CHAPTER 1

管理者向け情報の設定

この章では、ご使用のプラットフォームの『VPN Client User Guide』および Cisco シリーズ 5500 適応型セキュリティ アプライアンスまたは Cisco VPN 3000 シリーズ Concentrator のいずれかを使用しているセキュア ゲートウェイの設定ガイドを補足する、ネットワーク管理者への情報について説明します。この章では、完全を期すため IPsec サイト間接続について述べている箇所がありますが、このマニュアルでは IPsec リモート アクセス接続についてのみ説明しています。

この章の主な内容は、次のとおりです。

IPsec の概念

IPSec は、VPN トンネルのアーキテクチャをほぼ完全に実現しており、最もセキュアなプロトコルとされています。IPSec は、LAN 間（サイト間）接続に使用することも、クライアントと LAN との接続に使用することもできます。

IPSec 用語で「ピア」とは、リモート アクセス クライアントまたは別のセキュアなゲートウェイを意味します。IPsec でトンネルを確立する間に、2 つのピアは、認証、暗号化、カプセル化、キー管理を制御するセキュリティ アソシエーションをネゴシエートします。これらのネゴシエーションには、トンネルの確立（IKE SA）と、トンネル内のトラフィックの制御（IPsec SA）という 2 つのフェーズが含まれます。

IPsec サイト間接続では、セキュリティ アプライアンスは発信側または応答側として動作できます。IPsec リモート アクセス（クライアントと LAN 間）接続では、セキュリティ アプライアンスは応答側としてのみ動作します。発信側は SA を提案し、応答側は、設定された SA パラメータに従って、SA の提示を受け入れるか、拒否するか、または対案を提示します。接続を確立するには、両方のエンティティで SA が一致する必要があります。

VPN クライアントは IPSec プロトコルに準拠しており、具体的にはセキュリティ アプライアンスで動作する設計になっています。ところが、セキュリティ アプライアンスは、多様なプロトコルに準拠するクライアントと IPSec 接続を確立できます。同様にセキュリティ アプライアンスは、セキュア ゲートウェイと呼ばれることが多い他のプロトコルに準拠した VPN デバイスとサイト間接続を確立できます。

サポートされる IPsec 属性

セキュリティ アプライアンスは次の IPsec 属性をサポートします。

- 認証にデジタル証明書を使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーションをネゴシエートするメイン モード
- 認証で事前共有キーを使用するときに、フェーズ 1 ISAKMP セキュリティ アソシエーション（SA）をネゴシエートするアグレッシブ モード
- 認証アルゴリズム：
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 認証モード：
  - 事前共有キー
  - X.509 デジタル証明書
- Diffie-Hellman グループ 1、2、5、および 7
- 暗号化アルゴリズム：
  - AES-128、-192、および -256
  - 3DES-168
  - DES-56
  - ESP-NULL
- 拡張認証（XAuth）
- モード コンフィギュレーション（別名 ISAKMP コンフィギュレーション方式）
- トンネル カプセル化モード
- LZS を使用した IP 圧縮（IPCOMP）

（注）　Smart Card 認証は VPN Client Release 5.0.3.0560 以降でサポートされています。

サポートされていない IPsec 属性

Cisco VPN Client for Windows Vista Rlease 5.x では、次の機能はサポートされて*いません*。

- Windows XP 以前の Windows オペレーティング システムから Vista にアップグレードされたシステム。（OS のクリーン インストールが必要）。
- 統合ファイアウォール
- InstallShield。
- 自動更新。
- 日本語版オンライン ヘルプ。オンライン ヘルプは英語版のみ提供されています。

（注）　Start Before Logon は Windows Vista、Windows XP でのみサポートされています。

システム要件

VPN クライアントを*任意*のシステムにインストールするには、次が必要です。

- CD-ROM ドライブ（CD-ROM からインストールする場合）
- 管理者特権

VPN クライアントは次の Cisco VPN デバイスをサポートしています。これらのデバイスはこのマニュアルでは、セキュア ゲートウェイまたは中央サイト デバイスと呼ばれています。

- すべてのバージョンの Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco VPN 3000 Concentrator シリーズ、バージョン 3.0 以降。
- Cisco PIX ファイアウォール、バージョン 6.2.2(122) またはバージョン 6.3(1)。
- Cisco IOS ルータ、バージョン 12.2(8)T 以降

