CHAPTER 3

CLI を使用した VPN クライアント パラメータの設定

この章では、適応型セキュリティ アプライアンスのコマンドライン インターフェイスを使用した VPN クライアント パラメータの設定方法について説明します。他の章と同じように、ここでは特に VPN クライアントに対して設定する必要があるパラメータに重点を置いて説明します。IPsec グループは、IPsec 接続パラメータを使用してトンネルを作成します。この章で詳しく説明するのは VPN に関連するパラメータのみです。CLI を使用した設定に関する詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Configuration Guide*』を参照してください。

CLI と ASDM はどちらも、次のような VPN クライアントに対するパラメータの設定を行う必要があり、その全般的な内容は同じです。

- IPsec 接続プロファイルを設定する。
- IPsec の拡張機能を設定する。
- クライアント アップデートを設定する。

この章は、次の項で構成されています。

IPsec 接続に対して設定可能なすべてのパラメータに関する詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Configuring Connection Profiles, Group Policies, and Users Using CLI」という章を熟読することを推奨します。その章には、リモート ユーザが IPsec トンネルを介して接続するための詳細な設定情報のほか、クライアント バナー、ファイアウォール、スプリット トンネリングなどの設定機能をはじめとするさまざまな機能の使用方法が記載されています。

接続プロファイルの設定：概要

この項で説明するパラメータは、トンネルグループ コマンドを使用して設定します。IPsec 接続は、IPsec VPN 接続の接続固有レコードを表すものです。要約すると、最初に接続プロファイルを設定して、接続用の値を設定します。次に、グループ ポリシーを設定します。グループ ポリシーでは、ユーザの集合に関する値が設定されます。その後、ユーザを設定します。ユーザはグループの値を継承でき、さらに個別のユーザ単位に特定の値を設定することができます。この章では、接続プロファイルおよびグループ ポリシーに対して VPN クライアント関連のパラメータを設定する方法および理由について説明します。

IPsec 接続プロファイルの設定を行う手順は次のとおりです。

ステップ 1　IPsec 接続プロファイルを設定する。接続プロファイルを追加または編集する場合は、接続プロファイル名を指定します。次の注意事項があります。

- 認証に事前共有キーを使用するクライアントの場合、接続プロファイル名は IPsec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
- 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、セキュリティ アプライアンスが証明書からこの名前を抽出します。

ステップ 2　[Access Interfaces] エリアで、適切なインターフェイス（設定済みの）を有効にして、IPsec アクセスができるようにします。

ステップ 3　必要に応じて [Connection Profiles] エリアで、新しい接続プロファイルを追加したり、既存のプロファイルを編集したりします。

接続プロファイルの一般パラメータの設定

一般パラメータは、すべての VPN 接続に共通です。これらのパラメータはすべて設定する（またはデフォルト値をそのまま使用する）必要がありますが、以下の項では VPN クライアント接続に対して設定が必要なパラメータに限って説明します。一般パラメータには、次のものがあります。

- 接続プロファイル名：接続プロファイル名は、接続プロファイルを追加または編集するときに指定します。次の注意事項があります。
  - 認証に事前共有キーを使用するクライアントの場合、接続プロファイル名は IPsec クライアントがセキュリティ アプライアンスに渡すグループ名と同じです。
  - 認証に証明書を使用するクライアントはこの名前を証明書の一部として渡し、セキュリティ アプライアンスが証明書からこの名前を抽出します。
- 接続タイプ：接続タイプには、IPsec リモート アクセス、IPsec LAN-to-LAN、クライアントレス SSL VPN などがあります。接続プロファイルでは、1 つの接続タイプだけ指定できます。VPN クライアントに対しては、IPsec リモート アクセス接続プロファイルを少なくとも 1 つ設定する必要があります。
- 認証、認可、アカウンティング サーバ：これらのパラメータでは、セキュリティ アプライアンスが次の目的で使用するサーバのグループまたはリストを指定します。
  - ユーザの認証
  - ユーザがアクセスを認可されたサービスに関する情報の取得
  - アカウンティング レコードの保存

  サーバ グループは、1 つ以上のサーバで構成されます。
- 接続用のデフォルト グループ ポリシー：グループ ポリシーは、ユーザ関連の属性のセットです。デフォルト グループ ポリシーは、セキュリティ アプライアンスがトンネル ユーザを認証または認可する際にデフォルトで使用する属性を含んだグループ ポリシーです。
- クライアント アドレスの割り当て方式：この方式には、セキュリティ アプライアンスがクライアントに割り当てる 1 つ以上の DHCP サーバまたはアドレス プールの値が含まれます。
- アカウント無効の上書き：このパラメータを使用すると、AAA サーバから受信した「account-disabled」インジケータを上書きできます。

- パスワード管理：このパラメータを使用すると、現在のパスワードが指定日数（デフォルトは 14 日）で期限切れになることをユーザに警告して、パスワードを変更する機会をユーザに提供できます。
- グループ除去および領域除去：これらのパラメータにより、セキュリティ アプライアンスが受信するユーザ名を処理する方法が決まります。これらは、user@realm の形式で受信するユーザ名にだけ適用されます。領域は @ デリミタ付きでユーザ名に付加される管理ドメインです（user@abc）。

  strip-group コマンドを指定すると、セキュリティ アプライアンスは、VPN クライアントによって提示されたユーザ名からグループ名を取得することによって、ユーザ接続の接続プロファイルを選択します。次に、セキュリティ アプライアンスは、認可および認証のためにユーザ名のユーザ部分だけを送信します。それ以外の場合（ディセーブルになっている場合）、セキュリティ アプライアンスは領域を含むユーザ名全体を送信します。

  レルム除去処理によって、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムが削除されます。このコマンドをイネーブルにすると、セキュリティ アプライアンスでは、ユーザ名のユーザ部分のみを認可 / 認証のために送信します。それ以外の場合、セキュリティ アプライアンスではユーザ名全体を送信します。
- 認可の要求：このパラメータを使用すると、ユーザ接続の前に認可を要求したり、またはその要求を取り下げたりできます。
- 認可 DN 属性：このパラメータは、認可を実行するときに使用する認定者名属性を指定します。

IPsec 接続プロファイルのパラメータ

IPsec 接続プロファイル / トンネル グループのパラメータは次のとおりです。

- クライアント認証方式：事前共有キー、証明書、または両方。
  - 事前共有キーに基づいた IKE 接続の場合、接続ポリシーに関連付けられた英数字のキー自体です（最大 128 文字）。
  - ピア ID 確認の要求：このパラメータでは、ピアの証明書を使用してピアの ID を確認することを要求するかどうかを指定します。
- 拡張ハイブリッド認証方式：XAUTH およびハイブリッド XAUTH。

  isakmp ikev1-user-authentication コマンドを使用すると、セキュリティ アプライアンス認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、SecurID などのレガシー方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装することができます。
- ISAKMP（IKE）キープアライブの設定：この機能により、セキュリティ アプライアンスはリモート ピアの継続的な存在をモニタし、自分自身の存在をピアに報告します。ピアが応答しなくなると、セキュリティ アプライアンスは接続を削除します。IKE キープアライブをイネーブルにすると、IKE ピアが接続を失ったときに接続がハングしません。

  IKE キープアライブにはさまざまな形式があります。この機能が動作するには、セキュリティ アプライアンスとリモート ピアが共通の形式をサポートしている必要があります。この機能は、次のピアに対して動作します。
  - Cisco AnyConnet VPN Client
  - Cisco VPN Client（Release 3.0 以上）
  - Cisco VPN 3000 Client（Release 2.x）
  - Cisco VPN 3002 Hardware Client
  - Cisco VPN 3000 シリーズ Concentrator

  - Cisco IOS ソフトウェア
  - Cisco Secure PIX Firewall

  シスコ以外の VPN クライアントは IKE キープアライブをサポートしません。

  IKE キープアライブをサポートするピアとサポートしないピアが混在するグループを設定する場合は、グループ全体に対して IKE キープアライブをイネーブルにします。この機能をサポートしないピアに影響はありません。

