CHAPTER 8

AnyConnect セッションの管理、モニタリング、およびトラブルシューティング

この章では、次のテーマおよびタスクについて説明します。

すべての VPN セッションの接続解除

Cisco AnyConnect Secure Mobility Client セッションを含め、すべての SSL VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff svc** コマンドを使用します。

vpn-sessiondb logoff svc

これに応答して、システムが、VPN セッションをログオフすることの確認を要求します。Enter キーまたは y キーを押して確認します。ログオフをキャンセルするには、その他のキーを押します。

次に、すべての SSL VPN セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions logged off : 6
hostname#
```

個別の VPN セッションの接続解除

name オプション、または **index** オプションを使用すると、個別にセッションをログオフできます。

vpn-sessiondb logoff name *name*

vpn-sessiondb logoff index *index*

たとえば、ユーザ tester をログオフさせるには、次のコマンドを入力します。

```
hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
hostname#
```

ユーザ名とインデックス番号（クライアント イメージの順序で設定される）は、両方とも **show vpn-sessiondb svc** コマンドの出力で確認できます。

次の例では、**vpn-sessiondb logoff** コマンドの **name** オプションを使用して、セッションを終了しています。

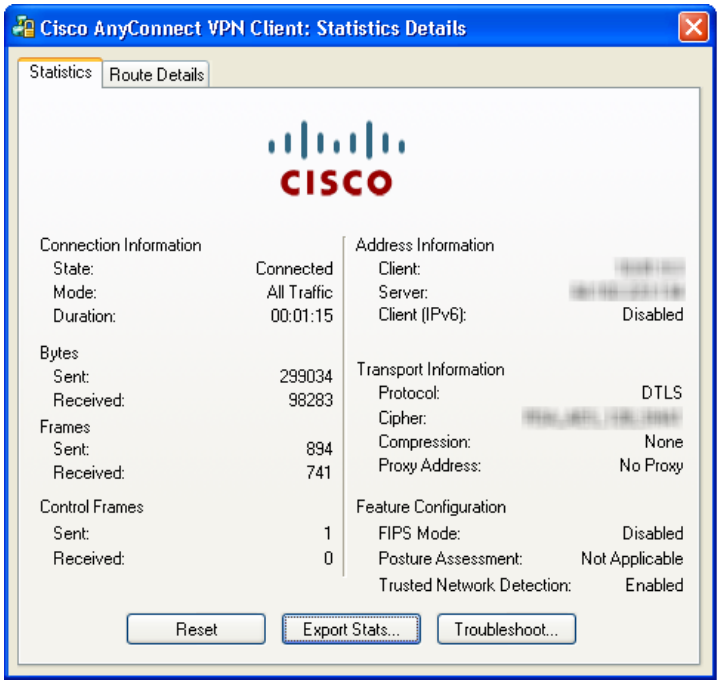
```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

詳細な統計情報の表示

現在の AnyConnect セッションに関する統計情報を表示するには、ユーザの GUI の [Details] ボタンをクリックします。

[Statistics Details] ダイアログが表示されます。このウィンドウの [Statistics] タブでは、統計情報のリセットとエクスポート、およびトラブルシューティング用のファイル収集を行えます。

図 8-1　AnyConnect VPN クライアントの [Statistics Details] ダイアログ



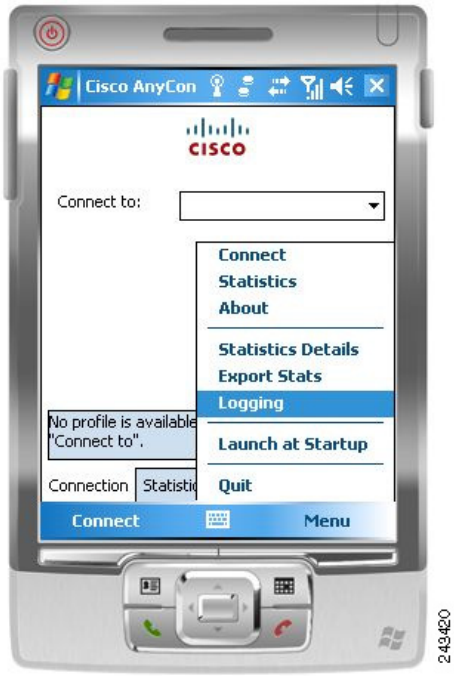
このウィンドウに表示されるオプションは、クライアント PC にロードされているパッケージによって異なります。オプションを使用できない場合は、ダイアログボックスでそのボタンがアクティブにならず、オプション名の横に「(Not Installed)」と表示されます。オプションは次のとおりです。

- [Reset] をクリックすると、接続情報がゼロにリセットされます。AnyConnect による新しいデータの収集がすぐに開始されます。
- [Export Stats...] をクリックすると、接続の統計情報がテキスト ファイルに保存され、あとから分析とデバッグを行えます。
- [Troubleshoot...] をクリックすると、DART（Diagnostic AnyConnect Reporting Tool）ウィザードが起動されます。指定したログ ファイルと診断情報を結び付けることで、クライアント接続の分析とデバッグに使用できます。DART パッケージの詳細については、「DART を使用したトラブルシューティング情報の収集」（P.8-5）を参照してください。

Windows Mobile デバイスでの統計情報の表示

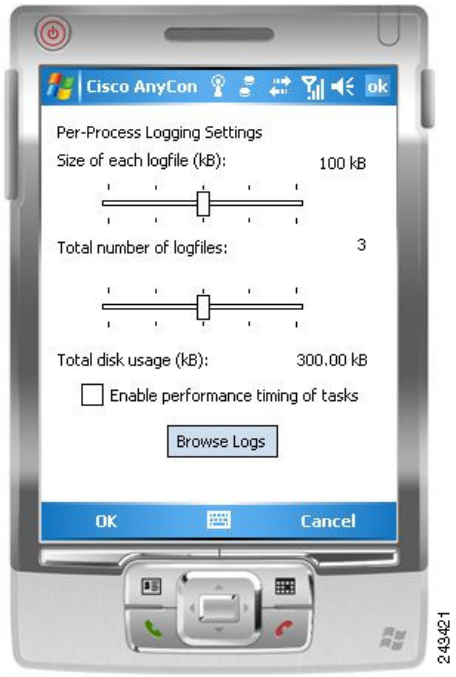
Windows Mobile デバイスの AnyConnect ユーザも、画面右下の [Menu] をクリックし、表示されたメニューから希望する機能を選択すると、統計情報の詳細のエクスポート機能とロギング機能を使用できます（図 8-2）。

