



## Tunneling Protocols

トンネリング・プロトコルは、バーチャル・プライベート・ネットワークの中核です。このトンネル機能は、インターネットなどのパブリック TCP/IP ネットワークを使用して、複数のリモート・ユーザと特定の企業のプライベート・ネットワークで安全が確保された接続を構築することができます。

この安全性が確保された接続はトンネルと呼ばれています。VPN 3000 Concentrator シリーズでは、トンネリング・プロトコルを使用して、次の機能を実行します。

- トンネル・パラメータをネゴシエーションする
- トンネルを確立する
- ユーザとデータを認証する
- セキュリティ・キーを管理する
- データの暗号化と復号を行う
- トンネル全体でのデータ転送を管理する
- トンネルのエンドポイントまたはルータとして、データ転送の着信と発信を管理する

VPN Concentrator は、両方向のトンネル・エンドポイントとして機能します。すなわち、VPN Concentrator は、プライベート・ネットワークからプレーン・パケットを受信し、受信したデータをカプセル化し、トンネルを構築したうえで、トンネルの相手側にカプセル化したパケットを送信します。トンネルの相手側では、パケットのカプセル化を解除し、最終宛先に送信します。また一方では、VPN Concentrator は、カプセル化されたパケットをパブリック・ネットワークから受信し、そのカプセル化を解除し、プライベート・ネットワーク上の最終の宛先に送信します。

VPN Concentrator は、次の 3 つの一般的な VPN トンネリング・プロトコルをサポートしています。

- PPTP ポイントツーポイント・トンネリング・プロトコル
- L2TP レイヤ 2 トンネリング・プロトコル
- IPSec IP セキュリティ・プロトコル

また、VPN Concentrator は、L2TP over IPSec もサポートします。L2TP over IPSec は、Windows 2000 VPN クライアントとの相互運用性を提供します。また、L2TP/IPSec 標準に準拠するその他のクライアントとも相互運用可能ですが、正式にそれらのクライアントをサポートしているわけではありません。

このセクションでは、PPTP と L2TP に対するシステム全体のパラメータを設定する方法、IPSec LAN-to-LAN の接続を設定する方法、および IPSec Security Association と LAN-to-LAN 接続用の、IKE プロポーザルを設定する方法について説明します。

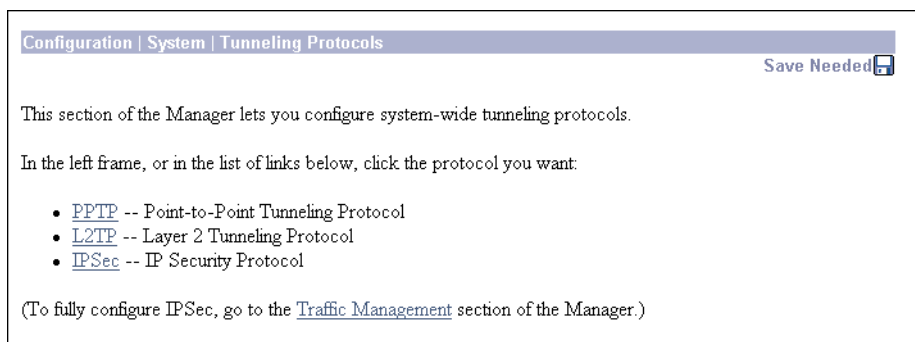
L2TP over IPSec を設定するには、[Configuration | System | Tunneling Protocols | IPSec | IKE Proposals](#) および [Configuration | User Management](#) を参照してください。

## Configuration | System | Tunneling Protocols

VPN Concentrator Manager のこの「Tunneling Protocols」セクションでは、トンネリング・プロトコルに対するシステム全体のパラメータを設定します。

- **PPTP** PPTP パラメータを設定します。
- **L2TP** L2TP パラメータを設定します。
- **IPSec** IPSec パラメータと接続を設定します。
  - **LAN-to-LAN** 2 台の VPN Concentrator 間(または VPN Concentrator と別のセキュア・ゲートウェイ間)の IPSec LAN-to-LAN の接続
  - **IKE Proposals** IPSec Security Association と LAN-to-LAN 接続に対する IKE プロポーザル

図 7-1 Configuration | System | Tunneling Protocols の画面



## Configuration | System | Tunneling Protocols | PPTP

この画面では、システム全体に関わる PPTP (ポイントツーポイント・トンネリング・プロトコル) パラメータを設定します。

PPTP プロトコルでは、トンネルの確立と、制御するメカニズムを定義しますが、データ転送には、ジェネリック・ルーティング・カプセル化 (GRE) を使用します。

PPTP は、クライアント・サーバ・プロトコルです。VPN Concentrator は、常に PPTP Network Server (PNS) として機能し、リモート PC クライアントをサポートします。PPTP トンネルは、PC から VPN Concentrator に達しています。

PPTP は、Microsoft クライアントでよく使用されます。Windows 95/98 での Microsoft ダイアルアップ・ネットワーク (DUN) 1.2 および 1.3 は、Windows NT 4.0 および Windows 2000 のバージョンと同様に、PPTP をサポートしています。PPTP は、通常、Microsoft encryption (MPPE) と連携して使用されます。

PPTP は、フィルタ内のルールに従って設定します。**Configuration | Policy Management | Traffic Management** を参照してください。また、グループとユーザにも PPTP パラメータがあります。**Configuration | User Management** を参照してください。

図 7-2 Configuration | System | Tunneling Protocols | PPTP の画面



(注) Cisco 社は、PPTP パラメータのデフォルト設定値を提供しています。このデフォルト値は、一般的な VPN を使用する際の最適なパフォーマンスを確保します。Cisco 社の技術員から要請がある場合を除いて、このデフォルト値を変更しないように、強くお勧めします。

## Enabled

VPN Concentrator 上で PPTP 機能をシステム全体で使用可能にする場合は、このボックスにチェックマークを付けてください。使用不可にする場合は、チェックマークを外してください。デフォルトでは、このボックスにチェックマークが付いています。



(注) PPTP を使用不可にすると、すべてのアクティブ PPTP セッションが終了します。

## Maximum Tunnel Idle Time

アクティブ・セッションをもたない確立済みの PPTP トンネルを切り離す前に待機する時間を、秒単位で入力します。トンネルがオープンしていると、システム・リソースを消費します。最後のセッションが終了した後、ただちにトンネルの接続を解除する（アイドル時間なし）場合には、0 を入力してください。最大値は 86400 秒（24 時間）です。デフォルト値は 5 秒です。

## Packet Window Size

システムが、受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を入力します。システムは、無応答の PPTP パケットを処理できるまで、待ち行列に入れておく必要があります。最小のパケット数は 0、最大は 32、デフォルトは 16 です。

## Limit Transmit to Window

クライアントの Packet Window Size に合わせて、送信する PPTP パケット数を制限する場合、このボックスにチェックマークを付けます。クライアントがウィンドウ違反を無視できる場合は、このウィンドウの制限を無視すると、パフォーマンスが向上します。デフォルトでは、このボックスにチェックマークが付いていません。

## Max. Tunnels

PPTP トンネルを同時にアクティブにする最大許容数を入力します。最小値は 0 です。最大値は、VPN Concentrator のモデルによって異なります。たとえば、モデル 3060 : 5000 です。トンネル数を制限しない場合は、0 を入力します（デフォルト）。

## Max. Sessions/Tunnel

PPTP トンネルごとに許可される最大セッション数を入力します。最小値は 0 です。最大値は、VPN Concentrator のモデルによって異なります。たとえば、モデル 3060 : 5000 です。セッション数を制限しない場合には、0 を入力します（デフォルト）。

## Packet Processing Delay

PPTP フロー・コントロール用のパケット処理遅延を入力します。このパラメータは、PPTP コントロール・パケット内でクライアントに送信されます。入力単位は、100 ミリ秒（0.1 秒）です。最大値は 65535、デフォルトは 1（0.1 秒）です。

## Acknowledgement Delay

確認応答を運ぶデータ・パケットがないときに、VPN Concentrator がクライアントに確認応答を送信するために待機する時間をミリ秒単位で入力します。即時確認応答を送信する場合には、0 を入力します。最小遅延は 50 ミリ秒、最大は 5000 ミリ秒、デフォルトは 500 ミリ秒です。

