Información sobre el Flujo de Conexión VPN SSL de AnyConnect

Contenido

Introducción

Este documento se centra en el flujo de eventos que tienen lugar entre AnyConnect y el gateway seguro durante una conexión SSLVPN.

Antecedentes

AnyConnect

AnyConnect es el cliente Cisco VPN diseñado para los protocolos SSL e IKEv2. Está disponible para la mayoría de las plataformas de escritorio y móviles. AnyConnect establece principalmente conexiones seguras con Firepower Threat Defence (FTD), Adaptive Security Appliances (ASA) o routers Cisco IOS®/Cisco IOS® XE denominados gateways seguros.

Gateway seguro

En la terminología de Cisco, un servidor VPN SSL se denomina gateway seguro, mientras que un

servidor IPSec (IKEv2) se conoce como gateway VPN de acceso remoto. Cisco admite la terminación del túnel SSL VPN en las siguientes plataformas:

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

Flujo de conexión VPN SSL de AnyConnect

Este documento desglosa los eventos que tienen lugar entre AnyConnect y el gateway seguro durante un establecimiento de conexión VPN SSL en seis fases:

1. Protocolo de enlace SSL

2. POST - Selección de grupo

3. POST - Autenticación de usuario con nombre de usuario/contraseña (Opcional)

4. Descargador VPN (opcional)

5. CONEXIÓN CSTP

6. Conexión DTLS (opcional)

1. Protocolo de enlace SSL

El protocolo de enlace SSL es iniciado por el cliente AnyConnect después de la finalización del protocolo de enlace de 3 vías TCP con un mensaje de 'saludo del cliente'. El flujo de eventos y los puntos clave son los mencionados.

Hola de cliente

La sesión SSL comienza cuando el cliente envía un mensaje de 'Saludo del cliente'. En este mensaje:

a) El ID de sesión SSL se establece en 0, lo que indica el inicio de una nueva sesión.

b) La carga útil incluye los conjuntos de cifrado admitidos por el cliente y un nonce aleatorio generado por el cliente.

Hola de servidor

El servidor responde con un mensaje de "Saludo del servidor", que incluye:

a) El conjunto de cifrado seleccionado de la lista proporcionada por el cliente.

b) El servidor generó el ID de sesión SSL y un servidor generó un nonce aleatorio.

Certificado de servidor

Después de "Server Hello", el servidor transmite su certificado SSL, que sirve como su identidad. Entre los puntos clave a tener en cuenta se incluyen:

a) Si este certificado no supera una comprobación de validación estricta, AnyConnect bloquea el servidor de forma predeterminada.

b) El usuario tiene la opción de desactivar este bloque, pero las conexiones posteriores muestran una advertencia hasta que se resuelven los errores notificados.

Solicitud de certificado de cliente

El servidor también puede solicitar un certificado de cliente y enviar una lista de DN de nombre de sujeto de todos los certificados de CA cargados en el gateway seguro. Esta solicitud tiene dos fines:

a) Ayuda al cliente (usuario) a elegir el certificado de identidad correcto si hay varios certificados de ID disponibles.

b) Garantiza que el certificado devuelto es de confianza para Secure Gateway, aunque debe seguir produciéndose la validación del certificado.

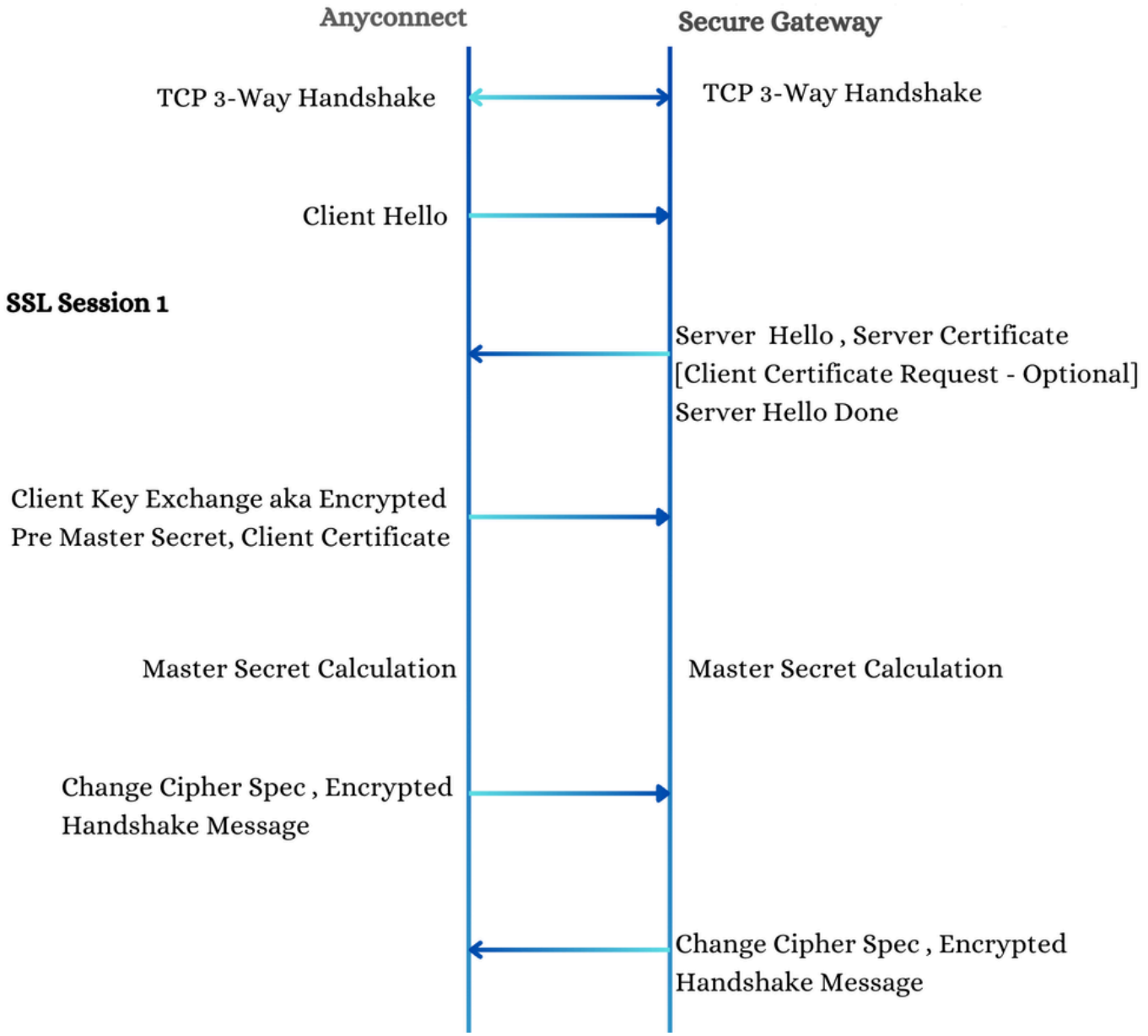
Intercambio de claves de cliente

A continuación, el cliente envía un mensaje de 'Intercambio de claves de cliente', que incluye una clave secreta anterior a la maestra. Esta clave se cifra mediante:

a) La clave pública del servidor del certificado del servidor, si el conjunto de cifrado seleccionado está basado en RSA (por ejemplo, TLS_RSA_WITH_AES_128_CBC_SHA).

b) La clave pública DH del servidor proporcionada en el mensaje de saludo del servidor, si el conjunto de cifrado seleccionado está basado en DHE (por ejemplo, TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Basándose en el secreto anterior al maestro, el nonce aleatorio generado por el cliente y el nonce aleatorio generado por el servidor, tanto el cliente como el gateway seguro generan independientemente un secreto maestro. Este secreto principal se utiliza para derivar claves de sesión, lo que garantiza una comunicación segura entre el cliente y el servidor.



