De AnyConnect SSL VPN-verbindingsstroom begrijpen

Inhoud

Inleiding

Dit document richt zich op de stroom van gebeurtenissen die plaatsvinden tussen AnyConnect en de beveiligde gateway tijdens een SSL VPN-verbinding.

Achtergrondinformatie

AnyConnect

AnyConnect is de Cisco VPN-client die is ontworpen voor SSL- en IKEv2-protocollen. Het is beschikbaar voor de meeste desktop en mobiele platforms. AnyConnect maakt voornamelijk beveiligde verbindingen met Firepower Threat Defence (FTD), Adaptieve security applicaties (ASA) of Cisco IOS®/Cisco IOS® XE-routers, aangeduid als Secure Gateways.

Beveiligde gateway

In Cisco-terminologie wordt een SSL VPN-server een Secure Gateway genoemd, terwijl een

IPSec (IKEv2) server bekend staat als een Remote Access VPN-gateway. Cisco ondersteunt SSL VPN-tunnelbeëindiging op deze platforms:

- Cisco ASA 5500 en 5500-X Series-switches
- Cisco FTD (2100, 4100 en 9300 Series)
- Cisco ISR 4000 en ISR G2 Series
- Cisco CRS-1000 Series
- Cisco Catalyst 8000 Series

AnyConnect SSL VPN-verbindingsstroom

In dit document worden de gebeurtenissen die plaatsvinden tussen AnyConnect en de beveiligde gateway tijdens een SSL VPN-verbinding, opgesplitst in zes fasen:

1. SSL-handdruk

2. Selectie achteraf

3. POST - Gebruikersverificatie met gebruikersnaam/wachtwoord (optioneel)

4. VPN-downloads (optioneel)

5. CSTP CONNECT

6. DTLS-verbinding (optioneel)

1. SSL-handdruk

De SSL-handdruk wordt geïnitieerd door de AnyConnect-client na voltooiing van de TCP 3-weg-handdruk met een 'Client Hello'-bericht. De gebeurtenissen en de belangrijkste afhaallijnen zijn zoals gezegd.

Hallo client

De SSL-sessie begint met de client die een bericht 'Client Hello' verstuurt. In dit bericht:

a) De SSL-sessie-ID is ingesteld op 0, wat de initiatie van een nieuwe sessie aangeeft.

b) De payload omvat de door de client ondersteunde algoritmen en een client-gegenereerde willekeurige.

Server Hallo

De server reageert met een "Server Hello"-bericht, dat het volgende bevat:

a) Het geselecteerde algoritme reeks van de lijst die door de cliënt wordt verstrekt.

b) De server genereerde de SSL Session ID, en een server genereerde een willekeurige nonce.

Servercertificaat

Na de 'Server Hello' stuurt de server zijn SSL-certificaat, dat fungeert als zijn identiteit. Belangrijke opmerkingen zijn onder meer:

a) Als dit certificaat een strikte validatiecontrole niet doorstaat, blokkeert AnyConnect standaard de server.

b) De gebruiker heeft de optie om dit blok uit te schakelen, maar volgende verbindingen geven een waarschuwing weer tot de gerapporteerde fouten zijn opgelost.

Clientcertificaataanvraag

De server kan ook een clientcertificaat aanvragen, door een lijst met onderwerpnamen DN's te verzenden van alle CA-certificaten die op de beveiligde gateway zijn geladen. Dit verzoek dient twee doelen:

a) Het helpt de klant (gebruiker) het juiste identiteitscertificaat te kiezen als er meerdere ID-certificaten beschikbaar zijn.

b) Zorg ervoor dat het teruggekeerde certificaat wordt vertrouwd door de beveiligde gateway, hoewel verdere certificaatvalidatie nog moet plaatsvinden.

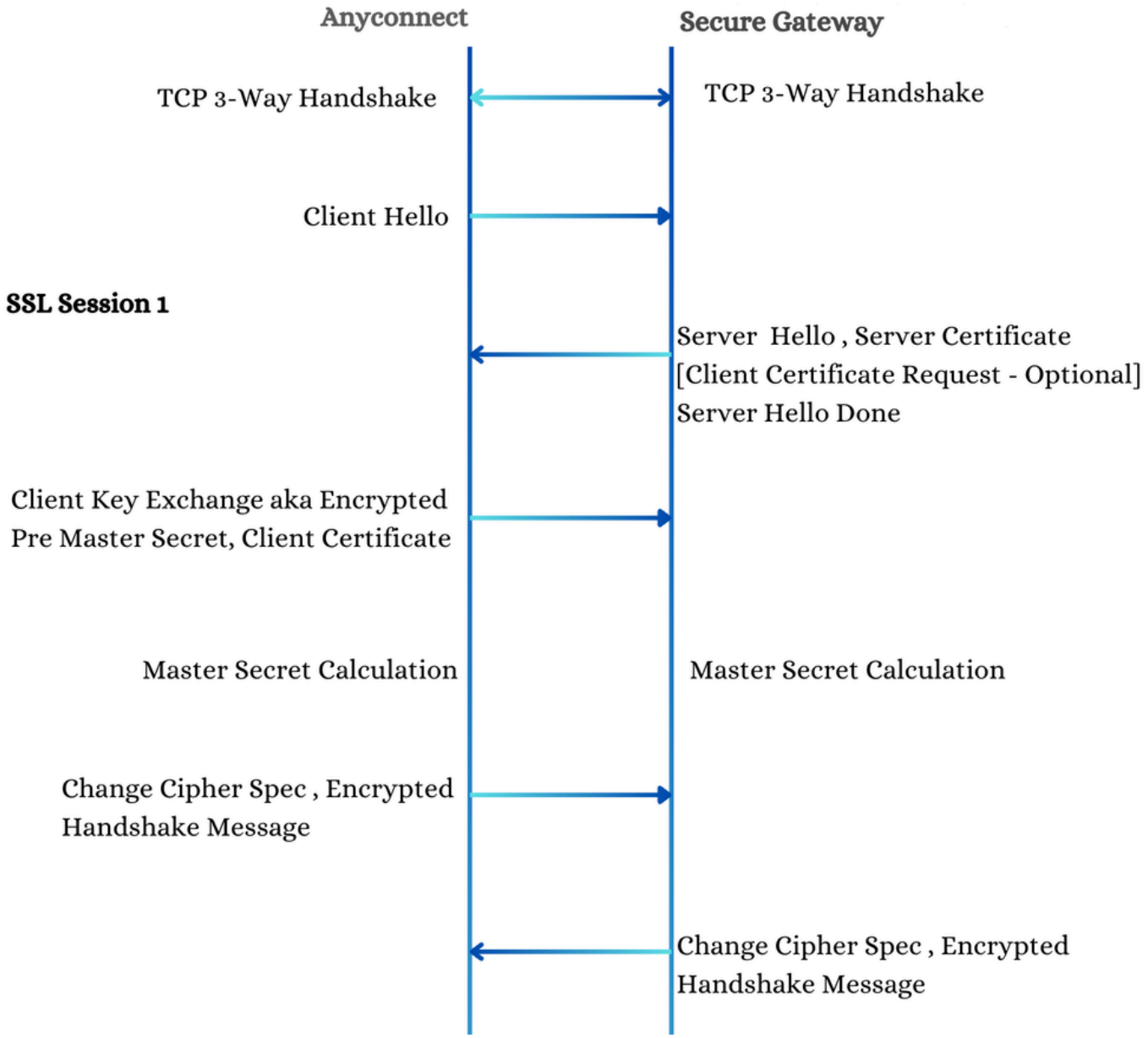
Toetsuitwisseling voor client

De client stuurt dan een 'Client Key Exchange'-bericht, dat een pre-master geheime sleutel bevat. Deze sleutel wordt versleuteld met:

a) De openbare sleutel van de server vanaf het servercertificaat, als de gekozen algoritme suite op RSA-gebaseerd is (bijvoorbeeld, TLS_RSA_WITH_AES_128_CBC_SHA).

b) De openbare DH-sleutel van de server in het bericht Server Hello, als de gekozen algoritme suite is gebaseerd op DHE (bijvoorbeeld TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Gebaseerd op het pre-master geheim, genereren de client-gegenereerde willekeurige nonce, en de server-gegenereerde willekeurige nonce, zowel de client als de Secure Gateway onafhankelijk een master geheim. Dit hoofdgeheim wordt dan gebruikt om sessiesleutels af te leiden, waardoor een veilige communicatie tussen de client en de server wordt gewaarborgd.



