

AnyConnect VPN クライアントのトラブルシューティング ガイド - 一般的な問題

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トラブルシューティングのプロセス](#)

[インストールと仮想アダプタの問題](#)

[接続の解除と初期接続確立の失敗](#)

[通過トラフィックの問題](#)

[AnyConnect のクラッシュの問題](#)

[フラグメンテーションまたは通過トラフィックの問題](#)

[自動的なアンインストール](#)

[クラスタ FQDN の設定問題](#)

[バックアップ サーバリストの設定](#)

[AnyConnect : 破損したドライバ データベースの問題](#)

[修復](#)

[修復の失敗](#)

[データベースの分析](#)

[エラー メッセージ](#)

[エラー : セッション管理データベースを更新できません](#)

[解決策 1](#)

[解決策 2](#)

[エラー : 「Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register」](#)

[解決方法](#)

[エラー : 「VPNネゴシエーション要求に対する応答で、セキュアゲートウェイからエラーを受信しました。Please contact your network administrator」](#)

[解決方法](#)

[エラー : セッションを確立できませんでした。Session limit of 2 reached.](#)

[解決策 1](#)

[解決策 2](#)

[エラー : AnyconnectをASAに接続しようとしたときに、AnyconnectがVPNサーバで有効になっていません](#)

[解決方法](#)

[エラー : 「%ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 \(threshold 1206\)」](#)

[解決方法](#)

[エラー : セキュアゲートウェイがエージェントのVPN接続または再接続の要求を拒否しました。](#)

[解決方法](#)

エラー：「Unable to update the session management database」

解決方法

エラー：「The VPN client driver has encountered an error」

解決方法

エラー：「Unable to process response from xxx.xxx.xxx.xxx」

解決方法

エラー：「Login Denied , unauthorized connection mechanism , contact your administrator」

解決方法

エラー：「Anyconnect package unavailable or corrupted.Contact your system administrator

解決方法

エラー：「The AnyConnect package on the secure gateway could not be located」

解決方法

エラー：「Secure VPN via remote desktop is not supported」

解決方法

エラー：「受信したサーバー証明書またはそのチェーンがFIPSに準拠していません。A VPN connection will not be established

解決方法

エラー：「証明書検証エラー」

解決方法

エラー：「VPN Agent Serviceは問題が発生したため、終了する必要があります。We are sorry for the inconvenience

解決方法

エラー：「このインストールパッケージを開くことができませんでした。Verify that the package exists

解決方法

エラー：「Error applying transforms.Verify that the specified transform paths are valid」

解決方法

エラー：「The VPN client driver has encountered an error」

解決方法

エラー：「A VPN reconnect resulted in different configuration setting.The VPN network setting is being re-initialized.Applications utilizing the private network may need to be restored.

解決方法

ログイン時の AnyConnect エラー

解決方法

Windows 7 で AnyConnect の切断後に IE Proxy の設定値が復元されない

解決方法

エラー： AnyConnect Essentialsは、これらすべてのセッションが終了するまで有効にできません。

解決方法

エラー： AnyConnectクライアントに接続すると、Internet Explorerの[インターネット]オプションの[接続]タブが非表示になります。

解決方法

エラー：他のユーザがAnyConnect VPNを介して正常に接続できる場合に「Login Failed」エラーメッセージが表示されるユーザがほとんどいない

解決方法

エラー：表示している証明書が、表示しようとしているサイトの名前と一致しません。

解決方法

[Windows 7 マシンで CSD の Vault から AnyConnect を起動できない](#)

[解決方法](#)

[フェールオーバー後に AnyConnect プロファイルがスタンバイ側へ複製されない](#)

[解決方法](#)

[Internet Explorer がオフラインになると AnyConnect クライアントがクラッシュする](#)

[解決方法](#)

[エラーメッセージ : TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER](#)

[解決方法](#)

[エラーメッセージ : 「Connection attempt has failed due to invalid host entry.」](#)

[解決方法](#)

[エラー : 「Ensure your server certificates can pass strict mode if you configure always-on VPN」](#)

[解決方法](#)

[エラー : 「An internal error occurred in the Microsoft Windows HTTP Services.」](#)

[解決方法](#)

[エラー : 「The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.」](#)

[解決方法](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco AnyConnect VPN Client を介して動作しないアプリケーションに適用されるトラブルシューティングのシナリオ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情報は、バージョン 8.x が稼働する Cisco 適応型セキュリティ アプライアンス (ASA) に基づいています。

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

トラブルシューティングのプロセス

この一般的なトラブルシューティング シナリオは、Microsoft Windows ベースのコンピュータを使用するエンドユーザを対象に、Cisco AnyConnect VPN Client で動作しないアプリケーション

に適用されます。以降のセクションでは下記の問題に対応し、そのソリューションを提供しています。

- [インストールと仮想アダプタの問題](#)
- [接続の解除と初期接続確立の失敗](#)
- [通過トラフィックの問題](#)
- [AnyConnect のクラッシュの問題](#)
- [フラグメンテーションまたは通過トラフィックの問題](#)

インストールと仮想アダプタの問題

次のステップを実行します。

1. 次のように、デバイスのログ ファイルを取得します。

- Windows XP または Windows 2000 :

```
<#root>
```

```
\Windows\setupapi.log
```

- Windows Vista :



注：これらのファイルを表示するには、非表示フォルダを表示する必要があります。

```
<#root>
```

```
\Windows\Inf\setupapi.app.log
```

```
\Windows\Inf\setupapi.dev.log
```

setupapi ログファイルにエラーが表示される場合は、詳細度を 0x2000FFFF に上げることができます。

2. 次のように、MSI インストーラのログ ファイルを取得します。

<#root>

\Windows\Temp

ファイル名の形式は anyconnect-win-x.x.xxxx-k9-install-yyyyyyyyyyyyyyyy.log です。インストールするクライアントのバージョンの最新ファイルを取得します。x.xxxx は 2.0.0343 のようにバージョンに従って変更され、yyyyyyyyyyyyyyyy はインストールの日付と時間を示します。

3. 次のように、PC のシステム情報ファイルを取得します。

a. コマンド プロンプトまたは DOS ボックスから、次のように入力します。

- Windows XP または Windows 2000 :


<#root>

```
winmsd /nfo c:\msinfo.nfo
```

- Windows Vista :