Internet Explorer を使用する場合は、バージョン 5.0 Service Pack 2 以降を使用します。

制限事項

VPN クライアントには次の制限事項が適用します。

- VPN クライアントは複数のイーサネットまたは PPP アダプタを搭載したコンピュータはサポートしません。
- インターネット メディアとして使用される Bluetooth モデムは VPN クライアントでは動作したり、しない場合がありますが、正式にテストまたはサポートされているわけではありません。
- VPN クライアントと AnyConnect VPN クライアントを同時に同じシステムで使用することはできません。

表 1-1 は、各対応プラットフォームに VPN クライアントをインストールする場合のシステム要件を示します。最新の情報については、Cisco VPN クライアントの最新版のリリース ノートを参照してください。

表 1-1　システム要件

コンピュータ	オペレーティング システム	要件
Pentium® 以降クラスのプロセッサを搭載した Tablet PC などのコンピュータ[1]	• Windows 7 32/64 ビット版 • Windows Vista 32/64 ビット版 • Windows XP 32 ビット版[2]	• Microsoft TCP/IP インストール済み。([Start] > [Settings] > [Control Panel] > [Network] > [Protocols] または [Configuration] から確認)。 • 50 MB のハード ディスク領域。 • RAM : – 128 MB（Windows XP の場合）（256 MB を推奨）
Intel x86 プロセッサ搭載コンピュータ	カーネル バージョン 2.2.12 以降を使用した RedHat バージョン 6.2 以降の Linux（Intel）、または glibc バージョン 2.1.1-6 以降の互換ライブラリ[3] **（注）** VPN クライアントは SMP（マルチプロセッサ）または 64 ビット プロセッサ カーネルをサポートしません。	• 32 MB RAM • 50 MB のハード ディスク領域
Sun UltraSPARC コンピュータ	32 ビットまたは 64 ビット版 Solaris カーネル OS バージョン 2.6 以降	• 32 MB RAM • 50 MB のハード ディスク領域
Macintosh コンピュータ	Mac OS X、バージョン 10.4.0 以降	• 50 MB のハード ディスク領域 • PPC または Intel プロセッサ。

1. VPN クライアントには、Windows XP および Windows Vista のデュアルプロセッサ ワークステーションおよびデュアルコア ワークステーションのサポートが含まれています。
2. Windows VPN Client Release 4.8.00.440 は、Windows 98 オペレーティング システムを正式にサポートした最後のバージョンでした。Windows VPN Client Release 4.6.04.0043 は、Windows NT オペレーティング システムを正式にサポートした最後のバージョンでした。
3. Linux Unified VPN クライアントのインストールは、Linux カーネル 2.2.19 以降でカーネル モジュールを構築中に正しく行われます（CSCsg98579）

MSI インストーラのリブートレス クライアント アップグレード

次の状況では、VPN クライアント インストール用の MSI インストーラを使用して、リブートせずに VPN クライアントをアップグレードできます。

- VPN クライアントの以前の MSI バージョンがインストールされている場合、4.8.00.0440 MSI VPN クライアント インストールで上書きするときにリブートが必要なのは、以前の VPN クライアント インストールをアンインストールときだけです。(過去のインストールではさらにリブートが必要でしたが、これが不要になりました)。
- 4.8.00.0440 MSI VPN クライアントを新規インストールする場合は、リブートは必要ありません。
- 以降の MSI インストールで 4.8.00.0440 MSI VPN クライアントからアップグレードする場合は、リブートは必要*ありません*（CSCsb35946）。
- VPN Client Release 5.x 以降のバージョンからアップグレードする場合は、リブートは必要ありません。

VPN クライアントを Windows にさらに簡単にインストールできるようにするため、MSI インストーラはファイルが解凍されると自動的に開始します（CSCeg81066）。

（注）　DNE インストーラの結果によっては、稀に MSI リブートが必要になる場合があります。

MSI インストールと日本語ヘルプ ファイル

MSI トランスフォームの日本語ヘルプ ファイルは VPN クライアント インストール パッケージから削除されました。現在は、「vpnclient_help_jp_4.8.00.0440.zip」として www.cisco.com に別途掲載されています（CSCei23559）。

ステートフル ファイアウォールが不要な場合のファイアウォール ファイルのインストールのバイパス方法

VPN クライアントのステートフル ファイアウォール ファイルが他のサード パーティ アプリケーションと競合する場合があります。この競合を最小限に抑えるため、次の手順で、ステートフル ファイアウォール ファイルを使用せずに VPN クライアントをインストールできます。