  IKE キープアライブをディセーブルにすると、応答しないピアとの接続はタイムアウトになるまでアクティブのままになるため、アイドル タイムアウトを短くすることを推奨します。アイドル タイムアウトを変更する場合は、「グループ ポリシーの設定」（P.3-15）を参照してください。

- デジタル証明書を使用して認証を設定する場合、証明書チェーン全体を送信する（ID 証明書と発行するすべての証明書をピアに送信する）か、証明書だけを発行する（ルート証明書とすべての下位 CA 証明書を含む）かを指定できます。
- Windows クライアント ソフトウェアの古いバージョンを使用しているユーザに、クライアントをアップデートする必要があることを通知し、アップデートされたクライアント バージョンをユーザが取得するためのメカニズムを提供できます。VPN 3002 ハードウェア クライアント ユーザの場合は、自動アップデートをトリガーできます。すべての接続プロファイルまたは特定の接続プロファイルに対して、client-update を設定および変更できます。
- デジタル証明書を使用して認証を設定する場合は、IKE ピアに送信する証明書を識別するトラストポイントの名前を指定できます。

接続プロファイルの設定：詳細

次の項では、接続プロファイルの内容および設定について説明します。

- 「デフォルトの IPsec リモートアクセス接続プロファイルの設定」（P.3-4）
- 「IPsec リモート アクセス接続プロファイルの名前とタイプの指定」（P.3-5）
- 「IPsec リモートアクセス接続プロファイルの設定」（P.3-5）

デフォルトの接続プロファイルを変更し、3 つのトンネルグループ タイプのいずれかで新しい接続プロファイルを設定できます。接続プロファイル内で明示的に設定しない属性に対しては、その値がデフォルトの接続プロファイルから取得されます。デフォルトの接続プロファイル タイプはリモートアクセスです。その後のパラメータは、選択したトンネル タイプによって異なります。デフォルト接続プロファイルも含めて、すべての接続プロファイルの現在のコンフィギュレーションとデフォルトのコンフィギュレーションを確認するには、**show running-config all tunnel-group** コマンドを入力します。

デフォルトの IPsec リモートアクセス接続プロファイルの設定

デフォルトのリモートアクセス接続プロファイルの内容は、次のとおりです。

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
```

```
 no strip-group
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

IPsec トンネルグループの一般属性の設定

一般属性は、複数の接続プロファイル タイプに共通です。IPsec リモートアクセス トンネルとクライアントレス SSL VPN トンネルでは、同じ一般属性の大部分を共有しています。IPsec LAN-to-LAN トンネルでは、サブセットが使用されます。すべてのコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。以下の項では、IPsec リモートアクセス接続プロファイルの設定方法を、順を追って説明します。

IPsec リモートアクセス接続プロファイルの設定

ハードウェア クライアントまたはソフトウェア クライアントを使用してリモート クライアントと中央サイト セキュリティ アプライアンスとの接続を設定する場合には、IPsec リモートアクセス接続プロファイルを使用します。IPsec リモートアクセス接続プロファイルの設定を行うには、まずトンネルグループの一般属性を設定し、さらに IPsec リモートアクセス属性を設定します。IPsec リモート アクセス VPN 接続プロファイルは、リモートアクセス IPsec クライアント接続に対してのみ適用されます。IPsec リモートアクセス接続プロファイルの設定を行う場合は、次の項を参照してください。

- 「IPsec リモート アクセス接続プロファイルの名前とタイプの指定」（P.3-5）。
- 「IPsec リモートアクセス接続プロファイルの一般属性の設定」（P.3-6）。
- 「IPsec リモートアクセス接続プロファイルの IPsec 属性の設定」（P.3-7）。

IPsec リモート アクセス接続プロファイルの名前とタイプの指定

tunnel-group コマンドを入力し、名前とタイプを指定して、接続プロファイルを作成します。IPsec リモートアクセス トンネルの場合、タイプは **remote-access** です。

```
hostname(config)# tunnel-group tunnel_group_name type remote-access
hostname(config)#
```

たとえば、TunnelGroup1 という名前の IPsec リモートアクセス接続プロファイルを作成する場合は、次のようなコマンドを入力します。

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

IPsec リモートアクセス接続プロファイルの一般属性の設定

通常は、すべての一般属性に対してデフォルト値を使用することができますが、場合によっては特定のパラメータ群の値を変更する必要があります。接続プロファイルの一般属性を設定または変更するには、次の手順でパラメータを指定します。

ステップ 1　一般属性を設定するには、**tunnel-group general-attributes** コマンドを入力します。これで、トンネルグループ一般属性コンフィギュレーション モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

ステップ 2　認証サーバ グループがある場合、使用するグループの名前を指定します。指定したサーバ グループに障害が発生したときにローカル データベースを認証に使用する場合は、キーワード **LOCAL** を追加します。

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

認証サーバ グループの名前は、最大 16 文字です。

オプションで、グループ名の後ろにインターフェイス名を指定することにより、インターフェイス固有の認証を設定することもできます。IPsec トンネルの終了場所を指定するインターフェイス名は、丸カッコで囲む必要があります。次のコマンドでは、認証にサーバ servergroup1 を使用する test という名前のインターフェイスのインターフェイス固有の認証が設定されます。

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

ステップ 3　使用する認可サーバ グループの名前を指定します（存在する場合）。この値を設定する場合、ユーザは接続する認可データベースに存在する必要があります。

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

認可サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、認可サーバ グループ FinGroup を使用することを指定しています。

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

ステップ 4　アカウンティングサーバ グループがある場合、使用するグループの名前を指定します。

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

アカウンティング サーバ グループの名前は、最大 16 文字です。たとえば、次のコマンドは、アカウンティングサーバ グループ comptroller を使用することを指定しています。

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

ステップ 5　デフォルト グループ ポリシーの名前を指定します。

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

グループ ポリシーの名前は、最大 64 文字です。次の例では、デフォルト グループ ポリシーの名前として DfltGrpPolicy を設定しています。

```
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
hostname(config-tunnel-general)#
```

ステップ 6　DHCP サーバ（最大 10 サーバ）の名前または IP アドレス、および DHCP アドレス プール（最大 6 プール）の名前を指定します。デフォルトでは、DHCP サーバとアドレス プールは使用されません。

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

（注）　インターフェイス名を指定する場合は、丸カッコで囲む必要があります。

アドレス プールは、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して設定します。

ステップ 7　証明書から認可クエリー用の名前を得るために使用する 1 つまたは複数の属性を指定します。この属性により、サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかが指定されます。

```
hostname(config-tunnel-general)# username-from-certificate {primary-attribute
[secondary-attribute] | use-entire-name}
```

たとえば、次のコマンドは、CN 属性を認可用のユーザ名として使用することを指定しています。

```
hostname(config-tunnel-general)# username-from-certificate CN
hostname(config-tunnel-general)#
```

authorization-dn-attributes は、**C**（国）、**CN**（通常名）、**DNQ**（DN 修飾子）、**EA**（電子メール アドレス）、**GENQ**（世代修飾子）、**GN**（名）、**I**（イニシャル）、**L**（地名）、**N**（名前）、**O**（組織）、**OU**（組織ユニット）、**SER**（シリアル番号）、**SN**（姓）、**SP**（州または都道府県）、**T**（役職）、**UID**（ユーザ ID）、および **UPN**（ユーザ プリンシパル ネーム）があります。

IPsec リモートアクセス接続プロファイルの IPsec 属性の設定

リモートアクセス接続プロファイルの IPsec 属性を設定する手順は次のとおりです。次の説明は、IPsec リモートアクセス接続プロファイルが作成済みであることを前提としています。

IKE メイン モードを使用する LAN-to-LAN コンフィギュレーションの場合は、2 つのピアの IKE キープアライブのコンフィギュレーションが同じであることを確認してください。両方のピアで IKE キープアライブがイネーブルになっているか、または両方のピアで IKE キープアライブがディセーブルになっている必要があります。