<#root>

```
msinfo32 /nfo c:\msinfo.nfo
```

 注：このプロンプトに入力したら、しばらく待ちます。このファイルの完了には、2 ~ 5 分かかかる可能性があります。

b. 次のように、コマンド プロンプトから systeminfo ファイル ダンプを取得します。

Windows XP および Windows Vista :

<#root>

systeminfo c:\sysinfo.txt

ドライバの問題をデバッグするには、「[AnyConnect : 破損したドライバ データベースの問題](#)」を参照してください。

接続の解除と初期接続確立の失敗

接続の解除や初期接続確立の失敗など、AnyConnect クライアントで接続の問題が発生する場合は、次のファイルを取得します。

- どの設定が接続障害の原因となっているのかを判断するための ASA からのコンフィギュレーション ファイル :

ASA のコンソールから、write net x.x.x.x:ASA-Config.txt と入力します (x.x.x.x はネットワーク上の TFTP サーバの IP アドレスです)。

または

ASA のコンソールから、show running-config と入力します。画面上に設定がすべて表示されるようにして、テキスト エディタにカット アンド ペーストして保存します。

- ASA イベント ログ :
 1. ASA 上で auth、WebVPN、セキュア ソケット レイヤ (SSL)、および SSL VPN クライアント (SVC) のイベントのロギングをイネーブルにするには、次の CLI コマンドを発行します。

```
<#root>
```

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

2. AnyConnect セッションを開始して、障害が再現できることを確認します。コンソールからロギング出力をテキスト エディタへキャプチャして、保存します。
3. ロギングを無効にするには、no logging enable を実行します。

- クライアント PC の Windows Event Viewer からの Cisco AnyConnect VPN Client ログ :

1. [Start] > [Run] を選択します。

2. 次のように入力します。

```
eventvwr.msc /s
```

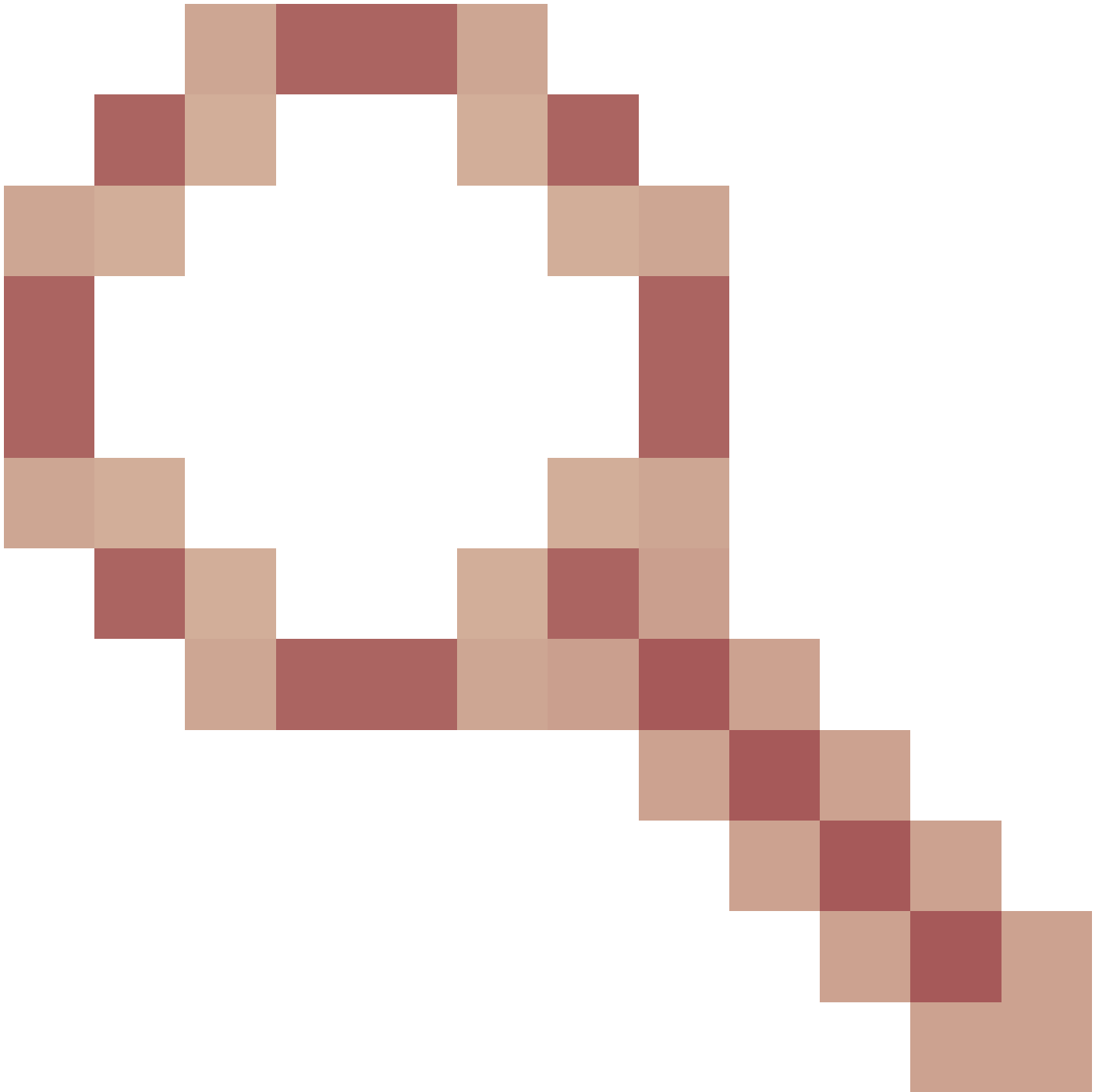
3. [Cisco AnyConnect VPN Client] ログを右クリックし、[Save Log File As AnyConnect.evt] を選択します。




注 : 常に .evt ファイル形式で保存してください。

ユーザが AnyConnect VPN クライアントと接続できない場合は、確立済みの Remote Desktop Protocol (RDP) セッションまたはクライアント PC で有効になっている Fast User Switching に関連した問題の可能性があります。その場合は、AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection will not be established というエラーメッセージがクライアント PC に表示されます。この問題を解決するには、確立済みの RDP セッションの接続を解除し、Fast User Switching を無効にします。この動作は、クライアントプロファイルの [Windows ログインの強制 (Windows Logon Enforcement)] 属性によって制御されますが、現時点では、複数のユーザが同じマシンに同時にログオンしているときにユーザが VPN 接続を確立することを可能にする設定はありません。機能拡張要求

