AnyConnect SSL VPNの接続フローについて

内容

はじめに

このドキュメントでは、SSLVPN接続中にAnyConnectとセキュアゲートウェイの間で発生するイベントのフローについて説明します。

背景説明

AnyConnect

AnyConnectは、SSLおよびIKEv2プロトコル用に設計されたCisco VPN Clientです。ほとんどのデスクトッププラットフォームとモバイルプラットフォームで使用できます。AnyConnectは主に、Firepower Threat Defense(FTD)、適応型セキュリティアプライアンス(ASA)、またはセキュアゲートウェイと呼ばれるCisco IOS®/Cisco IOS® XEルータとのセキュア接続を確立します。

セキュアゲートウェイ

シスコの用語では、SSL VPNサーバはセキュアゲートウェイと呼ばれ、IPSec(IKEv2)サーバはリモートアクセスVPNゲートウェイと呼ばれます。シスコでは、次のプラットフォームでSSL VPNトンネルの終端をサポートしています。

- Cisco ASA 5500および5500-Xシリーズ
- Cisco FTD（2100、4100、および9300シリーズ）
- Cisco ISR 4000およびISR G2シリーズ
- Cisco CSR 1000シリーズ
- Cisco Catalyst 8000 シリーズ

AnyConnect SSL VPNの接続フロー

このドキュメントでは、SSL VPN接続の確立中にAnyConnectとセキュアゲートウェイの間で発生するイベントを6つのフェーズに分けて説明します。

1. SSLハンドシェイク

2. POST – グループの選択

3. POST – ユーザ名/パスワードによるユーザ認証（オプション）

4. VPNダウンローダ（オプション）

5. CSTP接続

6. DTLS接続（オプション）

1. SSLハンドシェイク

SSLハンドシェイクは、「Client Hello」メッセージを使用したTCP 3ウェイハンドシェイクの完了後に、AnyConnectクライアントによって開始されます。イベントの流れと重要なポイントは前述の通りです。

Client Hello

SSLセッションは、クライアントが「Client Hello」メッセージを送信することから始まります。このメッセージ内：

a) SSLセッションIDは0に設定されており、新しいセッションが開始されたことを示しています。

b)ペイロードには、クライアントがサポートする暗号スイートと、クライアントが生成するランダムナンスが含まれます。

Server Hello

サーバは、次のような「Server Hello」メッセージで応答します。

a)クライアントから提供されたリストから選択された暗号スイート。

b)サーバはSSLセッションIDを生成し、サーバはランダムなナンスを生成しました。

サーバ証明書

「Server Hello」の後、サーバは自身のIDとして機能するSSL証明書を送信します。注意すべき主なポイントは次のとおりです。

a)この証明書が厳密な検証チェックに失敗すると、デフォルトではAnyConnectによってサーバがブロックされます。

b)ユーザはこのブロックを無効にするオプションを使用できますが、報告されたエラーが解決されるまで、以降の接続では警告が表示されます。

クライアント証明書要求

サーバは、クライアント証明書を要求し、セキュアゲートウェイにロードされたすべてのCA証明書のサブジェクト名DNのリストを送信することもできます。この要求には、次の2つの目的があります。

a)複数のID証明書が使用可能な場合、クライアント（ユーザ）が正しいID証明書を選択するのに役立ちます。

b)返された証明書がセキュアゲートウェイによって信頼されていることを確認しますが、証明書の検証がさらに行われる必要があります。

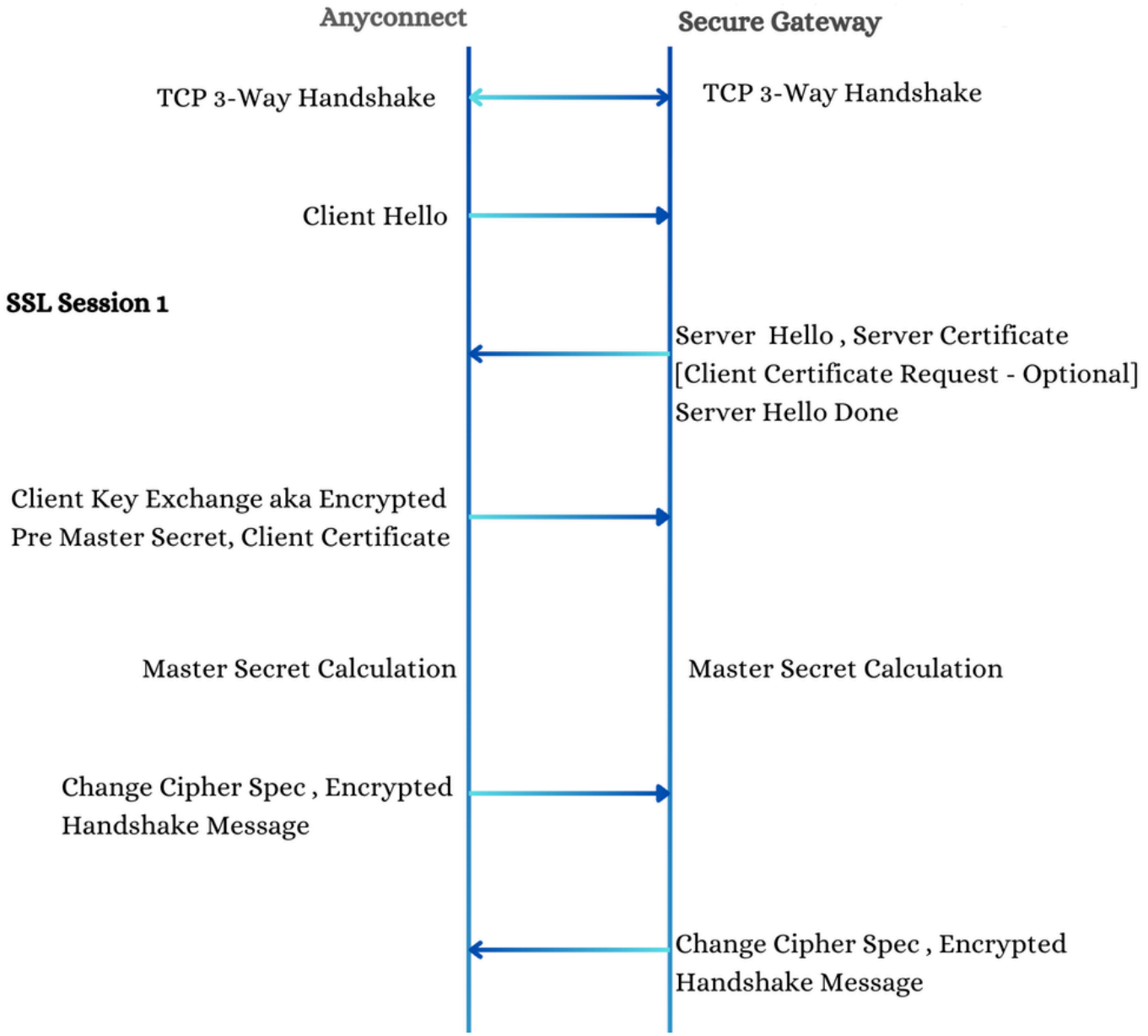
Client Key Exchange

次に、クライアントは「Client Key Exchange」メッセージを送信します。このメッセージには、プレマスター秘密キーが含まれています。このキーは次を使用して暗号化されます。

a)サーバ証明書のサーバの公開キー(選択した暗号スイートがRSAベースの場合（たとえば、TLS_RSA_WITH_AES_128_CBC_SHA）。

b)選択された暗号スイートがDHEベースの場合（たとえば、TLS_DHE_DSS_WITH_AES_256_CBC_SHA）、Server Helloメッセージで提供されるサーバのDH公開キー。

