AnyConnectの再接続によるトラフィックフローの中断を修正する

内容

はじめに

このドキュメントでは、AnyConnectクライアントが適応型セキュリティアプライアンス(ASA)にわずか1分で再接続した場合に何が起こるかについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

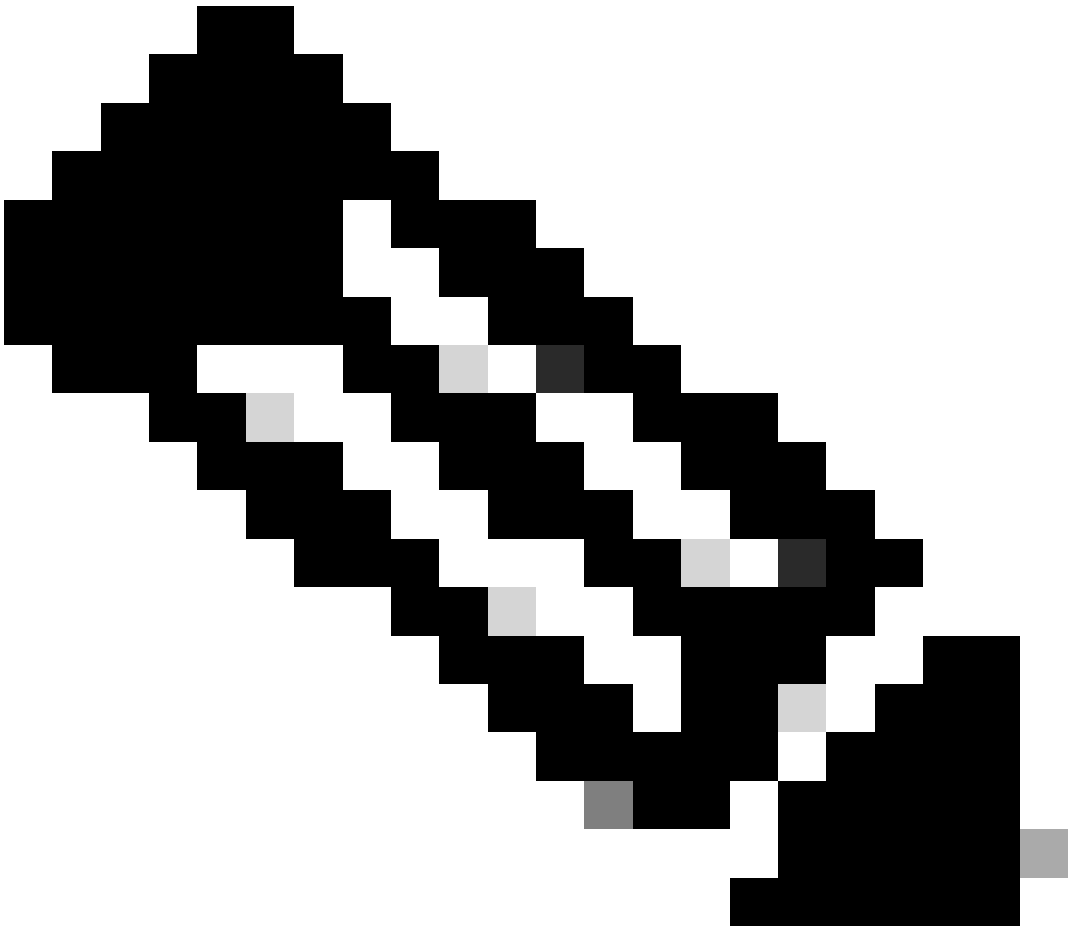
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

