AnyConnectに関するFAQへの回答：トンネル、DPD、非アクティビティタイマー

内容

概要
背景説明
トンネルの種類
ASA の出力例
DPD および非アクティブ タイマー
セッションが非アクティブ セッションと見なされるのは、どんなときですか。
ASA は SSL トンネルをドロップするのは、いつですか。
DPD がすでに有効な場合は、キープアライブが有効である必要があるのはなぜですか。
再接続の場合の AnyConnect クライアントの動作
実際のプロセス
システムが一時停止した場合の AnyConnect クライアントの動作
よく寄せられる質問（FAQ）
Q1.Anyconnect DPD に間隔がありますが、再試行が行われません。受信できないパケットの数がいくつになると、リモート エンドに障害があるとマークされるのですか。
Q2.DPD の処理は、IKEv2 を使用する AnyConnect では異なりますか。
Q3.AnyConnect の親トンネルには、他の目的がありますか。
Q4.非アクティブのセッションだけをフィルタリングし、ログオフできますか。
Q5.DTLS または TLS トンネルのアイドル タイムアウトの時間が切れると、親トンネルはどうなりますか。
Q6.DPDタイマーがセッションを切断した後もセッションを保持する理由と、ASAがIPアドレスを解放しない理由は何ですか。
Q7.ASA がアクティブからスタンバイにフェールオーバーする場合は、どのように動作しますか。
Q8両方が同じ値なのに、なぜ、アイドル タイムアウトと接続切断タイムアウトという 2 種類のタイムアウトがあるのですか。
Q9.クライアント マシンが一時停止されるとどうなりますか。
Q10. 再接続が発生すると、AnyConnect Virtual Adapter でフラップが発生するのですか。また、ルーティング テーブルが変更されるのですか。
Q11. [Auto Reconnect]はセッションの持続性を提供しますか。提供される場合、AnyConnect クライアントに追加される別の機能はありますか。
Q12. この機能は Microsoft Windows（Vista 32 ビットおよび 64 ビット、XP）のすべてのバリアントで動作します。Macintosh ではどうですか。OS X 10.4 で動作しますか。
Q13. 接続（有線、Wi-Fi、3G など）に関する機能に制限はありますか。異なるモードへの移行（Wi-Fi から 3G、3G から有線など）はサポートされますか。
Q14. 再開操作はどのように認証されますか。
Q15. 再接続時には LDAP 認可も実行されますか。それとも認証のみですか。
Q16. 再開時に PreLogin や Hostscan は実行されますか。
Q17. VPNロードバランシング(LB)と接続再開に関して、クライアントは以前に接続していたクラスタメンバーに直接接続しますか。
関連情報

概要

このドキュメントでは、Cisco AnyConnectセキュアモビリティクライアントトンネル、再接続動作とDead Peer Detection(DPD)、および非アクティビティタイマーについて説明します。

背景説明

トンネルの種類

AnyConnect セッションの接続に使用する方法は、次の 2 種類です。

- ポータルを使用（クライアントレス）
- スタンドアロン アプリケーションを使用

接続方法に基づいて、Cisco適応型セキュリティアプライアンス(ASA)上に3つの異なるトンネル（セッション）を作成します。各トンネル（セッション）には特定の目的があります。

1. クライアントレスまたは親トンネル：これは、ネットワーク接続の問題または休止状態のために再接続が必要な場合に必要なセッショントークンを設定するためにネゴシエーションで作成されるメインセッションです。接続メカニズムに基づいて、ASAはセッションをクライアントレス（ポータル経由のWeblaunch）または親（スタンドアロンAnyConnect）としてリストします。

   注：AnyConnect-Parentは、クライアントがアクティブに接続されていない場合のセッションを表します。実際には、cookie と同様に機能します。つまり、特定のクライアントから接続へのマッピングを行う、ASA のデータベース エントリです。クライアントがスリープ状態または休止状態になると、トンネル(IPsec/インターネットキー交換(IKE)/トランスポート層セキュリティ(TLS)/データグラムトランスポート層セキュリティ(DTLS)プロトコル)は破棄されますが、親はアイドルタイマーまたは最大接続時間が有効になるまで維持されます。これにより、ユーザは、再び認証を行わずに再接続することができます。