## Acknowledgement Timeout

確認応答が失われたことを判断する前、すなわち送信ウィンドウがクローズしている場合であっても、クライアントへの送信を再開する前に待機する時間を秒単位で入力します。最小値は 1 秒、最大値は 10 秒、デフォルト値は 3 秒です。

## Apply / Cancel

設定済みの PPTP 設定値を適用し、アクティブ・コンフィギュレーションに組み込む場合には、**Apply** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols** の画面に戻ります。



注意

---

アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

---

設定を破棄する場合には、**Cancel** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols** の画面に戻ります。

## Configuration | System | Tunneling Protocols | L2TP

この画面では、システム全体の L2TP (レイヤ 2 トンネリング・プロトコル) パラメータを設定できます。

L2TP は、クライアント・サーバ・プロトコルです。L2TP は、PPTP と L2F (Layer 2 Forwarding) の複数の機能を結合しているため、PPTP と L2F の後継プロトコルとみなされています。L2TP プロトコルは、トンネルの確立と制御、およびデータ転送の両方のメカニズムを定義します。

VPN Concentrator は、常に L2TP Network Server (LNS) として機能し、リモート PC クライアントをサポートします。L2TP トンネルは、PC から VPN Concentrator に達しています。クライアント PC が Windows 2000 を実行している場合、L2TP トンネルは、一般に、IPSec トランスポート接続上に階層化されます。

L2TP は、フィルタ内のルールに従って設定できます。**Configuration | Policy Management | Traffic Management** を参照してください。また、グループとユーザにも L2TP パラメータがあります。**Configuration | User Management** を参照してください。

図 7-3 Configuration | System | Tunneling Protocols | L2TP の画面



(注) Cisco 社は、L2TP パラメータのデフォルト設定値を提供しています。このデフォルト値は、一般的な VPN を使用する際の最適なパフォーマンスを確保します。Cisco 社の技術員から要請がある場合を除いて、このデフォルト値を変更しないように、強くお勧めします。

### Enabled

VPN Concentrator 上で L2TP 機能をシステム全体で使用可能にする場合に、このボックスにチェックマークを付けてください。使用不可にする場合は、チェックマークを外してください。デフォルトでは、このボックスにチェックマークが付いています。



(注) L2TP を使用不可にすると、アクティブ L2TP セッションがすべて終了します。

## Maximum Tunnel Idle Time

アクティブ・セッションをもたない、確立済みの L2TP トンネルを切り離す前に待機する時間を、秒単位で入力します。トンネルがオープンしていると、システム・リソースを消費します。最後のセッションが終了した後、ただちにトンネルの接続を解除する（アイドル時間なし）場合には、0 を入力してください。最大値は 86400 秒（24 時間）です。デフォルト値は 60 秒です。

## Control Window Size

システムが受信し、バッファに入れることができる、無応答の L2TP 制御チャネル・パケットの最大数を入力します。最小パケット数は 1、最大は 16、デフォルトは 4 です。

## Control Retransmit Interval

無応答の L2TP トンネル制御メッセージをリモート・クライアントに再送信する前に待機する時間を、秒数で入力します。最小値は 1 秒（デフォルト）、最大値は 10 秒です。

## Control Retransmit Limit

リモート・クライアントが応答しなくなったとみなす前に、L2TP トンネル制御パケットを再送信する回数を入力します。最小は 1 回、最大は 32 回、デフォルトは 4 回です。

## Max. Tunnels

L2TP トンネルを同時にアクティブにする最大許容数を入力します。最小値は 0 です。最大値は、VPN Concentrator のモデルによって異なります。たとえば、モデル 3060 : 5000 です。トンネル数を制限しない場合は、0 を入力します（デフォルト）。

## Max. Sessions/Tunnel

L2TP トンネルごとに許可される最大セッション数を入力します。最小値は 0 です。最大値は、VPN Concentrator のモデルによって異なります。たとえば、モデル 3060 : 5000 です。セッション数を制限しない場合には、0 を入力します（デフォルト）。

## Hello Interval

L2TP トンネルがアイドルである（制御パケットもペイロード・パケットも受信しない）ときに、Hello（または「キープアライブ」）パケットをリモート・クライアントに送信する前に待機する時間を、秒単位で入力します。最小値は 1 秒、最大値は 3600 秒、デフォルト値は 60 秒です。

## Apply / Cancel

設定済みの L2TP 設定値を適用し、アクティブ・コンフィギュレーションに組み込む場合には、Apply をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols** の画面に戻ります。



注意

---

アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

---

設定を破棄する場合には、**Cancel** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols** の画面に戻ります。

## Configuration | System | Tunneling Protocols | IPSec

このセクションでは、IPSec LAN-to-LAN の接続の設定、および IPSec Security Association と LAN-to-LAN 接続用の IKE ( Internet Key Exchange ) パラメータの設定をします。

IPSec は、VPN トンネル用の最も完全なアーキテクチャを備え、最も安全なプロトコルとみなされています。LAN-to-LAN 接続と client-to-LAN 接続はどちらも、IPSec を使用できます。

IPSec 用語では、「ピア」とは、リモート・アクセス・クライアントまたは別の保護ゲートウェイです。IPSec でのトンネル確立時に、2つのピアが、認証、暗号化、カプセル化、キー管理などを制御する Security Association をネゴシエーションします。このネゴシエーションには、2つの段階があります。最初の段階は、トンネルの確立 ( IKE SA ) であり、2番目の段階は、トンネル内のトラフィックの制御 ( IPSec SA ) です。

IPSec LAN-to-LAN 接続では、VPN Concentrator は発信側または応答側として機能することができます。IPSec client-to-LAN の接続では、VPN Concentrator は応答側としてのみ機能します。発信側が SA を提案し、応答側が、設定済みの SA パラメータにしたがって、その提案を受け入れるか、拒否するか、または代案を提案します。接続を確立するには、両方のエンティティが SA に合意する必要があります。

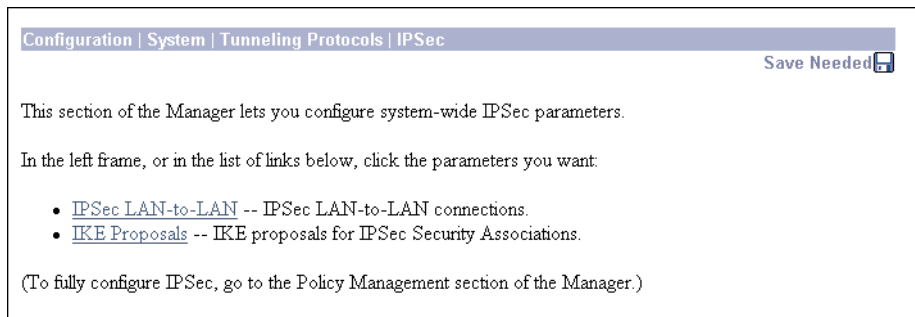
Cisco VPN Client は、IPSec プロトコルに準拠し、VPN Concentrator と連携して動作するように設計されます。しかし、VPN Concentrator は、プロトコル準拠の複数のクライアントとの IPSec 接続を確立できます。同様に、VPN Concentrator は、他のプロトコルに準拠する VPN デバイス ( 多くの場合、「セキュア・ゲートウェイ」と呼ばれます ) との LAN-to-LAN 接続を確立できます。

Cisco VPN Client は、次の IPSec 属性をサポートしています。

- Main モード。認証にデジタル証明書を使用する場合に、Phase 1 ISAKMP Security Association ( SA ) をネゴシエーションします。
- Aggressive モード。認証に事前共有キーを使用する場合に、Phase 1 ISAKMP Security Association ( SA ) をネゴシエーションします。
- 認証アルゴリズム
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- 認証モード
  - Preshared Keys
  - X.509 デジタル証明書
- Diffie-Hellman Group 1 および 2
- 暗号化アルゴリズム
  - DES-56
  - 3DES-168
  - ESP-NUL
- Extended Authentication ( XAuth )
- Mode Configuration ( ISAKMP Configuration Method と呼ばれます )
- Tunnel Encapsulation Mode

