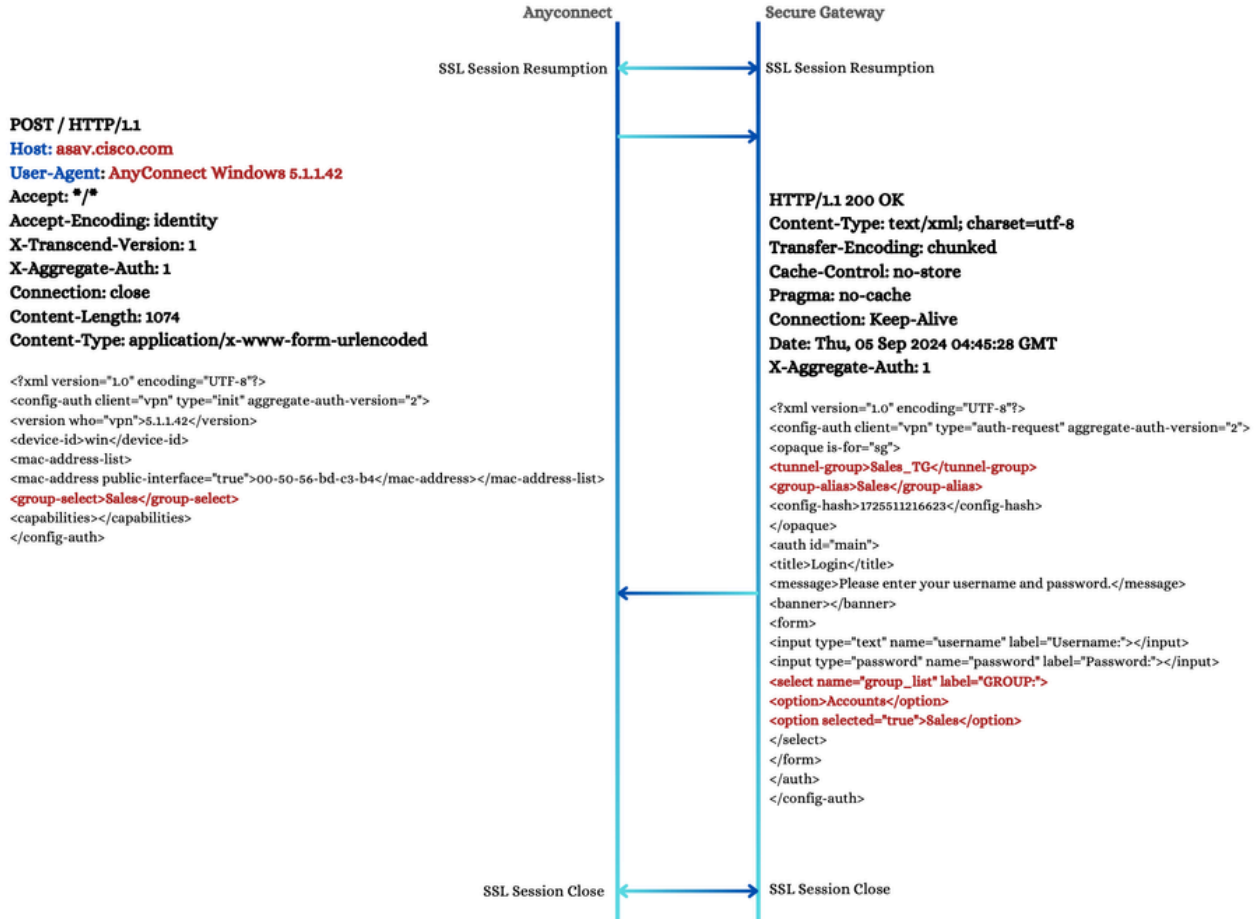


Remarque : le formulaire inclut un élément « select » qui répertorie les alias de groupe de tous les profils de connexion configurés sur la passerelle sécurisée. Par défaut, l'un de ces alias de groupe est mis en surbrillance avec l'attribut booléen = "true" sélectionné. Les éléments tunnel-group et group-alias correspondent à ce profil de connexion choisi.



POST - Sélection de groupe 1

Si l'utilisateur choisit un profil de connexion différent dans cette liste, une autre opération POST a lieu. Dans ce cas, le client envoie une requête POST avec l'élément « group-select » mis à jour afin de refléter le profil de connexion choisi, comme illustré ici.



