



ユーザ ガイドラインのやりとり

VPN ユーザと次のガイドラインをやりとりするようにしてください。また、ユーザからガイドラインを求められたときに、この項を参考にしてください。内容は、次のとおりです。

- 「[Mac OS X 10.5 での TUN/TAP エラー メッセージへの応答](#)」(P.B-1)
- 「[未対応 64 ビット版 Internet Explorer](#)」(P.B-2)
- 「[Wireless Hosted Network の回避](#)」(P.B-2)
- 「[暗号化せずにすべての DNS クエリーを送信する Mac OS X 10.6](#)」(P.B-2)
- 「[Start Before Logon と DART インストール](#)」(P.B-3)
- 「[検疫状態への応答](#)」(P.B-3)
- 「[AnyConnect CLI コマンドを使用した接続 \(スタンドアロン モード\)](#)」(P.B-3)
- 「[セキュア接続 \(Lock\) アイコンの設定](#)」(P.B-5)

Mac OS X 10.5 での TUN/TAP エラー メッセージへの応答

Mac OS X 10.5 以前のバージョンへ AnyConnect をインストールしている場合、次のエラー メッセージが表示される場合があります。

A version of the TUN virtual network driver is already installed on this system that is incompatible with the AnyConnect client. This is a known issue with OS X version 10.5 and prior, and has been resolved in 10.6. Please uninstall any VPN client, speak with your System Administrator, or reference the AnyConnect Release Notes for assistance in resolving this issue.

Mac OS X 10.6 ではこの問題は解決されています。AnyConnect で必要なバージョンの TUN/TAP 仮想ネットワーク ドライバが提供されているためです。

10.6 以前のバージョンの Mac OS X には TUN/TAP 仮想ネットワーク ドライバは組み込まれていないため、AnyConnect はこれらのオペレーティング システムでは独自のドライバをインストールします。ただし、データ カードを管理する Parallels など一部のソフトウェアや一部の VPN アプリケーションは独自の TUN/TAP ドライバをインストールします。AnyConnect インストール ソフトウェアでは、ドライバがすでに存在するという理由で上記のエラー メッセージが表示されますが、そのドライバのバージョンは AnyConnect とは互換性がありません。

AnyConnect をインストールするには、TUN/TAP 仮想ネットワーク ドライバを削除する必要があります。



(注)

TUN/TAP 仮想ネットワーク ドライバを削除すると、システムで最初にドライバをインストールしたソフトウェアに問題が発生するおそれがあります。

TUN/TAP 仮想ネットワーク ドライバを削除するには、コンソール アプリケーションを開き、次のコマンドを入力します。

```
sudo rm -rf /Library/Extensions/tap.kext
```

```
sudo rm -rf /Library/Extensions/tun.kext
```

```
sudo rm -rf /Library/StartupItems/tap
```

```
sudo rm -rf /Library/StartupItems/tun
```

```
sudo rm -rf /System/Library/Extensions/tun.kext
```

```
sudo rm -rf /System/Library/Extensions/tap.kext
```

```
sudo rm -rf /System/Library/StartupItems/tap
```

```
sudo rm -rf /System/Library/StartupItems/tun
```

これらのコマンドを入力したら、Mac OS を再起動し、AnyConnect を再インストールします。

未対応 64 ビット版 Internet Explorer

WebLaunch からの AnyConnect のインストールでは 64 ビット版の Internet Explorer はサポートされていません。Windows on x64 (64 ビット版) を使用している場合、32 ビット版の Internet Explorer または Firefox を使用して WebLaunch をインストールしてください。現時点では、Firefox は 32 ビット版でのみ使用できます。

Wireless Hosted Network の回避

Windows 7 [Wireless Hosted Network](#) 機能を使用すると AnyConnect が不安定になるおそれがあります。AnyConnect を使用する場合、この機能をイネーブルにしたり、(Connectify または Virtual Router など) この機能をイネーブルにするフロントエンド アプリケーションを実行したりすることはお勧めしません。

暗号化せずにすべての DNS クエリーを送信する Mac OS X 10.6

スプリット DNS がイネーブルになっている場合、Mac OS X 10.6 はすべての DNS クエリーを暗号化せずに送信します。スプリット DNS ドメインに向けた DNS クエリーは VPN セッション経由で送信されなければなりません。次のアップデートでこの問題を解決する予定です。

Start Before Logon と DART インストール

Start Before Logon コンポーネントでは、最初に AnyConnect をインストールしておく必要があります。

SBL または DART が接続しているエンドポイントから手動でアンインストールされている場合、これらのコンポーネントは再インストールされます。ヘッドエンド設定でこれらのコンポーネントをインストールし、(エンドポイントに設定されている) プリファレンスでアップグレードを許可するよう指定されている場合のみ、この動作が発生します。

検疫状態への応答

アクセスに関して企業のポリシーに準拠しないエンドポイントのネットワーク ステータスは、[AnyConnect Connection] タブで [Quarantined] と表示されます。

通常、検疫されたセッションに適用されるダイナミック アクセス ポリシーに割り当てられた ACL では、アンチウイルスおよびアンチスパイウェアのアップデートなど修復サービスへのアクセスのみ許可されます。

検疫状態のセッションでは、エンドポイントの修復に十分な時間が必要です。この時間に続き、ユーザは [Reconnect] をクリックし、その状態を終了し新しいポスチャ アセスメントを開始する必要があります。

