CHAPTER 4

VPN 3000 シリーズ Concentrator における VPN クライアントの設定

この章では、Cisco VPN 3000 シリーズ Concentrator で VPN クライアント パラメータを設定する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。CLI を使用した設定に関する詳細は、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』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。

この章の主な内容は、次のとおりです。

VPN 3000 シリーズ Concentrator における VPN クライアントの設定

『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「User Management」の章を熟読することを推奨します。この「User Management」の章では、IPsec トンネルを介して接続するリモート ユーザの設定方法を詳しく説明し、またクライアント バナーの設定、ファイアウォール、スプリット トンネリングなどの機能の使用方法についても説明しています。

ここでは、次の作業について説明します。

クイック コンフィギュレーションの完了

クイック コンフィギュレーションのステップについては、『*Cisco VPN 3000 Series Concentrator Getting Started*』またはクイック コンフィギュレーションのオンライン ヘルプを参照してください。

必ず次の作業を実行してください。

- イーサネット インターフェイス 1 と 2（プライベートとパブリック）の両方に適切な IP アドレスとフィルタを設定し、これらのインターフェイスをイネーブルにする。
- DNS サーバとデフォルト ゲートウェイを設定する。
- IPsec をトンネリング プロトコルの 1 つとしてイネーブルにする（デフォルト）。
- IPsec グループのグループ名とパスワードを入力する。
- ユーザ IP アドレスを割り当てるための方法を 1 つ以上設定する。

（注） スプリット トンネルまたは除外するトンネルを設定する場合は、適切なマスクがアドレス プール、または割り当て済みの IP アドレスに割り当てられていることを確認してください。デフォルトでは、クラスフル マスクが仮想アダプタ対応クライアントに適用されますが、このデフォルト マスクによりクライアントは、意図しないトラフィックをトンネリングするおそれがあります。

- グループおよびユーザ認証用の認証サーバを設定する。説明では、両方の認証に内部サーバを使用することを想定していますが、外部サーバを設定することもできます。
- 設定を保存する。

IPsec グループの作成

クイック コンフィギュレーションの間に、IPsec グループを自動的に作成できます。IPsec グループを追加または変更する場合は、この項の手順を実行します。

グループ設定に関する詳細については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「User Management」を参照してください。

IPsec グループを作成する前に、基本グループ属性を以下のように設定することもできます。

- ASDM の場合は、[ASDM Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles] ウィンドウを確認します。
- VPN 3000 Concentrator の場合は、[Configuration | User Management | Base Group] 画面を確認します。

上記ウィンドウの IPsec Connection Parameters（ASDM）または General Parameters および IPsec Parameters（VPN 3000 Concentrator）を慎重に確認することを推奨します。

外部ユーザ認証を使用する場合は、デフォルト属性または基本グループ属性が特に重要です。その理由は、外部サーバで提供されていないすべての属性が、これらの 2 つの属性によって管理されるからです。

VPN クライアントでは、セキュア トンネルを作成および使用するために IPsec プロトコルを使用します。IPsec の認証は、2 段階で実行します。つまり、最初にグループに対して認証を実行し、続いてユーザに対して認証を実行します。次の説明では、グループ認証とユーザ認証の両方に VPN 3000 Concentrator の内部認証サーバを使用することを前提としています。

[Configuration | User Management | Groups | Add] 画面を使用して、IPsec グループを作成する手順は、次のとおりです。

ステップ 1　[Identity] タブで、グループ名とパスワードを入力します。VPN クライアント ユーザが接続エントリを設定し、VPN クライアント経由で接続するには、このグループ名とパスワードが必要です。ご使用のプラットフォームの『*VPN Client User Guide*』の第 2 章の「Gathering Information You Need」を参照してください。

ステップ 2　次に、認証方式を選択します。Type パラメータにより、グループ認証方式（Internal または External）が決定されます。内部グループは、VPN Concentrator に設定されます。External を選択する場合は、適切なグループ属性を認証および表示するように外部 RADIUS サーバを設定する必要があります。

ステップ 3　[General] タブ | Tunneling Protocols で、[IPsec] がオンになっていることを確認してください。

ステップ 4　[IPsec] タブ | [IPsec SA] で、[**ESP-3DES-MD5**] を選択して、トリプル DES 認証を要求するようにします。その代わりに、**ESP-DES-MD5** を選択することもできます。ESP-DES-MD5 では、DES 認証を使用し、最低限のセキュリティを確保します。または、AES を使用するために、**ESP-AES128-SHA** などの AES プロトコルのいずれかを選択してください。AES が最もセキュアです。

（注）　セキュリティ アソシエーション（SA）を作成またはカスタマイズするには、[Configuration | Policy Management | Traffic Management | Security Associations] 画面を表示します。

ステップ 5　[IPsec] > [Authentication] で、グループのメンバーに対して使用する方式（Internal または RADIUS など）を選択します。None または Internal 以外の認証方式を選択した場合は、必ず外部認証サーバを正しく設定し、VPN クライアントのインストールに関する適切な情報をユーザに提供してください。

ステップ 6　ユーザがログインするたびにパスワードの入力を要求するには、[Client Config] タブにある [Allow Password Storage on the Client] をオンに*しない*ことを推奨します。このパラメータをオンにしないことで、セキュリティが向上します。

ステップ 7　グループを追加するには、[Add] をクリックし、設定を保存します。

VPN クライアント ユーザ プロファイルの作成

グループ内における VPN クライアント ユーザの設定に関する詳細については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「User Management」を参照してください。

VPN クライアント ユーザを設定するには、[Configuration | User Management | Users | Add or Modify] 画面を使用して、次の手順を実行します。

ステップ 1　[User Name]、[Password]、および [Verify Password] に入力します。VPN クライアント ユーザは、VPN Concentrator に接続する際に認証用のユーザ名とパスワードを入力する必要があります。ご使用のプラットフォームに該当する『*VPN Client User Guide*』の第 2 章「Gathering Information You Need」を参照してください。

（注）　リリース 4.6.04.x 以降の VPN クライアントでは、最大 128 文字の事前共有パスワードを使用できます。ただし、VPN 3000 Concentrator では 32 文字以下に制限されます。

ステップ 2　[Group] で、「IPsec グループの作成」で設定したグループ名を選択します。

ステップ 3　[General] および [IPsec] の他の属性を慎重に確認し、設定します。ユーザを追加する場合は、[Inherit?] チェックボックスがベースグループ属性を参照していることに注意してください。ユーザを変更すると、このチェックボックスはユーザの割り当て済みのグループ属性を参照します。

ステップ 4　[Add] または [Apply] をクリックし、設定を保存します。

デジタル証明書による認証用の VPN クライアント ユーザの設定

デジタル証明書を使用した IPsec クライアント接続用に VPN 3000 Concentrator を設定するには、次の手順を実行します。

- IKE SA をアクティブにします。
- VPN 3000 Concentrator の ID 証明書を使用するように、セキュリティ アソシエーション（SA）を設定します。

- 証明書を使用して接続するクライアントに対して、新しいグループを作成します。
- VPN クライアント ユーザを新しいグループに追加します。
- 詳細については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の以下の項を参照してください。
  - IKE プロポーザルの設定については、「Tunneling Protocols」を参照してください。
  - SA の設定については、「Policy Management」を参照してください。
  - グループおよびユーザの設定については、「User Management」を参照してください。

次のステップを実行します。

ステップ 1　[Configuration | System | Tunneling Protocols | IPsec | IKE Proposal] 画面を使用して、証明書の IKE プロポーザルを次のように起動します。

a. Cisco VPN Client-3DES-MD5-RSA-DH5、Cisco VPN Client-3DES-SHA-DSA-DH5、または Cisco VPN Client-AES128-SHA などの IKE プロトコルのいずれかをアクティブにします。

（注） AES を使用するには、AES プロポーザルをリストの先頭に移動します。AES を使用するには、VPN クライアント ソフトウェアのリリース 3.6 以上を実行する必要があります。

b. 標準的なプロポーザルのいずれも変更しない場合は、アクティブなプロポーザルをコピーし、これに新しい名前を付けます。たとえば、Cisco VPN Client-3DES-MD5-RSA-DH5 をコピーして、これに「IKE-Proposal for digital certificate use」という名前を付けます。

c. [Security Associations] をクリックして、次のステップに進みます。

ステップ 2　[Configuration | Policy Management | Traffic Management | Security Associations] 画面を使用して、新しい SA を作成します。[IKE Proposals] 画面の [Security Associations] リンクを使用できます。

a. 新しい SA を追加します。たとえば、これに「Security association for digital certificate use」という名前を付けます。

b. [Digital Certificates] パラメータを変更して、VPN 3000 Concentrator のデジタル証明書を指定します。これは、変更する必要がある唯一のフィールドです。