次の製品はこの問題の影響を受けます。

- ASAリリース9.17
- AnyConnectクライアントリリース4.10

背景説明

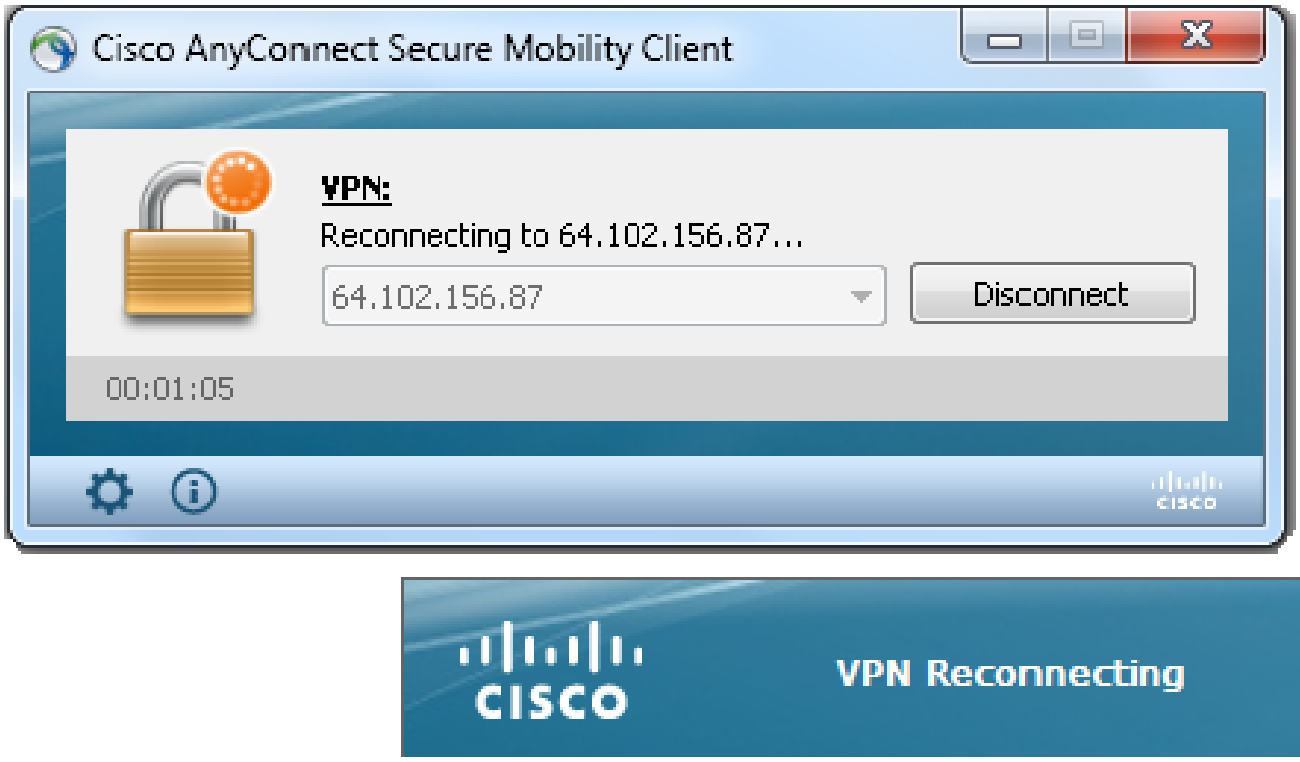


注:AnyConnectはCisco Secure Clientのブランドに変更されました。名前だけが変更され、インストールプロセスは同じです。

AnyConnectクライアントが適応型セキュリティアプライアンス(ASA)にわずか1分で再接続した場合、AnyConnectが再接続するまで、ユーザはTransport Layer Security(TLS)トンネルを介してトラフィックを受信できません。これは、このドキュメントで説明する他のいくつかの要因によって異なります。

症状

この例では、ASA に再接続される AnyConnect クライアントを示します。



ASA に次の syslog が表示されます。

```
%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347).
```

事象の説明

この問題では、次のDiagnostics and Reporting Tool(DART)ログが表示されます。

<#root>

```
****************************************
```

Date : 11/16/2022
Time : 01:28:50
Type : Warning
Source : acvpnagent

Description : Reconfigure reason code 16:

New MTU configuration.

```
****************************************
Date        : 11/16/2022
```

```
Time        : 01:28:50
Type        : Information
Source      : acvpnagent

Description : The entire VPN connection is being reconfigured.

********************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Information
Source      : acvpnui

Description : Message type information sent to the user:
Reconnecting to 10.1.1.2...

********************************************

Date        : 11/16/2022
Time        : 01:28:51
Type        : Warning
Source      : acvpnagent


Description : A new MTU needs to be applied to the VPN network interface.
Disabling and re-enabling the Virtual Adapter. Applications utilizing the
private network may need to be restarted.




********************************************
```

原因

この問題の原因は Datagram Transport Layer Security（DTLS）トンネルの構築に失敗したことです。失敗した理由は、次の 2 つが考えられます。

- DTLS がパスのどこかでブロックされている.
- デフォルト以外の DTLS ポートを使用している.