プレマスターシークレット、クライアントが生成したランダムナンス、およびサーバが生成したランダムナンスに基づいて、クライアントとセキュアゲートウェイの両方が独立してマスターシークレットを生成します。このマスター・シークレットを使用してセッション・キーを取得し、クライアントとサーバ間の安全な通信を確保します。



SSLセッション1

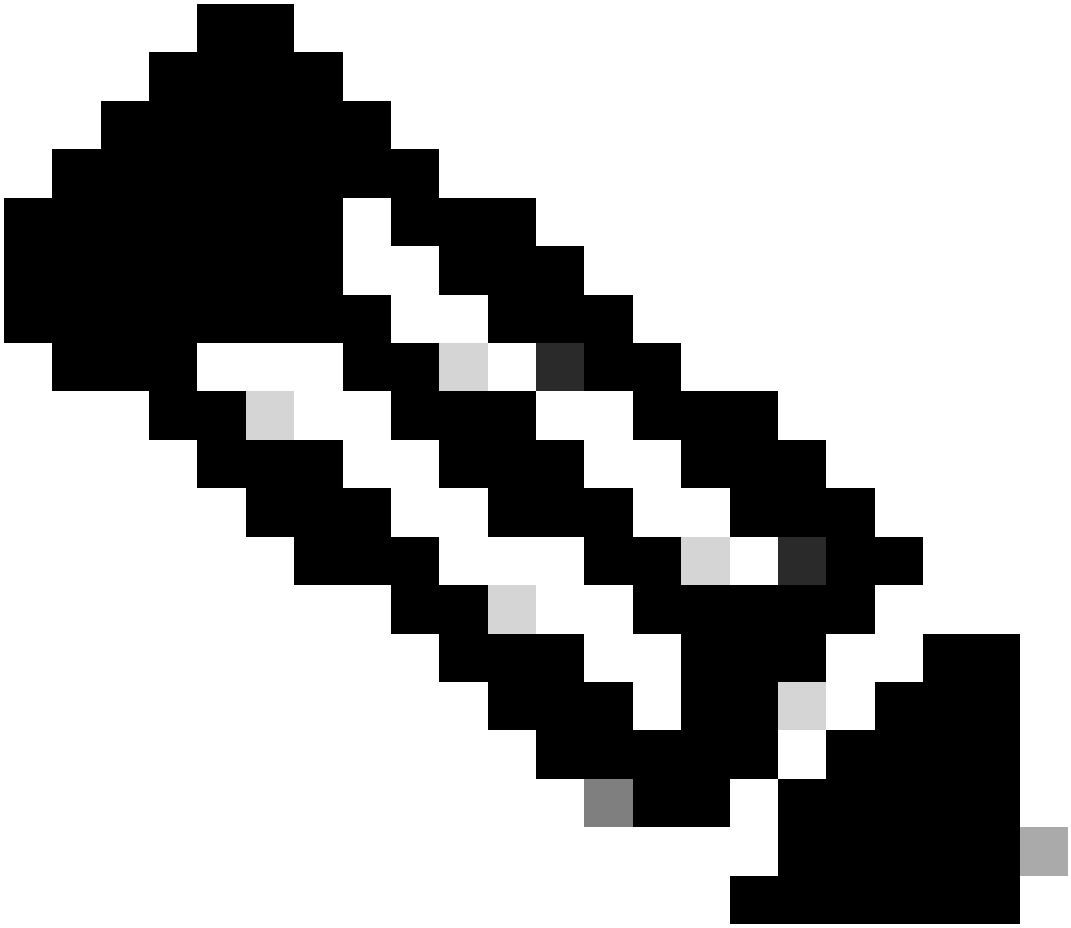
2. POST – グループの選択

この操作の間、クライアントは、ユーザが明示的に指定しない限り、接続プロファイルに関する情報を持ちません。要求の「group-access」要素に示されているように、接続の試行はセキュアゲートウェイURL(asav.cisco.com)に誘導されます。クライアントでは、「aggregate-authentication」バージョン2がサポートされています。このバージョンは、特に効率的なXMLトランザクションの点で、以前のバージョンに比べて大幅に改善されています。セキュアゲートウェイとクライアントの両方が、使用するバージョンに合意する必要があります。セキュアゲートウェイがバージョン2をサポートしていないシナリオでは、追加のPOST操作がトリガーされ、クライアントはバージョンにフォールバックします。