2. Secure Sockets Layer(SSL)トンネル：最初にSSL接続が確立され、DTLS接続の確立を試行する間に、データがこの接続を介して渡されます。DTLS の接続が確立すると、クライアントは、SSL 接続ではなく、DTLS 接続を介してパケットを送信します。一方、制御パケットは常に SSL 接続を通過します。

3. DTLSトンネル：DTLSトンネルが完全に確立されると、すべてのデータがDTLSトンネルに移動し、SSLトンネルは散発的な制御チャネルトラフィックに対してのみ使用されます。ユーザ データグラム プロトコル（UDP）に問題が発生した場合は、DTLS トンネルが削除され、すべてのデータは再び SSL トンネルを通過します。

ASA の出力例

2 つの接続方法の出力例を次に示します。

WebLaunch で接続された AnyConnect：

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1435
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : Clientless: (1)RC4 SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : Clientless: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 335765 Bytes Rx : 31508
Pkts Tx : 214 Pkts Rx : 18
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:13:37 UTC Fri Nov 30 2012
Duration : 0h:00m:34s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Clientless:
Tunnel ID : 1435.1
Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : Web Browser
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 329671 Bytes Rx : 31508

SSL-Tunnel:
Tunnel ID : 1435.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1241
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6094 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1435.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1250 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