AnyConnect CLI コマンドを使用した接続（スタンドアロンモード）

Cisco AnyConnect VPN Client には、グラフィカル ユーザ インターフェイスを使用せずにコマンドを発行することを希望するユーザ向けに、CLI があります。次の項では、CLI コマンドプロンプトの起動方法について説明します。

Windows の場合

Windows システムで CLI コマンドプロンプトを起動し、コマンドを発行するには、Windows のフォルダ C:\Program Files\Cisco\Cisco AnyConnect VPN Client にあるファイル `vpncli.exe` を探します。ファイル `vpncli.exe` をダブルクリックします。

Linux および Mac OS X の場合

Linux システムまたは Mac OS X システムで CLI コマンドプロンプトを起動し、コマンドを発行するには、フォルダ `/opt/cisco/vpn/bin/` にあるファイル `vpn` を探します。ファイル `vpn` を実行します。

インタラクティブ モードで CLI を実行する場合、独自のプロンプトが表示されます。コマンドラインを使用することもできます。表 B-1 に、CLI コマンドを示します。

表 B-1 AnyConnect クライアント CLI コマンド

コマンド	アクション
<code>connect IP アドレスまたはエイリアス</code>	特定の ASA への接続を確立します。
<code>disconnect</code>	前に確立した接続を閉じます。
<code>stats</code>	確立した接続に関する統計情報を表示します。

表 B-1 AnyConnect クライアント CLI コマンド (続き)

コマンド	アクション
quit	CLI インタラクティブ モードを終了します。
exit	CLI インタラクティブ モードを終了します。

次の例は、ユーザがコマンドラインから接続を確立し、終了する例です。

Windows

connect 209.165.200.224

アドレスが 209.165.200.224 のセキュリティ アプライアンスへの接続を確立します。要求されたホストに接続した後、AnyConnect クライアントは、ユーザが属するグループを表示し、ユーザのユーザ名とパスワードを要求します。オプションのバナーを表示するよう指定されている場合、ユーザはバナーに応答する必要があります。デフォルトの応答は **n** で、接続試行を終了します。次に例を示します。

```
VPN> connect 209.165.200.224
  >>contacting host (209.165.200.224) for login information...
  >>Please enter your username and password.
Group: testgroup
Username: testuser
Password: *****
  >>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour. The system will not be available during that time.

accept? [y/n] y
  >> notice: Authentication succeeded. Checking for updates...
  >> state: Connecting
  >> notice: Establishing connection to 209.165.200.224.
  >> State: Connected
  >> notice: VPN session established.
VPN>
```

stats

現在の接続の統計情報を表示します。次の例を参考にしてください。

```
VPN> stats
[ Tunnel Information ]

    Time Connected:01:17:33
    Client Address:192.168.23.45
    Server Address:209.165.200.224

[ Tunnel Details ]

    Tunneling Mode:All Traffic
    Protocol: DTLS
    Protocol Cipher: RSA_AES_256_SHA1
    Protocol Compression: None

[ Data Transfer ]

    Bytes (sent/received): 1950410/23861719
    Packets (sent/received): 18346/28851
    Bypassed (outbound/inbound): 0/0
    Discarded (outbound/inbound): 0/0

[ Secure Routes ]
```

```
Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

disconnect

前に確立した接続を閉じます。次の例を参考にしてください。

```
VPN> disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit または **exit**

どちらかのコマンドで、CLI のインタラクティブ モードを終了します。次の例を参考にしてください。

```
quit
goodbye
>>state: Disconnected
```

Linux または Mac OS X

```
/opt/cisco/vpn/bin/vpn connect 1.2.3.4
```

アドレスが *1.2.3.4* の ASA への接続を確立します。

```
/opt/cisco/vpn/bin/vpn connect some_asa_alias
```

プロファイルを読み込み、エイリアス *some_asa_alias* を検索してアドレスを探し、ASA への接続を確立します。

```
/opt/cisco/vpn/bin/vpn stats
```

VPN 接続に関する統計情報を表示します。

```
/opt/cisco/vpn/bin/vpn disconnect
```

VPN セッションがある場合、接続解除します。

セキュア接続 (Lock) アイコンの設定

Lock アイコンは、セキュアな接続を示しています。Windows XP では、このアイコンは最近使用されていない他のアイコンと同様に自動的に非表示になります。Windows XP でこのアイコンが非表示にされないようにするには、次の手順に従ってください。

-
- ステップ 1** トレイ アイコンが表示されたタスクバーの、かぎカッコ (<) を右クリックします。
 - ステップ 2** [Customize Notifications...] を選択します。
 - ステップ 3** [Cisco Systems AnyConnect VPN Client] を選択し、[Always Show] に設定します。
-

[Internet Explorer Connections] タブを非表示にする AnyConnect

ある条件では、[Internet Explorer Tools]、[Internet Options] にある [Connections] タブが非表示になります。このタブが表示されている場合、ユーザはプロキシ情報を設定できます。このタブを非表示にすると、ユーザが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックは接続解除すると反転され、このタブに関する管理者定義のポリシーの方が優先されます。このロックは、次のいずれかの条件で行われます。

- ASA の設定で、プライベート側プロキシが指定されている。
- AnyConnect が、Internet Explorer で定義されたパブリック側プロキシを使用してトンネルを確立する。この場合は、ASA のスプリット トンネリング ポリシーが [Tunnel All Networks] に設定されている必要があります。