（注） ISDN 回線経由で接続するクライアントがグループに含まれる場合は、接続コストを削減するために IKE キープアライブをディセーブルにしてください。通常、ISDN 接続はアイドルになると切断されますが、IKE キープアライブのメカニズムによって接続がアイドル状態にならないため、切断されなくなります。

IKE キープアライブをディセーブルにすると、クライアントは IKE キーまたは IPSec キーのいずれかの期限が満了した場合にだけ切断されます。IKE キープアライブがイネーブルになっている場合とは異なり、障害が発生したトラフィックは Peer Timeout Profile 値を持つトンネルから切断されません。

IPsec 接続プロファイルの IPsec 属性を設定する手順は次のとおりです。

ステップ 1　IPsec リモートアクセス接続プロファイルの属性を指定するため、次のコマンドを入力してトンネルグループ ipsec 属性モードに入ります。プロンプトが変化して、モードが変更されたことがわかります。

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

このコマンドにより、トンネルグループ ipsec 属性コンフィギュレーション モードに入ります。このモードで、リモートアクセス トンネルグループの IPsec 属性を設定します。

たとえば、次のコマンドは、TG1 という名前の接続プロファイルに関係するトンネルグループ ipsec 属性モードのコマンドが続くことを指定しています。プロンプトが変化して、トンネルグループ ipsec 属性モードに入ったことがわかります。

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 2　事前共有キーに基づく IKE 接続をサポートするために、事前共有キーを指定します。たとえば、次のコマンドでは、IPsec リモートアクセス接続プロファイルの IKE 接続をサポートするために、事前共有キー xyzx が指定されています。

```
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

ステップ 3　ピアの証明書を使用してピアの ID を検証するかどうかを指定します。

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

使用できるオプションは、**req**（必須）、**cert**（証明書でサポートされている場合）、**nocheck**（調べない）です。デフォルトは **req** です。

たとえば、次のコマンドは peer-id 検証が必要なことを指定しています。

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

ステップ 4　証明書チェーンを送信できるかどうかを指定します。次のコマンドは、ルート証明書とすべての下位 CA 証明書を送信しています。

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

この属性は、すべての IPsec トンネルグループ タイプに適用されます。

ステップ 5　IKE ピアに送信する証明書を識別するトラストポイントの名前を指定します。

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
```

```
hostname(config-tunnel-ipsec)#
```

次のコマンドは、IKE ピアに送信する証明書の名前として mytrustpoint を指定しています。

```
hostname(config-ipsec)# trust-point mytrustpoint
```

ステップ 6　ISAKMP（IKE）キープアライブのしきい値と許可されるリトライ回数を指定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

threshold パラメータでは、ピアがキープアライブ モニタリングを開始するまでの最長アイドル時間を秒数（10 ～ 3600）で指定します。**retry** パラメータは、キープアライブ応答が受信されなくなった後のリトライ間の間隔です（2 ～ 10 秒）。IKE キープアライブは、デフォルトでイネーブルです。IKE キープアライブを無効にする場合は、**isakmp** コマンドの **no** 形式を入力します。

たとえば、次のコマンドは、IKE キープアライブのしきい値を 15 秒に設定し、リトライ インターバルを 10 秒に設定します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

threshold パラメータのデフォルト値は、リモートアクセスの場合は 300、LAN-to-LAN の場合は 10 です。また、retry パラメータのデフォルト値は 2 です。

中央サイト（「ヘッド エンド」）で、ISAKMP モニタリングを決して開始しないように指定する場合は、次のコマンドを入力します。

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

ステップ 7　ISAKMP ハイブリッド認証方式、XAUTH またはハイブリッド XAUTH を指定します。

isakmp ikev1-user-authentication コマンドは、セキュリティ アプライアンス認証にデジタル証明書を使用する必要がある場合、およびリモート VPN ユーザ認証に RADIUS、TACACS+、または SecurID などのレガシーな方式を別途使用する必要がある場合に、ハイブリッド XAUTH 認証を実装するために使用します。ハイブリッド XAUTH によって、IKE のフェーズ 1 が次の 2 つの手順に分割されます。2 つ合せてハイブリッド認証と呼ばれます。

a. セキュリティ アプライアンスは、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。

b. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

isakmp ikev1-user-authentication コマンドとオプションの **interface** パラメータを使用して、特定のインターフェイスを指定できます。**interface** パラメータを省略すると、このコマンドはすべてのインターフェイスに適用され、インターフェイスごとにコマンドが指定されていない場合のバックアップとして機能します。接続プロファイルに 2 つの **isakmp ikev1-user-authentication** コマンドを指定していて、1 つで **interface** パラメータを使用し、もう 1 つで使用しない場合、インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

たとえば、次のコマンドは、example-group と呼ばれる接続プロファイルの内部インターフェイスでハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
```

```
hostname(config-tunnel-ipsec)#
```

ASDM を使用したクライアント ソフトウェア アップデートの設定

オプションのクライアント アップデート機能を使用すると、許可されるクライアントのリビジョン レベルを確保できます。この機能を使用すると、中央にいる管理者は、VPN クライアント ソフトウェアおよび VPN 3002 ハードウェア クライアント イメージのアップデート時期を、VPN クライアント ユーザに自動的に通知できます。

リモート ユーザは、旧式の VPN ソフトウェア バージョンまたはハードウェア クライアント バージョンを使用している可能性があります。クライアント アップデート機能を使用すれば、いつでもクライアント リビジョンのアップデートを有効にして、アップデートが適用されるクライアントのタイプおよびリビジョン番号を指定し、アップデートを取得する URL または IP アドレスを通知することができます。また Windows クライアントの場合は、オプションとして VPN クライアント バージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントに対しては、更新を実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知せずに自動的に行われます。この機能は、IPsec リモート アクセス トンネル グループ タイプにのみ適用されます。

リビジョン番号のリストに含まれるソフトウェア バージョンより新しいバージョンがすでにクライアントで実行されている場合は、そのソフトウェアをアップデートする必要はありません。リストにあるソフトウェア バージョン（またはそれ以降のバージョン）が実行されていないクライアントでは、ソフトウェアを更新する必要があります。

VPN クライアントのコマンドを使用すると、インストール済みのクライアント VPN ソフトウェア パッケージごとに、クライアント タイプ、VPN クライアントのリビジョン、およびイメージの URL をリスト表示できます。クライアント タイプごとに、許可されるクライアント ソフトウェア リビジョンと、必要に応じて、ソフトウェア アップグレードをダウンロードする URL または IP アドレスを指定できます。クライアント アップデート メカニズム（[Client Update] ウィンドウに詳細説明があります）は、この情報を使用して、各 VPN クライアントが適切なリビジョン レベルで実行されているかどうかを判断し、適切であれば、通知メッセージとアップデート メカニズムを、旧式のソフトウェアを実行しているクライアントに提供します。クライアント アップデートを設定するには、次のフィールドで指定します。

VPN クライアント ソフトウェアのアップデート機能を設定するには、次の手順を実行します。

ステップ 1　クライアント アップデートを有効にします。

