アドミニストレーション ガイド

Cisco Small Business

RVS4000 4 ポート ギガビット VPN セキュリティ ルータ

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

78-19997-02

目　次

1

はじめに

Cisco RVS4000 4 ポート ギガビット VPN セキュリティ ルータをお買い上げいただき、誠にありがとうございます。4 ポート ギガビット VPN セキュリティ ルータは、スモール ビジネスのニーズに対応するインターネット共有型の高度なネットワーク ソリューションです。他のルータと同じように、このルータからオフィスにある複数のコンピュータをインターネットに接続させられます。

また 4 ポート ギガビット VPN セキュリティ ルータには、4 ポートの全二重方式 10/100/1000 イーサネット スイッチが内蔵されているため、4 台の PC を直接接続できます。また、必要に応じてハブやスイッチを追加接続することにより、大規模なネットワークを構築することもできます。

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）機能によりインターネットを介して暗号化した「トンネル」が作成されるため、最大 5 つのリモートおよび最大 5 人の移動ユーザがオフサイトからオフィス ネットワークに安全に接続できます。VPN トンネルを介して接続するユーザは、社内にいるのと同じように社内ネットワークに接続でき、ファイル、E メール、およびイントラネットに安全にアクセスできます。また、VPN 機能を使用して、スモール オフィス ネットワークのユーザには社内ネットワークへの安全な接続を許可することができます。Quality of Service（QoS）機能によりビジネス全体を通じて一貫性のある音声とビデオの品質が提供されます。

4 ポート ギガビット VPN セキュリティ ルータは、DHCP サーバとしても機能するほか、強力な SPI ファイアウォールと Intrusion Prevention System（IPS; 侵入防御システム）を装備しているため、侵入者や広く知られたインターネット攻撃のほとんどからユーザの PC を保護することができます。ルータは、内部ユーザによるインターネットへのアクセスをフィルタするように設定できます。また、IP および MAC アドレス フィルタを設定することにより、社内ネットワークへのアクセスを許可するユーザを正確に指定することができます。Web ブラウザ ベースの設定ユーティリティを利用すれば、設定は簡単に実行できます。

このアドミニストレーション ガイドでは、ルータの接続、セットアップ、および設定について総合的に説明します。

2

ネットワーキングとセキュリティの基本事項

この章では、ネットワーキングとセキュリティの基本事項について説明します。この章の内容は次のとおりです。

LAN の導入説明

ルータは、2 つのネットワークを接続するためのネットワーク デバイスです。

ルータにより、Local Area Network（LAN; ローカル エリア ネットワーク）、つまり自宅やオフィスにある一連の PC をインターネットに接続することができます。ルータは、こうした 2 つのネットワークの間を行き来するデータを処理したり、規制したりします。

ルータの Network Address Translation（NAT; ネットワーク アドレス変換）テクノロジーにより、PC のネットワークが保護されるため、自分の PC がインターネット上の別のユーザから「見られる」ことはありません。この機能により、LAN のプライバシーが守られます。ルータでは、いずれかのイーサネット ポートにある最終的な宛先に向けてパケットを転送する前に、まずインターネット ポートを介して受信された最初のパケットを検査することによって、ネットワークを保護します。ルータは、Web サーバ、FTP サーバ、その他のインターネット アプリケーションといったインターネット ポート サービスの検査を行い、許可されれば、LAN 側の該当する PC にパケットを転送します。

IP アドレスの使用方法

IP は、Internet Protocol（インターネット プロトコル）の略称です。PC、プリント サーバ、およびルータを含め、IP ベース ネットワークにある個々のデバイスには、ネットワークにおけるそれぞれのロケーション、またはアドレスを識別するための IP アドレスが必要になります。これは、インターネットと LAN の両方の接続に適用されます。

ネットワーク デバイスに IP アドレスを割り当てる方法は 2 つあります。

スタティック IP アドレスは、ネットワーク上の PC またはその他のデバイスに手動で割り当てる静的な IP アドレスです。スタティック IP アドレスは、ユーザが無効にするまで有効になるため、スタティック IP アドレスが割り当てられたデバイスには、ユーザが変更しない限り、常に同じ IP アドレスが使用されます。スタティック IP アドレスは、サーバ PC やプリント サーバのようなネットワーク デバイスとともに使用されます。

ルータを使用して、ケーブルや DSL による接続を共有する場合は、ISP に問い合せて、自分のアカウントにスタティック IP アドレスが割り当てられているかを確認してください。スタティック IP アドレスが割り当てられている場合は、ルータの設定時にこのアドレスが必要になります。必要な情報は ISP より入手できます。

ダイナミック IP アドレスは、ネットワーク上の特定のデバイスに自動的に割り当てられるアドレスです。これらの IP アドレスは、PC、その他のデバイスに一時的に割り当てられるという意味でダイナミック（動的）と呼ばれます。ダイナミック IP アドレスは、一定の期間が経過すると、期限が満了するため、アドレスが変わる可能性があります。ある PC でネットワーク（またはインターネット）にログインし、そのダイナミック IP アドレスの期限が満了すると、DHCP サーバにより、別のダイナミック IP アドレスが割り当てられます。

DHCP サーバには、ネットワーク上の指定された PC、またはその他のネットワーク デバイス（たとえばルータ）がなることができます。デフォルトで、ルータのインターネット接続タイプは、**IP アドレスを自動的に取得する**（DHCP）ように設定されます。

特定の IP アドレスを含む PC またはネットワーク デバイスのことを DHCP クライアントと呼びます。DHCP により、ネットワークに新規のユーザを追加するときにマニュアルで IP アドレスを割り当てる必要がなくなります。

DSL ユーザの場合、多くの ISP がインターネットへのアクセスを確保するためにユーザ名とパスワードを使用したログインを要求することがあります。DSL は、Point to Point Protocol over Ethernet（PPPoE）という専用の高速接続回線です。PPPoE はダイヤルアップ接続に似ていますが、接続の確立時に電話番号のダイヤルは行いません。ダイナミック IP アドレスを割り当てたルータにより、インターネットへの接続を確立します。

DHCP サーバ（LAN 側のサーバ）は、デフォルトによりルータ上で有効になります。ネットワーク上にすでに別の DHCP サーバが設定されている場合は、2 つの DHCP サーバのうち一方を無効にする必要があります。ネットワーク上で複数の DHCP サーバを実行すると、IP アドレスの競合といったネットワーク エラーが生じます。ルータの DHCP を無効にする方法については、**第 5 章「ルータのセットアップおよび設定」**の基本セットアップに関するセクションを参照してください。

（注） ルータは、2 つのネットワークを接続するデバイスであるため、IP アドレスが 2 つ（LAN 用として 1 つ、インターネット用として 1 つ）必要になります。このアドミニストレーション ガイドでは、「インターネット IP アドレス」および「LAN IP アドレス」について言及しています。

ルータでは、NAT テクノロジーが使用されているため、当該のネットワークについてインターネットから見ることのできる IP アドレスは、ルータのインターネット IP アドレスだけです。ただし、このインターネット IP アドレス自体もブロックが可能であるため、該当するルータとネットワークをインターネット上で非表示にすることもできます。

侵入防御システム（IPS）

IPS は、ネットワークを悪意ある攻撃から保護するための高度なテクノロジーです。IPS は、SPI ファイアウォール、IP ベースの Access Control List（ACL; アクセス コントロール リスト）、Network Address Port Translation（NAPT）、および Virtual Private Network（VPN; バーチャル プライベート ネットワーク）と組み合わせることにより、最も高いレベルのセキュリティを実現できます。IPS は、ルータ中のインライン モジュールとしてリアルタイムの検出と防御を行います。

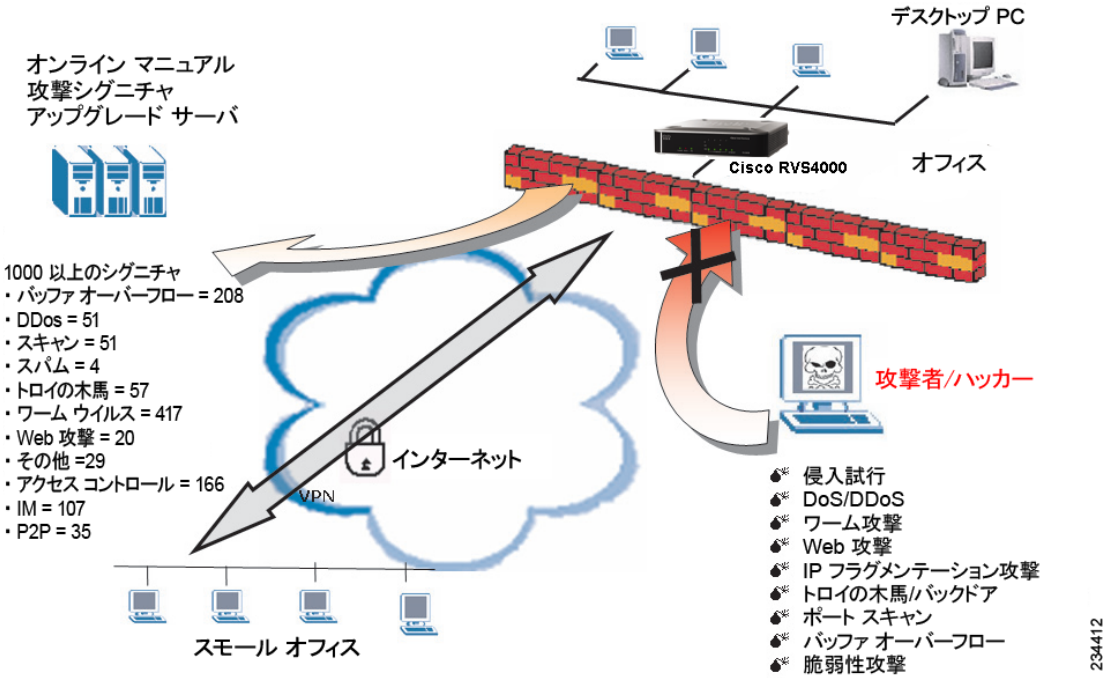
RVS4000 には、悪意ある攻撃を検出できるように、リアルタイムのパターンマッチを行うためのハードウェア ベース アクセラレーションが組み込まれています。このアクセラレーション機能により、TCP/UDP/ICMP/IGMP の悪意あるパケットが積極的にフィルタ、およびドロップされます。また TCP 接続をリセットできます。この機能によって、Windows、Linux、および Solaris を含む各オペレーティング システムで動作するクライアント PC、およびサーバがネットワーク ワームによる攻撃から保護されます。ただし、このシステムでは E メール添付に含まれるウイルスを防止できません。

Peer-to-Peer（P2P; ピアツーピア）、および Instant Messaging（IM; インスタント メッセージング）のコントロールにより、システム管理者は、ネットワーク ユーザがこれらのプロトコルによりインターネットを介して別のユーザとやり取りするのを防止できます。これにより、管理者はインターネットの帯域幅を効果的に使用する方法について、企業のポリシーを定めることができます。

シグニチャ ファイルは、IPS システムの中心となるものです。シグニチャ ファイルは、PC のアンチウイルス ソフトウェアに含まれるウイルス定義ファイルに似た働きをします。IPS ではシグニチャ ファイルを使用して、ルータに着信するパケットの照合を行い、状況に応じたアクションを実行します。RVS4000 には、DDoS、バッファ オーバーフロー、アクセス コントロール、スキャン、トロイの木馬、P2P、IM、ウイルス、ワーム、Web 攻撃、その他といったカテゴリに対応する 1000 を超えるルールを定めたシグニチャ ファイルがあります。

お客様には、インターネットに登場する新種の攻撃から守るためにご使用の IPS シグニチャ ファイルを定期的に更新することをお勧めします。

IPS のシナリオ



3

バーチャル プライベート ネットワーク（VPN）の計画

この章では、VPN の計画に関連する情報について説明します。この章の内容は次のとおりです。

VPN が必要な理由

コンピュータ ネットワーキングにより、旧来の紙ベースのシステムでは考えられなかったような柔軟性が提供されるようになっています。その一方で、この柔軟性によりセキュリティの面でのリスクが拡大しています。このようなリスクに対応する技術がファイアウォールです。ファイアウォールによって、ローカル ネットワークの内部にあるデータが保護されます。一方、E メールが宛先に到着したときや、ホテルやリモート オフィスから社内ネットワークに接続したときに、ローカル ネットワークから送出される情報についてはどのように対処したらよいのでしょう。社内のデータはどのように保護されるのでしょう。

この場合に役立つのが VPN です。VPN が「バーチャル（仮想）」プライベート ネットワークと呼ばれるのは、社内のネットワークから送信されるデータが実際にまだそのネットワーク内に存在するかのように、その安全性が確保されるという理由によります。

データがコンピュータから出てインターネット上を移動するときは、常に攻撃の危険にさらされます。すでにファイアウォールを設定して、ネットワークのデータがネットワーク外部のエンティティによる破損や傍受から保護するための対策が講じられている場合もあるでしょう。しかし、データがネットワークの外部に向かって出て行く場合、つまり E メールを介して他のユーザにデータを送信したり、インターネットを介して他のユーザとやり取りを行ったりする場合、ファイアウォールはそのデータを保護できません。

この時点でそのデータは、さまざまな手法を駆使して盗用を試みるハッカーによる攻撃の対象になり得るということです。さらにハッカーは転送されるデータに限らず、ネットワーク ログインやセキュリティ データも狙っています。次のページに、最も一般的な手法の一部をまとめてあります。

1）MAC アドレス スプーフィング

ローカル ネットワークやインターネットといったネットワークを介して転送されるパケットの前にはパケット ヘッダーが付いています。これらのパケット ヘッダーには、当該のパケットを効率的に転送するための送信元と送信先の両方の情報が含まれています。ハッカーはこの情報を利用して、ネットワーク上で許可された MAC アドレスのスプーフィング（なりすまし）を試みます。ハッカーは、スプーフィングした MAC アドレスを利用して、本来、別のユーザに宛てられた情報を傍受することもできます。

2）データ スニフィング

ハッカーは、ネットワーク データが安全性の低いネットワーク（たとえばインターネット）を移動するときに、「スニフィング」によってデータを手に入れます。プロトコル アナライザやネットワーク診断ツールなど、この種のアクティビティ用のツールは、オペレーティング システムの内部に組み込まれていることが多いため、データがクリア テキストのまま表示されることになります。

3）中間者攻撃

ハッカーは、スニフィングやスプーフィングによって十分な情報を手にすると、「中間者攻撃」を実行できるようになります。ハッカーは、あるネットワークから別のネットワークにデータが転送されるときに、このデータを別の宛先に再ルーティングすることにより、中間者攻撃を行います。データが実際には、意図した受信者には到達していない場合でも、発信者には送信が成功したように見えます。

これらは、ハッカーが使用する手法の一部にすぎず、絶えず新しい手法が考案されています。VPN のセキュリティが欠けていると、データがインターネット上を移動するときに、常にこのような攻撃の対象になり得ます。インターネット上を移動するデータは、世界中のさまざまなサーバを通過してから最終的な宛先に到着します。これはセキュリティ対策のないデータにとっては、長い行程です。こうした状況で、VPN がその効果を発揮します。

VPN とは

VPN（バーチャル プライベート ネットワーク）は、異なるネットワークにある VPN ルータなどの 2 つのエンドポイントを接続するもので、インターネットのような共有型、つまりパブリックのネットワークを介してプライベートなデータを安全に送信できるようにします。VPN により、2 つのロケーション、またはネットワークの間で安全なデータ送信を保証するプライベート ネットワークが確立されます。

これは「トンネル」の作成によって行います。VPN により、2 つの PC、またはネットワークが接続されるため、やり取りするデータがそれぞれのネットワーク内に存在する場合と同じように、インターネットを介したデータ転送が可能になります。文字どおりの「トンネル」という意味ではなく、2 つネットワークの間でやり取りするデータを暗号化して、接続の安全性を確保するということです。

VPN は、プライベート ネットワークに対する私設の専用回線を敷設する方法に代わるコスト効果に優れた技術として考案されたものです。VPN では、業界標準の暗号化および認証の手法である IPSec（IP Security の略称）を使用することにより、ローカル ネットワークに直接接続されているのと同じように動作する実質的に安全な接続が確立されます。VPN を使用して、セントラル オフィスと支店、在宅勤務者、出張中の専門家を結ぶ安全なネットワークを構築できます（出張先からは、Cisco QuickVPN クライアント ソフトウェアを実行した任意のコンピュータから VPN ルータに接続できます）。

VPN 接続は次の 2 つの方法で設定できます。

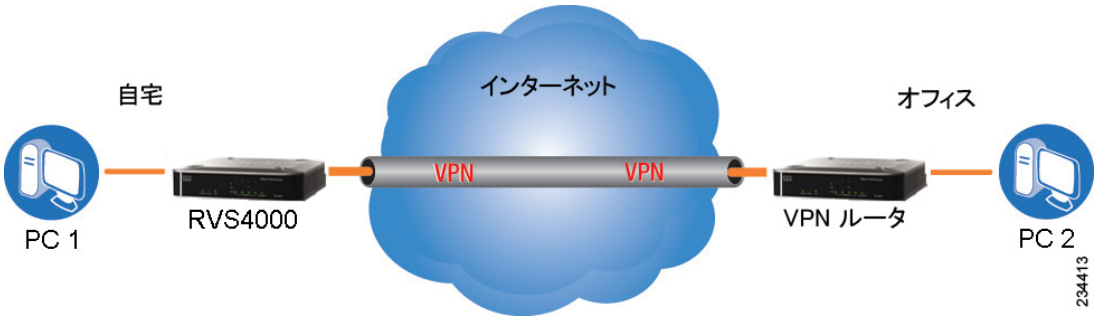
- VPN ルータと VPN ルータの接続
- コンピュータと VPN ルータの接続（Cisco QuickVPN クライアント ソフトウェアを使用）

VPN ルータにより、2 つのエンドポイントの間に「トンネル」、またはチャネルが設定されるため、データの転送が安全に実行されます。Cisco QuickVPN クライアント ソフトウェアを実行したコンピュータは、2 つのエンドポイントのいずれか一方になることができます（**付録 B「Windows 2000、XP または Vista での Cisco QuickVPN の使用」**を参照してください）。VPN クライアント ソフトウェアを実行しない場合は、IPSec Security Manager を内蔵するいずれかのコンピュータ（Microsoft 2000 および XP）を使用することで、VPN ルータで IPSec を使用して VPN トンネルを作成できます（**付録 C「Windows 2000/XP コンピュータでの IPSec の設定」**を参照してください）。これ以外の Microsoft オペレーティング システムでは、サードパーティの VPN クライアント ソフトウェア アプリケーションを追加して、IPSec をインストールできるようにする必要があります。

VPN ルータと VPN ルータの接続

VPN ルータと VPN ルータを接続することにより、在宅勤務者は自分の VPN ルータを使用してインターネットに常時接続できます。在宅勤務者のルータには、会社の VPN 設定が適用されます。在宅勤務者が会社のルータに接続すると、2 つのルータの間に VPN トンネルが設定され、データの暗号化と復号化が行われます。VPN でインターネットを利用するときに、物理的な距離は問題になりません。VPN を使用している間、在宅勤務者には、セントラル オフィスのネットワークに物理的に接続されている場合と同じように、安全な接続が提供されます。詳細については、**付録 D「ゲートウェイ間 VPN トンネル」**を参照してください。

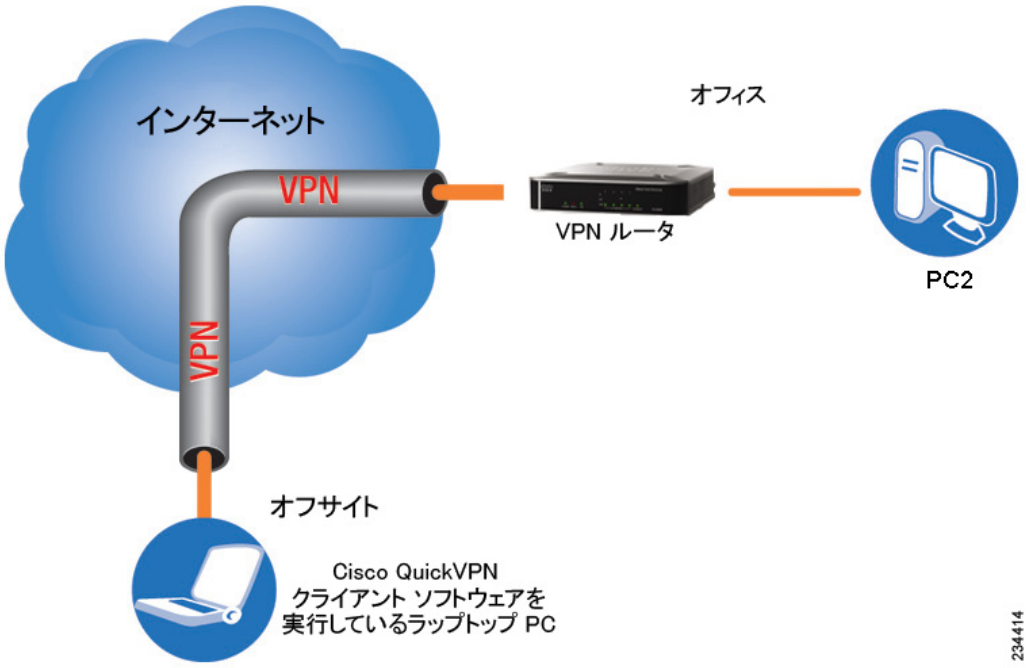
VPN ルータと VPN ルータの接続



コンピュータと VPN ルータの接続（Cisco QuickVPN クライアント ソフトウェアを使用）

この図は、コンピュータと VPN ルータを接続した VPN の例を示したものです。ホテルの部屋で、出張中の社員が自分の ISP に接続します。ノートブック コンピュータの Cisco QuickVPN クライアント ソフトウェアには会社の IP アドレスが設定されています。Cisco QuickVPN クライアント ソフトウェアにアクセスして、セントラル オフィスの VPN ルータに接続します。VPN でインターネットを利用するときに、物理的な距離は問題になりません。VPN を使用している間、このユーザには、セントラル オフィスのネットワークに物理的に接続されている場合と同じように、安全な接続が提供されます。

コンピュータと VPN ルータの接続



独自の VPN の作成に関する情報と説明については、www.cisco.com を参照してください。また、**付録 B「Windows 2000、XP または Vista での Cisco QuickVPN の使用」**、**付録 C「Windows 2000/XP コンピュータでの IPSec の設定」**、および**付録 D「ゲートウェイ間 VPN トンネル」**も参照してください。

4

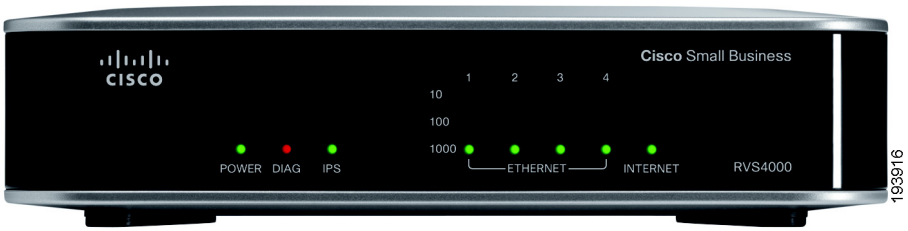
RVS4000 ルータ スタートアップ ガイド

この章では、RVS4000 ルータの物理的特長、およびルータの設置方法について説明します。この章の内容は次のとおりです。

前面パネル

LED は、ルータの前面パネルに配置されています。

前面パネル



[POWER] LED：ルータの電源がオンのときにグリーンに点灯します。診断テストの実行中は、LED が点滅します。

[DIAG] LED：システムの準備が完了すると、消灯します。ファームウェアのアップグレード中はレッドに点滅します。

[IPS] LED：Intrusion Prevention System（IPS; 侵入防御システム）機能が有効になるとグリーンに点灯します。IPS 機能が無効のときは、消灯します。外部からの攻撃が検出されると、グリーンで点滅します。内部の攻撃が検出されると、レッドで点滅します。

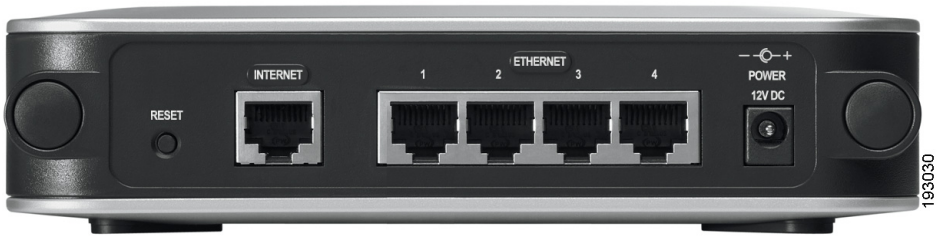
[ETHERNET] ポート LED（1 ～ 4）：各 LAN ポートに 3 つの LED があります。ルータが、対応するポート（1 ～ 4）を通じて指定の速度でデバイスに接続されると、グリーンに点灯します。そのポートでデータのアクティブな送受信が実行されているときは、グリーンで点滅します。

[INTERNET] LED：グリーンに点灯して、インターネット ポートに接続されたデバイスの回線速度を示します。点滅はアクティビティがあることを示します。ルータがケーブルまたは DSL モデムに接続されている場合、通常 [100] LED だけが点灯し、速度が 100 Mbps であることを示します。

背面パネル

イーサネット ポート、インターネット ポート、リセット ボタン、電源ポートはルータの背面パネルにあります。

背面パネル



[RESET] ボタン：[RESET] ボタンには 2 つの使用方法があります。

- ルータとインターネットとの接続に問題が生じた場合、[RESET] ボタンをクリップや鉛筆の先で短時間押します。これは、PC のリセット ボタンを押してリブートするのと似ています。
- ルータに深刻な問題が発生していて、他のトラブルシューティングもすべて実行済みの場合は、[RESET] ボタンを 10 秒間押し続けます。これにより工場出荷時設定が復元され、ポート フォワーディングや新規パスワードといったすべてのルータ設定がクリアされます。

[INTERNET] ポート：ケーブル モデムまたは DSL モデムとの WAN 接続に使用します。

[ETHERNET] ポート（1 ～ 4）：PC やプリント サーバ、追加スイッチといったネットワーク デバイスとの LAN 接続に使用します。

[POWER] ポート：付属の AC 電源アダプタで電源に接続します。

設置オプション

このルータは、ゴム足を使用した横置き設置、スタンドへの取り付け、壁面への取り付けが可能です。

デスクトップへの設置

デスクトップに設置する場合は、Cisco RVS4000 ルータを平面に水平に置き、4 本のゴム足で支えるようにします。

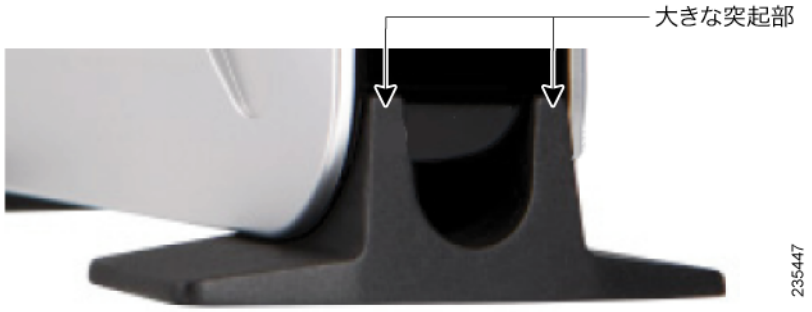
スタンドでの設置

付属のスタンドを使用して縦置きで設置する場合、次の手順を実行します。

ルータを縦置き設置するには、次の手順に従います。

ステップ 1 ルータの左側面パネルを確認します。

ステップ 2 片方のスタンドの 2 つの大きな突起部を外側に向け、短い突起部をルータにある小さなスロットへ差し込み、カチッとはまるまでスタンドを押し込みます。



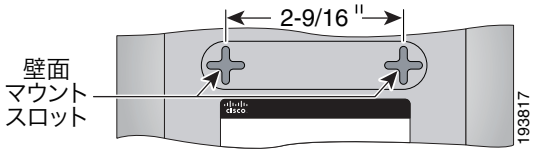
ステップ 3 もう一方のスタンドでも手順 2 を繰り返します。

壁面への設置

Cisco RVS4000 ルータを壁面に設置するには、次の手順に従います。

ステップ 1 ルータを設置する位置を決め、ネジ 2 本（付属していません）を約 64.5 mm（2-9/16 インチ）間隔で取り付けます。

ステップ 2 背面パネルを上に向け（縦置き設置の場合）、ルータの底面にある十字形の壁面マウント スロットが 2 本のネジと揃うようにルータの位置を合わせます。



ステップ 3 壁面マウント スロットをネジの上に配置し、ネジが壁面マウント スロットにぴったりと合うまで、ルータをスライドさせます。

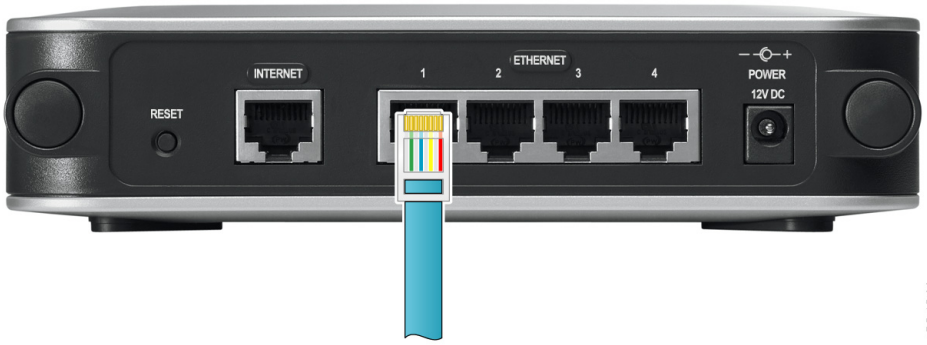
ルータの設置

ルータを設置する前の準備として、次の作業を実施します。

- Internet Service Provider（ISP; インターネット サービス プロバイダー）から、使用中のインターネット接続タイプに適した設定情報を入手します。
- ルータや PC、ケーブル モデム、DSL モデムを含め、すべてのネットワーク ハードウェアの電源をオフにします。

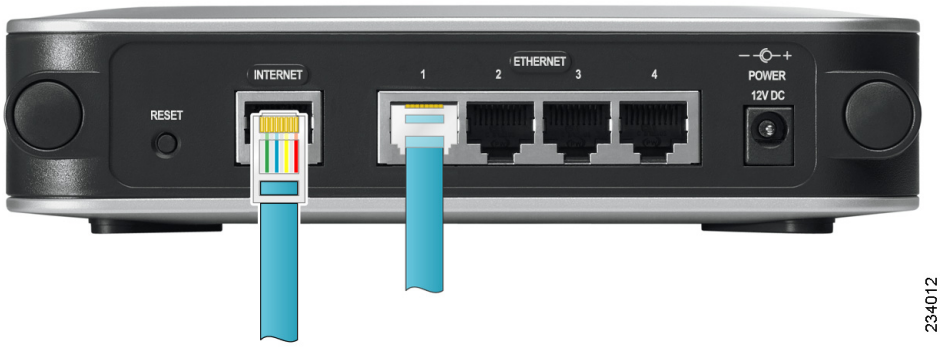
ハードウェアを設置するには、次の手順に従います。

ステップ 1 イーサネット ネットワーク ケーブルの一方の端を、ルータの背面パネルにある [LAN] ポート（1 ～ 4 の番号付き）のいずれかに挿入します。もう一方の端を PC のイーサネット ポートに挿入します。



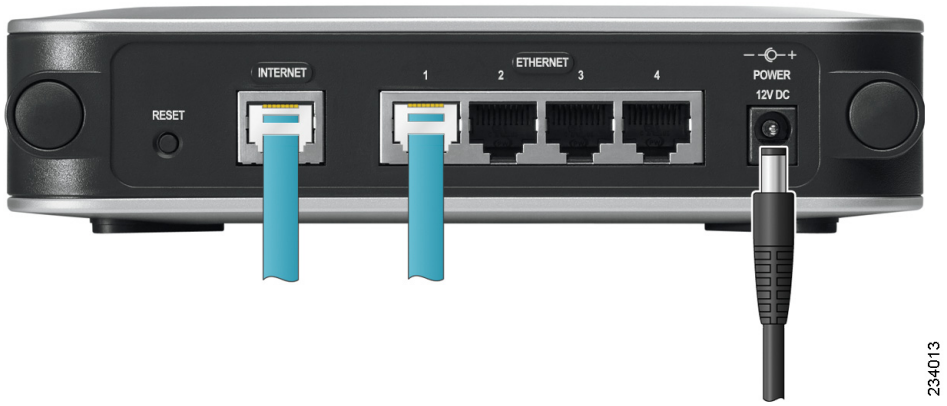
ステップ 2 手順 1 を繰り返して、最大 4 台まで PC やスイッチ、その他のネットワーク デバイスをルータに接続します。

ステップ 3 使用中のケーブル モデムまたは DSL モデムからのイーサネット ネットワーク ケーブルを、ルータの背面パネルにあるインターネット ポートに挿入します。



ステップ 4 ケーブル モデムまたは DSL モデムの電源を入れます。

ステップ 5 電源アダプタをルータの電源ポートに差し込み、逆の端を電源コンセントに挿入します。



ステップ 6 電源アダプタが接続されるとすぐに、前面パネルの [POWER] LED と [INTERNET] LED が点灯します。

ステップ 7 PC の電源を入れます。

以上で、ルータ ハードウェアの設置は完了です。

ルータの設定

RVS4000 を設定するには、PC をルータに接続し、設定ユーティリティを起動します。

（注） ルータのセットアップ前に、使用する PC がルータから IP（または TCP/IP）アドレスを自動的に取得する設定になっていることを確認します。

ステップ 1 Internet Explorer や Mozilla Firefox といった Web ブラウザを起動します。

ステップ 2 アドレス フィールドに **http://192.168.1.1** と入力し、Enter キーを押します。

ステップ 3 [ユーザ名] フィールドと [パスワード] フィールドに、**admin** と入力します。

デフォルトのユーザ名とパスワードは **admin** です。

ステップ 4 [OK] をクリックします。

セキュリティ向上のため、後で設定ユーティリティの [各種管理] > [管理] ウィンドウを使用して、新しいパスワードを設定するようにしてください。

ステップ 5 設定ユーティリティは、[設定] メニューの [概要] が選択された状態で表示されます。[設定] メニューで [WAN] をクリックします。

ステップ 6 ISP（通常はケーブル ISP）から要求された場合、[ホスト名] および [ドメイン名] フィールド、さらに [MTU] および [MTU サイズ] フィールドに必要事項を入力します。要求がない場合は、デフォルトのままにします。

ステップ 7 [WAN] 画面の [インターネット接続タイプ] ドロップダウン メニューで、インターネット接続タイプを選択します。選択したインターネット接続タイプによっては、追加のセットアップが必要になることがあります。

インターネット接続タイプには、次の選択肢があります。

[自動コンフィギュレーション - DHCP]：DHCP またはダイナミック IP アドレスで ISP に接続している場合、このデフォルト設定のままにしておきます。

[スタティック IP]：ISP からスタティック IP アドレスが割り当てられている場合、ドロップダウン メニューで [スタティック IP] を選択します。[インターネット IP アドレス]、[サブネットマスク]、[デフォルトゲートウェイ]、DNS（プライマリ / セカンダリ）の各フィールドに入力します。DNS アドレスは少なくとも 1 つ入力してください。

[PPPoE]：PPPoE 経由で接続する場合、ドロップダウン メニューでこの項目を選択します。[ユーザ名] と [パスワード] フィールドに入力します。

[PPTP]：PPTP はヨーロッパだけで使用されているサービスです。PPTP 接続を使用する場合、必要な情報について ISP に問い合せてください。

[ハートビート信号]：ハートビート信号は、主にオーストラリアで使用されています。必要な設定情報について、ISP に確認してください。

[L2TP]：L2TP は、主にヨーロッパで使用されています。必要な設定情報について、ISP に確認してください。

ステップ 8 インターネット接続設定の入力が終わったら、[保存] をクリックします。

ステップ 9 ルータの新しい設定を取得するため、PC を再起動するか、電源を入れます。

ステップ 10 任意のコンピュータで Web ブラウザを開き、www.cisco.com/jp/go/sb と入力して、設定をテストします。

以上で、ルータの設置は完了です。

（注） さらに細かい設定やセキュリティ オプションの詳細については、**第 5 章「ルータのセットアップおよび設定」**を参照してください。

5

ルータのセットアップおよび設定

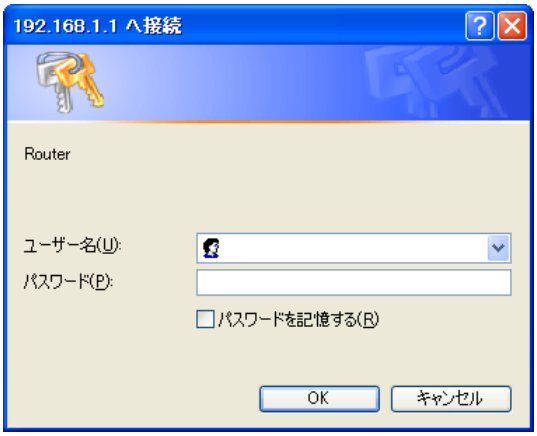
この章では、次のルータの機能を設定する方法について説明します。

組み込みの Web ベースの設定ユーティリティを使用してルータを設定します。ルータの設定ユーティリティにアクセスするには、Web ブラウザを開き、アドレス フィールドに **http://192.168.1.1** と入力します。Enter キーを押すと、ログイン ウィンドウが表示されます。

（注） デフォルトの IP アドレスは **192.168.1.1** です。DHCP によって、またはコンソール インターフェイスを使用して IP アドレスが変更された場合は、デフォルトではなく、割り当てられた IP アドレスを入力します。