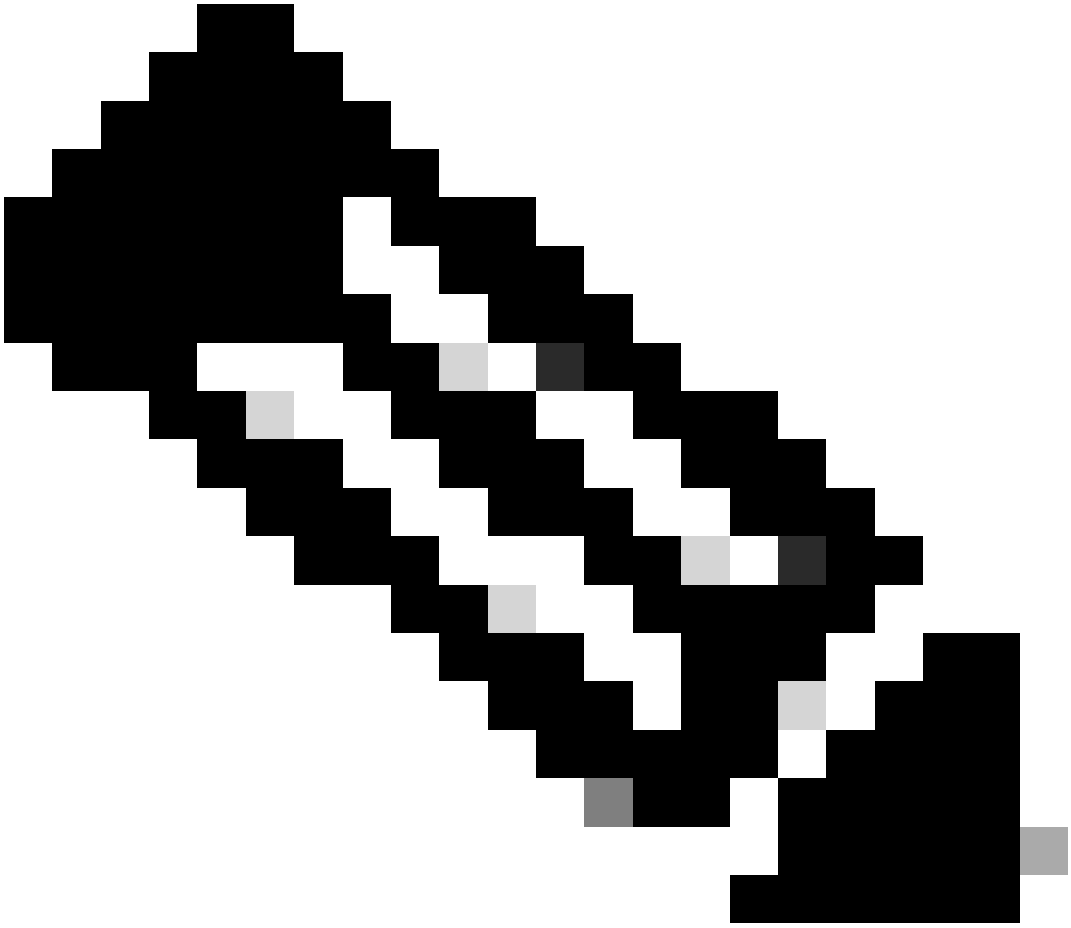
POST - Sélection de groupe 2

3. POST - Authentification utilisateur

Dans cette opération, qui suit la sélection du groupe POST, AnyConnect envoie ces informations à la passerelle sécurisée :

1. Information de profil de connexion sélectionnée : inclut le nom du groupe de tunnels et l'alias du groupe, comme indiqué par la passerelle sécurisée lors de l'opération précédente.

2. Nom d'utilisateur et mot de passe : identifiants d'authentification de l'utilisateur.



Remarque : ce flux étant spécifique à l'authentification AAA, il peut différer des autres méthodes d'authentification.

En réponse à l'opération POST, la passerelle sécurisée envoie un fichier XML contenant ces informations :

1. ID de session : différent de l'ID de session SSL.

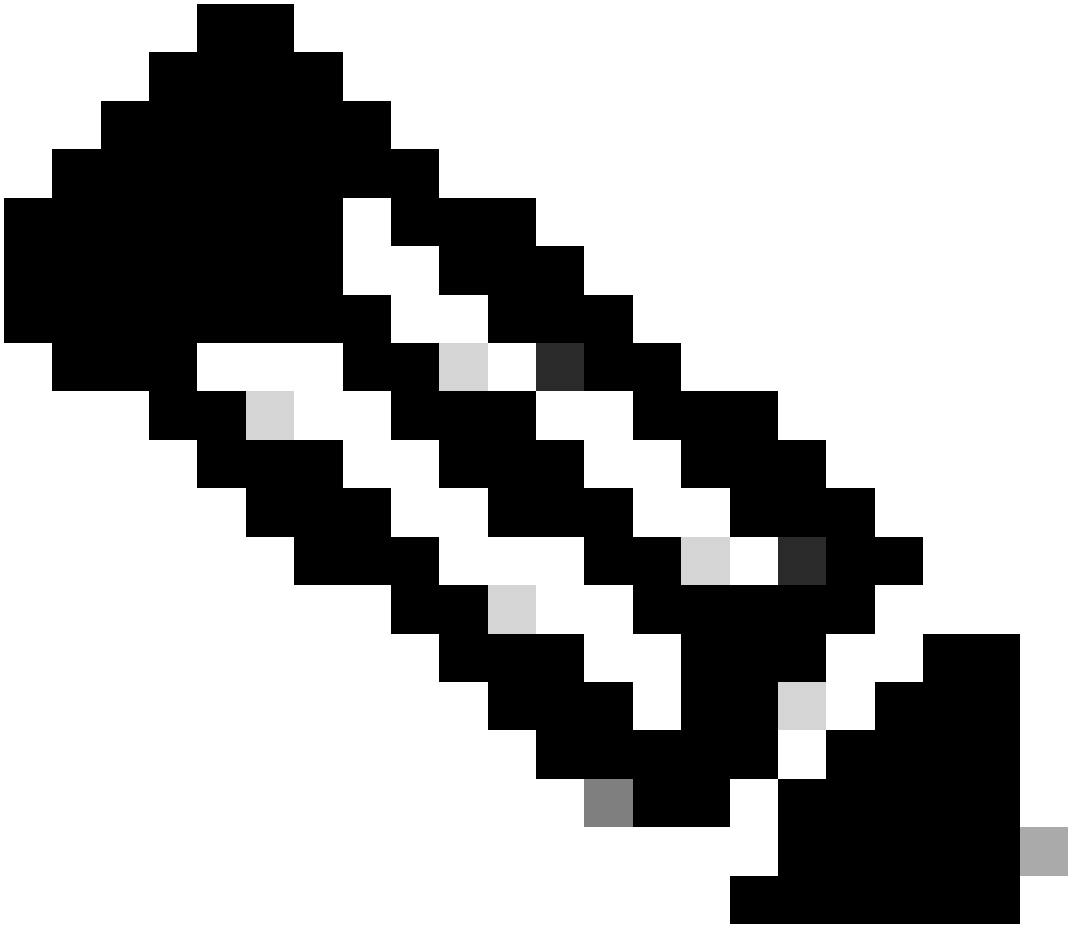
2. Jeton de session : ce jeton est utilisé par la suite par le client comme cookie WebVPN.