ここで IKE プロポーザル ( IKE SA のパラメータ ) を設定します。IKE プロポーザルを、このセクションの IPSec LAN-to-LAN の接続、および **Configuration | Policy Management | Traffic Management | Security Associations** の画面の IPSec SA に適用します。したがって、他の IPSec パラメータを設定する前に、IKE プロポーザルを設定しておく必要があります。Cisco 社は、デフォルトの IKE プロポーザルを提供していますが、アドミニストレータは使用または変更ができます。

図 7-4 Configuration | System | Tunneling Protocols | IPSec の画面



## Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN

このセクションでは、2 台の VPN Concentrator 間の IPSec LAN-to-LAN の接続の設定、追加、変更、および削除を行います。

VPN Concentrator は、他のプロトコルに準拠する VPN 保護ゲートウェイとの LAN-to-LAN 接続を確立できますが、以下の説明では、両側に VPN Concentrator があることを前提としています。ここで、「ピア」とは、相手側の VPN Concentrator または保護ゲートウェイのことです。

LAN-to-LAN 接続では、IPSec は、2 台の VPN Concentrator のパブリック・インターフェイス間にトンネルを構築します。VPN Concentrator は、それに応じて、プライベート LAN 上の複数のホストとの間の保護トラフィックをルート指定します。LAN-to-LAN 接続には、ユーザ設定もユーザ認証もありません。プライベート・ネットワーク上で設定されているすべてのホストは、接続の相手側にあるホストにいつでもアクセスできます。

パブリック・インターフェイスとして WAN 接続を使用する場合は、引き続きこのセクションで、LAN-to-WAN 接続を設定します。

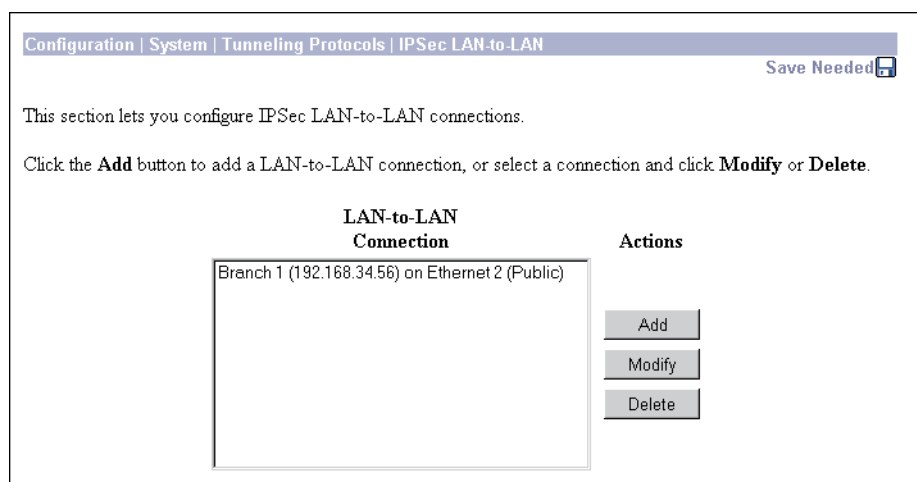
LAN-to-LAN 接続を完全に設定するには、両方の VPN Concentrator 上で同一の基本 IPSec パラメータを設定し、プライベート・ネットワーク・アドレスまたはネットワーク・リストのミラー・イメージを設定する必要があります。

また、VPN Concentrator は、ネットワーク・オートディスカバリ機能も備えています。この機能は、LAN-to-LAN 接続の両側にあるプライベート・ネットワーク・アドレスを動的に検出し、更新します。したがって、アドミニストレータは明示的にこれらのアドレスを設定する必要はありません。この機能が有効なのは、両方のデバイスが VPN Concentrator であるときに、両方の VPN Concentrator で、ルーティングがプライベート・インターフェイス上で使用可能になっている場合だけです。ただし、ネットワーク・オートディスカバリ機能は、WAN インターフェイスでは使用できません。

IPSec LAN-to-LAN の接続を設定する前に、VPN Concentrator 上でパブリック・インターフェイスを設定しておく必要があります。**Configuration | Interfaces** 画面を参照してください。また、LAN-to-LAN 接続を設定する前に、IKE プロポーザルも設定しておく必要があります。**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** の画面を参照してください。

各 VPN Concentrator (または他の保護ゲートウェイ) ピアとの LAN-to-LAN 接続は、1 つしか設定できません。

図 7-5 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN の画面



## LAN-to-LAN Connection

LAN-to-LAN Connection のリストは、設定済みの接続を表示します。この接続は、次の形式で、設定された順にリストされます。Name (Peer IP Address) on Interface。

たとえば、Branch 1 (192.168.34.56) on Ethernet 2 (Public) です。設定されている接続がない場合、このリストには、--Empty-- と表示されます。

## Add / Modify / Delete

新しい接続を設定し、追加する場合には、**Add** をクリックします。**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** の画面を参照してください。パブリック・インターフェイスを設定していない場合、VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces** の画面を表示します。

設定済みの接続のパラメータを変更する場合には、リストからその接続を選択し、**Modify** をクリックします。**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify** の画面を参照してください。

設定済みの接続を削除する場合には、リストからその接続を選択し、**Delete** をクリックしてください。**確認も取り消しありません**。VPN Concentrator Manager は、その接続、その接続の LAN-to-LAN フィルタ・ルール、SA、およびグループを削除します。VPN Concentrator Manager は、画面を最新表示し、リスト内に残っている接続を表示します。



(注)

注意接続を削除すると、その接続を使用するすべてのトンネル(およびユーザ・セッション)がただちに削除されます。



注意

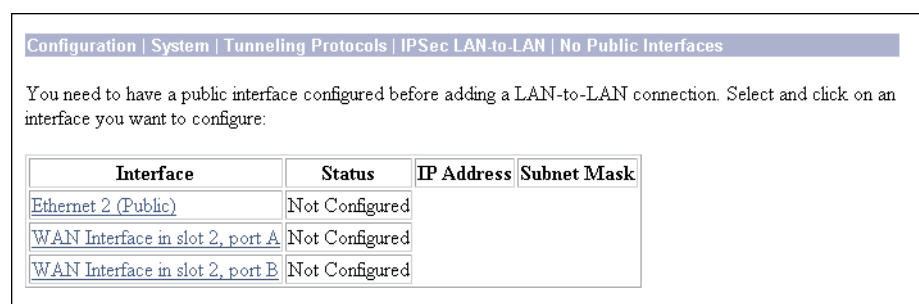
VPN Concentrator Manager は、アドミニストレータが加えた変更を、ただちにアクティブ・コンフィギュレーションに組み込みます。アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

## Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces

VPN Concentrator Manager がこの「No Public Interfaces」画面を表示するのは、アドミニストレータが VPN Concentrator 上でパブリック・インターフェイスを設定していないときに、IPSec LAN-to-LAN の接続を追加しようとした場合です。パブリック・インターフェイスを使用可能にする必要はありませんが、IP アドレスを指定してパブリック・インターフェイスを設定し、**Public Interface** パラメータを使用可能にする必要があります。

パブリック・インターフェイスとして指定できるのは、1 つの VPN Concentrator インターフェイスだけです。

図 7-6 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces の画面



強調表示されているリンクをクリックして、必要なパブリック・インターフェイスを設定してください。VPN Concentrator Manager は、該当する **Configuration | Interfaces** 画面を開きます。

## Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add または Modify

これらの画面では、次のことが可能です。

**Add** 新しい IPSec LAN-to-LAN の接続を設定し、追加します。

**Modify** 設定済みの IPSec LAN-to-LAN の接続のパラメータを変更します。

IPSec LAN-to-LAN の接続を設定する前に、VPN Concentrator 上でパブリック・インターフェイスを設定しておく必要があります。**Configuration | Interfaces** 画面を参照してください。

