CHAPTER 79

AnyConnect VPN Client 接続の設定

この章では、AnyConnect VPN Client 接続を設定する方法について説明します。次の項目を取り上げます。

AnyConnect VPN Client 接続に関する情報

Cisco AnyConnect Secure Mobility Client によりリモート ユーザは、ASA へのセキュアな SSL 接続または IPsec/IKEv2 接続を確立できます。事前にクライアントがインストールされていない場合、リモート ユーザは、SSL または IPsec/IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。ASA が、http:// 要求を **https**:// にリダイレクトするように設定されていない限り、ユーザは URL を https://<*address*> の形式で入力する必要があります。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインと認証に成功し、そのユーザがクライアントを要求していると ASA で識別されると、セキュリティ アプライアンスは、リモート コンピュータのオペレーティング システムに合うクライアントをダウンロードします。ダウンロード後、クライアントは自分自身でインストールと設定を行い、セキュアな SSL または IPsec/IKEv2 接続を確立します。接続の終了時には、（設定に応じて）そのまま残るか、または自分自身をアンインストールします。

以前にインストールされているクライアントの場合は、ユーザの認証時に、ASA がクライアントのリビジョンを検査して、必要に応じてクライアントをアップグレードします。

クライアントが ASA と SSL VPN 接続をネゴシエートした場合は、Transport Layer Security（TLS）を使用して接続します。状況に応じて、Datagram Transport Layer Security（DTLS）が使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

AnyConnect クライアントは、ASA からダウンロードできます。または、システム管理者が手動でリモート PC にインストールできます。クライアントを手動でインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

ASA は、ユーザが確立している接続のグループ ポリシーまたはユーザ名属性に基づきクライアントをダウンロードします。自動的にクライアントをダウンロードするように ASA を設定するか、またはクライアントをダウンロードするかをリモート ユーザに確認するように設定できます。後者の場合、ユーザが応答しなかった場合は、タイムアウト時間が経過した後にクライアントをダウンロードするか、ログイン ページを表示するように ASA を設定できます。

AnyConnect 接続のライセンス要件

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1,2]
ASA 5505	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンスまたは Security Plus ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* – *共有ライセンスはサポートされていません。[3]* • AnyConnect Essentials ライセンス[4]：25 セッション。
ASA 5510	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンスと Security Plus ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：250 セッション。
ASA 5520	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：750 セッション。

モデル	ライセンス要件[1,2]
ASA 5540	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：2500 セッション。
ASA 5550	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：5000 セッション。
ASA 5580	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：10000 セッション。
ASA 5512-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：250 セッション。
ASA 5515-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：250 セッション。

モデル	ライセンス要件[1,2]
ASA 5525-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：750 セッション。
ASA 5545-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：2500 セッション。
ASA 5555-X	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：5000 セッション。
ASA 5585-X（SSP-10）	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：5000 セッション。

モデル	ライセンス要件[1,2]
ASA 5585-X（SSP-20、-40、および -60）	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：10000 セッション。
ASASM	次のいずれかを使用します。 • AnyConnect Premium ライセンス： – 基本ライセンス：2 セッション。 – *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* – *オプションの共有ライセンス[3]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* • AnyConnect Essentials ライセンス[4]：10000 セッション。

1. クライアントレス SSL VPN セッションを開始した後、ポータルから AnyConnect クライアント セッションを開始した場合は、合計 1 つのセッションが使用されています。これに対して、最初に AnyConnect クライアントを（スタンドアロン クライアントなどから）開始した後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されています。
2. すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を越えることはできません。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
3. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。
4. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、このライセンスをディセーブルにして他のライセンスを使用するには **no anyconnect-essentials** コマンドを使用します。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

リモート PC のシステム要件

AnyConnect Secure Mobility Client を実行するエンドポイント コンピュータの要件については、ASA で展開する AnyConnect クライアント バージョンのリリース ノートを参照してください。

リモート HTTPS 証明書の制限事項

ASA では、リモート HTTPS 証明書は確認されません。

AnyConnect 接続の設定

この項では、AnyConnect VPN クライアント接続を受け入れるように ASA を設定するための前提条件、制限事項、および詳細なタスクについて説明します。次の項目を取り上げます。