スタンドアロン アプリケーションで接続された AnyConnect：

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

DPD および非アクティブ タイマー

セッションが非アクティブ セッションと見なされるのは、どんなときですか。

セッションは、SSL トンネルがセッションに存在しなくなったときにだけ、非アクティブと見なされます (タイマーの値が増加し始めます) 。したがって、各セッションには、SSL トンネルのドロップ時間のタイムスタンプが付けられます。

```
ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

ASA は SSL トンネルをドロップするのは、いつですか。

SSL トンネルの接続が切断される状況は、2 種類あります。

1. **DPD：DPD は、AnyConnect クライアントと ASA ヘッドエンドの間の通信の障害を検出するためにクライアントによって使用されます。**DPD は、ASA 上のリソースをクリーンアップするためにも使用されます。これにより、エンドポイントが DPD の ping に応答しない場合に、ヘッドエンドがデータベースで接続を保持しないことが保証されます。ASA がエンドポイントに DPD を送信し、DPD が応答した場合、アクションは実行されません。エンドポイントが応答しない場合、再送信の最大回数 (IKEv1またはIKEv2が使用されているかどうかによる) 後、ASAはセッションデータベース内のトンネルを切断し、セッションを「再開待ち」モードに移行します。これは、ヘッドエンドからの DPD が起動し、ヘッドエンドがクライアントと通信しなくなっていることを意味します。このような場合、ASA は、ユーザが各ネットワークをローミングし、スリープ状態にし、セッションを再確立できるように親トンネルを保留状態にします。これらのセッションは、アクティブに接続されているセッションをカウントし、次の状況になるとクリアされます。
   ユーザのアイドル タイムアウトクライアントが元のセッションを再開し、正常にログアウトした
   DPDを設定するには、 **anyconnect dpd-interval** コマンドを発行します。デフォルトでは、DPD が有効になっており、ASA (ゲートウェイ) とクライアントの両方について 30 秒に設定されています。

注意:Cisco Bug ID CSCts66926 - DPDがクライアント接続を失った後にDTLSトンネルの終了に失敗することに注意してください。

2. **アイドル タイムアウト：SSL トンネルの接続が切断される 2 番目の状況は、このトンネルのアイドル タイムアウトの時間が経過した場合です。**ただし、SSL トンネルだけではなく、DTLS トンネルもアイドル状態である必要があることに注意してください。DTLS セッションがタイムアウトしない限り、SSL トンネルはデータベースに保持されます。

DPD がすでに有効な場合は、キープアライブが有効である必要があるのはなぜですか。