```
client-update enable
```

このコマンドにより、クライアント アップデートをグローバルにも特定のトンネル グループに対しても有効にすることができます。クライアント アップデートをイネーブルにしてから、Windows、MAC OS X、および Linux の VPN クライアントにクライアント アップデート通知を送信するか、またはハードウェア クライアントの自動アップデートを開始する必要があります。

ステップ 2　設定するクライアント アップデートのタイプを指定します。次のような client-update コマンドを使用します。

client-update type *client-type* **url** *image-url revisions*

それぞれの説明は次のとおりです。

- *client-type*：アップグレードするクライアント（ソフトウェアまたはハードウェア）をリスト表示します。Windows ソフトウェア クライアントの場合には、すべての Windows またはサブセットを表示します。値は次のとおりです。

- Win9X：Windows 95、Windows 98、および Windows ME の各プラットフォーム。
- WinNT：Windows NT 4.0、Windows 2000、Windows XP、および Windows Vista の各プラットフォーム。
- Windows：あらゆる Windows ベースのプラットフォーム。
- linux：Linux クライアント。
- Mac OS X：Mac OS X クライアント。
- solaris：Solaris クライアント。
- vpn3002：VPN3002 ハードウェア クライアント。

windows を指定する場合は、個別の Windows バージョンを指定しないでください。セキュア ゲートウェイからは、クライアント アップデート リストのエントリごとに個別の通知メッセージが送信されます。そのため、クライアント アップデート エントリは重複しないようにする必要があります。たとえば、「Windows」という値にはすべての Windows プラットフォームが含まれ、「WinNT」という値には Windows Vista、Windows XP、Windows 2000、および Windows NT 4.0 が含まれます。そのため、「Windows」と「Windows NT」を同時に指定することはできません。クライアント タイプおよびバージョン情報を確認する場合は、Cisco Systems VPN Client のメイン ウィンドウの左上隅にある鍵アイコンをクリックし、[About VPN Client] を選択します。

ハードウェア クライアントは、ASA 5505 ソフトウェアまたは VPN 3002 ハードウェア クライアントのリリースと一緒にアップデートされます。

（注） すべての Windows クライアントをサポートするようにクライアント アップデート機能がすでに設定されている場合、個々の Windows クライアント タイプを指定するためには、あらかじめその設定を解除しておく必要があります。

- *image-url*：ソフトウェア イメージのダウンロード元となる URL または IP アドレスを指定します。この URL は、クライアントに適合するファイルを指している必要があります。Windows、MAC OS X、および Linux ベースのクライアントの場合は、URL を http:// または https:// 形式にする必要があります。ハードウェア クライアントの場合、URL は tftp:// という形式にする必要があります。
  - Windows、MAC OS X、および Linux ベースの VPN クライアントの場合：VPN クライアント通知で [Launch] ボタンをアクティブにするには、URL に、HTTP または HTTPS というプロトコル名と、アップデートが格納されているサイトのサーバ アドレスを含める必要があります。URL の形式は、http(s):// サーバ_アドレス : ポート / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。例：

    ```
    http://10.10.99.70/vpnclient-win-4.6.Rel-k9.exe
    ```

    ディレクトリはオプションです。ポート番号は、80 以外の HTTP ポート、443 以外の HTTPS ポートを使用する場合にだけ必要です。
  - ハードウェア クライアントの場合、URL の形式は、tftp:// サーバ_アドレス / ディレクトリ / ファイル名です。DNS サーバが設定済みの場合、IP アドレスまたはホスト名のどちらもサーバ アドレスとして使用できます。例：

    ```
    tftp://10.1.1.1/vpn3002-4.1.Rel-k9.bin
    ```

- *revisions*：このクライアントに合ったソフトウェア イメージ リビジョンのカンマ区切りリストを指定します。ユーザのクライアント リビジョン番号が、指定されているリビジョン番号のいずれかと同じかそれより新しい場合には、クライアントを更新する必要はありません。Windows ベースのクライアントの場合、ユーザはアップデート通知を受信しません。次の警告が適用されます。
  - リビジョン リストには、このアップデートのソフトウェア バージョンが記載されている必要があります。

- 自分のエントリが、VPN クライアントの場合には URL と、ハードウェア クライアントの場合には TFTP サーバと正確に一致する必要があります。
- ハードウェア クライアント イメージを配布するための TFTP サーバは堅牢である必要があります。
- VPN クライアント ユーザは、一覧表示されている URL から適切なソフトウェア バージョンをダウンロードする必要があります。
- VPN 3002 ハードウェア クライアント ソフトウェアは、ユーザに通知することなく、自動的に TFTP 経由でアップデートされます。

グループ ポリシーの設定

グループ ポリシーは、IPsec 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の RADIUS サーバに保存されます。接続プロファイルでは、トンネル確立後、ユーザ接続の条件を設定するグループ ポリシーが使用されます。グループ ポリシーを使用すると、ユーザまたはユーザのグループに属性セット全体を適用できるので、ユーザごとに各属性を個別に指定する必要がありません。

ユーザにグループ ポリシーを割り当てたり、特定のユーザのグループ ポリシーを変更したりするには、グローバル コンフィギュレーション モードで **group-policy** コマンドを入力します。

セキュリティ アプライアンスには、デフォルトのグループ ポリシーが含まれています。変更はできても削除はできないデフォルトのグループ ポリシーに加え、自分の環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

内部グループ ポリシーと外部グループ ポリシーを設定できます。内部グループは セキュリティ アプライアンスの内部データベースで設定されます。外部グループは RADIUS などの外部認証サーバに設定されます。グループ ポリシーには、次の属性があります。

- アイデンティティ
- サーバの定義
- クライアント ファイアウォールの設定
- トンネリング プロトコル
- IPsec の設定
- ハードウェア クライアントの設定
- フィルタ
- クライアント コンフィギュレーションの設定
- 接続の設定

グループポリシーのパラメータのうち、VPN クライアントに特化しているものは一部のみです。ここでは、セキュリティ アプライアンス上でこれらのパラメータを設定する際に使用するコマンドについてのみ説明します。セキュリティ アプライアンスのグループ ポリシーを設定する詳細な方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

デフォルトのグループ ポリシー

セキュリティ アプライアンスでは、デフォルトのグループ ポリシーが提供されます。このデフォルトグループ ポリシーは変更できますが、削除はできません。デフォルトのグループ ポリシーは、DfltGrpPolicy という名前でセキュリティ アプライアンスに常に存在していますが、このデフォルトのグループ ポリシーは、セキュリティ アプライアンスでそれを使用するように設定しない限り有効にはなりません。その他のグループ ポリシーを設定する場合、明示的に指定しない属性の値はデフォルトのグループ ポリシーから取得されます。デフォルトのグループ ポリシーを表示するには、次のコマンドを入力します。

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

デフォルトのグループ ポリシーを設定するには、次のコマンドを入力します。

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

（注） デフォルトのグループ ポリシーは、常に内部（internal）です。コマンドの構文は `hostname(config)# group-policy DfltGrpPolicy {internal | external}` ですが、タイプを外部（external）に変更することはできません。

デフォルトのグループ ポリシーの任意の属性を変更する場合は、**group-policy attributes** コマンドを使用して属性モードに入り、その後、変更対象の属性を変更するためのコマンドを指定します。

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

（注） 属性モードは内部グループ ポリシーにだけ適用されます。

セキュリティ アプライアンスで提供されるデフォルトのグループ ポリシー DfltGrpPolicy は、次のとおりです。

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 ipv6-vpn-filter none
 vpn-tunnel-protocol IPSec svc webvpn
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 intercept-dhcp 255.255.255.255 disable
```

```
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 msie-proxy server none
 msie-proxy method no-modify
 msie-proxy except-list none
 msie-proxy local-bypass disable
 msie-proxy pac-url none
 vlan none
 nac-settings none
 address-pools none
 ipv6-address-pools none
 smartcard-removal-disconnect enable
 client-firewall none
 client-access-rule none
 webvpn
  url-list value Engineering
  filter none
  homepage none
  html-content-filter none
  port-forward name Application Access
  port-forward disable
  mapi disable
  http-proxy disable
  sso-server none
  svc dtls enable
  svc mtu 1406
  svc keep-installer installed
  svc keepalive 20
  svc rekey time none
  svc rekey method none
  svc dpd-interval client 30
  svc dpd-interval gateway 30
  svc compression deflate
  svc modules none
  svc profiles none
  svc ask none
  ike-retry-timeout 10
  ike-retry-count 3
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none
  smart-tunnel disable
  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information
hostname(config)#
```

デフォルト グループ ポリシーは変更可能です。また、環境に固有の 1 つ以上のグループ ポリシーを作成することもできます。

グループ ポリシーの設定

グループ ポリシーは、すべての種類のトンネルに適用できます。どちらの場合も、パラメータが明示的に指定されていなければ、そのグループはデフォルト グループ ポリシーの値を使用します。グループ ポリシーを設定するには、後続の項の手順を実行します。