Sesión SSL 1

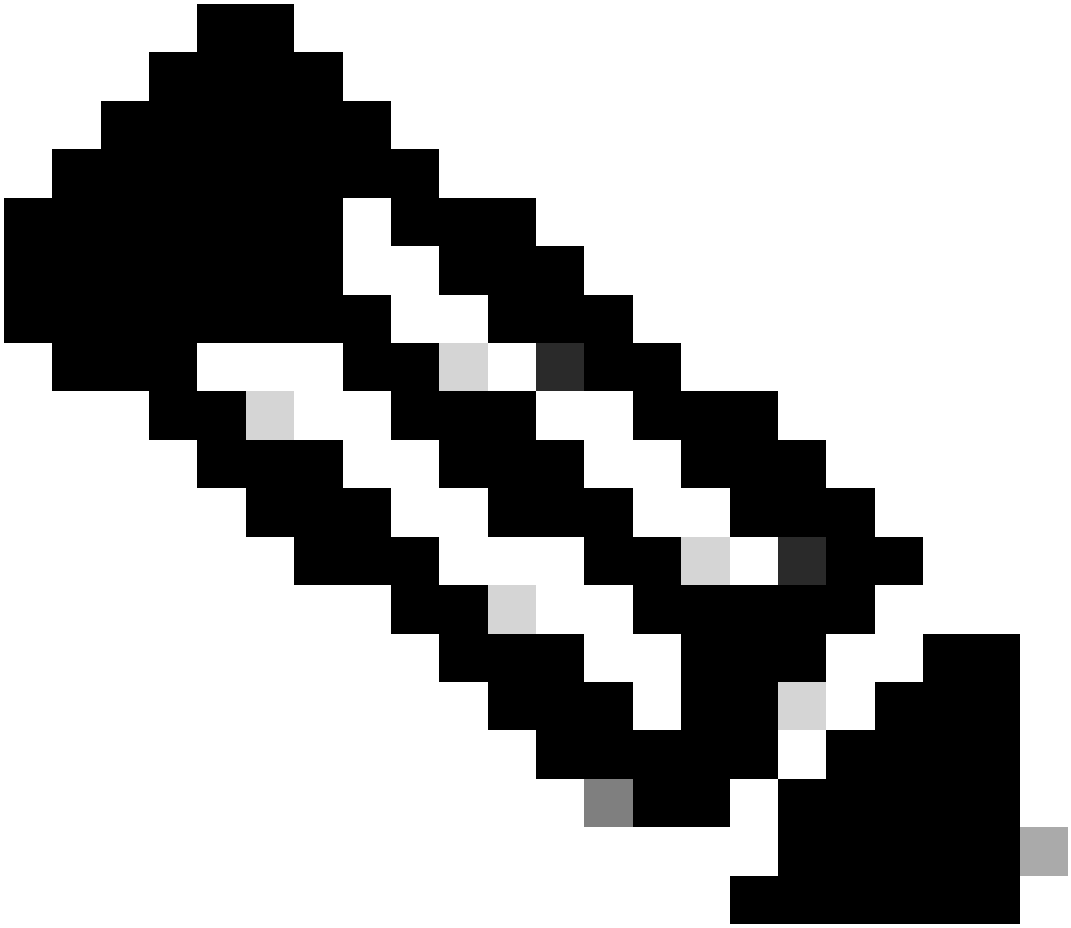
2. POST - Selección de grupo

Durante esta operación, el cliente no posee información sobre el perfil de conexión a menos que lo especifique explícitamente el usuario. El intento de conexión se dirige a la URL de gateway seguro (asav.cisco.com), como indica el elemento 'group-access' en la solicitud. El cliente indica su soporte para la versión 2 de 'aggregate-authentication'. Esta versión representa una mejora significativa con respecto a la versión anterior, especialmente en términos de transacciones XML eficaces. Tanto el gateway seguro como el cliente deben coincidir en la versión que se va a utilizar. En los escenarios en los que el gateway seguro no admite la versión 2, se activa una operación POST adicional, lo que hace que el cliente recurra a la versión anterior.

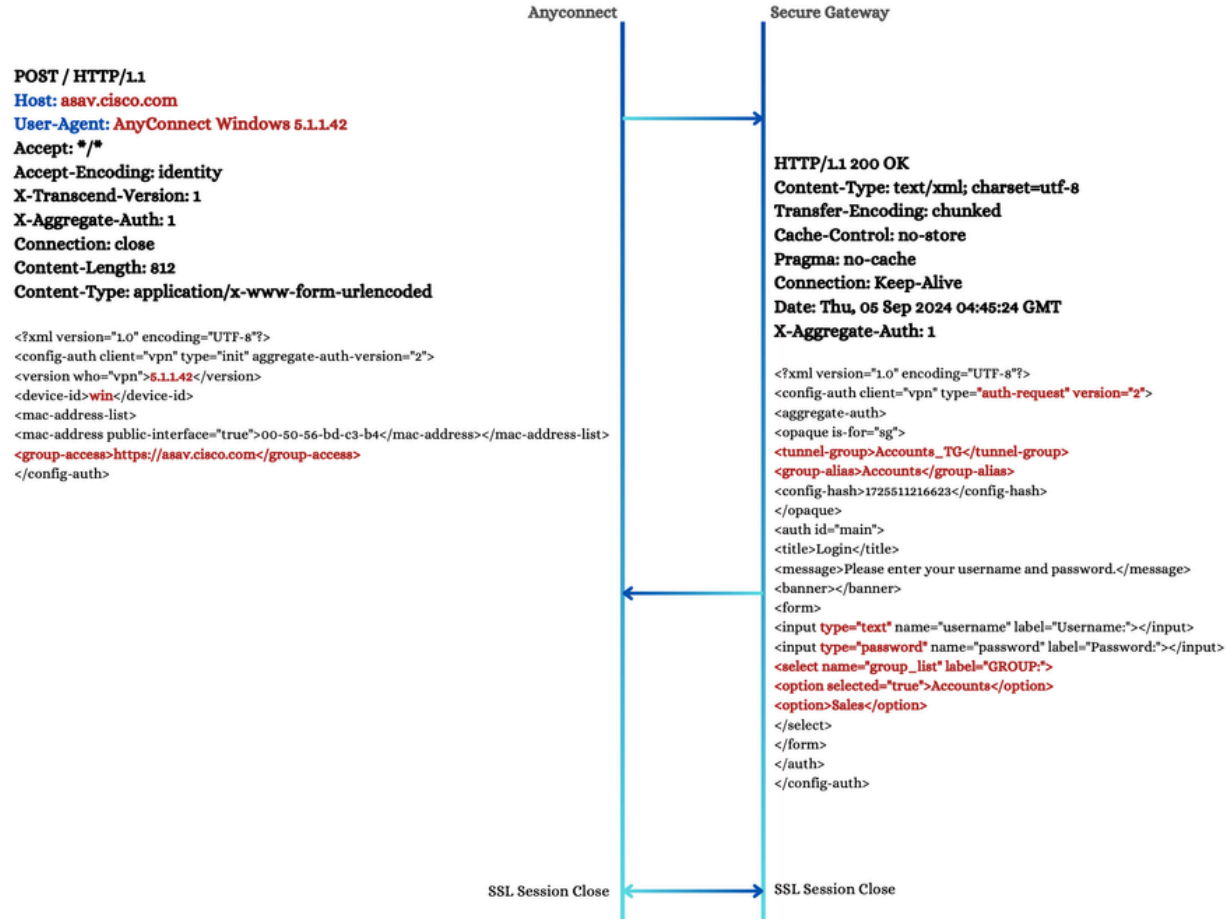
En la respuesta HTTP, el gateway seguro indica lo siguiente:

1. La versión de autenticación agregada que admite el gateway seguro.

2. Lista de grupos de túneles y la pantalla Nombre de usuario/Contraseña.

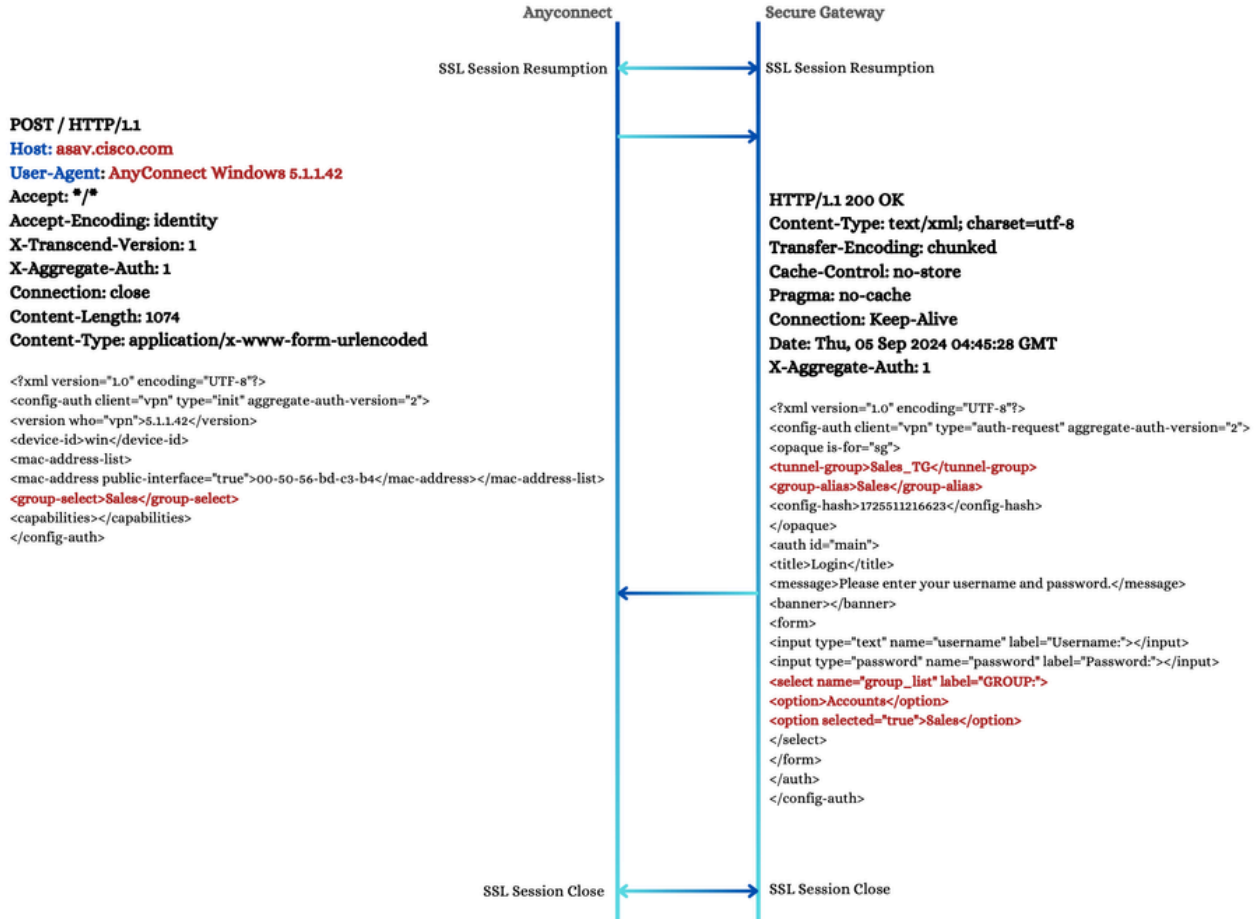


Nota: El formulario incluye un elemento 'select', que enumera los alias de grupo de todos los perfiles de conexión configurados en el gateway seguro. De forma predeterminada, uno de estos alias de grupo se resalta con el atributo booleano seleccionado = "true". Los elementos tunnel-group y group-alias corresponden a este perfil de conexión seleccionado.



POST - Selección de grupo 1

Si el usuario elige un perfil de conexión diferente de esta lista, se realiza otra operación POST. En este caso, el cliente envía una solicitud POST con el elemento 'group-select' actualizado para reflejar el perfil de conexión elegido, como se muestra aquí.