ステップ 3　[Configuration | User Management | Groups | Add or Modify] 画面を使用して、デジタル証明書を使用するグループを次の手順で設定します。

a. [Organizational Unit] を使用してグループを設定するには、[Identity] タブで、このグループの証明書の [OU] フィールドと同じグループ名を入力します。たとえば、VPN クライアント証明書の OU が「Finance」である場合、グループ名として「Finance」と入力します。OU は ASN.1 Distinguished Name（DN; 識別名）のフィールドです。パスワードを入力し、このパスワードを確認してください。
または
証明書グループ照合のポリシーを設定することもできます。この方法を使用するには、[Configuration | Policy Management | Certificate Group Matching | Policy] に進みます。ルール作成の手順については、『*VPN 3000 Series Concentrator Reference I: Configuration*』の該当する項またはオンライン ヘルプを参照してください。

b. [IPsec] タブ > [IPsec SA] で、ステップ 2 で作成した IPsec SA（たとえば、「Security association for digital certificate use」）を選択します。

c. [IPsec] タブ > [Authentication] で、ユーザ認証に使用する方法（たとえば、Internal）を選択します。RADIUS などの外部認証方法を選択する場合は、必ず外部認証サーバを正しく設定し、『*VPN Client User Guide*』の第 2 章に記載されている該当プラットフォームの「Gathering the Information You Need」項に従ってユーザに適切なエントリを指定してください。

d. [Add] または [Apply] をクリックし、設定を保存します。

ステップ 4　[Configuration | User Management | Users | Add or Modify | Identity] 画面を使用して、次の手順で VPN クライアント ユーザをデジタル証明書に設定します。

a. グループ名として、ステップ 3 でグループ パラメータとして設定したグループを入力します。ここでも例として、「Finance」と入力します。

b. [Add] または [Apply] をクリックし、設定を保存します。

- 次の新しい証明書機能では、ユーザが手動で選択しなくても証明書がプロファイルに動的にマッピングされます。
  - 証明書識別名照合（Windows および Linux）
  - 証明書キーの使用状況（Windows、Linux、および Mac）
  - 証明書フォールスルー（Windows および Linux）

  次の項では、これらの機能について説明します。

証明書識別名の照合

Windows プラットフォームおよび Linux プラットフォームでは、プロファイル キーワードである CertMatchDN パラメータを使用して、照合するワイルドカード文字列を指定し、接続の試行時に識別名を基に所定の証明書ストアから特定の証明書を選択します。ワイルドカード文字列が複数の証明書と一致した場合は、そのワイルドカード文字列と最初に一致した証明書が選択されます。このパラメータの値は擬似正規表現で、その書式は VerifyCertDN プロファイル キーワードの書式とまったく同じです。

ワイルドカード文字列に使用できるキーワードは次のとおりです。

- "CN" SubjectCommonName
- "SN" SubjectSurName
- "GN" SubjectGivenName
- "N" SubjectUnstructName
- "I" SubjectInitials
- "GENQ" SubjectGenQualifier
- "DNQ" SubjectDnQualifier
- "C" SubjectCountry
- "L" SubjectCity
- "SP" SubjectState
- "ST" SubjectState
- "O" SubjectCompany
- "OU" SubjectDept
- "T" SubjectTitle
- "EA" SubjectEmailAddr

- "ISSUER-CN" IssuerCommonName

- "ISSUER-SN" IssuerSurName
- "ISSUER-GN" IssuerGivenName
- "ISSUER-N" IssuerUnstructName
- "ISSUER-I" IssuerInitials
- "ISSUER-GENQ" IssuerGenQualifier
- "ISSUER-DNQ" IssuerDnQualifier
- "ISSUER-C" IssuerCountry
- "ISSUER-L" IssuerCity
- "ISSUER-SP" IssuerState
- "ISSUER-ST" IssuerState
- "ISSUER-O" IssuerCompany
- "ISSUER-OU" IssuerDept
- "ISSUER-T" IssuerTitle
- "ISSUER-EA" IssuerEmailAddr

例：

```
CertMatchDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland"
CN="ID Cert"--Specifies an exact match on the CN.
OU*"Cisco"--Specifies any OU that contains the string "Cisco".
ISSUER-CN!"Entrust"--Specifies that the Issuer CN must not equal "Entrust".
ISSUER-OU!*"wonderland"--Specifies that the Issuer OU must not contain "wonderland".
```

証明書キーの用途

Windows、Linux、および Mac の各プラットフォームでは、vpnent.ini 内の [Main] キーワード配下の CertificateKeyUsage により、全ストアにある証明書のうち使用できるものが、証明書キーの用途に関するパラメータとして Digital Signature または Non-Repudiation が指定されている証明書に制限されます。

クライアントの起動時に「CertificateKeyUsage=1」である場合、[Certificates] タブにはキーの用途が適切な証明書のみ表示されます。さらに、キーの用途が適切でない証明書を使用するようプロファイルが設定されている場合は、証明書が見つからないという内容のエラーが表示されます。

このキーワードのデフォルトは「CertificateKeyUsage=0」で、使用可能なすべての証明書を選択して使用することができます。

このキーワードは、CertMatchDN などその他のあらゆる証明書一致基準に優先します。

証明書キーの用途の照合

Windows および Linux プラットフォームでは、証明書キーの使用状況の照合機能を使用すると、証明書のプロファイルを [Key Usage] フィールド、[DN] フィールドおよび [Extended Key Usage] フィールドに基づいて選択できます。プロファイル キーワードである CertMatchKU を指定すると、vpnent.ini キーワード「CertificateKeyUsage」が上書きされます。

例：

```
CertMatchKU=0,3,4,5
```

```
DIGITAL_SIGNATURE  8
NON_REPUDIATION    7
KEY_ENCIPHERMENT   6
DATA_ENCIPHERMENT  5
KEY_AGREEMENT      4
KEY_CERT_SIGN      3
CRL_SIGN           2
ENCIPHER_ONLY      1
DECIPHER_ONLY      0
```

証明書が [CertMatchKU] フィールドの使用状況のいずれかに一致すると、次の基準に渡されます。一致しない場合、証明書は選択されません。

次のようなプロファイルに対して、キーの用途以外は同一である 2 つの証明書が使用可能である場合は、Non-Repudiation が指定された証明書のみ選択されます。

```
[Main]
Host=1.2.3.4
AuthType=3
CertStore=2
CertName=myMultipleCerts
CertMatchKU=7
!CertSubjectName=
!CertSerialHash=
```

拡張証明書キーの用途の照合

プロファイル キーワード パラメータ CertMatchEKU は、VPN クライアントで受け入れる拡張キー使用状況フィールドのリストを指定します。このプロファイル キーワードを指定すると、接続試行中に VPN クライアントは、（証明書ストアに関係なく）拡張キーの使用状況フィールドがプロファイル キーワードで指定されたフィールドと一致する証明書だけを参照します。つまり、このプロファイル キーワードを指定すると、どのような証明書であっても、プロファイル キーワードで指定した [Extended Key Usage] フィールドの少なくとも 1 つが証明書の [Extended key Usage] フィールドに存在する必要があります。

このキーワードは、接続の試行に対してのみ適用され、証明書に関するその他の動作（証明書のリスト表示、証明書の内容表示など）には適用されません。このキーワードは、あらゆる基準による証明書選択（CertSerialHash、CertMatchDN、CertSubjectName、CertName など）に適用されます。このはーワードの値は、キーの拡張用途 OID 文字列で構成されるカンマ区切りのリストです。カスタムのキーの拡張用途文字列は、1.3.6.1.5.5.7.3.n という書式にする必要があります。n は任意の数字です。

例：

```
CertMatchEKU=1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1
```

それぞれの説明は次のとおりです。

1.3.6.1.5.5.7.3.2：クライアント認証

1.3.6.1.5.5.7.3.1：サーバ認証

証明書が見つからない場合

特定の接続試行で、以下のキーワードの 1 つ以上を使用して証明書を（優先度順に）選択できます。

1. CertSerialHash
2. CertMatchDN
3. CertSubjectName

4. CertName

VPN クライアントが上記の証明書キーワードをすべて使用しても指定の証明書ストアで証明書を検出できない場合、接続試行は失敗します。

この場合の処理は暗黙的に行われ、それに関連付けられるプロファイル キーワードはありません。

以下にプロファイルのサンプルを示します。

```
[Main]
Host=10.10.10.10
AuthType=3
CertStore=2
!UserName=
!UserPassword=
CertMatchDN=issuer-ou*"vpn group",ea*"Cisco.com"
!CertSerialHash=
```

このプロファイルに一致するのは、キーの用途が「Non-Repudiation」であり、かつキーの拡張用途がクライアント認証またはサーバ認証の*いずれか*である証明書に限ります。Issuer-ou フィールドには "vpn group" を指定することが*必要*であり、ユーザ証明書の電子メール アドレスには "cisco.com"（大文字と小文字は区別される）が指定されている*必要*があります。

Windows 環境の場合（Linux および Mac 用の VPN クライアントではスマート カードをサポートしていない）、前記のシナリオでは共用のワークステーションからでもスマート カード証明書に基づいてユーザを接続することができます。ユーザは移動した先でスマート カードを挿入し、[Connect] をクリックします。この汎用プロファイルを使用すると、（クライアントのリスタートやプロファイルの修正を行うことなく）カード上で適切な証明書が検索され、ユーザに対してそれぞれの証明書パスワード、ユーザ名、およびパスワードに関するプロンプトが表示されます。また、ユーザ名を使用することなく接続し証明書のみを使用して認証が行われるよう、セキュア ゲートウェイを設定することもできます。

（注） プロファイル内で文字「!」を使用すると、接続間で以前のユーザ情報が維持されないようにすることができます。

証明書照合では、使用可能な証明書のうち証明書照合に対して設定されたルールに最初に適合したものが一致対象となります。ただしその有効性は問われないため、接続失敗の原因になることがあります。有効な証明書が使用可能な場合に、失効した証明書が選択されないようにするため、Windows 用の VPN クライアントでは現在、証明書ストア内にある無効な証明書および失効した証明書は無視されるようになっています。（CSCsd38373、CSCsd38360）。

CertSerialHash の使用に関する重要な注意事項

以下に示すのは、DN などの一致基準を使用して証明書を検索する例です。

```
CertMatchDN=CN*"User"
!CertSerialHash=
```