初めて設定ユーティリティを開く場合、[ユーザ名] フィールドに **admin**（デフォルトのユーザ名）、[パスワード] フィールドに **admin** と入力します。[OK] ボタンをクリックします。パスワードは、後で [各種管理] > [管理] ウィンドウを使用して変更できます。

ログイン ウィンドウ



ログインすると、設定ユーティリティが起動します。画面の左側のナビゲーション ペインに、メニューがリンクとして表示されます。メニューを選択すると、ウィンドウのリストが表示されます。特定の機能を実行するには、メニューを選択して該当するウィンドウを選択します。デフォルトでは、ログイン後に [設定] メニューの [概要] ウィンドウが表示されます。

ユーティリティのメニューおよびウィンドウについては、次で説明します。簡略化のため、ウィンドウ名は [（メニュー名）] > [（ウィンドウ名）] の形式で示します。

[設定]

[設定] メニューを使用すると、ルータの基本セットアップ機能すべてにアクセスできます。ネットワーク設定のほとんどのデフォルト値を変更せずに、ルータを使用できます。一部のユーザは、Internet Service Provider（ISP; インターネット サービス プロバイダー）やブロードバンド（DSL、ケーブル モデム）キャリアを介してインターネットに接続するため、追加情報を入力する必要がある場合があります。

[設定] > [概要]

[設定] > [概要] ウィンドウは、ルータの基本情報の読み取り専用の概要を表示します。ハイパーリンク（下線付きのテキスト）をクリックすると、情報を更新できる関連ページが開きます。

[設定] > [概要]

[システム情報]

[ファームウェアバージョン]：ルータの現在のファームウェア バージョンが表示されます。

[CPU]：ルータの CPU のタイプが表示されます。

[システムアップタイム]：ルータが最後にリセットされてから経過した時間が表示されます。

[DRAM]：ルータに搭載されている DRAM の容量が表示されます。

[フラッシュ]：ルータに搭載されているフラッシュ メモリの容量が表示されます。

[ポート統計情報]

このセクションでは、ルータのイーサネット ポートの色別のステータス情報を示します。

- **緑**：ポートが接続されていることを示します。
- **黒**：ポートが接続されていないことを示します。

[ネットワークの設定ステータス]

[LAN IP]：ルータの LAN インターフェイスの IP アドレスです。

[WAN IP]：ルータの WAN インターフェイスの IP アドレスです。このアドレスが DHCP を使用して割り当てられた場合は、[DHCP リリース] をクリックするとアドレスを解除でき、[DHCP 更新] をクリックするとアドレスを更新できます。

[モード]：動作モードです。[ゲートウェイ] または [ルータ] の選択肢があります。

[ゲートウェイ]：ISP のサーバの IP アドレスを示すゲートウェイ アドレスです。

[DNS1] ～ [DNS2]：ルータが使用している Domain Name System（DNS; ドメイン ネーム システム）サーバの IP アドレスです。

[DDNS]：Dynamic Domain Name System（DDNS; ダイナミック ドメイン ネーム システム）機能が有効であることを示します。

[DMZ]：DMZ ホスティング機能が有効であるかどうかを示します。

[ファイアウォールの設定ステータス]

[DoS(サービス拒絶)]：DoS 攻撃をブロックする DoS 保護機能が有効であるかどうかを示します。

[WAN 要求のブロック]：ブロック WAN 要求機能が有効であるかどうかを示します。

[リモート管理]：リモート管理機能が有効であるかどうかを示します。

[IPSec VPN の設定ステータス]

[IPSec VPN の概要]：[IPSec VPN の概要] ハイパーリンクをクリックすると、[VPN] > [概要] ウィンドウが表示されます。

[使用中のトンネル]：現在使用されている VPN トンネルの数が表示されます。

[使用可能なトンネル]：使用できる VPN トンネルの数が表示されます。

[ログの設定ステータス]

[E メール]：「E メールを送信できません。発信 SMTP サーバアドレスが指定されていません。」と表示されている場合は、メール サーバが設定されていません。[E メール] ハイパーリンクをクリックすると、SMTP メール サーバを設定できる [各種管理] > [ログ] ウィンドウが表示されます。

[設定] > [WAN]

[インターネット接続タイプ]

ルータは、6 種類の接続をサポートしています。[設定] > [WAN] ウィンドウおよび使用可能な機能はそれぞれ、選択した接続タイプによって異なります。

[自動コンフィギュレーション - DHCP]

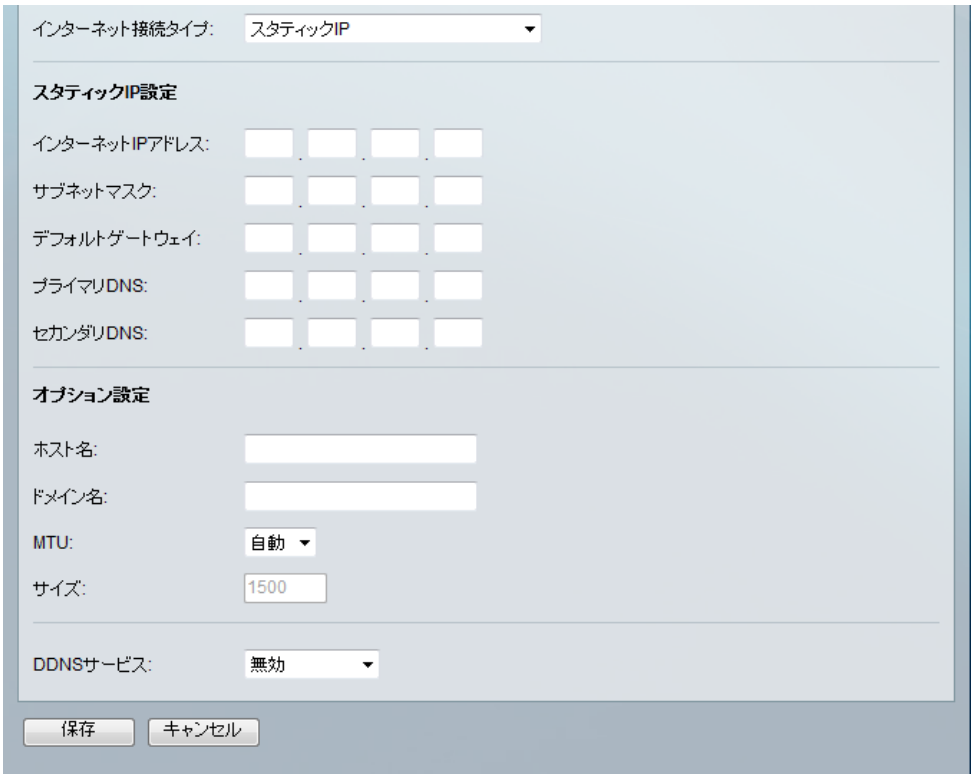
ルータのコンフィギュレーション タイプはデフォルトで [自動コンフィギュレーション - DHCP] に設定されており、ISP が DHCP をサポートしている場合、またはダイナミック IP アドレスを介して接続している場合にだけ保持されます。

[自動コンフィギュレーション - DHCP]

[スタティック IP]

インターネットに接続するために永続的な IP アドレスを使用している場合は、[スタティック IP] を選択します。

[スタティック IP]



[インターネット IP アドレス]：WAN またはインターネットから見た、ルータの IP アドレスです。ここで指定する IP アドレスは ISP から入手できます。

[サブネットマスク]：（ISP を含む）インターネット上の外部ユーザから見たルータのサブネット マスクです。ISP からこのサブネット マスクが提供されます。

[デフォルトゲートウェイ]：ISP から、ISP サーバの IP アドレスであるデフォルト ゲートウェイ アドレスが提供されます。

[プライマリ DNS]（必須）および [セカンダリ DNS]（オプション）：ISP から少なくとも 1 つのドメイン ネーム システム（DNS）サーバ IP アドレスが提供されます。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[PPPoE]

一部の DSL ベースの ISP はインターネット接続の確立に Point-to-Point Protocol over Ethernet（PPPoE）を使用します。DSL 回線を通じてインターネットに接続している場合は、利用する ISP で PPPoE を使用しているか確認してください。使用している場合は、PPPoE を有効にします。

[PPPoE]

[ユーザ名] および [パスワード]：ISP から提供されるユーザ名とパスワードを入力します。

[オンデマンド接続：最大アイドル時間]：指定された時間（最大アイドル時間）非アクティブになるとルータがインターネット接続を切断し、インターネットへの再アクセスが試行されると自動的にすぐ接続を再確立するように設定できます。オンデマンド接続を有効にするには、[オンデマンド接続] オプションを選択し、[最大アイドル時間] フィールドに、インターネット接続が自動的に終了するまでの非アクティブ状態の経過時間（分数）を入力します。

[キープアライブ: リダイアル間隔]：このオプションを選択すると、ルータが定期的にインターネット接続を確認します。接続されていない場合、ルータは自動的に接続を再確立します。このオプションを使用するには、[キープアライブ] の隣にあるオプション ボタンをオンにします。[リダイアル間隔] フィールドには、ルータがインターネット接続を確認する頻度を指定します。デフォルトのリダイアル間隔は **30** 秒です。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[PPTP]

Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）は、ヨーロッパおよびイスラエルの接続だけに適用されるサービスです。

[PPTP]

[IP アドレス]：WAN またはインターネットから見たルータの IP アドレスです。ここに指定する必要がある IP アドレスは ISP から入手できます。

[サブネットマスク]：（ISP を含む）インターネット上の外部ユーザから見たルータのサブネット マスクです。ISP からこのサブネット マスクが提供されます。

[デフォルトゲートウェイ]：ISP からデフォルト ゲートウェイ アドレスが提供されます。

[PPTP サーバ]：PPTP サーバの IP アドレスを入力します。

[ユーザ名] および [パスワード]：ISP から提供されるユーザ名とパスワードを入力します。

[オンデマンド接続：最大アイドル時間]：指定された時間（最大アイドル時間）非アクティブになるとルータがインターネット接続を切断し、インターネットへの再アクセスが試行されると自動的にすぐ接続を再確立するように設定できます。オンデマンド接続を有効にするには、[オンデマンド接続] オプションを選択し、[最大アイドル時間] フィールドに、インターネット接続が自動的に終了するまでの非アクティブ状態の経過時間（分数）を入力します。

[キープアライブ：リダイアル間隔]：このオプションを選択すると、ルータが定期的にインターネット接続を確認します。接続されていない場合、ルータは自動的に接続を再確立します。このオプションを使用するには、[キープアライブ] の隣にあるオプション ボタンをオンにします。[リダイアル間隔] フィールドには、ルータがインターネット接続を確認する頻度を指定します。デフォルトのリダイアル間隔は **30** 秒です。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[ハートビート信号]

ハートビート信号は、オーストラリアだけで使用されるサービスです。必要な設定情報について、ISP に確認してください。

[ハートビート信号]

[ユーザ名] および [パスワード]：ISP から提供されるユーザ名とパスワードを入力します。

[ハートビートサーバ]：ハートビート サーバの IP アドレスを入力します。

[オンデマンド接続：最大アイドル時間]：指定された時間（最大アイドル時間）非アクティブになるとルータがインターネット接続を切断し、インターネットへの再アクセスが試行されると自動的にすぐ接続を再確立するように設定できます。オンデマンド接続を有効にするには、[オンデマンド接続] オプションを選択し、[最大アイドル時間] フィールドに、インターネット接続が自動的に終了するまでの非アクティブ状態の経過時間（分数）を入力します。

[キープアライブ：リダイアル間隔]：このオプションを選択すると、ルータが定期的にインターネット接続を確認します。接続されていない場合、ルータは自動的に接続を再確立します。このオプションを使用するには、[キープアライブ] の隣にあるオプション ボタンをオンにします。[リダイアル間隔] フィールドには、ルータがインターネット接続を確認する頻度を指定します。デフォルトのリダイアル間隔は **30** 秒です。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[L2TP]

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）は、インターネット間を Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）で伝送するサービスです。このサービスは主にヨーロッパの各国で使用されています。必要な設定情報について、ISP に確認してください。

[L2TP]

[IP アドレス]：WAN またはインターネットから見たルータの IP アドレスです。ここに指定する必要がある IP アドレスは ISP から入手できます。

[サブネットマスク]：（ISP を含む）インターネット上の外部ユーザから見たルータのサブネット マスクです。ISP からこのサブネット マスクが提供されます。

[ゲートウェイ]：ISP からデフォルト ゲートウェイ アドレスが提供されます。

[L2TP サーバ]：L2TP サーバの IP アドレスを入力します。

[ユーザ名] および [パスワード]：ISP から提供されるユーザ名とパスワードを入力します。

[オンデマンド接続：最大アイドル時間]：指定された時間（最大アイドル時間）非アクティブになるとルータがインターネット接続を切断し、インターネットへの再アクセスが試行されると自動的にすぐ接続を再確立するように設定できます。オンデマンド接続を有効にするには、[オンデマンド接続] オプションを選択し、[最大アイドル時間] フィールドに、インターネット接続が自動的に終了するまでの非アクティブ状態の経過時間（分数）を入力します。

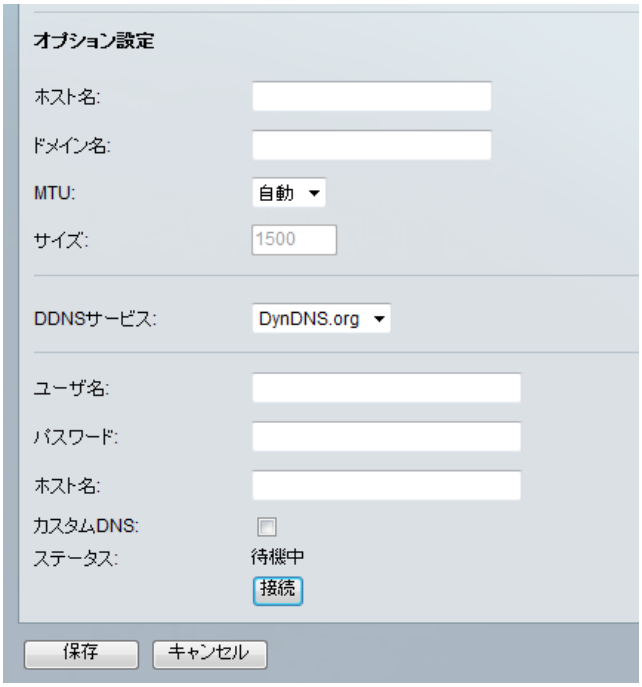
[キープアライブ：リダイアル間隔]：このオプションを選択すると、ルータが定期的にインターネット接続を確認します。接続されていない場合、ルータは自動的に接続を再確立します。このオプションを使用するには、[キープアライブ] の隣にあるオプション ボタンをオンにします。[リダイアル間隔] フィールドには、ルータがインターネット接続を確認する頻度を指定します。デフォルトのリダイアル間隔は **30** 秒です。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[オプション設定]（一部の ISP では必須）

設定によっては、ISP から要求がある場合があります。変更する前に、ISP に確認してください。

[オプション設定]



[ホスト名]：ケーブル ISP といった一部の ISP では、識別のためにホスト名の指定が必要な場合があります。使用するブロードバンド インターネット サービスにホスト名が設定されているかを ISP に確認する必要があることがあります。ほとんどの場合、このフィールドは空白のままにしてもかまいません。

[ドメイン名]：ケーブル ISP といった一部の ISP では、識別のためにドメイン名の指定が必要な場合があります。使用するブロードバンド インターネット サービスにドメイン名が設定されているかを ISP に確認する必要があることがあります。ほとんどの場合、このフィールドは空白のままにしてもかまいません。

[MTU]：MTU は Maximum Transmission Unit の略称です。インターネット転送で許可される最大パケット サイズを指定します。転送する最大パケット サイズを手動で入力する場合は、[手動] を選択します。インターネット接続時の最適 MTU をルータに選択させるには、デフォルト設定の [自動] のままにしておきます。

[サイズ]：[MTU] フィールドで [手動] を選択すると、このオプションが有効になります。この値は、1200 ～ 1500 に設定することが推奨されますが、128 ～ 1500 の値を定義できます。

[DDNS サービス]：DDNS サービスは、デフォルトで無効になっています。DDNS サービスを有効にするには、下記の手順に従います。

[接続]：[接続] ボタンは、DDNS が有効であるときに表示されます。このボタンをクリックすると、DDNS サーバに接続して、IP アドレスを手動で更新できます。このウィンドウ上の [ステータス] 領域も更新されます。

ステップ 1 DDNS サービスにサインアップします。

- DynDNS：www.dyndns.org で DDNS サービスを申し込み、ユーザ名、パスワード、およびホスト名情報を記入します。
- TZO：www.tzo.com で DDNS サービスを申し込み、E メール アドレス、パスワード、およびドメイン名情報を記入します。

ステップ 2 DDNS サービス プロバイダーを選択します。

ステップ 3 次のフィールドを設定します。

- [ユーザ名]（DynDNS）または [E メールアドレス]（TZO）。
- [パスワード]
- [ホスト名]（DynDNS）または [ドメイン名]（TZO）。
- [カスタム DNS]（DynDNS）

ステップ 4 [保存] をクリックします。

現在の WAN（インターネット）IP アドレスが変更されると、常にルータから DDNS サービスに通知されます。TZO をご使用の場合は、TZO ソフトウェアを使用してこの「IP アドレス更新」を実行しないでください。

[設定] > [LAN]

[設定] > [LAN] ウィンドウでは、ルータのローカル ネットワーク設定を変更できます。

[設定] > [LAN]

[VLAN]：ドロップダウン メニューから、DHCP サーバ用の VLAN を選択します。

（注） このオプションは、[L2 スイッチ] > [VLAN の作成] ウィンドウで少なくとも 1 つの VLAN を作成した場合だけ表示されます。

[IPv4]

ルータのローカル IP アドレスであり、ここにサブネット マスクが表示されます。ほとんどの場合、デフォルトのままでかまいません。

[ローカル IP アドレス]：デフォルト値は 192.168.1.1 です。

[サブネットマスク]：デフォルト値は 255.255.255.0 です。

[サーバ設定 (DHCP)]

ネットワーク上の各 PC に IP アドレスを自動的に割り当てる、ネットワークの Dynamic Host Configuration Protocol（DHCP）サーバとして、このルータを使用できます。DHCP サーバがまだない場合は、ルータを DHCP サーバとして有効にしたままにしておくことを強く推奨します。

[DHCP サーバ]：DHCP は工場出荷時設定ですでに有効に設定されています。DHCP サーバがすでにネットワーク上に存在する場合、または DHCP サーバを使用しない場合は、[無効]（他の DHCP 機能は利用不可）を選択します。DHCP サーバがすでにネットワーク上に存在する場合で、このルータを既存の DHCP サーバのリレーとして使用する場合は、[DHCP リレー] を選択してから [DHCP サーバ] に IP アドレスを入力します。DHCP を無効にする場合は、スタティック IP アドレスをルータに割り当てます。

[開始 IP アドレス]:DHCP サーバが IP アドレスを発行するときに開始する値を入力します。この値は 192.168.1.2 以上で、192.168.1.254 よりも小さい値にする必要があります。その理由は、ルータのデフォルトの IP アドレスが 192.168.1.1 であり、192.168.1.255 はブロードキャスト IP アドレスであるからです。

[DHCP ユーザの最大数]：DHCP サーバが IP アドレスを割り当てる対象となる PC の最大数を入力します。この数字は 253 以下になるようにしてください。DHCP IP アドレスの範囲を決定するために、開始 IP アドレス（例：100）を DHCP ユーザの数に追加します。

[クライアントリース時間]：DHCP クライアントが DHCP サーバに更新要求を送信するまでに、割り当てられた IP アドレスを保持できる時間です。

[スタティック DNS 1] ～ [スタティック DNS 3]：該当する場合は、DNS サーバの IP アドレスを入力します。

[WINS]：Windows Internet Naming Service（WINS）は、Windows ネットワークで（DNS と同様の）名前解決サービスを提供します。WINS サーバを使用する場合は、そのサーバの IP アドレスをここに入力します。それ以外の場合は空白のままにします。

[スタティック IP のマッピング]

スタティック IP のマッピングは、特定の IP アドレスを特定の MAC アドレスにバインドするために使用します。これにより、外部（WAN）ユーザは、NAPT ポート フォワーディングでアドバタイズされている LAN サーバにアクセスできます。50 エントリまで定義できます。

[スタティック IP アドレス]：マッピングする IP アドレスを入力します。

[MAC アドレス]：マッピングする MAC アドレスを入力します。

[ホスト名]：マッピングするホスト名を入力します。

エントリを作成し、リストに追加する場合は、[追加] をクリックします。既存のエントリを変更するには、そのエントリをリストから選択し、該当するフィールドを編集し、[変更] をクリックします。エントリを削除するには、そのエントリをリストから選択し、[削除] をクリックします。

[IPv6]

[IPv6 アドレス]：ネットワークに IPv6 が実装されている場合は、このフィールドに正しい IPv6 アドレスを入力します。

[プレフィクス長]：適切な IPv6 プレフィクス長を入力します。

[ルータアドバタイズメント]：このオプションを有効にすると、IPv6 ホストはルータによる IPv6 プレフィクス ブロードキャストを使用することによって IP アドレスを自動的に設定できるようになります。

[DHCPv6]

DHCP v6 機能を有効にするには、[有効] を選択します。DHCP v6 を無効にするには、[無効] を選択します。

[リース時間]：リース時間を分単位で入力します。

[HCP6 アドレス範囲の先頭]：開始 DHCP v6 IP アドレスを入力します。

[HCP6 アドレス範囲の末尾]：終了 DHCP v6 IP アドレスを入力します。

[プライマリ DNS]：プライマリ DHCP v6 DNS サーバ アドレスを入力します。

[セカンダリ DNS]：セカンダリ DHCP v6 DNS サーバ アドレスを入力します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[設定] > [DMZ]

インターネット ゲームやテレビ会議のような特殊サービスのために、1 台のローカル PC をインターネットから見られるように DMZ を設定できます。ポート範囲のフォワーディングでは最大 10 の範囲のポートしか転送できませんが、DMZ ホスティングは 1 つの PC のすべてのポートを同時に転送します。

[設定] > [DMZ]

[DMZ ホスティング]: DMZ 機能は、インターネット ゲームやテレビ会議のような特殊用途のサービスを使用するために、あるローカル PC をインターネットに公開することを許可する機能です。この機能を使用するには、[有効] を選択します。DMZ 機能を無効にするには、[無効] を選択します。

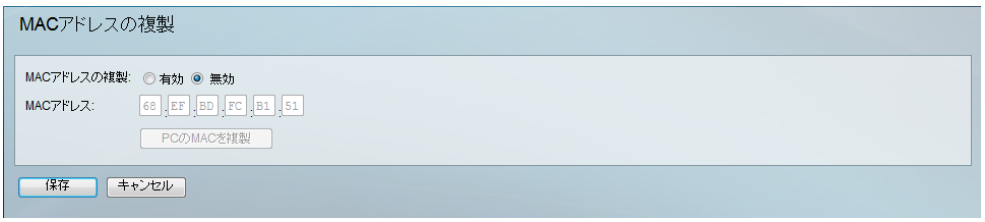
[DMZ ホストの IP アドレス]: ある PC を公開するには、コンピュータの IP アドレスを入力します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[設定] > [MAC アドレスの複製]

一部の ISP には、MAC アドレスを登録する必要があります。この機能は、ネットワーク アダプタの MAC アドレスをルータに「クローン」し、ISP に連絡して登録済みの MAC アドレスをルータの MAC アドレスに変更する必要性をなくします。ルータの MAC アドレスは、識別のために固有数のハードウェアに割り当てられる 12 桁のコードです。

[設定] > [MAC アドレスの複製]



[MAC アドレスの複製]: ドロップダウン メニューから、[有効] または [無効] を選択します。

[MAC アドレス]: このフィールドに、ISP に登録した MAC アドレスを入力します。

[PC の MAC を複製]：[MAC アドレスの複製] が無効になっている場合、このボタンをクリックすると、Web インターフェイスに接続するために使用する、コンピュータのネットワークアダプタの MAC アドレスをコピーできます。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[設定] > [拡張ルーティング]

[設定] > [拡張ルーティング]

[動作モード]

[動作モード] は、このルータの動作モードを選択します。

- **[ゲートウェイ]**：通常の動作モードです。これにより、LAN 上のすべてのデバイスは同じ WAN（インターネット）IP アドレスを共有できます。ゲートウェイ モードでは、Network Address Translation（NAT; ネットワーク アドレス変換）メカニズムが有効になります。
- **[ルータ]**：別のルータをインターネット ゲートウェイとして動作させるか、または LAN 上のすべての PC に（固定の）インターネット IP アドレスを割り当てる必要があります。ルータ モードでは、NAT メカニズムが無効になります。

[ダイナミックルーティング]

ルータのダイナミック ルーティング機能を使用すると、ネットワークのレイアウトの物理的な変更に対して自動的に適応できます。ルータはダイナミック Routing Information Protocol（RIP）プロトコルを使用して、ネットワークのデータ パケットが送信元と宛先との間で伝送される最も効率的なルートを最短パスに基づいて計算できます。RIP プロトコルは、ネットワーク上の他のルータにルーティング情報を定期的にブロードキャストします。

[RIP] (Routing Information Protocol)：ルータで RIP プロトコルを使用する場合は、[有効] を選択し、使用しない場合はデフォルト設定 [無効] のままにします。

[RIP送信パケットのバージョン]：ネットワーク上でデータを送信するために使用する TX プロトコルとして、[RIPv1] または [RIPv2] を選択します。この設定は、LAN 上の他のルータがサポートするバージョンに一致する必要があります。

[RIP受信パケットのバージョン]：ネットワーク上でデータを受信するために使用する RX プロトコルとして、[RIPv1] または [RIPv2] を選択します。この設定は、LAN 上の他のルータがサポートするバージョンに一致する必要があります。

[スタティックルーティング]

ルーティング テーブルを作成するために、ダイナミック ルーティング プロトコルを使用しないでスタティック ルートを使用する場合があります。スタティック ルートでは、CPU リソースがピア ルータとルーティング情報を交換する必要はありません。また、スタティック ルートを使用すると、ダイナミック ルーティング プロトコルをサポートしないピア ルータに接続できます。スタティック ルートは、ダイナミック ルートと併用できます。ネットワークにルーティング ループを導入しないように注意してください。

スタティック ルーティングを設定するには、ルーティング テーブル内に、特定の IP 宛先に対するパケットの転送先をルータに通知するルート エントリを追加する必要があります。

このデータを入力すると、スタティック ルート エントリを作成できます。

[セット番号の選択]：表示または設定するセット番号（ルーティング テーブルのエントリ番号）を選択します。必要な場合には、[このエントリを削除] をクリックしてエントリをクリアします。

[宛先IPアドレス]：リモート LAN セグメントのネットワーク アドレスを入力します。標準のクラス C IP ドメインの場合、宛先 LAN IP の最初の 3 つのフィールドがネットワーク アドレスであり、最後のフィールドが 0 である必要があります。

[サブネットマスク]：宛先 LAN IP ドメインで使用するサブネット マスクを入力します。クラス C IP ドメインの場合、サブネット マスクは **255.255.255.0** です。

[ゲートウェイ]：このルータを使用してネットワークをインターネットに接続する場合は、ゲートウェイ IP アドレスがルータの IP アドレスになります。ネットワークのインターネット接続を管理するルータが別にある場合は、そのルータの IP アドレスを代わりに入力します。

[ホップカウント]：この値は、データ パケットが宛先に到着するまでに通過するノードの数を示します。ノードとは、スイッチや PC などのネットワーク上のデバイスです。[ホップカウント] の最大値は 16 です。

[ルーティングテーブルの表示]：このボタンをクリックすると、ダイナミック ルーティング方式またはスタティック ルーティング方式で確立したルーティング テーブルが表示されます。

[VLAN 間ルーティング]

[VLAN 間ルーティング]：[有効] を選択すると、異なるサブネット VLAN 間でパケットがルーティングできます。デフォルトは [有効] です。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[設定] > [時間]

[設定] > [時間]

[現地時間を手動で設定する]：時刻と日付を手動で入力する場合は、このオプションを選択し、ドロップ ダウン フィールドから [日付] を選択し、[時間] フィールドに時、分、秒を 24 時間形式で入力します。たとえば、10:00 pm の場合は、時を入力するフィールドに **22**、分を入力するフィールドに **0**、秒を入力するフィールドに **0** を入力します。

[ネットワークタイムプロトコル (NTP) を使用して現地時間を自動的に設定する]：Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバを使用して日時を設定する場合は、このオプションを選択し、次のフィールドを完成させます。

[時間帯]：居住する地域の時間帯を選択します。時間設定はインターネットを介して同期されます。

[夏時間自動調整]：夏時間を導入している地域の場合は、[有効] オプションを選択します。

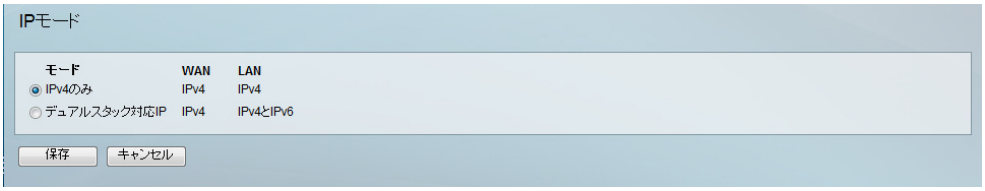
[ユーザ定義の NTP サーバ]：ユーザ定義の NTP サーバを指定するには、[有効] オプションを選択し、NTP サーバの IP アドレスを [NTP サーバの IP] フィールドに入力します。

[NTP サーバの IP]：[ユーザ定義の NTP サーバ] オプションを [有効] に設定する場合は、NTP サーバの IP アドレスを入力します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[設定] > [IP モード]

[設定] > [IP モード]



[IPv4 のみ]：このオプションを選択すると、インターネットおよびローカル ネットワークで IPv4 を利用します。

[デュアルスタック対応 IP]：このオプションを選択すると、インターネットでは IPv4、ローカル ネットワークでは IPv4 および IPv6 を利用します。LAN の IPv6 ホストは、6to4 トンネル（RFC3056 による）を経由してリモートの IPv6 アイランドに接続します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[ファイアウォール]

[ファイアウォール] メニューを使用すると、特定ユーザのインターネットへアクセスを拒否または許可できるようにルータを設定できます。特定のインターネット ユーザが内部サーバにアクセスすることを拒否または許可するようにルータを設定することもできます。内部（LAN）または外部（WAN）の異なるユーザに対して、各ユーザの IP アドレスまたはネットワーク ポート番号に基づいて、異なるパケット フィルタを設定できます。

[ファイアウォール] > [基本設定]

[ファイアウォール] > [基本設定]

[ファイアウォール]：この機能を有効にすると、ルータの NAT ファイアウォール機能が有効になります。

[DoS 保護]：この機能を有効にすると、ルータはサービス拒絶（DoS）攻撃をブロックします。DoS 攻撃はデータを盗用したり PC を損傷させたりはしませんが、インターネット接続を過負荷状態にするため、インターネットに接続できなくなります。

[WAN 要求のブロック]：この機能を有効にすると、ルータは WAN からの匿名要求をフィルタリングします。

[リモート管理]：この機能により、HTTP ポートまたは HTTPS ポートを使用してルータをリモート管理できます。この機能を有効にするには、[有効] を選択して [ポート] フィールドにポート番号を入力し、下に表示されている [HTTPS] および [リモート IP アドレス] の設定を行います。

[HTTPS]：このオプションは、WAN から設定ユーティリティへのアクセスを、HTTPS セッションのみに制限します。HTTPS セッションでは、HTTP の場合よりも優れた保護をリモート セッションに提供する SSL 暗号化が使用されます。デフォルトは [有効] です。

[リモート IP アドレス]：ルータへのアクセスが許可された外部の IP アドレスを指定する適切な値を選択します。

- **[任意の IP アドレス]**：外部のあらゆる IP アドレスからのアクセスを許可します。
- **[単一の IP アドレス]**：表示されるフィールドに入力された 1 つの IP アドレスからのアクセスを許可します。
- **[IP 範囲]**：表示されるフィールドに入力された一定範囲の IP アドレスからのアクセスを許可します。
- **[サブネット]**：表示されるフィールドに入力されたサブネットからのアクセスを許可します。

[リモートアップグレード]：このオプションを使用すると、ルータをリモートでアップグレードできます。リモートでアップグレードできるようにするには、[有効] を選択します。[リモート管理] 機能も [有効] に設定する必要があります。デフォルトは [無効] です。

[マルチキャストパススルー]：ルータ上で IGMP プロキシが実行中である場合、この機能を有効にすると、インターネットから IP マルチキャスト トラフィックを受信できます。デフォルトは [無効] です。

[SIP アプリケーション層ゲートウェイ]：この機能を有効にすると、SIP Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）によって、Voice over IP（VoIP）に使用される Session Initiation Protocol（SIP）パケットが NAT ファイアウォールを通過できます。VoIP サービス プロバイダーが STUN、TURN、ICE などの他の NAT 通過ソリューションを提供している場合は、この機能を無効にしてもかまいません。

[ブロック]：制限する Web 機能の隣にあるチェックボックスをオンにします。

- **[Java]**：Java は Web サイトのプログラミング言語です。Java を拒否すると、このプログラミング言語を使用しているインターネット サイトにアクセスできなくなる可能性があります。
- **[Cookies]**：Cookie は、ご使用の PC に保存されるデータで、インターネット サイトと情報をやり取りする際に、インターネット サイトにより使用されます。そのため、Cookie は拒否しないでください。
- **[ActiveX]**：ActiveX は、Microsoft（Internet Explorer）による Web サイトのプログラミング言語です。ActiveX を拒否すると、このプログラミング言語を使用しているインターネット サイトにアクセスできなくなる可能性があります。また、ActiveX は Windows Update でも使用されます。ActiveX がブロックされると、Windows Update は使用できません。

- **[プロキシ HTTP サーバへのアクセス]**：ローカル ユーザが WAN プロキシ サーバにアクセスできる場合、ローカル ユーザはルータのコンテンツ フィルタを迂回して、ルータによりブロックされているインターネット サイトにアクセスできる可能性があります。プロキシを拒否することで、すべての WAN プロキシ サーバへのアクセスをブロックできます。

[ファイアウォール] > [IP ベースの ACL]

IP ベースの ACL ウィンドウでは、最大 50 のルールを持つ Access Control List（ACL; アクセス コントロール リスト）を作成できます。プライオリティ、サービス タイプ、インターフェイス、送信元 IP アドレス、宛先 IP アドレス、曜日、時刻など、さまざまな基準に基づいて、各 ACL ルールはネットワークへのアクセスを拒否または許可します。

[ファイアウォール] > [IP ベースの ACL]

[プライオリティ]：ルールのプライオリティです。

[有効]：ルールが有効になっているか無効になっているかを示します。

[アクション]：ルールのアクションであり、[許可] と [拒否] のいずれかです。

[サービス]：ルールが適用されるサービスです。

[送信元インターフェイス]：送信元インターフェイスとして [WAN]、[LAN]、または [任意] を選択します。

[送信元]：送信元 IP アドレスであり、1 つの特定の IP アドレス、[任意]（すべての IP アドレス）、ある範囲の IP アドレス、または特定の IP サブネットに設定できます。

[宛先]：宛先 IP アドレスであり、1 つの特定の IP アドレス、[任意]（すべての IP アドレス）、ある範囲の IP アドレス、または特定の IP サブネットに設定できます。

[時間]：ルールが有効となる時刻であり、[常時]（24 時間）、または特定の開始時間と終了時間です。

[曜日]：ルールが有効となる曜日です。任意の曜日、またはユーザ指定の一組の曜日に設定できます。

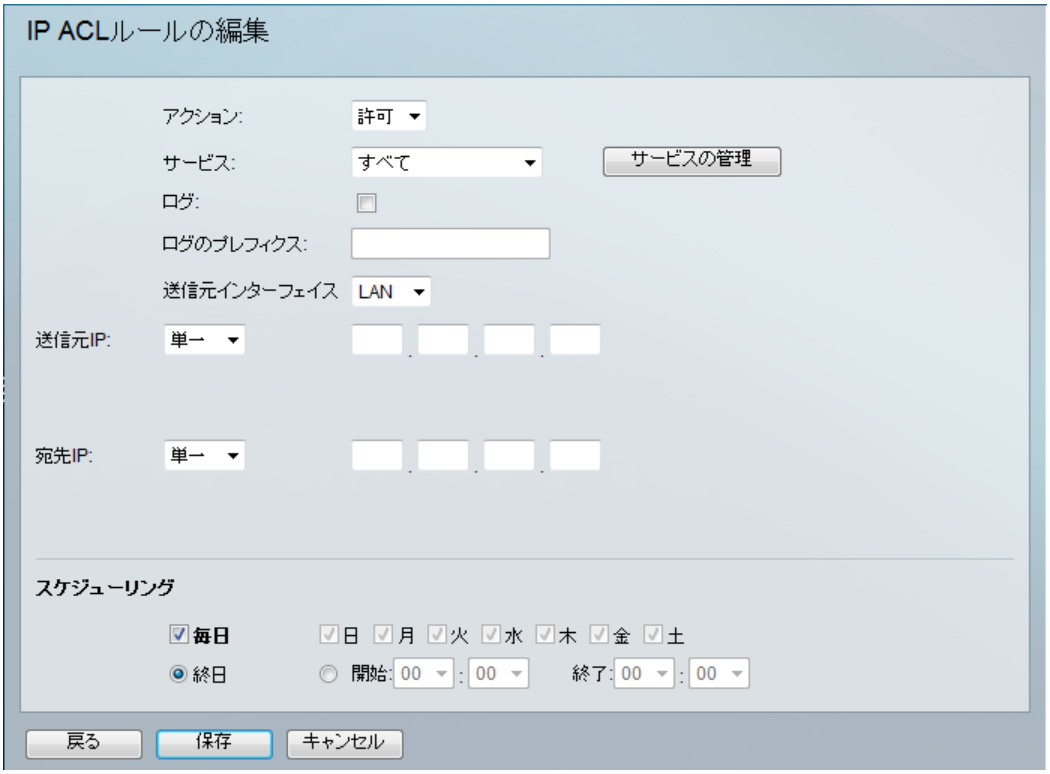
[編集] ボタン：行の最後の [編集] をクリックすると、関連付けられているルールを編集できます。