3. État de l'authentification : indiqué par un élément auth avec id = 'success'.

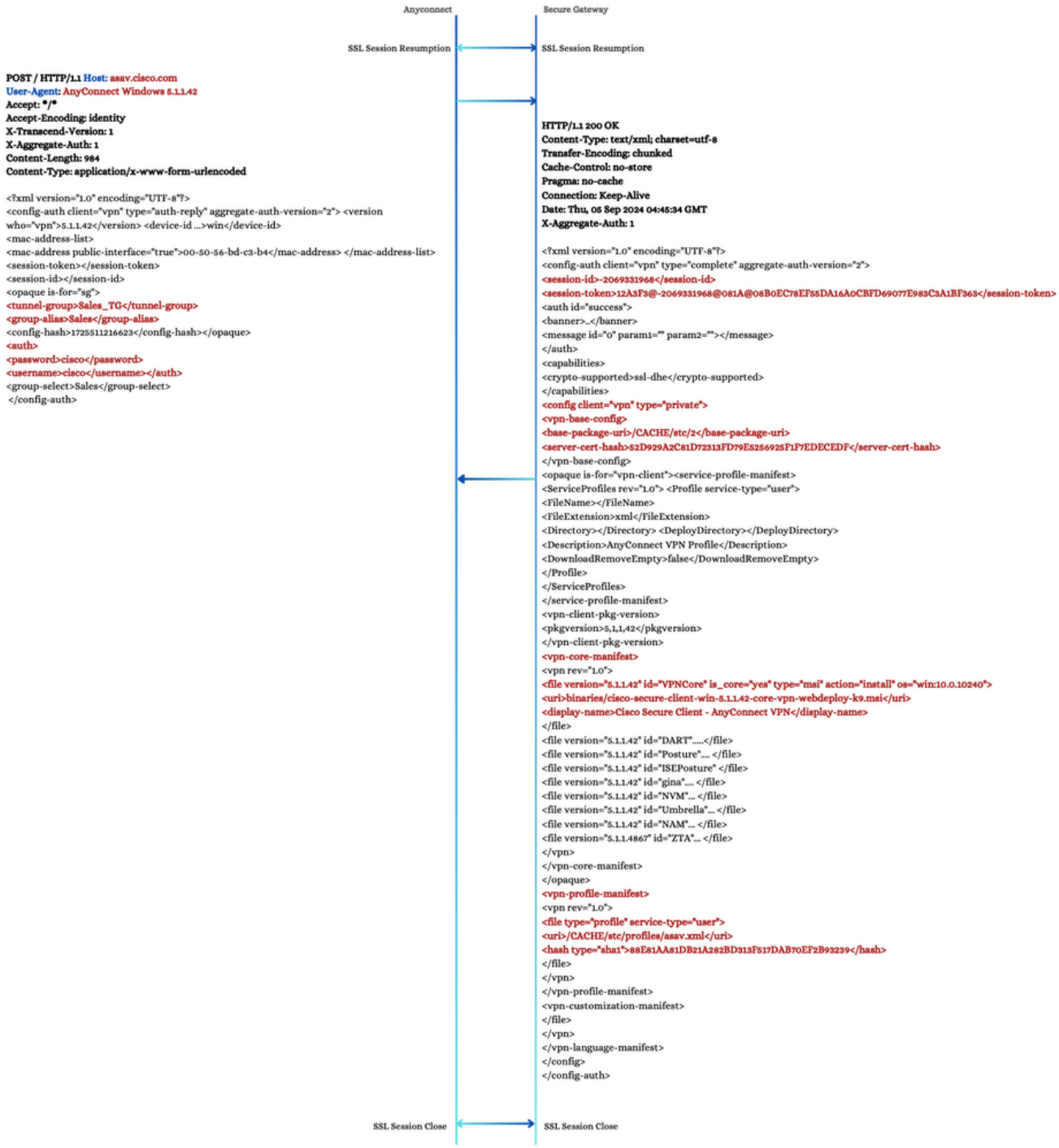
4. Hachage du certificat de serveur : ce hachage est mis en cache dans le fichier préférences.xml.

