Überblick über den AnyConnect SSL VPN-Verbindungsverlauf

Inhalt

Einleitung

Das vorliegende Dokument beschreibt den Fluss von Ereignissen zwischen AnyConnect und dem sicheren Gateway während einer SSL VPN-Verbindung.

Hintergrundinformationen

AnyConnect

AnyConnect ist der Cisco VPN-Client für SSL- und IKEv2-Protokolle. Es ist für die meisten Desktop- und mobilen Plattformen verfügbar. AnyConnect stellt in erster Linie sichere Verbindungen mit Firepower Threat Defense (FTD), Adaptive Security Appliances (ASA) oder Cisco IOS®/Cisco IOS® XE-Routern her, die als Secure Gateways bezeichnet werden.

Sicheres Gateway

In der Terminologie von Cisco wird ein SSL VPN-Server als sicheres Gateway bezeichnet,

während ein IPSec (IKEv2)-Server als Remote Access VPN Gateway bezeichnet wird. Cisco unterstützt die Terminierung von SSL-VPN-Tunneln auf folgenden Plattformen:

- Cisco Serien ASA 5500 und 5500-X
- Cisco FTD (Serien 2100, 4100 und 9300)
- Cisco ISR der Serien 4000 und ISR G2
- Cisco Serie CSR 1000
- Switches der Cisco Catalyst 8000-Serie

AnyConnect SSL VPN-Verbindungsablauf

In diesem Dokument werden die Ereignisse zwischen AnyConnect und dem Secure Gateway bei der Herstellung einer SSL VPN-Verbindung in sechs Phasen unterteilt:

1. SSL-Handshake

2. POST - Gruppenauswahl

3. POST - Benutzerauthentifizierung mit Benutzername/Kennwort (optional)

4. VPN-Downloader (optional)

5. CSTP-VERBINDUNG

6. DTLS-Verbindung (optional)

1. SSL-Handshake

Der SSL-Handshake wird vom AnyConnect-Client initiiert, nachdem der TCP-3-Wege-Handshake mit der Meldung "Client Hello" abgeschlossen wurde. Der Ablauf der Ereignisse und die wichtigsten Erkenntnisse sind wie erwähnt.

Client-Hello

Die SSL-Sitzung beginnt, indem der Client eine 'Client Hello'-Nachricht sendet. In dieser Nachricht:

a) Die SSL-Sitzungs-ID ist auf 0 gesetzt, was auf die Initiierung einer neuen Sitzung hinweist.

b) Die Nutzlast umfasst die vom Client unterstützten Verschlüsselungssuiten und einen vom Client generierten Zufallsgenerator.

Server-Hello

Der Server antwortet mit einer "Server Hello"-Nachricht, die Folgendes enthält:

a) Die ausgewählte Verschlüsselungssuite aus der vom Client bereitgestellten Liste.

b) Der Server hat die SSL-Sitzungs-ID generiert, und ein Server hat einmal einen Zufallsgenerator generiert.

Serverzertifikat

Nach dem 'Server Hello' überträgt der Server sein SSL-Zertifikat, das als Identität dient. Zu den wichtigsten Punkten gehören:

a) Wenn dieses Zertifikat einer strengen Validierungsprüfung nicht standhält, blockiert AnyConnect den Server standardmäßig.

b) Der Benutzer kann diesen Block deaktivieren, aber nachfolgende Verbindungen zeigen eine Warnung an, bis die gemeldeten Fehler behoben sind.

Clientzertifikatanforderung

Der Server kann auch ein Clientzertifikat anfordern und eine Liste der DNs des Antragstellernamens aller Zertifizierungsstellenzertifikate senden, die auf das sichere Gateway geladen wurden. Diese Anforderung hat zwei Zwecke:

a) Er unterstützt den Client (Benutzer) bei der Auswahl des richtigen Identitätszertifikats, wenn mehrere ID-Zertifikate verfügbar sind.

b) Stellt sicher, dass das zurückgegebene Zertifikat vom sicheren Gateway als vertrauenswürdig eingestuft wird. Eine weitere Zertifikatvalidierung muss jedoch weiterhin erfolgen.

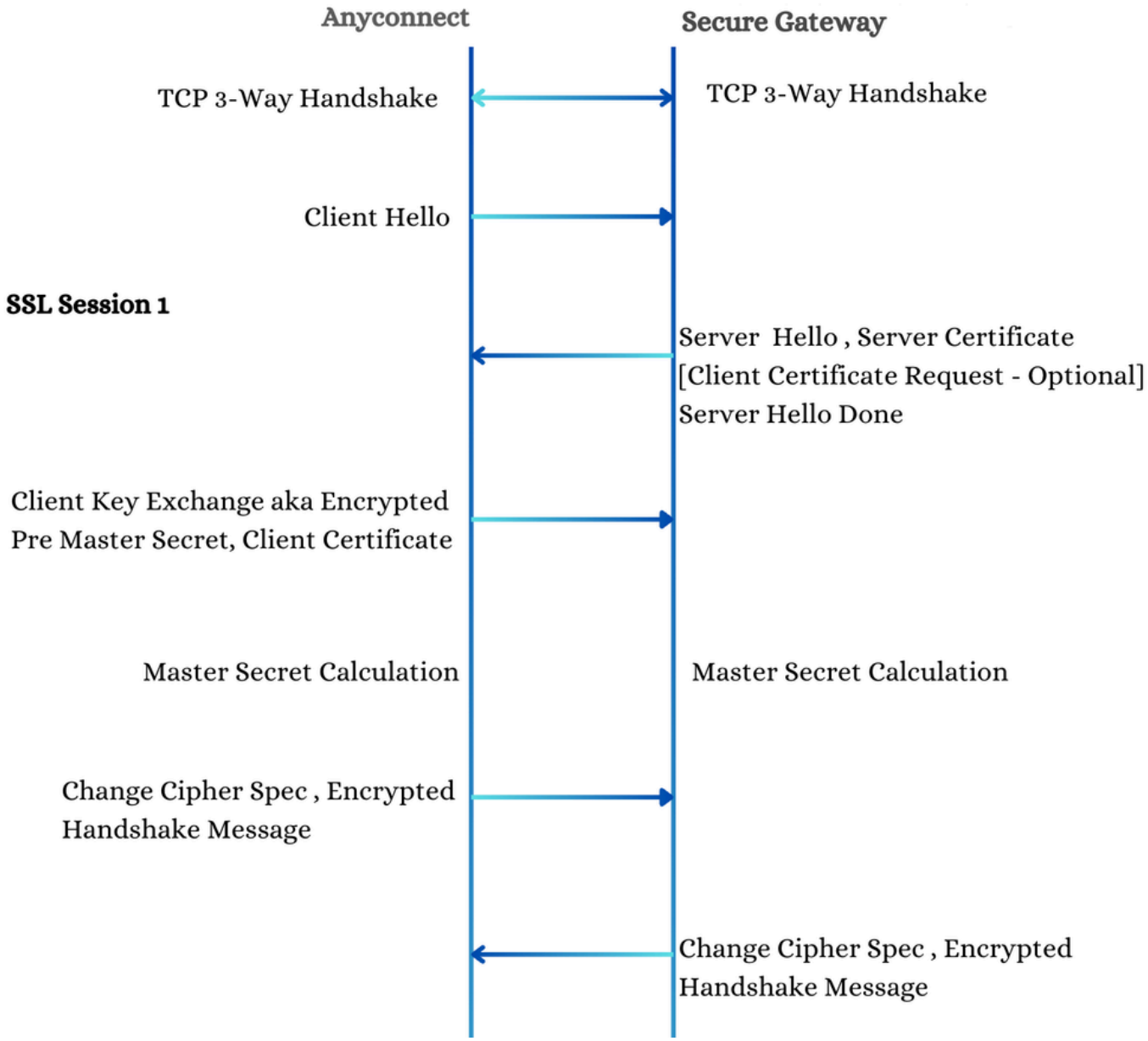
Client-Schlüsselaustausch

Der Client sendet dann eine 'Client Key Exchange'-Nachricht, die einen geheimen Pre-Master-Schlüssel enthält. Dieser Schlüssel wird verschlüsselt mit:

a) Der öffentliche Schlüssel des Servers aus dem Serverzertifikat, wenn die ausgewählte Verschlüsselungs-Suite RSA-basiert ist (z. B. TLS_RSA_WITH_AES_128_CBC_SHA).