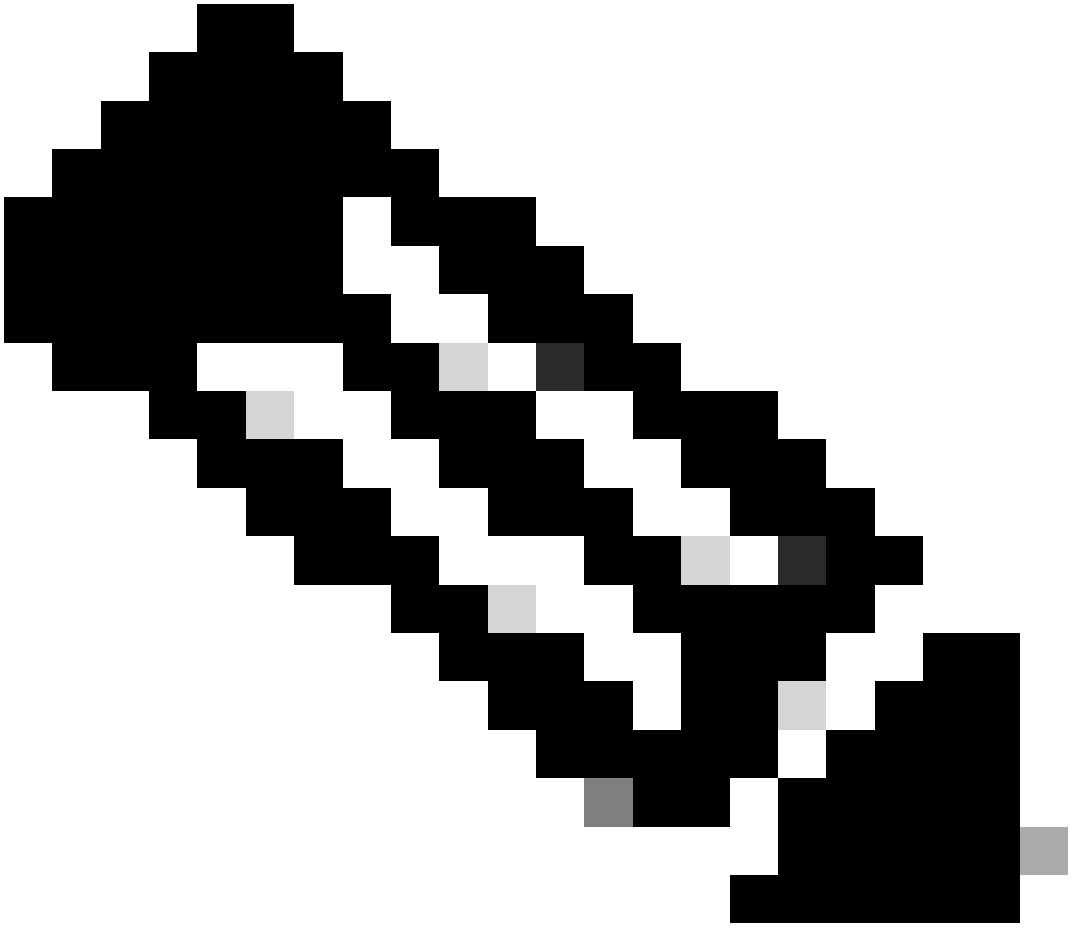
POST - Selección de grupo 2

3. POST - Autenticación de usuario

En esta operación, que sigue a la selección de grupo posterior, AnyConnect envía esta información al gateway seguro:

1. Información de Perfil de Conexión Seleccionada: Incluye el nombre del grupo de túnel y el alias del grupo tal como lo indicó el gateway seguro en la operación anterior.

2. Nombre de usuario y Contraseña: Credenciales de autenticación del usuario.



Nota: Dado que este flujo es específico de la autenticación AAA, puede diferir de otros métodos de autenticación.

En respuesta a la operación POST, Secure Gateway envía un archivo XML que contiene esta información:

1. Id. de sesión: No es lo mismo que el Id. de sesión SSL.

2. Token de sesión: Este token es utilizado más tarde por el cliente como la cookie de WebVPN.

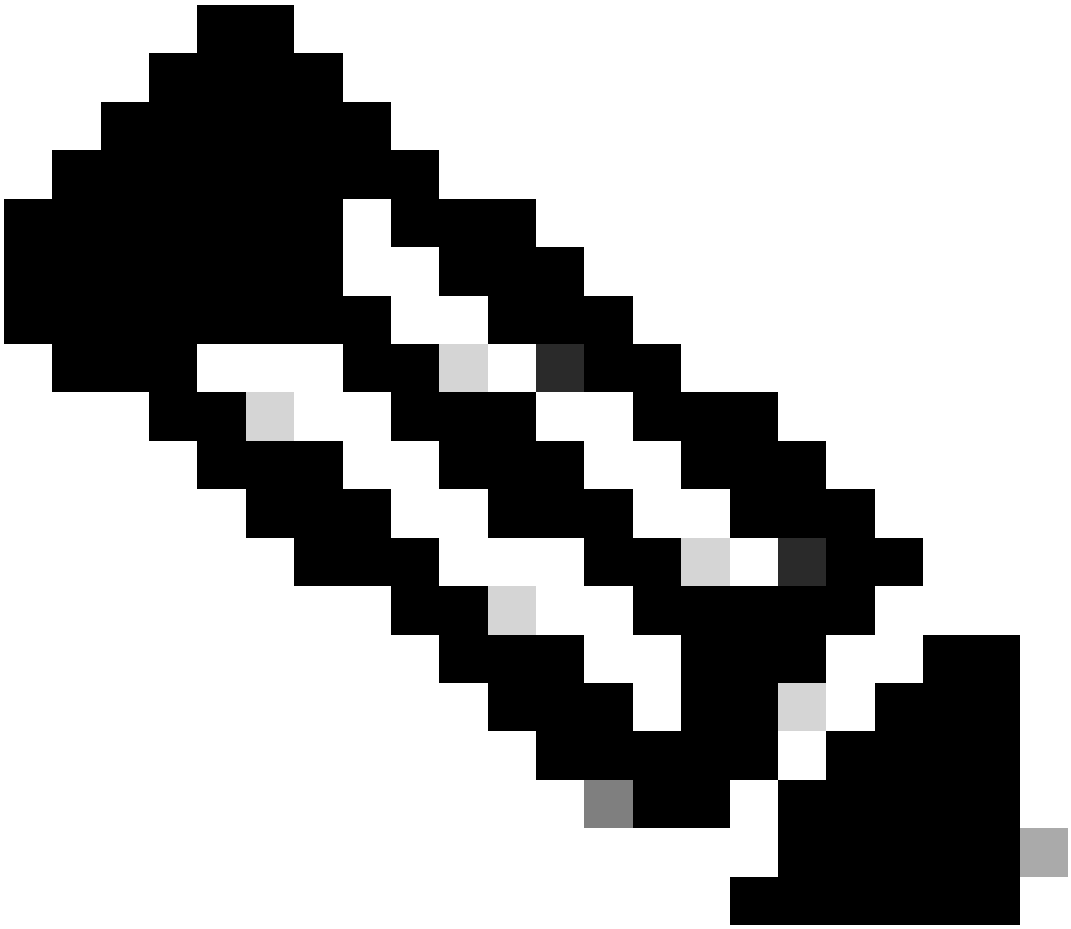
3. Estado de autenticación: indicado por un elemento auth con id = 'success'.