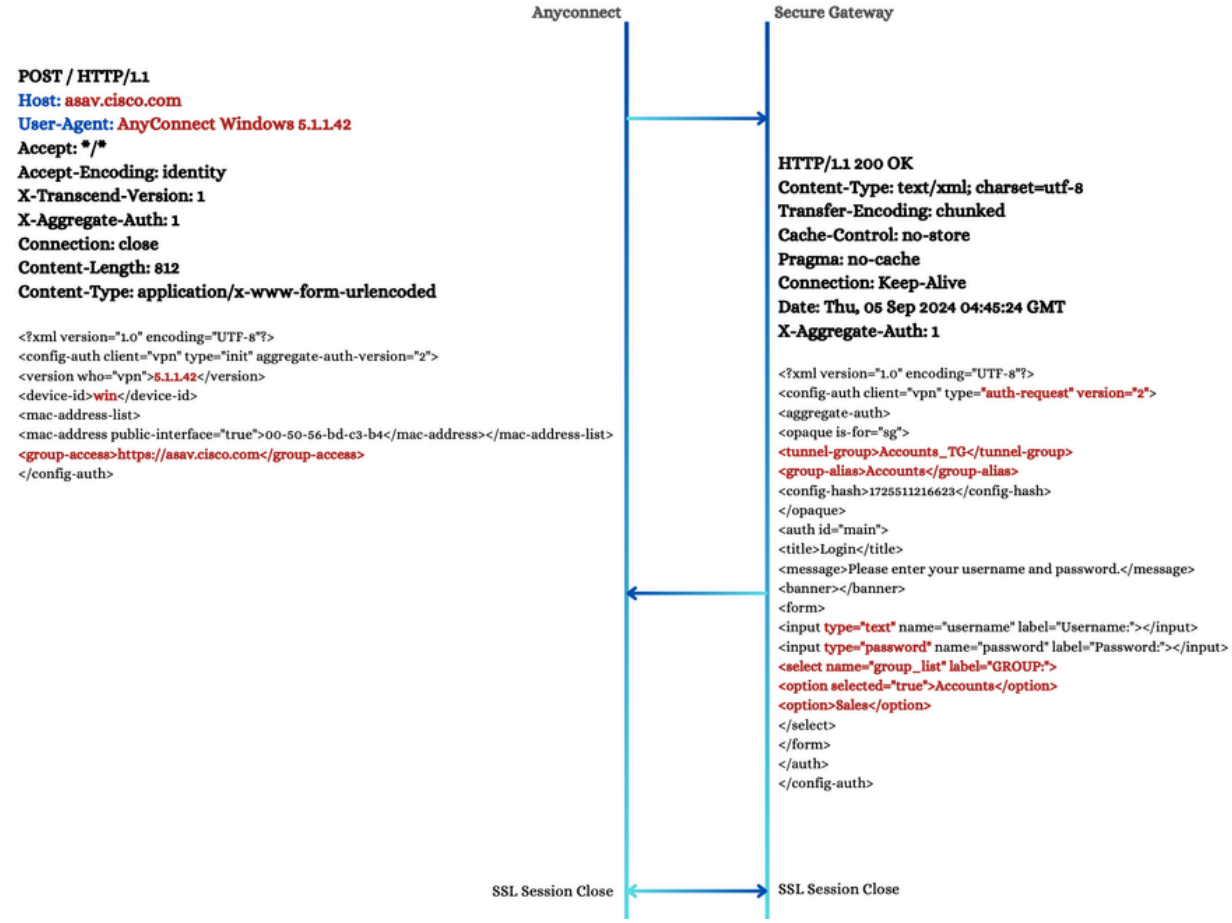
HTTP応答で、セキュアゲートウェイは次のように示します。

1. セキュアゲートウェイがサポートする集約認証のバージョン。

2. トンネルグループリストとユーザ名/パスワードフォーム。

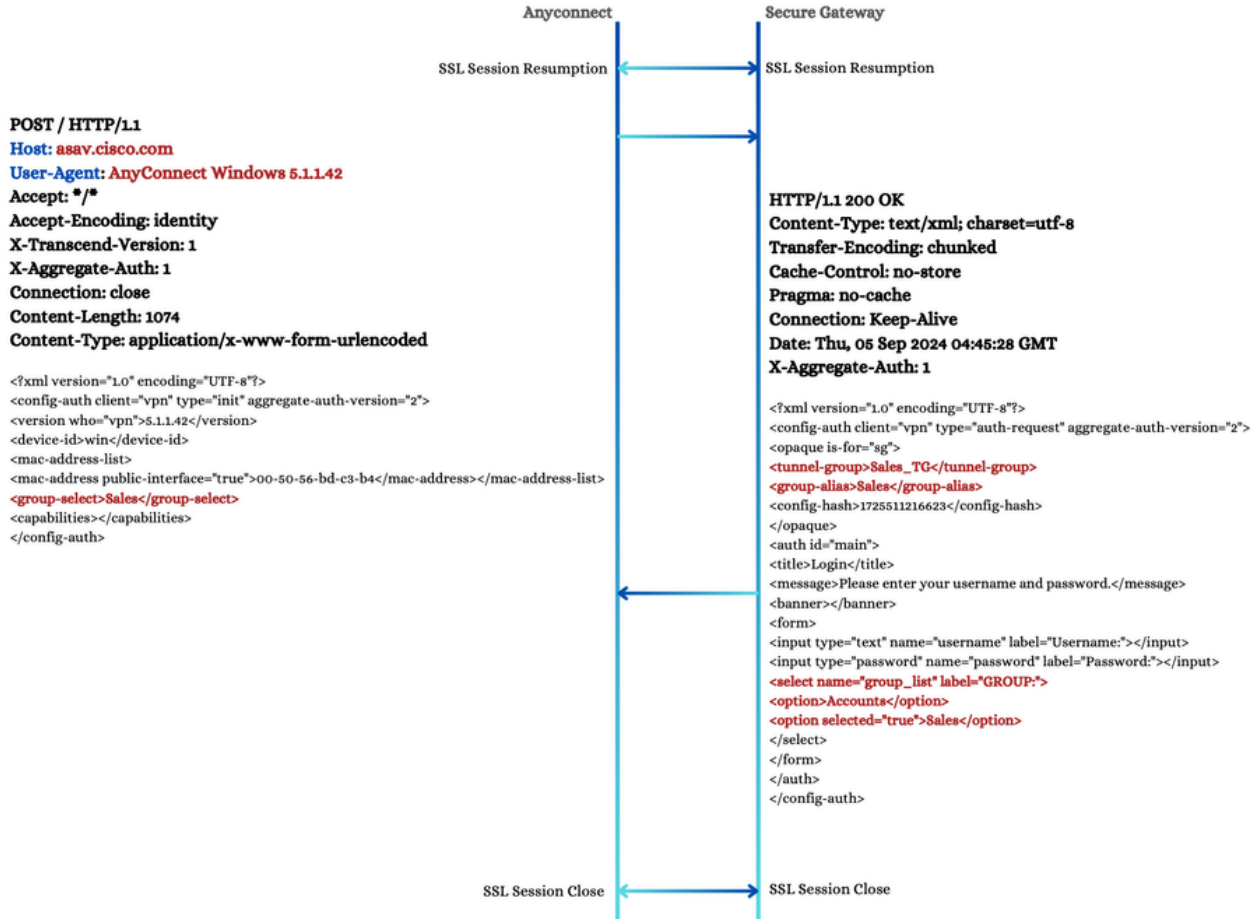


注：このフォームには、「select」要素が含まれています。この要素には、セキュアゲートウェイで設定されたすべての接続プロファイルのグループエイリアスが一覧表示されます。デフォルトでは、これらのグループエイリアスの1つがselected = "true"ブール属性でハイライト表示されます。tunnel-group要素とgroup-alias要素は、この選択された接続プロファイルに対応します。



POST – グループ選択1

ユーザがこのリストから別の接続プロファイルを選択すると、別のPOST処理が実行されます。この場合、次に示すように、クライアントは選択された接続プロファイルを反映するために、「group-select」要素を更新した状態でPOST要求を送信します。