クライアントを Web 展開するための ASA の設定

この項では、AnyConnect クライアントを Web 展開するように ASA を設定する手順について説明します。

前提条件

TFTP や別の方法を使用して、クライアント イメージ パッケージを ASA にコピーします。

手順の詳細

	コマンド	目的
ステップ 1	**anyconnect image** *filename order* **Example:** hostname(config-webvpn)#**anyconnect image anyconnect-win-2.3.0254-k9.pkg 1** hostname(config-webvpn)#**anyconnect image anyconnect-macosx-i386-2.3.0254-k9.pkg 2** hostname(config-webvpn)#**anyconnect image anyconnect-linux-2.3.0254-k9.pkg 3**	フラッシュのファイルを AnyConnect クライアント パッケージ ファイルとして指定します。 ASA は、リモート PC にダウンロードするために、キャッシュ メモリのファイルを展開します。複数のクライアントがある場合は、order 引数を使用して、クライアント イメージに順序を割り当てます。 ASA は、リモート PC のオペレーティング システムと一致するまで、指定されている順序で各クライアントの一部をダウンロードします。そのため、最も一般的に使用されているオペレーティング システム用のイメージには、最も低い数値を割り当てます。 **（注）** **anyconnect image xyz** コマンドで AnyConnect イメージを設定した後に **anyconnect enable** コマンドを発行する必要があります。**anyconnect enable** コマンドをイネーブルにしない場合、AnyConnect の動作は不完全になり、**show webvpn anyconnect** コマンドは SSL VPN クライアントがイネーブルにされていないと見なし、インストールされた AnyConnect パッケージをリストしません。
ステップ 2	**enable** *interface* **Example:** hostname(config)# **webvpn** hostname(config-webvpn)# **enable outside**	クライアントレス接続または AnyConnect SSL 接続のインターフェイスの SSL をイネーブルにします。
ステップ 3	**anyconnect enable**	このコマンドを発行しないと、AnyConnect は想定したとおりに機能せず、**show webvpn anyconnect** コマンドは、インストールされた AnyConnect パッケージをリストする代わりに、「SSL VPN is not enabled」というメッセージを返します。
ステップ 4	**ip local pool** *poolname startaddr-endaddr* **mask** *mask* **Example:** hostname(config)# **ip local pool vpn_users 209.165.200.225-209.165.200.254 mask 255.255.255.224**	（任意）アドレス プールを作成します。DHCP やユーザによる割り当てのアドレスの指定など、別のアドレス割り当ての方法を使用することもできます。
ステップ 5	**address-pool** *poolname* **Example:** hostname(config)# **tunnel-group telecommuters general-attributes** hostname(config-tunnel-general)# **address-pool vpn_users**	アドレス プールをトンネル グループに割り当てます。
ステップ 6	**default-group-policy** *name* **Example:** hostname(config-tunnel-general)# **default-group-policy sales**	デフォルトのグループ ポリシーをトンネル グループに割り当てます。

	コマンド	目的
ステップ 7	**group-alias** *name* **enable** **Example:** hostname(config)# **tunnel-group telecommuters webvpn-attributes** hostname(config-tunnel-webvpn)# **group-alias sales_department enable**	クライアントレス ポータルおよび AnyConnect GUI のログイン ページでのトンネルグループ リストの表示をイネーブルにします。エイリアスのリストは、*group-alias name enable* コマンドによって定義されます。
ステップ 8	**tunnel-group-list enable** **Example:** hostname(config)# **webvpn** hostname(config-webvpn)# **tunnel-group-list enable**	グループまたはユーザの許可された VPN トンネリング プロトコルとして AnyConnect クライアントを指定します。
ステップ 9	**vpn-tunnel-protocol** **Example:** hostname(config)# **group-policy sales attributes** hostname(config-group-policy)# **webvpn** hostname(config-group-webvpn)# **vpn-tunnel-protocol**	グループまたはユーザの許可された VPN トンネリング プロトコルとして SSL を指定します。その他のプロトコルを追加して指定することもできます。詳細については、『*Cisco ASA 5500 Series Command Reference*』の **vpn-tunnel-protocol** コマンドを参照してください。 グループ ポリシーに対するユーザの割り当ての詳細については、第 6 章「接続プロファイル、グループ ポリシー、およびユーザの設定」を参照してください。

永続的なクライアント インストールのイネーブル化

永続的なクライアント インストールをイネーブルにすると、クライアントの自動アンインストール機能がディセーブルになります。クライアントは、後続の接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザの接続時間が短縮されます。