5. vpn-core-manifest Element : cet élément indique le chemin d'accès et la version du package principal AnyConnect, ainsi que d'autres composants tels que Dart, Posture, ISE Posture, etc. Il est utilisé par le téléchargeur VPN dans la section suivante.

6. vpn-profile-manifest Element : cet élément indique le chemin (le nom du profil) et le hachage SHA-1 du profil.



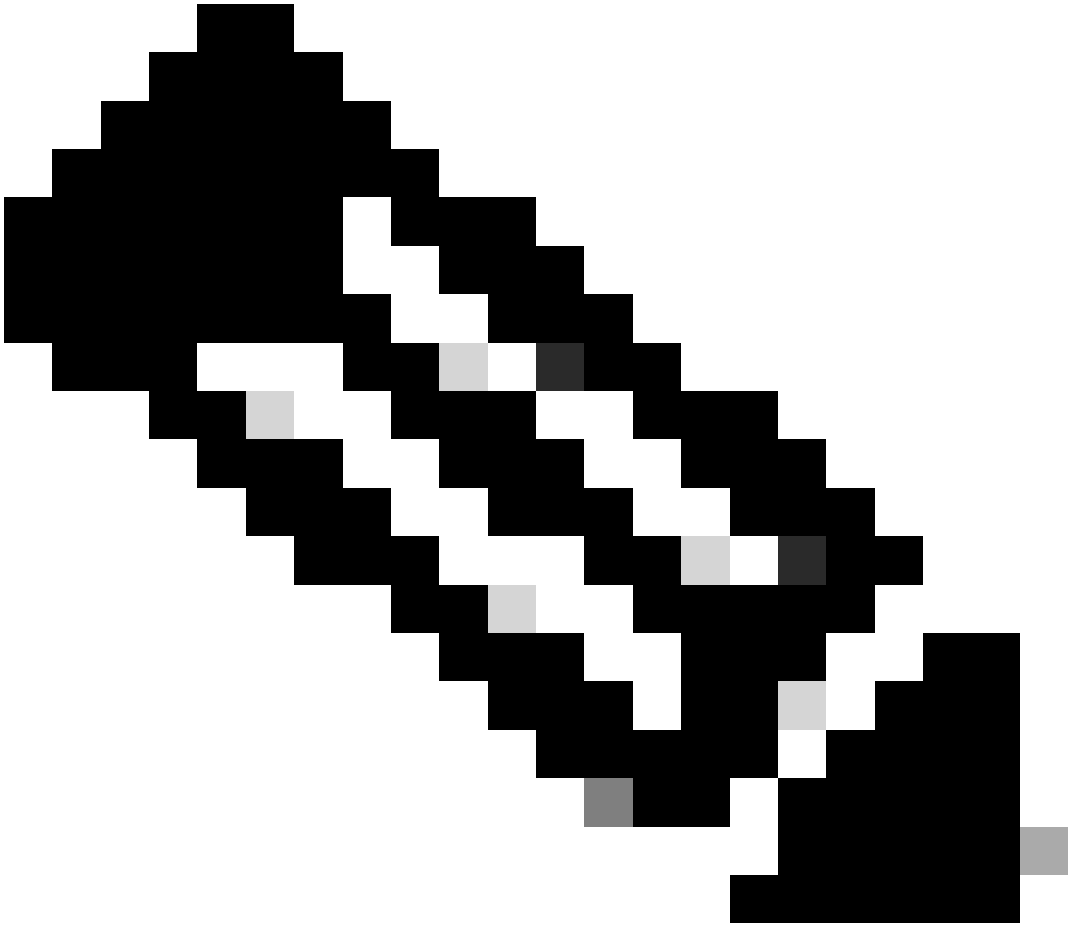
Remarque : si le client n'a pas le profil, le téléchargeur VPN de la section suivante le télécharge. Si le client possède déjà le profil, le hachage SHA-1 du profil client est comparé à celui du serveur. En cas de non-correspondance, le téléchargeur VPN remplace le profil client par celui de la passerelle sécurisée. Cela garantit que le profil de la passerelle sécurisée est appliqué au client après l'authentification.