すでに説明したように、DPD は、AnyConnect セッション自体を強制終了しません。DPD は、クライアントがトンネルを再確立できるよう、そのセッション内のトンネルを強制終了するだけです。クライアントがトンネルを再確立できない場合は、ASA でアイドル タイマーの時間が切れるまで、セッションが残ります。DPDはデフォルトで有効になっているため、ネットワークアドレス変換(NAT)、ファイアウォール、およびプロキシデバイスを使用して一方向でフローが閉じるため、クライアントが接続解除される場合があります。20 秒などの短い間隔でキープアライブを有効にすると、これを防止できます。

キープアライブは、特定のグループポリシーのWebVPN属性の下で、 **anyconnect ssl keepalive** コマンドが表示されない場合もあります。デフォルトでは、タイマーが 20 秒に設定されています。

再接続の場合の AnyConnect クライアントの動作

接続が中断された場合、AnyConnectは再接続を試みます。これは設定可能ではなく、自動的に行われます。ASA上のVPNセッションが有効である限り、AnyConnectが物理接続を再確立できる場合は、VPNセッションが再開されます。

再接続機能は、セッション タイムアウトまたは接続切断タイムアウト（実際はアイドル タイムアウト）の期限が切れるまで（タイムアウトが設定されていない場合は 30 分）続きます。期限が切れると、VPNセッションがすでにASAでドロップされているため、クライアントは続行できません。クライアントは、ASAが引き続きVPNセッションを保持していると認識している限り続行します。

AnyConnectは、ネットワークインターフェイスの変更に関係なく再接続します。ネットワークインターフェイス カード（NIC）の IP アドレスが変わっても、異なる NIC（無線から有線、またはその逆）に接続が切り替えられても問題ありません。

AnyConnect の再接続プロセスを検討する場合、注意が必要なセッションのレベルが 3 つあります。また、これらの各セッションの再接続動作は、弱く結合されており、あらゆる動作は、前のレイヤのセッション要素に依存せずに再確立できます。

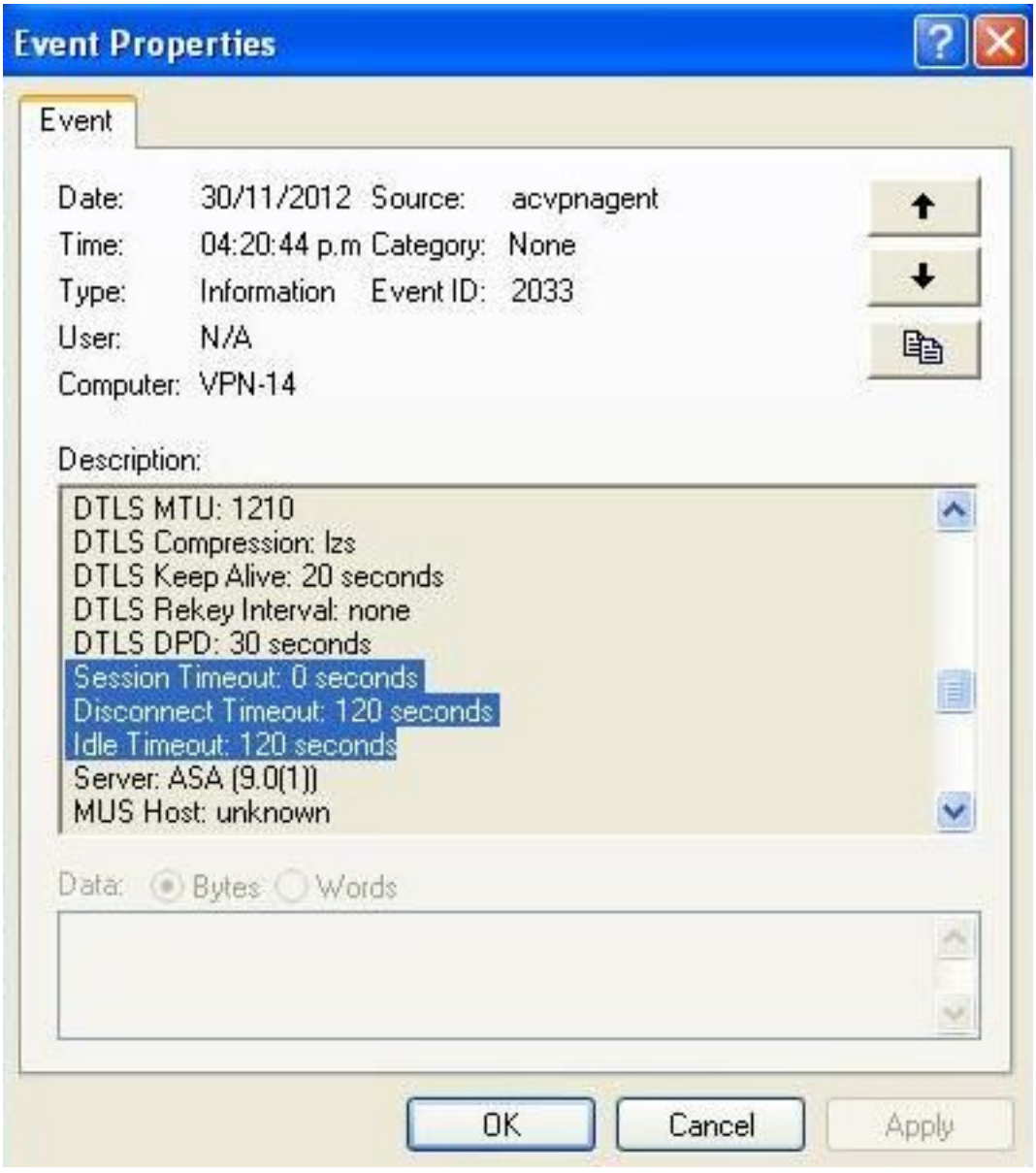
1. TCP または UDP 再接続 [OSI レイヤ 3]
2. TLS、DTLS、または IPsec（IKE+ESP）[OSI レイヤ 4]：TLS の再起動はサポートされていません。
3. VPN [OSI レイヤ 7]：VPN セッション トークンが認証トークンとして使用され、中断時に、安全なチャネル上で VPN セッションが再確立されます。 これは、独自のメカニズムであり、Kerberos トークンまたはクライアント証明書が認証に使用される方法に概念上、非常に似ています。 トークンは一意で、ヘッドエンドにより暗号化されて生成されます。これには、セッション ID の他に、暗号化されて生成された任意のペイロードが含まれます。ヘ

ッドエンドへの安全なチャネルが確立された後に、トークンは、最初の VPN 確立の一部としてクライアントに渡されます。トークンは、ヘッドエンドでのセッションのライフタイム中は有効であり、クライアントのメモリに保存されます。これは特権プロセスです。