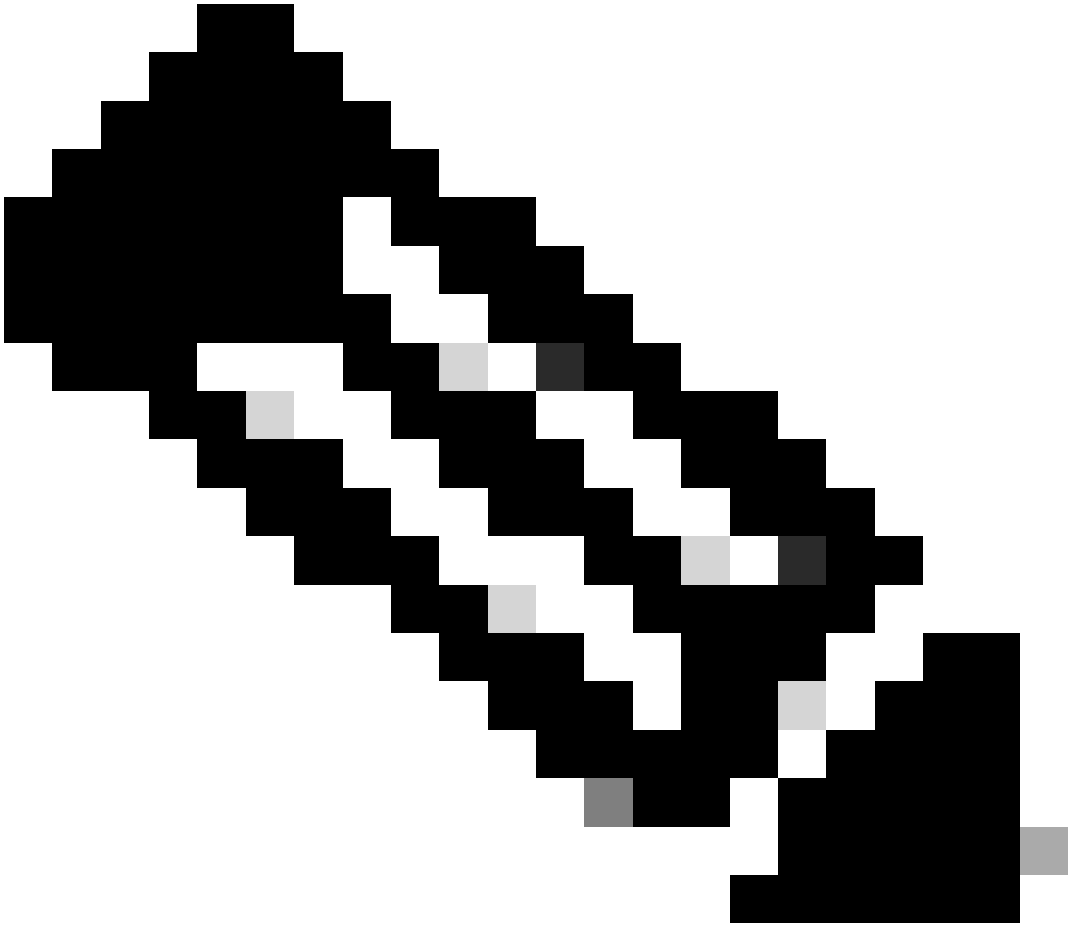
POST – グループ選択2

3. POST – ユーザ認証

POST-Group Selectionに続くこの操作では、AnyConnectは次の情報をセキュアゲートウェイに送信します。

1. 選択された接続プロファイル情報：これには、以前の操作でセキュアゲートウェイによって示されたトンネルグループ名とグループエイリアスが含まれます。

2. ユーザ名とパスワード：ユーザの認証資格情報。



注：このフローはAAA認証に固有であるため、他の認証方式とは異なる場合があります。

POST操作への応答として、セキュアゲートウェイは次の情報を含むXMLファイルを送信します。

1. セッションID：これは、SSLセッションIDとは異なります。

2. セッショントークン：このトークンは、後でクライアントによってWebVPN Cookieとして使用されます。

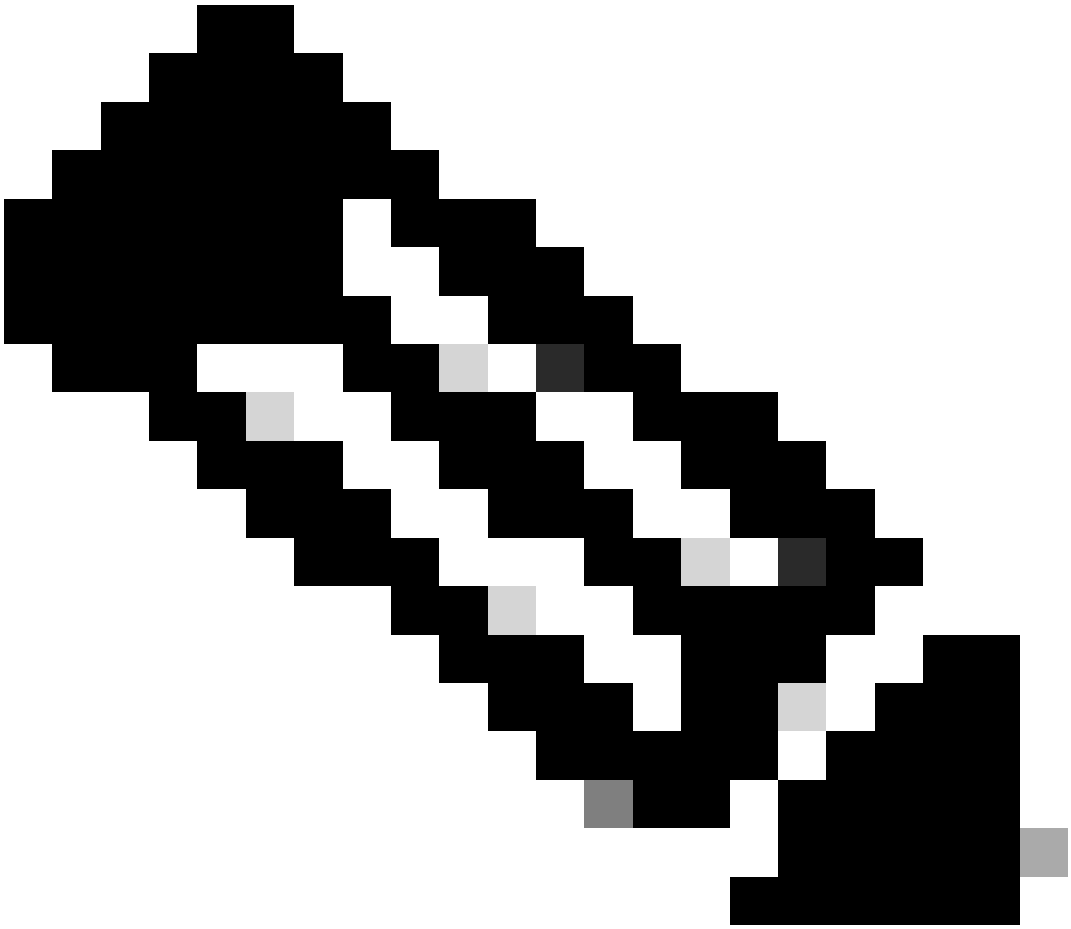
3. Authentication Status:id = 'success'のauth要素によって示されます。