[削除] ボタン：行の最後の [削除] をクリックすると、関連付けられているルールを削除できます。

ACL ルール テーブルに新しい ACL ルールを追加するには、[新規ルールの追加] をクリックし、[IP ACL ルールの編集] ウィンドウを表示します。新しい ACL ルールを作成するには、次のセクションの手順に従います。すべてのルールを削除せずに無効にするには、[すべてのルールを無効にする] をクリックします。テーブルからすべてのルールを削除するには、[すべてのルールを削除] をクリックします。

[IP ACL ルールの編集]

[IP ACL ルールの編集]



[アクション]：ドロップダウン メニューから、[許可] または [拒否] の目的のアクションを選択します。

[サービス]：ルールが適用されるサービスの種類を選択します。ドロップダウン メニューから定義済みのサービスを 1 つ選択できます。[すべて] を選択すると、すべての種類の IP トラフィックを許可または拒否できます。新しいサービスを定義するには、[サービスの管理] をクリックして [サービスの管理] ウィンドウを開きます。その後、新しいサービスの名前を指定し、種類（[TCP]、[UDP]、[TCP/UDP]）を選択し、[開始ポート] と [終了ポート] を入力後、[保存] をクリックします。新しいサービスが、[IP ACL ルールの編集] ウィンドウ上のドロップダウン メニューに表示されます。

[ログ]：このオプションを選択すると、このルールによってフィルタリングされるすべてのトラフィックのログを記録できます。

[ログのプレフィクス]：ログ内で一致する各イベントの先頭に追記する文字列を入力します。

[送信元インターフェイス]：ドロップダウン メニューから、送信元インターフェイスとして [WAN]、[LAN]、または [任意] を選択します。

[送信元 IP]：1 つの送信元 IP アドレスにルールを適用するには、ドロップダウン メニューから [単一] を選択し、フィールドにアドレスを入力します。すべての送信元 IP アドレスにルールを適用するには、ドロップダウン メニューから [任意] を選択します。ある範囲の IP アドレスにルールを適用するには、[範囲] を選択し、開始 IP アドレスと終了 IP アドレスを入力します。サブネットにルールを適用するには、[ネット] を選択し、IP アドレスとサブネット マスクを入力します。

[宛先 IP]：1 つの宛先 IP アドレスにルールを適用するには、ドロップダウン メニューから [単一] を選択し、フィールドにアドレスを入力します。すべての宛先 IP アドレスにルールを適用するには、ドロップダウン メニューから [任意] を選択します。ある範囲の IP アドレスにルールを適用するには、[範囲] を選択し、開始 IP アドレスと終了 IP アドレスを入力します。サブネットにルールを適用するには、[ネット] を選択し、IP アドレスとサブネット マスクを入力します。

曜日：ルールを毎日適用するには、[毎日] を選択します。ルールを特定の曜日だけ適用するには、目的の曜日を選択します。

時間：ルールを一日中適用するには、[終日] を選択します。ルールを一日の特定の時間だけ適用する場合は、[開始] フィールドに開始時間を入力し、[終了] フィールドに終了時間を入力します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。IP ベースの ACL ウィンドウに戻るには、[戻る] をクリックします。

[ファイアウォール] > [インターネットアクセスポリシー]

[ファイアウォール] > [インターネットアクセスポリシー]

ポリシーを設定することによって、ネットワークへのアクセスを管理できます。このウィンドウ上の設定を使用すると、アクセス ポリシーを確立できます。ドロップダウン メニューからポリシーを選択すると、ポリシーの設定が表示されます。その後、次の操作を行います。

- ポリシーの作成：下記の手順を参照してください。
- 現在のポリシーの削除：[削除] をクリックします。

- **すべてのポリシーの表示**:[概要] をクリックすると [インターネットポリシーの概要] ウィンドウが表示されます。このウィンドウは、すべてのインターネット アクセス ポリシーを表示し、また、[番号]、[ポリシー名]、[曜日]、[時刻]、およびポリシーを削除（クリア）するチェックボックスも備えています。ポリシーを削除するには、[削除] 列のチェックボックスをオンにして、[削除] をクリックします。
- **現在のポリシーが適用される PC の表示および変更**：[PC リストの編集] をクリックすると、[PC リスト] ウィンドウが表示されます。

[インターネットポリシーの概要]

[PC リスト]

[PC リスト] ポップアップ上で、MAC アドレスまたは IP アドレスによって PC を定義できます。このポリシーが PC のグループに影響を及ぼすようにする場合は、ある範囲の IP アドレスを入力できます。

インターネット アクセス ポリシーを作成するには、次の手順に従います。

ステップ 1 [インターネットアクセスポリシー] ドロップダウン メニューから目的のポリシー番号を選択します。

ステップ 2 表示されるフィールドにポリシー名を入力します。

ステップ 3 このポリシーを有効にするには、[ステータス] オプションを [有効] に設定します。

ステップ 4 [PC リストの編集] をクリックすると、ポリシーの影響を受ける PC を選択できます。[PC リスト] ポップアップが表示されます。MAC アドレスまたは IP アドレスに基づいて PC を選択できます このポリシーが PC のグループに影響を及ぼすようにする場合は、ある範囲の IP アドレスを入力できます。変更後、[保存] をクリックすると、その変更内容が適用されます。

ステップ 5 [PC リスト] ポップアップに記載されている PC のインターネット アクセスをブロックするか許可するかによって、[拒否] または [許可] の該当するオプションをクリックします。

ステップ 6 このポリシーを実行する曜日と時間を決定します。ポリシーが有効となる単一の曜日を選択するか、または [毎日] を選択します。ポリシーが有効となる時間の範囲を入力するか、または [終日] を選択します。

ステップ 7 Web サイトへのアクセスをブロックする場合は、[URL アドレスによる Web サイトのブロック] 機能、または [キーワードによる Web サイトのブロック] 機能を使用します。

- **[URL アドレスによる Web サイトのブロック]**: ブロックする Web サイトの URL またはドメイン名を入力します。
- **[キーワードによる Web サイトのブロック]**: 表示されるフィールドに、ブロックするキーワードを入力します。このキーワードが Web サイトの URL に表示された場合、そのサイトへのアクセスはブロックされます。各 Web ページのコンテンツではなく、URL だけが確認されることに注意してください。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[ファイアウォール] > [単一ポートのフォワーディング]

[ファイアウォール] > [単一ポートのフォワーディング]

[アプリケーション]：設定するアプリケーションの名前を入力します。

[外部ポート]：サーバまたはインターネット アプリケーションによって使用されるポート番号です。インターネット ユーザはこのポート番号を使用して接続する必要があります。詳細については、インターネット アプリケーションのソフトウェア マニュアルを確認してください。

[内部ポート]：インターネット トラフィックを LAN 上の PC またはサーバに転送するときにルータが使用するポート番号です。通常、このポート番号は [外部ポート] の番号と同じです。番号が異なる場合、ルータは「ポート変換」を行います。このため、インターネット ユーザが使用するポート番号は、サーバまたはインターネット アプリケーションで使用されるポート番号とは別のものになります。

たとえば、80 番のポート（標準）と 8080 番のポートの両方で接続を受け入れるように Web サーバを設定できます。次に、ポート フォワーディングを有効にし、[外部ポート] を 80、[内部ポート] を 8080 に設定します。こうすると、インターネット ユーザが標準の 80 番ポートを使用する場合でも、インターネットから Web サーバに送信されるすべてのトラフィックは 8080 番ポートを使用します （ローカル LAN 上のユーザは、標準の 80 番ポートを使用して Web サーバに接続可能であり、このように接続する必要があります）。

[プロトコル]：アプリケーションで使用するプロトコルを選択します。[TCP] または [UDP]、あるいはその両方になります。

[IP アドレス]：各アプリケーションで、特定のアプリケーションを実行する PC の IP アドレスを入力します。

[有効]：[有効] チェックボックスをオンにすると、関連アプリケーションのポート フォワーディングが有効になります。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[ファイアウォール] > [ポート範囲のフォワーディング]

[ファイアウォール] > [ポート範囲のフォワーディング]

[アプリケーション]：設定するアプリケーションの名前を入力します。

[開始]：ポート範囲の先頭です。サーバまたはインターネット アプリケーションで使用されるポート番号の範囲（外部ポート）の開始ポート番号を入力します。必要に応じて、対象のインターネット アプリケーションのソフトウェア マニュアルで詳細を確認してください。

[終了]：ポート範囲の終了ポート番号です。サーバまたはインターネット アプリケーションで使用されるポート番号の範囲（外部ポート）の終了ポート番号を入力します。必要に応じて、対象のインターネット アプリケーションのソフトウェア マニュアルで詳細を確認してください。

[プロトコル]：アプリケーションで使用するプロトコルを選択します。[TCP] または [UDP]、あるいはその両方になります。

[IP アドレス]：各アプリケーションで、特定のアプリケーションを実行する PC の IP アドレスを入力します。

[有効]：[有効] チェックボックスをオンにすると、関連アプリケーションのポート範囲のフォワーディングが有効になります。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[ファイアウォール] > [ポート範囲のトリガー]

[ファイアウォール] > [ポート範囲のトリガー]

[アプリケーション名]：設定するアプリケーションの名前を入力します。

[トリガー範囲]：各アプリケーションに対し、トリガーされるポート番号の範囲がリストされます。これらのポートは、発信トラフィックによって使用されます。必要なポート番号についての詳細は、インターネット アプリケーションのマニュアルを参照してください。最初のフィールドには、トリガーされる範囲の開始ポート番号を入力します。2 番目のフィールドには、トリガーされる範囲の終了ポート番号を入力します。

[フォワード範囲]：各アプリケーションに対し、転送されるポート番号の範囲がリストされます。これらのポートは、着信トラフィックによって使用されます。必要なポート番号についての詳細は、インターネット アプリケーションのマニュアルを参照してください。最初のフィールドには、転送される範囲の開始ポート番号を入力します。2 番目のフィールドには、転送される範囲の終了ポート番号を入力します。

[有効]：[有効] チェックボックスをオンにすると、関連アプリケーションのポート範囲のトリガーが有効になります。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[VPN]

[VPN] > [概要]

[VPN] > [概要]

[トンネルのステータス]

[x 個のトンネルを使用中]：使用されるトンネルの数が表示されます。

[x 個のトンネルが使用可能]：使用できるトンネルの数が表示されます。

[詳細] ボタン：[詳細] をクリックすると、トンネルの詳細情報が表示されます。

[番号]：トンネル番号が表示されます。

[名前]：[VPN] > [IPSec VPN] ウィンドウ上に表示される [トンネル名] フィールドによって定義されるトンネル名が表示されます。

[ステータス]：トンネルのステータスが表示されます。「接続済み」、「ホスト名の解決失敗」、「ホスト名の解決中」、「接続待機中」のいずれかになります。

[フェーズ 2 暗号化 / 認証]：選択したフェーズ 2 暗号化タイプ（3DES）、認証タイプ（MD5 または SHA1）、およびグループ（768 ビット、1024 ビット、または 1536 ビット）を [VPN] > [IPSec VPN] ウィンドウに表示します。

[ローカルグループ]：ローカル グループの IP アドレスおよびサブネットが表示されます。

[リモートグループ]：リモート グループの IP アドレスおよびサブネットが表示されます。

[リモートゲートウェイ]：リモート ゲートウェイの IP アドレスが表示されます。

[トンネルテスト]：[接続] をクリックすると、トンネル ステータスを確認でき、[ステータス] 列にテスト結果が更新されます。トンネルが接続されている場合は、[接続解除] をクリックすると、IPSec VPN 接続を切断できます。

[設定]：[編集] をクリックすると、トンネルの設定を変更できます。ごみ箱をクリックすると、すべてのトンネル設定を削除できます。

[x 個のトンネルが有効]：現在有効になっているトンネルの合計数が表示されます。

[x 個のトンネルが定義済み]：現在定義されているトンネルの数が表示されます。定義されたトンネルで無効にされているものがある場合、この数は [x 個のトンネルが有効] フィールドの値よりも大きくなります。

[VPN クライアントのステータス]

[番号]：1 ～ 5 のユーザ番号が表示されます。

[ユーザ名]：VPN クライアントのユーザ名が表示されます。

[ステータス]：VPN クライアントの接続ステータスが表示されます。

[開始時間]:指定した VPN クライアントの最新の VPN セッションの開始日時が表示されます。

[終了時間]：VPN クライアントが接続解除されている場合、VPN セッションの終了日時が表示されます。

[期間]：最後の VPN セッションの合計の接続時間が表示されます。

[接続解除]：VPN クライアント テーブルの各行の最後にある、[接続解除] ボックスをオンにし、[接続解除] ボタンをクリックすると、VPN クライアント セッションが接続解除されます。

[VPN] > [IPSec VPN]

[VPN] > [IPSec VPN] ウィンドウを使用すると、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）トンネルを作成および設定できます。

[VPN] > [IPSec VPN]

[トンネルエントリの選択]：新しいトンネルを作成するには、[new] を選択します。既存のトンネルを設定するには、そのトンネルをドロップダウン メニューから選択します。

[削除]：このボタンをクリックすると、選択したトンネルのすべての設定が削除されます。

[概要]：このボタンをクリックすると、有効にしたすべてのトンネルの設定とステータスが表示されます。

[IPSec VPN トンネル]:[有効] オプションをオンにすると、このトンネルが有効になります。

[トンネル名]：「Anaheim Office」のようにこのトンネルの名前を入力します。

[ローカルグループの設定]

[ローカルセキュリティゲートウェイのタイプ]：[IP のみ] と [IP とドメイン名 (FQDN) による認証] の 2 つの設定があります。

- **[IP のみ]**: この設定では、[IP アドレス] フィールドにルータの WAN IP アドレスが自動的に表示されます。
- **[IP とドメイン名 (FQDN) による認証]**：この設定では、[IP アドレス] フィールドに WAN IP アドレスと、セキュリティ強化のためにドメイン名も自動的に表示されます。[ドメイン名] フィールドに任意のドメイン名を入力します。

[ローカルセキュリティグループのタイプ]:この VPN トンネルを使用できるルータの背後のローカル LAN ユーザを選択します。これには単一の IP アドレスまたはサブネットワークが指定できます。[ローカルセキュリティグループのタイプ] は、その他のルータの [リモートセキュリティグループのタイプ] に一致する必要があることに注意してください。

[IP アドレス]：ローカル ネットワーク上の IP アドレスを入力します。

[サブネットマスク]:[ローカルセキュリティグループのタイプ] が [サブネット] に設定されている場合は、マスクを入力してローカル ネットワーク上の IP アドレスを判断します。

[リモートグループの設定]

[リモートセキュリティゲートウェイのタイプ]:[IP のみ] または [IP とドメイン名 (FQDN) による認証] を選択します。この設定は、トンネルのもう一端の VPN デバイスの [ローカルセキュリティゲートウェイのタイプ] に一致する必要があります。

- **[IP のみ]**：このオプションを選択すると、トンネルにアクセスできるリモート デバイスを指定できます。その後、ドロップダウン メニューから [IP アドレス] を選択してリモート ゲートウェイの WAN IP アドレスを [IP アドレス] フィールドに入力するか、またはドロップダウン メニューから [DNS 解決による IP] を選択してリモート ゲートウェイのドメイン名を [ドメイン名] フィールドに入力します。
- **[IP とドメイン名 (FQDN) による認証]**：このオプションを選択すると、セキュリティを高めるために、IP アドレスおよびドメイン名を含めることが可能です。任意のド

メイン名を [ドメイン名] フィールドに入力します。その後、ドロップダウン メニューから [IP アドレス] または [DNS 解決による IP] を選択し、[IP アドレス] フィールドまたは [ドメイン名] フィールドに記入します。

[リモートセキュリティグループのタイプ]：リモート ゲートウェイの背後でこの VPN トンネルを使用可能なリモート LAN ユーザを選択します。これには単一の IP アドレスまたはサブネットワークが指定できます。[リモートセキュリティグループのタイプ] は、その他のルータの [ローカルセキュリティグループのタイプ] に一致する必要があることに注意してください。

[IP アドレス]：リモート ネットワークの IP アドレスを入力します。

[サブネットマスク]：[リモートセキュリティグループのタイプ] が [サブネット] に設定されている場合は、マスクを入力してリモート ネットワーク上の IP アドレスを判断します。

[IPSec の設定]

[キー入力モード]：ルータは、自動キー管理と手動キー管理の両方をサポートしています。自動キー管理を選択すると、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルを使用して Security Association（SA; セキュリティ アソシエーション）のキー マテリアルをネゴシエートします。手動キー管理を選択する場合は、キー ネゴシエーションは不要です。基本的に、手動キー管理は小規模の固定環境またはトラブルシューティング目的で使用されます。接続する両側で同一のキー管理方式を使用する必要があることに注意してください。

フェーズ 1

- **[暗号化]**：[暗号化] 方式で ESP パケットの暗号化 / 復号化に使用されるキーの長さを決定します。3DES だけがサポートされています。接続する両側で同一のキー暗号化方式を使用する必要があります。
- **[認証]**：[認証] で ESP パケットの認証方式を決定します。[MD5] または [SHA1] のいずれかを選択できます。両側（VPN の両エンドポイント）で同一の認証方式を使用する必要があります。
- **[MD5]**：単方向のハッシュ アルゴリズムで、128 ビットのダイジェストを生成します。
- **[SHA1]**：単方向のハッシュ アルゴリズムで、160 ビットのダイジェストを生成します。
- **[グループ]**：キー エクスチェンジに使用される Diffie-Hellman（DH）グループです。[768 ビット]（グループ 1）、[1024 ビット]（グループ 2）、または [1536 ビット]（グループ 5）のアルゴリズムを選択します。セキュリティは、グループ 5 が最も高く、グループ 1 が最も低くなります。
- **[キーライフタイム]**：IKE 生成キーのライフタイムを指定します。時間が期限切れになると、新しいキーが自動的に再ネゴシエートされます。300 ～ 100,000,000 秒の値を入力します。デフォルトは **28800** 秒です。

フェーズ 2

- **[暗号化]**:[暗号化] 方式で ESP パケットの暗号化/復号化に使用されるキーの長さを決定します。3DES だけがサポートされています。両側で同一の暗号化方式を使用する必要があることに注意してください
- **[認証]**：[認証] で ESP パケットの認証方式を決定します。[MD5] または [SHA1] のいずれかを選択できます。両側（VPN エンドポイント）で同一の認証方法を使用する必要があることに注意してください。
- **[MD5]**：単方向のハッシュ アルゴリズムで、128 ビットのダイジェストを生成します。
- **[SHA1]**：単方向のハッシュ アルゴリズムで、160 ビットのダイジェストを生成します。
- **[PFS(完全転送秘密)]**：PFS を有効にすると、IKE フェーズ 2 のネゴシエーションで IP トラフィックの暗号化および認証用の新しいキー マテリアルが生成されます。この設定は両側で選択する必要があることに注意してください。
- **[事前共有キー]**：IKE は、[事前共有キー] フィールドを使用してリモート IKE ピアを認証します。このフィールドには、たとえば、「My_@123」や「0x4d795f40313233」のように、文字と 16 進数の両方を入力できます。両側で同じ事前共有キーを使用する必要があるので注意してください。
- **[グループ]**：キー エクスチェンジに使用される Diffie-Hellman（DH）グループです。[768 ビット]（グループ 1）、[1024 ビット]（グループ 2）、または [1536 ビット]（グループ 5）のアルゴリズムを選択します。セキュリティは、グループ 5 が最も高く、グループ 1 が最も低くなります。
- **[キーライフタイム]**：IKE 生成キーのライフタイムを指定します。時間が期限切れになると、新しいキーが自動的に再ネゴシエートされます。300 ～ 100,000,000 秒の値を入力します。デフォルトは **3600** 秒です。

[ステータス]

[ステータス]：選択したトンネルの接続ステータスが表示されます。状態は接続、または接続解除のいずれかになります。

[接続]：このボタンをクリックすると、現在の VPN トンネルの接続が確立されます。変更を加えた場合は、[保存] をクリックしてまず変更を適用してください。

[接続解除]：このボタンをクリックすると、現在の VPN トンネルの接続が切断されます。

[ログの表示]：このボタンをクリックすると、VPN ログを確認でき、確立したそれぞれのトンネルの詳細が表示されます。

[詳細設定]：このボタンをクリックすると、次の追加設定が表示されます。

[アグレッシブモード]：フェーズ 1 の交換の種類として、メイン モード、またはアグレッシブ モードを指定します。このチェックボックスをオンにするとアグレッシブ モードが選択され、オフ（デフォルト）にするとメイン モードが選択されます。アグレッシブ モードでは、SA 交換のフェーズ 1 で、メイン モードメッセージの半分の量が交換される必要があります。ネットワーク セキュリティを重視する場合は、メイン モードを選択してください。

[NetBios ブロードキャスト]：このチェックボックスをオンにすると、NetBIOS トラフィックが VPN トンネルを通過できるようになります。デフォルトでは、RVS4000 はこのブロードキャストをブロックします。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[VPN] > [VPN クライアントアカウント]

このウィンドウを使用すると、VPN クライアント ユーザを管理できます ウィンドウ上部に情報を入力すると、指定されたユーザの情報が表に表示されます。この機能は、Cisco QuickVPN クライアントだけで使用できます （ルータはデフォルトで、最大 5 つの Cisco QuickVPN クライアントをサポートします）。

[VPN] > [VPN クライアントアカウント]

[ユーザ名]：ユーザ名を入力します。ユーザ名には、キーボードの任意の文字の組み合わせを使用できます。

[パスワード]：このユーザに割り当てるパスワードを入力します。

[パスワードの再入力]：パスワードを再入力して、正しく入力されたことを確認できます。

[ユーザによるパスワードの変更を許可する]：このオプションは、ユーザが自分のパスワードを変更できるかどうかを決定します。

[VPN クライアントリストテーブル]

[番号]：ユーザ番号が表示されます。

[アクティブ]：オンにすると、指定されたユーザが接続できますが、オフにすると、VPN クライアント アカウントが無効にされます。

[ユーザ名]：ユーザ名が表示されます。

[編集]：ユーザ名とパスワードの編集ができます。

[削除]：このボタンをクリックすると、ユーザ アカウントが削除されます。

[証明書管理]

このセクションでは、ルータと QuickVPN クライアント間の通信を確実に行うために使用される証明書を管理できます。

[生成]：このボタンをクリックすると、新しい証明書が作成されて、ルータの既存の証明書と交換されます。

[管理者用エクスポート]：このボタンをクリックすると、管理者の証明書がエクスポートされます。プロンプトが表示されたら、証明書の保存先を指定します。デフォルトのファイル名は「RVS4000_Admin.pem」ですが、別の名前も使用できます。管理者の証明書は秘密鍵を含んでおり、バックアップとして安全な場所に保存する必要があります。ルータのコンフィギュレーションを工場出荷時のデフォルト設定にリセットすると、この証明書をインポートしてルータに保存できます。

[クライアント用エクスポート]：このボタンをクリックすると、クライアントの証明書がエクスポートされます。プロンプトが表示されたら、証明書の保存先を指定します。デフォルトのファイル名は「RVS4000_Client.pem」ですが、別の名前も使用できます。QuickVPN ユーザがルータに確実に接続するためには、この証明書を QuickVPN クライアントのインストール ディレクトリに置く必要があります。

[インポート]：このボタンをクリックすると、前に [管理者用エクスポート] または [クライアント用エクスポート] を使用してファイルに保存した証明書がインポートされます。ファイル名をフィールドに入力するか、または [参照] をクリックしてコンピュータ上のファイルを見つけて、[インポート] をクリックします。

[証明書の最終生成 / インポート日時]:証明書が最後に作成またはインポートされた日時が表示されます。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[VPN] > [VPN パススルー]

[VPN] > [VPN パススルー]

[IPSec パススルー]:Internet Protocol Security（IPSec; インターネット プロトコル セキュリティ）は、IP レイヤでパケットの安全な交換を実装するために使用されるプロトコルのスイートです。IPSec パススルーはデフォルトで有効になっており、IPSec トンネルはルータを通過できます。IPSec パススルーを無効にするには、[無効] を選択します。

[PPTP パススルー]:ポイントツーポイント トンネリング プロトコル（PPTP）によって、ポイント ツー ポイント プロトコル（PPP）は IP ネットワーク経由でトンネリングできます。PPTP パススルーはデフォルトで有効になっています。無効にするには、[無効] を選択します。

[L2TP パススルー]:レイヤ 2 トンネリング プロトコルは、レイヤ 2 レベルでインターネット経由のポイント ツー ポイント セッションを有効にするために使用される方法です。L2TP パススルーはデフォルトで有効になっています。L2TP パススルーを無効にするには、[無効] を選択します。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[QoS]

QoS（Quality of Service）を使用すると、[レート制御] または [プライオリティ] によって帯域幅管理を実行できます。QoS の Trust Mode および DSCP 設定も設定できます。

[QoS] > [帯域幅管理]

[QoS] > [帯域幅管理] : [レート制御]

[帯域幅管理]

このセクションでは、WAN インターフェイス上の ISP によって提供される最大帯域幅を、アップストリームとダウンストリームの両方向に対して指定できます。

[帯域幅管理のタイプ]

[タイプ]：帯域幅管理のタイプです。[レート制御]、[プライオリティ]（デフォルト）のいずれかになります。選択内容によって、ウィンドウ下部に [レート制御] セクション、または [プライオリティ] セクションが表示されます。

[レート制御]

[サービス]：ドロップダウン メニューからサービスを選択します。必要なサービスがない場合は、[サービスの管理] をクリックし、そのサービスを追加します。

[IP]：制御する IP アドレスまたは IP 範囲を入力します。デフォルトは 0 であり、すべての内部 IP アドレスが含まれます。

[方向]：発信トラフィックの場合は [アップストリーム]、着信トラフィックの場合は [ダウンストリーム] を選択します。

[最小 レート]：保証帯域幅としての最低速度を入力します。

[最大レート]：保証帯域幅としての最高速度を入力します。

[有効]：この速度制御ルールを有効にする場合は、このチェックボックスをオンにします。

[リストに追加]：ルールを設定した後、このボタンをクリックすると、そのルールがリストに追加されます。リストには、最大 15 のエントリを含ませることが可能です。

[選択したアプリケーションを削除]：このボタンをクリックすると、リストからルールが削除されます。

[プライオリティ]

[QoS] > [帯域幅管理] : [プライオリティ]

[サービス]：ドロップダウン メニューからサービスを選択します。必要なサービスがない場合は、[サービスの管理] をクリックし、そのサービスを追加します。

[方向]：ドロップダウン メニューから、発信トラフィックの場合は [アップストリーム]、着信トラフィックの場合は [ダウンストリーム] を選択します。

[プライオリティ]：サービスのプライオリティとして、[高]、[中]、[標準]、または [低] を選択します。デフォルトは [中] です。

[有効]：このプライオリティ ルールを有効にする場合は、このチェックボックスをオンにします。

[リストに追加]：ルールを設定した後、このボタンをクリックすると、そのルールがリストに追加されます。リストには、最大 15 のエントリを含ませることが可能です。

[選択したアプリケーションを削除]：このボタンをクリックすると、リストからルールが削除されます。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[QoS] > [QoS の設定]

[QoS の設定] ウィンドウを使用すると、各 LAN ポートの QoS Trust Mode を設定できます。

[QoS] > [QoS の設定]

[ポート ID]：LAN ポートの数です。

[信頼モード]：[ポート]、[CoS]、[DSCP] のいずれかを選択します。デフォルトは [ポート] です。

[デフォルト CoS/ ポート] のプライオリティ：Trust Mode が [ポート] に設定されている場合は、ドロップダウン メニューからポートのプライオリティとして、[1] ～ [4] を選択します。ここで、[4] が最高のプライオリティです。Trust Mode が [CoS] に設定されている場合は、ドロップダウン メニューから、デフォルトの CoS プライオリティとして、[0] ～ [7] を選択します。

[CoS の設定]

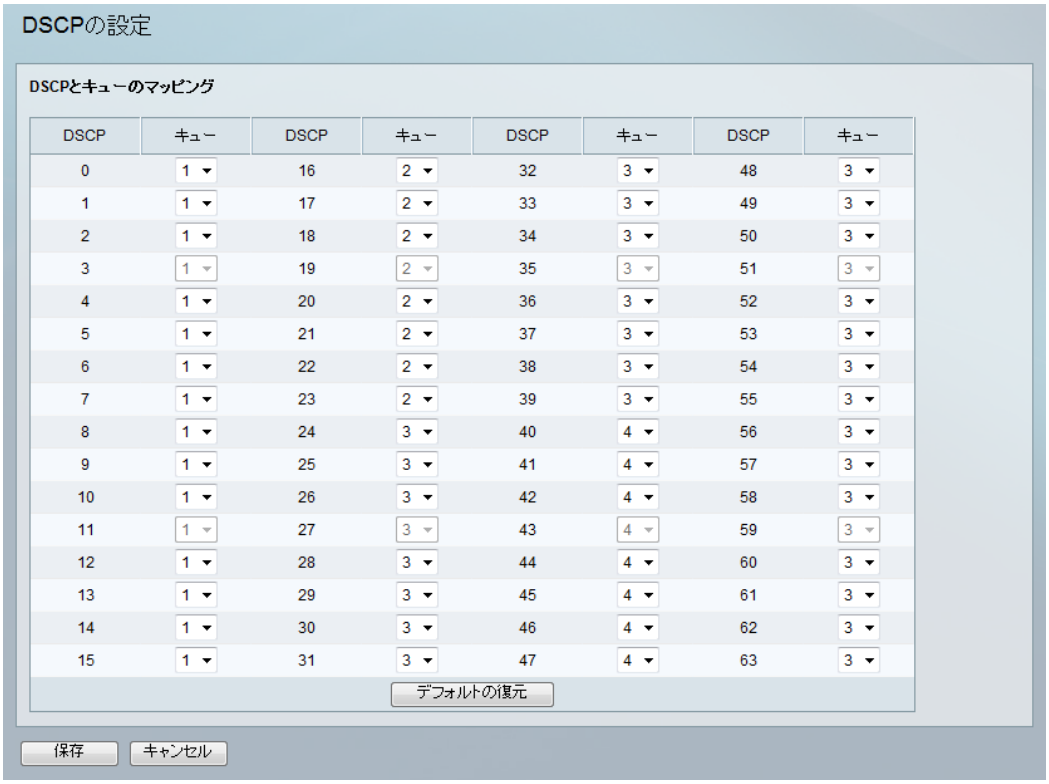
[プライオリティ]：[0] ～ [7] の CoS プライオリティです。

[キュー]：CoS プライオリティがマッピングされるトラフィック フォワーディング キューとして、[1] ～ [4] を選択します。[キュー] が [4] の場合が、最高のプライオリティとなります。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[QoS] > [DSCP の設定]

[QoS] > [DSCP の設定]



[DSCP]：着信パケットの DiffServ コード ポイント値です。

[キュー]：DSCP プライオリティがマッピングされるトラフィック フォワーディング キューとして、[1] ～ [4] を選択します。[キュー] が [4] の場合が、最高のプライオリティとなります。

[デフォルトの復元]：このボタンをクリックすると、デフォルトの DSCP 値が復元されます。

[保存] をクリックして変更を保存するか、[キャンセル] をクリックして変更を元に戻します。

[各種管理]

[各種管理] メニューでは、システム管理設定とツールを設定できます。

[各種管理] > [管理]

[各種管理] > [管理]

[ルータへのアクセス]

[ルータのユーザリスト]：目的のルータ ユーザ リストを選択します。

[ルータのユーザ名]：ユーザ名をここに入力します。

[ルータのパスワード]：パスワードを入力します。

[パスワードの再入力]：このフィールドにパスワードを入力します。

[SNMP]

[SNMP]：SNMP を使用する場合は、[有効] を選択します。SNMP を使用するには、ご使用の PC に SNMP ソフトウェアがインストールされている必要があります。

[システム名]：このデバイスを識別する適切な名前を入力します。この名前は、ご使用の SNMP ソフトウェアに表示されます。

[システムコンタクト先]：システムのコンタクト先情報を入力します。

[システムロケーション]：システムのロケーションを入力します。

[読み取りコミュニティ]：SNMP の「Get」コマンドに使用する SNMP のコミュニティ名を入力します。

[書き込みコミュニティ]：SNMP の「Set」コマンドに使用する SNMP のコミュニティ名を入力します。

[トラップコミュニティ]：SNMP の「Trap」コマンドに使用する SNMP のコミュニティ名を入力します。

[トラップ先]：トラップの送信先となる SNMP マネージャの IP アドレスを入力します。必要に応じて空白にもできます。

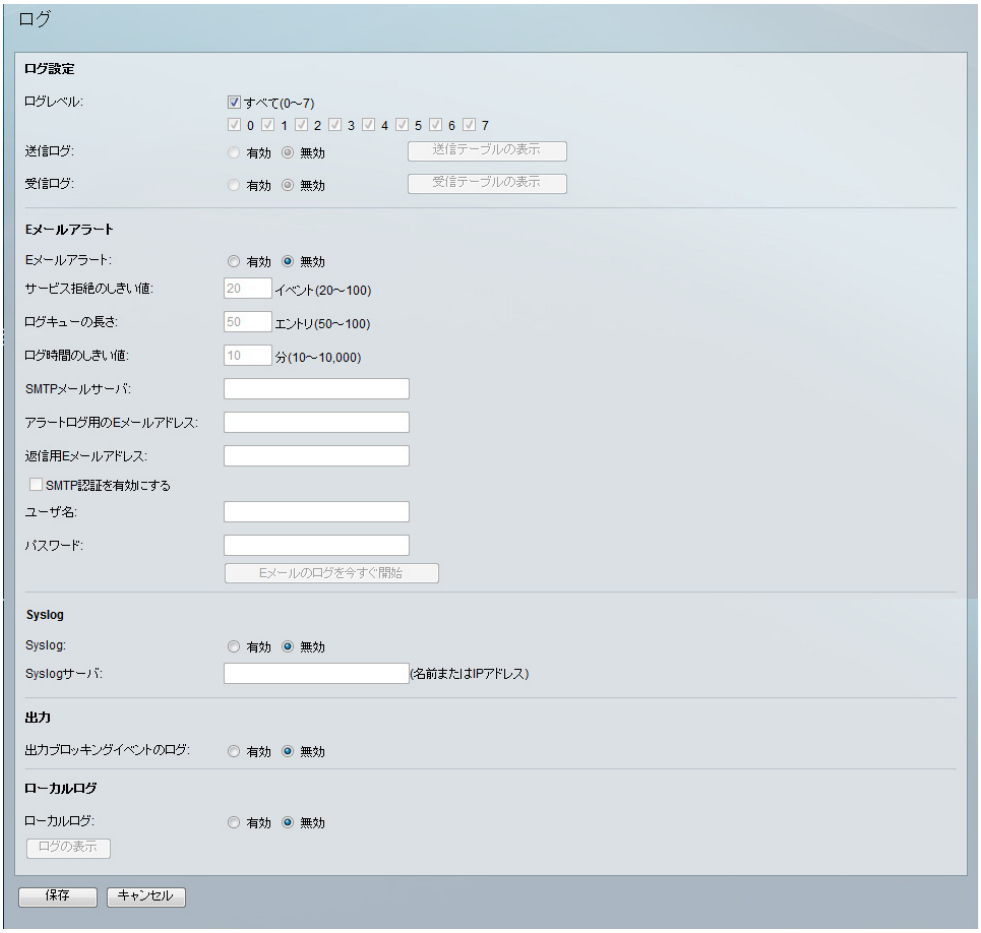
[UPnP]

Universal Plug and Play（UPnP; ユニバーサル プラグ アンド プレイ）を使用すると、ネットワーク上にパブリック サービスを設定できます。UPnP 機能を有効にすると、Windows XP は、UPnP フォワーディング テーブルでエントリを追加または削除できます。一部のインターネット ゲームでは、UPnP を有効にする必要があります。

[UPnP]：UPnP を使用する場合は、デフォルト設定の [有効] のままにします。それ以外の場合は、[無効] を選択します。

[各種管理] > [ログ]

[各種管理] > [ログ]



[ログ設定]

[ログレベル]：ルータが記録する必要があるログ レベルを選択します。各ログ レベルと、その意味を次に示します。

ログ レベル

レベル	重大度名	説明
7	LOG_DEBUG	デバッグ レベルのメッセージ
6	LOG_INFO	通知メッセージ
5	LOG_NOTICE	正常であるが注意を要する状態

ログ レベル

レベル	重大度名	説明
4	LOG_WARNING	警告状態
3	LOG_ERR	エラー状態
2	LOG_CRIT	クリティカルな状態
1	LOG_ALERT	ただちに対処が必要
0	LOG_EMERG	システム使用不能

[送信ログ]：[有効] を選択すると、すべての発信パケットのログが記録されます。その後、[送信テーブルの表示] をクリックすると、送信元 IP、宛先 IP、サービス番号、ポート番号などの発信パケットの情報が表示されます。

[受信ログ]：[有効] を選択すると、すべての着信パケットのログが記録されます。その後、[受信テーブルの表示] をクリックすると、送信元 IP、宛先 IP、サービス番号、ポート番号などの着信パケットの情報が表示されます。

[E メールアラート]