内部グループ ポリシーの設定

内部グループ ポリシーを設定するには、グループ ポリシーの名前とタイプを指定します。

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

たとえば、次のコマンドは GroupPolicy1 という名前の内部グループ ポリシーを作成します。

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

デフォルトのタイプは **internal** です。

キーワード **from** を追加して既存のポリシーの名前を指定することにより、内部グループ ポリシーの属性をその既存のグループ ポリシーの値に初期設定することができます。

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
hostname(config-group-policy)#
```

グループ ポリシー属性の設定

内部グループ ポリシーの場合、特定の属性値を指定できます。まず、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを入力して、グループ ポリシー属性モードに入ります。

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

プロンプトが変化して、モードが変更されたことがわかります。グループ ポリシー属性モードでは、指定したグループ ポリシーの属性と値のペアを設定することができます。グループ ポリシー属性モードで、デフォルト グループから継承しない属性と値のペアを明示的に設定します。これを行うためのコマンドは、次の項で説明します。

VPN 固有の属性の設定

この項の手順に従って、VPN 属性値を設定します。VPN 属性により、アクセス時間、同時に許可されるログインの数、タイムアウト、VPN セッションに適用される出力 VLAN または ACL、およびトンネル プロトコルが制御されます。

ステップ 1　VPN アクセス時間を設定します。これを行うには、グループ ポリシー コンフィギュレーション モードで **vpn-access-hours** コマンドを使用して、グループ ポリシーを設定済みの time-range ポリシーに関連付けます。

```
hostname(config-group-policy)# vpn-access-hours value {time-range | none}
```

グループ ポリシーは、デフォルトまたは指定されたグループ ポリシーの time-range の値を継承することができます。この継承が発生しないようにするには、このコマンドで time-range の名前ではなく **none** キーワードを入力します。このキーワードにより、VPN アクセス時間がヌル値に設定され、time-range ポリシーは許可されなくなります。

time-range 変数は、グローバル コンフィギュレーション モードで **time-range** コマンドを使用して定義されたアクセス時間のセットの名前です。次に、FirstGroup というグループ ポリシーを 824 という time-range ポリシーに関連付ける例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours value 824
```

ステップ 2　グループ ポリシー コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用して、任意のユーザに許可される同時ログイン数を指定します。

```
hostname(config-group-policy)# vpn-simultaneous-logins integer
```

デフォルト値は 3 です。値の範囲は 0 ～ 2147483647 の整数です。グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。次に、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
hostname(config-group-policy)#
```

（注）　同時ログイン数の最大制限は非常に大きい値ですが、複数の同時ログインを許可すると、セキュリティが侵害されたり、パフォーマンスが低下したりすることがあります。

失効した AnyConnect、IPsec クライアント、またはクライアントレス セッション（異常終了したセッション）は、同じユーザ名で「新しい」セッションが確立されても、セッション データベースに残る場合があります。

vpn-simultaneous-logins の値が 1 の場合は、異常終了後に同じユーザが再度ログインすると、失効したセッションはデータベースから削除され、新しいセッションが確立されます。ただし、既存のセッションがまだアクティブな接続である場合は、同じユーザが別の PC などから再度ログインすると、最初のセッションがログオフし、データベースから削除されて、新しいセッションが確立されます。

同時ログイン数が 1 より大きい値の場合、その最大数に達した状態で再度ログインしようとすると、最もアイドル時間の長いセッションがログオフします。現在のすべてのセッションが同じくらい長い間アイドル状態の場合は、最も古いセッションがログオフします。このアクションにより、セッションが解放されて新しいログインが可能になります。

ステップ 3　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを入力して、ユーザ タイムアウト期間を設定します。

```
hostname(config-group-policy)# vpn-idle-timeout {minutes | none}
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルトは 30 分です。この期間中に接続上で通信アクティビティがない場合、セキュリティ アプライアンスは接続を終了します。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを指定して、このコマンドを入力します。**none** キーワードを指定すると、グローバル WebVPN **default-idle-timeout** コマンドに指定されたグローバル WebVPN アイドル タイムアウト時間がこの接続に使用されます。このキーワードにより、アイドル タイムアウトにヌル値が設定され、アイドル タイムアウトが拒否されます。

次の例は、FirstGroup という名前のグループ ポリシーに 15 分の VPN アイドル タイムアウトを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

ステップ 4　グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用して、VPN 接続の最大時間を設定します。

```
hostname(config-group-policy)# vpn-session-timeout {minutes | none}
hostname(config-group-policy)#
```

最小時間は 1 分で、最大時間は 35791394 分です。デフォルト値はありません。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、分を指定する代わりに **none** キーワードを指定して、このコマンドを入力します。**none** キーワードを指定すると、無制限のセッション タイムアウト期間が許可されます。セッション タイムアウトにはヌル値が設定され、セッション タイムアウトが拒否されます。

次に、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

ステップ 5　このグループ ポリシーの VPN 接続ポリシーを指定します。IPsec 接続の場合は、**ipsec** を指定します。

```
hostname(config-group-policy)# vpn-tunnel-protocol {webvpn | ipsec | l2tp-ipsec}
hostname(config-group-policy)#
```

デフォルトは ipsec です。この属性を実行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** 形式を入力します。

```
hostname(config-group-policy)# no vpn-tunnel-protocol [webvpn | ipsec | l2tp-ipsec]
hostname(config-group-policy)#
```

このコマンドのパラメータの値は、次のとおりです。

- **ipsec**：2 つのピア（リモート アクセス クライアントまたは別のセキュア ゲートウェイ）間の IPsec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションを作成します。
- **webvpn**：HTTPS 対応 Web ブラウザ経由でリモート ユーザに VPN サービスを提供します。クライアントは不要です。
- **l2tp-ipsec**：L2TP 接続用の IPsec トンネルをネゴシエートします。

このコマンドを入力して、1 つ以上のトンネリング モードを設定します。VPN トンネルを介して接続するユーザには、少なくとも 1 つのトンネリング モードを設定する必要があります。