4. サーバ証明書ハッシュ：このハッシュは、preferences.xmlファイルにキャッシュされます。

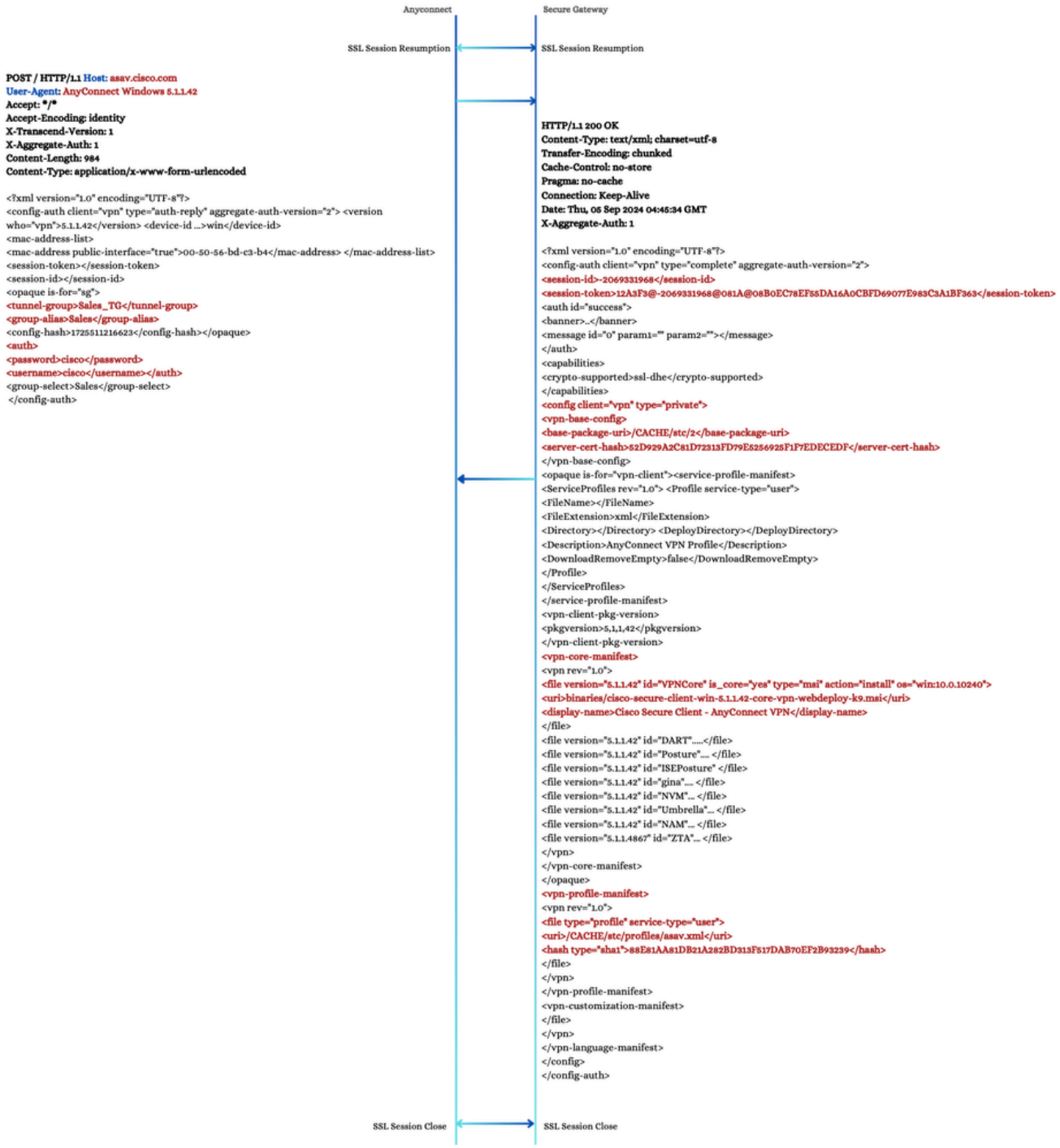
5. vpn-core-manifest要素：この要素は、AnyConnectコアパッケージのパスとバージョンに加え、Dart、ポスチャ、ISEポスチャなどの他のコンポーネントを示します。これは、次のセクションで

VPNダウンローダによって使用されます。

6. vpn-profile-manifest要素：この要素は、プロファイルのパス（プロファイルの名前）とSHA-1ハッシュを示します。



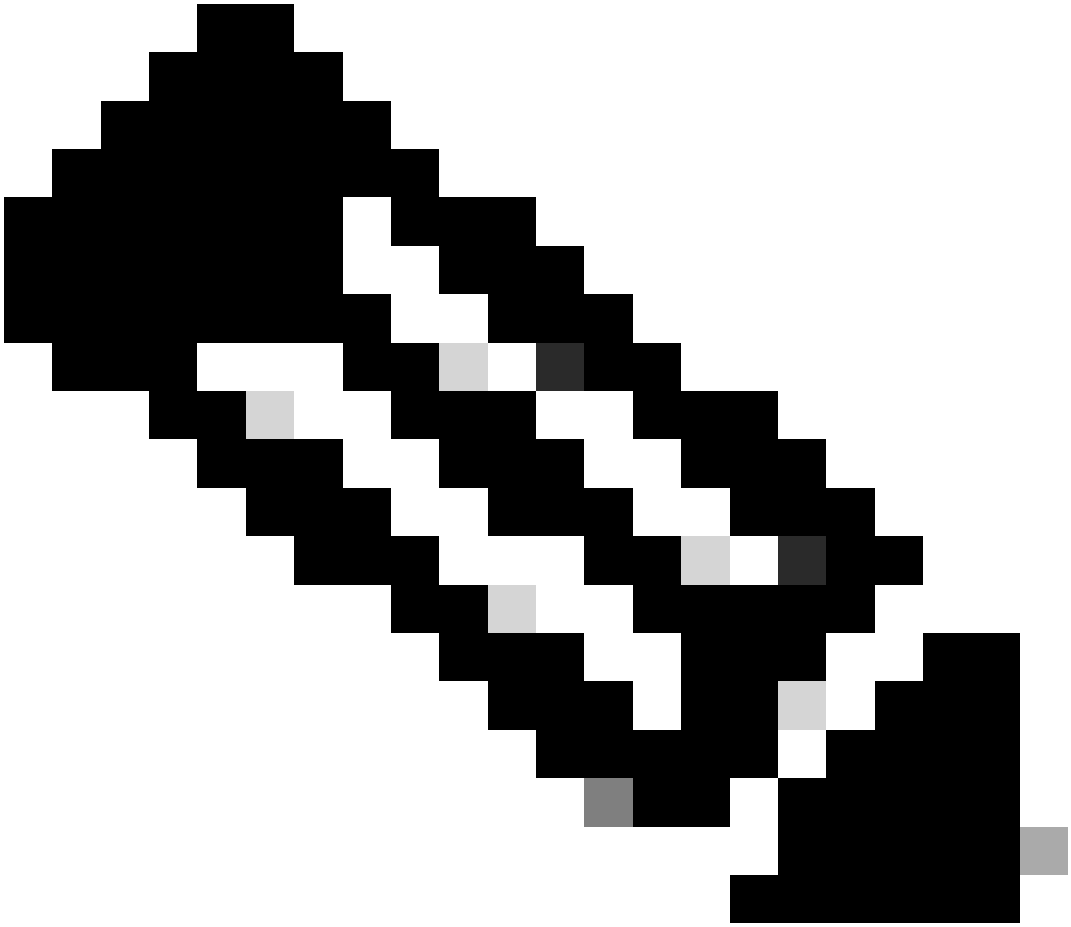
注：クライアントにプロファイルがない場合は、次のセクションのVPNダウンローダがプロファイルをダウンロードします。クライアントがすでにプロファイルを持っている場合、クライアントプロファイルのSHA-1ハッシュがサーバのものと比較されます。不一致が発生すると、VPNダウンローダはクライアントプロファイルをセキュアゲートウェイ上のプロファイルで上書きします。これにより、Secure Gateway上のプロファイルが認証後のクライアントに確実に適用されます。