特定のグループまたはユーザに対する永続的なクライアント インストールをイネーブルにするには、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **anyconnect keep-installer** コマンドを使用します。

anyconnect keep-installer installer

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。次の例では、セッションの終了時点でリモート コンピュータのクライアントを削除するように既存のグループ ポリシー *sales* を設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

DTLS の設定

Datagram Transport Layer Security（DTLS）を使用すると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つのトンネル（SSL トンネルと DTLS トンネル）を同時に使用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

デフォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセスをイネーブルにした場合です。DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

（注）　DTLS を TLS 接続にフォール バックさせるには、Dead Peer Detection（DPD; デッドピア検知）をイネーブルにする必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS にフォール バックする代わりに接続は終了します。DPD のイネーブル化の詳細については、「Dead Peer Detection のイネーブル化と調整」（P.79-18）を参照してください。

webvpn コンフィギュレーション モードで、**enable** コマンドの **tls-only** オプションを使用すると、すべての AnyConnect クライアント ユーザに対して DTLS をディセーブルにできます。

enable <*interface*> **tls-only**

たとえば、次のように入力します。

hostname(config-webvpn)# **enable outside tls-only**

デフォルトでは、特定のグループまたはユーザに対して DTLS をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl dtls** コマンドを使用します。

[**no**] **anyconnect ssl dtls enable**

DTLS をディセーブルにする必要がある場合は、このコマンドの **no** 形式を使用します。たとえば、次のように入力します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl dtls enable
```

リモート ユーザに対するプロンプト

ASA で、リモート SSL VPN クライアント ユーザがクライアントをダウンロードするためのプロンプトをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

anyconnect enable を指定すると、クライアントをダウンロードするか、クライアントレス ポータル ページに移動するかをリモート ユーザに尋ねるプロンプトを表示し、ユーザの応答を無期限に待機します。

anyconnect ask enable default を指定すると、クライアントをすぐにダウンロードします。

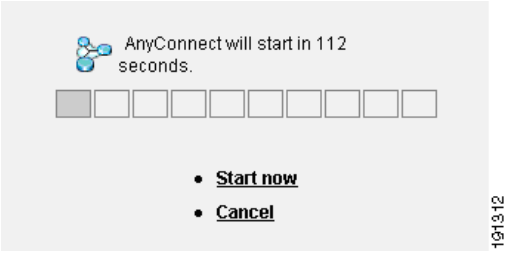
anyconnect ask enable default webvpn を指定すると、ポータル ページにすぐに移動します。

anyconnect ask enable default timeout *value* を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトをリモート ユーザに表示し、デフォルト アクション（クライアントのダウンロード）を実行する前に、*value* の間待機します。

anyconnect ask enable default clientless timeout *value* を指定すると、クライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトをリモート ユーザに表示し、デフォルト アクション（クライアントレス ポータル ページの表示）を実行する前に、*value* の間待機します。

図 79-1 に、**default anyconnect timeout** *value* または *default webvpn timeout* value が設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 79-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



次の例では、ASA でクライアントをダウンロードするか、またはクライアントレス ポータル ページに移動するかを尋ねるプロンプトを表示して、クライアントをダウンロードする前に*応答を 10 秒*待機するように設定しています。

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout 10
```

AnyConnect クライアント プロファイル ダウンロードのイネーブル化

AnyConnect プロファイルで Cisco AnyConnect Secure Mobility Client 機能をイネーブルにします（コア クライアントのコンフィギュレーション設定と VPN 機能、およびオプションのクライアント モジュールのコンフィギュレーション設定を含む XML ファイル、ネットワーク アクセス マネージャ（NAM）、ポスチャ、テレメトリ、Web セキュリティ）。ASA は AnyConnect のインストールおよびアップデート中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

ASDM のプロファイル エディタ

プロファイルは、AnyConnect プロファイル エディタを使用して設定できます。このエディタは、ASDM から起動できる便利な GUI ベースの設定ツールです。Windows 用 AnyConnect ソフトウェア パッケージ バージョン 2.5 以降には、エディタが含まれています。このエディタは、AnyConnect パッケージを ASA にロードし、AnyConnect クライアント イメージとして指定するとアクティブ化されます。

スタンドアロン プロファイル エディタ

ASDM に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロン バージョンも使用できます。クライアントを事前展開する場合は、ソフトウェア管理システムを使用してコンピュータに展開する、VPN サービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイル エディタを使用して作成できます。プロファイル エディタの使用の詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