[E メールアラート]：[有効] を選択すると、サービス拒絶（DoS）攻撃が検出されるとすぐに E メールが送信されます。有効にする場合は、このセクションの残りのフィールドに E メール アドレス情報を記入します。

[サービス拒否のしきい値]：E メールの通知が送信される前に、内蔵のファイアウォールによってブロックする必要があるサービス拒絶（DoS）攻撃の数を入力します。最小値は 20、最大値は 100 です。

[ログキューの長さ]：デフォルトは 50 エントリです。50 を超えるエントリがある場合、ルータはログを E メールで送信します。

[ログ時間のしきい値]：デフォルトは **10** 分です。ルータは、10 分ごとにログを E メールで送信します。

[SMTP メールサーバ]：E メールの送信に使用する Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）サーバのアドレス（ドメイン名）または IP アドレスを入力します。

[アラートログ用の E メールアドレス]：ログの送信先 E メール アドレスを入力します。

[返信用 E メールアドレス]：このアドレスは、E メール内の送信者のアドレスとして表示されます。

[SMTP 認証を有効にする]：ご使用の SMTP サーバが認証を必要とする場合は、ここで有効にし、ユーザ名およびパスワードを入力できます。

[E メールのログを今すぐ開始]：このボタンをクリックすると、ただちにログが E メールで送信されます。

[Syslog]

[Syslog] - [有効]：この機能を使用する場合に、このチェックボックスをオンにします。

[Syslog サーバ]：[Syslog] の [有効] チェックボックスをオンにした場合は、このフィールドに IP アドレスを入力します。

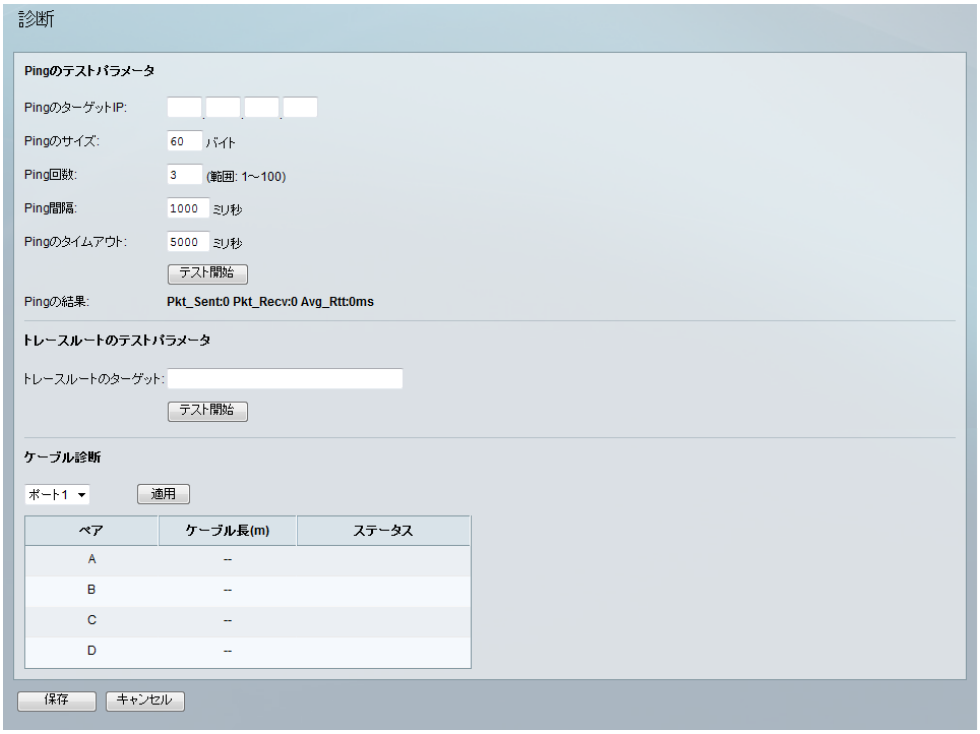
[ローカルログ]

[ローカルログ]：着信 URL および発信 URL、または IP アドレスのログをすべて表示する場合は、これを [有効] にします。

[ログの表示]：ログを表示する場合、このボタンをクリックします。ログ データが新しいウィンドウに表示されます。

[各種管理] > [診断]

[各種管理] > [診断]



[Pingのテストパラメータ]

[Pingのターゲット IP]：Ping する IP アドレスまたは URL を入力します。

[Pingのサイズ]：使用するパケットのサイズを入力します。

[Ping回数]：対象のデバイスを Ping する回数を入力します。

[Ping間隔]：各 Ping の間隔時間（ミリ秒単位）を入力します。

[Pingのタイムアウト]：目的の時間（ミリ秒単位）を入力します。定義された Ping の時間内に応答が受信されない場合は、Ping が失敗したと見なされます。

[テスト開始]：ボタンをクリックすると、テストが開始されます。テスト結果が新しいウィンドウに表示されます。

[Pingの結果]：Ping 状態が表示されます。

[トレースルートのテストパラメータ]

[トレースルートのターゲット]：トレース ルート テストの対象 IP アドレスを入力します。

[テスト開始]：ボタンをクリックすると、テストが開始されます。テスト結果が新しいウィンドウに表示されます。

[ケーブル診断]

[ポート]：ドロップダウン メニューからポート番号を選択します。

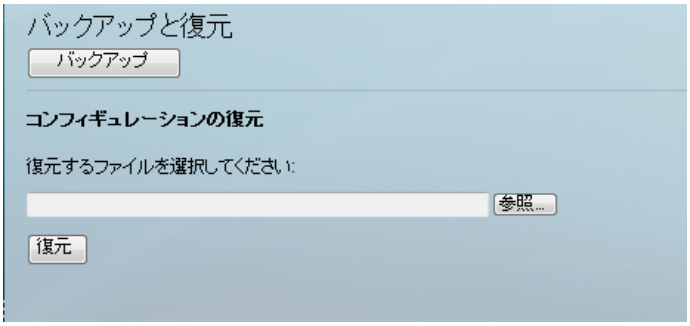
[ペア]：ケーブルの特定のペア（A、B、C、D）を識別します。各ケーブルは 8 ピン（4 ペア）で構成されます。

[ケーブル長 (m)]：ケーブルの長さをメートル単位で表示します。

[ステータス]：ペアの状態が表示されます。

[各種管理] > [バックアップと復元]

[各種管理] > [バックアップと復元]



現在のコンフィギュレーションのコピーをダウンロードして PC にそのファイルを保存するには、[バックアップ] をクリックすると、ダウンロードが開始されます。

[コンフィギュレーションの復元]

前に保存した config ファイルをルータに復元するには、このフィールドにファイル名を入力し、[参照] をクリックして config ファイルを選択し、[復元] をクリックして config ファイルをアップロードします。

[各種管理] > [工場出荷時設定]

[各種管理] > [工場出荷時設定]

[工場出荷時設定の復元]：このボタンをクリックすると、すべてのコンフィギュレーション設定が工場出荷時のデフォルト値にリセットされます。デフォルト設定が復元されると、前に保存したすべての設定が失われます。このボタンをクリックすると、別のウィンドウが表示されます。継続するには [OK] をクリックします。システムのリブート中に別のウィンドウが表示されます。

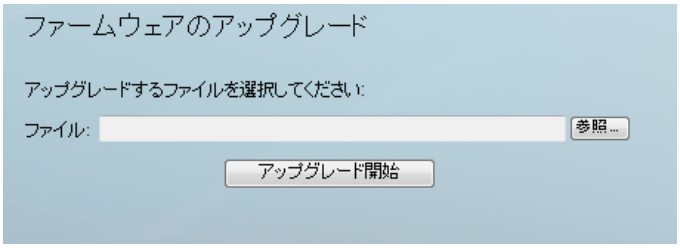
[各種管理] > [リブート]

[各種管理] > [リブート]

[リブート]：このボタンをクリックすると、ルータがリブートします。この操作では、ルータに保存されている設定が失われません。

[各種管理] > [ファームウェアのアップグレード]

[各種管理] > [ファームウェアのアップグレード]

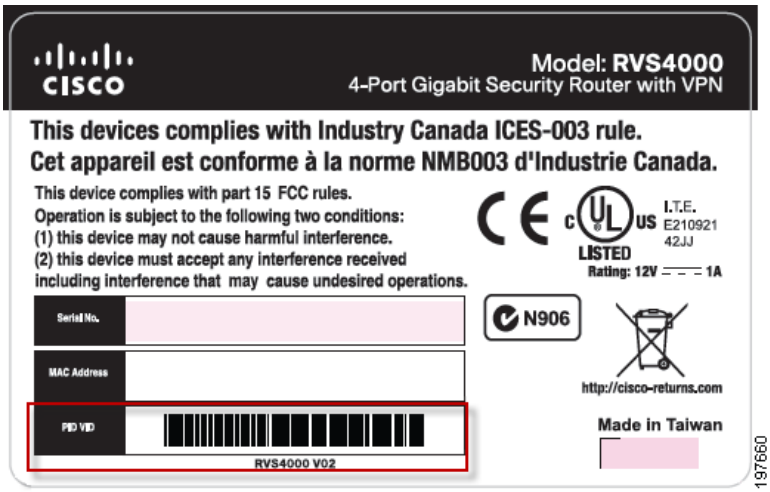


このページを使用すると、Cisco.com からのファームウェアを使用してルータをアップグレードできます。段階的な手順を次のページに示します。

[ファイル]：展開したファームウェア アップグレードの名前を入力するか、または [参照] をクリックしてファイルを検索します。

[アップグレード開始]：該当するファイルを選択したら、[アップグレード開始] をクリックし、画面上の手順に従ってファームウェアをアップグレードします。

ステップ 1 ルータのバージョンを、底面パネルのラベルを参照して確認します。PIDVID 番号には、V01（バージョン 1）または V02（バージョン 2）が含まれています。



ステップ 2 ルータの最新ファームウェアを確認するには、www.cisco.com/jp/go/sb にアクセスします。

ステップ 3 ルータのリンクをクリックします。

ステップ 4 [Download Firmware] ボタンをクリックします。

ステップ 5 画面の指示に従って、最新のファームウェアをダウンロードします。

ステップ 6 ファームウェア ファイルをコンピュータで展開します。

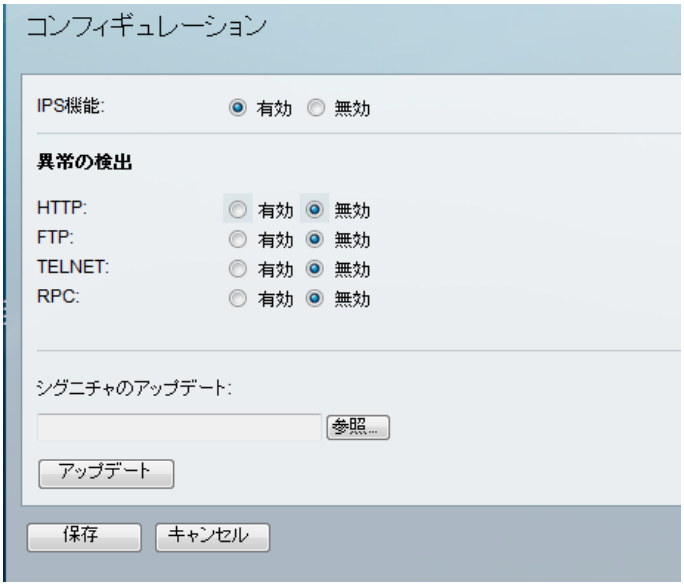
ステップ 7 [各種管理] > [ファームウェアのアップグレード] ページで、[参照] をクリックし、ファイルを検索します。

ステップ 8 [アップグレード開始] をクリックします。

[IPS]

[IPS] > [コンフィギュレーション]

[IPS] > [コンフィギュレーション]



[IPS 機能]：IPS 機能を有効にするには [有効] を選択し、無効にするには [無効] を選択します。

[異常の検出]

[HTTP]：Web 攻撃シグニチャが照合されます。HTTP 要求デコーダにより、パターン マッチの前に（Whisker で説明されている回避メソッドに従って）UTF-8（1、2、および 3 バイト）コードがデコードされ、URI が正規化されます。

[FTP]：FTP バウンスが検知され、Telnet オペコードの FTP コマンド ストリームへの挿入が検知されます。

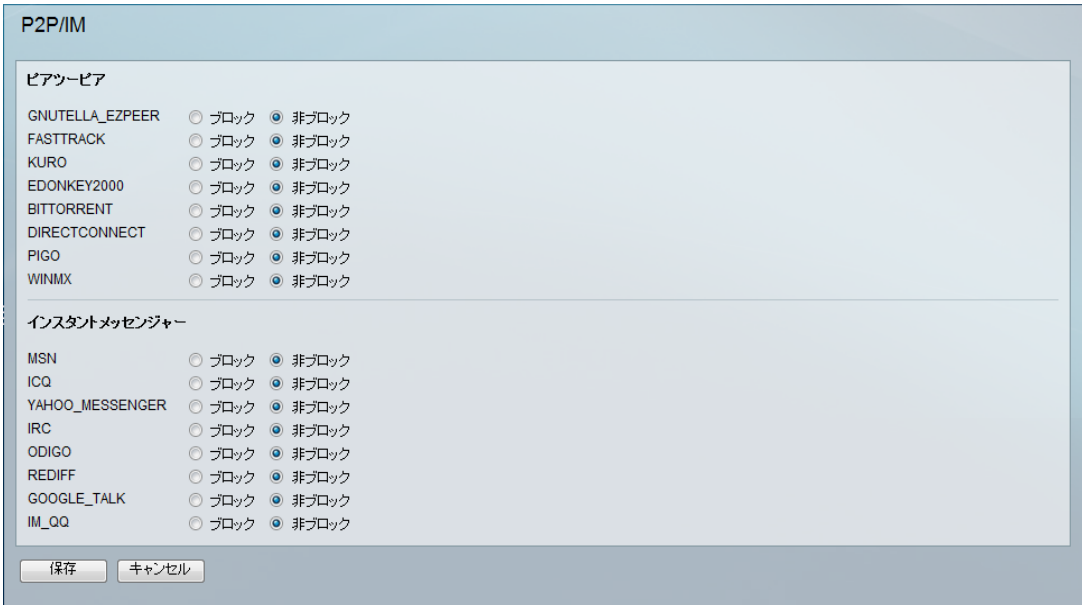
[TELNET]：Telnet ネゴシエーション文字列が正規化されます。

[RPC]：RPC レコードの断片化を検知します。

[シグニチャのアップデート]：シグニチャ ファイルをアップグレードする前に、Cisco Web サイトから Router Intrusion Prevention System（IPS; 侵入防御システム）ファイルを取得します。ファイルを見つけるには、www.cisco.com/go/software（登録とログインが必要）にアクセスして、RVS4000 を検索します。ファイルのダウンロードおよび展開を行った後、IPS シグニチャ ファイル名を [シグニチャのアップデート] フィールドに入力するか、または [参照] をクリックしてファイルを検索します。その後、[アップデート] をクリックし、画面上の手順に従ってください。

[IPS] > [P2P/IM]

[ピアツーピア]



[ピアツーピア]

ピアツーピア ファイル共有アプリケーションを、ブロック（[ブロック]）または許可（[非ブロック]）できます。事前に設定されたファイル共有ネットワークは、GNUTELLA（EZPEER）、FASTTRACK、KURO、EDONKEY2000、BITTORRENT、DIRECTCONNECT、PIGO、および WINMX です。

[インスタントメッセンジャー]

インスタント メッセージング アプリケーションを、ブロック（[ブロック]）または許可（[非ブロック]）できます。事前に設定されたインスタント メッセージング アプリケーションは、MSN、ICQ、YAHOO_MESSENGER、IRC、ODIGO、REDIFF、GOOGLE_TALK、および IM_QQ です。

[IPS] > [レポート]

過去 24 時間のネットワークのトラフィックおよび攻撃のレベルをグラフィカルに表示します。

[攻撃元]

攻撃元の IP アドレス、および攻撃の頻度（回数）が表示されます。

[攻撃されたカテゴリ]

攻撃のカテゴリ（種類）、および攻撃の頻度（回数）が表示されます。

[IPS] > [レポート]

[IPS] > [情報]

[IPS] > [情報]

[シグニチャバージョン]：悪意のある脅威を防ぐ、ルータのシグニチャ パターンのバージョンが表示されます。

[最終アップロード]:ルータのシグニチャ パターンが最後に更新された日時が表示されます。

[保護の範囲]：ルータの IPS 機能が防御した攻撃の種類が表示されます。

[L2 スイッチ]

[L2 スイッチ] > [VLAN の作成]

VLAN は、ハードウェア ソリューションを定義する代わりにソフトウェアを介して作成される Local Area Network（LAN; ローカル エリア ネットワーク）の論理サブグループです。VLAN は、接続する物理 LAN セグメントにかかわらず、ユーザ ステーションとネットワーク デバイスを単一のドメインに組み合わせます。VLAN は、より効率的なネットワーク トラフィック フローをサブグループで実現します。VLAN がソフトウェア経由で管理を行うと、ネットワークの変更を実装する時間が削減されます。

VLAN はソフトウェア ベースであり、物理的属性によって定義されないため、VLAN には最小ポート数がなく、ユニットごと、デバイスごと、スタックごと、または他の論理接続の組み合わせで作成できます。

VLAN は、レイヤ 2 で動作します。VLAN はトラフィックを VLAN 内に隔離するため、トラフィックが VLAN 間を流れるようにするためにレイヤ 3 ルータが必要です。レイヤ 3 ルータはセグメントを識別し、VLAN と協調します。

VLAN は、ブロードキャストおよびマルチキャスト ドメインです。ブロードキャストおよびマルチキャスト トラフィックは、トラフィックが生成される VLAN 内だけで伝送されます。

RVS4000 は、デフォルト VLAN を含む、最大 4 つの VLAN をサポートしています。

[L2 スイッチ] > [VLAN の作成]

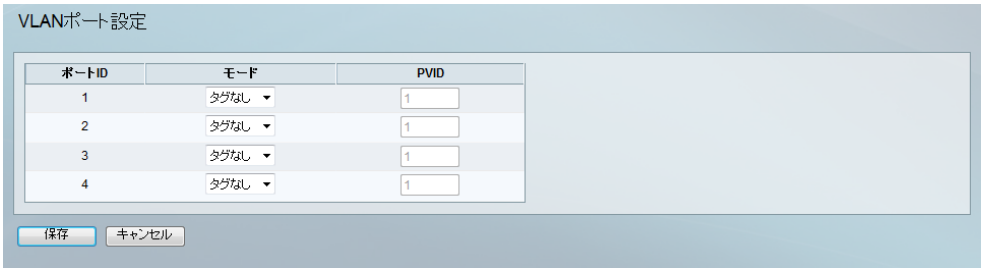
[VLAN ID]：VLAN ID 番号です。2 ～ 3290、または 3293 ～ 4094 の任意の値に設定できます（VLAN ID 1 はデフォルト VLAN 用に予約されており、インターフェイスで受信されたタグなしフレームに使用されます VLAN ID 3291 ～ 3292 は予約済みで使用不可です）。VLAN を作成するには、ID 番号を入力して [VLAN を追加] をクリックします。

[VLAN ID の範囲]：ある範囲の ID 番号を持つ複数の VLAN を作成するには、開始 ID 番号および終了 ID 番号を入力し、[範囲を追加] をクリックします。

[選択した VLAN を削除]：VLAN を削除するには、その VLAN を VLAN リストから選択し、[選択した VLAN を削除] をクリックします。

[L2 スイッチ] > [VLAN ポート設定]

[L2 スイッチ] > [VLAN ポート設定]



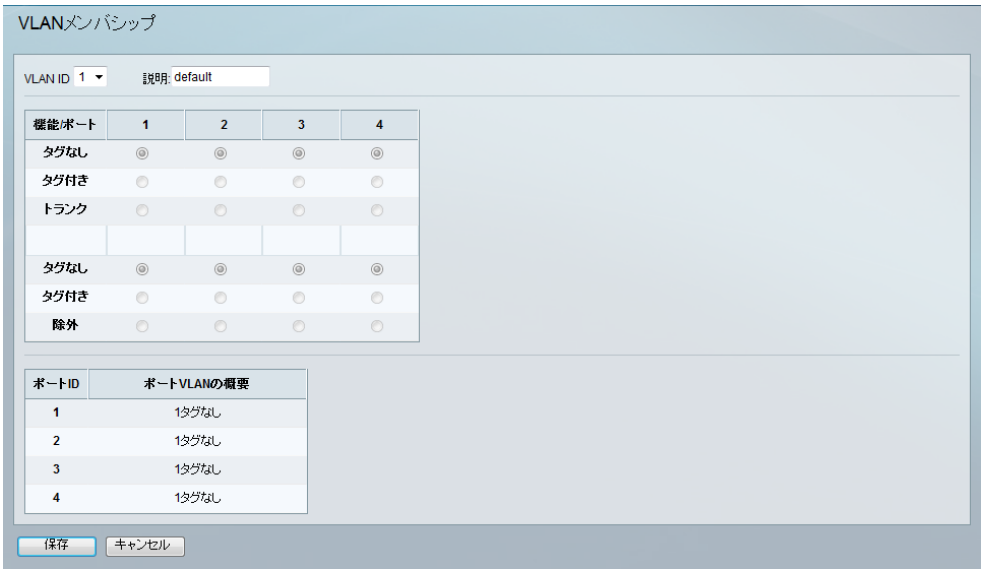
[ポート ID]：1 ～ 4 のポート番号が表示されます。

[モード]：ポートのモードを、[トランク]、[タグなし]、[タグ付き] から選択します。デフォルトは [タグなし] です。トランク モードでは、着信フレームおよび発信フレームをタグ付き、またはタグなしに設定でき、着信タグなしフレームはデフォルトの Port VLAN ID（PVID; ポート VLAN ID）でタグ付けされます。タグなしモードでは、すべての着信フレームおよび発信フレームはタグなしです。タグ付きモードでは、すべての着信フレームおよび発信フレームはタグ付きである必要があり、すべてのタグなしフレームはドロップされます。

[PVID]：インターフェイスで受信された、タグなしフレームに割り当てられたポート VLAN ID（PVID）です。デフォルトは **1** です。[モード] が [タグ付き] である場合、ポートがタグ付きフレームだけを受信するため、ポートには PVID がありません。

[L2 スイッチ] > [VLAN メンバシップ]

[L2 スイッチ] > [VLAN メンバシップ]



[VLAN ID]：メンバシップを設定する VLAN を選択します。

[説明]：最大 50 文字の VLAN グループ名を入力します。

[機能 / ポート] テーブル：テーブルの上半分に、各ポートの現在のモード（[タグなし]、[タグ付き]、または [トランク]）が表示されます。テーブルの下半分は、選択した VLAN のポート メンバシップを割り当てるために使用されます。各ポートのデフォルトは [除外]（ポートが VLAN のメンバでない）です。ポートを VLAN のメンバにするには、適用できるモードを選択します。たとえば、ポート モードが [タグなし] の場合は [タグなし] を選択し、モードが [タグ付き] の場合は [タグ付き] を選択し、モードが [トランク] の場合は [タグ付き] または [タグなし] を選択します。

[L2 スイッチ] > [RADIUS]

[L2 スイッチ] > [RADIUS]

[モード]：ドロップダウン メニューから [有効] または [無効] を選択して、RADIUS の有効/無効を切り替えます。

[RADIUS IP]：サーバ IP アドレスを入力します。

[RADIUS UDP ポート]：UDP ポートを入力します。UDP ポートは、RADIUS サーバ認証を確認するために使用します。

[RADIUS シークレット]：デバイスと RADIUS サーバ間のすべての RADIUS 通信を認証および暗号化するためのキー文字列を入力します。このキーは、RADIUS サーバの暗号キーと一致する必要があります。ホスト固有の値が指定されない場合、グローバル値が各ホストに適用されます。

[管理の状態]：ポートの許可状態を指定します。予想されるフィールド値は次のとおりです。

- **[自動]**：認証方式によって制御対象のポートの状態が設定されます。
- **[Force Authorized]**：制御対象のポートの状態は、[Force Authorized]（トラフィックを転送）に設定されます。
- **[Force Unauthorized]**：制御対象のポートの状態は、[Force Unauthorized]（トラフィックを廃棄）に設定されます。

[ポートの状態]：選択したポートの状態が表示されます。

[L2 スイッチ] > [ポート設定]

[L2 スイッチ] > [ポート設定]

[ポート]：物理ポート番号が表示されます。

[リンク]：ポートのデュプレックス モードおよび速度が表示されます。[全二重] は、デバイスとそのリンク パートナー間の双方向同時送信がインターフェイスによりサポートされていることを示します。[半二重] は、デバイスとそのクライアント間の送信が 1 回につき一方向だけインターフェイスによりサポートされていることを示します。

[モード]：ドロップダウン メニューから、ポートのデュプレックス モードと速度を選択します。[自動ネゴシエーション] も選択できます。これは 2 つのリンク パートナー間のプロトコルで、各ポートが自身の送信速度、デュプレックス モード、およびフロー制御機能をパートナーにアドバタイズできるようにするものです。

[フロー制御]：ポートのフロー制御ステータスが表示されます。ポートが全二重モードの場合に動作します。

[最大フレーム]：ポートが送受信できる最大フレーム サイズが表示されます。

[L2 スイッチ] > [統計情報]

[L2 スイッチ] > [統計情報]

[統計情報の概要]

[Tx バイト数]：選択したポートから送信されたバイト数が表示されます。

[Tx フレーム数]：選択したポートから送信されたフレーム数が表示されます。

[Rx バイト数]：選択したポートで受信したバイト数が表示されます。

[Rx フレーム数]：選択したポートで受信したフレーム数が表示されます。

[Tx エラー数]：選択したポートから送信されたエラー パケット数が表示されます。

[Rx エラー数]：選択したポートで受信したエラー パケット数が表示されます。

[L2 スイッチ] > [ポートミラーリング]

[L2 スイッチ] > [ポートミラーリング]

[ミラー元]：これを使用すると、ルータの各ポートの送信元ポート ミラーリングを有効または無効にすることができます。ポートの送信元ポート ミラーリングを有効にするには、そのポートの隣にあるチェックボックスをオンにします。ポートの送信元ポート ミラーリングを無効にするには、チェックボックスをオフにします。デフォルトは**無効**です。

[ミラーポート]：ドロップダウン メニューからミラー宛先ポートを選択します。

[L2 スイッチ] > [RSTP]

[L2 スイッチ] > [RSTP]

Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）は、ネットワークのループを防ぎ、スイッチのいずれの物理リンクでフレームを転送する必要があるかをダイナミックに再設定するプロトコルです。

[システムのプライオリティ]：システムのプライオリティとして、0 ～ 61440 の範囲で 4096 刻みの値を入力します。有効値は、0、4096、8192、12288、16384、20480、24576、28672、32768、40960、45056、49152、53248、57344、61440 です。システムのプライオリティが低いほど、ルータがスパニング ツリー内でルートになる可能性が高くなります。デフォルトは **32768** です。

[ハロータイム]：1 ～ 10 の値を入力します。デフォルトは **2** です。

[最大経過時間]：6 ～ 40 の値を入力します。デフォルトは **20** です。

[転送遅延]：4 ～ 30 の値を入力します。デフォルトは **15** です。

[Force Version]：使用するデフォルト プロトコル バージョンです。[標準]（RSTP 使用）を選択するか、または [互換]（古い STP との互換性あり）を選択します。デフォルトは [標準] です。

[プロトコルの有効化]：このチェックボックスをオンにすると、関連するポートの RSTP が有効になります。デフォルトはオフになっています（**RSTP** は**無効**）。

[エッジ]：このチェックボックスをオンにすと、関連するポートがエッジ ポート（エンド ステーション）になるように指定されます。オフにすると、関連するポートが別の STP デバイスへのリンク（ブリッジ）になるように指定されます デフォルトはオンになっています（**エッジ ポート**）。

[パスコスト]：指定されたポートの RSTP パス コストです。1 ～ 200000000 の数値を入力するか、または「auto」（自動生成されるパスコスト）と入力します。デフォルトは「auto」です。

[ステータス]

[ステータス] > [ゲートウェイ]

[ステータス] > [ゲートウェイ]

[ファームウェアバージョン]：ゲートウェイの現在のファームウェアが表示されます。

[MAC アドレス]：ISP から見たゲートウェイの MAC アドレスが表示されます。

[現在の時刻]：[設定] メニューで選択しているタイム ゾーンに基づいた時刻が表示されます。

[インターネット接続]

[接続タイプ]：接続の種類が表示されます。

[インターフェイス]：ゲートウェイ インターネット インターフェイスが表示されます。

[IP アドレス]：ゲートウェイ インターネット IP アドレスが表示されます。

[サブネットマスク]：上記の IP アドレスのサブネット マスクが表示されます。

[デフォルトゲートウェイ]：ISP のゲートウェイが表示されます。

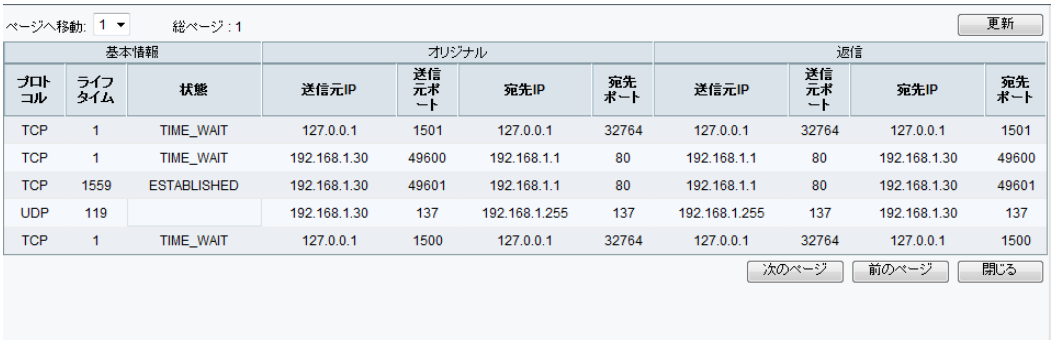
[DNS1] ～ [DNS2]：このゲートウェイが現在使用しているドメイン ネーム システム（DNS）の IP アドレスが表示されます。

[IP Conntrack]：このボタンをクリックすると、[IP Conntrack] ウィンドウが表示されます。

[IP Conntrack]

[IP Conntrack]（IP Connection Tracking）ウィンドウは、発信元 IP アドレス、宛先 IP アドレス、ポート番号のペア、プロトコル タイプ（TCP/UDP/ICMP）、接続状態とタイムアウトなどの、TCP/UDP 接続に関する情報を表示します。詳細情報を表示するには、[次のページ] または [前のページ] をクリックするか、あるいは [ページへ移動] ドロップダウン メニューからページを選択します。最新情報を表示するには、[更新] をクリックします。[閉じる] をクリックすると、[ステータス] > [ゲートウェイ] ウィンドウに戻ります。

[ステータス] > [ゲートウェイ] > [IP Conntrack]



[ステータス] > [ローカルネットワーク]

[ステータス] > [ローカルネットワーク]

[現在の IP アドレスシステム]：現在のシステムが表示されます。

[MAC アドレス]：ローカルのイーサネットから見た、ルータの MAC アドレスです。

[IP アドレス]：インターネット IP アドレスです。

[サブネットマスク]：上記の IP アドレスのサブネット マスクです。

[IPv6 アドレス]：該当する場合、IPv6 IP アドレスです。

[DHCP サーバ]：ルータの DHCP サーバ機能のステータスです。

[開始 IP アドレス]:DHCP サーバによって使用される IP アドレス範囲の開始アドレスです。

[終了 IP アドレス]:DHCP サーバによって使用される IP アドレス範囲の終了アドレスです。

[DHCP アクティブ IP テーブル]：このボタンをクリックすると、ルータを DHCP サーバとして使用する PC を表示するウィンドウが開きます。[DHCP アクティブ IP テーブル] ウィンドウは、クライアント名、インターフェイス、IP アドレス、MAC アドレス、および割り当てられた IP アドレスの有効期限が切れるまでの時間などの情報を示す、すべての DHCP クライアント（PC および他のネットワーク デバイス）を表示します。

[ARP/RARP テーブル]：このボタンをクリックすると、ルータを ARP/RARP サーバとして使用する PC を表示するウィンドウが開きます。[ARP/RARP テーブル] ウィンドウは、IP アドレス、MAC アドレスなどの情報を示す、すべての ARP/RARP（PC および他のネットワーク デバイス）を表示します。

6

VPN セットアップ ウィザードの使用

この章では、VPN セットアップ ウィザードの使用方法について説明します。この章の内容は次のとおりです。

VPN セットアップ ウィザード

VPN セットアップ ウィザードを使用することで、高速かつ効率的な方法で 2 つの VPN ルータ間でゲートウェイ間 VPN トンネルを設定できます。VPN セットアップ ウィザードは、Microsoft Windows 2000、XP および Vista を実行している場合に使用できます。本書では、VPN セットアップ ウィザードの実行方法について説明します。

作業を開始する前に

次に、VPN セットアップ ウィザードを使用できるルータを示します。

- Cisco RVS4000 4 ポート ギガビット VPN セキュリティ ルータ
- Cisco WRVS4400N v1.1 Wireless-N 4 ポート ギガビット VPN セキュリティ ルータ
- Cisco WRVS4400N v2 Wireless-N 4 ポート ギガビット VPN セキュリティ ルータ

次の手順に従い、Web 管理者インターフェイスを使用して必要なデータを設定します。Web 管理者インターフェイスについては、使用しているルータのアドミニストレーション ガイドを参照してください。

ステップ 1 [ファイアウォール] > [基本設定] をクリックします。

ステップ 2 [リモート管理] を [有効] にして、[ポート] フィールドに **8080** と入力します。VPN ウィザードを使用する場合、これ以外の値は入力できないので注意してください。また、HTTPS が選択されていることを確認してください。

ステップ 3 [保存] をクリックします。

ステップ 4 [VPN] > [概要] をクリックして、使用可能なトンネルの数が 0 でないことを確認します。

ステップ 5 VPN 接続が機能するには、VPN のルータの LAN IP アドレスが異なるサブネットにあることを確認してください。

（注） VPN セットアップ ウィザードは、ファイアウォール /NAT デバイスが VPN ルータの外側にないことを前提としています。

VPN セットアップ ウィザードの実行

ステップ 1 次のいずれかの方法で VPN セットアップ ウィザードにアクセスします。

- RVS4000、WRVS4400N v1.1、または WRVS4400N v2 インストール CD-ROM がある場合、これを CD-ROM ドライブに挿入します。
- VPN セットアップ ウィザードをルータの Cisco サポート サイトからダウンロードします。

ステップ 2 [スタート] メニューから [ファイル名を指定して実行] をクリックします。表示されるフィールドに、次のように入力します。

D:¥VPN Setup Wizard.exe

ステップ 3 [Welcome] ウィンドウが表示されます。[Start] ボタンをクリックします。

[Welcome] ウィンドウ

ステップ 4 VPN ウィザードの情報を示すウィンドウが表示されます。準備ができたら、[Next] をクリックして続行します。

情報ウィンドウ

ステップ 5 [Choose a way to build VPN] ウィンドウが表示されます。

- 使用している PC が 2 つのルータのいずれかのローカルである場合、[Build VPN connection from Local LAN port of one router] を選択し、[Next] をクリックして、指示に従います。
- 使用している PC がルータのリモートである場合、[Build VPN connection from Internet remotely] を選択します。このタイプのインストール手順については、**「VPN 接続のリモートでの構築」（P.105）**を参照してください。

VPN 接続のリモートでの構築

ステップ 6 [Build VPN connection from Local LAN port of one router] を選択した場合、必要なデータを [Configure VPN Tunnel] ウィンドウに入力し、[Next] をクリックして続行します。

VPN トンネルの設定

- **[Router 1 User Name]**：Router 1 のユーザ名を入力します。
- **[Router 1 Password]**：Router 1 のパスワードを入力します。
- **[Router 2 User Name]**：Router 2 のユーザ名を入力します。
- **[Router 2 Password]**：Router 2 のパスワードを入力します。
- **[Router 2 WAN IP address]**：Router 2 の WAN IP アドレスを入力します。
- **[Router 2 IP by DNS Resolved]**：インターネット接続のスタティック IP アドレスがない場合、Router 2 の DDNS ドメイン名を入力します。
- **[Tunnel Name]**：このトンネルの名前を入力します。
- **[Pre-shared Key]**：[Pre-shared Key] フィールドは、IKE により、リモート IKE ピアの認証に使用されます。このフィールドには、たとえば、「My_@123」や「0x4d795f40313233」のように、文字と 16 進数の両方を入力できます。両側で同じ事前共有キーを使用する必要があるので注意してください。