図 8-2　Windows Mobile の [Logging] メニュー



[Logging] をクリックすると、ロギング設定ダイアログボックスが表示されます（図 8-3）。

図 8-3　Windows Mobile のロギング設定ダイアログボックス



このダイアログボックスのスライダーを動かすと、ログ ファイルの総数と、1 つのログ ファイルの容量を制御し、タスクの実行タイミングをイネーブルにできます。

[Browse Logs] をクリックすると、別のブラウザ ウィンドウにログ メッセージの HTML リストが表示されます。

VPN 接続の問題の解決

次の項は、VPN 接続の問題を解決するために参照してください。

MTU サイズの調整

多くの家庭用エンド ユーザ終端装置（ホーム ルータなど）は、IP フラグメントの作成またはアセンブリを適切に処理しません。特に UDP の場合はそうなります。DTLS は UDP ベースのプロトコルであるため、場合によってはフラグメンテーションを防止するため、MTU を小さくする必要があります。MTU パラメータでは、クライアントと ASA にトンネルで転送するパケットの最大サイズが設定されます。VPN ユーザで大量のパケット損失が発生している場合、または Microsoft Outlook などのアプリケーションがトンネル経由で機能しない場合は、フラグメンテーションの問題が発生している可能性があります。ユーザまたはユーザのグループの MTU を減らすことで、問題を解決できることがあります。

AnyConnect が確立する SSL VPN 接続の最大転送ユニット サイズ（256 ～ 1406 バイト）を調整するには、次の手順に従ってください。

ステップ 1　ASDM インターフェイスで、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] の順に選択します。

[Edit Internal Group Policy] ダイアログボックスが表示されます。

ステップ 2　[Advanced] > [SSL VPN Client] の順に選択します。

ステップ 3　[Inherit] チェックボックスをオフにして、MTU フィールドで適切な値を指定します。

デフォルトのグループ ポリシーでは、このコマンドのデフォルトのサイズが 1406 です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

この設定が影響を与えるのは、SSL で確立された AnyConnect 接続と、SSL with DTLS で確立された AnyConnect 接続です。

圧縮の排除による VPN パフォーマンスの向上と Windows Mobile 接続の許可

低帯域幅の接続では、圧縮によって転送されるパケットのサイズが削減され、ASA とクライアントとの間の通信パフォーマンスが向上します。デフォルトでは、ASA では、グローバル レベルと特定のグループまたはユーザの両方において、すべての SSL VPN 接続に対する圧縮がイネーブルになっています。ブロードバンド接続では、圧縮によってパフォーマンスが低下することがあります。

（注）　Windows Mobile 用の Cisco AnyConnect Secure Mobility Client は、圧縮をサポートしていません。

グローバルに圧縮を設定するには、グローバル コンフィギュレーション モードから CLI コマンド **compression svc** コマンドを使用します。

DART を使用したトラブルシューティング情報の収集

DART は Diagnostic AnyConnect Reporting Tool の略で、AnyConnect のインストールと接続に関する問題のトラブルシューティングに役立つデータの収集に使用できます。DART は、Windows 7、Windows Vista、および Windows XP をサポートしています。

DART ウィザードは、AnyConnect が稼動するコンピュータ上で実行されます。DART によってログ、状態情報、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。DART の実行に管理者権限は不要です。

DART は、AnyConnect ソフトウェアのコンポーネントに依存せずに機能しますが、AnyConnect から起動可能で、AnyConnect ログ ファイル（ある場合）の収集を行います。

どのバージョンの DART も、すべてのバージョンの AnyConnect に使用できます。それぞれのバージョン番号は同期していません。DART を最適化するには、使用する AnyConnect バージョンにかかわらず、Cisco AnyConnect Client ソフトウェア ダウンロード サイトにある最新バージョンをダウンロードしてください。

現在のところ、DART は単独でインストールできますが、AnyConnect ダイナミック ダウンロード インフラストラクチャの一部として、このアプリケーションを管理者がクライアント PC にプッシュすることもできます。インストールされると、[Start] ボタンにある Cisco フォルダから、DART ウィザードを起動できます。

（注）　シスコがお客様に DART を提供しているのは、重要なトラブルシューティング情報を簡単に収集できるようにするためですが、DART はリリース サイクルの「ベータ」フェーズであることに注意してください。

DART ソフトウェアの入手

DART は、AnyConnect ダウンロードおよびインストレーションパッケージに含まれ、単体の .msi ファイルとしても入手できます。

どのバージョンの DART も、すべてのバージョンの AnyConnect に使用できます。それぞれのバージョン番号は同期していません。DART を最適化するには、使用する AnyConnect バージョンにかかわらず、Cisco AnyConnect Client ソフトウェア ダウンロード サイトにある最新バージョンをダウンロードしてください。

Cisco.com にある、DART ファイルを含む AnyConnect ダウンロード ファイルは次のとおりです。

- **anyconnect-all-packages-*Version*-k9.zip**：すべての AnyConnect パッケージが含まれています。
- **anyconnect-dart-win-*Version*-k9.pkg**：DART インストール パッケージ*だけ*が含まれ、AnyConnect または vpngina ソフトウェアは含まれていません。DART を単体のアプリケーションとしてインストールする場合は、これを使用してください。

DART のインストール

管理者は、DART を AnyConnect インストレーションの一部として含めることができます。または、Cisco.com の登録ユーザが DART ソフトウェアの入手の説明に従って、http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect からファイルをダウンロードし、PC に手動でインストールすることもできます。

AnyConnect を AnyConnect で動作する PC にダウンロードしたときに、新しいバージョンの DART がある場合は、その DART とともにダウンロードされます。自動アップグレードの一部として、新しいバージョンの AnyConnect がダウンロードされたときに、新しいバージョンの DART があれば、その DART が含まれます。

（注）　グループ ポリシー設定（**svc modules** コマンドまたは対応する ASDM ダイアログで設定）に **dart** キーワードがない場合は、DART がパッケージに含まれていても、AnyConnect は DART をインストールしません。