（注） AnyConnect クライアント プロトコルのデフォルトは SSL です。IPsec IKEv2 をイネーブルにするには、ASA で IKEv2 設定を設定し、また、クライアント プロファイルのプライマリ プロトコルとして IKEv2 を設定する必要があります。IKEv2enabled プロファイルは、エンドポイント コンピュータに展開する必要があります。それ以外の場合、クライアントは SSL を使用して接続を試行します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

次の手順に従いプロファイルを編集し、ASA でプロファイルのリモート クライアントへのダウンロードをイネーブルにします。

ステップ 1　ASDM のプロファイル エディタまたはスタンドアロン プロファイル エディタを使用して、プロファイルを作成します。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

ステップ 2　tftp または別の方式を使用して、ASA のフラッシュ メモリにプロファイル ファイルをロードします。

ステップ 3　webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、キャッシュ メモリにロードするクライアント プロファイルとしてこのファイルを識別します。

次に、プロファイルとしてファイル *sales_hosts.xml* と engineering_hosts.xml を指定する例を示します。

```
asa1(config-webvpn)# anyconnect profiles sales disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering disk0:/engineering_hosts.xml
```

これで、プロファイルをグループ ポリシーに利用できます。

キャッシュ メモリにロードされたプロファイルを表示するには、**dir cache:stc/profiles** コマンドを使用します。

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/
```

```
0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

ステップ 4　グループ ポリシー webvpn コンフィギュレーション モードを開始し、**anyconnect profiles** コマンドを使用して、グループ ポリシーのクライアント プロファイルを指定します。

使用可能なプロファイルを表示するには、**anyconnect profiles value** コマンドに続けて、疑問符（**?**）を入力します。たとえば、次のように入力します。

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

次の例では、クライアント プロファイル タイプが *vpn* のプロファイル *sales* を使用するようにグループ ポリシーを設定します。

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

AnyConnect クライアントの遅延アップグレードのイネーブル化

AnyConnect ユーザは、遅延アップグレードを使用して、クライアント アップグレードのダウンロードを遅らせることができます。クライアント アップデートが使用できる場合、AnyConnect は、更新するか、またはアップグレードを延期するかを尋ねるダイアログを開きます。

遅延アップグレードをイネーブルにするには、カスタム属性を ASA に追加して、グループ ポリシーでこれらの属性を参照および設定します。

次のカスタム属性は遅延アップグレードをサポートします。

表 79-1　遅延アップグレードのカスタム属性

カスタム属性	有効値	デフォルト値	コメント
DeferredUpdateAllowed	true false	false	true は遅延アップデートをイネーブルにします。遅延アップデートがディセーブル（false）の場合、次の設定は無視されます。
DeferredUpdateMinimumVersion	x.y.z	0.0.0	アップデートを延期できるようにインストールする必要がある AnyConnect の最小バージョン。 最小バージョン チェックは、ヘッドエンドでイネーブルになっているすべてのモジュールに適用されます。イネーブルになっているモジュール（VPN を含む）がインストールされていないか、最小バージョンを満たしていない場合、接続は遅延更新の対象になりません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、遅延プロンプトが表示されます（または自動消去されます）。

表 79-1　遅延アップグレードのカスタム属性 （続き）

カスタム属性	有効値	デフォルト値	コメント
DeferredUpdateDismissTimeout	0 ～ 300（秒）	なし（ディセーブル）	遅延アップグレード プロンプトが表示され、自動的に消去されるまでの秒数。この属性は、遅延更新プロンプトが表示される場合に限り適用されます（最小バージョン属性が最初に評価されます）。 この属性がない場合、自動消去機能がディセーブルになり、ユーザが応答するまでダイアログが表示されます（必要な場合）。 この属性をゼロに設定すると、自動遅延またはアップグレードを次に基づいて強制できます。 • インストールされているバージョンおよび DeferredUpdateMinimumVersion の値。 • DeferredUpdateDismissResponse の値。
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout が発生した場合に実行するアクション。

ステップ 1　webvpn コンフィギュレーション モードで **anyconnnect-custom-attr** コマンドを使用してカスタム属性を作成します。

[no] anyconnect-custom-attr *attr-name* **[description** *description***]**

次に、カスタム属性 DeferredUpdateAllowed を追加する例を示します。

```
hostname(config)# webvpn
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
"Indicates if the deferred update feature is enabled or not"
```