b) Der öffentliche DH-Schlüssel des Servers, der in der Server Hello-Nachricht angegeben wird, wenn die ausgewählte Verschlüsselungs-Suite auf DHE basiert (z. B. TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Sowohl der Client als auch das Secure Gateway generieren auf Basis des Pre-Master-Geheimnisses, des vom Client generierten Zufallszählers und des vom Server generierten Zufallszählers unabhängig voneinander ein Master-Geheimnis. Dieser geheime Hauptschlüssel wird dann zur Ableitung von Sitzungsschlüsseln verwendet, um eine sichere Kommunikation zwischen dem Client und dem Server zu gewährleisten.



SSL-Sitzung 1

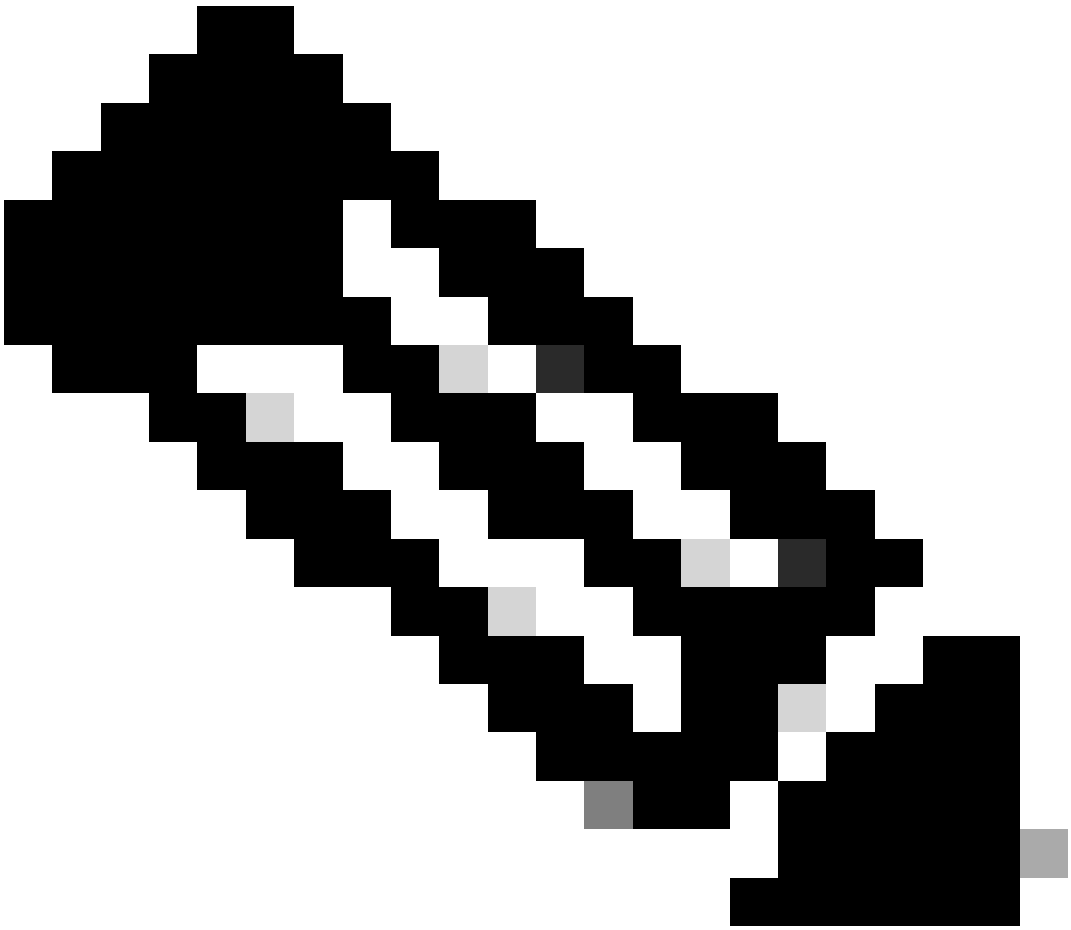
2. POST - Gruppenauswahl

Während dieses Vorgangs besitzt der Client keine Informationen über das Verbindungsprofil, es sei denn, der Benutzer gibt diese explizit an. Der Verbindungsversuch wird an die Secure Gateway-URL (asav.cisco.com) weitergeleitet, wie durch das Element "group-access" in der Anforderung angegeben. Der Client gibt seine Unterstützung für "aggregate-authentication" Version 2 an. Diese Version stellt eine erhebliche Verbesserung gegenüber der früheren Version dar, insbesondere im Hinblick auf effiziente XML-Transaktionen. Sowohl das sichere Gateway als auch der Client müssen sich auf die zu verwendende Version einigen. In Szenarien, in denen das sichere Gateway Version 2 nicht unterstützt, wird ein zusätzlicher POST-Vorgang ausgelöst, wodurch der Client auf die Version zurückgreift.

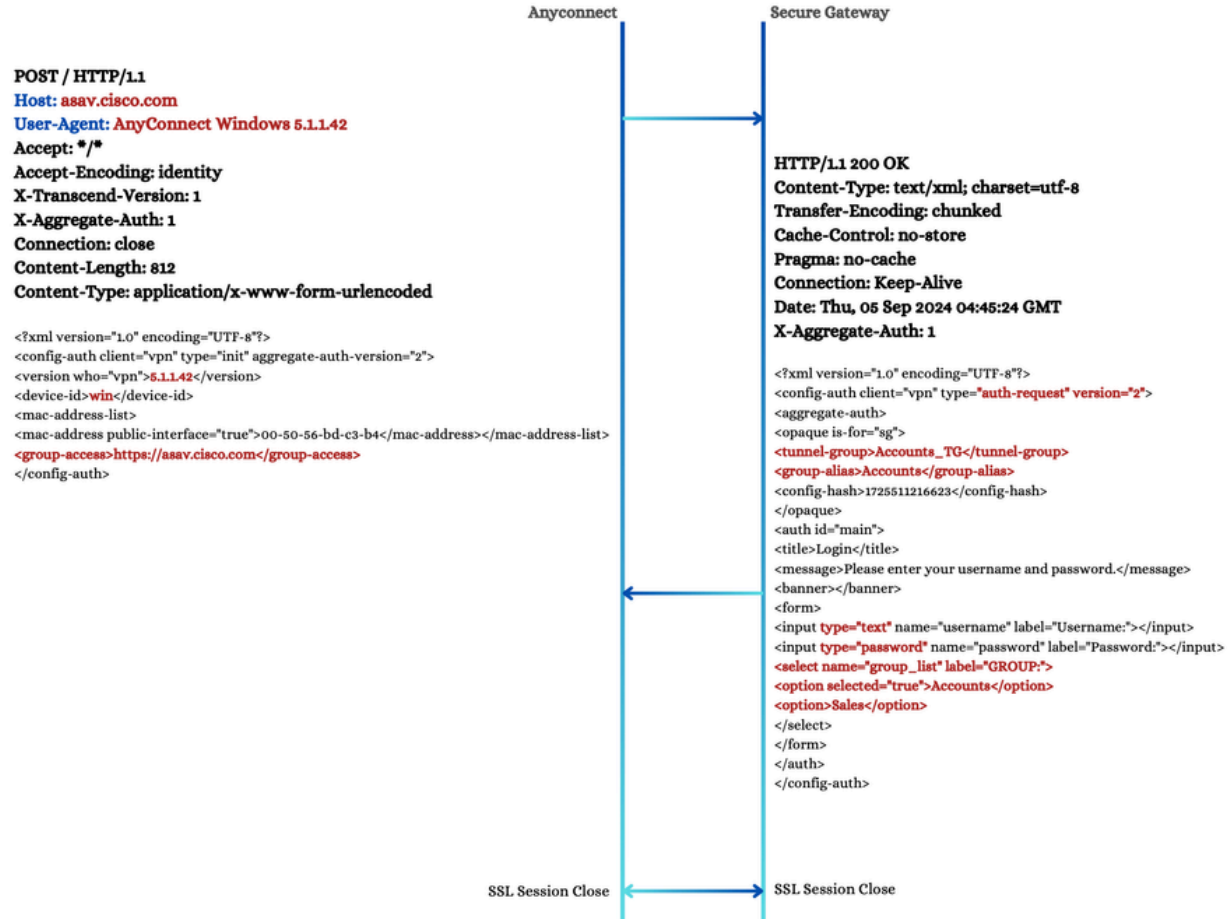
In der HTTP-Antwort gibt das sichere Gateway Folgendes an:

1. Die vom sicheren Gateway unterstützte Version der Aggregatauthentifizierung.

2. Tunnelgruppenliste und das Benutzername/Passwort-Formular.

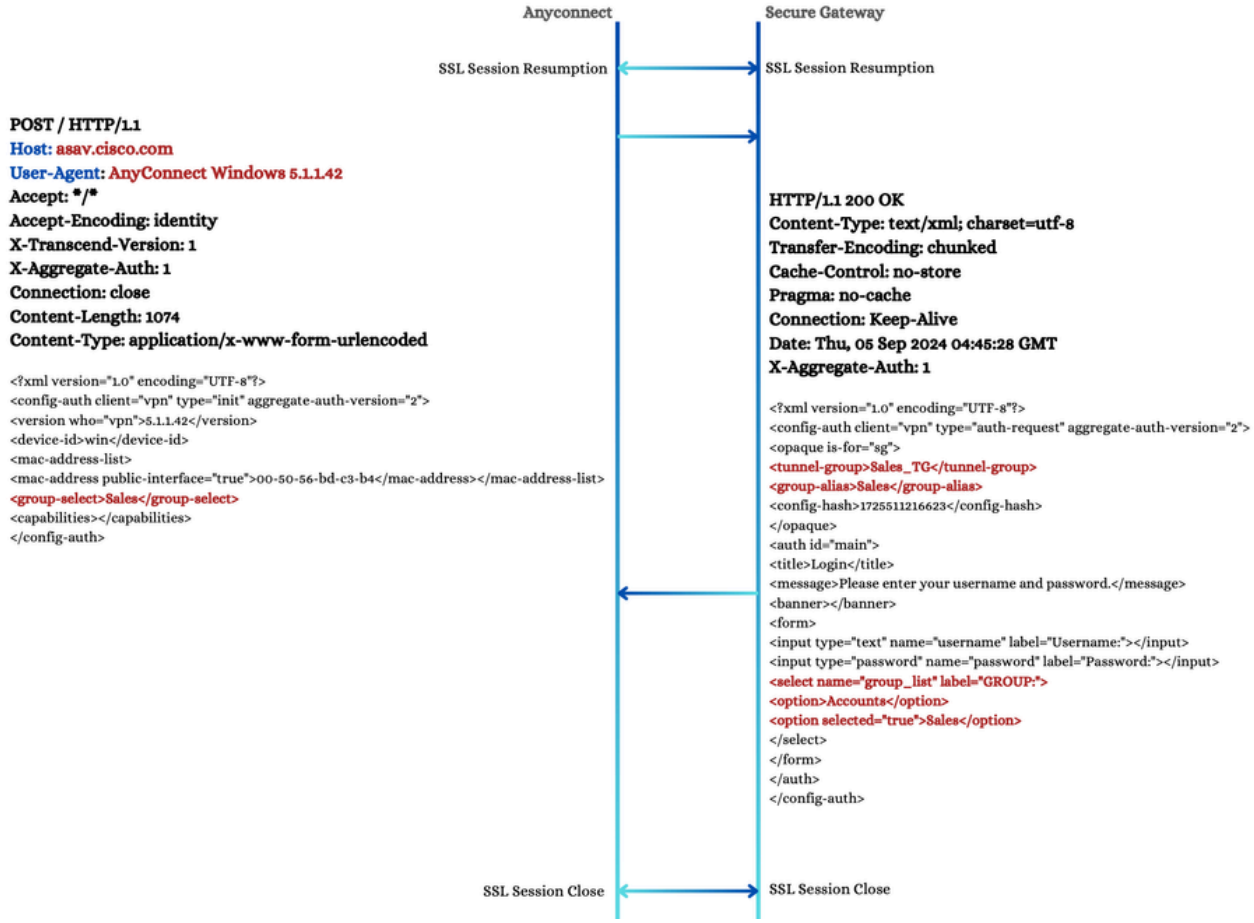


Hinweis: Das Form enthält ein 'select'-Element, das die Gruppenaliase aller auf dem sicheren Gateway konfigurierten Verbindungsprofile auflistet. Standardmäßig wird einer dieser Gruppenaliase mit dem ausgewählten booleschen Attribut = "true" hervorgehoben. Die Elemente tunnel-group und group-alias entsprechen diesem ausgewählten Verbindungsprofil.



POST - Gruppenauswahl 1

Wählt der Benutzer ein anderes Verbindungsprofil aus dieser Liste, wird ein weiterer POST-Vorgang durchgeführt. In diesem Fall sendet der Client eine POST-Anforderung mit dem 'group-select'-Element, das aktualisiert wird, um das ausgewählte Verbindungsprofil zu reflektieren, wie hier gezeigt.