AnyConnect を使用した DART のインストール

この手順では、次回リモート ユーザが接続するときに、そのユーザのマシンに DART がダウンロードされます。

ステップ 1　他のシスコのソフトウェア パッケージと同様に、DART を含む AnyConnect パッケージを ASA にロードします。

ステップ 2　DART を含む AnyConnect の .pkg ファイルをセキュリティ アプライアンスにインストール後、AnyConnect と一緒に DART をインストールするには、グループ ポリシーで DART を指定する必要があります。これは、次のように ASDM または CLI を使用して実行します。

- ASDM を使用する場合は、[Configuration] をクリックしてから、[Remote Access VPN] > [Network (Client) Access] > [Group Policy] の順にクリックします。

  新しいグループ ポリシーを追加するか、既存のグループ ポリシーを編集します。グループ ポリシーのダイアログボックスで、[Advanced] を展開し、[SSL VPN Client] をクリックします。

  [SSL VPN Client] ダイアログボックスで、[Optional Client Modules to Download] オプションの [Inherit] をオフにします。このオプションのドロップダウン リストから **dart** モジュールを選択します。

  使用するバージョンの ASDM に、DART オプションのチェックボックスがない場合は、フィールドにキーワード **dart** を入力します。DART と Start Before Logon の両方をイネーブルにするには、**dart** と **vpngina** の両方を任意の順序でカンマで区切ってフィールドに入力します。

  [OK] をクリックしてから、[Apply] をクリックします。
- CLI を使用する場合は、**svc modules value dart** コマンドを使用します。

（注） あとで **svc modules none** に変更したり、[Optional Client Modules to Download] フィールドの DART の選択を解除しても、DART はインストールされたままになります。セキュリティ アプライアンスからは DART をアンインストールできません。DART を削除するには、Windows のコントロール パネルの、[Add/Remove Programs] を使用してください。この方法で DART を削除しても、ユーザが AnyConnect を使用して再接続すると、自動的に再インストールされます。上位バージョンの DART を含んだ AnyConnect パッケージが ASA にアップロードされ、設定されている場合は、ユーザが接続すると DART が自動的にアップグレードされます。

DART の実行方法については、「Windows PC での DART の実行」（P.8-8）を参照してください。

ホストへの DART の手動インストール

ステップ 1　Cisco.com から DART ソフトウェアを入手します。「DART ソフトウェアの入手」（P.8-6）を参照して、**anyconnect-dart-win-2.4.*version*-k9.pkg** をローカルにインストールします。

ステップ 2　WinZip® などのファイル圧縮ユーティリティを使用して、**anyconnect-dart-win-2.4.*version*-k9.pkg** の内容を、ディレクトリ構造を維持した状態で展開します。

ステップ 3　**anyconnect-dart-win-2.4.*version*-k9.pkg** ファイルの内容を展開して作成された **binaries** ディレクトリを開きます。

ステップ 4　**anyconnect-dart-win-2.4.*version*-k9**.msi ファイルをダブルクリックして、[DART Setup Wizard] を起動します。

ステップ 5　初期画面で [Next] をクリックします。

ステップ 6　[I accept the terms in the License Agreement] を選択して、エンド ユーザのライセンス契約に同意し、[Next] をクリックします。

ステップ 7　[Install] をクリックして、DART をインストールします。インストール ウィザードによって、**DartOffline.exe** が <System Drive>:¥Program Files¥Cisco¥Cisco DART ディレクトリにインストールされます。

ステップ 8　[Finish] をクリックして、インストールを完了します。

DART の実行方法については、「Windows PC での DART の実行」（P.8-8）を参照してください。

Windows PC での DART の実行

Windows PC で DART ウィザードを実行して DART バンドルを作成するには、次の手順に従ってください。

ステップ 1　AnyConnect GUI を起動します。

ステップ 2　[Statistics] タブをクリックしてから、ダイアログボックス下部の [Details] ボタンをクリックします。[Statistics Details] ダイアログボックスが表示されます。

ステップ 3　[Statistics Details] ウィンドウ下部の [Troubleshoot] をクリックします。

ステップ 4　初期画面で [Next] をクリックします。[Bundle Creation Option] ダイアログボックスが表示されます。

ステップ 5　[Bundle Creation Option] エリアで、[Default] または [Custom] を選択します。

- [Default] オプションでは、代表的なログ ファイルと診断情報が含まれます。たとえば、AnyConnect ログ ファイルや Cisco Secure Desktop ログ ファイル、コンピュータの一般情報、DART が実行した内容と実行しなかった内容についての要約などが含まれます。

  [Default] を選択してから、ダイアログボックス下部の [Next] をクリックすると、DART のバンドル作成が開始されます。バンドルのデフォルト名は DARTBundle.zip で、ローカル デスクトップに保存されます。

- [Custom] を選択した場合は、[Next] をクリックすると、DART ウィザードによってさらにダイアログボックスが表示され、バンドルに含めるファイルや、バンドルの保存場所を指定します。

ヒント　[Custom] を選択すると、バンドルに含めるファイルはデフォルトのままにして、ファイルの保存場所だけは別の場所を指定するということもできます。

ステップ 6　DART バンドルを暗号化するには、[Encryption Option] エリアで [Enable Bundle Encryption] にチェックを入れてから、[Encryption Password] フィールドにパスワードを入力します。オプションで [Mask Password] を選択すると、[Encryption Password] フィールドおよび [Reenter Password] フィールドに入力したパスワードが、アスタリスク（*）でマスクされるようになります。

ステップ 7　[Next] をクリックします。[Default] を選択した場合、DART はバンドルの作成を開始します。[Custom] を選択した場合は、ウィザードが次のステップに進みます。

ステップ 8　[Log File Selection] ダイアログボックスで、バンドルに含めるログ ファイルと設定ファイルを選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 9　[Diagnostic Information Selection] ダイアログボックスで、バンドルに含める診断情報を選択します。DART が通常状態で収集するファイルのリストをデフォルトに戻すには、[Restore Default] をクリックします。[Next] をクリックします。

ステップ 10　[Comments and Target Bundle Location] ダイアログボックスで、次のフィールドを設定します。

- [Comments] エリアに、バンドルに含めるコメントを入力します。入力したコメントは、DART のバンドルに含められる comments.txt ファイルに保存されます。
- [Target Bundle Location] フィールドで、バンドルの保存場所を参照します。