ステップ 2　カスタム属性をグループ ポリシーに追加するか、グループ ポリシーから削除し、**anyconnect-custom** コマンドを使用して、各属性の値を設定します。

anyconnect-custom *attr-name* **value** *value*

no anyconnect-custom *attr-nam*

次に、sales という名前のグループ ポリシーに対して遅延更新をイネーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed value true
```

追加の AnyConnect クライアント機能のイネーブル化

ダウンロード時間を最小限に抑えるために、クライアントは必要なコア モジュールのダウンロード（ASA から）だけを要求します。追加機能が AnyConnect クライアントで使用可能になったら、それらの機能を使用できるようにするためにリモート クライアントをアップデートする必要があります。

新しい機能をイネーブルにするには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect modules** コマンドを使用して、新しいモジュール名を指定する必要があります。

[no] anyconnect modules {**none** | **value** *string*}

複数のストリングを指定する場合は、カンマで区切ります。

各クライアント機能に対して入力する値のリストについては、Cisco AnyConnect VPN Client のリリース ノートを参照してください。

Start Before Logon のイネーブル化

Start Before Logon（SBL）を使用すると、Windows PC にインストールされている AnyConnect クライアントに対するログイン スクリプト、パスワード キャッシング、ドライブ マッピングなどが使用できるようになります。SBL では、AnyConnect クライアントの Graphical Identification and Authentication（GINA）をイネーブルにするモジュールをダウンロードするようにASA をイネーブルにする必要があります。次の手順は、SBL をイネーブルにする方法を示しています。

ステップ 1　グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect modules** *vpngina* コマンドを使用して、ASA で特定のグループまたはユーザに VPN 接続に対する GINA モジュールをダウンロードできるようにします。

次の例では、ユーザはグループ ポリシー *telecommuters* でグループ ポリシー属性モードを開始し、そのグループ ポリシーで webvpn コンフィギュレーション モードを開始し、ストリング *vpngina* を指定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

ステップ 2　クライアント プロファイル ファイル（AnyConnectProfile.tmpl）のコピーを取得します。

ステップ 3　プロファイル ファイルを編集して SBL がイネーブルであることを指定します。次の例では、Windows 用のプロファイル ファイル（AnyConnectProfile.tmpl）の関係部分を示しています。

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
    </ClientInitialization>
```

<UseStartBeforeLogon> タグによって、クライアントが SBL を使用するかどうかが決まります。SBL をオンにするには、*false* を *true* で置き換えます。次の例は、SBL がオンになっているタグを示しています。

```
    <ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

ステップ 4　AnyConnectProfile.tmpl に対する変更を保存し、webvpn コンフィギュレーション モードで **profile** コマンドを使用して、ASA のグループまたはユーザに対するプロファイル ファイルをアップデートします。たとえば、次のように入力します。

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

AnyConnect ユーザ メッセージの言語の変換

ASA には、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および Cisco AnyConnect VPN Client ユーザに表示されるインターフェイスの言語変換機能があります。

この項では、これらのユーザ メッセージを変換するために ASA を設定する方法について説明します。次の項目を取り上げます。

- 「言語変換の概要」（P.79-15）
- 「変換テーブルの作成」（P.79-15）

言語変換の概要

リモート ユーザに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめられています。*Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるすべてのメッセージは、AnyConnect ドメイン内にあります。*

ASA のソフトウェア イメージ パッケージには、AnyConnect ドメインの変換テーブル テンプレートが含まれています。このテンプレートはエクスポートでき、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージ フィールドは空です。メッセージを編集して、テンプレートをインポートし、フラッシュ メモリに置かれる新しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、変換テーブル オブジェクトの新しいバージョンが作成され、以前のメッセージが上書きされます。AnyConnect ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント ユーザに表示されます。

変換テーブルの作成

次の手順では、AnyConnect ドメインの変換テーブルを作成する方法について説明します。

ステップ 1　特権 EXEC モードで **export webvpn translation-table** コマンドを使用して、コンピュータに変換テーブル テンプレートをエクスポートします。

次の例では、**show webvpn translation-table** コマンドによって、使用可能な変換テーブル テンプレートとテーブルを表示しています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

次に、AnyConnect 変換ドメイン用の変換テーブルをエクスポートします。作成された XML ファイルのファイル名は *client* という名前が付けられ、空のメッセージ フィールドが含まれています。