この場合、CertSerialHash キーワードは直前に感嘆符（!）があることにより読み取り専用フィールドとなっているため、クライアントでは連続ハッシュ値を更新できません。正しい連続ハッシュがないと、クライアントではウォッチ タイマーを作成してスマート カードが存在するかどうかを検証することができません。

「!CertSerialHash=」がない場合、クライアントではストア内の証明書により証明書ハッシュが更新され、次の行がプロファイルに追加されます。

```
CertSerialHash=...03CF...
```

プロファイル内に「CertSerialHash=0102...xyz」などの連続ハッシュ値がすでに存在する場合、DN に一致する別の証明書の入った別のスマートカードを使用すると、スマートカード ウォッチも開始され、IPsec では CertSerialHash パラメータの連続ハッシュ値が、使用している証明書の連続ハッシュ値に更新されます。

（注）　この状況では、VPN クライアントで連続ハッシュ値を目的の証明書に合わせて更新できるようにする必要があるため、「CertSerialHash=」の前に「!」を挿入*しない*ことが重要です。

デジタル証明書を使用した接続

デジタル証明書を使用して VPN クライアント接続エントリを作成するためには、あらかじめ公開キーインフラストラクチャ（PKI）に登録し、認証局（CA）から承認を受けたうえで、1 つまたは複数の証明書を VPN クライアント システム上にインストールしておくことが必要です。これらの作業を行っていない場合は、デジタル証明書を取得する必要があります。Certificate Manager 機能を使用すると直接 PKI に登録してデジタル証明書を取得できるほか、Entrust Entelligence を介して Entrust プロファイルを取得することもできます。現時点でテスト済みの PKI は次のとおりです。

- Baltimore Technologies の UniCERT（www.baltimoretechnologies.com）
- Entrust Technologies の Entrust PKI™ 5.0（www.entrust.com）
- Versign（www.verisign.com）
- RSA KEON 5.7 および 6.0
- Microsoft Certificate Services 2.0
- Cisco Certificate Store

このリストのうちカッコの中に記した Web サイトには、各 PKI から入手できるデジタル証明書についての情報が記載されています。

Windows の VPN クライアントのファイアウォール ポリシーの設定

セキュリティ レベルを向上させるために、VPN クライアントは、インターネット上のトラフィックに対して、サポートされているファイアウォールの動作を適用するか、プッシュされたステートフル ファイアウォール ポリシーを受け取ることができます。この項は、次の内容で構成されています。

- ファイアウォールの VPN クライアントとの連携動作。
- VPN クライアントがインターネット トラフィックに適用できるパーソナル ファイアウォール製品のリスト。
- VPN Concentrator 上で、VPN クライアントが実行するステートフル ファイアウォール ポリシーの設定方法。

パーソナル クライアント ファイアウォールの使用に関する概要

この項では、ネットワーク管理者が、ポリシー情報を伝達するセキュア ゲートウェイとして機能する VPN 3000 Concentrator のパーソナル ファイアウォール機能を制御する方法から、Windows プラットフォーム上で VPN クライアントを実行する方法にいたるまでを要約します。

オプション設定と必須設定

VPN Concentrator では、指定されたファイアウォール設定を使用する、またはこの設定をオプションにするように VPN クライアントに要求できます。指定のファイアウォール設定をオプションにすると、VPN クライアント ユーザは、クライアント PC に希望のファイアウォールをインストールすることができます。VPN クライアントは、接続を試行すると、クライアント PC にインストールされているファイアウォールについて VPN Concentrator に通知します。VPN Concentrator は、VPN クライアントが使用しなければならないファイアウォールに関する情報を返します。ファイアウォール設定がオプションの場合、VPN Concentrator は、不一致があっても、VPN クライアントによるトンネル確立を許可することを VPN クライアントに通知します。オプション機能により、VPN クライアントのネットワーク管理者は、トンネリングされた接続を維持しながら、必要なファイアウォールを取得し、インストールできます。

ステートフル ファイアウォール（常時オン）

VPN クライアント設定オプション [Stateful Firewall (Always On)] は、VPN クライアント上でイネーブルになっています。この設定オプションはネゴシエーションされません。VPN Concentrator からのポリシーも制御されません。VPN クライアント ユーザは、VPN クライアントの [Options] メニューでこのオプションをイネーブルにするか、VPN クライアントがアクティブのときに [VPN Client] アイコンを右クリックし、オプションを選択してイネーブルにします。

この機能がイネーブルになっていると、VPN 接続が有効かどうかにかかわらず、すべてのネットワークからの着信セッションが許可されなくなります。また、ファイアウォールもトンネリングされたトラフィックと、トンネリングされていないトラフィックの両方に対してアクティブになります。この機能をイネーブルにしているユーザは、自身の PC でサーバを実行できず、このようなユーザのシステムも ping 要求に応答できません。着信トラフィックが許可されない場合の 2 つの例外があります。1 つは DHCP です。DHCP では、あるポートから DHCP サーバに要求を送信し、DHCP からの応答を別のポートを経由して受信します。DHCP の場合、ステートフル ファイアウォールは着信トラフィックを許可します。もう 1 つは ESP（VPN データ）です。ステートフル ファイアウォールでは、セキュアゲートウェイからの ESP トラフィックを許可します。ESP でのルールは、パケット フィルタであり、セッションベースのフィルタではないからです。

ステートフル ファイアウォール（常時オン）は、VPN クライアントの最も基本的なファイアウォールであり、最高レベルのセキュリティを確保します。ただし、このファイアウォールは、ほとんどすべて着信のトラフィックをブロックしますが、発信トラフィックを制限できないため、最も柔軟性に欠けます。

（注）　Always On パーソナル ファイアウォールは、内部（トンネリングされた）ネットワークからの着信アクセスを許可し、内部のアプリケーションが適切に動作することを保証しながら、トンネリングされていないトラフィックの保護を強化します。

Cisco Integrated Client

Windows プラットフォーム上の VPN クライアントには、Zone Labs のテクノロジーを採用したステートフル ファイアウォールが組み込まれています。このファイアウォールは、ステートフル ファイアウォール（常時オン）機能と Centralized Protection Policy（「Centralized Protection Policy（CPP）」を参照）の両方に使用されます。このファイアウォールは VPN クライアントユーザに透過的で、「Cisco 統合クライアント ファイアウォール」または CIC と呼ばれます。「Always On」オプションを選択すると、VPN クライアント ユーザは、基本ファイアウォール保護を常に有効にしておくことができます。CPP では、管理者はスプリット トンネリング動作中に着信 / 発信インターネット トラフィックに適用するルールを定義できます。Tunnel Everything では、すべてのトラフィックがトンネルを経由して戻るように強制されるため、Tunnel Everything には CPP は使用されません。

Centralized Protection Policy（CPP）

Centralized Protection Policy（CPP）は、ファイアウォール *プッシュ ポリシー*として知られています。これにより、ネットワーク管理者は、VPN クライアントが VPN Concentrator とトンネル通信するときのインターネット トラフィックの許可または破棄に関する一連のルールを定義できます。ネットワーク管理者が VPN Concentrator 上でこのポリシーを定義すると、接続ネゴシエーション中にこのポリシーが VPN クライアントに送信されます。VPN クライアントは Cisco Integrated Client にこのポリシーを渡し、そこでこのポリシーが適用されます。クライアント ユーザがすでに「Always On」オプションを選択している場合は、トンネル確立中に、より制約の多いルールがインターネット トラフィックに適用されます。

CIC には、ステートフル ファイアウォール モジュールが組み込まれているため、ほとんどの設定ですべての着信トラフィックがブロックされ、すべての発信トラフィック、あるいは特定の TCP ポートと UDP 発信ポートからの発信トラフィックが許可されます。Cisco Integrated Client、Zone Alarm、および Zone Alarm Pro の各ファイアウォールでは、ファイアウォール ルールを割り当てることができます。CPP ルールはスプリット トンネリングの間に有効になり、発信接続に関連付けられていない限り、サーバが実行されるのを防いで、すべての着信接続をブロックすることで、VPN クライアント PC をインターネット攻撃から保護できます。

CPP を使用すると、許可するポートおよびプロトコルを細かく調整できるため、CPP はステートフル ファイアウォール（常時オン）機能よりも柔軟性に優れています。

リモート PC 上に設定されたポリシー：パーソナル ファイアウォールの強制

ネットワーク管理者は、VPN クライアントと同じ PC にインストールされているパーソナル ファイアウォールに、CPP の代わりにポリシーを定義できます。この方法では、ファイアウォールがすでに PC 上で設定され、使用されている場合に適しています。また、VPN クライアントはパーソナル ファイアウォールを 30 秒ごとにポーリングして、パーソナル ファイアウォールの動作状況を確認します。パーソナル ファイアウォールが動作していなければ、VPN Concentrator へのセキュア接続を終了します。この場合、VPN Concentrator はファイアウォール ポリシーを定義しません。VPN クライアントとファイアウォールとの唯一の接点は、ファイアウォールが動作しているかそうかを確認するためにポーリングすることです。これは Are You There（AYT）として知られている機能です。

現在、VPN クライアントは次のパーソナル ファイアウォールをサポートしています。

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal ファイアウォール
- Sygate Personal Pro ファイアウォール
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

Zone Labs Integrity エージェントおよび Integrity サーバ（IA/IS）

Zone Labs Integrity ソリューションは、Windows プラットフォームのリモート PC を保護します。この機能は、次の 4 つのコンポーネントで構成されるクライアント/サーバ ソリューションです。

