Entendendo o fluxo de conexão do AnyConnect SSL VPN

Contents

Introdução

Este documento enfoca o fluxo de eventos que ocorrem entre o AnyConnect e o gateway seguro durante uma conexão SSLVPN.

Informações de Apoio

AnyConnect

O AnyConnect é o cliente VPN da Cisco projetado para protocolos SSL e IKEv2. Ele está disponível para a maioria das plataformas móveis e de desktop. O AnyConnect estabelece principalmente conexões seguras com Firepower Threat Defense (FTD), Adaptive Security Appliances (ASA) ou roteadores Cisco IOS®/Cisco IOS® XE conhecidos como Gateways seguros.

Gateway seguro

Na terminologia da Cisco, um servidor VPN SSL é conhecido como um gateway seguro, enquanto um servidor IPSec (IKEv2) é conhecido como um gateway VPN de acesso remoto. A Cisco suporta terminação de túnel VPN SSL nestas plataformas:

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

Fluxo de conexão do AnyConnect SSL VPN

Este documento divide os eventos que ocorrem entre o AnyConnect e o Secure Gateway durante o estabelecimento de uma conexão VPN SSL em seis fases:

1. Handshake SSL

2. POST - Seleção de grupos

3. POST - Autenticação de Usuário com Nome de Usuário/Senha (Opcional)

4. Downloader VPN (Opcional)

5. CONEXÃO CSTP

6. Conexão DTLS (opcional)

1. Handshake de SSL

O handshake SSL é iniciado pelo cliente AnyConnect após a conclusão do handshake triplo do TCP com uma mensagem "Client Hello". O fluxo de eventos e os pontos principais são mencionados.

Client Hello

A sessão SSL começa com o cliente enviando uma mensagem 'Hello do cliente'. Nesta mensagem:

a) O ID da Sessão SSL é definido como 0, indicando o início de uma nova sessão.

b) O payload inclui pacotes de cifras suportados pelo cliente e um nonce aleatório gerado pelo cliente.

Server Hello

O servidor responde com uma mensagem "Hello do servidor", que inclui:

a) O conjunto de cifras selecionado na lista fornecida pelo cliente.

b) O servidor gerou o ID de sessão SSL e um servidor gerou um nonce aleatório.

Server Certificate

Após o 'Hello do servidor', o servidor transmite seu certificado SSL, que serve como sua identidade. Os pontos principais a serem observados incluem:

a) Se esse certificado falhar em uma verificação de validação estrita, o AnyConnect, por padrão, bloqueia o servidor.

b) O usuário tem a opção de desativar esse bloqueio, mas as conexões subsequentes exibem um aviso até que os erros relatados sejam resolvidos.

Solicitação de certificado do cliente

O servidor também pode solicitar um certificado de cliente, enviando uma lista de DNs de Nome do Requerente de todos os certificados CA carregados no Secure Gateway. Este pedido tem duas finalidades:

a) Ele ajuda o cliente (usuário) a escolher o certificado de identidade correto se houver vários certificados de ID disponíveis.

b) Garante que o certificado retornado seja confiável para o Secure Gateway, embora ainda deva ocorrer uma validação de certificado adicional.

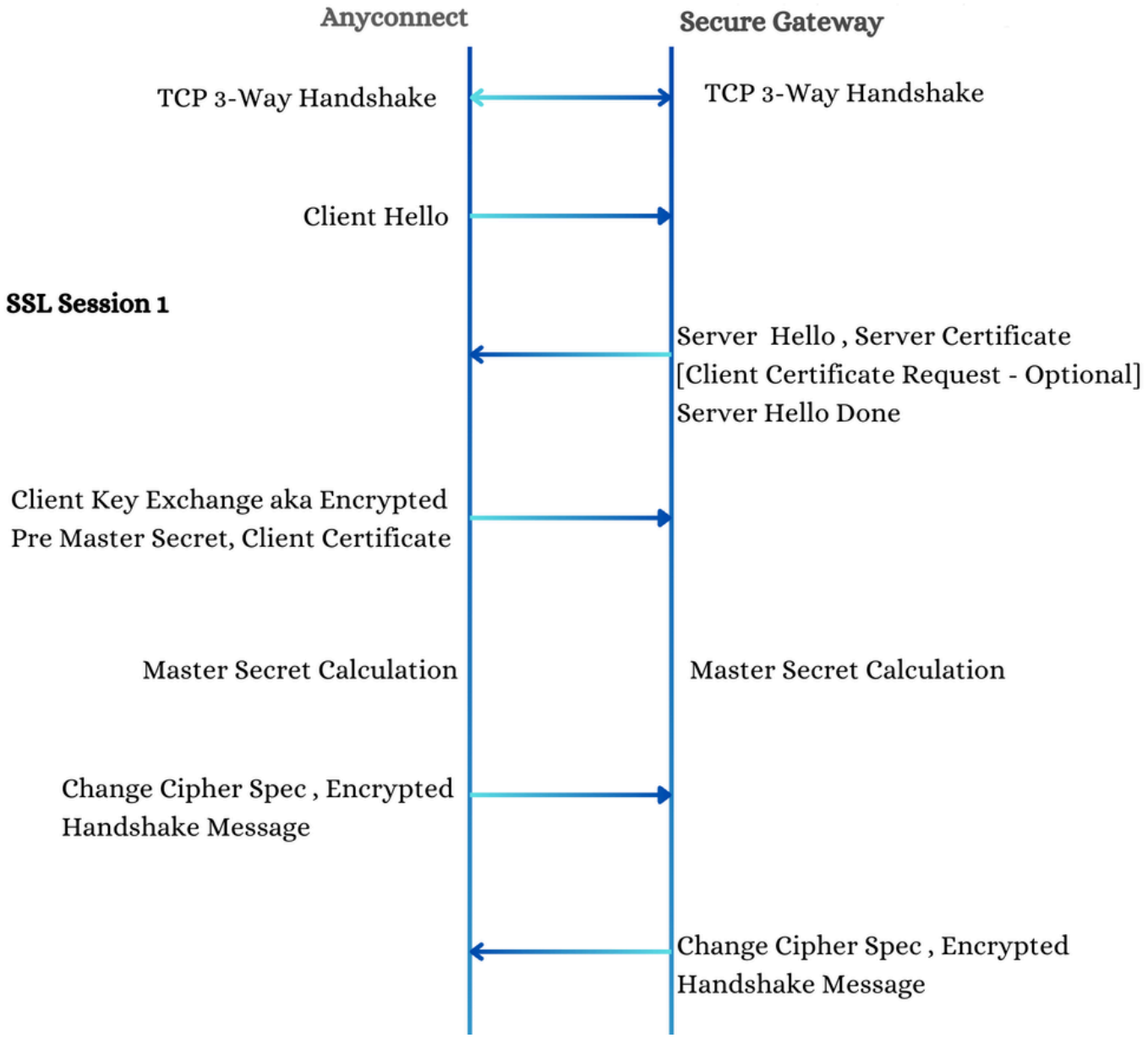
Troca de chave de cliente

Em seguida, o cliente envia uma mensagem 'Client Key Exchange', que inclui uma chave secreta pré-mestre. Esta chave é criptografada usando:

a) A chave pública do servidor do certificado do servidor, se o conjunto de codificação escolhido for baseado em RSA (por exemplo, TLS_RSA_WITH_AES_128_CBC_SHA).

b) A chave pública DH do servidor fornecida na mensagem Hello do servidor, se o conjunto de cifras escolhido for baseado em DHE (por exemplo, TLS_DHE_DSS_WITH_AES_256_CBC_SHA).