[Next] をクリックします。

ステップ 11　[Summary] ダイアログボックスでカスタマイズの内容を確認し、[Next] をクリックしてバンドルを作成するか、[Back] をクリックしてカスタマイズの内容に変更を加えます。

ステップ 12　DART のバンドル作成が終了したら、[Finish] をクリックします。

ヒント　状況によっては、DART の実行に数分以上かかったという報告を受けることがあります。デフォルト リストのファイル収集に長い時間を要している思われる場合は、[Cancel] をクリックしてからウィザードを再実行し、**カスタム** DART バンドルを作成して必要なファイルだけを選択してください。

ログ ファイルのインストール

ログ ファイルは、次のファイル内に保持されます。

- ¥Windows¥setupapi.log：Windows XP および Windows 2000
- ¥Windows¥Inf¥setupapi.app.log：Windows Vista
- ¥Windows¥Inf¥setupapi.dev.log：Windows Vista

（注）　Vista では、隠しファイルを表示する必要があります。

レジストリ情報が setupapi.log ファイルから欠落している場合は、Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにしてください。Windows XP ベースのコンピュータ上で冗長ロギングをイネーブルにするには、次の手順に従ってください。

（注）　レジストリを誤って変更すると、重大な問題が発生する可能性があります。念のため、レジストリを変更する前に、レジストリをバックアップしてください。

ステップ 1　[Start] > [Run] をクリックします。

ステップ 2　[Open] フィールドに **regedit** と入力し、[OK] をクリックします。

ステップ 3　HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Setup レジストリ サブキーにある **LogLevel** を見つけてダブルクリックします。

ステップ 4　[Edit DWORD Value] ウィンドウの [Base] ペインにある [Hexadecimal] を選択します。

ステップ 5　[Value] データ ボックスに **0x2000FFFF** と入力します。

ステップ 6　[OK] をクリックします。

（注）　冗長ロギングをイネーブルにすると、Setupapi.log ファイルのサイズは約 4MB に増加します。レジストリ値をリセットするには、上記のステップを繰り返しますが、ステップ 5 で DWORD 値を 0 に設定してください。

ログ ファイルの Web インストール

これが新規の Web 展開インストールの場合、このログは次のユーザ別の temp ディレクトリに格納されます。

%TEMP%¥anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log

アップグレードが最適なゲートウェイからプッシュされた場合、ログ ファイルは次の場所に格納されます。

%WINDIR%¥TEMP¥anyconnect-win-2.X.xxxx-k9-install-yyyyyyyyyyyyyy.log

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。*xxx* はバージョンによって異なり、**yyyyyyyyyyyyyy** はインストールの日時を示します。

ログ ファイルの単独インストール

MSI ロギングをオンにし、インストールのログをキャプチャするには、次のファイルを実行します。

MSIExec.exe/i anyconnect-win-2.X.xxxx-pre-deploy-k9.msi/lvx* c:¥AnyConnect.log

ここで、*anyconnect-win-2.X.xxxx-pre-deplay-k9.msi* は、インストールする実際の msi ファイルの完全な名前です。

ログは次の場所に表示されます。

- ¥Documents and Settings¥<username>¥Local Settings¥Temp（Windows XP および Windows 2000）
- ¥Users¥<username>¥AppData¥Local¥Temp（Windows Vista）
- ¥Windows¥Temp（自動アップグレードの場合）

単独で使用する（または ActiveX コントロールをシステムにインストールしない）場合は、次のいずれかの手順を実行します。

（注） 上記のいずれの操作も行わない場合、Cisco AnyConnect VPN エラー 1722 が表示されることがあります。このエラーは Windows Installer パッケージで問題が発生したことを示しています。

- MSI トランスフォームを作成し、ActiveX プロパティを次のようにディセーブルに設定する（NOINSTALLACTIVEX=1）。

```
MISExec /i anyconnect-win-x.x.xxxx-pre-deploy-k9.msi NOINSTALLACTIVEX=1
```

- リブートせずに、次のコマンドを実行して Quiet Install を実行する。

```
msiexec /quiet /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi
```

- リブートせずに、次のコマンドを実行して Quiet Uninstall を実行する。

```
msiexec /quiet /x "anyconnect-gina-x.x.xxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

（注） *x.x.xxx* の値は、インストールされているバージョンによって異なります。

AnyConnect の接続解除または初期接続の確立に関する問題

AnyConnect クライアントの接続解除または初期接続の確立で問題が発生する場合は、以下の推奨事項に従ってください。

1. 次の手順で ASA から設定ファイルを入手して、接続失敗の形跡がないか調べます。
   - ASA コンソールから **write net x.x.x.x:ASA-Config.txt** と入力します。この *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。
   - ASA コンソールから、**show running-config** と入力します。設定を切り取ってテキスト エディタに貼り付け、これを保存します。
2. ASA イベント ログを表示します。
   a. ASA コンソールで、次の行を追加して、ssl、webvpn、svc、および auth の各イベントを調べます。

```
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
```

   b. AnyConnect クライアントの接続を試行し、接続エラーが発生した場合は、そのコンソールのログ情報を切り取ってテキスト エディタに貼り付け、保存します。
   c. **no logging enable** と入力して、ロギングをディセーブルにします。
3. クライアント PC の Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。
   a. [Start] > [Run] の順に選択し、**eventvwr.msc /s** と入力します。
   b. アプリケーションおよびサービス ログ（Windows Vista および Windows 7 の）で、**Cisco AnyConnect VPN Client** を見つけ、[Save Log File As..] を選択します。
   c. AnyConnectClientLog.evt などのファイル名を割り当てます。.evt ファイル形式を使用してください。
4. AnyConnect GUI を接続解除または終了する際に問題が発生する場合は、vpnagent.exe プロセスを Windows 診断デバッグ ユーティリティにアタッチしてください。詳細については、WinDbg のマニュアルを参照してください。
5. IPv6/IPv4 IP アドレスの割り当てに競合が確認された場合は、スニファ トレースを取得し、使用中のクライアント PC のレジストリにルーティング デバッグを追加します。このような競合は、AnyConnect イベント ログで次のように表示されます。

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .¥VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .¥RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

   VPN 接続を確立する前に特定のレジストリ エントリ（Windows）またはファイル（Mac または Linux）を追加すると、ルート デバッグを 1 つの接続に対して 1 回だけイネーブルできます。

トンネル接続が開始され、このキーまたはファイルが検出されると、2 つのルート デバッグ テキスト ファイルがシステムの一時ディレクトリ（通常 Windows では C:¥Windows¥Temp、Mac または Linux では /tmp）に作成されます。2 つのファイル（debug_routechangesv4.txt4 と debug_routechangesv6.txt）がすでに存在する場合、これらのファイルは上書きされます。

トラフィックの通過に関する問題

いったん接続されたプライベート ネットワークに AnyConnect クライアントがデータを送信できない場合は、次の推奨事項に従ってください。

1. show vpn-sessiondb detail svc filter name <username> コマンドの出力を取得します。出力にフィルタ名 XXXXX が指定されている場合は、show access-list XXXXX コマンドの出力も取得してください。ACL によってトラフィック フローがブロックされていないか確認してください。
2. [AnyConnect VPN Client] > [Statistics] > [Details] > [Export] の順に選択し、DART のファイルまたは出力（AnyConnect-ExportedStats.txt）を取得します。統計情報、インターフェイス、およびルーティング テーブルを調べます。
3. ASA コンフィギュレーション ファイルの NAT 文を確認します。NAT が有効になっている場合は、クライアントに返されるデータをネットワーク アドレス変換から除外する必要があります。たとえば、AnyConnect プールから IP アドレスを NAT 除外するには、次のコードが使用されます。