各 VPN Concentrator (または他の保護ゲートウェイ) ピアとの LAN-to-LAN 接続は、1 つしか設定できません。

サポートされている LAN-to-LAN 接続の最大数は、ハードウェアによって決まり、モデルにより異なります (表 7-1 を参照)。

**表 7-1 VPN Concentrator モデルごとの最大の LAN-to-LAN 接続数**

VPN Concentrator モデル	最大セッション数
3005	100
3015	100
3030	500
3060	1,000
3080	1,000

図 7-7 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add または Modify の画面

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

---

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

<b>Name</b> <input type="text"/>	Enter the name for this LAN-to-LAN connection.
<b>Interface</b> <input type="text" value="Ethernet 2 (Public) (192.168.12.34)"/>	Select the interface to put this LAN-to-LAN connection on.
<b>Peer</b> <input type="text"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
<b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
<b>Preshared Key</b> <input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
<b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
<b>Encryption</b> <input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
<b>IKE Proposal</b> <input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
<b>Network Autodiscovery</b> <input type="checkbox"/>	Check to automatically discover networks. <b>Parameters below are ignored if checked.</b>

---

**Local Network**

<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask.</b> A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.mnn addresses.
<b>Wildcard Mask</b> <input type="text"/>	

---

**Remote Network**

<b>Network List</b> <input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
<b>IP Address</b> <input type="text"/>	<b>Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask.</b> A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.mnn addresses.
<b>Wildcard Mask</b> <input type="text"/>	

上記の画面上で接続を **Add** または **Modify** すると、VPN Concentrator は次の処理を自動的にを行います。

- **Apply IPSec** アクションを使用して、2つのフィルタ・ルールを作成または変更します。すなわち、名前が L2L:<Name> In と L2L:<Name> Out の1つの着信ルールと1つの発信ルールです。
- IPSec Security Association (名前が L2L:<Name>) を作成または変更します。
- 上記の2つのルールをパブリック・インターフェイス上のフィルタに適用し、上記のSAをルールに適用します。パブリック・インターフェイスにフィルタがない場合は、上記のルールに Public (デフォルト) フィルタを適用します。

- Peer IP アドレス名付きのグループを作成、または変更します。VPN Concentrator の内部認証サーバが設定されていない場合は、内部認証サーバの設定を行い、このグループをデータベースに追加します。

すべてのルール、SA、フィルタ、およびグループには、デフォルトのパラメータ、またはこの画面上で指定されているパラメータがあります。ルールと SA の変更は **Configuration | Policy Management | Traffic Management** の画面上で、グループの変更は **Configuration | User Management | Groups** の画面上で、インターフェイスの変更は **Configuration | Interfaces** 画面上で行うことができます。しかし、設定済みのデフォルトを使用するようにお勧めします。これらのルール、SA、またはグループは個別に削除できません。LAN-to-LAN 接続を削除すると、システムは自動的にまとめて削除します。

LAN-to-LAN 接続を完全に設定するには、両方の VPN Concentrator 上で同一の IPSec LAN-to-LAN のパラメータを設定し、ローカルとリモートのプライベート・ネットワーク・アドレスの、ミラー・イメージを設定する必要があります。たとえば、次のとおりです。

設定対象	こちら側の VPN Concentrator	ピア VPN Concentrator
<b>Local Network</b>	10.10.0.0/0.0.255.255	11.0.0.0/0.255.255.255
<b>Remote Network</b>	11.0.0.0/0.255.255.255	10.10.0.0/0.0.255.255

ネットワーク・リストを使用する場合は、2つの VPN Concentrator 上でネットワーク・リストをミラー・イメージとして設定し、適用することも必要です。ネットワーク・オートディスカバリ機能を使用する場合は、両方の VPN Concentrator 上でこの機能を使用する必要があります。



(注)

Modify 画面では、**Apply** をクリックするとただちに、変更内容がすべて有効になります。クライアント・セッションがこの接続を使用している場合は、変更を加えると、警告なしにトンネル（およびセッション）が削除されます。

## Name

この接続に固有の記述名を入力します。最大 32 文字を入力してください。作成されたルールと SA がこの名前を使用するので、この名前を短くしておくことをお勧めします。

## Interface

### Add 画面の場合

ドロップダウン・メニュー・ボタンをクリックし、LAN-to-LAN 接続のこちら側に対して、この VPN Concentrator 上で設定されているパブリック・インターフェイスを選択します。このリストは、**Public Interface** パラメータが有効になっている、すべてのインターフェイス（Ethernet または WAN）を表示します。**Configuration | Interfaces** を参照してください。

### Modify 画面の場合

この画面は、LAN-to-LAN 接続のこちら側に対して、この VPN Concentrator 上で設定されているパブリック・インターフェイスを表示します。このインターフェイスは変更できません。別のインターフェイスとの接続に切り替えるには、この接続を削除し、別のインターフェイス用の新しい接続を追加する必要があります。

## Peer

LAN-to-LAN 接続のリモート・ピアの IP アドレスを入力します。これは、ピア VPN Concentrator 上のパブリック・インターフェイスの IP アドレスでなければなりません。ドット付き 10 進表記を使用してください。たとえば、192.168.34.56 です。

## Digital Certificate

このパラメータは、Phase 1 IKE のネゴシエーション時のピア認証に、事前共有 (Preshared) キーを使用するか、PKI (Public Key Infrastructure) のデジタル ID 証明書を使用するかを指定します。**Administration | Certificate Management** の説明を参照してください。

ドロップダウン・メニュー・ボタンをクリックし、オプションを選択してください。このリストは、インストールされているすべてのデジタル証明書に加えて、次の選択項目を表示します。

**None( Use Preshared Keys )** = Phase 1 IKE のネゴシエーション時のピアの認証に、事前共有キーだけを使用します。これがデフォルトの選択肢です。

## Preshared Key

この接続の事前共有キーを入力します。最小 4 文字、最大 32 文字の英数字を使用してください(たとえば、sZ9s14ep7)。システムは、入力内容を平文で表示します。

このキーは、作成される IPSec LAN-to-LAN のグループのパスワードになります。ピア VPN Concentrator 上で同じキーを入力する必要があります。(これは、手作業で入力する暗号化キーまたは認証キーではありません。システムが、これらのセッション・キーを自動的に生成します。)

## Authentication

このパラメータは、データ(すなわちパケット)の認証アルゴリズムを指定します。パケットの認証により、データの発信元が、予想通りの発信元であることが証明されます。これは、VPN 資料では、多くの場合、「データの整合性(データ・インテグリティ)」と呼ばれます。IPSec ESP( Encapsulating Security Payload ) プロトコルは、暗号化と認証の両方を提供します。

ドロップダウン・メニュー・ボタンをクリックし、アルゴリズムを選択してください。

**None** = データ認証なし。

**ESP/MD5/HMAC-128** = 128 ビット・キーを使用する MD5 ハッシュ関数を備えた HMAC( Hashed Message Authentication Coding ) を使用する、ESP プロトコル。これがデフォルトの選択肢です。

**ESP/SHA/HMAC-160** = 160 ビット・キーを使用する SHA-1 ハッシュ関数を備えた HMAC を使用する、ESP プロトコル。この選択項目の方が、安全ですが、必要な処理オーバーヘッドが増えます。

## Encryption

このパラメータは、データ(すなわちパケット)の暗号化アルゴリズムを指定します。データの暗号化により、代行受信された場合にデータが読み取れなくなります。

ドロップダウン・メニュー・ボタンをクリックし、アルゴリズムを選択してください。

**Null** = 暗号化なしに ESP を使用します。パケットを暗号化しません。

**DES-56** = 56 ビット・キーで DES 暗号化を使用します。

**3DES-168** = 168 ビット・キーで Triple-DES 暗号化を使用します。この選択項目は、安全度が最も高く、デフォルトの選択項目です。

## IKE Proposal

このパラメータは、IKE プロポーザルと呼ばれる、Phase 1 IPSec ネゴシエーションに対する一連の属性を指定します。**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** の画面を参照してください。LAN-to-LAN 接続を設定する前に、IKE プロポーザルの設定、アクティブ化、および優先順位付けを行っておく必要があります。