注意　Zone Alarm 製品を使用している場合、類似のファイルが共有されるため、この手順は使用しないでください。

ワークステーションに vsdata.dll ファイルが *ない*（Cisco VPN クライアントがインストールされていない、または Zone Alarm 製品がない）場合、このファイルを削除するか名前を変更してから処理します。

MSI は、リリース 5.x 以前の VPN クライアント バージョンでは www.cisco.com に掲載された novsdata.zip トランスフォームを使用する必要があります。トランスフォームは 5.x リリースとは互換性がありません。VPN Client Release 5.0.3.0560 から、ファイアウォール ファイル中の guild がインストールされないよう、次のように MSI インストール フラグが追加されました（CSCsi45962）。

msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1

これにより VPN クライアントは次のファイルをインストールまたはアップデートしません。

vsdata.dll

vsinit.dll

vsdatant.sys

既存のインストールでこれらのファイルを手作業で削除または名前を変更しても、リブート後に内蔵ファイアウォールがディセーブルになります。

VPN クライアントを正しくインストールすると、オプション プルダウンにステートフル ファイアウォールは表示 *されません*。

VPN クライアントの使用方法

- VPN クライアントを使用するには、次が必要です。
  - ダイレクト ネットワーク接続（ケーブルまたは DSL モデム、およびネットワーク アダプタまたはインターフェイス カード）、または
  - 内部モデムまたは外部モデム
- 認証にデジタル証明書を使用して接続するには、PC にインストールされた次のいずれかの認証局（CA）により署名されたデジタル証明書が必要です。
  - Baltimore Technologies（www.baltimoretechnologies.com）
  - Entrust Technologies（www.entrust.com）
  - Netscape（www.netscape.com）
  - Verisign, Inc.（www.verisign.com）
  - Microsoft Certificate Services：Windows 2000
  - スマート カードに保存されたデジタル証明書。VPN クライアントは MS CAPI インターフェイス経由でスマート カードをサポートします。

Windows Vista ユーザ向けの勧告

Windows Vista ユーザは、次のような VPN クライアントの特性を意識している必要があります。

スマート カードのサポート

Cisco VPN Client for Windows Vista Release 5.0.3.0560 以降はスマート カード認証をサポートします（CSCsi25954）。

接続時間

VPN クライアントを使用して Windows Vista システムに接続する場合、Windows 2000 または Windows XP システムへの接続時よりも時間がかかる場合があります。実際に接続にかかる時間は、お客様ごとに異なる場合があります。

サポートされていない機能

Cisco VPN Client for Windows Vista では、次の機能はサポートされて*いません*。

- Windows XP から Vista にアップグレードされたシステム（OS のクリーン インストールが必要）。
- Start Before Logon
- 統合ファイアウォール
- InstallShield
- 64 ビットのサポート
- AutoUpdate
- 日本語版オンライン ヘルプ：英語版のみ提供

Cisco VPN クライアントの API

Cisco VPN クライアントは、アプリケーション プログラミング インターフェイス（API）を提供しています。ソフトウェア、サンプル プログラム、マニュアルは、残りの VPN クライアント ダウンロードとともに http://www.cisco.com/cgi-bin/tablebuild.pl/windows から入手できます。ファイル名は APIExample_Rev4.zip です。

CCO アカウントがない場合は、http://tools.cisco.com/RPF/register/register.do にアクセスして、guest アカウントに登録してください。アカウントを登録したら、ファイルを取得できるようにするため、アカウント ID を vpn-client-api-support@cisco.com に転送してください。

（注）　Solaris VPN クライアントは API をサポートしません。

すべての API コマンドで、VPN クライアントの 4.6.x 以降がインストールされている必要があります。

C 言語の使用を考えている場合は、vpnapi.dll を直接呼び出すことを推奨します。ただし、C++ 言語の使用を考えている場合は、zip ファイル中にある例を使用してください。その例は Visual Studio 2005 にも当てはまります。zip ファイル中のマニュアルは C 言語および C++ 言語のいずれにも使用できます。C#、Visual Basic、他のプログラミング言語の例やサポートはありません。既存の例は再コンパイルするためのものではなく、再コンパイルを意図している場合は「safestring」が見つからないというエラーがスローされます。Safestring は適切な文字列を確保する関数に過ぎず、場所を問わず別の string 関数と置き換えたり、書き換えたりできます。