```
hostname# export webvpn translation-table AnyConnect template
tftp://209.165.200.225/client
```

次の例では、*zh* という名前の変換テーブルをエクスポートします。このテーブルは、テンプレートから事前にインポートされたものです。zh は中国語用 Microsoft Internet Explorer で使用される省略形です。

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/chinese_client
```

ステップ 2　変換テーブルの XML ファイルを編集します。次の例は、AnyConnect テンプレートの一部を示しています。この出力の最後には、*Connected* メッセージのメッセージ ID フィールド（msgid）とメッセージ文字列フィールド（msgstr）が含まれています。このメッセージは、クライアントが VPN 接続を確立するときに AnyConnect クライアント GUI に表示されます。完全なテンプレートには、多くのメッセージ フィールドのペアが含まれています。

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid には、デフォルト変換が含まれています。msgid に続く msgstr が変換を提供します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、メッセージ「Connected」をスペイン語で変換するには、引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

ファイルは必ず保存してください。

ステップ 3　特権 EXEC モードで **import webvpn translation-table** コマンドを使用して、変換テーブルをインポートします。ブラウザと互換性がある言語の省略形を付けて新しい変換テーブルの名前を指定します。

次の例では、米国スペイン語用の Microsoft Internet Explorer で使用される省略形である *es-us* で XML ファイルがインポートされます。

```
hostname# import webvpn translation-table AnyConnect language es-us
tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder
csd
customization
keepout
url-list
webvpn
Citrix-plugin
```

```
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

高度な AnyConnect SSL 機能の設定

次の項では、AnyConnect SSL VPN 接続を調整する高度な機能について説明します。次の項目を取り上げます。

キーの再生成のイネーブル化

ASA と AnyConnect クライアントが SSL VPN 接続でキー再生成を行うときは、暗号キーと初期化ベクトルを再ネゴシエーションして、接続のセキュリティを高めます。

特定のグループまたはユーザの SSL VPN 接続で、クライアントによるキー再生成の実行をイネーブルにするには、グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **anyconnect ssl rekey** コマンドを使用します。

[no]anyconnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

method new-tunnel は、キーの再生成中にクライアントが新規トンネルを確立するように指定します。

method ssl は、キー再生成中にクライアントが新規トンネルを確立するように指定します。

method none は、キー再生成をディセーブルにします。

（注） キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。**anyconnect ssl rekey** コマンドの履歴については、『Cisco ASA 5500 Series Command Reference, 8.4』を参照してください。

time *minutes* は、セッションの開始からまたは前回のキー再生成から、キーの再生成が行われるまでの時間を 1 から 10080（1 週間）の分数で指定します。

次の例では、セッション開始の 30 分後に実施されるキー再生成中に、既存のグループ ポリシー *sales* に対する SSL との再ネゴシエーションを実施するようにクライアントを設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

Dead Peer Detection のイネーブル化と調整

Dead Peer Detection（DPD）により、ピアの応答がなく接続が失敗している場合には、ASA（ゲートウェイ）またはクライアント側で瞬時に検出できます。

ASA またはクライアントで特定のグループまたはユーザについて DPD をイネーブルにし、ASA またはクライアントが DPD を実行する頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで **anyconnect dpd-interval** コマンドを使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

それぞれの説明は次のとおりです。

gateway seconds は、ASA（ゲートウェイ）で実行する DPD をイネーブルにして、ASA（ゲートウェイ）での DPD の実行頻度（5 ～ 3600 秒）を指定します。

gateway none は、ASA による DPD をディセーブルにします。

client *seconds* は、クライアントによる DPD をイネーブルにし、クライアントが DPD を実行する頻度（5 ～ 3600 秒）を指定します。

client none は、クライアントによって実行される DPD をディセーブルにします。

anyconnect dpd-interval コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

no anyconnect dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

（注） DTLS をイネーブルにすると、Dead Peer Detection（DPD）もイネーブルになります。DPD により、失敗した DTLS 接続の TLS へのフォールバックがイネーブルになります。それ以外の場合、接続は終了します。

次の例では、ASA による DPD の実行頻度が 30 秒に設定され、クライアントによる既存のグループ ポリシー *sales* に対する DPD の実行頻度が 10 秒に設定されています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

キープアライブのイネーブル化

キープアライブ メッセージの頻度を調整することで、接続がアイドルでいられる時間がデバイスによって制限されている場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SSL VPN 接続をオープンのまま維持します。また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

（注） キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、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。

キープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで、次のように **keepalive** コマンドを使用します。

[no] anyconnect keepalive {none | *seconds***}**

none は、クライアントのキープアライブ メッセージをディセーブルにします。

seconds は、クライアントによるキープアライブ メッセージの送信をイネーブルにし、メッセージの頻度を 15 ～ 600 秒の範囲で指定します。

デフォルトでは、キープアライブ メッセージはイネーブルになっています。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

次の例では、既存のグループ ポリシー *sales* に対して、クライアントがキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるように ASA を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect keepalive 300
```