4. Hash de certificado de servidor: Este hash se almacena en caché en el archivo preferences.xml.

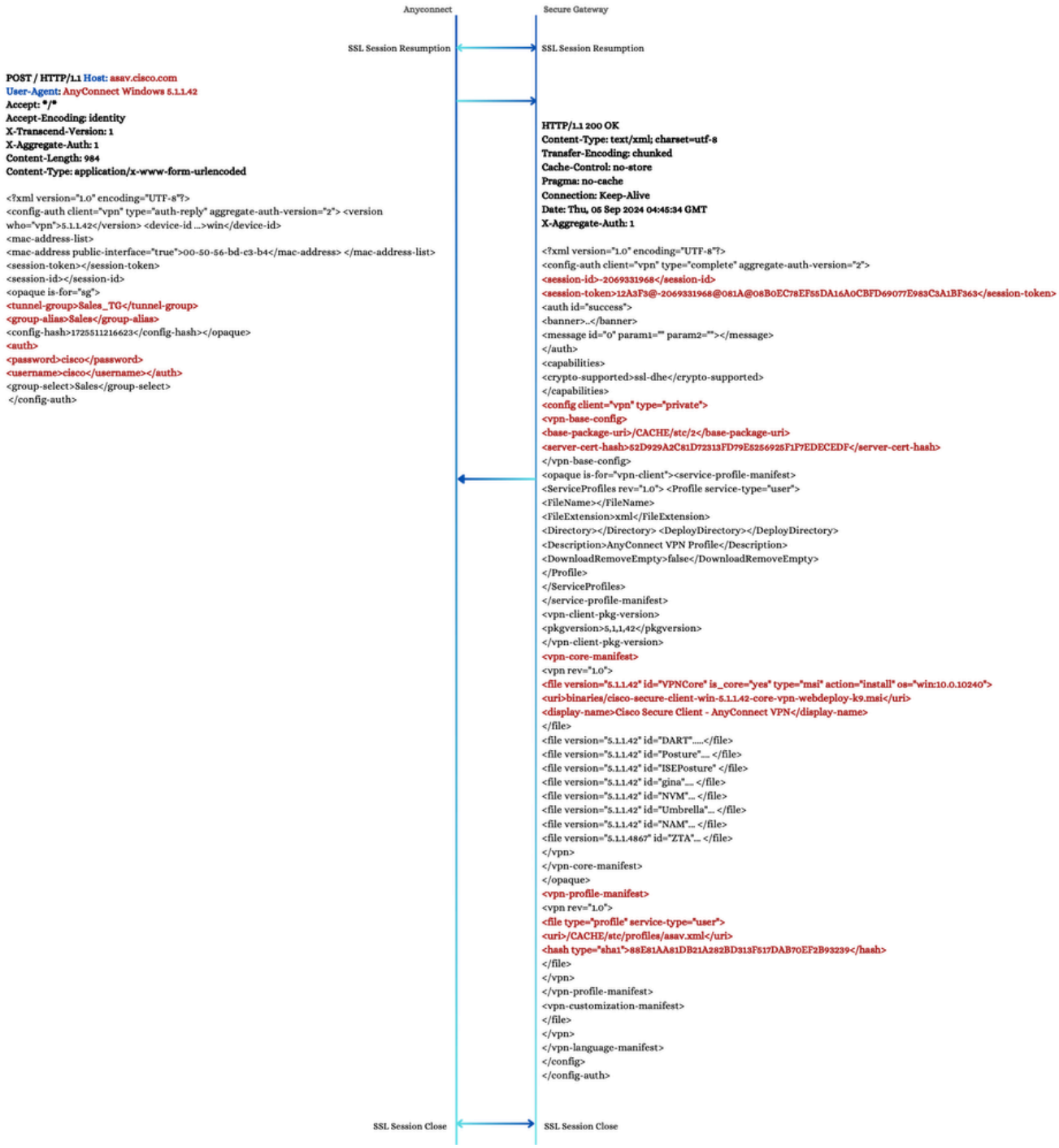
5. Elemento vpn-core-manifest: Este elemento indica la ruta y la versión del paquete de núcleo de AnyConnect, junto con otros componentes como Dart, Postura, Postura de ISE, etc. El

descargador de VPN lo utiliza en la siguiente sección.

6. Elemento vpn-profile-manifest: Este elemento indica la ruta de acceso (el nombre del perfil) y el hash SHA-1 del perfil.



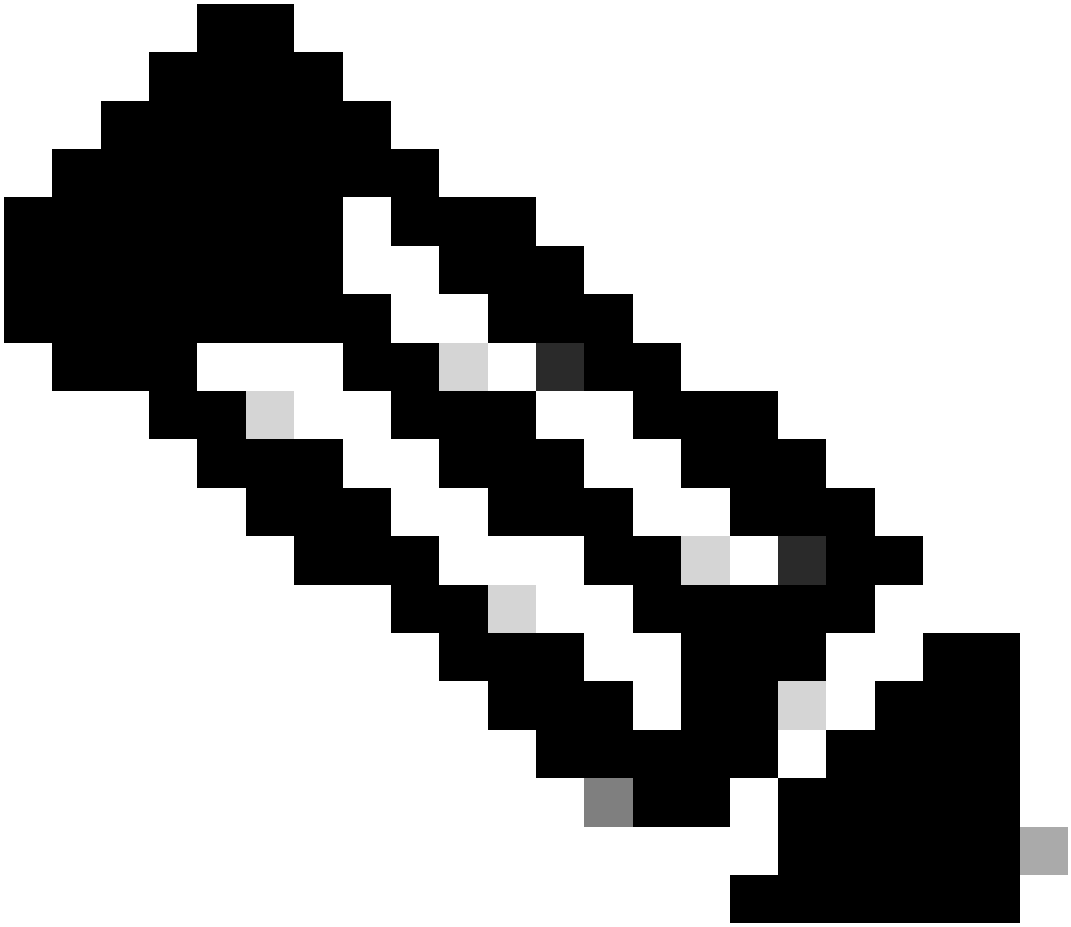
Nota: Si el cliente no tiene el perfil, el Descargador de VPN en la siguiente sección lo descarga. Si el cliente ya tiene el perfil, el hash SHA-1 del perfil del cliente se compara con el del servidor. En caso de una discordancia, el Descargador de VPN sobrescribe el perfil del cliente con el de la puerta de enlace segura. Esto garantiza que el perfil de la puerta de enlace segura se aplica en la autenticación posterior del cliente.