VPN クライアントの設定

この項に記載の手順は、VPN クライアントが接続するすべてのシスコ デバイス プラットフォーム（「中央サイト デバイス」）で共通です。

リモート アクセス ユーザの中央サイト デバイスの設定

VPN クライアント ユーザが中央サイト デバイス経由でリモート ネットワークにアクセスするには、デバイスで次の作業を完了する必要があります。

- 最低限、クイック コンフィギュレーションですべての手順を完了します。
- 属性を作成し、IPsec グループに割り当てます。
- 属性を作成し、IPsec グループのメンバーである VPN クライアント ユーザに割り当てます。
- 事前共有キーではなくデジタル証明書を使用して認証している VPN クライアント ユーザを設定します。

クイック コンフィギュレーションの実行

ほとんどの設定パラメータにデフォルト値または特定のパラメータに指定した値を使用することで、クイック コンフィギュレーションを行うことができます。

デフォルト値を使用したクイック コンフィギュレーション

クイック コンフィギュレーションは次の手順で構成されています。

ステップ 1　セキュア ゲートウェイ イーサネット 1 インターフェイスをプライベート ネットワークに設定します。

ステップ 2　パブリック ネットワークまたは他の外部ネットワークに接続されている他のイーサネット ネットワークを設定します。

ステップ 3　システム名、日付、時刻、DNS、ドメイン名、デフォルト ゲートウェイなどのシステム ID 情報を入力します。

ステップ 4　トンネリング プロトコルおよび暗号化オプションを指定します。

ステップ 5　トンネルが確立されたときに IP アドレスをクライアントに割り当てる方法を指定します。

ステップ 6　内部サーバ、RADIUS、NT Domain、SDI、Kerberos/Active Directory などユーザ認証サーバを選択し、特定します。

ステップ 7　内部認証サーバを使用している場合は、内部ユーザ データベースを読み込みます。

ステップ 8　IPsec トンネリング プロトコルを使用している場合は、名前およびパスワードを IPsec トンネル グループに割り当てます。

ステップ 9　ブラウザ WebVPN を使用している場合は、WebVPN ホーム ページを設定します。

ステップ 10　セキュリティを考えて admin パスワードを変更します。

ステップ 11　コンフィギュレーション ファイルを保存します。この手順を完了したら、クイック コンフィギュレーションは完了です。

デフォルト以外の値を使用したクイック コンフィギュレーション

多数のクイック コンフィギュレーション パラメータに適宜、デフォルト値を指定できますが、これらのうち 1 つ以上のパラメータに特定の値を指定することもできます。次の表に、クイック コンフィギュレーションで必要なパラメータを示し、入力する値を記入するスペースを設けています。データ入力の時間を節約するため、ここに値を書き込んでください。

表 1-2　クイック コンフィギュレーション パラメータ

パラメータ名	パラメータの説明と用途	入力する値
IP Interfaces > Ethernet 1 (Private)	セキュア ゲートウェイ インターフェイスの IP アドレスおよびサブネット マスク、速度、デュプレックス モードをプライベート ネットワークに指定します。	
IP Interfaces > Ethernet 2 (Private)	パブリック ネットワークへのセキュア ゲートウェイ インターフェイスの IP アドレスおよびサブネット マスク、速度、デュプレックス モードを指定します。	
IP Interfaces > Ethernet 3 (External)	左記のように接続されている場合は、他の外部ネットワークのセキュア ゲートウェイ インターフェイスの IP アドレスおよびサブネット マスク、速度、デュプレックス モードを指定します。	
System Info > System Name	（VPN01 など）セキュア ゲートウェイのデバイス名またはシステム名を指定します。	
System Info > DNS Server	ローカル DNS（ドメイン ネーム システム）サーバの IP アドレスを指定します。	
System Info > Domain	（cisco.com など）DNS で使用する登録済みインターネット名を指定します。	