ドロップダウン・メニュー・ボタンをクリックし、IKE プロポーザルを選択してください。このリストは、アクティブな IKE プロポーザルだけを優先順位順に表示します。Cisco 提供のデフォルトのアクティブ・プロポーザルは、次のとおりです。

**CiscoVPNClient-3DES-MD5** = 認証に事前共有キー (XAUTH) と MD5/HMAC-128 を使用します。3DES-168 暗号化を使用してください。SA キーの生成には、D-H Group 2 を使用してください。この項目を選択すると、XAUTH ユーザ・ベース認証を使用できるようになります。これがデフォルトです。

**IKE-3DES-MD5** = 認証に事前共有キーと MD5/HMAC-128 を使用します。3DES-168 暗号化を使用してください。SA キーの生成には、D-H Group 2 を使用してください。

**IKE-3DES-MD5-DH1** = 認証に事前共有キーと MD5/HMAC-128 を使用します。3DES-168 暗号化を使用してください。SA キーの生成には、D-H Group 1 を使用してください。この選択項目は、Cisco VPN 3000 Client と両立性があります。

**IKE-DES-MD5** = 認証に事前共有キーと MD5/HMAC-128 を使用します。DES-56 暗号化を使用してください。SA キーの生成には、D-H Group 1 を使用してください。この選択項目は、Cisco VPN 3000 Client と両立性があります。

**IKE-3DES-MD5-DH7** = 認証に事前共有キーと MD5/HMAC-128 を使用します。3DES-168 暗号化を使用してください。SA キーの生成には、D-H Group 7 (ECC) を使用してください。この IKE プロポーザルは、movianVPN クライアントで使用するためのものです。また、D-H の ECC グループをサポートする任意のピアでも使用できます。

## Network Autodiscovery

VPN Concentrator のネットワーク・オートディスカバリ機能を使用して、LAN-to-LAN 接続の両側でプライベート・ネットワーク・アドレスを動的に検出し、継続して更新する場合に、このボックスにチェックマークを付けます。この機能は、RIP を使用します。両方の VPN Concentrator の Ethernet 1 (Private) インターフェイス上で、**Inbound RIP RIPv2/v1** が使用可能になっている必要があります。**Configuration | Interfaces** を参照してください。このボックスにチェックマークを付ける場合は、下記の **Local** および **Remote Network** パラメータをスキップしてください。これらのパラメータは無視されます。

ネットワーク・オートディスカバリ機能は、WAN インターフェイスでは使用できません。

## Local Network

これらの入力項目は、ホストが LAN-to-LAN 接続を使用できるこの VPN Concentrator 上のプライベート・ネットワークを指定します。これらの項目は、ピア VPN Concentrator 上の **Remote Network** セクションの項目と一致する必要があります。

## Network List

ドロップダウン・メニュー・ボタンをクリックして、ローカル・ネットワーク・アドレスを指定している設定済みのネットワーク・リストを選択してください。ネットワーク・リストとは、単一のオブジェクトとして扱われるネットワーク・アドレスのリストです。**Configuration | Policy Management | Traffic Management | Network Lists** の画面を参照してください。ネットワーク・リストを選択しない場合は、次の項目を選択することもできます。

Use IP Address/Wildcard-mask below. この項目を選択すると、ネットワーク・アドレスを入力できます。

Create new Network List (Add 画面のみ)。この項目を選択すると、ローカル・ネットワーク・アドレスのネットワーク・リストを作成できます。Add をクリックすると、VPN Concentrator Manager は、自動的に Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List の画面を表示します。下記の説明を参照してください。

設定済みのネットワーク・リストを選択する場合は、VPN Concentrator Manager は、IP Address と Wildcard Mask のフィールド内の入力内容を無視します。



(注)

必要な細分性を提供するために、IP アドレスは **ワイルドカード・マスク** と一緒に使用されます。**ワイルドカード・マスクは、サブネット・マスクの逆です**。つまり、ワイルドカード・マスクでは、ビット位置の 1 を無視し、ビット位置の 0 を一致させます。たとえば、次のとおりです。

---

0.0.0.0/255.255.255.255 = 任意のアドレス  
10.10.1.35/0.0.0.0 = 10.10.1.35 のみ  
10.10.1.35/0.0.0.255 = 10.10.1.nnn のアドレスすべて

---

## IP アドレス

この VPN Concentrator 上のプライベート・ローカル・ネットワークの IP アドレスを入力します。ドット付き 10 進表記を使用してください。たとえば、10.100.00.0 です。

## Wildcard Mask

プライベート・ローカル・ネットワークのワイルドカード・マスクを入力します。ドット付き 10 進表記を使用してください。たとえば、0.0.255.255 です。システムは、IP アドレス・クラスに適したデフォルトのワイルドカード・マスクを指定します。

## Remote Network

これらの入力項目は、ホストが LAN-to-LAN 接続を使用できるプライベート・ネットワーク (**リモート・ピア VPN Concentrator 上**) を指定します。これらの入力項目は、ピア VPN Concentrator 上の **Local Network** セクションの項目と一致する必要があります。

## Network List

ドロップダウン・メニュー・ボタンをクリックして、リモート・ネットワーク・アドレスを指定している設定済みのネットワーク・リストを選択してください。ネットワーク・リストとは、単一のオブジェクトとして扱われるネットワーク・アドレスのリストです。Configuration | Policy Management | Traffic Management | Network Lists の画面を参照してください。ネットワーク・リストを選択しない場合は、次の項目を選択することもできます。

Use IP Address/Wildcard-mask below. この項目を選択すると、ネットワーク・アドレスを入力できます。

Create new Network List (Add 画面のみ)。この項目を選択すると、リモート・ネットワーク・アドレスのネットワーク・リストを作成できます。Add をクリックすると、VPN Concentrator Manager は、自動的に Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Remote Network List の画面を表示します。下記の説明を参照してください。

設定済みのネットワーク・リストを選択する場合、Manager は、IP Address と Wildcard Mask フィールド内の入力内容を無視します。

前述の「Wildcard Mask」の項を参照してください。

## IP Address

リモート・ピア VPN Concentrator 上のプライベート・ネットワークの IP アドレスを入力します。ドット付き 10 進表記を使用してください。たとえば、11.00.1.0 です。

## Wildcard Mask

プライベート・リモート・ネットワークのワイルドカード・マスクを入力します。ドット付き 10 進表記を使用してください。たとえば、0.255.255.255 です。システムは、IP アドレス・クラスに適したデフォルトのワイルドカード・マスクを指定します。

## Add または Apply / Cancel

**Add** 画面の場合 設定済み LAN-to-LAN 接続のリストにこの接続を追加するには、**Add** をクリックしてください。新しいネットワーク・リストを作成する場合、VPN Concentrator Manager は、該当する **Local** または **Remote Network List** の画面を自動的に表示します。それ以外の場合は、マネージャは **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** の画面を表示します。

**Modify** 画面の場合 この LAN-to-LAN 接続に変更を適用するには、**Apply** をクリックしてください。**Apply** をクリックするとただちに、変更内容が有効になります。クライアント・セッションがこの接続を使用している場合は、変更を加えると、警告なしにトンネル（およびセッション）が削除されます。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** の画面に戻ります。



注意

---

VPN Concentrator Manager は、アドミニストレータが加えた変更を、ただちにアクティブ・コンフィギュレーションに組み込みます。アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

---

入力内容を破棄する場合には、**Cancel** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** の画面に戻り、**LAN-to-LAN Connection** のリストは変更されません。

## Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local または Remote Network List

これらの画面では、新しい IPSec LAN-to-LAN 接続の **Local Network**、または **Remote Network** に対してネットワーク・リストを設定し、追加します。**Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** の画面の **Network List** で **Create new Network List** を選択すると、VPN Concentrator Manager は自動的にこれらの画面を表示します。

ネットワーク・リストとは、単一のオブジェクトとして扱われるネットワーク・アドレスのリストです。**Configuration | Policy Management | Traffic Management | Network Lists** の画面も参照してください。

**Local Network List** 画面で、VPN Concentrator Manager は、この VPN Concentrator の Ethernet 1( Private ) インターフェイス用のルーティング・テーブル内にある有効なネットワーク・ルートを使用して、ネットワーク・リストを自動的に生成します ( **Monitoring | Routing Table** を参照 )