ヒント：これらのASAリリース以降には、9.1(3)および8.4(7.1)という、より強力な暗号化セッショントークンが含まれています

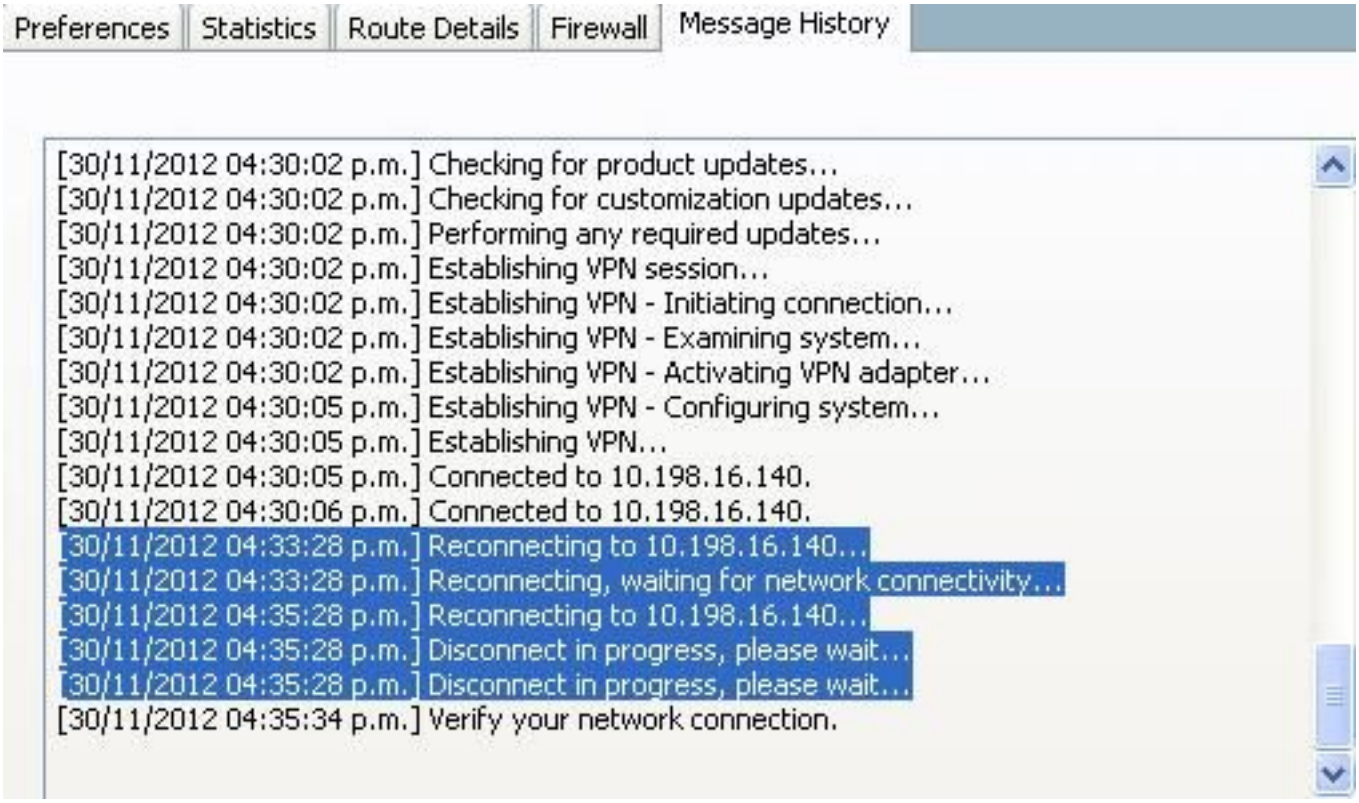
実際のプロセス

接続切断タイムアウトのタイマーは、ネットワーク接続が中断されるとすぐに開始されます。AnyConnect クライアントは、このタイマーの時間が切れるまでは再接続を試みます。接続切断タイムアウトは、グループ ポリシーの**アイドル タイムアウトおよび最大接続時間**のうち、最小の値に設定されます。

このタイマーの値は、ネゴシエーションの AnyConnect セッションのイベント ビューアに表示されます。



この例では、セッションは2分後（120秒）に切断されます。これは、AnyConnectのメッセージ履歴で確認できます。



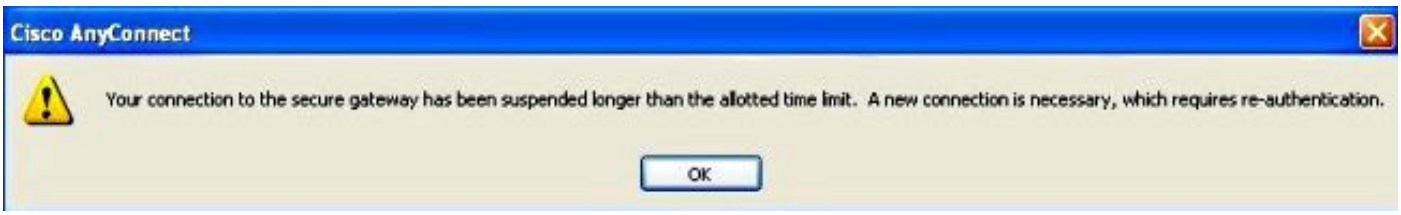
ヒント：再接続を試行するクライアントにASAが応答するには、ASAデータベースに親トンネルセッションが存在している必要があります。フェールオーバーの場合、再接続動作が機能するには、DPD が有効である必要があります。

前のメッセージに表示されているように、再接続は失敗しました。ただし、再接続が正常に完了すると、次の状況が発生します。

1. 親トンネルは同じままです。このトンネルは、再接続するためにセッションに必要なセッショントークンを維持するため、このトンネルは再ネゴシエートされません。
2. 新しい SSL および DTLS セッションが生成され、別のソース ポートが再接続で使用されます。
3. すべてのアイドル タイムアウト値が復元されます。
4. 非アクティブ タイムアウトが復元されます。

注意:Cisco Bug ID CSCtg33110に注意してください。VPN セッション データベースは、AnyConnect の再接続時に、ASA セッション データベースにあるパブリック IP アドレスを更新しません。

このように再接続が失敗する場合は、次のメッセージが表示されます。



注：この拡張要求は、さらに詳細な設定を行うために提出されました。Cisco Bug ID CSCsl52873 - ASAには、AnyConnectの設定可能な接続解除タイムアウトはありません。

システムが一時停止した場合の AnyConnect クライアントの動作

PC がスリープ状態になった後に AnyConnect による再接続を可能にするローミング機能が用意されています。クライアントは、アイドル タイムアウトまたはセッション タイムアウトの期限が切れるまで試行し続けます。システムが休止状態やスタンバイ状態になったとき、クライアントがただちにトンネルを削除することはありません。この機能を必要としないユーザの場合は、スリープ/再開再接続を防ぐために、セッションタイムアウトを低い値に設定します。

> **注**:Cisco Bug ID CSCso17627(バージョン2.3(111)+)の修正後、再開機能でこの再接続を無効にするために、制御ノブが導入されました。

AnyConnect の自動再接続の動作は、次の設定を含む AnyConnect XML プロファイルによって制御できます。