System Info > Default Gateway	特にルーティングされていないパケットのデフォルト ゲートウェイの IP アドレスまたはホスト名を指定します。	
Tunneling	イネーブルにするトンネリング方法および暗号化オプションを指定します。	
Address Assignment > DHCP > Server	リモート アドレス割り当てに Dynamic Host Configuration Protocol（DHCP）を使用している場合は、DHCP サーバの IP アドレスまたはホスト名を指定します。	
Address Assignment > Configured Pool > Range Start and Range End	セキュア ゲートウェイを使用してアドレスを割り当てる場合は、その初期設定プールの開始 IP アドレスと終了 IP アドレスを指定します。	
Authentication	選択内容により、以降の画面で表示されるパラメータが決まります。値は次のとおりです。 Internal Server/Local [Internal Server] を選択することは、内部 VPN Concentrator ユーザ認証サーバを使用するということです。[User Database] 画面で、ユーザごとにユーザ名とパスワードを指定します。 また、ユーザ単位のアドレス割り当てを指定する場合は、ユーザごとに IP アドレスとサブネット マスクを指定します。 RADIUS 外部 RADIUS ユーザ認証サーバを使用している場合は、その IP アドレスまたはホスト名、ポート番号、およびサーバ秘密キーまたはパスワードを指定します。 NT Domain 外部 Windows NT ドメイン ユーザ認証サーバを使用している場合は、その IP アドレス、ポート番号、およびプライマリ ドメイン コントローラ ホスト名を指定します。 SDI 外部 SDI ユーザ認証サーバを使用している場合は、その IP アドレスおよびポート番号を指定します。 Kerberos/Active Directory 外部 Kerberos/Active Directory 認証サーバを使用している場合は、その IP アドレス、ポート番号、および領域を指定します。	
User Database > Group Name, Password, Verify	IPsec トンネリング プロトコルをイネーブルにする場合は、IPsec トンネル グループの名前とパスワードを指定します。	セキュリティを考えて、ここではパスワードを記入しないでください。

IPsec Group	リモート アクセス IPsec クライアントのグループ名およびパスワードを決定します。
WebVPN	WebVPN をイネーブルにする場合は、デフォルト HTTPS、POP3S、SMTPS、または IMAP4S サーバを指定します。
WebVPN Home Page	HTTPS を使用して WebVPN をイネーブルにする場合は、WebVPN ホーム ページに表示するテキストおよび URL を設定します。

- 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。

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。

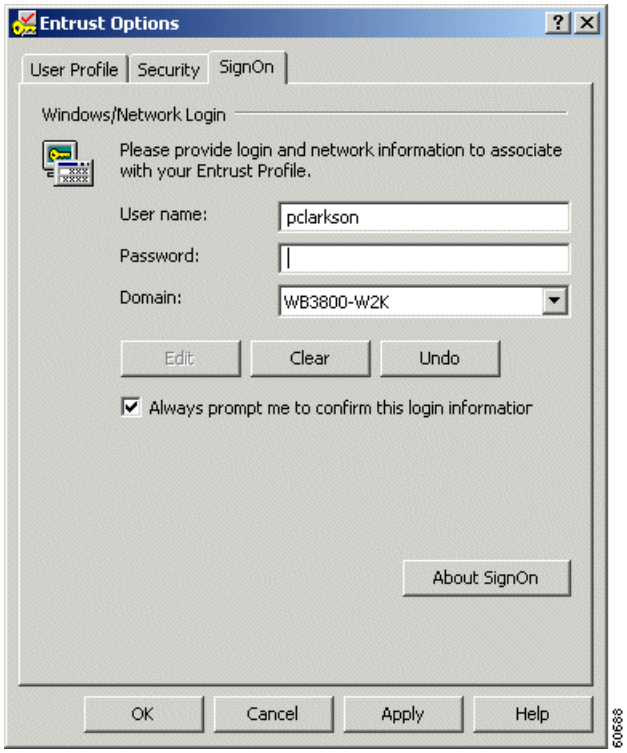
- Entrust Entelligence 参照番号
- Entrust Entelligence 認証コード
- プロファイルを保存するディレクトリの名前
- プロファイルの名前
- Entrust 管理者が設定したルールに従ったパスワード

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 1-1 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。このチェックボックスをオンにすると、[Entrust SignOn login] ダイアログボックスが一時停止し、リモート ユーザがログイン情報を入力する前に VPN 接続が表示できるようになります。

図 1-1　[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 Vista と Windows XP の場合、このディレクトリは c:¥Windows¥system32 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 カードをその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、PIN またはパスコードを入力してスマート カードにアクセス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。

たとえば ASDM を使用して、次の手順を実行します。

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　接続プロファイルまたはトンネル グループを次のように変更します。

a.　証明書認証を設定します。

b.　スマート カード証明書の使用をイネーブルにします。

VPN クライアント ユーザは、スマート カードが PC の正しいポートに差し込まれたそのリーダーに挿入され、正しい PIN またはパスコードを入力した場合のみ認証を完了できます。