DTLS がパスのどこかでブロックされている

ASAリリース9.xおよびAnyConnectリリース4.xでは、クライアント/ASA間のTLS/DTLSに対してネゴシエートされる個別の最大伝送ユニット(MTU)の形式で最適化が導入されています。以前は、クライアントは TLS/DTLS の両方をカバーするおおよその推定値

を導出し、明らかに最適な状態ではありませんでした。現在、ASA は TLS/DTLS の両方のカプセル化のオーバーヘッドを計算し、それに応じて MTU 値を導出します。

DTLS がイネーブルである限り、クライアントは最適なパフォーマンスを実現するために VPN アダプタ（DTLS トンネルを確立する前にイネーブルにし、ルート/フィルタ適用に必要）で DTLS の MTU（この場合 1418）を適用します。DTLS トンネルを確立できない、またはある時点でそれがドロップされる場合、クライアントは TLS にフェールオーバーし、仮想アダプタ（VA）の MTU を TLS の MTU 値に合わせます（これには、セッション レベルの再接続が必要です）。

解決方法

この DTLS から TLS への移行を非表示にするために、管理者は DTLS トンネルの確立に問題がある（ファイアウォールの制限によるなど）ユーザ用に TLS 専用アクセスの個別のトンネル グループを設定できます。

- 最適なオプションは、AnyConnect の MTU 値を後でネゴシエートされる TLS の MTU よりも低く設定することです。

```
group-policy ac_users_group attributes
 webvpn
  anyconnect mtu 1300
```

これにより、TLS および DTLS MTU の値が等しくなります。この場合、再接続は表示されません。

- 2 番目のオプションは、フラグメンテーションを許可することです。

```
group-policy ac_users_group attributes
 webvpn
  anyconnect ssl df-bit-ignore enable
```

フラグメンテーションを使用すると、大きいパケット（サイズが MTU 値を超える）をフラグメント化し、TLS トンネルを経由して送信できます。

- 3番目のオプションは、次に示すようにMaximum Segment Size（MSS；最大セグメントサイズ）を1460に設定することです。

```
sysopt conn tcpmss 1460
```

この場合、TLS MTUはDTLS MTU 1418(AES/SHA1/LZS)よりも大きい1427(RC4/SHA1)にすることができます。これにより、ASAからAnyConnectクライアントへのTCPの問題は解決しますが（MSSのおかげで）、ASAからAnyConnectクライアントへの大きなUDPトラフィックは、AnyConnectクライアントのMTU 1418が小さいためにAnyConnectクライアントによってドロップされる可能性があるため、この問題が発生する可能性があります。sysopt conn tcpmssが変更されると、LAN-to-LAN(L2L)IPSec VPNトンネルなどの他の機能に影響を与える可能性があります。

再接続のワークフロー

次の暗号化が設定されていると仮定します。

ssl cipher tlsv1.2 custom AES256-SHA256 AES128-SHA256 DHE-RSA-AES256-SHA256

この場合、次の一連のイベントが発生します。

- AnyConnectは、SSL暗号化としてAES256-SHA256を使用して、親トンネルとTLSデータトンネルを確立します。
- DTLS はパスでブロックされ、DTLS トンネルを確立できません。
- ASA は、2 つの別個の値である TLS および DTLS の MTU 値を含むパラメータを AnyConnect にアナウンスします。
- DTLS の MTU はデフォルトで 1418 です。
- sysopt conn tcpmss 値（デフォルトは 1380）から TLS の MTU が計算されます。次の方法で、TLS の MTU が導出されます（debug webvpn anyconnect 出力から見た場合）。

1380 - 5 (TLS header) - 8 (CSTP) - 0 (padding) - 20 (HASH) = 1347

- AnyConnectがVPNアダプタを起動し、DTLS経由で接続できるという想定でDTLS MTUを割り当てます。
- これで、AnyConnect クライアントが接続され、ユーザは特定の Web サイトに移動します。
- ブラウザは TCP SYN を送信し、そこで MSS = 1418-40 = 1378 を設定します。
- ASA 内の HTTP サーバはサイズ 1418 のパケットを送信します。
- ASAは、これらのパケットをトンネルに送れず、フラグメント化できません。これは、これらのパケットにはDo not Fragment(DF)ビットが設定されているためです。

- ASAは、mp-svc-no-fragment-ASPドロップの理由でパケットを印刷し、ドロップします。

%ASA-6-722036: Group <ac_users_group> User <vpn> IP <10.1.75.111>
Transmitting large packet 1418 (threshold 1347)

- 同時に、ASAはICMP「Destination Unreachable, Fragmentation Needed」を送信側に送信します。

```
%ASA-6-602101: PMTU-D packet 1418 bytes greater than effective mtu 1347,
dest_addr=10.10.10.1, src_addr=10.48.66.200, prot=TCP
```

- インターネット制御メッセージ プロトコル（ICMP）が許可されている場合、送信側はドロップされたパケットを再送信し、すべてが機能し始めます。ICMP がブロックされた場合、トラフィックは ASA でブラックホール化されます。

- 何回か再送信すると、DTLSトンネルを確立できないことが認識され、VPNアダプタに新しいMTU値を再割り当てする必要があります。

- この再接続の目的は、新しい MTU を割り当てることです。

再接続の動作とタイマーの詳細については、『AnyConnectに関するFAQ：トンネル、再接続の動作、および非アクティビティタイマー』を参照してください。

関連情報

- 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。