[CSCsx15061](#)



は、この機能に対処するために提出されました。

 注:AnyConnectクライアントがASAに接続できるように、ポート443がブロックされていないことを確認してください。

ユーザが AnyConnect VPN Client から ASA に接続できない場合は、AnyConnect クライアントのバージョンと ASA ソフトウェア イメージのバージョンの互換性がないために問題が生じた可能性があります。この場合、ユーザには「The installer was not able to start the Cisco VPN client, clientless access is not available」というエラーメッセージが表示されます。

この問題を解決するには、AnyConnect クライアントを、ASA ソフトウェア イメージと互換性があるバージョンにアップグレードします。

AnyConnect に初めてログインするとき、ログインスクリプトが実行されません。切断して再度ログインすると、ログインスクリプトが正常に実行されます。これは、正常な動作です。

AnyConnect VPN ClientをASAに接続すると、「User not authorized for AnyConnect Client access, contact your administrator」というエラーが表示されることがあります。

このエラーは、ASA が AnyConnect イメージを認識できない場合に生じます。イメージが ASA にロードされれば、AnyConnect から問題なく ASA に接続できます。

このエラーは、Datagram Transport Layer Security (DTLS) を無効にすると解決できます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択し、[Enable DTLS] チェック ボックスをオフにします。これで DTLS は無効になります。

dartbundleファイルは、ユーザが切断されたときに次のエラーメッセージを表示します。

TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE:The secure gateway failed to respond to Dead Peer Detection packets。このエラーは、デッドピア検出 (DPD) が原因で DTLS チャネルが切断されたことを意味します。このエラーは、DPD のキープアライブを微調整して、以下のコマンドを発行することによって解決します。

```
<#root>
```

```
webvpn
  svc keepalive 30
  svc dpd-interval client 80
  svc dpd-interval gateway 80
```

ASA バージョン 8.4(1) 以降では、svc keepalive と svc dpd-interval のコマンドを次のように、anyconnect keepalive と anyconnect dpd-interval のコマンドに置き換えます。

```
<#root>
```

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

通過トラフィックの問題

ASA を介した AnyConnect セッションでプライベート ネットワークへのトラフィックの通過に関する問題が検出された場合は、次の手順でデータを収集します。

1. コンソールから ASA コマンド show vpn-sessiondb detail svc filter name <username> を実行し、出力を取得します。出力に Filter Name: xxxxxが表示される場合は、show access-list XXXXXの出力を収集します。アクセスリスト XXXXXによって、対象のトラフィックフローがブロックされていないことを確認します。

2. [AnyConnect VPN Client] > [Statistics] > [Details] > [Export] の順に選択して、AnyConnect の統計情報 (AnyConnect-ExportedStats.txt) をエクスポートします。
3. ASA コンフィギュレーション ファイルで nat 設定文を確認します。ネットワーク アドレス変換 (NAT) がイネーブルになっている場合、これらの nat 設定文により、クライアントに戻されるデータが NAT の結果からは免除される必要があります。たとえば、AnyConnect プールの IP アドレスを NAT 免除 (nat 0) するには、CLI で次のコマンドを使用します。

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. トンネリングされたデフォルト ゲートウェイをセットアップに対して有効にする必要があるかどうかを判断します。従来型のデフォルト ゲートウェイは、非暗号化トラフィックのラストリゾート ゲートウェイです。

以下に例を挙げます。

```
<#root>
```

```
!--- Route outside 0 0 is an incorrect statement.
```

```
route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2
```

```
tunneled
```

例のように、VPN Client で、VPN Gateway のルーティング テーブルにないリソースへのアクセスが必要な場合、パケットは標準のデフォルト ゲートウェイを介してルーティングされます。VPN Gateway では、完全な内部ルーティング テーブルがなくてもこれを解決できます。この例では、tunneled キーワードを使用できます。

5. ASA のインスペクション ポリシーによって、AnyConnect トラフィックがドロップされるかどうかを確認します。Cisco ASA のモジュラ ポリシー フレームワークを導入することによって、AnyConnct クライアントで使用する特定のアプリケーションを除外できます。たとえば、次のコマンドを使用して、Skinny プロトコルを免除することができます。

```
<#root>
ASA(config)#
policy-map global_policy

ASA(config-pmap)#
class inspection_default

ASA(config-pmap-c)#
no inspect skinny
```

AnyConnect のクラッシュの問題

次のデータ収集手順を実行します。

1. Microsoft Utility Dr Watson が有効になっていることを確認します。これを確認するには、[Start] > [Run] を選択し、Drwtsn32.exe を実行します。次のように設定して、[OK] をクリックします。


```
Number of Instructions      : 25
Number of Errors To Save   : 25
Crash Dump Type            : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts  : Checked
Append To Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File    : Checked
```

クラッシュが発生する場合、.log および .dmp ファイルを C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson から収集します。これらのファイルが使用中として表示される場合は、ntbackup.exe を使用します。

2. クライアント PC の Windows Event Viewer で、Cisco AnyConnect VPN Client ログを次のように取得します。
 - a. [Start] > [Run] を選択します。
 - b. 次のように入力します。

```
<#root>
eventvwr.msc /s
```

c. [Cisco AnyConnect VPN Client] ログを右クリックし、[Save Log File As AnyConnect.evt] を選択します。

 注：常に.evtファイル形式で保存してください。

フラグメンテーションまたは通過トラフィックの問題

Microsoft Outlook など、一部のアプリケーションは機能しません。ただし、小さい ping など、他のトラフィックはトンネルを通過できます。

このことは、ネットワーク内のフラグメンテーションの問題に対するヒントとなります。一般消費者向けのルータは、パケットのフラグメンテーションと再構成に関しては特に貧弱です。

一連の ping の規模を変えてみて、特定のサイズで失敗するかどうかを確認します。たとえば、ping -l 500、ping -l 1000、ping -l 1500、ping -l 2000 などです。

フラグメンテーションが発生する特別なユーザグループを設定し、このグループの SVC Maximum Transition Unit (MTU) を 1200 に設定することが推奨されます。こうすることで、広範なユーザベースに影響を与えることなく、この問題が発生しているユーザに対して修正を加えることができます。