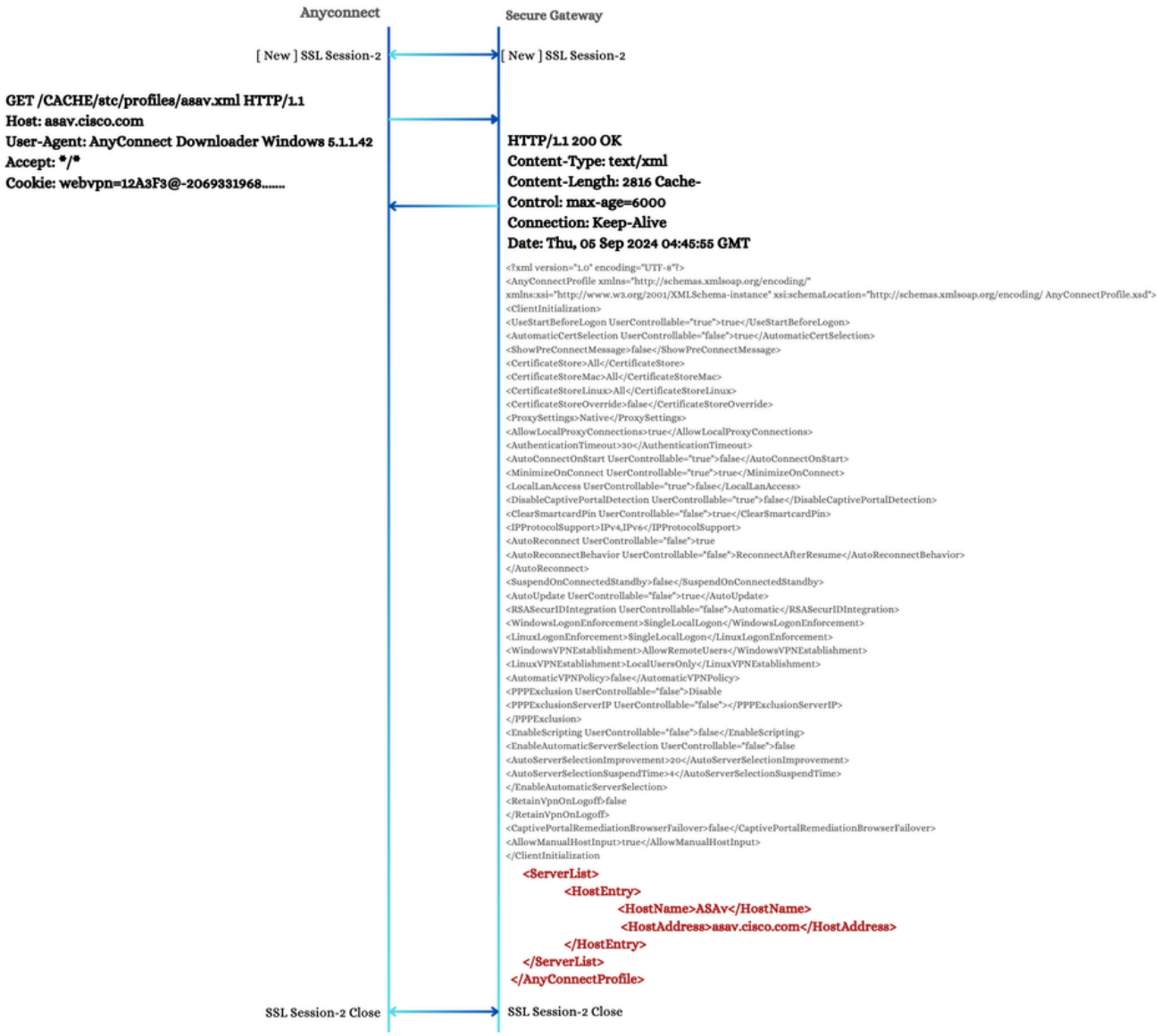
POST: autenticación de usuario

4. Descargador AnyConnect

AnyConnect Downloader siempre inicia una nueva sesión SSL, por lo que los usuarios pueden encontrar una segunda advertencia de certificado si el certificado de Secure Gateway no es de confianza. Durante esta fase, realiza operaciones GET independientes para cada elemento que debe descargarse.



Nota: si el perfil del cliente se carga en Secure Gateway, es obligatorio descargarlo; de lo contrario, se finaliza todo el intento de conexión.

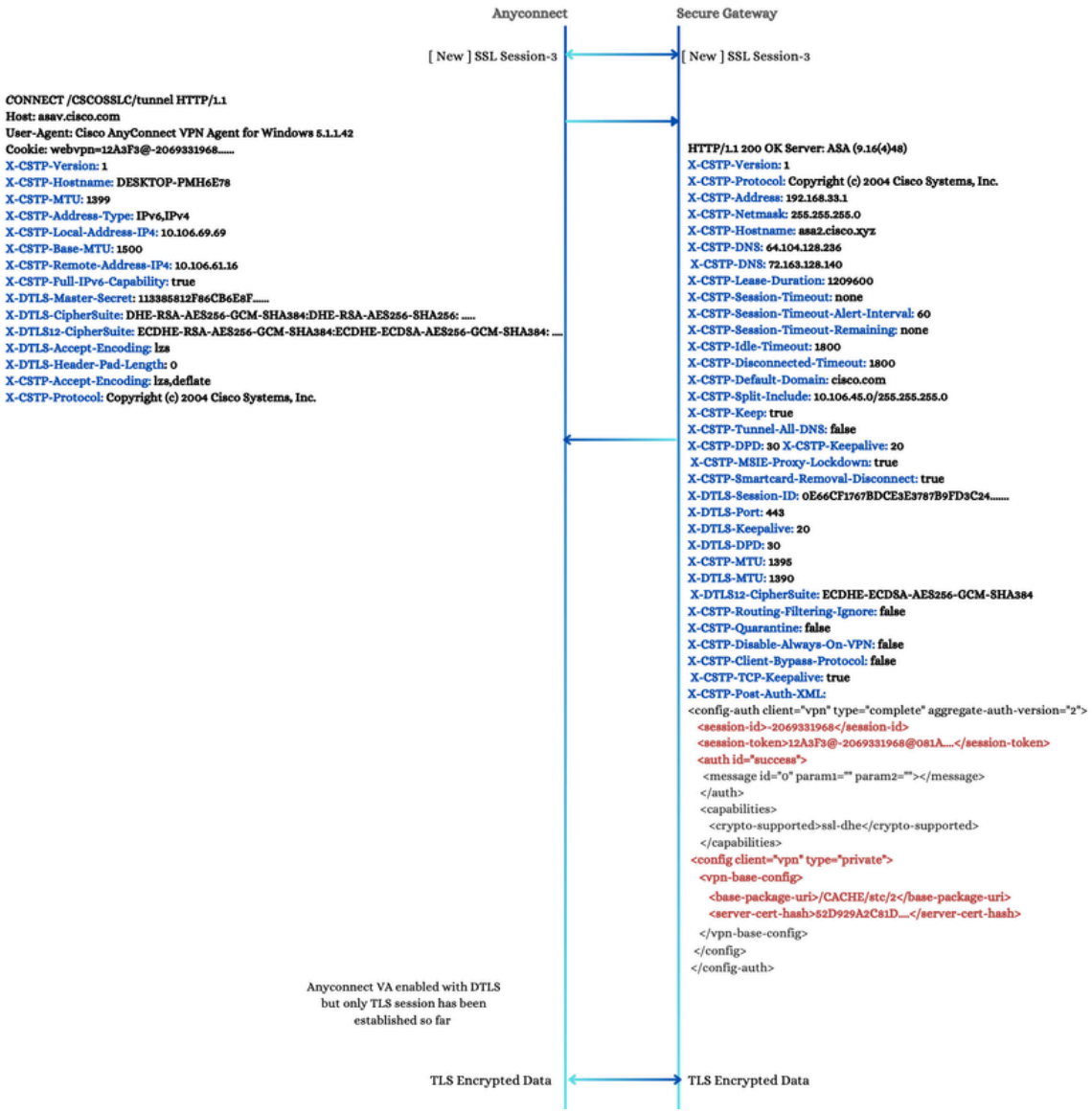


Descargador de VPN

5. CONEXIÓN CSTP

AnyConnect realiza una operación CONNECT como el paso final para establecer un canal seguro. Durante la operación CONNECT, el cliente AnyConnect envía varios atributos X-CSTP y X-DTLS para el gateway seguro para procesar. Secure Gateway responde con atributos X-CSTP y X-DTLS adicionales que el cliente aplica al intento de conexión actual. Este intercambio incluye X-CSTP-Post-Auth-XML, acompañado de un archivo XML, que es en gran medida similar al que se ve en el paso POST - User Authentication.