SSL-sessie 1

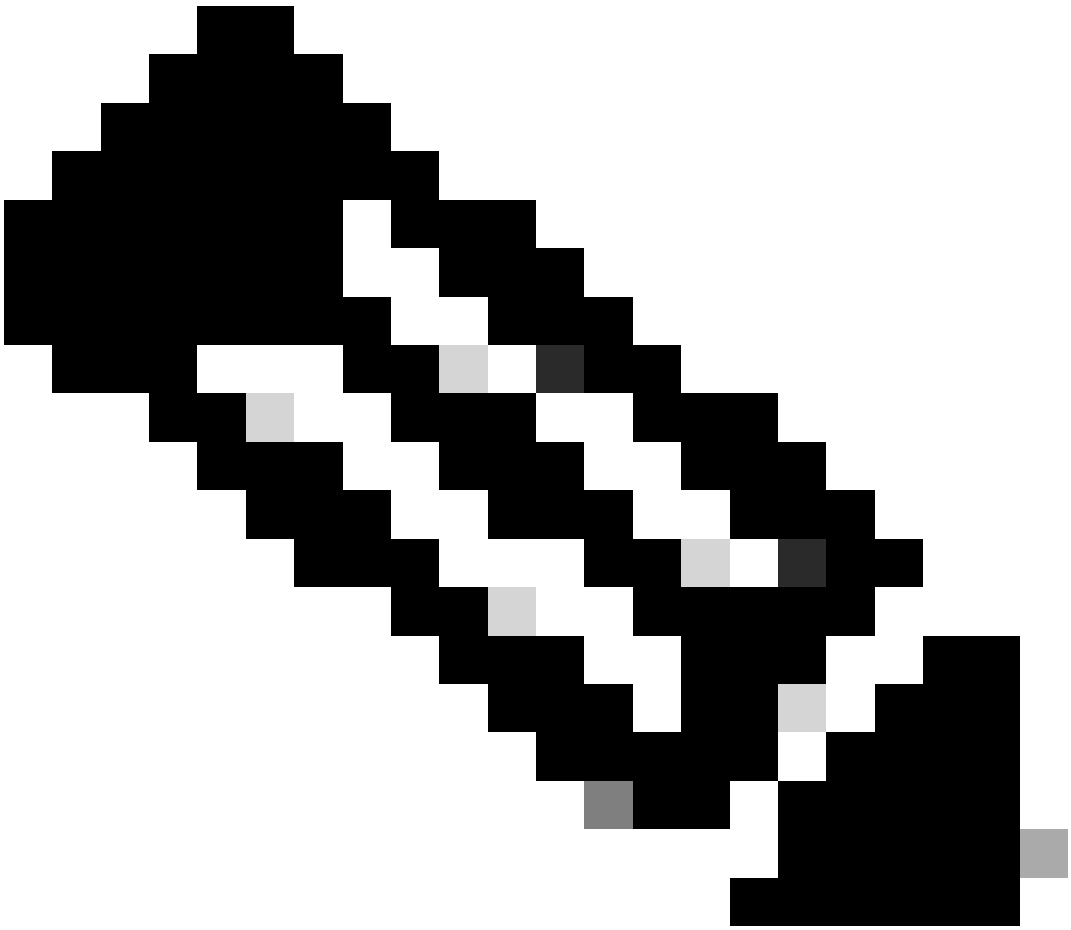
2. Selectie achteraf van de groep

Tijdens deze handeling beschikt de client niet over informatie over het verbindingsprofiel, tenzij dit expliciet door de gebruiker is gespecificeerd. De verbindingspoging is gericht op de Secure Gateway URL (asav.cisco.com), zoals aangegeven door het 'group-access' element in het verzoek. De client geeft aan dat het ondersteuning biedt voor 'aggregatie-authenticatie' versie 2. Deze versie is een aanzienlijke verbetering ten opzichte van de vorige versie, met name in termen van efficiënte XML transacties. Zowel de beveiligde gateway als de client moet akkoord gaan met de te gebruiken versie. In scenario's waar de beveiligde gateway versie 2 niet ondersteunt, wordt een extra POST-handeling geactiveerd, waardoor de client terugvalt naar de versie.

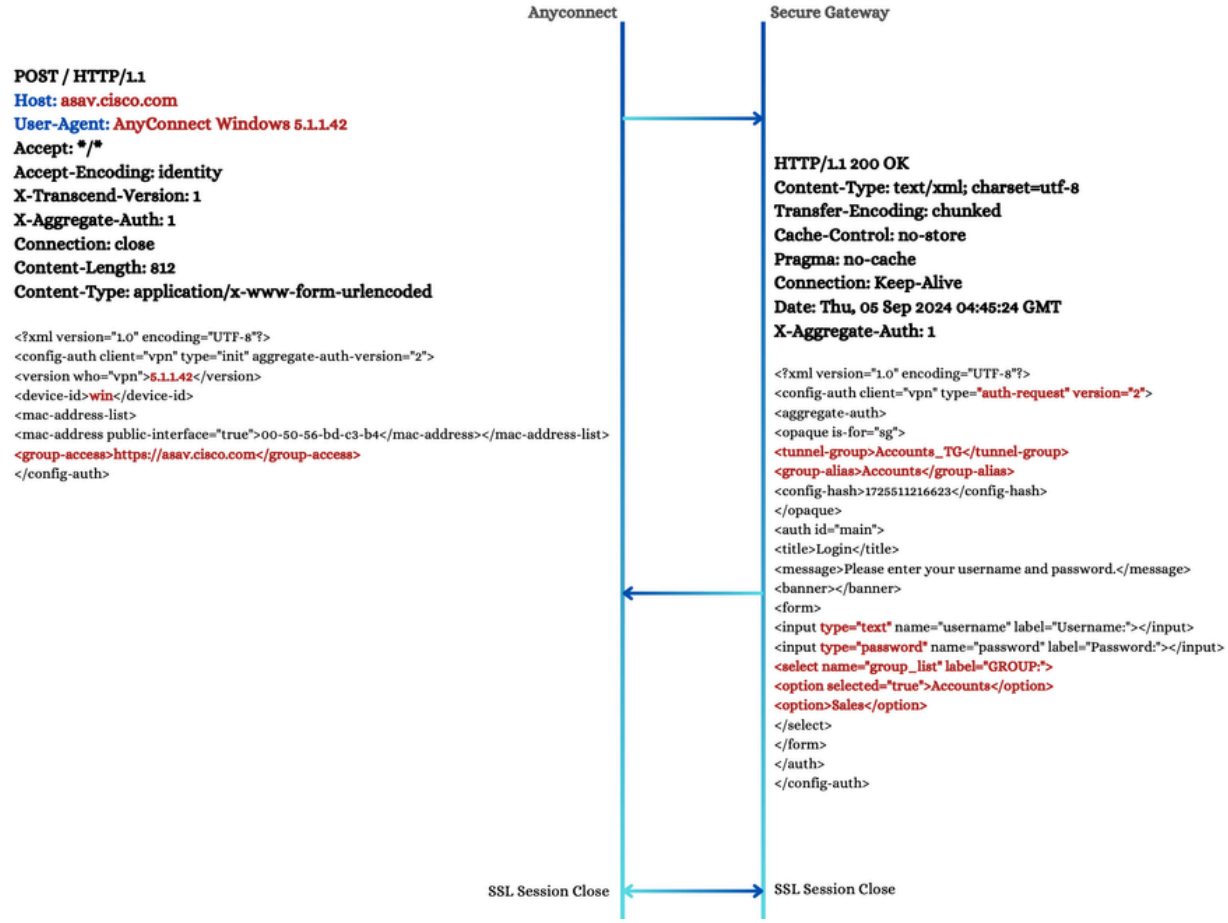
In de reactie van HTTP, wijst de veilige gateway op deze:

1. De versie van geaggregeerde verificatie die door de beveiligde gateway wordt ondersteund.

2. Tunnelgroeplijst en het Gebruikersnaam/Wachtwoord formulier.

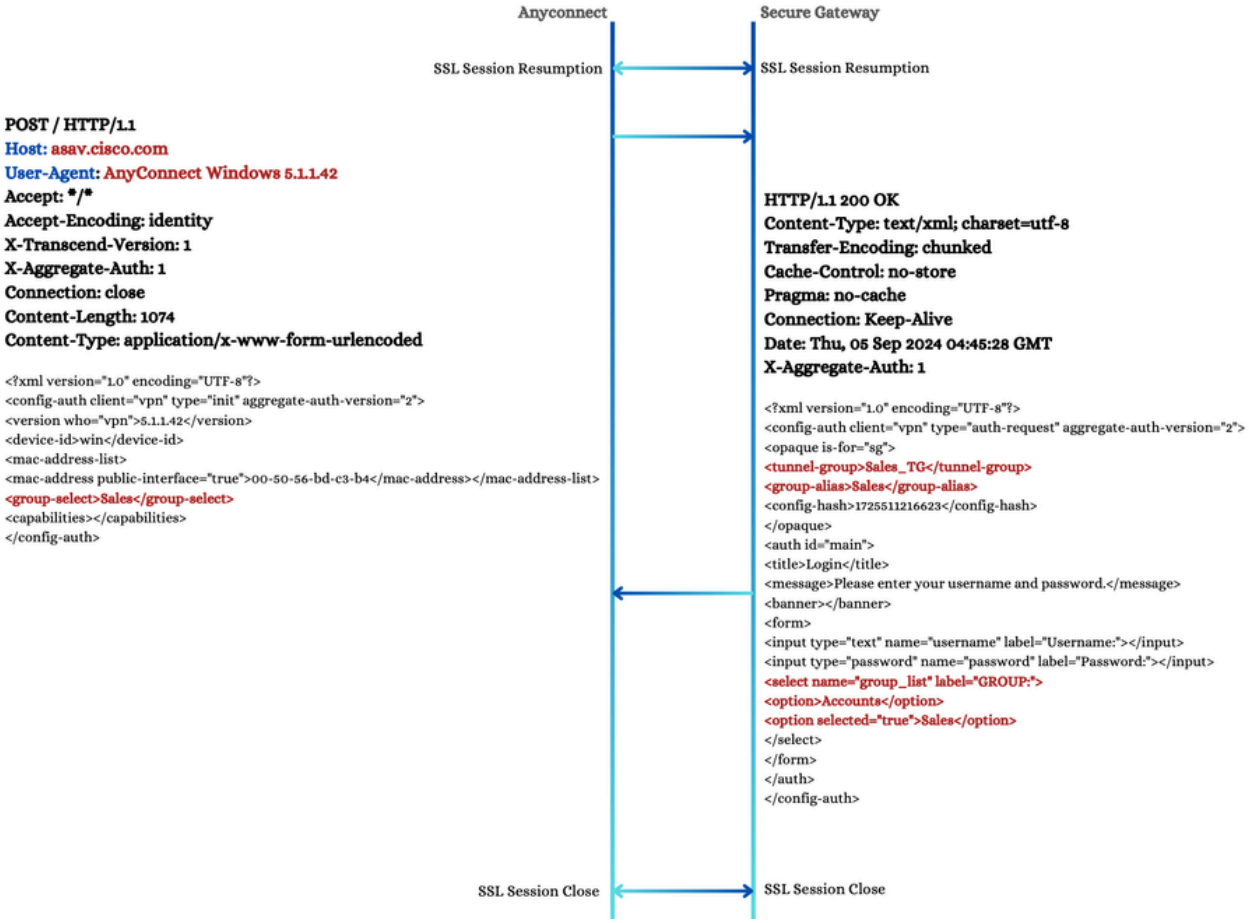


Opmerking: het formulier bevat een 'selecteer' element, dat een lijst bevat met de groepsaliassen van alle verbindingsprofielen die op de beveiligde gateway zijn geconfigureerd. Standaard wordt een van deze groepsaliassen gemarkeerd met het geselecteerde = "ware" booleaanse kenmerk. De elementen tunnelgroep en groepsalias komen overeen met dit gekozen verbindingsprofiel.



POST - groepsselectie 1

Als de gebruiker een ander verbindingsprofiel uit deze lijst kiest, vindt een andere POST-bewerking plaats. In dit geval stuurt de client een POST-verzoek met het 'groep-selecteer'-element bijgewerkt om het gekozen verbindingsprofiel weer te geven, zoals hier wordt getoond.