ステップ 7 ルータ コンフィギュレーションがチェックされます。

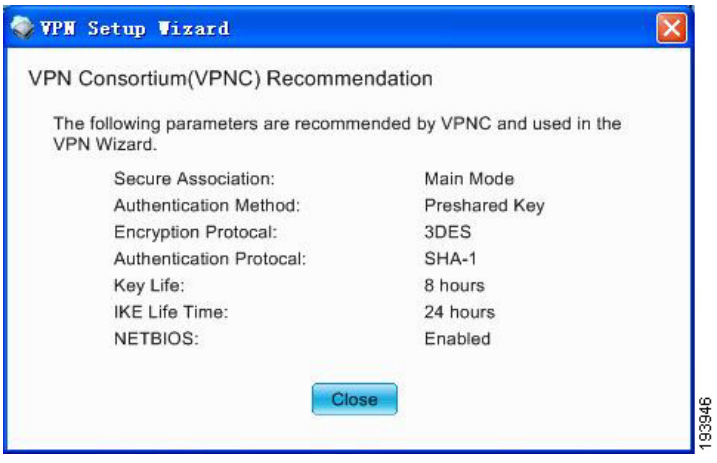
ルータ コンフィギュレーションのチェック

ステップ 8 概要ウィンドウが表示されます。[Click] ボタンを使用して、VPNC の概要ウィンドウを表示します。

概要ウィンドウ

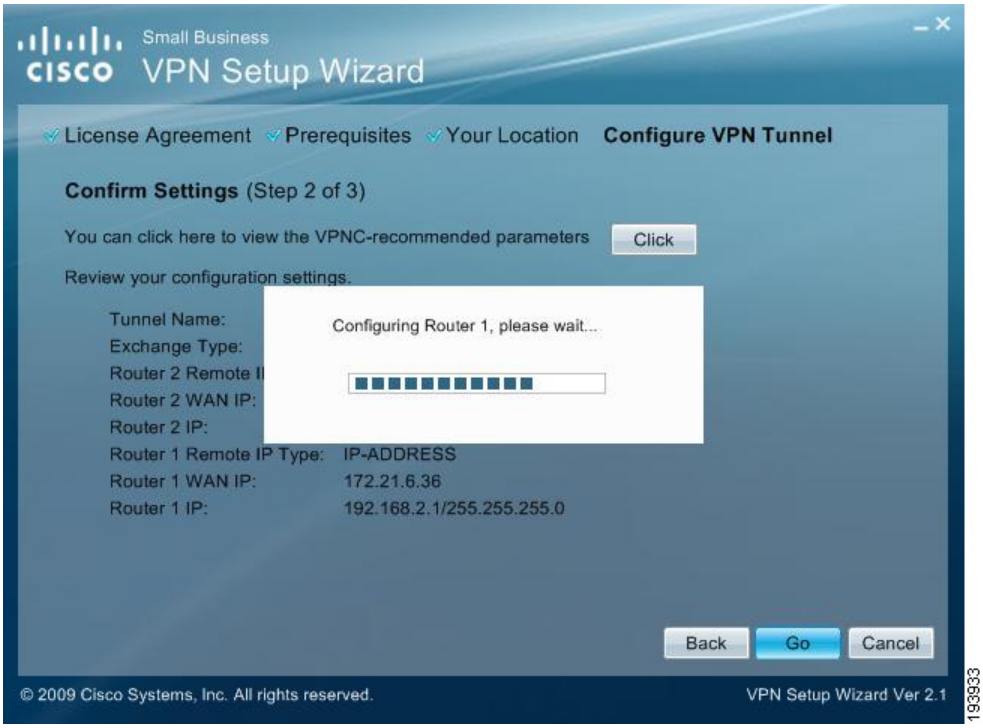
ステップ 9 VPNC の概要ウィンドウが表示され、業界標準の設定が示されます。続行する準備ができたら [Close] をクリックします。

VPNC の概要ウィンドウ



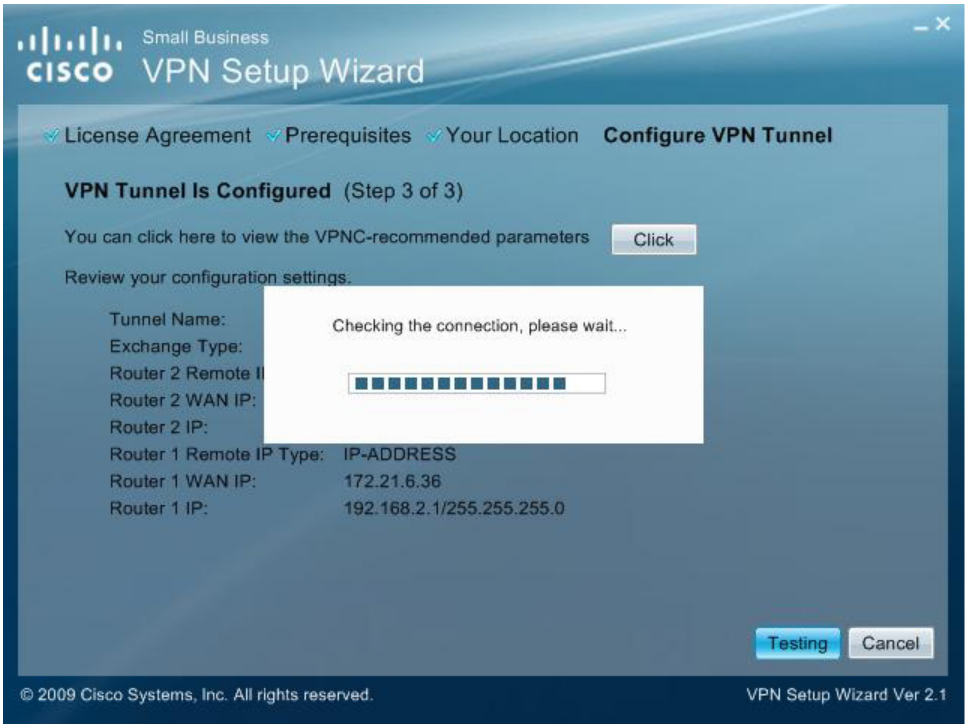
ステップ 10 概要ウィンドウの入力内容が正しい場合、[Go] をクリックします。入力内容を修正する場合、[Back] をクリックして戻ります。

ルータの設定



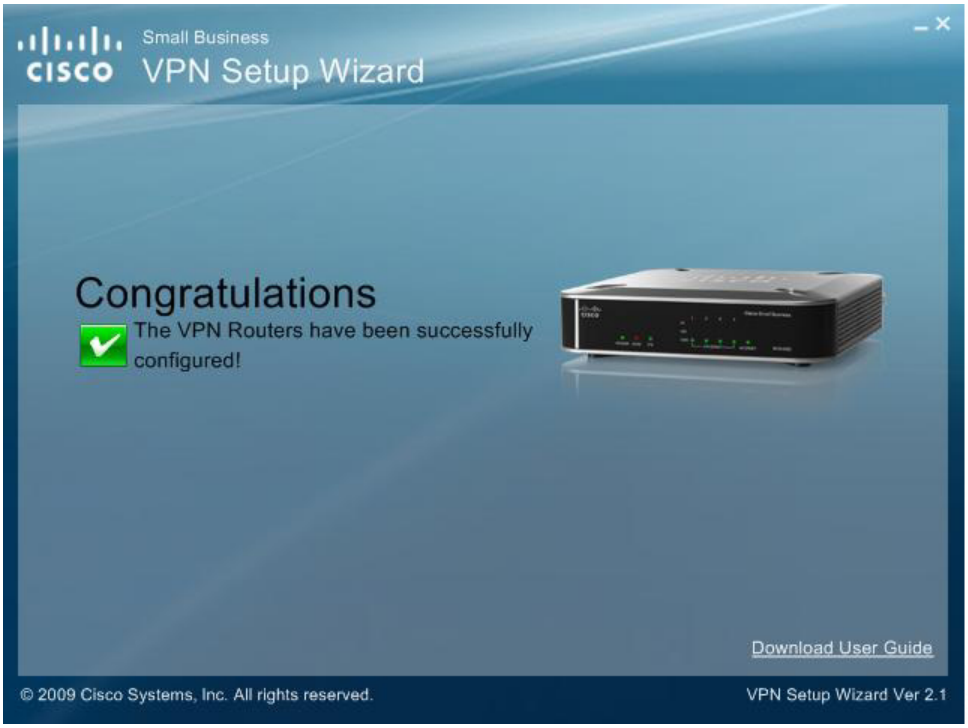
ステップ 11 [Testing] をクリックして、接続が正常に確立されたことを確認します。

接続のテスト



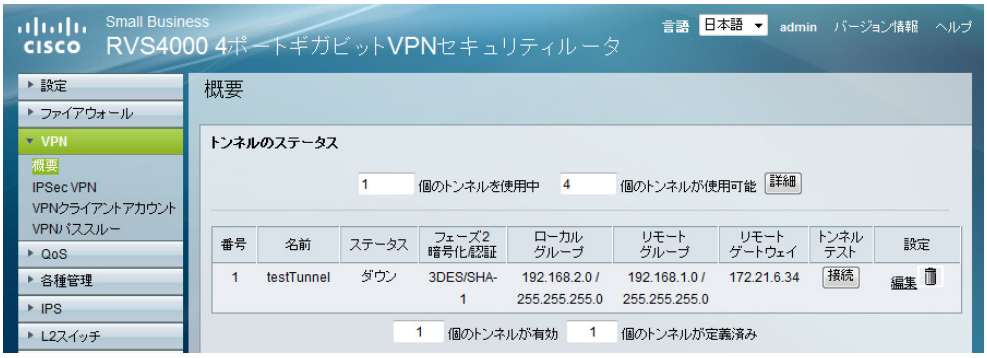
ステップ 12 テストが完了したら、[Exit] をクリックしてウィザードを終了します。

ウィザードの終了



以上で、設定は完了です。Web 管理者インターフェイスにログインして結果を確認できます。

結果のテスト



VPN 接続のリモートでの構築

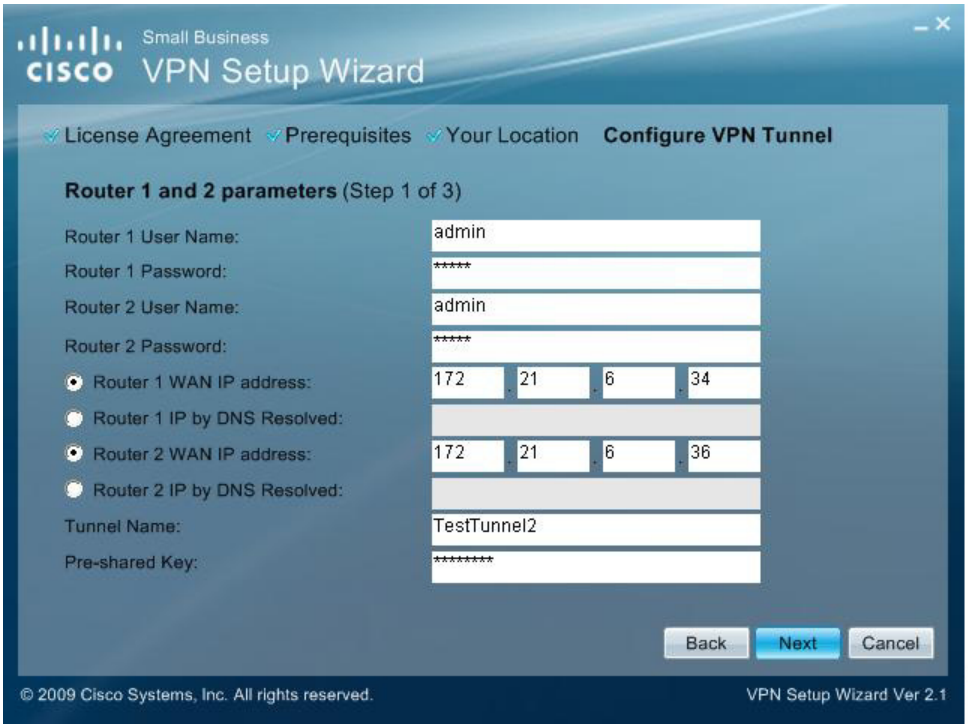
この手順はステップ 5（P.97）の続きです。この手順に従い、リモート PC から VPN 接続を構築します。

ステップ 1 [Build VPN connection from Internet remotely] を選択します。[Next] をクリックして続行します。

VPN 接続のリモートでの構築

ステップ 2 必要なデータを [Configure VPN Tunnel] ウィンドウに入力し、[Next] をクリックして続行します。

[Configure VPN Tunnel] ウィンドウ



- **[Router 1 User Name]**：Router 1 のユーザ名を入力します。
- **[Router 1 Password]**：Router 1 のパスワードを入力します。
- **[Router 2 User Name]**：Router 2 のユーザ名を入力します。
- **[Router 2 Password]**：Router 2 のパスワードを入力します。
- **[Router 1 WAN IP address]**：Router 1 の WAN IP アドレスを入力します。
- **[Router 1 IP by DNS Resolved]**：インターネット接続のスタティック IP アドレスがない場合、Router 1 の DDNS ドメイン名を入力します。
- **[Router 2 WAN IP address]**：Router 2 の WAN IP アドレスを入力します。
- **[Router 2 IP by DNS Resolved]**：インターネット接続のスタティック IP アドレスがない場合、Router 2 の DDNS ドメイン名を入力します。
- **[Tunnel Name]**：このトンネルの名前を入力します。
- **[Pre-shared Key]**：[Pre-shared Key] フィールドは、IKE により、リモート IKE ピアの認証に使用されます。このフィールドには、たとえば、「My_@123」や「0x4d795f40313233」のように、文字と 16 進数の両方を入力できます。両側で同じ事前共有キーを使用する必要があるので注意してください。

ステップ 3 ルータ コンフィギュレーションがチェックされます。

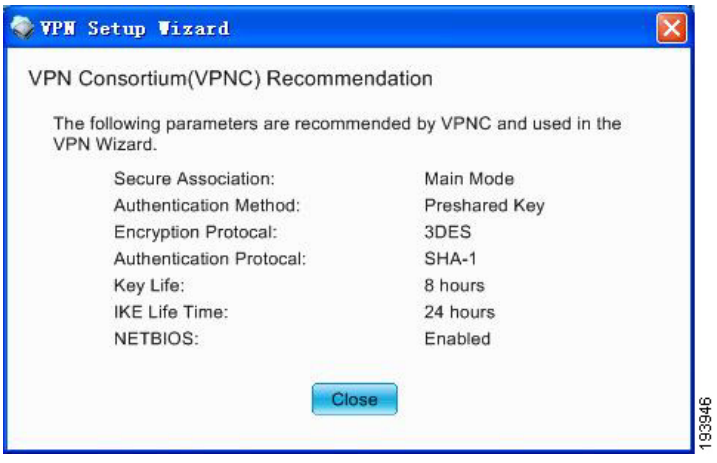
ルータ コンフィギュレーションのチェック

ステップ 4 概要ウィンドウが表示されます。[Click] ボタンを使用して、VPNC の概要ウィンドウを表示します。

概要ウィンドウ

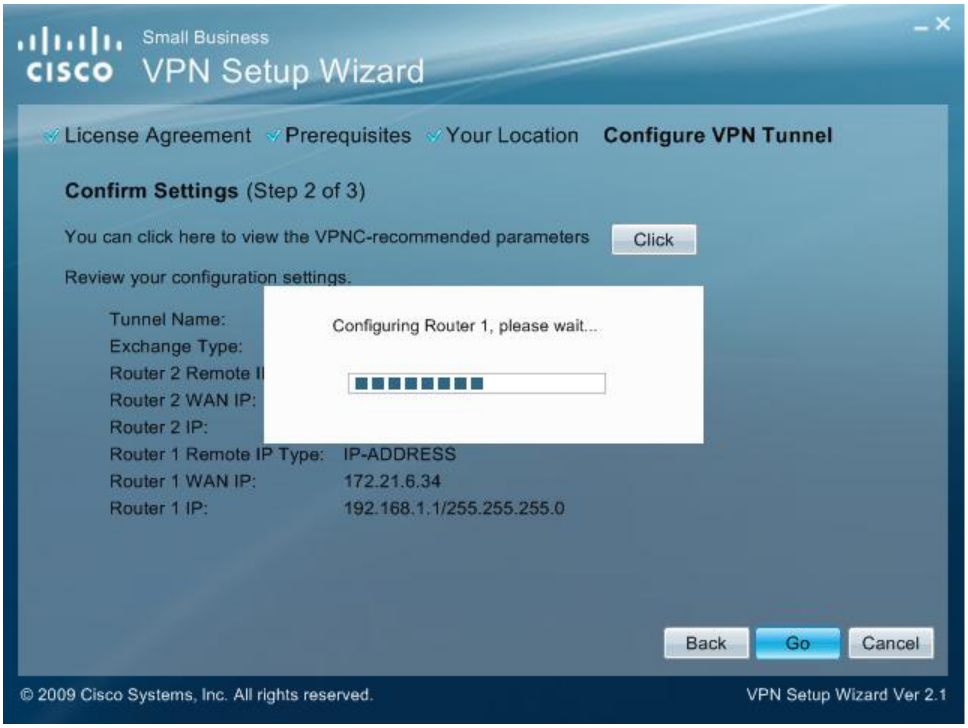
ステップ 5 VPNC の概要ウィンドウが表示され、業界標準の設定が示されます。続行する準備ができたら [Close] をクリックします。

VPNC の概要ウィンドウ



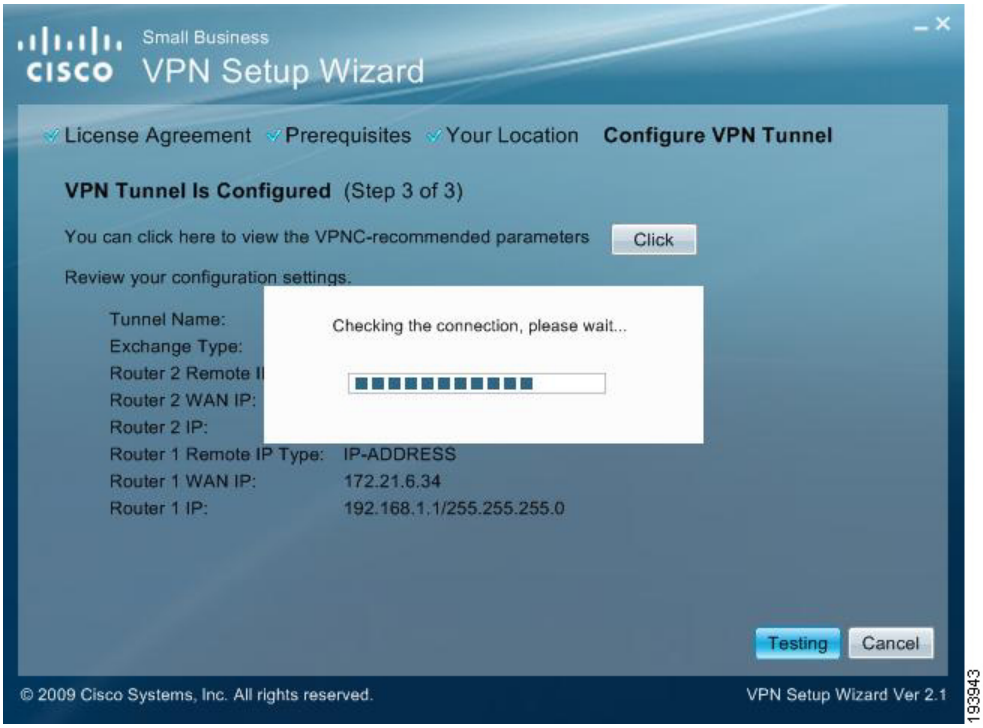
ステップ 6 概要ウィンドウの入力内容が正しい場合、[Go] をクリックします。入力内容を修正する場合、[Back] をクリックして戻ります。

ルータの設定

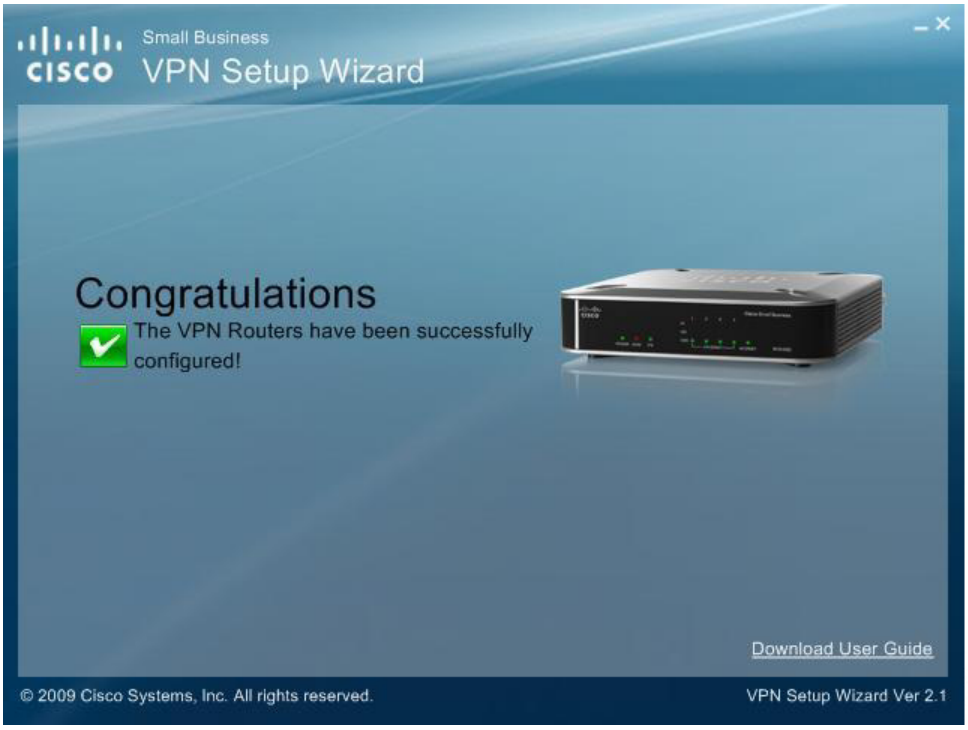


ステップ 7 [Testing] をクリックして、接続が正常に確立されたことを確認します。

接続のテスト

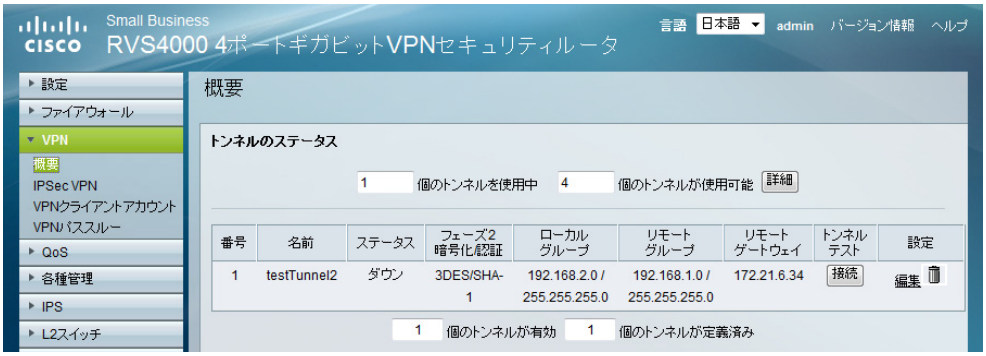


ステップ 8 テストが完了したら、[Exit] をクリックしてウィザードを終了します。



以上で、設定は完了です。Web 管理者インターフェイスにログインして結果を確認できます。

テスト結果の表示



A

トラブルシューティング

この付録では、本ルータの設置および操作中に発生する可能性がある問題の解決方法について説明します。次の説明は問題の解決に役立ちます。ここで解決方法が見つからない場合は、シスコの Web サイト（www.cisco.com）を参照してください。

PC でスタティック IP アドレスを設定する必要があります。

このルータはデフォルトで、ルータの DHCP サーバを使用して IP アドレス範囲 192.168.1.100 ～ 192.168.1.149 を割り当てます。スタティック IP アドレスを設定する場合は、範囲 192.168.1.2 ～ 192.168.1.99、および 192.168.1.150 ～ 192.168.1.254 だけを使用できます。TCP/IP を使用する各 PC またはネットワーク デバイスには、ネットワークでの識別のために一意なアドレスが必要です。IP アドレスがネットワークに対して一意でない場合、Windows では、IP 競合エラー メッセージが生成されます。スタティック IP アドレスを PC に割り当てるには、次の手順に従います。

Windows 2000

ステップ 1 [スタート] > [設定] > [コントロール パネル] の順にクリックします。[ネットワークとダイヤルアップ接続] をダブルクリックします。

ステップ 2 使用しているイーサネット アダプタに関連付けられている [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。

ステップ 3 [チェック マークがオンになっているコンポーネントがこの接続で使用されています] ボックスで、[インターネット プロトコル (TCP/IP)] を選択して、[プロパティ] をクリックします。[IP アドレスを指定する] を選択します。

ステップ 4 ルータに接続されているネットワーク上の他のコンピュータで使用されていない一意な IP アドレスを入力します。使用できる IP アドレスの範囲は 192.168.1.2 ～ 192.168.1.99 および 192.168.1.151 ～ 192.168.1.254 です。

ステップ 5 [サブネット マスク] に **255.255.255.0** と入力します。

ステップ 6 [デフォルト ゲートウェイ] に **192.168.1.1**（ルータのデフォルト IP アドレス）と入力します。

ステップ 7 [次の DNS サーバーのアドレスを使用する] を選択して、優先 DNS サーバと代替 DNS サーバ（ISP により提供）を入力します。これについては、ISP に問い合せるか、該当する Web サイトを参照してください。

ステップ 8 [インターネット プロトコル (TCP/IP) のプロパティ] ウィンドウで [OK] をクリックして、[ローカル エリア接続のプロパティ] ウィンドウで [OK] をクリックします。

ステップ 9 要求された場合は、コンピュータを再起動します。

Windows XP

ステップ 1 [スタート] > [コントロール パネル] の順にクリックします。

ステップ 2 [ネットワークとインターネット接続] アイコンをクリックして、[ネットワーク接続] アイコンをクリックします。

ステップ 3 イーサネット アダプタに関連付けられている [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。

ステップ 4 [この接続は次の項目を使用します] ボックスで、[インターネット プロトコル (TCP/IP)] を選択します。[プロパティ] をクリックします。

ステップ 5 [次の IP アドレスを使う] を選択して、ルータに接続されているネットワーク上の他のコンピュータで使用されていない一意な IP アドレスを入力します。使用できる IP アドレスの範囲は 192.168.1.2 ～ 192.168.1.99 および 192.168.1.151 ～ 192.168.1.254 です。

ステップ 6 [サブネット マスク] に **255.255.255.0** と入力します。

ステップ 7 [デフォルト ゲートウェイ] に **192.168.1.1**（ルータのデフォルト IP アドレス）と入力します。

ステップ 8 [次の DNS サーバーのアドレスを使用する] を選択して、優先 DNS サーバと代替 DNS サーバ（ISP により提供）を入力します。これについては、ISP に問い合せるか、該当する Web サイトを参照してください。

ステップ 9 [インターネット プロトコル (TCP/IP) のプロパティ] ウィンドウで [OK] をクリックします。[ローカル エリア接続のプロパティ] ウィンドウで [OK] をクリックします。

インターネット接続をテストする必要があります。

ステップ 1 TCP/IP 設定をチェックします。

Windows 2000

a. [スタート] > [設定] > [コントロール パネル] の順にクリックします。[ネットワークとダイヤルアップ接続] をダブルクリックします。

b. 使用しているイーサネット アダプタに関連付けられている [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。

c. [チェック マークがオンになっているコンポーネントがこの接続で使用されています] ボックスで、[インターネット プロトコル (TCP/IP)] を選択して、[プロパティ] をクリックします。[IP アドレスを自動的に取得する] および [DNS サーバーのアドレスを自動的に取得する] が選択されていることを確認します。

d. [インターネット プロトコル (TCP/IP) のプロパティ] ウィンドウで [OK] をクリックして、[ローカル エリア接続のプロパティ] ウィンドウで [OK] をクリックします。

e. 要求された場合は、コンピュータを再起動します。

Windows XP

これは、Windows XP のデフォルト インターフェイスに関する説明です。クラシック インターフェイスを使用している（アイコンおよびメニューが以前の Windows バージョンのように表示されている）場合、Windows 2000 に関する指示に従ってください。

a. [スタート] > [コントロール パネル] の順にクリックします。

b. [ネットワークとインターネット接続] アイコンをクリックして、[ネットワーク接続] アイコンをクリックします。

c. イーサネット アダプタに関連付けられている [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。

d. [この接続は次の項目を使用します] ボックスで、[インターネット プロトコル (TCP/IP)] を選択して、[プロパティ] をクリックします。[IP アドレスを自動的に取得する] および [DNS サーバーのアドレスを自動的に取得する] が選択されていることを確認します。

ステップ 2 コマンド プロンプトを開きます。

a. Windows 98 および Millennium：[スタート] > [ファイル名を指定して実行] の順にクリックします。[開く] フィールドで、**command** と入力します。Enter キーを押して、[OK] をクリックします。

b. Windows 2000 および XP：[スタート] > [ファイル名を指定して実行] の順にクリックします。[開く] フィールドで、**cmd** と入力します。Enter キーを押して、[OK] をクリックします。

ステップ 3 コマンド プロンプトで、**ping 192.168.1.1** と入力して、Enter キーを押します。

- 応答があった場合、コンピュータはルータと通信しています。
- 応答がない場合、ケーブルをチェックし、イーサネット アダプタの TCP/IP 設定で [IP アドレスを自動的に取得する] が選択されていることを確認します。

ステップ 4 コマンド プロンプトで、**ping** に続けてインターネット IP アドレスを入力して、Enter キーを押します。インターネット IP アドレスは、ルータの設定ユーティリティで確認できます。たとえば、インターネット IP アドレスが 1.2.3.4 の場合、**ping 1.2.3.4** と入力して、Enter キーを押します。

- 応答があった場合、コンピュータはルータに接続されています。
- 応答がない場合、別のコンピュータから ping コマンドを入力してみて、元のコンピュータが問題の原因でないことを確認します。

ステップ 5 コマンド プロンプトで、**ping www.cisco.com** と入力して、Enter キーを押します。

- 応答があった場合、コンピュータはインターネットに接続されています。Web ページを開くことができない場合、別のコンピュータから ping コマンドを入力してみて、元のコンピュータが問題の原因でないことを確認します。
- 応答がない場合、接続に問題が発生している可能性があります。別のコンピュータから ping コマンドを入力してみて、元のコンピュータが問題の原因でないことを確認します。

インターネット接続でインターネットの IP アドレスを取得できません。

ステップ 1 上記の**「インターネット接続をテストする必要があります。」（P.114）**を参照して接続を確認します。

ステップ 2 イーサネット アダプタの MAC アドレスのクローンをルータに作成する必要がある場合、**第 5 章「ルータのセットアップおよび設定」**の「MAC Address Clone」のセクションで詳細を参照してください。

ステップ 3 使用しているインターネット設定が正しいことを確認します。ISP に問い合せて、インターネット接続タイプが DHCP、スタティック IP アドレスまたは PPPoE（通常 DSL コンシューマにより使用されます）であるか確認します。インターネット接続タイプの設定の詳細については、**第 5 章「ルータのセットアップおよび設定」**の基本設定のセクションを参照してください。

ステップ 4 正しいケーブルを使用していることを確認します。[INTERNET] LED が点灯しているか確認します。

ステップ 5 ケーブルまたは DSL モデムの接続ケーブルが、ルータのインターネット ポートに接続されていることを確認します。ルータの設定ユーティリティの [ステータス] ページに ISP の有効な IP アドレスが表示されていることを確認します。

ステップ 6 コンピュータ、ルータおよびケーブル /DSL モデムの電源を切ります。30 秒後、ルータ、ケーブル /DSL モデムおよびコンピュータの電源を入れます。ルータの設定ユーティリティの [設定] > [概要] で、IP アドレスを取得していることを確認します。

ルータの設定ユーティリティの [設定] ウィンドウにアクセスできません。

ステップ 1 **「インターネット接続をテストする必要があります。」（P.114）**を参照して、コンピュータがルータに正しく接続されていることを確認します。

ステップ 2 コンピュータに IP アドレス、サブネット マスク、ゲートウェイおよび DNS があることを確認します。

ステップ 3 システムでスタティック IP アドレスを設定します（上記の**「PC でスタティック IP アドレスを設定する必要があります。」（P.112）**を参照してください）。

ステップ 4 **「PPPoE を使用しているのですが、プロキシ設定またはダイヤルアップ ポップアップ ウィンドウを削除する必要があります。」（P.120）**を参照します。

ルータ経由で VPN（バーチャル プライベート ネットワーク）が機能しません。

http://192.168.1.1 またはルータの IP アドレスに移動してルータの Web インターフェイスにアクセスし、[VPN] > [VPN パススルー] に移動します。IPSec パススルーまたは PPTP パススルー、あるいはこの両方が有効になっていることを確認します。

IPSec および Encapsulation Security Payload（ESP; 暗号ペイロード）（プロトコル 50）認証を使用する VPN は正常に機能します。少なくとも 1 つの IPSec セッションはルータで機能します。ただし、VPN によっては、同時 IPSec セッションが可能な場合もあります。

IPSec および Authentication Header（AH; 認証ヘッダー）（プロトコル 51）を使用する VPN は、ルータと互換性がありません。AH には、NAT 標準に準拠していない場合があるため制限があります。

ルータの IP アドレスを別のサブネットに変更して、VPN IP アドレスとローカル IP アドレスとの競合を避けます。たとえば、VPN サーバが IP アドレス 192.168.1.X（X は 1 ～ 254 の数）を割り当て、ローカル LAN IP アドレスが 192.168.1.X（X は VPN IP アドレスで使用される数と同じ）の場合、ルータによる正しい位置への情報のルーティングが困難になります。ルータの IP アドレスを 192.168.2.1 に変更すると、問題が解決します。設定ユーティリティの [設定] メニューからルータの IP アドレスを変更します。スタティック IP アドレスをネットワークの任意のコンピュータまたはネットワーク デバイスに割り当てた場合、その IP アドレスを 192.168.2.Y（Y は 1 ～ 254 の数です）に変更する必要があります。各 IP アドレスはネットワーク内で一意でなければならないので注意してください。

VPN によっては、ポート 500/UDP パケットを、IPSec サーバに接続するコンピュータに渡す必要があります。

詳細については、シスコの Web サイト（www.cisco.com）で確認してください。

サーバをルータの内側に設定する必要があります。

Web サーバ、FTP サーバ、またはメール サーバなどのサーバを使用するには、使用する各ポート番号を認識する必要があります。たとえば、ポート 80（HTTP）は Web に使用されます。ポート 21（FTP）は FTP に使用され、ポート 25（SMTP 発信）およびポート 110（POP3 着信）はメール サーバに使用されます。詳細については、インストールしているサーバの付属マニュアルを参照してください。ルータの設定ユーティリティからポート フォワーディングを設定するには、次の手順に従います。Web サーバ、FTP サーバ、メール サーバを設定する必要があります。

ステップ 1 **http://192.168.1.1** またはルータの IP アドレスに移動してルータの設定ユーティリティにアクセスします。[ファイアウォール] > [単一ポートのフォワーディング] に移動します。

ステップ 2 [アプリケーション] 列からサービスを選択します。

ステップ 3 インターネット ユーザにアクセスさせるサーバの IP アドレスを入力します。たとえば、Web サーバのイーサネット アダプタ IP アドレスが 192.168.1.100 の場合、提供されるフィールドに 100 を入力します。次に、エントリの [有効] チェックボックスをオンにします。次に例を示します。

アプリケーション	開始および終了	プロトコル	IP アドレス	有効
HTTP	80 ～ 80	両方	192.168.1.100	X
FTP	21 ～ 21	TCP	192.168.1.101	X
SMTP（発信）	25 ～ 25	両方	192.168.1.102	X
POP3（着信）	110 ～ 110	両方	192.168.1.102	X

ステップ 4 エントリを必要なだけ設定します。

ステップ 5 コンフィギュレーションが完了したら、[保存] をクリックします。

オンライン ゲーム ホスティングを設定するか、または他のインターネット アプリケーションを使用する必要があります。

オンライン ゲームをプレイしたり、インターネット アプリケーションを使用したい場合、ポート フォワーディングまたは DMZ ホスティングを行うことなくたいていの場合はうまく動作します。ただし、オンライン ゲームまたはインターネット アプリケーションをホスティングする要件がある場合もあります。この場合、着信パケットまたはデータを特定のコンピュータに配信するようにルータを設定する必要があります。これは、使用するインターネット アプリケーションにも適用されます。使用するポート サービスに関する情報については、使用するオンライン ゲームまたはアプリケーションの Web サイトにアクセスしてください。オンライン ゲーム ホスティングを設定したり、特定のインターネット アプリケーションを使用したりするには、次の手順に従います。

ステップ 1 **http://192.168.1.1** またはルータの IP アドレスに移動してルータの設定ユーティリティにアクセスします。[ファイアウォール] > [単一ポートのフォワーディング] に移動します。

ステップ 2 [アプリケーション] 列からサービスを選択します。

ステップ 3 インターネット ユーザにアクセスさせるサーバの IP アドレスを入力します。たとえば、Web サーバのイーサネット アダプタ IP アドレスが 192.168.1.100 の場合、提供されるフィールドに 100 を入力します。次に、エントリの [有効] チェックボックスをオンにします。次に例を示します。

アプリケーション	開始および終了	プロトコル	IP アドレス	有効
UT	7777 ～ 27900	両方	192.168.1.100	X
Halflife	27015 ～ 27015	両方	192.168.1.105	X
PC Anywhere	5631 ～ 5631	UDP	192.168.1.102	X
VPN IPSEC	500 ～ 500	UDP	192.168.1.100	X

ステップ 4 エントリを必要なだけ設定します。

ステップ 5 コンフィギュレーションが完了したら、[保存] をクリックします。

インターネット ゲーム、サーバ、またはアプリケーションを開始できません。

インターネット ゲーム、サーバ、またはアプリケーションを正しく機能できない場合、DeMilitarized Zone（DMZ; 非武装地帯）ホスティングを使用して、1 台の PC をインターネットに接続します。このオプションを使用できるのは、アプリケーションで必要なポートが多数ある場合、または使用するポート サービスがわからない場合です。フォワーディングは DMZ ホスティングより優先されるため、DMZ ホスティングを正常に使用するには、すべてのフォワーディング エントリを無効にする必要があります （つまり、ルータに送られるデータは、フォワーディング設定により最初にチェックされます。データが送られるポート番号でポート フォワーディングが設定されていない場合、ルータは、DMZ ホスティングに設定する PC またはネットワーク デバイスにデータを送信します）。DMZ ホスティングを設定するには、次の手順に従います。

ステップ 1 **http://192.168.1.1** またはルータの IP アドレスに移動してルータの設定ユーティリティにアクセスします。[ファイアウォール] > [単一ポートのフォワーディング] に移動します。