問題

AnyConnect との接続後に TCP 接続がハングします。

解決方法

ユーザにフラグメンテーションの問題が発生しているかどうかを確認するには、ASA で AnyConnect クライアントの MTU を調整します。

```
ASA(config)#group-policy <name> attributes
                webvpn
                svc mtu 1200
```

自動的なアンインストール

問題

接続が終了すると、AnyConnect VPN Client が自動的にアンインストールされます。クライアントログには、keep installed が無効になっていることが表示されます。

解決方法

AnyConnect は、Adaptive Security Device Manager (ASDM) で keep installed オプションが選択されていないと、自身のアンインストールを実行します。この問題を解決するには、グループポリシーの下で svc keep-installer installed コマンドを設定します。

クラスタ FQDN の設定問題

問題：AnyConnectクライアントには、クラスタの完全修飾ドメイン名(FQDN)ではなく、ホスト名が事前に入力されています。

SSL VPN にロードバランシング クラスタが設定されている場合、クライアントがクラスタへの接続を試行すると、この要求はノード ASA にリダイレクトされてクライアントは正常にログインします。少し経ってから、そのクライアントが再度クラスタに接続しようとする、[Connect to] エントリにそのクラスタの FQDN がありません。代わりに、クライアントのリダイレクト先となったノード ASA のエントリが存在します。

解決方法

これは最後に接続したホスト名を AnyConnect クライアントが保持するために発生します。この動作はバグとして登録されています。このバグの詳細については、Cisco Bug ID [CSCsz39019](#) を参照してください。推奨される回避策は、Cisco AnyConnect をバージョン 2.5 にアップグレードすることです。

バックアップ サーバ リストの設定

ユーザが選択したメイン サーバが到達不能になった場合に備えて、バックアップ サーバ リストが設定されています。これは、AnyConnect プロファイルの [Backup Server] ペインに定義されます。次のステップを実行します。

1. [AnyConnect Profile Editor](#) ([登録ユーザ専用](#)) をダウンロードします。ファイル名は AnyConnectProfileEditor2_4_1.jar です。
2. AnyConnect Profile Editor を使用して XML ファイルを作成します。
 - a. [server list] タブに移動します。
 - b. [Add] をクリックします。
 - c. [Hostname] フィールドにメイン サーバを入力します。
 - d. [Host address] フィールドのバックアップ サーバ リストの下に、バックアップ サーバを追加します。次に、[Add] をクリックします。
3. XML ファイルの入手後、これを ASA で使用している接続に割り当てる必要があります。
 - a. ASDM で、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

- b. 該当するプロファイルを選択して [Edit] をクリックします。
- c. [Default Group Policy] セクションの [Manage] をクリックします。
- d. 該当するグループ ポリシーを選択して、[Edit] をクリックします。
- e. [Advanced] を選択してから [SSL VPN Client] をクリックします。
- f. [New] をクリックします。さらに、プロファイルの名前を入力し、XML ファイルを割り当てる必要があります。

4. XML ファイルをダウンロードするために、クライアントをセッションに接続します。

AnyConnect : 破損したドライバ データベースの問題

SetupAPI.log ファイル内の次のエントリは、カタログ システムが破損していることを示しています。

W239 ドライバ署名クラス リスト : " C:\WINDOWS\INF\certclas.inf" was missing or invalid.Error 0xfffffde5: Unknown Error」を参照してください。

また、Error(3/17): Unable to start VA, setup shared queue, or VA gived up shared queueというエラーメッセージが表示されることもあります。

クライアントで次のログを受け取る可能性があります : 「The VPN client driver has encountered an error」。

修復

この問題は、Cisco Bug ID [CSCsm54689](#) が原因です。この問題を解決するには、AnyConnect を起動する前に、Routing and Remote Access Service が無効になっていることを確認します。それでも問題が解決されない場合は、次の手順を実行します。

1. PC 上で管理者としてコマンド プロンプトを開きます (Vista 上では昇格したプロンプト)。
2. net stop CryptSvc を実行します。
3. 次のコマンドを実行します。

```
esentutl /p%systemroot%\System32\catroot2\
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. 確認を求められたら [OK] を選択して修復を試行します。
5. コマンドプロンプトを終了します。
6. 再起動します。

修復の失敗

修復に失敗する場合は、次の手順を実行します。

1. PC 上で管理者としてコマンドプロンプトを開きます (Vista 上では昇格したプロンプト)。
2. net stop CryptSvc を実行します。
3. %WINDIR%\system32\catroot2 to catroot2_old ディレクトリの名前を変更します。
4. コマンドプロンプトを終了します。
5. 再起動します。

データベースの分析

データベースをいつでも分析して、その有効性を判断できます。

1. PC 上で管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行します。

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

詳細については、『[System Catalog Database Integrity](#)』を参照してください。

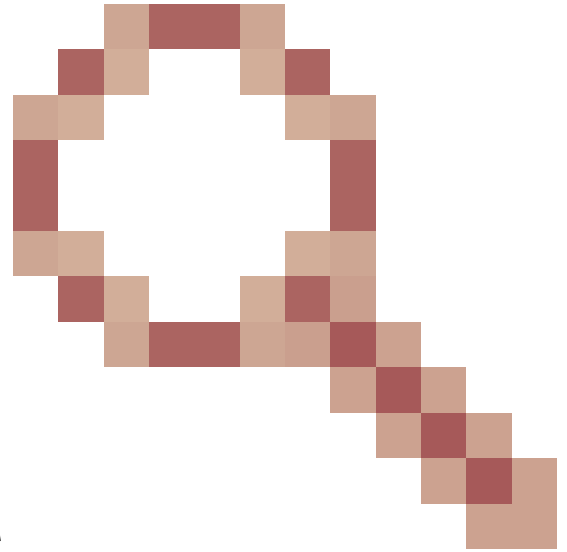
エラー メッセージ

エラー : セッション管理データベースを更新できません

SSL VPNがWebブラウザを介して接続されている場合、「Unable to Update the Session Management Database.」というエラーメッセージが表示され、ASAログに「%ASA-3-211001: Memory allocation Error」と表示されます。The adaptive security appliance failed to allocate RAM system memory」と表示されます。

解決策 1

この問題は、Cisco Bug ID [CSCsm51093](#) が原因です。この問題を解決するには、ASA をリロードするか、または ASA ソフトウェアを上記のバグに記載されている暫定リリースにアップグレー



ドします。Cisco Bug ID [CSCsm51093](#)を参照してください
参照してください。

解決策 2

脅威検出を使用している場合は、ASA で脅威検出を無効にすることによってもこの問題が解決することがあります。

エラー : 「Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register」

ラップトップまたは PC で AnyConnect のクライアントを使用する場合、インストール時にエラーが発生します。

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."
```