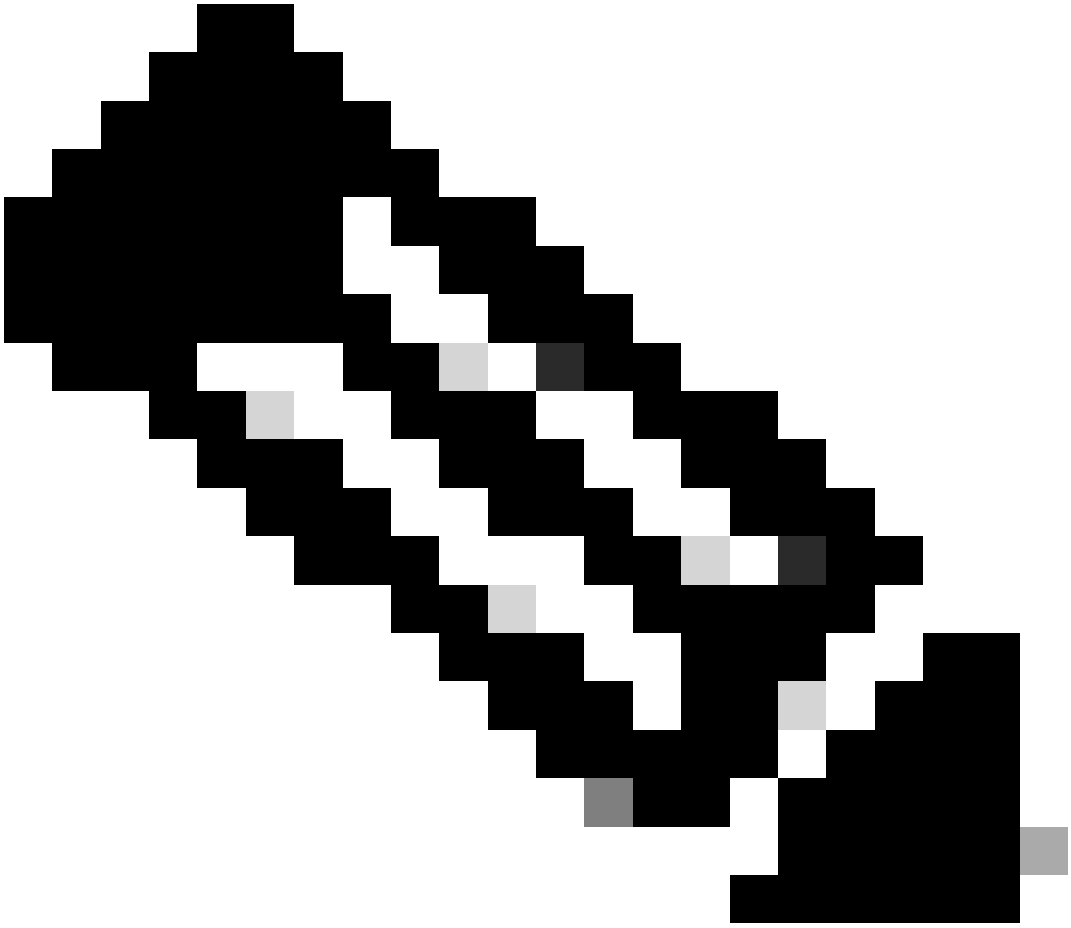
POST - groepsselectie 2

3. POST - Gebruikersverificatie

In deze bewerking, die de selectie van de POST-groep volgt, stuurt AnyConnect deze informatie naar de Secure Gateway:

1. Gekozen verbindingsprofielinformatie: dit omvat de naam van de tunnelgroep en de groepalias zoals aangegeven door de beveiligde gateway in de eerdere bewerking.

2. Gebruikersnaam en wachtwoord: de verificatiereferenties van de gebruiker.



Opmerking: aangezien deze stroom specifiek is voor AAA-verificatie, kan deze verschillen van andere verificatiemethoden.

In reactie op de POST-handeling stuurt de Secure Gateway een XML-bestand met deze informatie:

1. Sessie-ID: Dit is niet hetzelfde als de SSL-sessie-ID.

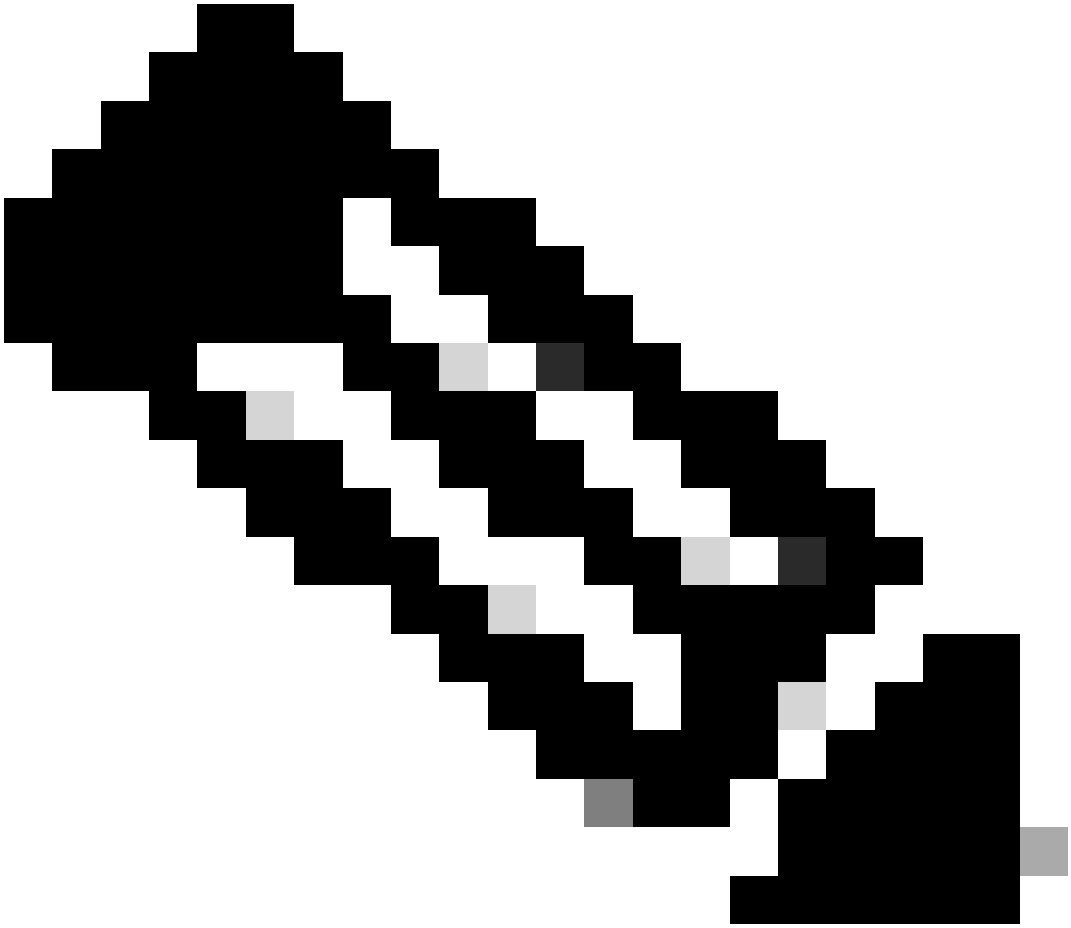
2. Session Token: Dit token wordt later door de client gebruikt als WebVPN-cookie.