Después de recibir una respuesta satisfactoria, AnyConnect inicia el canal de datos TLS. Simultáneamente, la interfaz del adaptador virtual de AnyConnect se activa con un valor de MTU igual a X-DTLS-MTU, suponiendo que el intercambio de señales DTLS subsiguiente sea exitoso.



Conexión CSTP

6. Protocolo de enlace DTLS

El protocolo de enlace DTLS continúa tal y como se describe aquí. Esta configuración es relativamente rápida debido a los atributos intercambiados entre el cliente y el servidor durante el evento CONNECT.

Cliente

X-DTLS-Master-Secret: el cliente genera el secreto principal de DTLS y lo comparte con el servidor. Esta clave es crucial para establecer una sesión DTLS segura.

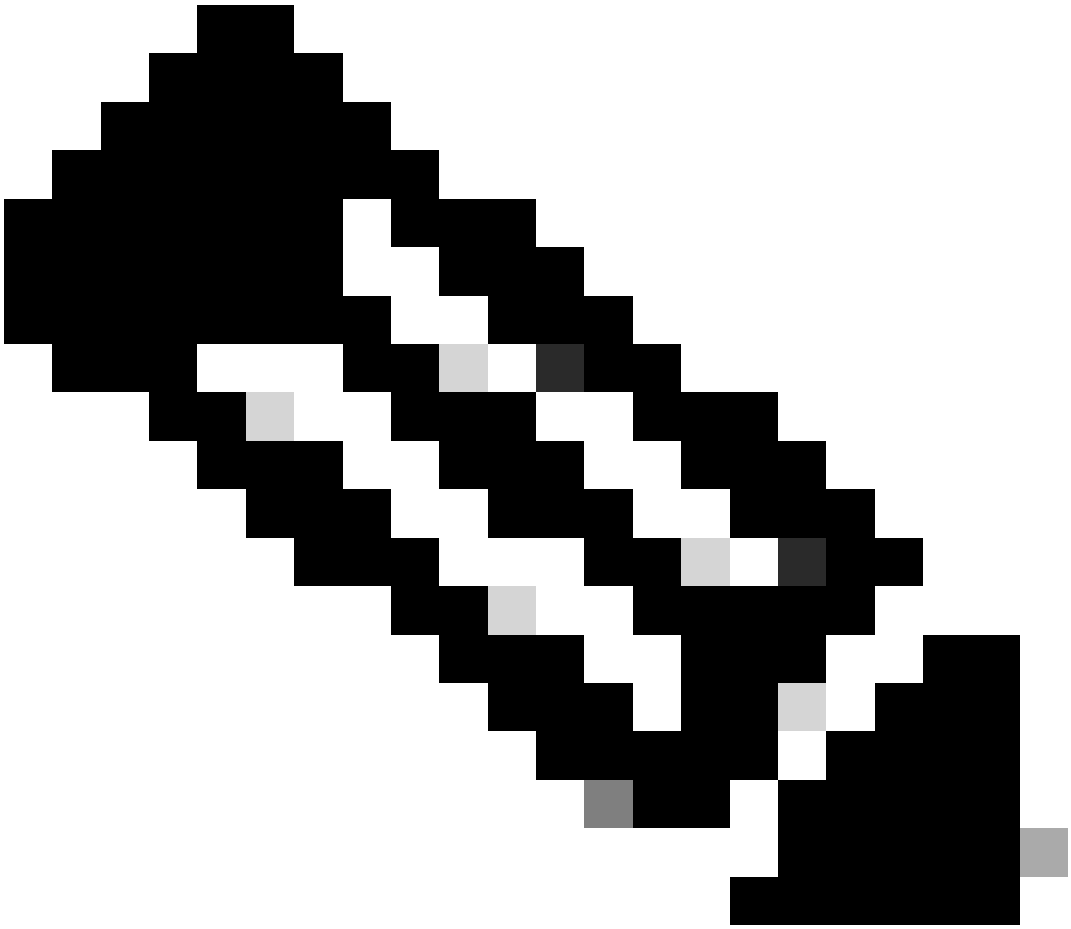
X-DTLS-CypherSuite: lista de conjuntos de cifrado DTLS admitidos por el cliente, que indica las capacidades de cifrado del cliente.

Servidor

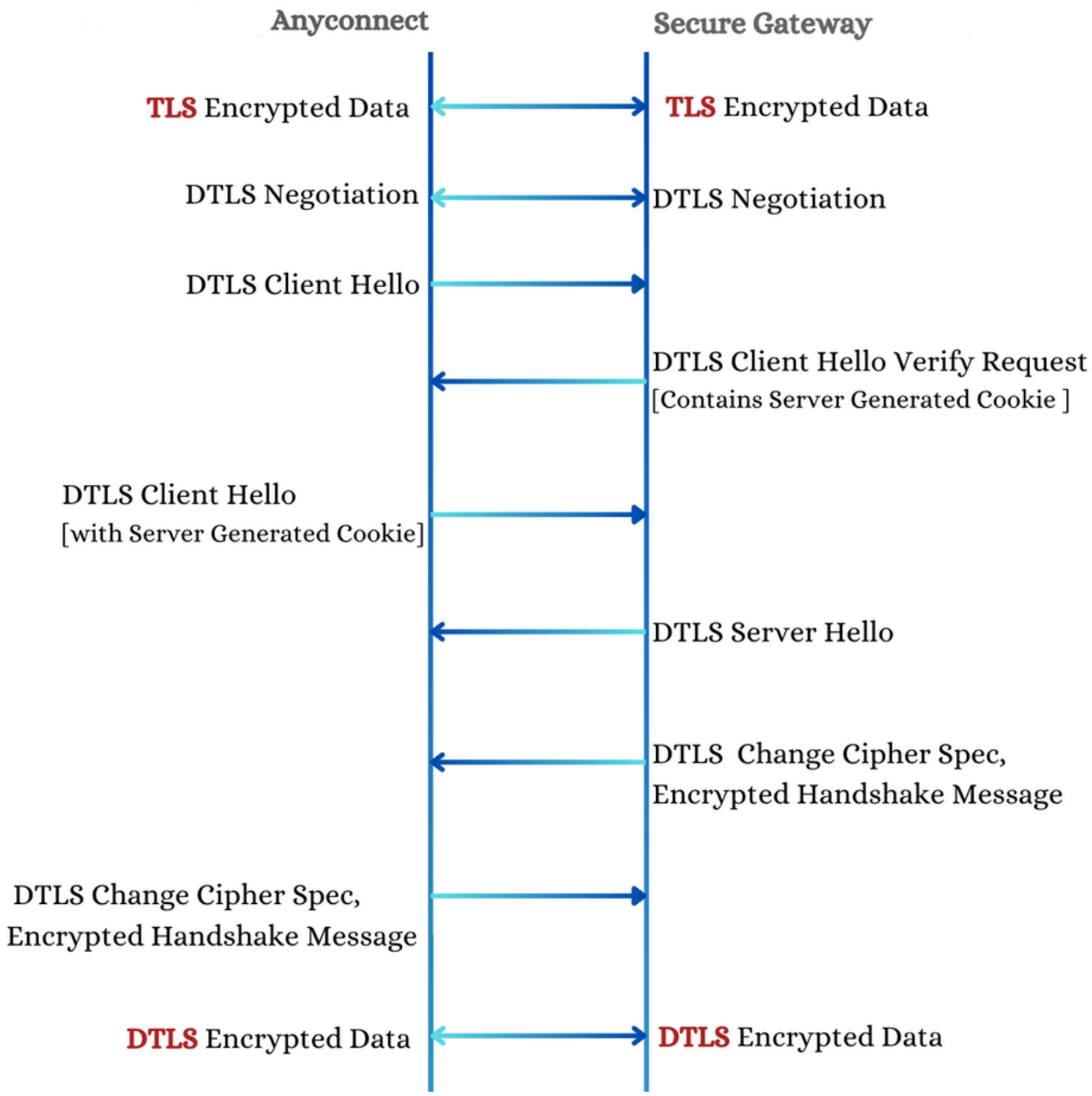
X-DTLS-Session-ID: Identificador de sesión DTLS asignado por el servidor para que lo utilice el