（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。

（注）　この機能をバイパスし、エントリ BypassCardPinReset=1 を vpnclient.ini ファイルに追加して、以前の VPN クライアント リリースの動作を保持できます。ただし、スマート カードの Cryptographic Service Provider（CSP）がキャッシュされた PIN を無視し、秘密キーにアクセスする PIN をユーザに求める場合、この回避方法は効果がありません（CSCsb73937）。

相互グループ認証の設定

この項は、管理者が VPN クライアント システムおよび中央サイト デバイスで認証を設定する場合に役立つ情報を記載します。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。

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。

IKE パラメータの設定

この機能では、VPN 接続を使用する場合のシステム全体の値を設定できます。次の項では、各オプションについて説明します。

インターフェイスでの IKE のイネーブル化

VPN 接続を使用するインターフェイスごとに、IKE をイネーブルにする必要があります。

IPsec over NAT-T のイネーブル化

NAT-T により IPSec ピアは、リモート アクセスとサイト間の両方の接続を NAT デバイスを介して確立できます。NAT-T は UDP データグラムの IPsec トラフィックをカプセル化し、ポート 4500 を使用して、NAT デバイスにポート情報を提供します。NAT-T はすべての NAT デバイスを自動検出し、必要な場合だけ IPsec トラフィックをカプセル化します。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。

- セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-T、および IPSec over UDP を同時にサポートできます。
- NAT-T と IPsec over UDP の両方がイネーブルになっている場合、NAT-T が優先されます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

セキュリティ アプライアンスによる NAT-T の実装では、次の場合において、単一の NAT/PAT デバイスの背後にある IPSec ピアをサポートします。

- サイト間接続 1 つ。
- サイト間接続または複数のリモート アクセス クライアントのいずれか。ただし、両方を混在させることはできません。

NAT-T を使用するには、次の手順を実行する必要があります。

- セキュリティ アプライアンスのポート 4500 を開きます。
- このパネルで、IPSec over NAT-T をグローバルにイネーブルにします。
- フラグメンテーション ポリシーに適切なオプションを選択します。これらのオプションにより、トラフィックは、IP フラグメンテーションをサポートしていない NAT デバイス間を移動できます。これによって、IP フラグメンテーションをサポートする NAT デバイスの動作が妨げられることはありません。

IPsec over TCP の有効化

IPSec over TCP を使用すると、標準 ESP や標準 IKE が機能できない環境、または既存のファイアウォール ルールを変更した場合に限って機能できる環境で、VPN クライアントが動作可能になります。IPSec over TCP は TCP パケット内で IKE プロトコルと IPSec プロトコルをカプセル化し、NAT と PAT の両方のデバイスおよびファイアウォールによりセキュアなトンネリングを実現します。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。

（注）　この機能は、プロキシベースのファイアウォールでは動作しません。

IPsec over TCP は、リモート アクセス クライアントで動作します。また、すべての物理インターフェイスと VLAN インターフェイスでも動作します。これは、セキュリティ アプライアンス機能に対応するクライアントに限られます。サイト間接続では機能しません。

- セキュリティ アプライアンスは、データ交換を行うクライアントに応じて、標準の IPSec、IPSec over TCP、NAT-Traversal、および IPSec over UDP を同時にサポートできます。
- 1 度に 1 つのトンネルをサポートする VPN 3002 ハードウェア クライアントは、標準の IPsec、IPsec over TCP、NAT-Traversal、または IPsec over UDP を使用して接続できます。
- イネーブルになっている場合、IPsec over TCP は他のすべての接続方式よりも優先されます。

セキュリティ アプライアンスとその接続先のクライアントの両方で IPsec over TCP をイネーブルにします。

最大 10 個のポートを指定して、それらのポートに対して IPsec over TCP をイネーブルにできます。ポート 80（HTTP）やポート 443（HTTPS）などのウェルノウン ポートを入力すると、そのポートに関連付けられているプロトコルが機能しなくなることを示す警告がシステムに表示されます。その結果、ブラウザを使用して、IKE がイネーブルのインターフェイスからセキュリティ アプライアンスを管理できなくなります。この問題を解決するには、HTTP/HTTPS 管理を別のポートに再設定します。

セキュリティ アプライアンスだけでなく、クライアントでも TCP ポートを設定する必要があります。クライアント設定には、セキュリティ アプライアンスに対して設定したポートを少なくとも 1 つ含める必要があります。