Com base no segredo pré-mestre, no nonce aleatório gerado pelo cliente e no nonce aleatório gerado pelo servidor, o cliente e o Gateway Seguro geram independentemente um segredo mestre. Esse segredo mestre é usado para derivar chaves de sessão, garantindo uma comunicação segura entre o cliente e o servidor.



Sessão SSL 1

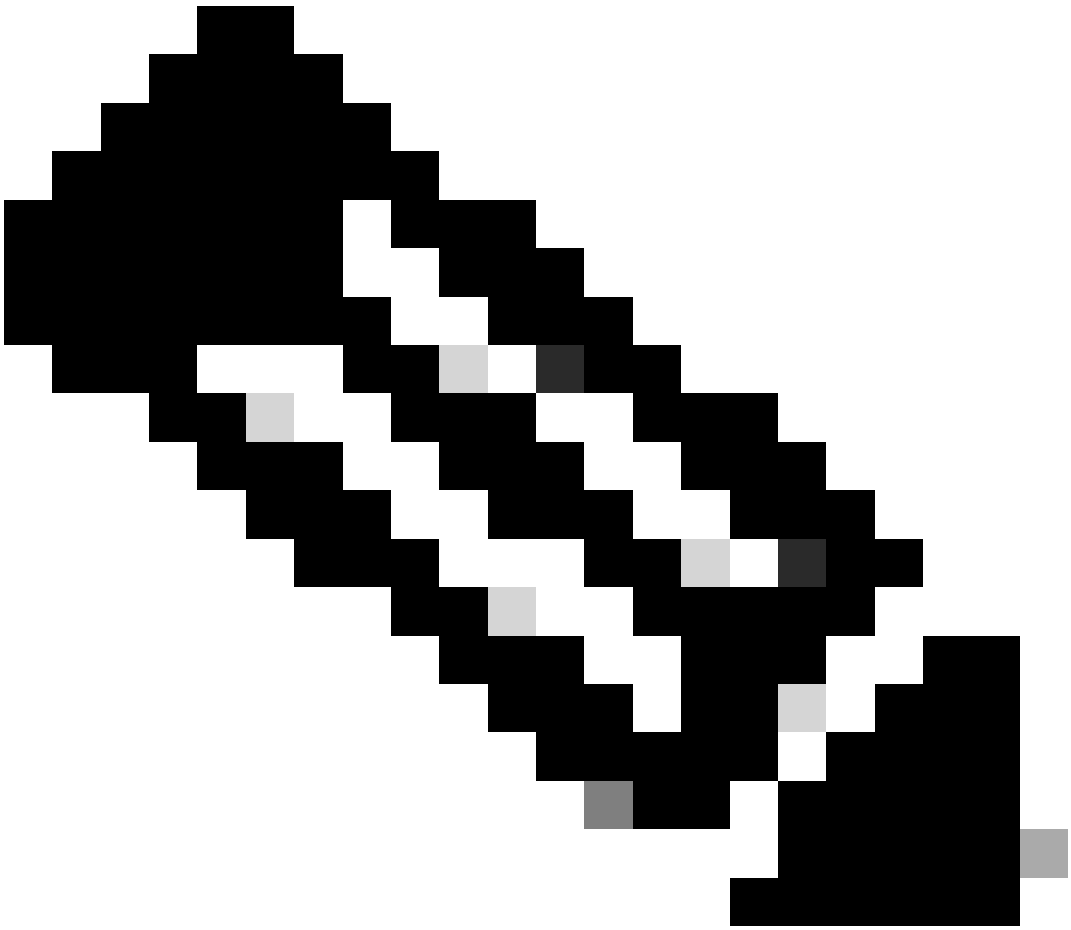
2. POST - Seleção de Grupo

Durante esta operação, o cliente não possui informações sobre o perfil de conexão, a menos que explicitamente especificado pelo usuário. A tentativa de conexão é direcionada para o URL do Secure Gateway (asav.cisco.com), conforme indicado pelo elemento 'group-access' na solicitação. O cliente indica seu suporte para 'aggregate-authentication' versão 2. Esta versão representa uma melhoria significativa em relação à versão anterior, particularmente em termos de transações XML eficientes. Tanto o gateway seguro quanto o cliente devem concordar com a versão a ser usada. Em cenários onde o gateway seguro não suporta a versão 2, uma operação POST adicional é acionada, fazendo com que o cliente retorne para a versão.

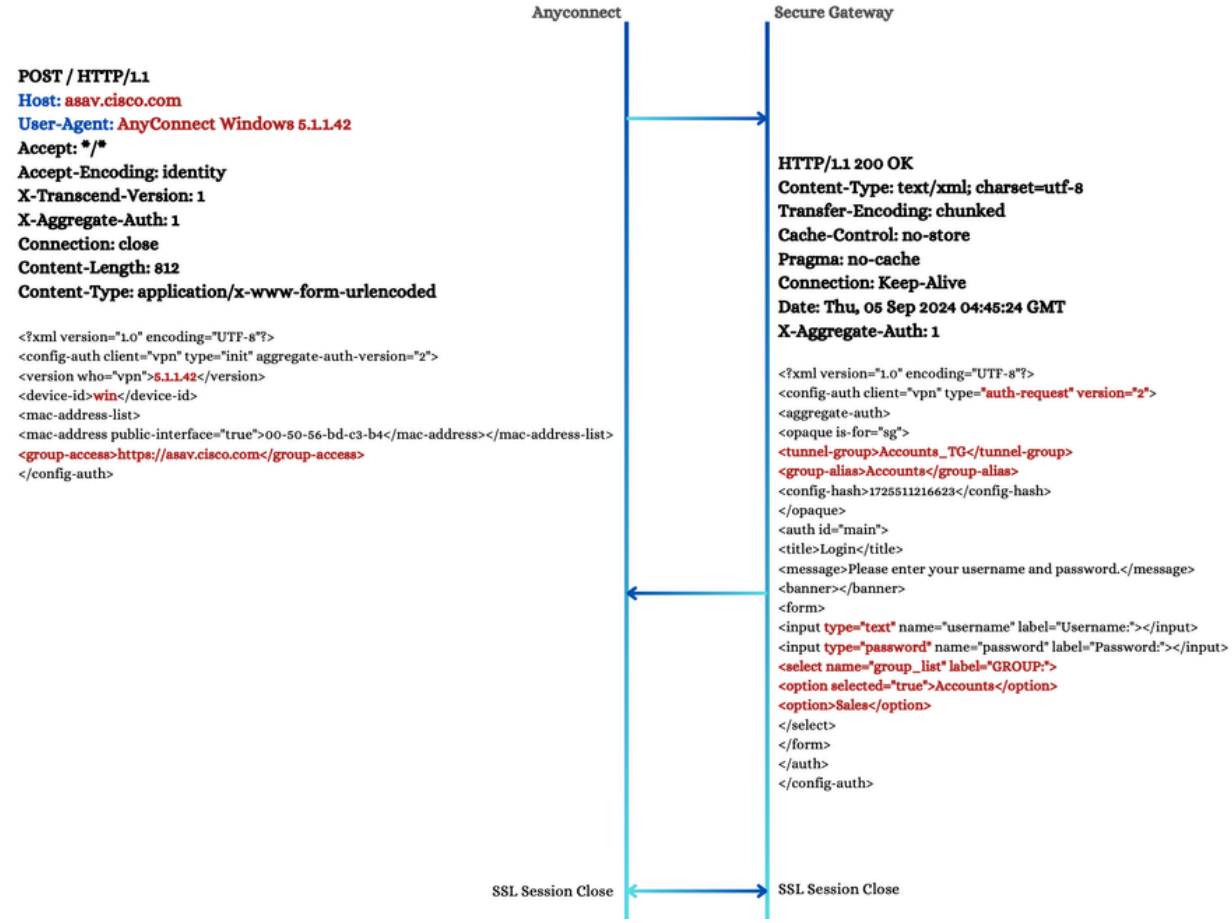
Na resposta HTTP, o gateway seguro indica o seguinte:

1. A versão de autenticação agregada suportada pelo gateway seguro.

2. Lista de grupos de túneis e Formulário de Nome de Usuário/Senha.

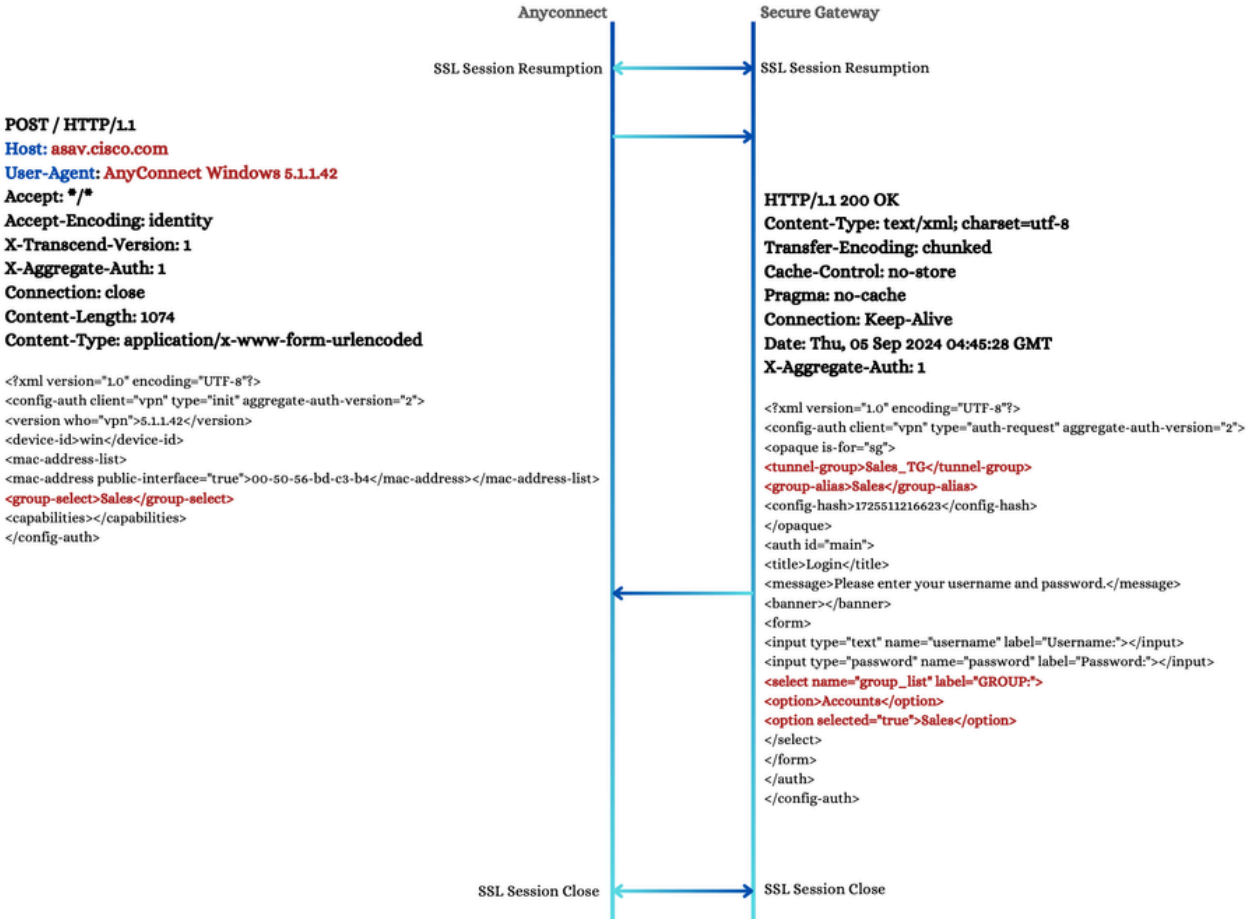


Observação: o formulário inclui um elemento 'select', que lista os aliases de grupo de todos os perfis de conexão configurados no gateway seguro. Por padrão, um desses aliases de grupo é realçado com o atributo booleano selecionado = "true". Os elementos tunnel-group e group-alias correspondem a esse perfil de conexão escolhido.



POST - Seleção de grupo 1

Se o usuário escolher um perfil de conexão diferente desta lista, outra operação POST ocorrerá. Nesse caso, o cliente envia uma solicitação POST com o elemento 'group-select' atualizado para refletir o perfil de conexão escolhido, como mostrado aqui.