1 つのネットワーク・リストには、最大 200 個のネットワーク・エントリを指定できます。

図 7-8 Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local または Remote の Network List 画面

### List Name

VPN Concentrator Manager は、LAN-to-LAN ローカル・リスト、またはリモート・リストとしてリストを識別するデフォルト名を指定します。このデフォルト名を使用するようにお勧めします。デフォルト名を使用しない場合は、このネットワーク・リストに固有の名前を入力してください。大文字と小文字を区別して、最大 48 文字を入力してください。スペースを使用できます。

**Local Network List** の画面で **Generate Local List** の機能を使用する場合は、システムがこのネットワーク・リストを生成した後で、この名前を編集してください。

## Network List

このネットワーク・リスト内のネットワークを入力してください。1 行ごとにネットワークを入力します。形式は `n.n.n.n/w.w.w.w` を使用してください。この場合、`n.n.n.n` はネットワーク IP アドレスであり、`w.w.w.w` はワイルドカード・マスクです。



(注)

**ワイルドカード・マスク** を入力してください。ワイルドカード・マスクは、サブネット・マスクの逆です。つまり、ワイルドカード・マスクでは、ビット位置の 1 を無視し、ビット位置の 0 を一致させます。たとえば、`10.10.1.0/0.0.0.255` = すべての `10.10.1.nnn` アドレスです。

ワイルドカード・マスクを省略すると、Manager は、そのネットワーク・アドレスのクラスに対するデフォルトのワイルドカード・マスクを指定します。たとえば、`192.168.12.0` はクラス C のアドレスであり、デフォルトのワイルドカード・マスクは `0.0.0.255` です。

1 つのネットワーク・リストに最大 200 のネットワークを入力できます。

## Generate Local List

**Local Network List** 画面でこのボタンをクリックすると、VPN Concentrator Manager は、この VPN Concentrator の Ethernet 1 (Private) インターフェイス用のルーティング・テーブル内にある、最初の 200 個の有効なネットワーク・ルートを使用して、ネットワーク・リストを自動的に生成します (**Monitoring | Routing Table** を参照)。VPN Concentrator Manager は、このリストを生成した後で最新の画面を表示します。その後、**Network List** と **List Name** を編集できます。

## Add

設定済みのネットワーク・リストにこのネットワーク・リストを追加する場合に、**Add** をクリックしてください。VPN Concentrator Manager は、**Remote Network List** の画面か、**Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add | Done** の画面のどちらかを表示します。

## Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

新しい IPSec LAN-to-LAN 接続に対してすべてのパラメータを設定し終わったら、VPN Concentrator Manager はこの画面を表示します。この画面では、追加された設定エンティティを表示します。

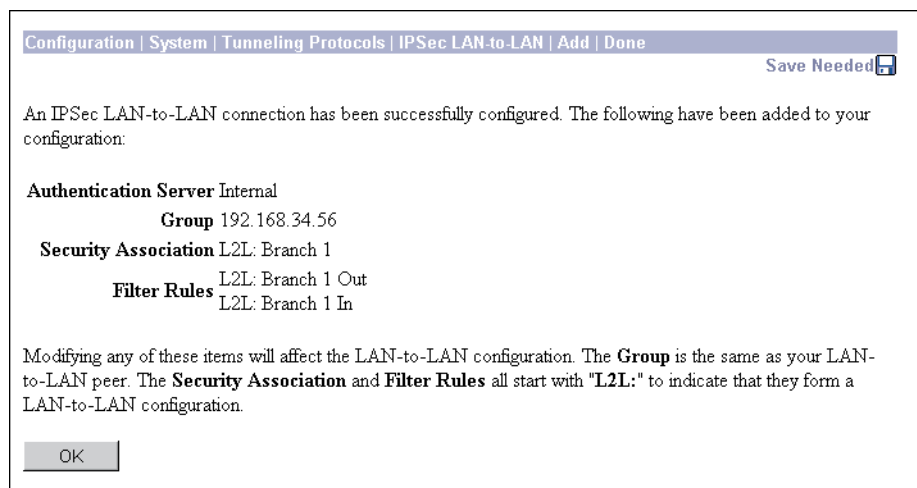
VPN Concentrator Manager は、この画面を一度だけ表示します。この画面のコピーを印刷して、記録用に保管しておくようにお勧めします。

エンティティを調べたり、変更したりする場合は、次の該当する画面を参照してください。

- **Group** Configuration | User Management | Groups を参照してください。
- **Security Association** Configuration | Policy Management | Traffic Management | Security Associations を参照してください。
- **Filter Rules** Configuration | Policy Management | Traffic Management | Rules を参照してください。

グループ、SA、またはルールを個別に削除することはできません。また、フィルタからルールを削除することもできません。LAN-to-LAN 接続を削除すると、システムはグループ、SA、およびルールを自動的に削除します。

**図 7-9** Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done の画面



OK

この画面をクローズし、Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN の画面に戻るには、OK をクリックしてください。LAN-to-LAN Connection リストは、新しい接続を表示します。VPN Concentrator Manager は、新しい設定値をすべて、アクティブ・コンフィギュレーションに組み込みます。



アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある Save Needed アイコンをクリックしてください。

## Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

このセクションでは、IKE プロポーザルの設定、追加、変更、アクティブ化、非アクティブ化、削除、および優先順位付けを行います。IKE プロポーザルは、Phase 1 IPSec ネゴシエーションに対する一連のパラメータです。Phase 1 中に、2 つのピアは、保護トンネルを確立し、その後、この保護トンネル内で Phase 2 パラメータをネゴシエーションします。

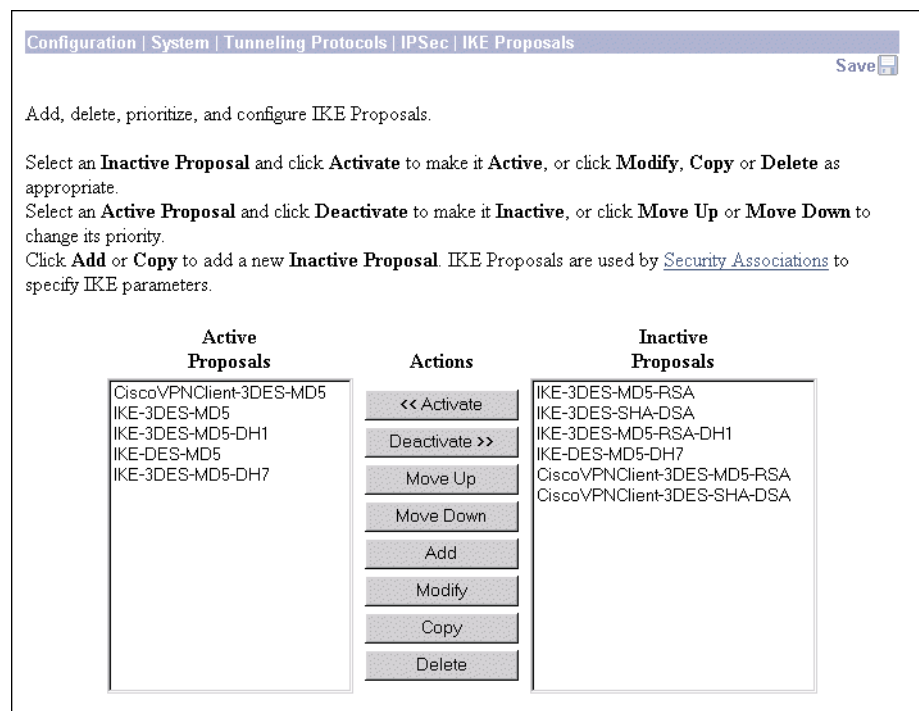
VPN Concentrator は、IPSec ネゴシエーションで、発信側と応答側の両方として IKE プロポーザルを使用します。LAN-to-LAN 接続では、VPN Concentrator は発信側または応答側として機能します。client-to-LAN 接続では、VPN Concentrator は応答側だけの機能をします。