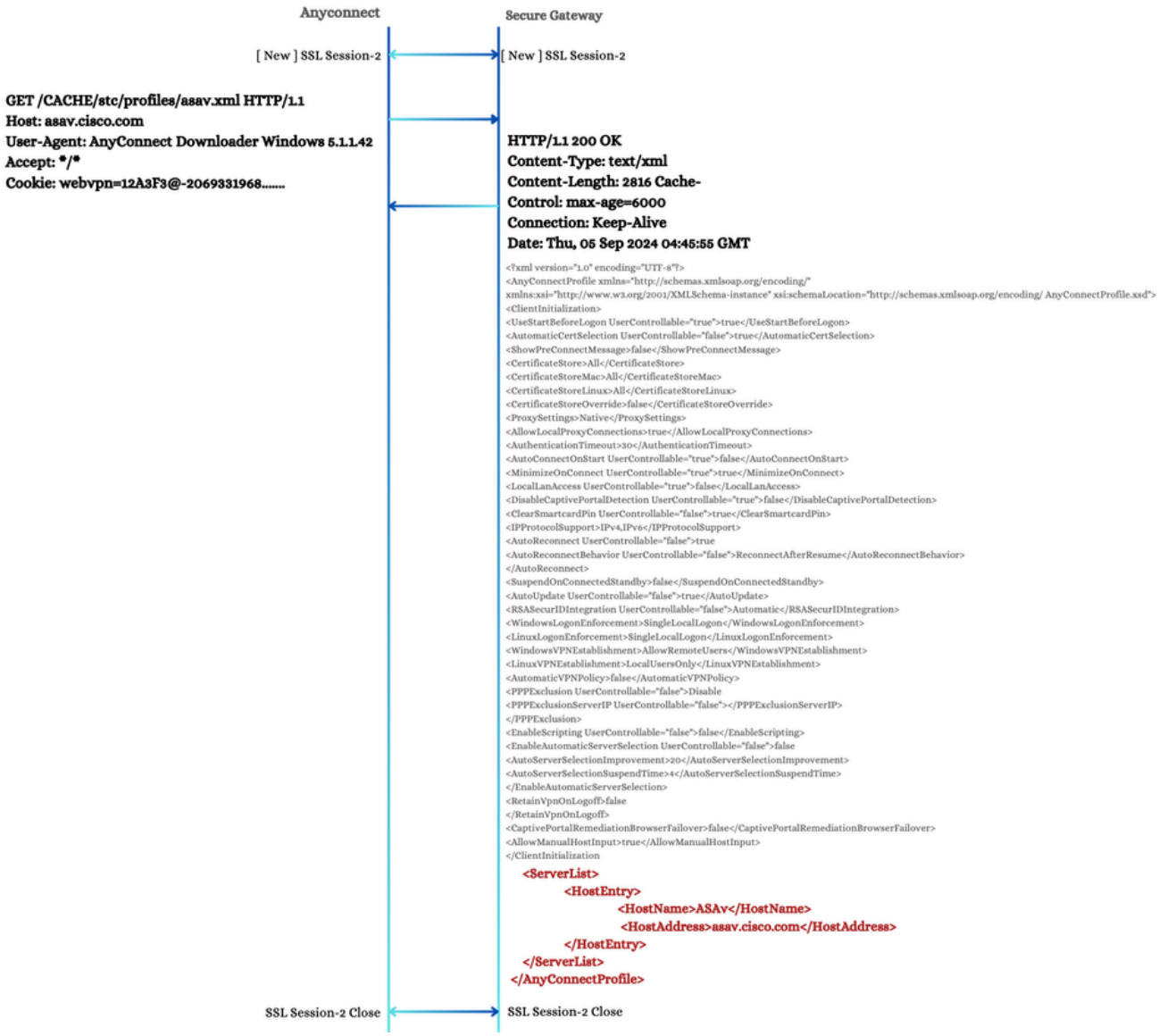
POST – ユーザ認証

4. AnyConnectダウンローダ

AnyConnectダウンローダは常に新しいSSLセッションを開始します。そのため、セキュアゲートウェイの証明書が信頼できない場合に2番目の証明書の警告がユーザに表示されます。このフェーズでは、ダウンロードする必要がある項目ごとに個別のGET操作を実行します。



注：クライアントプロファイルがSecure Gatewayにアップロードされている場合は、ダウンロードが必須です。アップロードされていない場合は、接続試行全体が終了します。

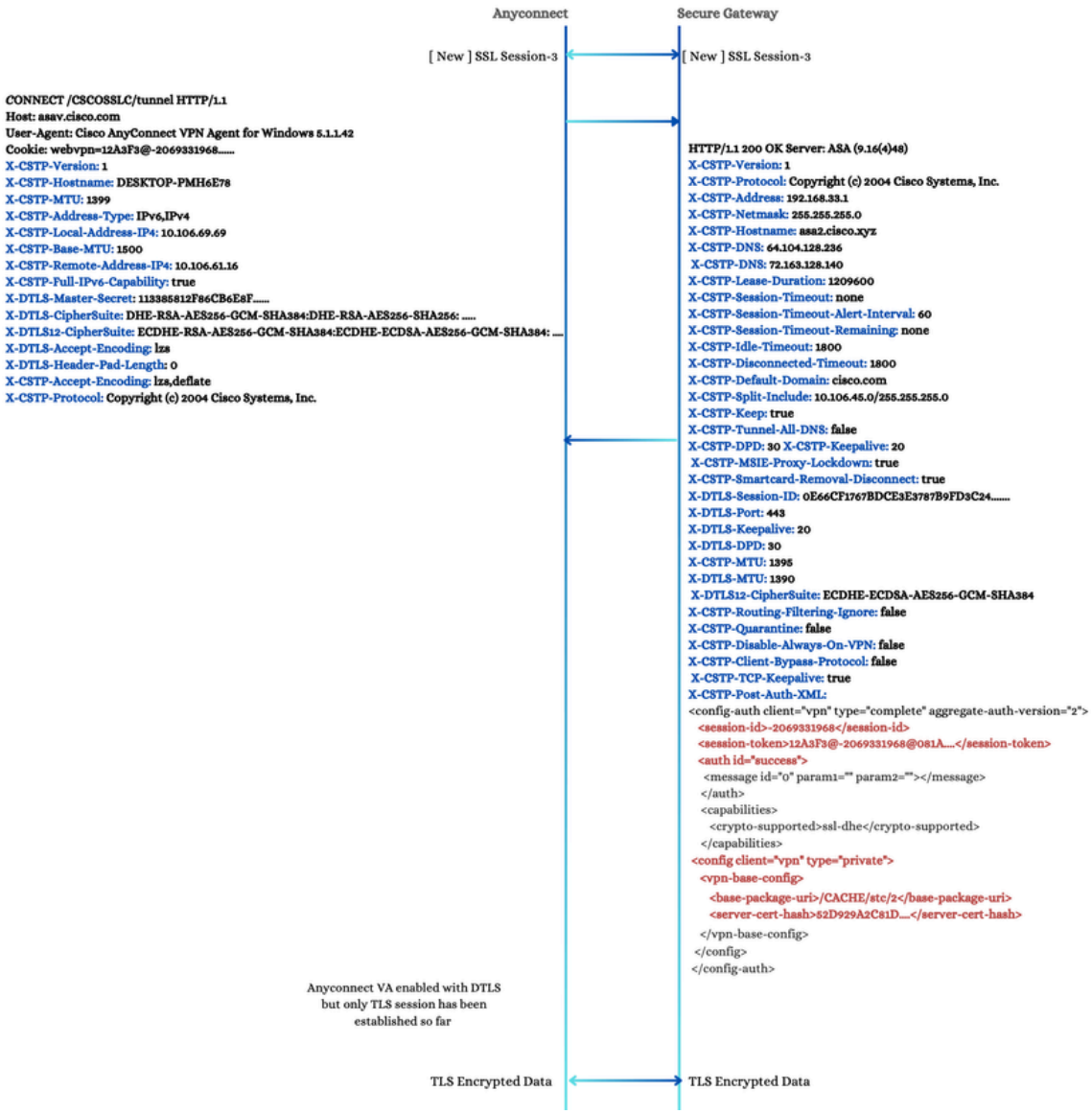


VPNダウンローダ

5. CSTP接続

AnyConnectは、セキュアチャネルを確立するための最後のステップとしてCONNECT操作を実行します。CONNECT操作中、AnyConnectクライアントは、処理するためにセキュアゲートウェイのさまざまなX-CSTP属性とX-DTLS属性を送信します。セキュアゲートウェイは、クライアントが現在の接続の試行に適用する追加のX-CSTP属性とX-DTLS属性で応答します。この交換には、X-CSTP-Post-Auth-XMLと、XMLファイルが含まれます。このファイルは、POST-User Authenticationステップで確認されるファイルとほぼ同じです。