- Integrity Server（IS）：組織の中枢ネットワークに配置されます。IS は、リモートの VPN クライアント PC 上のファイアウォールに関するポリシーを保持します。ネットワーク管理者が IS にポリシーを定義すると、IS は VPN Concentrator によって確立されたセキュア トンネルを介して、ポ

リシーをリモート PC 上の Integrity Agent（IA）にダウンロードします。IS は、確実にポリシーを実行するために、PC をモニタします。また、IS は VPN Concentrator と通信して、接続の確立と終了、セッションおよびユーザ情報の交換、ステータス情報の報告を行います。

- Integrity Agent（IA）：リモート PC 上で IS から受け取った保護ポリシーを実行し、IS と通信してポリシーおよびステータス情報を交換します。また、IA はリモート PC 上の VPN クライアントと通信して、サーバ アドレスを取得し、ステータス情報を VPN Concentrator と交換します。
- VPN Concentrator：ファイアウォール機能をグループごとに設定するための手段を提供します。また、IS の IP アドレスおよび他の VPN セッションに関する情報を VPN クライアントに報告し、VPN クライアントはこれらの情報を IA に渡します。また、VPN Concentrator は IS と通信して、セッションの確立と終了、セッションとユーザ情報の交換、認証ステータスの要求と取得を行います。
- VPN クライアント：リモート PC 上で、VPN Concentrator から IS のアドレスと情報を取得し、これらを IA に渡します。VPN クライアントも IA からのステータス情報の取得と報告、およびセッションの終了を行います。

接続がアップ状態になり、IS が IA にファイアウォール ポリシーを伝達すると、IS と IA はハートビート メカニズムを使用して連絡を取ります。

VPN クライアント Linux 版ファイアウォールの設定

シスコでは、VPN クライアント Linux 版リリース 4.7.00.640 仮想アダプタ専用に設計された次のファイアウォール設定を用意しています。以下のコードでは、トンネリングされたトラフィックを除く、eth0 のトラフィックがすべてブロックされます。

```
# Firewall configuration written by Cisco Systems
# Designed for the Linux VPN Client 4.7.00.0640 Virtual Adapter
# Blocks ALL traffic on eth0 except for tunneled traffic

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]

# Allow all traffic in both directions through the VA adapter
-A INPUT -i cipsec0 -j ACCEPT
-A OUTPUT -o cipsec0 -j ACCEPT

# Accept all encrypted VPN Client traffic in either direction on eth0
-A INPUT -i eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j ACCEPT

-A INPUT -i eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j ACCEPT

-A OUTPUT -o eth0 -p udp -s 0/0 --sport 1024: -d 0/0 --dport 29747 -j ACCEPT

# Block all other traffic in either direction on eth0
-A INPUT -i eth0 -j REJECT
-A OUTPUT -o eth0 -j REJECT
COMMIT
```

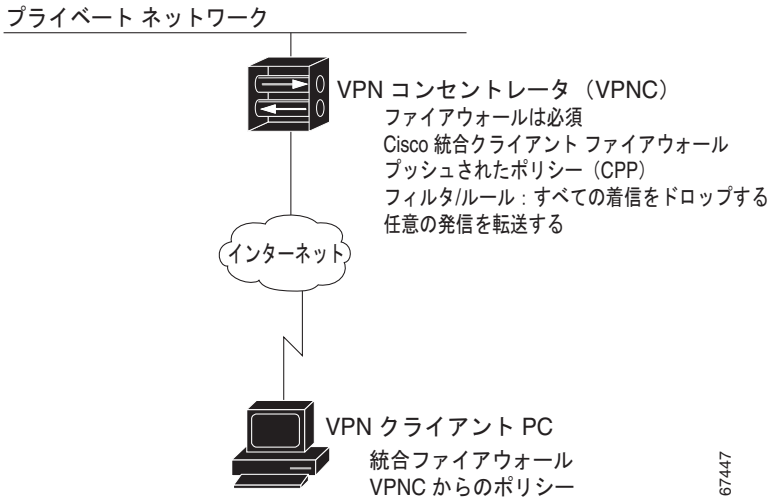
ファイアウォールの設定シナリオ

ここでは、3 つのファイアウォール設定例を示します。各図に、VPN Concentrator で有効なパラメータ設定および、VPN クライアントで有効なファイアウォール製品とポリシーを示します。

Cisco Integrated Client

図 4-1 に、Cisco Integrated Client の標準的な設定を示します。この設定では、ポリシー（CPP）が VPN クライアントにプッシュされます。このポリシーは、スプリット トンネリングが使用中のとき、インターネットからの着信トラフィックをブロックします。ただし、プライベート ネットワークからのトラフィックはブロックされません。

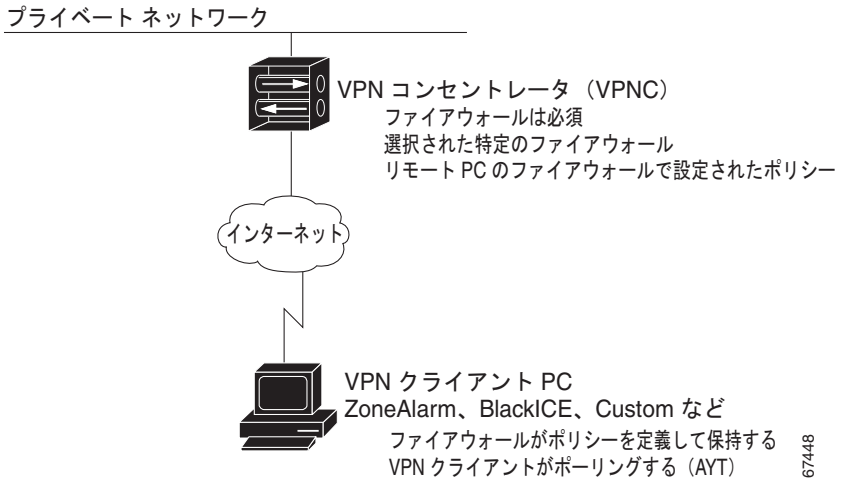
図 4-1　Cisco Integrated Client



リモート ファイアウォール

図 4-2 に、PC 上のパーソナル ファイアウォールにポリシーが設定されている設定例を示します。この場合、Are You There（AYT）がポリシーです。VPN クライアントは、30 秒後ごとにファイアウォールをポーリングしてファイアウォールが動作されているか、動作していないかを確認し、動作していなければ、VPN クライアントはセッションを終了します。

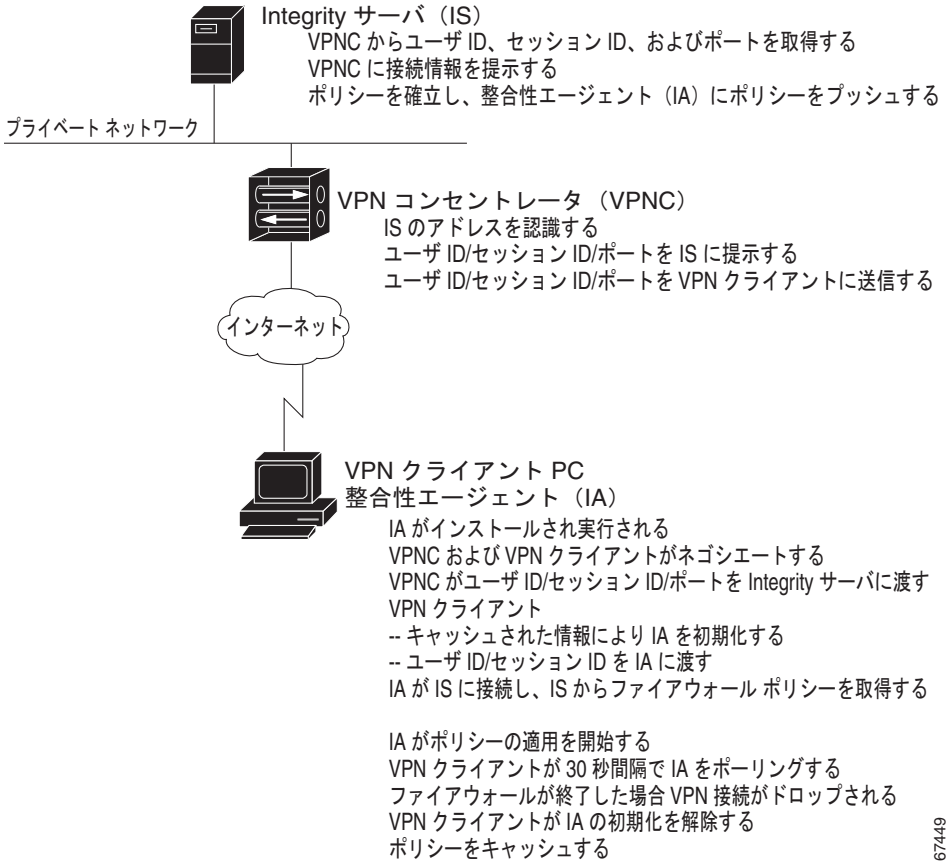
図 4-2　　リモート ファイア ウォールがポリシーを決定



クライアント/サーバの方式

図 4-3 に、Zone Labs Integrity の設定例を示します。

図 4-3　　クライアント/サーバ : Zone Labs Integrity Server との統合



CPP 用のファイアウォールで使用するフィルタとルールの定義

VPN Concentrator が VPN クライアントにファイアウォール ポリシーをプッシュするときは、最初に VPN Concentrator 上でポリシーを定義する必要があります。この場合、フィルタを作成し、パブリック ネットワーク上のフィルタにルールを追加する必要があります。VPN 3000 Concentrator は、メニューから選択して CPP 用に使用できるデフォルトのフィルタを備えています。このフィルタは、「Firewall Filter for VPN Client (Default)」という名前です。このフィルタは全発信トラフィックを許可し、全着信トラフィックを破棄します。