```
      <AutoReconnect UserControllable="true">true
<AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

この変更により、AnyConnectはコンピュータがスリープ状態から復帰したときに再接続を試みます。 AutoReconnectBehavior プリファレンスのデフォルトは DisconnectOnSuspend です。この動作は、AnyConnect クライアント リリース 2.2 の動作とは異なります。再開後の再接続については、ネットワーク管理者がプロファイルで ReconnectAfterResume を設定するか、プロファイルで AutoReconnect および AutoReconnectBehavior プリファレンスをユーザ制御可能にしてユーザが設定できるようにする必要があります。

よく寄せられる質問（FAQ）

Q1.Anyconnect DPD に間隔がありますが、再試行が行われません。受信できないパケットの数がいくつになると、リモート エンドに障害があるとマークされるのですか。

A. クライアントの観点からは、DPDはトンネル確立段階でトンネルを切断するだけです。クライアントがトンネル確立段階で3回の再試行（4つのパケットを送信）を行い、プライマリVPNサーバからの応答を受信しない場合、バックアップサーバが設定されていれば、バックアップサーバの1つを使用します。ただし、トンネルが確立された後は、欠落したDPDがクライアントの観点からトンネルに影響を与えることはありません。DPDの実際の影響は、「DPDと非アクティビティタイマー」セクションで説明されているように、VPNサーバに及びます。

Q2.DPD の処理は、IKEv2 を使用する AnyConnect では異なりますか。

A.はい、IKEv2では再試行回数が固定されています（6回の再試行/7パケット）。

Q3.AnyConnect の親トンネルには、他の目的がありますか。

A. クライアントはアップグレードプロセス中にアクティブに接続されていないため、ASAでのマッピングであることに加えて、親トンネルは、AnyConnectイメージアップグレードをASAからクライアントにプッシュするために使用されます。

Q4.非アクティブのセッションだけをフィルタリングし、ログオフできますか。

A. show vpn-sessiondb anyconnect filter inactiveコマンドを使用すると、非アクティブなセッションをフィルタリングできます。ただし、非アクティブ セッションだけをログオフするコマンドはありません。代わりに、特定のセッションをログオフするか、ユーザ (インデックス - 名前)、プロトコル、またはトンネル グループごとにすべてのセッションをログオフする必要があります。非アクティブなセッションだけをログオフするオプションを追加するための拡張要求、Cisco Bug ID CSCuh55707 (登録ユーザ専用) が提出されています。

Q5.DTLS または TLS トンネルのアイドル タイムアウトの時間が切れると、親トンネルはどうなりますか。

A. AnyConnect親セッションの「Idle TO Left」タイマーは、SSLトンネルまたはDTLSトンネルが切断された後にリセットされます。これにより「アイドルタイムアウト」を「接続切断」タイムアウトととして機能させることができます。実質的に、これはクライアントが再接続に使用できる時間になります。クライアントがタイマー内に再接続しない場合、親トンネルは終了します。

Q6.DPDタイマーがセッションを切断した後もセッションを保持する理由と、ASAがIPアドレスを解放しない理由は何ですか。

A.ヘッドエンドはクライアントの状態を認識していません。この場合、ASA は、セッションがアイドル タイマーでタイムアウトするまで、クライアントの再接続を期待して待機します。DPDはAnyConnectセッションを終了させません。クライアントがトンネルを再確立できるように、(そのセッション内で) トンネルを終了させるだけです。クライアントがトンネルを再確立しない場合は、アイドル タイマーの時間が切れるまでセッションが残ります。