正常な応答を受信すると、AnyConnectはTLSデータチャネルを開始します。同時に、AnyConnect仮想アダプタインターフェイスは、後続のDTLSハンドシェイクが成功したと仮定して、X-DTLS-MTUに等しいMTU値でアクティブ化されます。



CSTP接続

6. DTLSハンドシェイク

DTLSハンドシェイクは次のように行われます。CONNECTイベントの間にクライアントとサーバ間で属性が交換されるため、この設定は比較的短時間で行われます。

クライアント

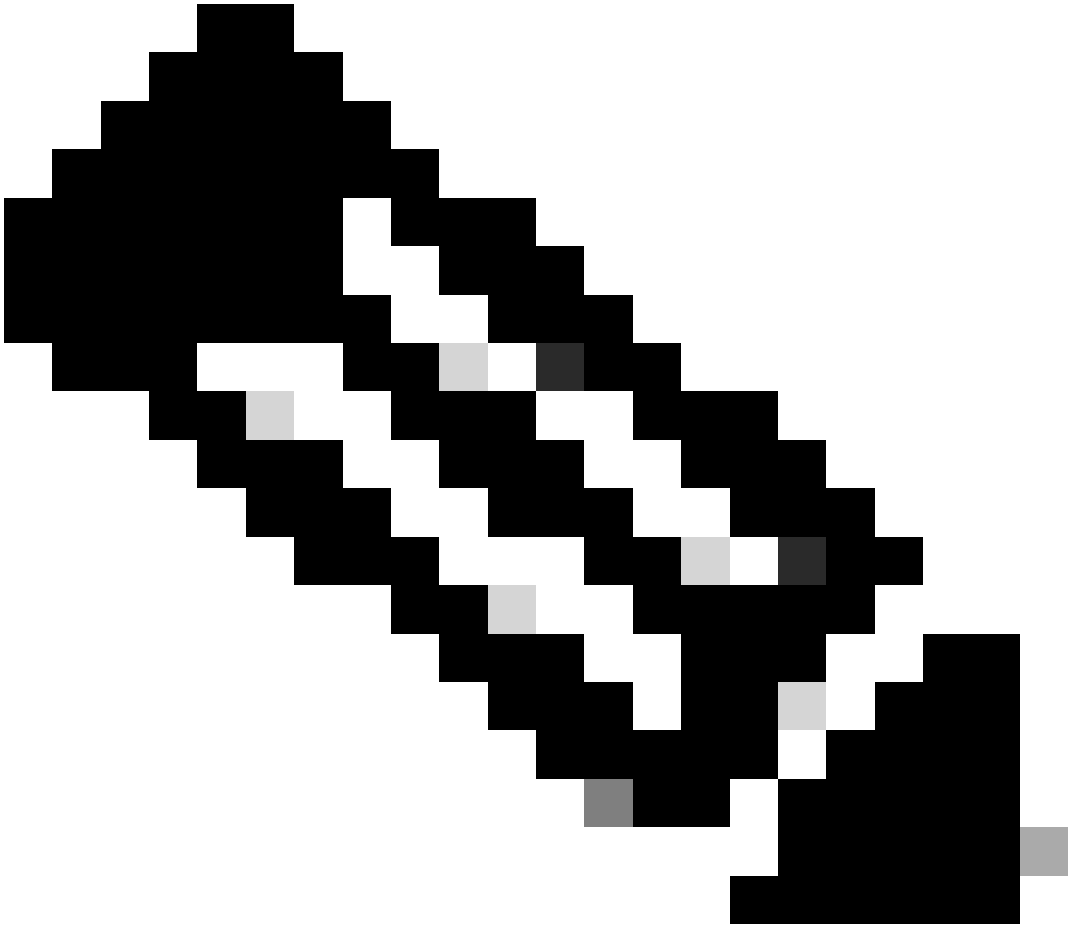
X-DTLS-Master-Secret:DTLSマスターシークレットは、クライアントによって生成され、サーバと共有されます。このキーは、セキュアなDTLSセッションを確立するために重要です。