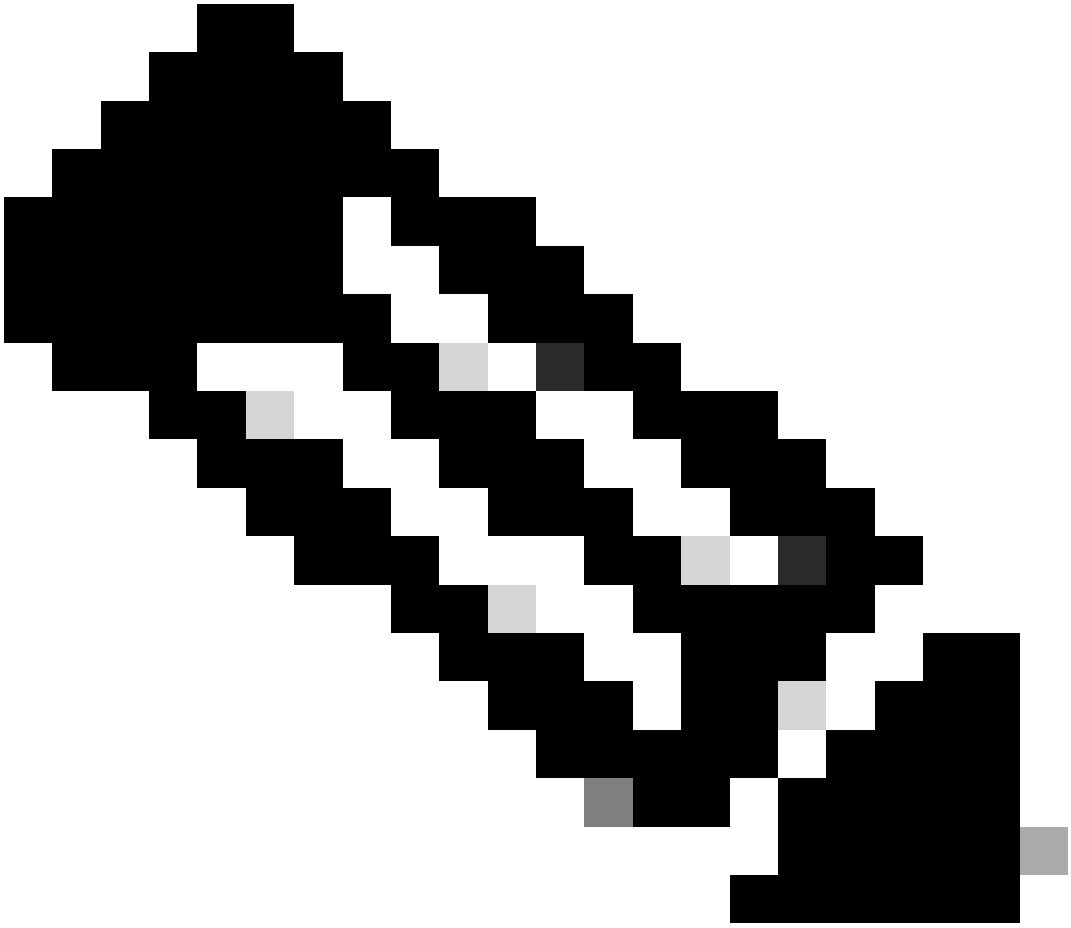
POST - Gruppenauswahl 2

3. POST - Benutzerauthentifizierung

Bei diesem Vorgang, der auf die POST-Gruppenauswahl folgt, sendet AnyConnect diese Informationen an das sichere Gateway:

1. Informationen zum ausgewählten Verbindungsprofil: Dazu gehören der Tunnelgruppenname und der Gruppenalias, wie vom sicheren Gateway im vorherigen Vorgang angegeben.

2. Benutzername und Passwort: Die Authentifizierungsdaten des Benutzers.



Hinweis: Da dieser Fluss spezifisch für die AAA-Authentifizierung ist, kann er sich von anderen Authentifizierungsmethoden unterscheiden.

Als Reaktion auf den POST-Vorgang sendet das sichere Gateway eine XML-Datei mit folgenden Informationen:

1. Sitzungs-ID: Dies entspricht nicht der SSL-Sitzungs-ID.

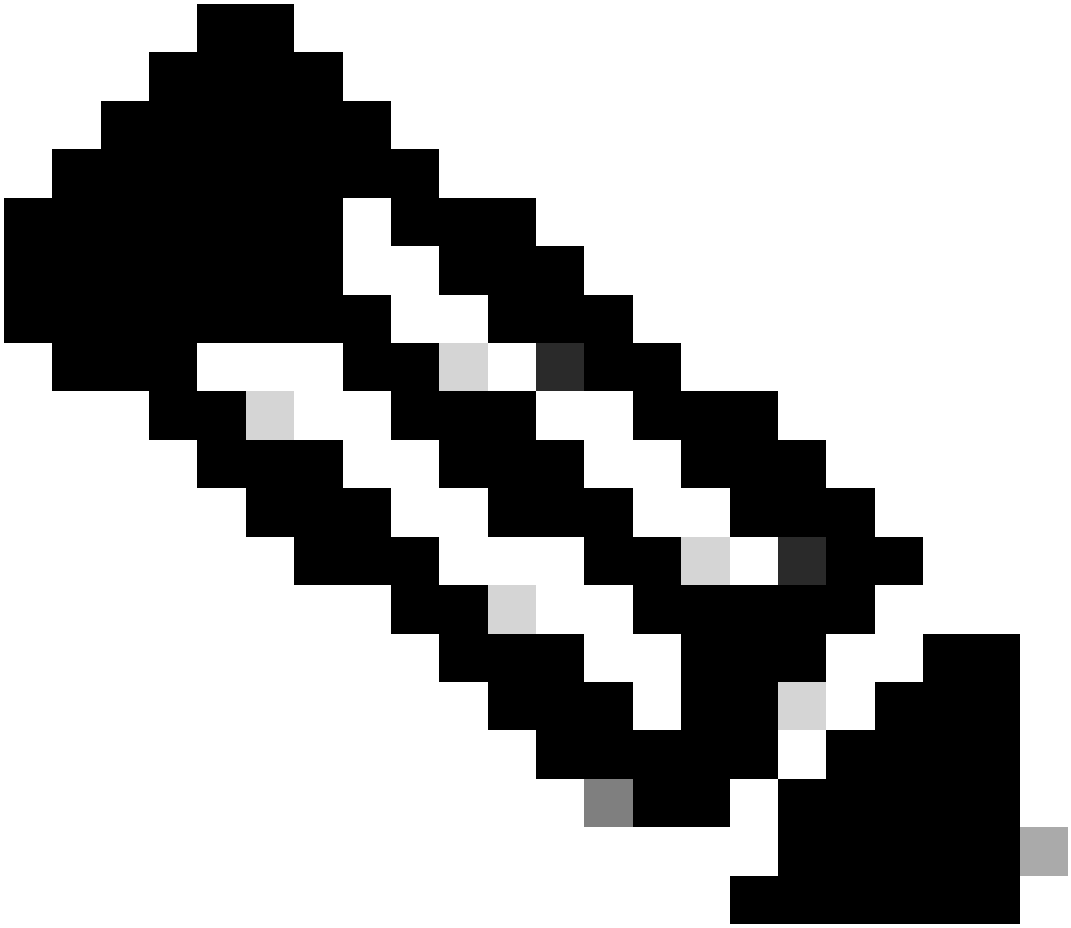
2. Sitzungstoken: Dieses Token wird später vom Client als WebVPN-Cookie verwendet.