識別方式の決定

IKE ネゴシエーションでは、ピアが相互に相手を識別する必要があります。この識別方式は、次のオプションから選択できます。

表 1-3　IKE 識別方式

パラメータ	使用目的
アドレス	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
ホスト名	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
キー ID	リモート ピアが事前共有キーの検索に使用する文字列を使用します。
自動	接続タイプによって IKE ネゴシエーションを決定します。 • 事前共有キーの IP アドレス • 証明書認証の cert DN。

インバウンド Aggressive モード接続のディセーブル化

フェーズ 1 の IKE ネゴシエーションでは、Main モードと Aggressive モードのいずれかを使用できます。どちらのモードも同じサービスを提供しますが、Aggressive モードの場合にピア間で必要とされる交換処理は、3 つではなく 2 つだけです。Agressive モードの方が高速ですが、通信パーティの ID は保護されません。そのため、情報を暗号化するセキュアな SA を確立する前に、ピア間で ID 情報を交換する必要があります。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。

接続解除の前にピアに警告

セキュリティ アプライアンスのシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、または管理者による停止などのいくつかの理由で、クライアント セッションまたはサイト間セッションがドロップすることがあります。

セキュリティ アプライアンスは、（サイト間コンフィギュレーションの場合）限定されたピアである、VPN クライアントと VPN 3002 ハードウェア クライアントに、セッションが接続解除される直前に通知し、その理由を伝えることができます。アラートを受信したピアまたはクライアントは、その理由を復号化してイベント ログまたはポップアップ パネルに表示します。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。

このパネルでは、セキュリティ アプライアンスがこれらのアラートを送信し、接続解除の理由を伝えることができるように、通知機能をイネーブルにできます。

限定されたクライアントとピアには次のものが含まれます。

- アラートがイネーブルになっているセキュリティ アプライアンス デバイス。
- バージョン 4.0 以降のソフトウェアを実行している VPN クライアント（設定は不要）。
- 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3002 ハードウェア クライアント。
- バージョン 4.0 以降のソフトウェアを実行し、アラートがイネーブルになっている VPN 3000 シリーズ Concentrator。

この機能は、次のクライアントには適用されません。

- Cisco AnyConnet VPN Client
- Cisco IOS ソフトウェア
- Cisco Secure PIX Firewall

IKE キープアライブを使用する場合の特記事項

ISAKMP（IKE）キープアライブ設定機能により、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 アプライアンスとそのリモート 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 4.0 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。グループ ポリシーを設定する場合に、アイドル タイムアウトを変更できます。

（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。

リブート前のアクティブ セッションの終了を待機

すべてのアクティブ セッションが自発的に終了した場合に限り、中央サイトのデバイスがリブートするようにスケジュールを設定できます。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。

次に一般的な手順を説明します。特定のコンフィギュレーション パラメータについて使用している環境に特化した章を参照してください。

ステップ 1　IKE をイネーブルにします。

ステップ 2　適宜、NAT 透過をイネーブルにします。

ステップ 3　このデバイスのピアに送信するデバイスの ID を指定します。これにより、IPSec のピアがお互いを識別する方法を設定できます。

ステップ 4　[Disable inbound aggressive mode connections]：アグレッシブ モードの接続をディセーブルにする場合に選択します。

ステップ 5　[Alert peers before disconnecting]：セッションを接続解除する前に、セキュリティ アプライアンスから限定されたサイト間ピアとリモート アクセス クライアントに通知する場合に選択します。

ステップ 6　[Wait for all active sessions to voluntarily terminate before rebooting]：セキュリティ アプライアンスにより、すべてのアクティブなセッションが終了するまで、予定されたリブートを延期させる場合に選択します。

（注）　IKE メイン モードを使用するサイト間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。

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。

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。

クライアント ファイアウォールの概要

この項では、ネットワーク管理者がセキュア ゲートウェイ通信ポリシー情報から Windows プラットフォームで動作する VPN クライアントへパーソナル ファイアウォール機能を制御する方法の概要を説明しています。

オプション設定と必須設定

セキュア ゲートウェイでは、VPN クライアントが指定のファイアウォール設定を使用する、またはこの設定を任意指定にすることができます。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 クライアントが接続しようとすると、クライアント PC に任意のファイアウォールがインストールされていることがセキュア ゲートウェイに通知されます。セキュア ゲートウェイは、どのファイアウォールを VPN クライアントが使用する必要があるかについての情報を返信します。ファイア