次の例は、FirstGroup という名前のグループ ポリシーに IPsec トンネリング モードを設定する方法を示したものです。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ipsec
hostname(config-group-policy)#
```

セキュリティ属性の設定

この項の属性では、グループに対する特定のセキュリティ設定を指定します。これらのパラメータにはデフォルト値をそのまま使用することを推奨します。それらを変更するのは、妥当な理由がある場合のみにしてください。

ステップ 1　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **password-storage** コマンドを使用し、ユーザがログイン パスワードをクライアント システムに保存できるようにするかどうかを指定します。パスワード保存をディセーブルにするには、**disable** キーワードを指定して **password-storage** コマンドを使用します。

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

セキュリティ上の理由から、パスワード保存はデフォルトでディセーブルになっています。セキュアサイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

password-storage 属性を実行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** 形式を入力します。

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

no 形式を指定すると、password-storage の値を別のグループ ポリシーから継承することができます。

このコマンドは、対話的なハードウェア クライアント認証やハードウェア クライアントの個別ユーザ認証には適用されません。

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

ステップ 2　デフォルトではディセーブルになっている IP 圧縮をイネーブルにするかどうかを指定します。

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **ip-comp** コマンドを入力します。IP 圧縮をディセーブルにするには、**disable** キーワードを指定して **ip-comp** コマンドを入力します。

ip-comp 属性を実行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** 形式を入力します。これにより、別のグループ ポリシーの値を継承できます。

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意　データ圧縮を使用すると、ユーザ セッションごとのメモリ要求と CPU 使用率が増加し、結果としてセキュリティ アプライアンスのスループット全体が低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

ステップ 3　グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **re-xauth** コマンドを使用し、IKE キーが再生成される際にユーザが再認証を受ける必要があるかどうかを指定します。IKE キー再生成時の再認証をイネーブルにすると、セキュリティ アプライアンスでは、最初のフェーズ 1 IKE ネゴシエーションにおいてユーザに対してユーザ名とパスワードの入力が求められ、その後 IKE キー再生成が行われるたびにユーザ認証が求められます。再認証によって、セキュリティが強化されます。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。認可要求が何度も繰り返されないようにするには、再認証をディセーブルにします。設定されているキーの再生成インターバルを確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを入力して、セキュリティ アソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。IKE キーが再生成される際のユーザの再認証をディセーブルにするには、**disable** キーワードを入力します。IKE キーが再生成される際の再認証は、デフォルトではディセーブルになっています。

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

IKE キーが再生成される際の再認証用の値を別のグループ ポリシーから継承することをイネーブルにするには、このコマンドの **no** 形式を入力して、実行コンフィギュレーションから re-xauth 属性を削除します。

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

（注）　接続先にユーザが存在しない場合、再認証は失敗します。

ステップ 4　グループ ポリシー コンフィギュレーション モードで **group-lock** コマンドを使用して、接続プロファイルを介してだけアクセスするようにリモート ユーザを制限するかどうかを指定します。

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

tunnel-grp-name 変数は、セキュリティ アプライアンスがユーザの接続に関して要求する既存の接続プロファイルの名前を指定します。group-lock は、VPN クライアントで設定されたグループが、そのユーザが割り当てられている接続プロファイルと同じかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、セキュリティ アプライアンスはユーザによる接続を禁止します。グループ ロックを設定しなかった場合、セキュリティ アプライアンスは、割り当てられているグループに関係なくユーザを認証します。グループのロックは、デフォルトではディセーブルになっています。

group-lock 属性を実行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。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

group-lock をディセーブルにするには、**none** キーワードを指定して **group-lock** コマンドを入力します。none キーワードにより、group-lock はヌル値に設定され、group-lock の制限が拒否されます。また、デフォルトまたは指定されたグループ ポリシーから group-lock の値が継承されなくなります。

ステップ 5　完全転送秘密をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、完全転送秘密により、新しい各暗号キーは以前のどのキーとも関連性がないことが保証されます。グループ ポリシーは、別のグループ ポリシーから完全転送秘密の値を継承できます。完全転送秘密は、デフォルトではディセーブルになっています。完全転送秘密をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、**enable** キーワードを指定して **pfs** コマンドを使用します。

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

完全秘密転送をディセーブルにするには、**disable** キーワードを指定して **pfs** コマンドを入力します。

完全秘密転送属性を実行コンフィギュレーションから削除して、値を継承しないようにするには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

バナー メッセージの設定

表示するバナーまたは初期メッセージ（ある場合）を指定します。デフォルトでは、バナーは表示されません。指定したメッセージは、リモート クライアントが接続したときに、そのクライアントに表示されます。バナーを指定するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを入力します。バナー テキストの長さは 510 文字までです。復帰改行を挿入する場合は、「\n」シーケンスを入力します。

（注）　バナー内の復帰改行は、2 文字として数えられます。

バナーを削除するには、このコマンドの **no** 形式を入力します。このコマンドの **no** 形式を使用すると、グループ ポリシーのすべてのバナーが削除されることに注意してください。

グループ ポリシーは、別のグループ ポリシーからこの値を継承できます。値を継承しないようにするには、次のように、バナー文字列の値を指定する代わりに **none** キーワードを入力します。

```
hostname(config-group-policy)# banner {value banner_string | none}
```

次の例は、FirstGroup という名前のグループ ポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

IPsec-UDP 属性の設定

IPsec over UDP（IPsec through NAT と呼ばれることもあります）を使用すると、Cisco VPN クライアントまたはハードウェア クライアントは、NAT を実行している セキュリティ アプライアンス に UDP 経由で接続できます。この機能はデフォルトではディセーブルになっています。IPsec over UDP は、リモートアクセス接続だけに適用される専用の機能で、モード コンフィギュレーションが必要です。セキュリティ アプライアンスは、SA のネゴシエート時にクライアントとの間でコンフィギュレーション パラメータをやり取りします。IPsec over UDP を使用すると、システム パフォーマンスが若干低下することがあります。

IPsec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、次のように **enable** キーワードを指定して **ipsec-udp** コマンドを設定します。

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

IPsec over UDP を使用するには、次のように **ipsec-udp-port** コマンドも設定する必要があります。

IPsec over UDP をディセーブルにするには、**disable** キーワードを入力します。IPsec over UDP 属性を実行コンフィギュレーションから削除する場合は、このコマンドの **no** 形式を入力します。これにより、別のグループ ポリシーから IPsec over UDP の値を継承できるようになります。

また、IPsec over UDP を使用するように Cisco VPN クライアントを設定しておく必要があります（Cisco VPN クライアントは、デフォルトで IPsec over UDP を使用するように設定されています）。VPN 3002 では、IPsec over UDP を使用するためのコンフィギュレーションが必要ありません。

次の例は、FirstGroup というグループ ポリシーの IPsec over UDP を設定する方法を示したものです。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

IPsec over UDP をイネーブルにした場合は、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドも設定する必要があります。このコマンドにより、IPsec over UDP 用の UDP ポート番号が設定されます。IPsec ネゴシエーションでは、セキュリティ アプライアンスは設定されたポートでリッスンし、他のフィルタ規則で UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。ポート番号の範囲は 4001 ～ 49151 です。デフォルトのポート値は 10000 です。

UDP ポートをディセーブルにするには、このコマンドの **no** 形を入力します。これにより、別のグループ ポリシーから IPsec over UDP ポートの値を継承できるようになります。

```
hostname(config-group-policy)# ipsec-udp-port port
```

次に、FirstGroup というグループ ポリシーの IPsec UDP ポートをポート 4025 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

スプリット トンネリング属性の設定

スプリット トンネリングを使用すると、リモートアクセス IPsec クライアントでは条件に応じて、パケットを暗号化形式により IPsec トンネルを介して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりすることができます。スプリット トンネリングが有効になっている場合、IPsec トンネルの相手側を宛先としないパケットを暗号化する必要はありません。このようなパケットはトンネル上を復号化された状態で送信され、その後、最終的な宛先にルーティングされます。このコマンドは、このスプリット トンネリング ポリシーを特定のネットワークに適用します。

スプリット トンネリング ポリシーの設定

スプリット トンネリング ポリシーを指定して、トラフィックのトンネリング規則を設定します。