ファイアウォール フィルタはパケット フィルタではなく、セッション フィルタです。つまり、「allow all outbound/drop all inbound」ルールに対して、CPP ポリシーは、TCP、UDP および ICMP の各 IP プロトコルからの発信セッションの着信応答*だけ*を許可します。これらのプロトコルだけが「ステートフル」プロトコルです。ほとんどの管理者は、すべて着信トラフィックをブロックし、すべての発信トラフィックを許可するか、発信トラフィックを特定の TCP ポートと UDP ポートに制限するルールを使用するでしょう。一般的なフィルタの作成とルールの追加に関する詳細は、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「Configuration | Policy Management | Traffic Management」を参照してください。

例 4-1　　VPN クライアントを Web サーバとして動作させるファイアウォール ポリシー用のフィルタの作成

この例では、任意のプロトコルへの発信トラフィックを許可し、着信トラフィックは HTTP プロトコルからのものだけを許可するフィルタの追加方法をステップごとに説明します。この方法では、VPN クライアントをイネーブルにすることによって Web サーバにすることができます。

ステップ 1　最初に、HTTP からの着信トラフィックだけを許可するルールを作成します。そのためには、[Configuration | Policy Management | Traffic Management | Rules] の順に選択します。

ステップ 2　[Add] をクリックします。

a. [Rule Name] には、`FW-Allow incoming HTTP` のような名前を入力します。

b. [Action] には、[Forward] を選択します。

c. [Protocol] には、[TCP] を選択します。

d. [TCP/UDP Destination Port] には、[HTTP(80)] を選択します。

e. [Add] をクリックします。

ステップ 3　次に、HTTP からのトラフィックを除く、すべての着信トラフィックを破棄しても、トンネル経由で接続されている間のすべての発信トラフィックを転送するフィルタを追加します。そのためには、[Traffic Management] で [Filters] をクリックします。

a. [Add Filter] ボックスをクリックします。

b. `FW-Allow Incoming HTTP` のようなフィルタ名を入力し、残りのパラメータにはデフォルトを選択します。

c. [Add] をクリックして、[Actions] 画面を表示します。

d. この画面では、ルールを [Filter] 列の [Current Rules] に移動するために、ステップ 2 で作成したルールを強調表示し、[Add] をクリックします。Any Out（forward/out）ルールに対しても、同じ手順を繰り返します。

e. [Done] をクリックします。

ステップ 4　設定を保存します。

このフィルタは、Base Group および CPP ポリシーを選択するグループで使用可能です。

VPN クライアント上でファイアウォールを使用させる VPN 3000 Concentrator の設定

ここでは、VPN クライアント PC 上で VPN クライアントがパーソナル ファイアウォールを使用するように、VPN Concentrator を設定する方法について説明します。VPN クライアント側でパーソナル ファイアウォール ポリシーを実行するために、VPN 3000 Concentrator 側で Base Group またはユーザの特定のグループを設定します。一般的な手順は、次のとおりです。

ステップ 1　Base Group 用のファイアウォールを設定するには、[Configuration | User Management | Base Group] を選択します。または、特定のグループのファイアウォールを設定するには、[Configuration | User Management | Groups] を選択します。

ステップ 2　ファイアウォールを追加するために、次のいずれかの操作を実行します。

- Base Group に対しては、[Client FW] タブを選択します。
- ファイアウォールを設定するために新規グループを作成するには、[Add Group] をクリックし、[Client FW] タブをクリックします。
- 既存のグループにファイアウォールを追加するには、グループ名を強調表示して [Modify Group] をクリックし、[Client FW] タブをクリックします。

ステップ 3　ファイアウォールを要求するには、[Firewall Setting] 属性で、[Firewall Required] を選択します。

ステップ 4　[Firewall] 属性で、[Firewall] プルダウンメニューからファイアウォールを選択します。使用しているファイアウォールがリストにない場合は、[Custom] を使用する必要があります。

ステップ 5　[Firewall Policy] を選択します。リモート ファイアウォールによって定義されるポリシー（AYT）またはプッシュされるポリシー（CPP）のいずれかを選択します。（次の項を参照してください）。

詳細については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』、「User Management」項または VPN 3000 Concentrator Network Manager のオンライン ヘルプを参照してください。

CPP 用 Cisco 統合クライアント ファイアウォール（CIC）の設定

ステップ 1　[Firewall Setting] の [Client FW] タブで、[Firewall Required] を選択します。

ステップ 2　[Firewall] プルダウン メニューで、[Cisco Integrated Client Firewall] を選択します。

ステップ 3　[Firewall Policy] で [Policy Pushed] をクリックし、ファイアウォール ポリシーのルールを含むフィルタを選択します。デフォルトのファイアウォール フィルタまたは、特殊な目的のために設定されたフィルタを選択できます（「CPP 用のファイアウォールで使用するフィルタとルールの定義」を参照）。

クライアント/サーバ ファイアウォール：Zone Labs Integrity の設定

ステップ 1　Zone Labs のマニュアルに従って、Integrity Server（IS）上でファイアウォール ポリシーを設定します。

ステップ 2　VPN Concentrator 上で、[Configuration | System | Servers | Firewall Server] を選択します。Zone Labs Integrity Server のホスト名または IP アドレスおよびポート番号を入力します。

ステップ 3　[Under Configuration | User Management | Base Group or Groups | Client FW] タブ（「CPP 用のファイアウォールで使用するフィルタとルールの定義」を参照）で、次のように設定します。

a. Firewall Setting = **Firewall Required**

b. Firewall = **Zone Labs Integrity**

c. Firewall Policy = **Policy from Server**

ステップ 4　設定を保存します。

カスタム ベンダー コード

VPN 3000 Concentrator では、カスタム ファイアウォールを設定できます。表 4-1 に、VPN クライアントがサポートするカスタム ベンダー コードと製品コードを示します。

表 4-1　カスタム ベンダー コードと製品コード

ベンダー	ベンダー コード	製品	製品コード
シスコ	1	Cisco Integrated Client（CIC）	1
	5	Cisco Intrusion Prevention Security Agent	1
Zone Labs	2	Zone Alarm	1
		Zone AlarmPro	2
		Zone Labs Integrity	3
NetworkICE	3	BlackIce Defender/Agent	1
Sygate	4	Personal Firewall	1
		Personal Firewall Pro	2
		Security Agent	3

ファイアウォールのトラブルシューティング情報の入手

ここでは、ファイアウォール ネゴシエーションに関する情報を入手する 2 つの方法（IPsec ログまたは VPN Concentrator からの通知）について説明します。

IPsec ログの調査

VPN クライアントと VPN Concentrator 間のトンネル ネゴシエーション中に発生した現象を確認する 1 つの方法は、VPN クライアントの IPsec ログのメッセージを調査することです。そのためには、Log Viewer アプリケーションを使用します（Log Viewer の使用に関する情報については、『*VPN Client User Guide for Windows*』の第 5 章を参照）。トンネル ネゴシエーションの間に、VPN クライアントは、PC にインストールされ動作しているファイアウォールがあれば、そのリストを VPN Concentrator に送り、ファイアウォールの交換を開始します。次に VPN Concentrator は、そのファイアウォール要件を示すメッセージを VPN クライアントに送信します。

以下に、このファイアウォールの交換例を示します。

最初に、VPN クライアントから VPN Concentrator への要求例を示します。

```
36      16:44:39.250  02/28/03  Sev=Info/5
IKE/0x6300005D
Client sending a firewall request to concentrator

37      16:44:39.250  02/28/03  Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).                    87647
```

次に、VPN Concentrator からの応答例を示します。

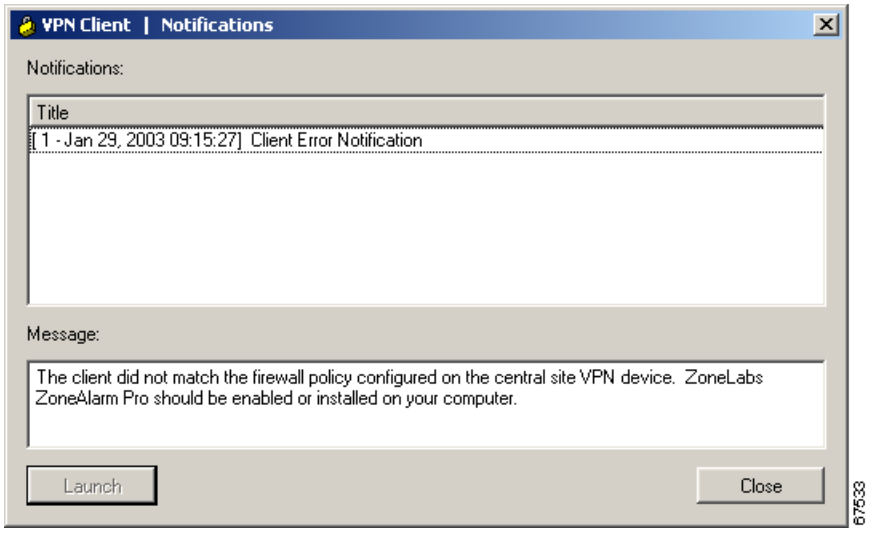
```
47      16:44:40.162  02/28/03  Sev=Info/5
IKE/0x6300005E
Client received a firewall reply from concentrator

48      16:44:40.162  02/28/03  Sev=Info/5
IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).                    87648
```