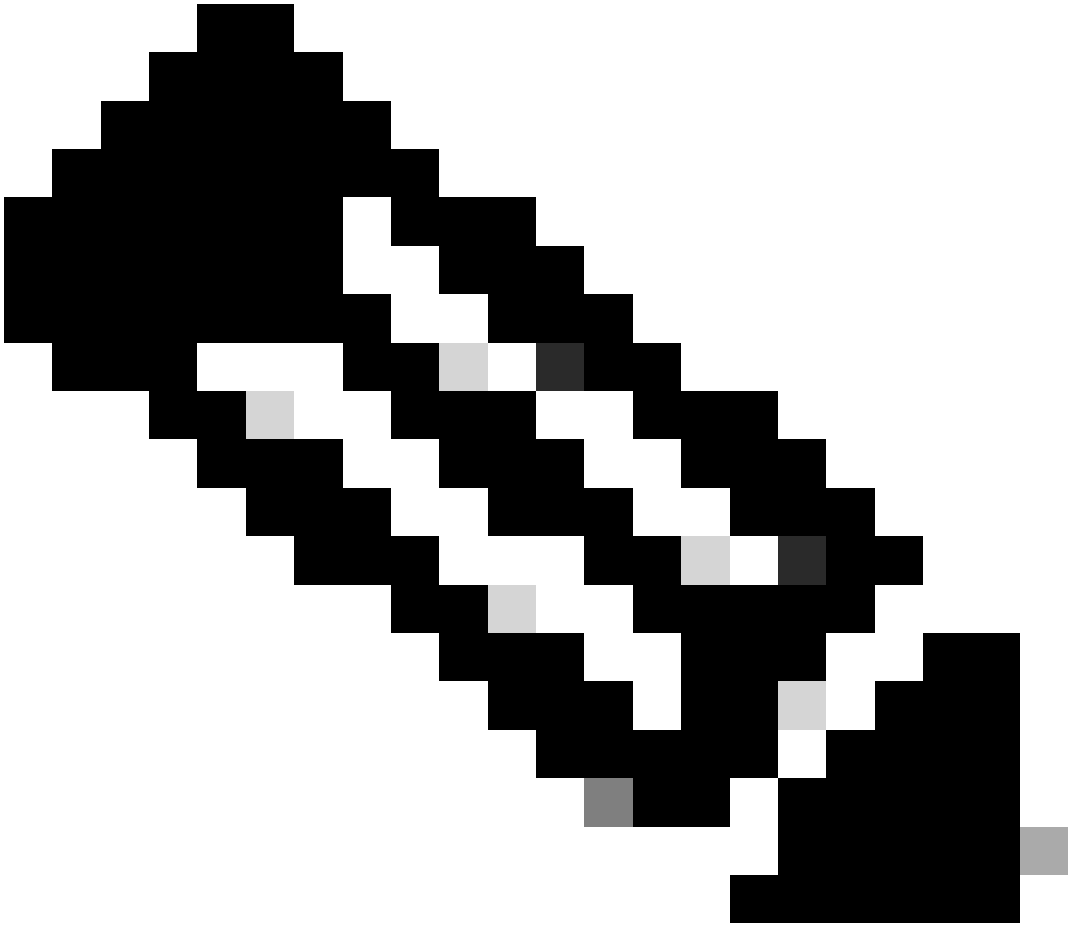
POST - Seleção de grupo 2

3. POST - Autenticação de Usuário

Nessa operação, que segue a Seleção de PÓS-grupo, o AnyConnect envia essas informações ao Gateway Seguro:

1. Informações de Perfil de Conexão Escolhidas: Inclui o nome do grupo de túneis e o apelido do grupo conforme indicado pelo Secure Gateway na operação anterior.

2. Nome de Usuário e Senha: As credenciais de autenticação do usuário.



Observação: como esse fluxo é específico para a autenticação AAA, ele pode diferir de outros métodos de autenticação.

Em resposta à operação POST, o Secure Gateway envia um arquivo XML contendo as seguintes informações:

1. ID da Sessão: Não é o mesmo que o ID da sessão SSL.

2. Token da Sessão: Este token é usado mais tarde pelo cliente como cookie WebVPN.

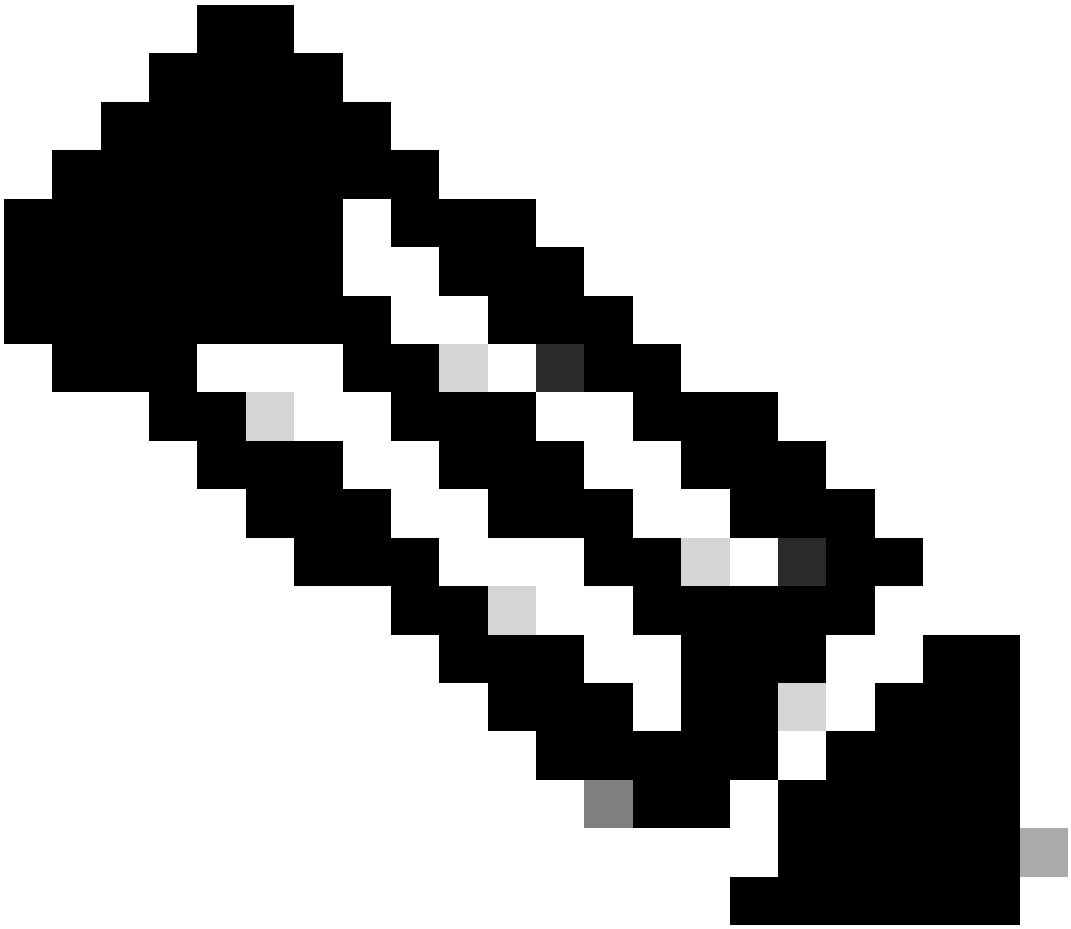
3. Status da Autenticação: Indicado por um elemento auth com id = 'success'.

