トラフィック フローで中断を発生させる AnyConnect クライアントの 1 分ごとの再接続

目次

概要

このドキュメントでは、AnyConnect クライアントが正確に 1 分後に適応型セキュリティ アプライアンス（ASA）に再接続する可能性がある特定のシナリオについて説明します。 ユーザは、AnyConnect が再接続するまで Transport Layer Security（TLS）トンネル経由でトラフィックを受信できなくなる場合があります。 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。

該当するコンポーネント

- ASA リリース 9.0 またはリリース 9.1
- AnyConnect クライアント リリース 3.0 またはリリース 3.1

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).
```

問題の説明

この問題によって次の Diagnostics and Reporting Tool（DART）の口グが表示されます。

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

Date         : 11/16/2013
Time         : 01:28:50
Type         : Warning
Source       : acvpnagent

Description : Reconfigure reason code 16:
New MTU configuration.

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

Date         : 11/16/2013
Time         : 01:28:50
Type         : Information
Source       : acvpnagent

Description : The entire VPN connection is being reconfigured.

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

Date         : 11/16/2013
Time         : 01:28:51
Type         : Information
Source       : acvpnui

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

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

Date         : 11/16/2013
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 と AnyConnect リリース 3.x では、クライアントと ASA 間の TLS/DTLS に対してネゴシエートされる異なる最大伝送単位（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）。

解決策

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。

1. 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. 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. 3 番目のオプションは、次のように最大セグメント サイズ（MSS）を 1460 に設定することです。`sysopt conn tcpmss 1460` この場合、TLS の MTU は DTLS の MTU 1418（AES/SHA1/LZS）よりも大きい 1427（RC4/SHA1）になります。 これにより、ASA から AnyConnect クライアントへの TCP に関する問題が解決されますが（MSS により）、TCP の問題を解決する必要がありますが、ASA から AnyConnect クライアントへの大きい UDP トラフィックは、AnyConnect の低い MTU 1418 が原因で AnyConnect クライアントによってドロップされるため、この被害を受ける場合があります。 **sysopt conn tcpmss** を変更すると、LAN-to-LAN（L2L）IPSec VPN トンネルなどの他の機能に影響する場合があります。

デフォルト以外の DTLS ポートを使用している

DTLS 障害に考えられるもう 1 つの原因は、WebVPN をイネーブルにした後にデフォルト以外のポートで DTLS をイネーブルにしていることです（たとえば、**webvpn enable outside** コマンドを入力した場合） これは、Cisco Bug ID CSCuh61321 が原因で、ASA がデフォルト以外のポートをクライアントにプッシュしても、デフォルト ポートをリスニングし続けるリリース 9.x で発生します。 その結果、DTLS が構築されず、AnyConnect は再接続します。

```
webvpn
 port 444
```

```
 enable outside
 dtls port 444
 anyconnect enable

ciscoasa(config-webvpn)# show asp table socket


Protocol  Socket    State      Local Address            Foreign Address
SSL       0001fc08  LISTEN     172.16.11.1:444          0.0.0.0:*

DTLS      00020dc8  LISTEN     172.16.11.1:443          0.0.0.0:*
```

TLS トンネルを確立した後、クライアントは期待どおりにポート 444 への DTLS トンネルの確立を試みます。

問題の原因となるコマンドの順序と開かれた高速セキュリティ パス (ASP) の表のソケットは次のとおりです。

1. イネーブルになっていない WebVPN のソケットから開始します。`ciscoasa(config)# show run webvpn`
   ```
   webvpn
    anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
    anyconnect enable


   ciscoasa(config)# show asp table socket
   Protocol  Socket    State      Local Address            Foreign Address
   ciscoasa(config)#
   ```
2. TLS ポートを 444 に変更して、WebVPN をイネーブルにします。`ciscoasa(config-webvpn)# show run webvpn`
   ```
   webvpn
    port 444
    enable outside
    anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
    anyconnect enable


   ciscoasa(config-webvpn)# show asp tabl socket
   Protocol  Socket    State      Local Address            Foreign Address
   SSL       0001fc08  LISTEN     172.16.11.1:444          0.0.0.0:*
   DTLS      00020dc8  LISTEN     172.16.11.1:443          0.0.0.0:*
   ```
3. DTLS ポートを 444 に変更します。`ciscoasa(config-webvpn)# dtls port 444`
   ```
   ciscoasa(config-webvpn)#
   ciscoasa(config-webvpn)# show run webvpn
   webvpn
    port 444
    enable outside
    dtls port 444
    anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
    anyconnect enable

   ciscoasa(config-webvpn)# show asp table socket


   Protocol  Socket    State      Local Address            Foreign Address
   SSL       0001fc08  LISTEN     172.16.11.1:444          0.0.0.0:*
   DTLS      00020dc8  LISTEN     172.16.11.1:443          0.0.0.0:*
   ```

   注: DTLS ソケットのポートは 443 のままです。 この時点で、AnyConnect クライアントは 444 への DTLS を確立します。

解決策

この問題を回避するには、次の順序に従ってください。

1. WebVPN をディセーブルにします。
2. DTLS ポートを入力します。
3. WebVPN をイネーブルにします。

この動作は、DTLS ソケットが設定の入力直後に設定されたポートにアップデートされるリリース 8.4.x バージョンには存在しません。

ASA リリース 8.4.6：

```
ciscoasa(config-webvpn)# port 444
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000d5df 172.16.11.1:443 0.0.0.0:* LISTEN

ciscoasa(config-webvpn)# dtls port 444
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# show asp table socket

Protocol Socket Local Address Foreign Address State
SSL 0000bf2f 172.16.11.1:444 0.0.0.0:* LISTEN
DTLS 0000eb5f 172.16.11.1:444 0.0.0.0:* LISTEN << changed immediately
```

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 encryption rc4-sha1 aes128-sha1 aes256-sha1
```

この場合、次の一連のイベントが発生します。

- AnyConnect は、SSL 暗号化に RC4-SHA 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** の MTU をそのアダプタに割り当てます。
- 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。
- Don't Fragment（DF）ビットが設定されているため、ASA はこれらをトンネルにプッシュできず、フラグメント化することもできません。
- ASA は以下の内容を出力します。`%ASA-6-722036: Group <ac_users_group> User <vpn> IP`

```
<10.1.75.111>
Transmitting large packet 1418 (threshold 1347)
```
さらに、mp-svc-no-fragment-ASP drop が原因でパケットをドロップします。

- 同時に、ASA は送信側に ICMP Destination Unreachable, Fragmentation Needed を送信します。

```
    %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。
- 複数の再送信後、DTLS トンネルを確立できないことが認識され、新しい MTU 値を VPN アダプタに割り当てる必要があります。
- 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： を参照してください。
トンネル、再接続動作、および非アクティビティ タイマー

警告

Cisco Bug ID CSCuh61321 AC 3.1：ASA 誤ってハンドルが代替 DTLS ポートを処理し、再接続が発生する

関連情報

- **AnyConnect に関する FAQ： トンネル、再接続動作、および非アクティビティ タイマー**
- **テクニカルサポートとドキュメント - Cisco Systems**