3. Authentifizierungsstatus: Wird durch ein auth-Element mit der ID = 'success' angegeben.

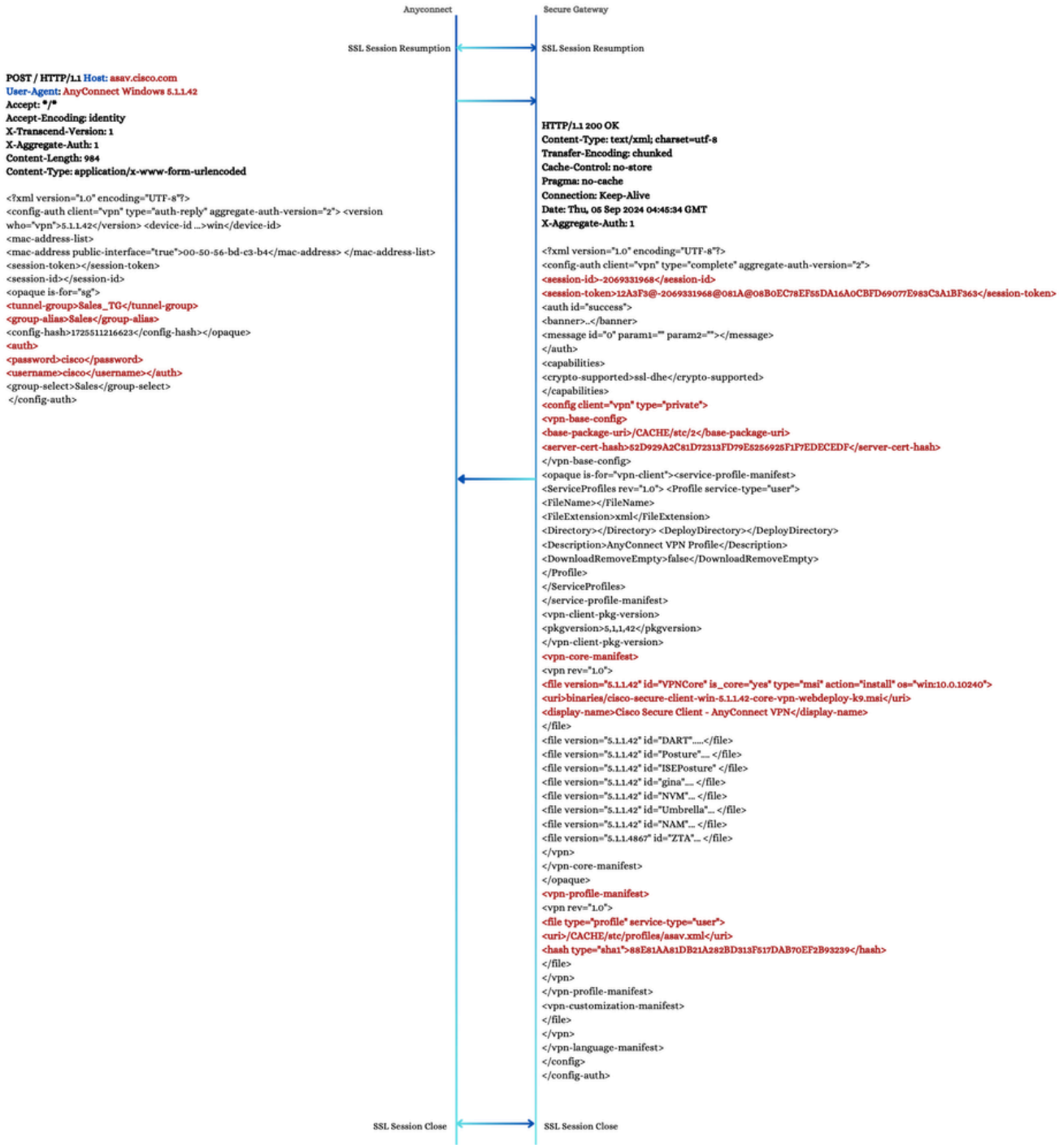
4. Hash für Serverzertifikate: Dieser Hash wird in der Datei preferences.xml zwischengespeichert.

5. vpn-core-manifest Element: Dieses Element gibt den Pfad und die Version des AnyConnect-Kernpakets zusammen mit anderen Komponenten wie Dart, Posture, ISE Posture usw. an. Es wird vom VPN Downloader im nächsten Abschnitt verwendet.

6. vpn-profile-manifest Element: Dieses Element gibt den Pfad (den Namen des Profils) und den SHA-1-Hash des Profils an.



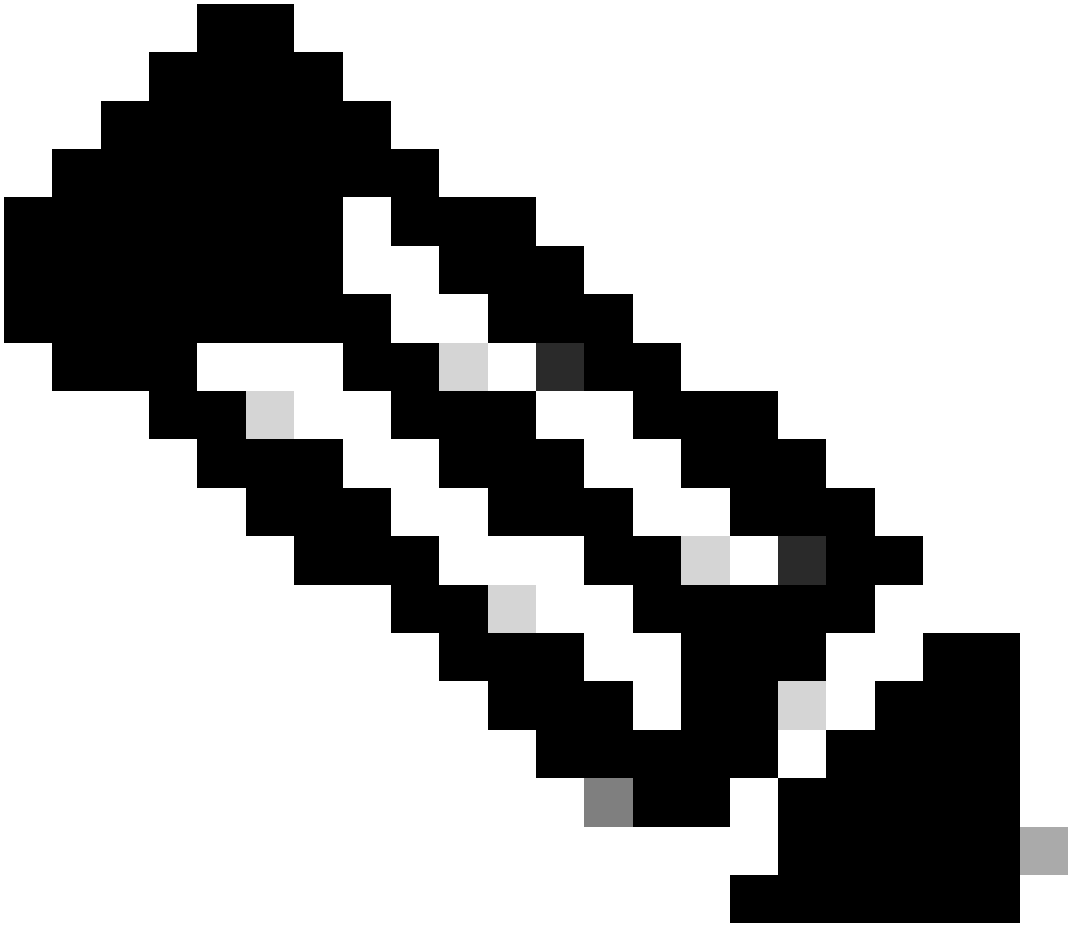
Hinweis: Wenn der Client nicht über das Profil verfügt, wird es vom VPN Downloader im nächsten Abschnitt heruntergeladen. Wenn der Client bereits über das Profil verfügt, wird der SHA-1-Hash des Clientprofils mit dem des Servers verglichen. Bei einer Diskrepanz überschreibt der VPN Downloader das Clientprofil mit dem Profil auf dem sicheren Gateway. Dadurch wird sichergestellt, dass das Profil auf dem sicheren Gateway nach der Authentifizierung auf dem Client durchgesetzt wird.