通知

VPN クライアントと VPN Concentrator のファイアウォールの設定が一致しない場合、VPN クライアント ユーザが接続を試行すると、VPN Concentrator は VPN クライアントに通知します。ファイアウォールの設定が必須の場合、接続試行は失敗し、ファイアウォールの設定が任意であれば、トンネルがアップ状態になります。

図 4-4　　ファイアウォールの不一致の通知



クライアント アップデートのリモート ユーザへの通知：すべての VPN クライアント プラットフォーム

セキュリティ アプライアンスまたは VPN 3000 Concentrator は、クライアント アップデート リスト内の各エントリに個別に通知メッセージを送信します。したがって、クライアント アップデート エントリに重複がないようにしてください。たとえば、値 Windows にはすべての Windows ベースのプラットフォームが含まれ、値 WinNT には Windows NT 4.0、Windows 2000、Windows XP、および Vista プラットフォームが含まれます。このため、Windows と WinNT を同時に指定することはできません。クライアントのタイプとバージョン情報を確認するには、VPN クライアントのメイン ウィンドウの左上隅にあるロック アイコンをクリックし、[About VPN Client] を選択してください。

VPN クライアント ユーザのリモート システムの VPN クライアント ソフトウェアを更新するときには、VPN クライアント ユーザに通知することができます。通知には、クライアント アップデートの格納場所を含めることができます（アップデートは自動的に行われません）。VPN 3000 Concentrator でのクライアント通知の設定は、次のクライアント アップデートの手順に従って行います。

ステップ 1　クライアント アップデートを有効にするため、[Configuration | System | Client Update] を選択し、[Enable] をクリックします。

ステップ 2　[Configuration | System | Client Update | Enable] 画面で、[Enabled] をオンにし（デフォルト）、[Apply] をクリックします。

ステップ 3　[Configuration | System | Client Update] 画面で、[Entries] をクリックします。

ステップ 4　[Entries] 画面で、[Add] をクリックします。VPN Concentrator Manager に、[Configuration | System | Client Update | Entries | Add or Modify] 画面が表示されます。

ステップ 5　[Client Type] に、通知対象となるオペレーティング システムを入力します。

- Windows には、すべての Windows ベースのプラットフォームが含まれます。
- WinNT には、WindowsNT 4.0、Windows 2000、Windows XP、および Windows Vista の各プラットフォームが含まれます。
- Linux
- Solaris
- Mac OS X

（注）　VPN 3000 Concentrator では、クライアント アップデート リスト内の各エントリに対して通知メッセージが個別に送信されます。したがって、クライアント アップデート エントリに重複がないようにしてください。たとえば、値 **Windows** にはすべての Windows ベースのプラットフォームが含まれ、値 WinNT には Windows NT 4.0、Windows 2000、Windows XP、および Vista プラットフォームが含まれます。このため、Windows と WinNT を同時に指定することはできません。クライアントのタイプとバージョン情報を確認するには、VPN クライアントのメイン ウィンドウの左上隅にあるロック アイコンをクリックし、[About VPN Client] を選択してください。

ステップ 6　[URL] フィールドに、通知を表示する URL を入力します。

[VPN Client Notification] の [Launch] ボタンをアクティブにするためには、プロトコルとして HTTP または HTTPS、およびアップデートが置かれているサイトのサーバ アドレスをメッセージに含める必要があります。メッセージには、http://www.oz.org/upgrades/clientupdate など、アップデートのディレクトリおよびファイル名を含めることもできます。リモート ユーザに対して [Launch] ボタンをアクティブにしない場合は、メッセージにプロトコルを含める必要はありません。

ステップ 7　すでに最新ソフトウェアを使用しているためアップデートが不要なクライアント リビジョンのカンマ区切りリストを [Revisions] フィールドに入力します。たとえば、値「3.6.5 (Rel), 4.0 (Rel)」は該当するリリースを示し、その他の VPN クライアントはアップグレードする必要があります。

ステップ 8　[Add] をクリックします。

リモート ユーザが VPN デバイスに初めて接続した場合、またはユーザが [Connection Status] ダイアログボックスの [Notification] ボタンをクリックした場合は [Notification] ダイアログボックスが表示されます。通知がポップアップ表示されたら、VPN クライアントの [Notification] ダイアログボックスにある [Launch] をクリックしてデフォルトのブラウザを開き、アップデートが置かれている URL にアクセスします。

VPN クライアント用のローカル LAN アクセスの設定

自宅から有線接続または DSL を使用してアクセスするリモート ユーザは、ホーム ネットワークを使用してファイルやプリンタを共有している場合があります。ネットワーク管理者は、リモート ユーザが（IPsec トンネル経由で）中央サイトへのセキュア接続を維持しつつ、クライアント側の LAN リソースにアクセスできるように、ローカル LAN アクセスを設定できます。

設定を開始する前に、『*VPN 3000 Series Concentrator Reference Volume 1: Configuration*』の「Split Tunneling」の項をよく読んでください。[Configuration | User Management | Groups | Add or Modify | IPsec] タブについて説明している項を参照してください。

ローカル LAN アクセスの設定の一般的な手順は、次のとおりです。

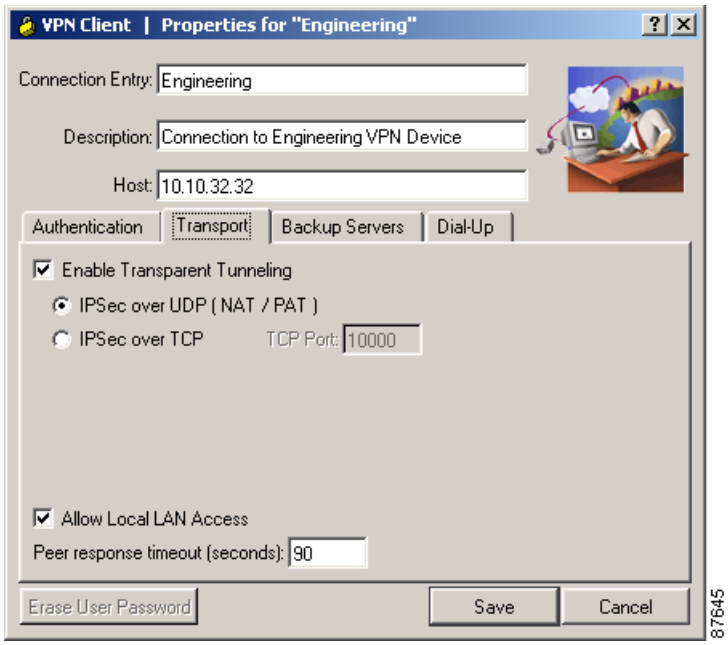
- VPN クライアントのローカル LAN アクセスをイネーブルにする。
- VPN 3000 Concentrator 上の特定のグループ内でローカル LAN アクセスをイネーブルにする。
- アクセス可能なネットワークをネットワーク リストに追加する（またはデフォルト ネットワーク アドレスを使用する）。

次の手順を使用します。

ステップ 1　VPN クライアントで、Allow Local LAN Access パラメータをイネーブルにします。

接続エントリを作成または変更する場合は、[Transport] タブを表示し、[Allow Local LAN Access] をオンにします。

図 4-5　VPN クライアントでの [Allow Local LAN Access Parameter] の設定



ステップ 2　VPN 3000 Concentrator 上で、次の手順で新規グループ追加するか、既存のグループを変更します。

a. 特定のグループのローカル LAN アクセスを設定するには、[Configuration | User Management | Groups] を選択します。

b. [Add] を選択して、新規グループを追加するか、[Modify] を選択して、既存のグループに対してローカル LAN イネーブルにします。

c. [Client Config] タブを表示します。

d. [Split Tunneling Policy] 属性の [Value] で、[Tunnel everything] オプション ボタンをクリックし、[Allow the networks in list to bypass the tunnel] をクリックします。VPN クライアント上でローカル LAN アクセスが有効になります。

e. [Split Tunneling Network List] の [Value] で、ローカル LAN アクセス用に作成したネットワーク リストがあれば、そのネットワーク リストを選択します。

VPN Client Local LAN がデフォルトで、アドレス 0.0.0.0/0.0.0.0 に割り当てられます。この IP アドレスを使用すると、そのネットワーク上で設定されたネットワーク アドレッシングに関係なく、クライアント側の LAN 上のホストすべてにアクセスできます。このローカル LAN アクセスは、1 つのローカル ネットワークだけに制限されるため、クライアント PC に複数のネットワーク カードを搭載している場合、VPN クライアントが VPN 接続を確立したネットワークにしかアクセスできません。

ネットワーク リストの作成については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「Configuration | Policy Management | Traffic Management | Network Lists」を参照してください。

（注） VPN クライアントがローカル LAN アクセス用に接続され設定されていると、ローカル LAN では名前によって印刷やブラウズを行うことはできません。VPN クライアントの接続が解除されると、名前を使用して印刷またはブラウズできるようになります。

IP アドレスでブラウズや印刷を行うことはできます。ネットワーク プリンタのプロパティを変更して、

印刷の際に、名前の代わりにの IP アドレスを使用するように設定できます。たとえば、構文 \\sharename\printername を使用するのではなく、構文 \\x.x.x.x\printername（x.x.x.x は IP アドレス）を使用します。