ステップ 2 フォワーディングに入力したエントリを無効にします。

ステップ 3 [設定] > [DMZ] に移動します。

ステップ 4 インターネットに公開するコンピュータのイーサネット アダプタの IP アドレスを入力します。これにより、そのコンピュータの NAT セキュリティをバイパスします。

ステップ 5 [有効] を選択して DMZ ホスティングを有効にします。

ステップ 6 コンフィギュレーションが完了したら、[保存] をクリックします。

パスワードを忘れてしまいました。または設定をルータに保存するときにパスワード プロンプトが常に表示されます。

[RESET] ボタンを 10 秒間押し続けてから放すことで、ルータを工場出荷時設定にリセットします。設定保存時にパスワード プロンプトがまだ表示される場合、次の手順を実行してください。

ステップ 1 http://192.168.1.1 またはルータの IP アドレスに移動してルータの Web インターフェイスにアクセスします。デフォルト パスワード **admin** を入力して、[各種管理] > [管理] をクリックします。

ステップ 2 新しいパスワードを [ルータのパスワード] フィールドに入力します。

ステップ 3 もう一度新しいパスワードを [パスワードの再入力] フィールドに入力します。

ステップ 4 [保存] をクリックします。

PPPoE を使用しているのですが、プロキシ設定またはダイヤルアップ ポップアップ ウィンドウを削除する必要があります。

プロキシ設定がある場合、コンピュータで無効にする必要があります。ルータはインターネット接続のゲートウェイであるため、コンピュータはアクセスを取得するためのプロキシ設定は必要としません。次の手順に従い、プロキシ設定がないこと、および使用するブラウザが LAN に直接接続するように設定されていることを確認してください。

Microsoft Internet Explorer 5.0 以降の場合：

ステップ 1 [スタート] > [設定] > [コントロール パネル] の順にクリックします。[インターネット オプション] をダブルクリックします。

ステップ 2 [接続] タブをクリックします。

ステップ 3 [LAN の設定] をクリックして、チェックマークをすべてオフにします。

ステップ 4 [OK] をクリックして、直前のウィンドウに戻ります。

ステップ 5 [ダイヤルしない] オプションをオンにします。これにより、PPPoE ユーザのダイヤルアップ ポップアップが削除されます。

Netscape 4.7 以降の場合：

ステップ 1 Netscape Navigator を起動して、[編集] > [設定] > [詳細] > [プロキシ] の順にクリックします。

ステップ 2 このウィンドウで [インターネットに直接接続する] が選択されていることを確認します。

ステップ 3 すべてのウィンドウを閉じて終了します。

元の設定に戻すため、ルータを工場出荷時設定に復元する必要があります。

[RESET] ボタンを 30 秒間まで押し、放します。これにより、ルータのパスワード、フォワーディングおよびその他の設定が工場出荷時設定に戻ります。つまり、ルータが元々設定されたコンフィギュレーションに戻ります。

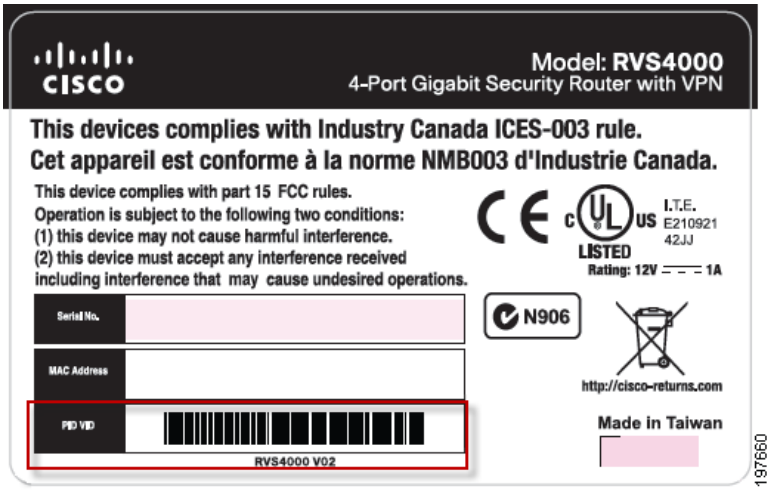
ファームウェアをアップグレードする必要があります。

「[各種管理] > [ファームウェアのアップグレード]」（P.78）の手順を実行します。

ファームウェアのアップグレードが失敗しました。

アップグレードが失敗する理由はたくさんあります。「[各種管理] > [ファームウェアのアップグレード]」（P.78）の手順を実行して、ファームウェア アップグレードを再試行します。また、ハードウェア バージョン 1 の場合、次に示す「修復」手順を実行することもできます。

（注） ハードウェア バージョンを確認するには、ルータの底面パネルにあるラベルに示されている PIDVID コードを参照してください。



ステップ 1 ルータがハードウェア バージョン 1 の場合、www.cisco.com/go/software に移動します。

ステップ 2 検索ボックスに、**RVS4000** と入力します。

ステップ 3 検索結果から、Download Software for Cisco RVS4000 4-port Gigabit Security Router - VPN を選択します。

プロンプトが表示されたら、Cisco.com ユーザ名およびパスワードを入力します。Cisco.com アカウントがない場合、新規ユーザとして登録できます。

ステップ 4 [Router Firmware Rescue Utility] リンクをクリックします。

ステップ 5 zip ファイルをコンピュータに保存します。

ステップ 6 zip ファイルからファイル **setup.exe** を抽出し、**setup.exe** を実行してユーティリティをコンピュータにインストールします。

ステップ 7 ファームウェア アップグレード ユーティリティがあるコンピュータのネットワーク ケーブル**以外、すべて**のルータの LAN および WAN ポートからネットワーク ケーブルを外します。

ステップ 8 デスクトップの [RVS4000 Upgrade Utility] アイコンをクリックしてユーティリティを実行します。または、[スタート] > [すべてのプログラム] > [Cisco Small Business] > [RVS4000 Upgrade Utility] をクリックすることでもユーティリティを実行できます。

ステップ 9 画面上の指示に従いアップグレードを実行します。

DSL サービスの PPPoE が常に切断されます。

PPPoE は実際には専用接続または常時接続ではありません。DSL ISP は、インターネットとの通常の電話ダイヤルアップ接続と同様に、非アクティブな状態が一定期間続いた後、サービスを切断できます。接続を「キープアライブ（常時接続）」にする設定オプションがあります。これは使用できない場合もあるため、接続を定期的に再接続する必要があります。

ステップ 1 ルータに接続するには、Web ブラウザに移動して、**http://192.168.1.1** またはルータの IP アドレスを入力します。

ステップ 2 要求された場合、パスワードを入力します（デフォルトのパスワードは **admin**）です。

ステップ 3 [設定] > [WAN] メニューで、[キープアライブ] オプションを選択して、[リダイアル間隔] オプションを **20**（秒）に設定します。

ステップ 4 [保存] をクリックします。

再び接続が切断された場合、手順 1 および 2 を実行して接続を再確立します。

E メール、Web、VPN にアクセスできません。またはインターネットからの取得データが壊れています。

場合によっては、Maximum Transmission Unit（MTU; 最大伝送ユニット）設定を調整する必要があります。デフォルトでは、MTU は 1500 に設定されています。ほとんどの DSL ユーザの場合、MTU 1492 を使用することを強くお勧めします。問題がある場合、次の手順を実行してください。

ステップ 1 ルータに接続するには、Web ブラウザに移動して、**http://192.168.1.1** またはルータの IP アドレスを入力します。

ステップ 2 要求された場合、パスワードを入力します（デフォルトのパスワードは **admin**）です。

ステップ 3 [設定] > [WAN] メニューに移動します。

ステップ 4 [MTU] オプションで、[手動] を選択します。[サイズ] フィールドに、**1492** と入力します。

ステップ 5 [保存] をクリックして続行します。

問題が解決されない場合、[サイズ] を別の値に変更します。問題が解決されるまで、次に示す値を 1 つずつ、示されている順番で試してみてください。

1462
1400
1362
1300

ポート トリガーを使用する必要があります。

ポート トリガーは、使用される発信ポート サービスを参照し、インターネット アプリケーションを使用するポートに応じて、ルータをトリガーして特定のポートを開きます。次の手順を実行します。

ステップ 1 ルータに接続するには、Web ブラウザに移動して、**http://192.168.1.1** またはルータの IP アドレスを入力します。

ステップ 2 要求された場合、パスワードを入力します（デフォルトのパスワードは **admin**）です。

ステップ 3 [ファイアウォール] > [ポート範囲のトリガー] をクリックします。

ステップ 4 [アプリケーション名] に使用する名前を入力します。

ステップ 5 [トリガー範囲] の開始ポートと終了ポートを入力します。使用する発信ポート サービスの詳細については、インターネット アプリケーション プロバイダーにお問い合せください。

ステップ 6 [フォワード範囲] の開始ポートと終了ポートを入力します。インターネット アプリケーションで必要な着信ポート サービスの詳細については、インターネット アプリケーション プロバイダーにお問い合せください。

ステップ 7 エントリの [有効] チェックボックスをオンにします。

ステップ 8 コンフィギュレーションが完了したら、[保存] をクリックします。

URL または IP アドレスを入力するとき、タイムアウト エラーが発生するか、再試行するように要求されます。

- 他の PC が機能するかチェックします。機能する場合、ワークステーションの IP 設定（IP アドレス、サブネット マスク、デフォルト ゲートウェイおよび DNS）が正しいことを確認します。問題があるコンピュータを再起動します。

- PC が正しく設定されているが、機能しない場合、ルータをチェックします。ルータが接続され、電源が入っていることを確認します。接続し、設定をチェックします（接続できない場合、LAN および電源接続をチェックします）。
- ルータが正しく設定されている場合、インターネット接続（DSL/ ケーブル モデムなど）をチェックして正しく機能しているか確認します。ルータを取り外して直接接続できるか確認できます。
- ISP から提供された DNS アドレスで TCP/IP を手動で設定します。
- ブラウザが正しく接続できるように設定されていること、およびダイヤルアップが無効になっていることを確認します。Internet Explorer の場合、[ツール] > [インターネット オプション] > [接続] タブの順にクリックします。Internet Explorer が [ダイヤルしない] に設定されていることを確認します。Netscape Navigator の場合、[編集] > [設定] > [詳細] > [プロキシ] の順にクリックします。Netscape Navigator が [インターネットに直接接続する] に設定されていることを確認します。

ルータの設定ユーティリティにアクセスしようとしても、ログイン ウィンドウが表示されず、「404 Forbidden」を示すウィンドウが表示されます。

Internet Explorer を使用する場合、設定ユーティリティのログイン ウィンドウが表示されるまで、次の手順を実行します（Netscape Navigator でも同様の手順が必要です）。

ステップ 1 [ファイル] をクリックします。[オフライン作業] のチェックマークがオフになっていることを確認します。

ステップ 2 **Ctrl キーを押した状態で F5 キー**を押します。これはハード リフレッシュであるため、Internet Explorer はキャッシュ ページではなく、新しい Web ページをロードします。

ステップ 3 [ツール] をクリックします。[インターネット オプション] をクリックします。[セキュリティ] タブをクリックします。[既定のレベル] ボタンをクリックします。セキュリティ レベルが [中] または [低] であることを確認します。[OK] ボタンをクリックします。

QuickVPN トンネルを RVS4000 に接続していますが、Internet Explorer からリモート ネットワークのコンピュータを表示できません。

QuickVPN トンネリングは、NetBIOS ブロードキャストをサポートしていません。リモート ネットワークのコンピュータまたは共有ドライブにアクセスするには、IP アドレスを使用してリソースを識別することをお勧めします。

2 つの RVS4000 ルータ間でゲートウェイ間 IPSec VPN トンネルの接続を確立しています。あるネットワーク内のユーザが、Internet Explorer からリモートネットワークのコンピュータを表示できません。

RVS4000 は、ゲートウェイ間 IPSec VPN トンネルで NetBIOS ブロードキャストをサポートしています。ただし、管理者は、[VPN] > [IPSec VPN] ウィンドウの [詳細設定] セクションでこの機能を有効にする必要があります。

FAQ

Q. ルータでサポートされる IP アドレスの最大数はどれくらいですか。

ルータは最大 253 の IP アドレスをサポートします。

Q. IPSec パススルーはルータでサポートされていますか。

はい。[VPN] > [VPN パススルー] ウィンドウで IPSec パススルーを有効または無効にすることができます。

Q. ルータはネットワークのどこに設置しますか。

一般的な環境では、ルータはケーブル /DSL モデムと LAN の間に設置します。ルータをケーブル /DSL モデムのイーサネット ポートに接続してください。

Q. ルータは IPX または AppleTalk をサポートしていますか。

いいえ。TCP/IP は、インターネットの唯一のプロトコル標準で、通信のグローバル標準になっています。ノード間でのメッセージのルーティングだけに使用される NetWare 通信プロトコルである、IPX、および Apple と Macintosh ネットワークで使用される通信プロトコルである、AppleTalk は、LAN 間接続に使用できますが、これらのプロトコルはインターネットから LAN には接続できません。

Q. NAT とは何ですか。また、何のために使用されますか。

Network Address Translation（NAT; ネットワーク アドレス変換）は、プライベート LAN の複数の IP アドレスを、インターネットに送信されるパブリック アドレスに変換します。これにより、プライベート LAN に接続される PC のアドレスはインターネットには転送されないため、セキュリティが強化されます。さらに、NAT により、ISP により提供される TCP/IP アドレスが 1 つだけの場合、DSL またはケーブル モデムなどの、低コストのインターネット アカウントでルータを使用できます。ユーザは、ISP により提供されるこの 1 つのアドレスの他に多くのプライベート アドレスを使用できます。

Q. ルータは、Windows 98、Millennium、2000 または XP 以外のオペレーティング システムをサポートしていますか。

はい。ただし、シスコは、現時点では、Windows 以外のオペレーティング システムのセットアップ、コンフィギュレーションまたはトラブルシューティングに関するテクニカル サポートは行っていません。

Q. ルータは ICQ 送信ファイルをサポートしていますか。

はい。このフィックスを適用し、[ICQ] メニューから [Preferences] > [Connection] タブをクリックして、[I am behind a firewall or proxy] チェックボックスをオンにします。次に、[Firewall Settings] でファイアウォール タイムアウトを 80 秒に設定します。インターネット ユーザは、ルータの内側にいるユーザにファイルを送信できるようになります。

Q. Unreal Tournament サーバを設定しましたが、LAN 上の他のユーザが参加できません。どうすればよいですか。

専用 Unreal Tournament サーバを実行している場合、各 LAN コンピュータのスタティック IP アドレスを作成して、ポート 7777、7778、7779、7780、7781 および 27900 をサーバの IP アドレスに転送する必要があります。また、ポート フォワーディング範囲 7777 ～ 27900 を使用することもできます。UT Server Admin を使用する場合、別のポートを転送します（通常 8080 で問題ありませんが、リモート admin に使用されるため、場合によっては、無効にする必要があります）。次に、server.ini ファイルの [UWeb.WebServer] セクションで、ListenPort を 8080（上記のマップされたポートに合わせます）、ServerName を ISP からルータに割り当てられた IP に設定します。

Q. LAN で複数のゲーマーが 1 台のゲーム サーバを使用して、1 つのパブリック IP アドレスだけで同時にプレイすることはできますか。

使用するネットワーク ゲームまたはゲーム サーバにより異なります。たとえば、Unreal Tournament は、1 つのパブリック IP で複数のログインをサポートしています。

Q. Half-Life の Team Fortress をルータで動作させるにはどうすればよいですか。

Half-Life のデフォルトのクライアント ポートは 27005 です。LAN のコンピュータは、「+clientport 2700x」を HL ショートカット コマンド ラインに追加する必要があります。x は 6、7、8 などです。これにより、複数のコンピュータを同じサーバに接続できます。ただし問題が 1 つあります。バージョン 1.0.1.6 では、同じ CD キーを持つ複数のコンピュータは、同じ LAN 上にあっても、同時には接続できません（1.0.1.3 に関する問題ではありません）。ホスティング ゲームである限り、HL サーバは DMZ にある必要はありません。ポート 27015 をサーバ コンピュータのローカル IP アドレスに転送するだけです。

Q. FTP ダウンロードの破損をどのようにブロックできますか。

FTP クライアントでファイルをダウンロードするときにファイルが壊れた場合、別の FTP プログラムを使用してみてください。

Q. Web ページがハングする、ダウンロードが破損する、または読めない文字だけがウィンドウに表示される現象が起こります。どうすればよいですか。

10 Mbps 半二重モードを使用するようにイーサネット アダプタを設定します（Windows PC で [コントロール パネル] > [システム] > [ハードウェア] を開き、[デバイス マネージャ] ボタンをクリックします。[ネットワーク アダプタ] のプロパティを開き、[詳細設定] タブをクリックします。[Speed & Duplex] の設定を [10 Mb Half] に変更します。「自動ネゴシエーション」設定は使用しないでください）。詳細については、シスコの Web サイト（www.cisco.com）で確認してください。

Q. 何をしてもインストールが失敗する場合はどうすればよいですか。

[RESET] ボタンを 10 秒間押してルータをリセットします。装置の電源を切ってから再び電源を入れ、ケーブルまたは DSL モデムをリセットします。シスコの Web サイト（www.cisco.com）で利用できる最新のファームウェア リリースを取得およびフラッシュします。

Q. 新しいルータ ファームウェア アップグレードの通知を受けるにはどうすればよいですか。

すべてのシスコ ファームウェア アップグレードは、www.cisco.com で公開され、ここから無料でファイルをダウンロードできます。ルータのファームウェアは、設定ユーティリティを使用してアップグレードできます。ルータのインターネット接続が正常に機能している場合、必要な新機能が含まれている場合、新しいファームウェア バージョンをダウンロードする必要はありません。さらに新しいバージョンのルータ ファームウェアをダウンロードすると、インターネット接続の品質または速度が改善されず、現在の接続の安定性が損なわれることがあります。

Q. ルータは Macintosh 環境でも動作しますか。

はい。ただし、Macintosh の場合、ルータの設定ページにアクセスできるのは、Internet Explorer 5.0 または Netscape Navigator 5.0 以上からだけです。

Q. ルータの Web コンフィギュレーション ウィンドウを表示できません。どうすればよいですか。

Netscape Navigator または Internet Explorer などのインターネット ブラウザのプロキシ設定を削除する必要があります。または、ブラウザのダイヤルアップ設定を削除します。ブラウザのマニュアルを確認して、ブラウザが正しく接続できるように設定されていること、およびダイヤルアップが無効になっていることを確認します。Internet Explorer の場合、[ツール] > [インターネット オプション] > [接続] タブの順にクリックします。Internet Explorer が [ダイヤルしない] に設定されていることを確認します。Netscape Navigator の場合、[編集] > [設定] > [詳細] > [プロキシ] の順にクリックします。Netscape Navigator が [インターネットに直接接続する] に設定されていることを確認します。

Q. DMZ ホスティングとは何ですか。

非武装地帯（DMZ）を使用することで、1 つの IP アドレス（コンピュータ）をインターネットに公開することができます。アプリケーションによっては、複数の TCP/IP ポートを開く必要があります。DMZ コンピュータを使用する場合、スタティック IP でコンピュータを設定することをお勧めします。

Q. DMZ ホスティングを使用する場合、公開されるユーザはパブリック IP をルータと共有しますか。

いいえ。

Q. ルータは PPTP パケットを転送したり、PPTP セッションをアクティブにルーティングしますか。

このルータを使用することで PPTP パケットのパススルーが可能になります。

Q. ルータにはプラットフォーム間の互換性がありますか。

このルータは、イーサネットおよび TCP/IP をサポートするあらゆるプラットフォームと互換性があります。

Q. 同時にいくつのポートを転送できますか。

理論上、ルータは、2,048 のセッションを同時に確立できますが、転送できるポート範囲は 30 だけです。

Q. ルータはモデムの代わりになりますか。また、ルータにはケーブルまたは DSL モデムがありますか。

いいえ。このバージョンのルータは、ケーブルまたは DSL モデムと連携で動作させる必要があります。

Q. ルータはどのモデルと互換性がありますか。

このルータは、実質的にイーサネットをサポートするすべてのケーブルまたは DSL モデムと互換性があります。

Q. スタティックまたは DHCP IP アドレスを使用しているか確認するにはどうすればよいですか。

ISP にお問い合せください。

Q. mIRC をルータで機能させるにはどうすればよいですか。

[ファイアウォール] > [単一ポートのフォワーディング] メニューから、mIRC を使用する PC のポート フォワーディングを 113 に設定します。

B

Windows 2000、XP または Vista での Cisco QuickVPN の使用

概要

この付録では、www.cisco.com からダウンロードできる Cisco QuickVPN ソフトウェアのインストールおよび使用方法について説明します。QuickVPN は、Windows 2000、XP、Vista または Windows 7 を実行するコンピュータで機能します（他のオペレーティング システムを使用するコンピュータはサードパーティ VPN ソフトウェアを使用する必要があります）。Windows Vista の場合、QuickVPN クライアント バージョン 1.2.5 以降が必要です。Windows 7 の場合、バージョン 1.4.0.5 以降が必要です。

この付録の内容は、次のとおりです。

作業を開始する前に

QuickVPN プログラムは、QuickVPN 接続を受け入れるように正しく設定されているシスコ 4 ポート ギガビット VPN セキュリティ ルータだけで機能します。次の手順に従い、ルータの VPN クライアント設定を行います。

ステップ 1 [VPN] > [VPN クライアントアカウント] をクリックします。

ステップ 2 ユーザ名を [ユーザ名] フィールドに入力します。

ステップ 3 パスワードを [パスワード] フィールドに入力して、同じパスワードを [パスワードの再入力] フィールドに再入力します。

ステップ 4 [追加/保存] をクリックします。

ステップ 5 VPN クライアント 1 の [アクティブ] チェックボックスをオンにします。

ステップ 6 [保存] をクリックします。

[VPN クライアントアカウント] ウィンドウ

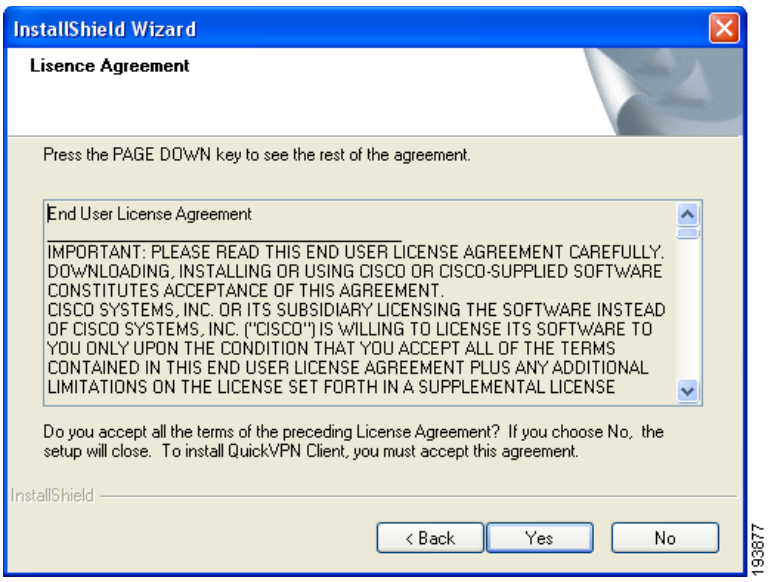
Cisco QuickVPN ソフトウェアのインストール

CD-ROM からのインストール

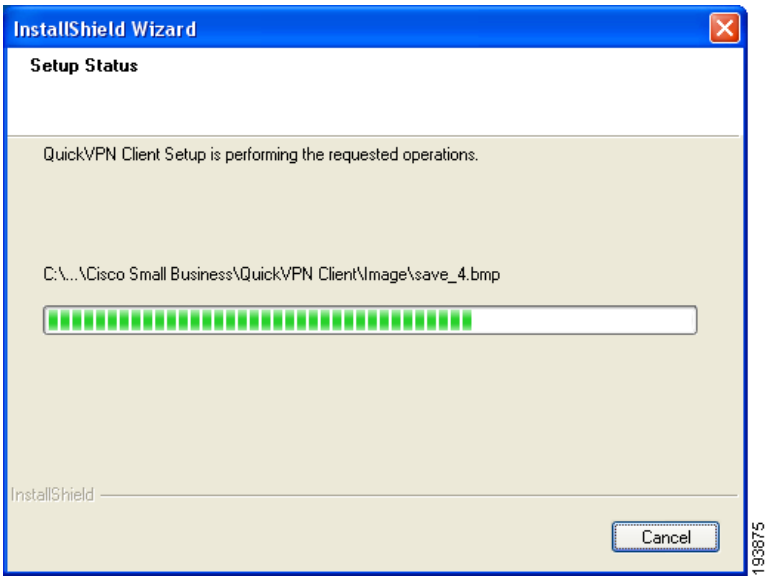
ステップ 1 RVS4000 CD-ROM を CD-ROM ドライブに挿入します。[スタート] メニューに移動して、[ファイル名を指定して実行] をクリックします。表示されたフィールドに、**D:¥VPN_Client.exe**（「**D**」が CD-ROM ドライブのドライブ レターである場合）と入力します。

ステップ 2 [License Agreement] ウィンドウが表示されます。[Yes] をクリックして、ライセンス規定に同意します。適切なファイルがコンピュータにコピーされます。

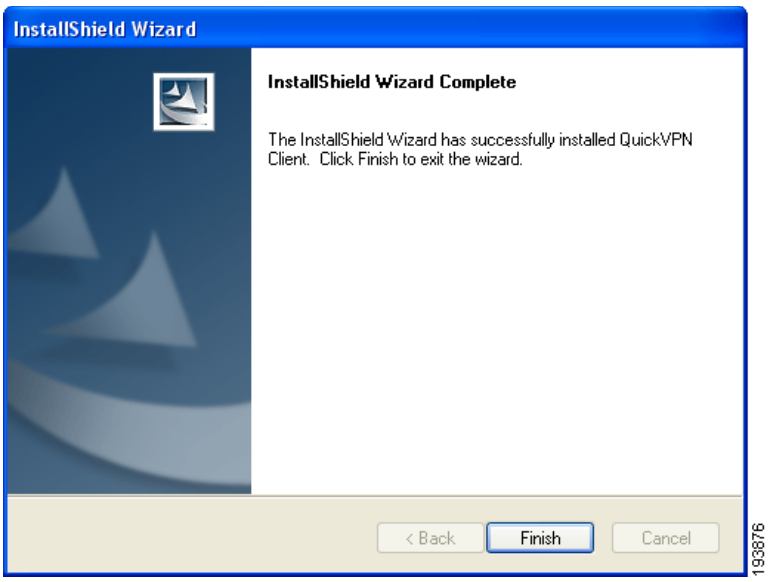
ライセンス契約書



ファイルのコピー



ファイルのインストール完了



ステップ 3 [Finish] をクリックしてインストールを完了します。**「Cisco QuickVPN ソフトウェアの使用」（P.133）**に進みます。

インターネットからのダウンロードおよびインストール

ステップ 1 **付録 G「関連情報」**のファームウェア ダウンロード リンクに移動します。

ステップ 2 ファームウェア ダウンロード リンクから、[Download Software] をクリックします。

ステップ 3 メニューから [Cisco Small Business Routers] > [RVS4000] を選択します。

ステップ 4 [QuickVPN Utility] を選択します。

ステップ 5 zip ファイルを PC に保存して、.exe ファイルを解凍します。

ステップ 6 .exe ファイルをダブルクリックして、画面の指示に従います。次の**「Cisco QuickVPN ソフトウェアの使用」（P.133）**に進みます。

Cisco QuickVPN ソフトウェアの使用

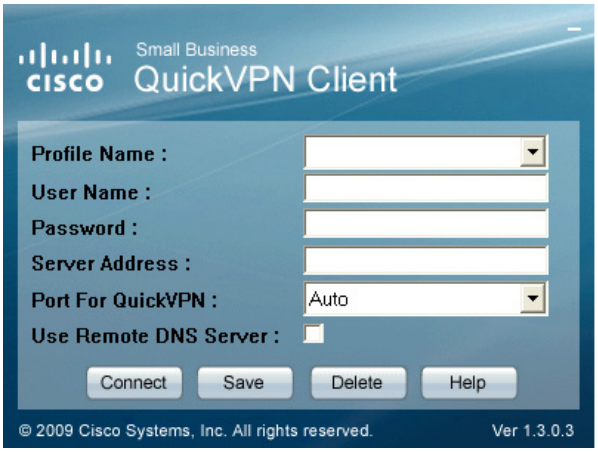
ステップ 1 デスクトップまたはシステム トレイの Cisco QuickVPN ソフトウェア アイコンをダブルクリックします。

QuickVPN のデスクトップ アイコン

QuickVPN のトレイ アイコン（未接続）

ステップ 2 [QuickVPN Login] ウィンドウが表示されます。[Profile Name] フィールドに、プロファイルの名前を入力します。[User Name] および [Password] フィールドに割り当てられたユーザ名およびパスワードを入力します。[Server Address] フィールドに、シスコ 4 ポート ギガビット VPN セキュリティ ルータの IP アドレスまたはドメイン名を入力します。[Port For QuickVPN] フィールドに、QuickVPN クライアントがリモート VPN ルータとの通信に使用するポート番号を入力するか、デフォルト設定 [Auto] をそのまま使用します。

QuickVPN ログイン



このプロファイルを保存するには、[Save] をクリックします（トンネルを作成する必要があるサイトが複数ある場合、複数のプロファイルを作成できますが、一度にアクティブにできるトンネルは 1 つだけなので注意してください）。このプロファイルを削除するには、[Delete] をクリックします。詳細については、[Help] をクリックしてください。

ステップ 3 QuickVPN 接続を開始するには、[Connect] をクリックします。接続の進捗状況として、「Connecting」、「Provisioning」、「Activating Policy」、および「Verifying Network」が表示されます。

ステップ 4 QuickVPN 接続が確立されると、QuickVPN トレイ アイコンが緑に変わり、[QuickVPN Status] ウィンドウが表示されます。このウィンドウには、VPN トンネルのリモート エンドの IP アドレス、VPN トンネルが開始した時間と日付、VPN トンネルがアクティブになっている時間が表示されます。

QuickVPN のトレイ
アイコン（接続中）

QuickVPN ステータス

VPN トンネルを終了するには、[Disconnect] をクリックします。パスワードを変更するには、[Change Password] をクリックします。詳細については、[Help] をクリックしてください。

ステップ 5 [Change Password] をクリックすると、独自のパスワードを変更できる権限がある場合、バーチャル プライベート接続ウィンドウが表示されます。パスワードを [Old Password] フィールドに入力します。新しいパスワードを [New Password] フィールドに入力します。次に、新しいパスワードを再び [Confirm New Password] フィールドに入力します。[OK] をクリックして新しいパスワードを保存します。変更をキャンセルする場合は [Cancel] をクリックします。詳細については、[Help] をクリックしてください。

バーチャル プライベート接続

（注） パスワードを変更できるのは、システム管理者によりその権限が付与されている場合だけです。

証明書の QuickVPN ユーザへの配布

次の手順に従い、QuickVPN ユーザに配布するために証明書を RVS4000 からエクスポートして、その証明書を QuickVPN ユーザの PC にインストールします。

ステップ 1 証明書は次のように生成します。

a. 設定ユーティリティにログインします。

b. [VPN] > [VPN クライアントアカウント] を選択します。

c. [生成] をクリックして新しい証明書を生成します。

d. [クライアント用エクスポート] をクリックして、証明書を **.PEM** ファイルとして保存します。

ステップ 2 証明書をすべての QuickVPN ユーザに配布します。

ステップ 3 各 QuickVPN ユーザは、次のように証明書をインストールする必要があります。

a. QuickVPN クライアントがインストールされているディレクトリに証明書を保存します。次に例を示します。
C:¥Program Files¥Cisco¥QuickVPN Client¥

b. QuickVPN クライアントを起動して、ユーザ名、パスワードおよびサーバ アドレス（IP アドレスまたはドメイン名）を指定します。

c. [接続] をクリックします。

証明書管理の詳細については、**第 5 章「ルータのセットアップおよび設定」の「[VPN] > [VPN クライアントアカウント]」（P.63）**を参照してください。

C

Windows 2000/XP コンピュータでの IPSec の設定

この付録では、Windows 2000 または Windows XP を使用したコンピュータでの IPSec の設定方法について説明します。次のトピックを参照してください。

はじめに

この付録では、ルータ内のプライベート ネットワークと Windows 2000/XP コンピュータを結合できるように、事前共有キーを使用して安全な IPSec トンネルを設定する方法について説明します。Windows 2000 サーバでの設定に関する詳細については Microsoft Web サイトを参照してください。

Microsoft KB Q252735：Windows 2000 における IPSec トンネリングの構成方法：
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225：Microsoft Windows 2000 Server での IPSec のトラブルシューティング：
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

（注）

- 加えた変更は必ず記録しておいてください。これらの変更については、Windows の「secpol」アプリケーションとルータの設定ユーティリティで同一の内容が保持されます。
- 画面に表示されるテキストは、[OK] や [閉じる] ボタンに関する説明と内容が異なることがあります。適宜、画面に応じたボタンをクリックしてください。

環境

この付録で例示する IP アドレス、および詳細事項は説明だけを目的としたものです。

Windows 2000 または Windows XP

IP アドレス：140.111.1.2 <= ユーザの ISP が提供する IP アドレス（一例です）

サブネット マスク：255.255.255.0

RVS4000

WAN IP アドレス：140.111.1.1 <= ユーザの ISP が提供する IP アドレス（一例です）

サブネット マスク：255.255.255.0

LAN IP アドレス：192.168.1.1

サブネット マスク：255.255.255.0

安全な IPSec トンネルを確立する方法

安全な IPSec トンネルを確立するには、次の 5 つのステップに従う必要があります。

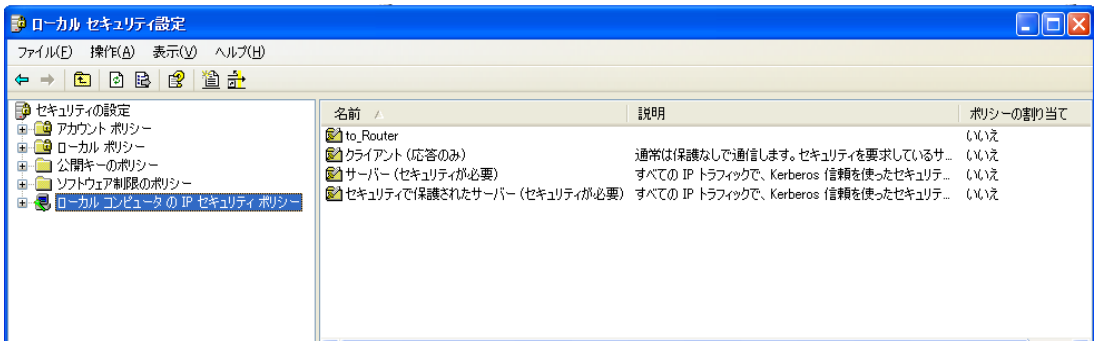
- ステップ 1：IPSec ポリシーの作成
- ステップ 2：フィルタ リストの作成
- ステップ 3：各トンネル規則の設定
- ステップ 4：新規 IPSec ポリシーの割り当て
- ステップ 5：設定ユーティリティによるトンネルの作成

安全な IPSec トンネルの確立

ステップ 1 IPSec ポリシーの作成

a. [スタート] をクリックし、[ファイル名を指定して実行] を選択して、開いたフィールドに **secpol.msc** と入力します。[ローカル セキュリティ設定] ウィンドウが表示されます。

[ローカル セキュリティ設定]



b. [ローカル コンピュータの IP セキュリティ ポリシー] (Windows XP または Windows 2000) を右クリックして、[IP セキュリティ ポリシーの作成] をクリックします。

c. [次へ] ボタンをクリックして、ポリシーの名前（たとえば to_Router）を入力します。さらに [次へ] をクリックします。

d. [既定の応答規則をアクティブにする] ボックスをオフにして、[次へ] をクリックします。

e. [編集] ボックスがオンになっていることを確認して [完了] をクリックします。

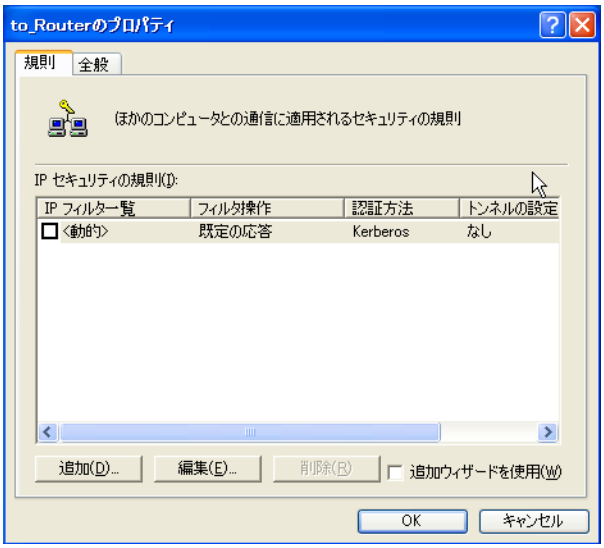
ステップ 2 フィルタ リストの作成

（注） このセクションでは「win」という用語は Windows 2000 と Windows XP の両方を指すものとします。

フィルタ リスト 1：win -> router

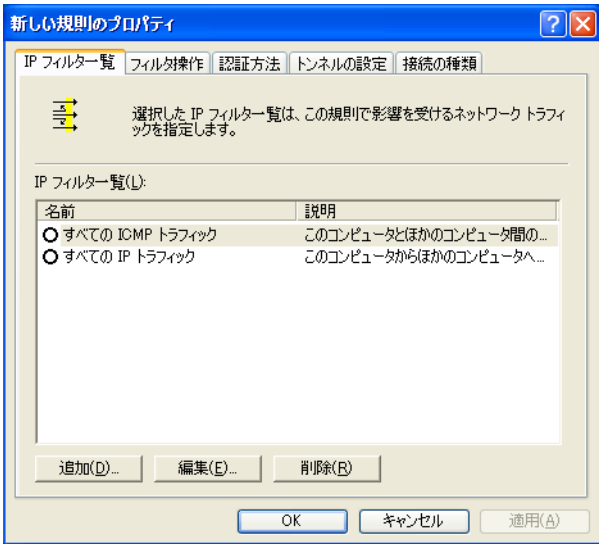
a. 新規ポリシーのプロパティ ウィンドウで、[規則] タブが選択されていることを確認します。[追加ウィザードを使用] ボックスをオフにした状態で [追加] をクリックし、新規の規則を作成します。