3. Verificatiestatus: Aangegeven door een auth element met id = 'succes'.

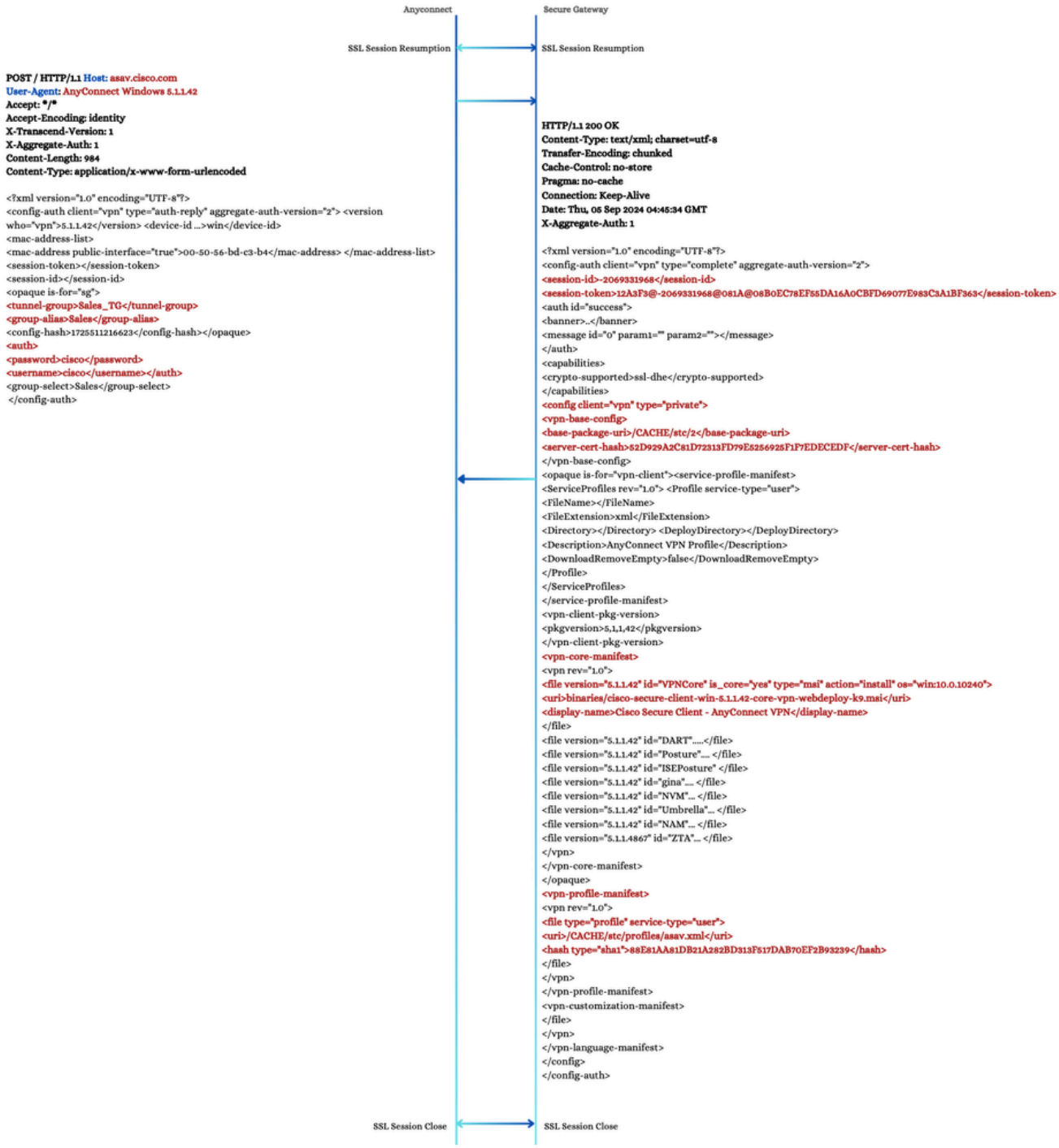
4. Server Certificate Hash: Deze hash wordt gecachet in het voorkeuren.xml bestand.

5. vpn-core-manifest element: dit element geeft het pad en de versie van het AnyConnect-corepakket aan, samen met andere componenten zoals Dart, Posture, ISE Posture, enzovoort. Het wordt gebruikt door VPN Downloader in de volgende sectie.

6. vpn-profiel-manifest element: Dit element geeft het pad (de naam van het profiel) en de SHA-1 hash van het profiel aan.



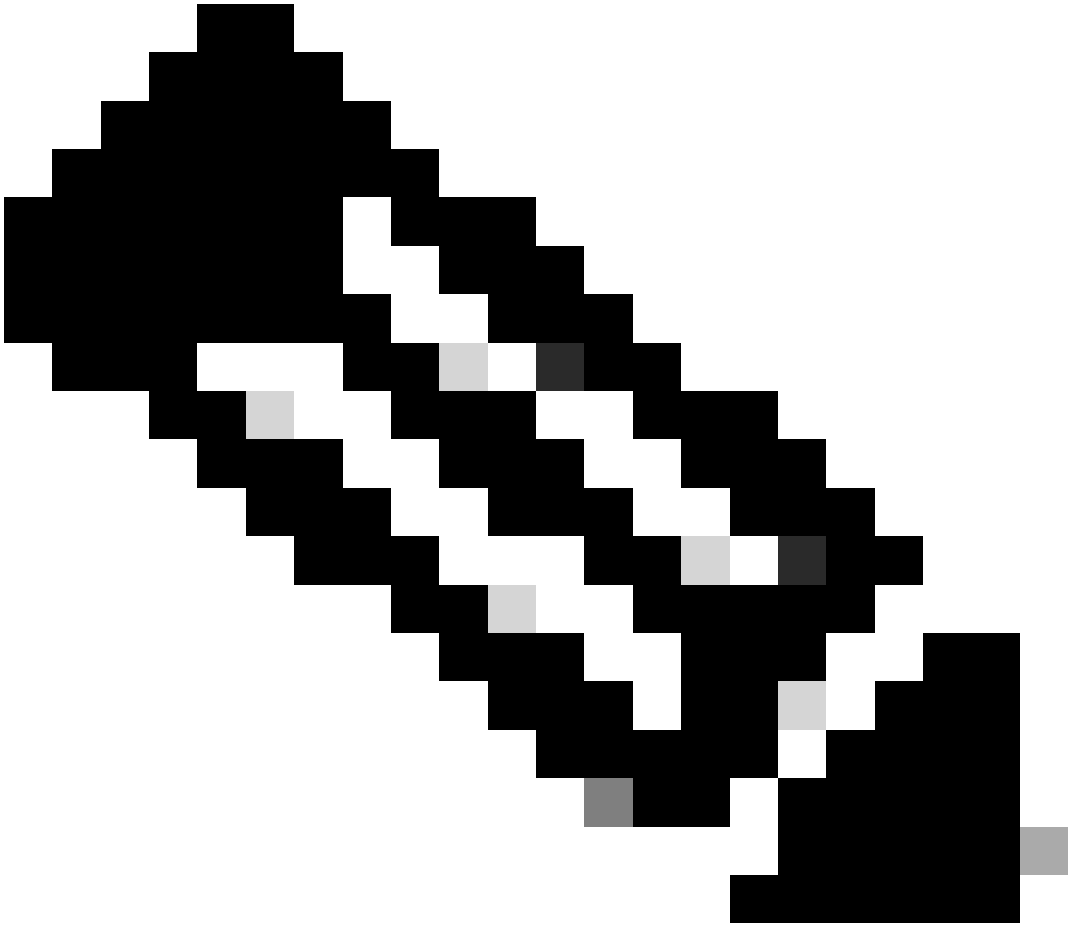
Opmerking: als de client niet over het profiel beschikt, wordt het profiel in de volgende sectie van VPN Downloader gedownload. Als de client al over het profiel beschikt, wordt de SHA-1 hash van het clientprofiel vergeleken met die van de server. In het geval van een wanverhouding, beschrijft VPN Downloader het clientprofiel met het profiel op de beveiligde gateway. Dit waarborgt dat het profiel op de beveiligde gateway na de verificatie op de client wordt afgedwongen.