名前を使用して印刷およびブラウズするために、LMHOSTS ファイルを使用できます。このファイルを使用するには、LMHOSTS という名前のテキスト ファイルに IP アドレスとローカル ホスト名を追加し、すべてのローカル PC 上の \Windows ディレクトリに保存します。PC の TCP/IP スタックは、印刷またはブラウズ時に、LMHOSTS ファイル内の IP アドレスとホスト名のマッピングを使用して名前を解決します。この方法では、すべてのローカル ホストにスタティック IP アドレスが必要です。また、DHCP を使用する場合は、常に同じ IP アドレスを取得するようにローカル ホストを設定する必要があります。

LMHOSTS ファイルの例は、次のとおりです。

```
192.168.1.100 MKPC
192.168.1.101 SBPC
192.168.1.101 LHPC
```

クライアント バックアップ サーバ用の VPN Concentrator の設定

ここでは、VPN Concentrator 上でグループを設定して、新しいバックアップ サーバの情報を VPN クライアントに自動的にプッシュする方法について説明します。

ステップ 1　VPN Concentrator で、[Configuration | User Management | Group] の順に選択します。

ステップ 2　新しいグループを追加するには、[Add] をクリックし、既存のグループを変更するには、ボックス内でそのグループを強調表示して、[Modify] をクリックします。

ステップ 3　[Client Config] タブを表示します。

ステップ 4　[IPsec Backup Servers] には、ドロップダウン メニューから [Use List Below] を選択します。

ステップ 5　優先順位の高いものから順に、最大 10 の IPsec バックアップ サーバのリストを入力します。

ステップ 6　[IPsec Backup Servers] ボックスに、各サーバのアドレスまたは名前を 1 行で入力します。

ステップ 7　[Apply] をクリックし、設定を保存します。

VPN クライアントの NAT Traversal の設定

NAT Traversal（NAT-T）は、VPN Concentrator と VPN クライアントとの間に NAT 装置があるときに、VPN Concentrator が VPN クライアントとの IPsec トンネルを確立できるようにします。これは、UDP データグラム内に ESP トラフィックをカプセル化することによって実現され、NAT 装置が要求するポート情報が ESP に提供されます。

ネットワーク管理者は、VPN Concentrator 上で NAT-T をグローバルに設定できます。これによって、VPN Concentrator 上で設定されたすべてのグループに対して NAT-T をアクティブにできます。

グローバル コンフィギュレーション

NAT-T をグローバルに設定するには、VPN Concentrator 上で次の手順を実行します。

ステップ 1　[Configuration | System | Tunneling Protocols| IPsec | NAT Transparency] の順に選択し、[IPsec over NAT-T] チェック ボックスをオンにします。

ステップ 2　[Apply] をクリックし、設定を保存します。

次に、VPN クライアント上で次のパラメータを設定します。

ステップ 1　新しい接続エントリを作成する場合は、[Connection Entries] の [New] をクリックします。既存の接続エントリを変更する場合は、エントリを強調表示して、[Modify] をクリックします。いずれの場合も、プロパティ ダイアログボックスが表示されます。

ステップ 2　[Transport] タブを開きます。

ステップ 3　[Enable Transparent Tunneling] チェックボックスをオンにします。

ステップ 4　[IPsec over UDP (NAT/PAT)] オプション ボタンをクリックします。

ブラウザの自動設定の設定（Windows のみ）

（注）　この機能は、Microsoft Internet Explorer Web ブラウザだけでサポートされます。

リモート ユーザが VPN Concentrator（セキュア ゲートウェイ）に接続すると、VPN クライアントは VPN Concentrator から Web ブラウザ プロキシ設定を受信し、ユーザの Web ブラウザ プロキシ設定を変更して組織の環境内で動作できるようにします。この設定は、ユーザがセキュア ゲートウェイに接続している間だけ有効です。ユーザが接続解除すると、VPN クライアントは PC のブラウザ プロキシを自動的に元の設定に戻します。

この設定は、ネットワーク管理者が VPN Concentrator 上で行います。VPN クライアントに対してブラウザ プロキシ設定を行うには、次の手順を実行します。

ステップ 1　VPN Concentrator で、[Configuration | User Management | Base Group] の順に選択します。

ステップ 2　[VPN Client Config] タブをクリックします。

ステップ 3　[Microsoft Client Parameters] セクションにスクロールします。

ステップ 4　次のセクションを編集します。

a.（画面上の説明に従って）[IP Proxy Server Policy] 方法を選択します。有効な選択肢は次のとおりです。これらの選択肢は互いに排他的です。

- [Do not modify proxy settings]：プロキシ設定を変更しないようにします。
- [No proxy]：VPN クライアント PC のプロキシ設定をディセーブルにします。
- [Autodetect proxy]：VPN クライアント PC のプロキシ サーバ設定の自動検知をイネーブルにします（ただし、この設定は変更されません）。

- [Use the proxy and server port configured in the IE Proxy Server box]。このオプションを選択する場合、[Client Config] タブ内にあるこのセクションの残りのボックスにも設定を入力してください。IE プロキシ サーバ ID が必要です。

b. [IE Proxy Server] ボックスに、Internet Explorer を使用するクライアントのプロキシ サーバ名、コロン（:）、ポート番号を入力します（例：myproxy.mycompany.com:8080）。

c. [IE Proxy Serve Exception List] に、プロキシ サーバ経由でアクセスできないアドレスまたはドメインを入力します。このリストは、Internet Explorer の [Proxy Stteings] ダイアログボックスにある [Exceptions] ボックスに相当します。ワイルドカードを入力できます（例：www.*.org または 10.10.*）。

d. ローカル要求を許可してプロキシ サーバをバイパスするには、[Bypass Proxy Server for Local Addresses] をクリックします。

ステップ 5　必ず設定を保存してください。

（注） VPN クライアントのブラウザ プロキシ機能は、次の点で Internet Explorer と異なります。Internet Explorer では、[Auto detect policy] と [Use proxy server/port] は相互に排他的ではありません。VPN クライアントはすべてのプロトコルに対して 1 つのプロキシ サーバしかサポートしませんが、Internet Explorer では、プロトコルごとに 1 つのプロキシ サーバを設定できます。

VPN クライアントは、Internet Explorer の [Use automatic configuration script] オプションをサポートしていません。

VPN クライアント用の Entrust Entelligence の設定（Windows のみ）

ここでは、VPN クライアントをセットアップして、Entrust Entelligence にアクセスし、Entrust ID 証明書を取得する方法について説明します。また、VPN クライアント ソフトウェアを Entrust と連携させて使用する際の情報についても説明します。Entrust のインストールおよび設定については、Entrust のマニュアル『*Entrust Entelligence Quick Start Guide*』または Entrust Entelligence オンライン ヘルプを参照してください。

次の手順を使用します。

ステップ 1　Entrust Entelligence ソフトウェアをリモート ユーザの PC にインストールします。

Entrust Entelligence ソフトウェアをインストールしてから、VPN クライアントをインストールしてください。VPN クライアントで Start before Logon と Entrust SignOn を同時に使用するときのために、この順序でインストールすることが重要です。これらの機能が両方とも VPN クライアントに設定されているときに発生する現象については、『*VPN Client User Guide for Windows*』の第 5 章を参照してください。

ステップ 2　Entust Entelligence のインストール中に、Create Entrust Profile ウィザードを使用して、新しい Entrust プロファイルを作成します。

Entrust Entelligence プロファイルを作成するには、次の情報が必要です。

- Entrust Entelligence 参照番号
- Entrust Entelligence 認証コード

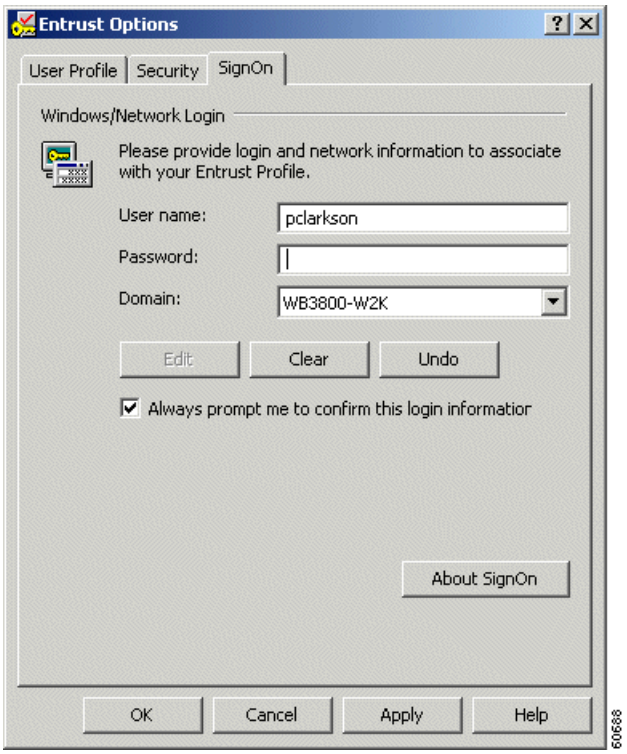
- プロファイルを保存するディレクトリの名前
- プロファイルの名前
- Entrust 管理者が設定したルールに従ったパスワード

ステップ 3　オプションとして、Entrust SignOn を Entrust のマニュアルに従ってインストールします。

a. Entrust SignOn のインストール中に、[Entrust Options] ダイアログボックスが表示されます。（図 4-6 を参照）。

b. [Always prompt me to confirm this login information] がオンになっていることを確認します。このボックスをオンにすると、[Entrust SignOn] ログイン ダイアログボックスが一時停止して、リモート ユーザが NT ログオン情報を入力する前に VPN 接続が確立されます。