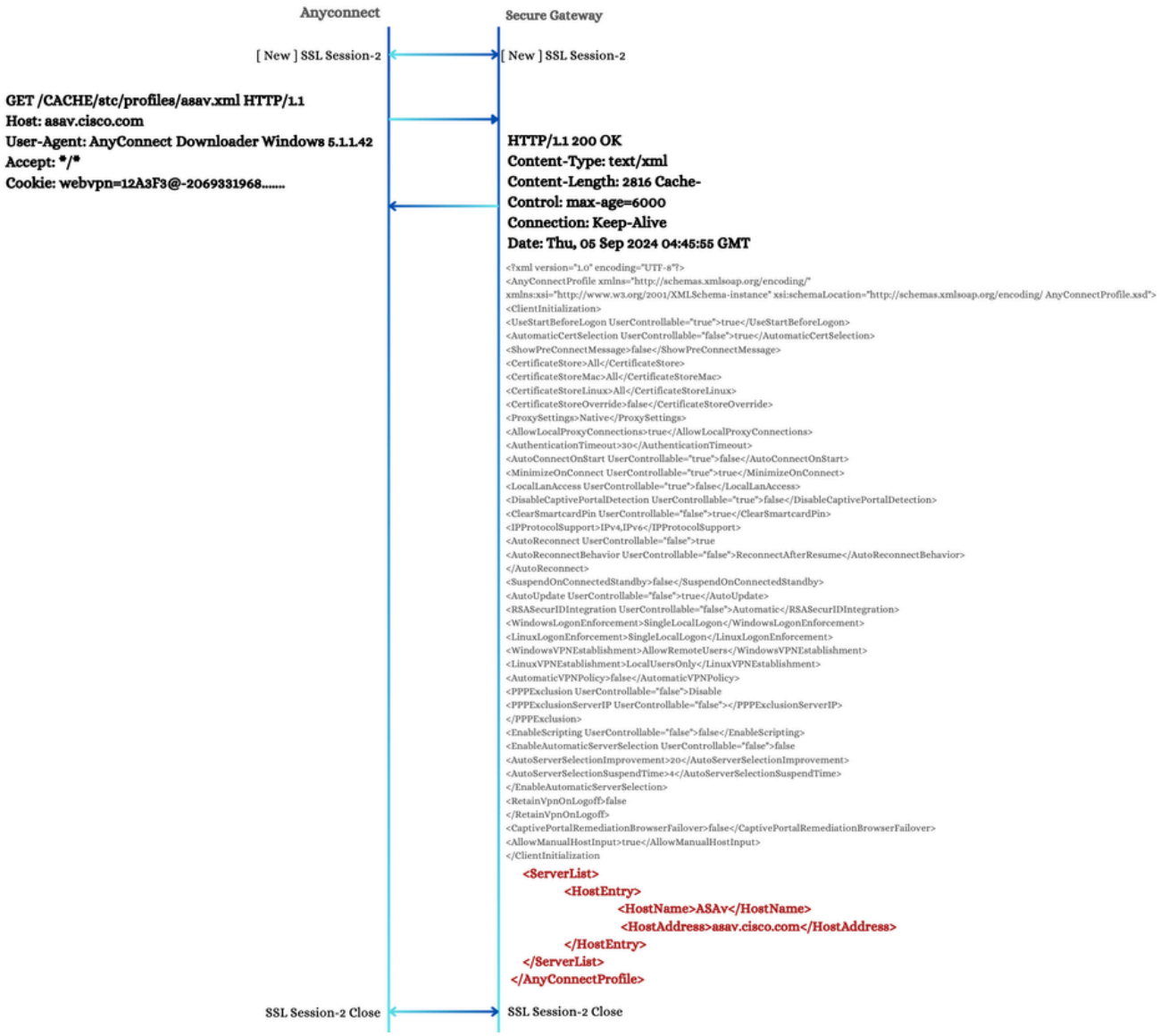
POST - Authentification utilisateur

4. Téléchargeur AnyConnect

AnyConnect Downloader lance toujours une nouvelle session SSL, ce qui explique pourquoi les utilisateurs peuvent rencontrer un deuxième avertissement de certificat si le certificat de la passerelle sécurisée n'est pas approuvé. Au cours de cette phase, il effectue des opérations GET distinctes pour chaque élément à télécharger.



Remarque : si le profil client est chargé sur Secure Gateway, il est obligatoire pour le téléchargement ; sinon, la tentative de connexion est terminée.