セッションが使い果たされることが懸念される場合は、simultaneous-loginsを1などの低い値に設定します。この設定にすると、セッション データベースにセッションがあるユーザが再度ログインすると、それらの既存のセッションが削除されます。

Q7.ASA がアクティブからスタンバイにフェールオーバーする場合は、どのように動作しますか。

A.最初は、セッションが確立されると、3つのトンネル (親、SSL、およびDTLS) がスタンバイユニットに複製されます。ASAがフェールオーバーすると、DTLSおよびTLSセッションはスタンバイユニットに同期されないため再確立されますが、トンネルを通過するすべてのデータフローは、AnyConnectセッションの再確立後も中断なく動作する必要があります。

SSL/DTLS セッションはステートフルではないため、SSL の状態とシーケンス番号が保持されず、かなりの負担となる場合があります。したがって、これらのセッションは最初の状態から再確立する必要があります。これは、親セッションとセッション トークンで実行されます。

> **ヒント**：フェールオーバーイベントが発生した場合、キープアライブが無効になっていると、SSL VPNクライアントセッションはスタンバイデバイスに引き継がれません。

Q8両方が同じ値なのに、なぜ、アイドル タイムアウトと接続切断タイムアウトという 2 種類のタイムアウトがあるのですか。

A. プロトコルが開発されたときに、2 台のタイムアウトが提供されました。

- アイドル タイムアウト：データが接続経由で渡されない場合のタイムアウトです。
- 接続切断タイムアウト：接続が失われ、再確立できないために、VPN セッションを断念した場合のタイムアウトです。

接続切断タイムアウトは、ASA には実装されていません。その代わりに、ASA はクライアントに、接続切断タイムアウトとアイドル タイムアウトの両方の値としてタイムアウト値を送信します。

クライアントは、ASA がアイドル タイムアウトを処理するため、アイドル タイムアウトを使用しません。クライアントは、アイドルタイムアウト値と同じ接続解除タイムアウト値を使用して、ASAがセッションをドロップした後に再接続の試行を中止するタイミングを判断します。

クライアントにアクティブに接続されていない間、ASAはアイドルタイムアウトによってセッションをタイムアウトします。ASA に接続切断タイムアウトが実装されていない主な理由は、VPN セッションのたびにタイマーを追加したり、ASA のオーバーヘッドが増加したりすることを避けるためです（ただし、両方のインスタンスで異なるタイムアウト値で同じタイマーを使用できます。これは、2 つの状況が相互に排他的であるためです）。

接続切断タイムアウトで追加された唯一の値で、管理者は、クライアントがアイドル状態ではないが、アクティブには接続されていない場合のための別のタイムアウトを指定することができます。すでに説明したように、この問題はCisco Bug ID CSCsl52873に記載されています。

Q9.クライアント マシンが一時停止されるとどうなりますか。

A. デフォルトでは、接続が失われると AnyConnect は VPN 接続の再確立を試行します。デフォルトで、システムの復帰後は VPN 接続の再確立を試行しません。詳細については、「システムが一時停止した場合の AnyConnect クライアントの動作」参照してください。

Q10. 再接続が発生すると、AnyConnect Virtual Adapter でフラップが発生するのですか。また、ルーティング テーブルが変更されるのですか。

A. トンネルレベルの再接続では、どちらも行われません。これは、SSL または DTLS だけでの再接続です。放棄されるまで、これらは約 30 秒間続きます。DTLS が失敗すると、これが単に廃棄されます。SSL が失敗すると、セッションレベルでの再接続が行われます。セッションレベルの再接続によって、ルーティングが完全に再実行されます。再接続に割り当てられたクライアント アドレス、または仮想アダプタ（VA）に影響を与える他の設定パラメータを変更しない場合、VA は無効になりません。ASA から受信した設定パラメータに変更が加えられる可能性はほとんどありませんが、VPN 接続に使用される物理インターフェイスでの変更（アンドックして有線から Wi-Fi に切り替えた場合など）は、VPN 接続の最大伝送ユニット（MTU）値が異なる原因になる可能性があります。MTU 値は VA に影響するため、変更を加えると VA が無効化されてから再度有効化されます。

Q11. [Auto Reconnect]はセッションの持続性を提供しますか。提供される場合、AnyConnect クライアントに追加される別の機能はありますか。