4. Hash de Certificado do Servidor: Esse hash é armazenado em cache no arquivo preferences.xml.

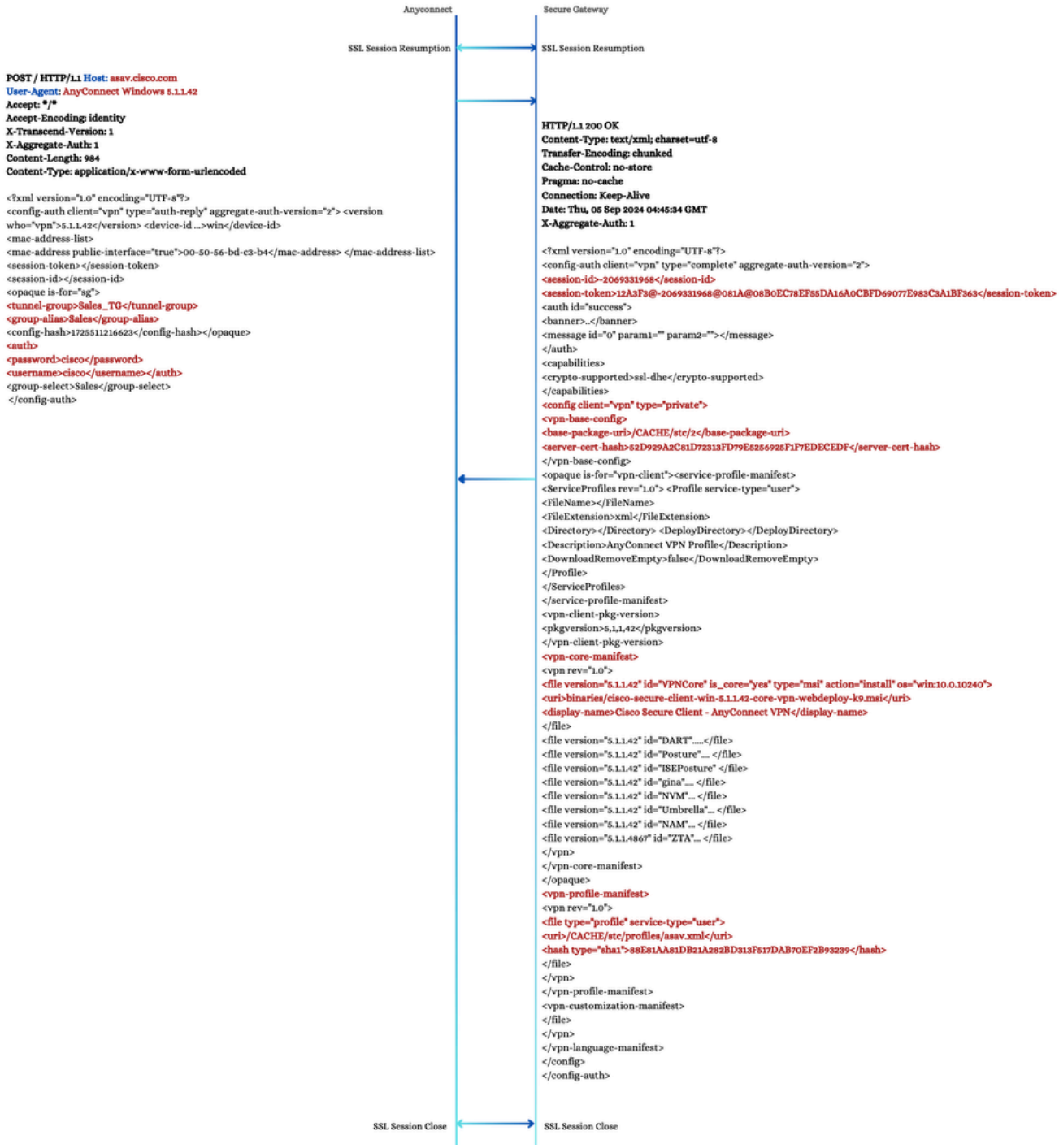
5. Elemento vpn-core-manifest: este elemento indica o caminho e a versão do pacote principal do AnyConnect, juntamente com outros componentes como Dart, Posture, ISE Posture e assim por

diante. Ele é usado pelo VPN Downloader na próxima seção.

6. Elemento vpn-profile-manifest: Este elemento indica o caminho (o nome do perfil) e o hash SHA-1 do perfil.



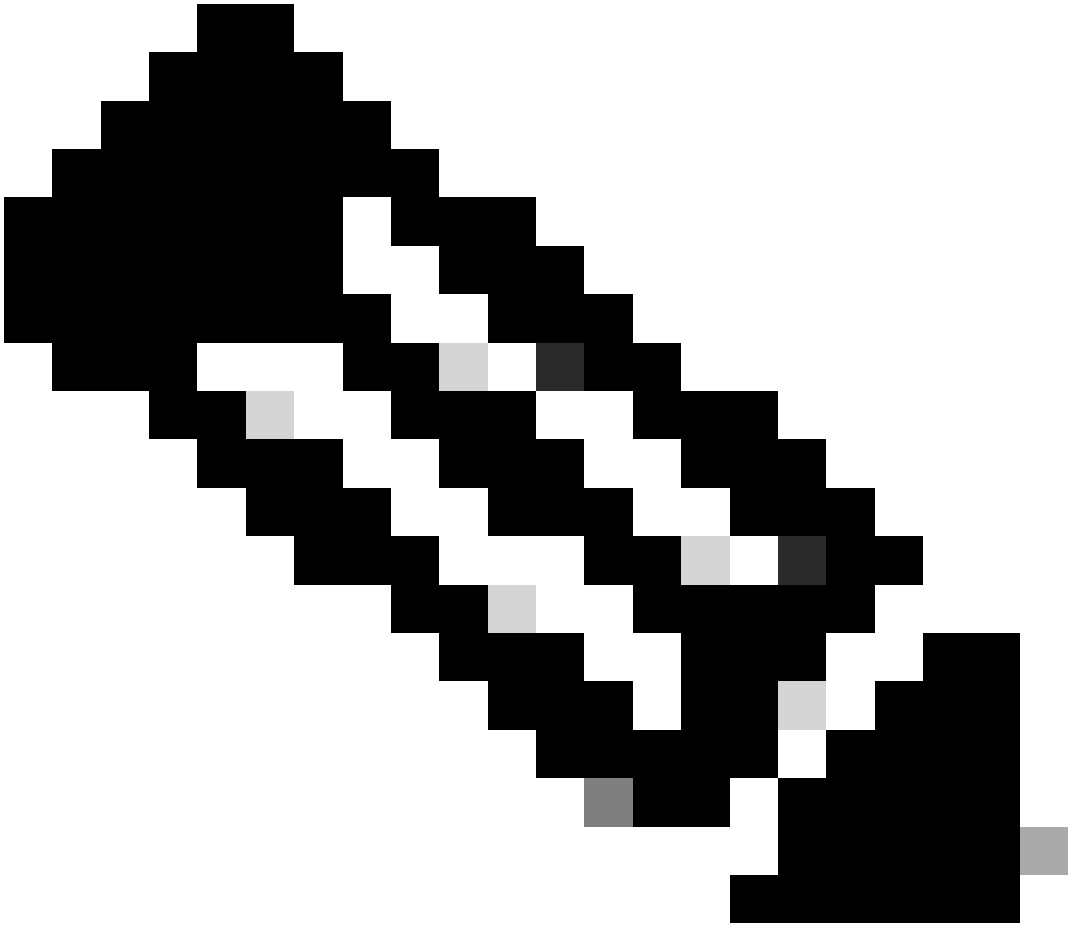
Observação: se o cliente não tiver o perfil, o VPN Downloader na próxima seção fará o download dele. Se o cliente já tiver o perfil, o hash SHA-1 do perfil do cliente será comparado com o do servidor. Em caso de incompatibilidade, o VPN Downloader sobrescreve o perfil do cliente com aquele no Secure Gateway. Isso garante que o perfil no Gateway Seguro seja aplicado na pós-autenticação do cliente.