図 4-6　[Entrust Options] の [SignOn] タブ



ステップ 4　プロファイルを作成したら、Entrust Entelligence からログアウトします。

ステップ 5　VPN クライアント ソフトウェアをインストールします。

ステップ 6　Entrust 証明書を使用した認証を含む、新しい接続エントリを作成します。作成方法については、『VPN Client User Guide for Windows』の第 4 章「*Configuring an Entrust Certificate for Authentication*」を参照してください。

（注）　VPN クライアントは最新の Entrust DLL ファイルに依存します。このファイルの名前は kmpapi32.dll です。Entrust Entelligence バージョン 5.1 を使用している場合、DLL ファイルは最新です。VPN クライアント システムにバージョン 4.0 または 5.0 がインストールされている場合、DLL ファイルは最新

ではありません。

VPN クライアントの [Certificate] メニューに「Entelligence Certificate (Entrust)」が表示されない場合、VPN クライアント ソフトウェアに付属の DLL ファイルが最新バージョンでない可能性があります。kmpapi32.dll ファイルを更新するには、そのファイルをリリース メディアから VPN クライアント システムにコピーし、Windows のデフォルト システム ディレクトリに保存します。Windows NT、Windows 2000、および Windows XP システムの場合、このディレクトリは c:¥WinNT¥System32 です。Windows 9x および Windows ME の場合、このディレクトリは ¥Windows¥System です。

スマート カードを使用した認証用に VPN クライアントを設定する（Windows のみ）

VPN クライアントは、スマート カードに保管された証明書を使用した認証をサポートします。接続エントリを作成し、認証用の証明書を選択したら、VPN クライアント ユーザはスマート カードをカード リーダーに挿入する必要があります。VPN クライアント接続が開始されると、ユーザは、スマート カードにアクセスするための PIN またはパスコードを入力するよう求められます。秘密キーはスマート カード上に存在し、PIN またはパスコードを入力しないと絶対にアクセスできません。また、ほとんどの場合、PIN またはパスコードの入力試行回数には制限があり、その回数を超えるとカードがロックされます。

各スマート カード ベンダーの製品に対して VPN クライアント認証を設定する方法については、本書では割愛します。個々のスマート カードにおける認証の設定方法については、該当するスマート カード ベンダーの説明書を参照してください。

一般的な手順は、次のとおりです。

ステップ 1　Web ベースの証明書登録を実行する場合は、[Key Options] で、プルダウン メニューからスマート カード プロバイダを選択します。

ステップ 2　キー使用状況については、[Signature] を選択し、[Create new key set] が選択されていることを確認します。

ステップ 3　証明書をインストールします。キーがスマート カード上に生成され、証明書のコピーが PC 上の Microsoft ストアに保管され、VPN クライアントの [Certificates] タブにリストされます。

ステップ 4　[Connection Entry] > [Modify] ダイアログを選択し、以下の操作を実行します。

a.　[Authentication] タブを開き、[Certificate Authentication] オプション ボタンをオンにします。

b.　[Name] ドロップダウン メニューを表示し、スマート カード証明書をクリックします。

VPN クライアント ユーザは、PC の適切なポートに接続されたカード リーダーにスマート カードが挿入され、ユーザが正しい PIN またはパスコードを入力したときにだけ認証を完了させることができます。

（注）　ほとんどのベンダー製品では、スマート カードが挿入されていないときにも、証明書が [Certificates] タブに表示されます。ただし、Aladdin の e-token では、接続解除されると証明書がリストから削除されます。e-token が挿入されアクティブのときだけ、証明書がリストに表示されます。

スマート カードを取り外したときのトンネルの切断

スマート カードをシステムから取り外すと、トンネルは自動的に切断されます。システムからスマート カードを取り外すと、ただちにトンネルがドロップされます。これが「Always on」機能です。

不正な PIN の入力回数が超過したためにスマート カードがロックされたときのユーザへの通知

正しくない PIN の入力回数が超過したために、スマート カードがブロックされると、VPN クライアントにログ メッセージが表示されます。このような状況では、結果的に接続は失敗します。通知は、ロックされているスマート カードについてのログ メッセージです（CSCsb927）。

新しい接続確立時におけるスマート カード パスワードの再要求

新しい接続が確立されると、必ずスマート カードは、ユーザにクレデンシャルを再度入力するよう要求します（新しい接続に対するパスワードの再入力要求（パスワードはキャッシュされない））。VPN クライアントでは、ユーザがクレデンシャルを再入力せずに接続を再確立して、スマート カードをアンロックすることはできません。

この機能を回避し、以前の VPN クライアント リリースと同様の動作を維持するには、vpnent.ini ファイルに「BypassCardPinReset=1」というエントリを追加してください。（CSCsb73937）。

キー再生成時のスマート カード ユーザの再認証

VPN クライアント バージョン 5.0.4 以降では、VPN セッションのキーが再生成されると、VPN クライアントはスマート カードのユーザに再認証を要求します。ユーザが再認証を実行しない場合、VPN 接続が終了します。この動作をディセーブルにするには、vpnclient.ini ファイルに CvpndSignHash パラメータを設定します。このパラメータの動作は、以下の設定によって定義されます。

- CvpndSignHash=0（デフォルト）、あるいはパラメータが欠落している場合：認証はキャッシュされず、ユーザは、クライアントによってキーの再生成時に再認証するよう要求されます。
- CvpndSignHash=1：VPN クライアントは認証をキャッシュします。キーの再生成時に、VPN クライアントはユーザに再認証するよう要求 *しません*。

相互認証の設定

ここでは、管理者が VPN クライアント システムおよび VPN Concentrator に認証を設定する際に役立つ情報を記載しています。これ以降の記述は、すべての VPN クライアント プラットフォームに適用されます。

VPN クライアント システム上での相互グループ認証の設定

グループ認証は、相互認証用に事前共有キーを使用する方法です。この方法では、VPN クライアントおよび VPN 中央サイト デバイスはグループ名とパスワードを使用して、接続を確認します。この方法は、ネゴシエーション時に両側で同じ認証方法が使用されることから、対称型の認証です。事前共有認証は、2 つの段階で行われます。

第 1 段階で、双方がセキュリティ パラメータを交換し、セキュア チャネルを確立します。第 2 段階で、ユーザ認証が行われます。VPN 中央サイト デバイスは、リモート ユーザが、VPN 中央サイト デバイス上で設定されたグループの有効なメンバーであるかを確認するためにユーザ名とパスワードの入力を要求します。

相互グループ認証は、セキュア トンネルを確立してグループ認証の基盤を形成しつつ、双方で異なる方法を使用して相互を認証するという点で非対称です。この方法では、2 段階で認証が行われます。第 1 段階では、VPN 中央サイト デバイスはそれ自体の公開キー技術（デジタル署名）を使用して認証し、双方がネゴシエーションして通信用のセキュア チャネルを確立します。第 2 段階では、VPN クライアント ユーザの実際の認証が、中央サイトの VPN デバイスによって実行されます。この方法は、中間者攻撃に対して脆弱ではなく、ピア認証に事前共有キーを使用しないため、グループ認証だけの場合よりもセキュリティが向上します。

相互グループ認証を使用するには、リモート ユーザの VPN クライアント システムには、ルート証明書がインストールされている必要があります。必要に応じて、インストール中にルート証明書を VPN クライアント システムに保存すると、ルート証明書を自動的にインストールできます。証明書は、拡張子の付いていない、rootcert という名前のファイルになければならず、リモート ユーザ VPN クライアント システムのインストール ディレクトリに配置する必要があります。rootcert のロード方法の詳細については、リモート ユーザのプラットフォームのインストール ユーザ ガイドを参照してください。

VPN Concentrator での相互認証の設定

相互認証を実行するために、VPN Concentrator は、VPN クライアント システムと同じ認証局（CA）を使用する必要があります。VPN Concentrator 側では、以下のように設定する必要があります。

ステップ 1　このマニュアルの表 11-2（P.11-11）の「コマンドライン スイッチ」に記載されている HYBID モード認証を許可する IKE プロポーザルを選択します。たとえば、VPN Concentrator では、IKE プロポーザルとして HYBRID-AES256-SHA-RSA を選択してください。IKE プロポーザルの設定方法については、『*VPN 3000 Series Concentrator Reference, Volume I, Configuration*』の「Configuration | Tunneling and Security | IPsec | IKE Proposals」を参照してください（http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1e36.html#1137591）。

（注）　HYBRID モード認証を含む IKE プロポーザルは、VPN 3000 Concentrator 4.1 Rel リリースにはありません。ただし、リリース 4.6 以降の VPN 3000 Concentrator ソフトウェアではこのような IKE プロポーザルを選択できます。

ステップ 2　VPN Concentrator にまだ ID 証明書ない場合は、証明書の CA に登録する必要があります。この手順については、『*VPN 3000 Series Concentrator Reference, Volume II, Administration and Monitoring*』の「Configuration Management」を参照してください（http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_administration_guide_chapter09186a00801f1dc5.html）。

ステップ 3　IPsec SA を設定して、VPN クライアントの CA 証明書で認証する ID 証明書を使用するようにします。詳細は、『*VPN 3000 Series Concentrator Reference, Volume I, Configuration*』の「Configuration | Policy Management | Traffic Management | Security Associations」を参照してください（http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1dbb.html#1563342）。

ステップ 4　VPN Concentrator で VPN グループを設定して、ステップ 3 の新しい IPsec SA を使用するようにします。VPN グループの設定方法については、『*VPN 3000 Series Concentrator Reference, Volume I, Configuration*』の「Configuration | User Management | Groups」にある [IPsec] タブを参照してください（http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00801f1df7.html#1907522）。