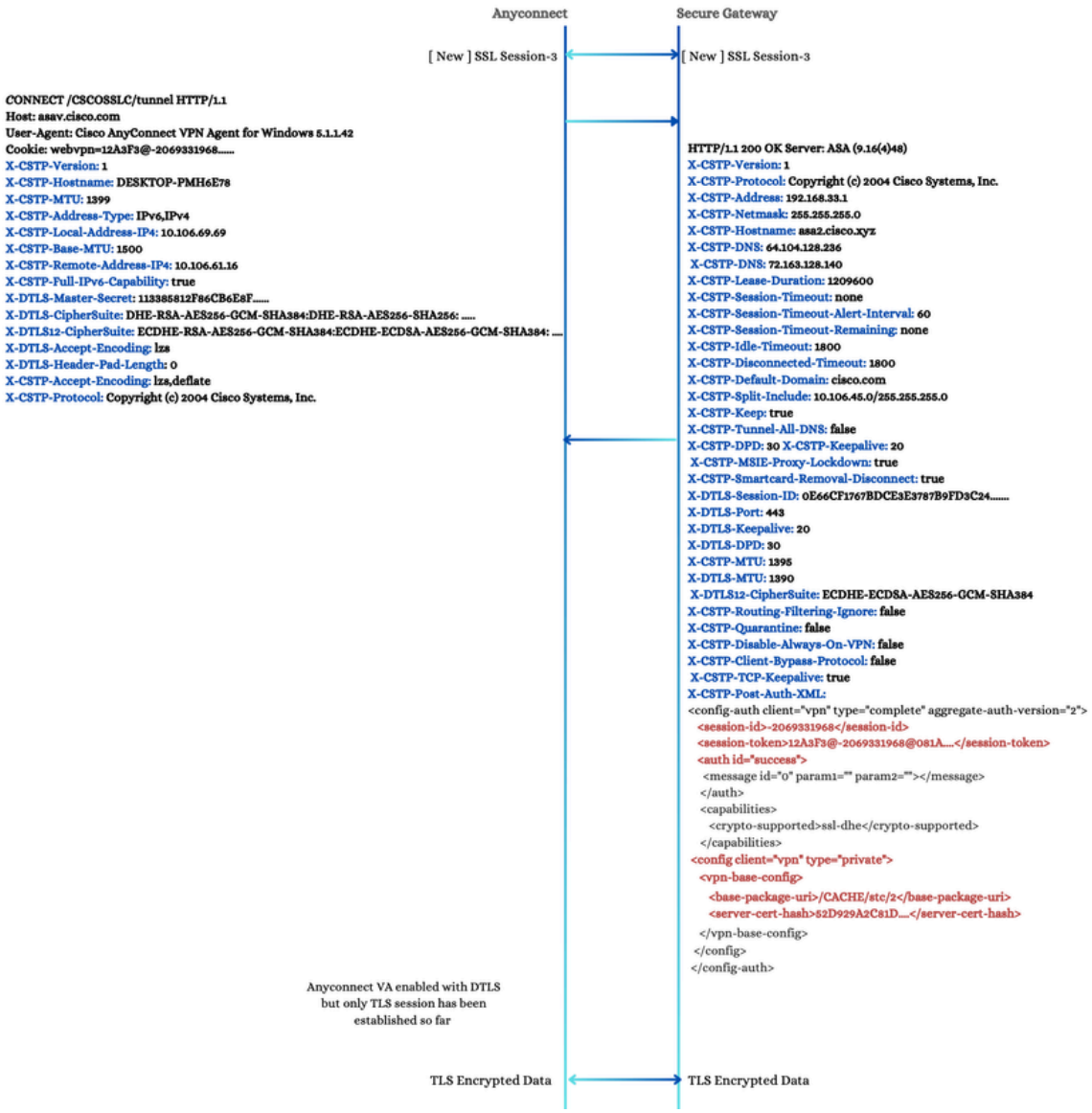


Téléchargeur VPN

5. CONNEXION CSTP

AnyConnect effectue une opération CONNECT comme dernière étape de l'établissement d'un canal sécurisé. Au cours de l'opération CONNECT, le client AnyConnect envoie divers attributs X-CSTP et X-DTLS pour la passerelle sécurisée afin de les traiter. La passerelle sécurisée répond avec des attributs X-CSTP et X-DTLS supplémentaires que le client applique à la tentative de connexion en cours. Cet échange inclut le X-CSTP-Post-Auth-XML, accompagné d'un fichier XML, qui est largement similaire à celui vu dans l'étape POST - User Authentication.

Une fois la réponse reçue, AnyConnect lance le canal de données TLS. Simultanément, l'interface de la carte virtuelle AnyConnect est activée avec une valeur MTU égale à X-DTLS-MTU, en supposant que la connexion DTLS suivante est réussie.



Connexion CSTP

6. Connexion DTLS

La connexion DTLS se poursuit comme indiqué ici. Cette configuration est relativement rapide en raison des attributs échangés entre le client et le serveur lors de l'événement CONNECT.

Client

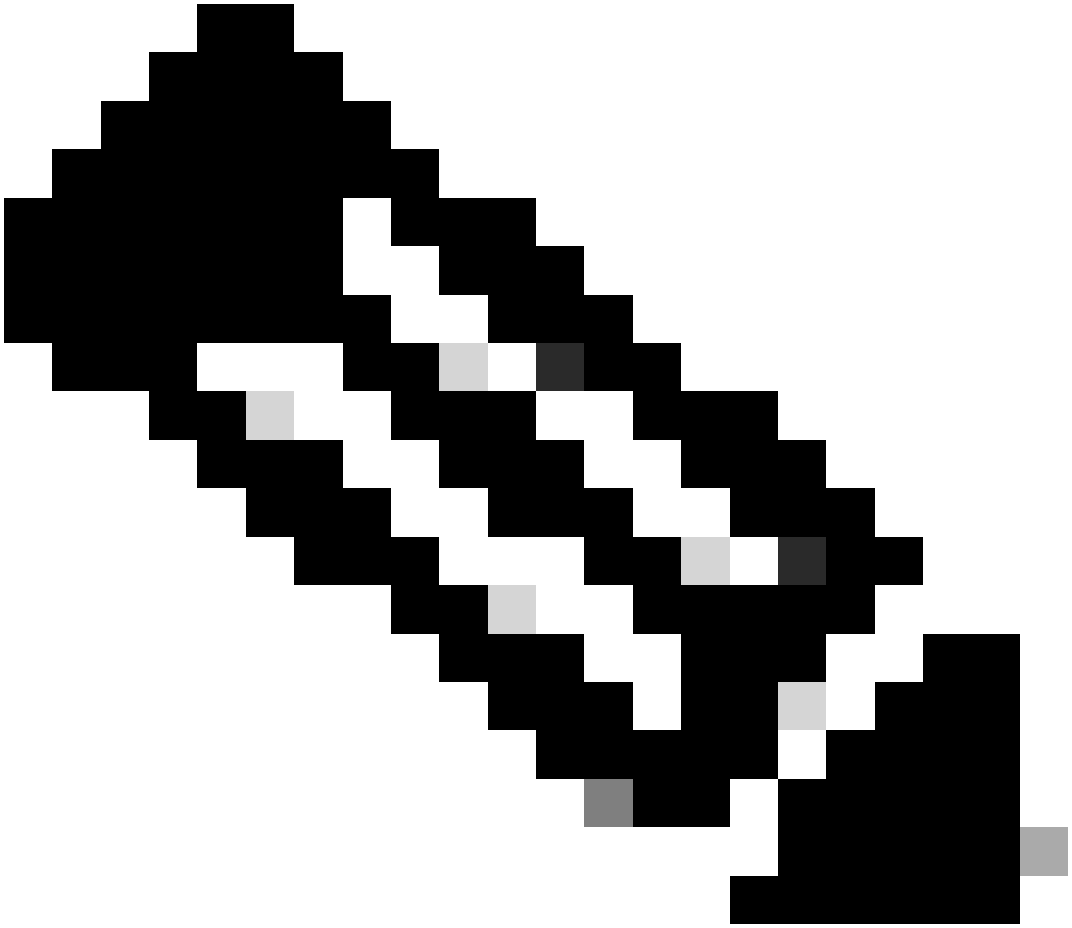
X-DTLS-Master-Secret : le mot de passe DTLS Master Secret est généré par le client et partagé avec le serveur. Cette clé est essentielle pour établir une session DTLS sécurisée.