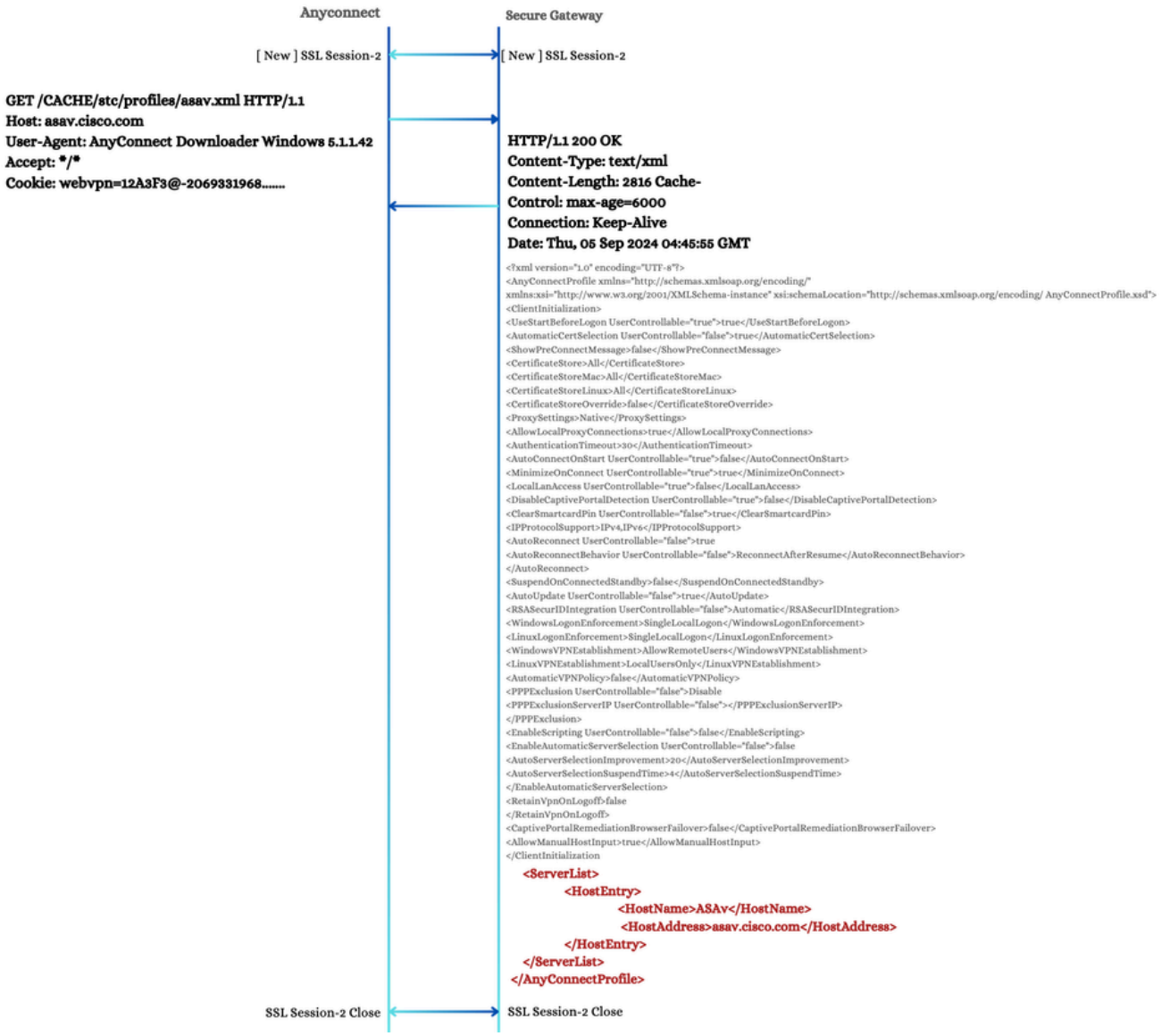
POST - Autenticação de usuário

4. AnyConnect Downloader

O AnyConnect Downloader sempre inicia uma nova sessão SSL, que é o motivo pelo qual os usuários podem encontrar um segundo aviso de certificado se o certificado do Secure Gateway não for confiável. Durante essa fase, ele executa operações GET separadas para cada item que precisa ser baixado.



Observação: se o perfil do cliente for carregado no Secure Gateway, ele será obrigatório para download; caso contrário, toda a tentativa de conexão será encerrada.

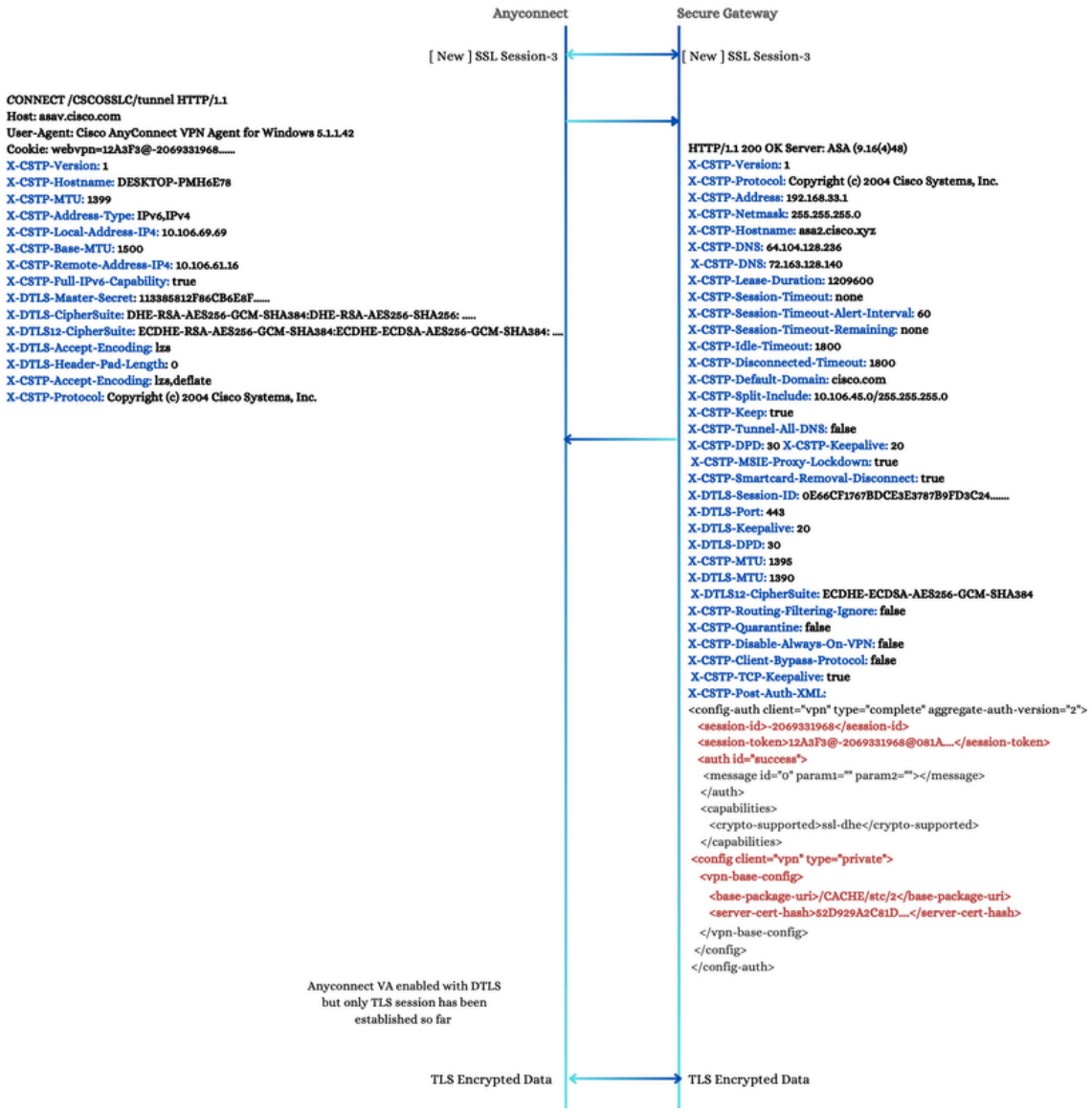


Downloader de VPN

5. CONEXÃO CSTP

O AnyConnect executa uma operação CONNECT como etapa final no estabelecimento de um canal seguro. Durante a operação CONNECT, o cliente AnyConnect envia vários atributos X-CSTP e X-DTLS para o Secure Gateway para que seja processado. O Secure Gateway responde com atributos X-CSTP e X-DTLS adicionais que o cliente aplica à tentativa de conexão atual. Esse intercâmbio inclui o X-CSTP-Post-Auth-XML, acompanhado de um arquivo XML, que é muito semelhante ao visto na etapa POST - User Authentication.