[規則] タブ



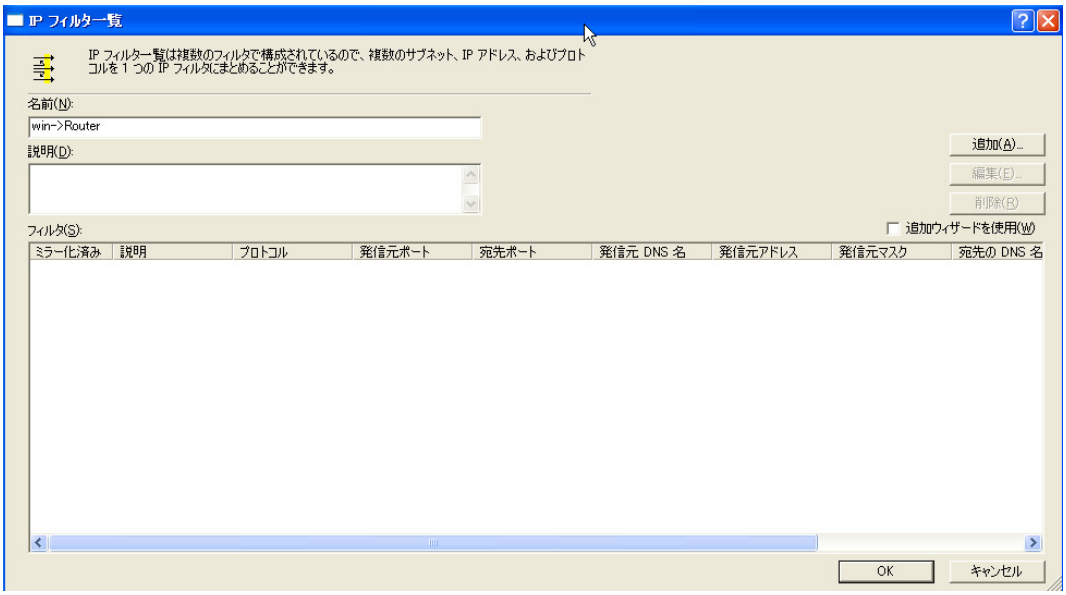
b. [IP フィルター一覧] タブが選択されていることを確認します。[追加] をクリックします。

[IP フィルター一覧] タブ



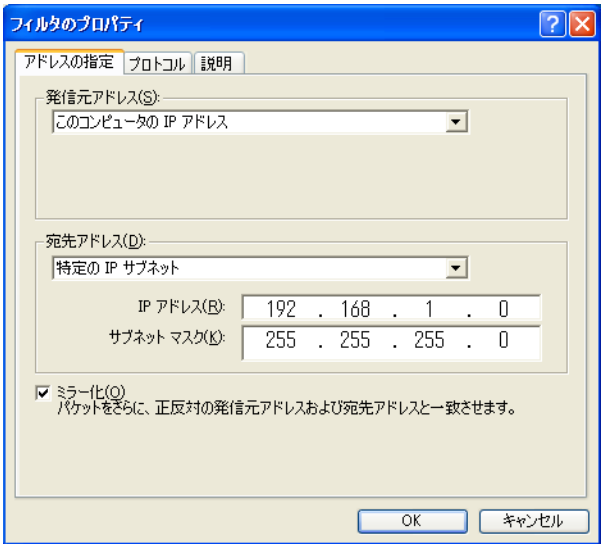
c. [IP フィルター一覧] ウィンドウが表示されます。フィルタ リストの適切な名前（たとえば win-> Router）を入力し、[追加ウィザードを使用] ボックスをオフにします。次に [追加] をクリックします。

[IP フィルター一覧]



d. [フィルタのプロパティ] ウィンドウが表示されます。[アドレスの指定] タブを選択します。

[フィルタのプロパティ]



[発信元アドレス] フィールドで、[このコンピュータの IP アドレス] を選択します。[宛先アドレス] フィールドで [特定の IP サブネット] を選択し、IP アドレス **192.168.1.0** とサブネット マスク **255.255.255.0** を入力します （これはルータのデフォルト設定です。この設定を変更したときは、新しい値を入力します）。

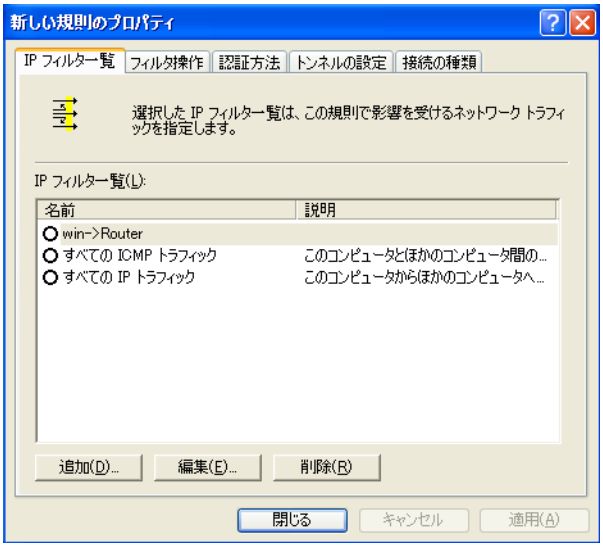
e. フィルタに関する説明を入力する場合は、[説明] タブをクリックして、フィルタの説明を入力します。

f. [OK] をクリックします。次に、[IP フィルター一覧] ウィンドウの [OK] または [閉じる] をクリックします。

フィルタ リスト 2：router -> win

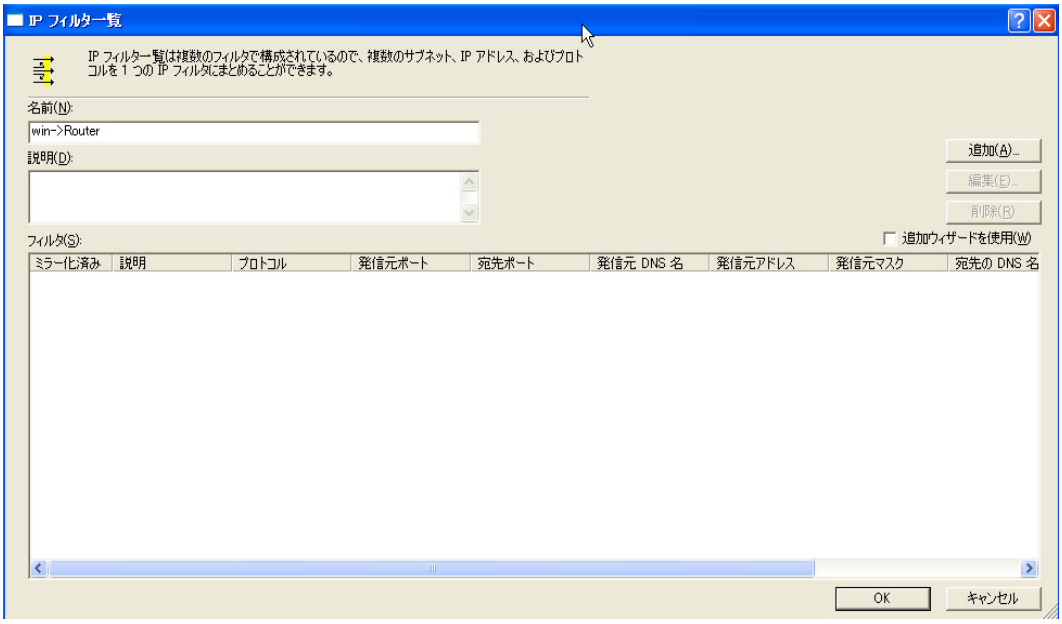
g. [新しい規則のプロパティ] ウィンドウが表示されます。[IP フィルター一覧] タブを選択して、[win -> Router] が強調表示されていることを確認します。次に [追加] をクリックします。

[新しい規則のプロパティ]



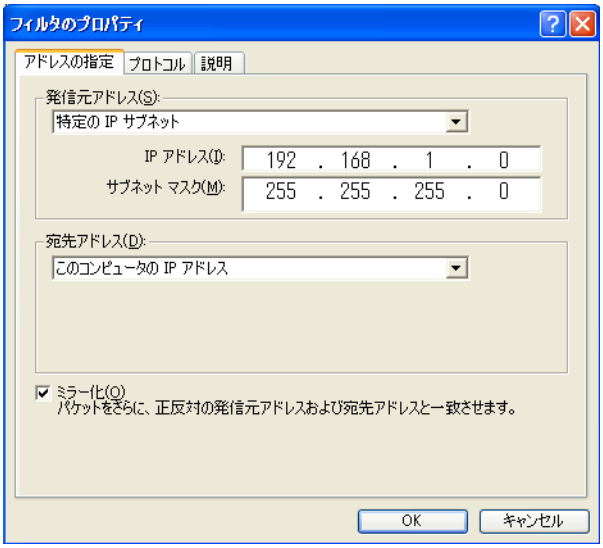
h. [IP フィルター一覧] ウィンドウが表示されます。フィルタ リストの適切な名前（たとえば Router->win）を入力し、[追加ウィザードを使用] ボックスをオフにします。[追加] をクリックします。

[IP フィルター覧]



i. [フィルタのプロパティ] ウィンドウが表示されます。[アドレスの指定] タブを選択します。[発信元アドレス] フィールドで [特定の IP サブネット] を選択し、IP アドレス **192.168.1.0** とサブネット マスク **255.255.255.0** を入力します （デフォルトの設定を変更した場合は、新しい値を入力します）。[宛先アドレス] フィールドで [このコンピュータの IP アドレス] を選択します。

[フィルタのプロパティ]

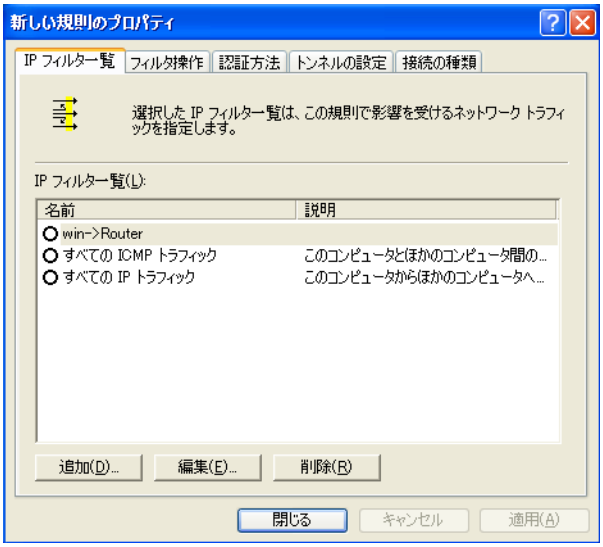


j. フィルタに関する説明を入力する場合は、[説明] タブをクリックして、フィルタの説明を入力します。

k. [OK] または [閉じる] をクリックします。

[IP フィルター覧] タブが選択された状態で [新しい規則のプロパティ] ウィンドウが表示されます。ウィンドウには、[Router->win] と [win->Router] のリストが表示されます。

[新しい規則のプロパティ]



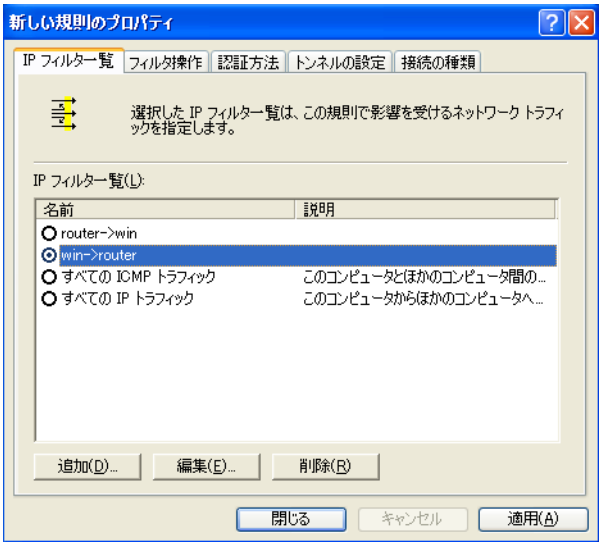
l. [IP フィルター覧] ウィンドウで [OK]（Windows XP）または [閉じる]（Windows 2000）をクリックします。

ステップ 3 各トンネル規則の設定

トンネル 1：win -> Router

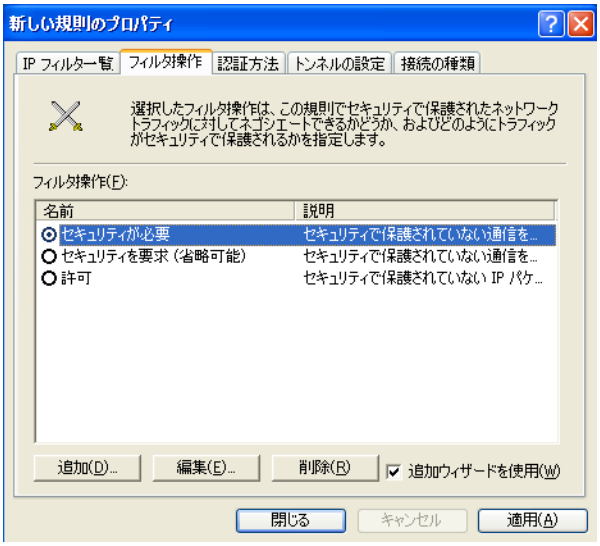
a. [IP フィルター一覧] タブで、フィルタ リストの win -> Router を選択します。

[IP フィルター一覧] タブ



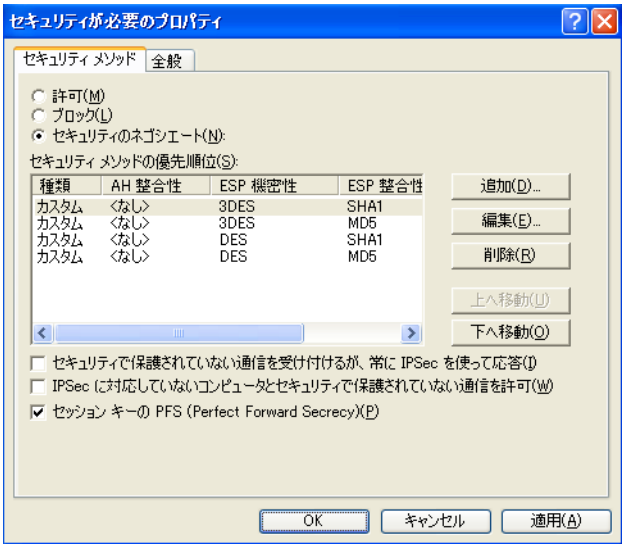
b. [フィルタ操作] タブをクリックし、フィルタ操作の [セキュリティが必要] オプション ボタンをクリックします。[編集] をクリックします。

[フィルタ操作] タブ



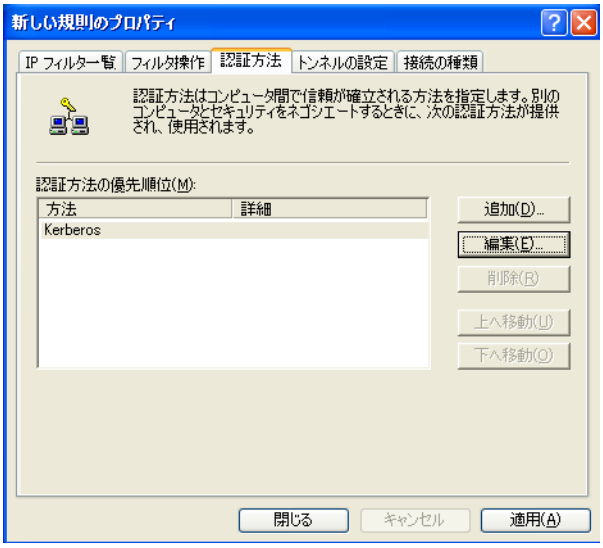
c. [セキュリティ メソッド] タブで、[セキュリティのネゴシエート] オプションが有効になっており、[セキュリティで保護されていない通信を受け付けるが、常に IPSec を使って応答] ボックスがオフになっていることを確認します。[セッション キーの PFS (Perfect Forward Secrecy)] を選択し、[OK] をクリックします。

[セキュリティ メソッド] タブ



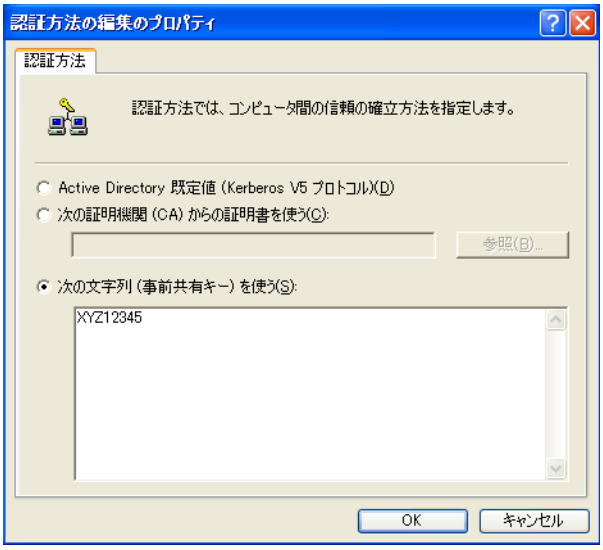
d. [認証方法] タブを選択して、[編集] をクリックします。

[認証方法] タブ



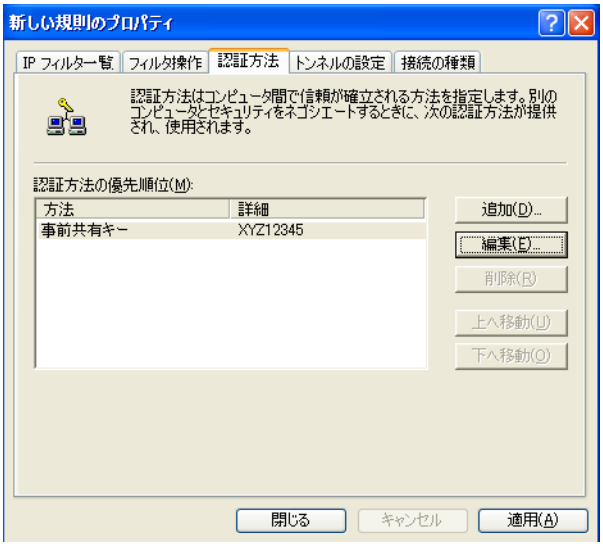
e. 認証方法を [次の文字列 (事前共有キー) を使う] に変更し、事前共有キー文字列（たとえば XYZ12345）を入力します。[OK] をクリックします。

事前共有キー



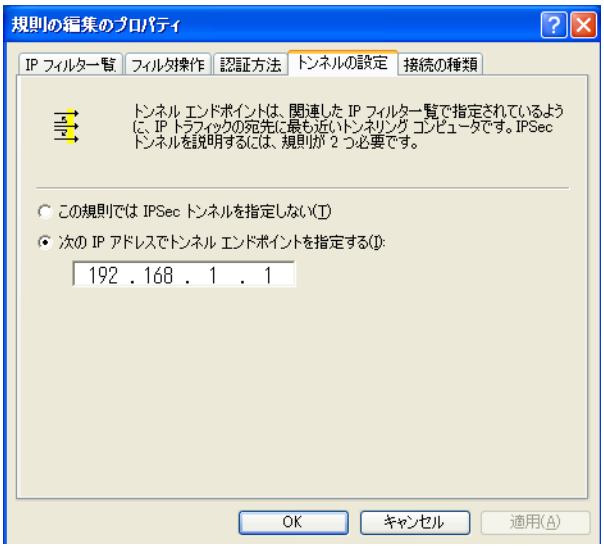
f. この新しい事前共有キーが表示されます。[適用] ボタン（画面に表示される場合）をクリックして、続行します。表示されない場合は、次のステップに進みます。

新しい事前共有キー



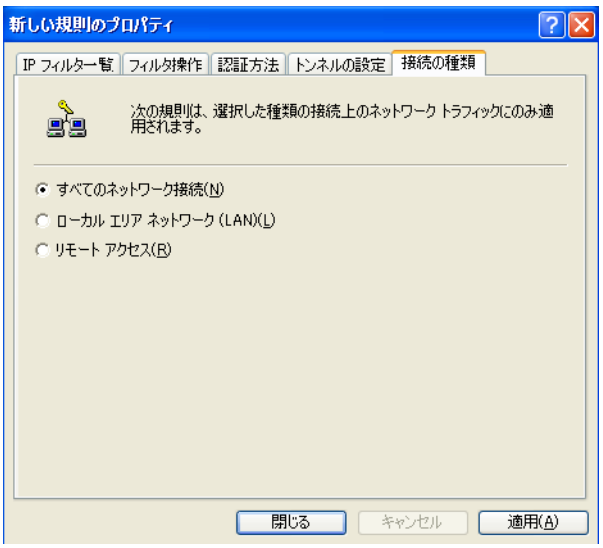
g. [トンネルの設定] タブを選択して、[次の IP アドレスでトンネル エンドポイントを指定する] オプション ボタンをクリックします。次にルータの WAN IP アドレスを入力します。

[トンネルの設定] タブ



h. [接続の種類] タブを選択して、[すべてのネットワーク接続] をクリックします。[OK] または [閉じる] ボタンをクリックして、この規則を終了します。

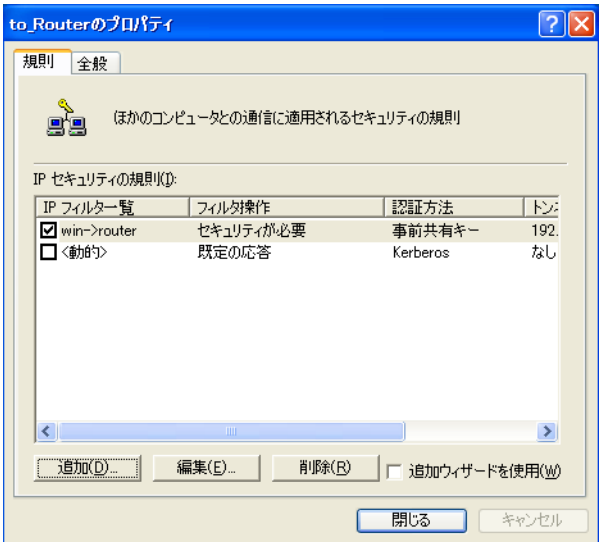
[接続の種類] タブ



トンネル 2：Router -> win

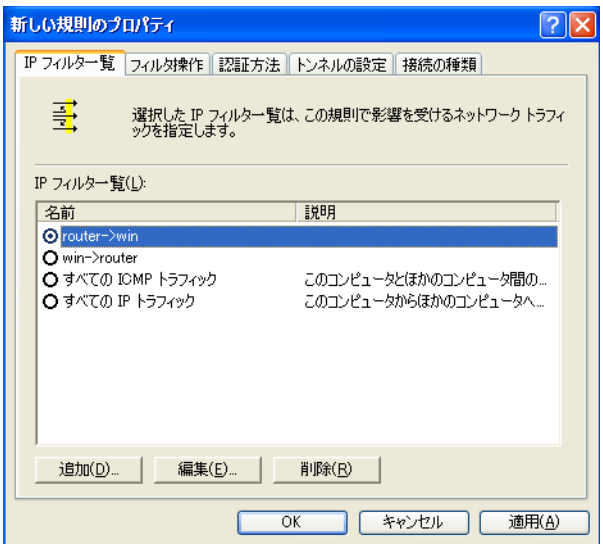
i. 新規ポリシーのプロパティ ウィンドウで、[win -> Router] が選択され、[追加ウィザードを使用] ボックスがオフになっていることを確認します。[追加] をクリックして、2 つ目の IP フィルタを作成します。

プロパティ ウィンドウ



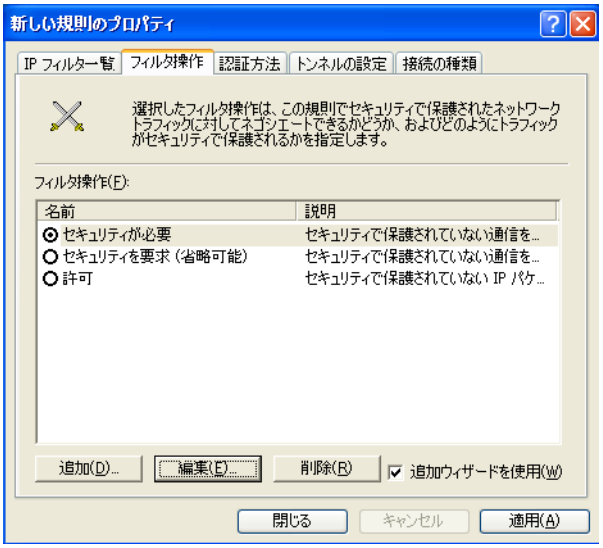
j. [IP フィルター覧] タブを選択して、フィルタ リストの [Router->win] をクリックします。

[IP フィルター覧] タブ



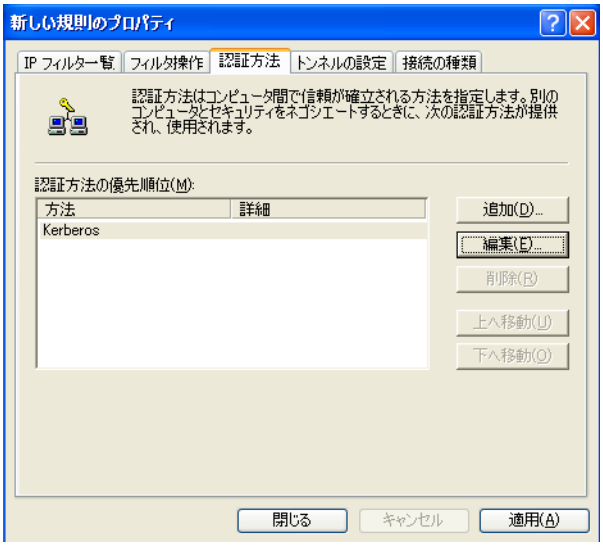
k. [フィルタ操作] タブをクリックして、フィルタ操作の [セキュリティが必要] を選択します。[編集] をクリックします。[セキュリティ メソッド] タブで [セキュリティのネゴシエート] オプションが有効になっており、[セキュリティで保護されていない通信を受け付けるが、常に IPSec を使って応答] ボックスがオフになっていることを確認します。[セッション キーの PFS (Perfect Forward Secrecy)] を選択し、[OK] をクリックします。

[フィルタ操作] タブ



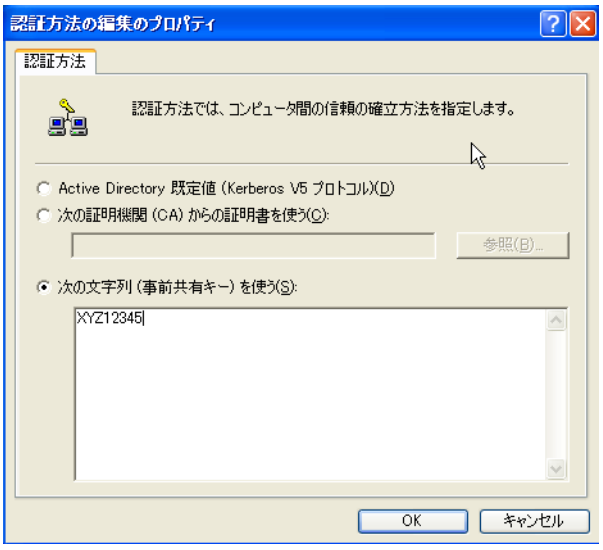
l. [認証方法] タブをクリックし、認証方法として [Kerberos] が選択されていることを確認します。[編集] をクリックします。

[認証方法] タブ



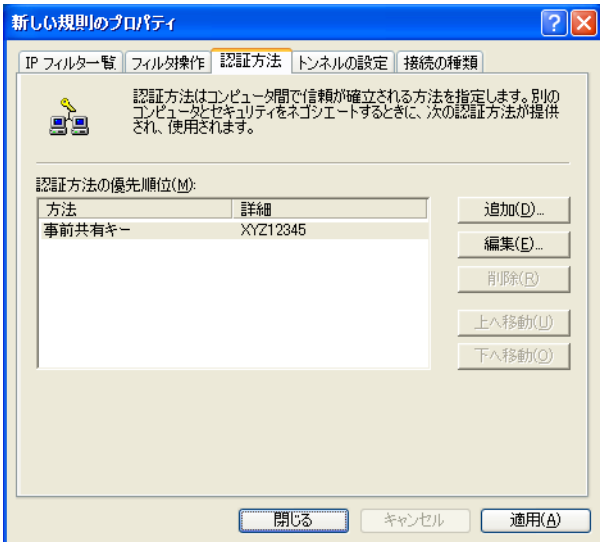
m. 認証方法を [次の文字列 (事前共有キー) を使う] に変更し、事前共有キー文字列（たとえば XYZ12345）を入力します （これは、キー文字列の一例です。実際には、覚えやすい一意のキーを使用してください)。[OK] をクリックします。

事前共有キー



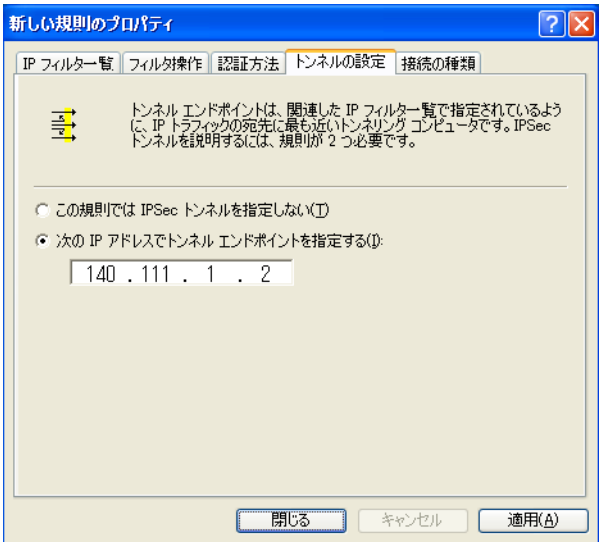
n. この新しい事前共有キーが表示されます。[適用] ボタン（画面に表示される場合）をクリックして、続行します。表示されない場合は、次のステップに進みます。

新しい事前共有キー



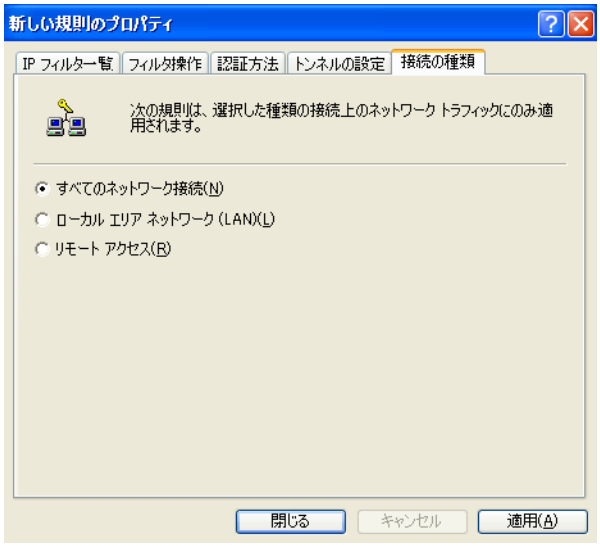
o. [トンネルの設定] タブをクリックします。[次の IP アドレスでトンネル エンドポイントを指定する] オプション ボタンをクリックして、Windows 2000/XP コンピュータの IP アドレスを入力します。

[トンネルの設定] タブ



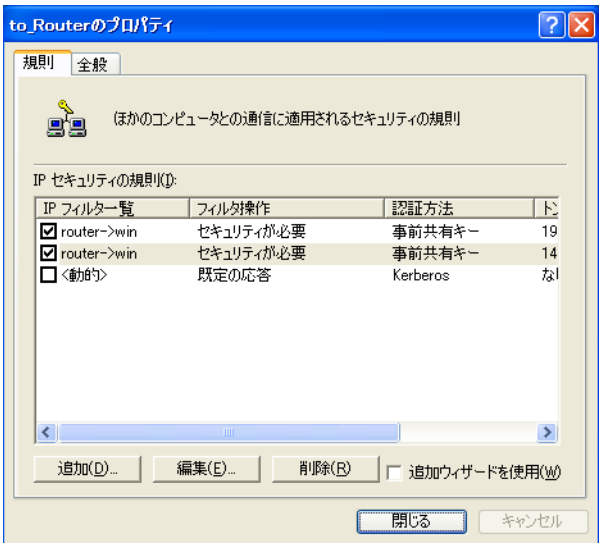
p. [接続の種類] タブをクリックして、[すべてのネットワーク接続] を選択します。[OK] または [閉じる] をクリックして終了します。

[接続の種類] タブ



q. [規則] タブで、[OK] または [閉じる] ボタンをクリックして、セキュリティ ポリシーを表示するウィンドウに戻ります。

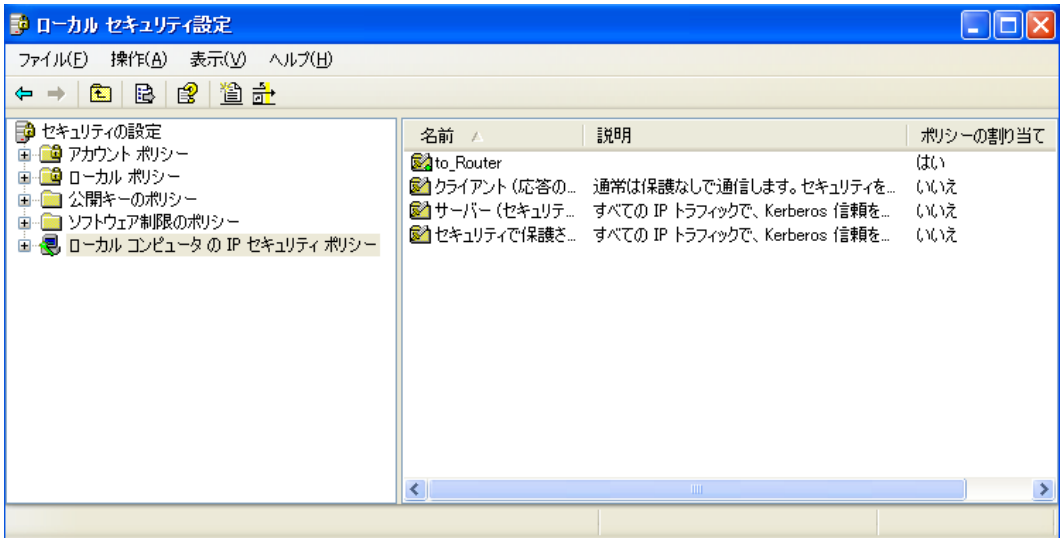
[規則] タブ



ステップ 4 新規 IPSec ポリシーの割り当て

[ローカル コンピュータの IP セキュリティ ポリシー] ウィンドウで「to_Router」というポリシーを右クリックし、[割り当て] をクリックします。フォルダ アイコンに緑の矢印が表示されます。

ローカル コンピュータ



ステップ 5 設定ユーティリティによるトンネルの作成

a. Web ブラウザを開き、アドレス フィールドに **192.168.1.1** と入力します。Enter キーを押します。

b. [ユーザ名] と [パスワード] のフィールドが現れたら、デフォルトのユーザ名とパスワード（**admin**）を入力します。Enter キーを押します。

c. [VPN] > [IPSec VPN] をクリックします。

[VPN] > [IPSec VPN]

d. [トンネルエントリの選択] ドロップダウン ボックスで作成するトンネルを選択します。[有効] をクリックします。[トンネル名] フィールドにトンネルの名前を入力します。これにより、複数のトンネルを識別できるようになります。トンネルの反対側で使用する名前に一致している必要はありません。

e. [ローカルグループの設定] フィールドにローカル VPN ルータの IP アドレスとサブネット マスクを入力します。IP サブネット全体へのアクセスを許可するには、IP アドレスの最後のセットに 0（たとえば 192.168.1.0）を入力します。

f. [リモートグループの設定] フィールドにトンネルの反対側にある VPN デバイス（リモート VPN ルータ、または通信相手となるデバイス）の IP アドレスとサブネット マスクを入力します。

g. 2 種類の認証方法（MD5 または SHA1）からいずれかを選択します（安全性が優れている点で SHA1 を推奨します）。暗号化の場合と同様に、トンネルの反対側の VPN デバイスで同じタイプの認証が使用されている限り、いずれの方法を選択してもかまいません。また、トンネルの両側で認証を無効にすることもできます。

h. [キー入力モード] リストから、[事前共有キー付き IKE] を選択します。次に [事前共有キー] フィールドに一連の数字、または英字を入力します。さらに [PFS(完全転送秘密)] を [有効] にして、初期のキー交換と IKE プロポーザルが保護されるようにします。最大 128 の英数字を任意に組み合わせた文字列をこのフィールドに入力できます。特殊文字、またはスペース文字は使用できません。[キーライフタイム] フィールドでは、指定した期間の終わりにキーの期限が満了するよう選択することができます。キーの有効期間として設定する時間（秒）を入力します。また空白にすると、キーは永続的に有効になります。

i. [保存] をクリックして、変更を保存します。

以上で、トンネルが確立されます。

D

ゲートウェイ間 VPN トンネル

概要

この付録では、2 台の VPN ルータ間に IPSec VPN トンネルを設定する方法について、例を用いて説明します。トンネルの有効性をテストするために 2 台のコンピュータを使用します。この付録は、次の項で構成されます。