```
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 ゲートウェイがその設定に対して有効になっているかどうかを確認してください。従来型のデフォルト ゲートウェイは、次のように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。

```
route outside 0.0.83.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

   VPN クライアントが VPN ゲートウェイのルーティング テーブルにないリソースにアクセスする必要がある場合は、パケットは標準的なデフォルト ゲートウェイでルーティングされます。VPN ゲートウェイは、内部ルーティング テーブル全体を持つ必要はありません。トンネリングされたキーワードを使用すると、ルートは IPsec/SSL VPN 接続から受信した復号化されたトラフィックを処理します。VPN ルートから受信したトラフィックは 10.0.4.2 にルーティングされて復号化されますが、標準トラフィックは最終的に 83.145.50.1 にルーティングされます。
5. AnyConnect とのトンネルを確立する前と後に、ipconfig /all および route print の出力のテキストダンプを収集します。
6. クライアントでネットワーク パケットキャプチャを実行するか、ASA のキャプチャをイネーブルにします。

（注） アプリケーション（Microsoft Outlook など）がトンネルで動作しない場合は、ping のスケーリング設定を使用して、ネットワークの既知のデバイスに ping を送信し、受信可能なサイズを確認してください（たとえば、ping -| 500、ping -| 1000、ping -| 1500、および ping -| 2000）。ping の結果から、ネットワークにフラグメンテーションの問題が発生しているかがわかります。このとき、フラグメンテーションが発生する可能性のあるユーザに専用のグループを設定し、このグループに対して svc mtu を 1200 に設定できます。また、古い IPsec クライアントから Set MTU.exe ユーティリティをコピーして、物理アダプタの MTU を強制的に 1300 に設定できます。リブート時に、違いがあるかどうか確認してください。

AnyConnect のクラッシュに関する問題

UI のクラッシュが発生した場合、結果は %temp% ディレクトリ（C:¥DOCUME~1¥jsmith¥LOCALS~1¥Temp など）に書き込まれます。リブート後に "The System has recovered from a serious error" メッセージが表示される場合は、C:¥Documents and Settings¥All Users¥Application Data¥Microsoft¥Dr Watson または同様のアプリケーションから生成された .log および .dmp ファイルを収集してください。これらのファイルをコピーするか、以下の手順に従ってファイルをバックアップしてください。

ステップ 1　[Start] > [Run] メニューから ワトソン博士（Drwtsn32.exe）という Microsoft ユーティリティを実行します。

ステップ 2　次のように設定し、[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
```

ステップ 3　クライアント PC で [Start] > [Run] メニューの順に選択し、**eventvwr.msc /s** と入力して、Windows イベント ビューアから Cisco AnyConnect VPN クライアント ログを取得します。

ステップ 4　（Windows Vista および Windows 7 の）[Applications and Services Logs] で **Cisco AnyConnect VPN Client** を見つけ、[Save Log File As..] を選択します。AnyConnectClientLog.evt などのファイル名を .evt ファイル形式で割り当ててください。

ステップ 5　ドライバ クラッシュが VPNVA.sys で発生する場合は、Cisco AnyConnect 仮想アダプタにバインドされているすべての中間ドライバを確認し、これらをオフにします。

ステップ 6　ドライバ クラッシュが vpnagent.exe で発生する場合は、vpnagent.exe プロセスを Windows のデバッグ ツールにアタッチします。ツールがインストールされたら、次の手順を実行します。

a. c:¥vpnagent というディレクトリを作成します。

b. タスク マネージャの [Process] タブを見て、vpnagent.exe のプロセス PID を判別します。

c. コマンド プロンプトを開き、デバッグ ツールをインストールしたディレクトリに変更します。デフォルトでは、Windows のデバッグ ツールは C:¥Program Files¥Debugging Tools にあります。

d. **cscript vpnagent4.vbs -crash -p PID -o c:¥vpnagent -nodumponfirst** と入力します。この *PID* は、ステップ b で判別した番号です。

開いているウインドウを最小化した状態で実行します。モニタリング中は、システムをログオフできません。

e. クラッシュが発生したときに、c:¥vpnagent の内容を zip ファイルに収集します。

f. **!analyze -v** を使用して、crashdmp ファイルを詳細に診断します。

VPN サービスへの接続に関する問題

"Unable to Proceed, Cannot Connect to the VPN Service" メッセージが表示される場合、AnyConnect の VPN サービスは実行されていません。VPN エージェントが予期せず終了した可能性があります。別のアプリケーションがサービスと競合したかどうかにかかわらず、トラブルシューティングするには、次の手順を実行します。

ステップ 1　Windows 管理ツールでサービスを確認して、Cisco AnyConnect VPN エージェントが動作していないか確認します。このエージェントが動作している場合、またはエラー メッセージが引き続き表示される場合は、ワークステーション上の別の VPN アプリケーションをディセーブルにする必要があります。また、このアプリケーションのアンインストール、リブート、または再テストが必要になる場合があります。