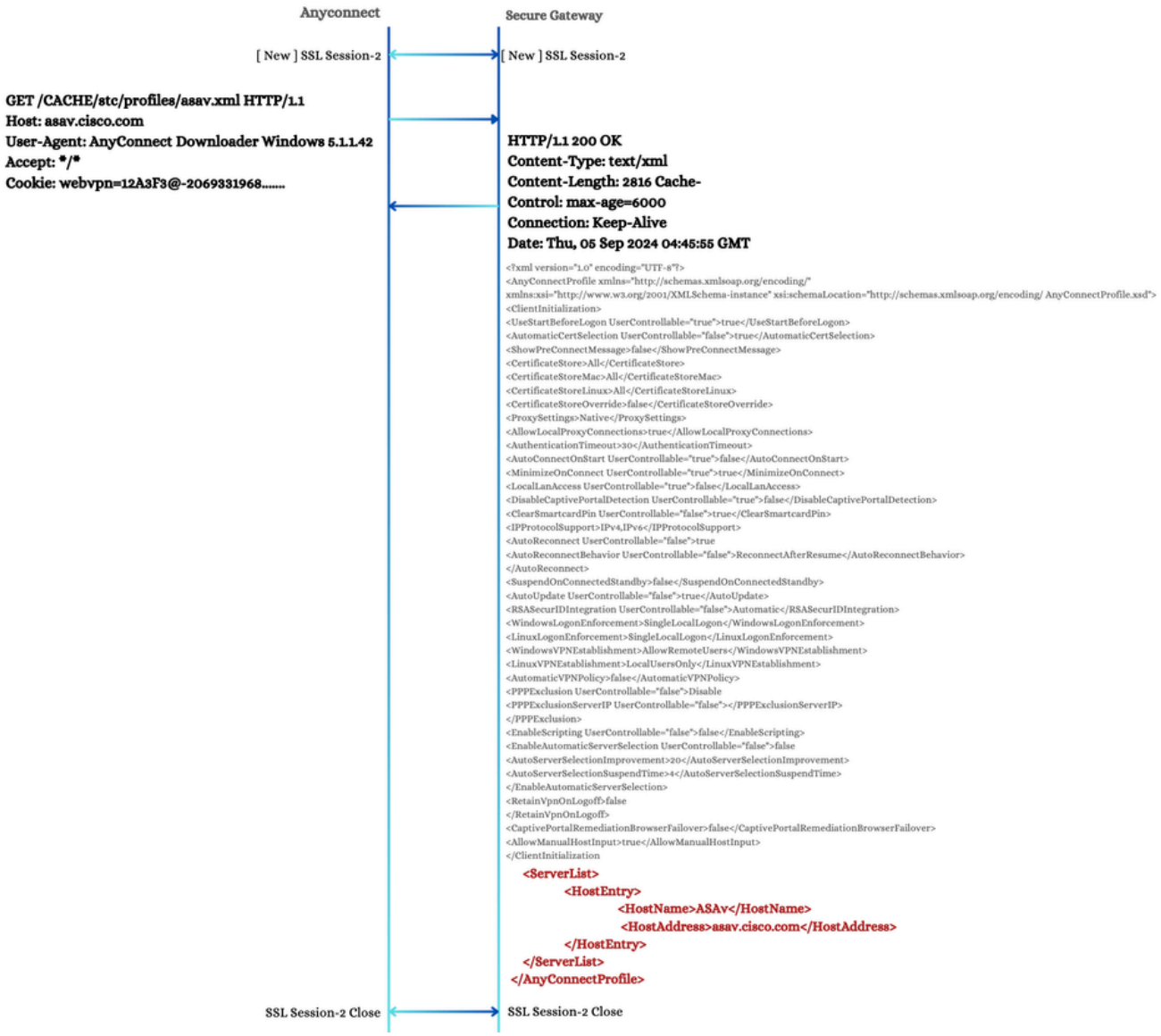
POST - Gebruikersverificatie

4. AnyConnect-downloads

AnyConnect Downloader start altijd een nieuwe SSL-sessie. Daarom kunnen gebruikers een tweede certificaatwaarschuwing krijgen als het certificaat van de beveiligde gateway onbetrouwbaar is. Tijdens deze fase, voert het afzonderlijke GET bewerkingen uit voor elk item dat moet worden gedownload.



Opmerking: als het clientprofiel is geüpload op Secure Gateway, is het verplicht om het te downloaden; anders wordt de gehele verbindingspoging beëindigd.

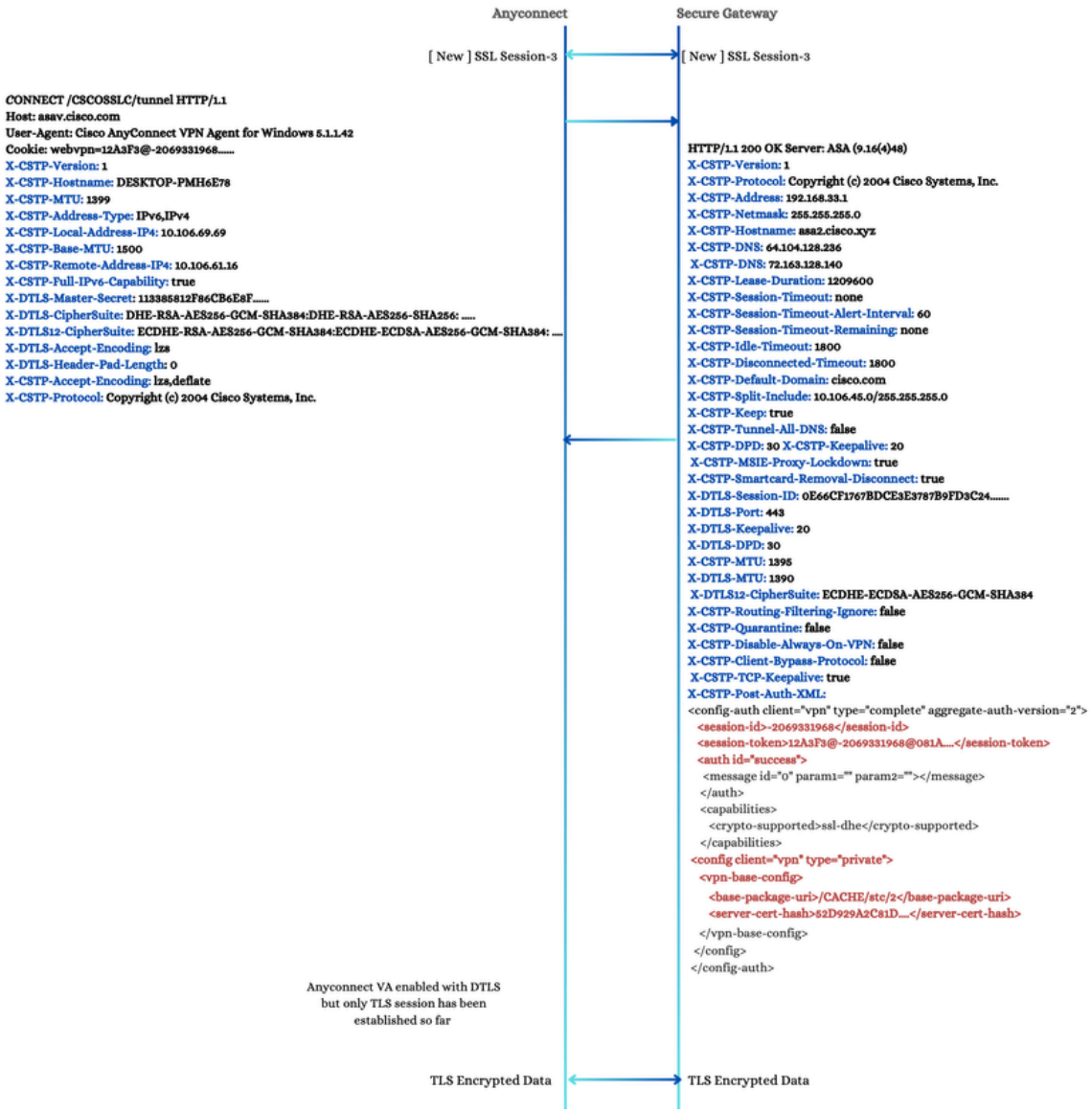


VPN-downloads

5. CSTP CONNECT

AnyConnect voert een CONNECT-bewerking uit als de laatste stap bij het opzetten van een beveiligd kanaal. Tijdens de CONNECT-bewerking verzendt de AnyConnect-client verschillende X-CSTP- en X-DTLS-kenmerken voor de beveiligde gateway om deze te kunnen verwerken. De Secure Gateway reageert met aanvullende X-CSTP- en X-DTLS-kenmerken die door de client worden toegepast op de huidige verbindingspoging. Deze uitwisseling omvat de X-CSTP-Post-Auth-XML, vergezeld van een XML-bestand, dat grotendeels vergelijkbaar is met het bestand dat in de POST - User Authentication-stap wordt gezien.