作業を開始する前に

必要な機器：

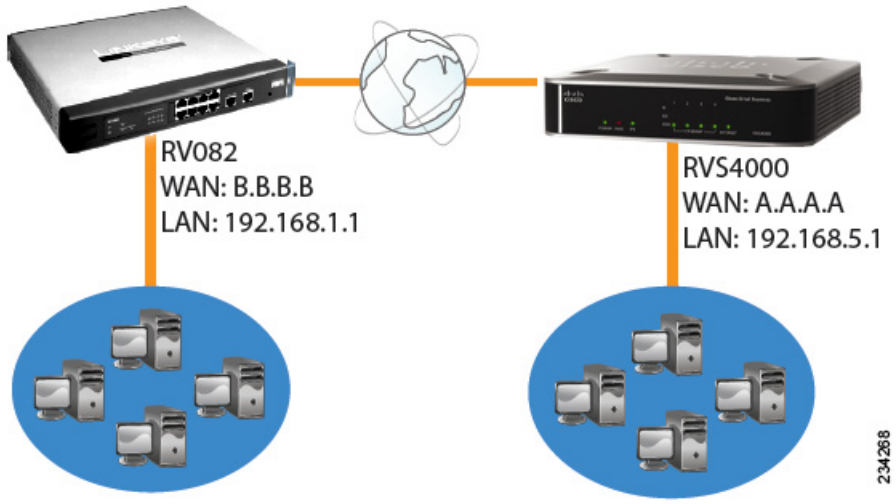
- 2 台の Windows デスクトップ コンピュータ。各コンピュータをそれぞれ 1 台の VPN ルータに接続します。
- 2 台の VPN ルータ（4 ポート ギガビット VPN セキュリティ ルータ：モデル番号 RVS4000、10/100 8 ポート VPN ルータ：モデル番号 RV082）。両方ともインターネットに接続します。

10/100 16 ポート、8 ポート、4 ポート VPN ルータ（モデル番号：RV016、RV082、または RV042）のような任意の VPN ルータを導入できます。なお、この例では RV082 を使用します。

リモート ゲートウェイでスタティック IP アドレスを使用したコンフィギュレーション

この例では、リモート ゲートウェイでスタティック IP アドレスが使用されていることを前提とします。リモート ゲートウェイでダイナミック IP アドレスを使用している場合は、**「リモート ゲートウェイがダイナミック IP アドレスを使用している場合のコンフィギュレーション」（P.163）**を参照してください。

ゲートウェイ間 IPSec VPN トンネル：スタティック IP を使用したリモート ゲートウェイ



（注） 各コンピュータともネットワーク アダプタがインストールされていなければなりません。

ステップ 1 RVS4000 のコンフィギュレーション

次の手順に従って最初の VPN ルータ（「RVS4000」とします）を設定します。もう一方の VPN ルータを「RV082」とします。

a. ネットワーク コンピュータ（「PC 1」とします）で Web ブラウザを起動します。

b. RVS4000 の設定ユーティリティにアクセスします（詳細については、**第 5 章「ルータのセットアップおよび設定」**を参照してください）。

c. [VPN] > [IPSec VPN] をクリックします。

d. [トンネル名] フィールドにトンネルの名前を入力します。

e. [IPSec VPN トンネル] の設定で、[有効] を選択します。

f. RVS4000 の WAN IP アドレス（A.A.A.A）が自動的に検出されます。

[ローカルセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

RVS4000 の IPSec VPN の設定

g. [リモートセキュリティゲートウェイのタイプ] で [IP アドレス] を選択します。[IP アドレス] フィールドに RV082 の WAN IP アドレスを入力します。

h. [リモートセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

i. [IPSec の設定] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します。

j. [事前共有キー] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RVS4000 の [IPSecの設定] の設定

k. さらに詳細な設定が必要な場合は、[詳細設定] をクリックします。そうでなければ、[保存] をクリックして、次の「RV082 のコンフィギュレーション」のステップに進みます。

ステップ 2 RV082 のコンフィギュレーション

RV082 についても同様の指示に従ってください。

a. ネットワーク コンピュータ（「PC 2」とします）で Web ブラウザを起動します。

b. RV082 の設定ユーティリティにアクセスします（詳細については、RV082 のドキュメンテーションを参照してください）。

c. [IPSec VPN] タブをクリックします。

d. [Gateway to Gateway] タブをクリックします。

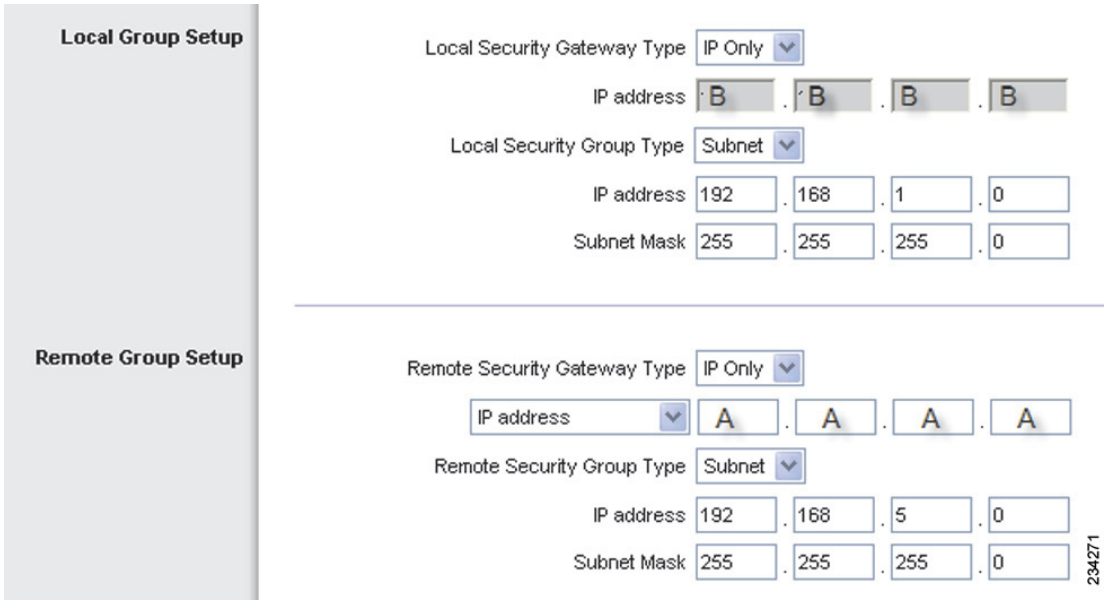
e. [Tunnel Name] フィールドにトンネルの名前を入力します。

f. [VPN Tunnel] の設定で、[Enable] を選択します。

g. RV082 の WAN IP アドレス（B.B.B.B）が自動的に検出されます。

[Local Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

RV082 VPN の設定



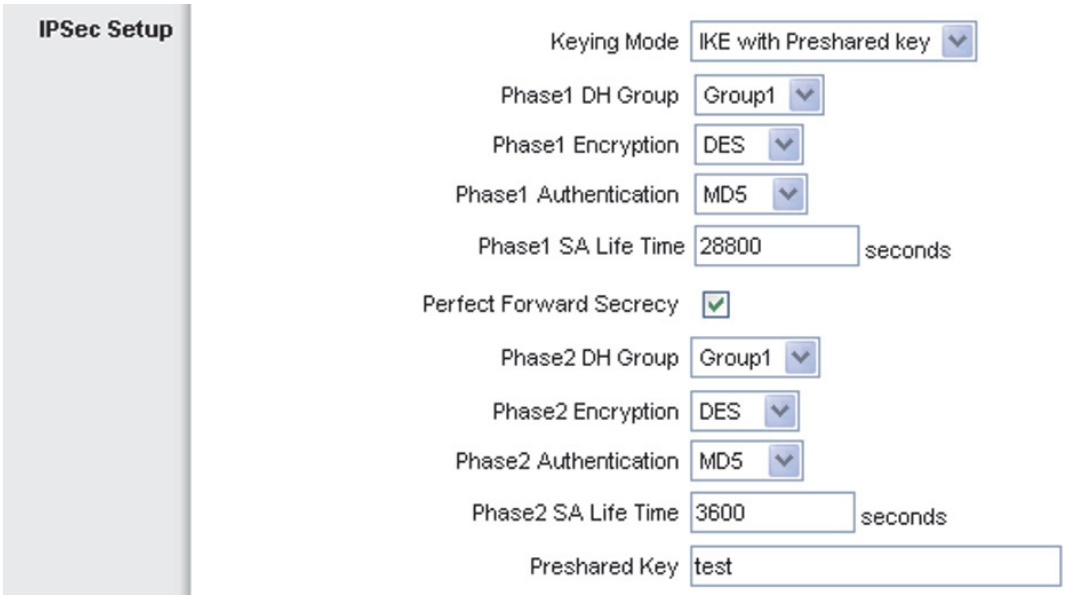
h. [Remote Security Gateway Type] で [IP address] を選択します。[IP address] フィールドに RVS4000 の WAN IP アドレスを入力します。

i. [Remote Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

j. [IPSec Setup] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します（これらの設定は、RVS4000 の設定に一致していなければなりません）。

k. [Preshared Key] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RV082 の [IPSec Setup] の設定



1. さらに詳細な設定が必要な場合は、[Advanced Settings] をクリックします。そうでなければ、[Save Settings] をクリックします。

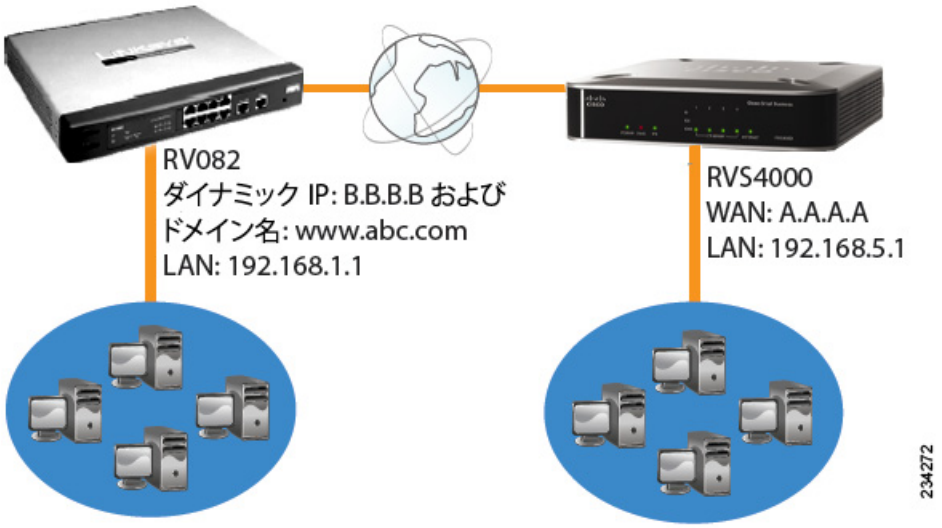
ステップ 3 PC 1 と PC 2 のコンフィギュレーション

Ping で PC 1 と PC 2 が相互通信していることを確認します（詳細については、Windows のヘルプを参照してください）。コンピュータ同士が Ping でやり取りできれば、VPN トンネルが正しく設定されていることになります。

リモート ゲートウェイがダイナミック IP アドレスを使用している場合のコンフィギュレーション

この例では、リモート ゲートウェイでダイナミック IP アドレスが使用されていることを前提とします。リモート ゲートウェイでスタティック IP アドレスを使用している場合は、**「リモート ゲートウェイでスタティック IP アドレスを使用したコンフィギュレーション」（P.158）**を参照してください。

ゲートウェイ間 IPSec VPN トンネル：ダイナミック IP を使用したリモート ゲートウェイ



（注） 各コンピュータともネットワーク アダプタがインストールされていなければなりません。

ステップ 1 RVS4000 のコンフィギュレーション

次の手順に従って最初の VPN ルータ（「RVS4000」とします）を設定します。もう一方の VPN ルータを「RV082」とします。

a. ネットワーク コンピュータ（「PC 1」とします）で Web ブラウザを起動します。

b. RVS4000 の設定ユーティリティにアクセスします（詳細については、**第 5 章「ルータのセットアップおよび設定」**を参照してください）。

c. [VPN] > [IPSec VPN] をクリックします。

d. [トンネル名] フィールドにトンネルの名前を入力します。

e. [IPSec VPN トンネル] の設定で、[有効] を選択します。

f. RVS4000 の WAN IP アドレス（A.A.A.A）が自動的に検出されます。

[ローカルセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

RVS4000 の IPSec VPN の設定

g. [リモートセキュリティゲートウェイのタイプ] で [DNS 解決による IP] を選択します。所定のフィールドに RV082 のドメイン名を入力します。

h. [リモートセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

i. [IPSec の設定] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します。

j. [事前共有キー] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RVS4000 の [IPSecの設定] の設定

k. さらに詳細な設定が必要な場合は、[詳細設定] をクリックします。そうでなければ、[保存] をクリックして、次の「RV082 のコンフィギュレーション」のステップに進みます。

ステップ 2 RV082 のコンフィギュレーション

RV082 についても同様の指示に従ってください。

a. ネットワーク コンピュータ（「PC 2」とします）で Web ブラウザを起動します。

b. RV082 の設定ユーティリティにアクセスします（詳細については、RV082 の説明を参照してください）。

c. [IPSec VPN] タブをクリックします。

d. [Gateway to Gateway] タブをクリックします。

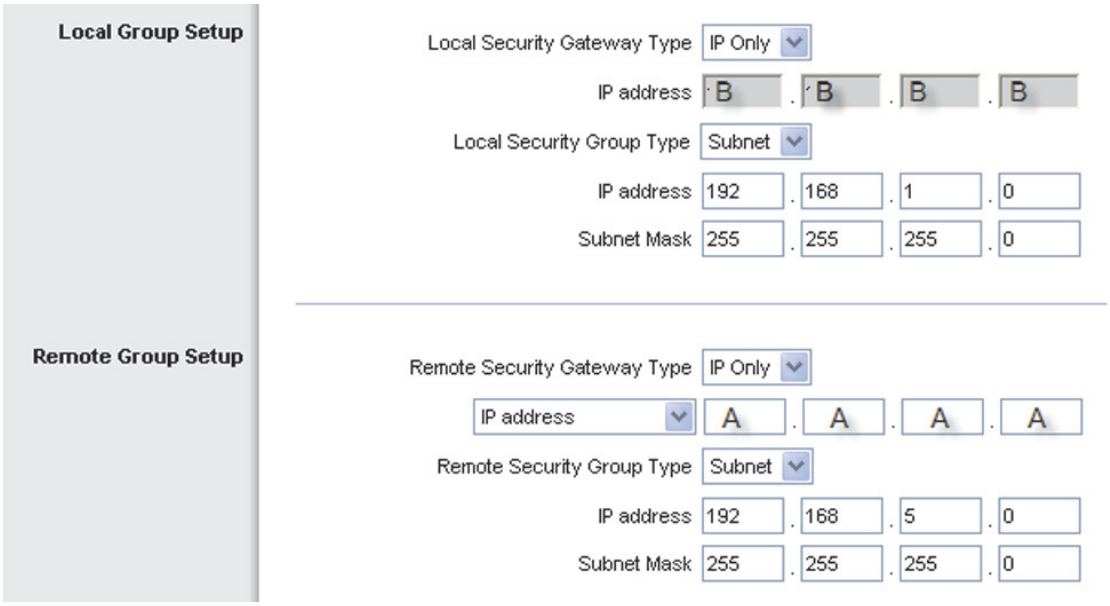
e. [Tunnel Name] フィールドにトンネルの名前を入力します。

f. [VPN Tunnel] の設定で、[Enable] を選択します。

g. RV082 の WAN IP アドレス（B.B.B.B）が自動的に検出されます。

[Local Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

RV082 VPN の設定



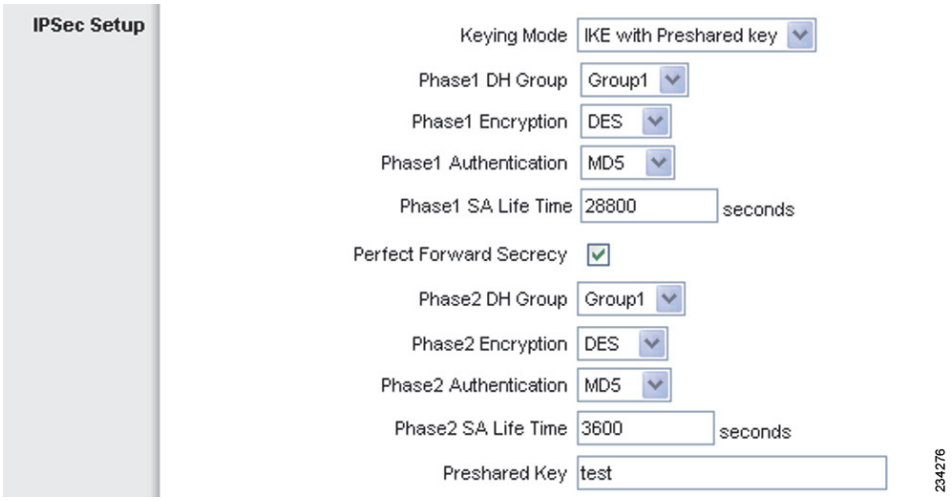
h. [Remote Security Gateway Type] で [IP address] を選択します。[IP address] フィールドに RVS4000 の WAN IP アドレスを入力します。

i. [Remote Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

j. [IPSec Setup] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します（これらの設定は、RVS4000 の設定に一致していなければなりません）。

k. [Preshared Key] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RV082 の [IPSec Setup] の設定



l. さらに詳細な設定が必要な場合は、[Advanced Settings] をクリックします。そうでなければ、[Save Settings] をクリックします。

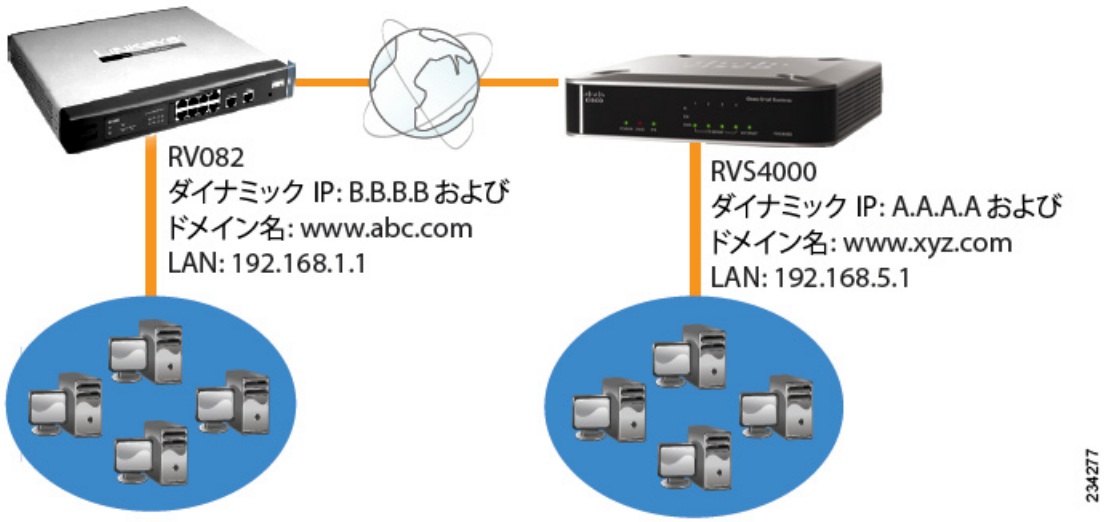
ステップ 3 PC 1 と PC 2 のコンフィギュレーション

Ping で PC 1 と PC 2 が相互通信していることを確認します（詳細については、Windows のヘルプを参照してください）。コンピュータ同士が Ping でやり取りできれば、VPN トンネルが正しく設定されていることになります。

両方のゲートウェイがダイナミック IP アドレスを使用している場合のコンフィギュレーション

この例では、両方のゲートウェイがダイナミック IP アドレスを使用していることを前提とします。一方のリモート ゲートウェイだけがダイナミック IP アドレスを使用している場合は、**「リモート ゲートウェイがダイナミック IP アドレスを使用している場合のコンフィギュレーション」（P.163）**を参照してください。

ゲートウェイ間 IPSec VPN トンネル：
両方のゲートウェイがダイナミック IP を使用している場合



（注） 各コンピュータともネットワーク アダプタがインストールされていなければなりません。

ステップ 1 RVS4000 のコンフィギュレーション

次の手順に従って最初の VPN ルータ（「RVS4000」とします）を設定します。もう一方の VPN ルータを「RV082」とします。

a. ネットワーク コンピュータ（「PC 1」とします）で Web ブラウザを起動します。

b. RVS4000 の設定ユーティリティにアクセスします（詳細については、**第 5 章「ルータのセットアップおよび設定」**を参照してください）。

c. [VPN] > [IPSec VPN] をクリックします。

d. [トンネル名] フィールドにトンネルの名前を入力します。

e. [IPSec VPN トンネル] の設定で、[有効] を選択します。

f. RVS4000 の WAN IP アドレス（A.A.A.A）が自動的に検出されます。

[ローカルセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

RVS4000 の IPSec VPN の設定

g. [リモートセキュリティゲートウェイのタイプ] で [DNS 解決による IP] を選択します。所定のフィールドに RV082 のドメイン名を入力します。

h. [リモートセキュリティグループのタイプ] で [サブネット] を選択します。[IP アドレス] と [サブネットマスク] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

i. [IPSec の設定] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します。

j. [事前共有キー] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RVS4000 の [IPSecの設定] の設定

k. さらに詳細な設定が必要な場合は、[詳細設定] をクリックします。そうでなければ、[保存] をクリックして、次の「RV082 のコンフィギュレーション」のステップに進みます。

ステップ 2 RV082 のコンフィギュレーション

RV082 についても同様の指示に従ってください。

a. ネットワーク コンピュータ（「PC 2」とします）で Web ブラウザを起動します。

b. RV082 の設定ユーティリティにアクセスします（詳細については、RV082 の説明を参照してください）。

c. [IPSec VPN] タブをクリックします。

d. [Gateway to Gateway] タブをクリックします。

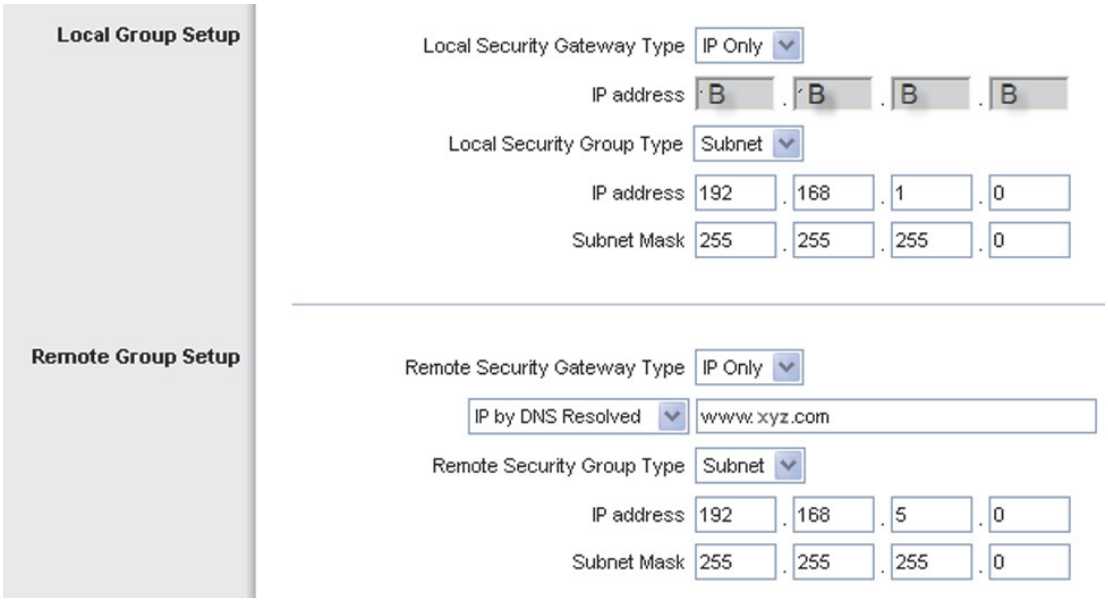
e. [Tunnel Name] フィールドにトンネルの名前を入力します。

f. [VPN Tunnel] の設定で、[Enable] を選択します。

g. RV082 の WAN IP アドレス（B.B.B.B）が自動的に検出されます。

[Local Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RV082 のローカル ネットワークの設定を入力します。

RV082 VPN の設定



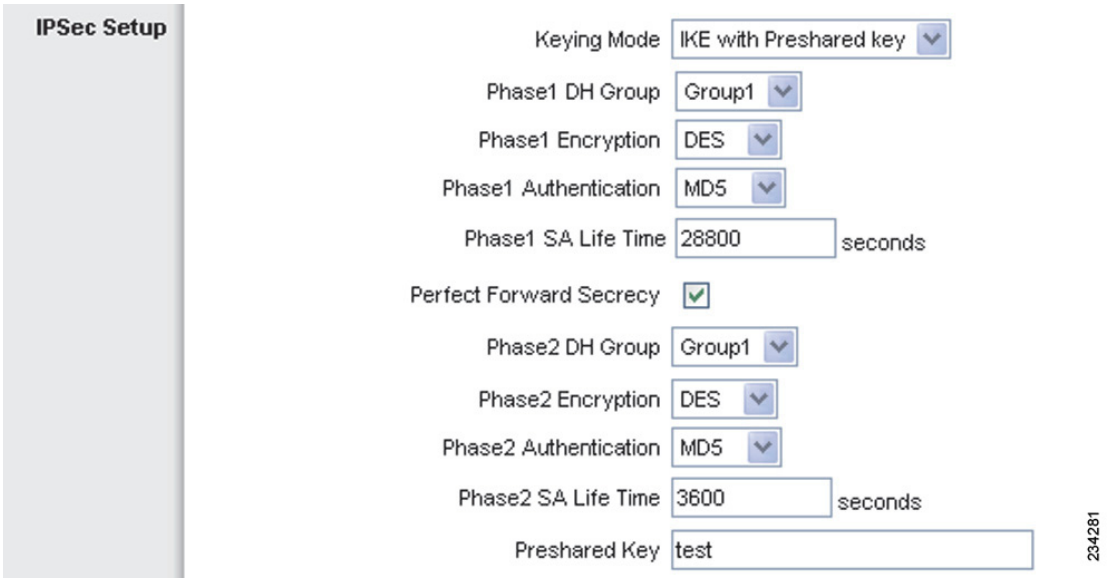
h. [Remote Security Gateway Type] で [IP by DNS Resolved] を選択します。所定のフィールドに RVS4000 のドメイン名を入力します。

i. [Remote Security Group Type] で [Subnet] を選択します。[IP address] と [Subnet Mask] の各フィールドに RVS4000 のローカル ネットワークの設定を入力します。

j. [IPSec Setup] セクションで該当する暗号化、認証、その他のキー管理の設定を選択します（これらの設定は、RVS4000 の設定に一致していなければなりません）。

k. [Preshared Key] フィールドにこのキーの文字列（たとえば、13572468）を入力します。

RV082 の [IPSec Setup] の設定



l. さらに詳細な設定が必要な場合は、[Advanced Settings] をクリックします。そうでなければ、[Save Settings] をクリックします。

ステップ 3 PC 1 と PC 2 のコンフィギュレーション

Ping で PC 1 と PC 2 が相互通信していることを確認します（詳細については、Windows のヘルプを参照してください）。コンピュータ同士が Ping でやり取りできれば、VPN トンネルが正しく設定されていることになります。

E

PPPoE 接続の設定

この付録では、Cisco RVS4000 4 ポート ギガビット VPN セキュリティ ルータでの PPPoE によるインターネット接続について補足説明します。

Unnumbered PPPoE 接続の設定

Unnumbered PPPoE を設定するには、次の手順に従います。

ステップ 1 設定ユーティリティを起動し、画面左側のナビゲーション ペインから [設定] > [WAN] を選択します。

ステップ 2 [WAN] ウィンドウが表示されます。[インターネット接続タイプ] ドロップダウン メニューから [Unnumbered PPPoE] を選択します。

ステップ 3 インターネット サービス プロバイダー（ISP）から提供される「認証 ID（ユーザ名）」、「認証パスワード」を準備して [Unnumbered PPPoE 設定] セクションに入力します。

[IP アドレス]：IP アドレスを入力します。

[サブネットマスク]：255.255.255.248 と入力します。

[ユーザ名]：ISP から提供された認証 ID（ユーザ名）を入力します。

[パスワード] および [パスワードの再入力]：ISP から提供された認証パスワードを入力します。

[Unnumbered ネットワークタイプ]：[Unnumbered IP] を選択します。

（注） [Unnumbered IP+ プライベート] を選択すると、プライベート LAN インターフェイスが 1 つ追加され、Unnumbered IP ネットワークもルータでサポートします。

ステップ 4 必要に応じて、[オプション設定] セクションに入力します。

ステップ 5 入力が完了したら、[保存] をクリックします。

ステップ 6 内容が更新されたら、画面左側のナビゲーション ペインから [ステータス] > [ゲートウェイ] を選択し、[ゲートウェイ] ウィンドウの [接続タイプ] に正しい設定が表示されていることを確認してください。

PPPoE マルチセッション接続の設定

PPPoE マルチセッションを設定するには、次の手順に従います。

ステップ 1 設定ユーティリティを起動し、画面左側のナビゲーション ペインから [設定] > [WAN] を選択します。

ステップ 2 [WAN] ウィンドウが表示されます。[インターネット接続タイプ] ドロップダウン メニューから [PPPoE] を選択します。

ステップ 3 インターネット サービス プロバイダー（ISP）から提供される「認証 ID（ユーザ名）」、「認証パスワード」を準備して [PPPoE 設定] セクションに入力します。

[ユーザ名]：ISP から提供された認証 ID（ユーザ名）を入力します。

[パスワード] および [パスワードの再入力]：ISP から提供された認証パスワードを入力します。

ステップ 4 [セカンダリ PPPoE] の [有効] オプションをオンにし、[セカンダリ PPPoE] ボタンをクリックします。

ステップ 5 [セカンダリ PPPoE] ウィンドウが表示されます。[セカンダリ PPPoE 設定] フィールドを設定します。

[ユーザ名]：ISP から提供されたユーザ名を入力します。

[パスワード] および [パスワードの再入力]：ISP から提供されたパスワードを入力します。

ステップ 6 [トラフィック ルール] フィールドを設定します。

セカンダリ PPPoE 接続でルータを正常に動作させるには、トラフィック ルールを定義する必要があります。セカンダリ PPPoE セッションのトラフィック ルールを定義するには 2 種類の設定方法があります。

ドメイン名で定義する場合：[宛先タイプ] ドロップダウン メニューで [ドメイン] を選択し、[ドメイン名] フィールドにドメイン名を入力します。

IP アドレスで定義する場合：[宛先タイプ] ドロップダウン メニューで [IP アドレス] を選択し、[宛先 IP アドレス] フィールドに IP アドレスとサブネット マスクを入力します。

[ドメイン名] または [宛先IPアドレス] フィールドに入力した後、[追加/保存] ボタンをクリックします。各トラフィック ルールの [有効] チェック ボックスをオンにすると、そのルールが有効になります。

ステップ 7 オンデマンド接続か、キープアライブを選択します。

[オンデマンド接続: 最大アイドル時間]：指定された時間（最大アイドル時間）非アクティブになるとルータがインターネット接続を切断し、インターネットへの再アクセスが試行されると自動的にすぐ接続を再確立するように設定できます。オンデマンド接続を有効にするには、[オンデマンド接続] オプションを選択し、[最大アイドル時間] フィールドに、インターネット接続が自動的に終了するまでの非アクティブ状態の経過時間（分数）を入力します。

[キープアライブ: リダイアル間隔]：このオプションを選択すると、ルータが定期的にインターネット接続を確認します。接続されていない場合、ルータは自動的に接続を再確立します。このオプションを使用するには、[キープアライブ] の隣にあるオプション ボタンをオンにします。[リダイアル間隔] フィールドには、ルータがインターネット接続を確認する頻度を指定します。デフォルトのリダイアル間隔は 30 秒です。

ステップ 8 入力が完了したら、[保存] をクリックします。

F

仕様

この付録では、Cisco RVS4000 4 ポート ギガビット VPN セキュリティ ルータの仕様について説明します。

仕様

モデル	RVS4000
標準規格	IEEE802.3、802.3u、802.1X、RFC791（IP プロトコル）、RFC2460、IPv4（RFC791）、IPv6（RFC2460）、RIPv1（RFC1058）、RIPv2（RFC1723）
ポート	[ETHERNET]、[POWER]
ボタン	[RESET]
ケーブル タイプ	UTP CAT 5e、またはそれ以上
LED	[POWER]、[DIAG]、[IPS]、[ETHERNET（1 ～ 4）]、[INTERNET]
オペレーティング システム	Linux

性能

NAT スループット	IPS 無効時で 800 Mbps

セットアップ / 設定

Web ユーザ インターフェイス	組み込みの Web UI による使いやすいブラウザ ベースでのコンフィギュレーション（HTTP/HTTPS）

管理

SNMP バージョン	SNMP バージョン 1、2c
イベント ロギング	ローカル、Syslog、E メール アラート
ファームウェア アップグレード	Web ブラウザによるファームウェアの提供
診断	フラッシュ、メモリ

セキュリティ機能

アクセス コントロール	Access Control List（ACL; アクセス コントロール リスト）機能：MAC ベース、IP ベース
ファイアウォール	SPI ステートフル パケット インスペクション ファイアウォール
IPS（侵入防御システム）	IP スイープ検出、アプリケーション異常検出（HTTP、FTP、Telnet、RCP）、P2P コントロール、Instant Messenger Control、L3-L4 プロトコル（IP、TCP、UDP、ICMP）正規化、L7 シグニチャ マッチング
セキュア管理	HTTPS、ユーザ名 / パスワード
802.1X	ポート ベース RADIUS 認証（EAP-MD5、EAP-PEAP）

QoS

サービス ベース	サービス ベースの帯域幅管理によりレート コントロールとプライオリティをサポート
プライオリティ タイプ	802.1p、DSCP、ポート ベース
キュー	4 キュー

ネットワーク

DHCP	DHCP サーバ、DHCP クライアント、DHCP リレー エージェント
DNS	DNS リレー、ダイナミック DNS（DynDNS、TZO）
NAT	PAT、NAPT
DMZ	任意の LAN ポート コンフィギュレーションに基づきソフトウェアで設定可能、DHCPv6、ICMPv6
IPv6	デュアル スタック IPv4、および IPv6、6to4、ステートレス アドレス オート コンフィギュレーション、DHCP v6、Intra Module Command Protocol（IMCP）v6
スタティック DHCP	DHCP サーバでは、MAC アドレスに基づくスタティック IP アドレスがサポートされます。

VPN

	リモート クライアント アクセスのための QuickVPN トンネル 5 本、ブランチ オフィス接続用 IPSec ゲートウェイ間トンネル 5 本、 3DES 暗号化、 MD5/SHA1 認証、 IPSec NAT-T、 PPTP の VPN パススルー、L2TP、IPSec

ルーティング

	スタティック、RIP v1、v2 VLAN 間ルーティング

レイヤ 2

VLAN	ポート ベース、802.1Q タグ ベース VLAN
VLAN 数	4 つの 802.1Q VLAN（VLAN ID 範囲：1 ～ 4094）をサポート
ポート ミラーリング	5 個の WAN/LAN ポートのうち 1 個を指定の LAN ポートにミラーリング可能
RSTP	高速スパニング ツリー プロトコルによりループ検出および迅速な再コンフィギュレーションをサポート

環境

寸法	170 mm × 41 mm × 170 mm
W × H × D	（6.69 インチ × 1.61 インチ × 6.69 インチ）
装置重量	0.38 kg（0.84 ポンド）
電源	12V 1A
適合認定	FCC Class B、CE、ICES-003
動作温度	0 ～ 40˚C（32 ～ 104˚F）
保管温度	-20 ～ 70˚C（-4 ～ 158˚F）
動作湿度	10 ～ 85%、結露なきこと
保管湿度	5 ～ 90%、結露なきこと

仕様は、予告なしに変更されることがあります。

G

関連情報

シスコでは、お客様が Cisco RVS4000 4 ポート ギガビット VPN セキュリティ ルータの利点を最大限に活用するために利用できる幅広いリソースを提供しています。

サポート	
日本のシスコ サポートコミュニティ	https://supportforums.cisco.com/community/netpro/small-business/international/japan2
スモール ビジネス保証とサポート	http://www.cisco.com/web/JP/solution/small_business/support/index.html
ソフトウェア ダウンロード	http://www.cisco.com/cisco/software/navigator.html
スモール ビジネス FindIT ユーティリティのダウンロード	http://www.cisco.com/web/JP/solution/small_business/tools/download.html
製品マニュアル	
シスコ スモール ビジネス ルータ：リソース	http://www.cisco.com/web/JP/solution/small_business/index.html
シスコ スモール ビジネス	
シスコ スモール ビジネス日本語ホームページ	http://www.cisco.com/web/JP/solution/small_business/index.html

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受像機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

接続ケーブル、電源コード、ACアダプタなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因になります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）ではなくUL認定（ULまたはCSAマークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。