X-DTLS-CipherSuite：クライアントでサポートされているDTLS暗号スイートのリスト。クライアントの暗号化機能を示します。

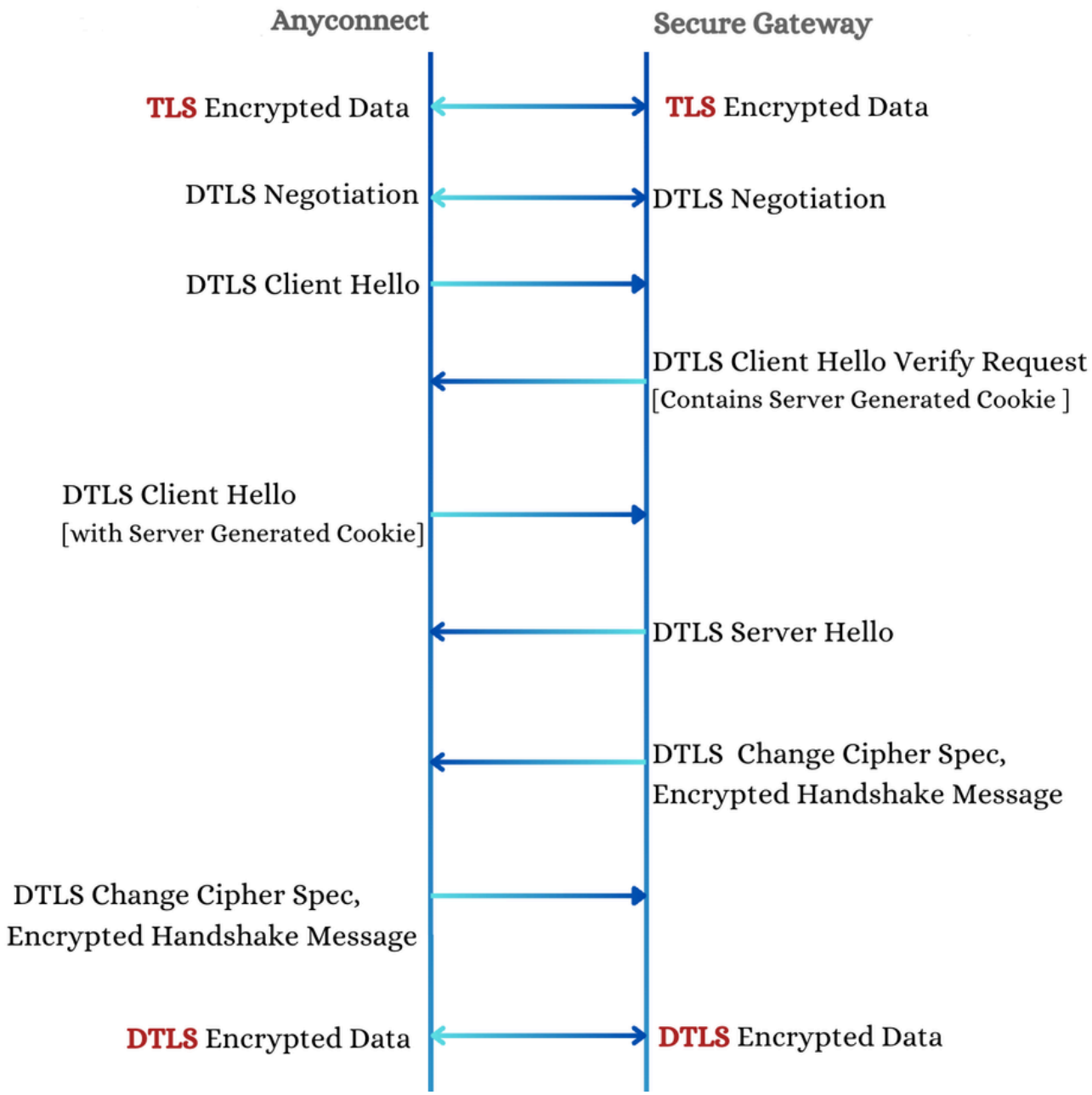
サーバ

X-DTLS-Session-ID：クライアントが使用するためにサーバによって割り当てられるDTLSセッションID。これにより、セッションの継続性が確保されます。

X-DTLS-CipherSuite：クライアントから提供されたリストからサーバが選択する暗号スイート。これにより、両当事者が互換性のある暗号化方式を使用することが保証されます。



注:DTLSハンドシェイクの進行中は、TLSデータチャネルが引き続き動作します。これにより、ハンドシェイクプロセス中にデータ伝送の一貫性と安全性が維持されます。DTLSデータ暗号化チャネルへのシームレスな移行は、DTLSハンドシェイクが完了した後にのみ行われます。

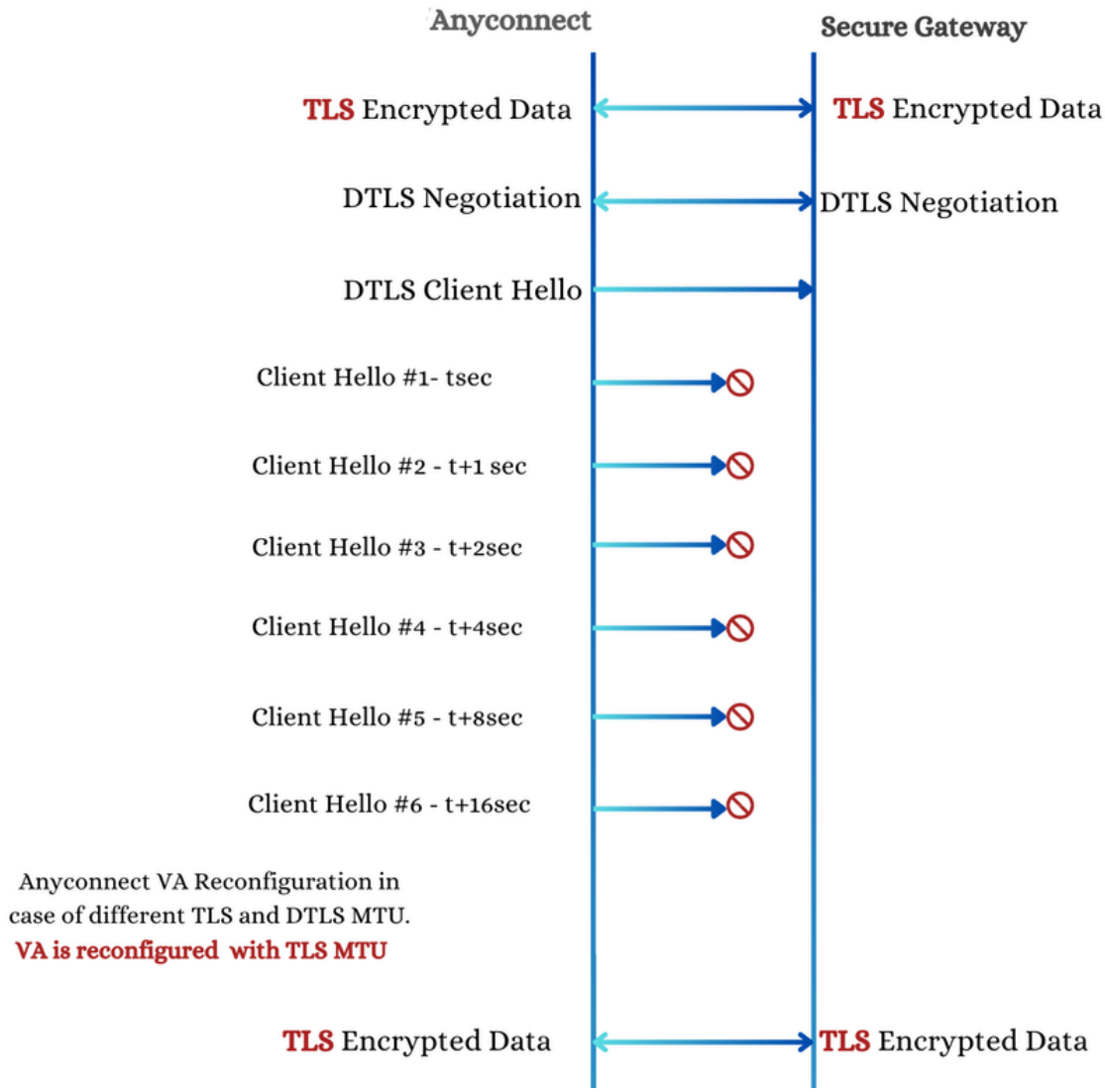


DTLSハンドシェイク

6.1. DTLSポートのブロック

DTLSポートがブロックされた場合、またはセキュアゲートウェイがDTLS Client Helloパケットへの応答に失敗した場合、AnyConnectは最大5回の再試行で指数関数的なバックオフを実行します（1秒間の遅延から最大16秒まで）。

これらの試行が失敗すると、AnyConnectは、フェーズ5.でセキュアゲートウェイから返されたX-CSTP-MTU値で指定された実際のTLS MTUをAnyConnect仮想アダプタに適用します。このMTUは、以前に適用されたMTU(X-DTLS-MTU)とは異なるため、仮想アダプタの再設定が必要です。この再設定は、エンドユーザにとっては再接続を試みるように見えますが、この処理中に新しいネゴシエーションは発生しません。仮想アダプタが再設定されると、TLSデータチャネルは引き続き動作します。



DTLSポートブロック

関連情報

- Cisco VPNテクノロジーに関するドキュメントリファレンス
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。