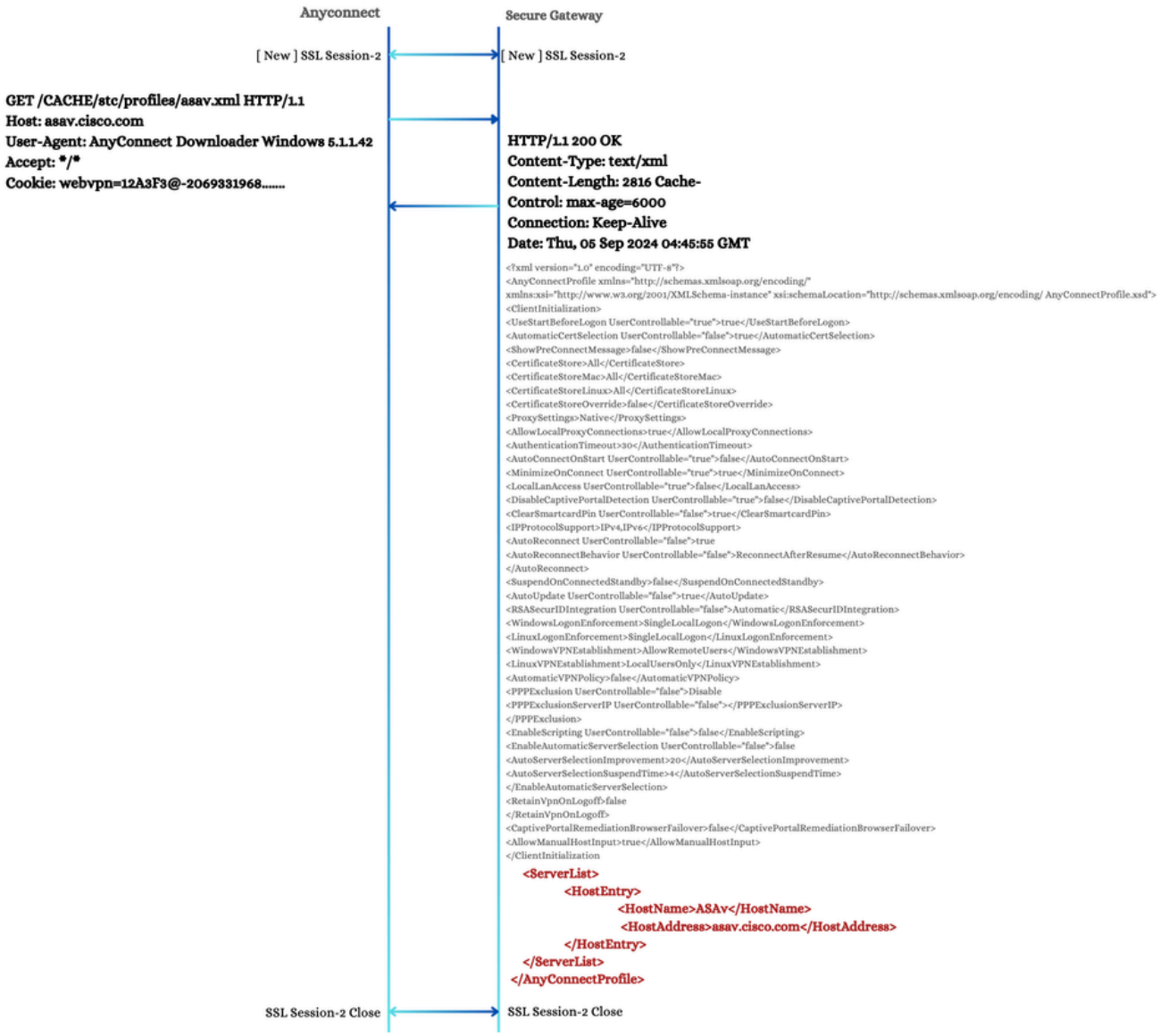
POST = User Authentication

4. AnyConnect-Downloader

Der AnyConnect Downloader initiiert immer eine neue SSL-Sitzung. Aus diesem Grund können Benutzer eine zweite Zertifikatwarnung erhalten, wenn das Zertifikat des sicheren Gateways nicht vertrauenswürdig ist. Während dieser Phase führt es separate GET-Vorgänge für jedes Element aus, das heruntergeladen werden muss.



Hinweis: Wenn das Clientprofil auf Secure Gateway hochgeladen wird, muss es heruntergeladen werden. Andernfalls wird die gesamte Verbindung abgebrochen.

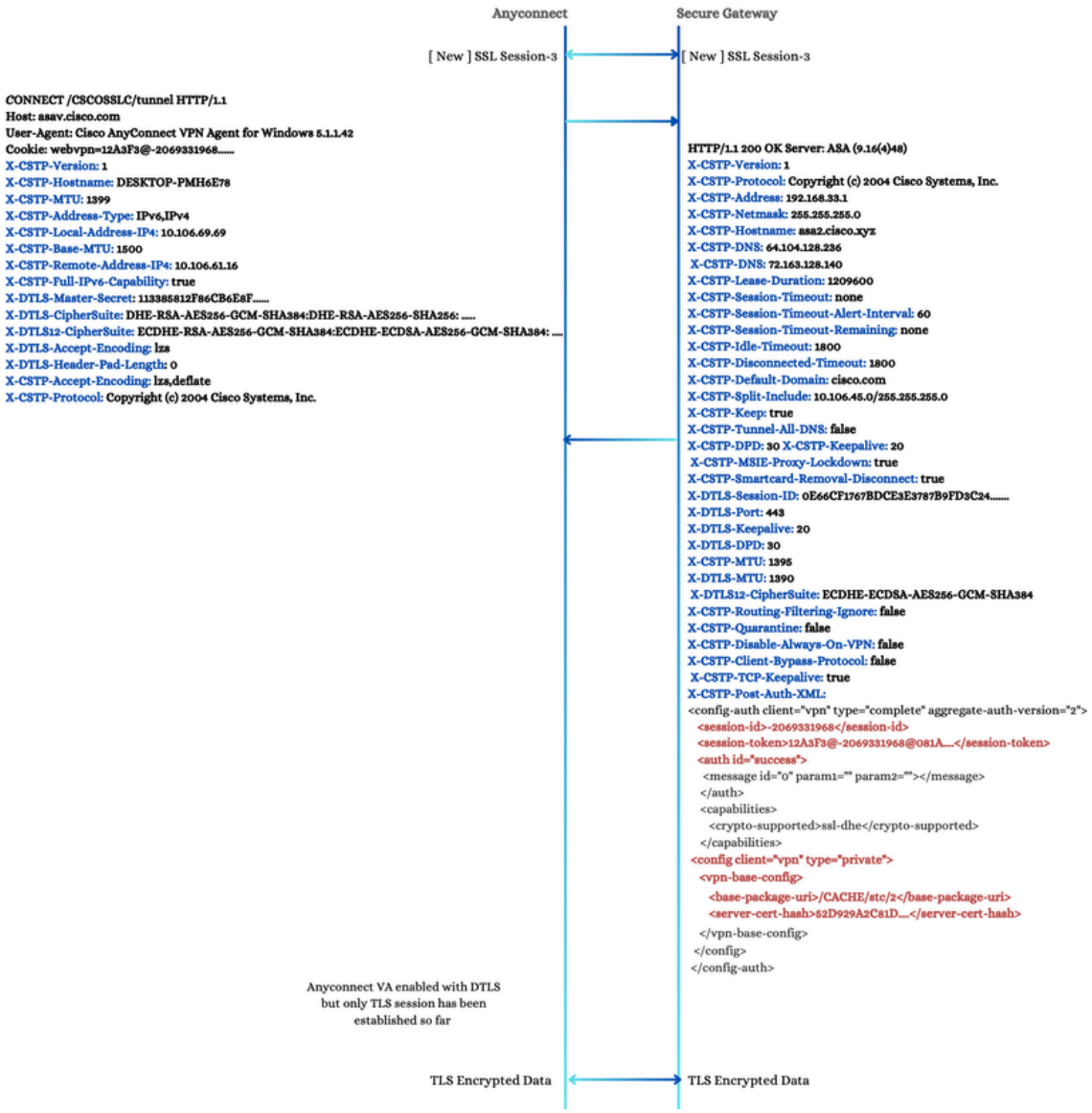


VPN-Downloader

5. CSTP-VERBINDUNG

AnyConnect führt als letzten Schritt zur Einrichtung eines sicheren Kanals eine CONNECT-Operation durch. Während des VERBINDUNGSVORGANGS sendet der AnyConnect-Client verschiedene X-CSTP- und X-DTLS-Attribute für das Secure Gateway, um diese zu verarbeiten. Das Secure Gateway antwortet mit zusätzlichen X-CSTP- und X-DTLS-Attributen, die der Client auf den aktuellen Verbindungsversuch anwendet. Dieser Austausch beinhaltet die X-CSTP-Post-Auth-XML, begleitet von einer XML-Datei, die weitgehend der im Schritt POST - User Authentication gezeigten entspricht.