ステップ 2　Cisco AnyConnect VPN エージェントを起動してみます。こうすることで、起動時にサーバの初期化または別の実行中のサービス（サービスの起動に失敗したため）と競合しているかどうかを判断します。

ステップ 3　イベント ビューアの AnyConnect ログに、サービスを起動できなかったこと示すメッセージがないか確認します。ステップ 2 の手動による再起動のタイム スタンプと、ワークステーションが起動した時刻に注意してください。

ステップ 4　イベント ビューアのシステムとアプリケーション ログに、競合を示すメッセージで同じタイム スタンプがないかを確認します。

ステップ 5　ログにサービスの起動失敗が示されている場合は、次のいずれかを示す同じタイムスタンプの前後に他の情報メッセージがないか探します。

- ファイルの欠落：MSI を単独でインストールして AnyConnect クライアントを再インストールし、欠落しているファイルをなくします。
- 別の依存するサービスでの遅延：起動アクティビティをディセーブルにして、ワークステーションのブート時間を短縮します。
- 別のアプリケーションまたはサービスとの競合：別のサービスが、vpnagent が使用するポートと同じポート上で受信していないか、または一部の HIDS ソフトウェアによって、シスコのソフトウェアがポート上で受信できなくなっているかどうかを判別します。

ログに原因が直接示されていない場合は、試行錯誤的な方法で競合を識別してください。最も可能性が高い原因が確認されたら、[Services] パネルから該当するサービス（VPN 製品、HIDS ソフトウェア、spybot クリーナ、スニファ、アンチウイルス ソフトウェアなどの）をディセーブルにします。リブート後も VPN エージェント サービスが起動しない場合は、オペレーティング システムのデフォルト インストールでインストールされなかったサービスをオフにしてください。

PC のシステム情報の取得

PC のシステム情報を取得するには、次のコマンドを入力し、約 2 分間待ってください。

- **winmsd /nfo c:¥msinfo.nfo** ：Windows XP または Windows 2000
- **msinfo32 /nfo c:¥msinfo.nfo**：Windows Vista

Systeminfo ファイル ダンプの取得

Windows XP または Vista で、systeminfo ファイル ダンプを取得するには、コマンド プロンプトで次のコマンドを入力します。

systeminfo >> c:¥sysinfo.txt

レジストリ ファイルの確認

次の SetupAPI ログ ファイル内のエントリは、ファイルが見つからないことを示しています。

```
E122 Device install failed. Error 2: The system cannot find the file specified.
```

```
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥RunOnce レジストリ キーが存在することを確認してください。このレジストリ キーが存在しない場合、すべての inf インストール パッケージが禁止されます。

サードパーティ製アプリケーションとの競合

一部のサードパーティ製アプリケーションでは、AnyConnect 仮想アダプタ ドライバのインストールが禁止されます。この場合、画面がブルー スクリーンになり、ルーティング テーブルを更新できなくなることがあります。DART ツール（「DART を使用したトラブルシューティング情報の収集」（P.8-5）で説明）を使用すると、お客様のオペレーティング システム環境の方法を収集できます。この診断に基づいて、シスコは次のサードパーティ製アプリケーションとの競合を識別し、解決策を推奨することができます。

Adobe および Apple：Bonjour Print Service

- Adobe Creative Suite 3
- BonJour Print Service
- iTunes

症状　IP 転送テーブルを正常に検証できない。

考えられる原因　AnyConnect イベント ログは、IP 転送テーブルの識別に失敗したことを示し、ルーティング テーブル内の次のエントリを示しています。

```
Destination 169.254.0.0
Netmask 255.255.0.0
Gateway 10.64.128.162
Interface 10.64.128.162
Metric 29
```

推奨処置　コマンド プロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service をディセーブルにしてください。mDNSResponder の新しいバージョン（1.0.5.11）が Apple から提供されています。この問題を解決するために、Bonjour の新しいバージョンが iTunes にバンドルされ、個別のダウンロードとして Apple の Web サイトで配布されています。

AT&T Communications Manager バージョン 6.2 および 6.7

症状　一部の PC に AT&T Sierra Wireless 875 カードを装着すると、接続に失敗したり、トラフィックが通過できなくなったりする。バージョン 6.2 ～ 6.7 が AnyConnect と競合していると思われる。

考えられる原因　CSTP 転送障害は、AnyConnect 仮想アダプタによってトランスポート層が損なわれていることを示します。

推奨処置　この問題を解決するには、次の手順を実行します。

1. Aircard のアクセラレーションをディセーブルにします。

2. [AT&T Communication Manager] > [Tools] > [Settings] > [Acceleration] > [Startup] の順に選択して、AT&T Communication Manager を起動します。
3. **manual** と入力します。
4. [Stop] をクリックします。

AT&T Global Dialer

症状　クライアントのオペレーティング システムでブルー スクリーンが発生し、ミニ ダンプ ファイルが生成されることがある。

考えられる原因　AT&T Dialer の中間ドライバが保留パケットを適切に処理できず、これがオペレーティング システムのクラッシュの原因となっています。他の NIC カード ドライバ（Broadcom など）では、この問題は発生していません。

推奨処置　AT&T Global Network Client を最新の 7.6.2 にアップグレードしてください。

Citrix Advanced Gateway Client バージョン 2.2.1

症状　AnyConnect セッションを接続解除するときに、次のようなエラーが発生する。

```
VPN Agent Service has encountered a problem and needs to close. We are sorry for
the inconvenience.
```

考えられる原因　メモリを解放するときに、Winsock を使用して Citrix CtxLsp.dll がすべてのプロセスにロードされるため、クラッシュが発生します。

推奨処置　CtxLsp.dll に関するこの問題が解決されるまで、Citrix Advanced Gateway Client を削除してください。

ファイアウォールとの競合

サードパーティ製ファイアウォールによって、ASA グループ ポリシーで設定されたファイアウォール機能が妨げられることがあります。

Juniper Odyssey Client

症状　ワイヤレス サプレッションが有効のときに有線接続を導入すると、無線接続がドロップする。ワイヤレス サプレッションがディセーブルのとき、ワイヤレス機能は期待どおりに動作する。

考えられる原因　Odyssey Client がネットワーク アダプタを管理していません。

推奨処置　Odyssey Client を次の手順で設定してください。

1. [Network Connections] で、アダプタの名前を接続プロパティの表示どおりにコピーします。レジストリを編集する場合、誤って変更すると重大な問題が発生する可能性があるため、バックアップを実行してから、細心の注意を払って変更してください。

2. レジストリを開き、HKEY_LOCAL_MACHINE¥SOFTWARE¥Funk Software, Inc.¥odyssey¥client¥configuration¥options¥adapterType¥virtual に移動します。
3. virtual の下に新しい文字列値を作成します。アダプタの名前をネットワーク プロパティからレジストリ部分にコピーします。追加のレジストリ設定を保存すると、MSI が作成されて他のクライアントにプッシュされたときに、この設定が移植されます。

Kaspersky AV Workstation 6.x

症状　Kaspersky 6.0.3 がインストールされると（ディセーブルであっても）、CSTP state = CONNECTED の直後に ASA への AnyConnect 接続が失敗する。次のメッセージが表示される。

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure
gateway (proxy authentication, handshake, bad cert, etc.).
```