このエラーが発生するとインストーラの処理が進まず、クライアントは削除されます。

解決方法

このエラーは、次の方法で解決される可能性があります。

- 最新の AnyConnect クライアントは、公式には Microsoft Windows 2000 をサポートしていません。これは、2000 コンピュータに関連したレジストリ問題です。
- VMware アプリケーションを削除します。AnyConnect のインストール後に VMware アプリケーションを再度 PC へ追加できます。

- 信頼済みサイトに ASA を追加します。
- これらのファイルを \ProgramFiles\Cisco\CiscoAnyconnect フォルダから新しいフォルダにコピーし、コマンドプロンプトで regsvr32 vpnapi.dll を実行します。
 - vpnapi.dll
 - vpncommon.dll
 - vpncommoncrypt.dll
- ラップトップまたは PC でオペレーティング システムのイメージを変更します。

AnyConnect クライアントでは、このエラーに関連して次のようなログ メッセージが表示されます。

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
Info 1721. There is a problem with this Windows Installer package. A program required for
this install to complete could not be run. Contact your support personnel or package
vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN
Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application
Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

エラー：「VPNネゴシエーション要求に対する応答で、セキュアゲートウェイからエラーを受信しました。Please contact your network administrator

Cisco AnyConnect VPN クライアントを使用して、クライアントが VPN に接続しようとしたときにこのエラーが発生します。

セキュアゲートウェイから、次のメッセージを受信します。

「Illegal address class」または「Host or network is 0」または「Other error」

解決方法

これは、ASA ローカル IP プールの枯渇が原因です。VPN プールのリソースが枯渇しているため、IP プールの範囲を拡大する必要があります。

この問題は Cisco Bug ID [CSCsl82188](#) でファイリングされています。このエラーは通常、アドレ


ス割り当て用のローカルプールが枯渇した場合、またはアドレスプールに 32 ビット サブネットマスクが使用されている場合に発生します。回避策は、アドレスプールを拡大し、プールに 24 ビットのサブネットマスクを使用することです。

エラー：セッションを確立できませんでした。Session limit of 2 reached.

AnyConnect VPN クライアントを使用して 3 つ以上のクライアントを接続しようとする、 「Login Failed」というエラーメッセージがクライアントに表示され、ASA のログには「Session could not be established.Session limit of 2 reached.ASA では AnyConnect essential ライセンスを使用していて、ASA のバージョンは 8.0.4 です。

解決策 1

このエラーは、ASA バージョン 8.0.4 が AnyConnect essential ライセンスをサポートしていないために発生します。つまり、ASA を 8.2.2 にアップグレードする必要があります。これによりエラーが解決されます。

 注：使用するライセンスに関係なく、セッションの制限に達すると、ユーザにlogin failedエラーメッセージが表示されます。

解決策 2

このエラーは、確立が許可される VPN セッションの上限を設定するために、vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit コマンドを使用すると発生する可能性があります。session-limit を 2 に設定すると、インストールされているライセンスでサポートされるセッション数に関係なく、ユーザが確立できるセッション数は最大 2 になります。このエラーメッセージを回避するには、必要な VPN セッション数を session-limit の値として設定してください。

エラー：AnyconnectをASAに接続しようとしたときに、AnyconnectがVPNサーバで有効になっていません

AnyConnect を ASA に接続しようとする、 「Anyconnect not enabled on VPN server error message」というエラーメッセージが出ます。

解決方法

このエラーは、ASDM を使用して ASA の外部インターフェイスで AnyConnect を有効にすることにより解決します。外部インターフェイスで AnyConnect を有効にする方法の詳細については、『[Configure Clientless SSL VPN \(WebVPN \) on the ASA](#)』を参照してください。

エラー：「%ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)」

エラーメッセージ「%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x > Transmitting large packet 1220 (threshold

1206)」がASAのログに表示されます。このログの意味と解決方法を教えてください。

解決方法

このログメッセージは、大きなパケットが該当クライアントに送信されたことを示しています。該当パケットの送信元は、クライアントのMTUを意識していません。また、圧縮不能なデータの圧縮が原因の場合もあります。その場合の回避策は、svc compression none コマンドを使用して、SVC 圧縮を無効にすることです。これにより問題は解決します。

エラー：セキュアゲートウェイがエージェントのVPN接続または再接続の要求を拒否しました。

AnyConnectクライアントに接続すると、「The secure gateway has rejected the agent's vpn connect or reconnect request.A new connection requires re-authentication and must be started manually.Please contact your network administrator if this problem persists.セキュアゲートウェイから次のメッセージを受信しました：アドレスが割り当てられていません」。

このエラーは、AnyConnectクライアントへの接続時にも表示されます。「The secure gateway has rejected the connection attempt.A new connection attempt to the same or another secure gateway is needed, which requires re-authentication.The following message was received from the secure gateway:Host or network is 0」

このエラーは、AnyConnectクライアントへの接続時にも表示されます。「The secure gateway has rejected the agent's vpn connect or reconnect request.A new connection requires a re-authentication and must be started manually.Please contact the network administrator if the problem persists.セキュアゲートウェイから次のメッセージを受信しました：「ライセンスがありません」。

解決方法

ルータでリロード後にプールの設定が失われました。該当する設定をルータに追加する必要があります。

```
<#root>
```

```
Router#
```

```
show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
  svc address-pool SSLP00
```

「The secure gateway has rejected the agent's vpn connect or reconnect request.A new connection requires a re-authentication and must be started manually.Please contact the network administrator if the problem persists.セキュアゲートウェイから次のメッセージを受信しました：「No License」エラーは、AnyConnectモビリティライセンスが欠落している場合に発生します。ライセンスがインストールされれば、問題は解決されます。

エラー：「Unable to update the session management database」

WebPortalで認証しようとする時、「Unable to update the session management database」というエラーメッセージが表示されます。