Na een succesvolle respons start AnyConnect het TLS-gegevenskanaal. Tegelijkertijd wordt de AnyConnect Virtual-adapterinterface geactiveerd met een MTU-waarde die gelijk is aan X-DTLS-MTU, ervan uitgaande dat de volgende DTLS-handdruk werkt.



CSTP Connect

6. DTLS-handdruk

De DTLS-handdruk gaat verder zoals hier wordt beschreven. Deze instelling is relatief snel vanwege de kenmerken die tijdens de CONNECT-gebeurtenis tussen de client en server zijn uitgewisseld.

Klant

X-DTLS-Master-Secret: Het DTLS Master Secret wordt gegenereerd door de client en gedeeld met de server. Deze sleutel is cruciaal voor het instellen van een beveiligde DTLS-sessie.

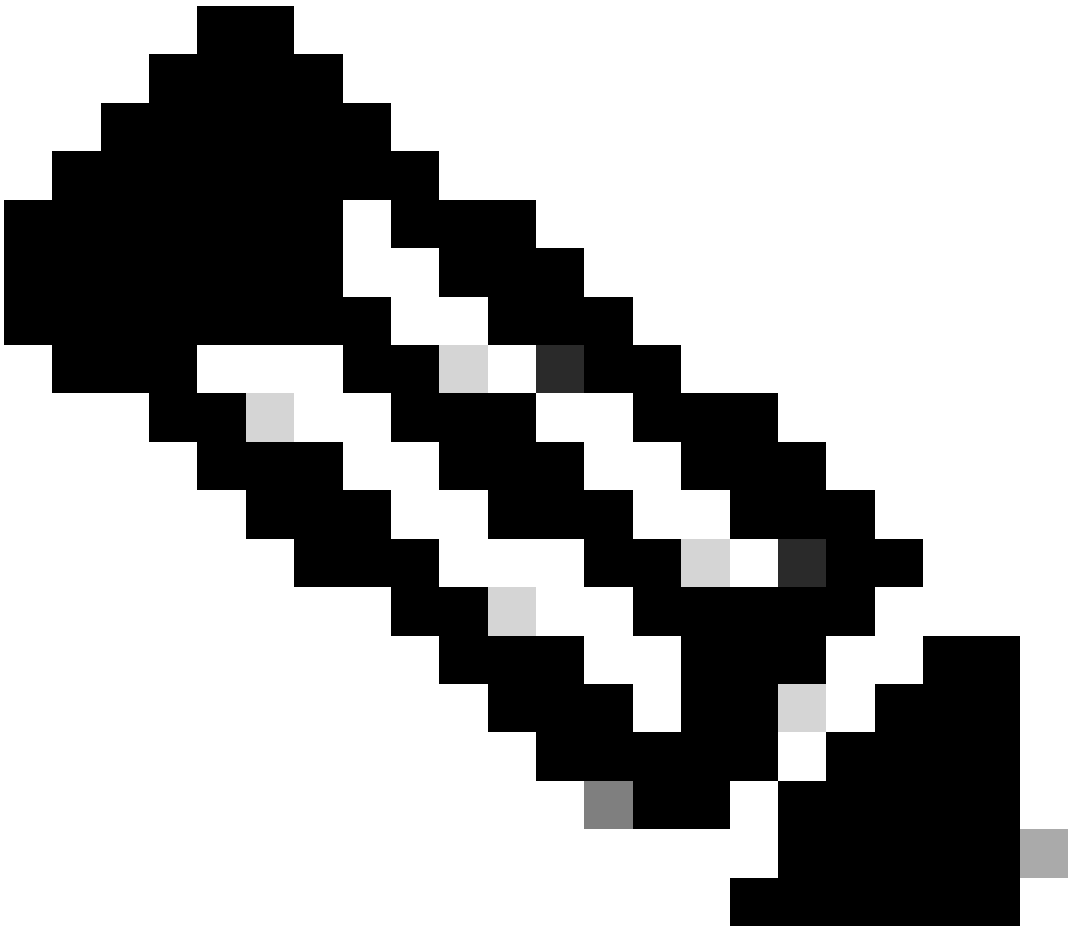
X-DTLS-CipherSuite: De lijst met DTLS-algoritmes die door de client worden ondersteund, die de coderingsmogelijkheden van de client aangeeft.

Server

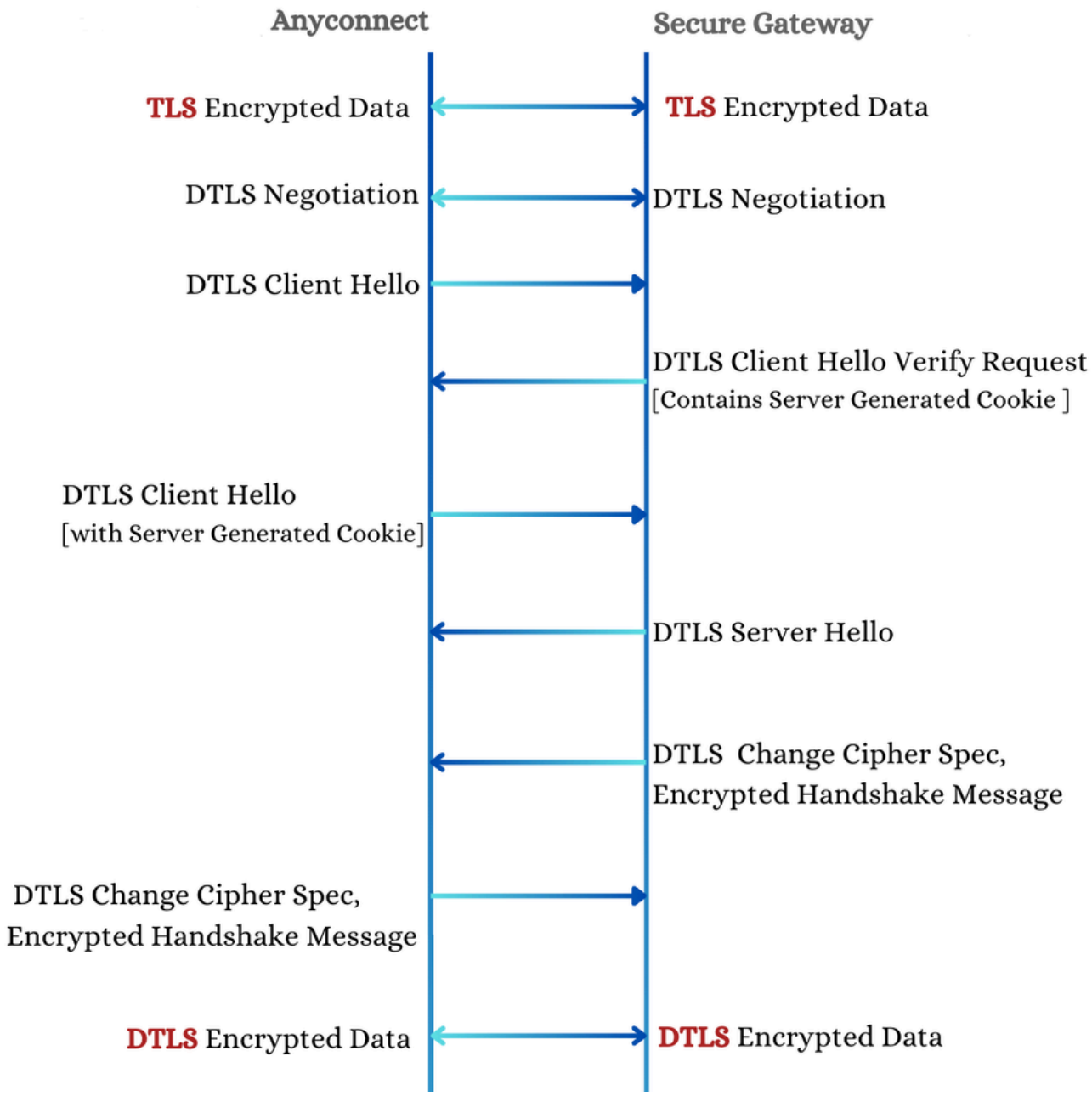
X-DTLS-Session-ID: de DTLS-sessie-ID die door de server aan de client is toegewezen om te