考えられる原因　Kaspersky AV Workstation 6.x と AnyConnect の間に既知の非互換性が存在します。

推奨処置　Kaspersky をアンインストールし、Kaspersky のフォーラムを参照して追加のアップデートがないか確認してください。

McAfee Firewall 5

症状　UDP DTLS 接続を確立できない。

考えられる原因　McAfee Firewall は、着信 IP フラグメントをデフォルトでブロックするように設定されているため、DTLS が分割されている場合は、DTLS をブロックします。

推奨処置　McAfee Firewall のセンター コンソールで、[Advanced Tasks] > [Advanced options and Logging] を選択し、McAfee Firewall の [Block incoming fragments automatically] チェックボックスをオフにします。

Microsoft Internet Explorer 8

症状　Windows XP SP3 で Internet Explorer 8 を使用すると、WebVPN ポータルから AnyConnect をインストールできない。

考えられる原因　インストール中にブラウザがクラッシュする。

推奨処置　Microsoft の推奨策に従って、MSJVM を削除してください。Microsoft Knowledge Base の記事 KB826878 を参照してください。

Microsoft Routing and Remote Access Server

症状　AnyConnect がホスト デバイスへの接続を確立しようとすると、イベント ログに次の終了エラーが返される。

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service "Routing and Remote Access" is incompatible with the Cisco
AnyConnect VPN Client.
```

考えられる原因　ルーティング テーブル上で RRAS と AnyConnect が競合しています。RRAS では、PC はイーサネット ルータとして機能するので、AnyConnect と同様にルーティング テーブルが変更されます。AnyConnect はトラフィックを適切に転送するためにルーティング テーブルに依存するので、この 2 つを一緒に実行できません。

推奨処置　RRAS サービスをディセーブルにします。

Microsoft Windows の更新プログラム

症状　VPN 接続の確立を試行すると、次のメッセージが表示される。

```
The VPN client driver has encountered an error.
```

考えられる原因　最近、certclass.inf ファイルに Microsoft 更新プログラムが適用されました。次のエラーが C:¥WINDOWS¥setupapi.log に表示されます。

```
#W239 The driver signing class list "C:¥WINDOWS¥INF¥certclass.inf" was missing or
invalid. Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject
to driver signing policy.
```

推奨処置　コマンド プロンプトで **C:¥>systeminfo** と入力するか、C:¥WINDOWS¥WindowsUpdate.log を確認して、最近インストールされた更新プログラムを確認してください。修復を試行するには、次の手順を実行します。

1. コマンド プロンプトを管理者として開きます。
2. **net stop CryptSvc** と入力します。
3. **esentutl /g %systemroot%¥System32¥catroot2¥{F750E6C3-38EE-11D1-85E5-00C04FC295EE}¥catdb** と入力してデータベースを分析し、そのデータベースの妥当性を検証するか、%/WINDIR%¥system32¥catroot2 ディレクトリの名前を catroot2_old に変更します。
4. プロンプトが表示されたら、[OK] を選択して修復を試行します。コマンド プロンプトを終了し、リブートしてください。

上記の手順を実行すると、カタログが破損していないことが示される場合がありますが、キー ファイルが無署名のもので上書きされた可能性があります。障害が解消されない場合は、ドライバ署名のデータベースの破損原因を特定するために Microsoft に依頼してケースをオープンしてください。

Windows XP（Service Pack 3）

症状　AnyConnect クライアントをインストールできない。次のエラー メッセージが表示されます。

```
This application has failed to start because dot3api.dll was not found.
Re-installing the application may fix this problem.
```

考えられる原因　dot3api.dll ファイルの欠落は既知の問題です。

推奨処置　regsvr32 dot3api.dll を再インストールし、オペレーティング システムをリブートします。

OpenVPN クライアント

症状　このバージョンの TUN がこのシステムにすでにインストールされていて、AnyConnect クライアントと互換性がないことを示すエラーが表示される。

考えられる原因　このようなエラーは、Mac OS X Shimo VPN クライアントが原因で発生することがあります。

推奨処置　Viscosity OpenVPN Client をアンインストールします。

ロード バランサ

症状　クレデンシャルがないために、接続が失敗する。

考えられる原因　ブラウザが DNS 結果をキャッシュしていても、ポート フォーワダやスマート トンネルなどの追加アプリケーションが DNS 結果をキャッシュしないことがあります。ユーザが X.4 にログインした後、DNS リゾルバが x.15 を使用するように設定されている場合、PF アプレットまたはスマート トンネル アプリケーションは DNS を解決して X.15 に接続します。セッションが確立されていないので、クレデンシャルがないことが原因で接続が失敗します。

推奨処置　サードパーティ製ロード バランサでは、ASA デバイスにかかる負荷を把握できません。ASA のロード バランシング機能は非常にインテリジェントで、VPN の負荷をデバイス全体で均等に分散できるため、ASA 内蔵のロード バランシングを使用することをお勧めします。

Ubuntu 8.04 i386

症状　Ubuntu バージョン 8.04 を使用すると、AnyConnect クライアントが ASA への接続確立に失敗する。VPN クライアント エージェント SSL エンジンでエラーが発生したことがエラー メッセージに示される。

考えられる原因　バージョン 7.04 と 8.04 とで、NSS ライブラリ エクステンションが変更されているため、AnyConnect クライアントは Network Security Service ライブラリを検出できません。

推奨処置　次のスクリプトを使用して NSS ライブラリのリンクを修正してください。