解決方法

これは、ASA のメモリ割り当てに関連した問題です。この問題は、ASA のバージョンが 8.2.1 の場合に発生することが多くなっています。本来 ASA が完全に機能するには 512 MB の RAM が必要です。

恒久的な解決策は、メモリを 512 MB にアップグレードすることです。

一時的な回避策として、次の手順によってメモリを解放してみてください。

1. threat-detection を無効にします。
2. SVC 圧縮を無効にします。
3. ASA をリロードします。

エラー：「The VPN client driver has encountered an error」


これは、AnyConnect に接続するときに、クライアント マシンで表示されるエラー メッセージです。

解決方法

このエラーを解決するには、次の手順に従って手動で AnyConnect VPN エージェントをインタラクティブに設定します。

1. [My Computer] を右クリックし、[Manage] > [Services and Applications] > [Services] の順に選択して [Cisco AnyConnect VPN Agent] を選択します。
2. [Properties] を右クリックしてログオンし、[Allow service to interact with the desktop] を選択します。

これにより、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent のレジストリ タイプ値 DWORD が 110 (デフォルトは 010) に設定されます。

 注：これが使用される場合、このインスタンスでは MST トランスフォームが優先されます。これは、これらの方法でこれを手動で設定すると、インストール プロセスまたはアップグレード プロセスの後で、設定が毎回必要になるためです。このため、この問題を発生させているアプリケーションを識別する必要があります。

Windows PCでルーティングとリモートアクセスサービス(RRAS)が有効になっていると、AnyConnectが失敗し、「The VPN client driver has encountered an error.」というエラーメッセージが表示されます。この問題を解決するには、AnyConnect を起動する前に RRAS が無効になっていることを確認します。詳細については、Cisco Bug ID [CSCsm54689](#) を参照してください。

エラー：「Unable to process response from xxx.xxx.xxx.xxx」

AnyConnect クライアントは、Cisco ASA に接続できません。AnyConnect ウィンドウに「Unable to process response from xxx.xxx.xxx.xxx」というエラー メッセージが表示されます。

解決方法

このエラーを解決するには、次の回避策を試してください。

- ASA から WebVPN を削除し、再度有効にします。
- ポート番号を既存の 443 から 444 に変更し、443 で再び有効にします。

WebVPN を有効にして WebVPN のポートを変更する方法の詳細についてはこの[ソリューション](#)を参照してください。

エラー：「Login Denied , unauthorized connection mechanism , contact your administrator」

AnyConnect クライアントは、Cisco ASA に接続できません。AnyConnect ウィンドウに「Login Denied , unauthorized connection mechanism , contact your administrator」というエラー メッセージが表示されます。

解決方法

このエラー メッセージが表示される原因の大部分は、不適切または不完全な設定です。この問題を解決するには、設定を調べて、必要な項目が適切に設定されていることを確認します。

<

エラー：「Anyconnect package unavailable or corrupted.Contact your system administrator

このエラーは、ASA に接続するために Macintosh クライアントから AnyConnect ソフトウェアを起動しようとするときに発生します。

解決方法

この問題を解決するには、次の手順を実行します。

1. Macintosh 版 AnyConnect パッケージを ASA のフラッシュにアップロードします。
2. 使用される AnyConnect パッケージを指定するために WebVPN の設定を変更します。

```
webvpn
  svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
  svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

ASA バージョン 8.4(1) 以降では、次のように、svc image コマンドを anyconnect image コマンドに置き換えます。

```
<#root>

hostname(config)#
webvpn

hostname(config-webvpn)#
anyconnect image disk0:/

anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#
anyconnect image disk0:/

anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

エラー：「The AnyConnect package on the secure gateway could not be located」

このエラーは、ユーザが Linux マシンで AnyConnect を起動して ASA に接続しようとするときに発生します。エラー全体を次に示します。

```
<#root>

"The AnyConnect package on the secure gateway could not be located. You may
be experiencing network connectivity issues. Please try connecting again."
```

解決方法

このエラーメッセージを解消するには、クライアントマシンで使用されているオペレーティングシステム (OS) に AnyConnect クライアントが対応しているかどうかを確認します。

その OS に対応している場合は、WebVPN の設定に目的の AnyConnect パッケージが指定されているかどうかを確認します。詳細については、このドキュメントの「[使用できないまたは破損している Anyconnect パッケージ](#)」を参照してください。

エラー : 「Secure VPN via remote desktop is not supported」

ユーザはリモート デスクトップへのアクセスを実行できません。「Secure VPN via remote desktop is not supported」というエラーメッセージが表示されます。

解決方法

この問題は、Cisco Bug ID [CSCsu22088](#)および[CSCso42825](#)が原因で発生します。AnyConnect VPN クライアントをアップグレードすると、この問題を解決できます。詳細については、これらのバグを参照してください。

エラー : 「受信したサーバー証明書またはそのチェーンがFIPSに準拠していません。A VPN connection will not be established

ASA 5505 への VPN を試行すると、「The server certificate received or its chain does not comply with FIPS.A VPN connection will not be established」というエラーメッセージが表示されます。

解決方法

このエラーを解決するには、AnyConnect ローカル ポリシー ファイルで連邦情報処理標準 (FIPS) を無効する必要があります。このファイルは、通常、C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml にあります。このファイルがこのパスにない場合は、C:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml などのパスを使用して、別のディレクトリにファイルを配置してください。目的の xml ファイルが見つかったら、それを次のように変更します。

変更前のフレーズは次のとおりです。

```
<FipsMode>>true</FipsMode>
```

これを、次のように変更します。

```
<FipsMode>>false</FipsMode>
```

その後、コンピュータを再起動します。このファイルを修正するユーザには、管理アクセス許可が必要です。

エラー : 「証明書検証エラー」

ユーザは AnyConnect を起動できず、「Certificate Validation Failure」というエラーが表示されます。

解決方法

AnyConnect と IPsec クライアントでは、証明書認証の機能が異なります。証明書認証が機能するためには、ブラウザにクライアント証明書をインポートし、証明書認証を使用するように接続プロファイルを変更する必要があります。外部インターフェイスで SSL クライアント証明書を使用できるようにするには、ASA でこのコマンドを有効にする必要もあります。

```
ssl certificate-authentication interface outside port 443
```