gebruiken, zodat de continuïteit van de sessie is gegarandeerd.

X-DTLS-CipherSuite: de coderingssuite die door de server is geselecteerd uit de lijst die door de client is geleverd, waarbij ervoor wordt gezorgd dat beide partijen een compatibele coderingsmethode gebruiken.



Opmerking: terwijl de DTLS-handdruk bezig is, blijft het TLS-gegevenskanaal werken. Dit waarborgt dat de gegevenstransmissie tijdens het handdrukproces consistent en veilig blijft. Een naadloze overgang naar het DTLS-gegevenscoderingskanaal vindt alleen plaats nadat de DTLS-handdruk is voltooid.

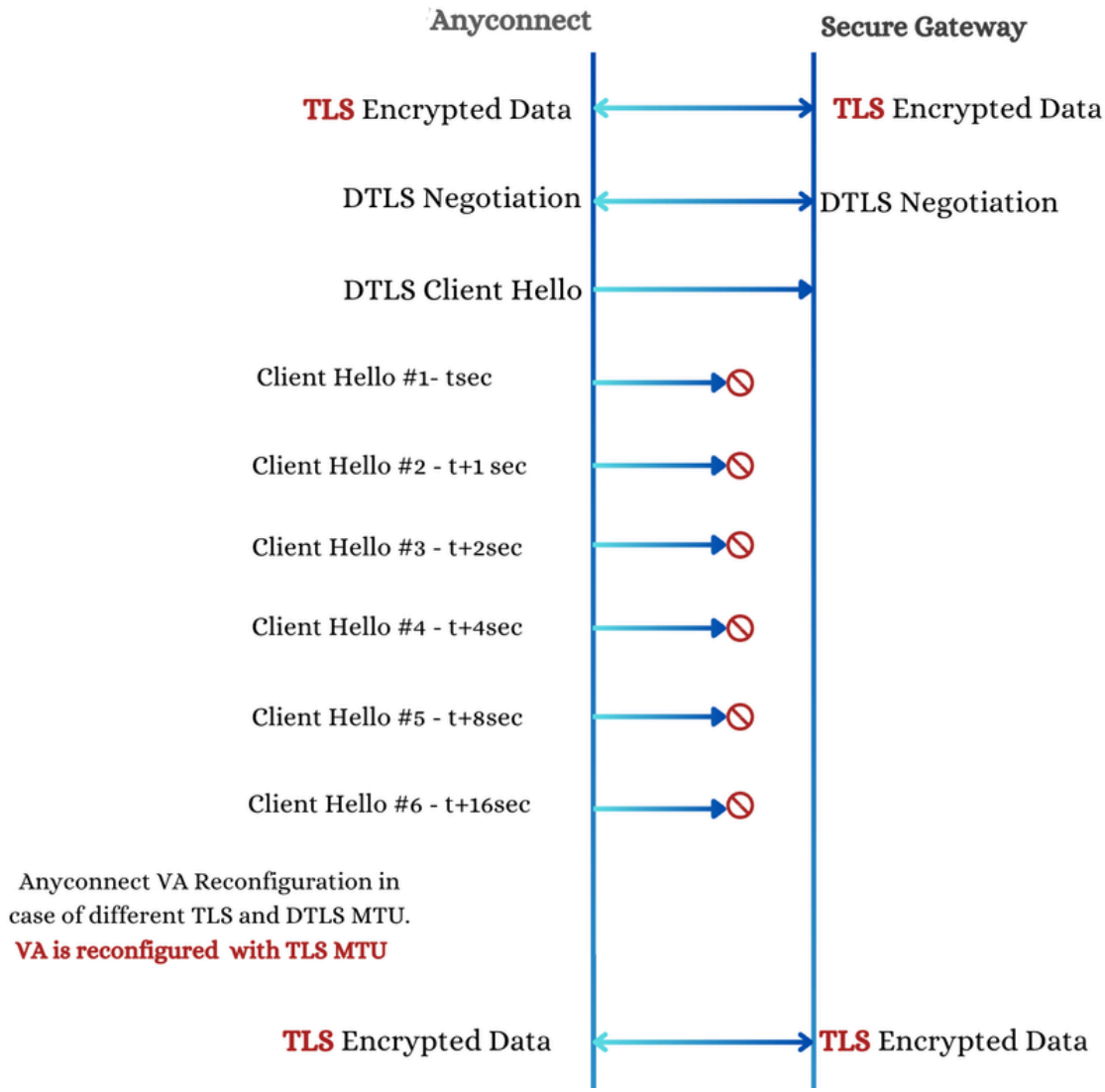


DTLS-handdruk

6.1. DTLS-poort geblokkeerd

In het geval dat de DTLS-poort wordt geblokkeerd of de Secure Gateway niet reageert op DTLS Client Hello-pakketten, voert AnyConnect een exponentiële back-up uit met maximaal vijf herhalingen, te beginnen met een vertraging van 1 seconde en oplopend tot 16 seconden.

Als deze pogingen niet succesvol zijn, past AnyConnect vervolgens het eigenlijke TLS MTU toe, zoals gespecificeerd door de X-CSTP-MTU-waarde die door de beveiligde gateway in fase 5 wordt geretourneerd, op de AnyConnect virtuele adapter. Aangezien deze MTU verschilt van de eerder toegepaste MTU (X-DTLS-MTU), is een herconfiguratie van de virtuele adapter noodzakelijk. Deze herconfiguratie wordt door de eindgebruiker weergegeven als een poging om verbinding te maken, hoewel er tijdens dit proces geen nieuwe onderhandelingen plaatsvinden. Wanneer de virtuele adapter opnieuw is geconfigureerd, blijft het TLS-gegevenskanaal actief.



DTLS-poortblok

Gerelateerde informatie

- Documentatiereferentie voor Cisco VPN-technologieën
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.