Após receber uma resposta com êxito, o AnyConnect inicia o canal de dados TLS. Simultaneamente, a interface do adaptador virtual do AnyConnect é ativada com um valor de MTU igual a X-DTLS-MTU, supondo que o handshake DTLS subsequente seja bem-sucedido.



Conexão CSTP

6. Handshake DTLS

O handshake DTLS continua conforme descrito aqui. Essa configuração é relativamente rápida devido aos atributos trocados entre o cliente e o servidor durante o evento CONNECT.

Cliente

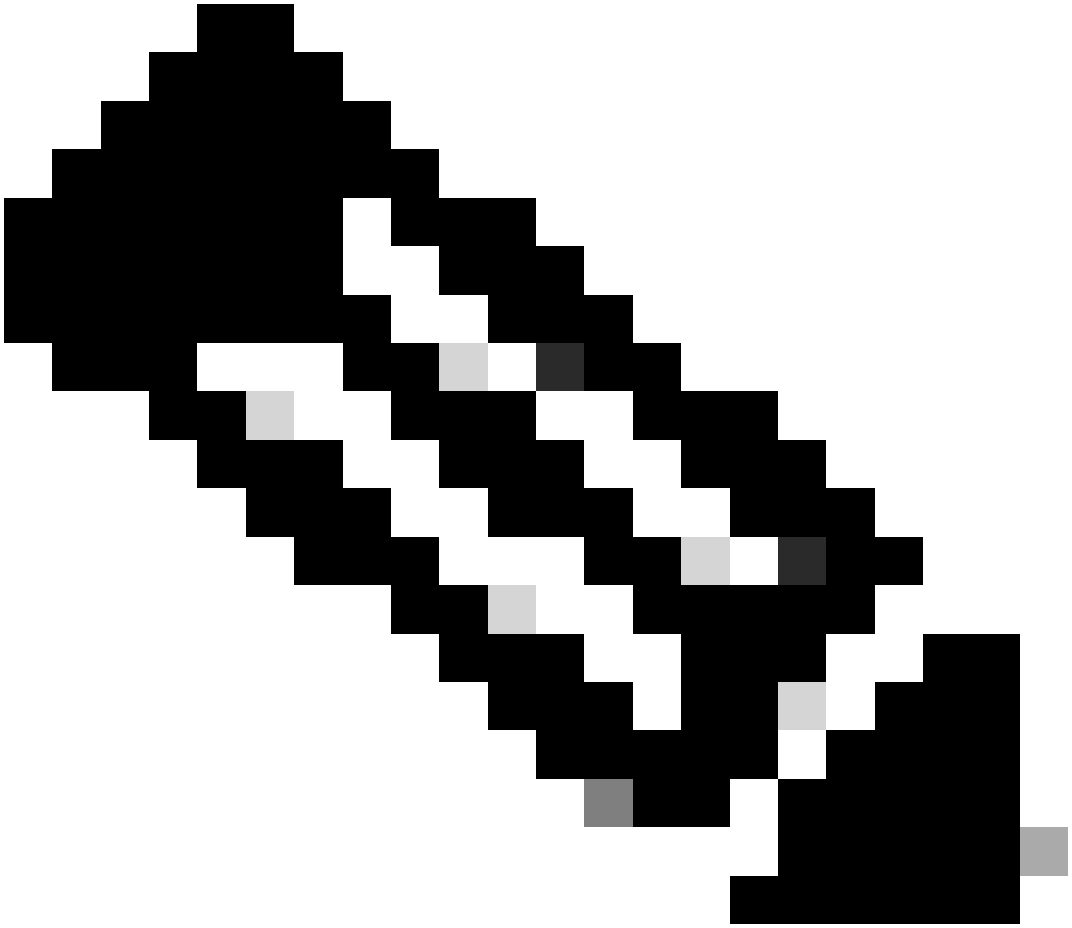
X-DTLS-Master-Secret: o segredo mestre do DTLS é gerado pelo cliente e compartilhado com o servidor. Essa chave é crucial para estabelecer uma sessão DTLS segura.

X-DTLS-CipherSuite: A lista de pacotes de cifras DTLS suportados pelo cliente, indicando os recursos de criptografia do cliente.