エラー：「VPN Agent Serviceは問題が発生したため、終了する必要があります。
We are sorry for the inconvenience

Windows XP PC に AnyConnect バージョン 2.4.0202 がインストールされている場合は、ローカリゼーションファイルのアップデートが停止し、「vpnagent.exe fails」というエラーメッセージが表示されます。

解決方法

この動作は、Cisco Bug ID [CSCsq49102](#) に記録されています。推奨される回避策は、Citrix クライアントを無効にすることです。

エラー：「このインストールパッケージを開くことができませんでした。Verify that the package exists

AnyConnect をダウンロードすると、次のエラーメッセージが表示されます。

```
「Contact your system administrator.インストーラは次のエラーで失敗しました：このインストールパッケージを開くことができませんでした。Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package.」
```

解決方法

この問題を解決するには、次の手順を実行します。

1. アンチウイルス ソフトウェアを削除します。
2. Windows ファイアウォールを無効にします。
3. 手順 1 と 2 のどちらも効果がない場合は、マシンをフォーマットしてからインストールします。
4. 問題がまだ解決しない場合は、[TAC ケース](#)をオープンします。

エラー：「Error applying transforms.Verify that the specified transform paths are valid」

ASA から AnyConnect を自動ダウンロードしている最中に、次のエラー メッセージが表示されま
す。

```
<#root>
```

```
"Contact your system administrator. The installer failed with the following error:  
Error applying transforms. Verify that the specified transform paths are valid."
```

MacOS 用の AnyConnect と接続している場合は、次のエラー メッセージが表示されます。

```
<#root>
```

```
"The AnyConnect package on the secure gateway could not be located. You may be  
experiencing network connectivity issues. Please try connecting again."
```

解決方法

この問題を解決するには、次のいずれかの回避策を実行します。

1. これは、MST トランスレーション ファイルの破損が根本原因である可能性があります (インポートした場合など)。この問題を修正するには、次の手順を実行します。
 - a. MST 変換テーブルを削除します。
 - b. ASA に MacOS 用の AnyConnect イメージを設定します。
2. ASDM から、[Network (Client) Access] > [AnyConnect Custom] > [Installs] のパスをたどり、AnyConnect のパッケージ ファイルを削除します。パッケージが [Network (Client) Access] > [Advanced] > [SSL VPN] > [Client Setting] に引き続きあることを確認します。

これらのいずれの方法でも問題を解決できない場合は、[シスコ テクニカル サポート](#)にお問い合わせください。

エラー : 「The VPN client driver has encountered an error」

次のエラー メッセージが表示されます。

```
<#root>
```

```
The VPN client driver has encountered an error when connecting through Cisco  
AnyConnect Client.
```

解決方法

AnyConnect クライアントをアンインストールしてからアンチウイルス ソフトウェアを削除すると、この問題が解決される場合があります。この後、AnyConnect クライアントを再インストールします。この方法で効果がない場合は、この問題を修正するために PC を再フォーマットしてください。

エラー : 「A VPN reconnect resulted in different configuration setting.The VPN network setting is being re-initialized.Applications utilizing the private network may need to be restored.

このエラーは、AnyConnect を起動しようとするとき出力されます。

```
<#root>
```

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

解決方法

このエラーを解決するには、次のコマンドを使用します。

```
group-policy <Name> attributes
    webvpn
    svc mtu 1200
```

ASA バージョン 8.4(1) 以降では、次のように svc mtu コマンドを anyconnect mtu コマンドに置き換えます。

```
<#root>
```

```
hostname(config)#
group-policy
```

```
attributes
```

```
hostname(config-group-policy)#
```

```
webvpn
```

```
hostname(config-group-webvpn)#
```

```
anyconnect mtu 500
```

ログイン時の AnyConnect エラー

問題

AnyConnect がクライアントに接続するときに、次のエラーが発生します。

```
The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.
```

解決方法

この問題は、AnyConnect のプロファイルに以下の変更を加えると解決することがあります。

AnyConnect プロファイルに次の行を追加します。

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

Windows 7 で AnyConnect の切断後に IE Proxy の設定値が復元されない

問題

Windows 7 で、IE プロキシが Automatically detect settings に設定され、AnyConnect が新しいプロキシの設定をプッシュすると、ユーザによる AnyConnect セッションの終了後に、IE プロキシの設定が Automatically detect settings へリストアされません。プロキシを Automatically detect settings に設定する必要のあるユーザの場合、これが LAN の問題につながります。

解決方法

この動作は、Cisco Bug ID [CSCtj51376](#) に記録されています。推奨される回避策は、[AnyConnect 3.0](#) にアップグレードすることです。

エラー： AnyConnect Essentialsは、これらすべてのセッションが終了するまで有効にできません。

このエラー メッセージは、AnyConnect Essentials ライセンスを有効にしようとしたときに Cisco ASDM で出力されます。

<#root>

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

解決方法

これは、ASA の正常な動作です。AnyConnect Essentials は、個別にライセンスされた SSL VPN クライアントです。これは ASA で完全に設定され、次の例外を除いて AnyConnect の全機能を提供します。

- Cisco Secure Desktop (CSD) がない (Host Scan、Vault、キャッシュ クリーナを含む)
- クライアントレス SSL VPN 非対応
- Windows Mobile サポートがオプション

このライセンスは、共有されている SSL VPN プレミアム ライセンスと同時に使用できません。一方のライセンスが必要な場合は、他方を無効にする必要があります。

エラー： AnyConnectクライアントに接続すると、Internet Explorerの[インターネット]オプションの[接続]タブが非表示になります。

AnyConnect クライアントに接続後、Internet Explorer の [Internet] オプションの [Connection] タブが非表示になります。

解決方法

これは、msie-proxy lockdown 機能が原因です。この機能を有効にすると、AnyConnect VPN セッションの間、Microsoft Internet Explorer の [Connections] タブが非表示になります。この機能を無効にしたとき、[Connections] タブの表示状態が変更されないままになります。

エラー： 他のユーザがAnyConnect VPNを介して正常に接続できる場合に「Login

Failed」エラーメッセージが表示されるユーザがほとんどいない

多くのユーザは AnyConnect VPN を介して接続できますが、一部のユーザに Login Failed Error メッセージが表示されます。

解決方法

この問題は、ユーザの [do not require pre-authentication] チェック ボックスをオンにすることにより解決できます。

エラー：表示している証明書が、表示しようとしているサイトの名前と一致しません。

AnyConnect プロファイルのアップデート中に、証明書が無効であることを示すエラー メッセージが表示されます。これは Windows のみで発生し、プロファイルのアップデート段階で起こります。次のエラー メッセージが表示されます。

```
<#root>
```


```
The certificate you are viewing does not match with the name of the site  
you are trying to view.
```