X-DTLS-CipherSuite : liste des suites de chiffrement DTLS prises en charge par le client, indiquant les capacités de chiffrement du client.

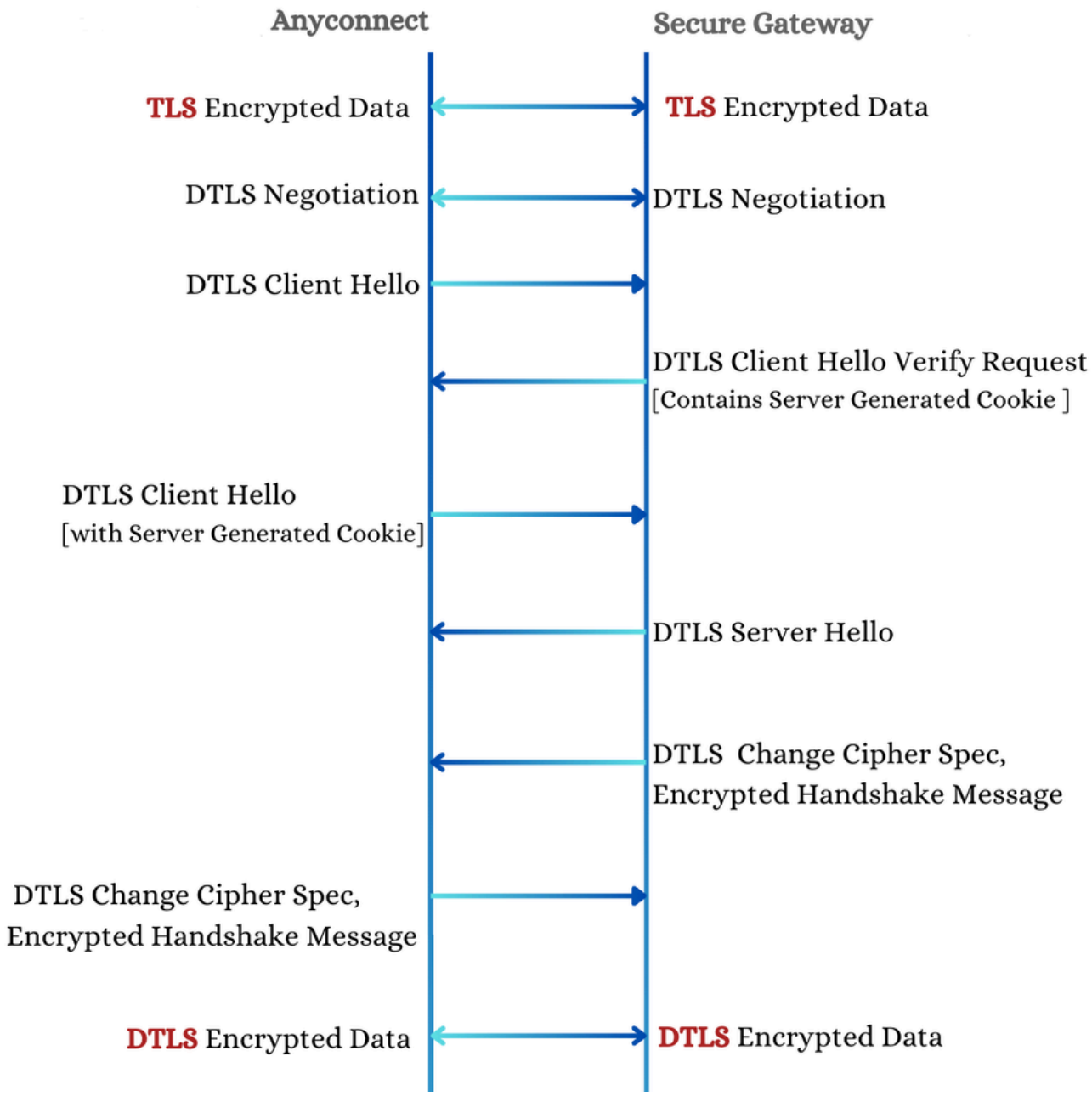
Serveur

X-DTLS-Session-ID : ID de session DTLS attribué par le serveur au client, assurant ainsi la continuité de la session.

X-DTLS-CipherSuite : suite de chiffrement sélectionnée par le serveur à partir de la liste fournie par le client, en s'assurant que les deux parties utilisent une méthode de chiffrement compatible.