A. AnyConnectは、アプリケーションのセッション持続性に対応する特別な「魔法」を提供しません。ただし、ASA に設定されているアイドル タイムアウトとセッション タイムアウトの期限が切れていなければ、VPN 接続はセキュア ゲートウェイへのネットワーク接続の再開直後に自動的に復元されます。また IPsec クライアントの場合とは異なり、同じクライアント IP アドレスに自動再接続されます。AnyConnect が再接続を試行する間、AnyConnect 仮想アダプタは有効で接続状態のままになるため、クライアント IP アドレスが全体の時間を通してクライアント PC で有効なまま残り、クライアント IP アドレスの持続性が提供されることになります。ただし、クラ

イアントPCアプリケーションは、VPN接続の復元に時間がかかりすぎる場合でも、企業ネットワーク上のサーバへの接続が失われていることを認識します。

Q12. この機能は Microsoft Windows (Vista 32 ビットおよび 64 ビット、XP) のすべてのバリアントで動作します。Macintosh ではどうですか。OS X 10.4 で動作しますか。

A. この機能は Mac および Linux で動作します。Mac および Linux では問題がありましたが、特に Mac 向けに新たな改善が行われました。Linuxでは依然として追加のサポートが必要ですが (Cisco Bug ID CSCsr16670、Cisco Bug ID CSCsm69213)、基本的な機能もあります。Linuxに関しては、AnyConnectは中断/再開 (スリープ/スリープ解除) が発生したことを認識しません。これによる基本的な影響は次の 2 つです。

- AutoReconnectBehaviorプロファイル/プリファレンス設定は、サスペンド/レジュームをサポートしないLinuxではサポートされないため、サスペンド/レジュームの後には常に再接続が行われます。
- Microsoft Windows と Macintosh の場合は、再開後すぐにセッション レベルで再接続が実行され、別の物理インターフェイスに迅速に切り替えることができます。Linuxでは、AnyConnectは中断/再開を完全に認識しないため、再接続は最初にトンネルレベル (SSLおよびDTLS) で行われます。これは再接続に少し時間がかかることを意味します。しかし、再接続はLinux上で引き続き発生します。

Q13. 接続 (有線、Wi-Fi、3G など) に関する機能に制限はありますか。異なるモードへの移行 (Wi-Fi から 3G、3G から有線など) はサポートされますか。

A. AnyConnectは、VPN接続が終了するまで、特定の物理インターフェイスに関連付けられません。VPN接続に使用される物理インターフェイスが失われた場合、または再接続が特定の障害しきい値を超えた場合、AnyConnectはそのインターフェイスを使用しなくなり、アイドルタイマーまたはセッションタイマーが切れるまで、使用可能なインターフェイスを使用してセキュアゲートウェイに到達しようとします。物理インターフェイスを変更すると、VAのMTU値が変わる可能性があります。そのため、VAを無効にして再度有効にする必要がありますが、引き続き同じクライアントIPアドレスが使用されます。

ネットワークの中断 (インターフェイスのダウン、ネットワークの変更、インターフェイスの変更) があると、AnyConnectは再接続を試みます。再接続時に再認証は必要ありません。これは物理インターフェイスを切り替えた場合にも適用されます。

例：

```
1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in
30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs
```

Q14. 再開操作はどのように認証されますか。

A. 再開では、セッションのライフタイム中に残っている認証済みトークンを再送信すると、セッションが再確立されます。

Q15. 再接続時には LDAP 認可も実行されますか。それとも認証のみですか。

A. LDAP 認可は最初の接続時にのみ実行されます。

Q16. 再開時に PreLogin や Hostscan は実行されますか。

A. いいえ、これらは最初の接続時にのみ実行されます。類似機能が、将来の定期的ポスチャ アセスメントの機能で予定されています。

Q17. VPNロードバランシング(LB)と接続再開に関して、クライアントは以前に接続していたクラスタメンバーに直接接続しますか。

A：**はい**、現在のセッションを再確立するためにDNS経由でホスト名を再解決することはないため、これは正しい動作です。

関連情報

- **ASA DPDリファレンス：Cisco Bug ID CSCsr63074 - 7.2.4のs2でピアが停止し、トンネルがアイドル状態でない場合にDPDが送信されない**
- **テクニカル サポートとドキュメント – Cisco Systems**

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。