Nach dem Empfang einer erfolgreichen Antwort initiiert AnyConnect den TLS-Datenkanal. Gleichzeitig wird die virtuelle AnyConnect-Adapterschnittstelle mit einem MTU-Wert aktiviert, der X-DTLS-MTU entspricht, vorausgesetzt, der anschließende DTLS-Handshake ist erfolgreich.



CSTP-Verbindung

6. DTLS-Handshake

Der DTLS-Handshake wird wie folgt durchgeführt: Diese Einrichtung erfolgt relativ schnell, da die Attribute zwischen dem Client und dem Server während des CONNECT-Ereignisses ausgetauscht werden.

Kunde

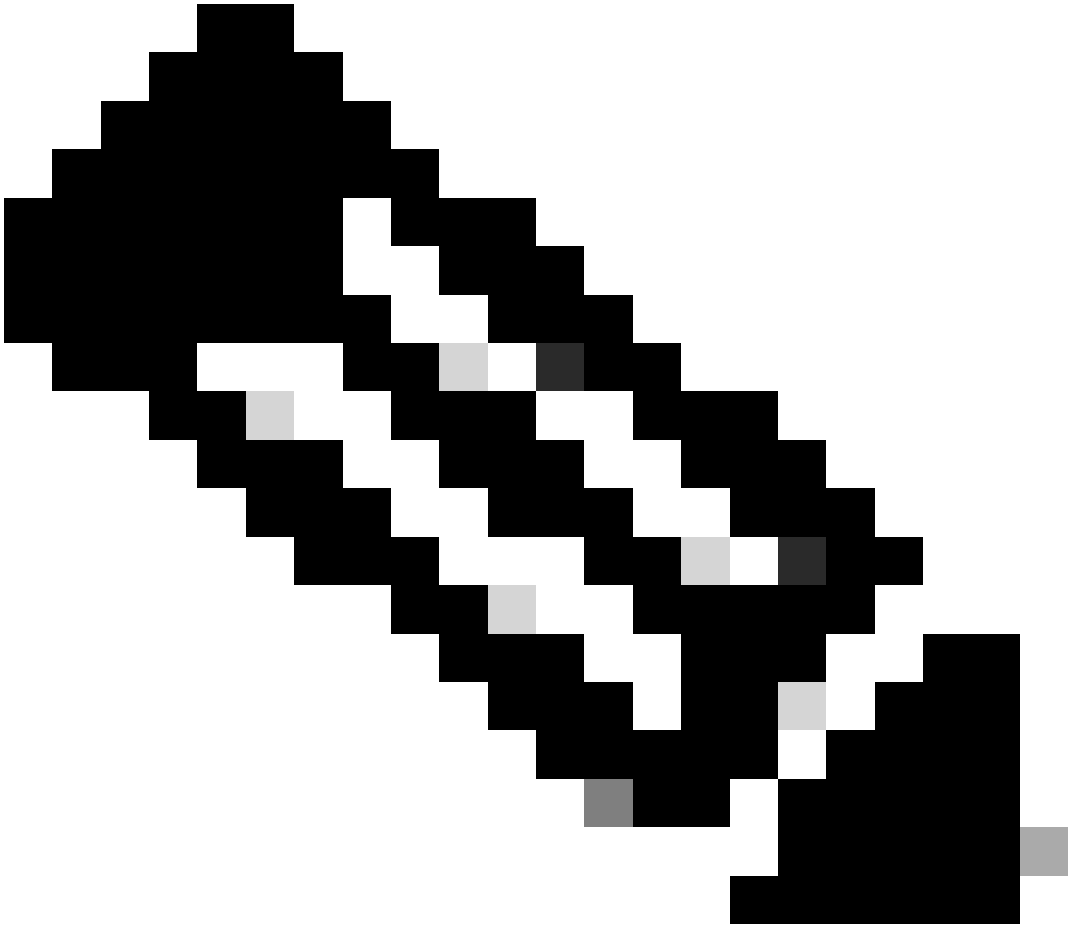
X-DTLS-Master-Secret: Der DTLS-Master-Secret wird vom Client generiert und vom Server freigegeben. Dieser Schlüssel ist für die Einrichtung einer sicheren DTLS-Sitzung von entscheidender Bedeutung.

X-DTLS-CipherSuite: Die Liste der vom Client unterstützten DTLS-Chiffriersuiten, die die Verschlüsselungsfunktionen des Clients angibt.