圧縮の使用

圧縮により、低帯域幅の接続に転送されるパケットのサイズが減少し、ASA とクライアント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。

（注）　ブロードバンド接続の圧縮を実装する場合は、圧縮が損失が少ない接続に依存していることを慎重に考慮する必要があります。これが、ブロードバンド接続ではデフォルトで圧縮がイネーブルになっていない主な理由です。

圧縮は、グローバル コンフィギュレーション モードで **anyconnect ssl compression** コマンドを使用してグローバルにオンにする必要があります。そうすることで、グループ ポリシーおよびユーザ名 webvpn モードで **anyconnect ssl compression** コマンドを使用して、特定のグループまたはユーザに圧縮を設定することができます。

圧縮のグローバルな変更

グローバルな圧縮の設定を変更するには、グローバル コンフィギュレーション モードで **anyconnect ssl compression** コマンドを使用します。

圧縮

no compression

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

次の例では、すべての SSL VPN 接続の圧縮は、グローバルにディセーブルになっています。

```
hostname(config)# no compression
```

グループおよびユーザに対する圧縮の変更

特定のグループまたはユーザに対する圧縮を変更するには、グループ ポリシーおよびユーザ名 webvpn モードで **anyconnect ssl compression** コマンドを使用します。

anyconnect ssl compression {**deflate** | **none**}

no anyconnect ssl compression {**deflate** | **none**}

デフォルトでは、グループおよびユーザに対する SSL 圧縮は *deflate*（イネーブル）に設定されています。

コンフィギュレーションから **anyconnect ssl compression** コマンドを削除し、グローバル設定から値が継承されるようにするには、このコマンドの **no** 形式を使用します。

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect ssl compression none
```

MTU サイズの調整

クライアントによって確立された SSL VPN 接続の MTU サイズ（256 ～ 1406 バイト）は、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect mtu** コマンドを使用して調整できます。

[no]anyconnect mtu *size*

このコマンドは、AnyConnect クライアントのみに影響します。レガシー Cisco SSL VPN クライアント（SVC）は、さまざまな MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no anyconnect mtu** 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。

このコマンドは、SSL で確立されたクライアント接続、および SSL with DTLS で確立されたクライアント接続に影響を与えます。

例　次の例では、グループ ポリシー *telecommuters* の MTU サイズを 1200 バイトに設定します。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect mtu 1200
```

AnyConnect クライアント イメージのアップデート

ASA のクライアント イメージは、次の手順を使用していつでもアップデートできます。

ステップ 1　特権 EXEC モードで **copy** コマンドを使用して、または別の方法で新しいクライアント イメージを ASA にコピーします。

ステップ 2　新しいクライアント イメージ ファイルの名前がすでにロードされているファイルと同じファイル名の場合は、コンフィギュレーションにある **anyconnect image** コマンドを再入力します。新しいファイル名が異なっている場合は、**noanyconnect image** コマンドを使用して古いファイルをアンインストールします。次に、**anyconnect image** コマンドを使用して、イメージに順序を割り当て、ASA が新しいイメージをロードするようにします。

IPv6 VPN アクセスのイネーブル化

IPv6 アクセスを設定する場合は、コマンドライン インターフェイスを使用して IPv6 を設定する必要があります。ASDM は IPv6 をサポートしていません。

（注）　ASA は、IPsec IKEv2 VPN セッションで IPv6 をサポートしません。

IPv6 アクセスをイネーブルにするには、SSL VPN 接続のイネーブル化の一部として **ipv6 enable** コマンドを使用します。次は、外部インターフェイスで IPv6 をイネーブルにする IPv6 接続の例です。

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

IPV6 SSL VPN をイネーブルにするには、次の一般的なアクションを実行します。

1. 外部インターフェイスで IPv6 をイネーブルにする。
2. 内部インターフェイスで IPv6 および IPv6 アドレスをイネーブルにする。
3. クライアント割り当て IP アドレス用に IPv6 アドレス ローカル プールを設定する。
4. IPv6 トンネルのデフォルト ゲートウェイを設定する。