cliente, lo que garantiza la continuidad de la sesión.

X-DTLS-CipherSuite: conjunto de cifrado seleccionado por el servidor de la lista proporcionada por el cliente, que garantiza que ambas partes utilizan un método de cifrado compatible.



Nota: mientras el intercambio de señales DTLS está en curso, el canal de datos TLS continúa funcionando. Esto garantiza que la transmisión de datos sea uniforme y segura durante el proceso de intercambio de señales. Una transición sin problemas al canal de cifrado de datos DTLS solo se produce después de que se haya completado el intercambio de señales DTLS.

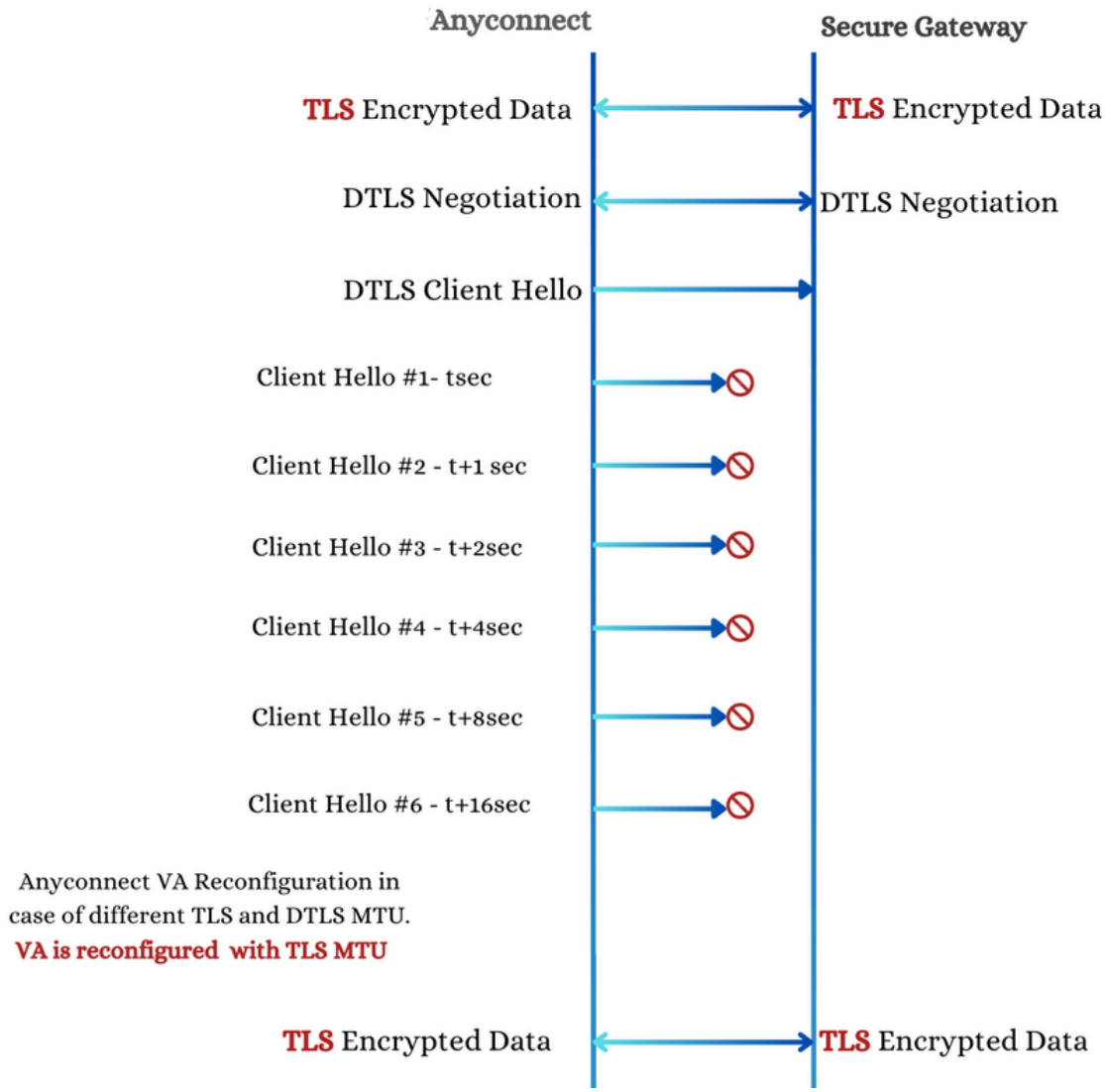


Protocolo de enlace DTLS

6.1. Puerto DTLS bloqueado

En caso de que el puerto DTLS se bloquee o el gateway seguro no pueda responder a los paquetes Hello del cliente DTLS, AnyConnect realiza un backoff exponencial con hasta cinco reintentos, comenzando con un retardo de 1 segundo y aumentando hasta 16 segundos.

Si estos intentos no tienen éxito, AnyConnect aplica la MTU de TLS real, según lo especificado por el valor X-CSTP-MTU devuelto por el gateway seguro en la fase 5.0, al adaptador virtual de AnyConnect. Dado que esta MTU difiere de la MTU aplicada anteriormente (X-DTLS-MTU), es necesario volver a configurar el adaptador virtual. Esta reconfiguración aparece para el usuario final como un intento de reconexión, aunque no se producen nuevas negociaciones durante este proceso. Una vez reconfigurado el adaptador virtual, el canal de datos TLS continúa funcionando.



Bloque de puerto DTLS

Información Relacionada

- Referencia de documentación de Cisco VPN Technologies
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).