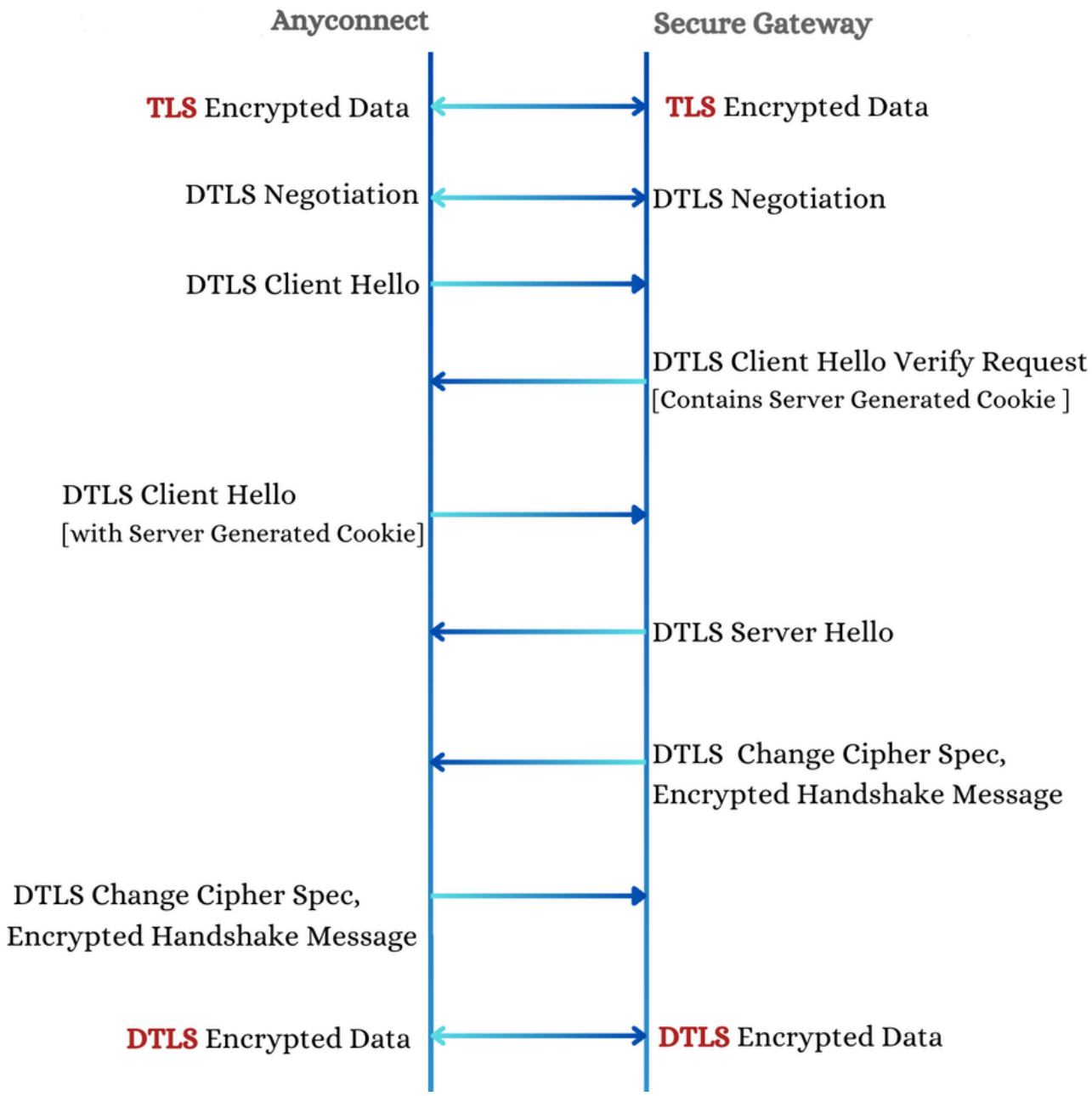
Server

X-DTLS-Session-ID: Die vom Server zugewiesene DTLS-Session-ID, die die Kontinuität der Sitzung sicherstellt.

X-DTLS-CipherSuite: Die vom Server aus der vom Client bereitgestellten Liste ausgewählte Verschlüsselungssuite, die sicherstellt, dass beide Parteien eine kompatible Verschlüsselungsmethode verwenden.



Hinweis: Während des DTLS-Handshakes läuft der TLS-Datenkanal weiter. Dadurch wird sichergestellt, dass die Datenübertragung während des Handshake-Vorgangs konsistent und sicher bleibt. Ein nahtloser Übergang zum DTLS-Datenverschlüsselungskanal erfolgt erst nach dem DTLS-Handshake.

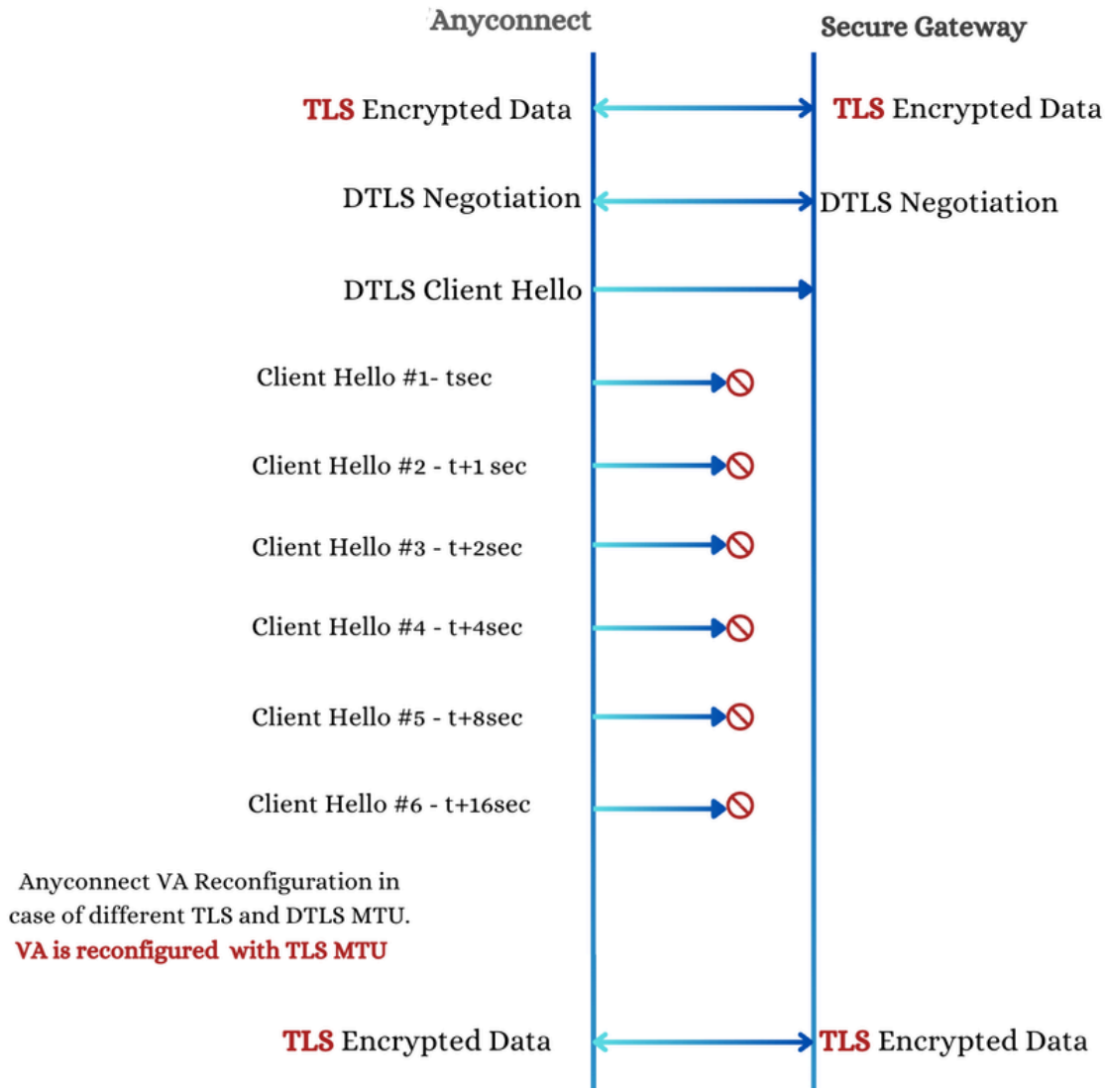


DTLS-Handshake

6.1. DTLS-Port gesperrt

Falls der DTLS-Port blockiert wird oder das Secure Gateway nicht auf DTLS Client Hello-Pakete antwortet, führt AnyConnect ein exponentielles Backoff mit bis zu fünf Wiederholungsversuchen durch, beginnend mit einer Verzögerung von einer Sekunde und ansteigend bis zu 16 Sekunden.

Wenn diese Versuche nicht erfolgreich sind, wendet AnyConnect die tatsächliche TLS-MTU, wie vom X-CSTP-MTU-Wert angegeben, der vom Secure Gateway in Phase 5. zurückgegeben wird, auf den virtuellen AnyConnect-Adapter an. Da sich diese MTU von der zuvor angewendeten MTU (X-DTLS-MTU) unterscheidet, ist eine Neukonfiguration des virtuellen Adapters erforderlich. Diese Neukonfiguration erscheint dem Endbenutzer als erneuter Verbindungsversuch, obwohl während dieses Prozesses keine neuen Verhandlungen stattfinden. Nach der Neukonfiguration des virtuellen Adapters wird der TLS-Datenkanal weiter betrieben.



DTLS-Port-Block

Zugehörige Informationen

- Dokumentationsreferenz zu Cisco VPN-Technologien
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.