IPSec Security Association を設定する前に、IKE プロポーザルを設定し、アクティブ化し、優先順位を付けておく必要があります。**Configuration | Policy Management | Traffic Management | Security Associations** を参照するか、この画面上の **Security Associations** リンクをクリックしてください。

また、IPSec LAN-to-LAN の接続を設定する前にも、IKE プロポーザルを設定し、アクティブ化しておく必要があります。上記の **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** を参照してください。

合計で最大 72 個の IKE プロポーザル (アクティブと非アクティブ) を設定できます。

図 7-10 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals の画面



Cisco 社は、アドミニストレータが使用または変更できるデフォルトの IKE プロポーザルを提供しています。表 7-2 を参照してください。パラメータの説明については、**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add** を参照してください。

表 7-2 Cisco 指定のデフォルト IKE プロポーザル

プロポーザル名	Authen.Mode	Authen. Algorithm	Encryption Algorithm	Diffie-Hellman Group	Lifetime Measurements	Data Lifetime	Time Lifetime
デフォルトでアクティブなプロポーザル							
CiscoVPNClient-3DES-MD5	Preshared Keys ( XAUTH )	MD5/ HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5	Preshared Keys	MD5/ HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-DH1	Preshared Keys	MD5/ HMAC-128	3DES-168	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-DES-MD5	Preshared Keys	MD5/ HMAC-128	DES-56	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-DH7	Preshared Keys	MD5/ HMAC-128	3DES-168	Group 7 (ECC) (163-bits)	Time	10000 KB	86400 sec
デフォルトでアクティブでないプロポーザル							
IKE-3DES-MD5-RSA	RSA Digital Certificate	MD5/ HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-SHA-DSA	RSA Digital Certificate	SHA/ HMAC-160	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
IKE-3DES-MD5-RSA-DH1	RSA Digital Certificate	MD5/ HMAC-128	3DES-168	Group 1 (768-bits)	Time	10000 KB	86400 sec
IKE-DES-MD5-DH7	Preshared Keys	MD5/ HMAC-128	DES-56	Group 7 (ECC) (163-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/ HMAC-128	3DES-168	Group 2 (1024-bits)	Time	10000 KB	86400 sec
CiscoVPNClient-3DES-SHA-DSA	DSA Digital Certificate (XAUTH)	SHA/ HMAC-160	3DES-168	Group 2 (1024-bits)	Time	100000 KB	86400 sec

## Active Proposals

このフィールドは、設定され、アクティブ化され、優先順位が付けられた IKE プロポーザルの名前を表示します。VPN Concentrator は、IPSec 応答側として、これらのプロポーザルを優先順位順にチェックして、発信側が提案する SA 内のパラメータと一致するプロポーザルを検出できるかどうかを調べます。

また、プロポーザルをアクティブ化すると、VPN Concentrator Manager が **IKE Proposal** リストを表示する場所で、プロポーザルを使用できるようになります。最初のアクティブ・プロポーザルがデフォルト選択項目として表示されます。

## Inactive Proposals

このフィールドは、設定されているにもかかわらず、非アクティブである IKE プロポーザルの名前を表示します。新しいプロポーザルは、初めて設定され、追加されるときに、このリストに表示されます。VPN Concentrator は、IPSec ネゴシエーションでこれらの非アクティブ・プロポーザルを使用しません。また、非アクティブ・プロポーザルは **IKE Proposal** リストにも表示されません。



(注)

L2TP over IPSec を設定する場合は、**IKE-3DES-MD5-RSA** をアクティブ化する必要があります。**Configuration | User Management** 画面も参照してください。

### << Activate

非アクティブな IKE プロポーザルをアクティブにするには、そのプロポーザルを **Inactive Proposals** リストから選択し、このボタンをクリックしてください。VPN Concentrator Manager は、そのプロポーザルを **Active Proposals** リストに移し、画面を最新表示します。

### >> Deactivate

アクティブな IKE プロポーザルを非アクティブにするには、そのプロポーザルを **Active Proposals** リストから選択し、このボタンをクリックしてください。そのアクティブ・プロポーザルが Security Association 上で設定されている場合、VPN Concentrator Manager はエラー・メッセージを表示します。非アクティブにする前に、そのプロポーザルを SA から削除する必要があります。Security Association 上で設定されていない場合は、VPN Concentrator Manager は、そのプロポーザルを **Inactive Proposals** リストに移し、画面を最新表示します。

### Move Up / Move Down

アクティブな IKE プロポーザルの優先順位を変更する場合は、そのプロポーザルを **Active Proposals** リストから選択し、**Move Up** または **Move Down** をクリックしてください。VPN Concentrator Manager は、画面を最新表示し、並べ替えられた **Active Proposals** リストを表示します。このアクションは、プロポーザルの位置を一つずつ、上または下に動かします。

### Add

新しい IKE プロポーザルを設定し、**Inactive Proposals** リストに追加する場合に、このボタンをクリックします。**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add** を参照してください。

### Modify

設定済みの IKE プロポーザルを変更する場合は、そのプロポーザルを **Active Proposals** または **Inactive Proposals** のどちらかから選択し、このボタンをクリックします。**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify** を参照してください。アクティブ・プロポーザルを変更すると、現在そのプロポーザルを使用している接続に影響するのではなく、後続の接続に影響を与えます。

## Copy

設定済みの IKE プロポーザルを、新しいプロポーザルの設定と追加のベースとして使用する場合には、そのプロポーザルを **Active Proposals** または **Inactive Proposals** のどちらかから選択し、このボタンをクリックします。Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy を参照してください。新しいプロポーザルが、**Inactive Proposals** リストに表示されます。

## Delete

設定済みの IKE プロポーザルを削除する場合は、そのプロポーザルを **Active Proposals** または **Inactive Proposals** のどちらかから選択し、このボタンをクリックしてください。アクティブ・プロポーザルが Security Association 上で設定されている場合、VPN Concentrator Manager はエラー・メッセージを表示します。削除する前に、そのプロポーザルを SA から削除する必要があります。**それ以外の削除の場合は、確認も取り消しありません**。VPN Concentrator Manager は、最新の画面を表示し、リスト内に残っている IKE プロポーザルを表示します。



### 注意

---

VPN Concentrator Manager は、アドミニストレータが加えた変更を、ただちにアクティブ・コンフィギュレーションに組み込みます。アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

---

## Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add、Modify または Copy

これらの画面では、次のことが可能です。

**Add** 新しい非アクティブな IKE プロポーザルを設定し、追加します。

**Modify** 設定済みの IKE プロポーザルを変更します。

**Copy** 設定済みの IKE プロポーザルをコピーし、そのパラメータを変更し、新しい名前を付けて保管し、設定済みの非アクティブな IKE プロポーザルに追加します。

合計で最大 25 個の IKE プロポーザル（アクティブと非アクティブ）を設定できます。

図 7-11 Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add、Modify または Copy の画面

The screenshot displays three overlapping configuration windows for IKE Proposals:

- Top Window (Copy):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy. Title: Copy a configured IKE Proposal.
- Middle Window (Modify):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify. Title: Modify a configured IKE Proposal.
- Bottom Window (Add):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add. Title: Configure and add a new IKE Proposal.

The 'Add' window contains the following fields and options:

- Proposal Name:** Text input field. Description: Specify the name of this IKE Proposal.
- Authentication Mode:** Dropdown menu (Preshared Keys). Description: Select the authentication mode to use.
- Authentication Algorithm:** Dropdown menu (MD5/HMAC-128). Description: Select the packet authentication algorithm to use.
- Encryption Algorithm:** Dropdown menu (3DES-168). Description: Select the encryption algorithm to use.
- Diffie-Hellman Group:** Dropdown menu (Group 2 (1024-bits)). Description: Select the Diffie Hellman Group to use.
- Lifetime Measurement:** Dropdown menu (Time). Description: Select the lifetime measurement of the IKE keys.
- Data Lifetime:** Text input field (10000). Description: Specify the data lifetime in kilobytes (KB).
- Time Lifetime:** Text input field (86400). Description: Specify the time lifetime in seconds.

Buttons: Add, Cancel.