ウォール設定が任意に指定されている場合、セキュア ゲートウェイは VPN クライアントに、不一致はあるものの、VPN クライアントはトンネルを確立できることを通知できます。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。ポリシーはセキュア ゲートウェイから制御されません。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*とも呼ばれており、ネットワーク管理者は、VPN クライアントがセキュア ゲートウェイにトンネリングされている間に、インターネット トラフィックを許可またはドロップするルール セットを定義できます。ネットワーク管理者はセキュア ゲートウェイでこのポリシーを定義し、接続ネゴシエーション中にポリシーは 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、セキュア ゲートウェイへのセキュア接続を終了します。この場合、セキュア ゲートウェイ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 はセキュア ゲートウェイと通信し、接続の確立および終了、セッションおよびユーザ情報の交換、および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 の VPN クライアントと通信し、サーバ アドレスを取得し、セキュア ゲートウェイとステータス情報を交換します。

- セキュア ゲートウェイ：グループごとにファイアウォール機能を設定する方法を提供します。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。またセキュア ゲートウェイは IS と通信し、セッションの確立および終了、セッションおよびユーザ情報の交換、および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 で、セキュア ゲートウェイから IS のアドレスと情報を取得し、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。

接続が完了し、IS がファイアウォール ポリシーを IA に伝えると、IS と IA はハートビート メカニズムで通信します。

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
```

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。

最初に、ASDM オンライン ヘルプまたは『ASDM User Guide』、『*Cisco Adaptive Security Appliance Configuration Guide*』、または『*VPN 3000 Series Concentrator Reference Volume 1: Configuration*』のスプリット トンネリングの項をよくお読みください。

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。

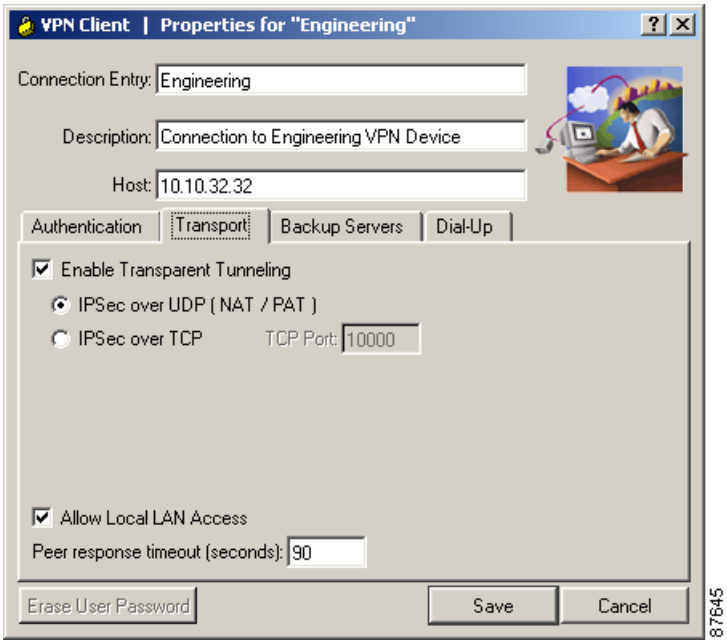
- VPN クライアントのローカル LAN アクセスをイネーブルにする。
- VPN 3000 Concentrator 上の特定のグループ内でローカル LAN アクセスをイネーブルにする。
- アクセス可能なネットワークをネットワーク リストに追加する（またはデフォルト ネットワーク アドレスを使用する）。

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 1-2　VPN クライアントでの [Allow Local LAN Access Parameter] の設定



ステップ 2　セキュア ゲートウェイで、次のように新しいグループを追加するか、既存のグループを変更します。

a. Split Tunneling Policy 属性を [Tunnel everything] として設定し、[Allow the networks in list to bypass the tunnel] を選択します。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。

b. スプリット トンネリング ネットワーク リストで、ローカル LAN アクセスに作成したネットワーク リストがある場合は、それを選択します。

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 リストの作成方法の詳細については、ASDM オンライン ヘルプ、『ASDM User Guide』、『*Cisco Adaptive Security Appliance Configuration Guide*』、または『*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
```

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 ユーザがセキュア ゲートウェイに接続すると、VPN クライアントはセキュア ゲートウェイから 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。

ネットワーク管理者は、セキュア ゲートウェイでこの設定を構成します。

（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。

中央サイト デバイスでの VPN クライアントの設定

Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイス（CLI）を使用して、Cisco ASA 5500 シリーズ セキュリティ アプライアンスまたは Cisco VPN 3000 シリーズ Concentrator で VPN クライアントを設定できます。以降の章では、これらの環境それぞれの手順について説明します。