Remarque : pendant que la connexion DTLS est en cours, le canal de données TLS continue à fonctionner. Cela garantit que la transmission des données reste cohérente et sécurisée pendant le processus d'échange. Une transition transparente vers le canal de cryptage de données DTLS ne se produit qu'une fois la connexion DTLS terminée.

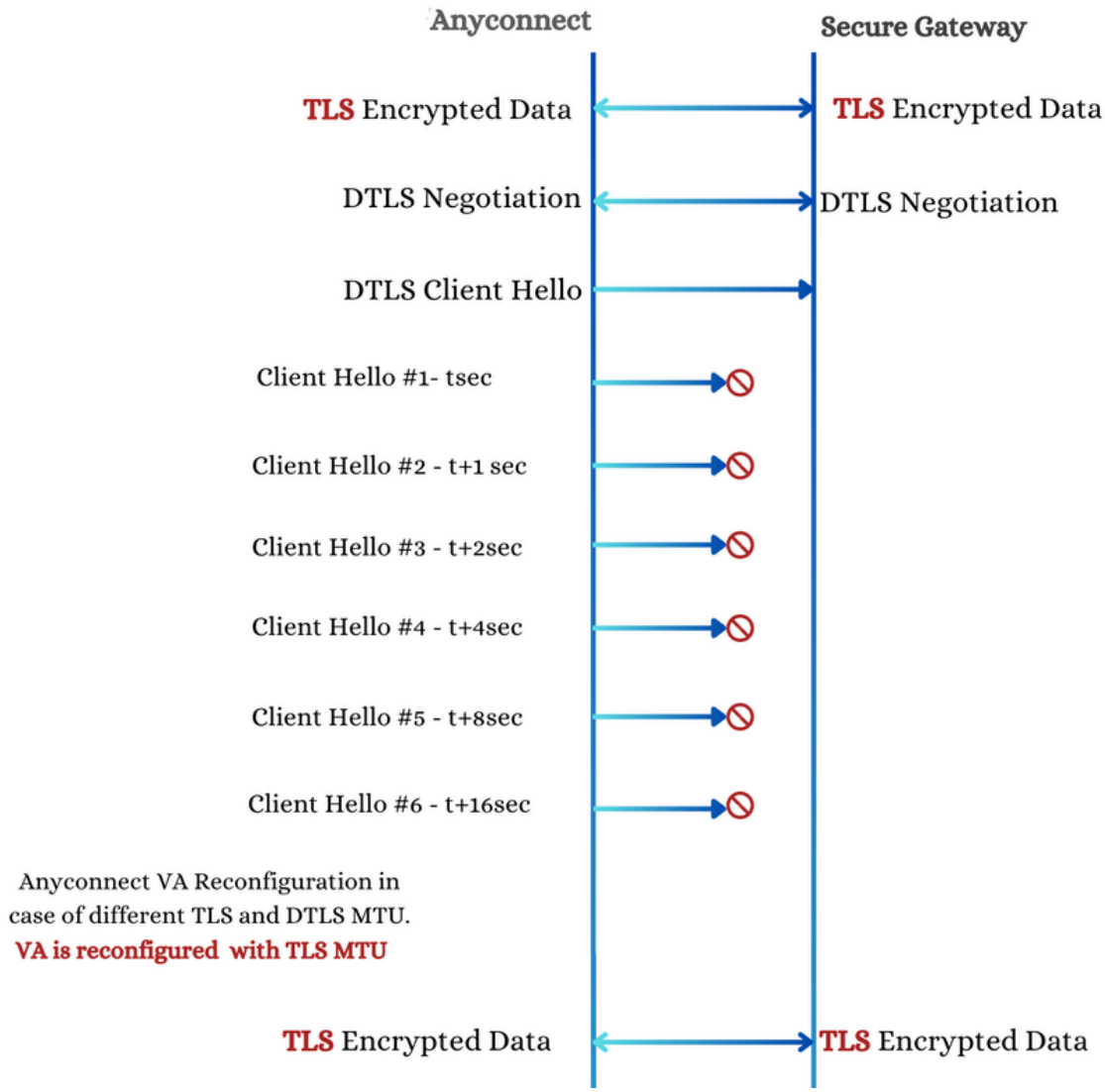


Connexion DTLS

6.1. Port DTLS bloqué

Si le port DTLS est bloqué ou si la passerelle sécurisée ne répond pas aux paquets Hello du client DTLS, AnyConnect effectue une réémission temporisée exponentielle avec un maximum de cinq tentatives, en commençant par un délai d'une seconde et en augmentant jusqu'à 16 secondes.

Si ces tentatives échouent, AnyConnect applique alors la MTU TLS réelle, telle que spécifiée par la valeur X-CSTP-MTU retournée par la passerelle sécurisée dans Phase 5., à la carte virtuelle AnyConnect. Étant donné que cette MTU diffère de la MTU précédemment appliquée (X-DTLS-MTU), une reconfiguration de la carte virtuelle est nécessaire. Cette reconfiguration apparaît à l'utilisateur final comme une tentative de reconnexion, bien qu'aucune nouvelle négociation n'ait lieu au cours de ce processus. Une fois la carte virtuelle reconfigurée, le canal de données TLS continue de fonctionner.



Bloc de ports DTLS

Informations connexes

- Référence de documentation des technologies VPN Cisco
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.