### Proposal Name

この IKE プロポーザルに固有の名前を入力します。大文字と小文字を区別して、最大 48 文字を入力してください。スペースを使用できます。

### Authentication Mode

このパラメータは、リモート・クライアントまたはピアの認証方法を指定します。認証により、接続しているエンティティが、予想したエンティティであることが証明されます。デジタル証明書モードのいずれかを選択する場合は、該当するデジタル証明書を、この VPN Concentrator、およびリモート・クライアントまたはピアにインストールする必要があります。**Administration | Certificate Management** の説明を参照してください。

ドロップダウン・メニュー・ボタンをクリックし、次の方式を選択してください。

**Preshared Keys** = 事前共有キーを使用します (デフォルト)。このキーは、ユーザのグループまたはピアのグループのパスワードから得られます。

**RSA Digital Certificate** = RSA アルゴリズムによって生成されたキーを備えたデジタル証明書を使用します。

**DSA Digital Certificate** = DSA アルゴリズムによって生成されたキーを備えたデジタル証明書を使用します。

**Preshared Keys ( XAUTH )** = 事前共有キーを使用します (デフォルト)。このキーは、ユーザのグループまたはピアのグループのパスワードから得られます。XAUTH を介したユーザ・ベースの認証が必要です。

**RSA Digital Certificate ( XAUTH )** = RSA アルゴリズムによって生成されたキーを備えたデジタル証明書を使用します。XAUTH を介したユーザ・ベースの認証が必要です。

**DSA Digital Certificate ( XAUTH )** = DSA アルゴリズムによって生成されたキーを備えたデジタル証明書を使用します。XAUTH を介したユーザ・ベースの認証が必要です。

### ユーザ・ベースの認証

VPN 3000 Client と VPN Client に対するユーザ・ベースの認証は、設定方法が異なります。VPN 3000 Client の場合、ユーザ・ベースの認証は、**Configuration | User Management | Groups | Add または Modify** で設定します。VPN Client に対するユーザ・ベースの認証を設定する場合には、次の手順を実行してください。

まず、**Configuration | User Management | Groups Add または Modify ( IP Sec タブ )**で、**Authentication** オプションを選択します。

次に、**Configuration | System | Tunneling Protocols | IPsec | IKE Proposals** で、両立可能な IKE プロポーザルを選択し、この IKE プロポーザルを、アクティブ IKE プロポーザルのリストの高い位置に指定します。

両立可能な IKE プロポーザルとは、名前が **CiscoVPNClient** で始まるプロポーザルです。独自の両立可能な IKE プロポーザルを作成することもできます。新しい IKE プロポーザルを作成したい場合は、**Configuration | System | Tunneling Protocols | IPsec | IKE Proposals | Add または Modify** で、次の **Authentication Mode** オプションのいずれかを選択してください。すなわち、**Preshared Keys ( XAUTH )**、**RSA Digital Certificate ( XAUTH )**、または **DSA Digital Certificate ( XAUTH )** のいずれかです。

## Authentication Algorithm

このパラメータは、データ (すなわちパケット) の認証アルゴリズムを指定します。データは、パケットの認証により予想した発信元から発信されたことが証明されます。

ドロップダウン・メニュー・ボタンをクリックし、アルゴリズムを選択してください。

**MD5/HMAC-128** = 128 ビット・キーを使用する MD5 ハッシュ関数を備えた HMAC ( Hashed Message Authentication Coding )。これがデフォルトの選択肢です。

**SHA/HMAC-160** = 160 ビット・キーを使用する SHA-1 ハッシュ関数を備えた HMAC。この選択項目の方が、安全ですが、必要な処理オーバーヘッドが増えます。

## Encryption Algorithm

このパラメータは、データ (すなわちパケット) の暗号化アルゴリズムを指定します。データの暗号化により、代行受信された場合にデータが読み取れなくなります。

ドロップダウン・メニュー・ボタンをクリックし、アルゴリズムを選択してください。

**DES-56** = 56 ビット・キーを使用する DES 暗号化。

**3DES-168** = 168 ビット・キーを使用する Triple-DES 暗号化。これが、デフォルトの選択項目であり、安全度が最も高くなります。

## Diffie-Hellman Group

このパラメータは、IPSec SA キーの生成に使用される Diffie-Hellman グループを指定します。Diffie-Hellman 技法は、素数と「generator」数を使用して、キーを生成します。

ドロップダウン・メニュー・ボタンをクリックし、次のグループを選択してください。

**Group 1 (768-bits)** = Diffie-Hellman Group 1 を使用して、IPSec SA キーを生成します。この場合、素数と generator 数は 768 ビットです。上記の **Encryption Algorithm** で **DES-56** を選択した場合は、このオプションを選択してください。

**Group 2 (1024-bits)** = Diffie-Hellman Group 2 を使用して、IPSec SA キーを生成します。この場合、素数と generator 数は 1024 ビットです。これは、上記の **3DES-168 Encryption Algorithm** で使用する場合のデフォルトの選択項目です。

**Group 7 (ECC)** = Diffie-Hellman Group 7 を使用して、IPSec SA キーを生成します。この場合、楕円曲線フィールドのサイズは 163 ビットです。このオプションは、任意の暗号化アルゴリズムで使用できます。このオプションは、movianVPN クライアントで使用するためのものですが、Group 7 (ECC) をサポートする任意のピアで使用できます。

## Lifetime Measurement

このパラメータは、IKE SA キーの存続時間を測定する方法を指定します。存続時間とは、IKE SA が終了するまで続く期間であり、新しいキーを使用する場合は、ネゴシエーションし直す必要があります。このパラメータは、下記の **Data Lifetime** または **Time Lifetime** パラメータと一緒に使用されます。



(注) ピアが規定する存続測定法 (lifetime measurement) が短い場合は、VPN Concentrator はピアの測定法を使用します。

ドロップダウン・メニュー・ボタンをクリックし、測定方式を選択してください。

**Time** = SA の存続時間の測定に時間 (秒数) を使用します (デフォルト)。下記の **Time Lifetime** パラメータを設定してください。

**Data** = SA の存続時間の測定にデータ (キロバイト数) を使用します。下記の **Data Lifetime** パラメータを設定してください。

**Both** = 存続時間の測定に、時間とデータで、どちらか先に発生した方を使用します。 **Time Lifetime** と **Data Lifetime** の両方のパラメータを設定してください。

**None** = 存続時間の測定なし。SA は、他の理由で終了するまで、存続します。最大存続時間は、86400 秒 (24 時間) です。

## Data Lifetime

上記の **Lifetime Measurement** で **Data** または **Both** を選択した場合は、IKE SA が終了した後に限界となる、ペイロード・データのキロバイト数を入力します。最小は 100 KB、デフォルト 10000 KB、最大は 2147483647 KB です。

## Time Lifetime

上記の **Lifetime Measurement** で **Time** または **Both** を選択した場合は、IKE SA が終了するまでの秒数を入力します。最小は 60 秒、デフォルトは 86400 秒 (24 時間)、最大は 2147483647 秒 (約 68 年) です。

## Add または Apply / Cancel

### Add または Copy 画面の場合

この IKE プロポーザルを **Inactive Proposals** リストに追加するには、**Add** または **Apply** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** の画面に戻ります。新しいプロポーザルを使用する場合は、その画面に説明されている通りに、そのプロポーザルをアクティブにし、優先順位を付ける必要があります。

### Modify 画面の場合

この IKE プロポーザルに変更を適用するには、**Apply** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** の画面に戻ります。アクティブ・プロポーザルを変更すると、現在そのプロポーザルを使用している接続に影響するのではなく、後続の接続に影響を与えます。



注意

---

VPN Concentrator Manager は、アドミニストレータが加えた変更を、ただちにアクティブ・コンフィギュレーションに組み込みます。アクティブ・コンフィギュレーションを保管し、ブート・コンフィギュレーションにするには、Manager ウィンドウの上部にある **Save Needed** アイコンをクリックしてください。

---

設定を破棄する場合には、**Cancel** をクリックしてください。VPN Concentrator Manager は、**Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** の画面に戻り、IKE プロポーザルのリストは変更されません。