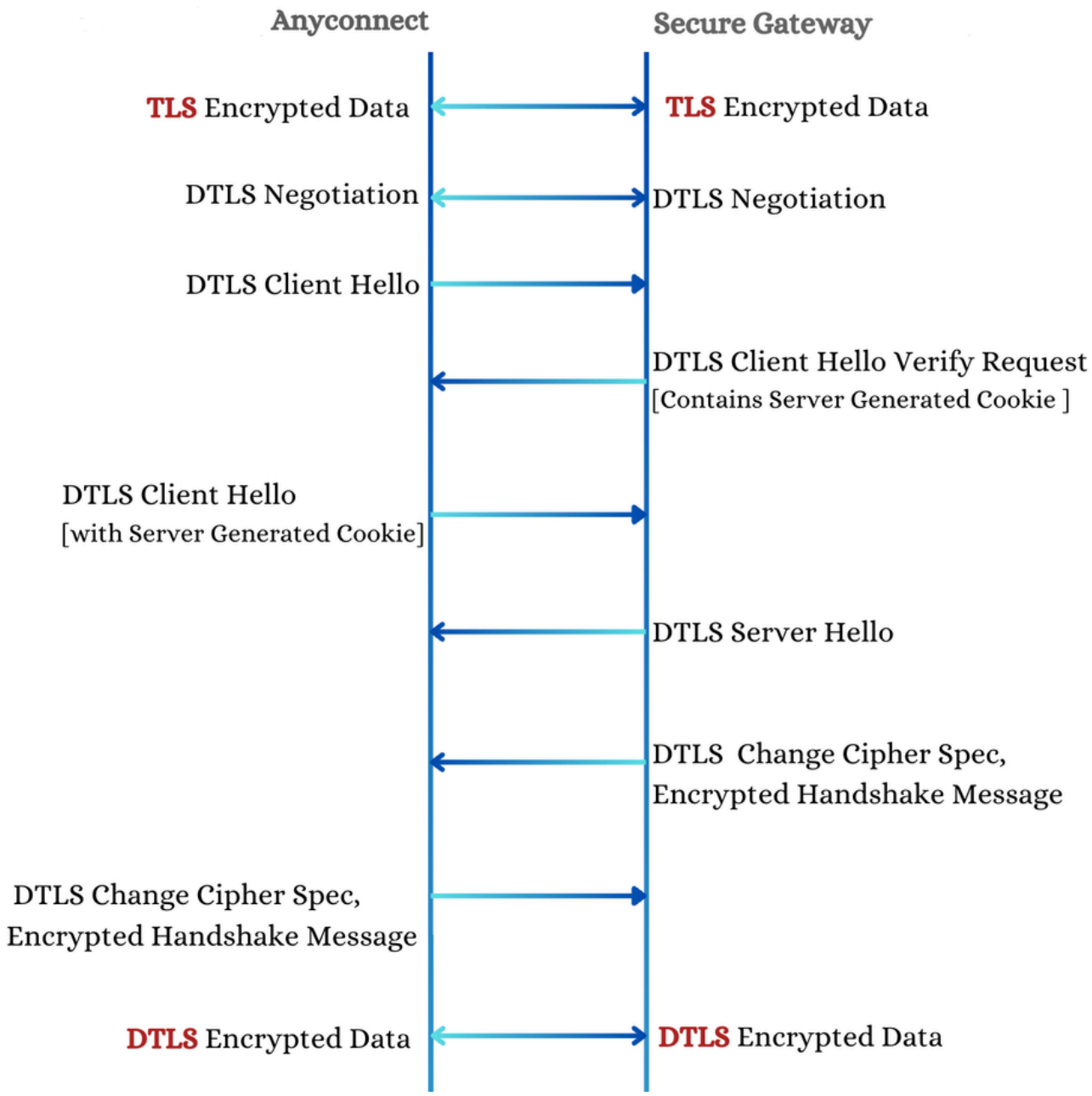
Servidor

X-DTLS-Session-ID: o ID da sessão DTLS atribuído pelo servidor para o cliente usar, garantindo a continuidade da sessão.

X-DTLS-CipherSuite: O conjunto de cifras selecionado pelo servidor na lista fornecida pelo cliente, garantindo que ambas as partes usem um método de criptografia compatível.



Observação: enquanto o handshake DTLS está em andamento, o canal de dados TLS continua a operar. Isso garante que a transmissão de dados permaneça consistente e segura durante o processo de handshake. Uma transição perfeita para o canal de criptografia de dados DTLS ocorre somente após a conclusão do handshake DTLS.

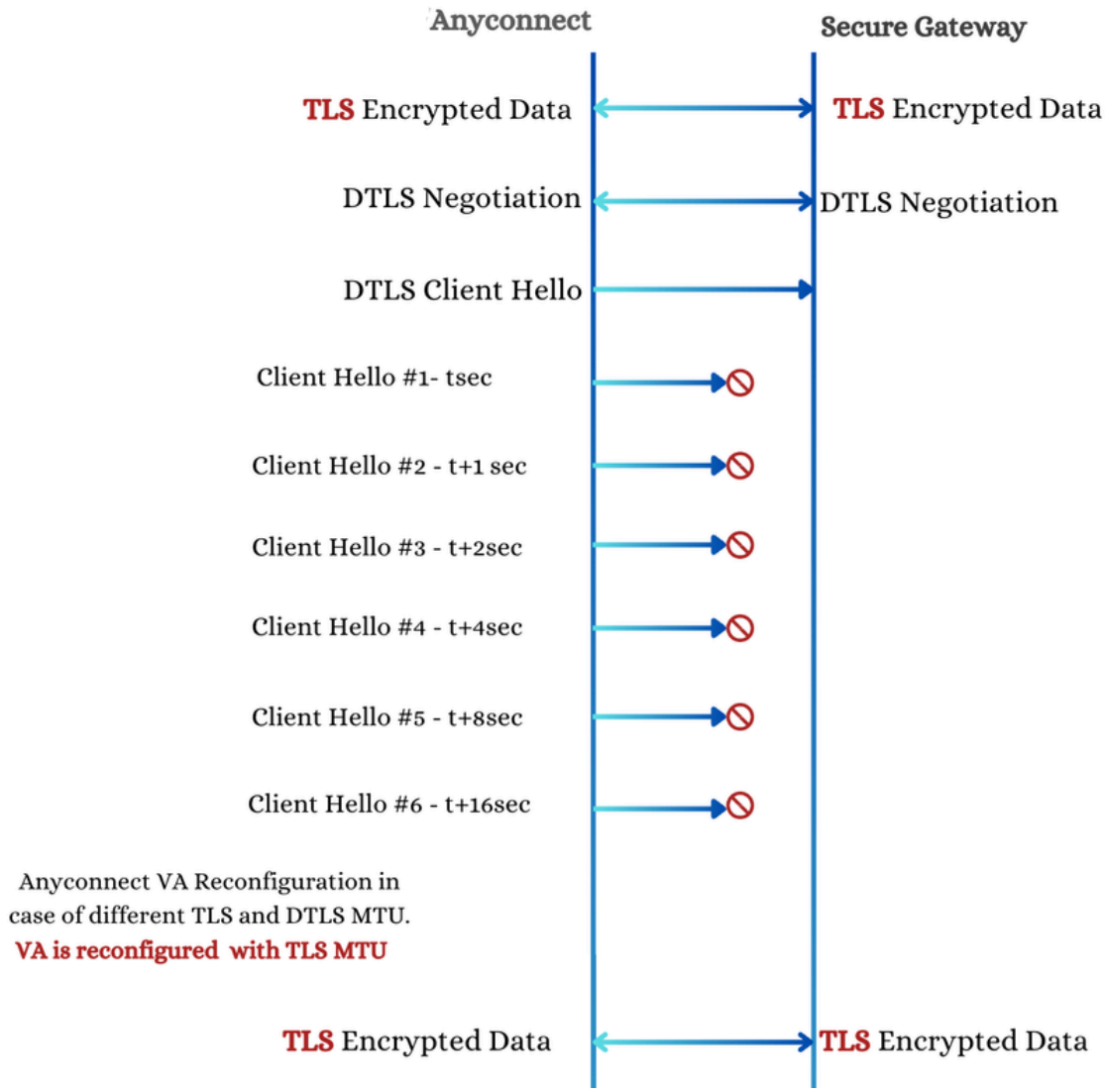


Handshake DTLS

6.1. Porta DTLS bloqueada

Caso a porta DTLS seja bloqueada ou o Secure Gateway falhe em responder aos pacotes Hello do cliente DTLS, o AnyConnect executa um backoff exponencial com até cinco tentativas, começando com um atraso de 1 segundo e aumentando para até 16 segundos.

Se essas tentativas não forem bem-sucedidas, o AnyConnect aplicará o MTU TLS real, conforme especificado pelo valor X-CSTP-MTU retornado pelo Secure Gateway na Fase 5., ao adaptador virtual do AnyConnect. Como esse MTU difere do MTU aplicado anteriormente (X-DTLS-MTU), uma reconfiguração do adaptador virtual é necessária. Essa reconfiguração aparece para o usuário final como uma tentativa de reconexão, embora nenhuma nova negociação ocorra durante esse processo. Depois que o adaptador virtual for reconfigurado, o canal de dados TLS continuará a operar.



Bloco de porta DTLS

Informações Relacionadas

- Referência da Documentação de Tecnologias VPN Cisco
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.