解決方法

これは、証明書の FQDN を使用するように AnyConnect プロファイルのサーバ リストを変更することによって解決できます。

次に XML プロファイルの例を示します。

```
<ServerList>  
  
<HostEntry>  
    <HostName>vpn1.ccsd.net</HostName>  
  
</HostEntry>  
  
</ServerList>
```

 注：サーバのパブリックIPアドレスに既存のエントリ(<HostAddress>など)がある場合は、それを削除し、サーバのFQDNのみを保持します(たとえば、<HostName>は保持されますが、<Host Address>は保持されません)。

Windows 7 マシンで CSD の Vault から AnyConnect を起動できない

CSD の Vault から AnyConnect を起動しようとしても実行できません。これは、Windows 7 マシンの使用時に発生します。

解決方法

現在のところ、サポートされていないため、この問題は解決できません。

フェールオーバー後に AnyConnect プロファイルがスタンバイ側へ複製されない

AnyConnect 3.0 VPN クライアントと ASA バージョン 8.4.1 ソフトウェアの組み合わせでは、正常に機能します。ただし、フェールオーバー後、AnyConnect プロファイル関連の設定は複製されません。

解決方法

この問題は、Cisco Bug ID [CSCtn71662](#) で観測され記録されています。一時的な回避策は、このファイルをスタンバイユニットに手動でコピーすることです。

Internet Explorer がオフラインになると AnyConnect クライアントがクラッシュする

この問題が発生すると、AnyConnect イベント ログに次のようなエントリが記録されます。

```
Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type

Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION
```

解決方法

この動作は、Cisco Bug ID [CSCtx28970](#) で観測され記録されています。これを解決するには、AnyConnect アプリケーションを終了し、再起動します。接続エントリは再起動後に表示されません。

エラーメッセージ : TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

AnyConnect クライアントが接続に失敗し、「Unable to establish a connection」というエラーメッセージが表示されます。AnyConnect のイベント ログには「TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER」エラーが記録されます。

解決方法

この問題が発生するのは、ヘッドエンドに設定されているスプリット トンネリングのスプリット トンネル リストが非常に大きく（約 180 ~ 200 エントリ）、グループ ポリシーに 1 つ以上のクライアント属性が設定されている場合です（dns-server など）。

この問題を解決するには、次の手順を実行します。

1. スプリット トンネル リストのエントリ数を減らします。
2. 次の設定を使用して、DTLS を無効にします。

```
group-policy groupName attributes
  webvpn
    svc dtls none
```

詳細は、Cisco Bug ID [CSCtc41770](#) を参照してください。

エラーメッセージ：「Connection attempt has failed due to invalid host entry」

AnyConnect で証明書を使用するために認証されているときに、「Connection attempt has failed due to invalid host entry」というエラーメッセージが出されます。

解決方法

この問題を解決するためには、次に示すいずれかの方法を試してください。

- AnyConnect をバージョン 3.0 へアップグレードします。
- ご使用のコンピュータで Cisco Secure Desktop を無効にします。

詳細は、Cisco Bug ID [CSCti73316](#) を参照してください。

エラー：「Ensure your server certificates can pass strict mode if you configure always-on VPN」

AnyConnect で Always-On 機能を有効にすると、「Ensure your server certificates can pass strict mode if you configure always-on VPN」というエラーメッセージが表示されます。

解決方法

このエラーメッセージは、[Always-On] 機能を使用する場合、ヘッドエンドに有効なサーバ証明

書が設定されている必要があることを意味します。有効なサーバ証明書がないと、この機能は動作しません。[Strict Cert Mode] は、AnyConnect のローカル ポリシー ファイルに設定するオプションで、有効な証明書を接続で使用することが保証されます。ポリシー ファイルでこのオプションを有効にして偽の証明書で接続すると、接続に失敗します。

エラー : 「An internal error occurred in the Microsoft Windows HTTP Services」

この Diagnostic AnyConnect Reporting Tool (DART) は試行が 1 回失敗したことを示しています。

<#root>

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1170

Invoked Function: HttpSendRequest

Return Code: 12004 (0x00002EE4)
Description:

An internal error occurred in the Microsoft Windows HTTP Services

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472

Invoked Function: ConnectIfc::sendRequest

Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode

Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Connection attempt failed. Please try again.

Windows マシンのイベント ビューア ログも参照してください。

解決方法

破損した Winsock 接続が原因である可能性があります。次のコマンドを使用してコマンド プロンプトから接続をリセットし、Windows マシンを再起動してください。

```
netsh winsock reset
```

詳細については、ナレッジ ベース記事『[How to determine and to recover from Winsock2 corruption in Windows Server 2003, in Windows XP, and in Windows Vista](#)』を参照してください。

エラー : 「The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.」

この Diagnostic AnyConnect Reporting Tool (DART) は試行が 1 回失敗したことを示しています。

```
Date       : 10/27/2014
Time       : 16:29:09
Type      : Error
Source    : acvpnu
```

```
Description : Function: CTransportWinHttp::handleRequestError
File: .\CTransportWinHttp.cpp
Line: 854
```

The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configura

```
Date       : 10/27/2014
Time       : 16:29:09
Type      : Error
Source    : acvpnu
```

```
Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1199
```

```
Invoked Function: CTransportWinHttp::handleRequestError
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE
```

```
Date       : 10/27/2014
Time       : 16:29:09
Type      : Error
Source    : acvpnu
```

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 3026
Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE
Connection attempt failed. Please try again.

解決方法

次の KB 更新によると、Windows 8.1 は RC4 をサポートしていません。

<http://support2.microsoft.com/kb/2868725>

「ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1」コマンドを使用して ASA で SSL VPN の DES/3DES 暗号を設定するか、次のドキュメントで説明されているように、クライアントマシンで Windows レジストリファイルを編集します。

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

関連情報

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [AnyConnect VPN Client に関する FAQ](#)
- [Cisco Secure Desktop \(CSD \) に関する FAQ](#)
- [Cisco AnyConnect VPN Client](#)
- [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。