```
hostname(config-group-policy)# split-tunnel-policy {tunnelall | tunnelspecified |
excludespecified}
hostname(config-group-policy)# no split-tunnel-policy
```

デフォルトでは、すべてのトラフィックがトンネリングされます。スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを入力します。**split-tunnel-policy** 属性を実行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** 形式を入力します。これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

トラフィックがクリア テキストで送信されるネットワークのリストは、**excludespecified** キーワードで定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。このオプションは、Cisco VPN クライアントに対してだけ適用されます。ACL は、次の 3 つの方法のうちいずれかを使用して設定します。

- 0.0.0.0/0.0.0.0（任意）：クライアントは、ローカル アダプタからローカル ネットワークを認識し、ローカル アダプタを介してローカル ネットワーク トラフィックをルーティングすると同時に、その他すべてのトラフィックを VPN トンネル経由で送信します。
- 0.0.0.0/255.255.255.255（ホスト 0.0.0.0）：クライアントは、ローカル アダプタを介してローカル ネットワーク トラフィックをルーティングすると同時に、その他すべてのトラフィックを VPN トンネル経由で送信します。
- 10.0.0.0/0.255.255.255：クライアントは、ローカル アダプタを介して 10.0.0.0/8 ネットワークへのトラフィックをルーティングすると同時に、その他すべてのトラフィックを VPN トンネル経由で送信します。

tunnelall キーワードを指定すると、すべてのトラフィックがクリア テキストとして送信されなくなるか、セキュリティ アプライアンス以外の宛先に送信されなくなります。この指定では、実質的にスプリット トンネリングはディセーブルになります。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。これはデフォルトのオプションです。

tunnelspecified キーワードを指定すると、指定されたネットワークとの間のすべてのトラフィックがトンネリングされます。このオプションによって、スプリット トンネリングがイネーブルになります。トンネリングするアドレスのネットワーク リストを作成できるようになります。それ他すべてのアドレスに対するデータは、クリア テキストで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

（注） スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最大限のセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

スプリット トンネリング用のネットワーク リストの作成

グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用して、スプリット トンネリング用のネットワーク リストを作成します。

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。セキュリティ アプライアンスは、ネットワーク リストに基づいてスプリット トンネリングを実行するかどうかを決定します。ネットワーク リストは、プライベート ネットワーク上のアドレスのリストで構成された ACL です。標準タイプの ACL だけが許可されます。

value *access-list name* パラメータでは、トンネリングを実行する、または実行しないネットワークを列挙したアクセス リストを指定します。

none キーワードは、スプリット トンネリング用のネットワーク リストが存在しないことを示し、セキュリティ アプライアンスはすべてのトラフィックをトンネリングします。**none** キーワードを指定すると、スプリット トンネリングのネットワーク リストにヌル値が設定され、スプリット トンネリングが拒否されます。また、これにより、デフォルトまたは指定されたグループ ポリシーから、デフォルトのスプリット トンネリング ネットワーク リストが継承されなくなります。

ネットワーク リストを削除するには、このコマンドの **no** 形式を入力します。すべてのスプリット トンネリング ネットワーク リストを削除するには、引数を指定せずに **no split-tunnel-network-list** コマンドを入力します。このコマンドにより、**none** キーワードを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのネットワーク リストが削除されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを入力します。

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

トンネリング用のドメイン属性の設定

トンネリングされたパケットのデフォルト ドメイン名、またはスプリット トンネルを経由して解決されるドメインのリストを指定できます。次の項では、これらのドメインの設定方法について説明します。

トンネリングされたパケットのデフォルト ドメイン名の定義

セキュリティ アプライアンス は、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPsec クライアントに渡します。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。グループ ポリシーのユーザのデフォルト ドメイン名を指定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを入力します。ドメイン名を削除するには、このコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

value *domain-name* パラメータは、グループのデフォルト ドメイン名を指定します。デフォルト ドメイン名が存在しないことを指定するには、**none** キーワードを入力します。このコマンドにより、デフォルト ドメイン名にヌル値が設定され、デフォルト ドメイン名が拒否されます。また、デフォルトまたは指定されたグループ ポリシーからデフォルト ドメイン名が継承されなくなります。

すべてのデフォルト ドメイン名を削除するには、引数を指定せずに **no default-domain** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **default-domain** コマンドを入力して作成したヌル リストがあればそれも含めて、設定済みのすべてのデフォルト ドメイン名が削除されます。**no** 形式を使用すると、ドメイン名の継承が許可されます。

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

スプリット トンネリング用のドメイン リストの定義

スプリット トンネルを介して解決されるドメインのリストを入力します。グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを入力します。リストを削除するには、このコマンドの **no** 形式を入力します。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルトのグループ ポリシー内に存在するリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承しないようにするには、**none** キーワードを指定して **split-dns** コマンドを入力します。

すべてのスプリット トンネリング ドメイン リストを削除するには、引数を指定せずに **no split-dns** コマンドを入力します。これにより、**none** キーワードを指定して **split-dns** コマンドを発行して作成したヌル リストを含めて、設定済みのすべてのスプリット トンネリング ドメイン リストが削除されます。

パラメータ **value** *domain-name* では、セキュリティ アプライアンスがスプリット トンネルを介して解決するドメイン名を指定します。**none** キーワードは、スプリット DNS リストが存在しないことを示します。また、このキーワードにより、スプリット DNS リストにヌル値が設定されます。そのため、スプリット DNS リストは拒否され、デフォルトまたは指定されたグループ ポリシーのスプリット DNS リストが継承されなくなります。このコマンドの構文は次のとおりです。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

ドメインのリスト内で各エントリを区切るには、スペースを 1 つ入力します。エントリ数に制限はありませんが、ストリング全体の長さは 255 文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。デフォルト ドメイン名がトンネルを介して解決される場合は、そのドメイン名をこのリストに明示的に含める必要があります。

次の例は、FirstGroup という名前のグループ ポリシーで、Domain1、Domain2、Domain3、Domain4 の各ドメインがスプリット トンネリングを介して解決されるように設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

DHCP 代行受信の設定

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、セキュリティ アプライアンスで送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信を使用することにより、Microsoft Windows XP クライアントでセキュリティ アプライアンスとともにスプリット トンネリングを使用できます。セキュリティ アプライアンスは、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows XP 以前の Windows クライアントの場合、DHCP 代行受信によってドメイン名とサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

intercept-dhcp コマンドは、DHCP 代行受信をイネーブルまたはディセーブルにします。このコマンドの構文は次のとおりです。

[no] intercept-dhcp

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

netmask 変数で、トンネル IP アドレスのサブネット マスクを提供します。このコマンドの **no** 形式は、コンフィギュレーションから DHCP 代行受信を削除します。

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

バックアップ サーバ属性の設定

バックアップ サーバを設定します（使用する予定がある場合）。IPsec バックアップ サーバを使用すると、VPN クライアントはプライマリ セキュア ゲートウェイが使用不可の場合も中央サイトに接続することができます。バックアップ サーバを設定すると、セキュリティ アプライアンスでは、IPsec トンネルの確立時にサーバ リストがクライアントへ転送されます。クライアントまたはプライマリ セキュア ゲートウェイのいずれかにバックアップ サーバを設定していない限り、バックアップ サーバは存在しません。

バックアップ サーバは、クライアントまたはプライマリ セキュア ゲートウェイのいずれかに設定します。セキュリティ アプライアンス上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを入力します。

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

バックアップ サーバを削除するには、バックアップ サーバを指定してこのコマンドの **no** 形式を入力します。backup-servers 属性を実行コンフィギュレーションから削除し、backup-servers の値を他のグループ ポリシーから継承できるようにするには、引数を指定せずにこのコマンドの **no** 形式を入力します。

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

clear-client-config キーワードは、クライアントでバックアップ サーバを使用しないことを指定します。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。

keep-client-config キーワードは、セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。これがデフォルトです。

server1 server 2....server10 パラメータ リストは、プライマリのセキュリティ アプライアンスが使用不可の場合に VPN クライアントが使用するサーバをプライオリティ順にスペースで区切ったリストです。このリストには、サーバを IP アドレスまたはホスト名で指定します。このリストの長さは 500 文字までで、格納できるエントリは最大 10 個までです。

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

アドレス プールの設定

リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを設定するには、グループ ポリシー属性コンフィギュレーション モードで **address-pools** コマンドを入力します。

```
hostname(config-group-policy)# address-pools value address_pool1 [...address_pool6]
hostname(config-group-policy)#
```

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

グループ ポリシーからこの属性を削除して、グループ ポリシーの別のソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

```
hostname(config-group-policy)# no address-pools value address_pool1 [...address_pool6]
hostname(config-group-policy)#
```

address-pools none コマンドは、ポリシーの別のソース（DefaultGrpPolicy など）からこの属性を継承することをディセーブルにします。

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

no address pools none コマンドは、**address-pools none** コマンドをコンフィギュレーションから削除して、デフォルト値（継承の許可）に戻します。

```
hostname(config-group-policy)# no address-pools none
hostname(config-group-policy)#
```

このコマンドの構文要素は次のとおりです。

- *address_pool* : **ip local pool** コマンドで設定されているアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
- **none** : アドレス プールを何も設定していないことを示し、グループ ポリシーの他のソースからの継承をディセーブルにします。
- **value** : アドレスの割り当てに使用するアドレス プールのリストを 6 個まで指定します。

次の例（config-general コンフィギュレーション モードで入力）は、GroupPolicy1 でリモート クライアントにアドレスを割り当てるのに使用するアドレス プールのリストとして pool1 と pool20 を設定しています。