この手順を実装するには、次の手順を実行します。

ステップ 1　インターフェイスを設定します。

```
interface GigabitEthernet0/0
     nameif outside
     security-level 0
     ip address 192.168.0.1 255.255.255.0
     ipv6 enable           ; Needed for IPv6.
    !
interface GigabitEthernet0/1
     nameif inside
     security-level 100
     ip address 10.10.0.1 255.255.0.0
     ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
     ipv6 enable           ; Needed for IPv6.
```

ステップ 2　「ipv6 local pool」（IPv6 アドレスの割り当てに使用）を設定します。

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

（注）　IPv6 を使用する場合でも、IPv4 アドレス プールを設定する必要があります（ip local pool コマンドを使用）。

ステップ 3　ipv6 アドレス プールをトンネルグループ ポリシー（またはグループ ポリシー）に追加します。

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

（注）　ここでも、「address-pool」コマンドを使用して IPv4 アドレス プールを設定する必要があります。

ステップ 4　IPv6 トンネルのデフォルト ゲートウェイを設定します。

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

AnyConnect 接続のモニタリング

アクティブなセッションについての情報を表示するには、**show vpn-sessiondb** を使用します。

コマンド	目的
show vpn-sessiondb	アクティブなセッションに関する情報を表示します。
vpn-sessiondb logoff	VPN セッションをログオフします。
show vpn-sessiondb anyconnect	VPN セッションの要約を拡張して、OSPFv3 セッション情報を表示します。
show vpn-sessiondb ratio encryption	Suite-B のアルゴリズム（AES-GCM-128、AES-GCM-192、AES-GCM-256、AES-GMAC-128 など）用のトンネル数およびパーセンテージを表示します。

例

Inactivity フィールドに、AnyConnect セッションが接続を失ってからの経過時間が表示されています。セッションがアクティブな状態の場合、このフィールドには 00:00m:00s が表示されます。

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client         Encryption   : 3DES
Hashing      : SHA1                   Auth Mode    : userPassword
TCP Dst Port : 443                    TCP Src Port : 54230
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity   : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

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
```

AnyConnect VPN セッションのログオフ

すべての 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** コマンドを使用します。

vpn-sessiondb logoff

次に、すべての VPN セッションをログオフする例を示します。

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

name 引数または index 引数のいずれかを使用して、個々のセッションをログオフできます。

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

ライセンス容量に達して新しいユーザがログインできなくることがないように、非アクティブの状態が最長時間続いたセッションはアイドル状態になります（自動的にログオフされます）。そのセッションが後で再開すると、そのセッションは非アクティブ リストから削除されます。

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 anyconnect** コマンドの出力で確認できます。次の例は、ユーザ名 *lee* とインデックス番号 *1* を示しています。

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

次の例は、**vpn-session-db 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 lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name “lee” logged off : 1

hostname#
```

AnyConnect 接続をイネーブルにする設定例

次の例は、L2TP over IPsec を設定する方法を示しています。

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
aaa-server sales_server protocol radius
crypto ipsec transform-set sales_l2tp_transform esp-3des esp-sha-hmac
crypto ipsec transform-set sales_l2tp_transform mode transport
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
l2tp tunnel hello 100

group-policy sales_policy internal
group-policy sales_policy attributes
 wins-server value 209.165.201.3 209.165.201.4
 dns-server value 209.165.201.1 209.165.201.2
 vpn-tunnel-protocol l2tp-ipsec
tunnel-group sales_tunnel type remote-access
tunnel-group sales_tunnel general-attributes
 address-pool sales_addresses
 authentication-server-group none
 accounting-server-group sales_server
 default-group-policy sales_policy
tunnel-group sales_tunnel ppp-attributes
 authentication pap
```

AnyConnect 接続の機能履歴

表 79-2 に、この機能のリリース履歴を示します。

表 79-2　AnyConnect 接続の機能履歴

機能名	リリース	機能情報
AnyConnect 接続	7.2(1)	**authentication eap-proxy**、**authentication ms-chap-v1**、**authentication ms-chap-v2**、**authentication pap**、**l2tp tunnel hello**、および **vpn-tunnel-protocol l2tp-ipsec** コマンドが導入または変更されました。
IPsec IKEv2	8.4(1)	AnyConnect および LAN-to-LAN の IPsec IKEv2 接続をサポートする IKEv2 が追加されました。