```
#!/bin/sh
if [ `id | sed -e `s/(.*//' ` != "uid=0" ]; then
    echo "Sorry, you need super user privileges to run this script.
    exit 1
fi
echo Creating Firefox NSS compatible symlinks...
ln -s /usr/lib/libnspr4.so.0d /usr/lib/libnspr4.so || exit 1
ln -s /usr/lib/libnss3.so.1d /usr/lib/libnss3.so || exit 1
ln -s /usr/lib/libplc4.so.0d /usr/lib/libplc4.so || exit 1
ln -s /usr/lib/libsmime3/so/1d /usr/lib/libsmime3.so || exit 1
echo "Success!"
```

また Ubuntu フォーラムで、AnyConnect で Ubuntu 64 ビットを使用可能にするための解説がないか確認することもできます。

Wave EMBASSY Trust Suite

症状　AnyConnect クライアントがダウンロードに失敗し、次のエラー メッセージが表示される。

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to
close."
```

考えられる原因　mdmp ファイルを収集している場合は、クラッシュ mdmp ファイルをデコードすると、サードパーティ製 dll が存在することが示されます。

推奨処置　dll の問題をすべて解決するために、パッチ アップデートをバージョン 1.2.1.38 に更新してください。

Layered Service Provider（LSP）モジュールおよび NOD32 AV

症状　AnyConnect が接続を確立しようと試みると、SSL セッションが正常に認証されて確立されるが、AnyConnect クライアントが vpndownloader でクラッシュする。

考えられる原因　LSP コンポーネントの imon.dll に非互換性問題があります。

推奨処置　ESET NOD32 AV のバージョン 2.7 で Internet Monitor コンポーネントを削除し、バージョン 3.0 にアップグレードしてください。

LSP の症状 2：競合

症状　クライアント上に LSP モジュールが存在する場合、Winsock カタログが競合することがあります。

考えられる原因　impbw.dll などの Intel モバイル帯域幅の LSP モジュールによって、Intel コードで障害が発生した可能性があります。

推奨処置　LSP モジュールをアンインストールしてください。

LSP のデータ スループット低下症状 3：競合

症状　NOD32 V4.0 を使用すると、データ スループットが低下することがあります。

考えられる原因　この競合は、Windows 7 で Cisco AnyConnect と NOD32 アンチウイルス 4.0.468 x64 を使用したときに発生します。

推奨処置　[Protocol Filtering] > [Advanced Setup] の [SSL] を選択し、SSL プロトコル スキャンをイネーブルにします。次に、[Web access protection] > [HTTP, HTTPS] の順に選択し、[Do not use HTTPS protocol checking] をオンにします。設定がイネーブルになったら、[Protocol filtering] > [SSL] に戻り、[SSL protocol scanning] スキャンをディセーブルにします。

EVDO ワイヤレ スカードおよび Venturi ドライバ

症状　クライアントが接続解除され、イベント ログに次のようなメッセージが生成される。

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing
connection: DPD failure.
```

考えられる原因　アプリケーション、システム、および AnyConnect の各イベント ログに関係する接続解除イベントがないか確認すると同時に、NIC カードのリセットが適用されたかどうか判別してください。

推奨処置　Venturi ドライバが最新のものであるか確認してください。AT&T Communications Manager バージョン 6.7 の [Use Rules Engine] をディセーブルにします。

DSL ルータがネゴシエーションに失敗する

症状　DTLS トラフィックが正常にネゴシエーションされたが、DTLS トラフィックに障害が発生した。

考えられる原因　DSL ルータがリターン DTLS トラフィックをブロックしていました。エアー リンク上の設定により、安定した DTLS 接続が許可されません。

推奨処置　工場出荷時の設定で Linksys ルータに接続すると、安定した DTLS セッションが許可され、ping が中断されません。DTLS リターン トラフィックを許可するルールを追加してください。

チェックポイント（および Kaspersky などの他のサードパーティ製ソフトウェア）

症状　AnyConnect ログに、セキュア ゲートウェイへの接続を完全に確立できなかったことが示される。

考えられる原因　クライアント ログに、NETINTERFACE_ERROR_INTERFACE_NOT_AVAILABLE が複数発生したことが示されています。これらのエラーは、セキュア ゲートウェイへの SSL 接続の確立に使用する PC のネットワーク インターフェイス上でクライアントがオペレーティング システム情報を取得しようとしているときに発生します。

推奨処置　整合性エージェントをアンインストールしてから AnyConnect をインストールする場合は、TCP/IP をイネーブルにしてください。整合性エージェントのインストール時に SmartDefense をディセーブルにすると、TCP/IP がチェックされます。サードパーティ製のソフトウェアがネットワーク インターフェイス情報の取得中に、オペレーティン グシステムの API コールを代行受信またはブロックしている場合は、疑わしい AV、FW、AS などがないか確認してください。デバイス マネージャに AnyConnect アダプタのインスタンスが 1 つだけ表示されていることを確認してください。インスタンスが 1 つだけの場合は、AnyConnect で認証し、5 秒後にデバイス マネージャからアダプタを手動でイネーブルにしてください。疑わしいドライバが AnyConnect アダプタ内でイネーブルにされている場合は、これらのドライバを [Cisco AnyConnect VPN Client Connection] ウィンドウでオフにしてディセーブルにしてください。

Virtual Machine Network Service ドライバでのパフォーマンス問題

症状　一部のクライアント PC で AnyConnect を使用すると、パフォーマンスの問題が発生した。

考えられる原因　仮想マシン ネットワーク ドライバは物理的なネットワーク カードまたは接続を仮想化します。Cisco AnyConnect VPN クライアント接続ネットワーク アダプタに他の仮想マシン ネットワーク サービスをバインドしたときに、パフォーマンス問題が発生しています。クライアント デバイスが何らかのマルウェアに感染し、SSL_write () の周囲で遅延が発生しました。

推奨処置　AnyConnect 仮想アダプタ内のすべての IM デバイスに対するバインドをオフにしてください。アプリケーション dsagent.exe は、C:¥Windows¥System¥dgagent にあります。これはプロセス リストに表示されませんが、TCPview（sysinternals）でソケットを開くと表示できます。このプロセスを終了すると、AnyConnect が正常に動作します。