```
hostname(config)# ip local pool pool 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool1 pool20
hostname(config-group-policy)#
```

ファイアウォール ポリシーの設定

*ファイアウォール*は、データの個々の着信パケットと発信パケットをそれぞれ検査して、パケットを許可するかドロップするかどうかを決定することにより、コンピュータをインターネットから分離して保護します。ファイアウォールは、グループのリモート ユーザがスプリット トンネリングを設定している場合、セキュリティの向上をもたらします。この場合ファイアウォールにより、インターネットまたはユーザのローカル LAN を経由する不正侵入からユーザの PC が保護され、ひいては企業ネットワークも保護されます。VPN クライアントを使用してセキュリティ アプライアンスに接続しているリモー

ト ユーザは、適切なファイアウォール オプションを選択できます。

グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用して、セキュリティ アプライアンスが IKE トンネル ネゴシエーション中に VPN クライアントに配信するパーソナル ファイアウォール ポリシーを設定します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を入力します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを入力します。このコマンドにより、**none** キーワードを指定して **client-firewall** コマンドを入力して作成したヌル ポリシーがあればそれも含めて、設定済みのすべてのファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがこのようなファイアウォール ポリシーを継承しないようにするには、**none** キーワードを指定して **client-firewall** コマンドを入力します。

[Add or Edit Group Policy] ウィンドウ、[Client Firewall] タブでは、追加または変更するグループ ポリシーに対して VPN クライアントのファイアウォール設定を指定できます。

（注） これらのファイアウォール機能を使用できるのは、Microsoft Windows を実行する VPN クライアントだけです。現在、ハードウェア クライアントまたは他（Windows 以外）のソフトウェア クライアントでは、これらの機能は使用できません。

最初のシナリオでは、リモート ユーザの PC 上にパーソナル ファイアウォールがインストールされています。VPN クライアントは、ローカル ファイアウォールで定義されているファイアウォール ポリシーを適用し、そのファイアウォールが実行されていることを確認するためにモニタします。ファイアウォールの実行が停止すると、VPN クライアントはセキュリティ アプライアンスへの通信をドロップします。（このファイアウォール適用メカニズムは *Are You There（AYT）* と呼ばれます。VPN クライアントが定期的に「are you there?」メッセージを送信することによってファイアウォールをモニタするからです。応答が返されない場合、VPN クライアントは、ファイアウォールがダウンしたためセキュリティ アプライアンスへの接続が終了したことを認識します）。ネットワーク管理者がこれらの PC ファイアウォールを独自に設定する場合もありますが、この方法を使用すれば、ユーザは各自の設定をカスタマイズできます。

第 2 のシナリオでは、VPN クライアント PC のパーソナル ファイアウォールに中央集中型ファイアウォール ポリシーを適用することが選択されることがあります。一般的な例としては、スプリット トンネリングを使用してグループのリモート PC へのインターネット トラフィックをブロックすることが挙げられます。この方法は、トンネルが確立されている間、インターネット経由の侵入から PC を保護するので、中央サイトも保護されます。このファイアウォールのシナリオは、*プッシュ ポリシー* または *Central Protection Policy（CPP）* と呼ばれます。セキュリティ アプライアンスでは、VPN クライアントに適用するトラフィック管理ルールのセットを作成し、これらのルールをフィルタに関連付けて、そのフィルタをファイアウォール ポリシーに指定します。セキュリティ アプライアンスは、このポリシーを VPN クライアントまで配信します。その後、VPN クライアントはポリシーをローカル ファイアウォールに渡し、そこでポリシーが適用されます。

次のコマンドを入力して、適切なクライアント ファイアウォールのパラメータを設定します。このコマンドに設定できるインスタンスは 1 つだけです。この一連のコマンドの後に記載された表 3-1 で、これらのコマンドの構文要素について説明します。

Cisco 統合ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated acl-in ACL
acl-out ACL
```

Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

ファイアウォールなし

```
hostname(config-group-policy)# client-firewall none
```

カスタム ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

Zone Labs ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

（注） ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm policy {AYT
| CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarmorpro policy
{AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out
ACL}
```

Sygate Personal ファイアウォール

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

Network Ice、Black Ice ファイアウォール：

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

表 3-1　client-firewall コマンドのキーワードと変数

パラメータ	説明
acl-in *ACL*	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out *ACL*	クライアントが発信トラフィックに使用するポリシーを指定します。

表 3-1　client-firewall コマンドのキーワードと変数 （続き）

AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。セキュリティ アプライアンスはファイアウォールが実行されていることを確認します。「Are You There?」と表示され、応答がない場合は、セキュリティ アプライアンスによりトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアントのファイアウォール ポリシーのソースとして Policy Pushed を指定します。
custom	カスタム ファイアウォール タイプを指定します。
description *string*	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーにヌル値を設定して、ファイアウォール ポリシーを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

クライアント アクセス ルールの設定

グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用して、セキュリティ アプライアンス を介して IPsec で接続できるリモート アクセス クライアントのタイプとバージョンを制限するルールを設定します。次のガイドラインに従ってルールを作成します。

- ルールを定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。

- クライアントがいずれのルールにも一致しない場合、セキュリティ アプライアンスは接続を拒否します。拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。定義しない場合、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらでも、タイプとバージョンは **show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。
- ***** 文字はワイルドカードです。ワイルドカードは各ルールで複数回入力することができます。たとえば、**client-access rule 3 deny type * version 3.*** では、バージョン 3.x のソフトウェア リリースを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールが作成されます。
- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプまたはバージョン（あるいはその両方）を送信しないクライアントには、n/a を入力できます。

ルールを削除するには、このコマンドの **no** 形式を入力します。このコマンドは、次のコマンドと同等です。

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

すべてのルールを削除するには、引数を指定せずに **no client-access-rule** コマンドを入力します。これにより、**none** キーワードを指定して **client-access-rule** コマンドを発行して作成したヌル ルールがあればそれも含めて、設定済みのすべてのルールが削除されます。

デフォルトでは、アクセス ルールはありません。クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。

ユーザがクライアント アクセス ルールを継承しないようにするには、**none** キーワードを指定して **client-access-rule** コマンドを入力します。このコマンドの結果、すべてのタイプとバージョンのクライアントが接続できるようになります。

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type
version {version | none}

hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type
version version]
```

表 3-2 に、これらのコマンドのキーワードとパラメータの意味を示します。

表 3-2　client-access rule コマンドのキーワードと変数

パラメータ	説明
deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。client-access-rule をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン（またはこのいずれか）に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、セキュリティ アプライアンスはそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、**show vpn-sessiondb remote** で表示される内容と完全に一致している必要があります。ただし、ワイルドカードとして * 文字を入力できます。

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、バージョン 4.x のソフトウェアを実行する Cisco VPN クライアントを許可し、すべての Windows NT クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client" version 4.*
```

（注）「type」フィールドは、任意の値が許可される自由形式の文字列ですが、その値は、接続時にクライアントからセキュリティ アプライアンスに送信される固定値と一致している必要があります。

例：CLI を使用した VPN クライアントに関するセキュリティ アプライアンスの設定

次は、VPN クライアント接続に関するセキュリティ アプライアンスの設定方法の一例を示したものです。特に VPN クライアントと関連のあるコマンドは太字で強調してあります。

```
group-policy Engineering attributes
        vpn-tunnel-protocol IPsec
      configure terminal
      tunnel-group TestTunnelGroup1 general-attributes
        accounting-server-group ACS-1
        default-group-policy Engineering
        strip-group
        strip-realm
```

```
  no dhcp-server  209.165.200.200
  dhcp-server  209.165.200.201
  override-account-disable
  password-management  password-expire-in-days 0
  authentication-server-group (inside) ACS-1 LOCAL
  authentication-server-group  ACS-1 LOCAL
  authorization-server-group (inside) ACS-1
  authorization-server-group  LOCAL
  address-pool (test) Engineering
tunnel-group TestTunnelGroup1 ipsec-attributes
  chain
  pre-shared-key **********
  isakmp keepalive disable
  trust-point ASDM_TrustPoint11
  client-update type Windows url http://www.cisco.com rev-nums 4.6,4.7,4.8,4.9,5.0
  client-update type vpn3002 url tftp://www.cisco.com rev-nums 4.6
 client-update type asa5505 component image url https://www.cisco.com rev-nums 7.2
  isakmp ikev1-user-authentication (inside) hybrid
tunnel-group TestTunnelGroup1 ppp-attributes
  authentication ms-chap-v2
vpn-addr-assign local reuse-delay 5
group-delimiter #
```